NIST SPECIAL PUBLICATION 1800-8C

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

August 2018

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-8

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order 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.

National Institute of Standards and Technology Special Publication 1800-8C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-8C, 257 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

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, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including 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. However, 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 by 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; virtual private network (VPN); Wi-Fi; wireless medical devices

ACKNOWLEDGMENTS

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

Name	Organization
Arnab Ray	Baxter Healthcare Corporation
Pavel Slavin	Baxter Healthcare Corporation
Phillip Fisk	Baxter Healthcare Corporation
Raymond Kan	Baxter Healthcare Corporation
Tom Kowalczyk	B. Braun Medical Inc.
David Suarez	Becton, Dickinson and Company (BD)
Robert Canfield	Becton, Dickinson and Company (BD)
Rob Suarez	Becton, Dickinson and Company (BD)
Robert Skelton	Becton, Dickinson and Company (BD)
Peter Romness	Cisco
Kevin McFadden	Cisco
Rich Curtiss	Clearwater Compliance
Darin Andrew	DigiCert
Kris Singh	DigiCert
Mike Nelson	DigiCert
Chaitanya Srinivasamurthy	Hospira Inc., a Pfizer Company (ICU Medical)
Joseph Sener	Hospira Inc., a Pfizer Company (ICU Medical)
Chris Edwards	Intercede
Won Jun	Intercede
Dale Nordenberg	Medical Device Innovation, Safety & Security Consortium (MDISS)

Name	Organization
Jay Stevens	Medical Device Innovation, Safety & Security Consortium (MDISS)
Carlos Aguayo Gonzalez	PFP Cybersecurity
Thurston Brooks	PFP Cybersecurity
Colin Bowers	Ramparts
Bill Hagestad	Smiths Medical
Axel Wirth	Symantec Corporation
Bryan Jacobs	Symantec Corporation
Bill Johnson	TDi Technologies, Inc.
Barbara De Pompa Reimers	The MITRE Corporation
Sarah Kinling	The MITRE Corporation
Marilyn Kupetz	The MITRE Corporation
David Weitzel	The MITRE Corporation
Mary Yang	The MITRE Corporation

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components 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:

Technology Partner/Collaborator	Build Involvement
Baxter Healthcare Corporation	• Sigma Spectrum™ Large Volume Pump (LVP) Version 8 • Sigma Spectrum Wireless Battery Module Version 8 • Sigma Spectrum Master Drug Library Version 8 • Care Everywhere Gateway Server Version 14
B. Braun Medical Inc.	• Infusomat® Space Infusion System / Large-Volume Pumps • DoseTrac® Infusion Management Software / Infusion Pump Software

Technology Partner/Collaborator	Build Involvement
Becton, Dickinson and Company (BD)	• Alaris® 8015 Patient Care Unit (PCU) Version 9.19.2 • Alaris Syringe Module 8110 • Alaris LVP Module 8100 • Alaris Systems Manager Version 4.2 • Alaris System Maintenance (ASM) Version 10.19
Cisco	• Aironet 1600 Series Access Point (AIR-CAP1602I-A-K9) • Wireless LAN [Local Area Network] (WLC) Controller 8.2.111.0 • Identity Services Engine (ISE) • Adaptive Security Appliance (ASA) • Catalyst 3650 Switch
Clearwater Compliance	• IRM|Pro™ • IRM|Analysis™
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 • MedNet™ Version 6.2
Intercede	MyID®
Medical Device Innovation, Safety & Security Consortium (MDISS)	Medical Device Risk Assessment Platform (MDRAP™)
PFP Cybersecurity	Device Monitor
Ramparts	Risk Assessment

Technology Partner/Collaborator	Build Involvement
Smiths Medical	• Medfusion® 3500 Version 5 Syringe Infusion System • PharmGuard® Toolbox Version 1.5 • Medfusion 4000 Wireless Syringe Infusion Pump • PharmGuard Toolbox 2 Version 3.0 use with Medfusion 4000 and 3500 Version 6 (US) • PharmGuard Server Licenses, PharmGuard Server Enterprise Edition Version 1.1 • CADD®-Solis Ambulatory Infusion Pump • CADD-Solis Medication Safety Software
Symantec Corporation	• Symantec Endpoint Protection (SEP) • Advanced Threat Protection: Network (ATP:N) • Data Center Security: Server Advanced (DCS:SA)
TDi Technologies, Inc.	ConsoleWorks®

Contents

List of Figures

List of Tables

1 Introduction

The following guides show information technology (IT) professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not recreate the product manufacturers' documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

1.1 Practice Guide Structure

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate commercially available technologies that can help secure the wireless infusion pump ecosystem. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST Special Publication (SP) 1800-8a: *Executive Summary*
- NIST SP 1800-8b: *Approach, Architecture, and Security Characteristics* – what we built and why
- 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 National Cybersecurity Center of Excellence (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 whole 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 the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of commercially available technologies that can help secure the wireless infusion pump ecosystem. 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. In *NIST SP 1800-8b*, Section 4.4, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

1.2 Typographical Conventions

The following table presents typographic conventions used in this volume.

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

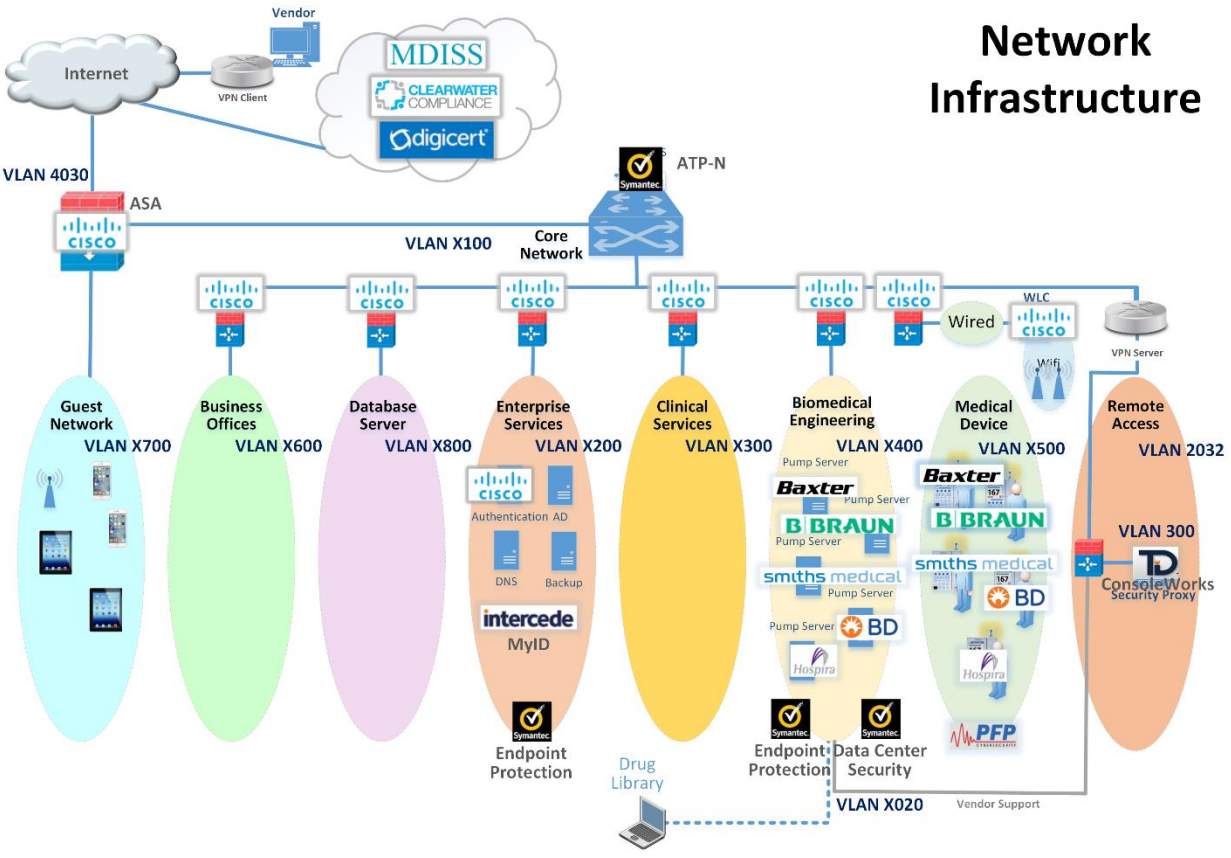
1.3 How-To Overview

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

1.4 Logical Architecture Summary

Figure 1-1 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 Logical Architecture Summary



2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring all of the products 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. The core network 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 that we built has its own ASA, with two interfaces to protect each 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 the *Cisco 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 interface to the wide area network (WAN), and the third interface 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.

Next, we configured the ASA with a baseline-configuration template that allows all outbound traffic, as well as only related inbound traffic as allowed by the stateful firewall. Internet Control Message Protocol (ICMP) [4] enables troubleshooting with ping and traceroute tools. Authenticated OSPF automated 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 of Appendix A 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 ASA interfaces are configured with equal security levels, they, by default, 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 of Appendix A 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 the 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 (SEP) server. Several ports are open for any host to the Symantec Data Center Security: Server Advanced (DCS:SA).

See Section A.3 of Appendix A 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, and 11444
- all pumps > *B. Braun Pump server* on Ports 443, 80, 8080, 1500, and 4080

See Section A.4 of Appendix A 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 electronic health record (EHR) system or vendor maintenance, are completed with the associated pump server on the biomedical engineering network. This enables us to deny 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; however, if you need 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 on Ports 8100, 9292, 443, and 8443
- *Baxter Pump Server* > all pumps on Port 51243
- *B. Braun Pump Server* > all pumps on Ports 80, 443, 8080, and 1500

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

2.1.6 Cisco Catalyst Switch Configuration

The Catalyst 3650 switch is configured with four virtual local area networks (VLANs) [7]. One port is assigned to a management VLAN, with Subnet 192.168.20.0/24. Wireless access points (APs) are connected to a Wi-Fi management VLAN, which is also trunked back to the virtual wireless LAN controller (WLC) software. Additionally, the biomedical engineering network and the medical device network 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 APs. 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* [8].

See Section A.6 of Appendix A 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. As a completely closed network, the Wi-Fi management network is used for management and communication between the Cisco Aironet wireless APs and the Cisco WLC. The WLC is the central point where wireless service set identifiers (SSIDs), VLANs, and Wi-Fi Protected Access II (WPA2) [9] security settings are managed for the entire enterprise. We defined two SSIDs: *IP_Dev* and *IP_Dev_Cert*. IP_Dev uses WPA2-PSK (Pre-Shared Key), 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* [10].

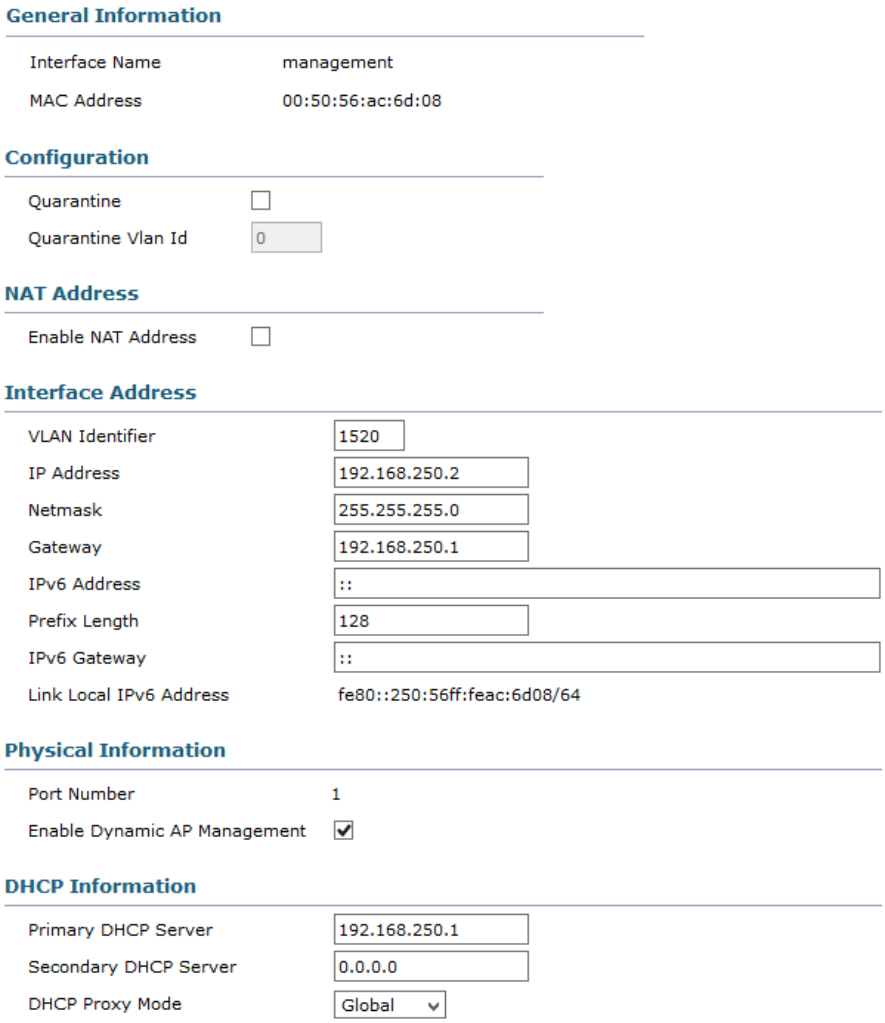
We imported the virtual appliance called *AIR_CTVM_K9_8_2_111_0.ova*, assigning the first interface to the management network, referred to as *service-port* in the web interface. The second interface is used as a trunk port, with VLAN tags for all user and Wi-Fi management traffic. In the web interface,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

The primary management mechanism for the WLC is the web interface. To configure an Internet Protocol (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

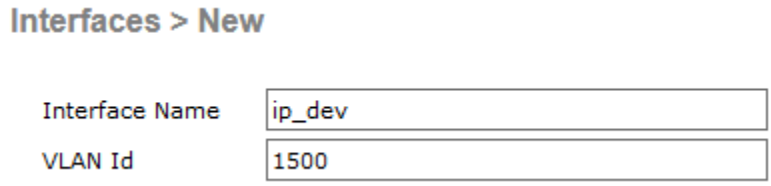
Follow these steps to configure network interfaces:

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

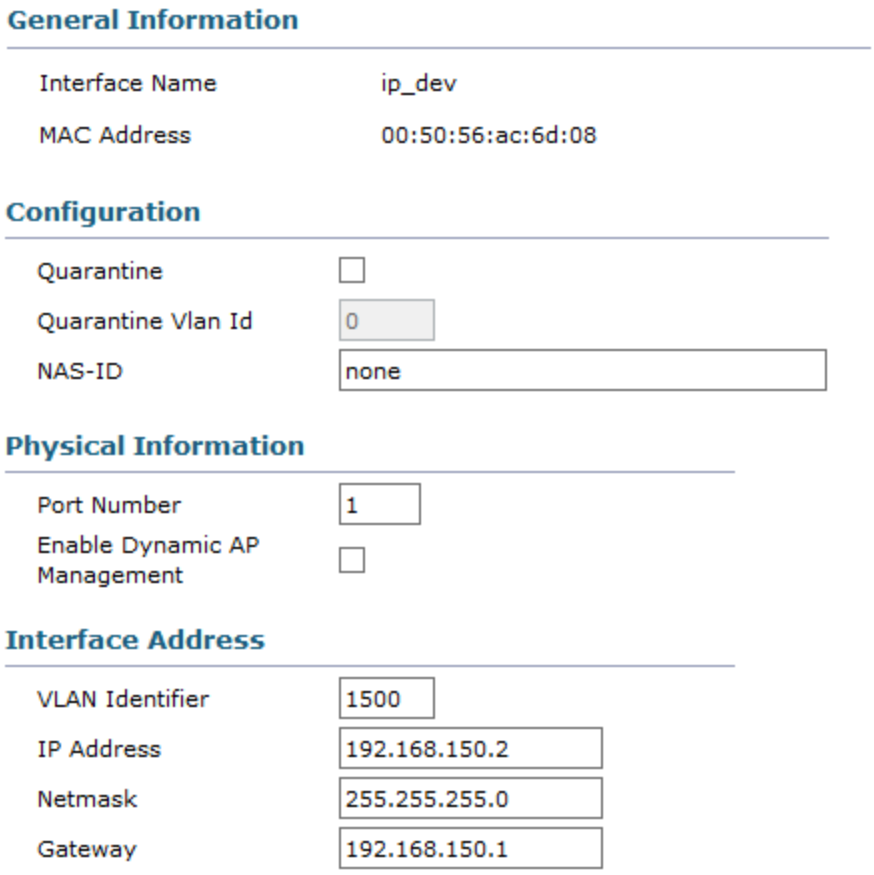


2. Configure interfaces for user Wi-Fi traffic by first mapping the interface to an Ethernet port and setting the VLAN and IP address, and then mapping to wireless SSIDs.

    a. Create the new interface at **Controller** > **Interfaces** > **New**.



    b. Configure the new interface by using the form shown below. Refer to the completed interface for the values that we used in the lab.

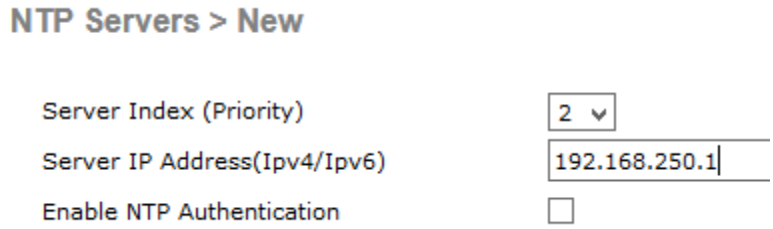


c. Our completed list of interfaces looks as shown below.

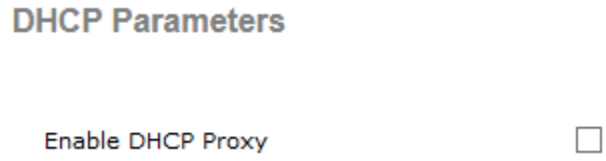
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ip_dev	1500	192.168.150.2	Dynamic	Disabled
ip_dev_biomedical	1400	192.168.140.2	Dynamic	Disabled
management	1520	192.168.250.2	Static	Enabled
service-port	N/A	192.168.29.146	Static	Disabled
virtual	N/A	1.1.1.1	Static	Not Supported

3. Configure the Network Time Protocol (NTP) server [11] at **Controller** > **NTP** > **Server** > **New**.



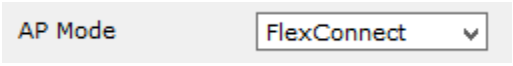
4. To configure the DHCP server, disable the DHCP Proxy at **Controller** > **Advanced** > **DHCP**.



2.1.7.3 Wireless AP Connection and Setup

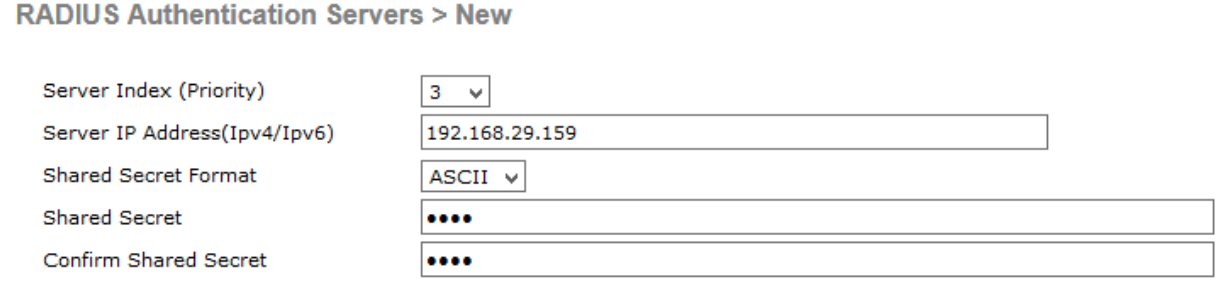
Connect the APs to the Ethernet ports configured for untagged VLAN 1520. The APs will automatically obtain their addresses and the WLC address via DHCP from the switch (see Section 2.1.6). No other VLANs should to be configured for the APs because we are using a centralized switching model where Wi-Fi 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**, as shown below.



2.1.7.4 Authentication Configuration

To use certificate-based authentication, the WLC must consult a remote authentication dial-in user service (RADIUS) server. Configure the Cisco Identity Services Engine (ISE) RADIUS server IP address and shared secret at **Security** > **RADIUS** > **Authentication** > **New**.



2.1.7.5 WLANs Configuration

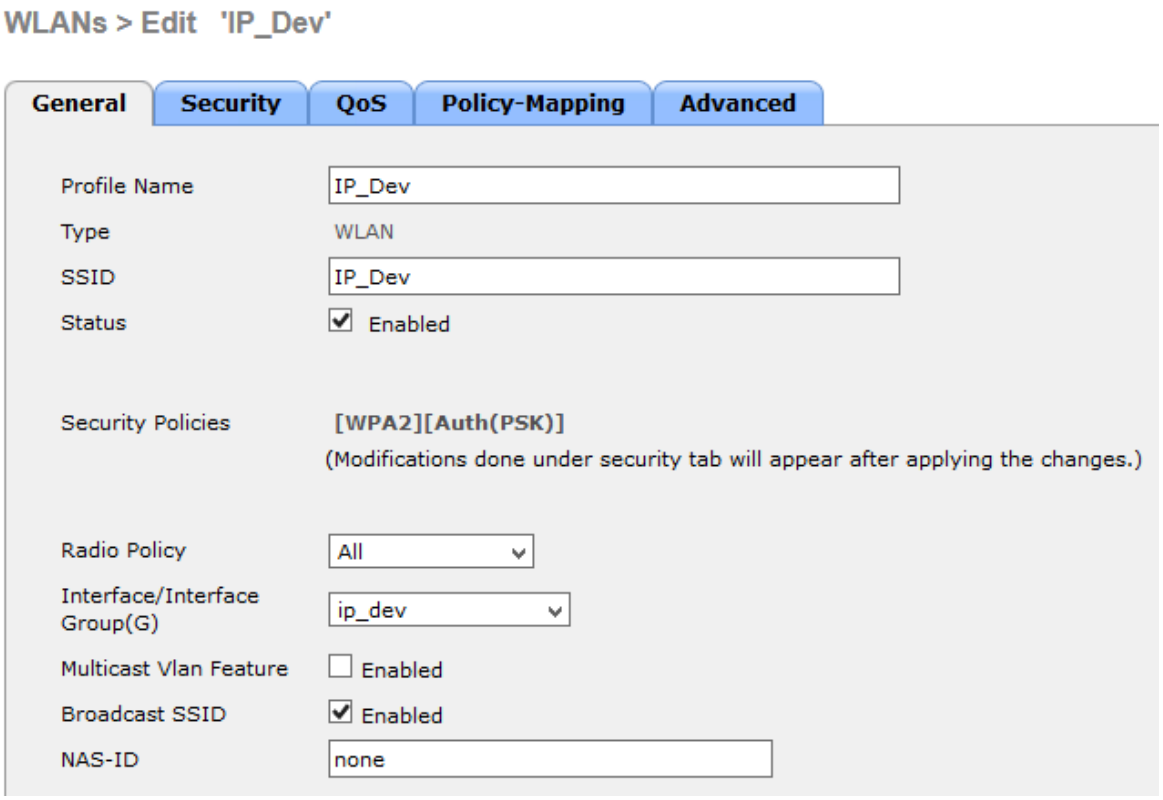
At this point, we configured two SSIDs for medical devices: IP_Dev and IP_Dev_Cert. IP_Dev is configured for WPA2-PSK (Advanced Encryption Standard [AES] [12]), and IP_Dev_Cert is configured for WPA2-Enterprise (AES). Both SSIDs use the same interface, and therefore connect to the same network VLAN; the only difference is the Wi-Fi security.

To create a new SSID, follow these steps:

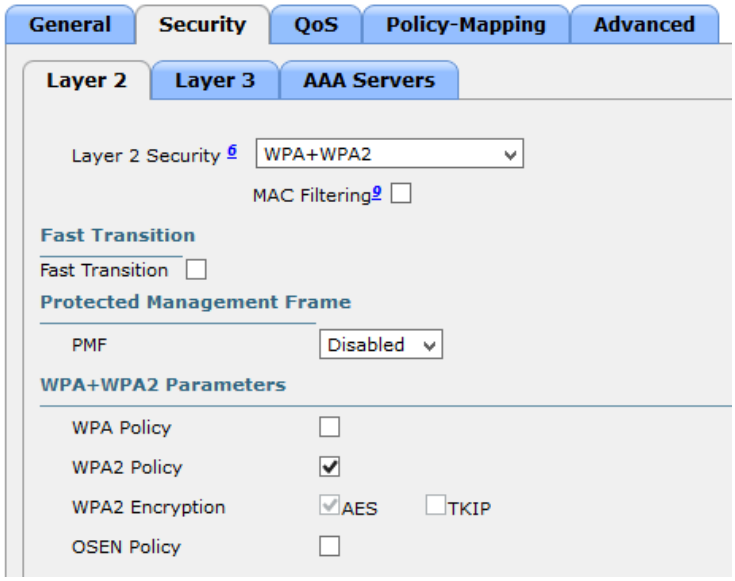
1. Use the **WLANS** tab, select **Create New** from the dropdown list and click **Go**.

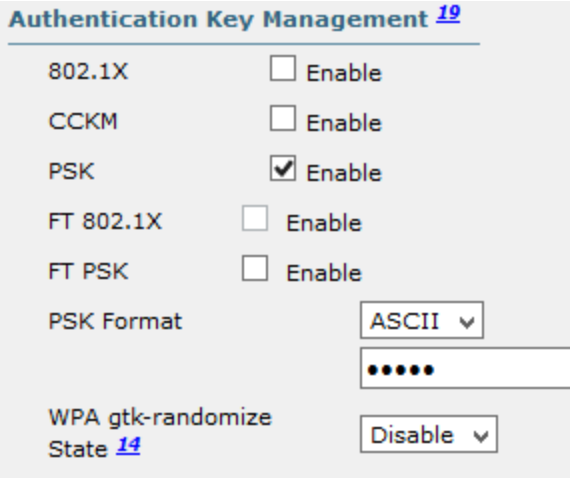
2. Enter your new SSID information.

3. In **WLANs** > **WLANs** > **WLANs**, select the WLAN identification (ID) number of the newly created SSID. For the **Status**, select the checkbox for **Enabled**. Set the **Interface/Interface Group(G)** to **ip_dev**.



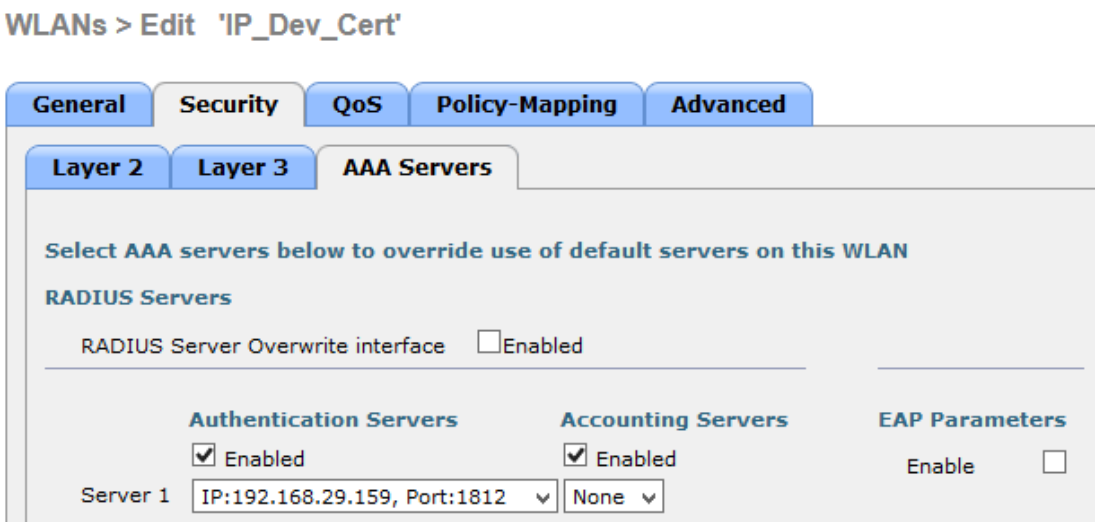
4. On the **Security** tab, on the **Layer 2** sub-tab, under **Authentication Key Management**, de-select the **Enable** checkbox for **802.1X**, select the **Enable** checkbox for **PSK**, and set the PSK Format.





5. For the SSID IP_Dev_Cert, repeat Steps 1 through 4 above (replacing IP_Dev with IP_Dev_Cert in the instructions), but do not change the security settings for **Authentication Key Management** (leave **802.1X** checked, and leave **PSK** unchecked).

6. On the **Security** tab, on the **AAA Servers** sub-tab, select the RADIUS server to authenticate with (**Server 1**).



