

NIST SPECIAL PUBLICATION 1800-8

Securing Wireless Infusion Pumps In Healthcare Delivery Organizations

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B),
and How-To Guides (C)

DRAFT

**Gavin O'Brien
Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng**

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



NIST SPECIAL PUBLICATION 1800-8

Securing Wireless Infusion Pumps In Healthcare Delivery Organizations

*Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B),
and How-To Guides (C)*

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*

DRAFT

May 2017



U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Kent Rochford, Acting Undersecretary of Commerce for Standards and Technology and Director

NIST SPECIAL PUBLICATION 1800-8A

Securing Wireless Infusion Pumps

In Healthcare Delivery Organizations

Volume A:
Executive Summary

DRAFT

Gavin O'Brien

National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards

Kevin Littlefield

Neil McNab

Sue Wang

Kangmin Zheng

The MITRE Corporation
McLean, VA

May 2017

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



Executive Summary

- 1 ▪ Broad technological advancements have contributed to the Internet of Things (IoT)
2 phenomenon, where physical devices now have technology that allow them to connect to the
3 internet and communicate with other devices or systems.ⁱ With billions of devices being
4 connected to the internet,ⁱⁱ many industries, including healthcare, have or are beginning to
5 leverage IoT devices to improve operational efficiency and enhance innovation.
- 6 ▪ Medical devices, such as infusion pumpsⁱⁱⁱ, were once standalone instruments that interacted
7 only with the patient or medical provider. With technological improvements designed to
8 enhance patient care, these devices now connect wirelessly to a variety of systems, networks,
9 and other tools within a healthcare delivery organization (HDO) – ultimately contributing to the
10 Internet of Medical Things (IoMT).
- 11 ▪ As IoMT grows, cybersecurity risks have risen. According to the Association for the
12 Advancement of Medical Instrumentation (AAMI) Technical Information Report 57 (TIR57), “this
13 has created a new source of risk for [the] safe operation [of medical devices].”^{iv} In particular, the
14 wireless infusion pump ecosystem (the pump, the network, and the data stored in and on a
15 pump) face a range of threats, including unauthorized access to protected health information
16 (PHI), changes to prescribed drug doses, and interference with a pump’s function.
- 17 ▪ In addition to managing interconnected medical devices, HDOs oversee complex, highly
18 technical environments, from back-office applications for billing and insurance services, supply
19 chain and inventory management, and staff scheduling to clinical systems such as radiological
20 and pharmaceutical support. In this intricate healthcare environment, HDOs and medical device
21 manufacturers that share responsibility and take a collaborative, holistic approach to reducing
22 cybersecurity risks of the infusion pump ecosystem can better protect healthcare systems,
23 patients, PHI, and enterprise information.
- 24 ▪ The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards
25 and Technology (NIST) analyzed risk factors in and around the infusion pump ecosystem using a
26 questionnaire-based risk assessment. With the results of that assessment, the NCCoE then
27 developed an example implementation that demonstrates how HDOs can use standards-based,
28 commercially available cybersecurity technologies to better protect the infusion pump
29 ecosystem, including patient information and drug library dosing limits.

30 CHALLENGE

31 Technology improvements happen rapidly across all sectors. For organizations focused on streamlining
32 operations and delivering high-quality patient care, it can be difficult to take advantage of the latest
33 technological advances, while also ensuring new medical devices or applications are secure. For many
34 HDOs, this can result in improperly configured information technology networks and components that
35 increase cybersecurity risks.

36 Unlike prior medical devices that were once standalone instruments, today’s wireless infusion pumps
37 connect to a variety of healthcare systems, networks, and other devices. Although connecting infusion
38 pumps to point-of-care medication systems and electronic health records (EHRs) can improve healthcare
39 delivery processes, using a medical device’s connectivity capabilities can create significant cybersecurity
40 risk, which could lead to operational or safety risks. Tampering, intentional or otherwise, with the

41 wireless infusion pump ecosystem can expose a healthcare provider’s enterprise to serious risks, such
42 as:

- 43 ▪ access by malicious actors
- 44 ▪ loss or corruption of enterprise information and patient data and health records
- 45 ▪ a breach of protected health information
- 46 ▪ loss or disruption of healthcare services
- 47 ▪ damage to an organization’s reputation, productivity, and bottom-line revenue

48 As IoMT grows, with an increasing number of infusion pumps connecting to networks, the vulnerabilities
49 and risk factors become more critical as they can expose the pump ecosystem to external attacks,
50 compromises, or interference.

51 SOLUTION

52 The NCCoE has developed cybersecurity guidance, NIST Special Publication 1800-8 *Securing Wireless*
53 *Infusion Pumps*, using standards-based commercially available technologies and industry best practices
54 to help HDOs strengthen the security of the wireless infusion pump ecosystem within healthcare
55 facilities.

56
57 This NIST cybersecurity publication provides best practices and detailed guidance on how to manage
58 assets, protect against threats, and mitigate vulnerabilities by performing a questionnaire-based risk
59 assessment. In addition, the security characteristics of wireless infusion pump ecosystem are mapped to
60 currently available cybersecurity standards and the Health Insurance Portability and Accountability Act
61 (HIPAA) Security Rule. Based on our risk assessment findings, we apply security controls to the pump’s
62 ecosystem to create a ‘defense-in-depth’ solution for protecting infusion pumps and their surrounding
63 systems against various risk factors. Ultimately, we show how biomedical, networking, and cybersecurity
64 engineers and IT professionals can securely configure and deploy wireless infusion pumps to reduce
65 cybersecurity risk.

66
67 Although the NCCoE used a suite of commercially available tools and technologies to address wireless
68 infusion pump cybersecurity challenges, this guide does not endorse any specific products, nor does it
69 guarantee compliance with any regulatory initiatives. Your organization’s information security experts
70 can identify solutions that will best integrate with your organization’s current tools and IT system
71 infrastructure. Your organization may choose to adopt this solution, or one that adheres to these
72 guidelines, or you may refer to this guide as a starting point for tailoring and implementing specific parts
73 that best suit your organization’s risk profile and needs.

74 BENEFITS

75 The NCCoE’s practice guide to securing the wireless infusion pump ecosystem can help your
76 organization:

- 77 ▪ reduce cybersecurity risk, and potentially reduce impact to safety and operational risk, such as
78 the loss of patient information or interference with the standard operation of a medical device
- 79 ▪ develop and execute a defense-in-depth strategy that protects the enterprise with layers of
80 security to avoid a single point of failure and provide strong support for availability

- 81 ▪ implement current cybersecurity standards and best practices, while maintaining the
82 performance and usability of wireless infusion pumps

83 **SHARE YOUR FEEDBACK**

84 You can view or download the guide at https://nccoe.nist.gov/projects/use_cases/medical_devices.
85 Help the NCCoE make this guide better by sharing your thoughts with us. We recognize that technical
86 solutions alone will not fully enable the benefits of a cybersecurity solution, so we encourage
87 organizations to share their lessons learned and best practices for transforming the processes associated
88 with implementing these guidelines. To provide comments or to learn more by arranging a
89 demonstration of this reference solution, contact the NCCoE at hit_nccoe@nist.gov.

90

91 **TECHNOLOGY PARTNERS/COLLABORATORS**

92 Technology vendors who participated in this project submitted their capabilities in response to a call in
93 the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and
94 Development Agreement with NIST, allowing them to participate in a consortium to build this example
95 solution.



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

100

101 The National Cybersecurity Center of Excellence (NCCoE), a part of the National
102 Institute of Standards and Technology (NIST), is a collaborative hub where
103 industry organizations, government agencies, and academic institutions work
104 together to address businesses’ most pressing cybersecurity challenges. Through
this collaboration, the NCCoE applies standards and best practices to develop
modular, easily adaptable example cybersecurity solutions using commercially
available technology.

LEARN MORE
<https://nccoe.nist.gov>
nccoe@nist.gov
301-975-0200

ⁱ *Internet of Things*, Gartner IT Glossary, <http://www.gartner.com/it-glossary/internet-of-things/> [accessed 4/5/2017].

ⁱⁱ *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*, IEEE Spectrum, 2016.
<http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated> [accessed 4/5/2017].

ⁱⁱⁱ Defined by the Food and Drug Administration (FDA) as “a medical device that delivers fluids into a patient’s body in a controlled manner, either through the use of interconnected servers or via a standalone drug library-based medication delivery system.”
<https://www.fda.gov/medicaldevices/productsandmedicalprocedures/generalhospitaldevicesandsupplies/infusionpumps/default.htm> [accessed 4/5/2017].

^{iv} *Principles of Medical Device Security*, Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report (TIR) 57, 2016, ix pp.

NIST SPECIAL PUBLICATION 1800-8B

Securing Wireless Infusion Pumps

In Healthcare Delivery Organizations

Volume B:
Approach, Architecture, and Security Characteristics

DRAFT

Gavin O'Brien

National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards

Kevin Littlefield

Neil McNab

Sue Wang

Kangmin Zheng

The MITRE Corporation
McLean, VA

May 2017

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



DRAFT

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 1800-8B Natl. Inst. Stand. Technol. Spec. Publ. 1800-8B, 90 pages, (May 2017), CODEN: NSPUE2

FEEDBACK

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

The NCCoE at NIST analyzed risk factors in and around the infusion pump ecosystem using a questionnaire-based risk assessment to develop an example implementation that demonstrates how

HDOs can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.

This practice guide will help HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk, while maintaining the performance and usability of wireless infusion pumps.

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

Name	Organization
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	MDISS
Jay Stevens	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 vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products were invited to sign a Cooperative

Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Baxter Healthcare Corporation	<ul style="list-style-type: none"> • Sigma Spectrum LVP, version 8 • Sigma Spectrum Wireless Battery Module, version 8 • Sigma Spectrum Master Drug Library, version 8 • CareEverywhere Gateway Server, version 14
B. Braun Medical Inc.	<ul style="list-style-type: none"> • Infusomat® Space Infusion System/ Large Volume Pumps • DoseTrac® Infusion Management Software/ Infusion Pump Software
Becton, Dickinson and Company (BD)	<ul style="list-style-type: none"> • Alaris® 8015 PC Unit v9.19.2 • Alaris® Syringe Module 8110 • Alaris® LVP Module 8100 • Alaris® Systems Manager v4.2 • Alaris® System Maintenance (ASM) v 10.19
Cisco	<ul style="list-style-type: none"> • Access Point (AIR-CAP1602I-A-K9) • Wireless LAN Controller 8.2.111.0 • Cisco ISE • Cisco: ASA Catalyst 3650 Switch
Clearwater Compliance	Clearwater: IRM Pro
DigiCert	CertCentral management account / Certificate Authority
Hospira Inc., a Pfizer Company (ICU Medical)	<ul style="list-style-type: none"> • Plum 360™ Infusion System, version 15.10 • LifeCare PCA™ Infusion System, version 7.02 • Hospira MedNet™, version 6.2

Technology Partner/Collaborator	Build Involvement
Intercede	MyID
MDISS	MDRAP
PFP Cybersecurity	Device Monitor
Ramparts	Risk Assessment
Smiths Medical	<ul style="list-style-type: none"> • Medfusion® 3500 V5 syringe infusion system • PharmGuard® Toolbox v1.5 • Medfusion 4000® Wireless Syringe Infusion Pump • CD, PHARMGUARD® TOOLBOX 2, V3.0 use with Medfusion® 4000 and 3500 V6 (US) • PharmGuard® Server Licenses, PharmGuard® Server Enterprise Edition, V1.1 • CADD®-Solis Ambulatory Infusion Pump • CADD™-Solis Medication Safety Software
Symantec Corporation	<ul style="list-style-type: none"> • Endpoint Protection (SEP) • Advanced Threat Protection: Network (ATP:N) • Server Advanced - DataCenter Security (DCS:SA):
TDi Technologies, Inc.	ConsoleWorks

Contents

1	Summary	1
1.1	Challenge	2
1.2	Solution	3
1.3	Benefits	4
2	How to Use This Guide	5
2.1	Typographical Conventions	6
3	Approach	7
3.1	Audience	8
3.2	Scope	8
3.2.1	Assumptions	8
3.2.2	Security	8
3.2.3	Existing Infrastructure	8
3.2.4	Technical Implementation	9
3.2.5	Capability Variation	9
4	Risk Assessment and Mitigation	9
4.1	Risk Assessments	11
4.1.1	Industry Analysis of Risk	11
4.1.2	Questionnaire-based Risk Assessment	12
4.1.3	Assets	12
4.1.4	Threats	12
4.1.5	Vulnerabilities	13
4.1.6	Risks	14
4.1.7	Recommendations and Best Practices	16
4.2	Risk Response Strategy	16
4.2.1	Risk Mitigation	17
4.3	Security Characteristics and Controls Mapping	18
4.4	Technologies	24

- 5 Architecture..... 31**
 - 5.1 Basic System..... 31
 - 5.2 Data Flow..... 32
 - 5.3 Cybersecurity Controls 33
 - 5.3.1 Network Controls33
 - 5.3.2 Pump Controls.....49
 - 5.3.3 Pump Server Controls50
 - 5.3.4 Enterprise Level Controls54
 - 5.4 Final Architecture..... 55
- 6 Life Cycle Cybersecurity Issues..... 56**
 - 6.1 Procurement..... 57
 - 6.2 Operation..... 57
 - 6.3 Maintenance..... 58
 - 6.4 Disposal..... 58
- 7 Security Characteristics Analysis..... 59**
 - 7.1 Assumptions and Limitations..... 59
 - 7.2 Application of Security Characteristics..... 59
 - 7.2.1 Supported CSF Subcategories59
 - 7.3 Security Analysis Summary..... 62
- 8 Functional Evaluation..... 63**
 - 8.1 Functional Test Plan 63
 - 8.1.1 Test Case: WIP-1.....64
 - 8.1.2 Test Case: WIP-2.....64
 - 8.1.3 Test Case: WIP-3.....65
 - 8.1.4 Test Case: WIP-4.....66
 - 8.1.5 Test Case: WIP-5.....66
 - 8.1.6 Test Case: WIP-6.....67
 - 8.1.7 Test Case: WIP-7.....68
- 9 Future Build Considerations 69**

Appendix A Threats.....	70
Appendix B Vulnerabilities.....	72
Appendix C Recommendations and Best Practices.....	75
Appendix D References.....	77

List of Figures

Figure 4-1: Tiered Risk Management Approach (NIST SP 800-37)	10
Figure 4-2: Relationship between Security and Safety Risks (AAMI TIR 57)	11
Figure 5-1: Basic System	32
Figure 5-2: Network Architecture with Segmentation	37
Figure 5-3: Wi-Fi Management	38
Figure 5-4: Wi-Fi Authentication	39
Figure 5-5: Wi-Fi Device Access	40
Figure 5-6: Network Access Control	43
Figure 5-7: Remote Access VPN	44
Figure 5-8: Remote Access	46
Figure 5-9: External	48
Figure 5-10: Pump Server Protection	53
Figure 5-11: Target Architecture	55
Figure 6-1: Asset Life Cycle.....	56

List of Tables

Table 4-1: Security Characteristics and Controls Mapping - NIST Cyber Security Framework	19
Table 4-2: Products and Technologies.....	24

1 **1 Summary**

2 Medical devices, such as infusion pumps, were once standalone instruments that interacted only with
3 the patient or medical provider [1]. With technological improvements designed to enhance patient care,
4 these devices now connect wirelessly to a variety of systems, networks, and other tools within a
5 healthcare delivery organization (HDO) – ultimately contributing to the Internet of Medical Things
6 (IoMT).

7 In addition to managing interconnected medical devices, HDOs oversee complex, highly technical
8 environments, from back-office applications for billing and insurance services, supply chain and
9 inventory management, and staff scheduling to clinical systems such as radiological and pharmaceutical
10 support. In this intricate healthcare environment, HDOs and medical device manufacturers that share
11 responsibility and take a collaborative, holistic approach to reducing cybersecurity risks of the wireless
12 infusion pump ecosystem can better protect healthcare systems, patients, PHI, and enterprise
13 information.

14 The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and
15 Technology (NIST) developed an example implementation that demonstrates how HDOs can use
16 standards-based, commercially available cybersecurity technologies to better protect the wireless
17 infusion pump ecosystem, including patient information and drug library dosing limits.

18 The NCCoE’s project has resulted in a NIST Cybersecurity Practice Guide, *Securing Wireless Infusion*
19 *Pumps*, that addresses how to manage this challenge in clinical settings with a reference design and
20 example implementation. Our example solution starts with two types of risk assessments: an industry
21 analysis of risk and a questionnaire-based-risk assessment. With the results of that assessment, we then
22 used a defense-in-depth strategy to secure the pump, server components, and surrounding network to
23 create a better protected environment for wireless infusion pumps.

24 The solution and architectures presented here are built upon standards-based, commercially available
25 products and represent one of many possible solutions and architectures. The example implementation
26 can be used by any organization that is deploying wireless infusion pump systems and is willing to
27 perform their own risk assessment and implement controls based on their risk posture.

28 For ease of use, here is a short description of the different sections of this volume.

29 **Section 1: [Summary](#)** presents the challenge addressed by the NCCoE project, with an in-depth look at
30 our approach, the architecture, and the security characteristics we used; the solution demonstrated to
31 address the challenge; benefits of the solution; and the technology partners that participated in
32 building, demonstrating, and documenting the solution. The Summary also explains how to provide
33 feedback on this guide.

34 **Section 2: [How to Use This Guide](#)** explains how readers like you—business decision makers, program
35 managers, information technology (IT) professionals (e.g., systems administrators), and biomedical
36 engineers—might use each volume of the guide.

37 **Section 3: [Approach](#)** offers a detailed treatment of the scope of the project, describes the assumptions
38 on which the security platform development was based, the risk assessment that informed platform
39 development, and the technologies and components that industry collaborators gave us to enable
40 platform development.

41 **Section 4: [Risk Assessment and Mitigation](#)** highlights the risks we found, along with the potential
42 response and mitigation efforts that can help lower risks for HDOs.

43 **Section 5: [Architecture](#)** describes the usage scenarios supported by project security platforms, including
44 Cybersecurity Framework functions supported by each component contributed by our collaborators.

45 **Section 6: [Life Cycle Cybersecurity Issues](#)** discusses cybersecurity considerations from a product life
46 cycle perspective including: procurement, maintenance, end of life.

47 **Section 7: [Security Characteristics Analysis](#)** provides details about the tools and techniques we used to
48 perform risk assessments pertaining to wireless infusion pumps.

49 **Section 8: [Functional Evaluation](#)** summarizes the test sequences we employed to demonstrate security
50 platform services, the Cybersecurity Framework functions to which each test sequence is relevant, and
51 the NIST SP 800-53-4 controls that applied to the functions being demonstrated.

52 **Section 9: [Future Build Considerations](#)** is a brief treatment of other applications that NIST might explore
53 in the future to further support wireless infusion pump cybersecurity.

54 Appendices provide acronym translations, references, a mapping of the wireless infusion pump project
55 to the Cybersecurity Framework Core (CFC), and a list of additional informative security references cited
56 in the CFC.

57 **1.1 Challenge**

58 The Food and Drug Administration (FDA) defines an *external infusion pump* as a medical device that
59 delivers fluids into a patient’s body in a controlled manner, using interconnected servers or via a
60 standalone drug library-based medication delivery system [1]. In the past, infusion pumps were
61 standalone instruments that interacted only with the patient and the medical provider. Now,
62 connecting infusion pumps to point-of-care medication systems and electronic health records (EHRs)
63 can help improve healthcare delivery processes, but using a medical device’s connectivity capabilities
64 can also create cybersecurity risk, which could lead to operational or safety risks.

65 Wireless infusion pumps are challenging to protect for several reasons. They can be infected by
66 malware, which can cause them to malfunction or operate differently than originally intended. And
67 traditional malware protection could negatively impact the pump’s ability to operate efficiently. In

68 addition, most wireless infusion pumps contain a maintenance default passcode. If HDOs do not change
69 the default passcodes when provisioning pumps, nor periodically change the passwords after pumps are
70 deployed, this creates a vulnerability. This can make it difficult to revoke access codes when a hospital
71 employee resigns from the job, for example. Furthermore, information stored inside infusion pumps
72 also must be properly secured, including data from drug library systems, infusion rates and dosages, or
73 protected health information (PHI) [2], [3], [4], [5], [6].

74 Additionally, like other devices with operating systems and software that connect to a network, the
75 wireless infusion pump ecosystem creates a large *attack surface* (i.e., the different points where an
76 attacker could get into a system, and where they could exfiltrate data out), primarily due to
77 vulnerabilities in operating systems, subsystems, networks or default configuration settings that allow
78 for possible unauthorized access [6], [7], [8]. Because many infusion pump models can be accessed and
79 programmed remotely through a healthcare facility's wireless network, this vulnerability could be
80 exploited to allow an unauthorized user to interfere with the pump's function, harming a patient
81 through incorrect drug dosing or the compromise of that patient's PHI.

82 These risk factors are real, exposing the wireless pump ecosystem to external attacks, compromise or
83 interference [6], [8], [9]. Digital tampering, intentional or otherwise, with a wireless infusion pump's
84 ecosystem (the pump, the network, and data in and on the pump) can expose a healthcare delivery
85 organization (HDO) to critical risk factors, such as malicious actors; loss of data; a breach of PHI; loss of
86 services; loss of health records; the potential for downtime; and damage to an HDO's reputation,
87 productivity, and bottom-line revenue.

88 This practice guide helps you address your assets, threats, and vulnerabilities by demonstrating how to
89 perform a questionnaire-based risk assessment survey. After you complete the assessment, you can
90 apply security controls to the infusion pumps in your area of responsibility to create a defense-in-depth
91 solution to protect them from cybersecurity risks.

92 1.2 Solution

93 The NIST Cybersecurity Practice Guide *Securing Wireless Infusion Pumps* shows how biomedical
94 engineers, networking engineers, security engineers and IT professionals, using commercially available,
95 open source tools and technologies that are consistent with cybersecurity standards, can help securely
96 configure and deploy wireless infusion pumps within HDOs.

97 In addition, the security characteristics of wireless infusion pump ecosystem are mapped to currently
98 available cybersecurity standards and the Health Insurance Portability and Accountability Act (HIPAA)
99 Security Rule. In developing our solution, we used standards and guidance from:

- 100 ▪ NIST Framework for Improving Critical Infrastructure Cybersecurity (commonly known as the
101 NIST CSF) [10]
- 102 ▪ NIST Risk Management Framework (RMF) [11], [12], [13]

- 103 ▪ NIST SP 800-53rev4 Security and Privacy Controls for Federal Information Systems and
104 Organizations [14]
- 105 ▪ Association for the Advancement of Medical Instrumentation (AAMI) Technical Information
106 Report (TIR) 57 [9]
- 107 ▪ International Electrotechnical Commission (IEC) 80001 and 80002 risk management for IT
108 networks incorporating medical devices [15], [16], [17], [18], [19]
- 109 ▪ Food and Drug Administration’s (FDA) Postmarket Management of Cybersecurity in Medical
110 Devices for building block standards for any medical device cybersecurity solution.

111 Ultimately, this practice guide:

- 112 ▪ maps security characteristics to standards and best practices from NIST and other standards
113 organizations, to the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
114 Security Rule [10], [14], [20], [21], [22]
- 115 ▪ provides a detailed architecture and capabilities that address security controls
- 116 ▪ provides a how-to for implementers and security engineers to recreate the reference design
- 117 ▪ is modular and uses products that are readily available and interoperable with existing IT
118 infrastructure and investments.

119 Your organization may choose to adopt this example solution, or one that adheres to these guidelines,
120 or you may refer to this guide as a starting point for tailoring and implementing specific parts that best
121 suit your organization’s needs. Although the NCCoE used a suite of commercially available tools and
122 technologies to address wireless infusion pump cybersecurity challenges, this guide does not endorse
123 any specific products, nor does it guarantee compliance with any regulatory initiatives. Refer to your
124 organization's information security experts to identify solutions that will best integrate with your
125 organization’s current tools and IT system infrastructure.

126 1.3 Benefits

127 The example solution presented in this practice guide offers several benefits, including:

- 128 ▪ illustrating cybersecurity standards and best practice guidelines to better secure the wireless
129 infusion pump ecosystem, such as the hardening of operating systems, segmenting the
130 network, white listing, code-signing, and using certificates for both authorization and
131 encryption, maintaining the performance and usability of wireless infusion pumps
- 132 ▪ reducing risks from the compromise of information, including the potential for breach or loss of
133 protected health information (PHI), as well as not allowing these medical devices to be used for
134 anything other than the intended purposes
- 135 ▪ documenting a defense-in-depth strategy to introduce layers of cybersecurity controls that
136 avoid a single point of failure and provide strong support for availability. This strategy may
137 include a variety of tactics: using network segmentation to isolate business units and user

- 138 access; applying firewalls to manage and control network traffic; hardening and enabling device
 139 security features to reduce zero-day exploits; and implementing strong network authentication
 140 protocols and proper network encryption, monitoring, auditing and intrusion detection and
 141 prevention services (IDS/IPS).
- 142 ▪ highlighting best practices for procurement of wireless infusion pumps by including the need for
 143 cybersecurity features at the point of purchase
 - 144 ▪ calling upon industry to create new best practices for healthcare providers to consider when on-
 145 boarding medical devices, with a focus on elements such as asset inventory, certificate
 146 management, device hardening and configuration, and a clean-room environment to limit the
 147 possibility of zero-day vulnerabilities.

148 2 How to Use This Guide

149 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides
 150 users with the information they need to replicate NCCoE’s questionnaire-based risk assessment and
 151 deployment of a defense in depth strategy. This reference design is modular and can be deployed in
 152 whole or in parts.

153 This guide contains three volumes:

- 154 ▪ NIST SP 1800-8A: *Executive Summary*
- 155 ▪ NIST SP 1800-8B: *Approach, Architecture, and Security Characteristics* – what we built and why
 156 **(you are here)**
- 157 ▪ NIST SP 1800-8C: *How-To Guides* – instructions for building the example solution.

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

- 159 ▪ **Business decision makers, including chief security and technology officers** will be interested in
 160 the *Executive Summary (NIST SP 1800-8A)*, which describes the:
 - 161 ▪ challenges enterprises face in securing the wireless infusion pump ecosystem
 - 162 • example solution built at the NCCoE
 - 163 • benefits of adopting the example solution.
- 164 ▪ **Technology or security program managers** concerned with how to identify, understand, assess,
 165 and mitigate risk will be interested in this part of the guide, *NIST SP 1800-8B*, which describes
 166 what we did and why. The following sections will be of particular interest:
 - 167 • Section 4, [Risk Assessment and Mitigation](#), describes the risk analysis we performed
 - 168 • Section 4.3, [Security Characteristics and Controls Mapping](#), maps the security
 169 characteristics of this example solution to cybersecurity standards and best practices.

170 You might share the *Executive Summary, NIST SP 1800-8A*, with your leadership team to help them
 171 understand the significant risk of unsecured IoMT and the importance of adopting standards-based,
 172 commercially available technologies that can help secure the wireless infusion pump ecosystem.

173 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.
 174 You can use the How-To portion of the guide, *NIST SP 1800-8C*, to replicate all or parts of the example
 175 implementation that we built in our lab. The How-To guide provides specific product installation,
 176 configuration, and integration instructions for implementing the example solution. We do not recreate
 177 the product manufacturers' documentation, which is generally widely available. Rather, we show how
 178 we incorporated the products together in our environment to create an example solution.

179 This guide assumes that IT professionals have experience implementing security products within the
 180 enterprise. While we have used a suite of commercial products to address this challenge, this guide
 181 does not endorse any products. Your organization can adopt this solution or one that adheres to these
 182 guidelines in part or in whole. Your organization's security experts should identify the products that will
 183 best integrate with your existing tools and IT system infrastructure. We hope you will seek products that
 184 are congruent with applicable standards and best practices. Section 4.4, [Technologies](#) lists the products
 185 we used and maps them to the cybersecurity controls provided by this reference solution.

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

190 2.1 Typographical Conventions

191 The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
Bold	names of menus, options, com- mand buttons and fields	Choose File > Edit .
Monospace	command-line input, on-screen computer output, sample code examples, status codes	<code>mkdir</code>

Typeface/Symbol	Meaning	Example
Monospace Bold	command-line user input contrasted with computer output	<code>service sshd start</code>
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 .

192 3 Approach

193 Medical devices have grown increasingly powerful, offering patients improved, safer healthcare options
 194 with less physical effort for providers. To accomplish this, medical devices now contain operating
 195 systems and communication hardware that allow them to connect to networks and other devices. The
 196 connected functionality responsible for much of the improvement of medical devices poses challenges
 197 not formerly seen with standalone instruments.

198 Clinicians and patients rely on infusion pumps for safe and accurate administration of fluids and
 199 medications. However, the FDA has identified problems that can compromise the safe use of external
 200 infusion pumps [2], [3], [7]. These issues can lead to over- or under-infusion, missed treatments, or
 201 delayed therapy. The NCCoE initiated this project to help healthcare providers develop a more secure
 202 wireless infusion pump ecosystem, which can be applied to similarly connected medical devices. The
 203 wireless infusion pump was selected as a representative medical device. Throughout the remainder of
 204 this guide, the focus will be on the secure operation of the wireless infusion pump ecosystem. Both the
 205 architecture and security controls may be applied to increase the security posture for other types of
 206 medical devices. However, any application should be reviewed and tailored to the specific environment
 207 in which the medical device will operate.

208 Throughout the wireless infusion pump project, we collaborated with our Healthcare Community of
 209 Interest (COI) and cybersecurity vendors to identify infusion pump threat actors, define interactions
 210 between the actors and systems, review risk factors, develop an architecture and reference design,
 211 identify applicable mitigating security technologies, and design an example implementation. This
 212 practice guide highlights the approach used to develop the NCCoE reference solution. Elements include
 213 risk assessment and analysis, logical design, build development, test and evaluation and security control
 214 mapping. The practice guide seeks to help the healthcare community evaluate the security environment
 215 surrounding infusion pumps deployed in a clinical setting.

216 3.1 Audience

217 This guide is primarily intended for professionals implementing security solutions within an HDO. It may
218 also be of interest to anyone responsible for securing non-traditional computing devices (i.e., the
219 Internet of Things, or IoT).

220 More specifically, Volume B of the practice guide is designed to appeal to a wide range of job functions.
221 This volume offers cybersecurity or technology decision makers within HDOs a view into how they can
222 make the medical device environment more secure to help improve their enterprise's security posture
223 and reduce enterprise risk. It offers technical staff guidance on architecting a more secure medical
224 device network and instituting compensating controls.

225 3.2 Scope

226 The NCCoE project focused on securing the environment of the medical device and not re-engineering
227 the device itself. To do this, we reviewed known vulnerabilities in wireless infusion pumps and
228 examined how the architecture and component integration could be designed to increase the security
229 of the device. The approach considered the life cycle of a wireless infusion pump from planning the
230 purchase, to decommissioning, with a concentration on the configuration, use, and maintenance
231 phases.

232 3.2.1 Assumptions

233 Considerable research, investigation, and collaboration went into the development of the reference
234 design in this guide. The actual build and example implementation of this architecture occurred in a lab
235 environment at the NCCoE. Although the lab is based on a clinical environment, it does not mirror the
236 complexity of an actual hospital network. It is assumed that any actual clinical environment would
237 represent additional complexity.

238 3.2.2 Security

239 We assume that those of you who plan to adopt this solution or any of its components have some
240 degree of network security already in place. As a result, we focused primarily on new vulnerabilities that
241 may be introduced if organizations implement the example solution. Section 4, [Risk Assessment and
242 Mitigation](#), contains detailed recommendations on how to secure the core components highlighted in
243 this practice guide.

244 3.2.3 Existing Infrastructure

245 This guide may help you design an entirely new infrastructure. However, it is geared toward those with
246 an established infrastructure, as that represents the largest portion of readers. Hospitals and clinics are
247 likely to have some combination of the capabilities described in this reference solution. Before applying

248 any measures addressed in this guide, we recommend that you review and test them for applicability to
249 your existing environment. No two hospitals or clinics are the same, and the impact of applying security
250 controls will differ.

251 3.2.4 Technical Implementation

252 The guide is written from a how-to perspective. Its foremost purpose is to provide details on how to
253 install, configure, and integrate components, and how to construct correlated alerts based on the
254 capabilities we selected.

255 3.2.5 Capability Variation

256 We fully understand that the capabilities presented here are not the only security options available to
257 the healthcare industry. Desired security capabilities may vary considerably from one provider to the
258 next.

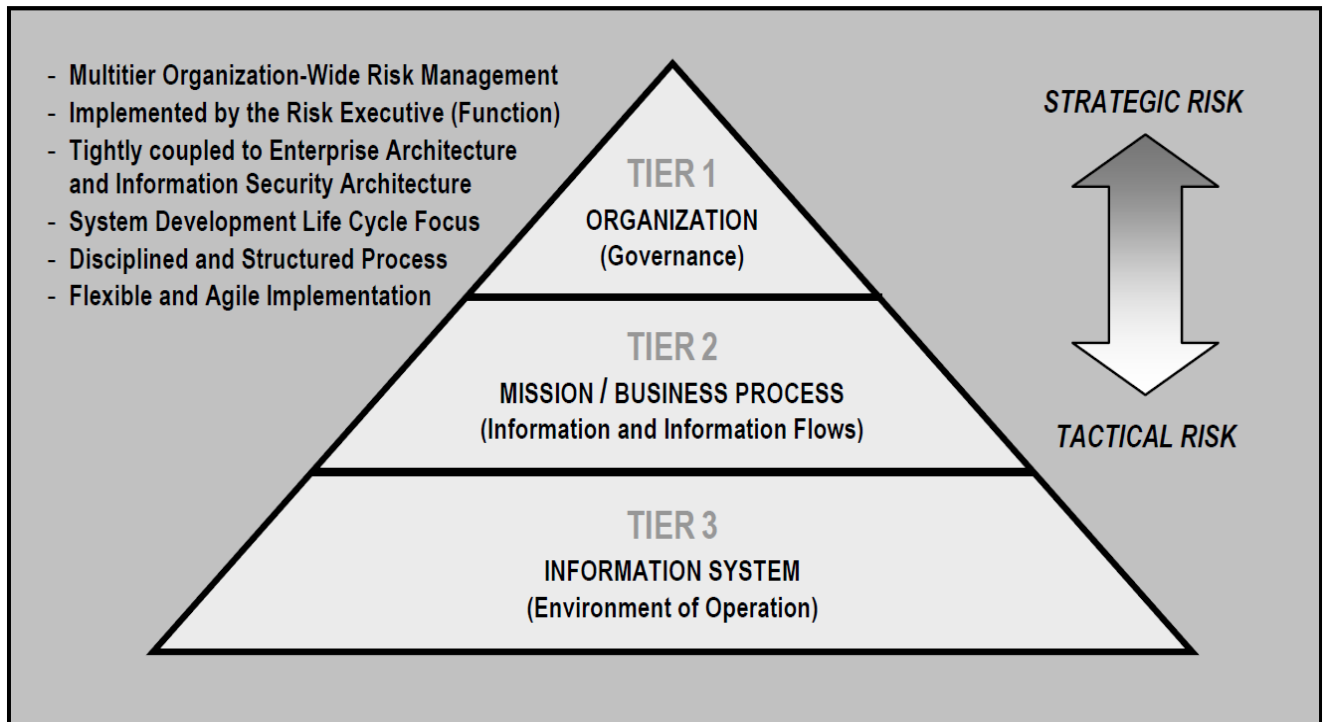
259 4 Risk Assessment and Mitigation

260 NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, states, "Risk is the net
261 negative impact of the exercise of a vulnerability, considering both the probability and the impact of
262 occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce
263 risk to an acceptable level" [11].

264 We recommend that any discussion of risk management, particularly at the enterprise level, begin with
265 a comprehensive review of NIST SP 800-37, *A Guide for Applying the Risk Management Framework to
266 Federal Information Systems* [12]. NIST's Risk Management Framework (RMF) guidance has provided
267 invaluable advice in providing a baseline to assess risks, from which the NCCoE developed the project,
268 the security characteristics of the solution, and this guide.

269 It is important to understand what constitutes the definition of risk as it relates to non-traditional
270 information systems such as wireless infusion pumps. NIST SP 800-37 presents three tiers in the risk
271 management hierarchy ([Figure 4-1](#)):

- 272 1. Organization
- 273 2. Business Processes
- 274 3. Information Systems

275 **Figure 4-1: Tiered Risk Management Approach (NIST SP 800-37)**

276

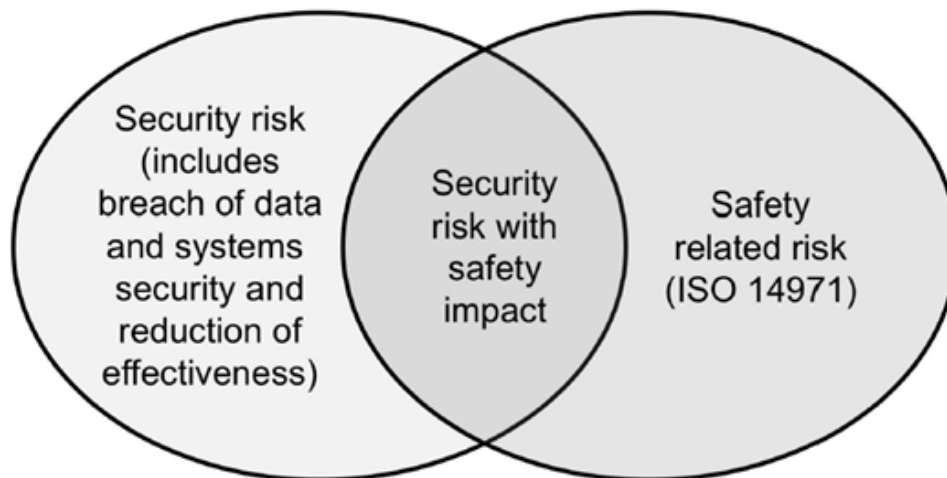
277 This guide focuses on the Tier 3 application of risk management but incorporates other industry risk
 278 management and assessment standards and best practices for the context of networked medical
 279 devices in HDOs. Relevant standards and best practices include:

- 280 ▪ International Electrotechnical Commission (IEC) 80001-1 (2010): Application of risk
 281 management for IT-networks incorporating medical devices—Part 1: Roles, responsibilities, and
 282 activities [23]
- 283 ▪ International Electrotechnical Commission/ Technical Report (IEC/TR) 80001-2: Application of
 284 risk management for IT networks incorporating medical devices [16], [17], [18], [19]
- 285 ▪ International Standards Organization (ISO) 14971:2007 Medical devices—Application of risk
 286 management to medical devices [24]
- 287 ▪ Association for the Advancement of Medical Instrumentation (AAMI) Technical Information
 288 Report (TIR) 57: 2016 Principles for medical device security—risk management [9]
- 289 ▪ Food and Drug Administration (FDA) Postmarket Management of Cybersecurity in Medical
 290 Devices [3].

291 For this NCCoE project, it was extremely important to understand the complexity of networked medical
 292 devices in a system-of-systems environment. Additionally, we felt it necessary to understand where
 293 security risks may have safety implications. The AAMI TIR57 was particularly useful in this regard, as it

294 specified elements of medical device security using NIST's RMF, IEC 80001-1, IEC/TR 80001-2 and ISO
295 14971 [9], [11], [12], [13], [15], [16], [17], [18], [19], [23], [24]. Also, the Venn diagram in [Figure 4-2](#)
296 illustrates the relationship between security and safety risks (AAMI TIR57). As seen in this diagram,
297 there are cybersecurity risks that may have safety impacts. For HDOs, these risks should receive special
298 attention from both security and safety personnel.

299 **Figure 4-2: Relationship between Security and Safety Risks (AAMI TIR 57) [7]**



300

301 **4.1 Risk Assessments**

302 For this NCCoE project, we performed two types of risk assessments: (1) industry analysis of risk and (2)
303 questionnaire-based risk assessment.

304 **4.1.1 Industry Analysis of Risk**

305 The first assessment was an industry analysis of risk performed while developing the initial use case.
306 This industry analysis provided insight into the challenges of integrating medical devices into a clinical
307 environment containing a standard IT network. Completion of the industry analysis narrowed the
308 objective of our use case to helping HDOs secure medical devices on an enterprise network, with a
309 specific focus on wireless infusion pumps.

310 Activities involved in our industry analysis included reaching out to our COI and other industry experts
311 through workshops and focus group discussions. After receiving feedback on the NCCoE's use case
312 publication through a period of public comment, NCCoE adjudicated the comments and clarified a
313 project description. These activities were instrumental to identifying primary risk factors as well as

314 educating our team on the uniqueness of cybersecurity risks involved in protecting medical devices in
315 healthcare environments.

