Securing Wireless Infusion Pumps
In Healthcare Delivery Organizations

Volume C:
How-to Guides

Gavin O’Brien
National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

May 2017

DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/use-cases/medical-devices
DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.


FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: hit_nccoe@nist.gov.

Public comment period: May 8, 2017 through July 7, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries or broad, cross-sector technology challenges. Working with technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider. But today’s medical devices connect to a variety of health care systems, networks, and other tools within a healthcare delivery organization (HDO). Connecting devices to point-of-care medication systems and electronic health records can improve healthcare delivery processes, however, increasing connectivity capabilities also creates cybersecurity risks. Potential threats include unauthorized access to patient health information, changes to prescribed drug doses, and interference with a pump’s function.

The NCCoE at NIST analyzed risk factors in and around the infusion pump ecosystem using a questionnaire-based risk assessment to develop an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.
This practice guide will help HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk, while maintaining the performance and usability of wireless infusion pumps.

**KEYWORDS**

authentication; authorization; digital certificates; encryption; infusion pumps; Internet of Things; IoT; medical devices; network zoning; pump servers; questionnaire-based risk assessment; segmentation; VPN; Wi-Fi; wireless medical devices

**ACKNOWLEDGMENTS**

We are grateful to the following individuals for their generous contributions of expertise and time.

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arnab Ray</td>
<td>Baxter Healthcare Corporation</td>
</tr>
<tr>
<td>Pavel Slavin</td>
<td>Baxter Healthcare Corporation</td>
</tr>
<tr>
<td>Phillip Fisk</td>
<td>Baxter Healthcare Corporation</td>
</tr>
<tr>
<td>Raymond Kan</td>
<td>Baxter Healthcare Corporation</td>
</tr>
<tr>
<td>Tom Kowalczyk</td>
<td>B. Braun Medical Inc.</td>
</tr>
<tr>
<td>David Suarez</td>
<td>Becton, Dickinson and Company (BD)</td>
</tr>
<tr>
<td>Robert Canfield</td>
<td>Becton, Dickinson and Company (BD)</td>
</tr>
<tr>
<td>Rob Suarez</td>
<td>Becton, Dickinson and Company (BD)</td>
</tr>
<tr>
<td>Robert Skelton</td>
<td>Becton, Dickinson and Company (BD)</td>
</tr>
<tr>
<td>Peter Romness</td>
<td>Cisco</td>
</tr>
<tr>
<td>Kevin McFadden</td>
<td>Cisco</td>
</tr>
<tr>
<td>Rich Curtiss</td>
<td>Clearwater Compliance</td>
</tr>
<tr>
<td>Darin Andrew</td>
<td>DigiCert</td>
</tr>
<tr>
<td>Kris Singh</td>
<td>DigiCert</td>
</tr>
<tr>
<td>Mike Nelson</td>
<td>DigiCert</td>
</tr>
<tr>
<td>Chaitanya Srinivasamurthy</td>
<td>Hospira Inc., a Pfizer Company (ICU Medical)</td>
</tr>
</tbody>
</table>
The technology vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joseph Sener</td>
<td>Hospira Inc., a Pfizer Company (ICU Medical)</td>
</tr>
<tr>
<td>Chris Edwards</td>
<td>Intercede</td>
</tr>
<tr>
<td>Won Jun</td>
<td>Intercede</td>
</tr>
<tr>
<td>Dale Nordenberg</td>
<td>MDISS</td>
</tr>
<tr>
<td>Jay Stevens</td>
<td>MDISS</td>
</tr>
<tr>
<td>Carlos Aguayo Gonzalez</td>
<td>PFP Cybersecurity</td>
</tr>
<tr>
<td>Thurston Brooks</td>
<td>PFP Cybersecurity</td>
</tr>
<tr>
<td>Colin Bowers</td>
<td>Ramparts</td>
</tr>
<tr>
<td>Bill Hagestad</td>
<td>Smiths Medical</td>
</tr>
<tr>
<td>Axel Wirth</td>
<td>Symantec Corporation</td>
</tr>
<tr>
<td>Bryan Jacobs</td>
<td>Symantec Corporation</td>
</tr>
<tr>
<td>Bill Johnson</td>
<td>TDi Technologies, Inc.</td>
</tr>
<tr>
<td>Barbara De Pompa Reimers</td>
<td>The MITRE Corporation</td>
</tr>
<tr>
<td>Sarah Kinling</td>
<td>The MITRE Corporation</td>
</tr>
<tr>
<td>Marilyn Kupetz</td>
<td>The MITRE Corporation</td>
</tr>
<tr>
<td>David Weitzel</td>
<td>The MITRE Corporation</td>
</tr>
<tr>
<td>Mary Yang</td>
<td>The MITRE Corporation</td>
</tr>
<tr>
<td>Technology Partner/Collaborator</td>
<td>Build Involvement</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Baxter Healthcare Corporation**                        | • Sigma Spectrum LVP, version 8  
• Sigma Spectrum Wireless Battery Module, version 8  
• Sigma Spectrum Master Drug Library, version 8  
• CareEverywhere Gateway Server, version 14 |
| **B. Braun Medical Inc.**                                | • Infusomat® Space Infusion System/ Large Volume Pumps  
• DoseTrac® Infusion Management Software/ Infusion Pump Software |
| **Becton, Dickinson and Company (BD)**                   | • Alaris® 8015 PC Unit v9.19.2  
• Alaris® Syringe Module 8110  
• Alaris® LVP Module 8100  
• Alaris® Systems Manager v4.2  
• Alaris® System Maintenance (ASM) v 10.19 |
| **Cisco**                                                 | • Access Point (AIR-CAP1602I-A-K9)  
• Wireless LAN Controller 8.2.111.0  
• Cisco ISE  
• Cisco: ASA  
• Catalyst 3650 Switch |
| **Clearwater Compliance**                                | Clearwater: IRM | Pro |
| **DigiCert**                                             | CertCentral management account / Certificate Authority |
| **Hospira Inc., a Pfizer Company (ICU Medical)**         | • Plum 360™ Infusion System, version 15.10  
• LifeCare PCA™ Infusion System, version 7.02  
• Hospira MedNet™, version 6.2 |
<p>| <strong>Intercede</strong>                                            | MyID |
| <strong>MDISS</strong>                                                | MDRAP |</p>
<table>
<thead>
<tr>
<th>Technology Partner/Collaborator</th>
<th>Build Involvement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PFP Cybersecurity</strong></td>
<td>Device Monitor</td>
</tr>
<tr>
<td><strong>Ramparts</strong></td>
<td>Risk Assessment</td>
</tr>
<tr>
<td><strong>Smiths Medical</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Medfusion® 3500 V5 syringe infusion system</td>
</tr>
<tr>
<td></td>
<td>• PharmGuard® Toolbox v1.5</td>
</tr>
<tr>
<td></td>
<td>• Medfusion 4000® Wireless Syringe Infusion Pump</td>
</tr>
<tr>
<td></td>
<td>• CD, PHARMGUARD® TOOLBOX 2, V3.0 use with</td>
</tr>
<tr>
<td></td>
<td>Medfusion® 4000 and 3500 V6 (US)</td>
</tr>
<tr>
<td></td>
<td>• PharmGuard® Server Licenses, PharmGuard® Server</td>
</tr>
<tr>
<td></td>
<td>Enterprise Edition, V1.1</td>
</tr>
<tr>
<td></td>
<td>• CADD®-Solis Ambulatory Infusion Pump</td>
</tr>
<tr>
<td></td>
<td>• CADD™-Solis Medication Safety Software</td>
</tr>
<tr>
<td><strong>Symantec Corporation</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Endpoint Protection (SEP)</td>
</tr>
<tr>
<td></td>
<td>• Advanced Threat Protection: Network (ATP:N)</td>
</tr>
<tr>
<td></td>
<td>• Server Advanced - DataCenter Security (DCS:SA):</td>
</tr>
<tr>
<td><strong>TDi Technologies, Inc.</strong></td>
<td>ConsoleWorks</td>
</tr>
</tbody>
</table>
## Contents

1 **Introduction** ......................................................................................................................... 1
1.1 Practice Guide Structure ....................................................................................................... 1
1.2 Typographical Conventions .................................................................................................. 2
1.3 How-to Overview ................................................................................................................. 2
1.4 Logical Architecture Summary ............................................................................................. 2

2 **Product Installation Guides** .................................................................................................. 3
2.1 The Core Network .................................................................................................................. 3
   2.1.1 Cisco ASA Baseline Configuration ................................................................................ 4
   2.1.2 External Firewall and Guest Network .......................................................................... 4
   2.1.3 Enterprise Services ...................................................................................................... 5
   2.1.4 Biomedical Engineering Network ................................................................................ 5
   2.1.5 Medical Devices .......................................................................................................... 5
   2.1.6 Cisco Catalyst Switch Configuration .......................................................................... 6
   2.1.7 Cisco Enterprise Wi-Fi Infrastructure ........................................................................ 6
   2.1.8 TDi ConsoleWorks External Remote Access ............................................................... 12
2.2 Infusion Pump and Pump Server ........................................................................................... 21
   2.2.1 Infusion Pumps ............................................................................................................ 21
   2.2.2 Infusion Pumps Server Systems .................................................................................. 25
2.3 Identity Services ..................................................................................................................... 26
   2.3.1 Cisco Identity Service Engine (ISE) ........................................................................... 26
   2.3.2 DigiCert Certificate Authority .................................................................................... 31
2.4 Symantec Endpoint Protection and Intrusion Detection ......................................................... 36
   2.4.1 Symantec Data Center Security: Server Advanced ..................................................... 37
   2.4.2 Symantec Endpoint Protection Manager ..................................................................... 40
   2.4.3 Symantec Advanced Threat Protection: Advanced Threat Protection: Network ....... 41
2.5 Risk Assessment Tools ............................................................................................................ 43
   2.5.1 Clearwater IRM|Analysis™ Software ............................................................................ 43
   2.5.2 MDISS MDRAP ........................................................................................................... 52
Appendix A  Baseline Configuration File ......................................................... 61
Appendix B  Sample Pump Configuration Parameters................................. 239
Appendix C  References .................................................................................. 246
List of Figures

Figure 1-1: Logical Architecture Summary ................................................................. 3
Figure 2-1: Importing Server Certificate .................................................................... 30
Figure 2-2: Data Center Security: Server Advanced Environment .......................... 37
Figure 2-3: IRM|Analysis™ Login Page ................................................................. 43
Figure 2-4: Asset List ......................................................................................... 44
Figure 2-5: New Asset ............................................................................... 45
Figure 2-6: Media/Asset Groups .................................................................. 46
Figure 2-7: Edit Media/Asset Group ............................................................. 46
Figure 2-8: Controls - Global/Media ............................................................. 47
Figure 2-9: Risk Questionnaire List ............................................................... 48
Figure 2-10: Risk Questionnaire Form (part 1) .................................................. 48
Figure 2-11: Risk Questionnaire Form (part 2) .................................................... 49
Figure 2-12: Risk Response List - Risk Registry .............................................. 50
Figure 2-13: Risk Treat and Evaluate Form ..................................................... 50
Figure 2-14: Dashboard Example .................................................................. 51
Figure 2-15: Report Example .................................................................. 52
Figure 2-16: MDRAP Login Page .................................................................. 53
Figure 2-17: MDRAP Welcome page ............................................................... 54
Figure 2-18: Device Inventory List ................................................................. 54
Figure 2-19: Add Device ........................................................................... 55
Figure 2-20: Edit Device ........................................................................... 56
Figure 2-21: Inventory Bulk Import .............................................................. 56
Figure 2-22: Device inventory Template Sample ............................................... 57
Figure 2-23: Create Assessment (part 1) ............................................................ 58
Figure 2-24: Create Assessment (part 2) ............................................................ 58
Figure 2-25: Assessment Step (example 1) ....................................................... 59
Figure 2-26: Assessment Step (example 2) ....................................................... 59
Figure 2-27: Assessment Result (dashboard example) ................................................................. 60
Figure 2-28: Assessment Result (report example) ....................................................................... 60

List of Tables

Table 2-1: Infusion Pump List ...................................................................................................... 21
Table 2-2: Summary of Infusion Pump Configuration Methods ..................................................... 23
Table 2-3: Pump Servers used in this Example Implementation ................................................... 25
1 Introduction

The following guidelines show IT professionals and security engineers how the NCCoE implemented this example solution. We discuss every product that we employed in this reference design. We do not, however, recreate the product manufacturers’ documentation, which is widely available. Rather, these guidelines show how we integrated the products in our environment on your behalf.

Note: These guidelines are not comprehensive tutorials. Many possible service and security configurations for these products exist but are out of scope for this reference design.

1.1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and gives users the information they need to replicate all or parts of the example implementation that we built in our lab. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-8A: Executive Summary
- NIST SP 1800-8C: How-To Guides – instructions for building the example solution (you are here)

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers will be interested in the Executive Summary (NIST SP 1800-8A), which describes the:

- challenges enterprises face in securing the wireless infusion pump ecosystem
- example solution built at the NCCoE
- benefits of adopting the example solution

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in NIST SP 1800-8B, which describes what we did and why. The following sections will be of particular interest:

- Section 4, Risk Assessment and Mitigation, describes the risk analysis we performed
- Section 4.3, Security Characteristics and Control Mapping, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the Executive Summary, NIST SP 1800-8A, with your leadership team members to help them understand the importance of adopting standards-based, commercially available technologies that can help secure the wireless infusion pump ecosystem.

IT professionals who want to implement an approach like this will find the entire practice guide useful. You can use the How-To portion of the guide, NIST SP 1800-8C, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers’ documentation, which is generally widely available. Rather, we show how we incorporated the products in our environment to create an example solution.
This guide assumes that IT professionals have experience implementing security products within their enterprise. Although we have used a suite of commercial products to address this challenge, this guide does not endorse these products. Your organization can adopt this solution or one that adheres to these guidelines in part or in whole. Your organization’s security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. Vol B. section 4.4, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe the solution, but rather a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to hit_nccoe@nist.gov.

1.2 Typographical Conventions

The following table presents typographic conventions used in this volume.

<table>
<thead>
<tr>
<th>Typeface/Symbol</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Italics</em></td>
<td>filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders</td>
<td>For detailed definitions of terms, see the NCCoE Glossary.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>names of menus, options, command buttons and fields</td>
<td>Choose File &gt; Edit.</td>
</tr>
<tr>
<td>Monospace</td>
<td>command-line input, on-screen computer output, sample code examples, status codes</td>
<td>mkdir</td>
</tr>
<tr>
<td>Monospace Bold</td>
<td>command-line user input contrasted with computer output</td>
<td>service sshd start</td>
</tr>
<tr>
<td>blue text</td>
<td>link to other parts of the document, a web URL, or an email address</td>
<td>All publications from NIST’s National Cybersecurity Center of Excellence are available at <a href="https://nccoe.nist.gov">https://nccoe.nist.gov</a>.</td>
</tr>
</tbody>
</table>

1.3 How-to Overview

Refer to NIST SP 1800-8B: Approach, Architecture, and Security Characteristics for an explanation of why we used each technology.

1.4 Logical Architecture Summary

Below depicts a reference network architecture that performs groupings that would translate to network segments or zones. The rationale behind segmentation and zoning is to limit trust between...
areas of the network. In considering a hospital infrastructure, NCCoE identified devices and usage, and grouped them by usage. The grouping facilitated the identification of network zones. Once zones are defined, infrastructure components may be configured such that those zones do not inherently have network access to other zones within the hospital network infrastructure. Segmenting the network in this fashion limits the overall attack surface posed to the infusion pump environment, and considers the network infrastructure configuration as part of an overall defense in depth strategy. Figure 1-1 is included from the architecture for your reference.

Figure 1-1: Logical Architecture Summary

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring the products that NCCoE used to build an instance of the example solution.

2.1 The Core Network

The NCCoE’s example architecture implements a core network zone which is used to establish the backbone network infrastructure. The external firewall/router also has an interface connected to the core enterprise network, just like other firewall/router devices in the other zones. This zone serves as the backbone of the enterprise network and consists only of routers connected by switches. The routers automatically share internal route information with each other via authenticated Open Shortest Path First (OSPF) [1] to mitigate configuration errors as zones are added or removed.
Several functional segments may be part of this core network:

- guest network
- business office (example only)
- database server (example only)
- enterprise services
- clinical services (example only)
- biomedical engineering
- medical devices with wireless LAN
- remote access for external vendor support

The NCCoE build uses Cisco Adaptive Security Appliances (ASA) as virtual router and firewall devices within the network. Each defined zone in the hospital network we built has its own ASA, with two interfaces to protect the zone. As we considered how many ASAs to use, we opted for a tradeoff between the complexity of the configuration and the number of interfaces on a single ASA.

### 2.1.1 Cisco ASA Baseline Configuration

In our environment, all ASAs are virtualized and are based on Cisco’s Adaptive Security Virtual Appliance (ASAv) product. In your environment, the responsible person would complete installation by following Cisco’s *Adaptive Security Virtual Appliance (ASAv) Quick Start Guide, 9.6* [2].

We imported the virtual appliance called *asav-vi.ovf*, assigning the first interface to the management network, the second to the wide area network (WAN), and the third to the local area network (LAN). For an unknown reason, the `'show version'` command did not work in the console; as a workaround, we configured secure shell (SSH) [3] access and ran the command via SSH instead.

Then we configured the ASA with a baseline configuration template that allows all outbound traffic, but only related traffic inbound as allowed by the stateful firewall. Internet Control Message Protocol (ICMP) [4] enables troubleshooting with ping and traceroute tools. Authenticated OSPF automates routing tables as we added or removed ASAs in the network. In your production environment, you may wish to make different decisions in your baseline configuration. All ASAs have an additional management interface on 192.168.29.0/24. We opted to configure Simple Network Management Protocol (SNMP) [5] and SSH for management use on this interface, but not on the other interfaces. See Section A.1 for the ASA configuration for this zone.

### 2.1.2 External Firewall and Guest Network

We configured the build network to use network address translation (NAT) at the external firewall. This is the only point in the network where NAT is used. The upstream provider uses 10.0.0.0/8 addresses on the WAN interface. We also defined a LAN interface on 192.168.100.0/24 as the core network where other ASAs connect. Another interface is defined as `GUEST` on 192.168.170.0/24. We assigned the `GUEST` and LAN interfaces equal security levels higher than those for the WAN interface. When ASAs interfaces are configured with equal security levels, by default they cannot communicate with each other, but they will both have WAN access. Dynamic Host Configuration Protocol (DHCP) [6] is enabled on the `GUEST` interface for addressing. See Section A.2 for the ASA configuration for this zone.
2.1.3 Enterprise Services

We defined a LAN interface on 192.168.120.0/24 as the LAN for all enterprise services. Ports are open for domain name system (DNS) from the Biomedical Engineering network to the DNS servers. Port 8114 is open for all hosts to the Symantec Endpoint Protection server. Several ports are open for any host to the Symantec Data Center Security server.

See Section A.3 for the ASA configuration for this zone.

2.1.4 Biomedical Engineering Network

This zone contains a dedicated wireless network to support the wireless infusion pumps. We defined a LAN interface on 192.168.140.0/24 for all biomedical equipment, including infusion pump servers. Each manufacturer has a custom set of ports opened to their server. These ports are only accessible from the medical device network.

Generally, the firewall is configured in this way:

- All pump servers -> internet/intranet (all destinations)
- All intranet -> all pump servers Ping and Traceroute (primarily for debugging)
- All pumps -> Smiths Medical Pump Server on port 1588
- All pumps -> Carefusion Pump Server on port 3613
- All pumps -> Baxter Pump Server on port 51244
- All pumps -> Hospira Pump server on ports 443, 8443, 8100, 9292, 11443, 11444
- All pumps -> B. Braun Pump server on ports 443, 80, 8080, 1500, 4080

See Section A.4 for the ASA configuration for this zone.

2.1.5 Medical Devices

We defined a LAN interface on 192.168.150.0/24 as the LAN for all medical devices. The infusion pump systems are designed such that all external connections to the pumps, such as an EHR system or vendor maintenance, is completed with the associated pump server on the Biomedical Engineering network. This enables us to disallow all outbound traffic not destined for the Biomedical Engineering network. In addition, because some pump servers initiate connections to open ports on the pumps, we added vendor-specific rules to allow this. A DNS server is not useful in this case, but, if you needed one, we recommend that the ASA act as a forwarder. The DHCP server on the ASA is enabled for LAN addressing.

In our lab, we discovered that at least one brand of infusion pump would not recognize network setup as complete unless at least one DNS server address was set. In this case, the DNS server address only needed to be included in the configuration; a DNS server did not actually need to be present at that address.

Generally, the firewall is configured in this way:

- All pumps -> all pumps servers
- All intranet -> all pumps Ping and Traceroute (primarily for debugging)
Hospira Pump Server -> All pumps ports 8100, 9292, 443, 8443
Baxter Pump Server-> All pumps port 51243
B. Braun Pump Server -> All pumps ports 80, 443, 8080, 1500

See Section A.5 for the ASA configuration for this zone.

2.1.6 Cisco Catalyst Switch Configuration

The Catalyst 3650 switch is configured with four virtual LANs (VLANs) [7]. One port is assigned to a management VLAN, with subnet 192.168.20.0/24. Wireless access points are connected to a Wi-Fi management VLAN, which also is trunked back to the virtual WLAN controller software. Additionally, the Biomedical and Device networks have some physical ports configured for testing, both of which are also trunked back to the virtualization hardware and ASAs. DHCP is enabled for the wireless access points. SNMP and SSH are enabled for management. The switch also supports Power over Ethernet (PoE), allowing for a single Ethernet cable, with both data and power for the APs.

To set up your organization’s configuration, follow the instructions in Cisco’s Catalyst 3650 Switch Getting Started Guide:

See Section A.6 for the switch configuration.

2.1.7 Cisco Enterprise Wi-Fi Infrastructure

The Wi-Fi management network is different in that it does not have a firewall/router that connects directly to the core network. A completely closed network, this is used for management and communication between the Cisco Aironet wireless access points (AP) and the Cisco Wireless LAN Controller (WLC). The WLC is the central point where wireless service set identifiers (SSID), virtual LANs (VLAN), and Wi-Fi-protected access version 2 (WPA2) [8] security settings are managed for the entire enterprise. We defined two SSIDs: IP_Dev and IP_Dev_Cert. IP_Dev uses WPA2-PSK and IP_Dev_Cert uses WPA2-Enterprise protocols.

2.1.7.1 Installation

In our environment, the Cisco WLC is virtualized. In your environment, the responsible person would complete installation by following Cisco’s Virtual Wireless LAN Controller Deployment Guide 8.2:

We imported the virtual appliance called AIR_CTVM_K9_8_2_111_0.ova, assigning the first interface to the management network, referred to as service-port in the web interface. The second interface is used as a trunk port, with VLAN tags for all user and Wi-Fi management traffic. In the web interface, the built-in management interface refers to the wireless system control traffic network that the APs are connected to.

The primary management mechanism for the WLC is the web interface. To configure an IP address for the web interface, we first needed to use the console and complete the setup wizard that sets the service-port address. What follows is our process, which your organization can adapt to your needs.
2.1.7.2 Controller Configuration

Configure Network Interfaces:

1. Configure the interface for AP management traffic at Controller -> Interfaces -> Management.

<table>
<thead>
<tr>
<th>General Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
</tr>
<tr>
<td>MAC Address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine</td>
</tr>
<tr>
<td>Quarantine VLAN Id</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NAT Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable NAT Address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Identifier</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Netmask</td>
</tr>
<tr>
<td>Gateway</td>
</tr>
<tr>
<td>IPv6 Address</td>
</tr>
<tr>
<td>Prefix Length</td>
</tr>
<tr>
<td>IPv6 Gateway</td>
</tr>
<tr>
<td>Link Local IPv6 Address</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Number</td>
</tr>
<tr>
<td>Enable Dynamic AP Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DHCP Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary DHCP Server</td>
</tr>
<tr>
<td>Secondary DHCP Server</td>
</tr>
<tr>
<td>DHCP Proxy Mode</td>
</tr>
</tbody>
</table>

2. Configure interfaces for user Wi-Fi traffic, by first mapping the interface to an Ethernet port and setting the VLAN and IP address, and then mapping to wireless SSIDs.

Create the new interface at Controller -> Interfaces -> New.

<table>
<thead>
<tr>
<th>Interfaces &gt; New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
</tr>
<tr>
<td>VLAN Id</td>
</tr>
</tbody>
</table>

Configure the new interface by using the form below. Refer to the completed interface for the values that we used in the lab.
Our completed Interfaces list looks like the following:

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>VLAN Identifier</th>
<th>IP Address</th>
<th>Interface Type</th>
<th>Dynamic AP Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_dev</td>
<td>1500</td>
<td>192.168.150.2</td>
<td>Dynamic</td>
<td>Disabled</td>
</tr>
<tr>
<td>ip_dev_biomedical</td>
<td>1400</td>
<td>192.168.140.2</td>
<td>Dynamic</td>
<td>Disabled</td>
</tr>
<tr>
<td>management</td>
<td>1520</td>
<td>192.168.250.2</td>
<td>Static</td>
<td>Enabled</td>
</tr>
<tr>
<td>service-port</td>
<td>N/A</td>
<td>192.168.29.146</td>
<td>Static</td>
<td>Disabled</td>
</tr>
<tr>
<td>virtual</td>
<td>N/A</td>
<td>1.1.1.1</td>
<td>Static</td>
<td>Net Supported</td>
</tr>
</tbody>
</table>

Configure NTP [9] at Controller -> NTP -> Server -> New:

**NTP Servers > New**

Server Index (Priority) 2
Server IP Address (IPv4/IPv6) 192.168.250.1
Enable NTP Authentication

To configure the DHCP server, disable the DHCP Proxy at Controller -> Advanced -> DHCP.
2.1.7.3 Wireless AP Connection and Setup

Connect the APs to the Ethernet ports configured for untagged VLAN 1520. They will obtain their addresses and the WLC address automatically via DHCP from the switch (see Cisco Catalyst Switch Configuration in Section 2.1.6). No other VLANs should be configured for the APs because we are using a centralized switching model where Wi-Fi traffic VLANs are connected to the Enterprise network through the WLC.

As each AP is connected, it should show up in the Wireless tab on the WLC. For each AP, the AP Mode needs to be set to FlexConnect (see below).

2.1.7.4 Authentication Configuration

To use certificate-based authentication, the WLC must consult a RADIUS server. Configure Cisco ISE RADIUS server IP Address and Shared Secret at Security -> RADIUS -> Authentication -> New.

2.1.7.5 WLANs Configuration

At this point, we configured two SSIDs for medical devices: IP_Dev is configured for WPA2 (AES [10]) PSK, and IP_Dev_Cert is configured for WPA2 (AES) Enterprise. They both use the same interface and therefore connect to the same network VLAN; the only difference is the Wi-Fi security.

To create a new SSID, follow these steps:

1. Use the WLAN tab.

2. Enter your new SSID information.
3. In WLANs > WLANs > WLANs, select the WLAN ID number of the newly created SSID. Set Status to Enabled and Interface/Interface Group(G) to ip_dev.

4. On the Security tab under Authentication Key Management, uncheck 802.1X, check PSK, and set the PSK field.
For the SSID IP_Deve_Cert, repeat the steps above, but do not change the Security Settings for Authentication Key Management; leave 802.1X checked, and leave PSK unchecked.

On the Security, AAA Servers tab, select the RADIUS server to authenticate with.
2.1.7.6 Monitoring

By using Monitor -> Clients, you will find the list of currently connected clients, which SSID they are connected to, and the User Name used to authenticate (Common Name from Certificate).

<table>
<thead>
<tr>
<th>Client MAC Addr</th>
<th>IP Address(Ipv4/Ipv6)</th>
<th>WLAN Profile</th>
<th>WLAN SSID</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:17:23:8e:be:32</td>
<td>192.168.250.116</td>
<td>IP_Delay_Cert</td>
<td>IP_Delay_Cert</td>
<td>BBraun</td>
</tr>
<tr>
<td>00:17:23:5f:9f:db</td>
<td>192.168.250.123</td>
<td>IP_Delay</td>
<td>IP_Delay</td>
<td>Unknown</td>
</tr>
<tr>
<td>00:17:23:ff:ff:ff</td>
<td>192.168.250.118</td>
<td>IP_Delay_Cert</td>
<td>IP_Delay_Cert</td>
<td>Carefusion</td>
</tr>
<tr>
<td>00:18:67:86:6d:1f</td>
<td>192.168.250.126</td>
<td>IP_Delay</td>
<td>IP_Delay</td>
<td>Unknown</td>
</tr>
<tr>
<td>00:1d:05:dd:de:ec</td>
<td>192.168.250.125</td>
<td>IP_Delay</td>
<td>IP_Delay</td>
<td>Unknown</td>
</tr>
<tr>
<td>00:1d:05:dd:de:06</td>
<td>192.168.250.124</td>
<td>IP_Delay</td>
<td>IP_Delay</td>
<td>Unknown</td>
</tr>
<tr>
<td>00:80:82:5a:21:26</td>
<td>192.168.250.117</td>
<td>IP_Delay_Cert</td>
<td>IP_Delay_Cert</td>
<td>Hospira</td>
</tr>
</tbody>
</table>

2.1.7.7 Final Configuration


2.1.8 TDi ConsoleWorks External Remote Access

The NCCoE lab implemented a VendorNet using TDi ConsoleWorks, which is a browser interface that enables healthcare organizations to manage, monitor, and record activities from external vendors in the IT infrastructure.

System Environment:

The NCCoE lab set up a fully updated (as of 4/20/2016) CentOS 7 Operating System, with the following hardware specifications:

- 8GB RAM
- 40 GB HDD
- 1 Network Interface
Other requirements:

- ConsoleWorks install media (we built from a CD)
- ConsoleWorksSSL-<version>.rpm
- ConsoleWorks_gui_gateway-<version>.rpm
- ConsoleWorks license keys (`TDI_Licenses.tar.gz`)
- Software installation command

yum install uuid libpng12 libvncserver

Installation:

As Root:

1. Place ConsoleWorks Media into the system
2. `mount /dev/sr0 /mnt/cdrom`
3. `mkdir /tmp/consoleworks`
4. `cp /mnt/cdrom/consolew.rpm /tmp/consoleworks/consolew.rpm`
5. `rpm -ivh /tmp/consoleworks/ConsoleWorksSSL-<version>.rpm`
6. `mkdir /tmp/consoleworkskeys/`
7. Copy ConsoleWorks keys to `/tmp/consoleworkskeys/`
8. `cd /tmp/consoleworkskeys/`
9. `tar xzf TDI_Licenses.tar.gz`
10. `cp /tmp/consoleworkskeys* /etc/TDI_licenses/`
11. `/opt/ConsoleWorks/bin/cw_add_invo`
12. Accept the License Terms.
13. Press Enter to continue.
14. Name the instance of ConsoleWorks.
15. Press Enter to accept default port (5176).
16. Press N to deny SYSLOG listening.
17. Press Enter to accept parameters entered.
18. Press Enter to return to `/opt/ConsoleWorks/bin/cw_add_invo`.
19. `rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-version>.rpm`
20. `/opt/gui_gateway/install_local.sh`
21. `/opt/ConsoleWorks/bin/cw_start <invocation name created early>`
22. `service gui_gatewayd start`
Usage:

1. Open a browser and navigate to https://<ConsoleWorksIP>:5176.
3. Change the default password.
4. Choose Register Now.

NCCoE chose ConsoleWorks to segregate and limit vendor access to our labs. Our data model groups consoles and graphical connections together into a tag. The tag is a collection of equipment that you need to connect to, although a vendor typically owns the equipment. This tag allows us to operate on a group of consoles and graphical connections. We group users from the same vendor into a profile that allows us to operate on the users. An Access Control Rule associates a profile with a tag and defines permissions for a particular component type (typically consoles or graphical connections).

Initial Configuration of Graphical Gateway

Use the menu in the sidebar to access all instructions below.

Configure Graphical Gateway (only required for graphical connections such as virtual network computing, VNC; and remote desktop protocol, RDP):

1. Click on Graphical->Gateways->Add.
2. Set a name: LOCAL, then set Host as Localhost and port as 5172.
3. Check the Enabled box and click Save.
4. Verify that it works by clicking Test in the top-left corner.

Create one tag for each vendor company:

1. Click on Security->Tags->Add.
2. Set Name, usually the company name.
3. Click Save.
Create one profile for each vendor company.

1. Click on Users->Profiles->Add.
2. Set Name, usually the company name.
3. Click Save.

Establish graphical access controls. (Repeat this section for each vendor company.)

2. Set Name to Vendor_Company_Graphical.
3. Check Enabled.
4. Set Order.
5. Set Allow.
6. Set Component Type to Graphical Connection.
7. Look under Profile Selection; you should see:
   - Property Profile Equals *Vendor Company Profile Name* <join>.
   - Vendor company profile should appear in the box on right.
Look under Resource Selection; you should see:

- Associated with a Tag that
- Property Tag Equals *Vendor Company Tag name* <join>.