2.1.7.6 Monitoring

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

Client MAC Addr	IP Address(Ipv4/Ipv6)	WLAN Profile	WLAN SSID	User Name
00:17:23:e1:8e:32	192.168.250.116	IP_Dev_Cert	IP_Dev_Cert	BBraun
00:17:23:f3:9f:db	192.168.250.123	IP_Dev	IP_Dev	Unknown
00:17:23:f4:f5:4e	192.168.250.118	IP_Dev_Cert	IP_Dev_Cert	Carefusion
00:18:e7:8f:cd:1f	192.168.250.126	IP_Dev	IP_Dev	Unknown
00:40:9d:96:04:0c	192.168.250.125	IP_Dev	IP_Dev	Unknown
00:40:9d:96:06:06	192.168.250.124	IP_Dev	IP_Dev	Unknown
00:80:92:68:62:26	192.168.250.117	IP_Dev_Cert	IP_Dev_Cert	Hospira
28:ed:6a:f2:4e:37	192.168.250.122	IP_Dev_Cert	IP_Dev_Cert	Baxter

2.1.7.7 Final Configuration

See Section A.7 of Appendix A for the WLC configuration. You can access details about additional configuration options in the *Cisco Wireless Controller Configuration Guide, Release 8.0* [13].

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 delivery organizations (HDOs) to manage, monitor, and record activities from external vendors in the IT infrastructure.

2.1.8.1 System Environment

The NCCoE lab set up a fully updated (as of April 20, 2016) CentOS 7 operating system, with the following hardware specifications:

- 8 gigabytes (GB) of random access memory (RAM)
- 40 GB hard disk drive
- one network interface

2.1.8.2 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 libbpng12 libvncserver

2.1.8.3 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/*.
    a. `cd /tmp/consoleworkskeys/`
    b. `tar xzf TDI_Licenses.tar.gz`
    c. `cp /tmp/consoleworkskeys* /etc/TDI_licenses/`
    `/opt/ConsoleWorks/bin/cw_add_invo`
8. Accept the License Terms.
9. Press the **Enter** key to continue.
10. Name the instance of ConsoleWorks.
11. Press the **Enter** key to accept the default port (Port 5176).
12. Press the **N** key to deny syslog listening.
13. Press the **Enter** key to accept the parameters entered.
14. Press the **Enter** key to return `to /opt/ConsoleWorks/bin/cw_add_invo.`
15. `rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-version>.rpm`
16. `/opt/gui_gateway/install_local.sh`
17. `/opt/ConsoleWorks/bin/cw_start` <invocation name created early>
18. `service gui_gatewayd start`

2.1.8.4 Usage

1. Open a browser, and navigate to https://<ConsoleWorksIP>:5176.
2. Log in with **Username**: console_manager, **Password**: Setup.
3. Change the default password.
4. Choose **Register Now**.

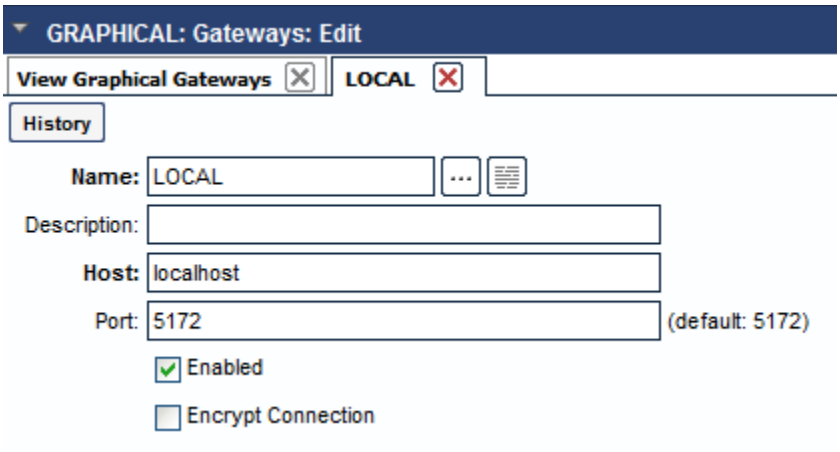
NCCoE chose ConsoleWorks to segregate and limit vendor access to our labs. Our data model groups *consoles* and *graphical connections* together into a *tag*. The tag is a collection of equipment to which you need to connect, although a vendor typically owns the equipment. This tag allows us to operate 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).

2.1.8.5 *Initial Configuration of Graphical Gateway*

This section is only required for graphical connections, such as virtual network computing (VNC) and remote desktop protocol (RDP).

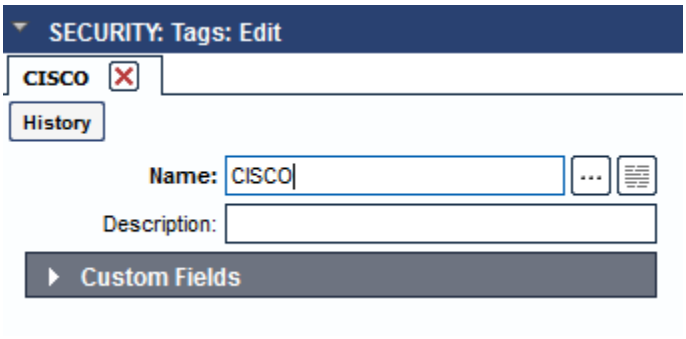
Use the menu in the sidebar to access all instructions provided in Section 2.1.8.5 through Section 2.1.8.12.

1. Click **Graphical** > **Gateways** > **Add**.
2. Set the **Name** as LOCAL, set the **Host** as localhost, and set the **Port** as 5172.
3. Select the **Enabled** checkbox, and then click **Save**.
4. Verify that it works by clicking **Test** in the top-left corner.



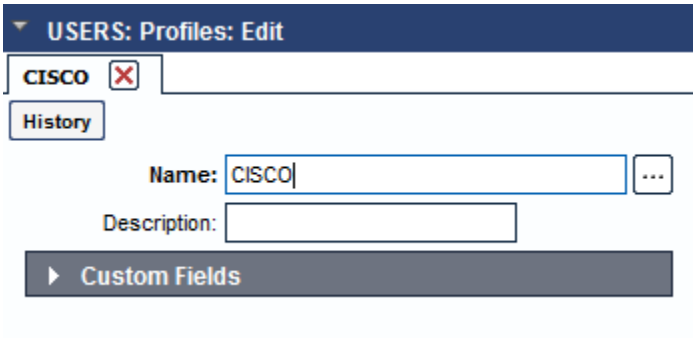
2.1.8.6 Create One Tag for Each Vendor Company

1. Click **Security** > **Tags** > **Add**.
2. Set the **Name** (usually the company name).
3. Click **Save**.



2.1.8.7 Create One Profile for Each Vendor Company

1. Click **Users** > **Profiles** > **Add**.
2. Set the **Name** (usually the company name).
3. Click **Save**.

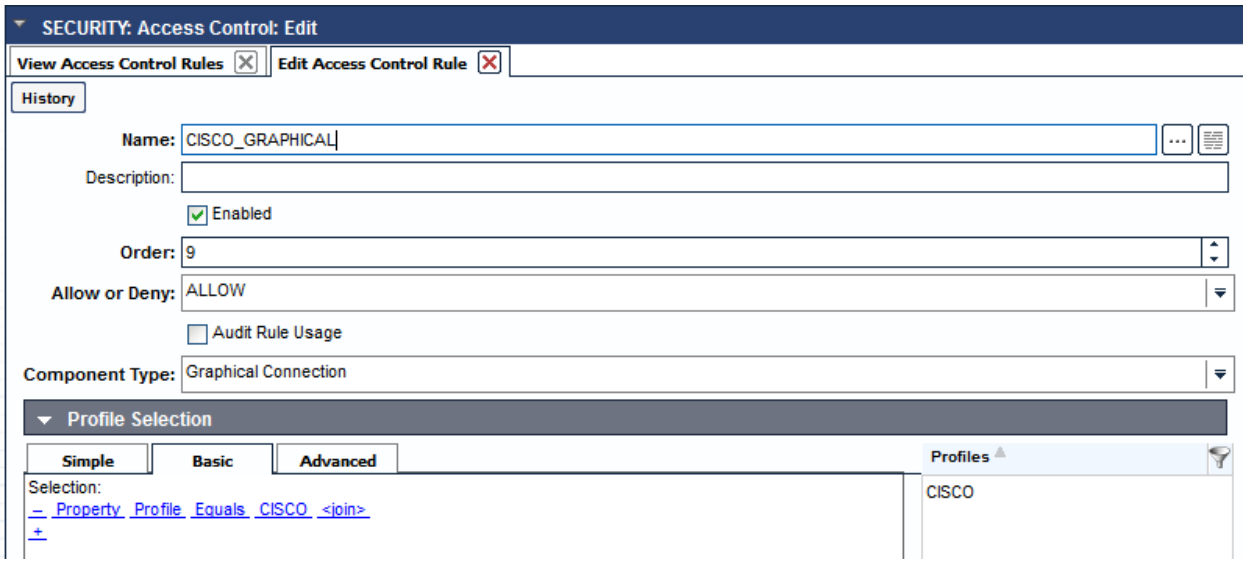


2.1.8.8 Establish Graphical Access Controls

Repeat this section for each vendor company.

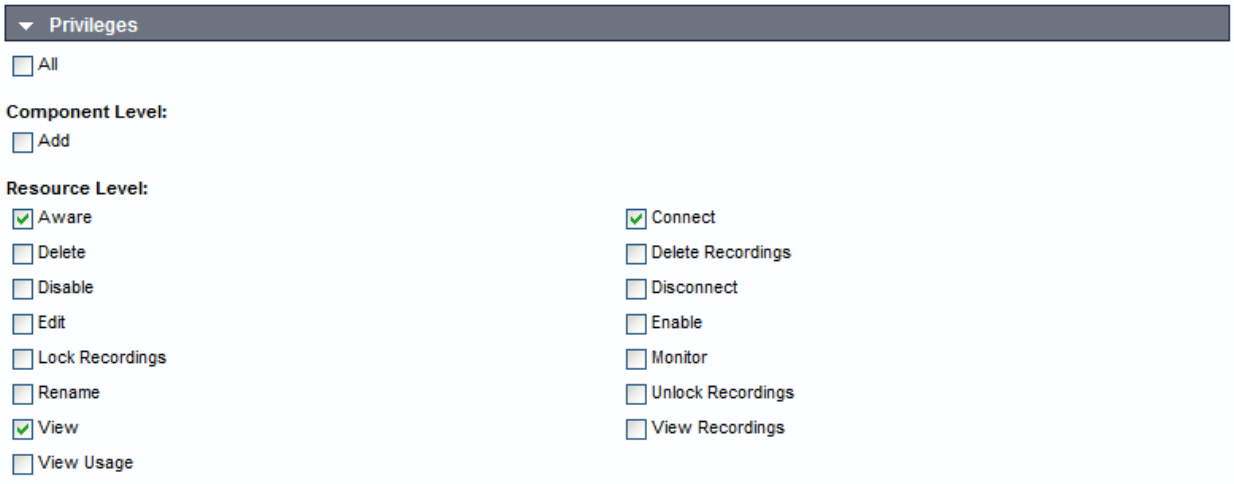
1. Click **Security** > **Access Control** > **Add**.
2. Set the **Name** to [VENDOR_COMPANY_NAME]_GRAPHICAL.
3. Select the **Enabled** checkbox.
4. Set the **Order**.

5. Set the **Allow or Deny** field to ALLOW.
6. Set the **Component Type** to Graphical Connection.
7. Look under **Profile Selection**; you should see:
    a. on the **Basic** tab, **Property Profile Equals [vendor company profile name] <join>**
    b. the vendor company profile in the box on the right



8. Look under **Resource Selection**; you should see:
    a. on the **Basic** tab, **Associated With a Tag** that
    Property Tag Equals [vendor company tag name] <join>

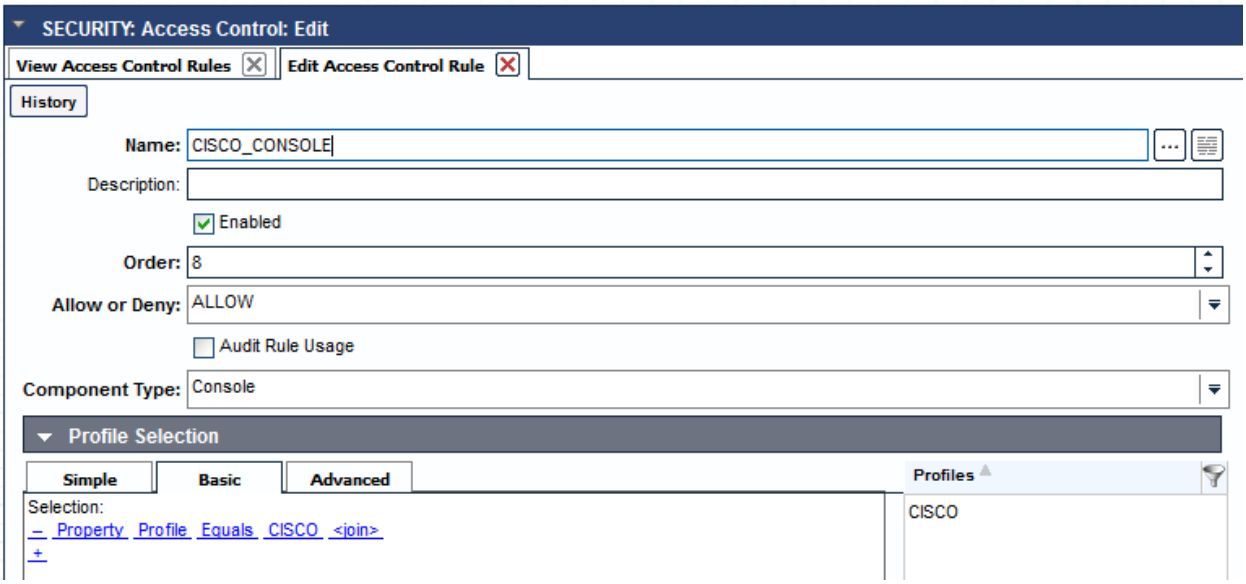
    b. matching graphical connections in the box on the right
9. Under **Privileges**, under **Resource Level**, select the following checkboxes:
    a. **Aware**
    b. **View**
    c. **Connect**



2.1.8.9 Console Access Controls

Repeat this section for each vendor company.

1. Click **Security** > **Access Control** > **Add**.
2. Set the **Name** to [VENDOR_COMPANY_NAME]_CONSOLE.
3. Select the **Enabled** checkbox.
4. Set the **Order**.
5. Set the **Allow or Deny** field to ALLOW.
6. Set the **Component Type** to Console.
7. Look under **Profile Selection**; you should see:
    a. on the **Basic** tab, **Property Profile Equals [vendor company profile name] <join>**
    b. the vendor company profile in the box on the right



8. Look under **Resource Selection**; you should see:

    a. on the **Basic** tab, Associated With a Tag that
    Property Tag Equals [vendor company tag name] <join>

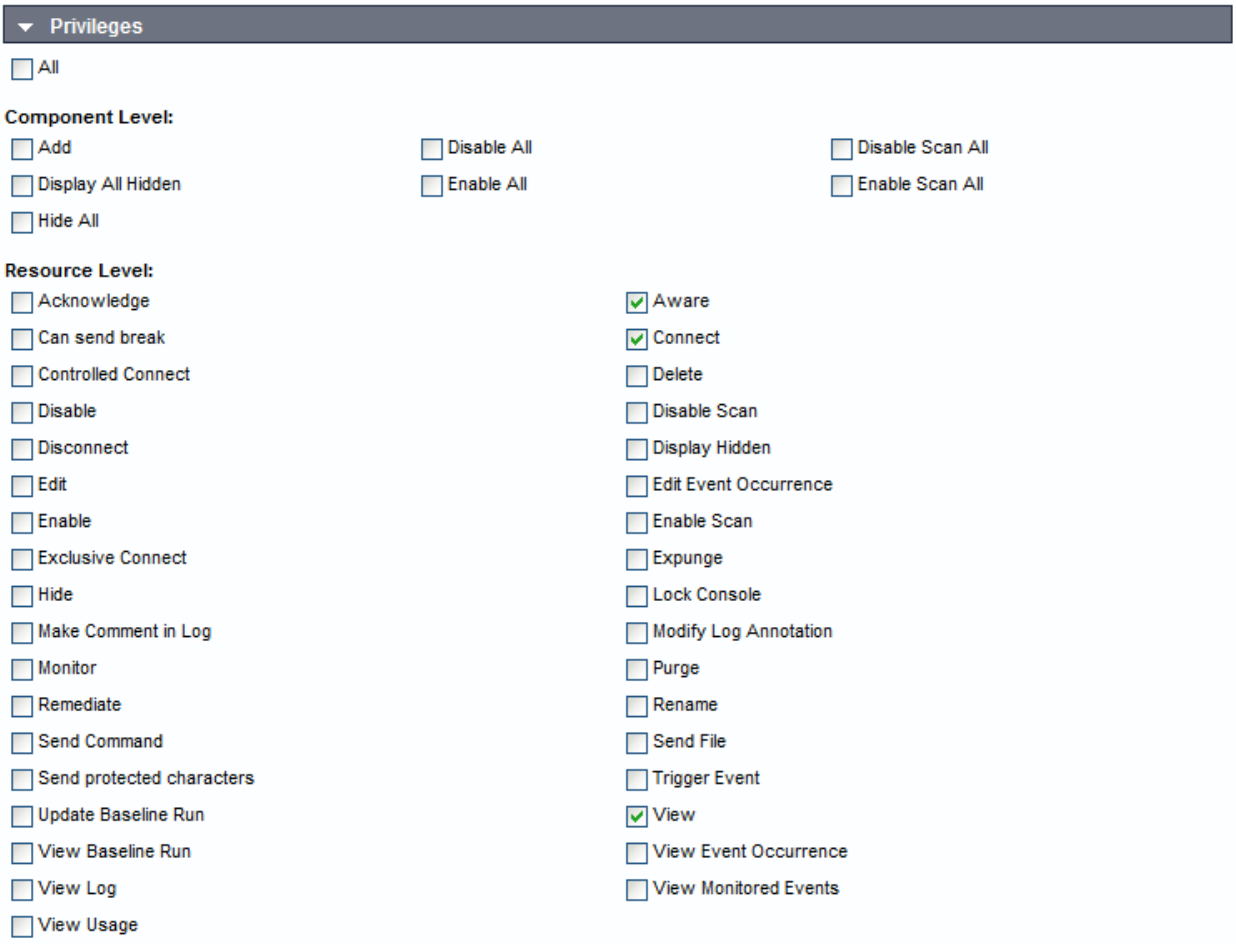
    b. matching consoles in the box on the right

9. Under **Privileges**, under **Resource Level**, select the following checkboxes:

    a. **Aware**

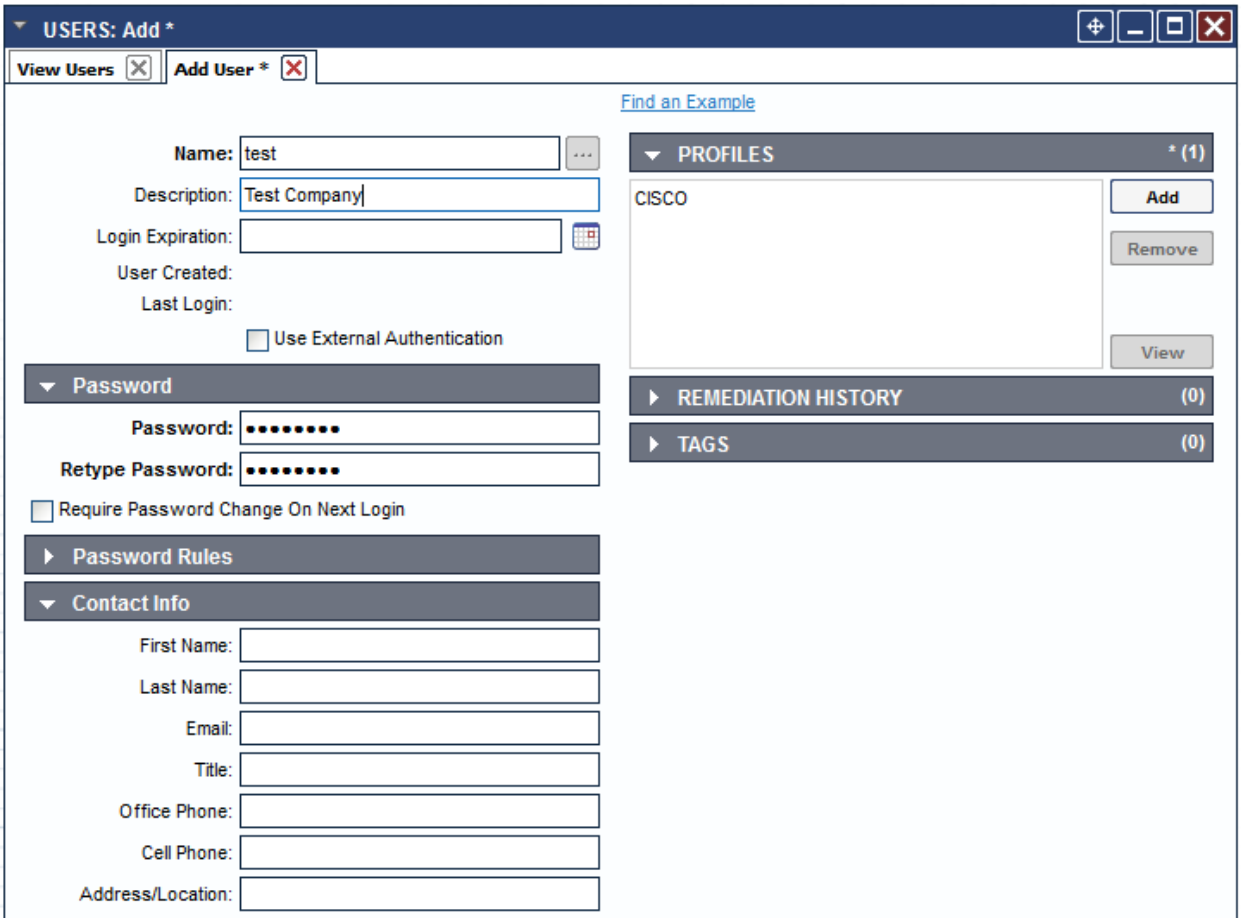
    b. **View**

    c. **Connect**



2.1.8.10 Users

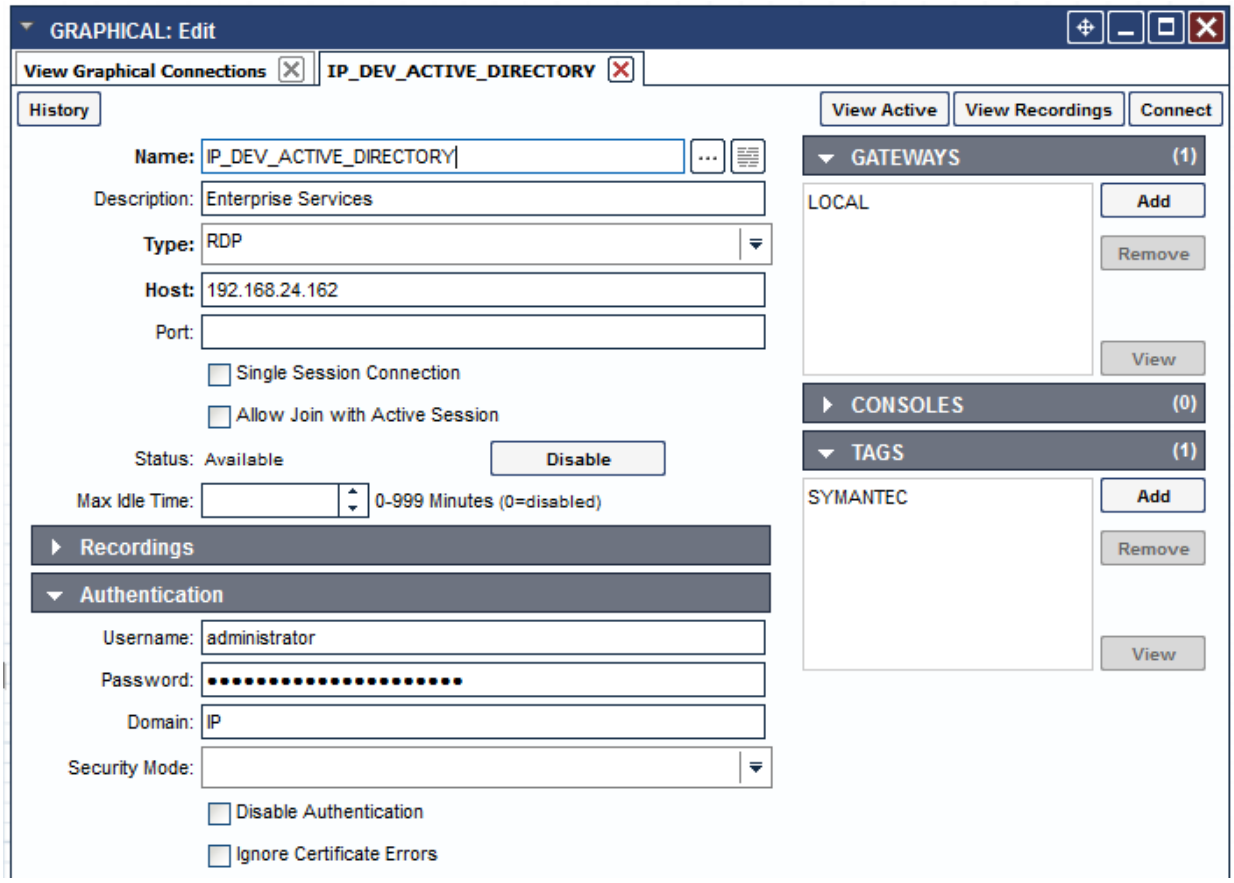
1. Click **Users** > **Add**.
2. Set the **Name** (usually the company name).
3. Set the **Description**.
4. Set the **Password**, and then retype the password to confirm (**Retype Password**).
5. Fill in contact information (under **Contact Info**).
6. Set the profile to the one defined for this user's company (under **PROFILES**).
7. Click **Save**.



2.1.8.11 Add an RDP Graphical Connection

1. Click Graphical > Add.
2. Set the **Name** for the device to which you are connecting.
3. Set the **Type** to RDP.
4. Set the **Host** for the device to which you are connecting.
5. Set the following **Authentication** fields:
    a. **Username**
    b. **Password**
    c. **Domain** (optional)
6. Add the Graphical Gateway named LOCAL (under **GATEWAYS**).

7. Add tags for all vendor companies that should have access (under **TAGS**).
8. Click **Save**.

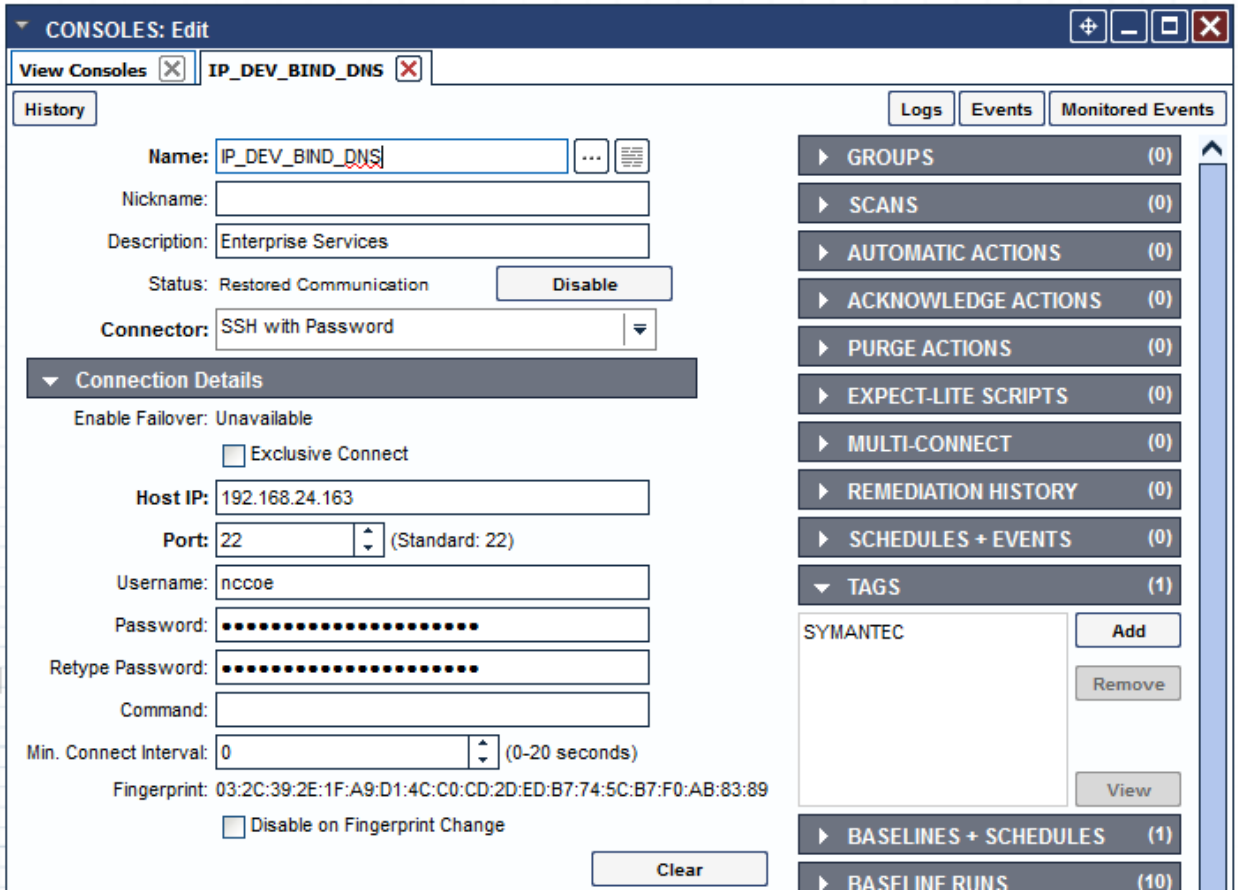


2.1.8.12 Add an SSH Console Connection

1. Click Consoles > Add.
2. Set the **Name** for the device to which you are connecting.
3. Set the **Connector** to SSH with Password.
4. Set the **Host IP** for the device to which you are connecting, by doing the following:
    a. Set the **Port** to **22**.
    b. Set the **Username**.
    c. Set the **Password**.

d. Retype the password (**Retype Password**).