316 4.1.2 Questionnaire-based Risk Assessment

317 For the second type of risk assessment, we conducted a formal questionnaire-based risk assessment,
318 using tools from two NCCoE Cooperative Research and Development Agreement (CRADA) collaborators.
319 We conducted this questionnaire-based risk assessment to gain greater understanding of the risks
320 surrounding the wireless infusion pump ecosystem. The tool identifies the risks and maps them to the
321 security controls. This type of risk assessment is considered appropriate for Tier 3: Information Systems,
322 per NIST's RMF. One tool focuses on medical devices and the surrounding ecosystem. The other tool
323 focuses on the HDO enterprise. Both questionnaire-based risk assessment tools leverage guidance and
324 best practices including the NIST RMF and CSF and focus on built-in threats, vulnerabilities, and controls
325 [10], [11], [12], [13]. The assessment results measure likelihood, severity, and impact of potential
326 threats.

327 All risk assessment activities provide an understanding of the challenges and risks involved when
328 integrating medical devices, in this case wireless infusion pumps, into a typical IT network. Based on this
329 analysis, this project has two fundamental objectives for this project:

- 330 ▪ to protect the wireless infusion pumps from cyberattacks;
- 331 ▪ to protect the healthcare ecosystem, should a wireless infusion pump be compromised.

332 Per AAMI's TIR57, "To assess security risk, several factors need to be identified and documented,"
333 (Hoyme & Geoff, 2016) [9].

334 Based on our risk assessments and additional research, we identified primary threats, vulnerabilities,
335 and risks that should be addressed when using wireless infusion pumps in HDOs.

336 4.1.3 Assets

337 Defining the asset is the first step in establishing the asset-threat-vulnerability construct necessary to
338 properly evaluate or measure risks, per NIST's RMF [11], [12], [13]. An information asset is typically
339 defined as a software application or information system that uses devices or third-party vendors for
340 support and maintenance. For the NCCoE's purposes, the information asset selected is a *Wireless*
341 *Infusion Pump System*. A risk assessment of this asset would include an evaluation of the cybersecurity
342 controls for the pump, pump server, end-point connections, network controls, data storage, remote
343 access, vendor support, inventory control, and any other associated elements.

344 4.1.4 Threats

345 Below are some potential known threats in HDOs that use network-connected medical devices, such as
346 wireless infusion pumps. Refer to [Appendix A](#) for a description of each threat.

- 347 • Targeted attacks
- 348 • Advanced Persistent Threats (APTs)
- 349 • Disruption of Service – Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- 350 • Malware infections
- 351 • Theft or loss of assets
- 352 • Unintentional misuse
- 353 • Vulnerable systems or devices directly connected to the device (e.g., via USB or other
- 354 hardwired, non-network connections).

355 It is important to understand that the threat landscape is constantly evolving and unknown threats exist
356 and may be unavoidable, which need to be identified and remediated as they are found.

357 4.1.5 Vulnerabilities

358 Vulnerabilities afflict wireless infusion pump devices, pump management applications, network
359 applications and even the physical environment and personnel using the device or associated systems.
360 Within a complex system-of-systems environment, vulnerabilities may be exploited at all levels. There
361 are multiple information resources available to keep you informed about potential vulnerabilities. This
362 guide recommends that security professionals turn to the National Vulnerability Database (NVD). The
363 NVD is the U.S. government repository of standards-based vulnerability management data
364 [<https://nvd.nist.gov>].

365 Here is a list of typical vulnerabilities that may arise when using wireless infusion pumps. Refer to
366 [Appendix B](#) for a description of each vulnerability.

- 367 ▪ Lack of asset inventory
- 368 ▪ Long useful life
- 369 ▪ Information/Data Vulnerabilities
 - 370 • Lack of encryption on private/sensitive data-at-rest
 - 371 • Lack of encryption on transmitted data
 - 372 • Unauthorized changes to device calibration or configuration data
 - 373 • Insufficient data backup
 - 374 • Lack of capability to de-identify private/sensitive data
 - 375 • Lack of data validation
- 376 ▪ Device/Endpoint (Infusion Pump) Vulnerabilities
 - 377 • Debug-enabled interfaces

- 378 • Use of removable media
- 379 • Lack of physical tamper detection and response
- 380 • Misconfiguration
- 381 • Poorly protected and patched devices
- 382 ▪ User or Administrator Accounts Vulnerabilities
- 383 • Hard-coded or factory default passcodes
- 384 • Lack of role-based access and/or use of principles of least privilege
- 385 • Dormant accounts
- 386 • Weak remote access controls
- 387 ▪ IT Network Infrastructure Vulnerabilities
- 388 • Lack of malware protection
- 389 • Lack of system hardening
- 390 • Insecure network configuration
- 391 • System complexity.

392 To mitigate risk factors, HDOs should also strive to work closely with medical device manufacturers and
393 follow FDA’s post-market guidance, as well as instructions from the U.S. Department of Homeland
394 Security’s Industrial Control System-Cyber Emergency Response Team (ICS-CERT).

395 4.1.6 Risks

396 NIST SP 800-30, *A Guide for Conducting Risk Assessments*, defines *risk* as, “a measure of the extent to
397 which an entity is threatened by potential circumstance or event, and is typically a function of: (i) the
398 adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of
399 occurrence” [11]

400 NIST SP 800-30 further notes within a definition of *risk assessment* that, “assessing risk requires careful
401 analysis of threat and vulnerability information to determine the extent to which circumstances or
402 events could adversely impact an organization and the likelihood that such circumstances or events will
403 occur.”

404 Based on the above guidance from NIST SP 800-30, several risks endanger medical devices:

- 405 ▪ Infusion pumps and server components may be leveraged for APTs and serve as pivot points to
406 cause adverse conditions throughout a hospital’s infrastructure.
- 407 ▪ Infusion pumps may be manipulated to prevent the effective implementation of safety
408 measures, such as the drug library.

- 409 ▪ Infusion pump interfaces may be used for unintended or unexpected purposes, with those
410 conditions leading to degraded performance of the pump.
- 411 ▪ PHI may be accessed remotely by unauthorized individuals.
- 412 ▪ PHI may be disclosed to unauthorized individuals should the device be lost, stolen, or
413 improperly decommissioned.
- 414 ▪ Improper third party vendor connections.

415 Although these risks may persist in infusion pumps and server components, HDOs should perform
416 appropriate due diligence in determining the extent of the business impact and likelihood of each risk
417 factor.

418 Vulnerabilities may be present in infusion pumps and their server components since these devices often
419 include embedded operating systems on the endpoints. Infusion pumps are designed to maintain a
420 prolonged period of useful life, and, as such, may include system components (e.g., an embedded
421 operating system) that may either reach end-of-life or reach a period of degraded updates prior to the
422 infusion pump being retired from service. Patching and updating may become difficult over the course
423 of time.

424 Infusion pumps may not allow for the addition of third-party mechanisms, such as antivirus or anti-
425 malware controls. Should limitations be identified in embedded operating systems used by an infusion
426 pump, vulnerabilities, weaknesses, and deficiencies may become known to malicious actors who may
427 seek to leverage those deficiencies to install malicious or unauthorized software on those devices.

428 Malicious software, or malware, may cause adverse conditions on the pump, degrading the
429 performance of the pump, or rendering the device unable to perform its function (e.g., ransomware).
430 Malware may also be used to convert the infusion pump into an access point for malicious actors to
431 subsequently access or disrupt the operations of other hospital systems.

432 As noted above, infusion pumps may allow for the manipulation of configurations or safety measures
433 implemented through the drug library (e.g., adjusting dosage or flow rates). This risk may be
434 instantiated through local access, such as an interface or port on the device with either no or weak
435 authentication or access control in place. Further, infusion pumps may be reachable across a hospital's
436 network, which provides an avenue for a malicious actor to cause an adverse event.

437 Pumps may implement local ports, such as USB ports serial interfaces, Bluetooth, radio frequency, or
438 other mechanisms that allow for close proximity connection to the pump. These ports may be
439 implemented with the intent to facilitate technical support; however, they also pose a risk by providing
440 a pathway for actors to cause adverse conditions to the pump.

441 Modern infusion pumps and server components may include PHI, such as a patient's name, medical
442 record number (MRN), procedure coding, and medication or treatment. Through similar deficiencies
443 that would allow configuration or use manipulation as noted above, this PHI may then be viewed,

444 accessed, or removed by unauthorized individuals. Also, individuals who have direct access to the
445 infusion pump may be able to extract information through unsecured ports or interfaces [2], [3], [7],
446 [17], [25].

447 Common vulnerabilities and control deficiencies that enable these risks may include:

- 448 ▪ **The implementation of default credentials and passwords:** Weak authentication, and default
449 passwords, or not implementing authentication or access control, may be discovered by
450 malicious actors who would seek to cause adverse conditions. Malicious actors may leverage
451 this control deficiency for risk factors that span from installing malware on the infusion pump,
452 to manipulating configuration settings, or to extract information such as PHI from the device.
- 453 ▪ **The use of unsecured network ports, such as Telnet or FTP:** Telnet and FTP are internet
454 protocols that do not secure or encrypt network sessions. Telnet and FTP may be used
455 nominally for technical support interfaces; however, malicious actors may attempt to leverage
456 these to access the infusion pump. Telnet and FTP may include deficiencies that allow for
457 compromise of the protocol itself, and, since the network session is not encrypted, malicious
458 actors may implement mechanisms to capture network sessions, including any authentication
459 traffic, or to identify sensitive information such as credentials, configuration information, or any
460 PHI stored on the device.
- 461 ▪ **Local interfaces with limited security controls:** Local interfaces, such as USB ports, serial ports,
462 Bluetooth, radio frequency, or other ports may be used for device technical support. These
463 ports, however, allow for malicious actors within close proximity to the device to access the
464 device, manipulate configuration settings, access or remove data from the device, or install
465 malware on the device. These ports may exist on the pump for support purposes, but use of the
466 ports for unauthorized or unexpected purposes, such as recharging a mobile device such as a
467 smart phone or tablet, may cause a disruption to the pump’s standard operation.

468 4.1.7 Recommendations and Best Practices

469 The recommendations in [Appendix C](#) address additional security concerns which, although not as
470 pressing as those listed above, are worthy of consideration. If applied, these additional
471 recommendations will likely reduce risk factors or prevent them from becoming greater risks.
472 Associated best practices for reducing the overall risk posture of infusion pumps are also included in
473 Recommendations and Best Practices list.

474 4.2 Risk Response Strategy

475 *Risk mitigation* is often confused with *risk response*. Per NIST SP 800-30, risk mitigation is defined as
476 “prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures
477 recommended from the risk management process.”

478 Risk mitigation is a subset of risk response. Risk response is defined by NIST SP 800-30 as: accepting;
479 avoiding; mitigating; sharing, or transferring risks. When considering risk response, your organization
480 should recommend to a corporate risk management board ways that the Information Risk Manager or
481 equivalent should treat risk.

482 4.2.1 Risk Mitigation

483 Organizations must determine their tolerance or appetite for risk, the response to which will drive risk
484 remediation or risk mitigation for identified risks. This tolerance should be codified in a Risk
485 Management Plan. Such a plan will include regulatory requirements and guidance, industry best
486 practices, and security controls. Organizations should set an appropriate risk tolerance based on the
487 factors noted above with the intent to remediate those risks above the established risk tolerance (i.e.,
488 critical or high risks.)

489 These remediation responses can take the form of administrative, physical, and technical controls, or an
490 appropriate mix. [Section 4.1.7](#) of this guide identifies several mitigation recommendations regarding
491 specific risk. Additional compensating safeguards, countermeasures, or controls are noted below:

- 492 ▪ Physical security controls, including standard tamper-evident physical seals, which can be
493 applied to hardware to indicate unauthorized physical access [10], [26].
- 494 ▪ Ensuring implementation of a physical asset management program that manages and tracks
495 unique, mobile media such as removable flash memory devices (e.g., SD cards, thumb drives)
496 used by pump software hosted on an endpoint client. Consider encryption of all portable media
497 used in such a fashion [10], [26], [27], [28].
- 498 ▪ Following procedures for clearing wireless network authentication credentials on the endpoint
499 client if the pump is to be removed or transported from the facility. These procedures can be
500 found in pump user manuals but should be referenced in official HDO policies and procedures
501 [29], [30], [31], [32].
- 502 ▪ Changing wireless network authentication credentials regularly and, if there is evidence of
503 unauthorized access to a pump system, immediately changing network authentication
504 credentials [10], [26].
- 505 ▪ Ensuring all wireless network access is minimally configured for WPA2 PSK encryption and
506 authentication. All pumps should be set to WPA2 encryption [33], [34], [35], [36].
- 507 ▪ All pumps and pump systems should include cryptographic modules that have been validated as
508 meeting NIST FIPS 140-2 [37].
- 509 ▪ All ports are disabled except when in use, and the device has no listening ports [3], [9], [10],
510 [25], [26].
- 511 ▪ Employing mutual transport layer security (TLS) encryption in transit between the client and
512 server [38].

- 513 ▪ Employing individual pump authentication with no shared key for all pumps [10], [26].
- 514 ▪ Certificate-based authentication for a pump server [29], [30], [31], [32].

515 **4.3 Security Characteristics and Controls Mapping**

516 As described in the previous sections, we derived the security characteristics by analyzing risk in
517 collaboration with our healthcare sector stakeholders as well as our participating vendor partners. In
518 the risk analysis process, we used IEC/TR 80001-2-2 as our basis for wireless infusion pump capabilities
519 in healthcare environments [16]. [Table 4-1](#) presents the desired security characteristics of the use case
520 in terms of the CSF subcategories [10], [14]. Each subcategory is mapped to relevant NIST standards,
521 industry standards, controls, and best practices. In our example implementation, we did not observe
522 any security characteristics that mapped to the Respond or Recover subcategories of the CSF.

523

Table 4-1: Security Characteristics and Controls Mapping - NIST Cyber Security Framework

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	SP800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45 [39]	ISO/IEC 27001:2013
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	CNFS	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)	A.8.1.1, A.8.1.2
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14	DTBK	C.F.R. § 164.308(a)(7)(ii)(E)	A.8.2.1
	Business Environment (ID.BE)	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	CP-8, PE-9, PE-11, PM-8, SA-14	DTBK	C.F.R. §§ 164.308(a)(7)(i), 164.308(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(2)(ii), 164.314(a)(1), 164.314(b)(2)(i)	A.11.2.2, A.11.2.3, A.12.1.3
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	RDMP	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E), 164.308(a)(8), 164.310(a)(1), 164.312(a)(1), 164.316(b)(2)(iii)	A.12.6.1, A.18.2.3

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	SP800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45 [39]	ISO/IEC 27001:2013
PROTECT (PR)	Identity Management and Access Control (PR.AC)	(note: not directly mapped in CSF)	AC-1, AC-11, AC-12	ALOF		
		PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes	AC-2, IA Family	AUTH, CNFS, EMRG, PAUT	C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
		PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	PLOK, TXCF, TXIG	C.F.R. §§ 164.308(a)(1)(ii)(B), 164.308(a)(7)(i), 164.308(a)(7)(ii)(A), 164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii)	A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
		PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20	NAUT, PAUT	C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)	A.6.2.2, A.13.1.1, A.13.2.1
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16	AUTH, CNFS, EMRG, NAUT, PAUT	C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	SP800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45 [39]	ISO/IEC 27001:2013
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-4, SC-7	NAUT	C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312€	A.13.1.1, A.13.1.3, A.13.2.1
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	SC-28	IGAU, STCF	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)	A.8.2.3
		PR.DS-2: Data-in-transit is protected	SC-8	IGAU, TXCF	C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
		PR.DS-4: Adequate capacity to ensure availability is maintained	AU-4, CP-2, SC-5	AUDT, DTBK	C.F.R. §§ 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7), 164.310(a)(2)(i), 164.310(d)(2)(iv), 164.312(a)(2)(ii)	A.12.3.1
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	IGAU	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	SP800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45 [39]	ISO/IEC 27001:2013
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	CNFS, CSUP, SAHD, RDMP	C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)	A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	CP-4, CP-6, CP-9	DTBK	C.F.R. §§ 164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(D), 164.310(a)(2)(i), 164.310(d)(2)(iv)	A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3
		PR.IP-6: Data is destroyed according to policy	MP-6	DIDT	C.F.R. §§ 164.310(d)(2)(i), 164.310(d)(2)(ii)	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-4	CSUP	C.F.R. §§ 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2)(ii), 164.310(d)(2)(iii), 164.312(a), 164.312(a)(2)(ii), 164.312(a)(2)(iv), 164.312(b), 164.312(d), 164.312(e), 164.308(a)(1)(ii)(D)	A.11.2.4, A.15.1.1, A.15.2.1

Cybersecurity Framework (CSF) v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	SP800-53R4	IEC TR 80001-2-2	HIPAA Security Rule 45 [39]	ISO/IEC 27001:2013
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4	AUTH, CNFS	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b)	none
	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	AUTH, CNFS, EMRG, MLDP	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)	none
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	AUTH, CNFS, EMRG, MLDP	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312€	A.12.4.1
		DE.CM-4: Malicious code is detected	SI-3	IGAU, MLDP, TXIG	C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	A.12.2.1
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4	RDMP	C.F.R. § 164.308(a)(1)(ii)(D)	A.14.2.7, A.15.2.1
	Detection Processes (DE.DP)	DE.DP-3: Detection processes are tested	CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	IGAU	C.F.R. § 164.306€	A.14.2.8
RESPOND (RS)						
RECOVER (RC)						

526 4.4 Technologies

527 [Table 4-2](#) lists all of the technologies used in this project and map the generic application term to the specific product we used and the security
528 control(s) we deployed. Refer to [Table 4-1](#) for an explanation of the CSF Subcategory codes [10].

529 The reference architecture design in [Section 5](#) is vendor agnostic such that any Wireless Infusion Pump (WIP) system can be integrated safely
530 and securely into a hospital's IT infrastructure. Therefore, for the infusion pump device, infusion pump server and wireless infusion pump
531 ecosystem, we captured the most common security features among all the products we tested in this use case. A normalized view of the list of
532 functions and NIST CSF Subcategories are presented in the table below.

533 Please note, some of the CSF Subcategory codes require people, and process controls, not solely technical controls.

534 **Table 4-2: Products and Technologies**

Component	Specific Product	Function	CSF Subcategories
Infusion Pump Device	Baxter: Sigma Spectrum LVP, Version 8	<ul style="list-style-type: none"> requires passcode to access the bio-medical engineering mode (on device or connect to device) for configuring and setting up the devices provides the capability to change the manufacture default passcode supports IEEE 802.11i enterprise wireless encryption/authentication standards, including WPA2-EAP-TLS for protecting data exchange restricted access to the server, application and stored data closes/disables all communication ports that are not required for the intended use 	PR.AC-1, PR.AC-2, PR.DS-2, PR.DS-6, PR.IP-1, PR.IP-6
	Baxter: Sigma Spectrum Wireless Battery Module, version 8		
	BBraun: Space Infusomat Infusion Pump (LVP) – s/w U		
	BD: Alaris® 8015 PC Unit v9.19.2		
	BD: Alaris® Syringe Module 8110		

Component	Specific Product	Function	CSF Subcategories
	BD: Alaris® LVP Module 8100	<ul style="list-style-type: none"> • closes/disables all services that are not required for intended use • provides an integrity checking mechanism to verify information • supports baseline configuration • supports removing/destroying data from the device • few models have a tamper-resist switch, with tamper-evident seals 	
	Hospira: Plum 360 version 15.10		
	Hospira: PCA version 7.02		
	Smiths Medical: Med-fusion® 3500 V5 syringe infusion system		
	Smiths Medical: Med-fusion 4000® Wireless Syringe Infusion Pump		
	Smiths Medical: CADD®-Solis Ambulatory Infusion Pump		
Infusion Pump Server	Baxter: CareEverywhere Gateway Server, version 14	<ul style="list-style-type: none"> • with appropriate configuration, discovers and identifies devices connected to the pump server via wired, wireless, and virtual private networks, to aid in building and maintaining accurate physical device inventories • supports role-based authentication and password rules and policies • supports the use of a HDO's Active Directory/LDAP solution • supports auto-logoff, data encryption/obscuration 	ID.AM-1, PR.AC-1, PR.AC-3, PR.AC-4, PR.DS-1, PR.DS-2, PR.MA-2
	BBraun: Space Online Suite Software, version AP 2.0.1		
	BD: Alaris® Systems Manager v4.2		
	Hospira: MedNet 6.2		

Component	Specific Product	Function	CSF Subcategories
Infusion Pump Eco-system	Smiths Medical: PharmGuard® Server Enterprise Edition, V1.1	<ul style="list-style-type: none"> • can be accessed remotely via VPN (or like) tools • a few models support FIPS 140-2 • operates on manufacturer-supported OS, DB Server and Web Server (allows software patches) • supports secure protocols, such as TLS • supports co-existence with firewall, anti-virus, backup software, and other types of security safeguard products • maintains different types of audit/log records for preventing unauthorized access 	
	Baxter: Sigma Spectrum Master Drug Library, version 8		
	BBraun: Space Dose-Trace and Space Dose-Link software – Eng version available for testing		
	BD: Alaris® System Maintenance (ASM) v 10.19		
	Smiths Medical: PharmGuard® Toolbox v1.5 Smiths Medical: CADD™-Solis Medication Safety Software		
Access Point (AP)	Cisco: Access Point (AIR-CAP1602I-A-K9)	<ul style="list-style-type: none"> • authenticates and connects infusion pumps to the Wi-Fi • supports Wireless Network Standards: IEEE 802.11a/b/g/n/ac 	PR.AC-5, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Wireless LAN Controller (WLC)	Cisco: Wireless LAN Controller 8.2.111.0	<ul style="list-style-type: none"> • supports Security Protocols: IEEE 802.11i (WPA2), EAP-TLS • AP joins a WLC to form a Control and Provisioning of Wireless Access Points protocol (CAPWAP) tunnel 	

Component	Specific Product	Function	CSF Subcategories
		<ul style="list-style-type: none"> • uses ISE as the authentication service • provides message authentication and encryption in data transmission 	
Identity Services Engine (ISE)	Cisco ISE	<ul style="list-style-type: none"> • discovers and identifies devices connected to wired, wireless, and virtual private networks. It gathers this information based on what's accurate connecting to the network, a key step toward building and maintaining accurate physical device inventories • provides advanced network access controls by connecting user identity with device profiling and access policy • provides log audit of events which can be monitored for the network traffic 	ID.AM-1, PR.AC-1, PR.AC-4, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Firewall/Router	Cisco: ASA	<ul style="list-style-type: none"> • delivers network integrity protection • used as external firewall for connecting to the internet for guest network • used as internal firewall for all other network zones with rules and policies 	PR.AC-5, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Switch	Cisco: Catalyst 3650 Switch	<ul style="list-style-type: none"> • provides port-level controls, port blocking, VLAN segmentation 	PR.AC-5, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Endpoint Protection	Symantec: Endpoint Protection (SEP)	<ul style="list-style-type: none"> • provides intrusion prevention, URL, and firewall policies • provides application behavioral controls • provides device control to restrict access • provides anti-virus file protection 	DE.CM-1, DE.CM-3, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1

Component	Specific Product	Function	CSF Subcategories
		<ul style="list-style-type: none"> • Provides behavioral monitoring • Provides file reputation analysis 	
Network Advanced Threat Protection	Symantec: Advanced Threat Protection: Network (ATP:N)	<ul style="list-style-type: none"> • monitors internal inbound and outbound internet traffic • uncovers advanced attacks • automatically prioritizes critical events • searches for known indicators-of-compromise (IoC) across the entire environment • blacklists or whitelists files and URLs once they are identified as malicious • can be integrated with third-party security information and events management (SIEM) tool 	DE.CM-1, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1
DataCenter Security	Symantec: Server Advanced - DataCenter Security (DCS:SA):	<ul style="list-style-type: none"> • out-of-the-box host intrusion detection system (IDS) and intrusion prevention systems (IPS) policies • provides sandboxing and Process Access Control (PAC) to prevent a new class of threats • hosts firewall to control inbound and outbound network traffic to and from servers • compensating host intrusion prevention system (HIPS) controls restrict application and operating system behavior using policy-based least privilege access control • prevents file and system tampering 	DE.CM-1, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1

Component	Specific Product	Function	CSF Subcategories
		<ul style="list-style-type: none"> provides application and device control by locking down 'configuration' settings, file systems, and use of removable media 	
Secure Remote Management and Monitoring	TDi Technologies: ConsoleWorks	<ul style="list-style-type: none"> authenticates system managers provides role-based access control of system management functions implements a protocol break between the system manager and the managed assets records all system management actions performs remote configuration management and monitoring of devices 	PR.AC-3, PR.AC-4, PR.MA-2, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-6
Physics-based integrity assessment	PFP: Device Monitor	<ul style="list-style-type: none"> detects device behavior detects cyberattacks in hardware and software detects tiny anomalies in power patterns to instantly catch attacks, thereby providing an early warning that a device has been tampered with integrity assessment uses side channel 	
Certificate Authority Service	DigiCert: Certificate Authority	<ul style="list-style-type: none"> provides certificate authority service 	Access Control (PR.AC) PR.DS-2
Certificate Management / Provisioning	Intercede: MyID	<ul style="list-style-type: none"> serves as device provisioner 	

Component	Specific Product	Function	CSF Subcategories
Risk Assessment	Clearwater: IRM Pro	<ul style="list-style-type: none">• provides tool for conducting risk assessments that focus on healthcare compliance and cyber risk management	ID.RA-1
	MDISS: MDRAP	<ul style="list-style-type: none">• provides tool for conducting risk assessments that focus on medical devices	

535

536 **5 Architecture**

537 Wireless infusion pumps are no longer standalone devices; they now also include pump servers for
538 managing the pumps, drug libraries, networks allowing for interoperability with other hospital systems,
539 and VPN tunnels to outside organizations for maintenance. While interconnectivity, enhanced
540 communications, and safety measures on the pump have added complexity to infusion pumps, these
541 components can help improve patient outcomes and safety.

542 As infusion pumps have evolved, one safety mechanism development was the invention of the “drug
543 library.” The drug library is a mechanism that is applied to an infusion pump that catalogs medications,
544 fluids, dosage, and flow rates. While hospital pharmacists may be involved in the maintenance of the
545 drug library, continuous application of the drug library to the infusion pump environment tends to be
546 managed through a team of biomedical engineers. Initially, the drug library file may be loaded onto the
547 pump through a communication port. When the drug library file is updated, all infusion pumps need to
548 be updated to ensure that they adhere to the current rendition of that drug library. Drug library
549 distribution, which may require that staff manually adjust individual pumps, may become onerous for
550 the biomedical staff in HDOs that use thousands of pumps [1], [40].

551 Manufacturers provide wireless communications on some pumps and use a pump server to manage the
552 drug library file, capture usage information on the pumps, and provide pump updates.

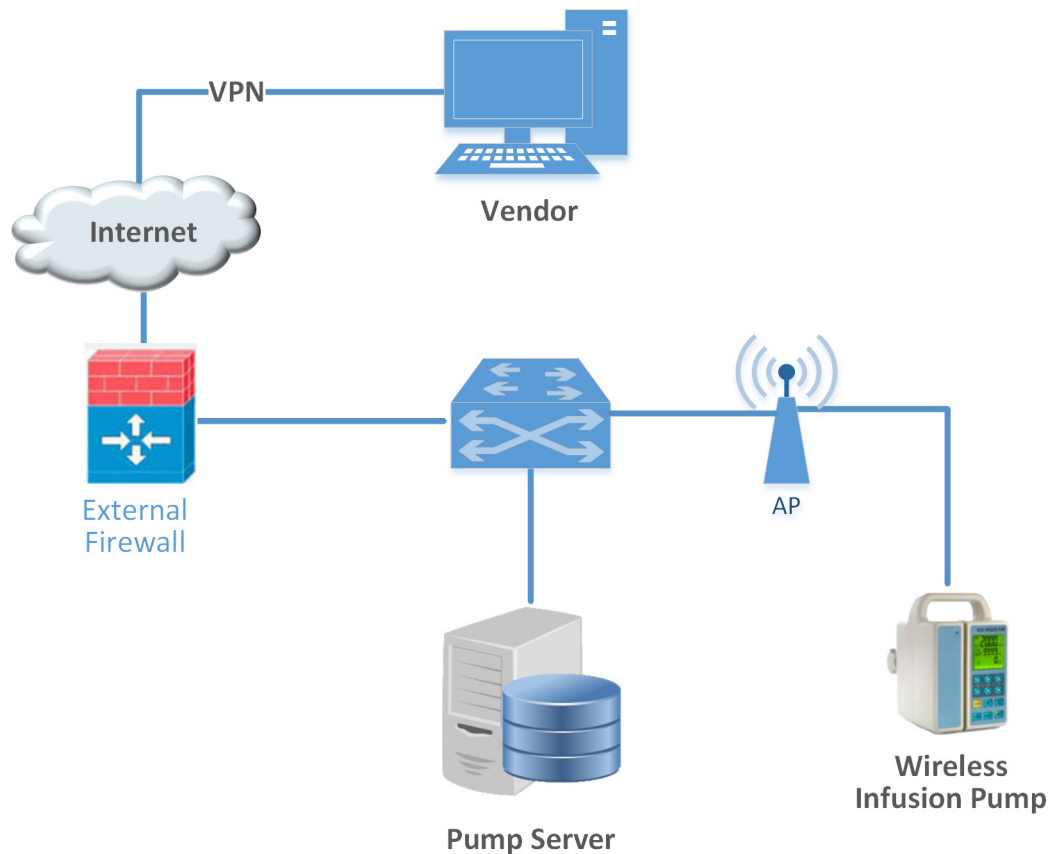
553 Medical devices manufacturers are subject to regulatory practices by the Food & Drug Administration
554 (FDA), and may tend to focus on the primary function of the pump (i.e., assurance that the pump
555 delivers fluids of a certain volume and defined flow rates, consistent with needs that providers may
556 have to ensure safe and appropriate patient care). Technology considerations, such as cybersecurity
557 controls, may not be primarily addressed in the device design and approval process. As such, infusion
558 pumps may include technology that does not lend itself to the same controls that an HDO may
559 implement on standard desktops, laptops, or workstations used for productivity [9], [18].

560 As technology has evolved, cybersecurity risk has expanded, both in visibility and in the number of
561 threats and vulnerabilities. This expansion has led to a heightened concern, from manufacturers, as well
562 as the FDA, and work has been established to identify measures to better respond to cybersecurity risk
563 [7], [9], [25]. In [Section 5.1](#), we describe the wireless infusion pump ecosystem by defining the
564 components. [Section 5.2](#) discusses the data flow, and [Section 5.3](#) explains the set of controls we use in
565 our example implementation, including those for networks, pumps, pump servers, and enterprise.
566 [Section 5.4](#) describes the target architecture for our example implementation.

567 **5.1 Basic System**

568 A basic wireless infusion pump ecosystem includes a wireless infusion pump, a pump server, a network
569 consisting of an access point, a wireless LAN controller, a firewall, and a VPN to a manufacturer.

570 Figure 5-1: Basic System



571

572 **5.2 Data Flow**

573 The flow of data between a wireless infusion pump and its corresponding server falls into the following
 574 transaction categories:

- 575 ▪ modifying the drug library
- 576 ▪ performing software updates
- 577 ▪ remotely managing the devices
- 578 ▪ auditing the data flow processes.

579 Infusion pumps may also include other advanced features such as auto-programming to receive patient
 580 prescription information and record patient treatment information to the patient's electronic health
 581 record.

582 5.3 Cybersecurity Controls

583 This section discusses security controls by their location, either on the network, pump, or pump server.
584 We also describe controls implemented in the NCCoE lab, and depict the controls implemented in our
585 final architecture.

586 In general, we recommend that a clinically focused network be designed to protect information used in
587 HDOs, whether that information is at-rest or in-transit. As described in *Cisco Medical-Grade Network*
588 *(MGN) 2.0-Wireless Architectures* (Higgins & Mah, 2012), no single architecture can be designed to meet
589 the security requirements of all organizations [41]. However, many cybersecurity best practices can be
590 applied by HDOs to meet regulatory compliance standards.

591 Our reference architecture uses Cisco's solution architecture as the baseline. This baseline
592 demonstrates how the network can be used to provide multi-tiered protection for medical devices
593 when exchanging information via a network connection. The goal of our reference architecture is to
594 provide countermeasures to deal with challenges identified in the assessment process. For our use case
595 solution, we use segmentation and defense-in-depth as security models to build and maintain a secure
596 device infrastructure. This section provides additional details on how to employ security strategies to
597 achieve specific targeted protections when securing wireless infusion pumps.

598 We used the following cybersecurity controls:

- 599 ▪ network controls
- 600 ▪ pump controls
- 601 ▪ pump server controls
- 602 ▪ enterprise level controls

603 5.3.1 Network Controls

604 Proper network segmentation or network zoning is essential to developing a strong cybersecurity
605 posture [33], [34], [35], [36], [42]. Segmentation uses network devices such as switches and firewalls to
606 split a large computer network into subnetworks, each referred to as a *network segment* [41]. Network
607 segmentation not only enhances network management, but also improves cybersecurity, allowing the
608 separation of networks based on network security requirements driven by business needs or asset
609 value.

610 The architecture designed for this build uses Cisco's solution architecture as the baseline for
611 demonstrating how the network can be used to provide a multi-tiered protection for medical devices
612 when exchanging information with the outside world during the operation involving network
613 communication. The goal of this architecture design is to provide countermeasures to mitigate
614 challenge areas identified in the assessment process. In our use case solution, *segmentation* and
615 *defense-in-depth* are the security models we used as security measures to build and maintain secure

616 device infrastructure. This section provides additional details on how to employ security strategies to
617 achieve the target security characteristics for securing wireless infusion pumps.

618 *5.3.1.1 Segmentation/Zoning*

619 Our network architecture uses a zone-based security approach. By using different local networks for
620 designated purposes, networked equipment identified for a specific purpose can be put together on the
621 same network segment and protected with an internal firewall. The implication is that there is no
622 inherent trust between network zones and that trust limitations are enforced by properly configuring
623 firewalls to protect equipment in one zone from other, less trusted zones. By limiting access from other,
624 less trusted areas, firewalls can more effectively protect the enterprise network.

625 For discussion purposes, we include some generic components of a typical HDO in our network
626 architecture examples. A given healthcare facility may be simpler or more complex and may contain
627 different subcomponents. The generic architecture contains several functional segments, including the
628 following elements:

- 629 ▪ core network
- 630 ▪ guest network
- 631 ▪ business office
- 632 ▪ database server
- 633 ▪ enterprise services
- 634 ▪ clinical server
- 635 ▪ biomedical engineering
- 636 ▪ medical devices with wireless LAN
- 637 ▪ remote access for external vendor support

638 At a high level, each zone is implemented as a virtual local area network (VLAN) with a combination
639 firewall/router Cisco Adaptive Security Appliance (ASA) device connecting it to the rest of the enterprise
640 through a backbone network, referred to as the core network [43], [44], [45]. Segments may consist of
641 physical or virtual networks. We implemented sub-nets that correspond exactly to VLANs for simplicity
642 and convenience. The routing configuration is the same for each, but the firewall configuration may vary
643 depending on each zone's specific purpose. An external router/firewall device is used to connect the
644 enterprise and guest network to the internet. Segmentation is implemented via a VLAN using Cisco
645 switches. A short description of each segment and the final network architecture follow.

646 *5.3.1.1.1 Core Network*

647 Our reference architecture implements a core network zone that consists of the equipment and systems
648 used to establish the backbone network infrastructure. The external firewall/router also has an

649 interface connected to the core enterprise network, just like other firewall/router devices in the other
650 zones. This zone serves as the backbone of the enterprise network and consists only of routers
651 connected by switches. The routers automatically share internal route information with each other via
652 authenticated Open Shortest Path First (OSPF) to mitigate configuration errors as zones are added or
653 removed.

654 5.3.1.1.2 Guest Network Zone

655 Hospitals often implement a guest network that allows visitors or patients to access internet services
656 during their visit. As shown in [Figure 5-2](#), network traffic here tends not to be clinical in nature but is
657 offered as a courtesy to hospital visitors and patients to access the internet. Refer to Section 5.3.1.5,
658 [External Access](#) for additional technical details.

659 5.3.1.1.3 Business Office Zone

660 A business office zone is established for systems dedicated to hospital office productivity and does not
661 include direct patient-facing systems. This zone consists of traditional clients on an enterprise network,
662 such as workstations, laptops, and possibly mobile devices. Within the enterprise, the business office
663 zone will primarily interact with the enterprise services zone. This zone may also include Wi-Fi access.

664 5.3.1.1.4 Database Server Zone

665 A database server zone is established to house server components that support data persistence. The
666 database server zone may include data stores that aggregate potentially sensitive information, and,
667 given the volume, require safeguards. Databases may include PHI, so HIPAA privacy and security
668 controls are applicable. This zone consists of servers with databases. Ideally, applications in the
669 enterprise services zone and biomedical engineering zone use these databases instead of storing
670 information on application servers. This type of centralization allows for simplified management of
671 security controls to protect the information stored in databases.

672 5.3.1.1.5 Enterprise Services Zone

673 The enterprise services zone consists of systems that support hospital staff productivity. Enterprise
674 services may not be directly patient specific systems, but rather support core office functions found in a
675 hospital. This zone consists of traditional enterprise services, such as DNS, Active Directory, Identity
676 Service System, and asset inventory that probably lives in a server room or data center. These services
677 must be accessible from various other zones in the enterprise.

678 5.3.1.1.6 Clinical Services Zone

679 The clinical services zone consists of systems that pertain to providing patient care. Examples of systems
680 that would be hosted in this zone include the electronic health record (EHR) system, pharmacy systems,
681 health information systems, and other clinical systems to support patient care.

682 5.3.1.1.7 Biomedical Engineering Zone

683 The biomedical engineering zone establishes a separate area that enables a biomedical engineering
684 team to manage and maintain systems such as medical devices as shown in [Figure 5-2](#). This zone
685 consists of all equipment needed to provision and maintain medical devices. In the case of wireless
686 infusion pumps, this is where the pump management servers are hosted on the network.

687 5.3.1.1.8 Medical Device Zone

688 The medical device zone provides a network space where medical devices may be hosted. Infusion
689 pumps would be deployed in this zone. Infusion pump systems are designed so that all external
690 connections to EHR systems or vendor maintenance operations can be completed through an
691 associated pump server that resides in the biomedical engineering network zone. Access to the rest of
692 the network and internet is blocked. This zone contains a dedicated wireless network to support the
693 wireless infusion pumps, as explained in Section 5.3.1.2, [Medical Device Zone's Wireless LAN](#).

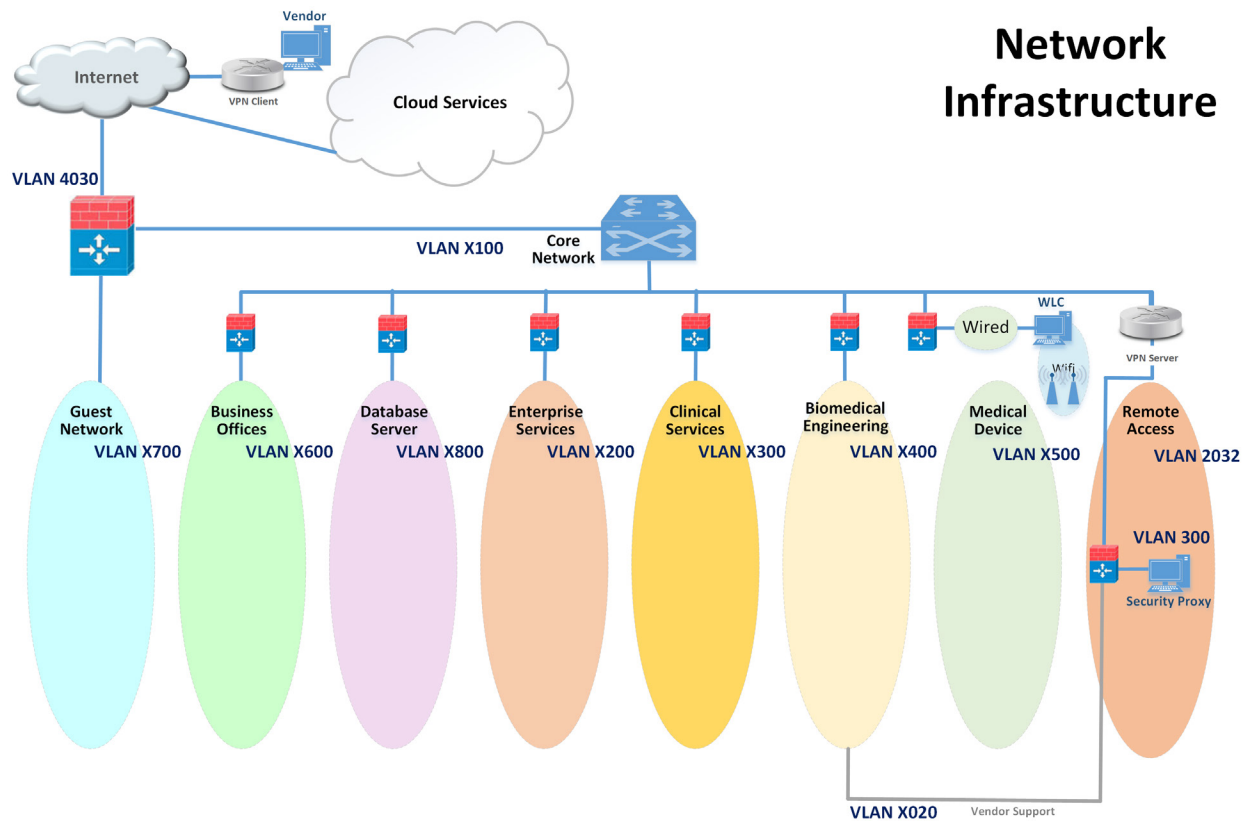
694 5.3.1.1.9 Remote Access Zone

695 The remote access zone provides a network segment that extends external privileged access so that
696 vendors may access their manufactured components and systems on the broader HDO network. Refer
697 to Section 5.3.1.4, [Remote Access](#) for additional technical details.