Matching Graphical Consoles should then appear in the box on right. Under Privileges, check:

- Aware
- View
- Connect

Console Access Controls (repeat this section for each vendor company):
1. Security->Access Control->Add
2. Set Name to Vendor_Company_Console.
3. Check Enabled.
4. Set Order.
5. Set Allow.
6. Set Component Type to Console.
7. Look at Profile Selection. You should see:
   - Property Profile Equals *Vendor Company Profile Name* <join>.
   - Vendor company Profile should appear in the box on right.
8. Look under Resource Selection; you should see:
   - Associated with a Tag that
   - Property Tag Equals *Vendor Company Tag name* <join>
9. Matching consoles should appear in the box on right. Under Privileges, check:
Users:

1. Set Name.
2. Set Password and retype password to confirm.
3. Fill in contact information.
4. Set Profile to the one defined for this user’s company.
5. Click Save.
RDP Graphical Connections
Follow these steps to add a RDP graphical connection:

1. Graphical->Add
2. Set Name for the device you are connecting to.
3. Set Type to RDP.
4. Set Hostname/IP for the device you are connecting to.
5. Set Authentication:
   - Username
   - Password
   - Domain (optional).
6. Add Graphical Gateway named Local.
7. Add Tags for all vendor companies that should have access.
8. Click Save.
SSH Console Connections

Follow these steps to add a SSH console connection:

1. Consoles->Add
2. Set Name for the device you are connecting to.
3. Set the Connector to SSH Session with Password Connection Details.
4. Set the Host IP for the device you are connecting to by doing the following:
   a. Set Port to 22.
   b. Set Username.
   c. Set Password.
   d. Retype the password.
5. Add tags for all vendor companies that should have access.
6. Click Save.
2.2 Infusion Pump and Pump Server

2.2.1 Infusion Pumps

Vendors collaborating with the NCCoE in this use case donated the following pump products.

Table 2-1: Infusion Pump List

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>Product Name</th>
<th>Product Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. Braun</td>
<td>SpaceStation</td>
<td>Station for hosting individual pump</td>
<td>Provides centralized power and network connection for pumps stacked on the station</td>
</tr>
<tr>
<td></td>
<td>Infusomat® Space</td>
<td>Wireless infusion pump</td>
<td>Designed for acute-care facilities for adults and children</td>
</tr>
<tr>
<td></td>
<td>large volume infusion pump</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perfusor® Space</td>
<td>Syringe infusion pump</td>
<td>Can be stacked in SpaceStation and uses SpaceStation for network communication</td>
</tr>
<tr>
<td></td>
<td>Syringe Pump</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Product Name</td>
<td>Product Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Baxter</td>
<td>Baxter Sigma Spectrum</td>
<td>Wireless infusion pump</td>
<td>Provides large-volume infusion capability for patients.</td>
</tr>
<tr>
<td>BD</td>
<td>Alaris PC 8015</td>
<td>Infusion pump core system</td>
<td>Provides a common user interface for programming infusion, network connection, and monitoring modules. The Alaris® 8015 PC Unit is the core of the Alaris® System and provides a common user interface for programming infusion and monitoring modules.</td>
</tr>
<tr>
<td></td>
<td>Alaris Syringe 8110</td>
<td>Syringe infusion pump</td>
<td>Provides syringe infusion capability for patients and it works with Alaris PC unit.</td>
</tr>
<tr>
<td></td>
<td>Alaris Pump 8100</td>
<td>Large-volume infusion pump</td>
<td>Provides large-volume infusion capability for patients and it works with Alaris PC unit.</td>
</tr>
<tr>
<td>Hospira</td>
<td>Plum 360</td>
<td>Infusion system</td>
<td>Builds on the air management and secondary delivery features of Plum A+, while expanding its drug library and wireless capability to enable streamlined electronic medical record integration.</td>
</tr>
<tr>
<td></td>
<td>Hospira PCA</td>
<td>PCA syringe infusion system</td>
<td>Complements Infusion pump to manage pain</td>
</tr>
<tr>
<td>Smiths Medical</td>
<td>MediFusion 4000</td>
<td>Syringe infusion pump</td>
<td>Delivers medication to patients in critical care units</td>
</tr>
<tr>
<td></td>
<td>CADD Solis 2000</td>
<td>Ambulatory infusion pump</td>
<td>Delivers medication to patients in hospital, home care, and alternative care facilities</td>
</tr>
</tbody>
</table>

### 2.2.1.1 Infusion Pump Setup

In our example solution, we generalized the infusion pump vendors’ products and systems as infusion pump devices, infusion pump servers, and infusion pump ecosystems. Our first goal was to connect each vendor’s infusion pump(s) to their corresponding pump server for performing the basic operational...
events, such as registering the devices to the server; pushing/installing the new drug library to the pumps; pushing/updating the new version of software to the pumps, and keeping the log of the pump usage.

Each pump vendor has a basic setup that includes configuring the pump to connect to the network and the pump server wirelessly. We used WPA2 security with Advanced Encryption Standard (AES) for encryption. In the case of WPA2-PSK mode, we assigned all infusion pumps the same access password for wireless network authentication. In the case of WPA2-Enterprise/EAP-TLS [11], we configured the pumps to use an individual certificate issued by DigiCert for wireless network authentication, using Cisco ISE, the enterprise authentication server.

Because each pump vendor has its own way of connecting, configuring, and setting up its pumps, we describe high-level steps in a generic way. The following table summarizes these key configuration steps. See Appendix B for the sample configuration files.

<table>
<thead>
<tr>
<th>Vendors</th>
<th>Infusion Pump Model</th>
<th>Configuration Tool</th>
<th>Connection Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baxter</td>
<td>Sigma Spectrum</td>
<td>Uses a PC with an IrDA interface to program multiple pumps with the same configuration. Edits the network configuration file (a simple text file) on a PC and send it via the IrDA to a pump.</td>
<td>Uses the IrDA Serial Infrared Link to a PC under the IrDA Serial Infrared Link Management Protocol v1.1.</td>
</tr>
<tr>
<td>B. Braun</td>
<td>Space Station</td>
<td>Connects PC with HiBaSeD Service program to the Space Station using a B. Braun interface cable for pump configuration setting.</td>
<td>Uses special B. Braun interface cable.</td>
</tr>
<tr>
<td></td>
<td>Infusomat® Space large volume infusion pump</td>
<td>Connects PC with HiBaSeD Service program to the Space Station using a B. Braun interface cable for pump configuration setting.</td>
<td>Uses special B. Braun interface cable.</td>
</tr>
<tr>
<td></td>
<td>Perfusor® Space Syringe Pump</td>
<td>Connects PC with HiBaSeD Service program to the Space Station using a B. Braun interface cable for pump configuration setting.</td>
<td>Uses special B. Braun interface cable.</td>
</tr>
<tr>
<td>BD</td>
<td>The Alaris® 8015 PC</td>
<td>Uses management system to do the configuration. The Alaris® 8015 PC Unit is</td>
<td>Uses series cable to connect pump to a local computer.</td>
</tr>
<tr>
<td>Vendors</td>
<td>Infusion Pump Model</td>
<td>Configuration Tool</td>
<td>Connection Methods</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hospira</td>
<td>Hospira PCA</td>
<td>Accesses Web Config utility on Pump through a web browser using the Local IP address of the pump</td>
<td>Uses pump's Ethernet Jack to connect to a LAN or to interface with host computer</td>
</tr>
<tr>
<td></td>
<td>Plum 360</td>
<td>Accesses Web Config utility on Pump through a web browser using the Local IP address of the pump</td>
<td>Uses pump's Ethernet Jack to connect to a LAN or to interface with host computer</td>
</tr>
<tr>
<td>Smiths Medical</td>
<td>MediFusion 4000</td>
<td>Pushes configuration text file to pump using the Telnet from a PC connected to the pump with the known IP address</td>
<td>Connects a PC to pump using micro USB-USB cable</td>
</tr>
<tr>
<td></td>
<td>CADD Solis 2000</td>
<td>Uses Smiths Medical Network Configuration Utility to update the pump’s configuration parameters</td>
<td>Connects a PC to pump using micro USB-USB cable</td>
</tr>
</tbody>
</table>

### 2.2.1.2 Infusion Pump Configuration

#### Pre-Conditions:

- You have set up wireless AP with pre-share password SSID
- You have installed and configured infusion pump servers
- You have made available the infusion pump configuration and setup manual available

#### Post-Conditions:

- You have connected the infusion pumps to AP
- You have estimated the pump server to discover the pumps to the corresponding pump server

NCCoE followed the pump vendors’ instructions to access to the pump in maintenance/biomedical model. We configured the pump as follows:

- For wireless properties
  - Enable wireless
  - Use DHCP
• Set SSID (IP_Dev or IP_Dev_Cert)

  ▪ For wireless security properties

    • Set Security Mode (WPA2-PSK or WPA2-Ent)
    • Set Encryption Protocol to AES/CCMP
    • Enter PSK password or install a PKI certificate

  ▪ For pump server properties

    • Set Server IP/port
    • Set Device Name or ID
    • Set Device Type

  ▪ To verify connectivity for each infusion pump and the corresponding pump server:

    • Connect pumps to AP (IP_Dev with PSK or IP_Dev_Cert with EAP-TLS)
    • Confirm that pump receives an IP address from the DHCP server from the AP
    • Confirm that the pump server can discover the pumps and display the pump status such connected, in use, or offline.

### 2.2.1.3 Infusion Pump Hardening

Hardening may include the following:

- disabling unused or unnecessary communication ports and services
- changing manufacture default administrative passwords
- securing the remote access points if there are any
- confirming the firmware version is up-to-date.

### 2.2.2 Infusion Pumps Server Systems

Table 2-3: Pump Servers used in this Example Implementation

<table>
<thead>
<tr>
<th>Vendor Name</th>
<th>Product Name</th>
<th>Operating Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B. Braun</td>
<td>DoseTrac® Infusion Management</td>
<td>Microsoft Windows</td>
<td>Drug library and infusion management system that provides real-time, infusion data reporting and analysis to add safety, efficiency and value</td>
</tr>
<tr>
<td>Baxter</td>
<td>Care Everywhere Infusion Pump Management System</td>
<td>Microsoft Windows</td>
<td>Provides interface capability to help hospital biomedical engineering department manage their infusion pump fleet</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Product Name</td>
<td>Operating Platform</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>BD</td>
<td>Alaris Systems Manager</td>
<td>Compatible with VMWare ESX and VMWare vSphere environment</td>
<td>Virtual server platform that provides two-way wireless communication with Alaris PC units</td>
</tr>
<tr>
<td>Hospira</td>
<td>Hospira MetNet Server</td>
<td>Microsoft Windows</td>
<td>Manages drug libraries, firmware updates, and configurations of intravenous pumps</td>
</tr>
<tr>
<td>Smiths Medical</td>
<td>PharmGuard Server</td>
<td>Microsoft Windows</td>
<td>Manages drug libraries, firmware updates, and configurations of Hospira intravenous pumps for Smiths Medical Pumps</td>
</tr>
</tbody>
</table>

NCCoE installed the pump servers in the network in the VLAN 1400. To do so, we prepared a virtual machine in the VMWare with the operating system and network as specified in the vendor installation manual. Because one or more database is associated with the infusion pump server for storing the data, installation and configuration of the database is part of the pump server installation procedure. After the installation, we implemented basic configuration: the user account setup, reporting template configuration, security hardening, license installation, pump metadata installation.

We have not included the pump server setup because the vendor performs this activity.

### 2.3 Identity Services

#### 2.3.1 Cisco Identity Service Engine (ISE)

The Cisco Identity Services Engine (ISE) enables your organization to:

- Centralize and unify identity and access policy management
- Have visibility and more assured device identification during certificate challenges
- Use business rules to segment access to sections of the network
- Make the user experience seamless during the challenge process, even with more assured and stronger authentication
System requirements

- Virtual Hypervisor (VH) capable of housing virtual machines (VMs)
- VM with CPU: Single Quad-core; 2.0 GHz or faster
- VM with minimum 4 GB memory
- VM with minimum 200 GB disk space

NCCoE installed the Cisco ISE 2.1 on a virtual machine using the OVA image provided by Cisco.

For your organization, follow the guidance from your VM vendor to import the OVA and start the install process. Once the system boots up, follow the console display to select one of the installation options.

The configuration parameter selected for this use case is shown below:

```bash
! hostname
ise
!ip domain-name
nccoe.lab
! ipv6
enable
!interface
GigabitEthernet 0 ip address 192.168.29.159 255.255.255.0 ipv6 address autoconfig ipv6 enable
! interface
GigabitEthernet 1 ip address 192.168.120.159 255.255.255.0 ipv6 address autoconfig ipv6 enable
! interface
GigabitEthernet 2 shutdown ipv6 address autoconfig ipv6 enable
! interface
GigabitEthernet 3 shutdown ipv6 address autoconfig ipv6 enable
! ip name-server
8.8.8.8 8.8.4.4
! ip default-gateway
192.168.120.1
!
! clock timezone
EST
! ntp server
```
time.nist.gov

! username admin password hash

$5$NPleEb4$YxDZH6oDF2Y4.02OqE/jBWxXFumRvte8JdNNZm1yj0 role admin

! max-ssh-sessions

5

! service sshd

enable

! password-policy

lower-case-required

upper-case-required

digit-required

no-username

no-previous-password

password-expiration-enabled

password-expiration-days 45

password-expiration-warning 30

min-password-length 4

password-lock-enabled

password-lock-timeout 15

password-lock-retry-count 3

! logging loglevel

6

! conn-limit 10

port 9060

! cdp timer

60 cdp holdtime 180 cdp run GigabitEthernet 0

! icmp echo

on

!
2.3.1.1 Configure ISE to Support EAP-TLS Authentication

Execute your management of the Cisco ISE with a web browser unless you intend to administer via command line. Using a web browser and the Cisco ISE host address, log on to the Cisco ISE Administration Portal. You will use the credentials (username and password) you created during the installation procedure.

2.3.1.2 Set ISE to Support RADIUS Authentication

Use the following steps to set up a communication connection from Cisco ISE to the network device (Access Point) you use as the authentication server during RADIUS [12] authentication:

1. Add a Network Resource

   From the ISE Admin Portal, navigate to the path: Administration > Network Resources > Network Devices. Then select Add. Fill out the required parameters as indicated in the form:

   - The name of the network device
   - The IP Address of the device with its subnet mask.

2. Select the RADIUS protocol as the selected protocol, and enter the shared secret that is configured on the network device.

3. Populate the system certificate with CA-signed certificates. We replaced the Cisco ISE default self-signed certificate with the CA-signed certificate issued through DigiCert Certificate Authority. The steps for acquiring the signing certificate from DigiCert are described in the next Section 2.3.2, DigiCert Certificate Authority.

4. Once the CA-signed certificate for ISE and the Root CA are issued, use the following steps to install the certificates to the System.

5. From the ISE Administration Portal, use the navigation path Administration > System > Certificates > System Certificate to show the installed certificates. Then select Import to open a screen for importing Server certificate. Fill in the required information as shown in the following screen shot.
Figure 2-1: Importing Server Certificate

6. Check the EAP Authentication to enable the imported certificate to be used for EAP Authentication. Then click the **Submit** button to complete the certificate importing.

7. Import the DigiCert Root CA and signing CA to ISE Trusted Certificates. From the ISE Administration Portal, use the navigation path **Administration > System > Certificates > Trusted Certificate** to show the installed certificates. Then select Import to open a screen for importing DigiCert Root CA and the signing CA individually.
   a. After importing, make sure the certificate status is Enabled.
   b. Establish the OCSP [13] client profile from the OCSP Client Profile page under the **Administration > System > Certificates > OCSP Client Profile**.
   c. If OCSP (Online Certificate Status Protocol) is used for Certificate Status Validation, check Validate against OCSP Service and enter the OCSP service name.

8. Set **Identity Source for Client Certificate Authentication**. When using the trusted certificate for EAP-TLS certificate-based authentication validation, set up the Certificate Authentication Profile in the ISE as the external identity source. Instead of authenticating via the traditional username and password, Cisco ISE compares the client certificate received from the Access Point to verify the authenticity of a device, in this case, the infusion pump.
To create a Certificate Authentication Profile:

- Use the Administration Portal to navigate to the path Administration > Identity Management > External Identity Sources > Certificate Authentication Profile and click Add.
- Name the profile as, for example, “Cert_Auth_Profile”, then fill out the form with proper parameters. Be sure to select Subject Name as the Principal Username X509 attribute because it is the field that will be used to validate the authenticity of the client.
- Select the Identity Resource Sequences tab, in the Certificate Based Authentication, check Select Certificate Authentication Profile and choose the Cert_Auth_Profile from the dropdown list.

9. Set Authentication Protocols. Cisco ISE uses authentication protocols to communicate with external identity sources. Cisco ISE supports many authentication protocols such as the Password Authentication Protocol (PAP), Protected Extensible Authentication Protocol (PEAP), and the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). For this build, we used the EAP-TLS protocol for user and machine authentication. To specify the allowed protocols services in Cisco ISE:

- From the Administration Portal navigate to the path Policy >Policy Elements > Results >Authentication > Allowed Protocols > Add
- Select the preferred protocol or list of protocols. In this build, the EAP_TLS is selected as the allowed authentication protocol.

10. Set up Authentication Policy. Define the authentication policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. To specify the authentication policy:

- From the Administration Portal navigate to the path Policy >Authentication Policy > Type > Rule Based.
- Set “if Protocol is Wireless 802.1x, use the Network Device as defined in Step 1 and the Identity Sequences as defined in Step 8.

2.3.2 DigiCert Certificate Authority

DigiCert is a cloud-based platform designed to provide a full line of SSL Certificates, tools, and platforms for optimal certificate life cycle management. After you set up an account with DigiCert, you can use a DigiCert dashboard and its built-in certificate management tools to issue PKI certificates for network authentication and encryption for data-at-rest or in-transition if needed.

The follow instruction describes the process we used to request a PKI certificate on behalf a wireless infusion pump using the DigiCert PKI services:

2.3.2.1 Create a Certificate Signing Request (CSR)

A CSR can be represented as a Base64 encoded PKCS#10 binary format. Many tools and utilities are available to help to generate a CSR, and the key pair containing the private key and public key is generated in the same time. The CSR identifies the applicant’s distinguished name, which must be digitally signed using the applicant’s private key and the information for the public key chosen for the applicant. In this build, Certificate Utility for Windows (DigiCertUtil.exe) provided by DigiCert is used to generate CSRs for infusion pumps.

1. Double-click DigiCertUtil.exe to start the utility:

2. Click the Create CSR link to open a CSR request window.

3. On the Create CSR window, fill in the key information (some is optional):
   - Certificate Type: Select SSL
   - Common Name: Enter the entity name
   - Organization: Enter your company’s legally registered name
City: Enter the city where your company is legally located

State: Select the state where your company is legally located

Country: Select the country where your company is legally located

Key Size: In the drop-down list, select 2048

Provider: Select Microsoft RSA SChannel Cryptographic Provider (unless you have a specific cryptographic provider)

Click Generate to generate a CSR:

This will also generate a corresponding private key in the Windows computer from which the CSR is requested. The Certificate Enrollment Request is stored under: (Console Root)\Certificates(Local Computer)\Certificate Enrollment Requests\Certificates).

2.3.2.2 Issue Signed Certificates

5. With a created applicant CSR, request a signed certificate using DigiCert CertCentral portal.

- Login to a DigiCert Dashboard <https://www.digicert.com/account/login.php> with your account user name and password.

- Once in the portal, go to Request a Certificate, then select Private SSL to open a certificate request form. Fill in the certificate settings in the fields shown in the form which includes pasting the CSR information to the area called Paste your CSR.
6. After filling in all the required information and scroll down to the bottom of the page and click on the “I agree to the Certificate Services Agreement above” check box, click the Submit Certificate Request button at the bottom of the form to submit the certificate for signing approval. The administrator of the CA authority will use the same portal with different privilege to prove the request after reviewing and verifying the submitted request information if needed.

7. To download the signed certificate, go to CERTIFICATES->Orders to list the ordered signed certificates:

![Orders](image)

8. Click a specific order number to display the certificate details with a list of actions for you to perform. Click the Download Certificate As to download certificates with signed CA and Root CA certificates. A variety of certificate formats can be downloaded, such as .crt, .p7b, or .PEM, etc.

9. Save the downloaded certificate in a location where it can be used for further processing if needed.

2.3.2.3 Import and Export the Signed Certificate

Using the DigiCert Utility and OpenSSL tool, you can further manipulate the certificates to combine with the private key and export the signed certificate, or you can convert certificates or keys to the formats specified for your organization’s devices.

10. To import a signed certificate, use DigiCert Utility to click the Import button to load a downloaded file to the utility. The download file was saved in Step 9 above. Click the Next button to import.

11. From the DigiCert Certificate utility for Windows, click SSL to list all the imported files.
To export the certificate, select the certificate that you want to export as a combined certificate file and key file in a `.pfx` file or separated as a certificate file and key file, and then click **Export Certificate**.

Click the **Next** button and follow the wizard instruction to save the certificate file and private key file to a location you desire.
2.3.2.4 Certificate and Key File Format Conversion

PKI certificates and key files can be in different formats. When PKI certificates are used in medical devices, device manufacturer user guides specify which formats are acceptable in their devices. Fortunately, many tools can perform format conversion. One utility tool that NCCoE used is the OpenSSL for Windows. It is open source and can be downloaded from https://www.openssl.org/community/binaries.html. Here are some of the useful convert commands:

- To convert .crt to .pem:
  ```bash
  openssl x509 -in mycert.crt -outform PEM -out mycert.pem.
  ```

- To convert a private key into PEM format:
  ```bash
  openssl rsa -in yourdomain.key -outform PEM -out yourdomain.pem.key.
  ```

- Separate a pfx file into two different .key/.crt files:
  ```bash
  openssl pkcs12 -in yourfile.pfx -nocerts -out keyfile-encrypted.key.
  ```

- For a key file: `openssl pkcs12 -in yourfile.pfx -nocerts -out keyfile-encrypted.key`.


- To convert a Cert PEM file to DER:
  ```bash
  openssl x509 -outform der -inform DEM -in certificate.pem -out certificate.der.
  ```

- To convert a key PEM file to DER:
  ```bash
  openssl rsa -inform DEM -in infile.key -out outfile.der -outform DER.
  ```

2.4 Symantec Endpoint Protection and Intrusion Detection

NCCoE protected the pump server application in the notional Biomedical Engineering network by using three Symantec cybersecurity products on an enterprise network, with a specific focus on wireless infusion pumps:
Each product protects components in the enterprise systems at different levels.

### 2.4.1 Symantec Data Center Security: Server Advanced

For data center security, Server Advanced provides a policy-based approach to endpoint security and compliance. It includes the management server, the agents, the unified management console, the database, and DCS Security Virtual Appliance (SVA). The agent components working with the server management provide intrusion prevention and detection on endpoint devices; the database is used for storing the policies, agent information, and real time actionable events; and the SVA provides agentless anti-malware protection for VMWare guest VMs running Windows.

The management server and the console can be installed on one system, and the agents are generally deployed to every supported host or endpoint devices. Figure 2-2 displays the Data Center Security: Server Advanced Environment.

![Figure 2-2: Data Center Security: Server Advanced Environment](image)

#### 2.4.1.1 Installing Data Center Security: Server Advanced Manager

**Minimum Hardware Requirement:** Server Advanced includes hardware support x86, EM64T, and AMD64 with 60 GB free disk space (all platforms) 8 GB RAM 4 CPUs.

**Minimum Software Requirement:** Windows Installer 2.0 or higher, Microsoft SQL Server 2008, .NET Framework 4.0 or 4.5.1, PowerShell 2.0, and Windows 2008 or later.

Operating the Symantec Data Center Security: Server Advanced installation requires to link to an instance of SQL Server locally or remotely. All installations allocate approximately 60 GB of space for the database on SQL Server Enterprise edition. We first installed a new instance of SQL Server that conforms to the Symantec installation requirements. The SQL Server was installed on the same machine as that for the Data Center Security: Server Advanced Manager.

Follow these steps to install the SQL Server software.
1. Use SCSP as the default instance name

2. Set authentication configuration to Mixed Mode (Windows authentication and SQL Server authentication)

3. Set the "sa" with a password when you set Mixed Mode authentication. You will need this password when you install Data Center.

4. After installing the instance of SQL Server, select to authenticate using SQL Server credentials.

5. Register the instance. Registering the instance also starts the instance.

Follow these steps to install Data Center Security: Server Advanced:

1. Double click server.exe, then in the Welcome panel, click Next and accept the license agreement

2. In the Installation Type panel, click Evaluation Installation, then click Use an Existing MSSQL Instance, and then click Next.

3. Follow the instructions and select the parameters suitable for your organization to complete the installation.


https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/9000/DOC9394/en_US/DCSSA_Planning_Deployment_Guide.pdf?__gda__=1494398285_572b0ff349979359e0cc9342b337f3bb

2.4.1.2 Configuration of Data Center Security: Server Advanced Manager

After you install the Management Server, the Server Configuration Wizard lets you configure various parameters of the installation.

One purpose of these configuration settings is to use the policy-based least privilege access control provided by DCS to lock down the configuration settings, files, and file systems in the pump for restricting application and operating system behavior and protecting the files and systems from tampering.

To enable a policy in DCS Management Server, follow these steps:

1. Login to the DCS console.

2. Create a policy folder.

3. In the Java console, click Policies.

4. Under the Policies tab, click Prevention or Detection.

5. On the Policies page, in the Workspace Folders, select the Workspace folder and then right-click Add Folder. Look for a new policy folder with the name New Folder. Rename this folder as Pump Server.

6. Copy an existing policy to the Pump Server folder.

7. From the default Symantec folder, find a proper policy example and copy it to the Pump Server.

8. Using the Move To command. In the Workspace pane, select a policy (e.g., “windows-baseline-detection” policy in Symantec folder for Detection), and then right-click Move To. In the MoveFolder dialog box, select Pump Server to receive the policy, and then click MoveTo.
To edit a policy, right-click a policy, and then click Edit Policy. Configure the setting based on your security protection needs.

DCS Advanced Server provides a variety of configurable protection from application data protection, application protection to network protection. For example, the Windows prevention policies have a Protected Whitelisting strategy that lets you specify an application to which you always want to allow access or give permission to run. When you whitelist a process or an application, all the other processes and applications that are not included in the list are denied access.

To allow a program to run by using the Protected Whitelisting strategy, follow these steps:

1. In the management console, click the Policies tab and then click Prevention.
2. In the Policies workspace, click Add.
4. In the Policy Name panel, from the Policy Pack drop-down list, select the policy pack that you want to use as the baseline for the new custom policy.
5. In the Name text box, enter a name for the policy that you create. In this build, we use “Windows Prevention Policy 6.0 Reference 31 Protected Whitelisting strategy.”
6. Check Create a custom prevention policy, and then click Next.
7. In the Protection Strategy panel, use the slider to select Protected Whitelisting.
8. In the Trusted Updaters panel, click Add, and then in the Select Type dialog box, select the type of updater that you want to add. The Trusted Updaters list is populated through the agent data retriever. You can edit or delete an updater that you have already added to the list.
9. Click Next.
10. In the Application Rules panel, click Add, and then in the Select Type dialog box, select the type of rules that you want to add. You can edit or delete a rule that you have already added to the list.
11. In the Global Policy Options panel, click Configure to configure the global policy settings, and then click Next.
12. In the Summary panel, click Save.

2.4.1.3 Installing Data Center Security: Server Advanced Agent

Use agent.exe to install the agent software on computers that run supported Windows operating systems. To install the Windows agent software, follow these steps:

1. On the installation package, double-click agent.exe.
2. In the Welcome panel, click Next.
3. In the License Agreement panel, select I accept the terms in the license agreement, and then click Next.
4. In the Destination Folder panel, change the folders if necessary, and then click Next.
5. In the Agent Configuration panel, accept or change the default settings, and then click Next. Ensure that Enable Intrusion Prevention is checked.
In the **Management Server Configuration** panel, in the Primary Management Server box, type the fully qualified host name or IP address of the primary server that is used to manage this agent. If you changed the Agent Port setting during management server installation, in the Agent Port box, type a port number that matches.

(Optional) In the **Management Server Configuration** panel, in the Alternate Management Servers box, type the fully qualified host name or IP address of the alternate servers that are used for failover for this agent. Type the servers in a comma-separated list.

In the **Management Server Configuration** panel, accept the directory for the SSL certificate `Agent-cert.ssl`, or click *Browse* to browse to and locate `Agent-cert.ssl`. Access to a copy of the SSL certificate `Agent-cert.ssl` is required to connect to the management server. All primary and alternate management servers must use the same certificate.

In the **Management Server Configuration** panel, click *Next*.

(Optional) In the **Agent Group Configuration** panel, in the group boxes, type the group names that you created with the Java console. You may add multiple detection policy group names separated with commas. You may include the name of an existing detection policy domain in the group path/name.

In the **Agent Group Configuration** panel, click *Next*.

In the **Service User Configuration** panel, accept the default Local System account, and then click *Next*.

In the **Ready to Install the Program** panel, confirm the installation parameters, and then click *Install*.

When the installation completes, click *Finish*.

Agent installation configures the appropriate networking for the environment. The agent installation configuration includes which Data Center Security: Server Advanced Management Servers to communicate with, which ports to use, and how often to poll for changes. The initial Data Center Security: Server Advanced installation also determines whether key product features are enabled or not. Particular key agent features can be installed, and each provides different protection:

- Enabling the intrusion prevention feature
- Enabling the real-time file integrity monitoring feature in intrusion detection
- Enabling the real-time file integrity monitoring feature in intrusion detection
- Creating agent registration groups.


**2.4.2 Symantec Endpoint Protection Manager**

**Minimum Hardware Requirement:** 2 GB RAM as minimum; 8 GB or more available recommended. Hard drive should be 40 GB as minimum (200 GB recommended) for the management server and database with a remote SQL Server database.
Minimum Software Requirement: Windows Installer 2.0 or higher, Microsoft SQL Server 2008, .NET Framework 4.0 or 4.5.1, PowerShell 2.0, and Windows 2008 Server or later. Intel Pentium Dual-Core or equivalent minimum, 8-core or greater is recommended.

The Symantec Endpoint Protection Manager includes an embedded database. You may instead choose to use a database from one of the following versions of Microsoft SQL Server: SQL Server 2008, SP4 up to SQL Server 2016.

2.4.2.1 Installing Symantec Endpoint Manager

1. Download the product, extract the entire installation file to a physical disk, such as a hard disk. Run Setup.exe. The installation should start automatically.

2. Follow the screen instruction and accept the license agreement.

3. Continue the installation until it is finished. After the initial installation completes, configure the server and database.


5. Select Default Configuration, and then click Next.

6. Enter company name, a password for the default administrator admin, and an email address.

7. If you run LiveUpdate as part of a new installation, content is more readily available for the clients you deploy.

8. If you want Symantec to receive anonymous data, click Next to begin the database creation.

9. When the database creation completes, click Finish to complete the Symantec Endpoint Protection Manager configuration.

2.4.2.2 Installing the Client

After installing Symantec Endpoint Protection Manager, install the Symantec Endpoint Protection client to the endpoint host with the Client Deployment Wizard. Of the several installation methods, we recommend using the Save package. This installation option creates an executable installation package that you save on the management server and then distribute to the client computers. Follow these steps:

1. Make your configuration selections as you install the Symantec Endpoint Protection Manager and then create the client installation packages.

2. Save the installation package to a folder on the computer that runs Symantec Endpoint Protection Manager.

3. Copy this package to a client machine where you have an administrator privilege.

4. The installation package comprises one setup.exe file. Click the executable file to start the installation. Follow the wizards to complete the installation.

2.4.3 Symantec Advanced Threat Protection: Advanced Threat Protection: Network

With Advanced Threat Protection: Network (ATP:N) installed on the network, it can provide Network-based protection of medical device subnets via monitor internal inbound and outbound internet traffic.
We integrate Symantec Advanced Threat Protection (ATP) with Symantec Endpoint Protection, it will allow ATP to monitor and manage all network traffic from the endpoints and provide threat assessment for dangerous activity to secure the medical devices on an enterprise network.

**Minimum Hardware Requirement:** 32 GB RAM; 4 CPUs. Hard drive should be at least 500 GB.

**Minimum Software Requirement:** ESXi 5.5 and 6.0, ATP virtual appliance includes an Integrated Dell Remote Access Controller (iDRAC). The iDRAC console requires the latest version of the Java Runtime Environment (JRE) installed on the administrative client.

### 2.4.3.1 ATP-N Installation

The installation of the ATP-N involves the deployment of the OVA template on the VMware ESXi Server. A sample installation steps are shown below:

1. Deploy the OVA. During the Deploying procedure, the Deploy OVA Template wizard prompts you to map the Source Network adapters, which are built into the APT OVA with Destination Networks that you already configured on your network.
2. In VMware vSphere Client, start the newly-created virtual appliance.
3. Open a console to the appliance and logon with the user name admin and the proper password to start the bootstrap.
4. From a computer that is on the same subnet as the appliance management port, use a browser to connect to the APT Manager using the ATP IP address. The user name is setup and the password is Symantec.