5. Add tags for all vendor companies that should have access (under **TAGS**).
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 pump products listed in Table 2-1.

Table 2-1 Infusion Pump List

Vendor Name	Product Name	Product Type	Description
B. Braun	Space Station	Station for hosting individual pump	Provides centralized power and network connection for pumps stacked on the station
	Infusomat® Space Large-Volume Infusion Pump	Wireless infusion pump	Designed for acute-care facilities for adults and children
	Perfusor® Space Syringe Pump	Syringe infusion pump	Can be stacked in Space Station and uses Space Station for network communication
Baxter	Baxter Sigma Spectrum	Wireless infusion pump	Provides a large-volume infusion capability for patients
BD	Alaris Patient Care Unit (PCU) 8015	Infusion pump core system	Provides a common user interface for programming infusion, network connection, and monitoring modules. The Alaris 8015 PCU is the core of the Alaris system and provides a common user interface for programming infusion and monitoring modules.
	Alaris Syringe 8110	Syringe infusion pump	Provides a syringe infusion capability for patients, and works with the Alaris PCU

Vendor Name	Product Name	Product Type	Description
	Alaris Pump 8100	Large-volume infusion pump	Provides a large-volume infusion capability for patients, and works with the Alaris PCU
Hospira	Plum 360	Infusion system	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
	Hospira PCA	PCA syringe infusion system	Complements the infusion pump to manage pain
Smiths Medical	Medfusion 4000	Syringe infusion pump	Delivers medication to patients in critical care units
	CADD-Solis 2000	Ambulatory infusion pump	Delivers medication to patients in hospital, home care, and alternative care facilities

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 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 with Extensible Authentication Protocol – Transport Layer Security

(EAP-TLS) [14], we configured the pumps to use an individual certificate issued by DigiCert for wireless network authentication, using the 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. Table 2-2 summarizes these key configuration steps. See Appendix B for the sample configuration files.

Table 2-2 Summary of Infusion Pump Configuration Methods

Vendor Name	Infusion Pump Model	Configuration Tool	Connection Method
Baxter	Sigma Spectrum	• uses a PC with an Infrared Data Association (IrDA) interface to program multiple pumps with the same configuration • edits the network configuration file (a simple text file) on a PC, and sends it via the IrDA to a pump	• uses the IrDA Serial Infrared • links to a PC under the IrDA Serial Infrared Link Management Protocol Version 1.1
B. Braun	Space Station	• connects a PC with the HiBaSeD service program to the Space Station by using a B. Braun interface cable for pump configuration setting	• uses a special B. Braun interface cable
	Infusomat Space Large-Volume Infusion Pump	• connects a PC with the HiBaSeD service program to the Space Station by using a B. Braun interface cable for pump configuration setting	• uses a special B. Braun interface cable

Vendor Name	Infusion Pump Model	Configuration Tool	Connection Method
	Perfusor Space Syringe Pump	• connects a PC with the HiBaSeD service program to the Space Station by using a B. Braun interface cable for pump configuration setting	• uses a special B. Braun interface cable
BD	Alaris 8015 PC	• uses a management system to do the configuration • is the core of the Alaris system and provides a common user interface for programming infusion and monitoring modules	• uses a series cable to connect the pump to a local computer
Hospira	Hospira PCA	• accesses Web Configuration Utility on the pump through a web browser using the local IP address of the pump	• uses the pump's Ethernet jack to connect to a LAN or to interface with the host computer
	Plum 360	• accesses Web Configuration Utility on the pump through a web browser using the local IP address of the pump	• uses the pump's Ethernet jack to connect to a LAN or to interface with the host computer

Vendor Name	Infusion Pump Model	Configuration Tool	Connection Method
Smiths Medical	Medfusion 4000	• pushes a configuration text file to the pump by using the Telnet from a PC that is connected to the pump with the known IP address	• connects a PC to pump using micro Universal Serial Bus (USB)-USB cable
	CADD-Solis 2000	• uses Smiths Medical Network Configuration Utility to update the pump's configuration parameters	• connects a PC to the pump by using a micro USB-USB cable

2.2.1.2 *Infusion Pump Configuration*

Pre-Conditions:

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

Post-Conditions:

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

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

- For wireless properties:
  - enable wireless.
  - use DHCP.
  - set the SSID (IP_Dev or IP_Dev_Cert).

- For wireless security properties:
  - set the **Security Mode** (WPA2-PSK or WPA2-Enterprise).
  - set the **Encryption Protocol** to AES/CCMP.
  - enter the **PSK password** or install a **PKI certificate**.
- For pump server properties:
  - set the **Server IP/port**.
  - set the **Device Name** or **ID**.
  - set the **Device Type**.
- To verify connectivity for each infusion pump and the corresponding pump server:
  - connect the pumps to the AP (IP_Dev with **PSK**, or IP_Dev_Cert with **EAP-TLS**).
  - confirm that the pump receives an IP address from the DHCP server from the AP.
  - confirm that the pump server can discover the pumps and can display the pump status, such as **connected**, **in use**, or **offline**.

2.2.1.3 Infusion Pump Hardening

Hardening may include the following actions:

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

2.2.2 Infusion Pumps Server Systems

The summary of the infusion pump server systems that are used in this example implementation is listed in Table 2-3 below.

Table 2-3 Pump Servers Used in this Example Implementation

Vendor Name	Product Name	Operating Platform	Description
B. Braun	DoseTrac Infusion Management	Microsoft® Windows®	A drug library and infusion management system that provides real-time, infusion data reporting and analysis to add safety, efficiency, and value
Baxter	Care Everywhere Infusion Pump Management System	Microsoft Windows	Provides an interface capability to help the hospital biomedical engineering department effectively manage their infusion pump fleet. The drug library publishing module helps the hospital pharmacy effectively distribute and enforce medication safety rules.
BD	Alaris Systems Manager	Compatible with VMware® ESX® and VMware vSphere® environment	A virtual server platform that provides two-way wireless communication with Alaris PC units
Hospira	Hospira MedNet Server	Microsoft Windows	Manages drug libraries, firmware updates, and configurations of intravenous pumps

Vendor Name	Product Name	Operating Platform	Description
Smiths Medical	PharmGuard Server	Microsoft Windows	Manages drug libraries, firmware updates, and configurations of Hospira intravenous pumps for Smiths Medical Pumps

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, the installation and configuration of the database are parts of the pump server installation procedure. After the installation, we implemented a 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

The Cisco 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 Central Processing Unit (CPU): single quad core, 2.0 gigahertz (GHz) or faster
- VM with a minimum 4 GB RAM
- VM with a minimum 200 GB disk space

NCCoE installed the Cisco ISE 2.1 on a VM by using the Open Virtual Appliance (OVA) image provided by Cisco.