698 5.3.1.1.10 Final Network Architecture

699 [Figure 5-2](#) shows the interconnection of all components and zones previously described. It also
700 illustrates the connection to vendor and cloud services via the internet. VLAN numbers shown are VLAN
701 identifiers used in the lab, but may vary on actual healthcare enterprise networks.

702 Figure 5-2: Network Architecture with Segmentation



703

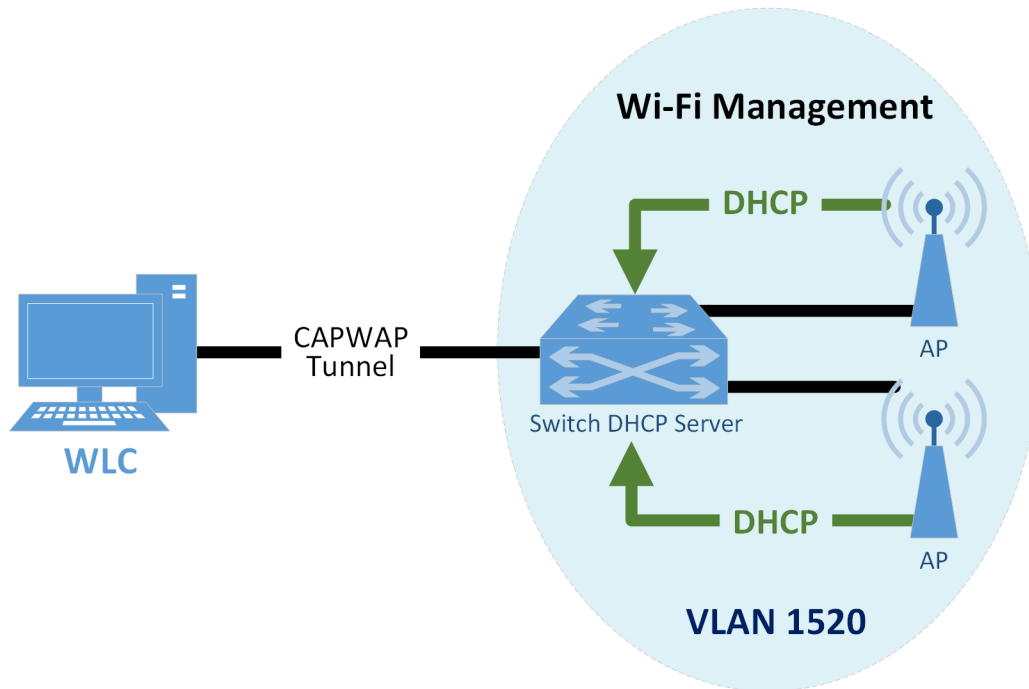
704 *5.3.1.2 Medical Device Zone's Wireless LAN*

705 The Wi-Fi management network is different in that it does not have a firewall/router that connects
 706 directly to the core network as shown in [Figure 5-3](#). This is a completely closed network used for the
 707 management and communication between the Cisco Aironet wireless Access Point (AP) and the Cisco
 708 Wireless LAN Controller (WLC). The WLC is the central point where wireless Service Set Identifiers
 709 (SSIDs), Virtual LANs (VLANs), and Wi-Fi Protected Access version 2 (WPA2) security settings are
 710 managed for the entire enterprise [8], [17], [33], [34], [35], [36], [42], [46], [47], [48], [49].

711 Two SSIDs were defined, IP_Dev and IP_Dev Cert. IP_Dev uses WPA2-PSK, and IP_Dev Cert uses WPA2-
 712 Enterprise protocols. In an actual HDO, two WLCs should be configured for redundancy. Initially, the
 713 wireless access points configure themselves for network connectivity like any other device using
 714 Dynamic Host Configuration Protocol (DHCP) from the switch DHCP server (see the green line in [Figure](#)
 715 [5-3](#)). The switch also sends DHCP option 43, which provides the IP address of the WLC. The AP then
 716 connects to the WLC to automatically download firmware updates and wireless configuration
 717 information. Finally, the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel and

718 encrypt wireless traffic (see the black line in [Figure 5-3](#)). The traffic is then routed to the enterprise
 719 network via the WLC [28], [37], [44], [50].

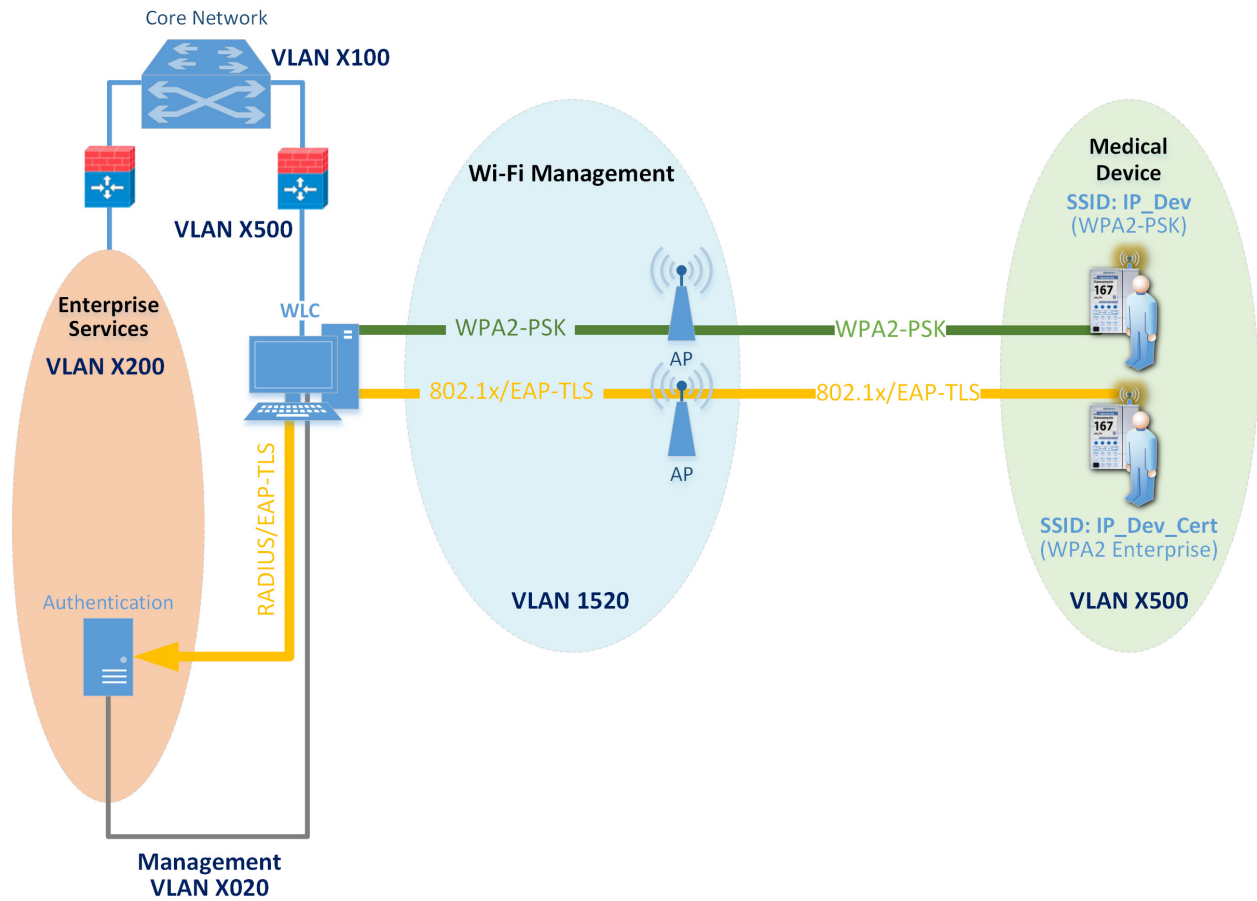
720 **Figure 5-3: Wi-Fi Management**



721

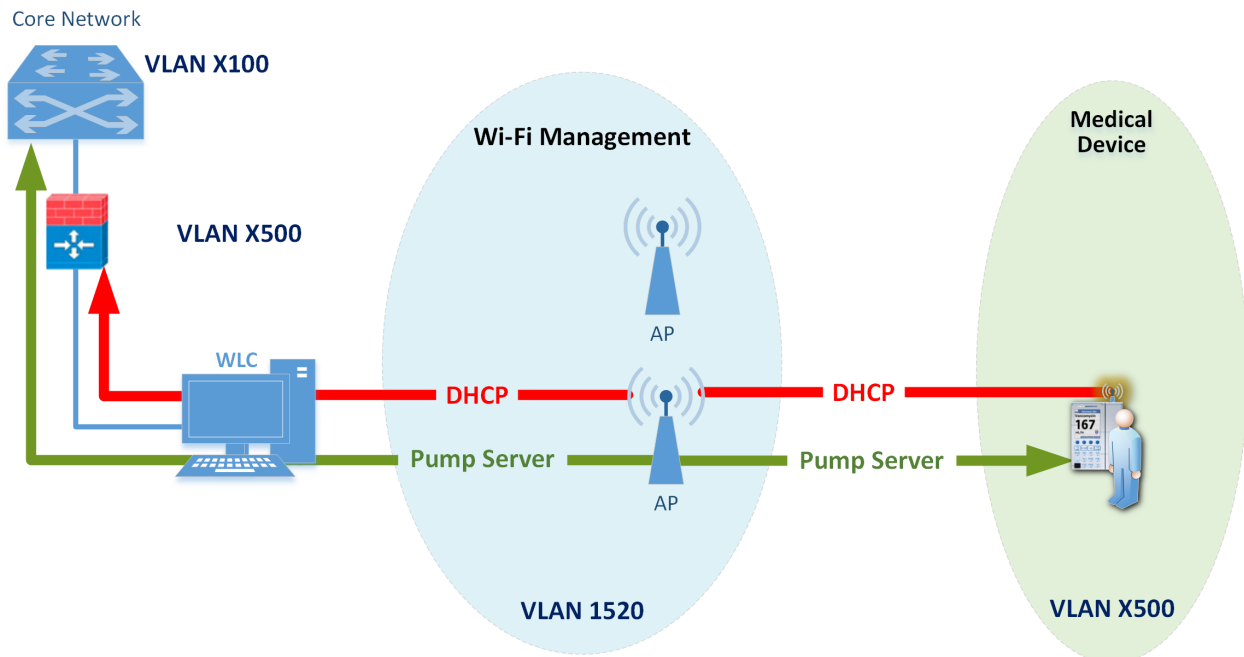
722 When a device first connects to the Wi-Fi network, it needs to authenticate with either the agreed-upon
 723 pre-shared key or certificate. The authentication process is tunneled from the AP back to the WLC as
 724 shown in [Figure 5-4](#). In the case of a pre-shared key, the WLC verifies that the client key matches (see
 725 green line). In the case of a certificate, the authentication process is passed from the WLC to the Cisco
 726 identity service engine (ISE) for validation using remote authentication dial-in user service (RADIUS)
 727 protocol (yellow line). Upon successful authentication, the device negotiates an encryption key and is
 728 granted link layer network access.

729 **Figure 5-4: Wi-Fi Authentication**



730

731 Once authentication is complete, typical network client activity is allowed. [Figure 5-5](#) shows how Dy-
 732 namic Host Configuration Protocol (DHCP) is used to contact the router to obtain network configuration
 733 information for the device (see red line). Once the network is configured, the infusion pump will at-
 734 tempt to connect to its provisioned pump server address on the enterprise network in the biomedical
 735 zone (see green line).

736 **Figure 5-5: Wi-Fi Device Access**

737

738 Using an enterprise-grade Wi-Fi system can simplify transitions to more secure protocols by decoupling
 739 Wi-Fi SSIDs and security parameters from the Wi-Fi spectrum and physical Ethernet connections. First,
 740 every AP only needs to broadcast on a single Wi-Fi channel (in each band) and can broadcast multiple
 741 SSIDs. This helps avoid interference due to multiple independent wireless systems trying to use the
 742 same frequencies. Second, each SSID can be tied to its own VLAN. This means logical network
 743 separation can be maintained in Wi-Fi without having to use additional spectrum. Third, multiple SSIDs
 744 can be tied to the same VLAN or standard Ethernet network. Each SSID can have its own security
 745 configuration as well. For example, in our use case, we have two different authentication mechanisms
 746 for granting access to the same network, one configured for WPA2-PSK and another for so-called
 747 *enterprise certificates*. This can be particularly useful for gradual transitions from old security
 748 mechanisms (e.g., WEP, WPA) or old Pre-Shared Keys (PSKs) to newer ones instead of needing to
 749 transition all devices at one time. In our case, to determine which devices may need reconfiguration to
 750 use certificates, we used the WLC to identify exactly which devices are using old PSK SSIDs. Once this
 751 number is reduced to an acceptable level, the old PSK SSID can be turned off and only certificate-based
 752 authentication will be allowed.

753 *5.3.1.3 Network Access Control*

754 This section describes how network access control using a wireless LAN, as shown above, is applied to
 755 the wireless infusion pumps.

756 Before we describe network access controls, it's important to discuss each pump's wireless protection
757 protocol. There are three available wireless protection protocols (WEP, WPA, and WPA2). We also
758 describe in-depth options for WPA2-PSK. Finally, we describe options for WPA2 across the HDO
759 enterprise. Many of the infusion pumps used in this NCCoE project are newer models, capable of
760 supporting various wireless protocols. For HDOs, WPA2 is the recommended wireless protocol to use.
761 WEP and WPA are considered insufficient for appropriately securing wireless network sessions. Our
762 architecture is designed to support multiple levels of access control for different groups of users. The
763 architecture is configured to use WPA2-PSK and WPA2-Enterprise security protocols for secure wireless
764 connections to accommodate the best available security mechanisms depending on which vendor
765 products your organization uses. Please note that a wireless infusion pump manufactured prior to 2004
766 may not be able to support these newer wireless security protocols [41].

767 The WPA2-PSK is often referred to as *pre-share key mode*. This protocol is designed for small office
768 networks and does not require an external authentication server. Each wireless network device
769 encrypts the network traffic using a 256-bit key. All pumps used in our example implementation support
770 this wireless security mode, and each pump performed properly using this mode. However, because all
771 devices share the same key in a pre-shared key mode using WPA2-PSK, if credentials are compromised,
772 significant manual reconfiguration and change management will be required.

773 WPA2 enterprise security uses 802.1x/EAP. By using 802.1x, an HDO can leverage the existing network
774 infrastructure's centralized authentication services such as remote authentication dial-in use service, or
775 RADIUS, authentication server to provide a strong client authentication. Cisco recommends that WPA2
776 Enterprise, which uses the AES (Advanced Encryption Standard) cypher for optimum encryption, be
777 used for wireless medical devices, if available. We implemented WPA2-Enterprise with EAP-TLS security
778 mode on several of our pumps to demonstrate that these pumps can leverage the public key
779 infrastructure (PKI) to offer strong endpoint authentication and the strongest encryption possible for
780 highly secure wireless transmissions. In this mode, pumps were authenticated to the wireless network
781 with a client certificate issued by DigiCert Certificate Authority. During the authentication process, the
782 pump's certificates are validated against a RADIUS authentication server using Cisco ISE. Automatic
783 logoff features allow the system to terminate the endpoints from the network after a predetermined
784 time of inactivity. Organizations manage and control the client certificates via the certificate authority.
785 With this capability, organizations may revoke and renew certificates as needed.

786 Once WPA2 is selected as the appropriate wireless protection protocol, certificates may be issued to
787 authenticate infusion pumps using 802.1x/EAP-TLS mode, as illustrated [Figure 5-6](#) [28], [29], [30], [31],
788 [32], [33], [34], [35], [36], [37], [38], [42], [46], [47], [48], [49], [50].

789 Certificate issuance involves the following three stages, denoted by shaded boxes in [Figure 5-6](#):

790 **1. Certificate Registration**

791 *Step 1:* Request a certificate from the DigiCert Certificate Authority, which is a Certificate Register
792 Manager. Request pump certificates through a standalone computer connected to the internet
793 using DigiCertUtil, a certificate request tool, on behalf a pump.

794 *Step 2:* The approved certificates are exported to the pumps using the specific tools provided by
795 pump vendors. Typically, this activity is performed by a biomedical engineer.

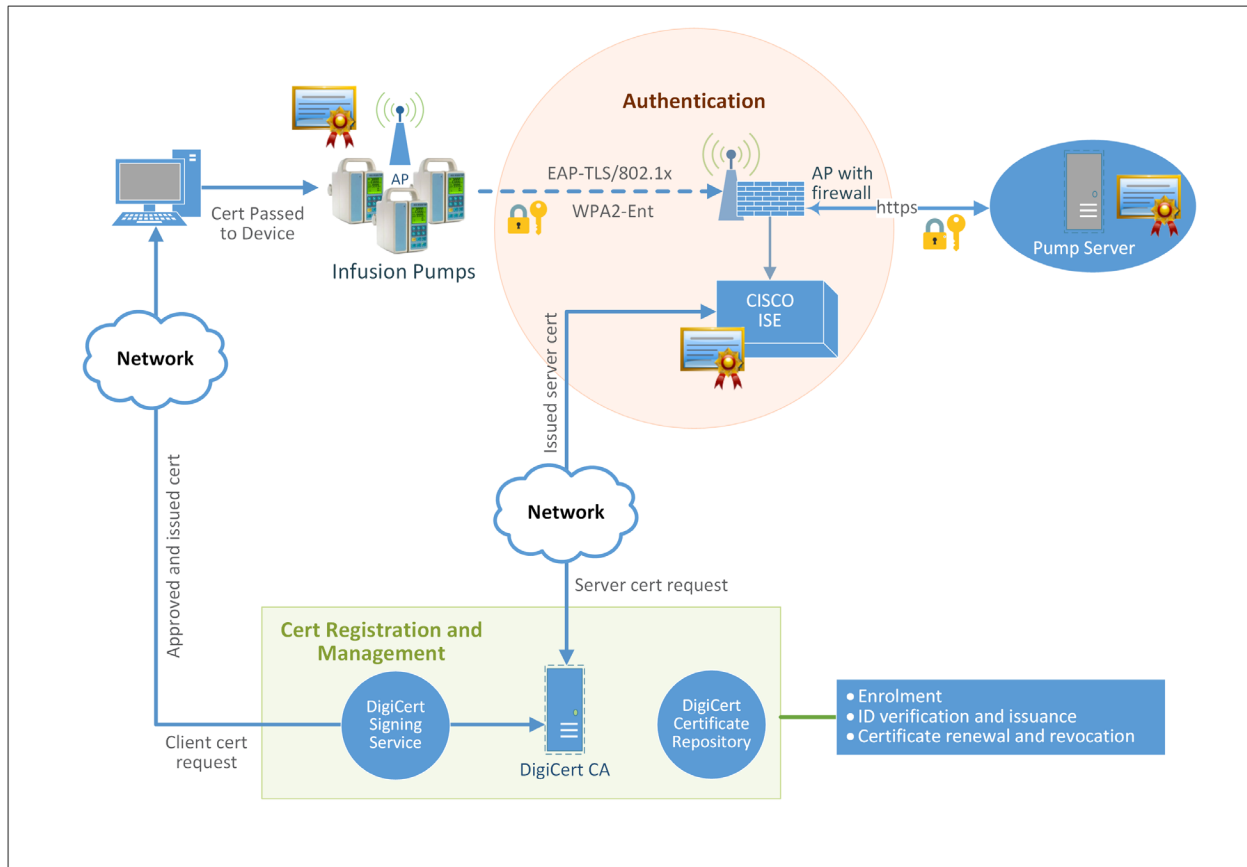
796 *Step 3:* Install the certificate into the Cisco ISE application.

797 **2. Authentication**

798 Authentication is performed by the Cisco ISE application to validate the pump certificate under the
799 802.1x/EAP-TLS. During the network access authentication procedure, the AP will pass the
800 certification information to ISE server for validation. Once passed, the connection between the
801 pump and the pump server will be established, and the data transmitted between the pump and AP
802 is encrypted.

803 **3. Certificate Management**

804 Certificate management will provide services to revoke certificates when they are no longer in use,
805 and will also manage the certificate revocation list, along with any related processes for renewing
806 old certificates.

807 **Figure 5-6: Network Access Control**

808

809 The detailed process for setting up the 802.1x network authentication for pump and pump server
 810 communication is documented in Volume C of the How-to guide.

811 *5.3.1.4 Remote Access*

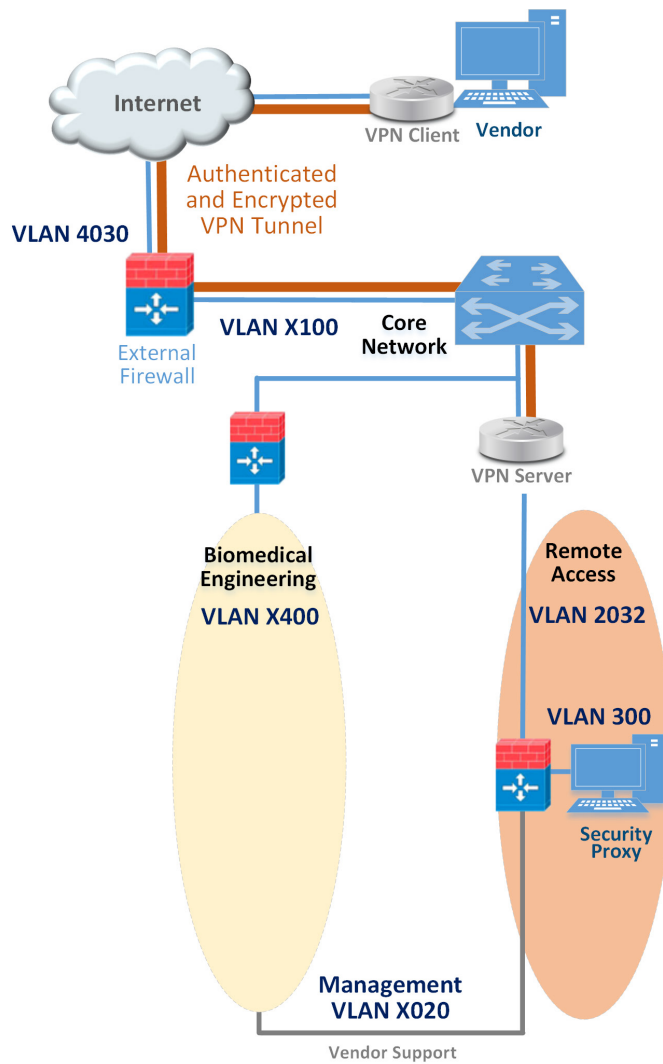
812 Many medical devices and their back-end management systems required access by manufacturers for
 813 device repairs, configuration, software, and firmware patching and updates, or maintenance. A vendor
 814 network segment (VendorNet) is designed to provide external privileged access for vendors to their
 815 manufactured components and systems that reside within an HDO's architecture. In the NCCoE lab, a
 816 VendorNet is implemented using TDi ConsoleWorks. ConsoleWorks is a vendor-agnostic interface that
 817 gives organizations the ability to manage, monitor, and record virtually any activities in the IT
 818 infrastructure that come from external vendors.

819 Communication using TDi ConsoleWorks for vendor access to products does not require the installation
 820 of software agents to establish connections for managing and monitoring targeted components.

821 Established connections are persistent to facilitate IT operations, enforce security, and maintain
822 comprehensive audit trails. All information collected by ConsoleWorks is time-stamped and digitally
823 signed to ensure information accuracy, empower oversight, and meet compliance requirements.
824 Through a standard web browser, ConsoleWorks can be securely accessed from any geographical
825 location, eliminating the need for administrators and engineers to be locally present to perform their
826 work.

827 Remote access is only allowed through a specific set of security mechanisms. This includes using a VPN
828 at the network layer as shown in [Figure 5-7](#) client, for vendors to authenticate to the VPN server [43],
829 [44], [51].

830 **Figure 5-7: Remote Access VPN**

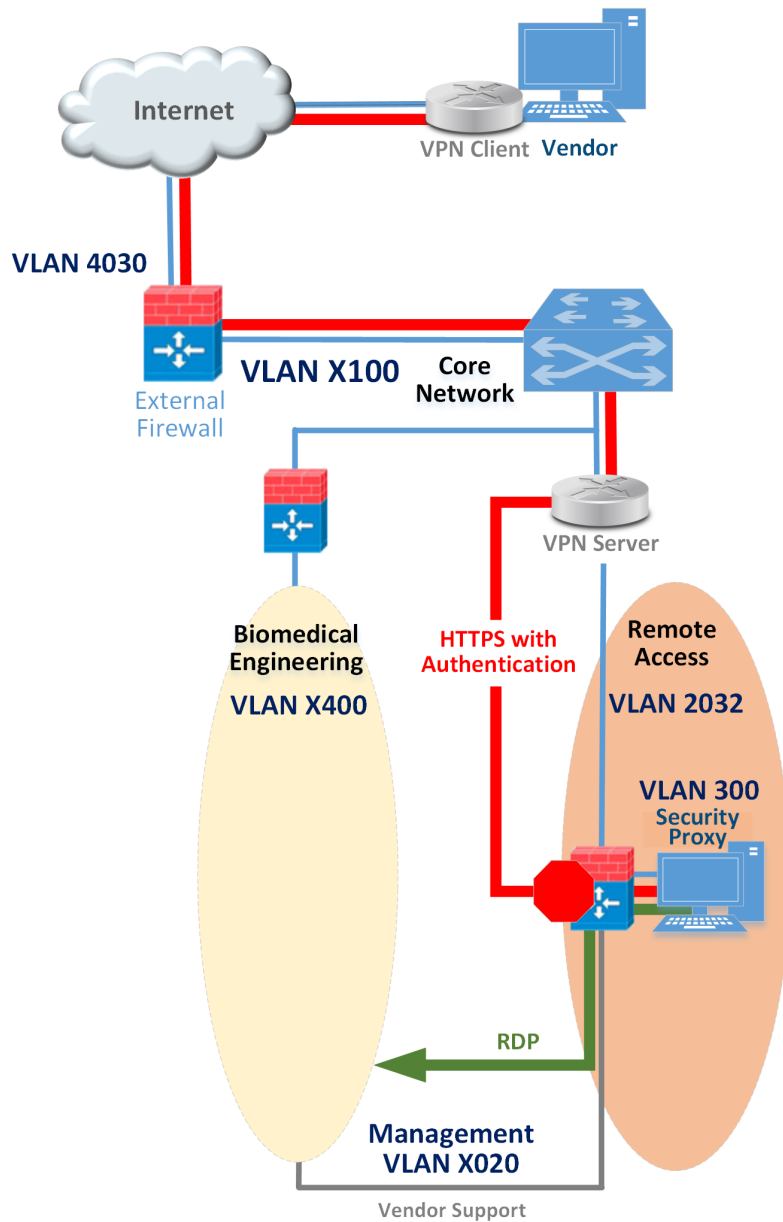


831

832 After the VPN connection is established at the application layer, the security proxy will restrict who can
833 access certain resources within the enterprise network, as depicted in [Figure 5-8](#). Vendors also
834 authenticate to the HTTPS-based security proxy (see red line). Based on the vendor's role, the security
835 proxy will facilitate a Remote Desktop Protocol (RDP) connection to equipment in the biomedical
836 engineering zone via the vendor support network (see green line). The credentials used to authenticate
837 the RDP connection are stored by the security proxy and not disclosed to the vendor.

838 The remote access firewall/router is configured so that direct access between the VPN and vendor
839 support is denied and the only allowed path is through the security proxy (see stop sign). Additionally,
840 the firewall/router can further restrict what is accessible at the network layer from the security proxy.
841 The security proxy is granted access to the internet to support patching and email alerts. The public IP
842 address of the external firewall is configured to forward VPN traffic to the IP address of the VPN server
843 [43], [44], [46], [47], [49], [51], [52], [53].

844 **Figure 5-8: Remote Access**



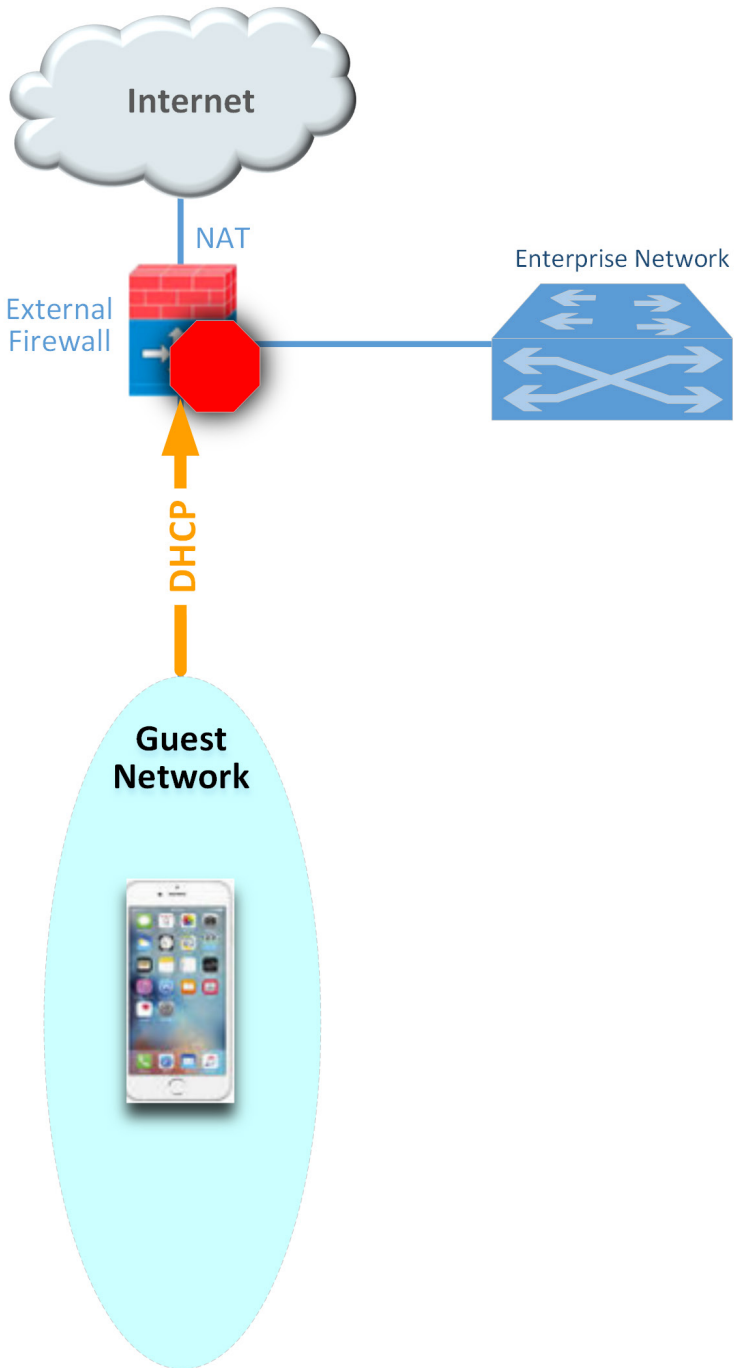
845

846 **5.3.1.5 External Access**

847 A guest network allows visitors or patients to access internet services during their visit. As explained in
 848 the previous section (Guest Network Zone), the work traffic tends not to be of a clinical nature, but is
 849 offered as a courtesy to hospital visitors and patients to access the internet. The external firewall marks
 850 the boundary between the enterprise and the internet. As shown in [Figure 5-9](#), this is the only point in

851 the network where network address translation (NAT) is used. Additionally, the guest network for
852 personal devices connects to the internet through the external firewall. The guest network is configured
853 such that traffic cannot go between the enterprise and guest networks – only out to the internet. This is
854 denoted by the stop sign. The external firewall is configured to provide the necessary services for guest
855 users to use the internet, such as DHCP, which allows dynamic addressing for anyone. Typically,
856 consumer equipment is connected here, such as smart phones, tablets, and personal entertainment
857 systems ([Figure 5-9](#)) [52].

858 Figure 5-9: External



859

860 5.3.2 Pump Controls

861 Wireless infusion pumps have the following controls:

- 862 ▪ endpoint protection
- 863 ▪ hardening
- 864 ▪ data protection.

865 5.3.2.1 Endpoint Protection

866 Traditional security relies on the network border to provide security protection to its internal nodes,
867 using security technologies such as application firewalls, proxy gateways, centralized virus scan, network
868 intrusion detection, and prevention systems. This is no longer considered a best practice. The nodes,
869 such as networked medical devices, should participate in their own security. Otherwise, the device can
870 become the weakest element in the enterprise and present a risk to the entire HDO network.

871 To avoid the single point of failure caused by an unsecured node, every system should have an
872 appropriate combination of local protections applied to it. These protections include code signing, anti-
873 tampering, encryption, access control, white listing, and others.

874 5.3.2.2 Hardening

875 Wireless infusion pumps and their servers are considered computing endpoints when it comes to
876 hardening the software contained within these devices. Medical devices usually contain third-party
877 commercial, off-the-shelf (COTS) products, including proprietary or commercial embedded operating
878 systems, network communication modules, runtime environments, web services, or databases. Because
879 these products can contain vulnerabilities, medical devices may also inherit these vulnerabilities just by
880 using the products [2], [3], [7], [9], [25]. Therefore, it is important to identify all software applications
881 used on medical devices, implement securing and hardening procedures recommended by the
882 manufacturers, and apply timely patches and updates to guard against any newly discovered threats.

883 Hardening may include the following:

- 884 ▪ disabling unused or unnecessary communication ports and services
- 885 ▪ changing manufacturer default administrative passwords
- 886 ▪ securing remote access points if there are any
- 887 ▪ confirming the firmware version is up to date
- 888 ▪ ensuring hashes or digital signatures are valid

889 However, please note that most infusion pumps do not have the same level of storage resources and
890 CPU processing capability as those provided for personal computers and servers.

891 *5.3.2.3 Data Protection*

892 The two primary reasons for data protection are confidentiality and integrity. Medical devices may
893 contain patient data such as patient name, medical record number, gender, age, height, weight,
894 procedure number, medication and treatment information, or other identifiers that may constitute PHI.
895 PHI must be appropriately protected, for example, through encryption or other safeguard measures
896 that would prevent unauthorized disclosure of such information.

897 Infusion pumps may also contain configuration data such as drug libraries specifying dosage and
898 threshold limits. This data must be protected against compromises as well. Our defense-in-depth
899 approach for data integrity involves sandboxing the critical system files stored in pump servers using
900 Symantec Advanced Data Center Security and encrypting messages when communicating between a
901 medical infusion pump and the backend infusion management system, via Internet Protocol Security or
902 secure sockets layer encryption (e.g., https, TLS).

903 *5.3.3 Pump Server Controls*

904 Pump server features vary. Usually, a pump server can be used to distribute firmware, the drug library,
905 other software updates used inside the devices, or as a tool for providing services such as reporting and
906 device asset management. Data collected by the infusion pump server is valuable for further analysis to
907 provide reports on trends, compliance checking, and to measure infusion safety.

908 Because pump servers connect to infusion pumps to deliver and receive infusion-related information, it
909 is also important to secure the infusion pump server, its associate applications, databases and
910 communication channels as well.

911 *5.3.3.1 User Account Controls*

912 Access to the pump server typically implements user name/password authentication. After the pump
913 server is installed, an initial step is to define the password policy that applies to users accessing the
914 pump server. When managing user accounts for a pump server, common cybersecurity hygiene should
915 include the following:

- 916 ▪ changing factory default passwords
- 917 ▪ enforcing password policies
- 918 ▪ assigning each user's access level using the least privilege principle
- 919 ▪ if supported, using centralized access management, such as LDAP for user account,
920 management at the enterprise level
- 921 ▪ configuring auto logout

922 *5.3.3.2 Communication Controls*

923 Pump servers interface with many other systems or components such as: databases, web services, and
924 web portals. Communications between different systems can be configured. Pump servers might
925 provide choices for selecting unsecure or secure TCP/IP ports for communication. We recommend using
926 secure (e.g., stateful, encrypted network sessions) ports for message communication or for package
927 download.

928 There may be a default setting for the communication interval, in number of seconds, for
929 communication attempts between the server and the pump. Be sure to set this idle time-out setting
930 properly.

931 *5.3.3.3 Application Protection*

932 Application protection refers to software applications running on the pump servers. Most of the
933 software application security concerns and security controls used on traditional personal computers and
934 servers may also be applied to pump servers to protect data integrity and confidentiality. These control
935 measures may include:

- 936 ▪ trusted applications
- 937 ▪ stronger access control mechanisms for pumps and pump servers
- 938 ▪ better key management
- 939 ▪ application white listing
- 940 ▪ sandboxing applications
- 941 ▪ performing code-signing verification for newly installed software
- 942 ▪ applying the latest patches and software updates
- 943 ▪ encrypting message data in-transit, or at rest

944 Server security baseline integrity is achieved via the use of three Symantec cybersecurity products on an
945 enterprise network with a specific focus on wireless infusion pumps:

- 946 ▪ Symantec Data Center Security: Server Advanced (DCS:SA)
- 947 ▪ Symantec Endpoint Protection (SEP)
- 948 ▪ Symantec Advanced Threat Protection: Network (APT:N)

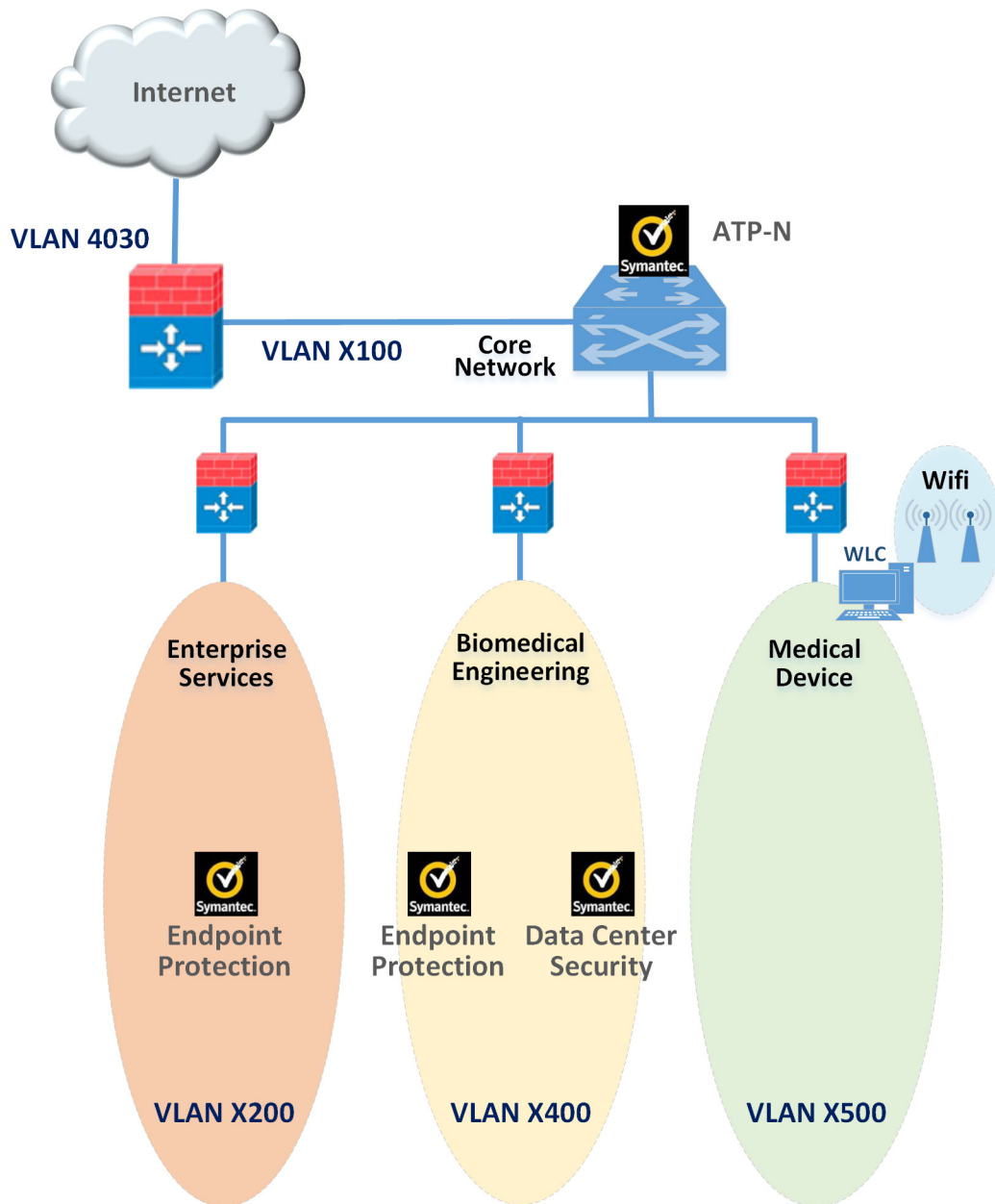
949 Each of these products provide protections for components in the enterprise systems in different levels.
950 With pre-built policies, the Data Center Security Server installed can provide out-of-the-box host
951 Intrusion IDS and IPS by monitoring and preventing suspicious server activities on pump servers. The use
952 of DCS also provides the host firewall service for controlling inbound and outbound network traffic to
953 and from a protected server. Using DCS, the configuration settings, file, and file systems in the pump

954 server can be locked down using policy-based least privilege access controls to restrict application and
955 operating system behavior and prevent file and system tampering.

