# **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

September 2019

DRAFT

This publication is available free of charge from <a href="https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs">https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs</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, 236 pages, (September 2019), CODEN: NSPUE2

# **FEEDBACK**

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

Comments on this publication may be submitted to: <u>hit\_nccoe@nist.gov</u>.

Public comment period: September 16, 2019 through November 18, 2019

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: nccoe@nist.gov

# **1 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

- 2 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards
- 3 and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and
- 4 academic institutions work together to address businesses' most pressing cybersecurity issues. This
- 5 public-private partnership enables the creation of practical cybersecurity solutions for specific
- 6 industries, as well as for broad, cross-sector technology challenges. Through consortia under
- 7 Cooperative Research and Development Agreements (CRADAs), including technology partners—from
- 8 Fortune 50 market leaders to smaller companies specializing in information technology security—the
- 9 NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity
- 10 solutions using commercially available technology. The NCCoE documents these example solutions in
- 11 the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework
- 12 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,
- 14 Maryland.

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

# 17 NIST CYBERSECURITY PRACTICE GUIDES

- 18 NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity
- 19 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
- 21 security community how to implement example solutions that help them align more easily with relevant
- standards and best practices, and provide users with the materials lists, configuration files, and other
- 23 information they need to implement a similar approach.
- 24 The documents in this series describe example implementations of cybersecurity practices that
- 25 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
- 26 or mandatory practices, nor do they carry statutory authority.

# 27 ABSTRACT

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

- 34 PACS fits within a highly complex healthcare delivery organization (HDO) environment that involves
- 35 interfacing with a range of interconnected systems. PACS may connect with clinical information systems
- 36 and medical devices and may involve engaging with health professionals who may be both internal and
- 37 external to the HDO. This complexity may introduce or expose opportunities that allow malicious actors
- to compromise the confidentiality, integrity, and availability of the PACS ecosystem.
- 39 The NCCoE at NIST analyzed risk factors regarding the PACS ecosystem by using a risk assessment based
- 40 on the NIST Risk Management Framework, and the NCCoE leveraged the NIST Cybersecurity Framework
- 41 and other relevant standards to identify measures to safeguard the ecosystem. The NCCoE developed an
- 42 example implementation that demonstrates how HDOs can use standards-based, commercially available
- 43 cybersecurity technologies to better protect the PACS ecosystem. This practice guide will help HDOs
- 44 implement current cybersecurity standards and best practices, to reduce their cybersecurity risk while
- 45 maintaining the performance and usability of PACS.

### 46 **KEYWORDS**

- 47 Access control; auditing; authentication; authorization; behavioral analytics; DICOM; encryption
- 48 *microsegmentation; multifactor authentication; PACS; picture archiving and communication system;*
- 49 PAM; privileged account management; vendor neutral archive; VNA.

# 50 ACKNOWLEDGMENTS

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

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

Name	Organization
Andy Gray	Forescout
Katherine Gronberg	Forescout
William Canter	Hyland
Kevin Dietz	Hyland
David Alfonso	Philips Healthcare
Jonathan Bagnall	Philips Healthcare
Julian Castro	Philips Healthcare
Sukanta Das	Philips Healthcare
Jason Dupuis	Philips Healthcare
Michael McNeil	Philips Healthcare
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

Name	Organization
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
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

- 52 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
- 54 components were invited to sign a Cooperative Research and Development Agreement (CRADA) with
- 55 NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
<u>Cisco</u>	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
Philips Healthcare	Philips Enterprise Imaging Domain Controller Philips Enterprise Imaging IntelliSpace PACS Philips Enterprise Imaging Universal Data Manager
<u>Symantec</u>	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
TDi Technologies	TDI Technologies ConsoleWorks Version 5.1-0u1
Tempered Networks	Tempered Networks Identity Defined Networking (IDN) Conductor and HIPSwitch Version 2.1
<u>Tripwire</u>	Tripwire Enterprise Version 8.7
<u>Virta Labs</u>	BlueFlow Version 2.6.4
Zingbox	Zingbox IoT Guardian

# 56 **Contents**

57	1	Intr	oduct	ion	1
58		1.1	Practic	e Guide Structure	1
59		1.2	Build C	Dverview	2
60		1.3	Туроді	raphic Conventions	3
61		1.4	Logica	I Architecture Summary	4
62	2	Pro	duct lı	nstallation Guides	4
63		2.1	Picture	e Archiving and Communication System (PACS)	5
64			2.1.1	Philips IntelliSpace PACS	5
65			2.1.2	DCM4CHEE	20
66		2.2	VNA		
67			2.2.1	Hyland Database Server	
68			2.2.2	Hyland Acuo VNA	
69			2.2.3	PACSgear Core Server	
70			2.2.4	Hyland NilRead	42
71		2.3	Secure	PICOM Communication Between PACS and VNA	
72			2.3.1	Public Key Infrastructure (PKI) Certificate Creation	46
73			2.3.2	PKI Certification Installation	48
74			2.3.3	TLS Secure DICOM Configuration	52
75			2.3.4	PACS and VNA TLS Integration Tests	
76		2.4	Modal	ities	60
77			2.4.1	DVTk Modality Emulator	60
78			2.4.2	DVTk RIS Emulator	65
79		2.5	Asset &	& Risk Management	67
80			2.5.1	Virta Labs BlueFlow	67
81			2.5.2	Tripwire Enterprise	74
82		2.6	Enterp	rise Domain Identity Management	
83			2.6.1	Domain Controller with AD, DNS, & DHCP	
84			2.6.2	DigiCert PKI	120

85	2.7	Netwo	ork Control & Security	127
86		2.7.1	Cisco Firepower	127
87		2.7.2	Cisco Stealthwatch	152
88		2.7.3	Tempered Networks Identity Defined Networking (IDN)	165
89		2.7.4	Zingbox IoT Guardian	171
90		2.7.5	Forescout CounterACT 8	178
91		2.7.6	Symantec Endpoint Detection and Response (EDR)	185
92	2.8	Endpo	pint Protection & Security	192
93		2.8.1	Symantec Data Center Security: Server Advanced (DCS:SA)	192
94		2.8.2	Symantec Endpoint Protection	205
95	2.9	Data S	Security	217
96	2.10	Secur	e Remote Access	218
97		2.10.1	TDi Technologies ConsoleWorks	218
98		2.10.2	Symantec Validation and ID Protection (VIP)	220
99	Append	A xib	List of Acronyms	
100	Append	dix B	References	

# 101 List of Figures

102	Figure 1-1 PACS Final Architecture	4
103	Figure 2-1 Hyland Systems and Applications Connectivity	0
104	Figure 2-2 Architecture of Networks IDN	6

# 105 List of Tables

106	Table 2-1 Base VM Configuration	Requirements	5	)
-----	---------------------------------	--------------	---	---

# 107 **1 Introduction**

- 108 The following volumes of this guide show information technology (IT) professionals and security
- 109 engineers how we implemented this example solution. We cover all of the products employed in this
- 110 reference design. We do not recreate the product manufacturers' documentation, which is presumed to
- be widely available. Rather, these volumes show how we incorporated the products together in our
- 112 environment.
- 113 Note: These are not comprehensive tutorials. There are many possible service and security configurations 114 for these products that are out of scope for this reference design.

# 115 **1.1 Practice Guide Structure**

- 116 This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a
- 117 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

- 119 (NCCoE) lab. This reference design is modular and can be deployed in whole or in part.
- 120 This guide contains three volumes:
- 121 NIST SP 1800-24A: Executive Summary
- 122 NIST SP 1800-24B: Approach, Architecture, and Security Characteristics what we built and why
- 123 NIST SP 1800-24C: *How-To Guides* instructions for building the example solution (you are here)
- 124 Depending on your role in your organization, you might use this guide in different ways:
- 125 **Business decision makers, including chief security and technology officers,** will be interested in the
- 126 *Executive Summary,* NIST SP 1800-24A, which describes the following topics:
- 127 challenges that enterprises face in securing the picture archiving and communication system (PACS)
- 128 example solution built at the NCCoE
- 129 benefits of adopting the example solution
- 130 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
- 132 following sections will be of particular interest:
- 133 Section 3.4, Risk Assessment, describes the risk analysis we performed.
- 134 Section 3.5, Security Control Map, maps the security characteristics of this example solution to
- 135 cybersecurity standards and best practices.

136 You might share the *Executive Summary*, NIST SP 1800-24A, with your leadership team members to help

- 137 them understand the importance of adopting standards-based, commercially available technologies that
- 138 can help secure the PACS ecosystem.
- 139 **IT professionals** who want to implement an approach like this will find this whole practice guide useful.
- 140 You can use this How-To portion of the guide, NIST SP 1800-24C, to replicate all or parts of the build
- 141 created in our lab. This How-To portion of the guide provides specific product installation, configuration,
- 142 and integration instructions for implementing the example solution. We do not recreate the product
- 143 manufacturers' documentation, which is generally widely available. Rather, we show how we
- 144 incorporated the products together in our environment to create an example solution.
- 145 This guide assumes that IT professionals have experience implementing security products within the
- 146 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
- 147 not endorse these particular products. Your organization can adopt this solution or one that adheres to
- 148 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
- parts of PACS security solution. Your organization's security experts should identify the products that
- 150 will best integrate with your existing tools and IT system infrastructure. We hope that you will seek
- 151 products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists
- 152 the products that we used and maps them to the cybersecurity controls provided by this reference
- 153 solution.
- A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a
- draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
- 156 success stories will improve subsequent versions of this guide. Please contribute your thoughts to
- 157 <u>hit\_nccoe@nist.gov</u>.
- 158 Acronyms used in figures can be found in <u>Appendix A</u>.

# 159 1.2 Build Overview

- 160 The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively 161 demonstrate the capabilities in securing the PACS ecosystem. While the project implemented PACS and 162 vendor neutral archive (VNA) solutions, as well as implemented security controls, the environment 163 leverages modality emulation to simulate medical image acquisition. The project also implemented an 164 emulated radiology information system (RIS), used to generate modality work lists and therefore 165 support common medical imaging workflows. The project then applied security controls to the lab 166 environment. Refer to NIST SP 1800-24B, *Approach, Architecture, and Security Characteristics,* for an
- 167 explanation of why we used each technology.

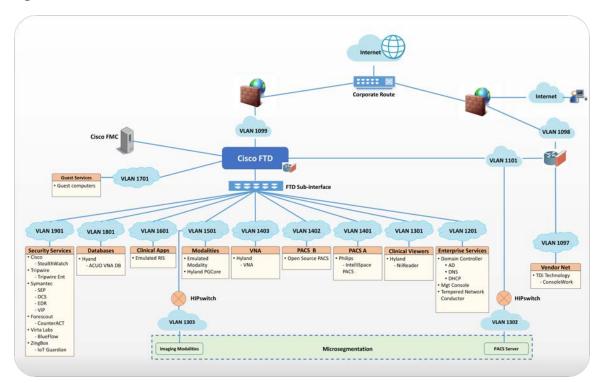
# 168 **1.3 Typographic Conventions**

169 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 https://www.nccoe.nist.gov.

# 170 1.4 Logical Architecture Summary

Figure 1-1 depicts a reference network architecture, introduced in NIST SP 1800-24B, Section 4.2, Final 171 172 Architecture, which performs groupings that would translate to network segments or zones. The rationale behind segmentation and zoning is to limit trust between areas of the network. In considering 173 a hospital infrastructure, the NCCoE identified devices and usage and grouped them by usage. The 174 175 grouping facilitated identification of network zones. Once zones are defined, infrastructure components may be configured so that those zones do not inherently have network access to other zones within the 176 177 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 178 179 overall defense-in-depth strategy.



#### 180 Figure 1-1 PACS Final Architecture

# **181 2 Product Installation Guides**

182 This section of the practice guide contains detailed instructions for installing and configuring the 183 products that the NCCoE used to build an instance of the example solution.

184 The project implemented security capabilities across the laboratory infrastructure, to safeguard the

185 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.

# 188 2.1 Picture Archiving and Communication System (PACS)

189 This project implemented two separate PACS: Philips IntelliSpace solution and an open source PACS

190 (DCM4CHEE). These PACS systems are used to emulate the case where healthcare delivery organizations

191 (HDOs) may have different PACS vendors installed in their environment.

# 192 2.1.1 Philips IntelliSpace PACS

193 The project implements the Philips IntelliSpace PACS solution as a central component to the lab build.

194 IntelliSpace includes several common features, such as the ability to integrate digital imaging and

195 communication in medicine (DICOM) and non-DICOM images and provides the project team the ability

196 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

198 working HDO environments. The project integrates IntelliSpace with the Hyland VNA solution also

installed in the lab.

### 200 System Requirements

- 201 Philips IntelliSpace system consists of several components installed on different VMware virtual
- 202 machines (VMs). Base configuration requirements to construct the IntelliSpace VMs are depicted in
- 203 Table 2-1.

VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
DC1	Domain Controller	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	4	8 GB RAM	200 GB	Microsoft Windows Server 2012	Microsoft SQL 2012, IIS 7

204 Table 2-1 Base VM Configuration Requirements

VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
	(DB), Anywhere Viewer (web client)					
UDM	Universal Data Manager (UDM), WEB DICOM services Image Lifecycle Management Image pre fetching from VNA	4	8 GB RAM	200 GB	Microsoft Windows Server 2012	Microsoft SQL 2012, IIS 7

#### 205 IntelliSpace PACS Client Installation

206 The project team collaborated with a team of Philips Healthcare deployment engineers to install the

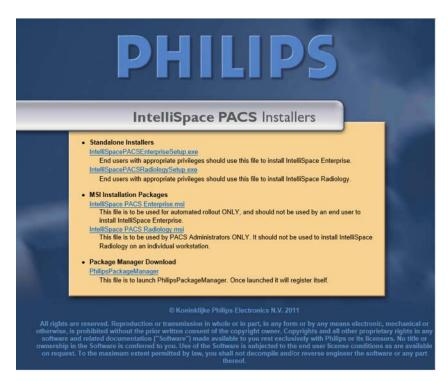
207 environment. Based on the base VM configuration requirements, the NCCoE team created the VMs by

208 using the open virtualization format (OVF) files provided by Philips Healthcare. Philips engineers

209 deployed the applications on the VMs and created instances for DC1, IntelliSpace server, and UDM, as

210 noted in Table 2-1. VM instances were deployed on respective servers.

- 211 IntelliSpace PACS is a web-based distributed system. Clinicians, referring physicians, nurses, or
- bioengineers use web-based client application on workstations to view, analyze, and qualify medical
- 213 images. Once the server components were installed, the web-based client installation was performed
- 214 using the following procedures:
- 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 URL: https://192.168.140.131/clientweb/installers.
- Select *InstelliSpacePACSEnterpriseSetup.exe* under the **Standalone Installers** bullet list of available
   IntelliSpace PACS Installers screen to start the installation.



An option to choose setup language appears. Select the English (United States) from the pull-down
 and click OK.



223

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

InstallShield Wizard	Preparing to Install
	IntelliSpace PACS Enterprise Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
	Extracting: IntelliSpace PACS Enterprise.msi
	$\mathbf{Y}$
	Cancel

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

Custom Setup Select the program features you wan	t installed.		22
Click on an icon in the list below to chan IntelliSpace PACS Enter IntelliSpace PACS IntelliSpace PACS Language-Specific Files PMS Integration Integration Tools	prise Web Control	Feature Description	
<	>	This feature requires your hard drive. It has subfeatures selected subfeatures require your hard drive.	as 1 of 1 I. The
Install to: C: \Program Files (x86) \Philips \IntelliSpac InstallShield	e PACS Enterprise \4.4	4	Change

228

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

Client Configuration I	nfo			
Please enter the Hos PACS Enterprise 4.4		Address of the server t will connect to.	r that the IntelliSpa	ce
	Server:	192.168.140.131		

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

🔀 IntelliSpace PACS Enterprise	e 4.4.553.20 - InstallShield Wizard	×
	InstallShield Wizard Completed	
	The InstallShield Wizard has successfully installe PACS Enterprise 4.4.553.20. Click Finish to exit	
	< Back Finish	Cancel

234

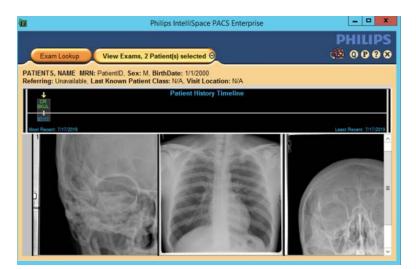
Once the installation is done, the installer places an IntelliSpace PACS Enterprise icon on the
 desktop. Type Tester in the User Name field and the corresponding password in the Password
 field, then click OK to log in.

Int	elliSpace PACS
	IntelliSpace PACS Enterprise Logon
User Name Password	
Log on to Logon Mode Location	Password

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

Shortcuts	Folder List X E Enterprise Tools	search F Exams with images	s only C Append results MRN	clear al
Patient Lookup	Patient Lookup	A Patients, Name     CR - No Descriptions	PatientID Acc: 123456	1/1/
	Couery     Couery     Couel Exam Cache     Couel Exams     Couel Exam Cache     Couel Exam Cachine Filters     My History     My History     My History     Coueues     My History     Statistics     My Filters     My Statistics     My Filters     My Filters     My Filters     My Filters     My Filters     My Filters     My History     My History	a 🚡 TST_Reiten, Michael	903-29-000-5C9E3870	12/1

- 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 shown below.



### 244 IntelliSpace PACS Client Configuration

245 Deployment and configuration were accomplished by Philips Deployment Engineers 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*.

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.

🧲 🔿 🏉 http	os://localhost/PACS	Administration/Authentication/Login.aspx	, Q
	Ρ	HILIPS 44.553.20	
	Intel	liSpace PACS AdminTool	
	Logon Mode	Logon admin 	

- 251 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 on Users and then click on **Add a New User**.

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

- To add a new user, navigate to SECURITY, found on the far-left column of the Common Tasks
   screen, and click on Users.
- a. Enter the User ID.
- 257 b. Enter the user's **First Name**.
- 258 c. Enter the user's **Middle Name** (optional).
- d. Enter the user's Last Name.
- 260 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.

#### 263 Configure Sources for User Authentication

- 264 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
- 266 internal authentication source, called iSite, implements a local database of users and groups.
- 267 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
- 269 following steps describe how to create an LDAP authentication source:
- 270 1. From the navigation bar, select the **Security** button and then click **Authorities**.

CS Administration	Name 🔺		Description	
	AD PACS			
Security	ISITE			
s				
ps				
s ies				
norities				
nizations				
tTrail				
dist Configuration				
ictionaries				
nfiguration				
		New Edi	Test Delete	
WorkLists				
Sessions				

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

tion General Informa	ition
Authority Name	•
Display Name:	
Description:	
Name Resolution:	
	✓ Enabled
	Show in Login Screen
on	
	Back Next Cancel

- 274 3. On the **External Authentication** source page, set the following values and then click **Next**.
- 275 Set Authority Name to AD.PACS.HCLAB
- 276 Set the **Display Name** to **AD PACS**
- 277 Select HostName for Name Resolution
- 278 Check the box next to **Enabled**

279 Check the box next to Show in Login Screen

ninistration Ge	neral Informa	tion			
	Authority Name	AD.PACS.HCLAB			_
rity	Display Name:	AD PACS			_
	Description:				_
Na	me Resolution:	HostName	~		
		☑ Enabled			
		Show in Login	Concer		
s		Show in Login	screen		
uration					
ries					1.1
mes					
tion					
ts			Back N	ext Cancel	
15					

- 280
- 4. In the Advanced Directory Configuration, set DNS Host Name as ad.pacs.hclab and Port as 389.

PHILIPS	Edit External Authentication Source	_
PACS Administration	Host Query Configuration	
	DNS Host Name: ad.pacs.hclab	
Security	Port: 389	
sers		
roups		
oles		
vlicies		
uthorities		
rganizations		
ıditTrail		
orklist Configuration		
Dictionaries		
Configuration		
configuration		
	Back Next Cancel	
WorkLists	Back Next Cancel	
Sessions		
Help		

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

	Configuration		-
Directory Type	ActiveDirectory	~	
Authentication	: Negotiate	~	
Search Root	t: DC=pacs, DC=hclab		-
Supporte	d Password		
Credentials	Certificates		
Referral Chasing	: None	V	
			1000
	Back	Save Cancel	

286 6. The interface provides a test feature to allow engineers to determine connectivity with the external
 287 authentication source. From the navigation bar, select the Security > Authorities. Click on the
 288 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	
Roles	Test Account
Policies Authorities	Username and Password
Organizations	User Name:
AuditTrail Worklist Configuration	Password:
Dictionaries	Test Cancel
Configuration	
WorkLists	
Sessions	
Help	

# 289

#### 290 Configure Connection to Modality Emulator

- 291 The open source DVTk Modality Emulator was used as a modality for testing the communication
- 292 between IntelliSpace PACS and a modality. The installation of the DVTk Modality Emulator can be found
- 293 in <u>Section 2.4.1</u>. Below are the configuration steps:

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

RK	Modality Emulator	×
File Help		
옷 🖀 😫 🛅 🍩 (수 🕇 🔿		
Control Activity Logging Configure	Emulator   Worklist Query   MPPS-Progress   MPPS-Disconti	inued   MPPS-Completed   Image Stora
System Name:	Modality	
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:	:1	
Listen Port	104	
Storage Commit Mode		
In Single Association (S)	nc 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 are needed. Particularly, the **AE Title** for the
 Philips IntelliSpace PACS is required for the **AE Title** field. These are the input values:

302	RIS System
303	IP Address: 192.168.160.201
304	Remote Port: 105
305	• AE Title: DVTK_RIS
306	MPPS Manager
307	IP Address: 192.168.160.201
308	Remote Port: 108
309	• AE Title: DVTK_MPPS
310	PACS/Workstation Systems–Storage Config
311	IP Address: 192.168.140.131

- **312 Remote Port:** 104
- 313 AE Title: STENTOR\_SCP
- 314 PACS/Workstation Systems–Storage Commit Config
- 315 IP Address: 192.168.140.131
- **316 Remote Port:** 104
  - AE Title: STENTOR\_SCU

X		Modality Emulator		
File Help				
r 🖬 😫 🛅	● ← ↑ →			
Control Activity L	ogging 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			Store Commit C	onfia
IP Address:	192.168.140.131		IP Address:	192.168.140.131
Remote Port:	104		Remote Port	104
AE Title:	STENTOR_SCP		AE Title:	STENTOR_SCU

- To configure the Philips IntelliSpace PACS AE Title and communication port, log on to the iSite
   Administration web site 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.
- 322 Normal AE Title: STENTOR\_SCP
- 323 High-Priority AE Title: STENTOR\_HI
- **324 Port:** 104
- **Secure Port:** 2762

← ⊕ 🧭 https://localhost/iSiteWeb/M	ain/Navigator.aspx	<del>،</del> م	🖴 C 🧭 Philips PACS Administration L
Configure View Test			
General Storage Tasks SLogs SystemCheck	CRefresh DB Cache CRestart DMWL CR	estart All	
🗄 System	General IExport Q/R SCP	IQuery S/C SCP	Import/Exp. Conformance
Main Location     Intervense ImageDistribution + neccess1	DICOM Support		
	Normal A ETRie	STENTOR_SCP	Default
	High Priority A ETitle	STENTOR_H	Default
	Port	104	Default
	Secure Port	2762	Default
	Replace Non Latin-1 During Import	Enable	Default
	Enable/Disable Export on DICOM     Advanced  Asset to Detauts Canol/Refe		

- 327 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 328
- 329 the success of the pings. You should receive Ping Successful and DICOM Echo Successful messages.

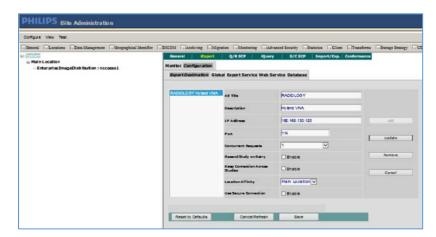
ulator   Worklist Query   MPPS-Prog		Completed   Image Stora 🗸 🕨
ulator   Worklist Query   MPPS-Prog		Completed   Image Stora 🔸   🕨
ulator   Worklist Query   MPPS-Prog		Completed   Image Stora 💶 🕨
<b>#</b> 2	10000	
	Ping RIS	
→ 🖗	DICOM Echo	
	Request Worklist	
	Send MPPS completed	
RIS System	Hint:	
1 100		
	Ping PACS/Workstation	Ping successful.
→ 🌳	DICOM Echo	DICOM Echo successful.
	Store Image	
	Storage Commitment	
PACS/Workstation	Hint	
	RIS System	RIS System Request Worklist Send MPPS completed Hint: Ping PACS/Workstation DICOM Echo Store Image Storage Commitment

330

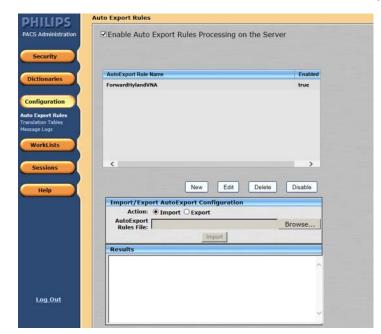
#### 331 Configure IntelliSpace PACS to Communicate with Hyland VNA

- 332 Refer to <u>Section 2.2.2</u> for detailed installation guidance for Hyland VNA.
- 333 1. Obtain the Hyland VNA AE Title and port information for communication. Log in to the iSite 334
  - 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.
- 336 3. Fill in the known Hyland AE Title (e.g., RADIOLOGY), IP Address (e.g., 192.168.130.120), Port (e.g.,
- 337 114), and other necessary information.



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



# 343

344 7. Set the **Trip Type** as **New Data Arrival**.

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

HILIPS	Edit AutoExport Rule
CS Administration	AutoExportRule Configuration
	Rule Name ForwardHylandVNA
Security	Trigger Type New Data Arrival
	Enable Priors
Dictionaries	Prior Criteria 🗌 Modality 🗌 BodyPart
	No. Of Priors 3 V
onfiguration	
	Matching Criteria
o Export Rules Islation Tables	Modality type
sage Logs	Manufacturer Name
WorkLists	Sending AE title
Sessions	Receiving AE title STENTOR_SCP
	Study description
Help	
	Manufacturer model
	Referring physician's first name
	Referring physician's last name
	Reading physician's first name
	Reading physician's last name
	Requested Procedure
	Description
	Study Date and Time
Log Out	
	Body Part
	Protocol Name
	Series Description
	Series Description
	Configured Export Destinations Selected Destinations
	Hyland VNA (RADIOLOGY)
	>>
	<<
	Save Cancel

# 348 2.1.2 DCM4CHEE

349 DCM4CHEE is a collection of open source applications that communicate with each other using DICOM
 350 and HL7 standards for clinical-image management and archiving. In this study, DCM4CHEE has JBoss and
 351 a web-based graphical user interface (GUI) application built in. JBoss is used to configure DCM4CHEE to

- 352 communicate with DVTk's Modality Emulator to store images in a PostgreSQL database. The JBoss web
- 353 interface allows an administrator to configure DCM4CHEE to listen for connection requests from specific
- application entities like DVTk's Modality Emulator. DCM4CHEE also has web-based GUI that displays
- 355 patient records sent from the Modality Emulator and stored in the PostgreSQL database.
- A 32-bit version of Java JDK6 [1], JBoss v4.2.3 [2], and PostgreSQL database v 9.4.23 [3], [4] were
- 357 installed as the prerequisites for the DCM4CHEE. Refer to each installation guide for the installation
- 358 procedures.
- 359 System Requirements
- 360 **CPU:** 4
- 361 Memory: 512 megabyte (MB) RAM
- 362 Storage: 200 MB
- 363 **Operating System:** Microsoft Windows Server 2016 Datacenter
- 364 Network Adapter: Virtual Local Area Network (VLAN) 1402

#### 365 DCM4CHEE Installation

- 366 The installation guide can be found at [5].
- 1. Go to <u>https://www.dcm4che.org</u> to download the software.
- 368 2. In the left-hand side of the page, click the **Wiki** link under Community.
- Click the here link under Download Latest Version nest to dcm4chee DICOM Archive 2 (includes
   dcm4che toolkit 1.4) [6] link on the right-hand side of the screen.
- 4. On the new web page, click **2.17.1** to download that version of DCM4CHEE.

#### 372 DCM4CHEE Audit Report Repository Installation

- 373 Download the file relevant to PostgreSQL from the SourceForge site [7]. Once downloaded, go to the
- 374 *dcm4chee-2.17.1-psql\bin* directory by using a command prompt, and execute this command:
- 375 Install\_arr.bat <path to the audit report file>.

#### 376 Test the DCM4CHEE Installation

- Go to *dcm4chee-2.17.1-psql\bin* directory by using a command prompt and run this command:
   Run.bat.
- 2. Successful run will produce this output:

Administrator: Command Prompt - run.bat	_		>
at org.jboss.aspects.tx.TxPolicy.invokeInCallerTx(TxPolicy.java:126)			
at org.jboss.aspects.tx.TxInterceptor\$Required.invoke(TxInterceptor.java:195)			
at org.jboss.aop.joinpoint.MethodInvocation.invokeNext(MethodInvocation.java:101)			
at org.jboss.ejb3.stateless.StatelessInstanceInterceptor.invoke(StatelessInstanceIntercepto	r.java:62)		
at org.jboss.aop.joinpoint.MethodInvocation.invokeNext(MethodInvocation.java:101)			
at org.jboss.ejb3.mdb.MessagingContainer.localInvoke(MessagingContainer.java:249)			
at org.jboss.ejb3.mdb.inflow.MessageInflowLocalProxy.delivery(MessageInflowLocalProxy.java:			
at org.jboss.ejb3.mdb.inflow.MessageInflowLocalProxy.invoke(MessageInflowLocalProxy.java:13	3)		
at com.sun.proxy.\$Proxy326.onMessage(Unknown Source)			
at org.jboss.resource.adapter.jms.inflow.JmsServerSession.onMessage(JmsServerSession.java:1			
at org.jboss.jms.client.container.ClientConsumer.callOnMessageStatic(ClientConsumer.java:16	3)		
at org.jboss.jms.client.container.SessionAspect.handleRun(SessionAspect.java:831)			
at org.jboss.aop.advice.org.jboss.jms.client.container.SessionAspect14.invoke(SessionAspect			
at org.jboss.jms.client.delegate.ClientSessionDelegate\$run_N8003352271541955702.invokeNext(0	ClientSessi	onDele	gat
ın_N8003352271541955702.java)			
at org.jboss.jms.client.container.ClosedInterceptor.invoke(ClosedInterceptor.java:170)			
at org.jboss.aop.advice.PerInstanceInterceptor.invoke(PerInstanceInterceptor.java:105)			
at org.jboss.jms.client.delegate.ClientSessionDelegate\$run_N8003352271541955702.invokeNext(	ClientSessi	onpere	gat
ın_N8003352271541955702.java)			
at org.jboss.jms.client.delegate.ClientSessionDelegate.run(ClientSessionDelegate.java)			
at org.jboss.jms.client.JBossSession.run(JBossSession.java:199)			
at org.jboss.resource.adapter.jms.inflow.JmsServerSession.run(JmsServerSession.java:237)			
at org.jboss.resource.work.WorkWrapper.execute(WorkWrapper.java:204) at org.jboss.util.threadpool.BasicTaskWrapper.run(BasicTaskWrapper.java:275)			
at EDU.oswego.cs.dl.util.concurrent.PooledExecutor\$Worker.run(PooledExecutor.java:2756)			
at java.lang.Thread.run(Unknown Source)			
35:24,470 INFO [FileSystemMgt2Service] Check file system group ONLINE STORAGE for deletion of o	anhanad ani	wata f	11
ss.24,470 into [Filesystemmigtzservice] thete file system group owline_stockade for deletion of o	-phaned pri	часе т.	116
35:24,470 INFO [FileSystemMgt2Service] Check file system group LOSSY STORAGE for deletion of or	hanod nniv	ato fi	1.01
55.24,470 Into [TILESysteming(25ervice] check Tile System group Lossy_StokAde Tor detection of or	phaned priv	ace II.	Les

#### 381 **DCM4CHEE Configuration Using the JMX Console**

- 382 1. Access the JMX Console GUI by navigating to http://localhost:8080/jmx-console/ and providing the following credentials: 383
- 384 Username: admin
- Password: \*\*\*\*\* 385
- 2. Click the link group=ONLINE\_STORAGE, service=FileSystemMgt under the dcmrchee.archive 386 387 heading.

#### dcm4chee.archive

- group=LOSSY\_STORAGE.service=FileSystemMgt
   group=NEARLINE\_STORAGE.service=FileSystemMgt
- group=ONLINE\_STORAGE,service=FileSystemMgt name=AttributesModificationScu,service=Queue
- 389 3. Click the Invoke button under the addRWFileSystem() section to instantiate where archived data 390 should be stored. If no specific file path is provided as a parameter, the default location is
- dcm4chee-2.7.1-psql\server\default\archive. 391

org.d	cm4chex.archive.e	jb.interfaces.FileSys	temDTO addRWFileSys	tem()
Add R	W file system to the	file system group man	aged by this service. The	file system is also linked to existing other file systems of the group.
Para	m ParamType	ParamValue	ParamDescription	
dirPa	th java.lang.String		Directory/Mount Point	
Invol	e			

392

388

380

393 4. Change the default AE Title:

395		b. Change the title by clicking the <b>service=AE</b> link under dcm4chee.archive heading.
396		<u>name=WadoPrefetch,service=Queue</u> <u>service=AE</u> <u>service=AttributesModificationScp</u>
397	5.	nder the <b>updateAETitle</b> section, provide the <b>default AETitle</b> and <b>new AETitle</b> as parameters, and
398		ick the <b>Invoke</b> button on the bottom left-hand side of the table.
		<b>Did updateAETitle()</b> Ddate specified AE Title to new value in AE Configuration and in all service attrib E Title of these file systems is updated to the new value as the Retrieve AE Title
		Param ParamType ParamValue ParamDescription
		revAET java.lang.String AE Title to update.

a. The default AE Title is DCM4CHEE.

399

394

400 6. You can also change the port number that DCM4CHEE uses. Default port numbers are **104** and
401 **11112.** Port **11112** was used for communicating with DVTk Modality Emulator.

PortNumbers	java,lang.String	RW	104,11112	Port numbers for AE auto configuration. The method getAE(title, hostname) use this list to find a DICOM service hosted by hostname. 'NONE' will disable auto AE configuration!
-------------	------------------	----	-----------	--

new AE Title.

402

408

#### 403 DVTk Modality to DCM4CHEE Configuration

newAET java.lang.String

Invoke

- Open a web browser to access *http://localhost:8080/dcm4chee-web3/* and provide the following
   credentials:
- 406 Username: admin
- 407 Password: \*\*\*\*\*

Username:	admin
Deserved	
Password:	
	Sign in Reset

AEs	AE Groups					_
O New AET	Filter by:	~				
VINEW AET	Filter by.					
Title	Туре	Host	Port	Description	TLS	MPPS
CDRECORD		localhost	10104	Media Creation Server (part of dcm4chee)	10	
DCMRCV		localhost	11112			
DVTK_Modality	-	192.168.150.160	124	DVTk Modality Emulator		
RADIOLOGY	-	192.168.130.120	114	Acuo VNA		

409 2. Click the **Application Entities** tab in the ribbon on the top of the screen.

413 • **Title**: PACS

information:

410 411

- 414
   Type: 

   415
   Hostname: 192.168.141.206

   416
   Port: 11112

   417
   User Id: Admin

   418
   Password: \*\*\*\*\*
- 419 4. Click the **Save** button at the bottom center of the screen.

Edit A	ET
Title:	PACS
Type:	<b>~</b>
Hostname:	192.168.141.206
Port:	11112
Ciphersuite #1:	- ~
Ciphersuite #2:	
Ciphersuite #3:	- v
Description:	
Issuer of Patient ID:	
Issuer of Accession Number:	
Filesystem Group ID:	
Wado URL:	
User Id:	admin
Password:	•••••
Station Name:	
Institution:	
Department:	
Installed:	
Emulate MPPS:	
Delay time for MPPS emulation:	
Save Canc	el Echo

### 421 View Stored Data

- 422 1. Click the **Folder** tab located on the top ribbon of the page on the left-hand side of the screen.
- 423 2. Click the Search button on the right-hand side of the screen above the buttons Delete, Move, and
  424 Export.
- 425 3. No parameters are needed if you want to see all documents stored.

Lolder Irash Applicat	tion Entities Modality Worklist	Teaching-Files Dashb	oard Roles S	isers Password	Los	20ut (admin)	Choose One 🐱	ds	m4che.org
Search									9
Patient Name Potient Name Phonetic Modality Source AET	Patient ID ID	Issuer	Study Date from	2	to		Accessi	on No	
Exact search					Search for Study	- Expand To a	uto 🤍 🔵 Re	set	Search
pesize 10 v Study 1 to 1 of 1							🧊 Delete 🗍 🔚	Move	expo
Show column titles Patient Name	Patient ID/Issuer	Birth Date	Sex	Comments					
		Accession No	Modality	Description	#5/#I	Availability			
Study Date/Time Patients^Name	Study ID PatientID	1/1/2000	н	Carcipitos			15	13	

### 427 DCM4CHEE to DVTk Modality Configuration

428 429 430	1. 2.	In the Modality Emulator, click the <b>Configure Remote Systems</b> tab at the top of the window. Navigate to the <b>PACS/Workstation Systems</b> section and input the information with the followin values:							
431		RIS System							
432		IP Address: 192.168.160.201							
433		Remote Port: 105							
434		• AE Title: RIS							
435		MPPS Manager							
436		IP Address: 192.168.160.201							
437		Remote Port: 106							
438		AE Title: MPPS							
439		PACS/Workstation Systems–Storage Config							
440		IP Address: 192.168.141.206							
441		Remote Port: 11112							
442		• AE Title: PACS							
443		PACS/Workstation Systems–Storage Commit Config							
444		IP Address: 192.168.141.206							
445		Remote Port: 11112							
446		AE Title: PACS							

Modality Em	ulator		-		>
ile Help		 			
Control Configur	re Remote Systems				
RIS System					
IP Address:	192.168.160.201				
Remote Port:	105				
AE Title:	RIS				
MPPS Manager					
IP Address:	192.168.160.201				
Remote Port:	106				
AE Title:	MPPS				
PACS/Workstat		Store Commit C	Config		_
IP Address:	192.168.141.206	IP Address:	192.168.14	1.206	
Remote Port:	11112	Remote Port:	11112		
AE Title:	PACS	AE Title:	PACS		

#### 448 Oviyam Installation

- 449 Once downloaded from the SourceForge [8] and unzipped, copy the *oviyam.war* file to the following
- directory: *dcm4chee-2.7.1\server\default\deploy.* Check if you successfully installed the software by
- 451 visiting *http://dcm4chee\_ip:8080/oviyam2* and accessing a log in screen.