For your organization, follow the guidance from your VM vendor to import the OVA and to 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.

```
! 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 [******] password [******]

$5$jNPleEb4$YxDZH6oDF2Y4.02OqE/jBWxXFumRvtpe8JdNNZm1yj0 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 into the Cisco ISE Administration Portal. You will use the credentials (username and password) that 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 the Cisco ISE to the network device (AP) that you use as the authentication server during RADIUS [15] authentication:

1. Add a Network Resource.
    a. From the ISE Administration Portal, navigate to the following path: **Administration** > **Network Resources** > **Network Devices**. Select **Add**. Fill out the required parameters as indicated in the form:

i. the **name** of the network device

ii. the **IP Address** of the device with its subnet mask

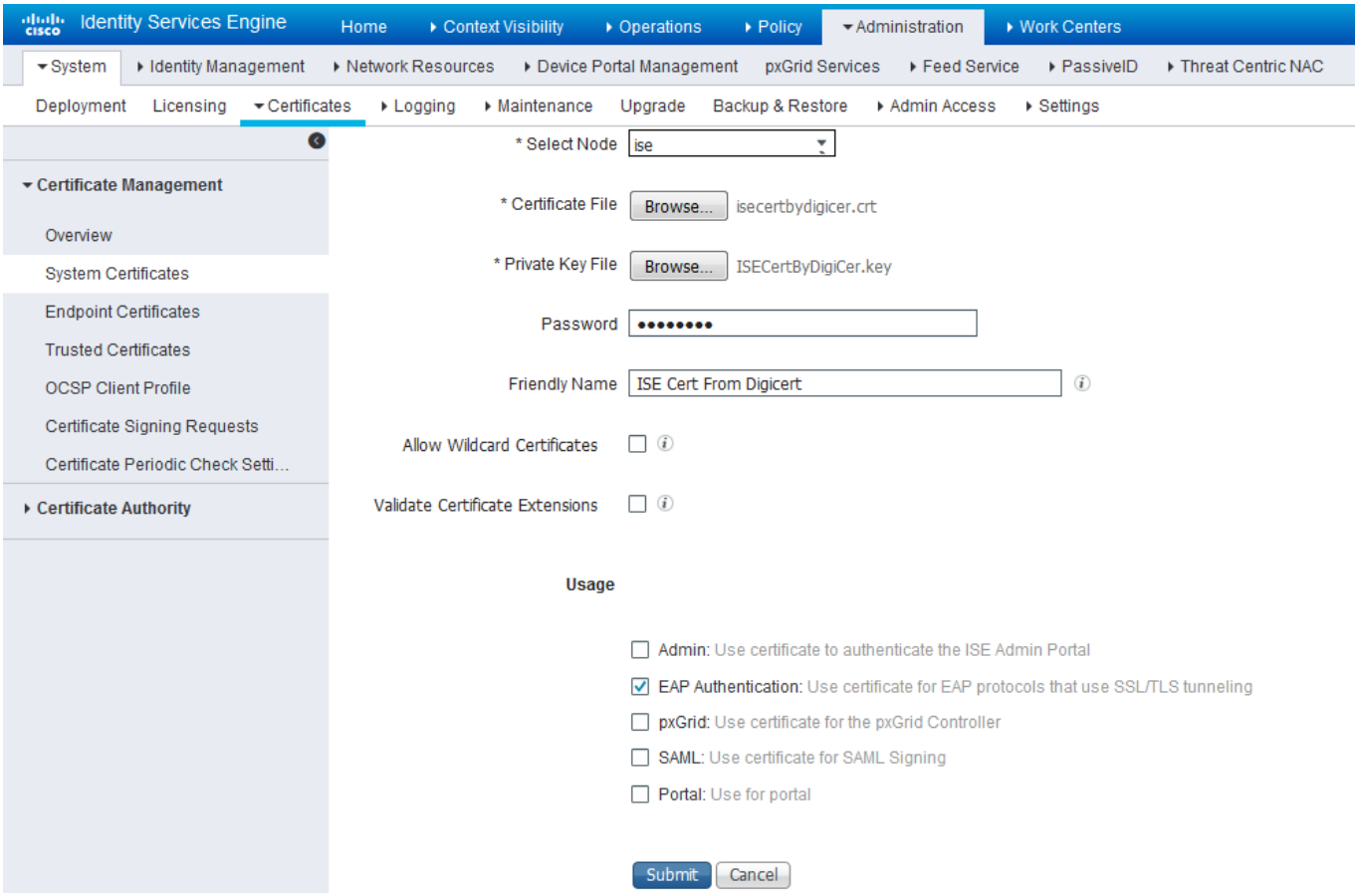
2. Select the RADIUS protocol as the selected protocol, and enter the shared secret that is configured on the network device.

3. Populate the system certificate with certificate-authority (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 Section 2.3.2.

4. Once the CA-signed certificate for the 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 following navigation path to show the installed certificates: **Administration** > **System** > **Certificates** > **System Certificates**. Select **Import** to open a screen for importing a server certificate. Fill in the required information as shown in Figure 2-1.

Figure 2-1 Importing Server Certificate



6. Under **Usage**, select the **EAP Authentication** checkbox to enable the imported certificate to be used for EAP authentication. Next, 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 following navigation path to show the installed certificates: **Administration** > **System** > **Certificates** > **Trusted Certificates**. Select **Import** to open a screen for importing the DigiCert Root CA and signing the CA individually.

    a. After importing, make sure that the certificate status is **Enabled**.

    b. Establish the Online Certificate Status Protocol (OCSP) [16] client profile from the **OCSP Client Profile** page (**Administration** > **System** > **Certificates** > **OCSP Client Profile**).

    c. If OCSP is used for **Certificate Status Validation**, check **Validate** against the **OCSP Service**, and enter the **OCSP service name**.

8. Set the **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, the Cisco ISE compares the client certificate received from the AP to verify the authenticity of a device—in this case, the infusion pump.

    a. Create a Certificate Authentication Profile:

        i. Use the Administration Portal to navigate to the following path: **Administration** > **Identity Management** > **External Identity Sources** > **Certificate Authentication Profile**. Click **Add**.

        ii. Name the profile as, for example, Cert_Auth_Profile, and 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.

    b. Select the **Identity Resource Sequence***s* tab. In the **Certificate Based Authentication**, select the **Select Certificate Authentication Profile** checkbox, and then choose **Cert_Auth_Profile** from the drop-down list.

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

    a. From the Administration Portal, navigate to the following path: **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols** > **Add**.

    b. 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 the ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. To specify the authentication policy, follow these steps:

    a. From the Administration Portal, navigate to the following path: **Policy** > **Authentication Policy** > **Type** > **Rule Based**.

    b. If Protocol is **Wireless 802.1x**, set the policy to use the **Network Device** as defined in Step 1 and the **Identity Sequences** as defined in Step 8 above.

2.3.2 DigiCert Certificate Authority

DigiCert is a cloud-based platform designed to provide a full line of Secure Sockets Layer (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 public key infrastructure (PKI) certificates for network authentication and encryption for data at rest or data in transition, if needed.

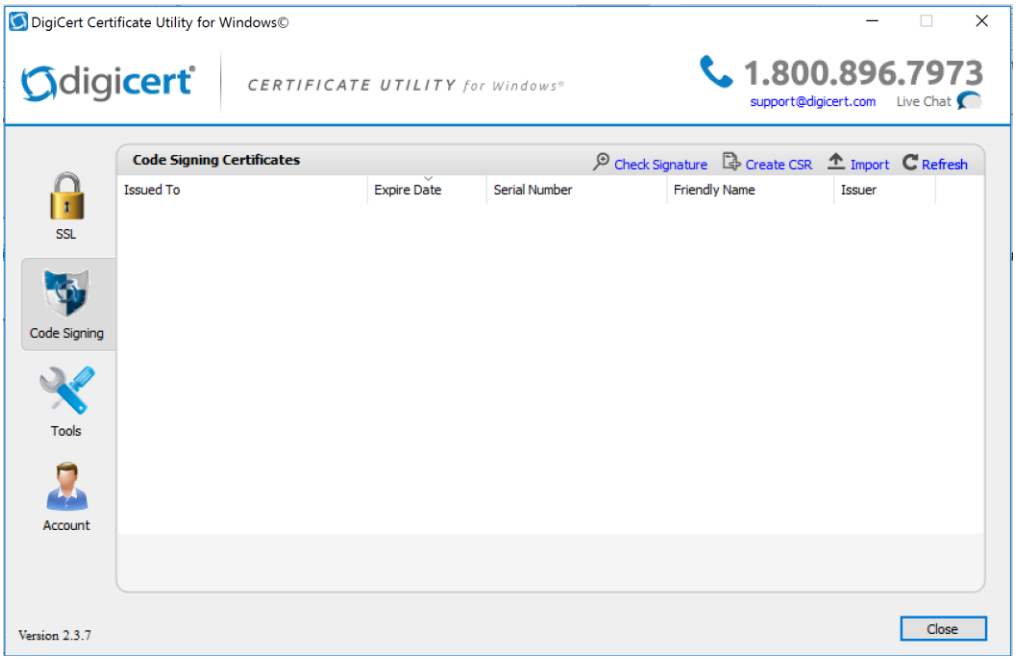
The following instruction describes the process that we used to request a PKI certificate on behalf a wireless infusion pump using the DigiCert PKI services.

2.3.2.1 Create a Certificate Signing Request

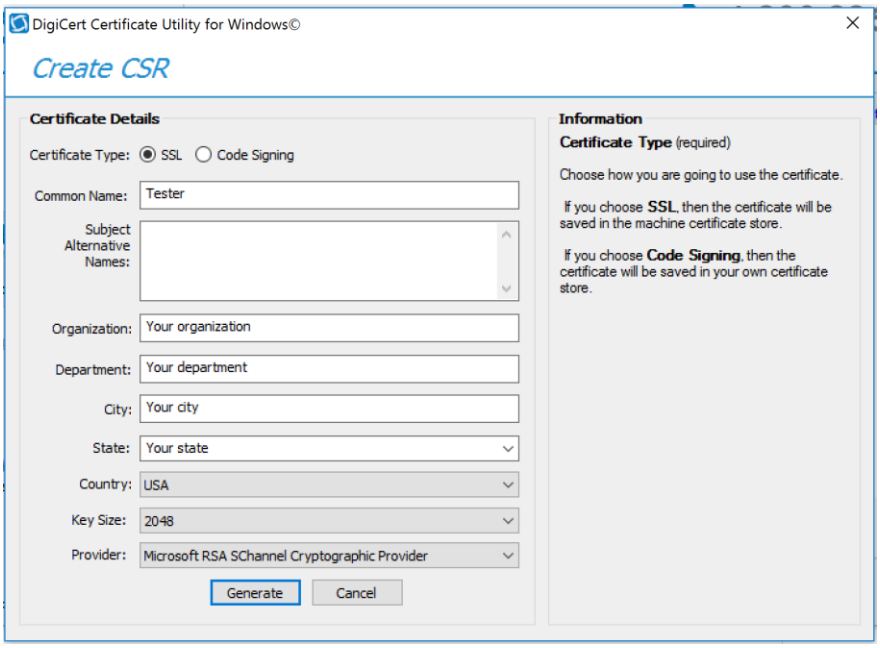
A Certificate Signing Request (CSR) can be represented as a Base64 encoded PKCS#10 binary format. Many tools and utilities are available to help generate a CSR, and the key pair containing the private key and public key is generated at the same time. The CSR identifies the applicant's distinguished name, 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.

Download and save the *DigiCertUtil.exe* from https://www.digicert.com/util/csr-creation-microsoft-servers-using-digicert-utility.htm.

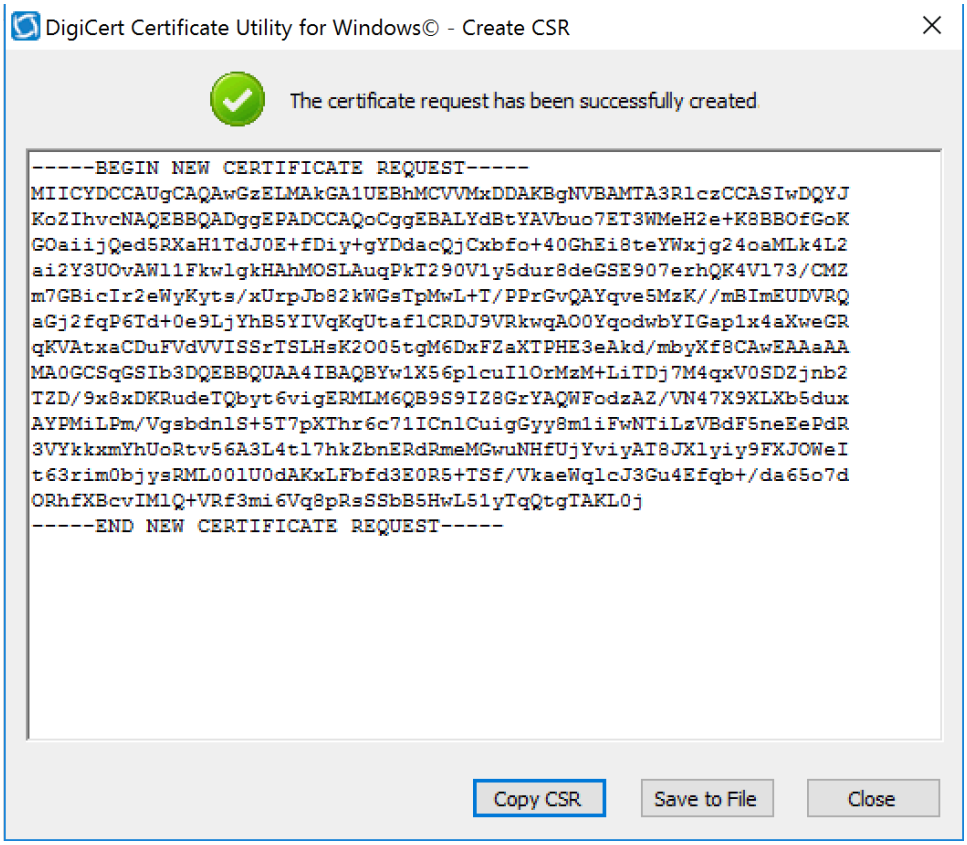
1. Double-click *DigiCertUtil.exe* to start the utility.



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



3. On the **Create CSR** window, fill in the key information (some of the information is optional).
    a. **Certificate Type**: Select **SSL**.
    b. **Common Name**: Enter the entity name.
    c. **Organization**: Enter your company's legally registered name.
    d. **City**: Enter the city where your company is legally located.
    e. **State**: Select the state where your company is legally located.
    f. **Country**: Select the country where your company is legally located.
    g. **Key Size**: Select **2048**.
    h. **Provider**: Select **Microsoft RSA SChannel Cryptographic Provider** (unless you have a specific cryptographic provider).
4. Click **Generate** to generate a CSR.



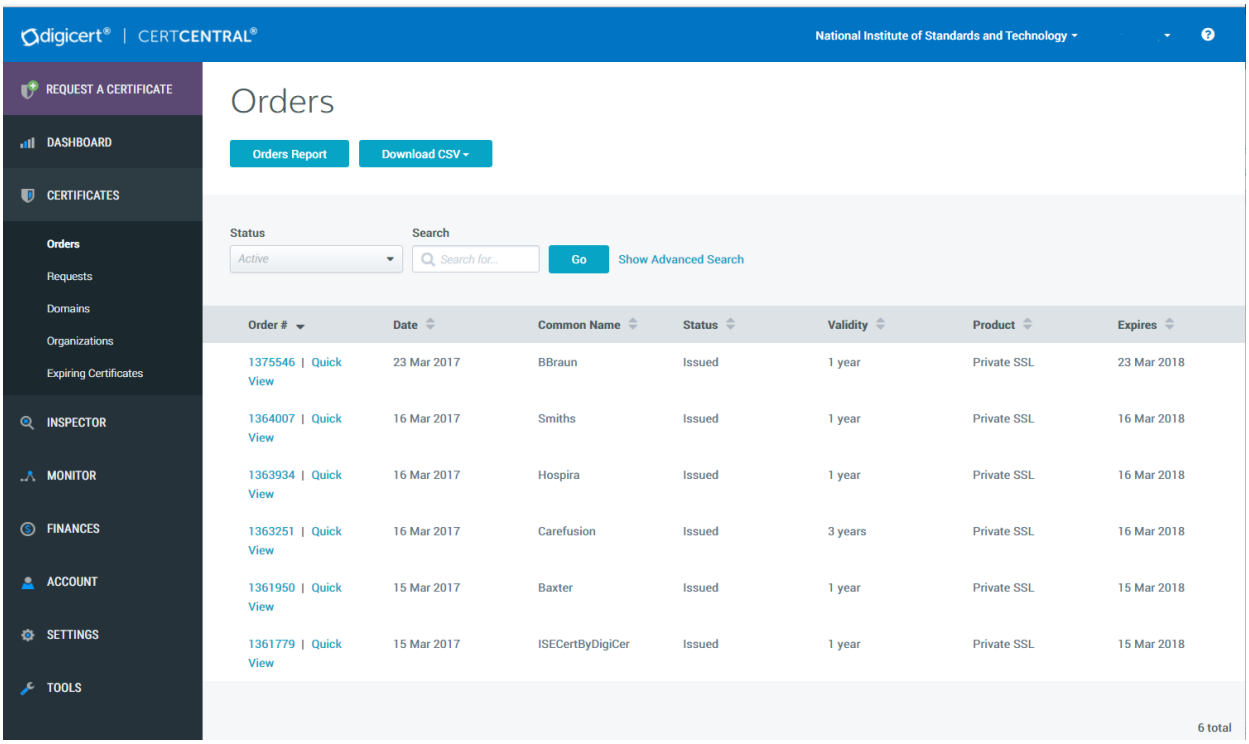
This will also generate a corresponding private key in the Windows computer from which the CSR is requested. The Certificate Enrollment Request is stored under *Console Root\Certificates(Local Computer)\Certificate Enrollment Requests\Certificates*.

2.3.2.2 Issue Signed Certificates

1. With a created applicant CSR, request a signed certificate using DigiCert CertCentral portal.
    a. Log into a DigiCert Dashboard (https://www.digicert.com/account/login.php) with your account username and password.
    b. Once in the portal, go to **Request a Certificate**, and 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**.
2. After filling in all of the required information, scroll down to the bottom of the page, and select the **I agree to the Certificate Services Agreement above** checkbox. Next, 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 privileges

to approve the request after reviewing and verifying the submitted request information if needed.

3. To download the signed certificate, go to **CERTIFICATES** > **Orders** to list the ordered signed certificates.



4. Click a specific order number to display the certificate details with a list of actions for you to perform. Click **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*, *.pem*, etc.

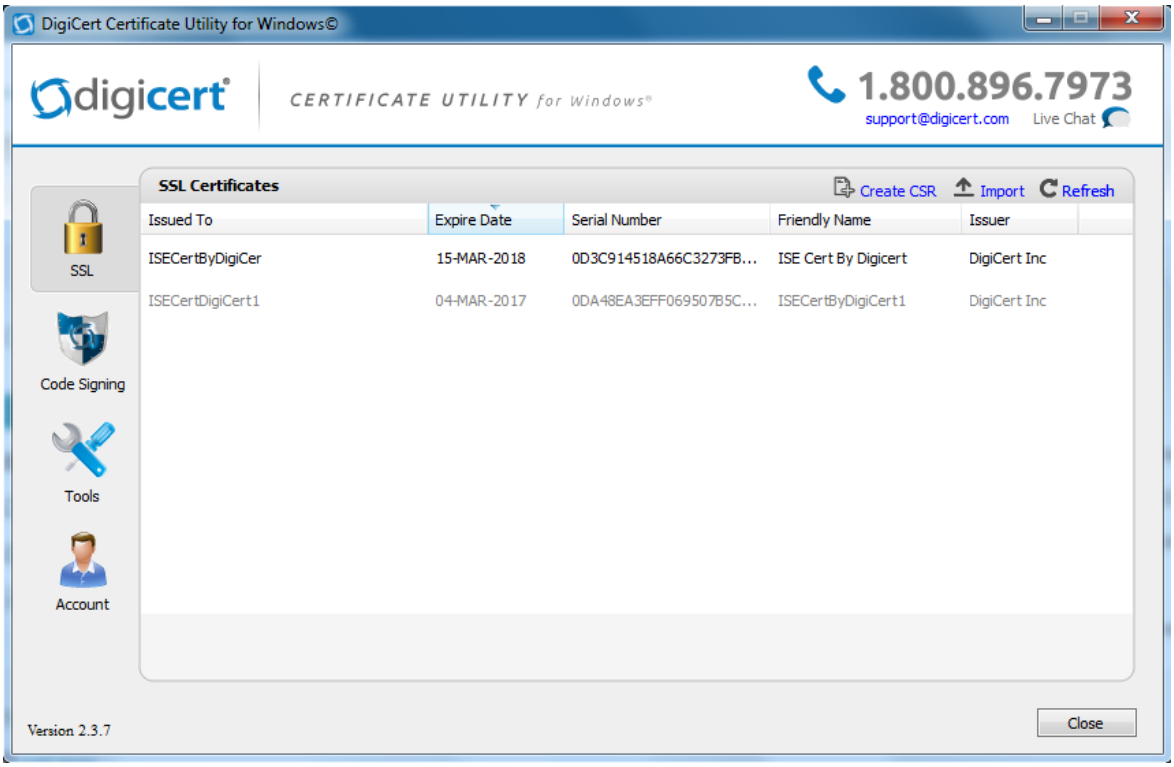
5. Save the downloaded certificate in a location where it can be used for further processing if needed.

2.3.2.3 *Import and Export the Signed Certificate*

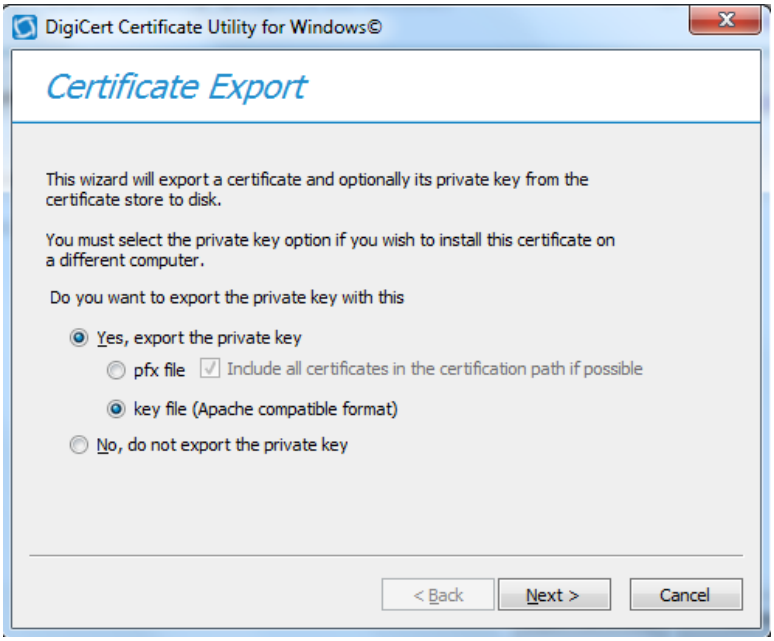
Using DigiCert Utility and the OpenSSL tool, you can further manipulate the certificates to combine with the private key and export the signed certificate, or you can convert certificates or keys into the formats specified for your organization's devices.

1. To import a signed certificate, use DigiCert Utility to click the **Import** button to load a downloaded file to the utility. The downloaded file was saved in Step 5 of Section 2.3.2.2. Click the **Next** button to import.

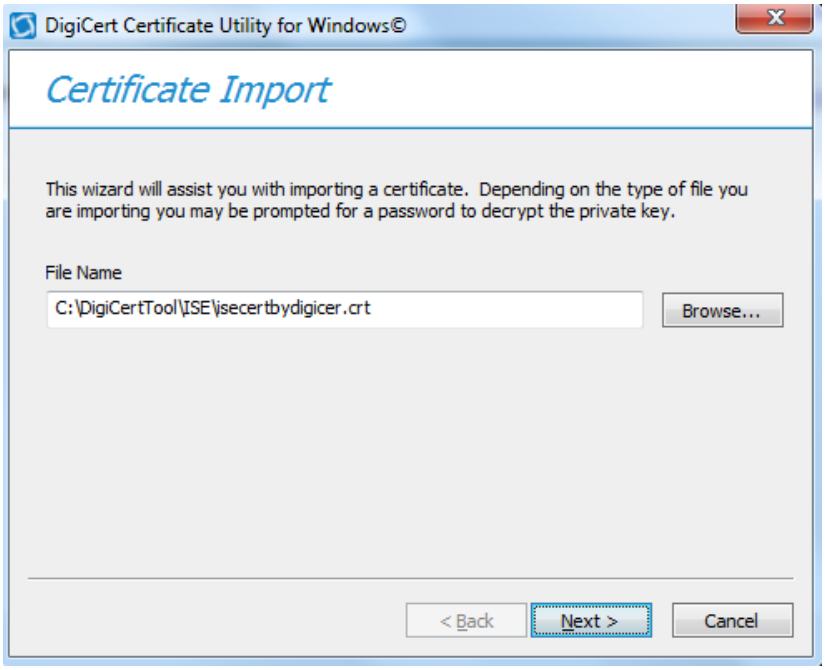
2. From the DigiCert Certificate Utility for Windows, click **SSL** to list all of the imported files.



3. 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**.



4. Click the **Next** button, and then follow the wizard instructions to save the certificate file and private key file to a desired location.



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 an open-source tool and can be downloaded from https://www.openssl.org/community/binaries.html.

Here are some of the useful convert commands:

- To convert a *.crt* file to a *.pem* file:
  - `openssl x509 -in mycert.crt -outform PEM -out mycert.pem`
- To convert a private key into *.pem* format:
  - `openssl rsa -in yourdomain.key -outform PEM -out yourdomain_pem.key`
- Separate a .pfx file into two different .key/.crt files:
  - For a key file: `openssl pkcs12 -in yourfile.pfx -nocerts -out keyfile-encrypted.key`
  - For a cert file: `openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out [certificate.crt]`
- To convert a certificate *.pem* file to a *.der* file:
  - `openssl x509 -outform der -inform DEM -in certificate.pem -out certificate.der`
- To convert a key *.pem* file to a .der file:
  - `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:

1. DCS:SA
2. SEP Manager Server
3. Advanced Threat Protection: Network (ATP:N)

Each of these Symantec products protects components in the enterprise systems, at different levels.

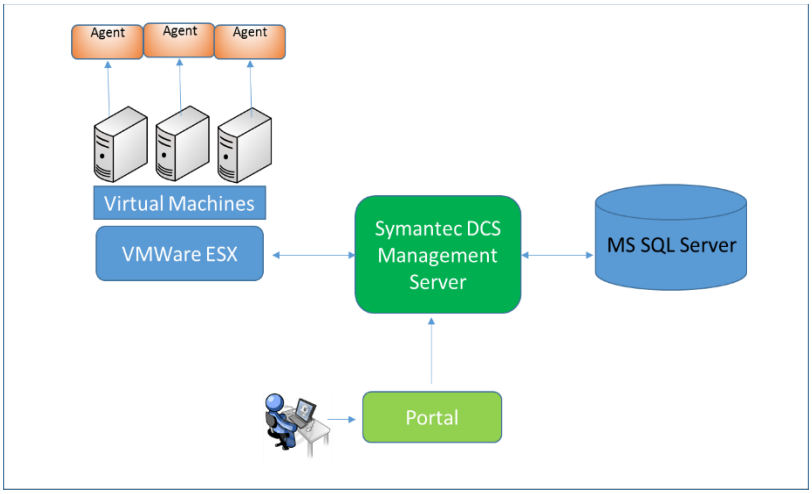
2.4.1 Symantec Data Center Security: Server Advanced

For data center security, DCS:SA provides a policy-based approach to endpoint security and compliance. DCS:SA 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 device. Figure 2-2 displays the DCS:SA environment.

Figure 2-2 DCS:SA Environment



2.4.1.1 *Installing DCS:SA Manager*

Minimum hardware requirements:

- hardware support x86, EM64T, and AMD64, with 60 GB free disk space (all platforms)
- 8 GB RAM
- four CPUs

Minimum software requirements:

- Windows Installer 2.0 or higher
- Microsoft Structured Query Language (SQL) Server 2008
- .NET Framework 4.0 or 4.5.1
- PowerShell 2.0
- Windows 2008 or later

Operating the Symantec DCS:SA 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 DCS:SA Manager.

Follow these steps to install the SQL Server software.

1. Use *SCSP* as the default instance name.
2. Set the 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 by using SQL Server credentials.
5. Register the instance. Registering the instance also starts the instance.

Follow these steps to install DCS:SA:

1. Double-click *server.exe*. Next, in the **Welcome** panel, click **Next**, and accept the license agreement.
2. In the **Installation Type** panel, click **Evaluation Installation**, 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.

See the *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 MP1 Planning and Deployment Guide* [17] for further details.

2.4.1.2 Configuration of DCS:SA 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. Log into 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** folder.
8. 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**.
9. To edit a policy, right-click a policy, and then click **Edit Policy**. Configure the setting based on your security protection needs.

DCS:SA provides a variety of configurable protection from application data protection, to 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 of 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**.
3. In the **Select a Prevention Policy Builder** wizard, in the **New Policy Builder** section, click **Launch**.
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** textbox, enter a name for the policy that you create. In this build, we use the following name: Windows Prevention Policy 6.0 Reference 31 Protected Whitelisting strategy.
6. Select the **Create a custom prevention policy** checkbox, 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**. 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**. 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 DCS:SA 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 the **I accept the terms in the license agreement** checkbox, 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 the **Enable Intrusion Prevention** checkbox is selected.
6. 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.
7. (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.
8. 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.
9. In the **Management Server Configuration** panel, click **Next**.
10. (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.

11. In the **Agent Group Configuration** panel, click **Next**.
12. In the **Service User Configuration** panel, accept the default **Local System** account, and then click **Next**.
13. In the **Ready to Install the Program** panel, confirm the installation parameters, and then click **Install**.
14. 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
- creating agent registration groups

See the *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 MP1 Planning and Deployment Guide* [17] for details.

2.4.2 Symantec Endpoint Protection Manager

Minimum hardware requirements:

- 2 GB RAM (minimum 8 GB or more recommended)
- 40 GB hard drive (minimum, 200 GB recommended) for the management server and database with a remote SQL Server database

Minimum software requirements:

- Windows Installer 2.0 or higher
- Microsoft SQL Server 2008
- .NET Framework 4.0 or 4.5.1
- PowerShell 2.0
- Windows 2008 Server or later

Intel Pentium Dual-Core or equivalent (minimum, 8-core or greater recommended)

SEP 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 SEP Manager

1. Download the product, and 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 instructions, and accept the license agreement.
3. Continue the installation until it is finished. After the initial installation completes, configure the server and database.
4. Click **Next**. The Management Server Configuration Wizard starts.
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 that 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 SEP Manager configuration.

2.4.2.2 Installing the Client

After installing SEP Manager, install the SEP 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. To install the SEP client, follow these steps:

1. Make your configuration selections as you install SEP Manager, and then create the client installation packages.
2. Save the installation package to a folder on the computer that runs SEP 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: Network

With ATP:N installed on the network, it can provide network-based protection of medical device subnets via monitor internal inbound and outbound internet traffic. Integrating Symantec ATP:N with SEP will

allow ATP:N to monitor and manage all network traffic from the endpoints and to provide threat assessment for dangerous activity to secure the medical devices on an enterprise network.

Minimum hardware requirements:

- 32 GB RAM
- four CPUs
- 500 GB hard drive (minimum)

Minimum software requirements: ESXi 5.5 and 6.0, ATP:N 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. Sample installation steps are listed 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 ATP:N 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 log on with the username *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 ATP:N Manager using the ATP:N IP address. The username is *setup*, and the password is *Symantec*.

2.4.3.2 Integrating ATP:N with SEP

Integrating Symantec ATP:N with SEP allows for the correlation of event data from SEP Manager to ATP:N. To do the integration, follow these steps:

1. On SEP Manager, prepare the database for log collection to allow ATP:N to access the database using DB administrator (sa) credentials.
2. Enable the **Symantec Endpoint Protection Correlation** option by selecting the checkbox the **Settings** > **Global** > **Synapse** area of ATP:N Manager.
3. In ATP:N Manager, configure the connection to SEP Manager instances.
4. In SEP Manager, configure host integrity and quarantine firewall policies, if not already enabled.
5. In SEP Manager, configure endpoints to send information to the ATP:N management node.

6. In ATP:N Manager, add SSL certificates for secure communication between endpoints and ATP:N, if needed.

More detail about integrating Symantec ATP:N and SEP can be found from the following reference: http://help.symantec.com/cs/ATP_2.2/ATP/v102658999_v117970559/About-integrating-ATP-with-Symantec-Endpoint-Protection?locale=EN_US.

2.5 Risk Assessment Tools

2.5.1 PFP Device Monitoring System: pMon 751 and P2Scan

The NCCoE lab deployed a PFP Monitoring System consisting of a pMon 751 appliance and the P2Scan analytics tool. The PFP system provides integrity assessment and intrusion detection by utilizing an external out-of-band channel (i.e., electromagnetic radiation or instantaneous power consumption), which are unintended emissions also known as *side-channels*. PFP takes fine-grained measurements of the device's side-channels to identify unique patterns created by the specific logic execution.

The pMon 751 appliance captures the side-channel signals by using a physical sensor, and sends them to P2Scan to be processed.

The P2Scan analysis tool collects data during controlled execution and uses it to build a baseline of authorized execution during a tool training phase. Once tool training is completed, P2Scan continuously monitors the device for deviations from the baseline to determine whether unauthorized execution, such as a malicious intrusion, has occurred.

Hardware requirements:

- pMon 751 data acquisition module
- Electromagnetic (EM) probe (Aaronia Magnetic Direction Finder [MDF])
- 12 Volts Direct Current (VDC) Power Supply
- SMA (SubMiniature version A) cables to connect probe
- Secure Digital (SD) card

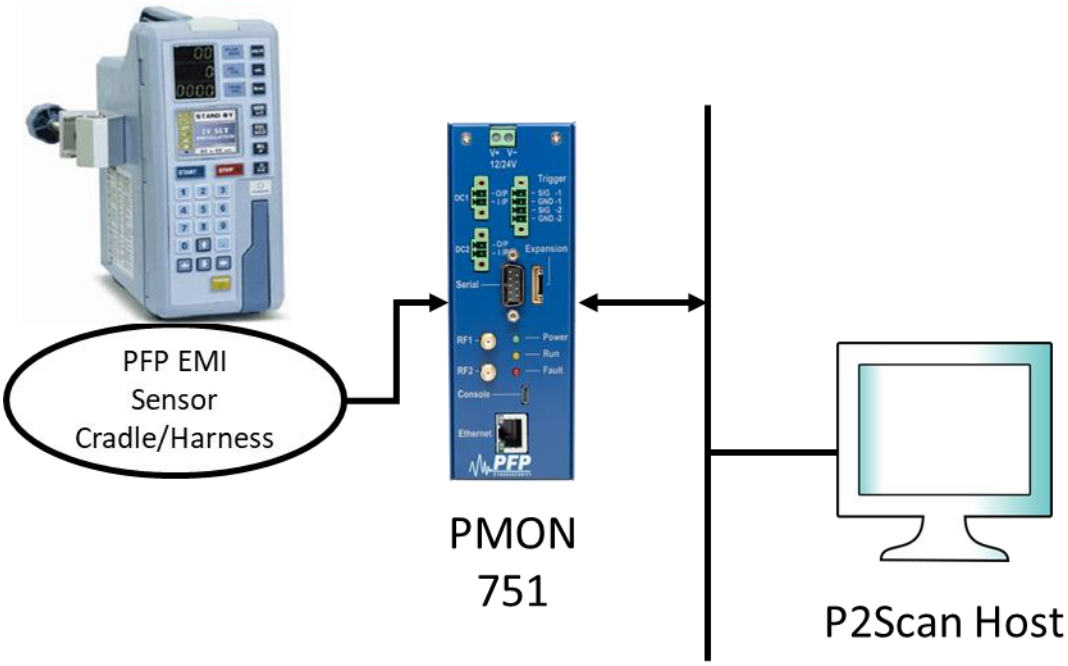
Host computer requirements:

- Operating system: Windows 10 Professional x64
- RAM: 16 GB or higher strongly recommended
- Hard drive: 1 GB of free space
- Ethernet connection
- hardware setup

The EM loop probe is sensitive to changes in the magnetic fields produced by the pump or the device under test (DUT). The intensity and signal structure of radiated magnetic fields from a device are typically spatially dependent. The probes must also be stationary during all tests, as P2Scan is highly sensitive in detecting changes in the radiated fields emitted from a device, which could alter data capture and analysis during the Data Collection and Baseline Extraction phases. A consistent EM probe placement using a cradle or harness is critical for the correct operation of the system.

The reference setup of the PFP Monitoring System is shown in Figure 2-3.

Figure 2-3 PFP Monitoring System Reference Setup



The following connections on the pMon 751 are required:

- 12 to 24 Volt DC on Terminal 1 of power block
- GND on Terminal 2 of power block
- EM probe on the **Signal** input SMA connector
- connection to Ethernet network to reach host computer running P2Scan (By default, pMon is set with the static IP address 172.16.1.93.)
- (optional) trigger signal on the trigger input

2.5.1.1 P2Scan Setup

The P2Scan installer will install P2Scan as well as the required dependencies. Launch the setup.exe file from the installation media (typically USB drive).

P2Scan uses a single project file to control the operation of P2Scan. As the user makes changes to the configuration parameters they will have the options to save the changes to the project file.

The project file is in the .ini (initialization) file format.

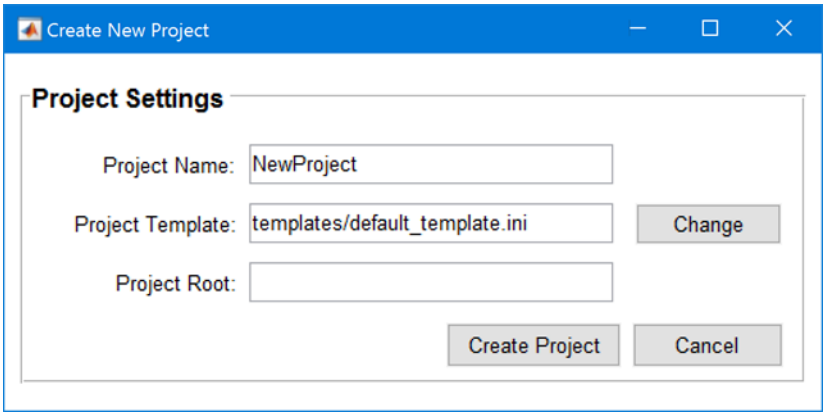
2.5.1.2 Operating P2Scan

1. Launch P2Scan. This will open the application home page, where it allows you to create a new monitoring project or to load an existing project (Figure 2-4).

Figure 2-4 P2Scan Home Page

a. To create a new project, click the **New Project** button on the home page (Figure 2-4). This will open the Create New Project window (Figure 2-5). You can change the **Project Name** (alters .ini name), the **Project Template** (select an .ini template to use), and the **Project Root** (creates a new directory to store the project). Once you have completed these fields, click **Create Project**.

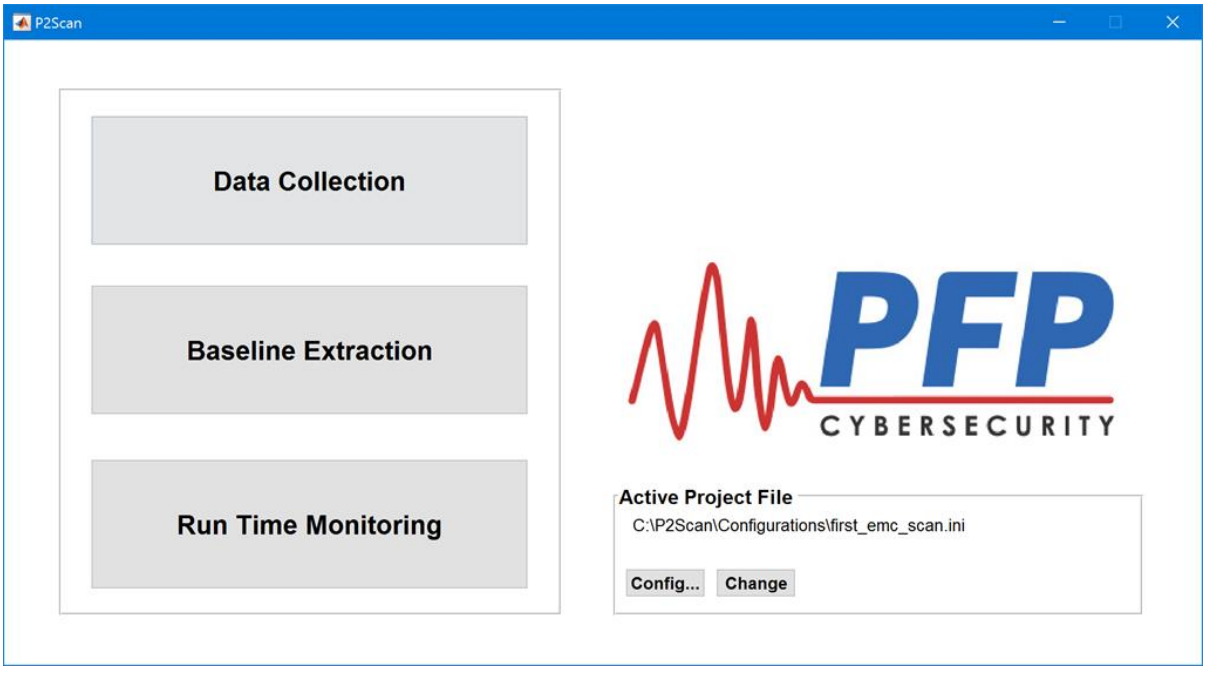
Figure 2-5 New Project Creation



2. Once a project (new or existing) has been created, click **Load Project** on the home page (Figure 2-4). Navigate to the directory specified in **Project Root**, and select the .ini file that you created, which holds default values for guiding P2Scan.

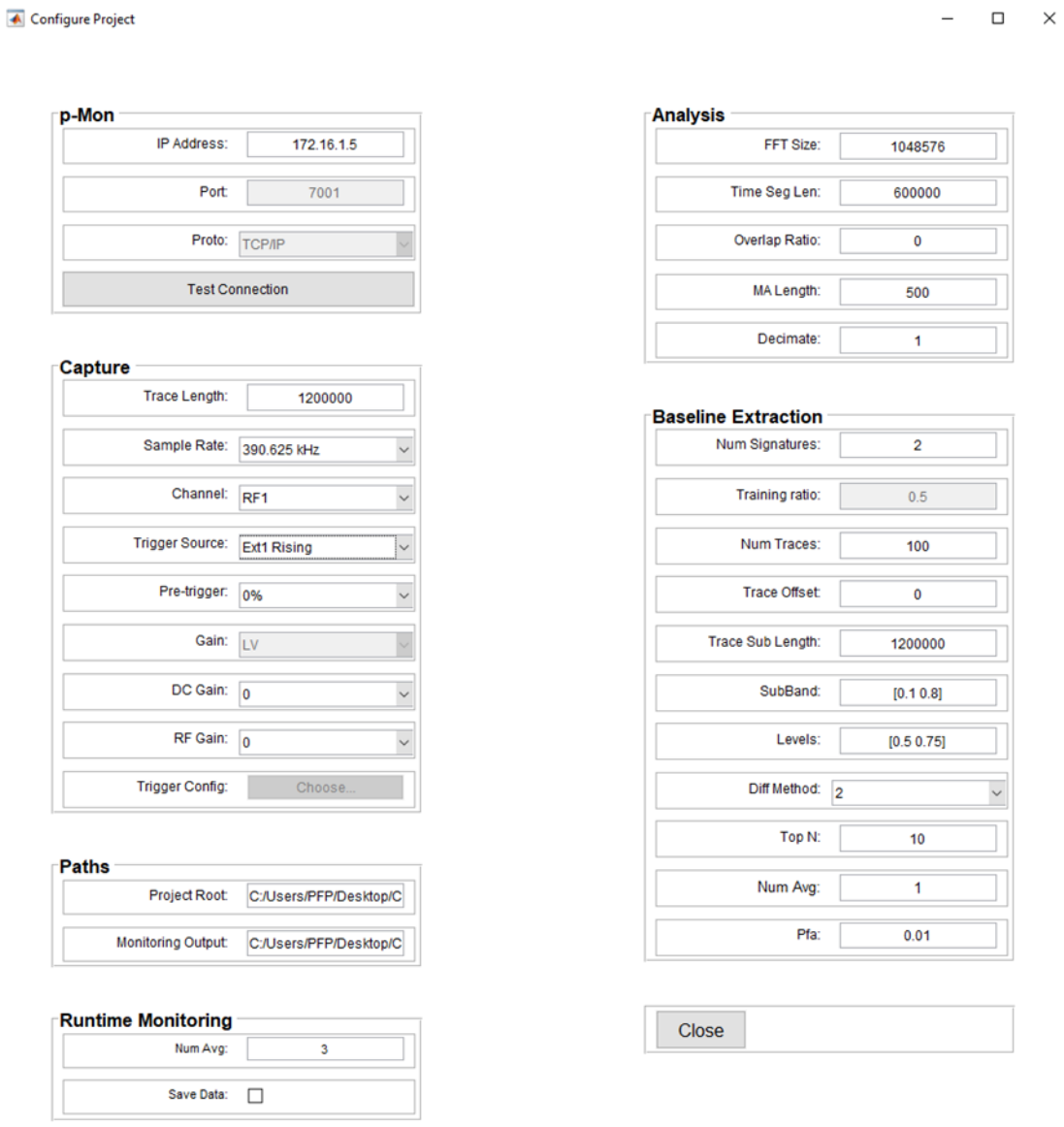
3. Once the configuration file is loaded, P2Scan shows the main screen (Figure 2-6). The user should see the path of their project file in the **Active Project File** dialogue box. To select a different file, click the **Change** button.

Figure 2-6 P2Scan Main Screen



4. Once the *.ini* file is selected, click Config to open the **Configure Project** screen with default parameters provided by the *.ini* file (Figure 2-7). The user can proceed to test their setup through pMon or modify the settings before entering the main program. For a detailed description of the different analysis parameters and their impact on the final result, please refer to the P2Scan User Manual.

Figure 2-7 P2Scan Configuration Parameters



2.5.1.3 Collection Process

The initial step in the PFP analysis process is to repetitively sample waveforms for each of the execution paths that are of interest to the user. These waveforms will ultimately form a bank of trusted references from which all unknown traces will be compared against to determine their validity during runtime monitoring.

P2Scan interfaces with the pMon digitizing hardware. P2Scan provides a **Capture** interface (under **Settings** in Figure 2-8), which allows the user to configure the sampling parameters used by P2Scan.

This graphical user interface provides the user with the sampling parameters that may be adjusted for the collection system being used. Once the settings have been entered, click the **Acquire Trace** button to collect a sample trace and to view the results. The current data buffer will be displayed as shown in Figure 2-8, but will not be saved for analysis.

After the capture parameters have been configured, select the **Start Capture** button to begin the data capture process. As data collection executes, the raw waveforms will be displayed on the screen, along with the percentage-complete indicator, as shown in Figure 2-8.

Figure 2-8 Data Collection Screen During Capture

Data collection will enable a supervised tool training approach and will pause between run states. Each run state becomes a label during the tool training process. An example run state could be a specific configuration on the infusion pump or a specific version of firmware. The number of pause(s) is dependent on the number of paths in the capture settings prior to collecting data. Change to the next state, and click **OK** to continue collecting data. Repeat the process until **Data Collection** is 100% complete.

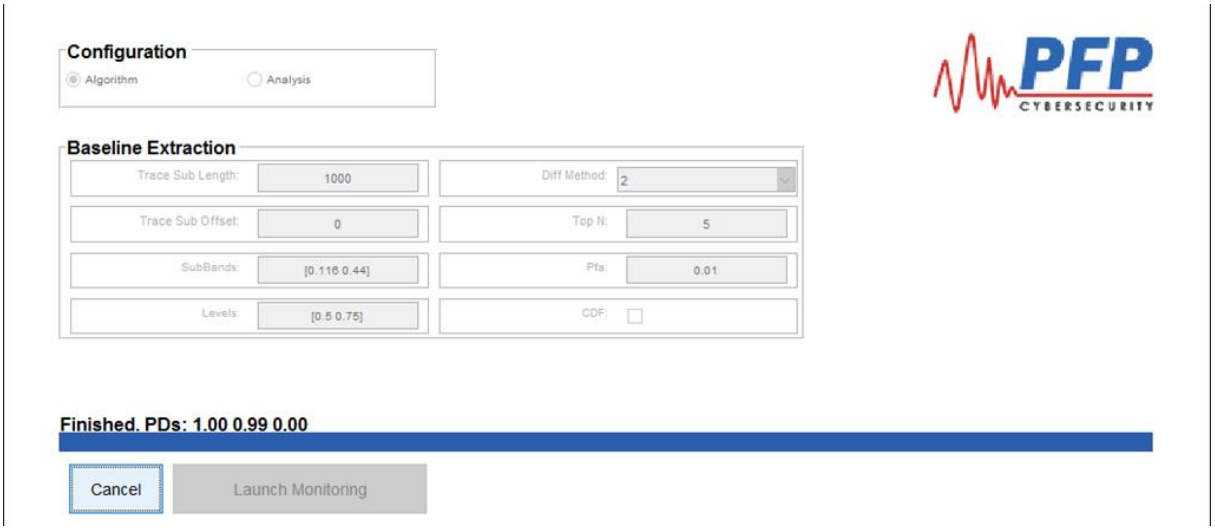
2.5.1.4 Baseline Extraction (Tool Training)

Once the data for all of the states has been collected, the next step is to train the system, for baseline extraction. The user has control over several analysis parameters during the Baseline Extraction phase. Several operational characteristics of the device being monitored can affect how to adjust the analysis parameter in order to achieve the desired results. For a detailed description of the different analysis parameters and their impact on the final system, please refer to the P2Scan User Manual.

The baseline analysis is launched by pressing the **Start** button. The status window will be updated with the current status. Depending on the complexity of the DUT, and the processing power of the host machine, the baseline extraction may take time to run.

After the Baseline Extraction phase has been completed, P2Scan will display the Percentage of correct Detection (PD) (Figure 2-9), which is calculated by comparing the sets of evaluation data to their respective baseline. The closer that the value is to 1, the better the ability of the system to discriminate that set of data. The detection statistics will be shown in the status bar, and, once complete, the user can click **Launch Monitoring** to enable runtime monitoring.

Figure 2-9 Completed Baseline Extraction Screen



2.5.1.5 Runtime Monitoring

Once the necessary baselines have been calculated during tool training, P2Scan is able perform runtime monitoring of devices that have been previously characterized. The runtime monitor compares the test signals captured by the appliance, and compares them against the baselines. If the test device is executing one of the states used during training, P2Scan will classify the signal and provide a visual indication, using distinct colors to signify different device execution paths, as shown in Figure 2-10. The straight, thick black line signifies the threshold created from the Baseline Extraction phase.

Figure 2-10 Runtime Monitoring Showing the Execution of Four Different States

If the software on the DUT changes to an unrecognized state, P2Scan will not be able to classify the test trace with the required confidence level, and will determine that an anomaly has occurred. In this case, P2Scan will show test results above the threshold, in a separate color from the successful states, as shown in Figure 2-11.

Figure 2-11 Runtime Monitoring Showing an Anomalous State

If the **Save Data** checkbox is selected (under **Runtime**), then the monitoring outputs shall be saved in a file in the directory specified by "**Monitoring Output**." This file displays the date/time of the monitoring, and the TestStat, which shows statistical error distances between analyzed data and the DUT. Sample file output is shown in Figure 2-12. If desired, the monitoring outputs can be sent to a Security Information and Events Management (a SIEM tool) via syslog.

Figure 2-12 Sample Contents Saved in the Runtime Results File

