

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
Sallie Edwards
Kevin Littlefield
Neil McNab
Sue Wang
Kangmin Zheng

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

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



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*

August 2018



U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter G. Copan, 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**

Gavin O'Brien

National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards

Kevin Littlefield

Neil McNab

Sue Wang

Kangmin Zheng

The MITRE Corporation
McLean, VA

August 2018

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

The first draft of this publication is available free of charge from:

<https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf>



Executive Summary

- Broad technological advancements have contributed to the Internet of Things (IoT) phenomenon, where physical devices now have technology that allow them to connect to the internet and communicate with other devices or systems. With billions of devices being connected to the internet, many industries, including healthcare, have leveraged, or are beginning to leverage, IoT devices to improve operational efficiency and enhance innovation.
- Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider. With technological improvements designed to enhance patient care, these devices now connect wirelessly to a variety of systems, networks, and other tools within a healthcare delivery organization (HDO)—ultimately contributing to the Internet of Medical Things (IoMT).
- As IoMT grows, cybersecurity risks have risen. According to the Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report 57 (TIR57), “this has created a new source of risk for [the] safe operation [of medical devices].” In particular, the wireless infusion pump ecosystem (the pump, the network, and the data stored in and on a pump) faces a range of threats, including unauthorized access to protected health information (PHI), changes to prescribed drug doses, and interference with a pump’s function.
- In addition to managing interconnected medical devices, HDOs oversee complex, highly technical environments, from back-office applications for billing and insurance services, supply chain and inventory management, and staff scheduling, to clinical systems, such as radiological and pharmaceutical support. In this intricate healthcare environment, HDOs and medical device manufacturers that share responsibility and take a collaborative, holistic approach to reducing cybersecurity risks of the infusion pump ecosystem can better protect healthcare systems, patients, PHI, and enterprise information.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) analyzed risk factors in and around the infusion pump ecosystem by using a questionnaire-based risk assessment. With the results of that assessment, the NCCoE then developed 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.

CHALLENGE

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

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

wireless infusion pump ecosystem can expose a healthcare provider's enterprise to serious risks, such as the following examples:

- access by malicious actors
- loss or corruption of enterprise information and patient data and health records
- a breach of PHI
- loss or disruption of healthcare services
- damage to an organization's reputation, productivity, and bottom-line revenue

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

SOLUTION

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

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

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide to securing wireless infusion pumps in HDOs can help your organization:

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

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

SHARE YOUR FEEDBACK

You can view or download the guide at <https://www.nccoe.nist.gov/projects/use-cases/medical-devices>.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at hit_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as “Technology Partners/Collaborators” herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.



Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit <https://www.nccoe.nist.gov/nccoe@nist.gov>
301-975-0200

NIST SPECIAL PUBLICATION 1800-8B

Securing Wireless Infusion Pumps in Healthcare Delivery Organizations

Volume B:
Approach, Architecture, and Security Characteristics

Gavin O'Brien

National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards

Kevin Littlefield

Neil McNab

Sue Wang

Kangmin Zheng

The MITRE Corporation
McLean, VA

August 2018

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

The first draft of this publication is available free of charge from:

<https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf>



DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-8B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-8B, 89 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

To learn more about the NCCoE, visit <https://www.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. However, today's medical devices connect to a variety of healthcare systems, networks, and other tools within a healthcare delivery organization (HDO). Connecting devices to point-of-care medication systems and electronic health records can improve healthcare delivery processes; however, increasing connectivity capabilities also creates cybersecurity risks. Potential threats include unauthorized access to patient health information, changes to prescribed drug doses, and interference with a pump's function.

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

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

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
<u>Baxter Healthcare Corporation</u>	<ul style="list-style-type: none"> • Sigma Spectrum™ Large Volume Pump (LVP) Version 8 • Sigma Spectrum Wireless Battery Module Version 8 • Sigma Spectrum Master Drug Library Version 8 • Care Everywhere Gateway Server Version 14

Technology Partner/Collaborator	Build Involvement
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 Patient Care Unit (PCU) Version 9.19.2 Alaris Syringe Module 8110 Alaris LVP Module 8100 Alaris Systems Manager Version 4.2 Alaris System Maintenance (ASM) Version 10.19
Cisco	<ul style="list-style-type: none"> Aironet 1600 Series Access Point (AIR-CAP1602I-A-K9) Wireless LAN [Local Area Network] (WLC) Controller 8.2.111.0 Identity Services Engine (ISE) Adaptive Security Appliance (ASA) Catalyst 3650 Switch
Clearwater Compliance	<ul style="list-style-type: none"> IRM Pro™ IRM Analysis™
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®
Medical Device Innovation, Safety & Security Consortium (MDISS)	Medical Device Risk Assessment Platform (MDRAP™)
PFP Cybersecurity	Device Monitor
Ramparts	Risk Assessment

Technology Partner/Collaborator	Build Involvement
<u>Smiths Medical</u>	<ul style="list-style-type: none">● Medfusion® 3500 Version 5 Syringe Infusion System● PharmGuard® Toolbox Version 1.5● Medfusion 4000 Wireless Syringe Infusion Pump● PharmGuard Toolbox 2 Version 3.0 use with Medfusion 4000 and 3500 Version 6 (US)● PharmGuard Server Licenses, PharmGuard Server Enterprise Edition Version 1.1● CADD®-Solis Ambulatory Infusion Pump● CADD-Solis Medication Safety Software
<u>Symantec Corporation</u>	<ul style="list-style-type: none">● Symantec Endpoint Protection (SEP)● Advanced Threat Protection: Network (ATP:N)● Data Center Security: Server Advanced (DCS:SA)
<u>TDi Technologies, Inc.</u>	ConsoleWorks®

Contents

1	Summary	1
1.1	Challenge	3
1.2	Solution.....	4
1.3	Benefits.....	5
2	How to Use This Guide	5
2.1	Typographic Conventions.....	7
3	Approach	7
3.1	Audience.....	8
3.2	Scope	8
3.3	Assumptions	8
3.4	Security.....	9
3.5	Existing Infrastructure	9
3.6	Technical Implementation.....	9
3.7	Capability Variation	9
4	Risk Assessment and Mitigation	9
4.1	Risk Assessments.....	11
4.1.1	Industry Analysis of Risk	12
4.1.2	Questionnaire-Based Risk Assessment	12
4.1.3	Assets	13
4.1.4	Threats	13
4.1.5	Vulnerabilities	13
4.1.6	Risks	15
4.1.7	Recommendations and Best Practices.....	17
4.2	Risk Response Strategy.....	17
4.2.1	Risk Mitigation	17
4.3	Security Characteristics and Controls Mapping	18
4.4	Technologies.....	28

5	Architecture	36
5.1	Basic System	37
5.2	Data Flow.....	37
5.3	Cybersecurity Controls	38
5.3.1	Network Controls.....	38
5.3.2	Pump Controls	52
5.3.3	Pump Server Controls	53
5.3.4	Enterprise-Level Controls.....	56
5.4	Final Architecture	57
6	Life-Cycle Cybersecurity Issues	59
6.1	Procurement.....	60
6.2	Operation	60
6.3	Maintenance.....	61
6.4	Disposal	61
7	Security Characteristics Analysis.....	62
7.1	Assumptions and Limitations	62
7.2	Application of Security Characteristics.....	62
7.2.1	Supported NIST Cybersecurity Framework Subcategories	62
7.3	Security Analysis Summary.....	66
8	Functional Evaluation.....	66
8.1	Functional Test Plan	66
8.1.1	Test Case WIP-1	67
8.1.2	Test Case WIP-2	68
8.1.3	Test Case WIP-3	69
8.1.4	Test Case WIP-4	70
8.1.5	Test Case WIP-5	70
8.1.6	Test Case WIP-6	71
8.1.7	Test Case WIP-7	72
9	Future Considerations	73

Appendix A Threats	74
Appendix B Vulnerabilities	76
Appendix C Recommendations and Best Practices.....	79
Appendix D Acronyms	81
Appendix E References	84

List of Figures

Figure 4-1 Tiered Risk Management Approach [12]	10
Figure 4-2 Relationship Between Security and Safety Risks [9]	11
Figure 5-1 Basic System	37
Figure 5-2 Network Architecture with Segmentation.....	42
Figure 5-3 Wi-Fi Management	43
Figure 5-4 Wi-Fi Authentication	44
Figure 5-5 Wi-Fi Device Access	45
Figure 5-6 Network Access Control.....	47
Figure 5-7 Remote Access VPN	49
Figure 5-8 Remote Access	50
Figure 5-9 External	51
Figure 5-10 Pump Server Protection.....	56
Figure 5-11 Target Architecture	58
Figure 6-1 Asset Life Cycle [53]	59

List of Tables

Table 4-1 Security Characteristics and Controls Mapping -- NIST Cyber Security Framework	20
Table 4-2 Products and Technologies	29
Table 8-1 Functional Test Plan.....	66
Table 8-2 Test Case WIP-1	67
Table 8-3 Test Case WIP-2	68
Table 8-4 Test Case WIP-3	69
Table 8-5 Test Case WIP-4	70
Table 8-6 Test Case WIP-5	70
Table 8-7 Test Case WIP-6	71
Table 8-8 Test Case WIP-7	72

1 Summary

Broad technological advancements have contributed to the Internet of Things (IoT) phenomenon, where physical devices now have technology that allow them to connect to the internet and communicate with other devices or systems. With billions of devices being connected to the internet, many industries, including healthcare, have or are beginning to leverage IoT devices to improve operational efficiency and enhance innovation.

Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider [1]. With technological improvements designed to enhance patient care, these devices now connect wirelessly to a variety of systems, networks, and other tools within a healthcare delivery organization (HDO)—ultimately contributing to the Internet of Medical Things (IoMT). The wireless infusion pump ecosystem (the pump, the network, and the data stored in and on a pump) faces a range of threats, including unauthorized access to protected health information (PHI), changes to prescribed drug doses, and interference with a pump's function.

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

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

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

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

For ease of use of this volume, the following paragraphs provide a short description of each section of this volume.

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

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

Section 3, Approach, offers a detailed treatment of the scope of the project, and describes the assumptions on which the security platform development was based, the risk assessment that informed platform development, and the technologies and components that industry collaborators gave us to enable platform development.

Section 4, Risk Assessment and Mitigation, highlights the risks that we found, along with the potential response and mitigation efforts that can help lower risks for HDOs.

Section 5, Architecture, describes the usage scenarios supported by project security platforms, including the NIST Cybersecurity Framework Functions supported by each component contributed by our collaborators.

Section 6, Life Cycle Cybersecurity Issues, discusses cybersecurity considerations from a product-life-cycle perspective, including procurement, maintenance, and end of life.

Section 7, Security Characteristics Analysis, provides details about the tools and techniques that we used to perform risk assessments pertaining to wireless infusion pumps.

Section 8, Functional Evaluation, summarizes the test sequences that we employed to demonstrate security platform services, the NIST Cybersecurity Framework Functions to which each test sequence is relevant, and the NIST Special Publication (SP) 800-53 Revision 4 controls that applied to the functions being demonstrated.

Section 9, Future Considerations, is a brief treatment of other applications that NIST might explore in the future to further support wireless infusion pump cybersecurity.

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

1.1 Challenge

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

Wireless infusion pumps are challenging to protect, for several reasons. They can be infected by malware, which can cause them to malfunction or operate differently than originally intended, and traditional malware protection could negatively impact the pump's ability to operate efficiently. In addition, most wireless infusion pumps contain a maintenance default passcode. If HDOs do not change the default passcodes when provisioning pumps, and do not periodically change the passwords after pumps are deployed, this creates a vulnerability. This can make it difficult to revoke access codes (e.g., when a hospital employee resigns from the job). Furthermore, information stored inside infusion pumps must be properly secured, including data from drug library systems, infusion rates and dosages, or PHI [2], [3], [4], [5], [6].

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

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

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

1.2 Solution

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

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

- NIST Framework for Improving Critical Infrastructure Cybersecurity [10]
- NIST Risk Management Framework (RMF) [11], [12], [13]
- NIST SP 800-53 Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations* [14]
- Association for the Advancement of Medical Instrumentation (AAMI) Technical Information Report (TIR)57 [9]
- International Electrotechnical Commission Technical Report (IEC/TR) 80001-2: *Application of risk management for IT-networks incorporating medical devices* [15], [16], [17], [18], [19]
- FDA's *Postmarket Management of Cybersecurity in Medical Devices* [3]

Ultimately, this practice guide:

- maps security characteristics to standards and best practices from NIST and other standards organizations, as well as to the HIPAA Security Rule [10], [14], [20], [21], [22]
- provides a detailed architecture and capabilities that address security controls
- provides a how-to for implementers and security engineers to recreate the reference design
- is modular and uses products that are readily available and interoperable with existing IT infrastructure and investments

1.3 Benefits

The NCCoE's practice guide to securing wireless infusion pumps in HDOs can help your organization:

- illustrate cybersecurity standards and best-practice guidelines to better secure the wireless infusion pump ecosystem, such as the hardening of operating systems, segmenting the network, file and program whitelisting, code-signing, and using certificates for both authorization and encryption, maintaining the performance and usability of wireless infusion pumps
- reduce risks from the compromise of information, including the potential for a breach or loss of PHI, as well as not allowing these medical devices to be used for anything other than the intended purposes
- document a defense-in-depth strategy to introduce layers of cybersecurity controls that avoid a single point of failure and provide strong support for availability. This strategy may include a variety of tactics: using network segmentation to isolate business units and user access; applying firewalls to manage and control network traffic; hardening and enabling device security features to reduce zero-day exploits; and implementing strong network authentication protocols and proper network encryption, monitoring, auditing, and intrusion detection systems (IDS) and intrusion prevention systems (IPS)
- highlight best practices for the procurement of wireless infusion pumps, by including the need for cybersecurity features at the point of purchase
- call upon industry to create new best practices for healthcare providers to consider when on-boarding medical devices, with a focus on elements such as asset inventory, certificate management, device hardening and configuration, and a clean-room environment to limit the possibility of zero-day vulnerabilities

2 How to Use This Guide

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

This guide contains three volumes:

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

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

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

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

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

- [Section 4](#), Risk Assessment and Mitigation, provides a description of the risk analysis we performed
- [Section 4.3](#), Security Characteristics and Controls Mapping, maps the security characteristics of this example solution to cybersecurity standards and best practices

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

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

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of NCCoE's questionnaire-based risk assessment and the deployment of a defense-in-depth strategy. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. [Section 4.4](#), Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

2.1 Typographic Conventions

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	service sshd start
<u>blue text</u>	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 .

3 Approach

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

Clinicians and patients rely on infusion pumps for a safe and accurate administration of fluids and medications. However, the FDA has identified problems that can compromise the safe use of external infusion pumps [2], [3], [7]. These issues can lead to over-infusion or under-infusion, missed treatments, or delayed therapy. The NCCoE initiated this project to help healthcare providers develop a more secure wireless infusion pump ecosystem, which can be applied to similarly connected medical devices. The wireless infusion pump was selected as a representative medical device. Throughout the remainder of this guide, the focus will be on the secure operation of the wireless infusion pump ecosystem. Both the

architecture and security controls may be applied to increase the security posture for other types of medical devices. However, any application should be reviewed and tailored to the specific environment in which the medical device will operate.

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

3.1 Audience

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

More specifically, Volume B of the practice guide (*NIST SP 1800-8B*) is designed to appeal to a wide range of job functions. This volume provides cybersecurity or technology decision makers within HDOs with a view into how they can make the medical device environment more secure to help improve their enterprise's security posture and help reduce enterprise risk. Additionally, this volume offers technical staff guidance on architecting a more secure medical device network and instituting compensating controls.

3.2 Scope

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

3.3 Assumptions

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

3.4 Security

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

3.5 Existing Infrastructure

This guide may help you design an entirely new infrastructure; however, this guide is geared toward those with an established infrastructure, as that represents the largest portion of readers. Hospitals and clinics are likely to have some combination of the capabilities described in this reference solution. Before applying any measures addressed in this guide, we recommend that you review and test them for applicability to your existing environment. No two hospitals or clinics are the same, and the impact of applying security controls will differ.

3.6 Technical Implementation

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

3.7 Capability Variation

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

4 Risk Assessment and Mitigation

[NIST Special Publication \(SP\) 800-30, Guide for Conducting Risk Assessments](#), states that risk is “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence” [11]. The guide further defines risk assessment as “the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.”

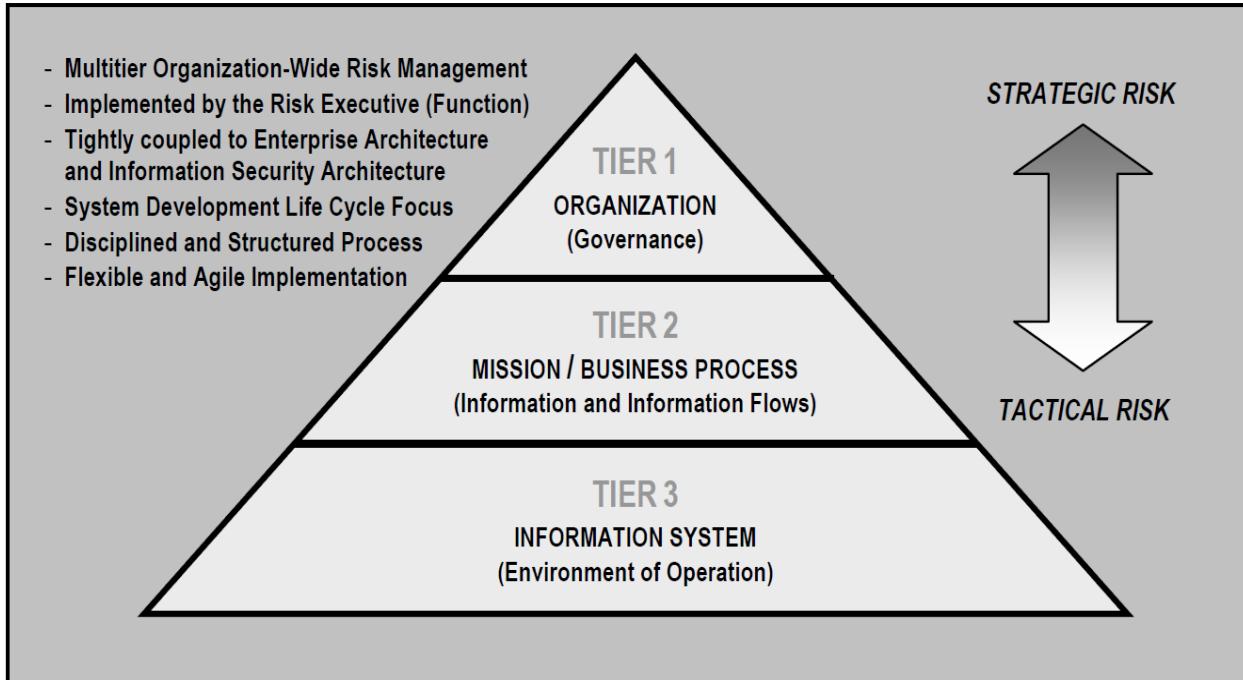
The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begins with a comprehensive review of [NIST SP 800-37, Guide for Applying the Risk Management](#)

[Framework to Federal Information Systems](#)—material that is available to the public [12]. The [risk management framework \(RMF\)](#) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

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

- Tier 1: Organization
- Tier 2: Mission/Business Process
- Tier 3: Information System

Figure 4-1 Tiered Risk Management Approach [12]



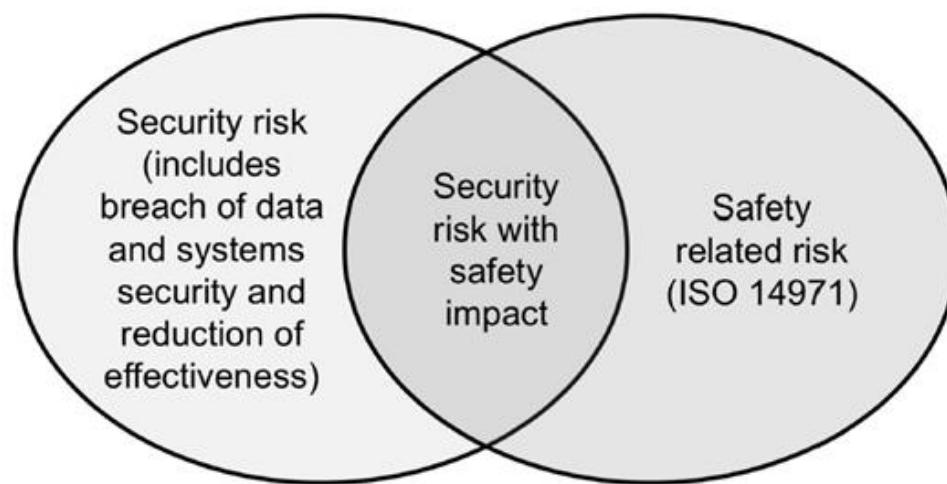
This guide focuses on the Tier 3 application of risk management, but incorporates other industry risk-management and risk-assessment standards and best practices for the context of networked medical devices in HDOs:

- American National Standards Institute (ANSI)/AAMI/IEC 80001-1:2010: *Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities* [23]

- IEC/TR 80001-2: *Application of risk management for IT-networks incorporating medical devices* [15], [16], [17], [18], [19]
- ANSI/AAMI/International Standards Organization (ISO) 14971:2007: *Medical devices – Application of risk management to medical devices* [24]
- AAMI TIR57: 2016: *Principles for medical device security – Risk management* [9]
- FDA's *Postmarket Management of Cybersecurity in Medical Devices* [3]

For this NCCoE project, it was extremely important to understand the complexity of networked medical devices in a system-of-systems environment. Additionally, we felt that it is necessary to understand where security risks may have safety implications. AAMI TIR57 [9] was particularly useful in this regard, as it specified elements of medical device security using NIST's RMF, ANSI/AAMI/IEC 80001-1, IEC/TR 80001-2, and ANSI/AAMI/ISO 14971:2007 [11], [12], [13], [15], [16], [17], [18], [19], [23], [24]. Also, the Venn diagram in Figure 4-2 illustrates the relationship between security and safety risks (AAMI TIR57). As seen in this diagram, there are cybersecurity risks that may have safety impacts. For HDOs, these risks should receive special attention from both security and safety personnel.

Figure 4-2 Relationship Between Security and Safety Risks [9]



4.1 Risk Assessments

For this NCCoE project, we performed two types of risk assessments: an industry analysis of risk and a questionnaire-based risk assessment.

4.1.1 Industry Analysis of Risk

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

Activities involved in our industry analysis included reaching out to our COI and other industry experts through workshops and focus group discussions. After receiving feedback on the NCCoE’s use case publication through a period of public comment, the NCCoE adjudicated the comments and clarified a project description. These activities were instrumental to identifying primary risk factors as well as educating our team on the uniqueness of cybersecurity risks involved in protecting medical devices in healthcare environments.

4.1.2 Questionnaire-Based Risk Assessment

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

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

- protect the wireless infusion pumps from cyber attacks
- protect the healthcare ecosystem, should a wireless infusion pump be compromised

Per AAMI TIR57, “To assess security risk, several factors need to be identified and documented” [9].

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

4.1.3 Assets

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

4.1.4 Threats

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

- targeted attacks
- advanced persistent threats (APTs)
- disruption of service: denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks
- malware infections
- theft or loss of assets
- unintentional misuse
- vulnerable systems or devices directly connected to the device (e.g., via Universal-Serial-Bus [USB] or other hardwired, non-network connections)

It is important to understand that the threat landscape is constantly evolving, and that unknown threats exist and may be unavoidable. These unknown threats need to be identified and remediated as soon as possible after they are found.

4.1.5 Vulnerabilities

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

Some typical vulnerabilities that may arise when using wireless infusion pumps are listed below. Refer to [Appendix B](#) for a description of each vulnerability.

- lack of asset inventory
- long useful life
- information/data vulnerabilities
 - lack of encryption on private/sensitive data at rest
 - lack of encryption on transmitted data
 - unauthorized changes to device calibration or configuration data
 - insufficient data backup
 - lack of capability to de-identify private/sensitive data
 - lack of data validation
- device/endpoint (infusion pump) vulnerabilities
 - debug-enabled interfaces
 - use of removable media
 - lack of physical tamper detection and response
 - misconfiguration
 - poorly protected and unpatched devices
- user or administrator accounts vulnerabilities
 - hard-coded or factory default passcodes
 - lack of role-based access and/or use of principles of least privilege
 - dormant accounts
 - weak remote access controls
- IT network infrastructure vulnerabilities
 - lack of malware protection
 - lack of system hardening
 - insecure network configuration
 - system complexity

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

4.1.6 Risks

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

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

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

- Infusion pumps and server components may be leveraged for APTs and may serve as pivot points to cause adverse conditions throughout a hospital’s infrastructure.
- Infusion pumps may be manipulated to prevent the effective implementation of safety measures, such as the drug library.
- Infusion pump interfaces may be used for unintended or unexpected purposes, with those conditions leading to degraded performance of the pump.
- PHI may be accessed remotely by unauthorized individuals.
- PHI may be disclosed to unauthorized individuals if the device is lost, stolen, or improperly decommissioned.
- Hospital’s network may have improper third-party vendor connections

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

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

Infusion pumps may not allow for the addition of third-party mechanisms, such as antivirus or anti-malware controls. Infusion pumps are validated medical devices, with set configuration and deployment specifications, and therefore may not accept third-party security controls or third-party-provided endpoint mitigation on the pump itself. Validation supports a manufacturer’s capabilities regarding the intended purpose of the device (i.e., infusing patients with medication, analgesics, or nutrients), and

requirements around the validation and approval process for medical devices fall under the auspices of the FDA. If limitations are identified in embedded operating systems used by an infusion pump, then vulnerabilities, weaknesses, and deficiencies may become known to malicious actors who may seek to leverage those deficiencies to install malicious or unauthorized software on those devices.

Malicious software, or malware, may cause adverse conditions on the pump, degrading the performance of the pump or rendering the device unable to perform its function (e.g., ransomware; trojans that may allow for remote access to use the device as a pivot point; backdoors; malicious software that may allow for data exfiltration or may inappropriately consume system resources, preventing the pump from rendering patient care functionality). Additionally, malware may be used to convert the infusion pump into an access point for malicious actors to subsequently access or disrupt the operations of other hospital systems.

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

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

Modern infusion pumps and server components may include PHI, such as a patient's name, medical record number (MRN), procedure coding, and medication or treatment. Through similar deficiencies that would allow configuration or use manipulation as noted above, this PHI may then be viewed, accessed, or removed by unauthorized individuals. Also, individuals who have direct access to the infusion pump may be able to extract information through unsecured ports or interfaces [2], [3], [7], [17], [25].

The following common vulnerabilities and control deficiencies may enable these risks:

- **Implementation of default credentials and passwords:** Weak authentication and default passwords, or not implementing authentication or access control, may be discovered by malicious actors who would seek to cause adverse conditions. Malicious actors may leverage this control deficiency for risk factors that span from installing malware on the infusion pump, to manipulating configuration settings, to extracting information, such as PHI, from the device.
- **Use of unsecured network ports, such as Telnet or File Transfer Protocol (FTP):** Telnet and FTP are internet protocols that do not secure or encrypt network sessions. Telnet and FTP may be used nominally for technical support interfaces; however, malicious actors may attempt to leverage these protocols to access the infusion pump. Telnet and FTP may include deficiencies

that allow for the protocol itself to be compromised, and, because the network session is not encrypted, malicious actors may implement mechanisms to capture network sessions, including any authentication traffic, or to identify sensitive information, such as credentials, configuration information, or any PHI stored on the device.

- **Local interfaces with limited security controls:** Local interfaces, such as USB ports, serial ports, Bluetooth, radio frequency, or other ports may be used for device technical support. These ports, however, allow for malicious actors within close proximity to the device to access the device, to manipulate configuration settings, to access or remove data from the device, or to install malware on the device. These ports may exist on the pump for support purposes; however, use of the ports for unauthorized or unexpected purposes, such as recharging a mobile device (e.g., smart phone, tablet), may cause a disruption to the pump's standard operation.

4.1.7 Recommendations and Best Practices

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

4.2 Risk Response Strategy

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

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

4.2.1 Risk Mitigation

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

These remediation responses can take the form of administrative, physical, and technical controls, or an appropriate mix. As previously mentioned, [Appendix C](#) identifies several mitigation recommendations

regarding specific risk. Additional compensating safeguards, countermeasures, or controls are noted below:

- physical security controls, including standard tamper-evident physical seals, which can be applied to hardware to indicate unauthorized physical access [10], [14]
- ensuring the implementation of a physical asset management program that manages and tracks unique, mobile media, such as removable flash memory devices (e.g., Secure Digital [SD] cards, thumb drives) used by pump software hosted on an endpoint client. Consider the encryption of all portable media used in such a fashion [10], [14], [26], [27].
- following procedures for clearing wireless network authentication credentials on the endpoint client if the pump is to be removed or transported from the facility. These procedures can be found in pump user manuals, but should be referenced in official HDO policies and procedures [28], [29], [30], [31].
- changing wireless network authentication credentials regularly and, if there is evidence of unauthorized access to a pump system, immediately changing network authentication credentials [10], [14]
- ensuring that all wireless network access is minimally configured for Wi-Fi Protected Access II (WPA2) Pre-Shared Key (PSK) encryption and authentication. All pumps should be set to WPA2 encryption [32], [33], [34], [35].
- ensuring that all patching has been applied, including those components that will use WPA2
- All pumps and pump systems should include cryptographic modules that have been validated as meeting NIST Federal Information Processing Standards (FIPS) Publication 140-2 [36].
- All ports are disabled, except when in use, and the device has no listening ports [3], [9], [10], [14], [25].
- employing mutual transport layer security (TLS) encryption in transit between the client and server [37]
- employing individual pump authentication with no shared key for all pumps [10], [14]
- certificate-based authentication for a pump server [28], [29], [30], [31]

During the course of this project, several vulnerabilities were published in the NVD (<https://nvd.nist.gov>) that identified means by which malicious actors may remotely compromise WPA2-secured sessions through the use of “key reinstallation attacks” (KRACKs). Individuals should review noted WPA2 vulnerabilities, refer to vendor/manufacturer patching and updates, and apply those patches and updates as soon as possible.

4.3 Security Characteristics and Controls Mapping

As described in the previous sections, we derived the security characteristics by analyzing risk in collaboration with our healthcare-sector stakeholders as well as our participating vendor partners. In

the risk analysis process, we used IEC/TR 80001-2-2 as our basis for wireless infusion pump capabilities in healthcare environments [16]. Table 4-1 presents the desired security characteristics of the use case, in terms of the NIST Cybersecurity Framework Subcategories [10], [14]. Each subcategory is mapped to relevant NIST standards, industry standards, controls, and best practices. In our example implementation, we did not observe any security characteristics that mapped to the Respond or Recover Subcategories of the NIST Cybersecurity Framework.

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

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	CNFS	45 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, SC-6	DTBK	45 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	45 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

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
PROTECT (PR)	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	45 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
	Identity Management and Access Control (PR.AC)	(Note: not directly mapped in the NIST Cybersecurity Framework)	AC-1, AC-11, AC-12	ALOF	None	None
		PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	AUTH, CNFS, EMRG, PAUT	45 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

NIST Cybersecurity Framework v1.1			Sector-Specific Standards & Best Practices			
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
		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	45 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	C-1, AC-17, AC-19, AC-20, SC-15	NAUT, PAUT	45 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

NIST Cybersecurity Framework v1.1			Sector-Specific Standards & Best Practices			
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	AUTH, CNFS, EMRG, NAUT, PAUT	45 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
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4, AC-10, SC-7	NAUT	45 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(e)	A.13.1.1, A.13.1.3, A.13.2.1

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	MP-8, SC-12, SC-28	IGAU, STCF	45 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, SC-11, SC-12	IGAU, TXCF	45 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

NIST Cybersecurity Framework v1.1			Sector-Specific Standards & Best Practices			
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
Information Protection Processes and Procedures (PR.IP)		PR.DS-4: Adequate capacity to ensure availability is maintained	AU-4, CP-2, SC-5	AUDT, DTBK	45 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	SC-16, SI-7	IGAU	45 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
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating 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	45 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

NIST Cybersecurity Framework v1.1			Sector-Specific Standards & Best Practices			
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
		PR.IP-4: Backups of information are conducted, maintained, and tested	CP-4, CP-6, CP-9	DTBK	45 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	45 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	45 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

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
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	45 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	45 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	45 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(e)	A.12.4.1
		DE.CM-4: Malicious code is detected	SI-3, SI-8	IGAU, MLDP, TXIG	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	A.12.2.1

NIST Cybersecurity Framework v1.1			Sector-Specific Standards & Best Practices			
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC/TR 80001-2-2	HIPAA Security Rule [38]	ISO/IEC 27001:2013 [39]
		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	45 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	45 C.F.R. §§ 164.306(e)	A.14.2.8
RESPOND (RS)	None	None	None	None	None	None
RECOVER (RC)	None	None	None	None	None	None

4.4 Technologies

Table 4-2 lists all of the technologies used in this project, and maps the generic application term to the specific product that we used and the security control(s) that we deployed. Refer to Table 4-1 for an explanation of the NIST Cybersecurity Framework Subcategory codes [10].

The reference architecture design in [Section 5](#) is vendor-agnostic, such that any wireless infusion pump system can be integrated safely and securely into a hospital's IT infrastructure. Therefore, for the infusion pump device, infusion pump server, and wireless infusion pump ecosystem, we captured the most-common security features among all the products that we tested in this use case. A normalized view of the list of Functions and NIST Cybersecurity Framework Subcategories are presented in Table 4-2.

Please note that some of the NIST Cybersecurity Framework Subcategory codes require people, and process controls, not solely technical controls.

Table 4-2 Products and Technologies

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Infusion Pump Device	Baxter: Sigma Spectrum™ LVP Version 8	<ul style="list-style-type: none">● requires a passcode to access the biomedical engineering mode (on device or connect to device) for configuring and setting up the devices● provides the capability to change the manufacturer default passcode● supports Institute of Electrical and Electronics Engineers (IEEE) 802.11i enterprise wireless encryption/authentication standards, including WPA2 with Extensible Authentication Protocol (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● closes/disables all services that are not required for the intended use● provides an integrity-checking mechanism to verify information● supports the baseline configuration● supports removing/destroying data from the device	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		
	B. Braun: Space Infusomat Infusion Pump (LVP)		
	BD: Alaris® 8015 Patient Care Unit (PCU) Version 9.19.2		
	BD: Alaris Syringe Module 8110		
	BD: Alaris LVP Module 8100		
	Hospira: Plum 360™ Version 15.10		

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
	Hospira: LifeCare PCA™ Version 7.02 Smiths Medical: Medfusion® 3500 Version 5 Syringe Infusion System Smiths Medical: Medfusion 4000 Wireless Syringe Infusion Pump Smiths Medical: CADD®-Solis Ambulatory Infusion Pump	<ul style="list-style-type: none"> • few models have a tamper-resist switch, with tamper-evident seals 	
Infusion Pump Server	Baxter: Care Everywhere Gateway Server Version 14 B. Braun: Space OnlineSuite Software Version Application Package 2.0.1 BD: Alaris Systems Manager Version 4.2	<ul style="list-style-type: none"> • with appropriate configuration, discovers and identifies devices connected to the pump server via wired networks, wireless networks, and virtual private networks (VPNs), to aid in building and maintaining accurate physical device inventories • supports role-based authentication and password rules and policies • supports the use of an HDO's Active Directory / Lightweight Directory Access Protocol (LDAP) solution 	ID.AM-1, PR.AC-1, PR.AC-3, PR.AC-4, PR.DS-1, PR.DS-2, PR.MA-2

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
	Hospira: MedNet™ 6.2 Smiths Medical: PharmGuard® Server Enterprise Edition Version 1.1	<ul style="list-style-type: none"> • supports auto-logoff, data encryption/obscuration • can be accessed remotely via VPN (or similar) tools • few models support FIPS Publication 140-2 • operates on a manufacturer-supported operating system, database server, and web server (allows software patches) 	
Infusion Pump Ecosystem	Baxter: Sigma Spectrum Master Drug Library Version 8 B. Braun: Space DoseTrac® and Space DoseLink™ software – Engineering version available for testing	<ul style="list-style-type: none"> • supports secure protocols, such as TLS • supports co-existence with firewall, antivirus, backup software, and other types of security safeguard products • maintains different types of audit/log records for preventing unauthorized access 	
	BD: Alaris System Maintenance (ASM) Version 10.19 Smiths Medical: PharmGuard Toolbox Version 1.5 Smiths Medical: CADD-Solis Medication Safety Software		

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Access Point (AP)	Cisco: Aironet 1600 Series AP (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 • supports security protocols: IEEE 802.11i (WPA2), EAP-TLS 	PR.AC-5, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Wireless LAN [Local Area Network] Controller (WLC)	Cisco: WLC 8.2.111.0	<ul style="list-style-type: none"> • AP joins a WLC to form a Control and Provisioning of Wireless Access Points protocol (CAPWAP) tunnel • uses Identity Services Engine (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 networks, wireless networks, and VPNs. It gathers this information based on what's actually 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 a 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: Adaptive Security Appliance (ASA)	<ul style="list-style-type: none"> • delivers network integrity protection • is used as an external firewall for connecting to the internet for guest network • is 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

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Switch	Cisco: Catalyst 3650 Switch	<ul style="list-style-type: none"> • provides port-level controls, port blocking, and virtual local area network (VLAN) segmentation 	PR.AC-5, PR.DS-1, PR.DS-2, DE.CM-1, DE.CM-3
Endpoint Protection	Symantec: Symantec Endpoint Protection (SEP)	<ul style="list-style-type: none"> • provides intrusion prevention, uniform resource locator (URL), and firewall policies • provides application behavioral controls • provides device control to restrict access • provides antivirus file protection • provides behavioral monitoring • provides file reputation analysis 	DE.CM-1, DE.CM-3, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1
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 (IoCs) across the entire environment • blacklists or whitelists files and URLs once they are identified as malicious • can be integrated with a third-party security information and events management (SIEM) tool 	DE.CM-1, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Data Center Security	Symantec: Data Center Security: Server Advanced (DCS:SA)	<ul style="list-style-type: none"> • out-of-the-box host intrusion detection system (HIDS) and host intrusion prevention system (HIPS) 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 HIPS controls restrict application and operating system behavior by using policy-based least-privilege access control • prevents file and system tampering • provides application and device control by locking down “configuration” settings, file systems, and the use of removable media 	DE.CM-1, DE.CM-4, PR.DS-1, PR.DS-2, DE.AE-1
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

Component	Specific Product	Function	NIST Cybersecurity Framework Subcategory
Physics-Based Integrity Assessment	PFP: pMon 751 and P2Scan	<ul style="list-style-type: none"> • baselines the device execution behavior • detects cyber attacks in hardware and software • detects tiny anomalies in analog side-channel patterns (e.g., power consumption, electromagnetic emissions) to instantly catch attacks, thereby providing an early warning that a device has been tampered with • integrity assessment uses side channel 	DE.AE-1, DE.CM-4
Certificate Authority Service	DigiCert: Certificate Authority	<ul style="list-style-type: none"> • provides a certificate authority service 	Access Control (PR.AC) PR.DS-2
Certificate Management / Provisioning	Intercede: MyID®	<ul style="list-style-type: none"> • serves as a device provisioner 	ID.AM-1, ID.AM-5
Risk Assessment	Clearwater: IRM Pro™ IRM Analysis™	<ul style="list-style-type: none"> • provides a tool for conducting risk assessments that focus on healthcare compliance and cyber risk management 	ID.RA-1
	Medical Device Innovation, Safety & Security Consortium (MDISS): Medical Device Risk Assessment Platform (MDRAP™)	<ul style="list-style-type: none"> • provides a tool for conducting risk assessments that focus on medical devices 	

5 Architecture

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

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

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

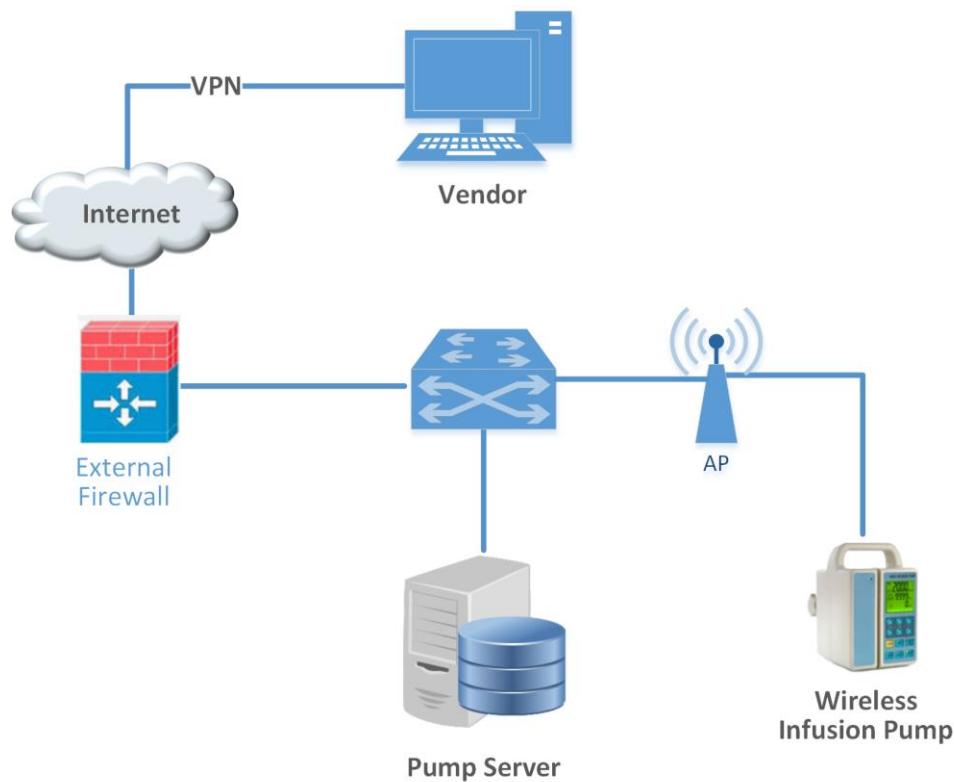
Medical device manufacturers are subject to regulatory practices by the FDA, and may tend to focus on the primary function of the pump (i.e., assurance that the pump delivers fluids of a certain volume and defined flow rates, consistent with needs that providers may have to ensure safe and appropriate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

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

5.1 Basic System

A basic wireless infusion pump ecosystem includes a wireless infusion pump, a pump server, a network consisting of an AP, a firewall, and a VPN to a manufacturer (Figure 5-1).

Figure 5-1 Basic System



5.2 Data Flow

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

- modifying the drug library
- performing software updates
- remotely managing the devices
- auditing the data flow processes

Infusion pumps may also include other advanced features, such as auto-programming to receive patient prescription information and to record patient treatment information to the patient's EHR.

5.3 Cybersecurity Controls

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

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

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

We used the following cybersecurity controls:

- network controls
- pump controls
- pump server controls
- enterprise-level controls

5.3.1 Network Controls

Proper network segmentation or network zoning is essential to developing a strong cybersecurity posture [32], [33], [34], [35], [42]. Segmentation uses network devices, such as switches and firewalls, to split a large computer network into subnetworks, each referred to as a *network segment* [41]. Network segmentation not only enhances network management, but also improves cybersecurity, allowing for the separation of networks based on network security requirements driven by business needs or asset value.

The architecture designed for this build uses Cisco's solution architecture as the baseline for demonstrating how the network can be used to provide multi-tiered protection for medical devices when exchanging information with the outside world during the operation involving network communication. The goal of this architecture design is to provide countermeasures to mitigate challenge areas identified in the assessment process. In our use-case solution, segmentation and defense-in-depth are the security models that we used as security measures to build and maintain secure device infrastructure. This section provides additional details on how to employ security strategies to achieve the target security characteristics for securing wireless infusion pumps.

5.3.1.1 Segmentation/Zoning

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

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

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

At a high level, each zone is implemented as a VLAN with a combination firewall/router Cisco ASA device connecting it to the rest of the enterprise through a backbone network, referred to as the core network [43], [44], [45]. Segments may consist of physical or virtual networks. For simplicity and convenience, we implemented subnets that correspond exactly to VLANs. The routing configuration is the same for each subnet, but the firewall configuration may vary depending on each zone's specific purpose. An external router/firewall device is used to connect the enterprise and guest network to the internet.

Segmentation is implemented via a VLAN by using Cisco switches. The following subsections provide a short description of each segment and the final network architecture.

5.3.1.1.1 Core Network Zone

Our reference architecture implements a core network zone that consists of the equipment and systems used to establish the backbone network infrastructure. The external firewall/router also has an interface connected to the core enterprise network, just like other firewall/router devices in the other zones. This zone serves as the backbone of the enterprise network and consists only of routers connected by switches. The routers automatically share internal route information with each other via authenticated Open Shortest Path First (OSPF) to mitigate configuration errors as zones are added or removed.

5.3.1.1.2 Guest Network Zone

Hospitals often implement a guest network that allows visitors or patients to access internet services during their visit. As shown in Figure 5-2 ([Section 5.3.1.1.10](#)), network traffic here tends not to be clinical in nature, but is offered as a courtesy to hospital visitors and patients to access the internet. Refer to [Section 5.3.1.5](#), External Access, for additional technical details.

5.3.1.1.3 Business Office Zone

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

5.3.1.1.4 Database Server Zone

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

5.3.1.1.5 Enterprise Services Zone

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

5.3.1.1.6 Clinical Services Zone

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

5.3.1.1.7 Biomedical Engineering Zone

The biomedical engineering zone establishes a separate area that enables a biomedical engineering team to manage and maintain systems, such as medical devices, as shown in Figure 5-2 ([Section 5.3.1.1.10](#)). This zone consists of all equipment needed to provision and maintain medical devices. In the case of wireless infusion pumps, this is where the pump management servers are hosted on the network.

5.3.1.1.8 Medical Device Zone

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

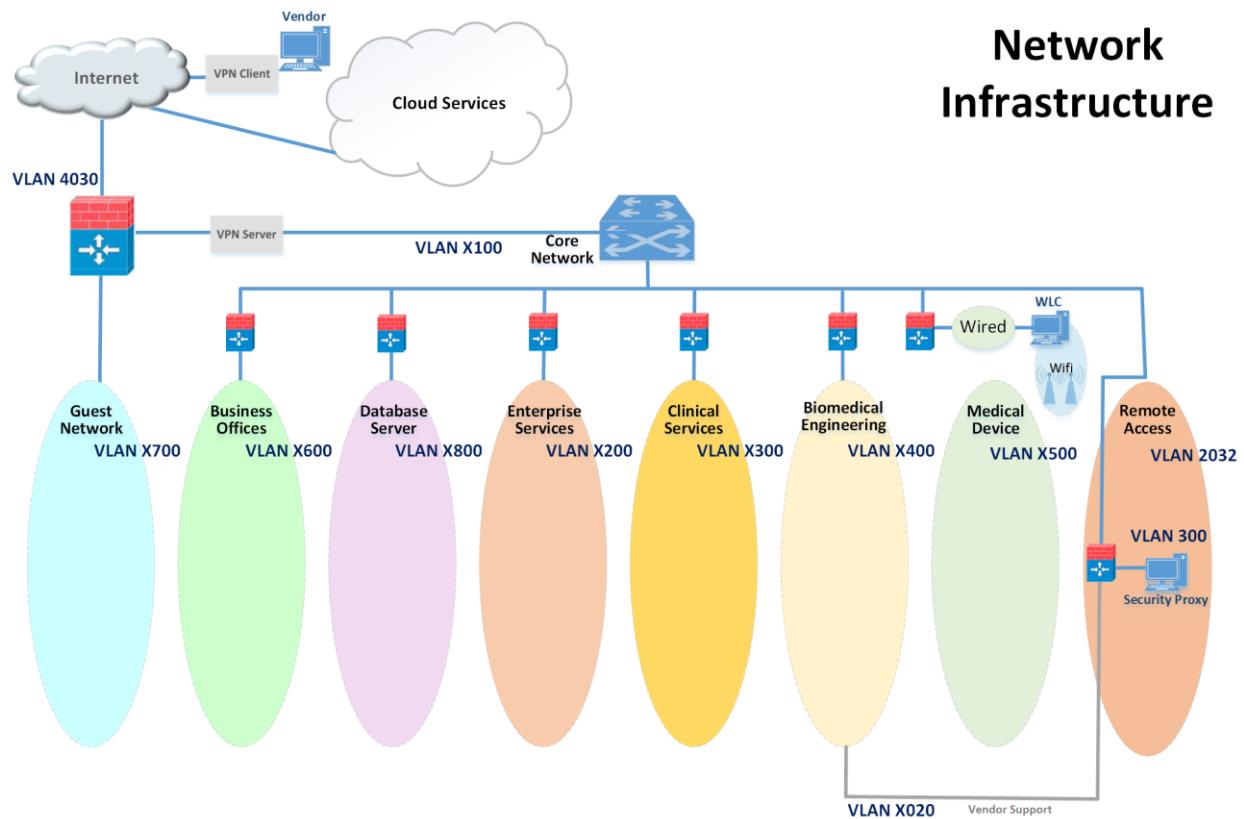
5.3.1.1.9 Remote Access Zone

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

5.3.1.1.10 Final Network Architecture

Figure 5-2 shows the interconnection of all components and zones previously described. It also illustrates the connection to vendor and cloud services via the internet. The VLAN numbers that are shown in Figure 5-2 are the VLAN identifiers used in the lab; however, these numbers may vary on actual healthcare enterprise networks.