#### 452 Oviyam Configuration

- 453 1. Using a browser, navigate to *http://dcm4chee\_ip:8080/oviyam2* and provide the following
  454 credentials:
- 455 Username: admin

456

Password: \*\*\*\*\*

Oviyam 2	
DICOM Web Workstation - Version 2.7.2	
User Name*	
admin	
Password	
Remember Me	

		Oviyar	Today CT.	admin 🙆 🗲 Settings
459				C Logout
460	3.	Unde	r the <b>Server</b> tab, click <b>Add</b> .	
461		Oviyal Version 2 Server Venth Server	Query Param     Preferences       /     Add     Edit     Delete	
462 463	4.		the PACS server parameters and click the <b>Save</b> button located to the far right of the neters.	е
464			Description: PACS	
465			AE Title: DCM4CHEE	
466			Host Name: localhost	
467			Port: 11112	
468			Retrieve Type: WADO	
469			WADO Context: wado	
470			WADO Port: 8080	
471			Image Type: JPEG	
		Oviyam Versites 2.7 Server Verity Server	2 Guery Param Preferences Add Edit Delete	

458 2. Navigate to the top right corner of the screen, click **admin**, and then click **Settings**.

- 472
- 5. Return to *http://dcm4chee\_ip:8080/oviyam2* to see query parameters now available.

No data available in table

8080 JPEG ~

.

474 6. Click the **Search** button under the parameters on the right-hand side of the screen.

PACS JCM4CHEE localhost 11112 WADO v wado

- Study Description Bludy Cesolistion Referring Physician Petering Physician Modelity ALL 0
- 475

476 7. Double-click on a patient record.

ACS								
atient ID	Patient ID	Patient Name	Patient Name	Study Date (From)	DDIMMYYYY		DO-MM/YYYY	
tudy Description	Study Description	Referring Physicia	Referring Physician	Modality		Search	Reset	
Display 10	<ul> <li>records per page</li> </ul>					Fit	ter:	
o Patie	entiD	Patients Name	м	27/06/2019 10:15	StudyDescription		CR	15

478 8. View images related to that patient record.



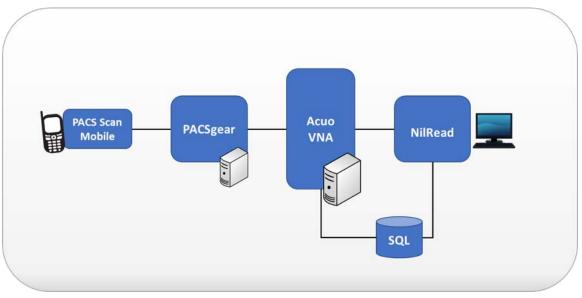
479

# 480 **2.2 VNA**

- 481 Hyland Acuo VNA features several different systems and applications, which include:
- 482 Acuo VNA: core application server with services used to store, track, and retrieve digital assets stored in
   483 an archive
- 484 PACSgear Core Server: image processing and routing server, and back-end services
- 485 **PACS Scan Mobile/Web:** mobile device image acquisition and file-import application
- 486 NilRead: enterprise image-viewing application

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





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

# 492 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:

- 495 System Requirements
- 496 **CPU:** 4

- 497 Memory: 12 GB RAM
- 498 Storage:
- 499 Hard Drive (HD)1: 80 GB (Operating System Install)
- 500 HD 2: 20 GB (DB Drives)
- 501 HD 3: 10 GB (Tx Logs)
- 502 **Operating System:** Microsoft Windows Server 2016
- 503 Network Adapter: VLAN 1801
- 504 Hyland Database Server Installation

505 Install the SQL Server 2017 according to the instructions detailed in *Install SQL Server from the* 506 *Installation Wizard (Setup)* [9].

### 507 Hyland Database Configuration

- 5081. The installation creates default service accounts for each service. The project maintained use of509these default service accounts. User and privileged log in accounts were created for the Hyland
- 510 application suite and linked to unique Microsoft domain users. The project created the
- 511 PACS\AcuoServiceUser and PACS\Administrator accounts.
- 512 2. The project implemented Windows Authentication Mode for the SQL Server.
- Application database instances were created as needed automatically when product applicationswere installed.
- This project implemented the following database instances through the SQL Server Management
   Studio: AcuoMed, HUBDB, NILDB, and PGCORE.
- 5. The project also implemented instances for OPHTHALMOLOGY, RADIOLOGY, and WOUND\_CARE.

# 518 2.2.2 Hyland Acuo VNA

- 519 Hyland Acuo VNA provides access to medical images and documents through interactions with a variety 520 of different PACS, modalities, and image viewers. Acuo VNA also supports various standards, including
- 521 HL7 and DICOM. The installation and configuration procedures can be found below.

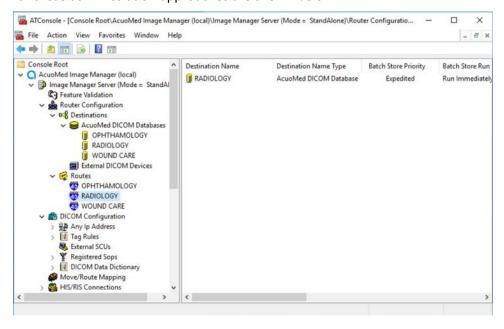
### 522 System Requirements

- 523 **CPU:** 6
- 524 Memory: 12 GB RAM
- 525 Storage:
- 526 HD 1: 80 GB (OS Install)
- 527 HD 2: 80 GB (Dilib Cache Drive)
- 528 HD 3: 500 GB (Image Cache Drive)
- 529 **Operating System:** Microsoft Windows Server 2016
- 530 Network Adapter: VLAN 1301
- 531 Hyland Acuo VNA Installation
- In the NCCoE test environment, the Hyland Acuo VNA was installed on a VM preconfigured with the
   OS and network requirements provided by Hyland. The project leveraged engineers supplied by
   Hyland to perform the installation.

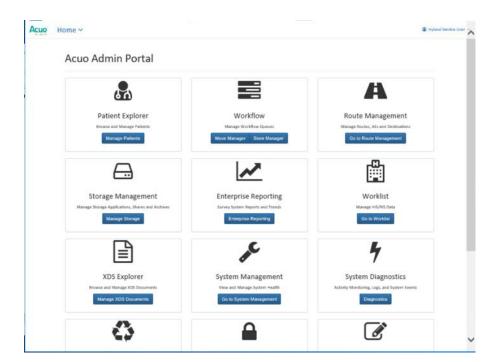
- 535 2. Upon completion of the installation, three Windows services were created: AcuoMed, AcuoAudit,
- and AcuoStore. AcuoMed is associated with a DICOM database containing the patient, study, and
- 537 series record information that describes the images physically present on the Acuo VNA archive
- 538 system. The AcuoStore also has its own database for storing information related to the bulk storage
- of digital images and related data, including information about the shares and about the applicationsthat use those shares.
- 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.

## 544 Hyland Acuo VNA Configuration

- 545 Hyland engineers performed configurations using the **Microsoft MMC** console and the **AcuoAdmin**
- 546 **Portal** (*https://192.168.130.120:8099/vnaweb/#1/home*). The screenshots of the console management 547 for these administration approaches are shown below:



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



# 553 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.

### 558 System Requirements

- 559 **CPU:** 4
- 560 Memory: 8 GB RAM
- 561 Storage:
- 562 HD 1: 80 GB (OS Install)
- 563 HD 2: 170 GB (Application)
- 564 **Operating System:** Microsoft Windows Server 2016
- 565 Network Adapter: VLAN 1501
- 566 PACSgear Core Server Installation
- 567 The installation of Hyland PACSgear Core Server was performed by Hyland engineers as listed below:

- The installation of Hyland PACSgear Core Server was performed by Hyland engineers per their
   technical guidelines.
- 570 2. The installation created a web application for the PACSgear Core Portal, where an SSL certificate 571 signed by DigiCert was created and assigned to the application for HTTPS enforcement.

### 572 PACSgear Core Server Configuration

- 573 Configuration of the PACSgear Core Server was performed by the Hyland engineers. The basic
- 574 configuration involves managing connection settings to external devices, lookup data sources, and event
- 575 trace; managing departments for multi tenancy architecture; managing user access; and many more
- 576 features. Each organization will configure the PACSgear based on its specific needs.
- 577 During the database configuration, the Hyland engineers created instances for representative
- 578 departments (e.g., ophthalmology, radiology, and departments that may see patients who need wound 579 treatment).
- 580 **Add New Departments:** To add the **ophthalmology** department, complete the following steps:
- 581 1. The Hyland engineers logged on to the PACSgear Admin portal by using *https:// hyland-pgcore.pacs.hclab/PGAPPS/Admin*.

PACSgear		+3 Log
	Log in	
	User name	
	admin	
	Password	
	Log In	

- 583
- 584 2. On the **Settings** menu, select **Departments.**

rver Status	C	Job Status			Defaults Server EHR		
Component	Status	Date	Message	Station	Device Provisionin	2	
Server Status	Running		No data av	allable in table			
Server Version	4.1.0.64						
Lo	gin Count	Date 6/25/2019 6/25/2019	Type INFO INFO	Message Checking port . Checking port done.	ĺ		
10 An 29 An 3	1 JUE JUE	6/26/2019	INFO	Verifying license			
vision Device	。 那些马	1					

589

- 586 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.

epartments				
how 10 * entries			Search:	
Default	* Name	Default Query Source		)
2	General			
8	RADIOLOGY	RADIOLOGY		
	WOUND CARE	RADIOLOGY		
owing 1 to 3 of 3 entries				Previous 1 Next
+ Add				- Edit E Delete

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

efault			AE title		
ame			Modality		
			None		
Destinations	XDS Lookup Sources	Client	Series	-	
8	VNA RAD		RADIOLOGY DEPT		
0	WOUND DEPT		Wound Care Department		

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

efault		AE title	
		Ophthalmology	
ame		Modality	
phthalmol	ogy	ст •	
Destination	Name	Client Series Description	
	VNA RAD	RADIOLOGY DEPT	
	WOUND DEPT	Wound Care Department	
	WOUND DEPT	Wound Care Department	

- 597 6. On the **Destinations** and **Lookup Sources** tabs, the engineers set up the destination and lookup598 sources for each department.
- 599 7. On the Client tab, the engineers set up the client access permissions to this department's
  600 resources.

/Edit Department											
fault				A	E titl	e					
ime				м	odal	ity					
				N	lone				,	•	
ply series per i											
estinations XDS	Lookup So	ources	Client	Serie	es			Marc			
estinations XDS	Lookup So Persisten Login	at	Client	Serie Phote Quali		Video Quali		Max. Video Lengtl	h.	Allow Came Impo	era
	Persisten	<sup>nt</sup> v		Phote				Video	•	Came	era
Client	Persisten Login	nt v	'ideo	Phote Quali	o ity	Quali	ity	Video Lengti	-	Came Impo	era ort

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

C Introductive procession of the procession o	1997-0479-0489-0499-0499-0499-0499-0499-0499-049	- O Settings - 📓 Logs - 🖌 Help -	tir 🙂 🔒
Departments			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 Next
+ Add			v. Eda: a Deleta

- 605 <u>Add LDAP/Active Directory Server: t</u>o use an LDAP/Active Directory server, configure these
   606 parameters:
- 607 1. Create an **LDAP\_User** account in Active Directory before proceeding.
- Using a browser, log on to the **PACSgear Admin** portal by using *https://hyland- pgcore.pacs.hclab/PGAPPS/Admin*.
- 610 3. On the **Settings** menu, select **Users**.

	s//nyiano-pgcc	vre.pacs.nciab/i	NGAPPS/Admin/User				1		<b>0</b> 4 G	1 (H)		
ACSgear	A Home E	🗄 ModLink 🗕	PACS Scan Web +	🔳 Image Link +	🗲 Tools -	Settings -	Logs -	<ul> <li>Help -</li> </ul>			1 adr	nin
USETS Restrict access per	missions to:					Users Connections Departments Defaults Server EHR						
Local Users 1.0	AP Users					Device Provisio	ming					
Show 10 • entri	es					Group	Search	admin				
admin						ADMIN						
kzheng						ADMIN						-
Showing 1 to 2 of 2 entries									Previous	1	Ne	ort
* Add										×	Déleti	

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

Users				
USEIS .				
Restrict access permissions to:				
Local Users LDAP Users				
Server:				
192 168 120 100				
Domain:				
pacs holab				
Test Save				
ihow 10 * entries	Search:	admin		
User Name * Group				
AcuoServiceUser ADMIN				_
howing 1 to 1 of 1 entries (littered from 2 total entries)		Previo	ious 1	N
+ Add			t 1	

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

Username:	
LDAP_User	
Password:	

620

619 7. A message box appears indicating the test is successful. Click **OK**.

hyland-pgcore.pacs.hclab says	
Test Successful	

- 621 **PACS Scan Mobile Configuration**—Install and configure the PACS Scan application to an Apple iPhone by applying these steps:
- 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.
- 626 2. On a workstation, log in to PACSgear Core Server by using the administrator credentials; a
   627 dashboard will display and provide a Provision Device QR code.

Serve	er Status	0	Job Status			0		
	Component	Status	Date	Message	Station	-		
•	Server Status	Running		No data a	valiable in table			
	Server Version	41.0.64						
Logis	ns: Last 30 Days	0	5 Most Rece	nt Logs		0		
0	Login Cour	11	Date	Туре	Message	1		
0			6/26/2019	INFO	Checking port			
0			6/26/2019	INFO	Checking port done.			
0			6/26/2019	INFO	Verifying license			
n 26	2 Nr. 38 Nr. 2	71.5 71.8	6/26/2019	INFO	TCPServer: TCPServe			
Provi	ision Device	0						
		80						
	12/04/04/08	ČARO I						

### 628

629 3. On the mobile device PACS Scan App, tap the QR code icon that appears under the Log In button.
630 This will turn 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 app to
 the address of its PACSgear Core Server instance.

- 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 emailattachment sent to the installer.
- 639 7. The installer opens the email from the iPhone and double-clicks on the attachment to install the640 certificate to the device.
- 8. To verify the certificate installation, go to Settings > General > Profiles & Device Management to
   list all the certificates profiles.
- 643 9. Find the certificate you installed and click to display the detail. Below is an example:



- 10. To verify the PACS Scan Mobile App functionality, from the iPhone, double-click the **PACS Scan**
- 646 **App.** The log in page will display. Use an account and password that has been associated with a
- 647 clinical department to log in. Successful log in displays a patient information input page, as shown 648 below:

3:02				al 🕈 🗖
≡	P/	ACS Scan M	obile	5
Patient				
MRN	Medic	al record numb	ber	
Last		ame		
First	First n	ame		
Middle	Middle	e name		
DOB	Date o	f birth		x
Mal	e	Female	0	ther
Study				
Acc.	Acces	sion number		
Desc.	Study			
Series				
	5	Select descrip	tion	-
s	tandard		Confident	ial
Search		Clear		Next
	-		_	

## 650 2.2.4 Hyland NilRead

651 Hyland NilRead provides image access and viewing from various devices including clinical viewing

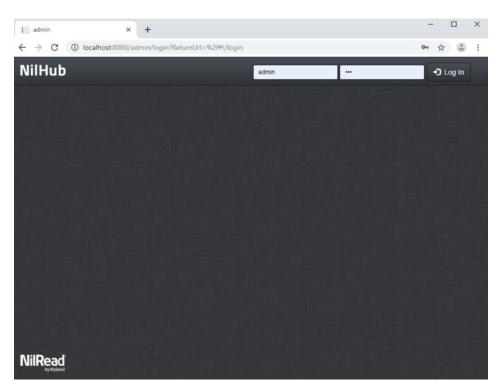
- stations, tablets, and mobile devices. NilRead also provides image manipulation, interpretation, and
- collaboration across departments. The installation and configuration procedures are found below.
- 654 System Requirements
- 655 **CPU:** 6
- 656 Memory: 12 GB RAM
- 657 Storage:
- 658 HD 1: 80 GB (OS Install)
- 659 HD 2: 200 GB (Web Application)
- 660 HD 3: 100 GB (Image Cache)
- 661 **Operating System:** Microsoft Windows Server 2016
- 662 Network Adapter: VLAN 1301

### 663 Hyland NilRead Installation

- The installation of Hyland NilRead was performed by Hyland engineers based on Hyland's proprietary installation package and installation guides. NilRead has three services: the Hub Front End service, Nil Back End service, and Nil Front End service. The Hub Front End service is used to provide management service for multi-tenant configuration. The operation context is defined by the Nil database content and includes user accounts, data life-cycle rules, hanging protocols, DICOM connectivity setup, and cached DICOM data index.
- 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.

### 672 Hyland NilRead Configuration

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



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

NilHub	Sites Lice	nses Setting:	s Logout			
Hub / Sites						
Sites		•	<b>s c</b> 1	i ø 8	4 +	6 8 8
Name	Code	AE Title	Partition	E-Mail	Version	State
RADIOLOGY	123	RADIOLOGY		none@yaho	4.3.31.98805	

678

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

- 681 Name: WOUND\_CARE
- 682 Details: Wound Care Department
- 683 **Code:** 974
- 684 AE Title: WOUND\_CARE
- 685 VNA Partition: WOUND\_CARE
- 686 **Database Name:** WOUND\_CARE
- 687 Email: none@hyland.com

lew	
NAME	
WOUND_CARE	1e0x3363-5144-4013-aetia 63x1b428225
DETAILS	VNA PARTITION
Wound Care Department	WOUND_CARE
cone	DATABASE NAME
974	WOUND_CARE
AE TITLE	
WOUND_CARE	C.WiRepostoryWOUND_CARE
E MAR	ENABLE SPORE FEDERADION
none@hyland.com	Alteretunation

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

Ni	
Site: User Name: Password: Domain:	admin
	ur connection speed Type: Auto detect

690

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

Set	tings	
Settings		
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	erences User Preferences Workstation Preferences Radiation Therapy Templates Reading Environment Verification Hanging Protocols Mouse, Keyboard And Tools Study Note Templates Assets Work Lists and Folders Confidentiality Profiles Confidentiality Masks • Advanced	
	Management Profile	
	Accounts	

5. Click **Add** on the bottom left-hand side of the screen and provide this information:

694		<ul> <li>User Name: pacs\ptester</li> </ul>
695		Last Name: Tester
696		First Name: Pacs
697		Role: User
698		E-Mail: ptester@hyland.pacs.com
699		Password: ****
700	6.	Identify Member Groups the user needs access to and click the Add button.

- 701 7. Specify the **Granted Privileges** the user needs to have and click the **Grant** button.
- 702 8. Click the **Save** button on the bottom left-hand side of the screen.

Account					
	pacs\ptester	_	Last Name	Tester	
Role	User T		First Name	Pacs	
	ptester@hylan	d pacs com	-		-
Skype ID			Prefix		
Phone	<u> </u>		Suffix		
Facility			Department		-
Password			Job Description	Physician	
			Expiry Date		00
	Notify on Sta	why Arrival			
highlighted fields are		wy central			
Groups					
Member			Not Member		
				,CN=Users,DC=pad	s.[ _
		-			
		~			
		Remove	Add		
		. terneve			
Privileges					
Granted DicomQueryRetr			Revoked BookmarkSaveS	and a	
DicomRt	eve	-	Collaboration		
EditHangingProto	ocols		ContentDownloa	1	
EditWorkItems		-	ContentUpload		-
		Revoke	Grant		
Licensing					
License Features					
adapterCoActiv					
adapterMach7Tec					- 10
adapterTeraMedic advancedDataQu					- 27
advancedMeasur					
Active Licenses					
NCCoE					
	_	In	fo		
DICOM Physician N	- second se				
	lames				
Associated					
					^
	14	0	Annalista		
		UISSOCIATE	Associate		
Timeline data sourc			16		

- 704 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
- 706 only the Ophthalmology VNA partition/tenant.

## 707 2.3 Secure DICOM Communication Between PACS and VNA

- 708 Hyland Acuo VNA and Philips IntelliSpace PACS support DICOM Transport Layer Security (TLS). DICOM
- 709 TLS provides a means to secure data in transit. This project implements DICOM TLS between the Acuo
- 710 VNA and IntelliSpace PACS via mutual authentication as part of the TLS handshake protocol [10].

# 711 2.3.1 Public Key Infrastructure (PKI) Certificate Creation

- 712 Server/client digital certificates are created for the Hyland Acuo VNA and Philips IntelliSpace server. This
- 713 project uses 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.

# 715 2.3.1.1 Create PKI Certificate for Hyland Acuo VNA

- Use 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 shown
   below:
- 719 Common Name: Hyland-VNA.pacs.hclab
- 720 Subject Alternative Name: Hyland-VNA.pacs.hclab
- 721 Organization: NIST
- 722 Department: NCCoE
- 723 City: Rockville
- 724 State: Maryland
- 725 Country: USA
- 726 Key Size: 2048
- 727 2. Submit the created CSR to DigiCert portal for certificate signing.
- 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, and then export thecertificate with its private key in the .pfx format.
- 732 5. The certificate is ready for installation.

## 733 2.3.1.2 Create PKI Certificate for Philips IntelliSpace PACS

- Use DigiCert Certificate Utility for Windows to generate a CSR for PACS server. Information
   needed for requesting the certificate is shown below:
- 736 Common Name: nccoess1.stnccoe.isyntax.net
- 737 Subject Alternative Name: nccoess1.stnccoe.isyntax.net
- 738 Organization: NIST
- 739 **Department:** NCCoE
- 740 City: Rockville
- 741 State: Maryland
- 742 Country: USA
- 743 Key Size: 2048

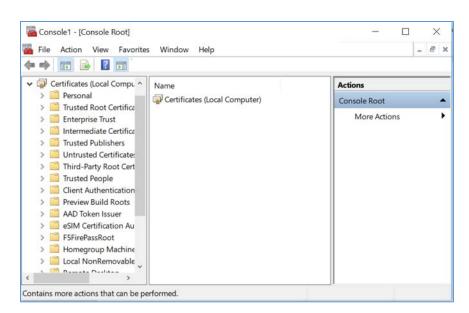
- 2. Submit the created CSR to DigiCert portal for certificate signing.
- 3. Download and save the signed certificate along with its root CA certificate in the .pem
- 746
   4. Import the saved certificate to DigiCert Certificate Utility for Windows, and then export the
   747
   certificate with its private key in the .pfx format.
- 748 5. The certificate is ready for installation.

## 749 2.3.2 PKI Certification Installation

- 750 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 per server instance and assume access to both.
- 753 2.3.2.1 Install PKI Certificate for Hyland Acuo VNA
- 754 Install the certificate on Hyland Acuo VNA server using the procedures below:
- 1. From the Acuo server, click on **Start > Run > mmc.**
- 756 2. Select File > Add/Remove Snap-in...

File				- 6
	New Open_	Ctrl+N Ctrl+O		1
	Save	Ctrl+S		Actions
	Save As	Ctri+5	There are no items to show in this view.	Console Root
			More Actions	
	Add/Remove Snap-in_	Ctrl+M		
	Options_			
	1 devrigmt.msc			
	Exit			

- 757
- 758 3. Select **Certificates** and click **Add**.
- 759 Choose Computer Account
- 760 Choose Local Computer
- 761 4. Click **Finish**, then click **OK**.



764

765

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

This snap-in will always manage o	ertificates for:			
◯ My user account				
⊖ Service account				
<ul> <li>Computer account</li> </ul>				
		Back		
			Next >	Cano

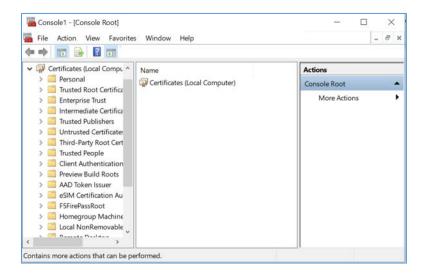
- a. Browse to the exported .pfx certificate.
- b. Select the file and click **Open**.

🚡 File Action '	View Favorites Window H	Help		- 8 3
	ocal Compu ^ Object Type			Actions
✓ Personal ○ Cer	Find Certificates_			Personal
> Trusted	All Tasks	: >	Find Certificates_	More Actions
> 🧾 Interme	View		Request New Certificate	
> Trusted	New Window from Here		Import_	
> Third-P	New Taskpad View		Advanced Operations	
> Client #	Refresh Export List			
> 🧮 Test Ro > 🧮 eSIM C	Help			
<ul> <li>Remote I</li> <li>Certificat</li> </ul>	up Machine Desktop e Enrollmen rd Trusted R v			

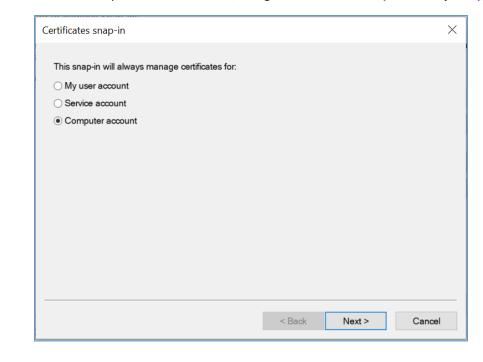
- 769 7. Add the appropriate permissions to the newly generated certificate private key.
- 770
  - a. Navigate to Certificates > Personal > Certificates.
- b. Right click on the certificate, select All Tasks > Manage Private Keys...
- c. Add the AcuoServiceUser and grant full control permissions. Click OK.
- 773 This procedure also installs the signing CA Root certificate (**DigiCert Test Root CA SHA2**) and its
- 774 Intermediate Root certificate (DigiCert Test Intermediate Root CA SHA2) into the server computer.
- 775 2.3.2.2 Install PKI Certificate for Philips IntelliSpace PACS
- 776 Install the certificate on the PACS server using the procedures that follow:
- 1. From the IntelliSpace server, click on **Start > Run > mmc**.
- 778 2. Select File > Add/Remove Snap-in...

File	Action View F	avorites W	/indow Help		- 8 ×
(H	New		1+N		
	Open		1+0		Actions
	Save	Cti	rl+S	There are no items to show in this view.	Console Root
	Save As				More Actions
	Add/Remove Snap-	in_ Ctrl	I+M		
	Options				
	1 devmgmt.msc				
	Exit				
-					

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



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



786

### 787 5. Right click and select All Tasks/Import.

- 788 a. Browse to the exported .pfx certificate.
  - b. Select the file and click **Open**.

File Action	View Favorites Window H	Help		- 8
	(Local Compl. ^ Object Type			Actions
<ul> <li>Persona</li> <li>Cer</li> </ul>				Personal
> Cer Trusted > Cer	All Tacks	. >	Find Certificates_	More Actions
> 🧾 Interme			Request New Certificate	
> 🧾 Trusted	New Window from Here		Import	
> 🧾 Untrus > 🧾 Third-P			Advanced Operations	
<ul> <li>Trusted</li> <li>Client A</li> <li>Preview</li> </ul>	r Refresh			
> 🧮 Test Ro				
<ul> <li>Homeg</li> <li>Remote</li> <li>Certific</li> </ul>	roup Machine a Desktop ate Enrollmen Card Trusted R.			

790

789

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

## 793 2.3.3 TLS Secure DICOM Configuration

794 With the signed certificates installed to the Acuo VNA and IntelliSpace PACS servers, proceed to

configuring DICOM TLS. The set of procedures that follows describe TLS configuration that must be

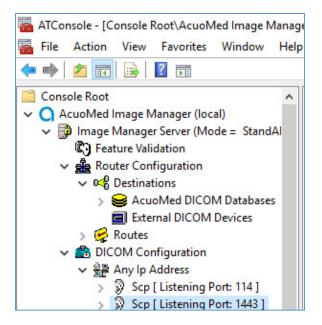
796 performed on both Acuo VNA and IntelliSpace PACS. This will enable DICOM TLS communications

- between these two endpoints, and secure data-in-transit communications bi-directionally between theVNA and PACS.
- 798 VNA and PACS.

## 799 2.3.3.1 TLS Configuration for Hyland Acuo VNA

For receiving TLS DICOM message 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)**:
- 803 2. From the Console > AcuoMed Image Manager (local) > DICOM Configuration, right click Any Ip
   804 Address > New Scp ... to create a new SCP for TLS encryption.

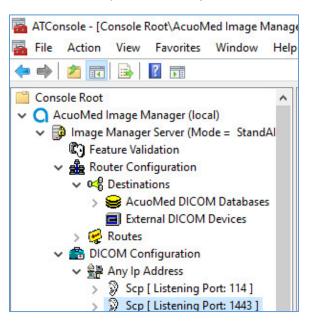


806 3. On the Connectivity tab of the SCP Properties page, provide the information below and click Add,
 807 Apply, and then Finish:

808 **Port**: 1443 809 Check the **TLS** checkbox 810 Client Certificate CN: nccoess1.stnccoe.issyntax.net 811 Server Certificate CN: HYLAND-VNA.pacs.hclab Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA 812 813 Check the **Authenticate Client Certificate** checkbox

ectivity Tuning Parameter	2
TCP/IP	
IP Address:	0.0.0.0
Port:	1443 🔽 TLS
TLS Settings	
	nccoess1.stnccoe.isyntax.net  Add Delete
Server Certificate CN:	HYLAND-VNA.pacs.hclab
Cipher Suite:	TLS_RSA_WITH_AES_128_CBC_SHA
	Authenticate Client Certificate

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



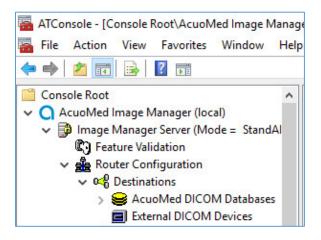
817

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

1	SOP Configuration   External SCU Authorization   Options   Reconciliation   Postfetch Prop	perties Domain	
	AE Identification		Page Actions
	Called AE Name: RADIOLOGY		Page Actions
	Collaborative Routing		1
	*Default Route Name: RADIOLOGY	•	
	□ Tag Rule Routing		1
	Associated Tag Rules (And the Associated Reconciliation Dependencies):		
	Tag Rules		
	*Tag Failure Route:	•	
		<u></u>	
	⊢ Stat Route		1
	**Stat Route Name:	•	
	* Immediate C-STORE processing depends on the Reconciliation Settings for this AE. C-S'	TORE processing will	
	be delayed until the reconciliation detected problem is resolved if reconciliation is set for th The C-STORE is always sent on this route even if it does not pass reconciliation.	is AE.	
	- Storage Destination Filtering - Storage Destination Filteri		(*)
	Enable Filtering Tag:		
	training reg.		

For sending 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**:
- Navigate to Image Manager Server > Router Configuration > External DICOM Devices, right click
   on External DICOM Devices and click New.



826

827 828	3.	On the <b>Main</b> tab of the <b>External DICOM Devices Properties</b> page, provide the information below and click <b>Apply,</b> and then click <b>Finish:</b>
829		SCP Destination Name: PHILIPS
830		Called AE Name: STENTOR_SCP
831		IP Address: 192.168.140.131
832		SCP Listening Port: 2762
833		Enable TLS by clicking the <b>TLS</b> checkbox next to the listening port number.
834		Called AE Name: ACUO
835		Implementation UID: 1.2.840.114158.1.1.3
836		Client Certificate CN: HYLAND-VNA.pacs.hclab
837		Server Certificate CN: nccoess1.stnccoe.isyntax.net
838		Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA
		External DICOM Device Properties ×
		Main SOP Configuration   Options   Domain
		SCP Destination Name: Page Actions External Device Called AE Name: STENTOR_SCP

Finish Cancel Apply

839

840

TCP/IP Connectivity

AcuoMed

TLS Settings

Connection Testing

C Host Name:

SCP Listening Port: 2762

Calling AE Name: ACUO Implementation UID: 12.840.114158.1.1.3 Version Name: AcuoMed

Client Cettificate CN: HYLAND-VNA pacs holab Server Cettificate CN: ncccess 1.stnccce.isyntax.net

Press the test button to validate DICOM connectivity.

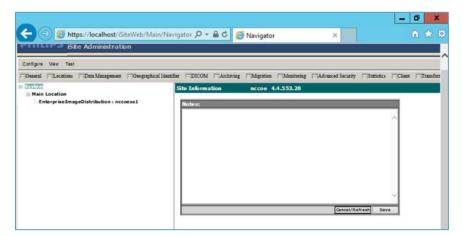
Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA -

TLS

Test

## 841 2.3.3.2 TLS Configuration for Philips IntelliSpace PACS

- 842 Next, configure TLS on the IntelliSpace PACS server. The steps below would be taken to enable this
- 843 feature on the PACS:
- 1. Access the Philips iSite Administration web site *https://192.168.140.131/iSiteWeb* using
- 845 administrator credentials.



### 846

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

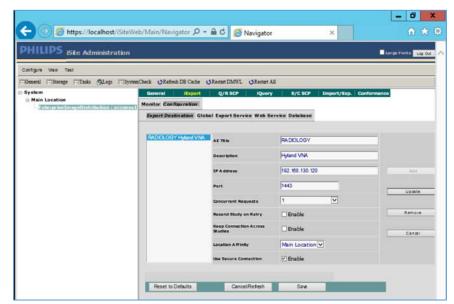
Configure Vew Test				Large Fonts Log Out
General ⊡Storage ⊡Tasks @Logs ⊡Syst	enCheck ORefresh DB Cache ORestart DM	NL ORestart All		
System	General IExport Q/R SC DICOM Support	P iQuery S/C SCP	Import/Exp. Conformant	
EnterpriseImageDistribution ; accors	Normal AETRic	STENTOR_SCP	Default	
	High Priority AETRie	STENTOR_HI	Default	
	Port	104	Default	
	Secure Port Replace Non Latin-1 During Import	2762	Default	
	Enable/Disable Export on DICC	DM Processing Host(s)		
	+ Advanced			

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

854 • **Port**: 1443

#### 855

#### Use Secure Connection: checked

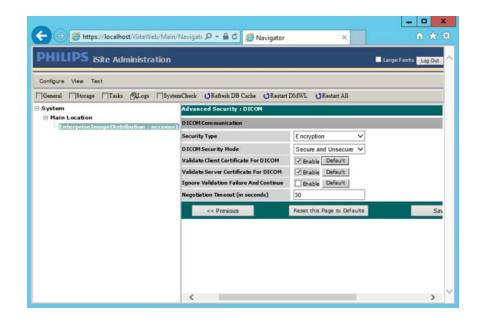


- 4. Click **Configuration** > **Advanced Security**, perform these selections:
- 858 **TLS 1.0 or higher**: Selected
- 859 Enable Secure Web Services Communication
- 860 Enable Image Access in Secure Mode
- 861 Default Client Certificate: CN= nccoess1.stnccoe.isyntax.net
- 862 Default Server Certificate: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

Configure Mew Test	stration					Large Fonts 10
General ⊟Storage ⊟Tasks ∰L System	ogs SystemCheck ORef		be (Restart I Security : Ge		Restart All	
Main Location	Directory					
Enter prise ImageDis tributio	n : nccoess1 Server DICOM	O SSL 3.0	) or higher 💌 1	LS 1.0 or high	her OTLS 1.1 or higher OTLS 1.2	
	Session	Secure Web Services		Enable		
	Management			Default		
		I mage Acc Mode	ess in Secure	Default		
		Certificate Manager				
		Default	CNenccosasi	sincese isynt	tax.net, OU=NCCoE, O=NIST-NCCoE, L=F	Rockville, V
		Certificate				
		Server Certificate	CN=nccoess1	.stnccoe.isynt	tax.net, OU=NCCoE, O=NIST-NCCoE, L=A	Rockville, V
		Allow Self 5 Certificate	ligned	Default		
		Certificate	Ficate Validations			
		EKU Check	DEnet(+	)etault		
		Certificate Revocation Check	Diretie 1	)efeult		
		CRL Caching	Comple C	Default		
		Revocation Check for Chain		itian of full ca	ertifica le chain	~
		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.
- 868 c. Click **Save** to save the settings.



870 6. Restart the **iSite Monitor** Service.

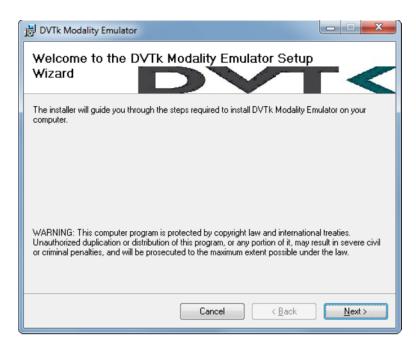
## 871 2.3.4 PACS and VNA TLS Integration Tests

- 872 After implementing the above PKI-certification installation and TLS enabling configuration, both 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 bi-direction data exchanges between
- 875 Acuo VNA and IntelliSpace PACS to confirm:
- 876 DICOM communication is still functional.
- 877 DICOM communication is encrypted.
- 878 The test proves the DICOM communication was successful, with the accurate data exchange between
- 879 Acuo VNA and IntelliSpace PACS.
- 880 The network flow and dataflows monitoring tool indicates that the mutual authentication between Acuo
- 881 VNA and IntelliSpace PACS are established. Encrypted application data were exchanged.