### 2.4.3.2 Integrating APT with Symantec Endpoint Protection

To integrate the Symantec Advanced Threat Protection (ATP) with Symantec Endpoint Protection allows us to Correlation of event data from Symantec Endpoint Protection Manager to ATP. To do the integration, follow these steps:

1. On Symantec Endpoint Protection Manager, prepare the database for log collection to allow ATP to access the database using DB administrator (sa) credentials.
2. Enable Symantec Endpoint Protection Correlation option by checking in the Settings > Global > Synapse area of ATP Manager.
3. In ATP Manager, configure the connection to Symantec Endpoint Protection Manager instances.
4. In Symantec Endpoint Protection Manager, configure host integrity and quarantine firewall policies, if not already enabled.
5. In Symantec Endpoint Protection Manager, configure endpoints to send information to the ATP management node.
6. In ATP Manager, add SSL certificates for secure communication between endpoints and ATP, if needed.

2.5 Risk Assessment Tools

2.5.1 Clearwater IRM|Analysis™ Software

We used Clearwater IRM|Analysis™ Software-as-a-Service (SaaS) application, a control-based risk tool for conducting a risk assessment with a focus on the Healthcare Delivery Organization (HDO) enterprise. In our environment, we built the enterprise network to simulate a typical HDO environment. Clearwater Compliance created an account for NCCoE under their cloud based tool, IRM|Analysis™. The software is based on the construct of an “Information Asset” which creates, maintains, receives or transmits electronically Protected Health Information (ePHI.) This can be a software application, information system, medical device system, etc.

This section does not show you how to conduct a risk assessment. Instead, we present some basic steps for using the IRM|Analysis™ tool to conduct the risk assessment:

1. Login to IRM|Analysis™.
2. Import Inventory of Information Assets or enter the data through the Asset Inventory Form.
3. Establish conformance with the NIST-based Security Controls.
4. Determine the Risk Rating predicated on a 5x5 matrix of likelihood x impact.
5. Identify those risks that are exceed the established “risk threshold.”
6. Document “Risk Response” and associated tasks necessary to mitigate, transfer, avoid or accept the risk in the IRM|Analysis™ software.
7. Leverage Dashboard and Reporting functionality to provide documentation and evidence of a credible and bona fide risk analysis.

2.5.1.1 Login to IRM|Analysis™

1. From a browser, type https://software.clearwatercompliance.com/login.
2. On the Login page (see Figure 2-3), enter the appropriate email and password.
3. Click on Sign In.

Figure 2-3: IRM|Analysis™ Login Page
2.5.1.2 Enter Asset Inventory

We used the New Asset page to add the assets to the system and the Edit Asset page to update the record. After all assets are entered, an analysis is conducted to determine if media (i.e., devices) associated with different assets can be grouped together based on a similar risk profile. For instance: all servers are virtual machines using the same Storage Area Network and identical Operating Systems. If you have 10 assets that have server selected and they are all the same, they can be grouped and evaluated as one. The Media/Asset Group is the logic group for organizing media into classes to reduce the number of identical security control assessments.

To add a new asset:

1. On the IRM|Analysis™ tool, expand Assets on the left menu bar.
2. Under Assets, click on Asset Inventory List.
3. On the Asset Inventory List page (see Figure 2-4), click on the New button.
4. On the New Asset form (see Figure 2-5), enter the required information and click on the Save button.

Figure 2-4: Asset Inventory List
To update an asset:

1. On the IRM|Analysis™ tool, expand Assets on the left menu bar.
2. Under Assets, click on Asset Inventory List.
3. On the Asset Inventory List page (see Figure 2-4), select the asset you want to edit, then click on the Edit button.
4. On the Edit Media/Asset Groups page (see Figure 2-7), enter the necessary information and click on the Save button.

To view and manage media/asset groups:

1. On the IRM|Analysis™ tool, expend Assets on the left menu bar.
2. Under Assets, click on Media/Asset Groups.
3. On the Media/Asset Groups (see Figure 2-6), scroll up and down to view the groups and select a group by clicking on the Edit button.
4. On the Edit Media/Asset Groups page (see Figure 2-7), enter the necessary information and click on the Save button.
Figure 2-6: Media/Asset Groups

Figure 2-7: Edit Media/Asset Group

2.5.1.3 Risk Determination

The IRM|Analysis™ tool uses different methods to determine risk. In this section, we show two ways to use the tool: Controls – Global/Media screen to document the status of a control; and the Risk Questionnaire List to select a given Media/Asset group.

To use the Risk Determination at Global/Media level:

1. On the IRM|Analysis™ tool, expand Risk Determination on the left menu bar.

2. Under Risk Determination, click on Controls – Global/Media.
On the Controls – Global/Media page (see Figure 2-8), scroll up and down to view the controls. For each control, select one of the responses (i.e., Yes, In Progress, No, and N/A) to indicate the response status.

Figure 2-8: Controls - Global/Media

To use the Risk Determination at the Asset/Media group level:

1. On the IRM|Analysis™ tool, expand Risk Determination on the left menu bar.

2. Under Risk Determination, click on Risk Questionnaire List.

3. On the Risk Questionnaire List page (see Figure 2-9), scroll up and down to view the media/asset groups.

4. For each relevant media/asset group, select the Risk Analyst, fill in the Due Date and click on the Continue button to get in the Risk Questionnaire Form (see Figure 2-10 – part 1 and Figure 2-11 – part 2).

5. For each control, select one of the responses (i.e., Yes, In Progress, No, and N/A) to indicate the response status (example shown in part 1), if it was already noted on the Controls Global/Media page.

6. Controls can be set globally or for individual Media/Asset Groups. The plus sign will expand the control to reveal the Media/Asset Groups so the control can be set individually. To illustrate, a global control can be set for Training for the Security Workforce but an individual control would be set for each of the Media/Asset groups associated with the User Activity Review since only a subset of assets may undergo a User Activity Review.

7. Then determine and select the Risk Likelihood and Risk Impact for the selected risk scenario (example shown in part 2) to populate the Risk Rating.

8. You may select the question mark for more information on the control and the NIST symbol for a quick reference to NIST SP800-53.
Figure 2-9: Risk Questionnaire List

Figure 2-10: Risk Questionnaire Form (part 1)
2.5.1.4 Risk Response

The IRM|Analysis™ tool enables users to try different methods of reviewing risk scenarios, acquiring a risk rating, and seeing progress in a risk response workflow. The basics of using the tool follow.

Consider following these risk response steps:

1. In the IRM|Analysis™ tool, expand Risk Response in the left menu bar.

2. Under Risk Response, click on Risk Response List.

3. Only those risks which exceed the risk threshold established under Framing/Governance in the left menu bar will move to the Risk Response portion of the software.

4. On the Risk Response List page (see Figure 2-12), scroll up and down to view the Medial/Asset Groups along with the associated threat source, vulnerability, and risk rating.

5. For each relevant risk response, click on the button under the Treatment column to enter the Risk Treat and Evaluate Form page of that risk (see Figure 2-13).

6. On the Risk Treat and Evaluate Form page, perform the risk response analysis by selecting the risk treatment type; evaluate the control or recommendation; select risk owner; put risk notes, and so on.
2.5.1.5 **Dashboard and Report**

The IRM|Analysis™ tool enables users to review their risk analyses with a dashboard or report format.

To access the dashboard views, follow these steps:

1. On the IRM|Analysis™ tool, expand **Dashboard** on the left menu bar
2. Under Dashboard, click on Rating Distribution by Asset
3. Example Dashboard: Rating Distribution by Asset page (see Figure 2-14 below)

You can also view other types of dashboards, such as Risk Rating Trends and Risk Rating Averages.

Figure 2-14: Dashboard Example

For report views, follow these steps:

1. On the IRM|Analysis™ tool, expand Reports on the left menu bar
2. Under Reports, click on Risk Rating Report
3. Example Report: Risk Rating Report page is showing (see Figure 2-15 below)

You can also view other types of dashboards, such as Risk Rating Trends and Risk Rating Averages.
2.5.2 MDISS MDRAP

We used MDISS’s cloud-based Medical Device Risk Assessment Platform (MDRAP), a questionnaire-based risk assessment tool to conduct the assessment on the medical devices. In our environment, we set up and configured wireless infusion pump systems from five manufactures and built the enterprise network to simulate a typical HDO environment.

Please note, this section does not show you how to conduct a risk assessment. Instead, we show these basic steps for using the MDRAP tool:

- Login to MDRAP
- Conduct Device Inventory
- Risk Assessment
- Dashboard and Reports.

2.5.2.1 Login to MDRAP

1. Within a browser, type https://mdrap.mdiss.org/ and click on Log In.
2. On the Login page (see Figure 2-16), enter the appropriate email and password.
3. Click on Submit.
2.5.2.2 Conduct Device Inventory

We use the Device Inventory module of MDRAP to keep track all the infusion pumps and servers in our sample implementation. Add Device, per its name, enables us to add individual devices, while Bulk Import enables us to add a group of devices. Steps for using both methods follow.

1. On the Welcome to MDRAP page (see Figure 2-17), click on Device Inventory on the menu bar or on the View Device Inventory link on the page.

2. On the Device Inventory page (Figure 2-18), add an individual device, or edit a device, or bulk import a group of devices.
Figure 2-17: MDRAP Welcome page

MDRAP, a product of the MDISS community, is the Medical Device Risk Assessment Platform which assists healthcare systems and device manufacturers in understanding, analyzing and mitigating the security risks of their medical devices.

Use the menu above to navigate.

Figure 2-18: Device Inventory List

Device Inventory

This is your Device Inventory. You may view/edit any of these by clicking on the title. To add a new Device, click the Add Device button.

Add device:

1. On the Device Inventory page (see Figure 2-18 above), click on ADD DEVICE.

2. On Add Device page (see Figure 2-19 below), locate the device from the Category List, then click on ADD.
Figure 2-19: Add Device

Select a Device from the Catalog

These are the available devices in the Catalog. Search for a device or scroll through the list to locate the Device. Then, add it to your Inventory by clicking the Add button.

Edit a device:

1. On the Device Inventory page (see Figure 2-18 above), locate the device from the list, click on the product name link or the Edit icon.

2. On the Edit Inventory page (see Figure 2-20 below), update the data and click on Save.
Bulk Import a group of devices:

1. On the Device Inventory page (see Figure 2-18: Device Inventory List above), click on BULK IMPORT button.

2. On Inventory Bulk Import page (see Figure 2-21 below), download the template, fill-in the data into the template.

3. Follow the instruction to upload and import the devices by using the template (see Figure 2-22).

Figure 2-21: Inventory Bulk Import

Inventory Bulk Import

Bulk Upload is a facilitated activity. To get started, please download the MDRAP Device Inventory template file. Then, open the file in Excel and enter each device in your inventory on a new row. The template will note any required columns and formatting guidelines.

Once you have completed adding your inventory, send your file to MDRAP customer support at support@mdrap.zendesk.com for the upload. We will contact you once the inventory is loaded into MDRAP.
2.5.2.3 Risk Assessment

We created a risk assessment for each device by responding to the MDRAP’s built-in questionnaire. The basic steps of creating a risk assessment for a given device follow:

1. Create assessment
   d. On the Welcome to MDRAP page (see Figure 2-17 above), click on Assessments on the menu bar or Go to Assessments link on the page.
   e. On Create Assessment page 1 (see Figure 2-23), select a device.
   f. On Create Assessment page 2 (see Figure 2-24), select Questionnaire type (i.e., MDISS Questionnaire).
   g. Answer the questions and then click Next button (see example questionnaire pages in Figure 2-25 and Figure 2-26).
Figure 2-23: Create Assessment (part 1)

Create Assessment

To add a new Assessment, first select a Device in your Inventory.

Search Inventory ...

ADVANCED

(14 devices)

NCCoE-P1
InfusionPump_1-1
located at Test Environment (Test Room)
Class 2 device
(ERN) Pump, Infusion
In Service Date: 02/07/2017

NCCoE-P1
InfusionPump_1-2
located at Test Environment (Test Room)
Class 2 device
(ERN) Pump, Infusion
In Service Date: 02/07/2017

Figure 2-24: Create Assessment (part 2)

Create Assessment

To add a new Assessment, first select a Device in your Inventory.

InfusionPump_1-2

Assessment Title
MDISS Assessment for InfusionPump_1-2

Select the Risk Assessment Questionnaire form to use

MDISS Questionnaire

The MDIS Questionnaire risk assessment form is based on the MDS2 Manufacturer’s Disclosure form and includes some additional details. It is designed to be compatible with the MDIS risk scoring analytics model and is the preferred and recommended risk assessment form for use with MDRAP.
2.5.2.4 Dashboard and Reports

MDRAP computes assessment results based on the responses to the questionnaires. For a given assessment (complete or partially complete), the assessment result is available for view as a dashboard (see Figure 2-27) or report (see Figure 2-28).
## Figure 2-27: Assessment Result (dashboard example)

### MDISS Assessment for InfusionPump_1-1

- **NCSI**: P1
- **Risk Level**: 100.0%
- Completed: 100.0%
- Assessment last updated on 02/10/2017 22:52:25

### Risk Scores

<table>
<thead>
<tr>
<th>Category</th>
<th>Level of Effort</th>
<th>Likelihood</th>
<th>Risk</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Controls</td>
<td>1</td>
<td>3.367</td>
<td>5.25</td>
<td>* Patient identity not captured.</td>
</tr>
<tr>
<td>Authorization</td>
<td>1</td>
<td>5.5</td>
<td>3.75</td>
<td>* Authorization can be bypassed using an API.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Operator can acquire root-level privilege.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Root-level privilege is the only authorization mode.</td>
</tr>
<tr>
<td>Automatic Logoff</td>
<td>1</td>
<td>0.7</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Product</td>
<td>1</td>
<td>1.295</td>
<td>1.175</td>
<td>* Device OS is not supported by the OS manufacturer.</td>
</tr>
<tr>
<td>Upgrades</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware Detection / Protection</td>
<td>1</td>
<td>5.5</td>
<td>4</td>
<td>* No Virus Protection</td>
</tr>
<tr>
<td>Other Scoreable MD52 Security</td>
<td>1</td>
<td>2.375</td>
<td>0.453</td>
<td>* No encryption of data at rest.</td>
</tr>
<tr>
<td>Categories</td>
<td></td>
<td></td>
<td></td>
<td>* No Fuzz-testing performed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Some device storage components not physically secured.</td>
</tr>
<tr>
<td>Other Security Considerations</td>
<td>1</td>
<td>1</td>
<td>3.275</td>
<td>* Maintenance users require root privilege.</td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Person Authentication</td>
<td>1</td>
<td>0.4</td>
<td>5.6</td>
<td>* Device does not store, display, transmit, or maintain ePHI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Passwords cannot be set to expire.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Person authentication is not supported.</td>
</tr>
<tr>
<td>System and Application</td>
<td>1</td>
<td>4.32</td>
<td>1.907</td>
<td>* Device transmits data in the clear on shared networks.</td>
</tr>
<tr>
<td>Hardening</td>
<td></td>
<td></td>
<td></td>
<td>* System does not allow file-level access controls.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Unnecessary services active.</td>
</tr>
<tr>
<td>Transmission Confidentiality &amp;</td>
<td>1</td>
<td>0.28</td>
<td>2.118</td>
<td></td>
</tr>
</tbody>
</table>
Appendix A  Baseline Configuration File

A.1 Baseline Configuration File

ASA Version 9.6(1)

!

interface Management0/0
ip address 192.168.29.149 255.255.255.0

!

! optional, SSH, version is important as v1 is insecure and on by default, also set your own password!
username cisco password XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
aaa authentication ssh console LOCAL

! set to network and interface you want to manage from, can be WAN
ssh 192.168.29.0 255.255.255.0 management
ssh version 2

!

hostname internal-kmcfadde

!

! Configure network interfaces
interface GigabitEthernet0/0
  nameif WAN
  security-level 50
  ip address 192.168.100.149 255.255.255.0
  no shutdown

! optional, authenticated OSPF for excellence
  ospf authentication-key [L]N@Uv
  ospf authentication message-digest

!

interface GigabitEthernet0/1
  nameif LAN
  security-level 100
  ip address 192.168.150.1 255.255.255.0
no shutdown
!
! optional, DHCP Server
dhcpd address 192.168.150.220-192.168.150.250 LAN
dhcpd dns 8.8.8.8 8.8.4.4
dhcpd option 3 ip 192.168.150.1
dhcpd enable LAN
!
! optional, OSPFv2
router ospf 1
network 192.168.100.0 255.255.255.0 area 0
redistribute connected subnets
redistribute static subnets
!
! Configure DNS resolution here, required for license activation
dns domain-lookup WAN
dns server-group DefaultDNS
  name-server 8.8.8.8
  name-server 8.8.4.4
!
license smart
  feature tier standard
  throughput level 1G
names
!
! optional, Configure time zone and NTP here
clock timezone EST -5
clock summer-time EDT recurring
ntp server 10.97.74.8
!
! Allow ping through LAN to WAN
policy-map global_policy
class inspection_default
    inspect icmp
    inspect icmp error
!
! Show up in traceroute
policy-map global_policy
class class-default
    set connection decrement-ttl
!
! Make ICMP/UDP traceroute work from LAN to WAN
object-group icmp-type PING-REPLIES
    icmp-object echo-reply
object-group icmp-type TRACEROUTE-REPLIES
    icmp-object time-exceeded
    icmp-object unreachable
    group-object PING-REPLIES
access-list 101 extended permit icmp any any object-group TRACEROUTE-REPLIES
access-list 101 extended permit icmp any any object-group PING-REPLIES
!
! Allow ICMP ping/traceroute from WAN to LAN
object-group icmp-type PING
    icmp-object echo
access-list 101 extended permit icmp any any object-group PING
!
! Allow UDP traceroute from WAN to LAN
object-group service TRACEROUTEUDP
    service-object udp destination gt 33434
access-list 101 extended permit object-group TRACEROUTEUDP any any
! example, allow a specific port on a host
! access-list 101 extended permit tcp any host 192.168.140.XXX eq www
!
! Add firewall rules we created to WAN interface
access-group 101 in interface WAN
!
! Example, set a static route
! route WAN 192.168.140.0 255.255.255.0 192.168.100.111
!
! SNMP
object network SNMPHOSTS
  subnet 192.168.29.0 255.255.255.0
snmp-server enable
snmp-server community public
snmp-server host-group management SNMPHOSTS
**A.2 External Firewall and Guest Network ASA Configuration File**

:: Saved

::

:: Serial Number: 9AK64JT2D2M
:: Hardware: ASAv, 2048 MB RAM, CPU Xeon E5 series 2200 MHz
::

ASA Version 9.6(1)

!
hostname border-kmcfadde
enable password 8Ry2Yjlyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
!
license smart
feature tier standard
throughput level 1G
names

!
interface GigabitEthernet0/0
nameif WAN
security-level 0
ip address 10.32.3.10 255.255.255.0
!
interface GigabitEthernet0/1
  nameif LAN
  security-level 100
  ip address 192.168.100.101 255.255.255.0  
  ospf authentication-key *****
  ospf authentication message-digest
!
interface GigabitEthernet0/2
  nameif GUEST
  security-level 100
  ip address 192.168.170.1 255.255.255.0
!
interface GigabitEthernet0/3
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/5
  shutdown
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/8
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
nameif management
security-level 0
ip address 192.168.29.147 255.255.255.0
!
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns domain-lookup WAN
dns server-group DefaultDNS
name-server 8.8.8.8
name-server 8.8.4.4
object network LAN-SUBNETS
subnet 192.168.0.0 255.255.0.0
object network SNMPHOSTS
subnet 192.168.29.0 255.255.255.0
object-group icmp-type PING-REPLIES
icmp-object echo-reply
object-group icmp-type TRACEROUTE-REPLIES
icmp-object time-exceeded
icmp-object unreachable
group-object PING-REPLIES
object-group icmp-type PING
icmp-object echo
object-group service TRACEROUTEUDP
service-object udp destination gt 33434
access-list 101 extended permit icmp any any object-group TRACEROUTE-REPLIES
pager lines 23
mtu WAN 1500
mtu LAN 1500
mtu management 1500
mtu GUEST 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network LAN-SUBNETS
nat (LAN,WAN) dynamic interface
access-group 101 in interface WAN
!
route-map DEFAULT permit 10
match interface WAN
!
router ospf 1
network 192.168.100.0 255.255.255.0 area 0
log-adj-changes
redistribute connected subnets
redistribute static subnets
default-information originate
!
route WAN 0.0.0.0 0.0.0.0 10.32.3.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
snmp-server host-group management SNMPHOSTS poll community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491
308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130
0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520 6f6620757365 206f7479 202d 20473530 1e170d31
30303230 38303030 3030305a 170d3230 30323037 32333539 35395a30 81b5310b
30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65
74776f72 6b313b30 39060355 040b1332 5465726d 73206f66 20757365 20617420
68747470 733a2f2f 776f7269 5369676e 203320 53657276 204341202d 20473330 82012230 060692a 864886f7
0d010101 05003082 010f0030 8201a02 82010100 b18781f c20c45f5 bcab2597
a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bbf68e 44f4dce 6fed094a d4af4e10
9c688b2e 957b899b 13cae234 341f35b f3497b62 83488174 d188786c 02539fbc
7f432657 58338333 33017b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b
15fca34b 3bce6388 d0f820dc 948610ca b69a3dca eb379c00 48358629 5078e845
63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
18b49a8e 3c681fd e4cd5356 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced
4a546ac9 4dc5bf11 b1ae1c67 81cb4455 33997f24 9b3f5345 7f861af3 3ca6d7f
81fb84a d3f85357 1cb5a6d0 09e4187b 384efa0f 02030100 01a38201 df308201
qq
quit
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 8.8.8.8 8.8.4.4
dhcpd option 3 ip 192.168.170.1
!
dhcpd address 192.168.170.220-192.168.170.250 GUEST
dhcpd enable GUEST
!
dynamic-access-policy-record DfltAccessPolicy
username cisco password YBYvHe595lIMVg7Y encrypted
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
  parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error

class class-default
  set connection decrement-ttl

!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
  no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
profile License
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http

Cryptochecksum:9ffa4947d875e0c501e036c54e80ee93

: end
A.3 Enterprise Services ASA Configuration File

: Saved

: Serial Number: 9AEHKLC171M

: Hardware: ASA, 2048 MB RAM, CPU Xeon E5 series 2200 MHz

ASA Version 9.6(1)

hostname enterprise-services-kmcfadde

enable password 8Ry2Yjlyt7RRXU24 encrypted

xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain

! license smart

feature tier standard

throughput level 1G

names

!

interface GigabitEthernet0/0

nameif WAN

security-level 50

ip address 192.168.100.154 255.255.255.0

ospf authentication-key *****

ospf authentication message-digest
interface GigabitEthernet0/1
  nameif LAN
  security-level 100
  ip address 192.168.120.1 255.255.255.0

interface GigabitEthernet0/2
  shutdown
  no nameif
  no security-level
  no ip address

interface GigabitEthernet0/3
  shutdown
  no nameif
  no security-level
  no ip address

interface GigabitEthernet0/4
  shutdown
  no nameif
  no security-level
  no ip address

interface GigabitEthernet0/5
  shutdown
  no nameif
  no security-level
  no ip address
interface GigabitEthernet0/6
shutdown	no nameif
no security-level
no ip address
!
interface GigabitEthernet0/7
shutdown	no nameif
no security-level
no ip address
!
interface GigabitEthernet0/8
shutdown	no nameif
no security-level
no ip address
!
interface Management0/0
management-only
nameif management
security-level 0
ip address 192.168.29.154 255.255.255.0
!
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns domain-lookup WAN
dns server-group DefaultDNS
name-server 8.8.8.8
name-server 8.8.4.4
object network SNMPHOSTS
subnet 192.168.29.0 255.255.255.0
object-group service DNS
  service-object tcp-udp destination eq domain
object-group service SYMANTEC-DCS
  service-object tcp destination eq 4443
  service-object tcp destination eq https
  service-object tcp destination eq 8443
  service-object tcp destination eq 2222
access-list 101 extended permit icmp any any time-exceeded
access-list 101 extended permit icmp any any unreachable
access-list 101 extended permit icmp any any echo-reply
access-list 101 extended permit icmp any any echo
access-list 101 extended permit udp any any gt 33434
access-list 101 extended permit object-group DNS 192.168.140.0 255.255.255.0 host 192.168.120.162
access-list 101 extended permit object-group DNS 192.168.140.0 255.255.255.0 host 192.168.120.163
access-list 101 extended permit tcp any host 192.168.120.166 eq 8114
access-list 101 extended permit object-group SYMANTEC-DCS any host 192.168.120.167
pager lines 23
mtu management 1500
mtu WAN 1500
mtu LAN 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group 101 in interface WAN
router ospf 1
network 192.168.100.0 255.255.255.0 area 0
log-adj-changes
redistribute connected subnets
redistribute static subnets
!
timeout xlate 3:00:00

timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
snmp-server host-group management SNMPHOSTS poll community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130 0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117 30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 53696766 2c20496e 74797072 6f6e65
20617574 686f7269 7a656420 53746570 6c697665 2c2074756e 67697468 696562
65726953 69676620 436c6173 73203030 30303030 30303030 30303030 30303030
30906032 0b133128 63292032 30303030 30303030 30303030 30303030 30303030
496e632e 311f301d 06035504 0b133128 63292032 30303030 30303030 30303030
74777f2f 6b313b30 30303030 30303030 30303030 30303030 30303030 30303030
68747747 733a2f2f 77657269 53696766 2c20436c 61737320 33205365 72696766
65726953 69676620 436c6173 73203030 30303030 30303030 30303030 30303030
a7ada23e 9cba8ca2 3ac56c6e 5bb65e9e 44444d8e 6ed094d4 af4af4e10
9c688b2e 957b899b 13ae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc
7f432657 5833333b 330a17b0 d04e9124 ad867d64 12dc44a4 34a11d0a ea961d0b
15fca34b 3bce6388 d0f82d0c 948610ca b69ad3ca eb379c00 48358629 5078e485
63cd1941 4ff595ec 7b98d4c7 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
18b49ae8 3c6e81fd e4cd5356 b351d369 ec12ba56 6669b57 c58b14e7 0ec79ced
4a546ca9 4dc5bf1f b1ae1c6f 81cb4455 33997f24 9b3f5345 7861af3 3cba6d7f
81f5b84a d3f58537 1cb5a6d0 09e4187b 384eaf0f 02030100 01a38201 df308201
db303406 088b20601 05050701 01042830 26302406 082b6001 05050701 01861686
7474703a 2f2f6f63 73702e76 65726973 6967662e 636f6e65 72656d69 6e67726f
7001030 70060355 1d130101 ff040830 060101ff 02010030 07000355 1d020046 30677065 60b6086 4801868f
45010717 03305630 2806082b 06010505 07020116 1c687474 70733a2f 2f777777
2e766572 69736967 6e2e6366 f6d2f630 73302a06 082b6001 05050702 02300a1a
0c687470 70733a2f 2f777777 2e766572 69736967 6e2e6366 f6d2f7270 61303406
03551df0 042d3021 3029a27b a0258623 68747747 3a2f2f63 726c2e76 65726973
69676e2e 636f6e65 72656d69 6e67726f 70060355 0e060355 1d0f0101 ff040a03
02010630 6d06082b 06010505 07010c04 61305fa1 5da05b30 59305730 55160969
6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
c3cf806a d448182c 6a73b82b 6a73b82b 7d494aca 99c71928 a2bed877 2f2f6c6f
c3cf806a d448182c 6a73b82b 6a73b82b 7d494aca 99c71928 a2bed877 2f2f6c6f
6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
c3cf806a d448182c 6a73b82b 6a73b82b 7d494aca 99c71928 a2bed877 2f2f6c6f
6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
c3cf806a d448182c 6a73b82b 6a73b82b 7d494aca 99c71928 a2bed877 2f2f6c6f

quit
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
username cisco password YBYvHe5951MVg7Y encrypted
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error
class class-default
set connection decrement-ttl
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile License

destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http

profile CiscoTAC-1

no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http

subscribe-to-alert-group diagnostic

subscribe-to-alert-group environment

subscribe-to-alert-group inventory periodic monthly

subscribe-to-alert-group configuration periodic monthly

subscribe-to-alert-group telemetry periodic daily

Cryptochecksum:e57e00145eb4fd26d97b4b0109308140

: end
A.4 Biomedical Engineering

: Saved

: Serial Number: 9A3RHJVFQPS

: Hardware: ASAv, 2048 MB RAM, CPU Xeon E5 series 2200 MHz

ASA Version 9.6(1)

hostname biomedical-kmcfadde

enable password 8Ry2Yjlyt7RRUXU24 encrypted

xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain

license smart

feature tier standard

throughput level 1G
	names

interface GigabitEthernet0/0

nameif WAN

security-level 50

ip address 192.168.100.152 255.255.255.0

ospf authentication-key ******

ospf authentication message-digest
! interface GigabitEthernet0/1
   nameif LAN
   security-level 100
   ip address 192.168.140.1 255.255.255.0
!
! interface GigabitEthernet0/2
   shutdown
   no nameif
   no security-level
   no ip address
!
! interface GigabitEthernet0/3
   shutdown
   no nameif
   no security-level
   no ip address
!
! interface GigabitEthernet0/4
   shutdown
   no nameif
   no security-level
   no ip address
!
! interface GigabitEthernet0/5
   shutdown
   no nameif
   no security-level
   no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/8
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
nameif management
security-level 0
ip address 192.168.29.152 255.255.255.0
!
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns domain-lookup WAN
dns server-group DefaultDNS
name-server 8.8.8.8
name-server 8.8.4.4
object network SNMPHOSTS
subnet 192.168.29.0 255.255.255.0
object network PUMPS
subnet 192.168.150.0 255.255.255.0
object-group icmp-type PING-REPLIES
icmp-object echo-reply
object-group icmp-type TRACEROUTE-REPLIES
icmp-object time-exceeded
icmp-object unreachable
group-object PING-REPLIES
object-group icmp-type PING
icmp-object echo
object-group service TRACEROUTEUDP
service-object udp destination gt 33434
object-group service BAXTERPORTS
service-object tcp-udp destination eq 51244
object-group service SMITHSPORTS
service-object tcp destination eq 1588
object-group service CAREFUSIONPORTS
service-object tcp destination eq 3613
object-group service PCAPORTS
service-object tcp destination eq https
service-object tcp destination eq 11443
service-object tcp destination eq 11444
object-group service PLUM360PORTS
service-object tcp destination eq 8100
service-object tcp destination eq 9292
object-group service HOSPIRAPUMPSIMPORTS
service-object tcp destination eq https
service-object tcp destination eq 8443
object-group service BBRAUNPORTS
service-object tcp destination eq www
service-object tcp destination eq https
service-object tcp destination eq 8080
service-object tcp destination eq 1500
service-object tcp destination eq 1500
access-list 101 extended permit icmp any any object-group TRACEROUTE-REPLIES
access-list 101 extended permit object-group TRACEROUTEUDP any any
access-list 101 extended permit icmp any any object-group PING
access-list 101 extended permit icmp any any object-group PING-REPLIES
access-list 101 extended permit object-group SMITHSPORTS object PUMPS host 192.168.140.150
access-list 101 extended permit object-group CAREFUSIONPORTS object PUMPS host 192.168.140.158
access-list 101 extended permit object-group PCAPORTS object PUMPS host 192.168.140.160
access-list 101 extended permit object-group PLUM360PORTS object PUMPS host 192.168.140.160
access-list 101 extended permit object-group HOSPIRAPUMPSIMPORTS object PUMPS host 192.168.140.160
access-list 101 extended permit object-group BAXTERPORTS object PUMPS host 192.168.140.165
access-list 101 extended permit object-group BBRAUNPORTS object PUMPS host 192.168.140.169
pager lines 23
mtu WAN 1500
mtu LAN 1500
mtu management 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group 101 in interface WAN
router ospf 1
network 192.168.100.0 255.255.255.0 area 0
log-adj-changes
redistribute connected subnets
redistribute static subnets
!
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
snmp-server host-group management SNMPHOSTS poll community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491
  308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130
  0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
quit
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 192.168.120.163 192.168.120.162
dhcpd option 3 ip 192.168.140.1
!
dhcpd address 192.168.140.220-192.168.140.250 LAN
dhcpd enable LAN
!
dynamic-access-policy-record DfltAccessPolicy
username cisco password YBYvHe595IIMVg7Y encrypted
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect smtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
    inspect icmp
    inspect icmp error
class class-default
  set connection decrement-ttl
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
  no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
profile License
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http

Cryptochecksum:627e549de0a7dd97cd1379bbf37bc168
: end
A.5 Medical Devices Zone ASA Configuration File