Figure 5-2 Network Architecture with Segmentation

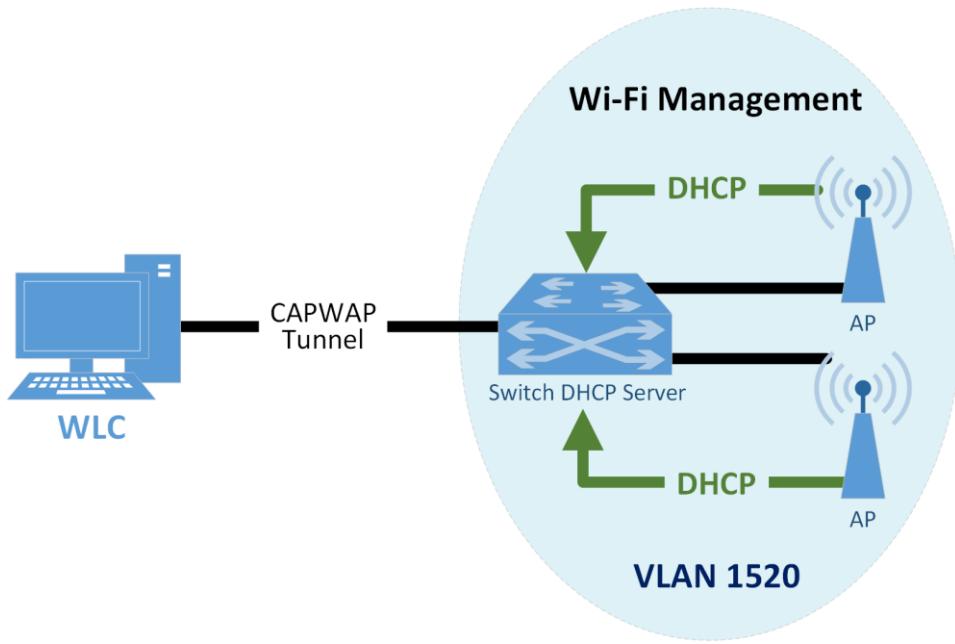


5.3.1.2 Medical Device Zone's Wireless LAN

The Wi-Fi management network is different, in that it does not have a firewall/router that connects directly to the core network, as shown in Figure 5-3. This is a completely closed network used for the management and communication between the Cisco Aironet wireless AP and the Cisco WLC. The WLC is the central point where wireless Service Set Identifiers (SSIDs), VLANs, and WPA2 security settings are managed for the entire enterprise [8], [17], [32], [33], [34], [35], [42], [46], [47], [48].

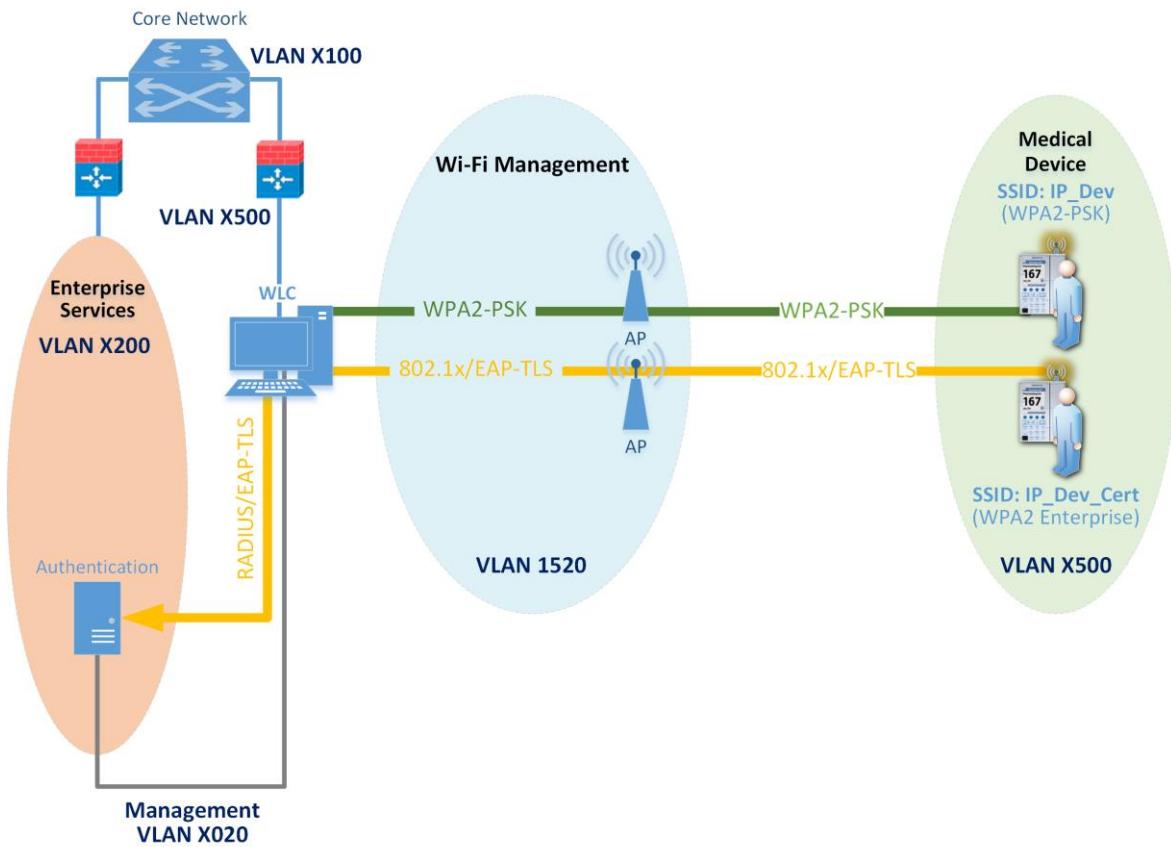
Two SSIDs were defined: IP_Dev and IP_Dev Cert. IP_Dev uses WPA2-PSK, and IP_Dev Cert uses WPA2-Enterprise protocols. In an actual HDO, two WLCs should be configured for redundancy. Initially, the wireless APs configure themselves for network connectivity, like any other device using Dynamic Host Configuration Protocol (DHCP) from the switch DHCP server (see the green line in Figure 5-3). The switch also sends DHCP Option 43, which provides the Internet Protocol (IP) address of the WLC. The AP then connects to the WLC to automatically download firmware updates and wireless configuration information. Finally, the CAPWAP tunnel is formed to encrypt wireless traffic (see the black line in Figure 5-3). The traffic is then routed to the enterprise network via the WLC [27], [36], [44], [49].

Figure 5-3 Wi-Fi Management



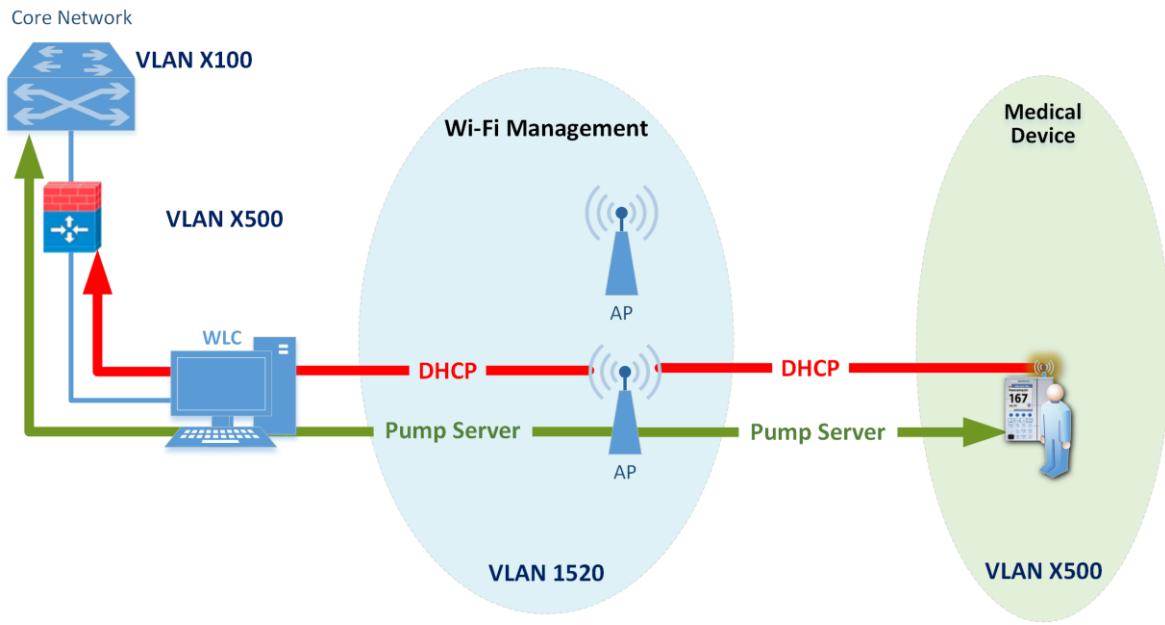
When a device first connects to the Wi-Fi network, it needs to authenticate with either the agreed-upon PSK or certificate. The authentication process is tunneled from the AP back to the WLC, as shown in Figure 5-4. In the case of a PSK, the WLC verifies that the client key matches (see the green line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

Figure 5-4 Wi-Fi Authentication



Once authentication is complete, typical network client activity is allowed. Figure 5-5 shows how DHCP is used to contact the router to obtain network configuration information for the device (see the red line in Figure 5-5). Once the network is configured, the infusion pump will attempt to connect to its provisioned pump server address on the enterprise network in the biomedical engineering zone (see the green line in Figure 5-5).

Figure 5-5 Wi-Fi Device Access



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

5.3.1.3 Network Access Control

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

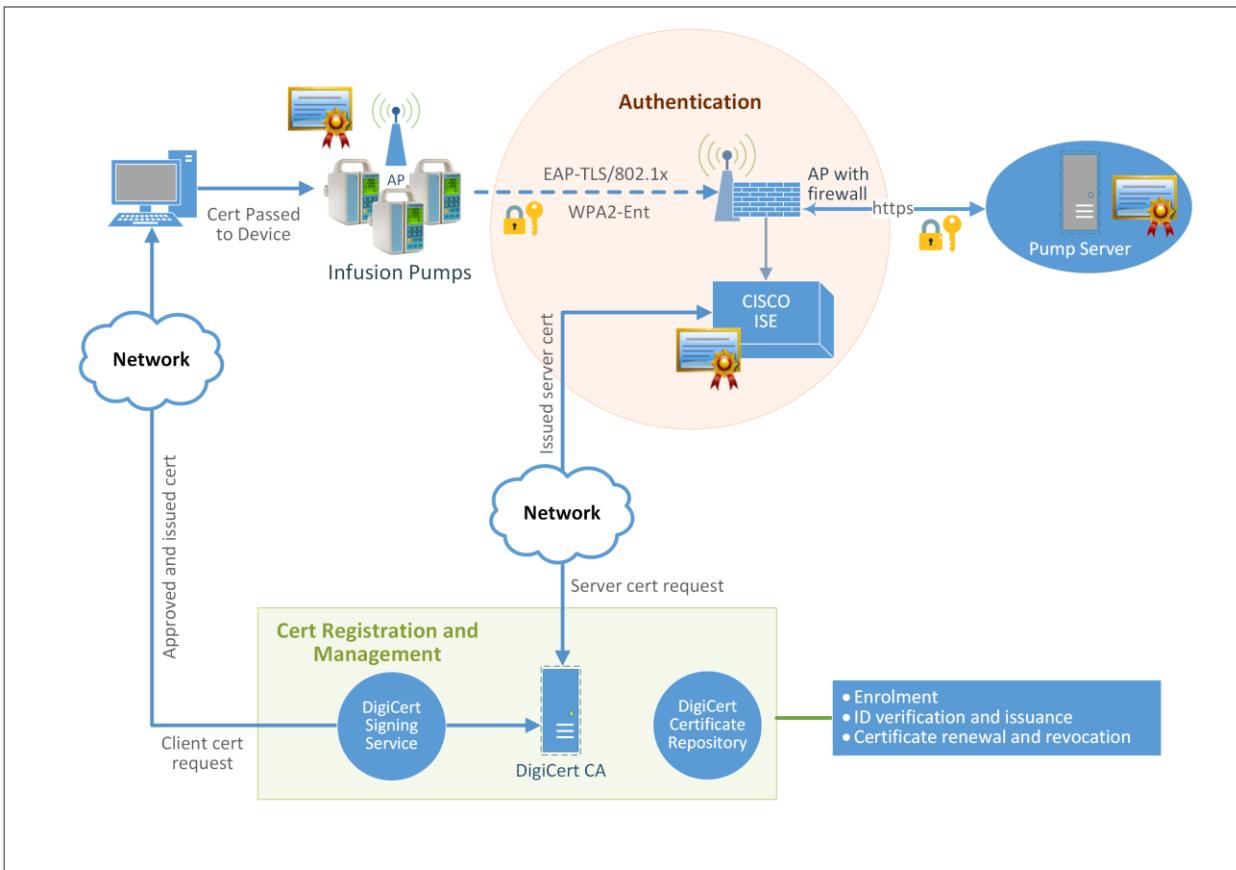
Before we describe network access controls, it is important to discuss each pump's wireless protection protocol. There are three available wireless protection protocols (WEP, WPA, and WPA2). We also describe in-depth options for WPA2-PSK. Finally, we describe options for WPA2 across the HDO enterprise.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

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

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

Once WPA2 is selected as the appropriate wireless protection protocol, certificates may be issued to authenticate infusion pumps by using 802.1x/EAP-TLS mode, as illustrated in Figure 5-6 [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [42], [46], [47], [48], [49].

Figure 5-6 Network Access Control



Certificate issuance involves the following three stages, which are outlined by the green and orange shaded objects in Figure 5-6:

1. Certificate Registration

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

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

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

2. Authentication

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

3. Certificate Management

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

The detailed process for setting up the 802.1x network authentication for pump and pump server communication is documented in the How-To portion of the guide (*NIST SP 1800-8C*).

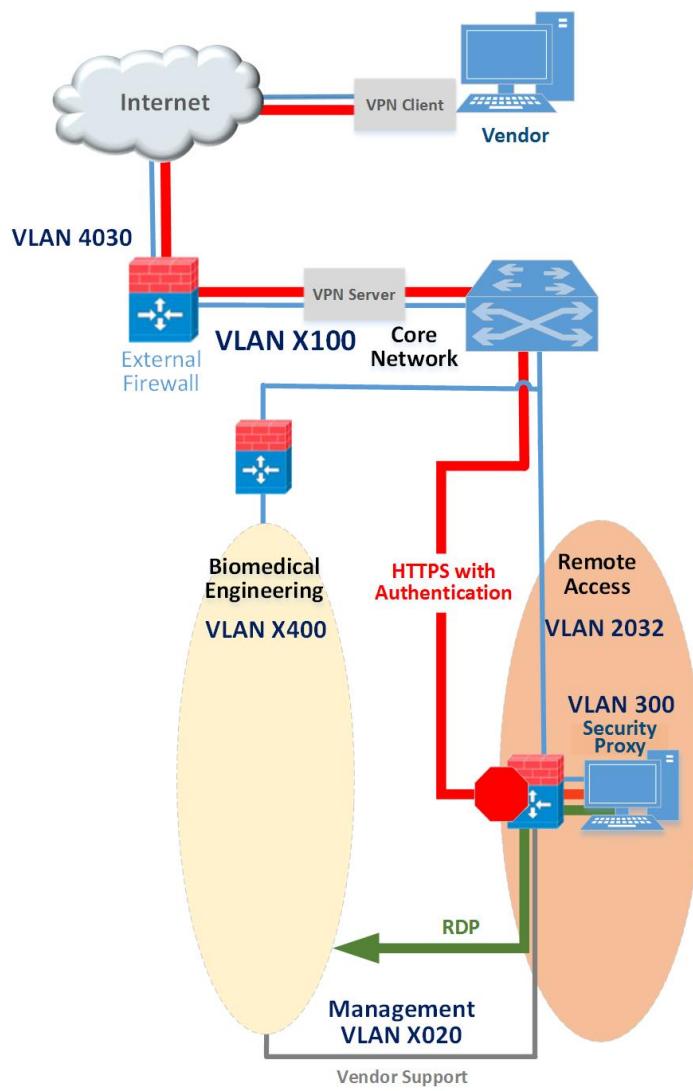
5.3.1.4 *Remote Access*

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

Communication using TDi ConsoleWorks for vendor access to products does not require the installation of software agents to establish connections for managing and monitoring targeted components. Established connections are persistent to facilitate IT operations, enforce security, and maintain comprehensive audit trails. All information collected by ConsoleWorks is time-stamped and digitally signed to ensure information accuracy, empower oversight, and meet compliance requirements. Through a standard web browser, ConsoleWorks can be securely accessed from any geographical location, eliminating the need for administrators and engineers to be locally present to perform their work.

Remote access is only allowed through a specific set of security mechanisms. This includes using a VPN client at the network layer, as shown in Figure 5-7, for vendors to authenticate to the VPN server [43], [44], [50].

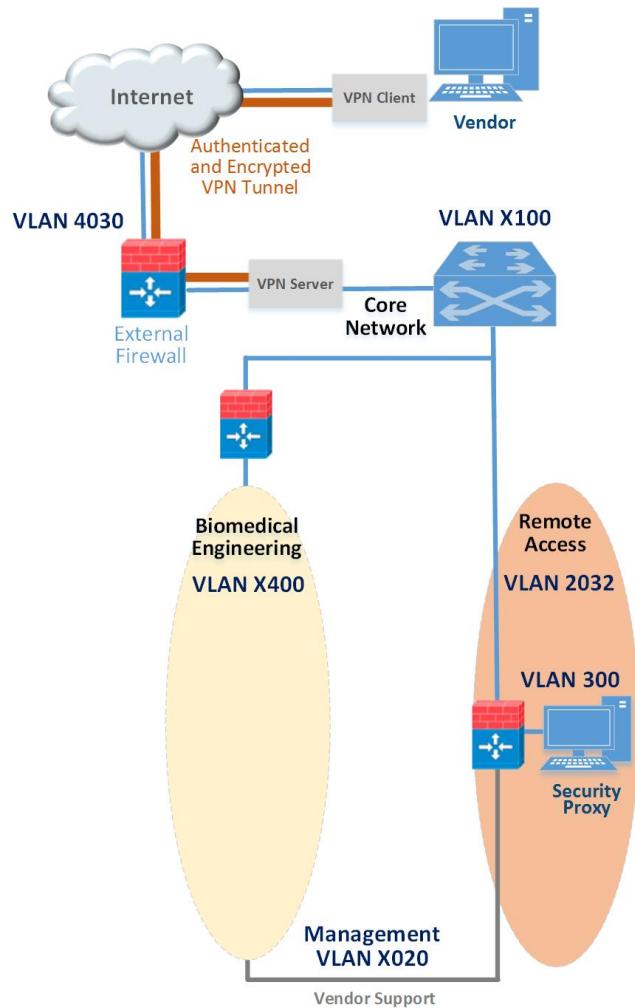
Figure 5-7 Remote Access VPN



After the VPN connection is established at the application layer, the security proxy will restrict who can access certain resources within the enterprise network, as depicted in Figure 5-8. Vendors also authenticate to the Hypertext Transfer Protocol Secure (HTTPS)-based security proxy (see the red line in Figure 5-7). Based on the vendor's role, the security proxy will facilitate a Remote Desktop Protocol (RDP) connection to equipment in the biomedical engineering zone via the vendor support network (see the green line in Figure 5-7). The credentials that are used to authenticate the RDP connection are stored by the security proxy and are not disclosed to the vendor.

The remote access firewall/router is configured so that direct access between the VPN and vendor support is denied and the only allowed path is through the security proxy (see the stop sign in Figure 5-7). Additionally, the firewall/router can further restrict what is accessible at the network layer from the security proxy. The security proxy is granted access to the internet to support patching and to email alerts. The public IP address of the external firewall is configured to forward VPN traffic to the IP address of the VPN server [35], [43], [44], [45], [46], [48], [50], [51].

Figure 5-8 Remote Access

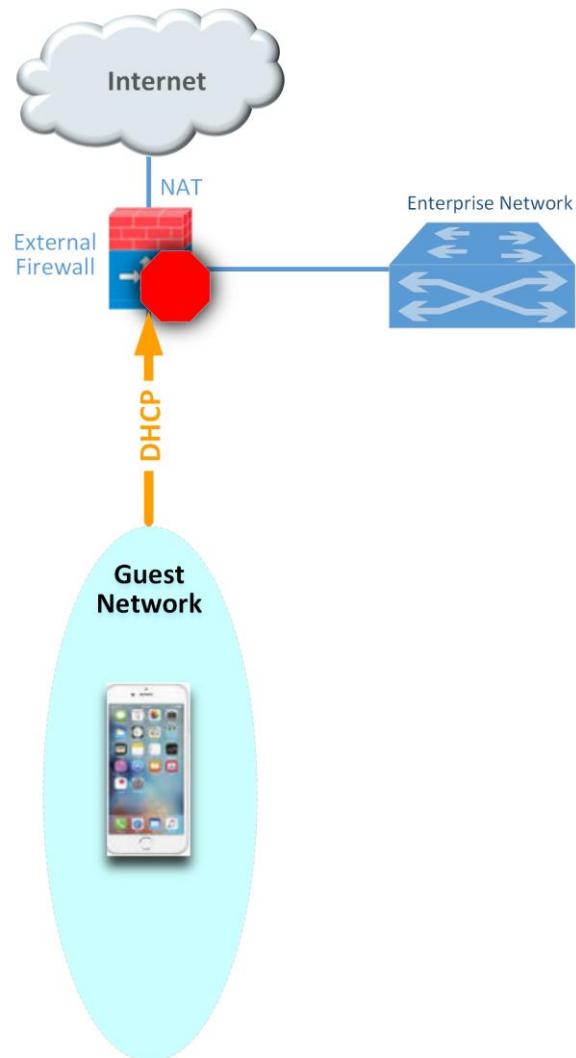


5.3.1.5 External Access

A guest network allows visitors or patients to access internet services during their visit. As explained in [Section 5.3.1.1.2](#), the work traffic tends not to be of a clinical nature, but is offered as a courtesy to hospital visitors and patients to access the internet. The external firewall marks the boundary between

the enterprise and the internet. As shown in Figure 5-9, this is the only point in the network where network address translation (NAT) is used. Additionally, the guest network for personal devices connects to the internet through the external firewall. The guest network is configured such that traffic cannot go between the enterprise and guest networks—only out to the internet. This is denoted by the stop sign in Figure 5-9. The external firewall is configured to provide the necessary services for guest users to use the internet, such as DHCP, which allows dynamic addressing for anyone. Typically, consumer equipment is connected here, such as smart phones, tablets, and personal entertainment systems (Figure 5-9) [45].

Figure 5-9 External



5.3.2 Pump Controls

Wireless infusion pumps have the following controls:

- endpoint protection
- hardening
- data protection

5.3.2.1 *Endpoint Protection*

Traditional security relies on the network border to provide security protection to its internal nodes, using security technologies, such as application firewalls, proxy gateways, centralized virus scan, and network IDS and IPS. The challenge faced here, however, is that medical devices, such as wireless infusion pumps, may not have the capability to have third-party tools installed or deployed to effectively provide control. As such, endpoint protection is applied to that equipment where possible. This may limit endpoint protection controls to servers or workstations that may operate in the hospital infrastructure. Nodes, such as networked medical devices, should participate in their own security. Otherwise, the device may become the weakest element in the enterprise and present a risk to the entire HDO network.

To avoid the single point of failure caused by an unsecured node, every system should have an appropriate combination of local protections applied to it. These protections include code signing, anti-tampering, encryption, access control, whitelisting, and others. Controls are layered across a technology stack, with the intent to improve the overall cybersecurity posture, recognizing that there may be limitations to applying a full set of controls for each node.

5.3.2.2 *Hardening*

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

Hardening may include the following actions:

- disabling unused or unnecessary communication ports and services
- changing manufacturer default administrative passwords
- securing remote APs, if there are any

- confirming that the firmware version is up-to-date
- ensuring that hashes or digital signatures are valid

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

Hardening or modifying devices, configurations, or settings should be performed based on guidance from the manufacturer. Wireless infusion pumps are medical devices that adhere to FDA regulation, where the manufacturer has validated appropriate functionality based on a defined configuration. Identified vulnerabilities should be disclosed to the manufacturer, who may advise on appropriate mitigation approaches and provide patches, fixes, and updates where appropriate.

5.3.2.3 Data Protection

The two primary reasons for data protection are confidentiality and integrity. Medical devices may contain patient data, such as the patient's name, MRN, gender, age, height, weight, procedure number, medication and treatment information, or other identifiers that may constitute PHI. PHI must be appropriately protected (e.g., through encryption or other safeguard measures that would prevent unauthorized disclosure of such information).

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

5.3.3 Pump Server Controls

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

Because pump servers connect to infusion pumps to deliver and receive infusion-related information, it is also important to secure the infusion pump server and its associated applications, databases, and communication channels.

5.3.3.1 User Account Controls

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

- changing factory default passwords
- enforcing password policies
- assigning each user's access level by using the least-privilege principle
- if supported, using centralized access management, such as LDAP, for user account management at the enterprise level APT:
- configuring automatic logoff

5.3.3.2 Communication Controls

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

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

5.3.3.3 Application Protection

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

- trusted applications
- stronger access control mechanisms for pumps and pump servers
- better key management
- application whitelisting
- sandboxing applications
- performing code-signing verification for newly installed software

- applying the latest patches and software updates
- encrypting message data in transit or data at rest

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

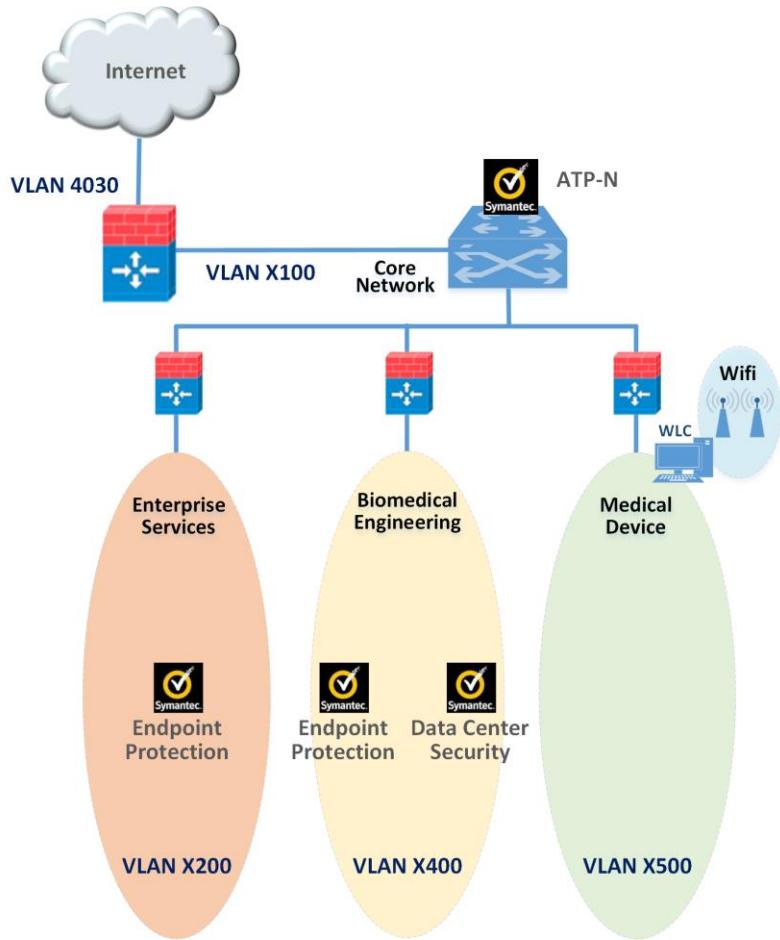
- DCS:SA
- SEP
- APT:N

Each of these Symantec products provides protections for components in the enterprise systems in different levels. With pre-built policies, the DCS:SA server that is installed can provide out-of-the-box HIDS and HIPS by monitoring and preventing suspicious server activities on pump servers. The use of DCS:SA also provides the host firewall service for controlling inbound and outbound network traffic to and from a protected server. Using DCS:SA, the configuration settings, files, and file systems in the pump server can be locked down using policy-based least-privilege access controls to restrict application and operating-system behavior and to prevent file and system tampering.

Like DCS:SA, SEP provides similar protection for endpoint devices and servers. SEP features in-memory exploit mitigation and antivirus file protection to block malware from infecting protected endpoint servers. This will reduce the possibility of zero-day exploits on popular software that may not have been properly patched or updated. To protect endpoint servers, an SEP agent must be installed on servers.

ATP:N can provide network-based protection of medical device subnets by monitoring internal inbound and outbound internet traffic. It can also be used as a dashboard to gain visibility to all devices and all network protocols. In addition, if ATP:N is integrated with the SEP, ATP:N can then monitor and manage all network traffic from the endpoints and provide threat assessments for dangerous activity to secure medical devices on an enterprise network. The use of these Symantec security products is depicted in Figure 5-10. As depicted, the ATP:N will inspect all traffic going through the core network switch via port mirroring between the enterprise services, biomedical engineering, and medical device zones. Wired traffic within each zone is also inspected via port mirroring on the switches used in those zones.

Figure 5-10 Pump Server Protection



5.3.4 Enterprise-Level Controls

5.3.4.1 Asset Tracking and Inventory Control

Medical asset management includes asset tracking and asset inventory control. Asset tracking is a management process used to maintain oversight of the equipment, using anything from simple methods (such as pen and paper), to record equipment, to more-sophisticated information technology asset management (ITAM) platforms. HDOs can use asset tracking to verify that a device is still in the possession of the assigned, authorized users. Some more-advanced tracking solutions may provide service for locating missing or stolen devices.

Inventory management is also important throughout a medical device's life cycle. Inventory tracking should not be limited to hardware inventory management. It should also be expanded to include software, software versions, and data stored and accessed in the devices, for security purposes. HDOs

can use this type of inventory information to verify compliance with security guidelines and to check for exposure of confidential information to unauthorized entities.

5.3.4.2 Monitoring and Audit Controls

Logging, monitoring, and auditing procedures are essential security measures that can be used to help HDOs prevent incidents and provide an effective response when a security breach occurs. The activities can include:

- logging - recording events to appropriate logs
- monitoring - overseeing the events for abnormal activities, such as scanning, compromises, malicious code, and DoSs in real time
- auditing - reviewing and checking these recorded events to find abnormal situations or to evaluate if the applied security measures are effective.

By combining the logging, monitoring, and auditing features, an organization will be able to track, record, review, and respond to abnormal activities, and provide historical records when needed.

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

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

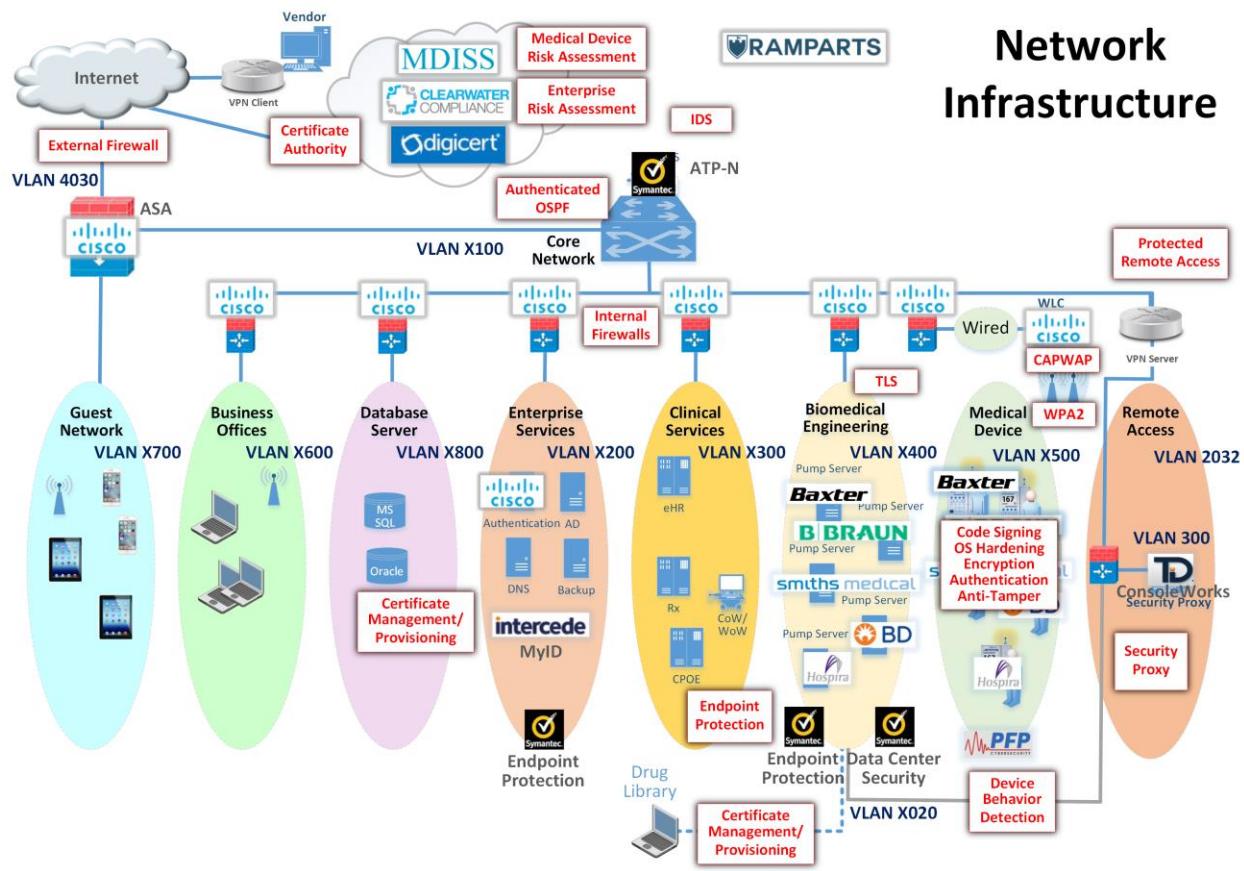
Each system is monitored for compliance with a secure configuration baseline. Each system is also monitored for risks to known good, secure configurations by vulnerability scanning tools. In our project, the Cisco AP, the Cisco ISE as the RADIUS authentication server, the TDi VendorNet, and the pump servers from each vendor, are all equipped with proper monitoring and logging capabilities. Real-time monitoring for events happening within these systems can be analyzed and compared to the baseline. If any abnormal behavior occurs, it can be detected. The auditing of data was considered out of scope for this reference design because the absence of an actual data center made auditing behavior impractical.

5.4 Final Architecture

The target architecture, depicted in Figure 5-11, indicates the implementation of network segmentation and controls as described by this practice guide. Segmentation identified nine zones, ranging from the guest network zone to the medical device zone, and includes zones for the Wi-Fi infrastructure and the core network infrastructure. The zoned concept implements firewall/router devices to enforce segmentation, with the firewall enforcing limited trust relationships between each zone. For example,

access between the biomedical engineering zone and the medical device zone is limited to only the ports identified by the vendor and the associated pump server. Noted in the diagram (Figure 5-11) are processes that have impact on the overall architecture. Security controls are implemented to enforce encryption on network sessions. For Wi-Fi, leveraging standard protocols, such as WPA2-PSK and WPA2 Enterprise, created a secure channel for the pumps to communicate with the APs, and to use TLS to secure the communication channel from the pumps to the server.

Figure 5-11 Target Architecture

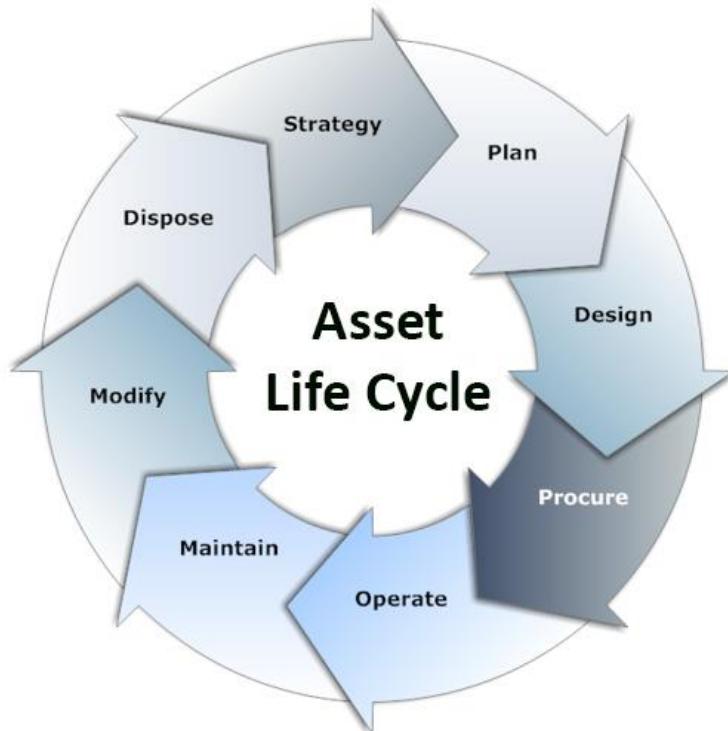


6 Life-Cycle Cybersecurity Issues

Configuration management throughout a device's life cycle is a key process that is necessary for the support and maintenance of medical devices [3]. NIST SP 1800-5: *IT Asset Management* discusses ITAM, and, although the focus of the document pertains to financial services, similar challenges exist in healthcare [52]. Establishing a product-life-cycle management program addresses a few of the risks noted in previous sections of this guide, and should be considered as part of a holistic program for managing risks associated with infusion pump deployments.

Figure 6-1 illustrates a typical life cycle for an asset, and this model can be applied to medical devices. The subsections below discuss the essential cybersecurity activities that should occur during specific phases of the asset life cycle.

Figure 6-1 Asset Life Cycle [53]



6.1 Procurement

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

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

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

Manufacturers maintain a document referred to as the MDS2 (*Manufacturer Disclosure Statement for Medical Devices*) that an HDO may review, enabling the HDO to determine possible vulnerabilities and risks [54]. Hospital purchasers may also determine if vulnerabilities exist in the proposed equipment by reviewing the FDA-hosted MAUDE (Manufacturer and User Facility Device Experience) database.

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

Performing research and risk analysis during the phases leading into procurement will allow HDOs to make informed decisions. For further reference, we note that the Mayo Clinic has produced a best-practice document that discusses procurement [55].

6.2 Operation

After hospitals procure their equipment, they onboard it during the Operate and Maintain phases. Equipment purchasers should apply asset management processes (e.g., asset tagging and entry into a configuration management database or some other form of inventory tracking), and should have standard baseline configurations implemented. Wireless infusion pumps may need to be configured to connect to a hospital's Wi-Fi network (medical device zone, as depicted in [Section 5.3.1.2](#), Medical Device Zone's Wireless LAN) and implement digital certificates to allow for device authentication.

As noted above, hospitals should implement some type of configuration management database or asset inventory that captures granular information about the device. Implementing an ITAM mechanism enables the hospital to have visibility into their infusion pump deployment, with captured information

that describes the make/model, firmware, operating system, software versions, the applied configuration along with change history, and the physical location within the hospital. Regular maintenance of the ITAM would reduce risks, for example, that may emerge based on loss/theft, as well as provide a central knowledge repository that allows the hospital to coordinate any required maintenance or refresh.

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

6.3 Maintenance

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

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

In addition to identifying patch frequency, organizations must be aware of likely vulnerabilities and the risks that they introduce into the enterprise, and then decide whether a patch should be applied. NIST SP 800-40, *Guide to Enterprise Patch Management Technologies* [56], discusses the importance of patch management, as well as the challenges.

6.4 Disposal

The Dispose phase of the ITAM life cycle comes into play when products reach their end of life and are removed from hospital service. Wireless infusion pumps have increased in sophistication and in the information that each device may use, process, or store. The information found on pumps and related equipment may include sensitive information or information that may be regarded as PHI. As such, hospitals should seek to implement mechanisms to ensure that any sensitive information and PHI are removed from all storage areas that a pump or its system components may maintain. Practices to remove that information may be found in NIST SP 800-88, *Guidelines for Media Sanitation* [26].

7 Security Characteristics Analysis

We identified the security benefits of the reference design, how they map to NIST Cybersecurity Framework Subcategories, and the mitigating steps to secure the reference design against potential new vulnerabilities [10], [14].

7.1 Assumptions and Limitations

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

7.2 Application of Security Characteristics

Using the NIST Cybersecurity Framework Subcategories to organize our analysis allowed us to systematically consider how well the reference design supports specific security activities, and provided additional confidence that the reference design addresses our use-case security objectives. The remainder of this subsection discusses how the reference design supports each of the identified Cybersecurity Framework Subcategories [10].

7.2.1 Supported NIST Cybersecurity Framework Subcategories

The reference design focuses primarily on the *Identify* and *Protect* Function areas (their Subcategories) of the NIST Cybersecurity Framework. Specifically, the reference design supports the following Subcategories:

- three Subcategories in the NIST Cybersecurity Framework *Identify* Function area, under the Categories of Asset Management, Business Environment, and Risk Assessment
- Subcategories from each Category of the NIST Cybersecurity Framework *Protect* Function area, except for the Awareness and Training Categories

We discuss these NIST Cybersecurity Framework Subcategories in the following subsections.

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

To address this Subcategory of the *Identify* Function, we conducted an asset inventory as part of the risk management process. For this project, we identified assets and entered them into the Clearwater Compliance IRM|Analysis™ tool. This risk analysis tool categorized project resources into types of assets. Additionally, it characterized the system, enabling us to address the criticality of our resources. Our

project only partially satisfies the Resources subcategory, as we focused on technical solutions and did not write a business impact assessment or business continuity plan.

7.2.1.2 ID.BE-1: The Organization’s Role in the Supply Chain Is Identified and Communicated

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

7.2.1.3 ID.RA-1: Asset Vulnerabilities Are Identified and Documented

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

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

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

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

Pump manufacturers who may need to reach a device for maintenance or troubleshooting can gain access only into a VendorNet zone, from which they can access pumps and pump servers, but not other

zones in the enterprise. Our example implementation uses ConsoleWorks for authentication, role-based access control, and recording system management actions of remote vendor activity.

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

This NIST Cybersecurity Framework Subcategory is supported for the pumps and pump servers with DCS:SA. The configuration settings, files, and file systems in the pump server are restricted, thereby implementing policy-based least-privilege access control. DCS:SA restricts application and operating-system behavior and prevents unauthorized users from tampering with files and systems.

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

7.2.1.6 PR.AC-5: Network Integrity Is Protected (e.g., network segregation, network segmentation)

Network segmentation is a key function of this reference design. Segregating the core network, guest network, business office, database server, enterprise services, clinical services, and biomedical engineering zones from the medical device zone reduces the risk of medical devices being negatively impacted from malware or an exploit in another zone. Using a combination firewall/router device to segregate the zones also limits risk to the enterprise, should a vulnerability be exploited within the medical device zone.

7.2.1.7 PR.DS-2: Data-in-Transit Is Protected

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

7.2.1.8 PR.DS-6: Integrity Checking Mechanisms Are Used to Verify Software, Firmware, and Information Integrity

This NIST Cybersecurity Framework Subcategory is supported with server and agent products to monitor and lock-down configuration settings, files, and file systems in the pump server by using the policy-based least-privilege access control. This limits the applications and operating system to the expected behavior, and reduces the likelihood of digital tampering with the system.

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

A mature cybersecurity program follows a documented secure baseline for traditional information technology components and medical devices. This NCCoE project has implemented hardening for each component used in the build, and has documented the steps taken. This initial step produces a secure baseline configuration. Because this project uses five different types of wireless infusion pumps, the baseline is of limited use; however, in a healthcare organization with many medical devices and multiple biomedical and IT professionals, it is essential to develop and implement a baseline configuration for vulnerability management.

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

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

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

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

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

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

This NIST Cybersecurity Framework Subcategory is supported by the Symantec IDS component of the reference design. This tool identifies, monitors, and reports anomalous network traffic that may indicate a potential intrusion. Endpoint protection implements policies for the expected behavior, and alerts when activities occur outside the usual patterns.

7.3 Security Analysis Summary

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

8 Functional Evaluation

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

The subsequent subsections explain the functional tests in more detail, and list the procedures for each of the functional tests.

8.1 Functional Test Plan

Table 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 the 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 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 the ATP:N to ensure that it follows defined policies	The URLs in the blacklist are blocked. The URLs in the whitelist are allowed.

Test Case	Purpose	Desired Outcomes
WIP-5: Protected Remote Access	Test the effectiveness of the remote access controls	The vendor can access only what has been granted for access with the correct privileges.
WIP-6: Pump and Pump Server Network Connection	Confirm that the installation and configuration of pumps and pump servers are fully completed	Pumps and pump servers are connected to the network, and pumps communicate to the corresponding pump servers.
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.

8.1.1 Test Case WIP-1

Table 8-2 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 its design. Show that the WIP solution blocks the inbound and outbound traffic of a given zone as per its 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 the medical device zone and the biomedical engineering zone as a test example. Review the port and communication protocol requirements from each tested pump vendor, for the pump and the corresponding pump server. Configure the ASA firewall access list to open only the needed ports and to allow access only to necessary protocols. Everything not explicitly allowed in a rule is denied.

Test Case Name	Network Segmentation
Result	<ol style="list-style-type: none"> 1. 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. 2. Use network discovery scanning tools, such as nmap, to check the open, closed, or filtered ports.

8.1.2 Test Case WIP-2

Table 8-3 Test Case WIP-2

Test Case Name	Data Center Security
Description	Show that the WIP solution detects files that are defined in policy and that 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. • The File and System Tamper Prevention policy is set. • Windows_Baseline_detect_TEST is used as the baseline for server hardening.
Procedure	<p>There are two admin applications for the DCS:SA, the console admin and the portal admin. The console admin is the thick client, and the portal admin is the thin client. The console is used to create and modify the policy, and the portal is used to publish the policy. The portal URL is <code>http://<portal IP Address></code></p> <ol style="list-style-type: none"> 1. Log into the DCS Console. 2. Select the <i>Policy > Work Space > Pump Server</i> folder. 3. Select the Detection tab to show the detection policies. 4. You should see a preinstalled policy: Windows_Baseline_detect_Test. Double-click it to open a detailed policy editing window for configuration. 5. Create a policy for hardening the server, such as “do not allow any file to be installed on the server.” 6. Enable the policy. 7. Publish the policy.
Result	Test to verify that no file is allowed to be installed on the protected server.

8.1.3 Test Case WIP-3

Table 8-4 Test Case WIP-3

Test Case Name	Endpoint Protection / Advance Threat Protection
Description	Show that the WIP solution has the capability to detect a “bad” file and to act (i.e., stop installing that bad file).
Preconditions	<ul style="list-style-type: none">• 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">1. Make sure that the test server has a SEP agent installed and enabled.2. From the server machine, open an Internet Explorer browser, and then type this URL in the browser: http://test.symantecatp.com. This is a test site provided by Symantec, containing some unharful links for testing purposes.3. Click some links, such as antivirus test, from the list to install some suspicious software on the test server.4. The installation should be blocked by the server’s SEP, and the violation incident should be reported in the ATP.5. To view the violation in ATP, log into the ATP server from a browser in a server that can access that sub network, such as the Active Directory server.6. Type this URL in the browser: http://<hostname>.7. View any violation incidents from the ATP to verify that the bad link is blocked.<ol style="list-style-type: none">a. If wanted, one can dive into the details to see to which bad sites it tried to connect.b. Close the open incident report after the review.
Result	To verify that the ATP:N and Symantec deployment and configuration offer the needed security protection to prevent malware installed in a server, and to view the violation, in ATP, log into the ATP server from a browser in a server that can access the network, where the tested server is located. <ol style="list-style-type: none">1. View any violation incidents from the ATP to verify that the bad link is blocked.2. Check the details to see to which bad sites it tried to connect.3. Close open incident report after the review.