# 882 2.4 Modalities

## 883 2.4.1 DVTk Modality Emulator

- 884 DVTk Modality is a modality emulator that can be used to 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, modality performed procedure step (MPPS), and Storage actions.
   Consequently, this project chose to use the DVTk Modality as an emulator to test the connectivity,
- communication, workflow, and interaction between PACS and modality in the lab.
- 889 System Requirements
- 890 Operating System: Microsoft Window 7 (with Microsoft .NET 4.0 Framework)
- 891 Network Adapter: VLAN 1402
- 892 DVTk Modality Installation
- 1. Download the installation software from the DVTK site [11].
- Click the Modality Installation file (e.g., *DVTk-Modality-Emulator-5.0.0.msi*) to start the installation process.



897 3. Follow the wizard instruction to continue the installation until it reaches successful completion.

😸 DVTk Modality Emulator	
Installation Complete	<b>Г</b> <
DVTk Modality Emulator has been successfully installed.	
Click "Close" to exit.	
Please use Windows Update to check for any critical updates to the .NET Frame	ework.
Cancel < <u>B</u> ack	Close

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

ile <u>H</u> elp			
≷ 🛢 🗐 🗇   ← ↑ →			
Control ) RIS System			
		Ping RIS	
NO		DICOM Echo	
Me S		Request Worklist	
~	12122332	Send MPPS Progress	
Modality	RIS System	Hint	
PACS/Workstation Systems			
		Ping PACS/Workstation	
(No)	<b>→</b>	DICOM Echo	
(PO)		Store Image	
		Storage Commitment	
Modality	PACS/Workstation	and the continuant	

### 903 DVTk Modality Configuration

Configuration of the DVTk Modality involves the configuration of the communications with different
external systems, including the RIS, which is the Worklist provider or a worklist broker connected to the
RIS; the MPPS manager that handles the MPPS messages for status reporting; and the PACS and its
database 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 (AETitle). Input the information
with these values:

- 910 RIS System
- 911 IP Address: 192.168.160.201
- 912 Remote Port: 105
- 913 **AE Title**: RIS
- 914 MPPS Manager
- 915 IP Address: localhost
- 916 Remote Port: 105
- 917 AE Title: RIS
- 918 PACS/Workstation Systems–Storage Config
- 919 IP Address: localhost

- 920 **Remote Port**: 106
- 921 AE Title: MPPS
- 922 PACS/Workstation Systems–Storage Commit Config
- 923 IP Address: localhost
- 924 **Remote Port**: 107
- 925 AE Title: PACS
- 926 Store Commit Config
- 927 IP Address: localhost
- 928 **Remote Port**: 107
- 929 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	er	
IP Address:	localhost	
Remote Port	106	
AE Title:	MPPS	
PACS/Works	lation Systems	i / Store Commit Conlig
IP Address:	localhost	IP Address: Jocalhost
Remote Port.	107	Remote Port: 107

- 931 The configuration of the modality itself is also needed to indicate its **AE Title** (e.g., **DVTK\_MODALITY**),
- 932 Local IP Address (e.g., 172.31.138.126), and Listen Port (e.g., 104) to be paired for association negation

933 with other remote systems. The screenshot that follows indicates the options for the **Modality Emulator** 

934 configuration:

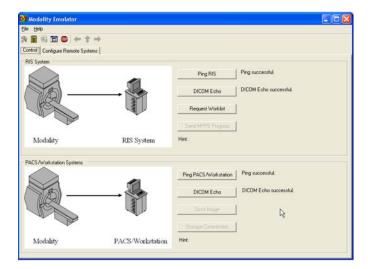
Modality Emulator		- 🗆 X
ile Help		
- + +   0 🖬 🖗	•	
Control Configure Emulator Work	ist Query   MPPS-Progress   MPPS-Discontinued   MPPS-C	ompleted   Image Storage   Dummy Patient
System Name:	Modaity	
AE Title:	DVTK_MODALITY	
Implementation Class UID:	1.2.826.0.1.3680043.2.1545.6.3.1.0	
Implementation Version Name:	ModalityEmulator	
Local IP Address:	172.31.138.126	
Listen Port	104	
Storage Commit Mode		
In Single Association (S)	iync commitment)	
C In Different Association	(Async commitment)	
Wait time for N-EVENT-REPOR	RT from PACS (in sec):	

936 Several tabs exist for configuring the behavior of the emulator. They can be configured as needed or use

937 the default settings. Once the configuration is done, the emulator front GUI interface provides some test

938 buttons for verifying the connectivity, including **RIS** and **PACS** server Internet Control Message Protocol

939 (ICMP) pings and **DICOM** echo:



940

## 941 2.4.2 DVTk RIS Emulator

942 DVTk, the Health Validation Toolkit, is an open-source software. The DVTk RIS Emulator is an application

- 943 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.
- 945 System Requirements
- 946 **Operating System**: Microsoft Windows 7 (Microsoft .NET framework 2.0)

## 947 DVTk RIS Emulator Installation

- 948 1. Download the DVTk RIS Software installer RIS Emulator .msi file from <u>http://www.dvtk.org.</u>
- 949 2. Start the installation procedure by double-clicking the .msi installation file.
- 950 3. Follow the wizard screen instruction to continue the installation until the end of successful951 installation is displayed.
- 952 4. Close the installation window and start to **RIS Emulator**. The User Interface of the **RIS Emulator** 953 tool that follows is shown with the tabs that follow for selecting the modes:
- 954 5. Worklist
- 955 MPPS
- 956 Edit DCM Files
- 957 Activity Logging
- 958 Validation results

RIS Emulator			
File Stored Files Ab	out		
The stored files Ab	and the second se	DCM Files Results Activity Logging	
Select Mode	Local AE title:	DVTK_RIS	
	Local port:	107	
Start	Remote AE title:	DVTK_MODALITY	
	Herioto AL date.	DVIK_MODALITY	
Stop			
Specify TS			
Save			
1	View information	n model View the MWL information model constructed from the Dicom files.	
$\leftarrow$			
	Import Dicom	files Import DICOM files to default data directory for emulating WLM res	ponses.
	E e e e e e e e		
	I▼ Set Scheduled F	Procedure Step Date\Time to current date\time	
		day for an first left Management	
	i Select data dire	ctory for sending WLM responses	

#### 960 DVTk RIS Emulator Configuration

961 1. Worklist Configuration

- 962 Local AT title: AE title of the RIS Emulator
- 963 Local Port: The port of the RIS Emulator for incoming association
- 964 Remote AE title: AE title for the service class user paired with the RIS emulator
- 965 View Information Model: Information model used for sending the emulator response, default
   966 value is taken
- 967 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* 969 *Emulator\Data\Worklist\*
- The **RIS Emulator** also supports other parameter configuration such as MPPS and Store Files
   functionality. These can be done as needed.
- 972 3. Configuration of the **RIS Emulator** and the Modality storage emulator should be done accordingly, so
   973 they can communicate with each other.

## 974 2.5 Asset & Risk Management

## 975 2.5.1 Virta Labs BlueFlow

976 Virta Labs BlueFlow is a medical asset management software that allows for the discovery and
977 management of medical devices on the network. For this project, we used BlueFlow to create an
978 organized inventory of the medical devices in the PACS architecture.

- 979 System Requirements
- 980 **CPU:** 2
- 981 Memory: 8 GB RAM
- 982 Storage: 100 GB (Thin Provision)
- 983 Operating System: CENTOS 7
- 984 Network Adapter: VLAN 1201

#### 985 Virta Labs BlueFlow Installation

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

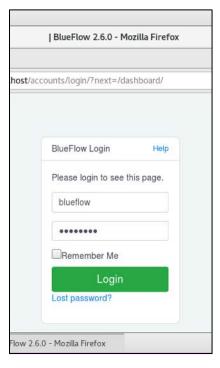


- 991 2. Run sysyemctl status blueflow.service in the CentOS 7 terminal.
- 992 3. Ensure **blueflow.service** is **active**.

Applications	Places	erminal		6	Wed 13:41	4	40)	Φ
		root@tes	t-blueflow:~/Documents			-		×
File Edit View	v Search	erminal Help						
<ul> <li>blueflow.se</li> <li>Loaded: lo</li> <li>Active: ac</li> <li>Process: 18</li> <li>atus=0/SUCCES</li> <li>Main PID: 18</li> <li>Tasks: 0</li> </ul>	arvice - baded (/o tive (e) 3711 Exec 35) 3711 (co	ted) since Wed 2019-07-03 13:	vice; enabled; vendor preset: di		es (code=e	exite	ed,	st
	09 test	<pre>lueflow systemd[1]: Starting lueflow systemd[1]: Started B cuments]#</pre>						

#### 4. Visit *https://localhost* to verify BlueFlow web service is operating as expected, with a **BlueFlow** 994 Login page.

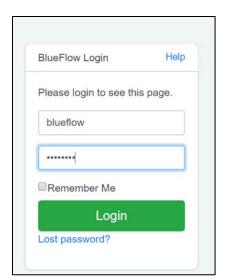
### 995



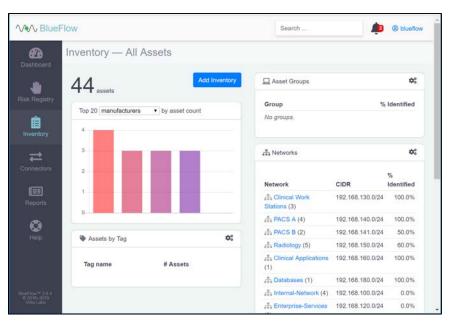
996

#### Virta Labs BlueFlow Network Groups Configuration 997

1. Log in to the **BlueFlow** web console. 998



- 1000 2. Navigate to the **Inventory** tab.
- 1001 3. Under the **Networks** section, click on the **gear** icon.



- 1003 4. Enter **Security Service** as a **Name** for the new **network group**.
- 1004 5. Enter **192.168.190.0/24** as a **CIDR** for the new **network group.**
- 1005 6. Click **create.**

A/V BlueFle	ow			Search	Blueflow
200 Dashboard	User Profile	A Network	5		
als.	Custom Asset Fields	Network		CIDR	Delete
sk Registry	Asset Groups	- Clinical	Work Stations (3)	192.168.130.0/24	亩
w rediany	Networks	A PACS A	(4)	192.168.140.0/24	窗
自	Tags	A PACS B	(2)	192.168.141.0/24	盲
iventory	Risk Factors &	A Radiolo	gy (5)	192.168.150.0/24	â
	Controls	+ Clinical	Applications (1)	192.168.160.0/24	亩
⇒	Connectors	🕂 Databas	ses (1)	192.168.180.0/24	ā
innectors	Logs	A Internal	-Network (4)	192.168.100.0/24	盲
Reports		🚓 Enterpri	se-Services (9)	192.168.120.0/24	ũ
0		New networ	k		
Help		Name	Security Services		
		CIDR	192.168.190.0/24		
					create
BlueFlow™ 2.0.4 © 2016–2019					create

- 1007 7. Verify that the new **network group (Security Services)** has been created.
- 1008 8. Click on the **name** of the new network group.

ashboard	User Profile	A Networks		
ىلك	Custom Asset Fields Asset Groups	Network	CIDR	Delete
k Registry	Networks	Clinical Work Stations (3)	192.168.130.0/24	Ô
- A-		PACS A (4)	192.168.140.0/24	Ô
自	Tags	PACS B (2)	192.168.141.0/24	Ē
ventory	Risk Factors &	Radiology (5)	192.168.150.0/24	ā
	Controls	Clinical Applications (1)	192.168.160.0/24	亩
₽	Connectors	Tatabases (1)	192.168.180.0/24	亩
nnectors	Logs	and Internal-Network (4)	192.168.100.0/24	窗
		Enterprise-Services (9)	192.168.120.0/24	窗
Reports		A Security Services (7)	192.168.190.0/24	Ô
<b>O</b> Help		New network		
		Name		
		CIDR		

## 1009

1010 9. Assets will be listed on this page if they match the network group's criteria.

1011 10. If there are no **assets** currently listed, you can manually add them by navigating to **Inventory** > **Add** 

1012 **Inventory** or by running an IP discovery scan (detailed in the next section).

VVV BlueFlo	W		<b>p</b>	Ø blueflow		
Dashboard	Network: Security	Services				
ىلل	Assets			Name:	Securit	y Services
Risk Registry	Actions -	1–7 o	f 7 Previous Next	CIDR:	192.16	8.190.0/24
finventory	Asset T	ags IP Address	Risk Score saf / sec / total <del>▼</del>	Details		
₽	Asset-130	192.168.190.122	0.0 / 2.0 / 1.0		These assets	All assets
Connectors	Asset-128	192.168.190.120	0.0 / 2.0 / 1.0	Asset	7	44
e	Asset-129	192.168.190.121	0.0 / 2.0 / 1.0	count:		
Reports	Asset-131	192.168.190.140	0.0 / 2.0 / 1.0	Assets identified:	0.0%	29.5%
Ø	Asset-132	192.168.190.160	0.0 / 2.0 / 1.0	Assets	100.0%	70.5%
Help	Asset-133	192.168.190.170	0.0 / 2.0 / 1.0	not identified:		
4	Asset-134	192.168.190.172	0.0 / 2.0 / 1.0	Average safety risk:	0.0	0.0
BlueFlow <sup>18</sup> 2.6.4 © 2016–2019 Virta Labs				Average	2.0	2.0

1013

### 1014 Running an IP Discovery Scan in Virta Labs BlueFlow

1015 1. Log in to the **BlueFlow** web console.

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

<b>∕∕∕∕ BlueFlo</b>	WC		Search	2 Solution
Dashboard	Connectors			
Ju	Connectors 🕫	Connector Tasks		
Risk Registry	17 connectors; showing only		Pre	vious Next
finventory	enabled connectors below.	Risk Metrics	finished Yesterday at 12:22 PM	Success
t ₽	BlueFlow Pulse	Fingerprint	finished Last Tuesday at 4:30 Pl	M Success
Connectors	CSV	Fingerprint	finished Last Tuesday at 4:29 Pl	M Success
	Discovery	Fingerprint	finished Last Tuesday at 4:28 Pl	M Success
Reports	Fingerprint	Fingerprint	finished Last Tuesday at 4:27 Pl	M Success
Ø	Nessus Import	Fingerprint	finished Last Tuesday at 4:14 PI	M Success
Help	Netflow	Fingerprint	finished Last Tuesday at 4:13 Pl	M Success
	Nexpose Import	Fingerprint	finished Last Tuesday at 4:04 PI	M Success
	Password Checker	Discovery	finished Last Tuesday at 3:23 Pl	M Success
BlueFlow™ 2.6.4 © 2016–2019 Virta Labs	Ping	Risk	finished Last Tuesday at 12:22	Success
bs://blueflow.pacs.hcla	ab/connectors/discovery/	Metrics	PM	

### 1017 2. Navigate to **Connectors > Discovery**.

1018

1019 3. Under **Discovery**, click the **gear** icon.

VV BlueFlow		Search		. (2) (2) (2) (2) (2) (2) (2) (2) (2) (2)
2 Dashboard	Connector: Discover	у		
ىلار	Discovery		00	Discovery
inventory	target IP, hostname or CIDR for discovery scan		Run	Discover assets using an ICMP ping scan. By default, this connector will not create new assets when it receives responses from connected assets. To configure this behavior, visit the connector settings.
	Connector Tasks			
Reports	Connector Tasks	Previo	us Next	
	Connector Tasks Discovery	Previor finished Last Tuesday at 3:23 PM	Success	
Reports		finished Last Tuesday at		
Reports	Discovery	finished Last Tuesday at 3:23 PM	Success	

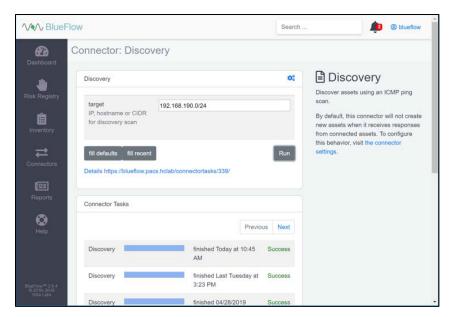
1021 4. Check the box next to allow\_create\_asset.

### 1022 5. Click **Save**.

WW BlueFl	ow		Search	
20 Dashboard	Settings: Connector			
Risk Registry	User Profile Custom Asset Fields Asset Groups Networks Tags	Discovery Settings enabled Enable or disable this connector	×	2
Connectors E Reports	rags Risk Factors & Controls Connectors Logs	allow_create_asset Allow creating new assets (not just updating existing)	×	Save
<b>O</b> Help				

1023

- 1024 6. Enter an IP (e.g., 192.168.190.0/24), host name or CIDR that you would like to scan.
- 1025 7. Click **Run.**
- 1026 8. Wait for the discovery scan to finish.



1028 9. Click on the **row** of the completed scan to view more details.

1029 Note: From this page, you can view the output of the scan, including how many devices were1030 discovered within the provided network range.

<b>∕∕∕∕√ BlueFlo</b>	ow			Search	<b>1</b> Blueflow
Dashboard	Connector Ta	isk			
-	Discovery				Success
Risk Registry	Inputs		Name	Value	
finventory			target	192.168.190.0/24	
	External URL				
Connectors	Submitted		Today at 10:45	AM	
	Started		Today at 10:45	5 AM	
Reports	Finished		Today at 10:45	AM	
Ø	Duration		a few seconds		
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 discover	ev ec an			
	created	0			
	updated	0			
	up-to-date	7			
	skipped	0			
	duplicate	0			
	errored	0			
Distances of a state					
© 2016–2019 Virta Labs	total	7			

### 1031

## 1032 2.5.2 Tripwire Enterprise

1033 Tripwire Enterprise is a security configuration management software that monitors file integrity through 1034 software-based agents. For this project, we used Tripwire Enterprise to monitor file changes on PACS 1035 servers and the VNA database.

- 1036 System Requirements
- 1037 **CPU**: 1
- 1038 Memory: 4 GB RAM
- 1039 Storage: 120 GB (Thin Provision)
- 1040 **Operating System**: Microsoft Windows Server 2016
- 1041 Network Adapter: VLAN 1201

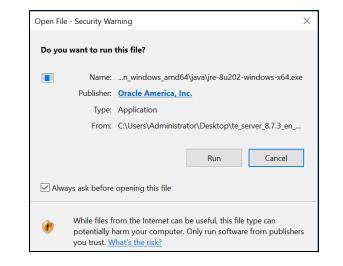
### 1042 Tripwire Enterprise Console Installation

1043 1. In the *tripwire install* folder under *java*, double-click on the *jre-8u202-windows-x64 application* file.

l I I I I I I I I I I I I I I I I I I I	Share	View			
← → • ↑ 🖡	> te_s	erver_8.7.3_en_windows_amd64 > java			
📌 Quick access		Name	Date modified	Туре	Size
늘 Desktop	*	🔬 jre-8u202-windows-x64	3/22/2019 8:04 AM	Application	75,467 KB
Downloads	$\mathcal{A}$				
Documents	*				

1044

#### 1045 2. Click on **Run**.



1046

1048

#### 1047 3. Click on Install >.

	Welcome to Java
	a world of amazing content. From business solutions to helpful utilities and nment, Java makes your Internet experience come to life.
Note: No personal informatio	n is gathered as part of our install process. <u>Click here</u> for more information what we do collect.
Click Ins	tall to accept the license agreement and install Java now.

1049 4. Click **OK**.



1051 5. Wait for the install process to complete.



### 1052

1053 6. Click **Close**.

	V You	have successful	ly installed Java		
You will be pro	mpted when Java upda	ates are available. Alw and security impro <u>More about update</u>	vements.	get the latest per	forma

# 1054

1055 7. With Java installed, double-click on the Tripwire install application, *install-server-windows-amd64*.

Home Share	Application Tools te_server_8.7.3_en	_windows_amd64		
→ × ↑ 📕 > te	server_8.7.3_en_windows_amd64			
Quick access	Name	Date modified	Туре	Size
Desktop *	3 docs	6/26/2019 12:14 PM	File folder	
	extras	6/26/2019 12:14 PM	File folder	
	📕 java	6/26/2019 12:14 PM	File folder	
Documents 🖈	twagents	6/26/2019 12:14 PM	File folder	
💺 Pictures 🛛 🖈	install-server-windows-amd64	2/4/2019 10:52 AM	Application	532,219 KB
Symantec DCS *	<ul> <li>license</li> </ul>	2/4/2019 10:52 AM	HTML Document	30 KB
Tripwire Enterprise	PORTS & CREDENTIALS	3/22/2019 9:42 AM	Text Document	1 KB

1059 1060

1057 8. Select the version of *Java, Oracle/Sun 1.8.0 64-bit,* that was previously installed.

### 1058 9. Click **OK**.

	Please select the Java	a(tm) Runtime t	to use	
Oracle/Sun 1	.8.0 64-bit C:/Program	Files/Java/jre1.	8.0_202/	bin/java.
12				
	ОК	Cancel		
lick Next >				
Click <b>Next &gt;</b> .				
	Console Installer			
Click Next >.	Console Installer		-	
	Console Installer			
	Console Installer		-	
te Tripwire Enterprise	Welcome to the Tripwir			
	Welcome to the Tripwir	nd configure Tripv se review the insta	vire Enterp Ilation doe	orise Conso cumentatio

1061

1062 11. Check I accept the agreement.

< Back

Next >

Cancel

#### 1063 12. Click **Next >**.

te Tripwire Enterprise Consol	le Installer	_		×
License Agreement		tr	ipwi	re
Please read the following Li before continuing with the	cense Agreement. You must accep installation.	ot the terms of th	his agree	ment
SUBJECT TO LICENSE RES AGREEMENT BEFORE USING COMPLETE AND UNCONDIT	LICENSED, NOT SOLD. USE OF STRICTIONS. CAREFULLY READ G THE SOFTWARE. USE OF SOF IONAL ACCEPTANCE OF THE TE EEMENT. ANY ADDITIONAL OR FIONS SHALL NOT APPLY.	THIS LICENS TWARE INDICA RMS AND COND	E TES ITIONS	,
Do you accept this license?	<ul> <li>I accept the agreement</li> <li>I do not accept the agreeme</li> </ul>	nt		
	< Back	Next >	Car	ncel

### 1064

1065 13. Specify an installation directory, *C:\Program Files\Tripwire\TE*, for the Tripwire installation.

### 1066 14. Click **Next >**.

e Tripwire Enterprise Console Installer		_	
Installation Directory		tr	ipwire
Please specify the directory where all Tripy	vire Enterprise compo	onents will be i	nstalled.
Installation Directory C:\Program Files\1	ripwire\TE	10	
InstallBuilder			

- 1068 15. Verify the host name for the machine on which you're installing Tripwire (e.g., WIN-1069 RUQDO7KL8A7).
- 1070 16. Click **Next >.**

Iripwire Enterprise	Console Installer		-		×
Tripwire Enterprise	Console Configuration Part 1 o	of 4	tr	ipwi	re:
Please provide the h installed.	ostname of the system where Tri	pwire Ente	erprise Console	will be	
TE Server Hostname	WIN-RUQDO7KL8A7				

- 1072 17. Specify the HTTPS Web Services port as 6000, HTTP EMS Integration Port as 8080, and Tripwire
   1073 Enterprise RMI Port as 9898.
- 1074 18. Click **Next >**.

Tripwire Enterprise Console (	Configuration F	art 2 of 4	<u> </u>	ipwire
Specify the ports that Tripwire	Enterprise Cons	ole uses to comr	nunicate.	
This port is used for user-initia	ted Web consol	e sessions.		
HTTPS Web Services port	6000			
This port is used for external in	tegrations (suc	n as plugins).		
HTTP EMS Integration Port	8080			
This port is used for Console/A	igent Java com	munications.		
Tripwire Enterprise RMI Port	9898			

- 1076 19. Create a password for Tripwire Enterprise services.
- 1077 20. Click **Next >.**

Tripwire Enterprise (	Console Configuration Part 3 of 4	j	tripwire
The services passphra	se is used to secure Tripwire Enterpris	e communicat	ions.
double-quote ("), less	e between 19 and 64 characters, and a-than (<), greater-than (>), or backsla d. See the Installation and Maintenan	sh (\) characte	rs, most other
Services Dassnhrase			
Services Passphrase Confirm Passphrase	·····		
	••••••		

- 1078
- 1079 21. Verify planned installation settings are correct.
- 1080 22. Click **Next >**.

C Tripwire Enterprise Console Installer	—		$\times$
Tripwire Enterprise Console Configuration Part 4 of 4	t	ripwi	re
Please review the installation settings for Tripwire Enterprise Consol	e.		
The following settings are configured for Tripwire Enterprise Consol	e:		
Installation Directory: C:\Program Files\Tripwire\TE Available Disk Space: 12709 MB Hostname: WIN-RUQDO7KL8A7			
IP Address(Listening): 0.0.0.0 HTTPS Web Services Port: 6000 HTTP EMS Integration Port: 8080			
TE Services (RMI) Port: 9898 TEConsoleInstaller: Java Version detected: 1.8.0_202 64			
nstallBuilder			
< Back	Next >	Ca	ncel

- 1081
- 1082 23. Check Install Real-time Monitoring.
- 1083 24. Specify **Real-time Port** as **1169** for monitoring.
- 1084 25. Click **Next >.**

te Tripwire Enterp	rise Console Installer	- [	
Tripwire Enterp	rise Agent Configuration	trip	wire
enable monitorin	se Agent software is installed on the Tripw ng of that system. Do you want to install R ent? The Real-time Monitoring feature can	eal-time Monitoring fu	unctional
🗹 Install Real	-time Monitoring		
Please specify t	he local port to be used by the Real-time s	ubsystem.	
Real-time Port	1169		
InstallBuilder	< Back	< Next >	Cancel
	< Baci	x Next >	Cancel
Click Next >.	< Back	x Next >	Cancel
Click <b>Next &gt;</b> .	rise Console Installer	c Next >	
Click <b>Next</b> >.	rise Console Installer		
Click Next >.	rise Console Installer		
Click Next >.	rise Console Installer	- Trip	

1087

1088 27. Wait for Tripwire Enterprise installation to complete.

InstallBuilder

Click Next to begin installing Tripwire Enterprise. Click Back to make any changes before you begin the installation.

< Back

Next >

Cancel

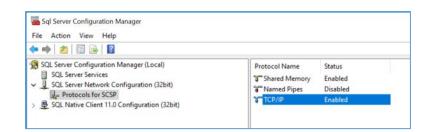
Tripwire Enterprise Console Installer		1	ripw	ire
Installing Unpacking C:\Program []Tripwire\TE\Ser	rver\lib\con	nmon\jsch-0	).1.40.jar	

### 1090 28. Click **Finish**.

1089

te Tripwire Enterprise	Console Installer	-		×
ENTERPRISE 8.7	<ul> <li>The installation is complete.</li> <li>Open a browser after clicking Finish to conti Tripwire Enterprise.</li> <li>✓</li> <li>✓</li> <li>To finish configuration later, use a browser t https://WIN-RUQDO7KL8A7</li> </ul>			
	< Back	nish	Can	cel

- 1092 29. Open SQL Server Configuration Manger.
- 30. Under SQL Server Network Configuration > Protocols for SQL Server ensure the TCP/IP protocol is
   set to Enabled.

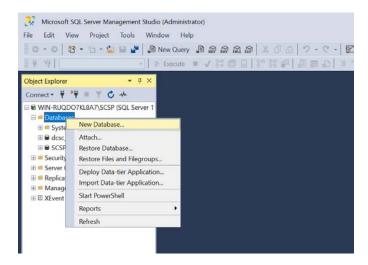


1096 31. Open SQL Server Management Studio.

File Edit View Project	Tools Window Help
0.0 3.00	🛛 🗎 🎥 🔎 New Query 🚇 😭 📾 🖓 🎧 🎧 🖓 🕹 🗇 🗇 🏷 - ペー
¥ ~4	-   ▷ Execute = ✓ 😵 🗇 🗟   😵 🕮 🗐 🕮 🗗   3
Object Explorer	- ų X
Connect - # *# = T d	<b>5</b> 44
B WIN-RUQDO7KL8A7\SCS	
■ ■ WIN-RUQDO7KL8A7\SCS ⊞ ■ Databases	
B WIN-RUQDO7KL8A7\SCS     Databases     Security	
⊞ ≡ Security ⊞ ≡ Server Objects	

1097

1098 32. In the **Object Explorer** expand the selection for your database, right click on **Databases** and select
 1099 New Database...



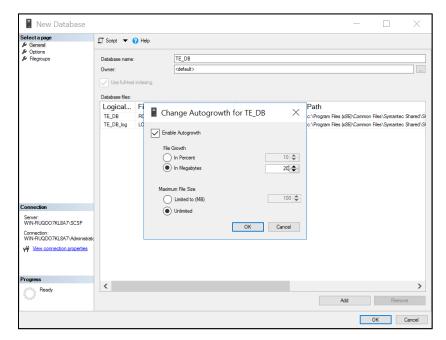
- 1101 33. On the left, under Select a page, select General.
- 1102 34. Enter a **Database name** as **TE\_DB**.
- 1103 35. Under **Database files**, for the data file, set **Initial Size** to at least **2,000**.

Select a page	💭 Script 🔻 🌔	2 Help						
<ul> <li>General</li> <li>Options</li> </ul>								
Filegroups	Database name:		TE_DB					
	Owner:		<default></default>					
	Use full-text	indexing						
	Database files:							
	Logical		Filegroup		Autogrowth / Max.			
	TE_DB		PRIMARY	2,000		c:\Program Files (x86)\Comm		
	TE_DB_log	LOG	Not Applicable	500	By 10 percent, Unlimited	c:\Program Files (x86)\Comm	on Files\Symantec	Shared\S
Connection Server: WIN-RUQDO7KL8A7-SCSP								
Server:								
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administrato								
WIN-RUQDO7KL8A7\SCSP								
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Administratu WIN-RUQDO7KL8A7\Administratu Wew connection properties	<							>

### 1104 36. Click the **button** under **Autogrowth**.

1105

- 1106 37. Check Enable Autogrowth, set File Growth to at least 20 MB, and set Maximum File Size to
   1107 Unlimited.
- 1108 38. Click **OK**.



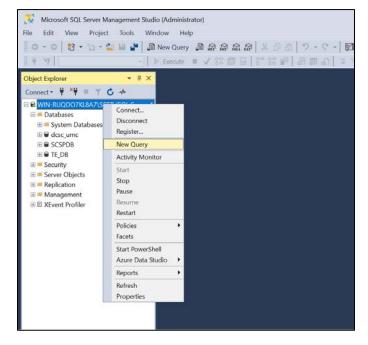
- 1110 39. Under **Database files**, for the log file, set **Initial Size** to at least **500**.
- 1111 40. Click the **button** under Autogrowth.
- 1112 41. Check Enable Autogrowth, set File Growth to at least 20 MB, and set Maximum File Size to
- 1113 Unlimited.
- 1114 42. Click **OK**.

Select appe General Cotors Friegroups Database name: Owner: Use fulfect Database files: Logical TE_DB TE_DB log TE_DB log Server: WINFNQDD7KLBA7SCSP Connection	TE_DB (default) ff R[ Change Autogrowth for TE_DB_log ×	Path
Fiegroups Database name: Owner: Use fulleet Database files: Logical TE_DB_TE_DB_TE_DB_Jog           Connection           Server: WIN-RUADO 7KLBAT/SCSP	rdering F∫ ■ Change Autogrowth for TE_DB_log ×	Path
Wini-RuGaD07KL8A7∿Administrate ₩ <u>View connection properties</u>	LL Prable Autogrowth File Growth In Percent In Megabytes Maximum File Size Unimed to (MB) I Unimed OK Cancel	e:Program Files (x86)/Common Files\Symantee: Shared\S c:\Program Files (x86)/Common Files\Symantee: Shared\S
Progress <		>
New Y		Add Remove

- 1116 43. On the left, under **select a page**, select **Options**.
- 1117 44. Set Collation to Latin1\_General\_CS\_AI.
- 1118 45. Set **Recovery model** to **Simple**.
- 1119 46. Under **Other Options > Miscellaneous** set **ANSI NULL Default** to **True**.
- 1120 47. Click **OK.**

New Database				—	$\times$
Selectapage 🖋 General	🖵 Script 🔻 😯 Help	,			
& Options					
🔑 Filegroups	Collation:	Latin1_General_CS_AI			$\sim$
	Recovery model:	Simple			~
					~
	Compatibility level:	SQL Server 2012 (110)			
	Containment type:	None			~
	Other options:				
	2↓ 📼				
	Default Cursor		GLOBAL		
	✓ FILESTREAM		GEOBAL		^
	FILESTREAM DI				
		on-Transacted Access	Off		
	Misc				
	AllowScripting		True		
	Hide File Settings		False		
	<ul> <li>Miscellaneous</li> </ul>				
	Allow Snapshot Is		False		
	ANSI NULL Defa		True		$\sim$
	ANSI NULLS En		False		
-	ANSI Padding Er		False		
Connection	ANSI Warnings E		False		
Server:	Arithmetic Abort E		False		
WIN-RUQD07KL8A7\SCSP	Concatenate Nul		False False		
Connection:	Data Campletian (	Ownership Chaining Enabled Optimization Enabled	False		_
WIN-RUQD07KL8A7\Administrate	Is Read Committee		False		
View connection properties	Numeric Round-/		False		
YT view connection properties	Parameterization		Simple		
	Quoted Identifier		False		
	Recursive Trigge	rs Enabled	False		
_	Trustworthy		False		~
Ready Ready	ANSI NULL Default	ł			

1122 48. In the **Object Explorer**, right click on your database and select **New Query**.



1123

1124 49. Type out the following query:

1125

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

- 1126 50. Click **Execute** in the toolbar above the **SQL Query** window.
- 1127 51. Under the SQL Query window, in the Messages window, verify the command was completed1128 successfully.

SQLQuery1 sql - WIN-RUQDO7KL8A7\S File Edit View Query Project To	CSP.master (WIN-RUQDO7KLBA7\Administrator (134))* - M bols Window Help	krosoft SQL Server Management Studie	e (A., Quick Laurch (Ctrl+Q)	- ۹		×
	New Query 희교요요요요 ★ 라리 ? - ▶ Execute = ✔ 28 륨 🖬 26 등 위 최종,		• \$\$ \$\$ \$\$ \$.			
Chijest Explorer + 9 × Chijest Explorer + 9 × Chijest Explorer = 0 With RUDCO/DIALAT/CSCB (SGI Scever 1 = 0 School - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 -	SOLOuey1.sql - WL_dministrator (134))* = × ALTER DATABASE [TE_DB]		SNAPSHOT ON		•	
۲	150 %	WIN-RUQDO7KEA7-SCSP (11.0	WIN-RUQDO7KIBA7VAdminimeete	00:00:00	0 гол	Ars

- 1130 52. Clear the **SQL Query** window, and then type out the following query.
- 1131 SELECT name, is\_read\_committed\_snapshot\_on FROM sys.databases WHERE
  1132 name='<db\_name>'
- 1133 53. Click **Execute** in the toolbar above the **SQL Query** window.
- 1134 54. Under the **SQL Query** window, in the **Messages** window, verify the **value for**
- 1135 **is\_read\_committed\_snapshot\_on** is set to **1**.

File Edit View Query Project Too	SP master (WNH-BUQDO7KUBA7Ndministrator (134)* - Microsoft SQL Server Management Studie (A., Quick Launch (Oth-Q) ア - □ bis Window Help New Outry 高会会会会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会社会	×
Chyles Lipscher Connect * * * * Connect * * * Connect * * * Connect * * * Connect * Co	SOLOuery1.sql - WL_dministrator (134))* @ ×	* * *
< >	Query executed successfully. WIN-RUQDO7KL8A7\SCSP [11.0 WIN-RUQDO7KL8A7\Admini master 00:00:00 1 rows	

1137 55. In the **Object Explorer**, expand the selection for your database, expand the **Security** section, right
1138 click on **Logins**, and select **New Login...**

Solution1	- Microsoft SQL Server	Management Studio (Administrator)	Quick Launch (Ctrl+Q) 🔑 🗕 🗖	×
File Edit Vi	ew Project Tools	Window Help		
0.0	3 • 15 • 🗳 🗎 🝟	• 鳥 New Query 鳥泉泉泉泉泉 X 市台 フ・マー 図 🍠	· . * =	
[ 4 4 ] me		· > Lecule = V업륨리 [안업란] 티라리 ( = 3   4 관   4 .		
Object Explorer		φ x		
Connect - ¥	*# = ¥ C ++			
E B WIN-RUQD	O7KUBA7\SCSP (SQL S	erver 1		
🖃 🗮 Database				
🗄 🗯 System				
E desc_u				
III @ SCSPD	6			
E TE_DB				
E = Security	Lange and the second			
li = Serve	New Login_			
E Gred	Filter			
🗄 🖷 Server	Start PowerShell			
🔠 💷 Replica	Reports I			
🗄 🖷 Manag	Refresh			
E 🗉 Xévent	Normer			
¢		3		
T Ready				

- 1140 56. On the left, under **Select a page**, select **General**.
- 1141 57. Create a **Login name**.

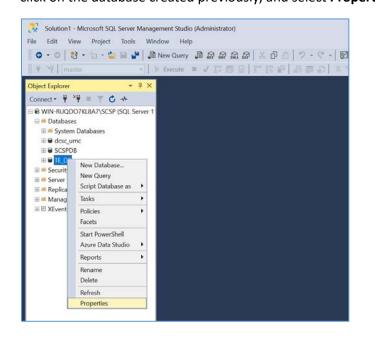
- 1142 58. Select **SQL Server authentication**.
- 1143 59. Create a **password**.
- 1144 60. For **Default database**, select the database previously created.
- 1145 61. For **Default language**, select **English**.