: Saved

: Serial Number: 9AEWS2E5JRA
: Hardware: ASAv, 2048 MB RAM, CPU Xeon E5 series 2200 MHz
: ASA Version 9.6(1)

hostname medical-devices-kmcfdde
enable password 8Ry2Yjlyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain

license smart
feature tier standard
throughput level 1G
names

interface GigabitEthernet0/0
  nameif WAN
  security-level 50
  ip address 192.168.100.149 255.255.255.0
  ospf authentication-key *****
  ospf authentication message-digest

interface GigabitEthernet0/1
  nameif LAN
  security-level 100
  ip address 192.168.150.1 255.255.255.0

interface GigabitEthernet0/2
  shutdown
  no nameif
  no security-level
  no ip address

interface GigabitEthernet0/3
  shutdown
  no nameif
no security-level
no ip address
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/8
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
nameif management
security-level 0
ip address 192.168.29.149 255.255.255.0
!
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns domain-lookup WAN
dns server-group DefaultDNS
name-server 8.8.8.8
name-server 8.8.4.4
object network SNMPHOSTS
subnet 192.168.29.0 255.255.255.0
object network PUMPSERVERS
subnet 192.168.140.0 255.255.255.0

object network PUMPS
subnet 192.168.150.0 255.255.255.0

object-group icmp-type PING-REPLIES
icmp-object echo-reply

object-group service PCAPORTS
service-object tcp destination eq https
service-object tcp destination eq 11444
service-object tcp destination eq 11443
service-object tcp destination eq 8443

object-group icmp-type TRACEROUTE-REPLIES
icmp-object time-exceeded
icmp-object unreachable

group-object PING-REPLIES
object-group icmp-type PING
icmp-object echo

object-group service TRACEROUTEUDP
service-object udp destination gt 33434

object-group service PLUM360PORTS
service-object tcp destination eq 8100
service-object tcp destination eq 9292

object-group service HOSPIRAPUMPSTPORTS
service-object tcp-udp destination eq 51243

object-group service BAXTERPUMPSTPORTS
service-object tcp-udp destination eq 8080
service-object tcp destination eq 1500

access-list LAN2WAN extended permit ip object PUMPS object PUMPSERVERS
access-list WAN2LAN extended permit object-group PCAPORTS host 192.168.140.160 object PUMPS

access-list WAN2LAN extended permit icmp any any object-group PING
access-list WAN2LAN extended permit object-group TRACEROUTEUDP any
access-list WAN2LAN extended permit icmp any any object-group TRACEROUTE-REPLIES
access-list WAN2LAN extended permit icmp any any object-group PING-REPLIES
access-list WAN2LAN extended permit object-group PLUM360PORTS host 192.168.140.160 object PUMPS

access-list WAN2LAN extended permit object-group HOSPIRAPUMPSTPORTS host 192.168.140.160 object PUMPS
access-list WAN2LAN extended permit object-group BAXTERPUMPSTPORTS host 192.168.140.160 object PUMPS

access-list WAN2LAN extended permit object-group BBRAUNPORTS host 192.168.140.160 object PUMPS

pager lines 23
mtu WAN 1500
mtu LAN 1500
mtu management 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group WAN2LAN in interface WAN
access-group LAN2WAN in interface LAN
router ospf 1
   network 192.168.100.0 255.255.255.0 area 0
   log-adj-changes
   redistribute connected subnets
   redistribute static subnets
!
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
snmp-server host-group management SNMPHOSTS poll community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491
  308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130
  0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
  30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
  13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
  0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466672
  20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
  65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
  65727469 66696361 74652075 7365206f 6e6c79 31453043 06035504 03133c56
  30303230 38303030 3030305a 170d3230 30323037 32333539 35395a30 81b5310b
QUIT
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 192.168.150.1
dhcpd option 3 ip 192.168.150.1
!
dhcpd address 192.168.150.220-192.168.150.250 LAN
dhcpd enable LAN
!
dynamic-access-policy-record DfltAccessPolicy
username cisco password YBYvHe595lIMVg7Y encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 parameters
 message-length maximum client auto
 message-length maximum 512
 policy-map global_policy
 class inspection_default
 inspect dns migrated_dns_map_1
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect ip-options
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
 inspect icmp
 inspect icmp error
 class class-default
 set connection decrement-ttl
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
 no active
 destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
 destination address email callhome@cisco.com
 destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
profile License

destination address http https://tools.cisco.com/its/service/oddce/services/DD

CEService
destination transport-method http

Cryptochecksum: b2e10eb9d982ddeb5330e964af80d2d3
A.6 **Switch Configuration File**

```
!
! Last configuration change at 22:21:08 UTC Wed Feb 22 2017 by cisco
! NVRAM config last updated at 23:22:47 UTC Wed Feb 22 2017 by cisco
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname Cisco3650-01
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-vrf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
logging console emergencies
enable secret 5 $4$FraY$34n8ay7c.l7qwJttjHas0
enable password 7 023624481811003348
!
username admin privilege 15 password 7 04734A125E75606E0B4A
user-name cisco
creation-time 1469560730
privilege 15
password 7 0523471B701862291B56
type mgmt-user
no aaa new-model
switch 1 provision ws-c3650-48ps
!
ip domain-name nist.gov
ip device tracking
ip dhcp excluded-address 192.168.250.1 192.168.250.9
!
ip dhcp pool WLAN
network 192.168.250.0 255.255.255.0
default-router 192.168.250.1
option 43 hex c0a8.fa02
```
vtp mode transparent

crypto pki trustpoint TP-self-signed-2035642131
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-2035642131
revocation-check none
rsakeypair TP-self-signed-2035642131

crypto pki certificate chain TP-self-signed-2035642131
certificate self-signed 01
3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 62D536967 6E65642D 43657274
69666963 6174652D 32303335 36343231 3331301E 170D3136 30373236 32303436
32355A17 0D323030 31303130 30303030 30A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 30333536
34323133 3130819F 300D0609 2A864886 F70D0101 01050003 81BD0030 8190281
8108F1C4 010AE138 9BD9BBCC 2E563180 698979B5 51F7B64B D122595E E7033DCA
D8C9432 0728E47F 8AC2629 40CEC617 5CDFBFD9 19744025 CB26CA75 8F6F0A9A
34F790DD 07DA9D60 737196C1 FDD9E764 6D22EDA3 8D9E7765 6CD934E3 D89FA9D5
C165F3EE E9E0EA9F 37742B00 2C4CF408 C262E61B 95565B42 302B2E7 A1C85D9F
5FDB0203 010001A3 75307330 0F063055 1D130101 FF040530 30300623 55101104
19301782 15436973 636F3336 35302D30 312E6E69 73742E67 6F76301F
0603515D 23041830 1680148F 3A1CDEB7 502D327F 4E9E64EA EA147F01 CDF1F730
1D060355 1D060416 04148F3A 1CDEB750 2DACB77F 4E9E64EA 1470F1CF 1A1F7300D
06092A86 4886F70D 01010040 00038181 004FE025 9B72B4D2 5391B847 F443B481
4493FB6D 692FF3A 3C26E96D 7D83B92 91DBB84D DD47E242 9B2F45AC A7C7C8BC
D7C9B660 2B87A9E9 0376D5A1 15CBA40B B326AADE AB213E81 D625F888 B2F54CCD
40B1EB91 C6DD5E33 DE8EEB3 20ECEDE96 F42527D6 AD1F6A55 AD51D394 FE358B8F
317FAF0E E853785D 777E1E1D 6F561A2A 07
quit

diagnostic bootup level minimal
spanning-tree mode pvst
spanning-tree extend system-id

redundancy
mode sso

vlan 20

vlan 1400
  name IP_DEV_BIOMEDICAL
!
vlan 1500
  name IP_DEV
!
vlan 1520
  name WIFI_MGMT
!
ip ssh version 2
!
class-map match-any non-client-nrt-class
  match non-client-nrt
!
policy-map port_child_policy
  class non-client-nrt-class
    bandwidth remaining ratio 10
!
!
!
!
interface GigabitEthernet0/0
  vrf forwarding Mgmt-vrf
  ip address 192.168.20.13 255.255.255.0
  negotiation auto
!
interface GigabitEthernet1/0/1
  switchport access vlan 1520
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet1/0/2
  switchport access vlan 1520
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet1/0/3
  switchport access vlan 1520
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet1/0/4
  switchport access vlan 1520
  switchport mode access
  spanning-tree portfast
!
interface GigabitEthernet1/0/5
  spanning-tree portfast
!
interface GigabitEthernet1/0/6
  spanning-tree portfast
!
interface GigabitEthernet1/0/7
  spanning-tree portfast
!
interface GigabitEthernet1/0/8
  spanning-tree portfast
!
interface GigabitEthernet1/0/9
  spanning-tree portfast
!
interface GigabitEthernet1/0/10
  spanning-tree portfast
!
interface GigabitEthernet1/0/11
  spanning-tree portfast
!
interface GigabitEthernet1/0/12
  spanning-tree portfast
!
interface GigabitEthernet1/0/13
  spanning-tree portfast
!
interface GigabitEthernet1/0/14
  spanning-tree portfast
!
interface GigabitEthernet1/0/15
  spanning-tree portfast
!
interface GigabitEthernet1/0/16
  spanning-tree portfast
!
interface GigabitEthernet1/0/17
  spanning-tree portfast
!
interface GigabitEthernet1/0/18
  spanning-tree portfast
!
interface GigabitEthernet1/0/19
  spanning-tree portfast
!
interface GigabitEthernet1/0/20
  spanning-tree portfast
!
interface GigabitEthernet1/0/21  
  spanning-tree portfast
!
interface GigabitEthernet1/0/22  
  spanning-tree portfast
!
interface GigabitEthernet1/0/23  
  spanning-tree portfast
!
interface GigabitEthernet1/0/24  
  spanning-tree portfast
!
interface GigabitEthernet1/0/25  
  spanning-tree portfast
!
interface GigabitEthernet1/0/26  
  spanning-tree portfast
!
interface GigabitEthernet1/0/27  
  spanning-tree portfast
!
interface GigabitEthernet1/0/28  
  spanning-tree portfast
!
interface GigabitEthernet1/0/29  
  spanning-tree portfast
!
interface GigabitEthernet1/0/30  
  spanning-tree portfast
!
interface GigabitEthernet1/0/31  
  spanning-tree portfast
!
interface GigabitEthernet1/0/32  
  spanning-tree portfast
!
interface GigabitEthernet1/0/33  
  spanning-tree portfast
!
interface GigabitEthernet1/0/34  
  spanning-tree portfast
!
interface GigabitEthernet1/0/35  
  spanning-tree portfast
!
interface GigabitEthernet1/0/36  
  spanning-tree portfast
!
interface GigabitEthernet1/0/37
  spanning-tree portfast
!
interface GigabitEthernet1/0/38
  spanning-tree portfast
!
interface GigabitEthernet1/0/39
  spanning-tree portfast
!
interface GigabitEthernet1/0/40
  spanning-tree portfast
!
interface GigabitEthernet1/0/41
  switchport access vlan 1400
  spanning-tree portfast
!
interface GigabitEthernet1/0/42
  switchport access vlan 1400
  spanning-tree portfast
!
interface GigabitEthernet1/0/43
  switchport access vlan 1400
  spanning-tree portfast
!
interface GigabitEthernet1/0/44
  switchport access vlan 1400
  spanning-tree portfast
!
interface GigabitEthernet1/0/45
  description Set to 10/Half for Hospira
  switchport access vlan 1500
  speed 10
  duplex half
  spanning-tree portfast
!
interface GigabitEthernet1/0/46
  switchport access vlan 1500
  spanning-tree portfast
!
interface GigabitEthernet1/0/47
  description VLAN trunk
  switchport trunk allowed vlan 1400,1500,1520
  switchport mode trunk
  spanning-tree portfast
!
interface GigabitEthernet1/0/48
  description management connection on VL20
  switchport access vlan 20
spanning-tree portfast
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan20
  ip address 192.168.20.13 255.255.255.0
!
interface Vlan1520
  description Wireless-MGMT
  ip address 192.168.250.1 255.255.255.0
!
  no ip http server
  no ip http secure-server
  ip route 0.0.0.0 0.0.0.0 192.168.20.254
!
  ip access-list extended SSH-Access
  permit tcp 192.168.20.0 0.0.0.255 any eq 22
  deny ip any any log
!
  access-list 10 permit 192.168.20.0 0.0.0.255
!
  snmp-server community public RO 10
  snmp-server location NCCoE
  snmp-server contact nccoe_healthcare_dev@nist.gov
!
!
  line con 0
  exec-timeout 0 0
  stopbits 1
  line aux 0
  stopbits 1
  line vty 0 4
  access-class SSH-Access in
  exec-timeout 300 0
  password 7 022E454F5A5223014E1D
  login local
  transport input ssh
  line vty 5 15
access-class SSH-Access in
exec-timeout 300 0
password 7 022E454F5A5223014E1D
login local
transport input ssh
!
nntp server 10.97.74.8
wsma agent exec
profile httplistener
profile httpslistener
wsma agent config
profile httplistener
profile httpslistener
wsma agent filesys
profile httplistener
profile httpslistener
wsma agent notify
profile httplistener
profile httpslistener
!
wsma profile listener httplistener
transport http
!
wsma profile listener httpslistener
transport https
ap group default-group
end
A.7 Wireless Configuration

System Inventory
NAME: "Chassis" , DESCR: "Cisco Wireless Controller"
PID: AIR-CTVM-K9, VID: V01, SN: 96NTPERK0A6

Burned-in MAC Address............................ 00:50:56:AC:6D:08
Maximum number of APs supported............... 200

System Information
Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.2.111.0
RTOS Version..................................... 8.2.111.0
Bootloader Version............................... 8.2.111.0
Emergency Image Version......................... 8.2.111.0

Build Type....................................... DATA + WPS

System Name...................................... wlc
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.1631
IP Address....................................... 192.168.250.2
IPv6 Address..................................... ::
System Up Time................................... 6 days 3 hrs 48 mins 20 secs
System Timezone Location.........................
System Stats Realtime Interval................... 5
System Stats Normal Interval.................... 180

Configured Country.............................. US - United States
State of 802.11b Network............................ Enabled
State of 802.11a Network............................ Enabled
Number of WLANs................................. 2
Number of Active Clients....................... 2

Burned-in MAC Address............................ 00:50:56:AC:6D:08
Maximum number of APs supported.............. 200
System Nas-Id....................................
WLC MIC Certificate Types...................... SHA1
Licensing Type.................................... RTU
vWLC config...................................... Small

Backup Controller Configuration

AP primary Backup Controller .................
AP secondary Backup Controller ..............

System Time Information:

Time............................................. Thu Aug 18 20:05:16 2016
Timezone delta.................................. 0:0
Timezone location...............................
<table>
<thead>
<tr>
<th>Index</th>
<th>NTP Key Index</th>
<th>NTP Server</th>
<th>Status</th>
<th>NTP Msg Auth Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>192.168.250.1</td>
<td>Not Synched</td>
<td>AUTH DISABLED</td>
</tr>
</tbody>
</table>

Redundancy Information

Redundancy Mode .................................. SSO DISABLED
Local State....................................... ACTIVE
Peer State....................................... N/A
Unit............................................. Primary
Unit ID.......................................... 00:50:56:AC:6D:08
Redundancy State................................. N/A
Mobility MAC..................................... 00:50:56:AC:6D:08
Redundancy Management IP Address.............. 0.0.0.0
Peer Redundancy Management IP Address........ 0.0.0.0
Redundancy Port IP Address..................... 0.0.0.0
Peer Redundancy Port IP Address............... 169.254.0.0

AP Bundle Information

<table>
<thead>
<tr>
<th>Primary AP Image</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap1g1</td>
<td>12660</td>
</tr>
<tr>
<td>ap1g2</td>
<td>11748</td>
</tr>
<tr>
<td>ap1g3</td>
<td>13672</td>
</tr>
<tr>
<td>ap1g4</td>
<td>19256</td>
</tr>
<tr>
<td>ap3g1</td>
<td>9736</td>
</tr>
<tr>
<td>ap3g2</td>
<td>13480</td>
</tr>
<tr>
<td>ap3g3</td>
<td>18696</td>
</tr>
<tr>
<td>ap801</td>
<td>8064</td>
</tr>
<tr>
<td>ap802</td>
<td>9536</td>
</tr>
</tbody>
</table>
Secondary AP Image    Size
------------------    ----
ap1g1             12660
ap1g2             11748
ap1g3             13672
ap1g4             19256
ap3g1             9736
ap3g2            13480
ap3g3            18696
ap801             8064
ap802             9536
c1140             8636
c1520             7344
c1550            10628
c1570            11536
c602i             3864
version.info     4

Switch Configuration
802.3x Flow Control Mode......................... Disable
FIPS prerequisite features....................... Disabled
WLANCC prerequisite features..................... Disabled
UCAPL prerequisite features...................... Disabled
secret obfuscation............................... Enabled

Strong Password Check Features
 case-check.................................... Enabled
 consecutive-check......................... Enabled
 default-check.............................. Enabled
 username-check................................ Enabled
 position-check.............................. Disabled
 case-digit-check............................ Disabled
 Min. Password length......................... 3
 Min. Upper case chars......................... 0
 Min. Lower case chars......................... 0
 Min. Digits chars............................. 0
 Min. Special chars............................ 0

Mgmt User
 Password Lifetime [days]...................... 0
 Password Lockout................................ Disabled
 Lockout Attempts............................. 3
 Lockout Timeout [mins]........................ 5

SNMPv3 User
 Password Lifetime [days]...................... 0
 Password Lockout................................ Disabled
 Lockout Attempts............................. 3
 Lockout Timeout [mins]........................ 5

Network Information
 RF-Network Name............................. WLAN
 DNS Server IP...................................
 Web Mode.................................... Disable
 Secure Web Mode............................. Enable
 Secure Web Mode Cipher-Option High...... Disable
Secure Web Mode Cipher-Option SSLv2........ Disable
Secure Web Mode RC4 Cipher Preference....... Disable
Secure Web Mode SSL Protocol............... Disable
OCSP..................................... Disabled
OCSP responder URL........................
Secure Shell (ssh)......................... Enable
Secure Shell (ssh) Cipher-Option High.... Disable
Telnet..................................... Disable
Ethernet Multicast Forwarding.............. Disable
Ethernet Broadcast Forwarding.............. Disable
IPv4 AP Multicast/Broadcast Mode........ Unicast
IPv6 AP Multicast/Broadcast Mode......... Unicast
IGMP snooping.............................. Disabled
IGMP timeout............................... 60 seconds
IGMP Query Interval........................ 20 seconds
MLD snooping............................... Disabled
MLD timeout............................... 60 seconds
MLD query interval.......................... 20 seconds
User Idle Timeout.......................... 300 seconds
ARP Idle Timeout.......................... 300 seconds
Cisco AP Default Master.................... Disable
AP Join Priority........................... Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface............... Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode...................... EAP
Mesh Full Sector DFS....................... Enable
Mesh Backhaul RRM........................ Disable
AP Fallback ............................... Enable
Web Auth CMCC Support .................. Disabled
Web Auth Redirect Ports .................... 80
Web Auth Proxy Redirect ..................... Disable
Web Auth Captive-Bypass ..................... Disable
Web Auth Secure Web ......................... Enable
Web Auth Secure Redirection .................. Disable
Fast SSID Change ............................ Disabled
AP Discovery - NAT IP Only .................... Enabled
IP/MAC Addr Binding Check .................... Enabled
Link Local Bridging Status .................... Disabled
CCX-lite status ............................... Disable
oeap-600 dual-rlan-ports ..................... Disable
oeap-600 local-network ....................... Enable
oeap-600 Split Tunneling (Printers) ........ Disable
WebPortal Online Client ...................... 0
WebPortal NTF_LOGOUT Client ................. 0
mDNS snooping ............................... Disabled
mDNS Query Interval ......................... 15 minutes
Web Color Theme ............................. Default
Capwap Prefer Mode ........................... IPv4
Network Profile .............................. Disabled
Client ip conflict detection (DHCP) ....... Disabled
Mesh BH RRM ................................. Disable
Mesh Aggressive DCA ......................... Disable
Mesh Auto RF ................................. Disable
HTTP Profiling Port ......................... 80

Port Summary

<table>
<thead>
<tr>
<th>STP</th>
<th>Admin</th>
<th>Physical</th>
<th>Physical</th>
<th>Link</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pr</td>
<td>Type</td>
<td>Stat</td>
<td>Mode</td>
<td>Mode</td>
<td>Status</td>
</tr>
<tr>
<td>---</td>
<td>-----</td>
<td>--------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>---</td>
<td>-----</td>
<td>--------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
</tr>
</tbody>
</table>

---
1 Normal Forw Enable Auto  1000 Full Up Enable N/A

## AP Summary

Number of APs........................................ 2

Global AP User Name................................. Not Configured

Global AP Dot1x User Name............................ Not Configured

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Slots</th>
<th>AP Model</th>
<th>Ethernet MAC</th>
<th>Location</th>
<th>Country</th>
<th>IP Address</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSE Location</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AP78da.6ee0.08ec</td>
<td>2</td>
<td>AIR-CAP1602I-A-K9</td>
<td>78:da:6e:e0:08:ec</td>
<td>default location</td>
<td>US</td>
<td>192.168.250.10</td>
<td>[0,0,0]</td>
</tr>
<tr>
<td>AP24e9.b34b.f1ed</td>
<td>2</td>
<td>AIR-CAP1602I-A-K9</td>
<td>24:e9:b3:4b:f1:ed</td>
<td>default location</td>
<td>US</td>
<td>192.168.250.11</td>
<td>[0,0,0]</td>
</tr>
</tbody>
</table>

## AP Tcp-Mss-Adjust Info

<table>
<thead>
<tr>
<th>AP Name</th>
<th>TCP State</th>
<th>MSS Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP78da.6ee0.08ec</td>
<td>disabled</td>
<td>-</td>
</tr>
<tr>
<td>AP24e9.b34b.f1ed</td>
<td>disabled</td>
<td>-</td>
</tr>
</tbody>
</table>

## AP Location

Total Number of AP Groups......................... 1

Site Name........................................... default-group

Site Description................................. <none>

NAS-identifier..................................... none

Client Traffic QinQ Enable....................... FALSE

DHCPv4 QinQ Enable............................... FALSE

AP Operating Class............................... Not-configured

Capwap Prefer Mode............................... Not-configured
RF Profile

----------
2.4 GHz band..................................... <none>
5 GHz band....................................... <none>

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>Interface</th>
<th>Network Admission Control</th>
<th>Radio Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ip_dev</td>
<td>Disabled</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>ip_dev</td>
<td>Disabled</td>
<td>None</td>
</tr>
</tbody>
</table>

*AP3600 with 802.11ac Module will only advertise first 8 WLANs on 5GHz radios.

Lan Port configs

-----------

<table>
<thead>
<tr>
<th>LAN</th>
<th>Status</th>
<th>POE</th>
<th>RLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disabled</td>
<td>Disabled</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>Disabled</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Disabled</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

External 3G/4G module configs

---------------------------------

<table>
<thead>
<tr>
<th>LAN</th>
<th>Status</th>
<th>POE</th>
<th>RLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Disabled</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
AP78da.6ee0.08ec  2  AIR-CAP1602I-A-K9  78:da:6e:e0:08:ec  default location  1  US  1

RF Profile

Number of RF Profiles............................ 6

Out Of Box State................................... Disabled

Out Of Box Persistence............................. Disabled

<table>
<thead>
<tr>
<th>RF Profile Name</th>
<th>Band</th>
<th>Description</th>
<th>11n-client-only</th>
<th>Applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-Client-Density-802.11a</td>
<td>5 GHz</td>
<td>&lt;none&gt;</td>
<td>disable</td>
<td>No</td>
</tr>
<tr>
<td>High-Client-Density-802.11bg</td>
<td>2.4 GHz</td>
<td>&lt;none&gt;</td>
<td>disable</td>
<td>No</td>
</tr>
<tr>
<td>Low-Client-Density-802.11a</td>
<td>5 GHz</td>
<td>&lt;none&gt;</td>
<td>disable</td>
<td>No</td>
</tr>
<tr>
<td>Low-Client-Density-802.11bg</td>
<td>2.4 GHz</td>
<td>&lt;none&gt;</td>
<td>disable</td>
<td>No</td>
</tr>
<tr>
<td>Typical-Client-Density-802.11a</td>
<td>5 GHz</td>
<td>&lt;none&gt;</td>
<td>disable</td>
<td>No</td>
</tr>
<tr>
<td>Typical-Client-Density-802.11bg</td>
<td>2.4 GHz</td>
<td>&lt;none&gt;</td>
<td>disable</td>
<td>No</td>
</tr>
</tbody>
</table>

RF Profile name.............................. High-Client-Density-802.11a
Description.................................... <none>
AP Group Name.................................. <none>
Radio policy................................. 5 GHz
11n-client-only............................... disabled
Transmit Power Threshold v1............... -65 dBm
Transmit Power Threshold v2............... -67 dBm
Min Transmit Power........................... 7 dBm
Max Transmit Power............................... 30 dBm

802.11a Operational Rates

802.11a 6M Rate.............................. Disabled
802.11a 9M Rate.............................. Disabled
802.11a 12M Rate......................... Mandatory
802.11a 18M Rate......................... Supported
802.11a 24M Rate......................... Mandatory
802.11a 36M Rate......................... Supported
802.11a 48M Rate......................... Supported
802.11a 54M Rate......................... Supported

Max Clients...................................... 200

WLAN ID          Max Clients
- ------          ------
1                600
2                600

Trap Threshold

   Clients...................................... 12 clients
   Interference............................... 10 %
   Noise....................................... -70 dBm
   Utilization................................. 80 %

Multicast Data Rate......................... 0
Rx Sop Threshold........................... -78 dBm
Cca Threshold................................ 0 dBm
Slot Admin State.......................... Enabled

Band Select

   Probe Response........................... Disabled
   Cycle Count.............................. 2 cycles
Cycle Threshold.............................. 200 milliseconds
Expire Suppression........................... 20 seconds
Expire Dual Band............................. 60 seconds
Client Rssı.................................. -80 dBm
Client Mid Rssı.............................. -80 dBm

Load Balancing
  Denial....................................... 3 count
  Window....................................... 5 clients

Coverage Data
  Data......................................... -80 dBm
  Voice......................................... -80 dBm
  Minimum Client Level......................... 3 clients
  Exception Level.............................. 25 %
  DCA Channel List.............................. 36,40,44,48,52,56,60,64,100,
  104,108,112,116,120,124,128,
  132,136,140,144,149,153,157,
  161
  DCA Bandwidth.................................... 20
  DCA Foreign AP Contribution...................... enabled

802.11n MCS Rates
  MCS-00 Rate.................................. enabled
  MCS-01 Rate.................................. enabled
  MCS-02 Rate.................................. enabled
  MCS-03 Rate.................................. enabled
  MCS-04 Rate.................................. enabled
  MCS-05 Rate.................................. enabled
  MCS-06 Rate.................................. enabled
MCS-07 Rate.................................. enabled
MCS-08 Rate.................................. enabled
MCS-09 Rate.................................. enabled
MCS-10 Rate.................................. enabled
MCS-11 Rate.................................. enabled
MCS-12 Rate.................................. enabled
MCS-13 Rate.................................. enabled
MCS-14 Rate.................................. enabled
MCS-15 Rate.................................. enabled
MCS-16 Rate.................................. enabled
MCS-17 Rate.................................. enabled
MCS-18 Rate.................................. enabled
MCS-19 Rate.................................. enabled
MCS-20 Rate.................................. enabled
MCS-21 Rate.................................. enabled
MCS-22 Rate.................................. enabled
MCS-23 Rate.................................. enabled
MCS-24 Rate.................................. enabled
MCS-25 Rate.................................. enabled
MCS-26 Rate.................................. enabled
MCS-27 Rate.................................. enabled
MCS-28 Rate.................................. enabled
MCS-29 Rate.................................. enabled
MCS-30 Rate.................................. enabled
MCS-31 Rate.................................. enabled
Client Network Preference....................... default

RF Profile name................................ High-Client-Density-802.11bg
Description...................................... <none>
AP Group Name.................................... <none>
Radio policy..................................... 2.4 GHz
11n-client-only............................... disabled
Transmit Power Threshold v1............... -70 dBm
Transmit Power Threshold v2............... -67 dBm
Min Transmit Power........................... 7 dBm
Max Transmit Power........................... 30 dBm

802.11b/g Operational Rates
   802.11b/g 1M Rate........................ Disabled
   802.11b/g 2M Rate........................ Disabled
   802.11b/g 5.5M Rate......................... Disabled
   802.11b/g 11M Rate........................ Disabled
   802.11g 6M Rate............................ Disabled
   802.11g 9M Rate............................ Supported
   802.11g 12M Rate........................... Mandatory
   802.11g 18M Rate........................... Supported
   802.11g 24M Rate........................... Supported
   802.11g 36M Rate........................... Supported
   802.11g 48M Rate........................... Supported
   802.11g 54M Rate........................... Supported

Max Clients.................................... 200

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>Max Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>600</td>
</tr>
<tr>
<td>2</td>
<td>600</td>
</tr>
</tbody>
</table>

Trap Threshold
   Clients..................................... 12 clients
   Interference................................ 10 %
   Noise...................................... -70 dBm
Utilization .................................. 80 %
Multicast Data Rate ................. 0
Rx Sop Threshold ....................... -82 dBm
Cca Threshold .......................... 0 dBm
Slot Admin State ................... Enabled

Band Select
Probe Response ...................... Disabled
Cycle Count .......................... 2 cycles
Cycle Threshold ...................... 200 milliseconds
Expire Suppression ................. 20 seconds
Expire Dual Band ..................... 60 seconds
Client Rssi .............................. -80 dBm
Client Mid Rssi ..................... -80 dBm

Load Balancing
Denial ................................. 3 count
Window .............................. 5 clients

Coverage Data
Data ................................. -80 dBm
Voice ................................. -80 dBm
Minimum Client Level ............ 3 clients
Exception Level .................. 25 %
DCA Channel List ................ 1,6,11
DCA Bandwidth .................. 20
DCA Foreign AP Contribution ........................ enabled

802.11n MCS Rates
MCS-00 Rate ........................ enabled
MCS-01 Rate............................... enabled
MCS-02 Rate............................... enabled
MCS-03 Rate............................... enabled
MCS-04 Rate............................... enabled
MCS-05 Rate............................... enabled
MCS-06 Rate............................... enabled
MCS-07 Rate............................... enabled
MCS-08 Rate............................... enabled
MCS-09 Rate............................... enabled
MCS-10 Rate............................... enabled
MCS-11 Rate............................... enabled
MCS-12 Rate............................... enabled
MCS-13 Rate............................... enabled
MCS-14 Rate............................... enabled
MCS-15 Rate............................... enabled
MCS-16 Rate............................... enabled
MCS-17 Rate............................... enabled
MCS-18 Rate............................... enabled
MCS-19 Rate............................... enabled
MCS-20 Rate............................... enabled
MCS-21 Rate............................... enabled
MCS-22 Rate............................... enabled
MCS-23 Rate............................... enabled
MCS-24 Rate............................... enabled
MCS-25 Rate............................... enabled
MCS-26 Rate............................... enabled
MCS-27 Rate............................... enabled
MCS-28 Rate............................... enabled
MCS-29 Rate............................... enabled
MCS-30 Rate............................... enabled
MCS-31 Rate............................... enabled
Client Network Preference............... default

RF Profile name.......................... Low-Client-Density-802.11a
Description.............................. <none>
AP Group Name........................... <none>
Radio policy.............................. 5 GHz
11n-client-only........................... disabled
Transmit Power Threshold v1............. -60 dBm
Transmit Power Threshold v2............. -67 dBm
Min Transmit Power...................... -10 dBm
Max Transmit Power...................... 30 dBm

802.11a Operational Rates
  802.11a 6M Rate.......................... Mandatory
  802.11a 9M Rate.......................... Supported
  802.11a 12M Rate.......................... Mandatory
  802.11a 18M Rate.......................... Supported
  802.11a 24M Rate.......................... Mandatory
  802.11a 36M Rate.......................... Supported
  802.11a 48M Rate.......................... Supported
  802.11a 54M Rate.......................... Supported
Max Clients.............................. 200

WLAN ID   Max Clients
---------   -------
  1   600
  2   600

Trap Threshold
  Clients................................. 12 clients
Interference ......................... 10 %
Noise .............................. -70 dBm
Utilization .......................... 80 %
Multicast Data Rate ................. 0
Rx Sop Threshold .................... -80 dBm
Cca Threshold ....................... 0 dBm
Slot Admin State ..................... Enabled

Band Select
Probe Response ..................... Disabled
Cycle Count .......................... 2 cycles
Cycle Threshold ..................... 200 milliseconds
Expire Suppression ................. 20 seconds
Expire Dual Band .................... 60 seconds
Client Rssi ........................ -80 dBm
Client Mid Rssi ...................... -80 dBm

Load Balancing
Denial ............................... 3 count
Window ............................... 5 clients

Coverage Data
Data ................................. -90 dBm
Voice ................................. -90 dBm
Minimum Client Level ............... 2 clients
Exception Level ..................... 25 %
DCA Channel List .................... 36,40,44,48,52,56,60,64,100,
                                  104,108,112,116,120,124,128,
                                  132,136,140,144,149,153,157,
                                  161
DCA Bandwidth................................. 20
DCA Foreign AP Contribution............... enabled