```
Time=2015/11/19 16:19:25.095, PathID=1, TestStat=0.51952
Time=2015/11/19 16:19:25.593, PathID=1, TestStat=0.651472
Time=2015/11/19 16:19:26.098, PathID=1, TestStat=0.725039
Time=2015/11/19 16:19:26.598, PathID=1, TestStat=0.852453
Time=2015/11/19 16:19:27.107, PathID=1, TestStat=0.981368
Time=2015/11/19 16:19:27.609, PathID=1, TestStat=0.789816
Time=2015/11/19 16:19:28.110, PathID=1, TestStat=0.71154
Time=2015/11/19 16:19:28.613, PathID=1, TestStat=0.620868
Time=2015/11/19 16:19:29.120, PathID=1, TestStat=0.615049
Time=2015/11/19 16:19:29.631, PathID=1, TestStat=0.574909
Time=2015/11/19 16:19:30.137, PathID=1, TestStat=0.57405
Time=2015/11/19 16:19:30.642, PathID=1, TestStat=0.47717
Time=2015/11/19 16:19:31.160, PathID=1, TestStat=0.501458
Time=2015/11/19 16:19:31.663, PathID=1, TestStat=0.737632
Time=2015/11/19 16:19:32.172, PathID=1, TestStat=0.780725
Time=2015/11/19 16:19:32.692, PathID=1, TestStat=0.826027
Time=2015/11/19 16:19:33.195, PathID=1, TestStat=0.833921
Time=2015/11/19 16:19:33.700, PathID=1, TestStat=0.669008
Time=2015/11/19 16:19:34.206, PathID=1, TestStat=0.518836
Time=2015/11/19 16:19:34.712, PathID=1, TestStat=0.539068
Time=2015/11/19 16:19:35.232, PathID=1, TestStat=0.498789
Time=2015/11/19 16:19:35.737, PathID=1, TestStat=0.468708
Time=2015/11/19 16:19:36.243, PathID=1, TestStat=0.5328
Time=2015/11/19 16:19:36.752, PathID=1, TestStat=0.305793
Time=2015/11/19 16:19:37.260, PathID=1, TestStat=0.178354
Time=2015/11/19 16:19:37.768, PathID=1, TestStat=0.285738
```

2.5.2 Clearwater IRM|Analysis™ Software

We used the Clearwater IRM|Analysis™ Software-as-a-Service (SaaS) application, a control-based risk tool for conducting a risk assessment focused on the 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" that creates, maintains, receives, or transmits electronic 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:

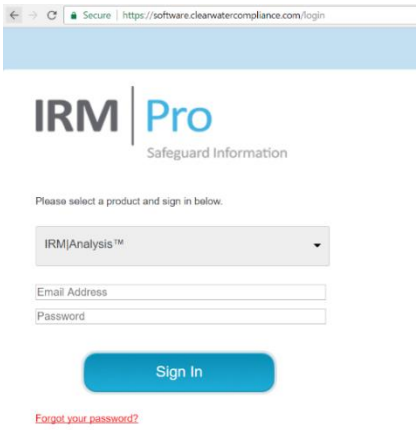
1. Log into IRM|Analysis.
2. Import **Inventory of Information Assets**, or enter the data through the **Asset Inventory Form**.
3. Establish conformance with the NIST-based Security Controls.
4. Determine the **Risk Rating** of the likelihood and impact.
5. Identify those risks that exceed the established **Risk Threshold**.

6. Document the **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.

2.5.2.1 Login to IRM|Analysis

1. Open a browser, and navigate to https://software.clearwatercompliance.com/login.
2. On the login page (Figure 2-13), enter the appropriate **Email Address** and **Password**.
3. Click the **Sign In** button.

Figure 2-13 IRM|Analysis Login Page



2.5.2.2 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 VMs using the same Storage Area Network and identical operating systems. If 10 assets are similarly configured using the same server, then the 10 assets can be grouped and evaluated as one asset. The Media/Asset Group is the logic group for organizing media into classes to reduce the number of identical security control assessments.

Follow these steps to add a new asset:

1. On the IRM|Analysis tool, expand **Assets** on the left menu bar.
2. Under **Assets**, click **Asset Inventory List**.
3. On the **Asset Inventory List** page (Figure 2-14), click the **New** button.

4. On the **New Asset** form (Figure 2-15), enter the required information, and then click **Save**.

Figure 2-14 Asset Inventory List

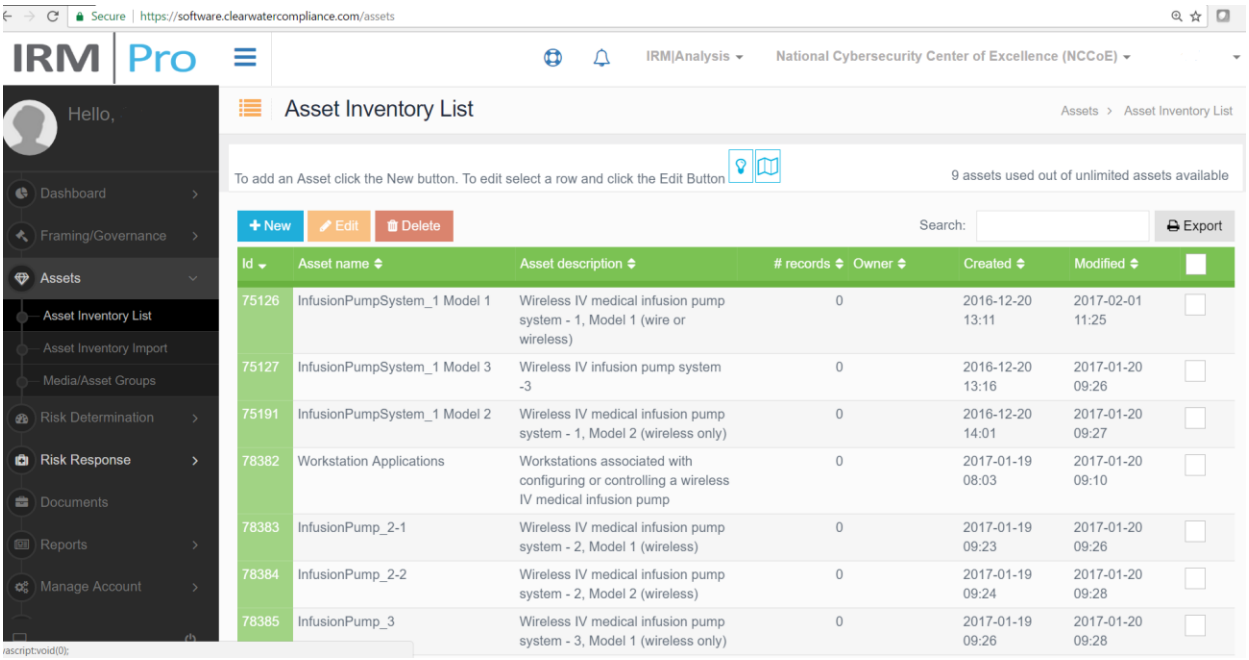
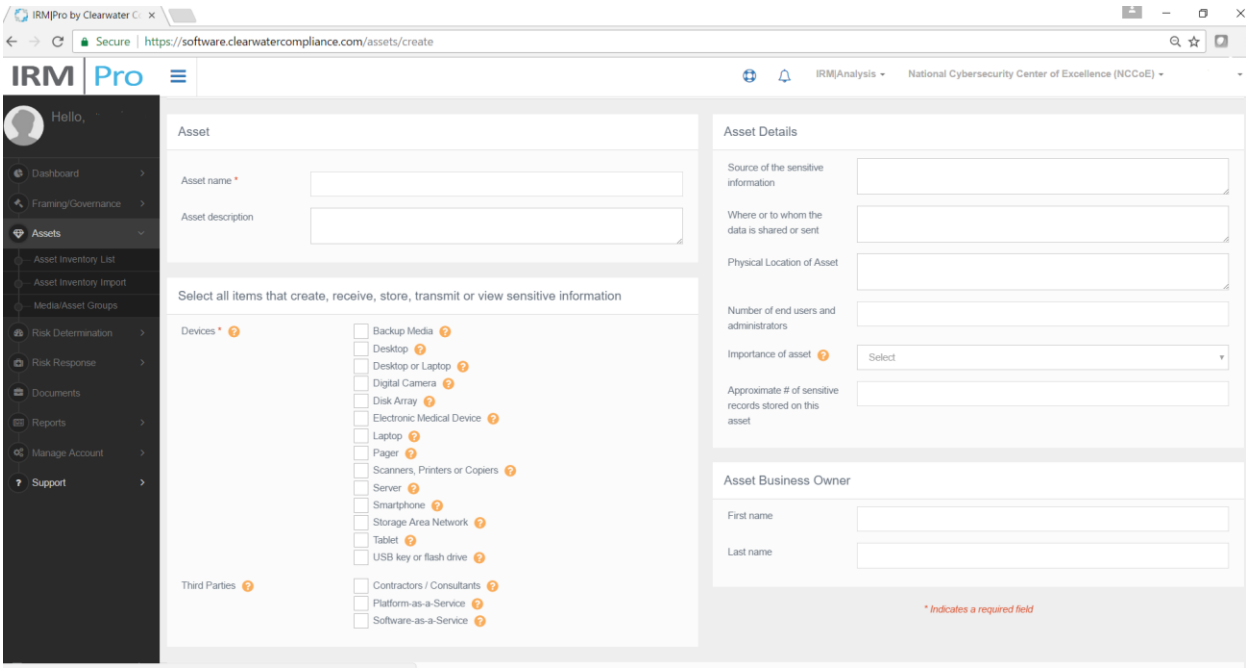


Figure 2-15 New Asset



Follow these steps to update an asset:

1. On the IRM|Analysis tool, expand **Assets** on the left menu bar.
2. Under **Assets**, click **Asset Inventory List**.
3. On the **Asset Inventory List** page (Figure 2-14), select the asset that you want to edit by clicking the checkbox next to that asset, and then click **Edit**.
4. On the **Edit Media/Asset Groups** page (see Figure 2-17 below), enter the necessary information, and then click **Save**.

Follow these steps to view and manage media/asset groups:

1. On the IRM|Analysis tool, expand **Assets** on the left menu bar.
2. Under **Assets**, click **Media/Asset Groups**.
3. On the **Media/Asset Groups** page (Figure 2-16), scroll up and down to view the groups, and edit a group by clicking the **Edit** button next to that group.
4. On the **Edit Media/Asset Groups** page (Figure 2-17), enter the necessary information, and then click **Save**.

Figure 2-16 Media/Asset Groups

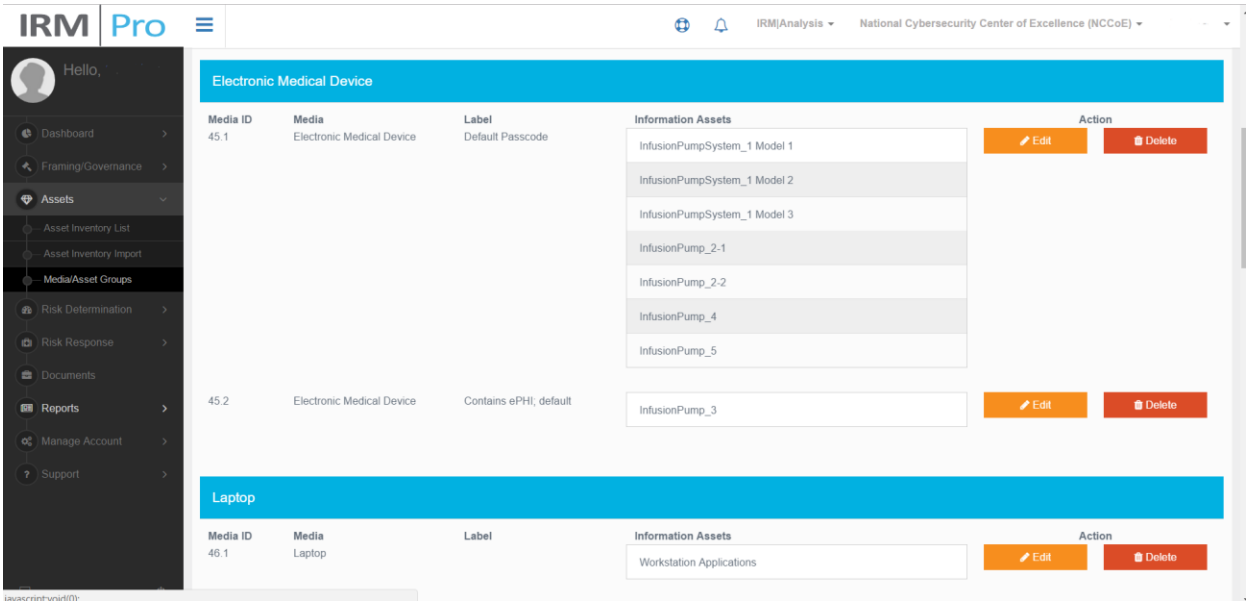
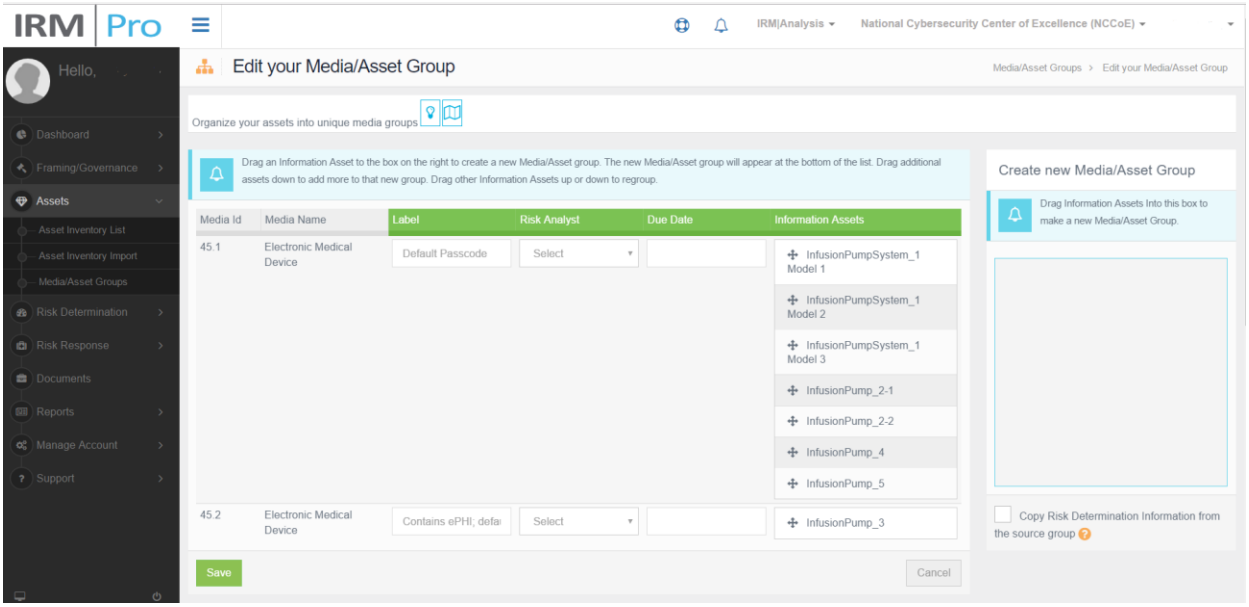


Figure 2-17 Edit Media/Asset Group



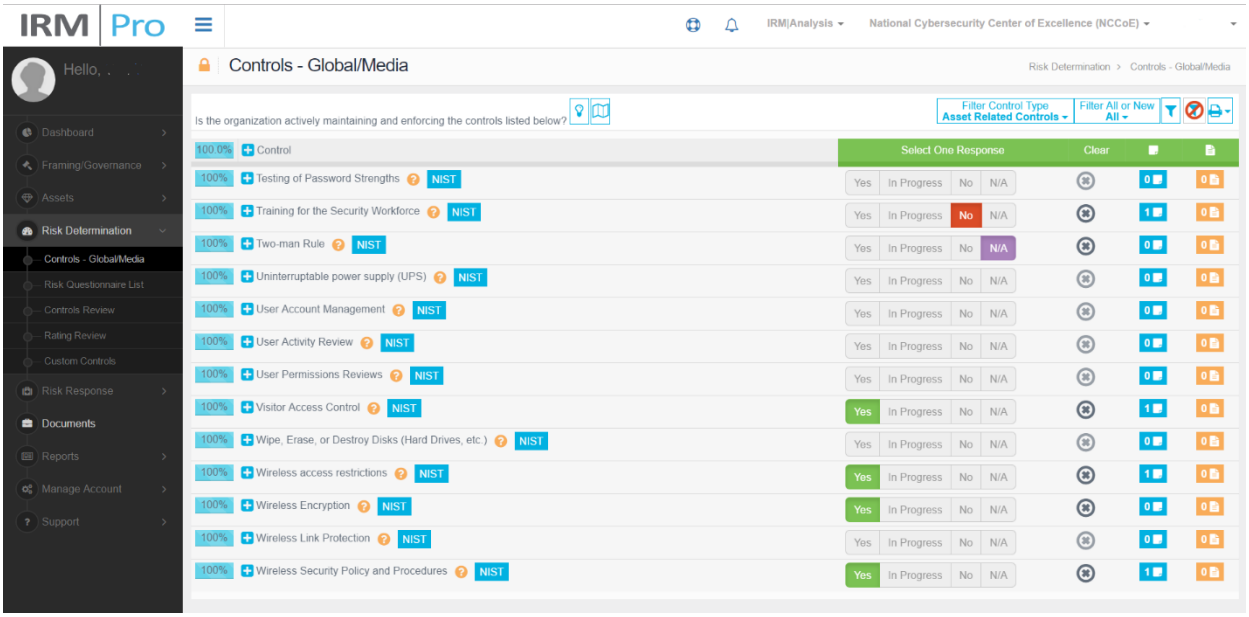
2.5.2.3 *Risk Determination*

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

Follow these steps to use the Risk Determination at the Global/Media level:

1. On the IRM|Analysis tool, expand **Risk Determination** on the left menu bar.
2. Under **Risk Determination**, click **Controls – Global/Media**.
3. On the **Controls – Global/Media** page (Figure 2-18), scroll up and down to view the controls. For each control, select one of the responses (i.e., **Yes**, **In Progress**, **No**, or **N/A**) to indicate the response status.

Figure 2-18 Controls – Global/Media



Follow these steps to use the Risk Determination at the Media/Asset Group level:

1. On the IRM|Analysis tool, expand **Risk Determination** on the left menu bar.
2. Under **Risk Determination**, click **Risk Questionnaire List**.
3. On the **Risk Questionnaire List** page (Figure 2-19), 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 then click the **Continue** button to access the **Risk Questionnaire Form** (Part 1: Figure 2-20, and Part 2: Figure 2-21).
5. For each control, select one of the responses (i.e., **Yes**, **In Progress**, **No**, or **N/A**) to indicate the response status (example shown in Part 1: Figure 2-20), 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 that 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**, as only a subset of assets may undergo a user activity review.
7. Determine and select the **Risk Likelihood** and **Risk Impact** for the selected risk scenario (example shown in Part 2: Figure 2-21) to populate the **Risk Rating**.

8. You may select the question mark (**?**) for more information on the control, and the **NIST** button for a quick reference to NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*.

Figure 2-19 Risk Questionnaire List

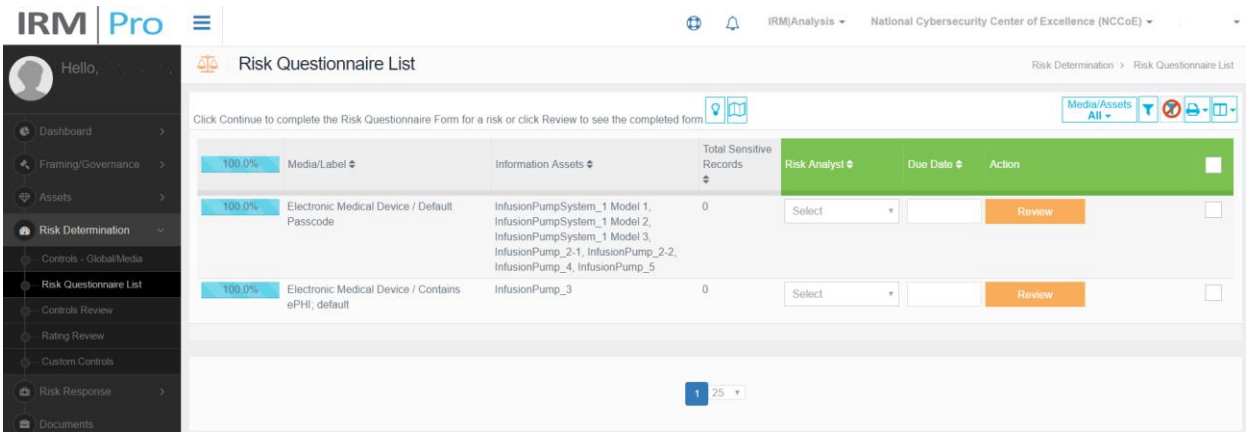


Figure 2-20 Risk Questionnaire Form (Part 1)

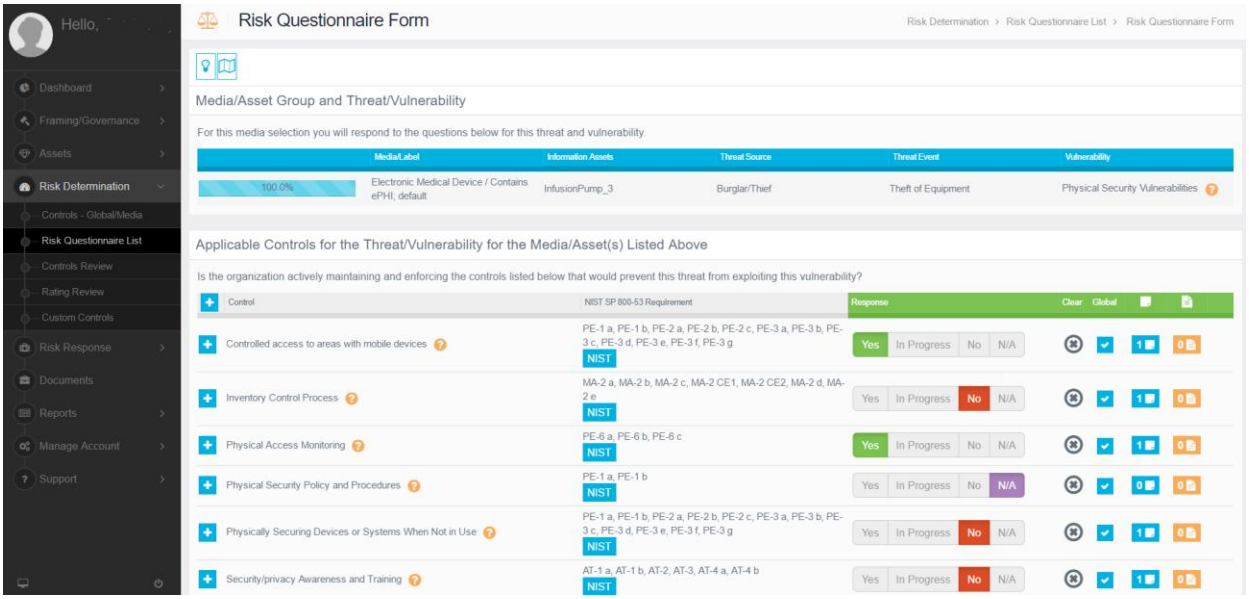
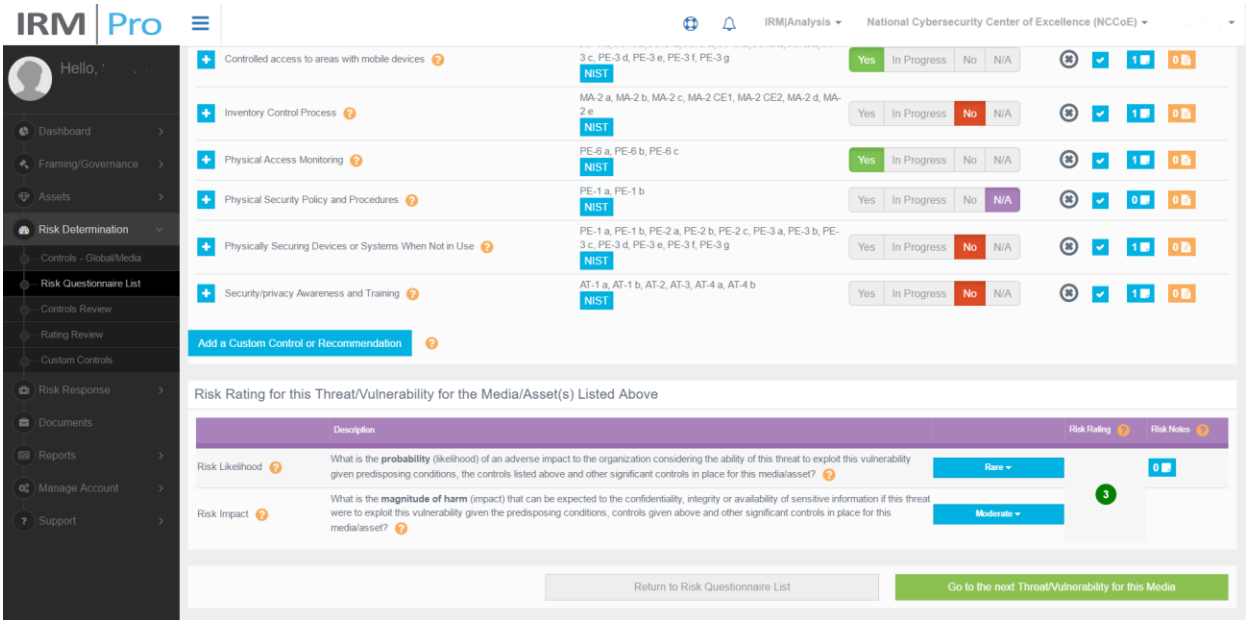


Figure 2-21 Risk Questionnaire Form (Part 2)



2.5.2.4 *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. This section provides the basics of using the tool.

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 **Risk Response List**.
3. Only the risks that 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 – Risk Registry** page (Figure 2-22), scroll up and down to view the Medial/Asset Groups, along with the associated **Threat Source/Event**, **Vulnerability**, and **Risk Rating**.
5. For each relevant risk response, click the associated button in the **Treatment** column to access the **Risk Treat and Evaluate Form** page of that risk (Figure 2-23).
6. On the **Risk Treat and Evaluate Form** page (Figure 2-23), perform the risk response analysis by selecting the **Risk Treatment Type**; evaluate the control or recommendation; **Select a Risk Owner**; enter **Risk Notes**; etc.

Figure 2-22 Risk Response List – Risk Registry

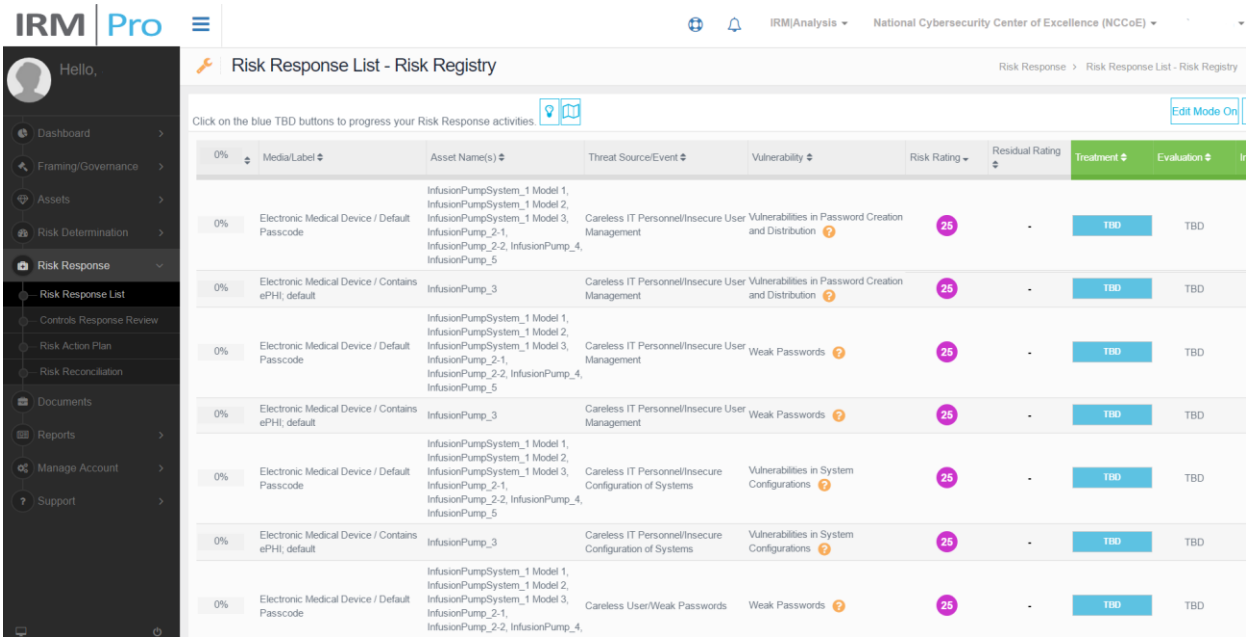
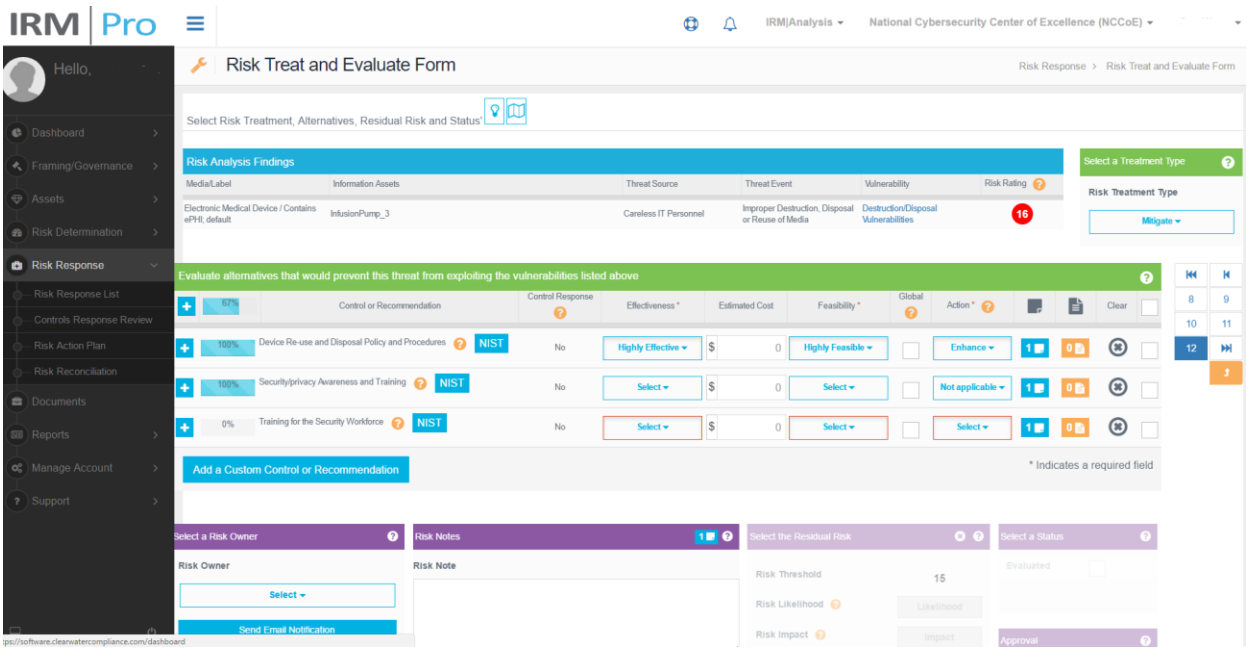


Figure 2-23 Risk Treat and Evaluate Form



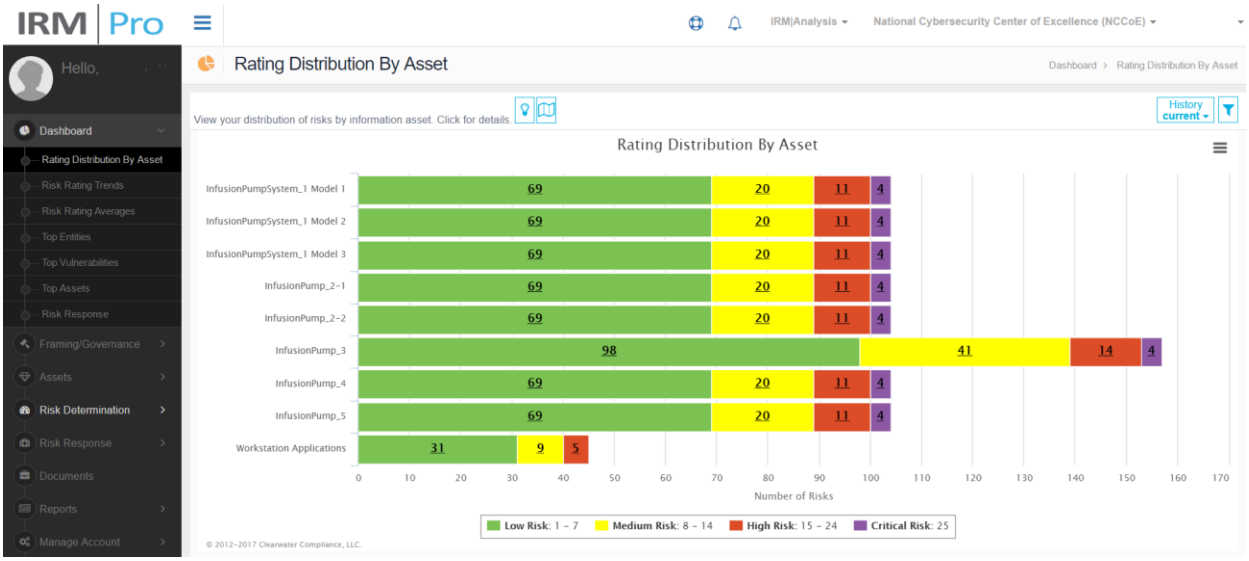
2.5.2.5 Dashboard and Report

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 **Rating Distribution By Asset**.
3. See the example dashboard on the **Rating Distribution By Asset** page shown in Figure 2-24.

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

Figure 2-24 Dashboard Example

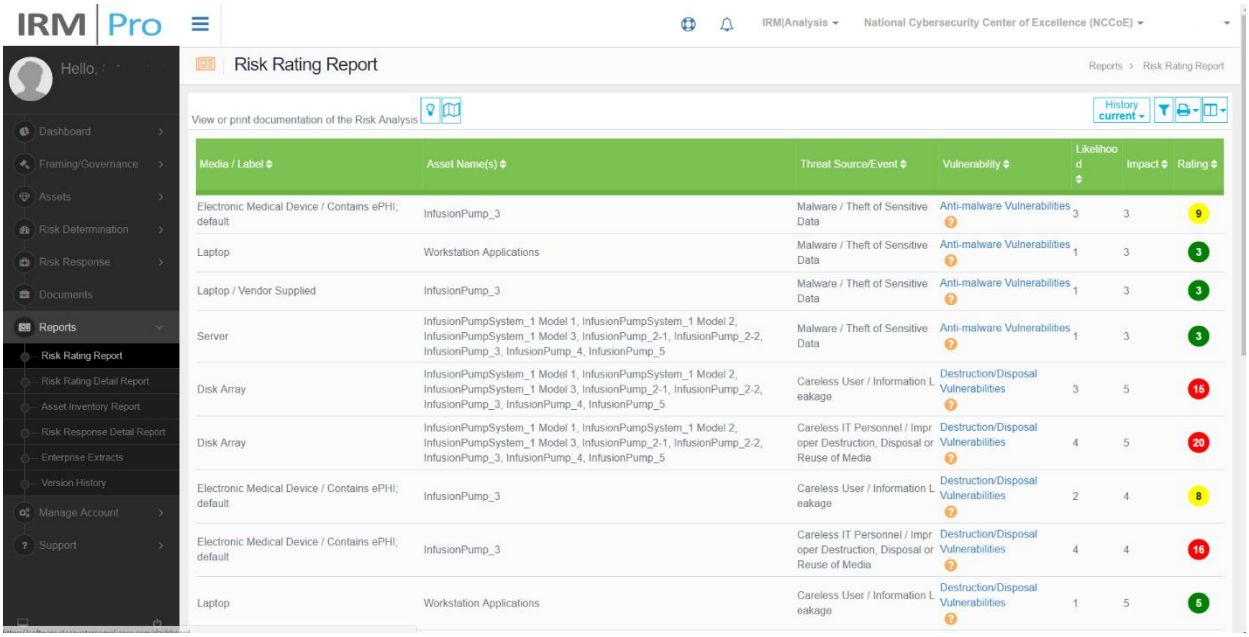


For report views, follow these steps:

1. On the IRM|Analysis tool, expand **Reports** on the left menu bar.
2. Under **Reports**, click **Risk Rating Report**.
3. See the example report on the **Risk Rating Report** page shown in Figure 2-25.

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

Figure 2-25 Report Example



2.5.3 MDISS MDRAP

We used the Medical Device Innovation, Safety & Security Consortium's (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.

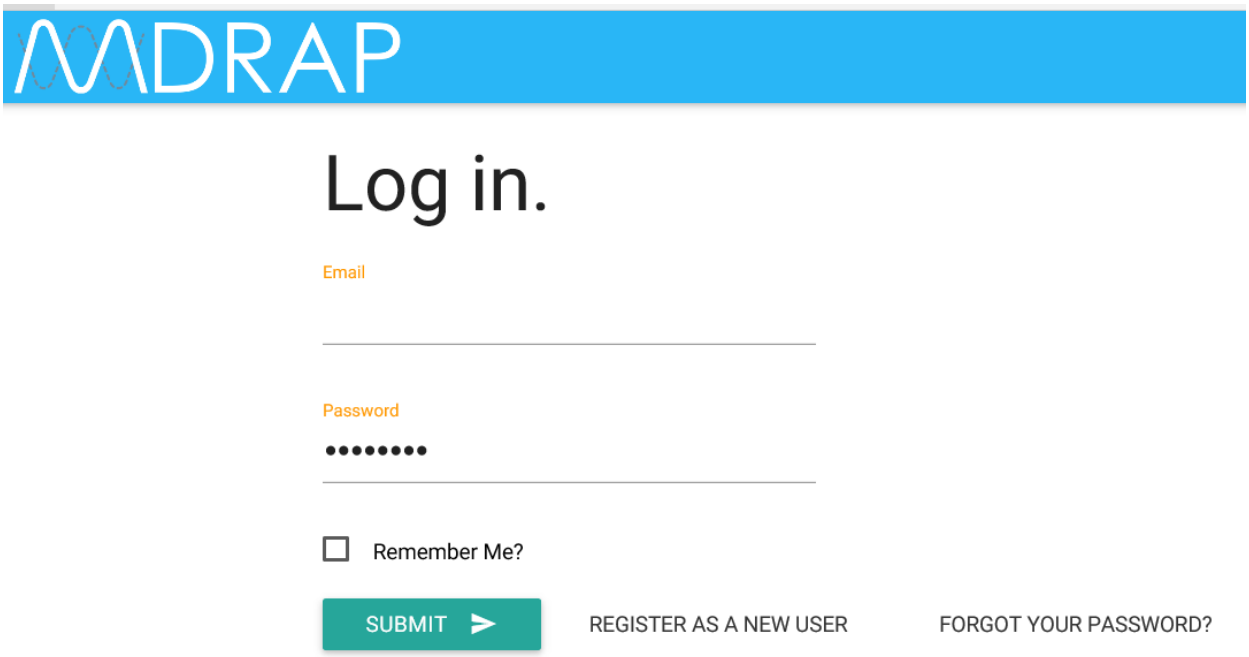
Please note that this section does not show you how to conduct a risk assessment. Instead, we show these basic steps for using the MDRAP tool:

- login to MDRAP
- conduct device inventory
- risk assessment
- dashboard and reports

2.5.3.1 Login to MDRAP

1. Within a browser, type https://mdrap.mdiss.org/,and then click **Log In**.
2. On the login page (Figure 2-26), enter the appropriate **Email** and **Password**.
3. Click **Submit**.

Figure 2-26 MDRAP Login Page



2.5.3.2 *Conduct Device Inventory*

We use the Device Inventory module of MDRAP to keep track of all of the infusion pumps and servers in our sample implementation. Add Device 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 (Figure 2-27), click **Device Inventory** on the menu bar, or click the **View Device Inventory** link on the page.
2. On the **Device Inventory** page (Figure 2-28), add an individual device, edit a device, or bulk import a group of devices.

Figure 2-27 MDRAP Welcome Page

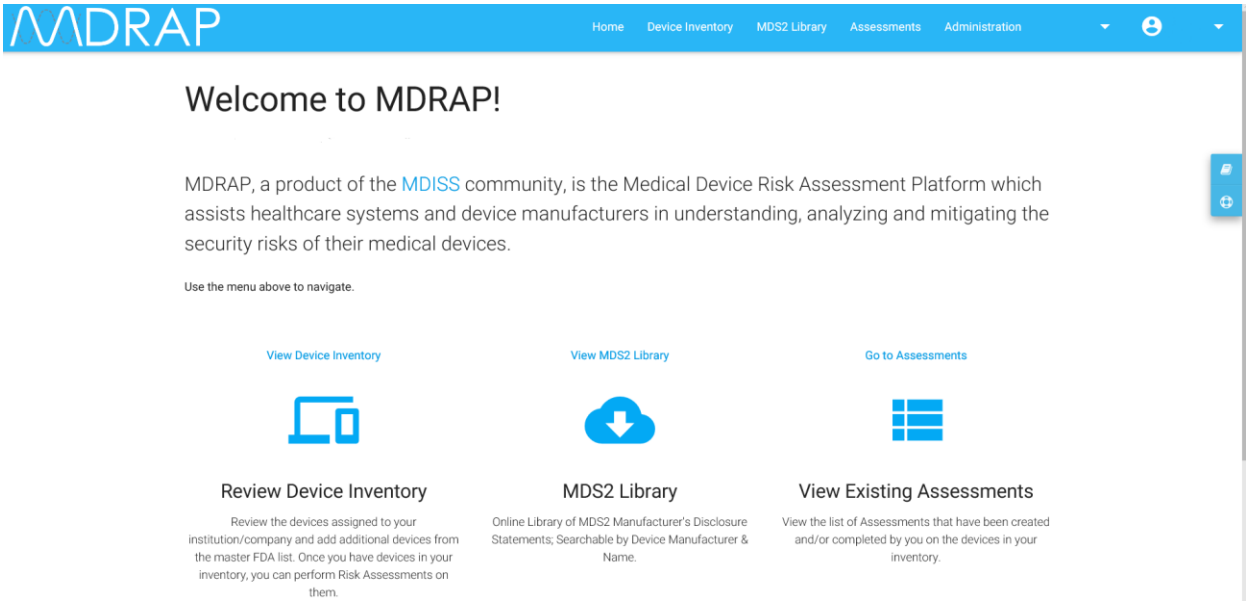
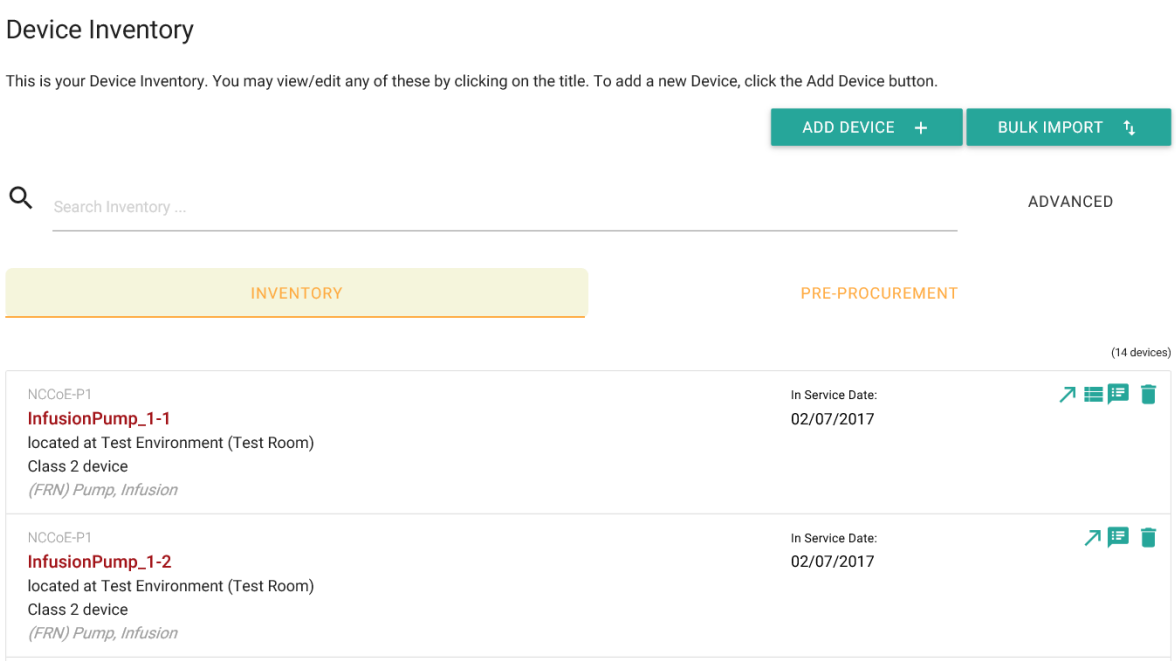


Figure 2-28 Device Inventory List

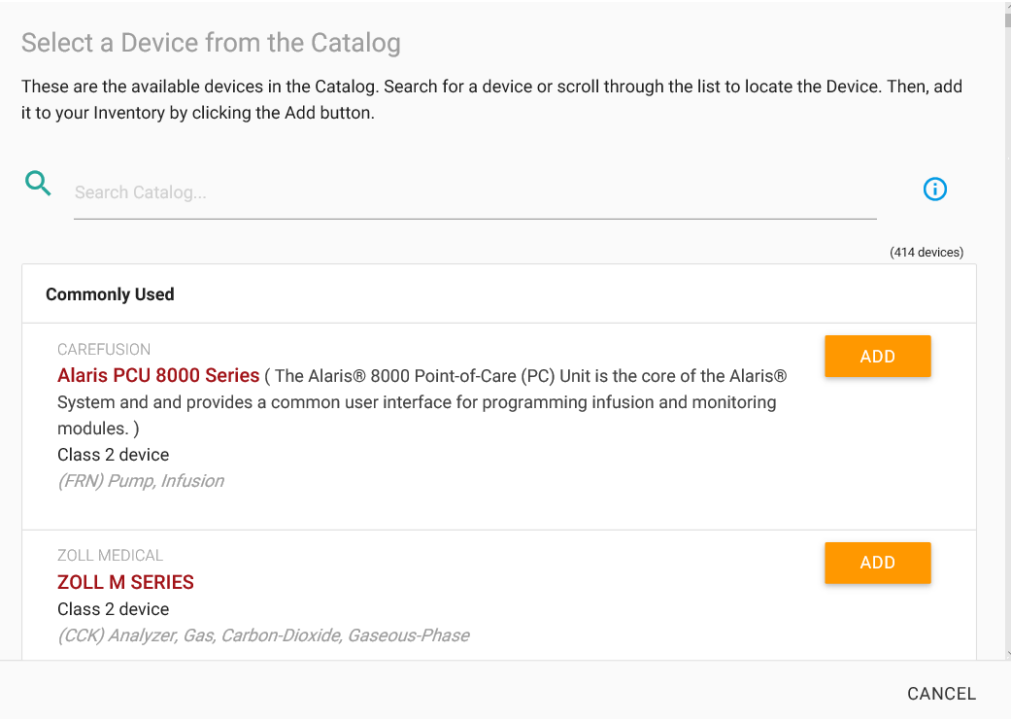


a. To add a device:

i. On the **Device Inventory** page (see Figure 2-28 above), click **ADD DEVICE**.

ii. On the **Add Device** page (Figure 2-29), locate the device from the category list, and then click **ADD**.

Figure 2-29 Add Device

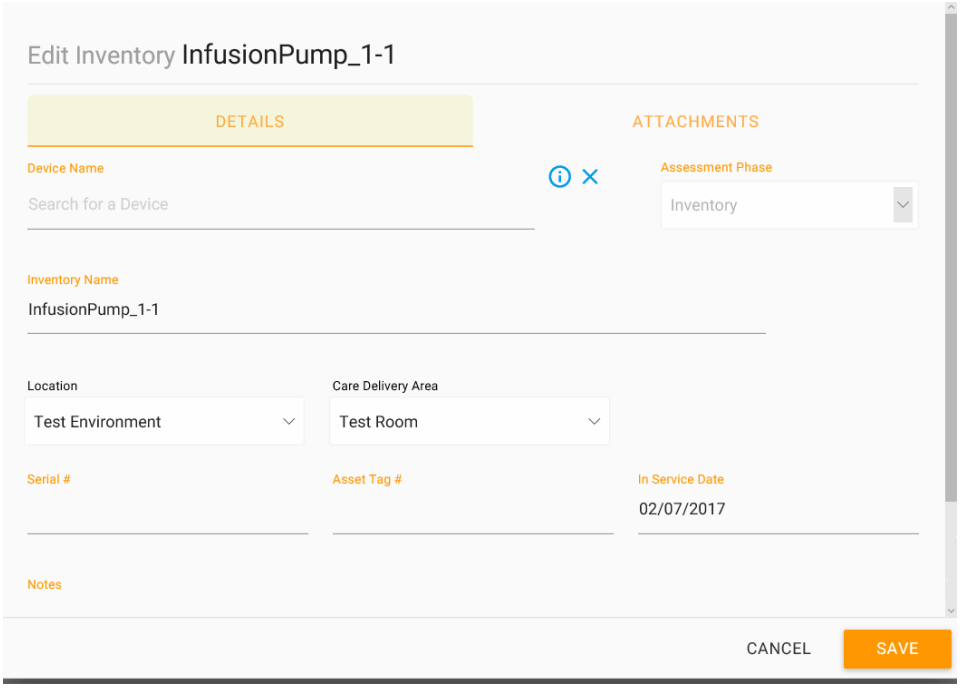


b. To edit a device:

i. On the **Device Inventory** page (see Figure 2-28 above), locate the device from the list, and then click the product name link or the edit icon.

ii. On the **Edit Inventory** page (Figure 2-30), update the data, and then click **Save**.

Figure 2-30 Edit Device



c. To bulk import a group of devices:

   i. On the **Device Inventory** page (Figure 2-28 above), click the **BULK IMPORT** button.

   ii. On the **Inventory Bulk Import** page (Figure 2-31), download the template, and then fill-in the data into the template.

   iii. Follow the instruction to upload and import the devices by using the template (Figure 2-32).

Figure 2-31 Inventory Bulk Import

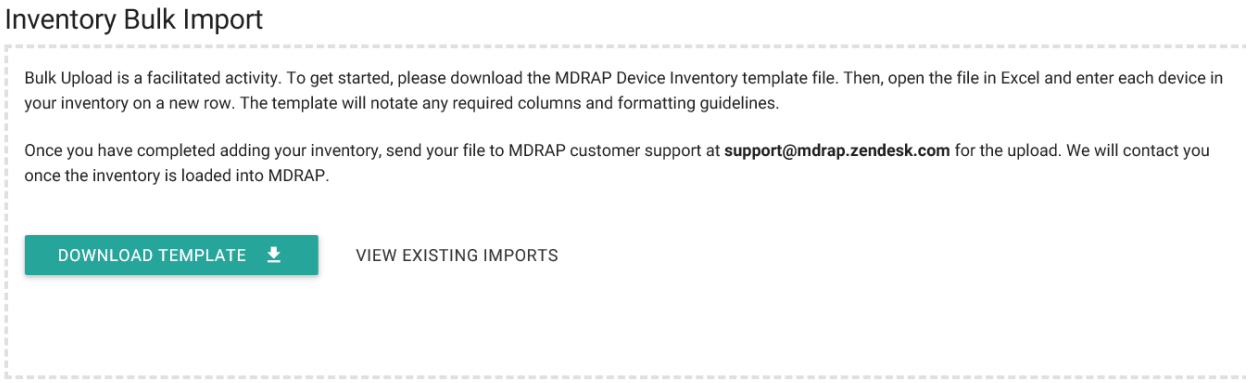


Figure 2-32 Device Inventory Template Sample

MDRAP Device Inventory Template

version 1.0.0
last updated 6/29/2016

** Required*
*** Enter a custom name as you refer to the device in your Organization; otherwise, leave it blank and it will default to the Device Name*

Device Name *	Manufacturer *	Location *	Department / Care Area *	Custom Name **	Serial #	Asset Tag	In Service On	Notes
InfusionPump_1-1	NCCoE-P1	NCCoE	Health Lab	CoE User				
PumpServer_1	NCCoE-P1	NCCoE	Health Lab	NCCoE User				
InfusionPump_1-2	NCCoE-P1	NCCoE	Health Lab	NCCoE User				
NetworkSetup_1	NCCoE-P1	NCCoE	Health Lab	NCCoE User				
InfusionPump_2-1	NCCoE-P2	NCCoE	Health Lab	NCCoE User				
InfusionPump_2-2	NCCoE-P2	NCCoE	Health Lab	NCCoE User				
PumpServer_2	NCCoE-P2	NCCoE	Health Lab	NCCoE User				
InfusionPump_3	NCCoE-P3	NCCoE	Health Lab	NCCoE User				
PumpServer_3	NCCoE-P3	NCCoE	Health Lab	NCCoE User				
NetworkSetup_3	NCCoE-P3	NCCoE	Health Lab	NCCoE User				
InfusionPump_4	NCCoE-P4	NCCoE	Health Lab	NCCoE User				
PumpServer_4	NCCoE-P4	NCCoE	Health Lab	NCCoE User				
InfusionPump_5	NCCoE-P5	NCCoE	Health Lab	NCCoE User				
PumpServer_5	NCCoE-P5	NCCoE	Health Lab	NCCoE User				

Inventory | Locations | Departments

2.5.3.3 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 are listed below.

1. On the **Welcome to MDRAP** page (Figure 2-27 above), click **Assessments** on the menu bar, or click the **Go to Assessments** link on the page.
2. On the **Create Assessment** page (Part 1: Figure 2-33), select a device.
3. On the **Create Assessment** page (Part 2: Figure 2-34), select the questionnaire type (i.e., **MDISS Questionnaire**).

4. Answer the questions, and then click **Next** (see example questionnaire pages in Figure 2-35 and Figure 2-36).

Figure 2-33 Create Assessment (Part 1)

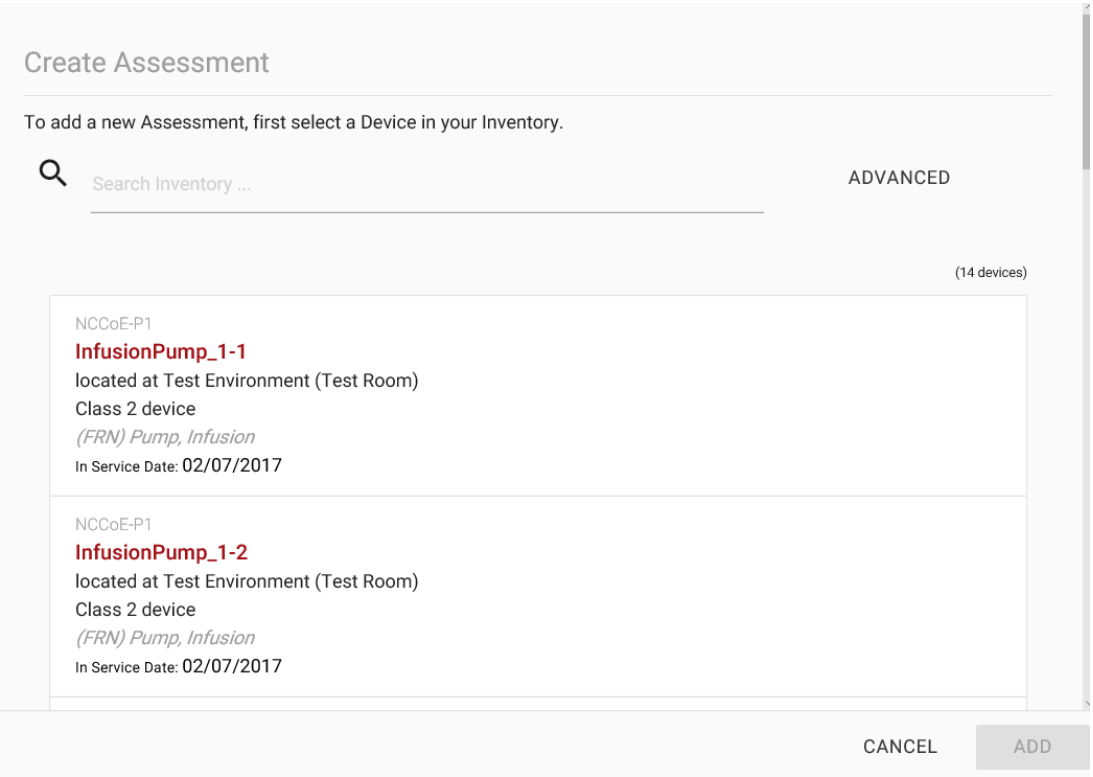


Figure 2-34 Create Assessment (Part 2)

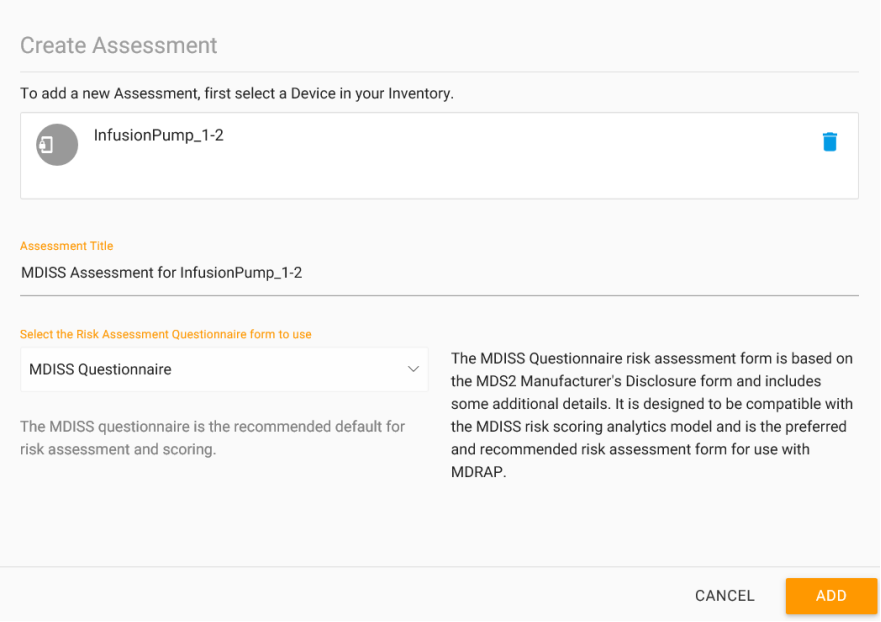


Figure 2-35 Assessment Step (Example 1)

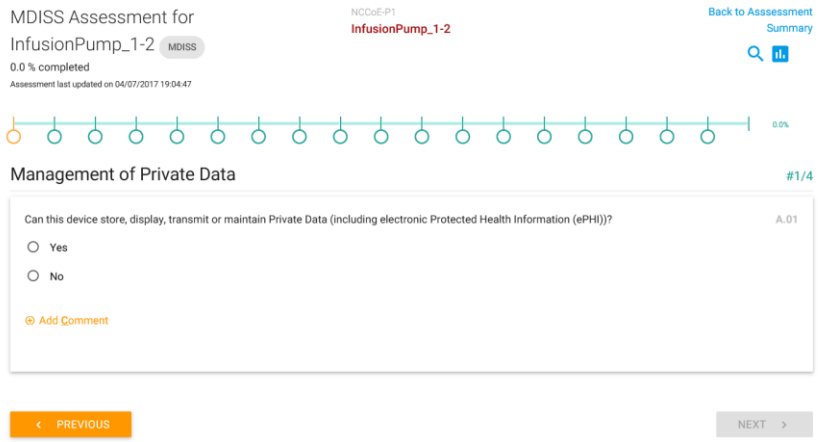
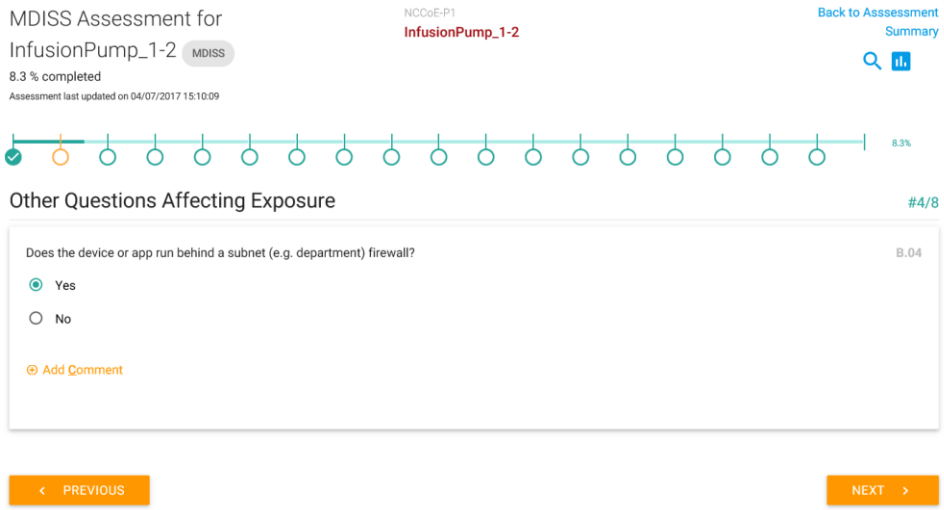


Figure 2-36 Assessment Step (Example 2)



2.5.3.4 *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 (Figure 2-37) or report (Figure 2-38).

Figure 2-37 Assessment Result (Dashboard Example)

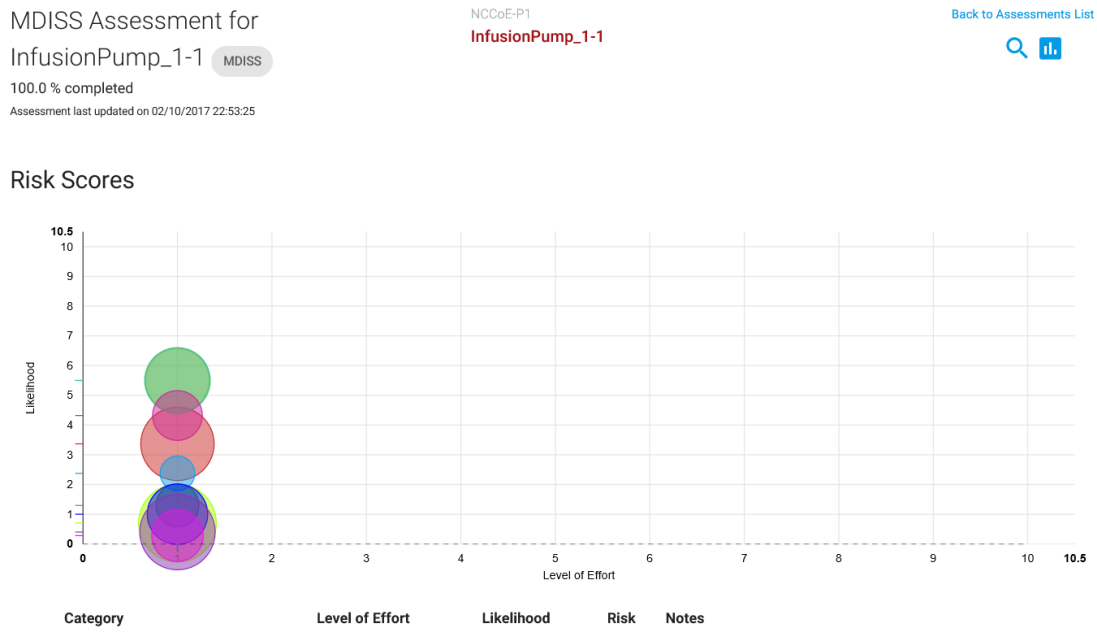


Figure 2-38 Assessment Result (Report Example)

	Category	Level of Effort	Likelihood	Risk	Notes
	Audit Controls	1	3.367	5.25	* Patient identity not captured.
	Authorization	1	5.5	3.75	* Authorization can be bypassed using an API. * Operator can acquire root-level privilege. * Root-level privilege is the only authorization mode.
	Automatic Logoff	1	0.7	6	
	Cyber Security Product Upgrades	1	1.295	1.175	* Device OS is not supported by the OS manufacturer.
	Malware Detection / Protection	1	5.5	4	* No Virus Protection
	Other Scoreable MDS2 Security Categories	1	2.375	0.453	* No encrypption of data at rest. * No Fuzz-testing performed * Some device storage components not physically secured.
	Other Security Considerations - Remote Access	1	1	3.275	* Maintenance users require root privilege.
	Person Authentication	1	0.4	5.6	* Device does not store, display, transmit, or maintain ePHI. * Passwords cannot be set to expire. * Person authentication is not supported.
	System and Application Hardening	1	4.32	1.907	* Device transmits data in the clear on shared networks. * System does not alllow file-level access controls. * Unnecessary services active.