Login - New			—		$\times$
Select a page	🖵 Script 🔻 😮 Help				
General     Server Roles     User Mapping     Securables     Status	Login name: Windows authentication SQL Server authentication Password: Confirm password: Specify old password Old password: Enforce password policy Enforce password expirat User must change password Mapped to certificate	tion			Search
Server: WIN-RUQDO7KL8A7\SCSP	Mapped to asymmetric key			$\sim$	
Connection: WIN-RUQDO7KL8A7\Administrato	Map to Credential			~	Add
	Mapped Credentials	Credential	Provider		
Progress					Remove
Ready	Default database: Default language:	TE_DB English		>>1 >>1	
	1		0	К	Cancel

- 1147 62. On the left, under **Select a page**, select **User Mapping**.
- 1148 63. Under the Users mapped to this login window, perform these actions for the row containing thepreviously created database:
- a. Check the box in the **Map** column.
- b. In the **Default Schema** column, type the name of the new user being created.
- 1152 64. Click **OK**.

Select a page			_		
General	<b>T</b> a	Script	🔻 🕜 Help		
<ul><li>Server Roles</li><li>User Mapping</li></ul>	Use	ers ma	pped to this login:		
<ul> <li>Securables</li> <li>Status</li> </ul>	N	lap	Database	User	Default Schema
			desc_ume		
			master		
			model		
			msdb		
			SCSPDB		
		$\checkmark$	TE_DB	te_admin	te_admin
			tempdb		
Connection					
Server:			st account enabled for:		
Server: WIN-RUQDO7KL8A7\SCSP	Dat	tabase	e role membership for: Ti		
		tabase	e role membership for: Tl accessadmin		
Server: WIN-RUQD07KL8A7\SCSP Connection: WIN-RUQD07KL8A7\Adminis	strate	tabase db_ db_	e role membership for: Ti		
Server: WIN-RUQDO7KL8A7\SCSP Connection:	strate	abase db_ db_ db_ db_	e role membership for: Tl accessadmin backupoperator datareader datawriter		
Server: WIN-RUQD07KL8A7\SCSP Connection: WIN-RUQD07KL8A7\Adminis	strate	abase db_ db_ db_ db_ db_	e role membership for: Tl accessadmin backupoperator datareader datawriter ddladmin		
Server: WIN-RUQD07KL8A7\SCSP Connection: WIN-RUQD07KL8A7\Adminis	strate	tabase db_ db_ db_ db_ db_ db_ db_	e role membership for: Ti accessadmin backupoperator datareader datawriter ddladmin denydatareader		
Server: WIN-RUQD07KL8A7\SCSP Connection: WIN-RUQD07KL8A7\Adminis	strate	abase db_ db_ db_ db_ db_ db_ db_ db_	e role membership for: Ti accessadmin backupoperator datareader datawriter ddladmin denydatareader denydatawriter owner		
Server: WIN-RUQDO7KL8A7\SCSP Connection: WIN-RUQDO7KL8A7\Adminis	strate	abase db_ db_ db_ db_ db_ db_ db_ db_	e role membership for: Ti accessadmin backupoperator datareader datamiter ddladmin denydatamiter denydatawriter owner securityadmin		

1154 65. In the **Object Explorer**, expand the selection for your database, expand the **Databases** section, right
 1155 click on the database created previously, and select **Properties**.



- 1157 66. On the left, under **select a page**, select **Permissions**.
- 1158 67. Under **Permissions for user**, check the box in the **Grant** column for the following permissions:
- 1159 **Connect**
- 1160 Create Function
- 1161 Create Procedure
- 1162 Create Table
- 1163 Create View
- 1164 **Delete**
- 1165 Insert
- 1166 Select
- 1167 **Update**
- 1168 68. Click **OK**.

冒 Database Propert	ies - TE_DB					_			$\times$
Select a page General	🖵 Script 🔻 😯 Help	)							
<ul> <li>Files</li> <li>Filegroups</li> <li>Options</li> </ul>	Server name: View server permissio	ns	WIN-RU	IQDO7	KL8A7	\SCSP			
<ul> <li>Change Tracking</li> <li>Permissions</li> <li>Extended Properties</li> </ul>	Database name:		TE_DB						
Extended Properties	Users or roles:							Sea	arch
	Name							Туре	
	🛔 te_admin							User	
Connection Server: WIN-RUQDO7KL8A7\SCSP	Permissions for te_adm	in:							
Connection:	Explicit Effective								
WIN-RUQDO7KL8A7\Administrate	Permission	Grantor		Gra	nt	With	ı	Deny	~
View connection properties	Connect replicati								
	Connect	dbo			/				
	Control								
Progress	Create aggregate								
Ready	Create assembly Create asymmetri								
Post Post	Create certificate								~
						[	0	К	Cancel

- 69. Open Internet Explorer and navigate to the webpage of the server on which Tripwire Enterprisewas installed.
- 1172 70. Enter the **services password** created during the install process.
- 1173 71. Click **Login**.

Tripwire Enterprise needs additional configuration.         To finish installing, please enter your Services Passphrase for authentication. The Services Passphrase was created when you installed Tripwire Enterprise.         Services Passphrase:	Tripwire Enter	prise Post-Install Configuration		
Services Passphrase:		• • • • • • • • • • • • • • • • • • •		
			when you installed Tripwire Enterprise.	

- 1175 72. Under **Database Configuration Settings**, provide the information that follows:
- 1176 Remote Database Type: Microsoft SQL Server 1177 Authentication Type: SQL Server 1178 Login Name: te admin Password: \*\*\*\*\*\*\*\* 1179 1180 Database Host: WIN-RUQDO7KL8A7 1181 Database Name: TE\_DB 1182 Instance Name: SCSP (Note: this may not be necessary, depending on how your SQL Server 1183 Database is configured)
- 1184 SSL: Request

atabase Configuration Setti	ngs
nese settings control how the TE Con ake any necessary changes in the fie	sole connects to a remote database that stores data for all TE operations. You can check the current configuration here, and Ids below.
Remote Database Type: Microsoft SQL Server V	Remote Database Type: The type of remote database used by TE.
Authentication Type:	
SQL Server	Authentication Type: Specifies whether the database login should authenticate using a Windows account (typica of the format domaintuser), 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 wi 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)	<b>Port:</b> 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 the 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:	SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate

- 1186 73. Click **Test Database Login** and verify the connection is successful.
- 1187 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)	<b>Port:</b> 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 ) ✓	
Connection Succeeded.	
Tripwire Enterprise 8.7.3.b8.7.3.r201901111	22005-03196dc.b24 Save Configuration and Restart Console Logout

- 1188
- 1189 75. Wait for Tripwire Enterprise to restart and redirect you to the log in 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.
1190	

- 1191 76. Enter the **services password** created during the install process.
- 1192 77. Click **Login**.



1194 78. Under Create Administrator Password, create a password for the Tripwire Enterprise administrator1195 account.

### 1196 79. Click **Confirm and Continue**.

nfiguration Steps Needed:	
Tripwire administrator account password needs to be changed from the	) default.
eate Administrator Password	
Passwords must:	Password:
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 information about your system and this installation. Attach the support bundle file to
Contact Tripwire Support: https://secure.tripwire.com/customers/contact-support.cfm	your web ticket or email. What is a Support Bundle? Generate Support Bundle
Or open a Support ticket: https://secure.tripwire.com/customers/	

- 1198 80. Enter the **username** and **password** for the Tripwire Enterprise administrator account.
- 1199 81. Click Sign In.

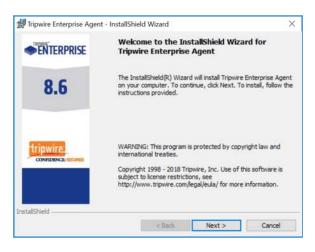


1201 82. Click **Configure Tripwire Enterprise** to begin the configuration process.



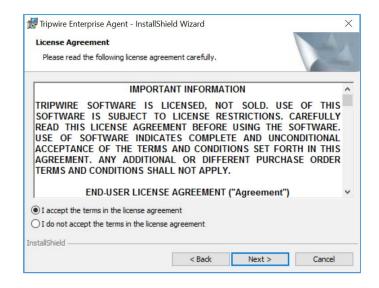
1202

- 1203 Tripwire Enterprise Agent Installation
- 1204 1. Run te\_agent.msi.
- 1205 2. Click **Next >**.

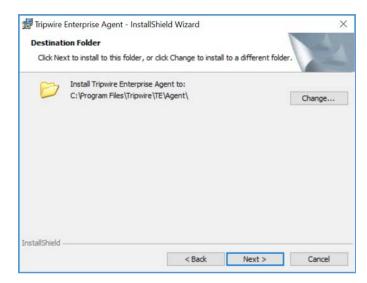


### 1207 3. Check I accept the terms in the license agreement.

#### 1208 4. Click Next >.



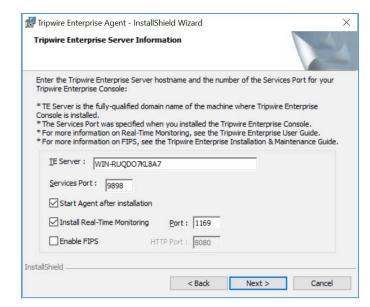
- 1210 5. Specify an install directory for the Tripwire Enterprise Agent.
- 1211 6. Click Next >.



1212

- 1213 7. Enter the **TE Server** (e.g., **WIN-RUQDO7KL8A7**) of the server where Tripwire Enterprise is installed.
- 1214 8. Enter **9898** as the **Services Port** established during the installation process of Tripwire Enterprise.
- 1215 9. Check **Start Agent**, after installation.

- 1216 10. Check **Install Real-Time Monitoring** and specify a **Monitoring Port**.
- 1217 11. Uncheck Enable FIPS.
- 1218 12. Click **Next** >.



- 1220 13. Specify a **Proxy Host** and **Proxy Port** if necessary.
- 1221 14. Click **Next >**.

E	nterprise Server	, enter the T		ommunicate with the Tripwire ostname and port number for your
P				
	Proxy <u>H</u> ost:	-		(leave blank for no proxy)
	Proxy Port:		(leave blank for default)	

1219

1223 15. Enter the **Services Password** created during the installation process for Tripwire Enterprise.

1224 16. Click **Next >**.



### 1225

### 1226 17. Click Install.

			100
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 settin	ngs, <mark>click Back. Click</mark>	Cancel to

- 1227
- 1228 18. Wait for the installation process to complete.

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

### 1230 19. Click **Finish**.

🚼 Tripwire Enterprise Agen	t - InstallShield Wizard	×
♦ ENTERPRISE	InstallShield Wizard Completed	
8.6	The InstallShield Wizard has successfully installed Tripwire Enterprise Agent. Click Finish to exit the wizard.	
InstallShield	< Back Finish Cancel	

## 1231

# 1232 2.6 Enterprise Domain Identity Management

# 1233 2.6.1 Domain Controller with AD, DNS, & DHCP

1234 Within the PACS architecture, we established a Windows Server 2012 R2 Domain Controller to manage

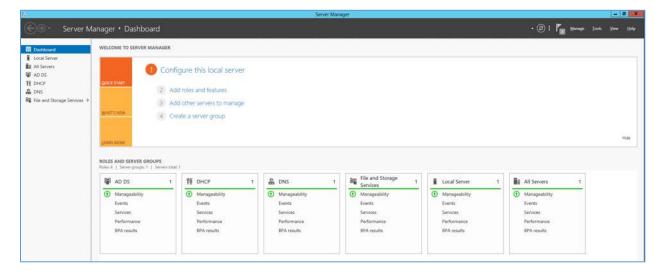
AD, DNS, and Dynamic Host Configuration Protocol (DHCP) services for the enterprise. The followingsection details how the services were installed.

### 1237 System Requirements

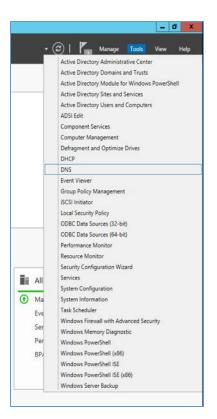
- 1238 **CPU**: 1
- 1239 Memory: 4 GB Ram
- 1240 Storage: 120 GB (Thin Provision)
- 1241 **Operating System**: Microsoft Windows Server 2012 R2
- 1242 Network Adapter: VLAN 1201
- 1243 Enterprise Domain Services Installation
- 1244 Install the Domain Controller, AD, and DNS appliances according to the instructions detailed in *Building*
- 1245 Your First Domain Controller on 2012 R2 [12].

### 1246 DNS Server Forward Lookup Zone Configuration

1247 1. Open Server Manager.



- 1249 2. In the top right, click on **Tools > DNS**.
- 1250 3. DNS forward lookup zone should have already been created during the DNS setup process
- 1251 performed previously. If not, follow these instructions:



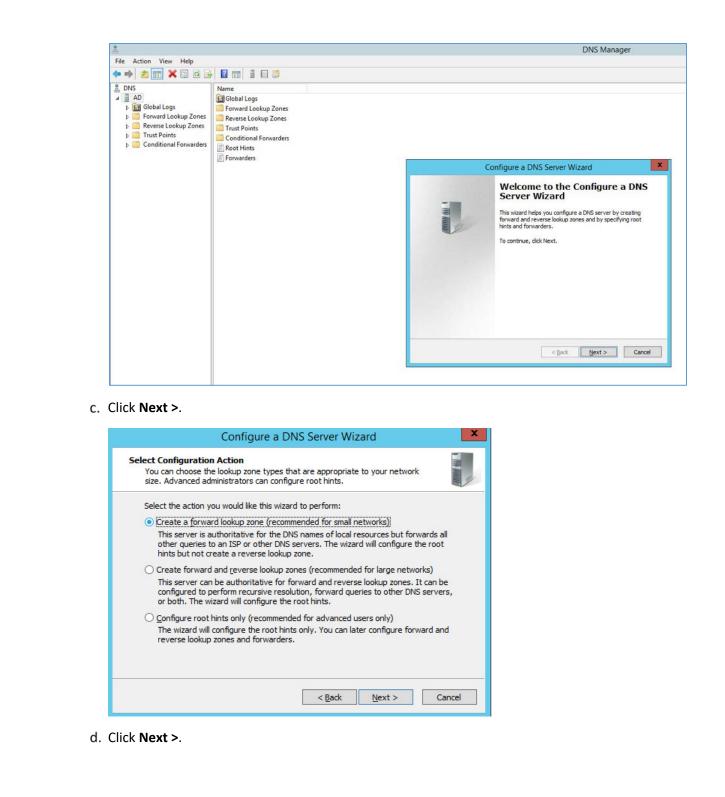
1253

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

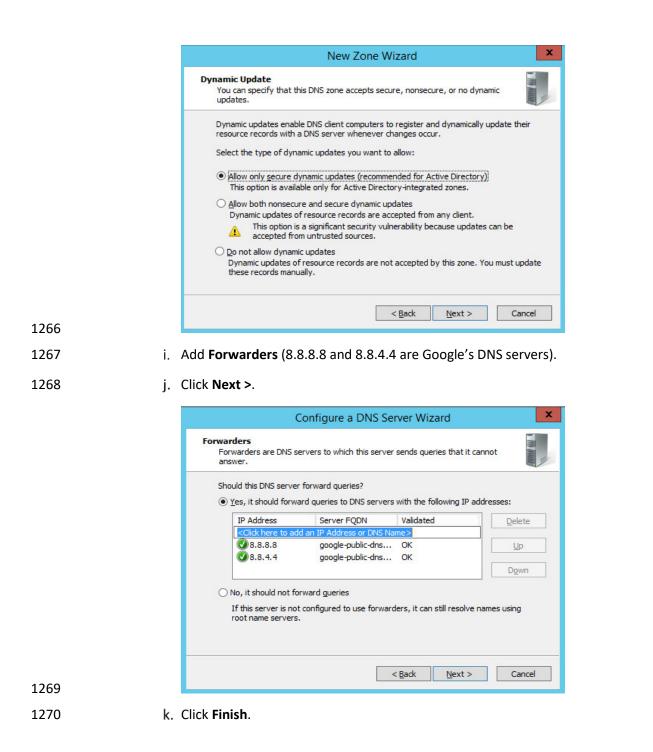
- => 2	📰 🗙 🖾 🛛	8 🛃 🛛 🖬 🗎 🗐 🖏		
DNS AD		Name Right Loss		
	Create Default New Zone Set Aging/Sca Scavenge Stale Update Server Clear Cache	Set Aging/Scavenging for All Zones Scavenge Stale Resource Records Update Server Data Files		
	All Tasks		•	
	View		•	
	Delete Refresh Export List			
	Properties			
	Help			

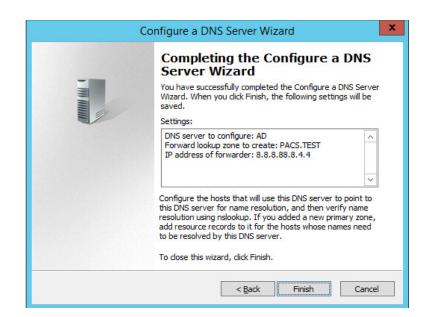
1254 1255

b. 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?
	This server maintains the zone The wizard will help you create a primary forward lookup zone.
	An 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.
1260	< <u>B</u> ack <u>N</u> ext > Cancel
1261	e. Enter <b>PACS.TEST</b> as the <b>Zone name</b> , that was established previo
1262	f. Click Next >.
1202	
	New Zone Wizard
	New Zone Wizard     X       Zone Name What is the name of the new zone?     Image: Constraint of the new zone
	Zone Name
	Zone Name       Image: Second Se
	Zone Name       Image: Second Se
	Zone Name       Image: Second Se
1263	Zone Name       Image: Second Se
1263 1264	Zone Name       Image: Control of the new zone?         What is the name of the new zone?       Image: Control of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com), or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.         Zone name:       PACS.TEST





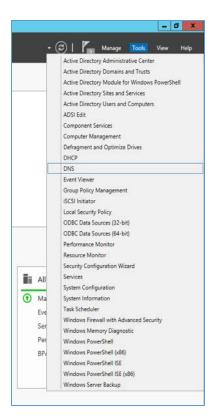
### 1272 DNS Server Reverse Lookup Zone Configuration

1273 1. Open Server Manager.

6			Server Ma	nager			- 5
) - Server M	anager • Dashboard					• 🗇   🍢 Managar Ioc	ts Yew H
	WELCOME TO SERVER MANAGER						
田 Darkhowd     Local Servers     Local Servers     Al Servers     W AD DS     TE DHCP     DHCF     DHS     Ticle and Storage Services. ト	Quick stant 2 Adde 3 Adde	gure this local server troles and features to ther servers to manage ate a server group					Hide
	AD DS 1 Managesbility Events Services Performance BPA results	TE         DHCP         1           Image: Auropeability         Events         Services           Performance         BPA results	DNS 1 Manageubiny Events Services Performance BPA results	File and Storage 1 Services 1 Manageability Events Services Performance BPA results	Local Server 1 Managasbility Events Services Performance BPA results	All Servers 1 Managesbility Events Services Performance BPA results	

1274

1275 2. In the top right, click on **Tools** > **DNS**.

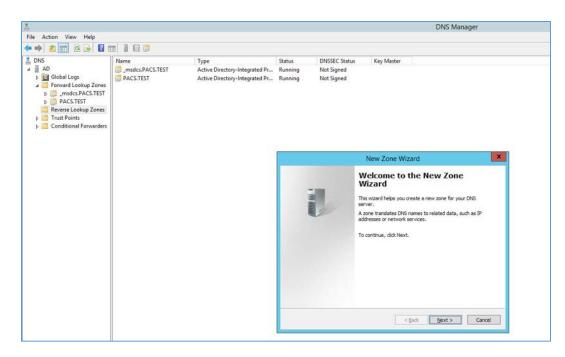


1278

1277 3. Right click on **Reverse Lookup Zones** folder and select **New Zone...** 

• 🔿 🖄 🕅 🧔	11	Name	Туре	Status	DNSSEC Status	Key Master	
AD AD		_msdcs.PACS.TEST	Active Directory-Integrated Pr	Running	Not Signed	Key Master	
b Global Logs							
Global Logs Global Logs Global Lookup Zones		PACS.TEST	Active Directory-Integrated Pr	tive Directory-Integrated Pr Running Not Sig	Not Signed		
p _msdcs.P							
p S PACS.TE							
Reverse Look							
p Trust Poir	New Zone.						
p Condition							
	Refresh						
	Help						

1279 4. Click Next >.



#### 1281 5. Click Next >.

Zone Type The DNS server supports various	types of zones and storage	
The Divo server supports various	s types of zones and storage.	
Select the type of zone you wan	t to create:	
Primary zone		
	at can be updated directly on this server.	
O Secondary zone		
	at exists on another server. This option help y servers and provides fault tolerance.	os balance
○ St <u>u</u> b zone		
	ntaining only Name Server (NS), Start of Au at (A) records. A server containing a stub zo	
Store the zone in <u>A</u> ctive Direct controller)	tory (available only if DNS server is a write	able doma
	< Back Next >	Can



1282

6. Click **Next >**.

INC	ew Zone Wizard
Active Directory Zone Replicatio You can select how you want DNS	on Scope S data replicated throughout your network.
Select how you want zone data re	eplicated:
O To all DNS servers running on	domain controllers in this forest: PACS.TEST
• To all DNS servers running on	domain controllers in this domain: PACS.TEST
<ul> <li>To all domain controllers in this</li> </ul>	s domain (for Windows 2000 compatibility): PACS.TEST
	s domain (for windows 2000 compatibility), PACS, TEST
O To all domain <u>controllers</u> specified	fied in the scope of this directory partition:
	,
	< Back Next > Cancel

1285 7. Choose Internet Protocol version 4 (IPv4), **IPv4 reverse Lookup Zone** option and click **Next** >.

New Zone Wizard
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

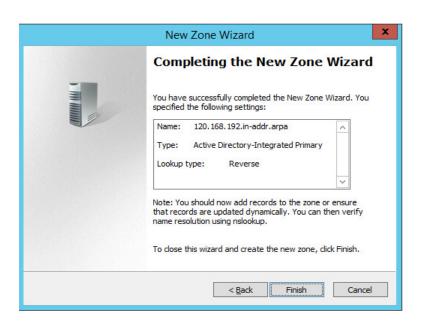
- 1287 8. Establish which IP addresses should be included in reverse lookup (the example above
- 1288 encompasses all devices in the **192.168.120.0/24** subnet), then click **Next** >.

	and a state of the second s
Reverse Lookup Zone Name A reverse lookup zone translates IP a	ddresses into DNS names.
To identify the reverse lookup zone, t Network ID:	ype the network ID or the name of the zone.
192 .168 .120 .	
The network ID is the portion of the network ID in its normal (not rever	ne IP addresses that belongs to this zone. Enter the rsed) order.
	D, it will appear in the zone name. For example, 10.in-addr.arpa, and network ID 10.0 would create
network ID 10 would create zone	
network ID 10 would create zone zone 0.10.in-addr.arpa.	

1290 9. Choose Allow only secure dynamic updates (recommended for Active Directory) option and then
 1291 click Next >.

Dynamic Up	date				
You can supdates.		DNS zone acce	pts secure, nonse	ecure, or no dynam	nic
			puters to register never changes o	and dynamically up ccur.	odate their
Select the	e type of dynami	ic updates you	want to allow:		
			recommended for e Directory-integ		
	both nonsecure				
Dyna			s are accepted fr	om any client. because updates c	an he
4	accepted from u				ande
	t allow dynamic u	2.0 K			
	nic updates of re records manuall		s are not accepte	d by this zone. You	ı must upda
		* ×			
			- Park	Nexts	
			< <u>B</u> ack	Next >	Cance

1293 10. Click **Finish**.



### 1295 DHCP Server Installation

1296 Install the DHCP server according to the instructions detailed in *Installing and Configuring DHCP Role on* 

1297 Windows Server 2012 [13].

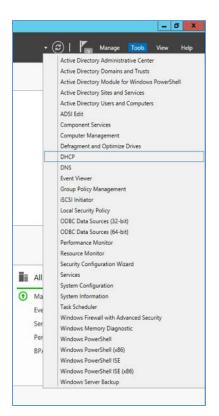
### 1298 DHCP Server Configuration

1299 1. Open Server Manager.

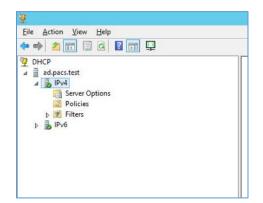
			Server Man	iger			-
)⊙ - Server №	lanager • Dashboard					• 🗇   🎢 Manage 3004	
Dashboard	WELCOME TO SERVER MANAGER						
Excert Server     Excert Server     W AD DS     Vor     AD DS     T1 OFCP     AD     OFS     Re and Storage Services     P	QUECK START 2 AC 3 AC	igure this local server Id roles and features Id other servers to manage eate a server group					
	aD DS 1	Î∰ DHCP 1	DNS 1	File and Storage	Local Server 1	All Servers 1	
	Manageability     Events     Services	Manageability     Events     Services     Performance	Manageability     Events     Services     Performance	Manageability     Events     Services     Performance	Manageability     Events     Services     Performance	Manageability     Events     Services     Performance	

1300

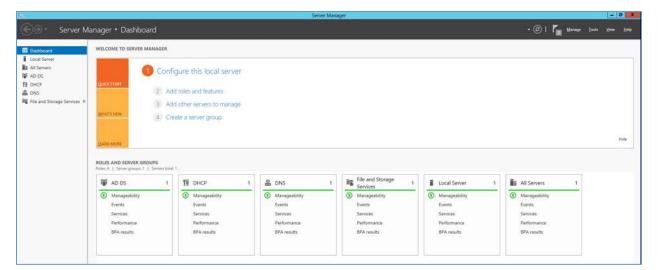
1301 2. In the top right, click on **Tools** > **DHCP**.



1303 3. If you see a green checkmark on the **IPv4** server, the DHCP server is up and running.



- 1305 DHCP Scopes Configuration
- 1306 *Performed on Windows Server 2012 R2.*
- 1307 1. Open Server Manager.



1309

### 2. In the top right, click on **Tools > DHCP**.



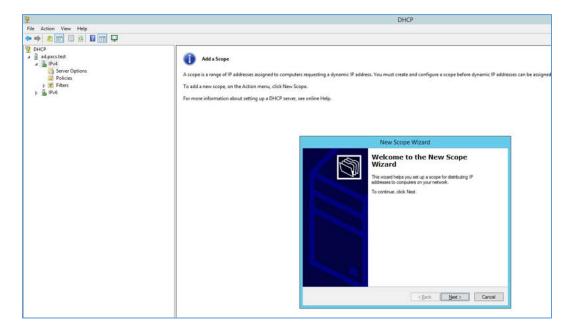
1310

1311 3. Right click on IPv4 and select New Scope...

		DHCP				
tion	View Help					
2 10						
pacs.te		Add a Scope				
IP.ut.	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 assigned				
IP	New Multicast Scope	To add a new scope, on the Action menu, click New Scope.				
	Configure Failover Replicate Failover Scopes	For more information about setting up a DHCP server, see online Help.				
	Define User Classes Define Vendor Classes					
	Reconcile All Scopes					
	Set Predefined Options					
	View					
	Refresh					
	Properties					
	Help					

1314

### 1313 4. Click Next >.



- 1315 5. Provide a Name as Radiology Devices and a Description as Collection of hospitals Radiology
  1316 equipment in the New Scope Wizard.
- 1317 6. Click Next >.

	New Scope Wizard
Scope Name You have to pr a description.	ovide 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.
Name:	Radiology Devices
Description:	Collection of hospitals Radiology equipment
	< <u>B</u> ack <u>N</u> ext > Cancel

- 1319
  7. Establish the IP range (192.168.120.200 192.168.120.254) from which the DHCP server should
  1320 hand out IPs for devices in this scope.
- 1321 8. Click **Next >**.

Configuration settings	for DHCP Server
	dresses that the scope distributes.
Start IP address:	192 . 168 . 120 . 200
End IP address:	192 . 168 . 120 . 254
Configuration settings	that propagate to DHCP Client
100 Cont	24
Length:	
Length: Subnet mask:	255.255.255.0
	255 . 255 . 255 . 0
	255 . 255 . 255 . 0

1323 9. Click **Next >**.

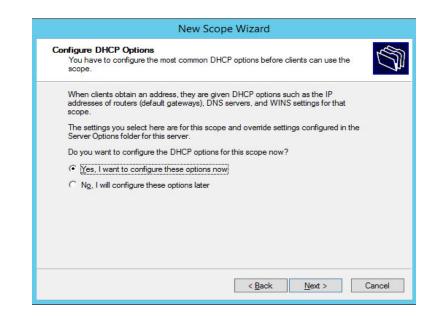
New Scope Wizard
es or a range of addresses that are not distributed by the ne duration by which the server will delay the transmission of a
nge that you want to exclude. If you want to exclude a single is in Start IP address only. End IP address:
Add
Remoye Subnet delay in milli second:
< <u>B</u> ack <u>N</u> ext > Cancel

1325 10. Configure preferred Lease Duration (e.g., 8 days), and click Next >.

	New Scope Wizard
Lease Duration The lease of	on duration specifies how long a client can use an IP address from this scope.
connected portable co Likewise, fo locations, k	tions should typically be equal to the average time the computer is to the same physical network. For mobile networks that consist mainly of imputers or dial-up clients, shorter lease durations can be useful. or a stable network that consists mainly of desktop computers at fixed onger lease durations are more appropriate. ation for scope leases when distributed by this server.
Limited to:	
Days:	Hours: Minutes:
	< <u>B</u> ack <u>N</u> ext > Cancel

## 1326

1327 11. Choose **Yes, I want to configure these options now**, and then click **Next >**.



- 1329 12. Enter the subnet's **Default Gateway** as **192.168.120.1**.
- 1330 13. Click **Add**.

You can specify the routers	s, or deradit gatew	ays, to be distribut	ed by this scope.	
To add an IP address for a IP address:	router used by cli	ents, enter the add	lress below.	
192 . 168 . 120 . 1	Add			
	Remove			
	Up			
	Down			
		< Back	Next >	Can

1332 14. Click **Next** >.

To add an IP address for IP address:	a router used by client	s, enter the addr	ess below.	
	Add			
192.168.120.1	<u>R</u> emove			
	<u>U</u> р			
	Down			

- 1334 15. Ensure IP address in bottom-right box is the IP address (192.168.120.101) for the DNS server1335 configured earlier.
- 1336 16. Click **Next >**.

	New Sco	ope Wizard	
Domain Name and DN The Domain Name Sy on your network.		d translates domain nar	nes used by clients
You can specify the parent DNS name resolution.	t domain you want the	e client computers on y	our network to use fo
Parent domain: PACS.T	EST		
To configure scope clients servers.	to use DNS servers		the IP addresses for t
Server name:		IP address:	
			Add
	R <u>e</u> solve	192.168.120.101	Add
	R <u>e</u> solve		

1338 17. Click **Next >**.

/INS Servers Computers running Windows can use WI names to IP addresses.	NS servers to convert NetBIOS	computer
Entering server IP addresses here enable broadcasts to register and resolve NetBIC	)S names.	IS before they use
Server name:	I <u>P</u> address:	Add
R <u>e</u> solve		<u>R</u> emove
		Up
		Down
To change this behavior for Windows DH Type, in Scope Options.	CP clients modify option 046, V	
Type, in Scope Options.		

1340 18. Choose **Yes, I want to activate this scope now** option and then click **Next >**.

New Scop	e Wizard	
Activate Scope Clients can obtain address leases only if a sco	pe is activated.	Ŕ
Do you want to activate this scope now?		
<ul> <li>Yes, I want to activate this scope now</li> </ul>		
O No, I will activate this scope later		

### 1342 19. Click **Finish**.

New Scope Wizard
Completing the New Scope Wizard You have successfully completed the New Scope wizard.
To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover. To close this wizard, click Finish.
< Back Finish Cancel

- 1344 20. Scope should appear under IPv4 dropdown. Ensure Scope Options are correctly established with
   1345 these values:
- **1346 003 Router**: 192.168.120.1
- 1347 **006 DNS Servers**: 192.168.120.101
- 1348 015 DNS Domain Name: PACS.TEST

2				DHCP
<u>File Action View H</u> elp				
* 🔿 🙍 🕢 🙆 🖌				
2 DHCP	Option Name	Vendor	Value	Policy Name
ad.pacs.test	E 003 Router	Standard	192.168.120.1	None
4 🐻 IPv4	006 DNS Servers	Standard	192.168.120.101	None
Address Pool     Server Options     Server Options     Policies     Policies	2 015 DNS Domain Name	Standard	PACS.TEST	None

1349

# 1350 2.6.2 DigiCert PKI

- 1351 DigiCert is a cloud-based platform designed to provide a full line of SSL certificates, tools, and platforms,
- 1352 for optimal certificate life-cycle management. To use the service, an account must be established with
- 1353 DigiCert. Once an account is established, access to a DigiCert dashboard is enabled. From the dashboard,
- 1354 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.

1356 The instructions below describe the process used to obtain an SSL certificate on behalf of medical

1357 devices using the DigiCert certificate signing services.

## 1358 Create CSR

A CSR is represented as a block Base64 encoded 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, and country. It also contains the applicant's private key and the public key pair. 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 the device to generate a CSR. Below is an instruction on how to use the Certificate Utility for Windows (*DigiCertUtil.exe*) provided

- 1365 by DigiCert to generate CSRs for a medical device or a server.
- 1366 Download and save the *DigiCertUtil.exe* from the DigiCert site [14].
- 1367 1. Double-click DigiCertUtil.exe to run the utility.
- 1368 2. Click the **Create CSR** link to open a CSR request window.
- 1369 3. On the Create CSR window, fill in the key information (some of the information is optional).
- 1370 Certificate Type: Select SSL
- 1371 Common Name: HYLAND-VNA.pacs.hclab
- 1372 Subject Alternative Names: HYLAND-VNA.pacs.hclab
- 1373 **Organization**: NIST-NCCoE
- 1374 Department: HCLAB
- 1375 City: Rockville
- 1376 State: Maryland
- 1377 Country: USA
- 1378 Key Size: 2048
- 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.*

ertificate 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:	HYLAND-VNA.pacs.hclab	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
Organization:	NIST-NCCoE	store.
Department:	HCLAB	
City:	Rockville	
State:	Maryland	v
Country:	USA	v
Key Size:	2048	×

1383 5. A sample CSR is shown in the figure below:

Digicert Certificate Util	ty for Windows©	- Renew Certificate	2	
0	The certificate re	quest has been succe	ssfully created.	
************************************	AFB_01748_27C116c1 419191681. DTTTTC1C58.VC7002C4.007011 BD11Na.0491911092114000369 BD11Na.0491911092114000369 Noresg3037142898271916308 DM129210110208351871910056 DM1292101110208351871910056 DM129210111020835187191005 DM129210110101101101010101010 DM1292011110208371201005 DM129211421/11080920319051905 DM129211421/11080920319051905 DM129211421/11080920319051905 DM129211421/11080920319051905 DM129211421/11080920319051905 DM2002015110500500071310050 DM20020151105005007130050 DM200201511050050007130050 DM200201511050050007130050 DM200201511050050007130050 DM200201511050050007130050 DM200201511050050007130050 DM200201511050050000000000000000000000000			
		Copy CSR	Save to File	Close

1384

13856. Select and copy the certificate contents to the clipboard or save it to an ascii text file. The text1386contents will be used to paste into the DigiCert order form.

1387	<ol> <li>Issue Signed Certificates. With a created applicant CSR, request a signed certificate using DigiCert</li></ol>
1388	CertCentral portal, using these steps:
1389 1390 1391	a. 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, select Private SSL to open a certificate request form.
1392	b. Paste the CSR information to the area called Add Your CSR, including theBEGIN NEW
1393	CERTIFICATE REQUEST andEND NEW CERTIFICATE REQUEST tags. Once the
1394	pasting is done, some of the fields will be populated automatically.
1395	c. After filling in all the required information, scroll down to the bottom of the page, and select
1396	the I Agree to the Certificate Services Agreement Above checkbox. Next, click the Submit
1397	Certificate Request button at the bottom of the form to submit the certificate for signing
1398	approval.

File Edit View Fav	vorites Tools Help	
Ødigicert*   CERTCENTRAL*	Enterprise	
REQUEST A CERTIFICATE	Ability a Product Request Private SSL Certificate For National Institute of Standards and Technology	
CERTIFICATES  Orders  Requests  Domains	Certificate Settings Add Your CSR ? Click to upload a CSR or paste one below	
Organizations Expiring Certificates Certificate Authority Teen	samplipert librate in altera supervariant ter schempenggengengengengen scheftigenen supervariant en schempenggengengengengengengengengengengengeng	
() FINANCES	Common Name +Show Recently Created Domains	
ACCOUNT	HYLAND-MAR pacs holds Com and www.[your-domain].com in the certificate	
SETTINGS	Validityperiod ○ 1 year	
م TOOLS	2 years     3 years     Oustom expiration date     Oustom length Important! After February 20, 2010, Dig/Cett will no longer offer 3-year public 35L/TLS certificates. For more informatic     Additional Certificate Options      Organization	n about this change, <b>dick here</b> .
	Organization Info :  INST-NCOSE Infor 320 Voldand 9700 Great Seneca Hwy Rod-Ville, MD, US 20850 301-975-0212	
	Contacts	
	Organization Contact	

1400 8. The certificate is listed under **Orders**. Once the order status changes to Issued, the certificate is1401 ready for download.