802.11n MCS Rates
  MCS-00 Rate........................ enabled
  MCS-01 Rate........................ enabled
  MCS-02 Rate........................ enabled
  MCS-03 Rate........................ enabled
  MCS-04 Rate........................ enabled
  MCS-05 Rate........................ enabled
  MCS-06 Rate........................ enabled
  MCS-07 Rate........................ enabled
  MCS-08 Rate........................ enabled
  MCS-09 Rate........................ enabled
  MCS-10 Rate........................ enabled
  MCS-11 Rate........................ enabled
  MCS-12 Rate........................ enabled
  MCS-13 Rate........................ enabled
  MCS-14 Rate........................ enabled
  MCS-15 Rate........................ enabled
  MCS-16 Rate........................ enabled
  MCS-17 Rate........................ enabled
  MCS-18 Rate........................ enabled
  MCS-19 Rate........................ enabled
  MCS-20 Rate........................ enabled
  MCS-21 Rate........................ enabled
  MCS-22 Rate........................ enabled
  MCS-23 Rate........................ enabled
  MCS-24 Rate........................ enabled
  MCS-25 Rate........................ enabled
MCS-26 Rate.............................. enabled
MCS-27 Rate.............................. enabled
MCS-28 Rate.............................. enabled
MCS-29 Rate.............................. enabled
MCS-30 Rate.............................. enabled
MCS-31 Rate.............................. enabled
Client Network Preference.................. default

RF Profile name............................. Low-Client-Density-802.11bg
Description................................. <none>
AP Group Name............................... <none>
Radio policy................................. 2.4 GHz
11n-client-only.............................. disabled
Transmit Power Threshold v1................. -65 dBm
Transmit Power Threshold v2................. -67 dBm
Min Transmit Power.......................... -10 dBm
Max Transmit Power.......................... 30 dBm
802.11b/g Operational Rates
  802.11b/g 1M Rate......................... Mandatory
  802.11b/g 2M Rate......................... Mandatory
  802.11b/g 5.5M Rate....................... Mandatory
  802.11b/g 11M Rate....................... Mandatory
  802.11g 6M Rate......................... Supported
  802.11g 9M Rate......................... Supported
  802.11g 12M Rate......................... Supported
  802.11g 18M Rate......................... Supported
  802.11g 24M Rate......................... Supported
  802.11g 36M Rate......................... Supported
  802.11g 48M Rate......................... Supported
  802.11g 54M Rate......................... Supported
Max Clients: 200

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>Max Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>600</td>
</tr>
<tr>
<td>2</td>
<td>600</td>
</tr>
</tbody>
</table>

**Trap Threshold**

- Clients: 12 clients
- Interference: 10%
- Noise: -70 dBm
- Utilization: 80%
- Multicast Data Rate: 0
- Rx Sop Threshold: -85 dBm
- Cca Threshold: 0 dBm
- Slot Admin State: Enabled

**Band Select**

- Probe Response: Disabled
- Cycle Count: 2 cycles
- Cycle Threshold: 200 milliseconds
- Expire Suppression: 20 seconds
- Expire Dual Band: 60 seconds
- Client Rssi: -80 dBm
- Client Mid Rssi: -80 dBm

**Load Balancing**

- Denial: 3 count
- Window: 5 clients
Coverage Data

- Data: -90 dBm
- Voice: -90 dBm
- Minimum Client Level: 2 clients
- Exception Level: 25%

DCA Channel List: 1, 6, 11
DCA Bandwidth: 20
DCA Foreign AP Contribution: enabled

802.11n MCS Rates

- MCS-00 Rate: enabled
- MCS-01 Rate: enabled
- MCS-02 Rate: enabled
- MCS-03 Rate: enabled
- MCS-04 Rate: enabled
- MCS-05 Rate: enabled
- MCS-06 Rate: enabled
- MCS-07 Rate: enabled
- MCS-08 Rate: enabled
- MCS-09 Rate: enabled
- MCS-10 Rate: enabled
- MCS-11 Rate: enabled
- MCS-12 Rate: enabled
- MCS-13 Rate: enabled
- MCS-14 Rate: enabled
- MCS-15 Rate: enabled
- MCS-16 Rate: enabled
- MCS-17 Rate: enabled
- MCS-18 Rate: enabled
- MCS-19 Rate: enabled
MCS-20 Rate.......................... enabled
MCS-21 Rate.......................... enabled
MCS-22 Rate.......................... enabled
MCS-23 Rate.......................... enabled
MCS-24 Rate.......................... enabled
MCS-25 Rate.......................... enabled
MCS-26 Rate.......................... enabled
MCS-27 Rate.......................... enabled
MCS-28 Rate.......................... enabled
MCS-29 Rate.......................... enabled
MCS-30 Rate.......................... enabled
MCS-31 Rate.......................... enabled
Client Network Preference............... default

RF Profile name......................... Typical-Client-Density-802.11a
Description............................ <none>
AP Group Name........................ <none>
Radio policy............................ 5 GHz
11n-client-only.......................... disabled
Transmit Power Threshold v1............. -70 dBm
Transmit Power Threshold v2............. -67 dBm
Min Transmit Power..................... -10 dBm
Max Transmit Power..................... 30 dBm
802.11a Operational Rates
  802.11a 6M Rate......................... Mandatory
  802.11a 9M Rate......................... Supported
  802.11a 12M Rate......................... Mandatory
  802.11a 18M Rate......................... Supported
  802.11a 24M Rate......................... Mandatory
  802.11a 36M Rate......................... Supported
802.11a 48M Rate......................... Supported
802.11a 54M Rate......................... Supported
Max Clients................................. 200

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>Max Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>600</td>
</tr>
<tr>
<td>2</td>
<td>600</td>
</tr>
</tbody>
</table>

Trap Threshold
- Clients................................. 12 clients
- Interference.......................... 10 %
- Noise.................................-70 dBm
- Utilization............................ 80 %
- Multicast Data Rate.................... 0
- Rx Sop Threshold....................... AUTO
- Cca Threshold.......................... 0 dBm
- Slot Admin State:........................ Enabled

Band Select
- Probe Response.......................... Disabled
- Cycle Count............................. 2 cycles
- Cycle Threshold.......................... 200 milliseconds
- Expire Suppression..................... 20 seconds
- Expire Dual Band....................... 60 seconds
- Client Rssi............................. -80 dBm
- Client Mid Rssi......................... -80 dBm

Load Balancing
- Denial.................................. 3 count
Window....................................... 5 clients

Coverage Data
Data........................................... -80 dBm
Voice.......................................... -80 dBm
Minimum Client Level......................... 3 clients
Exception Level.............................. 25 %
DCA Channel List............................. 36,40,44,48,52,56,60,64,100,
        104,108,112,116,120,124,128,
        132,136,140,144,149,153,157,
        161
DCA Bandwidth................................. 20
DCA Foreign AP Contribution............... enabled

802.11n MCS Rates
MCS-00 Rate................................. enabled
MCS-01 Rate................................. enabled
MCS-02 Rate................................. enabled
MCS-03 Rate................................. enabled
MCS-04 Rate................................. enabled
MCS-05 Rate................................. enabled
MCS-06 Rate................................. enabled
MCS-07 Rate................................. enabled
MCS-08 Rate................................. enabled
MCS-09 Rate................................. enabled
MCS-10 Rate................................. enabled
MCS-11 Rate................................. enabled
MCS-12 Rate................................. enabled
MCS-13 Rate................................. enabled
MCS-14 Rate................................. enabled
MCS-15 Rate............................... enabled
MCS-16 Rate............................... enabled
MCS-17 Rate............................... enabled
MCS-18 Rate............................... enabled
MCS-19 Rate............................... enabled
MCS-20 Rate............................... enabled
MCS-21 Rate............................... enabled
MCS-22 Rate............................... enabled
MCS-23 Rate............................... enabled
MCS-24 Rate............................... enabled
MCS-25 Rate............................... enabled
MCS-26 Rate............................... enabled
MCS-27 Rate............................... enabled
MCS-28 Rate............................... enabled
MCS-29 Rate............................... enabled
MCS-30 Rate............................... enabled
MCS-31 Rate............................... enabled
Client Network Preference.............. default

RF Profile name............................. Typical-Client-Density-802.11bg
Description................................... <none>
AP Group Name.............................. <none>
Radio policy................................... 2.4 GHz
11n-client-only............................. disabled
Transmit Power Threshold v1............. -70 dBm
Transmit Power Threshold v2............. -67 dBm
Min Transmit Power......................... -10 dBm
Max Transmit Power......................... 30 dBm
802.11b/g Operational Rates
   802.11b/g 1M Rate......................... Disabled
802.11b/g 2M Rate............................ Disabled
802.11b/g 5.5M Rate.......................... Disabled
802.11b/g 11M Rate........................... Disabled
802.11g 6M Rate.............................. Supported
802.11g 9M Rate.............................. Supported
802.11g 12M Rate............................. Mandatory
802.11g 18M Rate............................. Supported
802.11g 24M Rate............................. Supported
802.11g 36M Rate............................. Supported
802.11g 48M Rate............................. Supported
802.11g 54M Rate............................. Supported
Max Clients...................................... 200

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>Max Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>600</td>
</tr>
<tr>
<td>2</td>
<td>600</td>
</tr>
</tbody>
</table>

Trap Threshold

- Clients................................. 12 clients
- Interference............................ 10 %
- Noise.................................... -70 dBm
- Utilization.............................. 80 %

Multicast Data Rate................. 0
Rx Sop Threshold........................ AUTO
Cca Threshold............................ 0 dBm
Slot Admin State:....................... Enabled

Band Select

- Probe Response.......................... Disabled
Cycle Count.................................. 2 cycles
Cycle Threshold.............................. 200 milliseconds
Expire Suppression........................... 20 seconds
Expire Dual Band.................................. 60 seconds
Client Rssi.................................. -80 dBm
Client Mid Rssi.............................. -80 dBm

Load Balancing

Denial....................................... 3 count
Window....................................... 5 clients

Coverage Data

Data......................................... -80 dBm
Voice........................................ -80 dBm
Minimum Client Level......................... 3 clients
Exception Level.............................. 25 %
DCA Channel List................................ 1,6,11
DCA Bandwidth................................. 20
DCA Foreign AP Contribution............... enabled

802.11n MCS Rates

MCS-00 Rate.......................... enabled
MCS-01 Rate.......................... enabled
MCS-02 Rate.......................... enabled
MCS-03 Rate.......................... enabled
MCS-04 Rate.......................... enabled
MCS-05 Rate.......................... enabled
MCS-06 Rate.......................... enabled
MCS-07 Rate.......................... enabled
MCS-08 Rate.......................... enabled
MCS-09 Rate.......................... enabled
MCS-10 Rate.......................... enabled
MCS-11 Rate.......................... enabled
MCS-12 Rate.......................... enabled
MCS-13 Rate.......................... enabled
MCS-14 Rate.......................... enabled
MCS-15 Rate.......................... enabled
MCS-16 Rate.......................... enabled
MCS-17 Rate.......................... enabled
MCS-18 Rate.......................... enabled
MCS-19 Rate.......................... enabled
MCS-20 Rate.......................... enabled
MCS-21 Rate.......................... enabled
MCS-22 Rate.......................... enabled
MCS-23 Rate.......................... enabled
MCS-24 Rate.......................... enabled
MCS-25 Rate.......................... enabled
MCS-26 Rate.......................... enabled
MCS-27 Rate.......................... enabled
MCS-28 Rate.......................... enabled
MCS-29 Rate.......................... enabled
MCS-30 Rate.......................... enabled
MCS-31 Rate.......................... enabled

Client Network Preference.................. default

AP Config
Cisco AP Identifier....................... 3
Cisco AP Name........................... AP78da.6ee0.08ec
Country code............................ US - United States
Regulatory Domain allowed by Country.... 802.11bg:-A   802.11a:-AB
AP Country code: US - United States
AP Regulatory Domain: -A
Switch Port Number: 1
MAC Address: 78:da:6e:e0:08:ec
IP Address Configuration: DHCP
IP Address: 192.168.250.10
IP NetMask: 255.255.255.0
Gateway IP Addr: 192.168.250.1
NAT External IP Address: None
CAPWAP Path MTU: 1485
DHCP Release Override: Disabled
Telnet State: Globally Disabled
Ssh State: Globally Disabled
Cisco AP Location: default location
Cisco AP Floor Label: 0
Cisco AP Group Name: default-group
Primary Cisco Switch Name: 
Primary Cisco Switch IP Address: Not Configured
Secondary Cisco Switch Name: 
Secondary Cisco Switch IP Address: Not Configured
Tertiary Cisco Switch Name: 
Tertiary Cisco Switch IP Address: Not Configured
Administrative State: ADMIN_ENABLED
Operation State: REGISTERED
Mirroring Mode: Disabled
AP Mode: FlexConnect
Public Safety: Disabled
ATF Mode: Disable
AP SubMode: Not Configured
Rogue Detection: Enabled
DRAFT

AP Vlan Trunking ............................... Disabled
Remote AP Debug .............................. Disabled
Logging trap severity level ................. informational
Logging syslog facility ....................... kern
S/W Version ...................................... 8.2.111.0
Boot Version ..................................... 15.2.2.0
Mini IOS Version ............................... 7.5.1.73
Stats Reporting Period ....................... 180
Stats Collection Mode ......................... normal
LED State......................................... Enabled
PoE Pre-Standard Switch ...................... Disabled
PoE Power Injector MAC Addr................. Disabled
Power Type/Mode............................... PoE/Full Power
Number Of Slots............................... 2
AP Model........................................... AIR-CAP1602I-A-K9
AP Image.......................................... C1600-K9W8-M
IOS Version...................................... 15.3(3)JC2$
Reset Button..................................... Enabled
AP Serial Number............................... FGL1748W52Y
AP Certificate Type......................... Manufacture Installed
AP Lag Status ................................. Disable
Native Vlan Inheritance: ................. AP
FlexConnect Vlan mode ...................... Disabled
FlexConnect Group......................... Not a member of any group
Group VLAN ACL Mappings

Group VLAN Name to Id Mappings
Template in Modified State - apply it to see mappings

AP-Specific FlexConnect Policy ACLs:
L2Acl Configuration ......................... Not Available

FlexConnect Local-Split ACLs :

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>PROFILE NAME</th>
<th>ACL</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------</td>
<td>--------------------</td>
<td>--------</td>
<td>-------</td>
</tr>
</tbody>
</table>

Flexconnect Central-Dhcp Values :

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>PROFILE NAME</th>
<th>Central-Dhcp</th>
<th>DNS Override</th>
<th>Nat-Pat</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP_Dev No Encryption</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>Wlan</td>
</tr>
</tbody>
</table>

Flex AVC visibility Configurations..............

<table>
<thead>
<tr>
<th>WlanId</th>
<th>PROFILE NAME</th>
<th>Inherit-level Visibility</th>
<th>Flex Avc-profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP_Dev No Encryption</td>
<td>wlan-spec</td>
<td>disable</td>
</tr>
</tbody>
</table>

FlexConnect Backup Auth Radius Servers :

Primary Radius Server......................... Disabled
Secondary Radius Server....................... Disabled
AP User Mode................................. AUTOMATIC
AP User Name................................. Cisco
AP Dot1x User Mode............................ Not Configured
AP Dot1x User Name............................ Not Configured
Cisco AP system logging host............... 255.255.255.255
AP Core Dump Config......................... Disabled
AP Up Time.................................. 2 days, 22 h 22 m 20 s
AP LWAPP Up Time............................. 2 days, 22 h 18 m 20 s
Join Date and Time......................... Mon Aug 15 21:47:06 2016
Join Taken Time: 0 days, 00 h 03 m 59 s

Attributes for Slot 0

- Radio Type: RADIO_TYPE_80211n-2.4
- Administrative State: ADMIN_ENABLED
- Operation State: UP
- Mesh Radio Role: ACCESS
- Radio Role: Client Serving (Remote)
- CellId: 0

Station Configuration

- Configuration: AUTOMATIC
- Number Of WLANs: 1
- Medium Occupancy Limit: 100
- CFP Period: 4
- CFP MaxDuration: 60
- BSSID: 5c:a4:8a:be:ca:90

Operation Rate Set

- 1000 Kilo Bits: MANDATORY
- 2000 Kilo Bits: MANDATORY
- 5500 Kilo Bits: MANDATORY
- 11000 Kilo Bits: MANDATORY
- 6000 Kilo Bits: SUPPORTED
- 9000 Kilo Bits: SUPPORTED
- 12000 Kilo Bits: SUPPORTED
- 18000 Kilo Bits: SUPPORTED
- 24000 Kilo Bits: SUPPORTED
- 36000 Kilo Bits: SUPPORTED
- 48000 Kilo Bits: SUPPORTED
- 54000 Kilo Bits: SUPPORTED
MCS Set

MCS 0................................. SUPPORTED
MCS 1................................. SUPPORTED
MCS 2................................. SUPPORTED
MCS 3................................. SUPPORTED
MCS 4................................. SUPPORTED
MCS 5................................. SUPPORTED
MCS 6................................. SUPPORTED
MCS 7................................. SUPPORTED
MCS 8................................. SUPPORTED
MCS 9................................. SUPPORTED
MCS 10............................... SUPPORTED
MCS 11............................... SUPPORTED
MCS 12............................... SUPPORTED
MCS 13............................... SUPPORTED
MCS 14............................... SUPPORTED
MCS 15............................... SUPPORTED
MCS 16............................... DISABLED
MCS 17............................... DISABLED
MCS 18............................... DISABLED
MCS 19............................... DISABLED
MCS 20............................... DISABLED
MCS 21............................... DISABLED
MCS 22............................... DISABLED
MCS 23............................... DISABLED
MCS 24............................... DISABLED
MCS 25............................... DISABLED
MCS 26............................... DISABLED
MCS 27............................... DISABLED
MCS 28............................... DISABLED
MCS 29.................................. DISABLED
MCS 30.................................. DISABLED
MCS 31.................................. DISABLED
Beacon Period ......................... 100
Fragmentation Threshold ............. 2346
Multi Domain Capability Implemented .... TRUE
Multi Domain Capability Enabled .......... TRUE
Country String ......................... US

Multi Domain Capability
Configuration ......................... AUTOMATIC
First Chan Num ...................... 1
Number Of Channels .............. 11

MAC Operation Parameters
Configuration ......................... AUTOMATIC
Fragmentation Threshold ............. 2346
Packet Retry Limit .................. 64

Tx Power
Num Of Supported Power Levels .......... 6
Tx Power Level 1 ....................... 22 dBm
Tx Power Level 2 ....................... 19 dBm
Tx Power Level 3 ....................... 16 dBm
Tx Power Level 4 ....................... 13 dBm
Tx Power Level 5 ....................... 10 dBm
Tx Power Level 6 ....................... 7 dBm
Tx Power Configuration ............... AUTOMATIC
Current Tx Power Level .............. 1
Tx Power Assigned By .............. DTPC
Phy OFDM parameters

Configuration .................................. AUTOMATIC
Current Channel ............................. 11
Channel Assigned By ......................... DCA
Extension Channel .......................... NONE
Channel Width .............................. 20 Mhz
Allowed Channel List ....................... 1,2,3,4,5,6,7,8,9,10,11
TI Threshold .............................. -50
DCA Channel List ........................... Global
Legacy Tx Beamforming Configuration .... CUSTOMIZED
Legacy Tx Beamforming ..................... ENABLED
Antenna Type ............................... INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBi units).... 8
Diversity .................................... DIVERSITY_ENABLED

802.11n Antennas
  A ............................................ ENABLED
  B ............................................ ENABLED
  C ............................................ ENABLED

Performance Profile Parameters

Configuration ............................... AUTOMATIC
Interference threshold ..................... 10 %
Noise threshold ............................ -70 dBm
RF utilization threshold .................... 80 %
Data-rate threshold ....................... 1000000 bps
Client threshold ........................... 12 clients
Coverage SNR threshold .................... 12 dB
Coverage exception level ................. 25 %
Client minimum exception level .......... 3 clients
Rogue Containment Information
Containment Count....................... 0

CleanAir Management Information

CleanAir Capable............................ Yes
CleanAir Management Administration St.... Enabled
CleanAir Management Operation State...... Down
Rapid Update Mode......................... Off
Spectrum Expert connection.............. Enabled
CleanAir NSI Key........................... C44B365F4CF338BE94B85633D98944B
Spectrum Expert Connections counter.... 0
CleanAir Sensor State...................... Configured

Radio Extended Configurations

Beacon period.............................. 100 milliseconds
Beacon range............................... AUTO
Multicast buffer......................... AUTO
Multicast data-rate....................... AUTO
RX SOP threshold......................... AUTO
CCA threshold............................. AUTO

Attributes for Slot  1

Radio Type................................ RADIO_TYPE_80211n-5
Radio Subband.............................. RADIO_SUBBAND_ALL
Administrative State ....................... ADMIN_ENABLED
Operation State ............................. UP
Mesh Radio Role ......................... ACCESS
Radio Role.................................. Client Serving (Remote)
CellId ..................................... 0
Station Configuration

Configuration .................................. AUTOMATIC
Number Of WLANs ............................ 1
Medium Occupancy Limit ................... 100
CFP Period ................................. 4
CFP MaxDuration ........................... 60
BSSID ..................................... 5c:a4:8a:be:ca:90

Operation Rate Set

6000 Kilo Bits........................... MANDATORY
9000 Kilo Bits........................... SUPPORTED
12000 Kilo Bits........................... MANDATORY
18000 Kilo Bits........................... SUPPORTED
24000 Kilo Bits........................... MANDATORY
36000 Kilo Bits........................... SUPPORTED
48000 Kilo Bits........................... SUPPORTED
54000 Kilo Bits........................... SUPPORTED

MCS Set

MCS 0................................. SUPPORTED
MCS 1................................. SUPPORTED
MCS 2................................. SUPPORTED
MCS 3................................. SUPPORTED
MCS 4................................. SUPPORTED
MCS 5................................. SUPPORTED
MCS 6................................. SUPPORTED
MCS 7................................. SUPPORTED
MCS 8................................. SUPPORTED
MCS 9................................. SUPPORTED
MCS 10............................... SUPPORTED
MCS 11............................... SUPPORTED
MCS 12............................... SUPPORTED
MCS 13................................. SUPPORTED
MCS 14................................. SUPPORTED
MCS 15................................. SUPPORTED
MCS 16................................. DISABLED
MCS 17................................. DISABLED
MCS 18................................. DISABLED
MCS 19................................. DISABLED
MCS 20................................. DISABLED
MCS 21................................. DISABLED
MCS 22................................. DISABLED
MCS 23................................. DISABLED
MCS 24................................. DISABLED
MCS 25................................. DISABLED
MCS 26................................. DISABLED
MCS 27................................. DISABLED
MCS 28................................. DISABLED
MCS 29................................. DISABLED
MCS 30................................. DISABLED
MCS 31................................. DISABLED
Beacon Period ......................... 100
Fragmentation Threshold .............. 2346
Multi Domain Capability Implemented .... TRUE
Multi Domain Capability Enabled ....... TRUE
Country String ......................... US

Multi Domain Capability
Configuration .......................... AUTOMATIC
First Chan Num ......................... 36
Number Of Channels .................. 21
MAC Operation Parameters

Configuration ............................. AUTOMATIC
Fragmentation Threshold ................. 2346
Packet Retry Limit ....................... 64

Tx Power

Num Of Supported Power Levels .......... 6
Tx Power Level 1 ........................ 22 dBm
Tx Power Level 2 ........................ 19 dBm
Tx Power Level 3 ........................ 16 dBm
Tx Power Level 4 ........................ 13 dBm
Tx Power Level 5 ........................ 10 dBm
Tx Power Level 6 ........................ 7 dBm
Tx Power Configuration .................... AUTOMATIC
Current Tx Power Level ................... 1
Tx Power Assigned By ..................... DTPC

Phy OFDM parameters

Configuration ............................. AUTOMATIC
Current Channel ......................... 149
Channel Assigned By ..................... DCA
Extension Channel ....................... NONE
Channel Width ............................ 20 Mhz
TI Threshold ............................. -50
DCA Channel List ......................... Global
Legacy Tx Beamforming Configuration .... CUSTOMIZED
Legacy Tx Beamforming .................. ENABLED
Antenna Type ............................. INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBi units).... 8
Diversity.................................. DIVERSITY_ENABLED

802.11n Antennas
   A....................................... ENABLED
   B....................................... ENABLED
   C....................................... ENABLED

Performance Profile Parameters
   Configuration ............................. AUTOMATIC
   Interference threshold..................... 10 %
   Noise threshold............................ -70 dBm
   RF utilization threshold................... 80 %
   Data-rate threshold....................... 1000000 bps
   Client threshold........................... 12 clients
   Coverage SNR threshold................... 16 dB
   Coverage exception level.................. 25 %
   Client minimum exception level.......... 3 clients

Rogue Containment Information
   Containment Count......................... 0

CleanAir Management Information
   CleanAir Capable.......................... Yes
   CleanAir Management Administration St.... Enabled
   CleanAir Management Operation State...... Down
   Rapid Update Mode........................ Off
   Spectrum Expert connection............... Enabled
   CleanAir NSI Key.......................... C44B365F4CFF338BE94B85633D98944B
   Spectrum Expert Connections counter.... 0
   CleanAir Sensor State.................... Configured
Radio Extended Configurations

Beacon period.............................. 100 milliseconds
Beacon range............................... AUTO
Multicast buffer........................... AUTO
Multicast data-rate........................ AUTO
RX SOP threshold........................... AUTO
CCA threshold............................... AUTO

Cisco AP Identifier.......................... 4
Cisco AP Name............................... AP24e9.b34b.f1ed
Country code................................. US - United States
Regulatory Domain allowed by Country...... 802.11bg:-A  802.11a:-AB
AP Country code.............................. US - United States
AP Regulatory Domain......................... -A
Switch Port Number ........................... 1
MAC Address................................. 24:e9:b3:4b:f1:ed
IP Address Configuration..................... DHCP
IP Address................................. 192.168.250.11
IP NetMask.................................. 255.255.255.0
Gateway IP Addr............................. 192.168.250.1
NAT External IP Address...................... None
CAPWAP Path MTU............................ 1485
DHCP Release Override....................... Disabled
Telnet State................................. Globally Disabled
Ssh State................................. Globally Disabled
Cisco AP Location........................... default location
Cisco AP Floor Label......................... 0
Cisco AP Group Name......................... default-group
Primary Cisco Switch Name..................
Primary Cisco Switch IP Address............ Not Configured
Secondary Cisco Switch Name

Secondary Cisco Switch IP Address Not Configured

Tertiary Cisco Switch Name

Tertiary Cisco Switch IP Address Not Configured

Administrative State ADMIN_ENABLED

Operation State REGISTERED

Mirroring Mode Disabled

AP Mode FlexConnect

Public Safety Disabled

ATF Mode Disable

AP SubMode Not Configured

Rogue Detection Enabled

AP Vlan Trunking Disabled

Remote AP Debug Disabled

Logging trap severity level emergencies

Logging syslog facility system

S/W Version 8.2.111.0

Boot Version 15.2.2.0

Mini IOS Version 7.5.1.73

Stats Reporting Period 180

Stats Collection Mode normal

LED State Enabled

PoE Pre-Standard Switch Disabled

PoE Power Injector MAC Addr Disabled

Power Type/Mode PoE/Full Power

Number Of Slots 2

AP Model AIR-CAP1602I-A-K9

AP Image C1600-K9W8-M

IOS Version 15.3(3)JC2$

Reset Button Enabled
AP Serial Number............................... FGL1748W52S
AP Certificate Type......................... Manufacture Installed
AP Lag Status ................................. Disable
Native Vlan Inheritance:..................... Group
FlexConnect Vlan mode ....................... Disabled
FlexConnect Group............................ Not a member of any group

Group VLAN ACL Mappings

Group VLAN Name to Id Mappings
Template in Modified State - apply it to see mappings

AP-Specific FlexConnect Policy ACLs:
L2Acl Configuration ............................ Not Available

FlexConnect Local-Split ACLs:

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>PROFILE NAME</th>
<th>ACL</th>
<th>TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flexconnect Central-Dhcp Values:

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>PROFILE NAME</th>
<th>Central-Dhcp</th>
<th>DNS Override</th>
<th>Nat-Pat</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP_Dev No Encryption</td>
<td>False</td>
<td>False</td>
<td>False</td>
<td>Wlan</td>
</tr>
</tbody>
</table>

Flex AVC visibility Configurations..............

<table>
<thead>
<tr>
<th>WlanId</th>
<th>PROFILE NAME</th>
<th>Inherit-level Visibility</th>
<th>Flex Avc-profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP_Dev No Encryption</td>
<td>wlan-spec</td>
<td>disable</td>
</tr>
</tbody>
</table>
FlexConnect Backup Auth Radius Servers:
Primary Radius Server........................... Disabled
Secondary Radius Server......................... Disabled
AP User Mode..................................... AUTOMATIC
AP User Name..................................... Cisco
AP Dot1x User Mode............................... Not Configured
AP Dot1x User Name............................... Not Configured
Cisco AP system logging host.................... 255.255.255.255
AP Core Dump Config.............................. Disabled
AP Up Time....................................... 2 days, 22 h 22 m 16 s
AP LWAPP Up Time................................. 2 days, 22 h 18 m 14 s
Join Date and Time............................... Mon Aug 15 21:47:12 2016
Join Taken Time.................................. 0 days, 00 h 04 m 01 s

Attributes for Slot 0
Radio Type.................................. RADIO_TYPE_80211n-2.4
Administrative State ......................... ADMIN_ENABLED
Operation State ............................... UP
Mesh Radio Role .............................. ACCESS
Radio Role .................................. Client Serving (Remote)
CellId ...................................... 0

Station Configuration
Configuration ................................. AUTOMATIC
Number Of WLANs ............................. 1
Medium Occupancy Limit ....................... 100
CFP Period ................................. 4
CFP MaxDuration ............................. 60
BSSID ...................................... 1c:1d:86:31:e5:50
Operation Rate Set
1000 Kilo Bits........................... MANDATORY
2000 Kilo Bits........................... MANDATORY
5500 Kilo Bits........................... MANDATORY
11000 Kilo Bits.......................... MANDATORY
6000 Kilo Bits........................... SUPPORTED
9000 Kilo Bits........................... SUPPORTED
12000 Kilo Bits.......................... SUPPORTED
18000 Kilo Bits.......................... SUPPORTED
24000 Kilo Bits.......................... SUPPORTED
36000 Kilo Bits.......................... SUPPORTED
48000 Kilo Bits.......................... SUPPORTED
54000 Kilo Bits.......................... SUPPORTED

MCS Set
MCS 0................................. SUPPORTED
MCS 1................................. SUPPORTED
MCS 2................................. SUPPORTED
MCS 3................................. SUPPORTED
MCS 4................................. SUPPORTED
MCS 5................................. SUPPORTED
MCS 6................................. SUPPORTED
MCS 7................................. SUPPORTED
MCS 8................................. SUPPORTED
MCS 9................................. SUPPORTED
MCS 10............................... SUPPORTED
MCS 11............................... SUPPORTED
MCS 12............................... SUPPORTED
MCS 13............................... SUPPORTED
MCS 14............................... SUPPORTED
MCS 15............................... SUPPORTED
MCS 16............................... DISABLED
MCS 17............................... DISABLED
MCS 18............................... DISABLED
MCS 19............................... DISABLED
MCS 20............................... DISABLED
MCS 21............................... DISABLED
MCS 22............................... DISABLED
MCS 23............................... DISABLED
MCS 24............................... DISABLED
MCS 25............................... DISABLED
MCS 26............................... DISABLED
MCS 27............................... DISABLED
MCS 28............................... DISABLED
MCS 29............................... DISABLED
MCS 30............................... DISABLED
MCS 31............................... DISABLED

Beacon Period ..................... 100
Fragmentation Threshold ........... 2346
Multi Domain Capability Implemented ...... TRUE
Multi Domain Capability Enabled .......... TRUE
Country String ......................... US

Multi Domain Capability
Configuration ........................ AUTOMATIC
First Chan Num ........................ 1
Number Of Channels .................. 11

MAC Operation Parameters
Configuration ........................ AUTOMATIC
Fragmentation Threshold ............... 2346
Packet Retry Limit ..................... 64
Tx Power

Num Of Supported Power Levels .......... 6
Tx Power Level 1 ......................... 22 dBm
Tx Power Level 2 ......................... 19 dBm
Tx Power Level 3 ......................... 16 dBm
Tx Power Level 4 ......................... 13 dBm
Tx Power Level 5 ......................... 10 dBm
Tx Power Level 6 ......................... 7 dBm
Tx Power Configuration .................... AUTOMATIC
Current Tx Power Level .................... 1
Tx Power Assigned By ..................... DTPC

Phy OFDM parameters

Configuration ............................ AUTOMATIC
Current Channel ......................... 11
Channel Assigned By ...................... DCA
Extension Channel ....................... NONE
Channel Width ......................... 20 Mhz
Allowed Channel List ................... 1,2,3,4,5,6,7,8,9,10,11
TI Threshold .......................... -50
DCA Channel List ....................... Global
Legacy Tx Beamforming Configuration ...... CUSTOMIZED
Legacy Tx Beamforming .................. ENABLED
Antenna Type .......................... INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBi units) .... 8
Diversity .......................... DIVERSITY_ENABLED

802.11n Antennas

A ..................................... ENABLED
B ..................................... ENABLED
C....................................... ENABLED

Performance Profile Parameters
Configuration ................................ AUTOMATIC
Interference threshold.................... 10 %
Noise threshold............................ -70 dBm
RF utilization threshold............... 80 %
Data-rate threshold....................... 1000000 bps
Client threshold.......................... 12 clients
Coverage SNR threshold................... 12 dB
Coverage exception level............... 25 %
Client minimum exception level......... 3 clients

