# **NIST SPECIAL PUBLICATION 1800-24**

# Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector

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

Jennifer Cawthra Bronwyn Hodges Jason Kuruvilla\* Kevin Littlefield Bob Niemeyer Chris Peloquin Sue Wang Ryan Williams Kangmin Zheng

\*Former employee; all work for this publication done while at employer.

FINAL

This publication is available free of charge from: <u>https://doi.org/10.6028/NIST.SP.1800-24</u>

The first draft of this publication is available free of charge from: <u>https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-</u> 24-practice-guide





# Securing Picture Archiving and Communication System (PACS):

## Cybersecurity for the Healthcare Sector

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

> Jennifer Cawthra National Cybersecurity Center of Excellence National Institute of Standards and Technology

> > Bronwyn Hodges Jason Kuruvilla\* Kevin Littlefield Bob Niemeyer Chris Peloquin Sue Wang Ryan Williams Kangmin Zheng The MITRE Corporation McLean, Virginia

\*Former employee; all work for this publication done while at employer.

FINAL

December 2020



U.S. Department of Commerce Wilbur Ross, Secretary

National Institute of Standards and Technology Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

# **NIST SPECIAL PUBLICATION 1800-24A**

# Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector

Volume A: Executive Summary

#### **Jennifer Cawthra**

National Cybersecurity Center of Excellence National Institute of Standards and Technology

Jason Kuruvilla\* Kevin Littlefield Bob Niemeyer Sue Wang Ryan Williams Kangmin Zheng The MITRE Corporation McLean, Virginia

\*Former employee; all work for this publication done while at employer.

December 2020

**FINAL** 

This publication is available free of charge from <a href="https://doi.org/10.6028/NIST.SP.1800-24">https://doi.org/10.6028/NIST.SP.1800-24</a>

The first draft of this publication is available free of charge from <a href="https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-24-practice-guide">https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-24-practice-guide</a>





# **Executive Summary**

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to emulate a medical imaging environment, performed a risk assessment, and identified controls from the NIST Cybersecurity Framework to secure a medical imaging ecosystem. This project used picture archiving and communication system (PACS) and a vendor neutral archive (VNA) and implemented controls to safeguard medical images from cybersecurity and privacy threats. PACS and a VNA, hereafter referred to as PACS, comprise the systems to centrally manage medical imaging data. This effort resulted in a NIST Special Publication 1800 series Cybersecurity Practice Guide, based on the following considerations relative to PACS:

- PACS allows for the acceptance, transfer, display, storage, and digital processing of medical images. PACS centralizes functions surrounding medical imaging workflows and serves as an authoritative repository of medical image information. Medical imaging is a critical component in rendering patient care. PACS serves as the repository to manage these images and accompanying clinical information within a healthcare delivery organization (HDO).
- PACS fits within a highly complex HDO environment that includes back-office systems, electronic health record systems, and pharmacy and laboratory systems, as well as an array of electronic medical devices. This environment may include cloud storage for medical images. In managing these systems, HDOs work with a diverse group of individuals who interact with the enterprise information technology (IT) infrastructure and may include IT operations staff, internal support teams, and biomedical engineers, as well as vendors and manufacturers.
- Securing PACS presents several challenges. Various departments operating in the HDO have unique medical imaging needs and may operate their own PACS or other medical imaging archiving systems. Further, HDOs may use external medical imaging specialists when reviewing patient medical data. The PACS ecosystem, therefore, may include multiple systems for managing medical imaging data, along with a diverse clinical user community, accessing PACS from different locations. This complexity leads to cybersecurity challenges.
- PACS may have vulnerabilities that, given its central nature, may impact an HDO's ability to render patient care or to preserve patient privacy. These vulnerabilities could impede patients' timely diagnosis and treatment if medical images are altered or misdirected. These vulnerabilities could also expose an HDO to risks of significant data loss, malware and ransomware attacks, and unauthorized access to other parts of an HDO enterprise network.
- This NIST Cybersecurity Practice Guide demonstrates how organizations can securely configure and deploy PACS. This guide presents an example solution that helps HDOs improve medical imaging ecosystem privacy and cybersecurity.

## CHALLENGE

PACS, by its nature, is a system that cannot operate in isolation. The overall PACS ecosystem consists of diverse technologies that include medical imaging devices, patient registry systems, and worklist management systems. PACS also relies on systems to manage and maintain medical image archives, which may include cloud storage capabilities. The primary role of PACS is interaction with disparate medical imaging devices, interconnectivity with other clinical systems, and allowing a geographically and organizationally diverse team of healthcare professionals to review medical images to provide quality

and timely patient care. Therefore, the threat landscape is broad, and allows for a large attack surface. The PACS environment may include vulnerabilities. Unauthorized individuals may leverage vulnerabilities and compromise or corrupt stored information. Also, unauthorized individuals may use components found in the PACS ecosystem as pivot points to further compromise components in an integrated healthcare information system.

## **SOLUTION**

This practice guide demonstrates how an organization may implement a solution to mitigate identified cybersecurity and privacy risks. The reference architecture features technical and process controls to implement:

- a defense-in-depth solution, including network zoning that allows more granular control of network traffic flows and limits communications capabilities to the minimum necessary to support business function
- access control mechanisms that include multifactor authentication for care providers, certificate-based authentication for imaging devices and clinical systems, and mechanisms that limit vendor remote support to medical imaging components
- a holistic risk management approach that includes medical device asset management, augmenting enterprise security controls, and leveraging behavioral analytic tools for near realtime threat and vulnerability management in conjunction with managed security solution providers

The NCCoE sought existing technologies that provided the following capabilities:

- role-based access control
- microsegmentation
- behavioral analytics
- data security
- cloud storage

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, *Securing Picture Archiving and Communication Systems*, can help your organization:

- improve resilience in the network infrastructure, including limiting a threat actor's ability to leverage components as pivot points to attack other parts of the HDO's environment
- limit unauthorized movement within the HDO environment by authorized system users to address the "insider threat" as well as limit unauthorized actors once they gain network access

- analyze behavior and detect malware throughout the ecosystem to enable HDOs to determine when components evidence compromise and to enable those organizations to limit the effects of a potential advanced persistent threat such as ransomware
- secure sensitive data (e.g., personally identifiable information or protected health information) at rest, in transit, and in cloud environments; enhancing patient privacy by limiting malicious actors' ability to exfiltrate or expose that data
- consider and address risks that may be identified as HDOs examine cloud storage solutions as part of managing their medical imaging infrastructure

### **SHARE YOUR FEEDBACK**

You can view or download the guide at <u>https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs</u>. 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 <u>hit\_nccoe@nist.gov</u>.

## **COLLABORATORS**

Collaborators 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). Those respondents with relevant capabilities or product components 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 NCCoE, a part of 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, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology.

#### LEARN MORE

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

# **NIST SPECIAL PUBLICATION 1800-24B**

# Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector

Volume B: Approach, Architecture, and Security Characteristics

#### **Jennifer Cawthra**

National Cybersecurity Center of Excellence National Institute of Standards and Technology

Bronwyn Hodges Jason Kuruvilla\* Kevin Littlefield Bob Niemeyer Chris Peloquin Sue Wang Ryan Williams Kangmin Zheng The MITRE Corporation McLean, Virginia

\*Former employee; all work for this publication done while at employer.

December 2020

#### **FINAL**

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-24

The first draft of this publication is available free of charge from: <u>https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-</u> <u>24-practice-guide</u>





#### **DISCLAIMER**

Certain commercial entities, equipment, products, or materials may be identified by name of 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.

National Institute of Standards and Technology Special Publication 1800-24B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-24B, 102 pages, (December 2020), 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 <u>hit\_nccoe@nist.gov</u>.

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

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

## 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 information technology security—the NCCoE applies standards and best practices to develop modular, 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 Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

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

## NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) 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 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 imaging plays an important role in diagnosing and treating patients. The system that manages medical images is known as the picture archiving communication system (PACS) and is nearly ubiquitous in healthcare environments. PACS is defined by the Food and Drug Administration (FDA) as a Class II device that "provides one or more capabilities relating to the acceptance, transfer, display, storage, and digital processing of medical images." PACS centralizes functions surrounding medical imaging workflows and serves as an authoritative repository of medical image information.

PACS fits within a highly complex healthcare delivery organization (HDO) environment that involves interfacing with a range of interconnected systems. PACS may connect with clinical information systems and medical devices and engage with HDO-internal and affiliated health professionals. Complexity may introduce or expose opportunities that allow malicious actors to compromise the confidentiality, integrity, and availability of a PACS ecosystem.

The NCCoE at NIST analyzed risk factors regarding a PACS ecosystem by using a risk assessment based on the NIST Risk Management Framework. The NCCoE also leveraged the NIST Cybersecurity Framework and other relevant standards to identify measures to safeguard the ecosystem. The NCCoE developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect a PACS ecosystem. This practice guide helps HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk and protect patient privacy while maintaining the performance and usability of PACS.

### **KEYWORDS**

access control; auditing; authentication; authorization; behavioral analytics; cloud storage; DICOM; EHR; electronic health records; encryption; microsegmentation; multifactor authentication; PACS; PAM; picture archiving and communication system; privileged account management; vendor neutral archive; VNA

#### **ACKNOWLEDGMENTS**

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

Name	Organization	
Matthew Hyatt	Cisco	
Kevin McFadden	Cisco	
Cletis McLean	Cisco	
Peter Romness	Cisco	
Deidre Cruit	Clearwater Compliance	
Mike Nelson	DigiCert	
Taylor Williams	DigiCert	

Name	Organization	
Andy Gray	Forescout	
Katherine Gronberg	Forescout	
William Canter	Hyland	
Kevin Dietz	Hyland	
Joseph Davis	Microsoft	
Janet Jones	Microsoft	
Dan Menicucci	Microsoft	
Mehwish Akram	The MITRE Corporation	
Steve Edson	The MITRE Corporation	
Sallie Edwards	The MITRE Corporation	
Donald Faatz	The MITRE Corporation	
Harry Perper	The MITRE Corporation	
David Alfonso	Philips Healthcare	
Jonathan Bagnall	Philips Healthcare	
Julian Castro	Philips Healthcare	
Sukanta Das	Philips Healthcare	
Jason Dupuis	Philips Healthcare	
Michael McNeil	Philips Healthcare	

Name	Organization	
Dwayne Thaele	Philips Healthcare	
Steve Kruse	Symantec	
Derek Peters	Symantec	
Axel Wirth	Symantec	
Bill Johnson	TDi Technologies	
Pam Johnson	TDi Technologies	
Robert Armstrong	Tempered Networks	
Nicholas Ringborg	Tempered Networks	
Randy Esser	Tripwire	
Onyeka Jones	Tripwire	
Jim Wachhaus	Tripwire	
Sandra Osafo	University of Maryland University College	
Henrik Holm	Virta Labs	
Michael Holt	Virta Labs	
Ben Ransford	Virta Labs	
Jun Du	Zingbox	
Damon Mosk-Aoyama	Zingbox	
David Xiao	Zingbox	

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	
Cisco	Cisco Firepower Version 6.3.0 Cisco Stealthwatch Version 7.0.0	
Clearwater Compliance	Clearwater Information Risk Management Analysis	
<u>DigiCert</u>	DigiCert PKI Platform	
Forescout	Forescout CounterACT 8	
<u>Hyland</u>	Hyland Acuo Vendor Neutral Archive Version 6.0.4 Hyland NilRead Enterprise Version 4.3.31.98805 Hyland PACSgear Version 4.1.0.64	
<u>Microsoft</u>	Azure Active Directory (AD) Azure Key Vault Version Azure Monitor Azure Storage Azure Security Center Version Standard Azure Private Link	
Philips Healthcare	Philips Enterprise Imaging Domain Controller Philips Enterprise Imaging IntelliSpace PACS Philips Enterprise Imaging Universal Data Manager	
Symantec, a division of Broadcom	Symantec Endpoint Detection and Response (EDR) Version 4.1.0 Symantec Data Center Security: Server Advanced (DCS:SA) Version 6.7 Symantec Endpoint Protection (SEP 14) Version 14.2 Symantec Validation and ID Protection Version 9.8.4 Windows	

Technology Partner/Collaborator	Build Involvement
TDi Technologies	TDI Technologies ConsoleWorks Version 5.1-0u1
Tempered Networks	Tempered Networks Identity Defined Networking (IDN) Conductor and HIPSwitch Version 2.1
Tripwire	Tripwire Enterprise Version 8.7
<u>Virta Labs</u>	BlueFlow Version 2.6.4
Zingbox	Zingbox IoT Guardian

## Contents

1	Sum	nmary1		
	1.1	Challer	nge	2
	1.2	Solutio	n	3
	1.3	Benefit	ts	3
2	How	v to U	se This Guide	4
	2.1	Typogr	aphic Conventions	5
3	Арр	roach		6
	3.1	Audien	ıce	7
	3.2	Scope .		7
	3.3	Assum	ptions	8
	3.4	Risk As	sessment	8
		3.4.1	Establishing the Risk Context	9
		3.4.2	System Actors1	.1
		3.4.3	Use Case Scenarios1	.2
		3.4.4	Threats1	.7
		3.4.5	Vulnerabilities2	0
		3.4.6	Risk	3
	3.5	Securit	y Control Map2	5
	3.6	Techno	ologies3	8
4	Arch	nitectu	ure4	4
	4.1	Archite	ecture Description4	4
		4.1.1	PACS Ecosystem Components4	7
		4.1.2	Data and Process Flow4	8
		4.1.3	Security Capabilities4	.9
		4.1.4	Asset and Risk Management5	1
		4.1.5	Enterprise Domain and Identity Management5	1
		4.1.6	Network Control and Security5	4

		4.1.7	Endpoint Protection and Security	58
		4.1.8	Device Hardening and Configuration	59
		4.1.9	Data Security	59
		4.1.10	Remote Access	60
	4.2	Final A	Architecture	61
5	Sec	urity (	Characteristic Analysis	62
	5.1	Assum	ptions and Limitations	62
	5.2	Scenar	rios and Findings	63
	5.3		is of the Reference Design's Support for Cybersecurity Framework tegories	
		5.3.1	Asset Management (ID.AM)	
		5.3.2	Risk Assessment (ID.RA)	
		5.3.3	Identity Management and Access Control (PR.AC)	
		5.3.4	Data Security (PR.DS)	
		5.3.5	Information Protection and Procedures (PR.IP)	67
		5.3.6	Protective Technology (PR.PT)	
		5.3.7	Anomalies and Events (DE.AE) and Security Continuous Monitoring (DE.CM)	68
	5.4	Securi	ty Analysis Summary	69
6	Fun	ctiona	al Evaluation	69
	6.1	PACS F	Functional Test Plan	69
		6.1.1	PACS Functional Evaluation Requirements	70
		6.1.2	Test Case: PACS-1	71
		6.1.3	Test Case: PACS-2	73
		6.1.4	Test Case: PACS-3	74
		6.1.5	Test Case: PACS-4	75
		6.1.6	Test Case: PACS-5	76
		6.1.7	Test Case: PACS-6	78
		6.1.8	Test Case: PACS-7	79
		6.1.9	Test Case: PACS-8	81
		6.1.10	Test Case: PACS-9	82

6.1.11	Test Case: PACS-10	84
6.1.12	Test Case: PACS-11	86
6.1.13	Test Case: PACS-12	87
7 Future Bu	uild Considerations	. 88
Appendix A	List of Acronyms	. 89
Appendix B	References	92
Appendix C	Pervasive Versus Contextual Controls	.96
Appendix D	Aligning Controls Based on Threats	100

# List of Figures

Figure 3-1 Notional High-Level Architecture	10
Figure 3-2 Scenario One: Sample Radiology Practice Workflows1	13
Figure 3-3 Scenario Two: Image Data Access Across the Enterprise1	14
Figure 3-4 Scenario Three: Accessing, Monitoring, and Auditing1	15
Figure 3-5 Scenario Four: Imaging Object Change Management1	16
Figure 3-6 Scenario Five: Remote Access1	17
Figure 4-1 High-Level PACS Architecture4	45
Figure 4-2 PACS Ecosystem Components4	47
Figure 4-3 PACS Ecosystem Data Communication Flow4	49
Figure 4-4 Base Controls on Test Build Components5	51
Figure 4-5 NCCoE Lab Environment Network Architecture5	55
Figure 4-6 Microsegmentation Architecture5	57
Figure 4-7 PACS Final Architecture	<b>62</b>

# List of Tables

-1 Threats18
--------------

Table 3-2 Vulnerabilities	)
Table 3-3 Risk24	ŀ
Table 3-4 Security Characteristics and Controls Mapping–NIST Cybersecurity Framework	;
Table 3-5 Products and Technologies   38	\$
Table 5-1 Identity Management Characteristics         65	
Table 6-1 Test Case Fields	)
Table 6-2 Functional Evaluation Requirements	)
Table C-1 Pervasive Security Controls       97	1

## **1** Summary

Medical imaging is a critical component in rendering patient care. The system that provides the acceptance, transfer, display, storage, and digital processing of medical images is known as a picture archiving and communication system (PACS) [1] and is nearly ubiquitous in healthcare environments. The PACS environment serves as the repository to manage these images and accompanying clinical information within the healthcare delivery organization (HDO). Vendor neutral archive systems (VNAs) perform archive management functions similar to PACS, and hereafter, this practice guide includes VNAs when it refers to PACS. PACS fits within a highly complex HDO environment and may interface with a range of enterprise information technology (IT) systems and healthcare professionals internal and external to the HDO. This complexity leads to cybersecurity challenges.

To develop practical cybersecurity guidance for securing PACS, we must consider the ecosystem surrounding PACS, which includes interconnected medical imaging equipment generally described as modalities. The ecosystem also includes modalities; connected clinical systems such as radiology information systems (RIS), health information systems (HIS), or the electronic health record (EHR); cloud storage capabilities; viewer and administration workstations; VNAs; and the PACS itself.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory that emulates a medical imaging environment, performed a risk assessment, and developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect a PACS ecosystem. Any organization that deploys PACS and medical imaging systems can use the example implementation, which represents one of many possible solutions and architectures, but those organizations should perform their own risk assessment and implement controls based on their risk posture.

For ease of use, 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 we used; the solution demonstrated to address the challenge; benefits of the solution; and the technology partners who participated in building, demonstrating, and documenting the solution. The Summary also explains how to provide feedback on this guide.

<u>Section 2</u>, How to Use This Guide, explains how business decision makers, program managers, IT professionals (e.g., systems administrators), and biomedical engineers might use each volume of the guide.

<u>Section 3</u>, Approach, offers a detailed treatment of the scope of the project, the risk assessment that informed platform development, and the technologies and components that industry collaborators gave us to enable platform development.

<u>Section 4</u>, Architecture, specifies the components within the PACS ecosystem from business, security, and infrastructure perspectives and details how data and processes flow throughout the ecosystem. This section also describes the security capabilities and controls referenced in the NIST Cybersecurity Framework through tools provided by the project collaborators.

<u>Section 5</u>, Security Characteristic Analysis, provides details about the tools and techniques used to perform risk assessments pertaining to PACS.

<u>Section 6</u>, Functional Evaluation, summarizes the test sequences 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 demonstrated in the example implementation.

<u>Section 7</u>, Future Build Considerations, is a brief treatment of other applications that NIST might explore in the future to further protect a PACS ecosystem.

The appendixes provide acronym translations, references, a mapping of the PACS project to the NIST Cybersecurity Framework, and a list of additional informative security references cited in the framework. Acronyms used in figures and tables are in the List of Acronyms appendix.

## 1.1 Challenge

The challenge with PACS is securing disparate, interconnected systems. A medical imaging infrastructure offers a broad attack surface with equipment that may have varying vulnerabilities, configurations, and control implementations. Devices deployed in the ecosystem likely come from different vendors and suppliers, and how one may implement defensive measures can vary based on the nature of the devices and how they function vis-à-vis patients and other clinical systems. The ecosystem may also include legacy devices that are potentially more vulnerable to cyber risks. The care provider team (clinicians and other healthcare professionals) may reside in different departments and may have components hosted and used across a wide geography. HDOs may leverage cloud storage environments to store and maintain medical images. Some actors may be external to the HDO, interacting with sensitive information across the internet.

As threats to the operational environment increase, PACS and other healthcare systems may become increasingly vulnerable to:

- system disruption, leading to
  - inability to render timely diagnosis and treatment
  - inability to access the system for standard use, including inability to schedule procedures
- compromise of image data, leading to incorrect diagnosis and treatment

- compromise of components, allowing malicious actors to use the components as pivot points to attack other parts of the HDO infrastructure
- privacy concerns that may lead to
  - fraudulent or improper use of data
  - patient identity theft

### **1.2 Solution**

This NIST Cybersecurity Practice Guide, *Securing Picture Archiving and Communication System (PACS)*, shows how biomedical engineers, networking engineers, security engineers, and IT professionals can help securely configure and deploy PACS within HDOs by using commercially available, open-source tools and technologies that are consistent with cybersecurity standards.

This practice guide leveraged the NIST Cybersecurity Framework in selecting privacy and cybersecurity controls. Controls and solutions may be procured, obtained as part of an open-source solution, or internally developed. While the NCCoE obtained commercially available products for this practice guide, these do not represent the only methods available to HDOs in meeting control objectives.

The reference architecture features technical and process controls to implement the following solutions:

- a defense-in-depth solution, including network zoning that allows more granular control of network traffic flows and limits communications capabilities to the minimum necessary to support business function
- access control mechanisms that include multifactor authentication for care providers, certificate-based authentication for imaging devices and clinical systems, and mechanisms that limit vendor remote support to medical imaging components
- a holistic risk management approach that includes medical device asset management augmenting enterprise security controls. It should also leverage behavioral analytic tools for near real-time threat and vulnerability management in conjunction with managed security solution providers
- cloud storage for medical images, which makes images scalable and available for HDOs

## **1.3 Benefits**

The NCCoE's practice guide to securing PACS in HDOs can help your organization:

- improve resilience in the network infrastructure, including limiting a threat actor's ability to leverage components as pivot points to attack other parts of the HDO's environment
- limit unauthorized movement within the HDO enterprise network to address the potential risk of an insider threat or malicious actors who gain network access

- analyze behavior and detect malware throughout the ecosystem to enable HDOs to determine when components evidence compromise and to enable those organizations to limit the effects of a potential threat such as ransomware
- secure sensitive data (e.g., personally identifiable information or protected health information [PHI]) at rest, in transit, and in cloud environments; enhance patient privacy by limiting malicious actors' ability to exfiltrate or expose that data
- consider and address risks of potential cloud solutions to manage an HDO's medical imaging infrastructure

## 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 help secure a medical imaging ecosystem. This practice guide builds upon the network zoning concept described in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*. As part of the implementation, the project used microsegmentation, role-based access controls, and behavioral analytics in the lab's security controls. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-24A: *Executive Summary*
- NIST SP 1800-24B: Approach, Architecture, and Security Characteristics what we built and why (you are here)
- NIST SP 1800-24C: *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 1800-24A, which describes the following topics:

- challenges that enterprises face in securing PACS
- example solution built at the NCCoE
- benefits of adopting the example solution

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

- Section 3.4, Risk Assessment, provides a description of the risk analysis we performed.
- <u>Section 3.5</u>, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary*, NIST SP 1800-24A, with your leadership team members to help them understand the importance of adopting standards-based, commercially available technologies that can help secure a PACS 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 1800-24C, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create 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 the NCCoE's risk assessment and 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 that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to <u>hit\_nccoe@nist.gov</u>.

## 2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names;	For language use and style guidance,
	references to documents that	see the NCCoE Style Guide.
	are not hyperlinks; new	
	terms; and placeholders	
Bold	names of menus, options,	Choose File > Edit.
	command buttons, and fields	
Monospace	command-line input,	mkdir
	onscreen computer output,	
	sample code examples, and	
	status codes	
Monospace Bold	command-line user input	service sshd start
	contrasted with computer	
	output	
<u>blue text</u>	link to other parts of the	All publications from NIST's NCCoE
	document, a web URL, or an	are available at
	email address	https://www.nccoe.nist.gov.

## **3** Approach

An HDO enterprise network environment is complex, with IT infrastructure to handle a range of functions, including back office billing, supply chain and inventory management, EHRs, and a vast array of connected medical devices. PACS serves an important function within this already complex environment through its role in aggregating and centralizing the medical imaging ecosystem while interfacing with other clinical systems. Specialists involved in the workflow may reside in different departments, be in different parts of an HDO campus, and be external to the HDO, accessing systems and images from the internet. This practice guide seeks to help the healthcare community evaluate the security environment surrounding PACS and medical imaging in a clinical setting.

Throughout the Securing PACS project, we collaborated with our NCCoE Healthcare Community of Interest and technology and cybersecurity vendors to identify standard medical imaging workflows and actors, define interactions between actors and systems, and review risk factors. Based on this analysis, the NCCoE developed an architecture and reference design, identified applicable mitigating security technologies, and designed an example implementation to help better secure a PACS ecosystem. This volume provides 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.

To develop the reference solution, we reviewed known vulnerabilities in PACS, the Digital Imaging and Communications in Medicine (DICOM) protocol [2], [3], and medical imaging process flow, leveraging

use cases described by Integrating the Healthcare Enterprise (IHE) [4]. We examined how to design the architecture and component integration to increase the security of the device.

The practice guide used the systems security engineering (SSE) framework discussed in NIST SP 800-160 Volume 1 [5] to introduce a disciplined, structured, and standards-based set of SSE activities and tasks to the project. This SSE framework provides the starting point and the forcing function to introduce engineering-driven actions that lead to more defensible and resilient systems. The SSE framework starts with and builds upon standards for systems and software engineering, then introduces SSE techniques, methods, and practices into these standard system engineering processes.

Additionally, this project reviewed NIST SP 800-171 Rev. 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [6], as well as NIST SP 800-181 Rev.1, *Workforce Framework for Cybersecurity (NICE Framework)* [7], for further guidance. Organizations may refer to these documents in expanding their safeguarding environment as appropriate. These documents serve as background for this project, with primary emphasis on the NIST Cybersecurity Framework [8] and the NIST Risk Management Framework [9].

#### 3.1 Audience

The NCCoE provides this guide for professionals implementing security solutions within an HDO. It may also be of interest to anyone responsible for securing nonstandard computing devices (i.e., the Internet of Things [IoT]). More specifically, the NCCoE designed Volume B of this practice guide (NIST SP 1800-24B) to appeal to a wide range of job functions, including IT operations, storage support engineers, network engineers, PACS support biomedical engineers, cybersecurity engineers, healthcare technology management (HTM) professionals, and support staff who are responsible for medical imaging devices, viewing or administrative workstations, PACS, or VNAs. For cybersecurity or technology decision makers within HDOs, this volume provides a view into how they can make the medical device environment more secure, to help improve their enterprise's security posture and reduce enterprise risk. Additionally, this volume offers guidance to technical staff on building a more secure medical device network and instituting compensating controls.

#### 3.2 Scope

The NCCoE project focused on securing the environment of a PACS ecosystem but not on reengineering medical devices or altering medical imaging processes themselves. This project led to a standards-based practice guide that applies to the wider healthcare ecosystem. This practice guide describes how the project secured PACS in a laboratory environment at the NCCoE that replicated parts of a typical HDO environment. The project considered PACS users internal to the HDO as well as external users and partners needing access to certain components of the HDO environment.

## 3.3 Assumptions

In building this healthcare practice guide, the NCCoE began the project with the following fundamental assumptions:

- Medical devices will include flaws or weaknesses that may be leveraged as vulnerabilities.
- Patches or fixes for these vulnerabilities may not be available or deployable in a timely fashion.
- Other components within an HDO's network may include flaws and vulnerabilities.
- Security controls that one may deploy may themselves include flaws or weaknesses that could be used to compromise the HDO network.

This practice guide identifies controls that may be appropriate for mitigating risks associated with the medical imaging ecosystem made up of PACS and VNA. 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. As a result, in addition to the assumptions noted above, we also assume implementation of pervasive controls, discussed in more detail in <u>Appendix C</u>.

## 3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [10], 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." 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 Revision 2, *Risk Management Framework for Information Systems and Organizations* [11]—material that is available to the public. The Risk Management Framework (RMF) [9] 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.

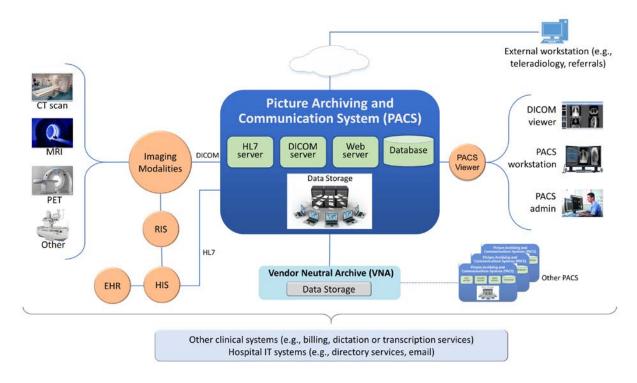
In conducting the risk assessment, this document considers threats and risks grouped under Confidentiality, Integrity, and Availability, commonly referred to as the CIA triad [12].

#### 3.4.1 Establishing the Risk Context

As we examine risk, we begin by considering the risk context. The ecosystem itself is complex and presumes different teams of people, varying processes, and different technologies involved in acquisition, interpretation, and maintenance of medical imaging information. This section presents the risk context of the Securing PACS Project, which is established around five scenarios that represent typical processes found in a medical imaging ecosystem [13]. The risk context, which in this practice guide is within the medical imaging ecosystem logical boundary, defines where to perform a risk assessment. Risk context of the PACS environment encompasses the physical and logical components of the medical imaging ecosystem that interconnect with PACS as well as the various stakeholders within the ecosystem. For the NCCOE PACS lab environment, risk context contains the components listed below and the system actors of the PACS, which include both human and system actors, as described in <u>Section 3.4.2</u>.

Figure 3-1 depicts the notional high-level architecture that bounds the PACS and medical imaging ecosystem [13]. This depiction provides a starting point in understanding the components addressed in this project. However, this project took a holistic approach in framing the risk context, beyond some of the technology components. This project leveraged concepts described in NIST SP 800-160 [5] in defining context for a PACS ecosystem, understanding risk based on context, and selecting appropriate controls when designing the control environment needed to mitigate that contextual risk. NIST SP 800-160, *Systems Security Engineering* [5], identifies concepts of examining system life cycle and components, performing holistic analysis on both technical and nontechnical processes, to deliver "trustworthy" systems. Trustworthiness describes a solution whose objective is to provide "adequate security" related to stakeholders' concerns. In order to achieve systems security engineering "trustworthiness" goals, practitioners should consider system life-cycle processes and frame the risk context based on a process and entity relationship analysis [5].

#### Figure 3-1 Notional High-Level Architecture



The system for this project is broadly identified as the PACS, though practically, it incorporates a set of processes and other systems that make up a medical imaging ecosystem [13]. For purposes of this project, and in accordance with NIST SP 800-160 [5], we consider the individual components as "systems of interest," noted below:

- workstations used to interact with the medical imaging ecosystem
  - viewer workstations residing within the HDO perimeter
  - viewer workstations residing external to the HDO perimeter, used by remote care specialists
  - workstations used by clinical staff to access peripheral systems, such as order entry systems, RIS, HIS, or EHR
- modalities, or medical imaging devices that acquire medical images and forward those to the PACS, based on orders typically received from the EHR or HIS and following workflows typically defined by the RIS
- clinical systems that interface with modalities and the PACS environment, supporting medical imaging processes such as scheduling, annotations, or reporting

- PACS will support interfaces, depicted in Figure 3-1, as "servers." These interfaces include the Health Level 7 (HL7) interface that allow clinical systems to interact with the PACS in sharing PHI; the DICOM interface, which represents a communications and medical imaging standard that represents a standard method by which medical imaging modalities interoperate with PACS; and the web server interface, which represents the PACS' ability to allow clinical interaction with the PACS to retrieve medical images using hypertext transfer protocol (http) via a standard web browser.
- a relational database server to manage metadata about the medical images or PACS administration data
- PACS and vendor neutral archive (VNA) application servers

In addition to the technology components described above and in the PACS Project Description, we considered other elements, such as stakeholders (system actors) as well as specific business process flows in which those stakeholders may participate. The processes align with profiles established by Integrating the Health Enterprise (IHE) [4], which this project leveraged to determine process and data flows. The four selected profiles translate to the scenarios described below. Based on the PACS Project Description document, the scenarios of note are Sample Radiology Practice Workflows; Access to Aggregations and Collections of Different Types of Images; Accessing, Auditing, and Monitoring; Image Object Change Management; and Remote Access [13].

This practice guide does not examine pervasive risks that an HDO may face but rather focuses on those risks specific to the medical imaging ecosystem. While this guide suggests specific requirements for safely and securely hosting PACS, the intent of the guide is not to serve as an omnibus guide for all facets potentially required to operate a secure HDO infrastructure. This guide addresses measures that would enhance the security posture for the overall PACS and medical imaging ecosystem, but there may be elements that HDOs should address beyond the recommendations offered in safeguarding a PACS and the overall medical imaging ecosystem.

## 3.4.2 System Actors

This project considered several roles that interact with the PACS and medical imaging system ecosystem. This project looked at both authorized human and system actors. Human actor roles consist of:

- medical imaging technologists
- clinicians
- clinical systems IT administrators
- HTM professionals
- IT staff

System actors that interact with the PACS and VNA consist of:

- modalities
- RIS and HIS
- EHRs

The system actor list excludes patients. The actions focused on medical images, which include creation of the image, annotation, storage of the image and annotations, interpretation, and changes to those images. The project limited radiology information systems and EHR systems actions to order entry/scheduling procedures and to pointing to images for reading/viewing. The scenarios below note process flows which describe use case profiles defined by IHE, a body that this project identified as authoritative in defining standard imaging workflow processes [4].

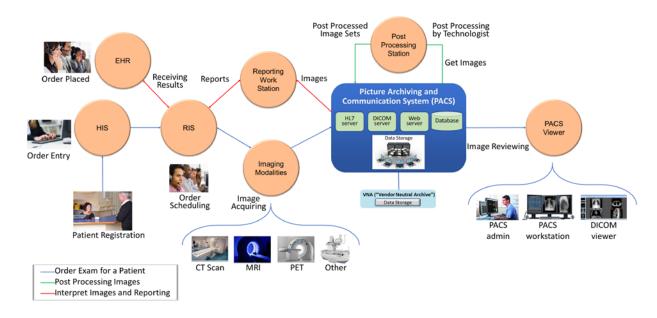
#### 3.4.3 Use Case Scenarios

This project assessed risk for the five scenarios [13] described below. Considering threats, vulnerabilities, likelihoods, and impacts on medical imaging operations under these scenarios contributed to the risks documented in <u>Section 3.4.6</u>.

These scenarios frame the processes wherein we considered introduction of threats. In addition to the scenario, this document investigates those vulnerabilities, threats, and risks that may be evident based on a holistic view of the architecture, as described in <u>Section 3.4.4</u>, <u>Section 3.4.5</u>, and <u>Section 3.4.6</u>. Within that viewpoint, the scenarios excluded several threats that are relevant for consideration. While this document investigates addressing modality interfaces, it does not examine specific modalities or the risks potentially associated with them. Modality devices themselves are medical devices that may include vulnerabilities or opportunity for systems or data compromise, loss of data integrity, or disruption of service, and HDOs should perform independent risk assessments in addressing those risks.

#### 3.4.3.1 Sample Radiology Practice Workflows

Scenario One, shown in Figure 3-2, starts with registration of a patient who requires an imaging procedure be performed [13]. For the purposes of this project, the assumption is that the HDO registers the patient into the EHR, determines the patient has appropriate identifiers to be admitted, and the patient is able to receive procedures. The scenario follows the process flow that begins at scheduling the procedure, acquiring the image, and allowing the care team to analyze and diagnose. The assumption is that all modality devices and clinical staff are on-premise, within the boundaries of the HDO. Systems in this sample radiology practice workflow convey patient information using the HL7 [14] protocol (e.g., patient registration and order entry messages). Medical imaging devices would interact with the PACS/VNA by using DICOM [2], [3].



#### Figure 3-2 Scenario One: Sample Radiology Practice Workflows

The scenario's processes are as follows:

- Patient Registration: The HDO enters a new patient's information into an HIS. An HIS may also be referred to as a clinical information system. The function of this process flow is to establish a patient identity within a hospital where one may not previously exist and then administer the patient as appropriate.
- **Order Entry:** Once the HDO establishes a patient identity, a clinician can order a medical imaging procedure for the patient by using some form of computerized physician order entry system.
- **Order Scheduling:** Following a submitted order, clinicians may schedule a medical imaging procedure involving an appropriate medical imaging modality using a RIS.
- Image Acquisition: After a clinician creates an order and scheduling has been performed, a clinician performs the imaging procedure using the appropriate modality. Acquisition results in creation of a medical image.
- Image Post-Processing: When the modality creates the medical image, imaging technologists will examine the image and may record initial annotations. The image and annotations are then pushed to the PACS.
- Image Analysis and Reporting: An imaging clinician may use a viewer workstation to examine the image, analyze, interpret, and diagnose, with subsequent notes pushed to the PACS for reporting.

<u>Stakeholders</u>: medical imaging technologists, clinicians (medical imaging specialists), and medical imaging devices (modalities)

Systems of Interest: order entry, RIS, medical imaging devices, viewer workstations, PACS

<u>Protocols Used</u>: DICOM, web (e.g., hypertext transfer protocol secure [https]), HL7, Host Identity Protocol (HIP)

#### 3.4.3.2 Image Data Access Across the Enterprise

Scenario Two, as shown in Figure 3-3, examines multiple departments that use disparate imaging devices for acquisition and may involve multiple PACS [13]. The assumption is that different departments have separate clinical staff and different medical imaging goals and may use different means to centralize their medical images. This scenario simulates a hospital, in that radiology is not the only department that uses medical imaging, nor does the radiology department mandate use of its PACS to centralize medical images across a hospital. Aggregation and centralized management remain the goal, but the practice guide describes other components in the ecosystem that enable broader clinical functionality. While PACS implements central medical image storage, access to images is not permitted for all clinical staff.

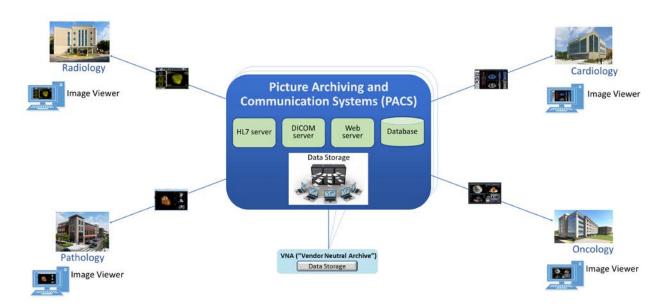


Figure 3-3 Scenario Two: Image Data Access Across the Enterprise

In demonstrating that different groups and technologies are involved, this project shows variables as "\_a" or "\_b." This allows us to show the separation between two components that may be similar in function but are separate, e.g., "component\_a" versus "component\_b."

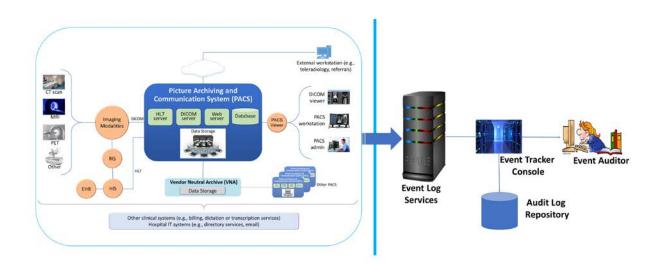
<u>Stakeholders</u>: medical imaging staff\_a, medical imaging staff\_b, healthcare technology management professionals, PACS\_a, PACS\_b, VNA

Systems of Interest: image viewer\_a, image viewer\_b, PACS\_a, PACS\_b, VNA

#### 3.4.3.3 Accessing, Monitoring, and Auditing

Scenario Three, as shown in Figure 3-4, examines the infrastructure required for access control, which includes identity management and authentication for actors who interact with the PACS and VNA environments, as well as logging, auditing, and monitoring actions with the stored information [13]. The scenario considers those actions where individuals or devices retrieve and view information (Read actions) and introduce new information (Write actions), as well as when individuals or devices modify stored information (Change actions).

Figure 3-4 Scenario Three: Accessing, Monitoring, and Auditing



This project established identities for users (humans who interact with the system), as well as for devices and systems. This scenario assumed that individuals have been appropriately identity-proofed and are provisioned accounts with which they may access and use viewer applications. Given that this project provisioned identities and accounts for both human and machine actors, all interactions require authentication. Authentication may involve exchange of passwords, passcodes, biometrics, or cryptographic keys to validate the actor. A log file recorded all transactions, including authentication attempts.

This scenario examines clinical use system interaction and does not address privileged user access. Controls to manage privileged access are discussed in <u>Section 4.1.5.1.1</u>, Privileged Access Management.

Stakeholders: medical imaging staff, medical devices, PACS, VNA

Systems of Interest: directory servers, user account systems, digital certificate servers

<u>Protocols</u>: public key infrastructure (PKI) (associated protocols such as Certificate Management Protocol, http, https), domain name system (DNS), Active Directory

#### 3.4.3.4 Imaging Object Change Management

Scenario 4, as shown in Figure 3-5, supports the changes that include (1) object rejection due to quality or patient safety reasons, (2) correction of incorrect modality worklist entry selection, and (3) expiration of objects due to data retention requirements [13]. This diagram depicts the change request process. The scenario considers those actions when an authorized healthcare professional, upon review of the image, determines that errors or qualitative defects found in an image may lead to an inappropriate conclusion.

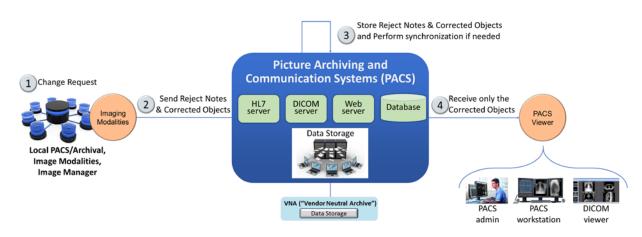


Figure 3-5 Scenario Four: Imaging Object Change Management

Stakeholders: medical imaging clinicians

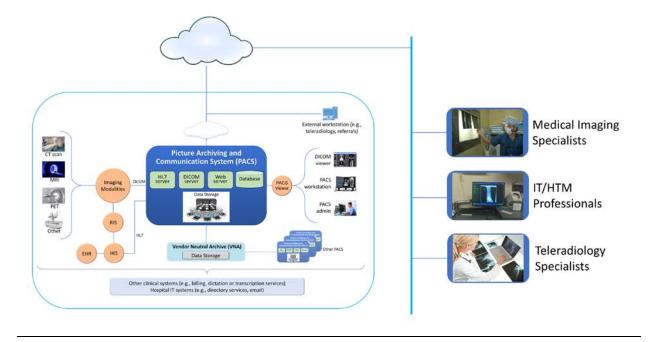
Systems of Interest: PACS, VNA

#### Protocols: HL7, http, https

#### 3.4.3.5 Remote Access

Scenario 5, depicted in Figure 3-6, supports external parties who may need access to the PACS ecosystem. The scenario provides a pathway for IT vendors to provide remote systems support as well as for third-party clinical participants to interact with the PACS. IT vendors may consist of clinical systems support staff who may need to help maintain the PACS or VNA system. Third-party clinical participants may consist of medical imaging specialists or teleradiology specialists who may need to review medical images acquired at the HDO.

#### Figure 3-6 Scenario Five: Remote Access



Stakeholders: medical imaging specialists, IT/HTM professionals, teleradiology specialists

Systems of Interest: PACS, VNA

#### 3.4.4 Threats

From NIST SP 800-30 Revision 1, "[a] threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service" [10].

In layman's terms, threats are adverse events that may occur. Threat actors may take actions to leverage vulnerabilities (described in the subsection below). Actions may include compromising credentials and accessing, removing, or changing data or making systems not available for legitimate use. The result of threats is risks [10]. Table 3-1 enumerates threats considered within this practice guide.

#### Table 3-1 Threats

C/I/A	Threat Event	Description	Unmitigated Likelihood
С	Abuse of credentials or insider threat	Aberrant behavior from an individual who may have legitimate access to the system; however, they may leverage granted privileges for unintended purposes.	High
С	Credential compromise	Malicious actor obtains the means to use credentials provisioned for others. Credentials may involve other users or those used by systems for process or data handling.	High
С	Data exfiltration	Removal of data to an unintended destination. Exfiltration may represent the unauthorized movement of data from one system to uncontrolled physical storage media or may represent movement to uncontrolled virtual destinations such as volatile memory, or to unknown storage such as cloud-hosted or virtual destinations.	High
I	Disruption of data in transit	Distortion or alteration of data in transit that results in potentially invalid information. The attack type seeks to distort or alter data in mid- communication stream. Received data may be unintelligible or otherwise unreadable when it arrives at the destination.	Moderate
1	Data alteration	Unauthorized changes to the content of the data. Clinicians may not detect altered information and misinterpret the image. The attack type seeks to make changes when data are in an at- rest state.	Moderate
I	Time synchronization	System components may rely on synchronizing internal clocks to ensure network session and data integrity. Attacks may seek to alter time stamping or ability for systems to synchronize with an authoritative time source.	Moderate
I	Introduction of malicious software	Introduction of foreign, unauthorized code into a system. Malicious software deployments may affect servers or workstations or both.	High

C/I/A	Threat Event	Description	Unmitigated Likelihood
		Server components: Server components may run unauthorized code. Workstations: Workstations connected to the PACS ecosystem may run unauthorized code.	
I	Unintended use of service	Operating systems may consist of services or processes used to support a system's functionality; individuals with access to the system may perform unintended functions.	High
A	Data storage disruption	Physical media or file space disruption evidenced by prolonged read/write access times or by corrupted data, thereby causing unavailability of service.	High
A	Network disruption	Network disruption attacks may take the form of several different approaches. Below are some disruption approaches that this practice guide examines: Denial of service (DoS) or packet flooding: Introduction of above-normal network traffic that saturates network infrastructure components' ability to deliver network communication appropriately <i>Routing:</i> inefficient network traffic flow DNS or name resolution: Networked hosts are associated with "friendly names" to facilitate interaction; however, name resolution to internet protocol (IP) addressing may be disrupted to make host discovery difficult. Similar or soundalike host and domain names may be introduced to compound confusion. <i>ARP:</i> Address Resolution Protocol (ARP) is a localized means by which hosts resolve IP addresses to media access control (MAC) addresses stored in host tables. Corruption of ARP tables may result in misdirected network traffic or in legitimate devices being unable to connect to the network.	High
A	Backup/recovery disruption	Measures that organizations use as a fail-over or recovery from a prolonged outage may be	High

C/I/A	Threat Event	Description	Unmitigated Likelihood
		compromised, e.g., through introduction of malicious software to backup storage media, inability to read and restore from backup media, or introduction of a supply chain compromise (per above) at a third-party recovery site. High availability or replication scenarios may also be prone to network disruption.	
A	Supply chain compromise	System components may be sourced from multiple vendors and may allow introduction of malicious software (noted above).	High

### 3.4.5 Vulnerabilities

Table 3-2 lists identified vulnerabilities that aggregate vulnerabilities identified in NIST SP 800-30 Revision 1 [10]. As noted in the document, a vulnerability is a deficiency or weakness that a threat source may exploit, resulting in a threat event. The document further describes that vulnerabilities may exist in a broader context, such as in organizational governance structures, external relationships, and mission/business processes. The following table enumerates those vulnerabilities using a holistic approach and represents those vulnerabilities that this project identified and for which it offers guidance. For further description, reference NIST SP 800-30 Revision 1 [10].

Table 3-2 Vulnerabilities

Vulnerability Description	Vulnerability Severity (Qualitative)	Predisposing Condition	Pervasiveness of Predisposing Condition (Qualitative)
Weak or no system use training	Moderate	Workforce may not be aware or may not have received training on appropriate use or configuration of the system. Users may not have sufficient awareness of action consequences.	High
Weak or no security training	High	Workforce may not be aware of procedures on how to report anomalies. Security teams may not have sufficient training on how to investigate or may not have procedures to address security incidents.	Moderate

Vulnerability Description	Vulnerability Severity (Qualitative)	Predisposing Condition	Pervasiveness of Predisposing Condition (Qualitative)
Deficient supply chain security controls	High	Organizations may not be aware of third- party practices or downstream suppliers who may implement technology into the healthcare organization's environment.	High
Deficient separation of duties	High	Privileged users may have extended responsibility to ensure system operations. "Super user" identities may allow escalated access to systems, data, and logging features.	High
Weak or no identity management	High	Organizations may have deficient identity proofing or review processes.	Moderate
Weak or no authentication controls	Very High	Trivial forms of authentication or using credentials with no authentication requirement. Also found in this category is the use of default credentials that tend to be generally discoverable.	Very High
Permissive privilege	Very High	Credentials may be established without examining the minimum necessary to perform the required function. As a result, credentials may exist with access to perform actions outside the work scope. Note that permissive privilege may extend to system services whereby services may run as "root" or "administrator," granting that credential the ability to perform inappropriate actions.	Very High
Out-of-date or unmanaged services	High	Operating systems, other third-party software, and the PACS application itself include a variety of services, allowing appropriate functionality. Over time, flaws, in the form of bugs (coding errors) or the use of libraries or binaries determined to have security weakness(es), may be discovered and	Very High

Vulnerability Description	Vulnerability Severity (Qualitative)	Predisposing Condition	Pervasiveness of Predisposing Condition (Qualitative)
		subsequently addressed, resulting in patches or updates. Systems that do not apply those patches and updates may operate with out-of-date services.	
Deficient vulnerability management	Very High	Organizations may have deficient application and operating system vulnerability scanning and monitoring practices. Flaws or deficiencies may exist in software elements associated with the overall medical imaging system.	Very High
Deficient data protection	High	Unauthorized individuals may be able to read, modify, delete, or exfiltrate sensitive data.	High
Deficient logging and monitoring	High	System interactions may not be captured or retained sufficiently for review. Logs, when tracked, may not be reviewed for anomalies on a timely or consistent basis.	High
Deficient time synchronization	Moderate	Systems may operate on individual internal clocks and may track transactions independently.	High
Permissive network boundaries	High	Configuration may permit unauthorized network traffic to access sensitive assets.	Very High
Lack of network segmentation	Very High	Components may operate on the same network or have implied trust with other components.	Very High
Lack of network session security	High	Network sessions may not be secured.	High
Deficient certificate management	High	Organizations using certificates to safeguard network sessions (e.g., secure sockets layer [SSL]/Transport Layer Security [TLS] certificates) may allow no certificate, expired certificates, or inappropriate certificates.	High

Vulnerability Description	Severity Predisposing Condition		Pervasiveness of Predisposing Condition (Qualitative)
Misconfigured network	High	Organizations may have misconfigured network routing or switch settings.	High
Misconfigured storage media	High	Medical image storage demands are great, and organizations may have misconfigured storage arrays.	Moderate
Recovery/restore procedures not tested or not performed	Very High	Organizations may not have created or tested recovery procedures.	High

The vulnerabilities in the table above represent types of known vulnerabilities, that is, based on vulnerabilities experienced in existing systems and networks.

### 3.4.6 Risk

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, defines risk as "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" [10]. Risk is the adverse impact; that is, risk is the result when a threat (attack) successfully leverages one or more vulnerabilities. As organizations consider risk, they should note that risk is not discrete; that is, a successful attack may involve multiple threats or take advantage of a combination of vulnerabilities. Also, when an organization suffers from an attack campaign, the organization may realize multiple adverse outcomes.

Ransomware or a DoS attack, for example, could adversely impact an HDO by compromising the availability of systems and preventing the HDO from treating patients. This practice guide, however, considers controls and practices that may be appropriate in mitigating or responding to threats affecting confidentiality, integrity, and availability holistically.

Another risk noted below is systemic disruption. Systemic disruption may affect availability and integrity of systems or data. An attacker may compromise the targeted system's operations, or the attacker may use the targeted system as a platform from which to conduct further attacks across an HDO's network. Systemic disruption prevents the HDO from treating patients by either making systems inoperative or altering patient data when malware is introduced. This practice guide also considers the specific case of when targeted systems are compromised and used to attack other components within the enterprise.

Table 3-3 is a list of unmitigated risks applicable to the PACS lab environment, based on the examples of threat types (Section 3.4.4) and vulnerabilities (Section 3.4.5). These risks are offered in terms relating to the healthcare environment, and similar risks can be expected in a typical healthcare environment. Note that the likelihood of threats and vulnerabilities would be based on having implemented effective controls, which would also affect the level of risk determined.

C/I/A	Risk	Description	Risk Level
С	Fraudulent use of health-related information	Should unauthorized individuals retrieve PHI that includes health insurance information, those actors may be able to submit fraudulent claims and receive reimbursement from a payer for services not rendered to the patient.	High
С	Identity theft and fraudulent use of PHI	Individuals may receive exfiltrated data to commit identity theft in obtaining healthcare. Fraudulent individuals may receive health services leveraging a victim patient's information and, as a result, introduce false information into a victim patient's medical history. This may result in a patient safety concern in that treatments performed for the fraudulent individual would be captured in the victim patient's history, potentially leading to future inaccurate diagnoses when that patient seeks legitimate care.	High
Ι	Patient misdiagnosed based on interpretations made from unauthorized changes to medical images	Unauthorized imaging data alteration compromises data integrity resulting in patient safety risk. Should an individual make an unauthorized image alteration, care providers may make inaccurate diagnoses and therefore delay appropriate treatment.	High
A	Patient diagnoses disrupted, leading to patient safety concerns	Patients may have conditions that require timely and accurate diagnosis to achieve optimum mortality rates. Communications disruptions that corrupt or deny data may adversely affect this so that care teams are not able to make a timely diagnosis, and patients may have to repeat imaging processes.	High
A	Process disruption due to malware	PACS or other systems within the ecosystem may succumb to ransomware or other forms of malware, rendering those systems and associated	High

C/I/A	Risk	Description	Risk Level
		data unavailable. Ransomware may cause complete system unavailability, while other forms of malware may delay processing capability or introduce data integrity risk. As a result, the HDO may not be able to treat patients appropriately or make diagnoses. Delays may result in patient safety concerns.	
A	Systemic disruption due to component compromise	Unauthorized individuals may compromise components within the PACS ecosystem and use compromised components as pivot points to attack other parts of the HDO network. This may result in delays in patient care.	High

The project identified the risks above as requirements that the lab environment should address. Organizations should note that the tables offered here are samples and notionally representative. Characterizing threats, vulnerabilities, and risk is contextual. HDOs with different security deficiencies or unique threat situations in their systems and network environments may find their categorization to be different from what this practice guide describes. HDOs need to consider their unique profile when categorizing vulnerabilities, threats, and risk. This project identified these risk elements and scored them accordingly, based on the assessment performed on the lab environment.

## 3.5 Security Control Map

As the project considered PACS ecosystem risks, the team performed a mapping to the NIST Cybersecurity Framework [8], establishing an initial set of appropriate control functions, categories, and subcategories, demonstrating how selected Cybersecurity Framework subcategories map to controls in NIST SP 800-53 Revision 4 [15]. The table also lists sector-specific standards and best practices from other standards bodies (e.g., the International Electrotechnical Commission [IEC], International Organization for Standardization [ISO]), as well as from the Health Insurance Portability and Accountability Act (HIPAA) [16], [17], [18]. The security control map, shown in Table 3-4, identifies a comprehensive set of controls, including those specifically implemented in the lab build-out, as well as the pervasive set of controls as described in <u>Appendix C</u> that HDOs should deploy.

NIST Cybe	rsecurity Framew	vork v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
identify (ID)	ID) Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried.	CM-8 PM-5	N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(4)(ii)(A) 164.308(a)(7)(ii)(E) 164.308(b) 164.310(d) 164.310(d)(2)(iii)	A.8.1.1 A.8.1.2
		ID.AM-2: Software platforms and applications within the organization are inventoried.	CM-8 PM-5	N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(4)(ii)(A) 164.308(a)(7)(ii)(E) 164.308(b) 164.310(d) 164.310(d)(2)(iii)	A.8.1.1 A.8.1.2 A.12.5.1
(ID.AM)	(ID.AM)	ID.AM-3: Organizational communication and data flows are mapped.	AC-4 CA-3 CA-9 PL-8	SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(3)(ii)(A) 164.308(a)(8) 164.310(d)	A.13.2.1 A.13.2.2
		ID.AM-4: External information systems are catalogued.	AC-20 SA-9	RDMP	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(4)(ii)(A) 164.308(a)(7)(ii)(E) 164.308(b) 164.310(d) 164.310(d)(2)(iii)	A.11.2.6

Table 3-4 Security Characteristics and Controls Mapping–NIST Cybersecurity Framework

NIST Cyber	NIST Cybersecurity Framework v1.1				Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001	
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	CP-2 RA-2 SA-14 SC-6	SGUD	45 C.F.R. §§ 164.308(a)(7)(ii)(E)	A.8.2.1	
		ID.RA-1: Asset vulnerabilities are identified and documented.	CA-2 CA-7 CA-8 RA-3 RA-5 SA-5 SA-5 SA-11 SI-2 SI-4 SI-5	MLDP RDMP SGUD	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.310(a)(1)	A.12.6.1 A.18.2.3	
	Risk Assessment (ID.RA)	ID.RA-4: Potential business impacts and likelihoods are identified.	RA-2 RA-3 SA-14 PM-9 PM-11	DTBK SGUD	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(6) 164.308(a)(7)(ii)(E) 164.308(a)(8)	A.16.1.6 Clause 6.1.2	
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	RA-2 RA-3 PM-16	SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(D) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.316(a)	A.12.6.1	

NIST Cyber	security Framewo	ork v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
		ID.RA-6: Risk responses are identified and prioritized.	PM-4 PM-9	DTBK SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(B) 164.314(a)(2)(i)(C) 164.314(b)(2)(iv)	Clause 6.1.3
PROTECT (PR)	Identity Management	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	ALOF AUTH EMRG NAUT 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)	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.6 A.9.3.1 A.9.4.2 A.9.4.3
	and Access Control (PR.AC)	PR.AC-2: Physical access to assets is managed and protected.	PE-2 PE-3 PE-4 PE-5 PE-6 PE-8	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)	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.5 A.11.2.6 A.11.2.7 A.11.2.8

NIST Cyber	security Frame	work v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.AC-3: Remote access is managed.	AC-1 AC-17 AC-19 AC-20 SC-15	ALOF AUTH CSUP EMRG 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.6.2.1 A.6.2.2 A.11.2.6 A.13.1.1 A.13.2.1
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	AC-1 AC-2 AC-3 AC-5 AC-6 AC-14 AC-16 AC-24	ALOF 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)	A.6.1.2 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	AC-4 AC-10 SC-7	MLDP 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)	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3

NIST Cyber	security Framew	ork v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	AC-7 AC-8 AC-9 AC-11 AC-12 AC-14 IA-1 IA-2 IA-3 IA-4 IA-5 IA-8 IA-9 IA-10 IA-11	ALOF AUTH CSUP EMRG NAUT PAUT	45 C.F.R. § 164.308(a)(4)	A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.2 A.9.4.3 A.18.1.4
	Data Security	PR.DS-1: Data-at-rest is protected.	MP-8 SC-12 SC-28	IGAU MLDP NAUT SAHD STCF TXCF	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)	A.8.2.3
	(PR.DS)	PR.DS-2: Data-in-transit is protected.	SC-8 SC-11 SC-12	IGAU NAUT STCF TXCF TXIG	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 Cybers	ecurity Framew	ork v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.DS-5: Protections against data leaks are implemented.	AC-4 AC-5 AC-6 PE-19 PS-3 PS-6 SC-7 SC-8 SC-13 SC-31 SI-4	AUTH IGAU MLDP PLOK STCF TXCF TXCF TXIG	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.310(b) 164.310(c) 164.312(a)	A.6.1.2 A.7.1.1 A.7.1.2 A.7.3.1 A.8.2.2 A.8.2.3 A.9.1.1 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5 A.10.1.1 A.11.1.4 A.11.1.5 A.11.2.1 A.13.1.1 A.13.1.3 A.13.2.1 A.13.2.3 A.13.2.4 A.14.1.2 A.14.1.3
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SC-16 SI-7	IGAU MLDP	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 A.14.2.4

NIST Cyber	security Framew	ork v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
	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 DTBK NAUT	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
		PR.IP-3: Configuration change control processes are in place.	CM-3 CM-4 SA-10	CNFS CSUP DTBK	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
		PR.IP-4: Backups of information are conducted, maintained, and tested.	CP-4 CP-6 CP-9	DTBK PLOK	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

NIST Cyber	security Framew	ork v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	CP-2 CP-7 CP-12 CP-13 IR-7 IR-8 IR-9 PE-17	DTBK SGUD	45 C.F.R. §§ 164.308(a)(6) 164.308(a)(6)(i) 164.308(a)(7) 164.310(a)(2)(i) 164.312(a)(2)(ii)	A.16.1.1 A.17.1.1 A.17.1.2 A.17.1.3
		PR.IP-10: Response and recovery plans are tested.	CP-4 IR-3 PM-14	DTBK SGUD	45 C.F.R. §§ 164.308(a)(7)(ii)(D)	A.17.1.3
	Protective	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	AU Family	AUDT	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(2) 164.308(a)(3)(ii)(A)	A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.7.1
	Technology (PR.PT)	PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	AC-3 CM-7	AUTH CNFS SAHD	45 C.F.R. §§ 164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.312(a)(1)	A.9.1.2

NIST Cyber	security Framewo	ork v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.PT-4: Communications and control networks are protected.	AC-4 AC-17 AC-18 CP-8 SC-7 SC-19 SC-20 SC-21 SC-22 SC-23 SC-24 SC-25 SC-29 SC-32 SC-36 SC-37 SC-38 SC-39 SC-40 SC-41 SC-43	AUTH MLDP PAUT SAHD	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(a)(1) 164.312(b) 164.312(e)	A.13.1.1 A.13.2.1 A.14.1.3
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	CNFS CSUP MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(b)	A.12.1.1 A.12.1.2 A.13.1.1 A.13.1.2

NIST Cybe	rsecurity Framev	vork v1.1		Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	AU-6 CA-7 IR-4 SI-4	AUDT MLDP	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(6)(i) 164.308(a)(6)(i)	A.12.4.1 A.16.1.1 A.16.1.4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	AU-6 CA-7 IR-4 IR-5 IR-8 SI-4	AUDT MLDP SGUD	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)(6)(ii) 164.308(a)(8) 164.310(d)(2)(iii)	A.12.4.1 A.16.1.7
		DE.AE-5: Incident alert thresholds are established.	IR-4 IR-5 IR-8	DTBK MLDP SGUD	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(6)(i) 164.308(a)(6)(i)	A.16.1.4
	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	AUDT CNFS CSUP MLDP NAUT	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(2) 164.308(a)(3)(ii)(A)	N/A

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-24.

NIST Cybe	rsecurity Frame	ework v1.1		Sector-Specific	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001	
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	AC-2 AU-12 AU-13 CA-7 CM-10 CM-11	AUDT EMRG PAUT	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)	A.12.4.1 A.12.4.3	
		DE.CM-4: Malicious code is detected.	SI-3 SI-8	IGAU MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)	A.12.2.1	
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	AU-12 CA-7 CM-3 CM-8 PE-3 PE-6 PE-20 SI-4	AUDT PAUT PLOK	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii)	A.12.4.1 A.14.2.7 A.15.2.1	
		DE.CM-8: Vulnerability scans are performed.	RA-5	MLDP PLOK	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(8)	A.12.6.1	
RESPOND (RS)	Response Planning (RS.RP)	RS.RP-1: Response plan is executed during or after an event.	CP-2 CP-10 IR-4 IR-8	DTBK MLDP SGUD	45 C.F.R. §§ 164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)	A.16.1.5	

NIST Cybersecurity Framework v1.1			Sector-Specific Standards and Best Practices			
Function	Category	Subcategory	NIST SP 800-53 Revision 4	IEC TR 80001- 2-2	HIPAA Security Rule	ISO/IEC 27001
RECOVER (RC)	Recovery Planning (RC.RP)	RC.RP-1: Recovery plan is executed during or after a cybersecurity incident.	CP-10 IR-4 IR-8	DTBK MLDP SGUD	45 C.F.R. §§ 164.308(a)(7) 164.308(a)(7)(i) 164.308(a)(7)(ii) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)	A.16.1.5

## 3.6 Technologies

Table 3-5 lists all the products and technologies used in this project and provides a mapping among the generic application term, the specific product used, and the security control(s) that the product provides or supports. Refer to Table 3-4 for an explanation of the NIST Cybersecurity Framework subcategory codes.

The Products and Technology table represents the solutions provided by the project collaborative partners and applied to the lab environment. This project selected these solutions based on their alignment to the NIST Cybersecurity Framework control objectives. Organizations should note that they may achieve control objectives through any number of means, including open-source or internally developed approaches.