	NTRAL <sup>®</sup> Enterprise						iology + Kangmin Zheng + 📞 📼 (
REQUEST A CERTIFICATE	Orders						
I DASHBOARD	Request a Certificate +	Orders Fleport	Download CSV =				
) CERTIFICATES							
Orders Requests	Status	Search	Go Show Advanced Search				
Domains Orgenizations	Order # 👻	Date 🕀	Common Name 🗢	Status 🕆	Validity 🕀	Product 0	Expires ‡
	6225463   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.hclab	Issued	3 years	Private SSL	04 Jun 2020
	5655577   Quick View	24 Apr 2019	HYLAND-PGCORE, pacs. hclab	issued	3 yearn	Private SSL	23 Apr 2020
	5643403   Quick View	23 Apr 2019	HYLAND PGCRE.pacs.htdab	Issued	3 years	Private SSL	22 Apr 2020
FINANCES							

- 1403 9. Click a specific order number to display the certificate details with a list of actions that can be
  1404 performed. Click **Download Certificate As** to download certificates with signed CA and Root CA
  1405 certificates. A variety of certificate formats can be downloaded, such as .crt, .p7b, .pem, etc.
- 1406 10. Save the downloaded certificate in a location where it can be used for further processing if needed.

### 1407 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 Section 2.6.2. Click
   the Next button to import.
- 1415 2. From the DigiCert Certificate Utility for Windows, click **SSL** to list all the imported files.
- 1416 3. To export the certificate, select the certificate you want to export as a combined certificate file and 1417 key file in a .pfx file, or separated as a certificate file and key file, and then click **Export Certificate**.

DigiCert Cert digi <mark>cert</mark>	CERTIFICATE UTILITY IN		<b>C</b> 1.	800.896.79	973		-		
						support@digi	cert.com	Live Chat	
	SSL Certificates		Creat	te CSR 单 Impo	C Refresh				
	Issued To E		Serial Number	Friendly Na	Issuer				
SSL	HYLAND-VNA.pacs 0								
SSL	ISECertByDigiCert 1	18-FEB (	IFU/4/E430	ISECertByD	DigiC				
101									
w de Signing									
ide Signing									
30									
Tools									
Tools									
-									
2									
Account									
	Export Cer	rtificate	Test Key	View	Certificate				
2332								Close	5

1419
4. Click the Next > button and then follow the wizard instructions to save the certificate file and
1420 private key file to a desired location in the device.

S DigiCert Certificate Utility for Windows©	×
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 Include all certificates in the certification path if possible	
O key file (Apache compatible format)	
$\bigcirc$ No, do not export the private key	
< Back Next >	Cancel

1421

# 1422 2.7 Network Control & Security

# 1423 2.7.1 Cisco Firepower

1424 Cisco Firepower, consisting of Cisco Firepower Management Center and Cisco Firepower Threat

1425 Defense, is a network management solution that provides firewall, intrusion prevention, and other

1426 networking services. For this project, Firepower was used to provide network segmentation and both

1427 internal and external routing. Access control and intrusion prevention policies were also implemented.

### 1428 <u>Cisco Firepower Management Center Appliance Information</u>

- 1429 **CPU**: 8
- 1430 **RAM**: 16 GB
- 1431 Storage: 250 GB (Thin Provision)
- 1432 Network Adapter 1: VLAN 1201
- 1433 **Operating System**: Cisco Fire Linux

## 1434 <u>Cisco Firepower Management Center Virtual Installation Guide</u>

- 1435 Install the Cisco Firepower Management Center Virtual appliance according to the instructions detailed
- 1436 in Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide [15].

## 1437 <u>Cisco Firepower Threat Defense Appliance Information</u>

- 1438 **CPU**: 8
- 1439 **RAM**: 16 GB
- 1440 Storage: 48.5 GB (Thin Provision)
- 1441 Network Adapter 1: VLAN 1201
- 1442 Network Adapter 2: VLAN 1201
- 1443 Network Adapter 3: VLAN 1099
- 1444 Network Adapter 4: VLAN 1099
- 1445 Network Adapter 5: Trunk Port
- 1446 **Network Adapter 6**: Trunk Port
- 1447 Network Adapter 7: VLAN 1101
- 1448 Network Adapter 8: VLAN 1101
- 1449 Network Adapter 9: VLAN 1701
- 1450 **Operating System**: Cisco Fire Linux

# 1451 <u>Cisco Firepower Threat Defense Virtual Installation Guide</u>

- 1452 Install the Cisco Firepower Threat Defense Virtual appliance, according to the instructions detailed at
- 1453 Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide [16].

# 1454 Adding Firepower Threat Defense (FTD) Appliance to Firepower Management Center (FMC)

- 1455 1. Log in to the **FMC Console**.
- 1456 2. Navigate to **Devices > Device Management**.
- 1457 3. Click the **Add drop-down** button and select **Add Device**.

	Devices Objects A	MP Intelligence		Deploy 🤑 S	System Help <b>▼ adn</b>
evice Management NAT V	PN V QoS Platform	Settings FlexConfig Cert	ficates		
evice Management					
t of all the devices currently registered	on the Firepower Management	Center.			
fiew By : Group 💌	All (1)   Error (1)   Warr	ning (0)   Offline (0)   Normal (0	)   Deployment Pending (0)	🔍 Search Device	e 🕢 🖓 Add 🗸
lame	Model	Vers Chassis	Licenses	Access Control Poli	<ul> <li>Device</li> </ul>
📁 Ungrouped (1)					O High Availability
					Stack

- 1459 4. Enter **192.168.120.141** as the **IP address** of the FTD appliance.
- 1460 5. Enter **FTD-PACS** as a **display name** to identify the FTD appliance.
- 1461 6. Enter the **manager key** created when configuring the manager on the FTD appliance.
- 1462 7. Click the Access Control Policy drop-down and select Create New Policy.
- 1463 a. Create a **name** for the policy.
- 1464 b. Select Block All Traffic.
- 1465 c. Click Save.
- 1466 8. Under Smart Licensing, check the boxes next to Malware, Threat, and URL.
- 1467 9. Under **Advanced** check the box next to **Transfer Packets**.
- 1468 10. Click **Register**.

		P Intelligence		
Device Management NAT VPN VQoS	Platform Se	ettings FlexConfig	Certificates	
Device Management List of all the devices currently registered on the Firepower M View By : Group All (1)   From /				
	Model	Version C	ormal (0)   Deployment Pending (0)	
Name	Model	Version C	nassis	Licenses
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:		
		On Firepower Threat VPN licenses can be enabled.	t Defense devices version 6.2.1 onwar bled from smart license page Register	rds, AnyConnect
			inegister.	

### 1470 11. The FTD appliance will be added to the FMC's **device list**.

Overview Analysis Policies Devices	Objects AMP Inte	lligence			Deploy 🎈	System	Help 🔻	admin 🔻
Device Management NAT VPN • Q	oS Platform Settings	FlexConfig	g Certificates					
Device Management List of all the devices currently registered on the Firepo	ower Management Center.							
View By : Group Y All (1)	Error (1)   Warning (0)	Offline (0)	Normal (0)   Deployment Pending (0	)	🔍 Search De	vice	💿 Ac	dd 🔹
Name	Model	Version	Chassis	Licenses	Access Control Policy			
a 📁 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 8	\$	

#### 1471

### 1472 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. In order to configure the eight subnets needed for the PACS architecture while
also allowing for 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 (Enterprise Services, Imaging Modalities, Security
Services, etc.), 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.

- 1480 1. Log in to the **FMC Console**.
- 1481 2. Navigate to **Devices > Device Management**.
- 1482 3. Find your FTD device and click the **edit** icon.
- 1483 4. Navigate to Add Interfaces > Redundant Interface.

D-PACS					You have unsaved char	ages 🔚 Save 🔞 Ca
Firepower Threat Defense for VMWare	Sets DHCP					
					Search by name	Sync Device 🔤 🔕 Add Interfa
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Sub Interface
Diagnostic0/0	diagnostic	Physical				Redundant Interface
GlgabitEthernet0/0		Physical				Bridge Group Interfac
GigabitEthernet0/1		Physical				0
GigabitEthernet0/2		Physical				0
GlgabitEthernet0/3		Physical				1
GlgabitEthernet0/4		Physical				1
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)	08
Redundant2	LAN	Redundant				/ 8
Redundant2.1201	Enterprise-Services	SubInterface	Enterprise-Services		192.168.120.1/24(Static)	/ 9
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)	/8
Redundant2.1402	PACS-B	SubInterface	PACS-B		192.168.141.1/24(Static)	00
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)	/ 6
Redundant2.1801	Data-Center	SubInterface	Data-Center		192.168.180.1/24(Static)	/ 8
<b>11</b> 12 12	erander eradiser	e. 6.1.1.1. d	essues essentes	Die	daying 1-18 of 18 interfaces  € ≪	

- 1485 5. Enter **Internal-Network** as the **name** for the redundant interface.
- 1486 6. Create and/or add a **security zone** to the redundant interface.
- 1487 7. Assign a **Redundant ID** (e.g., **Internal-Network**) to the redundant interface.
- 1488 8. Select a **primary interface** and **secondary interface** for the redundant pair.

TD-PACS								
co Firepower Threat Defense for VMWa Device Routing Interfaces In		ICP						
Interface	Loui	cal Name	Туре	Soruri	y Zones	MAC Adde	ess (Active/Standby)	Search b
Diagnostic0/0	dia	Add Redunda			Lones	MAC AUGI	cos (Active/ Standby)	7 X
GigabitEthernet0/0								
GigabitEthernet0/1		General IP	/4 IPv6	Advanced				
GigabitEthernet0/2		Name:		Internal-Netwo	rk		🗹 Enabled 🛛 🗐 Managerr	ent Only
GigabitEthernet0/3		Description:						
GigabitEthernet0/4		Security Zone:		Internal-Netwo	4.			
GigabitEthernet0/5					rk I	(64 - 9000)		
GigabitEthernet0/6	Gu	MTU:		1500				1
🗃 Redundant1	WA	Redundant ID *:		3		(1 - 8)		3
Redundant2	LAI	Primary Interfac	e:	GigabitEtherne	t0/4 ¥			
Redundant2.1201	En	Secondary Inter	ace:	GigabitEtherne	t0/5 ¥			
Redundant2.1301	Clin							

- 1490 9. Navigate to the **IPv4** tab.
- 1491 10. Assign an **IP address** and **netmask** (e.g., **192.168.100.101/24**) to the interface.
- 1492 11. Click **OK**.

TD-PACS co Firepower Threat Defense for VMWa evice Routing Interfaces In	ire					1144
ence Routing Interaces In	mie sets DHCr				Search by	y 1
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Ad	Id
Diagnostic0/0	dia Add Re	dundant Interfac	e		? X	
GigabitEthernet0/0	General	IPv4 IPv6	Advanced			
GigabitEthernet0/1						
GigabitEthernet0/2	IP Type:		e Static IP 👻	eg. 192.0.2.1/255.255.255.128 or		
GigabitEthernet0/3	IP Addre	is: 19	2.168.100.101/24	192.0.2.1/25	- 1	
GigabitEthernet0/4					- 1	
GigabitEthernet0/5						
GigabitEthernet0/6	Gu				1	68
Redundant1	Wź				2	.5
Redundant2	LA					
Redundant2.1201	En				1	68
Redundant2.1301	Cli				1	68
Redundant2.1401	PA				1	68
Redundant2.1402	PA			ОК С	ancel	68
Redundant2 1501	Radiology	SubInterfa	ice Radiology		192.1	65

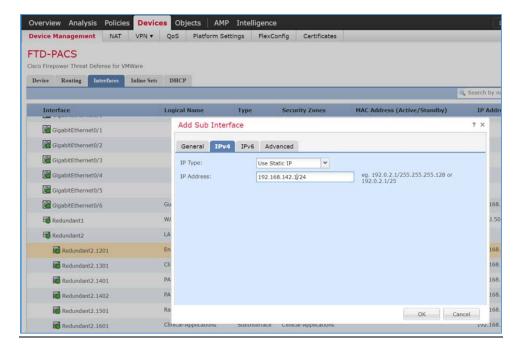
FTD-PACS						E Szur
Device Routing Interfaces In	line Sets DHCP				Search by name	c Device
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)		Sub Interface
ang					21.000000000000000000000000000000000000	Redundant Interfa
GigabitEthernet0/1		Physical			Q	Bridge Group Inter
GigabitEthernet0/2		Physical				62
GigabitEthernet0/3		Physical				0
GigabitEthernet0/4		Physical				a
GigabitEthernet0/5		Physical				a
GigabitEthernet0/6	Guest	Physical	GUEST		192.168.170.1/24(Static)	0
🐻 Redundant1	WAN	Redundant	WAN		10.32.50.130/28(Static)	01
Redundant2	LAN	Redundant				01
Redundant2.1201	Enterprise-Services	SubInterface	Enterprise-Services		192.168.120.1/24(Static)	01
Redundant2.1301	Clinical-Workstations	SubInterface	Clinical-Workstations		192.168.130.1/24(Static)	21
Redundant2.1401	PACS-A	SubInterface	PACS-A		192.168.140.1/24(Static)	01
Redundant2.1402	PACS-B	SubInterface	PACS-B		192.168.141.1/24(Static)	01
Redundant2.1501	Radiology	SubInterface	Radiology		192.168.150.1/24(Static)	0
Redundant2.1601	Clinical-Applications	SubInterface	Clinical-Applications		192.168.160.1/24(Static)	1
Redundant2.1801	Data-Center	SubInterface	Data-Center		192.168.180.1/24(Static)	0
Redundant2.1901	Security-Services	SubInterface	Security-Services		192.168.190.1/24(Static)	01
Redundant3	Internal-Network	Redundant	Internal-Network		192.168.100.101/24(Static)	0
6.W				Durch	ying 1-19 of 19 interfaces K < Page	1 of 1 > >

### 1494 12. Navigate to **Add Interfaces > Sub Interface**.

- 1496 13. Enter **VNA** as the **name** for the sub interface.
- 1497 14. Create and/or add a **security zone**, **VNA**, to the sub interface.
- 1498 15. Select an **interface** under which the sub interface will operate.
- 1499Note: For our build, we placed each sub-interface under **Redundant 2**, the redundant interface for1500**GigabitEthernet0/2** and **GigabitEthernet0/3**. These two physical interfaces were the destination for
- each VLAN's traffic.
- 1502 16. Assign **1403** as the **Sub Interface ID** to the sub interface.
- 1503 17. Assign **1403** as the **VLAN ID** to the sub interface.

PN • Qo	S Platform Set	tings	FlexConfig Certificates	5	
	100				
ie Sets D	ncr		_		Search by
Log	ical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Add
	Add Sub Inter	face			? ×
	General IPv4	IPv6	Advanced		_
	Name:		VNA	C Enabled Manage	ment Only
	Description:				
Gu	Security Zone:		VNA	*	16
W/	MTU:		1500	(64 - 9000)	2.5
LA	Interface *:		Redundant2		
En	Sub-Interface ID *	1:	1403	(1 - 4294967295)	16
Cli	VLAN ID:		1403	(1 - 4094)	16
PA					16
PA					16
	N ♥ Qo be Sets DI Log Gu W/ LA En Cli pA	Logical Name  Logical Name  Add Sub Interf  General IPv4 Name: Description:  Gu Security Zone: WV MTU: LA Interface *: Sub-Interface ID * VLAN ID: PA	N V QoS Platform Settings  te Sets DHCP  Logical Name Type  Add Sub Interface  General IPv4 IPv6 Name: Description:  Gu Security Zone:  W/ MTU: LA Interface *: Sub-Interface ID *: VLAN ID: PA	N V QoS Platform Settings FlexConfig Certificates te Sets DHCP Add Sub Interface General IPv4 IPv6 Advanced Name: VNA Description: Gu Security Zone: VNA W/ MTU: 1500 L140 Interface *: Redundant2 v Sub-Interface ID *: 1403 Cli VLAN ID: 1403	N V QoS Platform Settings FlexConfig Certificates  te Sets DHCP  Logical Name Type Security Zones MAC Address (Active/Standby)  Add Sub Interface General IPv4 IPv6 Advanced Name: VNA Cenabled Manage Description: Config Cenabled Manage Certificates  General IPv4 IPv6 IPv6 Advanced Name: VNA Cenabled Manage Description: Config Cenabled Manage Certificates  General IPv4 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6 IPv6

- 1505 18. Navigate to the **IPv4** tab.
- 1506 19. Assign an **IP address** and **netmask** (e.g., **192.168.142.1/24**) to the sub interface.
- 1507 20. Click **OK**.



- 1509 21. Click **Save**.
- 1510 22. Click **Deploy** and wait for deployment to FTD to complete.
- 1511 23. Refresh the page and confirm that the redundant interface and sub-interface are running (shown
- 1512 with a green dot on the interface's icon).

D-PACS						E s	over 🛛 🔀 Ca
Firepower Threat Defense for VMWar	e						
ice Routing Interfaces Inli	ne Sets DHCP				Search by name	2 Sync Device	Add Interfa
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	of the beauty	
GigabitEthernet0/2		Physical					0
GigabitEthernet0/3		Physical					0
GigabitEthernet0/4		Physical					a
GigabitEthernet0/5		Physical					0
GigabitEthernet0/6	Guest	Physical	GUEST		192.168.170.1/24(St	atic)	0
Redundant1	WAN	Redundant	WAN		10.32.50.130/28(Stat	tic)	08
Redundant2	LAN	Redundant					08
Redundant2.1201	Enterprise-Services	SubInterface	Enterprise-Services		192.168.120.1/24(St	atic)	00
Redundant2.1301	Clinical-Workstations	SubInterface	Clinical-Workstations		192.168.130.1/24(St	atic)	08
Redundant2.1401	PACS-A	SubInterface	PACS-A		192.168.140.1/24(St	atic)	08
Redundant2.1402	PACS-B	SubInterface	PACS-B		192.168.141.1/24(St	atic)	0
Redundant2.1403	VNA	SubInterface	VNA		192.168.142.1/24(St	atic)	28
Redundant2,1501	Radiology	SubInterface	Radiology		192.168.150.1/24(St	atic)	/8
Redundant2,1601	Clinical-Applications	SubInterface	Clinical-Applications		192.168.160.1/24(St	atic)	00
Redundant2.1801	Data-Center	SubInterface	Data-Center		192.168.180.1/24(St	atic)	08
Redundant2.1901	Security-Services	SubInterface	Security-Services		192.168.190.1/24(St	atic)	00
Redundant3	Internal-Network	Redundant	Internal-Network		192.168.100.101/24(	(Static)	08
				Dis	laying 1-20 of 20 interfaces	< Page 1	of1 > >

- 1514 DHCP Relay Through Cisco Firepower Management Center Configuration
- 1515 1. Log in to the **FMC Console**.
- 1516 2. Navigate to **Devices > Device Management**.
- 1517 3. Find your FTD device and click the **edit** icon.

Overview Analysis Policies	Devices Objects AMI	P Intelligence		Deploy 🧕	System Help 🔻 adm
Device Management NAT V	PN ▼ QoS Platform Se	ettings FlexConfig Ce	ertificates		
Device Management List of all the devices currently registered	on the Firepower Management Ce	enter.			
View By : Group	All (1)   Error (1)   Warnin	ng (0)   Offline (0)   Norma	(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 1 🔀
					Edit

# 1519 4. Navigate to the **DHCP** tab.

Overview Analysis Policies	Devices Objects AMP Inte	lligence	Deploy 🍳 System Help 🔻 admin 🔻
Device Management NAT	VPN VOS Platform Settings	FlexConfig Certificates	
FTD-PACS Cisco Firepower Threat Defense for VMV	Nare		Save Cancel
Device Routing Interfaces I	Inline Sets DHCP		
DHCP Server     DHCP Relay     DDNS	Ping Timeout     50       Lease Length     3600       Auto-Configuration     Interface       Override Auto Configured Settings:     Domain Name       Domain Name     Primary DNS Server       Secondary DNS Server     Server       Server     Advanced	(10 - 10000 ms) (300 - 10,48,575 sec)	
	Interface	Address Pool	Enable DHCP Server

### 1520

1521 5. Navigate to the **DHCP Relay Agent** section.

Overview Analysis Polici	es Devices Objects AMP	Intelligence	Deploy 🏮 System Help 🔻 admin 🕇
Device Management NAT	VPN VOS Platform Settin	ngs FlexConfig Certificates	
TD-PACS			🔚 Save 🛛 😢 Cancel
Cisco Firepower Threat Defense for V	VMWare		
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	2	
	Interface	Enable DHCP Relay	Set Route(IPv4)
	Clinical-Workstations	💜 (IPv4 only)	✓
	PACS-A	IPv4 only)	×
	PACS-B	V (IPv4 only)	✓
	Radiology	V (IPv4 only)	✓
	Clinical-Applications	✓ (IPv4 only)	✓
	Data-Center	✓ (IPv4 only)	✓
	Security-Services	✓ (IPv4 only)	<b>v</b>
	Internal-Network	✓ (IPv4 only)	·
	Guest		4
	outst	IPv4 only)	▼

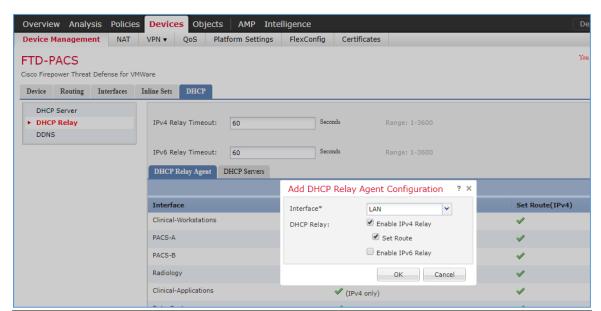
### 1523 6. Under **DHCP Relay Agent**, click **Add**.

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     IPv6 Relay Timeout:     60       Interface     Enable DHCP Relay     Set Route(IPv4)       Clinical-Workstations     IPv6 (IPv4 only)     Implement       PACS-A     IPv6 only     Implement       PACS-B     IPv6 only     Implement	O Add
IPv6 Relay Timeout:         60         Seconds         Range: 1-3600           DHCP Relay Agent         DHCP Servers         Set Route(IPv4)           Interface         Enable DHCP Relay         Set Route(IPv4)           Clinical-Workstations         Import (IPv4 only)         Import (IPv4 only)           PACS-B         Ipv4 only         Import (IPv4 only)         Import (IPv4 only)	O Add
Interface     Enable DHCP Relay     Set Route(IPv4)       Clinical-Workstations     IPv4 only)     Image: Clinical-Workstations       PACS-A     Image: Clinical-Workstations     Image: Clinical-Workstations       PACS-B     Image: Clinical-Workstations     Image: Clinical-Workstations	O Add
Clinical-Workstations     I/(IPv4 only)       PACS-A     I/(IPv4 only)       PACS-B     I/(IPv4 only)	O Add
Clinical-Workstations     I/(IPv4 only)       PACS-A     I/(IPv4 only)       PACS-B     I/(IPv4 only)	
PACS-A         IPv4 only)         IPv4           PACS-B         IPv4 only)         IPv4	
PACS-B	i 🖓
(1994 diny)	P 🖥
	Ø 🖥
Radiology 🗳 (IPv4 only)	Ø 🗎
Clinical-Applications 🖌 (IPv4 only)	6
Data-Center 🗳 (IPv4 only)	a 🖉
Security-Services 🗳 (IPv4 only)	a 🖉
Internal-Network 🖋 (IPy4 only)	a 🖉 🗑
Guest 🗳 (IPv4 only)	
Internal-Network 🖋 (IPv4 only)	

### 1524

1525 7. Assign an **FTD interface** as **LAN**.

- 1526 8. Check the box next to **Enable IPv4 Relay**.
- 1527 9. Check the box next to **Set Route**.
- 1528 10. Click **OK**.



1530 11. Ensure the new relay, LAN, is shown in the DHCP Relay Agent list.

evice Management NAT	VPN VOS Platform Settings	FlexConfig Certificates		•
TD-PACS			You ha	ave unsaved changes 📔 Save 🛛 🔀 Can
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		
				O Add
	Interface	Enable DHCP Relay	Set Route(IPv4)	
	PACS-A	V (IPv4 only)	4	Ø 6
	PACS-B	V (IPv4 only)	1	<i>i</i>
	Radiology	V (IPv4 only)	✓	a 6
	Clinical-Applications	V (IPv4 only)	×	Ø 8
	Data-Center	IPv4 only)	×	a 6
	Security-Services	IPv4 only)	×	a 🖉 🖥
	Internal-Network	IPv4 only)	×	a 🖉 🖥
	Guest	🖋 (IPv4 only)	✓	e 6
	LAN	V (IPv4 only)	4	Ø 🖥

#### 1531

1532 12. Under **DHCP Servers**, click **Add**.

		itelligence	Deploy 🏮 System Help 🔻
Device Management NAT	VPN      QoS Platform Settings	s FlexConfig Certificates	
FTD-PACS			E Save
Cisco Firepower Threat Defense for	VMWare		
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		
	Server	Interface	
	DHCP-AD-Server	Enterprise-Services	

1534 13. Click the green + button to create a new object for the DHCP server.

Overview Analysis Policies	Devices Objects AMP Int	telligence
Device Management NAT	VPN • QoS Platform Settings	FlexConfig Certificates
FTD-PACS Cisco Firepower Threat Defense for VMW Device Routing Interfaces In	are nline Sets DHCP	
DHCP Server DHCP Relay DDNS	IPv4 Relay Timeout: 60 IPv6 Relay Timeout: 60 DHCP Relay Agent DHCP Servers	Seconds Range: 1-3600 Seconds Range: 1-3600
	Server	Add DHCP Relay Server Configuration ? ×
	DHCP-AD-Server	Server V Concel

- 1536 14. Enter **Test-DHCP-Server** as a **name** for the DHCP server.
- 1537 15. Enter **192.168.100.170** as an **IP address** for the DHCP server.
- 1538 16. Click **Save**.

Overview Analysis Policies	Devices Objects AMP Intelligence	
Device Management NAT	VPN • QoS Platform Settings FlexConfig Certificates	
FTD-PACS Cisco Firepower Threat Defense for VMW	/are	
Device Routing Interfaces In	nline 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 A New Network Object	? ×
	Name: Test-DHCP-Server	
	Server Description:	
	DHCP-AD-Serv	
	Network:   Host  Range  Network  FQDN	
	192.168.100.170	
	Allow Overrides:	
	Save	Cancel

- 1540 17. Select the newly created **DHCP server**.
- 1541 18. Select an **FTD interface** through which the **DHCP server** can be connected.
- 1542 19. Click **OK**.

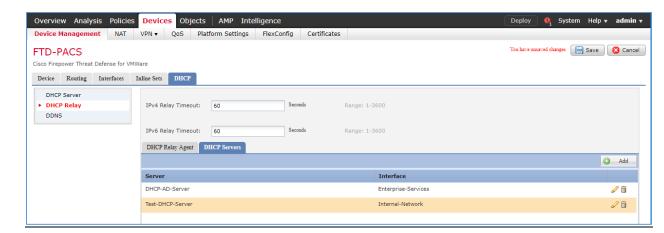
Overview Analysis Policies	Devices Objects AMP In	telligence
Device Management NAT	VPN • QoS Platform Settings	FlexConfig Certificates
FTD-PACS Cisco Firepower Threat Defense for VMV	Vare	
Device Routing Interfaces	Inline Sets DHCP	
DHCP Server • DHCP Relay DDNS	IPv4 Relay Timeout: 60	Seconds Range: 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 V
		OK Cancel

#### 1543

1544 20. Ensure the new server is shown in the **DHCP Server** list.

#### 1545 21. Click **Save**.

1546 22. **Deploy** the new configuration settings to the FTD appliance.



1547

#### 1548 Network Address Translation (NAT) Rules Configuration

1549 1. Navigate to **Devices** > **NAT**.

Device Management	NAT	VPN V	QoS	Platform Settings	FlexConfig	Certificates		
								New Policy
NAT Policy					Device Typ	e	Status	
PACS NAT					Threat Defer		Targeting 1 devices Up-to-date on all targeted devices	9000

#### 1550

1551 2. Click New Policy > Threat Defense NAT.

Device Management	NAT VPN VOS Plat	tform Settings FlexConfig Certificates		
				New Policy
NAT Policy		Device Type	Status	Firepower NAT
BACC NAT			Targeting 1 devices	Threat Defense NAT
PACS NAT		Threat Defense	Out-of-date on 1 targeted devices	

- 1553 3. Give the new policy a **Name** as **PACS NAT**.
- 1554 4. Assign the **FTD appliance** to the new NAT policy.
- 1555 5. Click **Save**.

AT Policy		Device Ty	pe	Stat	tus
PACS NAT	New Delieu	Thread Date		Targ	eting 1 devices
	New Policy Name: Description:	PACS NAT			
	-Targeted Device Select device Available D	es to which you want to ap	pply this policy.	Selected Devices	
	Sarch	by name of value	Add to Policy	FTD-PACS	Ð

- 1557 6. Click on the NAT policy's **edit** icon.
- 1558 7. Click **Add Rule**.
- 1559 8. Set **NAT Rule** to **Auto NAT Rule**.
- 1560 9. Set **Type** to **Dynamic**.
- 1561 10. Under Interface Objects set Source Interface Object to one of the FTD appliance's LAN interfaces.
- 1562 11. Set **Destination Interface Object** to the FTD appliance's **WAN interface**.

PA				Platform Settin	193 11	exConfig	Certificates				
Enter	CS NAT									You have unsa	ved change
Rule					_						_
Filt	ter by Device										
			Add NAT Rule								? X
#	Direction	Туре	NAT Rule:	Auto NAT Rule	~						
• NA	AT Rules Before		Type:	Dynamic	~	Enable					
• Au	ito NAT Rules		Interface Objects	Translation	PAT Pool	Advance					
#	+	Dynamic	Available Interface O		PAT POOL	Advance	Source Interface Obje	cts (1)	Destination Interfe	are Objects (1)	
ŧ	+	Dynamic	Search by name	ojecco o			VNA VNA	(L)	wan		8
	+	Dynamic	Guest-Services								
		Dynamic	Imaging-Modalities			Add to Source					
	1	8	PACS-A			Add to					
	+	Dynamic	PACS-B		De	estination					
ŧ.	+	Dynamic	Security-Services								
	+	Dynamic	VNA VNA								
	+	Dynamic	WAN		<b>*</b>						
	+	Dynamic							(	OK Car	
ŧ.											

- 12. Under Translation, set Original Source to the network that corresponds with the source interfaceobject established in the previous step.
- 1566 13. Set Translated Source to Destination Interface IP.
- 1567 14. Click **OK**.

Device Manage	ement NAT	VPN VOS	Platform Settings	FlexConfig Certific	ates	
PACS NAT						You have unsaved i
Rules Filter by Device		_	_			
		Add NAT Rule				***
# Direction	Туре	NAT Rule;	Auto NAT Rule	~		
NAT Rules Be	fore	Type:	Dynamic	▼ Ø Enable		
Auto NAT Rul	les					
•	Dynamic	Interface Objects	Translation PAT	Pool Advanced	Translated Packet	
+	Dynamic	Original Source:*	VNA	× 0	Translated Source:	Destination Interface IP
	Dynamic					The values selected for Destination Interface     Objects in 'Interface Objects' tab will be used
	Dynamic	Original Port:	ТСР 👻			
					Translated Port:	
+	Dynamic					
+	Dynamic					
+	Dynamic					
+	Dynamic					
+	Dynamic					
						OK Cancel

- 1569 15. Ensure the new **NAT Rule** has been created.
- 1570 16. Repeat these steps if needed for each **LAN interface** attached to FTD appliance.
- 1571 17. Click **Save**.
- 1572 18. **Deploy** changes to FTD appliance.

	ter Description									
ü	les								Policy /	Assignment
à.	Filter by Device				Original Packet		Translated	Dacket	0	Add Rul
#	Direction	Туре	Source Interface Objects	Destination Interface Objects	Original Packet	Ori De	Translated Sources		Options	
	NAT Rules Befo	re								
•	Auto NAT Rules									
#	+	Dynamic	🔒 Security-Services	WAN	🚔 Security-Services		🍓 Interface		🍓 Dns:false	28
#	+	Dynamic	🛻 Enterprise-Services	wan	Enterprise-Services		🍓 Interface		🚳 Dns:false	28
#	+	Dynamic	📇 Clinical-Viewers	wan	Clinical-Viewers		4 Interface		🍓 Dns:false	08
#.	+	Dynamic	ACS-A	🚓 WAN	PACS-A		🍓 Interface		🝓 Dns:false	00
#	+	Dynamic	PACS-B	A WAN	PACS-B		🚳 Interface		🝓 Dns:false	0
#	+	Dynamic	Imaging-Modalities	wan	Imaging-Modalities		🍓 Interface		🝓 Dns:false	28
#	+	Dynamic	👬 Clinical-Application-Services	🚓 WAN	Clinical-Application-Services		🝓 Interface		🧠 Dns:false	00
#	+	Dynamic	Guest-Services	A WAN	Guest-Services		🍓 Interface		🝓 Dns:false	18
#	+	Dynamic	Datacenter	wan	Datacenter		🍓 Interface		🥵 Dns:false	00
#	+	Dynamic	👬 Internal-Network	wan	🚃 Internal-Network		Interface		🝓 Dns:false	08
4	+	Dynamic	🚓 VNA	📇 WAN	🙀 VNA		Interface		🚳 Dns:false	08
•	NAT Rules Afte	r								

#### 1574 Access Control Policy Through Firepower Management Center Configuration

Firepower Management Center allows configuration of access control policies that can then be applied 1575 1576 to individual FTD appliances. The purpose of the access-control policy is to create rules that specify how 1577 traffic is managed within the network. Each access-control policy contains multiple rules followed by a 1578 default action established when the policy is created. For the PACS architecture, one access-control 1579 policy was established to manage the traffic on each FTD interface. The steps below describe how the 1580 policy and rules were created, as well as how to utilize an intrusion policy with the access-control policy. 1581 There is additional information on Cisco Firepower access control list and intrusion prevention 1582 configuration [17].

#### 1583 1. Navigate to Policies > Access Control > Access Control.

Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions •		
					Object Management Intrusion Network Analysis Policy DNS In	nport/Exp
						w Policy
					U Ne	w PORCY
Access Control Policy		Status			Last Modified	

#### 1584

- 1585 2. Click **New Policy**.
- 1586 3. Enter **PACS Global Policy** as the name for the access control policy.
- 1587 4. For **Select Base Policy** select **None**.
- 1588 5. For **Default Action** select **Block all traffic**.
- 1589 6. Add the FTD appliance to the policy.
- 1590 7. Click **Save**.

Overview Analysis Policies I Access Control + Access Control	Devices Objects AMP Network Discovery Appl	Intelligence	Correlation	Actions •		
					Object Management	Intrusio
Access Control Policy	New Policy	Status	_	_	Last Modified	? X
	Name:	PACS Global Polic	.y			
	Description: Select Base Policy:	None		×		-
	Default Action: Targeted Devices	Block all traffic	:   Intrusion Prever	ntion 🕘 Network Discove	ery	71
	Select devices to Available Device	which you want to es	apply this policy.	Selected Devices		
	FTD-PACS	me or value	_	FTD-PACS	6	
			Add to Poll	~		
					Save Cancel	

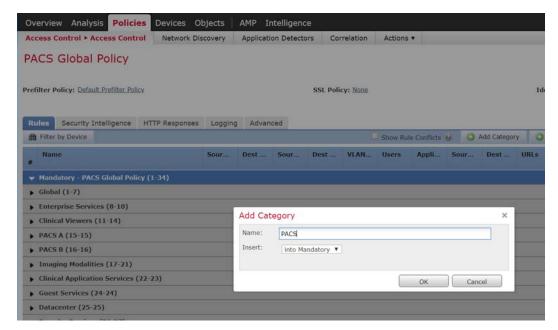
1592 8. Click the access-control policy's **edit** icon.

1593 Note: The policy in the screenshots that follow contain categories created during the process of 1594 building out the PACS architecture. These categories are not pre-configured.

Overview Analysis Policies	Devices Objects A	MP Intelligence					Dep	sloy 🍳	System Help v a	admin v
Access Control + Access Control	Network Discovery	Application Detectors	Correlation Ac	tions •						
PACS Global Policy									E Saves C	Cancel
refilter Policy: Default Prefilter Policy		55	Policy: None				Identity Polic	yr None		
Rules Security Intelligence HTT	P Responses Logging	Advanced					Ta Int	veritance Set	ttings   🥂 Policy Assignment	nents (1
Filter by Device			_ sh	w Rule Conflicts	Adi	d Category	Add Rule	Search Rok	6	1
Name	Sourc Dest .	Sourc Dest	VLAN Users	Applic S	ourc. De	st URL	ISE/S			
Handatory - PACS Global Policy (1	34)									
Global (1-7)										0
<ul> <li>Enterprise Services (8-10)</li> </ul>										0
Clinical Viewers (11-14)										2
PACS A (15-15)										0
PACS 8 (16-16)										0
<ul> <li>Imaging Hodalities (17-21)</li> </ul>										0
Clinical Application Services (22-2)	3)									0
<ul> <li>Guest Services (24-24)</li> </ul>										0
Datacenter (25-25)										10
<ul> <li>Security Services (26-27)</li> </ul>										2
Internal Network (28-30)										0
VNA (31-33)										2
• WAN (34-34)										0
Default - PACS Global Policy (-)										-
					and the second se		Block All Traffic			~

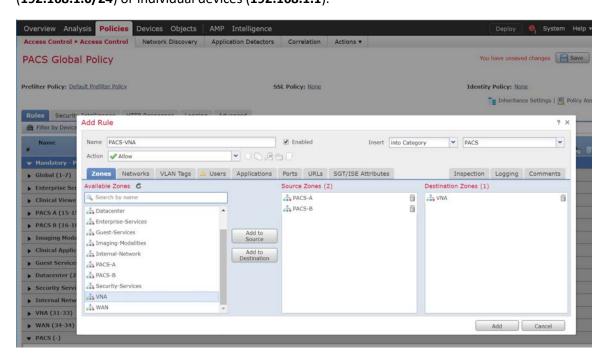
1601

- 1596 Creating a category:
- 1597 1. Click Add Category.
- 1598 2. Enter **PACS** as the name for the category.
- 1599 3. Insert the category into the **Mandatory** section.
- 1600 4. Click **OK**.