	Transmission Confidentiality &	1	0.28	2.118	

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 [********] password [******]

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 [******] 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 6f6e6c79 31453043 06035504 03133c56
    65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
    65727469 66696361 74696f6e 20417574 686f7269 7479202d 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 7777772e 76657269 7369676e 2e636f6d 2f727061 20286329
    3130312f 302d0603 55040313 26566572 69536967 6e20436c 61737320 33205365
    63757265 20536572 76657220 4341202d 20473330 82012230 0d06092a 864886f7
    0d010101 05000382 010f0030 82010a02 82010100 b187841f c20c45f5 bcab2597
    a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bb658e 444f4dce 6fed094a d4af4e10
    9c688b2e 957b899b 13cae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc
    7f432657 5833833b 330a17b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b
    15fca34b 3bce6388 d0f82d0c 948610ca b69a3dca eb379c00 48358629 5078e845
    63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
    18b49ae8 3c6e81fd e4cd3536 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced
    4a546ac9 4dc5bf11 b1ae1c67 81cb4455 33997f24 9b3f5345 7f861af3 3cfa6d7f
```

```
    81f5b84a d3f58537 1cb5a6d0 09e4187b 384efa0f 02030100 01a38201 df308201
    db303406 082b0601 05050701 01042830 26302406 082b0601 05050730 01861868
    7474703a 2f2f6f63 73702e76 65726973 69676e2e 636f6d30 12060355 1d130101
    ff040830 060101ff 02010030 70060355 1d200469 30673065 060b6086 480186f8
    45010717 03305630 2806082b 06010505 07020116 1c687474 70733a2f 2f777777
    2e766572 69736967 6e2e636f 6d2f6370 73302a06 082b0601 05050702 02301e1a
    1c687474 70733a2f 2f777777 2e766572 69736967 6e2e636f 6d2f7270 61303406
    03551d1f 042d302b 3029a027 a0258623 68747470 3a2f2f63 726c2e76 65726973
    69676e2e 636f6d2f 70636133 2d67352e 63726c30 0e060355 1d0f0101 ff040403
    02010630 6d06082b 06010505 07010c04 61305fa1 5da05b30 59305730 55160969
    6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
    c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
    69676e2e 636f6d2f 76736c6f 676f2e67 69663028 0603551d 11042130 1fa41d30
    1b311930 17060355 04031310 56657269 5369676e 4d504b49 2d322d36 301d0603
    551d0e04 1604140d 445c1653 44c1827e 1d20ab25 f40163d8 be79a530 1f060355
    1d230418 30168014 7fd365a7 c2ddecbb f03009f3 4339fa02 af333133 300d0609
    2a864886 f70d0101 05050003 82010100 0c8324ef ddc30cd9 589cfe36 b6eb8a80
    4bd1a3f7 9df3cc53 ef829ea3 a1e697c1 589d756c e01d1b4c fad1c12d 05c0ea6e
    b2227055 d9203340 3307c265 83fa8f43 379bea0e 9a6c70ee f69c803b d937f47a
    6decd018 7d494aca 99c71928 a2bed877 24f78526 866d8705 404167d1 273aeddc
    481d22cd 0b0b8bbc f4b17bfd b499a8e9 762ae11a 2d876e74 d388dd1e 22c6df16
    b62b8214 0a945cf2 50ecafce ff62370d ad65d306 4153ed02 14c8b558 28a1ace0
    5becb37f 954afb03 c8ad26db e6667812 4ad99f42 fbe198e6 42839b8f 8f6724e8
    6119b5dd cdb50b26 058ec36e c4c875b8 46cfe218 065ea9ae a8819a47 16de0c28
    6c2527b9 deb78458 c61f381e a4c4cb66
  quit
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
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 [******] password [******] 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:   ASAv, 2048 MB RAM, CPU Xeon E5 series 2200 MHz
:
ASA Version 9.6(1)
!
hostname enterprise-services-kmcfadde
enable password [******] 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 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 6f6e6c79 31453043 06035504 03133c56
    65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
    65727469 66696361 74696f6e 20417574 686f7269 7479202d 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 7777772e 76657269 7369676e 2e636f6d 2f727061 20286329
3130312f 302d0603 55040313 26566572 69536967 6e20436c 61737320 33205365
63757265 20536572 76657220 4341202d 20473330 82012230 0d06092a 864886f7
0d010101 05000382 010f0030 82010a02 82010100 b187841f c20c45f5 bcab2597
a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bb658e 444f4dce 6fed094a d4af4e10
9c688b2e 957b899b 13cae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc
7f432657 5833833b 330a17b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b
15fca34b 3bce6388 d0f82d0c 948610ca b69a3dca eb379c00 48358629 5078e845
63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
18b49ae8 3c6e81fd e4cd3536 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced
4a546ac9 4dc5bf11 b1ae1c67 81cb4455 33997f24 9b3f5345 7f861af3 3cfa6d7f
81f5b84a d3f58537 1cb5a6d0 09e4187b 384efa0f 02030100 01a38201 df308201
db303406 082b0601 05050701 01042830 26302406 082b0601 05050730 01861868
7474703a 2f2f6f63 73702e76 65726973 69676e2e 636f6d30 12060355 1d130101
ff040830 060101ff 02010030 70060355 1d200469 30673065 060b6086 480186f8
45010717 03305630 2806082b 06010505 07020116 1c687474 70733a2f 2f777777
2e766572 69736967 6e2e636f 6d2f6370 73302a06 082b0601 05050702 02301e1a
1c687474 70733a2f 2f777777 2e766572 69736967 6e2e636f 6d2f7270 61303406
03551d1f 042d302b 3029a027 a0258623 68747470 3a2f2f63 726c2e76 65726973
69676e2e 636f6d2f 70636133 2d67352e 63726c30 0e060355 1d0f0101 ff040403
02010630 6d06082b 06010505 07010c04 61305fa1 5da05b30 59305730 55160969
6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
69676e2e 636f6d2f 76736c6f 676f2e67 69663028 0603551d 11042130 1fa41d30
1b311930 17060355 04031310 56657269 5369676e 4d504b49 2d322d36 301d0603
551d0e04 1604140d 445c1653 44c1827e 1d20ab25 f40163d8 be79a530 1f060355
1d230418 30168014 7fd365a7 c2ddecbb f03009f3 4339fa02 af333133 300d0609
2a864886 f70d0101 05050003 82010100 0c8324ef ddc30cd9 589cfe36 b6eb8a80
4bd1a3f7 9df3cc53 ef829ea3 a1e697c1 589d756c e01d1b4c fad1c12d 05c0ea6e
b2227055 d9203340 3307c265 83fa8f43 379bea0e 9a6c70ee f69c803b d937f47a
```

```
    6decd018 7d494aca 99c71928 a2bed877 24f78526 866d8705 404167d1 273aeddc
    481d22cd 0b0b8bbc f4b17bfd b499a8e9 762ae11a 2d876e74 d388dd1e 22c6df16
    b62b8214 0a945cf2 50ecafce ff62370d ad65d306 4153ed02 14c8b558 28a1ace0
    5becb37f 954afb03 c8ad26db e6667812 4ad99f42 fbe198e6 42839b8f 8f6724e8
    6119b5dd cdb50b26 058ec36e c4c875b8 46cfe218 065ea9ae a8819a47 16de0c28
    6c2527b9 deb78458 c61f381e a4c4cb66
  quit
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
username [******] password [******] 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: 9A3RHJVFPQS
: Hardware:   ASAv, 2048 MB RAM, CPU Xeon E5 series 2200 MHz
:
ASA Version 9.6(1)
!
hostname biomedical-kmcfadde
enable password [******] 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 4080
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
    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 6f6e6c79 31453043 06035504 03133c56
    65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
```

```
65727469 66696361 74696f6e 20417574 686f7269 7479202d 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 7777772e 76657269 7369676e 2e636f6d 2f727061 20286329
3130312f 302d0603 55040313 26566572 69536967 6e20436c 61737320 33205365
63757265 20536572 76657220 4341202d 20473330 82012230 0d06092a 864886f7
0d010101 05000382 010f0030 82010a02 82010100 b187841f c20c45f5 bcab2597
a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bb658e 444f4dce 6fed094a d4af4e10
9c688b2e 957b899b 13cae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc
7f432657 5833833b 330a17b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b
15fca34b 3bce6388 d0f82d0c 948610ca b69a3dca eb379c00 48358629 5078e845
63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
18b49ae8 3c6e81fd e4cd3536 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced
4a546ac9 4dc5bf11 b1ae1c67 81cb4455 33997f24 9b3f5345 7f861af3 3cfa6d7f
81f5b84a d3f58537 1cb5a6d0 09e4187b 384efa0f 02030100 01a38201 df308201
db303406 082b0601 05050701 01042830 26302406 082b0601 05050730 01861868
7474703a 2f2f6f63 73702e76 65726973 69676e2e 636f6d30 12060355 1d130101
ff040830 060101ff 02010030 70060355 1d200469 30673065 060b6086 480186f8
45010717 03305630 2806082b 06010505 07020116 1c687474 70733a2f 2f777777
2e766572 69736967 6e2e636f 6d2f6370 73302a06 082b0601 05050702 02301e1a
1c687474 70733a2f 2f777777 2e766572 69736967 6e2e636f 6d2f7270 61303406
03551d1f 042d302b 3029a027 a0258623 68747470 3a2f2f63 726c2e76 65726973
69676e2e 636f6d2f 70636133 2d67352e 63726c30 0e060355 1d0f0101 ff040403
02010630 6d06082b 06010505 07010c04 61305fa1 5da05b30 59305730 55160969
6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
69676e2e 636f6d2f 76736c6f 676f2e67 69663028 0603551d 11042130 1fa41d30
1b311930 17060355 04031310 56657269 5369676e 4d504b49 2d322d36 301d0603
551d0e04 1604140d 445c1653 44c1827e 1d20ab25 f40163d8 be79a530 1f060355
1d230418 30168014 7fd365a7 c2ddecbb f03009f3 4339fa02 af333133 300d0609
```

```
    2a864886 f70d0101 05050003 82010100 0c8324ef ddc30cd9 589cfe36 b6eb8a80
    4bd1a3f7 9df3cc53 ef829ea3 a1e697c1 589d756c e01d1b4c fad1c12d 05c0ea6e
    b2227055 d9203340 3307c265 83fa8f43 379bea0e 9a6c70ee f69c803b d937f47a
    6decd018 7d494aca 99c71928 a2bed877 24f78526 866d8705 404167d1 273aeddc
    481d22cd 0b0b8bbc f4b17bfd b499a8e9 762ae11a 2d876e74 d388dd1e 22c6df16
    b62b8214 0a945cf2 50ecafce ff62370d ad65d306 4153ed02 14c8b558 28a1ace0
    5becb37f 954afb03 c8ad26db e6667812 4ad99f42 fbe198e6 42839b8f 8f6724e8
    6119b5dd cdb50b26 058ec36e c4c875b8 46cfe218 065ea9ae a8819a47 16de0c28
    6c2527b9 deb78458 c61f381e a4c4cb66
  quit
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
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 [******] password [******] 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: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-kmcfadde
enable password [******] 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 HOSPIRAPUMPSIMPORTS
 service-object tcp destination eq https
 service-object tcp destination eq 8443
object-group service BAXTERPUMPPORTS
 service-object tcp-udp destination eq 51243
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
access-list LAN2WAN extended permit ip object PUMPS object PUMPSERVERS
access-list WAN2LAN extended permit object-group PCAPORTS host 192.168.140.160 o
bject PUMPS
access-list WAN2LAN extended permit icmp any any object-group PING
access-list WAN2LAN extended permit object-group TRACEROUTEUDP any 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 192.168.140.1
60 object PUMPS
access-list WAN2LAN extended permit object-group HOSPIRAPUMPSIMPORTS host 192.16
8.140.160 object PUMPS
access-list WAN2LAN extended permit object-group BAXTERPUMPPORTS host 192.168.14
0.165 object PUMPS
access-list WAN2LAN extended permit object-group BBRAUNPORTS host 192.168.140.16
9 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 20466f72
    20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
    65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
    65727469 66696361 74696f6e 20417574 686f7269 7479202d 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 7777772e 76657269 7369676e 2e636f6d 2f727061 20286329
    3130312f 302d0603 55040313 26566572 69536967 6e20436c 61737320 33205365
    63757265 20536572 76657220 4341202d 20473330 82012230 0d06092a 864886f7
    0d010101 05000382 010f0030 82010a02 82010100 b187841f c20c45f5 bcab2597
    a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bb658e 444f4dce 6fed094a d4af4e10
    9c688b2e 957b899b 13cae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc
    7f432657 5833833b 330a17b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b
    15fca34b 3bce6388 d0f82d0c 948610ca b69a3dca eb379c00 48358629 5078e845
```

```
    63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
    18b49ae8 3c6e81fd e4cd3536 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced
    4a546ac9 4dc5bf11 b1ae1c67 81cb4455 33997f24 9b3f5345 7f861af3 3cfa6d7f
    81f5b84a d3f58537 1cb5a6d0 09e4187b 384efa0f 02030100 01a38201 df308201
    db303406 082b0601 05050701 01042830 26302406 082b0601 05050730 01861868
    7474703a 2f2f6f63 73702e76 65726973 69676e2e 636f6d30 12060355 1d130101
    ff040830 060101ff 02010030 70060355 1d200469 30673065 060b6086 480186f8
    45010717 03305630 2806082b 06010505 07020116 1c687474 70733a2f 2f777777
    2e766572 69736967 6e2e636f 6d2f6370 73302a06 082b0601 05050702 02301e1a
    1c687474 70733a2f 2f777777 2e766572 69736967 6e2e636f 6d2f7270 61303406
    03551d1f 042d302b 3029a027 a0258623 68747470 3a2f2f63 726c2e76 65726973
    69676e2e 636f6d2f 70636133 2d67352e 63726c30 0e060355 1d0f0101 ff040403
    02010630 6d06082b 06010505 07010c04 61305fa1 5da05b30 59305730 55160969
    6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
    c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
    69676e2e 636f6d2f 76736c6f 676f2e67 69663028 0603551d 11042130 1fa41d30
    1b311930 17060355 04031310 56657269 5369676e 4d504b49 2d322d36 301d0603
    551d0e04 1604140d 445c1653 44c1827e 1d20ab25 f40163d8 be79a530 1f060355
    1d230418 30168014 7fd365a7 c2ddecbb f03009f3 4339fa02 af333133 300d0609
    2a864886 f70d0101 05050003 82010100 0c8324ef ddc30cd9 589cfe36 b6eb8a80
    4bd1a3f7 9df3cc53 ef829ea3 a1e697c1 589d756c e01d1b4c fad1c12d 05c0ea6e
    b2227055 d9203340 3307c265 83fa8f43 379bea0e 9a6c70ee f69c803b d937f47a
    6decd018 7d494aca 99c71928 a2bed877 24f78526 866d8705 404167d1 273aeddc
    481d22cd 0b0b8bbc f4b17bfd b499a8e9 762ae11a 2d876e74 d388dd1e 22c6df16
    b62b8214 0a945cf2 50ecafce ff62370d ad65d306 4153ed02 14c8b558 28a1ace0
    5becb37f 954afb03 c8ad26db e6667812 4ad99f42 fbe198e6 42839b8f 8f6724e8
    6119b5dd cdb50b26 058ec36e c4c875b8 46cfe218 065ea9ae a8819a47 16de0c28
    6c2527b9 deb78458 c61f381e a4c4cb66
  quit
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
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 [******]password [******] 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/DD
CEService
  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:b2e10eb9d982ddbe5330e964af80d2d3

: end
```