8.1.4 Test Case WIP-4

Table 8-5 Test Case WIP-4

Test Case Name	Advanced Threat Protection
Description	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"> • The ATP:N is installed and configured. • Firewall and browser protection rules are defined.
Procedure	<ol style="list-style-type: none"> 1. Log onto a server with ATP:N installed. 2. Access a malicious website. 3. Check the results.
Result	See Test Case WIP-3.

8.1.5 Test Case WIP-5

Table 8-6 Test Case WIP-5

Test Case Name	Protected Remote Access
Description	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, compared to NIST/NCCoE/MITRE staff, to a lab. VendorNet is an NCCoE network created for each lab that is tied to an Active Directory group. This group of vendors 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. • The ConsoleWorks profile and user are created.
Procedure	<ol style="list-style-type: none"> 1. Using public internet, remotely log onto the NCCoE VPN. 2. Log onto ConsoleWorks by using the following URL: https://consoleworks.nccoe.nist.gov. 3. From the graphical menu, select View to view graphical connections. (Note: Each external vendor can only view the resources assigned to them.) 4. Access the granted hosts. 5. Perform the allowed operations as specified. 6. Check the results.

Test Case Name	Protected Remote Access
Result	<ol style="list-style-type: none"> Verify that the vendor can access the associated pump server by using VendorNet and ConsoleWorks. Verify that the vendor can perform the preassigned operational activities. Verify that the vendor <u>cannot</u> perform unauthorized operations, such as some administration task (e.g., adding a new user account). Verify that all activities performed by the external vendor are logged and can be audited as needed.

8.1.6 Test Case WIP-6

Table 8-7 Test Case WIP-6

Test Case Name	Pump and Pump Server Network Connection
Description	Show that the WIP solution establishes the wireless network connection between each vendor's pumps and their corresponding pump server.
Preconditions	<ul style="list-style-type: none"> The wireless router with the pre-shared 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 Enterprise / EAP-TLS for a secure wireless network connection. Cisco ISE is installed and configured with root Certificate Authority installed.
Procedure	<ol style="list-style-type: none"> Turn on the pump. Check the wireless indicator. Check the AP and ISE administration portals for device connection and authentication status. Check the infusion pump server management tool for discovered pumps.
Result	<ul style="list-style-type: none"> Both the AP and ISE portal should indicate that the pumps are successfully connected to the network. The pump server admin portal should indicate that the pump is online and in use. (Note: The way that the pump server portal displays these messages is vendor-dependent.) In the case of WPA2 Enterprise / EAP-TLS wireless access mode, the Cisco ISE should display that the pumps are successfully authenticated.

8.1.7 Test Case WIP-7

Table 8-8 Test Case WIP-7

Test Case Name	Pump and Pump Server Basic Functions
Description	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">• The test results of WIP-6 are successful.• 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 the drug library to its pumps. Listed below is an example procedure used by Hospira to send the drug library to its pump by using the MedNet software server:<ol style="list-style-type: none">a. Log into a MedNet software server.b. Request the download of the drug library to one or more pumps.c. MedNet displays the drug library download status as "Pending."d. MedNet, using MedNet Server, forwards the drug library to the infusion pump selected.e. The pump infuser downloads the drug library from the MedNet server.f. The pump infuser sends a download status update to the MedNet server to indicate that the drug library is successfully downloaded. Wait for installation.g. The pump server displays the download status as "On Pump."h. The operator of the pump powers-down the pump. Choose to install the new drug library when prompted by the infuser.i. The pump sends the update status to MedNet to indicate that the drug library was successfully installed, and a "Completed" download status is displayed.2. From the pump server, send the new version of software updates to its pumps (using a 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.<ol style="list-style-type: none">a. Log into a PharmGuard server.

Test Case Name	Pump and Pump Server Basic Functions
	<ol style="list-style-type: none"><li data-bbox="551 354 1383 418">b. Select Package Deployment from the Asset Management drop-down menu. All previously-deployed packages, if any, are listed.<li data-bbox="551 424 829 456">c. Click Add Package.<li data-bbox="551 466 1258 498">d. Click Browse to navigate to and select the package file.<li data-bbox="551 508 1383 572">e. Click Upload to upload the package. After the package file is read, information about the package is displayed in the package table.<li data-bbox="551 582 1383 646">f. Select the package that you would like to deploy, and then click View/Deploy. The package detailed information is displayed.<li data-bbox="551 656 1090 688">g. Click Deploy to deploy the new package.<li data-bbox="551 699 1356 730">h. Enter the name for the deployment, and specify a start deploy.<li data-bbox="551 741 1253 772">i. Enter the required password, and then click Continue.<li data-bbox="551 783 1405 889">j. After you confirm the package deployment, the name of the newly deployed package displays in the Deployment list with the status of "Active."<li data-bbox="551 899 1383 1005">k. 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	Use 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-specific and manufacturer-specific. For more information, please consult documentation for specific devices.

9 Future Considerations

During our development of this project and practice guide, we did not implement several components; however, these omitted components should be considered. We did not implement a commercially available EHR system. EHRs are often regarded as central within a hospital. Additionally, we did not implement a central asset inventory management tool, or mechanisms to perform malware detection or network monitoring in the medical device zone.

Limitations on control implementation exist based on endpoint capabilities. As infusion pumps continue to evolve as part of an IoMT ecosystem, capabilities, including endpoint encryption and identity and access management may become available, thus further enhancing automated management of the medical device zone. Over the course of time, manufacturers may consider the application of future technologies, or may need to address unanticipated threats in a novel fashion. An update to this practice guide could evaluate these components and other control mechanisms that may become available in the future.

Appendix A Threats

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

- **Targeted attacks:** Targeted attacks are threats involving actors that attempt to compromise the pump and system components directly affecting pump operations, including the pump, 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 virtual private networks (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):** APTs occur when the sophisticated 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 a 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 a degraded availability of equipment, and a possible breach of protected health information (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 Universal Serial Bus [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 by using external ports or interfaces for purposes outside the device's intended use (e.g., to extract data to portable storage media, 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

Some typical vulnerabilities that may arise when using wireless infusion pumps are listed below.

- **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, raise risks associated with a provider's ability to render patient care, and may expose protected health information (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 or updating, or cybersecurity 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, by 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 the device calibration or configuration, or the 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 that healthcare delivery organizations (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 factory-default passcodes. This would overcome a common information-technology (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 a greater access capability than necessary. HDOs should implement processes to limit access to privileged accounts, infusion pumps, and server components, and should 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 to 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 endpoint 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

The recommendations listed below address additional security concerns that are worthy of consideration. If applied, these additional recommendations will likely reduce risk factors or prevent them from becoming greater risks. 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, information technology (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 frequently audited.
- 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 to help staff locate devices that have been moved without documentation.
- Ensure that any Cybersecurity Incident Response Plan includes medical devices.
 - Recently, the Food and Drug Administration (FDA) and the Industrial Control Systems Cyber 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 that 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 II (WPA2). This protocol implements the National Institute of Standards and Technology (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 that 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, including monitoring 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 the exposure of unauthorized devices attempting to access the network. This would identify a bad actor attempting to 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 Acronyms

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

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

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

Appendix E References

- [1] FDA, *Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff*, December 2, 2014.
<http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf> [accessed 2/7/18].
- [2] FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, October 2, 2014.
<http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf> [accessed 2/7/18].
- [3] FDA, *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, December 28, 2016.
<https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm482022.pdf> [accessed 2/7/18].
- [4] Department of Homeland Security (DHS), *Attack Surface: Healthcare and Public Health Sector*, Bulletin 201205040900. <https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf> [accessed 2/8/18].
- [5] IHE PCD Technical Committee, *Medical Equipment Management (MEM): Overview and Profile Roadmap, Version 1*, IHE Patient Care Device (PCD) Technical Framework White Paper, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, 2009.
http://www.ihe.net/Technical_Framework/upload/IHE_PCD_Medical-Equipment-Management_MEM_White-Paper_V1-0_2009-09-01.pdf [accessed 2/7/18].
- [6] IHE PCD Technical Committee, *Medical Equipment Management (MEM): Cybersecurity*, IHE Patient Care Device (PCD) White Paper, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, 2011. http://www.ihe.net/Technical_Framework/upload/IHE_PCD_White-Paper_MEM_Cyber_Security_Rev2-0_2011-05-27.pdf [accessed 2/7/18].
- [7] FDA, *Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software*, January 14, 2005.
<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf> [accessed 2/7/18].
- [8] IHE PCD Technical Committee, *Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide, Revision 1.1*, IHE Patient Care Device (PCD) White Paper, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, 2015.
http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf [accessed 2/7/18].

- [9] AAMI TIR57: 2016: *Principles for medical device security – Risk management*, Advancement of Medical Instrumentation (AAMI) Technical Information Report (TIR)57, AAMI, Arlington, VA, June 5, 2016.
- [10] *Cybersecurity Framework*, National Institute of Standards and Technology [Web site], <http://www.nist.gov/itl/cyberframework.cfm> [accessed 2/7/18].
- [11] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST Special Publication (SP) 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012.
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> [accessed 2/7/18].
- [12] Joint Task Force Transformation Initiative, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication (SP) 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2010. <http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf> [accessed 2/7/18].
- [13] Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication (SP) 800-39, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2011.
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> [accessed 2/7/18].
- [14] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> [accessed 2/7/18].
- [15] International Electrotechnical Commission, *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*, IEC Technical Report (IEC/TR) 80001-2-1 Edition 1.0, 2012. https://webstore.iec.ch/preview/info_iec80001-2-1%7Bed1.0%7Den.pdf [accessed 2/7/18].
- [16] International Electrotechnical Commission, *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*, IEC Technical Report (IEC/TR) 80001-2-2 Edition 1.0, 2012. https://webstore.iec.ch/preview/info_iec80001-2-2%7Bed1.0%7Den.pdf [accessed 2/7/18].

- [17] International Electrotechnical Commission, *Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks*, IEC Technical Report (IEC/TR) 80001-2-3 Edition 1.0, 2012. https://webstore.iec.ch/preview/info_iec80001-2-3%7Bed1.0%7Den.pdf [accessed 2/7/18].
- [18] International Electrotechnical Commission, *Application of risk management for IT-networks incorporating medical devices – Part 2-4: Application guidance – General implementation guidance for healthcare delivery organizations*, IEC Technical Report (IEC/TR) 80001-2-4 Edition 1.0, 2012. https://webstore.iec.ch/preview/info_iec80001-2-4%7Bed1.0%7Den.pdf [accessed 2/7/18].
- [19] International Electrotechnical Commission, *Application of risk management for IT-networks incorporating medical devices – Part 2-5: Application guidance – Guidance on distributed alarm systems*, IEC Technical Report (IEC/TR) 80001-2-5 Edition 1.0, 2014. https://webstore.iec.ch/preview/info_iec80001-2-5%7Bed1.0%7Den.pdf [accessed 2/7/18].
- [20] M. Scholl, K. Stine, J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST Special Publication (SP) 800-66 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2008. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890098 [accessed 2/7/18].
- [21] *HIPAA Regulations*, hipaa survival guide.com (HSG) [Web site], <http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php> [accessed 2/7/18].
- [22] *HIPAA for Professionals*, U.S. Department of Health & Human Services (HHS) [Web site], <http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html> [accessed 2/7/18].
- [23] American National Standards Institute / Association for the Advancement of Medical Instrumentation / International Electrotechnical Commission, *Application of risk management for IT Networks incorporating medical devices – Part 1: Roles, responsibilities and activities*, ANSI/AAMI/IEC 80001-1:2010, 2010.
- [24] American National Standards Institute / Association for the Advancement of Medical Instrumentation / International Organization for Standardization, *Medical devices – Application of risk management to medical devices*, ANSI/AAMI/ISO 14971:2007, 2007 http://www.vcg1.com/files/ANSI_AAMI_ISO_149712007.pdf [accessed 2/7/18].

- [25] IHE PCD Technical Committee, *Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide, Draft for Public Comment Revision 1.0*, IHE Patient Care Device (PCD) White Paper, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, 2015.
http://ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.0_PC_2015-07-01.pdf [accessed 2/8/18].
- [26] A. R. Regenscheid, L. Feldman, and G. A. Witte, *Guidelines for Media Sanitization*, NIST Special Publication (SP) 800-88 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2015. <https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization> [accessed 2/7/18].
- [27] K. Scarfone, M. Souppaya, and M. Sexton, *Guide to Storage Encryption Technologies for End User Devices*, NIST Special Publication (SP) 800-111, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2007.
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf> [accessed 2/7/18].
- [28] D. R. Kuhn, V. C. Hu, W. T. Polk, and S. J. Chang, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, NIST Special Publication (SP) 800-32, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2001.
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf> [accessed 2/7/18].
- [29] E. Barker, W. Barker, W. Burr, W. T. Polk, and M. Smid, *Recommendation for Key Management – Part 1: General (Revision 3)*, NIST Special Publication (SP) 800-57 Part 1 Revision 3, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2012.
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf [accessed 2/7/18].
- [30] E. Barker, W. Barker, W. Burr, W. T. Polk, and M. Smid, *Recommendation for Key Management – Part 2: Best Practices for Key Management Organization*. NIST Special Publication (SP) 800-57 Part 2, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2005.
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf> [accessed 2/7/18].
- [31] E. Barker and Q. Dang, *Recommendation for Key Management: Part 3: Application-Specific Key Management Guidance*, NIST Special Publication (SP) 800-57 Part 3 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2015.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf> [accessed 2/7/18].

- [32] K. Scarfone, D. Dicoi, M. Sexton, and C. Tibbs, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, NIST Special Publication (SP) 800-48 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2008. <http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf> [accessed 2/7/18].
- [33] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST Special Publication (SP) 800-97, National Institute of Standards and Technology, Gaithersburg, Maryland, February 2007. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf> [accessed 2/7/18].
- [34] Institute of Electrical and Electronics Engineers, *Port Based Network Access Control*, IEEE 802.1X, 2001. <http://www.ieee802.org/1/pages/802.1x.html> [accessed 2/7/18].
- [35] Institute of Electrical and Electronics Engineers, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE 802.11, 2017. <http://www.ieee802.org/11/> [accessed 2/7/18].
- [36] U.S. Department of Commerce. *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards (FIPS) Publication 140-2, May 2001. <http://csrc.nist.gov/groups/STM/cmvp/standards.html> [accessed 2/7/18].
- [37] W. T. Polk, K. McKay, and S. Chokhani, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, NIST Special Publication (SP) 800-52 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2014. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf> [accessed 2/7/18].
- [38] *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, DHHS Office for Civil Rights, Washington, DC, 2016. <https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf> [accessed 2/7/18].
- [39] International Organization for Standardization/International Electrotechnical Commission, *Information technology – Security techniques – Information security management systems – Requirements*, ISO/IEC 27001:2013, 2013. <https://www.itgovernance.co.uk/shop/Product/isoiec-27001-2013-iso-27001-standard-isms-requirements> [accessed 2/7/18].
- [40] S. Iddir, P. Thongpradit, E. Sparnon, and I. Singureanu, *IHE Patient Care Device User Handbook, 2011 Edition*, Integrating the Healthcare Enterprise (IHE), Oak Brook, IL, August 2011. http://www.ihe.net/Technical_Framework/upload/IHE_PCD_User_Handbook_2011_Edition.pdf [accessed 2/7/18].

- [41] C. Mah and S. Higgins, *Cisco Medical-Grade Network (MGN) 2.0-Security Architectures*, Cisco, San Jose, CA, 2012.
https://www.cisco.com/c/dam/en_us/solutions/industries/docs/healthcare/mgn_security.pdf [accessed 2/8/18].
- [42] FDA, *Radio Frequency Wireless Technology in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, August 12, 2013.
<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf> [accessed 2/7/18].
- [43] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication (SP) 800-124 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013.
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf> [accessed 2/8/18].
- [44] S. Frankel, K. Kent, R. Lewkowski, A. D. Orebough, R. W. Ritchey, and S. R. Sharma, *Guide to IPsec VPNs*, NIST Special Publication (SP) 800-77, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2005.
<http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf> [accessed 2/7/18].
- [45] K. Scarfone and P. Hoffman, *Guidelines on Firewalls and Firewall Policy*, NIST Special Publication (SP) 800-41 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2009. <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf> [accessed 2/7/18].
- [46] Institute of Electrical and Electronics Engineers, *IEEE Standard for Ethernet*, IEEE 802.3, 2016.
<http://www.ieee802.org/3/> [accessed 2/7/18].
- [47] Institute of Electrical and Electronics Engineers, *Bridges and Bridged Networks*, IEEE 802.1Q, 2014. <http://www.ieee802.org/1/pages/802.1Q.html> [accessed 2/7/18].
- [48] S. Kent and K. Seo, *Security Architecture for the Internet Protocol*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 4301, December 2005.
<https://tools.ietf.org/html/rfc4301> [accessed 2/7/18].
- [49] U.S. Department of Commerce. *Advanced Encryption Standard (AES)*, Federal Information Processing Standards (FIPS) Publication 197, November 2001.
<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf> [accessed 2/7/18].
- [50] K. Scarfone, P. Hoffman, and M. Souppaya, *Guide to Enterprise Telework and Remote Access Security*, NIST Special Publication (SP) 800-46 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2009.
<http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf> [accessed 2/7/18].

- [51] A. Singhal, T. Winograd, and K. Scarfone, *Guide to Secure Web Services*, NIST Special Publication (SP) 800-95, National Institute of Standards and Technology, Gaithersburg, Maryland, August 2007. <http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf> [accessed 2/7/18].
- [52] M. Stone, C. Irrechukwu, H. Perper, and D. Wynne, *IT Asset Management*, NIST Special Publication (SP) 1800-5A, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2015. <https://nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5-draft.pdf> [accessed 2/7/18].
- [53] Image source: <http://wc1.smartdraw.com/cmsstorage/exampleimages/44b341d1-a502-465f-854a-4e68b8e4bf75.png>.
- [54] *Manufacturer Disclosure Statement for Medical Device Security (MDS2)*, Healthcare Information and Management Systems Society (HIMSS) [Web site], <http://www.himss.org/resourcelibrary/MDS2> [accessed 2/8/18].
- [55] *Vendor Deliverables to Initiate the Clinical Information Security Pre-Purchase Security Assessment*, Mayo Clinic, Rochester, MN, 2017. <http://www.mayo.edu/documents/vendor-deliverables/doc-20358150> [accessed 2/7/18].
- [56] M. Souppaya and K. Scarfone, *Guide to Enterprise Patch Management Technologies*, NIST Special Publication (SP) 800-40 Revision 3, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2013. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf> [accessed 2/7/18].

NIST SPECIAL PUBLICATION 1800-8C

Securing Wireless Infusion Pumps in Healthcare Delivery Organizations

Volume C:
How-to Guides

Gavin O'Brien

National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards

Kevin Littlefield

Neil McNab

Sue Wang

Kangmin Zheng

The MITRE Corporation
McLean, VA

August 2018

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

The first draft of this publication is available free of charge from:

<https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-infusion-pump-nist-sp1800-8-draft.pdf>



DISCLAIMER

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

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

FEEDBACK

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

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

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
Baxter Healthcare Corporation	<ul style="list-style-type: none"> • Sigma Spectrum™ Large Volume Pump (LVP) Version 8 • Sigma Spectrum Wireless Battery Module Version 8 • Sigma Spectrum Master Drug Library Version 8 • Care Everywhere Gateway Server Version 14
B. Braun Medical Inc.	<ul style="list-style-type: none"> • Infusomat® Space Infusion System / Large-Volume Pumps • DoseTrac® Infusion Management Software / Infusion Pump Software

Technology Partner/Collaborator	Build Involvement
Becton, Dickinson and Company (BD)	<ul style="list-style-type: none"> ● Alaris® 8015 Patient Care Unit (PCU) Version 9.19.2 ● Alaris Syringe Module 8110 ● Alaris LVP Module 8100 ● Alaris Systems Manager Version 4.2 ● Alaris System Maintenance (ASM) Version 10.19
Cisco	<ul style="list-style-type: none"> ● Aironet 1600 Series Access Point (AIR-CAP1602I-A-K9) ● Wireless LAN [Local Area Network] (WLC) Controller 8.2.111.0 ● Identity Services Engine (ISE) ● Adaptive Security Appliance (ASA) ● Catalyst 3650 Switch
Clearwater Compliance	<ul style="list-style-type: none"> ● IRM Pro™ ● IRM Analysis™
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 ● MedNet™ Version 6.2
Intercede	MyID®
Medical Device Innovation, Safety & Security Consortium (MDISS)	Medical Device Risk Assessment Platform (MDRAP™)
PFP Cybersecurity	Device Monitor
Ramparts	Risk Assessment

Technology Partner/Collaborator	Build Involvement
<u>Smiths Medical</u>	<ul style="list-style-type: none"> ● Medfusion® 3500 Version 5 Syringe Infusion System ● PharmGuard® Toolbox Version 1.5 ● Medfusion 4000 Wireless Syringe Infusion Pump ● PharmGuard Toolbox 2 Version 3.0 use with Medfusion 4000 and 3500 Version 6 (US) ● PharmGuard Server Licenses, PharmGuard Server Enterprise Edition Version 1.1 ● CADD®-Solis Ambulatory Infusion Pump ● CADD-Solis Medication Safety Software
<u>Symantec Corporation</u>	<ul style="list-style-type: none"> ● Symantec Endpoint Protection (SEP) ● Advanced Threat Protection: Network (ATP:N) ● Data Center Security: Server Advanced (DCS:SA)
<u>TDi Technologies, Inc.</u>	ConsoleWorks®

Contents

1	Introduction	1
1.1	Practice Guide Structure	1
1.2	Typographical Conventions	2
1.3	How-To Overview	3
1.4	Logical Architecture Summary	3
2	Product Installation Guides	4
2.1	The Core Network	4
2.1.1	Cisco ASA Baseline Configuration	4
2.1.2	External Firewall and Guest Network	5
2.1.3	Enterprise Services.....	5
2.1.4	Biomedical Engineering Network.....	5
2.1.5	Medical Devices	6
2.1.6	Cisco Catalyst Switch Configuration.....	6
2.1.7	Cisco Enterprise Wi-Fi Infrastructure.....	7
2.1.8	TDi ConsoleWorks External Remote Access	14
2.2	Infusion Pump and Pump Server	25
2.2.1	Infusion Pumps	25
2.2.2	Infusion Pumps Server Systems.....	31
2.3	Identity Services	32
2.3.1	Cisco Identity Service Engine	32
2.3.2	DigiCert Certificate Authority	38
2.4	Symantec Endpoint Protection and Intrusion Detection	44
2.4.1	Symantec Data Center Security: Server Advanced	44
2.4.2	Symantec Endpoint Protection Manager.....	49
2.4.3	Symantec Advanced Threat Protection: Network	50
2.5	Risk Assessment Tools.....	52
2.5.1	PFP Device Monitoring System: pMon 751 and P2Scan	52

2.5.2	Clearwater IRM Analysis™ Software	61
2.5.3	MDISS MDRAP.....	71

Appendix A Baseline Configuration File..... 81

A.1	Baseline Configuration File.....	81
A.2	External Firewall and Guest Network ASA Configuration File	84
A.3	Enterprise Services ASA Configuration File	93
A.4	Biomedical Engineering	101
A.5	Medical Devices Zone ASA Configuration File.....	110
A.6	Switch Configuration File	115
A.7	Wireless Configuration	122

Appendix B Sample Pump Configuration Parameters..... 246

Appendix C Acronyms 253

Appendix D References 256

List of Figures

Figure 1-1 Logical Architecture Summary	3
Figure 2-1 Importing Server Certificate	36
Figure 2-2 DCS:SA Environment	45
Figure 2-3 PFP Monitoring System Reference Setup	53
Figure 2-4 P2Scan Home Page.....	54
Figure 2-5 New Project Creation	55
Figure 2-6 P2Scan Main Screen	55
Figure 2-7 P2Scan Configuration Parameters.....	56
Figure 2-8 Data Collection Screen During Capture	57
Figure 2-9 Completed Baseline Extraction Screen.....	58
Figure 2-10 Runtime Monitoring Showing the Execution of Four Different States.....	59
Figure 2-11 Runtime Monitoring Showing an Anomalous State	60
Figure 2-12 Sample Contents Saved in the Runtime Results File.....	61
Figure 2-13 IRM Analysis Login Page	62
Figure 2-14 Asset Inventory List	63
Figure 2-15 New Asset.....	63
Figure 2-16 Media/Asset Groups	64
Figure 2-17 Edit Media/Asset Group	65
Figure 2-18 Controls – Global/Media	66
Figure 2-19 Risk Questionnaire List	67
Figure 2-20 Risk Questionnaire Form (Part 1)	67
Figure 2-21 Risk Questionnaire Form (Part 2)	68
Figure 2-22 Risk Response List – Risk Registry	69
Figure 2-23 Risk Treat and Evaluate Form	69
Figure 2-24 Dashboard Example	70
Figure 2-25 Report Example	71
Figure 2-26 MDRAP Login Page.....	72
Figure 2-27 MDRAP Welcome Page.....	73

Figure 2-28 Device Inventory List	73
Figure 2-29 Add Device.....	74
Figure 2-30 Edit Device.....	75
Figure 2-31 Inventory Bulk Import	76
Figure 2-32 Device Inventory Template Sample.....	76
Figure 2-33 Create Assessment (Part 1).....	77
Figure 2-34 Create Assessment (Part 2).....	78
Figure 2-35 Assessment Step (Example 1)	78
Figure 2-36 Assessment Step (Example 2)	79
Figure 2-37 Assessment Result (Dashboard Example)	79
Figure 2-38 Assessment Result (Report Example)	80

List of Tables

Table 2-1 Infusion Pump List.....	25
Table 2-2 Summary of Infusion Pump Configuration Methods	27
Table 2-3 Pump Servers Used in this Example Implementation	31

1 Introduction

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

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

1.1 Practice Guide Structure

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

This guide contains three volumes:

- NIST Special Publication (SP) 1800-8a: *Executive Summary*
- NIST SP 1800-8b: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-8c: *How-To Guides* – instructions for building the example solution (**you are here**)

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

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

- challenges enterprises face in securing the wireless infusion pump ecosystem
- example solution built at the National Cybersecurity Center of Excellence (NCCoE)
- benefits of adopting the example solution

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

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

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

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

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of commercially available technologies that can help secure the wireless infusion pump ecosystem. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices. In *NIST SP 1800-8b*, Section 4.4, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

1.2 Typographical Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<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	service sshd start
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at https://nccoe.nist.gov .

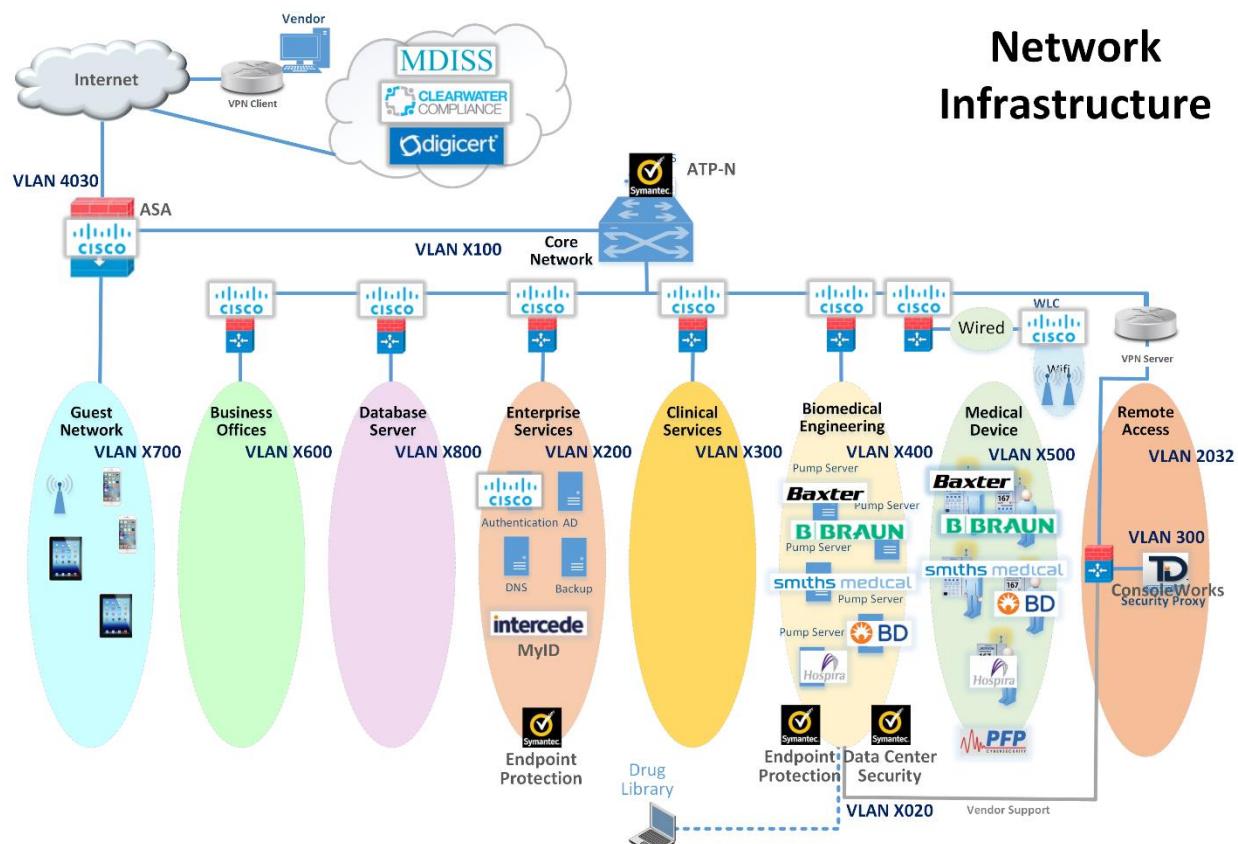
1.3 How-To Overview

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

1.4 Logical Architecture Summary

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

Figure 1-1 Logical Architecture Summary



2 Product Installation Guides

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

2.1 The Core Network

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

Several functional segments may be part of this core network:

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

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

2.1.1 Cisco ASA Baseline Configuration

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

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

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

See [Section A.1 of Appendix A](#) for the ASA configuration for this zone.

2.1.2 External Firewall and Guest Network

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

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

2.1.3 Enterprise Services

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

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

2.1.4 Biomedical Engineering Network

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

Generally, the firewall is configured in this way:

- all pump servers > internet/intranet (all destinations)
- all intranet > all pump servers Ping and Traceroute (primarily for debugging)
- all pumps > *Smiths Medical Pump Server* on Port 1588

- all pumps > *Carefusion Pump Server* on Port 3613
- all pumps > *Baxter Pump Server* on Port 51244
- all pumps > *Hospira Pump server* on Ports 443, 8443, 8100, 9292, 11443, and 11444
- all pumps > *B. Braun Pump server* on Ports 443, 80, 8080, 1500, and 4080

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

2.1.5 Medical Devices

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

Generally, the firewall is configured in this way:

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

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

2.1.6 Cisco Catalyst Switch Configuration

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

To set up your organization's configuration, follow the instructions in Cisco's *Catalyst 3650 Switch Getting Started Guide* [8].

See [Section A.6 of Appendix A](#) for the switch configuration.

2.1.7 Cisco Enterprise Wi-Fi Infrastructure

The Wi-Fi management network is different, in that it does not have a firewall/router that connects directly to the core network. As a completely closed network, the Wi-Fi management network is used for management and communication between the Cisco Aironet wireless APs and the Cisco WLC. The WLC is the central point where wireless service set identifiers (SSIDs), VLANs, and Wi-Fi Protected Access II (WPA2) [9] security settings are managed for the entire enterprise. We defined two SSIDs: *IP_Dev* and *IP_Dev_Cert*. *IP_Dev* uses WPA2-PSK (Pre-Shared Key), and *IP_Dev_Cert* uses WPA2-Enterprise protocols.

2.1.7.1 Installation

In our environment, the Cisco WLC is virtualized. In your environment, the responsible person would complete installation by following Cisco's *Virtual Wireless LAN Controller Deployment Guide 8.2* [10].

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

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

2.1.7.2 Controller Configuration

Follow these steps to configure network interfaces:

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

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

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

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

Interfaces > New

Interface Name ip_dev
VLAN Id 1500

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

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

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

Interfaces

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

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

NTP Servers > New

Server Index (Priority)	<input type="text" value="2"/>
Server IP Address(Ipv4/Ipv6)	<input type="text" value="192.168.250.1"/>
Enable NTP Authentication	<input type="checkbox"/>

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

DHCP Parameters

Enable DHCP Proxy	<input type="checkbox"/>
-------------------	--------------------------

2.1.7.3 Wireless AP Connection and Setup

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

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



2.1.7.4 Authentication Configuration

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

RADIUS Authentication Servers > New

Server Index (Priority)	<input type="text" value="3"/>
Server IP Address(Ipv4/Ipv6)	<input type="text" value="192.168.29.159"/>
Shared Secret Format	<input type="text" value="ASCII"/>
Shared Secret	<input type="text" value="****"/>
Confirm Shared Secret	<input type="text" value="****"/>

2.1.7.5 WLANs Configuration

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

To create a new SSID, follow these steps:

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



2. Enter your new SSID information.

WLANS > New

Type	WLAN
Profile Name	IP_Dev
SSID	IP_Dev
ID	4

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

WLANS > Edit 'IP_Dev'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	IP_Dev			
Type	WLAN			
SSID	IP_Dev			
Status	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	none			

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

General	Security	QoS	Policy-Mapping	Advanced
Layer 2	Layer 3	AAA Servers		
Layer 2 Security ⁶	WPA+WPA2			
MAC Filtering ⁹	<input type="checkbox"/>			
Fast Transition				
Fast Transition	<input type="checkbox"/>			
Protected Management Frame				
PMF	Disabled			
WPA+WPA2 Parameters				
WPA Policy	<input type="checkbox"/>			
WPA2 Policy	<input checked="" type="checkbox"/>			
WPA2 Encryption	<input checked="" type="checkbox"/> AES <input type="checkbox"/> TKIP			
OSEN Policy	<input type="checkbox"/>			

Authentication Key Management [19](#)

802.1X	<input type="checkbox"/> Enable
CCKM	<input type="checkbox"/> Enable
PSK	<input checked="" type="checkbox"/> Enable
FT 802.1X	<input type="checkbox"/> Enable
FT PSK	<input type="checkbox"/> Enable
PSK Format	ASCII <input type="button" value="▼"/>

WPA gtk-randomize State 14	Disable <input type="button" value="▼"/>

5. For the SSID IP_Dev_Cert, repeat Steps 1 through 4 above (replacing IP_Dev with IP_Dev_Cert in the instructions), but do not change the security settings for **Authentication Key Management** (leave **802.1X** checked, and leave **PSK** unchecked).
6. On the **Security** tab, on the **AAA Servers** sub-tab, select the RADIUS server to authenticate with (**Server 1**).

WLANS > Edit 'IP_Dev_Cert'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface Enabled

Authentication Servers	Accounting Servers	EAP Parameters
<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Enable <input type="checkbox"/>
Server 1 IP:192.168.29.159, Port:1812 <input type="button" value="▼"/>	None <input type="button" value="▼"/>	

2.1.7.6 Monitoring

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

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

2.1.7.7 Final Configuration

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

2.1.8 TDi ConsoleWorks External Remote Access

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

2.1.8.1 System Environment

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

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

2.1.8.2 Other Requirements

- ConsoleWorks install media (we built from a CD)
- ConsoleWorksSSL-<version>.rpm
- ConsoleWorks_gui_gateway-<version>.rpm
- ConsoleWorks license keys (*TDI_Licenses.tar.gz*)
- software installation command
- `yum install uuid libpng12 libvncserver`

2.1.8.3 Installation

As Root:

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

2.1.8.4 Usage

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

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

2.1.8.5 Initial Configuration of Graphical Gateway

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

Use the menu in the sidebar to access all instructions provided in Section 2.1.8.5 through [Section 2.1.8.12](#).

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

The screenshot shows a web-based configuration interface for a graphical gateway. At the top, there's a header bar with a back arrow and the title "GRAPHICAL: Gateways: Edit". Below the header, there are two tabs: "View Graphical Gateways" and "LOCAL". The "LOCAL" tab is active, indicated by a red X icon. Under the "LOCAL" tab, there are several input fields:

- Name:** A text input field containing "LOCAL".
- Description:** An empty text input field.
- Host:** A text input field containing "localhost".
- Port:** A text input field containing "5172" with a note "(default: 5172)" next to it.

Below these fields are two checkboxes:

- Enabled:** A checked checkbox.
- Encrypt Connection:** An unchecked checkbox.

2.1.8.6 Create One Tag for Each Vendor Company

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

The screenshot shows the 'SECURITY: Tags: Edit' interface. At the top, there is a header bar with the title. Below it, a row contains the name 'CISCO' and a red 'X' button for deletion. A 'History' button is also present. The main area has two input fields: 'Name:' containing 'CISCO' and a 'Description:' field which is empty. Below these fields is a 'Custom Fields' section.

2.1.8.7 Create One Profile for Each Vendor Company

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

The screenshot shows the 'USERS: Profiles: Edit' interface. It has a similar structure to the 'Tags' interface, with a header bar, a row for the name 'CISCO' with a delete button, and a 'History' button. The 'Name:' field is filled with 'CISCO'. The 'Description:' field is empty. A 'Custom Fields' section is at the bottom.

2.1.8.8 Establish Graphical Access Controls

Repeat this section for each vendor company.

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

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

SECURITY: Access Control: Edit

View Access Control Rules **Edit Access Control Rule**

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>](#)
+ [Property Tag Equals CISCO <join>](#)

Profiles

Profiles
CISCO

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

Resource Selection

Simple **Basic** **Advanced**

Selection:

- [Associated With a Tag that](#)
- [Property Tag Equals CISCO <join>](#)
+ [<join>](#)

Graphical Connections

Graphical Connections
No Graphical Connections match.

9. Under **Privileges**, under **Resource Level**, select the following checkboxes:
 - a. **Aware**
 - b. **View**
 - c. **Connect**

▼ Privileges

All

Component Level:

Add

Resource Level:

<input checked="" type="checkbox"/> Aware	<input checked="" type="checkbox"/> Connect
<input type="checkbox"/> Delete	<input type="checkbox"/> Delete Recordings
<input type="checkbox"/> Disable	<input type="checkbox"/> Disconnect
<input type="checkbox"/> Edit	<input type="checkbox"/> Enable
<input type="checkbox"/> Lock Recordings	<input type="checkbox"/> Monitor
<input type="checkbox"/> Rename	<input type="checkbox"/> Unlock Recordings
<input checked="" type="checkbox"/> View	<input type="checkbox"/> View Recordings
<input type="checkbox"/> View Usage	

2.1.8.9 Console Access Controls

Repeat this section for each vendor company.

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

▼ SECURITY: Access Control: Edit

[View Access Control Rules](#) [Edit Access Control Rule](#)

History

Name: CISCO_CONSOLE

Description:

Enabled

Order: 8

Allow or Deny: ALLOW

Audit Rule Usage

Component Type: Console

▼ Profile Selection

Simple Basic Advanced

Selection:

- [Property Profile Equals CISCO <join>](#)
- + [+](#)

Profiles

CISCO
CISCO

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

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

▼ Resource Selection

Simple Basic Advanced

Selection:

- [Associated With a Tag that](#)
- - [Property Tag Equals CISCO <join>](#)
- + [+ <join>](#)
- + [+](#)

Consoles

IPASA_BIOMEDICAL
IPASA_BORDER
IPASA_CLINICAL_SERVICES
IPASA_DATABASE
IPASA_ENTERPRISE
IPASA_ENTERPRISE_SERVIC
IPASA_MEDICAL_DEVICES
IP_CATALYST_3650
IP_DEV_CISCO_ISE

- b. matching consoles in the box on the right

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

- a. **Aware**
- b. **View**
- c. **Connect**

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	

2.1.8.10 Users

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

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

USERS: Add *

View Users **Add User ***

Name: test

Description: Test Company

Login Expiration:

User Created:

Last Login:

Use External Authentication

Password

Password: Retype Password:

Require Password Change On Next Login

Contact Info

First Name:
 Last Name:
 Email:
 Title:
 Office Phone:
 Cell Phone:
 Address/Location:

PROFILES * (1)

CISCO

REMEDIATION HISTORY (0)

TAGS (0)

2.1.8.11 Add an RDP Graphical Connection

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

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

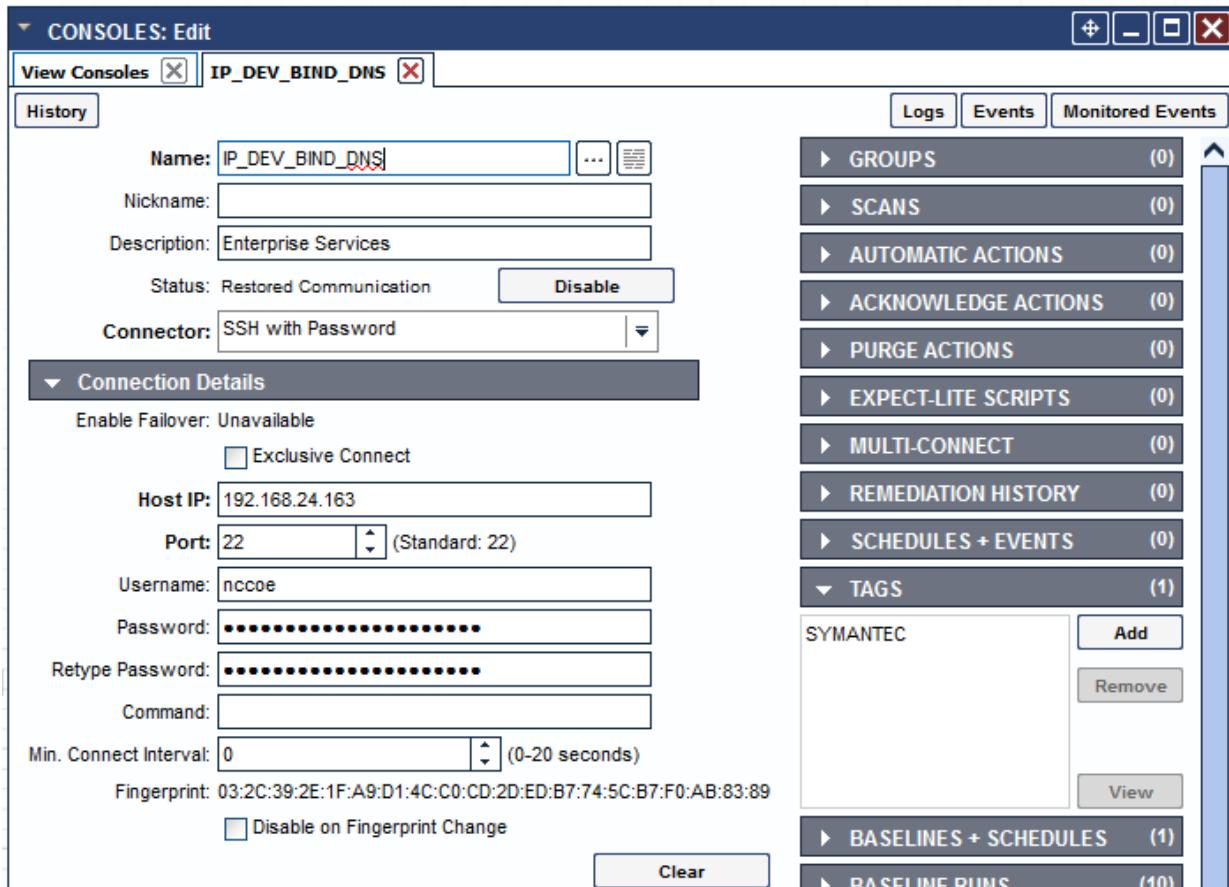
The screenshot shows the 'GRAPHICAL: Edit' interface with the following details:

- Name:** IP_DEV_ACTIVE_DIRECTORY
- Description:** Enterprise Services
- Type:** RDP
- Host:** 192.168.24.162
- Port:** (empty)
- Status:** Available
- Max Idle Time:** 0-999 Minutes (0=disabled)
- Recordings:** (0)
- Authentication:**
 - Username: administrator
 - Password: [REDACTED]
 - Domain: IP
 - Security Mode: (dropdown menu)
 - Disable Authentication
 - Ignore Certificate Errors
- GATEWAYS:** LOCAL (1)
 - Add
 - Remove
 - View
- CONSOLES:** (0)
- TAGS:** (1)
 - SYMANTEC
 - Add
 - Remove
 - View

2.1.8.12 Add an SSH Console Connection

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

- d. Retype the password (**Retype Password**).
5. Add tags for all vendor companies that should have access (under **TAGS**).
6. Click **Save**.



2.2 Infusion Pump and Pump Server

2.2.1 Infusion Pumps

Vendors collaborating with the NCCoE in this use case donated the pump products listed in Table 2-1.

Table 2-1 Infusion Pump List

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

Vendor Name	Product Name	Product Type	Description
	Alaris Pump 8100	Large-volume infusion pump	Provides a large-volume infusion capability for patients, and works with the Alaris PCU
Hospira	Plum 360	Infusion system	Builds on the air management and secondary delivery features of Plum A+, while expanding its drug library and wireless capability to enable streamlined electronic medical record integration
	Hospira PCA	PCA syringe infusion system	Complements the infusion pump to manage pain
Smiths Medical	Medfusion 4000	Syringe infusion pump	Delivers medication to patients in critical care units
	CADD-Solis 2000	Ambulatory infusion pump	Delivers medication to patients in hospital, home care, and alternative care facilities

2.2.1.1 Infusion Pump Setup

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

Each pump vendor has a basic setup that includes configuring the pump to connect to the network and the pump server wirelessly. We used WPA2 security with AES for encryption. In the case of WPA2-PSK mode, we assigned all infusion pumps the same access password for wireless network authentication. In the case of WPA2-Enterprise with Extensible Authentication Protocol – Transport Layer Security

(EAP-TLS) [14], we configured the pumps to use an individual certificate issued by DigiCert for wireless network authentication, using the Cisco ISE, the enterprise authentication server.

Because each pump vendor has its own way of connecting, configuring, and setting up its pumps, we describe high-level steps in a generic way. Table 2-2 summarizes these key configuration steps. See [Appendix B](#) for the sample configuration files.