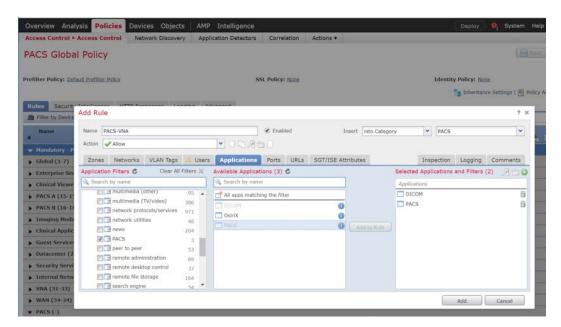


### 1602 Create a rule that allows application traffic between security zones

- 1603 1. Click Add Rule.
- 1604 2. Enter **PACS-VNA** as the name for the rule.
- 1605 3. Insert the rule into the category created in the previous step.
- 1606 4. Set Action to Allow.
- 1607 Note: Because we set the default action to block all traffic when creating the policy, all of the rules
   1608 we created were set to Allow.
- 1609 5. Add security zone(s) to the **Source Zone**, and also add security zone(s) to the **Destination Zone**.
- 1610 Note: The two primary methods for adding source and destination networks to an access control
- 1611 rule are through security zones or networks. Security zones are objects that can contain multiple
- 1612 FTD interfaces. Networks can be different types of network objects, including network segments
- 1613 (**192.168.1.0/24**) or individual devices (**192.168.1.1**).



- 1615 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 the type of traffic
   (e.g., DICOM) being sent.
- 1619 7. Click **Add**.



1622

1621 8. Verify that the **rule** has been created.

Access Control > Access Control	Network Disc	overy	Application	Detectors	Correla	ation A	ctions •							
PACS Global Policy											You have	unsaved chan	jes 🔚 Save 🕻	<b>3</b> Ca
Prefilter Policy: Default Prefilter Policy				5	iSL Policy:	None					dentity Polic	v: None		
											Ta Ini	heritance Setti	ngs   🧾 Policy Assign	men
Rules Security Intelligence HTT	P Responses	Logging	Advance	bd										
B Filter by Device						D sh	aw Rule Conflic	ts 😣	Add Categ	ory 🤇	Add Rule	Search Rules		
# Name	Sourcas	Dest Z	Sourc	Dest N	VLAN	Users	Applic	Sourc	Dest P	URLs	ISE/S			
Mandatory - PACS Global Policy (1-	35)													
Global (1-7)														
Enterprise Services (8-10)														
Clinical Viewers (11-14)														
PACS A (15-15)														
▶ PACS 8 (16-16)														
<ul> <li>Imaging Modalities (17-21)</li> </ul>														
Clinical Application Services (22-23	;)													
<ul> <li>Guest Services (24-24)</li> </ul>														
<ul> <li>Datacenter (25-25)</li> </ul>														
<ul> <li>Security Services (26-27)</li> </ul>														
Internal Network (28-30)														
VNA (31-33)														
▶ WAN (34-34)														
¥ PACS (35-35)														
35 PACS-VINA	A PACS-A	ش VNA	Any	Any	Any	Any	DICOM PACS	Αηγ	Any	Any	Amy	🖌 Allov	0.000.00	
Default - PACS Global Policy (-)														
Default Action									Access C	ontrol: Bl	ock All Traffic			~
								Die	playing 1 - 35 c	1 35 miles	12 d Day	1 000	>> C Page Siz	

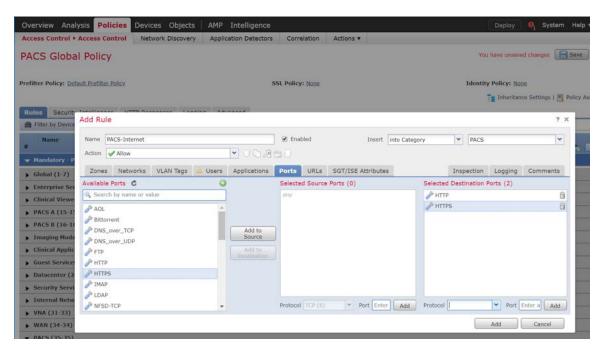
- 1623 <u>Create a rule that allows traffic on a specific port between networks</u>
- 1624 1. Click **Add Rule**.

- 1625 2. Enter **PACS-Internet** as the **name** for the rule.
- 1626 3. Insert the rule into the **category** created previously.
- 1627 4. Set Action to Allow.
- 1628 5. Under Networks, add a source network(s) and destination network(s).

Overview Analysis Policies Devices Objects	AMP Intelligence			Deploy	0 System Help
Access Control * Access Control Network Discover	Application Detectors	Correlation	Actions •		
PACS Global Policy				You have unsave	ed changes Save
Prefilter Policy: <u>Default Prefilter Policy</u>	5	SSI. Policy: <u>None</u>		Identity Policy: Nor	ne ce Settings   🛄 Policy A
Add Rule					? ×
Name Name PACS-Internet		🗷 Enabled	Insert Into Catego	pry PACS	·
Action Allow	• UD28	ġ			20
Global (1-7) Zones Networks VLAN Tags	🙆 Users 🛛 Applications	Ports URLs	SGT/ISE Attributes	Inspection Logging	Comments
Finterprise Ser Available Networks C	0	Source Network	s (2)	Destination Networks (1)	
Clinical Viewe		Source	Original Client	Real WAN	6
PACS A (15-1: PACS B (16-1: PACS B (16-1: Imaging Mode Clinical Applic Guest Service Datacenter (2 Security Servi Security Services VA	Add To Source Networks Add to Destination	PACS-A	6		
Internal Netw     WAN	3	Enter an IP addre	Add	Enter an IP address	Add
<ul> <li>VNA (31-33)</li> <li>WAN (34-34)</li> <li>PACS (35-35)</li> </ul>				Add	Cancel

1630 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.



1634 7. Under URLs, add URL categories that will be allowed (or leave this section blank).

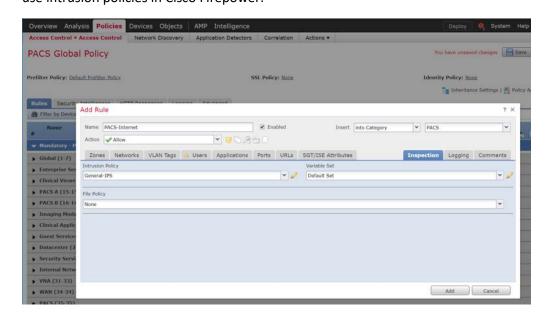
1635Note: The URL categories are generated by Cisco Firepower and updated regularly. Within each1636URL category, you can specify the reputation level the URL must meet in order for the rule to1637match.

Access Control +	Access Control	Network Discovery	Application	Detectors	Correlation	Actions *					
PACS Globa	I Policy							You	have unsaved	changes	
refilter Policy: <u>Def</u>	ault Prefilter Policy			55	SL Policy: None			Identity	Policy: None		
									Inheritance	Settings	图
Rules Securit	Add Rule	The December of Land		<u>(1)</u>							7
Name	Name PACS-Inter	met			🗷 Enabled	Insert	into Category	▼ PACS			~
<ul> <li>Mandatory – P</li> </ul>	Action Allow		*	08.00	ΒŪ						
• Global (1-7)	Zones Netwo	orks VLAN Tags	Users Ap	plications	Ports URLs	SGT/ISE Attribute	s	Inspection	Logging	Commen	its
Enterprise Ser	Categories and UP		O Repu	tations			Select	ted URLs (7)			
Clinical Viewe	Search for a cat	egory	A 🖌					isiness and Econor			đ
PACS A (15-1	Category	URLS		<ul> <li>Well Known</li> </ul>				lucational Instituti			0
PACS B (16-10	Any (Except Uni	categorized)	and the second second	- Benipa siter	with security risk			alth and Medicine			6
Imaging Moda	Uncategorized     Abortion			<ul> <li>Benign sites</li> <li>Suspicious s</li> </ul>				ternet Portals (Rej		sta 4.3)	10
<ul> <li>Clinical Applic</li> </ul>	Abused Drugs			- High Risk				ews and Media (Re			8
Guest Service	Adult and Porno	graphy					📰 Re	ference and Rese	arch (Reputatio	ns 4-5)	6
Datacenter (2	Alcohol and Tob	acco									
Security Servi	Auctions										
Internal Netw	Bot Nets						( Contraction of the second se	1.004			
	Business and Ec	conomy	*				Enter	URL		A	Add .

1638

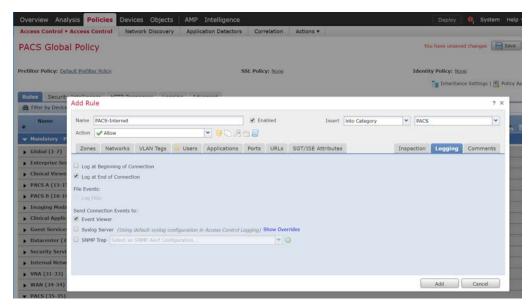
1639 8. Under **Inspection**, add an **intrusion policy** or leave this section blank.

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 [17] at the beginning of this section for more information on how to create and
use intrusion policies in Cisco Firepower.



- 1645 9. Under Logging, select Log at End of Connection, or leave this section blank.
- 1646 Note: If logging is enabled, select **Event Viewer**.
- 1647 10. Click **Add**.

1644



- 1649 11. Verify that the access control rules have been created and placed in the proper category.
- 1650 12. Click **Save**.
- 1651 13. **Deploy** changes to the FTD appliance.

Overview Analysis Policies	Devices Of	ojects	AMP Inte	lligence	ð.,						D	eploy 🍳 System	Help 🔻 admin
Access Control + Access Control	Network Dis	covery	Application	Detectors	Corre	lation	Actions *						
PACS Global Policy											You hav	e unsaved changes	Save 🚺 Canci
Prefilter Policy: Default Prefilter Policy					SSL Policy:	None				1	dentity Pol		
Rules Security Intelligence H	TTP Responses	Logging	Advanced								1.	nheritance Settings   📃	POICY Assignments (
Filter by Device			e.			Q	Show Rule Cont	flicts M	Add Cate	egory C	Add Rule	Search Rukes	
ø Name	Sourc	Dest	Sourc	Dest	VLAN	Users	Applic	Sourc	Dest	URLS	ISE/S	Act	
Mandatory - PACS Global Policy(1 - 3	6) > PACS(35 -	36)											0.0
PACS A (15-15)													08
PACS B (16-16)													0
Imaging Modalities (17-21)													08
Clinical Application Services (22-	23)												0.8
Guest Services (24-24)													0 5
<ul> <li>Datacenter (25-25)</li> </ul>													0.8
<ul> <li>Security Services (26-27)</li> </ul>													0.8
<ul> <li>Internal Network (28-30)</li> </ul>													25
VNA (31-33)													0.6
WAN (34-34)													Ø 8
▼ PACS (35-36)													26
35 PACS-VNA	A PACS-	A B -L VNA	Any	Any	Any	Any	DICOM PACS	Any	Any	Απγ	Any	Allov C Nolla V	to 🗇 🖉 🖥
36 PACS-Internet	Any	Acy	PACS-A PACS-E		Any	Any	Any	Any	HTTP HTTPS	Busine Educat Health Image (3 more	ik z Any z	🖌 💭 😽 volta 🗣	5 <b>8</b> • <b>/</b> 6
Default - PACS Global Policy (-)													
Default Action									Access Co	ntrol: Block	All Traffic		× .

### 1653 2.7.2 Cisco Stealthwatch

1654 Cisco Stealthwatch provides network visibility and analysis through the use of 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

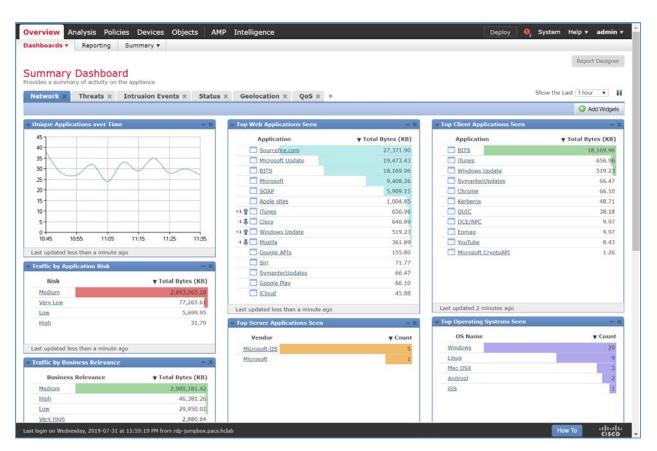
- 1657 to send NetFlow directly to Stealthwatch for analysis.
- 1658 Cisco Stealthwatch Management Console Appliance Information
- 1659 **CPU**: 3
- 1660 **RAM**: 16 GB
- 1661 **Storage**: 60 GB (Thin Provision)
- 1662 Network Adapter 1: VLAN 1901
- 1663 **Operating System**: Linux
- 1664 <u>Cisco Stealthwatch Management Console Virtual Edition Installation Guide</u>
- 1665 Install the Cisco Stealthwatch Management Console appliance according to the instructions detailed in
- 1666 the Cisco installation guide [18].

#### 1667 <u>Cisco Stealthwatch UDP Director Appliance Information</u>

- 1668 **CPU**: 1
- 1669 **RAM**: 4 GB
- 1670 **Storage**: 60 GB (Thin Provision)
- 1671 Network Adapter 1: VLAN 1901
- 1672 Network Adapter 2: VLAN 1901
- 1673 **Operating System**: Linux
- 1674 <u>Cisco Stealthwatch UDP Director Virtual Edition Installation Guide</u>
- 1675 Install the Cisco Stealthwatch UDP Director appliance according to the instructions provided at the Cisco
- 1676 installation guide [18].
- 1677 <u>Cisco Stealthwatch Flow Collector Appliance Information</u>
- 1678 **CPU**: 2
- 1679 **RAM**: 16 GB
- 1680 **Storage**: 60 GB (Thin Provision)
- 1681 Network Adapter 1: VLAN 1901
- 1682 **Operating System**: Linux

#### 1683 Cisco Stealthwatch Flow Collector Virtual Edition Installation Guide

- 1684 Install the Cisco Stealthwatch Flow Collector appliance according to the instructions provided at the
- 1685 Cisco installation guide [18].
- 1686 Configure NetFlow Parameters for Cisco Firepower
- 1687 1. Log in to the Cisco Firepower Management Console.



1689 2. Navigate to **Objects**.

bject Management Intru	sion Rules				
etwork			Add Network •	🔍 Filter	
	more TP addresses. Network objects are used in various places, inclu	uding access control policies, network variables, intrusion rules, i	dentity rules, network discov	ery rules, event sea	rches,
Network _	Name	Value	Туре	Override	
Port Interface	алу	0.0.0.0/0 ::/0	Group	×	- 43
Tunnel Zone	any-ipv4	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	×	a
Security Intelligence	Domain-Controller	192.168.120.100	Host	×	P
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
File List	Google-DNS-Primary	8.8.8.8	Host	×	0
Cipher Suite List	Google-DNS-Secondary	8.8.4.4	Host	×	0
Distinguished Name	Guest-Services	192.168.170.0/24	Network	×	1
Cobject Groups	Imaging-Modalities	192.168.150.0/24	Network	x	0
₽KI	Internal-Network	192.168.100.0/24	Network	×	0
DNS Server Group     SLA Monitor	Internal HIP	192.168.133.0/24	Network	×	0
Prefix List	IPv4-Benchmark-Tests	198.18.0.0/15	Network	x	
📑 IPv4 Prefix List					
IPv6 Prefix List P Route Map	IPv4-Link-Local	169.254.0.0/16	Network	×	
Access List	IPv4-Multicast	224.0.0.0/4	Network	×	
Standard	IPv4-Private-10.0.0.0-8	10.0.0/8	Network	×	
Extended 🗸		Displa	ring 1 - 20 of 33 rows 🛛 🔍	C Page 1 of 2	> >

# 1691 3. Navigate to **FlexConfig > Text Object**.

Value 1.1.1.1 3 5 10 15 abc.com There are 1 more items.	Type System Defined System Defined	Override	00
3 5 10 15 abc.com			0.0
5 10 15 abc.com	System Defined		
		0	0 6
	System Defined	0	0
2.2.2.2	System Defined	0	0
3 5 abc.com	System Defined	0	0
1	System Defined	0	0
	System Defined	0	0
	System Defined	0	0
false	System Defined	0	0
false	System Defined	0	0
60	System Defined	0	0
180	System Defined		0
	System Defined	100	0
	System Defined	0	0
false	System Defined		0
false	System Defined		0
false	System Defined	0	0
	Secon 1 false false 60 180 180	System Defined       1     System Defined       System Defined     System Defined       System Defined     System Defined       false     System Defined       false     System Defined       10     System Defined       50     System Defined       50     System Defined       60     System Defined       180     System Defined       System Defined     System Defined       180     System Defined       System Defined     System Defined       false     System Defined       false     System Defined	System Defined     Image:

ext Object			Add Text Object	🔍 Filter	
ext objects define free-form text	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	
Cobject Groups	IPv6RoutingHeaderDropLogList	4	System Defined	0	18
PKI BDNS Server Group	IPv6RoutingHeaderLogList	2	System Defined	0	00
SLA Monitor	isIsAddressFamily	ipv4	System Defined	0	00
🚯 Prefix List	isIsIntfList		System Defined	0	0
IPv4 Prefix List	IsIsISType	ievel-1-2	System Defined	0	
B Route Map		10V01-1-2		-	
Access List	isIsNet		System Defined	0	0
Standard	isServiceIdentifier	false	System Defined	0	10
Sextended	netflow_Destination	Security-Services 192.168.190.120 2055	System Defined	0	00
Community List	netflow_Event_Types	all flow-create flow-denied flow-teardown flow-update	System Defined	0	1.0
<ul> <li>IKEv2 Policy</li> <li>IKEv1 IPsec Proposal</li> <li>IKEv2 IPsec Proposal</li> </ul>	netflow_Parameters	1 0 30	System Defined	0	0
Group Policy AnyConnect File	PrefixDelegationInside	inside Inside-Prefix ::1:0:0:0:4/64	System Defined	0	00
Address Pools	PrefixDelegationOutside	outside Outside-Prefix ::/56	System Defined	0	0
IPv6 Pools	serviceIdentifier	1	System Defined	0	0 0
Text Object		0			
PlexConfig Object	tcp_conn_limit	0	System Defined	0	2.3

#### 1693 4. Under the **Name** column, find **netflow\_Destination**.

#### 1694

- 1695 5. Click the **edit** icon for **netflow\_Destination**.
- 1696 6. Set Variable Type to Multiple.
- 1697 7. Set **Count** to **3**.
- For Row 1, enter Security-Service to set the name of the Cisco FTD interface to which the Cisco
   Stealthwatch UDP appliance is connected.

1700 9. For **Row 2**, enter **192.168.190.120** to set the IP address of the Cisco Stealthwatch UDP appliance.

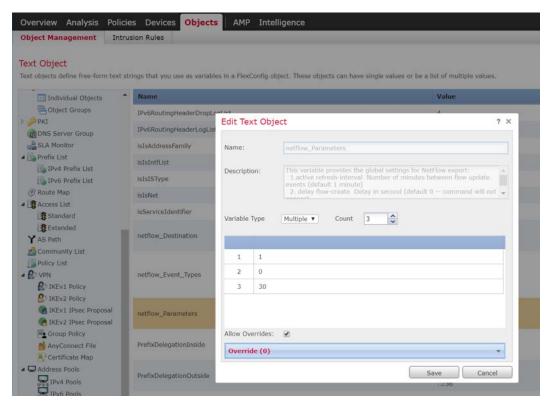
- 10. For **Row 3**, enter **2055** to set a port from which the Cisco Stealthwatch UDP appliance will receive
   NetFlow traffic.
- 1703 11. Click **Save**.

ext objects denne mee tothi text		or In a Flow	Config ob	ject. These objects can have single values or be a list of multiple values.	
- Individual Objects	Name	es in a riex	coning ob	values objects can nave single values of be a list of multiple values.	
Object Groups	IPv6RoutingHeaderDropLo	ol ist		A	
<i>₽</i> PKI	IPv6RoutingHeaderLogList	Edit Te:	xt Obje	ect	? >
DNS Server Group					
SLA Monitor	isIsAddressFamily	Name:		netflow_Destination	
IPv4 Prefix List	isIsIntfList	Descripti	001	This variable defines a single NetFlow export destination.	
Pv6 Prefix List	isIsISType	Descripti	011-	1. Interface 2. destination	
Ø Route Map	isIsNet			3. port <1-65535> UDP port number	
Access List	isServiceIdentifier				
Standard		Variable	Туре	Multiple 🔻 Count 3	
Sextended	netflow_Destination	-			
Community List					
Policy List		1	Secur	lty-Services	
	netflow_Event_Types	2	192.1	68.190.120	
IKEV1 Policy		3	2055		
IKEv2 Policy					
KEVI IPSec Proposal	netflow_Parameters				
Group Policy		Allow Ov	errides:	2	
AnyConnect File	PrefixDelegationInside				
R. Certificate Map		Overrie	de (0)		<b>T</b>

1705 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 objects can have single values or be a list of multiple values.			
Individual Objects	Name	Value	Туре	Override	
Object Groups	IPv6RoutingHeaderDropLogList	4	System Defined	0	28
PKI DNS Server Group	IPv6RoutingHeaderLogList	2	System Defined	0	00
SLA Monitor	IsIsAddressFamily	ipv4	System Defined	0	0
Prefix List	istsIntfUst		System Defined	0	0
19v4 Prefix List	IsIsISType	level-1-2	System Defined	0	0
3 Route Map	isIsNet		System Defined	0	0
& Access List	isServiceIdentifier	false	System Defined	0	0
Standard Extended	netflow_Destination	Security-Services 192.168.190.120 2055	System Defined	0	0
Community List	netflow_Event_Types	all flow-create flow-denied flow-teardown flow-update	System Defined	•	0
IKEv2 Policy     IKEv1 IPsec Proposal     IKEv2 IPsec Proposal	netflow_Parameters	1 0 30	System Defined	0	2
Group Policy AnyConnect File  Certificate Map	PrefixDelegationInside	Inside Inside-Prefix :::1:0:0:0:4/64	System Defined	0	1
Address Pools	PrefixDelegationOutside	outside Outside-Prefix ::/56	System Defined	0	2
FlexConfig	serviceIdentifier	1	System Defined	0	0
Text Object     FlexConfig Object     RADIUS Server Group	tcp_conn_limit	0	System Defined	0	0

- 1707 13. Click the **edit** icon for **netflow\_Parameters**.
- 1708 14. Set Variable Type to Multiple.
- 1709 15. Set **Count** to **3**.
- 1710 16. For **Row 1**, enter **1** as a number for minutes between flow update events.
- 1711 17. For **Row 2**, enter **0** as a number for seconds to delay flow create.
- 1712 18. For **Row 3**, enter **30** as a number for minutes for template timeout rate.
- 1713 19. Click **Save**.



1716

1715 20. Navigate to **Devices > FlexConfig**.

Overview Analysis	Policies	Devices	Objects AMP In	telligence			Deploy	0 System	Help 🔻 admin 🔻
Device Management	NAT VP	N V QoS	Platform Settings	FlexConfig	Certificates				
									O New Policy
FlexConfig Policy				Status		Last Modified			

1717 21. Click **New Policy**.

- 1718 22. Enter a **Name** (e.g., **Netflow**) for the policy.
- 1719 23. Under **Selected Devices**, add the Cisco FTD.
- 1720 24. Click **Save**.

FlexConfig Policy		Status		Last Modified
	New Policy			?
	Name:	Netflow		
	Description:	5		
		es to which you want to apply th	is policy. Selected Devices	
	FTD-F	ACS	Add to Policy	

1722 25. Click the **edit** icon for the new policy.

Overview Analysis	Policies Devices	Objects AMP In	telligence		Deploy	0 System	Help 🔻	admin v
Device Management	NAT VPN VQ0	S Platform Settings	FlexConfig	Certificates				
							New	Policy
FlexConfig Policy			Status		Last Modified			
Netflow			Targeting : Up-to-date	1 devices e on all targeted devices	2019-05-07 16:04:59 Modified by "admin"		Q	000
								Edit

1723

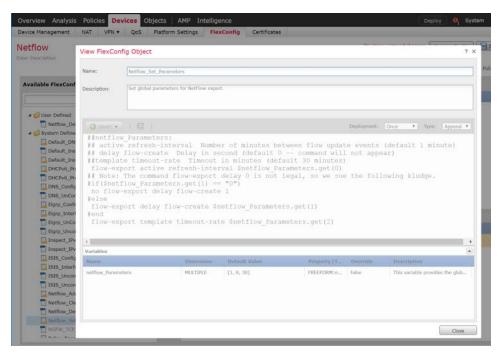
1724 26. Under Available FlexConfig, find Netflow\_Set\_Parameters, and add it to Selected Append
 1725 FlexConfigs.

rview Analysis Policies Devices Objects ce Management NAT VPN • QoS Platf		nce Config Certificates	Deploy 0, System Help +	adm
tflow Description			You have unsaved changes Preview Config Save	😢 Car
analow dividue)			Policy Assign	nments
ailable FlexConfig C StexConfig Object	Selected Pr	epend FlexConfigs		
×		Name	Description	
Our Defined     Netforw, Delete, Destination, Temp     System Defined     Default, DNs_Configure     Default, Inspection, Protocol, Disable     Default, Inspection, Protocol, Disable     Default, Inspection, Drotocol, Chable     DHCN-9, Prefix, Delegation, UnConfigure     DHS_Configure     DHS_Configure     DBS_Configure     DBS_Configure     DBS_Configure     DBS_Configure     DBS_Configure     DBS_Configure	*	opend FlexConfigs		
Elgrp_UnConfigure	Selected A	-		
E Egrp_Unconfigur_All Inspect_DPx6_UnConfigure Inspect_DPx6_UnConfigure IsISS_interime_Configure IsISS_Unconfigure ISISS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure_All IsiSS_Unconfigure IsiSS_Unconfigure_All IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigure IsiSS_Unconfigu	I	Name NetTlow_Set_Parameters	Description Set global parameters for NetFlow export.	4.6
Netflow Set Parameters				

1727 27. Click the **magnifier** icon for **Netflow\_Set\_Parameters**.

1728 28. Under Variables > Default Value, verify the minutes between flow data events, seconds to delay
 1729 flow create, and minutes for template timeout rate that were set for netflow\_Parameters.

1730 29. Click **Close**.



- 1732 30. Under Available FlexConfig, find Netflow\_Add\_Destination, and add it to Selected Append
   1733 FlexConfigs.
- 1734 31. Click the **magnifier** icon for **Netflow\_Add\_Destination**.
- 1735 32. Under **Variables > Default Value**, verify the Cisco FTD interface name, IP address of the Cisco
- 1736 Stealthwatch, and the NetFlow traffic port.
- 1737 33. Click **Close**.

Description: Create	ow_Add_Destination ie and configure a NetFlow ex	nart destination.			
Description: Create	e and configure a NetFlow ex				
ed.					
De O Insert - I II			Dept	oyment: On	ce 🔻 Type: Append
ten					
4 Variables					
Variables	Dimension	Default Value	Protectly	Override	Description
	Dimension	Default Value fail, flow-create, flow-denied, flow-teardown,	Property	Override:	Description This variable provides the

- 1738
- 1739 34. Click **Save**.
- 1740 35. Deploy changes to the Cisco FTD.
- 1741 Forwarding Rules for Cisco Stealthwatch UDP Configuration
- 1742 1. Log in to the web dashboard of the Cisco Stealthwatch Management Console.

	Dashboards	Monitor	Analyze	Jobs Con	figure Dep	oloy				
Security	/ Insight Das	hboard   Ins	ide Hosts							
Alarmin	gHosts 🕲									- ,
Concern	ndex Target Inde	x 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
0	0	0	0	0	0	0	0	0	0	0

### 1744 2. Navigate to **Settings > Central Management**.

				Jobs Conf	figure Des	oloy				Central Mar	anamant
2	Hosts 🛛	hboard   Insid	de Hosts	Exploitation	DDoS Source	DDoS Taroet	Data Hoarding	Exfiltration	Polic	UDP Directo	lyzer Configura or Configuration okup Configura gement
Concern tr	O O	O	0	O	O O	O	O	O	Molid	0	0

1745

1746 3. Click on the **ellipsis** for the Cisco Stealthwatch UDP appliance and select **Edit Forwarding Rules**.

/entory					
ppliances found					
Q Filter Appliance Inve	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	O
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- 423238f27759f21- 565093566172791d	Manage Licenses Support	O
				Edit Forwarding Rules	
				Reboot Appliance Shut Down Appliance Remove This Appliance	

1749

1748 4. Click on the **ellipsis** for the Cisco Stealthwatch UDP appliance, select **Configure Forwarding Rules**.

Isco Dashb	lthwatch <sub>oards Monitor</sub>	Analyze	Jobs	Configure	Deploy	888	esktop Client
	Configuration						
IDP Directors (	D.						
Name	Cevice IP		C Device	e Model	Management Channel Status	Configure Forwarding Rules	Actions

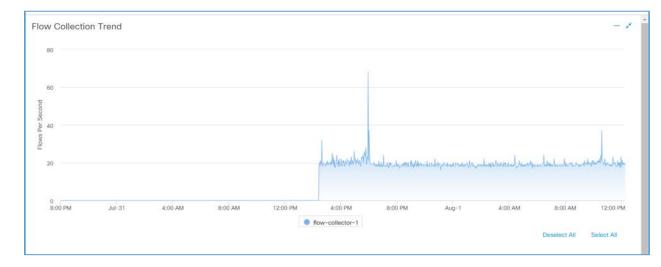
1750 5. Under Forwarding Rules, select Add New Rule.

isco	Stealthwatch Dashboards Monitor	Analyze Jobs Configure	Deploy	ktop Client
	dina Pulas Lew-uda	-director - 192.168.190.120		
orward	any Rules I sw-uup	0100001 102.100.100.120		
orward	ang Kules ( sw-dup	102.100.100.120		
orward	ang Rules ( sw-dop	(3) (333) (322, (332, (332, (23), (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (23), (232, (23), (232, (232, (232, (23), (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (232, (23), (232, (232, (232, (232, (23), (232, (23), (232, (232, (23), (232, (232, (232, (232, (23), (232, (232, (232, (232, (23), (232, (23), (232, (23), (232, (23), (23), (232, (23), (232, (23), (232, (232, (23), (232, (23), (23), (23), (23), (23), (23), (23), (23), (2		
	all Search			Sync ort/Export ~
		SOURCE IP ADDRESS & POR	DESTINATION IP ADDRESS	

- 1752 6. Enter a description (e.g., **Firepower FTD**) for the rule.
- 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.
- 1755Note: These parameters were established in Cisco FTD, found in the previous section, for the1756netflow\_Destination object.
- For destination IP address, enter the IP address (e.g., 192.168.190.122) of the Cisco Stealthwatch
   Flow Collector.
- 1759 9. For **destination port**, enter the port (e.g., **2055**) of the Cisco Stealthwatch Flow Collector.
- 1760 Note: This port was configured during the setup of the Flow Collector.

ISCO	Dashboards	Monitor	Analyze	Jobs	Configure	Deploy	
orwardi	ng Rules	sw-udp-d	lirector - 1	92.168.	190.120		
Forwardi	ng Rule						
DESCRIPTION	I (OPTIONAL)						
Firepower	ETD						
SOURCE IP AI	DDRESS:PORT =						
192.168.1	90.1:2055						
	IP ADDRESS *						
192.168.1	90.122						
DESTINATION	PORT NUMBER =						
2055							

1762 10. On the Cisco Stealthwatch Management Console dashboard, view the Flow Collection Trend graph
 1763 to verify that the Cisco Stealthwatch Flow Collector is receiving packets from the Cisco
 1764 Stealthwatch UDP.



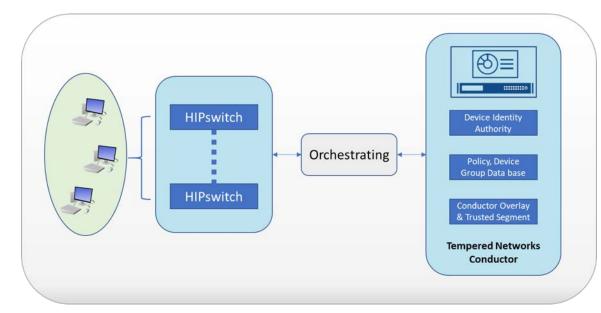
1765

# 1766 2.7.3 Tempered Networks Identity Defined Networking (IDN)

1767 Tempered Networks IDN provides cryptographically defined host identifiers using the HIP protocol
1768 rather than using IP addressing. Network traffic traverses an overlay network using HIP switches that

1769 effectively cloak that traffic from the production network. A notional architecture is depicted in Figure

# 1770 2-2 below.



1771 Figure 2-2 Architecture of Networks IDN

#### 1772

1773 Tempered Networks Conductor is the orchestration engine and intelligence behind an IDN. As shown in1774 the above figure, the Conductor is responsible for creating and executing security policies and overlays.

1775 It is also responsible for issuing unique Cryptographic IDs (CIDs) to the IDN endpoints that enforce

1776 explicit trust relationships through device-based whitelisting.

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.

1780 Installation involves the deployments of the Tempered Networks Conductor and HIPswitches. A

- 1781 Conductor open virtual appliance or application (OVA) file and a HIPswitches OVA file were provided by
- 1782 Tempered Networks.

### 1783 2.7.3.1 Conductor Installation

- 1784 System Requirements
- 1785 **CPU**: 4
- 1786 Memory: 4 GB RAM
- 1787 Storage: 120 GB
- 1788 **Operating System**: Linux Red Hat

1789 Network Adapter: VLAN 1201

### 1790 Tempered Networks Conductor Installation

- 1791 1. Log in to the vSphere Client.
- 1792 2. Select File > Deploy OVF Template.
- Respond to the prompts with information specific to your deployment, including the ova package
   location, name and location, storage, networking and provisioning, etc.
- 1795 4. Click **Power On After Deployment,** and click **Finish**.
- 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.

# 1798 2.7.3.2 HIPswitch Installation

### 1799 System Requirements

- 1800 **CPU**: 4
- 1801 Memory: 1 GB RAM
- 1802 **Storage**: 1 GB
- 1803 **Operating System**: Linux Red Hat
- 1804 Network Adapter: VLAN 1201
- 1805 HIPswitch Installation
- 1806 1. Log in to the vSphere Client.
- 1807 2. Select File > Deploy OVF Template.
- Respond to the prompts with information specific to your deployment, including the ova package
   location, name and location, storage, networking and provisioning, etc.
- 1810 4. Click **Power On After Deployment**, and click **Finish**.
- After the installation, use the username **mapconfig** and the corresponding password to connection
   the HIPswitch the conductor.
- 1813 6. Use the username underlayaddress and its corresponding password to setup the IP address,1814 netmask, gateway, and DNS for the HIPswitch.
- 1815 7. Repeat the above installation procedures to install additional HIPswitches.
- 1816 <u>Tempered Networks Conductor and HIPswitch Configuration</u>

1817 The configuration for the Conductor and HIPswitches is done through the browser connected to the

- 1818 Conductor *https://ConductorIP*. Below is the log in page.
- 1819 1. Enter the **username** and **password** to open the Dashboard.

Conductor		
	Sign In	
	Username	
UIITT	Password	
	Sign In	

### 1820

1821 2. Click Settings tab.

Conductor Dasht	oard Overlays Devic	es HPservices Peop	ke Settings		Search		4 4
ashboard	HIPservice mod	dels	HIPservice versions	10	Recently viewed items		
					No recently viewed items		
2/3 unline	sore I inPanito Hillhannice models in Conductor	HPsen	toos 1v213		Alert Notifications	Eve	nt Monitors
IPservices		Show all HIPsenvices	Filter	ж	No recent alerts		
IlPservice -	Model	Status			no recent diens		
HIPSwich Internal 1101 BHI@40130#4232576EA055	HIPswitch-300v v2.1.3	192.168,100,180	4040%		Overlay Network	ks	+New_
HPSwitch Radiology 1501 BHig40130#4232F030F338	HIPswitch-300v v2.1.3	192,168,150,180	TOUR		Name		
< > Sort by Name •		1	Display revoked HiPse	ervices na 1-2 of 2	PACS Systems		. 🕤
					Devices		
					Devices	Fitter	ж

#### 1822

1823 3. From this page, you can set up license and perform the system setup. Click the Setup button to1824 enter the system setup.