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 [******]
enable password [******]
!
username [******]privilege [**] password [******]
user-name [******]
 creation-time 1469560730
 privilege [**]
 password [******]
 type mgmt-user
no aaa new-model
switch 1 provision ws-c3650-48ps
!
ip domain-name [******]
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 2D536967 6E65642D 43657274
  69666963 6174652D 32303335 36343231 3331301E 170D3136 30373236 32303436
  32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 30333536
  34323133 3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100F1C4 010AE138 9BD9BBCC 2E563180 698979B5 51F7B46B D122595E E7033DCA
  D80C9432 0728E47F 8CAC2629 40CEC617 5CDFFBD9 19744025 CB62CA75 8F6F0A9A
  34F790DD 07DA9D60 737196C1 FDD9E764 6D22EDA3 8D9E7DF5 6CD934E3 D89FA9D5
  C165F3EE E9E0EA9F 37742B00 2C4CFA0B C262E61B 95565B42 302B23E7 A1C85D9F
```

```
  5FDB0203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF 30200603
  551D1104 19301782 15436973 636F3336 35302D30 312E6E69 73742E67 6F76301F
  0603551D 23041830 1680148F 3A1CDEB7 502DACB7 DF4E96E4 EA1470F1 CFD1F730
  1D060355 1D0E0416 04148F3A 1CDEB750 2DACB7DF 4E96E4EA 1470F1CF D1F7300D
  06092A86 4886F70D 01010405 00038181 004FE025 9B72B4D2 5391B847 F443B481
  4493F8BD 69D2FF3A 3C2E6D96 D7D83B92 91DBB84D DD47E242 9B2F45AC CA7C7CBC
  D7CB9660 2B07AE9B 0376D5A1 15CBA04B B326AADE AB213EB1 D625FBFF B2F54CCD
  40B1EB91 C6DD5E33 DEA8EEB3 20ECDE96 F42527D6 AD1F6A5D A261D394 FE358B8F
  317FAFD0 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 <email-address>
!
!
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 [******]
 login local
 transport input ssh
line vty 5 15
 access-class SSH-Access in
 exec-timeout 300 0
 password [******]
 login local
 transport input ssh
!
ntp 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...............................
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..............................