956 Like DCS, Symantec's Endpoint Protection (SEP) provides similar protection for endpoint devices and
957 servers. SEP features in-memory exploit mitigation and anti-virus file protection to block malware from
958 infecting protected endpoint servers. This will reduce the possibility of zero-day exploits on popular
959 software that may not have been properly patched or updated. To protect endpoint servers, an SEP
960 agent must be installed on servers.

961 Advanced Threat Protection: Network (ATP:N) can provide network-based protection of medical device
962 subnets by monitoring internal inbound and outbound internet traffic. It can also be used as a
963 dashboard to gain visibility to all devices and all network protocols. In addition, if ATP:N is integrated
964 with the SEP, ATP can then monitor and manage all network traffic from the endpoints and provide
965 threat assessments for dangerous activity to secure medical devices on an enterprise network. The use
966 of these Symantec security products is depicted in [Figure 5-10](#) below.

967 Figure 5-10: Pump Server Protection



968

969 5.3.4 Enterprise Level Controls

970 5.3.4.1 *Asset Tracking and Inventory Control*

971 Medical asset management includes asset tracking and asset inventory control. Asset tracking is a
972 management process used to maintain oversight of the equipment, using anything from simple
973 methods such as pen and paper to record equipment, to more sophisticated IT asset management
974 platforms. HDOs can use asset tracking to verify that a device is still in the possession of the assigned,
975 authorized users. Some more advance tracking solutions may provide service for locating missing or
976 stolen devices.

977 Inventory management is also important throughout a medical device’s life cycle. Inventory tracking
978 should not be limited to hardware inventory management. It should also be expanded to include
979 software, software versions, data stored and accessed in the devices, for security purpose. HDOs can
980 use this type of inventory information to verify compliance with security guidelines and check for
981 exposure of confidential information to unauthorized entities.

982 5.3.4.2 *Monitoring and Audit Controls*

983 Logging, monitoring, and auditing procedures are essential security measures that can be used to help
984 HDOs prevent incidents and provide an effective response when a security breach occurs. Logging
985 records events to various logs; monitoring oversees the events for abnormal activities, such as scanning,
986 compromises, malicious code, and denial of services in real time; and auditing reviews and checks these
987 recorded events to find abnormal situations or evaluate if the applied security measures are effective.
988 By combining the logging, monitoring, and auditing features, an organization will be able to track,
989 record, review and respond to abnormal activities and provide historical records when needed.

990 Many malware and virus infections can be almost completely avoided by using properly configured
991 firewalls or proxies with regularly updated knowledge databases and filters to prevent connections to
992 known malicious domains. It is also important to review your firewall logs for blocked connection
993 attempts so that you can identify the attached source and remedy infected devices if needed.

994 In our example implementation, user audit controls—simple audits—are in place. Although additional
995 security incident and event managers (SIEM) and centralized log aggregation tools are recommended to
996 maximize security event analysis capabilities, aggregation and analytics tools like these are considered
997 out of scope for this project iteration.

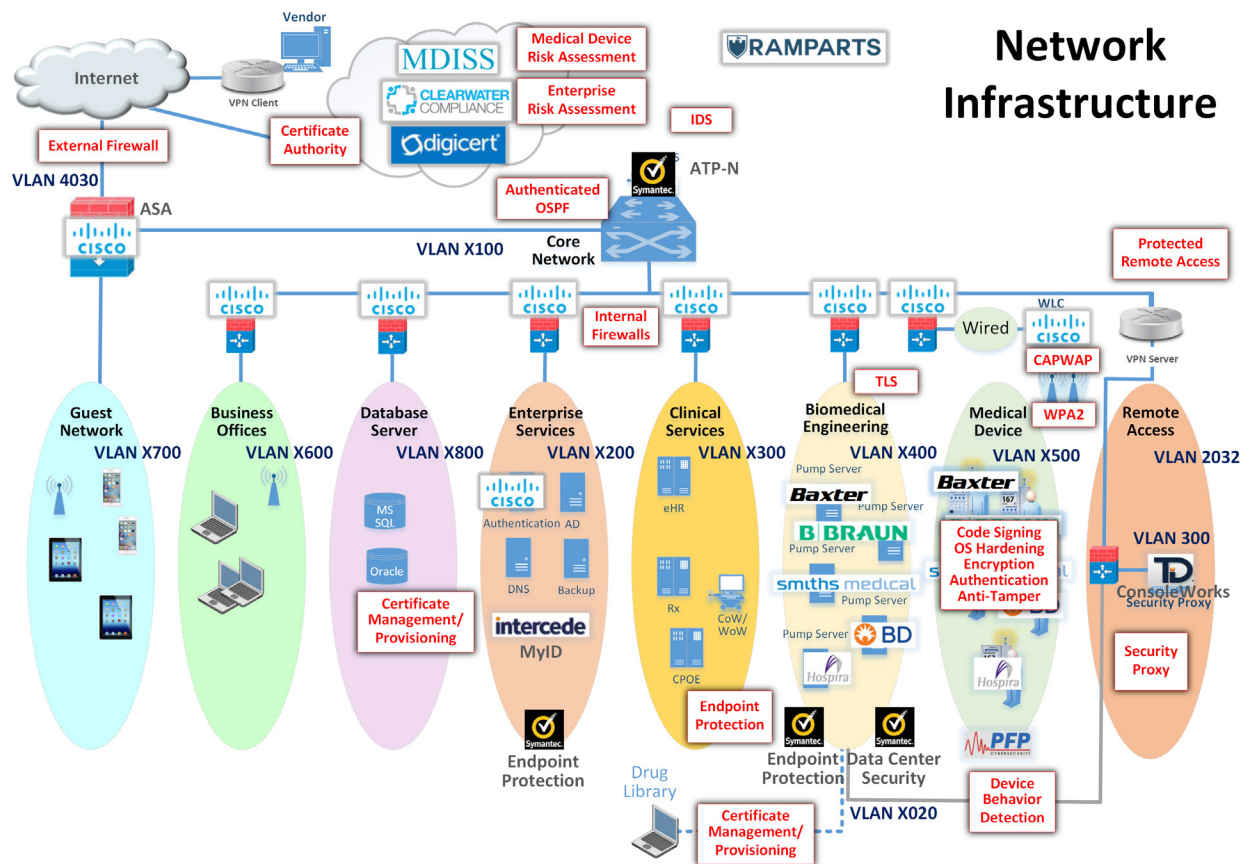
998 Each system is monitored for compliance with a secure configuration baseline. Each system is also
999 monitored for risks to known good, secure configurations by vulnerability scanning tools. In our project,
1000 the AP provided by Cisco, the Cisco ISE as Radius authentication server, VendorNet provided by TDI, and
1001 the pump servers from each vendor are all equipped with proper monitoring and logging capabilities.
1002 Real-time monitoring for events happening within these systems can be analyzed and compared to the
1003 baseline. If any abnormal behavior occurs, it can be detected. The auditing of data was considered out

1004 of scope for this reference design because the absence of an actual data center made auditing behavior
 1005 impractical.

1006 5.4 Final Architecture

1007 The target architecture, depicted in [Figure 5-11](#), indicates the implementation of network segmentation
 1008 and controls as described by this practice guide. Segmentation identified nine zones, ranging from the
 1009 guest network to the medical device zone, and includes zones for Wi-Fi infrastructure, and core network
 1010 infrastructure. The zoned concept implements firewall/router devices to enforce segmentation, with
 1011 the firewall enforcing limited trust relationships between each zone. Noted in the diagram are
 1012 processes that have impact on the overall architecture. Security controls are implemented to enforce
 1013 encryption on network sessions. For Wi-Fi, leveraging standard protocols such as WPA2- PSK and WPA2-
 1014 Enterprise created a secure channel for the pumps to communicate with the (AP)s, and to use TLS to
 1015 secure the communication channel from the pumps to the server.

1016 **Figure 5-11: Target Architecture**



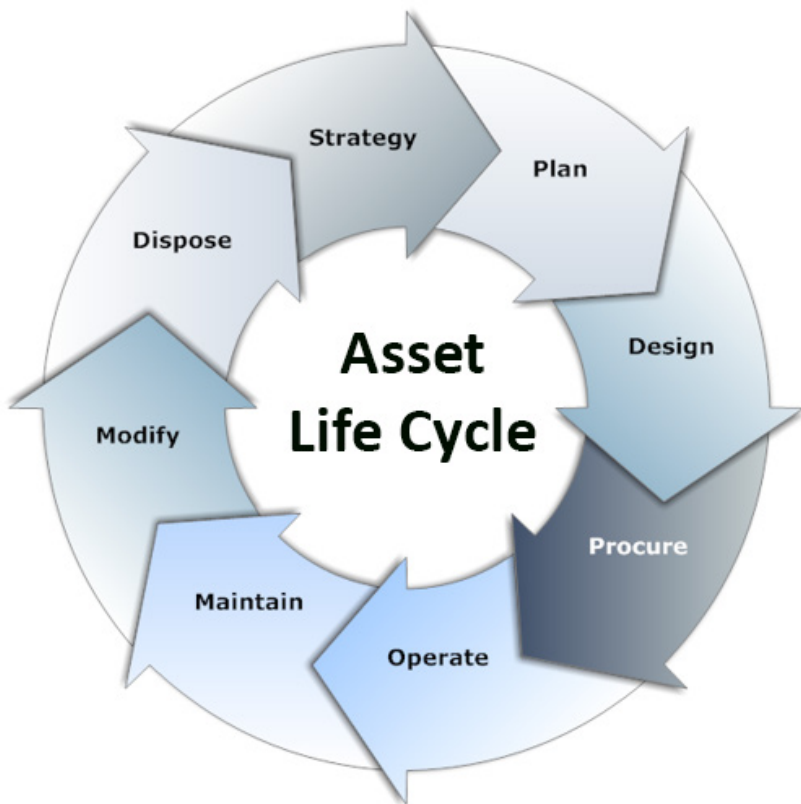
1017

1018 **6 Life Cycle Cybersecurity Issues**

1019 Configuration management throughout a device’s life cycle is a key process that is necessary for the
1020 support and maintenance of medical devices [3]. [NIST SP 1800-5: IT Asset Management for the Financial](#)
1021 [Services Sector](#) discusses IT Asset Management (ITAM), and, although the focus of the document
1022 pertains to financial services, similar challenges exist in healthcare [54]. Establishing a product life cycle
1023 management program addresses a few of the risks noted in previous sections of this guide, and should
1024 be considered as part of a holistic program for managing risks associated with infusion pump
1025 deployments.

1026 [Figure 6-1](#) illustrates a typical life cycle for an asset, and this model can be applied to medical devices.
1027 The sections below will take specific phases of the asset life cycle and discuss essential cybersecurity
1028 activities that should occur during those phases.

1029 **Figure 6-1: Asset Life Cycle [55]**



1030

1031 6.1 Procurement

1032 Asset life cycle management typically begins with Strategy, Plan, and Design phases, which lead into
1033 procurement. These phases are opportunities for hospitals to define requirements and identify where
1034 security controls may be implemented on infusion pumps or other devices that the hospital intends to
1035 acquire.

1036 Phases leading into procurement enable the HDO, reseller, or manufacturer to ensure that the
1037 equipment that the HDO will deploy offers the appropriate combination of security and functionality
1038 required to render patient care. These phases also enable the hospital to implement appropriate
1039 security controls to safeguard the device and the information that it may store or process.

1040 Purchasers at HDOs may request manifests or architectural guidance on secure deployment of the
1041 equipment and may perform research on products and the manufacturers that they have selected.
1042 While performing the research, HDOs may begin a risk assessment process to ensure that risks are
1043 mitigated.

1044 Manufacturers maintain a document referred to as the MDS2 (Manufacturer Disclosure Statement for
1045 Medical Devices) that an HDO may review, enabling the HDO to determine possible vulnerabilities and
1046 risks [56]. Hospital purchasers may also determine if vulnerabilities exist in the proposed equipment by
1047 reviewing the FDA-hosted MAUDE database (Manufacturer and User Facility Device Experience).

1048 Hospitals should also obtain any necessary training, education, and awareness material from the
1049 manufacturer and educate staff about the deployment, operation, maintenance, and security features
1050 available on their equipment. HDOs might consider writing user-friendly documentation to ensure that
1051 staff can use the equipment with confidence and competence.

1052 Performing research and risk analysis during the phases leading into procurement will allow HDOs to
1053 make informed decisions. For further reference, we note that the Mayo Clinic has produced a best
1054 practice document that discusses procurement.

1055 6.2 Operation

1056 After procuring their equipment, hospitals onboard it during the Operation and Maintenance phases.
1057 Equipment purchasers should apply asset management processes (e.g., asset tagging and entry into a
1058 configuration management database or some other form of inventory tracking), and have standard
1059 baseline configurations implemented. Wireless infusion pumps may need to be configured to connect to
1060 a hospital's Wi-Fi network (Medical Device zone, as depicted in the architecture section of this
1061 document; see Section 5.3.1.2, [Medical Device Zone's Wireless LAN](#) and implement digital certificates to
1062 allow for device authentication.)

1063 As noted above, hospitals should implement some type of configuration management database or asset
1064 inventory that captures granular information about the device. Implementing an ITAM mechanism

1065 enables the hospital to have visibility into their infusion pump deployment, with captured information
1066 that describes the make/model, firmware, OS, and software versions, a general description of the
1067 applied configuration along with change history, and physical location within the hospital. Regular
1068 maintenance of the ITAM would reduce risks, for example, that may emerge based on loss/theft, as well
1069 as provide a central knowledge repository that allows the hospital to coordinate any required
1070 maintenance or refresh.

1071 As part of deployment, hospitals should apply practices noted by the manufacturer (e.g., regarding
1072 access control and authentication). As noted above, digital certificates should be installed to allow for
1073 device authentication to Wi-Fi, but engineers should implement access control and auditing
1074 mechanisms where applicable.

1075 **6.3 Maintenance**

1076 Pump manufacturers have two types of systems that require updating: the pumps and the pump
1077 servers. Pumps may implement control systems in firmware (writeable, non-volatile storage that may
1078 include an embedded operating or other control system). Control systems may be maintained through
1079 an update process that involves replacing all or parts of the operating or control system. Server
1080 components may be implemented on more conventional IT systems, using commercial operating
1081 systems (e.g., Windows or Linux variants).

1082 Another aspect of configuration management that HDOs will want to pursue is that of patching.
1083 Patching, known colloquially as *bug fixing*, does not require a full replacement of software and is
1084 generally performed on pump servers. The patch frequency that manufacturers generally adhere to is
1085 monthly for patches and yearly for updates. This observation on timing comes from industry, not NIST—
1086 and is considered standard practice, rather than advice.

1087 In addition to identifying patch frequency, organizations must be aware of likely vulnerabilities and the
1088 risks they introduce into the enterprise, and then decide whether a patch should be applied. [NIST SP
1089 800-40 Guide to Enterprise Patch Management Technologies](#) discusses the importance of patch
1090 management and the challenges.

1091 **6.4 Disposal**

1092 The *Dispose* phase of the ITAM life cycle comes into play when products reach their end of life and are
1093 removed from hospital service. Wireless infusion pumps have increased in sophistication and
1094 information that each device may use, process, or store. The information found on pumps and related
1095 equipment may include sensitive information or information that may be regarded as PHI. As such,
1096 hospitals should seek to implement mechanisms to ensure that any sensitive information is removed
1097 from all storage areas that a pump or its system components may maintain. Practices to remove that
1098 information may be found in NIST SP 800-88 *Guidelines for Media Sanitation* [27].

1099 **7 Security Characteristics Analysis**

1100 We identified the security benefits of the reference design, how they map to NIST Cybersecurity
1101 Framework (CSF) subcategories, and the mitigating steps to secure the reference design against
1102 potential new vulnerabilities [10], [14].

1103 **7.1 Assumptions and Limitations**

1104 Our security analysts reviewed the reference architecture and considered if the integration described in
1105 this guide would meet security objectives. The analysts purposely avoided testing products, and readers
1106 should not assume any endorsement or diminution of the value of any vendor products. Although we
1107 have aimed to be thorough, we counsel those following this guide to evaluate their own
1108 implementation to adequately gauge risks particular to their organizations.

1109 **7.2 Application of Security Characteristics**

1110 Using the CSF subcategories to organize our analysis allowed us to systematically consider how well the
1111 reference design supports specific security activities and provides additional confidence that the
1112 reference design addresses our use case security objectives. The remainder of this subsection discusses
1113 how the reference design supports each of the identified CSF subcategories [10].

1114 **7.2.1 Supported CSF Subcategories**

1115 The reference design focuses primarily on the *Identify* and *Protect* function areas (i.e., subcategories) of
1116 the CSF. Specifically, the reference design supports:

- 1117 • three activities in the CSF *Identify* function area: Asset Management, Business Environment, and
1118 Risk Assessment
- 1119 • activities from each category of the CSF *Protect* function area, except for Awareness and
1120 Training

1121 We discuss these CSF subcategories in the following subsections.

1122 **7.2.1.1 *ID.AM-5: Resources (e.g., Hardware, Devices, Data, Time, and Software) are*** 1123 ***Prioritized Based on Their Classification, Criticality, and Business Value***

1124 To address this subcategory of the *Identify* function, we conducted an asset inventory as part of the risk
1125 management process. For this project, we identified assets and entered them into the Clearwater
1126 Compliance IRM|Analysis™ tool. This risk analysis tool categorized project resources into types of
1127 assets. Additionally, it characterized the system, enabling us to address the criticality of our resources.
1128 Our project only partially satisfies the *Resources* subcategory as we focused on technical solutions and
1129 did not write a business impact assessment or business continuity plan.

1130 *7.2.1.2 ID.BE-1: The Organization’s Role in the Supply Chain is Identified and*
1131 *Communicated*

1132 Organizations who may be using this guide are the end users of medical devices. NIST SP 800-53, control
1133 SA-12, most directly applies to such end users because it directs users to define which security
1134 safeguards to employ to protect against supply chain threats [14]. Our implementation uses network
1135 segmentation to limit exposure to the wireless infusion pump from other areas within a hospital
1136 network. This is done because if a vulnerability is identified in a device, segmentation and access control
1137 will help safeguard the medical device until the vulnerability can be properly addressed.

1138 *7.2.1.3 ID.RA-1: Asset Vulnerabilities are Identified and Documented*

1139 Given a reasonably long life cycle, even the best designed electronic asset will eventually be impacted
1140 by a vulnerability. Medical devices can have a long product life cycle, per TIR57, “Device or platform
1141 used for decades” [9], [25]. Identifying vulnerabilities in an asset may occur via various means. Some
1142 may be identified through onsite testing; however, often the manufacturer or a researcher will find the
1143 vulnerability. An effective risk management program is essential to reduce the likelihood that an
1144 identified vulnerability will be exploited. This implementation uses a combination of risk analysis tools
1145 and methods to help reduce the impact a vulnerability may have on the build.

1146 *7.2.1.4 PR.AC-1: Identities and Credentials are Issued, Managed, Revoked, and Audited*
1147 *for Authorized Devices, Users, and Processes*

1148 Following the segmentation approach used to separate hospital networks into zones, our
1149 implementation employs role-based security, which limits access based on who actually need to access
1150 the pump. HDO users with no business need are not permitted access to pumps, pump servers, or
1151 related components. Most users, including biomedical staff, are granted access via active directory.
1152 Although our NCCoE lab did not use single-sign-on (SSO), using SSO can make pump access seamless to
1153 an end user. How to manage credentials of clinicians who operate the pump directly is beyond the
1154 scope of this guide.

1155 Remote access is necessary to maintain proper functionality of infusion pumps, but the mechanism for
1156 gaining and controlling remote access varies depending on the user type. Hospital staff such as
1157 biomedical engineers remotely access pumps through a VPN and hardened gateway at the application
1158 layer. Such users are considered trusted HDO staff with access to other network resources throughout
1159 the enterprise.

1160 Pump manufacturers who may need to reach a device for maintenance or troubleshooting can gain
1161 access into a VendorNET zone only, from which they can access pumps and pump servers, but not other
1162 zones in the enterprise. Our example implementation uses ConsoleWorks for authentication, role-based
1163 access control, and recording system management actions of remote vendor activity.

1164 *7.2.1.5 PR.AC-4: Access Permissions and Authorizations are Managed, Incorporating the*
1165 *Principles of Least Privilege and Separation of Duties*

1166 This CSF subcategory is supported for the pumps and pump servers with Data Center Security (DCS). The
1167 configuration settings, file, and file systems in the pump server are restricted, thereby implementing
1168 policy-based least privilege access control. DCS restricts application and operating system behavior and
1169 prevents unauthorized users from tampering with files and systems.

1170 Least privilege is also addressed via the network design itself. By limiting user access to the zones where
1171 a user has a business need for access, the architecture seeks to enforce the concept of least privilege
1172 and separation of duties.

1173 *7.2.1.6 PR.AC-5: Network Integrity is Protected, Incorporating Network Segregation*
1174 *Where Appropriate*

1175 Network segmentation is a key function of this reference design. Segregating Guest, Business Office,
1176 Database, Enterprise Services, Clinical Server, and Biomedical Engineering networks from the Medical
1177 Device zone reduces the risk of medical devices being negatively impacted from malware or an exploit
1178 in another zone. Using a combination firewall/router device to segregate the zones also limits risk to the
1179 enterprise should a vulnerability be exploited within the medical device zone.

1180 *7.2.1.7 PR.DS-2: Data-In-Transit is Protected*

1181 Data-in-transit occurs when data travels from the drug library on a pump server to an infusion pump.
1182 The information being passed most frequently will be types of drugs and dosage range. This information
1183 is not PHI; however, the availability and integrity of this information are important. This project uses
1184 WPA2-AES, which authenticates pumps to the wireless network with client certificate issued by DigiCert
1185 Certificate Authority.

1186 *7.2.1.8 PR.DS-6: Integrity Checking Mechanisms are Used to Verify Software, Firmware,*
1187 *and Information Integrity*

1188 This CSF subcategory is supported with server and agent products to monitor and lock-down
1189 configuration settings, files, and file systems in the pump server using the policy-based least privilege
1190 access control. This limits application and operating system to expected behavior and reduces the
1191 likelihood of system from digital tampering.

1192 *7.2.1.9 PR.IP-1: A Baseline Configuration of Information Technology/Industrial Control*
1193 *Systems is Created and Maintained Incorporating Appropriate Security Principles*
1194 *(e.g., Concept of Least Functionality)*

1195 A mature cybersecurity program follows a documented secure baseline for traditional information
1196 technology components and medical devices. This NCCoE project has implemented hardening for each

1197 component used in the build and documented the steps taken. This initial step produces a secure
1198 baseline configuration. Because this project uses five different types of wireless infusion pumps, the
1199 baseline is of limited use; however, in a healthcare organization with many medical devices and multiple
1200 biomedical and information technology professionals, it is essential to develop and implement a
1201 baseline configuration for vulnerability management.

1202 *7.2.1.10 PR.MA-2: Remote Maintenance of Organizational Assets is Approved, Logged,*
1203 *and Performed in a Manner that Prevents Unauthorized Access*

1204 We controlled remote access to pump vendors by implementing ConsoleWorks, a software tool that
1205 records all the actions performed over a connection; thereby providing an audit trail that documents
1206 vendor activity.

1207 *7.2.1.11 PR.PT-1: Audit/Log Records are Determined, Documented, Implemented, and*
1208 *Reviewed in Accordance with Policy*

1209 Our example implementation supports this CSF subcategory by enabling logging on all devices in two
1210 ways: with a logging capability and with a process of identifying which events the log will record.
1211 Although our project employs auditing and recognizes its importance in a cybersecurity program, log
1212 aggregation and implementing a log review process, albeit vital activities, are beyond this project's
1213 scope.

1214 *7.2.1.12 DE.AE-1: A Baseline of Network Operations and Expected Data Flows for Users*
1215 *and Systems is Established and Managed*

1216 As we did with systems and medical devices, we took a least functionality approach when configuring
1217 the network. We followed best practices for configuring firewalls based on a default deny, restricted
1218 SSID broadcast, and limiting the power of wireless signals.

1219 This CSF subcategory is supported by the Symantec Intrusion Detection System (IDS) component of the
1220 reference design. This tool identifies, monitors, and reports anomalous network traffic that may
1221 indicate a potential intrusion. Endpoint protection implements policies for expected behavior and alerts
1222 when activities occur outside the usual patterns.

1223 **7.3 Security Analysis Summary**

1224 Our reference design's implementation of security surrounding wireless infusion pumps helps reduce
1225 risk from a pump, even if a vulnerability is identified in a pump, by creating a more secure environment
1226 for medical devices. The key feature is network segmentation. Supporting this zone approach, our
1227 project build follows security best practices to harden devices, monitor traffic, and limit access via the
1228 wireless network to only authorized users. Any organization following this guide must conduct its own
1229 analysis of how to employ the elements we've discussed here in their environment. It is essential that

1230 organizations follow security best practices to address potential vulnerabilities and minimize any risk to
1231 the operational network.

1232 8 Functional Evaluation

1233 We conducted a functional evaluation of our example implementation to verify that several common
1234 provisioning functions used in our laboratory test worked as expected. We also needed to ensure that
1235 the example solution would not alter normal pump and pump server functions. The test plan in
1236 Section 8.1 outlines our test cases, the purposes, and desired outcomes.

1237 The subsequent sections explain the functional tests in more details and list the procedures for each of
1238 the functional tests.

1239 8.1 Functional Test Plan

Test Case	Purpose	Desired Outcomes
WIP-1: Network Segmentation	Test the effectiveness of network segmentation	All firewall rules for each segment are implemented correctly, as designed.
WIP-2: Data Center Security	Test the effectiveness of Data Center Security (DCS:SA) to see that it follows defined policies	The inbound and outbound network traffic to and from servers is controlled per host firewall rules.
WIP-3: Endpoint Protection	Test the effectiveness of the Symantec (SEP) to ensure that it follows defined policies	A bad file is detected and the planned installation action is blocked.
WIP-4: Advanced Threat Protection	Test the effectiveness of Advanced Threat Protection: Network (ATP:N) to ensure it follows defined policies	The URLs in the blacklist are blocked. Also, the URLs in the whitelist are allowed.
WIP-5: Protected Remote Access	Test the effectiveness of the remote access controls	The vendor can only access to what's been granted for access with the correct privileges.
WIP-6: Pump and Pump server network connection	Confirm the installation and configuration of pumps and pump server are fully completed	Pumps and pump servers are connected to the network and pumps communicate to the corresponding pump servers.

Test Case	Purpose	Desired Outcomes
WIP-7: Pump and Pump server basic functions	Test a set of operational events between pumps and pump servers	Pumps are connected to the corresponding pump server, able to perform a set of operational events.

1240 **8.1.1 Test Case: WIP-1**

Test Case Name	Network Segmentation
Description	<ul style="list-style-type: none"> Show that the WIP solution allows the inbound and outbound traffic of a given zone as per design Show the WIP solution blocks the inbound and outbound traffic of a given zone as per design
Preconditions	<ul style="list-style-type: none"> WIP network segmentation is implemented Internal firewall rules of each zone are defined and implemented The ASAs are configured to use stateful filtering, so return traffic is automatically allowed if the initial connection is allowed. Everything not explicitly allowed in a rule is denied
Procedure	<ol style="list-style-type: none"> Use Medical Device and Biomedical Segment zones as a test example. Review the port and communication protocol requirements from each tested pump vendor, for pump and corresponding pump server Configure the ASA firewall access list to open only the needed ports and allow access only to necessary protocols Everything not explicitly allowed in a rule is denied.
Result	<ol style="list-style-type: none"> Review the ASA configuration file to verify that the ASA firewall is configured to only allow communication with a specific protocol and port as specified by the pump vendors. All other communication between these two segments will be denied and blocked using a command such as: “show access-list include eq” to see the opened ports Use network discovery scanning tools such as nmap to check the open, closed, or filtered ports

1241 **8.1.2 Test Case: WIP-2**

Test Case Name	Data Center Security
Description	<ul style="list-style-type: none"> Show that the WIP solution detects files that are defined in policy and apply the file and system tampering prevention methods by locking down files
Preconditions	<ul style="list-style-type: none"> DCS:SA is installed and configured File and System Tamper Prevention policy is set

Test Case Name	Data Center Security
	<ul style="list-style-type: none"> Windows_Baseline_detect_TEST is used as the baseline for server hardening
Procedure	<p>There are two admin applications for the DCS, the console admin and the portal admin. The console admin is the thick client and the portal is the thin client. The console is used to create and modify the policy, and the portal is used to publish the policy. Portal URL is https://192.168.120.167:8443/webportal/#/</p> <ul style="list-style-type: none"> Log in to the DCS Console Select the Policy->Work Space->Pump Server folder Select Detection tab to show the detection polices You should see a preinstalled policy-Windows_Baseline_detect_Test, double click it to open a detailed policy editing window for configuration Create a policy for hardening the server, such as “do not allow any file to be installed on the server” Enable the policy Publish the policy
Result	Test to verify that no file is allowed to be installed on the protected server

1242 **8.1.3 Test Case: WIP-3**

Test Case Name	Endpoint Protection/Advance Threat Protection
Description	<ul style="list-style-type: none"> Show that the WIP solution has the capability to detect a bad file and act (i.e., stop installing that bad file)
Preconditions	<ul style="list-style-type: none"> Symantec Endpoint Protection (SEP) is installed and configured Define the antivirus signature rule Create a ‘bad’ file that is part of the antivirus signature rule
Procedure	<ol style="list-style-type: none"> Make sure the test server has a Symantec End Protection agent installed and enabled. From the server machine, open an IE browser and type: http://test.symantecatp.com. This is a test site provided by Symantec containing some unharful links for testing purposes Click some links such as ‘antivirus test’ from the list to install some suspicious software on the test server The installation should be blocked by the server’s SEP and the violation incident should be reported in the ATP To view the violation in ATP: login to the ATP Server from a browser in a server that can access the 192.168.120.x network, such as the Active Directory server (192.168.120.162) Type this URL in the browser: https://192.168.120.168

Test Case Name	Endpoint Protection/Advance Threat Protection
	<ol style="list-style-type: none"> View any violation incidents from the ATP to verify that the bad link is blocked. <ul style="list-style-type: none"> If wanted, one can dive into the details to see which bad sites it tried to connect. Then for an open incident, need to close it.
Result	<p>To verify that the ATP:N and Symantec deployment and configuration offers needed security protection to prevent malware installed in a server.</p> <p>To view the violation, in ATP: login to the ATP Server from a browser in a server that can access the network, where the tested server is located.</p> <ol style="list-style-type: none"> View any violation incidents from the ATP to verify that the bad link is blocked. Check the details to see which bad sites it tried to connect. Close open incidents

1243 **8.1.4 Test Case: WIP-4**

Test Case Name	Advanced Threat Protection
Description	<ul style="list-style-type: none"> Show that the WIP solution has effective network threat protection based on network intrusion prevention, URL, and firewall policies.
Preconditions	<ul style="list-style-type: none"> Advanced Threat Protection: Network (ATP:N) is installed and configured Firewall and browser protection rules are defined
Procedure	<ol style="list-style-type: none"> Logon to a vm server with APT:N installed Access to a malicious website Check the results
Result	See Test Case WIP-3

1244 **8.1.5 Test Case: WIP-5**

Test Case Name	Protected Remote Access
Description	<ul style="list-style-type: none"> Show that the WIP solution has the protected remote access capability. The VendorNet concept was created out of a need to give vendors more restricted remote access to a lab than NIST/NCCoE/MITRE staff. VendorNet is an NCCoE network created for each lab that is tied to an active directory group. This group of people is then allowed to access the lab through VendorNet. VendorNet hosts controlled access mechanisms such as ConsoleWorks, file transfer servers, or other remote access proxy services.
Preconditions	<ul style="list-style-type: none"> VendorNet is created TDi ConsoleWorks is installed and configured

Test Case Name	Protected Remote Access
	<ul style="list-style-type: none"> • ConsoleWorks profile and user are created
Procedure	<ol style="list-style-type: none"> 1. Using public Internet, remotely logon to the NCCoE VPN 2. Logon to ConsoleWorks using the IP address: https://consoleworks.nccoe.nist.gov 3. From the graphical menu, select the View to view graphical connections 4. Each external vendor can only view the resources assigned to them 5. Access the granted hosts 6. Perform the allowed operations as specified 7. Check the results
Result	<ol style="list-style-type: none"> 1. Verify that the vendor can access associated pump server using VendorNet and ConsoleWorks 2. Verify that they can perform the preassigned operational activities 3. Verify that they cannot perform unauthorized operations, such as some administration task, such as adding a new user account 4. Verify that all activities performed by the external vendor are logged and can be audited as needed

1245 **8.1.6 Test Case: WIP-6**

Test Case Name	Pump and Pump Server Network Connection
Description	<ul style="list-style-type: none"> • Show that the WIP solution establish the wireless network connection between each vendor's pumps and their corresponding pump server
Preconditions	<ul style="list-style-type: none"> • Wireless router with pre-share password SSID has been set up • Infusion pump servers have been installed and configured • Infusion pumps have been installed and configured using WPA2-PSK or WPA2-ENT/EAP-TLS for secure wireless network connection • Cisco ISE is installed and configured with root CA installed
Procedure	<ol style="list-style-type: none"> 1. Turn on the pump 2. Check the wireless indicator 3. Check the Access Point and ISE administration portals for device connection and authentication status 4. Check the Infusion Pump server management tool for discovered pumps
Result	<p>Both the access point portal should indicate that the pumps are successfully connected to the network</p> <p>The pump server admin portal should indicate the pump is online and in use. (Note: the way the pump server portal displays these messages is vendor dependent.)</p>

Test Case Name	Pump and Pump Server Network Connection
	In the case of WPA2-Ent/EAP TLS wireless access mode, the Cisco ISE should display that the pumps are successfully authenticated

1246 8.1.7 Test Case: WIP-7

Test Case Name	Pump and Pump Server Basic Functions
Description	<ul style="list-style-type: none"> • Show that the WIP solution supports the basic operational events for each vendor's pumps and their corresponding pump server
Preconditions	<ul style="list-style-type: none"> • Successful test results of WIP-6 • The drug library for a specific pump has been created by a pharmacist and validation has been performed. • The drug library has been successfully published or loaded to the infusion pump server to be tested
Procedure	<ol style="list-style-type: none"> 1. From the pump server, send the new version of drug library to its pumps. Following is an example procedure used by Hospira to send Drug Library to its pump using the MedNet Software Server: <ul style="list-style-type: none"> • Log in to a Metnet software server • Request the download of the drug library to one or more pump • MedNet displays the drug library download status as "Pending" • MedNet using MedNet Service forwards the drug library to infusion pump selected • Pump infuser downloads the drug library from the MedNet Server • Pump Infuser sends a download status update to Hospira MedNet server to indicate the drug library is successfully downloaded and wait for installation • The pump server displays a download status as "On Pump" • The operator of the pump powers down the pump and choose to install the new drug library when prompted by the infuser • The pump sends the update status to MedNet to indicate that the drug library was successfully installed and a "Completed" status is displayed. 2. From the pump server, send the new version of software updates to its pumps (Using Smiths Medical pump as an example). Using the PharmGuard pump server, packages containing data such as device configuration data or firmware, specific to an installed Smiths Medical device model can be installed. The package tested is provided by Smiths Medical. <ul style="list-style-type: none"> • Log in to a PharmGuard server

Test Case Name	Pump and Pump Server Basic Functions
	<ul style="list-style-type: none"> • Select Package Deployment from the Asset Management drop-down menu, all previously-deployed packages, if any, are listed • Click Add Package • Click Browse to navigate to and select the package file • Click Upload to upload the package. After package file is read, information about the package is displayed in the package table • Select the package you like to deploy and click View/Deploy, the package detailed information is displayed • Click Deploy to deploy the new package • Enter the name for the deployment and specify a start deploy • Enter the required password and click Continue • After you confirm the package deployment, the name of the newly-deployed package displays in the Deployment list with the Status of Active • To check if a package has been received by the individual pump associated with the package deployment, you need to check the device itself
Result	Using the device or the corresponding pump server portal to verify that the intended package has been successfully deployed. How this information is displayed is device- and manufacturer-specific. Please consult documentation for specific devices for more information.

1247 9 Future Build Considerations

1248 During our development of this project and practice guide, we did not implement several components;
 1249 however, they should be considered. We did not implement a commercially available electronic health
 1250 record (EHR) system. EHRs are often regarded as central within a hospital.

1251 Other solutions that were not implemented in the lab were a central asset inventory management tool,
 1252 or mechanisms to perform malware detection or network monitoring in the Medical Device zone. An
 1253 update to this practice guide could evaluate these components and other control mechanisms that may
 1254 become available in the future.

Appendix A Threats

Below are some potential known threats in the healthcare environments that use network-connected medical devices, such as wireless infusion pumps.

- **Targeted attacks:** threats involving actors that attempt to compromise the pump and system components directly affecting pump operations, including the pump, the pump server, drug library, or drug library management systems. Actors who perform such targeted attacks may be external, in other words those who attempt to access the pump system through the public Internet, or via vendor support networks or VPNs. There may also be internal actors, such as those on staff who may be involved in accidental misconfiguration or who possess provisioned access and abuse their granted privileges, or patients or other visitors who attempt to modify the behavior of a pump.
- **Advanced Persistent Threats:** APTs occur when the threat actor attempts to place malicious software on the pump or pump system components, which may enable that threat actor to perform unauthorized actions, either on the pump system itself, or as a pivot point to cause adverse conditions for hospital internal systems that may have reachability from the pump network environment. Placement of malicious software may or may not cause adverse scenarios on the pump or its system components.
- **Disruption of Service – Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks:** DoS or DDoS attacks may be components found in a broader APT scenario. Such attacks are intended to cause the unavailability of the pump or pump system components, thus rendering providers with degraded capability to fulfill patient care.
- **Malware infections:** In this type of attack, a threat actor places malicious software on the pump, likely as part of an APT campaign, or to cause an adverse situation on the pump or pump systems. One example of a malware infection is that of ransomware, in which malicious software would cause a disruption of the availability of the pump for standard operations, and may affect patient safety by preventing providers from leveraging system functionality (e.g., the ability to associate the pump with a patient and deliver medications), or by preventing the pump from effectively using safety measures such as the drug library.
- **Theft or loss of assets:** This threat type applies when the pump or pump system components are not accounted for in an inventory, thereby leading to degraded availability of equipment, and a possible breach of PHI.
- **Unintentional misuse:** This threat considers the possibility that the pump or its components may be unintentionally misconfigured or used for unintended purposes, including errors introduced through the misapplication of updates to operating systems or firmware, misconfiguration of settings that allow the pump to achieve network connectivity or communication to the pump server, misapplication or errors found in the drug library, or errors associated with fluids applied to pumps.

- **Vulnerable systems or devices directly connected to the device (e.g., via USB, or other hardwired non-network connections):** Extending from the unintentional misuse of the device, this threat considers scenarios in which individuals may expose devices or server components using external ports or interfaces for purposes outside the device's intended use, for example, to extract data to portable storage media, or to connect a mobile device to recharge that device's battery. In leveraging ports for unintended purposes, threat actors may enable malicious software to migrate to the pump or server components, or to create adverse conditions based on unexpected connections.