Conductor Dashboard Overlays Devices HiPservices People	e Setlings	- Dan		
ettings				•
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	Serial number		
Email settings are incomplete. Click the Edit Settings button to update.	Los cenerge	4232D38A953A Conductor device ID		
		AMA@40130#4232D3	5A953A	
Monitor & Alert Settings		Network adapter 1		
•	Edit Settings	Web access is enab		
Global monitor settings		IP address	192.168.120.180	
Frequent events warning O		Netmask Default gateway	255.255.255.0 192.168.120.1	
Number of events 3		DNS servers	8.8.8.8.4.4.8.8	
In how many minutes 10				
		Network adapter 2		
		Disabled		
Conductor High Availability				

Enter the proper network parameters for the Conductor, including the IP address (e.g.,
 1827 192.168.120.180), Netmask (e.g., 255.255.255.0), Default gateway (e.g., 192.168.120.1), a

**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**.

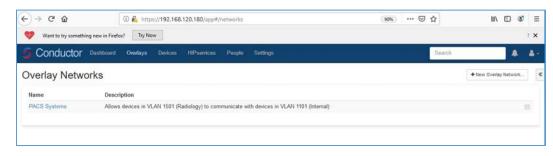
lost name	Domain name
conductor	
Network adapter 1 Network	adapter 2
Enable network adapter	☑ Enable web access to Conductor
letwork configuration	
Static IP	~
IP address	Netmask
192.168.120.180	255.255.255.0
Default gateway	
192.168.120.1	
DNS1	DN S2
8.8.8.8	4488

1829

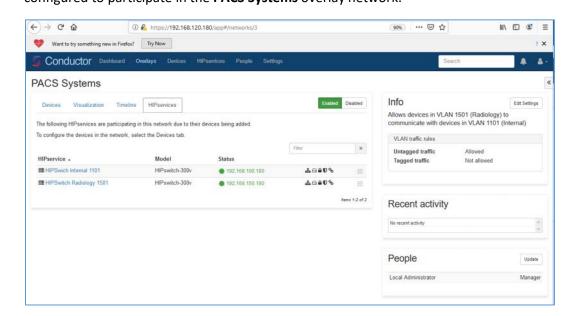
1825

1830 5. An Overlay is configured to support the microsegmentation. Click the **Overlay** tab to open the

following page, and you can add a new overlay by clicking the + New Overlay Network.... The page
below shows a configured overlay called PACS Systems.



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.



#### 1837

- 1838 7. Two special VLANs were created for each of these two HIPswitches under PACS Systems overlay:
- 1839 VLAN 1302 for HIPswitch Internal 1101
- 1840 VLAN 1303 for HIPswitch Radiology 1501
- 1841 8. Devices to be protected under the HIP network will be connected to these two HIPswitches1842 through the VLANs:
- 1843 PACS Servers are connected to VLAN 1302 under the HIPswitch Internal 1101
- 1844 Medical imaging devices are connected to VLAN 1303 under the HIPswitch Radiology 1501

- 1845 After creating a secure layer in the Conductor and adding those medical imaging devices and PACS
- 1846 servers to that layer, the medical imaging device and PACS server can be set up as trusted, by selecting
- 1847 the Enable button on the overlay page. Once they are trusted, communication between those medical
- 1848 imaging devices and PACS servers will be established. All the communication will be encrypted.
- 1849 The microsegmentation is achieved by using the HIPswitch. Other VMs will not be able to communicate1850 with these two devices unless they are configured to do so.

## 1851 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.

#### 1857 Zingbox Cloud Setup

- 1858 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.
- 1861 3. Download either the .ova or the .iso file, depending on your environment's requirements.

#### 1862 System Requirements

- 1863 **CPU**: 4
- 1864 **Memory**: 8 GB RAM
- 1865 Storage: 256 GB (Thin Provision)
- 1866 **Operating System**: CentOS 7
- 1867 Network Adapter 1: VLAN 1101
- 1868 Network Adapter 2: Trunk Port
- 1869 Zingbox Inspector Installation
- 1870 1. Create a new virtual machine, and under **configuration** select **Typical**.
- 1871 2. Click Next >.

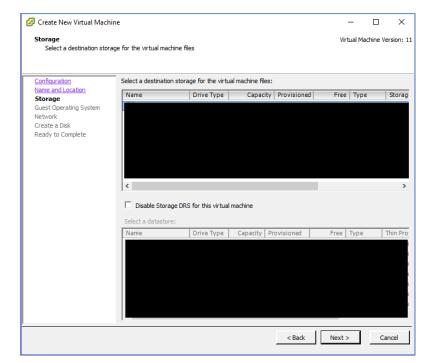
Configuration				
Select the configuration for	the virtual machine	Virtual M	lachine Ver	sion:
Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete	Configuration Typical Create a new virtual machine with the most common devices and of C custom Create a virtual machine with additional devices or specific configu-		ions.	

1873 3. Create a **Name** for the virtual machine and assign it an **Inventory Location**.

### 1874 4. Click **Next** >.

Create New Virtual Mach	ine	-		×
Name and Location Specify a name and locat	ion for this virtual machine	Virtual M	lachine Ver	sion:
Configuration	Name:			
Name and Location	[Test] Zingbox Inspector			
<u>Storage</u> Guest Operating System Network	, Virtual machine (VM) names may contain up to 80 characters and they mus vCenter Server VM folder.	st be unique wit	hin each	
Create a Disk Ready to Complete	Inventory Location:			
				~

- 1876 5. Select a **destination storage** for the VM.
- 1877 6. Click **Next** >.



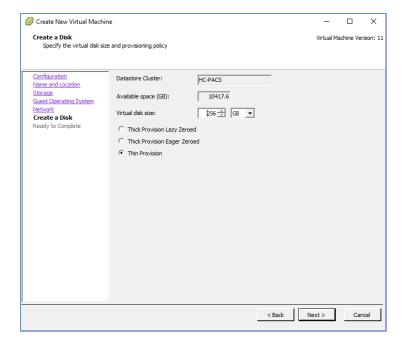
- 1879 7. Check Linux and set version to CentOS 4/5/6/7 (64-bit).
- 1880 8. Click Next >.

	1	-		>
Guest Operating System Specify the guest operatin	system to use with this virtual machine	Virtua	l Machine Ve	rsior
Configuration Name and Location Storage Guest Operating System Network Create a Disk Ready to Complete	Guest Operating System:	provide the appropri	iate default	s for

- 1882 9. Connect **2 NICs** to the virtual machine and assign them to a **network**.
- 1883 10. Check **Connect at Power On** for both NICs.
- 1884 11. Click **Next >**.

Create New Virtual Machin Network Which network connection	ne is will be used by the virtual machine?	— Virtual Ma	achine Vers	×
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? Network NIC 1: HC-PACS-VLAN-1701 (CommonLabSwitch) VM0NET NIC 2: HC-PACS-VLAN-1701 (CommonLabSwitch) VM0NET		Connect a Power O	
	If supported by this virtual machine version, more than 4NICs can be virtual machine is created, via its Edit Settings dialog. Adapter choice can affect both networking parformance and migration the VMware KnowledgeBase for more information on choosing among supported for various guest operating systems and hosts.	ompatibilit	y. Consult	
	< Back	lext >	Canc	el

- 1886 12. Set a Virtual disk size and Provisioning method.
- 1887 13. Click Next >.



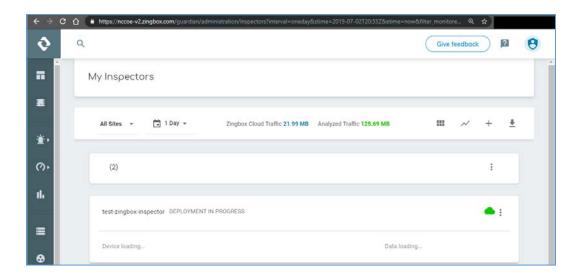
- 1889 14. Verify virtual machine settings are correct.
- 1890 15. Check **Edit the virtual machine settings before completion**.
- 1891 16. Click **Continue**.

Create New Virtual Mach	ine	- □ >
Ready to Complete Click Finish to start a tas	k that will create the new virtual mad	Virtual Machine Version
Configuration	Settings for the new virtual mac	hine:
Name and Location Storage	Name:	[Test]ZingboxInspector
Guest Operating System		
Network		
Create a Disk		
Ready to Complete	Guest OS:	
	NICs:	CentOS 4/5/6/7 (64-bit)
	NIC 1 Network:	Z 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 sett	tings before completion
	Show all storage recommend	dations
	Creation of the virtual mac	hine (VM) does not include automatic installation of the guest operating on the VM after creating the VM.
		< Back Continue Cancel

- 1893 17. Set **memory** to **8 GB**.
- 1894 18. Set **CPUs** to **4**.
- 1895 19. Under **New CD/DVD (adding)**, set these parameters:
- a. Check **Connect at power on.**
- 1897 b. Select **Datastore ISO File**, then browse for the *ZingOS.iso* file in your datastore.
- 1898 20. Click **Finish**.

Itest Zingbox Inspector - Virtua         Hardware       Options   Resources           Show All Devices         Hardware         Image: CPUs (adding)         CPUs (adding)         VHCI device (adding)         When CD/DVD (adding)         New Floppy (adding)         New SCSI Controller (add         Image: New NIC (adding)         New NIC (adding)         New Hard Disk (adding)	I Machine Properties Add Remove Summary Summary S122 MB 4 Video card Deprecated [HC-PACS_L02_APM Client Device LSI Logic Parallel HC-PACS-VLAN-1701 HC-PACS-VLAN-1701 Virtual Disk	Connected     Connected     Connect at power on      Device Type     Collent Device     Note: To connect this device, you must power on the     virbual machine and then click the Connect CD/DVD     button in the toolbar.      Host Device     [-[ZngBox/ZingOS-1.241-x86_64.iso]     Browse      Mode

- 1900 21. Connect to the inspector console and follow the on-screen prompts to finish the configuration.
- 1901 22. In a web browser, enter the **URL** of your Zingbox Cloud instance.
- 1902 23. Enter your Zingbox Cloud credentials.
- 1903 24. Click **Login**.
- 1904 25. On the home page, navigate to **Administration** > **My Inspectors**.
- 1905 26. Verify that the host name of the Zingbox Inspector set up previously is visible and connected1906 (shown by the green cloud icon).



# 1908 2.7.5 Forescout CounterACT 8

1909 Forescout CounterACT is a network access control tool that can perform device discovery and

1910 classification, risk assessment, and control automation through passive and active techniques. For this

1911 project, the intended use of Forescout is to manage device compliance and perform necessary

1912 remediation when devices fall out of compliance.

### 1913 System Requirements

- 1914 **CPU**: 2
- 1915 Memory: 8 GB RAM
- 1916 Storage: 80 GB (Thin Provision)
- 1917 **Operating System**: Linux Kernel 3.10
- 1918 Network Adapter 1: VLAN 1201
- 1919 Network Adapter 2: Trunk Port

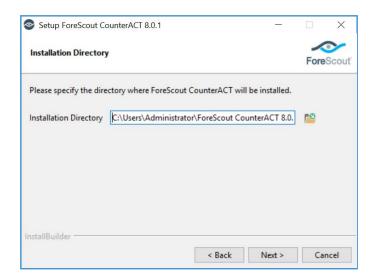
#### 1920 Forescout Appliance Installation

- To begin installation, obtain the Forescout ISO. Load the Forescout ISO into the VM's CD/DVD drive.
   Make sure the CD/DVD drive is set to **Connect at Power On**.
- 1923 2. Boot up the VM and begin the installation process.
- 1924 3. Select Install CounterACT.
- 1925 4. Press Enter to reboot.
- 1926 5. Select **option 1** to configure CounterACT.

- 1927 6. Select **option 1** for standard installation.
- 1928 7. Press **enter** to proceed.
- 1929 8. Select **option 1** for CounterACT Appliance.
- 1930 9. Select **option 1** for Per Appliance Licensing Mode.
- 1931 10. Enter appliance **description**.
- 1932 11. Give appliance a **password**.
- 1933 12. Enter **forescoutCA** and apply this as the appliance host name.
- 1934 13. Assign the appliance an IP address **192.168.120.160**.
- 1935 14. Assign appliance a network mask **255.255.255.0**.
- 1936 15. Enter **192.168.120.1** as the appliance's gateway.
- 1937 16. Enter domain name *pacs.hclab*.
- 1938 17. Enter DNS server address **192.168.120.100**.
- 1939 18. Review configuration and run test.
- 1940 19. Once the test passes, select **done**.
- 1941 Forescout CounterACT Console Installation
- 1942 1. Run Install\_Management.exe.
- 1943 2. Click **Next** >.



- 1944
- 1945 3. Verify Installation Directory as C:\Users\Administrator\ForeScout CounterACT 8.0.1; click Next >.

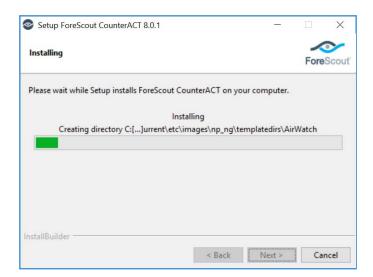


1947 4. When the **Ready to Install** screen appears, click **Next** > to begin the installation process.

Setup ForeScout CounterACT 8.0.1		-		×
Ready to Install			Fore	Scou
Setup is now ready to begin installing ForeScout Co	unterACT	on your comp	outer.	
nstallBuilder				
	Back			ncel

1948

An Installing screen will appear that provides a status bar indicating degree of installation
 completion. Click the Next> button to allow the installation to proceed.



As the installation nears completion, a screen indicating Completing the ForeScout 8.0.1 Setup
 Wizard appears. Check Create Desktop shortcut; click Finish.

Setup ForeScout Counte	ACT 8.0.1 - X Completing the ForeScout CounterACT 8.0.1 Setup Wizard
ForeScout	Setup has finished installing ForeScout CounterACT 8.0.1 on your computer.
	< Back Finish Cancel

1954

- 1955 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**.
- 1958 c. Enter Administrator in the User Name text box.
- 1959 d. Enter the password in the **Password** box.



### 1961 Forescout CounterACT Configuration

1962 To use the full function offered by the Forescout CounterACT, proper network configuration is required,

1963 which may include the monitor and response interface assignments at the data center, the network

1964 VLAN and segmentation information, IP address range that the CounterACT appliance will protect, user

1965 Directory account information, domain credentials, core switch IP address, and vendor and SNMP1966 parameters.

1967 After completing the installation, log in to the CounterACT Console using the steps below:

Select the CounterACT icon from the server on which you installed the CounterACT Console. A log
 on page appears, as depicted below.



- 1971 2. Provide the following information and select **Login** to open the Console:
- 1972 a. Enter the IP address **192.168.120.160** in the **IP/Name** field.
- b. In the **User Name** field, enter **admin**.
- 1974 c. In the **Password** field, enter the admin password which is defined during the installation.

		nsole - admin connec	ted to 192.168	3.120.160 - Licens	e: Demo - 114	days le	ft - Lice	-		×
Ella Baporta Actiona I	oola <u>L</u> og	p Display Help								
	uť		Home	Asset In		8				۲
Views	«	All Hosts		Search		Q	Online10ffline >	2	13 OF 13	B HOST
Search	Q	Host +	IPv4 Address	MAC Address	_ Display Name		Function	Actions		
All Hosts (13)		<ul> <li>blueflow pacs helab</li> </ul>	192 168 120 20	5			Computer	10		
> 🚺 Policies		* PACSIHYLAND-VNA	192,168,130,12		Hyland Service U	tér.	Computer	10		
History		* PACSIHYLAND-PGCO			Hyland Service U		Computer	18		
		* PACSIHYLAND-NILRE			Hyland Service U		Computer	10		
		* PACSIAD	192,168,120,10				Computer	18		
Filters			perating System endor and Mode		nknown					¥ ([
Search	Q	General	Genera	i						
🗢 All										
Segments (13) Crganizational Units Default Croups Croups Croups		More	Function Operatin Vendor : Function	on: inta: erprint: s SecureConnector Versi	2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	ICP tibly Linux ie nown nown nown interACT D	ame online 2.6.32 or Netgea avice Classificati avice Classificati	on Engine		

- 1976 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.
- 1978 The figure below shows the sample asset inventory page. (Further network configuration will be needed
- 1979 for complete inventory information.)

Ella Boporta Actiona Toola Log Displ	ay Hela			
	🖌 Home	Asset Inventory	Policy	۲
Views				
Search Q				
The Classification				
Classification (Advanced)				
Ners Users				
Suest Registration				
User Directory				
🖽 Open Ports				
💶 Windowa				
Filters				
Search Q				
All				
Segmenta (13)				
Organizational Units				
E Default Groups				
Groups				

1981 The figure below shows the sample **Policy Manager** page. Further network configuration and policy

1982 definition will be needed for complete policy information.

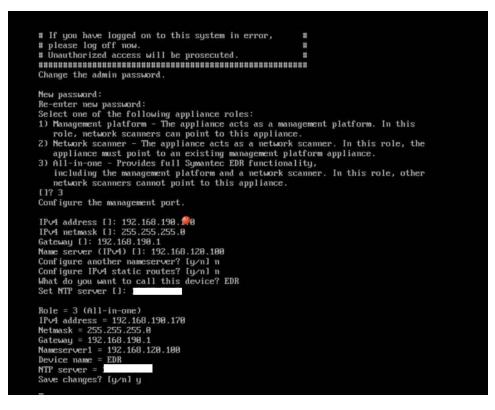
	ouť		Â		៨	Asset Inventory		Policy		
Policy Folders	Policy Man	lager			Search		Q. 🗹 Show	subfolder policies		
	Name	Category	St.	User Scope	Segments	Groups	Exceptions	Conditions	Actions	Add
Policy	🗢 Asset Classif	ica Classification		Complete	192.168.0.0/16			No Conditions		Edit
	NAT Devic	esClassifier						Device is NAT:	100	Categoria
	Mobile De	vicClassifier						Network Functi	100	Remove
	Windows	Classifier						Network Functi	78	Duplicat
	Printera	Classifier						Network Functi	100	Move to
	Linux/Upb	Classifier						Network Functi	<b>B</b>	Export
	Macintosh	Classifier						Network Functi		Start
	VolP Devi	resClassifier						Network Funct		Stop
	Network D	ev Classifier						Network Functi		Custom
	Unclassifie	ed Classifier						No Conditions	18	
										Comparis
										Help

1983

# 1984 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.

- 1988 System Requirements
- 1989 **CPU**: 12
- 1990 Memory: 5 GB RAM
- 1991 **Storage**: 500 GB (thin provisioned)
- 1992 **Operating System**: CentOS 7
- 1993 Network Adapter 1: VLAN 1901
- 1994 Network Adapter 2: SPAN\_PACS
- 1995 Symantec EDR Installation
- 1996 1. Launch the virtual appliance after deployment of the vendor-provided *SEDR-4.0.0-483-VE.ova* file.
- Enter default username **admin** and default password. You will be required to change the default
   password by entering a new password.
- After changing the default password, the bootstrap will automatically launch. Enter the following
   options during the bootstrap:
- 2001 IPv4 address []: 192.168.190.17
- 2002 IPv4 netmask []: 255.255.255.0
- 2003 Gateway []: 192.168.190.1
- 2004 Name server (IPv4) []: 192.168.120.100
- 2005 Configure another nameserver? [y/n]: n
- 2006 Configure IPv4 static routes? [y/n]: n
- 2007 What do you want to call this device?: EDR
- 2008 Set NTP server []: X.X.X.X
- 2009 4. After verifying the correct details, enter **Y** to save changes. The appliance will restart.
- 2010
- 2011



- 2013 5. Open a web browser and travel to the virtual appliance at *https://192.168.190.170*. Enter the
  2014 username setup and password \*\*\*\*\*.
- 2015 6. Follow the prompts to create the initial admin account.

•	• • • •
Create an Admini	strator Account
Login	admin
Password	- Annese
	Password Strength: Moderate
Confirm Password	- apparent
Display Name	Doptay Name
User Email	User Email
Receive email	notification when incidents occur
Prev	Finish

2020

- 2017 7. Select the **Settings** menu, and then select the **Global** sub-menu.
- 2018 8. Ensure Enable Symantec Endpoint Protection Correlation is checked.
- 2019 9. Select Add SEPM Database and enter the following options.

	Symantec EDR					Symantec EDR is Healthy 🧭	Admin
Q	🔹 Synapse	Enable Sym	antec Email Security cloud Corre	lation			
			ning Correlation antec Endpoint Cloud Correlation	í.			
ጜ		<ul> <li>Enable Sym</li> </ul>	antec Endpoint Protection Correl	ation			
12		Symantec Endpo	int Protection Manager (SEPM	I) Databases			
		Name	IP Address	Port	Enabled	Status	
				No data a	vailable.		
8		(+) Add SEPM	Database				
Ø		Download Synaps	a Log Collector for SEPM Ember	Ided DB			
	Endpoint Communication Channel, SEP Policies, and Endpoint Activity Recorder	SEPM Controller n	ot configured	e	Configure SEPM Controller		
	0	Enable ECC	2.0 (requires at least 1TB of har	d disk snace) 🔍			

2021 10. Provide the information that follows, and click **Save**:

- 2022 DB Type: Embedded DB
- 2023 Entry Name: SEPM
- 2024 Address: 192.168.190.172
- 2025 Port: 8081
- 2026 **Connection Password:** *enter your connection password* 
  - Enabled: Checked

	O Symantec EDR			
Q,	< Global ®	Add SEPM 💿		×
	< Global -	DB Туре	Embedded DB	~
	Cynic Sandboxing	Entry Name	SEPM	
		IP Address	192.168.190.172	
	Data Handling	Port	8081	
		Connection Password		
		Enabled	<b>v</b>	
	🛸 Synapse		Cancel	le Save
			Cance	

- 2029 11. After completing the integration with SEPM, select the Settings menu, then select the Appliances
   2030 sub-menu.
- 2031 12. Select Edit Default Appliance.
- 2032 13. Select Add Internal Network to create and add a Subnet, Netmask, and Description for each
- 2033 internal network listed below. Make sure to save after entering the network details.

= 0	Symantec EDR			Symantec EDR is	s Healthy 🧭 Admin
Q.	< Default Appl	iance •			
2		Subnet	Netmask	Description	
<u>&amp;</u>	Internal Network Configuration	192.168.100.0	255.255.255.0	VLAN 1101 Internal Network	1
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
2		192.168.140.0	255.255.255.0	VLAN 1401 PACS 1	T.
		192,168.141.0	255.255.255.0	VLAN 1402 PACS 2	1
<b>2</b> 1			SEE ALL 6		
<u>ې</u>					
				Add Internal Network	

2034
------

2035	 Subnet: 192.168.100.0 Netmask: 255.255.255.0 Description: VLAN 1101
2036	 Subnet: 192.168.120.0 Netmask: 255.255.255.0 Description: VLAN 1201
2037	 Subnet: 192.168.130.0 Netmask: 255.255.255.0 Description: VLAN 1301
2038	 Subnet: 192.168.140.0 Netmask: 255.255.255.0 Description: VLAN 1401
2039	Subnet: 192.168.141.0 Netmask: 255.255.255.0 Description: VLAN1402
2040	Subnet: 192.168.150.0 Netmask: 255.255.255.0 Description: VLAN 1501
2041	 Subnet: 192.168.160.0 Netmask: 255.255.255.0 Description: VLAN 1601
2042	 Subnet: 192.168.180.0 Netmask: 255.255.255.0 Description: VLAN 1801
2043	Subnet: 192.168.190.0 Netmask: 255.255.255.0 Description: VLAN 1901

ternal Network Configura	ation		
Subnet	Netmask	Description	
192.168.100.0	255.255.255.0	VLAN 1101 Internal Network	-
192.168.120.0	255.255.255.0	VLAN 1201 Enterprise Network	0
192.168.130.0	255.255.255.0	VLAN 1301 Clinical Workstations	:
192.168.140.0	255.255.255.0	VLAN 1401 PACS 1	:
192.168.141.0	255.255.255.0	VLAN 1402 PACS 2	:
192.168.150.0	255.255.255.0	VLAN 1501 Radiology Departments	1
192.168.160.0	255.255.255.0	VLAN 1601 Clinical Application Services	;

2045 14. Select **Settings** and then **Global**.



=	O Symantec EDR				Symantec EDR is Healthy 🥑	Admin 🗸
٩		Enable Symantec End				
		Symantec Endpoint Protec	tion Manager (SEPM) Databases			
<u></u>		Name A	ddress Por	rt Enabled	Status	
E		(+) Add SEPM Database		No data avaliable.		
Í		Download Synapse Log Colle	actor for SEPM Embedded DB			
ð	Endpoint Communication Channel, SEP Policies, and	SEPM Controller not configur	ed	Configure SEPM Contro	oliar	
٩	Endpoint Activity Recorder	Enable ECC 2.0 (requi	res at least 1TB of hard disk space) 🤅	2		
	Automatic Submission	Submit suspicious files	to sandbox for analysis			
	Backup	Backup is disabled	Configure Backup			
		Income Ro.	Izznad To	Evolution Date	Contiliento Statue	

2049 16. Select **Settings** and then **Appliances**.

≡	🚱 Symantec EDR					Symantec EDR is Healthy 🥥	Admin 🗸
Q	< Default Appliance	Q					
\$ \$		General Settings	Tons: services				
1		Internal Network Configuratio 192.168.100.0	255.255.255.0 NET INA SH		VLAN 1	1101 Internal Network	
		DNS Settings	месоноллу				
ø						Edit Dufauti Appliance 🕜	
	Appliances						
	Name Mgnt IP	Role	Mode	Scanning	Status		
	EDR 192.160.190	170 Management/Scanner/Proxy	Tap	Disabled	Healthy	o o	

2050

•

2051	17. Select <b>EDR</b> from the appliances list.
2052	18. Turn Scanning on under the Network Interface Settings.
2053	Symantec EDR and SEP Correlation
2054 2055	1. Open a web browser and travel to the virtual appliance at <i>https://192.168.190.170</i> . Log in with your administrator account.
2056	2. From the settings menu, select <b>global settings</b> .
2057	3. Select Download Synapse Log Collector for SEPM Embedded DB.
2058	4. After the SEPMLogCollector.msi finishes downloading move to the SEP Manager (SEPM).
2059	5. Launch the SEPMLogCollector.msi file from SEPM.
2060	6. Continue through the setup wizard prompts by clicking <b>Next</b> to use the default settings.
2061 2062	7. After installation is complete, launch the <b>Log Collection</b> for <b>SEPM</b> embedded database configuration utility, and enter the values below:
2063	Service Hostname (optional): Leave blank
2064	<ul><li>Service IP address: 192.168.190.172</li></ul>
2065	<ul> <li>Service port: 8082</li> </ul>
2066	<ul> <li>Log Collector connection password: enter connection password</li> </ul>
2067	Confirm connection password: enter connection password again
2068	• SEPM embedded database configuration password: enter embedded database password
2060	9 After entering values into configuration utility slick <b>Confirm</b>

2069 8. After entering values into configuration utility, click **Confirm**.

Convice Hestrome (antional)	
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

# 2071 2.8 Endpoint Protection & Security

## 2072 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
 whitelisting, intrusion prevention, and file integrity monitoring. For this project, a DCS:SA agent was
 installed on both PACS servers in our architecture.

- 2076 System Requirements
- 2077 **CPU**: 4
- 2078 Memory: 8 GB RAM
- 2079 Storage: 120 GB (Thin Provision)
- 2080 Operating System: Microsoft Windows Server 2016 Datacenter
- 2081 Network Adapter: VLAN 1901
- 2082 Symantec Data Center Security Installation
- 2083 1. Launch server.exe.
- 2084 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, click 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/.	

- 2086 3. Check I accept the terms of the license agreement.
- 2087 4. Click **Next >**.

AGREEMENT SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO LICENSE THE TRIALWARE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE TRIALWARE SOFTWARE (REFERENCED BELOW AS "YO OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS TEMPORARY TRIALWARE SOFTARE EVALUATION	ISE /
WILLING TO LICENSE THE TRIALWARE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE TRIALWARE SOFTWARE (REFERENCED BELOW AS "YO OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE	
LICENSE AGREEMENT ("TRIALWARE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS TRIALWARE AGREEMENT CAREFULLY	E
I accept the terms of the license agreement     F	Print

- 2089 5. Verify install location.
- 2090 6. Click Next >.

different		, or click Change	to install to a		
_	Install Symantec Data	Center Security	Server Manag	er to:	
	C:\Program Files (x86 Server\Server	)\Symantec\Data	Center Secur	ity	Change

2094

2092 7. Review settings.

2093 8. Click Install >.

Deadland Trade Haller D		
Ready to Install the P		
The wizard is ready to b	begin installation.	
Review the settings ar Cancel to exit the wiza	nd dick on 'Install'. If you want to change any ard.	settings, click Back. Clic
Installation Type: Server Settings:	Evaluation (Install Local Database)	
Directory: C:\Program	m Files (x86)\Symantec\Data Center Security	Server\Server
InstallChield		
InstallShield		

2095 9. Wait for setup and install process to complete.

Setup Status Symantec Data Center Security Server Manager is configuring your new software installation. Installing C:\\{65A60777-4A68-4691-AB60-FC5621BAFD35}\manager.exe	Symantec Data Center Sec	urity Server Manager 6.8.0	×
installation. Installing	Setup Status		
		ecurity Server Manager is configuring your new	software
C:\\{65A60777-4A68-4691-AB60-FC5621BAFD35}\manager.exe	Installing		
	C:\\{65A60777-4A68	4691-AB60-FC5621BAFD35}\manager.exe	
stallShield	nstallShield		
Cancel			Cancel

2097 10. SQL Server will automatically be installed during the setup process.

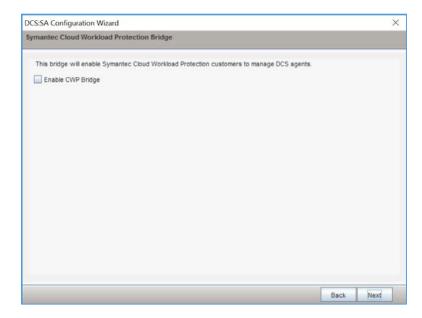
Install Setup Files			
	SQL Server Setup files are being inst	alled on the system.	
	Task	Status	
	Install Setup files	In Progress	

- 2099 11. Provide the information below, and click on **Next**:
- 2100 Agent port: 443

- 2101 Bridge port: 2443
- 2102 Console port: 4443
- **Web server administration port**: 8081
- **Web server shutdown port**: 8006

General Setting	15	Tomcat Connector Attributes -		
Agent port	443	Web server administration port	8081	
Bridge port	2443	Web server shutdown port	8006	_
Console port	4443		0000	

2106 12. Uncheck Enable CWP Bridge and click Next.



2108 13. Verify settings for FQDN Hostname as WIN-RUQDO7KL8A7, Static IP Address as 192.168.120.207,

and Java Heap Size as 6144 and then click Next.

DCS:SA Configuratio	n Wizard	
Server Settings		
Certificates		
Agent Certifica	ste	
Server Certific	ate	
This Server's Ne	twork Address Settings	
	Use FQDN Hostname for Certificate	
FQDN Hostname	WIN-RUQD07KL8A7	
Static IP Address	192.168.120.207	
JVM Settings		
Java Heap Size	(MB) 6144	

2110

2111 14. Create a **password** for the database connection.

### 2112 15. Click **Next**.

reate Database		
Connection Parameters -		
Hostname 1	27.0.0.1	
Database Instance		
O Database Port		
'sa' privileged User		
Password ★ 🔹	•••••	
Confirm Password ★ 🔒	******	

- 2113
- 2114 16. Verify **Unified Management Console** connection settings.
- 2115 17. Create a password for **Unified Management Console** connection.

2116 18. Click **Next**.

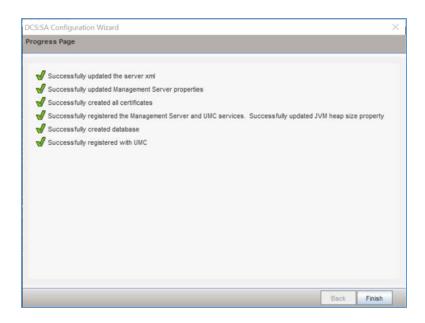
S:SA Configuration Wize	rd	
gister with Unified Man	agement Console	
UMC Details		
Hostname	192.168.120.207	
Port	8443	
User Name	dcsadmin	
Password ★	•••••	
Confirm Password ★	•••••	

## 2117

2118 19. Verify configuration settings and click **Next**.

Summary Page	
Review the settings and click on 'Configur wizard	e'. If you want to change any settings, click Back. Click Cancel to exit the
Installation Type: Evaluation (Install Loca	al Database)
Server Settings Directory: C:\Program Files (x86)\Syman Ports: Agent: 443, Console: 4443, Web	
Database Settings Host: 127.0.0.1 Instance: SCSP Database Name: SCSPDB	
JVM Settings Heap Size (MB): 6144	
UMC Registration Settings UMC Server: Hostname=192.168.120.20 Product Server: Hostname=WIN-RUQDO	17, Port=8443, Username=dcsadmin 7KL8A7, IP Address=192.168.120.207, Port=4443
Server Cert Attributes: extl SAN=DNS:V	VIN-RUODO7KI 847 JP-192 168 120 207 1

- 2120 20. Wait for configuration process to complete.
- 2121 21. Click **Finish**.



## 2123 22. Wait for install to complete and click **OK**.

Symantec Data	Center Security Server Manager 6.8.0	×
Setup Status		
Symantec Da installation.	ta Center Security Server Manager is configur	ring your new software
Symant	ec Data Center Security Server Manager 6	5.8.0 ×
Finis		
	The DCS Management Server was con	nfigured successfully.
		ОК
31		
InstallShield		
		Cancel

#### 2124

#### 2125 Symantec Datacenter Security Windows Agent Install

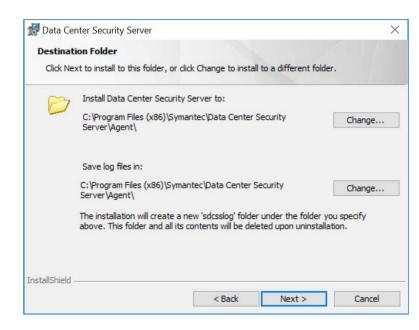
- 2126 1. Run agent.exe.
- 2127 2. Click **Next** >.



- 2129 3. Check I accept the terms in the license agreement.
- 2130 4. Click Next >.

License Agreement			
Please read the following license a	greement carefully.		
SYMANTEC SOFT	WARE END USER LIC	CENSE AGREEM	ENT
SYMANTEC CORPORATION (II			
THAILAND) OR SYMANTEC LI			
COUNTRY) ("SYMANTEC") IS V AS THE INDIVIDUAL, THE COM			
USING THE SOFTWARE (REFER			
CONDITION THAT YOU ACCES		AND CONDIT	TIONS OF
THIS SYMANTEC SOFTWARE I	LICENSE AGREEMEN	MS AND CONDIT T AND THE PRO	TIONS OF DUCT USE
THIS SYMANTEC SOFTWARE I RIGHTS SUPPLEMENT (AS DEF	LICENSE AGREEMEN FINED BELOW) (COLI	AS AND CONDIT T AND THE PRO LECTIVELY, THE	TIONS OF DUCT USE "LICENSE
THIS SYMANTEC SOFTWARE I	LICENSE AGREEMEN FINED BELOW) (COLI	AS AND CONDIT T AND THE PRO LECTIVELY, THE	TIONS OF DUCT USE "LICENSE
THIS SYMANTEC SOFTWARE I RIGHTS SUPPLEMENT (AS DEF	LICENSE AGREEMEN FINED BELOW) (COLL ENSE AGREEMENT (	AS AND CONDIT T AND THE PRO LECTIVELY, THE	TIONS OF DUCT USE "LICENSE
THIS SYMANTEC SOFTWARE I RIGHTS SUPPLEMENT (AS DEF AGREEMENT''). READ THE LIC	LICENSE AGREEMEN FINED BELOW) (COLL EENSE AGREEMENT ( greement	AS AND CONDIT T AND THE PRO LECTIVELY, THE	TIONS OF DUCT USE "LICENSE ORE
THIS SYMANTEC SOFTWARE I RIGHTS SUPPLEMENT (AS DEF AGREEMENT"). READ THE LIC I accept the terms in the license ag I do not accept the terms in the lice	LICENSE AGREEMEN FINED BELOW) (COLL EENSE AGREEMENT ( greement	AS AND CONDIT T AND THE PRO LECTIVELY, THE	TIONS OF DUCT USE "LICENSE ORE
THIS SYMANTEC SOFTWARE I RIGHTS SUPPLEMENT (AS DEF AGREEMENT'). READ THE LIC	LICENSE AGREEMEN FINED BELOW) (COLL EENSE AGREEMENT ( greement	AS AND CONDIT T AND THE PRO LECTIVELY, THE	TIONS OF DUCT USE "LICENSE ORE

- 2132 5. Verify installation and log files directories.
- 2133 6. Click Next >.



- 2135 7. Provide the information below, and click on **Next>**:
- 2136 Agent Name: WIN-RUQDO7KL8A
- Polling Interval (sec): 300

- 2138 Check Enable Intrusion Prevention
- 2139 Notification Port: 2222
- 2140 Agent Protocol: HTTPS

🛃 Data	a Center Security Server		
Agent	t Configuration		
Plea	se configure your agent's setting	JS	
	Agent Name:	WIN-RUQDO7KL8A7	
	Polling Interval (sec):	300	
	Enable Intrusion Prevention:		
	Enable Real-time notification if	f this agent requires immediate updates.	
	Enable Real-time Notification:	Notification Port: 2222	
	Agent Protocol:	HTTPS ~	
nstallShi	eld		
		< Back Next > 0	Cancel

- 2142 8. Provide the information below and click **Next**:
- 2143 Primary Management Server: 192.168.120.207
- **Agent Port**: 443
- 2145 Alternate Management Servers:
- **Management Server Certificate**: C:\User\Administrator\Desktop\agent-cert.ssh

Management Server Configuration	1	
Please configure your agent's Manage	ement Server settings	
Primary Management Server:	192.168.120.207	
Agent Port:	443	
If desired specify Alternate Mar		and the second second
ti desired, speciry Alternate Mai	nagement Servers in a comma-sep	arated list:
Alternate Management Server(s	-	arated list:
Alternate Management Server(s	-	d in order to connect
Alternate Management Server(s Access to a copy of the Manage to the Management Server. All	):	d in order to connect
Alternate Management Server(s Access to a copy of the Manage to the Management Server. All Certificate.	):    ment Server Certificate is required specified Management Servers mu	d in order to connect

- 2148 9. Specify a Server Security Group created through Symantec Datacenter Security Server or leave it
  2149 blank to use the default security group.
- 2150 10. Click **Next >**.



2153

2152 11. Verify installation and configuration settings and click **Install**.