Table 2-2 Summary of Infusion Pump Configuration Methods

Vendor Name	Infusion Pump Model	Configuration Tool	Connection Method
Baxter	Sigma Spectrum	<ul style="list-style-type: none">• uses a PC with an Infrared Data Association (IrDA) interface to program multiple pumps with the same configuration• edits the network configuration file (a simple text file) on a PC, and sends it via the IrDA to a pump	<ul style="list-style-type: none">• uses the IrDA Serial Infrared• links to a PC under the IrDA Serial Infrared Link Management Protocol Version 1.1
B. Braun	Space Station	<ul style="list-style-type: none">• connects a PC with the HiBaSeD service program to the Space Station by using a B. Braun interface cable for pump configuration setting	<ul style="list-style-type: none">• uses a special B. Braun interface cable
	Infusomat Space Large-Volume Infusion Pump	<ul style="list-style-type: none">• connects a PC with the HiBaSeD service program to the Space Station by using a B. Braun interface cable for pump configuration setting	<ul style="list-style-type: none">• uses a special B. Braun interface cable

Vendor Name	Infusion Pump Model	Configuration Tool	Connection Method
	Perfusor Space Syringe Pump	<ul style="list-style-type: none"> connects a PC with the HiBaSeD service program to the Space Station by using a B. Braun interface cable for pump configuration setting 	<ul style="list-style-type: none"> uses a special B. Braun interface cable
BD	Alaris 8015 PC	<ul style="list-style-type: none"> uses a management system to do the configuration is the core of the Alaris system and provides a common user interface for programming infusion and monitoring modules 	<ul style="list-style-type: none"> uses a series cable to connect the pump to a local computer
Hospira	Hospira PCA	<ul style="list-style-type: none"> accesses Web Configuration Utility on the pump through a web browser using the local IP address of the pump 	<ul style="list-style-type: none"> uses the pump's Ethernet jack to connect to a LAN or to interface with the host computer
	Plum 360	<ul style="list-style-type: none"> accesses Web Configuration Utility on the pump through a web browser using the local IP address of the pump 	<ul style="list-style-type: none"> uses the pump's Ethernet jack to connect to a LAN or to interface with the host computer

Vendor Name	Infusion Pump Model	Configuration Tool	Connection Method
Smiths Medical	Medfusion 4000	<ul style="list-style-type: none"> pushes a configuration text file to the pump by using the Telnet from a PC that is connected to the pump with the known IP address 	<ul style="list-style-type: none"> connects a PC to pump using micro Universal Serial Bus (USB)-USB cable
	CADD-Solis 2000	<ul style="list-style-type: none"> uses Smiths Medical Network Configuration Utility to update the pump's configuration parameters 	<ul style="list-style-type: none"> connects a PC to the pump by using a micro USB-USB cable

2.2.1.2 Infusion Pump Configuration

Pre-Conditions:

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

Post-Conditions:

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

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

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

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

2.2.1.3 Infusion Pump Hardening

Hardening may include the following actions:

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

2.2.2 Infusion Pumps Server Systems

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

Table 2-3 Pump Servers Used in this Example Implementation

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

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

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

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

2.3 Identity Services

2.3.1 Cisco Identity Service Engine

The Cisco ISE enables your organization to:

- centralize and unify identity and access policy management
- have visibility and more-assured device identification during certificate challenges
- use business rules to segment access to sections of the network
- make the user experience seamless during the challenge process, even with more-assured and stronger authentication

System requirements:

- Virtual Hypervisor (VH) capable of housing virtual machines (VMs)
- VM with Central Processing Unit (CPU): single quad core, 2.0 gigahertz (GHz) or faster
- VM with a minimum 4 GB RAM
- VM with a minimum 200 GB disk space

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

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

```
! hostname
```

```
ise
!ip domain-name
nccoe.lab
! ipv6
enable
!interface
GigabitEthernet 0 ip address 192.168.29.159 255.255.255.0 ipv6 address autoconfig ipv6
enable
! interface
GigabitEthernet 1 ip address 192.168.120.159 255.255.255.0 ipv6 address autoconfig
ipv6 enable
!interface
GigabitEthernet 2 shutdown ipv6 address autoconfig ipv6 enable
! interface
GigabitEthernet 3 shutdown ipv6 address autoconfig ipv6 enable
! ip name-server
8.8.8.8 8.8.4.4
! ip default-gateway
192.168.120.1
!
! clock timezone
EST
! ntp server
time.nist.gov
! username [*****] password [*****]
$5$jNPleEb4$YxDZH6oDF2Y4.02OqE/jBWxFumRvtpe8JdNNZm1yj0 role admin
! max-ssh-sessions
5
! service sshd
enable
! password-policy
lower-case-required
```

```
upper-case-required  
digit-required  
no-username  
no-previous-password  
password-expiration-enabled  
password-expiration-days 45  
password-expiration-warning 30  
min-password-length 4  
password-lock-enabled  
password-lock-timeout 15  
password-lock-retry-count 3  
! logging loglevel  
6  
! conn-limit 10  
port 9060  
! cdp timer  
60 cdp holdtime 180 cdp run GigabitEthernet 0  
! icmp echo  
on  
!
```

2.3.1.1 Configure ISE to Support EAP-TLS Authentication

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

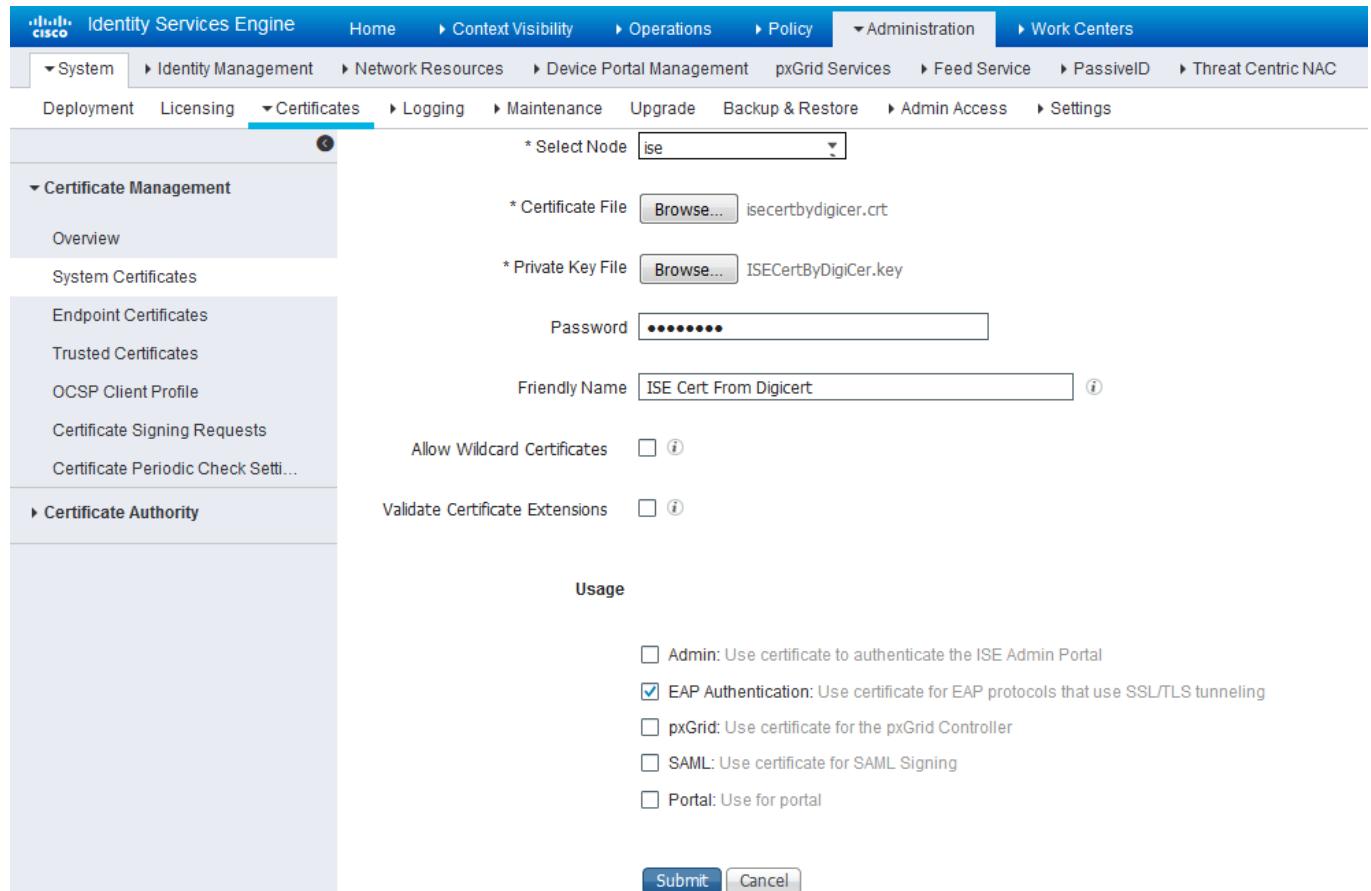
2.3.1.2 Set ISE to Support RADIUS Authentication

Use the following steps to set up a communication connection from the Cisco ISE to the network device (AP) that you use as the authentication server during RADIUS [15] authentication:

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

- i. the **name** of the network device
 - ii. the **IP Address** of the device with its subnet mask
2. Select the RADIUS protocol as the selected protocol, and enter the shared secret that is configured on the network device.
3. Populate the system certificate with certificate-authority (CA)-signed certificates. We replaced the Cisco ISE default self-signed certificate with the CA-signed certificate issued through DigiCert Certificate Authority. The steps for acquiring the signing certificate from DigiCert are described in [Section 2.3.2](#).
4. Once the CA-signed certificate for the ISE and the Root CA are issued, use the following steps to install the certificates to the system.
5. From the **ISE Administration Portal**, use the following navigation path to show the installed certificates: **Administration > System > Certificates > System Certificates**. Select **Import** to open a screen for importing a server certificate. Fill in the required information as shown in Figure 2-1.

Figure 2-1 Importing Server Certificate



6. Under **Usage**, select the **EAP Authentication** checkbox to enable the imported certificate to be used for EAP authentication. Next, click the **Submit** button to complete the certificate importing.
7. Import the DigiCert Root CA and signing CA to ISE Trusted Certificates. From the ISE Administration Portal, use the following navigation path to show the installed certificates: **Administration > System > Certificates > Trusted Certificates**. Select **Import** to open a screen for importing the DigiCert Root CA and signing the CA individually.
 - a. After importing, make sure that the certificate status is **Enabled**.
 - b. Establish the Online Certificate Status Protocol (OCSP) [16] client profile from the **OCSP Client Profile** page (**Administration > System > Certificates > OCSP Client Profile**).
 - c. If OCSP is used for **Certificate Status Validation**, check **Validate** against the **OCSP Service**, and enter the **OCSP service name**.

8. Set the **Identity Source for Client Certificate Authentication**. When using the trusted certificate for EAP-TLS certificate-based authentication validation, set up the Certificate Authentication Profile in the ISE as the external identity source. Instead of authenticating via the traditional username and password, the Cisco ISE compares the client certificate received from the AP to verify the authenticity of a device—in this case, the infusion pump.
 - a. Create a Certificate Authentication Profile:
 - i. Use the Administration Portal to navigate to the following path: **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**. Click **Add**.
 - ii. Name the profile as, for example, Cert_Auth_Profile, and then fill out the form with proper parameters. Be sure to select **Subject Name** as the **Principal Username X509** attribute because it is the field that will be used to validate the authenticity of the client.
 - b. Select the **Identity Resource Sequences** tab. In the **Certificate Based Authentication**, select the **Select Certificate Authentication Profile** checkbox, and then choose **Cert_Auth_Profile** from the drop-down list.
9. Set Authentication Protocols. The Cisco ISE uses authentication protocols to communicate with external identity sources. The Cisco ISE supports many authentication protocols, such as the Password Authentication Protocol (PAP), Protected Extensible Authentication Protocol (PEAP), and the EAP-TLS. For this build, we used the EAP-TLS protocol for user and machine authentication. To specify the allowed protocols services in the Cisco ISE, follow these steps:
 - a. From the Administration Portal, navigate to the following path: **Policy > Policy Elements > Results > Authentication > Allowed Protocols > Add**.
 - b. Select the preferred protocol or list of protocols. In this build, the **EAP_TLS** is selected as the allowed authentication protocol.
10. Set up Authentication Policy. Define the authentication policy by selecting the protocols that the ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. To specify the authentication policy, follow these steps:
 - a. From the Administration Portal, navigate to the following path: **Policy > Authentication Policy > Type > Rule Based**.
 - b. If Protocol is **Wireless 802.1x**, set the policy to use the **Network Device** as defined in Step 1 and the **Identity Sequences** as defined in Step 8 above.

2.3.2 DigiCert Certificate Authority

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

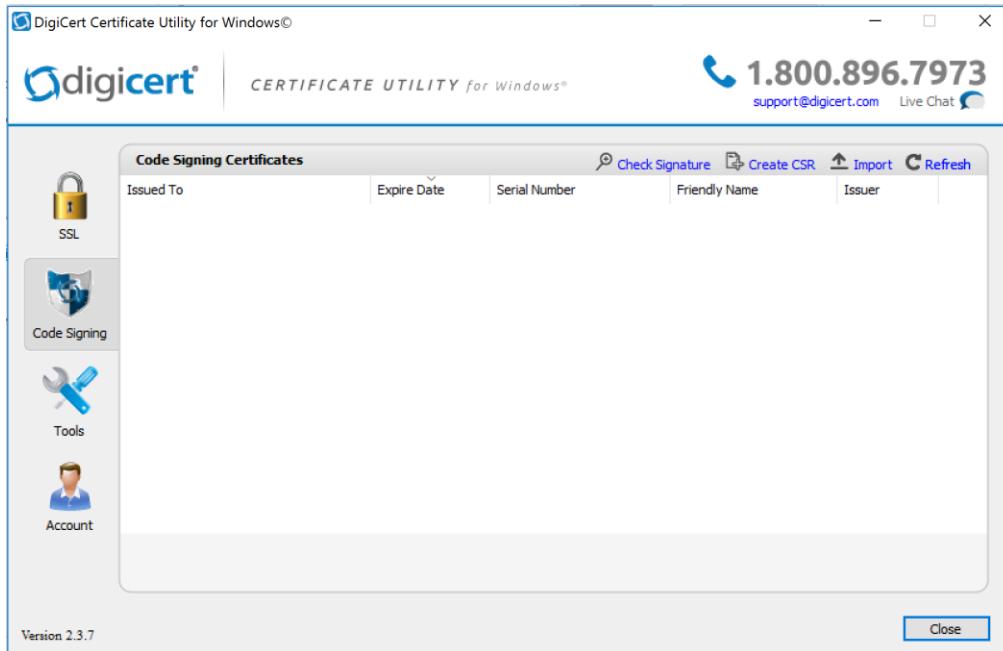
The following instruction describes the process that we used to request a PKI certificate on behalf a wireless infusion pump using the DigiCert PKI services.

2.3.2.1 *Create a Certificate Signing Request*

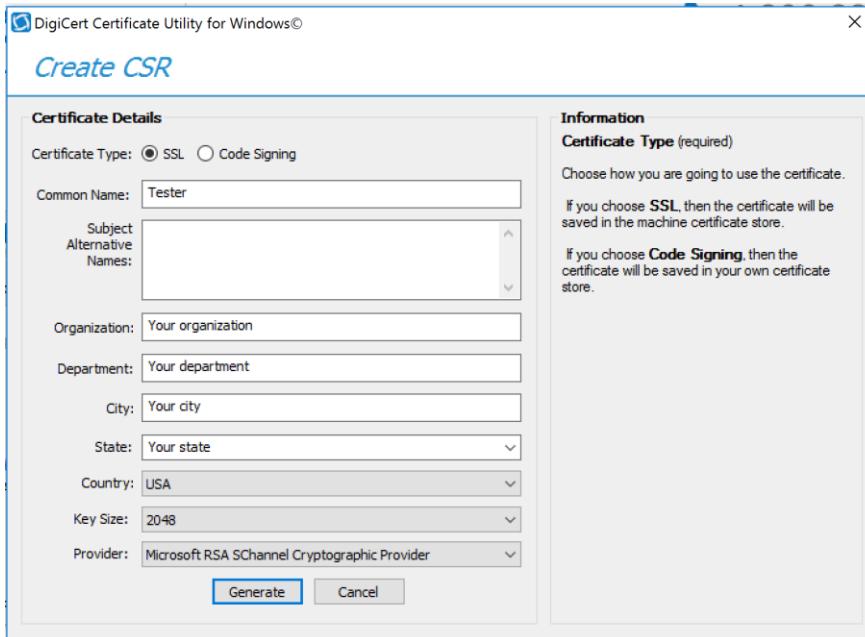
A Certificate Signing Request (CSR) can be represented as a Base64 encoded PKCS#10 binary format. Many tools and utilities are available to help generate a CSR, and the key pair containing the private key and public key is generated at the same time. The CSR identifies the applicant's distinguished name,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

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

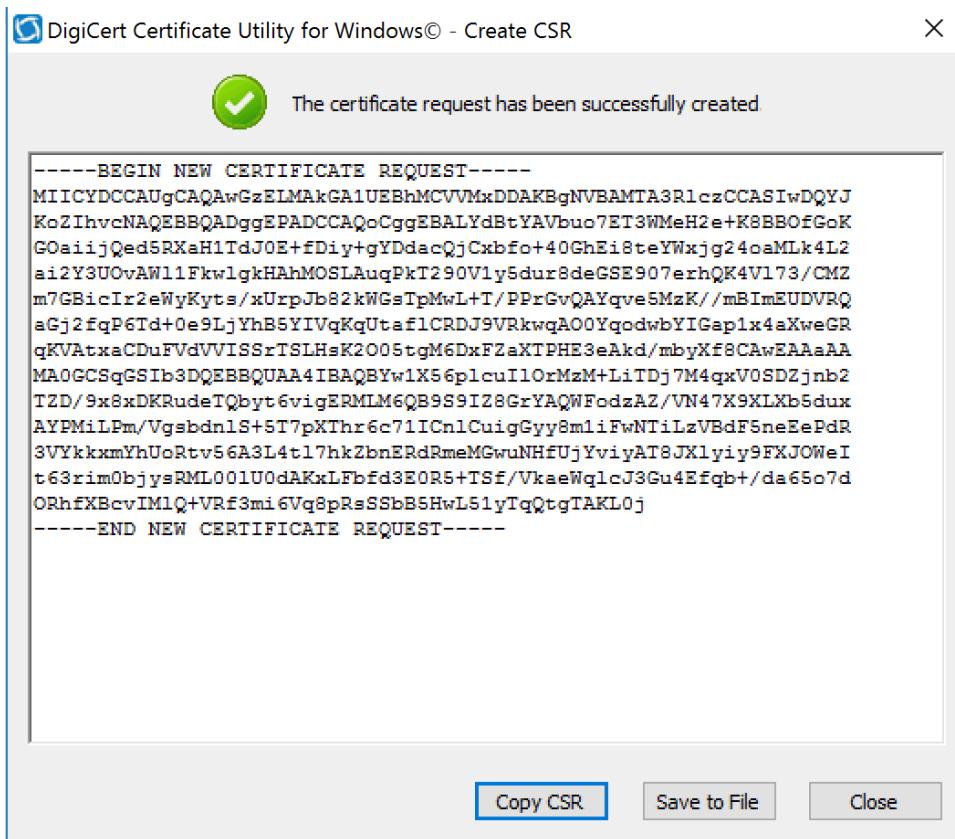
1. Double-click *DigiCertUtil.exe* to start the utility.



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



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



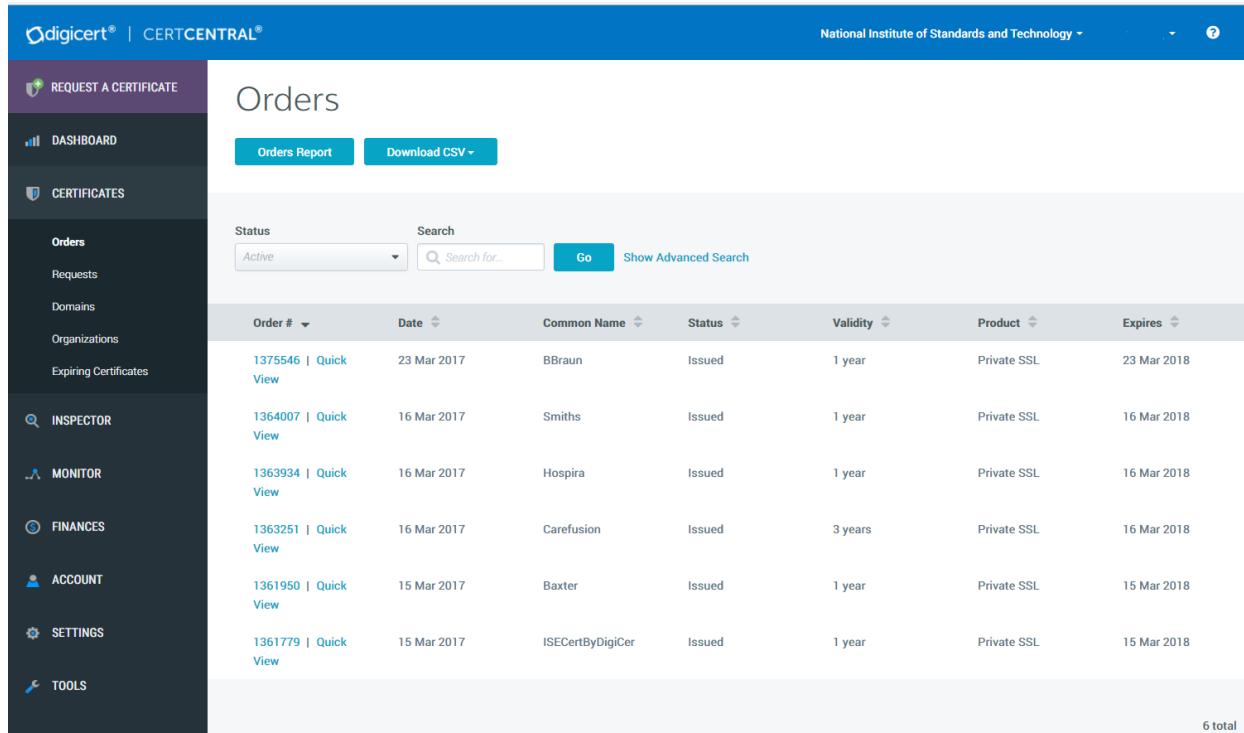
This will also generate a corresponding private key in the Windows computer from which the CSR is requested. The Certificate Enrollment Request is stored under *Console Root\Certificates(Local Computer)\Certificate Enrollment Requests\Certificates*.

2.3.2.2 Issue Signed Certificates

1. With a created applicant CSR, request a signed certificate using DigiCert CertCentral portal.
 - a. Log into a DigiCert Dashboard (<https://www.digicert.com/account/login.php>) with your account username and password.
 - b. Once in the portal, go to **Request a Certificate**, and then select **Private SSL** to open a certificate request form. Fill in the certificate settings in the fields shown in the form, which includes pasting the CSR information to the area called **Paste your CSR**.
2. After filling in all of the required information, scroll down to the bottom of the page, and select the **I agree to the Certificate Services Agreement above** checkbox. Next, click the **Submit Certificate Request** button at the bottom of the form to submit the certificate for signing approval. The administrator of the CA authority will use the same portal with different privileges

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

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



The screenshot shows the DigiCert CERTCENTRAL interface. The left sidebar has a dark theme with various navigation options like REQUEST A CERTIFICATE, DASHBOARD, CERTIFICATES, and MONITOR. The main content area is titled 'Orders' and displays a table of signed certificates. The table columns include Order #, Date, Common Name, Status, Validity, Product, and Expires. There are 6 total results listed.

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

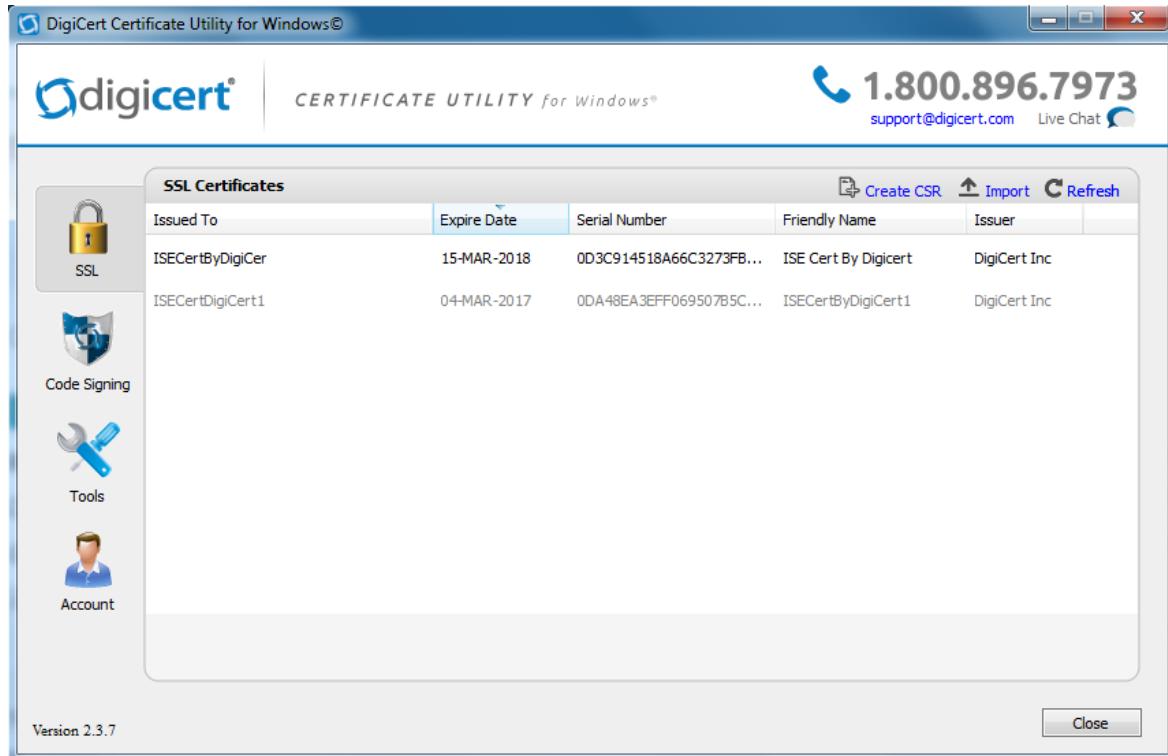
4. Click a specific order number to display the certificate details with a list of actions for you to perform. Click **Download Certificate As** to download certificates with signed CA and Root CA certificates. A variety of certificate formats can be downloaded, such as *.crt*, *.p7b*, *.pem*, etc.
5.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

2.3.2.3 Import and Export the Signed Certificate

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

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

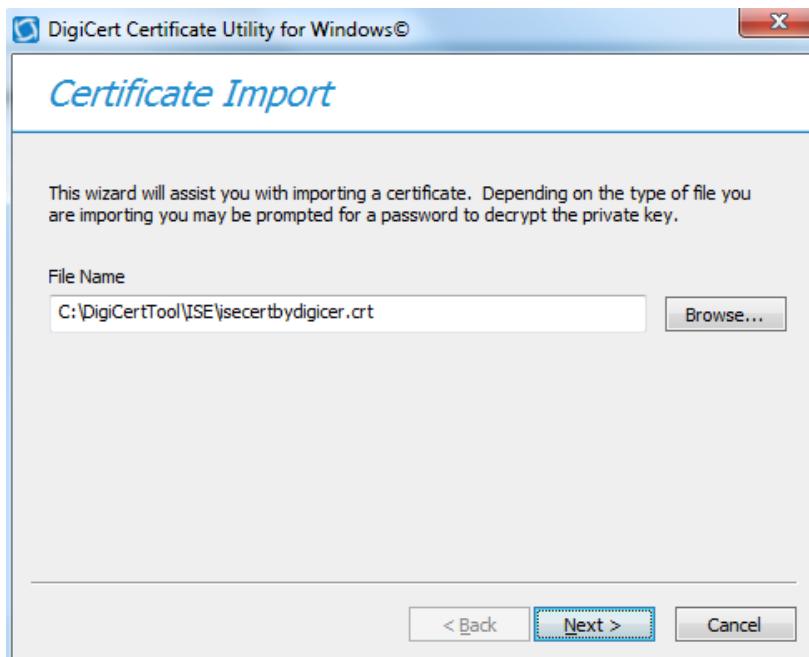
2. From the DigiCert Certificate Utility for Windows, click **SSL** to list all of the imported files.



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



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



2.3.2.4 Certificate and Key File Format Conversion

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

Here are some of the useful convert commands:

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

2.4 Symantec Endpoint Protection and Intrusion Detection

NCCoE protected the pump server application in the notional biomedical engineering network by using three Symantec cybersecurity products on an enterprise network, with a specific focus on wireless infusion pumps:

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

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

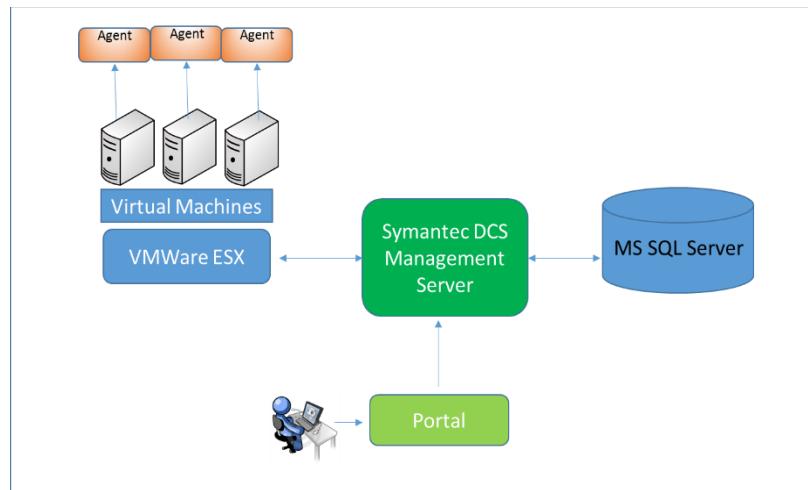
2.4.1 Symantec Data Center Security: Server Advanced

For data center security, DCS:SA provides a policy-based approach to endpoint security and compliance. DCS:SA includes the management server, the agents, the unified management console, the database,

and DCS Security Virtual Appliance (SVA). The agent components working with the server management provide intrusion prevention and detection on endpoint devices; the database is used for storing the policies, agent information, and real-time actionable events; and the SVA provides agentless anti-malware protection for VMware guest VMs running Windows.

The management server and the console can be installed on one system, and the agents are generally deployed to every supported host or endpoint device. Figure 2-2 displays the DCS:SA environment.

Figure 2-2 DCS:SA Environment



2.4.1.1 *Installing DCS:SA Manager*

Minimum hardware requirements:

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

Minimum software requirements:

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

Operating the Symantec DCS:SA installation requires to link to an instance of SQL Server locally or remotely. All installations allocate approximately 60 GB of space for the database on SQL Server Enterprise edition. We first installed a new instance of SQL Server that conforms to the Symantec

installation requirements. The SQL Server was installed on the same machine as that for the DCS:SA Manager.

Follow these steps to install the SQL Server software.

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

Follow these steps to install DCS:SA:

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

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

2.4.1.2 Configuration of DCS:SA Manager

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

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

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

1. Log into the DCS console.
2. Create a policy folder.

3. In the Java console, click **Policies**.
4. Under the **Policies** tab, click **Prevention or Detection**.
5. On the **Policies** page, in the **Workspace Folders**, select the **Workspace** folder, and then right-click **Add Folder**. Look for a new policy folder with the name **New Folder**. Rename this folder as **Pump Server**.
6. Copy an existing policy to the **Pump Server** folder.
7. From the default **Symantec** folder, find a proper policy example, and copy it to the **Pump Server** folder.
8. In the **Workspace** pane, select a policy (e.g., “windows-baseline-detection” policy in **Symantec** folder for **Detection**), and then right-click **Move To**. In the **MoveFolder** dialog box, select **Pump Server** to receive the policy, and then click **MoveTo**.
9. To edit a policy, right-click a policy, and then click **Edit Policy**. Configure the setting based on your security protection needs.

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

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

1. In the management console, click the **Policies** tab, and then click **Prevention**.
2. In the **Policies** workspace, click **Add**.
3. In the **Select a Prevention Policy Builder** wizard, in the **New Policy Builder** section, click **Launch**.
4. In the **Policy Name** panel, from the **Policy Pack** drop-down list, select the policy pack that you want to use as the baseline for the new custom policy.
5. In the **Name** textbox, enter a name for the policy that you create. In this build, we use the following name: Windows Prevention Policy 6.0 Reference 31 Protected Whitelisting strategy.
6. Select the **Create a custom prevention policy** checkbox, and then click **Next**.
7. In the **Protection Strategy** panel, use the slider to select **Protected Whitelisting**.
8. In the **Trusted Updaters** panel, click **Add**. In the **Select Type** dialog box, select the type of updater that you want to add. The **Trusted Updaters** list is populated through the agent data retriever. You can edit or delete an updater that you have already added to the list.

9. Click **Next**.
10. In the **Application Rules** panel, click **Add**. In the **Select Type** dialog box, select the type of rules that you want to add. You can edit or delete a rule that you have already added to the list.
11. In the **Global Policy Options** panel, click **Configure** to configure the global policy settings, and then click **Next**.
12. In the **Summary** panel, click **Save**.

2.4.1.3 Installing DCS:SA Agent

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

1. On the installation package, double-click *agent.exe*.
2. In the **Welcome** panel, click **Next**.
3. In the **License Agreement** panel, select the **I accept the terms in the license agreement** checkbox, and then click **Next**.
4. In the **Destination Folder** panel, change the folders if necessary, and then click **Next**.
5. In the **Agent Configuration** panel, accept or change the default settings, and then click **Next**. Ensure that the **Enable Intrusion Prevention** checkbox is selected.
6. In the **Management Server Configuration** panel, in the **Primary Management Server** box, type the fully qualified host name or IP address of the primary server that is used to manage this agent. If you changed the **Agent Port** setting during management server installation, in the **Agent Port** box, type a port number that matches.
7. (Optional) In the **Management Server Configuration** panel, in the **Alternate Management Servers** box, type the fully qualified host name or IP address of the alternate servers that are used for failover for this agent. Type the servers in a comma-separated list.
8. In the **Management Server Configuration** panel, accept the directory for the SSL certificate *Agent-cert.ssl*, or click **Browse** to browse to and locate *Agent-cert.ssl*. Access to a copy of the SSL certificate *Agent-cert.ssl* is required to connect to the management server. All primary and alternate management servers must use the same certificate.
9. In the **Management Server Configuration** panel, click **Next**.
10. (Optional) In the **Agent Group Configuration** panel, in the **group boxes**, type the **group names** that you created with the Java console. You may add multiple detection policy group names

separated with commas. You may include the name of an existing detection policy domain in the group path/name.

11. In the **Agent Group Configuration** panel, click **Next**.
12. In the **Service User Configuration** panel, accept the default **Local System** account, and then click **Next**.
13. In the **Ready to Install the Program** panel, confirm the installation parameters, and then click **Install**.
14. When the installation completes, click **Finish**.

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

- enabling the intrusion prevention feature
- enabling the real-time file integrity monitoring feature in intrusion detection
- creating agent registration groups

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

2.4.2 Symantec Endpoint Protection Manager

Minimum hardware requirements:

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

Minimum software requirements:

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

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

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

2.4.2.1 *Installing SEP Manager*

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

2.4.2.2 *Installing the Client*

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

1. Make your configuration selections as you install SEP Manager, and then create the client installation packages.
2. Save the installation package to a folder on the computer that runs SEP Manager.
3. Copy this package to a client machine where you have an administrator privilege.
4. The installation package comprises one *setup.exe* file. Click the executable file to start the installation. Follow the wizards to complete the installation.

2.4.3 Symantec Advanced Threat Protection: Network

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

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

Minimum hardware requirements:

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

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

2.4.3.1 ATP:N Installation

The installation of the ATP:N involves the deployment of the OVA template on the VMware ESXi Server. Sample installation steps are listed below.

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

2.4.3.2 Integrating ATP:N with SEP

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

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

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

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

2.5 Risk Assessment Tools

2.5.1 PFP Device Monitoring System: pMon 751 and P2Scan

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

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

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

Hardware requirements:

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

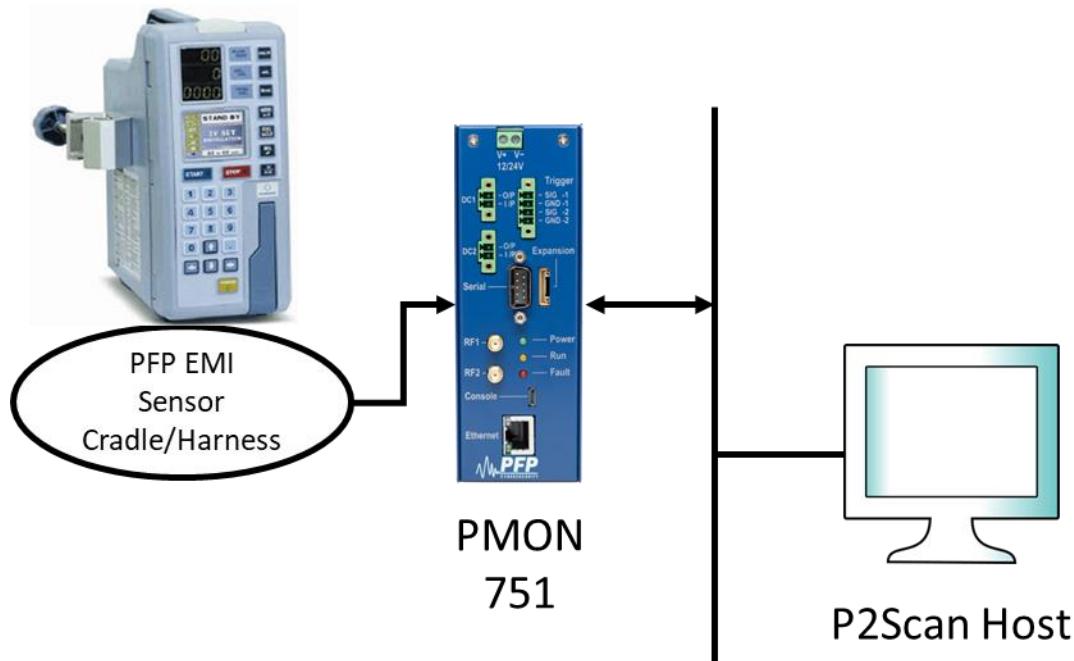
Host computer requirements:

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

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

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

Figure 2-3 PFP Monitoring System Reference Setup



The following connections on the pMon 751 are required:

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

2.5.1.1 P2Scan Setup

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

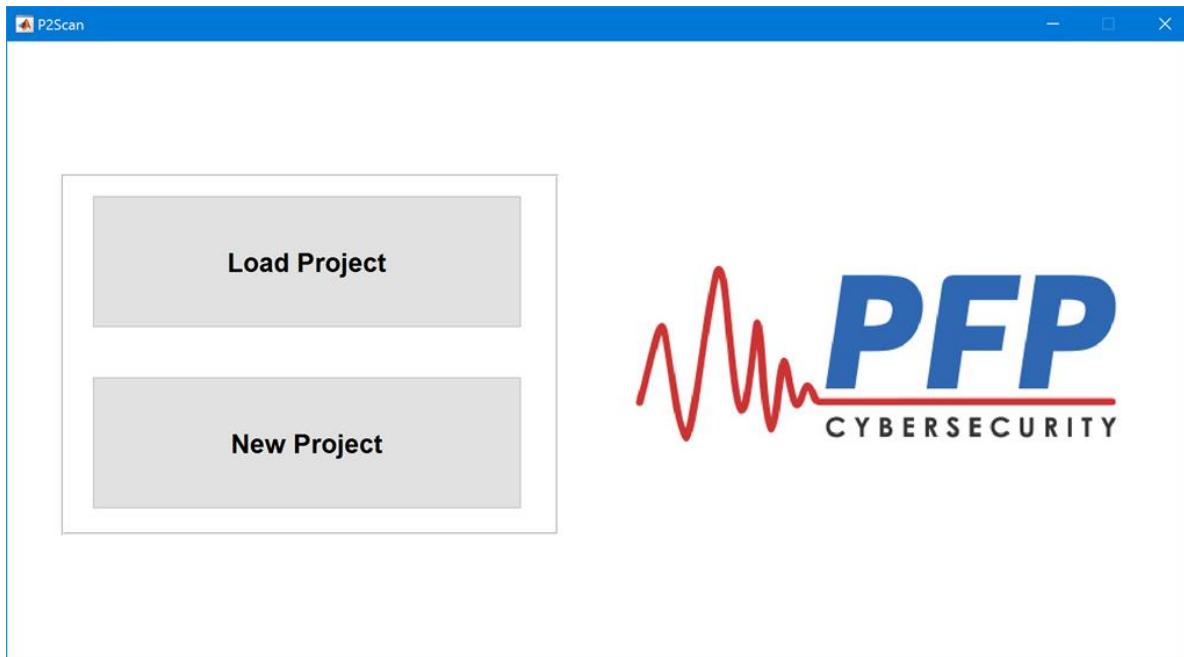
P2Scan uses a single project file to control the operation of P2Scan. As the user makes changes to the configuration parameters they will have the options to save the changes to the project file.

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

2.5.1.2 Operating P2Scan

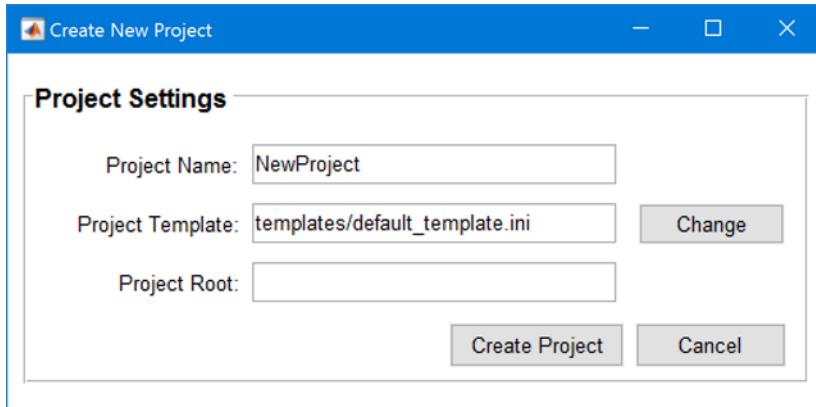
1. Launch P2Scan. This will open the application home page, where it allows you to create a new monitoring project or to load an existing project (Figure 2-4).

Figure 2-4 P2Scan Home Page



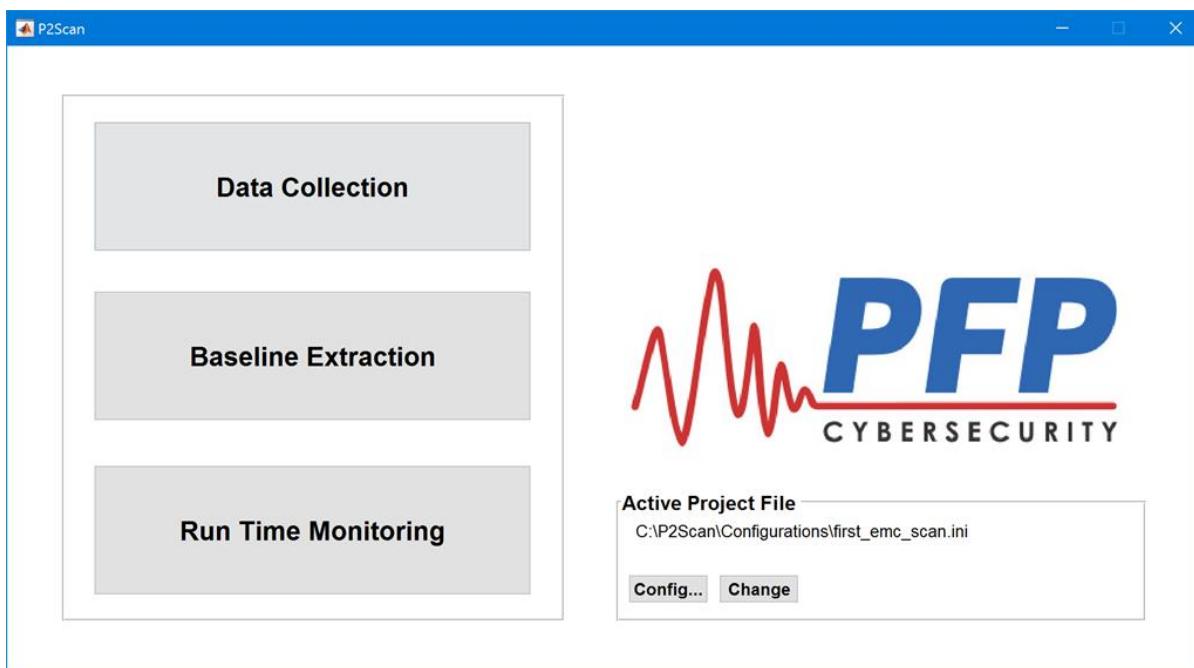
- a. To create a new project, click the **New Project** button on the home page (Figure 2-4). This will open the Create New Project window (Figure 2-5). You can change the **Project Name** (alters .ini name), the **Project Template** (select an .ini template to use), and the **Project Root** (creates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

Figure 2-5 New Project Creation



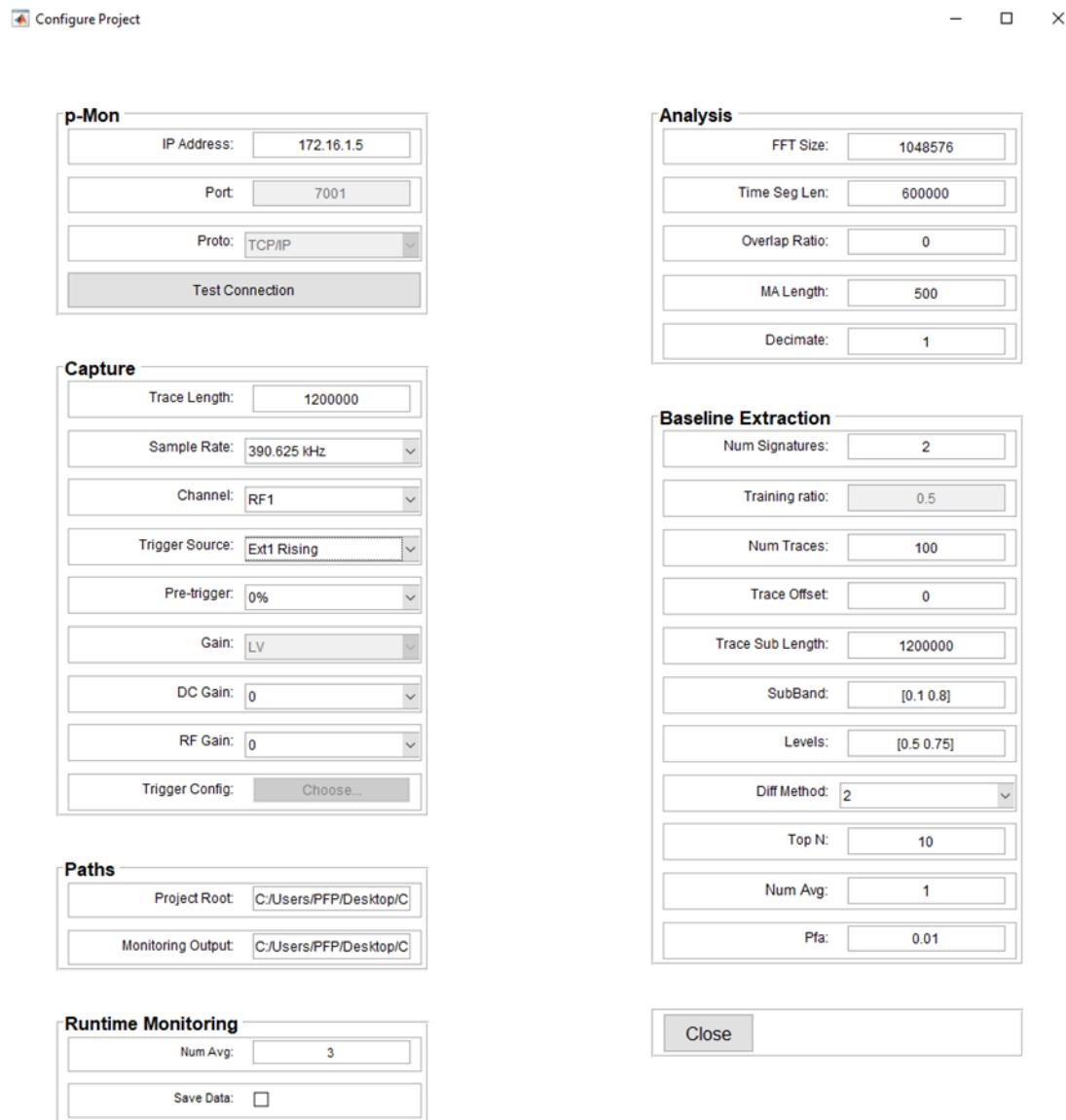
2. Once a project (new or existing) has been created, click **Load Project** on the home page (Figure 2-4). Navigate to the directory specified in **Project Root**, and select the .ini file that you created, which holds default values for guiding P2Scan.
3. Once the configuration file is loaded, P2Scan shows the main screen (Figure 2-6). The user should see the path of their project file in the **Active Project File** dialogue box. To select a different file, click the **Change** button.