Appendix B Vulnerabilities

Here's a list of typical vulnerabilities that may arise when using wireless infusion pumps:

- **Lack of asset inventory:** Deficient or out-of-date inventories represent a cybersecurity control deficiency that may lead to the loss/theft of devices or equipment, with little chance for the hospital to recover or take recourse against losses. Deficient asset inventory controls, when paired with a credible threat, such as the loss or theft of a device or equipment, raises risks associated with a provider's ability to render patient care, and may expose PHI to unauthorized individuals.
- **Long useful life:** Infusion pumps are designed to perform clinical functions for several years, and they tend to have long-term refresh rates. One vulnerability associated with infrequent refresh is that each device's technological attributes may become obsolete or insufficient to support patching, updating, or the support of cyber security controls that may become available in the future.
- Information/Data Vulnerabilities
 - **Lack of encryption on private/sensitive data at rest:** Pump devices may have local persistent storage, but they may not have a means to encrypt data stored on the device. Locally stored data may include sensitive configuration information, or patient information, including possible PHI.
 - **Lack of encryption on transmitted data:** Sensitive data should be safeguarded in transit as well as at rest. Where capabilities exist, pumps and server components should employ encryption on the network or when transmitting sensitive information. An inability to safeguard data in transit using appropriate encryption capabilities may expose sensitive information or allow malicious actors to determine how to connect to a pump or server to perform unauthorized activities.
 - **Unauthorized changes to device calibration or configuration data:** Modifications made to pump or server components that are not accurately approved, deployed, or tracked may lead to adverse operation of the equipment. Hospitals should ensure that changes to device calibration, configuration, or modification of safeguard measures such as the drug library are performed and managed using appropriate measures.
 - **Insufficient data backup:** Providing backup and recovery capability is a common cybersecurity control to ensure HDOs can restore services in a timely fashion after an adverse event. Hospitals should perform appropriate pump system backup and restore functions.
 - **Lack of capability to de-identify private/sensitive data:** As a secondary cybersecurity control to data encryption, hospitals may wish to consider the ability to de-identify or obfuscate sensitive information or PHI.

- **Lack of data validation:** Data used and captured by infusion pumps and associated server components may require data integrity assurance to support proper functioning and patient safety. Mechanisms should be used to provide assurance that data cannot be altered inappropriately.
- **Device/Endpoint (Infusion Pump) Vulnerabilities**
 - **Debug-enabled interfaces:** Interfaces required to support or troubleshoot infusion pump functions should be identified, with procedures noted to indicate when interfaces are available, and how interfaces may be disabled when not required for troubleshooting or system updates/fixes.
 - **Use of removable media:** Infusion pumps that include external or removable storage should be identified. Cybersecurity precautions are necessary because the use of removable media may lead to inappropriate information disclosure, and may provide a viable avenue for malicious software to migrate to the pump or server components.
 - **Lack of physical tamper detection and response:** Infusion pumps may involve physical interaction, including access to interfaces used for debugging. HDOs should enable mechanisms to prevent physical tampering with infusion pump devices, including alerting appropriate personnel whenever a pump or its server components are manipulated or altered.
 - **Misconfiguration:** Mechanisms should be used to ensure that pump configurations are well managed and may not be configured to produce adverse conditions.
 - **Poorly protected and patched devices:** Like the misconfiguration vulnerability, HDOs should implement processes to protect/patch/update pumps and server components. This may involve including controls on the device, or provisions that allow for external controls that would prevent exposure to flaws or weaknesses.
- **User or Administrator Accounts Vulnerabilities**
 - **Hard-coded or factory default passcodes:** Processes or mechanisms should be added to prevent the use of so-called hard coded or default passcodes. This would overcome a common IT systems deficiency in the use of authentication mechanisms for privileged access to devices in terms of using weak passwords or passcodes protection. Weak authentication mechanisms that are well known or published degrade the effectiveness of authentication control measures. HDOs should implement a means to update and manage passwords.
 - **Lack of role-based access and/or use of principles of least privilege:** When access management roles and principles of least privilege are poorly designed, they may allow the use of a generic identity (e.g., a so-called admin account) that enables greater access capability than necessary. Instead, HDOs should implement processes to limit access to privileged accounts, infusion pumps and server components, and use accounts or identities

that tie to specific functions, rather than providing/enabling the use of super user, root, or admin privileges.

- **Dormant accounts:** Accounts or identities that are not used may be described as *dormant*. Dormant account information should be disabled or removed from pumps and server components.
- **Weak remote access controls:** When remote access to a pump and or server components is required, access controls should be appropriately enforced to safeguard each network session and ensure appropriate authentication and authorization.
- IT Network Infrastructure Vulnerabilities
 - **Lack of malware protection:** Pumps and server components should be protected using processes or mechanisms to prevent malware distribution. When malware *protection* cannot be implemented on end-point devices, malware *detection* should be implemented to protect network traffic.
 - **Lack of system hardening:** Pumps and server components should incorporate protective measures that limit functionality only to the specific capabilities necessary for infusion pump operations.
 - **Insecure network configuration:** HDOs should employ a least privilege principle when configuring networks that include pumps and server components, limiting network traffic capabilities, and enforcing limited trust between zones identified in hospital environments.
 - **System complexity:** When implementing network infrastructure controls, hospitals should seek device models and communications paths/patterns that limit complexity where possible.

Appendix C Recommendations and Best Practices

Associated best practices for reducing the overall risk posture of infusion pumps are also included in the following list:

- Consider forming a Medical Device Security Committee composed of staff members from biomedical services, IT, and InfoSec that would report to C-suite governance.
 - Enable this committee to manage the security of all network-connected medical devices. Too often, for example, the biomedical services team is solely responsible for cradle-to-grave maintenance of all aspects of medical devices, including cybersecurity, leaving IT and InfoSec staff out-of-the-loop.
 - Develop a committee charter with roles and responsibilities and reporting requirements to the C-suite and Board of Directors.
- Consider the physical security of mobile medical devices including wireless infusion pumps.
 - Designate a secure and lockable space for storing these devices when they are not in use.
 - Ensure that only personnel with a valid need have access to these spaces. Ideally, a proximity system with logging should be used and audited frequently.
- Create a comprehensive inventory of medical devices and actively manage it.
 - Consider the use of Radio-frequency identification (RFID) or Real-time locating systems (RTLS) technologies to assist with inventory processes and help staff locate devices that have been moved without documentation.
- Ensure that any Cybersecurity Incident Response Plan includes medical devices.
 - Recently, the FDA and Industrial Control System – Computer Emergency Response Team (ICS-CERT) have both issued cybersecurity vulnerability advisories for medical devices. This was the first major warning to covered entities regarding medical device vulnerabilities. Most covered entities have not incorporated medical device response into their planning.
- Ensure that pumps cannot step down to a Wireless Encryption Protocol (WEP) encrypted network.
 - WEP is a compromised encryption protocol and should NEVER be used in operational wireless networks.
 - Operating any form of IT equipment including medical devices over a WEP network will result in the potential for data compromise and a regulatory breach.
 - Any wireless network should be using, at a minimum, Wi-Fi Protected Access 2 (WPA2). This protocol implements NIST-recommended Advanced Encryption Standard (AES).
- Put in place an Information Security department and functionally separate it from the IT department. This is necessary to ensure operational IT personnel are not responsible for any

information security measures, which may otherwise lead to a fox-guarding-the-hen-house situation.

- Enable a separate InfoSec department to report to the Chief Information Security Officer (CISO) rather than to the Chief Information Officer (CIO.)
- Make this organization part of the Medical Device Security Committee.
- Create an operational information security program. This can take the form of an in-house Security Operations Center (SOC) to monitor information systems and initiate cybersecurity incident response, to include monitoring of potential exploits of medical devices, as necessary. Alternatively, organizations may wish to consider a Managed Security Service Provider (MSSP) to perform these duties.
- Ensure that vendor management includes the evaluation of information security during the due diligence phase of any related procurement processes. Too often, the Information Security team is not brought in until after contracts have been signed.
 - When purchasing medical devices, ensure that devices incorporate the latest cybersecurity controls and capabilities.
 - Understand roles and responsibilities related to upgrades, patching, password management, remote access, etc., to ensure the cybersecurity of products or services.
- Consider media access control (MAC) address filtering to limit exposure of unauthorized devices attempting to access the network. This would identify a bad actor attempting access a medical device from within the network through an exposed wired Ethernet port.
- Develop or update policies and procedures to ensure a holistic approach to deployment, sanitization, and reuse of medical devices; include the Medical Device Security Committee.

Appendix D References

- [1] FDA, Infusion Pumps Total Product Life Cycle - Guidance for Industry and FDA Staff, Document issued on: December 2, 2014. Accessed 6 April 2017: <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf>
- [2] FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, Document Issued on: October 2, 2014. Accessed 6 April 2017: <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf>
- [3] FDA, Postmarket Management of Cybersecurity in Medical Devices - Guidance for Industry and Food and Drug Administration Staff, Document Issued on: December 28, 2016. Accessed 6 April 2017: <https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf>
- [4] Department of Homeland Security (DHS), Attack Surface: Healthcare and Public Health Sector. Accessed 6 April 2017: <https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf>
- [5] Integrating the Healthcare Enterprise (IHE) Patient Care Device (PCD), Technical Framework White Paper. Accessed 6 April 2017: http://www.ihe.net/Technical_Framework/upload/IHE_PCD_Medical-Equipment-Management_MEM_White-Paper_V1-0_2009-09-01.pdf
- [6] IHE PCD, White Paper, Medical Equipment Management (MEM): Cyber Security. Accessed 6 April 2017: http://www.ihe.net/Technical_Framework/upload/IHE_PCD_White-Paper_MEM_Cyber_Security_Rev2-0_2011-05-27.pdf
- [7] FDA, Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. Accessed 6 April 2017: <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf>
- [8] IHE PCD, White Paper, MEM: Medical Device Cyber Security – Best Practice Guide. Accessed 6 April 2017: http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf
- [9] AAMI TIR57, Principles for medical device security – risk management
- [10] NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure. Accessed 6 April 2017: <http://www.nist.gov/itl/cyberframework.cfm>
- [11] NIST SP 800-30, Guide for Conducting Risk Assessments. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- [12] NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Accessed 6 April 2017: <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>
- [13] NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>
- [14] NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organization. Accessed 10 April 2017: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

- [15] IEC Technical Report (TR) 80001-2-1, Edition 1.0 2012-07, Technical Report, Application of risk management for IT-networks incorporating medical devices – Part 2-1: Step-by-step risk management of medical IT-networks – Practical applications and examples
- [16] IEC TR 80001-2-2, Edition 1.0 2012-07, Technical Report, Application of risk management for IT Networks incorporating medical devices – Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
- [17] IEC TR 80001-2-3, Edition 1.0 2012-07, Technical Report, Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks
- [18] IEC TR 80001-2-4, Edition 1.0 2012-11, Technical Report, Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations
- [19] IEC TR 80001-2-5, Edition 1.0 2014-12, Technical Report, Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems
- [20] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Accessed 6 April 2017: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890098
- [21] Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Accessed 6 April 2017: <http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php>
- [22] Department of Health and Human Services (HHS) HIPAA Administrative Simplification Statute and Rules. Accessed 6 April 2017: <http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html>
- [23] American National Standards Institute (ANSI)/Association for the Advancement of Medical Instrumentation (AAMI)/International Electrotechnical Commission (IEC) 80001-1:2010, Application of risk management for IT Networks incorporating medical devices – Part 1: Roles, responsibilities and activities
- [24] ISO 14971, 2007 Medical devices – Application of risk management to medical devices
- [25] IHE PCD Medical Equipment Management: Medical Device Cybersecurity – Best Practice Guide
- [26] NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- [27] NIST SP 800-88, Guidelines for Media Sanitization. Accessed 6 April 2017: <https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization>
- [28] NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>
- [29] NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf>

- [30] NIST SP 800-57 Part 1 – Rev 3, Recommendation for Key Management: Part 1: General (Revision 3). Accessed 6 April 2017: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
- [31] NIST SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf>
- [32] NIST SP 800-57 Part 3 Rev 1, Recommendation for Key Management: Part 3: Application-Specific Key Management Guidance. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf>
- [33] NIST SP 800-48 Rev 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks. Accessed 6 April 2017: <http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>
- [34] NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf>
- [35] IEEE 802.1x, Port Based Network Access Control. Accessed 6 April 2017: <http://www.ieee802.org/1/pages/802.1x.html>
- [36] IEEE 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Accessed 6 April 2017: <http://www.ieee802.org/11/>
- [37] NIST Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules. Accessed 6 April 2017: <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- [38] NIST SP 800-52 Rev 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf>
- [39] DHHS Office for Civil Rights, HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Accessed 6 April 2017: <https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf>
- [40] IHE PCD User Handbook – 2011 Edition – Published 2011-08-12. Accessed 6 April 2017: http://www.ihe.net/Technical_Framework/upload/IHE_PCD_User_Handbook_2011_Edition.pdf
- [41] *Cisco Medical-Grade Network (MGN) 2.0-Wireless Architectures* (Higgins & Mah, 2012): http://www.cisco.com/c/dam/en_us/solutions/industries/docs/healthcare/mgn_wireless_arch.pdf
- [42] FDA, Radio Frequency Wireless Technology in Medical Devices – Guidance for Industry and Food and Drug Administration Staff, Document issued on August 12, 2013. Accessed 6 April 2017: <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf>
- [43] NIST SP 800-114, User’s Guide to Securing External Devices for Telework and Remote Access. Accessed 6 April 2017: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf>
- [44] NIST SP 800-77, Guide to IPsec VPNs. Accessed 6 April 2017: <http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf>

- [45] NIST SP 800-41 Rev 1, Guidelines on Firewalls and Firewall Policy. Accessed 6 April 2017: <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf>
- [46] IEEE 802.1x, Port Based Network Access Control. Accessed 6 April 2017: <http://www.ieee802.org/1/pages/802.1x.html>
- [47] IEEE 802.3, IEEE Standard for Ethernet. Accessed 6 April 2017: <http://www.ieee802.org/3/>
- [48] IEEE 802.1Q, Bridges and Bridged Networks. Accessed 6 April 2017: <http://www.ieee802.org/1/pages/802.1Q.html>
- [49] Internet Engineering Task Force (IETF) Request for Comments (RFC) 4301, Security Architecture for the Internet Protocol. Accessed 6 April 2017: <https://tools.ietf.org/html/rfc4301>
- [50] NIST FIPS 197, Advanced Encryption Standard (AES). Accessed 6 April 2017: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [51] NIST SP 800-46 Rev 1, Guide to Enterprise Telework and Remote Access Security. Accessed 6 April 2017: <http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf>
- [52] NIST SP 800-41 Rev 1, Guidelines on Firewalls and Firewall Policy. Accessed 6 April 2017: <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf>
- [53] NIST SP 800-95, Guide to Secure Web Services. Accessed 6 April 2017: <http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf>
- [54] NIST SP 1800-5A, IT Asset Management. Accessed 10 April 2017: <https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5-draft.pdf>
- [55] <http://wc1.smartdraw.com/cmsstorage/exampleimages/44b341d1-a502-465f-854a-4e68b8e4bf75.png>
- [56] Manufacturer Disclosure Statement for Medical Device Security (MDS2) <http://www.himss.org/resourcelibrary/MDS2>

NIST SPECIAL PUBLICATION 1800-8C

Securing Wireless Infusion Pumps

In Healthcare Delivery Organizations

Volume C:
How-to Guides

DRAFT

Gavin O'Brien

National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards

Kevin Littlefield

Neil McNab

Sue Wang

Kangmin Zheng

The MITRE Corporation
McLean, VA

May 2017

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



DRAFT

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-8C Natl. Inst. Stand. Technol. Spec. Publ. 1800-8C, 256 pages, (May 2017), CODEN: NSPUE2

FEEDBACK

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

The NCCoE at NIST analyzed risk factors in and around the infusion pump ecosystem using a questionnaire-based risk assessment to develop an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.

This practice guide will help HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk, while maintaining the performance and usability of wireless infusion pumps.

KEYWORDS

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

ACKNOWLEDGMENTS

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

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)

Name	Organization
Joseph Sener	Hospira Inc., a Pfizer Company (ICU Medical)
Chris Edwards	Intercede
Won Jun	Intercede
Dale Nordenberg	MDISS
Jay Stevens	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 vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Baxter Healthcare Corporation	<ul style="list-style-type: none"> • Sigma Spectrum LVP, version 8 • Sigma Spectrum Wireless Battery Module, version 8 • Sigma Spectrum Master Drug Library, version 8 • CareEverywhere Gateway Server, version 14
B. Braun Medical Inc.	<ul style="list-style-type: none"> • Infusomat® Space Infusion System/ Large Volume Pumps • DoseTrac® Infusion Management Software/ Infusion Pump Software
Becton, Dickinson and Company (BD)	<ul style="list-style-type: none"> • Alaris® 8015 PC Unit v9.19.2 • Alaris® Syringe Module 8110 • Alaris® LVP Module 8100 • Alaris® Systems Manager v4.2 • Alaris® System Maintenance (ASM) v 10.19
Cisco	<ul style="list-style-type: none"> • Access Point (AIR-CAP1602I-A-K9) • Wireless LAN Controller 8.2.111.0 • Cisco ISE • Cisco: ASA • Catalyst 3650 Switch
Clearwater Compliance	Clearwater: IRM Pro
DigiCert	CertCentral management account / Certificate Authority
Hospira Inc., a Pfizer Company (ICU Medical)	<ul style="list-style-type: none"> • Plum 360™ Infusion System, version 15.10 • LifeCare PCA™ Infusion System, version 7.02 • Hospira MedNet™, version 6.2
Intercede	MyID
MDISS	MDRAP

Technology Partner/Collaborator	Build Involvement
PFP Cybersecurity	Device Monitor
Ramparts	Risk Assessment
Smiths Medical	<ul style="list-style-type: none"> • Medfusion® 3500 V5 syringe infusion system • PharmGuard® Toolbox v1.5 • Medfusion 4000® Wireless Syringe Infusion Pump • CD, PHARMGUARD® TOOLBOX 2, V3.0 use with Medfusion® 4000 and 3500 V6 (US) • PharmGuard® Server Licenses, PharmGuard® Server Enterprise Edition, V1.1 • CADD®-Solis Ambulatory Infusion Pump • CADD™-Solis Medication Safety Software
Symantec Corporation	<ul style="list-style-type: none"> • Endpoint Protection (SEP) • Advanced Threat Protection: Network (ATP:N) • Server Advanced - DataCenter Security (DCS:SA):
TDi Technologies, Inc.	ConsoleWorks

Contents

1	Introduction	1
1.1	Practice Guide Structure.....	1
1.2	Typographical Conventions	2
1.3	How-to Overview	2
1.4	Logical Architecture Summary.....	2
2	Product Installation Guides.....	3
2.1	The Core Network	3
2.1.1	Cisco ASA Baseline Configuration.....	4
2.1.2	External Firewall and Guest Network	4
2.1.3	Enterprise Services	5
2.1.4	Biomedical Engineering Network	5
2.1.5	Medical Devices.....	5
2.1.6	Cisco Catalyst Switch Configuration	6
2.1.7	Cisco Enterprise Wi-Fi Infrastructure.....	6
2.1.8	TDi ConsoleWorks External Remote Access.....	12
2.2	Infusion Pump and Pump Server	21
2.2.1	Infusion Pumps.....	21
2.2.2	Infusion Pumps Server Systems	25
2.3	Identity Services.....	26
2.3.1	Cisco Identity Service Engine (ISE).....	26
2.3.2	DigiCert Certificate Authority.....	31
2.4	Symantec Endpoint Protection and Intrusion Detection	36
2.4.1	Symantec Data Center Security: Server Advanced.....	37
2.4.2	Symantec Endpoint Protection Manager.....	40
2.4.3	Symantec Advanced Threat Protection: Advanced Threat Protection: Network.....	41
2.5	Risk Assessment Tools.....	43
2.5.1	Clearwater IRM Analysis™ Software.....	43
2.5.2	MDISS MDRAP	52

DRAFT

Appendix A	Baseline Configuration File	61
Appendix B	Sample Pump Configuration Parameters	239
Appendix C	References	246

List of Figures

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

Figure 2-27: Assessment Result (dashboard example)..... 60
Figure 2-28: Assessment Result (report example)..... 60

List of Tables

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

1 Introduction

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

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

8 1.1 Practice Guide Structure

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

12 This guide contains three volumes:

- 13 ▪ NIST SP 1800-8A: Executive Summary
- 14 ▪ NIST SP 1800-8B: Approach, Architecture, and Security Characteristics – what we built and why
- 15 ▪ NIST SP 1800-8C: How-To Guides – instructions for building the example solution (**you are here**)

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

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

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

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

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

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

31 **IT professionals** who want to implement an approach like this will find the entire practice guide useful.
32 You can use the How-To portion of the guide, *NIST SP 1800-8C*, to replicate all or parts of the build
33 created in our lab. The How-To guide provides specific product installation, configuration, and
34 integration instructions for implementing the example solution. We do not recreate the product
35 manufacturers' documentation, which is generally widely available. Rather, we show how we
36 incorporated the products in our environment to create an example solution.

37 This guide assumes that IT professionals have experience implementing security products within their
 38 enterprise. Although we have used a suite of commercial products to address this challenge, this guide
 39 does not endorse these products. Your organization can adopt this solution or one that adheres to these
 40 guidelines in part or in whole. Your organization’s security experts should identify the products that will
 41 best integrate with your existing tools and IT system infrastructure. We hope you will seek products that
 42 are congruent with applicable standards and best practices. Vol B. section 4.4, Technologies, lists the
 43 products we used and maps them to the cybersecurity controls provided by this reference solution.

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

48 1.2 Typographical Conventions

49 The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
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	<code>mkdir</code>
Monospace Bold	command-line user input contrasted with computer output	<code>service sshd start</code>
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 .

50 1.3 How-to Overview

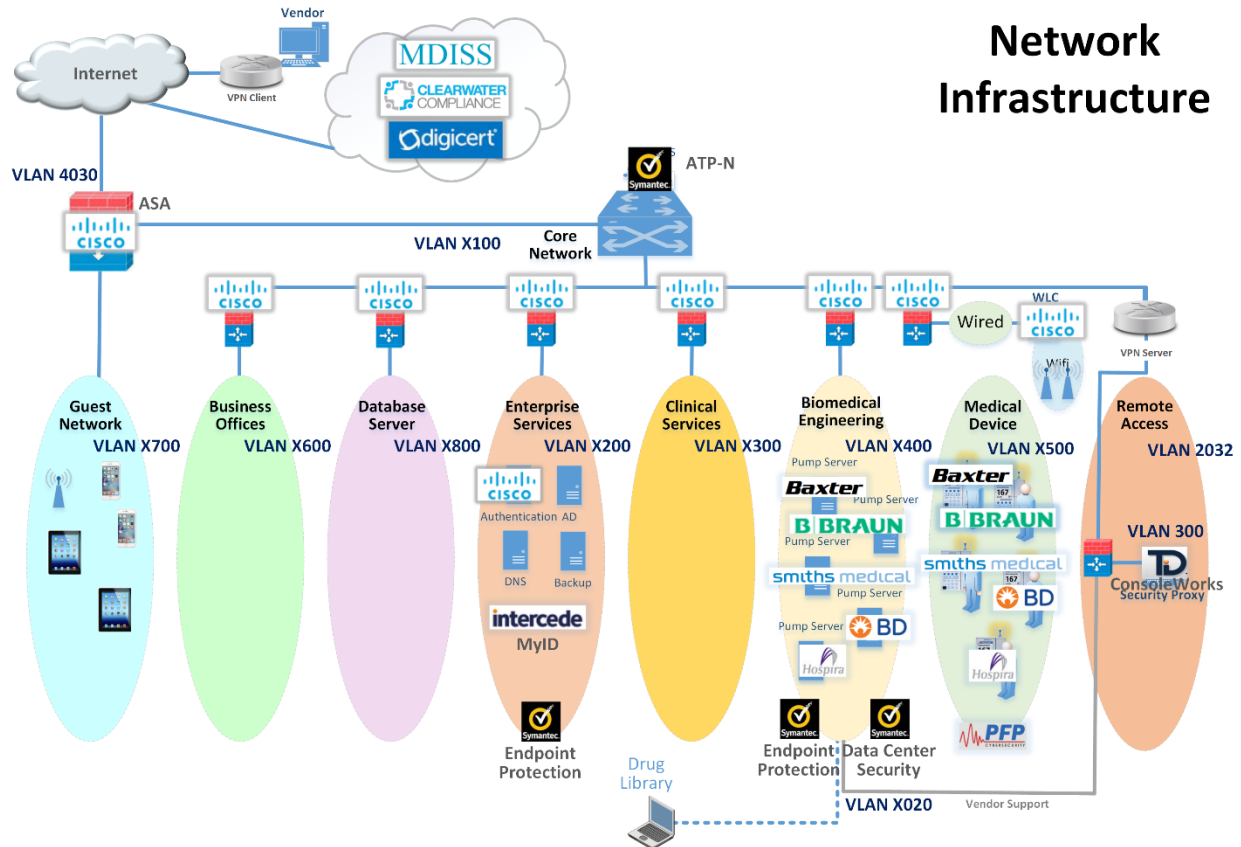
51 Refer to NIST SP 1800-8B: *Approach, Architecture, and Security Characteristics* for an explanation of why
 52 we used each technology.

53 1.4 Logical Architecture Summary

54 Below depicts a reference network architecture that performs groupings that would translate to
 55 network segments or zones. The rationale behind segmentation and zoning is to limit trust between

56 areas of the network. In considering a hospital infrastructure, NCCoE identified devices and usage, and
 57 grouped them by usage. The grouping facilitated the identification of network zones. Once zones are
 58 defined, infrastructure components may be configured such that those zones do not inherently have
 59 network access to other zones within the hospital network infrastructure. Segmenting the network in
 60 this fashion limits the overall attack surface posed to the infusion pump environment, and considers the
 61 network infrastructure configuration as part of an overall defense in depth strategy. [Figure 1-1](#) is
 62 included from the architecture for your reference.

63 **Figure 1-1: Logical Architecture Summary**



64

65 **2 Product Installation Guides**

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

68 **2.1 The Core Network**

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

75 Several functional segments may be part of this core network:

- 76 ▪ guest network
- 77 ▪ business office (example only)
- 78 ▪ database server (example only)
- 79 ▪ enterprise services
- 80 ▪ clinical services (example only)
- 81 ▪ biomedical engineering
- 82 ▪ medical devices with wireless LAN
- 83 ▪ remote access for external vendor support

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

88 2.1.1 Cisco ASA Baseline Configuration

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

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

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

104 2.1.2 External Firewall and Guest Network

105 We configured the build network to use network address translation (NAT) at the external firewall. This
106 is the only point in the network where NAT is used. The upstream provider uses 10.0.0.0/8 addresses on
107 the WAN interface. We also defined a LAN interface on 192.168.100.0/24 as the core network where
108 other ASAs connect. Another interface is defined as *GUEST* on 192.168.170.0/24. We assigned the
109 GUEST and LAN interfaces equal security levels higher than those for the WAN interface. When ASAs
110 interfaces are configured with equal security levels, by default they cannot communicate with each
111 other, but they will both have WAN access. Dynamic Host Configuration Protocol (DHCP) [6] is enabled
112 on the GUEST interface for addressing.

113 See Section [A.2](#) for the ASA configuration for this zone.

114 2.1.3 Enterprise Services

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

119 See Section [A.3](#) for the ASA configuration for this zone.

120 2.1.4 Biomedical Engineering Network

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

125 Generally, the firewall is configured in this way:

126 All pump servers -> internet/intranet (all destinations)

127 All intranet -> all pump servers Ping and Traceroute (primarily for debugging)

128 All pumps -> *Smiths Medical Pump Server* on port 1588

129 All pumps -> *Carefusion Pump Server* on port 3613

130 All pumps -> *Baxter Pump Server* on port 51244

131 All pumps -> *Hospira Pump server* on ports 443, 8443, 8100,9292,11443, 11444

132 All pumps -> *B. Braun Pump server* on ports 443, 80, 8080, 1500, 4080

133 See Section [A.4](#) for the ASA configuration for this zone.

134 2.1.5 Medical Devices

135 We defined a LAN interface on 192.168.150.0/24 as the LAN for all medical devices. The infusion pump
136 systems are designed such that all external connections to the pumps, such as an EHR system or vendor
137 maintenance, is completed with the associated pump server on the Biomedical Engineering network.
138 This enables us to disallow all outbound traffic not destined for the Biomedical Engineering network. In
139 addition, because some pump servers initiate connections to open ports on the pumps, we added
140 vendor-specific rules to allow this. A DNS server is not useful in this case, but, if you needed one, we
141 recommend that the ASA act as a forwarder. The DHCP server on the ASA is enabled for LAN addressing.
142 In our lab, we discovered that at least one brand of infusion pump would not recognize network setup
143 as complete unless at least one DNS server address was set. In this case, the DNS server address only
144 needed to be included in the configuration; a DNS server did not actually need to be present at that
145 address.

146 Generally, the firewall is configured in this way:

147 All pumps -> all pumps servers

148 All intranet -> all pumps Ping and Traceroute (primarily for debugging)

149 *Hospira Pump Server* -> All pumps ports 8100, 9292, 443, 8443

150 *Baxter Pump Server*-> All pumps port 51243

151 *B. Braun Pump Server* -> All pumps ports 80, 443, 8080, 1500

152 See Section [A.5](#) for the ASA configuration for this zone.

153 2.1.6 Cisco Catalyst Switch Configuration

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

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

163 http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/hardware/quick/guide/cat3650_gsg.html.

164
165 See Section [A.6](#) for the switch configuration.

166 2.1.7 Cisco Enterprise Wi-Fi Infrastructure

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

174 2.1.7.1 Installation

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

177 http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Virtual_Wireless_LAN_Controller_Deployment_Guide_8-2.html.

178
179 We imported the virtual appliance called *AIR_CTVM_K9_8_2_111_0.ova*, assigning the first interface to
180 the management network, referred to as *service-port* in the web interface. The second interface is used
181 as a trunk port, with VLAN tags for all user and Wi-Fi management traffic. In the web interface, the built-
182 in *management* interface refers to the wireless system control traffic network that the APs are
183 connected to.

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

187 **2.1.7.2 Controller Configuration**

188 Configure Network Interfaces:

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

General Information

Interface Name management
MAC Address 00:50:56:ac:6d:08

Configuration

Quarantine
Quarantine Vlan Id 0

NAT Address

Enable NAT Address

Interface Address

VLAN Identifier 1520
IP Address 192.168.250.2
Netmask 255.255.255.0
Gateway 192.168.250.1
IPv6 Address ::
Prefix Length 128
IPv6 Gateway ::
Link Local IPv6 Address fe80::250:56ff:feac:6d08/64

Physical Information

Port Number 1
Enable Dynamic AP Management

DHCP Information

Primary DHCP Server 192.168.250.1
Secondary DHCP Server 0.0.0.0
DHCP Proxy Mode Global ▾

190

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

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

Interfaces > New

Interface Name ip_dev
VLAN Id 1500

194

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

General Information

Interface Name ip_dev
 MAC Address 00:50:56:ac:6d:08

Configuration

Quarantine
 Quarantine Vlan Id 0
 NAS-ID none

Physical Information

Port Number 1
 Enable Dynamic AP Management

Interface Address

VLAN Identifier 1500
 IP Address 192.168.150.2
 Netmask 255.255.255.0
 Gateway 192.168.150.1

197

198 Our completed Interfaces list looks like the following:

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

199

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

NTP Servers > New

Server Index (Priority) 2
 Server IP Address(Ipv4/Ipv6) 192.168.250.1
 Enable NTP Authentication

201

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

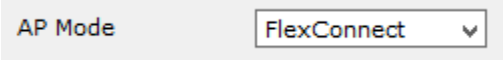
DHCP Parameters

203 Enable DHCP Proxy

204 *2.1.7.3 Wireless AP Connection and Setup*

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

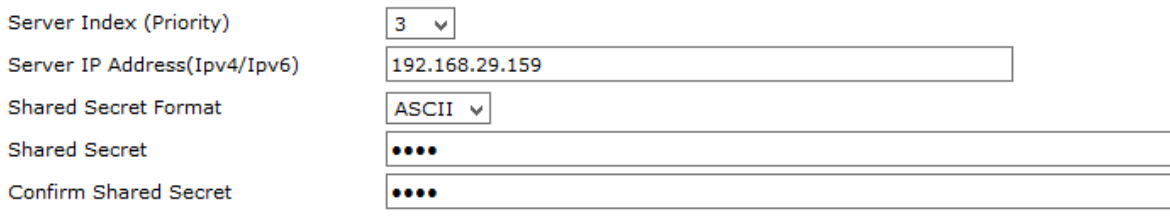
210 As each AP is connected, it should show up in the *Wireless* tab on the WLC. For each AP, the *AP Mode*
 211 needs to be set to *FlexConnect* (see below).

212 

213 *2.1.7.4 Authentication Configuration*

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

RADIUS Authentication Servers > New

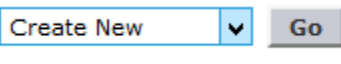
216 

217 *2.1.7.5 WLANs Configuration*

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

221 To create a new SSID, follow these steps:

222 1. Use the WLAN tab.

223 

224 2. Enter your new SSID information.

WLANs > New

Type	WLAN
Profile Name	IP_Dev
SSID	IP_Dev
ID	4

225

- 226 3. In **WLANs > WLANs** -> **WLANs**, select the WLAN ID number of the newly created SSID. Set *Status* to
227 *Enabled* and Interface/Interface Group(G) to *ip_dev*.

WLANs > Edit 'IP_Dev'

The screenshot shows the configuration page for a WLAN named 'IP_Dev'. The 'Security' tab is selected. The configuration includes:

- Profile Name: IP_Dev
- Type: WLAN
- SSID: IP_Dev
- Status: Enabled
- Security Policies: [WPA2][Auth(PSK)]
(Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface/Interface Group(G): ip_dev
- Multicast Vlan Feature: Enabled
- Broadcast SSID: Enabled
- NAS-ID: none

228

- 229 4. On the **Security tab** under **Authentication Key Management**, uncheck *802.1X*, check *PSK*, and set
230 the PSK field.

The screenshot shows the configuration interface for AAA Servers, specifically the Layer 2 Security section. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. 'MAC Filtering' is unchecked. Under 'Fast Transition', 'Fast Transition' is unchecked. Under 'Protected Management Frame', 'PMF' is set to 'Disabled'. Under 'WPA+WPA2 Parameters', 'WPA Policy' is unchecked, 'WPA2 Policy' is checked, 'WPA2 Encryption' is set to 'AES' (with 'TKIP' unchecked), and 'OSEN Policy' is unchecked.

231

The screenshot shows the 'Authentication Key Management' section. '802.1X' is unchecked, 'CCKM' is unchecked, 'PSK' is checked, 'FT 802.1X' is unchecked, and 'FT PSK' is unchecked. 'PSK Format' is set to 'ASCII'. There is a password field with six dots. 'WPA gtk-randomize State' is set to 'Disable'.

232

- 233 5. For the SSID *IP_Dev_Cert*, repeat the steps above, but do not change the Security Settings for
- 234 Authentication Key Management; leave *802.1X* checked, and leave *PSK* unchecked.
- 235 6. On the **Security, AAA Servers** tab, select the *RADIUS* server to authenticate with.

WLANs > Edit 'IP_Dev_Cert'

236

237

2.1.7.6 Monitoring

238 By using **Monitor -> Clients**, you will find the list of currently connected clients, which SSID they are
 239 connected to, and the User Name 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

240

241

2.1.7.7 Final Configuration

242 See Section [A.7](#) for the WLC configuration, accessing details about additional configuration options at
 243 *Cisco Wireless Controller Configuration Guide, Release 8.0*,
 244 http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80.html.

245

2.1.8 TDi ConsoleWorks External Remote Access

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

249 System Environment:

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

- 252 ▪ 8GB RAM
- 253 ▪ 40 GB HDD
- 254 ▪ 1 Network Interface

255 Other requirements:

- 256 ▪ ConsoleWorks install media (we built from a CD)
- 257 ▪ ConsoleWorksSSL-<version>.rpm
- 258 ▪ ConsoleWorks_gui_gateway-<version>.rpm
- 259 ▪ ConsoleWorks license keys (*TDI_Licenses.tar.gz*)
- 260 ▪ Software installation command
- 261 ▪ `yum install uuid libpng12 libvncserver`

262 Installation:

263 As Root:

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

286 Usage:

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

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

297 Initial Configuration of Graphical Gateway

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

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

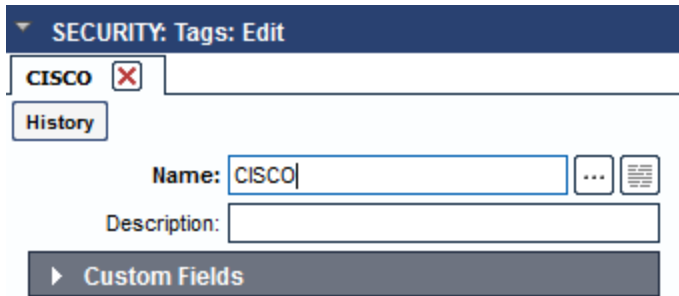
- 301 1. Click on Graphical->Gateways->Add.
- 302 2. Set a name: LOCAL, then set Host as Localhost and port as 5172.
- 303 3. Check the Enabled box and click Save.
- 304 4. Verify that it works by clicking Test in the top-left corner.

305

306 Create one tag for each vendor company:

- 307 1. Click on Security->Tags->Add.
- 308 2. Set Name, usually the company name.
- 309 3. Click *Save*.

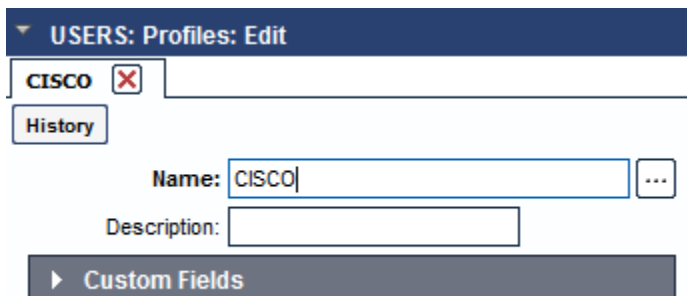
DRAFT



310

311 Create one profile for each vendor company.

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



315

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

- 317 1. Click on Security->Access Control->Add.
- 318 2. Set Name to Vendor_Company_Graphical.
- 319 3. Check *Enabled*.
- 320 4. Set *Order*.
- 321 5. Set *Allow*.
- 322 6. Set Component Type to Graphical Connection.
- 323 7. Look under *Profile Selection*; you should see:
 - 324 ■ Property Profile Equals *Vendor Company Profile Name* <join>.
 - 325 ■ Vendor company profile should appear in the box on right.

SECURITY: Access Control: Edit

View Access Control Rules [X] Edit Access Control Rule [X]

History

Name: CISCO_GRAPHICAL

Description:

Enabled

Order: 9

Allow or Deny: ALLOW

Audit Rule Usage

Component Type: Graphical Connection

Profile Selection

Simple Basic Advanced

Selection: - Property_Profile_Equals_CISCO <join>

Profiles

CISCO

326

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

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

Resource Selection

Simple Basic Advanced

Selection: - Associated With a Tag that - Property_Tag_Equals_CISCO <join>

Graphical Connections

No Graphical Connections match.