Rogue Containment Information
Containment Count......................... 0

CleanAir Management Information
CleanAir Capable......................... Yes
CleanAir Management Administration St.... Disabled
CleanAir Management Operation State...... Down
Rapid Update Mode .................. Off
Spectrum Expert connection .......... Enabled
CleanAir NSI Key............................. 8994C2313910BF9588C6693603B8F970
Spectrum Expert Connections counter.... 0
CleanAir Sensor State .................. Configured

Radio Extended Configurations
Beacon period......................... 100 milliseconds
Beacon range.......................... AUTO
Multicast buffer...................... AUTO
Multicast data-rate.................. AUTO
RX SOP threshold.......................... AUTO
CCA threshold............................ AUTO

Attributes for Slot  1
Radio Type................................. RADIO_TYPE_80211n-5
Radio Subband............................. RADIO_SUBBAND_ALL
Administrative State ....................... ADMIN_ENABLED
Operation State ............................ UP
Mesh Radio Role ............................. ACCESS
Radio Role .................................. Client Serving (Remote)
CellId ...................................... 0

Station Configuration
Configuration ............................... AUTOMATIC
Number Of WLANs ............................. 1
Medium Occupancy Limit .................... 100
CFP Period .................................. 4
CFP MaxDuration ............................ 60
BSSID ...................................... 1c:1d:86:31:e5:50

Operation Rate Set
6000 Kilo Bits.............................. MANDATORY
9000 Kilo Bits.............................. SUPPORTED
12000 Kilo Bits............................. MANDATORY
18000 Kilo Bits............................. SUPPORTED
24000 Kilo Bits............................. MANDATORY
36000 Kilo Bits............................. SUPPORTED
48000 Kilo Bits............................. SUPPORTED
54000 Kilo Bits............................. SUPPORTED

MCS Set
MCS 0..................................... SUPPORTED
MCS 1...................... SUPPORTED
MCS 2...................... SUPPORTED
MCS 3...................... SUPPORTED
MCS 4...................... SUPPORTED
MCS 5...................... SUPPORTED
MCS 6...................... SUPPORTED
MCS 7...................... SUPPORTED
MCS 8...................... SUPPORTED
MCS 9...................... SUPPORTED
MCS 10..................... SUPPORTED
MCS 11..................... SUPPORTED
MCS 12..................... SUPPORTED
MCS 13..................... SUPPORTED
MCS 14..................... SUPPORTED
MCS 15..................... SUPPORTED
MCS 16..................... DISABLED
MCS 17..................... DISABLED
MCS 18..................... DISABLED
MCS 19..................... DISABLED
MCS 20..................... DISABLED
MCS 21..................... DISABLED
MCS 22..................... DISABLED
MCS 23..................... DISABLED
MCS 24..................... DISABLED
MCS 25..................... DISABLED
MCS 26..................... DISABLED
MCS 27..................... DISABLED
MCS 28..................... DISABLED
MCS 29..................... DISABLED
MCS 30..................... DISABLED
MCS 31................................. DISABLED
Beacon Period ....................... 100
Fragmentation Threshold ............. 2346
Multi Domain Capability Implemented .... TRUE
Multi Domain Capability Enabled ........ TRUE
Country String ......................... US

Multi Domain Capability
  Configuration ........................ AUTOMATIC
  First Chan Num ....................... 36
  Number Of Channels .................. 21

MAC Operation Parameters
  Configuration ........................ AUTOMATIC
  Fragmentation Threshold ............. 2346
  Packet Retry Limit ................... 64

Tx Power
  Num Of Supported Power Levels .......... 6
  Tx Power Level 1 ...................... 22 dBm
  Tx Power Level 2 ...................... 19 dBm
  Tx Power Level 3 ...................... 16 dBm
  Tx Power Level 4 ...................... 13 dBm
  Tx Power Level 5 ...................... 10 dBm
  Tx Power Level 6 ...................... 7 dBm
  Tx Power Configuration ............... AUTOMATIC
  Current Tx Power Level ............... 1
  Tx Power Assigned By .................. DTPC

Phy OFDM parameters
Configuration ......................... AUTOMATIC
Current Channel ....................... 48
Channel Assigned By ................. DCA
Extension Channel .................... NONE
Channel Width ......................... 20 Mhz
Allowed Channel List .................. 36,40,44,48,52,56,60,64,100,
.......................................... 104,108,112,116,132,136,140,
.......................................... 149,153,157,161,165
TI Threshold ............................. -50
DCA Channel List ....................... Global
Legacy Tx Beamforming Configuration .... CUSTOMIZED
Legacy Tx Beamforming .................. ENABLED
Antenna Type ............................ INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBi units).... 8
Diversity ................................. DIVERSITY_ENABLED
802.11n Antennas
  A ....................................... ENABLED
  B ....................................... ENABLED
  C ....................................... ENABLED

Performance Profile Parameters
Configuration ......................... AUTOMATIC
Interference threshold ............... 10 %
Noise threshold ........................ -70 dBm
RF utilization threshold ............. 80 %
Data-rate threshold .................... 1000000 bps
Client threshold ....................... 12 clients
Coverage SNR threshold ............... 16 db
Coverage exception level ............. 25 %
Client minimum exception level ...... 3 clients
Rogue Containment Information
Containment Count....................... 0

CleanAir Management Information
CleanAir Capable.......................... Yes
CleanAir Management Administration St.... Disabled
CleanAir Management Operation State...... Down
Rapid Update Mode......................... Off
Spectrum Expert connection............... Enabled
CleanAir NSI Key............................ 8994C2313910BF9588C6693603B8F970
Spectrum Expert Connections counter.... 0
CleanAir Sensor State....................... Configured

Radio Extended Configurations
Beacon period.............................. 100 milliseconds
Beacon range............................... AUTO
Multicast buffer........................... AUTO
Multicast data-rate........................ AUTO
RX SOP threshold........................... AUTO
CCA threshold.............................. AUTO

AP Airewave Director Configuration
AP does not have the 802.11-abgn radio.
Number Of Slots........................... 2
AP Name........................................ AP78da.6ee0.08ec
MAC Address................................. 78:da:6e:e0:08:ec
Slot ID......................................... 0
Radio Type................................. RADIO_TYPE_80211b/g
Sub-band Type.............................. All

Noise Information
Noise Profile................................ PASSED

Interference Information
Interference Profile......................... PASSED
Rogue Histogram (20)

Load Information
Load Profile.................................. PASSED
Receive Utilization.......................... 0 %
Transmit Utilization.......................... 0 %
Channel Utilization............................ 38 %
Attached Clients.............................. 0 clients

Coverage Information
Coverage Profile.............................. PASSED
Failed Clients............................... 0 clients

Client Signal Strengths
RSSI -100 dbm................................. 0 clients
RSSI -92 dbm.................................. 0 clients
RSSI -84 dbm.................................. 0 clients
RSSI -76 dbm.................................. 0 clients
RSSI -68 dbm.................................. 0 clients
RSSI -60 dbm.................................. 0 clients
RSSI -52 dbm.................................. 0 clients

Client Signal To Noise Ratios
SNR  0 dB.................................... 0 clients
SNR  5 dB.................................... 0 clients
SNR  10 dB................................... 0 clients
SNR  15 dB................................... 0 clients
SNR  20 dB................................... 0 clients
SNR  25 dB................................... 0 clients
SNR  30 dB................................... 0 clients
SNR  35 dB.................................. 0 clients
SNR  40 dB.................................. 0 clients
SNR  45 dB.................................. 0 clients

Nearby APs

Radar Information

Channel Assignment Information

Current Channel Average Energy............. -127 dBm
Previous Channel Average Energy............. -127 dBm
Channel Change Count....................... 415

Last Channel Change Time.................... Thu Aug 18 20:01:53 2016
Recommended Best Channel.................. 11

RF Parameter Recommendations

Power Level................................. 1
RTS/CTS Threshold.......................... 2347
Fragmentation Threshold...................... 2346
Antenna Pattern............................. 0

Persistent Interference Devices

Class Type  Channel  DC (%)  RSSI (dBm)  Last Update Time

--------------------------------- ----- ------ --------------

All third party trademarks are the property of their respective owners.

Number Of Slots............................ 2

AP Name..................................... AP78da.6ee0.08ec
MAC Address............................... 78:da:6e:e0:08:ec
Slot ID..................................... 1
Radio Type.................................. RADIO_TYPE_80211a
Sub-band Type.............................. All
Noise Information

Noise Profile.............................. PASSED

Interference Information
Interference Profile....................... PASSED
Rogue Histogram (20/40/80/160)

Load Information
Load Profile............................... PASSED
Receive Utilization...................... 0 %
Transmit Utilization..................... 0 %
Channel Utilization..................... 1 %
Attached Clients....................... 0 clients

Coverage Information
Coverage Profile.......................... PASSED
Failed Clients.......................... 0 clients

Client Signal Strengths
RSSI -100 dbm........................... 0 clients
RSSI -92 dbm.............................. 0 clients
RSSI -84 dbm.............................. 0 clients
RSSI -76 dbm.............................. 0 clients
RSSI -68 dbm.............................. 0 clients
RSSI -60 dbm.............................. 0 clients
RSSI -52 dbm.............................. 0 clients

Client Signal To Noise Ratios
SNR   0 dB............................... 0 clients
SNR   5 dB............................... 0 clients
SNR   10 dB............................. 0 clients
SNR   15 dB............................. 0 clients
SNR   20 dB............................. 0 clients
SNR   25 dB............................. 0 clients
SNR   30 dB............................. 0 clients
SNR   35 dB............................. 0 clients
SNR   40 dB............................. 0 clients
SNR: 45 dB, 0 clients

Nearby APs:

Radar Information:

Channel Assignment Information:

Current Channel Average Energy: -127 dBm
Previous Channel Average Energy: -127 dBm
Channel Change Count: 417
Last Channel Change Time: Thu Aug 18 20:05:14 2016
Recommended Best Channel: 149

RF Parameter Recommendations:

Power Level: 1
RTS/CTS Threshold: 2347
Fragmentation Threshold: 2346
Antenna Pattern: 0

Persistent Interference Devices:

Class Type | Channel | DC (%) | RSSI (dBm) | Last Update Time
---------- | ------ | ------ | ---------- | ------------------------

All third party trademarks are the property of their respective owners.

AP does not have the 802.11-abgn radio.

Number Of Slots: 2

AP Name: AP24e9.b34b.f1ed
MAC Address: 24:e9:b3:4b:f1:ed
Slot ID: 0
Radio Type: RADIO_TYPE_80211b/g
Sub-band Type: All

Noise Information:

Noise Profile: PASSED

Interference Information:
Interference Profile....................... PASSED
Rogue Histogram (20)

.............................................

Load Information
Load Profile............................... PASSED
Receive Utilization....................... 0 %
Transmit Utilization....................... 0 %
Channel Utilization....................... 34 %
Attached Clients......................... 1 clients

Coverage Information
Coverage Profile.......................... PASSED
Failed Clients............................ 0 clients

Client Signal Strengths
RSSI -100 dbm............................ 0 clients
RSSI  -92 dbm............................... 0 clients
RSSI  -84 dbm............................... 0 clients
RSSI  -76 dbm............................... 0 clients
RSSI  -68 dbm............................... 0 clients
RSSI  -60 dbm............................... 0 clients
RSSI  -52 dbm............................... 1 clients

Client Signal To Noise Ratios
SNR   0 dB................................. 0 clients
SNR   5 dB................................. 0 clients
SNR   10 dB................................. 0 clients
SNR   15 dB................................. 0 clients
SNR   20 dB................................. 0 clients
SNR   25 dB................................. 0 clients
SNR   30 dB................................. 0 clients
SNR   35 dB................................. 0 clients
SNR   40 dB................................. 0 clients
SNR  45 dB.................................. 1 clients

Nearby APs

Radar Information

Channel Assignment Information

Current Channel Average Energy.............. -127 dBm
Previous Channel Average Energy.............. -127 dBm
Channel Change Count.......................... 415
Last Channel Change Time..................... Thu Aug 18 20:01:53 2016
Recommended Best Channel.................... 11

RF Parameter Recommendations

Power Level................................. 1
RTS/CTS Threshold............................ 2347
Fragmentation Threshold...................... 2346
Antenna Pattern............................. 0

Persistent Interference Devices

<table>
<thead>
<tr>
<th>Class Type</th>
<th>Channel</th>
<th>DC (%)</th>
<th>RSSI (dBm)</th>
<th>Last Update Time</th>
</tr>
</thead>
</table>
| All third party trademarks are the property of their respective owners.

Number Of Slots.............................. 2

AP Name.................................. AP24e9.b34b.f1ed
MAC Address.................................. 24:e9:b3:4b:f1:ed
Slot ID................................... 1
Radio Type................................. RADIO_TYPE_80211a
Sub-band Type............................ All

Noise Information

Noise Profile............................... PASSED

Interference Information

Interference Profile...................... PASSED
Rogue Histogram (20/40/80/160)
Load Information

Load Profile............................... PASSED
Receive Utilization..................... 0 %
Transmit Utilization..................... 0 %
Channel Utilization..................... 0 %
Attached Clients........................ 0 clients

Coverage Information

Coverage Profile.......................... PASSED
Failed Clients............................ 0 clients

Client Signal Strengths

RSSI -100 dbm............................. 0 clients
RSSI -92 dbm............................... 0 clients
RSSI -84 dbm............................... 0 clients
RSSI -76 dbm............................... 0 clients
RSSI -68 dbm............................... 0 clients
RSSI -60 dbm............................... 0 clients
RSSI -52 dbm............................... 0 clients

Client Signal To Noise Ratios

SNR    0 dB.................................. 0 clients
SNR    5 dB.................................. 0 clients
SNR    10 dB................................. 0 clients
SNR    15 dB................................. 0 clients
SNR    20 dB................................. 0 clients
SNR    25 dB................................. 0 clients
SNR    30 dB................................. 0 clients
SNR    35 dB................................. 0 clients
SNR    40 dB................................. 0 clients
SNR    45 dB................................. 0 clients

Nearby APs
Radar Information

Channel Assignment Information

Current Channel Average Energy.............. -127 dBm
Previous Channel Average Energy.............. -127 dBm
Channel Change Count......................... 417
Last Channel Change Time..................... Thu Aug 18 20:05:14 2016
Recommended Best Channel...................... 48

RF Parameter Recommendations

Power Level.................................. 1
RTS/CTS Threshold............................ 2347
Fragmentation Threshold...................... 2346
Antenna Pattern.............................. 0

Persistent Interference Devices

<table>
<thead>
<tr>
<th>Class Type</th>
<th>Channel</th>
<th>DC (%)</th>
<th>RSSI (dBm)</th>
<th>Last Update Time</th>
</tr>
</thead>
</table>

All third party trademarks are the property of their respective owners.

802.11a Configuration

802.11a Network............................... Enabled
11acSupport.................................. Enabled
11nSupport.................................... Enabled
  802.11a Low Band........................... Enabled
  802.11a Mid Band........................... Enabled
  802.11a High Band......................... Enabled

802.11a Operational Rates

802.11a 6M Rate............................... Mandatory
802.11a 9M Rate............................... Supported
802.11a 12M Rate............................. Mandatory
802.11a 18M Rate............................. Supported
802.11a 24M Rate............................ Mandatory
802.11a 36M Rate............................ Supported
802.11a 48M Rate............................ Supported
802.11a 54M Rate............................ Supported

802.11n MCS Settings:
MCS 0........................................ Supported
MCS 1........................................ Supported
MCS 2........................................ Supported
MCS 3........................................ Supported
MCS 4........................................ Supported
MCS 5........................................ Supported
MCS 6........................................ Supported
MCS 7........................................ Supported
MCS 8........................................ Supported
MCS 9........................................ Supported
MCS 10................................. Supported
MCS 11.............................. Supported
MCS 12............................ Supported
MCS 13............................ Supported
MCS 14............................ Supported
MCS 15............................ Supported
MCS 16............................ Supported
MCS 17............................ Supported
MCS 18............................ Supported
MCS 19............................ Supported
MCS 20............................ Supported
MCS 21............................ Supported
MCS 22............................ Supported
MCS 23............................ Supported
MCS 24............................ Supported
MCS 25....................................... Supported
MCS 26....................................... Supported
MCS 27....................................... Supported
MCS 28....................................... Supported
MCS 29....................................... Supported
MCS 30....................................... Supported
MCS 31....................................... Supported

802.11ac MCS Settings:
  Nss=1: MCS 0-9 .............................. Supported
  Nss=2: MCS 0-9 .............................. Supported
  Nss=3: MCS 0-9 .............................. Supported
  Nss=4: MCS 0-7 .............................. Supported

802.11n Status:
  A-MPDU Tx:
    Priority 0............................... Enabled
    Priority 1............................... Enabled
    Priority 2............................... Enabled
    Priority 3............................... Enabled
    Priority 4............................... Enabled
    Priority 5............................... Enabled
    Priority 6............................... Disabled
    Priority 7............................... Disabled
  Aggregation scheduler............... Enabled
  Frame Burst......................... Automatic
    Realtime Timeout.................. 10
    Non Realtime Timeout............. 200

  A-MSDU Tx:
    Priority 0............................... Enabled
    Priority 1............................... Enabled
    Priority 2............................... Enabled
Priority 3.................................. Enabled
Priority 4.................................. Enabled
Priority 5.................................. Enabled
Priority 6.................................. Disabled
Priority 7.................................. Disabled
A-MSDU Max Subframes .................... 3
A-MSDU MAX Length ......................... 8k
Rifs Rx .................................... Enabled
Guard Interval ......................... Any
Beacon Interval .................. 100
CF Pollable mandatory............. Disabled
CF Poll Request mandatory........ Disabled
CFP Period .......................... 4
CFP Maximum Duration ............. 60
Default Channel .................... 36
Default Tx Power Level ............ 0
DTPC Status ......................... Enabled
Fragmentation Threshold .......... 2346
RSSI Low Check ..................... Disabled
RSSI Threshold .................... -80
TI Threshold ....................... -50
Legacy Tx Beamforming setting .... Disabled
Traffic Stream Metrics Status ...... Disabled
Expedited BW Request Status ...... Disabled
World Mode......................... Enabled
dfs-peakedetect .................... Enabled
EDCA profile type ................ default-wmm
Voice MAC optimization status .... Disabled
Call Admission Control (CAC) configuration
Voice AC:
Voice AC - Admission control (ACM)............ Disabled
Voice Stream-Size............................ 84000
Voice Max-Streams............................ 2
Voice max RF bandwidth....................... 75
Voice reserved roaming bandwidth............. 6
Voice CAC Method............................ Load-Based
Voice tspec inactivity timeout............... Disabled

CAC SIP-Voice configuration
SIP based CAC................................ Disabled
SIP Codec Type............................ CODEC_TYPE_G711
SIP call bandwidth......................... 64
SIP call bandwidth sample-size............ 20

Video AC:
Video AC - Admission control (ACM)............ Disabled
Video max RF bandwidth....................... Infinite
Video reserved roaming bandwidth........... 0
Video load-based CAC mode.................. Disabled
Video CAC Method............................ Static

CAC SIP-Video Configuration
SIP based CAC................................ Disabled

Best-effort AC - Admission control (ACM).... Disabled
Background AC - Admission control (ACM).... Disabled

Maximum Number of Clients per AP Radio...... 200

802.11a Advanced Configuration

Member RRM Information

<table>
<thead>
<tr>
<th>AP Name</th>
<th>MAC Address</th>
<th>Slot Admin</th>
<th>Oper</th>
<th>Channel</th>
<th>TxPower</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP78da.6ee0.08ec</td>
<td>5c:a4:8a:be:ca:90</td>
<td>1</td>
<td>ENABLED UP</td>
<td>149*</td>
<td>*1/6 (22 dBm)</td>
</tr>
<tr>
<td>AP24e9.b34b.f1ed</td>
<td>1c:1d:86:31:e5:50</td>
<td>1</td>
<td>ENABLED UP</td>
<td>48*</td>
<td>*1/6 (22 dBm)</td>
</tr>
</tbody>
</table>
802.11a Airewave Director Configuration

RF Event and Performance Logging

Channel Update Logging......................... Off
Coverage Profile Logging......................... Off
Foreign Profile Logging........................ Off
Load Profile Logging............................ Off
Noise Profile Logging........................... Off
Performance Profile Logging..................... Off
TxPower Update Logging......................... Off

Default 802.11a AP performance profiles

802.11a Global Interference threshold........ 10 %
802.11a Global noise threshold.............. -70 dBm
802.11a Global RF utilization threshold..... 80 %
802.11a Global throughput threshold........ 1000000 bps
802.11a Global clients threshold.......... 12 clients

Default 802.11a AP monitoring

802.11a Monitor Mode............................. enable
802.11a Monitor Mode for Mesh AP Backhaul...... disable
802.11a Monitor Channels......................... Country channels
802.11a RRM Neighbor Discover Type.......... Transparent
802.11a RRM Neighbor RSSI Normalization..... Enabled
802.11a AP Coverage Interval.................. 90 seconds
802.11a AP Load Interval......................... 60 seconds
802.11a AP Monitor Measurement Interval........ 180 seconds
802.11a AP Neighbor Timeout Factor .......... 5
802.11a AP Report Measurement Interval......... 180 seconds

Leader Automatic Transmit Power Assignment

Transmit Power Assignment Mode............... AUTO
Transmit Power Update Interval............... 600 seconds
Transmit Power Threshold..................... -70 dBm
Transmit Power Neighbor Count.................. 3 APs
Min Transmit Power.............................. -10 dBm
Max Transmit Power.............................. 30 dBm

Update Contribution
Noise........................................ Enable
Interference.................................... Enable
Load.......................................... Disable
Device Aware................................. Disable

Transmit Power Assignment Leader............. wlc (192.168.250.2) (::)
Last Run....................................... 21 seconds ago
Last Run Time................................. 0 seconds

TPC Mode........................................ Version 1
TPCv2 Target RSSI............................... -67 dBm
TPCv2 VoWLAN Guide RSSI....................... -67.0 dBm
TPCv2 SOP...................................... -85.0 dBm
TPCv2 Default Client Ant Gain............... 0.0 dBi
TPCv2 Path Loss Decay Factor................. 3.6
TPCv2 Search Intensity......................... 10 Iterations

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Channel</th>
<th>TxPower</th>
<th>Allowed Power Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP78da.6ee0.08ec</td>
<td>149*</td>
<td>*1/6 (22 dBm) [22/19/16/13/10/7/7/7]</td>
<td></td>
</tr>
<tr>
<td>AP24e9.b34b.f1ed</td>
<td>48*</td>
<td>*1/6 (22 dBm) [22/19/16/13/10/7/7/7]</td>
<td></td>
</tr>
</tbody>
</table>

Coverage Hole Detection
802.11a Coverage Hole Detection Mode........ Enabled
802.11a Coverage Voice Packet Count.......... 100 packets
802.11a Coverage Voice Packet Percentage..... 50%
802.11a Coverage Voice RSSI Threshold........ -80 dBm
802.11a Coverage Data Packet Count............ 50 packets
802.11a Coverage Data Packet Percentage...... 50%
802.11a Coverage Data RSSI Threshold......... -80 dBm
802.11a Global coverage exception level........ 25 %
802.11a Global client minimum exception lev.... 3 clients

OptimizedRoaming

802.11a OptimizedRoaming Mode.................. Disabled
802.11a OptimizedRoaming Reporting Interval.... 90 seconds
802.11a OptimizedRoaming Rate Threshold....... disabled
802.11a OptimizedRoaming Hysteresis.......... 6 dB

OptimizedRoaming Stats

802.11a OptimizedRoaming Disassociations....... 0
802.11a OptimizedRoaming Rejections.......... 0

Leader Automatic Channel Assignment

Channel Assignment Mode......................... AUTO
Channel Update Interval......................... 600 seconds
Anchor time (Hour of the day)................... 0

Update Contribution

Noise........................................ Enable
Interference..................................... Enable
Load............................................ Disable
Device Aware.................................... Disable

CleanAir Event-driven RRM option.............. Disabled
Channel Assignment Leader...................... wlc (192.168.250.2) (::)
Last Run....................................... 21 seconds ago
Last Run Time.................................. 0 seconds

DCA Sensitivity Level.......................... MEDIUM (15 dB)
DCA 802.11n/ac Channel Width............... 20 MHz
DCA Minimum Energy Limit.................... -95 dBm

Channel Energy Levels
Minimum...................................... -127 dBm
Average...................................... -127 dBm
Maximum...................................... -127 dBm

Channel Dwell Times
Minimum...................................... 0 days, 00 h 00 m 19 s
Average...................................... 0 days, 00 h 00 m 19 s
Maximum...................................... 0 days, 00 h 00 m 19 s

802.11a 5 GHz Auto-RF Channel List
Allowed Channel List......................... 36,40,44,48,52,56,60,64,100,
104,108,112,116,120,124,128,
132,136,140,144,149,153,157,
161
Unused Channel List.......................... 165

802.11a 4.9 GHz Auto-RF Channel List
Allowed Channel List.........................
Unused Channel List......................... 1,2,3,4,5,6,7,8,9,10,11,12,
13,14,15,16,17,18,19,20,21,
22,23,24,25,26

DCA Outdoor AP option...................... Disabled

802.11a Radio RF Grouping
RF Group Name.............................. WLAN
RF Protocol Version(MIN).................... 101(30)
RF Packet Header Version.................... 2
Group Role(Mode)............................ LEADER(AUTO)
Group State.................................. Idle
Group Update Interval....................... 600 seconds
Group Leader................................ wlc (192.168.250.2) (:)
Group Member
......................................... wlc (192.168.250.2)
Maximum/Current number of Group Member........ 20/1
Maximum/Current number of AP................... 500/2
Last Run....................................... 21 seconds ago

802.11a CleanAir Configuration

Clean Air Solution............................ Disabled
Air Quality Settings:
   Air Quality Reporting....................... Enabled
   Air Quality Reporting Period (min)........ 15
   Air Quality Alarms.......................... Enabled
   Air Quality Alarm Threshold............... 35
   Unclassified Interference.................. Disabled
   Unclassified Severity Threshold.......... 20
Interference Device Settings:
   Interference Device Reporting............. Enabled
Interference Device Types:
   TDD Transmitter.......................... Enabled
   Jammer.................................... Enabled
   Continuous Transmitter................... Enabled
   DECT-like Phone.......................... Enabled
   Video Camera............................... Enabled
   WiFi Inverted............................ Enabled
   WiFi Invalid Channel..................... Enabled
   SuperAG.................................. Enabled
   Canopy................................... Enabled
   WiMax Mobile............................. Enabled
   WiMax Fixed.............................. Enabled
   Interference Device Alarms................. Enabled
   Interference Device Types Triggering Alarms:
      TDD Transmitter......................... Disabled
      Jammer.................................. Enabled
Continuous Transmitter................. Disabled
DECT-like Phone.......................... Disabled
Video Camera............................. Disabled
WiFi Inverted............................ Enabled
WiFi Invalid Channel..................... Enabled
SuperAG.................................. Disabled
Canopy................................... Disabled
WiMax Mobile............................. Disabled
WiMax Fixed.............................. Disabled

Additional Clean Air Settings:
CleanAir ED-RRM State..................... Disabled
CleanAir ED-RRM Sensitivity............... Medium
CleanAir ED-RRM Custom Threshold....... 50
CleanAir Rogue Contribution............... Disabled
CleanAir Rogue Duty-Cycle Threshold...... 80
CleanAir Persistent Devices state........ Disabled
CleanAir Persistent Device Propagation... Disabled

802.11a CleanAir AirQuality Summary
AQ = Air Quality
DFS = Dynamic Frequency Selection

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Channel Avg AQ Min AQ Interferers DFS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-------------------</td>
</tr>
</tbody>
</table>

802.11b Configuration
802.11b Network.......................... Enabled
11gSupport.................................. Enabled
11nSupport.................................. Enabled
802.11b/g Operational Rates
802.11b/g 1M Rate.......................... Mandatory
802.11b/g 2M Rate.......................... Mandatory
802.11b/g 5.5M Rate.......................... Mandatory
802.11b/g 11M Rate.......................... Mandatory
802.11g 6M Rate............................ Supported
802.11g 9M Rate............................ Supported
802.11g 12M Rate............................ Supported
802.11g 18M Rate............................ Supported
802.11g 24M Rate............................ Supported
802.11g 36M Rate............................ Supported
802.11g 48M Rate............................ Supported
802.11g 54M Rate............................ Supported

802.11n MCS Settings:
  MCS 0........................................ Supported
  MCS 1........................................ Supported
  MCS 2........................................ Supported
  MCS 3........................................ Supported
  MCS 4........................................ Supported
  MCS 5........................................ Supported
  MCS 6........................................ Supported
  MCS 7........................................ Supported
  MCS 8........................................ Supported
  MCS 9........................................ Supported
  MCS 10...................................... Supported
  MCS 11...................................... Supported
  MCS 12...................................... Supported
  MCS 13...................................... Supported
  MCS 14...................................... Supported
  MCS 15...................................... Supported
  MCS 16...................................... Supported
MCS 17................................. Supported
MCS 18................................. Supported
MCS 19................................. Supported
MCS 20................................. Supported
MCS 21................................. Supported
MCS 22................................. Supported
MCS 23................................. Supported
MCS 24................................. Supported
MCS 25................................. Supported
MCS 26................................. Supported
MCS 27................................. Supported
MCS 28................................. Supported
MCS 29................................. Supported
MCS 30................................. Supported
MCS 31................................. Supported

802.11n Status:
A-MPDU Tx:
  Priority 0......................... Enabled
  Priority 1......................... Enabled
  Priority 2......................... Enabled
  Priority 3......................... Enabled
  Priority 4......................... Enabled
  Priority 5......................... Enabled
  Priority 6......................... Disabled
  Priority 7......................... Disabled
Aggregation scheduler........... Enabled
  Realtime Timeout............... 10
  Non Realtime Timeout......... 200
A-MSDU Tx:
  Priority 0......................... Enabled
Priority 1............................... Enabled
Priority 2............................... Enabled
Priority 3............................... Enabled
Priority 4............................... Enabled
Priority 5............................... Enabled
Priority 6............................... Disabled
Priority 7............................... Disabled
A-MSDU Max Subframes ...................... 3
A-MSDU MAX Length ......................... 8k
Rifs Rx..................................... Enabled
Guard Interval ............................. Any
Beacon Interval............................. 100
CF Pollable mode............................. Disabled
CF Poll Request mandatory............... Disabled
CFP Period................................. 4
CFP Maximum Duration..................... 60
Default Channel............................ 1
Default Tx Power Level.................... 0
DTPC  Status................................ Enabled
RSSI Low Check............................ Disabled
RSSI Threshold........................... -80
Call Admission Limit ..................... 105
G711 CU Quantum ......................... 15
ED Threshold............................... -50
Fragmentation Threshold................... 2346
PBCC mandatory.......................... Disabled
RTS Threshold.................... 2347
Short Preamble mandatory.............. Enabled
Short Retry Limit......................... 7
Legacy Tx Beamforming setting......... Disabled
Traffic Stream Metrics Status.................... Disabled
Expedited BW Request Status....................... Disabled
World Mode........................................ Enabled
Faster Carrier Tracking Loop....................... Disabled
EDCA profile type................................. default-wmm
Voice MAC optimization status.................... Disabled

Call Admission Control (CAC) configuration
Voice AC - Admission control (ACM)............. Disabled
Voice Stream-Size............................... 84000
Voice Max-Streams............................... 2
Voice max RF bandwidth........................ 75
Voice reserved roaming bandwidth.............. 6
Voice CAC Method................................. Load-Based
Voice tspec inactivity timeout................. Disabled

CAC SIP-Voice configuration
SIP based CAC ..................................... Disabled
SIP Codec Type ................................. CODEC_TYPE_G711
SIP call bandwidth: .............................. 64
SIP call bandwidth sample-size ............... 20
Video AC - Admission control (ACM)............ Disabled
Video max RF bandwidth........................ Infinite
Video reserved roaming bandwidth............ 0
Video load-based CAC mode..................... Disabled
Video CAC Method ................................. Static

CAC SIP-Video configuration
SIP based CAC ..................................... Disabled
Best-effort AC - Admission control (ACM)...... Disabled
Background AC - Admission control (ACM)..... Disabled
Maximum Number of Clients per AP............. 200
802.11b Advanced Configuration

Member RRM Information

<table>
<thead>
<tr>
<th>AP Name</th>
<th>MAC Address</th>
<th>Admin</th>
<th>Oper</th>
<th>Channel</th>
<th>TxPower</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP78da.6ee0.08ec</td>
<td>5c:a4:8a:be:ca:90</td>
<td>ENABLED</td>
<td>UP</td>
<td>11*</td>
<td>*1/6 (22 dBm)</td>
</tr>
<tr>
<td>AP24e9.b34b.f1ed</td>
<td>1c:1d:86:31:e5:50</td>
<td>ENABLED</td>
<td>UP</td>
<td>11*</td>
<td>*1/6 (22 dBm)</td>
</tr>
</tbody>
</table>

802.11b Airewave Director Configuration

RF Event and Performance Logging

Channel Update Logging......................... Off
Coverage Profile Logging....................... Off
Foreign Profile Logging........................ Off
Load Profile Logging............................ Off
Noise Profile Logging........................... Off
Performance Profile Logging.................... Off
Transmit Power Update Logging............... Off