Figure 2-6 P2Scan Main Screen



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

Figure 2-7 P2Scan Configuration Parameters



2.5.1.3 Collection Process

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

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

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

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

Figure 2-8 Data Collection Screen During Capture



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

2.5.1.4 Baseline Extraction (Tool Training)

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

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

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

Figure 2-9 Completed Baseline Extraction Screen



The figure shows a screenshot of the P2Scan software interface. At the top right is the PFP Cybersecurity logo. On the left, there's a 'Configuration' section with radio buttons for 'Algorithm' (selected) and 'Analysis'. Below it is the 'Baseline Extraction' configuration panel with the following settings:

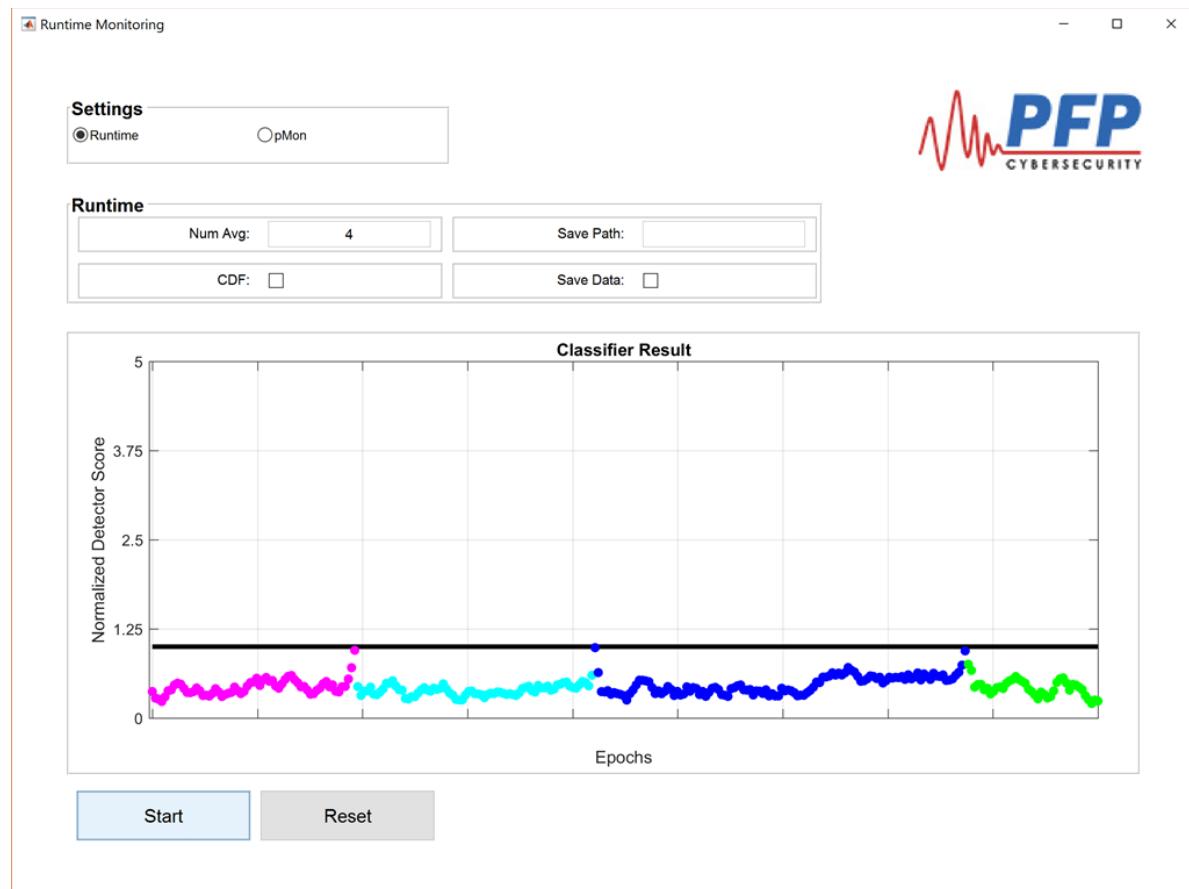
Trace Sub Length:	1000
Trace Sub Offset:	0
SubBands:	[0.116 0.44]
Levels:	[0.5 0.75]
Diff Method:	Z
Top N:	5
Pfa:	0.01
CDF:	<input type="checkbox"/>

At the bottom of the configuration panel, a blue progress bar indicates completion: **Finished. PDs: 1.00 0.99 0.00**. Below the progress bar are two buttons: 'Cancel' (in a blue box) and 'Launch Monitoring'.

2.5.1.5 Runtime Monitoring

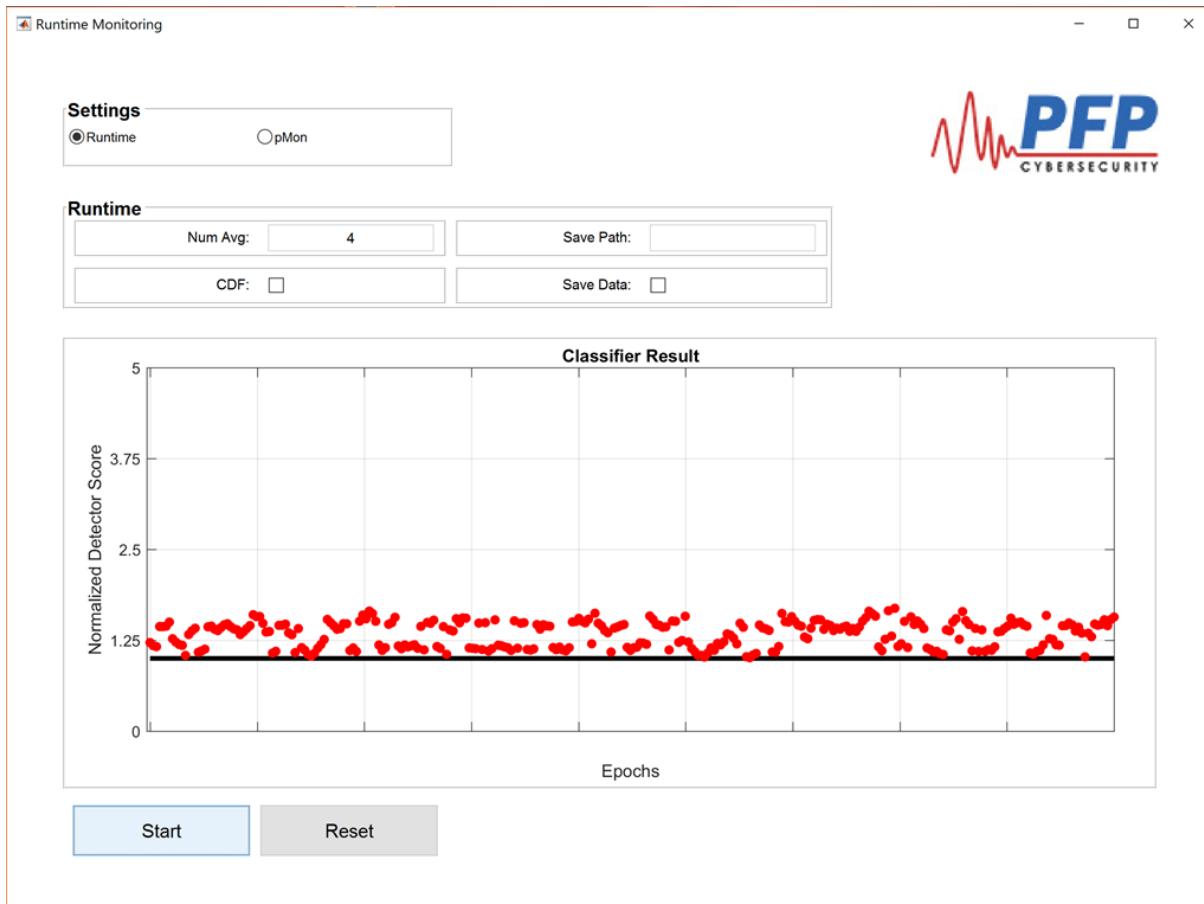
Once the necessary baselines have been calculated during tool training, P2Scan is able to perform runtime monitoring of devices that have been previously characterized. The runtime monitor compares the test signals captured by the appliance, and compares them against the baselines. If the test device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

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



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

Figure 2-11 Runtime Monitoring Showing an Anomalous State



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

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

```
1 Time=2015/11/19 16:19:25.095, PathID=1, TestStat=0.51952
2 Time=2015/11/19 16:19:25.593, PathID=1, TestStat=0.651472
3 Time=2015/11/19 16:19:26.098, PathID=1, TestStat=0.725039
4 Time=2015/11/19 16:19:26.598, PathID=1, TestStat=0.852453
5 Time=2015/11/19 16:19:27.107, PathID=1, TestStat=0.981368
6 Time=2015/11/19 16:19:27.609, PathID=1, TestStat=0.789816
7 Time=2015/11/19 16:19:28.110, PathID=1, TestStat=0.71154
8 Time=2015/11/19 16:19:28.613, PathID=1, TestStat=0.620868
9 Time=2015/11/19 16:19:29.120, PathID=1, TestStat=0.615049
10 Time=2015/11/19 16:19:29.631, PathID=1, TestStat=0.574909
11 Time=2015/11/19 16:19:30.137, PathID=1, TestStat=0.57405
12 Time=2015/11/19 16:19:30.642, PathID=1, TestStat=0.47717
13 Time=2015/11/19 16:19:31.160, PathID=1, TestStat=0.501458
14 Time=2015/11/19 16:19:31.663, PathID=1, TestStat=0.737632
15 Time=2015/11/19 16:19:32.172, PathID=1, TestStat=0.780725
16 Time=2015/11/19 16:19:32.692, PathID=1, TestStat=0.826027
17 Time=2015/11/19 16:19:33.195, PathID=1, TestStat=0.833921
18 Time=2015/11/19 16:19:33.700, PathID=1, TestStat=0.669008
19 Time=2015/11/19 16:19:34.206, PathID=1, TestStat=0.518836
20 Time=2015/11/19 16:19:34.712, PathID=1, TestStat=0.539068
21 Time=2015/11/19 16:19:35.232, PathID=1, TestStat=0.498789
22 Time=2015/11/19 16:19:35.737, PathID=1, TestStat=0.468708
23 Time=2015/11/19 16:19:36.243, PathID=1, TestStat=0.5328
24 Time=2015/11/19 16:19:36.752, PathID=1, TestStat=0.305793
25 Time=2015/11/19 16:19:37.260, PathID=1, TestStat=0.178354
26 Time=2015/11/19 16:19:37.768, PathID=1, TestStat=0.285738
```

2.5.2 Clearwater IRM|Analysis™ Software

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

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

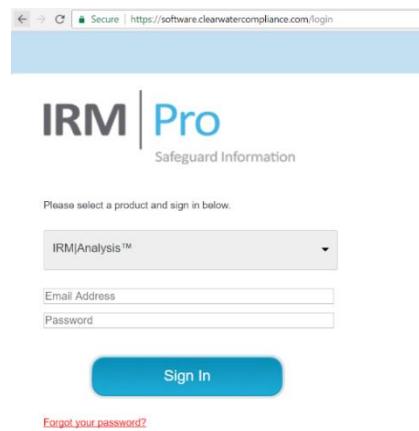
1. Log into IRM|Analysis.
2. Import **Inventory of Information Assets**, or enter the data through the **Asset Inventory Form**.
3. Establish conformance with the NIST-based Security Controls.
4. Determine the **Risk Rating** of the likelihood and impact.
5. Identify those risks that exceed the established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

6. Document the **Risk Response** and associated tasks necessary to mitigate, transfer, avoid, or accept the risk in the IRM|Analysis software.
7. Leverage **Dashboard and Reporting** functionality to provide documentation and evidence of a credible and bona fide risk analysis.

2.5.2.1 Login to IRM|Analysis

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

Figure 2-13 IRM|Analysis Login Page



The screenshot shows the IRM|Analysis login page. At the top, there is a header bar with a back arrow, forward arrow, and a secure connection indicator. Below the header, the IRM|Pro logo is displayed with the tagline "Safeguard Information". A message "Please select a product and sign in below." is present. A dropdown menu is open, showing "IRM|Analysis™" as the selected option. Below the dropdown are two input fields for "Email Address" and "Password". At the bottom of the form is a blue "Sign In" button. A small link "Forgot your password?" is located just above the "Sign In" button.

2.5.2.2 Enter Asset Inventory

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

Follow these steps to add a new asset:

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

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

Figure 2-14 Asset Inventory List

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"/>

Figure 2-15 New Asset

Asset

Asset name *

Asset description

Select all items that create, receive, store, transmit or view sensitive information

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

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 ?

Selected

Approximate # of sensitive records stored on this asset

Asset Business Owner

First name

Last name

* Indicates a required field

Follow these steps to update an asset:

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

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

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

Figure 2-16 Media/Asset Groups

The screenshot shows the IRM|Analysis tool interface. The left sidebar has a dark theme with white icons and text. The main area has a light blue header bar. Below it, there are two sections: 'Electronic Medical Device' and 'Laptop'. Each section contains a table with columns: Media ID, Media, Label, and Information Assets. The 'Edit' and 'Delete' buttons are located at the bottom right of each table.

Media ID	Media	Label	Information Assets	Action
45.1	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	Edit Delete
45.2	Electronic Medical Device	Contains ePHI; default	InfusionPump_3	Edit Delete

Media ID	Media	Label	Information Assets	Action
46.1	Laptop		Workstation Applications	Edit Delete

Figure 2-17 Edit Media/Asset Group

The screenshot shows the IRM|Analysis tool's interface for managing media/asset groups. On the left, there is a navigation sidebar with various menu items like Dashboard, Framing/Governance, Assets (with Asset Inventory List, Asset Inventory Import, and Media/Asset Groups), Risk Determination, Risk Response, Documents, Reports, Manage Account, and Support. The main area is titled 'Edit your Media/Asset Group' and contains a table for organizing assets into unique media groups. The table has columns for Media Id, Media Name, Label, Risk Analyst, Due Date, and Information Assets. Two rows are visible: one for '45.1 Electronic Medical Device' and another for '45.2 Electronic Medical Device'. The 'Information Assets' column lists several infusion pump models. To the right of the table is a 'Create new Media/Asset Group' section with a large input box for dragging assets and a checkbox for 'Copy Risk Determination Information from the source group'. At the bottom are 'Save' and 'Cancel' buttons.

2.5.2.3 Risk Determination

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

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

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

Figure 2-18 Controls – Global/Media

Control	Status	Response	Count
Testing of Password Strengths (NIST)	Yes	In Progress	0
Training for the Security Workforce (NIST)	Yes	In Progress	1
Two-man Rule (NIST)	Yes	In Progress	0
Uninterruptable power supply (UPS) (NIST)	Yes	In Progress	0
User Account Management (NIST)	Yes	In Progress	0
User Activity Review (NIST)	Yes	In Progress	0
User Permissions Reviews (NIST)	Yes	In Progress	0
Visitor Access Control (NIST)	Yes	In Progress	1
Wipe, Erase, or Destroy Disks (Hard Drives, etc.) (NIST)	Yes	In Progress	0
Wireless access restrictions (NIST)	Yes	In Progress	1
Wireless Encryption (NIST)	Yes	In Progress	0
Wireless Link Protection (NIST)	Yes	In Progress	0
Wireless Security Policy and Procedures (NIST)	Yes	In Progress	1

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

1. On the IRM|Analysis tool, expand **Risk Determination** on the left menu bar.
2. Under **Risk Determination**, click **Risk Questionnaire List**.
3. On the **Risk Questionnaire List** page (Figure 2-19), scroll up and down to view the media/asset groups.
4. For each relevant **Media/Asset Group**, select the **Risk Analyst**, fill in the **Due Date**, and then click the **Continue** button to access the **Risk Questionnaire Form** (Part 1: Figure 2-20, and Part 2: Figure 2-21).
5. For each control, select one of the responses (i.e., **Yes**, **In Progress**, **No**, or **N/A**) to indicate the response status (example shown in Part 1: Figure 2-20), if it was already noted on the **Controls – Global/Media** page.
6. Controls can be set globally or for individual **Media/Asset Groups**. The plus sign (+) will expand the control to reveal the **Media/Asset Groups** so that the control can be set individually. To illustrate, a global control can be set for **Training for the Security Workforce**, but an individual control would be set for each of the Media/Asset Groups associated with the **User Activity Review**, as only a subset of assets may undergo a user activity review.
7. Determine and select the **Risk Likelihood** and **Risk Impact** for the selected risk scenario (example shown in Part 2: Figure 2-21) to populate the **Risk Rating**.

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

Figure 2-19 Risk Questionnaire List

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

Figure 2-20 Risk Questionnaire Form (Part 1)

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

Control	NIST SP 800-53 Requirement	Response	Clear	Global
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	Yes In Progress No N/A	(X)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Inventory Control Process ?	MA-2 a, MA-2 b, MA-2 c, MA-2 CE1, MA-2 CE2, MA-2 d, MA-2 e	Yes In Progress No N/A	(X)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Physical Access Monitoring ?	PE-6 a, PE-6 b, PE-6 c	Yes In Progress No N/A	(X)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Physical Security Policy and Procedures ?	PE-1 a, PE-1 b	Yes In Progress No N/A	(X)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Physically Securing Devices or Systems When Not in Use ?	PE-3 c, PE-3 d, PE-3 e, PE-3 f, PE-3 g	Yes In Progress No N/A	(X)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Security/privacy Awareness and Training ?	AT-1 a, AT-1 b, AT-2, AT-3, AT-4 a, AT-4 b	Yes In Progress No N/A	(X)	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Figure 2-21 Risk Questionnaire Form (Part 2)

Description	NIST	Status	Treatment Options
Controlled access to areas with mobile devices	3 c, PE-3 d, PE-3 e, PE-3 f, PE-3 g NIST	Yes, In Progress, No, N/A	[Treatment Options]
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	[Treatment Options]
Physical Access Monitoring	PE-6 a, PE-6 b, PE-6 c NIST	Yes, In Progress, No, N/A	[Treatment Options]
Physical Security Policy and Procedures	PE-1 a, PE-1 b NIST	Yes, In Progress, No, N/A	[Treatment Options]
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	[Treatment Options]
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	[Treatment Options]

Add a Custom Control or Recommendation

Risk Rating for this Threat/Vulnerability for the Media/Asset(s) Listed Above

Description	Risk Rating	Risk Notes
Risk Likelihood	Rare	0
Risk Impact	Moderate	3

Return to Risk Questionnaire List Go to the next Threat/Vulnerability for this Media

2.5.2.4 Risk Response

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

Consider following these risk response steps:

1. In the IRM|Analysis tool, expand **Risk Response** in the left menu bar.
2. Under **Risk Response**, click **Risk Response List**.
3. Only the risks that exceed the risk threshold established under **Framing/Governance** (in the left menu bar) will move to the **Risk Response** portion of the software.
4. On the **Risk Response List – Risk Registry** page (Figure 2-22), scroll up and down to view the Media/Asset Groups, along with the associated **Threat Source/Event**, **Vulnerability**, and **Risk Rating**.
5. For each relevant risk response, click the associated button in the **Treatment** column to access the **Risk Treat and Evaluate Form** page of that risk (Figure 2-23).
6. On the **Risk Treat and Evaluate Form** page (Figure 2-23), perform the risk response analysis by selecting the **Risk Treatment Type**; evaluate the control or recommendation; **Select a Risk Owner**; enter **Risk Notes**; etc.

Figure 2-22 Risk Response List – Risk Registry

The screenshot shows the IRM|Pro interface for the Risk Response List - Risk Registry. The left sidebar includes options like Dashboard, Framing/Governance, Assets, Risk Determination, Risk Response (selected), Risk Response List, Controls Response Review, Risk Action Plan, Risk Reconciliation, Documents, Reports, Manage Account, and Support. The main content area has a header "Risk Response List - Risk Registry" with a "Edit Mode On" button. It displays a table of risk items:

Media/Label	Asset Name	Threat Source/Event	Vulnerability	Risk Rating	Residual Rating	Treatment	Evaluation	Ir
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 Vulnerabilities in Password Creation and Distribution	?	25	-	TBD	TBD	
0% Electronic Medical Device / Contains ePHI; default	InfusionPump_3	Careless IT Personnel/Insecure User 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	Careless User/Weak Passwords	Weak Passwords	?	25	-	TBD	TBD

Figure 2-23 Risk Treat and Evaluate Form

The screenshot shows the IRM|Pro interface for the Risk Treat and Evaluate Form. The left sidebar includes options like Dashboard, Framing/Governance, Assets, Risk Determination, Risk Response (selected), Risk Response List, Controls Response Review, Risk Action Plan, Risk Reconciliation, Documents, Reports, Manage Account, and Support. The main content area has a header "Risk Treat and Evaluate Form" with a "Select Risk Treatment, Alternatives, Residual Risk and Status" button. It displays a table of risk analysis findings:

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

Below this, there's a section titled "Evaluate alternatives that would prevent this threat from exploiting the vulnerabilities listed above" with a table of control recommendations:

Control or Recommendation	Effectiveness *	Estimated Cost	Feasibility *	Global	Action *	Enhance	Not applicable	Approve
Control or Recommendation	?							
Control or Recommendation	Highly Effective	\$	Highly Feasible					
Control or Recommendation	Select	\$	Select					
Control or Recommendation	Select	\$	Select					
Control or Recommendation	Select	\$	Select					

At the bottom, there are sections for "Add a Custom Control or Recommendation", "Select a Risk Owner", "Risk Notes", "Select the Residual Risk", "Select a Status", and "Send Email Notification".

2.5.2.5 Dashboard and Report

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

1. On the IRM|Analysis tool, expand **Dashboard** on the left menu bar.
2. Under **Dashboard**, click **Rating Distribution By Asset**.
3. See the example dashboard on the **Rating Distribution By Asset** page shown in Figure 2-24.

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

Figure 2-24 Dashboard Example



For report views, follow these steps:

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

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

Figure 2-25 Report Example

The screenshot shows the IRM Pro interface with a sidebar menu and a main report view. The report is titled 'Risk Rating Report' and displays a table of vulnerabilities. The columns include Media / Label, Asset Name(s), Threat Source/Event, Vulnerability, Likelihood, Impact, and Rating. The table lists various assets like InfusionPump_3, Workstation Applications, and Server, along with their respective threat sources, vulnerabilities, and risk scores.

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	15
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 / Impaired 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 / Impaired 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

2.5.3 MDISS MDRAP

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

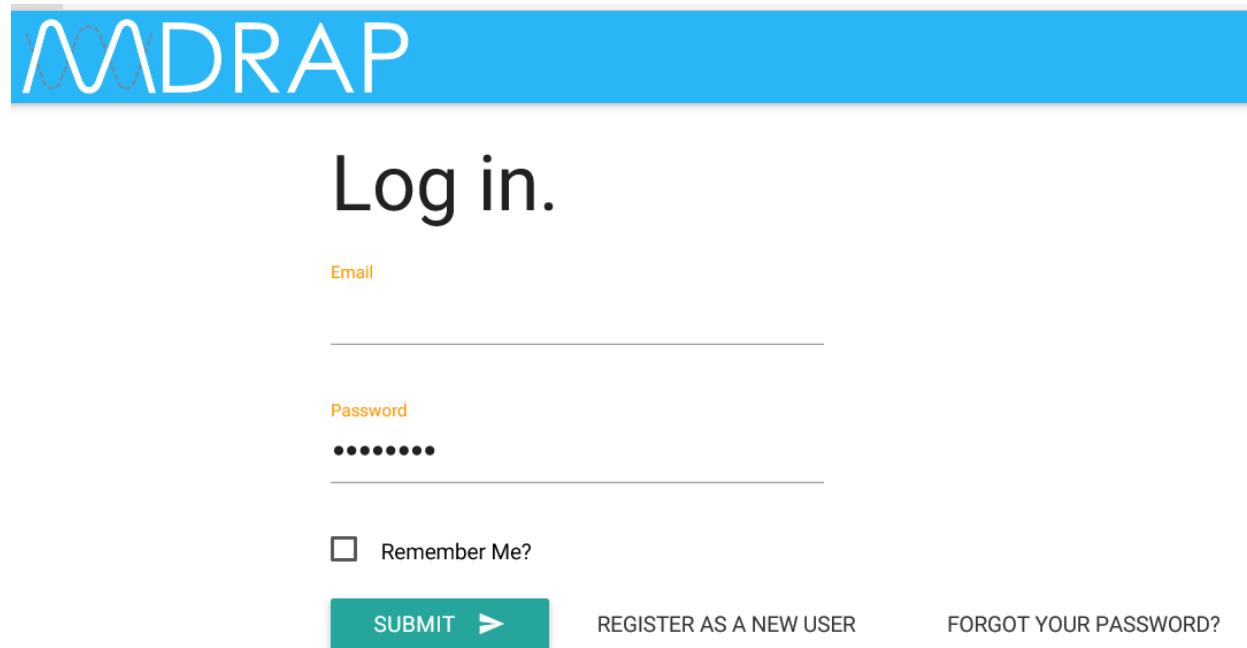
Please note that this section does not show you how to conduct a risk assessment. Instead, we show these basic steps for using the MDRAP tool:

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

2.5.3.1 Login to MDRAP

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

Figure 2-26 MDRAP Login Page



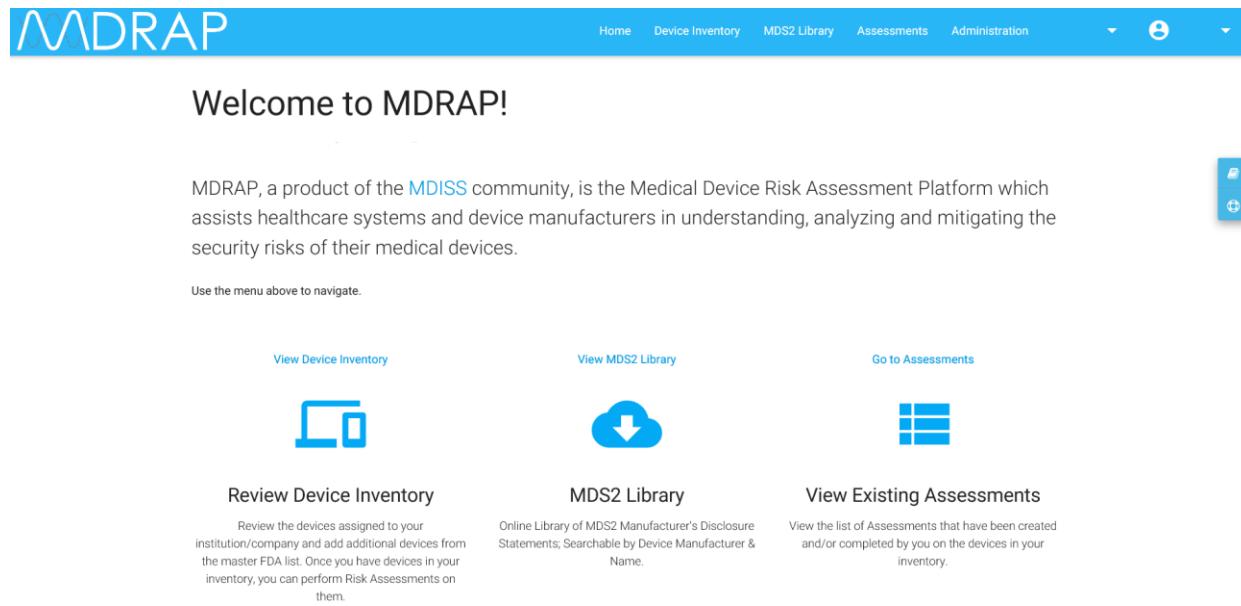
The image shows the MDRAP login page. At the top, there is a blue header bar with the MDRAP logo. Below the header, the word "Log in." is displayed in a large, bold, black font. There are two input fields: one for "Email" containing "admin@nist.gov" and one for "Password" containing "*****". Below the password field is a checkbox labeled "Remember Me?". At the bottom left is a teal "SUBMIT" button with a white arrow icon. To the right of the submit button are links for "REGISTER AS A NEW USER" and "FORGOT YOUR PASSWORD?".

2.5.3.2 Conduct Device Inventory

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

1. On the **Welcome to MDRAP** page (Figure 2-27), click **Device Inventory** on the menu bar, or click the **View Device Inventory** link on the page.
2. On the **Device Inventory** page (Figure 2-28), add an individual device, edit a device, or bulk import a group of devices.

Figure 2-27 MDRAP Welcome Page



The screenshot shows the MDRAP welcome page. At the top, there is a blue header bar with the MDRAP logo on the left and navigation links for Home, Device Inventory, MDS2 Library, Assessments, and Administration. On the right side of the header are user profile icons. Below the header, the main content area has a title "Welcome to MDRAP!". A paragraph explains that MDRAP is a product of the MDISS community, designed to assist healthcare systems and device manufacturers in understanding, analyzing, and mitigating security risks of medical devices. A note says "Use the menu above to navigate." Below this, there are three main sections with icons and titles: "View Device Inventory" (icon of two overlapping rectangles), "View MDS2 Library" (icon of a cloud with a downward arrow), and "Go to Assessments" (icon of a grid). Each section also has a detailed description below its title.

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

Use the menu above to navigate.

[View Device Inventory](#) [View MDS2 Library](#) [Go to Assessments](#)

Review Device Inventory
Review the devices assigned to your institution/company and add additional devices from the master FDA list. Once you have devices in your inventory, you can perform Risk Assessments on them.

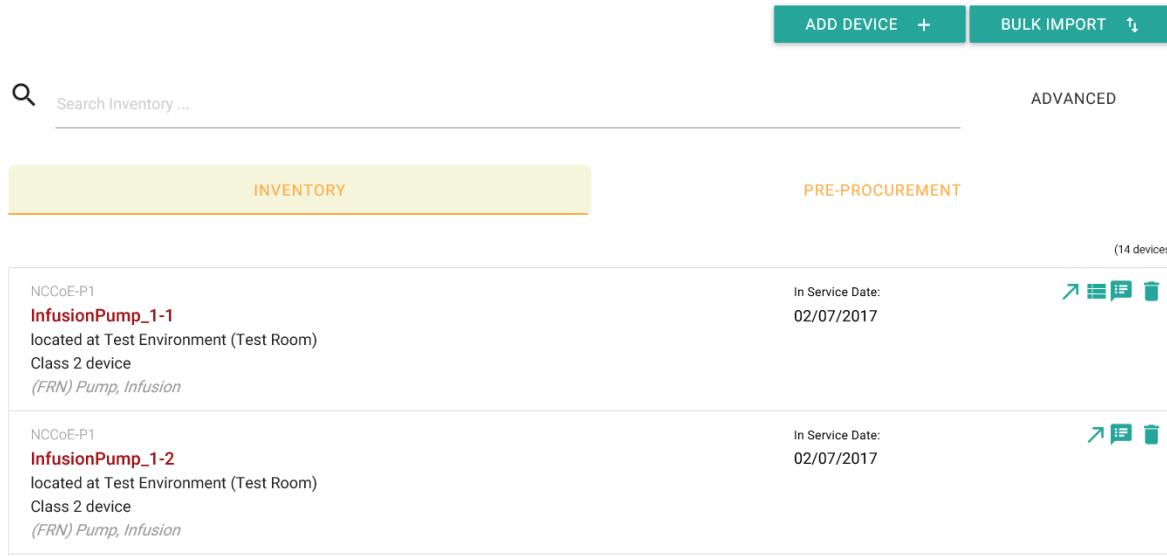
MDS2 Library
Online Library of MDS2 Manufacturer's Disclosure Statements; Searchable by Device Manufacturer & Name.

View Existing Assessments
View the list of Assessments that have been created and/or completed by you on the devices in your inventory.

Figure 2-28 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.



The screenshot shows the Device Inventory list page. At the top, there is a header with a search bar containing "Search Inventory ...", a "BULK IMPORT" button, and an "ADVANCED" link. Below the header, there are two tabs: "INVENTORY" (which is selected) and "PRE-PROCUREMENT". A total count of "(14 devices)" is shown. The main content area displays a table with two rows of device information. Each row includes the device name, location, classification, description, service date, and edit/delete icons.

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

a. To add a device:

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

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

Figure 2-29 Add Device

The screenshot shows a web-based application for selecting devices from a catalog. At the top, a header reads "Select a Device from the Catalog". Below it, a search bar says "Search Catalog...". To the right of the search bar is an information icon (i) and a link "(414 devices)". A "Commonly Used" section is displayed, containing two entries:

- CAREFUSION**
Alaris PCU 8000 Series (The Alaris® 8000 Point-of-Care (PC) Unit is the core of the Alaris® System and provides a common user interface for programming infusion and monitoring modules.)
Class 2 device
(FRN) Pump, Infusion
An "ADD" button is located to the right of the device description.
- ZOLL MEDICAL**
ZOLL M SERIES
Class 2 device
(CCK) Analyzer, Gas, Carbon-Dioxide, Gaseous-Phase
An "ADD" button is located to the right of the device description.

At the bottom right of the page is a "CANCEL" button.

- b. To edit a device:
- On the **Device Inventory** page (see Figure 2-28 above), locate the device from the list, and then click the product name link or the edit icon.
 - On the **Edit Inventory** page (Figure 2-30), update the data, and then click **Save**.

Figure 2-30 Edit Device

Edit Inventory InfusionPump_1-1

DETAILS

Device Name
Search for a Device

Inventory Name
InfusionPump_1-1

Location
Test Environment

Care Delivery Area
Test Room

Serial # Asset Tag #

In Service Date
02/07/2017

Notes

ATTACHMENTS

Assessment Phase
Inventory

CANCEL **SAVE**

- c. To bulk import a group of devices:
- i. On the **Device Inventory** page (Figure 2-28 above), click the **BULK IMPORT** button.
 - ii. On the **Inventory Bulk Import** page (Figure 2-31), download the template, and then fill-in the data into the template.
 - iii. Follow the instruction to upload and import the devices by using the template (Figure 2-32).

Figure 2-31 Inventory Bulk Import

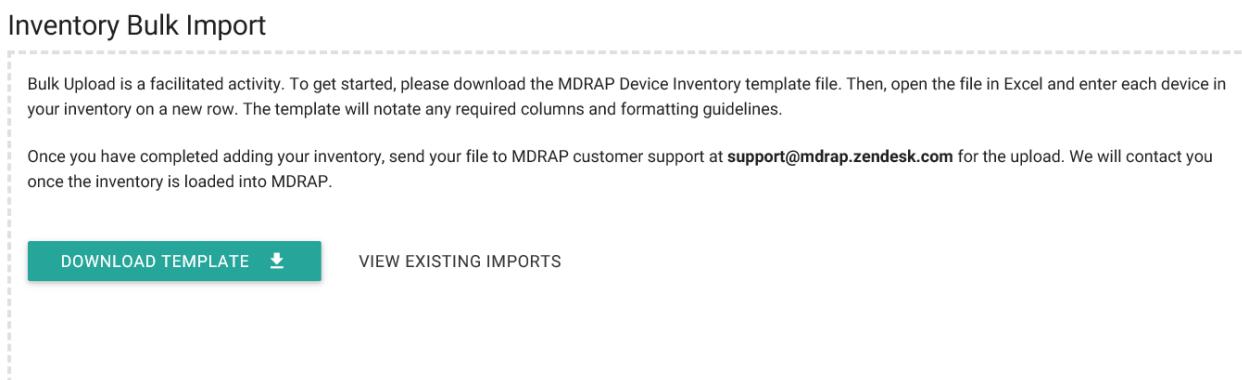


Figure 2-32 Device Inventory Template Sample

2.5.3.3 Risk Assessment

We created a risk assessment for each device by responding to the MDRAP's built-in questionnaire. The basic steps of creating a risk assessment for a given device are listed below.

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

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

Figure 2-33 Create Assessment (Part 1)

The screenshot shows a 'Create Assessment' interface. At the top, it says 'To add a new Assessment, first select a Device in your Inventory.' Below this is a search bar with a magnifying glass icon and the placeholder 'Search Inventory ...'. To the right of the search bar is an 'ADVANCED' button. A list of devices is displayed in a table format. The first device listed is 'NCCoE-P1 InfusionPump_1-1', which is described as 'located at Test Environment (Test Room)', a 'Class 2 device', and '(FRN) Pump, Infusion'. Its 'In Service Date' is listed as '02/07/2017'. The second device listed is 'NCCoE-P1 InfusionPump_1-2', also located at 'Test Environment (Test Room)' and described as a 'Class 2 device'. Its '(FRN) Pump, Infusion' and 'In Service Date' are both listed as '02/07/2017'. In the top right corner of the device list area, it says '(14 devices)'. At the bottom right of the interface are 'CANCEL' and 'ADD' buttons.

Figure 2-34 Create Assessment (Part 2)

Create Assessment

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

 InfusionPump_1-2	
--	---

Assessment Title
MDISS Assessment for InfusionPump_1-2

Select the Risk Assessment Questionnaire form to use
MDISS Questionnaire

The MDISS questionnaire is the recommended default for risk assessment and scoring.

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

CANCEL **ADD**

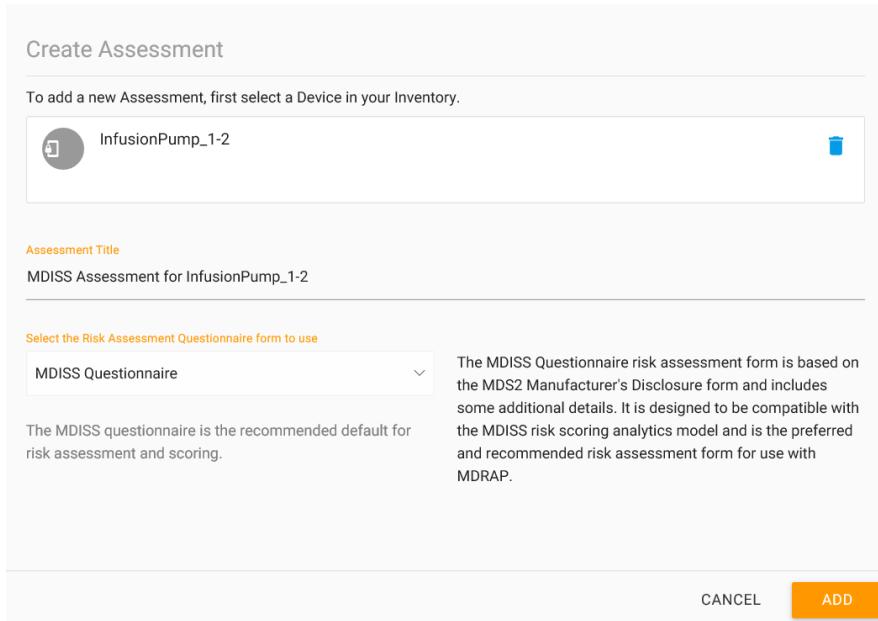


Figure 2-35 Assessment Step (Example 1)

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

Back to Assessment Summary  

#1/4

Management of Private Data

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

Yes
 No



PREVIOUS 

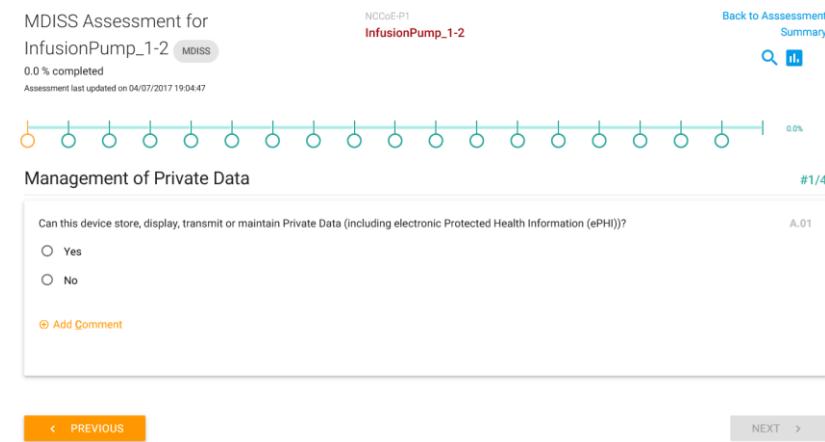


Figure 2-36 Assessment Step (Example 2)

MDISS Assessment for InfusionPump_1-2 MDISS

NCCoE-P1
InfusionPump_1-2

8.3 % completed
Assessment last updated on 04/07/2017 15:10:09

Back to Assessment Summary 🔍 ⓘ

Other Questions Affecting Exposure #4/8

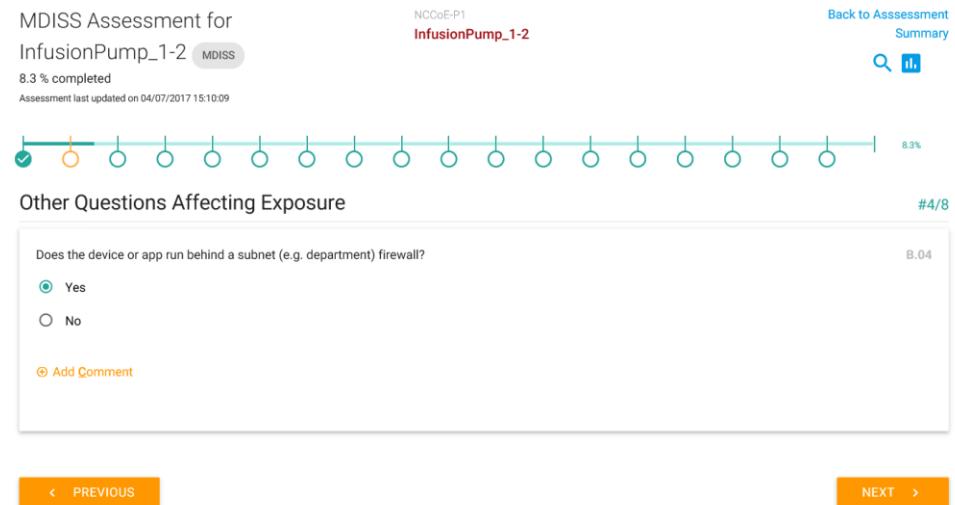
Does the device or app run behind a subnet (e.g. department) firewall? B.04

Yes

No

ⓘ Add Comment

PREVIOUS NEXT >



2.5.3.4 Dashboard and Reports

MDRAP computes assessment results based on the responses to the questionnaires. For a given assessment (complete or partially complete), the assessment result is available for view as a dashboard (Figure 2-37) or report (Figure 2-38).

Figure 2-37 Assessment Result (Dashboard Example)

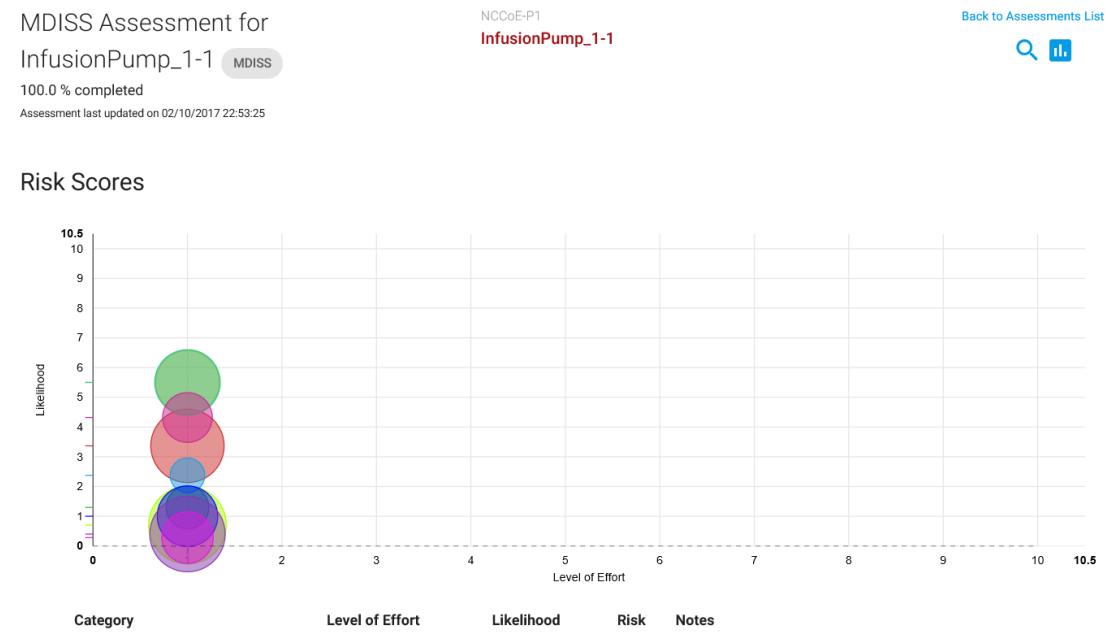


Figure 2-38 Assessment Result (Report Example)

Category	Level of Effort	Likelihood	Risk	Notes
█ Audit Controls	1	3.367	5.25	* Patient identity not captured.
█ Authorization	1	5.5	3.75	* Authorization can be bypassed using an API. * Operator can acquire root-level privilege. * Root-level privilege is the only authorization mode.
█ Automatic Logoff	1	0.7	6	
█ Cyber Security Product Upgrades	1	1.295	1.175	* Device OS is not supported by the OS manufacturer.
█ Malware Detection / Protection	1	5.5	4	* No Virus Protection
█ Other Scoreable MDS2 Security Categories	1	2.375	0.453	* No 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	

Appendix A Baseline Configuration File

A.1 Baseline Configuration File

```
ASA Version 9.6(1)
!
interface Management0/0
    ip address 192.168.29.149 255.255.255.0
!
! optional, SSH, version is important as v1 is insecure and on by default, also set
your own password!
username [*****] password [*****]
aaa authentication ssh console LOCAL
!
! set to network and interface you want to manage from, can be WAN
ssh 192.168.29.0 255.255.255.0 management
ssh version 2
!
hostname internal-kmcfadde
!
! Configure network interfaces
interface GigabitEthernet0/0
    nameif WAN
    security-level 50
    ip address 192.168.100.149 255.255.255.0
    no shutdown
!
! optional, authenticated OSPF for excellence
    ospf authentication-key [L}N]@Uv
    ospf authentication message-digest
!
interface GigabitEthernet0/1
    nameif LAN
    security-level 100
    ip address 192.168.150.1 255.255.255.0
```

```
no shutdown
!
! optional, DHCP Server
dhcpd address 192.168.150.220-192.168.150.250 LAN
dhcpd dns 8.8.8.8 8.8.4.4
dhcpd option 3 ip 192.168.150.1
dhcpd enable LAN
!
! optional, OSPFv2
router ospf 1
network 192.168.100.0 255.255.255.0 area 0
redistribute connected subnets
redistribute static subnets
!
! Configure DNS resolution here, required for license activation
dns domain-lookup WAN
dns server-group DefaultDNS
name-server 8.8.8.8
name-server 8.8.4.4
!
license smart
feature tier standard
throughput level 1G
names
!
! optional, Configure time zone and NTP here
clock timezone EST -5
clock summer-time EDT recurring
ntp server 10.97.74.8
!
! Allow ping through LAN to WAN
policy-map global_policy
```

```

class inspection_default
    inspect icmp
    inspect icmp error
!
! Show up in traceroute
policy-map global_policy
    class class-default
        set connection decrement-ttl
!
! Make ICMP/UDP traceroute work from LAN to WAN
object-group icmp-type PING-REPLIES
    icmp-object echo-reply
object-group icmp-type TRACEROUTE-REPLIES
    icmp-object time-exceeded
    icmp-object unreachable
    group-object PING-REPLIES
access-list 101 extended permit icmp any any object-group TRACEROUTE-REPLIES
access-list 101 extended permit icmp any any object-group PING-REPLIES
!
! Allow ICMP ping/traceroute from WAN to LAN
object-group icmp-type PING
    icmp-object echo
access-list 101 extended permit icmp any any object-group PING
!
! Allow UDP traceroute from WAN to LAN
object-group service TRACEROUTEUDP
    service-object udp destination gt 33434
access-list 101 extended permit object-group TRACEROUTEUDP any any
!
! example, allow a specific port on a host
! access-list 101 extended permit tcp any host 192.168.140.XXX eq www
!
```

```

! Add firewall rules we created to WAN interface
access-group 101 in interface WAN
!
! Example, set a static route
! route WAN 192.168.140.0 255.255.255.0 192.168.100.111
!
! SNMP
object network SNMPHOSTS
  subnet 192.168.29.0 255.255.255.0
snmp-server enable
snmp-server community public
snmp-server host-group management SNMPHOSTS