330

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

- 332 Aware
- 333 View
- 334 Connect

Privileges

All

Component Level:

Add

Resource Level:

Aware Connect

Delete Delete Recordings

Disable Disconnect

Edit Enable

Lock Recordings Monitor

Rename Unlock Recordings

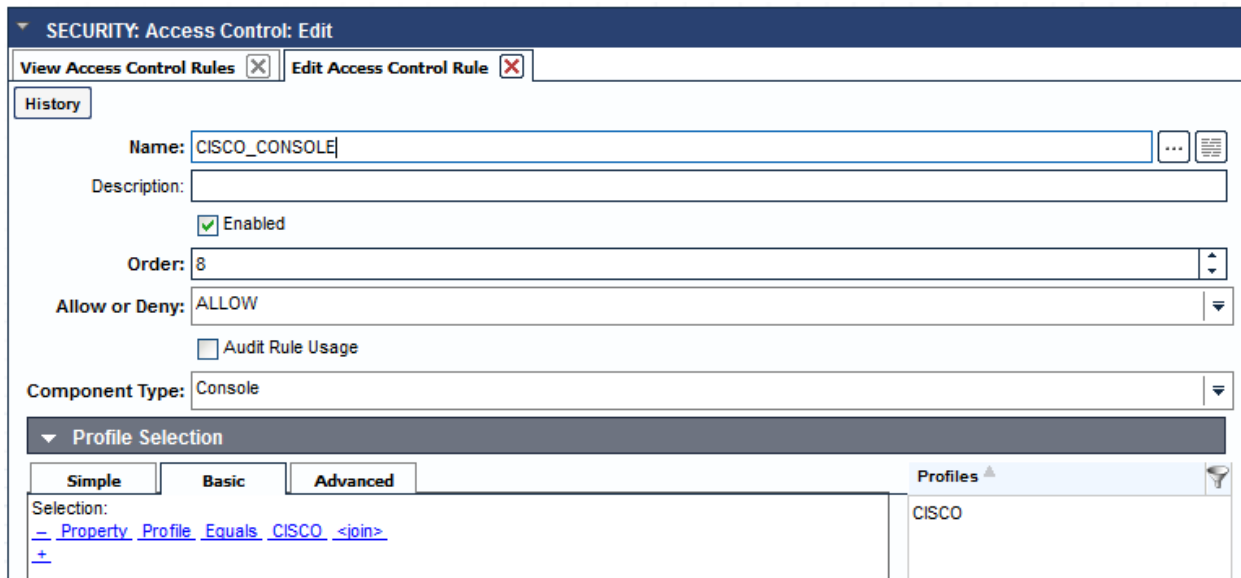
View View Recordings

View Usage

335

336 Console Access Controls (repeat this section for each vendor company):

- 337 1. Security->Access Control->Add
- 338 2. Set Name to Vendor_Company_Console.
- 339 3. Check *Enabled*.
- 340 4. Set *Order*.
- 341 5. Set *Allow*.
- 342 6. Set Component Type to Console.
- 343 7. Look at *Profile Selection*. You should see:
 - 344 ▪ Property Profile Equals **Vendor Company Profile Name** <join>.
 - 345 ▪ Vendor company Profile should appear in the box on right.



- 346
- 347 8. Look under *Resource Selection*; you should see:
 - 348 ▪ Associated with a Tag that
 - 349 • Property Tag Equals **Vendor Company Tag name** <join>



- 350
- 351 9. Matching consoles should appear in the box on right. Under Privileges, check:

DRAFT

- 352 ▪ Aware
- 353 ▪ View
- 354 ▪ Connect

▼ Privileges

All

Component Level:

<input type="checkbox"/> Add	<input type="checkbox"/> Disable All	<input type="checkbox"/> Disable Scan All
<input type="checkbox"/> Display All Hidden	<input type="checkbox"/> Enable All	<input type="checkbox"/> Enable Scan All
<input type="checkbox"/> Hide All		

Resource Level:

<input type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Aware
<input type="checkbox"/> Can send break	<input checked="" type="checkbox"/> Connect
<input type="checkbox"/> Controlled Connect	<input type="checkbox"/> Delete
<input type="checkbox"/> Disable	<input type="checkbox"/> Disable Scan
<input type="checkbox"/> Disconnect	<input type="checkbox"/> Display Hidden
<input type="checkbox"/> Edit	<input type="checkbox"/> Edit Event Occurrence
<input type="checkbox"/> Enable	<input type="checkbox"/> Enable Scan
<input type="checkbox"/> Exclusive Connect	<input type="checkbox"/> Expunge
<input type="checkbox"/> Hide	<input type="checkbox"/> Lock Console
<input type="checkbox"/> Make Comment in Log	<input type="checkbox"/> Modify Log Annotation
<input type="checkbox"/> Monitor	<input type="checkbox"/> Purge
<input type="checkbox"/> Remediate	<input type="checkbox"/> Rename
<input type="checkbox"/> Send Command	<input type="checkbox"/> Send File
<input type="checkbox"/> Send protected characters	<input type="checkbox"/> Trigger Event
<input type="checkbox"/> Update Baseline Run	<input checked="" type="checkbox"/> View
<input type="checkbox"/> View Baseline Run	<input type="checkbox"/> View Event Occurrence
<input type="checkbox"/> View Log	<input type="checkbox"/> View Monitored Events
<input type="checkbox"/> View Usage	

355

356 Users:

357 Users->Add:

- 358 1. Set *Name*.
- 359 2. Set *Password* and retype password to confirm.
- 360 3. Fill in contact information.
- 361 4. Set *Profile* to the one defined for this user's company.
- 362 5. Click *Save*.

USERS: Add *

View Users X Add User * X

Find an Example

Name: test

Description: Test Company

Login Expiration:

User Created:

Last Login:

Use External Authentication

▼ Password

Password: ●●●●●●

Retype Password: ●●●●●●

Require Password Change On Next Login

► Password Rules

▼ Contact Info

First Name:

Last Name:

Email:

Title:

Office Phone:

Cell Phone:

Address/Location:

▼ PROFILES * (1)

CISCO

Add

Remove

View

► REMEDIATION HISTORY (0)

► TAGS (0)

363

364 RDP Graphical Connections

365 Follow these steps to add a *RDP* graphical connection:

- 366 1. Graphical->Add
- 367 2. Set *Name* for the device you are connecting to.
- 368 3. Set *Type* to *RDP*.
- 369 4. Set *Hostname/IP* for the device you are connecting to.
- 370 5. Set Authentication:
 - 371 ▪ Username
 - 372 ▪ Password
 - 373 ▪ *Domain* (optional).
- 374 6. Add Graphical Gateway named Local.
- 375 7. Add Tags for all vendor companies that should have access.
- 376 8. Click *Save*.

The screenshot shows a software interface for editing a graphical connection. The main window is titled 'GRAPHICAL: Edit' and has a tab for 'IP_DEV_ACTIVE_DIRECTORY'. The configuration is as follows:

- Name:** IP_DEV_ACTIVE_DIRECTORY
- Description:** Enterprise Services
- Type:** RDP
- Host:** 192.168.24.162
- Port:** (empty)
- Single Session Connection
- Allow Join with Active Session
- Status:** Available (with a 'Disable' button)
- Max Idle Time:** 0-999 Minutes (0=disabled)
- Recordings:** (collapsed)
- Authentication:**
 - Username:** administrator
 - Password:** (masked with dots)
 - Domain:** IP
 - Security Mode:** (empty)
 - Disable Authentication
 - Ignore Certificate Errors

The right-hand sidebar contains three sections:

- GATEWAYS (1):** LOCAL (with 'Add', 'Remove', and 'View' buttons)
- CONSOLES (0):** (collapsed)
- TAGS (1):** SYMANTEC (with 'Add', 'Remove', and 'View' buttons)

377

378 *SSH Console Connections*379 Follow these steps to add a *SSH* console connection:

380 1. Consoles->Add

381 2. Set *Name* for the device you are connecting to.382 3. Set the *Connector* to *SSH Session with Password Connection Details*.

383 4. Set the Host IP for the device you are connecting to by doing the following:

384 a. Set Port to 22.

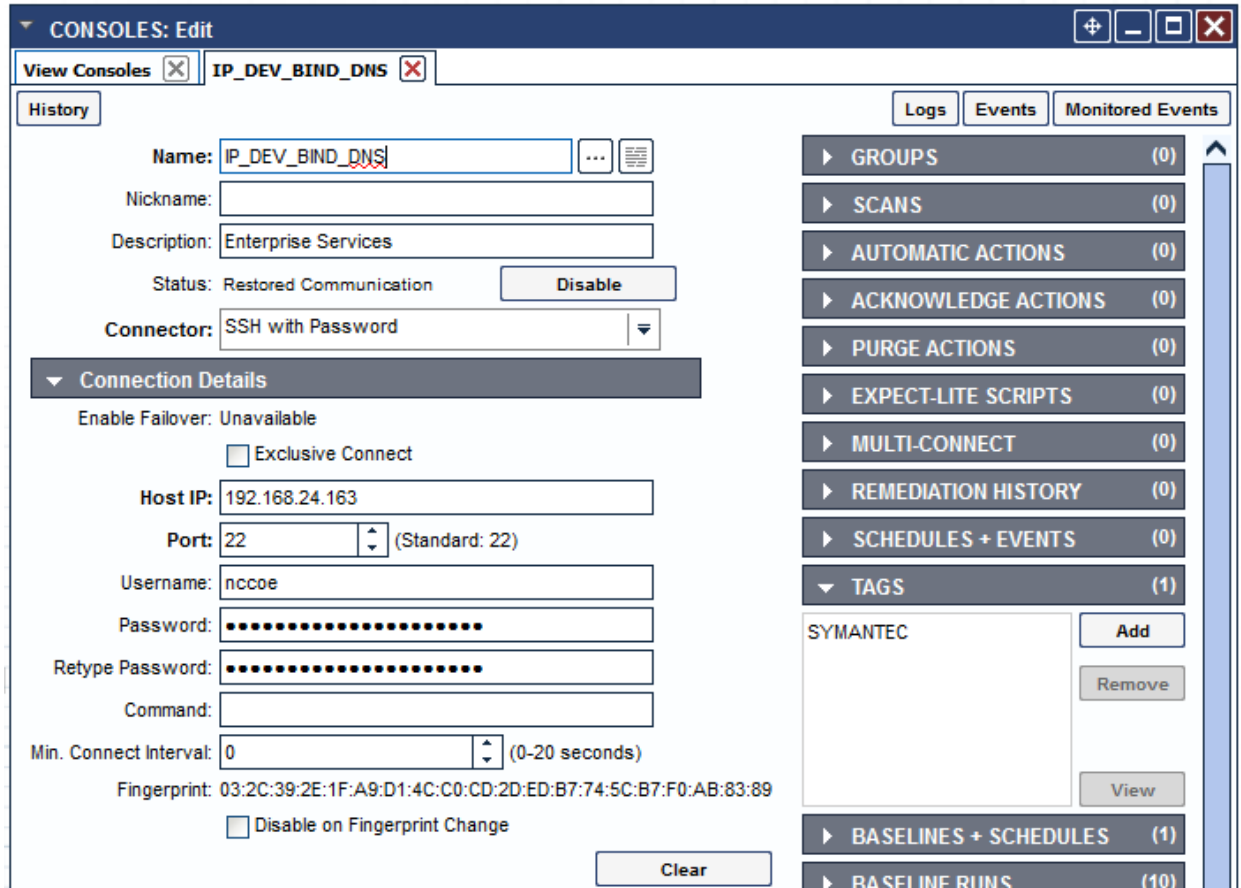
385 b. Set Username.

386 c. Set Password.

387 d. Retype the password.

388 5. Add tags for all vendor companies that should have access.

389 6. Click *Save*.



390

391 2.2 Infusion Pump and Pump Server

392 2.2.1 Infusion Pumps

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

394 Table 2-1: Infusion Pump List

Vendor Name	Product Name	Product Type	Description
B. Braun	SpaceStation	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 SpaceStation and uses SpaceStation for network communication

Vendor Name	Product Name	Product Type	Description
Baxter	Baxter Sigma Spectrum	Wireless infusion pump	Provides large-volume infusion capability for patients.
BD	Alaris PC 8015	Infusion pump core system	Provides a common user interface for programming infusion, network connection, and monitoring modules. The Alaris® 8015 PC Unit is the core of the Alaris® System and provides a common user interface for programming infusion and monitoring modules.
	Alaris Syringe 8110	Syringe infusion pump	Provides syringe infusion capability for patients and it works with Alaris PC unit.
	Alaris Pump 8100	Large-volume infusion pump	Provides large-volume infusion capability for patients and it works with Alaris PC unit.
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 Infusion pump to manage pain
Smiths Medical	MediFusion 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

395 *2.2.1.1 Infusion Pump Setup*

396 In our example solution, we generalized the infusion pump vendors' products and systems as infusion
397 pump devices, infusion pump servers, and infusion pump ecosystems. Our first goal was to connect each
398 vendor's infusion pump(s) to their corresponding pump server for performing the basic operational

399 events, such as registering the devices to the server; pushing/installing the new drug library to the
 400 pumps; pushing/updating the new version of software to the pumps, and keeping the log of the pump
 401 usage.

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

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

411 **Table 2-2: Summary of Infusion Pump Configuration Methods**

Vendors	Infusion Pump Model	Configuration Tool	Connection Methods
Baxter	Sigma Spectrum	Uses a PC with an IrDA interface to program multiple pumps with the same configuration Edits the network configuration file (a simple text file) on a PC and send it via the IrDA to a pump	Uses the IrDA Serial Infrared Link to a PC under the IrDA Serial Infrared Link Management Protocol v1.1
B. Braun	Space Station	Connects PC with HiBaSeD Service program to the Space Station using a B. Braun interface cable for pump configuration setting	Uses special B. Braun interface cable
	Infusomat® Space large volume infusion pump	Connects PC with HiBaSeD Service program to the Space Station using a B. Braun interface cable for pump configuration setting	Uses special B. Braun interface cable
	Perfusor® Space Syringe Pump	Connects PC with HiBaSeD Service program to the Space Station using a B. Braun interface cable for pump configuration setting	Uses special B. Braun interface cable
BD	The Alaris® 8015 PC	Uses management system to do the configuration. The Alaris® 8015 PC Unit is	Uses series cable to connect pump to a local computer.

Vendors	Infusion Pump Model	Configuration Tool	Connection Methods
		the core of the Alaris® System and provides a common user interface for programming infusion and monitoring modules.	
Hospira	Hospira PCA	Accesses Web Config utility on Pump through a web browser using the Local IP address of the pump	Uses pump's Ethernet Jack to connect to a LAN or to interface with host computer
	Plum 360	Accesses Web Config utility on Pump through a web browser using the Local IP address of the pump	Uses pump's Ethernet Jack to connect to a LAN or to interface with host computer
Smiths Medical	MediFusion 4000	Pushes configuration text file to pump using the Telnet from a PC connected to the pump with the known IP address	Connects a PC to pump using micro USB-USB cable
	CADD Solis 2000	Uses Smiths Medical Network Configuration Utility to update the pump's configuration parameters	Connects a PC to pump using micro USB-USB cable

412 2.2.1.2 Infusion Pump Configuration

413 Pre-Conditions:

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

417 Post-Conditions:

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

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

- 422 ▪ For wireless properties
 - 423 • Enable wireless
 - 424 • Use DHCP

- 425 • Set SSID (IP_Dev or IP_Dev_Cert)
- 426 ▪ For wireless security properties
- 427 • Set Security Mode (WPA2-PSK or WPA2-Ent)
- 428 • Set Encryption Protocol to AES/CCMP
- 429 • Enter PSK password or install a PKI certificate
- 430 ▪ For pump server properties
- 431 • Set Server IP/port
- 432 • Set Device Name or ID
- 433 • Set Device Type
- 434 ▪ To verify connectivity for each infusion pump and the corresponding pump server:
- 435 • Connect pumps to AP (*IP_Dev* with PSK or *IP_Dev_Cert* with *EAP-TLS*)
- 436 • Confirm that pump receives an IP address from the DHCP server from the AP
- 437 • Confirm that the pump server can discover the pumps and display the pump status such
- 438 connected, in use, or offline.

439 2.2.1.3 *Infusion Pump Hardening*

440 Hardening may include the following:

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

445 2.2.2 Infusion Pumps Server Systems

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

Vendor Name	Product Name	Operating Platform	Description
B. Braun	DoseTrac® Infusion Management	Microsoft Windows	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 interface capability to help hospital biomedical engineering department manage their infusion pump fleet

Vendor Name	Product Name	Operating Platform	Description
			effectively. Drug Library publishing module helps hospital pharmacy distribute and enforce medication safety rules effectively.
BD	Alaris Systems Manager	Compatible with VMWare ESX and VMWare vSphere environment	Virtual server platform that provides two-way wireless communication with Alaris PC units
Hospira	Hospira MetNet Server	Microsoft Windows	Manages drug libraries, firmware updates, and configurations of intravenous pumps
Smiths Medical	PharmGuard Server	Microsoft Windows	Manages drug libraries, firmware updates, and configurations of Hospira intravenous pumps for Smiths Medical Pumps

447

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

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

455 2.3 Identity Services

456 2.3.1 Cisco Identity Service Engine (ISE)

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

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

463 System requirements

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

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

469 For your organization, follow the guidance from your VM vendor to import the OVA and start the install
470 process. Once the system boots up, follow the console display to select one of the installation options.
471 The configuration parameter selected for this use case is shown below:

```
472 ! hostname
473 ise
474 !ip domain-name
475 nccoe.lab
476 ! ipv6
477 enable
478 !interface
479 GigabitEthernet 0 ip address 192.168.29.159 255.255.255.0 ipv6 address autoconfig ipv6 enable
480 ! interface
481 GigabitEthernet 1 ip address 192.168.120.159 255.255.255.0 ipv6 address autoconfig ipv6 enable
482 !interface
483 GigabitEthernet 2 shutdown ipv6 address autoconfig ipv6 enable
484 ! interface
485 GigabitEthernet 3 shutdown ipv6 address autoconfig ipv6 enable
486 ! ip name-server
487 8.8.8.8 8.8.4.4
488 ! ip default-gateway
489 192.168.120.1
490 !
491 ! clock timezone
492 EST
493 ! ntp server
```

DRAFT

```
494 time.nist.gov
495 ! username admin password hash
496 $5$jnPlEeb4$YxDZH6oDF2Y4.02OqE/jBWxXFumRvtpe8JdNNZm1yj0 role admin
497 ! max-ssh-sessions
498 5
499 ! service sshd
500 enable
501 ! password-policy
502 lower-case-required
503 upper-case-required
504 digit-required
505 no-username
506 no-previous-password
507 password-expiration-enabled
508 password-expiration-days 45
509 password-expiration-warning 30
510 min-password-length 4
511 password-lock-enabled
512 password-lock-timeout 15
513 password-lock-retry-count 3
514 ! logging loglevel
515 6
516 ! conn-limit 10
517 port 9060
518 ! cdp timer
519 60 cdp holdtime 180 cdp run GigabitEthernet 0
520 ! icmp echo
521 on
522 !
```


523 [2.3.1.1 Configure ISE to Support EAP-TLS Authentication](#)

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

528 [2.3.1.2 Set ISE to Support RADIUS Authentication](#)

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

531 1. Add a Network Resource

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

534 ▪ The name of the network device

535 ▪ The IP Address of the device with its subnet mask.

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

538 3. Populate the system certificate with CA-signed certificates. We replaced the Cisco ISE default self-
539 signed certificate with the CA-signed certificate issued through DigiCert Certificate Authority. The
540 steps for acquiring the signing certificate from DigiCert are described in the next Section [2.3.2,](#)
541 [DigiCert Certificate Authority](#).

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

544 5. From the ISE Administration Portal, use the navigation path **Administration > System > Certificates**
545 **> System Certificate** to show the installed certificates. Then select Import to open a screen for
546 importing Server certificate. Fill in the required information as shown in the following screen shot.

547 **Figure 2-1: Importing Server Certificate**

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > System > Certificates. The page is titled "Certificate Management" and includes a left-hand navigation menu with options like Overview, System Certificates, Endpoint Certificates, Trusted Certificates, OCSP Client Profile, Certificate Signing Requests, and Certificate Periodic Check Setti... Below the menu, there are several configuration fields and checkboxes:

- * Select Node: ise
- * Certificate File: Browse... isecertbydigicer.crt
- * Private Key File: Browse... ISECertByDigiCer.key
- Password: [Redacted]
- Friendly Name: ISE Cert From DigiCert
- Allow Wildcard Certificates:
- Validate Certificate Extensions:
- Usage:
 - Admin: Use certificate to authenticate the ISE Admin Portal
 - EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
 - pxGrid: Use certificate for the pxGrid Controller
 - SAML: Use certificate for SAML Signing
 - Portal: Use for portal

At the bottom of the form, there are "Submit" and "Cancel" buttons.

548

549

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

552 7. Import the DigiCert Root CA and signing CA to ISE Trusted Certificates. From the ISE Administration
 553 Portal, use the navigation path **Administration > System > Certificates > Trusted Certificate** to show
 554 the installed certificates. Then select Import to open a screen for importing DigiCert Root CA and the
 555 signing CA individually.

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

557 b. Establish the OCSP [13] client profile from the OCSP Client Profile page under the
 558 **Administration > System > Certificates > OCSP Client Profile**.

559 c. If OCSP (Online Certificate Status Protocol) is used for Certificate Status Validation, check
 560 Validate against OCSP Service and enter the OCSP service name.

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

566 To create a Certificate Authentication Profile:

- 567 ▪ Use the Administration Portal to navigate to the path Administration > Identity Management >
568 External Identity Sources > Certificate Authentication Profile and click *Add*.
- 569 ▪ Name the profile as, for example, “Cert_Auth_Profile”, then fill out the form with proper
570 parameters. Be sure to select *Subject Name* as the Principal Username X509 attribute because it
571 is the field that will be used to validate the authenticity of the client.
- 572 ▪ Select the *Identity Resource Sequences* tab, in the Certificate Based Authentication, check *Select*
573 *Certificate Authentication Profile* and choose the *Cert_Auth_Profile* from the dropdown list.
- 574 9. Set *Authentication Protocols*. Cisco ISE uses authentication protocols to communicate with external
575 identity sources. Cisco ISE supports many authentication protocols such as the Password
576 Authentication Protocol (PAP), Protected Extensible Authentication Protocol (PEAP), and the
577 Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). For this build, we used the
578 EAP-TLS protocol for user and machine authentication. To specify the allowed protocols services in
579 Cisco ISE:
- 580 ▪ From the Administration Portal navigate to the path Policy >Policy Elements > Results
581 >Authentication > Allowed Protocols > Add
- 582 ▪ Select the preferred protocol or list of protocols. In this build, the EAP_TLS is selected as the
583 allowed authentication protocol.
- 584 10. Set up *Authentication Policy*. Define the authentication policy by selecting the protocols that ISE
585 should use to communicate with the network devices, and the identity sources that it should use for
586 authentication. To specify the authentication policy:
- 587 ▪ From the Administration Portal navigate to the path **Policy >Authentication Policy > Type > Rule**
588 **Based**.
- 589 ▪ Set “if Protocol is Wireless 802.1x, use the Network Device as defined in Step 1 and the Identity
590 Sequences as defined in Step 8.

591 2.3.2 DigiCert Certificate Authority

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

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

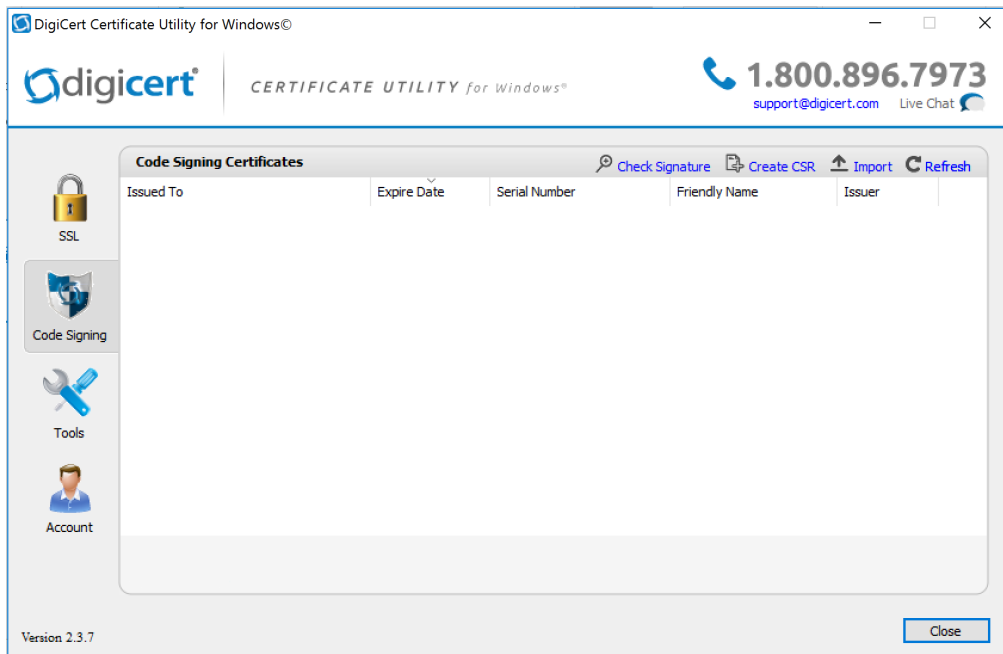
598 2.3.2.1 Create a Certificate Signing Request (CSR)

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

DRAFT

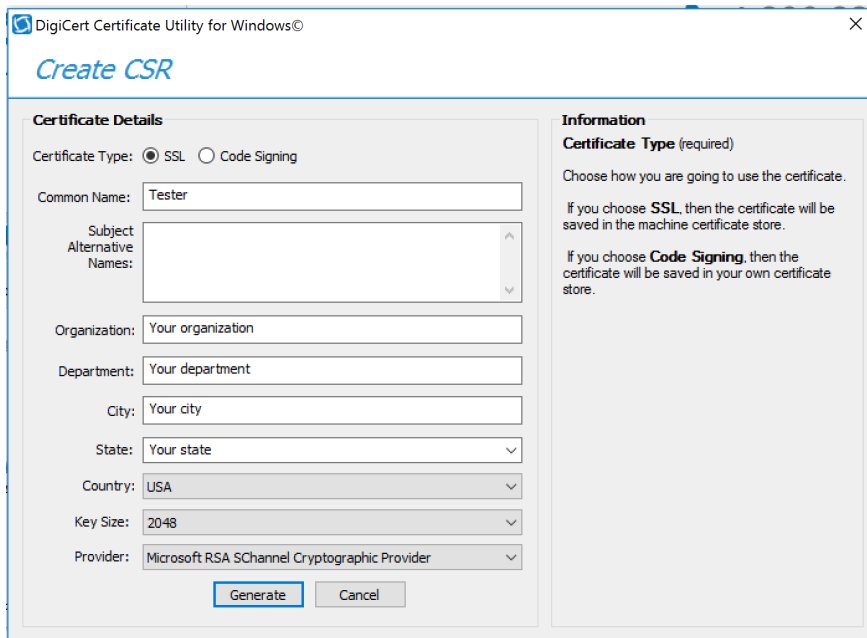
605 Download and save the DigiCertUtil.exe from [https://www.digicert.com/util/csr-creation-microsoft-](https://www.digicert.com/util/csr-creation-microsoft-servers-using-digicert-utility.htm)
606 [servers-using-digicert-utility.htm](https://www.digicert.com/util/csr-creation-microsoft-servers-using-digicert-utility.htm).

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



608

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

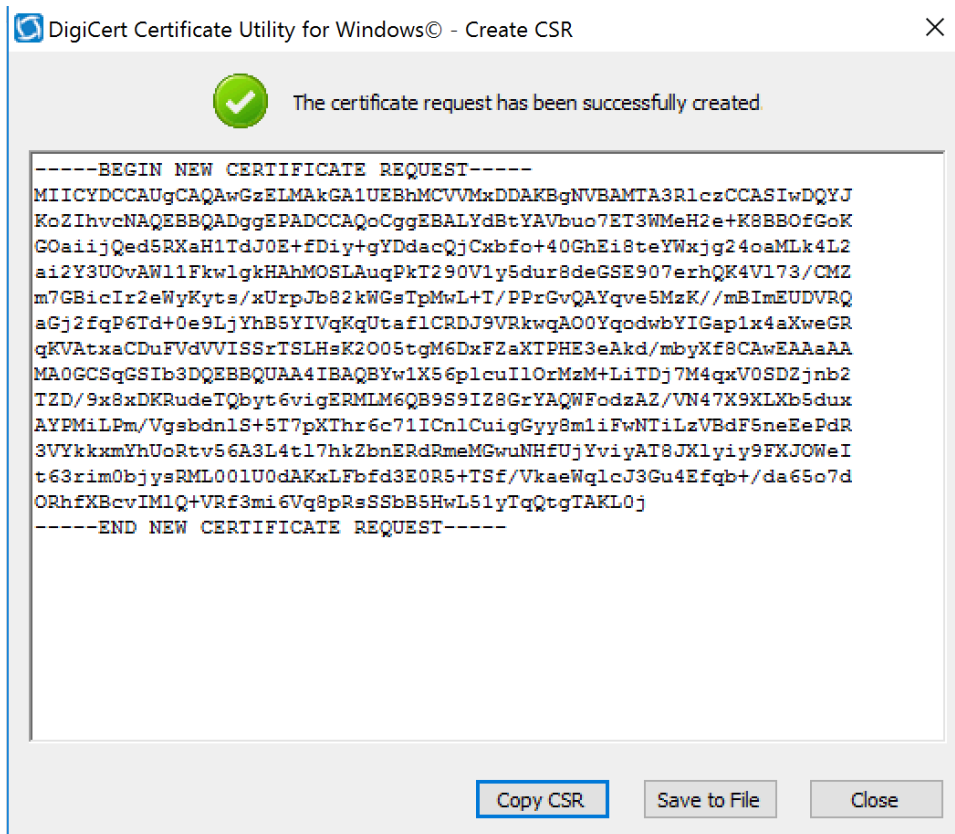


610

611 3. On the Create CSR window, fill in the key information (some is optional):

- 612 ▪ Certificate Type: Select *SSL*
- 613 ▪ Common Name: Enter the entity name
- 614 ▪ Organization: Enter your company's legally registered name

- 615 ▪ City: Enter the city where your company is legally located
- 616 ▪ State: Select the state where your company is legally located
- 617 ▪ Country: Select the country where your company is legally located
- 618 ▪ Key Size: In the drop-down list, select *2048*
- 619 ▪ Provider: Select *Microsoft RSA SChannel Cryptographic Provider* (unless you have a
620 specific cryptographic provider)
- 621 4. Click **Generate** to generate a CSR:



- 622
- 623 This will also generate a corresponding private key in the Windows computer from which the CSR is
624 requested. The Certificate Enrollment Request is stored under: (*Console Root\Certificates(Local*
625 *Computer)\Certificate Enrollment Requests\Certificates*).

626 2.3.2.2 Issue Signed Certificates

- 627 5. With a created applicant CSR, request a signed certificate using DigiCert CertCentral portal.
- 628 ▪ Login to a DigiCert Dashboard <<https://www.digicert.com/account/login.php>> with your
629 account user name and password.
 - 630 ▪ Once in the portal, go to **Request a Certificate**, then select **Private SSL** to open a certificate
631 request form. Fill in the certificate settings in the fields shown in the form which includes
632 pasting the CSR information to the area called *Paste your CSR*.

- 633 6. After filling in all the required information and scroll down to the bottom of the page and click on
 634 the “I agree to the Certificate Services Agreement above” check box, click the **Submit Certificate**
 635 **Request** button at the bottom of the form to submit the certificate for signing approval. The
 636 administrator of the CA authority will use the same portal with different privilege to prove the
 637 request after reviewing and verifying the submitted request information if needed.
- 638 7. To download the signed certificate, go to **CERTIFICATES->Orders** to list the ordered signed
 639 certificates:

The screenshot shows the 'Orders' page in the DigiCert CERTCENTRAL portal. The page header includes the DigiCert logo and 'CERTCENTRAL' branding, along with the text 'National Institute of Standards and Technology'. The left sidebar contains navigation options: REQUEST A CERTIFICATE, DASHBOARD, CERTIFICATES, Orders, Requests, Domains, Organizations, Expiring Certificates, INSPECTOR, MONITOR, FINANCES, ACCOUNT, SETTINGS, and TOOLS. The main content area is titled 'Orders' and features a search bar with a dropdown menu set to 'Active', a search input field, a 'Go' button, and a 'Show Advanced Search' link. Below the search bar is a table of certificate orders.

Order #	Date	Common Name	Status	Validity	Product	Expires
1375546 Quick View	23 Mar 2017	BBraun	Issued	1 year	Private SSL	23 Mar 2018
1364007 Quick View	16 Mar 2017	Smiths	Issued	1 year	Private SSL	16 Mar 2018
1363934 Quick View	16 Mar 2017	Hospira	Issued	1 year	Private SSL	16 Mar 2018
1363251 Quick View	16 Mar 2017	Carefusion	Issued	3 years	Private SSL	16 Mar 2018
1361950 Quick View	15 Mar 2017	Baxter	Issued	1 year	Private SSL	15 Mar 2018
1361779 Quick View	15 Mar 2017	ISECertByDigiCer	Issued	1 year	Private SSL	15 Mar 2018

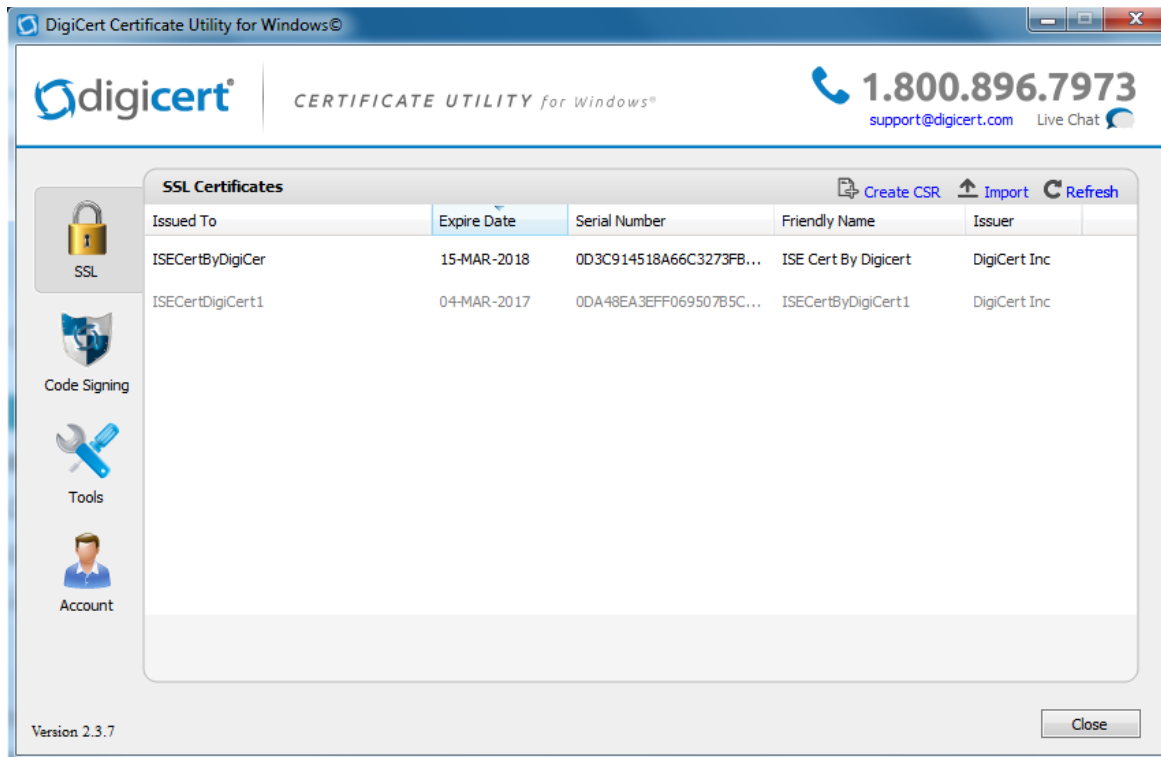
640 6 total

- 641 8. Click a specific order number to display the certificate details with a list of actions for you to
 642 perform. Click the **Download Certificate As** to download certificates with signed CA and Root CA
 643 certificates. A variety of certificate formats can be downloaded, such as .crt, .p7b, or .PEM, etc.
- 644 9. Save the downloaded certificate in a location where it can be used for further processing if needed.

645 2.3.2.3 Import and Export the Signed Certificate

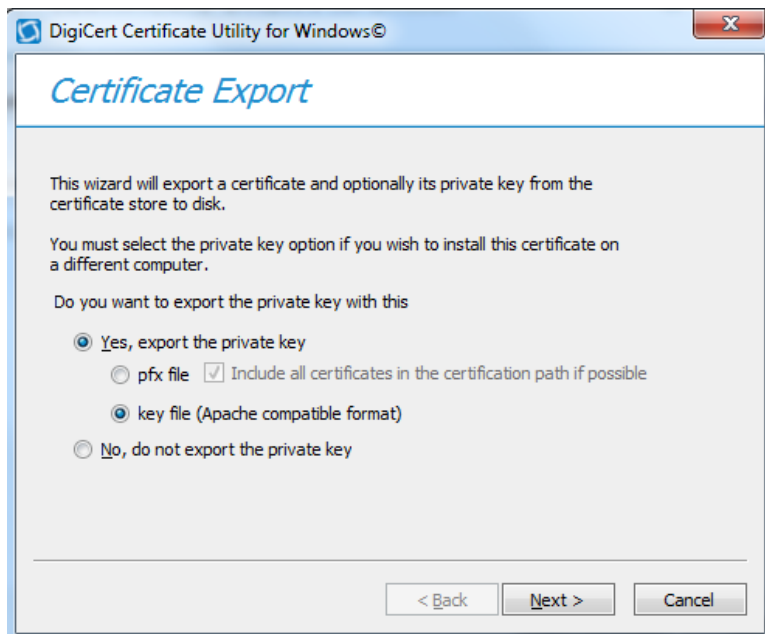
646 Using the DigiCert Utility and OpenSSL tool, you can further manipulate the certificates to combine with
 647 the private key and export the signed certificate, or you can convert certificates or keys to the formats
 648 specified for your organization’s devices.

- 649 10. To import a signed certificate, use DigiCert Utility to click the **Import** button to load a downloaded
 650 file to the utility. The download file was saved in Step 9 above. Click the **Next** button to import.
- 651 11. From the DigiCert Certificate utility for Windows, click **SSL** to list all the imported files.



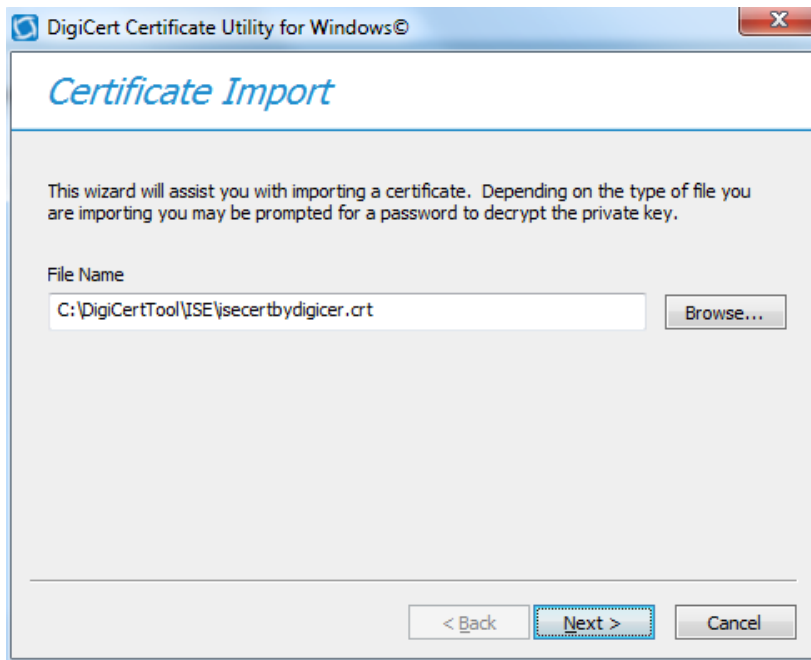
652

653 12. To export the certificate, select the certificate that you want to export as a combined certificate file
 654 and key file in a .pfx file or separated as a certificate file and key file, and then click *Export*
 655 *Certificate*.



656

657 13. Click the *Next* button and follow the wizard instruction to save the certificate file and private key file
 658 to a location you desire.



659

660 *2.3.2.4 Certificate and Key File Format Conversion*

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

- 666 ▪ To convert .crt to .pem:
 - 667 • `openssl x509 -in mycert.crt -outform PEM -out mycert.pem.`
- 668 ▪ To convert a private key into PEM format:
 - 669 • `openssl rsa -in yourdomain.key -outform PEM -out yourdomain_pem.key.`
- 670 ▪ Separate a pfx file into two different .key/.crt files:
 - 671 • For a key file: `openssl pkcs12 -in yourfile.pfx -nocerts -out keyfile-encrypted.key.`
 - 672 • For cert file: `openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out [certificate.crt].`
- 673 ▪ To convert a Cert PEM file to DER:
 - 674 • `openssl x509 -outform der -inform DEM -in certificate.pem -out certificate.der.`
- 675 ▪ To convert a key PEM file to DER:
 - 676 • `openssl rsa -inform DEM -in infile.key -out outfile.der -outform DER.`

677 **2.4 Symantec Endpoint Protection and Intrusion Detection**

678 NCCoE protected the pump server application in the notional Biomedical Engineering network by using
 679 three Symantec cybersecurity products on an enterprise network, with a specific focus on wireless
 680 infusion pumps:

- 681 ▪ Symantec Data Center Security- Server Advanced
- 682 ▪ Symantec Endpoint Protection Manager Server
- 683 ▪ Symantec Advanced Threat Protection Server.