Default 802.11b AP performance profiles

802.11b Global Interference threshold........ 10 %
802.11b Global noise threshold............. -70 dBm
802.11b Global RF utilization threshold..... 80 %
802.11b Global throughput threshold........ 1000000 bps
802.11b Global clients threshold........... 12 clients

Default 802.11b AP monitoring

802.11b Monitor Mode.......................... enable
802.11b Monitor Channels..................... Country channels
802.11b RRM Neighbor Discovery Type......... Transparent
802.11b RRM Neighbor RSSI Normalization........ Enabled
802.11b AP Coverage Interval.................. 90 seconds
802.11b AP Load Interval.......................... 60 seconds
802.11b AP Monitor Measurement Interval....... 180 seconds
802.11b AP Neighbor Timeout Factor............. 5
802.11b AP Report Measurement Interval........ 180 seconds

Leader Automatic Transmit Power Assignment

Transmit Power Assignment Mode.................. AUTO
Transmit Power Update Interval.................. 600 seconds
Transmit Power Threshold........................ -70 dBm
Transmit Power Neighbor Count.................. 3 APs
Min Transmit Power.............................. -10 dBm
Max Transmit Power.............................. 30 dBm

Update Contribution

Noise............................................... Enable
Interference........................................ Enable
Load.................................................. Disable
Device Aware....................................... Disable

Transmit Power Assignment Leader................ wlc (192.168.250.2) (::)
Last Run........................................... 225 seconds ago
Last Run Time..................................... 0 seconds
TPC Mode......................................... Version 1
TPCv2 Target RSSI................................. -67 dBm
TPCv2 VoWLAN Guide RSSI........................ -67.0 dBm
TPCv2 SOP......................................... -85.0 dBm
TPCv2 Default Client Ant Gain................... 0.0 dBi
TPCv2 Path Loss Decay Factor.................... 3.6
TPCv2 Search Intensity........................... 10 Iterations
<table>
<thead>
<tr>
<th>AP Name</th>
<th>Channel</th>
<th>TxPower</th>
<th>Allowed Power Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP78da.6ee0.08ec</td>
<td>*11</td>
<td>*1/6 (22 dBm)</td>
<td>[22/19/16/13/10/7/7/7]</td>
</tr>
<tr>
<td>AP24e9.b34b.f1ed</td>
<td>*11</td>
<td>*1/6 (22 dBm)</td>
<td>[22/19/16/13/10/7/7/7]</td>
</tr>
</tbody>
</table>

Coverage Hole Detection

802.11b Coverage Hole Detection Mode........... Enabled
802.11b Coverage Voice Packet Count............ 100 packets
802.11b Coverage Voice Packet Percentage....... 50%
802.11b Coverage Voice RSSI Threshold......... -80 dBm
802.11b Coverage Data Packet Count............. 50 packets
802.11b Coverage Data Packet Percentage....... 50%
802.11b Coverage Data RSSI Threshold........... -80 dBm
802.11b Global coverage exception level........ 25 %
802.11b Global client minimum exception level... 3 clients

OptimizedRoaming

802.11b OptimizedRoaming Mode................... Disabled
802.11b OptimizedRoaming Reporting Interval..... 90 seconds
802.11b OptimizedRoaming Rate Threshold........... disabled
802.11b OptimizedRoaming Hysteresis............. 6 dB

OptimizedRoaming Stats

802.11b OptimizedRoaming Disassociations....... 0
802.11b OptimizedRoaming Rejections............. 0

Leader Automatic Channel Assignment

Channel Assignment Mode.......................... AUTO
Channel Update Interval......................... 600 seconds
Anchor time (Hour of the day).................... 0

Update Contribution

Noise........................................ Enable
Interference.................................... Enable
Load......................................... Disable
Device Aware.................................. Disable
CleanAir Event-driven RRM option.......... Disabled
Channel Assignment Leader............... wlc (192.168.250.2) (::)
Last Run....................................... 225 seconds ago
Last Run Time............................... 0 seconds

DCA Sensitivity Level: ...................... MEDIUM (10 dB)
DCA Minimum Energy Limit............... -95 dBm
Channel Energy Levels
Minimum...................................... -127 dBm
Average...................................... -127 dBm
Maximum...................................... -127 dBm
Channel Dwell Times
Minimum...................................... 0 days, 00 h 03 m 43 s
Average...................................... 0 days, 00 h 03 m 43 s
Maximum...................................... 0 days, 00 h 03 m 43 s

802.11b Auto-RF Allowed Channel List....... 1,6,11
802.11b Auto-RF Unused Channel List......... 2,3,4,5,7,8,9,10

802.11b Radio RF Grouping
RF Group Name.............................. WLAN
RF Protocol Version(MIN).................. 101(30)
RF Packet Header Version.................. 2
Group Role(Mode)............................ LEADER(AUTO)
Group State.................................. Idle
Group Update Interval....................... 600 seconds
Group Leader................................. wlc (192.168.250.2) (::)
Group Member
............................................. wlc (192.168.250.2)
Maximum/Current number of Group Member... 20/1
Maximum/Current number of AP .................. 500/2
Last Run ........................................ 225 seconds ago

802.11b CleanAir Configuration

Clean Air Solution ............................ Disabled

Air Quality Settings:

Air Quality Reporting ....................... Enabled
Air Quality Reporting Period (min) ....... 15
Air Quality Alarms ............................ Enabled
Air Quality Alarm Threshold ............... 35
Unclassified Interference .................... Disabled
Unclassified Severity Threshold ........... 20

Interference Device Settings:

Interference Device Reporting .............. Enabled

Interference Device Types:

Bluetooth Link ............................... Enabled
Microwave Oven ............................. Enabled
802.11 FH ...................................... Enabled
Bluetooth Discovery ....................... Enabled
TDD Transmitter ............................. Enabled
Jammer ......................................... Enabled
Continuous Transmitter .................... Enabled
DECT-like Phone ............................ Enabled
Video Camera ............................... Enabled
802.15.4 ....................................... Enabled
WiFi Inverted ................................. Enabled
WiFi Invalid Channel ....................... Enabled
SuperAG ...................................... Enabled
Canopy ...................................... Enabled
Microsoft Device ........................... Enabled
WiMax Mobile.......................... Enabled
WiMax Fixed............................ Enabled
BLE Beacon.............................. Enabled
Interference Device Alarms.............. Enabled

Interference Device Types Triggering Alarms:
  Bluetooth Link........................ Disabled
  Microwave Oven......................... Disabled
  802.11 FH................................ Disabled
  Bluetooth Discovery..................... Disabled
  TDD Transmitter........................ Disabled
  Jammer.................................. Enabled
  Continuous Transmitter................. Disabled
  DECT-like Phone......................... Disabled
  Video Camera............................ Disabled
  802.15.4................................ Disabled
  WiFi Inverted........................... Enabled
  WiFi Invalid Channel.................... Enabled
  SuperAG.................................. Disabled
  Canopy.................................. Disabled
  Microsoft Device......................... Disabled
  WiMax Mobile............................ Disabled
  WiMax Fixed.............................. Disabled
  BLE Beacon.............................. Disabled

Additional Clean Air Settings:
  CleanAir ED-RRM State.................. Disabled
  CleanAir ED-RRM Sensitivity............. Medium
  CleanAir ED-RRM Custom Threshold....... 50
  CleanAir Rogue Contribution............ Disabled
  CleanAir Rogue Duty-Cycle Threshold... 80
  CleanAir Persistent Devices state...... Disabled
CleanAir Persistent Device Propagation...... Disabled

802.11a CleanAir AirQuality Summary
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name            Channel Avg AQ Min AQ Interferers DFS
------------------ ------- ------ ------ ----------- ---

RF Density Optimization Configurations

FRA State......................... Disabled
FRA Sensitivity.................... low (100)
FAR Interval....................... 1 Hour(s)
Last Run.......................... 2703 seconds ago
Last Run Time..................... 0 seconds

AP Name                          MAC Address       Slot Current Band   COF %                Suggested Mode
-------------------------------- ----------------- ---- -------------- -------------------- -------------------------

COF : Coverage Overlap Factor

RF Client Steering Configurations
Client Steering Configuration Information
Macro to micro transition threshold............ -55 dBm
micro to Macro transition threshold............ -65 dBm
micro-Macro transition minimum client count.... 3
micro-Macro transition client balancing win.... 3
Probe suppression mode.......................... disabled
Probe suppression validity window.............. 100 s
Probe suppression aggregate window............ 200 ms
Probe suppression transition aggressiveness.... 3
Probe suppression hysteresis..................... -6 dBm

Mobility Configuration
Mobility Protocol Port........................... 16666
Default Mobility Domain.......................... WLAN
Multicast Mode ................................... Disabled
Mobility Domain ID for 802.11r.................... 0xf6a2
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count......................... 3
Mobility Group Members Configured............. 1
Mobility Control Message DSCP Value............ 0

Controllers configured in the Mobility Group

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Group Name</th>
<th>Multicast IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:50:56:ac:6d:08</td>
<td>192.168.250.2</td>
<td>WLAN</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Up</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mobility Hash Configuration

Default Mobility Domain......................... WLAN

IP Address      Hash Key
---------------------------------------------------------
192.168.250.2   7a9b864fa2922672949cf9a66fd012a0ce8cc7b0

Self Signed Certificate details

SSC Hash validation.............................. Enabled.

SSC Device Certificate details:

Subject Name :
C=US, ST=California, L=San Jose, O=Cisco Virtual Wireless LAN Controller,
CN=DEVICE-vWLC-AIR-CTVM-K9-005056AC6338, emailAddress=support@vwlc.com

Validity :
Start : Jul 26 20:52:54 2016 GMT
End   : Jun  4 20:52:54 2026 GMT

Hash key : 7a9b864fa2922672949cf9a66fd012a0ce8cc7b0
Mobility Foreign Map Configuration

<table>
<thead>
<tr>
<th>Wlan ID</th>
<th>Foreign Mac Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>

Advanced Configuration

Probe request filtering.......................... Enabled
Probes fwd to controller per client per radio.... 2
Probe request rate-limiting interval............. 500 msec
Aggregate Probe request interval................. 500 msec
Increased backoff parameters for probe respon.... Disabled

EAP-Identity-Request Timeout (seconds)........... 30
EAP-Identity-Request Max Retries............... 2
EAP Key-Index for Dynamic WEP.................... 0
EAP Max-Login Ignore Identity Response.......... enable
EAP-Request Timeout (seconds).................. 30
EAP-Request Max Retries......................... 2
EAPOL-Key Timeout (milliseconds).............. 1000
EAPOL-Key Max Retries......................... 2
EAP-Broadcast Key Interval..................... 3600

dot11-padding.................................... Disabled

padding-size..................................... 0
Advanced Hotspot Commands

ANQP 4-way state................................. Disabled
GARP Broadcast state: ......................... Enabled
GAS request rate limit ......................... Disabled
ANQP comeback delay in TUs(TU=1024usec)......... 1 TUs (=1mSec)

Location Configuration
RFID Tag data Collection......................... Enabled
RFID timeout.................................... 1200 seconds
RFID mobility....................................

Interface Configuration
Interface Name................................... ip_dev
MAC Address...................................... 00:50:56:ac:6d:08
IP Address....................................... 192.168.150.2
IP Netmask....................................... 255.255.255.0
IP Gateway....................................... 192.168.150.1
External NAT IP State......................... Disabled
External NAT IP Address....................... 0.0.0.0
VLAN............................................. 1500
Quarantine-vlan................................. 0
NAS-Identifier................................... none
Physical Port.................................... 1
DHCP Proxy Mode................................. Global
Primary DHCP Server.............................. Unconfigured
Secondary DHCP Server........................... Unconfigured
DHCP Option 82.................................... Disabled
DHCP Option 82 bridge mode insertion.......... Disabled
IPv4 ACL......................................... Unconfigured
mDNS Profile Name............................... Unconfigured
AP Manager....................................... No
Guest Interface................................. N/A
3G VLAN.......................................... Disabled
L2 Multicast....................................... Enabled

Interface Name................................. management
MAC Address..................................... 00:50:56:ac:6d:08
IP Address....................................... 192.168.250.2
IP Netmask....................................... 255.255.255.0
IP Gateway....................................... 192.168.250.1
External NAT IP State........................... Disabled
External NAT IP Address........................ 0.0.0.0
Link Local IPv6 Address......................... fe80::250:56ff:feac:6d08/64
STATE ........................................... REACHABLE
Primary IPv6 Address......................... ::/128
STATE ........................................... NONE
Primary IPv6 Gateway.......................... ::
Primary IPv6 Gateway Mac Address........... 00:00:00:00:00:00
STATE ........................................... INCOMPLETE
VLAN............................................. 1520
Quarantine-vlan................................. 0
Physical Port.................................... 1
DHCP Proxy Mode............................... Global
Primary DHCP Server......................... 192.168.250.1
Secondary DHCP Server............................ Unconfigured
DHCP Option 82................................. Disabled
DHCP Option 82 bridge mode insertion......... Disabled
IPv4 ACL........................................ Unconfigured
IPv6 ACL........................................ Unconfigured
mDNS Profile Name.............................. Unconfigured
AP Manager...................................... Yes
Guest Interface................................. N/A
L2 Multicast..................................... Enabled

Interface Name.................................... service-port
MAC Address..................................... 00:50:56:ac:63:38
IP Address....................................... 192.168.29.146
IP Netmask....................................... 255.255.255.0
Link Local IPv6 Address......................... fe80::250:56ff:feac:6338/64
STATE ........................................... NONE
IPv6 Address..................................... ::/128
STATE ........................................... NONE
SLAAC........................................... Disabled
DHCP Protocol................................... Disabled
AP Manager...................................... No
Guest Interface................................. N/A
Speed ........................................... 1Gbps
Duplex .......................................... Full
Auto Negotiation ............................... Enabled
Link Status...................................... Up

Port specific Information:
    inet addr:192.168.29.146  Bcast:192.168.29.255
    Mask:255.255.255.0
    inet6 addr: fe80::250:56ff:feac:6338/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1430  Metric:1
RX packets:258830 errors:0 dropped:298 overruns:0 frame:0
TX packets:95115 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:25069479 (23.9 MiB)  TX bytes:55852901 (53.2 MiB)

Interface Name................................... virtual
MAC Address...................................... 00:50:56:ac:6d:08
IP Address....................................... 1.1.1.1
Virtual DNS Host Name............................ Disabled
AP Manager....................................... No
Guest Interface.................................. N/A

Interface Group Configuration

WLAN Configuration

WLAN Identifier.................................. 1
Profile Name..................................... IP_Dev No Encryption
Network Name (SSID).............................. IP_Dev
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID.................................. Enabled
AAA Policy Override.............................. Disabled
Network Admission Control

Client Profiling Status

Radius Profiling ...................... Disabled
DHCP ................................. Disabled
HTTP ................................. Disabled
Local Profiling ....................... Disabled
DHCP ................................. Disabled
HTTP ................................. Disabled
Radius-NAC State ...................... Disabled
SNMP-NAC State ....................... Disabled
Quarantine VLAN .................. 0
Maximum number of Associated Clients .......... 0
Maximum number of Clients per AP Radio ........ 200
ATF Policy ............................. 0
Number of Active Clients ............ 0
Exclusion list Timeout ............... 60 seconds
Session Timeout ...................... 86400 seconds
User Idle Timeout .................... Disabled
Sleep Client ......................... disable
Sleep Client Timeout ................. 720 minutes
User Idle Threshold ................ 0 Bytes
NAS-identifier ....................... none
CHD per WLAN ....................... Enabled
Webauth DHCP exclusion ............ Disabled
Interface ......................... ip_dev
Multicast Interface ................ Not Configured
WLAN IPv4 ACL ....................... unconfigured
WLAN IPv6 ACL ....................... unconfigured
WLAN Layer2 ACL .................... unconfigured
mDNS Status ....................... Disabled
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mDNS Profile Name</td>
<td>unconfigured</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>Default</td>
</tr>
<tr>
<td>DHCP Address Assignment Required</td>
<td>Disabled</td>
</tr>
<tr>
<td>Static IP client tunneling</td>
<td>Disabled</td>
</tr>
<tr>
<td>Tunnel Profile</td>
<td>Unconfigured</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>Silver</td>
</tr>
<tr>
<td>Per-SSID Rate Limits</td>
<td></td>
</tr>
<tr>
<td>Average Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Average Realtime Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Burst Realtime Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Per-Client Rate Limits</td>
<td></td>
</tr>
<tr>
<td>Average Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Average Realtime Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Burst Realtime Data Rate</td>
<td>0</td>
</tr>
<tr>
<td>Scan Defer Priority</td>
<td>4,5,6</td>
</tr>
<tr>
<td>Scan Defer Time</td>
<td>100 milliseconds</td>
</tr>
<tr>
<td>WMM</td>
<td>Allowed</td>
</tr>
<tr>
<td>WMM UAPSD Compliant Client Support</td>
<td>Disabled</td>
</tr>
<tr>
<td>Media Stream Multicast-direct</td>
<td>Disabled</td>
</tr>
<tr>
<td>CCX - Aironet Support</td>
<td>Enabled</td>
</tr>
<tr>
<td>CCX - Gratuitous ProbeResponse (GPR)</td>
<td>Disabled</td>
</tr>
<tr>
<td>CCX - Diagnostics Channel Capability</td>
<td>Disabled</td>
</tr>
<tr>
<td>Dot11-Phone Mode (7920)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Wired Protocol</td>
<td>802.1P (Tag=0)</td>
</tr>
<tr>
<td>Passive Client Feature</td>
<td>Disabled</td>
</tr>
<tr>
<td>Peer-to-Peer Blocking Action</td>
<td>Disabled</td>
</tr>
<tr>
<td>Radio Policy</td>
<td>All</td>
</tr>
<tr>
<td>DTIM period for 802.11a radio</td>
<td>1</td>
</tr>
</tbody>
</table>
DTIM period for 802.11b radio................. 1

Radius Servers
  Authentication.......................... Global Servers
  Accounting............................. Global Servers
  Interim Update.......................... Enabled
  Interim Update Interval............... 0
  Framed IPv6 Acct AVP .................. Prefix
  Dynamic Interface..................... Disabled
  Dynamic Interface Priority............ wlan
  Local EAP Authentication.............. Disabled
  Radius NAI-Realm....................... Disabled
  Mu-Mimo.................................. Enabled

Security

  802.11 Authentication.................. Open System
  FT Support.............................. Disabled
  Static WEP Keys......................... Disabled
  802.1X.................................. Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Disabled
  Wi-Fi Direct policy configured........ Disabled
  EAP-Passthrough....................... Disabled
  CKIP .................................. Disabled
  Web Based Authentication............. Disabled
  Web Authentication Timeout........... 300
  Web-Passthrough....................... Disabled
  Mac-auth-server....................... 0.0.0.0
  Web-portal-server..................... 0.0.0.0
  Conditional Web Redirect............. Disabled
  Splash-Page Web Redirect............... Disabled
  Auto Anchor............................ Disabled
FlexConnect Local Switching.................... Enabled
FlexConnect Central Association............... Disabled
flexconnect Central Dhcp Flag.................... Disabled
flexconnect nat-pat Flag.......................... Disabled
flexconnect Dns Override Flag.................... Disabled
flexconnect PPPoE pass-through.................. Disabled
flexconnect local-switching IP-source-guar.... Disabled
FlexConnect Vlan based Central Switching ..... Disabled
FlexConnect Local Authentication............... Disabled
FlexConnect Learn IP Address.................... Enabled
Client MFP...................................... Optional but inactive (WPA2 not configured)
PMF............................................. Disabled
PMF Association Comeback Time.................. 1
PMF SA Query RetryTimeout....................... 200
Tkip MIC Countermeasure Hold-down Timer...... 60
Eap-params..................................... Not Applicable
Flex Avc Profile Name............................. None
Flow Monitor Name............................... None
Split Tunnel Configuration
  Split Tunnel................................... Disabled
Call Snooping.................................... Disabled
Roamed Call Re-Anchor Policy.................... Disabled
SIP CAC Fail Send-486-Busy Policy............... Enabled
SIP CAC Fail Send Dis-Association Policy....... Disabled
KTS based CAC Policy............................ Disabled
Assisted Roaming Prediction Optimization....... Disabled
802.11k Neighbor List............................ Disabled
802.11k Neighbor List Dual Band.................... Disabled
802.11v Directed Multicast Service............... Disabled
802.11v BSS Max Idle Service.................... Enabled
802.11v BSS Transition Service.................. Disabled
802.11v BSS Transition Disassoc Imminent........ Disabled
802.11v BSS Transition Disassoc Timer.......... 200
802.11v BSS Transition OpRoam Disassoc Timer... 40
DMS DB is empty
Band Select.................................... Disabled
Load Balancing.................................. Disabled
Multicast Buffer.............................. Disabled
Universal Ap Admin............................ Disabled

Mobility Anchor List

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>IP Address</th>
<th>Status</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------</td>
<td>------------</td>
<td>--------</td>
<td>----------</td>
</tr>
</tbody>
</table>

802.11u...................................... Disabled

MSAP Services.................................. Disabled

Local Policy

----------------
Priority Policy Name
-------- ---------------

WLAN Configuration

WLAN Identifier............................ 2
Profile Name.................................. IP_Dev All WPA/WPA2 PSK
Network Name (SSID)......................... IP_Dev
Status........................................ Enabled
MAC Filtering............................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override............................. Disabled

Network Admission Control

Client Profiling Status

Radius Profiling ................................ Disabled
DHCP ............................................. Disabled
HTTP ............................................. Disabled
Local Profiling .................................. Disabled
DHCP ............................................. Disabled
HTTP ............................................. Disabled
Radius-NAC State............................ Disabled
SNMP-NAC State............................... Disabled

Quarantine VLAN.............................. 0

Maximum number of Associated Clients......... 0
Maximum number of Clients per AP Radio........ 200

ATF Policy....................................... 0

Number of Active Clients...................... 2
Exclusionlist Timeout......................... 60 seconds
Session Timeout............................... 1800 seconds
User Idle Timeout............................ Disabled
Sleep Client................................. disable
Sleep Client Timeout.......................... 720 minutes
User Idle Threshold.......................... 0 Bytes
NAS-identifier............................... none

CHD per WLAN............................... Enabled
Webauth DHCP exclusion....................... Disabled

Interface................................. ip_dev
Multicast Interface.......................... Not Configured
WLAN IPv4 ACL.............................. unconfigured
WLAN IPv6 ACL.............................. unconfigured
WLAN Layer2 ACL................................. unconfigured
mDNS Status................................. Disabled
mDNS Profile Name......................... unconfigured
DHCP Server................................. Default
DHCP Address Assignment Required........ Disabled
Static IP client tunneling................. Disabled
Tunnel Profile............................... Unconfigured
Quality of Service......................... Silver
Per-SSID Rate Limits........................ Upstream Downstream
  Average Data Rate......................... 0  0
  Average Realtime Data Rate............... 0  0
  Burst Data Rate........................... 0  0
  Burst Realtime Data Rate.................. 0  0
Per-Client Rate Limits..................... Upstream Downstream
  Average Data Rate......................... 0  0
  Average Realtime Data Rate............... 0  0
  Burst Data Rate........................... 0  0
  Burst Realtime Data Rate.................. 0  0
Scan Defer Priority......................... 4,5,6
Scan Defer Time............................ 100 milliseconds
WMM............................................ Allowed
WMM UAPSD Compliant Client Support......... Disabled
Media Stream Multicast-direct............ Disabled
CCX - Aironetle Support..................... Enabled
CCX - Gratuitous ProbeResponse (GPR)......... Disabled
CCX - Diagnostics Channel Capability........ Disabled
Dot11-Phone Mode (7920).................... Disabled
Wired Protocol.................................. 802.1P (Tag=0)
Passive Client Feature..................... Disabled
Peer-to-Peer Blocking Action.............. Disabled
Radio Policy..................................... All
DTIM period for 802.11a radio.................... 1
DTIM period for 802.11b radio.................... 1

Radius Servers
  Authentication................................ Global Servers
  Accounting.................................. Global Servers
    Interim Update............................ Enabled
    Interim Update Interval................. 0
  Framed IPv6 Acct AVP ...................... Prefix
  Dynamic Interface.......................... Disabled
  Dynamic Interface Priority.............. wlan
  Local EAP Authentication................... Disabled
  Radius NAI-Realm.......................... Disabled
  Mu-Mimo.................................... Enabled

Security

  802.11 Authentication........................ Open System
  FT Support.................................. Disabled
  Static WEP Keys............................ Disabled
  802.1X..................................... Disabled
  Wi-Fi Protected Access (WPA/WPA2)......... Enabled
    WPA (SSN IE).............................. Enabled
      TKIP Cipher............................ Enabled
      AES Cipher............................. Enabled
    WPA2 (RSN IE)............................ Enabled
      TKIP Cipher............................ Disabled
      AES Cipher............................. Enabled
    OSEN IE.................................. Disabled
  Auth Key Management
    802.1x................................... Disabled
PSK.............................. Enabled
CCKM......................... Disabled
FT-1X(802.11r).................. Disabled
FT-PSK(802.11r)................. Disabled
PMF-1X(802.11w)............... Disabled
PMF-PSK(802.11w)............. Disabled
OSEN-1X........................ Disabled
FT Reassociation Timeout........ 20
FT Over-The-DS mode............. Disabled
GTK Randomization............... Disabled
SKC Cache Support............... Disabled
CCKM TSF Tolerance............. 1000
Wi-Fi Direct policy configured... Disabled
EAP-Passthrough................ Disabled
CKIP ............................ Disabled
Web Based Authentication........ Disabled
Web Authentication Timeout...... 300
Web-Passthrough................ Disabled
Mac-auth-server................ 0.0.0.0
Web-portal-server............... 0.0.0.0
Conditional Web Redirect......... Disabled
Splash-Page Web Redirect........ Disabled
Auto Anchor...................... Disabled
FlexConnect Local Switching..... Disabled
FlexConnect Central Association Disabled
flexconnect Central Dhcp Flag.... Disabled
delconnect nat-pat Flag.......... Disabled
delconnect Dns Override Flag.... Disabled
delconnect PPoE pass-through..... Disabled
delconnect local-switching IP-source-guar... Disabled
FlexConnect Vlan based Central Switching ..... Disabled
FlexConnect Local Authentication............. Disabled
FlexConnect Learn IP Address............... Enabled
Client MFP.................................. Optional
PMF......................................... Disabled
PMF Association Comeback Time.......... 1
PMF SA Query RetryTimeout................. 200
Tkip MIC Countermeasure Hold-down Timer.. 60
Eap-params................................. Disabled
Flex Avc Profile Name......................... None
Flow Monitor Name......................... None
Split Tunnel Configuration
    Split Tunnel........................... Disabled
Call Snooping.............................. Disabled
Roamed Call Re-Anchor Policy............... Disabled
SIP CAC Fail Send-486-Busy Policy......... Enabled
SIP CAC Fail Send Dis-Association Policy... Disabled
KTS based CAC Policy....................... Disabled
Assisted Roaming Prediction Optimization.. Disabled
802.11k Neighbor List....................... Disabled
802.11k Neighbor List Dual Band............. Disabled
802.11v Directed Multicast Service......... Disabled
802.11v BSS Max Idle Service............... Enabled
802.11v BSS Transition Service............. Disabled
802.11v BSS Transition Disassoc Imminent... Disabled
802.11v BSS Transition Disassoc Timer..... 200
802.11v BSS Transition OpRoam Disassoc Timer.. 40
DMS DB is empty
Band Select.................................. Disabled
Load Balancing............................. Disabled
Multicast Buffer................................. Disabled
Universal Ap Admin............................... Disabled

Mobility Anchor List

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>IP Address</th>
<th>Status</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------</td>
<td>------------</td>
<td>--------</td>
<td>---------</td>
</tr>
</tbody>
</table>

802.11u........................................ Disabled

MSAP Services.................................. Disabled

Local Policy

----------------

Priority Policy Name

--------  ---------------

Policy Configuration

L2ACL Configuration

ACL Configuration
CPU ACL Configuration

CPU Acl Name................................ NOT CONFIGURED
Wireless Traffic............................. Disabled
Wired Traffic................................. Disabled

RADIUS Configuration

Vendor Id Backward Compatibility.............. Disabled

Call Station Id Case.............................. lower

Accounting Call Station Id Type............... Mac Address
Auth Call Station Id Type..................... AP's Radio MAC Address:SSID
Extended Source Ports Support.................. Enabled
Aggressive Failover............................ Enabled
Keywrap.......................................... Disabled

Fallback Test:
  Test Mode.................................... Passive
  Probe User Name............................. cisco-probe
  Interval (in seconds)....................... 300

MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages......... hyphen
RADIUS Authentication Framed-MTU............. 1300 Bytes

Authentication Servers

Idx  Type  Server Address    Port    State     Tout  MgmtTout  RFC3576  IPSec -
AuthMode/Phase1/Group/Lifetime/Auth/Encr/Region
Accounting Servers

<table>
<thead>
<tr>
<th>Idx</th>
<th>Type</th>
<th>Server Address</th>
<th>Port</th>
<th>State</th>
<th>Tout</th>
<th>MgmtTout</th>
<th>RFC3576</th>
<th>IPSec - AuthMode/Phase1/Group/Lifetime/Auth/Encr/Region</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TACACS Configuration

Fallback Test:
Interval (in seconds)...................... 0

Authentication Servers

<table>
<thead>
<tr>
<th>Idx</th>
<th>Server Address</th>
<th>Port</th>
<th>State</th>
<th>Tout</th>
<th>MgmtTout</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Authorization Servers

<table>
<thead>
<tr>
<th>Idx</th>
<th>Server Address</th>
<th>Port</th>
<th>State</th>
<th>Tout</th>
<th>MgmtTout</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Accounting Servers

<table>
<thead>
<tr>
<th>Idx</th>
<th>Server Address</th>
<th>Port</th>
<th>State</th>
<th>Tout</th>
<th>MgmtTout</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
LDAP Configuration

Local EAP Configuration

User credentials database search order:

Primary ..................................... Local DB

Timer:

Active timeout ......................... 300

Configured EAP profiles:

EAP Method configuration:

EAP-FAST:

Server key ............................... <hidden>
TTL for the PAC ....................... 10
Anonymous provision allowed ........ Yes
Authority ID ............................ 436973636f000000000000000000000000000000
Authority Information ............... Cisco A-ID

Dns Configuration

Radius port............................... 
Radius secret............................. 
Dns url ................................. 
Dns timeout............................
Dns Serverip...........................
Dns state............................... Disable
Dns Auth Retransmit Timeout................. 2
Dns Acct Retransmit Timeout.................. 2
Dns Auth Mgmt-Retransmit Timeout.......... 2
Dns Network Auth.......................... Enable
Dns Mgmt Auth............................. Enable
Dns Network Acct......................... Enable
Dns RFC 3576 Auth......................... Disable

Tacacs port.................................
Tacacs secret.............................. 2
Dns url....................................
Dns timeout..............................
Dns Serverip..............................
Dns state................................. Disable

Fallback Radio Shut configuration:
Fallback Radio Shut: Disabled
Arp-caching: Disabled
Subnet Broadcast Drop: Disabled

FlexConnect Group Summary

FlexConnect Group Summary: Count: 0
## FlexConnect Group Detail

### FlexConnect Vlan name Summary

<table>
<thead>
<tr>
<th>Vlan-Name Id</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>------</td>
</tr>
</tbody>
</table>

### FlexConnect Vlan Name Detail

## Route Info

Number of Routes: 0
## Destination Network

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Netmask</th>
<th>Gateway</th>
</tr>
</thead>
</table>

### Peer Route Info

Number of Routes: 32555

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Netmask</th>
<th>Gateway</th>
</tr>
</thead>
</table>

### QoS Queue Length Info

- Platinum queue length: 100
- Gold queue length: 75
- Silver queue length: 50
- Bronze queue length: 25

### QoS Profile Info

- Description: For Voice Applications
- Maximum Priority: voice
- Unicast Default Priority: voice
- Multicast Default Priority: voice

<table>
<thead>
<tr>
<th>Per-SSID Rate Limits</th>
<th>Upstream</th>
<th>Downstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Average Realtime Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Burst Data Rate</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Burst Realtime Data Rate.......................... 0  0
Per-Client Rate Limits.......................... Upstream  Downstream
Average Data Rate............................... 0  0
Average Realtime Data Rate..................... 0  0
Burst Data Rate................................. 0  0
Burst Realtime Data Rate......................... 0  0
protocol.......................................... dot1p
dot1p............................................. 5
Description....................................... For Video Applications
Maximum Priority............................... video
Unicast Default Priority......................... video
Multicast Default Priority....................... video
Per-SSID Rate Limits............................ Upstream  Downstream
Average Data Rate............................... 0  0
Average Realtime Data Rate..................... 0  0
Burst Data Rate................................. 0  0
Burst Realtime Data Rate......................... 0  0
Per-Client Rate Limits.......................... Upstream  Downstream
Average Data Rate............................... 0  0
Average Realtime Data Rate..................... 0  0
Burst Data Rate................................. 0  0
Burst Realtime Data Rate......................... 0  0
protocol.......................................... dot1p
dot1p............................................. 4
Description....................................... For Best Effort
Maximum Priority............................... besteffort
Unicast Default Priority......................... besteffort
Multicast Default Priority....................... besteffort
Per-SSID Rate Limits............................ Upstream  Downstream
Average Data Rate............................... 0  0
Average Realtime Data Rate....................... 0 0
Burst Data Rate..................................... 0 0
Burst Realtime Data Rate.................................. 0 0
Per-Client Rate Limits............................... Upstream  Downstream
Average Data Rate................................. 0 0
Average Realtime Data Rate....................... 0 0
Burst Data Rate..................................... 0 0
Burst Realtime Data Rate.................................. 0 0
protocol............................................... dot1p
dot1p.................................................. 0
Description........................................ For Background
Maximum Priority................................. background
Unicast Default Priority......................... background
Multicast Default Priority....................... background
Per-SSID Rate Limits............................... Upstream  Downstream
Average Data Rate................................. 0 0
Average Realtime Data Rate....................... 0 0
Burst Data Rate..................................... 0 0
Burst Realtime Data Rate.................................. 0 0
Per-Client Rate Limits............................... Upstream  Downstream
Average Data Rate................................. 0 0
Average Realtime Data Rate....................... 0 0
Burst Data Rate..................................... 0 0
Burst Realtime Data Rate.................................. 0 0
protocol............................................... dot1p
dot1p.................................................. 1

Mac Filter Info
Authorization List

Authorize MIC APs against Auth-list or AAA ...... disabled
Authorize LSC APs against Auth-List ............. disabled
APs Allowed to Join
  AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate................ no
  AP with Locally Significant Certificate....... no

Load Balancing Info

Aggressive Load Balancing...................... per WLAN enabling
Aggressive Load Balancing Window............... 5 clients
Aggressive Load Balancing Denial Count........ 3
Aggressive Load Balancing Uplink Threshold..... 50

Statistics (client-count based)

Total Denied Count.............................. 0 clients
Total Denial Sent................................ 0 messages
Exceeded Denial Max Limit Count................ 0 times
None 5G Candidate Count....................... 0 times
None 2.4G Candidate Count..................... 0 times

Statistics (uplink-usage based)
Total Denied Count............................... 0 clients
Total Denial Sent................................. 0 messages
Exceeded Denial Max Limit Count............... 0 times
None 5G Candidate Count......................... 0 times
None 2.4G Candidate Count....................... 0 times

DHCP Info

DHCP Opt-82 RID Format: <AP radio MAC address>
DHCP Opt-82 Format: binary

DHCP Proxy Behaviour: disabled

Exclusion List Configuration Unable to retrieve exclusion-list entry

CDP Configuration

cdp version v2
Country Channels Configuration

Configured Country............................. US - United States

KEY: * = Channel is legal in this country and may be configured manually.
     A = Channel is the Auto-RF default in this country.
     . = Channel is not legal in this country.
     C = Channel has been configured for use by Auto-RF.
     x = Channel is available to be configured for use by Auto-RF.
     (-,-) = (indoor, outdoor) regulatory domain allowed by this country.