NTP Servers
```

```
    NTP Polling Interval.........................     3600


     Index     NTP Key Index                  NTP Server                Status
NTP Msg Auth Status

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

       1              0                                  192.168.250.1     Not Synched
AUTH DISABLED


Redundancy Information

Redundancy Mode ................................ SSO DISABLED

Local State..................................... ACTIVE

Peer State...................................... N/A

Unit............................................ Primary

Unit ID......................................... 00:50:56:AC:6D:08

Redunadancy 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


Primary 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

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
           STP   Admin   Physical   Physical   Link   Link
Pr  Type   Stat   Mode     Mode      Status   Status  Trap     POE
-- ------- ---- ------- ---------- ---------- ------ ------- ---------
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
```

```
AP Name             Slots  AP Model             Ethernet MAC       Location
Country     IP Address       Clients   DSE Location

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

AP78da.6ee0.08ec     2     AIR-CAP1602I-A-K9     78:da:6e:e0:08:ec  default location
US          192.168.250.10     0       [0 ,0 ,0 ]

AP24e9.b34b.f1ed     2     AIR-CAP1602I-A-K9     24:e9:b3:4b:f1:ed  default location
US          192.168.250.11     1       [0 ,0 ,0 ]


AP Tcp-Mss-Adjust Info

AP Name              TCP State  MSS Size

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

AP78da.6ee0.08ec     disabled   -

AP24e9.b34b.f1ed     disabled   -


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>


WLAN ID          Interface          Network Admission Control          Radio Policy
```

```
-------          -----------        ---------------------------         ------------
 1               ip_dev               Disabled                           None
 2               ip_dev               Disabled                           None

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


 Lan Port configs
 ----------------


LAN          Status        POE          RLAN
---          -------       ----         -----
 1           Disabled      Disabled     None
 2           Disabled                   None
 3           Disabled                   None

 External 3G/4G module configs
 -----------------------------


LAN          Status        POE          RLAN
---          -------       ----         -----
 1           Disabled                   None


AP Name             Slots  AP Model             Ethernet MAC       Location
Port  Country  Priority
------------------  -----  -------------------  -----------------  ----------------  -
---  -------  --------
AP78da.6ee0.08ec     2     AIR-CAP1602I-A-K9    78:da:6e:e0:08:ec  default location  1
US       1
AP24e9.b34b.f1ed     2     AIR-CAP1602I-A-K9    24:e9:b3:4b:f1:ed  default location  1
US       1


RF Profile
```

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


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


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


RF Profile Name                     Band     Description                          11n-
client-only     Applied

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

High-Client-Density-802.11a         5 GHz    <none>
disable             No

High-Client-Density-802.11bg        2.4 GHz  <none>
disable             No

Low-Client-Density-802.11a          5 GHz    <none>
disable             No

Low-Client-Density-802.11bg         2.4 GHz  <none>
disable             No

Typical-Client-Density-802.11a      5 GHz    <none>
disable             No

Typical-Client-Density-802.11bg     2.4 GHz  <none>
disable             No



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

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............................................ -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

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........................................... -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

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

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................................. 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
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 :

WLAN ID   PROFILE NAME                       ACL                                TYPE
-------  -------------------------------   --------------------------------   ------
-


 Flexconnect Central-Dhcp Values :

WLAN ID   PROFILE NAME                         Central-Dhcp      DNS Override
Nat-Pat     Type
-------  ---------------------------------    --------------    --------------    ----
-----   ------
```

```
  1       IP_Dev No Encryption                      False             False
False      Wlan


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


WlanId  PROFILE NAME                     Inherit-level Visibility       Flex Avc-
profile

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

1          IP_Dev No Encryption             wlan-spec     disable    none


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

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
  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.... 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 :

WLAN ID   PROFILE NAME                       ACL                                TYPE
-------  --------------------------------   --------------------------------   ------
-


 Flexconnect Central-Dhcp Values :

WLAN ID   PROFILE NAME                         Central-Dhcp      DNS Override
Nat-Pat     Type
-------  --------------------------------    --------------    --------------    ----
-----   ------
  1       IP_Dev No Encryption                    False             False
False      Wlan


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

WlanId  PROFILE NAME                    Inherit-level Visibility       Flex Avc-
profile
------- ------------------------------- ------------- ---------- --------------------
------------
```

```
1          IP_Dev No Encryption             wlan-spec     disable    none

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
  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........................................... 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
  Class Type                 Channel  DC (%%)  RSSI (dBm)  Last Update Time
  -------------------------  -------  ------  ----------  ------------------------
  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-peakdetect..... 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 bandwith 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

AP Name                          MAC Address       Slot Admin    Oper        Channel
TxPower
-------------------------------- ----------------- ---- -------- ----------- ---------
--------- -------------
AP78da.6ee0.08ec                 5c:a4:8a:be:ca:90  1   ENABLED  UP          149*
*1/6 (22 dBm)
AP24e9.b34b.f1ed                 1c:1d:86:31:e5:50  1   ENABLED  UP          48*
*1/6 (22 dBm)

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

AP Name                          Channel    TxPower       Allowed Power Levels
-------------------------------- ---------- ------------- ------------------------
AP78da.6ee0.08ec                 149*       *1/6 (22 dBm) [22/19/16/13/10/7/7/7]
AP24e9.b34b.f1ed                 48*        *1/6 (22 dBm) [22/19/16/13/10/7/7/7]
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

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

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

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



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
```

```
AP Name                          Channel    TxPower       Allowed Power Levels
-------------------------------- ---------- ------------- ------------------------
AP78da.6ee0.08ec                 *11        *1/6 (22 dBm) [22/19/16/13/10/7/7/7]
AP24e9.b34b.f1ed                 *11        *1/6 (22 dBm) [22/19/16/13/10/7/7/7]
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 lev.... 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
  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
 MAC Address        IP Address                                  Group Name
Multicast IP                                  Status

 00:50:56:ac:6d:08  192.168.250.2                               WLAN
0.0.0.0                                       Up




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

 WLAN ID     Foreign Mac Address     Interface

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




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
Exclusionlist 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
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 - AironetIe 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)........ 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
 WLAN ID     IP Address            Status                              Priority
 -------     ---------------       ------                              --------

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 - AironetIe 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
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
```

```
   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
 WLAN ID     IP Address            Status                          Priority
 -------     ---------------       ------                          --------
```

```
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


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

```
TACACS Configuration
Fallback Test:
    Interval (in seconds)..... 0
Authentication Servers

Idx      Server Address        Port    State   Tout   MgmtTout
---  ----------------------   ------  -------  -----  --------

Authorization Servers

Idx      Server Address        Port    State   Tout   MgmtTout
---  ----------------------   ------  -------  -----  --------

Accounting Servers

Idx      Server Address        Port    State   Tout   MgmtTout
---  ----------------------   ------  -------  -----  --------



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 .............................. 436973636f00000000000000000000000
      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
Group Name                 # Aps




FlexConnect Group Detail




FlexConnect Vlan name Summary

Vlan-Name Id                     Status
-------------------------------- -------
```

```
FlexConnect Vlan Name Detail




Route  Info
Number of Routes.............................. 0

Destination Network          Netmask               Gateway
-------------------    --------------------   --------------------




Peer Route  Info
Number of Routes.............................. 32555

Destination Network          Netmask               Gateway
-------------------    --------------------   --------------------




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
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........................................... 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 ConfigurationUnable 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     :                   1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-A   ,-AB  ): A * * * * A * * * * A . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    802.11a      :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
    Channels     : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 4 5 5 6 6 6 7
                 : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 4 9 3 7 1 5 9 3
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB  ,-AB  ): . A . A . A . A A A A A A A A A A A A A A A A A A A A A * . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 4.9GHz 802.11a  :
    Channels     :                   1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 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


                                    WLAN       Client

WLAN ID  WLAN Name                  Status     Protection

-------  -------------------------  ---------  ----------
```

```
1        IP_Dev No Encryption       Disabled   Optional but inactive (WPA2 not
configured)

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

MAC Address        Classification     # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
04:bd:88:b5:2f:40  Friendly           2     0         Thu Aug 18 20:06:04 2016
04:bd:88:b5:2f:45  Friendly           2     0         Thu Aug 18 20:06:04 2016
04:bd:88:b5:2f:50  Friendly           0     0         Not Heard
04:bd:88:b5:2f:55  Friendly           0     0         Not Heard
04:bd:88:b5:4e:e0  Friendly           0     0         Not Heard
04:bd:88:b5:4e:f0  Friendly           0     0         Not Heard
04:bd:88:b5:5a:20  Unclassified       2     0         Thu Aug 18 20:06:04 2016
04:bd:88:b5:5a:21  Unclassified       2     0         Thu Aug 18 20:06:04 2016
04:bd:88:b6:0d:60  Friendly           0     0         Not Heard
04:bd:88:b6:0d:70  Friendly           0     0         Not Heard
04:bd:88:b6:0d:75  Friendly           0     0         Not Heard
04:bd:88:b6:0e:e0  Friendly           0     0         Not Heard
04:bd:88:b6:0e:f0  Friendly           0     0         Not Heard
```

```
04:bd:88:b6:0e:f5  Friendly          0     0         Not Heard
04:bd:88:b6:10:00  Friendly          0     0         Not Heard
04:bd:88:b6:10:10  Friendly          0     0         Not Heard
04:bd:88:b6:10:15  Friendly          0     0         Not Heard
04:bd:88:b6:10:60  Friendly          2     0         Thu Aug 18 20:06:04 2016
04:bd:88:b6:10:65  Unclassified      2     0         Thu Aug 18 20:06:04 2016
04:bd:88:b6:10:70  Friendly          0     0         Not Heard
04:bd:88:b6:10:75  Friendly          0     0         Not Heard
04:bd:88:b6:10:b5  Friendly          0     0         Not Heard
62:6d:c7:27:a6:98  Unclassified      2     0         Thu Aug 18 20:06:04 2016
6c:72:20:3e:af:26  Friendly          0     0         Not Heard
6c:72:20:3e:af:28  Friendly          0     0         Not Heard
6c:72:20:3e:af:2a  Friendly          0     0         Not Heard
88:dc:96:30:d9:1b  Friendly          0     0         Not Heard
8a:dc:96:30:d9:1b  Friendly          0     0         Not Heard
9a:dc:96:30:d9:1b  Friendly          0     0         Not Heard
e0:d1:73:02:b7:ab  Friendly          0     0         Not Heard
e0:d1:73:02:b7:af  Friendly          0     0         Not Heard
e0:d1:73:02:bc:2b  Friendly          0     0         Not Heard
e0:d1:73:02:bc:2f  Friendly          0     0         Not Heard
e0:d1:73:02:f6:6b  Friendly          0     0         Not Heard
e0:d1:73:02:f6:6f  Friendly          0     0         Not Heard
e0:d1:73:02:f9:4b  Friendly          0     0         Not Heard
e0:d1:73:02:f9:4f  Friendly          0     0         Not Heard
e0:d1:73:02:fa:4b  Friendly          0     0         Not Heard
e0:d1:73:02:fa:4f  Friendly          0     0         Not Heard
e0:d1:73:02:ff:1b  Friendly          0     0         Not Heard
e0:d1:73:02:ff:1f  Friendly          0     0         Not Heard

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

MAC Address        State              # APs Last Heard
-----------------  ------------------ ----- ----------------------
```

```
Ignore List Configuration


MAC Address

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


Rogue Rule Configuration


Priority         Rule Name                 Rule state Class Type   Notify   State
Match Hit Count

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









Media-Stream Configuration


Multicast-direct State.......................... disable

Allowed WLANs...................................



Stream Name   Start IP                                End IP
Operation Status

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




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 Voice Bandwidth....................... 75
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 insufficent 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 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 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 insufficent 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................ passthrough
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

Service-Name                       LSS   Origin     No SP    Service-string

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

AirTunes                           No    All           0     _raop._tcp.local.

Airplay                            No    All           0     _airplay._tcp.local.

Googlecast                         No    All           0     _googlecast._tcp.local.

HP_Photosmart_Printer_1            No    All           0
_universal._sub._ipp._tcp.local.

HP_Photosmart_Printer_2            No    All           0     _cups._sub._ipp._tcp.local.

HomeSharing                        No    All           0     _home-sharing._tcp.local.

Printer-IPP                        No    All           0     _ipp._tcp.local.

Printer-IPPS                       No    All           0     _ipps._tcp.local.

Printer-LPD                        No    All           0     _printer._tcp.local.

Printer-SOCKET                     No    All           0     _pdl-datastream._tcp.local.

                * -> 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


 Sl No           Service Group Name                        Description
Origin
```

```
 -----    -------------------------------     -------------------------------------
----------

 1         default-mdns-policy                Default Access Policy created by WLC
WLC




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

Domain Name        Gateways           Active Gateway
--------------   ------------------   --------------------
```

```
EoGRE Profile Configuration




 WLAN Express Setup Information.

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




 Flex Avc Profile summary.

  Profile-Name                      Number of Rules  status
  ============                      ===============  ========



 Flex Avc Profile Detailed Configuration.



 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
0     16        50000          5351          5468    /4771    /697
1     64        40000          16626         6250    /4789    /1460
2     128       52800          52677         11550   /11534   /15
3     256       9400           9377          3231    /3225    /5
4     384       6000           287           2812    /670     /2142
5     512       16000          15            9500    /1507    /7992
6     1024      13100          12985         14328   /14213   /115
7     2048      1000           712           2093    /1517    /576
8     4096      1000           74            4093    /389     /3704
```

```
9     Raw-Pool  0              524           290800  /290800  /0
------------------------  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

```
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-----
MIIEowIBAAKCAQEAuhKvGS9womnF7tmM1lOWuzbvMct7u+TDYtoQSNEitAYe5Bjr
XR+tQOT/2b08nJUjVNl91/+3t2i9qUDDU58DTKKir9dmR5ridHlaIyhts8fB7h2a
rZ74YK+4/A1C2mNpmwqwDQlwWhJzJgSe5XeZF0ALTdS3LEggwpuPb6Eo2Wbnqwr0
/tbsRvaeEjwcIGOwmuy1v8TkrbSKeFt9I4B54Pcl3KsxbnnUjH7JIV9h/0nyrOKi
z2P+3maogCnOwxRQp79j/IgCS3JbUBMG14gKnxorJgLuBovqpsWIYO6k/qohIpyg
Vevc0UUj8XiyEun1ldT1SCXYke/I9jauLBB6OQIDAQABAoIBAHjnmw7qXG2r/Qju
IywTNOYBE/tvFL9KLgsVVm96NOp0762W45hm9NSt9/ErnS7BWWvQxoyLhHyQemx3
wHOdZy9snflUJQlyAqNcFs2xf1bJ/aETa2ZVXV61z6U3mLD+16f+kdZmw7JDOr8B
UZ4Y0EjjPHUeOsdzNpY9Lj6CoWBg+V3+TEo3WCqHsqHN8yoVKP30Xnfb1JMgRLf/
infhI6Qg6QKBM++vWQjlUYuM4hbQtQ6HmwWv2epu8YHFdmm3jTSrv+W8lBbY2N5D
N9tZsdUJ54NHiVZTjVmAXCxSpBp3+yTOMRpnzgW0v8MLMhFanjIC5QypG712HIQx
```

gk7LZGECgYEA4vB26UpZNxsOlgzcEQP8fQ82Dk5xNjb9e7qDSD85LUppR6F4xwNs
QPyFVYRemb+pQyIwn1X2SNAdRvsDwSsFVTV9ENi1PzlHbOfaBWE9/VNMaz8vCjfr
teC3So6bIWllHNeoOl8d1wrTOtGZFENH/H4DoOBC7U0aoYjvtnYBplMCgYEA0eaJ
mITPESmZRZI8kaCb/TrWLTZmH2SOCPgC/qVmJ2FiQ8iT3KJXJ5d8ophY84Kay4le
axVUUgIdKNyvNrf038Rx0DirN+qznSKPJuMdY+tnCxaXBjTj/tSwkeiNamZOXHeH
boVlReX6ONDvT+u9MkvMxDmhwBb9G4izw26a88MCgYAhqyFJLTGdPlNkqZXApIHC
IA6aAsNDEtd6kspFXrPh50dFTEx54iUeYxh4/oF2d/vprNnf2cYHOXEOhdEhyHsr
EBt082G4dowFOUScRbgHrGMLCj21W2SKAEPROOUFCPjqVYhs2I25yK5b7Jq0aeL1
L9Dj/kGPqT/JNWKzBEDsZwKBgQDFNt5BN0d20Kb5/xR5n3Xwz788a8g35rqtIplt
uOnqRk2Vcne67a0FvgeUnZ+17BiU9FSKOFgpVWMgaXkW6HBjbqehBB2bRCHOmhH2
b53Fq//9IxRy+G7fl+busJluRwGJT6Un6p3kttgLWgQAC3aQMzgJhjy7xt25aQ+9
p8ZfEQKBgB6jQAT31FxvPFHyjU4NdFeogJd2c2nFbkC7aqOEPKNG9Nbzn/VVWh7x
Rx7Axua3D2OYrCH7V1NcR9X1dInpyj/hYXc5/VdtLZ2yhEc2GiG/jfgNWk2W2BZd
2NLf54bgV67lkC2yKMK/5wBru+V73WmqvWfQ4KsMesLLBBzMRvJa
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIFWzCCBEOgAwIBAgIQAr0FxoUrLR0mLxVp3m/RJzANBgkqhkiG9w0BAQsFADBx
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMTAwLgYDVQQDEydEaWdpQ2VydCBUZXN0IEludGVybWVk
aWF0ZSBSb290IENBIFNIQTIwHhcNMTcwMzE1MDAwMDAwWhcNMTgwMzE1MTIwMDAw
WjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1EMRIwEAYDVQQHEwlSb2Nrdmls
bGUxNzA1BgNVBAoTLk5hdGlvbmFsIEluc3RpdHV0ZSBvZiBTdGFuZGFyZHMgYW5k
IFRlY2hub2xvZ3kxDjAMBgNVBAsTBU5DQ29FMQ8wDQYDVQQDEwZCYXh0ZXIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6Eq8ZL3CiacXu2YzUg5a7Nu8x
y3u75MNi2hBI0SK0Bh7kGOtdH61A5P/ZvTyclSNU2X3X/7e3aL2pQMNTnwNMoqKv
12ZHmuJ0eVojKG2zx8HuHZqtnvhgr7j8DULaY2mbCrANCXBaEnMmBJ7ld5kXQAtN
1LcsSCDCm49voSjZZuerCvT+1uxG9p4SPBwgY7Ca7LW/xOSttIp4W30jgHng9yXc
qzFuedSMfskhX2H/SfKs4qLPY/7eZqiAKc7DFFCnv2P8iAJLcltQEwbXiAqfGism
Au4Gi+qmxYhg7qT+qiEinKBV69zRRSPxeLIS6fWV1PVIJdiR78j2Nq4sEHo5AgMB
AAGjggHVMIIB0TAfBgNVHSMEGDAWgBSJVf2JvOIQPPttTh8w+fmCi1xh4jAdBgNV
HQ4EFgQU3PsIuQqjWZ2eFYrcKNhdYi7Rf1owEQYDVR0RBAowCIIGQmF4dGVyMA4G

```
A1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwgZUG
A1UdHwSBjTCBijBDoEGgP4Y9aHR0cDovL2NybDN0ZXN0LmRpZ2ljZXJ0LmNvbS9E
aWdpQ2VydFRlc3RJbnRlcm1lZGlhdGVTSEEyLmNybDBDoEGgP4Y9aHR0cDovL2Ny
bDN0ZXN0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFRlc3RJbnRlcm1lZGlhdGVTSEEy
LmNybDAhBgNVHSAEGjAYMAwGCmCGSAGG/WxjAQEwCAYGZ4EMAQICMIGDBggrBgEF
BQcBAQR3MHUwKAYIKwYBBQUHMAGGHGh0dHA6Ly9vY3NwdGVzdC5kaWdpY2VydC5j
b20wSQYIKwYBBQUHMAKGPWh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdp
Q2VydFRlc3RJbnRlcm1lZGlhdGUtU0hBMi5jcnQwDAYDVR0TAQH/BAIwADANBgkq
hkiG9w0BAQsFAAOCAQEAe7Rc6PbIfEjSQpCZ3UpZ7zqWruov44nmSKvR/X4MJITM
z9k3S+TzGOGYnq7bHBF1mjLt0l5K/BDWSG6LY5clSYJuGCbC/dSNFk9G+lzBKs5S
5xJxk8HeAt4OHOWmtEhZ7S4np7zUBcRu1koHbw4vW/lYJBvxRF1Sdd0ypyBP4X81
D2mX+LmFo2rlLSExurr5rd1s6Pna2FRBEjoyM78ID9AmKENqeioDi+hxGLlQROOt
y7aZU8yWcec7nad9iUGO/pMDdhbWexpvp4CBihxYkUMQcf8RaqTkJM8fLAdvPq9P
oQuBuMi+qPtI3WkTgfwr49usBzgbrdNPc/5MRQEz8Q==
-----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
UzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQu
Y29tMSMwIQYDVQQDExpEaWdpQ2VydCBUZXN0IFJvb3QgQ0EgU0hBMjAeFw0wNjEx
MTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMHExCzAJBgNVBAYTAlVTMRUwEwYDVQQK
EwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5jb20xMDAuBgNV
BAMTJ0RpZ2lDZXJ0IFRlc3QgSW50ZXJtZWRpYXRlIFJvb3QgQ0EgU0hBMjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJiahU+gQ8Brmcov1LwvynLKgxMc
buqjeyYeiDEUXtTEJKoPm1Pc5YE39fBY1ydwaBJ6k3LbLZM+zqw2pCXwaf4LBhLv
t4ppHMfXlgI2IVpWibSYVcvJ4waD09AQ47u/SQhDHSVf17HRUIs1tIw+MMpMyGH0
9YzgI/ZI5KTWBY+nlnz9t1/RpPdcJfAWin3T/s7xNu364OFDURX+3Rxb7bVnV1xI
```

GZUwQx23GGcSnypsflr1rBc2yvXaUnwl4DbQMUo10tdZtd1wZNQE3C1L3MXndvn0
WdFB4cM6kQlSky0RFW+TJqQIMmb29n09P/ez7Ipo0cpV3vlBAC0DWm2z/FMCAwEA
AaOCAvQwggLwMA4GA1UdDwEB/wQEAwIBhjCCAcYGA1UdIASCAb0wggG5MIIBtQYL
YIZIAYb9bAEDAAIwggGkMDoGCCsGAQUFBwIBFi5odHRwOi8vd3d3LmRpZ2ljZXJ0
LmNvbS9zc2wtY3BzLXJlcG9zaXRvcnkuaHRtMIIBZAYIKwYBBQUHAgIwggFWHoIB
UgBBAG4AeQAgAHUAcwBlACAAbwBmACAAdABoAGkAcwAgAEMAZQByAHQAaQBmAGkA
YwBhAHQAZQAgAGMAbwBuAHMAdABpAHQAdQB0AGUAcwAgAGEAYwBjAGUAcAB0AGEA
bgBjAGUAIABvAGYAIAB0AGgAZQAgAEQAaQBnAGkAQwBlAHIAdAAgAEMAUAAvAEMA
UABTACAAYQBuAGQAIAB0AGgAZQAgAFIAZQBsAHkAaQBuAGcAIABQAGEAcgB0AHkA
IABBAGcAcgBlAGUAbQBlAG4AdAAgAHcAaABpAGMAaAAgAGwAaQBtAGkAdAAgAGwA
aQBhAGIAaQBsAGkAdAB5ACAAYQBuAGQAIABhAHIAZQAgAGkAbgBjAG8AcgBwAG8A
cgBhAHQAZQBkACAAaABlAHIAZQBpAG4AIABiAHkAIAByAGUAZgBlAHIAZQBuAGMA
ZQAuMA8GA1UdEwEB/wQFMAMBAf8wOAYIKwYBBQUHAQEELDAqMCgGCCsGAQUFBzAB
hhxodHRwOi8vb2NzcHRlc3QuZGlnaWNlcnQuY29tMIGIBgNVHR8EgYAwfjA9oDug
OYY3aHR0cDovL2NybDN0ZXN0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFRlc3RSb290
Q0FTSEEyLmNybDA9oDugOYY3aHR0cDovL2NybDR0ZXN0LmRpZ2ljZXJ0LmNvbS9E
aWdpQ2VydFRlc3RSb290Q0FTSEEyLmNybDAdBgNVHQ4EFgQUiVX9ibziEDz7bU4f
MPn5gotcYeIwHwYDVR0jBBgwFoAU9kZ+Gxa7N5lj9z/YhSzkyepYDx4wDQYJKoZI
hvcNAQELBQADggEBALFxPxkcHgaXBuoZ10FGWsq3bybGnxC6llfDETcWVrPajudx
asm8EXOTSVnqKNIXZTlm1BY0chhnVGA3YyNN7XF7XrT1HtRH5NDhWO2lzFEGSFLw
hlCiGQBuzKOelbBWDhpN7icm+Y/u+DPaK6oFu0tX/u9kPzoc8OYSBe412sHAD1/l
kUDPAEO4yHSXDnoe0fhk24/yCuO6Wc+mMe7YXzEkq8pOEWjNw/9E1dsP20L7jD3F
97q5uVNe1wEaeE3U5Eq1xKUBdyQqitinpTv/yo/UPTDLpfjBmK2nh2HK6r0RH+YC
OicqQ99N+q6YeAlhejLa7+7FkKYKK1YEAbE1Icc=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDpjCCAo6gAwIBAgIBMzANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQGEwJVUzEV
MBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29t
MSMwIQYDVQQDExpEaWdpQ2VydCBUZXN0IFJvb3QgQ0EgU0hBMjAeFw0wNjExMTAw
MDAwMDBaFw0zMTExMTAwMDAwMDBaMGQxCzAJBgNVBAYTAlVTMRUwEwYDVQQKEwxE
aWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5jb20xIzAhBgNVBAMT

GkRpZ2lDZXJ0IFRlc3QgUm9vdCBDQSBTSEEyMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEA0DLGgpMXqI2YZ15ULS61yqyqiBMpmRtM9/w/1pqoA/GEri19
VMFuvtPTWgu9IQf0dQsRMy2d8V4INSj43YyQeXnxPzanTSqza95yoH/h4xUM/pNq
AlXlO8c+cYMyCDzTQ0vrEWcvPZOtXYABac9E9ceT015RdD5pORjMwTcb6NxydZr8
nRd9/J66L4R17IKvTU74IwA6fwNd0UnXbhVhGdeEAe+eIEvJ5WlWxDeS6ZdZuSZv
h24QxhxpucTzSq81HHCHw4a1kOel2oqlDlUY698atS0nxfw3IR30heQ/g793Mce9
SX9u2dPPAZtSaW8/38TwKbNOa9zkRFn7oF+cZQIDAQABo2MwYTAOBgNVHQ8BAf8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU9kZ+Gxa7N5lj9z/YhSzk
yepYDx4wHwYDVR0jBBgwFoAU9kZ+Gxa7N5lj9z/YhSzkyepYDx4wDQYJKoZIhvcN
AQELBQADggEBAAeQacFm1sFPOIEvXDVi3IH2RKF7he0p/M0bK2Soj137LMf+ctpM
3bFKJPY97YIE0g7T1qgR8TN2sK0moumMTPjWCdFWJyN4yakS6tPIWEG2XobJ9H1r
iuVXLKd2M/1yhqUyt1o5KtbOGQXLFd3qdp4A1tcXuK2wyMTiSCYS3Uow61JdEw6M
eyrMIpZl9GtvaXTz6LdnozAbhKC7bVUy7ob0T4E03fQ8hIQCNPupvY7Db1/XmIw8
QWVd6AOH7EE3P8xbWOvcTWZ5XbstWY014GeJFXZ7YreaAg8sYa6CzasuHkr/rxeZ
8yzOmCTTTSPk5Ju5bTfAyEpgkl5fDvntJQg=
-----END CERTIFICATE-----

Appendix C Acronyms

AAMI	Advancement of Medical Instrumentation
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
APT	Advanced Persistent Threat
ASA	Adaptive Security Appliance
ASM	Alaris System Maintenance
ATP:N	Advanced Threat Protection: Network
BD	Becton, Dickinson and Company
CAPWAP	Control and Provisioning of Wireless Access Points
CFC	Cybersecurity Framework Core
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COI	Community of Interest
CRADA	Cooperative Research and Development Agreement
DCS:SA	Data Center Security: Server Advanced
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EHR	Electronic Health Record
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
HDO	Healthcare Delivery Organization
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
HTTPS	Hypertext Transfer Protocol Secure

ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
ISE	Identity Services Engine
ISO	International Standards Organization
IT	Information Technology
ITAM	Information Technology Asset Management
KRACK	Key Reinstallation Attack
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LVP	Large Volume Pump
MAC	Media Access Control
MAUDE	Manufacturer and User Facility Device Experience
MDISS	Medical Device Innovation, Safety & Security Consortium
MDRAP	Medical Device Risk Assessment Platform
MSSP	Managed Security Service Provider
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OSPF	Open Shortest Path First
PAC	Process Access Control
PCU	Patient Care Unit
PHI	Protected Health Information
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial-In User Service
RDP	Remote Desktop Protocol

RFID	Radio-Frequency Identification
RMF	Risk Management Framework
RTLS	Real-Time Locating Systems
SD	Secure Digital
SEP	Symantec Endpoint Protection
SIEM	Security Information and Events Management
SOC	Security Operations Center
SP	Special Publication
SSID	Service Set Identifier
SSO	Single Sign-On
TCP	Transmission Control Protocol
TIR	Technical Information Report
TLS	Transport Layer Security
U.S.	United States
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WLC	Wireless LAN Controller
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II

Appendix D References

[1] J. Moy, *OSPF Version 2*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 2328, April 1998. https://www.ietf.org/rfc/rfc2328.txt [accessed 2/7/18].

[2] *Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide, 9.6*, Cisco [Web site], http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start/asav-quick/intro-asav.html [accessed 2/7/18].

[3] D. Bider and M. Baushke, *SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 6668, July 2012. https://tools.ietf.org/html/rfc6668 [accessed 2/7/18].

[4] J. Postel, *Internet Control Message Protocol: DARPA Internet Program Protocol Specification*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 792, September 1981. https://tools.ietf.org/html/rfc792 [accessed 2/7/18].

[5] J. Case, M. Fedor, M. Schoffstall, and J. Davin, *A Simple Network Management Protocol (SNMP)*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 1157, May 1990. https://tools.ietf.org/html/rfc1157 [accessed 2/7/18].

[6] R. Droms, *Dynamic Host Configuration Protocol*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 2131, March 1997. https://www.ietf.org/rfc/rfc2131.txt [accessed 2/7/18].

[7] Institute of Electrical and Electronics Engineers (IEEE), *Bridges and Bridged Networks*, IEEE 802.1Q, 2014. http://www.ieee802.org/1/pages/802.1Q-2014.html [accessed 2/7/18].

[8] *Catalyst 3650 Switch Getting Started Guide*, Cisco [Web site], http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/hardware/quick/guide/cat3650_gsg.html [accessed 2/7/18].

[9] Institute of Electrical and Electronics Engineers (IEEE), *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements*, 802.11i, 2004. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1318903 [accessed 2/7/18].

[10] *Virtual Wireless LAN Controller Deployment Guide 8.2*, Cisco [Web site], http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Virtual_Wireless_LAN_Controller_Deployment_Guide_8-2.html [accessed 2/7/18].

[11] D. Mills, J. Martin, Ed., J. Burbank, and W. Kasch, *Network Time Protocol Version 4: Protocol and Algorithms Specification*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 5905, June 2010. https://www.ietf.org/rfc/rfc5905.txt [accessed 2/7/18].

[12] U.S. Department of Commerce. *Announcing the Advanced Encryption Standard (AES)*, Federal Information Processing Standards (FIPS) Publication 197, November 2001. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [accessed 2/7/18].

[13] *Cisco Wireless Controller Configuration Guide, Release 8.0*, Cisco [Web site], http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80.html [accessed 2/7/18].

[14] D. Simon, B. Aboba, and R. Hurst, *The EAP-TLS Authentication Protocol*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 5216, March 2008. https://www.ietf.org/rfc/rfc5216.txt [accessed 2/7/18].

[15] C. Rigney, S. Willens, A. Rubens, and W. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 2865, June 2000. https://tools.ietf.org/html/rfc2865 [accessed 2/7/18].

[16] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 6960, June 2013. https://tools.ietf.org/html/rfc6960 [accessed 2/7/18].

[17] *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 MP1 Planning and Deployment Guide*, Symantec [Web site], http://help.symantec.com/cs/DCS6.7/DCS6_7/v118490468_v110163010/Installing-Data-Center-Security:-Server-Advanced-6.7-or-6.7-MP1/?locale=EN_US [accessed 2/7/18].