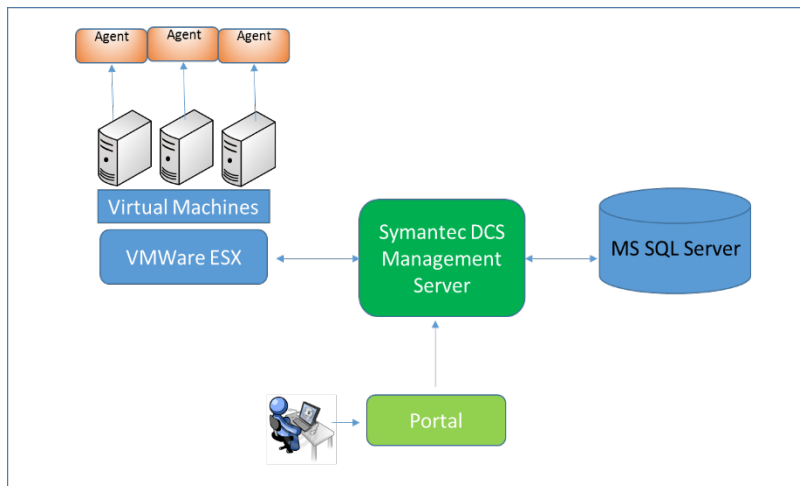
684 Each product protects components in the enterprise systems at different levels.

685 2.4.1 Symantec Data Center Security: Server Advanced

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

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

695 **Figure 2-2: Data Center Security: Server Advanced Environment**



696

697 2.4.1.1 Installing Data Center Security: Server Advanced Manager

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

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

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

707 Follow these steps to install the SQL Server software.

- 708 1. Use *SCSP* as the default instance name
- 709 2. Set authentication configuration to Mixed Mode (Windows authentication and SQL Server
710 authentication)
- 711 3. Set the “*sa*” with a password when you set Mixed Mode authentication. You will need this password
712 when you install Data Center.
- 713 4. After installing the instance of SQL Server, select to authenticate using SQL Server credentials.
- 714 5. Register the instance. Registering the instance also starts the instance.

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

- 716 1. Double click *server.exe*, then in the Welcome panel, click *Next* and accept the license agreement
- 717 2. In the Installation Type panel, click Evaluation Installation, then click Use an Existing MSSQL
718 Instance, and then click Next.
- 719 3. Follow the instructions and select the parameters suitable for your organization to complete the
720 installation.

721 See *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 MP1 Planning
722 and Deployment Guide* for further details:

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

724

725

726 *2.4.1.2 Configuration of Data Center Security: Server Advanced Manager*

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

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

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

- 734 1. Login to the DCS console.
- 735 2. Create a policy folder.
- 736 3. In the Java console, click *Policies*.
- 737 4. Under the *Policies* tab, click *Prevention* or *Detection*.
- 738 5. On the *Policies* page, in the *Workspace Folders*, select the *Workspace* folder and then right-click *Add
739 Folder*. Look for a new policy folder with the name *New Folder*. Rename this folder as *Pump Server*.
- 740 6. Copy an existing policy to the Pump Server folder.
- 741 7. From the default Symantec folder, find a proper policy example and copy it to the Pump Server.
- 742 8. Using the *Move To* command. In the *Workspace* pane, select a policy (e.g., “windows-baseline-
743 detection” policy in *Symantec folder* for *Detection*), and then right-click *Move To*. In the *MoveFolder*
744 dialog box, select *Pump Server* to receive the policy, and then click *MoveTo*.

- 745 9. To edit a policy, right-click a policy, and then click *Edit Policy*. Configure the setting based on your
746 security protection needs.
- 747 DCS Advanced Server provides a variety of configurable protection from application data protection,
748 application protection to network protection. For example, the Windows prevention policies have a
749 Protected Whitelisting strategy that lets you specify an application to which you always want to allow
750 access or give permission to run. When you whitelist a process or an application, all the other processes
751 and applications that are not included in the list are denied access.
- 752 To allow a program to run by using the Protected Whitelisting strategy, follow these steps:
- 753 10. In the management console, click the *Policies* tab and then click *Prevention*.
- 754 11. In the *Policies* workspace, click *Add*.
- 755 12. In the Select a Prevention Policy Builder wizard, in the New Policy Builder section, click *Launch*.
- 756 13. In the *Policy Name* panel, from the *Policy Pack* drop-down list, select the policy pack that you want
757 to use as the baseline for the new custom policy.
- 758 14. In the *Name* text box, enter a name for the policy that you create. In this build, we use “Windows
759 Prevention Policy 6.0 Reference 31 Protected Whitelisting strategy.”
- 760 15. Check *Create a custom prevention policy*, and then click *Next*.
- 761 16. In the *Protection Strategy* panel, use the slider to select *Protected Whitelisting*.
- 762 17. In the *Trusted Updaters* panel, click *Add*, and then in the *Select Type* dialog box, select the type of
763 updater that you want to add. The Trusted Updaters list is populated through the agent data
764 retriever. You can edit or delete an updater that you have already added to the list.
- 765 18. Click *Next*.
- 766 19. In the *Application Rules* panel, click *Add*, and then in the *Select Type* dialog box, select the type of
767 rules that you want to add. You can edit or delete a rule that you have already added to the list.
- 768 20. In the *Global Policy Options* panel, click *Configure* to configure the global policy settings, and then
769 click *Next*.
- 770 21. In the *Summary* panel, click *Save*.
- 771 **2.4.1.3 Installing Data Center Security: Server Advanced Agent**
- 772 Use agent.exe to install the agent software on computers that run supported Windows operating
773 systems. To install the Windows agent software, follow these steps:
- 774 1. On the installation package, double-click *agent.exe*.
- 775 2. In the *Welcome* panel, click *Next*.
- 776 3. In the *License Agreement* panel, select *I accept the terms in the license agreement*, and then click
777 *Next*.
- 778 4. In the *Destination Folder* panel, change the folders if necessary, and then click *Next*.
- 779 5. In the *Agent Configuration* panel, accept or change the default settings, and then click *Next*. Ensure
780 that *Enable Intrusion Prevention* is checked.

- 781 6. In the *Management Server Configuration* panel, in the Primary Management Server box, type the
782 fully qualified host name or IP address of the primary server that is used to manage this agent. If you
783 changed the Agent Port setting during management server installation, in the Agent Port box, type a
784 port number that matches.
- 785 7. (Optional) In the *Management Server Configuration* panel, in the Alternate Management Servers
786 box, type the fully qualified host name or IP address of the alternate servers that are used for
787 failover for this agent. Type the servers in a comma-separated list.
- 788 8. In the *Management Server Configuration* panel, accept the directory for the SSL certificate *Agent-*
789 *cert.ssl*, or click *Browse* to browse to and locate *Agent-cert.ssl*. Access to a copy of the SSL certificate
790 *Agent-cert.ssl* is required to connect to the management server. All primary and alternate
791 management servers must use the same certificate.
- 792 9. In the Management Server Configuration panel, click *Next*.
- 793 10. (Optional) In the *Agent Group Configuration* panel, in the group boxes, type the group names that
794 you created with the Java console. You may add multiple detection policy group names separated
795 with commas. You may include the name of an existing detection policy domain in the group
796 path/name.
- 797 11. In the *Agent Group Configuration* panel, click *Next*.
- 798 12. In the *Service User Configuration* panel, accept the default Local System account, and then click
799 *Next*.
- 800 13. In the *Ready to Install the Program* panel, confirm the installation parameters, and then click *Install*.
- 801 14. When the installation completes, click *Finish*.

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

- 807 ▪ Enabling the intrusion prevention feature
- 808 ▪ Enabling the real-time file integrity monitoring feature in intrusion detection
- 809 ▪ Enabling the real-time file integrity monitoring feature in intrusion detection
- 810 ▪ Creating agent registration groups.

811 See the Symantec Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 MP1 Planning and
812 Deployment Guide for details: 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.

814 2.4.2 Symantec Endpoint Protection Manager

815 **Minimum Hardware Requirement:** 2 GB RAM as minimum; 8 GB or more available recommended. Hard
816 drive should be 40 GB as minimum (200 GB recommended) for the management server and database
817 with a remote SQL Server database.

818 **Minimum Software Requirement:** Windows Installer 2.0 or higher, Microsoft SQL Server 2008, .NET
819 Framework 4.0 or 4.5.1, PowerShell 2.0, and Windows 2008 Server or later. Intel Pentium Dual-Core or
820 equivalent minimum, 8-core or greater is recommended.

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

824 **2.4.2.1 Installing Symantec Endpoint Manager**

- 825 1. Download the product, extract the entire installation file to a physical disk, such as a hard disk. Run
826 *Setup.exe*. The installation should start automatically.
- 827 2. Follow the screen instruction and accept the license agreement.
- 828 3. Continue the installation until it is finished. After the initial installation completes, configure the
829 server and database.
- 830 4. Click *Next*. The Management Server Configuration Wizard starts.
- 831 5. Select *Default Configuration*, and then click *Next*.
- 832 6. Enter company name, a password for the default administrator admin, and an email address.
- 833 7. If you run *LiveUpdate* as part of a new installation, content is more readily available for the clients
834 you deploy.
- 835 8. If you want Symantec to receive anonymous data, click *Next* to begin the database creation.
- 836 9. When the database creation completes, click *Finish* to complete the Symantec Endpoint Protection
837 Manager configuration.

838 **2.4.2.2 Installing the Client**

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

- 844 1. Make your configuration selections as you install the Symantec Endpoint Protection Manager and
845 then create the client installation packages.
- 846 2. Save the installation package to a folder on the computer that runs Symantec Endpoint Protection
847 Manager.
- 848 3. Copy this package to a client machine where you have an administrator privilege.
- 849 4. The installation package comprises one *setup.exe* file. Click the executable file to start the
850 installation. Follow the wizards to complete the installation.

851 **2.4.3 Symantec Advanced Threat Protection: Advanced Threat Protection: 852 Network**

853 With Advanced Threat Protection: Network (ATP:N) installed on the network, it can provide Network-
854 based protection of medical device subnets via monitor internal inbound and outbound internet traffic.

855 We integrate Symantec Advanced Threat Protection (ATP) with Symantec Endpoint Protection, it will
856 allow ATP to monitor and manage all network traffic from the endpoints and provide threat assessment
857 for dangerous activity to secure the medical devices on an enterprise network.

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

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

862 *2.4.3.1 ATP-N Installation*

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

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

874 *2.4.3.2 Integrating APT with Symantec Endpoint Protection*

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

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

889 More detail about integrating ATP and Symantec Endpoint Protection can be found from the following
890 reference: http://help.symantec.com/cs/ATP_2.2/ATP/v102658999_v117970559/About-integrating-ATP-with-Symantec-Endpoint-Protection?locale=EN_US.
891

892 2.5 Risk Assessment Tools

893 2.5.1 Clearwater IRM|Analysis™ Software

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

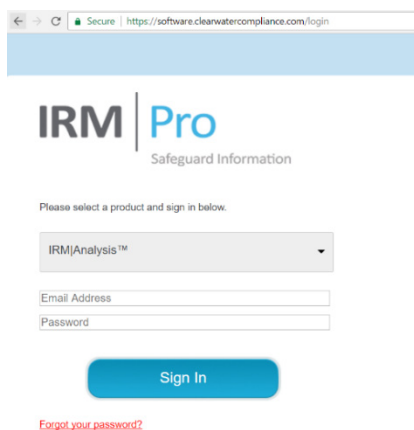
901 This section does not show you how to conduct a risk assessment. Instead, we present some basic steps
 902 for using the IRM|Analysis™ tool to conduct the risk assessment:

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

912 2.5.1.1 Login to IRM|Analysis™

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

916 **Figure 2-3: IRM|Analysis™ Login Page**



917

918 **2.5.1.2 Enter Asset Inventory**

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

926 To add a new asset:

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

932 **Figure 2-4: Asset Inventory List**

933

Id	Asset name	Asset description	# records	Owner	Created	Modified	
75126	InfusionPumpSystem_1 Model 1	Wireless IV medical infusion pump system - 1, Model 1 (wire or wireless)	0		2016-12-20 13:11	2017-02-01 11:25	<input type="checkbox"/>
75127	InfusionPumpSystem_1 Model 3	Wireless IV infusion pump system -3	0		2016-12-20 13:16	2017-01-20 09:26	<input type="checkbox"/>
75191	InfusionPumpSystem_1 Model 2	Wireless IV medical infusion pump system - 1, Model 2 (wireless only)	0		2016-12-20 14:01	2017-01-20 09:27	<input type="checkbox"/>
78382	Workstation Applications	Workstations associated with configuring or controlling a wireless IV medical infusion pump	0		2017-01-19 08:03	2017-01-20 09:10	<input type="checkbox"/>
78383	InfusionPump_2-1	Wireless IV medical infusion pump system - 2, Model 1 (wireless)	0		2017-01-19 09:23	2017-01-20 09:26	<input type="checkbox"/>
78384	InfusionPump_2-2	Wireless IV medical infusion pump system - 2, Model 2 (wireless)	0		2017-01-19 09:24	2017-01-20 09:28	<input type="checkbox"/>
78385	InfusionPump_3	Wireless IV medical infusion pump system - 3, Model 1 (wireless only)	0		2017-01-19 09:26	2017-01-20 09:28	<input type="checkbox"/>

934 **Figure 2-5: New Asset**

The screenshot displays the 'New Asset' page in the IRM Pro application. The interface is divided into several sections:

- Header:** Shows the application name 'IRM Pro' and the user's role 'National Cybersecurity Center of Excellence (NCCoE)'.
- Left Sidebar:** A navigation menu with options like Dashboard, Framing/Governance, Assets, Asset Inventory List, Asset Inventory Import, Media/Asset Groups, Risk Determination, Risk Response, Documents, Reports, Manage Account, and Support.
- Asset Form:**
 - Asset name:** A required text input field.
 - Asset description:** A text input field.
 - Select all items that create, receive, store, transmit or view sensitive information:** A list of checkboxes for various device and service categories:
 - Devices:** Backup Media, Desktop, Desktop or Laptop, Digital Camera, Disk Array, Electronic Medical Device, Laptop, Pager, Scanners, Printers or Copiers, Server, Smartphone, Storage Area Network, Tablet, USB key or flash drive.
 - Third Parties:** Contractors / Consultants, Platform-as-a-Service, Software-as-a-Service.
- Asset Details:** A series of input fields and a dropdown menu:
 - Source of the sensitive information
 - Where or to whom the data is shared or sent
 - Physical Location of Asset
 - Number of end users and administrators
 - Importance of asset (dropdown menu)
 - Approximate # of sensitive records stored on this asset
- Asset Business Owner:** Fields for First name and Last name.
- Footer:** A red asterisk note: '* Indicates a required field'.

935

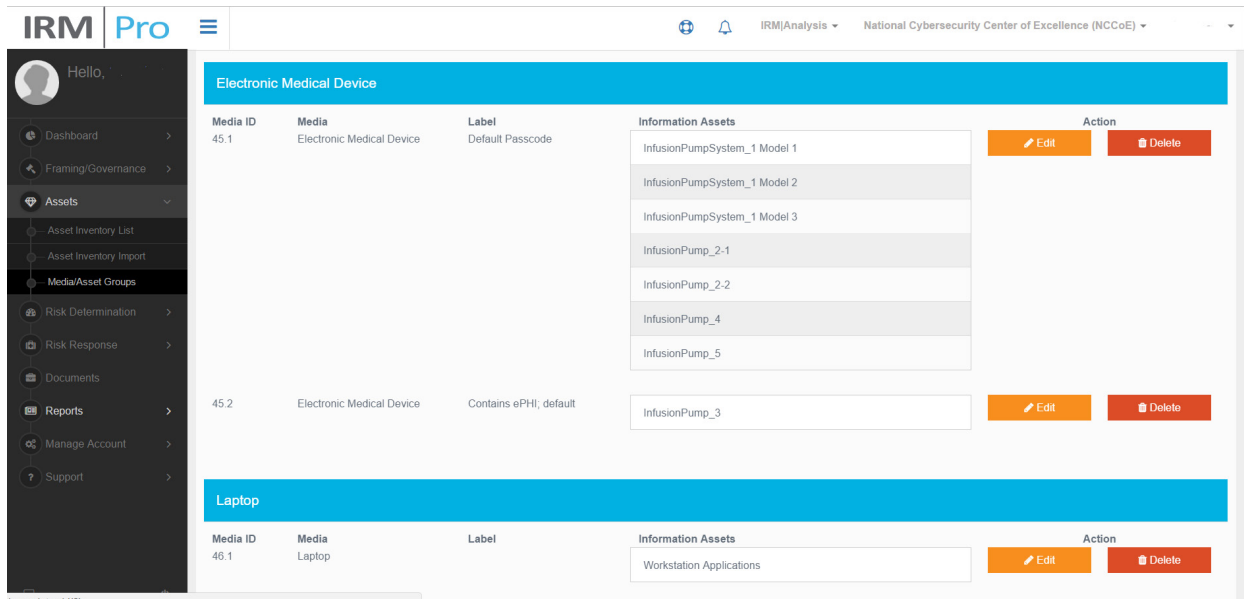
936 To update an asset:

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

943 To view and manage media/asset groups:

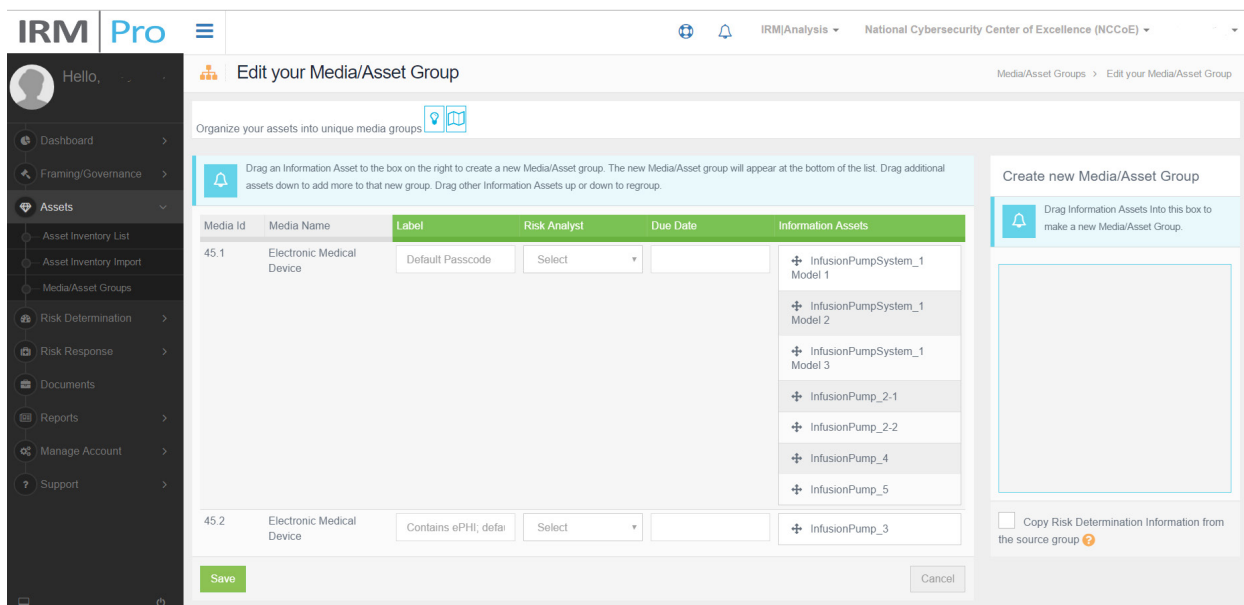
- 944 1. On the IRM|Analysis™ tool, expand *Assets* on the left menu bar.
- 945 2. Under *Assets*, click on *Media/Asset Groups*.
- 946 3. On the *Media/Asset Groups* (see [Figure 2-6](#)), scroll up and down to view the groups and select a
- 947 group by clicking on the *Edit* button.
- 948 4. On the *Edit Media/Asset Groups page* (see [Figure 2-7](#)), enter the necessary information and click on
- 949 the *Save* button.

950 **Figure 2-6: Media/Asset Groups**



951

952 **Figure 2-7: Edit Media/Asset Group**



953

954 **2.5.1.3 Risk Determination**

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

958 To use the Risk Determination at Global/Media level:

- 959 1. On the IRM|Analysis™ tool, expand *Risk Determination* on the left menu bar.
- 960 2. Under Risk Determination, click on Controls – Global/Media.

- 961 3. On the *Controls – Global/Media* page (see [Figure 2-8](#)), scroll up and down to view the controls. For
 962 each control, select one of the responses (i.e., Yes, In Progress, No, and N/A) to indicate the
 963 response status.

964 **Figure 2-8: Controls - Global/Media**

Control	100%	Select One Response	Clear	0	0
Control	+	Yes In Progress No N/A			
Testing of Password Strengths	+	Yes In Progress No N/A		0	0
Training for the Security Workforce	+	Yes In Progress No N/A		1	0
Two-man Rule	+	Yes In Progress No N/A		0	0
Uninterruptible power supply (UPS)	+	Yes In Progress No N/A		0	0
User Account Management	+	Yes In Progress No N/A		0	0
User Activity Review	+	Yes In Progress No N/A		0	0
User Permissions Reviews	+	Yes In Progress No N/A		0	0
Visitor Access Control	+	Yes In Progress No N/A		1	0
Wipe, Erase, or Destroy Disks (Hard Drives, etc.)	+	Yes In Progress No N/A		0	0
Wireless access restrictions	+	Yes In Progress No N/A		1	0
Wireless Encryption	+	Yes In Progress No N/A		0	0
Wireless Link Protection	+	Yes In Progress No N/A		0	0
Wireless Security Policy and Procedures	+	Yes In Progress No N/A		1	0

965

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

- 967 1. On the IRM|Analysis™ tool, expand *Risk Determination* on the left menu bar.
- 968 2. Under Risk Determination, click on Risk Questionnaire List.
- 969 3. On the *Risk Questionnaire List* page (see [Figure 2-9](#)), scroll up and down to view the media/asset
 970 groups.
- 971 4. For each relevant media/asset group, select the *Risk Analyst*, fill in the *Due Date* and click on the
 972 *Continue* button to get in the Risk Questionnaire Form (see [Figure 2-10](#) – part 1 and [Figure 2-11](#) –
 973 part 2).
- 974 5. For each control, select one of the responses (i.e., *Yes*, *In Progress*, *No*, and *N/A*) to indicate the
 975 response status (example shown in part 1), if it was already noted on the Controls Global/Media
 976 page.
- 977 6. Controls can be set globally or for individual Media/Asset Groups. The plus sign will expand the
 978 control to reveal the Media/Asset Groups so the control can be set individually. To illustrate, a
 979 global control can be set for Training for the Security Workforce but an individual control would be
 980 set for each of the Media/Asset groups associated with the User Activity Review since only a subset
 981 of assets may undergo a User Activity Review.
- 982 7. Then determine and select the Risk Likelihood and Risk Impact for the selected risk scenario
 983 (example shown in part 2) to populate the Risk Rating.
- 984 8. You may select the question mark for more information on the control and the NIST symbol for a
 985 quick reference to NIST SP800-53.

986 Figure 2-9: Risk Questionnaire List

IRM Pro

Risk Questionnaire List

Click Continue to complete the Risk Questionnaire Form for a risk or click Review to see the completed form

100.0%	Media/Label	Information Assets	Total Sensitive Records	Risk Analyst	Due Date	Action
100.0%	Electronic Medical Device / Default Passcode	InfusionPumpSystem_1 Model 1, InfusionPumpSystem_1 Model 2, InfusionPumpSystem_1 Model 3, InfusionPump_2-1, InfusionPump_2-2, InfusionPump_4, InfusionPump_5	0	Select		Review
100.0%	Electronic Medical Device / Contains ePHI; default	InfusionPump_3	0	Select		Review

987
988 Figure 2-10: Risk Questionnaire Form (part 1)

IRM Pro

Risk Questionnaire Form

Media/Asset Group and Threat/Vulnerability

For this media selection you will respond to the questions below for this threat and vulnerability.

Media/Label	Information Assets	Threat Source	Threat Event	Vulnerability	
100.0%	Electronic Medical Device / Contains ePHI; default	InfusionPump_3	Burglar/Theft	Theft of Equipment	Physical Security Vulnerabilities

Applicable Controls for the Threat/Vulnerability for the Media/Asset(s) Listed Above

Is the organization actively maintaining and enforcing the controls listed below that would prevent this threat from exploiting this vulnerability?

Control	NIST SP 800-53 Requirement	Response
Controlled access to areas with mobile devices	PE-1 a, PE-1 b, PE-2 a, PE-2 b, PE-2 c, PE-3 a, PE-3 b, PE-3 c, PE-3 d, PE-3 e, PE-3 f, PE-3 g NIST	Yes In Progress No N/A
Inventory Control Process	MA-2 a, MA-2 b, MA-2 c, MA-2 CE1, MA-2 CE2, MA-2 d, MA-2 e NIST	Yes In Progress No N/A
Physical Access Monitoring	PE-6 a, PE-6 b, PE-6 c NIST	Yes In Progress No N/A
Physical Security Policy and Procedures	PE-1 a, PE-1 b NIST	Yes In Progress No N/A
Physically Securing Devices or Systems When Not in Use	PE-1 a, PE-1 b, PE-2 a, PE-2 b, PE-2 c, PE-3 a, PE-3 b, PE-3 c, PE-3 d, PE-3 e, PE-3 f, PE-3 g NIST	Yes In Progress No N/A
Security/privacy Awareness and Training	AT-1 a, AT-1 b, AT-2, AT-3, AT-4 a, AT-4 b NIST	Yes In Progress No N/A

990 Figure 2-11: Risk Questionnaire Form (part 2)

The screenshot displays the IRM|Pro Risk Questionnaire Form. The top navigation bar includes the IRM|Pro logo, a user profile icon, and the text 'National Cybersecurity Center of Excellence (NCCoE)'. A sidebar on the left contains a menu with items like Dashboard, Framing/Governance, Assets, Risk Determination, Risk Questionnaire List, Risk Response, Documents, Reports, and Manage Account. The main content area shows a list of controls with columns for control name, NIST reference, status (Yes, In Progress, No, N/A), and action icons. Below the list is a section for 'Risk Rating for this Threat/Vulnerability for the Media/Asset(s) Listed Above', which includes a table with 'Risk Likelihood' and 'Risk Impact' rows, each with a description and a dropdown menu for 'Risk Rating'. The 'Risk Rating' dropdown is currently set to 'Moderate' and shows a score of 3. At the bottom, there are buttons for 'Return to Risk Questionnaire List' and 'Go to the next Threat/Vulnerability for this Media'.

991

992

2.5.1.4 Risk Response

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

995 Consider following these risk response steps:

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

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

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

1000 4. On the *Risk Response List* page (see [Figure 2-12](#)), scroll up and down to view the Media/Asset
 1001 Groups along with the associated threat source, vulnerability, and risk rating.

1002 5. For each relevant risk response, click on the button under the Treatment column to enter the *Risk
 1003 Treat and Evaluate Form* page of that risk (see [Figure 2-13](#)).

1004 6. On the *Risk Treat and Evaluate Form* page, perform the risk response analysis by selecting the risk
 1005 treatment type; evaluate the control or recommendation; select risk owner; put risk notes, and so
 1006 on.

1007 **Figure 2-12: Risk Response List - Risk Registry**

0%	Media/Label	Asset Name(s)	Threat Source/Event	Vulnerability	Risk Rating	Residual Rating	Treatment	Evaluation
0%	Electronic Medical Device / Default Passcode	InfusionPumpSystem_1 Model 1, InfusionPumpSystem_1 Model 2, InfusionPumpSystem_1 Model 3, InfusionPump_2-1, InfusionPump_2-2, InfusionPump_4, InfusionPump_5	Careless IT Personnel/Insecure User Management	Vulnerabilities in Password Creation and Distribution	25	-	TBD	TBD
0%	Electronic Medical Device / Contains ePHI, default	InfusionPump_3	Careless IT Personnel/Insecure User Management	Vulnerabilities in Password Creation and Distribution	25	-	TBD	TBD
0%	Electronic Medical Device / Default Passcode	InfusionPumpSystem_1 Model 1, InfusionPumpSystem_1 Model 2, InfusionPumpSystem_1 Model 3, InfusionPump_2-1, InfusionPump_2-2, InfusionPump_4, InfusionPump_5	Careless IT Personnel/Insecure User Management	Weak Passwords	25	-	TBD	TBD
0%	Electronic Medical Device / Contains ePHI, default	InfusionPump_3	Careless IT Personnel/Insecure User Management	Weak Passwords	25	-	TBD	TBD
0%	Electronic Medical Device / Default Passcode	InfusionPumpSystem_1 Model 1, InfusionPumpSystem_1 Model 2, InfusionPumpSystem_1 Model 3, InfusionPump_2-1, InfusionPump_2-2, InfusionPump_4, InfusionPump_5	Careless IT Personnel/Insecure Configuration of Systems	Vulnerabilities in System Configurations	25	-	TBD	TBD
0%	Electronic Medical Device / Contains ePHI, default	InfusionPump_3	Careless IT Personnel/Insecure Configuration of Systems	Vulnerabilities in System Configurations	25	-	TBD	TBD
0%	Electronic Medical Device / Default Passcode	InfusionPumpSystem_1 Model 1, InfusionPumpSystem_1 Model 2, InfusionPumpSystem_1 Model 3, InfusionPump_2-1, InfusionPump_2-2, InfusionPump_4, InfusionPump_5	Careless User/Weak Passwords	Weak Passwords	25	-	TBD	TBD

1008

1009 **Figure 2-13: Risk Treat and Evaluate Form**

Select Risk Treatment, Alternatives, Residual Risk and Status

Risk Analysis Findings

Media/Label	Information Assets	Threat Source	Threat Event	Vulnerability	Risk Rating
Electronic Medical Device / Contains ePHI, default	InfusionPump_3	Careless IT Personnel	Improper Destruction, Disposal or Reuse of Media	Destruction/Disposal Vulnerabilities	16

Evaluate alternatives that would prevent this threat from exploiting the vulnerabilities listed above

Control or Recommendation	Control Response	Effectiveness *	Estimated Cost	Feasibility *	Global	Action *
57% Device Re-use and Disposal Policy and Procedures	NIST	No	Highly Effective	\$ 0	Highly Feasible	Enhance
100% Security/privacy Awareness and Training	NIST	No	Select	\$ 0	Select	Not applicable
0% Training for the Security Workforce	NIST	No	Select	\$ 0	Select	Select

Select a Risk Owner

Risk Notes

Select the Residual Risk

Select a Status

Risk Threshold: 15

Risk Likelihood: Likelihood

Risk Impact: Impact

Approved:

1010

1011 **2.5.1.5 Dashboard and Report**

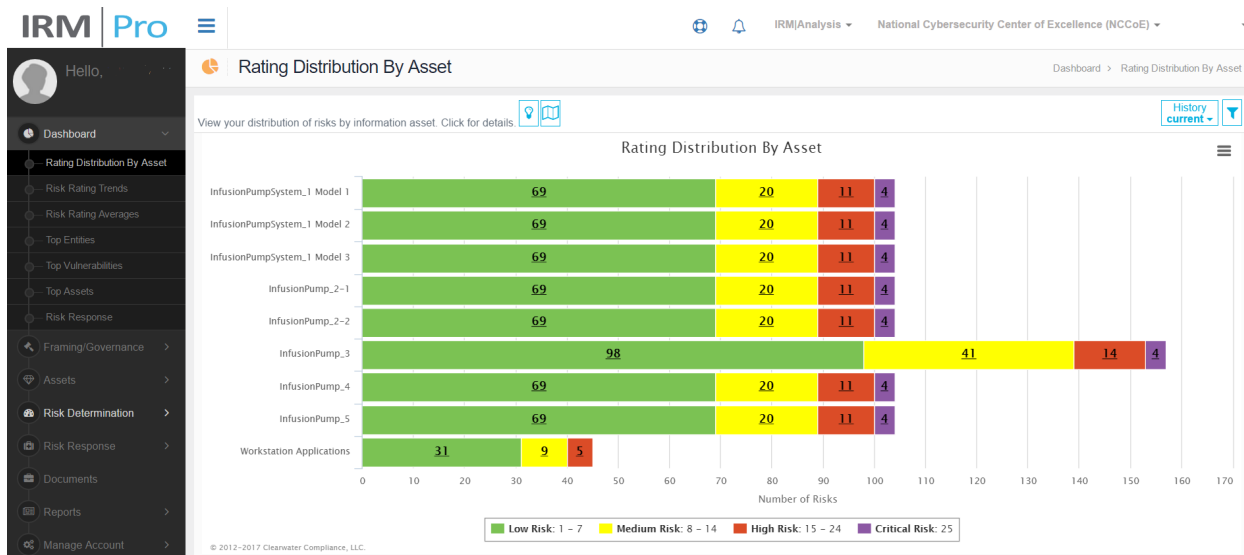
1012 The IRM|Analysis™ tool enables users to review their risk analyses with a dashboard or report format.
 1013 To access the dashboard views, follow these steps:

- 1014 1. On the IRM|Analysis™ tool, expand *Dashboard* on the left menu bar
- 1015 2. Under Dashboard, click on Rating Distribution by Asset

1016 3. Example Dashboard: Rating Distribution by Asset page (see [Figure 2-14](#) below)

1017 You can also view other types of dashboards, such as *Risk Rating Trends* and *Risk Rating Averages*.

1018 **Figure 2-14: Dashboard Example**



1019

1020

1021 For report views, follow these steps:

1022 1. On the IRM|Analysis™ tool, expand *Reports* on the left menu bar

1023 2. Under Reports, click on Risk Rating Report

1024 3. Example Report: *Risk Rating Report* page is showing (see [Figure 2-15](#) below)

1025 You can also view other types of dashboards, such as *Risk Rating Trends* and *Risk Rating Averages*.

1026 Figure 2-15: Report Example

Media / Label	Asset Name(s)	Threat Source/Event	Vulnerability	Likelihood	Impact	Rating
Electronic Medical Device / Contains ePHI; default	InfusionPump_3	Malware / Theft of Sensitive Data	Anti-malware Vulnerabilities	3	3	9
Laptop	Workstation Applications	Malware / Theft of Sensitive Data	Anti-malware Vulnerabilities	1	3	3
Laptop / Vendor Supplied	InfusionPump_3	Malware / Theft of Sensitive Data	Anti-malware Vulnerabilities	1	3	3
Server	InfusionPumpSystem_1 Model 1, InfusionPumpSystem_1 Model 2, InfusionPumpSystem_1 Model 3, InfusionPump_2-1, InfusionPump_2-2, InfusionPump_3, InfusionPump_4, InfusionPump_5	Malware / Theft of Sensitive Data	Anti-malware Vulnerabilities	1	3	3
Disk Array	InfusionPumpSystem_1 Model 1, InfusionPumpSystem_1 Model 2, InfusionPumpSystem_1 Model 3, InfusionPump_2-1, InfusionPump_2-2, InfusionPump_3, InfusionPump_4, InfusionPump_5	Careless User / Information Leakage	Destruction/Disposal Vulnerabilities	3	5	16
Disk Array	InfusionPumpSystem_1 Model 1, InfusionPumpSystem_1 Model 2, InfusionPumpSystem_1 Model 3, InfusionPump_2-1, InfusionPump_2-2, InfusionPump_3, InfusionPump_4, InfusionPump_5	Careless IT Personnel / Improper Destruction, Disposal or Reuse of Media	Destruction/Disposal Vulnerabilities	4	5	20
Electronic Medical Device / Contains ePHI; default	InfusionPump_3	Careless User / Information Leakage	Destruction/Disposal Vulnerabilities	2	4	8
Electronic Medical Device / Contains ePHI; default	InfusionPump_3	Careless IT Personnel / Improper Destruction, Disposal or Reuse of Media	Destruction/Disposal Vulnerabilities	4	4	16
Laptop	Workstation Applications	Careless User / Information Leakage	Destruction/Disposal Vulnerabilities	1	5	5

1027

1028

2.5.2 MDISS MDRAP

1029 We used MDISS's cloud-based Medical Device Risk Assessment Platform (MDRAP), a questionnaire-
 1030 based risk assessment tool to conduct the assessment on the medical devices. In our environment, we
 1031 set up and configured wireless infusion pump systems from five manufactures and built the enterprise
 1032 network to simulate a typical HDO environment.

1033 Please note, this section does not show you how to conduct a risk assessment. Instead, we show these
 1034 basic steps for using the MDRAP tool:

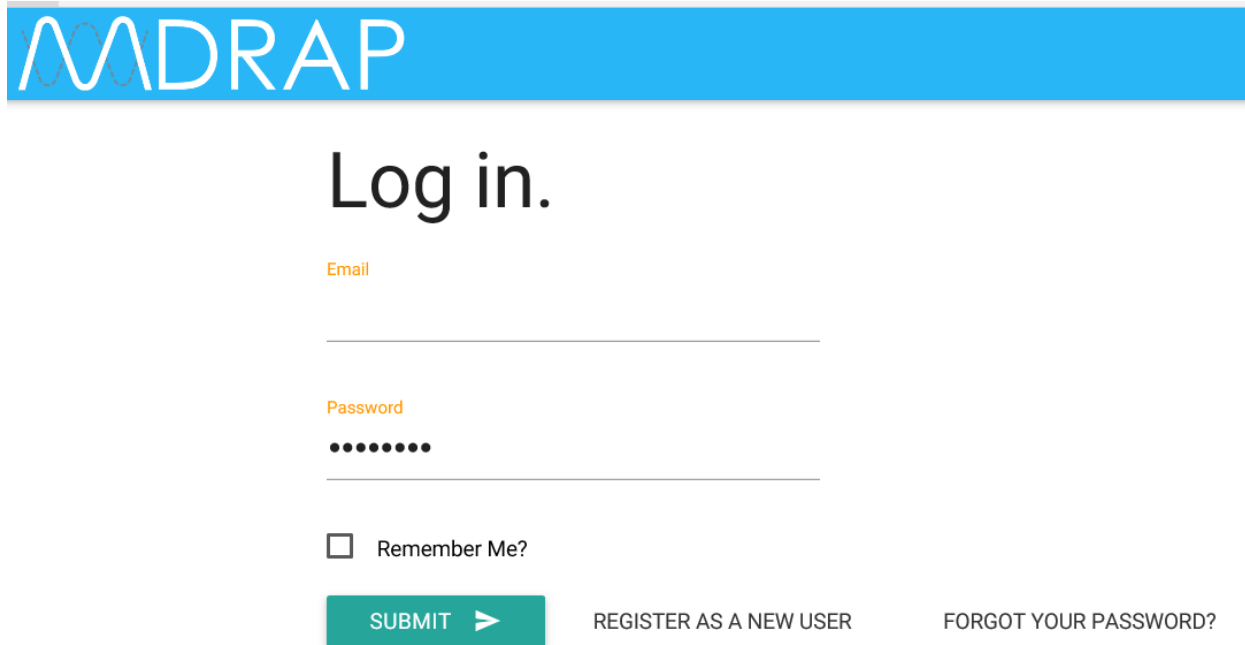
- 1035 ▪ Login to MDRAP
- 1036 ▪ Conduct Device Inventory
- 1037 ▪ Risk Assessment
- 1038 ▪ Dashboard and Reports.

1039

2.5.2.1 Login to MDRAP

- 1040 1. Within a browser, type <https://mdrap.mdiss.org/> and click on *Log In*
- 1041 2. On the Login page (see [Figure 2-16](#)), enter the appropriate email and password
- 1042 3. Click on *Submit*.

1043 Figure 2-16: MDRAP Login Page



MDRAP

Log in.

Email

Password

●●●●●●

Remember Me?

[SUBMIT >](#) [REGISTER AS A NEW USER](#) [FORGOT YOUR PASSWORD?](#)

1044

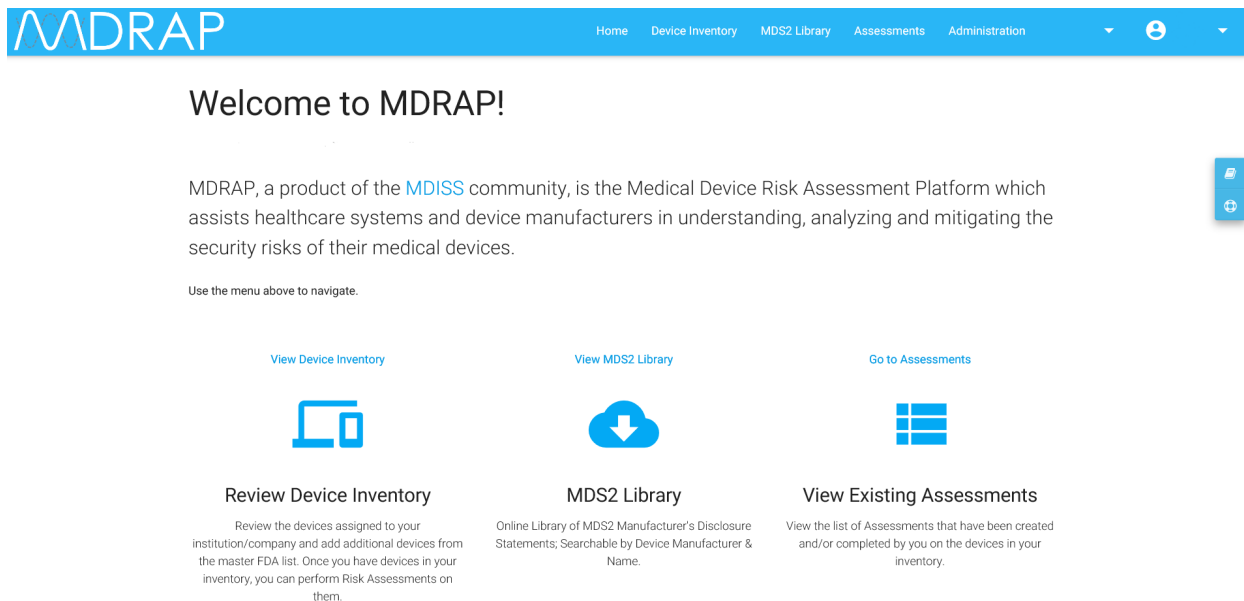
1045

2.5.2.2 Conduct Device Inventory

1046 We use the Device Inventory module of MDRAP to keep track all the infusion pumps and servers in our
1047 sample implementation. Add Device, per its name, enables us to add individual devices, while Bulk
1048 Import enables us to add a group of devices. Steps for using both methods follow.