-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
802.11bg     :
Channels : 11111
     : 12345678901234
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
US (-A   ,-AB  ): A * * * * A * * * * A . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
802.11a      :
Channels : 333444445566001122233444556667
     : 46802468260482604826049371593
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
4.9GHz 802.11a :
Channels : 1111111111122222222
     : 12345678901234567890123456
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
US (-AB  ,-AB  ): * * * * * * * * * * * * * * A * * * * A
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
WPS Configuration Summary

Auto-Immune

Auto-Immune........................................ Disabled
Auto-Immune by aWIPS Prevention................ Disabled

Client Exclusion Policy

Excessive 802.11-association failures........ Enabled
Excessive 802.11-authentication failures....... Enabled
Excessive 802.1x-authentication................ Enabled
IP-theft........................................... Enabled
Excessive Web authentication failure.......... Enabled
Maximum 802.1x-AAA failure attempts.......... 3

Signature Policy

Signature Processing............................ Enabled

Management Frame Protection

Global Infrastructure MFP state.............. DISABLED (*all infrastructure settings are overridden)
AP Impersonation detection.................... Disabled
Controller Time Source Valid............... False

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>WLAN Name</th>
<th>Status</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IP_Dev No Encryption</td>
<td>Disabled</td>
<td>Optional but inactive (WPA2 not configured)</td>
</tr>
</tbody>
</table>
2   IP_Dev All WPA/WPA2 PSK  Enabled  Optional

Custom Web Configuration

Radius Authentication Method.................. PAP
Cisco Logo........................................ Enabled
CustomLogo....................................... None
Custom Title................................. None
Custom Message............................. None
Custom Redirect URL......................... None
Web Authentication Type....................... Internal Default
Logout-popup................................. Enabled
External Web Authentication URL.............. None

Configuration Per Profile:

Core dump Configuration

Core Dump upload is disabled
Rogue AP Configuration

Rogue Detection Security Level.................. custom
Rogue Pending Time............................ 180 secs
Rogue on wire Auto-Contain.................. Disabled
Rogue using our SSID Auto-Contain........... Disabled
Valid client on rogue AP Auto-Contain........ Disabled
Rogue AP timeout............................. 1200
Rogue Detection Report Interval.............. 10
Rogue Detection Min Rssi...................... -90
Rogue Detection Transient Interval......... 0
Rogue Detection Client Num Thershold........ 0
Validate rogue AP against AAA............... Disabled
Rogue AP AAA validation interval........... 0 secs
Total Rogues(AP+Ad-hoc) supported........... 800
Total Rogues classified..................... 41

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Classification</th>
<th># APs</th>
<th># Clients</th>
<th>Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td>04:bd:88:b5:2f:50</td>
<td>Friendly</td>
<td>0</td>
<td>0</td>
<td>Not Heard</td>
</tr>
<tr>
<td>04:bd:88:b5:2f:55</td>
<td>Friendly</td>
<td>0</td>
<td>0</td>
<td>Not Heard</td>
</tr>
<tr>
<td>04:bd:88:b5:4e:e0</td>
<td>Friendly</td>
<td>0</td>
<td>0</td>
<td>Not Heard</td>
</tr>
<tr>
<td>04:bd:88:b5:4e:f0</td>
<td>Friendly</td>
<td>0</td>
<td>0</td>
<td>Not Heard</td>
</tr>
<tr>
<td>04:bd:88:b6:0d:60</td>
<td>Friendly</td>
<td>0</td>
<td>0</td>
<td>Not Heard</td>
</tr>
<tr>
<td>04:bd:88:b6:0d:70</td>
<td>Friendly</td>
<td>0</td>
<td>0</td>
<td>Not Heard</td>
</tr>
<tr>
<td>04:bd:88:b6:0d:75</td>
<td>Friendly</td>
<td>0</td>
<td>0</td>
<td>Not Heard</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Type</td>
<td>Count</td>
<td>Time</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>-------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:0e:e0</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:0e:f0</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:0e:f5</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:10:00</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:10:10</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:10:15</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:10:70</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:10:75</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>04:bd:88:b6:10:b5</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>6c:72:20:3e:af:26</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>6c:72:20:3e:af:28</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>6c:72:20:3e:af:2a</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>88:dc:96:30:d9:1b</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>8a:dc:96:30:d9:1b</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>9a:dc:96:30:d9:1b</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:b7:ab</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:b7:af</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:bc:2b</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:bc:2f</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:f6:6b</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:f6:6f</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:f9:4b</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:f9:4f</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:fa:4b</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:fa:4f</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:ff:1b</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
<tr>
<td>e0:d1:73:02:ff:1f</td>
<td>Friendly</td>
<td>0</td>
<td>Not Heard</td>
<td></td>
</tr>
</tbody>
</table>
Rogue AP RLDP Configuration

Rogue Location Discovery Protocol................. Disabled
RLDP Schedule Config............................. Disabled
RLDP Scheduling Operation......................... Disabled
RLDP Retry....................................... 1

RLDP Start Time       RLDP End Time       Day
---------------       -------------       ---

Rogue Auto Contain Configuration

Containment Level................................. 1
monitor_ap_only.................................. false

Adhoc Rogue Configuration

Detect and report Ad-Hoc Networks............... Enabled
Auto-Contain Ad-Hoc Networks..................... Disabled
Total Rogues(Ad-Hoc+AP) supported .............. 800
Total Ad-Hoc entries............................. 0

Client MAC Address  Adhoc BSSID     State   # APs Last Heard
------------------  ------------------  ------  ------  ---------------

Rogue Client Configuration

Validate rogue clients against AAA............... Disabled
Validate rogue clients against MSE.............. Disabled
Total Rogue Clients supported.................... 3000
Total Rogue Clients present....................... 0

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>State</th>
<th># APs Last Heard</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ignore List Configuration

MAC Address

--------------

Rogue Rule Configuration

<table>
<thead>
<tr>
<th>Priority</th>
<th>Rule Name</th>
<th>Rule state Class Type</th>
<th>Notify</th>
<th>State</th>
<th>Match Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Media-Stream Configuration

Multicast-direct State......................... disable
Allowed WLANs..................................

<table>
<thead>
<tr>
<th>Stream Name</th>
<th>Start IP</th>
<th>End IP</th>
<th>Operation Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NIST SP 1800-8C: Securing Wireless Infusion Pumps
DRAFT

URL..............................................
E-mail...........................................
Phone.......................................... 
Note............................................
State............................................ disable

2.4G Band Media-Stream Configuration

Multicast-direct................................. Enabled
Best Effort........................................ Disabled
Video Re-Direct.................................... Enabled
Max Allowed Streams Per Radio................. Auto
Max Allowed Streams Per Client................... Auto
Max Video Bandwidth.............................. 0
Max Media Bandwidth.............................. 85
Min PHY Rate..................................... 6000
Max Retry Percentage............................ 80

5G Band Media-Stream Configuration

Multicast-direct..................................... Enabled
Best Effort......................................... Disabled
Video Re-Direct...................................... Enabled
Max Allowed Streams Per Radio............... Auto
Max Allowed Streams Per Client............... Auto
Max Video Bandwidth.............................. 0
Max Voice Bandwidth.............................. 75
Max Media Bandwidth.............................. 85
Min PHY Rate..................................... 6000
Max Retry Percentage............................. 80

Number of Clients.................................. 0

Client Mac   Stream Name  Stream Type  Radio WLAN  QoS  Status
------------- ----------- ----------- ---- ---- -------

WLC Voice Call Statistics
WLC Voice Call Statistics for 802.11b Radio

WMM TSPEC CAC Call Stats
Total num of Calls in progress................. 0
Num of Roam Calls in progress............... 0
Total Num of Calls Admitted.................... 0
Total Num of Roam Calls Admitted.......... 0
Total Num of exp bw requests received........ 0
Total Num of exp bw requests Admitted....... 0
Total Num of Calls Rejected.................... 0
Total Num of Roam Calls Rejected............. 0
Num of Calls Rejected due to insufficient bw.. 0
Num of Calls Rejected due to invalid params.. 0
Num of Calls Rejected due to PHY rate........ 0
Num of Calls Rejected due to QoS policy..... 0

SIP CAC Call Stats
Total Num of Calls in progress................. 0
Num of Roam Calls in progress................. 0
Total Num of Calls Admitted.................... 0
Total Num of Roam Calls Admitted............... 0
Total Num of Preferred Calls Received........ 0
Total Num of Preferred Calls Admitted......... 0
Total Num of Ongoing Preferred Calls......... 0
Total Num of Calls Rejected(Insuff BW)....... 0
Total Num of Roam Calls Rejected(Insuff BW).... 0

KTS based CAC Call Stats
Total Num of Calls in progress................. 0
Num of Roam Calls in progress................. 0
Total Num of Calls Admitted.................... 0
Total Num of Roam Calls Admitted............... 0
Total Num of Calls Rejected.................... 0
Total Num of Roam Calls Rejected............... 0

WLC Voice Call Statistics for 802.11a Radio

WMM TSPEC CAC Call Stats
Total num of Calls in progress................. 0
Num of Roam Calls in progress................. 0
Total Num of Calls Admitted.................... 0
Total Num of Roam Calls Admitted............... 0
Total Num of Calls Rejected.................... 0
Total Num of Roam Calls Rejected............... 0
Num of Calls Rejected due to insufficient bw.... 0
Num of Calls Rejected due to invalid params.... 0
Num of Calls Rejected due to PHY rate........ 0
Num of Calls Rejected due to QoS policy........ 0

SIP CAC Call Stats
Total Num of Calls in progress............... 0
Num of Roam Calls in progress............... 0
Total Num of Calls Admitted............... 0
Total Num of Roam Calls Admitted............... 0
Total Num of Preferred Calls Received........ 0
Total Num of Preferred Calls Admitted........ 0
Total Num of Ongoing Preferred Calls........ 0
Total Num of Calls Rejected(Insuff BW)........ 0
Total Num of Roam Calls Rejected(Insuff BW)... 0

KTS based CAC Call Stats
Total Num of Calls in progress............... 0
Num of Roam Calls in progress............... 0
Total Num of Calls Admitted............... 0
Total Num of Roam Calls Admitted............... 0
Total Num of Calls Rejected(Insuff BW)........ 0
Total Num of Roam Calls Rejected(Insuff BW)... 0

WLC IPv6 Summary

Global Config.......................... Enabled
Reachable-lifetime value.................. 300
Stale-lifetime value.................. 86400
Down-lifetime value.................. 30
RA Throttling.......................... Disabled
RA Throttling allow at-least.............. 1
RA Throttling allow at-most............... 1
RA Throttling max-through............... 10
RA Throttling throttle-period........... 600
RA Throttling interval-option............ passsthrough
NS Mulitcast CacheMiss Forwarding...... Disabled
NA Mulitcast Forwarding.................. Enabled
IPv6 Capwap UDP Lite..................... Enabled
Operating System IPv6 state............. Enabled

mDNS Service Summary

Number of Services..................... 10
Mobility learning status................. Enabled

<table>
<thead>
<tr>
<th>Service-Name</th>
<th>LSS</th>
<th>Origin</th>
<th>No SP</th>
<th>Service-string</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirTunes</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_raop._tcp.local.</td>
</tr>
<tr>
<td>Airplay</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_airplay._tcp.local.</td>
</tr>
<tr>
<td>Googlecast</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_googlecast._tcp.local.</td>
</tr>
<tr>
<td>HP_Photosmart_Printer_1</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_universal._sub._ipp._tcp.local.</td>
</tr>
<tr>
<td>HP_Photosmart_Printer_2</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_cups._sub._ipp._tcp.local.</td>
</tr>
<tr>
<td>HomeSharing</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_home-sharing._tcp.local.</td>
</tr>
<tr>
<td>Printer-IPP</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_ipp._tcp.local.</td>
</tr>
<tr>
<td>Printer-IPPS</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_ipps._tcp.local.</td>
</tr>
<tr>
<td>Printer-LPD</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_printer._tcp.local.</td>
</tr>
<tr>
<td>Printer-socket</td>
<td>No</td>
<td>All</td>
<td>0</td>
<td>_pdl-datastream._tcp.local.</td>
</tr>
</tbody>
</table>

* -> If access policy is enabled LSS will be ignored.
mDNS service-group Summary

Access Policy Status............................ Disabled
Total number of mDNS Policies.................... 1

Number of Admin configured Policies.......... 1

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Service Group Name</th>
<th>Description</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default-mdns-policy</td>
<td>Default Access Policy created by WLC</td>
<td>WLC</td>
</tr>
</tbody>
</table>

mDNS profile detailed

Profile Name................................. default-mdns-profile
Profile Id.................................... 1
No of Services.............................. 10
Services...................................... AirTunes
                                           Airplay
                                           Googlecast
                                           HP_Photosmart_Printer_1
                                           HP_Photosmart_Printer_2
                                           HomeSharing
                                           Printer-IPP
                                           Printer-IPPS
Printer-LPD

Printer-SOCKET

No. Interfaces Attached......................... 0
No. Interface Groups Attached.................... 0
No. Wlans........................................ 0
No. Local Policies Attached....................... 0

mDNS AP Summary

Number of mDNS APs.............................. 0

PMIPv6 Global Configuration

PMIPv6 Profile Summary

No Profile Created.

PMIPv6 MAG Statistics

PMIPv6 domain has to be configured first
EoGRE Global Configuration

Heartbeat Interval..............60
Max Heartbeat Skip Count......3
Interface.......................management

EoGRE Gateway Configuration

EoGRE Domain Configuration

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Gateways</th>
<th>Active Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EoGRE Profile Configuration

WLAN Express Setup Information.

WLAN Express Setup - ......................... False

Flex Avc Profile summary.
<table>
<thead>
<tr>
<th>Profile-Name</th>
<th>Number of Rules</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flex Avc Profile Detailed Config.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Certificate Summary.**

- Web Administration Certificate................ 3rd Party
- Web Authentication Certificate................ Locally Generated
- Certificate compatibility mode:............... off
- Lifetime Check Ignore for MIC ............... Disable
- Lifetime Check Ignore for SSC ............... Disable

**Smart-licensing status Summary.**

**Call-home Summary.**
Hotspot Icon Summary.

Unable to find Icon directory in flash.

Coredump Summary

Core Dump upload is disabled

Memory Summary

-------------------- System Memory Summary --------------------

System Name:wlc Primary SW Ver:8.2.111.0
Current Time:Thu Aug 18 20:06:33 2016 System UP Time:6 days 3 hrs 49 mins 39 secs
NAME: "Chassis" , DESCR: "Cisco Wireless Controller"
PID: AIR-CTVM-K9, VID: V01, SN: 96NTPERK0A6
Total System Memory............................... (2057560 KB) 2009 MB
Total System Free Memory............................ (909360 KB) 888 MB (44 %)
Total Memory in Buffers............................. (1104 KB)
Total Memory in Cache............................... (266564 KB) 260 MB
Total Active Memory............................... (511540 KB) 499 MB
Total InActive Memory............................. (238112 KB) 232 MB
Total Memory in Anon Pages......................... (481984 KB) 470 MB
Total Memory in Slab............................... (11004 KB) 10 MB
Total Memory in Page Tables...................... (2748 KB) 2 MB
WLC Peak Memory.................................. (1402280 KB) 1369 MB
WLC Virtual Memory Size......................... (1383912 KB) 1351 MB
WLC Resident Memory.............................. (506340 KB) 494 MB
WLC Data Segment Memory......................... (1318240 KB) 1287 MB
Total Heap Including Mapped Pages.............. (399115 KB) 389 MB
Total Memory in Pmalloc Pools.................... (350174 KB) 341 MB
Total Used Memory in Pmalloc Pools............... (324913 KB) 317 MB
Total Free Memory in Pmalloc Pools............... (16706 KB) 16 MB

------------------------- Pmalloc Pools Information --------------------
Index Pool-Size Chunks-In-Pool Chunks-In-Use Memory(Size/Used/Free)KB

<table>
<thead>
<tr>
<th>Pool-Size</th>
<th>Chunks-In-Pool</th>
<th>Chunks-In-Use</th>
<th>Memory(Size/Used/Free)KB</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16</td>
<td>50000</td>
<td>5351 5468 /4771 /697</td>
</tr>
<tr>
<td>1</td>
<td>64</td>
<td>40000</td>
<td>16626 6250 /4789 /1460</td>
</tr>
<tr>
<td>2</td>
<td>128</td>
<td>52800</td>
<td>52677 11550 /11534 /15</td>
</tr>
<tr>
<td>3</td>
<td>256</td>
<td>9400</td>
<td>9377 3231 /3225 /5</td>
</tr>
<tr>
<td>4</td>
<td>384</td>
<td>6000</td>
<td>287 2812 /670 /2142</td>
</tr>
<tr>
<td>5</td>
<td>512</td>
<td>16000</td>
<td>15 9500 /1507 /7992</td>
</tr>
<tr>
<td>6</td>
<td>1024</td>
<td>13100</td>
<td>12985 14328 /14213 /115</td>
</tr>
<tr>
<td>7</td>
<td>2048</td>
<td>1000</td>
<td>712 2093 /1517 /576</td>
</tr>
<tr>
<td>8</td>
<td>4096</td>
<td>1000</td>
<td>74 4093 /389 /3704</td>
</tr>
<tr>
<td>9</td>
<td>Raw-Pool</td>
<td>0</td>
<td>524 290800 /290800 /0</td>
</tr>
</tbody>
</table>

------------------------- MBUF Information ----------------------------
Maximum number of Mbufs......................... 24576
Number of Mbufs Free............................ 24560
Number of Mbufs In Use.......................... 16

Mesh Configuration
Mesh Range....................................... 12000
Mesh Statistics update period.................... 3 minutes
Backhaul with client access status.............. disabled
Backhaul with extended client access status...... disabled
Background Scanning State....................... disabled
Subset Channel Sync State........................ disabled
Backhaul Amsdu State............................. enabled
Backhaul RRM..................................... disabled
Mesh Auto RF..................................... disabled

Mesh Security

Security Mode................................... EAP
External-Auth..................................... disabled
Use MAC Filter in External AAA server........ disabled
Force External Authentication................... disabled
LSC Only MAP Authentication.................... disabled

Mesh Alarm Criteria

Max Hop Count.................................... 4
Recommended Max Children for MAP.......... 10
Recommended Max Children for RAP.......... 20
Low Link SNR.................................... 12
High Link SNR................................... 60
Max Association Number......................... 10
Association Interval............................ 60 minutes
Parent Change Numbers......................... 3
Parent Change Interval......................... 60 minutes
Mesh Multicast Mode.......................... In-Out
Mesh CAC Mode............................... enabled
Mesh Full Sector DFS......................... enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... enabled

Mesh DCA channels for serial backhaul APs.......... disabled

Outdoor Ext. UNII B Domain channels(for BH)....... disabled
Mesh Advanced LSC............................. disabled
Advanced LSC AP Provisioning......................... disabled
  Open Window.................................. disabled
  Provision Controller.......................... disabled

Mesh Slot Bias.................................. enabled
Mesh Convergence Method.......................... standard
Mesh Channel Change Notification..................... disabled
Mesh Ethernet Bridging STP BPDU Allowed............ disabled
Mesh RAP downlink backhaul.......................... 802.11Radio-A (Slot 1)
Appendix B  Sample Pump Configuration Parameters

B.1  Example of Pump Configuration File

SN=2011304

# Pump serial number - must match SN of receiving pump

# SIGMA Spectrum Settings

[NETWORK CONFIGURATION]

# DHCP=0 DHCP disabled - IP, GATEWAY, NETMASK, and DNS must be valid
# DHCP=1 DHCP enabled - IP, GATEWAY, NETMASK, and DNS must be blank

DHCP=1

IP=

GATEWAY=

NETMASK=

DNS=  

# Leave either SIGMAGW or MULTICAST blank

# SIGMAGW set to DNS name or IP address of SIGMA gateway server

SIGMAGW=192.168.140.165

# MULTICAST group default is 239.237.12.87

MULTICAST=

# DEVICEID set to device alias

# Limited to 20 alpha-numeric characters (0-1,A-Z,a-z), blank is acceptable

DEVICEID=000345

[WIFI CONFIGURATION]

# BSS=0 Infrastructure mode (Access point)

# BSS=1 Join or Create Ad-Hoc (peer-to-peer)

# BSS=2 Join only Ad-Hoc (peer-to-peer)

# BSS=3 Join any

BSS=0

# SSID= set to wireless network name

SSID=IP_Dev_Cert

# 802.11 Mode - ‘b’, ‘g’, and/or ‘a’
802.11b=1
802.11g=1
802.11a=1
# CHANNEL=0 search channels
CHANNEL=0
# SECURITY=0 Any available security method
# SECURITY=1 Open system (no-encryption)
# SECURITY=2 WEP shared key
# SECURITY=3 WPA pre-shared key
# SECURITY=4 WPA with 802.1x authentication
# SECURITY=5 WEP with 802.1x authentication
# SECURITY=6 LEAP
# SECURITY=7 EAP-FAST
SECURITY=4
# WEPKEYINDEX=0-3
WEPKEYINDEX=0
# WEPKEY may be blank or 10 (64-bit) or 26 (128-bit) hex (0-1 and a-f) characters long
WEPKEY=
# WPAENCRYPTION=0 Any
# WPAENCRYPTION=1 WEP
# WPAENCRYPTION=2 TKIP
# WPAENCRYPTION=3 CCMP (AES)
# WPAENCRYPTION=4 Open (no encryption)
WPAENCRYPTION=3
# WPAPSK must be blank if WPA PSK is not used
# WPAPSK may 64 hex (0-1 and a-f) characters long to specify a PSK
# WPAPSK may be 8-63 ascii characters long to specify a passphrase
WPAPSK=
# 802.1X/EAP Authentication method
# Set one, or more, authentication methods to 1 to enable them, all others should be 0
LEAP=0
PEAP/MSCHAPv2=0
EAP-TLS=1
EAP-FAST=0

# IDENTITY= 802.1X Identity (username)
IDENTITY=BaxterCert

# PASSWORD= 802.1X Password
PASSWORD=

# Certificate information follows, required for authentication modes that use a certificate.

# All certificates and private keys must be PEM format (base64 encoded).
# Client certificate, both cert and private key are required.
# Certificate and key information is not output for security reasons.
# Certificate information is radio specific, so the MAC address of the Wireless Battery Module
# of the attached, or soon to be attached module must match.

# If the certs or keys required a password, it should be specified in the 802.1x PASSWORD field above.

# The MAC address specified below must match the module connected to the pump.
MAC=00:40:9d:66:db:45

CLIENTCERT=

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAuhKvGS9womnF7tmM1iOWuzbvMct7u+TDYtoQSNeItAYe5Bjr
XR+tQOT/2b08nJUjVNI91/+3t2i9qUDDU58DTKKir9dmR5ridHLalylhts8fB7h2a
rZ74YK+4/A12cmNpmwqwDQlwWhJzJgSe5XeZF0ALTd53LEggwpuPb6Eo2Wbnqwr0
/tbsRvaeEjwclGowmuy1v8TrkbSKeFt9l4B54PcI3KxgbnUjH7JIv9h/0nyrOKi
z2P+3maogCnOwxRQp79j/IgCS3JbUBMG14gKnxrJgLuBovvqpsWIYO6k/qohlpyg
Vevc0UUj8XiYEn1lIT1SCXYke/l9jauLBB6OQlIDAQAABAIjBjnmw7qXG2r/Qju
------END RSA PRIVATE KEY------
```
IywTNOYBE/tvFL9KLgsVVm96NOp0762W45hm99St9f/ErnS7BWVVQxyoyLhHyQemx3
wH0dZy9snfIUQyAqNcF52xf1b/ja/EtA2ZVXV61z6U3mLD+16f+kdZmw71D0R8B
UZ4Y0EjjPHUeOsdfnYpjL6oWBG+v3+TEo3WCCqHs9H8yoVKP30Xnfb1JMMgRLf/
inflh6Qg6QKBMM+vWQJlUYuM4hBQtQ6HmwWv2epeu8YFdm3m3TSrv+W81BbY2N5D
N9TZsdUJ54NHtVzTjVmAAXCspBp3+yTOMRPnzgW0v8MLMhFanjiC5QypG712HIQx
gk7LZGECgYEA4vb26UpZNSsOlgzcEQP8fQ82Dk5xNjb9e7qDSD85LUppR6F4xwNs
QPyFVYRemb+pQylwI1X2SNAAdRvsDwSsFVT9ENi1PzlHbOfaBWE9/VNMAz8vcJfr
tcC3So6IWWIHNeol81dwrT0gZFENH/H4D0OBC7U0aoyjvtnYBpIMcGYEa0eaJ
mITPEmZRI8kaCb/TwLTLzmH2SOPCPgc/qVmJ2Fl8I8T3KJX5d8ophY84Kay4le
axVUugldKnyNvr038RX0Dirn+qzn5PkJumdY+tnCxaXbT/tSwkeiNamZOHxeH
boVReX6ONDvT+u9MkvwMdmhwBb9G4izw26a88MCgYAhqyFJLTGdPINkqZXApIHC
IA6aAsNDetd6kspFXrkPh50dfFTEs54iUeYxh4/oF2d/vprNnf2yCCHOEOhdEhyHsr
EBt0824dowFOUScRbgmRGljC21W2SKAEPROOUCFpqjvYhs2I2s5b7qoaeL1
L9Dj/kGpQpT/JNJWk2BEdsZwkbQDFNt5BN0d20K5/xR5n3Wwx778a8g35rtplt
uOnqRk2Vcne67a0FvgeUnZ+17t1U9FSkOFgpVWMgaxKw6HbJqehBB2bRCHOmhH2
b53Fq/9lIxRy+G7fl+busJllfRwGJT6Un6p3kttgLWqAC3aQMzghjhy7xt25aQ+9
p8ZfeEQKbgB6jQAT31FxvPFHyju4NdeQogJd2c2nFbkc7aqOEPKNG9Nbz/VVWh7x
Rx7Aaxa3D20YrC7H7V1ncRX1dlnpYj/hYxc5/VdtdLZ2yhEc2GiG/jfgNKw2W2BZd
2NLf54bgV67lck2yKMK/5wBru+V73WmqvWFq4KsMesLBBzMRvJa

-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFWzCCBEOgAwIBAgIQArl0FxoUrLR0mlXvP3m/RJzANBgkqhkiG9w0BAQsFADBy
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMTAwLgYDVQQDEwZCYXhlZDIwMAYGCSqGSIb3DQEJE
aWF0ZSBsB290IENBMIIFNQIITmWhcNMTcwMzE1MDAwMDAwWhcNMTgwMzE1MTlwMDAw
WjCBI3DLMAkGA1UEBhMCVVMXczA1BgNVBAGkTWjCBI3DLMAkGA1UEBhMCVVMXczA1BgNV
bGUxNzA1BgNVBAoTLk5hdGlvbmZsb3d3cyBlb3BzIENlcnQlMAsGA1UEAwwlZm92LjA4
MA0GCSqGSIb3DQEBAQUAA4IBAwIBBgBEGINCERTIFICATE-----
-----END CERTIFICATE-----

# Client certificate expiration date, GMT in the format: MM/DD/YYYY HH:MM:SS.

CLIENTCERTEXPIRE=

# Trusted certificates, maximum of 5.

TRUSTEDCERTS=

-----BEGIN CERTIFICATE-----

MIIGSTCCBTGgAwIBAgIEM6qqqjANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQGEwJV

-----END CERTIFICATE-----
kUDPAEO4yHSXDnoe0fhk24/yCuO6Wc+mMe7YXzEkw8pOEWjNw/9E1dsP20L7jD3F
97q5uVNe1wEaeE3UEqIxEKUbdyQgitinpTv/y0/UPTDLpfjBmK2nh2HK6r0RH+YC
OicqQ99N+q6YeAlhejLa7+7FkKYK1YEAhE1cc=

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIDpjCCAo6gAwIBAgIBMzANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQGEwJVUzEV
MBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29t
MSMwIuYDVQQLDExwM0g2LzAgejKAg0iME0lMjIzMQswCQYDVQQGEwJjMCkGA1UE
BxMlMjIzMQ showdownMQswCQYDVQQGEwJjMCkGA1UEBxMlMjIzMQswCQYDVQQGEwJj
MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AIIIBNgKCAQEACgkCAQEA0DLgpmXl2Y15UL561qqyqiBMpmRtM9/w/1pqoA/Geri19
VMFvrtPTGw9I9f0dQsRMy2d8V4INSj43YqXeXnTPzanTSqza95yoH/h4xUM/pNq
AIIO8c+cYMyCdZTQ0veEwcvPZotXYABac9E9ceT015RdDS5eRjMwTcb6NxydZr8
nRd9/J66L4R171KVtU74lwA6fwNd0UnxhVhGdeEae+eIEvJ5IWxDeS6ZdZuSZv
h24QxhxpucTzSg81HHCHw4a1kOe2oIDUJY698atS0nxw3lR30heQ/g793Mce9
SX9u2dPPAztSaW8/38TwkNOa9zkRFn7oF+cQIDAQABo2MwYTAOBgNVHQ8BAf8E
BAMCAAYwDwYDV0TAQH/BBAwAwEB/zAdBgNVHQQ4FgQU9kZGxa7N5lj9z/YhSzk
yepFDx4wHwYDVR0jBBgwFwOAU9kZGxa7N5lj9z/YhSzyepYDx4wDQYJJoZihvcN
AQELBQUQdEBAeQacFm1sFPOIEvXDVl3IH2RK7Fhe0pM0bK2Soj137LMf+ctpM
3bFKJPPY97IE0g7T1qgR8TN2sk0moumMTPjWCdFWJyY4nak56tPiWEG2XobJ9H1r
iuVXlKd2M/1yhquy1o5ktbOGXLFsd3qdp4A1tcXuK2wyMTiSCYS3Uow61JdEw6M
eyrylMlpy9GtvaXZ6LdnzoAbhKC7bVUY7ob0T4E03fQ8h1QCPupvY7Db1/Xmlw8
QWVd6AOH7EEP3P8xbW0VCWZSW5XbstWY014GeJFXZ7YreaAg8sYa6CzasuHkr/rxeZ
8yzOmCTTTSPK5Ju5bTfAyEpargk5fDvntJQg=

-----END CERTIFICATE-----
Appendix C  References