 Table 3-5 Products and Technologies

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
PACS and VNA	Hyland Acuo Vendor Neutral Archive Version 6.0.4	<ul> <li>Provides access to medical images and documents.</li> <li>Stores and retrieves images in a standard format for various vendor-neutral systems to access.</li> </ul>	PR.AC-1 PR.AC-4 PR.DS-2 PR.IP-4 PR.PT-1
	Hyland NilRead Enterprise Version 4.3.31.98805	<ul> <li>Provides medical image viewing and manipulation.</li> </ul>	PR.AC-1 PR.DS-2 PR.PT-1
	Hyland PACSgear Version 4.1.0.64	<ul> <li>Provides ability to capture and share medical images.</li> <li>Provides ability to scan and share medical documents.</li> </ul>	PR.AC-1 PR.DS-2 PR.PT-1
	Philips Enterprise Imaging Domain Controller	<ul> <li>Provides role-based user-access control.</li> </ul>	PR.AC-1
	Philips Enterprise Imaging IntelliSpace PACS	<ul> <li>Manages medical images through access and collaboration.</li> </ul>	PR.DS-2 PR.IP-4 PR.PT-1

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
	Philips Enterprise Imaging Universal Data Manager	<ul> <li>provides web-based DICOM integration</li> <li>provides image life-cycle management</li> </ul>	PR.DS-2 PR.IP-4 PR.PT-1
	DCM4CHEE Open- Source Clinical Image and Object Management Enterprise Version DCM4CHEE-arc- light5 v. 5.21.0	<ul> <li>Open-source PACS solution</li> <li>allows the lab to demonstrate data-in-transit workflow control</li> </ul>	N/A
	DVTk Modality Emulator	<ul> <li>open-source utility used to demonstrate clinical workflow and interaction with medical imaging devices</li> <li>allows the lab to demonstrate data-in-transit workflow between clinical systems and medical devices</li> </ul>	N/A
	DVTk RIS Emulator	<ul> <li>open-source utility used to demonstrate clinical workflow and interaction with medical imaging devices</li> <li>allows the lab to demonstrate data-in-transit workflow between clinical systems and medical devices</li> </ul>	N/A
Asset Management	Virta Labs BlueFlow Version 2.6.4	<ul> <li>provides discovery, categorization, grouping, tagging, and identification of medical devices</li> <li>provides flexible user-defined risk assessment and scoring</li> <li>provides vulnerability management capabilities</li> </ul>	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5 ID.RA-1 ID.RA-5 PR.IP-1

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
		<ul> <li>provides reporting on risk and security properties for groups of assets</li> <li>provides threat feed for known medical devices</li> </ul>	
	Clearwater Information Risk Management Analysis	<ul> <li>provides asset inventory management</li> <li>provides risk assessment and compliance</li> </ul>	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5
	Tripwire Enterprise Version 8.7	<ul> <li>provides security configuration management</li> <li>provides file integrity monitoring (FIM)</li> <li>provides patch management.</li> </ul>	ID.RA-1 ID.RA-5 PR.DS-6 PR.IP-1 PR.IP-3 PR.PT-3
Enterprise Domain and Identity Management	Active Directory	<ul> <li>provides authentication and authorization for users and computers in the domain</li> <li>provides authentication and authorization to multiple applications within the environment</li> </ul>	PR.AC-1 PR.AC-4 PR.AC-7 PR.PT-3
	DigiCert PKI Platform	<ul> <li>provides SSL/TLS certificates for secure communication between devices</li> <li>enables devices to perform data-in- transit encryption</li> <li>provides certificate management</li> </ul>	PR.AC-1 PR.AC-4 PR.AC-7 PR.DS-2
	Symantec Validation and ID Protection Version 9.8.4 Windows	<ul> <li>integrates with TDi ConsoleWorks using the Remote Authentication Dial-In User Service (RADIUS) protocol</li> </ul>	PR.AC-1 PR.AC-3 PR.AC-7

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
		<ul> <li>provides multifactor authentication for remote access</li> </ul>	
Network Control and Security	Cisco Firepower Management Center (FMC) 6.3.0	<ul> <li>provides console management for Firepower Threat Defense</li> <li>provides centralized control over network and communication</li> <li>provides network visibility</li> </ul>	PR.AC-5 PR.PT-4
	Cisco Firepower Threat Defense (FTD) 6.3.0	<ul> <li>prevents intrusion</li> <li>provides network segmentation</li> <li>provides policy-based network protection</li> </ul>	PR.AC-5 PR.PT-4
	Tempered Networks Identity Defined Networking (IDN) Conductor and HIPswitch Version 2.1	<ul> <li>provides network segmentation</li> <li>provides end-to-end encryption for device traffic</li> </ul>	PR.AC-5 PR.DS-2 PR.PT-4
	Zingbox IoT Guardian	<ul> <li>provides passive device discovery and classification</li> <li>provides behavioral modeling to identify suspicious behavior</li> <li>assesses vulnerability</li> </ul>	ID.AM-3 ID.RA-1 ID.RA-5 DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-5 DE.CM-1 DE.CM-7
	Forescout CounterACT 8	<ul> <li>provides passive device discovery and profiling</li> <li>provides network access control</li> </ul>	PR.AC-4 PR.AC-7 PR.PT-4 DE.AE-1 DE.AE-3 DE.CM-1 DE.CM-7

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
	Symantec Endpoint Detection and Response (EDR) Version 4.1.0	<ul> <li>centrally manages threats across endpoint, network, and web traffic</li> </ul>	DE.CM-1 DE.CM-4
	Cisco Stealthwatch Version 7.0.0	<ul> <li>provides insight into who and what is on the network</li> <li>analyzes the network through machine learning and global threat intelligence</li> <li>detects malware for encrypted traffic</li> </ul>	ID.AM-3 DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-5 DE.CM-1 DE.CM-3 DE.CM-7
Secure Remote Access	TDi Technologies ConsoleWorks Version 5.1-0u1	<ul> <li>provides remote access for external collaborators</li> <li>logs and monitors remote access activities</li> </ul>	PR.AC-3 PR.AC-7
Endpoint Protection and Security	Symantec Data Center Security: Server Advanced (DCS:SA) Version 6.7	<ul> <li>protects physical and virtual servers</li> <li>detects and prevents intrusion</li> <li>monitors file integrity</li> </ul>	PR.DS-6 PR.IP-3
	Symantec Endpoint Protection Version 14.2	<ul> <li>centrally manages assets through agent-based protection</li> <li>provides advanced machine learning and behavioral analysis techniques to identify known and unknown threats</li> <li>provides anti-virus capabilities</li> </ul>	DE.CM-4 DE.CM-8
Cloud Storage	Microsoft Azure Block Blob Storage account	<ul> <li>cloud storage for medical images (unstructured data)</li> <li>access control using storage access keys and policies</li> <li>encryption at rest using service- managed or customer-managed keys</li> <li>encryption in transit using https</li> </ul>	PR.AC-1 PR.AC-4 PR.AC-7 PR.DS-1 PR.DS-2 PR.DS-6 PR.PT-4

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
		<ul> <li>storage firewalls to limit attack surface and to control communications</li> </ul>	
	Microsoft Azure Security Center Standard	<ul> <li>strengthen security posture by identifying weak or insecure configurations</li> <li>identify threats against Azure resources, including Azure Storage accounts</li> </ul>	ID.RA-1 ID.RA-5 DE.AE-1 DE.AE-2 DE.CM-1 DE.CM-8
	Microsoft Azure Key Vault Premium	<ul> <li>safeguard cryptographic keys and other secrets used by cloud applications and services</li> <li>holds storage account encryption key.</li> </ul>	PR.AC-1 PR.DS-1
	Microsoft Azure Monitor	<ul> <li>management and monitoring services</li> <li>centralized collection and retention of audit logs from various Azure services</li> </ul>	PR.AC-1 PR.IP-1 PR.PT-1 DE.CM-7
	Microsoft Azure Active Directory	<ul> <li>identity and access management for Azure services</li> <li>user and sign-in risk detection and remediation</li> </ul>	PR.AC-1 PR.AC-4 PR.AC-7 PR.PT-3 DE.CM-3
	Microsoft Azure Private Link	<ul> <li>private virtual network connectivity for platform as a service (PaaS) services hosted on the Azure platform</li> </ul>	PR.DS-2 PR.PT-4

# **4** Architecture

When designing the PACS reference architecture, this practice guide implements the PACS environment within an HDO enterprise. NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* describes implementing the HDO enterprise infrastructure and a network zone approach. This practice guide leverages that larger enterprise described in NIST SP 1800-8 and in Section 4.1 identifies zones in as they relate to PACS. This practice guide extends data storage by provisioning a cloud storage provider for long-duration storage.

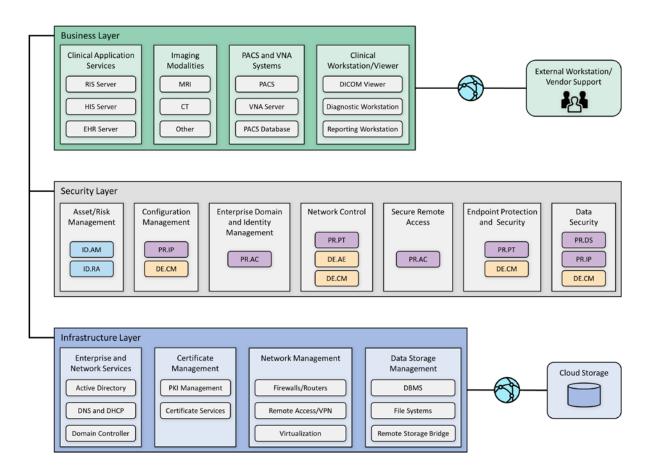
The FDA defines the PACS as "a device that provides one or more capabilities relating to the acceptance, transfer, display, storage, and digital processing of medical images. Its hardware components may include workstations, digitizers, communications devices, computers, video monitors, magnetic, optical disk, or other digital data storage devices, and hardcopy devices. The software components may provide functions for performing operations related to image manipulation, enhancement, compression or quantification" [19]. In addition to the PACS, this project used VNA solutions that meet the Food and Drug Administration's definition of PACS but have other features that HDOs may use to enhance their overall image management ecosystem. This guide recognizes that healthcare systems interoperate and that the reference architecture needs to accommodate a broad view of the medical imaging ecosystem.

## 4.1 Architecture Description

This practice guide's architecture looks at components from three primary layers:

- business, where we deployed our core medical imaging components
- security, where we implemented security tools
- infrastructure, which represents our network

Figure 4-1 illustrates the project's high-level architecture.



#### Figure 4-1 High-Level PACS Architecture

A PACS ecosystem includes components that address data in transit, data at rest, and data processing and provides applications allowing authorized individuals to review and interact with data stored in their respective systems. Clinical systems are also part of our architecture, including imaging modalities and applications such as the RIS, that each play business process roles that interact with the PACS and VNA. Medical imaging generally uses standard protocols, including DICOM.

DICOM is an international standard specific to storing, retrieving, printing, processing, and displaying medical information. The DICOM standard assures medical image information operability and provides a common standard, allowing different medical imaging product vendors to integrate their solutions into the medical imaging ecosystem [2], [3].

In addition to the DICOM standard, PACS uses the HL7 protocol for clinical documentation and image reporting. HL7 defines a markup standard for exchanging health information in a structured format by using a clinical document architecture [20].

This document examines standard technology components in addition to the protocols noted above. Central to PACS are storage media, the network infrastructure, supporting operating systems, as well as application servers to support information exchange (e.g., HL7, DICOM, and web servers).

The architecture described for this project implemented several zones composed of:

**Clinical application services** consist of systems such as the EHR, order entry, health information systems, and others used by patient care teams in recording information during patient treatment.

**Clinical workstation/viewer** establishes a network zone that segregates clinical workstations from the nonclinical production network. Clinical workstations are special-purpose devices used to interact with clinical systems. Those devices may use vendor-specified operating systems, applications, and configurations that vary from the HDO standard build. Configuration and patch management may be asynchronous with how the HDO manages its productivity or standard build systems.

**Enterprise network services** are grouped into a separate zone for enterprise operations. Enterprise operations include services such as email communications, Active Directory, DNS, and security services that include certificate management.

**Imaging modalities** provide a zone for departments using imaging equipment, generally termed as modalities. These are medical devices using operating systems that are not consistent with an HDO's baseline. Configuration and patch management are likely asynchronous with how the HDO manages its productivity or standard build systems. For purposes of this project, this zone includes emulated modalities. This project used simulation software to generate medical images.

**PACS and VNA systems** segregate the PACS and VNA applications from clinical applications, general workstations, and storage media. This zone provides the higher-level application functionality to interact with aggregated medical images.

**Data storage management** isolates large-scale storage, such as storage area networks (SANs) or network-attached storage (NAS) devices. Data stored in this zone may be unstructured, large files that may contain sensitive, personal, or PHI.

**Cloud storage** is external to the HDO infrastructure and represents the use of a third-party cloud storage provider where medical images are archived.

**Vendor Net** supports remote connectivity, e.g., remote vendor support. This zone segregates external network traffic used when vendors may need to perform maintenance on systems or other equipment while the support engineer is off premises.

## 4.1.1 PACS Ecosystem Components

The PACS ecosystem includes those components that support the clinical processes associated with medical imaging acquisition, review, annotation, and storage. Clinical applications, such as the RIS, generate image acquisition worklists and apply worklists to associated modalities. Modalities retrieve worklists from the RIS. The lab environment included two distinct PACS and a VNA systems and deployed image viewing software associated with those systems on workstations to review and annotate medical images. In building the lab environment, this project emulated some of the components rather than obtaining full-scale solutions. This project emulated both modalities and an RIS. The project also used a mobile phone device for document scanning. Figure 4-2 depicts a high-level view of these components and how we approached implementing them in the lab environment.

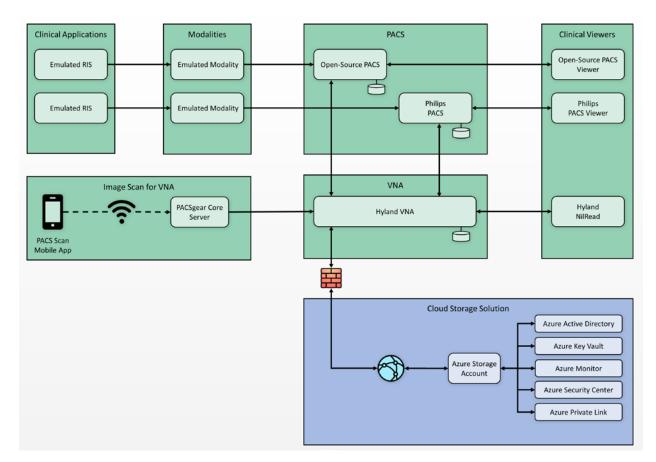


Figure 4-2 PACS Ecosystem Components

The open-source tool from DVTk (https://www.dvtk.org) includes packages that allowed this project to emulate medical imaging modalities and an RIS. The project deployed two instances of the RIS Emulator

into the clinical application services zone. The DVTk RIS Emulators associate the modalities with separate PACS and provide worklists for those modalities associated with two respective PACS, reflective of an HDO that may operate multiple PACS. The project used Philips IntelliSpace PACS and DCM4CHEE (https://www.dcm4che.org/), an open-source PACS, to support this premise. Hyland Acuo VNA was deployed to model HDOs using this technology.

This project deployed the modalities to a modalities network zone. Using emulated modalities allowed the project team to simulate DICOM image acquisition, interaction with the RIS, and transferring images from the modality device to the PACS and VNA for storage and management. The project used an iPhone to operate the PACS Scan Mobile app provided by Hyland, connecting to a PACSgear Core Server. The iPhone was treated as a modality, with the application facilitating document scanning and, through the PACSgear server, transferring mobile-acquired images to the VNA.

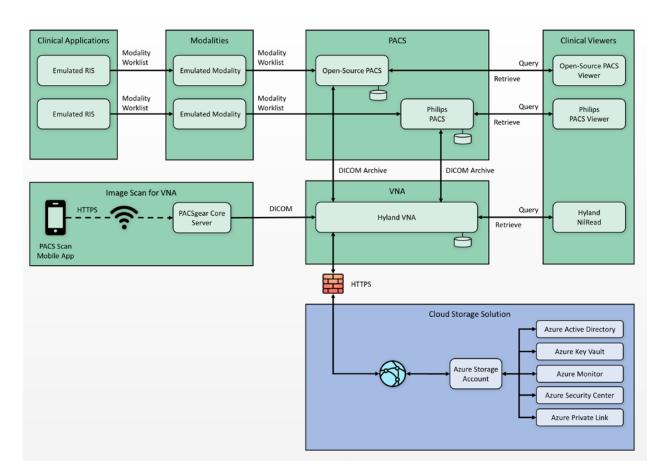
## 4.1.2 Data and Process Flow

For this project, we examined data and process flows as described in <u>Section 3.4.1</u>, Establishing the Risk Context, that include the following scenarios:

- sample radiology practice flows
- access to aggregations and collections of different types of images
- accessing monitoring and auditing
- image object change management
- remote access

The scenarios identify medical imaging acquisition processes, starting with scheduling the patient for a procedure, and follow the life cycle through when the patient interacts with an imaging device to when a medical imaging specialist processes and forwards the annotated image to a clinician for interpretation and diagnosis. Scenarios also examine processes after direct patient interaction, such as when authorized individuals access images for later review or when images need to be updated.

Figure 4-3 shows a simplified data communication flow in the PACS ecosystem.



#### Figure 4-3 PACS Ecosystem Data Communication Flow

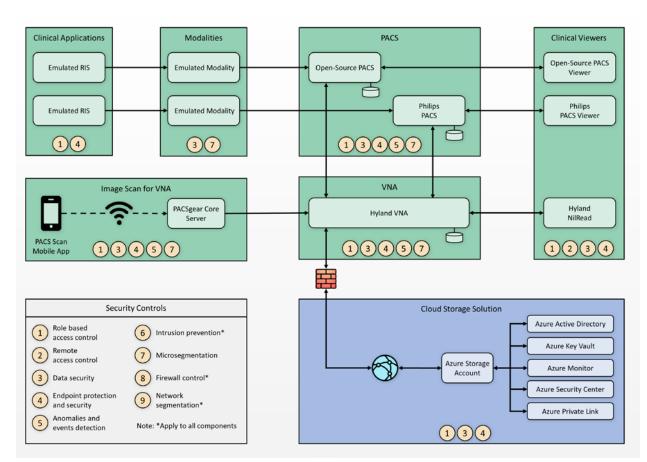
A typical radiology department workflow may begin with patient registration and admission, followed by a physician ordering an imaging procedure. The order is entered into a RIS to create a worklist. A medical imaging technologist attends to a patient and performs the image capture procedure. The medical imaging technologist may make annotations for a physician's review. The system forwards that information to a PACS or VNA. A physician retrieves the images from the PACS or VNA and uses an image viewing station to review the images and document findings and diagnoses. On completion, the physician transfers the information back to the PACS. Results may cross-reference with the EHR system.

## 4.1.3 Security Capabilities

This practice guide built upon the zoned network architecture described in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* [21]. Network zoning provided a baseline upon which engineers deployed the medical imaging ecosystem infrastructure. The practice guide identified and deployed security capabilities to the environment, consisting of the following:

- enterprise domain and identity management
  - access control
    - o privileged access controls
    - o user authentication
    - o device and system authentication
    - o data access control
- network control and security
  - network segmentation and virtual local area networks (VLANs)
  - firewall and control policies
  - microsegmentation
  - anomalies and events detection (behavioral analytics)
  - intrusion detection and prevention systems
- endpoint protection and security
  - device hardening and configuration
  - malware detection
- data security
  - data encryption (at-rest)
  - data encryption (in-transit)
- secure remote access

While the project takes a holistic approach when evaluating the medical imaging environment, the control scope noted in this practice guide is bound to those elements that are inherently or highly supportive of acquiring, interpreting, or storing medical images. An HDO's infrastructure is larger in scope than that used to support the medical imaging environment. An HDO may and should implement additional pervasive controls to secure the overall environment. This document references pervasive controls not implemented during this project and assumes an organization will implement appropriate controls to address its broader risk profiles. Refer to <u>Appendix C</u> for details. Figure 4-4 below depicts contextual controls deployed in the project's test build.



#### Figure 4-4 Base Controls on Test Build Components

### 4.1.4 Asset and Risk Management

Asset management is a critical control that aligns with the function known as Identify in the NIST Cybersecurity Framework [8]. This project assumes a pervasive control exists, such as a governance, risk and compliance (GRC) solution. The HDO manages IT general assets through the GRC solution. Medical imaging devices may fall outside the scope of IT general assets for many HDOs. For this reason, this project implemented Virta Labs BlueFlow for asset and inventory management for medical imaging devices. BlueFlow captures inventory, configuration, and patch management information [16], [22], [23].

### 4.1.5 Enterprise Domain and Identity Management

This project looked at identity management controls as including several concepts that encompass identity proofing, credentialing, and providing a means to authenticate devices and systems. Human

actors (clinical, IT administrative, and general HDO staff), medical devices, and systems may have identities established within the HDO. An identity is a broader concept than credentials or user accounts. This project assumed that HDOs perform adequate identity proofing and provisioning. This involves processes that allow HDOs to verify that an individual is who they claim to be, also ensuring that the individual has appropriate credentials to interact with clinical systems and medical imaging information. Regarding provisioning, this project assumed that following identity proofing, the organization can create and securely deliver credentials (e.g., user accounts in which the individual can select and update passwords or challenge responses known only to that individual).

Identities may include multiple user accounts or access mechanisms that may be applied. For example, an individual may have a job function as an IT administrator. As a member of the HDO workforce, they may be credentialed to access certain systems such as email or productivity software. They may also have access to separate privileged accounts to be used when they perform IT administrative duties. Having separate credentials established based on functionality or role is a common practice in healthcare and provides a form of separation of duties.

Medical devices and systems may also have identities, that are authenticated using digital certificates, keys, or other unique identifiers such as host identifiers or MAC addresses.

### 4.1.5.1 Access Control

Access control is applied contextually, based on the identity type. This project implemented access control for privileged users, clinical users, devices, and systems. Subsections below provide more detail on the project's approach.

### 4.1.5.1.1 Privileged Access Management

Privileged access includes those credentials that have permissions to systems that are greater than standard users. Privileged access accounts often allow greater visibility of resources stored on systems and may allow modifying configuration settings or permitting installation of software components. One measure that this guide implements is segregating privileged access accounts. These accounts were unique and distinct from those accounts we created that were able to access information via DICOM viewer applications. When activities required privileged access, access actions routed through lab environment's TDi ConsoleWorks implementation, which enforced the project's multifactor authentication solution.

For further guidance on privileged account management, HDOs should reference NIST SP 1800-18, *Privileged Account Management for the Financial Services Sector* [24]. While the document identifies solutions for financial services, the underlying technology solution applies to healthcare and other sectors.

#### 4.1.5.1.2 User Authentication

User authentication involves the use of different factors. Factors are characteristics by which a user may be able to assert their identity. In many cases, users are authenticated using a single factor (e.g., a username and password combination). One means to strengthen single-factor authentication is to use pass phrases rather than passwords. This approach reduces the possibility that a malicious actor may be able to brute-force-attack the credential [25].

Another aspect that HDOs may consider is to implement multifactor authentication where appropriate or feasible. Multifactor authentication includes a need to pass two or more factors that represent something a user knows, has, or is. Memorized passwords or pass phrases represent factors that a user knows. Including other factors, such as something a user has, which may represent a physical token; or something a user is, such as biometrics that include fingerprints, retinal, or facial scans, would provide greater assurance that the user is whom they claim to be. Multifactor authentication may not be implementable in all cases, and HDOs may need to determine their risk tolerance and implementation practicality when considering enhancing their authentication models [26].

#### 4.1.5.1.3 Device and System Authentication

For this project, we emulated medical imaging devices and implemented the HIP. Emulated modality devices authenticated to a HIPswitch, routing modality traffic across a HIP-secured software-defined network. For further information, refer to the discussion in <u>Section 4.1.6.3</u>, Microsegmentation.

For systems authentication within the HDO, this project used digital certificates and keys. This project deployed digital certificates to the PACS and VNA servers as well as to a mobile device where we installed software used to scan documents and images that would be added to our medical imaging store. Authentication between VNA servers and cloud data storage is achieved using access keys.

This practice guide uses digital certificates to secure network sessions using a key management solution provided by the cloud provider. The HDO configures key management to maintain private key control. However, this project did not implement a data security manager or hardware security manager on premise.

#### 4.1.5.1.4 Data Access Control

PACS and VNA solutions often support a "multitenant" concept to allow for different departments, clinics, or hospitals within a larger healthcare system. These applications may implement or integrate with directory services that allow solutions administrators to provide access based on role or business function. This project used role-based access control capabilities found in the Philips IntelliSpace and Hyland Acuo systems. For this project, the VNA plays a vital role for managing medical images across the simulated HDO. The VNA manages, retrieves, and stores medical images to a cloud storage provider. Access to the data in the storage account is managed through access keys and policies.

#### 4.1.6 Network Control and Security

This project continued with the network zoning and segmentation concepts established in NIST SP 1800-8 and built on those concepts by implementing several tools to advance protective and detective capabilities. As examples of these enhancements, this project deployed a next-generation firewall, introduced microsegmentation, and implemented behavioral analytics in its network control and security in its approach. Subsections below provide additional information on these topics.

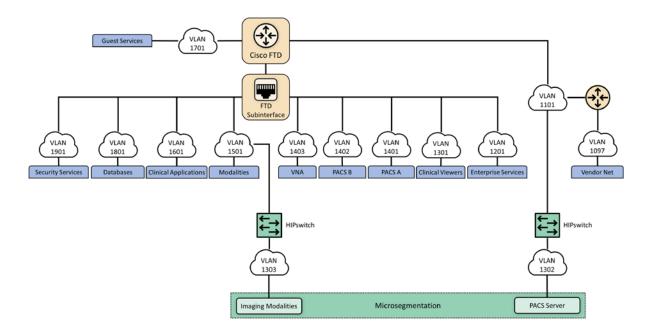
#### 4.1.6.1 Network Segmentation and VLANs

The PACS ecosystem is made up of a variety of different devices with independent requirements to ensure proper functionality. While some devices may require network access to remote services, others may operate effectively with limited connectivity outside their subnet. To meet these needs, we implemented VLANs to segment the PACS network based on devices of similar needs and functionalities. This complies with the concept of network zoning introduced in NIST SP 1800-8 [21]. With this approach, we eliminated inherent trust between VLANs. The project allowed devices to communicate with only trusted devices based on carefully crafted network policies.

The PACS project implemented the architecture described in <u>Section 4.1</u> by constructing a network that was segmented into VLANs. The project limited the implementation to the main components necessary for the PACS ecosystem. The project segmented the network into the following VLANs:

- vendor net
- enterprise services
- clinical viewers
- PACS A
- PACS B
- modalities
- clinical applications
- guest services
- databases
- remote storage
- security services

This project established segmentation through virtualization, with separate subnets implemented for each VLAN listed above. The project placed each VLAN behind a router/firewall that implements policies defined by VLAN's purpose. Figure 4-5 below depicts the network architecture.



#### Figure 4-5 NCCoE Lab Environment Network Architecture

#### 4.1.6.2 Firewall and Control Policies

This project used Cisco's Firepower Next Generation Firewall (NGFW). The NGFW provides several features that combine features previously found in separate perimeter security products such as intrusion prevention systems, application firewalls, proxy servers, and network packet inspection tools. The NGFW allows integration of other tools to defend the network against malicious activity.

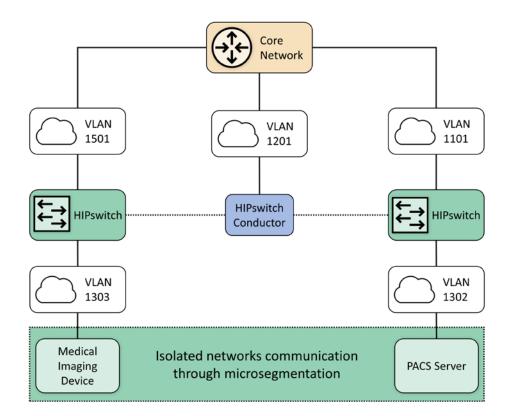
As network and application attacks become more advanced, network controls should be enhanced beyond stateful traffic filtering. NGFW goes beyond ports, protocols, and IP addresses, providing standard policy-based protection, while including more advanced tools such as intrusion prevention systems, application filtering, uniform resource locator (URL) filtering, and geo-location blocking. The PACS ecosystem faces a variety of threats from different sources, and a comprehensive approach to network security is vital. The lab implemented network zoning by using policy and configuration settings through Firepower. This allowed the project to implement network zoning and proactive network traffic filtering.

#### 4.1.6.3 Microsegmentation

Microsegmentation uses software-defined networking (SDN) to create a virtual overlay network over the existing network infrastructure. Devices may be grouped based on usage, with developed policies that establish granular degrees of trust. This project implemented the SDN overlay using host identity protocol (HIP) over the existing network infrastructure and offers in-transit network encryption. This project used microsegmentation to establish network control for modalities. Modalities represent medical imaging devices. These endpoint devices may contain exploitable vulnerabilities and may not have practical means to mitigate compromise beyond network protection. While VLAN-defined network zoning may afford network protection, this guide implements microsegmentation for these medical devices to reduce VLAN management complexity and provide more robust network segregation for medical devices. A microsegmentation approach may offer a solution that requires less impact to network configuration while limiting adverse interaction with the modalities.

This practice guide implemented microsegmentation through Tempered Networks' HIP solution that includes HIPswitches implementing HIP, as described in the Internet Engineering Task Force (IETF) request for comments 4423 [27]. HIP provides a cryptographically defined host identifier bound to endpoints rather than IP addresses. Network traffic between HIP-enabled endpoints traverses a series of HIPswitches deployed in the lab network infrastructure, creating a cloaked network that operates on top of the physical network. The cloaked network uses advanced encryption standard (AES)-256 encryption to secure data in transit and uses secure hash algorithm (SHA)-256 to authenticate data packets from HIP-enabled endpoints [27], [28], [29]. Figure 4-6 below depicts the microsegmentation architecture deployed in the project's test build.

#### **Figure 4-6 Microsegmentation Architecture**



While VLAN segmentation can help reduce unwanted lateral movement within a network, it does not restrict lateral movement within that zone. For some devices and workloads, it may be necessary to isolate their operations and allow only a select few interactions with other devices. The project team determined that microsegmentation would be an appropriate control to protect medical imaging devices that may operate embedded operating systems or firmware where patch release cycles may be different from current commercial off-the-shelf operating systems. Microsegmentation provides this fine-grained approach to isolation and can be implemented within an existing network.

Within the PACS ecosystem, we identified an area where microsegmentation would improve operational security. This guide implements microsegmentation through a solution based on HIP. HIP uses cryptographic host identifiers rather than IP addresses to address and authenticate endpoints and to create secure tunnels. This guide uses this concept to abstract IP addressing away from the modalities, using identity-defined perimeters where endpoint devices are authenticated to HIPswitches and allow secure tunnel communications to other HIPswitches [27].

For this practice guide's architecture, it was important to secure this line of communication and ensure that appropriate defenses protect devices from potential threats. To accomplish this, the project

established two identity-defined perimeters on two separate VLANs. This project then placed a modality behind one perimeter and a PACS behind the other. This project configured these perimeters to allow only authorized traffic between them, meaning the modality was allowed to communicate only with the PACS and vice versa. Additionally, the project encrypted all traffic between the two perimeters, ensuring the data were secure in-transit.

#### 4.1.6.4 Anomalies and Events Detection (Behavioral Analytics)

Medical devices often operate within strict requirements and limited resources. This makes certain tasks like vulnerability assessment difficult to manage, as they often require obtrusive operations such as a host-installed agent. Network-based behavioral analytics can perform the same assessments, identifying suspicious operations without affecting medical device function or performance. Behavioral analytics is an automated feature that collects and analyzes network traffic flow and compares the results to a pre-established baseline to determine whether devices are operating abnormally.

For the PACS architecture, the project identified network flows, primarily among PACS, VNA, and modalities, where it is important to monitor for abnormal behavior. With a baseline established, the project can identify when endpoints attempt to conduct network operations outside their normal profile. With this information, we can verify and remediate the threat. The project implemented the Zingbox IoT Guardian solution.

#### 4.1.6.5 Intrusion Detection and Prevention Systems

Components managed through an HDO's IT operations team would implement control mechanisms to perform malware detection, vulnerability scanning, and remediation. This project involved several workstations (e.g., image viewing devices), as well as servers that may operate commercially available operating systems. This project deployed host-based agents, as appropriate, to permit the IT team to perform regular vulnerability scanning for those non-modality systems. This project implemented Symantec Endpoint Protection on image viewing workstations. Also, the project implemented the Cisco Firepower NGFW that included a network-based intrusion prevention mechanism [30].

#### 4.1.7 Endpoint Protection and Security

This practice guide implements endpoint protection and security through device hardening and configuration controls. Protected endpoints include both workstations and servers. This project used several workstations to represent clinical workstations and used medical image viewers as the means to connect to the PACS and VNA servers. The project deployed endpoint protection to servers by installing Symantec Endpoint Protection as the automated solution addressing vulnerability management requirements. The practice guide installed Tripwire Enterprise for configuration management on the servers.

**Endpoints represent potential targets for malicious actors, and assuring appropriate control** is critical to enterprise risk management. Automated tools that leverage endpoint-deployed agents that process policy may provide HDOs greater asset control and limit potential compromise.

#### 4.1.8 Device Hardening and Configuration

This project deployed Tripwire Enterprise on server components (e.g., the Hyland Acuo server and the Philips IntelliSpace server) to address device hardening and configuration management.

This project deployed a host intrusion prevention system (HIPS) to protect servers performing critical functions in the HDO. The HIPS tool prevents the internals of an operating system from performing unintended or malicious activity. This mechanism can provide further protection from attackers attempting to compromise the system by preventing installation or execution of malicious software. This tool supports policy-based rules for monitoring file system changes of critical operating system application and system file directories. This allows the tool to monitor critical settings of the operating system, such as Windows registry keys. In our environment, we used these tools to ensure that new executables were not installed, thus reducing the attack surface of critical systems.

In conjunction with HIPS, a FIM system protects clinical servers in the reference architecture. This system monitors file system changes, looking for suspicious changes. The FIM system also evaluates policy compliance to ensure the critical servers comply with the HDO policies.

#### 4.1.8.1 Malware Detection

An endpoint-based malware detection system, commonly referred to as anti-virus software, prevents, detects, and removes malicious software from systems. This function is critical to protecting the systems that healthcare professionals use to interact with the PACS, such as the imaging workstations. The anti-virus software implemented in our reference architecture analyzes suspicious behavior, performs firewall functions, and allows custom, policy-based enforcement. These added functions enhance the ability for HDOs to respond to the threat of malicious software on healthcare systems. This practice guide deployed the Symantec Endpoint Protection solution on workstations hosting our DICOM image viewers.

A network-based malware detection system, commonly referred to as an intrusion detection system (IDS), detects malicious activity over the network. In our reference architecture, the IDS interfaces directly with the manager of the endpoint-based malware detection system. This gives the IDS the ability to use data collected from the endpoint to better detect malicious activity on the network [30].

#### 4.1.9 Data Security

This project considered challenges associated with data loss and data alteration. A challenge noted while looking at the medical imaging ecosystem is the diversity of data types that may be prone to varying threat types, with compromise resulting in different adverse outcomes. This project examined data

flows between the implemented components and identified a need to secure data in-transit and data atrest.

#### 4.1.9.1 Data Encryption (at-rest and in-transit)

Microsoft Azure provides cloud storage for this practice guide. Encrypted network sessions between the HDO and the cloud storage provider use TLS, Internet Protocol Security (IPSec) and Internet Key Exchange (IKE). Azure assigns a storage account to the HDO. Access to medical images stored in the cloud service requires storage account credentials. Azure enforces storage account access control using HTTPS with TLS, Perfect Forward Secrecy, and Rivest-Shamir-Adleman (RSA) cryptosystem 2048-bit encryption keys. Azure assures data-at-rest encryption using service-managed keys. Azure encrypts partitions or blocks of data using AES-256 bit keys [31].

This practice guide recommends referring to NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events* [32], for measures that address backup and recovery. This project implemented PACS and VNA solutions on Windows servers, and this practice guide recommends implementing secure server message block best practices, e.g., as provided by Department of Homeland Security Cybersecurity and Infrastructure Security Agency [33].

Examining the communications traffic flow, the project team determined that relevant data are sensitive in nature. Medical images and accompanying clinical notes and diagnoses are PHI and have requirements that align with confidentiality, integrity, and availability.

This project authenticates communications from the modalities to the PACS and VNA using HIP, which also provides network encryption. HIP employs AES-256 encryption [27], [28], [29] to secure network sessions. By deploying HIP, this project sought to defend against network-borne attacks, including manin-the-middle attacks where data may be altered in transit.

When multiple PACS data were aggregated into the VNA, the project enabled TLS tunneling. TLS uses DigiCert TLS certificates to implement AES-256 network encryption [28], [29], [35].

Image viewers, as well as mobile devices using Hyland's PACSgear scanning tool, use https/TLS when connecting and communicating to the VNA or PACS respectively [35].

#### 4.1.10 Remote Access

Both healthcare and IT systems require access by vendor-support technicians for remote configuration, maintenance, patching, and updates to software and firmware. The project used a remote access network segment to provide these external privileged users with privileged access to these components that reside within our reference architecture. A virtual private network (VPN) solution provides a secure way in which an organization can extend its private network across the internet, ensuring that only properly authenticated users can access their organization's private network. This project configured

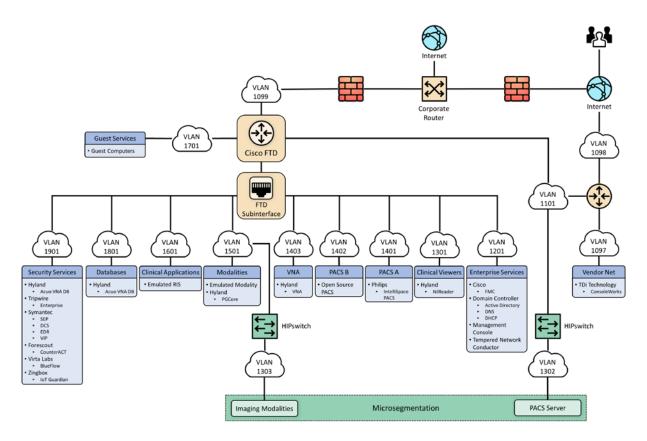
and managed the NCCOE VPN in our environment using vendor-recommended practices [36]. This project implemented TDi ConsoleWorks as a remote access mechanism into the infrastructure.

To further secure access to remote resources, the team implemented a privileged access management (PAM) solution [24]. The PAM solution provides two-factor authentication (2FA), fine-grained access control, and monitoring user access to remote resources. 2FA is provided via domain-based username and password and an application-based security token available on the user's mobile device. This project implemented 2FA in the test build using Symantec Validation and ID Protection (VIP) solution. The project integrated Symantec VIP into the ConsoleWorks authentication mechanism to enforce username password plus onetime passcode to make up the two factors.

#### 4.2 Final Architecture

The target architecture, depicted in Figure 4-7, demonstrates control measures such as microsegmentation and network segmentation as described by this practice guide. The architecture depicts network zones using VLANs, with the modalities zone implemented using microsegmentation. The target architecture also includes using cloud storage for long-term archiving and serves to enhance resiliency and recoverability should the HDO be subject to an adverse event.

#### **Figure 4-7 PACS Final Architecture**



# **5** Security Characteristic Analysis

The purpose of the security characteristic analysis is to understand the extent to which the project meets its objective of demonstrating the security capabilities described in the reference architecture in <u>Section 4</u>. This evaluation focuses on the security of the reference design itself. In addition, it seeks to understand the security benefits and drawbacks of the example solution.

#### **5.1 Assumptions and Limitations**

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

#### 5.2 Scenarios and Findings

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard cited in reference to a subcategory. The cited sections provide validation points that the example solution would be expected to exhibit. Using the Cybersecurity Framework subcategories as a basis for organizing our analysis allowed us to systematically consider how well the reference design supports the intended security characteristics.

## 5.3 Analysis of the Reference Design's Support for Cybersecurity Framework Subcategories

Using the NIST Cybersecurity Framework subcategories to organize our analysis also 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 [8].

Table 3-5 lists the reference design functions and the security characteristics, along with products that we used to instantiate each capability. The focus of the security evaluation is not on these specific products but on the Cybersecurity Framework subcategories. There may be other commercially available products that meet the objectives found in the NIST Cybersecurity Framework. Practitioners may substitute other products that provide comparable security control within the reference design.

#### 5.3.1 Asset Management (ID.AM)

This practice guide considered ID.AM-1, ID.AM-2, ID.AM-4, and ID.AM-5 to address asset management.

The practice guide implemented ID.AM-1 using Virta Labs BlueFlow to address modality asset management. Establishing an asset inventory is a fundamental component in determining appropriate controls for the environment. The ID.AM-1 Subcategory specifies, "[p]hysical devices and systems within the organization are inventoried," and ID.AM-2 specifies, "[s]oftware platforms and applications within the organization are inventoried." This practice guide groups the ID.AM-1 and ID.AM-2 subcategories together. The practice guide identifies tools that align with objectives defined by one or more of the Cybersecurity Framework subcategories. Physical devices include workstation, server, and storage components, whereas software assets include those applications that run on the physical components.

The practice guide emulates HDOs in that HDOs often have separate biomedical engineering teams, distinct from central IT operations. The implication is that IT general assets and medical devices may have distinct asset-tracking mechanisms. BlueFlow captures inventory, configuration, and patch management information.

ID.AM-4 specifies, "[e]xternal information systems are catalogued." The Clearwater Information Risk Management Analysis tool would track cloud services as part of the IT asset inventory.

Medical device asset tracking may be distinct from what is maintained in a general IT asset database. For this project, the team maintained simulated medical imaging devices and implemented the Virta Labs BlueFlow tool for asset tracking and configuration management.

ID.AM-5 specifies, "[r]esources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value." To address ID.AM-5, this project implemented solutions to identify communication and data flows between IT and biomedical engineering assets. The project implemented the Zingbox IoT Guardian and Cisco Stealthwatch solution to analyze NetFlow traffic across the laboratory infrastructure. In capturing NetFlow patterns, the project provided two primary benefits: 1) a baseline of communication flows between medical imaging devices, workstations, and PACS/VNA systems, and 2) an ability to determine when communication patterns were anomalous.

#### 5.3.2 Risk Assessment (ID.RA)

This project selected ID.RA-1 and ID.RA-5 to address the Risk Assessment category. ID.RA-1 specifies, "[a]sset vulnerabilities are identified and documented," and ID.RA-5 specifies "[t]hreats, vulnerabilities, likelihoods, and impacts are used to determine risk." The project identified and deployed tools to address these control requirements.

This project used Symantec's Endpoint Protection solution to address threats to image viewer workstations. The project used Tripwire Enterprise to monitor server assets. This practice guide implemented Virta Labs BlueFlow to manage and assess medical imaging devices. The project also used Zingbox IoT Guardian to perform NetFlow analysis. Practitioners may use information from these tools when needed to determine the risk profile of the HDO environment.

#### 5.3.3 Identity Management and Access Control (PR.AC)

To implement identity management and access control, the project team focused on PR.AC-1, PR.AC-4, and PR.AC-7 Subcategories. PR.AC-1 specifies, "[i]dentities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes." PR.AC-4 specifies, "[a]ccess permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties." PR-AC7 specifies, "[u]sers, devices, and other assets are authenticated commensurate with the risk of the transaction."

#### 5.3.3.1 Identity Management

The project used Microsoft Active Directory to provision human user access to workstations and systems. This project implemented the Symantec VIP. The Symantec VIP tool gave the project multifactor authentication (MFA) capability. MFA enhances non-repudiation within the authentication

process. MFA provides additional factors, apart from a password, that assures that when an individual presents a credential, they are doing so appropriately. For further information on MFA, practitioners may consult with NIST 800-63-3 Digital Identity Guidelines [34]. Table 5-1 describes how the project managed different user types and describes some general characteristics of that user type.

User Type	Identity	ΤοοΙ	Characteristics
Human Users	Active Directory	Active Directory	Human user authentication method dependent on interaction type
Medical Imaging Devices	Host Identifier	Tempered Networks IDN	Imaging devices abstracted from the production network over a cloaked network implementing HIP
System to System	Certificate	DigiCert Managed PKI	Automated interactions between systems authenticated
HDO to Cloud Storage Provider	Access Keys; Azure Active Directory	Microsoft Azure	Authentication to cloud storage provider is provided using access keys.

This project emulated medical imaging devices. They authenticate using HIP, implemented in Tempered Networks' microsegmentation capability. The Tempered Networks solution, IDN, uses the HIP, which incorporates a key exchange capability between endpoint devices and gateways, or HIPswitches.

The practice guide included a document scan utility installed on a mobile device. To enable device authentication in this case, the project used DigiCert Managed PKI, providing certificate-based authentication.

The project augmented device authorization management by limiting PACS accessibility based on workstation zone provisioning. The practice guide installed Symantec VIP to enable multifactor authentication for certain devices. The practice guide secured network sessions with TLS applying DigiCert-issued certificates [35].

#### 5.3.3.2 Access Control

To implement PR.AC-4, this project used role-based access control (RBAC) features built into the PACS and the VNA systems. Philips IntelliSpace and Hyland Acuo VNA implement RBAC, allowing least privilege access enforcement.

This project also took advantage of the network zoning concept and limited access based on firewall policies that restrict traffic between different zones. For example, the project limited image viewer

workstation network traffic to the PACS and VNA for image retrieval and interaction to specified network zones.

Administrative functions are restricted and are performed through TDi ConsoleWorks sessions that enforce multifactor authentication.

The project implemented PR.AC-3 using TDi Technologies ConsoleWorks to provide remote access to the lab network. The ConsoleWorks environment provided a solution for vendor remote access as well as general user remote VPN, including access by third-party medical imaging services that may need access to patient images [36].

To implement PR.AC-5, the project made significant use of network segmentation through VLANs implemented with Cisco Firepower NGFW and through microsegmentation implemented using Tempered Networks IDN. Identity Defined Networking (IDN) implements an SDN that this project used to secure communications between the simulated medical imaging devices and the PACS/VNA environment.

The project managed access to Azure resources in two ways. Management plane functions, which include creation, modification, and deletion of cloud resources, are protected using Azure AD and RBAC. Best practices for management plane access include least privilege, MFA, and secure administrative workstations. Access to services inside Azure resources is referred to as data plane functions. Authentication at this layer occurs in multiple ways. For storage accounts, authentication occurs using access keys and policies. The interaction between storage accounts and the Key Vault for encryption key retrieval uses Azure Active Directory.

#### 5.3.4 Data Security (PR.DS)

For this project, the team identified PR.DS-1, "[d]ata-at-rest is protected;" PR.DS-2, "[d]ata-in-transit is protected;" PR.DS-6, "[i]ntegrity checking mechanisms are used to verify software, firmware, and information integrity" subcategories to address data security.

This practice guide implements Microsoft Azure for cloud storage. The HDO environment establishes a TLS tunnel using digital certificates that Azure manages. The TLS tunnel assures data-in-transit protection. Azure also implements AES-256 encryption for data-at-rest.

The project installed Symantec Encryption Platform to protect workstations in this practice guide.

This project implemented TLS and HIP to assure data in-transit protection. Image viewing workstations connecting to the PACS/VNA environments use TLS encryption to ensure data-in-transit protection [27], [28], [35]. This project also implements microsegmentation with Tempered Networks and ensures data-in-transit protection by HIP-managed encryption between emulated medical imaging devices and the PACS/VNA environment.

The practice guide uses Tripwire Enterprise and Symantec DCS:SA to provide integrity monitoring of system software files.

PR.DS-6 includes a control objective to additionally manage firmware; however, the lab used emulated medical imaging devices for its modalities, operating as virtual machines. These emulated devices did not include a firmware component.

#### 5.3.5 Information Protection and Procedures (PR.IP)

This project selected PR.IP-1, PR.IP-3, and PR.IP-4 to implement the Information Protection and Procedures Category. PR.IP-1 specifies, "[a] baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)." PR.IP-3 specifies, "[c]onfiguration change control processes are in place;" and PR.IP-4 specifies, "[b]ackups of information are conducted, maintained, and tested."

Servers supporting the PACS and VNA systems were built using guidance received from Philips and Hyland, respectively. This project regarded these configurations as baseline configurations and determined them to be based on application functionality requirements. Tripwire Enterprise monitors modifications.

Virta Labs BlueFlow manages medical imaging device configurations. The practice guide emulated medical imaging devices deployed in the lab. Emulated medical devices did not involve firmware.

## 5.3.6 Protective Technology (PR.PT)

To implement Protective Technology, this project selected PR.PT-1, PR.PT-3, and PR.PT-4. PR.PT-1 specifies, "[a]udit/log records are determined, documented, implemented, and reviewed in accordance with policy." PR.PT-3 specifies, "[t]he principle of least functionality is incorporated by configuring systems to provide only essential capabilities;" and PR.PT-4 specifies, "[c]ommunications and control networks are protected."

To address PR.PT-1, the Hyland Acuo VNA, Hyland NilRead Enterprise, Hyland PACSgear, Philips Enterprise Imaging IntelliSpace PACS, and Philips Enterprise Imaging Universal Data Manager components provided the capability to create audit log records.

The practice guide implemented Zingbox IoT Guardian to assure regular network traffic monitoring. The tool aggregated NetFlow traffic across the lab environment and performed behavioral analytics. HDOs should also consider using a security incident event management (SIEM) system that would aggregate logs from different operating systems, applications, and component types. SIEM tools often can support scripts that may trigger alerting to incident response teams.

To address PR.PT-3, this project implemented operating systems that were configured with the minimum functionality necessary to support PACS and VNA operations, based on guidance from Hyland

and Philips, respectively. These collaborators provided configuration recommendations that were applied as baseline settings. The practice guide then used Tripwire Enterprise to monitor this baseline.

This project implements PR.PT-4 through constructing network zones with VLANs and using the Tempered Networks microsegmentation solution. The project used VLANs to establish a base set of network zones, and the Tempered Networks IDN created a means to control network traffic between the simulated medical imaging devices and the PACS/VNA leveraging the HIP, which protects data on networks via data encryption.

The project used the Cisco Firepower NGFW to protect the infrastructure from malicious activity.

TLS and IPsec tunneling protected external connections where appropriate [35], [36].

# 5.3.7 Anomalies and Events (DE.AE) and Security Continuous Monitoring (DE.CM)

This project grouped together the Functions DE.AE Anomalies and Events and DE.CM Security Continuous Monitoring. The project then selected DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-5, DE.CM-1, DE.CM-3, and DE.CM-7 to address these control areas.

Selected controls for DE.AE Anomalies and Events include DE.AE-1: "[a] baseline of network operations and expected data flows for users and systems is established and managed"; DE.AE-2: "[d]etected events are analyzed to understand attack targets and methods"; DE.AE-3: "[e]vent data are collected and correlated from multiple sources and sensors"; and DE.AE-5: "[i]ncident alert thresholds are established." This project implemented Zingbox IoT Guardian and Cisco Stealthwatch to achieve these objectives through implementing behavioral analytics. The practice guide configured Zingbox for continuous monitoring by directing NetFlow traffic to its cloud-hosted back end where it performed analysis. The practice guide configured Stealthwatch for monitoring and analysis on-premise.

DE.CM-1 specifies, "[t]he network is monitored to detect potential cybersecurity events"; DE.CM-3: "[p]ersonnel activity is monitored to detect potential cybersecurity events"; and DE.CM-7: "[m]onitoring for unauthorized personnel, connections, devices, and software is performed." The project addresses DE.CM-1 through the Zingbox and Stealthwatch implementations. The solutions perform network monitoring and cybersecurity event detection by analyzing NetFlow traffic. The project performed additional network monitoring using the Cisco Firepower Next Generation Firewall deployment.

DE.CM-4 specifies, "[m]alicious code is detected"; and DE.CM-7 specifies, "[m]onitoring for unauthorized personnel, connection, devices, and software is performed." This project implemented Symantec Endpoint Protection to address DE.CM-4 and DE.CM-7. The practice guide implemented intrusion prevention with the Cisco Firepower Next Generation Firewall. The practice guide deployed Symantec Endpoint Protection on workstations, including image viewer workstations.

#### 5.4 Security Analysis Summary

The practice guide's reference design implementation of security surrounding the PACS/VNA helps reduce risk from the PACS/VNA, even when practitioners identify vulnerabilities in a PACS or VNA. The key feature is the multilayered security capabilities defined in <u>Section 4.1.3</u>. This practice guide followed our collaborative partners' recommended security practices to harden devices and systems; monitor traffic; limit access to only authorized users, devices, and systems; and ensure data security across the ecosystem. Any organization following this guide must conduct its own analysis of how to employ the elements discussed here, in its own environment. It is essential that organizations follow security best practices to address potential vulnerabilities and to minimize any risk to the operational network.

# **6** 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 PACS and VNA functions.

In developing a test plan, this project identified implemented cybersecurity controls and identified a method to demonstrate control functionality. Also, this project identified five IHE use case scenarios that implemented multiple cybersecurity controls to augment business process functionality. The identified scenarios found in <u>Section 3.4.3</u> served as the basis of a functional test plan to demonstrate overall security control efficacy.

<u>Section 6.1</u> describes the format and components of the functional test cases. Each functional test case is designed to assess the security capabilities of the example implementation to perform the functions listed in <u>Section 4.1.3</u>.

#### 6.1 PACS Functional Test Plan

Each test case consists of multiple fields that collectively identify the goal of the test, the specifics required to implement the test, and how to assess the results of the test. Table 6-1 describes each field in the test case.

Test Case Field	Description
Parent Requirement	Identifies the top-level requirement or the series of top-level
	requirements leading to the testable requirement
Testable Requirement	Drives the definition of the remainder of the test case fields and
	specifies the capability to be evaluated
Associated Cybersecurity	Lists the NIST Cybersecurity Framework Subcategories addressed by the
Framework Subcategories	test case

Table 6-1 Test Case Fields

Test Case Field	Description
Description	Describes the objective of the test case
Associated Test Cases	In some instances, a test case may be based on the outcome of (an)other test case(s). For example, analysis-based test cases produce a result that is verifiable through various means (e.g., log entries, reports, and alerts).
Preconditions	The starting state of the test case. Preconditions indicate various starting-state items, such as a specific capability configuration required or specific protocol and content.
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
Expected Results	The expected results for each variation in the test procedure
Actual Results	The observed results

#### 6.1.1 PACS Functional Evaluation Requirements

Table 6-2 identifies the PACS functional evaluation requirements addressed in the test plan and associated test cases. The evaluations are aligned with the basic architecture design and capability requirements from <u>Section 4</u>, Architecture.

**Table 6-2 Functional Evaluation Requirements** 

Capability Requirement (CR) ID	Parent Requirement	Subrequirement	Test Case
CR-1	Business workflows that support image acquisition and transfer to archival (e.g., PACS and VNA) are performed.	Sample Radiology Practice Workflows	PACS-1 PACS-11
CR-2	Asset and Inventory Management		PACS-2
CR-3	Enterprise Domain and Identity Management–Access Control		
CR-3.a		Privileged Access Management	PACS-3 PACS-10
CR-3.b		User Authentication	PACS-3 PACS-4

Capability Requirement (CR) ID	Parent Requirement	Subrequirement	Test Case
			PACS-5
			PACS-10
CR-3.c		Device and System	PACS-3
		Authentication	PACS-4
			PACS-5
			PACS-11
CR-3.d		Data Access Control	PACS-3
			PACS-5
CR-4	Network Control and Security		
CR-4.a		Network Segmentation and VLANs	PACS-7
CR-4.b		Firewall and Control Policies	PACS-7
CR-4.c		Microsegmentation	PACS-4
CR-4.d		Anomalies and Events Detection (Behavioral Analytics)	PACS-8
CR-4.e		Intrusion Detection and Prevention	PACS-9
CR-5	Endpoint Protection and Security		
CR-5.a		Device Hardening and Configuration	PACS-9
CR-5.b		Malware Detection and Prevention	PACS-9
CR-6	Data Security		
		In-Transit Encryption	PACS-4
CR-6.a			PACS-5
			PACS-12
CR-7	Remote Access	Remote Access	PACS-10

## 6.1.2 Test Case: PACS-1

Parent Requirement	(CR-1) Business workflows that support image acquisition and transfer	
Parent Requirement	to archival (e.g., PACS and VNA) are performed.	

Testable Requirement	(CR-1) Sample Radiology Practice Workflows	
Description	Demonstrate that the installed PACS can be used to acquire images from a simulated modality, store those images based on department, and view those images by using a DICOM viewer.	
Associated Test Case	N/A	
Associated Cybersecurity Framework Subcategories	N/A	
	<ul> <li>Implement PACS architecture, and test that network connections are operational.</li> <li>Configure DICOM communication between DVTk RIS Emulator and DVTk NA delity Emulator.</li> </ul>	
	<ul><li>DVTk Modality Emulator.</li><li>Load patient studies into the RIS.</li></ul>	
Preconditions	<ul> <li>Configure DICOM communication between DVTk Modality Emulator and the PACS.</li> </ul>	
	<ul> <li>Configure the DICOM viewer to connect to the PACS archiving system.</li> </ul>	
	<ul> <li>Provision and give proper permissions to user accounts.</li> </ul>	
	1. Start the DVTk RIS simulator.	
	2. Start the Modality Emulator.	
	<ol> <li>Click the Request Worklist button on the Modality Emulator to display the RIS' preinstalled patient studies.</li> </ol>	
	4. Select one of the Patient Names from the given list.	
	<ol><li>Click the enabled Store Image button to send the images for the selected patient to the connected PACS server.</li></ol>	
Procedure	<ol><li>To verify the archived images stored in the Philips PACS server, run Explorer as a Manager.</li></ol>	
	<ol> <li>Log in to the client web by using the URL https://192.168.140.131/clientweb. (Alternatively, use a thin client Philips IntelliSpace PACS Enterprise to verify the archived images.)</li> </ol>	
	<ol> <li>From the Folder List &gt; Exam Lookup, click the Search button to list the patient studies. The image for the patient selected in this test should be listed in the exam lookup view table.</li> </ol>	
Expected Posulte	<ul> <li>The user should be able to display the image by using the Philips Client Web or the Philips PACS Enterprise client.</li> </ul>	
Expected Results	Note: If you need to repeat the same procedure using the same samples, clear the stored image from the Philips PACS. The cleared	

	image stored in the <b>Default</b> folder will be moved to the <b>Exceptions</b> <b>Lookup</b> folder. Clear the image from the <b>Exceptions Lookup</b> folder as well.
Actual Results	The implemented PACS environment successfully scheduled images by using the RIS, sent and stored the images in the PACS using the modality, and viewed the stored images using a web client.

## 6.1.3 Test Case: PACS-2

Parent Requirement	(CR-2) Asset and Inventory Management	
Testable Requirement	(CR-2) Asset and Inventory Management	
Description	Demonstrate how to identify and manage medical assets.	
Associated Test Case	N/A	
Associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, ID.AM-4, ID.AM-5, ID.RA-1, ID.RA-5, PR.IP-1	
Preconditions	<ul> <li>PACS network infrastructure is operational.</li> <li>Virta Labs BlueFlow is deployed in the Security Services VLAN.</li> <li>Network groups are created in the BlueFlow interface to allow automatic organization of discovered devices.</li> </ul>	
Procedure	<ol> <li>Open a web browser, navigate to the Virta Labs BlueFlow web portal URL, and authenticate to the portal.</li> <li>Navigate to Connectors &gt; Discovery.</li> <li>Enter a subnet range (192.168.0.0/16) from which BlueFlow will discover devices.</li> <li>Click Run and allow the discovery process to populate a network group.</li> <li>Navigate to Inventory. Under Networks, click a network object, and display a list of discovered devices.</li> <li>Click a device name, navigate to the Tools tab, and click Fingerprint.</li> <li>Verify the populated information and click Run to perform a scan.</li> <li>Once the scan is complete, navigate back to the device's information page, and verify that the fingerprint tool has accurately identified information about the device such as operating system and Open TCP Ports.</li> <li>Manually fill in other information about the device if needed.</li> </ol>	

	<ul> <li>Devices are discovered within the specified subnets and appear as devices in the network group.</li> </ul>
Expected Results	<ul> <li>The fingerprint tool identifies device operating system and open transmission control protocol (TCP)ports.</li> </ul>
	<ul> <li>Device information can be modified manually.</li> </ul>
Actual Results	More than 20 new devices were discovered within the PACS VLANs. These new devices were placed automatically into predefined network segments, and devices that did not fit into a predefined network segment were placed into an <b>Other Assets</b> category. The fingerprint tool populated descriptive information for several discovered devices while all other necessary information was filled in manually.

#### 6.1.4 Test Case: PACS-3

Parent Requirement	(CR-3) Enterprise Domain and Identity Management–Access Control	
Testable Requirement	(CR-3.a) Privileged Access Management, (CR-3.b) User Authentication, (CR-3.c) Device and System Authentication, (CR-3.d) Data Access Control	
Description	Demonstrate the capability authentication to the PACS application by using enterprise active directory (AD).	
Associated Test Case	N/A	
Associated Cybersecurity Framework Subcategories	PR.AC-1, PR.AC-4, PR.AC-7	
Preconditions	<ul> <li>Domain controller has been deployed and configured in the Enterprise Services VLAN.</li> <li>The Philips PACS has been configured to incorporate the enterprise AD with a display name of AD PACS.</li> <li>Domain groups have been created and assigned proper policies and roles.</li> <li>A test user with username pacs-user has been set up in the test AD PACS.</li> </ul>	
Procedure	<ol> <li>Launch the IntelliSpace PACS application on the IntelliSpace PACS Enterprise server.</li> <li>To set the authentication source, select AD PACS from the Log on to drop-down list.</li> <li>Enter the username and password, and then click the login button to login.</li> </ol>	
Expected Results	<ul> <li>Authentication via AD PACS is successful.</li> <li>Access to patient data is based on group policy settings.</li> </ul>	

Actual Results	A PACS-user, who is in the AD, was used to test the access setup. After entering the username and the correct password to the Philips IntelliSpace PACS Enterprise login page by using the AD PACS as the authentication source, the login was successful. The PACS-user account was validated to assure that appropriate access control settings were applied.
	PACS-user authentication was further tested, first by entering an incorrect password and next by incorrectly spelling the username. These attempts failed.

### 6.1.5 Test Case: PACS-4

Parent Requirement	(CR-4) Network Control and Security (CR-6) Data Security
Testable Requirement	(CR-4.c) Microsegmentation, (CR-6.a) In-Transit Encryption
Description	Demonstrate secure transfer of medical images from modalities to archive systems by using microsegmentation.
Associated Test Case	PACS-3
Associated Cybersecurity Framework Subcategories	PR.DS-2, PR.PT-1, PR.PT-3, PR.PT-4
Preconditions	<ul> <li>Deploy and configure microsegmentation into the network infrastructure.</li> </ul>
	<ul> <li>Install, configure, and deploy modalities.</li> </ul>
	<ul> <li>Configure network connections between RIS and modalities to establish a DICOM connection.</li> </ul>
	<ul> <li>Configure network connections between modalities and PACS to establish a DICOM connection.</li> </ul>
	<ul> <li>Populate RIS with simulated patient studies.</li> </ul>
	<ul> <li>Install and configure a network traffic analyzer.</li> </ul>
Procedure	To schedule radiology patient studies with the DVTk Modality Emulator
	1. Launch the RIS Emulator desktop application and click the <b>Start</b>
	button to open a DICOM connection with the Modality Emulator.
	<ol> <li>Using the Modality Emulator, click the Request Worklist button to display a list of requested patient studies being sent from the RIS.</li> </ol>
	<ol> <li>Select a requested patient study from the list to send to the Philips PACS server.</li> </ol>

	To store patient studies on the Philips PACS server by using DVTk Modality Emulator
	<ol> <li>Click the Store Images button to send the selected patient study to the Philips PACS.</li> </ol>
	To verify that data are encrypted between the modality and the PACS
	<ol> <li>Start a packet capture with Cisco Firepower between the HIPswitches associated with the modality and the PACS, respectively. A new window will appear with attribute text boxes. For the <b>Source Host</b>, provide the IP address of the modality's HIPswitch. For the <b>Destination Host</b>, provide the IP address of the PACS HIPswitch.</li> </ol>
	<ol><li>Export the produced packet captures to a packet capture (PCAP) file.</li></ol>
	<ol> <li>Import the PCAP file into Wireshark and try to read the data captured.</li> </ol>
	<ul> <li>RIS establishes a DICOM connection with the modality to schedule patient studies.</li> </ul>
Expected Results	<ul> <li>DICOM communications channel is established between modalities and the PACS.</li> </ul>
	<ul> <li>Modality Emulator can send patient studies to the PACS.</li> </ul>
	<ul> <li>In-transit data are encrypted.</li> </ul>
Actual Results	The RIS, Modality, and the PACS succeeded in establishing DICOM connections after microsegmentation was implemented. Data being transferred from Modality to the PACS was encrypted through the secured connection.

## 6.1.6 Test Case: PACS-5

Parent Requirement	(CR-3) Enterprise Domain and Identity Management–Access Control (CR-6) Data Security
Testable Requirement	(CR-3.b) User Authentication, (CR-3.c) Device and System Authentication, (CR-3.d) Data Access Control, (CR-6.a) In-Transit Encryption
Description	Show how clinical departments have access to only their department's medical images and show that an encrypted connection is used when clinical departments are accessing medical images.
Associated Test Case	PACS-3

Associated Cybersecurity Framework Subcategories	PR.AC-1, PR.AC-4, PR.AC-7, PR.DS-2, PR.PT-1, PR.PT-3, PR.PT-4
Preconditions	<ul> <li>Define different clinical departments (e.g., radiology, cardiology, and dermatology).</li> <li>Create role-based access control by assigning user accounts to clinical departments.</li> <li>Configure and enable TLS connections on the PACS and VNA.</li> <li>Patient records for multiple departments are stored on the VNA.</li> </ul>
Procedure	<ul> <li>To transfer patient studies from the Philips PACS server to the radiology user group on the Hyland VNA server</li> <li>Log in to the Philips PACS to view stored patient records.</li> <li>Start a packet capture on Cisco Firepower on the PACS A interface. A new window will appear with attribute text boxes. For the Source Host, provide the IP address of the PACS. For the Destination Host, provide the IP address of the VNA.</li> <li>Select a patient study to send to Hyland VNA to be stored in the radiology department.</li> <li>Export the selected patient study to the radiology department on the Hyland VNA.</li> <li>To confirm that Hyland VNA user accounts can access only approved departments</li> <li>Log in to the Hyland VNA by using credentials with access to the radiology department's patient records.</li> <li>Verify that the patient study sent in the steps above is shown.</li> <li>Export the produced packet captures in step 2 to a PCAP file.</li> <li>Import the PCAP file into Wireshark and try to read the captured data.</li> <li>Verify that the PACS applies encryption to data in-transit and is unreadable.</li> </ul>
Expected Results	<ul> <li>The PACS transfers patient studies to a specific department group on an archiving system.</li> <li>User accounts on the archiving system are restricted to view records to assigned department.</li> <li>Data transfers from the PACS to the VNA are encrypted through TLS communication.</li> </ul>
Actual Results	PACS was able to securely transfer patient studies by using TLS encryption to the radiology group on the archiving system. User

accounts with access to view radiology patient studies were able to
access only studies linked to the radiology department.

#### 6.1.7 Test Case: PACS-6

Parent Requirement	(CR-3) Enterprise Domain and Identity Management–Access Control (CR-6) Data Security
Testable Requirement	(CR-3.b) User Authentication, (CR-3.c) Device and System Authentication, (CR-6.a) In-Transit Encryption
Description	Show how to securely review archived medical images.
Associated Test Case	PACS-3
Associated Cybersecurity Framework Subcategories	PR.AC-1, PR.AC-4, PR.AC-7, PR.DS-2, PR.PT-1, PR.PT-3, PR.PT-4
	<ul> <li>Enable https connections on a web server and outside web browser.</li> </ul>
	<ul> <li>Configure DICOM image web viewer to connect to outside web browser.</li> </ul>
Preconditions	<ul> <li>Define different clinical departments (e.g., radiology, cardiology, and dermatology), and create user accounts to correspond to clinicians who may work in those departments.</li> </ul>
	<ul> <li>Create role-based access-control by assigning user accounts to clinical departments.</li> </ul>
	To authenticate as a radiology user and securely view patient studies
	for radiology department on the VNA
Procedure	<ol> <li>Access Hyland NilRead on a web browser by using https (https://<ip address="" nilread="" of="" viewer="">).</ip></li> </ol>
	<ol> <li>Start a packet capture on Cisco Firepower on the Clinical Viewers interface. A new window will appear with attribute text boxes. For the Source Host, provide the IP address of the web viewer. For the Destination Host, provide the IP address of the client computer accessing the PACS viewer through a web browser.</li> </ol>
	3. Log in to the viewer as a radiology user.
	<ol> <li>Click the patient study record stored from Test Case 4 and verify that the viewer is using https when displaying patient images.</li> </ol>
	To evaluate encrypted data transfers from Hyland VNA to Hyland
	NilRead Viewer
	5. Export the produced packet captures in step 2 to a PCAP file.

	<ol> <li>Import the PCAP file into Wireshark and try to read the data captured.</li> <li>Verify that the VNA applies encryption to data in-transit and is unreadable.</li> </ol>
Expected Results	<ul> <li>DICOM image web viewer should be accessible and display patient images using https.</li> <li>Data sent from an archiving server to the DICOM image web viewer should be encrypted.</li> </ul>
Actual Results	Web viewer securely connected to the archiving server and transmitted patient images to a client computer over https.

#### 6.1.8 Test Case: PACS-7

Parent Requirement	(CR-4) Network Control and Security
Testable Requirement	(CR-4.a) Network Segmentation and VLANs, (CR-4.b) Firewall, and Control Policies
Description	Demonstrate network segmentation and routing between VLANs within the PACS architecture by restricting guest network access.
Associated Test Case	N/A
Associated Cybersecurity Framework Subcategories	PR.AC-5, PR.PT-1, PR.PT-3, PR.PT-4
Preconditions	<ul> <li>Domain controller is deployed and configured in the Enterprise Services VLAN.</li> <li>Windows computer is deployed to the guest network.</li> <li>Cisco FTD interfaces are configured.</li> <li>Cisco Firepower access control policy, with a default action of Block All Traffic, is created and applied to the Cisco FTD Appliance.</li> <li>Cisco Firepower access control policy is configured with the following access control rules:         <ul> <li>Allow dynamic host configuration protocol (DHCP) traffic from Guest network to Domain Controller.</li> <li>Allow DNS traffic from Guest network to Domain Controller.</li> <li>Allow http and https traffic from Guest network to wide area network (WAN) interface.</li> </ul> </li> <li>DHCP relay is configured on the Guest network interface through Firepower Management Center.</li> </ul>
Procedure	To test that DHCP services are available for Guest network 1. Power on Windows computer on the Guest network and log in.

Right-click the Windows Start button and select Network 2. Connections. 3. Right-click the **network interface** connected to the Guest network and select Properties. 4. Click Internet Protocol Version 4 (TCP/IPv4), click Properties, select Obtain an IP address automatically, then click OK. 5. Run the **Command Prompt** from the **Windows Start** button. 6. At the command line, type ipconfig /all 7. Ensure the **DHCP Enabled** is set to **Yes**. 8. Ensure the IPv4 Address, Subnet Mask, Default Gateway, and **DHCP Server** are populated according to your DHCP settings. To test that DNS services are available for Guest network 1. Right-click the **Windows Start** button and select **Network Connections.** 2. Right-click the **network interface** connected to the Guest network and select Properties. 3. Click Internet Protocol Version 4 (TCP/IPv4) and click Properties. Select Obtain the DNS server address automatically and click OK. 4. Run the Command Prompt from the Windows Start button. 5. At the command line, type ipconfig /all 6. Ensure the DNS Server is populated according to your DHCP settings. 7. At the **command line**, type nslookup 8. Verify that the **Default Address** and **Address** are populated with the correct DNS server. 9. At the prompt, type a URL (nist.gov) and ensure that an IP address (129.6.13.49) is returned by the DNS server. To test that traffic from Guest network to internal VLANs is blocked 1. Open a web browser from the Windows computer connected to the Guest network. 2. Type into the address bar an IP address (192.168.140.131) that corresponds to a PACS web server from one of the internal PACS VLANs. The web browser should not be able to retrieve the web page. 3. Right-click on the Windows Start button and select Command **Prompt.** At the **command line**, attempt to ping the VNA server from one of the internal PACS VLANs by typing ping 192.168.130.120

	<ol> <li>Ensure command prompt returns Request timed out and no packets are received.</li> </ol>
	To test that only web traffic from Guest network to the WAN is allowed
	<ol> <li>Open a web browser from the Windows computer connected to the Guest network.</li> </ol>
	2. Type a URL ( <u>https://www.nist.gov/</u> ) into the address bar.
	3. Wait for website to load properly.
	<ol> <li>Right-click the Windows Start button and select Command Prompt.</li> </ol>
	<ol> <li>At the command line, attempt to ping an external web server by typing ping nist.gov</li> </ol>
	<ol> <li>Ensure the command prompt returns Request timed out and no packets are received.</li> </ol>
Expected Results	<ul> <li>Computers with interfaces connected to the Guest network will automatically be provisioned an IPv4 address.</li> <li>Computers with interfaces connected to the Guest network will automatically be provisioned a DNS server address.</li> <li>All traffic, excluding the exceptions for DNS and DHCP, originating from the Guest network and destined for any internal PACS VLAN will be blocked.</li> <li>http and https traffic originating from the Guest network and destined for the WAN interface will be allowed.</li> </ul>
Actual Results	Upon booting up for the first time, the Windows computer on the Guest network was allocated an IPv4 address within the DHCP scope address pool and provisioned a DNS server address and was successfully able to resolve the IP address of a provided URL. The computer was not able to communicate with other devices in the internal PACS VLANs (192.168.140.131 and 192.168.130.120) using different network protocols (https and internet control message protocol) but was able to communicate with external web servers through a web browser using http and https.

# 6.1.9 Test Case: PACS-8

Parent Requirement	(CR-4) Network Control and Security
Testable Requirement	(CR-4.d) Anomalies and Events Detection (Behavioral Analytics)
Description	Demonstrate the capability to detect abnormal network traffic across the PACS architecture.
Associated Test Case	PACS-7

Associated Cybersecurity Framework Subcategories	DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-5, DE.CM-1, DE.CM-3, and DE.CM-7
Preconditions	<ul> <li>PACS architecture is implemented and network connections have been tested and are operational.</li> </ul>
	<ul> <li>Zingbox Inspector is deployed and configured in the Security Services VLAN.</li> </ul>
	<ul> <li>Virta Labs BlueFlow is deployed and configured in the Security Services VLAN.</li> </ul>
	<ol> <li>Open a web browser and navigate to the web portal of Virta Labs BlueFlow.</li> </ol>
	2. Enter credentials and log in.
	3. Navigate to Connectors > Discovery.
	<ol> <li>Enter a subnet range (192.168.0.0/16) on which BlueFlow will run an IP scan.</li> </ol>
	5. Click <b>Run</b> and wait for the discovery process to finish.
Procedure	<ol> <li>Open a web browser and navigate to the web portal of Zingbox Cloud.</li> </ol>
	7. Enter credentials and log in.
	8. Navigate to Alerts > Security Alerts.
	<ol> <li>Under Alerts, look for an alert named Suspicious internal IP scans and an alert type of scanner.</li> </ol>
	10. Expand the alert, hover over a subsection, and click View Details.
	<ol> <li>On the Alert Details page, verify that the client IP that the IP scans originated from corresponds to the BlueFlow device.</li> </ol>
Expected Results	<ul> <li>Zingbox correctly identifies BlueFlow's IP scan and creates a security alert for suspicious activity.</li> </ul>
Actual Results	Zingbox identified BlueFlow's IP scan as suspicious activity and created a security alert. Zingbox also created a security alert the second time a BlueFlow IP scan was run but stopped creating alerts for subsequent IP scans from the BlueFlow device. While the BlueFlow scan was approved and not malicious, this type of scanning can be performed by malicious devices attempting to discover devices on the network.

### 6.1.10 Test Case: PACS-9

Parent Requirement	(CR-4) Network Control and Security
	(CR-5) Endpoint Protection and Security

Testable Requirement	(CR-4.e) Intrusion Detection and Prevention, (CR-5.a) Device Hardening and Configuration, (CR-5.b) Malware Detection and Prevention
Description	Demonstrate the capability to detect threats affecting PACS servers and related end points. This test also demonstrates an intrusion detection capability.
Associated Test Case	N/A
Associated Cybersecurity Framework Subcategories	DE.CM-1, DE.CM-4, PR.PT-1, PR.PT-3, PR.PT-4
Preconditions	<ul> <li>PACS architecture is implemented and network connections have been tested and are operational.</li> <li>Symantec Endpoint Protection appliance is deployed and configured in the Security Services VLAN.</li> <li>Symantec Endpoint Protection agent is installed on an end point.</li> <li>The endpoint agent is connected to the Symantec Endpoint Protection Manager.</li> </ul>
Procedure	<ul> <li>To verify that the endpoint agent is connected to the SEP management.</li> <li><u>server</u></li> <li>1. Log in to the SEP management console (https://192.168.190.172:8443/console/apps/sepm), click Clients, and select the target group (e.g., PACS).</li> <li>2. Click the Client tab in the PACS group to list the client information in a table.</li> <li>3. The endpoint is listed under the Name column with a Health State of online.</li> <li>To verify that the endpoint receives the current policy updates</li> <li>1. Navigate to the Client tab in the SEP management console.</li> <li>2. The policy serial number should match the serial number of the endpoint found at Help &gt; Troubleshooting in the endpoint agent.</li> <li>To verify that the proper protections are enforced on the endpoint</li> <li>1. Navigate to the Client tab in the SEP management console.</li> <li>2. In the PACS group, change the drop-down list selection to Protection Technology, and review the protection categories status (enabled or disabled).</li> <li>To add a System Lockdown policy to prevent unwanted applications from running</li> <li>1. Enable the System Lockdown policy from the parent group of PACS.</li> <li>2. Select the Blacklist Mode, add a test application (e.g., <i>7zFM.exe</i>) to the list, and save the policy.</li> </ul>

	3. From the end point, click the <b>Symantec shield</b> icon, and click <b>Update Policy.</b>
	To verify that the virus and spyware protection policy works
	<ol> <li>Use a browser on the end point to download an anti-virus test file from the EICAR website (<u>https://www.eicar.org/</u>).</li> </ol>
	2. Click the image labeled <b>DOWNLOAD ANTI MALWARE TESTFILE.</b>
	3. Click the eicar.com link under <b>Download area using the secure, SSL</b> enabled protocol https.
	<ol> <li>A Symantec notification will appear, informing you that a risk is found.</li> </ol>
Expected Results	<ul> <li>Files added to this list are not allowed to be run.</li> <li>Linking to the test virus file will lead to a warning, and the threat should be locked.</li> </ul>
Actual Results	Prior to the lockdown policy enforcement, the <i>7zFM.exe</i> file and 7zFM file manager console were able to run on the end point. After the lockdown policy enforcement, the <i>7zFM.exe</i> file was not able to run, and a warning message appeared stating, "Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item."
	When accessing the malware test file, the following message appeared: "Symantec Endpoint Protection [SID:24461] Diagnostic: EICAR Standard Anti-Virus Test File detected, Symantec Service Framework."

## 6.1.11 Test Case: PACS-10

Parent Requirement	(CR-3) Enterprise Domain and Identity Management–Access Control (CR-7) Remote Access
Testable Requirement	(CR-3.a) Privileged Access Management, (CR-3.b) User Authentication
Description	Demonstrate the capability to provide controlled remote access to PACS using two-factor authentication.
Associated Test Case	PACS-3
Associated Cybersecurity Framework Subcategories	PR.AC-3
Preconditions	<ul> <li>TDi Technology ConsoleWorks is installed and configured to use active directory for username and password authentication.</li> <li>Proper access control rules, tags, and profiles are defined to allow access to necessary resources.</li> </ul>

	<ul> <li>User accounts for remote access are set up and linked to profiles set for each remote user who needs to access the PACS servers.</li> <li>Symantec VIP Enterprise Gateway is installed and integrated with ConsoleWorks by using the RADIUS connection.</li> <li>To supplement standard username/password logins on a variety of servers and services, the VIP Access mobile phone application is installed, and a credential ID has been acquired from Symantec for receiving time-sensitive tokens.</li> <li>Test user credentials are registered in the VIP manager and associated to the account.</li> </ul>
Procedure	<ol> <li><u>To verify that username/password are not sufficient to log in</u></li> <li>Use a web browser to connect to the TDi console (https://192.168.1.4:5176) and log in with username/password.</li> <li>Verify that the login is unsuccessful.</li> </ol>
	<ul> <li>To verify the two-factor authentication using username/password with a VIP token</li> <li>1. Use a browser to connect to the TDi console: (https://192.168.1.4:5176).</li> <li>2. Open the VIP Access mobile phone application. It should display a security code with a valid time duration.</li> </ul>
	<ol> <li>Log in to the TDi console with username/password followed by the VIP security token found in the mobile phone application.</li> <li><u>To verify that the user can access only the granted resources</u></li> </ol>
	<ol> <li>Select the Graphical menu to open a Graphical View.</li> <li>Check the list of graphical connections to ensure that only allowed connections are visible.</li> <li>Check each of the graphical connections by clicking Connect and varifying that the console property connects.</li> </ol>
Expected Results	<ul> <li>verifying that the console properly connects.</li> <li>Logging in to the TDi console with a valid username/password without a 2FA token should fail with the message "Invalid User Credentials."</li> <li>Logging in to the TDi console with a valid username/password with valid 2FA token should be successful.</li> <li>Authenticated user should have access to the list of approved graphical connections and should be able to connect to these servers.</li> </ul>
Actual Results	Using a pre-created Hyland user as an example, the first attempt to log in to the TDi console with only a username and password failed. The second attempt to log in, this time with a 2FA token, was successful.

From the dashboard, the Graphical View menu was opened, and only
approved graphical connections that were visible to the Hyland user
(e.g., Hyland VNA, Hyland Database). The user was able to connect to
these remote servers and authenticate with a Hyland service account.

## 6.1.12 Test Case: PACS-11

	(CR-1) Business workflows that support image archiving and retrieving
Parent Requirement Testable Requirement	from archival (e.g., PACS and VNA) are performed.
	(CR-3) Enterprise Domain and Identity Management–Access Control
	(CR-1) Sample Radiology Practice Workflows, (CR-3.c) Device and System
	Authentication
	Demonstrate that the installed PACS and the VNA system can connect to
Description	a dedicated remote cloud storage server to archive patient images.
	PACS-1
Associated Test Case	
Associated Cybersecurity	PR.AC-1, PR.AC-7
Framework Subcategories	
	<ul> <li>PACS-1 test case produces successful results that prove the PACS</li> </ul>
	created patient studies and the VNA stored the studies.
Preconditions	<ul> <li>A Microsoft Azure storage account exists.</li> </ul>
Freconditions	• The VNA contains a Microsoft Azure storage archive device instance.
	<ul> <li>The VNA radiology storage application connects to the VNA Azure</li> </ul>
	Archive device.
	1. Log in to the Hyland VNA Acuo Admin Portal.
	2. Navigate to Storage Management > Archive Devices.
	3. Add a New Azure Archive Device.
	4. Enter Microsoft Azure account information provided after creating a
	storage blob for the VNA (e.g., Account Name, Account Key)
	5. Click Test Connection.
	6. Change a few characters in the Account Key.
	7. Click Test Connection.
	To identify when images should be archived in the Azure cloud storage
Procedure	for testing purposes
	8. Log in to Hyland Acuo Admin Portal.
	9. Navigate to Storage Applications > RADIOLOGY.
	10. Click Azure Archive Device.
	11. Set the parameters for when the VNA should store patient studies in
	Microsoft Azure for archival. For testing purposes, set all parameters
	to <b>0.</b>
	12. Check Write files to archive.
	To identify how long images should stay in the cache for testing
	purposes
	purposes

	13. Log in to Hyland Acuo Admin Portal.
	14. Navigate to Storage Applications > RADIOLOGY.
	15. Click Edit Cache Cleaner Configuration.
	16. Set the parameters for how long the VNA should retain patient
	studies in the cache. For testing purposes, keep patient studies in the
	cache for <b>3 days.</b>
	17. Check Verify Archive Location Before Removing from Image Cache.
	To store images in Microsoft Azure Cloud Storage
	18. Log in to the PACS server.
	19. Select a patient study to send to Hyland VNA to store in the
	radiology department.
	20. Export the selected patient study to the radiology department on the
	Hyland VNA.
	21. The VNA will receive the patient study and automatically send the
	patient study to Microsoft Azure.
	To retrieve images stored in Microsoft Azure Cloud Storage
	22. Log in to NilRead and verify that the patient study stored is
	accessible.
	23. Open the patient study.
	24. Verify the study retrieval from cloud storage by evaluating metadata
	stored in the underlying database.
	To retrieve images stored in VNA Cache
	25. Log in to NilRead and verify that the patient study stored is
	accessible.
	26. Open the patient study.
	27. Verify the study retrieval from cache by evaluating metadata stored
	in the underlying database.
	<ul> <li>Hyland Acuo VNA should automatically store patient studies in</li> </ul>
	Microsoft Azure within the time frame identified.
Expected Results	<ul> <li>VNA should retain studies in the cache for the time frame identified.</li> </ul>
	<ul> <li>The user should be able to retrieve images stored in Microsoft Azure</li> </ul>
	cloud storage or the VNA's cache.
	Microsoft Azure successfully received and stored a patient study in the
Actual Results	dedicated storage blob. Users were able to retrieve the study stored in
	the cloud instance and in the VNA's cache.

## 6.1.13 Test Case: PACS-12

Parent Requirement	(CR-6) Data Security
Testable Requirement	(CR-6.a) In-Transit Encryption
Description	Demonstrate secure transfer of medical images from VNA to Remote
	Cloud Storage using TLS.

Associated Test Case	N/A
Associated Cybersecurity	PR.DS-2, PR.PT-4
Framework Subcategories	
Preconditions	<ul> <li>VNA and Microsoft Azure can communicate with each other.</li> <li>Microsoft Azure cloud storage instance is associated with the VNA's radiology department.</li> <li>PACS server contains simulated patient studies.</li> <li>A network traffic analyzer is set up to evaluate packet transfers between the VNA and Microsoft Azure.</li> </ul>
Procedure	<ol> <li>Log in to the PACS server.</li> <li>Select a patient study to send to Hyland VNA to store in the radiology department.</li> <li>Export the selected patient study to the radiology department on the Hyland VNA.</li> <li>Start a packet capture on Cisco Firepower on the PACS A interface. A new window will appear with attribute text boxes. For the Source Host, provide the IP address of the VNA. For the Destination Host, provide the IP address of the cloud storage blob.</li> <li>The VNA will receive the patient study and automatically store the patient study to Microsoft Azure.</li> <li>Export the packet captures produced from step 4 to a PCAP file.</li> <li>Import the PCAP file into Wireshark and try to read the data captured.</li> <li>Verify that the VNA applies encryption to data in-transit and is unreadable.</li> </ol>
Expected Results	<ul> <li>VNA utilizes TLS encryption for data transfers from the VNA to a Microsoft Azure cloud storage blob.</li> </ul>
Actual Results	VNA was able to securely transfer patient studies by using TLS encryption to the Microsoft Azure storage blob.

# 7 Future Build Considerations

The healthcare landscape continues to evolve as industry develops and adopts new technologies and services. In the medical imaging ecosystem, one such new development is the use of cloud-based enterprise imaging solutions. These solutions can help ensure data security in the event of a disaster, increase patient access to their own data, and improve efficiencies within the HDO. However, cloud-based enterprise imaging solutions may introduce new cybersecurity risks. An update to this practice guide could review the implications and potentially improve the cybersecurity of cloud-based enterprise imaging solutions.

# Appendix A List of Acronyms

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
AD	Active Directory
ARP	Address Resolution Protocol
AV	Anti-Virus
CIA	Confidentiality, Integrity, and Availability
СТ	Computed Tomography
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DNS	Domain Name System
DoS	Denial of Service
EHR	Electronic Health Record
FDA	Food and Drug Administration
FIM	File Integrity Monitoring
FTD	Firepower Threat Defense
GRC	Governance, Risk, and Compliance
HDO	Healthcare Delivery Organization
НІР	Host Identity Protocol
ΗΙΡΑΑ	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
HIS	Health Information System
HL7	Health Level 7
НТМ	Healthcare Technology Management
http	Hypertext Transfer Protocol

https	Hypertext Transfer Protocol Secure	
IDN	Identity Defined Networking	
IDS	Intrusion Detection System	
IEC	International Electrotechnical Commission	
IETF	Internet Engineering Task Force	
IHE	Integrating the Health Enterprise	
ΙοΤ	Internet of Things	
IPSec	Internet Protocol Security	
ІТ	Information Technology	
MAC	Media Access Control	
MFA	Multifactor Authentication	
MRI	Magnetic Resonance Imaging	
NCCoE	National Cybersecurity Center of Excellence	
NGFW	Next Generation Firewall	
NIST	National Institute of Standards and Technology	
PaaS	Platform as a Service	
PACS	Picture Archiving and Communication System(s)	
ΡΑΜ	Privileged Access Management	
РСАР	Packet Capture	
PET	Positron Emission Tomography	
РНІ	Protected Health Information	
РКІ	Public Key Infrastructure	
RADIUS	Remote Authentication Dial-In User Service	
RBAC	Role Based Access Control	
RIS	Radiology Information System	
RMF	Risk Management Framework	

RSA	Rivest-Shamir-Adleman	
SDN	Software Defined Networking	
SP	Special Publication	
SSE	Systems Security Engineering	
SSL/TLS	Secure Socket Layer/Transport Layer Security	
TCP/IP	Transmission Control Protocol/Internet Protocol	
URL	Uniform Resource Locator	
VIP	Validation and ID Protection	
VLAN	Virtual Local Area Network	
VNA	Vendor Neutral Archive	
VPN	Virtual Private Network	

## Appendix B References

- [1] Food and Drug Administration, "Display Devices for Diagnostic Radiology, Guidance for Industry and Food and Drug Administration Staff," Oct. 2, 2017. Available: <u>https://www.fda.gov/media/95527/download</u>.
- [2] National Electrical Manufacturers Association, PS3.1: DICOM PS3.1 2020c Introduction and Overview, 2018. Available: <u>http:/dicom.nema.org/medical/dicom/current/output/pdf/part01.pdf</u>.
- [3] DICOM. Digital Imaging and Communications in Medicine. Available: https://dicomstandard.org.
- [4] Radiology Technical Framework. Integrating the Healthcare Enterprise. Available: <u>http://www.ihe.net/Technical\_Frameworks/#radiology</u>.
- [5] R. Ross et al., Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 1, NIST, Gaithersburg, Md., Nov. 2016. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf</u>.
- [6] R. Ross et al., Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST SP 800-171 Revision 2, NIST, Gaithersburg, Md., Feb. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.
- [7] R. Petersen et al., Workforce Framework for Cybersecurity (NICE Framework), NIST SP 800-181 Revision 1, NIST, Gaithersburg, Md., Nov. 2020. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf</u>.
- [8] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, Gaithersburg, Md., Apr. 16, 2018. Available: <u>https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf</u>.
- [9] NIST. Risk Management Framework: Quick Start Guides. Available: <u>https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides</u>.
- [10] Joint Task Force Transformation Initiative, Guide for Conducting Risk Assessments, NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: <u>https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf</u>.

- [11] Joint Task Force Transformation Initiative, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf</u>.
- [12] NIST. Computer Security Resource Center. Available: https://csrc.nist.gov/glossary/term/confidentiality\_integrity\_availability.
- [13] National Cybersecurity Center of Excellence, Securing Picture Archiving and Communication System (PACS) Project Description, NIST, Gaithersburg, Md., Jan. 2018. Available: <u>https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-pacs-project-description-final.pdf</u>.
- [14] Health Level 7 International. Introduction to HL7 Standards. Available: http://www.hl7.org/implement/standards/index.cfm?ref=nav.
- [15] Joint Task Force Transformation Initiative, Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53 Revision 4, NIST, Gaithersburg, Md., Apr. 2013. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf</u>.
- [16] International Electrotechnical Commission (IEC) Technical Report (TR) 80001-2-2, Edition 1.0
   2012-07, "Application of risk management for IT networks incorporating medical devices—Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls."
- [17] U.S. Department of Health and Human Services Office for Civil Rights, HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework, Feb. 2016. Available: <u>https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf</u>.
- [18] International Organization for Standardization/International Electrotechnical Commission, "Information technology–Security techniques–Information security management systems– Requirements," ISO/IEC 27001:2013, 2013.
- [19] Picture archiving and communications system, §892.2050, July 2020. Available: <u>https://www.ecfr.gov/cgi-bin/text-</u> idx?SID=126d1713c9a312989c2173a5bdd4aaae&mc=true&node=se21.8.892\_12050&rgn=div8.
- [20] Health Level 7 International. *Clinical Document Architecture (CDA®) Release 2*. Available: <u>https://www.hl7.org/implement/standards/product\_brief.cfm?product\_id=7</u>.
- [21] G. O'Brien et al., Securing Wireless Infusion Pumps in Healthcare Delivery Organizations, NIST SP 1800-8, NIST, Gaithersburg, Md., Aug. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf.

- [22] American National Standards Institute /Association for the Advancement of Medical Instrumentation /IEC 80001-1:2010, "Application of risk management for IT networks incorporating medical devices–Part 1: Roles, responsibilities and activities."
- [23] IEC TR 80001-2-1, Edition 1.0 2012-07, "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."
- [24] K. Waltermire et al., Privileged Account Management for the Financial Services Sector, NIST SP 1800-18, NIST, Gaithersburg, Md., Sept. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-pam-nist-sp1800-18-draft.pdf.
- [25] NIST. "Easy Ways to Build a Better P@\$5wOrd. Available: <u>https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5wOrd</u>.
- [26] M. Grassi et al., *Digital Identity Guidelines*, NIST SP 800-63-3, NIST, Gaithersburg, Md., June 2017. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf</u>.
- [27] R. Moskowitz and P. Nikander, *Host Identity Protocol (HIP) Architecture*, Request for Comments 4423, May 2006. Available: <u>https://tools.ietf.org/html/rfc4423</u>.
- [28] E. Barker et al., Recommendation for Key-Derivation Methods in Key-Establishment Schemes, NIST SP 800-56C Revision 1, NIST, Gaithersburg, Md., Apr. 2018. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf</u>.
- [29] U.S. Department of Commerce, Advanced Encryption Standard (AES), NIST Federal Information Processing Standard Publication 197, Nov. 26, 2001. Available: <u>https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf</u>.
- [30] K. Scarfone and P. Mell, Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft), NIST SP 800-94 Revision 1 (Draft), NIST, Gaithersburg, Md., July 2012. Available: <u>https://csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft\_sp800-94-rev1.pdf</u>.
- [31] Microsoft, *Azure Data Encryption-at-Rest*, Apr. 2020. Available: <u>https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest.</u>
- [32] T. McBride et al., *Data Integrity: Recovering from Ransomware and Other Destructive Events*, NIST SP 1800-11, NIST, Gaithersburg, Md., Sept. 2017. Available: <u>https://www.nccoe.nist.gov/publication/1800-11/index.html</u>.
- [33] U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency. SMB Security Best Practices. Available: <u>https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices</u>.

- [34] P. Grassi et al., *Digital Identity Guidelines*, NIST SP 800-63-3, NIST, Gaithersburg, Md., Jun. 2017. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf</u>.
- [35] K. McKay and D. Cooper, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, NIST SP 800-52 Revision 2, NIST, Gaithersburg, Md., Aug. 2019. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf</u>.
- [36] E. Barker et al., *Guide to IPsec VPNs*, NIST SP 800-77 Revision 1, NIST, Gaithersburg, Md., June 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1.pdf.
- [37] Securities and Exchange Commission, Public Company Accounting Oversight Board; Notice of Filing of Proposed Rule on Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements, and Related Independence Rule and Conforming Amendments. June 7, 2007. Available: <u>https://www.sec.gov/rules/pcaob/2007/34-55876.pdf</u>.

## Appendix C Pervasive Versus Contextual Controls

This practice guide limits its scope to a defined boundary regarding scheduling, acquiring, using, and storing medical imaging and associated information for those images. Conceptually, this is bound in a medical imaging ecosystem and applies contextual controls to that ecosystem. Healthcare delivery organization (HDO) environments, however, feature greater complexity than this practice guide may address. That is, the medical imaging ecosystem resides within an enterprise infrastructure that should implement a pervasive set of controls. The project assumes that an HDO implements pervasive controls that may have material impact on mitigating the HDO's overall cybersecurity risk profile, but the project did not implement in the lab build. Pervasive controls may be inherited by systems that operate within the HDO infrastructure, but coverage may not be absolute. Therefore, practitioners may implement contextual controls to address gaps or to augment pervasive control capabilities. Pervasive controls tend to be organizational in scope, although they may also apply to specific systems and network components within the organization. Pervasive controls may be technical or procedural in nature. The pervasive control concept is borrowed from auditing frameworks that discuss the use of entity controls that have varying degrees of effects that are pervasive or have a widespread effect across an entity or organization [37].

An analogy can help explain the pervasive control concept. An individual may live in a house or apartment, which exists in a neighborhood. That neighborhood may then be part of a town or a city. The town or city may include a number of services, such as police, fire, and rescue. The town or city (or through a third-party service) may also provide utilities, such as water and electricity, to its residents. Pervasive controls are those that, while available to the house or apartment, the occupant has not implemented or have direct control over. The house or apartment may have locks, alarms, or firesuppressant devices that the occupant installed or has direct control over. Those controls are contextual to the house or apartment. In this analogy, the medical imaging ecosystem is the house that resides in an HDO town or city.

Pervasive control examples within HDOs include governance, risk, and compliance (GRC) systems that address a diverse range of functions needed to operate a cybersecurity strategy, including performance and management of enterprise risk, tracking information technology (IT) assets, incident response processes, IT disaster recovery and business continuity, and data loss prevention (DLP), which would prevent data exfiltration by using tools that are outside the picture archiving and communication system (PACS) and medical imaging ecosystem. This project implemented contextual controls pertinent to the medical imaging ecosystem and assumes implementation of pervasive controls across the enterprise. For purposes of this project, pervasive controls that we feel are material but are not implemented in the medical imaging ecosystem context pertinent to the immediate control environment of the laboratory's PACS environment are noted in Table C-1 below.

 Table C-1 Pervasive Security Controls

Cybersecurity Framework Subcategory	Description	Potential Implementation
ID.AM-1, ID.AM-2	ID.AM-1: Physical devices and systems within the organization are inventoried. ID.AM-2: Software platforms and applications within the organization are inventoried.	GRC suite that includes an asset management module. A potential tool that may address may be Clearwater Compliance IRM Analysis tool. The application of such tools would address IT general assets such as servers, workstations, and other components that may interact with the PACS environment but do not fall within the control environment established for this project. IT general assets may be managed by a centralized IT organization that is not directly involved in supporting or maintaining the PACS environment or medical imaging devices.
ID.RA-4, ID.RA-6	ID.RA-4: Potential business impacts and likelihoods are identified. ID-RA6: Risk responses are identified and periodized.	These two controls address enterprise risk management. ID.RA-4 may be addressed through implementing business impact assessments or enterprise risk assessments. ID.RA-6 considers the case where enterprise risk has been identified or where the HDO has determined that existing controls need to be enhanced or added. Those determinations are often documented in a Plan of Action and Milestones that describes tasks needing to be addressed, resources required, and milestone dates for realizing tasks. Typical control implementation to address ID.RA-4 and ID.RA-6 would include a GRC suite with an enterprise risk management module. The Clearwater Compliance IRM Analysis tool may be relevant as well.
PR.AC-2	PR.AC-2: Physical access to assets is managed and protected.	Server assets may be hosted in a data center with appropriate physical security and environmental controls.

Cybersecurity Framework Subcategory	Description	Potential Implementation
PR.DS-5	PR.DS-5: Protections against data leaks are implemented.	This control addresses the possibility of data exfiltration and may consider options wherein clinical or other sensitive data are migrated outside the HDO perimeter by using email or web services. Typical controls to be deployed at the internet border may include DLP tools. An example tool may be the Symantec DLP solution.
PR.IP-6	PR.IP-6: Data is destroyed according to policy.	This control addresses the need to destroy data as appropriate should that data reach its end of life. PACS and VNA control mechanisms would address objects within their purview, but HDOs should look at pervasive mechanisms to address when data may reside on workstations, endpoint devices, or removable media. In addressing appropriate data destruction measures, HDOs should consult National Institute of Standards and Technology Special Publication 800-88 Rev. 1, <i>Guidelines for Media Sanitation</i> .
PR.IP-9 PR.IP-10	PR.IP-9: Response plans (Incident Response and Business Continuity) and	These controls pertain to enterprise response and recovery planning, including disaster recovery, and assurance that the plans are regularly tested.
	recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. PR.IP-10: Response and recovery plans are tested.	Incident response planning may be addressed in several different ways that include establishing an incident response team, capturing data regarding reported or detected security events, and remediating. Inclusive of establishing incident response procedures, organizations may consider developing "play books" that could consist of established procedures based on determining certain threat types that may require courses of action different from standard incident handling. Recovery plans, which may consist of business
		continuity plans, and disaster recovery plans should be established. Organizations may consider maintaining these plans, including establishing play

Cybersecurity Framework Subcategory	Description	Potential Implementation
		books, as maintained out of band, e.g., in physical format or in mechanisms that provide assurance that the plans themselves are inaccessible in case of a security event. Management of such plans may be maintained in
		GRC suites that include modules designed to house such plans and establish regular testing schedules.
RS.RP-1	Response plan is executed during or after an event.	Response plans may be managed through a GRC solution. Physical copies of response plans should be maintained to allow for potential system outages.
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident.	Recovery plans may be managed through a GRC solution. Physical copies of recovery plans should be maintained to allow for potential system outages.

## Appendix D Aligning Controls Based on Threats

C/I/A	Threat Event	National Institute of Standards and Technology Cybersecurity Framework Mitigating Control
С	Abuse of credentials or	PROTECT (PR)
	insider threat	Access Control
		User Identification and Authentication
		DETECT (DE)
		Anomalies and Events Detection
		Security Continuous Monitoring
С	Credential compromise	PROTECT (PR)
		Access Control
		User Identification and Authentication
		DETECT (DE)
		Anomalies and Events Detection
		Security Continuous Monitoring
С	Data exfiltration	PROTECT (PR)
		Data Security and Privacy
		Information Protection Processes and Procedures
		Protective Technology
		DETECT (DE)
		Anomalies and Events Detection
		Security Continuous Monitoring
I	Data-in-transit disruption	PROTECT (PR)
		Data Security and Privacy
		Communications and Network Security
		DETECT (DE)
		Anomalies and Events Detection
		Security Continuous Monitoring
1	Data alteration	PROTECT (PR)
		Access Control
		Data Security and Privacy

C/I/A	Threat Event	National Institute of Standards and Technology
		Cybersecurity Framework Mitigating Control
		DETECT (DE)
		Anomalies and Events Detection
		Security Continuous Monitoring
T	Time synchronization	PROTECT (PR)
		Data Security and Privacy
		Maintenance
		Communications and Network Security
		DETECT (DE)
		Anomalies and Events Detection
		Security Continuous Monitoring
T	Introduction of malicious	PROTECT (PR)
	software	Protective Technology
		DETECT (DE)
		Anomalies and Events Detection
		Security Continuous Monitoring
T	Unintended use of service	IDENTIFY (ID)
		ID.AM-2: Software platforms and applications within the organization are inventoried.
		PROTECT (PR)
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		DETECT (DE)
		Security Continuous Monitoring
		Security continuous monitoring
Α	Data storage disruption	IDENTIFY (ID)
		ID.BE-5: Resilience requirements to support delivery of
		critical services are established for all operating states (e.g.,
		under duress/attack, during recovery, during normal operations).
		PROTECT (PR)

C/I/A	Threat Event	National Institute of Standards and Technology Cybersecurity Framework Mitigating Control
		Data Security and Privacy
		Information Protection Processes and Procedures
		Communications and Network Security
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap)
		are implemented to achieve resilience requirements in
		normal and adverse situations.
А	Network disruption	PROTECT (PR)
		Data Security and Privacy
		Communications and Network Security
		DETECT (DE)
		Anomalies and Events Detection
		Security Continuous Monitoring
А	Backup/recovery disruption	PROTECT (PR)
		Information Protection Processes and Procedures
		RECOVER (RC)
		Recovery and Restoration
А	Supply chain compromise	IDENTIFY (ID)
		ID.SC-5: Response and recovery planning and testing are
		conducted with suppliers and third-party providers.

## **NIST SPECIAL PUBLICATION 1800-24C**

# Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector

Volume C: How-To Guides

#### **Jennifer Cawthra**

National Cybersecurity Center of Excellence National Institute of Standards and Technology

Bronwyn Hodges Kevin Littlefield Chris Peloquin Sue Wang Ryan Williams Kangmin Zheng The MITRE Corporation McLean, Virginia

December 2020

**FINAL** 

This publication is available free of charge from <a href="https://doi.org/10.6028/NIST.SP.1800-24">https://doi.org/10.6028/NIST.SP.1800-24</a>

The first draft of this publication is available free of charge from <a href="https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-24-practice-guide">https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-24-practice-guide</a>





#### **DISCLAIMER**

Certain commercial entities, equipment, products, or materials may be identified by name of 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.

National Institute of Standards and Technology Special Publication 1800-24C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-24C, 255 pages, (December 2020), 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 <u>hit\_nccoe@nist.gov</u>.

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

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

### 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 information technology security—the NCCoE applies standards and best practices to develop modular, 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 Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

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

### NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) 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 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 imaging plays an important role in diagnosing and treating patients. The system that manages medical images is known as the picture archiving communication system (PACS) and is nearly ubiquitous in healthcare environments. PACS is defined by the Food and Drug Administration as a Class II device that "provides one or more capabilities relating to the acceptance, transfer, display, storage, and digital processing of medical images." PACS centralizes functions surrounding medical imaging workflows and serves as an authoritative repository of medical image information.

PACS fits within a highly complex healthcare delivery organization (HDO) environment that involves interfacing with a range of interconnected systems. PACS may connect with clinical information systems and medical devices and engage with HDO-internal and affiliated health professionals. Complexity may introduce or expose opportunities that allow malicious actors to compromise the confidentiality, integrity, and availability of a PACS ecosystem.

The NCCoE at NIST analyzed risk factors regarding a PACS ecosystem by using a risk assessment based on the NIST Risk Management Framework. The NCCoE also leveraged the NIST Cybersecurity Framework and other relevant standards to identify measures to safeguard the ecosystem. The NCCoE developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect a PACS ecosystem. This practice guide helps HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk and protect patient privacy while maintaining the performance and usability of PACS.

### **KEYWORDS**

access control; auditing; authentication; authorization; behavioral analytics; cloud storage; DICOM; EHR; electronic health records; encryption; microsegmentation; multifactor authentication; PACS; PAM; picture archiving and communication system; privileged account management; vendor neutral archive; VNA

### ACKNOWLEDGMENTS

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

Name	Organization
Matthew Hyatt	Cisco
Kevin McFadden	Cisco
Cletis McLean	Cisco
Peter Romness	Cisco
Deidre Cruit	Clearwater Compliance
Mike Nelson	DigiCert
Taylor Williams	DigiCert

Name	Organization
Andy Gray	Forescout
Katherine Gronberg	Forescout
William Canter	Hyland
Kevin Dietz	Hyland
Joseph Davis	Microsoft
Janet Jones	Microsoft
Dan Menicucci	Microsoft
Mehwish Akram	The MITRE Corporation
Steve Edson	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Donald Faatz	The MITRE Corporation
Harry Perper	The MITRE Corporation
David Alfonso	Philips Healthcare
Jonathan Bagnall	Philips Healthcare
Julian Castro	Philips Healthcare
Sukanta Das	Philips Healthcare
Jason Dupuis	Philips Healthcare
Michael McNeil	Philips Healthcare

Name	Organization
Dwayne Thaele	Philips Healthcare
Steve Kruse	Symantec
Derek Peters	Symantec
Axel Wirth	Symantec
Bill Johnson	TDi Technologies
Pam Johnson	TDi Technologies
Robert Armstrong	Tempered Networks
Nicholas Ringborg	Tempered Networks
Randy Esser	Tripwire
Onyeka Jones	Tripwire
Jim Wachhaus	Tripwire
Sandra Osafo	University of Maryland University College
Henrik Holm	Virta Labs
Michael Holt	Virta Labs
Ben Ransford	Virta Labs
Jun Du	Zingbox
Damon Mosk-Aoyama	Zingbox
David Xiao	Zingbox

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
Cisco	Cisco Firepower Version 6.3.0 Cisco Stealthwatch Version 7.0.0
Clearwater Compliance	Clearwater Information Risk Management Analysis
DigiCert	DigiCert PKI Platform
Forescout	Forescout CounterACT 8
Hyland	Hyland Acuo Vendor Neutral Archive Version 6.0.4 Hyland NilRead Enterprise Version 4.3.31.98805 Hyland PACSgear Version 4.1.0.64
<u>Microsoft</u>	Azure Active Directory Azure Key Vault Version Azure Monitor Azure Storage Azure Security Center Version Standard Azure Private Link
Philips Healthcare	Philips Enterprise Imaging Domain Controller Philips Enterprise Imaging IntelliSpace PACS Philips Enterprise Imaging Universal Data Manager
Symantec, a division of Broadcom	Symantec Endpoint Detection and Response (EDR) Version 4.1.0 Symantec Data Center Security: Server Advanced (DCS:SA) Version 6.7 Symantec Endpoint Protection (SEP 14) Version 14.2 Symantec Validation and ID Protection Version 9.8.4 Windows

Technology Partner/Collaborator	Build Involvement
TDi Technologies	TDI Technologies ConsoleWorks Version 5.1-0u1
Tempered Networks	Tempered Networks Identity Defined Networking (IDN) Conductor and HIPSwitch Version 2.1
Tripwire	Tripwire Enterprise Version 8.7
<u>Virta Labs</u>	BlueFlow Version 2.6.4
Zingbox	Zingbox IoT Guardian

## Contents

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-24.

1	Intr	oduct	ion1
	1.1	How to	DUse this Guide1
	1.2	Build C	2. Dverview
	1.3	Туроді	raphic Conventions
	1.4	Logica	Architecture Summary
2	Pro	duct lı	nstallation Guides4
	2.1	Picture	e Archiving and Communication System (PACS)4
		2.1.1	Philips IntelliSpace PACS5
		2.1.2	DCM4CHEE
	2.2	VNA	25
		2.2.1	Hyland Database Server25
		2.2.2	Hyland Acuo VNA
		2.2.3	PACSgear Core Server28
		2.2.4	Hyland NilRead37
	2.3	Secure	DICOM Communication Between PACS and VNA41
		2.3.1	Public Key Infrastructure (PKI) Certificate Creation41
		2.3.2	Public Key Infrastructure (PKI) Certification Installation43
		2.3.3	TLS Secure DICOM Configuration47
		2.3.4	PACS and VNA TLS Integration Tests55
	2.4	Modal	ities55
		2.4.1	DVTk Modality Emulator55
		2.4.2	DVTk RIS Emulator60
	2.5	Asset a	and Risk Management
		2.5.1	Virta Labs BlueFlow62
		2.5.2	Tripwire Enterprise69
	2.6	Enterp	rise Domain Identity Management95
		2.6.1	Domain Controller with AD, DNS, and DHCP96
		2.6.2	DigiCert PKI115

2.7	Netwo	ork Control and Security	122
	2.7.1	Cisco Firepower	122
	2.7.2	Cisco Stealthwatch	147
	2.7.3	Tempered Networks Identity Defined Networking (IDN)	160
	2.7.4	Zingbox IoT Guardian	
	2.7.5	Forescout CounterACT 8	
	2.7.6	Symantec Endpoint Detection and Response (EDR)	
2.8	Endpo	int Protection and Security	187
	2.8.1	Symantec Data Center Security: Server Advanced (DCS:SA)	
	2.8.2	Symantec Endpoint Protection	200
2.9	Data S	Security	212
	2.9.1	Microsoft Azure Cloud Storage	213
	2.9.2	Hyland VNA Cloud Archive Device	233
2.10	Secure	e Remote Access	237
	2.10.1	TDi Technologies ConsoleWorks	237
	2.10.2	Symantec Validation and ID Protection (VIP)	239
Append	lix A	List of Acronyms	251
Append	lix B	References	254

## **List of Figures**

Figure 1-1 PACS Final Architecture	4
Figure 2-1 Hyland Systems and Applications Connectivity	25
Figure 2-2 Architecture of Networks IDN1	61

## **List of Tables**

## **1** Introduction

The following volumes of this guide 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 re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes 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 How to Use this Guide

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 all or parts of the example implementation that was built in the National Cybersecurity Center of Excellence (NCCoE) lab. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-24A: Executive Summary
- NIST SP 1800-24B: Approach, Architecture, and Security Characteristics what we built and why
- NIST SP 1800-24C: 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 1800-24A, which describes the following topics:

- challenges that enterprises face in securing a Picture Archiving and Communication System (PACS)
- example solution built at the NCCoE
- benefits of adopting the example solution

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

- Section 3.4, Risk Assessment, describes the risk analysis we performed.
- Section 3.5, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary*, NIST SP 1800-24A, with your leadership team members to help them understand the importance of adopting standards-based, commercially available technologies that can help secure a PACS ecosystem.

**IT professionals** who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, NIST SP 1800-24C, to replicate all or parts of the build created in our lab. This How-To portion of the 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 a PACS security solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, in NIST SP 1800-24B lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to <u>hit\_nccoe@nist.gov</u>.

Acronyms used in figures can be found in Appendix A.

### **1.2 Build Overview**

The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively demonstrate the capabilities in securing a PACS ecosystem. While the project implemented PACS and vendor neutral archive (VNA) solutions as well as security controls, the environment leveraged modality emulation to simulate medical image acquisition. The project also implemented an emulated radiology information system (RIS), used to generate modality work lists and therefore, support common medical imaging workflows. The project then applied security controls to the lab environment. Refer to NIST Special Publication (SP) 1800-24B, *Approach, Architecture, and Security Characteristics,* for an explanation of why we used each technology.

## **1.3 Typographic Conventions**

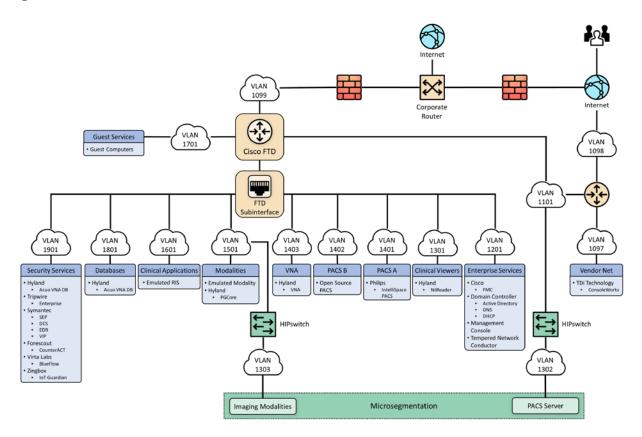
The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit.
Monospace	command-line input, onscreen computer output, sample code examples, and status codes	mkdir
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 NCCoE are available at <u>https://www.nccoe.nist.gov</u> .

## **1.4 Logical Architecture Summary**

**Figure 1-1** depicts a reference network architecture, introduced in NIST SP 1800-24B, Section 4.2, Final Architecture, which defines groupings that 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, the NCCoE identified devices and usage and grouped them by usage. The grouping facilitated network zone identification. Once zones are defined, infrastructure components may be configured so 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 PACS environment and considers the network infrastructure configuration as part of an overall defense-in-depth strategy.

#### **Figure 1-1 PACS Final Architecture**



## **2** Product Installation Guides

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

The project implemented security capabilities across the laboratory infrastructure to safeguard the emulated modalities, emulated RIS, viewer workstations, and PACS and VNA systems. Security control products that align with capabilities were implemented for the environment. Products that align with the security capabilities are enumerated in NIST 1800-24B, Section 3.6, Technologies, Table 3-5.

### 2.1 Picture Archiving and Communication System (PACS)

This project implemented two separate PACS: Philips IntelliSpace solution and an open-source PACS (DCM4CHEE). These PACS emulate the case where a healthcare delivery organization (HDO) may have different PACS vendors installed in its environment.

## 2.1.1 Philips IntelliSpace PACS

The project implemented the Philips IntelliSpace PACS solution as a central component to the lab build. IntelliSpace includes several common features, such as the ability to integrate Digital Imaging and Communications in Medicine (DICOM) and non-DICOM images and allowed the project team to emulate common medical-imaging workflow processes. The project deploys an IntelliSpace instance to receive images from an open-source modality emulator tool, which allows the project to simulate working HDO environments. The project integrates IntelliSpace with the Hyland VNA solution also installed in the lab.

#### System Requirements

The Philips IntelliSpace system consists of several components installed on different VMware virtual machines (VMs). Table 2-1 depicts base configuration requirements to construct the IntelliSpace VMs.

VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
DC1	Domain Controller (DC)	4	8 gigabytes (GB) of random access memory (RAM)	200 GB	Microsoft Windows Server 2012	Microsoft Structured Query Language (SQL) 2012, Internet Information Services (IIS) 7
IntelliSpace Server	Infrastructure, Integration, Rhapsody Health Level 7 (HL7), DICOM processor, SQL Database (DB), Anywhere Viewer (web client)	4	8 GB RAM	200 GB	Microsoft Windows Server 2012	Microsoft SQL 2012, IIS 7
Universal Data Manager (UDM)	UDM, WEB DICOM services Image Lifecycle Management	4	8 GB RAM	200 GB	Microsoft Windows Server 2012	Microsoft SQL 2012, IIS 7

Table 2-1 Base VM Configuration Requirements

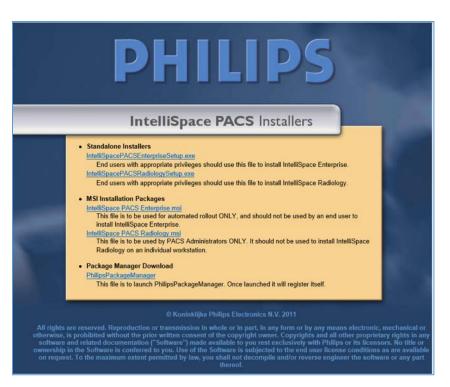
VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
	Image pre- fetching from VNA					

#### **IntelliSpace PACS Client Installation**

The project team collaborated with a team of Philips Healthcare deployment engineers to install the environment. Based on the base VM configuration requirements, the NCCoE team created the VMs by using the open virtualization format (OVF) files provided by Philips Healthcare. Philips engineers deployed the applications on the VMs and created instances for DC1, IntelliSpace server, and UDM, as noted in Table 2-1. VM instances were deployed on respective servers.

IntelliSpace PACS is a web-based distributed system. Clinicians, referring physicians, nurses, or bioengineers use web-based client applications on workstations to view, analyze, and qualify medical images. Once the server components were installed, the web-based client installation was performed using the following procedures:

- 1. Open **Internet Explorer** from a workstation and assign the IntelliSpace server with the internet protocol (IP) address 192.168.140.131. Enter the IntelliSpace server IP address in the address bar by using the following uniform resource locator (URL): https://192.168.140.131/clientweb/installers.
- 2. Select *IntelliSpacePACSEnterpriseSetup.exe* under the **Standalone Installers** bullet list of available IntelliSpace PACS Installers screen to start the installation.



3. An option to choose setup language displays. Select the **English (United States)** from the drop-down and click **OK**.

Choose	Setup Language
ٹ	Select the language for this installation from the choices below.
	English (United States)
	OK Cancel

4. After the setup language has been set, the **InstallShield Wizard** begins the installation process.



5. Use the default setting for the **Custom Setup** and click the **Next** > button that appears at the bottom of this window.

🛃 IntelliSpace PACS Enterprise 4.4.553.20 - InstallShield W	/izard X
Custom Setup Select the program features you want installed.	4
Click on an icon in the list below to change how a feature is ins	Feature Description
< >	This feature requires 166MB on your hard drive. It has 1 of 1 subfeatures selected. The subfeatures require 177KB on your hard drive.
Install to: C:\Program Files (x86)\Philips\IntelliSpace PACS Enterprise \4.4 InstallShield	Change
Help < Back	Next > Cancel

6. On the **Client Configuration Info** window, enter **192.168.140.131** as the Server IP address, and click **Install.** 

Client Configuration Info		
Please enter the Hostname or I PACS Enterprise 4.4.553.20 die	P Address of the server that the IntelliSpa ent will connect to.	ace
Server:	192.168.140.131	
nstallShield		

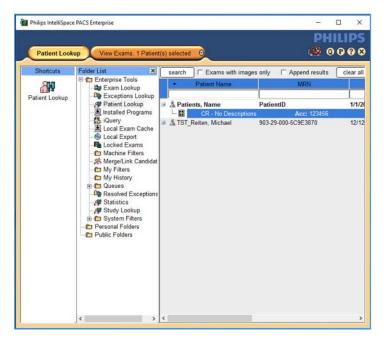
7. When installation is finished, the **InstallShield Wizard** provides a message indicating successful installation. Click **Finish.** 

🖟 IntelliSpace PACS Enterprise 4.4.553	20 - InstallShield Wizard	<
Insta	allShield Wizard Completed	
	stallShield Wizard has successfully installed IntelliSpace Enterprise 4.4.553.20. Click Finish to exit the wizard.	
	< Back Finish Cancel	

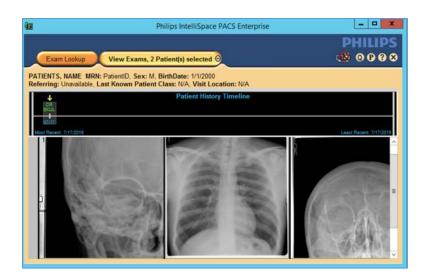
8. Once the installation is done, the installer places an **IntelliSpace PACS Enterprise** icon on the desktop. Type **Tester** in the **User Name** field and the corresponding password in the **Password** field, then click **OK** to log in.

w	elcome to IntelliSpace PACS @ NCCOE
Inte	elliSpace PACS
	IntelliSpace PACS Enterprise Logon
User Name Password Log on to Logon Mode Location	Tester AD PACS Password Main Location
	ок

9. When the program launches, the default page launches the **Patient Lookup** screen.



10. To view an exam, navigate to **Exam Lookup**, which lists a summary of a patient's exams. Double-click an exam in the list. If the exam has an image, it will be displayed. An example is below.



#### **IntelliSpace PACS Client Configuration**

Philips Deployment Engineers accomplished deployment and configuration by using PowerCLI and scripts. Other basic configurations can be implemented through the administration web page provided by the IntelliSpace PACS by using the URL https://192.168.140.131/PACSAdministration.

1. Enter the admin as the User Name, enter the proper Password, select AD PACS from the Logon to drop-down list, select Password from the Logon Mode, then click OK.

C 🕞 🧭 https://le	-	Administration/Authentication/I	-	م
	Intel	liSpace PACS Admin	nTool	
		Logon		
	User Name	admin		
	Password	•••••	-	
	Logon to	AD PACS		
	Logon Mode	November 2010		
		using Integrated Windows authen	-	
	Licogn	OK		

2. On the admin home page, add a new user by navigating to **Security**, found on the far-left column of the **Common Tasks** screen. Click **Users**, then click **Add a New User**.

PHILIPS	Common Tasks
PACS Administration	Last Successful Logon Date and Time: 6/5/2019 11:01:05 AM More Details
PACS AUTIMISCIEDU	
Security	Select a task:
Users	Add a New User
Groups Roles	Change Password Policy
Policies Authorities	Add an Authentication Source
Organizations AuditTrail	Manage Worklists Query Configuration
Worldist Configuration	
Dictionaries	
Configuration	
WorkLists	
WORKLISTS	
Sessions	
Help	
40000000	
Log Out	

- 3. To add a new user, navigate to **SECURITY**, found on the far-left column of the Common Tasks screen, and click **Users**.
  - a. Enter the User ID.
  - b. Enter the user's First Name.
  - c. Enter the user's Middle Name (optional).
  - d. Enter the user's Last Name.
  - e. Enter the user's Email Address (optional).
  - f. Assign an IntelliSpace PACS AdminTool **Password** for the user (required). Enter the password again to confirm it.

#### **Configure Sources for User Authentication**

IntelliSpace supports either a locally hosted or an external authentication source. An authentication source provides a directory structure that authenticates and manages user and group accounts. The internal authentication source, called iSite, implements a local DB of users and groups. IntelliSpace also supports a lightweight directory access protocol (LDAP) server connected to a Microsoft Active Directory (AD). The external user authentication is used as the configuration source. The following steps describe how to create an LDAP authentication source:

1. From the navigation bar, click the **Security** button, then click **Authorities.** 

	Name 🔺			Description	
	AD PACS				
Security	ISITE				
rs ups					
ups IS					
cies					
horities					
anizations					
itTrail					
klist Configuration					
Dictionaries					
onfiguration					
onfiguration					
		New	Edit Tes	t Delete	
WorkLists					
WORKEISES					
Sessions					
Sessions					

2. Click **New** to open the External Authentication Source wizard.

Administration General Informat	tion	
guration rkLists ssions telp	Back Next Cancel	

- 3. On the External Authentication Source page, set the following values, then click Next.
  - a. Set Authority Name to AD.PACS.HCLAB.
  - b. Set the Display Name to AD PACS.
  - c. Select HostName for Name Resolution.
  - d. Check the box next to Enabled.

e. Check the box next to **Show** in **Login Screen**.

tion General Informa	tion	
Authority Name	AD.PACS.HCLAB	-
Display Name:	AD PACS	
Description:		-
Name Resolution:	HostName	
	I Enabled	-
	Show in Login Screen	
	Show in Login Screen	
ion		
		-
	Back Next Cancel	

4. In the Advanced Directory Configuration, set DNS Host Name as ad.pacs.hclab and Port as 389.

ILIPS	Host Query Configur	ation			
					-
	DNS Host Name: ad.pa	acs.hclab			
curity	Port: 389				-
ties					
ations					
il .					1
Configuration					
ionaries					·
iguration )					
			Back Nex	t Cancel	
rkLists			Back Nex	Cancel	
ssions					
ssions					

5. Navigate to the Edit External Authentication Source screen. In this project, the Directory Type is ActiveDirectory, and the Supported Credentials is Password. Click Save to save the settings.

inistration Advanced Director	y Configuration		
Directory Typ	e: ActiveDirectory	~	
ity Authenticatio	n: Negotiate	~	
Search Roo	ot: DC=pacs, DC=hclab		-
Support	ed Password		
Credentia	Is: Certificates		
Referral Chasin	g: None	~	
iguration			
nries			
			1000
ation			
	Ba	ck Save Cancel	
	Da	ck Save Cancer	
sts			
SIS			
ists			

6. The interface provides a test feature to allow engineers to determine connectivity with the external authentication source. From the navigation bar, select **Security > Authorities.** Click the name of the **External Authentication Source,** and click **Test.** 

PHILIPS	Test External Authentication Source	
PACS Administration	External Realm	
Security	Authority Name: AD.PACS.HCLAB Name: AD PACS Description:	
Users		
Groups	Test Account	
Roles Policies	Username and Password	
Authorities		
Organizations	User Name:	
AuditTrail Worklist Configuration	Password:	
Dictionaries Configuration WorkLists Sessions	Test Cancel	
Help		

#### **Configure Connection to Modality Emulator**

We used the open-source DVTk Modality Emulator as a modality for testing the communication between IntelliSpace PACS and a modality. Installation of the DVTk Modality Emulator can be found in <u>Section 2.4.1</u>. The following procedures configure several components. These components include the

Radiology information system (RIS), modality performed procedure step manager (MPPS manager), and PACS/Workstation systems storage.

1. From the DVTk Modality application, click the **Configure Emulator** tab to set up a proper **System Name**, e.g., **Modality**; an application entity title **(AE Title)**, e.g., **DVTK\_MODALITY**; and a communication **Listen Port**, e.g., **104** for the emulator itself.

Pč	Modality Emulator
File Help	
% 🗐 🖏 🛅 🍩 🗕 🕈 =	
Control Activity Logging Configure	Emulator   Worklist Query   MPPS-Progress   MPPS-Discontinued   MPPS-Completed   Image Stora
System Name:	Modaity
AE Title:	DVTK_MODALITY
Implementation Class UID:	12826.0.1.3680043.2.1545.6.3.1.0
Implementation Version Name:	ModalityEmulator
Local IP Address:	::1 <b>v</b>
Listen Port.	104
Storage Commit Mode	
In Single Association (S	ync commitment)
C In Different Association	(Async commitment)
Wait time for N-EVENT-REPOR	T from PACS (in sec):

From the DVTk Modality application, click the Remote Systems tab to configure the remote systems, including RIS System, MPPS Manager, and PACS/Workstation Systems. Information for each system's IP address as well as the port number is needed. Particularly, the AE Title for the Philips IntelliSpace PACS is required for the AE Title field. These are the input values:

#### **RIS System**

- IP Address: 192.168.160.201
- Remote Port: 105
- AE Title: DVTK\_RIS

#### **MPPS Manager**

- IP Address: 192.168.160.201
- Remote Port: 108
- AE Title: DVTK\_MPPS

#### PACS/Workstation Systems–Storage Config

- IP Address: 192.168.140.131
- Remote Port: 104
- AE Title: STENTOR\_SCP

#### PACS/Workstation Systems–Storage Commit Config

- IP Address: 192.168.140.131
- Remote Port: 104
- **AE Title:** STENTOR\_SCU

		Modality Emulator	
le Help			
Sector States	● ← ↑ →		
ontrol Activity	Logging Configure Remote Systems		
RIS System			
IP Address:	192.168.160.201		
Remote Port:	105		
AE Title:	DVTK_RIS		
MPPS Manager			
IP Address:	192.168.160.201		
Remote Port:	108		
AE Title:	DVTK_MPPS		
PACS/Workstati Storage Config		Store C	Commit Config
IP Address:	192.168.140.131	IP Addr	
Remote Port:	104	Remote	e Port. 104
AE Title:	STENTOR_SCP	AE Titl	e: STENTOR_SCU

- To configure the Philips IntelliSpace PACS AE Title and communication port, log on to the iSite Administration web site by using the URL https://192.168.140.131/iSiteWeb. Select Configure > DICOM > General, set the following values, and then click Save to save the settings.
  - Normal AE Title: STENTOR\_SCP
  - High-Priority AE Title: STENTOR\_HI
  - **Port:** 104
  - Secure Port: 2762

PHILIPS ISite Administration			
Configure View Test			
General Storage Tasks &Logs SystemCheck	k ORefresh DB Cache ORestart DMWL	Restart All	
🗄 System	General IExport Q/R SC	P IQuery S/C SCP Im	port/Exp. Conformance
Main Location     EntergriseImageDistribution : nccess1	DICOM Support		
	Normal A ETRie		Default
	High Priority A ETitle	STENTOR_SCP	Default
	Port	104	Default
	Secure Port	2762	Default
	Replace Non Latin-1 During Import	- Enable	Default

4. To test the connectivity, go to the DVTk Emulator application, then go to the Modality Emulator home page as shown below. Click the **Ping PACS/Workstation** and **DICOM Echo** buttons to verify the success of the pings. You should receive **Ping Successful** and **DICOM Echo Successful** messages.

Ϋ́	Modality Em	ulator	_ <b>_</b> ×
File Help			
R 🖩 😫 🛅 🌚 🖛 🕇			
Control Activity Logging Conf	gure Emulator   Worklist Query   MPPS-Pro	gress MPPS-Discontinued MPPS-	Completed Image Stora
RIS System			
		Ping RIS	
No la	S.C.		
$( \mathbb{N} \mathbb{Q} ) - $		DICOM Echo	
1 POL		Request Worklist	
		Send MPPS completed	
Modality	RIS System	Hint:	
PACS/Workstation Systems -			
$\wedge$		Ping PACS/Workstation	Ping successful.
		Fing PACOMORSIBION	
(MA)	→ 🌑	DICOM Echo	DICOM Echo successful
1 Masse			
		Store Image	
¥		Storage Commitment	
Modality	PACS/Workstation	Hint	

### Configure IntelliSpace PACS to Communicate with Hyland VNA

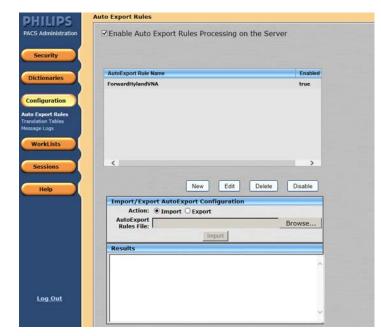
Refer to <u>Section 2.2.2</u> for detailed installation guidance for Hyland VNA.

1. Obtain the Hyland VNA AE Title and port information for communication. Log in to the iSite Administration page by using the URL https://192.168.140.131/iSiteWeb.

- 2. From the **Configure** drop-down list, select **DICOM** to open the DICOM configuration page.
- 3. Fill in the known Hyland **AE Title** (e.g., **RADIOLOGY**), **IP Address** (e.g., **192.168.130.120**), **Port** (e.g., 114), and other necessary information.

General Executions Data Management Geographical M	testifier DICOM Dankiving Di	ignation (Chambering (Chambering	meet Security Statistics Scient S	Transforms -Brurage Strategy -				
Hain Location	General IXxport Q/R SCP IQuery S/C SCP Emport/Exp. Conformance							
EnterpriseImageDistribution : nccoess1	Monitor Configuration							
	Export Destination G	lobal Export Service Web S	ervice Database					
		1912						
	RADIOLO BY Hyland VN	AE 16.	RADOLOGY					
		Description	Hy and VNA					
		17 Address	192.163.130.120					
		Put	114	U veter 1				
		Concurrent Requests	1	1				
		Recent Study on Reiny	🗌 Bhable	Rampie				
		Keep Connection Across Studies	Denace	Central				
		Location Affinity	Main Location					
		Um Seture Connection	Enable					

- 4. Log in to the IntelliSpace PACS Administration page by using https://192.168.140.131/PACSAdministration.
- 5. Click the **Configuration** button on the left panel to configure the **Auto Export Rule.**
- 6. Click the New button to create a new rule named ForwardHylandVNA.



7. Set the Trigger Type as New Data Arrival.

- 8. Set the **Receiving AE Title** as **Stentor\_SCP**, which is the AE Title for Philips IntelliSpace PACS.
- 9. Choose Hyland VNA (RADIOLOGY) from the Selected Destination box.

Rule Name ForwardHylandVNA	Administration	AutoExportRule Configuration
Trigger Type New Data Arrival V Enable Priors D Prior Criteria Modality D BodyPart No. Of Priors D Matching Criteria Modality type Manufacturer Name Sending AE title Receiving AE title STENTOR_SCP Study description Manufacturer model Referring physician's first name Referring physician's first name Reading physician's last name Reading physician's last name Reading physician's last name Study Date and Time Body Part Protocol Name		
Enable Priors   Prior Criteria    Modality    BodyPart No. Of Priors       Matching Criteria Modality type Manufacturer Name Sending AE title Receiving AE title Receiving AE title    Study description Manufacturer model Referring physician's first name Reading physician's first name Reading physician's last name Reading physi		
Prior Criteria    Modality    BodyPart No. Of Priors ]		
No. Of Priors 3 2 Matching Criteria Modality type Manufacturer Name Sending AE title Receiving AE title STENTOR_SCP Study description Manufacturer model Referring physician's first name Referring physician's last name Reading physician's last name Reading physician's last name Reading physician's last name Requested Procedure Description Study Date and Time Body Part Protocol Name		
Matching Criteria       Modality type         Manufacturer Name		
Modality type         Manufacturer Name         Sending AE title         Receiving AE title         Study description         Manufacturer model         Referring physician's first name         Reading physician's last name         Reading physician's last name         Reading physician's last name         Requested Procedure         Description         Study Date and Time         Body Part         Protocol Name		
Manufacturer Name         Sending AE title         Receiving AE title         Study description         Manufacturer model         Referring physician's first name         Referring physician's last name         Reading physician's last name         Reading physician's last name         Reading physician's last name         Requested Procedure         Description         Study Date and Time         Body Part         Protocol Name		
Sending AE title Receiving AE title Receiving AE title STENTOR_SCP Study description Manufacturer model Referring physician's first name Reading physician's first name Reading physician's first name Reading physician's last name Reading physician's first name Reading physician's first name Reading physician's last name Reading physician's first name Reading physician's last name Reading physic		Piodaity type
Receiving AE title       STENTOR_SCP         Study description		Manufacturer Name
Receiving AE title       STENTOR_SCP         Study description		Sending AE title
Study description         Manufacturer model         Referring physician's first name         Referring physician's last name         Reading physician's first name         Reading physician's last name         Reading physician's last name         Requested Procedure         Description         Study Date and Time         Body Part         Protocol Name		
Manufacturer model         Referring physician's first name         Referring physician's last name         Reading physician's first name         Reading physician's last name         Reading physician's last name         Requested Procedure         Description         Study Date and Time         Body Part         Protocol Name		Receiving AE title STENTOR_SCP
Manufacturer model         Referring physician's first name         Reading physician's last name         Reading physician's first name         Reading physician's last name         Reading physician's last name         Requested Procedure         Description         Study Date and Time         Body Part         Protocol Name		Study description
Referring physician's first name         Referring physician's last name         Reading physician's first name         Reading physician's last name         Reading physician's last name         Requested Procedure         Description         Study Date and Time         Body Part         Protocol Name		
Referring physician's last name Reading physician's first name Reading physician's last name Requested Procedure Description Study Date and Time Body Part Protocol Name		Manufacturer model
Reading physician's first name         Reading physician's last name         Requested Procedure         Description         Study Date and Time         Body Part         Protocol Name		Referring physician's first name
Reading physician's first name         Reading physician's last name         Requested Procedure         Description         Study Date and Time         Body Part         Protocol Name		
Reading physician's last name Requested Procedure Description Study Date and Time Body Part Protocol Name		Referring physician's last name
Requested Procedure Description Study Date and Time Body Part Protocol Name		Reading physician's first name
Requested Procedure Description Study Date and Time Body Part Protocol Name		Reading physician's last name
Description Study Date and Time Body Part Protocol Name		
Study Date and Time Body Part Protocol Name		
Body Part Protocol Name		
Protocol Name		Study Date and Time
		Body Part
Series Description		Protocol Name
		Series Description
Configured Export Destinations Selected Destinations		Configured Executionations Colorted Destinations

# 2.1.2 DCM4CHEE

DCM4CHEE is a collection of open-source applications that communicate with each other using DICOM and HL7 standards for clinical image management and archival. In this study, DCM4CHEE listens for connection requests from specific application entities like DVTk's Modality Emulator to receive patient

studies. DCM4CHEE will store these patient studies in a PostgreSQL DB and can archive these studies to the Hyland VNA. This build utilizes Docker to deploy the DCM4CHEE software.

#### System Requirements

- CPUs: 2
- Memory: 4 GB
- Storage: 80 GB
- Operating System: Ubuntu Linux 18.04
- Network Adapter: VLAN 1402
- Software: Docker

#### **DCM4CHEE Installation**

The guide for installing Docker on Ubuntu 18.04 can be found at [1].

- 1. Go to <u>https://github.com/dcm4che-dockerfiles/dcm4chee-arc-psql/tree/5.21.0</u> to download the software.
- 2. On the right-hand side of the page, click the **Clone** button to begin the file download.
- 3. Extract the downloaded content from the *dcm4chee-arc-psql-5.21.0.zip* file to a preferred directory.
- 4. Open a terminal with root privileges.
- 5. Navigate to the directory where the extracted content is located.
- 6. Run docker-compose up.
- 7. Open a web browser and navigate to https://localhost:8443/dcm4chee-arc/ui2.

)→ ଫ ଢ	0 🔒 https://localho	st:8443/dcm4chee-arc/ui2/#	/study/study				(\$0%)	··· 🖾 🕁	II\ 🖸 🎕
Studies Patients	MWL UWL DIFFs					1			08:17
Studies					-	-			
Patient name	C Fuzzy Matching	Study description	Modality	Sending AET of Series	Study Instance UI		Order By	Web App Service	•
Patient ID	issuer of patient	20 0	all -	Study date	Study time		SUBMIT		
		Referring physician nan	Institutional Departmer	Study Received	Study Access			C SIZE	

#### **DCM4CHEE to VNA Configuration**

- 1. Click the dark blue menu dongle (
  ) on the left-hand side of the screen.
- 2. Select Configuration.

- 3. Select AE list.
- 4. Click **New AET**, and provide the following information:
  - Name: RADIOLOGY
  - Hostname: 192.168.130.120
  - **Port:** 114
  - AE Title: RADIOLOGY
- 5. Click Apply.

gister new Application Entity		
eate new device Select existing device		
New Device		
New Network Connection RADIOLOGY		
Name	RADIOLOGY	Arbitrary/Meaningful name for the Network Connection object
Hostname	192.168.130.120	DNS name for this particular connection
Port	114 🛞	TCP/UDP port that a service is listening on. May be missing if this network connection is only used for outbound connections
letwork AE		
AE Title	RADIOLOGY	Unique AE title for this Network AE
Network Connection Reference	RADIOLOGY	JSON Painters to the Network Connection objects for this AE
AE Description		Unconstrained text description of the application entity
Application Cluster		Locally defined names for a subset of related applications
	+ Add	

### **DCM4CHEE to DVTk Modality Configuration**

- 1. In the Modality Emulator, click the **Configure Remote Systems** tab at the top of the window.
- 2. Navigate to the **PACS\Workstation Systems** section, and input the information with the following values:

#### **RIS System**

- IP Address: 192.168.140.160
- Remote Port: 105
- AE Title: RIS

#### **MPPS Manager**

- IP Address: 192.168.140.160
- Remote Port: 108

• **AE Title:** MPPS

#### PACS/Workstation System–Storage Config

- IP Address: 192.168.141.210
- **Remote Port:** 11112
- AE Title: PACS

### PACS/Workstation System–Storage Commit Config

- IP Address: 192.168.141.210
- **Remote Port:** 11112
- **AE Title:** PACS

X Modality Emi File Help	ulator		-		
	◎ ← ↑ →				
Control Configur	e Remote Systems				
RIS System					
IP Address:	192.168.140.160				
Remote Port:	105				
AE Title:	RIS				
MPPS Manager					
IP Address:	192.168.140.160				
Remote Port:	108				
AE Title:	MPPS				
PACS/Workstati		Store Commit C	onfin		
IP Address:	192.168.141.210	IP Address:	192.168.14	41.210	-
Remote Port:	11112	Remote Port:	11112		
AE Title:	DCM4CHEE	AE Title:	DCM4CHE	F	

#### DCM4CHEE View Stored Data and Archive to VNA

- 1. Click the dark blue menu dongle ( $\blacksquare$ ) on the left-hand side of the screen.
- 2. Select Navigation.
- 3. Select **DCM4CHEE** under **Web App Service** on the right-hand side of the screen.

Partnert Harnin Partnert 43	Churry Halthing Stowe of potient	Budy description		Study state	Study Indunus (20) Study Inne	Mik App Service •	
Accusate surther	labor of accession rule	-Beforning proyaction rate	Institutional Departmen	Muly Received	Mushy Access		
Hare					-	 KOCHLING, SAFETY	
	-	-				IOCH_REGULAR_USE IOCH_WIONG_MINL	-
	1				10	 -	
				-	The I		

4. Select **Submit** to see stored patient studies.

	Patient name	Chazy Matching	Study description	Modally	Sending AIT of Series		Order Ry DOMACHE	
	Patient ID Accusation mandaer	Issuer of patient	20 E Referring physician nam	et e	Study date Study Anceived	Study bine	G COUNT C	9276
ľ	How .	Search current list	More functions	Actions for selections				
ļ		Shudy ID Shudy Initian re*Secondary Cepture SC		se	udy Eats Study Time R. Ph	ysician's Name Accession No	mber Modalities Study Description	#5
h	1 1 1 3		2005 2 1 1132055956 125 1	20	200425 132418 HUM		OLE	9 3

- 5. Click the dark blue ellipsis (1) on the left-hand side of the study on the second row.
- 6. Click the **Export** ( ) icon.

Patient name	Chiazy Matching	Study description	Medality	Sending AET of Series	Stiety Instance UID	Criter By • DOM4CHEE	•
Publicit (D	insur of patient	20 3	al ·	Study date	Study Stree	SUBMIT	
Accession number	itative of accession new	Referring physician can	Inditutional Department	Study Received	Study Access	C COUNT C	SIZE .
More -	Search current list	More functions .	Actions for selections •				
	Study ID Study Instan	cr 00	91.0	Date Study Time A. Physi	ician's Name Accession Num	ber Modulities Study Description	
1 III * 11er	re "Secondary Capture SC-	d.		0			
	1 100.116.136	2005.2 1 1132055956 125.3	2020	0625 132418 HUME		KNEE	9

- 7. Select **RADIOLOGY** from the drop-down list.
- 8. Click Export.



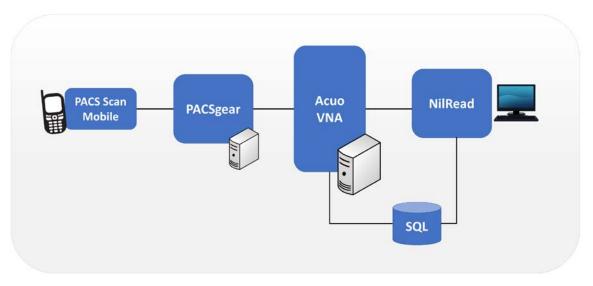
# 2.2 VNA

Hyland Acuo VNA features several different systems and applications, which include:

- Acuo VNA: core application server with services used to store, track, and retrieve digital assets stored in an archive
- PACSgear Core Server: image processing and routing server, and back-end services
- PACS Scan Mobile/Web: mobile device image acquisition and file-import application
- NilRead: enterprise image-viewing application

The diagram in Figure 2-1 shows the connectivity between the Hyland Acuo VNA systems and applications.

Figure 2-1 Hyland Systems and Applications Connectivity



Installation procedures for the above Hyland products are described in the sections that follow.

# 2.2.1 Hyland Database Server

Hyland Database Server supports operations for other Hyland products, including Hyland Acuo VNA and Hyland NilRead. The installation and configuration procedures can be found below:

### System Requirements

- **CPUs:** 4
- Memory: 12 GB RAM
- Storage:

- Hard Drive (HD)1: 80 GB (operating system [OS] installation)
- HD 2: 20 GB (DB drives)
- HD 3: 10 GB (Tx logs)
- Operating System: Microsoft Windows Server 2016
- Network Adapter: VLAN 1801

### **Hyland Database Server Installation**

Install the SQL Server 2017 according to the instructions detailed in *Install SQL Server from the Installation Wizard (Setup)* [2].

### **Hyland Database Configuration**

- The installation creates default service accounts for each service. The project used these default service accounts. User and privileged login accounts were created for the Hyland application suite and linked to unique Microsoft domain users. The project created the PACS\AcuoServiceUser and PACS\Administrator accounts.
- 2. The project implemented Windows Authentication Mode for the SQL Server.
- 3. Application DB instances were created as needed automatically when product applications were installed.
- 4. This project implemented the following DB instances through the SQL Server Management Studio: AcuoMed, HUBDB, NILDB, and PGCORE.
- 5. The project also implemented instances for OPHTHALMOLOGY, RADIOLOGY, and WOUND\_CARE.

# 2.2.2 Hyland Acuo VNA

Hyland Acuo VNA provides access to medical images and documents through interactions with a variety of different PACS, modalities, and image viewers. Acuo VNA also supports various standards, including HL7 and DICOM. The installation and configuration procedures can be found below.

## System Requirements

- **CPUs:** 6
- Memory: 12 GB RAM
- Storage:
  - HD 1: 80 GB (OS installation)
  - HD 2: 80 GB (Dilib cache drive)
  - HD 3: 500 GB (image cache drive) was installed

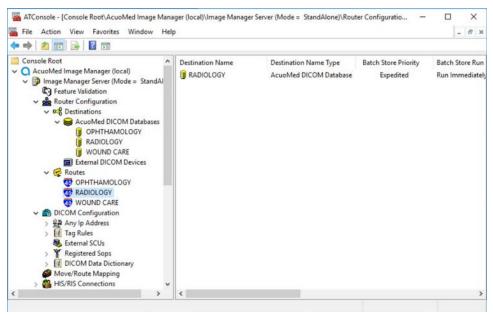
- Operating System: Microsoft Windows Server 2016
- Network Adapter: VLAN 1301

### **Hyland Acuo VNA Installation**

- 1. In the NCCoE test environment, the Hyland Acuo VNA was installed on a VM preconfigured with the OS and network requirements provided by Hyland. Engineers supplied by Hyland performed the installation.
- 2. Upon completion of the installation, three Windows services were created: AcuoMed, AcuoAudit, and AcuoStore. AcuoMed is associated with a DICOM DB containing the patient, study, and series record information that describes the images physically present on the Acuo VNA archive system. The AcuoStore also has its own DB for storing information related to bulk storage of digital images and related data, including information about the shares and about the applications that use those shares.
- 3. The installation created a web application for the AcuoAdmin Portal, where a secure sockets layer (SSL) certificate signed by DigiCert was created and assigned to the application for hypertext transfer protocol secure (https) enforcement.

### **Hyland Acuo VNA Configuration**

Hyland engineers performed configurations using the **Microsoft MMC** console and the **AcuoAdmin Portal** (https://192.168.130.120:8099/vnaweb/#1/home). The screenshots of the console management for these administration approaches are below:



To verify successful completion of the VNA installation, the Hyland engineers launched the **Acuo Administrator Portal** application from the VNA server (local host). The **Acuo Administrator Portal** screen sample is below.

		4
610		-
Patient Explorer	Workflow Manager Workflow Querues	Route Management Manage Routes, AEs and Destinations
Manage Patienta	Move Manager Store Manager	Go to Route Management
$\square$	~	Ē
Storage Management	Enterprise Reporting	Worklist
Manage Storage Applications, Shares and Archives	Survey System Reports and Trends	Manage Hit/Rit Data
Manage Storage	Enterprise Reporting	Go to Workint
	an C	4
XDS Explorer	System Management	System Diagnostics
Browse and Manage XDS Documents	View and Manage System Health	Activity Monitoring, Lags, and System Events

# 2.2.3 PACSgear Core Server

PACSgear Core Server is a capture and connectivity suite used to process DICOM and non-DICOM medical data, including patient demographics, images, videos, and HL7 messages. PACSgear Core Server can be accessed from a web browser to handle user accounts, security, and client connectivity configuration. Installation and configuration procedures are described below.

### System Requirements

- **CPUs:** 4
- Memory: 8 GB RAM
- Storage:
  - HD 1: 80 GB (OS installation)
  - HD 2: 170 GB (application)
- Operating System: Microsoft Windows Server 2016
- Network Adapter: VLAN 1501

#### **PACSgear Core Server Installation**

Hyland engineers installed the Hyland PACSgear Core Server as listed below:

- 1. Hyland engineers installed the PACSgear Core Server following their technical guidelines.
- 2. The installation created a web application for the PACSgear Core Portal, where an SSL certificate signed by DigiCert was created and assigned to the application for https enforcement.

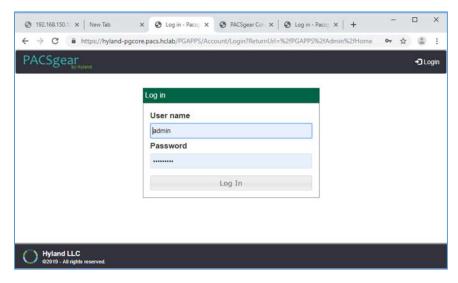
#### **PACSgear Core Server Configuration**

The Hyland engineers configured the PACSgear Core Server. The basic configuration involves managing connection settings to external devices, lookup data sources, and event trace-managing departments for multitenancy architecture, and managing user access, among many more features. Each organization will configure the PACSgear based on its specific needs.

During the DB configuration, the Hyland engineers created instances for representative departments (e.g., ophthalmology, radiology, and departments that may see patients who need wound treatment).

Add New Departments: To add the ophthalmology department, complete the following steps:

1. The Hyland engineers logged on to the PACSgear Admin portal by using https://hylandpgcore.pacs.hclab/PGAPPS/Admin.



2. On the Settings menu, select Departments.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-24

Server Status Server Version	Running 4.1.0.64		No data a	wailable in table	-		
Server Version	410.64						
Last 30 Days	¢	5 Most Rec	ent Logs		0		
Log	ogin Count	Date	Туре	Message	1		
		6/26/2019	INFO	Checking port			
		6/26/2019	INFO	Checking port done.			
-		6/26/2019	INFO	Verifying license			
Arr 29 - 24 2	12 2018 2018	6/26/2019	INFO	TCPServer: TCPServer-	-		

3. After selecting **Departments** from the **Settings** pull-down, the screen advances to a **Departments** screen. The **Departments** screen lists sample hospital departments created during the installation. The project then added a new department by clicking the **+ Add** button.

			Search:	
Default	* Name	Default Query Source		
	General			
e.	RADIOLOGY	RADIOLOGY		
	WOUND CARE	RADIOLOGY		
rowing 1 to 3 of 3 entries				Previous 1 N
+ Add				- Edit E Dele

4. After clicking the **+ Add** button, the **Add/Edit Department** screen opened and allowed the engineers to enter corresponding information.

30

Default				AE title	
lame				Modality	
				None	•
pply series	per im	age			
Destinations	XDS	Lookup Sources	Client	Series	
Destinations	AUS	Lookup Sources	Client	Selles	
	Nam	ie		Description	
	Alexandra and a	AD		RADIOLOGY DEPT	
8	VNA RA				
0	1.00000000000	D DEPT		Wound Care Department	
	1.00000000000			Wound Care Department	
	1.00000000000			Wound Care Department	
	1.00000000000			Wound Care Department	
	1.00000000000			Wound Care Department	
	1.00000000000			Wound Care Department	Cancel Save

5. In the **Name** text box, the engineers entered Ophthalmology to create a department that ties with the ophthalmology database instance created during DB configuration. Engineers also added the **AE title** as **Ophthalmology** and selected a **CT Scan** for the modality.

	tment			
Default			AE title	
			Ophthalmology	
lame			Modality	
Ophthalmology			СТ	•
Destinations	S per image	Client S	eries	
	Name		Description	
8	VNA RAD	R	ADIOLOGY DEPT	
	WOUND DEPT	W	ound Care Department	

- 6. On the **Destinations** and **Lookup Sources** tabs, the engineers set up the destination and lookup sources for each department.
- 7. On the **Client** tab, the engineers set up the client access permissions to this department's resources.

efault					AI	E title	e					
ime					м	odali	ity					
					N	lone				•		
ply series per i	mage											
estinations XDS	-	1										
ADS XDS	LOOKUP	Source	s C	lient	Serie	s						
Client	Persiste Login		s C Vide		Serie Photo Quali		Video Quali		Max. Video Lengti		Allow Came Impor	
Client	Persiste				Photo				Video	,	Came	
	Persiste Login	ent	Vide	:0	Phote Quali	o ty	Quali	ty	Video Lengti	-	Came Impor	t

- 8. On the Series tab, click Add, type a description, click Save.
- 9. Verify that the department has been added to the list, based on what is displayed.

PACSgear 🔺 нопе 🔳 мо	ab/PGAPPS/Admin/Department/Department/des	ols + 🔍 Settings + 📕 Logs + 🛛 Help +	ڭ ۵ مە
Departments			
Show 10 • entries			Search:
Default	Name	Default Query Source	
a	General		
	RADIOLOGY	RADIOLOGY	
	WOUND CARE	RADIOLOGY	
ie:	Ophthalmology	RADIOLOGY	
Showing 1 to 4 of 4 entries			Previous 1

Add LDAP/Active Directory Server: To use an LDAP/Active Directory server, configure these parameters:

- 1. Create an LDAP\_User account in Active Directory before proceeding.
- 2. Using a browser, log on to the **PACSgear Admin** portal by using https://hyland-pgcore.pacs.hclab/PGAPPS/Admin.
- 3. On the Settings menu, select Users.

	s.//hytand-pgcol	re.pacs.hclab/1	PGAPPS/Admin/Uset						<b>97</b> Q	☆	4
ACSgear	A Home E	ModLink -	PACS Scan Web •	📰 Image Link +	🗲 Tools -	O Settings -	🗖 Logs -	🛛 Help -		1	L adn
JSETS Restrict access per	missions to:					Users Connections Departments Defaults Server EHR					
	DAP Users				3	Device Provisio	oning				
Save											
ihow 10 + entri	es						Search	n: admin			
User Name					*	Group					
admin						ADMIN					
kzheng						ADMIN			24246762927		1
ihowing 1 to 2 of 2 entries									Previous	1	Ne
+ Add										# D	

4. On the Users screen, navigate to Restrict access permissions to: and click the LDAP Users button. Enter 192.168.120.100 to populate the Server text box, and then enter pacs.hclab for Domain.

PACSgear + Home ModLink - PACS Scan Web	• 🖽 Image Link •	≁ Tools •	Settings •	Logs •	🛛 Help -			, admin +
Users								
Restrict access permissions to:								
LOAD Users LDAP Users Server:								
192 168 120 100								
Domain:								
pacs.hclab								
Test Save								
Show 10 • entries				Searc	h: admin			
User Name			Group					٠
AcuoServiceUser			ADMIN					
Showing 1 to 1 of 1 entries (filtered from 2 total entries)						Previous	1	Next
+ Add							= D	
2000/02/02/02/02/02								
Hyland LLC econo - All rights reserved.								

- 5. Click the **Test** button located under the **Domain** entry box.
- 6. Enter the LDAP\_User credentials to verify connectivity to the AD.

Test LDAP Settings	ж
Username:	
LDAP_User	
Password:	

7. A message box displays indicating the test is successful. Click OK.

hyland-pgcore.pacs.hclab says	
Test Successful	

**PACS Scan Mobile Configuration:** Install and configure the PACS Scan application to an Apple iPhone by applying these steps:

- 1. On the iPhone, navigate to the **App Store.** Search for PACS Scan Mobile, from Perceptive Software. Perceptive Software is a Hyland business unit. Select the **GET** button to install the software, and then select the **OPEN** button. Select **Allow** to permit the software to send notifications.
- 2. On a workstation, log in to **PACSgear Core Server** by using the administrator credentials; a dashboard displays and provide a **Provision Device QR code**.

Status     Pluming       ef Status     Pluming       ef Status     Pluming       ef Version     4.10.94       State     No data available in table       100 Days     C       Login Count     States       0 Date     Type       Message     Station       6282019     NFO       Checking port.     States available in table	Funnting     No data available in table       4 1 0 64     No data available in table       No data available in table     Difference in table       Outer     Open in Ecology       020001     04601 Recent Logs       020011     04601 Recent Logs       020011     04601 Recent Logs       0200119     14FO
er Version 41964	4 10 94           Image: Constant State S
Lobays Count Date Type Message 6/26/2519 NFO Checking port	Count     C
Login Count Date Type Message 6/26/2019 INFO Checking port	Date         Type         Message           628/2019         N#FO         Checking port
Login Count Date Type Message 6/26/2019 INFO Checking port	Date         Type         Message           628/2019         N#FO         Checking port
Login Count Date Type Message 6/26/2019 INFO Checking port	Date         Type         Message           628/2019         N#FO         Checking port
Login Count Date Type Message 6/26/2019 INFO Checking port	Date         Type         Message           628/2019         N#FO         Checking port
0282019 INFO Checking port	Date         Type         Message           6/28/2019         INFO         Checking part           6/28/2019         INFO         Checking part done.           6/28/2019         INFO         Verifying license
	6/28/2019 INFO Checking port done. 6/28/2019 INFO Versfying license
6/26/2019 INFO Checking part done.	6/26/2019 INFO Verlývig license
6/26/2019 INFO Verifying license	JUS JUB EDEDOTS INCO TOPParter TOPParter
n 29 Jul 2 Jul 3 Jul 8 6/28/2019 INFO TCPServer: TCPServer- +	WARANT IN O IN ORDER SCOOL
evice O	
	0
	0

3. On the mobile device **PACS Scan App**, tap the Quick Response **(QR) code** icon that appears under the **Log In** button. This turns on the built-in camera on the iPhone.



- 4. Point the camera at the **QR code** on the PC screen until a message box appears indicating **Setting Updated Your settings have been updated.** This setting configures the mobile **PACS Scan application** to the address of its **PACSgear Core Server** instance.
- 5. From a workstation, acquire the trusted root certificate from DigiCert. Further information for using DigiCert is described in <u>Section 2.6.2</u>.
- 6. Download the root certificate to the workstation local drive and attach the certificate as an email attachment sent to the installer.
- 7. The installer opens the email from the iPhone and double-clicks on the attachment to install the certificate to the device.
- 8. To verify the certificate installation, go to **Settings > General > Profiles & Device Management** to list all the certificate profiles.
- 9. Find the certificate you installed and click to display the detail. An example appears below:



10. To verify the PACS Scan Mobile App functionality, from the iPhone, double-click the **PACS Scan App.** The login page displays. Use an account and password that has been associated with a clinical department to log in. Successful login displays a patient information input page, as shown below:

=	PA			-
D. C.		ACS Scan M	obile	-
Patient				
MRN	Medic	al record num	ber	
Last		ame		
First	First n	ame		
Middle	Middle	name		
DOB	Date o	f birth		x
Male		Female	Othe	r
Study				
Acc.	Acces	sion number		
Desc.				
Series				
	S	Select descrip	tion	-
SI	tandard		Confidential	
		Clear		Next

# 2.2.4 Hyland NilRead

Hyland NilRead provides image access and viewing from various devices, including clinical viewing stations, tablets, and mobile devices. NilRead also provides image manipulation, interpretation, and collaboration across departments. The installation and configuration procedures are below.

### System Requirements

- **CPUs:** 6
- Memory: 12 GB RAM
- Storage:
  - HD 1: 80 GB (OS installation)
  - HD 2: 200 GB (web application)
  - HD 3: 100 GB (image cache)
- Operating System: Microsoft Windows Server 2016
- Network Adapter: VLAN 1301

### Hyland NilRead Installation

- Hyland engineers installed Hyland NilRead based on Hyland's proprietary installation package and installation guides. NilRead has three services: Hub Front End service, Nil Back End service, and Nil Front End service. The Hub Front End service provides management service for multitenant configuration. The operation context is defined by the Nil DB content and includes user accounts, data life-cycle rules, hanging protocols, DICOM connectivity setup, and cached DICOM data index.
- 2. The installation created two web applications for the NilHub and NilRead Viewer, where SSL certificates signed by DigiCert were created and assigned to the applications for https enforcement.

#### **Hyland NilRead Configuration**

NilHub configuration is done from the NilHub web application. Launch a web browser from the NilHub server, and authenticate as admin, using the URL https://localhost:8080/, as follows:

NilHub		admin	 +) Log In	, T
		dennin	9 cog in	

1. To add a new site from the **NilHub** home page, click the **Sites** tab in the top left-hand side of the screen.

lilHub	Sites L	icenses Setting	s Logout			
Hub / Sites						
Sites		•	<b>s c</b>	£ 10 8	< +	6 6 8
Name	Code	AE Title	Partition	E-Mail	Version	State
RADIOLOGY	123	RADIOLOGY		none@yaho	4.3.31.98805	

2. Click the + icon on the right-hand side of the screen to create a new site for the **WOUND\_CARE** department, provide the information below, then click **Save.** 

- Name: WOUND\_CARE
- Details: Wound Care Department
- **Code:** 974
- AE Title: WOUND\_CARE
- VNA Partition: WOUND\_CARE
- Database Name: WOUND\_CARE
- Email: none@hyland.com

ew	
AME	
WOUND_CARE	1e0e3303-5164-4513-addin 83c(bd3h2)-5
ETAILS.	VNA PARTITION
Wound Care Department	WOUND_CARE
oor	DATABASE NAME
974	WOLAD_CAPE
E MILE	CACINE PATH
WOUND_CARE	C.WilRepository/WOUND_CARE
MAL	ENABLE SPOKE FEDERATION
none@hyland.com	<ul> <li>Address Pression</li> </ul>

3. Log back in to NilHub specifying the WOUND\_CARE Site in the top section of the login screen.

Nil	Read
Site:	WOUND_CARE
User Name:	admin
Password:	
Domain:	<b>T</b>
	Login
	r connection <u>speed</u> <sub>/pe:</sub> Auto detect

4. Click the Settings tab. Navigate to the User Management section and click Accounts.

Settings	
Preferences	
User Preferences	
<ul> <li>Workstation Preferences</li> </ul>	
<ul> <li>Modality Preferences</li> </ul>	
<ul> <li>Radiation Therapy Templates</li> </ul>	
<ul> <li>Reading Environment Verification</li> </ul>	
<ul> <li>Hanging Protocols</li> </ul>	
<ul> <li>Mouse, Keyboard And Tools</li> </ul>	
<ul> <li>Study Note Templates</li> </ul>	
<ul> <li>Assets</li> </ul>	
<ul> <li>Work Lists and Folders</li> </ul>	
<ul> <li>Confidentiality Profiles</li> </ul>	
<ul> <li>Confidentiality Masks</li> </ul>	
<ul> <li>Advanced</li> </ul>	
User Management	
<ul> <li>Profile</li> <li>Accounts</li> </ul>	

- 5. Click **Add** on the bottom left-hand side of the screen, and provide this information:
  - User Name: pacs\ptester
  - Last Name: Tester
  - First Name: Pacs
  - Role: User
  - E-Mail: ptester@hyland.pacs.com
  - Password: \*\*\*\*\*
- 6. Identify **Member Groups** to which the user needs access and click the **Add** button.
- 7. Specify the **Granted Privileges** that the user needs and click the **Grant** button.
- 8. Click the **Save** button on the bottom left-hand side of the screen.

Account				
User Name	pacs\ptester		Last Name	Tester
Role	User 🔻		First Name	Pacs
E-mail	ptester@hylan	d pacs.com	Middle Name	
Skype ID			Prefix	
Phone			Suffix	
Facility			Department	
Password			Job Description	Physician
			Expiry Date	Unlimited
	Notify on St	Invine view		
Nighlighted fields are				
Groups				
Member			Not Member	
1		-	CN=Wound_Can	e,CN=Users,DC=pacs,
			1	
		*		
		Remove	Add	
Privileges				
Granted			Revoked	
DicomQueryRetr	eve	BookmarkSaveS	end	
DicomRt EditHangingProtocols			Collaboration ContentDownloa	2
EditWorkItems *		ContentUpload		
		Revoke	Grant	
Licensing		16		
License Features				
adapterCoActiv				
adapterMach7Tec adapterTeraMedic				
advancedDataQu	alityControl			
advanced1/easur	emente			
Active Licenses				
NCCoE				
		1	nfo	
DICOM Physician N	ames			
Associated				
	1	0	A second sta	
			Associate	
Timeline data source	e access restricti	ons		
Effective permissi		ound Care V		

Hyland engineers repeated the above steps to have multiple sites that accessed different VNA partitions/tenants, such as Radiology with access to all VNA tenants and Ophthalmology with access to only the Ophthalmology VNA partition/tenant.

# 2.3 Secure DICOM Communication Between PACS and VNA

Hyland Acuo VNA and Philips IntelliSpace PACS support DICOM Transport Layer Security (TLS). DICOM TLS provides a means to secure data in transit. This project implemented DICOM TLS between the Acuo VNA and IntelliSpace PACS via mutual authentication as part of the TLS handshake protocol [3].

# 2.3.1 Public Key Infrastructure (PKI) Certificate Creation

Server/client digital certificates are created for the Hyland Acuo VNA and Philips IntelliSpace server. This project used DigiCert for certificate creation and management. The procedures that follow assume familiarity with DigiCert. Refer to <u>Section 2.6.2</u> for further detail.

## 2.3.1.1 Create PKI Certificate for Hyland Acuo VNA

- 1. Use the DigiCert Certificate Utility for Windows to generate a certificate signing request (CSR) for Hyland Acuo VNA. Information needed for requesting the certificate for Hyland Acuo VAN is below:
  - Common Name: Hyland-VNA.pacs.hclab
  - Subject Alternative Name: Hyland-VNA.pacs.hclab
  - Organization: NIST
  - Department: NCCoE
  - City: Rockville
  - State: Maryland
  - Country: USA
  - Key Size: 2048
- 2. Submit the created CSR to DigiCert portal for certificate signing.
- 3. Download and save the signed certificate along with its root certificate authority (CA) certificate in the .pem file format.
- 4. Import the saved certificate to DigiCert Certificate Utility for Windows, then export the certificate with its private key in the .pfx format.
- 5. The certificate is ready for installation.

## 2.3.1.2 Create PKI Certificate for Philips IntelliSpace PACS

- 1. Use **DigiCert Certificate Utility for Windows** to generate a CSR for PACS server. Information needed for requesting the certificate is below:
  - Common Name: nccoess1.stnccoe.isyntax.net
  - Subject Alternative Name: nccoess1.stnccoe.isyntax.net
  - Organization: NIST
  - Department: NCCoE
  - City: Rockville
  - State: Maryland
  - Country: USA
  - Key Size: 2048
- 2. Submit the created CSR to DigiCert portal for certificate signing.

- 3. Download and save the signed certificate along with its root CA certificate in the .pem format.
- 4. Import the saved certificate to **DigiCert Certificate Utility for Windows**, then export the certificate with its private key in the .pfx format.
- 5. The certificate is ready for installation.

# 2.3.2 Public Key Infrastructure (PKI) Certification Installation

After creating the signed certificates for Acuo and IntelliSpace respectively, the certificates must be installed to the servers. The steps that follow describe how to install those certificates. Certificates must be applied for each server instance and assume access to both.

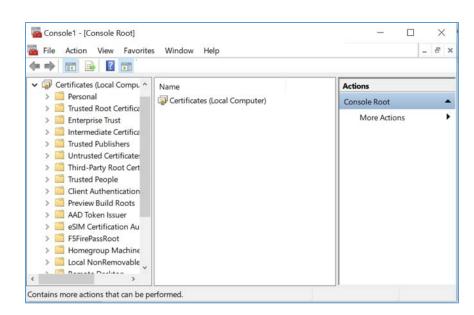
## 2.3.2.1 Install PKI Certificate for Hyland Acuo VNA

Install the certificate on Hyland Acuo VNA server by using the procedures below:

- 1. From the Acuo server, click **Start > Run > mmc.**
- 2. Select File > Add/Remove Snap-in...

	New	Ctrl+N		
	Open_	Ctrl+O		Actions
	Save	Ctrl+S	There are no items to show in this view.	Console Root
	Save As			More Actions
	Add/Remove Snap-in_	Ctrl+M		
	Options_			
	1 devingmt.msc			
	Exit			
-				

- 3. Select Certificates and click Add.
  - a. Choose Computer Account.
  - b. Choose Local Computer.
- 4. Click Finish, then click OK.



5. Once the snap-in has been added, navigate to Certificates (local computer)/Personal/Certificates.

Certificates snap-in			×
This snap-in will always manage certificates for: My user account Service account Computer account			
	< Back	Next >	Cancel

- 6. Right-click and select All Tasks/Import.
  - a. Browse to the exported .pfx certificate.
  - b. Select the file and click Open.

File	Action Vie	ew Favorites Window Help		- 8
- 🗊 c	Certificates (Loo	and the second		Actions
×	Personal	Find Certificates		Personal
	Trusted	All Tasks	> Find Certificates_	More Actions
> [	Interme	View	Request New Certificate	
2	Trusted	New Window from Here	Import	
> [	Third-P	New Taskpad View	Advanced Operations	
	Client / Preview	Refresh Export List		
2	Test Ro	Help		
2	Homegroup Remote De Certificate B Smart Card SMS	sktop Enrollmen		

- 7. Add the appropriate permissions to the newly generated certificate private key.
  - a. Navigate to **Certificates > Personal > Certificates.**
  - b. Right-click the certificate, select All Tasks > Manage Private Keys...
  - c. Add the AcuoServiceUser and grant full control permissions. Click OK.

This procedure also installs the signing root CA certificate (**DigiCert Test Root CA SHA2**) and its Intermediate Root certificate (**DigiCert Test Intermediate Root CA SHA2**) into the server computer.

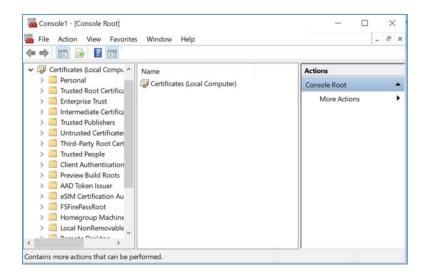
## 2.3.2.2 Install PKI Certificate for Philips IntelliSpace PACS

Install the certificate on the PACS server by using the procedures that follow:

- 1. From the IntelliSpace server, click **Start > Run > mmc.**
- 2. Select File > Add/Remove Snap-in...

iii)	File	Action View	Favorites	Window	Help	- 6 ×
4		New		Ctrl+N		
		Open		Ctrl+O		Actions
		Save		Ctrl+S	There are no items to show in this view.	Console Root
		Save As				More Actions
		Add/Remove Sna	p-in_	Ctrl+M		
		Options				
		1 devmgmt.msc				
		Exit				
			1			

- 3. Select Certificates and click Add.
  - a. Choose Computer Account.
  - b. Choose Local Computer.
  - c. Click Finish; click OK.



4. Once the snap-in has been added, navigate to Certificates (local computer)/Personal/Certificates.

Certificates snap-in			$\times$
This snap-in will always manage certificates for: O My user account Service account O Computer account			
	< Back	Next >	Cancel

- 5. Right-click and select All Tasks/Import.
  - a. Browse to the exported .pfx certificate.
  - b. Select the file and click **Open.**

	2 00 0	ew Favorites Window Help		- 8
· 🗊 d	Certificates (Loo	cal Compu ^ Object Type		Actions
~	Personal	Find Certificates_	1	Personal
-	Cer Trusted	Find Certificates_		More Actions
1	Enterpr	All Tasks	Find Certificates_	
5	Interme	View	Request New Certificate	
	Trusted		and the second	
	Untrust	New Window from Here	Import_	
5	Third-P	New Taskpad View	Advanced Operations	
>	Trusted			
>	Client /	Refresh		
2	Preview	Export List_		
>	Test Ro	Help		
>	eSIM C			
2	Homegroup			
	Remote Der Certificate 8			
1	Smart Card			
	SMS SMS	irusted k		
	31913	w.		

This procedure also installs the signing root CA certificate (**DigiCert Test Root CA SHA2**) and its Intermediate Root certificate (**DigiCert Test Intermediate Root CA SHA2**) into the server computer.

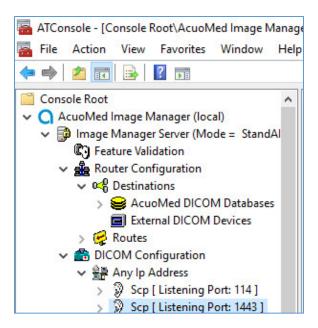
# 2.3.3 TLS Secure DICOM Configuration

With the signed certificates installed to the Acuo VNA and IntelliSpace PACS servers, proceed to configuring DICOM TLS. The procedures that follow describe TLS configuration that must be performed on both Acuo VNA and IntelliSpace PACS. This will enable DICOM TLS communications between these two end points, and secure data-in-transit communications bidirectionally between the VNA and PACS.

# 2.3.3.1 TLS Configuration for Hyland Acuo VNA

For receiving TLS DICOM messages from IntelliSpace PACS, configure a new service-class provider (SCP) in Acuo VNA using Microsoft Windows Console. Configuration is done from the Acuo VNA server.

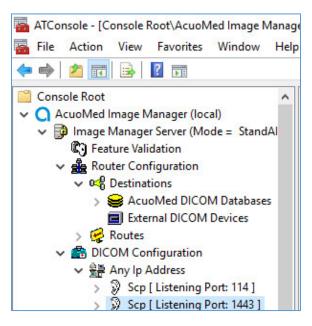
- 1. Open Microsoft MMC to access the AcuoMed Image Manager (local):
- From the Console > AcuoMed Image Manager (local) > DICOM Configuration, right-click Any IP Address > New SCP ... to create a new service class provider (SCP) for TLS encryption.



- 3. On the **Connectivity** tab of the **SCP** Properties page, provide the information below and click **Add**, **Apply**, then **Finish**:
  - Port: 1443
  - Check the **TLS** checkbox.
  - Client Certificate CN: nccoess1.stnccoe.issyntax.net
  - Server Certificate CN: HYLAND-VNA.pacs.hclab
  - Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
  - Check the Authenticate Client Certificate checkbox.

TCD (ID	
TCP/IP IP Address:	0.0.0.0
Port:	1443 🔽 TLS
	nccoess1.stnccoe.isyntax.net  Add Delete HYLAND-VNA.pacs.hclab
Cipher Suite:	TLS_RSA_WITH_AES_128_CBC_SHA

4. To add the **Called AE** to the SCP, right-click the created **SCP** [Listening Port:1443] and select New > Called AE ... to open the AE Properties form.

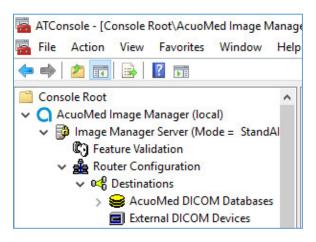


5. Fill in the **Called AE Name:** e.g., **RADIOLOGY;** and **Default Route Name:** e.g., **RADIOLOGY.** After populating the information, click **Add.** 

'n	SOP Configuration   External	CU Authorization   Options   Reconciliation	Postfetch Properties   Domain	
	AE Identification			Page Actions
	Called AE Name:	RADIOLOGY		rage Actions
	Collaborative Routing			
	*Default Route Name:	RADIOLOGY	•	
	Tag Rule Routing			
	and the second second second second	(And the Associated Reconciliation Depender	ncies):	
	Tag Rules			
	Tag Failure Houte:	<no defined="" route=""></no>	-	
	Stat Route			
		<no defined="" route=""></no>	•	
	* Immediate C-STORE proces	sing depends on the Reconciliation Settings fo	r this AF. C-STORE processing will	
	be delayed until the reconcil	iation detected problem is resolved if reconcilia	tion is set for this AE.	
		t on this route even if it does not pass reconcil	ation.	
	Storage Destination Filtering			
	Enable F	itering Tag:		

For sending a TLS DICOM message to IntelliSpace PACS, configure an External DICOM Device from the Acuo VNA by using Microsoft Windows Console.

- 1. Open Microsoft **MMC** to access the **Image Manager Server**:
- 2. Navigate to Image Manager Server > Router Configuration > External DICOM Devices, right-click External DICOM Devices, and click New.



- 3. On the **Main** tab of the **External DICOM Devices Properties** page, provide the information below and click **Apply**, then click **Finish**:
  - SCP Destination Name: PHILIPS
  - Called AE Name: STENTOR\_SCP
  - IP Address: 192.168.140.131
  - SCP Listening Port: 2762
  - Enable TLS by clicking the **TLS** checkbox next to the listening port number.
  - Called AE Name: ACUO
  - Implementation UID: 1.2.840.114158.1.1.3
  - Client Certificate CN: HYLAND-VNA.pacs.hclab
  - Server Certificate CN: nccoess1.stnccoe.isyntax.net
  - **Cipher Suite:** TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

SCP Destination Name: Page Actions  External Device  Called AE Name: STENTOR_SCP  TCP/IP Connectivity  C Host Name:  C Ip Address: 192 . 168 . 140 . 131  SCP Listening Pot: 2762  AcuoMed  Calling AE Name: ACUO	
Caled AE Name: STENTOR_SCP  TCP/IP Connectivity  C Host Name: G Ip Address: 192168140131  SCP Listening Pot: 2762 F TLS  AcuoMed	
C         Host Name:           Image: Provide the second	
C Host Name:     G  p Address: 192168140131      SCP Listening Pot: 2762	
Image: Point of the Address:         192 . 168 . 140 . 131           SCP Listening Pot:         2762           AcuoMed         Image: Point of the Poi	
Image: Point of the Address:         192 . 168 . 140 . 131           SCP Listening Port:         2762           Acuo Med         Image: Point of the Address of the Addres of the Addres of the Address of the Address of the Addres of th	
SCP Listening Pot: 2762 IF TLS	
AcuoMed	
AcuoMed	
completioned and a second seco	
Inplementation UID: 12.840.114158.1.1.3	
Version Name: AcuoMed	
TLS Settings Client Certificate CN: HYLAND-VNA pacs holds	
Server Certificate CN: In Concess 1 strucces isyntax net	
Copher Suite: TLS_RSA_WITH_AES_128_CBC_SHA	
Connection Testing	
Press the test button to validate DICOM connectivity.	
vTest	
in the second	

4. Restart the **AcuoMed** service.

## 2.3.3.2 TLS Configuration for Philips IntelliSpace PACS

Next, configure TLS on the IntelliSpace PACS server. Take the steps below to enable this feature on the PACS:

1. Access the Philips iSite Administration web site https://192.168.140.131/iSiteWeb by using administrator credentials.

C 🗇 🧭 https://localhost/iSiteWeb/Main	/Navigator 🔎 🗕 C 🧔	Navigator	×		o × n ★ 3
Configure Vea Test					-
FOrent Filection Fibri Mangement FiGeoprophical in Main Location EnterpriseImageDistribution : nccoss1	Site Information Notes:	™Mgraisa ™Montreng neccon 4.4.553.20	Cancel/Re	~	512 Transform

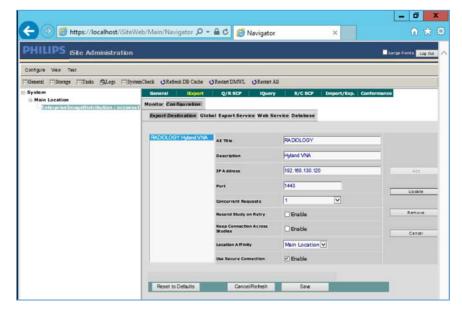
2. Click **Configuration > DICOM** to navigate to the DICOM configuration screen.

Configure Vew Test			
∏General ∏Storage ∏Tasks @Logs ∏Sy	temCheck ORefresh DB Cache ORestart DMM	L ORestart All	
System	General iExport Q/R.SCP	iQuery S/C SCP	Import/Exp. Conformance
EnterpriseImageDistribution . accord	DICOM Support		
	Normal AETEle	STENTOR_SCP	Default
	High Priority AETitie	STENTOR_HI	Default
	Part	104	Default
	Secure Port	2762	Default
	Replace Non Latin-1 During Import	Disble	Default
	Enable/Disable Export on DICO     Advanced	M Processing Host(s)	

- 3. On the top menu, click **iExport** to open the **iExport** screen. Provide the information below, and click **Save:** 
  - AE Title: RADIOLOGY
  - Description: Hyland VNA
  - IP Address: 192.168.130.120

#### • **Port:** 1443

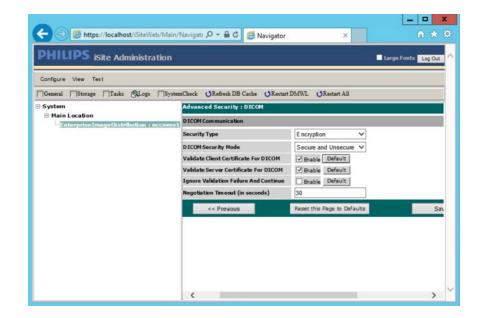
• Use Secure Connection: checked



- 4. Click **Configuration > Advanced Security**, and make these selections:
  - TLS 1.0 or higher: Selected
  - Enable Secure Web Services Communication.
  - Enable Image Access in Secure Mode.
  - Default Client Certificate: CN= nccoess1.stnccoe.isyntax.net
  - Default Server Certificate: CN=HYLAND-VNA.pacs.hclab
  - Click Save to save the settings.

Configure Vew Test Configure Vew Configure Configur	PHILIPS iSite Administration						Large F	onts Logo
System Main Location Tetterperior Textory and Disk Justices Texcorest Dicestory DiCoM Managerrent Managerrent Managerrent Managerrent Conflicate Manager Conflicate State Conflicate State Co		mCheck (SRef	healt DB Car	he (SRestart I	MWL (SRestar	t All		
Server	System	General	-					
DICOM Session Management Management Secure Web Services Index Secure Secure Web Services Index Secure Secure Secure Veb Secure Index Secure Secu		Server	O \$51.34	) or higher 🖲 1	LS 1.0 or higher	TLS 1.1 or higher O T	51.2	
Image Access is Secure Mode     Image Access is Secure Default       Chinaccess is Secure Default     Chinaccess is indose isyntax.net. OUHINCOSE. OHNEST-NCCOEL LaRadoville. V Default Server       Certificate Server     Chinaccess istnose isyntax.net. OUHINCOSE. OHNEST-NCCOEL LaRadoville. V Default Server       Chinaccess istnose isyntax.net. OUHINCOSE. OHNEST-NCCOEL LaRadoville. V Default       Control Con		Session						
Default Gentricate Berver Gentricate Berver Berver Chancocessi strocce isyntax.net. OU=NCCoE. OwNIST-NCCoE. LaRodovite. V Chancocessi strocce isyntax.net. OU=NCCoE. OwNIST-NCCoE. LaRodovite. V Comment ison ison ison ison ison ison ison ison			Image Acc Mode	ess in Secure	Carlos Carlos Carlos Carlos			
Cientificate Default Default Cientificate Default Cientificate Cientif			Certificate	Manager				
Server Urbencoessi stroce inymian.net. OU wICCot, OwNIST-NCCot, LuRodoville, V Abox Ser Signed Cristicate Validations EXU Onech Certificate Cer			Client Certificate	CN#nccoess1	strccoe.isyntax.ne	et. OU=NCCoE. O=NIST-P	CCoE. LaRockville, V	
Centrificate Validations EKU Once: Centrificate Validations EKU Once: Centrificate			Server	CN=nccoess1	streese.isyntax.ne	et, OU=NCCoE, O=NIST-?	CCoE, L=Rockville, 👻	
DKU Oheck Erstein Centricate Revocation Check CRL Cathing Erstein Check			Allow Self : Certificate	Signed				
Centrificate Revocation Check CRL Cathing			Certificate	Velidations				
Caching Default			Certificate Revocation					
Check for Check or restation of full certificate chain			Caching Revocation					
			IpAddress	Tracking	Default			

- 5. On the **iSite Administration** screen, click **Next**, and click **Next** again to open the page that follows:
  - a. Enable Validate Client Certificate for DICOM.
  - b. Enable Validate Server Certificate for DICOM.
  - c. Click **Save** to save the settings.



### 6. Restart the iSite Monitor Service.

# 2.3.4 PACS and VNA TLS Integration Tests

After implementing the above PKI-certification installation and TLS-enabling configuration, the Acuo VNA and IntelliSpace PACS servers are ready to perform the TLS secure DICOM communication tests. The secure DICOM communication tests were conducted for bidirectional data exchanges between Acuo VNA and IntelliSpace PACS to confirm:

- DICOM communication is still functional.
- DICOM communication is encrypted.

The test proves the DICOM communication was successful, with the accurate data exchange between the Acuo VNA and IntelliSpace PACS.

The network flow and dataflows monitoring tool indicate that the mutual authentication between Acuo VNA and IntelliSpace PACS is established. Encrypted application data were exchanged.

# 2.4 Modalities

Modalities represent medical devices used to capture medical images. The build did not implement physical devices but rather used virtualized or simulated modalities to source image files. The RIS was also emulated using open-source tools.

# 2.4.1 DVTk Modality Emulator

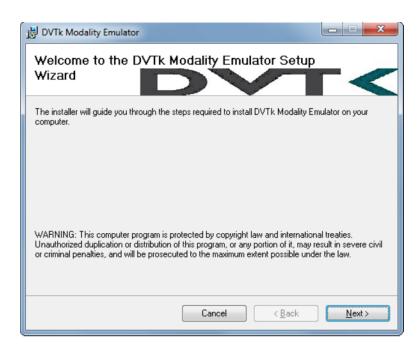
DVTk Modality is a modality emulator that can emulate all the DICOM functions of a modality system. It can simulate a real modality to test and verify communication with all the DICOM services. It uses DICOM files as input for queries, MPPS, and storage actions. Consequently, this project used the DVTk Modality as an emulator to test the connectivity, communication, workflow, and interaction between PACS and modality in the lab.

### System Requirements

- Operating System: Microsoft Windows 7 (with Microsoft .NET 4.0 Framework)
- Network Adapter: VLAN 1402

### **DVTk Modality Installation**

- 1. Download the installation software from the DVTK site [4].
- 2. Click the **Modality Installation** file (e.g., *DVTk-Modality-Emulator-5.0.0.msi*) to start the installation process.



3. Follow the wizard instructions to continue the installation until it successfully completes.

B DVTk Modality Emulator		
Installation Complet		Т<
DVTk Modality Emulator has been Click ''Close'' to exit.	successfully installed.	
Please use Windows Update to ch	neck for any critical updates to the .f	NET Framework. Back Close

- 4. **Close** the installation window.
- 5. The DVTk Modality Emulator can be launched from the **PC Start** menu. The Modality Emulator interface is below.

ile Help			
≷ 📕 🕾 🛅 🗇   ← † ⇒ Control ]			
RIS System			
		Ping RIS	
(No)	<b>→</b>	DICOM Echo	
John Star		Request Worklist	
$\Psi$	00000000	Send MPPS Progress	
Modality	RIS System	Hint	
PACS/Workstation Systems			
	-	Ping PACS/Workstation	
	<b>→</b>	DICOM Echo	
John Start		Store Image	
$\Psi$	DA COMPLEX S	Storage Commitment	
Modality	PACS/Workstation	Hint	

### **DVTk Modality Configuration**

Configuration of the DVTk Modality involves configuration of the communications with different external systems, including the RIS, which is the worklist provider or a work-list broker connected to the RIS; the MPPS manager that handles the MPPS messages for status reporting; and the PACS and its DB where the images will be stored. The information needed for these external systems should include the correct IP address, Port number, and Application Entity Title (AE Title). Input the information with these values:

- RIS System
- IP Address: 192.168.160.201
- Remote Port: 105
- AE Title: RIS
- MPPS Manager
- IP Address: localhost
- Remote Port: 105
- AE Title: RIS
- PACS/Workstation Systems–Storage Config
- IP Address: localhost

- Remote Port: 106
- AE Title: MPPS
- PACS/Workstation Systems–Storage Commit Config
- IP Address: localhost
- Remote Port: 107
- AE Title: PACS
- Store Commit Config
- IP Address: localhost
- Remote Port: 107
- **AE Title:** PACS

Modality	Emulator	
jle <u>H</u> elp		
Control Config	gure Remote Systems	
RIS System		
IP Address:	localhost	
Remote Port	105	
AE Title:	RIS	
MPPS Manag	let	
IP Address:	localhost	
Remote Port	106	
AE Title:	MPPS	
PACS Av/orks	talion Systems	Commit Config
IP Address:	localhost	IP Address: Jocalhost
Remote Port.	107	Remote Port: 107
	PACS	AE Title: PACS

The configuration of the modality itself is also needed to indicate its **AE Title** (e.g., **DVTK\_MODALITY**), **Local IP Address** (e.g., **172.31.138.126**), and **Listen Port** (e.g., **104**) to be paired for association negation with other remote systems. The screenshot that follows indicates the options for the **Modality Emulator** configuration:

Modality Emulator		- 🗆 X		
File Help				
≈∎ 🕄 🗂 💿 (← ↑ →	N			
Control Configure Emulator Workli	st Query   MPPS-Progress   MPPS-Discontinued   MPPS-C	ompleted   Image Storage   Dummy Patient		
System Name:	Modaity			
AE Title:	DVTK_MODALITY			
Implementation Class UID:	1.2.826.0.1.3680043.2.1545.6.3.1.0			
Implementation Version Name:	ModalityEmulator			
Local IP Address:	172.31.138.126			
Listen Port:	104			
Storage Commit Mode				
In Single Association (S	ync commitment)			
C In Different Association	(Async commitment)			
Wait time for N-EVENT-REPOR	T from PACS (in sec):			

Several tabs exist for configuring the behavior of the emulator. They can be configured as needed or by using the default settings. Once the configuration is done, the emulator front graphical user interface (GUI) provides some test buttons for verifying the connectivity, including **RIS System** and **PACS/Workstation Systems** server Internet Control Message Protocol pings and **DICOM** echo:

Modality Emulator				
Elle Help				
余日前首 (1) 十十	+			
Control Configure Remote System	12			
RIS System				
		Ping RIS	Ping successful	
Sta	<b>→</b> 🌄	DICOM Echo	DICOM Echo successful	
1 Alexandre		Request Worklist		
- Day		Send MPPS Progress		
Modality	RIS System	Hint:		
PACS/Workstation Systems				
		Ping PACS/Workstation	Ping successful.	
NB	<b>→</b>	DICOM Echo	DICOM Echo successful	
A CONTRACTOR		Store Image	D3	
- Sa-		Storage Commitment		
Modality	PACS/Workstation	Hint		

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-24.

# 2.4.2 DVTk RIS Emulator

DVTk, the Health Validation Toolkit, is an open-source software. The DVTk RIS Emulator is an application that handles Modality Worklist and Modality Performance Procedure Step requests from remote applications and then responds with the emulated results using the DICOM files specified by the users.

### System Requirements

• Operating System: Microsoft Windows 7 (Microsoft .NET Framework 2.0)

### **DVTk RIS Emulator Installation**

- 1. Download the DVTk RIS Software installer RIS Emulator .msi file from http://www.dvtk.org.
- 2. Start the installation procedure by double-clicking the .msi installation file.
- 3. Follow the wizard screen instructions to continue the installation until the end of successful installation displays.
- 4. Close the installation window and start the **RIS Emulator.** The user interface of the **RIS Emulator** tool that follows is shown with the tabs that follow for selecting the modes:
  - Worklist
  - MPPS
  - Edit DCM Files
  - Activity Logging
  - Results

File Stored Files Ab	The state of the s	DCM Files   Results   Activity Logging
Select Mode	Local AE title:	DVTK_RIS
Start	Remote AE title:	DVTK_MODALITY
Stop		
Specify TS		
Save		
	View information	n model View the MWL information model constructed from the Dicom files.
4 4	Import Dicom	files Import DICOM files to default data directory for emulating WLM responses
	Set Scheduled F	Procedure Step Date\Time to current date\time
	☐ Select data dire	ctory for sending WLM responses

### **DVTk RIS Emulator Configuration**

- 1. Worklist Configuration
  - Local AE title: AE title of the RIS Emulator
  - Local Port: the port of the RIS Emulator for incoming association
  - Remote AE title: AE title for the service-class user paired with the RIS Emulator
  - View Information Model: information model used for sending the emulator response; default value is taken
- 2. Select Data Directory for sending WLM responses: location for storing the emulated responses to the Worklist requests. A default setting can be used, which is C:\Progam Files\DVTk\RIS Emulator\Data\Worklist\
- 3. The **RIS Emulator** also supports other parameter configurations such as MPPS and Store Files functionality. These can be done as needed.
- 4. Configuration of the **RIS Emulator** and the modality storage emulator should be done accordingly so they can communicate with each other.

## 2.5 Asset and Risk Management

The build includes commercially available tools used to implement asset and risk management for medical devices. The implemented tool provides an asset inventory of medical devices that are identified via NetFlow traffic data. The tool also automates vulnerability detection and depicts a risk score. In addition to modality devices, we used other tools to manage server components.

## 2.5.1 Virta Labs BlueFlow

Virta Labs BlueFlow is a medical asset management software that allows discovery and management of medical devices on the network. This project used BlueFlow to create an organized inventory of the medical devices in the PACS architecture.

### System Requirements

- CPUs: 2
- Memory: 8 GB RAM
- Storage: 100 GB (thin provision)
- Operating System: CentOS 7
- Network Adapter: VLAN 1201

### Virta Labs BlueFlow Installation

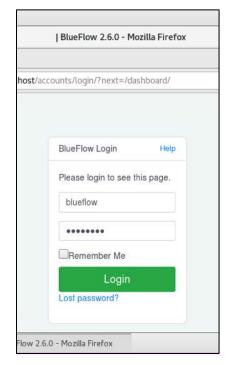
- 1. Run rpm -ihv blueflow-2.6.0-1.x86\_64.rpm in the CentOS 7 terminal.
  - a. Wait for the package installation process to complete.
  - b. Depending on your environment, you may need to install some dependencies before the BlueFlow package can be successfully installed.

🚯 Applications Places Terminal	0	Wed 13:35	4	ф))	С
root@test-blueflow:~/Documents			-		×
File Edit View Search Terminal Help					
[root@test-blueflow Documents]# rpm -ihv blueflow-2.6.0-1.x86_64.rpm					

- 2. Run sysyemctl status blueflow.service in the CentOS 7 terminal.
- 3. Ensure **blueflow.service** is **active.**

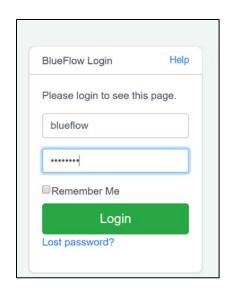
Applications Places Terminal	3	Wed 13:41	4	40)	Φ
root@test-blueflow:~/Documents			-		×
File Edit View Search Terminal Help					
<pre>[root@test-blueflow Documents]# systemctl status blueflow.service blueflow.service - BlueFlow Service Loaded: loaded (/etc/systemd/system/blueflow.service; enabled; vendor preset: disabled Active: active (exited) since Wed 2019-07-03 13:39:09 EDT; 2min 31s ago Process: 18711 ExecStart=/bin/echo blueflow.service governs all the other blueflow_ ser atus=0/SUCCESS) Main PID: 18711 (code=exited, status=0/SUCCESS) Tasks: 0 CGroup: /system.slice/blueflow.service</pre>		es (code=e	xite	ed,	st
Jul 03 13:39:09 test-blueflow systemd[1]: Starting BlueFlow Service Jul 03 13:39:09 test-blueflow systemd[1]: Started BlueFlow Service. [root@test-blueflow Documents]#					

4. Visit https://localhost to verify that BlueFlow web service is operating as expected, with a BlueFlow Login page.

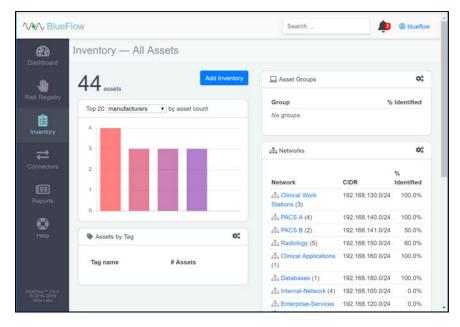


## Virta Labs BlueFlow Network Groups Configuration

1. Log in to the **BlueFlow** web console.



- 2. Navigate to the **Inventory** tab.
- 3. Under the **Networks** section, click the **gear** icon.



- 4. Enter Security Service as a Name for the new network group.
- 5. Enter **192.168.190.0/24** as a classless inter-domain routing (CIDR) for the new **network group.**
- 6. Click create.

æ					
Dashboard	User Profile	The Network	5		
Call C	Custom Asset Fields	Network		CIDR	Delete
	Asset Groups		Work Stations (3)	192.168.130.0/24	
Risk Registry	Networks	A PACS A		192.168.140.0/24	1
自	Tags	A PACS B		192.168.141.0/24	ā
Inventory	Risk Factors &	A Radiolo	gy (5)	192.168.150.0/24	面
	Controls	+ Clinical	Applications (1)	192.168.160.0/24	亩
⇒_	Connectors	- Databar	ses (1)	192.168.180.0/24	亩
Connectors	Logs	A Internal	Network (4)	192.168.100.0/24	盲
Reports		🚓 Enterpri	se-Services (9)	192.168.120.0/24	亩
۵		New networ	k		
Help		Name	Security Services		
		CIDR	192.168.190.0/24		

- 7. Verify that the new **network group (Security Services)** has been created.
- 8. Click the **name** of the new network group.

<i>2</i> 6		C		
Dashboard	User Profile	-T. Networks		
.th	Custom Asset Fields	Network	CIDR	Delete
sk Registry	Asset Groups	Clinical Work Stations (3)	192.168.130.0/24	Ô
	Networks		192.168.140.0/24	窗
Ê	Tags	PACS B (2)	192.168.141.0/24	Ē
Inventory	Risk Factors &	Radiology (5)	192.168.150.0/24	窗
	Controls	Clinical Applications (1)	192.168.160.0/24	盲
₽	Connectors	<u>a≣a</u> Databases (1)	192.168.180.0/24	Ē
lonnectors	Logs	Internal-Network (4)	192.168.100.0/24	窗
		Enterprise-Services (9)	192.168.120.0/24	面
Reports		A Security Services (7)	192.168.190.0/24	â
O Help		New network		
		Name		
		CIDR		

9. Assets will be listed on this page if they match the network group's criteria.

10. If there are no **assets** currently listed, you can manually add them by navigating to **Inventory > Add Inventory** or by running an IP discovery scan (detailed in the next section).

Asset-130       192.168.190.122       0.0/2.0/1.0       assets       assets	Bashboard	Netwo	rk: Secu	rity Se	rvices						
Actions *       1-7 of 7       Previous       Next         Actions *       1-7 of 7       Previous       Next         Risk Score saf / sc / total *       Risk Score saf / sc / total *       These assets       Asset         Asset-130       192.168.190.122       0.0/2.0/1.0       Asset       These assets       Asset         Asset-128       192.168.190.120       0.0/2.0/1.0       Asset       Asset       7       4         Asset-131       192.168.190.121       0.0/2.0/1.0       Assets       0.0%       2         Asset-132       192.168.190.170       0.0/2.0/1.0       Assets       100.0%       7         Asset-133       192.168.190.170       0.0/2.0/1.0       Assets       100.0%       7         Asset-134       192.168.190.170       0.0/2.0/1.0       Assets       0.0%       2	ىلل	Asset	s						Name:	Securit	y Services
Inventory         Asset         Tegs         IP Address         saf/sc/re         Tegs         IP Address           Asset:130         192.168.190.122         0.0/2.0/1.0         Asset:130         192.168.190.120         0.0/2.0/1.0         Asset: 7         Asset: 7         Asset: 7         Asset: 7         Asset: 131         192.168.190.121         0.0/2.0/1.0         Asset: 0.0%         2           Mark         Asset:131         192.168.190.121         0.0/2.0/1.0         Asset: 0.0%         2           Asset:132         192.168.190.140         0.0/2.0/1.0         Asset: 0.0%         2           Asset:133         192.168.190.170         0.0/2.0/1.0         Assets         100.0%         7           Asset:133         192.168.190.170         0.0/2.0/1.0         Assets         100.0%         7           Asset:133         192.168.190.170         0.0/2.0/1.0         Assets         0.0         0	lisk Registry	Acti	ons 💌		1–7	of 7	Previous	Next	CIDR:	192.16	8.190.0/24
Connectors       Asset-130       192.168.190.122       0.0/2.0/1.0       assets       asset       ass	and a second	D	Asset	Tags	IP Address			al +	Details		
Image: Asset-128       192.168.190.120       0.0/2.0/1.0         Image: Asset-129       192.168.190.121       0.0/2.0/1.0         Image: Asset-131       192.168.190.121       0.0/2.0/1.0         Image: Asset-132       192.168.190.160       0.0/2.0/1.0         Image: Asset-132       192.168.190.160       0.0/2.0/1.0         Image: Asset-133       192.168.190.170       0.0/2.0/1.0         Image: Asset-134       192.168.190.172       0.0/2.0/1.0	₽	٠	Asset-130		192.168.190.122	0.0	/ 2.0 / 1.0				All assets
Reports         Asset-129         192.168.190.121         0.0/2.0/1.0         Assets         0.0%         2           Image: Help         Asset-132         192.168.190.140         0.0/2.0/1.0         Assets         0.0%         2           Image: Help         Asset-132         192.168.190.160         0.0/2.0/1.0         Assets         100.0%         7           Image: Help         Asset-133         192.168.190.170         0.0/2.0/1.0         Assets         100.0%         7           Image: Help         Asset-133         192.168.190.172         0.0/2.0/1.0         Assets         0.0         0	Connectors		Asset-128		192.168.190.120	0.0	/ 2.0 / 1.0		Asset	7	44
Asset-131         192.168.190.140         0.0/2.0/1.0         Asset-100.00%         2           Asset-132         192.168.190.160         0.0/2.0/1.0         Assets         100.0%         7           Asset-133         192.168.190.170         0.0/2.0/1.0         Assets         100.0%         7           Asset-133         192.168.190.172         0.0/2.0/1.0         Assets         0.00%         7           Asset-134         192.168.190.172         0.0/2.0/1.0         Average         0.0         0	e		Asset-129		192.168.190.121	0.0	/ 2.0 / 1.0		count:		
Help         Asset-133         192.168.190.170         0.0/2.0/1.0         Assets         100.0%         And           Asset-134         192.168.190.172         0.0/2.0/1.0         Average         0.0         0	Reports	0	Asset-131		192.168.190.140	0.0	/ 2.0 / 1.0			0.0%	29.5%
Asset-133 192.168.190.170 0.0/2.0/1.0 not identified: Asset-134 192.168.190.172 0.0/2.0/1.0 Average 0.0 0		•	Asset-132		192.168.190.160	0.0	/ 2.0 / 1.0		Assets	100.0%	70.5%
Average 0.0 0	Help		Asset-133		192.168.190.170	0.0	/ 2.0 / 1.0				
safety risk: c.200-200 Virs Labr		0	Asset-134		192.168.190.172	0.0	/ 2.0 / 1.0		safety	0.0	0.0

### **Running an IP Discovery Scan in Virta Labs BlueFlow**

1. Log in to the **BlueFlow** web console.

BlueFlow Login	Help
Please login to see th	is page.
blueflow	
••••••	
Remember Me	
Login	

## 2. Navigate to **Connectors > Discovery.**

<b>∕∕•∕</b> ∧ BlueFl	wo		Search	Ø blueflov
Dashboard	Connectors			
. dh	Connectors	Connector Tasks		
Risk Registry	17 connectors; showing only		Previou	s Next
Inventory	enabled connectors below.	Risk Metrics	finished Yesterday at 12:22 PM	Success
₽	BlueFlow Pulse	Fingerprint	finished Last Tuesday at 4:30 PM	Success
Connectors	CSV	Fingerprint	finished Last Tuesday at 4:29 PM	Success
	Discovery	Fingerprint	finished Last Tuesday at 4:28 PM	Success
Reports	Fingerprint	Fingerprint	finished Last Tuesday at 4:27 PM	Success
Ø	Nessus Import	Fingerprint	finished Last Tuesday at 4:14 PM	Success
Help	Netflow	Fingerprint	finished Last Tuesday at 4:13 PM	Success
	Nexpose Import	Fingerprint	finished Last Tuesday at 4:04 PM	Success
	Password Checker	Discovery	finished Last Tuesday at 3:23 PM	Success
BlueFlaw™ 2.6.4 © 2016–2019	Ping	Risk	finished Last Tuesday at 12:22	Success
s://blueflow.pacs.hc	lab/connectors/discovery/	Metrics	PM	

3. Under **Discovery**, click the **gear** icon.

<b>∕∕∕∕</b> BlueF	low		Search	<b>2</b> (2) blueflow
200 Dashboard	Connector: Discovery			
ىلار	Discovery			iscovery
Risk Registry	target IP, hostname or CIDR for discovery scan		scan. By defa new as from co	r assets using an ICMP ping ult, this connector will not create sets when it receives responses nnected assets. To configure lavior, visit the connector
e	Connector Tasks			
Reports	Connector Tasks	Previous N	lext	
	Connector Tasks Discovery	Previous N finished Last Tuesday at Succ 3:23 PM		
Reports		finished Last Tuesday at Succ	2855	
Reports	Discovery	finished Last Tuesday at Suco 3:23 PM	2055	

4. Check the box next to allow\_create\_asset.

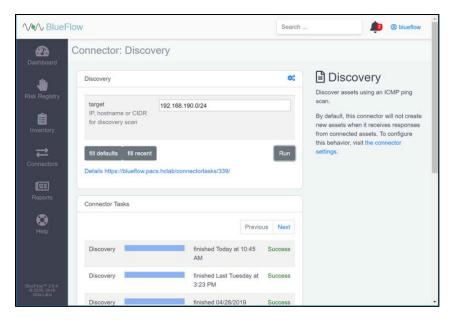
#### 5. Click Save.

VVV Blue				
20 Dashboard	Settings: Connector			
	User Profile	Discovery Settings		=
isk Registry	Custom Asset Fields Asset Groups Networks Tags	enabled Enable or disable this connector	×	
Connectors	Risk Factors & Controls Connectors Logs	allow_create_asset Allow creating new assets (not just updating existing)	x	
Reports				Save

6. Enter an IP (e.g., 192.168.190.0/24), host name, or CIDR that you would like to scan.

### 7. Click Run.

8. Wait for the discovery scan to finish.



9. Click the **row** of the completed scan to view more details.

Note: From this page, you can view the output of the scan, including how many devices were discovered within the provided network range.

∧ No BlueFlo	w			Search	
Dashboard	Connector Ta	isk			
	Discovery				Success
isk Registry	Inputs		Name	Value	
Inventory			target	192.168.190.0/24	
	External URL				
Connectors	Submitted		Today at 10:4	5 AM	
	Started		Today at 10:4	5 AM	
Reports	Finished		Today at 10:4	5 AM	
0	Duration		a few seconds	i.	
Help	Returned				
	Output				
	nmap -oXsn -	P scan on 192.168 PE 192.168.190.0/	.190.0/24. This might 24	take a while.	
	Version 6.40 Finished discove	ev scan			
	created	Ø			
	updated	e			
	up-to-date	7			
	skipped	Ø			
	duplicate	0			
	errored	0			
A CLARKER MARKED	total	7			

# 2.5.2 Tripwire Enterprise

Tripwire Enterprise is a security configuration management software that monitors file integrity through software-based agents. For this project, we used Tripwire Enterprise to monitor file changes on PACS servers and the VNA DB.

### System Requirements

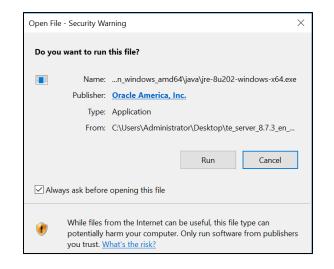
- CPU: 1
- Memory: 4 GB RAM
- Storage: 120 GB (thin provision)
- Operating System: Microsoft Windows Server 2016
- Network Adapter: VLAN 1201

### **Tripwire Enterprise Console Installation**

1. In the *tripwire install* folder under java, double-click the *jre-8u202-windows-x64 application* file.

i	Share	View			
÷ → • ↑ 📕	> te_s	erver_8.7.3_en_windows_amd64 > java			
📌 Quick access		Name	Date modified	Туре	Size
besktop	*	🔬 jre-8u202-windows-x64	3/22/2019 8:04 AM	Application	75,467 KE
🔈 Downloads	$\mathcal{A}$				
Documents	*				

#### 2. Click Run.



### 3. Click Install >.

	Welcome to Java
Java provide	s access to a world of amazing content. From business solutions to helpful utilities and entertainment, Java makes your Internet experience come to life.
Note: No persona	al information is gathered as part of our install process. <u>Click here</u> for more information on what we do collect.
	Click Install to accept the license agreement and install Java now.

4. Click OK.

inge in License Tern	15		
E Java			
	Important Information about Oracle Jav	va SE Roadmap	
Change	es are coming which will impact your access to future rel	leases of Java SE from Ora	cle.
	Corporate users will be impacted with the Ap	pril 2019 update.	
	These changes do not affect the version you are	about to install.	
	For additional guidance please follow the li	ink below.	
	More information		
			OK

5. Wait for the installation process to complete.

	Va <sup>-</sup>		
Status:	Installing Java		
	ATMs, Smartcards, POS Terminals, Blu-ray Play, Set Top The Martine Martine Structure Servers, Ser		
	<b>3 Billion</b>	Devices	
	Devices Run Java	tochilen	

## 6. Click Close.

Setup - Complete	1				
CHALLE	✓ You have successfully inst	talled Java			
You will be prompted when	n Java updates are available. Always inst and security improvement <u>More about update setting</u>	s.	est per	forman	ce
				Close	

7. With Java installed, double-click the Tripwire install application, *install-server-windows-amd64*.

ie Home Shar	e View Manage	te_server_8.7.3_en_wind	lows_amd64		
→ × ↑ 🖡 > 1	te_server_8.7.3_en_windows_a	md64			
Quick access	Name	~	Date modified	Туре	Size
	docs		6/26/2019 12:14 PM	File folder	
	extras		6/26/2019 12:14 PM	File folder	
Second and the second s	📕 java		6/26/2019 12:14 PM	File folder	
	twagents		6/26/2019 12:14 PM	File folder	
E Pictures	🐔 🙋 install-server-windo	ows-amd64	2/4/2019 10:52 AM	Application	532,219 KB
Symantec DCS	🕈 🛯 🙋 license		2/4/2019 10:52 AM	HTML Document	30 KB
Tripwire Enterprise	PORTS & CREDENT	IALS	3/22/2019 9:42 AM	Text Document	1 KB

8. Select the version of Java, Oracle/Sun 1.8.0 64-bit, that was previously installed.

### 9. Click **OK.**

Please select the Java(tm) Runtime to use	Please select the Java(tm) Runtime to use Oracle/Sun 1.8.0 64-bit C:/Program Files/Java/jre1.8.0_202/bin/java.e <	LIVM Selection					×
Oracle/Sun 1.8.0.64-bit C/Program Files/Java/ire1.8.0.202/bin/java (	Oracle/Sun 1.8.0 64-bit C:/Program Files/Java/jre1.8.0_202/bin/java.e $\vee$	Plea	ise select the Jav	va(tm) Runtime	to use		
oracle/sun no.o of bit c./ rrogram mcs/suva/jrcno.o_coc/bin/java.v		Oracle/Sun 1.8.0 64	4-bit C:/Program	n <mark>Files/Java/j</mark> re1	.8.0_202/	bin/java.	e ~

### 10. Click Next >.



## 11. Check I accept the agreement.

#### 12. Click Next >.

te Tripwire Enterprise Console	e Installer		_		×
License Agreement			t	ipwi	re <sup>:</sup>
Please read the following Lic before continuing with the in		st accept th	e terms of t	his agree	ment
IMPORTANT INFORMATION					^
TRIPWIRE SOFTWARE IS L SUBJECT TO LICENSE RES AGREEMENT BEFORE USING COMPLETE AND UNCONDITI SET FORTH IN THIS AGRE ORDER TERMS AND CONDIT	TRICTIONS. CAREFULL THE SOFTWARE. USE ONAL ACCEPTANCE OF EMENT. ANY ADDITION	Y READ TH OF SOFTWA THE TERMS AL OR DIF	IS LICENS RE INDICA AND CONE	E TES DITIONS	~
Do you accept this license?	<ul> <li>I accept the agreement</li> <li>I do not accept the agreement</li> </ul>	ent igreement			
InstallBuilder					
	<	Back	Next >	Car	ncel

13. Specify an installation directory, *C*:\*Program Files*\*Tripwire*\*TE*, for the Tripwire installation.

## 14. Click Next >.

te Tripwire Enterprise Console Installer		-		×
Installation Directory		j	tripw	ire:
Please specify the directory where all Tripwire Enterpr	rise compo	onents will b	e installed	I.
Installation Directory C:\Program Files\Tripwire\TE		<u> </u>		
InstallBuilder				
	< Back	Next >	Ca	ancel

15. Verify the host name for the machine on which you are installing Tripwire (e.g., WIN-RUQDO7KL8A7).

### 16. Click Next >.

Tripwire Enterprise (	Console Installer		-		X
Tripwire Enterprise	Console Configuration	Part 1 of 4	tr	ipwi	re <sup>:</sup>
Please provide the ho installed.	stname of the system	where Tripwire Ente	rprise Console	will be	
TE Server Hostname	WIN-RUQDO7KL8A7				
nstallBuilder					
		< Back	Next >	Car	ncel

- 17. Specify the HTTPS Web Services port as 6000, HTTP EMS Integration Port as 8080, and Tripwire Enterprise RMI Port as 9898.
- 18. Click Next >.

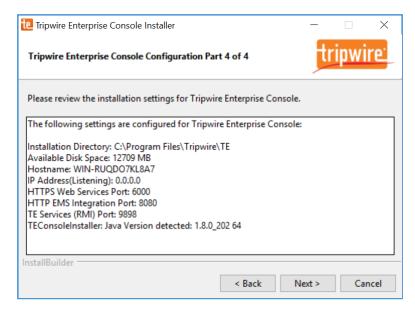
Tripwire Enterprise Console Co	onfiguration	n Part 2 of 4	t	ripwi	re <sup>:</sup>
Specify the ports that Tripwire E	interprise Co	onsole uses to comr	municate.		
This port is used for user-initiate	ed Web con:	sole sessions.			
HTTPS Web Services port	6000				
This port is used for external int	egrations (su	uch as plugins).			
HTTP EMS Integration Port	8080				
This port is used for Console/Ag	gent Java co	mmunications.			
Tripwire Enterprise RMI Port	9898				
nstallBuilder					

- 19. Create a password for Tripwire Enterprise services.
- 20. Click Next >.

Tripwire Enterprise (	Console Configuration Part 3 of 4		Ľ	ipwi	re
The services passphra	se is used to secure Tripwire Enterprise	e comm	unication	5.	
This password must b	e between 19 and 64 characters, and o	annot c			te ('),
double-quote ("), less	-than (<), greater-than (>), or backsla d. See the Installation and Maintenand				ier
double-quote ("), less					ier
double-quote ("), less characters are allowed					er

21. Verify that planned installation settings are correct.

#### 22. Click Next >.



- 23. Check Install Real-time Monitoring.
- 24. Specify Real-time Port as 1169 for monitoring.
- 25. Click Next >.

Tripwire Enterprise Agent software is installed on the Tripwire Enterprise Console system to enable monitoring of that system. Do you want to install Real-time Monitoring functionali for this local Agent? The Real-time Monitoring feature can also be installed later. Install Real-time Monitoring Please specify the local port to be used by the Real-time subsystem. Real-time Port 1169	Tripwire Enterpri	se Agent Configuration		ţ	ipwi	re'
Real-time Port 1169	enable monitoring for this local Agen	of that system. Do you want to in ? The Real-time Monitoring featu ime Monitoring	nstall Real-time ure can also be i	Monitorin nstalled lat	g functio	
	Real-time Port	1169				

### 26. Click Next >.

te Tripwire Enterprise Console Installer			-		Х
Ready to Install			tr	ipwi	re:
The installer is ready to begin installing Trip	wire Enterprise Co	nsole.			
Click Next to begin installing Tripwire Enter Click Back to make any changes before you		tion.			
InstallBuilder					
	< Back	Ne	d >	Car	ncel

## 27. Wait for Tripwire Enterprise installation to complete.

Tripwire Enterprise Console Installer		_		×
Installing		ţ	ipwi	re <sup>:</sup>
Inst Unpacking C:\Program []Tripwire\	alling TE\Server\lib\comm	non\jsch-0.1	.40.jar	
stallBuilder				

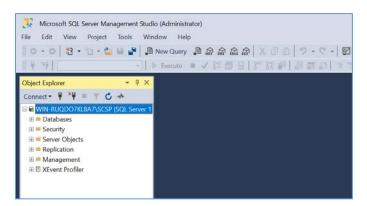
### 28. Click Finish.

te Tripwire Enterprise	Console Installer	_		×
<b>ENTERPRISE</b>	The installation is complete. Open a browser after clicking Finish to co Tripwire Enterprise. To finish configuration later, use a brows https://WIN-RUQDO7KL8A7			
	< Back	Finish	Can	cel

- 29. Open SQL Server Configuration Manger.
- 30. Under SQL Server Network Configuration > Protocols for SQL Server, ensure that the TCP/IP protocol is set to Enabled.



31. Open SQL Server Management Studio.



32. In the **Object Explorer**, expand the selection for your DB, right-click **Databases**, and select **New Database**...

	ew Project Tools Window Help S・ロ・コービー 単一 Mew Query 通知なななが、そのの「ア・マート -   ) Execute = V 認同日 87 認可日の語の日本
B WIN-RUQD	₩         ₩           ₩         ₩           07KL8A7/SCSP (SQL Server 1
🕀 🖷 Database	New Database
	Attach Restore Database Restore Files and Filegroups
⊞ ■ Server ( ⊞ ■ Replica ⊞ ■ Manage	Deploy Data-tier Application Import Data-tier Application
⊞ I XEvent	Start PowerShell
	Reports •
	Refresh

- 33. On the left, under Select a page, select General.
- 34. Enter a Database name as TE\_DB.
- 35. Under Database files, for the data file, set Initial Size to at least 2,000.

### 36. Click the **button** under **Autogrowth.**

Select a page General	🖵 Script 🔻	Help							
<ul> <li>Options</li> <li>Filegroups</li> </ul>	Database name		TE_DB						
	Owner:		<default></default>						
	Use full-text	t indexing							
	Database files:								
	Logical	File	Filegroup	Initial Si	Autogrowth / Max	Path			
	TE_DB	ROWS		2,000	By 1 MB, Unlimited				
	TE_DB_log	LOG	Not Applicable	500	By 10 percent, Unlimited	c:\Program Files (	<86)\Common I	Files\Symantec	Shared
Server									
Server: WIN-RUQDO7KL8A7\SCSP									
Connection Sener WIN-RUQDO7KL8A7-SCSP Connection: WIN-RUQDO7KL8A7-Johnnistrat									
Server: WIN-RUQDO7KL8A7\SCSP Connection:									
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administrato WIN-RUQDO7KL8A7\Administrato WiN-RUQDO7KL8A7\Administrato									
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administrato	<								>

37. Check Enable Autogrowth, set File Growth to at least 20 MB, and set Maximum File Size to Unlimited.

### 38. Click **OK.**

. New Database			- 🗆 X
Select a page	🖵 Script 🔻 😯 He	þ	
<ul> <li>Options</li> <li>Filegroups</li> </ul>	Database name:	TE_DB	
	Owner:	<default></default>	
	Use full-text index	ing	
	Database files: Logical Fi		Path
	TE_DB RC	Change Autogrowth for TE_DB	c:\Program Files (x86)\Common Files\Symantec Shared\Si
	TE_DB_log LC	Enable Autogrowth	c:\Program Files (x86)\Common Files\Symantec Shared\S
		File Growth	
		In Percent 10	
		In Megabytes     20	•
		Maximum File Size	
Connection		Limited to (MB)     100     Unlimited	
Server: WIN-RUQD07KL8A7\SCSP		<u> </u>	
Connection: WIN-RUQDO7KL8A7\Administrate		OK Cancel	
Vew connection properties			
Progress			
Ready	<		>
			Add Remove
			OK Cancel

- 39. Under Database files, for the log file, set Initial Size to at least 500.
- 40. Click the in Megabytes button under Enable Autogrowth.
- 41. Check Enable Autogrowth, set File Growth to at least 20 MB, and set Maximum File Size to Unlimited.
- 42. Click OK.

Select a page	🖵 Script 🔻 😮 Help						
Connection Connection Server: WIN-RUQDOTKLBAT/SCSP Correction: WIN-RUQDOTKLBAT/ACSP CORRECTION: WIN-RUQDOTKLBAT/ACMINIST WIN-RUDD/ACMINIST WIN-RUDD/ACM	TE_DB_log LC	TE_DB cdefault> Change Autogrowth Ele Growth in Percent in Percent in Megabytes Maximum File Size Limited to (MB) in Unlimited		Path c:Program Files c:\Program Files			
Progress Ready	<				Add	Remo	<b>&gt;</b>

- 43. On the left, under **select a page**, select **Options**.
- 44. Set Collation to Latin1\_General\_CS\_AI.
- 45. Set Recovery model to Simple.
- 46. Under Other Options > Miscellaneous, set ANSI NULL Default to True.
- 47. Click OK.

Select a page	_	-				
👂 General	So	rript 🔻 🕜 Help				
<ul> <li>Options</li> <li>Filegroups</li> </ul>	Colla	tion:	Latin1 General CS A	J		,
	Reco	overv model:	Simple			,
		patibility level:	SQL Server 2012 (110	n		
				"		
		ainment type:	None			
	Othe	r options:				
	•	2↓ 🖻				
		Default Cursor		GLOBAL		
	~	FILESTREAM				
		FILESTREAM Directory N				
		FILESTREAM Non-Trans	acted Access	Off		
	~	Misc		-		
		AllowScripting HideFileSettings		True False		
		Miscellaneous		False		_
	~	Allow Snapshot Isolation		False		
		ANSI NULL Default		True		V
		ANSI NULLS Enabled		False		
		ANSI Padding Enabled		False		
Connection		ANSI Warnings Enabled		False		
		Arithmetic Abort Enabled		False		
Server: WIN-RUQD07KL8A7\SCSP		Concatenate Null Yields N	lul	False		
		Cross-database Ownershi	p Chaining Enabled	False		
Connection: WIN-RUQDO7KL8A7\Administratic		Date Correlation Optimizat		False		
		Is Read Committed Snaps	hot On	False		
View connection properties		Numeric Round-Abort		False		
		Parameterization		Simple		
		Quoted Identifiers Enabled		False		
		Recursive Triggers Enable	ed	False False		
Progress		Trustworthy		False		
C) Ready	AN:	SI NULL Default				

## 48. In the **Object Explorer**, right-click your DB and select **New Query**.

File Edit View Project	agement Studio (Administrator) Tools Window Help 留計 Mew Query 画 品 品 品 二 本 で つ つ つ つ つ つ つ 	
Object Explorer Connect - ♥ ×♥ ■ ▼ (	<b>▼</b> ₽ X	
Source of the second seco	Connect Disconnect Register	
III SCSPDB	New Query	
	Activity Monitor Start Stop Pause Resume Resume	
	Policies Facets	
	Start PowerShell Azure Data Studio	
	Reports +	
	Refresh Properties	

49. Type the following query:

ALTER DATABASE [TE\_DB] SET READ\_COMMITTED\_SNAPSHOT ON

- 50. Click **Execute** in the toolbar above the **SQL Query** window.
- 51. Under the **SQL Query** window, in the **Messages** window, verify that the command completed successfully.

	இNew Quary இஇஇஇஇஇ ¥ பிற் / - ் - இ / ச இ / ச	
Xoject Explorer 🔷 🤗 🕻		
Connect• ¥ ¥ ≡ ⊤ & ↔	ALTER DATABASE [TE_DB] SET READ_COMMITTED_SNAPSHOT ON	
WIN-RUQDO7KL8A7\SCSP (SQL Server		
B # System Databases		
E B desc une		
III @ SCSPDB		
E TE_DB		
Security		
E = Server Objects		
E Replication		
🗉 🥌 Management		
E E XEvent Profiler		
	150.36 - 4	
	150 % - 4	
	(if Wanger	
	(if Wanger	
	(d Hamana Commanda completed successfully.	
	(if Wanger	0.00

52. Clear the **SQL Query** window, then type the following query:

- 53. Click **Execute** in the toolbar above the **SQL Query** window.
- 54. Under the SQL Query window, in the Messages window, verify the value for is\_read\_committed\_snapshot\_on is set to 1.

SELECT name, is\_read\_committed\_snapshot\_on FROM sys.databases WHERE
name='<db\_name>'

File Edit View Query Project Too	New Query 3 2 2 2 2 2 4 7 - 1 - 2 -	(° -   🛛   🔎	A_ Quick Launch (Otrl+Q)	P -		×
With masker     I       Object Eucliver     ● N       Connect -     ● N       Example:     ● N       Example: <td< th=""><th>ESELECT name, is_read_co</th><th></th><th>FROM sys.databases</th><th>WHERE</th><th>•</th><th>* * *</th></td<>	ESELECT name, is_read_co		FROM sys.databases	WHERE	•	* * *
< >	© Query encoded successfully.	WIN-RUDDO7KL8A7/SCSP (11.0 W	N-RUQDO76.BATV.Admini maste	× 00.00.00	1 гоз	1/5

55. In the **Object Explorer**, expand the selection for your DB, expand the **Security** section, right-click **Logins**, and select **New Login...** 

Image: Interference       Image:	Solution1	- Microsoft SQL Serv	er Management Studio (Administrator)	Quick Launch (Chil+Q) 🔎 = 🗖 🗙
Vierente     · · · · · · · · · · · · · · · · · · ·	File Edit V	ew Project Too	ls Window Help	
Vierente     · · · · · · · · · · · · · · · · · · ·	0.01	8 • 15 • 🛀 🖬	😹 🔍 New Query 鳥 岛 岛 岛 島 島 (メ 団 白 ) フ -	· . * =
Object Lybler        • P × Conset.       • P × • With RUXCOPCEAD/SSCP 008 Server 1       • State Database       • System Databas				
Concel - V V V RUDORIANSCE SCH COL Server I D Unbases Social Cababases Concel - Social Social V V V V V V V V V V V V V V V V V V V	-			
With RUQDOVRIBATISS? POBLE Several       South RugDovrib Saladise:       South RugDovrib Saladi	and the second se		• • ×	
Image: Control         Image: Contro         Image: Contro <td>and the second second</td> <td></td> <td></td> <td></td>	and the second			
System Chabbase          © System       Security         © Social       Security			Server 3	
Comparison of the second se				
K				
Secondary Secondary	III @ SCSPD	8		
Image: Source Filter Image: Source	E TE_DB			
Image: Some of the state of				
Flor Grad Fords Flor Fords Flor		New Login_		
Weill Store for the Store f			•	
III E Forking     Reports       III E Married     Referation       III E Xterritory     Referation		Start PowerShell		
B Marsa B Xevent wave				
B Z Xevert/Viewer		Defeash		
	E E XEvent	nestest.		
C Redy	C			
	Ready			

- 56. On the left, under Select a page, select General.
- 57. Create a Login name.

- 58. Select SQL Server authentication.
- 59. Create a **password**.
- 60. For **Default database**, select the DB previously created.
- 61. For Default language, select English.

Select a page General	🖵 Script 🔻 😯 Help				
<ul> <li>Server Roles</li> <li>User Mapping</li> <li>Securables</li> <li>Status</li> </ul>	Login name:	te_admin			Search
	SQL Server authentication				
	Password:	•••••			
	Confirm password:	•••••			
	Specify old password				
	Old password:				
	Enforce password policy				
	Enforce password expira	tion			
Connection	User must change passv	vord at next login			
Server	Mapped to certificate			$\sim$	
WIN-RUQDO7KL8A7\SCSP	Mapped to asymmetric key			$\sim$	
Connection: WIN-RUQDO7KL8A7\Administrate	Map to Credential			$\sim$	Add
View connection properties	Mapped Credentials	Credential	Provider		
Progress					Remove
	Default database:	TE_DB		$\sim$	
Ready	bordan adrabado.				

- 62. On the left, under Select a page, select User Mapping.
- 63. Under the **Users mapped to this login** window, perform these actions for the row containing the previously created DB:
  - a. Check the box in the **Map** column.
  - b. In the **Default Schema** column, type the name of the new user being created.

64. Click OK.

Select a page		<b>•</b> • • •			
🔑 General	L Script	🔻 😯 Help			
<ul> <li>Server Roles</li> <li>User Mapping</li> </ul>	Users ma	apped to this login:			
<ul> <li>Securables</li> <li>Status</li> </ul>	Map	Database	User	Default Schema	a
		dcsc_umc			
		master			
		model			
		msdb			
		SCSPDB			
		TE_DB	te_admin	te_admin	1
	~				
		tempdb			
Connection	Gui	tempdb			
C <b>onnection</b> Server: WIN-RUQDO7KL8A7\SCSP		tempdb	TE_DB		
Server:	Databas	tempdb est account enabled for: e role membership for: TI accessadmin	TE_DB		
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Admin	Databas	tempdb est account enabled for: e role membership for: Ti	TE_DB		
Server: WIN-RUQDO7KL8A7\SCSP Connection:	Databas Databas istratc ies db db db db	tempdb est account enabled for: e role membership for: TI accessadmin backupoperator datareader datawriter	TE_DB		
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Admin	istratc	tempdb est account enabled for: e role membership for: TI accessadmin backupoperator datamiter datamin	TE_DB		
Server: WIN-RUQDO7KLBA7\SCSP Connection: WIN-RUQDO7KLBA7\Admin WIN-RUQDO7KLBA7\Admin	istrato istrato ies db db db db	tempdb est account enabled for: e role membership for: TI accessadmin backupoperator datareader datawriter	TE_DB		
Server: WIN-RUQDO7KLBA7\SCSP Connection: WIN-RUQDO7KLBA7\Admin WIN-RUQDO7KLBA7\Admin	Databas	tempdb est account enabled for: e role membership for: TI accessadmin backupoperator datareader datawiter ddladmin denydatareader denydatawriter owner	TE_DB		
WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Admin	Databas	tempdb est account enabled for: e role membership for: TI accessadmin backupoperator datareader datawitter daladmin denydatareader denydatareader denydatawitter owner securityadmin	TE_DB		

65. In the **Object Explorer**, expand the selection for your DB, expand the **Databases** section, right-click the DB created previously, and select **Properties**.

File Edit Vi	3 • 🛅 • 😩 🔛 🚰   🔊 New Query 🚽	▲1991年1991年19月1日(1991年19月)→
Object Explorer	× # × ★ © ▼ = ₩	
<ul> <li>□ ■ Database</li> <li>① ■ System</li> <li>① 0 dcsc_u</li> <li>① 0 SCSPD</li> </ul>	Databases nc	
<ul> <li>■ IE_D<sup>as</sup>.</li> <li>■ Securit</li> <li>■ Server</li> <li>■ Replica</li> <li>■ Manag</li> <li>■ XEvent</li> </ul>	New Database New Query Script Database as	
	Tasks 🕨	
	Policies  Facets	
	Start PowerShell Azure Data Studio	
	Reports	
	Rename Delete	
	Refresh	
	Properties	

66. On the left, under **select a page**, select **Permissions**.

67. Under **Permissions for user,** check the box in the **Grant** column for the following permissions:

- Connect
- Create Function
- Create Procedure
- Create Table
- Create View
- Delete
- Insert
- Select
- Update

68. Click OK.

Select a page						
Select a page	🖵 Script 🔻 😮 He	elp				
<ul> <li>Files</li> <li>Filegroups</li> <li>Options</li> </ul>	Server name:		N-RUQDO7KL8A7	7\SCSP		
👂 Change Tracking	View server permiss					
<ul> <li>Permissions</li> <li>Extended Properties</li> </ul>	Database name:	TE	_DB			
Extended Propentes	Users or roles:				Sea	arch
	Name				Туре	Search B
	🔓 te_admin				User	
Connection						
Server:	Permissions for te ad	min:				
Server: WIN-RUQDO7KL8A7\SCSP	Permissions for te_ad	min:				
Server:	Explicit Effective		Grant	With	Denv	
Server: WIN-RUQDO7KL8A7\SCSP Connection:	Explicit Effective Permission	Grantor	Grant	With	Deny	^
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administrato	Explicit Effective	Grantor	Grant	With	Deny	^
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administrato	Explicit         Effective           Permission         Connect replicati	Grantor	Grant	With	Deny	^
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administrator WIN-RUQDO7KL8A7\Administrator	Explicit Effective Permission Connect replicati	Grantor	Grant	With	Deny	^
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administrate Y View connection properties	Explicit Effective Permission Connect replicati Connect Control	Grantor	Grant	With	Deny	^
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administrator WIN-RUQDO7KL8A7\Administrator	Explicit Effective Permission Connect replicati Connect Control Create aggregate	Grantor dbo	Grant	With	Deny	^

- 69. Open **Internet Explorer** and navigate to the web page of the server where Tripwire Enterprise was installed.
- 70. Enter the services password created during the installation process.
- 71. Click Login.

💿 👁 https://win-ruqdo7kl8a7:6000/config: Ρ - Ο 💿 Tripwire Enterprise Console 🛛 🛛	-	合会	× © (
ripwire Enterprise Post-Install Configuration			
Tripwire Enterprise needs additional configuration.			
To fnish installing, please enter your Services Passphrase for authentication. The Services Passphrase was created	when you installed Trinwire Enterprise		
To minor misualing, please enter your services nasspirates for addrenic autor in centros nasspirates was created Services Passpirate:	when you installed Tripwile Enterprise.		
Services r-asspriate:			
Login			

72. Under **Database Configuration Settings,** provide the information that follows:

- Remote Database Type: Microsoft SQL Server
- Authentication Type: SQL Server
- Login Name: \*\*\*\*\*\*\*
- Password: \*\*\*\*\*\*\*\*
- Database Host: WIN-RUQD07KL8A7
- Database Name: TE\_DB
- Instance Name: SCSP (Note: This may not be necessary, depending on how your SQL Server Database is configured.)
- SSL: Request

Tripwire Enterprise Post-Install Configurati	on	
Database Configuration Settings		
These settings control how the TE Console con make any necessary changes in the fields below	nects to a remote database that stores data for all TE operations. You can check the current configuration here, and w.	
Remote Database Type: Microsoft SQL Server V	Remote Database Type: The type of remote database used by TE.	
Authentication Type:	Authentication Type: Specifies whether the database login should authenticate using a Windows account (typically of the format domain/user), or an SQL Server account (an account defined only in SQL Server). With the Windows authentication type, NTLMv2 should be used, as it is cryptographically superior to the first version of NTLM. However, as NTLMv2 is configured in the operating system, not in the database or application, TE can be used with NTLM to ensure compatibility.	
Login Name: te_admin	Login Name: The login name that TE will use to authenticate with the database.	
Password:	Password: The password that TE will use to authenticate with the database.	
Database Host: WIN-RUQDO7KL8A7	Database Host: The fully qualified domain name, hostname or IP address of the system where the database is installed.	
Port (default 1433): (UDP 1434)	Port: The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.	
Database Name: TE_DB	Database Name: The name of the database that TE should use when connecting to the remote database. Note that the login name in SQL Server should have this database set as the default, and the login name should be mapped to this database.	
Instance Name (Optional): SCSP	Instance Name (Optional): The location/name of the database instance on the server. Ask your DBA if a non- default instance should be used for TE.	
SSL: Request	SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL.	

- 73. Click **Test Database Login** and verify that the connection is successful.
- 74. Click Save Configuration and Restart Console.

Login Name: te_admin	Login Name: The login name that TE will use to authenticate with the database.	
Password:	Password: The password that TE will use to authenticate with the database.	
Database Host: WIN-RUQDO7KL8A7	Database Host: The fully qualified domain name, hostname or IP address of the system where the database is installed.	
Port (default 1433): (UDP 1434)	Port: The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.	
Database Name: TE_DB	Database Name: The name of the database that TE should use when connecting to the remote database. Note that the login name in SQL Server should have this database set as the default, and the login name should be mapped to this database.	
Instance Name (Optional): SCSP	Instance Name (Optional): The location/name of the database instance on the server. Ask your DBA if a non- default instance should be used for TE.	
SSL: Request ✓	<ul> <li>SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL.</li> <li>Require - SSL will be used if available.</li> <li>Require - SSL will always be used, and an error will occur if SSL is not available for the database.</li> <li>Authenticate - SSL will always be used, and an error will occur if SSL is not available for the database. In addition, the certificate chain of the database server's public key will be authenticated using TE's trust store. If the certificate chain does not originate from a trusted source, an error will occur.</li> <li>Off - SSL will never be used. This setting is not recommended.</li> </ul>	
Test Database Login ) ✓ Test Results:		
Connection Succeeded.		
Tripwire Enterprise 8.7.3.b8.7.3.r2019011112200	5-03196dc.b24 Save Configuration and Restart Console Logout	

75. Wait for Tripwire Enterprise to restart and redirect you to the login page.

Tripwire Enterprise
Tripwire Enterprise is restarting. Your browser will be automatically redirected to the Tripwire Enterprise loading page when the service is successfully restarted.

76. Enter the **services password** created during the installation process.

# 77. Click Login.



78. Under **Create Administrator Password,** create a password for the Tripwire Enterprise administrator account.

### 79. Click Confirm and Continue.

Tripwire administrator account password needs to be changed from th	e default.
eate Administrator Password	Password:
asswords must: Be between 8 and 128 characters in length	
Contain at least 1 numeric character Contain at least 1 uppercase character	Confirm Password:
Contain at least 1 non-alphanumeric character Supported characters: `-!@#\$%^&*()=+[{]}\\ ;:""<,>./?	••••••
	Confirm and Continue
pport Information	
Still having problems with your installation?	For faster assistance from Support, please generate a support bundle to collect
Contact Tripwire Support:	information about your system and this installation. Attach the support bundle file your web ticket or email. What is a Support Bundle?
https://secure.tripwire.com/customers/contact-support.cfm	Generate Support Bundle

80. Enter the **username** and **password** for the Tripwire Enterprise administrator account.

# 81. Click Sign In.



82. Click **Configure Tripwire Enterprise** to begin the configuration process.



# **Tripwire Enterprise Agent Installation**

- 1. **Run** te\_agent.msi.
- 2. Click Next >.



#### 3. Check I accept the terms in the license agreement.

#### 4. Click Next >.



5. Specify an installation directory for the Tripwire Enterprise Agent.

#### 6. Click Next >.

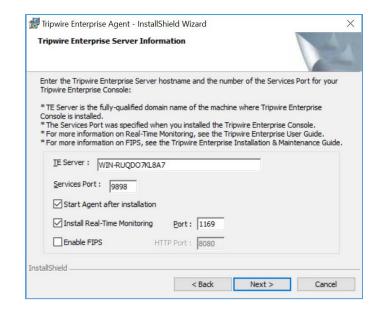
	ext to install to this folder, or click Change to install to a different folder.	-	
D	Install Tripwire Enterprise Agent to: C:\Program Files\Tripwire\TE\Agent\ Chan	Change	

- 7. Enter the **TE Server** identifier (e.g., **WIN-RUQDO7KL8A7**) of the server where Tripwire Enterprise is installed.
- 8. Enter **9898** as the **Services Port** established during the installation process of Tripwire Enterprise.
- 9. After installation, check Start Agent.

### 10. Check Install Real-Time Monitoring and specify a Monitoring Port.

#### 11. Uncheck Enable FIPS.

12. Click Next >.



13. Specify a **Proxy Host** and **Proxy Port** if necessary.

#### 14. Click Next >.

Enterprise Server		Enterprise Proxy hos	municate with the Tripwire tname and port number for your
Proxy Host:			(leave blank for no proxy)
Proxy Port:	(leave	blank for default)	(), (d)
	,		

15. Enter the Services Password created during the installation process for Tripwire Enterprise.

#### 16. Click Next >.



# 17. Click Install.

Ready to Install the Program			
The wizard is ready to begin installation			
Click Install to begin the installation.			
If you want to review or change any of exit the wizard.	your installation s	ettings, dick Back. C	lick Cancel to
nstallShield			

18. Wait for the installation process to complete.

The prog	gram features you selected are being installed.
i 🖗	Please wait while the InstallShield Wizard installs Tripwire Enterprise Agent. This may take several minutes. Status:

# 19. Click Finish.

👮 Tripwire Enterprise Agent	t - InstallShield Wizard	×
<b>ENTERPRISE</b>	InstallShield Wizard Completed	
8.6	The InstallShield Wizard has successfully installed Tripwire Enterprise Agent. Click Finish to exit the wizard.	
CONFEDENCE SECURED		
nstallShield		
	< Back Finish Cancel	

# 2.6 Enterprise Domain Identity Management

For this build, enterprise domain identity management relied upon Microsoft Active Directory, domain name system (DNS), and dynamic host configuration protocol (DHCP). Digital certificates were also implemented for services that enable certificate-based authentication. The build implemented these core services.

# 2.6.1 Domain Controller with AD, DNS, and DHCP

Within the PACS architecture, we established a Windows Server 2012 R2 Domain Controller to manage AD, DNS, and DHCP services for the enterprise. The following section details how the services were installed.

## System Requirements

- CPU: 1
- Memory: 4 GB RAM
- Storage: 120 GB (thin provision)
- Operating System: Microsoft Windows Server 2012 R2
- Network Adapter: VLAN 1201

## **Enterprise Domain Services Installation**

Install the DC, AD, and DNS appliances according to the instructions detailed in *Building Your First Domain Controller on 2012 R2* [5].

## **DNS Server Forward Lookup Zone Configuration**

1. Open Server Manager.

shboard	WELCOME TO SERVER MANAGER						
Local Server:     MA Servers     MA DOS     GO     CONTRACTOR OF CONTRACTOR     DOS     Montanti Contractor     Contreator     Contractor     Contractor     Contractor     Contracto	QRACESTART	gure this local server I roles and features I other servers to manage ate a server group					
	Riteric 1   Server granger 1   Servers total	Yiii         DHCP         1           O         Manageability         Events           Services         Performance         BPA results	DNS 1 Manageability Events Services Performance BPA results	File and Storage 1 Services 1 Thread Services 1 Events Services Performance BPA results	Local Server 1     Managasbility     Events     Services     Performance     BPA results	All Servers T Manageability Events Services Performance BPA results	

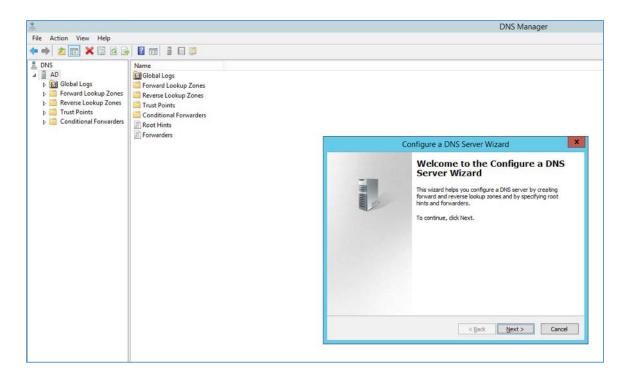
- 2. In the top right, click **Tools > DNS.**
- 3. The DNS forward lookup zone should have already been created during the DNS setup process performed previously. If not, follow these instructions:

•	🕲   🍢 Manage Tools View Help
_	Active Directory Administrative Center
	Active Directory Domains and Trusts
	Active Directory Module for Windows PowerShell
	Active Directory Sites and Services
	Active Directory Users and Computers
	ADSI Edit
	Component Services
	Computer Management
	Defragment and Optimize Drives
_	DHCP
	DNS
	Event Viewer
	Group Policy Management
	iSCSI Initiator
	Local Security Policy
_	ODBC Data Sources (32-bit)
	ODBC Data Sources (64-bit)
	Performance Monitor
	Resource Monitor
	Security Configuration Wizard
All	Services
_	System Configuration
🗊 Ma	System Information
Eve	Task Scheduler
Ser	Windows Firewall with Advanced Security
Per	Windows Memory Diagnostic
100.00	Windows PowerShell
BP	Windows PowerShell (x86)
	Windows PowerShell ISE
	Windows PowerShell ISE (x86) Windows Server Backup

a. Right-click your server's name, and select **Configure a DNS Server...** 

• m) 🙎	1 📰 🗙 🖾 🙆	🕒 🖬 🖬 🖬 🖓	
DNS		Name Right Logr	
Þ	Configure a DN		
	New Zone Set Aging/Scave		
	All Tasks		
	View	•	
	Delete Refresh Export List		
	Properties		
	Help		

b. Click Next >.



- c. Click Next >.
- d. Under Select Configuration Action, select Create a forward loading zone...

Configure a DNS Server Wizard
Select Configuration Action You can choose the lookup zone types that are appropriate to your network size. Advanced administrators can configure root hints.
Select the action you would like this wizard to perform:
Create a forward lookup zone (recommended for small networks) This server is authoritative for the DNS names of local resources but forwards all other queries to an ISP or other DNS servers. The wizard will configure the root hints but not create a reverse lookup zone.
Create forward and reverse lookup zones (recommended for large networks) This server can be authoritative for forward and reverse lookup zones. It can be configured to perform recursive resolution, forward queries to other DNS servers, or both. The wizard will configure the root hints.
Configure root hints only (recommended for advanced users only) The wizard will configure the root hints only. You can later configure forward and reverse lookup zones and forwarders.
< <u>B</u> ack <u>N</u> ext > Cancel

e. Click Next >.

- f. Under Primary Server Location, select This server maintains the zone
- g. Click Next >.

Configure a DNS Server Wizard
Primary Server Location You can choose where the DNS data is maintained for your network resources.
Which DNS server maintains your primary forward lookup zone?
<ul> <li>This server maintains the zone The wizard will help you create a primary forward lookup zone.</li> <li><u>A</u>n ISP maintains the zone, and a read-only secondary copy resides on this server The wizard will help you create a secondary forward lookup zone.</li> </ul>
< <u>B</u> ack <u>N</u> ext > Cancel

- h. Enter **PACS.TEST** as the **Zone name** that was established previously during setup.
- i. Click Next >.

New Zone Wizard	>
Zone Name What is the name of the new zone?	
The zone name specifies the portion of the DNS namespace for which this se authoritative. It might be your organization's domain name (for example, mi or a portion of the domain name (for example, newzone.microsoft.com). The not the name of the DNS server. Zone name:	icrosoft.com)
PACS.TEST	
PACS.TEST	
< <u>B</u> ack <u>N</u> ext >	Cancel

j. Select Allow only secure dynamic updates.

NIST SP 1800-24C: Securing Picture Archiving and Communication System (PACS)

#### k. Click Next >.

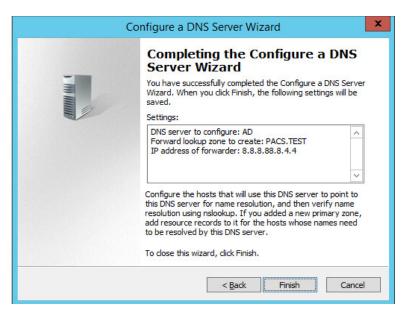
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur. Select the type of dynamic updates you want to allow: Allow only secure dynamic updates (recommended for Active Directory)) This option is available only for Active Directory-integrated zones. Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any client. This option is a significant security vulnerability because updates can be	Dynamic U You can updates	specify that this DNS zone accepts secure, nonsecure, or no dynamic
<ul> <li>Allow only secure dynamic updates (recommended for Active Directory)) This option is available only for Active Directory-integrated zones.</li> <li>Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any client.</li> <li>This option is a significant security vulnerability because updates can be</li> </ul>		
This option is available only for Active Directory-integrated zones.  Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any client. This option is a significant security vulnerability because updates can be	Select th	e type of dynamic updates you want to allow:
Dynamic updates of resource records are accepted from any client. This option is a significant security vulnerability because updates can be		
A This option is a significant security vulnerability because updates can be		
accepted from untrusted sources.	Dyna 🗘	
O Do not allow dynamic updates Dynamic updates of resource records are not accepted by this zone. You must updat these records manually.		mic updates of resource records are not accepted by this zone. You must update

I. Add Forwarders (8.8.8.8 and 8.8.4.4 are Google's DNS servers).

### m. Click Next >.

	ould this DNS serve Yes, it should forw	r forward queries? ard queries to DNS servers	with the following IP	addresses:
	IP Address	Server FQDN	Validated	Delete
	Click here to ad 8.8.8.8	d an IP Address or DNS Na google-public-dns		
	8.8.4.4	google-public-dris		Up
				Down
0	No, it should not fo	orward queries		
		t configured to use forward	lers, it can still resolv	e names using

n. Click Finish.

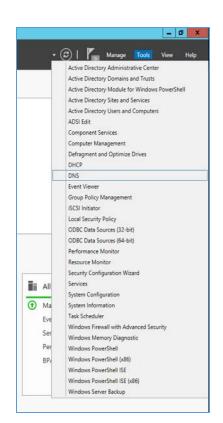


## **DNS Server Reverse Lookup Zone Configuration**

1. Open Server Manager.

			Server Man	ager			- 0
) - Server Ma	anager • Dashboard					• 🗇   🍢 Mariage Iook	Xew
Dashboard Local Server	WELCOME TO SERVER MANAGER						
Local before: # Al Servers # AD DS # DHO ▲ DHS # File and Storage Services ♪	Quick start 2 Add 3 Add	gure this local server I roles and features I other servers to manage ate a server group					3
	AD DS 1 Managesbilty Events Services Performance BPA results	Image: DHCP         1           Image: DHCP </th <th>DNS 1 Manageability Events Services Performance BPA results</th> <th>Image         File and Storage         1           Image: Services         1         1           Image: Services         1         1           Services         1         1           Services         1         1           Performance         1         1           BPA results         1         1</th> <th>Local Server 1     Marageability     Events     Services     Performance     BPA results</th> <th>All Servers 1 C Manageability Events Services Performance BPA results</th> <th></th>	DNS 1 Manageability Events Services Performance BPA results	Image         File and Storage         1           Image: Services         1         1           Image: Services         1         1           Services         1         1           Services         1         1           Performance         1         1           BPA results         1         1	Local Server 1     Marageability     Events     Services     Performance     BPA results	All Servers 1 C Manageability Events Services Performance BPA results	

2. In the top right, click **Tools > DNS.** 



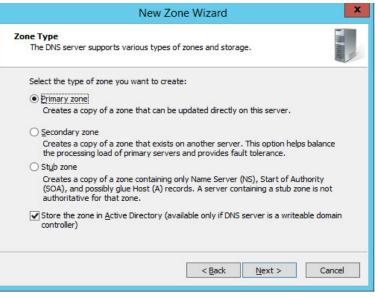
3. Right-click Reverse Lookup Zones folder, and select New Zone...

å							DNS Manager
File Action View							
🗢 🔿 🙍 🙆	) 🗟 🛛 🖬						
a DNS		Name	Туре	Status	DNSSEC Status	Key Master	
A D		_msdcs.PACS.TEST	Active Directory-Integrated Pr	Running	Not Signed		
Global Logs		PACS.TEST	Active Directory-Integrated Pr	Running	Not Signed		
Forward Lookup Zones     msdcs.PACS.TEST							
p S PACS.TE							
Reverse Loo							
<ul> <li>Trust Point</li> <li>Condition</li> </ul>	New Zon	e					
	Refresh						
	Help						

4. Click **Next >.** 

🔿 🙋 🛅 🧟 🕞 🖬 🖬				
DNS     DNS     DNS     DNS     Global Logs     Gnotal Lookup Zones     D    modes/PACS.TEST     Reverse Lookup Zones     Trust Points     Conditional Forwarders	Name	Type Active Directory-Integrated Pr Active Directory-Integrated Pr	DNSSEC Status Not Signed Not Signed	: Key Master
				New Zone Wizard X Welcome to the New Zone Wizard This waard helps you create a new zone for your DNS server. A zone translates DNS names to related data, such as IP addresses or network services. To continue, dick Next.
				< [lock [jext > Cancel

- 5. Click Next >.
- 6. Under Zone Type, select Primary zone.
- 7. Select the **Store the zone in Active Directory...** checkbox.
- 8. Click Next >.



- 9. Click Next >.
- 10. Under Active Directory Zone Replication Scope, Select To all DNS servers running...
- 11. Click Next>.

	ne Replication Scope you want DNS data replicated throughout your netw	ork.
Select how you wa	nt zone data replicated:	
○ To <u>a</u> ll DNS serve	ers running on domain controllers in this forest: PACS.	TEST
● To all <u>D</u> NS serve	ers running on domain controllers in this domain: PACS	TEST
O To all domain co	ntrollers in this domain (for Windows 2000 compatibilit	ty): PACS.TEST
	ntrollers in this domain (for Windows 2000 compatibilit	
	•	
	•	
	•	

12. Choose the Internet Protocol version 4 (IPv4)—IPv4 Reverse Lookup Zone option—and click Next >.

New Zone Wizard	x
Reverse Lookup Zone Name A reverse lookup zone translates IP addresses into DNS names.	
Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.	
IPv <u>4</u> Reverse Lookup Zone	
○ IPv <u>6</u> Reverse Lookup Zone	
< <u>B</u> ack <u>N</u> ext > Cancel	]

13. Establish what IP addresses should be included in reverse lookup (the example above encompasses all devices in the **192.168.120.0/24** subnet), then click **Next** >.

	New 2	Zone Wizard	x
	rse Lookup Zone Name reverse lookup zone translates IP ac	dresses into DNS names.	
	Network ID: 192 .168 .120 . The network ID is the portion of th network ID in its normal (not reversed) If you use a zero in the network ID	rpe the network ID or the name of the zone e IP addresses that belongs to this zone. Er sed) order. 1, it will appear in the zone name. For examp .0.in-addr.arpa, and network ID 10.0 would	nter the
0	Re <u>v</u> erse lookup zone name: 120.168.192.in-addr.arpa		
		< <u>B</u> ack Next >	Cancel

14. Choose the Allow only secure dynamic updates (recommended for Active Directory) option, then click Next >.

New Zone Wizard
Dynamic Update You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur. Select the type of dynamic updates you want to allow: (     Allow only secure dynamic updates (recommended for Active Directory)) This option is available only for Active Directory-integrated zones.
<ul> <li>Allow both nonsecure and secure dynamic updates</li> <li>Dynamic updates of resource records are accepted from any client.</li> <li>This option is a significant security vulnerability because updates can be accepted from untrusted sources.</li> <li>Do not allow dynamic updates</li> <li>Dynamic updates of resource records are not accepted by this zone. You must update these records manually.</li> </ul>
< <u>B</u> ack <u>N</u> ext > Cancel

# 15. Click Finish.

Completing the New Zone Wizar
You have successfully completed the New Zone Wizard. Yo specified the following settings:
Name:       120.168.192.in-addr.arpa       ^         Type:       Active Directory-Integrated Primary         Lookup type:       Reverse         V
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.
To close this wizard and create the new zone, click Finish.

# **DHCP Server Installation**

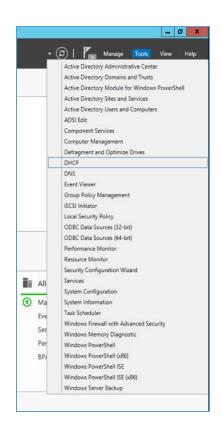
Install the DHCP server according to the instructions detailed in *Installing and Configuring DHCP Role on Windows Server 2012* [6].

## **DHCP Server Configuration**

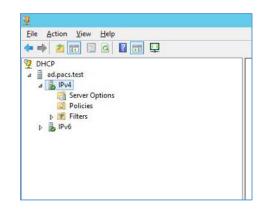
1. Open Server Manager.

			Server Man	ager		
)) - Server M	lanager • Dashboard					• 🕲   🎢 Manage Jook
Dashboard	WELCOME TO SERVER MANAGER					
Local Server All Servers AD DS DHCP DHCP DHS File and Storage Services IP	QUACISTANT 2 / 3 / BINATS NEW 4 0 LEANN MORE ROLES AND SERVER GROUPS	nfigure this local server Add roles and features Add other servers to manage Create a server group				
	Rolec 4   Server groups: 1   Servers to	1 1 1 DHCP 1	DNS 1	File and Storage 1	Local Server 1	All Servers 1
	Manageability     Events	Manageability     Events	Manageability     Events	Manageability     Events	Manageability     Events	Manageability     Events

2. In the top right, click **Tools > DHCP.** 



3. If you see a green check mark on the **IPv4** server, the DHCP server is up and running.



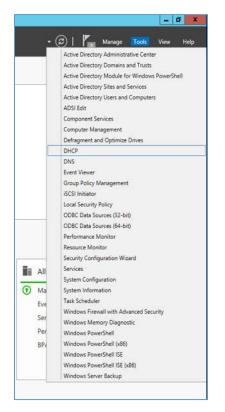
# **DHCP Scopes Configuration**

Performed on Windows Server 2012 R2

1. Open Server Manager.

			Server Man	ager			- 0
🖯 🕙 = 🛛 Server M	anager • Dashboard					• 🗇   🍢 Manage Ioc	ts Xiew
Dashboard Local Server	WELCOME TO SERVER MANAGER						
Local Berver AD DS AD DS DHCP DHCS File and Storage Services IP	ginox staat 3 Ad	gure this local server d roles and features d other servers to manage sate a server group					н
	Roles 4   Server groups 1   Server total AD DS 1	T T DHCP 1 T	DNS 1 Managesbitty Events Services Performance BPA results	File and Storage 1 Services 1 Manageability Events Services Performance BPA results	Local Server 1 C Manageability Events Services Performance BPA results	All Servers 1 C Manageability Events Services Performance BPA results	

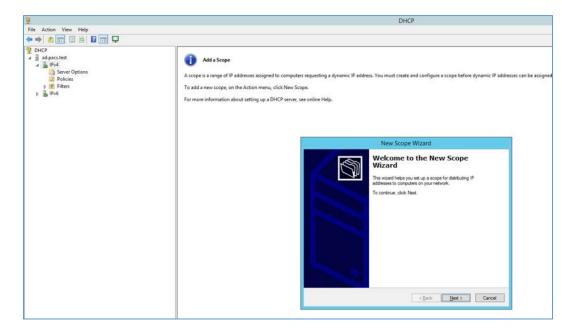
2. In the top right, click **Tools > DHCP**.



3. Right-click IPv4, and select New Scope...

		DHCP
	View Help	
	5 G 🛛 🖬 🖵	
pacs.t	est	Add a Scope
IP.d.	Display Statistics	
	New Scope	A scope is a range of IP addresses assigned to computers requesting a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assign
P	New Multicast Scope	To add a new scope, on the Action menu, click New Scope.
	Configure Failover	For more information about setting up a DHCP server, see online Help.
	Replicate Failover Scopes	
	Define User Classes	
	Define Vendor Classes	
	Reconcile All Scopes	
	Set Predefined Options	
	View	
	Refresh	
	Properties	
	Help	

### 4. Click Next >.



5. Provide a Name such as Radiology Devices and a Description such as Collection of hospitals Radiology equipment in the New Scope Wizard.

## 6. Click Next >.

	New Scope Wizard
Scope Name	Les ales and a second s
You have to pr a description.	rovide an identifying scope name. You also have the option of providing
	nd description for this scope. This information helps you quickly identify is to be used on your network.
N <u>a</u> me:	Radiology Devices
Description:	Collection of hospitals Radiology equipment
<u>_</u>	

- 7. Establish the IP range (192.168.120.200–192.168.120.254) from which the DHCP server should hand out IPs for devices in this scope.
- 8. Click Next >.

Configuration settings	for DHCP Server	
Enter the range of ad	dresses that the scope distributes.	
Start IP address:	192 . 168 . 120 . 200	
End IP address:	192 . 168 . 120 . 254	
<u>L</u> ength: S <u>u</u> bnet mask:	24 <u>+</u> 255 . 255 . 255 . 0	

9. Click Next >.

	New Scope Wizard
	ses or a range of addresses that are not distributed by the ime duration by which the server will delay the transmission of a
	ange that you want to exclude. If you want to exclude a single ess in Start IP address only.
Start IP address:	End IP address:
Excluded address rang	ge: Remoye
	Subnet delay in milli second:
	0÷
	< Back Next > Cancel

10. Configure preferred Lease Duration (e.g., 8 days), and click Next >.

11. Choose Yes, I want to configure these options now, then click Next >.



12. Enter the subnet's Default Gateway as 192.168.120.1.

## 13. Click Add.

New Sco	pe Wizard	
, or default gatew	rays, to be distributed by this scope.	Ø
router used by cli	ents, enter the address below.	
Add		
<u>R</u> emove		
Up		
Down		
	< <u>B</u> ack <u>N</u> ext > C	Cancel
	, or default gatew router used by cli Add <u>Remove</u>	Eemove Up Down

#### 14. Click Next >.

2 address:     Add       192.168.120.1     Bemove       Up     Down	Add           68.120.1         Remove           Up         1
Цр	
Down	Down
	DOWN

- 15. Ensure IP address in bottom-right box is the IP address (**192.168.120.101**) for the DNS server configured earlier.
- 16. Click Next >.

You can specify the pare DNS name resolution	ent domain you want	the client computers on your ne	twork to use for
	TEST		
Parent domain: PACS.	.1631		
	nts to use DNS serve	rs on your network, enter the IP	addresses for those
servers.			
Server name:		I <u>P</u> address:	-
1			Add
	Resolve	192.168.120.101	Remove
			<u>Ш</u> р

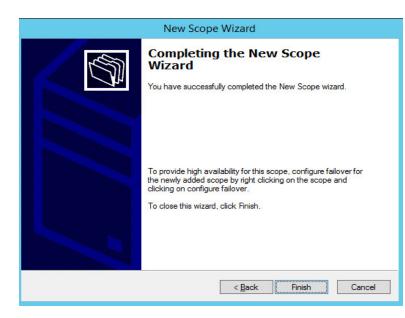
17. Click Next >.

Entering server IP addresses here enables V		S before they use
broadcasts to register and resolve NetBIOS r Server name:	names. I <u>P</u> address:	
		A <u>d</u> d
Resolve		<u>R</u> emove
		Up
		D <u>o</u> wn
To change this behavior for Windows DHCP Type, in Scope Options.	clients modify option 046, W	INS/NBT Node

18. Choose Yes, I want to activate this scope now option, then click Next >.

New Scope Wizard	
Activate Scope Clients can obtain address leases only if a scope is activated.	Ŋ
Do you want to activate this scope now? • Yes, I want to activate this scope now • No. I will activate this scope later	
< <u>B</u> ack <u>N</u> ext > Cancel	

19. Click Finish.



- 20. Scope should appear under the **IPv4** drop-down. Ensure **Scope Options** are correctly established with these values:
  - **003 Router:** 192.168.120.1
  - 006 DNS Servers: 192.168.120.101
  - 015 DNS Domain Name: PACS.TEST

2				DHCP
<u>File Action View H</u> elp				
🗭 🔿 📶 🙆 🕞 📓 🚮 🖑				
	Option Name O03 Router O06 DNS Servers	Vendor Standard Standard	Value 192.168.120.1 192.168.120.101	Policy Name None None
Cope (152: 106: 2000) Address Pool     Address Pool     Address Pool     Address Pool     Scope Options     Policies     Policies     Policies     Policies     Policies     Policies     Policies     Policies	👔 015 DNS Domain Name	Standard	PACS.TEST	None

# 2.6.2 DigiCert PKI

DigiCert is a cloud-based platform designed to provide a full line of SSL certificates, tools, and platforms for optimal certificate life-cycle management. To use the service, an account must be established with DigiCert. Once an account is established, access to a DigiCert dashboard is enabled. From the dashboard, DigiCert provides a set of certificate management tools to issue PKI certificates for network authentication and encryption for data-at-rest or data-in-transit as needed.

The instructions below describe the process to obtain an SSL certificate on behalf of medical devices using the DigiCert certificate signing services.

## Create CSR

A CSR is represented as a block Base64 encoded Public Key Cryptography Standards (PKCS)#10 binary format text that will be sent to a CA for digital signature when applying for an SSL certificate. The CSR identifies the applicant's distinguished common name (domain name), organization name, locality, country, and the public key. The CSR is usually generated from the device where the certificate will be installed, but it can also be generated using tools and utilities on behalf of the device to generate a CSR. Below are instructions on how to use the Certificate Utility for Windows (*DigiCertUtil.exe*) provided by DigiCert to generate CSRs for a medical device or a server.

Download and save the *DigiCertUtil.exe* from the DigiCert site [7].

- 1. Double-click *DigiCertUtil.exe* to run 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).
  - Certificate Type: Select SSL
  - Common Name: HYLAND-VNA.pacs.hclab
  - Subject Alternative Names: HYLAND-VNA.pacs.hclab
  - Organization: \*\*\*\*\*\*\*
  - Department: HCLAB
  - City: Rockville
  - State: Maryland
  - Country: USA
  - Key Size: 2048
- 4. Click **Generate** to create 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*.

rtificate Details		Information
Certificate Type:	● SSL ○ Code Signing	Certificate Type (required)
Common Name:	HYLAND-VNA.pacs.hclab	Choose how you are going to use the certificate.
Subject Alternative Names:		If you choose SSL, then the certificate will be saved in the machine certificate store. If you choose Code Signing, then the certificate will be saved in your own certificate store.
Organization:	NIST-NCCoE	Store.
Department:	HCLAB	
City:	Rockville	
State:	Maryland	✓
Country:	USA	×
Key Size:	2048	~

5. The figure below is a sample CSR.

0			
The certificate real	quest has been succ	essfully created.	
BEGIN HEW CERTIFICATE REQUEST HILDITCOLAICA, AND TEALANGAL URBANCHALTARBANTALA TANAN HILDITCOLAICA, AND TEALANGAL URBANCHALTARBANTALA TANAN HILDITCOLAICA, AND TEALANGAL URBANCHALTARBANTALA TANAN HILDITCOLAICA, AND TEALANGAL UNBANCHALTARBANTALA TANAN HILDITCOLAINAN HILDI			
	Copy CSR	Save to File	Close

6. Select and copy the certificate contents to the clipboard or save to an American Standard Code for Information Interchange text file. Use the text contents to paste into the DigiCert order form.

- 7. Issue Signed Certificates. With a created applicant CSR, request a signed certificate using DigiCert CertCentral portal by following these steps:
  - Log in to a DigiCert dashboard (<u>https://www.digicert.com/account/login.php</u>) with your account username and password. In the portal, select CERTIFICATES > Requests, then navigate to Request a Certificate, and select Private SSL to open a certificate request form.
  - Paste the CSR information to the area called Add Your CSR, including the -----BEGIN NEW CERTIFICATE REQUEST----- and -----END NEW CERTIFICATE REQUEST----- tags. Once the pasting is done, some of the fields will be populated automatically.
  - c. After filling in all 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.

digicert <sup>®</sup>   CERTCENTR	AL <sup>®</sup> Enterprise					
👎 REQUEST A CERTIFICATE						
The QUEUT A GENTINATE	4 Select a Product					
I DASHBOARD	Request Private SSL Certificate					
II DAGIBOARD	For National Institute of Standards and Techno	ology				
CERTIFICATES						
Orders	Certificate Settings					
Requests	Add Your CSR 🕜					
	Click to upload a CSR or paste one below					
Domains	madem waw Cantoniana angonia wandinichaningkwawanakialumaha/wamanaywamagulahinalawalkama marejiyarilahanilahinani yangwamanahaningkamajyarijiana					
Organizations	2gi2004eeinggevrewigenterviewick(rvkins.nebrievrevggeteeing2					
Expiring Certificates	Bith bighter dynawic marken warger waar mad proch op mennen wer gen gin 1 is die werge 7 wie an een ich- Der Victure - kannanzen die genaan Sterken die maans dwer Land (2014 ALT) geneier gelaat D mal gin 2- okteere - Toa mal wer 70 zu 66 die dat die gelaag voor door zoor al 2014 zij voor door die die die d					
Certificate Authority New	m Saja Lei-Johnen Taran Marina Jun Kalaga Lei Andra Jangarova Saran Saran Sala Saran Sala Saran Sala Saran Sala Januar Jangarova Saran Sala Orang Sala Sala Sala Sala Sala Sala Sala Sal					
Ceruicate Authority Nam	warmanalin Sing in Lincole Vieweller and fan Sing in Sing Sing Sing Sing Sing Sing					
( INSPECTOR	To remain secure, certificates must use keys which are at least 2048 bits in length.					
	Common Name					
FINANCES	+Show Recently Created Domains					
ACCOUNT	HYLAND-VNA.pacs.hclab					
	Include both [your-domain].com and www.[your-domain].com in the certificate					
SETTINGS	Validity period					
	1 year					
F TOOLS	2 years					
P TOOLS	<ul> <li>3 years</li> </ul>					
	Oustom expiration date					
	O Custom length					
	Important! After February 20, 2018, DigiCert will no longer offer 3-year public SSL/TLS certificates	. For more information a	bout this change, <b>click here</b> .			
	Additional Certificate Options 🗸					
	Additional Certificate Options V					
	Organization					
	Organization Info :	Û				
	NIST-NCCoE	_				
	Private SSL Validated					
	9700 Great Seneca Hwy					
	Rockville, MD, US 20850					
	301-975-0212					
	Cantanta					
	Contacts					
	Organization Contact	Û				
	Kangmin Zheng					
	Sr. Cybersecurity Engineer kzheng@mitre.org					
	301-975-0291					

8. The certificate is listed under **Orders.** Once the order status changes to Issued, the certificate is ready for download.

REQUEST A CERTIFICATE	Ordore						
	Orders						
d DASHBOARD	Request a Certificate +	Orders Report	Download CSV -				
Orders	Status	Search					
	Active		Go Show Advanced Search				
	Order # 👻	Date 0	Common Name	Status 🗘	Validity 🖗	Product 0	Expires 🛡
	6226463   Quick View	05 Jun 2019	HYLAND-NILREAD.pacs.hclab	Issued	3 years	Private SSL	04 Jun 2020
Certificate Authority	6221759   Quick View	05 Jun 2019	nccoess1.stnccoe.isyntax.net	Issued	3 years	Private SSL	04 Jun 2020
INSPECTOR	6221720   Quick View	05 Jun 2019	HYLAND-VNA-pacs helab	Issued	3 years	Private SSL	04 Jun 2020
	5655577   Quick View	24 Apr 2019	HYLAND-PGCORE,pacs.hclab	Issued	3 years	Private SSL	23 Apr 2020
		23 Apr 2019	HYLAND PGCRE.pacs.hdab	Issued	3 years	Private SSL	22 Apr 2020
) FINANCES	5643403   Quick View	20 10 2019					

- 9. Click a specific order number to display the certificate details with a list of actions that can be performed. 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.
- 10. Save the downloaded certificate in a location where it can be used for further processing if needed.

# Import and Export the Signed Certification

After downloading the SSL certificate from DigiCert, you can use the DigiCert Certificate Utility for Windows to install it. With the DigiCert Utility tool, you can further manipulate the certificates to combine with the private key and export the signed certificate to the certificate requesting device server.

- From the DigiCert Certificate Utility for Windows, click the Import button to load the downloaded signed Certificate file to the utility. The downloaded file was saved in step 10 of <u>Section 2.6.2</u>. Click the Next button to import.
- 2. From the DigiCert Certificate Utility for Windows, click SSL to list all the imported files.
- 3. To export the certificate, select the certificate 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, then click **Export Certificate**.

digicert	CERTIFICATE UTILITY I	ir stindaws*	<b>C</b> 1.	800.896.79	73			
						support@digicert.com	Live Chat	
	SSL Certificates		<sup>Ch</sup> Crea	te CSR 🏝 Impo	rt <sup>C</sup> Refresh			
	Issued To	Expire	Serial Number					
G	HYLAND-VNA.pacs	04-JUN	071B282BD0	Hyland-vna	DigiC			
SSL	ISECertByDigiCert	18-FEB	0F0747E430	ISECertByD	DigiC			
SSL								
-								
Code Signing								
code Signing								
×								
Tools								
Z								
Account								
	Export C	ertificate	Test Key	View	Certificate			
	Captore C	er er retrou	reactivey	Tien				

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

🖸 DigiCert Certificate Utility for Windows©	Х
Certificate Export	
This wizard will export a certificate and optionally its private key from the certificate store to disk.	
You must select the private key option if you wish to install this certificate on a different computer.	
Do you want to export the private key with this	
● Yes, export the private key	
● pfx file	
O key file (Apache compatible format)	
$\bigcirc$ No, do not export the private key	
< Back Next > Cancel	

## 2.7 Network Control and Security

Network control and security was implemented throughout the network infrastructure. The build features perimeter security that includes firewall feature sets and network traffic monitoring. The internal lab environment implements VLANs to establish network zones. Modality devices are further isolated by using micro-segmentation. The build also includes behavioral analysis tools that alert upon anomalous activity.

## 2.7.1 Cisco Firepower

Cisco Firepower, consisting of Cisco Firepower Management Center and Cisco Firepower Threat Defense, is a network management solution that provides firewall, intrusion prevention, and other networking services. For this project, Firepower was used to provide network segmentation and both internal and external routing. Access control and intrusion prevention policies were also implemented.

## **Cisco Firepower Management Center Appliance Information**

- CPUs: 8
- RAM: 16 GB
- Storage: 250 GB (thin provision)
- Network Adapter 1: VLAN 1201
- Operating System: Cisco Fire Linux

## **Cisco Firepower Management Center Virtual Installation Guide**

Install the Cisco Firepower Management Center Virtual appliance according to the instructions detailed in *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide* [8].

## **Cisco Firepower Threat Defense Appliance Information**

- CPUs: 8
- RAM: 16 GB
- Storage: 48.5 GB (thin provision)
- Network Adapter 1: VLAN 1201
- Network Adapter 2: VLAN 1201
- Network Adapter 3: VLAN 1099
- Network Adapter 4: VLAN 1099
- Network Adapter 5: Trunk Port
- Network Adapter 6: Trunk Port

- Network Adapter 7: VLAN 1101
- Network Adapter 8: VLAN 1101
- Network Adapter 9: VLAN 1701
- Operating System: Cisco Fire Linux

#### **Cisco Firepower Threat Defense Virtual Installation Guide**

Install the Cisco Firepower Threat Defense Virtual appliance, according to the instructions detailed at *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide* [9].

#### Adding Firepower Threat Defense (FTD) Appliance to Firepower Management Center (FMC)

- 1. Log in to the FMC Console.
- 2. Navigate to **Devices > Device Management.**
- 3. Click the Add drop-down button and select Add Device.

Overview Analysis Policies Dev	vices Objects AMP	Intelligence		Deploy 🔒 S	ystem Help <del>v</del> adm
Device Management NAT VPN	<ul> <li>QoS Platform Set</li> </ul>	tings FlexConfig C	ertificates		
Device Management					
ist of all the devices currently registered on the	he Firepower Management Cen	ter.			
View By : Group Y All	(1)   Error (1)   Warning	(0)   Offline (0)   Norma	(0)   Deployment Pending (0)	🔍 Search Device	💿 Add 🗸
Name	Model	Vers Chassis	Licenses	Access Control Poli	<ul> <li>Device</li> </ul>
📁 Ungrouped (1)					High Availability
					Stack
					Group

- 4. Enter **192.168.120.141** as the **IP address** of the FTD appliance.
- 5. Enter **FTD-PACS** as a **display name** to identify the FTD appliance.
- 6. Enter the manager key created when configuring the manager on the FTD appliance.
- 7. Click the Access Control Policy drop-down and select Create New Policy.
  - a. Create a **name** for the policy.
  - b. Select Block All Traffic.
  - c. Click Save.
- 8. Under Smart Licensing, check the boxes next to Malware, Threat, and URL.
- 9. Under Advanced, check the box next to Transfer Packets.

### 10. Click Register.

st of all the devices currently registered on the Firepow	ver Management C	enter.		
View By : Group Y All (1)	rror (1)   Warni Model	ng (0)   Offline (0)   No Version C	ormal (0)   Deployment P	ending (0)
4 💋 Ungrouped (1)		Add Device		? ×
		Host:†	192.168.120.141	
		Display Name:	FTD-PACS	
		Registration Key:*	cisco123	
		Group:	None	~
		Access Control Policy:*	PACS Global Policy	•
		Smart Licensing Malware:		
		Threat:		
		URL Filtering:	•	
		Advanced Unique NAT ID:†		
		Transfer Packets:	<ul> <li>✓</li> </ul>	
		On Firepower Threat VPN licenses can be enabled	t Defense devices version 6 abled from smart license pa	.2.1 onwards, AnyConnect ge tegister Cancel

11. The FTD appliance will be added to the FMC's **device list.** 

Overview Analysis Policies Devices	Objects AMP Inte	elligence			Deploy 🎈	System	Help 🔻	admin
Device Management NAT VPN -	QoS Platform Settings	FlexConfig	) Certificates					
Device Management								
ist of all the devices currently registered on the Fire	power Management Center.							
View By : Group Y All (1)	Error (1)   Warning (0)	Offline (0)	Normal (0)   Deployment Pending (0	)	🔍 Search De	vice	() A(	dd 🕶
Name	Model	Version		Licenses	Access Control Policy			
4 🧔 Ungrouped (1)					1			
FTD-PACS 192.168.120.141 - Routed	FTD for VMWare	6.3.0.3	N/A	Base, Threat (2 more)	PACS Global Policy	0 🗑	2	

### FTD Interfaces for PACS Architecture Configuration

Each physical interface connected to the Cisco FTD will appear in the FMC device management section under the interface tab. To configure the eight subnets needed for the PACS architecture while also allowing management, diagnostic, and wide area network (WAN) traffic, we dedicated two interfaces set up as a redundant pair for all internal subnet traffic. To accomplish this, a sub-interface was created for each of the eight PACS subnets (e.g., Enterprise Services, Imaging Modalities, Security Services) and established redundant interfaces for WAN traffic and traffic on VLAN 1101. The following guidance describes how the redundant interfaces and sub-interfaces were created.

- 1. Log in to the FMC Console.
- 2. Navigate to **Devices > Device Management.**
- 3. Find your FTD device and click the **edit** icon.
- 4. Navigate to Add Interfaces > Redundant Interface.

D-PACS					You have unsaved char	ages 🔚 Save 🔞
Firepower Threat Defense for VMWard	ne Sets DHCP					
					🔍 Search by name	Sync Device 🛛 🔇 Add Inte
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Sub Interface
Diagnostic0/0	diagnostic	Physical				Redundant Interface
GigabitEthernet0/0		Physical				Bridge Group Inter
GigabitEthernet0/1		Physical				J
GigabitEthernet0/2		Physical				P
GigabitEthernet0/3		Physical				0
GigabitEthernet0/4		Physical				2
GigabitEthernet0/5		Physical				<i>\$</i>
GigabitEthernet0/6	Guest	Physical	GUEST		192.168.170.1/24(Static)	0
Redundant1	WAN	Redundant	WAN		10.32.50.130/28(Static)	Ø 6
Redundant2	LAN	Redundant				eP E
Redundant2.1201	Enterprise-Services	SubInterface	Enterprise-Services		192.168.120.1/24(Static)	08
Redundant2.1301	Clinical-Workstations	SubInterface	Clinical-Workstations		192.168.130.1/24(Static)	Ø 6
Redundant2.1401	PACS-A	SubInterface	PACS-A		192.168.140.1/24(Static)	P 6
Redundant2.1402	PACS-B	SubInterface	PACS-B		192.168.141.1/24(Static)	e 6
Redundant2.1501	Radiology	SubInterface	Radiology		192.168.150.1/24(Static)	🧈 B
Redundant2.1601	Clinical-Applications	SubInterface	Clinical-Applications		192.168.160.1/24(Static)	🥔 B
Redundant2.1801	Data-Center	SubInterface	Data-Center		192.168.180.1/24(Static)	08
108 C. C.	Provide Produce	P. 6.1.4	erender eredere	Disp	aying 1-18 of 18 interfaces   € 《 )	

- 5. Enter Internal-Network as the name for the redundant interface.
- 6. Create and/or add a **security zone** to the redundant interface.
- 7. Assign a **Redundant ID** (e.g., **Internal-Network**) to the redundant interface.
- 8. Select a primary interface and secondary interface for the redundant pair.

Device Management NAT V		S Platforr			FlexConfig				
Isco Firepower Threat Defense for VMWar									
Device Routing Interfaces Inli	ine Sets D	НСР	-	-	_	_	-	_	Search b
Interface	Log	ical Name		Туре	Sec	urity Zones	MAC Add	lress (Active/Standby)	IP Ad
Diagnostic0/0	dia	Add Redu	ndant	Interfa	ace				? ×
GigabitEthernet0/0			IPv4	IPv6	Advanced				
GigabitEthernet0/1		General	1974	IPV6	Advanced				
GigabitEthernet0/2		Name:			Internal-Net	twork		Enabled 🛛 Manag	gement Only
GigabitEthernet0/3		Description:							
GigabitEthernet0/4		Security Zon	0"		Internal-Net	huade		-	
GigabitEthernet0/5		MTU:	<b></b>			work	(64 - 9000)		
GigabitEthernet0/6	Gu				1500				1
🗃 Redundant1	WA	Redundant I	D *:		3		(1 - 8)		2
🗃 Redundant2	LA	Primary Inte	rface:		GigabitEthe	met0/4 ¥			
	En	Secondary In	nterface		GigabitEthe	met0/5 💌			1
Redundant2.1201									
Redundant2.1201	Cliv								1

- 9. Navigate to the **IPv4** tab.
- 10. Assign an IP address and netmask (e.g., 192.168.100.101/24) to the interface.
- 11. Click **OK.**

TD-PACS sco Firepower Threat Defense for VMWar	0	m Settings 🛛 Fle	xConfig Certificates		
Device Routing Interfaces Inli	ne Sets DHCP				Search by r
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Add
Diagnostic0/0	dia Add Redu	ndant Interface	8		? X
GigabitEthernet0/0		IPv4 IPv6	Advanced		
GigabitEthernet0/1	General				
GigabitEthernet0/2	IP Type:		e Static IP 👻	eg. 192.0.2.1/255.255.255.128 or	
GigabitEthernet0/3	IP Address:	192	2.168.100.101/24	192.0.2.1/25	
GigabitEthernet0/4					
GigabitEthernet0/5					
GigabitEthernet0/6	Gu				168
🗃 Redundant1	W£				2.5
Redundant2	LA				
Redundant2.1201	En				168
Redundant2.1301	CII				168
Redundant2.1401	PA				168
Redundant2.1402	PA			OK Ca	ancel 168

#### 12. Navigate to Add Interfaces > Sub Interface.

D-PACS						Sine 🛛 🔞
o Firepower Threat Defense for VMWar	8					
evice Routing Interfaces Inlin	ne Sets DHCP					
		-				Sync Device O Add Inte
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Redundant Interfac
GigabitEthernet0/1		Physical				Bridge Group Interf
GigabitEthernet0/2		Physical				67
GigabitEthernet0/3		Physical				a
GigabitEthernet0/4		Physical				0
GigabitEthernet0/5		Physical				1
GigabitEthernet0/6	Guest	Physical	GUEST		192.168.170.1/24(Static)	1
Redundant1	WAN	Redundant	WAN		10.32.50.130/28(Static)	08
Redundant2	LAN	Redundant				/6
Redundant2.1201	Enterprise-Services	SubInterface	Enterprise-Services		192.168.120.1/24(Static)	/ 6
Redundant2.1301	Clinical-Workstations	SubInterface	Clinical-Workstations		192.168.130.1/24(Static)	28
🐻 Redundant2.1401	PACS-A	SubInterface	PACS-A		192.168.140.1/24(Static)	/ 8
Redundant2.1402	PACS-B	SubInterface	PACS-B		192.168.141.1/24(Static)	26
Redundant2.1501	Radiology	SubInterface	Radiology		192.168.150.1/24(Static)	00
Redundant2.1601	<b>Clinical-Applications</b>	SubInterface	Clinical-Applications		192.168.160.1/24(Static)	a 🖉
Redundant2.1801	Data-Center	SubInterface	Data-Center		192.168.180.1/24(Static)	28
Redundant2.1901	Security-Services	SubInterface	Security-Services		192.168.190.1/24(Static)	28
Redundant3	Internal-Network	Redundant	Internal-Network		192.168.100.101/24(Stati	ic) 🥔 🖥
				Dir	playing 1-19 of 19 interfaces 🔣 🔇 1	Page 1 of 1 > >

- 13. Enter **VNA** as the **name** for the subinterface.
- 14. Create and/or add a **security zone**, **VNA**, to the subinterface.
- 15. Select an interface under which the subinterface will operate.

Note: For our build, we placed each subinterface under **Redundant 2**, the redundant interface for **GigabitEthernet0/2** and **GigabitEthernet0/3**. These two physical interfaces were the destination for each VLAN's traffic.

- 16. Assign **1403** as the **Sub Interface ID** to the subinterface.
- 17. Assign 1403 as the VLAN ID to the subinterface.

	/PN V Qo	S Platform Se	ttings	FlexConfig Certificat	es		
TD-PACS							
isco Firepower Threat Defense for VMWa							
Device Routing Interfaces In	ine Sets D	нср	_			Search I	by na
Interface	Log	ical Name	Туре	Security Zones	MAC Address (Active/Standby)		Addre
GigabitEthernet0/1		Add Sub Inter	rface			7 ×	
GigabitEthernet0/1							
GigabitEthernet0/2	-	General IPv	4 IPv6	Advanced			
		Name:		VNA	C Enabled 🔲 Mana	agement Only	
GigabitEthernet0/4		Description:					
GigabitEthernet0/5	Gu	Security Zone:			~		168.1
GigabitEthernet0/6				VNA	(64 - 9000)		1
Redundant1	W/	MTU:		1500	(64 - 9000)		2.50.
Redundant2	LA	Interface *:		Redundant2	<ul> <li>Image: A set of the set of the</li></ul>		-
Redundant2.1201	En	Sub-Interface ID	*:	1403	(1 - 4294967295)		168,1
Redundant2.1301	Cli	VLAN ID:		1403	(1 - 4094)		168.1
Redundant2.1401	PA						168.1
Redundant2.1402	PA						168.1
Redundant2.1501	Ra						168.1

- 18. Navigate to the **IPv4** tab.
- 19. Assign an IP address and netmask (e.g., 192.168.142.1/24) to the subinterface.
- 20. Click **OK.**

TD-PACS					
sco Firepower Threat Defense for VMWar	e				
Device Routing Interfaces Inl	ne Sets DHCP	_			Search I
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP A
GigabitEthernet0/1	Add Sub I	interface			? ×
GigabitEthernet0/2	General	IPv4 IPv6	Advanced		
GigabitEthernet0/3	IP Type:	Use	e Static IP		
GigabitEthernet0/4	IP Address:	192	2.168.142.1/24	eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25	
GigabitEthernet0/5				192.0.2.1/25	
GigabitEthernet0/6	Gu				
Redundant1	W/				
Redundant2	LA				
Redundant2.1201	En				
Redundant2.1301	Cli				
Redundant2.1401	PA				
Redundant2.1402	PA				
Redundant2.1501	Ra			OK Can	ral

### 21. Click Save.

- 22. Click **Deploy** and wait for deployment to FTD to complete.
- 23. Refresh the page and confirm that the redundant interface and subinterface are running (shown with a green dot on the interface's icon).

TD-PACS						Save 🛛 🕄 G
co Firepower Threat Defense for VMWar						
levice Routing Interfaces Inli	ne Sets DHCP				Search by name	a 🕢 Add Inters
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	
GigabitEthernet0/2		Physical				0
GigabitEthernet0/3		Physical				0
GlgabitEthernet0/4		Physical				0
GigabitEthernet0/5		Physical				0
GigabitEthernet0/6	Guest	Physical	GUEST		192.168.170.1/24(Static)	0
Redundant1	WAN	Redundant	WAN		10.32.50.130/28(Static)	/8
Redundant2	LAN	Redundant				08
Redundant2.1201	Enterprise-Services	SubInterface	Enterprise-Services		192.168.120.1/24(Static)	00
Redundant2.1301	Clinical-Workstations	SubInterface	Clinical-Workstations		192.168.130.1/24(Static)	/8
Redundant2.1401	PACS-A	SubInterface	PACS-A		192.168.140.1/24(Static)	00
Redundant2.1402	PACS-B	SubInterface	PACS-B		192.168.141.1/24(Static)	/8
Redundant2.1403	VNA	SubInterface	VNA		192.168.142.1/24(Static)	28
Redundant2,1501	Radiology	SubInterface	Radiology		192.168.150.1/24(Static)	28
Redundant2,1601	Clinical-Applications	SubInterface	Clinical-Applications		192.168.160.1/24(Static)	00
Redundant2.1801	Data-Center	SubInterface	Data-Center		192.168.180.1/24(Static)	/ 6
Redundant2.1901	Security-Services	SubInterface	Security-Services		192.168.190.1/24(Static)	00
Redundant3	Internal-Network	Redundant	Internal-Network		192.168.100.101/24(Static)	08
				Display:	ng 1-20 of 20 interfaces 🔣 🔇 Page 🛛	of1 > >

### DHCP Relay Through Cisco Firepower Management Center Configuration

- 1. Log in to the FMC Console.
- 2. Navigate to **Devices > Device Management.**
- 3. Find your FTD device and click the **edit** icon.

Overview Analysis Policies Device	s Objects AMP	Intelligence		Deploy 0	System Help <del>v</del> admin
Device Management NAT VPN •	QoS Platform Set	tings FlexConfig	Certificates		
Device Management					
List of all the devices currently registered on the Fi	epower Management Cen	ter.			
View By : Group Y All (1)	Error (1) Warning	(0)   Offline (0)   Non	mal (0)   Deployment Pending (0)	🔍 Search Dev	vice 💽 Add 🔹
Name	Model	Vers Chassis	Licenses	Access Control Poli	
4 📁 Ungrouped (1)					
FTD-PACS 192.168.120.141 - Routed	FTD for VMWare	6.3.0.3 N/A	Base, Threat (2 more)	PACS Global Policy	0
					Edit

4. Navigate to the **DHCP** tab.

Overview Analysis Policies	Devices Objects AMP Inte	lligence	Deploy 🏮 System Help 🔻 admin 🔻
Device Management NAT	VPN • QoS Platform Settings	FlexConfig Certificates	
FTD-PACS Cisco Firepower Threat Defense for VMV	Ware		Save Cancel
Device Routing Interfaces	Inline Sets DHCP		
DHCP Server     DHCP Relay     DDNS	Ping Timeout     50       Lease Length     3600       Auto-Configuration     Interface       Override Auto Configured Settings:     Domain Name       Primary DNS Server     Interface	(10 - 10000 ms) (300 - 10,48,575 sec)	× ©
	Secondary DNS Server Server Advanced Interface	Secondary WINS Server      Address Pool	Co     Enable DHCP Server

5. Navigate to the **DHCP Relay Agent** section.

TD-PACS	- 10414		🔚 Save 🛛 😢 Cano
sco Firepower Threat Defense fo Device Routing Interface			
DHCP Server	IPv4 Relay Timeout: 60	Seconds Range: 1-3600	
DDNS		interiger 2 5005	
	IPv6 Relay Timeout: 60	Seconds Range: 1-3600	
	DHCP Relay Agent DHCP Servers		
	Interface	Enable DHCP Relay	Set Route(IPv4)
	Clinical-Workstations	V (IPv4 only)	✓
	PACS-A	V (IPv4 only)	✓
	PACS-A PACS-B	<ul><li>✓ (IPv4 only)</li><li>✓ (IPv4 only)</li></ul>	4
			•
	PACS-B	✓ (IPv4 only)	×
	PACS-B Radiology	<ul><li>✓ (IPv4 only)</li><li>✓ (IPv4 only)</li></ul>	√ √
	PACS-B Radiology Clinical-Applications	<ul> <li>✓ (IPv4 only)</li> <li>✓ (IPv4 only)</li> <li>✓ (IPv4 only)</li> </ul>	✓ ✓ ✓
	PACS-B Radiology Clinical-Applications Data-Center	<ul> <li>✓ (IPv4 only)</li> </ul>	✓ ✓ ✓ ✓ ✓

## 6. Under DHCP Relay Agent, click Add.

۸dd م
۵. Add
C Add
O Add
Ø 🖥
0
a 🖉 🖯
Ø 8
J 8
a 🖉 🗄
J 8
Ø 🖥
/ 0

7. Assign an FTD interface as LAN.

- 8. Check the box next to Enable IPv4 Relay.
- 9. Check the box next to Set Route.
- 10. Click OK.

Overview Analysis Policies	Devices Objects AMP Inte	lligence	De
Device Management NAT	VPN VOS Platform Settings	FlexConfig Certificates	
FTD-PACS			You
Cisco Firepower Threat Defense for VM	Ware		
Device Routing Interfaces	Inline Sets DHCP		
DHCP Server			
DHCP Relay	IPv4 Relay Timeout: 60	Seconds Range: 1-3600	
DDNS			
	IPv6 Relay Timeout: 60	Seconds Range: 1-3600	
	DHCP Relay Agent DHCP Servers		
		Add DHCP Relay Agent Configuration 🦙 🛪	
	Interface	Interface*	Set Route(IPv4)
	Clinical-Workstations	DHCP Relay: Chable IPv4 Relay	✓
	PACS-A	✓ Set Route	1
	PACS-B	Enable IPv6 Relay	4
	Radiology	OK Cancel	<b>√</b>
	Clinical-Applications	✓ (IPv4 only)	4
		(II VY ONY)	

11. Ensure that the new relay, LAN, is in the DHCP Relay Agent list.

TD-PACS			You have un	isaved changes 📄 Save 🔀 C
to Firepower Threat Defense for VMW	are			
evice Routing Interfaces In	aline Sets DHCP			
DHCP Server				
DHCP Relay	IPv4 Relay Timeout: 60	Seconds Range: 1-3600		
DDNS				
	IPv6 Relay Timeout: 60	Seconds Range: 1-3600		
	DHCP Relay Agent DHCP Servers			
				O Ado
	Interface	Enable DHCP Relay	Set Route(IPv4)	
	PACS-A	V (IPv4 only)	✓	a 🖉 🖥
	PACS-B	V (IPv4 only)	✓	a 🖉
	Radiology	V (IPv4 only)	✓	a 🖉 🖥
	and the second			6
	Clinical-Applications	(IPv4 only)	<b>v</b>	
	Data-Center		4	a 🖉 🖥
		✓ (IPv4 only)		J 1
	Data-Center	<ul><li>✓ (IPv4 only)</li><li>✓ (IPv4 only)</li></ul>	×	
	Data-Center Security-Services	✓ (IPv4 only)	4 4	J 1

12. Under DHCP Servers, click Add.

Overview Analysis Policies	Devices Objects AMP Inte	lligence	Deploy 🍳 System Help 🔻 admin 🔻
Device Management NAT	VPN  ve QoS Platform Settings	FlexConfig Certificates	
FTD-PACS Cisco Firepower Threat Defense for VM	IWare		E Save Cancel
Device Routing Interfaces	Inline Sets DHCP		
DHCP Server  DHCP Relay DDNS	IPv4 Relay Timeout: 60	Seconds Range: 1-3600	
	IPv6 Relay Timeout: 60 DHCP Relay Agent DHCP Servers	Seconds Range: 1-3600	
	DHCr Keiay Agent DHCr Servers		O Add
	Server	Interface	
	DHCP-AD-Server	Enterprise-Services	a 🖉 🛱

13. Click the green + button to create a new object for the DHCP server.

Overview Analysis Policies	Devices Objects AMP Intelligence	
Device Management NAT	VPN <b>v</b> QoS Platform Settings FlexConfig Certificates	
FTD-PACS Cisco Firepower Threat Defense for VMW Device Routing Interfaces I	are DHCP	
DHCP Server  DHCP Relay DDNS	IPv4 Relay Timeout: 60 Seconds Range: 1-3600	
	IPv6 Relay Timeout:     60     Seconds     Range: 1-3600       DHCP Relay Agent     DHCP Servers	
	Server Add DHCP Relay Server Configuration ? ×	
	DHCP-AD-Server Contract Contra	
	OK Cancel	

- 14. Enter **Test-DHCP-Server** as a **name** for the DHCP server.
- 15. Enter **192.168.100.170** as an **IP address** for the DHCP server.
- 16. Click Save.

	Devices Objects AMP PN ▼ QoS Platform Setti	Intelligence ngs FlexConfig Certificat	es	_	_
FTD-PACS Cisco Firepower Threat Defense for VMWare Device Routing Interfaces Inlin	e ne Sets DHCP				
DHCP Server  DHCP Relay DDNS	IPv4 Relay Timeout: 60	Seconds	Range: 1-3600		
	IPv6 Relay Timeout: 60	Seconds			
	DHCP Relay A New Network	Object			? ×
	Name:	Test-DHCP-Server			
	Server Description:				
1	DHCP-AD-Serv				
	Network:	Host     Range	Network	FQDN	
		192.168.100.170			
	Allow Overrides:				
				Save	Cancel

- 17. Select the newly created DHCP server.
- 18. Select an **FTD interface** through which the **DHCP server** can be connected.
- 19. Click OK.

Overview Analysis Policies	Devices Objects AMP In	telligence
Device Management NAT	VPN VOS Platform Settings	FlexConfig Certificates
FTD-PACS Cisco Firepower Threat Defense for VM	Ware	
Device Routing Interfaces	Inline Sets DHCP	
DHCP Server  DHCP Relay DDNS	IPv4 Relay Timeout: 60	Seconds Range: 1-3600
	IPv6 Relay Timeout: 60	Seconds Range: 1-3600
	DHCP Relay Agent DHCP Servers	
	Server	Add DHCP Relay Server Configuration ? ×
	DHCP-AD-Server	Server Test-DHCP-Server   Interface Internal-Network
		OK Cancel

20. Ensure that the new server is in the **DHCP Server** list.

#### 21. Click Save.

22. Click **Deploy** to add the new configuration settings to the FTD appliance.

Overview Analysis Policies	Devices Objects AMP Int	elligence		Deploy 🕛 System	Help 🔻 🛛 admin 👻
Device Management NAT	VPN VOS Platform Settings	FlexConfig Certificates			
FTD-PACS				You have unsaved changes	Save 🔀 Cancel
Cisco Firepower Threat Defense for VMW	Nare				
Device Routing Interfaces I	Inline Sets DHCP				
DHCP Server					
DHCP Relay	IPv4 Relay Timeout: 60	Seconds Range: 1-	3600		
DDNS					
	IPv6 Relay Timeout: 60	Seconds Range: 1-	3600		
	DHCP Relay Agent DHCP Servers				
					O Add
	Server		Interface		
	DHCP-AD-Server		Enterprise-Services		Ø
	Test-DHCP-Server		Internal-Network		Ø 🗎

## Network Address Translation (NAT) Rules Configuration

1. Navigate to **Devices > NAT.** 

Device Management	NAT VPN .	QoS	Platform Setting	s FlexCor	fia	Certificates				
								C	🔾 New	r Policy
NAT Policy				Devio	е Тур	е	Status		1	
PACS NAT				Threat			Targeting 1 devices Up-to-date on all targeted devices		ФE.	0

2. Click New Policy > Threat Defense NAT.

Device Management	NAT VPN	QoS	Platform Settings	FlexConfig	Certificates			
								New Policy
NAT Policy				Device Typ	e	Status		Firepower NAT
PACS NAT		Threat Defense		Targeting 1 devices		Threat Defense NAT		
PACSINAT				Inreat Deren	150	Out-of-date on 1 targeted devices	<u> </u>	

- 3. Give the new policy a Name as PACS NAT.
- 4. Assign the **FTD appliance** to the new NAT policy.
- 5. Click Save.

IAT Policy		Device Type		Status
PACS NAT	1	Threat Dafanas		Targeting 1 devices
	New Policy Name: Description: Targeted Device	PACS NAT		1
	Select devic Available D	es to which you want to apply thi	is policy. Selected De	
	CT 1	ACS :	Add to Policy	

- 6. Click the NAT policy's **edit** icon.
- 7. Click Add Rule.
- 8. Set NAT Rule to Auto NAT Rule.
- 9. Set Type to Dynamic.
- 10. Under Interface Objects, set Source Interface Object to one of the FTD appliance's LAN interfaces.
- 11. Set Destination Interface Object to the FTD appliance's WAN interface.

	evice Managemen	t NAT	VPN VOS	Platform Sett	ings riex	Config	Certificates				
P/	ACS NAT									You have unsave	d chan
int	ter Description										
łu	les										
	Filter by Device										
			Add NAT Rule								? ×
	Direction	Туре	NAT Rule:	Auto NAT Rule	<b>~</b>						
P	NAT Rules Before		Type:	Dynamic		Enable					
A	Auto NAT Rules		Interface Objects	Translation	PAT Pool	Advance					
2	+	Dynamic	Available Interface O	CONVERSION ON T	PAT POOL		<ul> <li>Source Interface Object</li> </ul>	s (1)	Destination Interfac	e Objects (1)	
	+	Dynamic	Search by name				- VNA	6	wan		3
	+	Dynamic	Guest-Services		•						
	+	Dynamic	Imaging-Modalities			id to ource					
	+	Dynamic	PACS-A			id to ination					
	+	Dynamic	ACS-B								
	+	Dynamic	VNA								
	+	Dynamic	WAN								
		Dynamic									
1											

12. Under **Translation,** set **Original Source** to the **network** that corresponds with the source interface object established in the previous step.

## 13. Set Translated Source to Destination Interface IP.

### 14. Click OK.

	verview Ana vice Manageme			bjects AMI Platform Set		xConfig Certificat	tes	Depl	ογ 🍕
PA	CS NAT							You have u	nsaved char
B F	ilter by Device								
			Add NAT Rule						? >
1	Direction	Туре	NAT Rule:	Auto NAT Rule	~				
N	AT Rules Befor	e	Type:	Dynamic	~	🖉 Enable			
A	uto NAT Rules		Interface Objects	Translation	PAT Pool	Advanced			
	+	Dynamic	Original Packet	Translation	PAT FOUL	Advanced	Translated Packet		
	+	Dynamic	Original Source:*	VNA		× 0	Translated Source:	Destination Interface IP	¥
	+	Dynamic						Objects in 'Interface Objects' tab will be u	sed
	+	Dynamic	Original Port:	TCP.	¥				
	+	Dynamic					Translated Port:		
	+	Dynamic							
	+	Dynamic							
	+	Dynamic							
	+	Dynamic							Cancel
								OK	Cancel

15. Ensure that the new **NAT Rule** has been created.

16. Repeat these steps if needed for each LAN interface attached to FTD appliance.

### 17. Click Save.

18. Click **Deploy** to add the changes to the FTD appliance.

	ter Description					You have unsaved	changes .	Save Save	🔀 Cano
łu	les							Policy A	ssignmen
h,	Filter by Device							0	Add Rul
	Direction	Туре	Source Interface Objects	Destination Interface Objects		Ori Translated Pac De Sources	2002 <b>-</b>	Options	
	NAT Rules Befo	re							
	Auto NAT Rules								
#	+	Dynamic	🔒 Security-Services	WAN	Security-Services	🍓 Interface	¢	🖲 Dns:false	0
#	+	Dynamic	🔒 Enterprise-Services	wan	Enterprise-Services	🥵 Interface		🖲 Dns:false	28
÷	+	Dynamic	📇 Clinical-Viewers	WAN	Clinical-Viewers	4 Interface	t	🖲 Dns:false	/8
#	+	Dynamic	ACS-A	wan	PACS-A	4 Interface	6	B Dns:false	00
#	+	Dynamic	PACS-B	A WAN	PACS-B	🝓 Interface		B Dns:false	0
#	+	Dynamic	Imaging-Modalities	wan	Imaging-Modalities	🍓 Interface		S Dns:false	08
#	+	Dynamic	👬 Clinical-Application-Services	🚓 WAN	Clinical-Application-Services	4 Interface		S Dns:false	08
#	+	Dynamic	Guest-Services	AN WAN	Guest-Services	🍓 Interface	d	B Dns:false	18
#	+	Dynamic	Datacenter	🚓 WAN	Datacenter	🧠 Interface	ė	B Dns:false	00
#	+	Dynamic	📩 Internal-Network	📇 WAN	🚎 Internal-Network	🝓 Interface	¢	B Dns:false	08
4	+	Dynamic	👬 VNA	📇 WAN	VNA VNA	4 Interface		B Dns:false	08
	NAT Rules After	÷							

## Access Control Policy Through Firepower Management Center Configuration

The Firepower Management Center allows configuration of access-control policies that can then be applied to individual FTD appliances. The purpose of the access-control policy is to create rules that specify how traffic is managed within the network. Each access-control policy contains multiple rules followed by a default action established when the policy is created. For the PACS architecture, one access-control policy was established to manage the traffic on each FTD interface. The steps below describe how the policy and rules were created, as well as how to utilize an intrusion policy with the access-control policy. Additional information on the Cisco Firepower access control list and intrusion prevention configuration is available [10].

1. Navigate to Policies > Access Control > Access Control.

Overview Analysis Policies	Devices Objects	AMP Intelligence			Deploy 🧕 System	Help 🔻 admin 🔻
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions •		
					Object Management Intrusion Network Analysis Policy	DNS Import/Export
Access Control Policy		Status			Last Modified	

- 2. Click New Policy.
- 3. Enter PACS Global Policy as the name for the access control policy.
- 4. For Select Base Policy, select None.
- 5. For Default Action, select Block all traffic.
- 6. Add the FTD appliance to the policy.
- 7. Click Save.

Overview Analysis Policies Access Control + Access Control		Intelligence ication Detectors	Correlation	Actions •	_	
					Object Management	Intrusio
Access Control Policy		Statue	_	_	Last Modified	
	New Policy					? ×
	Name:	PACS Global Polic	y			
	Description:					
	Select Base Policy:	None		*		
	Default Action: Targeted Devices	Block all traffic	Intrusion Prev	vention 🔘 Network Dis	covery	
	Select devices to Available Device	which you want to	apply this policy.	Selected Device	15	
	Search by na	ime or value		FTD-PACS	6	
	FTD-PACS					
			Add to P	olicy		

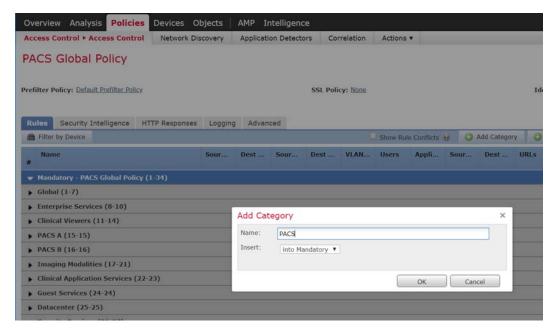
8. Click the access-control policy's edit icon.

Note: The policy in the screenshots that follow contains categories created during the process of building the PACS architecture. These categories are not preconfigured.

Overview Analysis Policies De	evices Object	s AMF	Intellig	ence							Depl	oy 🍳	System	Help ¥	admin
Access Control > Access Control	Network Discover	у Арр	lication De	tectors	Correlatio	n Actio	ns 🔻								
PACS Global Policy														Seve.	Cancel
refilter Policy: Default Prefilter Policy				55L	Policy: Nut					Identi	ity Policy	t None			
											Ta Inhe	ritance Set	ttings   🦉	Policy Assi	griments (1
Rules Security Intelligence HTTP	Responses Log	ging A	dvanced												
Filter by Device						Show	Aule Conflicts	9 0	Add Categor	y 🔾 Ad	d Rule	Search Ruk	es .		
# Name	Sourc	Dest	Sourc	Dest	VLAN	Users.	Applic	Sourc	Dest	URLS 1	SE/S			• <b>1</b> 0 - 1	•
➡ Handatory PACS Global Policy (1 3)	4)														
▶ Global (1-7)															0
Enterprise Services (8-10)															0
Clinical Viewers (11-14)															0
PACS A (15-15)															0
PACS 8 (16-16)															0
Imaging Modalities (17-21)															0
Clinical Application Services (22-23)															0
<ul> <li>Guest Services (24-24)</li> </ul>															0
Datacenter (25-25)															10
<ul> <li>Security Services (26-27)</li> </ul>															0
<ul> <li>Internal Network (28-30)</li> </ul>															0
VNA (31-33)															0
• WAN (34-34)															0
Default - PACS Global Policy (-)															

## Create a Category

- 1. Click Add Category.
- 2. Enter **PACS** as the name for the category.
- 3. Insert the category into the Mandatory section.
- 4. Click **OK.**



Create a Rule that Allows Application Traffic Between Security Zones

- 1. Click Add Rule.
- 2. Enter **PACS-VNA** as the name for the rule.
- 3. Insert the rule into the category created in the previous step.
- 4. Set Action to Allow.

Note: Because we set the default action to **block all traffic** when creating the policy, all of the rules we created were set to **Allow**.

5. Add security zone(s) to the **Source Zone**, and add security zone(s) to the **Destination Zone**.

Note: The two primary methods for adding source and destination networks to an access control rule are through security zones or networks. Security zones are objects that can contain multiple FTD interfaces. Networks can be different types of network objects, including network segments **(192.168.1.0/24)** or individual devices **(192.168.1.1)**.

Provide a contraction of the second s	intelligence tion Detectors Correlation	Actions •	Deploy 🧕 System Help 🖲
PACS Global Policy			You have unsaved changes Save
Prefilter Policy: Default Prefilter Policy Rules Security	SSI. Policy: <u>None</u>		Identity Policy: Nons
Mandatory - P	■ J C 2 2 2 2	Insert into Catego	
P OLOGICITY	Applications Ports URLs Source Zones (	SGT/ISE Attributes	Inspection Logging Comments Destination Zones (1)
	Add to Source Add to Destination	; 3	
<ul> <li>▶ WAN (34-34)</li> <li>▼ PACS (-)</li> </ul>			Add Cancel

6. Under Applications, add the application(s) you would like to allow between the specified zones.

Note: This can also be accomplished by specifying the **port** you would like to allow under the **Ports** tab. By specifying a specific port, this will open the port to all traffic regardless of the type of traffic (e.g., DICOM) being sent.

7. Click Add.

ccess Control *	Access Control Network Discover	ry Appli	cation Detectors	Correlation	Actions •				
ACS Globa	I Policy								
efilter Policy: Def	ault Prefilter Policy		S	SL Policy: None				Identity Policy:	None
								Ta Inberit	ance Settings   🗒
Rules Security	Tabelliances UTTO December 1 a							a in all a resolution	
B Filter by Device	Add Rule								?
Name	Name PACS-VNA			🕑 Enabled	In	sert Into Categor	ry 👻	PACS	~
	Action Allow		- U C.84	10					
and the second second in the	DAGREENE CONTRACTOR								
Mandatory - P		Users	-		SGT/ISE Attr	ibutes	Ins	pection Loggin	o Comments
Global (1-7)	Zones Networks VLAN Tags Application Filters C Clear All	👍 Users Filters 🗶	Applications Available Applicat	Ports URLs	SGT/ISE Attr	ibutes		pection Loggin	the second second second second
Global (1-7)	Zones Networks VLAN Tags	a his sector of the sector of	Applications	Ports URLs	SGT/ISE Attr	ibutes		Conversion and the second	tere and the second second second
Global (1-7) Enterprise Ser Clinical Viewe	Zones Networks VLAN Tags Application Filters C Clear All Search by name um multimedia (other)	a his sector of the sector of	Applications Available Applicat	Ports URLs ions (3) C	SGT/ISE Attr	lbutes	Selected App	Conversion and the second	* (2) 🧟 🖂 🕻
<ul> <li>Global (1-7)</li> <li>Enterprise Ser</li> <li>Clinical Viewe</li> <li>PACS A (15-1)</li> </ul>	Zones Networks VLAN Tags Application Filters C Clear All Search by name multimedia (other)	Filters 🗶 95 🔺 386	Applications Available Applicat	Ports URLs ions (3) C	SGT/ISE Attr	ibutes	Selected App Applications	Conversion and the second	* (2) <u>3</u> (1) (
<ul> <li>Global (1-7)</li> <li>Enterprise Ser</li> <li>Clinical Viewe</li> <li>PACS A (15-1)</li> <li>PACS B (16-1)</li> </ul>	Zones Networks VLAN Tags Application Filters C Clear All Search by name um multimedia (other)	Filters X 95 • 386 971	Applications Available Applicat Search by name All apps match DICOM OSIRIX	Ports URLs ions (3) C	0	ibutes	Selected App Applications	Conversion and the second	* (2) 🧟 🗇 🕻
<ul> <li>Global (1-7)</li> <li>Enterprise Ser</li> <li>Clinical Viewe</li> <li>PACS A (15-1)</li> <li>PACS B (16-1)</li> <li>Imaging Mode</li> </ul>	Zones Networks VLAN Tags Application Filters C Clear All Search by name multimedia (other) multimedia (VI/video) network protocols/services network utilities network utilities	Filters 🗶 95 🔺 386	Applications Available Applicat Search by name All apps matching DICOM	Ports URLs ions (3) C	SGT/ISE Attr	Add to Rule	Selected App Applications	Conversion and the second	* (2) <u>3</u> (2) (3
Global (1-7) Enterprise Ser Clinical Viewe PACS A (15-1: PACS B (16-1) Imaging Moda Clinical Applic	Zones Networks VLAN Tags Application Filters C Clear All Search by name I multimedia (other) I network protocols/services I network utilities I network utilities I news V PACS	Filters X 95 • 386 971 46 204 3	Applications Available Applicat Search by name All apps match DICOM OSIRIX	Ports URLs ions (3) C	0		Selected App Applications	Conversion and the second	* (2) <u>3</u> (2) (3
<ul> <li>Mandatory P</li> <li>Global (1-7)</li> <li>Enterprise Sei</li> <li>Clinical Viewe</li> <li>PACS A (15-1)</li> <li>PACS B (16-1)</li> <li>Imaging Mode</li> <li>Clinical Applic</li> <li>Guest Service</li> <li>Datacenter (2)</li> </ul>	Zones Networks VLAN Tags Application Filters C Clear All Search by name muttmedia (otner) muttmedia (tV/video) network protocols/services network utilities network utilities network utilities network utilities network utilities network utilities network operational services network protocols/services network utilities	Filters X           95           386           971           46           204           3           53	Applications Available Applicat Search by name All apps match DICOM OSIRIX	Ports URLs ions (3) C	0		Selected App Applications	Conversion and the second	* (2) <u>3</u> (2) (3
Global (1-7) Enterprise Ser Clinical Viewe PACS A (15-1) PACS B (16-1) Imaging Mode Clinical Applic Guest Service	Zones Networks VLAN Tags Application Filters C Clear All Search by name I multimedia (other) I network protocols/services I network utilities I network utilities I network utilities I network Quites	Filters X 95 • 386 971 46 204 3	Applications Available Applicat Search by name All apps match DICOM OSIRIX	Ports URLs ions (3) C	0		Selected App Applications	Conversion and the second	* (2) <u>3</u> (2) (3
Global (1-7) Enterprise Ser Clinical Viewe PACS A (15-1) PACS B (16-1) Imaging Mode Clinical Applic Guest Service Datacenter (2	Zones Networks VLAN Tags Application Filters C Clear All Search by name multimedia (other) multimedia (tV/video) network protocols/services network protocols/services network utilities per to peer remote administration	Pitters         X           95         •           386         •           971         •           46         •           204         •           3         •           53         •           69         •	Applications Available Applicat Search by name All apps match DICOM OSIRIX	Ports URLs ions (3) C	0		Selected App Applications	Conversion and the second	* (2) <u>3</u> (2) (3

8. Verify that the **Rule** has been created.

Overview Analysis Policies D	evices Ot	ojects	AMP Inte	lligence							Dep	loy 🍳	System	Help v	admin •
Access Control > Access Control	Network Dis	covery	Application	Detectors	Correla	tion .	Actions •								
PACS Global Policy											You have a	unsaved cha	mges 📳	Save	Cancel
refilter Policy: Default Prefilter Policy				5	SI. Policy:	None				Id	entity Polic				
Rules Security Intelligence HTTP	Responses	Logging	Advanced	£							Inh	eritance Se	ttings   📕 P	olicy Assign	ments (1
B Filter by Device						0.5	ihow Rule Conflic	ts 😣	Add Categor	Y O	Add Rule	Search Rul	65		
Name	Sourc	Dest Z	Sourc	Dest N	VLAN	Users	Applic	Sourc	. Dest P I	URLS	ISE/S	Acti		•	
Mandatory - PACS Global Policy (1-3	15)														
Global (1-7)															2
<ul> <li>Enterprise Services (8-10)</li> </ul>															0
Clinical Viewers (11-14)															0
PACS A (15-15)															0
PACS 8 (16-16)															2
Imaging Modalities (17-21)															0
Clinical Application Services (22-23	)														0
<ul> <li>Guest Services (24-24)</li> </ul>															0
Datacenter (25-25)															0
Security Services (26-27)															0
Internal Network (28-30)															0
VNA (31-33)															2
• WAN (34-34)															0
▼ PACS (35-35)															0
35 PACS-VNA	A PACS-A	als VNA	Any	Any	Any	Any	DICOM PACS	Αηγ	Ληγ	Any	Ame	🖌 Allo	•0 © /8	由口。	
Default - PACS Global Policy (-)															
Default Action									Access Co	ntrol: Bloc	k All Traffic				× .
								Dis	splaying 1 - 35 of	35 rules	K < Pag	e 1 of	1 > > 0	Page Si	ze: 100 +
Last login on Thursday, 2019-07-18 at 09:23:0	0 AM from rdp-	iumnhov nic	s.hdab										-	v To	alude

- Create a Rule that Allows Traffic on a Specific Port Between Networks
- 1. Click Add Rule.

- 2. Enter **PACS-Internet** as the **name** for the rule.
- 3. Insert the rule into the **category** created previously.
- 4. Set Action to Allow.
- 5. Under Networks, add a source network(s) and destination network(s).

erview Analysis Policies Devices C		Intelligence				Deploy 0 System
ess Control > Access Control Network Di	iscovery Applica	tion Detectors	Correlation Act	ions 🔻		
CS Global Policy					Yo	u have unsaved changes
Iter Policy: Default Prefilter Policy		S	SL Policy: <u>None</u>		Identit	ty Policy: <u>None</u>
						Ta Inheritance Settings   🛄
les Security Totallance UTTO Deservoire	Landan Ada					
Filter by Device Add Rule						? >
Name Name PACS-Internet			Enabled	Insert Into Catego	ry PACS	*
Action Allow		· UD.8:	5			
Mandatory - P Zones Networks VLAI	N Tags 🔥 Users	Applications	Ports URLs SG	T/ISE Attributes	Inspection	Logging Comments
Available Networks C	0		Source Networks (2)		Destination Networks	
Linical Viewe			Source	Original Client	👼 WAN	6
	Geolocation		PACS-A	6		
IPv6-Link-Local	*		PACS-B	6		
Imaging Moda IPv6-Private-Unique-Local-Add	dresses	Add To Source				
Clinical Applic		Networks				
uest Service PACS-B						
Patacenter (2 RDP_Jumpbox						
Security Services						
VNA			Enter an IP address			1
WAN			Conter an in dutress	Add	Enter an IP address	Add
VNA (31-33)						

6. Under **Ports**, add (a) port(s) to the **Selected Destination Ports**.

Note: Select from a group of pre-created ports or add your own port by filling out the **protocol** and **port** boxes, then click **Add** under the selected destination ports.

ccess Control + Acc	ess Control Ne	twork Discover	v Applic	ation Detectors	Correlation	Actions •				
			1 Hopking			Accord				
ACS Global P	olicy							-10	u nave unsave	d changes
efilter Policy: <u>Default (</u>	Prefilter Policy			5	SL Policy: None			Identit	y Policy: Nor	10
									Ta Inheritan	ce Settings   🛄 P
Rules Security Ad	d Rule	eessen las	alaa Adu							? ×
Name N	ame PACS-Internet				C Enabled	Insert	into Category	Y PACS		~
A Mandatory - P	ction 🕜 Allow			<ul> <li>0.0.8</li> </ul>	¥ .					
• Global (1-7)	Zones Networks	VLAN Tags	👍 Users	Applications	Ports URLs	SGT/ISE Attribute	s	Inspection	Logging	Comments
Enterprise Ser	allable Ports C		0		Selected Source	Ports (0)		Destination	Ports (2)	
Clinical Viewe	Search by name or v	alue			any		аттн %			6
PACS A (15-1	AOL .		-				🖉 нтт	S		8
	Bittorrent									
The state of the s	DNS_over_TCP			Add to Source						
	DNS_over_UDP			Add to						
	Р FTP Р HTTP									
Contraction of the local division of the loc	HTTPS									
	IMAP									
Security Servi	LDAP									
· Texternal Mater					Protocol TCP (6)	Y Port Ente	Add Protocol	1	Y Port	Enter a Add
<ul> <li>Internal Network</li> </ul>	NFSD-TCP		· ·						- Internet in the	

7. Under URLs, add URL categories that will be allowed (or leave this section blank).

Note: Cisco Firepower generates the URL categories and updates them regularly. Within each URL category, you can specify the reputation level that the URL must meet for the rule to match.

ccess Control + Access Control Network Discovery Ap	plication Detectors	Correlation	Actions *						
ACS Global Policy						You	have unsave	d changes	E
filter Policy: Default Prefilter Policy		SSL Policy: <u>None</u>				Identity	Policy: Non	a.	
						1	Inheritanc	e Settings	
Filter by Device Add Rule	diament .								? :
Name PACS-Internet		Enabled	Insert	into Category	~	PACS			~
Action Allow	· 00/8	Ca 🗉							
Global (1-7) Zones Networks VLAN Tags 🧰 User	Applications	Ports URLs	SGT/ISE Attributes	5	Ins	pection	Logging	Commen	nts
Enterprise Ser Categories and URLs C	Reputations			Select	ed URL	\$ (7)			
Clinical Viewe	Any			Bu	siness a	nd Econor	ny (Reputatio	ns 4-5)	0
PACS A (15-1: Category URLs	🚽 5 - Well Know	m		Ed.	ucationa	l Institutio	ons (Reputatio	ons 4-5)	0
PACS B (16-11	all 4 - Benign sit						(Reputations		0
Uncategorized		es with security risk	8				arch (Reputat		8
Imaging Mode Abortion	2 - Suspiciou	s sites					outations 4-5)		8
Clinical Applic Abused Drugs	着 1 - High Risk						putations 4-5		
Guest Service Stadult and Pornography				E Rei	rerence	and Resea	arch (Reputati	ons 4-5)	0
Datacenter (2 Alcohol and Tobacco									
Security Servi									
Internal Netw				(Control of the second s	000				
VNA (31-33)				Enter	URL				Add
									_

8. Under Inspection, add an intrusion policy, or leave this section blank.

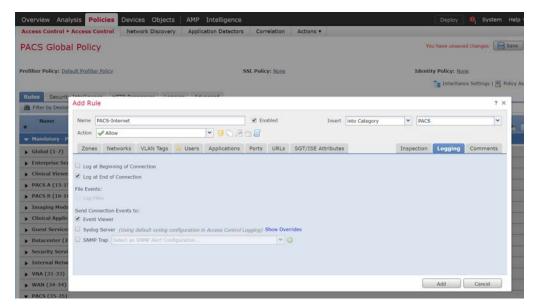
Note: Intrusion policies are created separately from the access-control policy. Once created, an intrusion policy can be applied to a specific access-control rule or an entire access-control policy. See the link posted [10] at the beginning of this section for more information on how to create and use intrusion policies in Cisco Firepower.

Overview Analy	ysis Policies	Devices Object	s AMP Intelligence					Deploy	0 System
Access Control +	Access Control	Network Discover	ry Application Detectors	s Correlation	Actions •				
PACS Globa	I Policy						1	fou have unsav	ed changes [ 🔚 S
refilter Policy: <u>Defa</u>	ault Prefilter Policy			SSL Policy: None			Iden	tity Policy: <u>No</u>	ne
								Ta Inheritar	ice Settings   🧾 Po
Roles Securit	Add Rule	The formation in the							? ×
Name	Name PACS-Int	ernet		Enabled	Insert	into Category	Y PAC	s	~
<ul> <li>Mandatory · P</li> </ul>	Action Allow		B. C 😺 💌	rea D					
• Global (1-7)	Zones Netv	vorks VLAN Tags	👛 Users Applications	Ports URLs	SGT/ISE Attributes		Inspectio	Logging	Comments
Enterprise Ser	Intrusion Policy				Variable Set				
Clinical Viewe	General-IPS			× 0	Default Set				× 0
PACS A (15-1	File Policy								
PACS B (16-10	None								~
Imaging Mode									
Clinical Applic									
Guest Service									
Datacenter (2									
Security Servi									
Internal Netw									
• VNA (31-33)									
• WAN (34-34)								Add	Cancel

9. Under Logging, select Log at End of Connection, or leave this section blank.

Note: If logging is enabled, select Event Viewer.

10. Click Add.



- 11. Verify that the access control rules have been created and placed in the proper category.
- 12. Click Save.
- 13. Click **Deploy** to add changes to the FTD appliance.

Overview Analysis Policies	Devices Ob	jects	AMP Inte	lligence	ð.,						D	epicy	Q System	Help 🔻	admin
Access Control + Access Control	Network Disc	covery	Application	Detectors	Corre	ation	Actions •								_
PACS Global Policy											You hav	e unsaver	t changes	Save	🔀 Cancel
Prefilter Policy: Default Prefilter Policy					SSL Policy:	None				Id	entity Po		e Settings   🖲 P	olicy Assig	nments (1
Rules Security Intelligence HTT	P Responses	Logging	Advanced	i											
A Filter by Device						0	Show Rule Con	flicts 💓	Add Cate	egory Q	Add Rule	Search	Rukes		3
ø Name	Sourc	Dest	Sourc	Dest	VLAN	Users	Applic	Sourc	Dest	URLS	ISE/S	Act	0 🗟 Ja 🕁		
Handatory - PACS Global Policy(1 - 36)	> PACS(35 - 3	16)													00
PACS A (15-15)															08
• PACS B (16-16)															08
Imaging Modalities (17-21)															08
Clinical Application Services (22-23	1)														08
Guest Services (24-24)															0.6
<ul> <li>Datacenter (25-25)</li> </ul>															0.6
<ul> <li>Security Services (26-27)</li> </ul>															08
<ul> <li>Internal Network (28-30)</li> </ul>															28
▶ VNA (31-33)															0.8
WAN (34-34)															08
▼ PACS (35-36)															08
35 PACS-VNA	A PACS-A	-th VNA	Any	Any	Any	Απγ	DICOM PACS	Aay	Any	Amr	Any	🖋 All	000.88	0 [] 0	/ 8
36 PACS-Internet	Any	Any	PACS-I PACS-I		Any	Any	Any	Any	HTTP HTTP	Busines Education Health a Image a (3 more	Any	🛹 All	∾ <b>∛</b> ⊜ ,8 d	9 🗐 o	08
Default - PACS Global Policy (-)															
Default Action									Access Co	ntrol: Block /	M Traffic	_	_	_	~

# 2.7.2 Cisco Stealthwatch

Cisco Stealthwatch provides network visibility and analysis through network telemetry. It provides threat detection and remediation as well as network segmentation using machine learning and behavioral modeling. This project integrates Cisco Stealthwatch with Cisco Firepower to allow Cisco FTD to send NetFlow directly to Stealthwatch for analysis.

### **Cisco Stealthwatch Management Console Appliance Information**

- **CPUs:** 3
- RAM: 16 GB
- Storage: 60 GB (thin provision)
- Network Adapter 1: VLAN 1901
- Operating System: Linux

### **Cisco Stealthwatch Management Console Virtual Edition Installation Guide**

Install the Cisco Stealthwatch Management Console appliance according to the instructions detailed in the Cisco installation guide [11].

## Cisco Stealthwatch User Datagram Protocol (UDP) Director Appliance Information

- CPU: 1
- **RAM:** 4 GB
- Storage: 60 GB (thin provision)
- Network Adapter 1: VLAN 1901
- Network Adapter 2: VLAN 1901
- Operating System: Linux

## **Cisco Stealthwatch UDP Director Virtual Edition Installation Guide**

Install the Cisco Stealthwatch UDP Director appliance according to the instructions provided in the Cisco installation guide [11].

## **Cisco Stealthwatch Flow Collector Appliance Information**

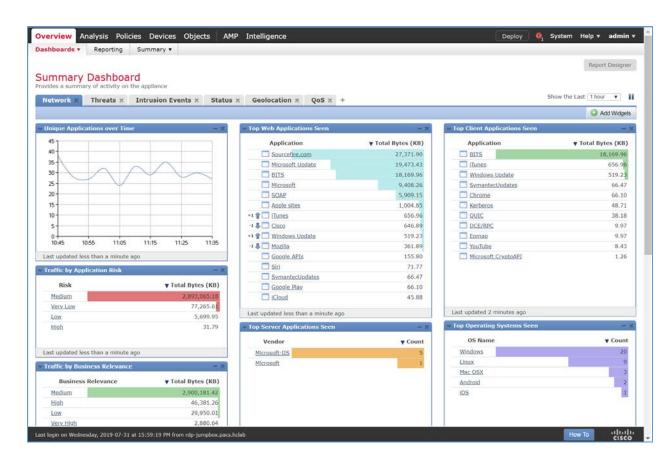
- **CPUs:** 2
- RAM: 16 GB
- Storage: 60 GB (thin provision)
- Network Adapter 1: VLAN 1901
- Operating System: Linux

## **Cisco Stealthwatch Flow Collector Virtual Edition Installation Guide**

Install the Cisco Stealthwatch Flow Collector appliance according to the instructions provided in the Cisco installation guide [11].

## **Configure NetFlow Parameters for Cisco Firepower**

1. Log in to the Cisco Firepower Management Console.



2. Navigate to **Objects.** 

etwork			Add Network •	G Filter	
	nore IP addresses. Network objects are used in various places, incl	luding access control policies, network variables, intrusion rules,	dentity rules, network disco	very rules, event sear	rches,
Network 🔶	Name	Value	Туре	Override	
J <sup>a</sup> Port Sinterface	апу	0.0.0.0/0 ::/0	Group	×	-
Tunnel Zone	any-lpv4	0.0.0.0/0	Network	×	
VLAN Tag	any-ipv6	::/0	Host	×	
Security Group Tag	Clinical-Application-Services	192.168.160.0/24	Network	×	0
Geolocation	Clinical-Viewers	192,168.130.0/24	Network	×	0
Time Range	ConsoleWorks-Network	192.168.1.0/24	Network	×	0
\$ Variable Set	Datacenter	192.168.180.0/24	Network	×	2
Security Intelligence	Domain-Controller	192.168.120.100	Host	×	0
DNS Lists and Feeds	Enterprise-Services	192.168.120.0/24	Network	×	0
URL Lists and Feeds	External_HIP	192.168.132.0/24	Network	×	0
C File List	Google-DNS-Primary	8.8.8.8	Host	×	0
Gipher Suite List	Google-DNS-Secondary	8.8.4.4	Host	×	0
Distinguished Name	Guest-Services	192.168.170.0/24	Network	×	1
B Object Groups	Imaging-Modalities	192.168.150.0/24	Network	×	0
PKI	Internal-Network	192.168.100.0/24	Network	×	0
SLA Monitor	Internal HIP	192.168.133.0/24	Network	×	0
Prefix List	IPv4-Benchmark-Tests	198.18.0.0/15	Network	×	
B IPv4 Prefix List	IPv4-Link-Local	169.254.0.0/16	Network	×	
B IPv6 Prefix List	IPv4-Multicast	224.0.0.0/4	Network	×	
Access List	1Pv4-Private-10.0.0.0-8	10.0.0.0/8	Network	Ŷ	
Standard	The survey of the second secon	10.0.0.0/8	metwork	~	

## 3. Navigate to FlexConfig > Text Object.

ext Object	trings that you use as variables in a FlexConfig object. These obje	rts ran hava sinnla values or he a list of multiple values	Add Text Object	🔍 Filter	
Individual Objects		Value	Туре	Override	
Cobject Groups	defaultDNSNameServerList	1.1.1.1	System Defined	0	0.0
PKI DNS Server Group SLA Monitor Prefix List IPv4 Prefix List	defaultDNSParameters	3 5 10 15 abc.com There are 1 more items.	System Defined	0	0 6
🛐 IPv6 Prefix List	disableInspectProtocolList		System Defined	0	15
Route Map     Access List	dnsNameServerList	2.2.2.2	System Defined	0	00
Standard Extended Y AS Path	dnsParameters	3 5 abc.com	System Defined	0	0.0
Community List	eigrpAS	1	System Defined	0	00
Policy List	elgrpAuthKey		System Defined	0	10
KEV1 Policy	eigrpAuthKeyId		System Defined	0	0
KEv2 Policy	eigrpDisableAutoSummary	false	System Defined	0	05
IKEv1 IPsec Proposal IKEv2 IPsec Proposal	eigrpDisableSplitHorizon	false	System Defined	0	0
Group Policy	eigrpHelloInterval	60	System Defined	0	0
AnyConnect File	eigrpHoldTime	180	System Defined	0	0.8
Address Pools	A. The second	100	System Defined	0	0
IPv4 Pools	eigrpIntfList				0
IPv6 Pools	eigrpRouterId		System Defined	0	
FlexConfig	elgrpStubConnected	false	System Defined	0	2 8
Generation FlexConfig Object	elgrpStubRecelveOnly	false	System Defined	0	0.0
RADIUS Server Group	eigrpStubRedistributed	false	System Defined	0	26

4. Under the Name column, find netflow\_Destination.

Overview Analysis Polic Object Management Intr	ties Devices Objects AMP Intelligence		Deploy 0 S	ystem Help	
Text Object			Add Text Object	🔍 Filter	
	strings that you use as variables in a FlexConfig object. These objects	s can have single values or be a list of multiple values. Value	Туре	Override	
Object Groups	IPv6RoutingHeaderDropLogList	4	System Defined	0	18
🤊 🔑 PKI	IPv6RoutingHeaderLogList	2	System Defined	0	0
@DNS Server Group		-		-	
SLA Monitor	isIsAddressFamily	ipv4	System Defined	0	0
Prefix List     Prefix List	isIsIntfList		System Defined	0	03
IPv6 Prefix List	isIsISType	level-1-2	System Defined	0	00
③ Route Map	istsNet		System Defined	0	00
Access List	isServiceIdentifier	false	System Defined	0	00
Sextended Y AS Path	netflow_Destination	Security-Services 192.168.190.120 2055	System Defined	0	00
Community List Policy List VPN IKEv1 Policy	netflow_Event_Types	all flow-create flow-denied flow-teardown flow-update	System Defined	0	10
IKEv2 Policy IKEv1 IPsec Proposal IKEv2 IPsec Proposal	netflow_Parameters	1 0 30	System Defined	0	0
Group Policy AnyConnect File	PrefixDelegationInside	Inside Inside-Prefix ::1:0:0:0:4/54	System Defined	0	/ 3
Address Pools	PrefixDelegationOutside	outside Outside-Prefix ::/56	System Defined	0	10
IPv6 Pools	serviceIdentifier	1	System Defined	0	1 11
Text Object	a second	0			
PlexConfig Object	tcp_conn_limit	0	System Defined	0	2 13
RADIUS Server Group		0			
· ·	e	Displ	aying 21 - 40 of 43 rows 🔣 🕻	Page 2	K ( E to

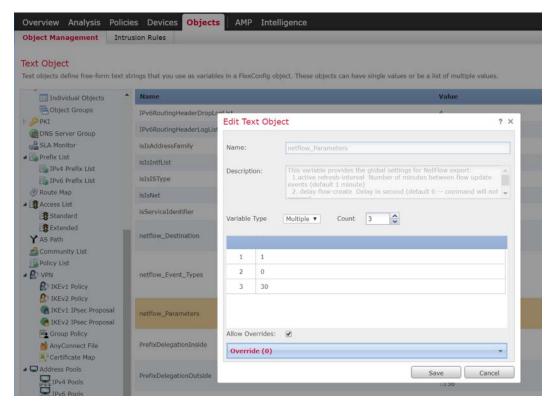
- 5. Click the edit icon for netflow\_Destination.
- 6. Set Variable Type to Multiple.
- 7. Set **Count** to **3.**
- 8. For **Row 1**, enter **Security-Service** to set the name of the Cisco FTD interface to which the Cisco Stealthwatch UDP appliance is connected.
- 9. For Row 2, enter 192.168.190.120 to set the IP address of the Cisco Stealthwatch UDP appliance.
- 10. For **Row 3**, enter **2055** to set a port from which the Cisco Stealthwatch UDP appliance will receive NetFlow traffic.
- 11. Click Save.

	strings that you use as torneet	es in a Flexe	Config ob	oject. These objects can have single values or be a list of multiple value	ues.	
- Individual Objects	* Name			Value		
Cbject Groups	IPv6RoutingHeaderDropLo	Edit Te	xt Obje	ect	?	
SLA Monitor	isIsAddressFamily	Name:		netflow Destination		
Prefix List     IPv4 Prefix List	isIsIntfList	Descript	ion:	This variable defines a single NetFlow export destination.		
IPv6 Prefix List	isIsISType	o courpe		1. Interface 2. destination		
OR Route Map	isIsNet			3. port <1-65535> UDP port number		
Access List	isServiceIdentifier	identifier Variable Type Multiple Variable Type				
Extended Y AS Path	netflow_Destination	Vundore	1700			
Community List		1	Secur	ity-Services		
A Co VPN	netflow_Event_Types	2	192.1	68.190.120		
E IKEv1 Policy		3	2055			
<ul> <li>IKEv2 Policy</li> <li>IKEv1 IPsec Proposal</li> <li>IKEv2 IPsec Proposal</li> </ul>	netflow_Parameters					
Group Policy		Allow Ov	errides:	2		
AnyConnect File	PrefixDelegationInside	Overri			_	5

12. Under the Name column, find netflow\_Parameters.

ext Object			Add Text Object	🔍 Filter
Contraction of the second second second	strings that you use as variables in a FlexConfig object. These object	s can have single values or be a list of multiple values.		
Individual Objects	* Name	Value	Туре	Override
Object Groups	IPv6RoutingHeaderDropLogList	4	System Defined	0 /
PKI () DNS Server Group	IPv6RoutingHeaderLogList	2	System Defined	0 /
SLA Monitor	IsIsAddressFamily	ipv4	System Defined	0 /
Prefix List	isIsIntflist		System Defined	0 2
IPv4 Prefix List	IsIsISType	level-1-2	System Defined	0 /
3 Route Map	isIsNet		System Defined	0 /
Access List	isService]dentifier	false	System Defined	0 /
Standard Extended Y AS Path	netflow_Destination	Security-Services 192.168.190.120 2055	System Defined	0 0
Community List Policy List VPN Community List Policy List Community List Policy List Community List	netflow_Event_Types	all flow-create flow-denied flow-teardown flow-update	System Defined	• •
IKEv2 Policy     IKEv1 IPsec Proposal     EKEv2 IPsec Proposal	netflow_Parameters	1 0 30	System Defined	• 2
Group Policy AnyConnect File R <sup>+</sup> Certificate Map	PrefxDelegationInside	inside Inside-Prefix ::1:0:0:0:4/64	System Defined	• •
Address Pools	PrefixDelegationOutside	outside Outside-Prefix ::/56	System Defined	• •
Prv6 Pools	serviceIdentifier	1	System Defined	0 /
G Text Object FlexConfig Object	tcp_conn_limit	0	System Defined	0 0

- 13. Click the edit icon for netflow\_Parameters.
- 14. Set Variable Type to Multiple.
- 15. Set Count to 3.
- 16. For **Row 1**, enter **1** as a number for minutes between flow update events.
- 17. For **Row 2**, enter **0** as a number for seconds to delay flow create.
- 18. For **Row 3**, enter **30** as a number for minutes for template time-out rate.
- 19. Click Save.



20. Navigate to **Devices > FlexConfig.** 

Overview Analysis Policies Dev	ces Objects AMP Intelligence		Deploy 🍳 System Help 🔻 admin 🔻
Device Management NAT VPN •	QoS Platform Settings FlexConfig	Certificates	
			S New Policy
FlexConfig Policy	Status		Last Modified
Hexconfig Policy	Status		Last Modified

#### 21. Click New Policy.

- 22. Enter a Name (e.g., Netflow) for the policy.
- 23. Under Selected Devices, add the Cisco FTD.
- 24. Click Save.

lexConfig Policy		Status			Last Modified
	New Policy				
	Name:	Netflow			
	Description:				
	Targeted Devices	1			
	Select device Available De	es to which you want to ap evices	ply this policy.	Selected Devices	
	Search b	y name or value		FTD-PACS	8
			Add to Policy		

25. Click the **edit** icon for the new policy.

Overview Analysis	Policies	Devices	Objects AMP In	telligence	o 30	Deplo	y 🔍 System	Help 🔻	admin v
Device Management	NAT V	PN V QoS	Platform Settings	FlexConfig	Certificates				
							0	O New	Policy
FlexConfig Policy				Status		Last Modified			
Netflow				Targeting 1 Up-to-date	t devices on all targeted devices	2019-05-07 16:04:59 Modified by "admin"		C	000
									Edit

26. Under Available FlexConfig, find Netflow\_Set\_Parameters, and add it to Selected Append FlexConfigs.

erview Analysis Policies Devices	Objects AMP	Intelligence	Deploy 0, System Help	adm
ice Management NAT VPN • Qu	oS Platform Setting	gs FlexConfig Certificates		
tflow			You have unsaved changes Preview Config Save	🖸 Ca
r bascipoon			Policy Assi	gnments
vailable FlexConfig C I PlexConfig	Object 🗖 S	Selected Prepend FlexConfigs		
	× .	Name	Description	
a 👩 User Defined				
Netflow_Delete_Destination_Temp				
4 💋 System Defined				
Default_DNS_Configure				
Default_Inspection_Protocol_Disable				
Default_Inspection_Protocol_Enable				
DHCPv6 Prefix Delegation Configure				
DHCPv6 Prefix Delegation UnConfig				
DNS Configure				
DNS_UnConfigure				
Eigrp_Configure				
Eigrp_Interface_Configure	>	Selected Append FlexConfigs		
Elgrp_UnConfigure		verected Append Hexcomigs		
Elgrp_Unconfigure_All		Name	Description	
Inspect_IPv6_Configure	1	Netflow_Set_Parameters	Set global parameters for NetFlow export.	9,8
Inspect_IPv6_UnConfigure				
ISIS Configure				
ISIS Interface Configuration				
ISIS_Unconfigure				
ISIS_Unconfigure_All				
Netflow_Add_Destination				
Netflow_Clear_Parameters				
Netflow_Delete_Destination				
Netflow_Set_Parameters				
NGFW TCP. NORMALIZATION				

- 27. Click the magnifier icon for Netflow\_Set\_Parameters.
- 28. Under Variables > Default Value, verify the minutes between flow data events, seconds to delay flow create, and minutes for template time-out rate that were set for netflow\_Parameters.

### 29. Click Close.

Description	View FlexCon	fig Object						?
	Name:	Netflow_Set_	Parameters					
iilable FlexCon	Description:	Set global par	rameters for NetFlow expo	et.				
User Defined								
Netflow_De						Deployment:	Once • Type:	Append 1
DHCPv6_P							owing kludge.	
DNS_Confil DNS_UnCo Bgrp_Confil Eigrp_Inter Eigrp_Unco Eigrp_Unco	no flow #else flow-exp #end flow-exp	-export de port delay		= "0")	rs.get(1)		oning krouger	
DNS_UnCo	no flow #else flow-exp #end flow-exp * Variables	-export de port delay	lay flow-creat	= "O") e 1 netflow_Parameter	rs.get(1)	Override .	Description	

- 30. Under Available FlexConfig, find Netflow\_Add\_Destination, and add it to Selected Append FlexConfigs.
- 31. Click the magnifier icon for Netflow\_Add\_Destination.
- 32. Under **Variables > Default Value**, verify the Cisco FTD interface name, IP address of the Cisco Stealthwatch, and the NetFlow traffic port.
- 33. Click Close.

levice Management	NAT VPN .	QoS Platform	m Settings	FlexConfig Certificates						
etflow er Description	View FlexCor	View FlexConfig Object ?								
	Name:	Netflow_Add_Desti	nation							
vailable FlexConf	Description:	Create and configu	re a NetFlow ex	port destination.						
🖌 🧭 User Defined										
Netflow_De					Dept	ayment: On	ce • Type: Append •			
DHCPv6_Pr	#forea		ype in \$	netflow Event Types )						
DNS_Config DNS_UnCor Eigrp_Confi Eigrp_Inter Eigrp_UnCo Eigrp_Unco	¢forea flow-e ≬end	ch ( \$event t	ype in \$	netflow_Event Types ) t type destination \$netflow_	Destinatio	on.get(1)				
DNS_Config DNS_UNCod Eigrp_Confi Eigrp_Inter Eigrp_UnCo	¢forea flow-e ≹end Variables	ch ( \$event t	ype in \$1 ype Sever	nt_type <sup>-</sup> destination \$netflow_						
DNS_Conflig DNS_UnCol Elgrp_Conflig Elgrp_Uncol Elgrp_Uncol Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA	¢forea flow-e ∳end Variables Kime:	ch ( \$event_t xport event-t	ype in \$	nt_type destination \$netflow_	Destinatio	Override	Description			
DNS_Config DNS_UnCod Egrp_Confi Egrp_Unco Egrp_Unco Egrp_Unco Inspect_IPA Inspect_IPA Inspect_IPA	¢forea flow-e ¢end Variables Name nettlow_Event, nettlow_Destin	ch ( \$event_t xport_event_t	ype in \$i ype \$ever Dimension	nt_type <sup>-</sup> destination \$netflow_	Property	Override				
DNS_Config DNS_Unconfig Eigrp_Config Eigrp_Unco Eigrp_Unco Eigrp_Unco Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA Inspect_IPA	forea flow-e fend Variables Name netflow_Event, netflow_Destin	ch ( \$event_t xport_event_t	ype in \$1 ype \$eve; Dimension MULTIPLE	nt_type destination \$netflow_ Default Value [al, Now-create, Now-denied, Now-teardown,	Property FREEFORM:	Override	Description This variable provides the			

### 34. Click Save.

35. Deploy changes to the Cisco FTD.

### Forwarding Rules for Cisco Stealthwatch UDP Configuration

1. Log in to the web dashboard of the Cisco Stealthwatch Management Console.

ISCO Dat	shboards	Monitor	Analyze	Jobs Cont	figure Dep	oloy		-		sktop Client 🚿
ecurity Ins	ight Dashb	oard   Ins	ide Hosts							
Alarming Ho	sts 🜒									- /
Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	0	0	0	0

2. Navigate to Settings > Central Management.

(	Dashboards	Monitor A	Analyze .	lobs Conf	igure Dep	bloy				Global Setti	ngs
-										Central Mar	nagement
ecurity Ir	nsight Dashb	oard   Insid	de Hosts								lyzer Configura
Alarming H	Josta @										or Configuration
Alarming r	iosis 🖤										okup Configura
Concern Inde	x Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Polic	User Manag	ement
0	0	0	0	0	0	0	0	0		0	0

3. Click the ellipsis for the Cisco Stealthwatch UDP appliance and select Edit Forwarding Rules.

entory					
Q Filter Appliance Inv	entory Table				
APPLIANCE STATUS	LICENSE STATUS	HOST NAME		IP ADDRESS ^	ACTIONS
Up	Up to date	flow-collector-1	Flow Collector FCNFVE-VMware- 42327ed5ea4835b5- e78156b8e8c5d80a	192.168.190.122	•
Up	Up to date	sw-management	SMC SMCVE-VMware- 4232e3086e8de2bb- 279d73cf6c6703f0	Edit Appliance Configuration View Appliance Statistics	Θ
Up	Up to date	sw-udp-director	UDP Director UDVE-VMware- 423238ff27759f21- 565093566172791d	Manage Licenses Support	o
				Edit Forwarding Rules	
				Reboot Appliance Shut Down Appliance Remove This Appliance	

4. Click the ellipsis for the Cisco Stealthwatch UDP appliance, select Configure Forwarding Rules.

sco Dashb	lthwatch <sub>oards Monitor</sub>	Analyze	Jobs	Configure	Deploy	886	esktop Client
OP Director	Configuration						
DP Directors (	Cevice IP		Device	e Model	Management Channel Status	Configure Forwarding Rules	Actions
<ul> <li>Name</li> </ul>					• •	Conligure Forwarding Rules	U.a.

5. Under Forwarding Rules, select Add New Rule.

ISCO	Dashboards Monitor	Analyze Jobs Configure	Deploy	
orwar	ding Rules   sw-udp	-director - 192.168.190.120		
	al Search			Syne rt/Export ~
	bal Search DESCRIPTION	SOURCE IP ADDRESS & POR	DESTINATION IP ADDRESS	

- 6. Enter a description (e.g., **Firepower FTD**) for the rule.
- 7. For **source IP address** and **source port**, enter the IP address and port (e.g., **192.168.190.1:2055**) of the Cisco FTD interface sending the NetFlow traffic.

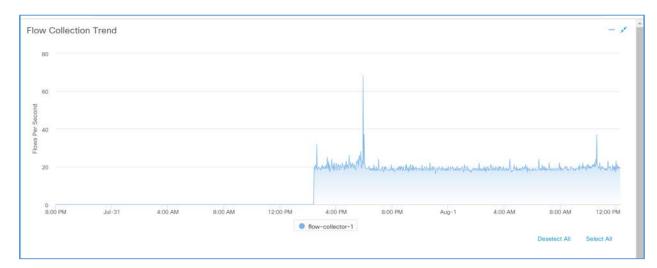
Note: These parameters were established in Cisco FTD, found in the previous section, for the netflow\_Destination object.

- 8. For **destination IP address**, enter the IP address (e.g., **192.168.190.122**) of the Cisco Stealthwatch Flow Collector.
- 9. For **destination port**, enter the port (e.g., **2055**) of the Cisco Stealthwatch Flow Collector.

Note: This port was configured during setup of the Flow Collector.

Dashboards	Monitor	Analyze	Jobs	Configure	Deploy	
orwarding Rules	sw-udp-o	director - 1	92.168.	190.120		
Forwarding Rule						
DESCRIPTION (OPTIONAL)						
Firepower ETD						
SOURCE IP ADDRESS:PORT						
192.168.190.1:2055						
DESTINATION IP ADDRESS #						
192.168.190.122						
DESTINATION PORT NUMBER	2 =					
2055						

10. On the Cisco Stealthwatch Management Console dashboard, view the **Flow Collection Trend** graph to verify that the Cisco Stealthwatch Flow Collector is receiving packets from the Cisco Stealthwatch UDP.

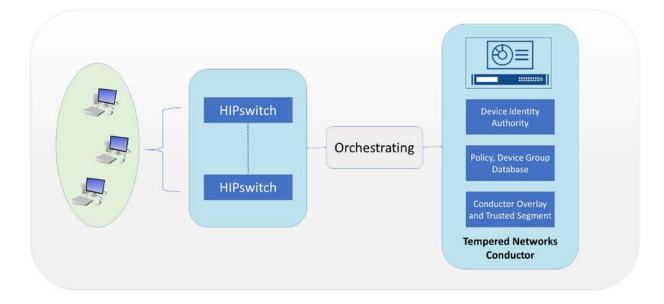


# 2.7.3 Tempered Networks Identity Defined Networking (IDN)

Tempered Networks IDN provides cryptographically defined host identifiers using the HIP protocol rather than IP addressing. Network traffic traverses an overlay network using HIPswitches that

effectively cloak that traffic from the production network. A notional architecture appears in Figure 2-2 below.





Tempered Networks Conductor is the orchestration engine and intelligence behind an IDN. As shown in the above figure, the Conductor is responsible for creating and executing security policies and overlays. It is also responsible for issuing unique cryptographic IDs to the IDN end points that enforce explicit trust relationships through device-based allow-listing.

HIPswitches are typically deployed in front of devices or hosts that cannot protect themselves, like medical devices such as modalities and other legacy systems and machines, or when customers are unable to install the proper endpoint-protection applications.

Installation involves deployments of the Tempered Networks Conductor and HIPswitches. Tempered Networks provided a conductor open virtual appliance or application (OVA) file and a HIPswitches OVA file.

## 2.7.3.1 Conductor Installation

## System Requirements

- **CPUs:** 4
- Memory: 4 GB RAM
- Storage: 120 GB

- Operating System: Linux Red Hat
- Network Adapter: VLAN 1201

### **Tempered Networks Conductor Installation**

- 1. Log in to the vSphere Client.
- 2. Select File > Deploy OVF Template.
- 3. Respond to the prompts with information specific to your deployment, including the ova package location, name and location, storage, networking, and provisioning.
- 4. Click Power On After Deployment, and click Finish.
- 5. Once the installation is done, power on the Conductor server, and log in with username **macinfo** and the corresponding password to set up the necessary MAC address and IP address.

## 2.7.3.2 HIPswitch Installation

### System Requirements

- **CPUs:** 4
- Memory: 1 GB RAM
- Storage: 1 GB
- Operating System: Linux Red Hat
- Network Adapter: VLAN 1201

### **HIPswitch Installation**

- 1. Log in to the vSphere Client.
- 2. Select File > Deploy OVF Template.
- 3. Respond to the prompts with information specific to your deployment, including the ova package location, name and location, storage, networking, and provisioning.
- 4. Click Power On After Deployment, and click Finish.
- 5. After the installation, use the username and password to connect the HIPswitch to the conductor.
- 6. Use the username **underlayaddress** and its corresponding password to set up the IP address, netmask, gateway, and DNS for the HIPswitch.
- 7. Repeat the above installation procedures to install additional HIPswitches.

## Tempered Networks Conductor and HIPswitch Configuration

Configuration for the Conductor and HIPswitches is done through the browser connected to the Conductor https://ConductorIP. The login page appears below.

1. Enter the **username** and **password** to open the dashboard.

💋 Conducto	pr	
	Sign In	
	Username Password Sign In	

2. Click the Settings tab.

ashboard						
IPservices online	HIPservice mod	Jels	HIPservice versions		Recently viewed items	
					No recently viewed items	
2/2 police	loos I nPaveto Phensios models in Constuator		toon 1v2.1.3 a forware sensors Filter	*	Alert Notifications	Event Monitor
HPservice -	Model	Status			no recent alerts	
HPSwich Internal 1101 BH@40130#4232576EA055	HPswitch-300v v2.1.3	192, 160, 100, 180	4020%		Overlay Networks	+ New.
HPSwitch Radiology 1501	HPswitch-300v v2.1.3	192 168 150 180	4080%	•	Name	
BHI@40130#4232F03DF338			Display revoked HIPse	rvices	PACS Systems	. 🖸
		0		u 1-2 of 2		
BHIQ4013044232F030F338     Sort by Name +		C		u 1-2 of 2	Devices	Filter x

3. From this page, you can set up the license and perform the system setup. Click the **Setup** button to enter the system setup.

ettings			Support Functions •
General settings Cloud providers Licensing			
Firmware Updates	Upload Firmware	Configuration	Setup
No firmware updates have been uploaded as of yet.		Hostname	
		Firmware version	
Email Settings	Edit Settings	2.1.3 Serial number	
Email Settings Email settings are incomplete. Click the Edit Settings button to update.	Edit Setanga	4232D38A953A Conductor device ID	
contraction of the second s		AMA@40130#4232D3	8A953A
Marilan & Alast Cattlera		Network adapter 1	
Monitor & Alert Settings	Edit Settings	Web access is enab	led
Global monitor settings		IP address	192.168.120.180
Frequent events warning O		Netmask	255 255 255 0
Number of events 3		Default gateway DNS servers	192 168 120 1
In how many minutes 10		Diva servers	0.0.0.0 4.4.0.0
		Network adapter 2	

4. Enter the proper network parameters for the Conductor, including the IP address (e.g., 192.168.120.180), Netmask (e.g., 255.255.255.0), Default gateway (e.g., 192.168.120.1), and DNS (e.g., 8.8.8.8, 4.4.8.8), then click Configure.

lost name conductor		Domain name
Network adapter 1	Network a	dapter 2
Enable network ada	apter	Enable web access to Conductor
letwork configuration		
Static IP		~
P address		Netmask
192.168.120.180		255.255.255.0
)efault gateway		
192.168.120.1		
ONS1		DN S2
8.8.8.8		4.4.8.8
Static Routes +		
lo static routes defined		

5. An overlay is configured to support the micro-segmentation. Click the **Overlay** tab to open the following page and add a new overlay by clicking the **+ New Overlay Network...** The screenshot below shows a configured overlay called **PACS Systems.** 

-)→ ଫ ໖	(1) Attps://192.168.120.180/app#/networks	90% ···· 🖾 🕁	W\ 🖸 📽	Ξ
🧐 Want to try someth	ning new in Firefax? Try Now			? ×
Conductor	Dashboard Overlays Devices HilPservices People Settings	Search		۵.
Overlay Netw	orks		+ New Overlay Network	
Name	Description			
PACS Systems	Allows devices in VLAN 1501 (Radiology) to communicate with devices in VLAN 1101 (Internal	D		

6. Two HIPswitches were installed to test for this project. These two HIPswitches are Model HIPswtich-300v, and they are named **HIPswitch Internal** and **HIPswitch Radiology.** Both were configured to participate in the **PACS Systems** overlay network.

-)→ C @ @	A https://192.168.120.	180/app#/networks/3			90% … 🖂 🕁	III\ 🗉 📽
Want to try something new in Firefox?	Try Now					13
Conductor Dashboard	Overlays Devices Hilf	Pservices People Setting	<b>P</b> -		Sea	rch 🔒 🛔
PACS Systems						
Devices Visualization Timeline	HIPservices		Enabled	Disabled	Info	Edit Settings
The following HIPservices are participating	in this network due to their r	levices being added.			Allows devices in VLAN communicate with device	1501 (Radiology) to es in VLAN 1101 (Internal)
To configure the devices in the network, se	ect the Devices tab.				VLAN traffic rules	
HIPservice .	Model	Status	Fiter	×	Untagged traffic Tagged traffic	Allowed Not allowed
HIPSwich Internal 1101	HIPswitch-300v	192.168.100.180	4040%			
HIPSwitch Radiology 1501	HIPswitch-300v	192, 168, 150, 180	#080%			
				Rems 1-2 of 2	Recent activity	
					No recent activity	ŝ
					People	Update

- 7. Two special VLANs were created for each of these two HIPswitches under PACS Systems overlay:
  - VLAN 1302 for HIPswitch Internal 1101
  - VLAN 1303 for HIPswitch Radiology 1501
- 8. Devices to be protected under the HIP network will be connected to these two HIPswitches through the VLANs:
  - PACS servers are connected to VLAN 1302 under the HIPswitch Internal 1101.
  - Medical imaging devices are connected to VLAN 1303 under the HIPswitch Radiology 1501.

After creating a secure layer in the Conductor and adding those medical imaging devices and PACS servers to that layer, the medical imaging device and PACS server can be set up as trusted by selecting the Enable button on the overlay page. Once they are trusted, communication between those medical imaging devices and PACS servers will be established. All the communication will be encrypted.

The microsegmentation is achieved by using the HIPswitch. Other VMs will not be able to communicate with these two devices unless they are configured to do so.

# 2.7.4 Zingbox IoT Guardian

Zingbox IoT Guardian consists of two separate components that work together to monitor and analyze network traffic. The first component is a cloud-based platform called Zingbox Cloud, which aggregates and analyzes data to provide insights into the devices on the local network. The second component is Zingbox Inspector, a local appliance that receives network flows from devices on the local network and sends specific metadata to Zingbox Cloud for further analysis.

## Zingbox Cloud Setup

- 1. Visit <u>https://zingbox.com</u> and register for an account.
- Log in to the Zingbox console and navigate to Administration > My Inspectors > Download Inspector.
- 3. Download either the .ova or the .iso file, depending on your environment's requirements.

## System Requirements

- **CPUs:** 4
- Memory: 8 GB RAM
- Storage: 256 GB (thin provision)
- Operating System: CentOS 7
- Network Adapter 1: VLAN 1101
- Network Adapter 2: Trunk Port

## **Zingbox Inspector Installation**

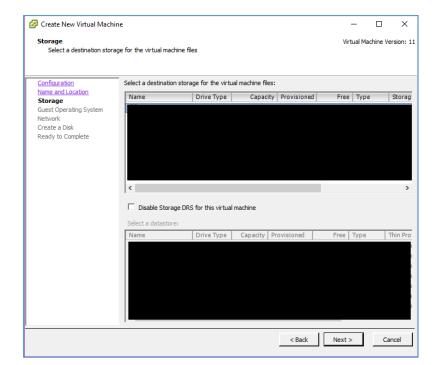
- 1. Create a new virtual machine, and under configuration, select Typical.
- 2. Click Next >.

Configuration Select the configuration for t	the virtual machine	Virtual M	lachine Ver	rsion:
Storage Guest Operating System Network Create a Disk Ready to Complete	Configuration  Create a new virtual machine with the most common devices and cor  C Custom Create a virtual machine with additional devices or specific configura		ions.	

- 3. Create a Name for the virtual machine and assign it an Inventory Location.
- 4. Click Next >.

Create New Virtual Mach	ne	-		>
Name and Location Specify a name and locat	on for this virtual machine	Virtual M	Virtual Machine Ver	
Configuration	Name:			
Name and Location Storage Guest Operating System	[Test] Zingbox Inspector  Virtual machine (VM) names may contain up to 80 characters and they mu vCenter Server VM folder.	ust be unique wit	hin each	
Network Create a Disk Ready to Complete	Inventory Location:			
	< Back	Next >	Can	ncel

- 5. Select a **destination storage** for the VM.
- 6. Click Next >.



7. Check Linux and set the version to CentOS 4/5/6/7 (64-bit).

### 8. Click Next >.

Tamica du Cocadori Storace Guest Operating System Network Create a biok Ready to Complete Vers Cer		achine Versio
Name and Location Gue Storage Guest Operating System C Network Create a Disk C Ready to Complete Vers Cere Identification (Cere Identif	© Windows ■ Linux © Other sion:	
	ntifying the guest operating system here allows the wizard to provide the appropriate operating system installation.	e defaults fo

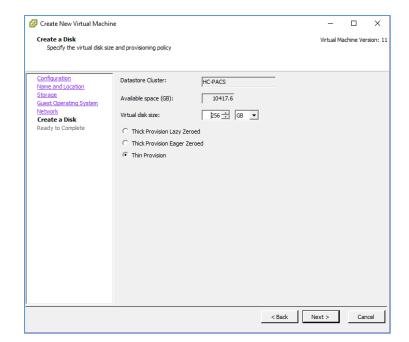
9. Connect **2 NICs** to the virtual machine and assign them to a **network.** 

### 10. Check Connect at Power On for both NICs.

#### 11. Click Next >.

🕝 Create New Virtual Machin	e	-		×
Network Which network connection:	will be used by the virtual machine?	Virtual I	Machine Ver	sion: 11
Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete	Create Network Connections How many NICs do you want to connect? 2 Network Adapter NIC 1: H-C-PACS-VLAN-1701 (CommonLabSwitch) VMXNET NIC 2: H-C-PACS-VLAN-1701 (CommonLabSwitch) VMXNET If supported by this virtual machine version, more than 4NICs can b virtual machine is created, via its Edit Settings dialog. Adapter choice can affect both networking performance and migration the VMware KnowledgeBase for more information on choosing among supported for various guest operating systems and hosts.	3 3 be added af	lity. Consul	Dn
1	< Back	Next >	Can	cel

- 12. Set a Virtual disk size and Provisioning method.
- 13. Click Next >.



14. Verify that virtual machine settings are correct.

### 15. Check Edit the virtual machine settings before completion.

#### 16. Click Continue.

Ready to Complete		Virtual Machine Ve
Click Finish to start a tas	k that will create the new virtual mac	hine
	_	
Configuration	Settings for the new virtual mad	hine:
<u>Name and Location</u> Storage	Name:	[Test] Zingbox Inspector
Guest Operating System		
Network		
Create a Disk		
Ready to Complete		
	Guest OS:	CentOS 4/5/6/7 (64-bit)
	NICs:	2
	NIC 1 Network:	HC-PACS-VLAN-1701 (CommonLabSwitch)
	NIC 1 Type:	VMXNET 3
	NIC 2 Network:	HC-PACS-VLAN-1701 (CommonLabSwitch)
	NIC 2 Type:	VMXNET 3
	Disk provisioning:	Thin Provision
	Virtual Disk Size:	256 GB
	Edit the virtual machine set	ings before completion
	Show all storage recommen	dations
		hine (VM) does not include automatic installation of the guest opera on the VM after creating the VM.

## 17. Set memory to 8 GB.

#### 18. Set CPUs to 4.

- 19. Under New CD/DVD (adding), set these parameters:
  - a. Check Connect at power on.
  - b. Select **Datastore ISO File**, then browse for the *ZingOS.iso* file in your data store.

## 20. Click Finish.

Add Remove Summary 8192 MB 4 Video card Deprecated [HC-PACS_L02_APM Client Device LS1 Logic Parallel HC-PACS-VLAN-1701 HC-PACS-VLAN-1701 Virtual Disk	Device Status     Connected     Connect at power on     Device Type     Clent Device     Note: To connect this device, you must power on th     virtual machine and then click the Connect CD/DVD     button in the toolbar.     Host Device     Datastore ISO File     [e/ZingBox/ZingOS-1.241-x86_64.iso     Browse     Mode						
	Passthrough IDE (recommended)     C Emulate IDE     Virtual Device Node     (IDE (1:0)     IDE (1:0)	▼ ish	Cancel				

- 21. Connect to the inspector console and follow the onscreen prompts to finish the configuration.
- 22. In a web browser, enter the **URL** of your Zingbox Cloud instance.
- 23. Enter your Zingbox Cloud credentials.
- 24. Click Login.
- 25. On the home page, navigate to **Administration > My Inspectors.**
- 26. Verify that the host name of the Zingbox Inspector set up previously is visible and connected (shown by the green cloud icon).

<u>ک</u>	٩	Give fee	dback
	My Inspectors		
	All Sites - Day - Zingbox Cloud Traffic 21.99 MB	Analyzed Traffic 125.69 MB	~ + ±
	(2)		1
	test-zingbox-inspector DEPLOYMENT IN PROGRESS		

# 2.7.5 Forescout CounterACT 8

Forescout CounterACT is a network access control tool that can perform device discovery and classification, risk assessment, and control automation through passive and active techniques. For this project, the intended use of Forescout is to manage device compliance and perform necessary remediation when devices fall out of compliance.

## System Requirements

- **CPUs:** 2
- Memory: 8 GB RAM
- Storage: 80 GB (thin provision)
- Operating System: Linux Kernel 3.10
- Network Adapter 1: VLAN 1201
- Network Adapter 2: Trunk Port

## Forescout Appliance Installation

- To begin installation, obtain the Forescout ISO file. Load the Forescout ISO file into the VM's compact disc/digital versatile disc (CD/DVD) drive. Make sure the CD/DVD drive is set to Connect at Power On.
- 2. Boot up the VM and begin the installation process.
- 3. Select Install CounterACT.
- 4. Press Enter to reboot.

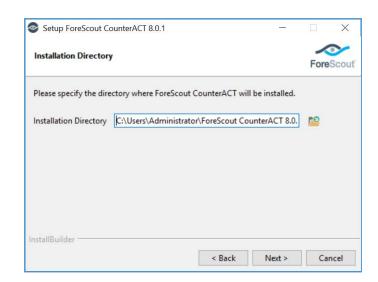
- This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-24
- 5. Select **option 1** to configure CounterACT.
- 6. Select **option 1** for standard installation.
- 7. Press enter to proceed.
- 8. Select **option 1** for CounterACT Appliance.
- 9. Select **option 1** for Per Appliance Licensing Mode.
- 10. Enter appliance description.
- 11. Give appliance a password.
- 12. Enter ForescoutCA and apply this as the appliance host name.
- 13. Assign the appliance IP address 192.168.120.160.
- 14. Assign appliance network mask 255.255.255.0.
- 15. Enter **192.168.120.1** as the appliance's gateway.
- 16. Enter domain name \*\*\*\*\*\*\*
- 17. Enter DNS server address 192.168.120.100.
- 18. Review configuration and run test.
- 19. Once the test passes, select done.

## Forescout CounterACT Console Installation

- 1. Run Install\_Management.exe.
- 2. Click Next >.



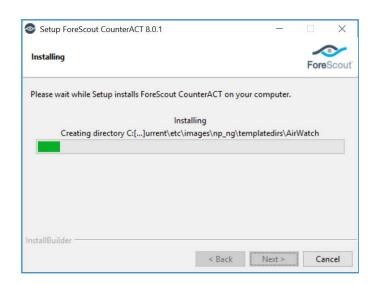
3. Verify Installation Directory as C:\Users\Administrator\ForeScout CounterACT 8.0.1; click Next >.



4. When the **Ready to Install** screen appears, click **Next** > to begin the installation process.

Setup ForeScout CounterACT 8.0.1			-		×
Ready to Install				Fore	Scout
Setup is now ready to begin installing ForeScout Count	terACT	on yo	ur com	outer.	
InstallBuilder Karakara Karaka	ack	N	lext >	Ca	ncel

5. An **Installing** screen will appear that provides a status bar indicating the degree of installation completion. Click the **Next** > button to allow the installation to proceed.



6. As the installation nears completion, a screen indicating **Completing the ForeScout 8.0.1 Setup Wizard** displays. Check **Create Desktop shortcut**; then click **Finish.** 

	Completing the ForeScout CounterACT 8.0.1 Setup Wizard					
ForeScout	Setup has finished installing ForeScout CounterACT 8.0.1 on your computer.					

- 7. Launch Forescout CounterACT Console, and enter the information that follows, then click Login:
  - a. Enter 192.168.120.160 in the IP/Name text box.
  - b. Select Password as the Login Method.
  - c. Enter Administrator in the User Name text box.
  - d. Enter the password in the **Password** box.



### **Forescout CounterACT Configuration**

To use the full function offered by the Forescout CounterACT, proper network configuration is required, which may include the monitor and response interface assignments at the data center, the network VLAN and segmentation information, the IP address range that the CounterACT appliance will protect, user directory account information, domain credentials, the core switch IP address, and vendor and Simple Network Management Protocol parameters.

After completing the installation, log in to the CounterACT Console by using the steps below:

1. Select **the CounterACT** icon from the server on which you installed the **CounterACT Console.** A logon page displays, as depicted below.



- 2. Provide the following information, and select **Login** to open the console:
  - a. Enter the IP address 192.168.120.160 in the IP/Name field.
  - b. In the User Name field, enter admin.
  - c. In the **Password** field, enter the admin password, which is defined during the installation.

ForeScout	^	Home	Asset Inv	entory	1	Policy			۲
« Views	All Hosts		Search		Q	OnlineiOffline	~	13 OF 1	3 HOST
Search Q	Host +	IPv4 Address	MAC Address	Display N	ame .	Function	Actions		
All Hosts (13)	<ul> <li>blueflow pacs hciab</li> </ul>	192 168 120 205				Computer	10		
Policies	PACSHYLAND-VNA	192,168,130,120		Hyland Ser	vice i Iter	Computer	10		
til History	PACSIHYLAND-PGCOR			Hyland Ser		Computer	18		
	PACSIHYLAND-NILREA			Hyland Ser		Computer	38		
	* PACSIAD	192.168.120.100	005656b2acd8	citiana adi	nice Osei	Computer	18		
	Profile Compliance	All Policies							
Filters		v4 Address: 19216 perating System: ( endor and Model:	Jinknown Unknown	known					* (
Filters Search Q		v4 Address: 192.16 perating System: ( endor and Model:	Inknown	known					* (
		v4 Address: 192.16 perating System: ( endor and Model:	Inknown Unknown ation: Unclassified	known	19216814				* (

The console manager can be used to view, track, and analyze network activities detected by the appliance. It can also be used to define the threat protection, firewall, and other polices.

The figure below shows the sample asset inventory page. (Further network configuration will be needed for complete inventory information.)

Ella Baparta Actiona Toola Log Displ	ay Esta				
🛷 ForeScout	🏫 Home	Asset Inventory	Policy		
Views					
Search Q					
같은 Classification					
Classification (Advanced)					
Sec. 19					
La Guest Registration					
Te User Directory					
CD Open Ports					
📲 Windows					
Filters					
Search Q					
⊳ All					
Segmenta (13)					
Organizational Units					
E Detault Groups					
🛛 🔚 Groups					
				10 12 14 18 8/8/19	

The figure below shows the sample **Policy Manager** page. Further network configuration and policy definition will be needed for complete policy information.

	out				a	Asset Inventor		Policy		٢
	out		n	Home		Asset Inventor	ά.	Policy		G
Policy Folders	Policy Man	nager			Search		Q 🗹 Sho	w subfolder policies		
+201800	Name	Category	St.	User Scope	Segments	Groups	Exceptions	Conditions	Actions	Add
Policy	🗠 Asset Classif	icaClassification		Complete	192.168.0.0/16			No Conditions		Edit
	NAT Devic	es Classifier						Device is NAT:	10	Categoriz
	Mobile De	vicClassifier						Network Functi	1	Remove
	Windows	Classifier						Network Functi	28	Duplicate
	Printera	Classifier						Network Functi	201	Move to
	Linux/Unb	Classifier						Network Functi		Export
	Macintosh	Classifier						Network Functi.		Start
	VolP Devi	cesClassifier						Network FunctL.	20	Stop
		lev Classifier						Network Functi		Custom
	Unclassifie	ed Classifier						No Conditions	18	
										Compariso Help
										Apply

# 2.7.6 Symantec Endpoint Detection and Response (EDR)

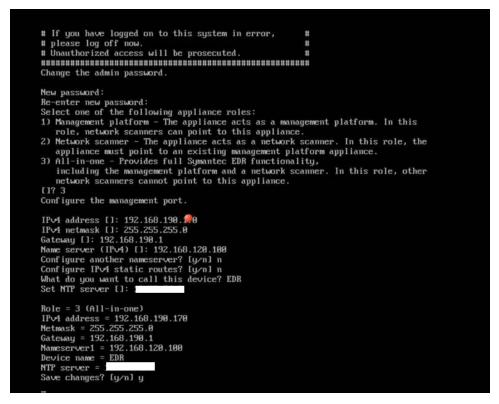
Symantec Endpoint Detection and Response performs behavioral analytics on endpoint events from Symantec Endpoint Protection to identify potentially malicious behavior. It can sandbox impacted endpoints, prioritize risks, and provide tailored remediation guides.

### System Requirements

- CPUs: 12
- Memory: 5 GB RAM
- Storage: 500 GB (thin provision)
- Operating System: CentOS 7
- Network Adapter 1: VLAN 1901
- Network Adapter 2: SPAN\_PACS

### **Symantec EDR Installation**

- 1. Launch the virtual appliance after deployment of the vendor-provided *SEDR-4.0.0-483-VE.ova* file.
- 2. Enter default username **admin** and default password. You will be required to change the default password by entering a new password.
- 3. After changing the default password, the bootstrap will automatically launch. Enter the following options during the bootstrap:
  - IPv4 address []: 192.168.190.17
  - IPv4 netmask []: 255.255.255.0
  - Gateway []: 192.168.190.1
  - Name server (IPv4) []: 192.168.120.100
  - Configure another nameserver? [y/n]: n
  - Configure IPv4 static routes? [y/n]: n
  - What do you want to call this device?: EDR
  - Set NTP server []: X.X.X.X
- 4. After verifying the correct details, enter Y to save changes. The appliance will restart.



- 5. Open a web browser, and travel to the virtual appliance at https://192.168.190.170. Enter the username setup and password \*\*\*\*\*.
- 6. Follow the prompts to create the initial admin account.

•	• •	•
Create an Admini	strator Account	
Login	admin	
Password	- Advertised of	
	Password Strength: Moderate	
Confirm Password	Tenterset	
Display Name	Doptay Ranse	
User Email	User Email	
Receive email	notification when incidents occur	
Prez	Firest	
		-

- 7. Select the **Settings** menu, and then select the **Global** submenu.
- 8. Ensure Enable Symantec Endpoint Protection Correlation is checked.
- 9. Select Add SEPM Database.

$\equiv$	O Symantec EDR					Symantec EDR is Healthy $\oslash$	Admin 🗸
へ 図 録	synapse	Enable Roam Enable Syma Enable Syma Symantec Endpoi	intec Email Security cloud Correl ling Correlation intec Endpoint Cloud Correlation intec Endpoint Protection Correl nt Protection Manager (SEPM	) ation ) Databases			
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Name  Add part PM  Download Synapse	IP Address Database Log Collector for SEPM Embed	Port No data e Ided DB	Enabled	Status	
0	Endpoint Communication Channel, SEP Policies, and Endpoint Activity Recorder	SEPM Controller no	ot configured 2.0 (requires at least 1TB of hard		Configure SEPM Controller		

10. Provide the information that follows, and click Save:

- DB Type: Embedded DB
- Entry Name: SEPM
- Address: 192.168.190.172
- Port: 8081
- **Connection Password:** Enter your connection password.
- Enabled: checked

=	💮 Symantec EDR				
Q.	< Global *	Add SEPM 🍥			×
	< Giobai -	DB Туре	Embedded DB	~	
	Cynic Sandboxing	Entry Name	SEPM		
~% ~%		IP Address	192.168.190.172		
1	Data Handling	Port	8081		
Ø		Connection Password			
$\overline{\Box}$		Enabled	$\checkmark$		
⊚	🛸 Synapse				
				Cancel Save	

- 11. After completing the integration with SEPM, select the **Settings** menu, then select the **Appliances** submenu.
- 12. Select Edit Default Appliance.
- 13. Select **Add Internal Network** to create and add a **Subnet**, **Netmask**, and **Description** for each internal network listed below. Make sure to save after entering the network details.

<   Default Appl	iance •			
Internal Network	Subnet	Netmask	Description	
Configuration	192.168.100.0	255.255.255.0	VLAN 1101 Internal Network	1
	192.168.120.0	255.255.255.0	VLAN 1201 Enterprise Network	1
	192.168.130.0	255.255.255.0	VLAN 1301 Clinical Workstations	E.
	192.168.140.0	255.255.255.0	VLAN 1401 PACS 1	E
	192,168,141.0	255,255,255,0	VLAN 1402 PACS 2	1
		SEE ALL 6		

- Subnet: 192.168.100.0 Netmask: 255.255.255.0 Description: VLAN 1101
- Subnet: 192.168.120.0 Netmask: 255.255.255.0 Description: VLAN 1201
- Subnet: 192.168.130.0 Netmask: 255.255.255.0 Description: VLAN 1301
- Subnet: 192.168.140.0 Netmask: 255.255.255.0 Description: VLAN 1401
- Subnet: 192.168.141.0 Netmask: 255.255.255.0 Description: VLAN1402
- Subnet: 192.168.150.0 Netmask: 255.255.255.0 Description: VLAN 1501
- Subnet: 192.168.160.0 Netmask: 255.255.255.0 Description: VLAN 1601
- Subnet: 192.168.180.0 Netmask: 255.255.255.0 Description: VLAN 1801
- Subnet: 192.168.190.0 Netmask: 255.255.255.0 Description: VLAN 1901

Subnet	Netmask	Description	
92.168.100.0	255.255.255.0	VLAN 1101 Internal Network	:
92.168.120.0	255.255.255.0	VLAN 1201 Enterprise Network	1
92.168.130.0	255.255.255.0	VLAN 1301 Clinical Workstations	1
92.168.140.0	255.255.255.0	VLAN 1401 PACS 1	:
92.168.141.0	255.255.255.0	VLAN 1402 PACS 2	:
92.168.150.0	255.255.255.0	VLAN 1501 Radiology Departments	:
192 168 160 0	255 255 255 0	VLAN 1601 Clinical Application Services	:

14. Select Settings and then Global.

15. Uncheck Enable ECC 2.0 under Endpoint Communication Channel, SEP Policies, and Endpoint Activity Recorder.

≡	📀 Symantec EDR				Symantec EDR is Healthy 🧭	Admin 🗸
م III		Enable Symantec Endpoint C	rotection Correlation			
000 COL		Symantec Endpoint Protection Ma Name Address		Enabled	Status	
ŝ			No data	available.		
1		(+) Add SEPM Database				
Ì		Download Synapse Log Collector fo	r SEPM Embodded DB			
۵ ه	Endpoint Communication Channel, SEP Policies, and Endpoint Activity Recorder	SEPM Controller not configured	east 1TB of hard disk space) 🔒	Configure SEPM Controller		
	Automatic Submission	Submit suspicious files to same	dbox for analysis			
	Backup	Backup is disabled	Configure Backup			
		Ireand Ru	Izzuari To E	unis ation Date	Contilexto Statue	

16. Select Settings and then Appliances.

≡	🚱 Symantec EDR					Symantec EDR is Healthy	) Admin 🗸
Q	< Default Appli	ance 💿					
	$\square$	General Settings					
<u>&amp;</u>		avelou.	Tonic barrenes				
1	$\bigcirc$	Internal Network 192.168.100.0	Configuration 255.255.255.0 NETTINA DE		VLAN 1101 I	Internal Network	
		DNS Settings					
8		PETIMANTY .	RECONDAILY				
٢					li ili	Edit Dutasti Appliance 🛛 😰	
	Appliances						
	Name M	ignit iP Role	Mode	Scanning	Status		
	EDR 1	92.168.190.170 Management/Sci	nner/Proxy Tap	Disabled	Healthy	o o	

- 17. Select **EDR** from the appliances list.
- 18. Turn on Scanning under the Network Interface Settings.

#### Symantec EDR and SEP Correlation

- 1. Open a web browser and navigate to the virtual appliance at https://192.168.190.170. Log in with your administrator account.
- 2. From the settings menu, select global settings.
- 3. Select Download Synapse Log Collector for SEPM Embedded DB.
- 4. After the SEPMLogCollector.msi finishes downloading, move to the SEP Manager (SEPM).
- 5. Launch the SEPMLogCollector.msi file from SEPM.
- 6. Continue through the setup wizard prompts by clicking **Next** to use the default settings.
- 7. After installation is complete, launch the **Log Collection** for **SEPM** embedded DB configuration utility, and enter the values below:
  - Service Hostname (optional): Leave blank.
  - Service IP address: 192.168.190.172
  - Service port: 8082
  - Log Collector connection password: Enter connection password.
  - Confirm connection password: Enter connection password again.
  - **SEPM embedded database configuration password:** Enter the embedded DB password.
- 8. After entering values into the configuration utility, click Confirm.

Service Hostname (optional):	
Service IP address:	192.168.190.172 ~
Service port:	8081
Log Collector connection password:	•••••
Confirm connection password:	•••••
EPM embedded database configuration —	
Password:	•••••
	Test Database Connection

# 2.8 Endpoint Protection and Security

Endpoint protection and security measures are deployed to workstation end points to further emphasize defense in depth. The build includes an agent-based endpoint protection solution that is centrally managed within the enterprise. Endpoint protection provides anti-malware features with centralized servers assuring that managed assets receive regular updates.

## 2.8.1 Symantec Data Center Security: Server Advanced (DCS:SA)

Symantec DCS:SA utilizes a software agent to provide various server protections, including application allow-listing, intrusion prevention, and file integrity monitoring. For this project, a DCS:SA agent was installed on both PACS servers in our architecture.

### System Requirements

- CPUs: 4
- Memory: 8 GB RAM
- Storage: 120 GB (thin provision)
- Operating System: Microsoft Windows Server 2016 Datacenter
- Network Adapter: VLAN 1901

### Symantec Data Center Security Installation

- 1. Launch server.exe.
- 2. Click Next >.

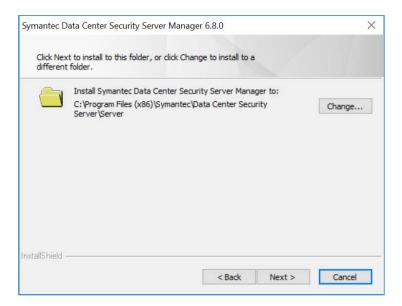
	Welcome to the InstallShield Wizard for Symantec Data Center Security Server Manager 6.8.0
	The InstallShield® Wizard will install Symantec Data Center Security Server Manager 6.8.0 on your computer. To continue, dick Next.
	WARNING: This program is protected by copyright law and international treaties.
	This Symantec product may contain open source and other third party materials that are subject to a separate license. Please see the applicable Third Party Notices file provided with the Symantec product.
Symantec.	For the specific Symantec product licensing please see documentation provided at https://www.symantec.com/about/profile/policies/eulas/.

- 3. Check I accept the terms of the license agreement.
- 4. Click Next >.

Please read the following	license agreement carefully.
SYMANTEC TEMPO	RARY TRIALWARE SOFTWARE EVALUATION LICENSE AGREEMENT
WILLING TO LICENS INDIVIDUAL, THE CO UTILIZING THE TRIAI OR "YOUR") ONLY O TERMS OF THIS TEM	ATION AND/OR ITS AFFILIATES ("SYMANTEC") IS E THE TRIALWARE SOFTWARE TO YOU AS THE MPANY, OR THE LEGAL ENTITY THAT WILL BE WARE SOFTWARE (REFERENCED BELOW AS "YOU" N THE CONDITION THAT YOU ACCEPT ALL OF THE PORARY TRIALWARE SOFTARE EVALUATION IT ("TRIALWARE AGREEMENT"). READ THE TERMS F THIS TRIALWARE AGREEMENT CAREFULLY
	THIS TRIALWARE AGREEMENT CAREFOLLT
AND CONDITIONS O	the Barrows and the State of th

5. Verify installation location.

#### 6. Click Next >.



- 7. Review settings.
- 8. Click Install >.

Symantec Data Center Sec	urity Server Manager 6.8.0	X
Ready to Install the Pr The wizard is ready to be	The second s	
Review the settings an Cancel to exit the wiza	d dick on 'Install'. If you want to change any settings, rd.	click Back. Click
Installation Type: Server Settings:	Evaluation (Install Local Database)	
	Files (x86)\Symantec\Data Center Security Server\Se	rver
InstallShield		
	< Back Install >	Cancel

9. Wait for the setup and installation process to complete.

mantec Data Center Security S	erver Manager 6.8.0	>
Setup Status		
Symantec Data Center Security installation.	y Server Manager is configuring your new software	
Installing		
C:\\{65A60777-4A68-4691-/	AB60-FC5621BAFD35}\manager.exe	
stallShield		

## 10. SQL Server will be installed automatically during the setup process.

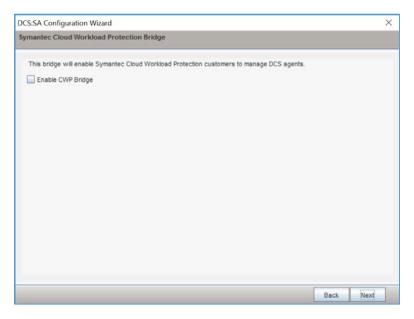
Install Setup Files						
	SQL Server Setup files are being installed on the system.					
	Task	Status				
	Install Setup files	In Progress				

- 11. Provide the information below, and click Next:
  - Agent port: 443

- Bridge port: 2443
- Console port: 4443
- Web server administration port: 8081
- Web server shutdown port: 8006

gs				
		ector Attributes -		
	vveb server	vveb server administration port	8081	
	Web server	shutdown port	8006	
4443				
	443 2443 4443	2443 Web server	2443 Web server shutdown port	2443 Web server shutdown port 8006

12. Uncheck Enable CWP Bridge and click Next.



13. Verify settings for FQDN Hostname as WIN-RUQDO7KL8A7, Static IP Address as 192.168.120.207, and Java Heap Size as 6144, then click Next.

CS:SA Configuratio	on Wizard	
erver Settings		
Certificates		
Agent Certifica	ste	
🖌 Server Certific	cate	
This Server's Ne	twork Address Settings	
	Use FQDN Hostname for Certificate	
FQDN Hostname Static IP Address	WIN-RUQD07KL8A7	
	192.168.120.207	
JVM Settings —		
Java Heap Size	(MB) 6144	

14. Create a **password** for the DB connection.

### 15. Click Next.

Create Database		
Connection Parameter	3	
Hostname	127.0.0.1	
Database Instance O Database Port		
'sa' privileged User		
Password ★	•••••	
Confirm Password ★	•••••	

- 16. Verify Unified Management Console connection settings.
- 17. Create a password for the **Unified Management Console** connection.

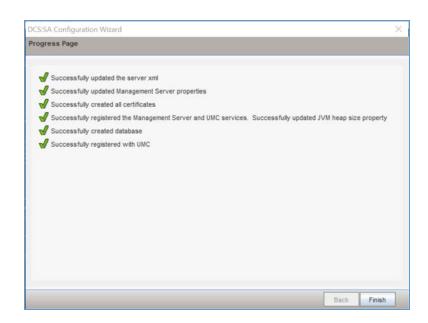
#### 18. Click Next.

CS:SA Configuration Wiza	rd	×
egister with Unified Man	agement Console	
UMC Details		
Hostname	192.168.120.207	
Port	8443	
User Name	dcsadmin	
Password ★	•••••	
Confirm Password ★	•••••	

19. Verify the configuration settings and click Next.

CS:SA Configuration Wizard	2
ummary Page	
Review the settings and click on 'Configure'. If you want to change any s wizard	ettings, click Back. Click Cancel to exit the
Installation Type: Evaluation (Install Local Database)	
Server Settings	
Directory: C:\Program Files (x86)\Symantec\Data Center Security Serve Ports: Agent: 443, Console: 4443, Web Admin: 8081, Web Shutdown: I	
Database Settings	=
Host: 127.0.0.1 Instance: SCSP	
Database Name: SCSPDB	
JVM Settings	
Heap Size (MB): 6144	
UMC Registration Settings	
UMC Server: Hostname=192.168.120.207, Port=8443, Username=dcsa	
Product Server: Hostname=WIN-RUQDO7KL8A7, IP Address=192.168.	
Server Cert Attributes: extl SAN=DNS:WIN_RUODO7KL8A7 IP:192.168	
	•

- 20. Wait for the configuration process to complete.
- 21. Click Finish.



# 22. Wait for the installation to complete and click **OK**.

ymantec Data Center Security Server Manager 6.8.0	×
Setup Status	
Symantec Data Center Security Server Manager is configuring your new so installation.	ftware
Symantec Data Center Security Server Manager 6.8.0	×
Finis	
The DCS Management Server was configured succe	ssfully.
	ОК
stallShield	
	Cancel

## Symantec Datacenter Security Windows Agent Install

- 1. Run agent.exe.
- 2. Click Next >.



- 3. Check I accept the terms in the license agreement.
- 4. Click Next >.

License Agreement		
Please read the following license agree	ement carefully.	
SYMANTEC SOFTWA	RE END USER LICENSE AGREEMENT	^
SYMANTEC CORPORATION (IF YO	DU ARE LOCATED IN THE AMERICAS OR	
	TED (IF YOU ARE LOCATED IN ANY OTHER	
	LING TO LICENSE THE SOFTWARE TO YOU	
AS THE INDIVIDUAL, THE COMPA	NY OR THE EGALENTTY THAT WILL BE	
LIGINIC THE COPTUADE (DEPENDEN		
	D TO AS "YOU" OR "YOUR") ONLY ON THE	
CONDITION THAT YOU ACCEPT A		
CONDITION THAT YOU ACCEPT A THIS SYMANTEC SOFTWARE LICE	D TO AS "YOU" OR "YOUR") ONLY ON THE ALL OF THE TERMS AND CONDITIONS OF	
CONDITION THAT YOU ACCEPT A THIS SYMANTEC SOFTWARE LICE RIGHTS SUPPLEMENT (AS DEFINE	D TO AS "YOU" OR "YOUR") ONLY ON THE ALL OF THE TERMS AND CONDITIONS OF ENSE AGREEMENT AND THE PRODUCT USE	
CONDITION THAT YOU ACCEPT A THIS SYMANTEC SOFTWARE LICE RIGHTS SUPPLEMENT (AS DEFINE	D TO AS "YOU" OR "YOUR") ONLY ON THE ALL OF THE TERMS AND CONDITIONS OF ENSE AGREEMENT AND THE PRODUCT USE ED BELOW) (COLLECTIVELY, THE "LICENSE SE AGREEMENT CAREFULLY BEFORE	
CONDITION THAT YOU ACCEPT A THIS SYMANTEC SOFTWARE LICE RIGHTS SUPPLEMENT (AS DEFINE AGREEMENT"). READ THE LICENS	D TO AS "YOU" OR "YOUR") ONLY ON THE ALL OF THE TERMS AND CONDITIONS OF ENSE AGREEMENT AND THE PRODUCT USE ED BELOW) (COLLECTIVELY, THE "LICENSE SE AGREEMENT CAREFULLY BEFORE Ment Print	
CONDITION THAT YOU ACCEPT A THIS SYMANTEC SOFTWARE LICE RIGHTS SUPPLEMENT (AS DEFINE AGREEMENT"). READ THE LICENS	D TO AS "YOU" OR "YOUR") ONLY ON THE ALL OF THE TERMS AND CONDITIONS OF ENSE AGREEMENT AND THE PRODUCT USE ED BELOW) (COLLECTIVELY, THE "LICENSE SE AGREEMENT CAREFULLY BEFORE Ment Print	

- 5. Verify the installation and log files directories.
- 6. Click Next >.



- 7. Provide the information below, and click Next >:
  - Agent Name: WIN-RUQD07KL8A
  - Polling Interval (sec): 300
  - Check Enable Intrusion Prevention.
  - Notification Port: 2222
  - Agent Protocol: HTTPS

🛃 Data Center Security Server		×
Agent Configuration Please configure your agent's setting	s	
Agent Name:	WIN-RUQDO7KL8A7	
Polling Interval (sec):	300	
Enable Intrusion Prevention:		
Enable Real-time notification if	this agent requires immediate updates.	
Enable Real-time Notification:	Notification Port: 2222	
Agent Protocol:	HTTPS ~	
InstallShield		
	< Back Next >	Cancel

- 8. Provide the information below, and click Next:
  - Primary Management Server: 192.168.120.207
  - Agent Port: 443
  - Alternate Management Servers:
  - Management Server Certificate: C:\User\Administrator\Desktop\agent-cert.ssh

Please configure your agent's Manag	ement Server settings	
Primary Management Server:	192.168.120.207	_
Agent Port:	443	
If desired, specify Alternate Ma	nagement Servers in a comma-separated list:	
Alternate Management Server(	s):	
	ement Server Certificate is required in order to specified Management Servers must use the s	
to the Management Server. All	specified Management Servers must use the s	

- 9. Specify a **Server Security Group** created through Symantec Datacenter Security Server or leave it blank to use the default security group.
- 10. Click Next >.

Server Security Group		
Please enter the Server S	Security Group name	
the agent to join. If you	f an existing Security Group in the man leave the field blank, the agent will joi e agent to another Security Group at a	n the Default Security
[		
allShield		

11. Verify installation and configuration settings and click Install.

Ready to Install		
	gs are summarized below. If you want to review or change any of click Back. Click Install to start the installation using these settings.	the
Installation Directories		~
Installation Directory: \Agent\	C:\Program Files (x86)\Symantec\Data Center Security Server	
Log Files Directory: \Agent\	C:\Program Files (x86)\Symantec\Data Center Security Server	
Agent Configuration		
Agent Name:	WIN-RUQDO7KL8A7	
Agent Polling Interval:	300	
Enable IPS Feature:	enabled	
Agent Notifications:	enabled	
Notifications Port:	2222	
Agent Protocol:	https	
Management Server Co	nfiguration	
Primary Management Se Alternate Management		
Management Server Por		~
stallShield		

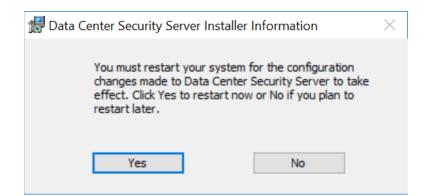
12. Wait for the installation process to complete.

Installing	) Data Center Secu	rity Server					
The pro	gram features you sele	ected are being	installed.				
13	Please wait while th Server. This may ta			Data Cente	r <mark>Secur</mark> it	у	
	Status:						

# 13. Click Finish.

	InstallShield Wizard Completed
	The InstallShield Wizard has successfully installed Data Center Security Server. Click Finish to exit the wizard.
Symantec.	

14. Click **Yes** to restart the agent machine.



# 2.8.2 Symantec Endpoint Protection

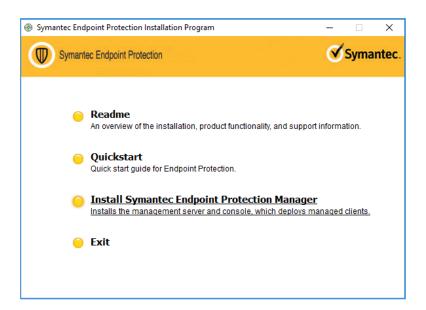
Symantec Endpoint Protection is an agent-based security solution that provides anti-virus, intrusion prevention, application allow-listing, and other capabilities. For this project, Symantec SEP protects endpoints from malicious software and integrates with Symantec Endpoint Detection and Response to detect suspicious behavior.

## System Requirements

- **CPUs:** 4
- Memory: 8GB RAM
- Storage: 240 GB (thin provision)
- Operating System: Microsoft Windows Server 2016
- Network Adapter: VLAN 1901

## Symantec Endpoint Protection Manager Installation

- 1. Launch Symantec\_Endpoint\_Protection\_14.2.0.MP1\_Part1\_Trialware\_EN.exe file.
- 2. Select the Install Symantec Protection Endpoint Manager option.



3. Proceed through the installation wizard by clicking Next >.

🛃 Symantec Endpoint Protect	ion Manager X
	Symantec Endpoint Protection Manager
	The Installation Wizard will perform the following steps:
	<ul> <li>Install the management server and console</li> </ul>
	Configure the management server
	Create the database
	Click Next to begin.
Symantec.	WARNING: This program is protected by copyright law and international treaties.
	< Back Next > Cancel

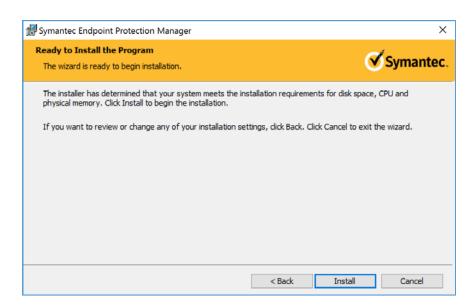
- 4. Check I accept the terms in the license agreement.
- 5. Click Next >.

License Agreement Please read the following license agreement carefully.	<b>Symante</b>
SYMANTEC SOFTWARE LICENSE AGREEMENT	^
SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") SP ENTITLEMENT CONFIRMATION IS WILLING TO LICENSE THE LICENSED SOFT THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL B	TWARE TO YOU AS
LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR", CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF SOFTWARE LICENSE AGREEMENT AND THE PRODUCT USE RIGHTS & DEFINED BELOW) (COLLECTIVELY, THE "LICENSE AGREEMENT"). REA AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY DOWNLOAD	THIS SYMANTEC SUPPLEMENT (AS D THE LICENSE S IS A LEGAL AND
CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF SOFTWARE LICENSE AGREEMENT AND THE PRODUCT USE RIGHTS S DEFINED BELOW) (COLLECTIVELY, THE "LICENSE AGREEMENT"). REA AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS	THIS SYMANTEC SUPPLEMENT (AS D THE LICENSE S IS A LEGAL AND

 Select the location you want to install Symantec Endpoint Protection Manager and click Next >. Keep the default location of C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\.

🔛 Symante	c Endpoint Protection Manager		×
	ion Folder xt to install to this folder, or click Browse to inst	all to a different folder.	Symantec.
<u></u>	Install Symantec Endpoint Protection Manage C:\Program Files (x86)\Symantec\Symantec E Free disk space on C:\drive (system drive): CPU(s): 4 Physical Memory: 8.00 GB	Indpoint Protection Manager\	Browse
	Recommended Installation Requirements: CPU(s): Physical Memory: Free disk space for system drive (C: \):	4 8 GB 40 GB	
		< Back Ne	xt > Cancel

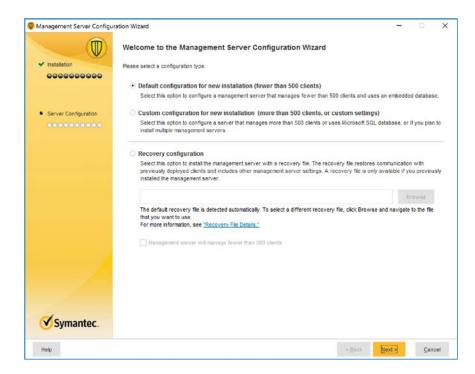
# 7. Select Install.



8. After installation is complete, click **Next >** to continue with configuration of the management server.

👷 Symantec Endpoint Protect	🛃 Symantec Endpoint Protection Manager		
	Management Server and Console Installation Summary The Installation Wizard has successfully installed Symantec Endpoint Protection		
	Manager. Click Next to begin the configuration wizard.		
	Configure the management server     Create the database		
Symantec.	Click Next to configure the management server.		
- Symantee.	< Back Next > Cancel		

9. Select Default configuration for new installation ...; then click Next >.



10. Provide the following information and click Next >.

- Company Name: \*\*\*\*\*\*\*
- User name: \*\*\*\*\*\*\*
- Password: \*\*\*\*\*\*\*
- Confirm password: \*\*\*\*\*\*\*
- Email address: \*\*\*\*\*\*\*

	ration Wizard					
	Create a system administrator account.	The password will be required to log on to the	e management console.			
✓ Installation	Company name:	NCCoE				
0000000000	User name:	admin				
	Password:*					
	Confirm password.*	•••••				
Server Configuration		Password Strength: Good				
	The password selected here is use password after installation, the data	d for both the administrator password and the base password will not change.	database password. If you change the admi			
	Email address.*	admin@nccce.labs				
	The server sends notifications and p	password recovery information to this address	k.			
	✓ Use a specified email server					
		ese settings to communicate with your email a ese settings by editing the server properties fr e: symantec-manager				
	Sender email address:	admin@pacs.hclab				
	User name:	admin				
	Password:	•••••				
	Require the specified serve	r to use a secure connection				
	O Use TLS	O Use SSL				
1	Send Test Email	Did you receive the test email?	O Yes O No			
Symantec.						

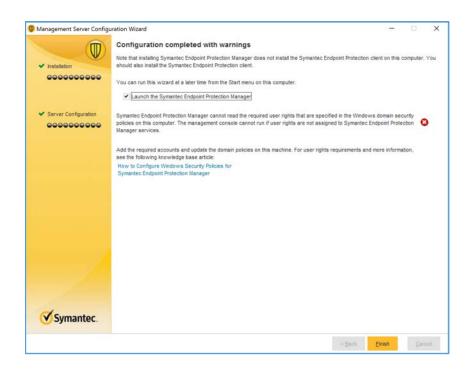
# 11. Confirm that Run LiveUpdate during installation is checked; click Next >.

Management Server Configu	ration Wizard		100		
	Run LiveUpdate				
<ul> <li>Installation</li> <li>OOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOO</li></ul>	Symantec recommends that you run LiveUpdate during installation. LiveUpdate n few hours to complete, depending on your server configuration and network ba		uter resources a	and might	take
	Run LiveUpdate during installation				
Server Configuration					
000000000	Partner Information (Optional) If a partner manages your licenses, you should specify the contact information of your licenses. Specify partner information	here. Partners receive	updates about t	he status	
	Partner email address:				
	Customer ID:				
	Partner Website:				
Symantec.					

12. Uncheck Send anonymous data to Symantec to receive enhanced threat protection intelligence and click Next >.

	Server Data Collection	
✓ Installation	Send anonymous data to Symantec to receive enhanced threat protection intelligence	
0000000000	This data provides the following benefits:	
	<ul> <li>Improved detection of targeted attacks on your endpoints</li> <li>Optimized product performance</li> </ul>	
Server Configuration	After Symantec Endpoint Protection Manager is enrolled in the cloud portal, this setting is automatically turned on.	
Server configuration	Learn more about data collection	
	View privacy statement	
	Click Back to change the installation settings, or click Next to begin the datat	pase cre
Symantec.		

13. After installation is completed, check Launch the Symantec Endpoint Protection Manager to configure your hosts; click Finish.

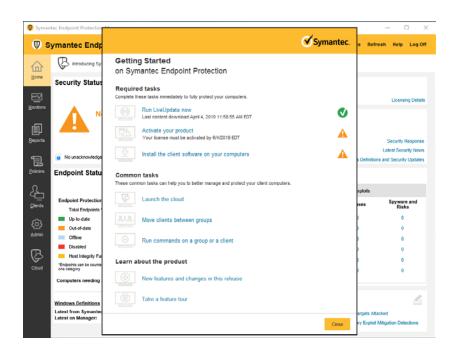


Symantec Endpoint Protection Host Windows Installation

1. Launch the **Symantec Endpoint Protection Manager**, and log in as the **admin**.

	Symantec Endpoint Pro	otection I	Manager
User name:	admin		
Password:	••••••		
Server:	symantec-manage	ement:8443	~
	Forgot your passy	vord?	
	Log On	Exit	Options >>

2. Select Install the client software on your computers from the Getting Started screen.



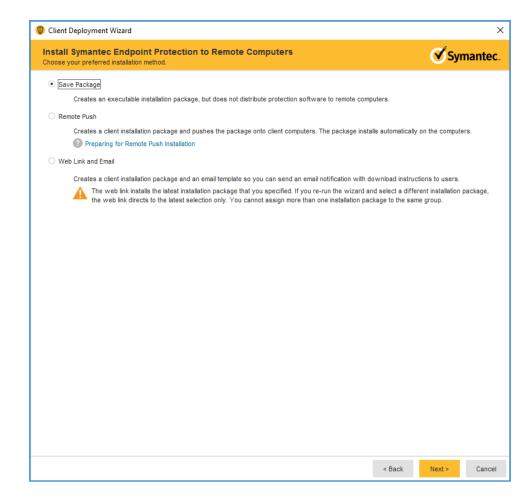
3. Confirm that New Package Deployment is checked and click Next >.

🦁 Client Deployment Wizard	×
Select Deployment Type	Symantec.
Welcome to the Client Deployment Wizard	
Use this wizard to install the protection client on computers in your network or update existing client communication settings.	
Note: For instructions to install the client on a computer that runs Symantec Mail Security or Symantec Scan Engine, see the Syma knowledge base article:	antec Technical Support
② Click here	
New Package Deployment	
Select packages from the server and specify client group and features.	
C Existing Package Deployment	
Choose from previously exported packages that are located on your hard drive.	
Browse	
Communication Update Package Deployment	
Create a package that changes the communication settings on an existing Symantec Endpoint Protection client installati restore communication between the client and Symantec Endpoint Protection Manager, to connect the client to a new S Protection Manager, or to convert an unmanaged client to a managed client.	
🔿 Create a package for Symantec Endpoint Protection clients that run on Windows. 🖉	
○ Create a package for Symantec Endpoint Protection clients that run on Mac. 🕷	
< Back	Next > Cancel

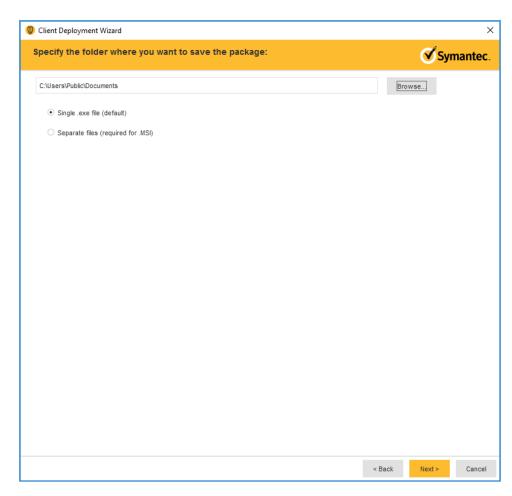
 Confirm the settings for the Install Packages: Windows—Symantec Endpoint Protection version 14.2.1023.0100—English, Group: My Company, Install Feature Sets: Full Protection for Clients, Install Settings: Default Standard client installation settings for Windows. Click Next >.

Select Group a	nd Install Feature Sets	Symante
Install Packages:	Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English	V
	This selection includes: WIN64BIT: Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English (4/4/19) WIN32BIT: Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English (4/4/19)	
Group:	My Company	Browse
Install Feature Sets:	Full Protection for Clients Recommended for laptops and desktops - Includes all protection technologies. Some security features are not supported on some platforms. Please refer to product documentation for details.	V
Install Settings:	Default Standard client installation settings for Windows	Options
Content Options:	Include virus definitions in the client installation package. Uncheck this option to create a smaller client installation package that does not include virus definitions but doe other content. After the client is installed, run LiveUpdate immediately on the clients to download the virus definitions of the virus definitions.	

5. Confirm that Save Package is selected and click Next >.



6. Specify the location to save the installation files and click Next >.



7. Confirm the details of the custom installation files and click Next >.

Ready to save package	🗹 Syn	aanta
	<b>v</b> Syn	nante
New computers will join the group "My Company", and will have the following client features in	stalled:	
Core Files		
<ul> <li>Virus And Spyware Protection</li> </ul>		
Download Protection		
<ul> <li>Microsoft Outlook Scanner</li> </ul>		
Lotus Notes Scanner		
POP3/SMTP Scanner		
<ul> <li>Proactive Threat Protection</li> </ul>		
<ul> <li>SONAR Protection</li> </ul>		
<ul> <li>Application and Device Control</li> </ul>		
<ul> <li>Network and Host Exploit Mitigation</li> </ul>		
Intrusion Prevention		
Firewall		
<ul> <li>Application Hardening</li> </ul>		
A single self-extracting SETUP.EXE file will be created in: C:\Users\Public\Documents		
Click Next to create the installation file SETUP.EXE.		

- 8. Move the installation package to the operating system where you want to install Symantec Endpoint Protection.
- 9. Launch the executable file and follow the prompts to install Symantec Endpoint Protection.

# 2.9 Data Security

A cloud storage solution, Microsoft Azure, was used to provide data security safeguards for medical images. The Azure solution provides data-at-rest encryption and, through a combination of access control and encryption, provides data security assurance.

The NCCoE lab used several different solutions to address data-in-transit encryption. As described in <u>Section 2.6.2</u>, DigiCert PKI, the lab implemented SSL/TLS encryption using DigiCert-issued certificates. Communications between modalities and clinical systems are secured using HIP, as described in <u>Section 2.7.3</u>, Tempered Networks Identity Defined Networking (IDN).

# 2.9.1 Microsoft Azure Cloud Storage

Microsoft Azure is a cloud service provider that provides storage and encryption for unstructured data in a remote location separate from the HDO environment. This project used an Azure blob storage account as a remote archive for medical images managed by the VNA. For more information on configuring Azure Storage accounts, including recommended security practices, visit *Microsoft's Azure Blob Storage Documentation* [13].

## **Microsoft Azure Blob Storage Creation**

To proceed with the following steps, a Microsoft Storage account needs to be established.

- 1. From a web browser, navigate to <a href="https://portal.azure.com/">https://portal.azure.com/</a>.
- 2. Log in to the Microsoft account.
- 3. On the home screen, click Create a resource.

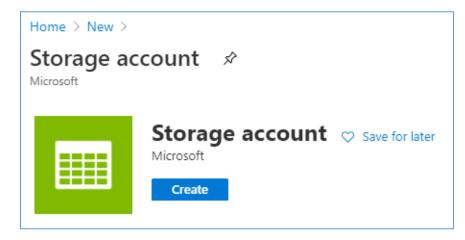
Azure servic	es				
Create a	All resources	Storage	Virtual	App Services	SQL databases
resource		accounts	machines	. ap services	502 636000505

4. Type storage account into the search bar, then click Storage account.

Home >		
New		
	>	<
Storage account		
·		
Get started	Windows Server 2016 Datacenter Quickstarts + tutorials	
Recently created		
AI + Machine Learning	Ubuntu Server 18.04 LTS	
Analytics	Learn more	

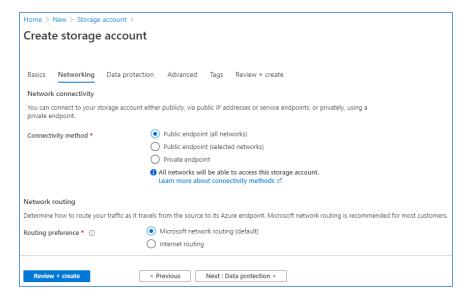
5. On the Storage Account screen, click the **Create** button. A new screen will appear that requires information to be populated, found in the **Basics** tab. When complete, click the **Next: Networking** button. Populate the **Basics** information using the following values:

- a. On the **Subscription** field, select **Enterprise** from the pull-down menu.
- b. Navigate to the **Resource Group** field. Select the corresponding **r**esource group. If one is not available, create a new resource group.
- c. Navigate to the **Storage Account Name** field. From the pull-down menu, select the storage account name that had previously been created.
- d. Navigate to the Location field. From the pull-down menu, select (US) East US.
- e. Navigate to the Performance field and select Standard.
- f. Navigate to the Account Kind field. From the pull-down menu, select StorageV2.
- g. Navigate to the **Replication** field. From the pull-down menu, select **Geo-redundant storage** (GRS).
- h. Navigate to the Access Tier field and select Hot.



Home $>$ New $>$ Storage account $>$	
Create storage accou	nt
5	
Basics Networking Data prote	ection Advanced Tags Review + create
Project details	
Select the subscription to manage depl your resources.	loyed resources and costs. Use resource groups like folders to organize and manage all
Subscription *	Visual Studio Enterprise Subscription
Resource group *	✓
5 1	Create new
Instance details	
The default deployment model is Resou the classic deployment model instead.	urce Manager, which supports the latest Azure features. You may choose to deploy using Choose classic deployment model
Storage account name * 🔅	
Location *	(US) East US 🗸 🗸
Performance 🗊	Standard      Premium
Account kind (i)	StorageV2 (general purpose v2)
Replication (i)	Geo-redundant storage (GRS)
Access tier (default)	🔘 Cool 💿 Hot
Review + create	< Previous Next : Networking >

- 6. Select the **Networking** tab. This will display a form with a series of fields that need to be populated. Fill out the **Networking** information using the following respective values.
  - a. Navigate to the Connectivity Method field and select Public endpoint (all network).
  - b. Navigate to the Network Routing Preference field and select Microsoft network routing.

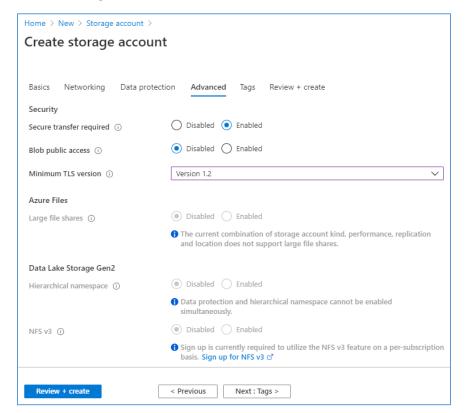


- 7. After supplying the values above, click the Next: Data Protection button.
- 8. Select the Data Protection tab, and populate the information as follows:
  - a. Navigate to the Blob Soft Delete field and select Enabled.
  - b. Navigate to the Blob Retainment Period in Days field and enter 60.
  - c. Navigate to the File Share Soft Delete field and select Disabled.

Home > New > Storage ac	count >
Create storage a	account
Basics Networking	Data protection Advanced Tags Review + create
Blob soft delete 🔅	O Disabled ( Enabled
Blob retainment period in da	ays ① 60 days
File share soft delete (i)	Disabled      Enabled
Versioning ()	Disabled      Enabled
	The current combination of subscription, storage account kind, performance, replication and location does not support versioning.
Review + create	< Previous Next : Advanced >

- 9. Click the Next: Advanced button.
- 10. Populate the Advanced information as follows:

- a. Navigate to the Secure Transfer Required: field and select Enabled.
- b. Navigate to the Blob Public Access field and select Disabled.
- c. Navigate to the Minimum TLS Version pull-down menu and select Version 1.2.
- 11. Click **Next: Tags** button.



12. Fill out the Tags information, then click Next: Review + create.

Home >	New > Storage	account >				
Creat	e storage	account				
Basics	Networking	Data protection	Advanced	Tags	Review +	create
	Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags 🖉					
Note tha	t if you create tag	gs and then change re	source settings	on other	tabs, your f	tags will be automatically updated.
Name	D	Val	ue 🛈			Resource
		:				Storage account
Reviev	/ + create	< Pr	evious	Next : Re	eview + cre	ate >

13. Review the **Create storage account** configuration page, verify the configuration information, then click **Create.** 

## Basics

- Subscription: Visual Studio Enterprise Subscription
- Resource group: \*\*\*\*\*\*\*
- Location: East US
- Storage account name: \*\*\*\*\*\*\*
- Deployment model: Resource manager
- Account kind: StorageV2 (general purpose v2)
- Replication: Geo-redundant storage (GRS)
- Performance: Standard
- Access tier (default): Hot

#### Networking

- Connectivity method: Public endpoint (all networks)
- Default routing tier: Microsoft network routing (default)

#### **Data protection**

- Blob soft delete: Enabled
- Blob Retainment Period in Days: 60

- File share soft delete: Disabled
- Blob change feed: Disabled
- Versioning: Disabled

## Advanced

- Secure transfer required: Enabled
- Blob public access: Disabled
- Minimum TLS version: TLS 1.2
- Large File Shares: Disabled
- Hierarchical namespace: Disabled
- NSF v3: Disabled

✓ Validation passed	
Basics Networking	Data protection Advanced Tags Review + crea
Basics	
Subscription	Visual Studio Enterprise Subscription
Resource group	
Location	East US
Storage account name	
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Geo-redundant storage (GRS)
Performance	Standard
Access tier (default)	Hot
Networking	
Connectivity method	Public endpoint (all networks)
Default routing tier	Microsoft network routing (default)
Data protection	
Blob soft delete	Enabled
Blob retainment period in d	ays 60 days
File share soft delete	Disabled
Blob change feed	Disabled
Versioning	Disabled
Advanced	
Secure transfer required	Enabled
Blob public access	Disabled
Minimum TLS version	Version 1.2
Large file shares	Disabled
Hierarchical namespace	Disabled
NFS v3	Disabled

14. Wait for the deployment process to finish. When the deployment is ready, a screen will announce that the deployment has been created.

Ø	Your deployment is complete
	Deployment name: Microsoft.StorageAccount Subscription: Visual Studio Enterprise Subscription Resource group:
$\sim$	Deployment details (Download)
^	Next steps
	Go to resource

15. Navigate to the home screen and click All resources.

Navigate			
<b>?</b> Subscriptions	()	Resource groups	All resources

- 16. Click the newly created storage account.
- 17. Navigate to Firewalls and virtual networks on the left.
- 18. Make the following modifications, then click Save:
  - Allow access from: Selected networks
  - Address range: \*\*\*\*\*\*\*

🔚 Save 🗙 Discard	🖒 Refresh	
i Firewall settings allow	wing access to storage service	s will remain in effect for up to a minu
Allow access from All networks	lected networks	
1 Configure network sec	urity for your storage acco	unts. Learn more 🗗
Virtual networks		
Secure your storage accou	nt with virtual networks.	+ Add existing virtual network +
Virtual Network	Subnet	Address range
No network selected.		
Firewall		
Filewall		
	ess from the internet or you	ur on-premises networks. Learn mor
	-	
Add IP ranges to allow acc	-	
Add IP ranges to allow acc	-	-
Add IP ranges to allow acc	-	-

- 19. Navigate to **Encryption** on the left.
- 20. Under Encryption type, select Customer-managed keys.
- 21. Under Encryption key, select Select from key vault.
- 22. Under Key vault and key, click Select a key vault and key.

Encryption Encryption scopes	
🔚 Save 🗙 Discard	
Storage service encryption protects you access it.	ur data at rest. Azure Storage encrypts your data as it's written in our datacent
By default, data in the storage account	is encrypted using Microsoft-managed keys. You may choose to bring your o
	e Service Encryption, only new data will be encrypted, and any existing files in t .earn more about Azure Storage encryption 🖙
Encryption type	O Microsoft-managed keys
	<ul> <li>Customer-managed keys</li> </ul>
	The storage account named 'nccoepacstest' will be granted access to protection will be enabled on the key vault and cannot be disabled.
Encryption key	O Enter key URI
	<ul> <li>Select from key vault</li> </ul>
Key vault and key *	Select a key vault and key

## 23. Under Key Vault, click Create New.

Home > All resources >	Encryption >	
Select key from Azure	e Key Vault	
-	2	
Subscription *	Visual Studio Enterprise Subscription	$\sim$
Key vault *		$\sim$
	Create new	,
Key		$\sim$
-	Create new	

- 24. On the Create key vault screen, select the Basics tab, and populate the information as follows:
  - a. Navigate to the **Resource Group** field, select the corresponding resource group.
  - b. Navigate to the Key Vault Name field, select the corresponding key vault name.
  - c. Navigate to the **Pricing Tier** field; select **Premium.**
  - d. Navigate to the **Soft-Delete** field; select **Enabled.**
  - e. Navigate to the Days to Retain Deleted Vaults field; enter 60.
  - f. Navigate to the Purge Protection field; select Allow purging.

Create key vault	
Basics Access policy Netwo	orking Tags Review + create
	Jiking lags Review Create
Project details	
2	ployed resources and costs. Use resource groups like folders to organize and manage al
your resources.	,, ,
Subscription	Visual Studio Extension Subscription
Subscription	Visual Studio Enterprise Subscription
Resource group *	\
	Create new
Instance details	
Key vault name * 🕠	· · · · · · · · · · · · · · · · · · ·
Region	East US N
Pricing tier * (i)	Premium (includes support for HSM backed keys)
Recovery options	
	eleted key vault and its objects within the retention period you specify. Purging triggers of the key vault. When purge protection is enabled, vault and its object in the deleted ntion period has passed. Learn more
Soft-delete 🛈	Enable recovery of this vault and its objects
_	Disable recovery of this vault and its objects
	1 Once enabled, this option cannot be disabled
Days to retain deleted vaults * 🕢	60
Purge protection ①	Allow purging of this vault and its objects during retention period
	Enable purge protection of this vault and its objects during retention period

## 25. Click the Next: Access Policy button.

- 26. Fill out the Access Policy information, then click Next: Networking.
  - a. Navigate to the Enable Access to group, and set the following checkboxes:
    - Azure Virtual Machines for deployment: Unchecked
    - Azure Resource Manager for template deployment: Unchecked
    - Azure Disk Encryption for volume encryption: Unchecked
  - b. Navigate to the Current Access Policies: group and keep the Default User Permissions.

Create key vau	t				
ciedte key vau	·				
Basics Access policy	Networking Tags	Review + create			
nable Access to:					
Azure Virtual Machines	for deployment ①				
_	er for template deploymer	nt 🙃			
Azure Disk Encryption in	or volume encryption ①				
Add Access Policy					
urrent Access Policies					
unent Access Policies					
Name	Email	Key Permissions	Secret Permissions	Certificate Permissions	Action
Name					
USER					
		9 selected	7 selected	15 selected	Dele
		9 selected	7 selected V	15 selected V	Dele

27. On the **Create key vault** screen, under the **Networking** tab, navigate to the line labelled **Connectivity method** and select **Public endpoint(all networks)** and then click on **Next:Tags>.** 

Home >	Encryption > Select key from Azure Key Vault >
Creat	e key vault
Basics	Access policy Networking Tags Review + create
Network	connectivity
You can co endpoint.	onnect to this key vault either publicly, via public IP addresses or service endpoints, or privately, using a privat
Connectiv	vity method   Public endpoint (all networks)
	<ul> <li>Public endpoint (selected networks)</li> </ul>
	O Private endpoint
Review	<pre>v + create &lt; Previous Next : Tags &gt;</pre>

28. Fill out the Tags information, then click Next: Review + create.

Home >   Encryption > Select key from Azure Key Vault >					
Create key vau	Create key vault				
-					
Basics Access policy	Networking Tags Review + creat	ie			
	Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more				
Name 🛈	Value 🛈	Resource			
	:	Key vault			
Review + create	< Previous Next : Review +	create >			

29. Review the **Create key value** configuration page, verify the configuration information, then click **Create.** 

## Basics

- Subscription: Visual Studio Enterprise Subscription
- Resource group: \*\*\*\*\*\*\*
- Key vault name: \*\*\*\*\*\*\*
- Region: East US
- Pricing tier: Premium
- Soft-Delete: Enabled
- Purge Protection During Retention Period: Disabled
- Retention period (days): 60 days

#### Access policy

- Azure Virtual Machines for deployment: Disabled
- Azure Resource Manager for template deployment: Disabled
- Azure Disk Encryption for volume encryption: Disabled
- **Permission model:** Access control list
- Access policies: 1

NIST SP 1800-24C: Securing Picture Archiving and Communication System (PACS)

# Networking

Connectivity method: Public endpoint (all networks)

Home >	Encryption >	Select key f	rom Azure K	ey Vault 🗦
Create key va	ult			
<ul> <li>Validation passed</li> </ul>				
Basics Access policy	/ Networkir	ig Tags	Review +	create
Review + create				
Basics				
Subscription Resource group Key vault name		Visual Studi	o Enterprise S	ubscription
Region		East US		
Pricing tier		Premium		
Soft-delete		Enabled		
Purge protection during re	etention period	Disabled		
Days to retain deleted vau	ılts	60 days		
Access policy				
Azure Virtual Machines for	r deployment	Disabled		
Azure Resource Manager deployment	for template	Disabled		
Azure Disk Encryption for encryption	volume	Disabled		
Permission model		Access cont	rol list	
Access policies		1		
Networking				
Connectivity method		Public endp	oint (all netw	orks)
Create	< Pr	evious	Next >	Download a

- 30. Wait for the creation process to finish.
- 31. Navigate to the **Key** field and click **Create New.**

Home > E	acryption >	
Select key from Azure Key Vault		
-		
Subscription *	Visual Studio Enterprise Subscription	$\sim$
Key vault *	Create new	$\checkmark$
Kev *		~
	Create new	

- 32. Fill out the form with the following information, then click **Create:** 
  - **Options**: Generate
  - Name: \*\*\*\*\*\*\*
  - Key Type: RSA
  - RSA Key Size: 2048
  - Enabled?: Yes

Home >	Encryption $>$ Select key from Azure Key Vault $>$
Create a key	
Options	
Generate	$\sim$
Name * (i)	
	~
Key Type 🔋	
RSA EC	$\supset$
RSA Key Size	
2048 3072 4096	
Set activation date? ①	
Set expiration date? 🗊	
Enabled?	Yes No
Create	

- 33. Once the key has been successfully created, ensure the values for **Subscription**, **Key Vault**, and **Key** are correct as follows, then click **Select**:
  - Subscription: Visual Studio Enterprise Subscription
  - Key vault: \*\*\*\*\*\*\*
  - Key: \*\*\*\*\*\*\*

Select key fi	om Azure Key Vault	
1 The key '	has been successfully created.	
Subscription *	Visual Studio Enterprise Subscrip	ption 🗸
Key vault *		~
	Create new	
Key *		~
	Create new	

34. Verify the following Encryption information, then click Save:

- Encryption type: Customer-managed keys
- Encryption key: Select from key vault
- Key vault: \*\*\*\*\*\*\*
- Key: \*\*\*\*\*\*\*

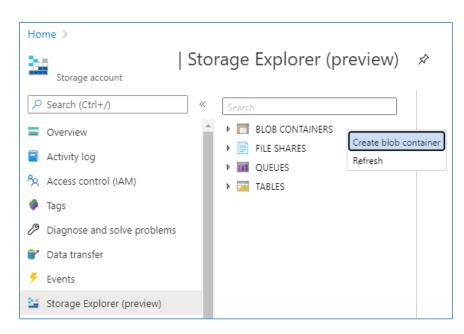


Encryption Encryption scopes	
🖫 Save 🗙 Discard	
Encryption type	O Microsoft-managed keys
	<ul> <li>Customer-managed keys</li> </ul>
	The storage account named ' ' will be protection will be enabled on the key vault and can
Current key	
Automated key rotation 🔅	Enabled - Using the latest key version
Key version in use	
Change key	

- 35. Take note of the key strings. These will be used to authenticate the VNA's requests to the storage account:
  - Storage account name: \*\*\*\*\*\*\*
  - Key: \*\*\*\*\*\*
  - Connection string: \*\*\*\*\*\*\*

Storage account name
key1 💭
Key
Connection string

- 36. Navigate to Storage Explorer on the left of the Storage Explorer (preview) page.
- 37. Right-click BLOB CONTAINERS, then click Create blob container.



38. Fill out value of the Name field for the New container, then click Create.

New container	×
Name *	
	$\sim$
Public access level (i)	
Private (no anonymous access)	$\sim$
The public access level is set to private because public acc disabled on this storage account.	ess is
✓ Advanced	
<b>Create</b> Discard	

39. The established storage account is ready for use, and the VNA can be configured to send and receive medical images to and from the storage account container.

## 2.9.2 Hyland VNA Cloud Archive Device

For this project, a Hyland engineer upgraded the Hyland Acuo VNA v6.0.4 and NilRead Enterprise v4.3.31.98805 to Acuo VNA v6.0.4.2798\_H2\_P2 and NilRead Enterprise v4.4.32.103830. These upgrades enabled the Hyland VNA to store patient studies in a Microsoft Azure storage account. When configuring the connection to the Azure account, the VNA allowed an engineer to determine the number of days that patient studies were held in the cache. For testing purposes, this project kept studies in the VNA cache for three days and immediately stored these studies in the Azure storage. When configuring for production, identify time frames for cache and cloud storage that coincide with an HDO's business practices.

#### **Hyland NilRead Archive Device Configuration**

- 1. Open a web browser and navigate to the Acuo Admin Portal created in <u>Section 2.2.2</u>, Hyland Acuo VNA.
- 2. Enter the Username and Password for the Admin Portal, and click Sign In.

🛊 Jose Almon Partal 🛛 🗴 🕂		- 5
A → C (C) localhost1000/VnaWeb/%/login		~ @ ☆ @
Acuo		
	Acuo Admin Portal	
	Username	
	Password	
	Sign In	
	1.7.149.31764	

3. Navigate to the Archive Devices section of the portal by clicking the drop-down list on the top left corner of the screen and selecting **Storage Management** and then **Archive Devices**.

		- 0 × + 0 \$ 0 ;
Acuo	Home *	September 1000 • • •
	Runnert Hopbour Wardew Runne Management Storige Anangement	
	Enteriora Reporter	
	Vytem Explorer Patient Explorer Veccole Management > Senantiz > Administration Automy > Veccole Manage Patients Administration Automy > Veccole Manage Patients	Workflow Manage Norther Centers More Manages Store Manager
	Apost Marinto A	
	Route Management Manage Roths, Alls and Destinations Gis to Route Management	Storage Management Manage Storage Applications, 50 executed Arthrees Manage Storage
	<b>1</b>	r <sup>m</sup> n

4. Click Add New Archive Device in the top of the screen, then select Azure.

Aue tonin hirtel	x +	- 0 X
€ → C © localhost8099	NinaWeb/#Utorage2/archives/fat	• Q & O :
Acuo Archive De	vices ~	🕼 Hyland Service Der
O. Search systems	I systems Add New Arowa blevice + Search	
A Default	Nome 7 Storage Management / Archive Devices	

- 5. In the Add New Azure Archive Device window, provide the following Azure account information:
  - Name: \*\*\*\*\*\*\*
  - Container Size: 20 MB
  - Account Name: \*\*\*\*\*\*\*
- 6. Click Add Archive Device.

cuo Archive Dev	nces >	Add New Azure Archive Device	La regione Service La
	Barner Calif		
Detault	-Hinter - Marriel Line		
C. She age Applications	Incore de	VoerAunt Consistentian	Providence of Applications
Anthias Devices	Autor	Container Sine 2004E	4
Re Darage between 1	North Adda	0 12 20 140 0 10 0 kms 20240	1
		Security Settines	
		Access Name	
		ALL	
		Access Nov	
		Advanced Options	
		Mastrum Addresses	
		16	
		Mercey Stream Buffer	
		8	
		Connection	
		Tout Connection	

#### Connect Microsoft Azure Archive Device to the RADIOLOGY Storage Application

- 1. Click **Storage Applications** on the left-hand side of the screen.
- 2. Click RADIOLOGY.
- 3. Scroll down and click Add Archive.
  - Device: \*\*\*\*\*\*\*
  - Write files older than: 1 day(s)
  - Enable Write files to archive.
- 4. Click Add Archive.

Acuo Storage App	lications~										a mysere service Low	
	I terms	Add Archiv	e to Applic	ation								
ADres		Device Settle	ngs									
C Margan Applications	Application Settings	Device										
Els transport i transm Active Devices		Novelaat (kort)										
& Brage solation Harre & Compositor M200,000	Name	Wite Net older 1	With fire sider than							Adding Topol		
C competition		1	Unvo.	0	tion in	8	virales		seconds			
	Websleis Source	Container Size										
			168	10	V.	19	69.	*: ·	Daylees		markan Settings i 🗰 Delete dua fala	
	Cache Cleaner-Confi	-	nive							1.000	the sum second ( ) at press strains	
	Clean Films Older Than	The value can be a	and in terroraria	dualie writing #	on the epitement	the action de-	on the sill of affect	the solicato	to that with to the	Centre		
	Jano	Security Set	tines									
		Account Name									If List Lacte Dearer Sartyurs	
	Reter	/stoepurt have										
	Rene	Account lice									(1146)	
	AADREDGY /	Carlot and the second									5	
		Connection									Different Australian Pre	
	Arthur Caulors									Burtle Elles to archive	to electron	
	mandaire (	Test Connection	in .							Test Lines Into archive	0	
										2000 C	1. <b>1</b> . 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	

#### Set Parameters for Image Archival to Microsoft Azure

- 1. Select **Nccoe-Azure** under Archive Devices at the bottom of the screen.
- 2. Set Write files older than to 0 days.
- 3. Click Save Changes.

Acuo Storage App	alications~										La injuré lanice Lour
	II below	Edit Archive	Settings								
Acres		Device Setting	15								
C Harage Applications Die Universitätieren E Antree Devices On Durage sedarium	Application Setting	Name Noort-Acare Wite Resolvert				Type Asure				dilling Trape	
Compositor	14210.00	0	sins	0	here's	8	rorsdes	6	seconda		
	Metadata Saurae Providente Saurae Cartonica Ca	Container Sizz	68		50		-03		b/re-	P18.	
	Cache Cleaner Conf	. Herbe Kies to at	chie							.e.	hit haats also betrege ) 🗷 Debie daa karb
	clean files Older than 3 days	fio žesla		iy dabir ortrg	trow the application	e to the archite	device. This will rest aff	let strie apples	Assoc (Dail dai the Ro	Carlos	
		Connection Se	ettings								If the lacks Oscer fortgam
	Barne .	00									Artise
	ALDICOTA	Post									0
	Northean Charleses	Connection									E Hange Australia Part
	No. 14	_								Worthe Block to archive	te Miller
	think down (								Cancel	The state of the s	0

#### Set Parameters for Storing Images in the VNA's Cache

- 1. Click Edit Cache Cleaner Configuration.
- 2. Set Clean Files Older Than to 3 days.
- 3. Click Save Changes.

Acuo Storage App	lications ~							A mainte Lanice Low
	2 hours	Edit Ca	che Cleaner Con	figuration		9	2	
A Carlante	Hole During Maria	* India	Cache Cleaner					
C Manage Applications	Application Settin	Granifie 1	s Older Than 38/1	a here a	sinute: 0	seconds		
Active Second     Active Second     Active Second	Name AADIO.009	# Yesty	Archive Location Before Re	moving from Image Cache			akiling Tepe	
	Metadata Source President MSCOPPEND	200				San Charges Canol	ant:	
	Cache Cleaner Co	nfiguration					and the second	isariw Settings I 🕷 Delete Asabatis
	Clean Dies Older Then				Marily Aug	vie Location Balance Removing Insue in	age Cashe	
	3 days							(# lat Dete Dener Gortgunter
	1000 C							
	Nite							ritie
	AAGREEDON .			PTURIC-INFINITION OF T			4	
								15 Manage Replector Stars
	Alttine (Insign	Tape	Consection M (bg		Continuine		W/M Bistonitine	is wiles
	APPENDIAL COLUMN	Tran	fasserflat Mileg		- Copyranter - Milleriger		Web Bests whee	k min

### 2.10 Secure Remote Access

Both healthcare and IT systems require access by vendor support technicians for remote configuration, maintenance, patching, and updates to software and firmware. This project implemented secure remote access by integrating Symantec Validation and ID Protection (VIP) into the ConsoleWorks authentication mechanism. This implementation enforced two-factor authentication with username, password, and a onetime passcode.

## 2.10.1 TDi Technologies ConsoleWorks

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

#### System Requirements

- **CPUs:** 1
- Memory: 8 GB RAM
- Storage: 40 GB
- Operating System: CentOS 7
- Network Adapter: VLAN 1097

#### **TDi ConsoleWorks Installation**

The TDi ConsoleWorks installation in this PACS environment replicates the installation in the Wireless Infusion Pumps Project. For detailed installation guidance, please refer to Section 2.1.8, TDi ConsoleWorks External Remote Access, in NIST SP 1800-8C, *Securing Wireless Infusion Pumps* [12].

#### **TDi ConsoleWorks Radius Authentication Configuration**

In our project, we integrated TDi ConsoleWorks with the Symantec VIP for two-factor authentication. This section explains how to enable external authentications for ConsoleWorks. In the next section, we explain how we configured Symantec VIP to integrate with ConsoleWorks.

- 1. Download *extern\_auth\_radius.so* file from ConsoleWorks support site [14].
- 2. Move *extern\_auth\_radius.so* file to */opt/ConsoleWorks/bin* directory.
- 3. Restart ConsoleWorks by executing *cw\_stop* and *cw\_start* scripts located in the /opt/ConsoleWorks/bin directory.
- 4. From the ConsoleWorks web interface, navigate to Security, and click External Authentication.
- 5. Click **add** to create a new external authentication source.

- 6. Fill out the required fields. The setup we used is below:
  - Record Name: Radius
  - Ensure **Enable** is checked.
  - For Library, select radius.
  - Parameter 1: 192.168.120.190:1812/\*\*\*\*\*\*
  - Parameter 2: 30
  - Parameter 6: 15
  - **Template User:** CONSOLE\_MANAGER
- 7. Continue through the prompt by clicking **Next**; click **Save** on the final prompt.

External Authentica	tion Record	>
Record Name:	RADIUS	
	Enabled	
Library:	radius 🔫	
Parameter 1:	192.168.120.190:1812/******	
Parameter 2:	30	
Parameter 3:		
Parameter 4:		
Parameter 5:		
Parameter 6:	15	
Required Profile:		
Template User:	CONSOLE_MANA =	
	Cancel Next	

8. Ensure that Enable External Authentication is checked.

<ul> <li>SECURITY: External Auth</li> </ul>	+_ <b></b>		
External Authentication 🗙			
Enable External Authenticati	on		
External Authentication assu	med for pre-existing User ac	counts	
External Authentication	Library	Enabled	Param 1
RADIUS	radius	Υ	192.168.120.190:1812/
Up Down		Delete	Rename Edit Save

## 2.10.2 Symantec Validation and ID Protection (VIP)

Symantec Validation and ID Protection is an authentication service that provides various forms of authentication such as push, short message service (SMS), and biometric. This project used Symantec VIP as a second form of authentication for remote access to the PACS architecture through TDi Technologies ConsoleWorks.

#### System Requirements

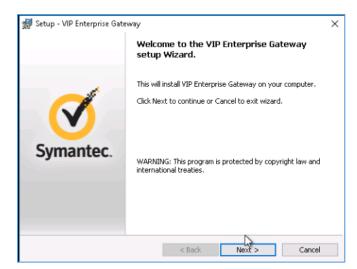
- **CPUs:** 4
- Memory: 8192 MB RAM
- Storage: 240 GB (thin provision)
- Operating System: Microsoft Windows Server 2016
- Network Adapter: VLAN 1201

#### **Symantec VIP Installation**

1. Right-click on *setup.exe* file for VIP Enterprise Gateway 9.8.0; select **Run as administrator.** 

<mark> </mark>   🖓 📘 🖛			Application Tools	VIP_Enterprise_	Gateway_9_8_0_WINDO	SWC	
File Home	Share	View	Manage				
$\leftarrow \rightarrow \checkmark \uparrow$	> VIP	_Enterprise_	Gateway_9_8_0_WINI	DOWS			
	_	Name	^		Date modified	Туре	Size
🖈 Quick access		🔄 setup			5/2/2019 4:33 PM	Application	142,557 KB
Desktop	*						
Downloads	Я Я						
Documents				VIP Entern	rise Gateway - InstallSh	ield Wizard	
📰 Pictures 💻 This PC 💣 Network	A			۲	IP Enterprise Gateway Se Vizard, which will guide yo ease wait.	etup is preparing the I	
				Extracting	: VIP Enterprise Gateway	/.msi	
				-			Cancel

2. Proceed through the installation wizard by clicking Next >.



- 3. Check I accept the agreement.
- 4. Click **Next >.**

License Agreement Please read the following License Agreement carefully. You must accept the Symantec. Validation & DProtection terms of this agreement before continuing the installation.					
	SYMANTEC SOF	FTWARE LICENSE AGREEMENT	^		
LICENSE THE LICE	NSED SOFTWARE ( THAT WILL BE U	R ITS AFFILIATES ("SYMANTEC") IS V TO YOU AS THE INDIVIDUAL, THE CO JTILIZING THE LICENSED SOFTWARE (F LY ON THE CONDITION THAT YOU AC	MPANY, OR REFERENCED		
THE TERMS OF TH AND CONDITION LICENSED SOFTWA	S OF THIS LICEN ARE. THIS IS A LE	EMENT ("LICENSE AGREEMENT"). READ ISE AGREEMENT CAREFULLY BEFORE GAL AND ENFORCEABLE CONTRACT BE IF "LAGREF" OR "YES" BLITTON OR	THE TERMS USING THE TWEEN YOU		
THE TERMS OF TH AND CONDITION LICENSED SOFTWA	S OF THIS LICEN ARE. THIS IS A LE	SE AGREEMENT CAREFULLY BEFORE GAL AND ENFORCEABLE CONTRACT BE	THE TERMS USING THE TWEEN YOU		
THE TERMS OF TH AND CONDITION LICENSED SOFTWANTEC	S OF THIS LICEN ARE. THIS IS A LE BY CLICKING TH rement.	SE AGREEMENT CAREFULLY BEFORE GAL AND ENFORCEABLE CONTRACT BE	THE TERMS USING THE TWEEN YOU		

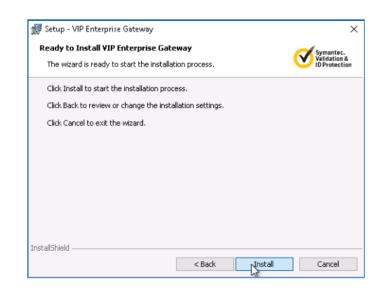
5. Create a username as admin and a password and click Next >.

Configuration Console Access	Ø	Symanted Validation ID Protect
Enter the name of the user who will mar password that user will use to log into th are case sensitive.		ł
Username (minimum 5 characters)		
admin	 	
Password (minimum 8 characters)		
•••••	 	]
Confirm your password.		
•••••	 	1
		1
stallShield	 	
		Cancel

6. Keep the default installation location by clicking Next >.

	Destination Folder Click Next to install to this folder or click Change to install to a different folder.					
Þ	Install VIP Enterprise Gateway C:\Program Files (x86)\Syman		e_Gateway\	Change		
InstallShield -		< Back	Next >	Cancel		

7. Click Install.



8. Click **Finish** after installer is complete.

孆 Setup - VIP Enterprise Gate	way X VIP Enterprise Gateway successfully installed.
Symantec.	This wizard has successfully installed VIP Enterprise Gateway on your computer Click Finish to exit the setup. ☑ Launch the Configuration Console
	< Back Finish Cancel

9. On the Symantec VIP local machine, open a web browser, and navigate to http://localhost:8232. Sign in with the **User Name** as **admin** and corresponding **Password** specified during installation.

U oginanteor	/IP Enterprise Gateway			
	_	Sign In		
	User Name	admin ]		
	Password	•••••	Sign In	

10. Select **User Store** from the menu bar.

Symantec. VIP Enterprise Gateway							
Home User Store	Validation	Identity Providers	Logs	Settings	Help		
User Store > User Store							
Links	Add User	Store					
User Store	> You must conf	gure a connection with each	new user store th	at you add to VIP B	Enterprise Gateway.		
LDAP Directory Synchronization			Us	er Store			
VIP Administrator Configuration							
Console Authentication	Type:		LDAP				
	*Name:					(?)	
		Server Information					
		server information					
	*Connection	x				(?)	
	*Host					(?)	
	*Port:		?	0			
	Timeout:		2 🗸 Sec	onds			
	Enable SS	La					
	Bind Information						
	*User DN:					3	
	*Password:					(?)	
			Sear	ch Criteria			
	Base DN:					(?)	
	0000.014						

11. Add a user store with the following information:

- Name: AD PACS
- Connection: ad-main
- Host: ad.pacs.hclab
- **Port:** 389
- User DN: CN=symantec, DC=pacs, DC=hclab
- Password: \*\*\*\*\*\*\*\*
- Base DN: DC=pacs, DC=hclab
- User Filter: (&(&objectClass=user)(objectCategory=person))(sAMAcountName=%s))

Console Authentication	iype.	LUAP		
	"Name:	AD-PACS	?	
		Server Information		
	*Connection:	ad-main	?	
	*Host	ad.pacs.hclab	(?)	
	*Port:	389 (?)		
	Timeout:	2 Seconds		
	Enable SSL:			
		Bind Information		
	*User DN:	CN=cpeloquin,DC=pacs,DC=hclab	(?)	
	*Password:		?	
		Search Criteria		
	Base DN:	DC=pacs,dc=hclab	?	
	*User Filter:	(&(&(objectClass=user)(objectCategory=person)) (sAMAccountName=%s))	?	
		Edit Default VIP User Name Attribute		
		Test Settings		
	*Test User Name:	kangmin Te	st 🛛 🏵 🕐	
		Test bind failed. Be sure you have the correct Host, Port, and Bind information for the User Store AD-PACS.	SSL (if selected),	
	*Required Information	Cancel		

- 12. Log into VIP Manager by navigating to https://manager.vip.symantec.com/vipmgr. Use the account provided by Symantec.
- 13. Select **Register Your VIP Credential.** Provide **the Credential ID** and **Security Code** of your credentials. Credentials can be downloaded by navigating to <u>https://vip.symantec.com/</u>.

Symantec.   VIP MANAGER			
		Register Your VIP Credential	
	Provide your crede credential	ntial ID and a security code to register your VIP	
	Credential ID:	VSST22651643	
	Security Code:	Typically 12 alphanumeric characters           286928         ×	
		6 digits generated from your VIP credential	
		Cancer report	

14. After registering the credential, select Go to My Account.

ashboard	Users	Credentials	Account	Policies	Reports	Help	
0							
		ntial Was Registe			ir account.		
	Go to My Account						

15. Select Account from menu bar, then select Manage VIP Credentials.

Dashboard	Users	Credent	ials Accou	nt Polic	ies Reports	Help	
Account Summar			θE				Units  VIP Account Management  VIP Account Details
Account Information	Single Sign-on	Features	Dynamic Provisioning	Registration File			Manage User Groups
	Management		Ornaniza	tion Information			Create Administrator Group
Organization Name UNVERIFIED - NCCet			Organizational Unit		Organization Address 9700 Creat Seneca Hwy Rockville MD 20050 United States		Find / Modify Administrator Groups     Create VIP Administrators     Find / Modify VIP Administrators
Contact Information							Manage VIP Certificates
Corporate Contact Sue Wang NA swang@mitre.org 301975-0288 (preferre	d)		Technical Contact Sue Wang NA swang@mitre.org 301975-0288 (preferred)		Billing Contact Sue Wang NA swang@mitre.org 301975-0288 (preferred)		SMS Credential Settings     SMS Credential Security Settings     Download Files
			Accou	nt Information			
Jurisdiction Hash	14004610-	4					
Account Creation Dat	te* 2019-May-	03					
Service Start Date*	2019-May-	-03					
Service End Date*	2019-Jul-0	2					
Member Type	Trial						
Account Usage	Test						
Sales Reference Num	ber						

#### 16. Select Request a Certificate.

Manage VIP Certificat	25					
Use this page to request a new	es					
Use this page to request a new						Links
	certificate or to track your	existing certificates.				VIP Account Management
Click Request a Certificate to						View Account Details
80						Manage User Groups
		Certific	cates			Create Administrator Group
Cert	ficate Name A	You have no certificates assoc	Expiration*	State	Action	Find / Modify Administrator Groups
		Cancel Regu	vest a Certificate			Find / Modify VIP Administra     Manage VIP Certificates     StMS Credential Settings     Credential Security Settings     Download Files

17. Provide a Certificate Name as NCCoE\_VIP\_Cert. Click Submit Request.

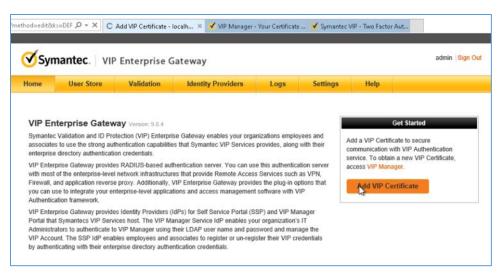
Dashboard	Users	Credentials	Account	Policies	Reports	Help	
http://dianalesia.count							Links
Request a Cer	tificate						VIP Account Management
Enter an easily-reco	gnizable name for you	ar certificate (such as "VIP Certi	ficate 1") in the	e field below.			View Account Details
If you have your own	n private key, enter a C	Certificate Signing Request (CS	R) that you've	generated by clicking here	Symantec supports 2048	bit keys in the CSR.	
* Required Informati	on						Manage User Groups
			Certificat	ta Nama			Create Administrator Group
*Certificate Name	1000 F 100 F	7	Ceroncar				Find / Modify Administrator Groups
	NCCoE_VIP_Ce	biđ		× (?)			Create VIP Administrators
							Find / Modify VIP Administration
Important Service Req	puirements: If you discove	er or have reason to believe that the	re has been a co	mpromise of your private key, y	ou must immediately revoke th	e certificate or notify Symantec to do	Manage VIP Certificates
		ate or your organization name has of					SMS Credential Settings
nosce if (i) you fail to pe systems.	norm your obligations und	ser the terms of your service agreem	writ, or (A) in Syn	nantecs sole discretion, you have	e engages in activities which t	lymanitec determines are harmful to its	
							Credential Security Settings
			lack Su	ti Nit Request			Download Files
			Sur Su	a and and a start and a start a			

18. Select PKCS#12 format and create a password for the requested certificate. Then select Download Certificate.

* Required information  *Format  PEM  PKCS#12    Must be at least eight characters and include one uppercase and one lowercase letter, plus one number.  Download Cortificate		Links  VIP Account Management VIP Account Details Manage User Groups Create Administrator Groups Create Administrator Groups Create VIP Administrator Groups Find / Modity VIP Administrator
Your certificate named NCCGE_VIP_Cert expires on 2921 May 06.  Solect a certificate format, enter a password to encryst the certificate, and then cick Download Certificate.  *Required information *Tormat OPEM OPECSe12  *Assword Counting of the still sat sight characters and include one supprase and one lowercase letter, plus one number. Counting of Certificate		VIP Account Management     View Account Details     Manage User Groups     Create Administrator Group     Find / Modify Administrator     Oroops     Create VIP Administrator
Your certificate named NCCOE_VIP_Cert expires on 2921 May 06. Select a certificate format, enter a password to encryst the certificate, and then click Download Certificate. *Required information *Format *Pessword Counties and one towercase lefter, plus one number. Counties of Certificate *Counties of Ce		View Account Details     Manage User Groups     Create Administrator Group     Find / Modily Administrator     Groups     Create VIP Administrators
Select a certificate formul, enter a password to encrypt the certificate, and then click Download Certificate.     Required Information     Point     Password     Petronat     Petronat     Point     Po		Manage User Groups     Create Administrator Group     Find / Modify Administrator     Groups     Create VIP Administrators
Required Information     Format     PEM      PKCS#12     ⑦     Wont be at least eight characters and include one     wepercase and one lowercase letter, plus one number.     Coverboad Certificate     ⑧		Create Administrator Group     Find / Modify Administrator     Groups     Create VIP Administrators
*Format O PEM © PKC5#12 ⑦ *Password ⑦ Must be at least eight characters and include one uppercase and one towercase letter, plus one number. Coventional Certificate		Find / Modify Administrator Groups     Create VIP Administrators
*Password () what be at least eight characters and include one suppresses and one towercase letter, plus one number.  Download Certificate		Groups     Greate VIP Administrators
uppercase and one lowercase letter, plus one number.  Download Certificate		
Orentoad Certificate		> Find / Modify VIP Administra
3		
After downleading your certificate. you will need to install it.		Manage VIP Certificates
After downloading your certificate, you will need to install it.		SMS Credential Settings
		Credential Security Settings
Go to the Help and Support page for PKCS#12 format if you need help installing the certificate to use with VIP Web s	vervices.	Download Files
Go to the Help and Support page for PEM format if you need help installing the certificate to use with a Cisco SA 500	series VPN router.	
Return Home		

19. Save the certificate on the Symantec VIP local machine.

#### 20. Navigate to http://localhoat:8232. After logging, select Add VIP Certificate.



21. Select **Browse** and upload the certificate from the previous step. Enter the correct password and alias for the certificate, then click **Submit.** 

	VIP Enterprise G	ateway				admin   Sign O
Home User Store	Validation	Identity Providers	Logs	Settings	Help	
ettings > VIP Certificate						
Links	Add VIP C	ertificate				
/IP Certificate		following steps to import a VI	P Certificate in .p1	12 format. If you do	o not have a VIP certifi	icate, click VIP Manager
SSL Certificate	to obtain a new	w certificate.				
rusted CA Certificate						
Export Settings	Failed to i	mport PKCS12 cert. Make su	Ire PKCS12 File a	nd Password are o	correct.	
mport Settings						
Console Settings			Add VI	P Certificate		
HTTP Proxy Settings						
	*File Name	κ.	C:\Users\Sym	nantec\Desktop\v	vip_cer Browse	
lealth Check Settings						
Health Check Settings Jpdate Settings	*Password:					

- 22. Select **Validation** from the menu bar, select **Custom configuration**, and provide the information that follows:
  - Server Name: vip
  - Local IP: 192.168.120.190

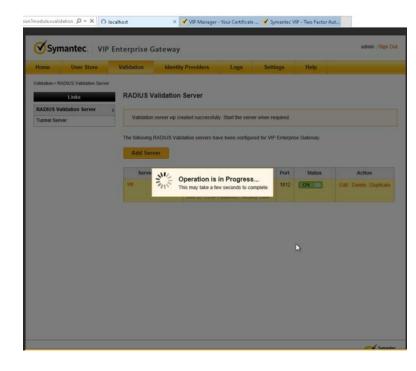
- **Port:** 1812
- RADIUS Shared Secret: \*\*\*\*\*
- Confirm RADIUS Shared Secret: \*\*\*\*\*
- Enable First Factor: Checked
- Authentication on: Enterprise
- Authentication Sequence: LDAP Password–VIP Authentication
- User Store: AD PACS

	tee. vii	Enterprise (	sateway				
Home U	ser Store	Validation	Identity Providers	Logs	Settings	Help	
alidation > RADIUS	Validation Server						
Lin	ks	Add RAD	US Validation Server	r:			
RADIUS Validatio	on Server	> Configure ser	ver parameters to create a va	lidation server.			
Tunnel Server				Serve	er Information		
		* Server N	ame				0
		* Local IP	C	192.168.120	190	-	~
		* Port		1812	0	L	1
		* RADIUS	Shared Secret				(?)
		* Confirm	RADIUS Shared Secret				0
		Logging L	evelt	INFO V	7		
		Log Rotat	ion Interval:	1 🗸			
		Number o	f Files to Keep:	4 🗸	1		
		Enable Sy	slog :	O Yes	No 🥐		
		* Passwor	d Encoding:	UTF-8	• •		
				RADIUS	Access Challenge		
				Enable Ac	cess Challenge 🥐		
		*Challenge	Timeout	60	(?)		
				VIP Pus	h Authentication		
				Enable Pu	ish		
		Remote A	ccess Service Name/URL:	Remote Acce	ess Service Name		1
		have a second	aliantian Timaaud	00	1.0		

#### 23. Click Submit.

VIP Authentication Timeout	60 🕐
*Enforce Local Authentication	○ Yes ● No ⑦
	First-Factor Authentication
	C Enable First Factor
Authentication on:	Enterprise     O VIP Services
Authentication Sequence:	LDAP Password - VIP Authentication
	O VIP Authentication - LDAP Password
	User Store Configuration
	User resides in user store ?
	Enable User Store data for Out-of-Band     ?
User Store:	AD-PACS
	Business Continuity
Business Continuity:	Disabled
	Delegation
	Enable Delegation (?)
	LDAP to RADIUS Mapping
	Enable LDAP to RADIUS Mapping
*Required Information	
	Cancel Shipmit

24. Ensure that VIP Server Status is set to ON.



# Appendix A List of Acronyms

AD	Active Directory
AES	Advanced Encryption Standard
AE Title	Application Entity Title
CA	Certificate Authority
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CSR	Certificate Signing Request
DB	Database
DC	Domain Controller
DCS:SA	Data Center Security: Server Advanced
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DNS	Domain Name System
EDR	Endpoint Detection and Response
FMC	Firepower Management Center
FTD	Firepower Threat Defense
GB	gigabyte
GUI	Graphical User Interface
HD	Hard Drive
HDO	Healthcare Delivery Organization
HIP	Host Identity Protocol
HL7	Health Level 7
http	Hypertext Transfer Protocol
https	Hyper Text Transfer Protocol Secure

IDN	Identity Defined Networking
IIS	Internet Information Services
ют	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MPPS	Modality Performed Procedure Step
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NTP OS	Network Time Protocol Operating System
OS	Operating System
OS OVA	Operating System Open Virtual Appliance or Application
OS OVA OVF	Operating System Open Virtual Appliance or Application Open Virtualization Format
OS OVA OVF PACS	Operating System Open Virtual Appliance or Application Open Virtualization Format Picture Archiving and Communication System
OS OVA OVF PACS PKCS	Operating System Open Virtual Appliance or Application Open Virtualization Format Picture Archiving and Communication System Public Key Cryptography Standards
OS OVA OVF PACS PKCS PKI	Operating System Open Virtual Appliance or Application Open Virtualization Format Picture Archiving and Communication System Public Key Cryptography Standards Public Key Infrastructure
OS OVA OVF PACS PKCS PKI QR Code	Operating System Open Virtual Appliance or Application Open Virtualization Format Picture Archiving and Communication System Public Key Cryptography Standards Public Key Infrastructure Quick Response Code
OS OVA OVF PACS PKCS PKI QR Code RAM	Operating System Open Virtual Appliance or Application Open Virtualization Format Picture Archiving and Communication System Public Key Cryptography Standards Public Key Infrastructure Quick Response Code Random Access Memory
OS OVA OVF PACS PKCS PKI QR Code RAM RIS	Operating System Open Virtual Appliance or Application Open Virtualization Format Picture Archiving and Communication System Public Key Cryptography Standards Public Key Infrastructure Quick Response Code Random Access Memory Radiology Information System

SMS	Short Message Service
SP	Special Publication
SQL	Structured Query Language
SSL/TLS	Secure Sockets Layer/Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol
UDM	Universal Data Manager
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VIP	Validation and ID Protection
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNA	Vendor Neutral Archive
WAN	Wide Area Network
WLM	Workload Management

## Appendix B References

- [1] Docker. Install Docker Desktop on Windows. Available: <u>https://docs.docker.com/docker-for-windows/install/</u>.
- [2] Microsoft Docs. Install SQL Server from the Installation Wizard (Setup). Available: <u>https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server-from-</u> <u>the-installation-wizard-setup?view=sql-server-2017.</u>
- [3] K. McKay and D. Cooper, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Revision 2, NIST, Gaithersburg, Md., Aug. 2019. Available: <u>https://doi.org/10.6028/NIST.SP.800-52r2</u>.
- [4] DVTk. DVTk open source project main contributors ICT Group and Philips. Available: <u>https://www.dvtk.org/.</u>
- [5] Microsoft TechNet. Building Your First Domain Controller on 2012 R2. Available: <u>https://social.technet.microsoft.com/wiki/contents/articles/22622.building-your-first-domain-controller-on-2012-r2.aspx.</u>
- [6] Microsoft TechNet. Installing and Configuring DHCP role on Windows Server 2012. Available: <u>https://blogs.technet.microsoft.com/teamdhcp/2012/08/31/installing-and-configuring-dhcp-role-on-windows-server-2012/.</u>
- [7] DigiCert. CSR Creation Instructions for Microsoft Servers. Available: <u>https://www.digicert.com/util/csr-creation-microsoft-servers-using-digicert-utility.htm.</u>
- [8] Cisco. Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide. Available: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/quick\_start/vmware/fmcv/FMCv-quick.html.</u>
- [9] Cisco. Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide. Available: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/quick\_start/vmware/ftdv/ftdv-vmware-gsg.html.</u>
- [10] Cisco Systems, Inc. Basic Policy Creation for Firepower. Jan. 30, 2019. Available: <u>https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/Basic Policy Creation on Cisco Firepower Devices.pdf</u>.
- [11] Cisco Systems, Inc. *Cisco Stealthwatch: Installation and Configuration Guide* 7.0. 2019. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system\_installation\_config uration/SW 7\_0\_0\_Installation\_and\_Configuration\_Guide\_DV\_3\_1.pdf.

- [12] G. O'Brien et al., Securing Wireless Infusion Pumps in Healthcare Delivery Organizations, NIST SP 1800-8, NIST, Gaithersburg, Md., Aug. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf.
- [13] Microsoft. Storage Account Overview. Available: <u>https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview?toc=/azure/storage/blobs/toc.json</u>.
- [14] TDi Technologies, External Authentication libraries, ConsoleWorks Cybersecurity Operations Platform. Available: <u>https://support.tditechnologies.com/content/external-authentication-libraries</u>.