```

A.2 External Firewall and Guest Network ASA Configuration File

```

: Saved
:
: Serial Number: 9AK64JT2D2M
: Hardware:    ASA V, 2048 MB RAM, CPU Xeon E5 series 2200 MHz
:
ASA Version 9.6(1)
!

hostname border-kmcfadde
enable password [*****] encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
!
```

```
license smart
feature tier standard
throughput level 1G
names

!
interface GigabitEthernet0/0
nameif WAN
security-level 0
ip address 10.32.3.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif LAN
security-level 100
ip address 192.168.100.101 255.255.255.0
ospf authentication-key *****
ospf authentication message-digest
!
interface GigabitEthernet0/2
nameif GUEST
security-level 100
ip address 192.168.170.1 255.255.255.0
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/4
shutdown
no nameif
```

```
no security-level
no ip address
!
interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/8
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
nameif management
security-level 0
ip address 192.168.29.147 255.255.255.0
```

```
!
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns domain-lookup WAN
dns server-group DefaultDNS
  name-server 8.8.8.8
  name-server 8.8.4.4
object network LAN-SUBNETS
  subnet 192.168.0.0 255.255.0.0
object network SNMPHOSTS
  subnet 192.168.29.0 255.255.255.0
object-group icmp-type PING-REPLIES
  icmp-object echo-reply
object-group icmp-type TRACEROUTE-REPLIES
  icmp-object time-exceeded
  icmp-object unreachable
  group-object PING-REPLIES
object-group icmp-type PING
  icmp-object echo
object-group service TRACEROUTEUDP
  service-object udp destination gt 33434
access-list 101 extended permit icmp any any object-group TRACEROUTE-REPLIES
pager lines 23
mtu WAN 1500
mtu LAN 1500
mtu management 1500
mtu GUEST 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
```

```
arp timeout 14400
no arp permit-nonconnected
!
object network LAN-SUBNETS
nat (LAN,WAN) dynamic interface
access-group 101 in interface WAN
!
route-map DEFAULT permit 10
match interface WAN

!
router ospf 1
network 192.168.100.0 255.255.255.0 area 0
log-adj-changes
redistribute connected subnets
redistribute static subnets
default-information originate
!
route WAN 0.0.0.0 0.0.0.0 10.32.3.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
snmp-server host-group management SNMPHOSTS poll community *****
no snmp-server location
no snmp-server contact
```

```
snmp-server community *****  
crypto ipsec security-association pmtu-aging infinite  
crypto ca trustpoint _SmartCallHome_ServerCA  
no validation-usage  
crl configure  
crypto ca trustpool policy  
auto-import  
crypto ca certificate chain _SmartCallHome_ServerCA  
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491  
308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130  
0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117  
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b  
13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504  
0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72  
20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56  
65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043  
65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d31  
30303230 38303030 3030305a 170d3230 30323037 32333539 35395a30 81b5310b  
30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20  
496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65  
74776f72 6b313b30 39060355 040b1332 5465726d 73206f66 20757365 20617420  
68747470 733a2f2f 7777772e 76657269 7369676e 2e636f6d 2f727061 20286329  
3130312f 302d0603 55040313 26566572 69536967 6e20436c 61737320 33205365  
63757265 20536572 76657220 4341202d 20473330 82012230 0d06092a 864886f7  
0d010101 05000382 010f0030 82010a02 82010100 b187841f c20c45f5 bcab2597  
a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bb658e 444f4dce 6fed094a d4af4e10  
9c688b2e 957b899b 13cae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc  
7f432657 5833833b 330a17b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b  
15fca34b 3bce6388 d0f82d0c 948610ca b69a3dca eb379c00 48358629 5078e845  
63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8  
18b49ae8 3c6e81fd e4cd3536 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced  
4a546ac9 4dc5bf11 blaelc67 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 589cf36 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 4ad99f42fbe198e6 42839b8f 8f6724e8
6119b5dd cdb50b26 058ec36e c4c875b8 46cfe218 065ea9ae a8819a47 16de0c28
6c2527b9 deb78458 c61f381e a4c4cb66

quit

telnet timeout 5

ssh stricthostkeycheck

ssh 192.168.29.0 255.255.255.0 management

ssh timeout 5

ssh version 2

console timeout 0
```

```
dhcpd dns 8.8.8.8 8.8.4.4
dhcpd option 3 ip 192.168.170.1
!
dhcpd address 192.168.170.220-192.168.170.250 GUEST
dhcpd enable GUEST
!
dynamic-access-policy-record DfltAccessPolicy
username [*****] password [*****] encrypted
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
```

```
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error
class class-default
  set connection decrement-ttl
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
    no active
    destination address http
    https://tools.cisco.com/its/service/oddce/services/DDCEService
    destination address email callhome@cisco.com
    destination transport-method http
    subscribe-to-alert-group diagnostic
    subscribe-to-alert-group environment
    subscribe-to-alert-group inventory periodic monthly
    subscribe-to-alert-group configuration periodic monthly
    subscribe-to-alert-group telemetry periodic daily
  profile License
    destination address http
    https://tools.cisco.com/its/service/oddce/services/DDCEService
    destination transport-method http
Cryptochecksum:9ffa4947d875e0c501e036c54e80ee93
: end
```

A.3 Enterprise Services ASA Configuration File

```
: Saved  
:  
:  
: Serial Number: 9AEHKLC171M  
:  
: Hardware:    ASA V, 2048 MB RAM, CPU Xeon E5 series 2200 MHz  
:  
ASA Version 9.6(1)  
!  
hostname enterprise-services-kmcfadde  
enable password [*****] encrypted  
xlate per-session deny tcp any4 any4  
xlate per-session deny tcp any4 any6  
xlate per-session deny tcp any6 any4  
xlate per-session deny tcp any6 any6  
xlate per-session deny udp any4 any4 eq domain  
xlate per-session deny udp any4 any6 eq domain  
xlate per-session deny udp any6 any4 eq domain  
xlate per-session deny udp any6 any6 eq domain  
!  
license smart  
feature tier standard  
throughput level 1G  
names  
!  
interface GigabitEthernet0/0  
nameif WAN  
security-level 50  
ip address 192.168.100.154 255.255.255.0  
ospf authentication-key *****  
ospf authentication message-digest  
!
```

```
interface GigabitEthernet0/1
    nameif LAN
    security-level 100
    ip address 192.168.120.1 255.255.255.0
!
interface GigabitEthernet0/2
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/3
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/4
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/5
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/6
    shutdown
    no nameif
```

```
no security-level
no ip address
!
interface GigabitEthernet0/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/8
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
nameif management
security-level 0
ip address 192.168.29.154 255.255.255.0
!
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns domain-lookup WAN
dns server-group DefaultDNS
name-server 8.8.8.8
name-server 8.8.4.4
object network SNMPHOSTS
subnet 192.168.29.0 255.255.255.0
object-group service DNS
service-object tcp-udp destination eq domain
```

```
object-group service SYMANTEC-DCS
    service-object tcp destination eq 4443
    service-object tcp destination eq https
    service-object tcp destination eq 8443
    service-object tcp destination eq 2222
access-list 101 extended permit icmp any any time-exceeded
access-list 101 extended permit icmp any any unreachable
access-list 101 extended permit icmp any any echo-reply
access-list 101 extended permit icmp any any echo
access-list 101 extended permit udp any any gt 33434
access-list 101 extended permit object-group DNS 192.168.140.0 255.255.255.0 host
192.168.120.162
access-list 101 extended permit object-group DNS 192.168.140.0 255.255.255.0 host
192.168.120.163
access-list 101 extended permit tcp any host 192.168.120.166 eq 8114
access-list 101 extended permit object-group SYMANTEC-DCS any host 192.168.120.167
pager lines 23
mtu management 1500
mtu WAN 1500
mtu LAN 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group 101 in interface WAN
router ospf 1
    network 192.168.100.0 255.255.255.0 area 0
    log-adj-changes
    redistribute connected subnets
    redistribute static subnets
!
```

```
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
snmp-server host-group management SNMPHOSTS poll community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491
308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130
0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72
20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d31
30303230 38303030 3030305a 170d3230 30323037 32333539 35395a30 81b5310b
30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20
```

496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65
74776f72 6b313b30 39060355 040b1332 5465726d 73206f66 20757365 20617420
68747470 733a2f2f 7777772e 76657269 7369676e 2e636f6d 2f727061 20286329
3130312f 302d0603 55040313 26566572 69536967 6e20436c 61737320 33205365
63757265 20536572 76657220 4341202d 20473330 82012230 0d06092a 864886f7
0d010101 05000382 010f0030 82010a02 82010100 b187841f c20c45f5 bcab2597
a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bb658e 444f4dce 6fed094a d4af4e10
9c688b2e 957b899b 13cae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc
7f432657 5833833b 330a17b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b
15fca34b 3bce6388 d0f82d0c 948610ca b69a3dca eb379c00 48358629 5078e845
63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
18b49ae8 3c6e81fd e4cd3536 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced
4a546ac9 4dc5bf11 b1ae1c67 81cb4455 33997f24 9b3f5345 7f861af3 3cfa6d7f
81f5b84a d3f58537 1cb5a6d0 09e4187b 384efa0f 02030100 01a38201 df308201
db303406 082b0601 05050701 01042830 26302406 082b0601 05050730 01861868
7474703a 2f2f6f63 73702e76 65726973 69676e2e 636f6d30 12060355 1d130101
ff040830 060101ff 02010030 70060355 1d200469 30673065 060b6086 480186f8
45010717 03305630 2806082b 06010505 07020116 1c687474 70733a2f 2f777777
2e766572 69736967 6e2e636f 6d2f6370 73302a06 082b0601 05050702 02301e1a
1c687474 70733a2f 2f777777 2e766572 69736967 6e2e636f 6d2f7270 61303406
03551d1f 042d302b 3029a027 a0258623 68747470 3a2f2f63 726c2e76 65726973
69676e2e 636f6d2f 70636133 2d67352e 63726c30 0e060355 1d0f0101 ff040403
02010630 6d06082b 06010505 07010c04 61305fa1 5da05b30 59305730 55160969
6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
69676e2e 636f6d2f 76736c6f 676f2e67 69663028 0603551d 11042130 1fa41d30
1b311930 17060355 04031310 56657269 5369676e 4d504b49 2d322d36 301d0603
551d0e04 1604140d 445c1653 44c1827e 1d20ab25 f40163d8 be79a530 1f060355
1d230418 30168014 7fd365a7 c2ddecbb f03009f3 4339fa02 af333133 300d0609
2a864886 f70d0101 05050003 82010100 0c8324ef ddc30cd9 589cf36 b6eb8a80
4bd1a3f7 9df3cc53 ef829ea3 a1e697c1 589d756c e01d1b4c fad1c12d 05c0ea6e
b2227055 d9203340 3307c265 83fa8f43 379bea0e 9a6c70ee f69c803b d937f47a

```
6decd018 7d494aca 99c71928 a2bed877 24f78526 866d8705 404167d1 273aeddc
481d22cd 0b0b8bbc f4b17bfd b499a8e9 762ae11a 2d876e74 d388dd1e 22c6df16
b62b8214 0a945cf2 50ecafce ff62370d ad65d306 4153ed02 14c8b558 28a1ace0
5becb37f 954afb03 c8ad26db e6667812 4ad99f42 fbe198e6 42839b8f 8f6724e8
6119b5dd cdb50b26 058ec36e c4c875b8 46cfe218 065ea9ae a8819a47 16de0c28
6c2527b9 deb78458 c61f381e a4c4cb66

quit

telnet timeout 5

ssh stricthostkeycheck

ssh 192.168.29.0 255.255.255.0 management

ssh timeout 5

ssh version 2

console timeout 0

dynamic-access-policy-record DfltAccessPolicy

username [*****] password [*****] encrypted

!

class-map inspection_default

match default-inspection-traffic

!

!

policy-map type inspect dns migrated_dns_map_1

parameters

    message-length maximum client auto

    message-length maximum 512

policy-map global_policy

    class inspection_default

        inspect dns migrated_dns_map_1

        inspect ftp

        inspect h323 h225

        inspect h323 ras

        inspect ip-options

        inspect netbios
```

```
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error
class class-default
set connection decrement-ttl
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile License
destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
profile CiscoTAC-1
no active
destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
```

```
subscribe-to-alert-group telemetry periodic daily  
Cryptochecksum:e57e00145eb4fd26d97b4b0109308140  
: end
```

A.4 Biomedical Engineering

```
: Saved  
  
:  
  
: Serial Number: 9A3RHJVFPQS  
  
: Hardware: ASA v, 2048 MB RAM, CPU Xeon E5 series 2200 MHz  
  
:  
  
ASA Version 9.6(1)  
!  
  
hostname biomedical-kmcfadde  
enable password [*****] encrypted  
xlate per-session deny tcp any4 any4  
xlate per-session deny tcp any4 any6  
xlate per-session deny tcp any6 any4  
xlate per-session deny tcp any6 any6  
xlate per-session deny udp any4 any4 eq domain  
xlate per-session deny udp any4 any6 eq domain  
xlate per-session deny udp any6 any4 eq domain  
xlate per-session deny udp any6 any6 eq domain  
!  
license smart  
feature tier standard  
throughput level 1G  
names  
!  
interface GigabitEthernet0/0  
nameif WAN  
security-level 50  
ip address 192.168.100.152 255.255.255.0
```

```
ospf authentication-key *****
ospf authentication message-digest
!
interface GigabitEthernet0/1
    nameif LAN
    security-level 100
    ip address 192.168.140.1 255.255.255.0
!
interface GigabitEthernet0/2
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/3
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/4
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/5
    shutdown
    no nameif
    no security-level
    no ip address
!
```

```
interface GigabitEthernet0/6
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/7
    shutdown
    no nameif
    no security-level
    no ip address
!
interface GigabitEthernet0/8
    shutdown
    no nameif
    no security-level
    no ip address
!
interface Management0/0
    management-only
    nameif management
    security-level 0
    ip address 192.168.29.152 255.255.255.0
!
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns domain-lookup WAN
dns server-group DefaultDNS
    name-server 8.8.8.8
    name-server 8.8.4.4
object network SNMPHOSTS
```

```
subnet 192.168.29.0 255.255.255.0
object network PUMPS
subnet 192.168.150.0 255.255.255.0
object-group icmp-type PING-REPLIES
icmp-object echo-reply
object-group icmp-type TRACEROUTE-REPLIES
icmp-object time-exceeded
icmp-object unreachable
group-object PING-REPLIES
object-group icmp-type PING
icmp-object echo
object-group service TRACEROUTEUDP
service-object udp destination gt 33434
object-group service BAXTERPORTS
service-object tcp-udp destination eq 51244
object-group service SMITHSPORTS
service-object tcp destination eq 1588
object-group service CAREFUSIONPORTS
service-object tcp destination eq 3613
object-group service PCAPORTS
service-object tcp destination eq https
service-object tcp destination eq 11443
service-object tcp destination eq 11444
object-group service PLUM360PORTS
service-object tcp destination eq 8100
service-object tcp destination eq 9292
object-group service HOSPIRAPUMPSIMPORTS
service-object tcp destination eq https
service-object tcp destination eq 8443
object-group service BBRAUNPORTS
service-object tcp destination eq www
service-object tcp destination eq https
```

```
service-object tcp destination eq 8080
service-object tcp destination eq 1500
service-object tcp destination eq 4080
access-list 101 extended permit icmp any any object-group TRACEROUTE-REPLIES
access-list 101 extended permit object-group TRACEROUTEUDP any any
access-list 101 extended permit icmp any any object-group PING
access-list 101 extended permit icmp any any object-group PING-REPLIES
access-list 101 extended permit object-group SMITHSPORTS object PUMPS host
192.168.140.150
access-list 101 extended permit object-group CAREFUSIONPORTS object PUMPS host
192.168.140.158
access-list 101 extended permit object-group PCAPORTS object PUMPS host
192.168.140.160
access-list 101 extended permit object-group PLUM360PORTS object PUMPS host
192.168.140.160
access-list 101 extended permit object-group HOSPIRAPUMPSIMPORTS object PUMPS host
192.168.140.160
access-list 101 extended permit object-group BAXTERPORTS object PUMPS host
192.168.140.165
access-list 101 extended permit object-group BBRAUNPORTS object PUMPS host
192.168.140.169
pager lines 23
mtu WAN 1500
mtu LAN 1500
mtu management 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group 101 in interface WAN
router ospf 1
network 192.168.100.0 255.255.255.0 area 0
log-adj-changes
```

```
 redistribute connected subnets
 redistribute static subnets
 !
 timeout xlate 3:00:00
 timeout pat-xlate 0:00:30
 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
 timeout tcp-proxy-reassembly 0:01:00
 timeout floating-conn 0:00:00
 user-identity default-domain LOCAL
 aaa authentication ssh console LOCAL
 snmp-server host-group management SNMPHOSTS poll community *****
 no snmp-server location
 no snmp-server contact
 snmp-server community *****
 crypto ipsec security-association pmtu-aging infinite
 crypto ca trustpoint _SmartCallHome_ServerCA
   no validation-usage
   crl configure
 crypto ca trustpool policy
   auto-import
 crypto ca certificate chain _SmartCallHome_ServerCA
   certificate ca 6ecc7aa5a7032009b8cebcf4e952d491
     308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130
     0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
     30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
     13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
     0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72
     20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
     65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
```

65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d31
30303230 38303030 3030305a 170d3230 30323037 32333539 35395a30 81b5310b
30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20
496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65
74776f72 6b313b30 39060355 040b1332 5465726d 73206f66 20757365 20617420
68747470 733a2f2f 7777772e 76657269 7369676e 2e636f6d 2f727061 20286329
3130312f 302d0603 55040313 26566572 69536967 6e20436c 61737320 33205365
63757265 20536572 76657220 4341202d 20473330 82012230 0d06092a 864886f7
0d010101 05000382 010f0030 82010a02 82010100 b187841f c20c45f5 bcab2597
a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bb658e 444f4dce 6fed094a d4af4e10
9c688b2e 957b899b 13cae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc
7f432657 5833833b 330a17b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b
15fca34b 3bce6388 d0f82d0c 948610ca b69a3dca eb379c00 48358629 5078e845
63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
18b49ae8 3c6e81fd e4cd3536 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced
4a546ac9 4dc5bf11 b1ae1c67 81cb4455 33997f24 9b3f5345 7f861af3 3cfa6d7f
81f5b84a d3f58537 1cb5a6d0 09e4187b 384efa0f 02030100 01a38201 df308201
db303406 082b0601 05050701 01042830 26302406 082b0601 05050730 01861868
7474703a 2f2f6f63 73702e76 65726973 69676e2e 636f6d30 12060355 1d130101
ff040830 060101ff 02010030 70060355 1d200469 30673065 060b6086 480186f8
45010717 03305630 2806082b 06010505 07020116 1c687474 70733a2f 2f777777
2e766572 69736967 6e2e636f 6d2f6370 73302a06 082b0601 05050702 02301e1a
1c687474 70733a2f 2f777777 2e766572 69736967 6e2e636f 6d2f7270 61303406
03551d1f 042d302b 3029a027 a0258623 68747470 3a2f2f63 726c2e76 65726973
69676e2e 636f6d2f 70636133 2d67352e 63726c30 0e060355 1d0f0101 ff040403
02010630 6d06082b 06010505 07010c04 61305fa1 5da05b30 59305730 55160969
6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
69676e2e 636f6d2f 76736c6f 676f2e67 69663028 0603551d 11042130 1fa41d30
1b311930 17060355 04031310 56657269 5369676e 4d504b49 2d322d36 301d0603
551d0e04 1604140d 445c1653 44c1827e 1d20ab25 f40163d8 be79a530 1f060355
1d230418 30168014 7fd365a7 c2ddecbb f03009f3 4339fa02 af333133 300d0609

```
2a864886 f70d0101 05050003 82010100 0c8324ef ddc30cd9 589cf36 b6eb8a80
4bd1a3f7 9df3cc53 ef829ea3 ale697c1 589d756c e01d1b4c fad1c12d 05c0ea6e
b2227055 d9203340 3307c265 83fa8f43 379bea0e 9a6c70ee f69c803b d937f47a
6dec018 7d494aca 99c71928 a2bed877 24f78526 866d8705 404167d1 273aedd
481d22cd 0b0b8bbc f4b17bfd b499a8e9 762ae11a 2d876e74 d388dd1e 22c6df16
b62b8214 0a945cf2 50ecafce ff62370d ad65d306 4153ed02 14c8b558 28a1ace0
5becb37f 954afb03 c8ad26db e6667812 4ad99f42fbe198e6 42839b8f 8f6724e8
6119b5dd cdb50b26 058ec36e c4c875b8 46cfe218 065ea9ae a8819a47 16de0c28
6c2527b9 deb78458 c61f381e a4c4cb66

quit

telnet timeout 5

ssh stricthostkeycheck

ssh 192.168.29.0 255.255.255.0 management

ssh timeout 5

ssh version 2

console timeout 0

dhcpd dns 192.168.120.163 192.168.120.162

dhcpd option 3 ip 192.168.140.1

!

dhcpd address 192.168.140.220-192.168.140.250 LAN

dhcpd enable LAN

!

dynamic-access-policy-record DfltAccessPolicy

username [*****] password [*****] encrypted

!

class-map inspection_default

match default-inspection-traffic

!

!

policy-map type inspect dns migrated_dns_map_1

parameters

    message-length maximum client auto
```

```
message-length maximum 512

policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect ip-options
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
    inspect icmp
    inspect icmp error
  class class-default
    set connection decrement-ttl
  !
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
profile CiscoTAC-1
  no active
  destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
```

```

destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
profile License
destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
Cryptochecksum:627e549de0a7dd97cd1379bbf37bc168
: end

```

A.5 Medical Devices Zone ASA Configuration File

```

: Saved

:
: Serial Number: 9AEWS2E5JRA
: Hardware: ASAv, 2048 MB RAM, CPU Xeon E5 series 2200 MHz
:
ASA Version 9.6(1)
!
hostname medical-devices-kmcfadde
enable password [*****] encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
!
license smart
feature tier standard
throughput level 1G
names

!
interface GigabitEthernet0/0
nameif WAN
security-level 50
ip address 192.168.100.149 255.255.255.0
ospf authentication-key *****
ospf authentication message-digest
!
interface GigabitEthernet0/1

```

```
nameif LAN
security-level 100
ip address 192.168.150.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/7
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/8
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
nameif management
security-level 0
ip address 192.168.29.149 255.255.255.0
!
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns domain-lookup WAN
```

```
dns server-group DefaultDNS
    name-server 8.8.8.8
    name-server 8.8.4.4
object network SNMPPHOSTS
    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 object 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 192.168.140.160 object PUMPS
access-list WAN2LAN extended permit object-group HOSPIRAPUMPSIMPORTS host 192.168.140.160 object PUMPS
access-list WAN2LAN extended permit object-group BAXTERPUMPPORTS host 192.168.140.160 object PUMPS
access-list WAN2LAN extended permit object-group BBRAUNPORTS host 192.168.140.160 object PUMPS
pager lines 23
mtu WAN 1500
mtu LAN 1500
mtu management 1500
```

```

no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group WAN2LAN in interface WAN
access-group LAN2WAN in interface LAN
router ospf 1
  network 192.168.100.0 255.255.255.0 area 0
  log-adj-changes
  redistribute connected subnets
  redistribute static subnets
!
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
snmp-server host-group management SNMPHOSTS poll community *****
no snmp-server location
no snmp-server contact
snmp-server community *****
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
  no validation-usage
  crl configure
crypto ca trustpool policy
  auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491
  308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130
  0d06092a 864886f7 0d010105 05003081 ca310b30 09060355 04061302 55533117
  30150603 55040a13 0e566572 69536967 6e2c2049 6e632e31 1f301d06 0355040b
  13165665 72695369 676e2054 72757374 204e6574 776f726b 313a3038 06035504
  0b133128 63292032 30303620 56657269 5369676e 2c20496e 632e202d 20466f72
  20617574 686f7269 7a656420 75736520 6f6e6c79 31453043 06035504 03133c56
  65726953 69676e20 436c6173 73203320 5075626c 69632050 72696d61 72792043
  65727469 66696361 74696f6e 20417574 686f7269 7479202d 20473530 1e170d31
  30303230 38303030 3030305a 170d3230 30323037 32333539 35395a30 81b5310b
  30090603 55040613 02555331 17301506 0355040a 130e5665 72695369 676e2c20
  496e632e 311f301d 06035504 0b131656 65726953 69676e20 54727573 74204e65
  74776f72 6b313b30 39060355 040b1332 5465726d 73206f66 20757365 20617420
  68747470 733a2f2f 7777772e 76657269 7369676e 2e636f6d 2f727061 20286329
  3130312f 302d0603 55040313 26566572 69536967 6e20436c 61737320 33205365
  63757265 20536572 76657220 4341202d 20473330 82012230 0d06092a 864886f7
  0d010101 05000382 010f0030 82010a02 82010100 b187841f c20c45f5 bcab2597
  a7ada23e 9cbaf6c1 39b88bca c2ac56c6 e5bb658e 444f4dce 6fed094a d4af4e10
  9c688b2e 957b899b 13cae234 34c1f35b f3497b62 83488174 d188786c 0253f9bc
  7f432657 5833833b 330a17b0 d04e9124 ad867d64 12dc744a 34a11d0a ea961d0b
  15fca34b 3bce6388 d0f82d0c 948610ca b69a3dca eb379c00 48358629 5078e845

```

```
63cd1941 4ff595ec 7b98d4c4 71b350be 28b38fa0 b9539cf5 ca2c23a9 fd1406e8
18b49ae8 3c6e81fd e4cd3536 b351d369 ec12ba56 6e6f9b57 c58b14e7 0ec79ced
4a546ac9 4dc5bf11 b1ae1c67 81cb4455 33997f24 9b3f5345 7f861af3 3cfa6d7f
81f5b84a d3f58537 1cb5a6d0 09e4187b 384efa0f 02030100 01a38201 df308201
db303406 082b0601 05050701 01042830 26302406 082b0601 05050730 01861868
7474703a 2f2f6f63 73702e76 65726973 69676e2e 636f6d30 12060355 1d130101
ff040830 060101ff 02010030 70060355 1d200469 30673065 060b6086 480186f8
45010717 03305630 2806082b 06010505 07020116 1c687474 70733a2f 2f777777
2e766572 69736967 6e2e636f 6d2f6370 73302a06 082b0601 05050702 02301e1a
1c687474 70733a2f 2f777777 2e766572 69736967 6e2e636f 6d2f7270 61303406
03551d1f 042d302b 3029a027 a0258623 68747470 3a2f2f63 726c2e76 65726973
69676e2e 636f6d2f 70636133 2d67352e 63726c30 0e060355 1d0f0101 ff040403
02010630 6d06082b 06010505 07010c04 61305fa1 5da05b30 59305730 55160969
6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b
c3cf806a d448182c 7b192e30 25162368 7474703a 2f2f6c6f 676f2e76 65726973
69676e2e 636f6d2f 76736c6f 676f2e67 69663028 0603551d 11042130 1fa41d30
1b311930 17060355 04031310 56657269 5369676e 4d504b49 2d322d36 301d0603
551d0e04 1604140d 445c1653 44c1827e 1d20ab25 f40163d8 be79a530 1f060355
1d230418 30168014 7fd365a7 c2dddecbb f03009f3 4339fa02 af333133 300d0609
2a864886 f70d0101 05050003 82010100 0c8324ef ddc30cd9 589cfe36 b6eb8a80
4bd1a3f7 9df3cc53 ef829ea3 a1e697c1 589d756c e01d1b4c fad1c12d 05c0ea6e
b2227055 d9203340 3307c265 83fa8f43 379bea0e 9a6c70ee f69c803b d937f47a
6decd018 7d494aca 99c71928 a2bed877 24f78526 866d8705 404167d1 273aeddc
481d22cd 0b0b8bbc f4b17bfd b499a8e9 762ae11a 2d876e74 d388dd1e 22c6df16
b62b8214 0a945cf2 50ecafce ff62370d ad65d306 4153ed02 14c8b558 28a1ace0
5becb37f 954afb03 c8ad26db e6667812 4ad99f42 fbe198e6 42839b8f 8f6724e8
6119b5dd cdb50b26 058ec36e c4c875b8 46cfe218 065ea9ae a8819a47 16de0c28
6c2527b9 deb78458 c61f381e a4c4cb66
quit
telnet timeout 5
ssh stricthostkeycheck
ssh 192.168.29.0 255.255.255.0 management
ssh timeout 5
ssh version 2
console timeout 0
dhcpd dns 192.168.150.1
dhcpd option 3 ip 192.168.150.1
!
dhcpd address 192.168.150.220-192.168.150.250 LAN
dhcpd enable LAN
!
dynamic-access-policy-record DfltAccessPolicy
username [*****]password [*****] encrypted
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
 class inspection_default
 inspect dns migrated_dns_map_1
 inspect ftp
```

```
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
inspect icmp error
class class-default
  set connection decrement-ttl
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
  profile CiscoTAC-1
    no active
    destination address http https://tools.cisco.com/its/service/oddce/services/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:b2e10eb9d982ddbe5330e964af80d2d3
:
: end
```

A.6 Switch Configuration File

```
!
! Last configuration change at 22:21:08 UTC Wed Feb 22 2017 by cisco
! NVRAM config last updated at 23:22:47 UTC Wed Feb 22 2017 by cisco
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname Cisco3650-01
!
```

```
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-vrf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
logging console emergencies
enable secret [*****]
enable password [*****]
!
username [*****] privilege [**] password [*****]
user-name [*****]
creation-time 1469560730
privilege [**]
password [*****]
type mgmt-user
no aaa new-model
switch 1 provision ws-c3650-48ps
!
ip domain-name [*****]
ip device tracking
ip dhcp excluded-address 192.168.250.1 192.168.250.9
!
ip dhcp pool WLAN
network 192.168.250.0 255.255.255.0
default-router 192.168.250.1
option 43 hex c0a8.fa02
!
!
vtp mode transparent
!
crypto pki trustpoint TP-self-signed-2035642131
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-2035642131
revocation-check none
rsakeypair TP-self-signed-2035642131
!
!
crypto pki certificate chain TP-self-signed-2035642131
certificate self-signed 01
3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 32303335 36343231 3331301E 170D3136 30373236 32303436
32355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 30333536
34323133 3130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100F1C4 010AE138 9BD9BBCC 2E563180 698979B5 51F7B46B D122595E E7033DCA
D80C9432 0728E47F 8CAC2629 40CEC617 5CDFFBD9 19744025 CB62CA75 8F6F0A9A
34F790DD 07DA9D60 737196C1 FDD9E764 6D22EDA3 8D9E7DF5 6CD934E3 D89FA9D5
C165F3EE E9E0EA9F 37742B00 2C4CFA0B C262E61B 95565B42 302B23E7 A1C85D9F
```

```

5FDB0203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF 30200603
551D1104 19301782 15436973 636F3336 35302D30 312E6E69 73742E67 6F76301F
0603551D 23041830 1680148F 3A1CDEB7 502DACP7 DF4E96E4 EA1470F1 CFD1F730
1D060355 1D0E0416 04148F3A 1CDEB750 2DACP7DF 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
317FAFDO E853785D 777E1E1D 6F561A2A 07
    quit
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
spanning-tree portfast
!
interface GigabitEthernet1/0/2
switchport access vlan 1520
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/3
switchport access vlan 1520
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/4
switchport access vlan 1520
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/5
spanning-tree portfast
!
interface GigabitEthernet1/0/6
spanning-tree portfast
!
interface GigabitEthernet1/0/7
spanning-tree portfast
!
interface GigabitEthernet1/0/8
spanning-tree portfast
!
interface GigabitEthernet1/0/9
spanning-tree portfast
!
interface GigabitEthernet1/0/10
spanning-tree portfast
!
interface GigabitEthernet1/0/11
spanning-tree portfast
!
interface GigabitEthernet1/0/12
spanning-tree portfast
!
interface GigabitEthernet1/0/13
spanning-tree portfast
!
interface GigabitEthernet1/0/14
spanning-tree portfast
!
interface GigabitEthernet1/0/15
spanning-tree portfast
!
interface GigabitEthernet1/0/16
spanning-tree portfast
!
interface GigabitEthernet1/0/17
spanning-tree portfast
!
```

```
interface GigabitEthernet1/0/18
  spanning-tree portfast
!
interface GigabitEthernet1/0/19
  spanning-tree portfast
!
interface GigabitEthernet1/0/20
  spanning-tree portfast
!
interface GigabitEthernet1/0/21
  spanning-tree portfast
!
interface GigabitEthernet1/0/22
  spanning-tree portfast
!
interface GigabitEthernet1/0/23
  spanning-tree portfast
!
interface GigabitEthernet1/0/24
  spanning-tree portfast
!
interface GigabitEthernet1/0/25
  spanning-tree portfast
!
interface GigabitEthernet1/0/26
  spanning-tree portfast
!
interface GigabitEthernet1/0/27
  spanning-tree portfast
!
interface GigabitEthernet1/0/28
  spanning-tree portfast
!
interface GigabitEthernet1/0/29
  spanning-tree portfast
!
interface GigabitEthernet1/0/30
  spanning-tree portfast
!
interface GigabitEthernet1/0/31
  spanning-tree portfast
!
interface GigabitEthernet1/0/32
  spanning-tree portfast
!
interface GigabitEthernet1/0/33
  spanning-tree portfast
!
interface GigabitEthernet1/0/34
  spanning-tree portfast
!
interface GigabitEthernet1/0/35
  spanning-tree portfast
!
interface GigabitEthernet1/0/36
  spanning-tree portfast
```

```
!
interface GigabitEthernet1/0/37
  spanning-tree portfast
!
interface GigabitEthernet1/0/38
  spanning-tree portfast
!
interface GigabitEthernet1/0/39
  spanning-tree portfast
!
interface GigabitEthernet1/0/40
  spanning-tree portfast
!
interface GigabitEthernet1/0/41
  switchport access vlan 1400
  spanning-tree portfast
!
interface GigabitEthernet1/0/42
  switchport access vlan 1400
  spanning-tree portfast
!
interface GigabitEthernet1/0/43
  switchport access vlan 1400
  spanning-tree portfast
!
interface GigabitEthernet1/0/44
  switchport access vlan 1400
  spanning-tree portfast
!
interface GigabitEthernet1/0/45
  description Set to 10/Half for Hospira
  switchport access vlan 1500
  speed 10
  duplex half
  spanning-tree portfast
!
interface GigabitEthernet1/0/46
  switchport access vlan 1500
  spanning-tree portfast
!
interface GigabitEthernet1/0/47
  description VLAN trunk
  switchport trunk allowed vlan 1400,1500,1520
  switchport mode trunk
  spanning-tree portfast
!
interface GigabitEthernet1/0/48
  description management connection on VL20
  switchport access vlan 20
  spanning-tree portfast
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
```

```
!
interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan20
  ip address 192.168.20.13 255.255.255.0
!
interface Vlan1520
  description Wireless-MGMT
  ip address 192.168.250.1 255.255.255.0
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.20.254
!
ip access-list extended SSH-Access
  permit tcp 192.168.20.0 0.0.0.255 any eq 22
  deny   ip any any log
!
access-list 10 permit 192.168.20.0 0.0.0.255
!
snmp-server community public RO 10
snmp-server location NCCoE
snmp-server contact <email-address>
!
!
line con 0
  exec-timeout 0 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  access-class SSH-Access in
  exec-timeout 300 0
  password [*****]
  login local
  transport input ssh
line vty 5 15
  access-class SSH-Access in
  exec-timeout 300 0
  password [*****]
  login local
  transport input ssh
!
ntp server 10.97.74.8
wsma agent exec
  profile httplistener
  profile httpslistener
wsma agent config
  profile httplistener
  profile httpslistener
wsma agent filesys
  profile httplistener
```

```
profile httpslistener
wsma agent notify
profile httplistener
profile httpslistener
!
wsma profile listener httplistener
  transport http
!
wsma profile listener httpslistener
  transport https
ap group default-group
end
```

A.7 Wireless Configuration

System Inventory

```
NAME: "Chassis"      , DESCRIPTOR: "Cisco Wireless Controller"
PID: AIR-CTVM-K9, VID: V01, SN: 96NTPERK0A6
```

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

System Information

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

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

```
System Name..... wlc
System Location..... .
System Contact..... .
System ObjectID..... 1.3.6.1.4.1.9.1.1631
IP Address..... 192.168.250.2
IPv6 Address..... ::
```

System Up Time..... 6 days 3 hrs 48 mins 20 secs
System Timezone Location.....
System Stats Realtime Interval..... 5
System Stats Normal Interval..... 180

Configured Country..... US - United States

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

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

Backup Controller Configuration

AP primary Backup Controller

AP secondary Backup Controller

System Time Information:

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

Timezone delta..... 0:0
Timezone location.....

NTP Servers

NTP Polling Interval..... 3600

Index NTP Msg	NTP Key Index Auth Status	NTP Server	Status
1 AUTH DISABLED	0	192.168.250.1	Not Synched

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
c1140	8636
c1520	7344
c1550	10628
c1570	11536
c602i	3864
version.info	4

Secondary AP Image	Size
-----	-----
ap1g1	12660
ap1g2	11748
ap1g3	13672
ap1g4	19256
ap3g1	9736
ap3g2	13480
ap3g3	18696
ap801	8064
ap802	9536
c1140	8636
c1520	7344
c1550	10628
c1570	11536
c602i	3864
version.info	4

Switch Configuration

802.3x Flow Control Mode.....	Disable
FIPS prerequisite features.....	Disabled
WLANCC prerequisite features.....	Disabled
UCAPL prerequisite features.....	Disabled

secret obfuscation..... Enabled

Strong Password Check Features

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

Mgmt User

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

SNMPv3 User

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

Network Information

RF-Network Name.....	WLAN
DNS Server IP.....	
Web Mode.....	Disable
Secure Web Mode.....	Enable
Secure Web Mode Cipher-Option High.....	Disable
Secure Web Mode Cipher-Option SSLv2.....	Disable
Secure Web Mode RC4 Cipher Preference.....	Disable

Secure Web Mode SSL Protocol.....	Disable
OCSP.....	Disabled
OCSP responder URL.....	
Secure Shell (ssh).....	Enable
Secure Shell (ssh) Cipher-Option High.....	Disable
Telnet.....	Disable
Ethernet Multicast Forwarding.....	Disable
Ethernet Broadcast Forwarding.....	Disable
IPv4 AP Multicast/Broadcast Mode.....	Unicast
IPv6 AP Multicast/Broadcast Mode.....	Unicast
IGMP snooping.....	Disabled
IGMP timeout.....	60 seconds
IGMP Query Interval.....	20 seconds
MLD snooping.....	Disabled
MLD timeout.....	60 seconds
MLD query interval.....	20 seconds
User Idle Timeout.....	300 seconds
ARP Idle Timeout.....	300 seconds
Cisco AP Default Master.....	Disable
AP Join Priority.....	Disable
Mgmt Via Wireless Interface.....	Disable
Mgmt Via Dynamic Interface.....	Disable
Bridge MAC filter Config.....	Enable
Bridge Security Mode.....	EAP
Mesh Full Sector DFS.....	Enable
Mesh Backhaul RRM.....	Disable
AP Fallback	Enable
Web Auth CMCC Support	Disabled
Web Auth Redirect Ports	80
Web Auth Proxy Redirect	Disable
Web Auth Captive-Bypass	Disable
Web Auth Secure Web	Enable

Web Auth Secure Redirection Disable
Fast SSID Change Disabled
AP Discovery - NAT IP Only Enabled
IP/MAC Addr Binding Check Enabled
Link Local Bridging Status Disabled
CCX-lite status Disable
oeap-600 dual-rlan-ports Disable
oeap-600 local-network Enable
oeap-600 Split Tunneling (Printers) Disable
WebPortal Online Client 0
WebPortal NTF_LOGOUT Client 0
mDNS snooping Disabled
mDNS Query Interval 15 minutes
Web Color Theme Default
Capwap Prefer Mode IPv4
Network Profile Disabled
Client ip conflict detection (DHCP) Disabled
Mesh BH RRM Disable
Mesh Aggressive DCA Disable
Mesh Auto RF Disable
HTTP Profiling Port 80

Port Summary

Pr	STP	Admin	Physical	Physical	Link	Link		
	Type	Stat	Mode	Mode	Status	Status	Trap	POE
<hr/>								
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 Country	Slots IP Address	AP Model Clients	Ethernet MAC DSE Location	Location
AP78da.6ee0.08ec US	2 192.168.250.10	AIR-CAP1602I-A-K9 0	78:da:6e:e0:08:ec [0 ,0 ,0]	default location
AP24e9.b34b.f1ed US	2 192.168.250.11	AIR-CAP1602I-A-K9 1	24:e9:b3:4b:f1:ed [0 ,0 ,0]	default location

AP Tcp-Mss-Adjust Info

AP Name	TCP State	MSS Size
AP78da.6ee0.08ec	disabled	-
AP24e9.b34b.f1ed	disabled	-

AP Location

Total Number of AP Groups..... 1

Site Name.....	default-group
Site Description.....	<none>
NAS-identifier.....	none
Client Traffic QinQ Enable.....	FALSE
DHCPv4 QinQ Enable.....	FALSE
AP Operating Class.....	Not-configured
Capwap Prefer Mode.....	Not-configured

RF Profile

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

WLAN ID	Interface	Network Admission Control	Radio Policy
---------	-----------	---------------------------	--------------

1	ip_dev	Disabled	None
2	ip_dev	Disabled	None

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

Lan Port configs

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

External 3G/4G module configs

LAN	Status	POE	R LAN
---	-----	----	-----
1	Disabled		None

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

RF Profile

Number of RF Profiles..... 6

Out Of Box State..... Disabled

Out Of Box Persistence..... Disabled

RF Profile Name client-only	Applied	Band	Description	11n-
High-Client-Density-802.11a disable	No	5 GHz	<none>	
High-Client-Density-802.11bg disable	No	2.4 GHz	<none>	
Low-Client-Density-802.11a disable	No	5 GHz	<none>	
Low-Client-Density-802.11bg disable	No	2.4 GHz	<none>	
Typical-Client-Density-802.11a disable	No	5 GHz	<none>	
Typical-Client-Density-802.11bg disable	No	2.4 GHz	<none>	

RF Profile name..... High-Client-Density-802.11a

Description..... <none>

AP Group Name..... <none>

Radio policy..... 5 GHz

11n-client-only..... disabled

Transmit Power Threshold v1..... -65 dBm

Transmit Power Threshold v2..... -67 dBm

Min Transmit Power..... 7 dBm

Max Transmit Power..... 30 dBm

802.11a Operational Rates

802.11a 6M Rate..... Disabled

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

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

Trap Threshold

Clients.....	12 clients
Interference.....	10 %
Noise.....	-70 dBm
Utilization.....	80 %
Multicast Data Rate.....	0
Rx Sop Threshold.....	-78 dBm
Cca Threshold.....	0 dBm
Slot Admin State:.....	Enabled

Band Select

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

Load Balancing

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

Coverage Data

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

802.11n MCS Rates

MCS-00 Rate.....	enabled
MCS-01 Rate.....	enabled
MCS-02 Rate.....	enabled
MCS-03 Rate.....	enabled
MCS-04 Rate.....	enabled
MCS-05 Rate.....	enabled
MCS-06 Rate.....	enabled
MCS-07 Rate.....	enabled
MCS-08 Rate.....	enabled
MCS-09 Rate.....	enabled
MCS-10 Rate.....	enabled
MCS-11 Rate.....	enabled
MCS-12 Rate.....	enabled
MCS-13 Rate.....	enabled

MCS-14 Rate.....	enabled
MCS-15 Rate.....	enabled
MCS-16 Rate.....	enabled
MCS-17 Rate.....	enabled
MCS-18 Rate.....	enabled
MCS-19 Rate.....	enabled
MCS-20 Rate.....	enabled
MCS-21 Rate.....	enabled
MCS-22 Rate.....	enabled
MCS-23 Rate.....	enabled
MCS-24 Rate.....	enabled
MCS-25 Rate.....	enabled
MCS-26 Rate.....	enabled
MCS-27 Rate.....	enabled
MCS-28 Rate.....	enabled
MCS-29 Rate.....	enabled
MCS-30 Rate.....	enabled
MCS-31 Rate.....	enabled
Client Network Preference.....	default
RF Profile name.....	High-Client-Density-802.11bg
Description.....	<none>
AP Group Name.....	<none>
Radio policy.....	2.4 GHz
11n-client-only.....	disabled
Transmit Power Threshold v1.....	-70 dBm
Transmit Power Threshold v2.....	-67 dBm
Min Transmit Power.....	7 dBm
Max Transmit Power.....	30 dBm
802.11b/g Operational Rates	
802.11b/g 1M Rate.....	Disabled
802.11b/g 2M Rate.....	Disabled

802.11b/g 5.5M Rate.....	Disabled
802.11b/g 11M Rate.....	Disabled
802.11g 6M Rate.....	Disabled
802.11g 9M Rate.....	Supported
802.11g 12M Rate.....	Mandatory
802.11g 18M Rate.....	Supported
802.11g 24M Rate.....	Supported
802.11g 36M Rate.....	Supported
802.11g 48M Rate.....	Supported
802.11g 54M Rate.....	Supported
Max Clients.....	200

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

Trap Threshold

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

Band Select

Probe Response.....	Disabled
Cycle Count.....	2 cycles
Cycle Threshold.....	200 milliseconds
Expire Suppression.....	20 seconds

Expire Dual Band..... 60 seconds
Client Rssi..... -80 dBm
Client Mid Rssi..... -80 dBm

Load Balancing

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

Coverage Data

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

802.11n MCS Rates

MCS-00 Rate..... enabled
MCS-01 Rate..... enabled
MCS-02 Rate..... enabled
MCS-03 Rate..... enabled
MCS-04 Rate..... enabled
MCS-05 Rate..... enabled
MCS-06 Rate..... enabled
MCS-07 Rate..... enabled
MCS-08 Rate..... enabled
MCS-09 Rate..... enabled
MCS-10 Rate..... enabled
MCS-11 Rate..... enabled
MCS-12 Rate..... enabled
MCS-13 Rate..... enabled

MCS-14 Rate.....	enabled
MCS-15 Rate.....	enabled
MCS-16 Rate.....	enabled
MCS-17 Rate.....	enabled
MCS-18 Rate.....	enabled
MCS-19 Rate.....	enabled
MCS-20 Rate.....	enabled
MCS-21 Rate.....	enabled
MCS-22 Rate.....	enabled
MCS-23 Rate.....	enabled
MCS-24 Rate.....	enabled
MCS-25 Rate.....	enabled
MCS-26 Rate.....	enabled
MCS-27 Rate.....	enabled
MCS-28 Rate.....	enabled
MCS-29 Rate.....	enabled
MCS-30 Rate.....	enabled
MCS-31 Rate.....	enabled
Client Network Preference.....	default
RF Profile name.....	Low-Client-Density-802.11a
Description.....	<none>
AP Group Name.....	<none>
Radio policy.....	5 GHz
11n-client-only.....	disabled
Transmit Power Threshold v1.....	-60 dBm
Transmit Power Threshold v2.....	-67 dBm
Min Transmit Power.....	-10 dBm
Max Transmit Power.....	30 dBm
802.11a Operational Rates	
802.11a 6M Rate.....	Mandatory
802.11a 9M Rate.....	Supported

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

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

Trap Threshold

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

Band Select

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

Load Balancing

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

Coverage Data

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

802.11n MCS Rates

MCS-00 Rate.....	enabled
MCS-01 Rate.....	enabled
MCS-02 Rate.....	enabled
MCS-03 Rate.....	enabled
MCS-04 Rate.....	enabled
MCS-05 Rate.....	enabled
MCS-06 Rate.....	enabled
MCS-07 Rate.....	enabled
MCS-08 Rate.....	enabled
MCS-09 Rate.....	enabled
MCS-10 Rate.....	enabled
MCS-11 Rate.....	enabled
MCS-12 Rate.....	enabled
MCS-13 Rate.....	enabled
MCS-14 Rate.....	enabled

MCS-15 Rate.....	enabled
MCS-16 Rate.....	enabled
MCS-17 Rate.....	enabled
MCS-18 Rate.....	enabled
MCS-19 Rate.....	enabled
MCS-20 Rate.....	enabled
MCS-21 Rate.....	enabled
MCS-22 Rate.....	enabled
MCS-23 Rate.....	enabled
MCS-24 Rate.....	enabled
MCS-25 Rate.....	enabled
MCS-26 Rate.....	enabled
MCS-27 Rate.....	enabled
MCS-28 Rate.....	enabled
MCS-29 Rate.....	enabled
MCS-30 Rate.....	enabled
MCS-31 Rate.....	enabled
Client Network Preference.....	default
RF Profile name.....	Low-Client-Density-802.11bg
Description.....	<none>
AP Group Name.....	<none>
Radio policy.....	2.4 GHz
11n-client-only.....	disabled
Transmit Power Threshold v1.....	-65 dBm
Transmit Power Threshold v2.....	-67 dBm
Min Transmit Power.....	-10 dBm
Max Transmit Power.....	30 dBm
802.11b/g Operational Rates	
802.11b/g 1M Rate.....	Mandatory
802.11b/g 2M Rate.....	Mandatory
802.11b/g 5.5M Rate.....	Mandatory

802.11b/g 11M Rate.....	Mandatory
802.11g 6M Rate.....	Supported
802.11g 9M Rate.....	Supported
802.11g 12M Rate.....	Supported
802.11g 18M Rate.....	Supported
802.11g 24M Rate.....	Supported
802.11g 36M Rate.....	Supported
802.11g 48M Rate.....	Supported
802.11g 54M Rate.....	Supported
Max Clients.....	200

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

Trap Threshold

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

Band Select

Probe Response.....	Disabled
Cycle Count.....	2 cycles
Cycle Threshold.....	200 milliseconds
Expire Suppression.....	20 seconds
Expire Dual Band.....	60 seconds

Client Rssi..... -80 dBm
Client Mid Rssi..... -80 dBm

Load Balancing

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

Coverage Data

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

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

802.11n MCS Rates

MCS-00 Rate..... enabled
MCS-01 Rate..... enabled
MCS-02 Rate..... enabled
MCS-03 Rate..... enabled
MCS-04 Rate..... enabled
MCS-05 Rate..... enabled
MCS-06 Rate..... enabled
MCS-07 Rate..... enabled
MCS-08 Rate..... enabled
MCS-09 Rate..... enabled
MCS-10 Rate..... enabled
MCS-11 Rate..... enabled
MCS-12 Rate..... enabled
MCS-13 Rate..... enabled
MCS-14 Rate..... enabled

MCS-15 Rate.....	enabled
MCS-16 Rate.....	enabled
MCS-17 Rate.....	enabled
MCS-18 Rate.....	enabled
MCS-19 Rate.....	enabled
MCS-20 Rate.....	enabled
MCS-21 Rate.....	enabled
MCS-22 Rate.....	enabled
MCS-23 Rate.....	enabled
MCS-24 Rate.....	enabled
MCS-25 Rate.....	enabled
MCS-26 Rate.....	enabled
MCS-27 Rate.....	enabled
MCS-28 Rate.....	enabled
MCS-29 Rate.....	enabled
MCS-30 Rate.....	enabled
MCS-31 Rate.....	enabled
Client Network Preference.....	default
RF Profile name.....	Typical-Client-Density-802.11a
Description.....	<none>
AP Group Name.....	<none>
Radio policy.....	5 GHz
11n-client-only.....	disabled
Transmit Power Threshold v1.....	-70 dBm
Transmit Power Threshold v2.....	-67 dBm
Min Transmit Power.....	-10 dBm
Max Transmit Power.....	30 dBm
802.11a Operational Rates	
802.11a 6M Rate.....	Mandatory
802.11a 9M Rate.....	Supported
802.11a 12M Rate.....	Mandatory

802.11a 18M Rate.....	Supported
802.11a 24M Rate.....	Mandatory
802.11a 36M Rate.....	Supported
802.11a 48M Rate.....	Supported
802.11a 54M Rate.....	Supported
Max Clients.....	200

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

Trap Threshold

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

Band Select

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

Load Balancing

Denial.....	3 count
Window.....	5 clients
Coverage Data	
Data.....	-80 dBm
Voice.....	-80 dBm
Minimum Client Level.....	3 clients
Exception Level.....	25 %
DCA Channel List.....	36,40,44,48,52,56,60,64,100, 104,108,112,116,120,124,128, 132,136,140,144,149,153,157, 161
DCA Bandwidth.....	20
DCA Foreign AP Contribution.....	enabled
802.11n MCS Rates	
MCS-00 Rate.....	enabled
MCS-01 Rate.....	enabled
MCS-02 Rate.....	enabled
MCS-03 Rate.....	enabled
MCS-04 Rate.....	enabled
MCS-05 Rate.....	enabled
MCS-06 Rate.....	enabled
MCS-07 Rate.....	enabled
MCS-08 Rate.....	enabled
MCS-09 Rate.....	enabled
MCS-10 Rate.....	enabled
MCS-11 Rate.....	enabled
MCS-12 Rate.....	enabled
MCS-13 Rate.....	enabled
MCS-14 Rate.....	enabled
MCS-15 Rate.....	enabled

MCS-16 Rate.....	enabled
MCS-17 Rate.....	enabled
MCS-18 Rate.....	enabled
MCS-19 Rate.....	enabled
MCS-20 Rate.....	enabled
MCS-21 Rate.....	enabled
MCS-22 Rate.....	enabled
MCS-23 Rate.....	enabled
MCS-24 Rate.....	enabled
MCS-25 Rate.....	enabled
MCS-26 Rate.....	enabled
MCS-27 Rate.....	enabled
MCS-28 Rate.....	enabled
MCS-29 Rate.....	enabled
MCS-30 Rate.....	enabled
MCS-31 Rate.....	enabled
Client Network Preference.....	default
RF Profile name.....	Typical-Client-Density-802.11bg
Description.....	<none>
AP Group Name.....	<none>
Radio policy.....	2.4 GHz
11n-client-only.....	disabled
Transmit Power Threshold v1.....	-70 dBm
Transmit Power Threshold v2.....	-67 dBm
Min Transmit Power.....	-10 dBm
Max Transmit Power.....	30 dBm
 802.11b/g Operational Rates	
802.11b/g 1M Rate.....	Disabled
802.11b/g 2M Rate.....	Disabled
802.11b/g 5.5M Rate.....	Disabled
802.11b/g 11M Rate.....	Disabled

802.11g 6M Rate.....	Disabled
802.11g 9M Rate.....	Supported
802.11g 12M Rate.....	Mandatory
802.11g 18M Rate.....	Supported
802.11g 24M Rate.....	Supported
802.11g 36M Rate.....	Supported
802.11g 48M Rate.....	Supported
802.11g 54M Rate.....	Supported
Max Clients.....	200

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

Trap Threshold

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

Band Select

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

Client Mid Rssi..... -80 dBm

Load Balancing

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

Coverage Data

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

802.11n MCS Rates

MCS-00 Rate.....	enabled
MCS-01 Rate.....	enabled
MCS-02 Rate.....	enabled
MCS-03 Rate.....	enabled
MCS-04 Rate.....	enabled
MCS-05 Rate.....	enabled
MCS-06 Rate.....	enabled
MCS-07 Rate.....	enabled
MCS-08 Rate.....	enabled
MCS-09 Rate.....	enabled
MCS-10 Rate.....	enabled
MCS-11 Rate.....	enabled
MCS-12 Rate.....	enabled
MCS-13 Rate.....	enabled
MCS-14 Rate.....	enabled
MCS-15 Rate.....	enabled

MCS-16 Rate.....	enabled
MCS-17 Rate.....	enabled
MCS-18 Rate.....	enabled
MCS-19 Rate.....	enabled
MCS-20 Rate.....	enabled
MCS-21 Rate.....	enabled
MCS-22 Rate.....	enabled
MCS-23 Rate.....	enabled
MCS-24 Rate.....	enabled
MCS-25 Rate.....	enabled
MCS-26 Rate.....	enabled
MCS-27 Rate.....	enabled
MCS-28 Rate.....	enabled
MCS-29 Rate.....	enabled
MCS-30 Rate.....	enabled
MCS-31 Rate.....	enabled
Client Network Preference.....	default

AP Config

Cisco AP Identifier.....	3
Cisco AP Name.....	AP78da.6ee0.08ec
Country code.....	US - United States
Regulatory Domain allowed by Country.....	802.11bg:-A 802.11a:-AB
AP Country code.....	US - United States
AP Regulatory Domain.....	-A
Switch Port Number	1
MAC Address.....	78:da:6e:e0:08:ec
IP Address Configuration.....	DHCP
IP Address.....	192.168.250.10
IP NetMask.....	255.255.255.0
Gateway IP Addr.....	192.168.250.1
NAT External IP Address.....	None

CAPWAP Path MTU.....	1485
DHCP Release Override.....	Disabled
Telnet State.....	Globally Disabled
Ssh State.....	Globally Disabled
Cisco AP Location.....	default location
Cisco AP Floor Label.....	0
Cisco AP Group Name.....	default-group
Primary Cisco Switch Name.....	
Primary Cisco Switch IP Address.....	Not Configured
Secondary Cisco Switch Name.....	
Secondary Cisco Switch IP Address.....	Not Configured
Tertiary Cisco Switch Name.....	
Tertiary Cisco Switch IP Address.....	Not Configured
Administrative State	ADMIN_ENABLED
Operation State	REGISTERED
Mirroring Mode	Disabled
AP Mode	FlexConnect
Public Safety	Disabled
ATF Mode:	Disable
AP SubMode	Not Configured
Rogue Detection	Enabled
AP Vlan Trunking	Disabled
Remote AP Debug	Disabled
Logging trap severity level	informational
Logging syslog facility	kern
S/W Version	8.2.111.0
Boot Version	15.2.2.0
Mini IOS Version	7.5.1.73
Stats Reporting Period	180
Stats Collection Mode	normal
LED State.....	Enabled
PoE Pre-Standard Switch.....	Disabled

PoE Power Injector MAC Addr..... Disabled
 Power Type/Mode..... PoE/Full Power
 Number Of Slots..... 2
 AP Model..... AIR-CAP1602I-A-K9
 AP Image..... C1600-K9W8-M
 IOS Version..... 15.3(3)JC2\$
 Reset Button..... Enabled
 AP Serial Number..... FGL1748W52Y
 AP Certificate Type..... Manufacture Installed
 AP Lag Status Disable
 Native Vlan Inheritance: AP
 FlexConnect Vlan mode :..... Disabled
 FlexConnect Group..... Not a member of any group
 Group VLAN ACL Mappings

Group VLAN Name to Id Mappings

Template in Modified State - apply it to see mappings

AP-Specific FlexConnect Policy ACLs :

L2Acl Configuration Not Available

FlexConnect Local-Split ACLs :

WLAN ID	PROFILE NAME	ACL	TYPE
-	-	-	-

Flexconnect Central-Dhcp Values :

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

1	IP_Dev No Encryption	False	False
False	Wlan		

Flex AVC visibility Configurations.....

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

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

FlexConnect Backup Auth Radius Servers :

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

Attributes for Slot 0

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

Station Configuration

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

Operation Rate Set

1000 Kilo Bits.....	MANDATORY
2000 Kilo Bits.....	MANDATORY
5500 Kilo Bits.....	MANDATORY
11000 Kilo Bits.....	MANDATORY
6000 Kilo Bits.....	SUPPORTED
9000 Kilo Bits.....	SUPPORTED
12000 Kilo Bits.....	SUPPORTED
18000 Kilo Bits.....	SUPPORTED
24000 Kilo Bits.....	SUPPORTED
36000 Kilo Bits.....	SUPPORTED
48000 Kilo Bits.....	SUPPORTED
54000 Kilo Bits.....	SUPPORTED

MCS Set

MCS 0.....	SUPPORTED
MCS 1.....	SUPPORTED
MCS 2.....	SUPPORTED
MCS 3.....	SUPPORTED
MCS 4.....	SUPPORTED
MCS 5.....	SUPPORTED
MCS 6.....	SUPPORTED
MCS 7.....	SUPPORTED
MCS 8.....	SUPPORTED
MCS 9.....	SUPPORTED
MCS 10.....	SUPPORTED

MCS 11.....	SUPPORTED
MCS 12.....	SUPPORTED
MCS 13.....	SUPPORTED
MCS 14.....	SUPPORTED
MCS 15.....	SUPPORTED
MCS 16.....	DISABLED
MCS 17.....	DISABLED
MCS 18.....	DISABLED
MCS 19.....	DISABLED
MCS 20.....	DISABLED
MCS 21.....	DISABLED
MCS 22.....	DISABLED
MCS 23.....	DISABLED
MCS 24.....	DISABLED
MCS 25.....	DISABLED
MCS 26.....	DISABLED
MCS 27.....	DISABLED
MCS 28.....	DISABLED
MCS 29.....	DISABLED
MCS 30.....	DISABLED
MCS 31.....	DISABLED
Beacon Period	100
Fragmentation Threshold	2346
Multi Domain Capability Implemented	TRUE
Multi Domain Capability Enabled	TRUE
Country String	US
 Multi Domain Capability	
Configuration	AUTOMATIC
First Chan Num	1
Number Of Channels	11

MAC Operation Parameters

Configuration	AUTOMATIC
Fragmentation Threshold	2346
Packet Retry Limit	64

Tx Power

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

Phy OFDM parameters

Configuration	AUTOMATIC
Current Channel	11
Channel Assigned By	DCA
Extension Channel	NONE
Channel Width.....	20 Mhz
Allowed Channel List.....	1,2,3,4,5,6,7,8,9,10,11
TI Threshold	-50
DCA Channel List.....	Global
Legacy Tx Beamforming Configuration	CUSTOMIZED
Legacy Tx Beamforming	ENABLED
Antenna Type.....	INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBi units)....	8
Diversity.....	DIVERSITY_ENABLED
802.11n Antennas	

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

Performance Profile Parameters

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

Rogue Containment Information

Containment Count.....	0
------------------------	---

CleanAir Management Information

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

Radio Extended Configurations

Beacon period.....	100 milliseconds
Beacon range.....	AUTO
Multicast buffer.....	AUTO
Multicast data-rate.....	AUTO

RX SOP threshold.....	AUTO
CCA threshold.....	AUTO

Attributes for Slot 1

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

Station Configuration

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

Operation Rate Set

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

MCS Set

MCS 0.....	SUPPORTED
MCS 1.....	SUPPORTED
MCS 2.....	SUPPORTED

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

Multi Domain Capability Enabled	TRUE
Country String	US
Multi Domain Capability	
Configuration	AUTOMATIC
First Chan Num	36
Number Of Channels	21
MAC Operation Parameters	
Configuration	AUTOMATIC
Fragmentation Threshold	2346
Packet Retry Limit	64
Tx Power	
Num Of Supported Power Levels	6
Tx Power Level 1	22 dBm
Tx Power Level 2	19 dBm
Tx Power Level 3	16 dBm
Tx Power Level 4	13 dBm
Tx Power Level 5	10 dBm
Tx Power Level 6	7 dBm
Tx Power Configuration	AUTOMATIC
Current Tx Power Level	1
Tx Power Assigned By	DTPC
Phy OFDM parameters	
Configuration	AUTOMATIC
Current Channel	149
Channel Assigned By	DCA
Extension Channel	NONE
Channel Width.....	20 Mhz
Allowed Channel List.....	36,40,44,48,52,56,60,64,100,,104,108,112,116,132,136,140,

..... 149, 153, 157, 161, 165

TI Threshold -50

DCA Channel List..... Global

Legacy Tx Beamforming Configuration CUSTOMIZED

Legacy Tx Beamforming ENABLED

Antenna Type..... INTERNAL_ANTENNA

Internal Antenna Gain (in .5 dBi units).... 8

Diversity..... DIVERSITY_ENABLED

802.11n Antennas

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

Performance Profile Parameters

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

Rogue Containment Information

Containment Count.....	0
------------------------	---

CleanAir Management Information

CleanAir Capable.....	Yes
CleanAir Management Administration St....	Enabled
CleanAir Management Operation State.....	Down
Rapid Update Mode.....	Off
Spectrum Expert connection.....	Enabled

CleanAir NSI Key..... C44B365F4CFF338BE94B85633D98944B
Spectrum Expert Connections counter.... 0
CleanAir Sensor State..... Configured

Radio Extended Configurations

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

Cisco AP Identifier..... 4
Cisco AP Name..... AP24e9.b34b.f1ed
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A 802.11a:-AB
AP Country code..... US - United States
AP Regulatory Domain..... -A
Switch Port Number 1
MAC Address..... 24:e9:b3:4b:f1:ed
IP Address Configuration..... DHCP
IP Address..... 192.168.250.11
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 192.168.250.1
NAT External IP Address..... None
CAPWAP Path MTU..... 1485
DHCP Release Override..... Disabled
Telnet State..... Globally Disabled
Ssh State..... Globally Disabled
Cisco AP Location..... default location
Cisco AP Floor Label..... 0
Cisco AP Group Name..... default-group

Primary Cisco Switch Name.....	
Primary Cisco Switch IP Address.....	Not Configured
Secondary Cisco Switch Name.....	
Secondary Cisco Switch IP Address.....	Not Configured
Tertiary Cisco Switch Name.....	
Tertiary Cisco Switch IP Address.....	Not Configured
Administrative State	ADMIN_ENABLED
Operation State	REGISTERED
Mirroring Mode	Disabled
AP Mode	FlexConnect
Public Safety	Disabled
ATF Mode:	Disable
AP SubMode	Not Configured
Rogue Detection	Enabled
AP Vlan Trunking	Disabled
Remote AP Debug	Disabled
Logging trap severity level	emergencies
Logging syslog facility	system
S/W Version	8.2.111.0
Boot Version	15.2.2.0
Mini IOS Version	7.5.1.73
Stats Reporting Period	180
Stats Collection Mode	normal
LED State.....	Enabled
PoE Pre-Standard Switch.....	Disabled
PoE Power Injector MAC Addr.....	Disabled
Power Type/Mode.....	PoE/Full Power
Number Of Slots.....	2
AP Model.....	AIR-CAP1602I-A-K9
AP Image.....	C1600-K9W8-M
IOS Version.....	15.3(3)JC2\$
Reset Button.....	Enabled

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

Group VLAN Name to Id Mappings

Template in Modified State - apply it to see mappings

AP-Specific FlexConnect Policy ACLs :

L2Acl Configuration Not Available

FlexConnect Local-Split ACLs :

WLAN ID	PROFILE NAME	ACL	TYPE
-	-	-	-

Flexconnect Central-Dhcp Values :

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

Flex AVC visibility Configurations.....

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

```

1           IP_Dev No Encryption          wlan-spec      disable      none

FlexConnect Backup Auth Radius Servers :
Primary Radius Server..... Disabled
Secondary Radius Server..... Disabled
AP User Mode..... AUTOMATIC
AP User Name..... Cisco
AP Dot1x User Mode..... Not Configured
AP Dot1x User Name..... Not Configured
Cisco AP system logging host..... 255.255.255.255
AP Core Dump Config..... Disabled
AP Up Time..... 2 days, 22 h 22 m 16 s
AP LWAPP Up Time..... 2 days, 22 h 18 m 14 s
Join Date and Time..... Mon Aug 15 21:47:12 2016
Join Taken Time..... 0 days, 00 h 04 m 01 s

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

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

```

1000 Kilo Bits.....	MANDATORY
2000 Kilo Bits.....	MANDATORY
5500 Kilo Bits.....	MANDATORY
11000 Kilo Bits.....	MANDATORY
6000 Kilo Bits.....	SUPPORTED
9000 Kilo Bits.....	SUPPORTED
12000 Kilo Bits.....	SUPPORTED
18000 Kilo Bits.....	SUPPORTED
24000 Kilo Bits.....	SUPPORTED
36000 Kilo Bits.....	SUPPORTED
48000 Kilo Bits.....	SUPPORTED
54000 Kilo Bits.....	SUPPORTED
MCS Set	
MCS 0.....	SUPPORTED
MCS 1.....	SUPPORTED
MCS 2.....	SUPPORTED
MCS 3.....	SUPPORTED
MCS 4.....	SUPPORTED
MCS 5.....	SUPPORTED
MCS 6.....	SUPPORTED
MCS 7.....	SUPPORTED
MCS 8.....	SUPPORTED
MCS 9.....	SUPPORTED
MCS 10.....	SUPPORTED
MCS 11.....	SUPPORTED
MCS 12.....	SUPPORTED
MCS 13.....	SUPPORTED
MCS 14.....	SUPPORTED
MCS 15.....	SUPPORTED
MCS 16.....	DISABLED
MCS 17.....	DISABLED
MCS 18.....	DISABLED

MCS 19.....	DISABLED
MCS 20.....	DISABLED
MCS 21.....	DISABLED
MCS 22.....	DISABLED
MCS 23.....	DISABLED
MCS 24.....	DISABLED
MCS 25.....	DISABLED
MCS 26.....	DISABLED
MCS 27.....	DISABLED
MCS 28.....	DISABLED
MCS 29.....	DISABLED
MCS 30.....	DISABLED
MCS 31.....	DISABLED
Beacon Period	100
Fragmentation Threshold	2346
Multi Domain Capability Implemented	TRUE
Multi Domain Capability Enabled	TRUE
Country String	US

Multi Domain Capability

Configuration	AUTOMATIC
First Chan Num	1
Number Of Channels	11

MAC Operation Parameters

Configuration	AUTOMATIC
Fragmentation Threshold	2346
Packet Retry Limit	64

Tx Power

Num Of Supported Power Levels	6
Tx Power Level 1	22 dBm

Tx Power Level 2	19 dBm
Tx Power Level 3	16 dBm
Tx Power Level 4	13 dBm
Tx Power Level 5	10 dBm
Tx Power Level 6	7 dBm
Tx Power Configuration	AUTOMATIC
Current Tx Power Level	1
Tx Power Assigned By	DTPC

Phy OFDM parameters

Configuration	AUTOMATIC
Current Channel	11
Channel Assigned By	DCA
Extension Channel	NONE
Channel Width.....	20 Mhz
Allowed Channel List.....	1,2,3,4,5,6,7,8,9,10,11
TI Threshold	-50
DCA Channel List.....	Global
Legacy Tx Beamforming Configuration	CUSTOMIZED
Legacy Tx Beamforming	ENABLED
Antenna Type.....	INTERNAL_ANTENNA
Internal Antenna Gain (in .5 dBi units)....	8
Diversity.....	DIVERSITY_ENABLED
802.11n Antennas	
A.....	ENABLED
B.....	ENABLED
C.....	ENABLED

Performance Profile Parameters

Configuration	AUTOMATIC
Interference threshold.....	10 %
Noise threshold.....	-70 dBm

RF utilization threshold..... 80 %
Data-rate threshold..... 1000000 bps
Client threshold..... 12 clients
Coverage SNR threshold..... 12 dB
Coverage exception level..... 25 %
Client minimum exception level..... 3 clients

Rogue Containment Information
Containment Count..... 0

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

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

Attributes for Slot 1
Radio Type..... RADIO_TYPE_80211n-5
Radio Subband..... RADIO_SUBBAND_ALL
Administrative State ADMIN_ENABLED
Operation State UP

Mesh Radio Role	ACCESS
Radio Role	Client Serving (Remote)
CellId	0
Station Configuration	
Configuration	AUTOMATIC
Number Of WLANs	1
Medium Occupancy Limit	100
CFP Period	4
CFP MaxDuration	60
BSSID	1c:1d:86:31:e5:50
Operation Rate Set	
6000 Kilo Bits.....	MANDATORY
9000 Kilo Bits.....	SUPPORTED
12000 Kilo Bits.....	MANDATORY
18000 Kilo Bits.....	SUPPORTED
24000 Kilo Bits.....	MANDATORY
36000 Kilo Bits.....	SUPPORTED
48000 Kilo Bits.....	SUPPORTED
54000 Kilo Bits.....	SUPPORTED
MCS Set	
MCS 0.....	SUPPORTED
MCS 1.....	SUPPORTED
MCS 2.....	SUPPORTED
MCS 3.....	SUPPORTED
MCS 4.....	SUPPORTED
MCS 5.....	SUPPORTED
MCS 6.....	SUPPORTED
MCS 7.....	SUPPORTED
MCS 8.....	SUPPORTED
MCS 9.....	SUPPORTED
MCS 10.....	SUPPORTED

MCS 11.....	SUPPORTED
MCS 12.....	SUPPORTED
MCS 13.....	SUPPORTED
MCS 14.....	SUPPORTED
MCS 15.....	SUPPORTED
MCS 16.....	DISABLED
MCS 17.....	DISABLED
MCS 18.....	DISABLED
MCS 19.....	DISABLED
MCS 20.....	DISABLED
MCS 21.....	DISABLED
MCS 22.....	DISABLED
MCS 23.....	DISABLED
MCS 24.....	DISABLED
MCS 25.....	DISABLED
MCS 26.....	DISABLED
MCS 27.....	DISABLED
MCS 28.....	DISABLED
MCS 29.....	DISABLED
MCS 30.....	DISABLED
MCS 31.....	DISABLED
Beacon Period	100
Fragmentation Threshold	2346
Multi Domain Capability Implemented	TRUE
Multi Domain Capability Enabled	TRUE
Country String	US
 Multi Domain Capability	
Configuration	AUTOMATIC
First Chan Num	36
Number Of Channels	21

MAC Operation Parameters

Configuration	AUTOMATIC
Fragmentation Threshold	2346
Packet Retry Limit	64

Tx Power

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

Phy OFDM parameters

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

Diversity..... DIVERSITY_ENABLED

802.11n Antennas

A..... ENABLED

B..... ENABLED

C..... ENABLED

Performance Profile Parameters

Configuration AUTOMATIC

Interference threshold..... 10 %

Noise threshold..... -70 dBm

RF utilization threshold..... 80 %

Data-rate threshold..... 1000000 bps

Client threshold..... 12 clients

Coverage SNR threshold..... 16 dB

Coverage exception level..... 25 %

Client minimum exception level..... 3 clients

Rogue Containment Information

Containment Count..... 0

CleanAir Management Information

CleanAir Capable..... Yes

CleanAir Management Administration St.... Disabled

CleanAir Management Operation State..... Down

Rapid Update Mode..... Off

Spectrum Expert connection..... Enabled

CleanAir NSI Key..... 8994C2313910BF9588C6693603B8F970

Spectrum Expert Connections counter.... 0

CleanAir Sensor State..... Configured

Radio Extended Configurations

Beacon period..... 100 milliseconds

Beacon range..... AUTO

Multicast buffer.....	AUTO
Multicast data-rate.....	AUTO
RX SOP threshold.....	AUTO
CCA threshold.....	AUTO

AP Airewave Director Configuration

AP does not have the 802.11-abgn radio.

Number Of Slots.....	2
AP Name.....	AP78da.6ee0.08ec
MAC Address.....	78:da:6e:e0:08:ec
Slot ID.....	0
Radio Type.....	RADIO_TYPE_80211b/g
Sub-band Type.....	All

Noise Information

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

Interference Information

Interference Profile.....	PASSED
---------------------------	--------

Rogue Histogram (20)

.....

Load Information

Load Profile.....	PASSED
-------------------	--------

Receive Utilization.....	0 %
--------------------------	-----

Transmit Utilization.....	0 %
---------------------------	-----

Channel Utilization.....	38 %
--------------------------	------

Attached Clients.....	0 clients
-----------------------	-----------

Coverage Information

Coverage Profile.....	PASSED
-----------------------	--------

Failed Clients.....	0 clients
---------------------	-----------

Client Signal Strengths

RSSI -100 dbm.....	0 clients
--------------------	-----------

RSSI -92 dbm.....	0 clients
-------------------	-----------

RSSI -84 dbm.....	0 clients
-------------------	-----------

RSSI -76 dbm..... 0 clients
RSSI -68 dbm..... 0 clients
RSSI -60 dbm..... 0 clients
RSSI -52 dbm..... 0 clients

Client Signal To Noise Ratios

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

Nearby APs

Radar Information

Channel Assignment Information

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

RF Parameter Recommendations

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

Persistent Interference Devices

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

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

Number Of Slots.....	2
AP Name.....	AP78da.6ee0.08ec
MAC Address.....	78:da:6e:e0:08:ec
Slot ID.....	1
Radio Type.....	RADIO_TYPE_80211a
Sub-band Type.....	All
Noise Information	
Noise Profile.....	PASSED
Interference Information	
Interference Profile.....	PASSED
Rogue Histogram (20/40/80/160)	
.....	
Load Information	
Load Profile.....	PASSED
Receive Utilization.....	0 %
Transmit Utilization.....	0 %
Channel Utilization.....	1 %
Attached Clients.....	0 clients
Coverage Information	
Coverage Profile.....	PASSED
Failed Clients.....	0 clients
Client Signal Strengths	
RSSI -100 dbm.....	0 clients
RSSI -92 dbm.....	0 clients
RSSI -84 dbm.....	0 clients
RSSI -76 dbm.....	0 clients
RSSI -68 dbm.....	0 clients
RSSI -60 dbm.....	0 clients
RSSI -52 dbm.....	0 clients
Client Signal To Noise Ratios	
SNR 0 dB.....	0 clients

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

Nearby APs

Radar Information

Channel Assignment Information

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

RF Parameter Recommendations

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

Persistent Interference Devices

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

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

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

AP does not have the 802.11-abgn radio.

Number Of Slots.....	2
AP Name.....	AP24e9.b34b.f1ed
MAC Address.....	24:e9:b3:4b:f1:ed

Slot ID..... 0

Radio Type..... RADIO_TYPE_80211b/g

Sub-band Type..... All

Noise Information

 Noise Profile..... PASSED

Interference Information

 Interference Profile..... PASSED

 Rogue Histogram (20)

Load Information

 Load Profile..... PASSED

 Receive Utilization..... 0 %

 Transmit Utilization..... 0 %

 Channel Utilization..... 34 %

 Attached Clients..... 1 clients

Coverage Information

 Coverage Profile..... PASSED

 Failed Clients..... 0 clients

Client Signal Strengths

 RSSI -100 dbm..... 0 clients

 RSSI -92 dbm..... 0 clients

 RSSI -84 dbm..... 0 clients

 RSSI -76 dbm..... 0 clients

 RSSI -68 dbm..... 0 clients

 RSSI -60 dbm..... 0 clients

 RSSI -52 dbm..... 1 clients

Client Signal To Noise Ratios

 SNR 0 dB..... 0 clients

 SNR 5 dB..... 0 clients

 SNR 10 dB..... 0 clients

 SNR 15 dB..... 0 clients

 SNR 20 dB..... 0 clients

SNR	25 dB.....	0 clients
SNR	30 dB.....	0 clients
SNR	35 dB.....	0 clients
SNR	40 dB.....	0 clients
SNR	45 dB.....	1 clients

Nearby APs

Radar Information

Channel Assignment Information

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

RF Parameter Recommendations

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

Persistent Interference Devices

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

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

Number Of Slots..... 2

AP Name..... AP24e9.b34b.f1ed

MAC Address..... 24:e9:b3:4b:f1:ed

Slot ID..... 1

Radio Type..... RADIO_TYPE_80211a

Sub-band Type..... All

Noise Information

Noise Profile..... PASSED

Interference Information

Interference Profile..... PASSED
Rogue Histogram (20/40/80/160)
.....
Load Information
Load Profile..... PASSED
Receive Utilization..... 0 %
Transmit Utilization..... 0 %
Channel Utilization..... 0 %
Attached Clients..... 0 clients
Coverage Information
Coverage Profile..... PASSED
Failed Clients..... 0 clients
Client Signal Strengths
RSSI -100 dbm..... 0 clients
RSSI -92 dbm..... 0 clients
RSSI -84 dbm..... 0 clients
RSSI -76 dbm..... 0 clients
RSSI -68 dbm..... 0 clients
RSSI -60 dbm..... 0 clients
RSSI -52 dbm..... 0 clients
Client Signal To Noise Ratios
SNR 0 dB..... 0 clients
SNR 5 dB..... 0 clients
SNR 10 dB..... 0 clients
SNR 15 dB..... 0 clients
SNR 20 dB..... 0 clients
SNR 25 dB..... 0 clients
SNR 30 dB..... 0 clients
SNR 35 dB..... 0 clients
SNR 40 dB..... 0 clients
SNR 45 dB..... 0 clients
Nearby APs

Radar Information

Channel Assignment Information

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

RF Parameter Recommendations

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

Persistent Interference Devices

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

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

802.11a Configuration

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

802.11a Operational Rates

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

802.11a 48M Rate.....	Supported
802.11a 54M Rate.....	Supported
802.11n MCS Settings:	
MCS 0.....	Supported
MCS 1.....	Supported
MCS 2.....	Supported
MCS 3.....	Supported
MCS 4.....	Supported
MCS 5.....	Supported
MCS 6.....	Supported
MCS 7.....	Supported
MCS 8.....	Supported
MCS 9.....	Supported
MCS 10.....	Supported
MCS 11.....	Supported
MCS 12.....	Supported
MCS 13.....	Supported
MCS 14.....	Supported
MCS 15.....	Supported
MCS 16.....	Supported
MCS 17.....	Supported
MCS 18.....	Supported
MCS 19.....	Supported
MCS 20.....	Supported
MCS 21.....	Supported
MCS 22.....	Supported
MCS 23.....	Supported
MCS 24.....	Supported
MCS 25.....	Supported
MCS 26.....	Supported
MCS 27.....	Supported
MCS 28.....	Supported

MCS 29.....	Supported
MCS 30.....	Supported
MCS 31.....	Supported
802.11ac MCS Settings:	
Nss=1: MCS 0-9	Supported
Nss=2: MCS 0-9	Supported
Nss=3: MCS 0-9	Supported
Nss=4: MCS 0-7	Supported
802.11n Status:	
A-MPDU Tx:	
Priority 0.....	Enabled
Priority 1.....	Enabled
Priority 2.....	Enabled
Priority 3.....	Enabled
Priority 4.....	Enabled
Priority 5.....	Enabled
Priority 6.....	Disabled
Priority 7.....	Disabled
Aggregation scheduler.....	Enabled
Frame Burst.....	Automatic
Realtime Timeout.....	10
Non Realtime Timeout.....	200
A-MSDU Tx:	
Priority 0.....	Enabled
Priority 1.....	Enabled
Priority 2.....	Enabled
Priority 3.....	Enabled
Priority 4.....	Enabled
Priority 5.....	Enabled
Priority 6.....	Disabled
Priority 7.....	Disabled
A-MSDU Max Subframes	3

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

```

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

Video AC:

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

CAC SIP-Video Configuration

SIP based CAC ..... Disabled
Best-effort AC - Admission control (ACM) ..... Disabled
Background AC - Admission control (ACM) ..... Disabled
Maximum Number of Clients per AP Radio ..... 200

```

802.11a Advanced Configuration

Member RRM Information

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

802.11a Airewave Director Configuration

RF Event and Performance Logging

```

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

```

```
Performance Profile Logging..... Off
TxPower Update Logging..... Off
Default 802.11a AP performance profiles
    802.11a Global Interference threshold..... 10 %
    802.11a Global noise threshold..... -70 dBm
    802.11a Global RF utilization threshold..... 80 %
    802.11a Global throughput threshold..... 1000000 bps
    802.11a Global clients threshold..... 12 clients
Default 802.11a AP monitoring
    802.11a Monitor Mode..... enable
    802.11a Monitor Mode for Mesh AP Backhaul..... disable
    802.11a Monitor Channels..... Country channels
    802.11a RRM Neighbor Discover Type..... Transparent
    802.11a RRM Neighbor RSSI Normalization..... Enabled
    802.11a AP Coverage Interval..... 90 seconds
    802.11a AP Load Interval..... 60 seconds
    802.11a AP Monitor Measurement Interval..... 180 seconds
    802.11a AP Neighbor Timeout Factor..... 5
    802.11a AP Report Measurement Interval..... 180 seconds
Leader Automatic Transmit Power Assignment
    Transmit Power Assignment Mode..... AUTO
    Transmit Power Update Interval..... 600 seconds
    Transmit Power Threshold..... -70 dBm
    Transmit Power Neighbor Count..... 3 APs
    Min Transmit Power..... -10 dBm
    Max Transmit Power..... 30 dBm
    Update Contribution
        Noise..... Enable
        Interference..... Enable
        Load..... Disable
        Device Aware..... Disable
    Transmit Power Assignment Leader..... wlc (192.168.250.2) (::)
```

Last Run..... 21 seconds ago
 Last Run Time..... 0 seconds
 TPC Mode..... Version 1
 TPCv2 Target RSSI..... -67 dBm
 TPCv2 VoWLAN Guide RSSI..... -67.0 dBm
 TPCv2 SOP..... -85.0 dBm
 TPCv2 Default Client Ant Gain..... 0.0 dBi
 TPCv2 Path Loss Decay Factor..... 3.6
 TPCv2 Search Intensity..... 10 Iterations

AP Name	Channel	TxPower	Allowed Power Levels
<hr/>			
AP78da.6ee0.08ec	149*	*1/6 (22 dBm)	[22/19/16/13/10/7/7/7]
AP24e9.b34b.fled	48*	*1/6 (22 dBm)	[22/19/16/13/10/7/7/7]
Coverage Hole Detection			
802.11a Coverage Hole Detection Mode.....	Enabled		
802.11a Coverage Voice Packet Count.....	100 packets		
802.11a Coverage Voice Packet Percentage.....	50%		
802.11a Coverage Voice RSSI Threshold.....	-80 dBm		
802.11a Coverage Data Packet Count.....	50 packets		
802.11a Coverage Data Packet Percentage.....	50%		
802.11a Coverage Data RSSI Threshold.....	-80 dBm		
802.11a Global coverage exception level.....	25 %		
802.11a Global client minimum exception lev....	3 clients		
OptimizedRoaming			
802.11a OptimizedRoaming Mode.....	Disabled		
802.11a OptimizedRoaming Reporting Interval....	90 seconds		
802.11a OptimizedRoaming Rate Threshold.....	disabled		
802.11a OptimizedRoaming Hysteresis.....	6 dB		
OptimizedRoaming Stats			
802.11a OptimizedRoaming Disassociations.....	0		
802.11a OptimizedRoaming Rejections.....	0		

Leader Automatic Channel Assignment

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

Update Contribution

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

CleanAir Event-driven RRM option..... Disabled

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

DCA Sensitivity Level..... MEDIUM (15 dB)

DCA 802.11n/ac Channel Width..... 20 MHz

DCA Minimum Energy Limit..... -95 dBm

Channel Energy Levels

Minimum.....	-127 dBm
Average.....	-127 dBm
Maximum.....	-127 dBm

Channel Dwell Times

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

802.11a 5 GHz Auto-RF Channel List

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

802.11a 4.9 GHz Auto-RF Channel List

Allowed Channel List.....	
---------------------------	--

Unused Channel List..... 1,2,3,4,5,6,7,8,9,10,11,12,
13,14,15,16,17,18,19,20,21,
22,23,24,25,26

DCA Outdoor AP option..... Disabled

802.11a Radio RF Grouping

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

802.11a CleanAir Configuration

Clean Air Solution.....	Disabled
Air Quality Settings:	
Air Quality Reporting.....	Enabled
Air Quality Reporting Period (min).....	15
Air Quality Alarms.....	Enabled
Air Quality Alarm Threshold.....	35
Unclassified Interference.....	Disabled
Unclassified Severity Threshold.....	20
Interference Device Settings:	
Interference Device Reporting.....	Enabled
Interference Device Types:	
TDD Transmitter.....	Enabled
Jammer.....	Enabled

Continuous Transmitter..... Enabled
DECT-like Phone..... Enabled
Video Camera..... Enabled
WiFi Inverted..... Enabled
WiFi Invalid Channel..... Enabled
SuperAG..... Enabled
Canopy..... Enabled
WiMax Mobile..... Enabled
WiMax Fixed..... Enabled
Interference Device Alarms..... Enabled
Interference Device Types Triggering Alarms:
TDD Transmitter..... Disabled
Jammer..... Enabled
Continuous Transmitter..... Disabled
DECT-like Phone..... Disabled
Video Camera..... Disabled
WiFi Inverted..... Enabled
WiFi Invalid Channel..... Enabled
SuperAG..... Disabled
Canopy..... Disabled
WiMax Mobile..... Disabled
WiMax Fixed..... Disabled
Additional Clean Air Settings:
CleanAir ED-RRM State..... Disabled
CleanAir ED-RRM Sensitivity..... Medium
CleanAir ED-RRM Custom Threshold..... 50
CleanAir Rogue Contribution..... Disabled
CleanAir Rogue Duty-Cycle Threshold..... 80
CleanAir Persistent Devices state..... Disabled
CleanAir Persistent Device Propagation..... Disabled

802.11a CleanAir AirQuality Summary

AQ = Air Quality

DFS = Dynamic Frequency Selection

AP Name	Channel	Avg AQ	Min AQ	Interferers	DFS
<hr/>					
802.11b Configuration					
802.11b Network.....					Enabled
11gSupport.....					Enabled
11nSupport.....					Enabled
802.11b/g Operational Rates					
802.11b/g 1M Rate.....					Mandatory
802.11b/g 2M Rate.....					Mandatory
802.11b/g 5.5M Rate.....					Mandatory
802.11b/g 11M Rate.....					Mandatory
802.11g 6M Rate.....					Supported
802.11g 9M Rate.....					Supported
802.11g 12M Rate.....					Supported
802.11g 18M Rate.....					Supported
802.11g 24M Rate.....					Supported
802.11g 36M Rate.....					Supported
802.11g 48M Rate.....					Supported
802.11g 54M Rate.....					Supported
802.11n MCS Settings:					
MCS 0.....					Supported
MCS 1.....					Supported
MCS 2.....					Supported
MCS 3.....					Supported
MCS 4.....					Supported
MCS 5.....					Supported
MCS 6.....					Supported
MCS 7.....					Supported

MCS 8.....	Supported
MCS 9.....	Supported
MCS 10.....	Supported
MCS 11.....	Supported
MCS 12.....	Supported
MCS 13.....	Supported
MCS 14.....	Supported
MCS 15.....	Supported
MCS 16.....	Supported
MCS 17.....	Supported
MCS 18.....	Supported
MCS 19.....	Supported
MCS 20.....	Supported
MCS 21.....	Supported
MCS 22.....	Supported
MCS 23.....	Supported
MCS 24.....	Supported
MCS 25.....	Supported
MCS 26.....	Supported
MCS 27.....	Supported
MCS 28.....	Supported
MCS 29.....	Supported
MCS 30.....	Supported
MCS 31.....	Supported

802.11n Status:

A-MPDU Tx:

Priority 0.....	Enabled
Priority 1.....	Enabled
Priority 2.....	Enabled
Priority 3.....	Enabled
Priority 4.....	Enabled
Priority 5.....	Enabled

Priority 6.....	Disabled
Priority 7.....	Disabled
Aggregation scheduler.....	Enabled
Realtime Timeout.....	10
Non Realtime Timeout.....	200
A-MSDU Tx:	
Priority 0.....	Enabled
Priority 1.....	Enabled
Priority 2.....	Enabled
Priority 3.....	Enabled
Priority 4.....	Enabled
Priority 5.....	Enabled
Priority 6.....	Disabled
Priority 7.....	Disabled
A-MSDU Max Subframes	3
A-MSDU MAX Length	8k
Rifs Rx	Enabled
Guard Interval	Any
Beacon Interval.....	100
CF Pollable mode.....	Disabled
CF Poll Request mandatory.....	Disabled
CFP Period.....	4
CFP Maximum Duration.....	60
Default Channel.....	1
Default Tx Power Level.....	0
DTPC Status.....	Enabled
RSSI Low Check.....	Disabled
RSSI Threshold.....	-80
Call Admission Limit	105
G711 CU Quantum	15
ED Threshold.....	-50
Fragmentation Threshold.....	2346

PBCC mandatory.....	Disabled
RTS Threshold.....	2347
Short Preamble mandatory.....	Enabled
Short Retry Limit.....	7
Legacy Tx Beamforming setting.....	Disabled
Traffic Stream Metrics Status.....	Disabled
Expedited BW Request Status.....	Disabled
World Mode.....	Enabled
Faster Carrier Tracking Loop.....	Disabled
EDCA profile type.....	default-wmm
Voice MAC optimization status.....	Disabled
Call Admission Control (CAC) configuration	
Voice AC - Admission control (ACM).....	Disabled
Voice Stream-Size.....	84000
Voice Max-Streams.....	2
Voice max RF bandwidth.....	75
Voice reserved roaming bandwidth.....	6
Voice CAC Method.....	Load-Based
Voice tspec inactivity timeout.....	Disabled
CAC SIP-Voice configuration	
SIP based CAC	Disabled
SIP Codec Type	CODEC_TYPE_G711
SIP call bandwidth:	64
SIP call bandwidth sample-size	20
Video AC - Admission control (ACM).....	Disabled
Video max RF bandwidth.....	Infinite
Video reserved roaming bandwidth.....	0
Video load-based CAC mode.....	Disabled
Video CAC Method	Static
CAC SIP-Video configuration	
SIP based CAC	Disabled
Best-effort AC - Admission control (ACM).....	Disabled

Background AC - Admission control (ACM) Disabled
Maximum Number of Clients per AP..... 200

802.11b Advanced Configuration

Member RRM Information

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

802.11b Airewave Director Configuration

RF Event and Performance Logging

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

Default 802.11b AP performance profiles

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

Default 802.11b AP monitoring

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

Leader Automatic Transmit Power Assignment

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

Update Contribution

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

Transmit Power Assignment Leader..... wlc (192.168.250.2) (::)

Last Run.....	225 seconds ago
Last Run Time.....	0 seconds
TPC Mode.....	Version 1
TPCv2 Target RSSI.....	-67 dBm
TPCv2 VoWLAN Guide RSSI.....	-67.0 dBm
TPCv2 SOP.....	-85.0 dBm
TPCv2 Default Client Ant Gain.....	0.0 dBi
TPCv2 Path Loss Decay Factor.....	3.6
TPCv2 Search Intensity.....	10 Iterations

AP Name	Channel	TxPower	Allowed Power Levels
<hr/>			
AP78da.6ee0.08ec	*11	*1/6 (22 dBm)	[22/19/16/13/10/7/7/7]
AP24e9.b34b.fled	*11	*1/6 (22 dBm)	[22/19/16/13/10/7/7/7]
Coverage Hole Detection			
802.11b Coverage Hole Detection Mode.....	Enabled		
802.11b Coverage Voice Packet Count.....	100 packets		
802.11b Coverage Voice Packet Percentage.....	50%		
802.11b Coverage Voice RSSI Threshold.....	-80 dBm		
802.11b Coverage Data Packet Count.....	50 packets		
802.11b Coverage Data Packet Percentage.....	50%		
802.11b Coverage Data RSSI Threshold.....	-80 dBm		
802.11b Global coverage exception level.....	25 %		
802.11b Global client minimum exception lev....	3 clients		
OptimizedRoaming			
802.11b OptimizedRoaming Mode.....	Disabled		
802.11b OptimizedRoaming Reporting Interval....	90 seconds		
802.11b OptimizedRoaming Rate Threshold.....	disabled		
802.11b OptimizedRoaming Hysteresis.....	6 dB		
OptimizedRoaming Stats			
802.11b OptimizedRoaming Disassociations.....	0		
802.11b OptimizedRoaming Rejections.....	0		
Leader Automatic Channel Assignment			
Channel Assignment Mode.....	AUTO		
Channel Update Interval.....	600 seconds		
Anchor time (Hour of the day).....	0		
Update Contribution			
Noise.....	Enable		
Interference.....	Enable		

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

DCA Sensitivity Level: MEDIUM (10 dB)
 DCA Minimum Energy Limit..... -95 dBm

Channel Energy Levels

Minimum.....	-127 dBm
Average.....	-127 dBm
Maximum.....	-127 dBm

Channel Dwell Times

Minimum.....	0 days, 00 h 03 m 43 s
Average.....	0 days, 00 h 03 m 43 s
Maximum.....	0 days, 00 h 03 m 43 s

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

802.11b Radio RF Grouping

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

802.11b CleanAir Configuration

Clean Air Solution..... Disabled

Air Quality Settings:

Air Quality Reporting..... Enabled

Air Quality Reporting Period (min)..... 15

Air Quality Alarms..... Enabled

Air Quality Alarm Threshold..... 35

Unclassified Interference..... Disabled

Unclassified Severity Threshold..... 20

Interference Device Settings:

Interference Device Reporting..... Enabled

Interference Device Types:

Bluetooth Link..... Enabled

Microwave Oven..... Enabled

802.11 FH..... Enabled

Bluetooth Discovery..... Enabled

TDD Transmitter..... Enabled

Jammer..... Enabled

Continuous Transmitter..... Enabled

DECT-like Phone..... Enabled

Video Camera..... Enabled

802.15.4..... Enabled

WiFi Inverted..... Enabled

WiFi Invalid Channel..... Enabled

SuperAG..... Enabled

Canopy..... Enabled

Microsoft Device..... Enabled

WiMax Mobile..... Enabled

WiMax Fixed..... Enabled

BLE Beacon..... Enabled

Interference Device Alarms..... Enabled

Interference Device Types Triggering Alarms:

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

Additional Clean Air Settings:

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

802.11a CleanAir AirQuality Summary

AQ = Air Quality

DFS = Dynamic Frequency Selection

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

RF Density Optimization Configurations

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

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

COF : Coverage Overlap Factor

RF Client Steering Configurations

Client Steering Configuration Information

Macro to micro transition threshold.....	-55 dBm
micro to Macro transition threshold.....	-65 dBm
micro-Macro transition minimum client count....	3
micro-Macro transition client balancing win....	3
Probe suppression mode.....	disabled

Probe suppression validity window..... 100 s
Probe suppression aggregate window..... 200 ms
Probe suppression transition aggressiveness.... 3
Probe suppression hysteresis..... -6 dBm

Mobility Configuration

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

Controllers configured in the Mobility Group

MAC Address	IP Address	Status	Group Name
Multicast IP			
00:50:56:ac:6d:08	192.168.250.2		WLAN
0.0.0.0		Up	

Mobility Hash Configuration

Default Mobility Domain..... WLAN

IP Address	Hash Key

192.168.250.2 7a9b864fa2922672949cf9a66fd012a0ce8cc7b0

Self Signed Certificate details

SSC Hash validation..... Enabled.

SSC Device Certificate details:

Subject Name :

C=US, ST=California, L=San Jose, O=Cisco Virtual Wireless LAN Controller,

CN=DEVICE-vWLC-AIR-CTVM-K9-005056AC6338,
emailAddress=support@vwlc.com

Validity :

Start : Jul 26 20:52:54 2016 GMT

End : Jun 4 20:52:54 2026 GMT

Hash key : 7a9b864fa2922672949cf9a66fd012a0ce8cc7b0

Mobility Foreign Map Configuration

WLAN ID	Foreign Mac Address	Interface
-----	-----	-----

Advanced Configuration

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

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

dot11-padding..... Disabled

padding-size..... 0

Advanced Hotspot Commands

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

Location Configuration

RFID Tag data Collection..... Enabled
RFID timeout..... 1200 seconds

RFID mobility.....

Interface Configuration

Interface Name.....	ip_dev
MAC Address.....	00:50:56:ac:6d:08
IP Address.....	192.168.150.2
IP Netmask.....	255.255.255.0
IP Gateway.....	192.168.150.1
External NAT IP State.....	Disabled
External NAT IP Address.....	0.0.0.0
VLAN.....	1500
Quarantine-vlan.....	0
NAS-Identifier.....	none
Physical Port.....	1
DHCP Proxy Mode.....	Global
Primary DHCP Server.....	Unconfigured
Secondary DHCP Server.....	Unconfigured
DHCP Option 82.....	Disabled
DHCP Option 82 bridge mode insertion.....	Disabled
IPv4 ACL.....	Unconfigured
mDNS Profile Name.....	Unconfigured
AP Manager.....	No
Guest Interface.....	N/A
3G VLAN.....	Disabled
L2 Multicast.....	Enabled
Interface Name.....	management
MAC Address.....	00:50:56:ac:6d:08
IP Address.....	192.168.250.2
IP Netmask.....	255.255.255.0

IP Gateway.....	192.168.250.1
External NAT IP State.....	Disabled
External NAT IP Address.....	0.0.0.0
Link Local IPv6 Address.....	fe80::250:56ff:feac:6d08/64
STATE	REACHABLE
Primary IPv6 Address.....	::/128
STATE	NONE
Primary IPv6 Gateway.....	::
Primary IPv6 Gateway Mac Address.....	00:00:00:00:00:00
STATE	INCOMPLETE
VLAN.....	1520
Quarantine-vlan.....	0
Physical Port.....	1
DHCP Proxy Mode.....	Global
Primary DHCP Server.....	192.168.250.1
Secondary DHCP Server.....	Unconfigured
DHCP Option 82.....	Disabled
DHCP Option 82 bridge mode insertion.....	Disabled
IPv4 ACL.....	Unconfigured
IPv6 ACL.....	Unconfigured
mDNS Profile Name.....	Unconfigured
AP Manager.....	Yes
Guest Interface.....	N/A
L2 Multicast.....	Enabled
Interface Name.....	service-port
MAC Address.....	00:50:56:ac:63:38
IP Address.....	192.168.29.146
IP Netmask.....	255.255.255.0
Link Local IPv6 Address.....	fe80::250:56ff:feac:6338/64
STATE	NONE
IPv6 Address.....	::/128

STATE	NONE
SLAAC.....	Disabled
DHCP Protocol.....	Disabled
AP Manager.....	No
Guest Interface.....	N/A
Speed	1Gbps
Duplex	Full
Auto Negotiation	Enabled
Link Status.....	Up
Port specific Information:	
inet	
addr:192.168.29.146	Bcast:192.168.29.255 Mask:255.255.255.0
inet6 addr:	
fe80::250:56ff:feac:6338/64 Scope:Link	
UP BROADCAST RUNNING MULTICAST MTU:1430 Metric:1	
RX packets:258830 errors:0 dropped:298 overruns:0 frame:0	
TX packets:95115 errors:0	
dropped:0 overruns:0 carrier:0	
collisions:0 txqueuelen:1000	
RX bytes:25069479	
(23.9 MiB) TX bytes:55852901 (53.2 MiB)	
Interface Name..... virtual	
MAC Address.....	00:50:56:ac:6d:08
IP Address.....	1.1.1.1
Virtual DNS Host Name.....	Disabled
AP Manager.....	No
Guest Interface.....	N/A

Interface Group Configuration

WLAN Configuration

WLAN Identifier.....	1
Profile Name.....	IP_Dev No Encryption
Network Name (SSID)	IP_Dev
Status.....	Disabled
MAC Filtering.....	Disabled
Broadcast SSID.....	Enabled
AAA Policy Override.....	Disabled
Network Admission Control	
Client Profiling Status	
Radius Profiling	Disabled
DHCP	Disabled
HTTP	Disabled
Local Profiling	Disabled
DHCP	Disabled
HTTP	Disabled
Radius-NAC State.....	Disabled
SNMP-NAC State.....	Disabled
Quarantine VLAN.....	0
Maximum number of Associated Clients.....	0
Maximum number of Clients per AP Radio.....	200
ATF Policy.....	0
Number of Active Clients.....	0
Exclusionlist Timeout.....	60 seconds
Session Timeout.....	86400 seconds
User Idle Timeout.....	Disabled
Sleep Client.....	disable

Sleep Client Timeout.....	720 minutes
User Idle Threshold.....	0 Bytes
NAS-identifier.....	none
CHD per WLAN.....	Enabled
Webauth DHCP exclusion.....	Disabled
Interface.....	ip_dev
Multicast Interface.....	Not Configured
WLAN IPv4 ACL.....	unconfigured
WLAN IPv6 ACL.....	unconfigured
WLAN Layer2 ACL.....	unconfigured
mDNS Status.....	Disabled
mDNS Profile Name.....	unconfigured
DHCP Server.....	Default
DHCP Address Assignment Required.....	Disabled
Static IP client tunneling.....	Disabled
Tunnel Profile.....	Unconfigured
Quality of Service.....	Silver
Per-SSID Rate Limits.....	Upstream Downstream
Average Data Rate.....	0 0
Average Realtime Data Rate.....	0 0
Burst Data Rate.....	0 0
Burst Realtime Data Rate.....	0 0
Per-Client Rate Limits.....	Upstream Downstream
Average Data Rate.....	0 0
Average Realtime Data Rate.....	0 0
Burst Data Rate.....	0 0
Burst Realtime Data Rate.....	0 0
Scan Defer Priority.....	4,5,6
Scan Defer Time.....	100 milliseconds
WMM.....	Allowed
WMM UAPSD Compliant Client Support.....	Disabled
Media Stream Multicast-direct.....	Disabled

CCX - AironetIE Support.....	Enabled
CCX - Gratuitous ProbeResponse (GPR)	Disabled
CCX - Diagnostics Channel Capability.....	Disabled
Dot11-Phone Mode (7920).....	Disabled
Wired Protocol.....	802.1P (Tag=0)
Passive Client Feature.....	Disabled
Peer-to-Peer Blocking Action.....	Disabled
Radio Policy.....	All
DTIM period for 802.11a radio.....	1
DTIM period for 802.11b radio.....	1
Radius Servers	
Authentication.....	Global Servers
Accounting.....	Global Servers
Interim Update.....	Enabled
Interim Update Interval.....	0
Framed IPv6 Acct AVP	Prefix
Dynamic Interface.....	Disabled
Dynamic Interface Priority.....	wlan
Local EAP Authentication.....	Disabled
Radius NAI-Realm.....	Disabled
Mu-Mimo.....	Enabled
Security	
802.11 Authentication:.....	Open System
FT Support.....	Disabled
Static WEP Keys.....	Disabled
802.1X.....	Disabled
Wi-Fi Protected Access (WPA/WPA2)	Disabled
Wi-Fi Direct policy configured.....	Disabled
EAP-Passthrough.....	Disabled
CKIP	Disabled
Web Based Authentication.....	Disabled

Web Authentication Timeout.....	300
Web-Passthrough.....	Disabled
Mac-auth-server.....	0.0.0.0
Web-portal-server.....	0.0.0.0
Conditional Web Redirect.....	Disabled
Splash-Page Web Redirect.....	Disabled
Auto Anchor.....	Disabled
FlexConnect Local Switching.....	Enabled
FlexConnect Central Association.....	Disabled
flexconnect Central Dhcp Flag.....	Disabled
flexconnect nat-pat Flag.....	Disabled
flexconnect Dns Override Flag.....	Disabled
flexconnect PPPoE pass-through.....	Disabled
flexconnect local-switching IP-source-guar....	Disabled
FlexConnect Vlan based Central Switching	Disabled
FlexConnect Local Authentication.....	Disabled
FlexConnect Learn IP Address.....	Enabled
Client MFP.....	Optional but inactive (WPA2 not configured)
PMF.....	Disabled
PMF Association Comeback Time.....	1
PMF SA Query RetryTimeout.....	200
Tkip MIC Countermeasure Hold-down Timer.....	60
Eap-params.....	Not Applicable
Flex Avc Profile Name.....	None
Flow Monitor Name.....	None
Split Tunnel Configuration	
Split Tunnel.....	Disabled
Call Snooping.....	Disabled
Roamed Call Re-Anchor Policy.....	Disabled
SIP CAC Fail Send-486-Busy Policy.....	Enabled
SIP CAC Fail Send Dis-Association Policy.....	Disabled

KTS based CAC Policy..... Disabled
Assisted Roaming Prediction Optimization..... Disabled
802.11k Neighbor List..... Disabled
802.11k Neighbor List Dual Band..... Disabled
802.11v Directed Multicast Service..... Disabled
802.11v BSS Max Idle Service..... Enabled
802.11v BSS Transition Service..... Disabled
802.11v BSS Transition Disassoc Imminent..... Disabled
802.11v BSS Transition Disassoc Timer..... 200
802.11v BSS Transition OpRoam Disassoc Timer..... 40
DMS DB is empty
Band Select..... Disabled
Load Balancing..... Disabled
Multicast Buffer..... Disabled
Universal Ap Admin..... Disabled

Mobility Anchor List

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

802.11u..... Disabled

MSAP Services..... Disabled

Local Policy

Priority Policy Name

WLAN Configuration

WLAN Identifier..... 2

Profile Name.....	IP_Dev All WPA/WPA2 PSK
Network Name (SSID)	IP_Dev
Status.....	Enabled
MAC Filtering.....	Disabled
Broadcast SSID.....	Enabled
AAA Policy Override.....	Disabled
Network Admission Control	
Client Profiling Status	
Radius Profiling	Disabled
DHCP	Disabled
HTTP	Disabled
Local Profiling	Disabled
DHCP	Disabled
HTTP	Disabled
Radius-NAC State.....	Disabled
SNMP-NAC State.....	Disabled
Quarantine VLAN.....	0
Maximum number of Associated Clients.....	0
Maximum number of Clients per AP Radio.....	200
ATF Policy.....	0
Number of Active Clients.....	2
Exclusionlist Timeout.....	60 seconds
Session Timeout.....	1800 seconds
User Idle Timeout.....	Disabled
Sleep Client.....	disable
Sleep Client Timeout.....	720 minutes
User Idle Threshold.....	0 Bytes
NAS-identifier.....	none
CHD per WLAN.....	Enabled
Webauth DHCP exclusion.....	Disabled
Interface.....	ip_dev
Multicast Interface.....	Not Configured

WLAN IPv4 ACL.....	unconfigured	
WLAN IPv6 ACL.....	unconfigured	
WLAN Layer2 ACL.....	unconfigured	
mDNS Status.....	Disabled	
mDNS Profile Name.....	unconfigured	
DHCP Server.....	Default	
DHCP Address Assignment Required.....	Disabled	
Static IP client tunneling.....	Disabled	
Tunnel Profile.....	Unconfigured	
Quality of Service.....	Silver	
Per-SSID Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0
Per-Client Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0
Scan Defer Priority.....	4,5,6	
Scan Defer Time.....	100 milliseconds	
WMM.....	Allowed	
WMM UAPSD Compliant Client Support.....	Disabled	
Media Stream Multicast-direct.....	Disabled	
CCX - AironetIE Support.....	Enabled	
CCX - Gratuitous ProbeResponse (GPR)	Disabled	
CCX - Diagnostics Channel Capability.....	Disabled	
Dot11-Phone Mode (7920).....	Disabled	
Wired Protocol.....	802.1P (Tag=0)	
Passive Client Feature.....	Disabled	
Peer-to-Peer Blocking Action.....	Disabled	

Radio Policy.....	All
DTIM period for 802.11a radio.....	1
DTIM period for 802.11b radio.....	1
Radius Servers	
Authentication.....	Global Servers
Accounting.....	Global Servers
Interim Update.....	Enabled
Interim Update Interval.....	0
Framed IPv6 Acct AVP	Prefix
Dynamic Interface.....	Disabled
Dynamic Interface Priority.....	wlan
Local EAP Authentication.....	Disabled
Radius NAI-Realm.....	Disabled
Mu-Mimo.....	Enabled
Security	
802.11 Authentication:.....	Open System
FT Support.....	Disabled
Static WEP Keys.....	Disabled
802.1X.....	Disabled
Wi-Fi Protected Access (WPA/WPA2).....	Enabled
WPA (SSN IE).....	Enabled
TKIP Cipher.....	Enabled
AES Cipher.....	Enabled
WPA2 (RSN IE).....	Enabled
TKIP Cipher.....	Disabled
AES Cipher.....	Enabled
OSEN IE.....	Disabled
Auth Key Management	
802.1x.....	Disabled
PSK.....	Enabled
CCKM.....	Disabled

FT-1X(802.11r)	Disabled
FT-PSK(802.11r)	Disabled
PMF-1X(802.11w)	Disabled
PMF-PSK(802.11w)	Disabled
OSEN-1X.....	Disabled
FT Reassociation Timeout.....	20
FT Over-The-DS mode.....	Disabled
GTK Randomization.....	Disabled
SKC Cache Support.....	Disabled
CCKM TSF Tolerance.....	1000
Wi-Fi Direct policy configured.....	Disabled
EAP-Passthrough.....	Disabled
CKIP	Disabled
Web Based Authentication.....	Disabled
Web Authentication Timeout.....	300
Web-Passthrough.....	Disabled
Mac-auth-server.....	0.0.0.0
Web-portal-server.....	0.0.0.0
Conditional Web Redirect.....	Disabled
Splash-Page Web Redirect.....	Disabled
Auto Anchor.....	Disabled
FlexConnect Local Switching.....	Disabled
FlexConnect Central Association.....	Disabled
flexconnect Central Dhcp Flag.....	Disabled
flexconnect nat-pat Flag.....	Disabled
flexconnect Dns Override Flag.....	Disabled
flexconnect PPoE pass-through.....	Disabled
flexconnect local-switching IP-source-guar....	Disabled
FlexConnect Vlan based Central Switching	Disabled
FlexConnect Local Authentication.....	Disabled
FlexConnect Learn IP Address.....	Enabled
Client MFP.....	Optional

PMF..... Disabled
 PMF Association Comeback Time..... 1
 PMF SA Query RetryTimeout..... 200
 Tkip MIC Countermeasure Hold-down Timer..... 60
 Eap-params..... Disabled
 Flex Avc Profile Name..... None
 Flow Monitor Name..... None
Split Tunnel Configuration
 Split Tunnel..... Disabled
 Call Snooping..... Disabled
 Roamed Call Re-Anchor Policy..... Disabled
 SIP CAC Fail Send-486-Busy Policy..... Enabled
 SIP CAC Fail Send Dis-Association Policy..... Disabled
 KTS based CAC Policy..... Disabled
 Assisted Roaming Prediction Optimization..... Disabled
 802.11k Neighbor List..... Disabled
 802.11k Neighbor List Dual Band..... Disabled
 802.11v Directed Multicast Service..... Disabled
 802.11v BSS Max Idle Service..... Enabled
 802.11v BSS Transition Service..... Disabled
 802.11v BSS Transition Disassoc Imminent..... Disabled
 802.11v BSS Transition Disassoc Timer..... 200
 802.11v BSS Transition OpRoam Disassoc Timer..... 40
 DMS DB is empty
 Band Select..... Disabled
 Load Balancing..... Disabled
 Multicast Buffer..... Disabled
 Universal Ap Admin..... Disabled

Mobility Anchor List

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

802.11u..... Disabled

MSAP Services..... Disabled

Local Policy

Priority Policy Name

Policy Configuration

L2ACL Configuration

ACL Configuration

CPU ACL Configuration

CPU Acl Name..... NOT CONFIGURED

Wireless Traffic..... Disabled

Wired Traffic..... Disabled

RADIUS Configuration

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Accounting Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Enabled
Keywrap..... Disabled
Fallback Test:
 Test Mode..... Passive
 Probe User Name..... cisco-probe
 Interval (in seconds)..... 300
MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages..... hyphen
RADIUS Authentication Framed-MTU..... 1300 Bytes

Authentication Servers

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

Accounting Servers

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

TACACS Configuration

Fallback Test:

Interval (in seconds) 0

Authentication Servers

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

Authorization Servers

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

Accounting Servers

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

LDAP Configuration

Local EAP Configuration

User credentials database search order:

Primary Local DB

Timer:

Active timeout 300

Configured EAP profiles:

EAP Method configuration:

EAP-FAST:

Server key	<hidden>
TTL for the PAC	10
Anonymous provision allowed	Yes
Authority ID	436973636f00000000000000000000000000000000
Authority Information	Cisco A-ID

Dns Configuration

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

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

Dns state..... Disable

Fallback Radio Shut configuration:

Fallback Radio Shut: Disabled

Arp-caching: Disabled

Subnet Broadcast Drop: Disabled

FlexConnect Group Summary

FlexConnect Group Summary: Count: 0

Group Name	# Aps
------------	-------

FlexConnect Group Detail

FlexConnect Vlan name Summary

Vlan-Name	Id	Status

FlexConnect Vlan Name Detail

Route Info

Number of Routes..... 0

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

Peer Route Info

Number of Routes..... 32555

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

Qos Queue Length Info

Platinum queue length..... 100

Gold queue length..... 75

Silver queue length..... 50

Bronze queue length..... 25

Qos Profile Info

Description.....	For Voice Applications	
Maximum Priority.....	voice	
Unicast Default Priority.....	voice	
Multicast Default Priority.....	voice	
Per-SSID Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0
Per-Client Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0
protocol.....	dot1p	
dot1p.....	5	
Description.....	For Video Applications	
Maximum Priority.....	video	
Unicast Default Priority.....	video	
Multicast Default Priority.....	video	
Per-SSID Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0
Per-Client Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0

protocol.....	dot1p	
dot1p.....	4	
Description.....	For Best Effort	
Maximum Priority.....	besteffort	
Unicast Default Priority.....	besteffort	
Multicast Default Priority.....	besteffort	
Per-SSID Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0
Per-Client Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0
protocol.....	dot1p	
dot1p.....	0	
Description.....	For Background	
Maximum Priority.....	background	
Unicast Default Priority.....	background	
Multicast Default Priority.....	background	
Per-SSID Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0
Per-Client Rate Limits.....	Upstream	Downstream
Average Data Rate.....	0	0
Average Realtime Data Rate.....	0	0
Burst Data Rate.....	0	0
Burst Realtime Data Rate.....	0	0

protocol.....	dot1p
dot1p.....	1

Mac Filter Info

Authorization List

Authorize MIC APs against Auth-list or AAA	disabled
Authorize LSC APs against Auth-List	disabled
APs Allowed to Join	

AP with Manufacturing Installed Certificate....	yes
AP with Self-Signed Certificate.....	no
AP with Locally Significant Certificate.....	no

Load Balancing Info

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

Statistics (client-count based)

Total Denied Count.....	0 clients
Total Denial Sent.....	0 messages
Exceeded Denial Max Limit Count.....	0 times

None 5G Candidate Count..... 0 times
None 2.4G Candidate Count..... 0 times

Statistics (uplink-usage based)

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

DHCP Info

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

DHCP Proxy Behaviour: disabled

Exclusion List ConfigurationUnable to retrieve exclusion-list entry

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

CDP Configuration

cdp version v2

Country Channels Configuration

Configured Country..... US - United States

KEY: * = Channel is legal in this country and may be configured manually.

A = Channel is the Auto-RF default in this country.

. = Channel is not legal in this country.

C = Channel has been configured for use by Auto-RF.

x = Channel is available to be configured for use by Auto-RF.

(-, -) = (indoor, outdoor) regulatory domain allowed by this country.

-----:+++-+-+--+-+---+-+--+-----

802.11bg ::

Channels : 1 1 1 1 1
 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4

Channels : 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2

-----:+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+----+

WPS Configuration Summary

Auto-Immune

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

Client Exclusion Policy

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

Signature Policy

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

Management Frame Protection

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

	WLAN	Client	
WLAN ID	WLAN Name	Status	Protection
-----	-----	-----	-----

1	IP_Dev No Encryption	Disabled	Optional but inactive (WPA2 not configured)
2	IP_Dev All WPA/WPA2 PSK	Enabled	Optional

Custom Web Configuration

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

Configuration Per Profile:

Core dump Configuration

Core Dump upload is disabled

Rogue AP Configuration

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

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

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

Rogue AP RLDP Configuration

Rogue Location Discovery Protocol..... Disabled

RLDP Schedule Config..... Disabled
RLDP Scheduling Operation..... Disabled
RLDP Retry..... 1

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

Rogue Auto Contain Configuration

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

Adhoc Rogue Configuration

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

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

Rogue Client Configuration

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

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

Ignore List Configuration

MAC Address

Rogue Rule Configuration

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

Media-Stream Configuration

Multicast-direct State..... disable

Allowed WLANs.....

Stream Name Operation Status	Start IP	End IP
---------------------------------	----------	--------

URL.....

E-mail.....

Phone.....

Note.....

State..... disable

2.4G Band Media-Stream Configuration

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

5G Band Media-Stream Configuration

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

Number of Clients..... 0

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

WLC Voice Call Statistics

WLC Voice Call Statistics for 802.11b Radio

WMM TSPEC CAC Call Stats

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

SIP CAC Call Stats

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

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

WLC 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
Num of Calls Rejected due to PHY rate..... 0
Num of Calls Rejected due to QoS policy..... 0

SIP CAC Call Stats

Total Num of Calls in progress..... 0
Num of Roam Calls in progress..... 0
Total Num of Calls Admitted..... 0
Total Num of Roam Calls Admitted..... 0
Total Num of Preferred Calls Received..... 0
Total Num of Preferred Calls Admitted..... 0
Total Num of Ongoing Preferred Calls..... 0

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

WLC IPv6 Summary

Global Config..... Enabled
Reachable-lifetime value..... 300
Stale-lifetime value..... 86400
Down-lifetime value..... 30
RA Throttling..... Disabled
RA Throttling allow at-least..... 1
RA Throttling allow at-most..... 1
RA Throttling max-through..... 10
RA Throttling throttle-period..... 600
RA Throttling interval-option..... passthrough
NS 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 _universal._sub._ipp._tcp.local.	No	All	0	
HP_Photosmart_Printer_2	No	All	0	_cups._sub._ipp._tcp.local.
HomeSharing	No	All	0	_home-sharing._tcp.local.
Printer-IPP	No	All	0	_ipp._tcp.local.
Printer-IPPS	No	All	0	_ipps._tcp.local.
Printer-LPD	No	All	0	_printer._tcp.local.
Printer-SOCKET	No	All	0	_pdl-datastream._tcp.local.

* -> If access policy is enabled LSS will be ignored.

mDNS service-group Summary

Access Policy Status..... Disabled

Total number of mDNS Policies..... 1

Number of Admin configured Policies..... 1

Sl No Origin	Service Group Name	Description
-----------------	--------------------	-------------

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

mDNS profile detailed

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

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

mDNS AP Summary

Number of mDNS APs..... 0

PMIPv6 Global Configuration

PMIPv6 Profile Summary

No Profile Created.

PMIPv6 MAG Statistics

PMIPv6 domain has to be configured first

EoGRE Global Configuration

Heartbeat Interval..... 60

Max Heartbeat Skip Count..... 3

Interface..... management

EoGRE Gateway Configuration

EoGRE Domain Configuration

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

EoGRE Profile Configuration

WLAN Express Setup Information.

WLAN Express Setup - False

Flex Avc Profile summary.

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

Flex Avc Profile Detailed Configuration.

Certificate Summary.

Web Administration Certificate..... 3rd Party

Web Authentication Certificate..... Locally Generated

Certificate compatibility mode:..... off

Lifetime Check Ignore for MIC Disable

Lifetime Check Ignore for SSC Disable

Smart-licensing status Summary.

Call-home Summary.

Hotspot Icon Summary.

Unable to find Icon directory in flash.

Coredump Summary

Core Dump upload is disabled

Memory Summary

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

System Name:wlc Primary SW Ver:8.2.111.0

Current Time:Thu Aug 18 20:06:33 2016 System UP Time:6 days 3 hrs 49 mins 39 secs

NAME: "Chassis" , DESCRIPTOR: "Cisco Wireless Controller"

PID: AIR-CTVM-K9, VID: V01, SN: 96NTPERK0A6

Total System Memory.....	(2057560	KB)	2009 MB
Total System Free Memory.....	(909360	KB)	888 MB (44 %)
Total Memory in Buffers.....	(1104	KB)	
Total Memory in Cache.....	(266564	KB)	260 MB
Total Active Memory.....	(511540	KB)	499 MB
Total InActive Memory.....	(238112	KB)	232 MB
Total Memory in Anon Pages.....	(481984	KB)	470 MB
Total Memory in Slab.....	(11004	KB)	10 MB
Total Memory in Page Tables.....	(2748	KB)	2 MB
WLC Peak Memory.....	(1402280	KB)	1369 MB
WLC Virtual Memory Size.....	(1383912	KB)	1351 MB
WLC Resident Memory.....	(506340	KB)	494 MB
WLC Data Segment Memory.....	(1318240	KB)	1287 MB
Total Heap Including Mapped Pages.....	(399115	KB)	389 MB
Total Memory in Pmalloc Pools.....	(350174	KB)	341 MB
Total Used Memory in Pmalloc Pools.....	(324913	KB)	317 MB
Total Free Memory in Pmalloc Pools.....	(16706	KB)	16 MB

----- Pmalloc Pools Information -----

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

9 Raw-Pool 0 524 290800 /290800 /0

----- MBUF Information -----

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

Mesh Configuration

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

Mesh Security

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

Mesh Alarm Criteria

Max Hop Count..... 4
Recommended Max Children for MAP..... 10
Recommended Max Children for RAP..... 20

Low Link SNR.....	12
High Link SNR.....	60
Max Association Number.....	10
Association Interval.....	60 minutes
Parent Change Numbers.....	3
Parent Change Interval.....	60 minutes
Mesh Multicast Mode.....	In-Out
Mesh CAC Mode.....	enabled
Mesh Full Sector DFS.....	enabled
Mesh Ethernet Bridging VLAN Transparent Mode.....	enabled
Mesh DCA channels for serial backhaul APs.....	disabled
Outdoor Ext. UNII B Domain channels(for BH).....	disabled
Mesh Advanced LSC.....	disabled
Advanced LSC AP Provisioning	disabled
Open Window.....	disabled
Provision Controller.....	disabled
Mesh Slot Bias.....	enabled
Mesh Convergence Method.....	standard
Mesh Channel Change Notification.....	disabled
Mesh Ethernet Bridging STP BPDU Allowed.....	disabled
Mesh RAP downlink backhaul.....	802.11Radio-A (Slot 1)

Appendix B Sample Pump Configuration Parameters

```
SN=2011304

# Pump serial number - must match SN of receiving pump

# SIGMA Spectrum Settings

[NETWORK CONFIGURATION]

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

DHCP=1

IP=

GATEWAY=

NETMASK=

DNS=

# Leave either SIGMAGW or MULTICAST blank
# SIGMAGW set to DNS name or IP address of SIGMA gateway server
SIGMAGW=192.168.140.165

# MULTICAST group default is 239.237.12.87

MULTICAST=

# DEVICEID set to device alias
# Limited to 20 alpha-numeric characters (0-1,A-Z,a-z), blank is acceptable
DEVICEID=000345

[WIFI CONFIGURATION]

# BSS=0 Infrastructure mode (Access point)
# BSS=1 Join or Create Ad-Hoc (peer-to-peer)
# BSS=2 Join only Ad-Hoc (peer-to-peer)
# BSS=3 Join any

BSS=0

# SSID= set to wireless network name
SSID=IP_Dev_Cert

# 802.11 Mode - 'b', 'g', and/or 'a'
802.11b=1
802.11g=1
```

```
802.11a=1

# CHANNEL=0 search channels
CHANNEL=0

# SECURITY=0 Any available security method
# SECURITY=1 Open system (no-encryption)
# SECURITY=2 WEP shared key
# SECURITY=3 WPA pre-shared key
# SECURITY=4 WPA with 802.1x authentication
# SECURITY=5 WEP with 802.1x authentication
# SECURITY=6 LEAP
# SECURITY=7 EAP-FAST
SECURITY=4

# WEPKEYINDEX=0-3
WEPKEYINDEX=0

# WEPKEY may be blank or 10 (64-bit) or 26 (128-bit) hex (0-1 and a-f)
characters long
WEPKEY=

# WPAENCRYPTION=0 Any
# WPAENCRYPTION=1 WEP
# WPAENCRYPTION=2 TKIP
# WPAENCRYPTION=3 CCMP (AES)
# WPAENCRYPTION=4 Open (no encryption)
WPAENCRYPTION=3

# WPAPSK must be blank if WPA PSK is not used
# WPAPSK may 64 hex (0-1 and a-f) characters long to specify a PSK
# WPAPSK may be 8-63 ascii characters long to specify a passphrase
WPAPSK=

# 802.1X/EAP Authentication method
# Set one, or more, authentication methods to 1 to enable them, all others
should be 0
LEAP=0

PEAP/MSCHAPv2=0
```

```
EAP-TLS=1
EAP-FAST=0
# IDENTITY= 802.1X Identity (username)
IDENTITY=BaxterCert
# PASSWORD= 802.1X Password
PASSWORD=
# Certificate information follows, required for authentication modes that use a
certificate.
# All certificates and private keys must be PEM format (base64 encoded).
# Client certificate, both cert and private key are required.
# Certificate and key information is not output for security reasons.
# Certificate information is radio specific, so the MAC address of the Wireless
Battery Module
# of the attached, or soon to be attached module must match.
# If the certs or keys required a password, it should be specified in the 802.1x
PASSWORD field above.
# The MAC address specified below must match the module connected to the pump.
MAC=00:40:9d:66:db:45
CLIENTCERT=

-----BEGIN RSA PRIVATE KEY-----
MIIEcjCBQgIBAAKCAQEAEuhKvGS9womnF7tmM1IOWuzbvMct7u+TDYtoQSNEitAYe5Bjr
XR+tQOT/2b08nJUjVN191/+3t2i9qUDDU58DTKKir9dmR5ridHlaIyhts8fB7h2a
rZ74YK+4/A1C2mNpmwqwDQlwWhJzJgSe5XeZF0ALTdS3LEggwpuPb6Eo2Wbnqwr0
/tbsRvaeEjwcIGowmuy1v8TkrbSKef9I4B54Pcl3KsbnnUjh7JIV9h/OnyrOKi
z2P+3maogCnOwxRQp79j/IgCS3JbUBMG14gKnxorJgLuBovqpsWIY06k/qohIpyg
Vevc0UUj8XiYEu1ldT1SCXYke/I9jauLBB6OQIDAQABoIBAHjnwmw7qXG2r/Qju
IywTNOYBE/tvFL9KLgsVVm96NOp0762W45hm9NST9/ErnS7BWWvQxoyLhHyQemx3
wHOdZy9snf1UJQlyAqNcFs2xf1bJ/aETa2ZVXV61z6U3mLD+16f+kdZmw7JDOr8B
UZ4Y0EjjPHUeOsdzNpY9Lj6CoWBg+v3+TEo3WCqHsqHN8yoVKP30Xnfb1JMgRLf/
infhI6Qg6QKBM++vWQj1UYuM4hbQtQ6HmwWv2epu8YHFdmm3jTSrv+W81BbY2N5D
N9tZsdUJ54NHiVZTjVmAXCxSpBp3+yTOMRpznzgW0v8MLMhFanjIC5QypG712HIQx
```

gk7LZGECgYEA4vB26UpZNxsOlgzcEQP8fQ82Dk5xNjb9e7qDSD85LUppR6F4xwNs
QPyFVYRemb+pQyIwn1X2SNAdRvsDwSsFVTv9ENi1PzlHbOfaBWE9/VNMaz8vCjfr
teC3So6bIW1lHNeoOl8d1wrTOtGZFENH/H4DoOBC7U0aoYjvtnYBplMCgYEA0eaJ
mITPESmZRZI8kaCb/TrWLTzmH2SOCPgC/qVmJ2FiQ8iT3KJXJ5d8ophY84Kay4le
axVUUgIdKNyvNrf038Rx0DirN+qznSKPJUmdY+tnCxaXBjTj/tSwkeiNamZOXHeH
boVlReX6ONDvT+u9MkvMxDmhwb9G4izw26a88MCgYAhqyFJLTGdPlNkqZXApIHC
IA6aAsNDEtd6kspFXrPh50dFTEx54iUeYxh4/oF2d/vprNnf2cYHOXEohdEhyHsr
EBt082G4dowFOUScRbgHrGMLCj21W2SKAEPROOUFCPjqVYhs2I25yK5b7Jq0aeL1
L9Dj/kGPqT/JNWkzBEDsZwKBgQDFnt5BN0d20Kb5/xR5n3Xwz788a8g35rqtiplt
uOnqRk2Vcne67a0FvgeUnZ+17BiU9FSKOFgpVWMgaXkW6HBjbqehBB2bRCHOmhH2
b53Fq//9IxRy+G7f1+busJluRwGJT6Un6p3kttgLwgQAC3aQMzgJhjy7xt25aQ+9
p8ZfEQKBgB6jQAT31FxvPFHyjU4NdFeogJd2c2nFbkC7aqOEPKNG9Nbzn/vVWh7x
Rx7Axua3D2OYrCH7V1NcR9X1dInpyj/hYXc5/VdtLZ2yhEc2GiG/jfgNWk2W2Bzd
2NLf54bgV671kC2yKMK/5wBru+v73WmqvWfQ4KsMesLLBBzMRvJa
-----END RSA PRIVATE KEY-----

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

MIIFWzCCBEoGAwIBAgIQAr0FxourLR0mLxVp3m/RJzANBgkqhkiG9w0BAQsFADBX
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUN1cnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWN1cnQuY29tMTAwLgYDVQQDEydEaWdpQ2VydCBUZXN0IEludGVybWVk
aWF0ZSBsb290IENBIFNIQTiWHzcNMTcwMzE1MDAwMDAwWhcNMTgwMzE1MTiWMDAw
WjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk1EMRIwEAYDVQQHEwlSb2Nrdmls
bGUxNzA1BgNVBAoTLk5hdGlvbmFsIEluc3RpdtHV0ZSBvZiBTdGFuZGFyZHMgYW5k
IFR1Y2hub2xvZ3kxDjAMBgNVBAsTBU5DQ29FMQ8wDQYDVQQDEwZCYXh0ZXIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6Eq8ZL3CiacXu2YzUg5a7Nu8x
y3u75MNi2hBI0SK0Bh7kG0tdH61A5P/ZvTyclsNU2X3X/7e3aL2pQMNTnwNMoqKv
12ZHmuJ0eVojKG2zx8HuHzqtvhgr7j8DULaY2mbCrANCXBaEnMmBJ7ld5kXQAtN
1LcsSCDCm49voSjZZuerCvT+1uxG9p4SPBwgY7Ca7LW/xOSTtIp4W30jgHng9yXc
qzFuedSMfskhX2H/SfKs4qLPY/7eZqiAKc7DFFCnv2P8iAJLcltQEwbXiAqfGism
Au4Gi+qmxYhg7qt+qiEinKBV69zRRSPxeLIS6fWV1PVIJdiR78j2Nq4sEHo5AgMB
AAGjggHVMIIBoTAFBgNVHSMEGDAwgbSJvf2JvOIQPPTtTh8w+fmCi1xh4jAdBgNV
HQ4EFgQU3PsIuQqjWZ2eFYrcKNhdYi7Rf1owEQYDVR0RBAAowCIIGQmF4dGVyMA4G

```
A1UdDwEB/wQEAwIFoDAdBgNVHSUEfjAUBggrBgfFBQcDAQYIKwYBBQUHAWIwgZUG
A1UdHwSBjTCBijBDoEGgP4Y9aHR0cDovL2NybDN0ZXN0LmRpZ2ljZXJ0LmNvbS9E
aWdpQ2VydFRlc3RJbnR1cm11ZGlhdGVTSEEyLmNybDBDoEGgP4Y9aHR0cDovL2Ny
bDN0ZXN0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFRlc3RJbnR1cm11ZGlhdGVTSEEy
LmNybDAhBgNVHSAEGjAYMAwGCMCGSAGG/WxjAQEwCAYGZ4EMAQICMIGDBggrBgfEF
BQcBAQR3MHUwKAYIKwYBBQUHMAKGPh0dHA6Ly9vY3NwdGVzdc5kaWdpY2VydC5j
b20wSQYIKwYBBQUHMAKGPh0dHA6Ly9jYWN1cnRzLmRpZ2ljZXJ0LmNvbS9EaWdp
Q2VydFRlc3RJbnR1cm11ZGlhdGUTU0hBMi5jcnQwDAYDVR0TAQH/BAIwADANBgkq
hkiG9w0BAQsFAAACQAe7Rc6PbIfEjSQpCZ3UpZ7zqWruov44nmSKvR/X4MJITM
z9k3S+TzGOGYnq7bHBF1mjLt015K/BDWSG6LY5c1SYJuGCbC/dSNFk9G+lzBKs5S
5xJxk8HeAt4OHOWmtEhZ7S4np7zUBcRu1koHbw4vW/1YJBvxRF1Sdd0ypyBP4X81
D2mX+LmFo2rlSExurr5rd1s6Pna2FRBEjoyM78ID9AmKENqeioDi+hxGL1QROOT
y7azU8yWcec7nad9iUGO/pMDdhbWexpvp4CBihxYkUMQcf8RaqTkJM8fLAdvPq9P
oQuBuMi+qPtI3WkTgfwr49usBzgbrdNPc/5MRQEz8Q==

-----END CERTIFICATE-----
```

```
# Client certificate expiration date, GMT in the format: MM/DD/YYYY HH:MM:SS.
CLIENTCERTEXPIRE=
# Trusted certificates, maximum of 5.
TRUSTEDCERTS=
```

```
-----BEGIN CERTIFICATE-----
MIIGSTCCBTGgAwIBAgIEM6qqqjANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQGEwJV
UzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWN1cnQu
Y29tMSMwiQYDVQQDExpEaWdpQ2VydCBUZXN0IFJvb3QgQ0EgU0hBMjAeFw0wNjEx
MTAwMDAwMDBaFw0zMTExMTAwMDAwMHExCzAJBgNVBAYTA1VTMRUwEwYDVQQK
EwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5jb20xMDAuBgNV
BAMTJ0RpZ2lDZXJ0IFRlc3QgSW50ZXJtZWpYXR1IFJvb3QgQ0EgU0hBMjCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJiahU+gQ8Brmcov1LwvynLKgxMc
buqjeyYeIDEUXtTEJKoPm1Pc5YE39fBY1ydwabJ6k3LbLZM+zqw2pCXwaf4LBhLv
t4ppHMfXlgI2IVpWibSYVcvJ4waD09AQ47u/SQhDHSVf17HRUIs1tIw+MMpMyGH0
9YzgI/ZI5KTWBBy+nlnz9t1/RpPdcJfAWin3T/s7xNu364OFDURX+3Rxb7bVnV1xI
```

GZUwQx23GGcSnypsflr1rBc2yvXaUnwl4DbQMUo10tdZtd1wZNQE3C1L3MXndvn0
WdFB4cM6kQ1Sky0RFW+TJqQIMmb29n09P/ez7Ipo0cpV3vlBAC0DWm2z/FMCAwEA
AaOCAvQwggLwMA4GA1UdDwEB/wQEAvIBhjCCAcYGA1UdIASCAb0wggG5MIIBtQYL
YIZIAyB9bAEDAAIwggGkMDoGCCsGAQUFBwIBFi5odHRwOi8vd3d3LmRpZ21jZXJ0
LmNvbS9zc2wtY3BzLXJ1cG9zaXRvcnkuahRtMIIBZAYIKwYBBQUHAgIwggFWHoIB
UgBBAG4AeQAgAHUAcwB1ACAAbwBmAACAdABoAGkAcwAgAEMAZQByAHQAAQBmAGkA
YwBhAHQAZQAgAGMAbwBuAHMAdABpAHQAdQB0AGUAcwAgAGEAYwbjAGUAcAB0AGEA
bgBjAGUAIAbVAGYAIAB0AGgAZQAgAEQAAQbnAGkAQwB1AHIAdAAgAEMAUAAvAEMA
UABTACAAYQBuAGQAIAB0AGgAZQAgAFIAZQBsAHkAaQBuAGcAIABQAGEAcgB0AHkA
IABBAGcAcgB1AGUAbQB1AG4AdAAgAHcAaABpAGMAaAAGAGwAaQbtAGkAdAAgAGwA
aQBhAGIAaQBsAGkAdAB5ACAAYQBuAGQAIABhAHIAZQAgAGkAbgBjAG8AcgBwAG8A
cgBhAHQAZQBkACAAaAb1AHIAZQBpAG4AIAbiAHkAIAbYAGUAZgB1AHIAZQBuAGMA
ZQAUmA8GA1UdEwEB/wQFMAMBAf8wOAYIKwYBBQUHAQEELDAqMCgGCCsGAQUFBzAB
hhxodHRwOi8vb2NzchR1c3QuZGlnaWN1cnQuY29tMIGIBgNVHR8EgYAwfjA9oDug
OYY3aHR0cDovL2NybdN0ZXN0LmRpZ21jZXJ0LmNvbS9EaWdpQ2VydFR1c3RSb290
Q0FTSEEyLmNybdA9oDugOYY3aHR0cDovL2NybdR0ZXN0LmRpZ21jZXJ0LmNvbS9E
aWdpQ2VydFR1c3RSb290Q0FTSEEyLmNybdAAdBgNVHQ4EFgQUiVX9ibziEDz7bU4f
MPn5gotcYeIwHwYDVR0jBBgwFoAU9kZ+Gxa7N5ljq9z/YhSzkyepYDx4wDQYJKoZI
hvcNAQELBQADggEBALFxPxkcHgaXBuoZ10FGWsq3bybGnxC611fDETcWVrPajudx
asm8EXOTSVnqKNIXZT1m1BY0chhnVGA3YyNN7XF7XrT1HtRH5NDhWO21zFEGSFLw
hlCiGQBuzKOelbBWdhpn7icm+Y/u+DPaK6oFu0tX/u9kPzoc8OYSBe412sHAD1/1
kUDPAEO4yHSxDnoe0fhk24/yCuO6Wc+mMe7YXzEkq8pOEWjNw/9E1dsP20L7jD3F
97q5uVNelwEaeE3U5Eq1xKUBdyQqitinpTv/yo/UPTDLpfjBmK2nh2HK6r0RH+YC
OicqQ99N+q6YeAlhejLa7+7FkKYKK1YEAbE1Icc=

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

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

MII DpjCCAo6gAwIBAgIBMzANBgkqhkiG9w0BAQsFADBkMQswCQYDVQQGEwJVUzEV
MBMGA1UEChMMRGlnaUN1cnQgSW5jMRkwFwYDVQQLExB3d3cuZGlnaWN1cnQuY29t
MSMwIiQYDVQQDEXpEaWdpQ2VydCBUZXN0IFJvb3QgQ0EgU0hBMjAeFw0wNjExMTAw
MDAwMDBaFw0zMTExMTAwMDAwMDBaMGQxCzAJBgNVBAYTA1VTMRUwEwYDVQQKEwx
aWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5jb20xIzAhBggNVBAMT

GkRpZ21DZXJ0IFRlc3QgUm9vdCBDQSBTSEEyMIIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIIBCgKCAQEA0DLGgpMXqI2YZ15ULS61yqyqiBMpmRtM9/w/1pquoA/GEri19
VMFuvtPTWgu9IQf0dQsRMy2d8V4INSj43YyQeXnxPzanTSqza95yoH/h4xUM/pNq
AlXl08c+cYMyCDzTQ0vrEWcvPZOtXYABac9E9ceT015RdD5pORjMwTcb6NxydZr8
nRd9/J66L4R17IKvTU74IwA6fwNd0UnXbhVhGdeEAe+eIEvJ5WlWxDeS6ZdZuSzv
h24QxhxpuctzSq81HHChw4a1kOel2oql1UY698atS0nxfw3IR30heQ/g793Mce9
SX9u2dPPAZtSaW8/38TwKbNOa9zkRFn7oF+cZQIDAQABo2MwYTAOBgNVHQ8BAf8E
BAMCAYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU9kZ+Gxa7N51j9z/YhSz
yepYDx4wHwYDVR0jBBgwFoAU9kZ+Gxa7N51j9z/YhSzkyepYDx4wDQYJKoZIhvcN
AQELBQADggEBAAeQacFm1sFPOIEvXDVi3IH2RKF7he0p/M0bK2Soj137LMf+ctpM
3bFKJPY97YIE0g7T1ggR8TN2sK0moumMTPjWCdFWJyN4yakS6tPIWEG2XobJ9H1r
iuVXLKd2M/1yhqUyt1o5KtbOGQQLFd3qdp4A1tcXuK2wyMTiSCYS3Uow61JdEw6M
eyrMIpZ19GtvaXTz6Ldn0zAbhKC7bVUy7ob0T4E03fQ8hIQCNPupvY7Db1/XmIw8
QWVd6AOH7EE3P8xbWovcTWZ5XbstWY014GeJFXZ7YreaAg8sYa6CzasuHkr/rxeZ
8yzOmCTTSPk5Ju5bTfAyEpgk15fDvntJQg=

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

Appendix C Acronyms

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

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

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

Appendix D References

- [1] J. Moy, *OSPF Version 2*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 2328, April 1998. <https://www.ietf.org/rfc/rfc2328.txt> [accessed 2/7/18].
- [2] *Cisco Adaptive Security Virtual Appliance (ASA) Quick Start Guide*, 9.6, Cisco [Web site], <http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asav/quick-start/asav-quick/intro-asav.html> [accessed 2/7/18].
- [3] D. Bider and M. Baushke, *SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 6668, July 2012. <https://tools.ietf.org/html/rfc6668> [accessed 2/7/18].
- [4] J. Postel, *Internet Control Message Protocol: DARPA Internet Program Protocol Specification*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 792, September 1981. <https://tools.ietf.org/html/rfc792> [accessed 2/7/18].
- [5] J. Case, M. Fedor, M. Schoffstall, and J. Davin, *A Simple Network Management Protocol (SNMP)*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 1157, May 1990. <https://tools.ietf.org/html/rfc1157> [accessed 2/7/18].
- [6] R. Droms, *Dynamic Host Configuration Protocol*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 2131, March 1997. <https://www.ietf.org/rfc/rfc2131.txt> [accessed 2/7/18].
- [7] Institute of Electrical and Electronics Engineers (IEEE), *Bridges and Bridged Networks*, IEEE 802.1Q, 2014. <http://www.ieee802.org/1/pages/802.1Q-2014.html> [accessed 2/7/18].
- [8] *Catalyst 3650 Switch Getting Started Guide*, Cisco [Web site], http://www.cisco.com/c/en/us/td/docs-switches/lan/catalyst3650/hardware/quick-guide/cat3650_gsg.html [accessed 2/7/18].
- [9] Institute of Electrical and Electronics Engineers (IEEE), *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements*, 802.11i, 2004. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1318903> [accessed 2/7/18].

- [10] *Virtual Wireless LAN Controller Deployment Guide 8.2*, Cisco [Web site], http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Virtual_Wireless_LAN_Controller_Deployment_Guide_8-2.html [accessed 2/7/18].
- [11] D. Mills, J. Martin, Ed., J. Burbank, and W. Kasch, *Network Time Protocol Version 4: Protocol and Algorithms Specification*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 5905, June 2010. <https://www.ietf.org/rfc/rfc5905.txt> [accessed 2/7/18].
- [12] U.S. Department of Commerce. *Announcing the Advanced Encryption Standard (AES)*, Federal Information Processing Standards (FIPS) Publication 197, November 2001. <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf> [accessed 2/7/18].
- [13] *Cisco Wireless Controller Configuration Guide, Release 8.0*, Cisco [Web site], http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80.html [accessed 2/7/18].
- [14] D. Simon, B. Aboba, and R. Hurst, *The EAP-TLS Authentication Protocol*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 5216, March 2008. <https://www.ietf.org/rfc/rfc5216.txt> [accessed 2/7/18].
- [15] C. Rigney, S. Willens, A. Rubens, and W. Simpson, *Remote Authentication Dial In User Service (RADIUS)*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 2865, June 2000. <https://tools.ietf.org/html/rfc2865> [accessed 2/7/18].
- [16] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 6960, June 2013. <https://tools.ietf.org/html/rfc6960> [accessed 2/7/18].
- [17] *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 MP1 Planning and Deployment Guide*, Symantec [Web site], http://help.symantec.com/cs/DCS6.7/DCS6_7/v118490468_v110163010/Installing-Data-Center-Security:-Server-Advanced-6.7-or-6.7-MP1/?locale=EN_US [accessed 2/7/18].