Ready to Install		
	igs are summarized below. If you want to review or change any of click Back. Click Install to start the installation using these settings.	
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	rver: 192.168.120.207	
Alternate Management		
Management Server Por	t: 443	~
InstallShield		

2154 12. Wait for the installation process to complete.

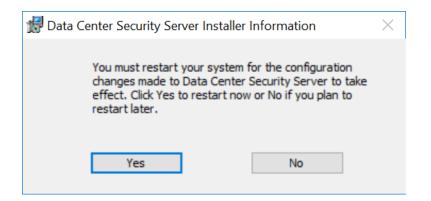
	Data Center Security Se gram features you selected a			
1	Please wait while the Insta Server. This may take sev Status:	Data Center Secur	ity	

2157

## 2156 13. Click **Finish**.

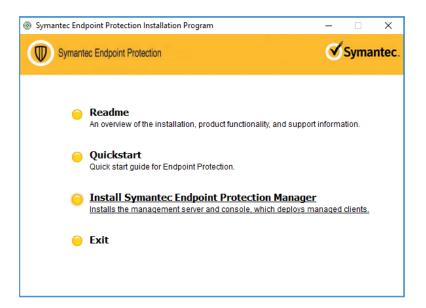
	InstallShield Wizard Completed
	The InstallShield Wizard has successfully installed Data Center Security Server. Click Finish to exit the wizard.
Symantec.	

# 2158 14. Click **Yes** to restart the agent machine.



# 2160 2.8.2 Symantec Endpoint Protection

- 2161 Symantec Endpoint Protection is an agent-based security solution that provides antivirus, intrusion
- 2162 prevention, application whitelisting, and other capabilities. For this project Symantec SEP is used to
- 2163 protect endpoints from malicious software and integrates with Symantec Endpoint Detection and
- 2164 Response to detect suspicious behavior.
- 2165 System Requirements
- 2166 **CPU**: 4
- 2167 Memory: 8GB RAM
- 2168 Storage: 240GB (thin provisioned)
- 2169 **Operating System**: Microsoft Windows Server 2016
- 2170 Network Adapter: VLAN 1901
- 2171 Symantec Endpoint Protection Manager Installation
- 2172 1. Launch Symantec\_Endpoint\_Protection\_14.2.0.MP1\_Part1\_Trialware\_EN.exe file.
- 2173 2. Select Install Symantec Protection Endpoint Manager option.



2175 3. Proceed through the install wizard by clicking **Next >.** 

🔀 Symantec Endpoint Protect	ion Manager X		
	Symantec Endpoint Protection Manager		
	The Installation Wizard will perform the following steps:		
	Install the management server and console		
	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			

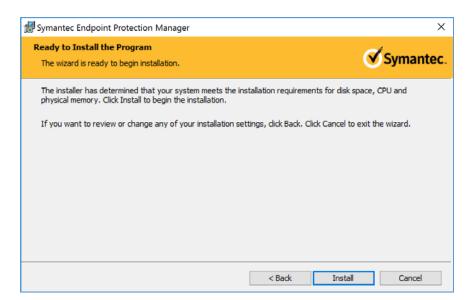
- 2177 4. Check I accept the terms in the license agreement.
- 2178 5. Click Next >.

Please read the follow	ving license agreement carefully.	Symant 🗹
	SYMANTEC SOFTWARE LICENSE AGREEMENT	,
	ORATION AND/OR ITS AFFILIATES ("SYMANTEC") SPE FIRMATION IS WILLING TO LICENSE THE LICENSED SOFTW	
LICENSED SOFTWA CONDITION THAT YO SOFTWARE LICENS DEFINED BELOW) AGREEMENT CAREF	HE COMPANY, OR THE LEGAL ENTITY THAT WILL BE ARE (REFERENCED BELOW AS "YOU" OR "YOUR") OU ACCEPT ALL OF THE TERMS AND CONDITIONS OF T SE AGREEMENT AND THE PRODUCT USE RIGHTS SL (COLLECTIVELY, THE "LICENSE AGREEMENT"). READ FULLY BEFORE USING THE LICENSED SOFTWARE. THIS ITRACT BETWEEN YOU AND SYMANTEC. BY DOWNLOADIN	ONLY ON THE THIS SYMANTEC JPPLEMENT (AS ) THE LICENSE IS A LEGAL AND

Select the location you want to install Symantec Endpoint Protection Manger and click Next >. Keep
the default location of *C*:\*Program Files (x86)*\*Symantec*\*Symantec Endpoint Protection Manager*\.

🔛 Symante	ec Endpoint Protection Manager		×
Deseniae	ion Folder xt to install to this folder, or click Browse to insta	II to a different folder.	Symantec.
	Install Symantec Endpoint Protection Manager C: \Program Files (x86)\Symantec\Symantec E Free disk space on C:\drive (system drive): 1 CPU(s): 4 Physical Memory: 8.00 GB	ndpoint 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

- 2182
- 2183 7. Select Install.



8. After installation is complete, click Next > to continue with configuration of the management
 server.

Symantec Endpoint Protect	ion Manager	Х
	Management Server and Console Installation Summary	
	The Installation Wizard has successfully installed Symantec Endpoint Protection Manager. Click Next to begin the configuration wizard.	
	<ul> <li>Install the management server and console</li> <li>Configure the management server</li> <li>Create the database</li> </ul>	
Symantec.	Click Next to configure the management server.	
Jymantee.		
	< Back Next > Cancel	

2187

2188 9. Select **Default configuration** for new installation; click **Next >**.

nanagement verter company	ation Wizard —
	Welcome to the Management Server Configuration Wizard
✓ Installation	Please select a configuration type.
000000000	Default configuration for new installation (fewer than 500 clients)
	Select this option to configure a management server that manages fewer than 500 clients and uses an embedded databas
Server Configuration	<ul> <li>Custom configuration for new installation (more than 500 clients, or custom settings)</li> </ul>
*********	Select this option to configure a server that manages more than 500 clients or uses Microsoft SQL database, or if you plan install multiple management servers.
	Recovery configuration
	Select this option to install the management server with a recovery file. The recovery file restores communication with previously deployed clenesh and includes other management server settings. A recovery file is only available if you previou installed the management server.
	Browse
	The default recovery file is detected automatically. To select a different recovery file, click Browse and navigate to the file that you want to use. For more information, see <u>Thecovery File Details.</u>
	Management server will manage fewer than 500 clients
	C mendioners and company provide provide provide provide
	The consideration of the second second second second
Symantec.	

2190 10. Provide the following information and click **Next>**.

2191	Company Name: NCCoE
2192	User name: admin
2193	Password: ******
2194	Confirm password: *******
2195	Email address: admin@nccoe.labs

ation	Create a system administrator account.			
tion		The password will be required to log on to the r	nanagement console.	
	Company name:	NCCoE		
0000000	User name:	admin		
	Password:*	•••••		
	Confirm password.*			
r Configuration	P	assword Strength: Good		
000000		for both the administrator password and the d	atabase password. If you change the	e adr
	Email address.*	admin@nccoe.labs		
	The server sends notifications and p	assword recovery information to this address.		
	V Use a specified email server			
		se settings by editing the server properties fro	m the management server console.	25
	Sender email address:	admin@pacs.hclab		
	User name:	admin		
100 C	Password:			
100 C				
	Require the specified server	to use a secure connection		
	C Use TLS	O Use SSL		
Z	-		O Yes O No	
	values. You can later change the Email server IP address or name Sender email address: User name:	aymantec-manager admin@pacs.hciab admin *******	m the management server console.	

2197 11. Confirm that **Run LiveUpdate** during installation is checked; click **Next >**.

Management Server Configu	uration Wizard —	>
	Run LiveUpdate	
✓ Installation	Symantec recommends that you run LiveUpdate during installation. LiveUpdate requires maximum computer resources and mig few hours to complete, depending on your server configuration and network bandwidth.	nt take a
	Run LiveUpdate during installation	
Server Configuration		
0000000000	Partner Information (Optional)	
	If a partner manages your licenses, you should specify the contact information here. Partners receive updates about the statu of your licenses.	IS
	Specify partner information	
	Partner email address:	
	Customer ID:	
	Partner Website:	
Symantec.		
	Rack Next > C	ancel

2199 12. Uncheck Send anonymous data to Symantec to receive enhanced threat protection intelligence
 and click Next >.

V				
<ul> <li>Installation</li> </ul>	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>			
	After Symantec Endpoint Protection Manager is enrolled in the cloud portal, this setting is automatically turned	d on.		
Server Configuration	Learn more about data collection			
000000000	View privacy statement			
			00000	
-	Click Back to change the installation settings, or click Next to begin	the data	base c	C.
Symantec.				

2201

2202 13. After installation is completed, check Launch the Symantec Endpoint Protection Manager to
 2203 configure your hosts; click Finish.

m	Configuration completed with warnings
	Note that installing Symantec Endpoint Protection Manager does not install the Symantec Endpoint Protection client on this computer. Yo
<ul> <li>Installation</li> </ul>	should also install the Symantec Endpoint Protection client.
0000000000	You can run this wizard at a later time from the Start menu on this computer.
	Launch the Symantec Endpoint Protection Manager
<ul> <li>Server Configuration</li> </ul>	Symantec Endpoint Protection Manager cannot read the required user rights that are specified in the Windows domain security
0000000000	policies on this computer. The management console cannot run if user rights are not assigned to Symantec Endpoint Protection Manager services.
	Add the required accounts and update the domain policies on this machine. For user rights requirements and more information, see the following knowledge base article:
	How to Configure Windows Security Policies for
	Symantec Endpoint Protection Manager
-	
Symantec.	

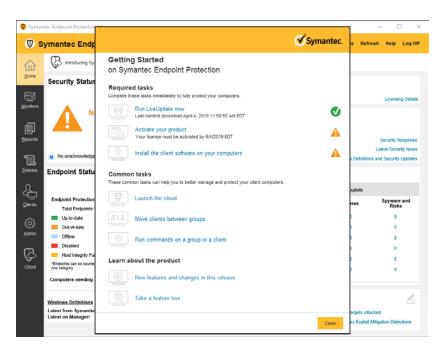
2207

2205 Symantec Endpoint Protection Host Windows Installation

1. Launch the **Symantec Endpoint Protection Manager** and log in as the **admin**.

	Symantec Endpoint Protec	tion Mana	ger
User name:	admin		
Password:	•••••		
Server:	symantec-management:	3443	`
	Forgot your password?		
	Log On	Exit Opt	ions >>

2208 2. Select **Install the client software on your computers** from the **Getting Started** screen.



2211

2210 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 exit	sting client communication settings.
Note: For instructions to install the client on a computer that runs Symantec Mail Security of knowledge base article:	or Symantec Scan Engine, see the Symantec Technical Support
Click here	
New Package Deployment	
Select packages from the server and specify client group and features.	
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 Sym restore communication between the client and Symantec Endpoint Protection M Protection Manager, or to convert an unmanaged client to a managed client.	
Create a package for Symantec Endpoint Protection clients that run on Wir	ndows. 輝
Create a package for Symantec Endpoint Protection clients that run on Ma	c. 🗰

4. Confirm the settings Install Packages: Windows - Symantec Endpoint Protection version

2213 14.2.1023.0100 - English, Group: My Company, Install Feature Sets: Full Protection for Clients,

2214 Install Settings: **Default Standard client installation settings for Windows**. Click **Next >**.

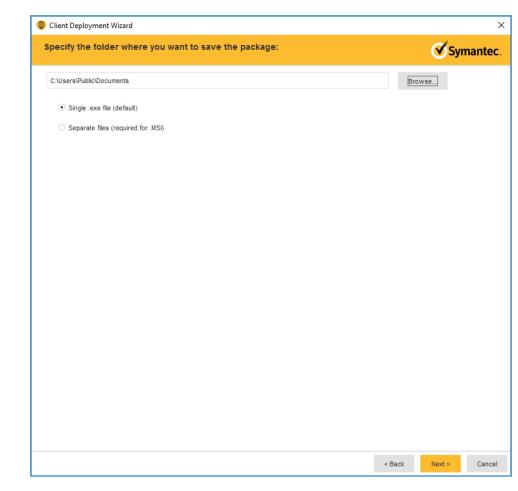
Select Group a	nd Install Feature Sets	Syman
Install Packages:	Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English	r
	This selection includes: WIN64BIT: Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English (4/4/19) WIN32BIT: Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English (4/4/19)	
Group:	My Company	Brow
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.	P
Install Settings:	Default Standard client installation settings for Windows	Option
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 defin	

#### 2215

2216 5. Confirm that Save Package is selected and click Next >.

Install Computer Endnai	A Protection to Remote Commuters	
Choose your preferred installation	nt Protection to Remote Computers method.	Symant 🗹
<ul> <li>Save Package</li> </ul>		
Creates an executable in	stallation package, but does not distribute protection software to remote o	computers.
O Remote Push		
Creates a client installati Preparing for Remote	on package and pushes the package onto client computers. The package e Push Installation	installs automatically on the computers.
O Web Link and Email		
Creates a client installati	on package and an email template so you can send an email notification w	vith download instructions to users.
	Is the latest installation package that you specified. If you re-run the wiza s to the latest selection only. You cannot assign more than one installation	
		< Back Next > Can

2218 6. Specify the location to save the installation files and click **Next** >.



2220 7. Confirm details of custom installation files and click Next >.

		-
Ready to save package		Symante
New computers will join the group "My Company", and will have the following client features ins	stalled:	
Core Files		
<ul> <li>Virus And Spyware Protection</li> </ul>		
Download Protection     Microsoft Outlook Scanner		
Lotus Notes Scanner		
POP3/SMTP Scanner		
Proactive Threat Protection		
SONAR Protection		
Application and Device Control     Network and Host Exploit Mitigation		
Intrusion Prevention		
Firewall		
Application Hardening		
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 on which you want to install SymantecEndpoint Protection.
- 9. Launch the executable file and follow the prompts to install Symantec Endpoint Protection.

## 2225 2.9 Data Security

- 2226 No specific solution was implemented in the NCCoE lab to address data-at-rest encryption.
- 2227 The NCCoE lab used several different solutions to address data-in-transit encryption. As described in
- 2228 <u>Section 2.6.2</u>, DigiCert PKI, the lab implements SSL/TLS encryption using DigiCert-issued certificates.
- 2229 Communications between modalities and clinical systems are secured using HIP, as described in <u>Section</u>
- 2230 <u>2.7.3</u>, Tempered Networks Identity Defined Networking (IDN).

## 2231 2.10 Secure Remote Access

## 2232 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.

- 2235 System Requirements
- 2236 **CPU**: 1
- 2237 Memory: 8 GB RAM
- 2238 Storage: 40 GB
- 2239 **Operating System**: CentOS 7
- 2240 Network Adapter: VLAN 1097
- 2241 TDi ConsoleWorks Installation
- 2242 The TDi ConsoleWorks installation in this PACS environment replicates the installation in the Wireless
- 2243 Infusion Pumps project. For detailed installation guidance, please refer to the Section 2.1.8 *TDi*
- 2244 ConsoleWorks External Remote Access in NIST SP 1800-8C, Securing Wireless Infusion Pumps [19].
- 2245 TDi ConsoleWorks Radius Authentication Configuration
- In our project, we integrated TDi ConsoleWorks with the Symantec VIP, for two-factor authentication.

2247 This section explains how to enable external authentications for ConsoleWorks. In the next section we

2248 explain how we configured Symantec VIP to integrate with ConsoleWorks.

- 1. Download *extern\_auth\_radius.so* file from ConsoleWorks support site [20].
- 2250 2. Move *extern\_auth\_radius.so* file to */opt/ConsoleWorks/bin* directory.
- 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**.
- 2254 5. Click **add** to create a new external authentication source.
- 2255 6. Fill out the required fields. Below is the setup we used:
- 2256 Record Name: Radius
- 2257 Ensure Enable is checked
- 2258 For Library select radius

- 2259 Parameter 1: 192.168.120.190:1812/\*\*\*\*\*\*\*
- 2260 Parameter 2: 30
- **2261 Parameter 6**: 15
- 2262 Template User: CONSOLE\_MANAGER
- 2263 7. Continue through the prompt by clicking **Next**; click **Save** on the final prompt.

✓ Enabled         Library:       radius         Parameter 1:       192.168.120.190:1812/******         Parameter 2:       30         Parameter 3:	Record Name:	RADIUS
Parameter 1:       192.168.120.190:1812/******         Parameter 2:       30         Parameter 3:		V Enabled
Parameter 2: 30 Parameter 3: Parameter 4: Parameter 5: Parameter 6: 15 Required Profile:	Library:	radius 🔻
Parameter 3: Parameter 4: Parameter 5: Parameter 6: 15 Required Profile:	Parameter 1:	192.168.120.190:1812/*****
Parameter 4: Parameter 5: Parameter 6: 15 Required Profile:	Parameter 2:	30
Parameter 5: Parameter 6: 15 Required Profile:	Parameter 3:	
Parameter 6: 15	Parameter 4:	
Required Profile:	Parameter 5:	
	Parameter 6:	15
Template User: CONSOLE_MANA ▼	Required Profile:	
	Template User:	CONSOLE_MANA 🔻

2265 8. Ensure that **Enable External Authentication** is checked.

SECURITY: External Author	entication		⊕_□⊠
External Authentication 🗙			
Enable External Authenticatio	n		
External Authentication assun	ned for pre-existing User ac	counts	
External Authentication	Library	Enabled	Param 1
RADIUS	radius	Y	192.168.120.190:1812/
Up Down		Delete	Rename Edit Save

## 2267 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, SMS, and biometric. For this project, Symantec VIP is used as a second form

- of authentication for remote access to the PACS architecture through TDi Technologies ConsoleWorks.
- 2271 System Requirements
- 2272 **CPU**: 4
- 2273 Memory: 8192MB RAM
- 2274 Storage: 240GB (thin provisioned)
- 2275 Operating System: Microsoft Windows Server 2016
- 2276 Network Adapter: VLAN 1201

#### 2277 Symantec VIP Installation

1. Right click on the *setup.exe* file for VIP Enterprise Gateway 9.8.0; select **Run as administrator**.

🖌 🖛			Application Tools	VIP_Enterprise_0	Gateway_9_8_0_WINDO	SWC	
File Home	Share	View	Manage				
	> VIP	_Enterprise_(	Gateway_9_8_0_WINI	DOWS			
		Name	^		Date modified	Туре	Size
📌 Quick access		setup			5/2/2019 4:33 PM	Ann Eastinn	140 557 1/0
📃 Desktop	*	Setup			3/2/20194:33 PIVI	Application	142,557 KB
👆 Downloads	*						
😭 Documents	*						
Pictures	*			VIP Enterpri	se Gateway - InstallSh	ield Wizard	
💻 This PC				S w	P Enterprise Gateway Se izard, which will guide yo ease wait.		
💣 Network							
				Extracong	VIP Enterprise Gateway	r.msi	
							Cancel

- 2279
- 2280 2. Proceed through the install wizard by clicking Next >.



2284

2282 3. Check I accept the agreement.

#### 2283 4. Click **Next >**.

License Agreement Please read the following License Agreement carefully. You must accept the Viliation & UD Protection terms of this agreement before continuing the installation.					
SYMANTEC SOFTV	WARE LICENSE AG	REEMENT	^		
SYMANTEC CORPORATION AND/OR LICENSE THE LICENSED SOFTWARE TO THE LEGAL ENTITY THAT WILL BE UTIT BELOW AS "YOU" OR "YOUR") ONLY THE TERMS OF THIS LICENSE AGREEM AND CONDITIONS OF THIS LICENSE LICENSED SOFTWARE. THIS IS A LEGA AND SYMANTEC. BY CLICKING THE	O YOU AS THE IN UIZING THE LICEN ON THE CONDITI ENT ("LICENSE AG AGREEMENT CA LI AND ENFORCEA	DIVIDUAL, THE CO ISED SOFTWARE ( ON THAT YOU AC REEMENT"). REAL REFULLY BEFORE ABLE CONTRACT BI	OMPANY, OR REFERENCED CCEPT ALL OF D THE TERMS USING THE ETWEEN YOU		
<ul> <li>I accept the agreement.</li> <li>I do not accept the agreement.</li> </ul>					

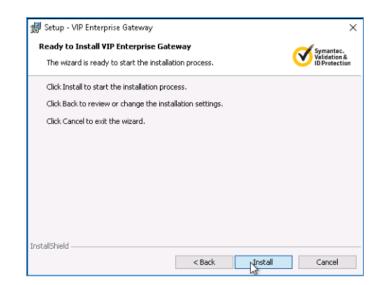
5. Create a username as admin and password and click Next >.

Configuration	Console Access		Symantec. Validation & ID Protection
	of the user who will m user will use to log into ive.		
Username (mini	mum 5 characters)		
Username (mini admin	mum 5 characters)		
admin	mum 5 characters) mum 8 characters)		
admin			
admin Password (mini	mum 8 characters)		
admin Password (mini	mum 8 characters)	 	

2287 6. Keep the default installation location by clicking **Next** >.

	i <b>on Folder</b> to install to this folder or click Cl	hange to install to	a different folder.	Vali ID P
Þ	Install VIP Enterprise Gatewa C:\Program Files (x86)\Syma		e_Gateway\	Char
InstallShield -				
		< Back	Next >	Ca

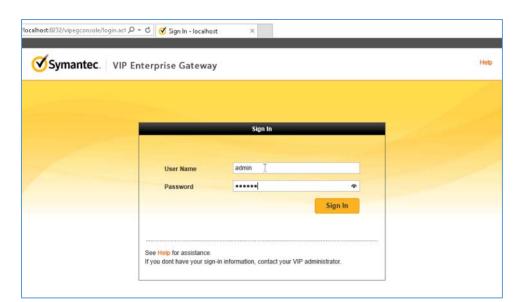
2289 7. Click Install.



2291 8. Click **Finish** after installer is complete.

👷 Setup - VIP Enterprise Gate	way ×
Symantec.	VIP Enterprise Gateway successfully installed. This wizard has successfully installed VIP Enterprise Gateway on your computer Click Finish to exit the setup. ☑ Launch the Configuration Console
	< Back Finish Cancel

- 2293 9. On the Symantec VIP local machine, open a web browser and navigate to *http://localhost:8232*.
- 2294 Sign in with the **User Name** as **admin** and corresponding **Password** specified during installation.



#### 10. Select **User Store** from the menu bar.

Home User Store						
	Validation	Identity Providers	Logs	Settings	Help	
User Store > User Store						
Links	Add User Sto	ore				
User Store	> You must configur	e a connection with each	new user store th	nat you add to VIP E	Enterprise Gateway.	
LDAP Directory Synchronization			Us	ser Store		
VIP Administrator Configuration			2			
Console Authentication	Type:		LDAP			
	*Name:					?
			Server	r Information		
	*Connection:					?
	*Host					0
	*Port		2	Y		
	Timeout			onds		
	Enable SSL:			on ao		
			Bind	Information		
	*User DN:		12			0
	*Password:					(?)
	10000000000					
			Sear	ch Criteria		

## 2297

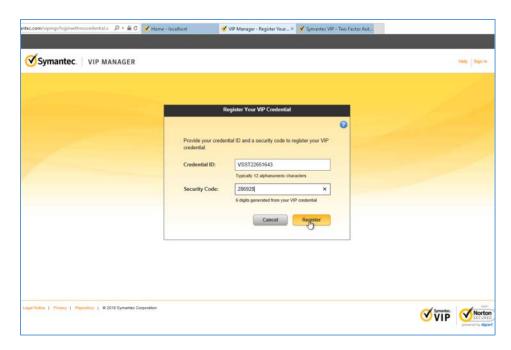
## 2298 11. Add a user store with the following information:

- 2299 Name: AD PACS
- 2300 Connection: ad-main
- 2301 Host: ad.pacs.hclab
- 2302 Port: 389

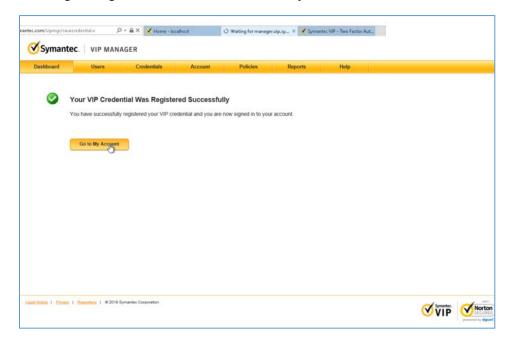
- 2303 User DN: CN=symantec, DC=pacs, DC=hclab
- 2304 Password: \*\*\*\*\*\*\*\*
- 2305 Base DN: DC=pacs, DC=hclab
  - User Filter: (&(&objectClass=user)(objectCategory=person))(sAMAcountName=%s))

nsole Authentication	rype.	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:	•••••	0
		Search Criteria	
	Base DN:	DC=pacs,dc=hclab	?
	Base DN: *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		
	rangement intertimeter	Cancel	

- Log into VIP Manager by navigating to *https://manager.vip.symantec.com/vipmgr*. Use the account
   provided by Symantec.
- 2310 13. Select Register Your VIP Credential. Provide the Credential ID and Security Code of your
- 2311 credentials. Credentials can be downloaded by navigating to <u>https://vip.symantec.com/</u>.



2313 14. After registering the credential, select **Go to My Account**.



## 2314

2315 15. Select Account from menu bar, then select Manage VIP Credentials.

Dashboard	Users	Credentia	als Acco	unt P	Policies	Reports	Help	
hboard > Account								
								Links
Account Summary	- UNVERIFIE	D - NCCol	E					VIP Account Management
Click one of the following	tabs to view additio	nal detaits						and the second se
	In the second	0200000						View Account Details
Account Information	Single Sign-on	Features	Dynamic Provisioning	Registration File				Manage User Groups
			Organiz	ation Information				S Create Administrator Group
Organization Name			Organizational Unit			ization Address		
UNVERIFIED - NCCoE					Rocky	Great Seneca Hwy llie		Find / Modify Administrator Groups
					MD 20850			Create VIP Administrators
						States		Find / Modify VIP Administrat
	Contact Information							Manage VIP Certificates
Corporate Contact Sue Wang				chnical Contact Billing Contact e Wang Sue Wang			SMS Credential Settings	
NA			NA		NA			Credential Security Settings
swang@mitre.org 301975-0288 (preferred			swang@mitre.org 301975-0288 (preferred	÷		@mitre.org 5-0288 (preferred)		
								Download Files
			Acco	ant Information				
Jurisdiction Hash	14004610	4						
Account Creation Date	* 2019-May	-03						
Service Start Date*	2019-May	-03						
Service End Date*	2019-Jul-0	12						
Member Type	Trial							
Account Usage	Test							
Sales Reference Numb	ier							
Reflects either PST or PDT, as	applicable.			Back				

## 2317 16. Select **Request a Certificate**.

Manage VIP Certifie Use this page to request a Click Request a Certificati						Links
Use this page to request a						Links
Use this page to request a						
Click Request a Certificate		ur existing certificates.				VIP Account Management
	to request a new certificati	e and to download it.				S View Account Details
						Manage User Groups
		Cen	tificates			Create Administrator Group
	Certificate Name A		Expiration* societed with your VIP account	State	Action	Find / Modify Administrator Groups
			9			Manage VIP Certificates     Mis Credential Settings     Credential Security Settings     Download Files

#### 2318

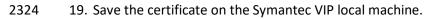
2319 17. Provide a **Certificate Name** as **NCCoE\_VIP\_Cert**; click **Submit Request**.

Internet + Account	Users	Credentials	Account	Policies	Reports	Help	
TOTAL P ACCOUNT							Links
Request a Cer	tificate						▼ VIP Account Management
Enter an easily-reco	gnizable name for your	certificate (such as "VIP Certi	ficate 1") in th	he field below.			> View Account Details
If you have your own	n private key, enter a Ce	ertificate Signing Request (CS	R) that you've	e generated by clicking here	Symantec supports 2048	bit keys in the CSR.	Manage User Groups
* Required Informati	on						
			Certifica	ate Name			<ul> <li>Create Administrator Group</li> <li>Find / Modify Administrator</li> </ul>
*Certificate Name	NCCoE VIP Cer	t		× (?)			Find / Modify Administrator Groups
	[noose_m_os						Create VIP Administrators
							Find / Modify VIP Administrate
						e certificate or notify Symantec to do	Manage VIP Certificates
						your certificate at any time without ymantec determines are harmful to its	SMS Credential Settings
systema.							Credential Security Settings
			lack St	ub wit Request			Download Files
			interest when	La la			

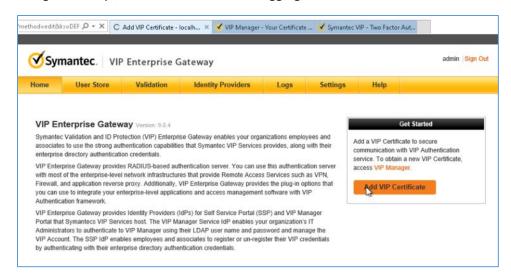
2321 18. Select PKCS#12 format and create a password for the requested certificate. Then select Download
 2322 Certificate.

Dashboard	Users	Credentials	Account	Policies	Reports	Help	
Your certificate nar	the Request has be need NCCOE_VIP_Cert e cate format, enter a pass ormation O PEM ® PK	copires on 2021-May-06 word to encrypt the cert ccsa12 (2) (2) Must be at	tificate, and then click D t least eight characters ar one lowercase letter, plu	nd include one			Links VIP Account Management VIW Account Details View Account Details Manage User Groups Create Administrator Group Create Administrator Groups Create VIP Administrators Find / Modify VIP Administrators Manage VIP Certificates
Go to the Help	ting your certificate, you and Support page for P and Support page for P	KCS#12 format if you ne			Web services. IA 500 series VPN router		SMS Credential Settings     SMS Credential Settings     Credential Security Settings     Download Files
			Return Ho	me			

## 2323



2325 20. Navigate to *http://localhoat:8232*. After logging, select **Add VIP Certificate**.



2326

2327 21. Select **Browse** and upload the certificate from the previous step. Enter the correct password and2328 alias for the certificate, then click **Submit**.

		Enterprise (	sateway				admin   Sign (
Home	User Store	Validation	Identity Providers	Logs	Settings	Help	
ettings > VIP	Certificate						
	Links	Add VIP C	Certificate				
VIP Certifi		Complete the	following steps to import a V	IP Certificate in .p12	2 format. If you do n	ot have a VIP certifica	te, click VIP Manager
SSL Certifi		to obtain a ne					
	Certificate						
Export Sett		Failed to	import PKCS12 cert. Make s	ure PKCS12 File an	d Password are cor	rect.	
Import Sett	inas						
State 197							
Console Se	ettings	_		Add VIP	Certificate		
Console Se HTTP Prox	ettings	*File Name	ĸ		Certificate	_cer Browse	
Console Se HTTP Prox	ettings y Settings eck Settings	*File Name *Password				_cer Browse	

- 2330 22. Select Validation from the menu bar, select Custom configuration, and provide the information thatfollows:
- 2332 Server Name: vip
- **Local IP**: 192.168.120.190

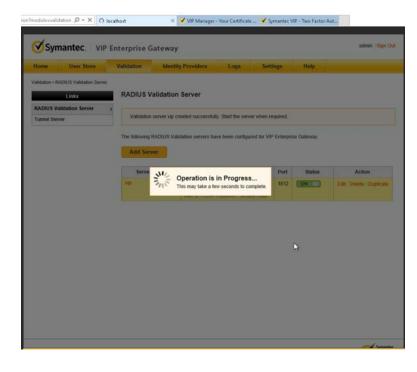
- 2334Port: 18122335RADIUS Shared Secret: \*\*\*\*\*2336Confirm RADIUS Shared Secret: \*\*\*\*\*2337Enable First Factor: Checked2338Authentication on: Enterprise
- 2339 Authentication Sequence: LDAP Password VIP Authentication
- 2340 User Store: AD PACS

lome User Store	Validation Identity Providers	Logs Settings Help	
iidation > RADIUS Validation Serve Links RADIUS Validation Server	Add RADIUS Validation Serve		
unnel Server			
	* Server Name: * Local IP : * Port : * RADIUS Shared Secret: * Confirm RADIUS Shared Secret: Logging Level: Log Rotation Interval: Number of Files to Keep: Enable Systog : * Password Encoding:	Ib2.168.120.190       Ib12       Ib12<	9 9 9 9
		RADIUS Access Challenge	
	*Challenge Timeout	Enable Access Challenge	
		VIP Push Authentication	
	Remote Access Service Name/URL:	Enable Push     ⑦      Remote Access Service Name	0

2342 23. Click **Submit**.

VIP Authentication Timeout	60 (7)
*Enforce Local Authentication	○ Yes ● No ⑦
	First-Factor Authentication
	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      Automatic      Enabled
	Delegation
	Enable Delegation     ?
	LDAP to RADIUS Mapping
	Enable LDAP to RADIUS Mapping
*Required Information	
	Cancel Shomit

#### 2344 24. Ensure VIP Server Status is set to **ON**.



# Appendix A List of Acronyms

AD	Active Directory
AES	Advanced Encryption Standard
AE Title	Application Entity Title
СА	Certificate Authority
CID	Cryptographic ID
CSR	Certificate Signing Request
CPU	Central Processing Unit
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 Service
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
нттр	l kur enter til Tur vefen Duete er l
	Hypertext Transfer Protocol

ICMP	Internet Control Message Protocol
IDN	Identity Defined Networking
IHE	Integrating Health Enterprise
IIS	Internet Information Services
ют	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
ISO	International Standards Organization
ІТ	Information Technology
JDK	Java Development Kit
LDAP	Lightweight Directory Access Protocol
MB	megabyte
MPPS	Modality Performed Procedure Step
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIC	Network Interface Controller
NIST	Nation Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
OVA	Open Virtual Appliance or Application
OVF	Open Virtualization Format
PACS	Picture Archiving and Communication System
РКІ	Public Key Infrastructure
QR Code	Quick Response Code
RAM	Random Access Memory
RIS	Radiology Information System

SCP	Service Class Provider
SCU	Service Class User
SEP	Symantec Endpoint Protection
SEPM	Symantec Endpoint Protection Manager
SNMP	Simple Network Management Protocol
SP	Special Publication
SQL	Structured Query Language
SSL/TLS	Secure Socket Layer/Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol
UDM	Universal Data Manager
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNA	Vendor Neutral Archive
WAN	Wide Area Network

# Appendix B References

- [1] ORACLE. Java SE 6 Downloads. [Website]. Available: <u>https://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-</u> <u>419409.html</u>
- [2] Red Hat. JBoss Application Server Downloads. [Website]. Available: https://jbossas.jboss.org/downloads.
- [3] dcm4che.org Wiki. PostgreSQL Installation. [Website]. Available: https://dcm4che.atlassian.net/wiki/spaces/ee2/pages/2556071/PostgreSQL.
- [4] EDB POSTGRES. PostgreSQL Database Download. [Website]. Available: https://www.enterprisedb.com/downloads/postgres-postgresql-downloads.
- [5] Dcm4che.org Wiki. Installation. [Website]. Available: <u>https://dcm4che.atlassian.net/wiki/spaces/ee2/pages/2555918/Installation.</u>
- [6] SourceForge. dcm4che, a DICOM Implementation in JAVA. [Website]. Available: <u>https://sourceforge.net/projects/dcm4che/files/dcm4chee/.</u>
- [7] SourceForge. dcm4che, a DICOM Implementation in JAVA. [Website]. Available: <u>https://sourceforge.net/projects/dcm4che/files/dcm4chee-arr/3.0.11.</u>
- [8] SourceForge. dcm4che, a DICOM Implementation in JAVA. [Website]. Available: https://sourceforge.net/projects/dcm4che/files/Oviyam/.
- [9] Microsoft Docs. Install SQL Server from the Installation Wizard (Setup). [Website]. 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>
- [10] T. Polk et al., 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 1, NIST, Gaithersburg, Md., Apr. 2014. Available: <u>https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf.</u>
- [11] DVTk. DVTk open source project main contributors ICT Group and Philips. [Website]. Available: <u>https://www.dvtk.org/.</u>
- [12] Microsoft TechNet. *Building Your First Domain Controller on 2012 R2*. [Website]. Available: https://social.technet.microsoft.com/wiki/contents/articles/22622.building-your-first-domaincontroller-on-2012-r2.aspx.
- [13] Microsoft TechNet. Installing and Configuring DHCP role on Windows Server 2012. [Website]. Available: <u>https://blogs.technet.microsoft.com/teamdhcp/2012/08/31/installing-and-</u> configuring-dhcp-role-on-windows-server-2012/.

- [14] *DigiCert.* CSR Creation Instructions for Microsoft Servers. [Website]. Available: <u>https://www.digicert.com/util/csr-creation-microsoft-servers-using-digicert-utility.htm.</u>
- [15] Cisco. Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide. [Website]. Available: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/quick\_start/vmware/fmcv/FMCv-quick.html.</u>
- [16] Cisco. Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide. [Website]. Available: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/quick\_start/vmware/ftdv/ftdv-vmware-gsg.html.</u>
- [17] Cisco Systems, Inc. *Basic Policy Creation for Firepower*. Jan. 30, 2019 [Online]. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/Basic Policy Creation on Cisco Firepower Devices.pdf.
- [18] Cisco Systems, Inc. Cisco Stealthwatch Installation and Configuration Guide 7.0. 2019 [Online]. Available: <u>https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system\_installation\_configuration/SW 7\_0\_0\_Installation\_and\_Configuration\_Guide\_DV\_3\_1.pdf.</u>
- [19] G. O'Brien et al., Securing Wireless Infusion Pumps in Healthcare Delivery Organizations, NIST SP 1800-8, NIST, Gaithersburg, Md., Aug. 2018. Available: <u>https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf.</u>
- [20] *External Authentication libraries*, ConsoleWorks Cybersecurity Operations Platform [Website]. Available: <u>https://support.tditechnologies.com/content/external-authentication-libraries</u>.