- 1049 1. On the Welcome to MDRAP page (see [Figure 2-17](#)), click on Device Inventory on the menu bar or
1050 on the View Device Inventory link on the page.
- 1051 2. On the Device Inventory page ([Figure 2-18](#)), add an individual device, or edit a device, or bulk import
1052 a group of devices.

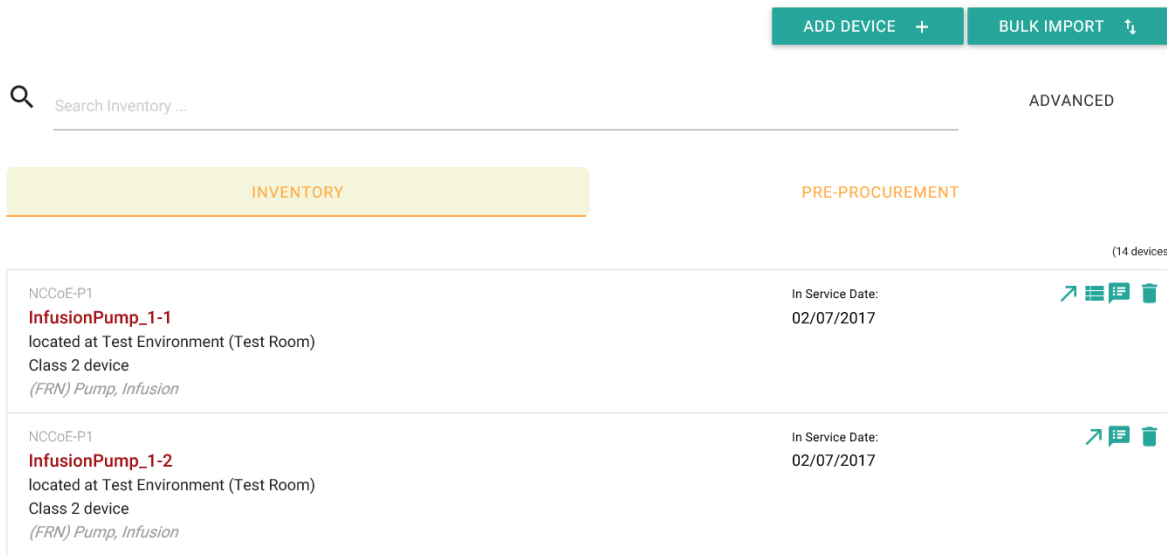
1053 **Figure 2-17: MDRAP Welcome page**



1054
1055 **Figure 2-18: Device Inventory List**

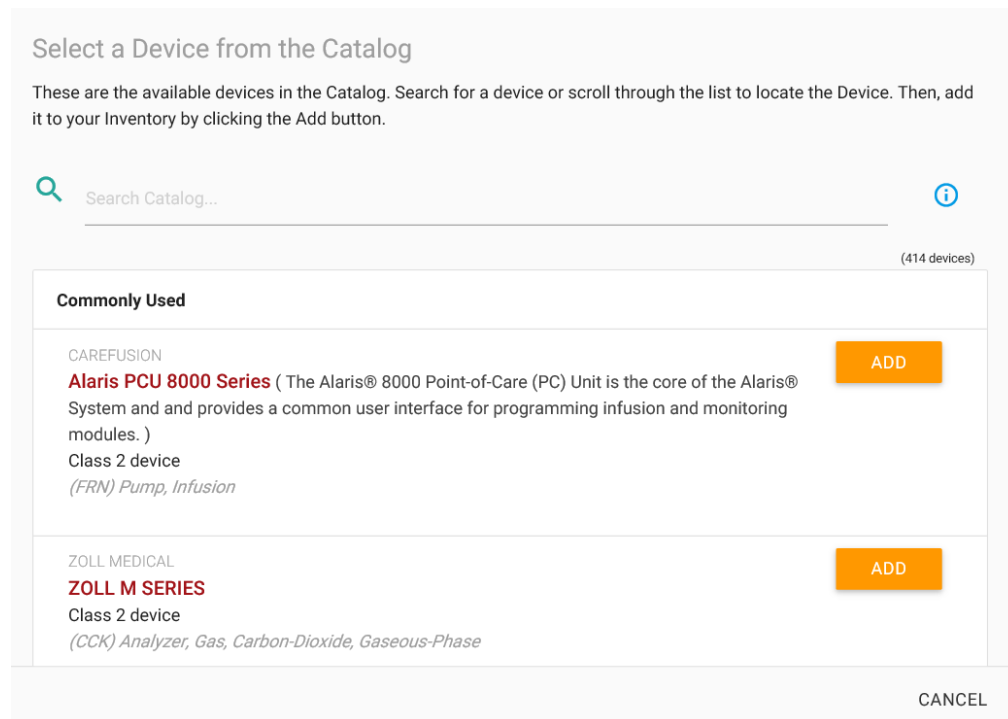
Device Inventory

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



1056
1057 **Add device:**

- 1058 **1.** On the Device Inventory page (see [Figure 2-18](#) above), click on ADD DEVICE.
- 1059 **2.** On Add Device page (see [Figure 2-19](#) below), locate the device from the Category List, then click on
- 1060 **ADD.**

1061 **Figure 2-19: Add Device**

1062

1063 Edit a device:

- 1064 1. On the Device Inventory page (see [Figure 2-18](#) above), locate the device from the list, click on the
- 1065 product name link or the Edit icon.
- 1066 2. On the Edit Inventory page (see [Figure 2-20](#) below), update the data and click on Save.

1067 **Figure 2-20: Edit Device**

1068

1069

1069 Bulk Import a group of devices:

- 1070 1. On the Device Inventory page (see [Figure 2-18: Device Inventory List](#) above), click on BULK IMPORT
- 1071 button.
- 1072 2. On Inventory Bulk Import page (see [Figure 2-21](#) below), download the template, fill-in the data into
- 1073 the template.
- 1074 3. Follow the instruction to upload and import the devices by using the template (see [Figure 2-22](#)).

1075

1076 **Figure 2-21: Inventory Bulk Import**

Inventory Bulk Import

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

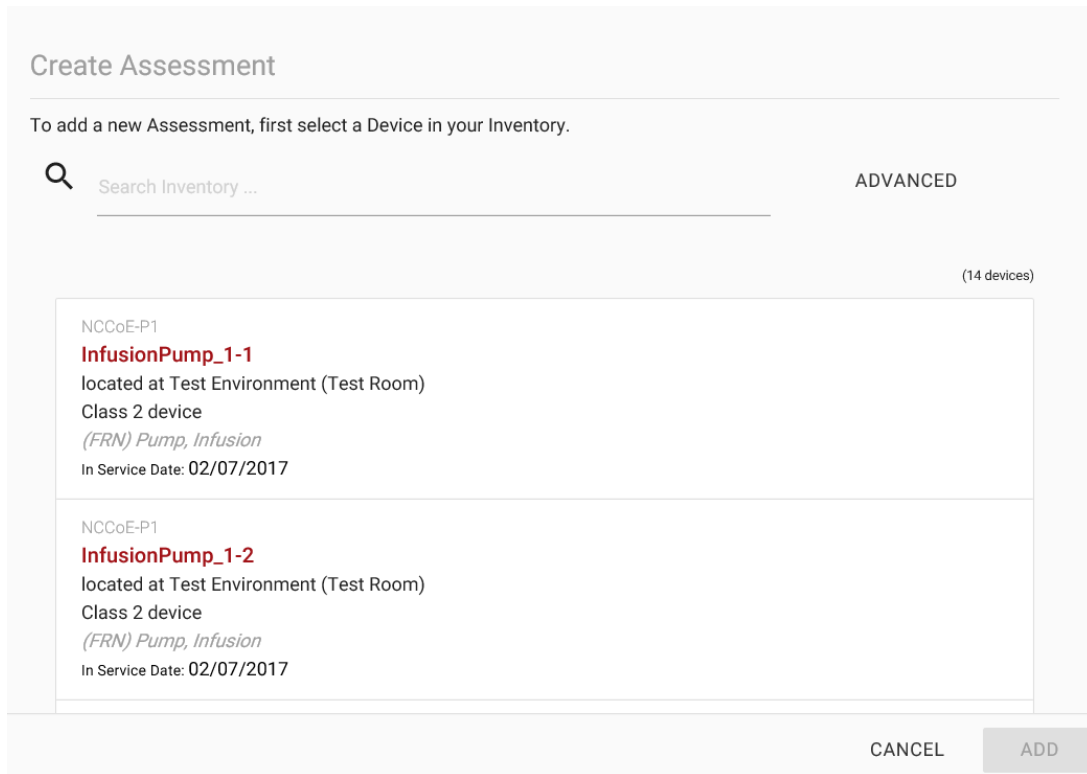
Once you have completed adding your inventory, send your file to MDRAP customer support at support@mdrap.zendesk.com for the upload. We will contact you once the inventory is loaded into MDRAP.

DOWNLOAD TEMPLATE 

[VIEW EXISTING IMPORTS](#)

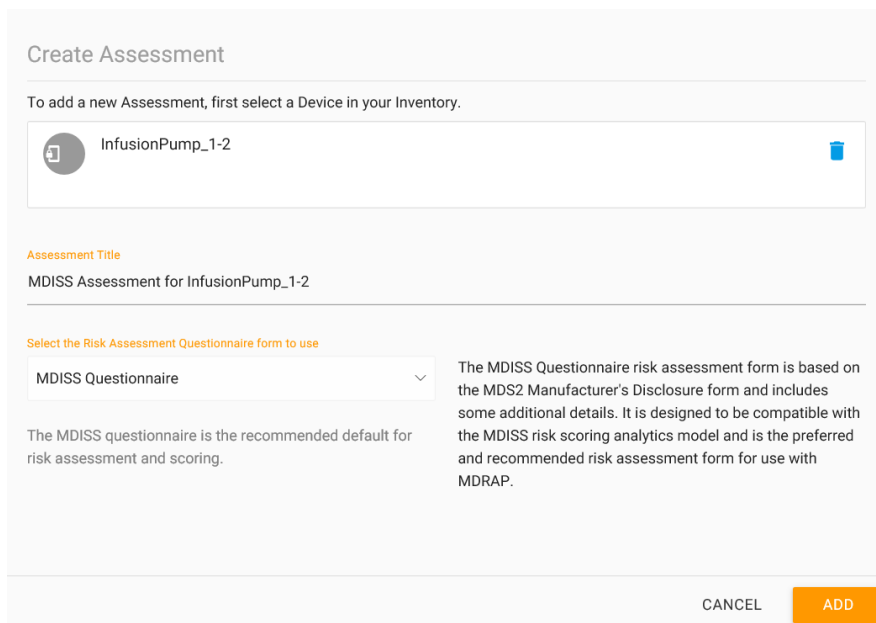
1077

1091 **Figure 2-23: Create Assessment (part 1)**



1092

1093 **Figure 2-24: Create Assessment (part 2)**



1094

1095 **Figure 2-25: Assessment Step (example 1)**

MDISS Assessment for InfusionPump_1-2 (MDISS) 0.0 % completed
Assessment last updated on 04/07/2017 19:04:47

NCCOE-P1
InfusionPump_1-2

Back to Assessment Summary

0.0%

Management of Private Data #1/4

Can this device store, display, transmit or maintain Private Data (including electronic Protected Health Information (ePHI))? A.01

Yes
 No

[Add Comment](#)

< PREVIOUS

NEXT >

1096

1097 **Figure 2-26: Assessment Step (example 2)**

MDISS Assessment for InfusionPump_1-2 (MDISS) 8.3 % completed
Assessment last updated on 04/07/2017 15:10:09

NCCOE-P1
InfusionPump_1-2

Back to Assessment Summary

8.3%

Other Questions Affecting Exposure #4/8

Does the device or app run behind a subnet (e.g. department) firewall? B.04

Yes
 No

[Add Comment](#)

< PREVIOUS

NEXT >

1098

1099 **2.5.2.4 Dashboard and Reports**

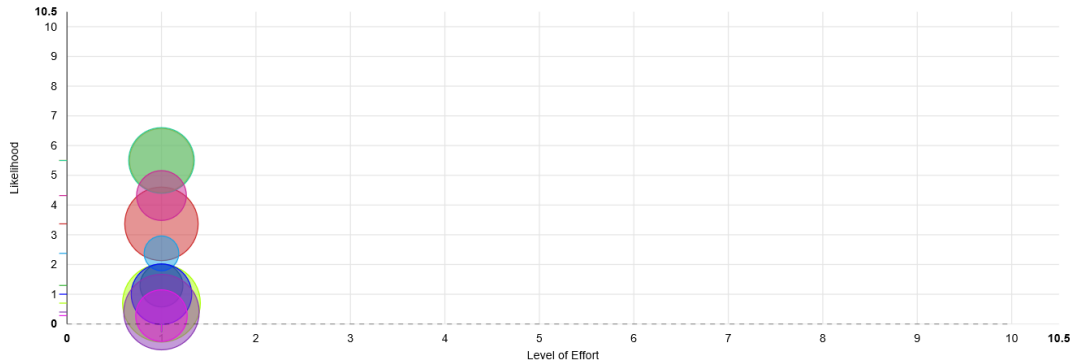
1100 MDRAP computes assessment results based on the responses to the questionnaires. For a given
1101 assessment (complete or partially complete), the assessment result is available for view as a dashboard
1102 (see [Figure 2-27](#)) or report (see [Figure 2-28](#)).

1103 **Figure 2-27: Assessment Result (dashboard example)**

MDISS Assessment for InfusionPump_1-1 MDISS NCCoE-P1 **InfusionPump_1-1** [Back to Assessments List](#)

100.0 % completed
Assessment last updated on 02/10/2017 22:53:25

Risk Scores



1104 **Category** **Level of Effort** **Likelihood** **Risk** **Notes**

1105 **Figure 2-28: 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 encryption 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 allow file-level access controls. * Unnecessary services active.
■ Transmission Confidentiality &	1	0.28	2.118	

1106

Appendix A Baseline Configuration File

A.1 Baseline Configuration File

ASA Version 9.6(1)

!

interface Management0/0

ip address 192.168.29.149 255.255.255.0

!

! optional, SSH, version is important as v1 is insecure and on by default, also set your own password!

username cisco password XX

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

DRAFT

```
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
!
```

DRAFT

! 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
```

DRAFT

!

! 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

DRAFT

A.2 External Firewall and Guest Network ASA Configuration File

: Saved

:

: Serial Number: 9AK64JT2D2M

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

:

ASA Version 9.6(1)

!

hostname border-kmcfadde

enable password 8Ry2Yjlyt7RRXU24 encrypted

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

!

license smart

feature tier standard

throughput level 1G

names

!

interface GigabitEthernet0/0

nameif WAN

security-level 0

ip address 10.32.3.10 255.255.255.0

!

DRAFT

```
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
```

!

DRAFT

```
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
```

DRAFT

```
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
```


DRAFT

```
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
```

DRAFT

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 77777772e 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

DRAFT

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

DRAFT

```
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 8.8.8.8 8.8.4.4
dhcpd option 3 ip 192.168.170.1
!
dhcpd address 192.168.170.220-192.168.170.250 GUEST
dhcpd enable GUEST
!
dynamic-access-policy-record DfltAccessPolicy
username cisco password YBYvHe595IIMVg7Y encrypted
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
```

DRAFT

```
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
```

DRAFT

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 8Ry2Yjlyt7RRXU24 encrypted

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

!

license smart

feature tier standard

throughput level 1G

names

!

interface GigabitEthernet0/0

nameif WAN

security-level 50

ip address 192.168.100.154 255.255.255.0

ospf authentication-key *****

ospf authentication message-digest

DRAFT

```
!  
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  
!
```

DRAFT

```
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
```


DRAFT

```
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
```

DRAFT

```
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 77777772e 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

DRAFT

```
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

ssh key-exchange group dh-group1-sha1

console timeout 0

dynamic-access-policy-record DfltAccessPolicy

username cisco password YBYvHe595IIMVg7Y encrypted

!

class-map inspection_default

match default-inspection-traffic

!

!

DRAFT

```
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
```

DRAFT

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

DRAFT

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 8Ry2Yjlyt7RRXU24 encrypted

xlate per-session deny tcp any4 any4

xlate per-session deny tcp any4 any6

xlate per-session deny tcp any6 any4

xlate per-session deny tcp any6 any6

xlate per-session deny udp any4 any4 eq domain

xlate per-session deny udp any4 any6 eq domain

xlate per-session deny udp any6 any4 eq domain

xlate per-session deny udp any6 any6 eq domain

!

license smart

feature tier standard

throughput level 1G

names

!

interface GigabitEthernet0/0

nameif WAN

security-level 50

ip address 192.168.100.152 255.255.255.0

ospf authentication-key *****

ospf authentication message-digest

DRAFT

```
!  
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  
!
```


DRAFT

```
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
```

DRAFT

```
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
```

DRAFT

```
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
```

DRAFT

```
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

DRAFT

```
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

ssh key-exchange group dh-group1-sha1

console timeout 0

dhcpd dns 192.168.120.163 192.168.120.162

dhcpd option 3 ip 192.168.140.1

!

dhcpd address 192.168.140.220-192.168.140.250 LAN

dhcpd enable LAN

!

DRAFT

```
dynamic-access-policy-record DfltAccessPolicy
username cisco password YBYvHe595IIMVg7Y encrypted
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns migrated_dns_map_1
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error
```

DRAFT

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

!
interface GigabitEthernet0/0
 nameif WAN
 security-level 50
 ip address 192.168.100.149 255.255.255.0
 ospf authentication-key *****
 ospf authentication message-digest
!
interface GigabitEthernet0/1
 nameif LAN
 security-level 100
 ip address 192.168.150.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
```

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

```
object network PUMPSERVERS
 subnet 192.168.140.0 255.255.255.0
object network PUMPS
 subnet 192.168.150.0 255.255.255.0
object-group icmp-type PING-REPLIES
 icmp-object echo-reply
object-group service PCAPORTS
 service-object tcp destination eq https
 service-object tcp destination eq 11444
 service-object tcp destination eq 11443
 service-object tcp destination eq 8443
object-group icmp-type TRACEROUTE-REPLIES
 icmp-object time-exceeded
 icmp-object unreachable
 group-object PING-REPLIES
object-group icmp-type PING
 icmp-object echo
object-group service TRACEROUTEUDP
 service-object udp destination gt 33434
object-group service PLUM360PORTS
 service-object tcp destination eq 8100
 service-object tcp destination eq 9292
object-group service 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 bcb2597
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
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd dns 192.168.150.1
```

```
dhcpd option 3 ip 192.168.150.1
!
dhcpd address 192.168.150.220-192.168.150.250 LAN
dhcpd enable LAN
!
dynamic-access-policy-record DfltAccessPolicy
username cisco password YBYvHe595IIMVg7Y encrypted
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect 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
```

DRAFT

```
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 5 $1$FraY$.34n8ay7c.l7qwJttjHas0  
enable password 7 023624481811003348  
!  
username admin privilege 15 password 7 04734A125E75606E0B4A  
user-name cisco  
creation-time 1469560730  
privilege 15  
password 7 0523471B701862291B56  
type mgmt-user  
no aaa new-model  
switch 1 provision ws-c3650-48ps  
!  
ip domain-name nist.gov  
ip device tracking  
ip dhcp excluded-address 192.168.250.1 192.168.250.9  
!  
ip dhcp pool WLAN  
network 192.168.250.0 255.255.255.0  
default-router 192.168.250.1  
option 43 hex c0a8.fa02
```



```
!  
!  
vtp mode transparent  
!  
crypto pki trustpoint TP-self-signed-2035642131  
  enrollment selfsigned  
  subject-name cn=IOS-Self-Signed-Certificate-2035642131  
  revocation-check none  
  rsakeypair TP-self-signed-2035642131  
!  
!  
crypto pki certificate chain TP-self-signed-2035642131  
  certificate self-signed 01  
    3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030  
    31312F30 2D060355 04031326 494F532D 53656C66 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 nccoe_healthcare_dev@nist.gov
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
access-class SSH-Access in
exec-timeout 300 0
password 7 022E454F5A5223014E1D
login local
transport input ssh
line vty 5 15
```

DRAFT

```
access-class SSH-Access in
exec-timeout 300 0
password 7 022E454F5A5223014E1D
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
```

DRAFT

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

DRAFT

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 2
Number of Active Clients..... 2

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

Backup Controller Configuration

AP primary Backup Controller
AP secondary Backup Controller

System Time Information:

Time..... Thu Aug 18 20:05:16 2016

Timezone delta..... 0:0

Timezone location.....

NTP Servers

NTP Polling Interval..... 3600

DRAFT

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
Redundancy State..... N/A
Mobility MAC..... 00:50:56:AC:6D:08
Redundancy Management IP Address..... 0.0.0.0
Peer Redundancy Management IP Address..... 0.0.0.0
Redundancy Port IP Address..... 0.0.0.0
Peer Redundancy Port IP Address..... 169.254.0.0

AP Bundle Information

Primary AP Image	Size
ap1g1	12660
ap1g2	11748
ap1g3	13672
ap1g4	19256
ap3g1	9736
ap3g2	13480
ap3g3	18696
ap801	8064
ap802	9536

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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	

DRAFT

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

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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>

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

Interference..... 10 %
Noise..... -70 dBm
Utilization..... 80 %
Multicast Data Rate..... 0
Rx Snp 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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

Group VLAN Name to Id Mappings

Template in Modified State - apply it to see mappings

AP-Specific FlexConnect Policy ACLs :

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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)

DRAFT

.....

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

DRAFT

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

DRAFT

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:

DRAFT

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

CAC SIP-Voice configuration

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

Video AC:

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

CAC SIP-Video Configuration

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

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

802.11a Advanced Configuration

Member RRM Information

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)

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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:

Mask:255.255.255.0
inet addr:192.168.29.146 Bcast:192.168.29.255
inet6 addr: fe80::250:56ff:feac:6338/64 Scope:Link

DRAFT

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

DRAFT

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

DRAFT

mDNS Profile Name..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Disabled
Tunnel Profile..... Unconfigured
Quality of Service..... Silver
Per-SSID Rate Limits..... Upstream Downstream
Average Data Rate..... 0 0
Average Realtime Data Rate..... 0 0
Burst Data Rate..... 0 0
Burst Realtime Data Rate..... 0 0
Per-Client Rate Limits..... Upstream Downstream
Average Data Rate..... 0 0
Average Realtime Data Rate..... 0 0
Burst Data Rate..... 0 0
Burst Realtime Data Rate..... 0 0
Scan Defer Priority..... 4,5,6
Scan Defer Time..... 100 milliseconds
WMM..... Allowed
WMM UAPSD Compliant Client Support..... Disabled
Media Stream Multicast-direct..... Disabled
CCX - Aironetle Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... 802.1P (Tag=0)
Passive Client Feature..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

WLAN Layer2 ACL..... unconfigured
mDNS Status..... Disabled
mDNS Profile Name..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Static IP client tunneling..... Disabled
Tunnel Profile..... Unconfigured
Quality of Service..... Silver
Per-SSID Rate Limits..... Upstream Downstream
Average Data Rate..... 0 0
Average Realtime Data Rate..... 0 0
Burst Data Rate..... 0 0
Burst Realtime Data Rate..... 0 0
Per-Client Rate Limits..... Upstream Downstream
Average Data Rate..... 0 0
Average Realtime Data Rate..... 0 0
Burst Data Rate..... 0 0
Burst Realtime Data Rate..... 0 0
Scan Defer Priority..... 4,5,6
Scan Defer Time..... 100 milliseconds
WMM..... Allowed
WMM UAPSD Compliant Client Support..... Disabled
Media Stream Multicast-direct..... Disabled
CCX - Aironetle Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... 802.1P (Tag=0)
Passive Client Feature..... Disabled
Peer-to-Peer Blocking Action..... Disabled

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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 436973636f0000000000000000000000

Authority Information Cisco A-ID

Dns Configuration

Radius port.....

Radius secret.....

Dns url.....

Dns timeout.....

Dns Serverip.....

Dns state..... Disable

DRAFT

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

DRAFT

Group Name # Aps

FlexConnect Group Detail

FlexConnect Vlan name Summary

Vlan-Name Id Status

FlexConnect Vlan Name Detail

Route Info

Number of Routes..... 0

DRAFT

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

DRAFT

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

DRAFT

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)

DRAFT

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

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)

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

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

2.4G Band Media-Stream Configuration

Multicast-direct..... Enabled
Best Effort..... Disabled
Video Re-Direct..... Enabled
Max Allowed Streams Per Radio..... Auto
Max Allowed Streams Per Client..... Auto
Max Video Bandwidth..... 0
Max 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

DRAFT

Max Media Bandwidth..... 85
Min PHY Rate..... 6000
Max Retry Percentage..... 80

Number of Clients..... 0

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

WLC Voice Call Statistics

WLC Voice Call Statistics for 802.11b Radio

WMM TSPEC CAC Call Stats

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

SIP CAC Call Stats

DRAFT

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 insufficient bw.... 0
Num of Calls Rejected due to invalid params.... 0

DRAFT

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

DRAFT

RA Throttling allow at-most..... 1
RA Throttling max-through..... 10
RA Throttling throttle-period..... 600
RA Throttling interval-option..... passthrough
NS Multicast CacheMiss Forwarding..... Disabled
NA Multicast 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

SI 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

DRAFT

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

DRAFT

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.

DRAFT

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.

DRAFT

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

DRAFT

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

DRAFT

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

DRAFT

Mesh Multicast Mode..... In-Out

Mesh CAC Mode..... enabled

Mesh Full Sector DFS..... enabled

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

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

Outdoor Ext. UNII B Domain channels(for BH)..... disabled

Mesh Advanced LSC..... disabled

Advanced LSC AP Provisioning disabled

Open Window..... disabled

Provision Controller..... disabled

Mesh Slot Bias..... enabled

Mesh Convergence Method..... standard

Mesh Channel Change Notification..... disabled

Mesh Ethernet Bridging STP BPDU Allowed..... disabled

Mesh RAP downlink backhaul..... 802.11Radio-A (Slot 1)

Appendix B Sample Pump Configuration Parameters

B.1 Example of Pump Configuration File

```
SN=2011304
# Pump serial number - must match SN of receiving pump
# SIGMA Spectrum Settings
[NETWORK CONFIGURATION]
# DHCP=0 DHCP disabled - IP, GATEWAY, NETMASK, and DNS must be valid
# DHCP=1 DHCP enabled - IP, GATEWAY, NETMASK, and DNS must be blank
DHCP=1
IP=
GATEWAY=
NETMASK=
DNS=
# Leave either SIGMAGW or MULTICAST blank
# SIGMAGW set to DNS name or IP address of SIGMA gateway server
SIGMAGW=192.168.140.165
# MULTICAST group default is 239.237.12.87
MULTICAST=
# DEVICEID set to device alias
# Limited to 20 alpha-numeric characters (0-1,A-Z,a-z), blank is acceptable
DEVICEID=000345
[WIFI CONFIGURATION]
# BSS=0 Infrastructure mode (Access point)
# BSS=1 Join or Create Ad-Hoc (peer-to-peer)
# BSS=2 Join only Ad-Hoc (peer-to-peer)
# BSS=3 Join any
BSS=0
# SSID= set to wireless network name
SSID=IP_Dev_Cert
# 802.11 Mode - 'b', 'g', and/or 'a'
```

DRAFT

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

DRAFT

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-----

MIIIEowIBAAKCAQE AuhKvGS9womnF7tmM1IOWuzbvMct7u+TDYtoQSNEitAYe5Bjr
XR+tQOT/2b08nJUjvNI91/+3t2i9qUDDU58DTKKir9dmR5ridHlalyhts8fB7h2a
rZ74YK+4/A1C2mNpmwqwDQlwWhJzJgSe5XeZF0ALTdS3LEggwpuPb6Eo2Wbnqwr0
/tbsRvaeEjwclGOwmuy1v8TkrbSKeFt9I4B54Pcl3KsxbnnUjH7JIV9h/OnyrOKi
z2P+3maogCnOwxRQp79j/IgCS3JbUBMG14gKnxorJgLuBovqpsWIYO6k/qohlpyg
Vevc0UUj8XiyEun1ldT1SCXYke/I9jauLBB6OQIDAQABAoIBAHjnmw7qXG2r/Qju

DRAFT

lywTNOYBE/tvFL9KLgsVVM96NOp0762W45hm9NSt9/ErnS7BWWvQxoyLhHyQemx3
wHOdzY9snflUJQlyAqNcFs2xf1bJ/aETa2ZVXV61z6U3mLD+16f+kdZmw7JDO8B
UZ4Y0EjjPHUeOsdzNpY9Lj6CoWBg+V3+TEo3WCqHsqHN8yoVKP30Xnfb1JMgRLf/
infhI6Qg6QKBM++vWQjIUyU4hbQtQ6HmwWv2epu8YHFdmm3jTSrv+W8IBbY2N5D
N9tZsdUJ54NHIVZTjVmAXCxSpBp3+yTOMRpnzgW0v8MLMhFanjIC5QypG712HIQx
gk7LZGEGcYEA4vB26UpZNxsOlgzcEQP8fQ82Dk5xNjb9e7qDSD85LUppR6F4xwNs
QPyFVYRemb+pQylwn1X2SNAdRvsDwSsFVTV9ENi1PzIHbOfaBWE9/VNMaz8vCjfr
teC3So6bIWIIHNeoOI8d1wrTOtGZFENH/H4DoOBC7U0aoYjvtnYBplMCgYEA0eaJ
mITPESmZRZI8kaCb/TrWLTZmH2SOCPgC/qVmJ2FiQ8iT3KJXJ5d8ophY84Kay4le
axVUUGldKNyvNrf038Rx0DirN+qznSKPJUMdY+tnCxaXBJTj/tSwkeiNamZOXHeH
boVIREX6ONDvT+u9MkvMxDmhwBb9G4izw26a88MCgYAhqyFJLTGdPINkqZXAplHC
IA6aAsNDEtd6kspFXrPh50dFTE54iUeYxh4/oF2d/vprNnf2cYHOXE0hdEhyHsr
EBt082G4dowFOUScRbgHrGMLCj21W2SKAEPROOUFCpjQVYhs2I25yK5b7Jq0aeL1
L9Dj/kGPqT/JNWKzBEDsZwKbgQDFnt5BN0d20Kb5/xR5n3Xwz788a8g35rqtIplt
uOnqRk2Vcne67a0FvgeUnZ+17BiU9FSKOFgpVWMgaXk6W6HBjbqehBB2bRCHOmhH2
b53Fq//9lxRy+G7fl+busJluRwGJT6Un6p3kttgLWgQAC3aQMzgJhjy7xt25aQ+9
p8ZFEQKBgB6jQAT31FvxPFHyjU4NdFeogJd2c2nFbkC7aqOEPKNG9Nbnz/VVWh7x
Rx7Axua3D2OYrCH7V1NcR9X1dInpyj/hYXc5/VdtLZ2yhEc2GiG/jfgNWk2W2Bzd
2NLf54bgV67IkC2yKMK/5wBru+V73WmqvWfQ4KsMesLLBBzMRvJa

-----END RSA PRIVATE KEY-----

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

MIIIFWzCCBEOgAwIBAgIQAr0FxoUrLR0mLxVp3m/RJzANBgkqhkiG9w0BAQsFADBx
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMFRGlnaUNlcnQgSW5jMRkwFwYDVQQLEXB3
d3cuZGlnaWNlcnQuY29tMTAwLgYDVQQDEydEaWdpQ2VydCBUZXN0IEludGVybWVx
aWF0ZSBSb290IENBIFNIQTlW HhcNMTcwMzE1MDAwMDAwW hcNMTgwMzE1MTIwMDAw
WjCBiDELMAkGA1UEBhMCVVMxZzA1BgNVBAgTAK1EMRIwEAYDVQQHEwIsb2Nrdmls
bGUxNzA1BgNVBAoTLk5hdGlvbmFsiEluc3RpdHV0ZSBvZiBTdGFuZGFyZHMgYW5k
IFRIY2hub2xvZ3kxDjAMBgNVBA5TBUS5DQ29FMQ8wDQYDVQQDEwZCYXh0ZlIwggEi
MAOGCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6Eq8ZL3CiacXu2YzUg5a7Nu8x

DRAFT

y3u75MNI2hBI0SK0Bh7kG0tdH61A5P/ZvTyclSNU2X3X/7e3aL2pQMNTnwNMoqKv
12ZHmuJ0eVojKG2zx8HuHZqtnvhgr7j8DULaY2mbCrANCXBaEnMmBJ7ld5kXQAtN
1LcsSCDCm49voSjZZuerCvT+1uxG9p4SPBwgY7Ca7LW/xOSttlp4W30jgHng9yXc
qzFuedSMfskhX2H/SfKs4qLPY/7eZqiAKc7DFFCnv2P8iAJLcltQEwbXiAqfGism
Au4Gi+qmxYhg7qT+qiEinKBV69zRRSPxeLIS6fWV1PVIJdiR78j2Nq4sEHO5AgMB
AAGjggHVMIIIB0TAFBgNVHSMEGDAWgBSJVf2JvOIQPPttTh8w+fmCi1xh4jAdBgNV
HQ4EFgQU3PsluQqjWZ2eFYrcKNhdYi7Rf1owEQYDVR0RBAowCIIGQmF4dGVyMA4G
A1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQCDAQYIKwYBBQUHAWIwZUG
A1UdHwSBjTCBijBDoEGgP4Y9aHR0cDovL2NybdN0ZXN0LmRpZ2ljZXJ0LmNvbS9E
aWdpQ2VydFRlc3RjbnRlcm1lZGlhdGVtSEEyLmNybDBDoEGgP4Y9aHR0cDovL2Ny
bdN0ZXN0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFRlc3RjbnRlcm1lZGlhdGVtSEEy
LmNybDAhBgNVHSAEGjAYMAwGCmCGSAGG/WxjAQEwCAYGZ4EMAQICMIGDBggrBgEF
BQCBAQR3MHUwKAYIKwYBBQUHMAGGHGh0dHA6Ly9vY3NwdGVzdC5kaWdpY2VydC5j
b20wSQYIKwYBBQUHMAKGPWh0dHA6Ly9jYWNlcnRzLmRpZ2ljZXJ0LmNvbS9EaWdp
Q2VydFRlc3RjbnRlcm1lZGlhdGUtU0hBmi5jcnQwDAYDVR0TAQH/BAIwADANBgkq
hkiG9w0BAQsFAAOCAQEAE7Rc6PbIfEjSQpCZ3UpZ7zqWruov44nmSKvR/X4MJITM
z9k3S+TzGOGYnq7bHBF1mjLt0l5K/BDWSG6LY5clSYJuGCbC/dSNFk9G+lzBKs5S
5xJxk8HeAt4OHOWmtEhZ7S4np7zUBcRu1koHbw4vW/IYJBvxRF1Sdd0ypyBP4X81
D2mX+LmFo2rlLSExurr5rd1s6Pna2FRBEjoyM78ID9AmKENqeioDi+hxGLIQROOt
y7aZU8yWcec7nad9iUGO/pMDdhhbWexpvp4CBihxYkUMQcf8RaqTkJM8fLAdvPq9P
oQuBuMi+qPtl3WkTgfwr49usBzgbdrdNpc/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-----

MIIGSTCCBTGgAwIBAgIEM6qqqjANBgkqhkiG9w0BAQsFAADBkMQswCQYDVQQGEwJV

DRAFT

kUDPAEO4yHSXDnoe0fhk24/yCuO6Wc+mMe7YXzEkq8pOEWjNw/9E1dsP20L7jD3F
97q5uVNe1wEaeE3U5Eq1xKUBdyQqitinpTv/yo/UPTDLpfjBmK2nh2HK6r0RH+YC
OicqQ99N+q6YeAlhejLa7+7FkKYKK1YEAbE1Icc=

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

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

MIIDpjCCAo6gAwIBAgIBMzANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQGEwJVUzEV
MBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWNlcnQuY29t
MSMwIQYDVQQDEExpEaWdpQ2VydCBUZXN0IFJvb3QgQ0EgU0hBMjAeFw0wNjExMTAw
MDAwMDBaFw0zMTExMTAwMDAwMDBaMGQxCzAJBgNVBAYTAiVTMRUwEwYDVQQKEwxE
aWdpQ2VydCBjbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5jb20xIzAhBgNVBAMT
GkRzZ2lDZXJ0IFRlc3QgUm9vdCBDQSBTSEEyMIIlBjANBgkqhkiG9w0BAQEFAAOc
AQ8AMIIBCgKCAQEA0DLGgpMXqI2YZ15ULS61yqqqiBMpmRtM9/w/1pqoA/GEri19
VMFuvtPTWgu9IQf0dQsRMy2d8V4INSj43YyQeXnxPzanTSqza95yoH/h4xUM/pNq
AIXIO8c+cYMYCdZTQ0vrEWcvPZOtXYABac9E9ceT015RdD5pORjMwTcb6NxydZr8
nRd9/J66L4R17IKvTU74lwA6fwNd0UnXbhVhGdeEAe+eIEvJ5WIWxDeS6ZdZuSzv
h24QxhxpuCtzSq81HHCHw4a1kOel2oqlDIUY698atS0nxfw3IR30heQ/g793Mce9
SX9u2dPPAZtSaW8/38TwKbNOa9zkRFn7oF+cZQIDAQABo2MwYTAOBgNVHQ8BAf8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU9kZ+Gxa7N5lj9z/YhSzk
yepYDx4wHwYDVR0jBBgwFoAU9kZ+Gxa7N5lj9z/YhSzkypYDx4wDQYJKoZIhvcN
AQELBQADggEBAAeQacFm1sFPOIEvXDVi3IH2RKF7he0p/M0bK2Soj137LMf+ctpM
3bFKJPY97YIE0g7T1qgR8TN2sK0moumMTPjWCdFWJyN4yakS6tPIWEG2XobJ9H1r
iuVXLkd2M/1yhqUyt1o5KtbOGQXLFd3qdp4A1tcXuK2wyMTiSCYS3Uow61JdEw6M
eyrMIpZl9GtvaXTz6LdnozAbhKC7bVUy7ob0T4E03fQ8hIQCNPupvY7Db1/Xmlw8
QWVd6AOH7EE3P8xbWOvcTWZ5XbstWY014GeJFXZ7YreaAg8sYa6CzasuHkr/rxeZ
8yzOmCTTSPk5Ju5bTfAyEpgkl5fDvntJQg=

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

Appendix C 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 4/20/2017]
- [2] Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide, 9.6 [Web site], <http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start/asav-quick/intro-asav.html> [accessed 4/20/17]
- [3] 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 4/20/2017]
- [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 4/20/2017]
- [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 4/20/2017]
- [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 4/20/2017]
- [7] Institute of Electrical and Electronics Engineers (IEEE), *802.1Q-2014 - Bridges and Bridged Networks*, December 2014 <http://www.ieee802.org/1/pages/802.1Q-2014.html> [accessed 4/20/2017]
- [8] Institute of Electrical and Electronics Engineers (IEEE), 802.11i-2004 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1318903>
- [9] 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 4/20/2017]
- [10] 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 4/20/2017]
- [11] D. Simon, B. Aboba, and R. Hurst *The EAP-TLS Authentication Protocol* Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 5016, March 2008. <https://www.ietf.org/rfc/rfc5216.txt> [accessed 4/20/2017]
- [12] 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 4/20/2017]
- [13] 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 4/20/2017]



National Security Archive,
Suite 701, Gelman Library, The George Washington University,
2130 H Street, NW, Washington, D.C., 20037,
Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu