

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
<https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs>



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: hit_nccoe@nist.gov.

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 hit_nccoe@nist.gov.

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
13 established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,
14 Maryland.

15 To learn more about the NCCoE, visit <https://www.nccoe.nist.gov/>. To learn more about NIST, visit
16 <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
20 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
22 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
 38 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**

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

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

Name	Organization
Andy Gray	Forescout
Katherine Gronberg	Forescout
William Canter	Hyland
Kevin Dietz	Hyland
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
53 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
Cisco	Cisco Firepower Version 6.3.0 Cisco Stealthwatch Version 7.0.0
Clearwater Compliance	Clearwater Information Risk Management Analysis
DigiCert	DigiCert PKI Platform
Forescout	Forescout CounterACT 8
Hyland	Hyland Acuo Vendor Neutral Archive Version 6.0.4 Hyland NilRead Enterprise Version 4.3.31.98805 Hyland PACSgear Version 4.1.0.64
Philips Healthcare	Philips Enterprise Imaging Domain Controller Philips Enterprise Imaging IntelliSpace PACS Philips Enterprise Imaging Universal Data Manager
Symantec	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
Tripwire	Tripwire Enterprise Version 8.7
Virta Labs	BlueFlow Version 2.6.4
Zingbox	Zingbox IoT Guardian

56 **Contents**

57 **1 Introduction 1**

58 1.1 Practice Guide Structure 1

59 1.2 Build Overview 2

60 1.3 Typographic Conventions 3

61 1.4 Logical Architecture Summary 4

62 **2 Product Installation Guides 4**

63 2.1 Picture Archiving and Communication System (PACS) 5

64 2.1.1 Philips IntelliSpace PACS 5

65 2.1.2 DCM4CHEE 20

66 2.2 VNA 29

67 2.2.1 Hyland Database Server 30

68 2.2.2 Hyland Acuo VNA 31

69 2.2.3 PACSgear Core Server 33

70 2.2.4 Hyland NilRead 42

71 2.3 Secure DICOM Communication Between PACS and VNA 46

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 60

76 2.4 Modalities 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 Enterprise Domain Identity Management 100

83 2.6.1 Domain Controller with AD, DNS, & DHCP 100

84 2.6.2 DigiCert PKI 120

85	2.7	Network 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	Endpoint 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 Security	217
96	2.10	Secure Remote Access.....	218
97	2.10.1	TDi Technologies ConsoleWorks.....	218
98	2.10.2	Symantec Validation and ID Protection (VIP).....	220
99		Appendix A List of Acronyms.....	232
100		Appendix B References	235
101		List of Figures	
102		Figure 1-1 PACS Final Architecture.....	4
103		Figure 2-1 Hyland Systems and Applications Connectivity	30
104		Figure 2-2 Architecture of Networks IDN.....	166
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
111 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
118 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,
131 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
149 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.

154 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a
155 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 hit_nccoe@nist.gov.

158 Acronyms used in figures can be found in [Appendix A](#).

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**

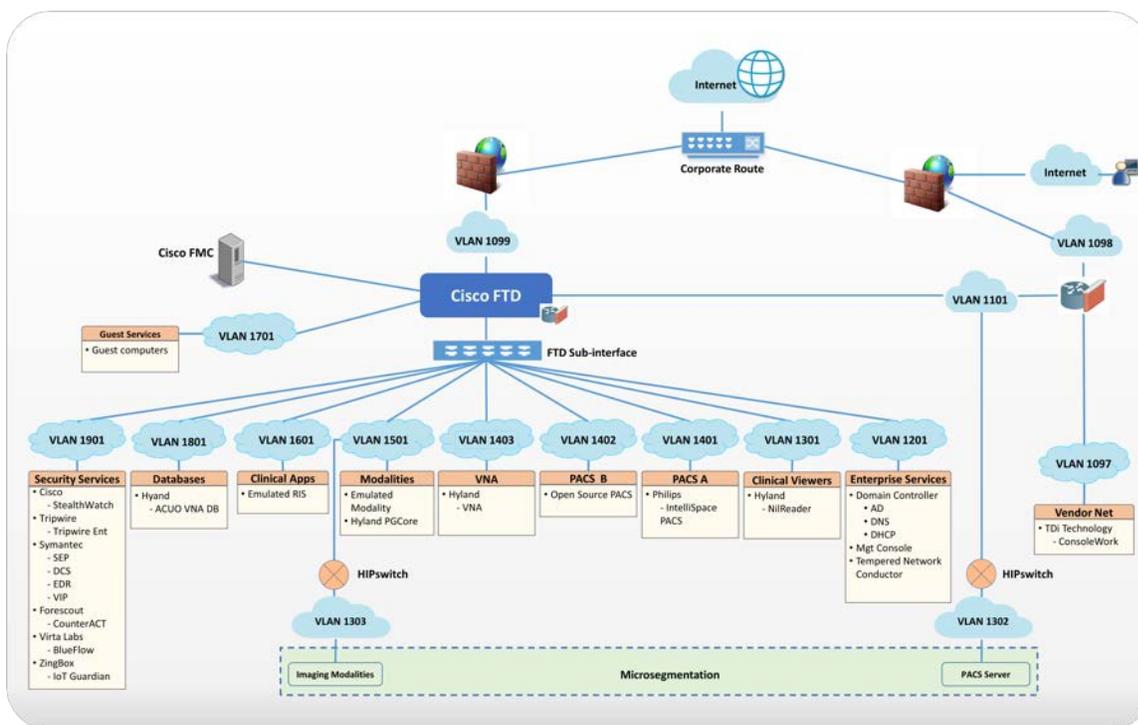
169 The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	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	<code>mkdir</code>
Monospace Bold	command-line user input contrasted with computer output	<code>service sshd start</code>
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov .

170 1.4 Logical Architecture Summary

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

186 products that align with capabilities were implemented for the environment. Products that align with
 187 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
 197 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
 199 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.

204 **Table 2-1 Base VM Configuration Requirements**

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

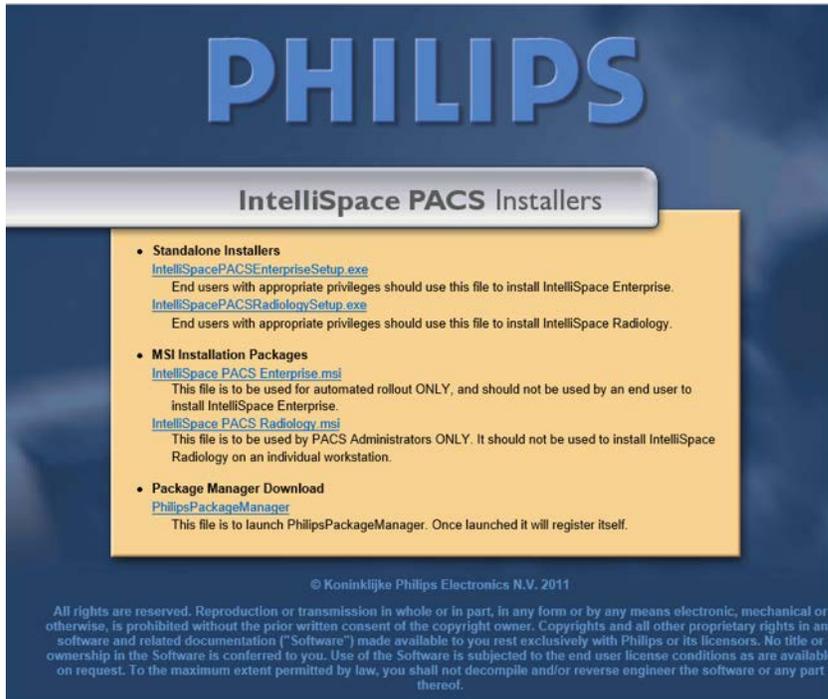
VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
	(DB), Anywhere Viewer (web client)					
UDM	Universal Data Manager (UDM), WEB DICOM services Image Lifecycle Management Image pre fetching from VNA	4	8 GB RAM	200 GB	Microsoft Windows Server 2012	Microsoft SQL 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
 212 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:

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



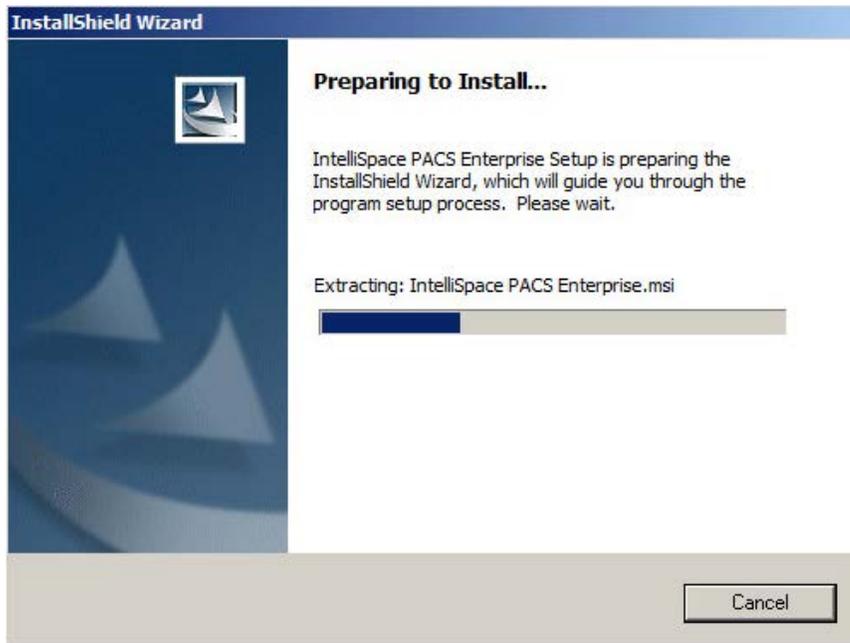
220

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



223

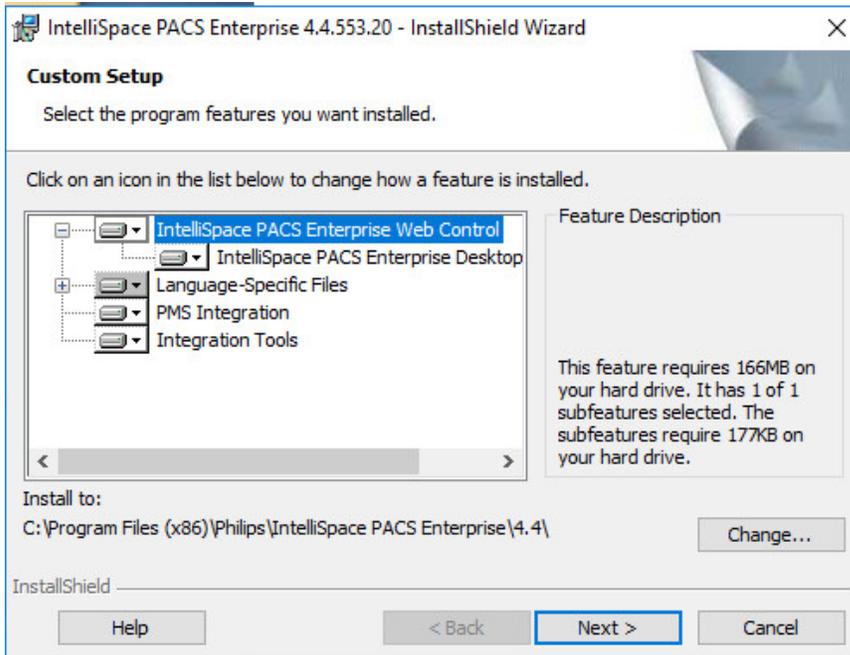
224 4. After the setup language has been set, the **InstallShield Wizard** begins the installation process.



225

226
227

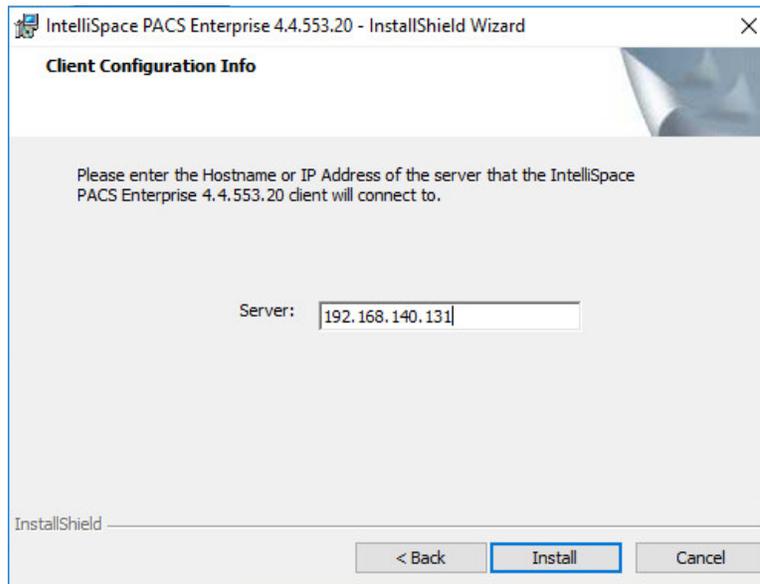
5. Use the default setting for the **Custom Setup** and click on the **Next >** button that appears at the bottom of this window.



228

229
230

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

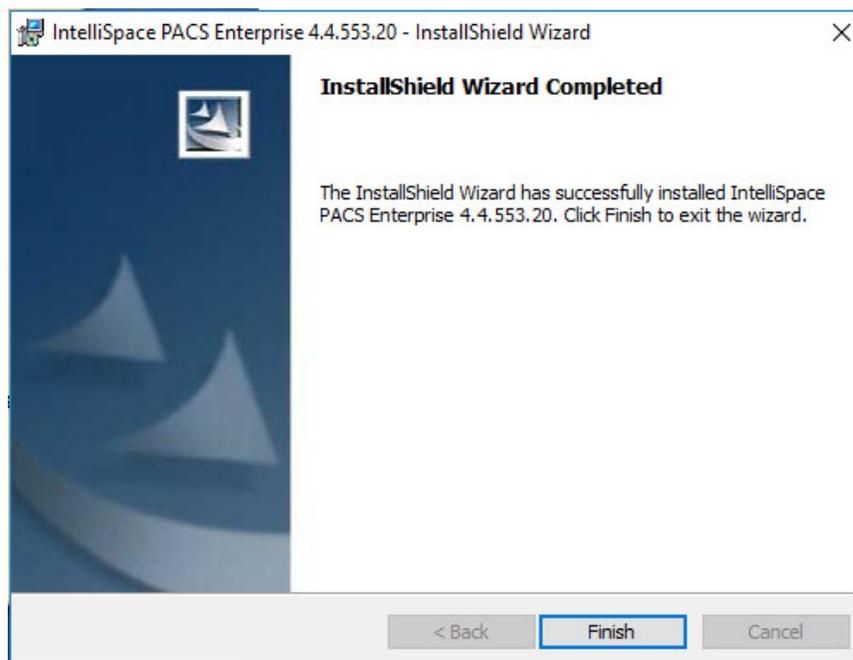


231

232

233

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



234

235

236

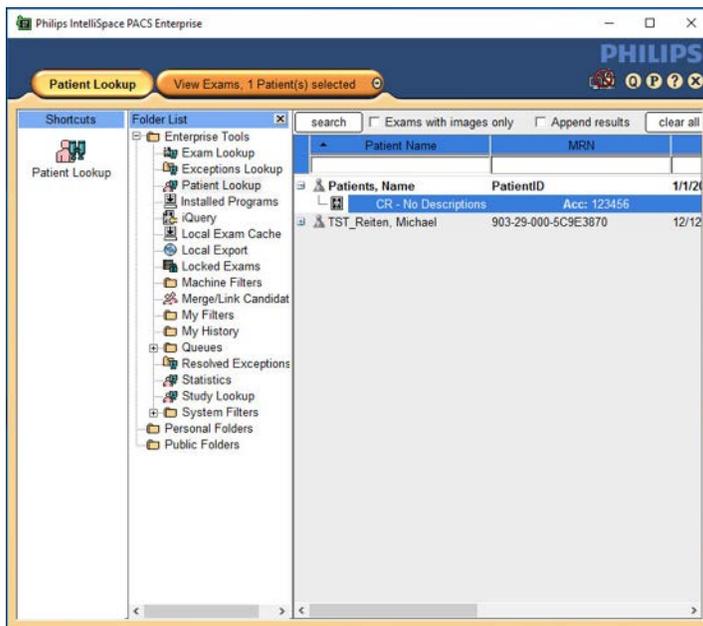
237

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



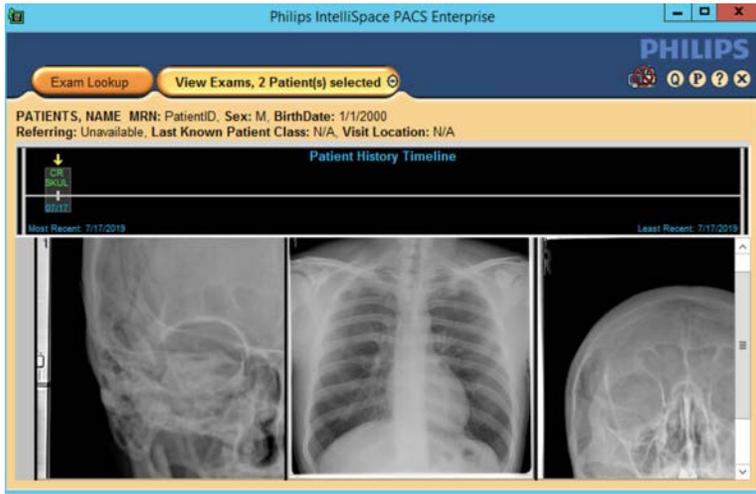
238

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



240

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

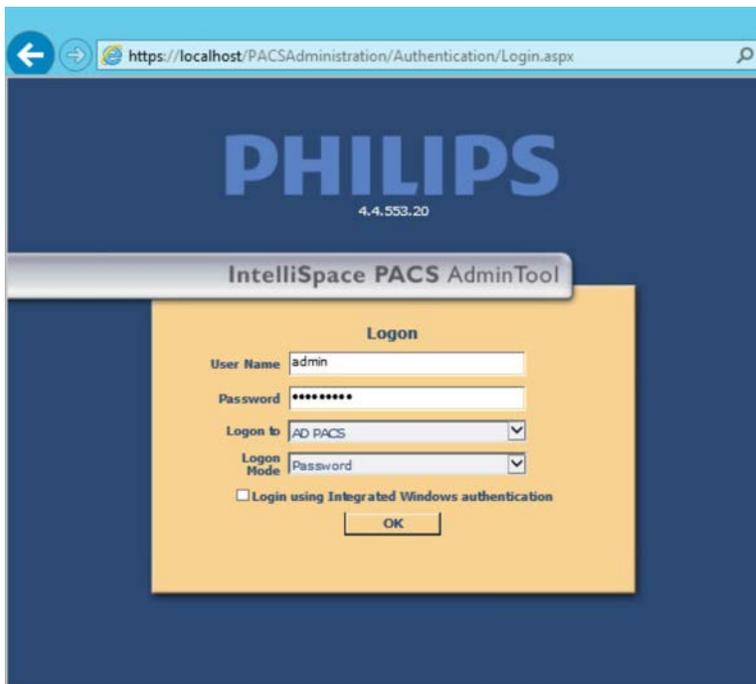


243

244 IntelliSpace PACS Client Configuration

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

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



250

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

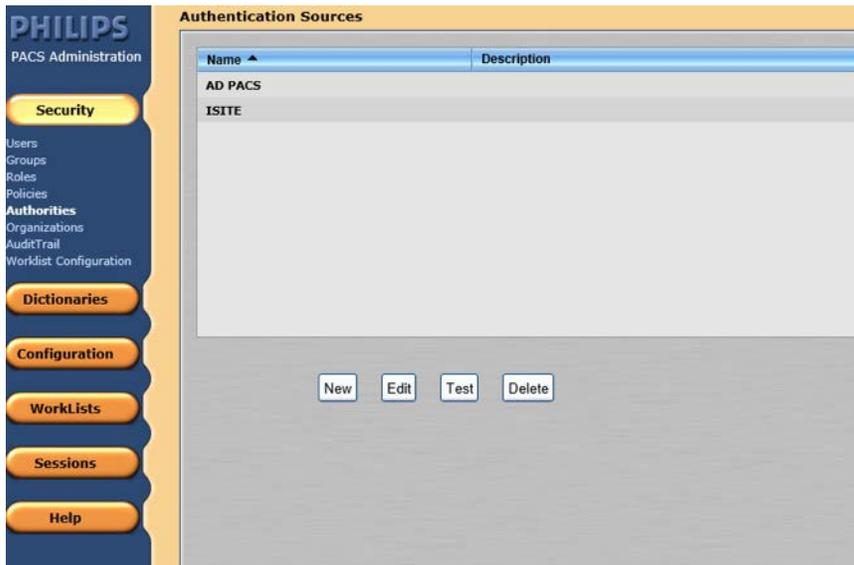


- 253
- 254 3. To add a new user, navigate to **SECURITY**, found on the far-left column of the Common Tasks
 255 screen, and click on **Users**.
- 256 a. Enter the **User ID**.
- 257 b. Enter the user's **First Name**.
- 258 c. Enter the user's **Middle Name** (optional).
- 259 d. Enter the user's **Last Name**.
- 260 e. Enter the user's **Email Address** (optional).
- 261 f. Assign an IntelliSpace PACS AdminTool **Password** for the user (required). Enter the password
 262 again to confirm it.

263 Configure Sources for User Authentication

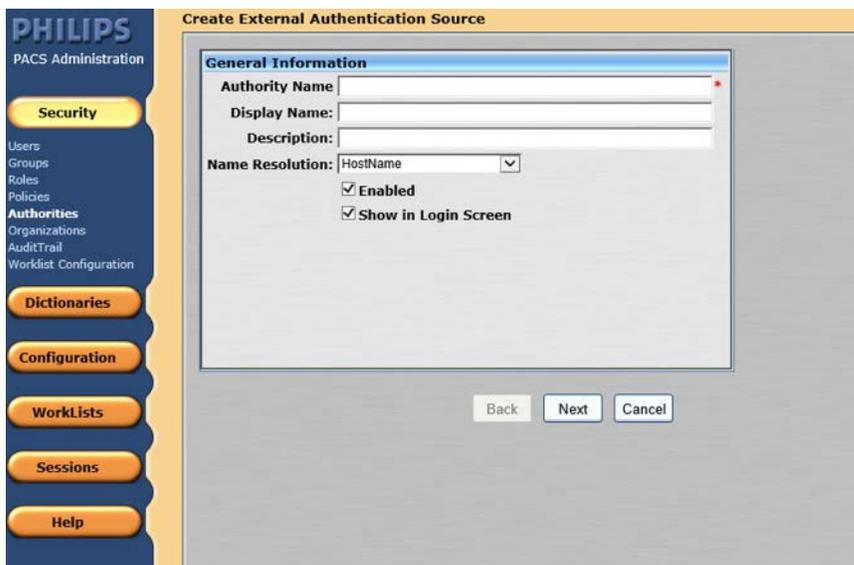
264 IntelliSpace supports either a locally hosted or an external authentication source. An authentication
 265 source provides a directory structure that authenticates and manages user and group accounts. The
 266 internal authentication source, called iSite, implements a local database of users and groups.
 267 IntelliSpace also supports a lightweight directory access protocol (LDAP) server connected to a Microsoft
 268 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**.



271

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



273

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**



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

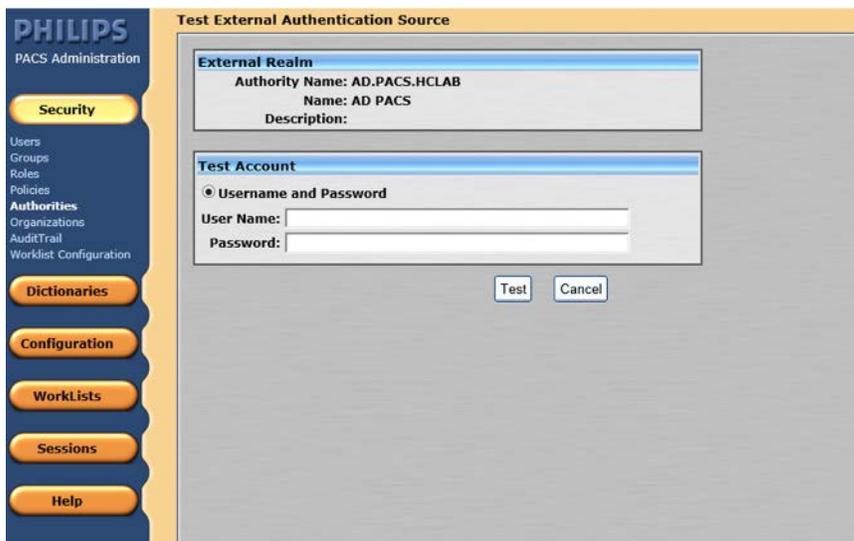


- 282
- 283 5. Navigate to the **Edit External Authentication Source** screen. In this project, the **Directory Type** is
- 284 **ActiveDirectory** and the **Supported Credentials** is **Password**. Click **Save** to save the settings.



285

- 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**.



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 [Section 2.4.1](#). Below are the configuration steps:

- 294 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
 296 communication **Listening Port**, e.g., **104** for the emulator itself.

- 297
 298 2. From the DVTk Modality application, click the **Remote Systems** tab to configure the remote
 299 systems, including **RIS System**, **MPPS Manager**, and **PACS/Workstation Systems**. Information for
 300 each system's IP address as well as the port number are needed. Particularly, the **AE Title** for the
 301 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

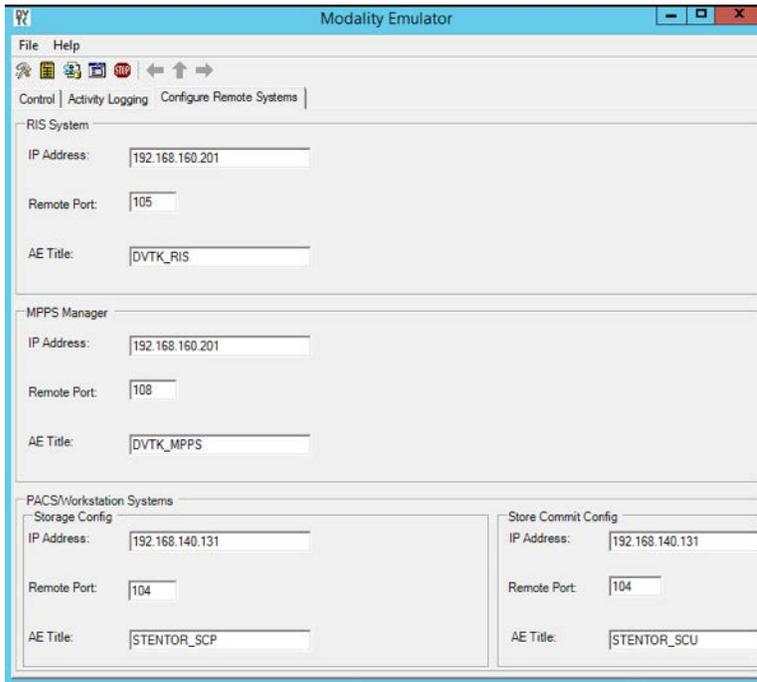
310 **PACS/Workstation Systems–Storage Config**

- 311 ■ **IP Address:** *192.168.140.131*

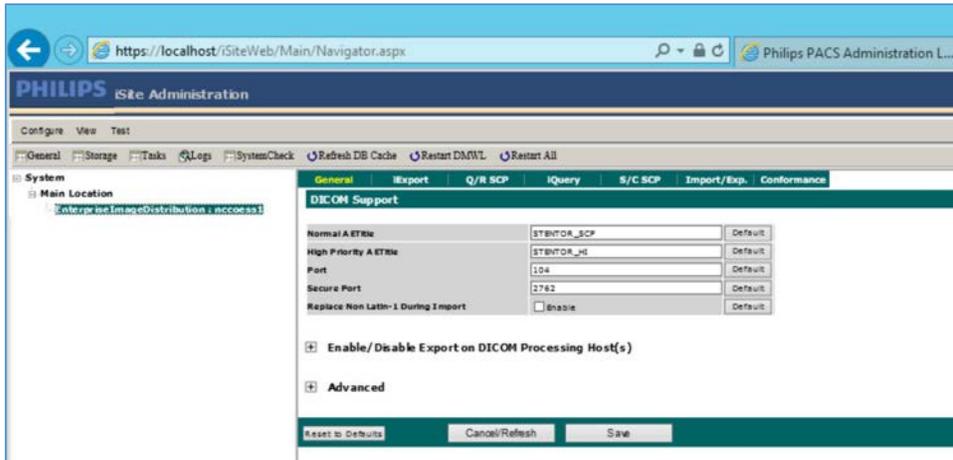
- 312 ▪ **Remote Port:** 104
- 313 ▪ **AE Title:** STENTOR_SCP

314 **PACS/Workstation Systems–Storage Commit Config**

- 315 ▪ **IP Address:** 192.168.140.131
- 316 ▪ **Remote Port:** 104
- 317 ▪ **AE Title:** STENTOR_SCU

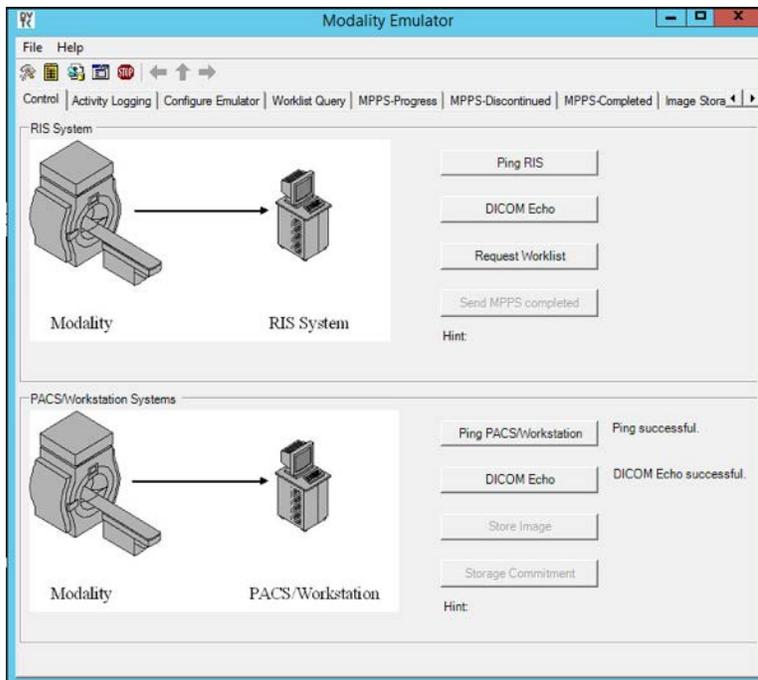


- 318
- 319 3. To configure the Philips IntelliSpace PACS AE Title and communication port, log on to the iSite
- 320 Administration web site using the URL *https://192.168.140.131/iSiteWeb*. Select **Configure >**
- 321 **DICOM > General**, set the following values, and then click **Save** to save the settings.
- 322 ▪ **Normal AE Title:** STENTOR_SCP
 - 323 ▪ **High-Priority AE Title:** STENTOR_HI
 - 324 ▪ **Port:** 104
 - 325 ▪ **Secure Port:** 2762



326

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



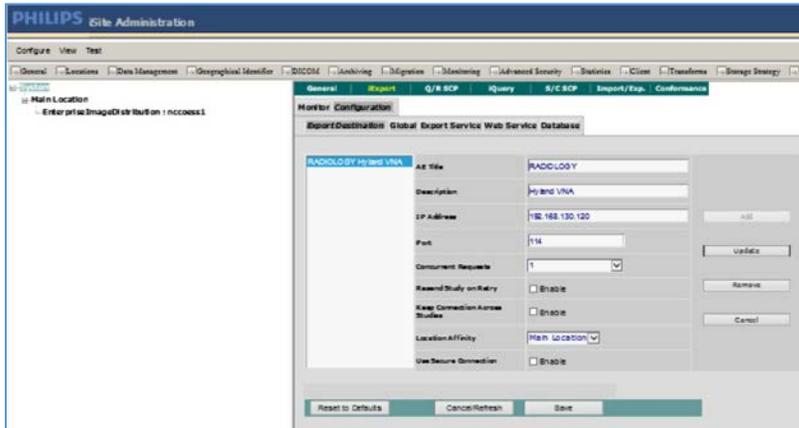
330

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

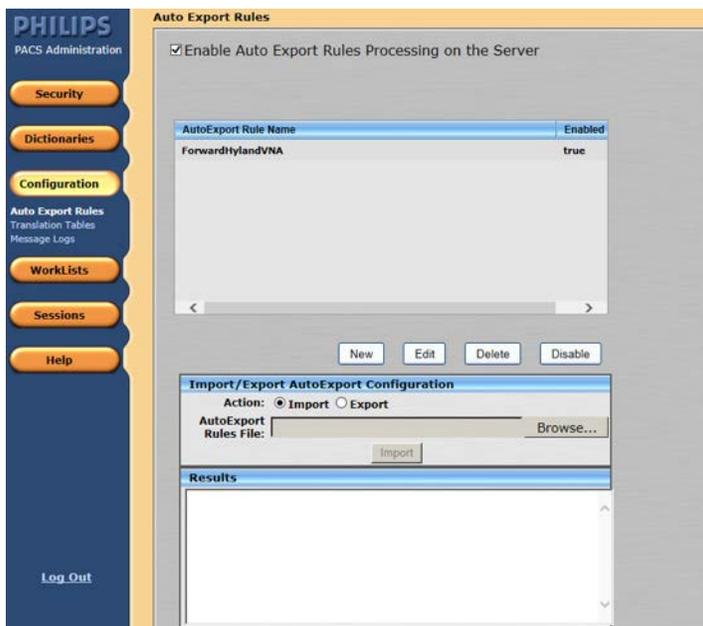
332 Refer to [Section 2.2.2](#) for detailed installation guidance for Hyland VNA.

- 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>

- 335 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.



- 338
- 339 4. Log in to the IntelliSpace PACS Administration page using
- 340 <https://192.168.140.131/PACSAdministration>.
- 341 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.

PHILIPS
PACS Administration

Security
Dictionaries
Configuration
Auto Export Rules
Translation Tables
Message Logs
WorkLists
Sessions
Help

Log Out

Edit AutoExport Rule

AutoExportRule Configuration

Rule Name: ForwardHylandVNA
Trigger Type: New Data Arrival
Enable Priors:
Prior Criteria: Modality BodyPart
No. Of Priors: 3

Matching Criteria

Modality type
Manufacturer Name
Sending AE title
Receiving AE title: STENTOR_SCP
Study description
Manufacturer model
Referring physician's first name
Referring physician's last name
Reading physician's first name
Reading physician's last name
Requested Procedure Description
Study Date and Time
Body Part
Protocol Name
Series Description

Configured Export Destinations | **Selected Destinations**

Hyland VNA (RADIOLOGY)

>>
<<

Save Cancel

347

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
354 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.

356 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].

- 367 1. Go to <https://www.dcm4che.org> to download the software.
- 368 2. In the left-hand side of the page, click the **Wiki** link under Community.
- 369 3. Click the **here** link under **Download Latest Version** nest to **dcm4chee DICOM Archive 2 (includes**
370 **dcm4che toolkit 1.4)** [6] link on the right-hand side of the screen.
- 371 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**

- 377 1. Go to *dcm4chee-2.17.1-psql\bin* directory by using a command prompt and run this command:
378 `Run.bat`.
- 379 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$Required.invoke(TxInterceptor.java:195)
at org.jboss.aop.joinpoint.MethodInvocation.invokeNext(MethodInvocation.java:101)
at org.jboss.ejb3.stateless.StatelessInstanceInterceptor.invoke(StatelessInstanceInterceptor.java:62)
at org.jboss.aop.joinpoint.MethodInvocation.invokeNext(MethodInvocation.java:101)
at org.jboss.ejb3.mdb.MessagingContainer.localInvoke(MessagingContainer.java:249)
at org.jboss.ejb3.mdb.inflow.MessageInflowLocalProxy.delivery(MessageInflowLocalProxy.java:268)
at org.jboss.ejb3.mdb.inflow.MessageInflowLocalProxy.invoke(MessageInflowLocalProxy.java:138)
at com.sun.proxy.$Proxy326.onMessage(Unknown Source)
at org.jboss.resource.adapter.jms.inflow.JmsServerSession.onMessage(JmsServerSession.java:178)
at org.jboss.jms.client.container.ClientConsumer.callOnMessageStatic(ClientConsumer.java:160)
at org.jboss.jms.client.container.SessionAspect.handleRun(SessionAspect.java:831)
at org.jboss.aop.advice.org.jboss.jms.client.container.SessionAspect14.invoke(SessionAspect14.java)
at org.jboss.jms.client.delegate.ClientSessionDelegate$run_N8003352271541955702.invokeNext(ClientSessionDelegate
$run_N8003352271541955702.java)
at org.jboss.jms.client.container.ClosedInterceptor.invoke(ClosedInterceptor.java:170)
at org.jboss.aop.advice.PerInstanceInterceptor.invoke(PerInstanceInterceptor.java:105)
at org.jboss.jms.client.delegate.ClientSessionDelegate$run_N8003352271541955702.invokeNext(ClientSessionDelegate
$run_N8003352271541955702.java)
at org.jboss.jms.client.delegate.ClientSessionDelegate.run(ClientSessionDelegate.java)
at org.jboss.jms.client.JBossSession.run(JBossSession.java:199)
at org.jboss.resource.adapter.jms.inflow.JmsServerSession.run(JmsServerSession.java:237)
at org.jboss.resource.work.WorkWrapper.execute(WorkWrapper.java:204)
at org.jboss.util.threadpool.BasicTaskWrapper.run(BasicTaskWrapper.java:275)
at EDU.oswego.cs.dl.util.concurrent.PooledExecutor$Worker.run(PooledExecutor.java:756)
at java.lang.Thread.run(Unknown Source)
10:35:24,470 INFO [FileSystemMgt2Service] Check file system group ONLINE_STORAGE for deletion of orphaned private files
10:35:24,470 INFO [FileSystemMgt2Service] Check file system group LOSSY_STORAGE for deletion of orphaned private files
  
```

380

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
 383 following credentials:

- 384 ■ **Username:** admin
- 385 ■ **Password:** *****

386 2. Click the link **group=ONLINE_STORAGE,service=FileSystemMgt** under the dcmrchee.archive
 387 heading.

dcm4chee.archive

- [group=LOSSY_STORAGE,service=FileSystemMgt](#)
- [group=NEARLINE_STORAGE,service=FileSystemMgt](#)
- [group=ONLINE_STORAGE,service=FileSystemMgt](#)
- [name=AttributesModificationScu,service=Queue](#)

388

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
 391 *dcm4chee-2.7.1-psql\server\default\archive*.

org.dcm4chex.archive.ejb.interfaces.FileSystemDTO addRWFileSystem()

Add RW file system to the file system group managed by this service. The file system is also linked to existing other file systems of the group.

Param	ParamType	ParamValue	ParamDescription
dirPath	java.lang.String	<input type="text"/>	Directory/Mount Point
<input type="button" value="Invoke"/>			

392

393 4. Change the default AE Title:

- 394 a. The default AE Title is **DCM4CHEE**.
- 395 b. Change the title by clicking the **service=AE** link under dcm4chee.archive heading.

- [name=WadoPrefetch.service=Queue](#)
- [service=AE](#)
- [service=AttributesModificationScp](#)

- 396
- 397 5. Under the **updateAETitle** section, provide the **default AETitle** and **new AETitle** as parameters, and
- 398 click the **Invoke** button on the bottom left-hand side of the table.

void updateAETitle()

Update specified AE Title to new value in AE Configuration and in all service attrib
 AE Title of these file systems is updated to the new value as the Retrieve AE Title

Param	ParamType	ParamValue	ParamDescription
prevAET	java.lang.String	<input type="text"/>	AE Title to update.
newAET	java.lang.String	<input type="text"/>	new AE Title.

- 399
- 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	<input type="text" value="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!
-------------	------------------	----	--	--

402

403 **DVTk Modality to DCM4CHEE Configuration**

- 404 1. Open a web browser to access <http://localhost:8080/dcm4chee-web3/> and provide the following
- 405 credentials:
- 406 ■ **Username:** admin
 - 407 ■ **Password:** *****

Username:

Password:

408

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

Title	Type	Host	Port	Description	TLS	MPPS	Station name
CDRECORD		localhost	10104	Media Creation Server (part of dcm4chee)	<input type="checkbox"/>	<input type="checkbox"/>	
DCMRCV	-	localhost	11112		<input type="checkbox"/>	<input type="checkbox"/>	
DVTk_Modality	-	192.168.150.160	124	DVTk Modality Emulator	<input type="checkbox"/>	<input type="checkbox"/>	
RADIOLOGY	-	192.168.130.120	114	Acuo VNA	<input type="checkbox"/>	<input type="checkbox"/>	

410

- 411 3. Click the **New AET** button in the left-hand side of the AEs page and provide the following
412 information:

413

- **Title:** PACS

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 AET

Title:

Type:

Hostname:

Port:

Ciphersuite #1:

Ciphersuite #2:

Ciphersuite #3:

Description:

Issuer of Patient ID:

Issuer of Accession Number:

Filesystem Group ID:

Wado URL:

User Id:

Password:

Station Name:

Institution:

Department:

Installed:

Emulate MPPS:

Delay time for MPPS emulation:

420

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.

426

The screenshot shows the application interface with the 'Folder' tab selected. Below the search filters, a table displays the search results for 'Study'.

Study Date/Time	Patient ID/Issuer	Birth Date	Sex	Comments	#5/#1	Availability
6/27/2019 10:15	3	1/1/2000	M	StudyDescription	9/15	ONLINE

427 **DCM4CHEE to DVTk Modality Configuration**

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

431 **RIS System**

- 432 ▪ **IP Address:** *192.168.160.201*
- 433 ▪ **Remote Port:** 105
- 434 ▪ **AE Title:** RIS

435 **MPPS Manager**

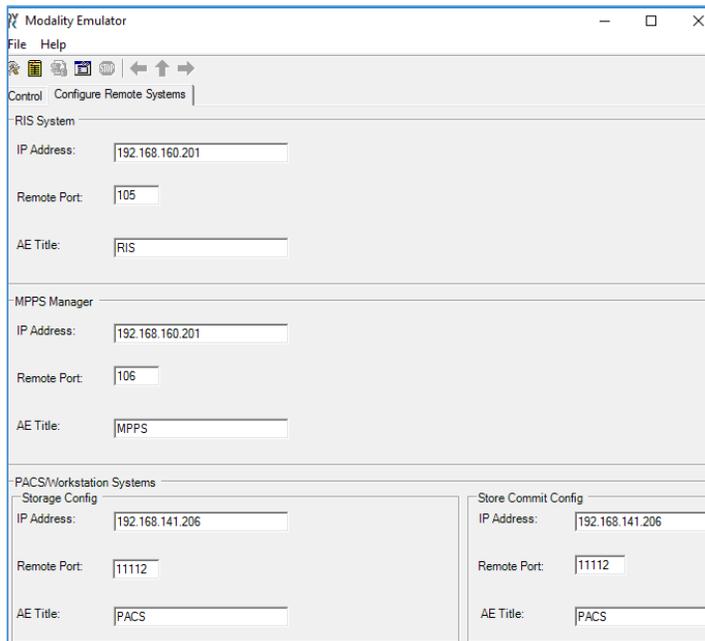
- 436 ▪ **IP Address:** *192.168.160.201*
- 437 ▪ **Remote Port:** 106
- 438 ▪ **AE Title:** MPPS

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



447

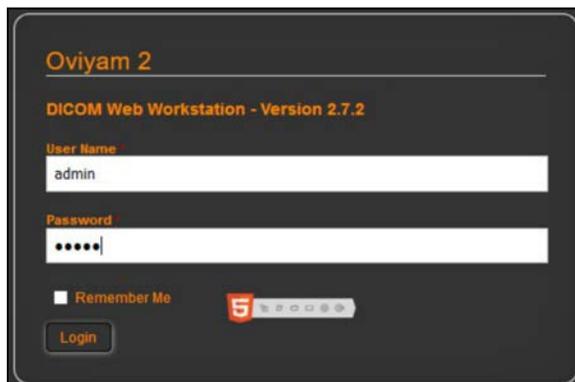
448 Oviyam Installation

449 Once downloaded from the SourceForge [8] and unzipped, copy the *oviyam.war* file to the following
 450 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

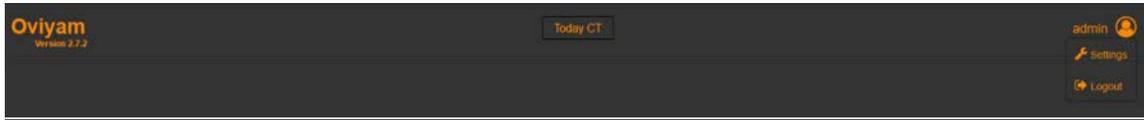
453 1. Using a browser, navigate to *http://dcm4chee_ip:8080/oviyam2* and provide the following
 454 credentials:

- 455 **Username:** admin
- 456 **Password:** *****

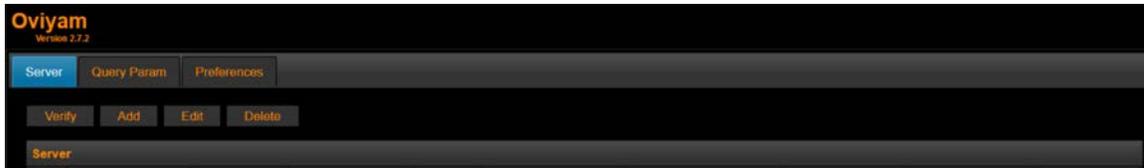


457

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



- 460 3. Under the **Server** tab, click **Add**.



- 462 4. Fill in the PACS server parameters and click the **Save** button located to the far right of the
463 parameters.

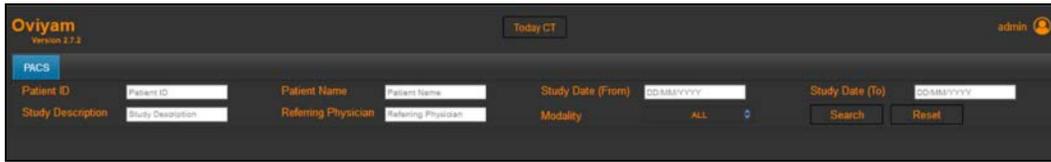
- 464 ▪ **Description:** PACS
- 465 ▪ **AE Title:** DCM4CHEE
- 466 ▪ **Host Name:** localhost
- 467 ▪ **Port:** 11112
- 468 ▪ **Retrieve Type:** WADO
- 469 ▪ **WADO Context:** wado
- 470 ▪ **WADO Port:** 8080
- 471 ▪ **Image Type:** JPEG



- 472 5. Return to http://dcm4chee_ip:8080/oviyam2 to see query parameters now available.

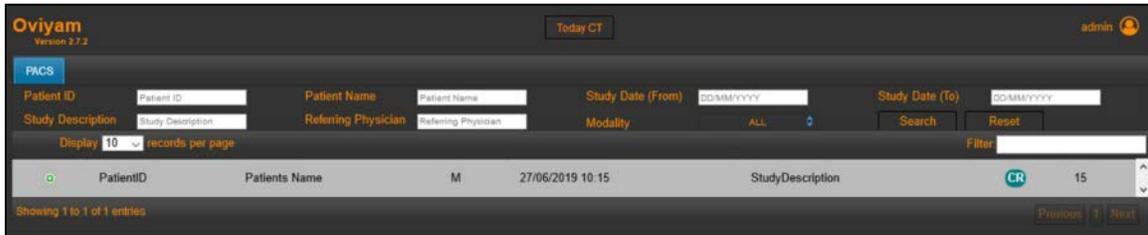
- 474 6. Click the **Search** button under the parameters on the right-hand side of the screen.

475



476 7. Double-click on a patient record.

477



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

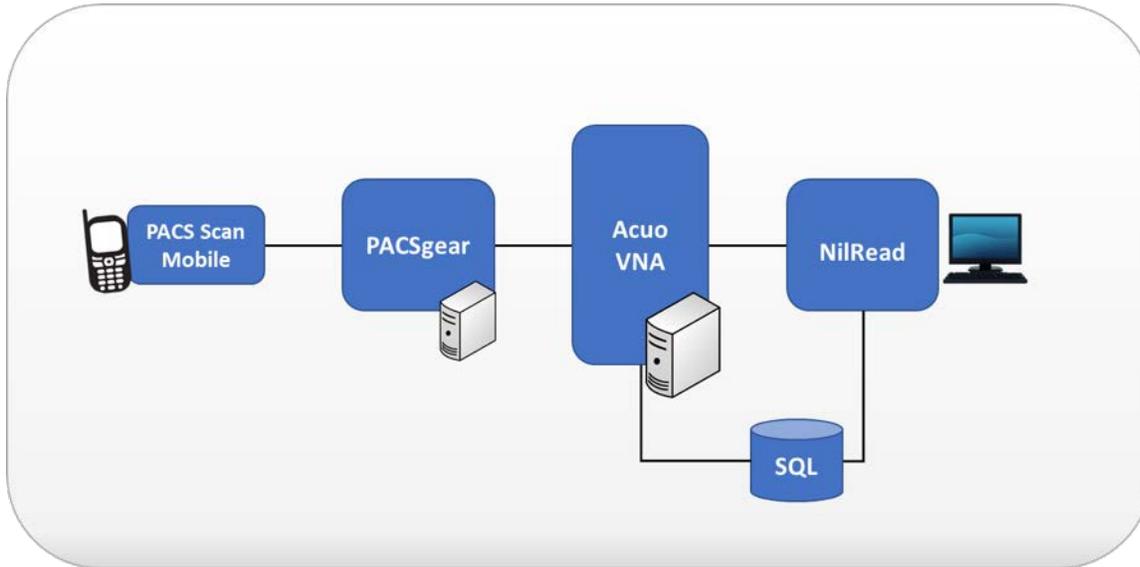
484 **PACSGear Core Server:** image processing and routing server, and back-end services

485 **PACS Scan Mobile/Web:** mobile device image acquisition and file-import application

486 **NilRead:** enterprise image-viewing application

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

489 **Figure 2-1 Hyland Systems and Applications Connectivity**



490
491 Installation procedures for the above Hyland products are described in the sections that follow.

492 2.2.1 Hyland Database Server

493 Hyland Database Server supports operations for other Hyland products, including Hyland Acuo VNA and
494 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**

- 508 1. The installation creates default service accounts for each service. The project maintained use of
509 these 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.
- 513 3. Application database instances were created as needed automatically when product applications
514 were installed.
- 515 4. This project implemented the following database instances through the SQL Server Management
516 Studio: AcuoMed, HUBDB, NILDB, and PGCORE.
- 517 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

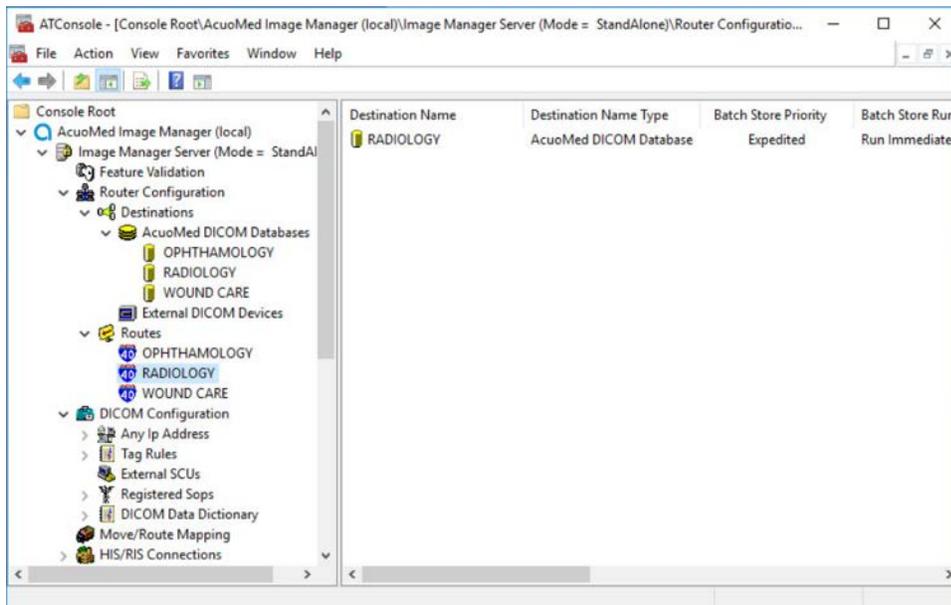
531 **Hyland Acuo VNA Installation**

- 532 1. In the NCCoE test environment, the Hyland Acuo VNA was installed on a VM preconfigured with the
533 OS and network requirements provided by Hyland. The project leveraged engineers supplied by
534 Hyland to perform the installation.

- 535 2. Upon completion of the installation, three Windows services were created: AcuoMed, AcuoAudit,
 536 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
 539 of digital images and related data, including information about the shares and about the applications
 540 that use those shares.
- 541 3. The installation created a web application for the AcuoAdmin Portal, where a Secure Sockets Layer
 542 (SSL) certificate signed by DigiCert was created and assigned to the application for hypertext transfer
 543 protocol secure (HTTPS) enforcement.

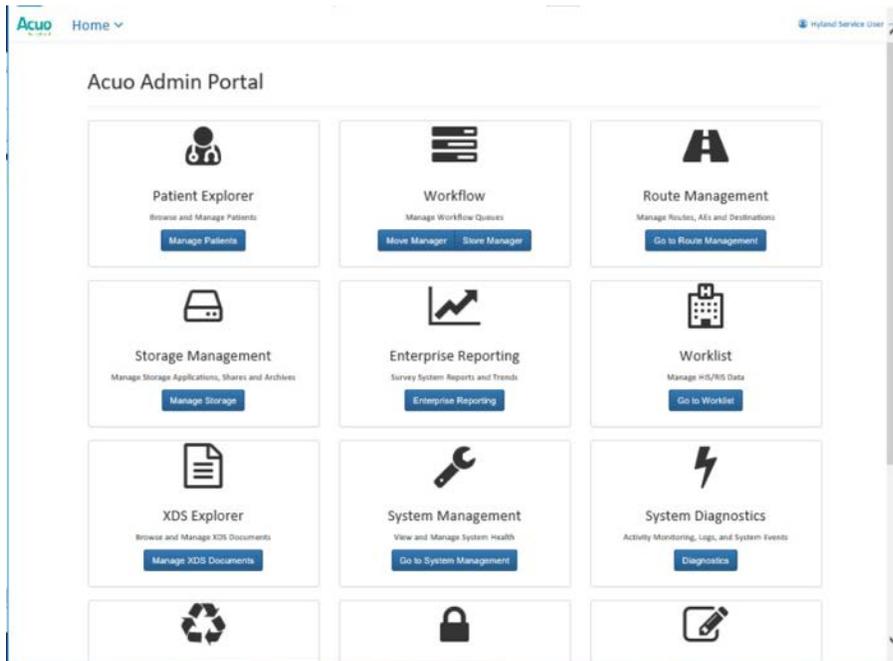
544 Hyland Acuo VNA Configuration

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:



548

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.



552

553 2.2.3 PACSgear Core Server

554 PACSgear Core Server is a capture and connectivity suite used to process DICOM and non-DICOM
 555 medical data, including patient demographics, images, videos, and HL7 messages. PACSgear Core Server
 556 can be accessed from a web browser to handle user accounts, security, and client connectivity
 557 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:

- 568 1. The installation of Hyland PACSgear Core Server was performed by Hyland engineers per their
569 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.

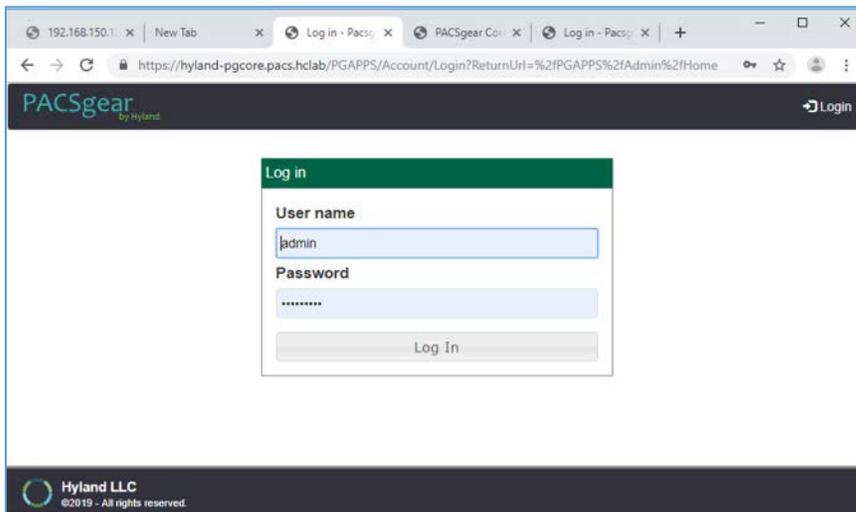
572 **PACSgear Core Server Configuration**

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.

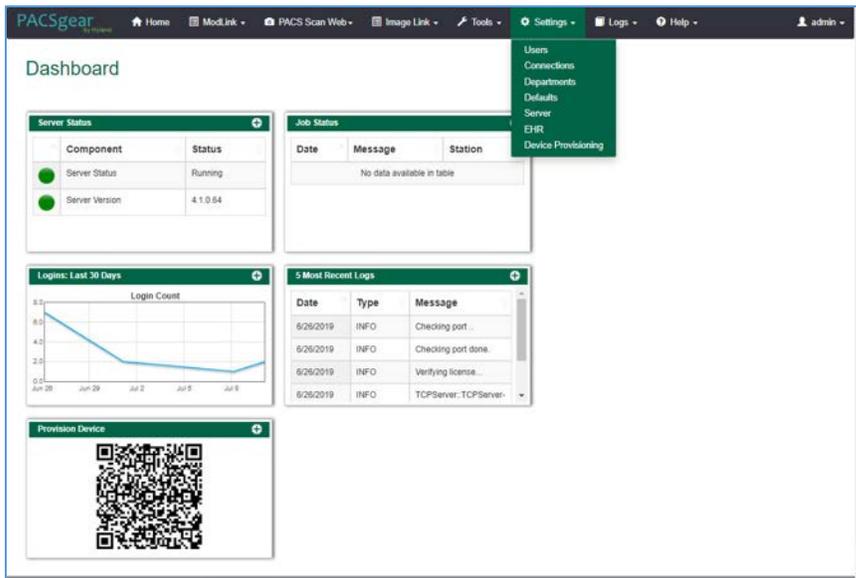
577 During the database configuration, the Hyland engineers created instances for representative
578 departments (e.g., ophthalmology, radiology, and departments that may see patients who need wound
579 treatment).

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-*
582 *pgcore.pacs.hclab/PGAPPS/Admin*.

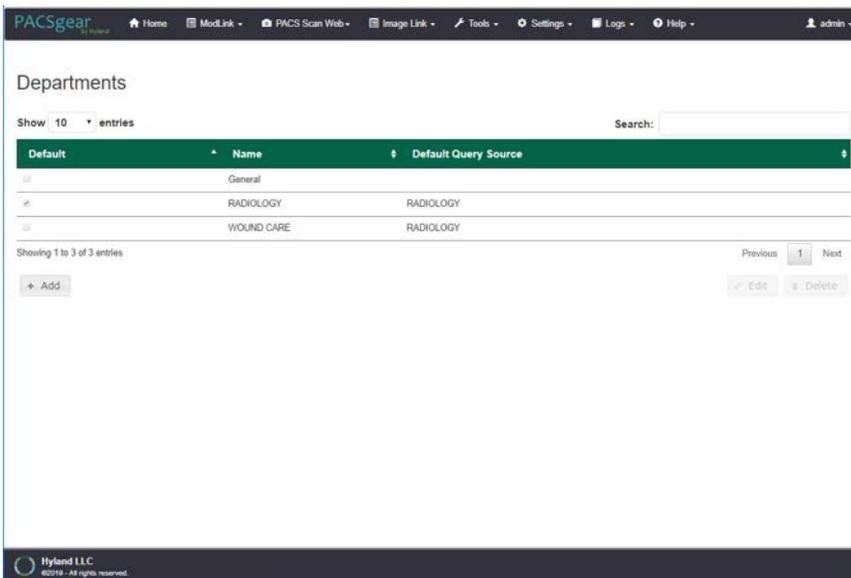


- 583
- 584 2. On the **Settings** menu, select **Departments**.



585

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



589

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

Add/Edit Department

Default

Name

AE title

Modality
 None

Apply series per image

Destinations | XDS | Lookup Sources | Client | Series

Name	Description
<input type="checkbox"/> VNA RAD	RADIOLOGY DEPT
<input type="checkbox"/> WOUND DEPT	Wound Care Department

Cancel Save

- 592
- 593 5. In the **Name** text box, the engineers entered **Ophthalmology** to create a department that ties with
- 594 the Ophthalmology database instance created during database configuration. Engineers also added
- 595 the **AE title** as **Ophthalmology** and selected a **CT Scan** for the modality.

Add/Edit Department

Default

Name
 Ophthalmology

AE title
 Ophthalmology

Modality
 CT

Apply series per image

Destinations | XDS | Lookup Sources | Client | Series

Name	Description
<input checked="" type="checkbox"/> VNA RAD	RADIOLOGY DEPT
<input type="checkbox"/> WOUND DEPT	Wound Care Department

Cancel Save

- 596
- 597 6. On the **Destinations** and **Lookup Sources** tabs, the engineers set up the destination and lookup
- 598 sources for each department.
- 599 7. On the **Client** tab, the engineers set up the client access permissions to this department's
- 600 resources.

601

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.

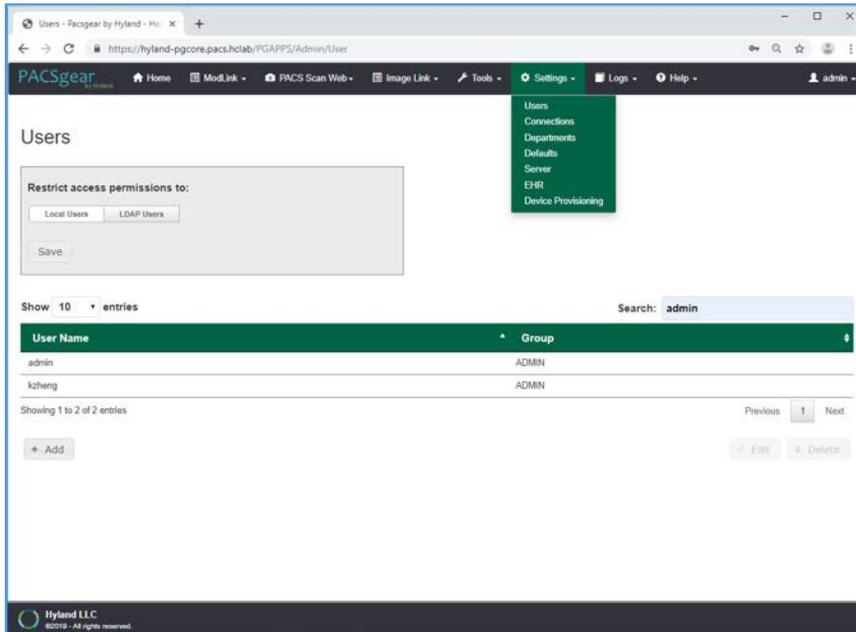
604

605 **Add LDAP/Active Directory Server:** - to use an LDAP/Active Directory server, configure these
606 parameters:

607 1. Create an **LDAP_User** account in Active Directory before proceeding.

608 2. Using a browser, log on to the **PACSGear Admin** portal by using *https://hyland-*
609 *pgcore.pacs.hclab/PGAPPS/Admin*.

610 3. On the **Settings** menu, select **Users**.



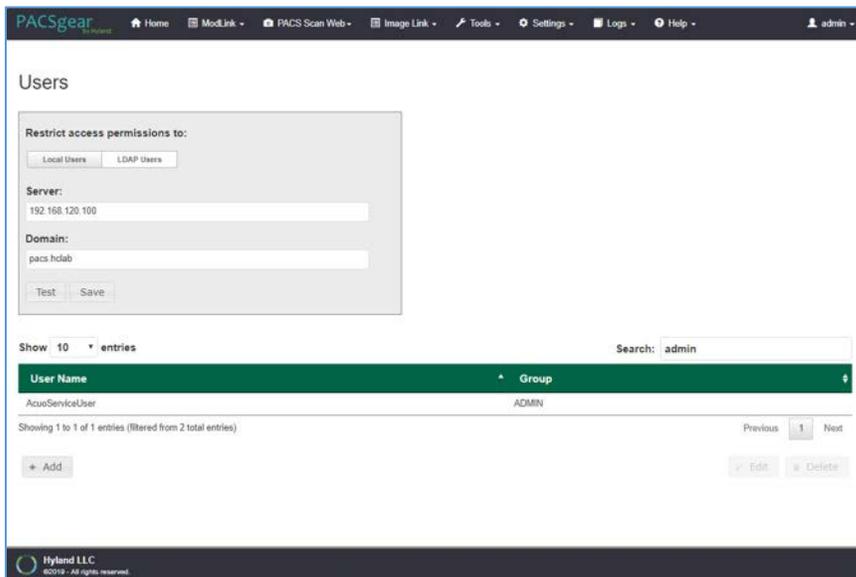
611

612

613

614

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



615

616

617

5. Click the **Test** button located under the **Domain** entry box.
6. Enter the **LDAP_User** credentials to verify connectivity to the AD.



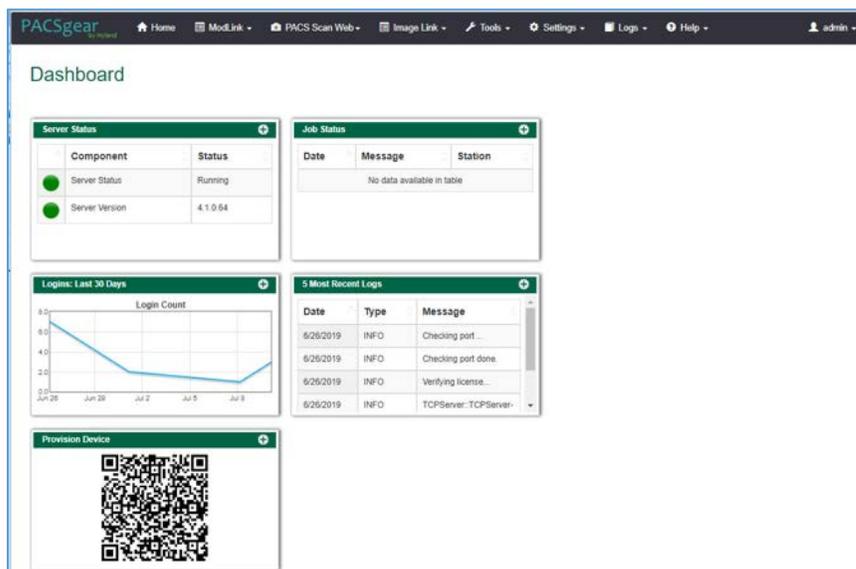
618

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

620

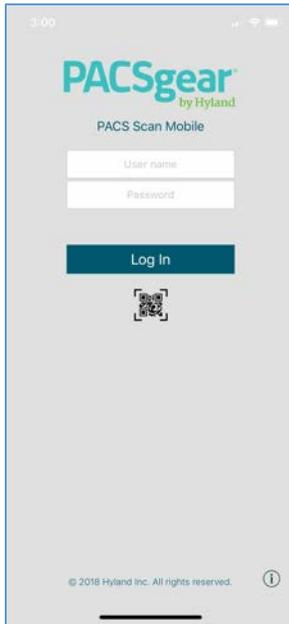
621 **PACS Scan Mobile Configuration**—Install and configure the PACS Scan application to an Apple iPhone by
 622 applying these steps:

- 623 1. On the iPhone, navigate to the **App Store**. Search for PACS Scan Mobile, from Perceptive Software.
 624 Perceptive Software is a Hyland business unit. Select the **GET** button to install the software, and
 625 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**.



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.



631

632

633

634

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.

635

636

5. From a workstation, acquire the trusted root certificate from DigiCert. Further information for using DigiCert is described in [Section 2.6.2](#).

637

638

6. Download the root certificate to the workstation local drive and attach the certificate as an email attachment sent to the installer.

639

640

7. The installer opens the email from the iPhone and double-clicks on the attachment to install the certificate to the device.

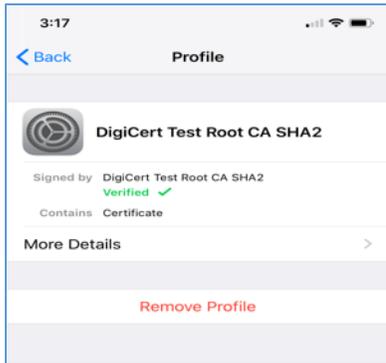
641

642

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:



644

645 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:



649

650 2.2.4 Hyland NilRead

651 Hyland NilRead provides image access and viewing from various devices including clinical viewing
652 stations, tablets, and mobile devices. NilRead also provides image manipulation, interpretation, and
653 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

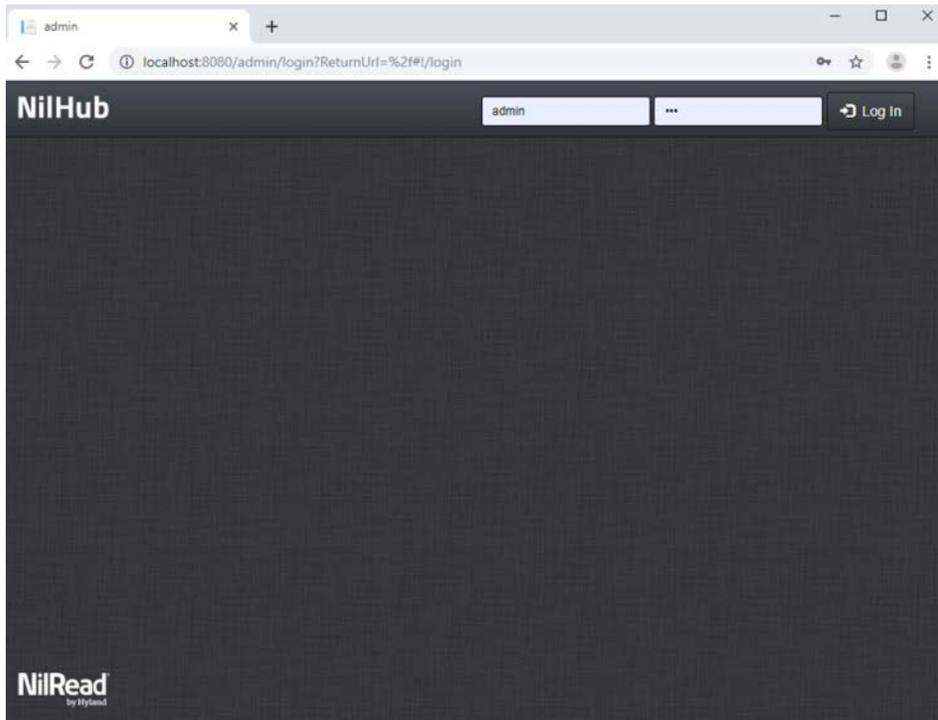
662 **Network Adapter:** VLAN 1301

663 **Hyland NilRead Installation**

- 664 1. The installation of Hyland NilRead was performed by Hyland engineers based on Hyland’s proprietary
665 installation package and installation guides. NilRead has three services: the Hub Front End service,
666 Nil Back End service, and Nil Front End service. The Hub Front End service is used to provide
667 management service for multi-tenant configuration. The operation context is defined by the Nil
668 database content and includes user accounts, data life-cycle rules, hanging protocols, DICOM
669 connectivity setup, and cached DICOM data index.
- 670 2. The installation created two web applications for the NilHub and NilRead Viewer, where SSL
671 certificates signed by DigiCert were created and assigned to the applications for HTTPS enforcement.

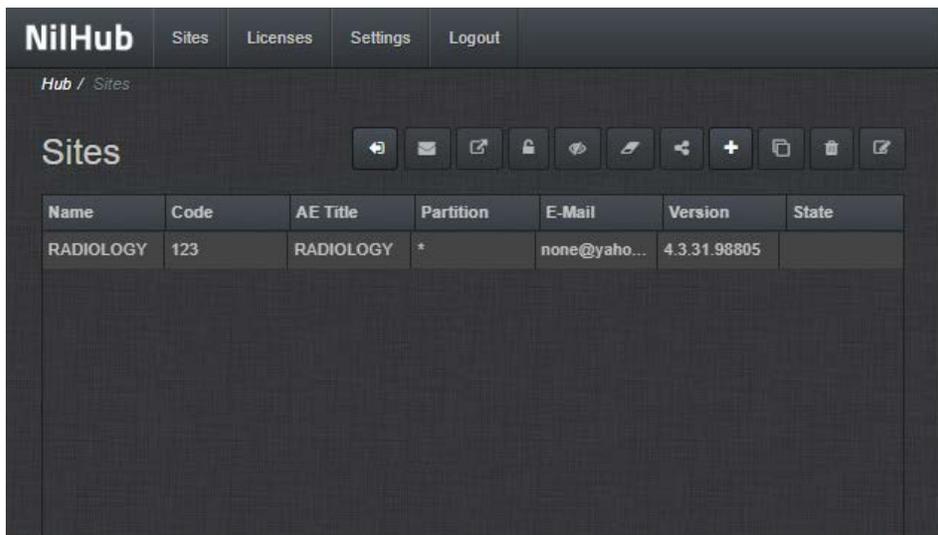
672 **Hyland NilRead Configuration**

673 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:



675

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



678

- 679 2. Click on the + icon on the right-hand side of the screen, to create a new **Site** for **WOUND_CARE**
680 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

The screenshot shows the 'New' form in NilHub. The fields are as follows:

Field	Value
NAME	WOUND_CARE
USER ID	admin@WOUND_CARE
DETAILS	Wound Care Department
VNA PARTITION	WOUND_CARE
CODE	974
DATABASE NAME	WOUND_CARE
AE TITLE	WOUND_CARE
CACHE PATH	C:\InRepository\WOUND_CARE
EMAIL	none@hyland.com
ENABLE SPORE FEDERATION	<input type="checkbox"/>

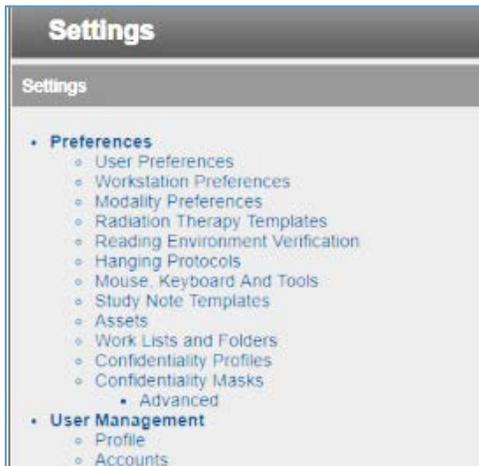
- 688
- 689 3. Log back in to **NilHub** specifying the **WOUND_CARE** Site in the top section of the log in screen.

The screenshot shows the NilRead by Hyland login screen. The fields are as follows:

Field	Value
Site	WOUND_CARE
User Name	admin
Password	***
Domain	

Below the login fields is a 'Login' button. At the bottom of the screen, there is a 'Test your connection speed' section with a 'Connection Type' dropdown set to 'Auto detect' and a 'Waiting Room' icon.

- 690
- 691 4. Click the **Settings** tab. Navigate to the **User Management** section and click on **Accounts**.



692

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

- 694 ▪ **User Name:** pacs\ptester
- 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.

The screenshot displays the 'pacs\plester' user management window. It is divided into several sections:

- Account:** Fields for User Name (pacs\plester), Role (User), E-mail (plester@hyland.pacs.com), Last Name (Tester), First Name (Pacs), Middle Name, Prefix, Suffix, Department, Job Description (Physician), and Expiry Date (Unlimited). There are also checkboxes for 'Notify on Study Arrival' and 'highlighted fields are mandatory'.
- Groups:** A table with 'Member' and 'Not Member' columns. The 'Not Member' column contains the text 'CN=Wound_Care,CN=Users,DC=pacs.l'.
- Privileges:** A table with 'Granted' and 'Revoked' columns. The 'Granted' column lists 'DicomQueryRetrieve', 'DicomRt', 'EditHangingProtocols', and 'EditWorkItems'. The 'Revoked' column lists 'BookmarkSaveSend', 'Collaboration', 'ContentDownload', and 'ContentUpload'.
- Licensing:** A section for 'License Features' with a list of features like 'adapterCoActiv', 'adapterMach7Tech', 'adapterTeraMedica', 'advancedDataQualityControl', and 'advancedMeasurements'. Below it is a section for 'Active Licenses' with 'NCCoE' listed.
- DICOM Physician Names:** A section for 'Associated' names with a list box.
- Timeline data source access restrictions:** A section for 'Effective permissions' with 'Local_Wound_Care_VNA' listed.

 At the bottom, there are 'Save' and 'Cancel' buttons.

703

704 Hyland engineers repeated the above steps to have multiple Sites that accessed different VNA
 705 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
 714 familiarity with DigiCert. Refer to [Section 2.6.2](#) for further detail.

715 *2.3.1.1 Create PKI Certificate for Hyland Acuo VNA*

716 1. Use DigiCert Certificate Utility for Windows to generate a certificate signing request (CSR) for
717 Hyland Acuo VNA. Information needed for requesting the certificate for Hyland Acuo VAN is shown
718 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.
- 728 3. Download and save the signed certificate along with its root Certificate Authority (CA) certificate in
729 the .pem file format.
- 730 4. Import the saved certificate to DigiCert Certificate Utility for Windows, and then export the
731 certificate 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*

734 1. Use **DigiCert Certificate Utility for Windows** to generate a CSR for PACS server. Information
735 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

- 744 2. Submit the created CSR to DigiCert portal for certificate signing.
745 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.

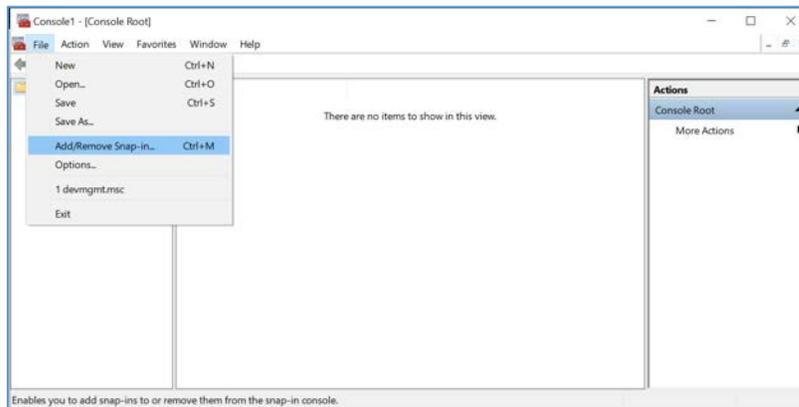
749 2.3.2 PKI Certification Installation

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

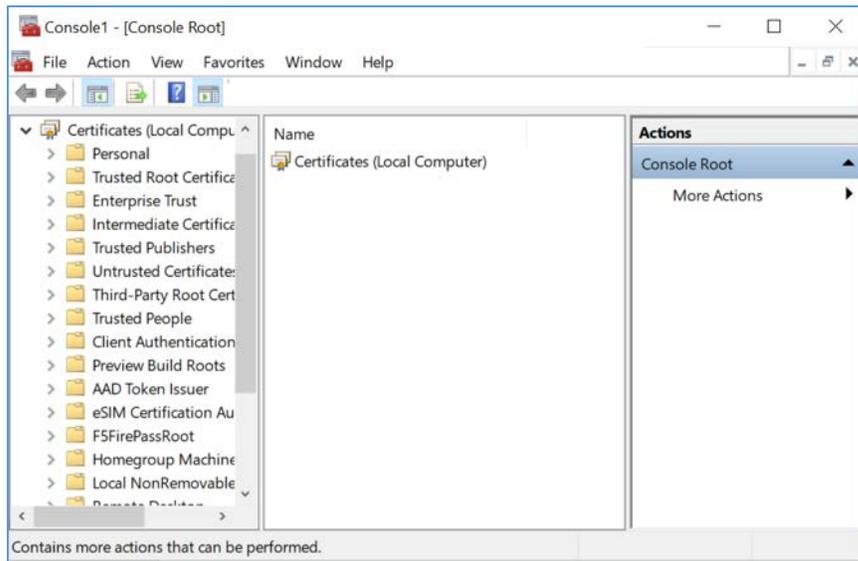
753 2.3.2.1 Install PKI Certificate for Hyland Acuo VNA

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

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

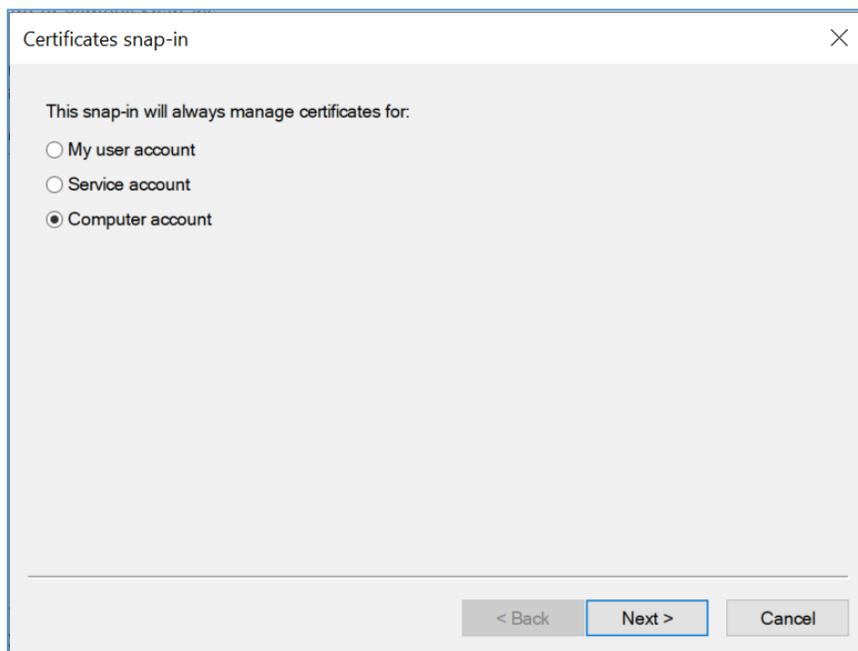


- 757
758 3. Select **Certificates** and click **Add**.
759 ▪ Choose **Computer Account**
760 ▪ Choose **Local Computer**
761 4. Click **Finish**, then click **OK**.



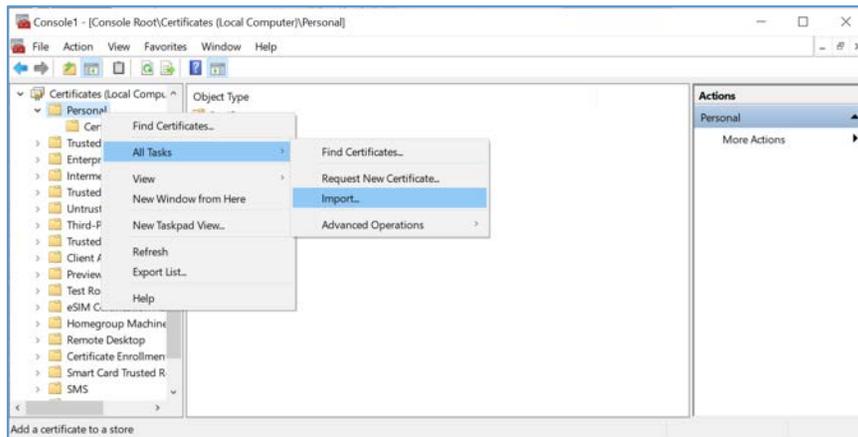
762

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



764

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



768

769 7. Add the appropriate permissions to the newly generated certificate private key.

770 a. Navigate to **Certificates > Personal > Certificates**.

771 b. Right click on the certificate, select **All Tasks > Manage Private Keys...**

772 c. Add the **AcuoServiceUser** and grant full control permissions. Click **OK**.

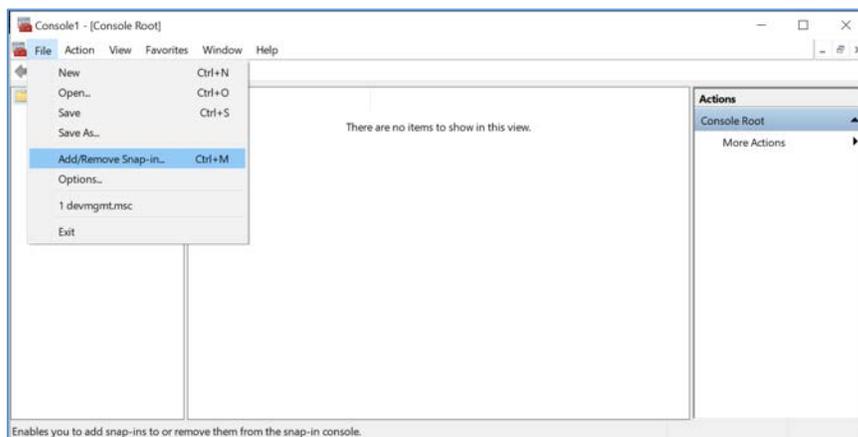
773 This procedure also installs the signing CA Root certificate (**DigiCert Test Root CA SHA2**) and its
774 Intermediate Root certificate (**DigiCert Test Intermediate Root CA SHA2**) into the server computer.

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:

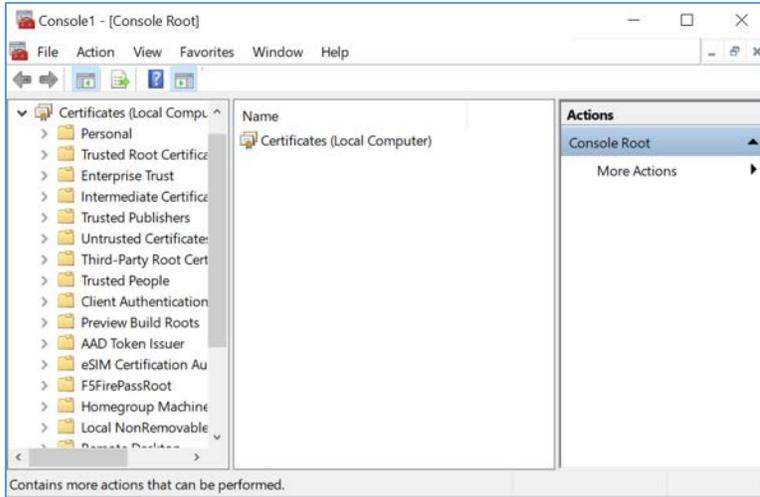
777 1. From the IntelliSpace server, click on **Start > Run > mmc**.

778 2. Select **File > Add/Remove Snap-in...**

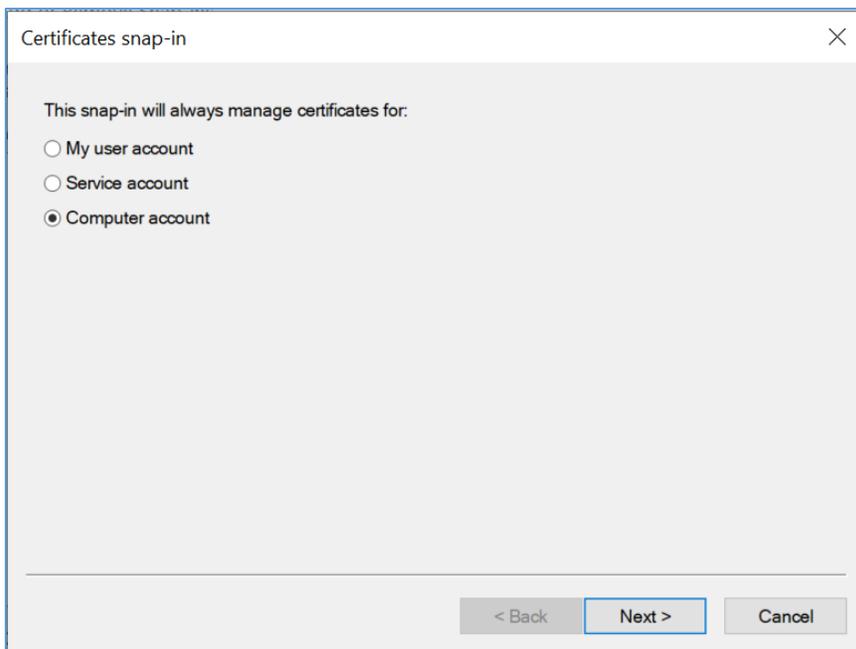


779

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

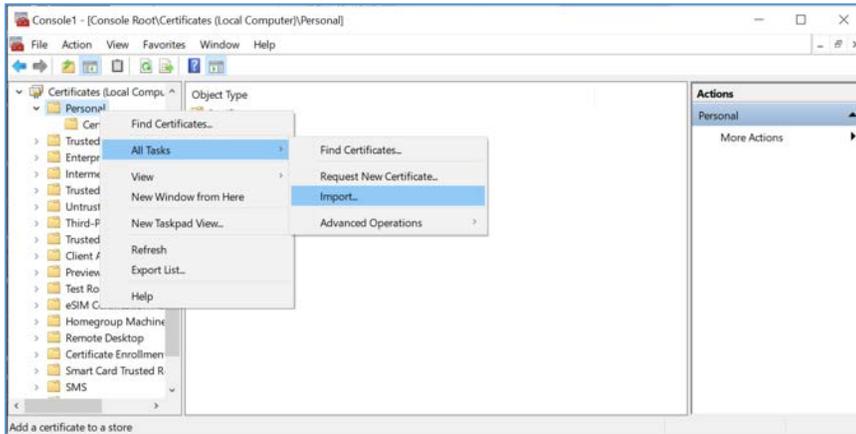


- 784
- 785 4. Once the snap-in has been added, navigate to **Certificates (local computer)/Personal/Certificates**.



786

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



- 790
- 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

795 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

797 between these two endpoints, and secure data-in-transit communications bi-directionally between the

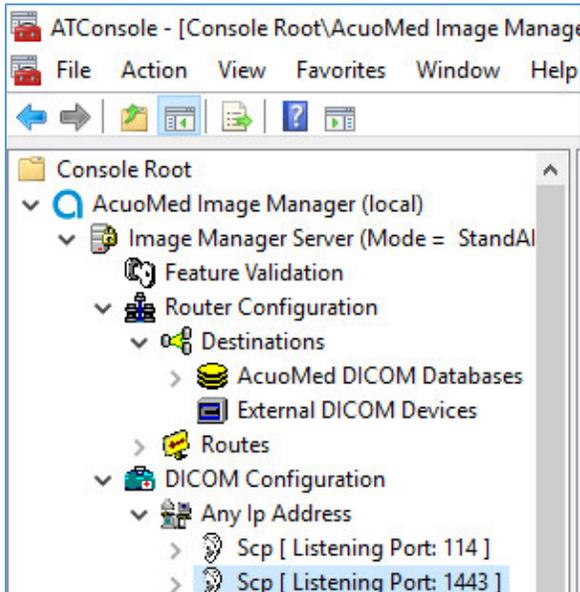
798 VNA and PACS.

799 2.3.3.1 TLS Configuration for Hyland Acuo VNA

800 For receiving TLS DICOM message from IntelliSpace PACS, configure a new service-class provider (SCP) in

801 Acuo VNA using Microsoft Windows Console. Configuration is done from the Acuo VNA server.

- 802 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.



805

806

807

808

809

810

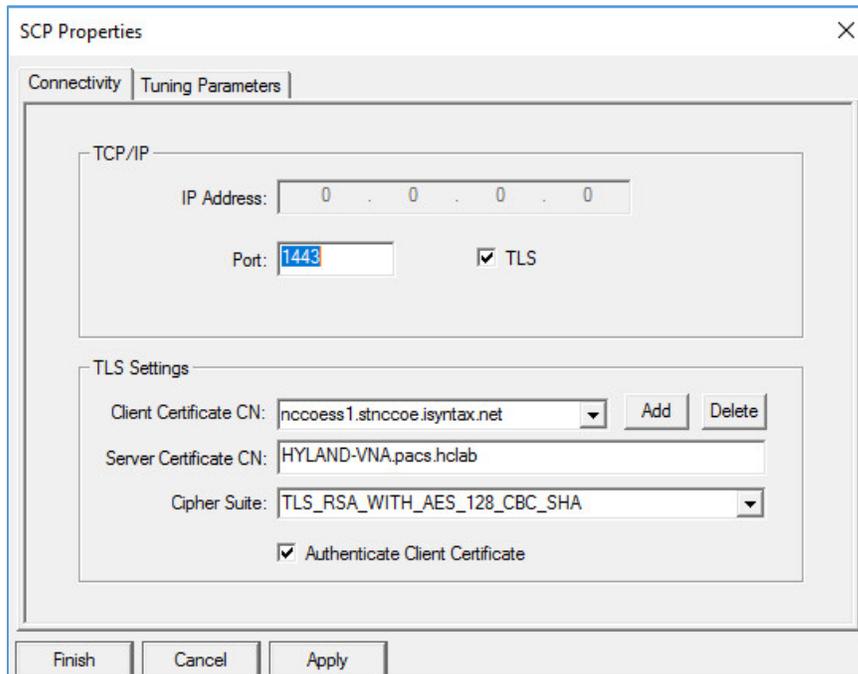
811

812

813

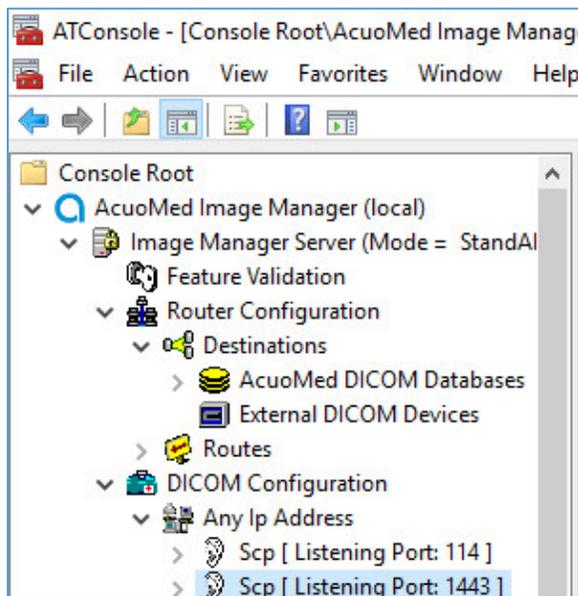
3. On the **Connectivity** tab of the **SCP** Properties page, provide the information below and click **Add**, **Apply**, and then **Finish**:

- **Port:** 1443
- Check the **TLS** checkbox
- **Client Certificate CN:** nccoess1.stnccoe.issyntax.net
- **Server Certificate CN:** HYLAND-VNA.pacs.hclab
- **Cipher Suite:** TLS_RSA_WITH_AES_128_CBC_SHA
- Check the **Authenticate Client Certificate** checkbox



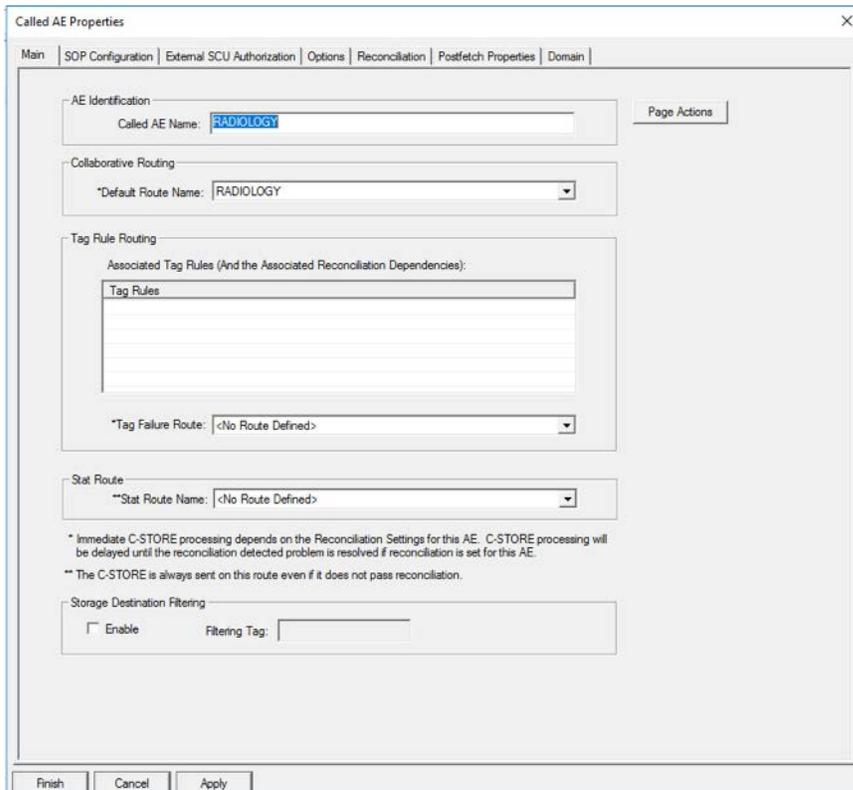
814

- 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

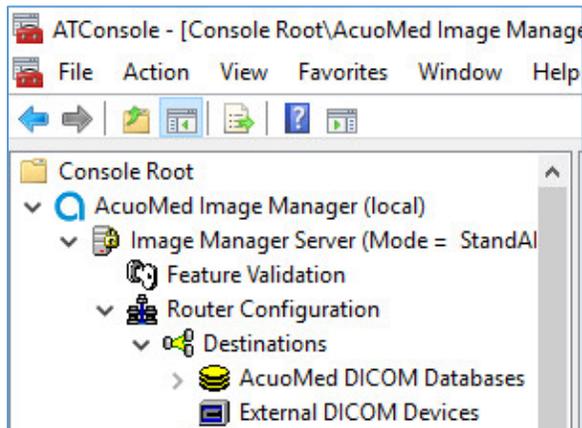
- 818 5. Fill in the **Called AE Name:** e.g., **RADIOLOGY** and **Default Route Name:** e.g., **RADIOLOGY**. After
 819 populating the information, click **Add**.



820

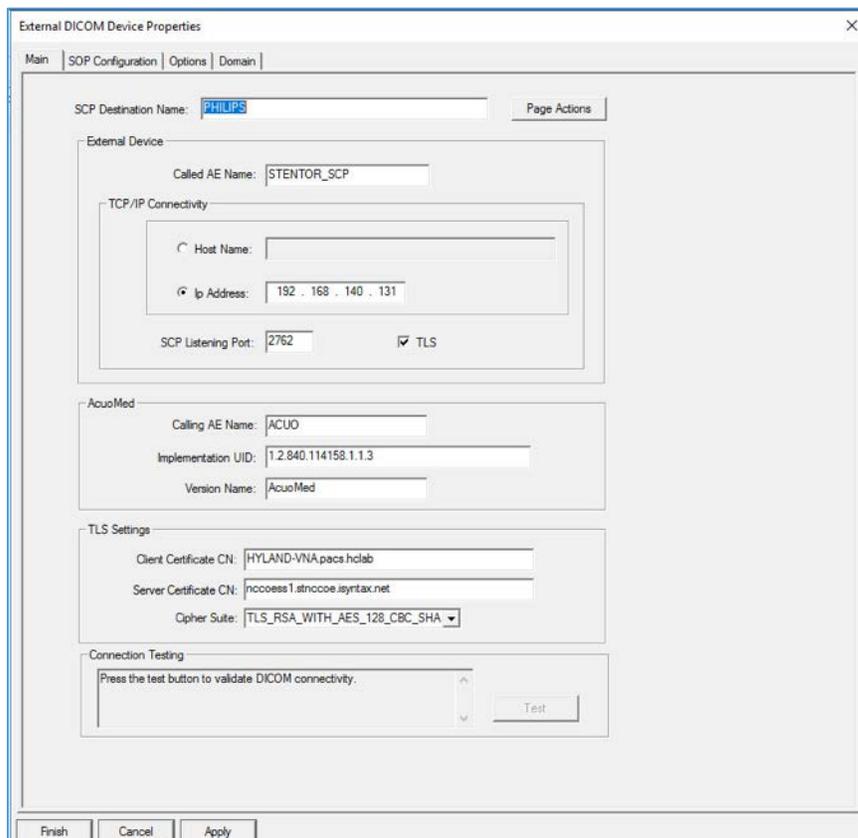
821 For sending TLS DICOM message to IntelliSpace PACS, configure an External DICOM Device from the
 822 Acuo VNA by using Microsoft Windows Console.

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



826

- 827 3. On the **Main** tab of the **External DICOM Devices Properties** page, provide the information below
828 and click **Apply**, and then click **Finish**:
- 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 **TLS** 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



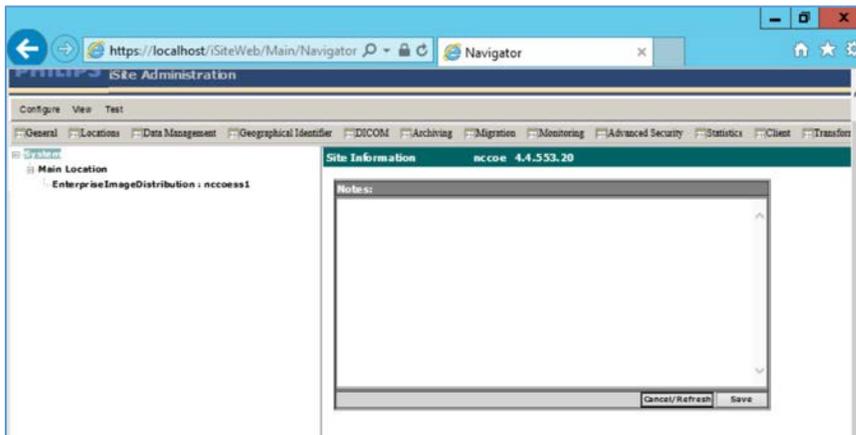
- 839
- 840 4. Restart the **AcuoMed** service.

841

2.3.3.2 TLS Configuration for Philips IntelliSpace PACS

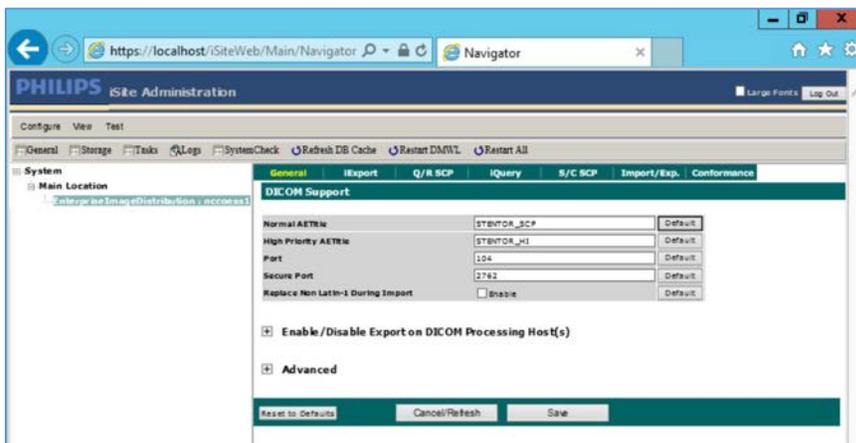
842 Next, configure TLS on the IntelliSpace PACS server. The steps below would be taken to enable this
843 feature on the PACS:

- 844 1. Access the Philips iSite Administration web site <https://192.168.140.131/iSiteWeb> using
845 administrator credentials.



846

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

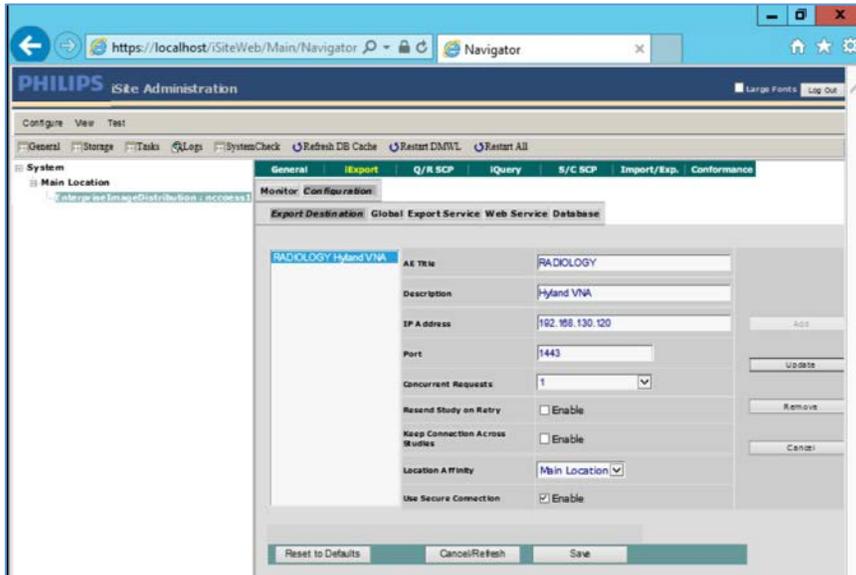


848

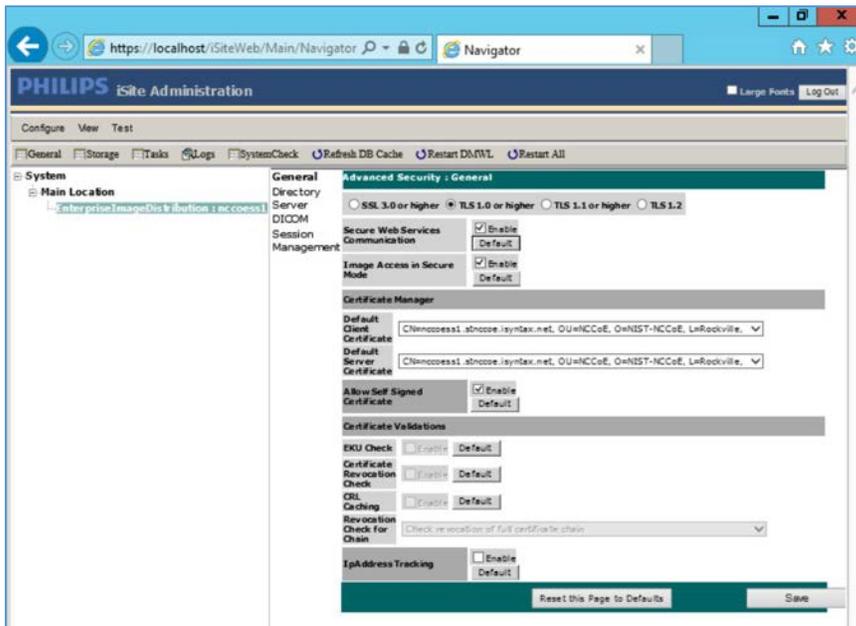
- 849 3. On the top menu, click **iExport** to open the **iExport** screen. Provide the information below, and click
850 **Save**:

- 851
- 852 ■ **AE Title:** RADIOLOGY
 - 853 ■ **Description:** Hyland VNA
 - 854 ■ **IP Address:** 192.168.130.120

- 854 ▪ **Port: 1443**
- 855 ▪ **Use Secure Connection: checked**

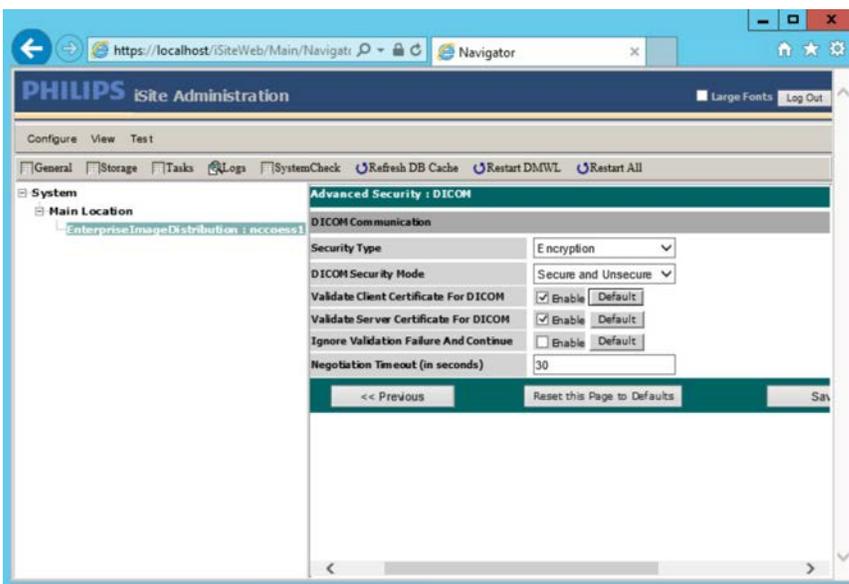


- 856
- 857 4. Click **Configuration > Advanced Security**, perform these selections:
- 858 ▪ **TLS 1.0 or higher: Selected**
- 859 ▪ **Enable Secure Web Services Communication**
- 860 ▪ **Enable Image Access in Secure Mode**
- 861 ▪ **Default Client Certificate: CN= nccoess1.stnccoe.isyntax.net**
- 862 ▪ **Default Server Certificate: CN=HYLAND-VNA.pacs.hclab**
- 863 ▪ **Click Save to save the settings**



864

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



869

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
873 Acuo VNA and IntelliSpace PACS servers are ready to perform the TLS secure DICOM communication
874 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
885 system. It can simulate a real modality to test and verify communication with all the DICOM services. It
886 uses DICOM files as input for Queries, modality performed procedure step (MPPS), and Storage actions.
887 Consequently, this project chose to use the DVTK Modality as an emulator to test the connectivity,
888 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

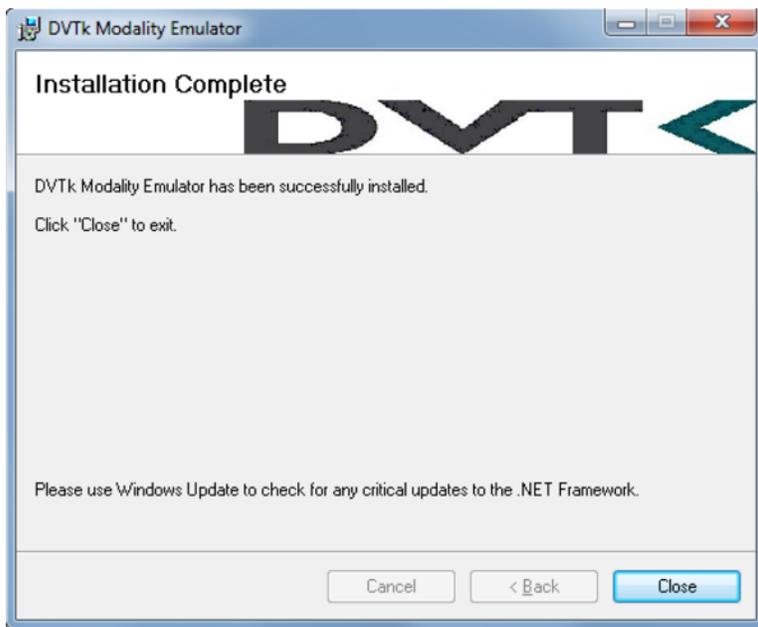
892 DVTK Modality Installation

- 893 1. Download the installation software from the DVTK site [11].
- 894 2. Click the **Modality Installation** file (e.g., *DVtk-Modality-Emulator-5.0.0.msi*) to start the installation
895 process.



896

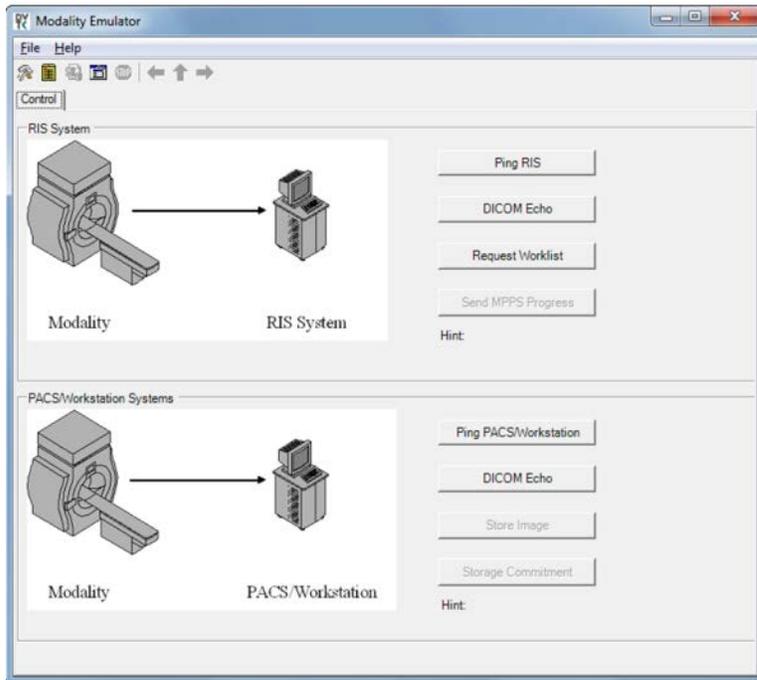
- 897 3. Follow the wizard instruction to continue the installation until it reaches successful completion.



898

- 899 4. **Close** the installation window.

- 900 5. The DVTk Modality Emulator can be launched from the **PC Start** menu. The Modality Emulator
901 interface is shown below.



902

903 **DVTk Modality Configuration**

904 Configuration of the DVTk Modality involves the configuration of the communications with different
 905 external systems, including the RIS, which is the Worklist provider or a worklist broker connected to the
 906 RIS; the MPPS manager that handles the MPPS messages for status reporting; and the PACS and its
 907 database where the images will be stored. The information needed for these external systems should
 908 include the correct IP-Address, Port number, and Application Entity Title (AETitle). Input the information
 909 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

DRAFT

920 ▪ **Remote Port:** 106

921 ▪ **AE Title:** MPPS

922 **PACS/Workstation Systems–Storage Commit Config**

923 ▪ **IP Address:** localhost

924 ▪ **Remote Port:** 107

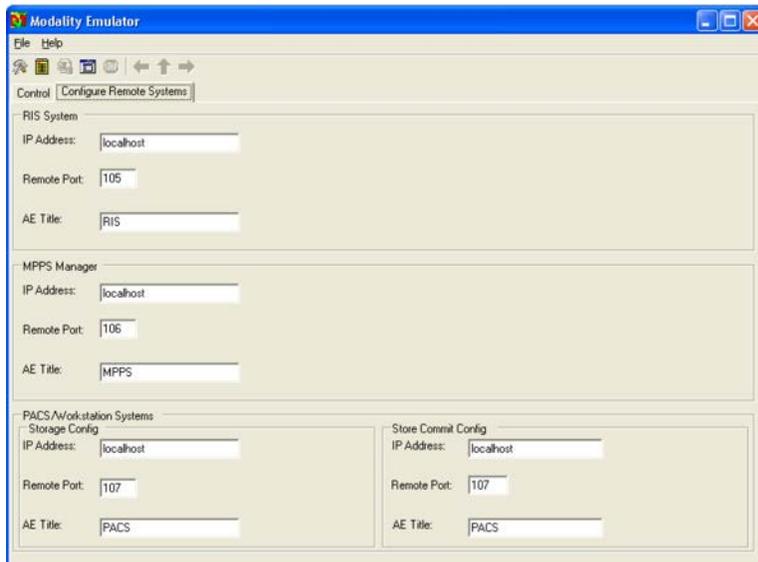
925 ▪ **AE Title:** PACS

926 **Store Commit Config**

927 ▪ **IP Address:** localhost

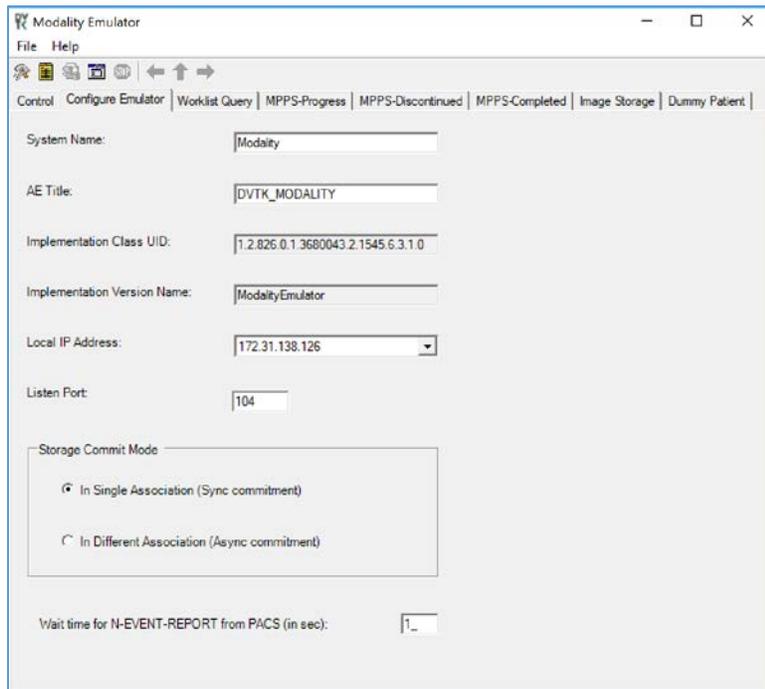
928 ▪ **Remote Port:** 107

929 ▪ **AE Title:** PACS



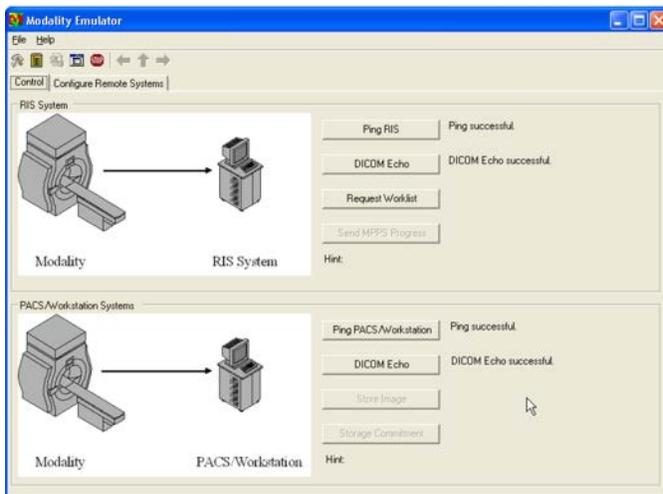
930

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



935

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**

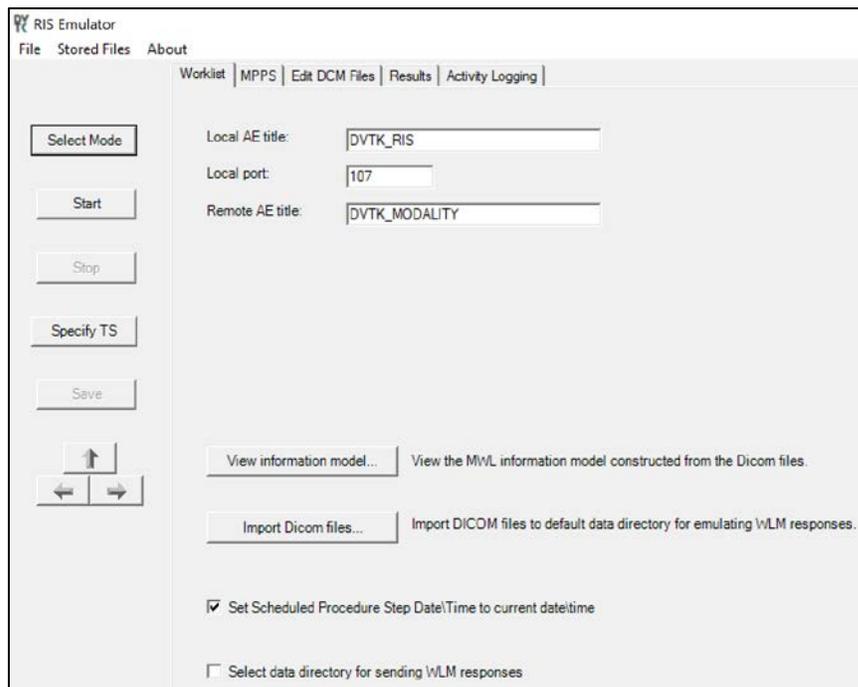
942 DVTk, the Health Validation Toolkit, is an open-source software. The DVTk RIS Emulator is an application
943 that handles Modality Worklist and Modality Performance Procedure Step requests from remote
944 applications and then responds with the emulated results using the DICOM files specified by 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 <http://www.dvtk.org>.
- 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 successful
951 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



959

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
- 968 to the Worklist requests. A default setting can be used which is *C:\Program Files\DVTk\RIS*
- 969 *Emulator\Data\Worklist*

970 2. The **RIS Emulator** also supports other parameter configuration such as MPPS and Store Files

971 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

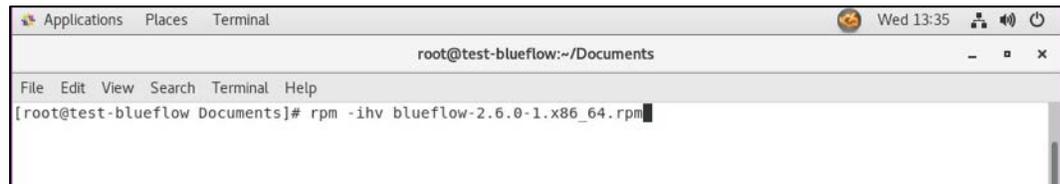
982 **Storage:** 100 GB (Thin Provision)

983 **Operating System:** CENTOS 7

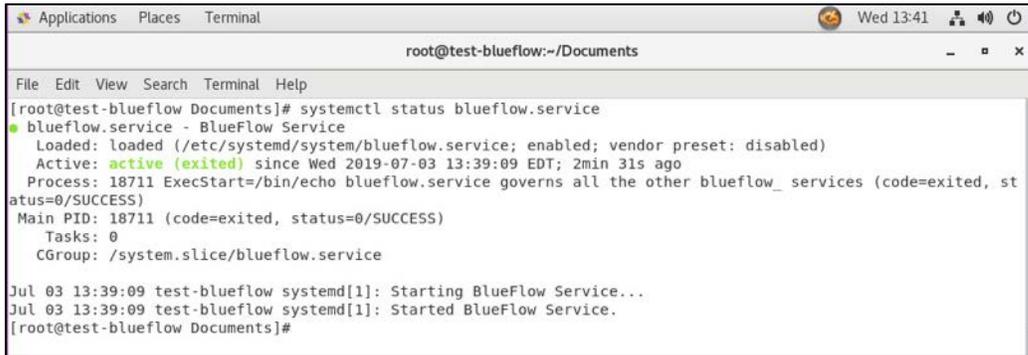
984 **Network Adapter:** VLAN 1201

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.

A screenshot of a terminal window. The window title is "Applications Places Terminal" and the current directory is "root@test-blueflow:~/Documents". The terminal shows the command "[root@test-blueflow Documents]# rpm -ihv blueflow-2.6.0-1.x86_64.rpm" being entered. The window also shows a menu bar with "File Edit View Search Terminal Help" and system icons for network, volume, and power in the top right corner.

- 990
- 991 2. Run `systemctl status blueflow.service` in the CentOS 7 terminal.
- 992 3. Ensure **blueflow.service** is active.

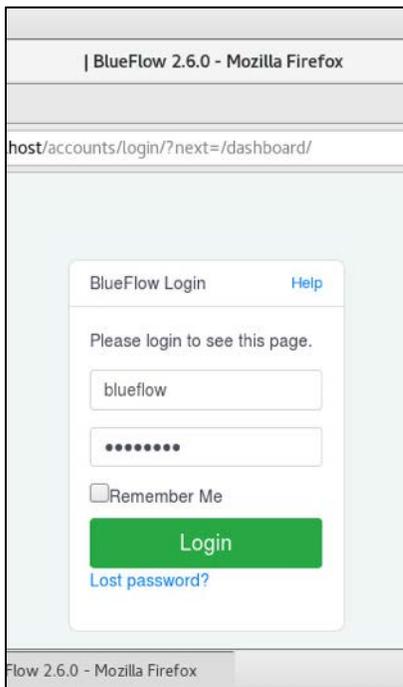


```
root@test-blueflow:~/Documents
File Edit View Search Terminal Help
[root@test-blueflow Documents]# systemctl status blueflow.service
● blueflow.service - BlueFlow Service
   Loaded: loaded (/etc/systemd/system/blueflow.service; enabled; vendor preset: disabled)
   Active: active (exited) since Wed 2019-07-03 13:39:09 EDT; 2min 31s ago
     Process: 18711 ExecStart=/bin/echo blueflow.service governs all the other blueflow_ services (code=exited, status=0/SUCCESS)
   Main PID: 18711 (code=exited, status=0/SUCCESS)
     Tasks: 0
    CGroup: /system.slice/blueflow.service

Jul 03 13:39:09 test-blueflow systemd[1]: Starting BlueFlow Service...
Jul 03 13:39:09 test-blueflow systemd[1]: Started BlueFlow Service.
[root@test-blueflow Documents]#
```

993

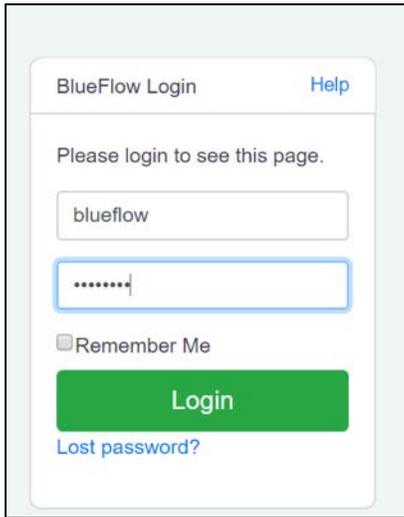
- 994 4. Visit <https://localhost> to verify BlueFlow web service is operating as expected, with a **BlueFlow**
995 **Login page.**



996

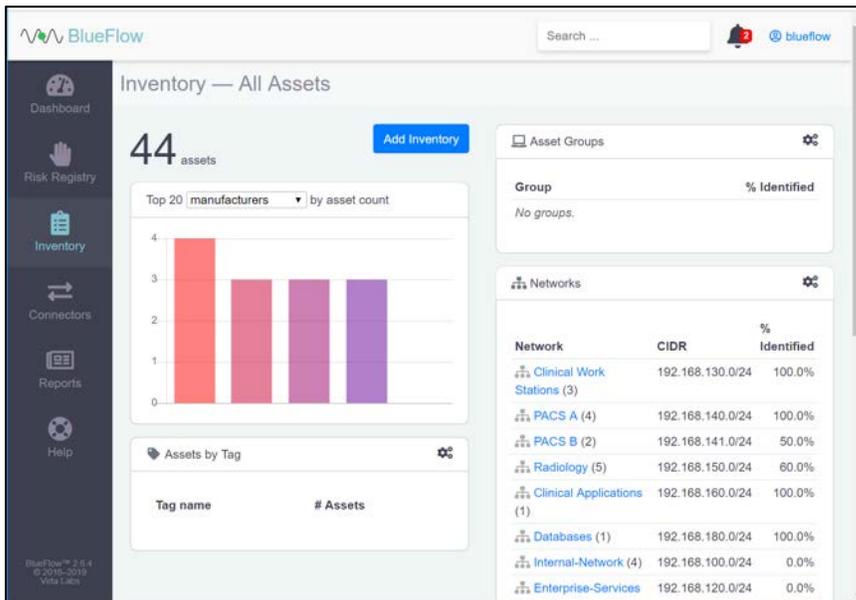
997 **Virta Labs BlueFlow Network Groups Configuration**

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



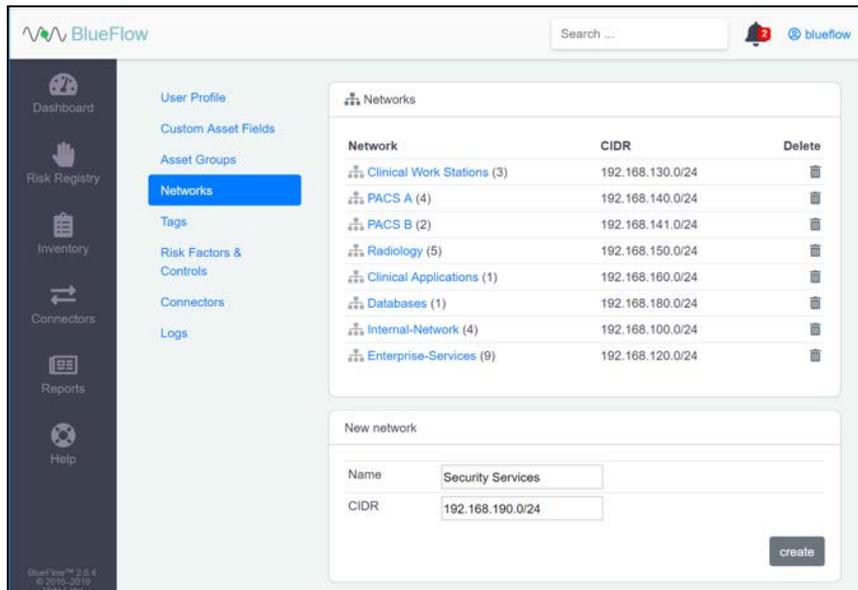
999

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



1002

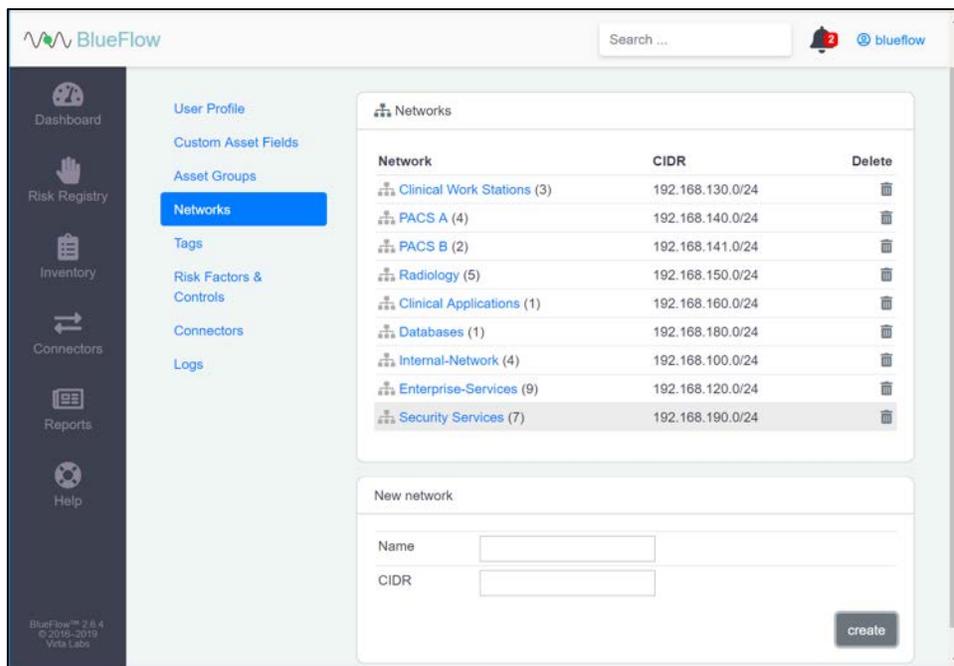
- 1003 4. Enter **Security Service** as a **Name** for the new **network group**.
- 1004 5. Enter **192.168.190.0/24** as a **CIDR** for the new **network group**.
- 1005 6. Click **create**.



1006

1007 7. Verify that the new **network group (Security Services)** has been created.

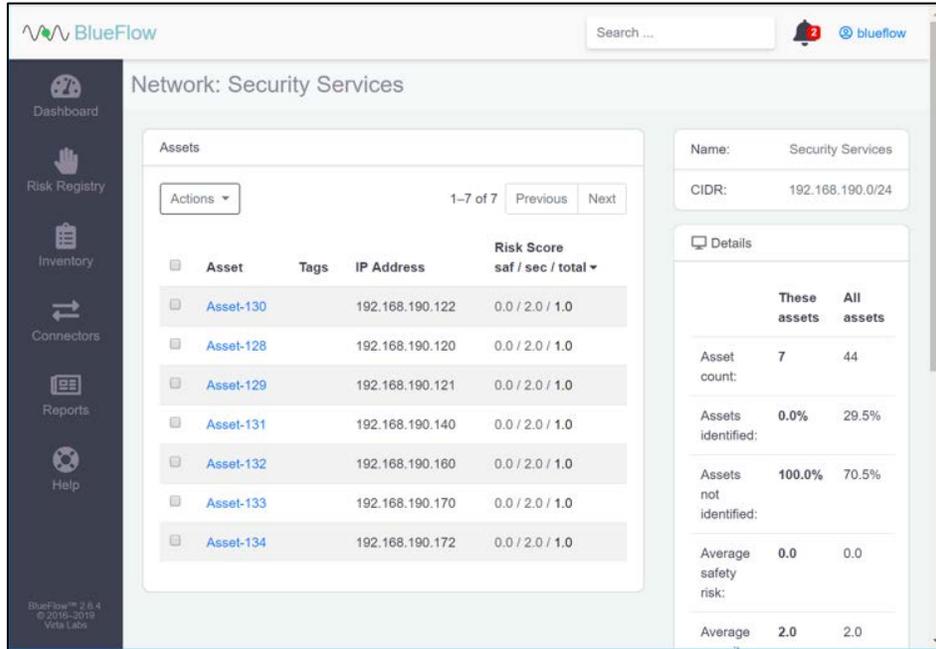
1008 8. Click on the **name** of the new network group.



1009

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

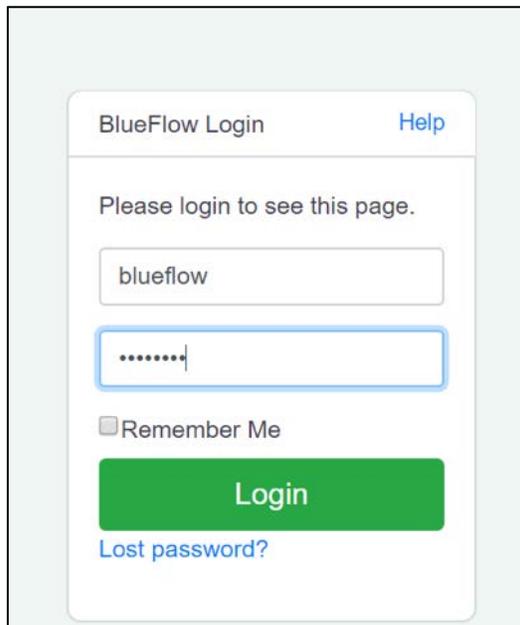
- 1011 10. If there are no **assets** currently listed, you can manually add them by navigating to **Inventory > Add**
1012 **Inventory** or by running an IP discovery scan (detailed in the next section).



1013

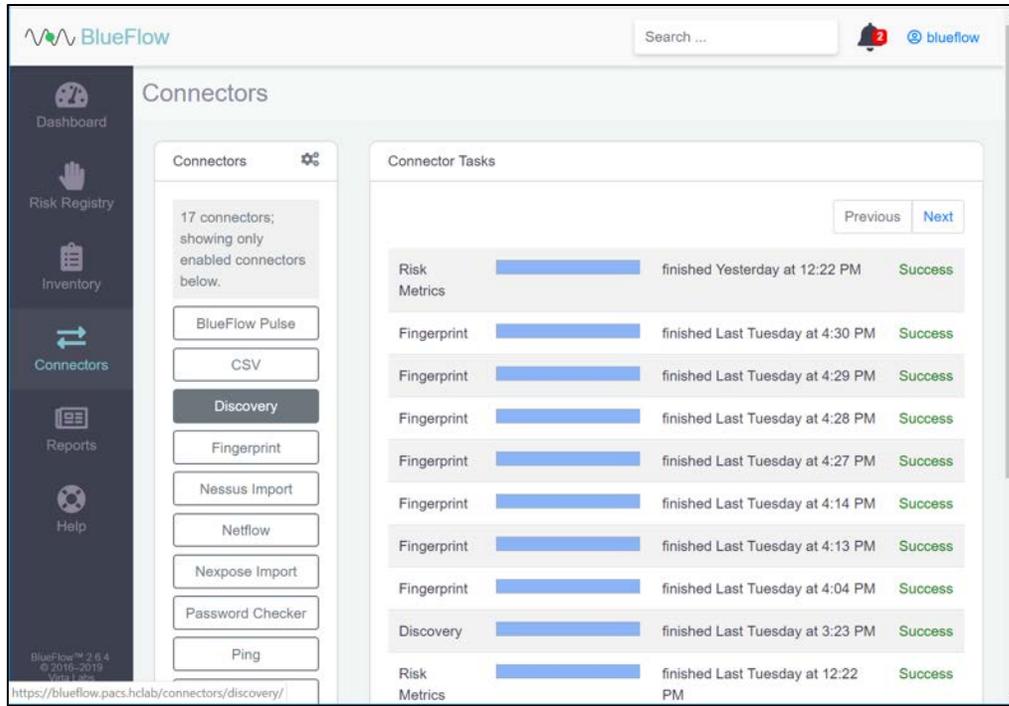
1014 **Running an IP Discovery Scan in Virta Labs BlueFlow**

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



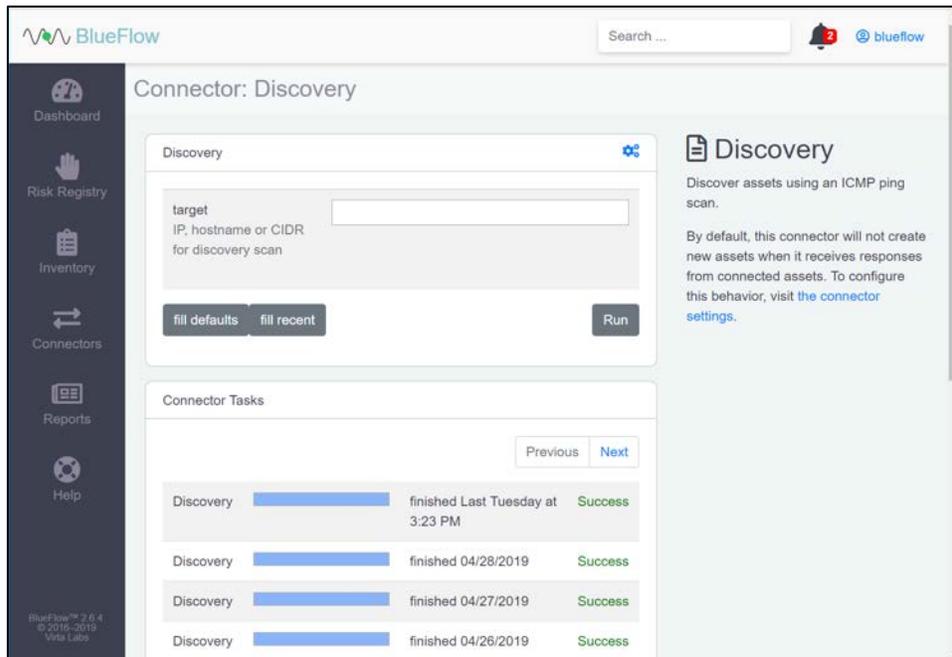
1016

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



1018

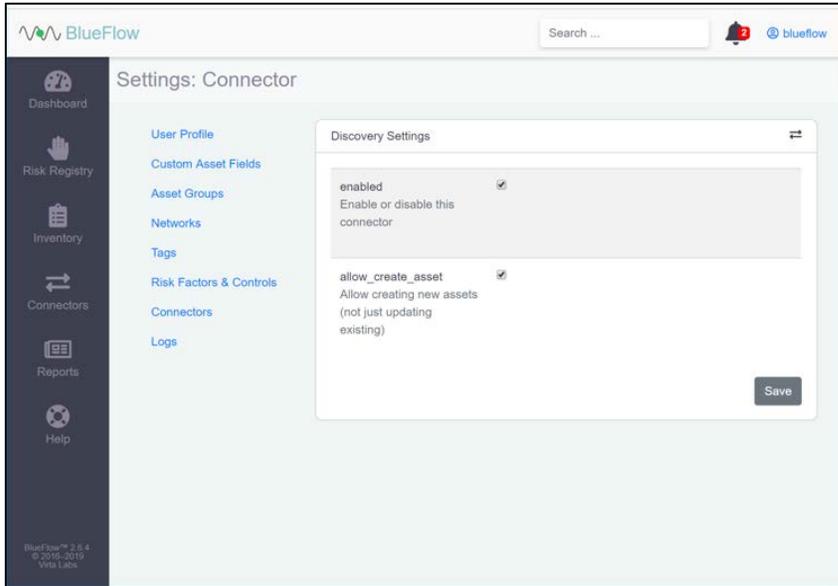
1019 3. Under **Discovery**, click the gear icon.



1020

1021 4. Check the box next to **allow_create_asset**.

1022 5. Click **Save**.

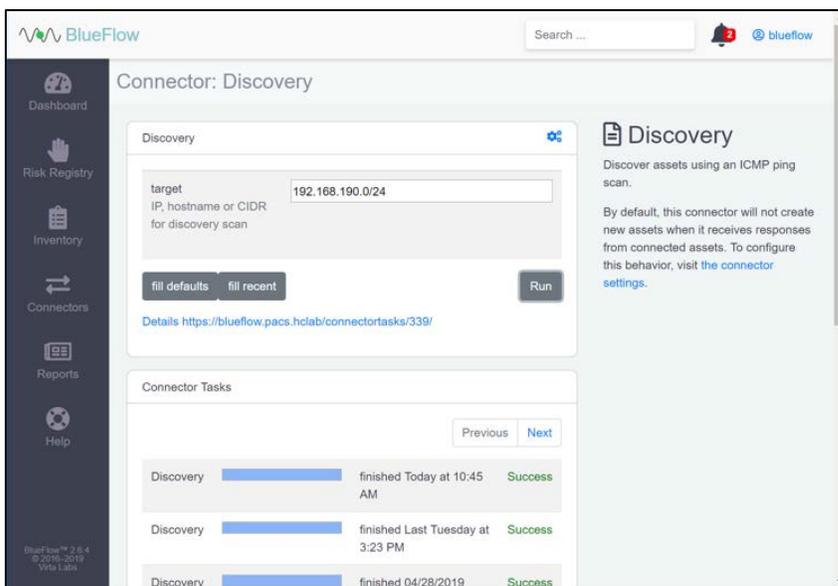


1023

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.



1027

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 were

1030 discovered within the provided network range.

The screenshot displays the BlueFlow web interface. On the left is a dark sidebar with navigation icons for Dashboard, Risk Registry, Inventory, Connectors, Reports, and Help. The main area is titled 'Connector Task' and shows a 'Discovery' scan that has completed successfully. A table lists the inputs, with 'target' set to '192.168.190.0/24'. Below this, a timeline shows the scan was submitted, started, and finished at 'Today at 10:45 AM', with a duration of 'a few seconds'. The 'Output' section shows a terminal window with the following text:

```
Running nmap ICMP scan on 192.168.190.0/24. This might take a while.
nmap -oX - -sn -PE 192.168.190.0/24
Version 6.40
Finished discovery scan
created      0
updated     0
up-to-date  7
skipped     0
duplicate   0
errored     0
-----
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

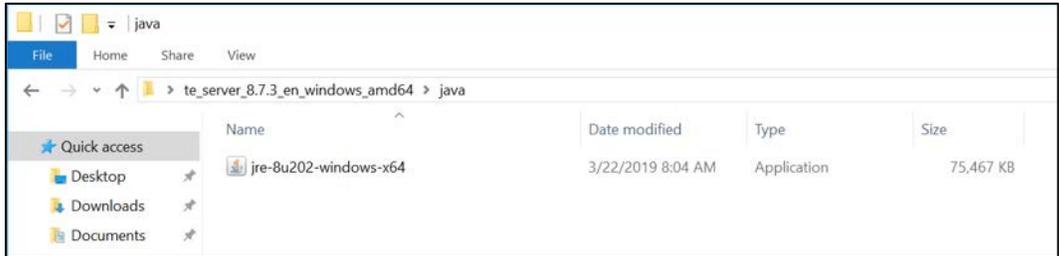
1039 **Storage:** 120 GB (Thin Provision)

1040 **Operating System:** Microsoft Windows Server 2016

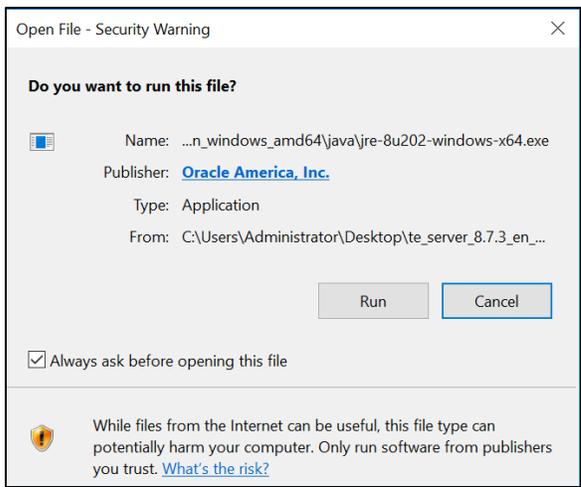
1041 **Network Adapter:** VLAN 1201

1042 **Tripwire Enterprise Console Installation**

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



1044
1045 2. Click on **Run**.

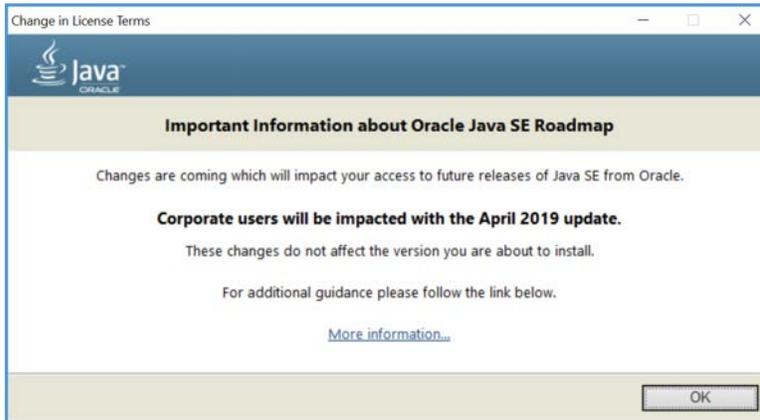


1046
1047 3. Click on **Install >**.



1048
1049 4. Click **OK**.

1050



1051 5. Wait for the install process to complete.

1052

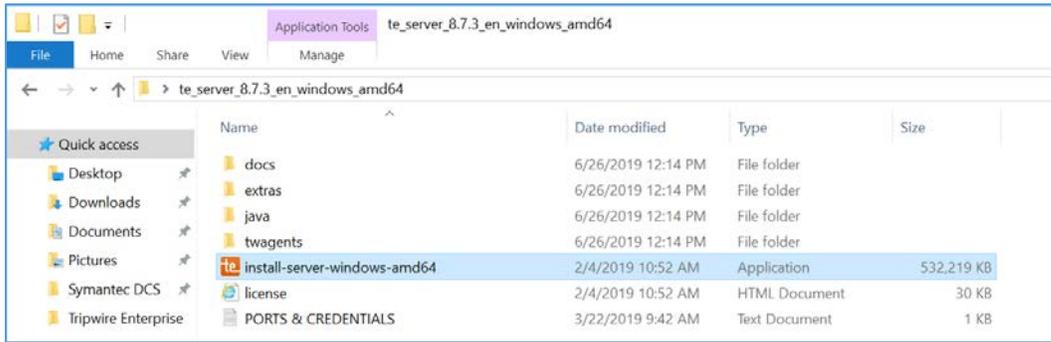


1053 6. Click Close.

1054



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

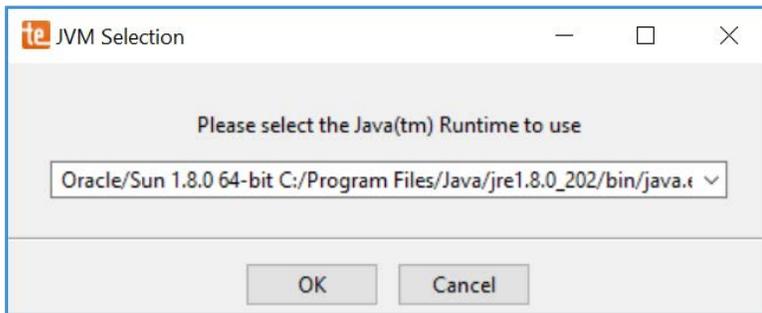


1056

1057

1058

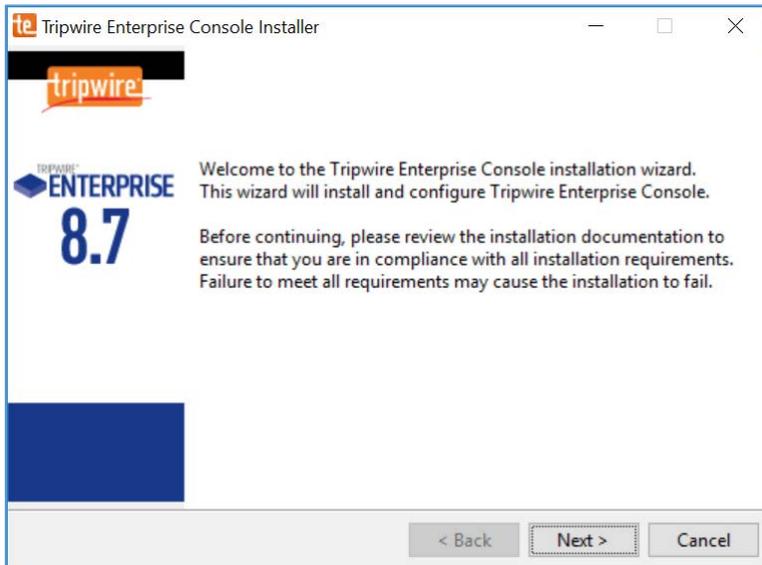
8. Select the version of *Java, Oracle/Sun 1.8.0 64-bit*, that was previously installed.
9. Click **OK**.



1059

1060

10. Click **Next >**.

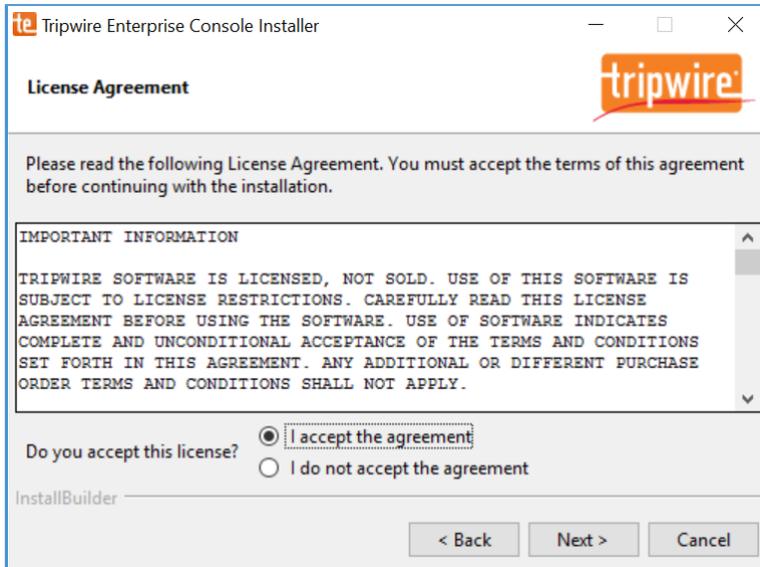


1061

1062

11. Check **I accept the agreement**.

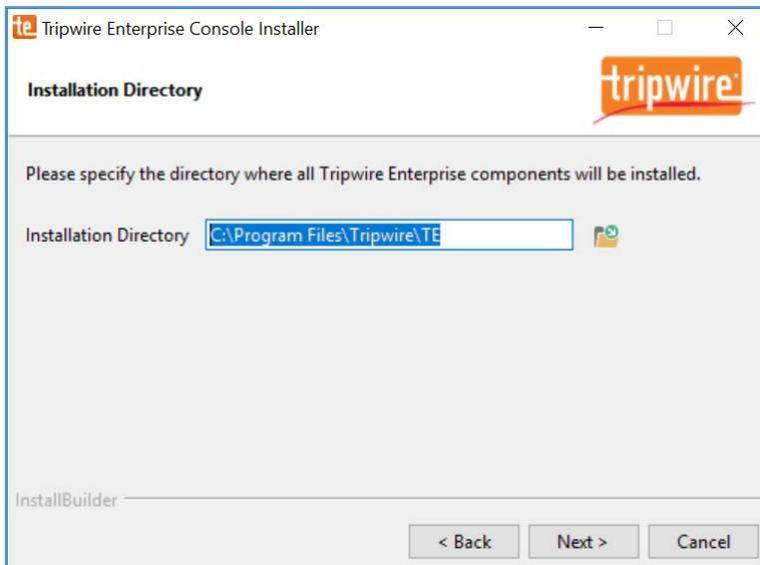
1063 12. Click **Next >**.



1064

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

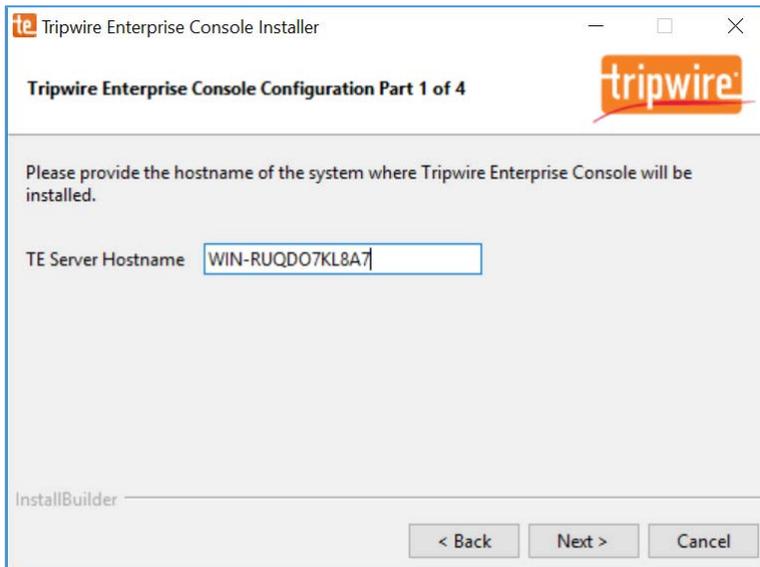
1066 14. Click **Next >**.



1067

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

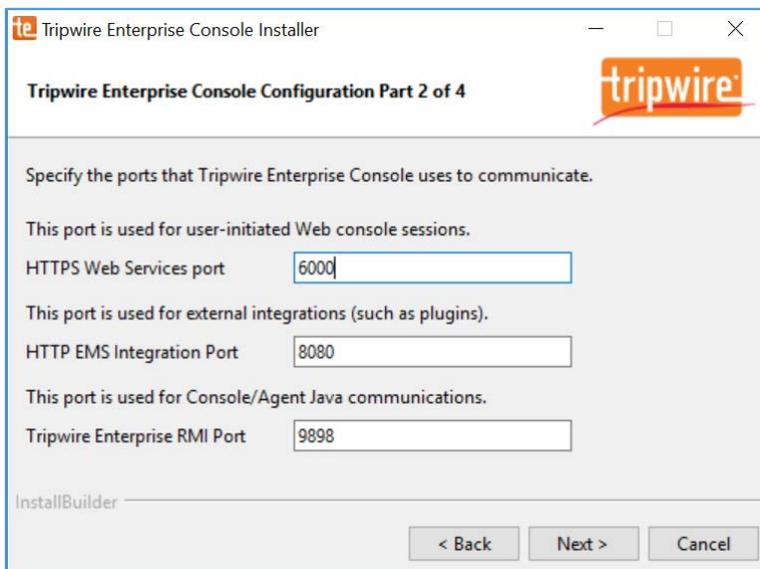
1070 16. Click **Next >**.



1071

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

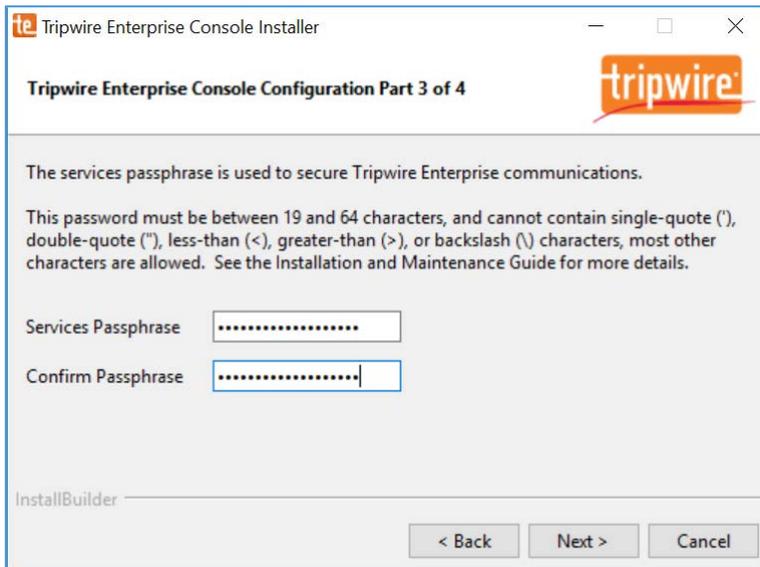
1074 18. Click **Next >**.



1075

1076 19. Create a password for Tripwire Enterprise services.

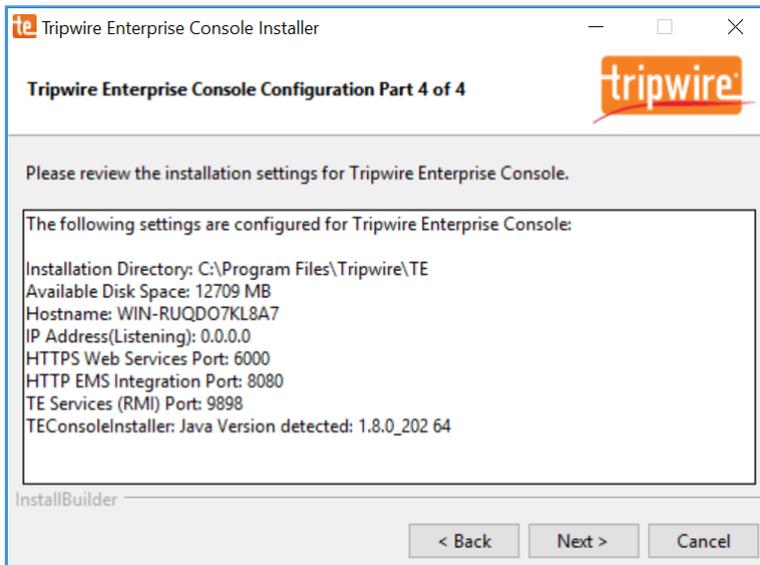
1077 20. Click **Next >**.



1078

1079 21. Verify planned installation settings are correct.

1080 22. Click **Next >**.

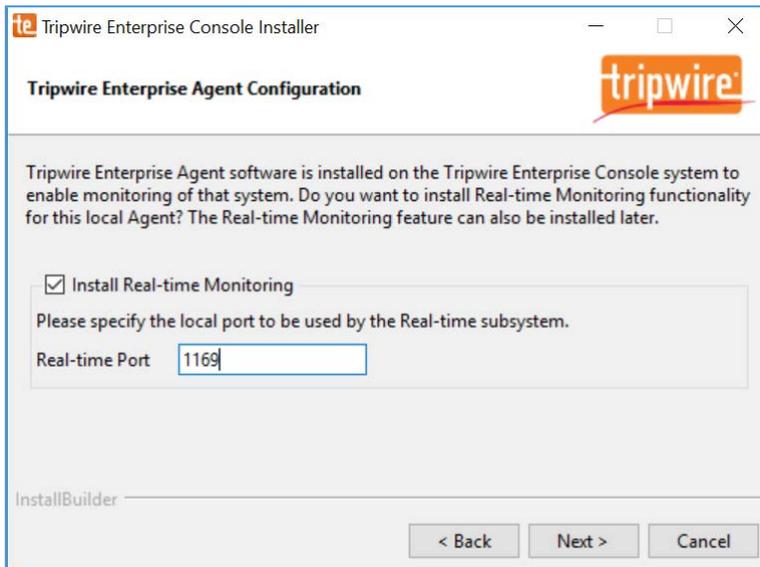


1081

1082 23. Check **Install Real-time Monitoring**.

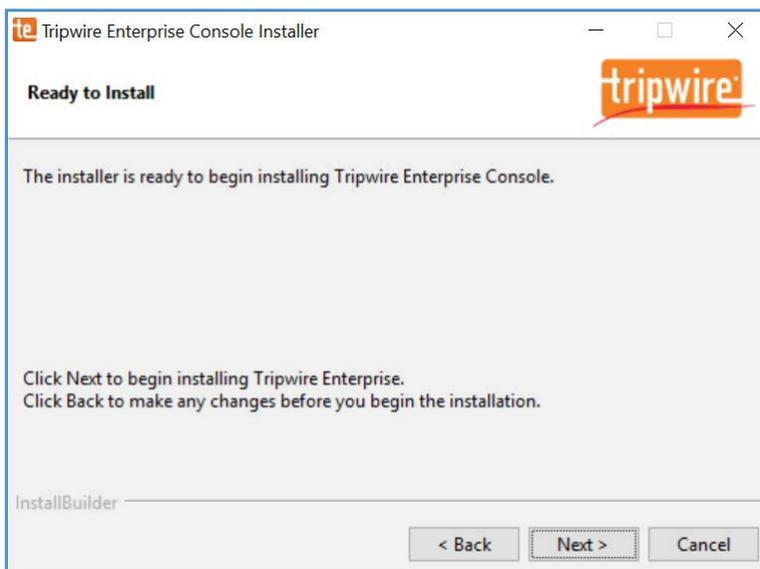
1083 24. Specify **Real-time Port** as **1169** for monitoring.

1084 25. Click **Next >**.



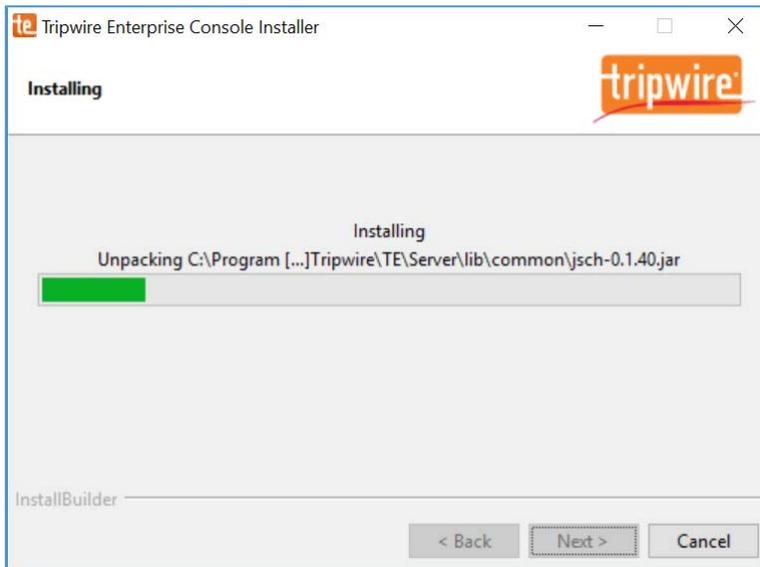
1085

1086 26. Click **Next >**.



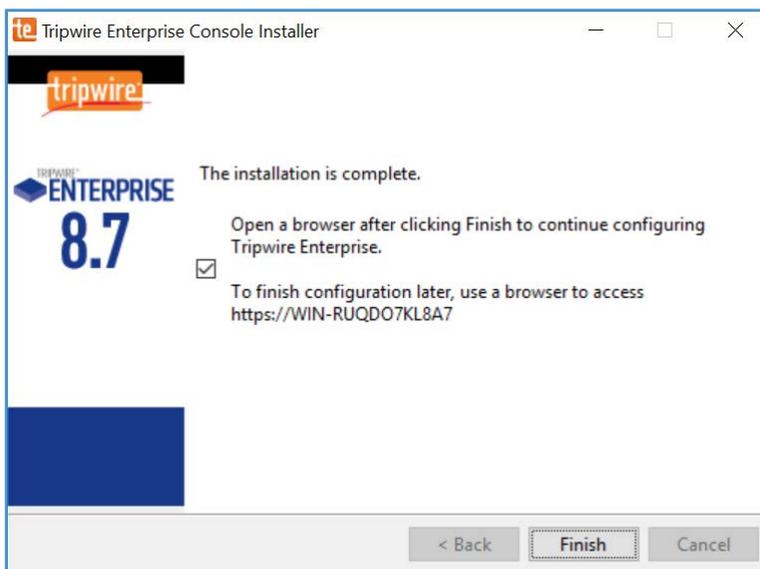
1087

1088 27. Wait for Tripwire Enterprise installation to complete.



1089

1090 28. Click **Finish**.

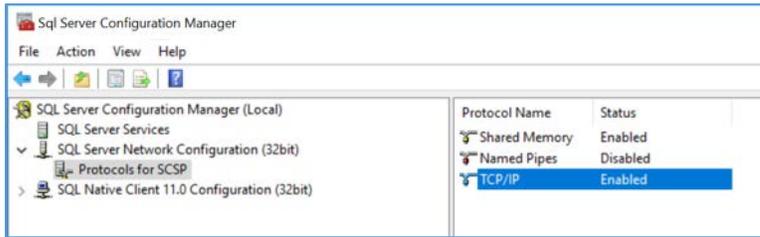


1091

1092 29. Open SQL Server Configuration Manger.

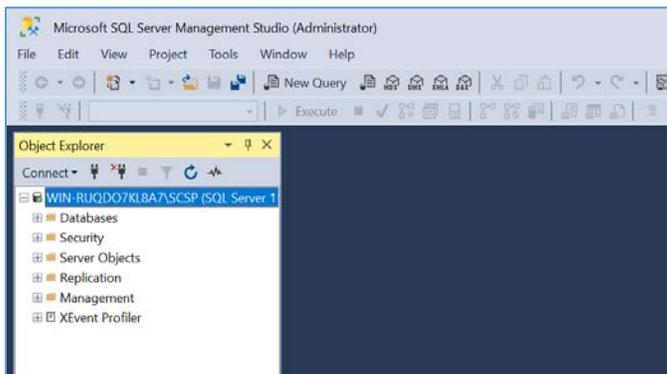
1093 30. Under **SQL Server Network Configuration > Protocols for SQL Server** ensure the **TCP/IP protocol** is
1094 set to **Enabled**.

DRAFT



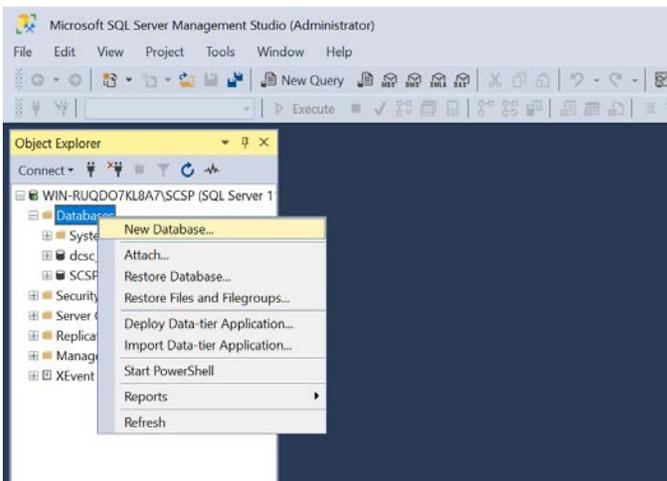
1095

1096 31. Open SQL Server Management Studio.



1097

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



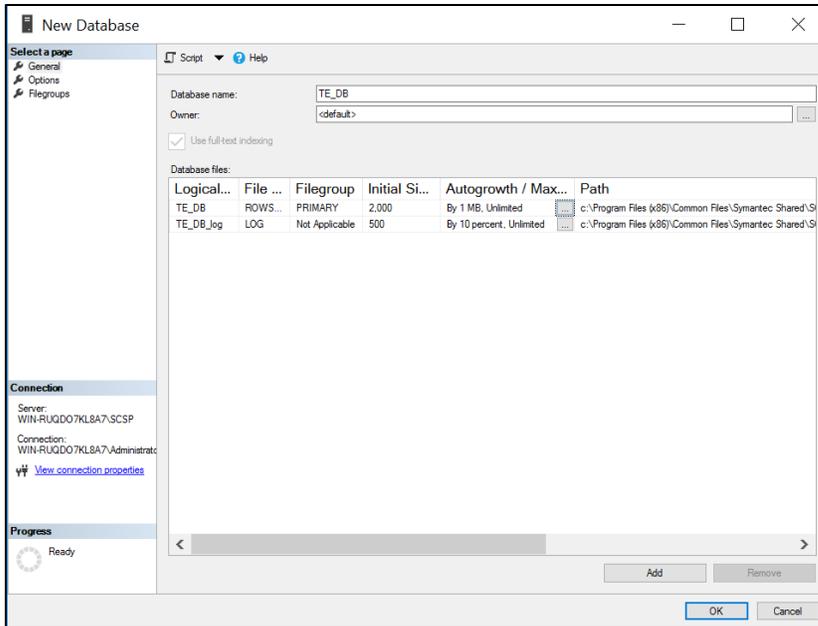
1100

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**.

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

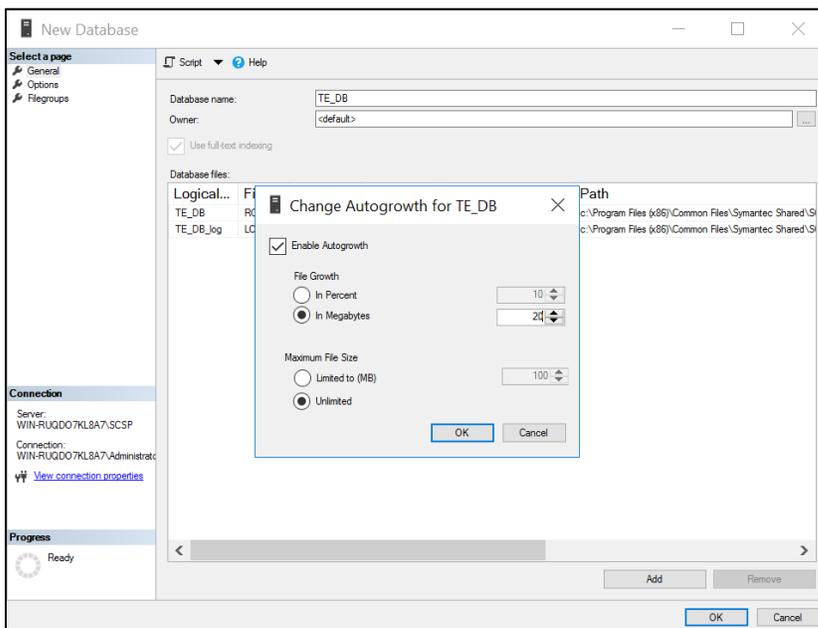


1105

1106 37. Check **Enable Autogrowth**, set **File Growth** to at least **20 MB**, and set **Maximum File Size** to **Unlimited**.

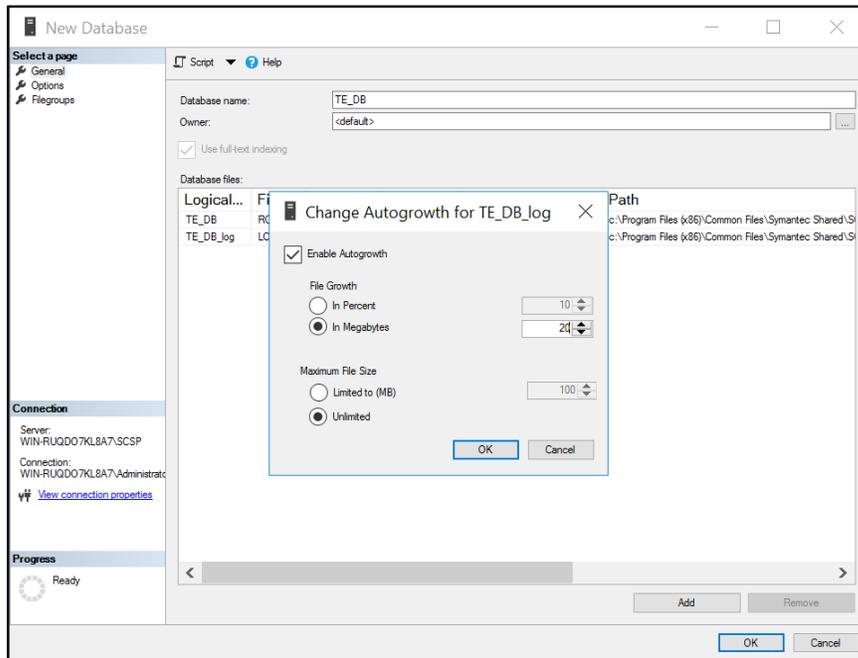
1107

1108 38. Click **OK**.

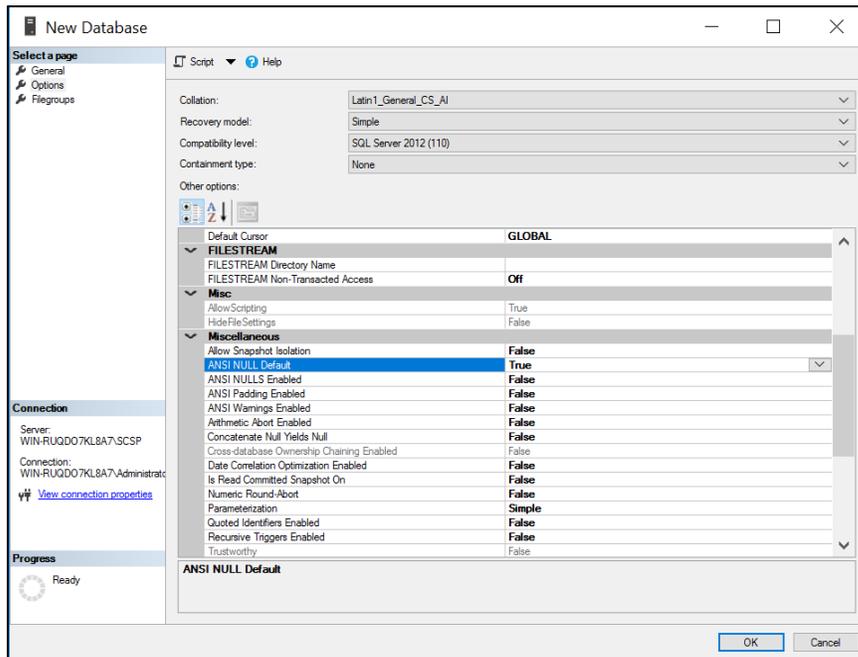


1109

- 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**.

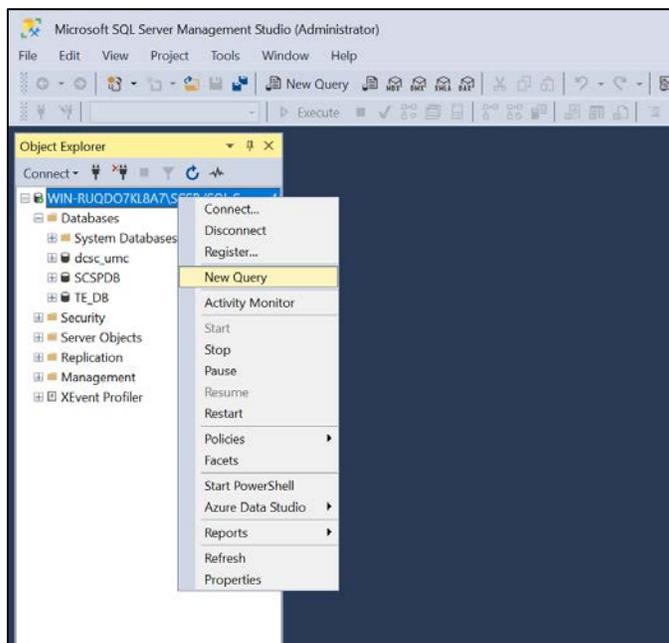


- 1115
- 1116 43. On the left, under **select a page**, select **Options**.
- 1117 44. Set **Collation** to **Latin1_General_CS_AI**.
- 1118 45. Set **Recovery model** to **Simple**.
- 1119 46. Under **Other Options > Miscellaneous** set **ANSI NULL Default** to **True**.
- 1120 47. Click **OK**.



1121

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



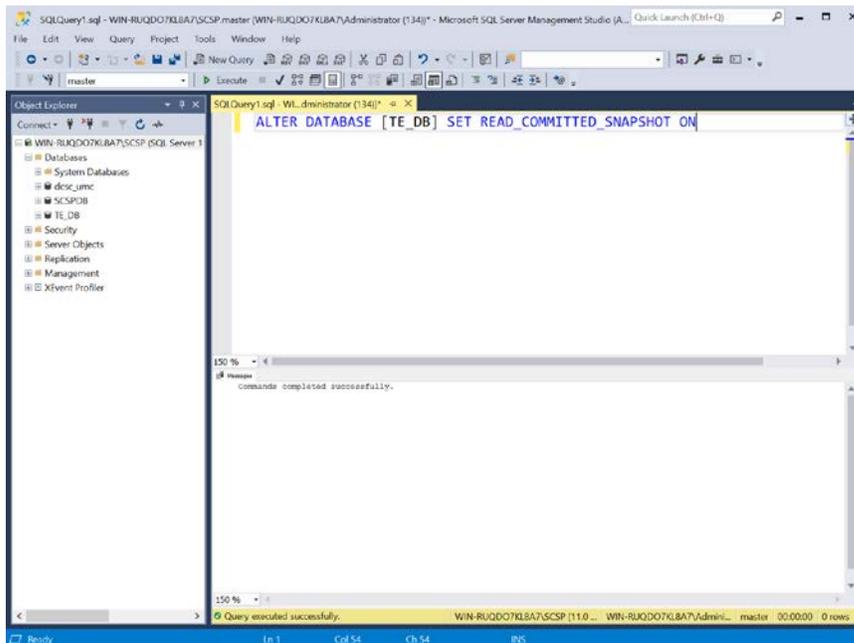
1123

1124 49. Type out the following query:

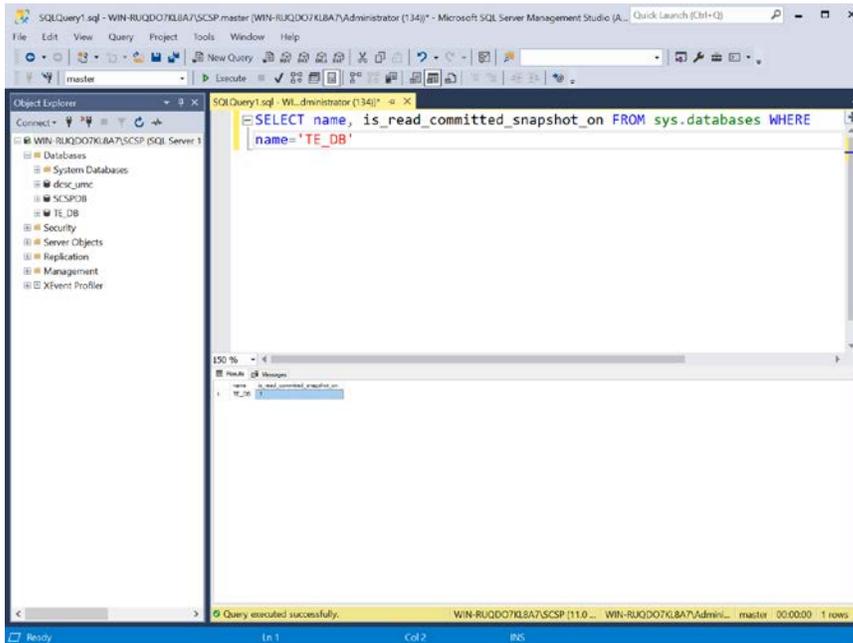
1125

```
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 completed
- 1128 successfully.



- 1129
- 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**.

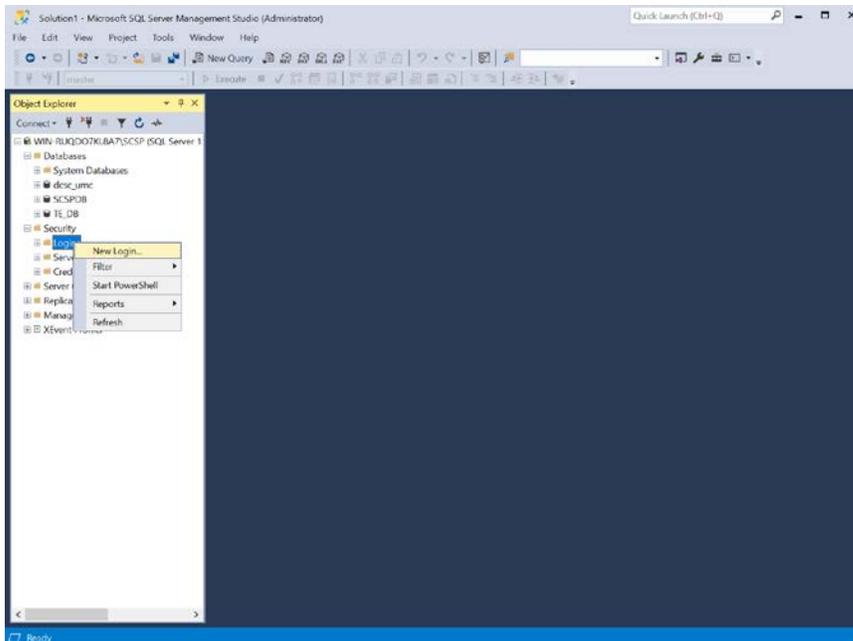


1136

1137

1138

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



1139

1140

1141

56. On the left, under **Select a page**, select **General**.

57. Create a **Login name**.

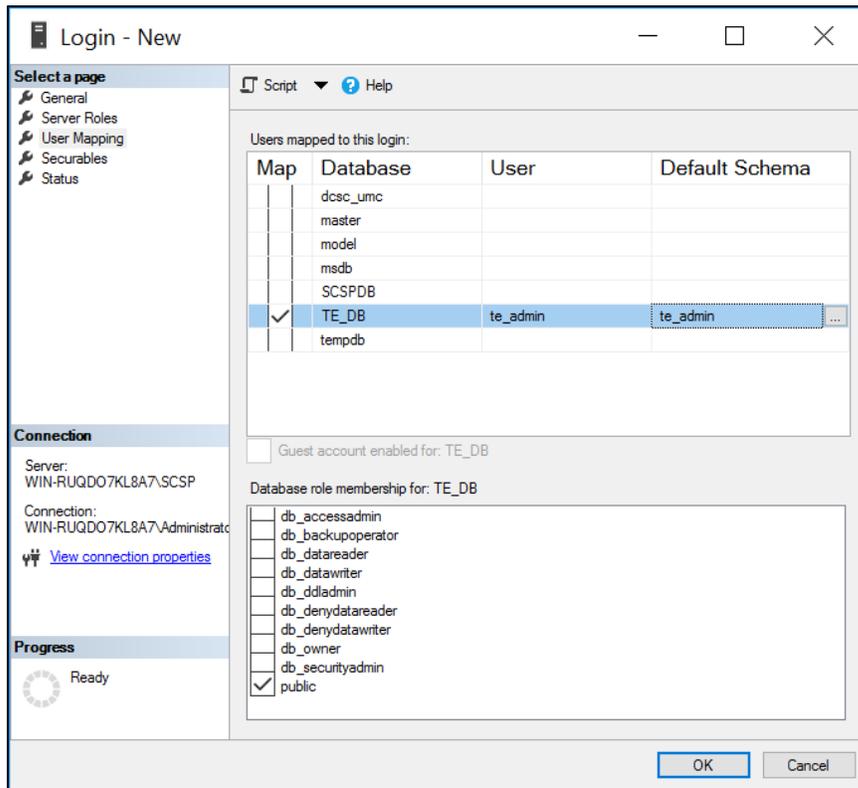
- 1142 58. Select **SQL Server authentication**.
- 1143 59. Create a **password**.
- 1144 60. For **Default database**, select the database previously created.
- 1145 61. For **Default language**, select **English**.

The screenshot shows the 'Login - New' dialog box with the following configuration:

- Select a page:** General, Server Roles, User Mapping, Securables, Status.
- Connection:** Server: WIN-RUQD07KL8A7\SCSP, Connection: WIN-RUQD07KL8A7\Administratc, [View connection properties](#)
- Progress:** Ready
- Login name:** te_admin
- Authentication:** SQL Server authentication, Windows authentication
- Passwords:** Password: [masked], Confirm password: [masked], Old password: [empty]
- Policy:** Enforce password policy, Enforce password expiration, User must change password at next login
- Mapping:** Mapped to certificate, Mapped to asymmetric key, Map to Credential
- Mapped Credentials Table:**

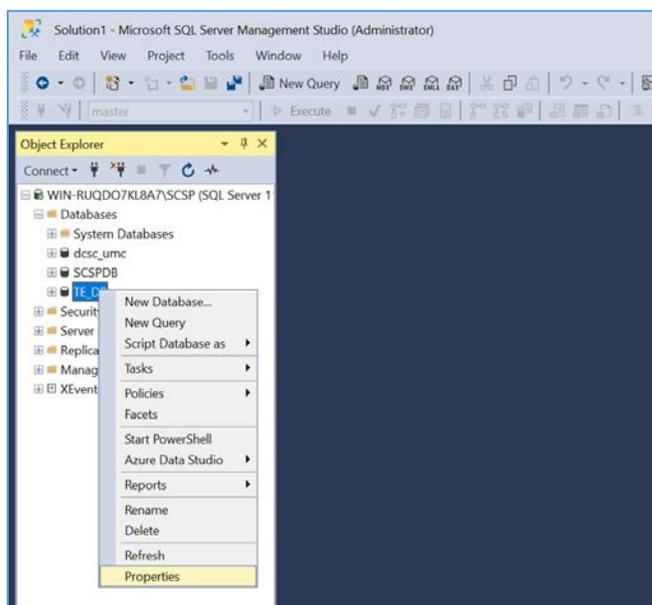
Credential	Provider
- Default database:** TE_DB
- Default language:** English
- Buttons:** OK, Cancel

- 1146
- 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 the
- 1149 previously created database:
- 1150 a. Check the box in the **Map** column.
- 1151 b. In the **Default Schema** column, type the name of the new user being created.
- 1152 64. Click **OK**.



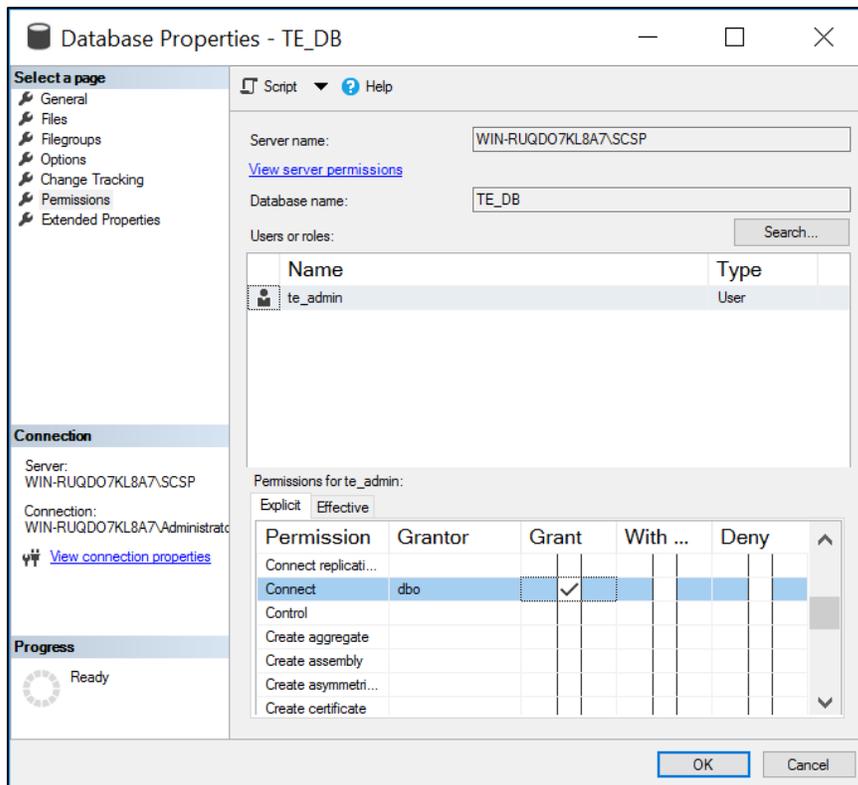
1153

- 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**.



1156

- 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**.

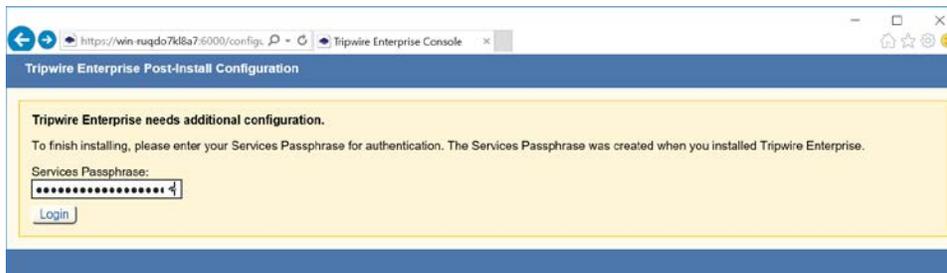


1169

1170 69. Open **Internet Explorer** and navigate to the webpage of the server on which Tripwire Enterprise
1171 was installed.

1172 70. Enter the **services password** created during the install process.

1173 71. Click **Login**.



1174

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

1179 ■ **Password:** *****

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

Tripwire Enterprise Post-Install Configuration

Database Configuration Settings

These settings control how the TE Console connects to a remote database that stores data for all TE operations. You can check the current configuration here, and make any necessary changes in the fields below.

Remote Database Type: <input type="text" value="Microsoft SQL Server"/>	Remote Database Type: The type of remote database used by TE.
<hr/>	
Authentication Type: <input type="text" value="SQL Server"/>	Authentication Type: Specifies whether the database login should authenticate using a Windows account (typically of the format domain\user), or an SQL Server account (an account defined only in SQL Server). With the Windows authentication type, NTLMv2 should be used, as it is cryptographically superior to the first version of NTLM. However, as NTLMv2 is configured in the operating system, not in the database or application, TE can be used with NTLM to ensure compatibility.
Login Name: <input type="text" value="te_admin"/>	Login Name: The login name that TE will use to authenticate with the database.
Password: <input type="password" value="••••••••"/>	Password: The password that TE will use to authenticate with the database.
Database Host: <input type="text" value="WIN-RUQDO7KL8A7"/>	Database Host: The fully qualified domain name, hostname or IP address of the system where the database is installed.
Port (default 1433): <input type="text" value="(UDP 1434)"/>	Port: The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.
Database Name: <input type="text" value="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): <input type="text" value="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: <input type="text" value="Request"/>	SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL.

1185

1186 73. Click **Test Database Login** and verify the connection is successful.1187 74. Click **Save Configuration and Restart Console**.

Login Name: **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: **Database Host:** The fully qualified domain name, hostname or IP address of the system where the database is installed.

Port (default 1433): **Port:** The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.

Database Name: **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): **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 SSL.

- Request - SSL will be used if available.
- Require - SSL will always be used, and an error will occur if SSL is not available for the database.
- 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.
- Off - SSL will never be used. This setting is not recommended.

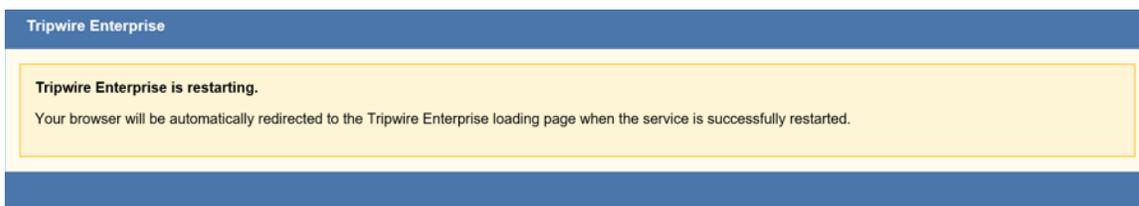
✓

Test Results:

Tripwire Enterprise 8.7.3.b8.7.3.r2019011122005-03196dc.b24

1188

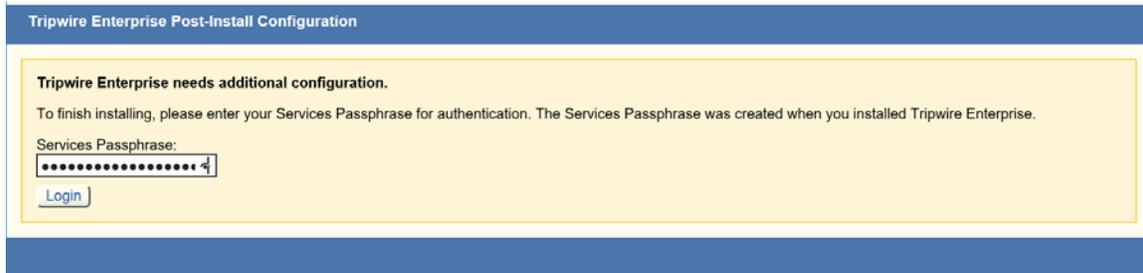
1189 75. Wait for Tripwire Enterprise to restart and redirect you to the log in page.



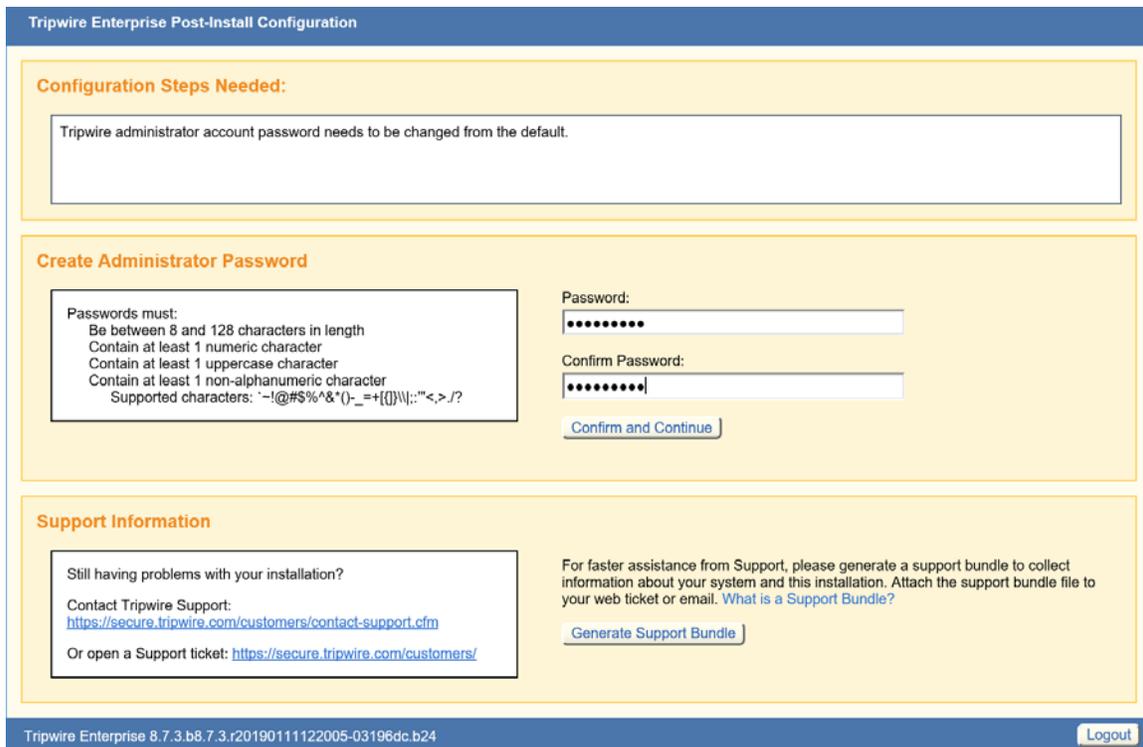
1190

1191 76. Enter the **services password** created during the install process.

1192 77. Click **Login**.



- 1193
- 1194 78. Under **Create Administrator Password**, create a password for the Tripwire Enterprise administrator
- 1195 account.
- 1196 79. Click **Confirm and Continue**.



- 1197
- 1198 80. Enter the **username** and **password** for the Tripwire Enterprise administrator account.
- 1199 81. Click **Sign In**.



1200

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

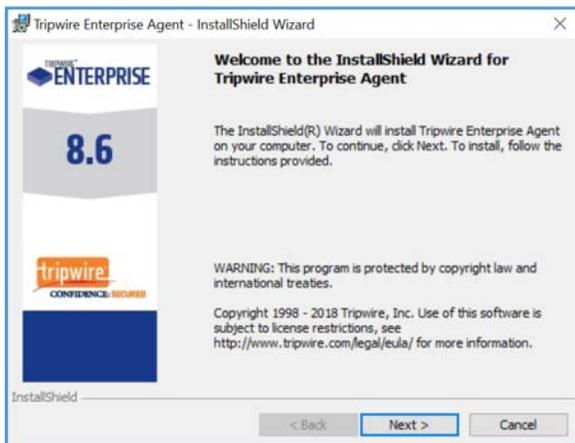


1202

1203 Tripwire Enterprise Agent Installation

1204 1. Run `te_agent.msi`.

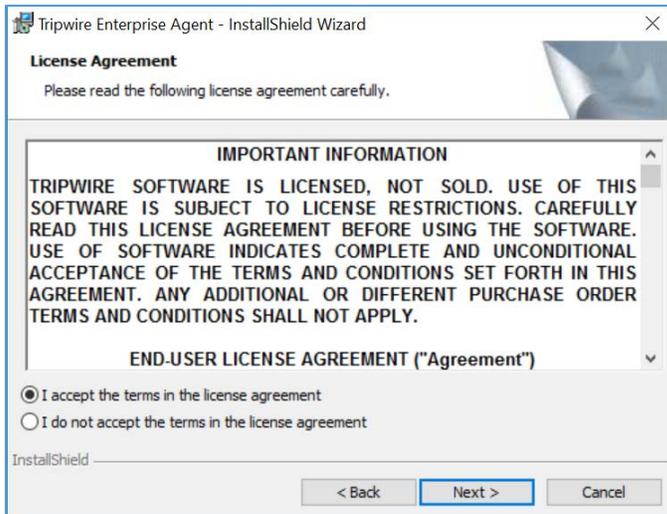
1205 2. Click **Next >**.



1206

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

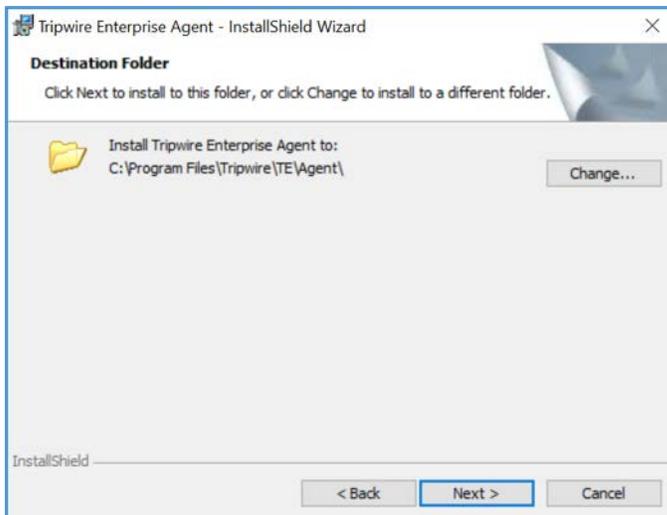
1208 4. Click **Next >**.



1209

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.

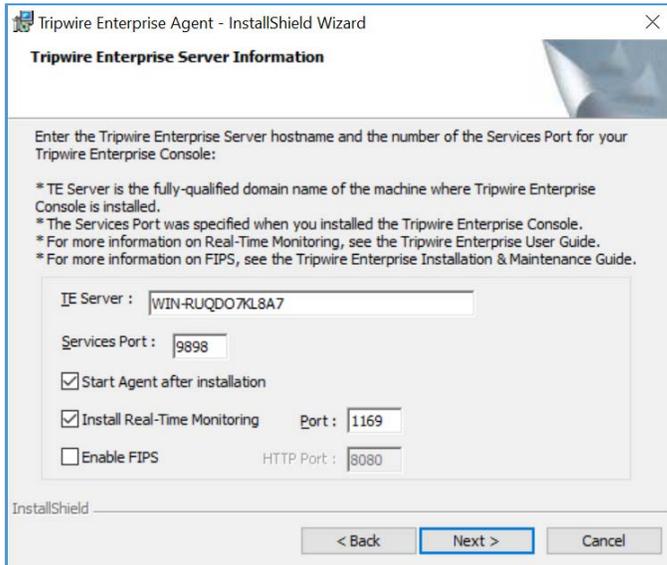
1214 8. Enter **9898** as the **Services Port** established during the installation process of Tripwire Enterprise.

1215 9. Check **Start Agent**, after installation.

1216 10. Check **Install Real-Time Monitoring** and specify a **Monitoring Port**.

1217 11. Uncheck **Enable FIPS**.

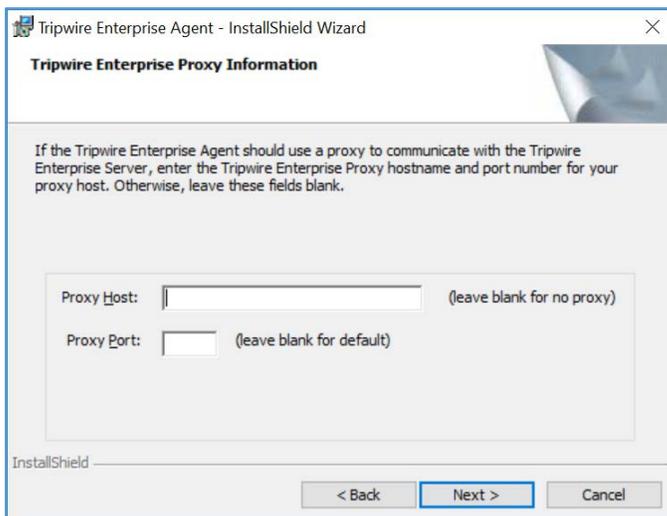
1218 12. Click **Next >**.



1219

1220 13. Specify a **Proxy Host** and **Proxy Port** if necessary.

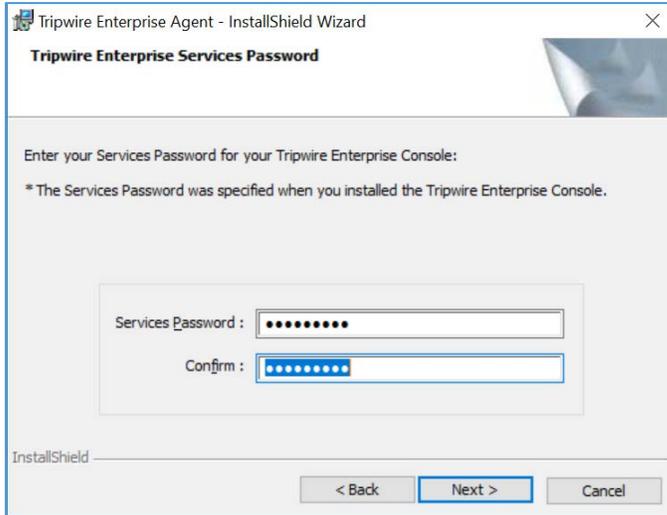
1221 14. Click **Next >**.



1222

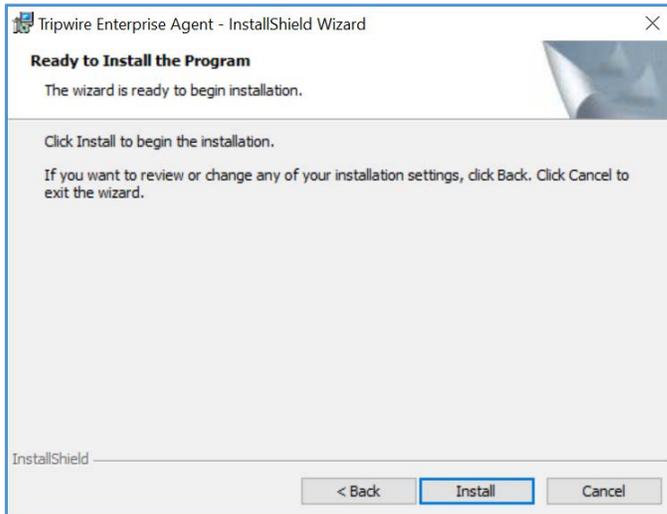
1223 15. Enter the **Services Password** created during the installation process for Tripwire Enterprise.

1224 16. Click **Next >**.



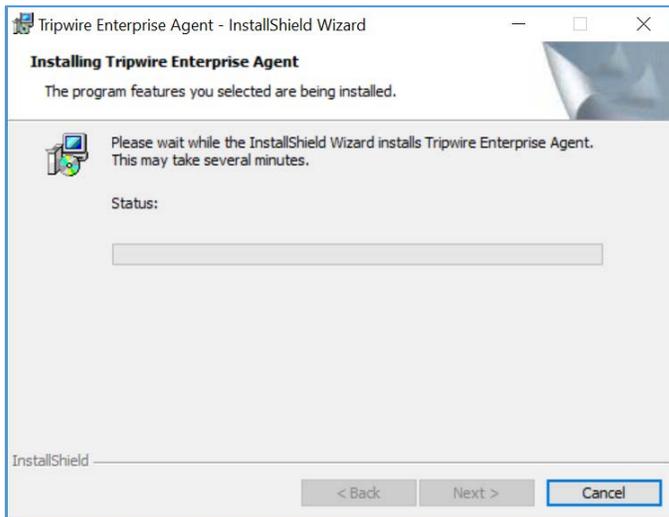
1225

1226 17. Click **Install**.



1227

1228 18. Wait for the installation process to complete.



1229

1230 19. Click **Finish**.



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
1235 AD, DNS, and Dynamic Host Configuration Protocol (DHCP) services for the enterprise. The following
1236 section details how the services were installed.

1237 **System Requirements**

DRAFT

1238 **CPU:** 1

1239 **Memory:** 4 GB Ram

1240 **Storage:** 120 GB (Thin Provision)

1241 **Operating System:** Microsoft Windows Server 2012 R2

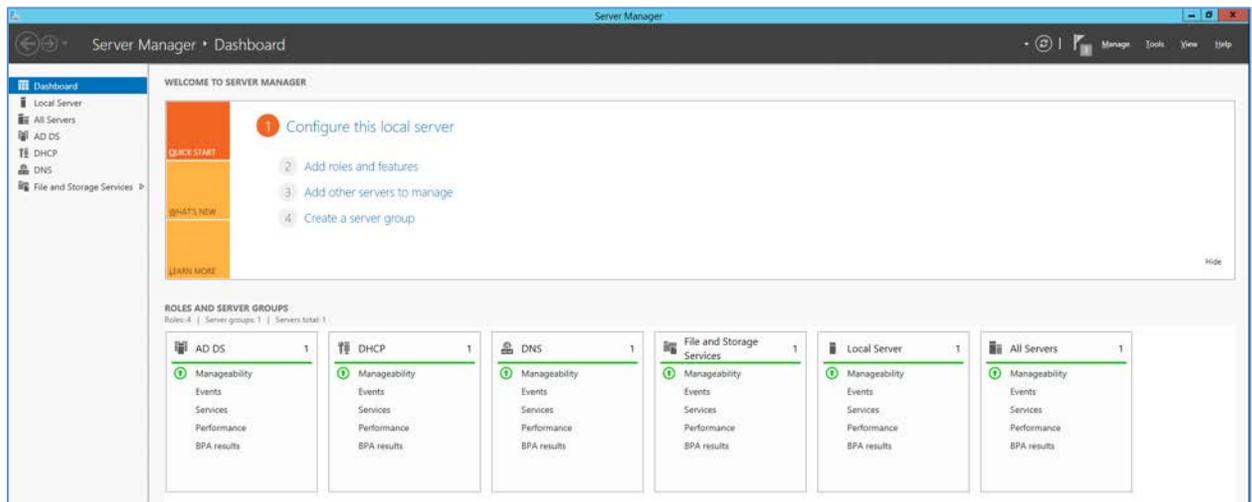
1242 **Network Adapter:** VLAN 1201

1243 **Enterprise Domain Services Installation**

1244 Install the Domain Controller, AD, and DNS appliances according to the instructions detailed in *Building Your First Domain Controller on 2012 R2* [12].

1246 **DNS Server Forward Lookup Zone Configuration**

1247 1. Open **Server Manager**.

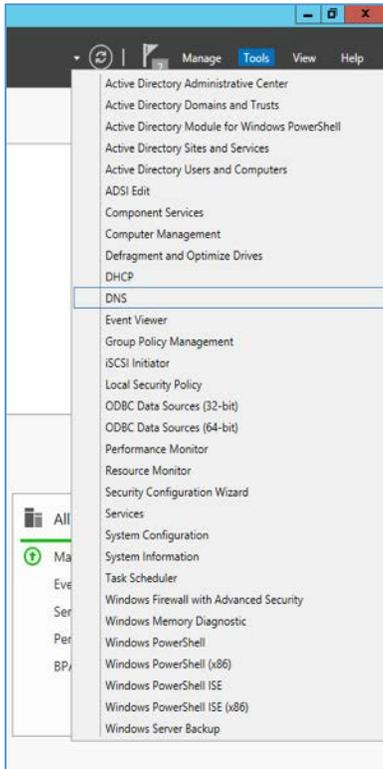


1248

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

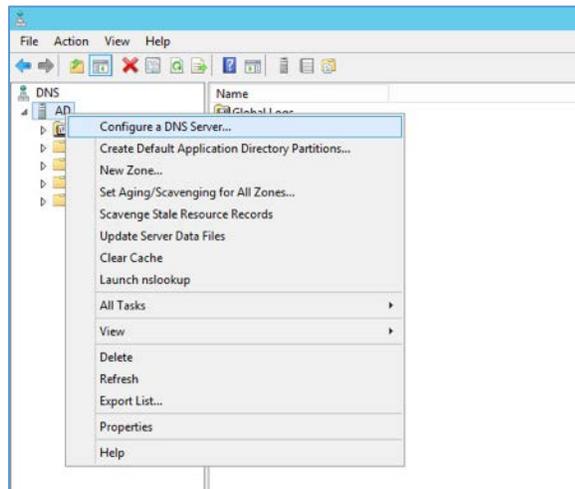
1251 performed previously. If not, follow these instructions:



1252

1253

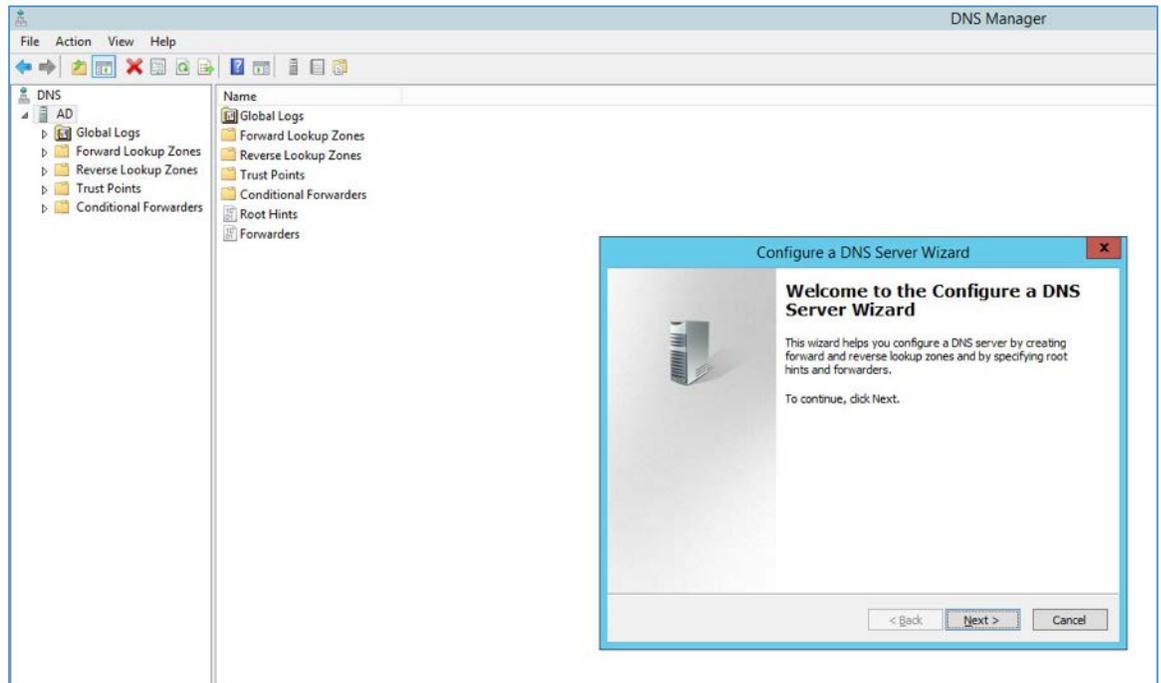
a. Right click on your server's name, and select **Configure a DNS Server...**



1254

1255

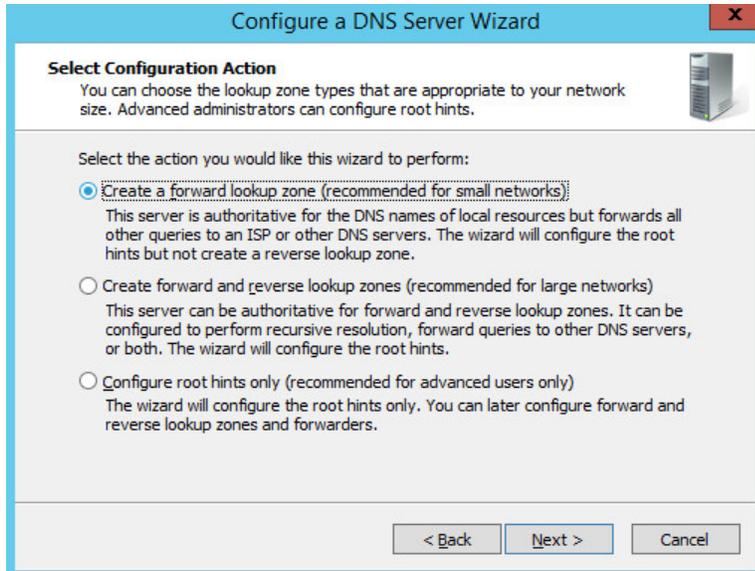
b. Click **Next >**.



1256

1257

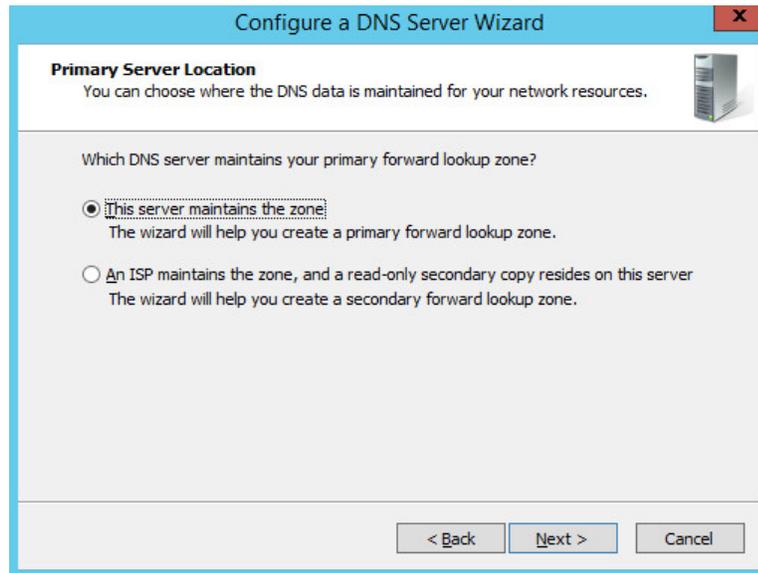
c. Click **Next >**.



1258

1259

d. Click **Next >**.



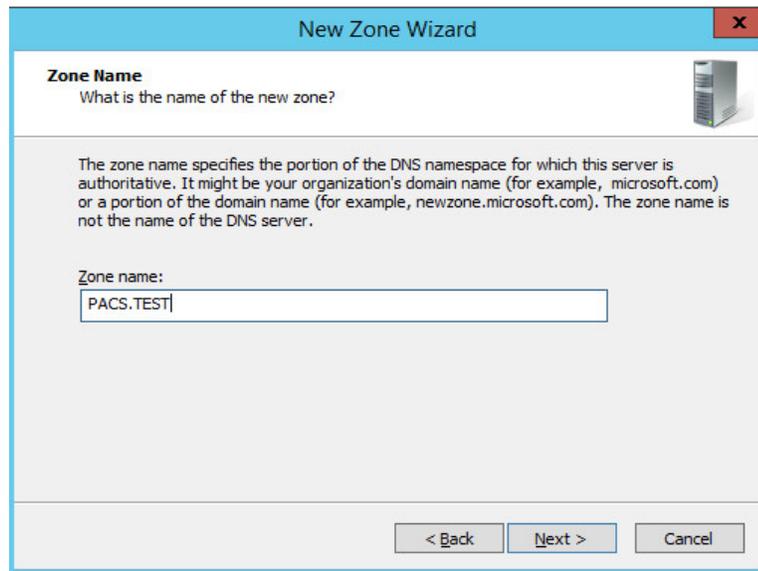
1260

1261

e. Enter **PACS.TEST** as the **Zone name**, that was established previously during setup.

1262

f. Click **Next >**.



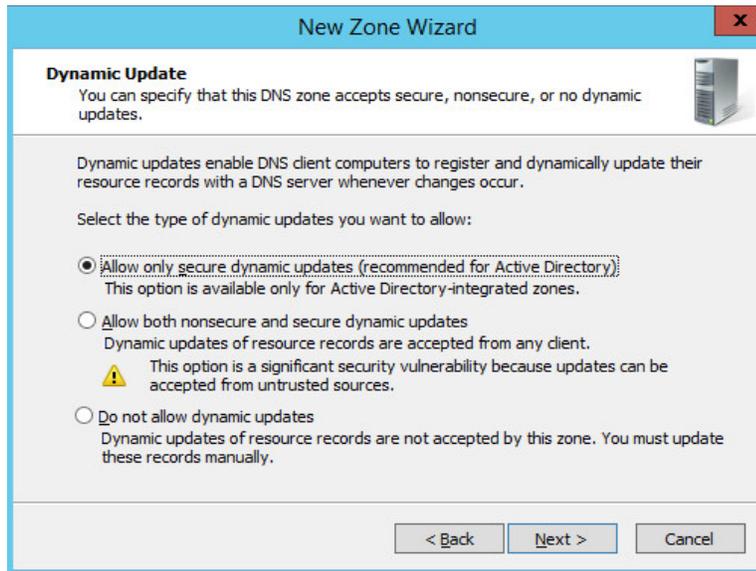
1263

1264

g. Select **Allow only secure dynamic updates**.

1265

h. Click **Next >**.



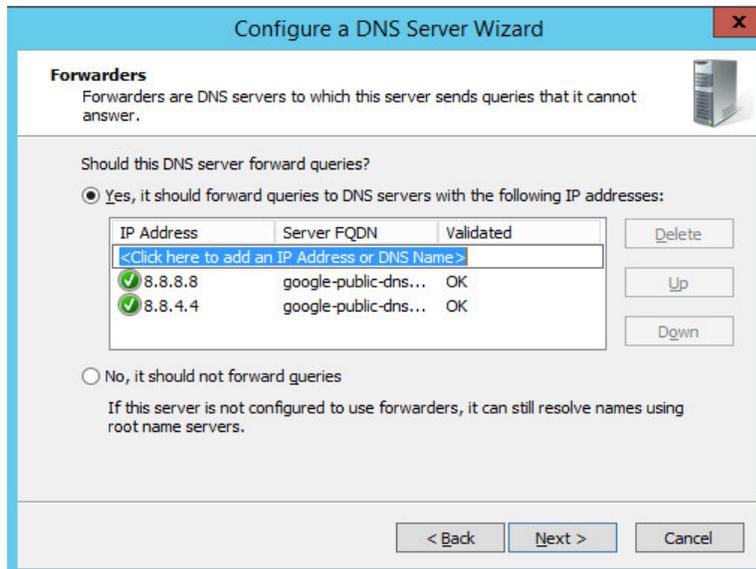
1266

1267

i. Add **Forwarders** (8.8.8.8 and 8.8.4.4 are Google’s DNS servers).

1268

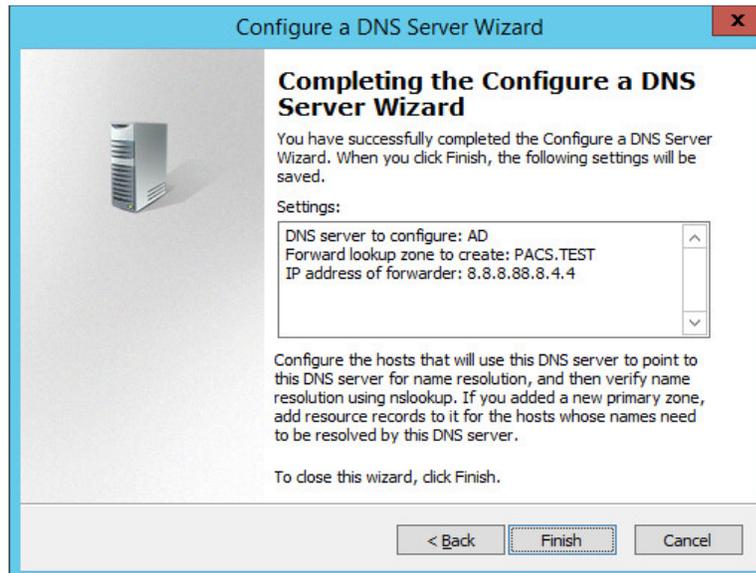
j. Click **Next >**.



1269

1270

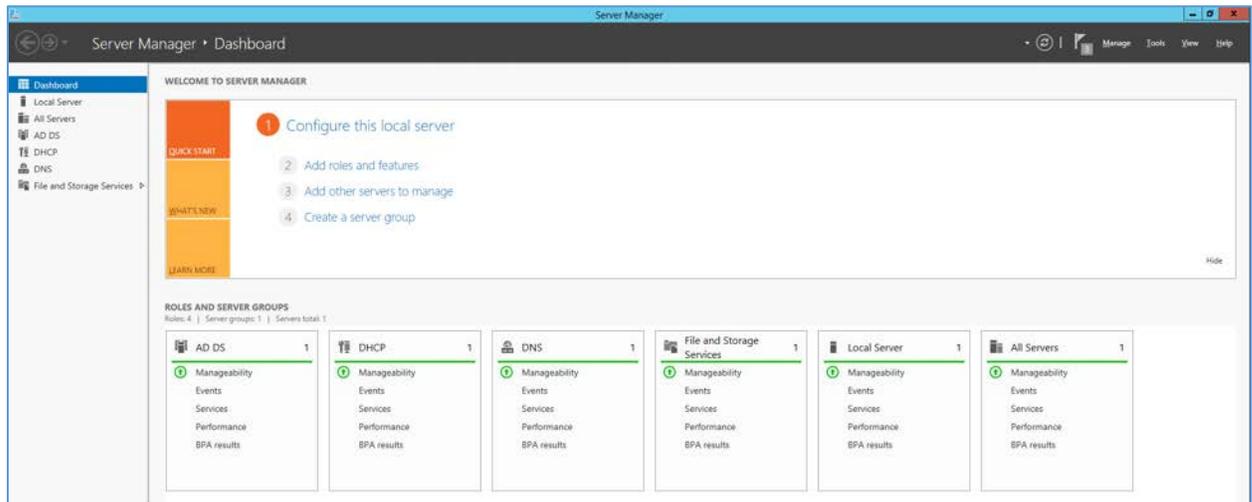
k. Click **Finish**.



1271

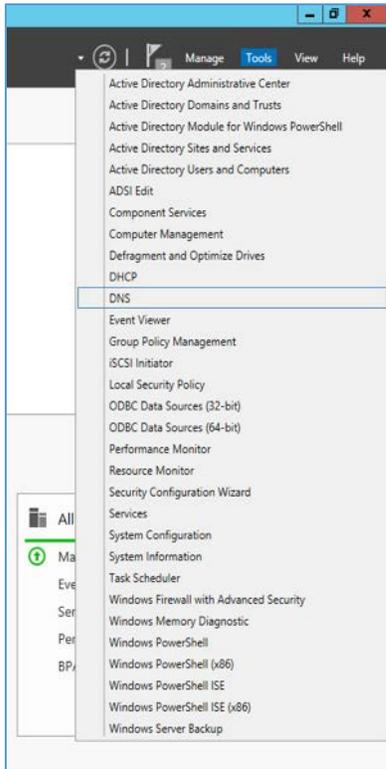
1272 **DNS Server Reverse Lookup Zone Configuration**

- 1273 1. Open **Server Manager**.



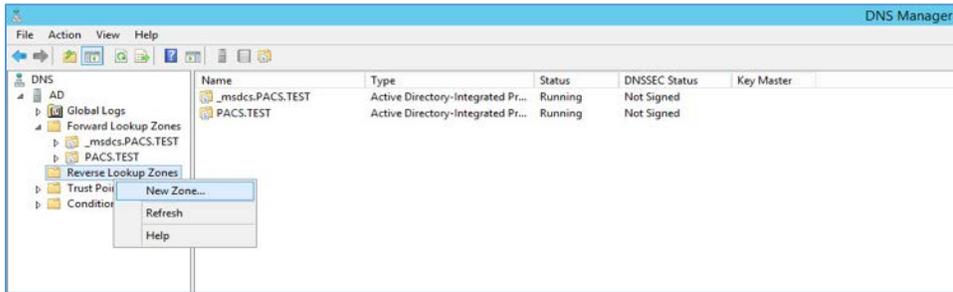
1274

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



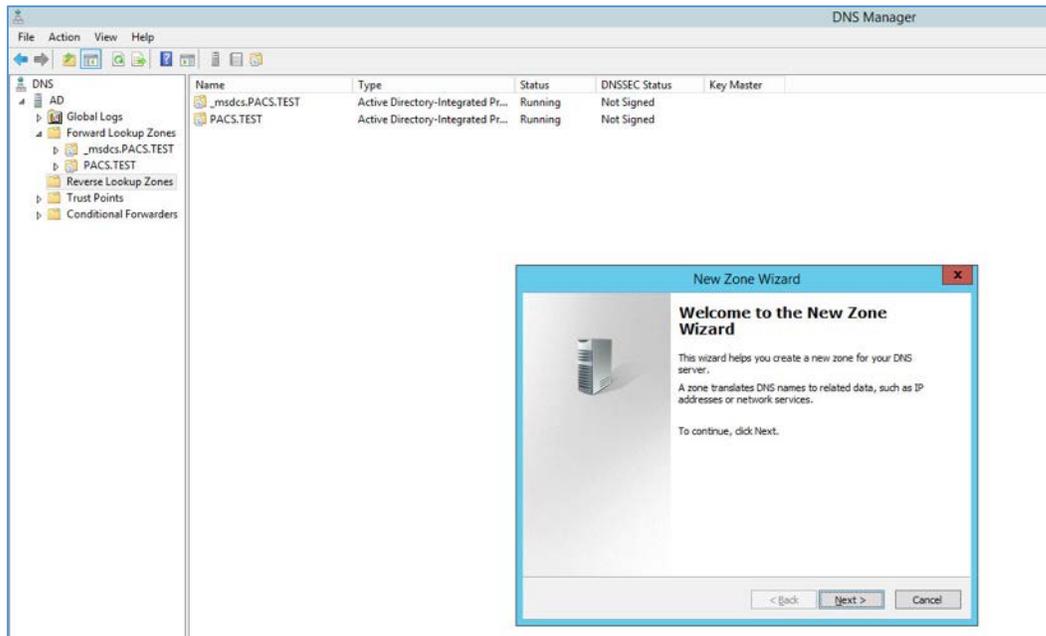
1276

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



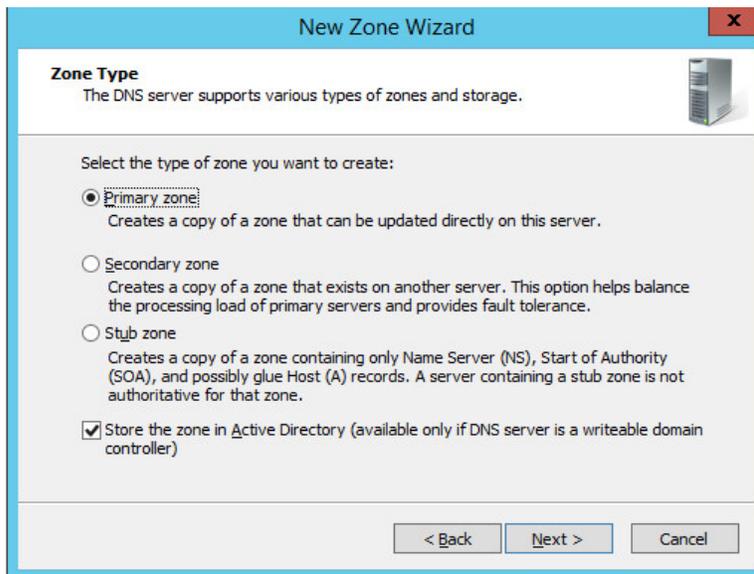
1278

1279 4. Click **Next >**.



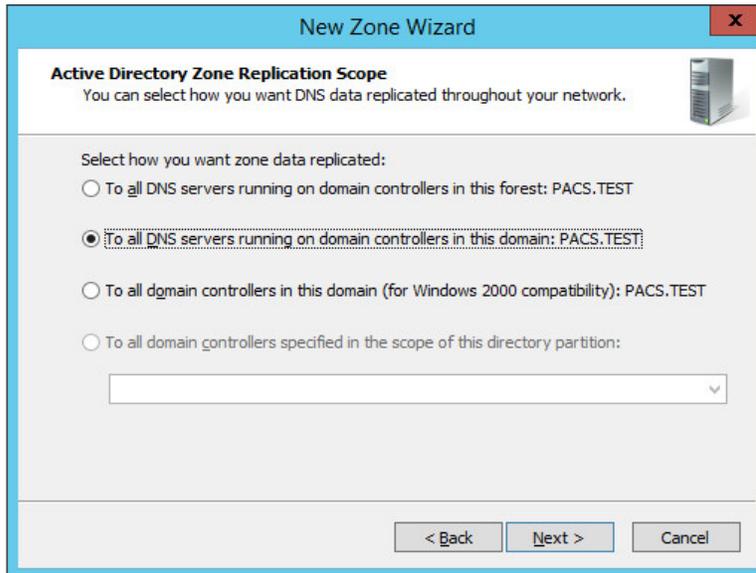
1280

1281 5. Click **Next >**.



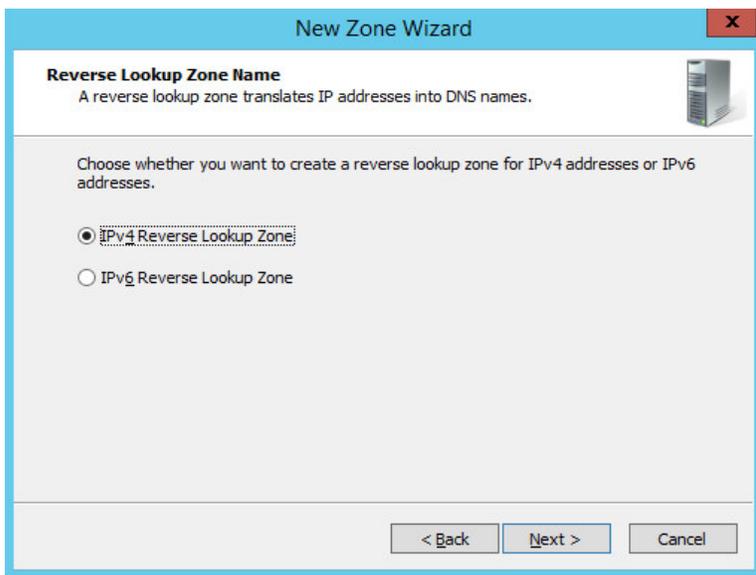
1282

1283 6. Click **Next >**.



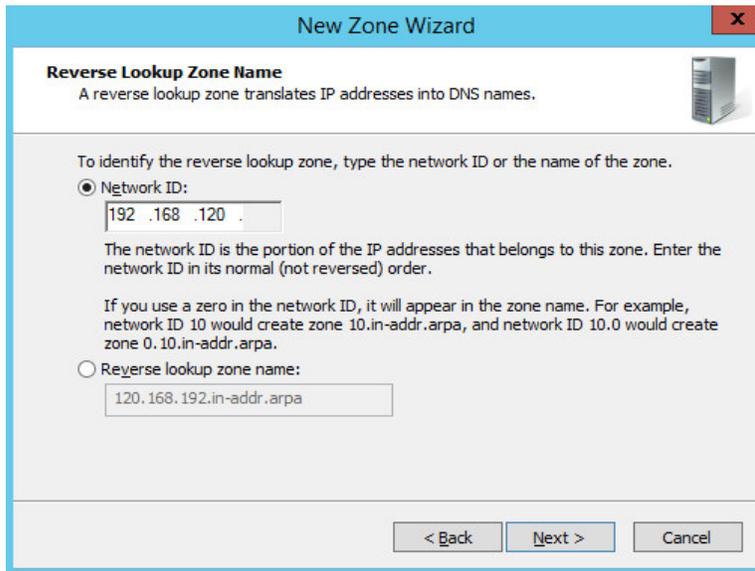
1284

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



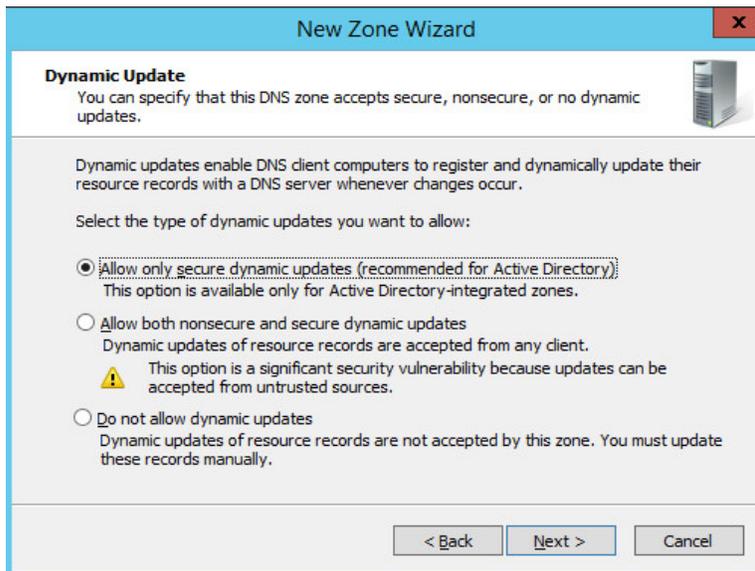
1286

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 >**.



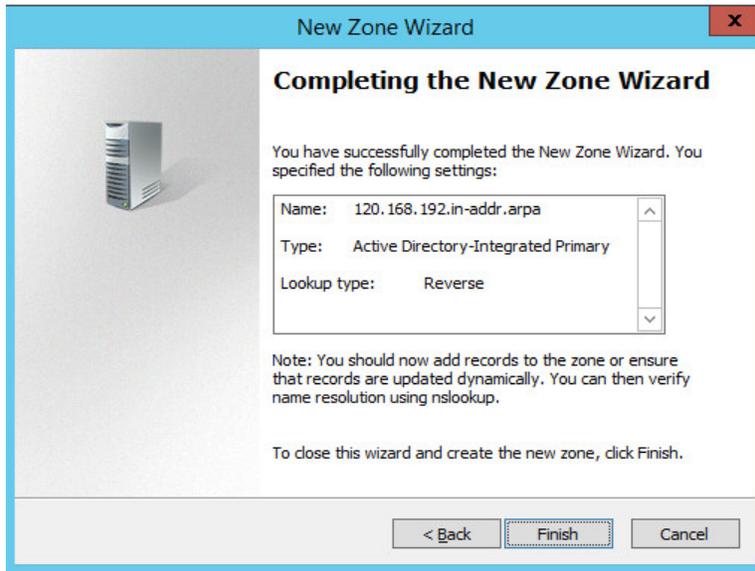
1289

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



1292

- 1293 10. Click **Finish**.



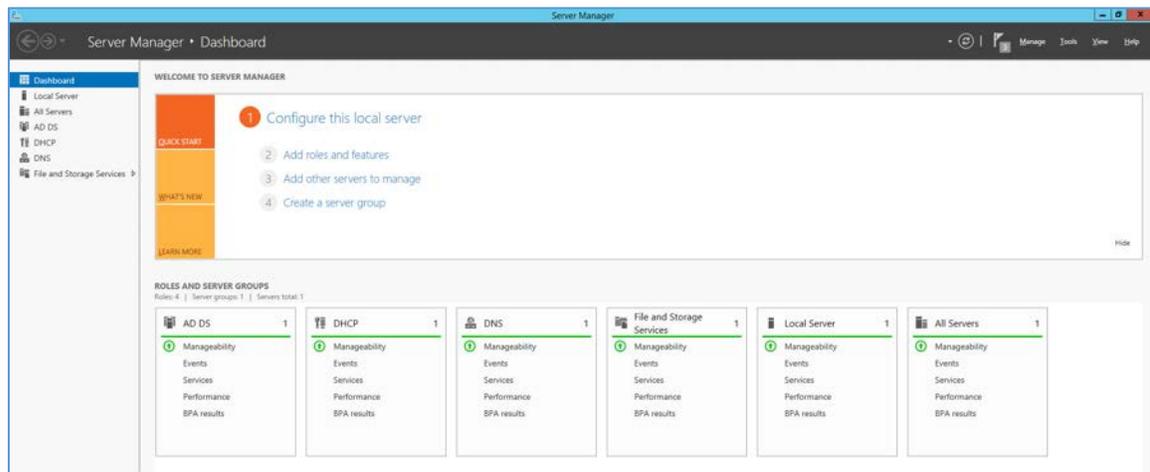
1294

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].

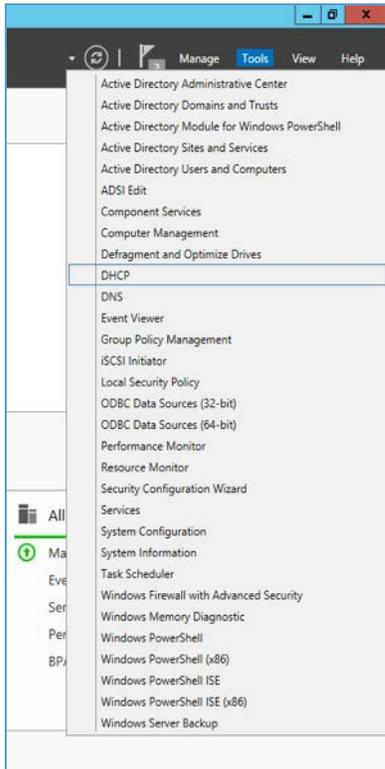
1298 **DHCP Server Configuration**

1299 1. Open **Server Manager**.



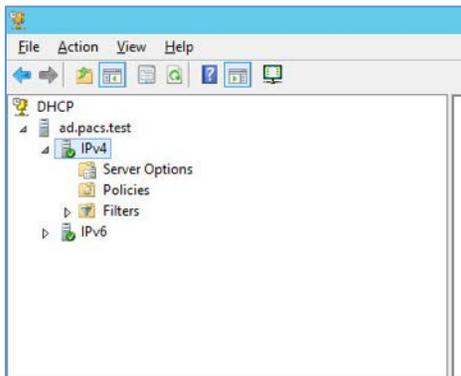
1300

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



1302

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

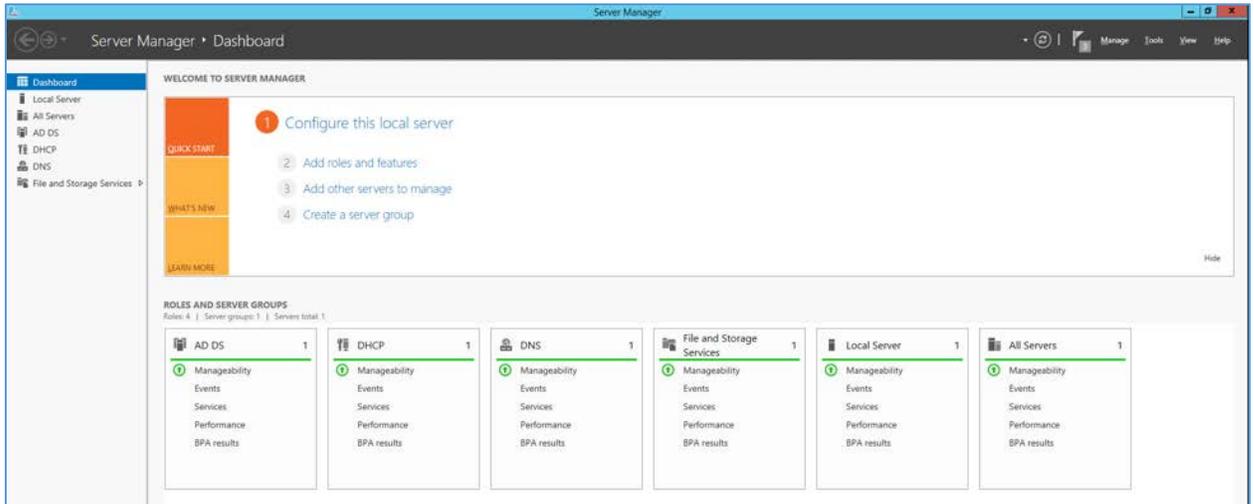


1304

1305 DHCP Scopes Configuration

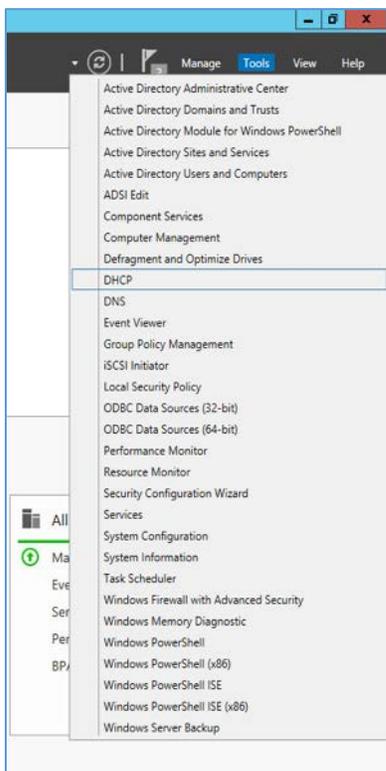
1306 *Performed on Windows Server 2012 R2.*

1307 1. Open **Server Manager**.



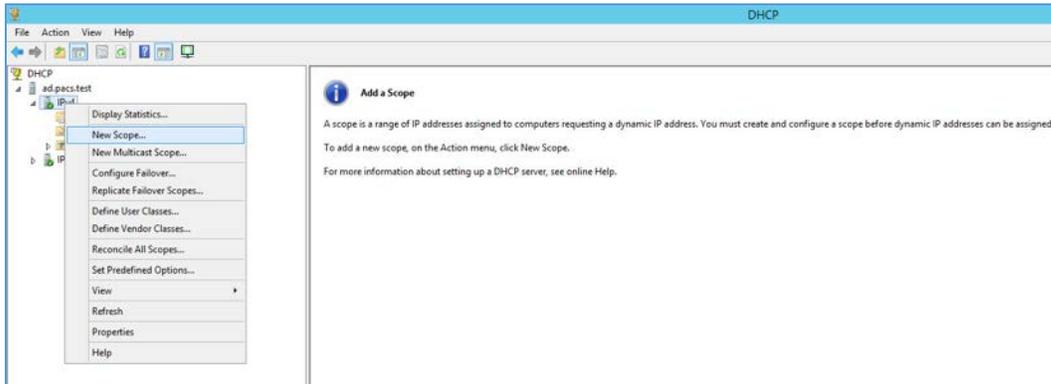
1308

1309 2. In the top right, click on **Tools > DHCP**.



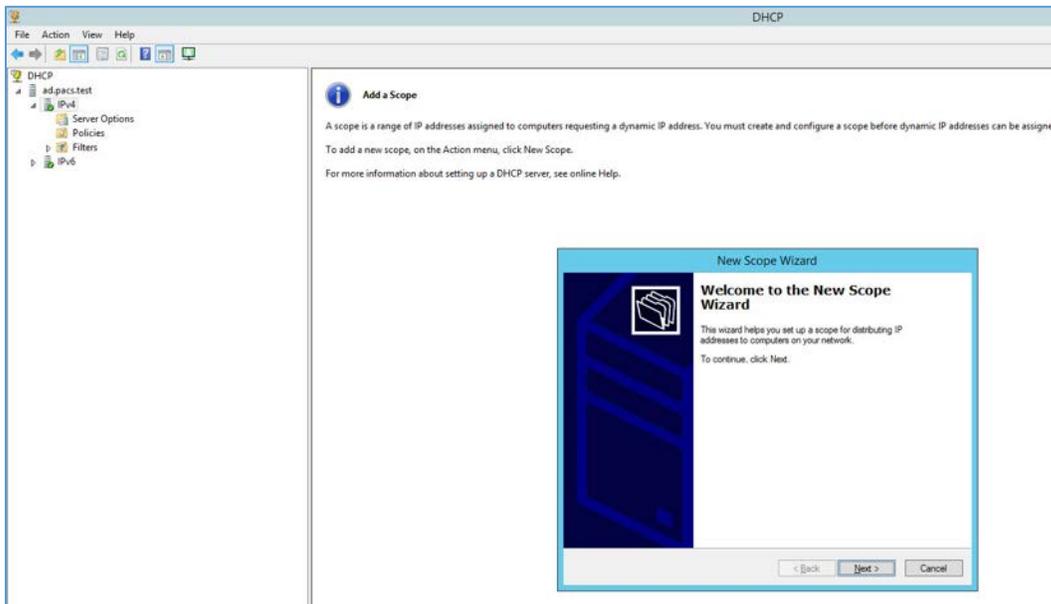
1310

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



1312

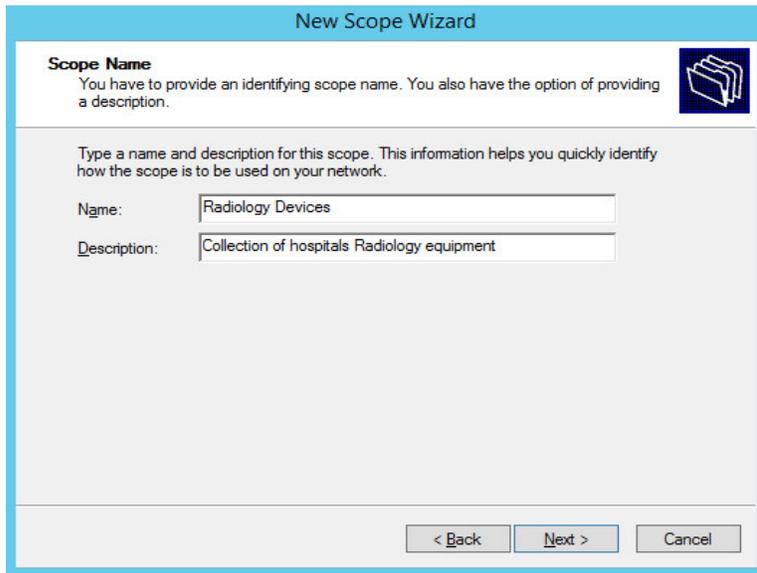
1313 4. Click **Next >**.



1314

1315 5. Provide a **Name** as **Radiology Devices** and a **Description** as **Collection of hospitals Radiology**
1316 **equipment** in the **New Scope Wizard**.

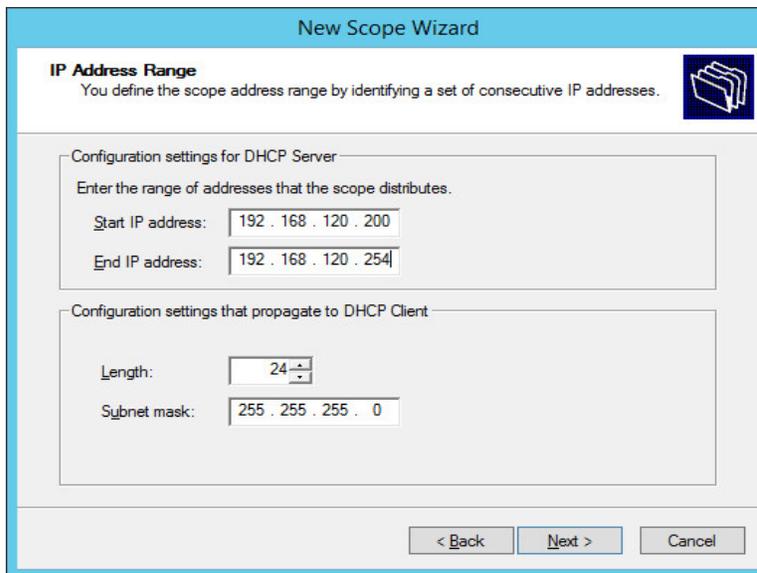
1317 6. Click **Next >**.



1318

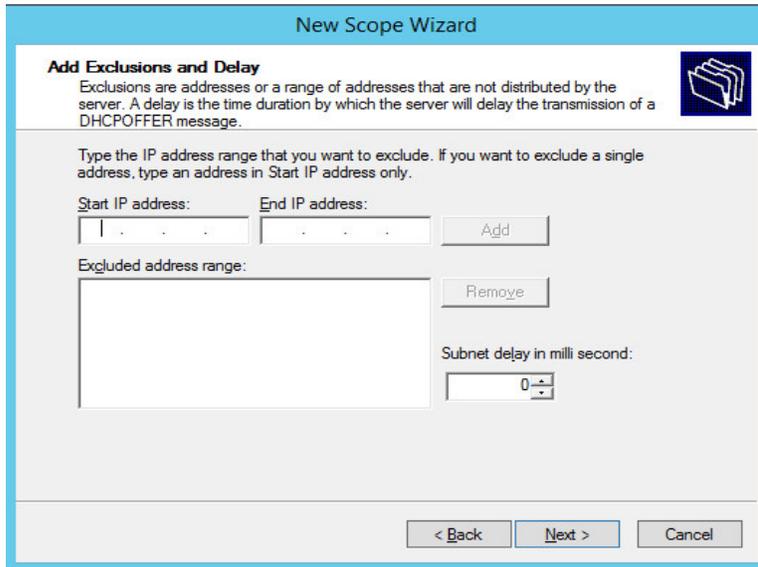
1319 7. Establish the IP range (**192.168.120.200 – 192.168.120.254**) from which the DHCP server should
1320 hand out IPs for devices in this scope.

1321 8. Click **Next >**.



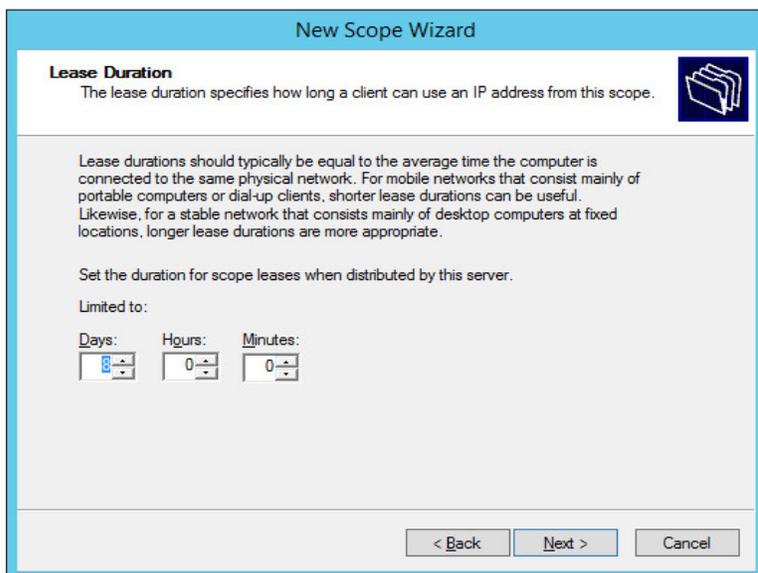
1322

1323 9. Click **Next >**.



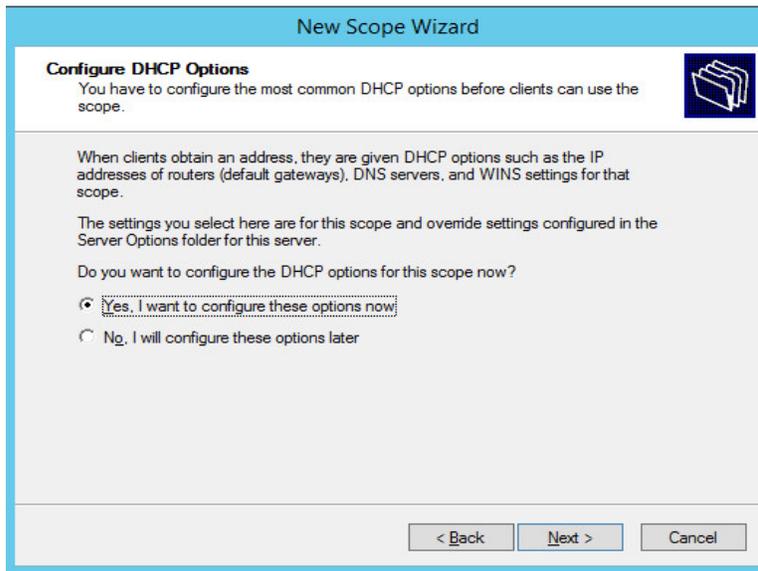
1324

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



1326

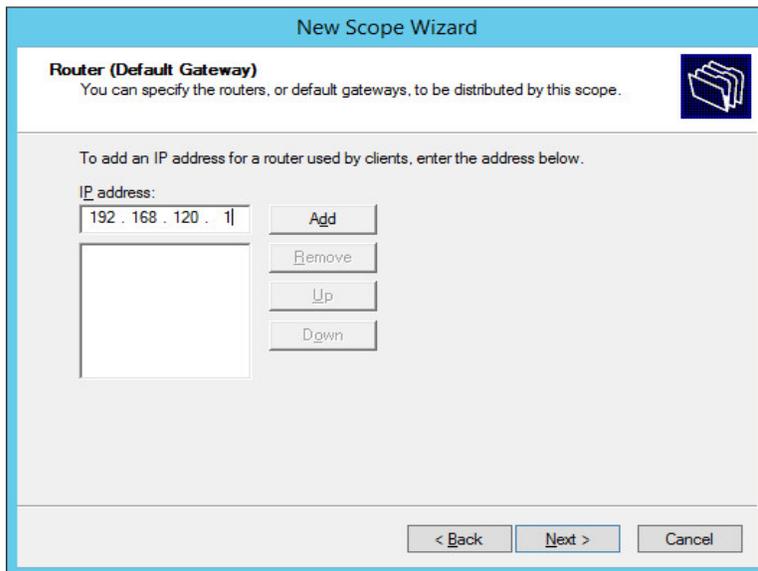
1327 11. Choose **Yes, I want to configure these options now**, and then click **Next >**.



1328

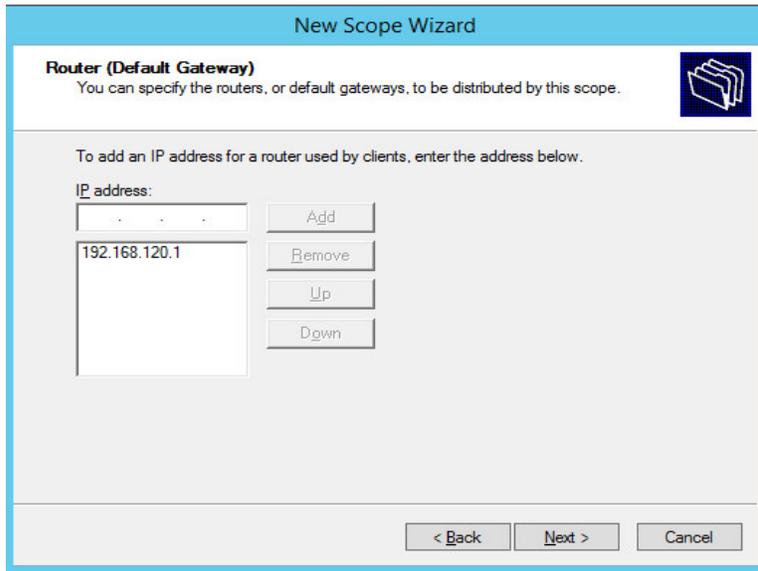
1329 12. Enter the subnet's **Default Gateway** as **192.168.120.1**.

1330 13. Click **Add**.



1331

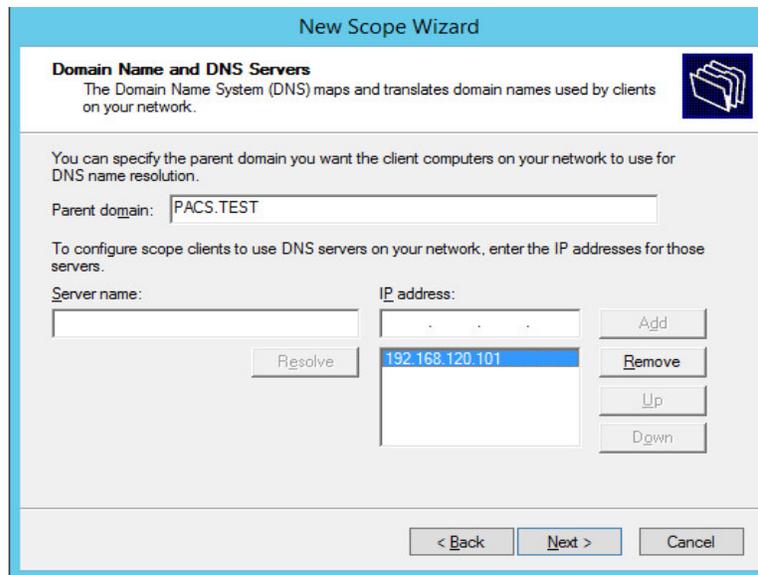
1332 14. Click **Next >**.



1333

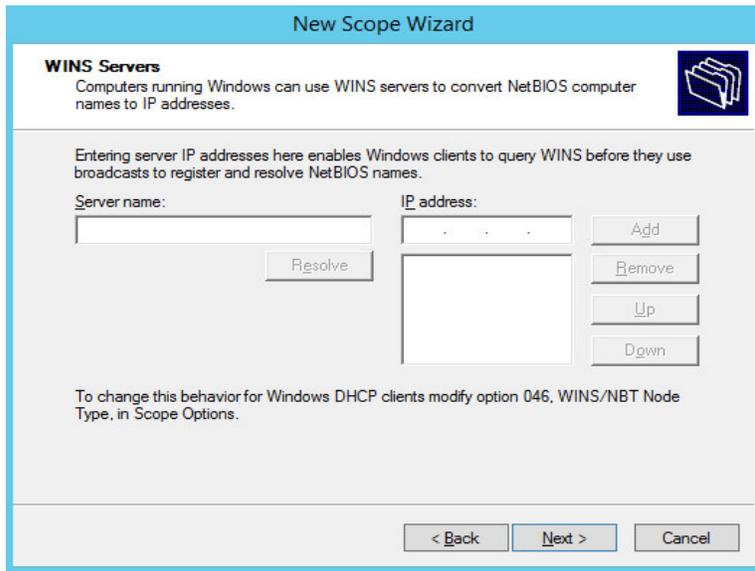
1334 15. Ensure IP address in bottom-right box is the IP address (**192.168.120.101**) for the DNS server
1335 configured earlier.

1336 16. Click **Next >**.



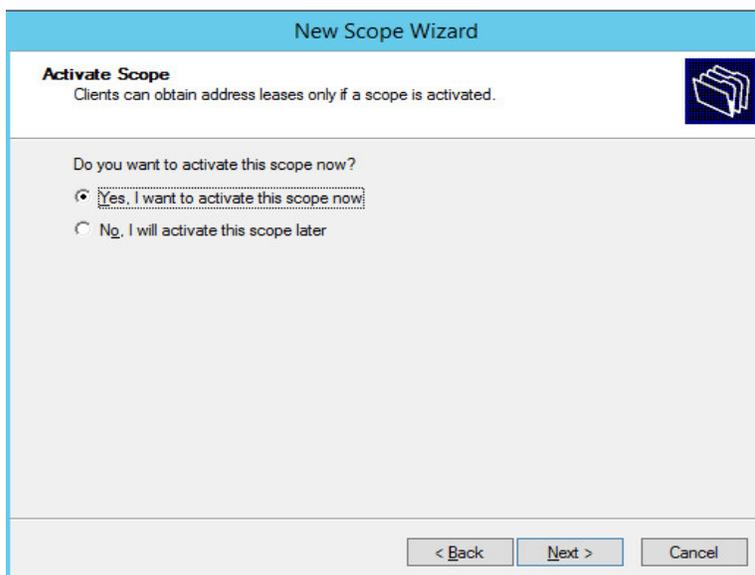
1337

1338 17. Click **Next >**.



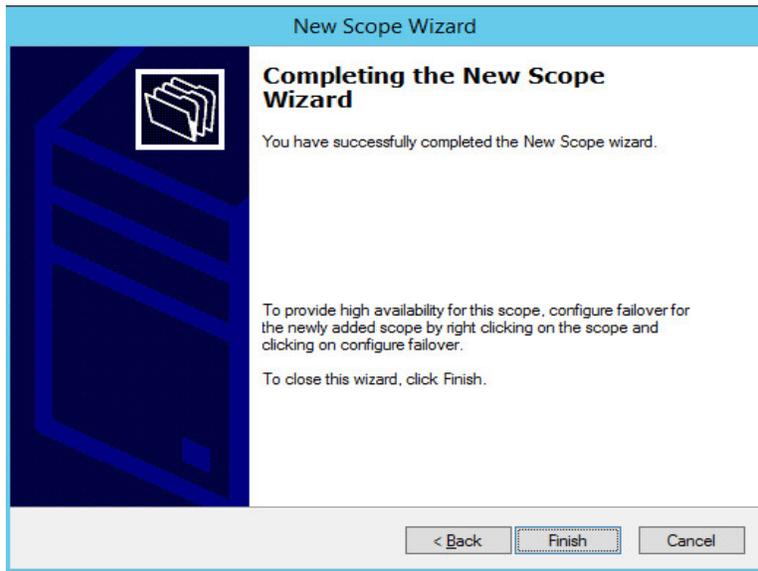
1339

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



1341

1342 19. Click **Finish**.



1343

1344 20. Scope should appear under **IPv4** dropdown. Ensure **Scope Options** are correctly established with
 1345 these values:

1346

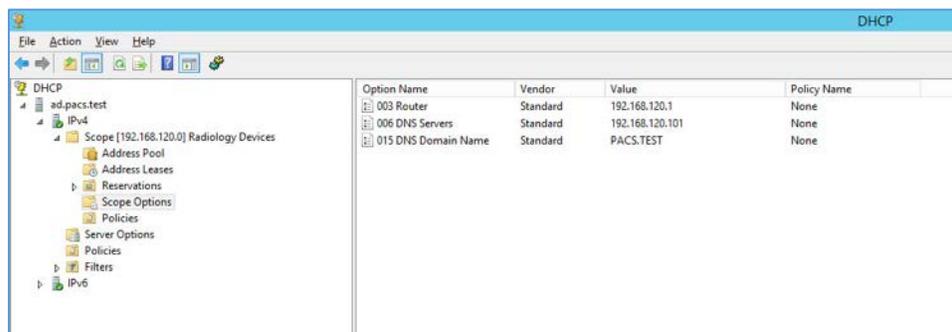
- **003 Router:** 192.168.120.1

1347

- **006 DNS Servers:** 192.168.120.101

1348

- **015 DNS Domain Name:** PACS.TEST



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
 1355 authentication and encryption for data-at-rest or data-in-transit as needed.

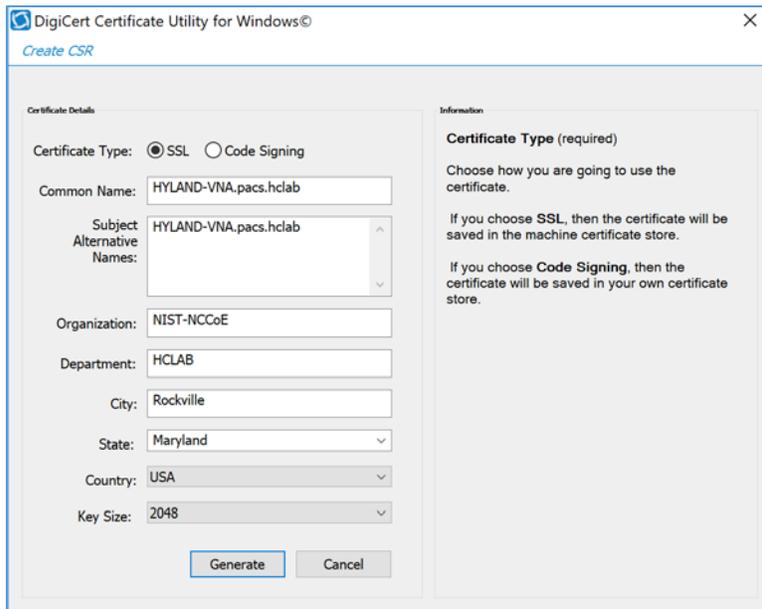
1356 The instructions below describe the process used to obtain an SSL certificate on behalf of medical
1357 devices using the DigiCert certificate signing services.

1358 **Create CSR**

1359 A CSR is represented as a block Base64 encoded PKCS#10 binary format text that will be sent to a CA for
1360 digital signature when applying for an SSL Certificate. The CSR identifies the applicant's distinguished
1361 common name (domain name), organization name, locality, and country. It also contains the applicant's
1362 private key and the public key pair. The CSR is usually generated from the device where the certificate
1363 will be installed, but it can also be generated using tools and utilities on behalf the device to generate a
1364 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.

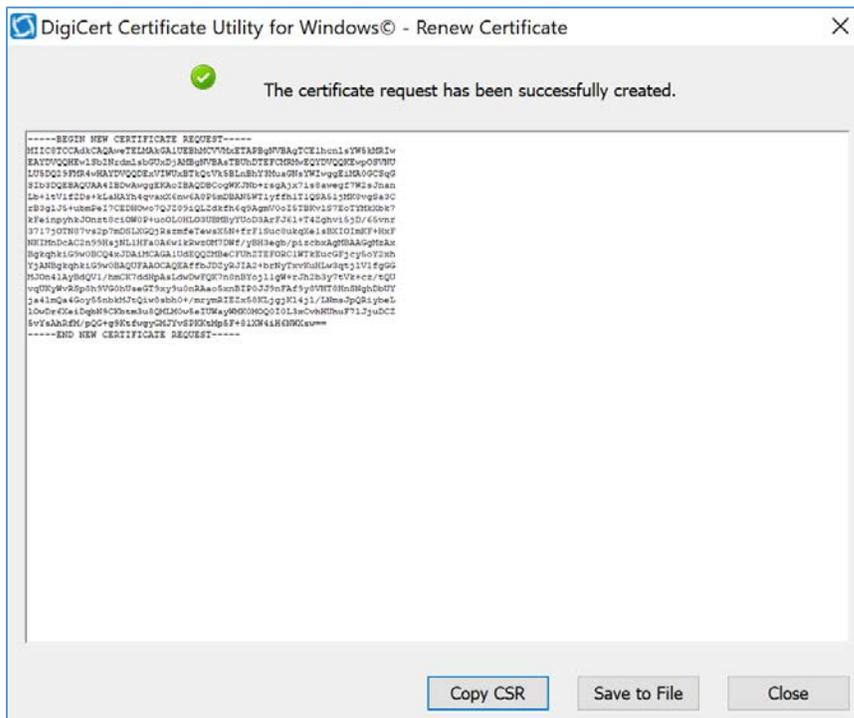
1366 Download and save the *DigiCertUtil.exe* from the DigiCert site [14].

- 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
- 1379 4. Click **Generate** to create a CSR. This will also generate a corresponding private key in the Windows
1380 computer from which the CSR is requested. The Certificate Enrollment Request is stored under
1381 *Console Root\Certificates(Local Computer)\Certificate Enrollment Requests\Certificates*.



1382

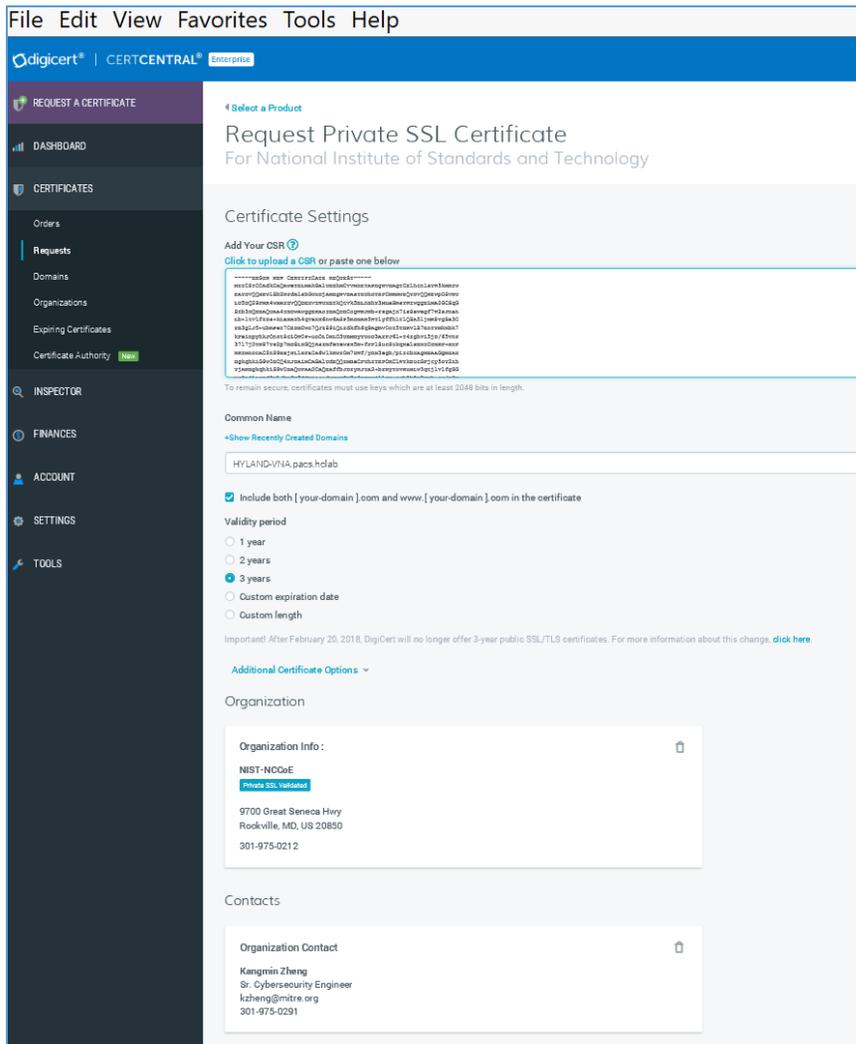
1383 5. A sample CSR is shown in the figure below:



1384

1385 6. Select and copy the certificate contents to the clipboard or save it to an ascii text file. The text
1386 contents will be used to paste into the DigiCert order form.

- 1387 7. **Issue Signed Certificates.** With a created applicant CSR, request a signed certificate using DigiCert
1388 **CertCentral** portal, using these steps:
- 1389 a. Log in to a DigiCert Dashboard (<https://www.digicert.com/account/login.php>) with your
1390 account username and password. In the portal, select **CERTIFICATES>Requests**, then
1391 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 the **-----BEGIN NEW**
1393 **CERTIFICATE REQUEST-----** and **-----END 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.



1399

1400

1401

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

Order #	Date	Common Name	Status	Validity	Product	Expires
6225403 Quick View	05 Jun 2019	HYLAND-NILREAD.pacs.hclab	Issued	3 years	Private SSL	04 Jun 2020
6221759 Quick View	05 Jun 2019	ncooess1.stncooe.lsyntax.net	Issued	3 years	Private SSL	04 Jun 2020
6221720 Quick View	05 Jun 2019	HYLAND-VMA.pacs.hclab	Issued	3 years	Private SSL	04 Jun 2020
565577 Quick View	24 Apr 2019	HYLAND-PGODRE.pacs.hclab	Issued	3 years	Private SSL	23 Apr 2020
5643403 Quick View	23 Apr 2019	HYLAND-PGCRE.pacs.hclab	Issued	3 years	Private SSL	22 Apr 2020

1402

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.

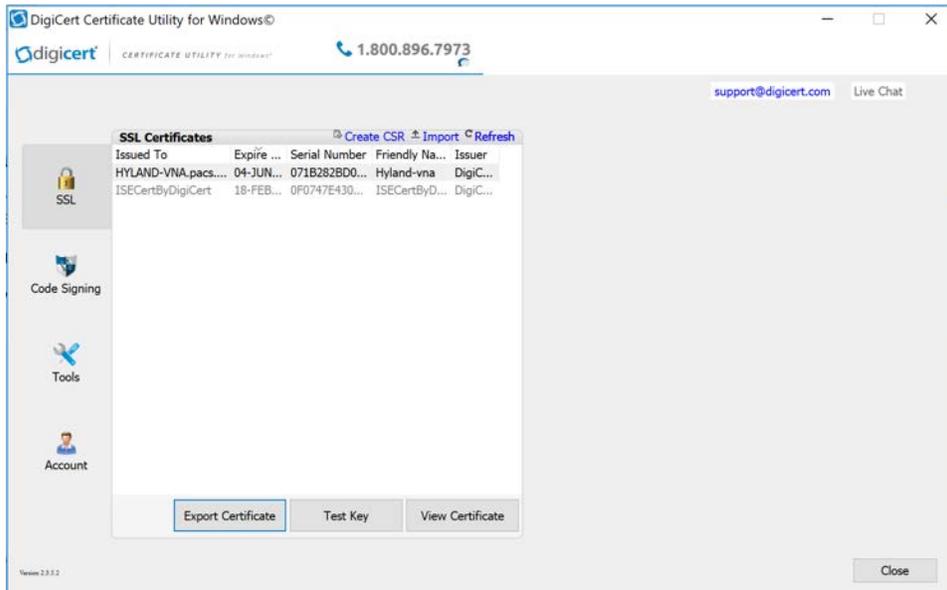
1407 Import and Export the Signed Certification

1408 After downloading the SSL Certificate from DigiCert, you can use the DigiCert Certificate Utility for
 1409 Windows to install it. With the DigiCert Utility tool, you can further manipulate the certificates to
 1410 combine with the private key and export the signed certificate to the certificate requesting device
 1411 server.

1412 1. From the DigiCert Certificate Utility for Windows, click the **Import** button to load the downloaded
 1413 signed Certificate file to the utility. The downloaded file was saved in Step 10 of [Section 2.6.2](#). Click
 1414 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**.



1418

- 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.



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 **Cisco Firepower Management Center Appliance Information**

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 **Cisco Firepower Management Center Virtual Installation Guide**

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 **Cisco Firepower Threat Defense Appliance Information**

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

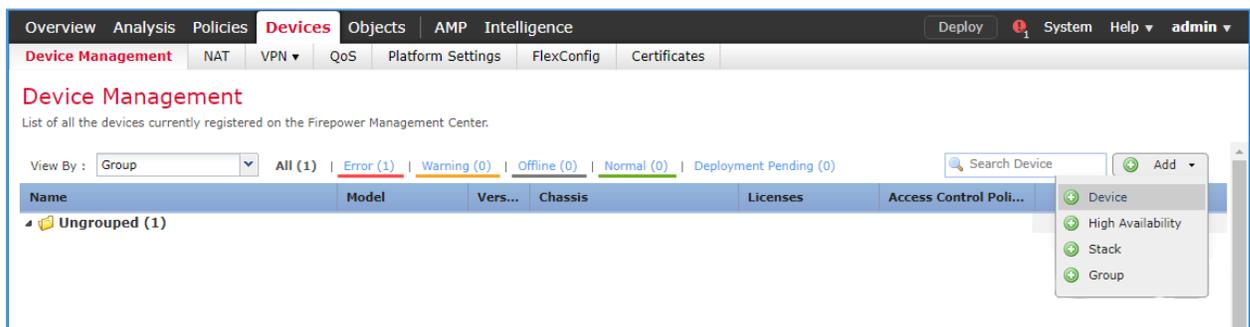
1450 **Operating System:** Cisco Fire Linux

1451 **Cisco Firepower Threat Defense Virtual Installation Guide**

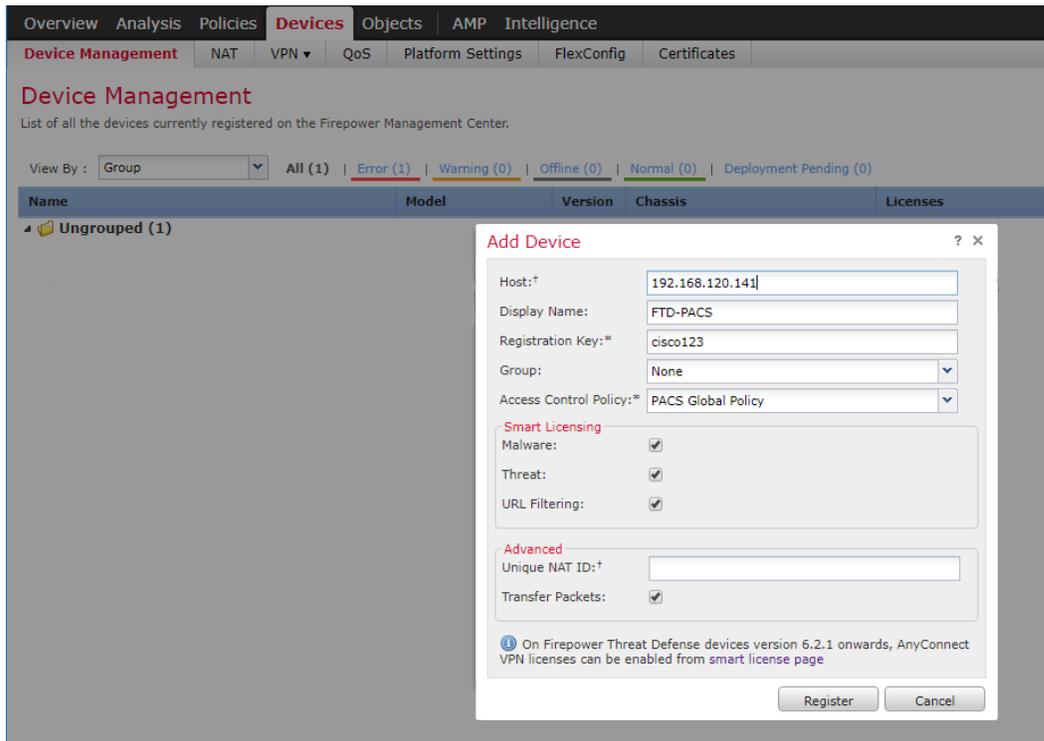
1452 Install the Cisco Firepower Threat Defense Virtual appliance, according to the instructions detailed at
 1453 Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide [16].

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**.

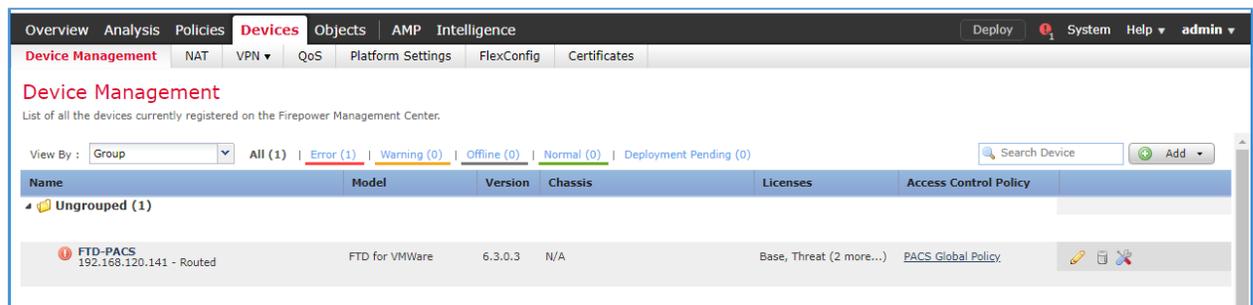


- 1458
- 1459 4. Enter **192.168.120.141** as the **IP address** of the FTD appliance.
- 1460 5. Enter **FTD-PACS** as a **display name** to identify the FTD appliance.
- 1461 6. Enter the **manager key** created when configuring the manager on the FTD appliance.
- 1462 7. Click the **Access Control 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**.



1469

1470 11. The FTD appliance will be added to the FMC’s device list.



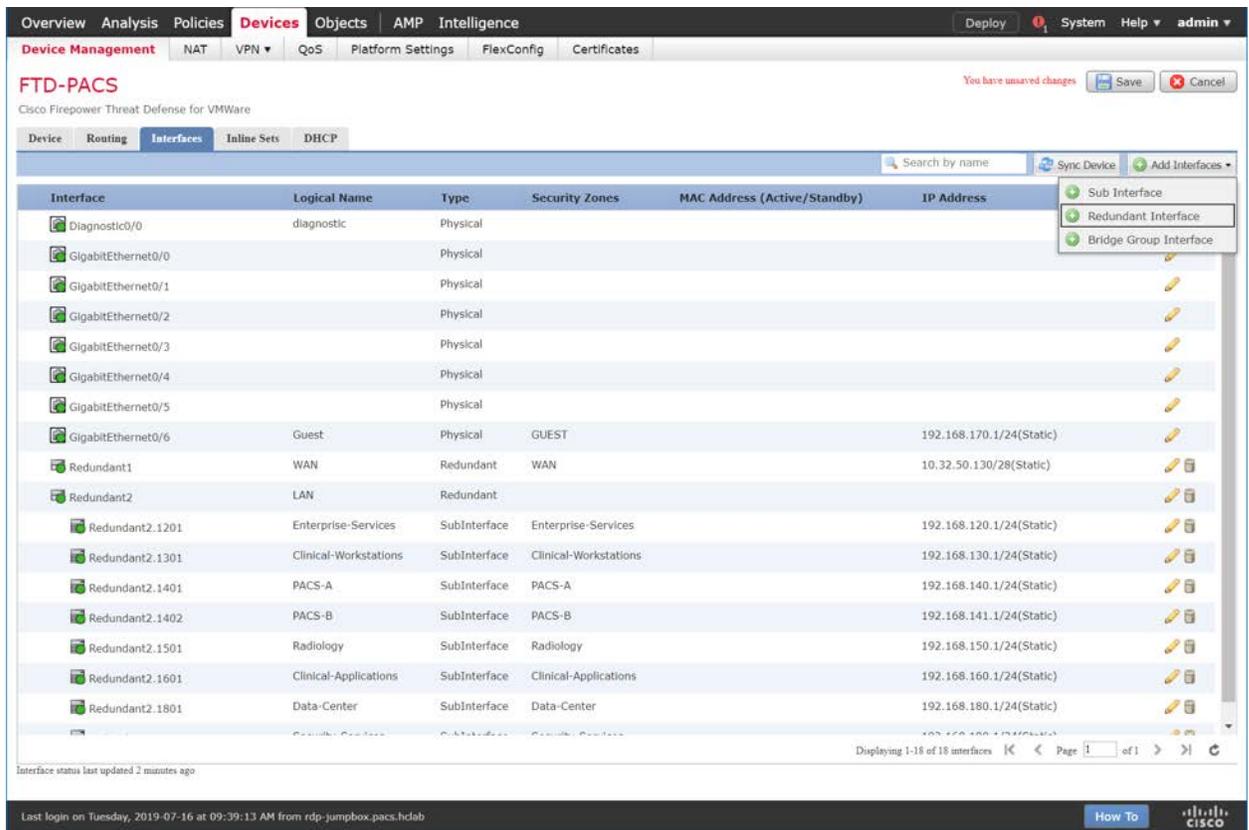
1471

1472 **FTD Interfaces for PACS Architecture Configuration**

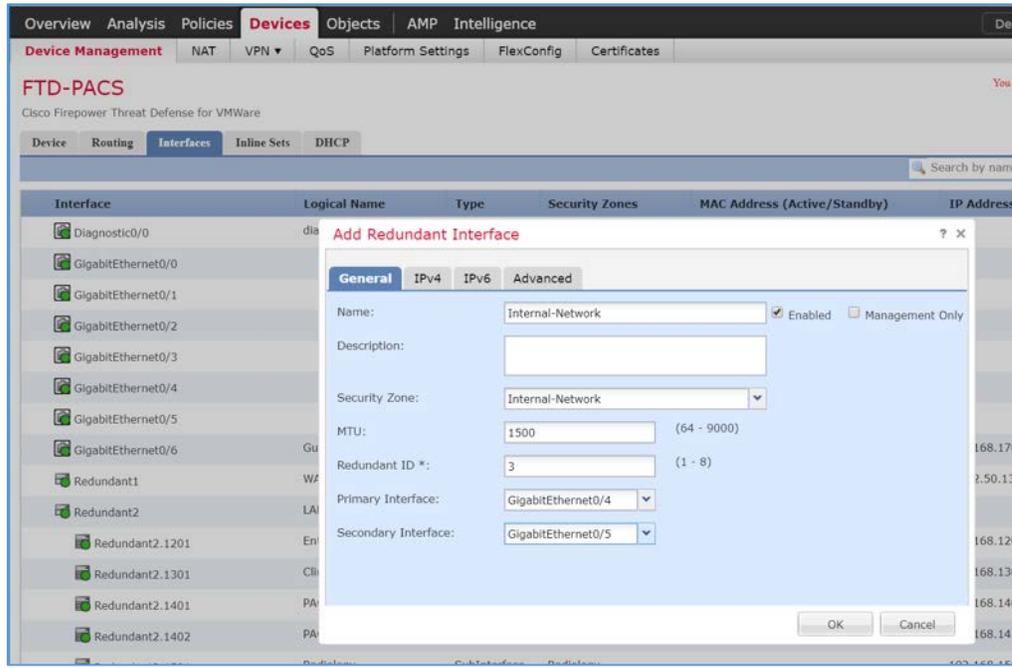
1473 Each physical interface connected to the Cisco FTD will appear in the FMC device management section
 1474 under the interface tab. In order to configure the eight subnets needed for the PACS architecture while
 1475 also allowing for management, diagnostic, and Wide Area Network (WAN) traffic, we dedicated two
 1476 interfaces set up as a redundant pair for all internal subnet traffic. To accomplish this, a sub-interface
 1477 was created for each of the eight PACS subnets (Enterprise Services, Imaging Modalities, Security
 1478 Services, etc.), and established redundant interfaces for WAN traffic and traffic on VLAN 1101. The
 1479 following guidance describes how the redundant interfaces and sub-interfaces were created.

DRAFT

- 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**.



- 1484
- 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.

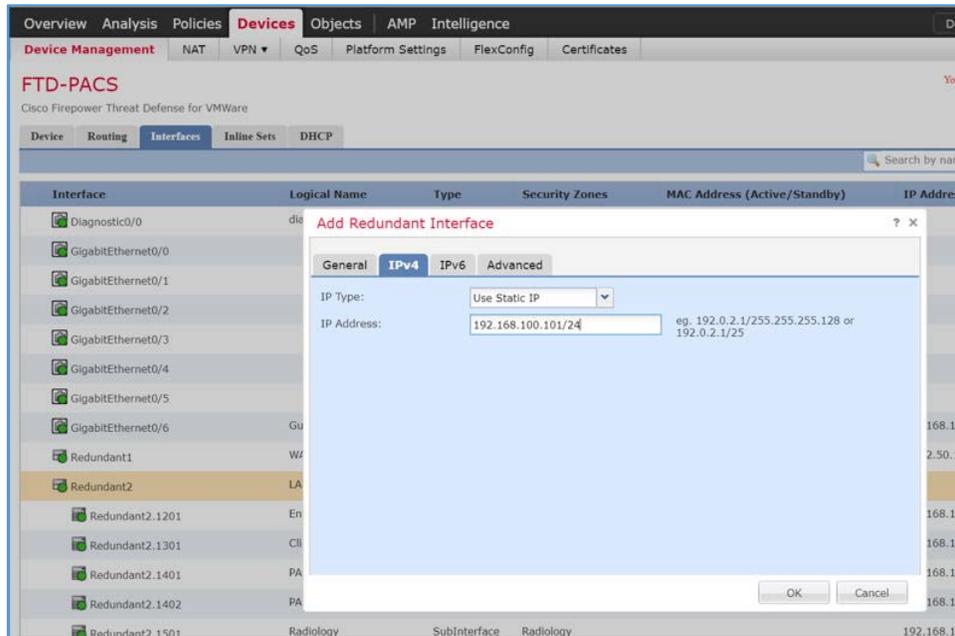


1489

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**.



1493

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

The screenshot shows the Cisco Firepower Threat Defense (FTD) web interface for 'FTD-PACS'. The 'Interfaces' tab is selected, displaying a table of interfaces. A dropdown menu is open for 'Add Interfaces', showing options: 'Sub Interface', 'Redundant Interface', and 'Bridge Group Interface'. The table lists various interfaces, including physical and redundant interfaces, with their logical names, types, security zones, MAC addresses, and IP addresses.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
GigabitEthernet0/1		Physical			
GigabitEthernet0/2		Physical			
GigabitEthernet0/3		Physical			
GigabitEthernet0/4		Physical			
GigabitEthernet0/5		Physical			
GigabitEthernet0/6	Guest	Physical	GUEST		192.168.170.1/24(Static)
Redundant1	WAN	Redundant	WAN		10.32.50.130/28(Static)
Redundant2	LAN	Redundant			
Redundant2.1201	Enterprise-Services	SubInterface	Enterprise-Services		192.168.120.1/24(Static)
Redundant2.1301	Clinical-Workstations	SubInterface	Clinical-Workstations		192.168.130.1/24(Static)
Redundant2.1401	PACS-A	SubInterface	PACS-A		192.168.140.1/24(Static)
Redundant2.1402	PACS-B	SubInterface	PACS-B		192.168.141.1/24(Static)
Redundant2.1501	Radiology	SubInterface	Radiology		192.168.150.1/24(Static)
Redundant2.1601	Clinical-Applications	SubInterface	Clinical-Applications		192.168.160.1/24(Static)
Redundant2.1801	Data-Center	SubInterface	Data-Center		192.168.180.1/24(Static)
Redundant2.1901	Security-Services	SubInterface	Security-Services		192.168.190.1/24(Static)
Redundant3	Internal-Network	Redundant	Internal-Network		192.168.100.101/24(Static)

1495

1496 13. Enter **VNA** as the **name** for the sub interface.

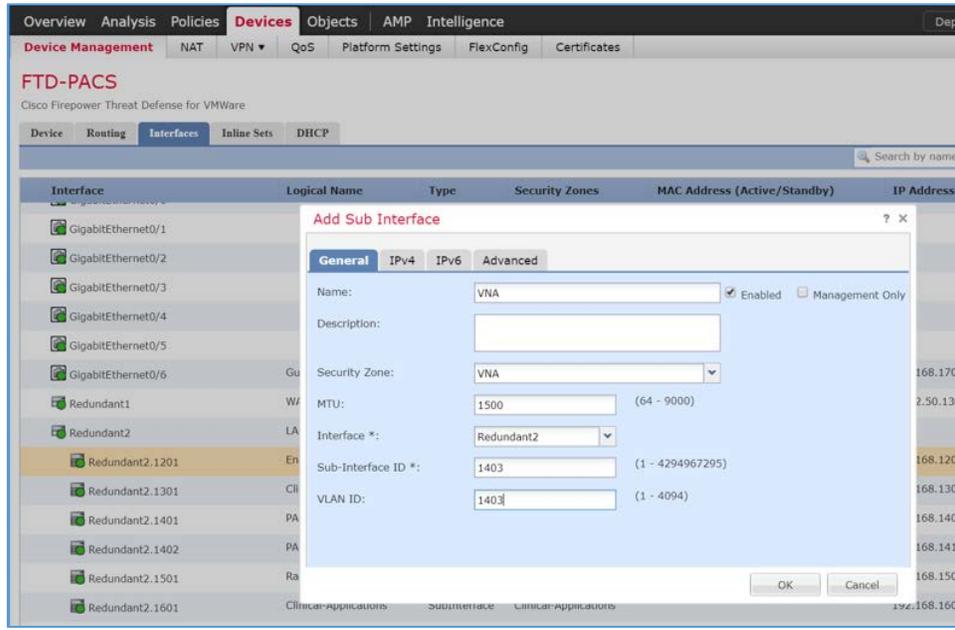
1497 14. Create and/or add a **security zone, VNA**, to the sub interface.

1498 15. Select an **interface** under which the sub interface will operate.

1499 Note: For our build, we placed each sub-interface under **Redundant 2**, the redundant interface for
 1500 **GigabitEthernet0/2** and **GigabitEthernet0/3**. These two physical interfaces were the destination for
 1501 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.

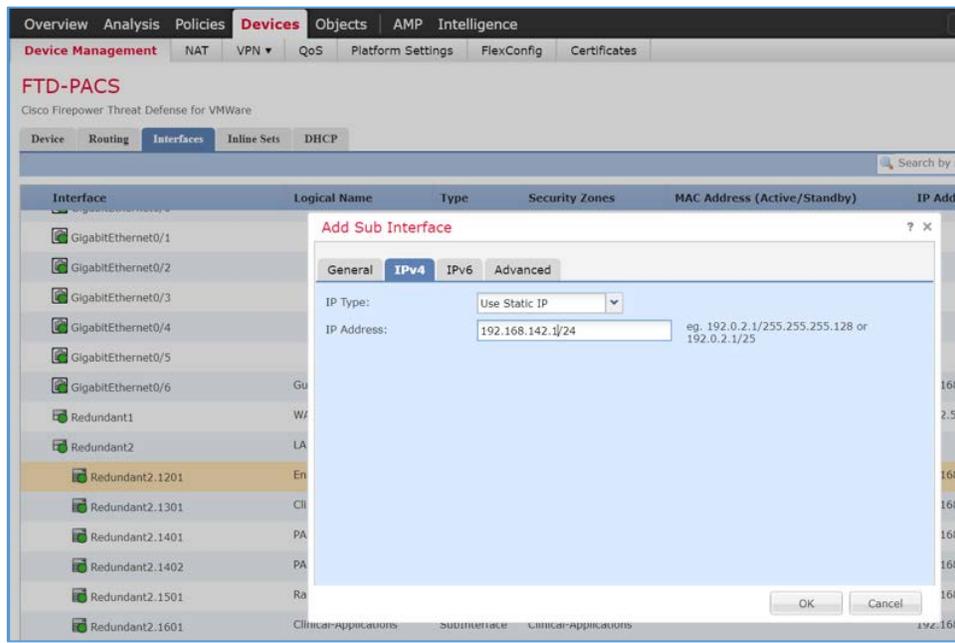


1504

1505 18. Navigate to the **IPv4** tab.

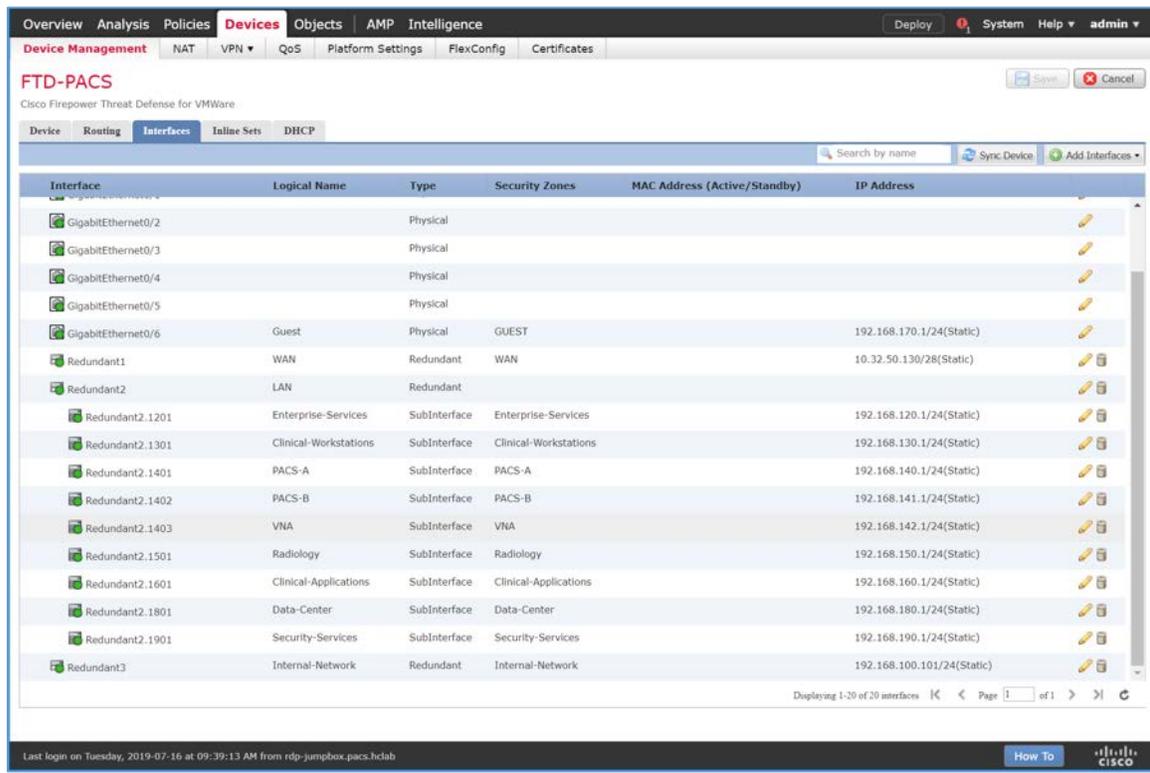
1506 19. Assign an **IP address** and **netmask** (e.g., **192.168.142.1/24**) to the sub interface.

1507 20. Click **OK**.



1508

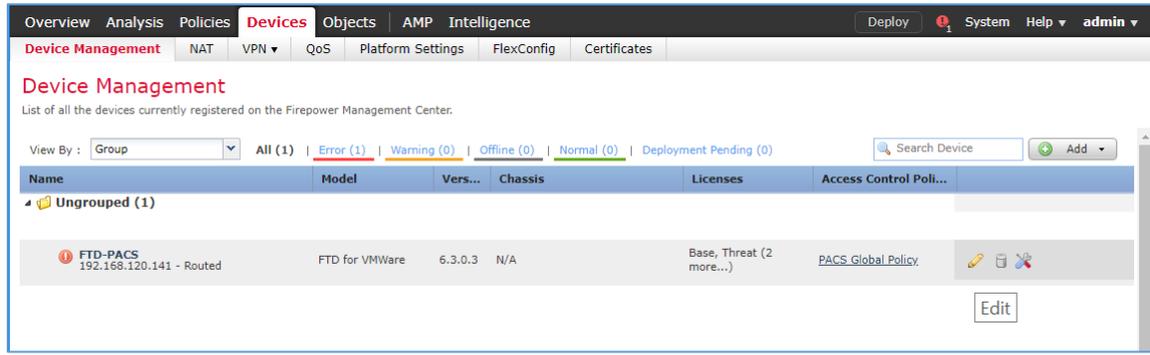
- 1509 21. Click **Save**.
- 1510 22. Click **Deploy** and wait for deployment to FTD to complete.
- 1511 23. Refresh the page and confirm that the redundant interface and sub-interface are running (shown
- 1512 with a green dot on the interface's icon).



1513

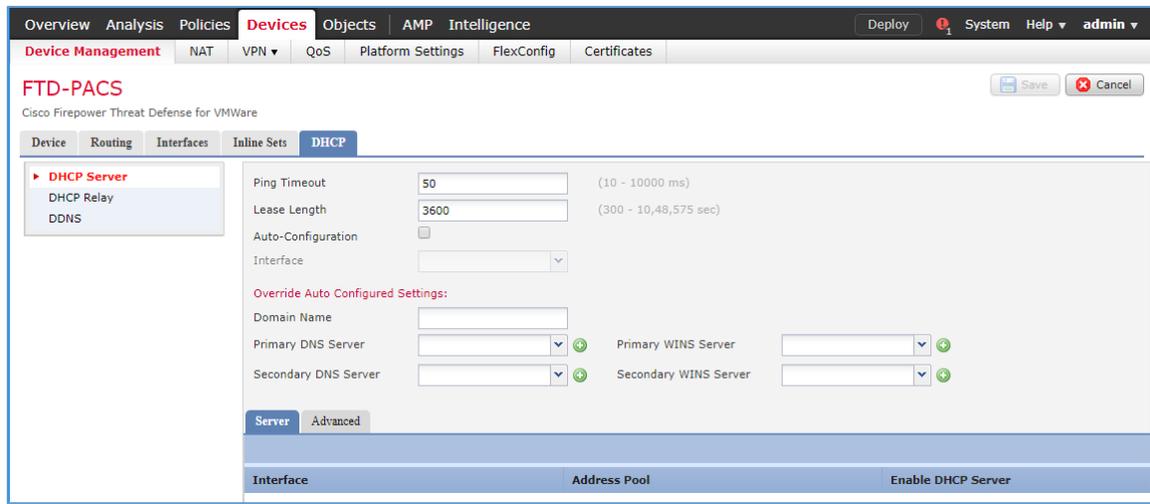
1514 DHCP Relay Through Cisco Firepower Management Center Configuration

- 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.



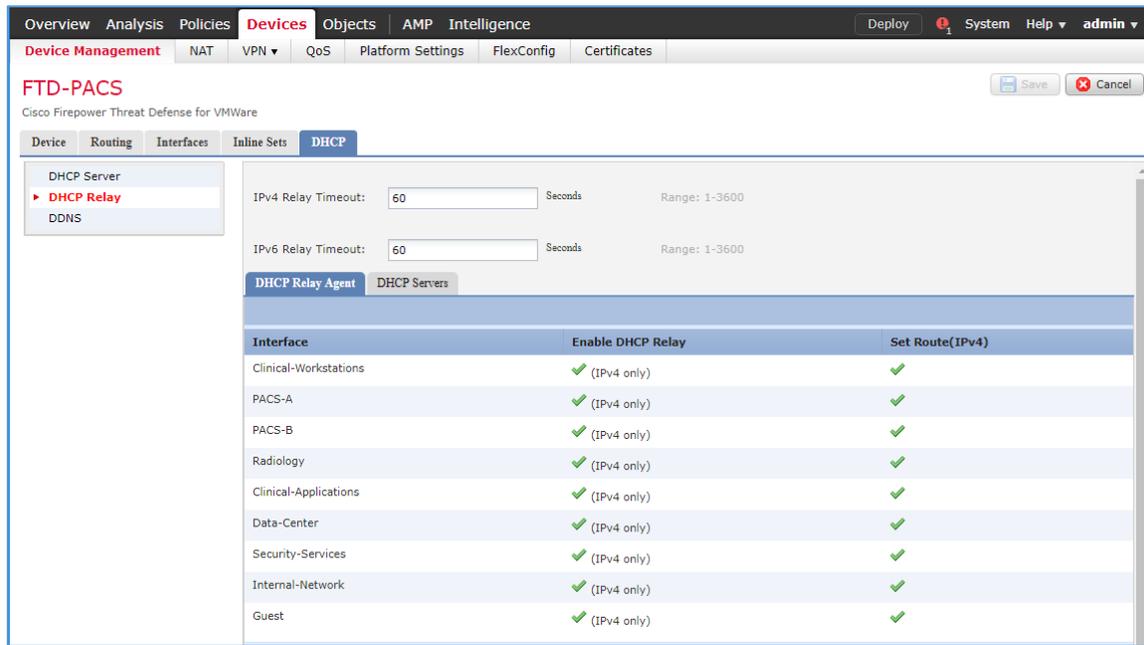
1518

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



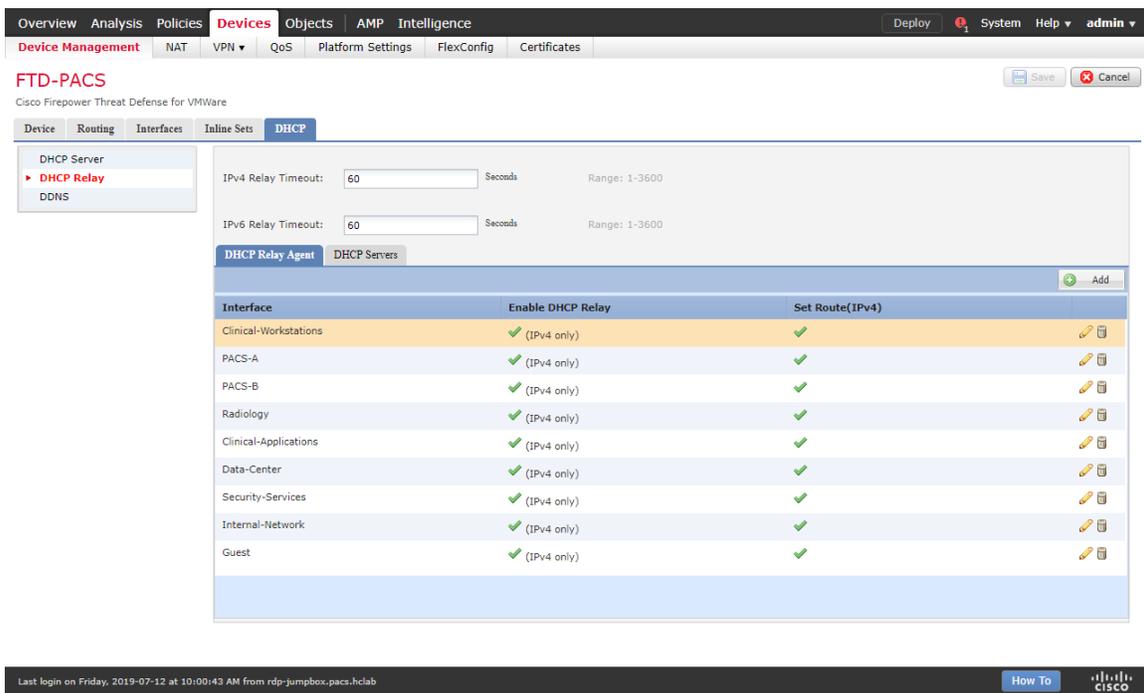
1520

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



1522

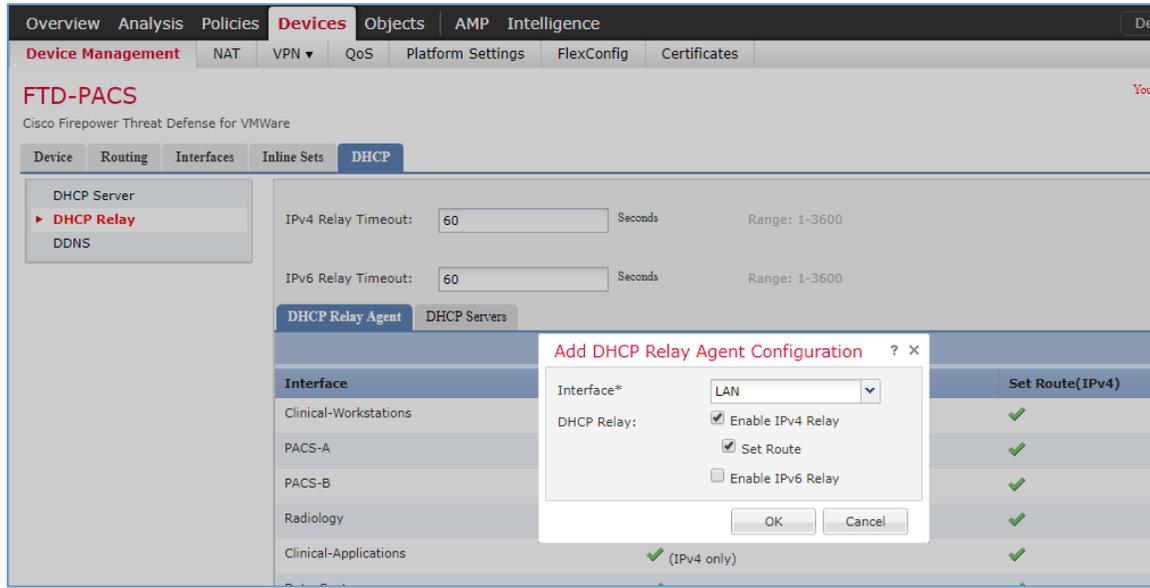
1523 6. Under **DHCP Relay Agent**, click **Add**.



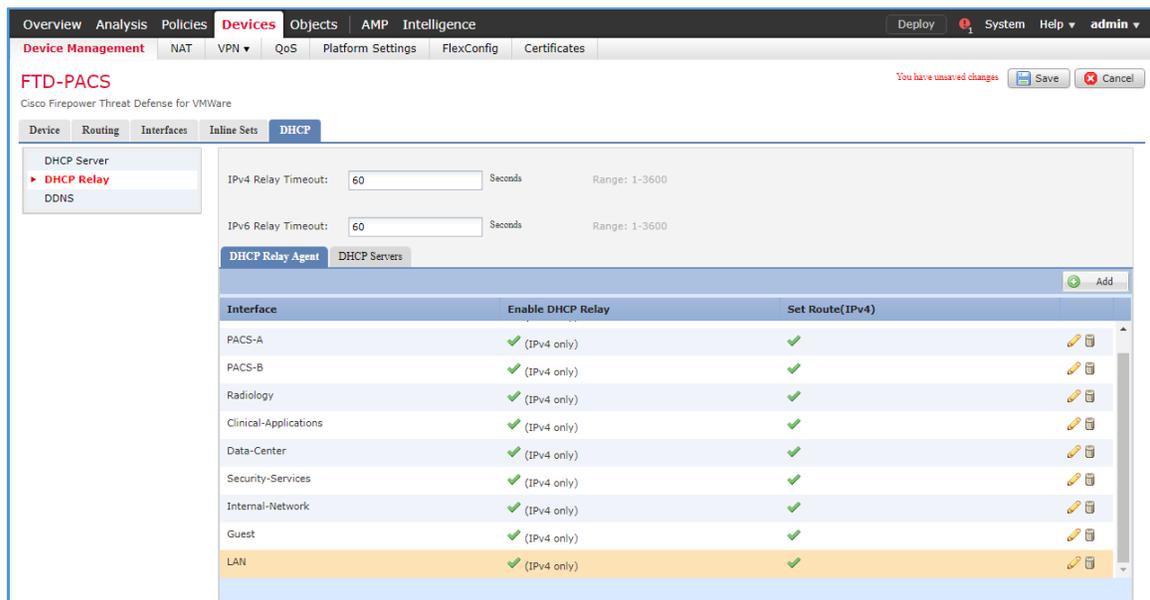
1524

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

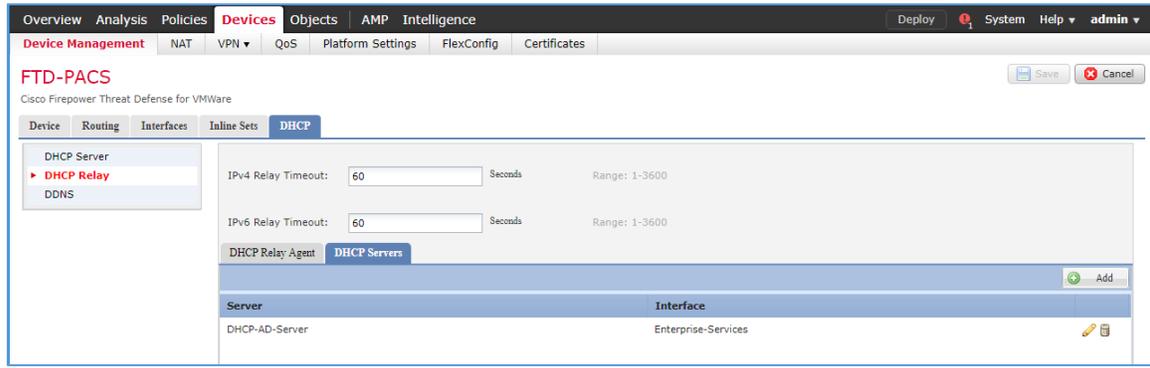
- 1526 8. Check the box next to **Enable IPv4 Relay**.
- 1527 9. Check the box next to **Set Route**.
- 1528 10. Click **OK**.



- 1529
- 1530 11. Ensure the new relay, **LAN**, is shown in the **DHCP Relay Agent** list.

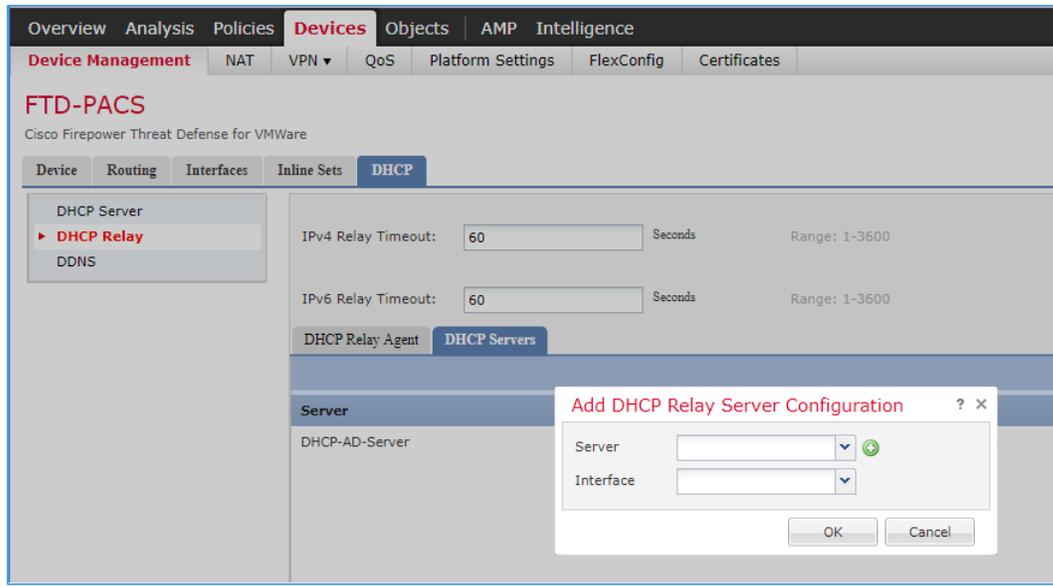


- 1531
- 1532 12. Under **DHCP Servers**, click **Add**.



1533

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

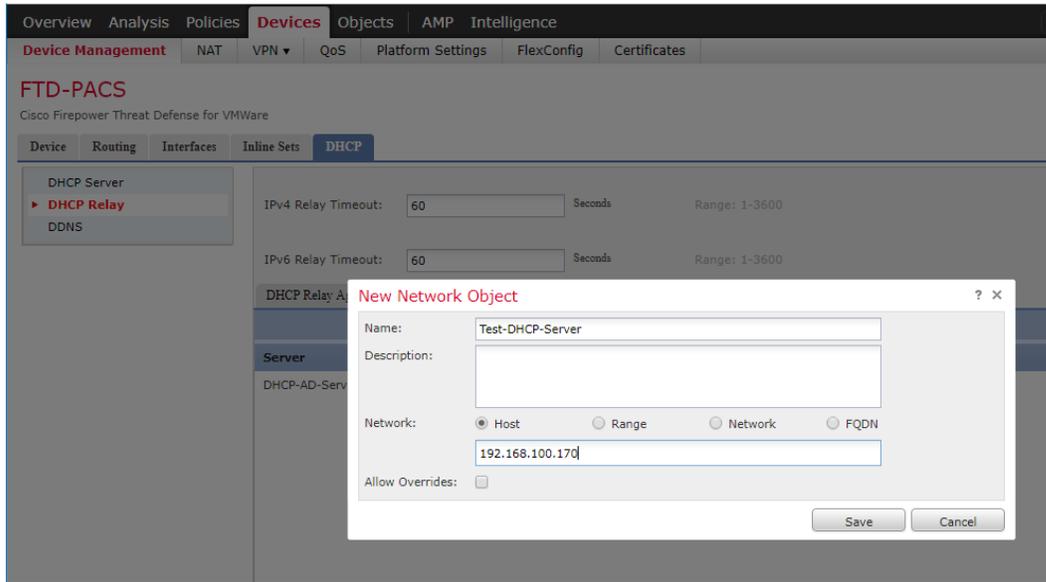


1535

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**.

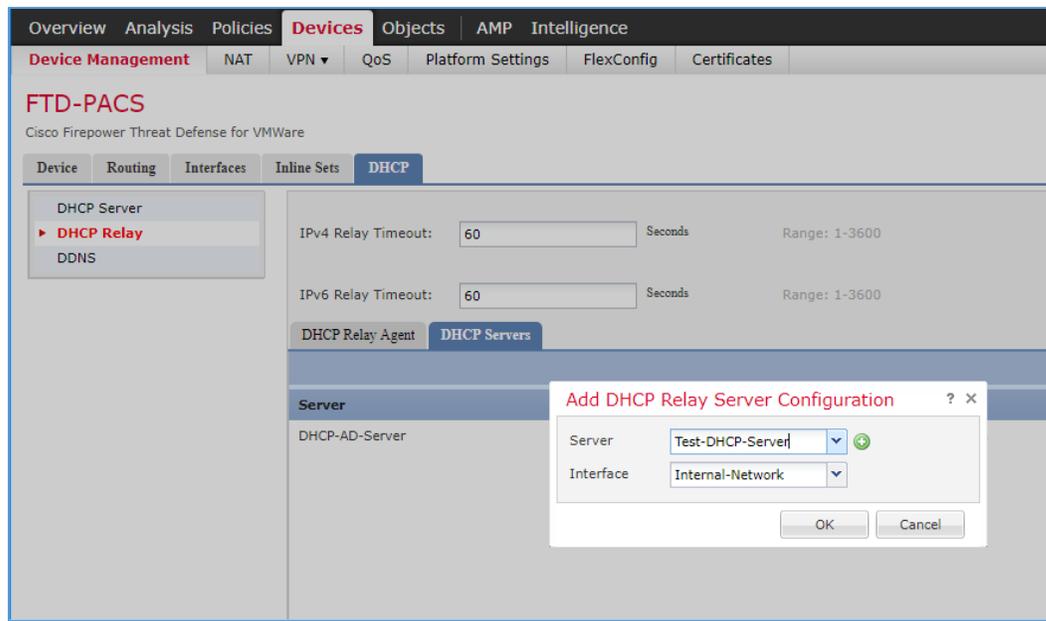


1539

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**.

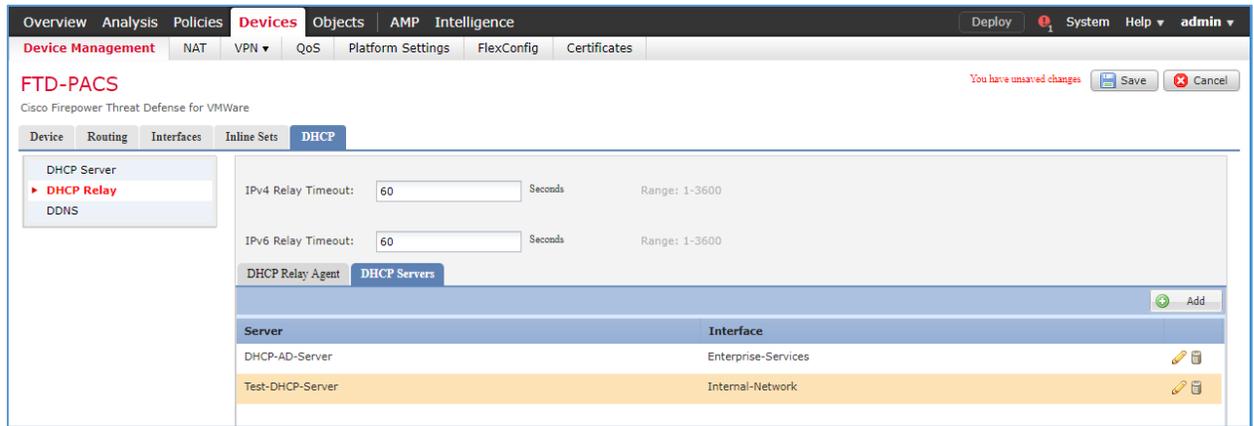


1543

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**.



1550

1551 2. Click **New Policy > Threat Defense NAT**.

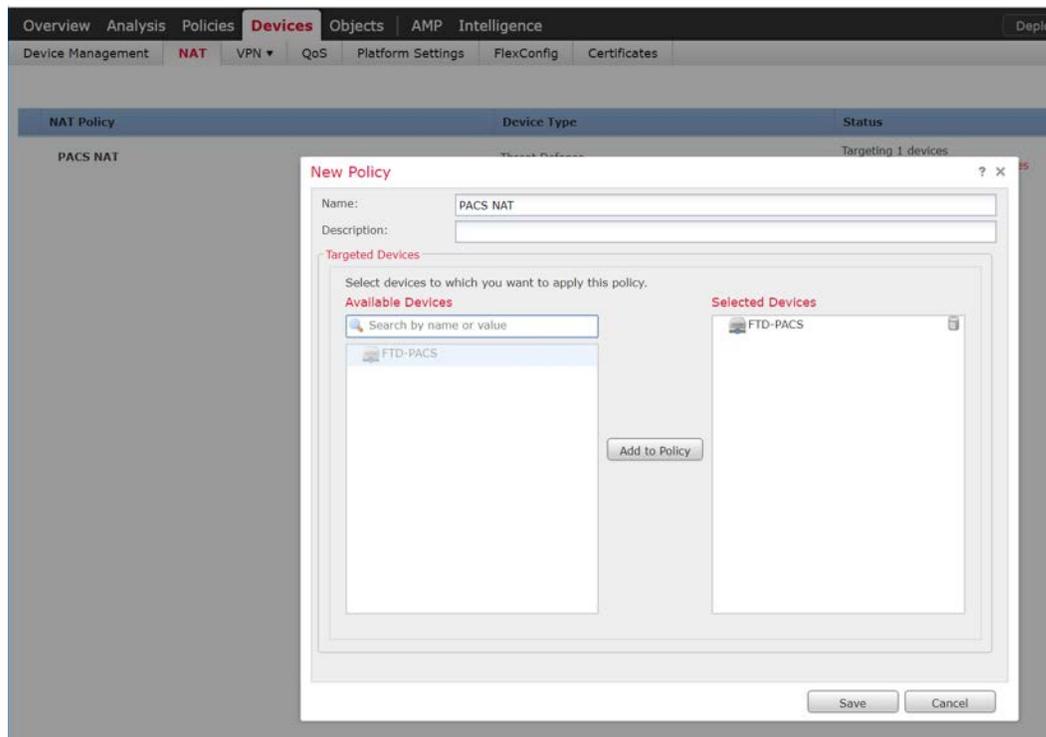


1552

1553 3. Give the new policy a **Name** as **PACS NAT**.

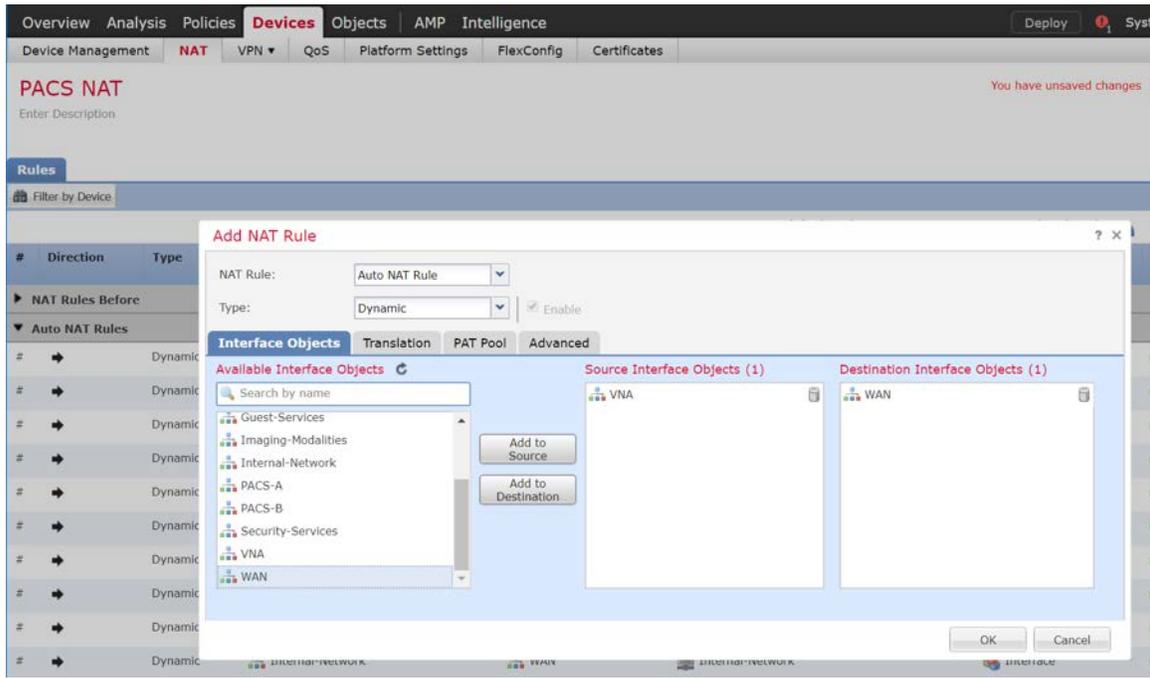
1554 4. Assign the **FTD appliance** to the new NAT policy.

1555 5. Click **Save**.



1556

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**.



1563

1564
1565

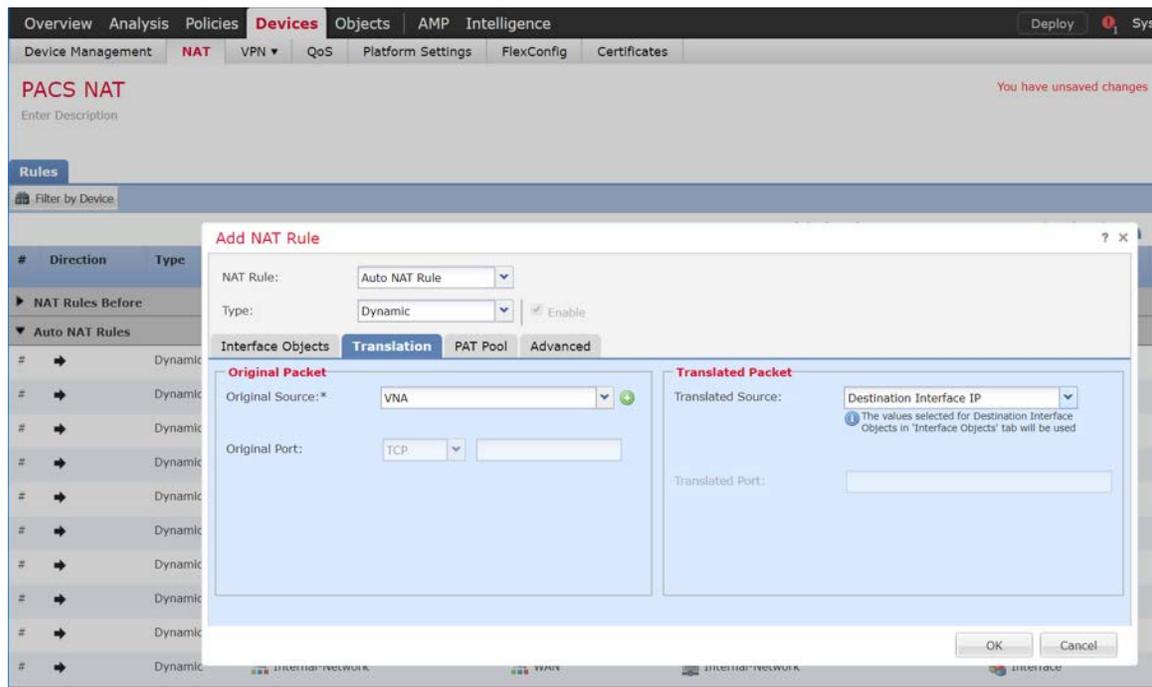
12. Under **Translation**, set **Original Source** to the **network** that corresponds with the source interface object established in the previous step.

1566

13. Set **Translated Source** to **Destination Interface IP**.

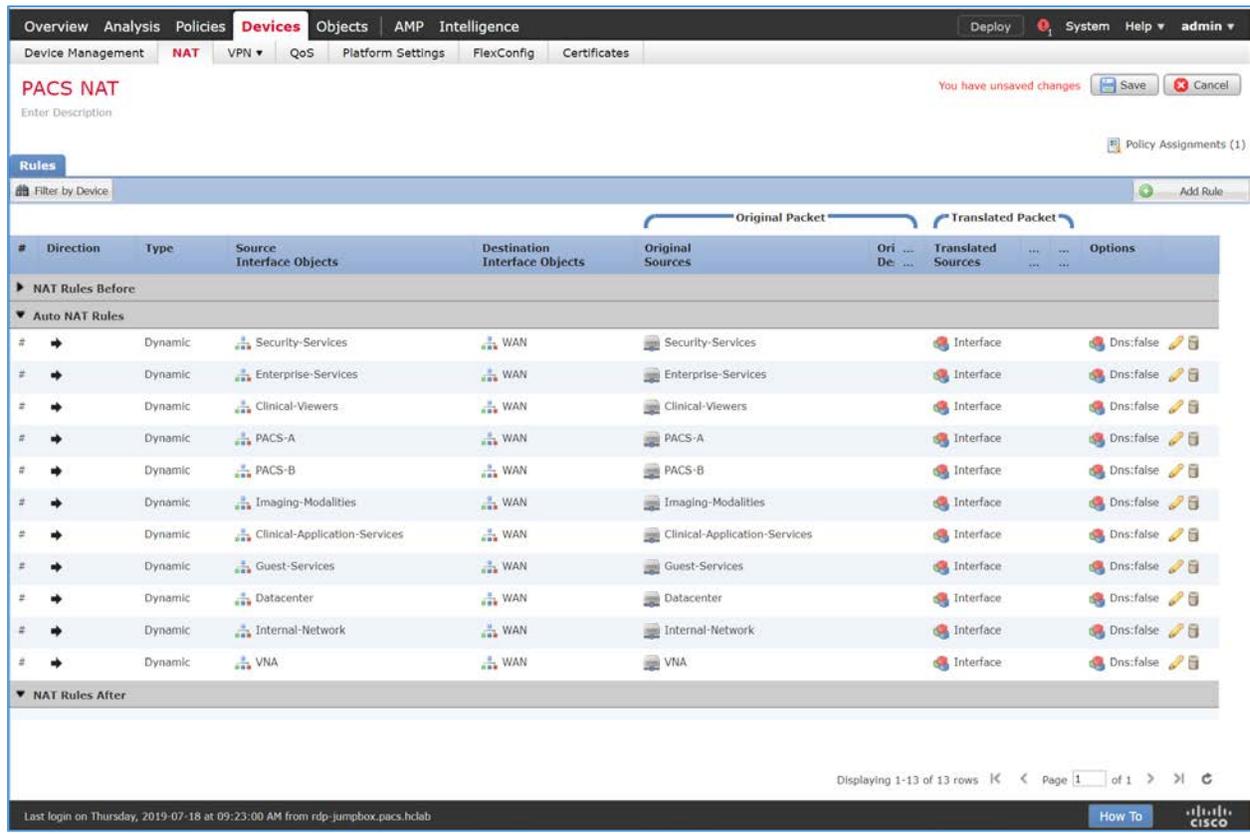
1567

14. Click **OK**.



1568

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.



1573

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

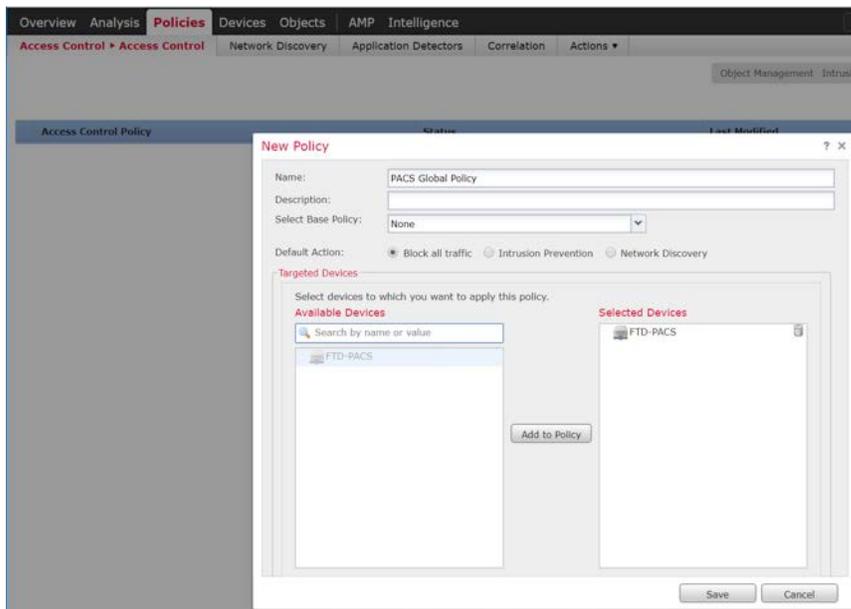
1575 Firepower Management Center allows configuration of access control policies that can then be applied
 1576 to individual FTD appliances. The purpose of the access-control policy is to create rules that specify how
 1577 traffic is managed within the network. Each access-control policy contains multiple 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**.



1584

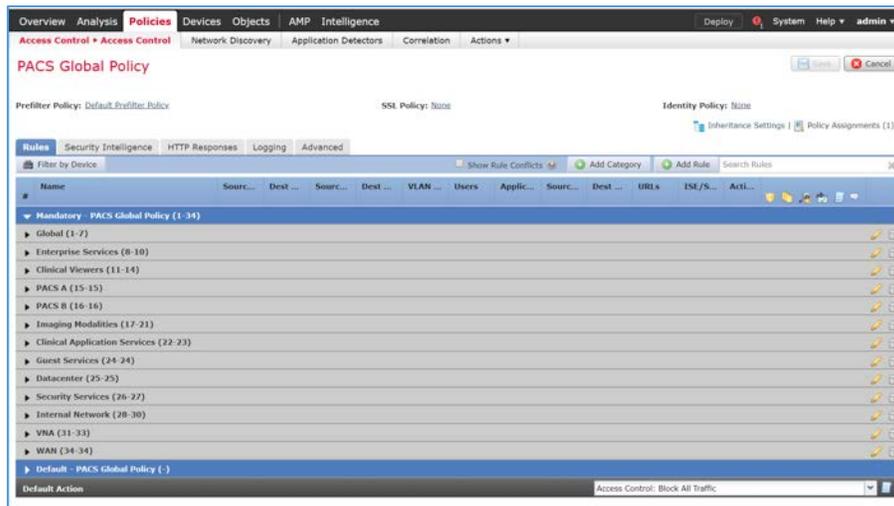
- 1585 2. Click **New Policy**.
- 1586 3. Enter **PACS Global Policy** as the name for the access control policy.
- 1587 4. For **Select Base Policy** select **None**.
- 1588 5. For **Default Action** select **Block all traffic**.
- 1589 6. Add the FTD appliance to the policy.
- 1590 7. Click **Save**.



- 1591
- 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.

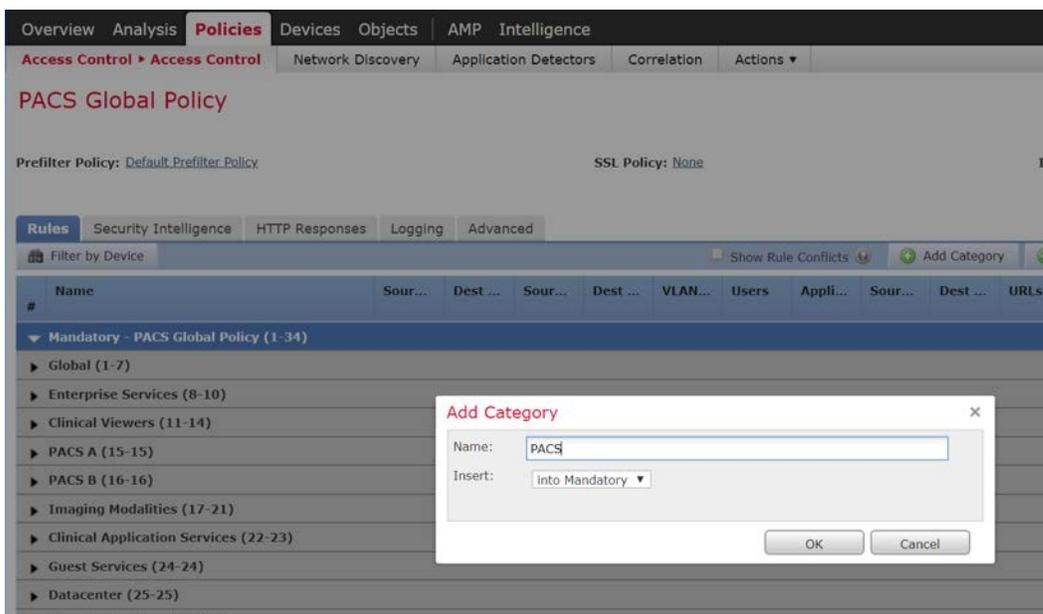
DRAFT



1595

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**.



1601

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.

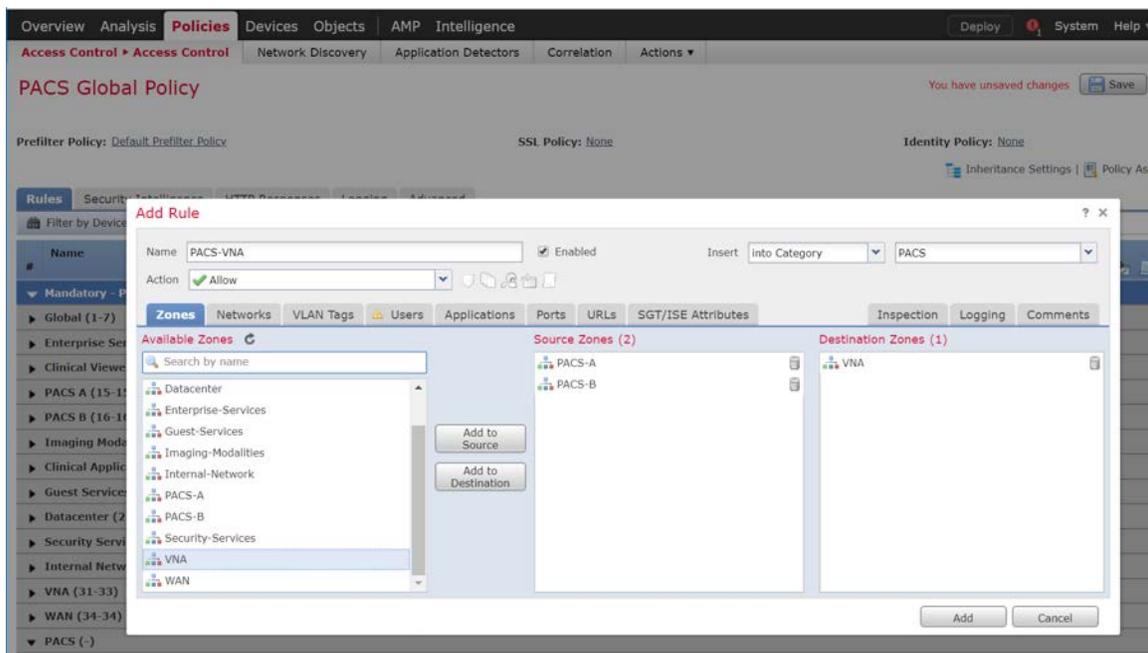
1605 3. Insert the rule into the category created in the previous step.

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**.

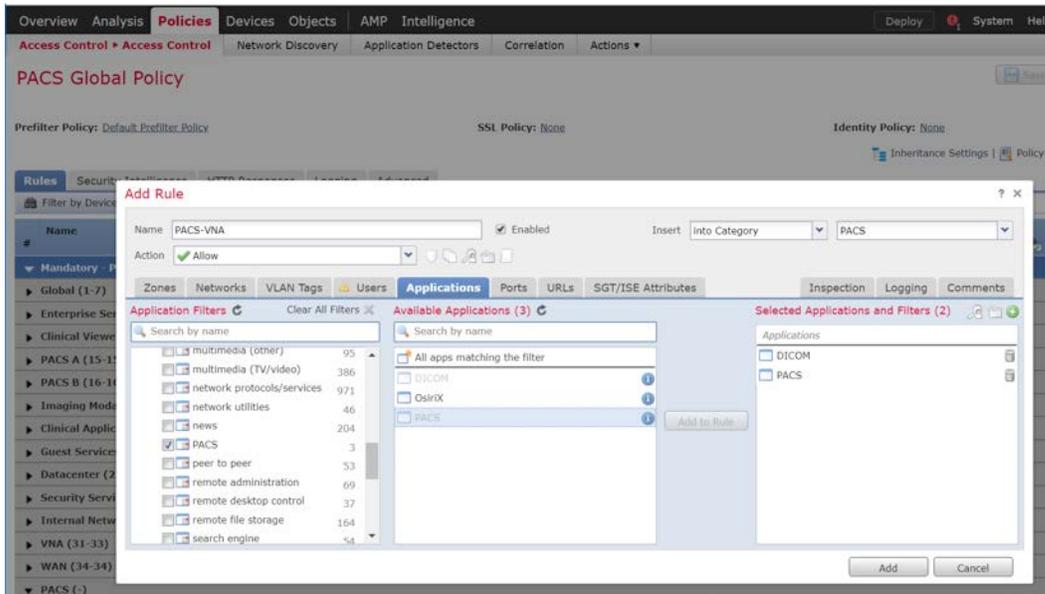
1610 Note: The two primary methods for adding source and destination networks to an access control
1611 rule are through security zones or networks. Security zones are objects that can contain multiple
1612 FTD interfaces. Networks can be different types of network objects, including network segments
1613 (**192.168.1.0/24**) or individual devices (**192.168.1.1**).



1614
1615 6. Under **Applications**, add the application(s) you would like to **allow** between the specified zones.

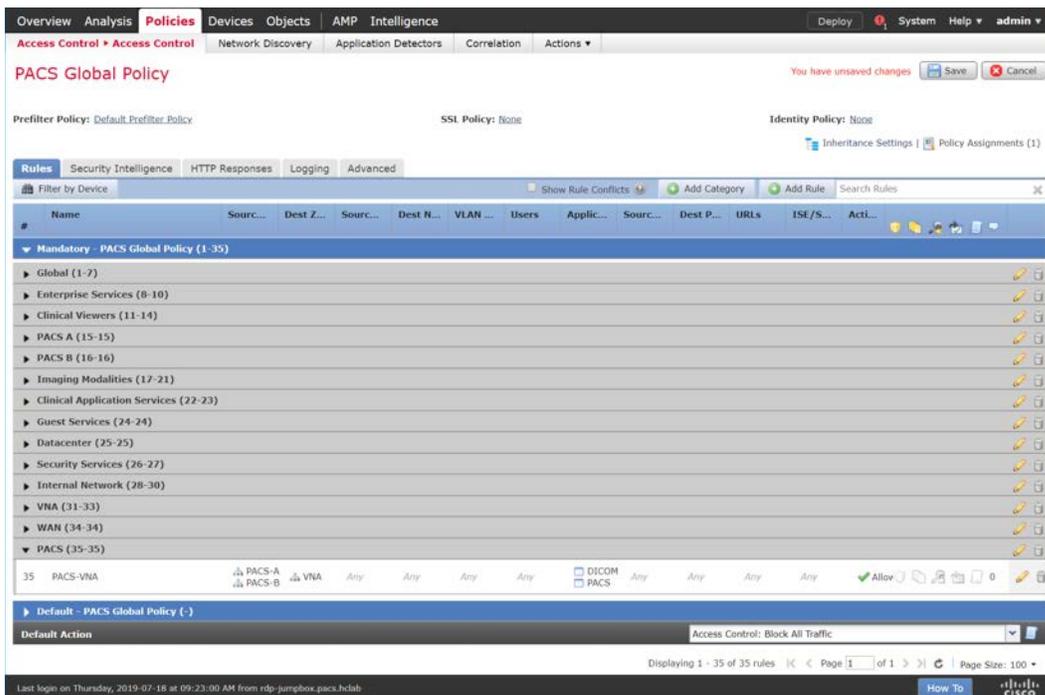
1616 Note: This can also be accomplished by specifying the **port** you would like to allow under the **Ports**
1617 tab. By specifying a specific port, this will open the port to all traffic regardless the type of traffic
1618 (e.g., DICOM) being sent.

1619 7. Click **Add**.



1620

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

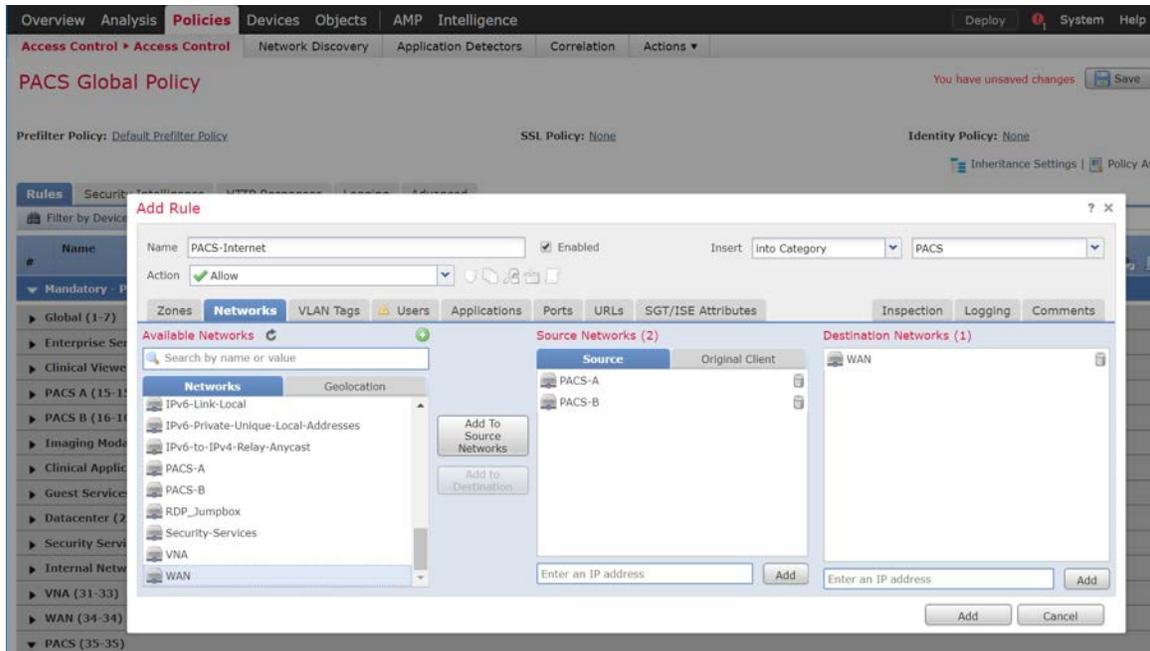


1622

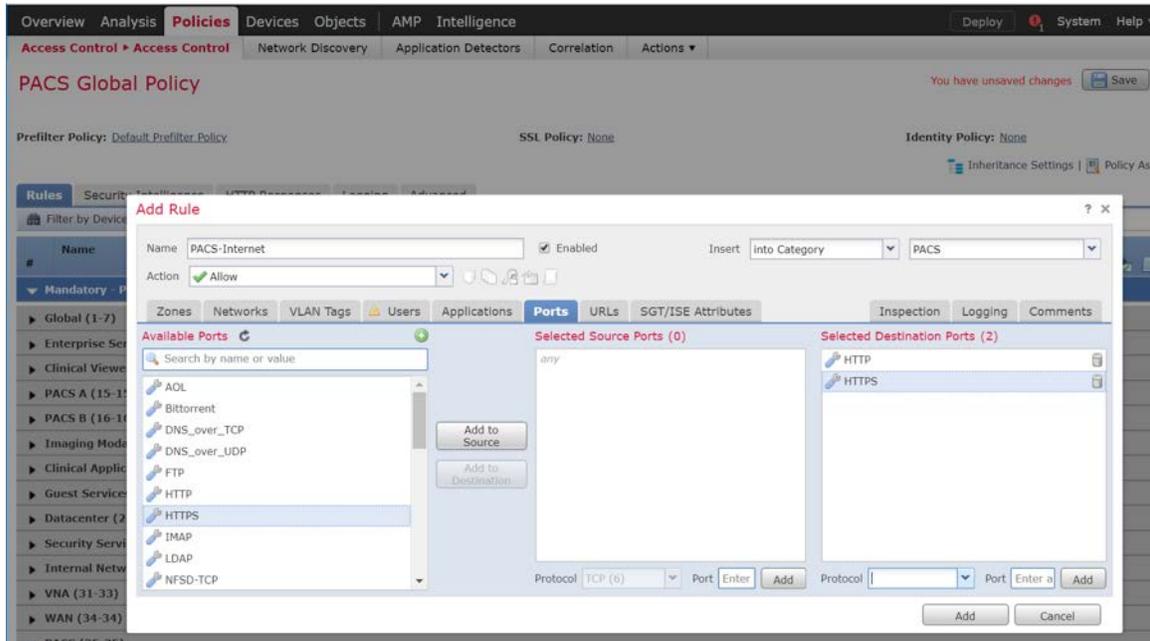
1623 **Create a rule that allows traffic on a specific port between networks**

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)**.



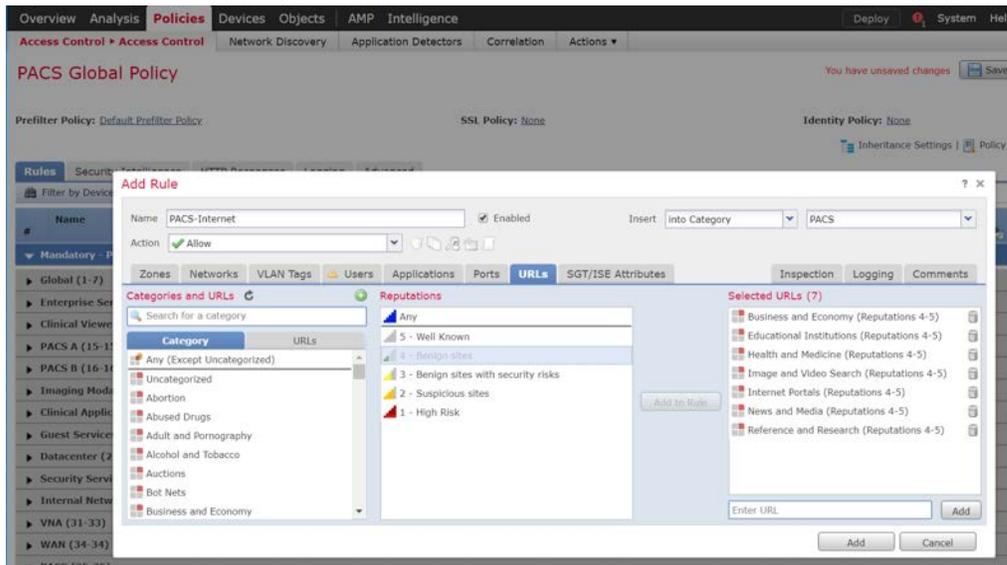
- 1629
- 1630 6. Under **Ports**, add a port(s) to the **Selected Destination Ports**.
- 1631 Note: Select from a group of pre-created ports or add your own port by filling out the **protocol** and
- 1632 **port** boxes, then click **Add** under the selected destination ports.



1633

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

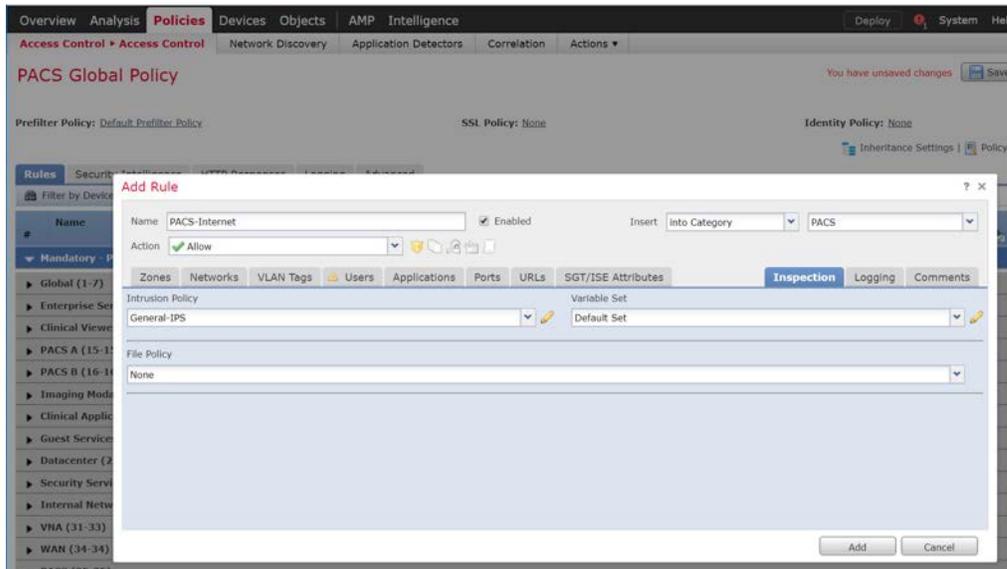
1635 Note: The URL categories are generated by Cisco Firepower and updated regularly. Within each
 1636 URL category, you can specify the reputation level the URL must meet in order for the rule to
 1637 match.



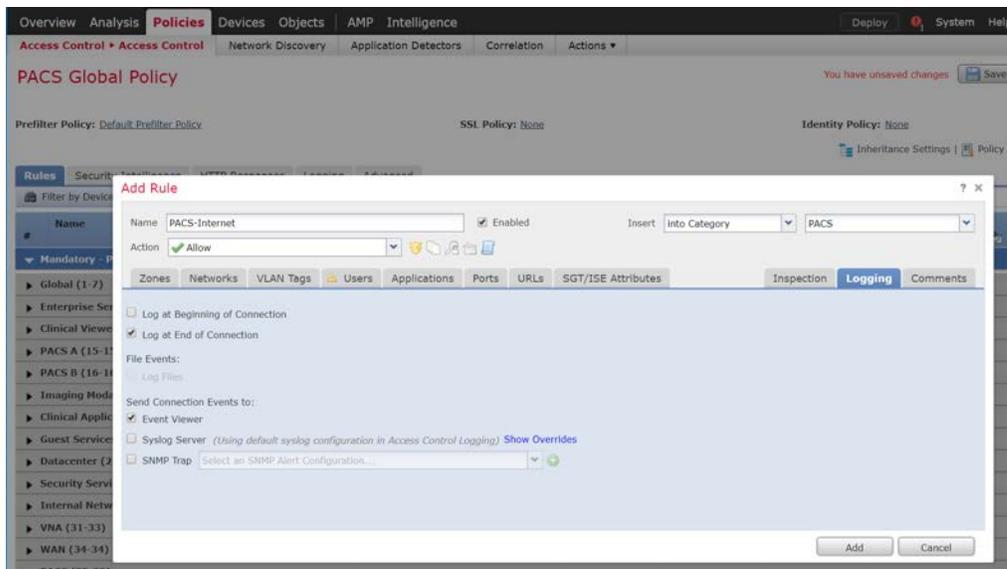
1638

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

1640 Note: Intrusion policies are created separately from the access-control policy. Once created, an
 1641 intrusion policy can be applied to a specific access-control rule or an entire access-control policy.
 1642 See the link posted [17] at the beginning of this section for more information on how to create and
 1643 use intrusion policies in Cisco Firepower.



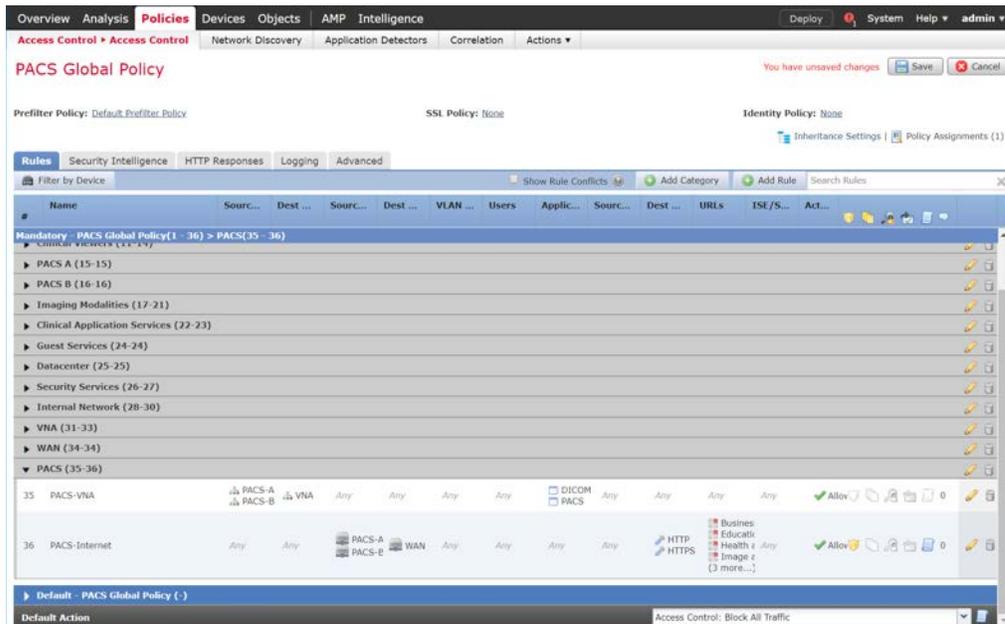
- 1644
- 1645 9. Under **Logging**, select **Log at End of Connection**, or leave this section blank.
- 1646 Note: If logging is enabled, select **Event Viewer**.
- 1647 10. Click **Add**.



1648

DRAFT

- 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.



1652

1653 2.7.2 Cisco Stealthwatch

1654 Cisco Stealthwatch provides network visibility and analysis through the use of network telemetry. It
1655 provides threat detection and remediation as well as network segmentation using machine learning and
1656 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 Cisco Stealthwatch Management Console Virtual Edition Installation Guide

1665 Install the Cisco Stealthwatch Management Console appliance according to the instructions detailed in
1666 the Cisco installation guide [18].

1667 **Cisco Stealthwatch UDP Director Appliance Information**

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 **Cisco Stealthwatch UDP Director Virtual Edition Installation Guide**

1675 Install the Cisco Stealthwatch UDP Director appliance according to the instructions provided at the Cisco
1676 installation guide [18].

1677 **Cisco Stealthwatch Flow Collector Appliance Information**

1678 **CPU:** 2

1679 **RAM:** 16 GB

1680 **Storage:** 60 GB (Thin Provision)

1681 **Network Adapter 1:** VLAN 1901

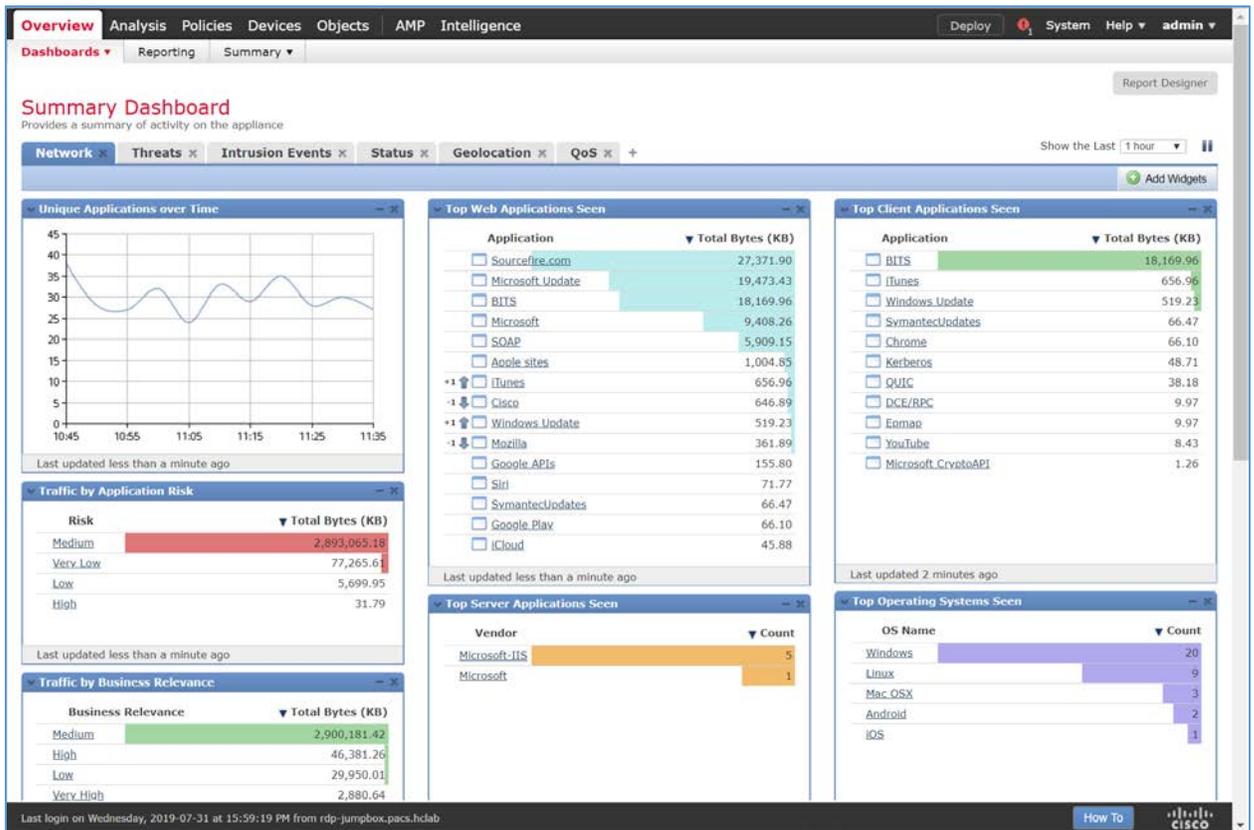
1682 **Operating System:** Linux

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].

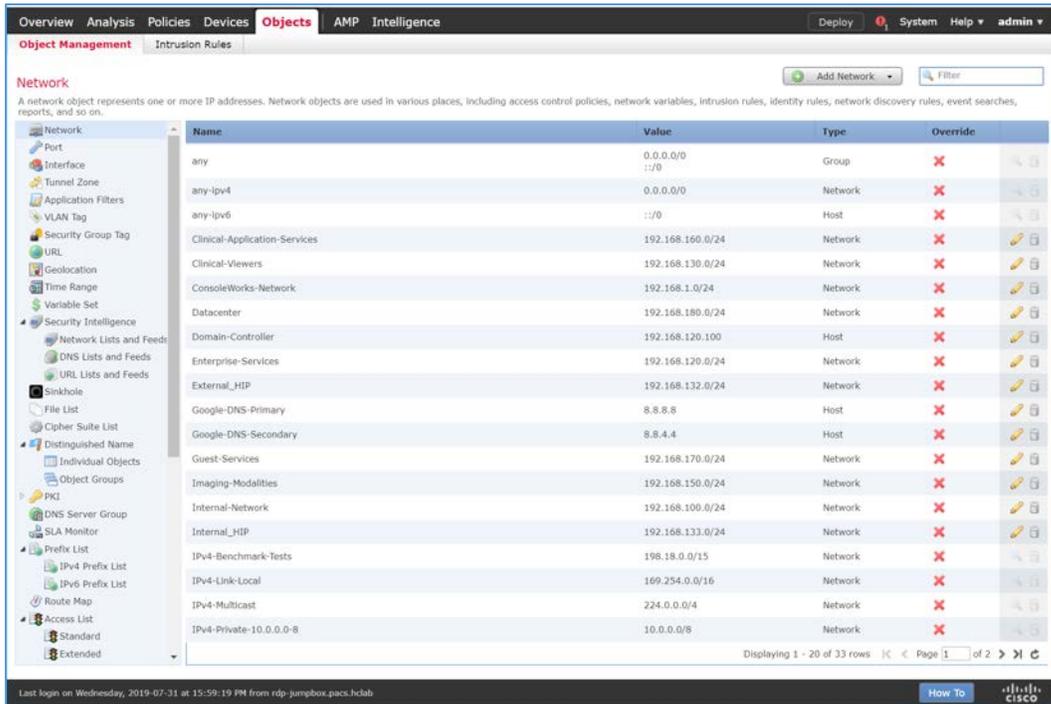
1686 **Configure NetFlow Parameters for Cisco Firepower**

1687 1. Log in to the Cisco Firepower Management Console.



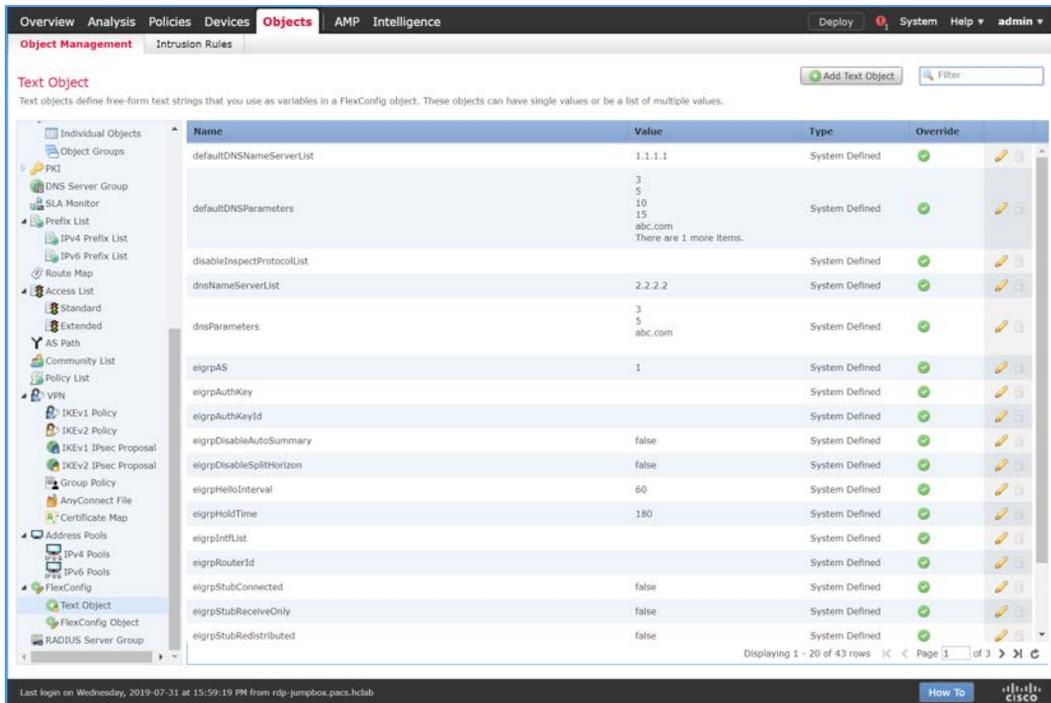
1688

1689 2. Navigate to **Objects**.



1690

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



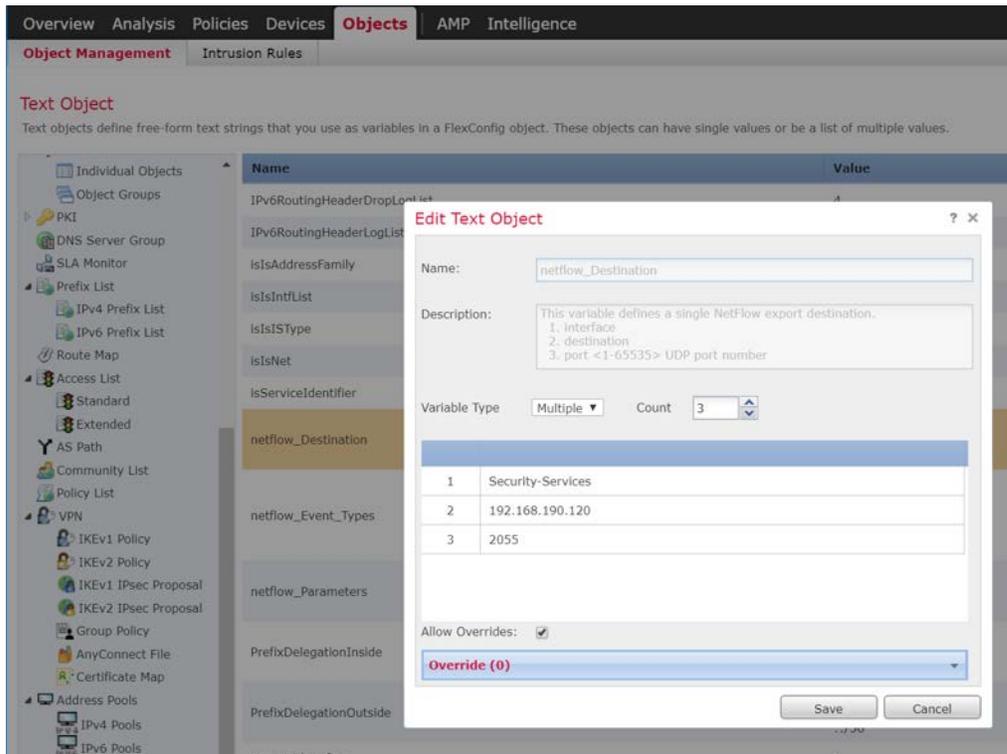
1692

- 1693 4. Under the **Name** column, find **netflow_Destination**.

The screenshot shows the Cisco FTD Object Management interface. The 'Text Object' section is active, displaying a table of objects. The 'netflow_Destination' object is highlighted in orange. The table columns are Name, Value, Type, and Override. The 'netflow_Destination' row has a Value of 'Security-Services 192.168.190.120 2055'.

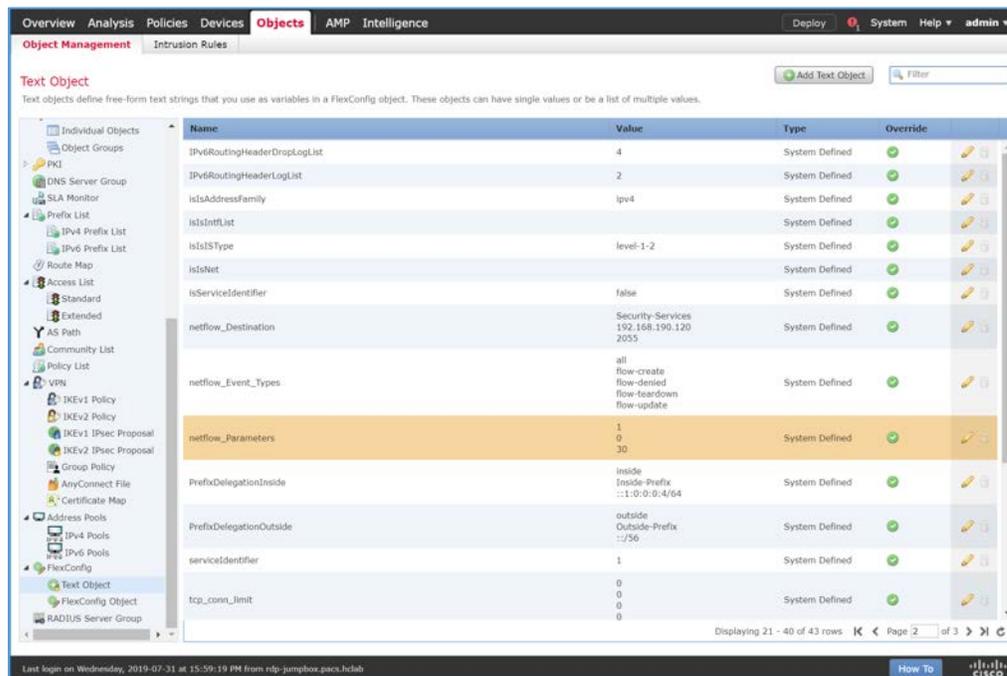
Name	Value	Type	Override
IPv6RoutingHeaderDropLogList	4	System Defined	✓
IPv6RoutingHeaderLogList	2	System Defined	✓
isisAddressFamily	ipv4	System Defined	✓
isisIntfList		System Defined	✓
isisISType	level-1-2	System Defined	✓
isisNet		System Defined	✓
isisServiceIdentifier	false	System Defined	✓
netflow_Destination	Security-Services 192.168.190.120 2055	System Defined	✓
netflow_Event_Types	all flow-create flow-denied flow-teardown flow-update	System Defined	✓
netflow_Parameters	1 0 30	System Defined	✓
PrefixDelegationInside	inside Inside-Prefix ::1:0:0:4/64	System Defined	✓
PrefixDelegationOutside	outside Outside-Prefix ::/56	System Defined	✓
serviceIdentifier	1	System Defined	✓
tcp_conn_limit	0 0 0 0	System Defined	✓

- 1694
- 1695 5. Click the **edit** icon for **netflow_Destination**.
- 1696 6. Set **Variable Type** to **Multiple**.
- 1697 7. Set **Count** to **3**.
- 1698 8. For **Row 1**, enter **Security-Service** to set the name of the Cisco FTD interface to which the Cisco
- 1699 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.
- 1701 10. For **Row 3**, enter **2055** to set a port from which the Cisco Stealthwatch UDP appliance will receive
- 1702 NetFlow traffic.
- 1703 11. Click **Save**.



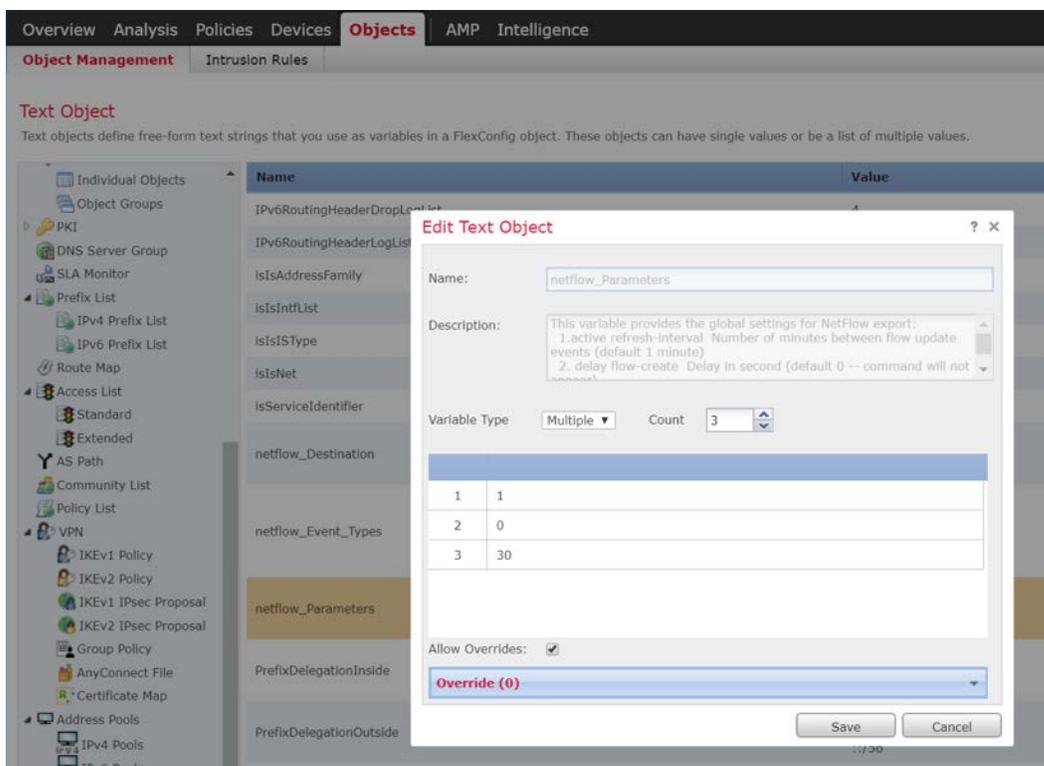
1704

1705 12. Under the **Name** column, find **netflow_Parameters**.



1706

- 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**.



- 1714
- 1715 20. Navigate to **Devices > FlexConfig**.



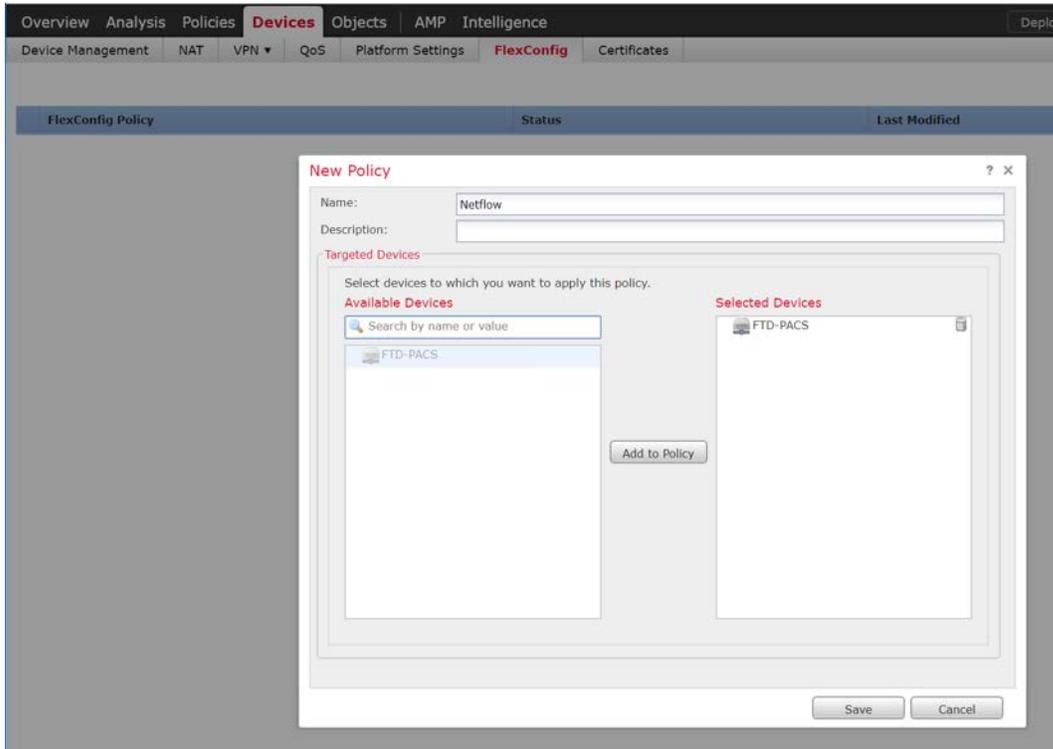
- 1716
- 1717 21. Click **New Policy**.

DRAFT

1718 22. Enter a **Name** (e.g., **Netflow**) for the policy.

1719 23. Under **Selected Devices**, add the Cisco FTD.

1720 24. Click **Save**.



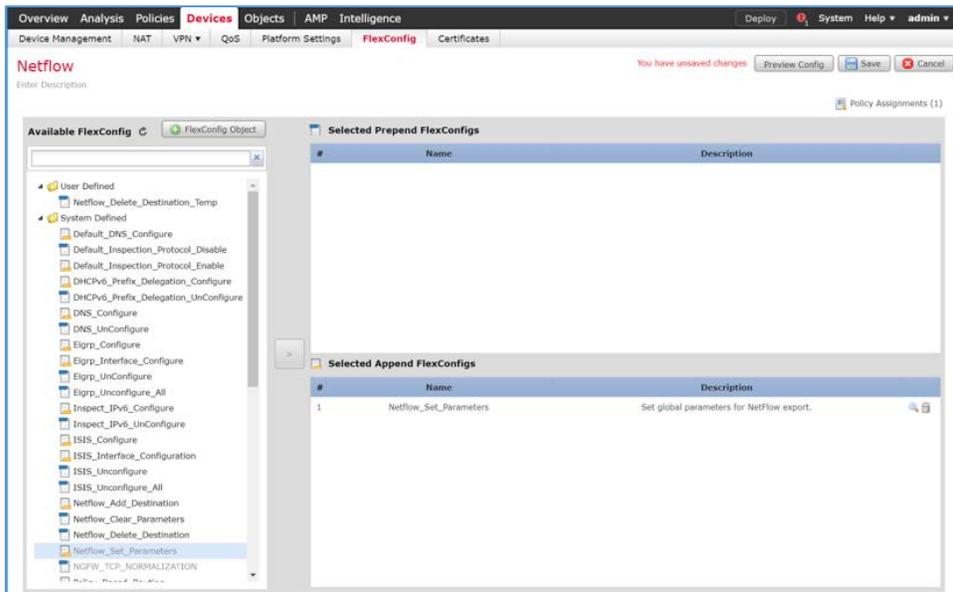
1721

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



1723

1724 26. Under **Available FlexConfig**, find **Netflow_Set_Parameters**, and add it to **Selected Append**
1725 **FlexConfigs**.

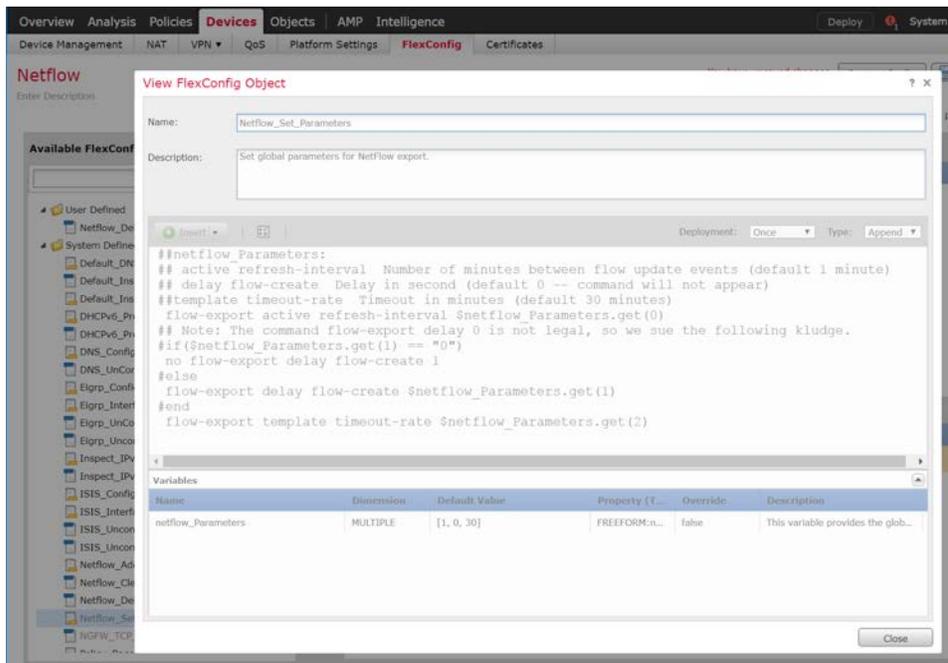


1726

1727 27. Click the **magnifier** icon for **Netflow_Set_Parameters**.

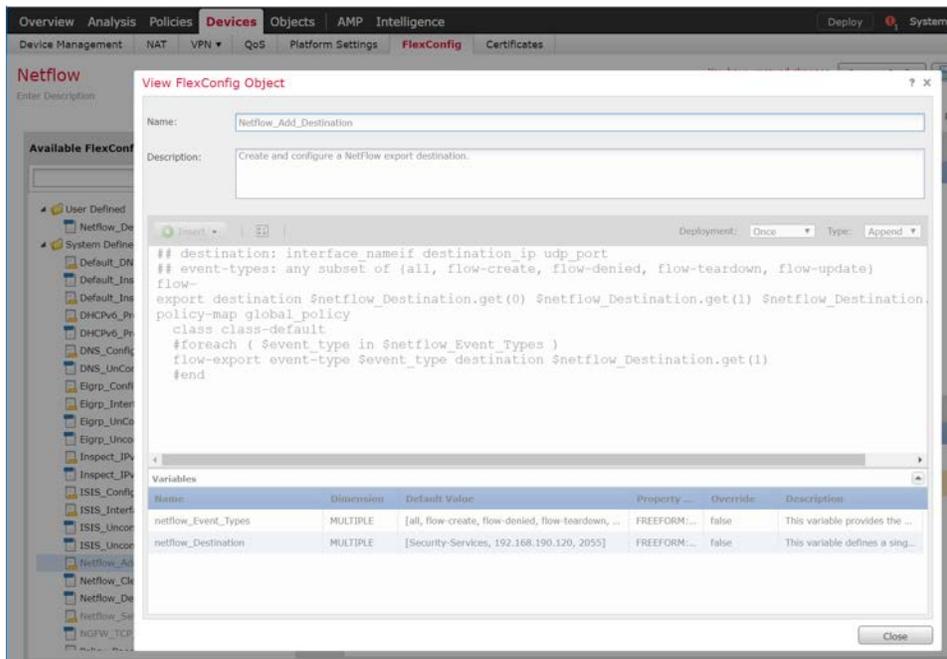
1728 28. Under **Variables > Default Value**, verify the minutes between flow data events, seconds to delay
 1729 flow create, and minutes for template timeout rate that were set for **netflow_Parameters**.

1730 29. Click **Close**.



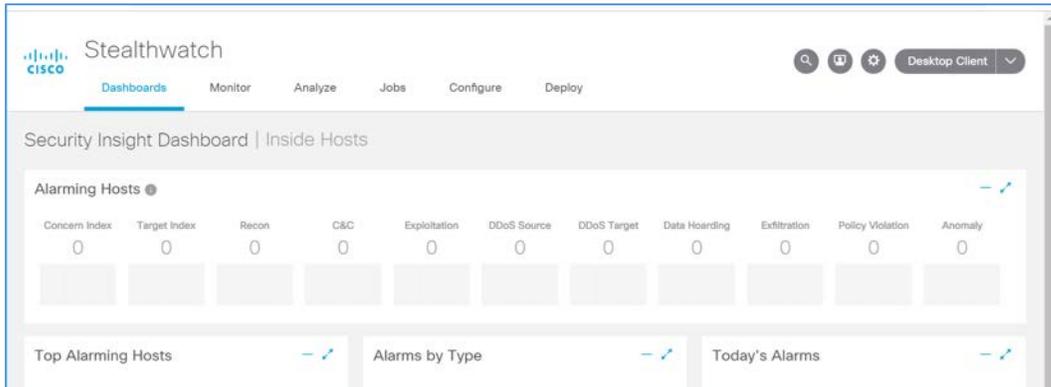
1731

- 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**.



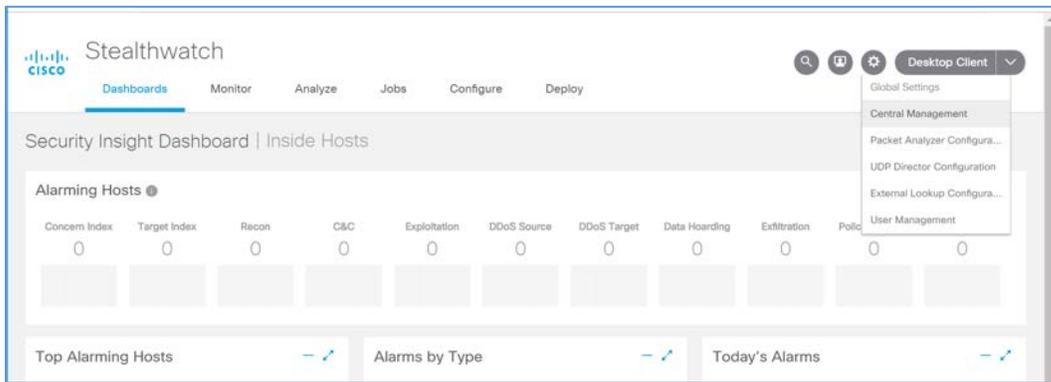
- 1738
- 1739 34. Click **Save**.
- 1740 35. Deploy changes to the Cisco FTD.
- 1741 **Forwarding Rules for Cisco Stealthwatch UDP Configuration**
- 1742 1. Log in to the web dashboard of the Cisco Stealthwatch Management Console.

DRAFT



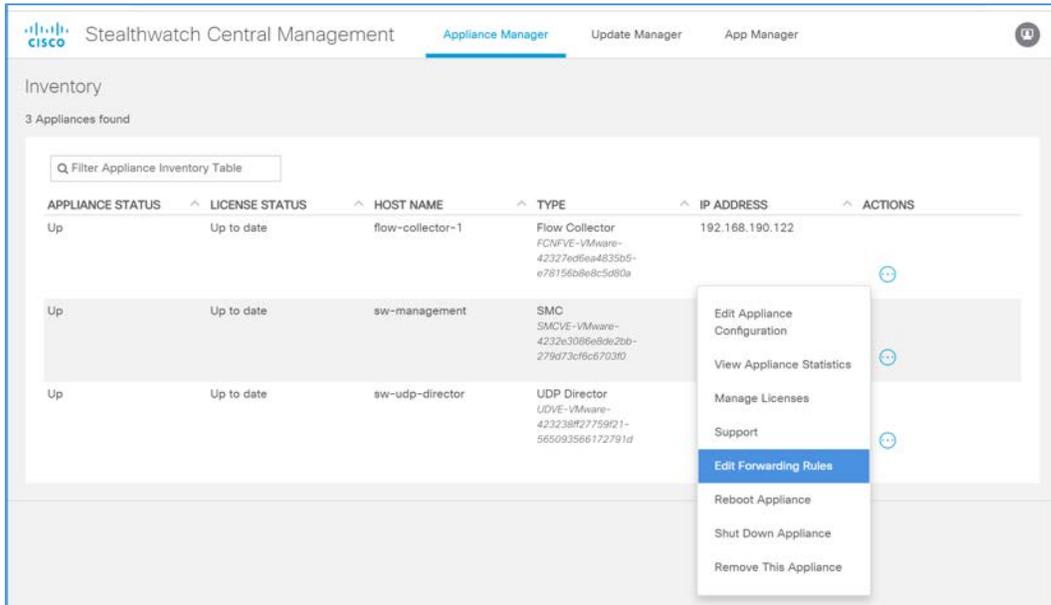
1743

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



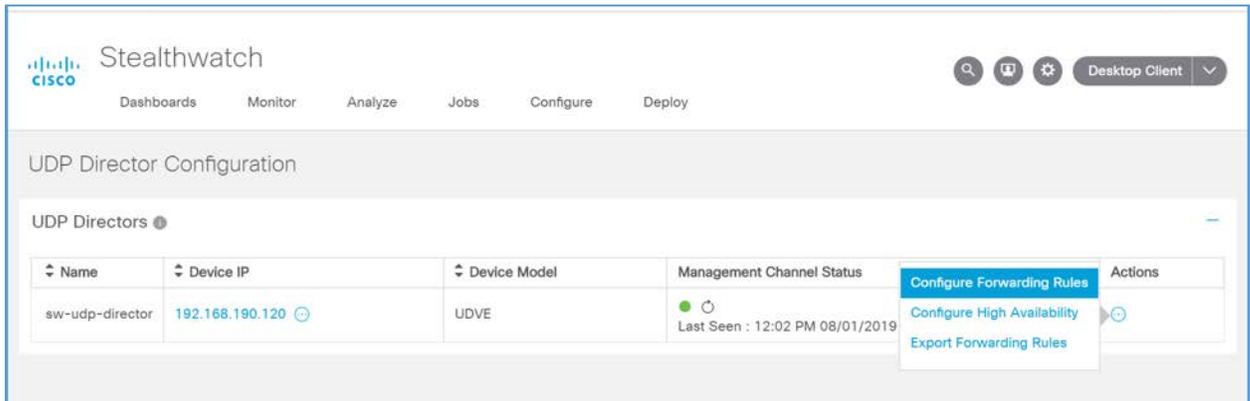
1745

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



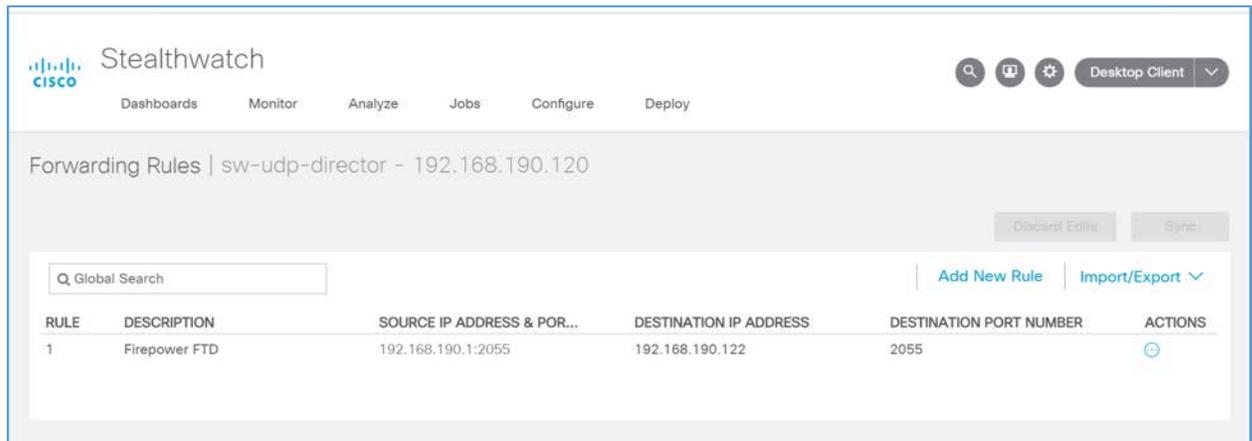
1747

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



1749

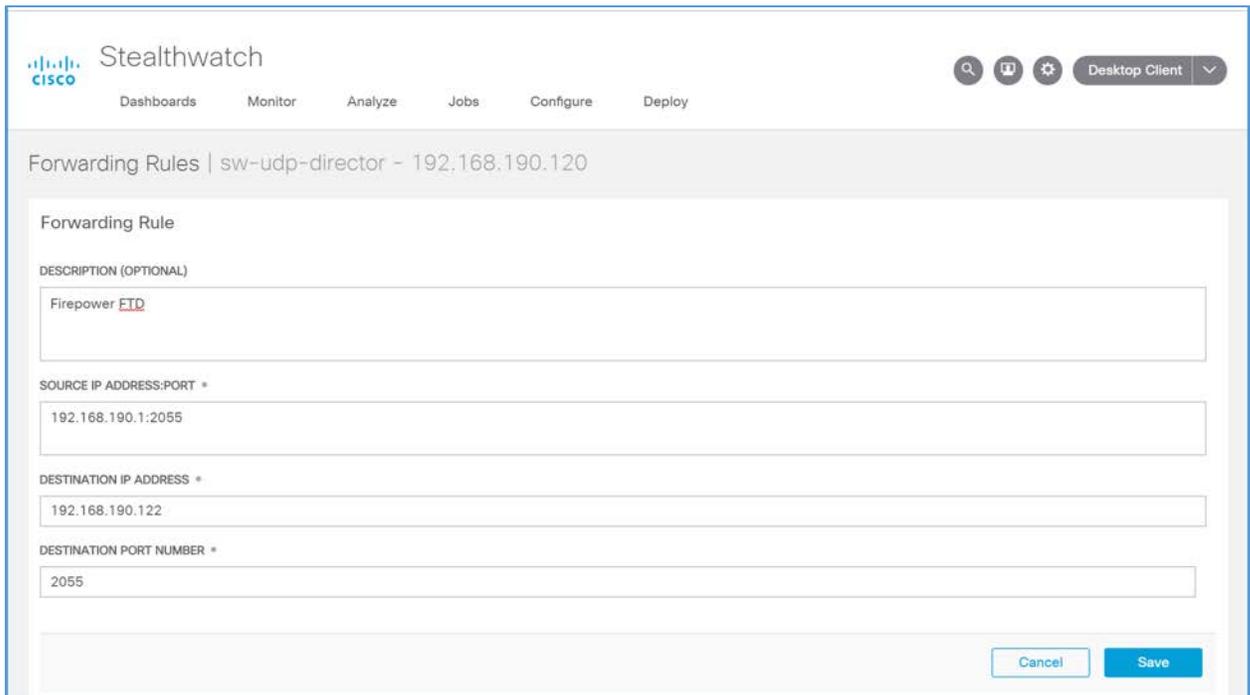
1750 5. Under **Forwarding Rules**, select **Add New Rule**.



1751

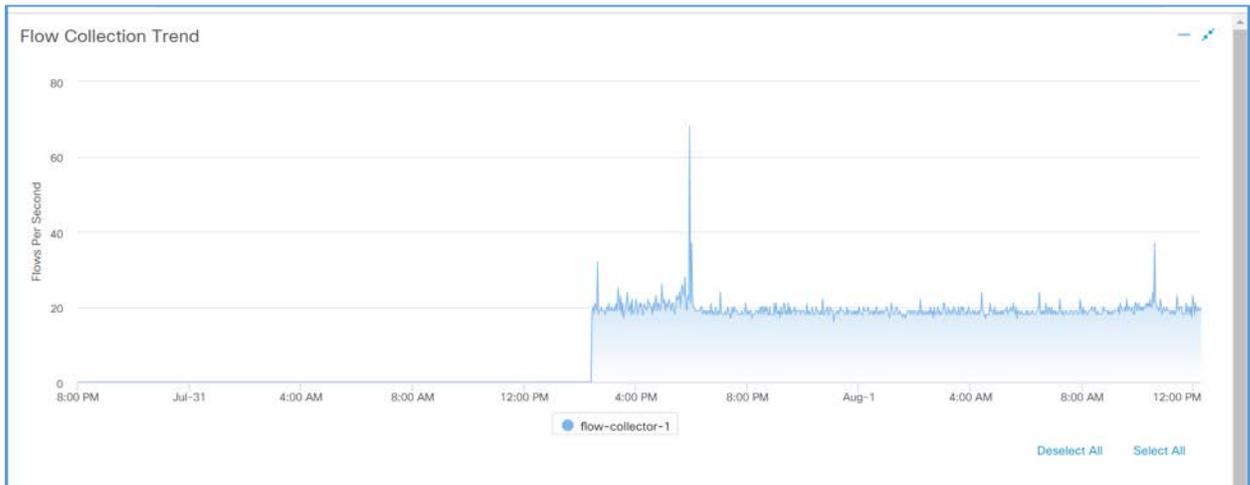
1752 6. Enter a description (e.g., **Firepower FTD**) for the rule.1753 7. For **source IP address** and **source port**, enter the IP address, and port (e.g., **192.168.190.1:2055**) of
1754 the Cisco FTD interface sending the NetFlow traffic.1755 Note: These parameters were established in Cisco FTD, found in the previous section, for the
1756 netflow_Destination object.1757 8. For **destination IP address**, enter the IP address (e.g., **192.168.190.122**) of the Cisco Stealthwatch
1758 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.



1761

- 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.



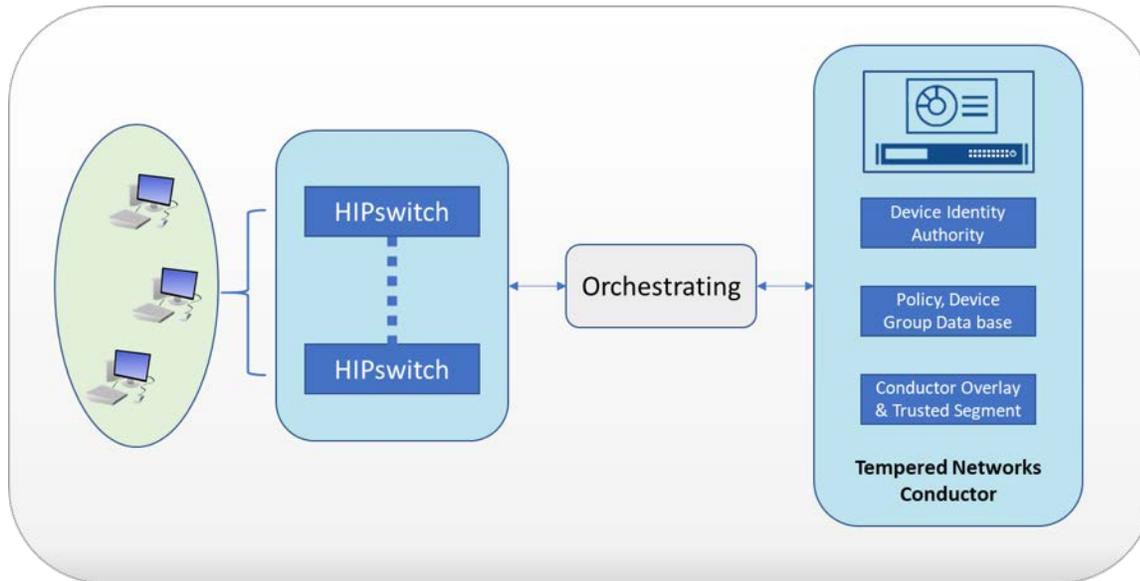
1765

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 in
 1774 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.

1777 HIPswitches are typically deployed in front of devices or hosts that cannot protect themselves, like
 1778 medical devices such as modalities and other legacy systems and machines, or when customers are
 1779 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**.
- 1793 3. Respond to the prompts with information specific to your deployment, including the ova package
1794 location, name and location, storage, networking and provisioning, etc.
- 1795 4. Click **Power On After Deployment**, and click **Finish**.
- 1796 5. Once the installation is done, power on the Conductor server and log in with username **macinfo**
1797 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**

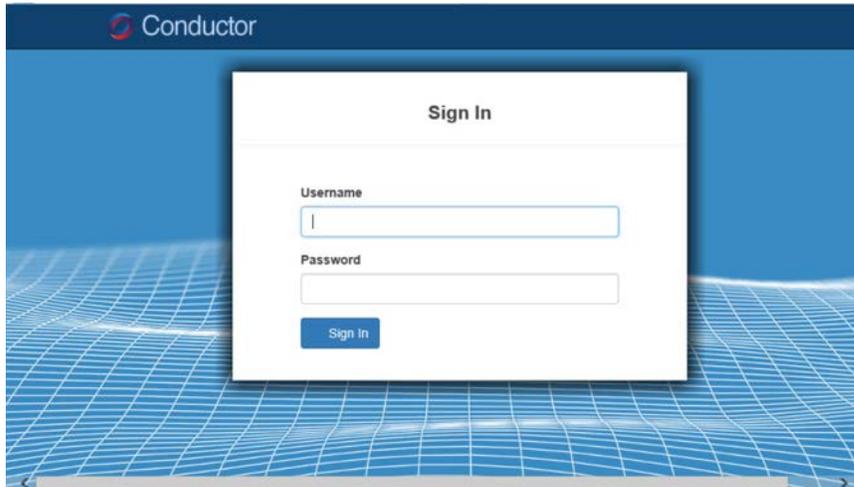
- 1806 1. Log in to the vSphere Client.
- 1807 2. Select **File > Deploy OVF Template**.
- 1808 3. Respond to the prompts with information specific to your deployment, including the ova package
1809 location, name and location, storage, networking and provisioning, etc.
- 1810 4. Click **Power On After Deployment**, and click **Finish**.
- 1811 5. After the installation, use the username **mapconfig** and the corresponding password to connection
1812 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 **Tempered Networks Conductor and HIPswitch Configuration**

DRAFT

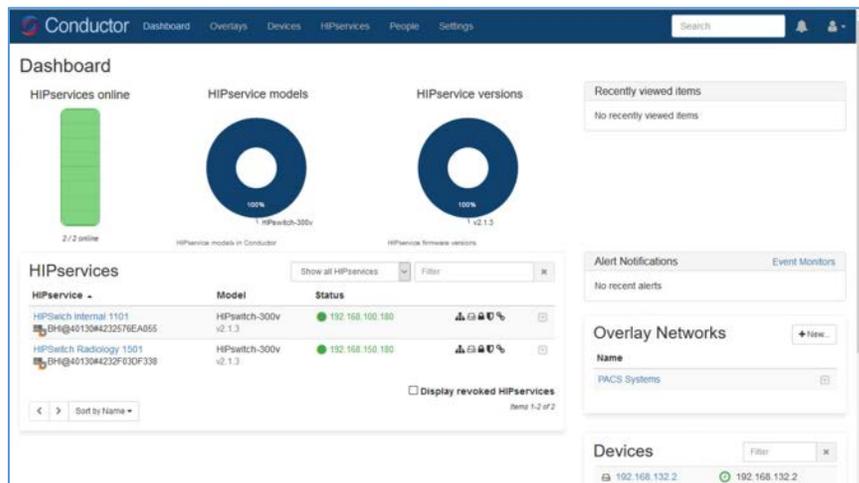
1817 The configuration for the Conductor and HIPswitches is done through the browser connected to the
1818 Conductor *https://ConductorIP*. Below is the log in page.

1819 1. Enter the **username** and **password** to open the Dashboard.



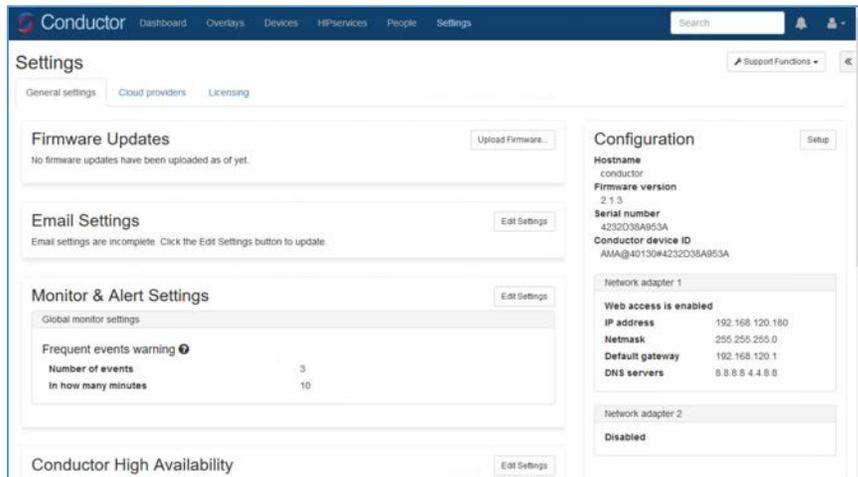
1820

1821 2. Click **Settings** tab.



1822

1823 3. From this page, you can set up license and perform the system setup. Click the **Setup** button to
1824 enter the system setup.



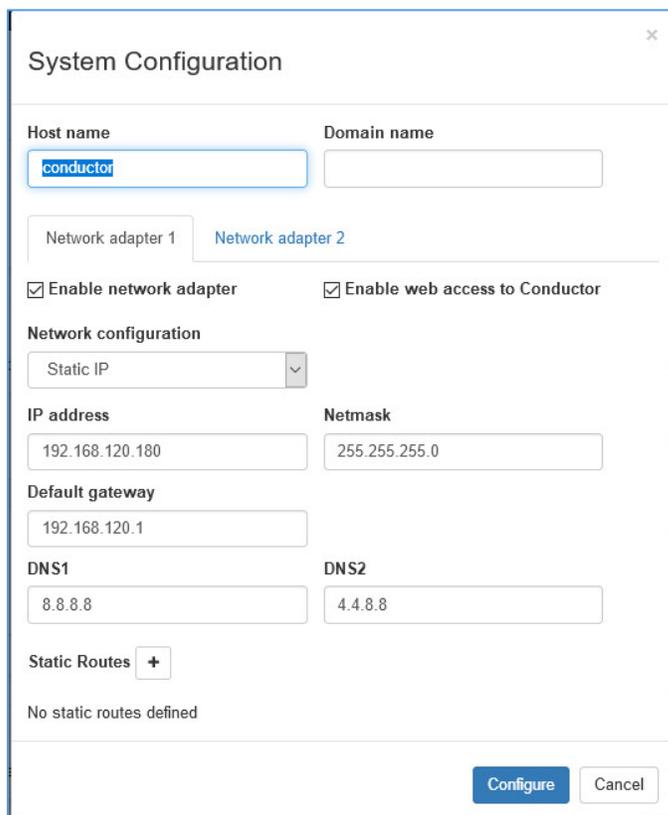
1825

1826

1827

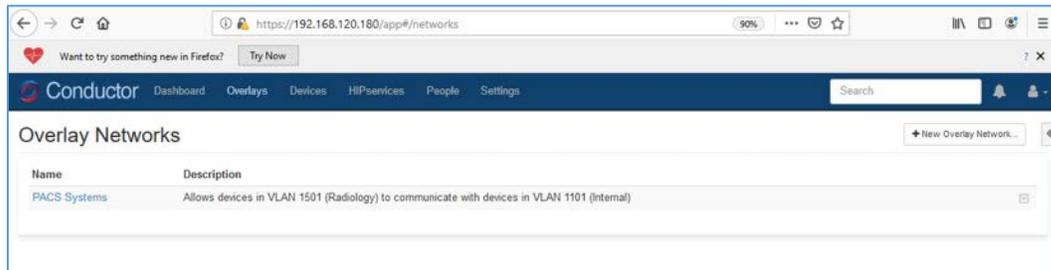
1828

4. Enter the proper network parameters for the **Conductor**, including the **IP address** (e.g., **192.168.120.180**), **Netmask** (e.g., **255.255.255.0**), **Default gateway** (e.g., **192.168.120.1**), and **DNS** (e.g., **8.8.8.8, 4.4.8.8**), then click **Configure**.

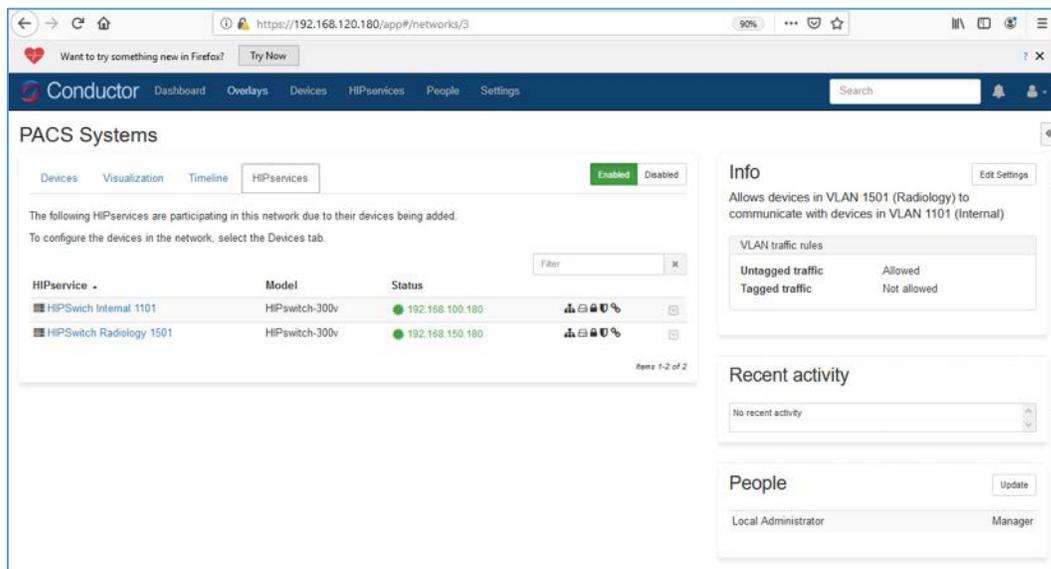


1829

- 1830 5. An Overlay is configured to support the microsegmentation. Click the **Overlay** tab to open the
 1831 following page, and you can add a new overlay by clicking the **+ New Overlay Network....** The page
 1832 below shows a configured overlay called **PACS Systems**.



- 1833
 1834 6. Two HIPswitches were installed to test for this project. These two HIPswitches are Model
 1835 HIPswitch-300v, and they are named **HIPswitch Internal** and **HIPswitch Radiology**. Both were
 1836 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
 - 1840 ■ VLAN 1302 for HIPswitch Internal 1101
 - 1841 ■ VLAN 1303 for HIPswitch Radiology 1501
 1842 8. Devices to be protected under the HIP network will be connected to these two HIPswitches
 1843 through the VLANs:
 1844
 - 1845 ■ PACS Servers are connected to VLAN 1302 under the HIPswitch Internal 1101
 - 1846 ■ 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 communicate
1850 with these two devices unless they are configured to do so.

1851 2.7.4 Zingbox IoT Guardian

1852 Zingbox IoT Guardian consists of two separate components that work together to monitor and analyze
1853 network traffic. The first component is a cloud-based platform called Zingbox Cloud, which aggregates
1854 and analyzes data to provide insights into the devices on the local network. The second component is
1855 Zingbox Inspector, a local appliance that receives network flows from devices on the local network and
1856 sends specific metadata to Zingbox Cloud for further analysis.

1857 **Zingbox Cloud Setup**

- 1858 1. Visit <https://zingbox.com> and register for an account.
- 1859 2. Log in to the Zingbox console and navigate to **Administration > My Inspectors > Download**
1860 **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)

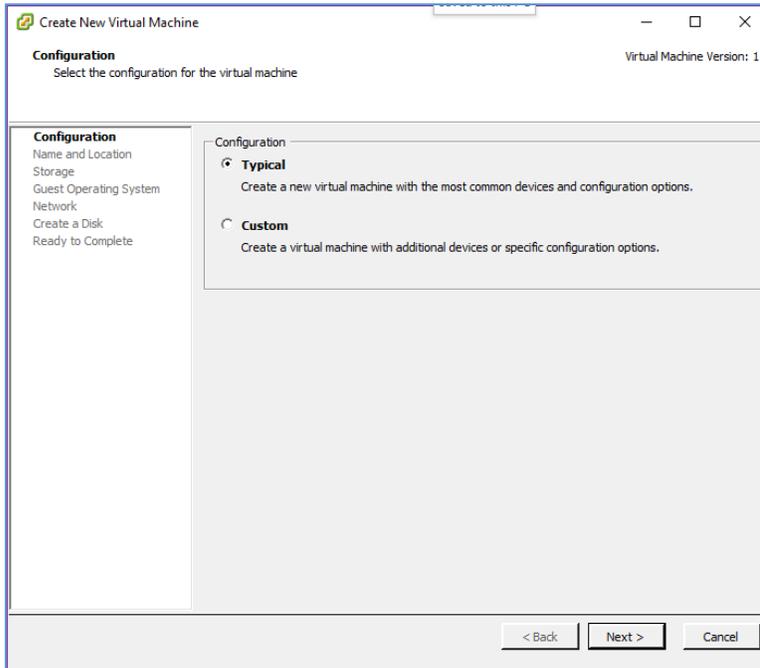
1866 **Operating System:** CentOS 7

1867 **Network Adapter 1:** VLAN 1101

1868 **Network Adapter 2:** Trunk Port

1869 **Zingbox Inspector Installation**

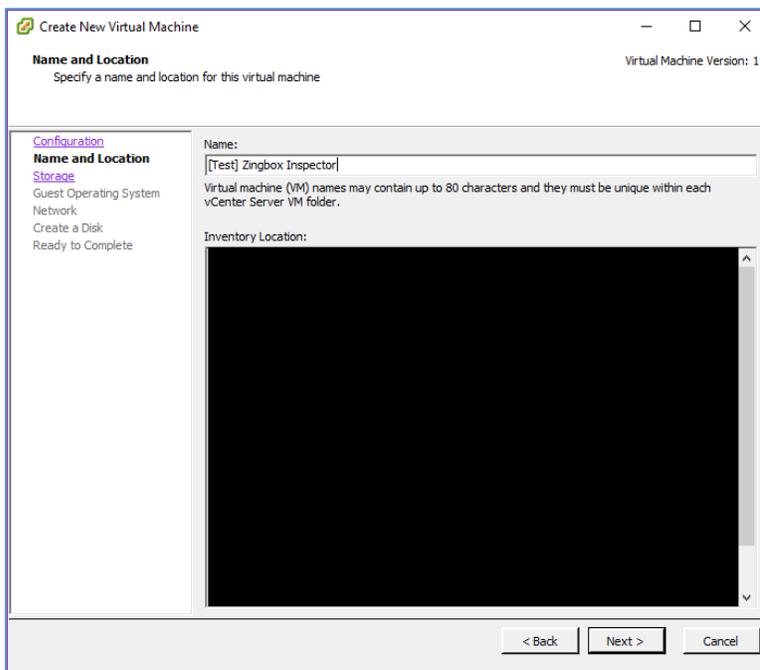
- 1870 1. Create a new virtual machine, and under **configuration** select **Typical**.
- 1871 2. Click **Next >**.



1872

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

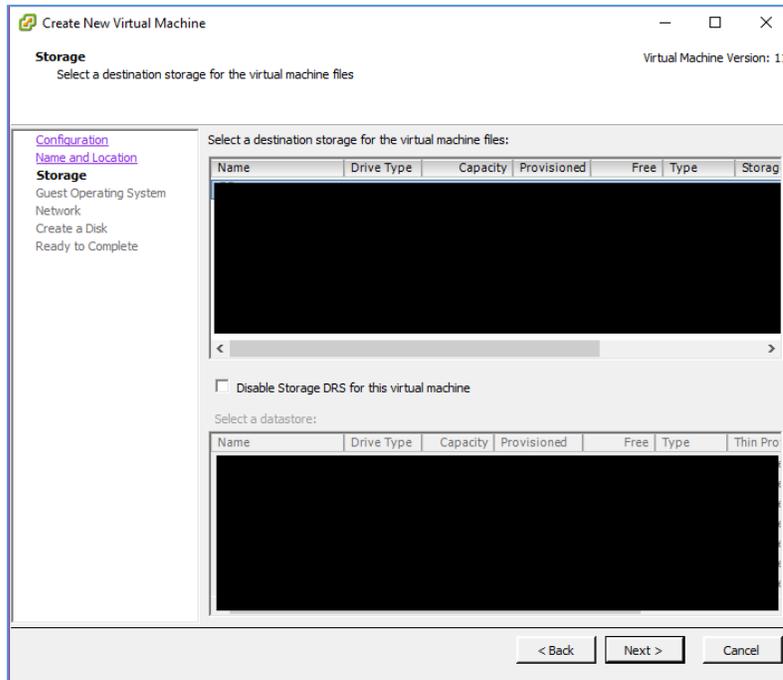
1874 4. Click **Next >**.



1875

1876 5. Select a **destination storage** for the VM.

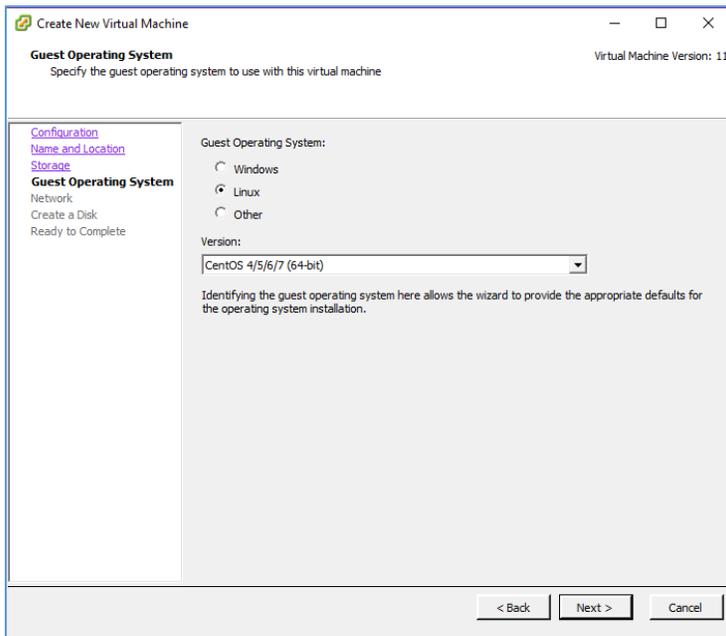
1877 6. Click **Next >**.



1878

1879 7. Check **Linux** and set version to **CentOS 4/5/6/7 (64-bit)**.

1880 8. Click **Next >**.

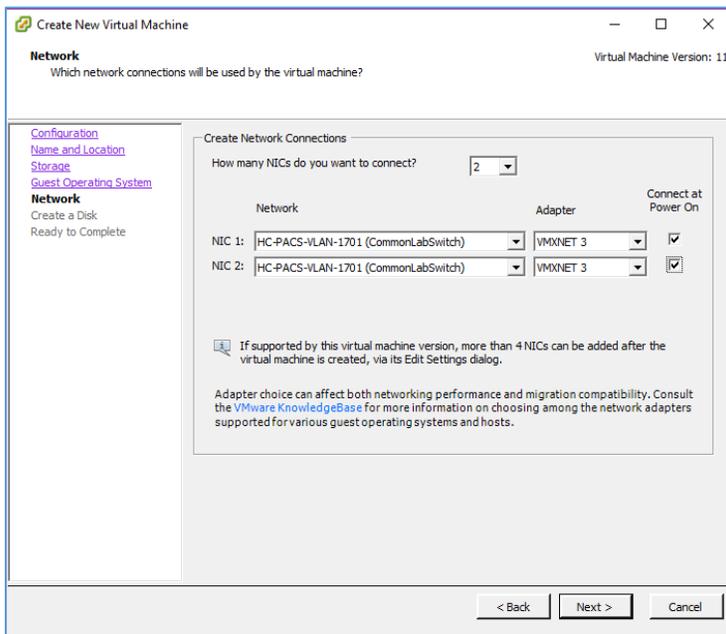


1881

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.

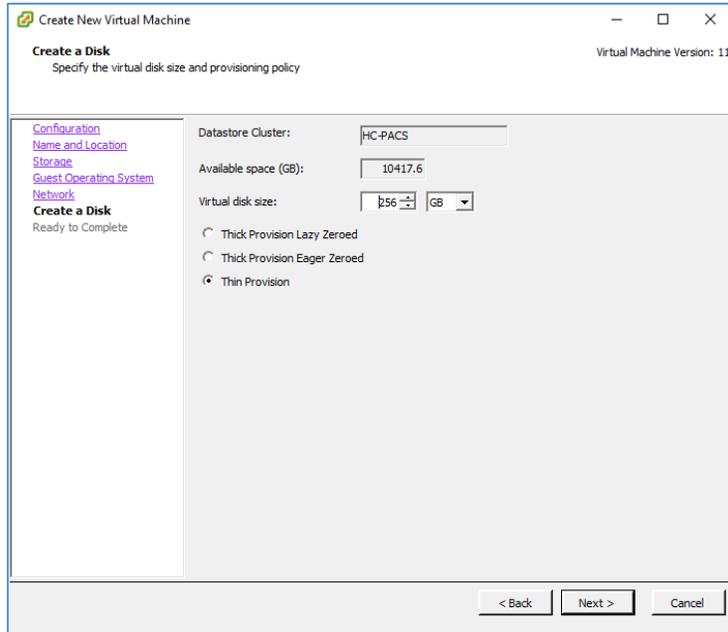
1884 11. Click **Next >**.



1885

1886 12. Set a **Virtual disk size** and **Provisioning method**.

1887 13. Click **Next >**.

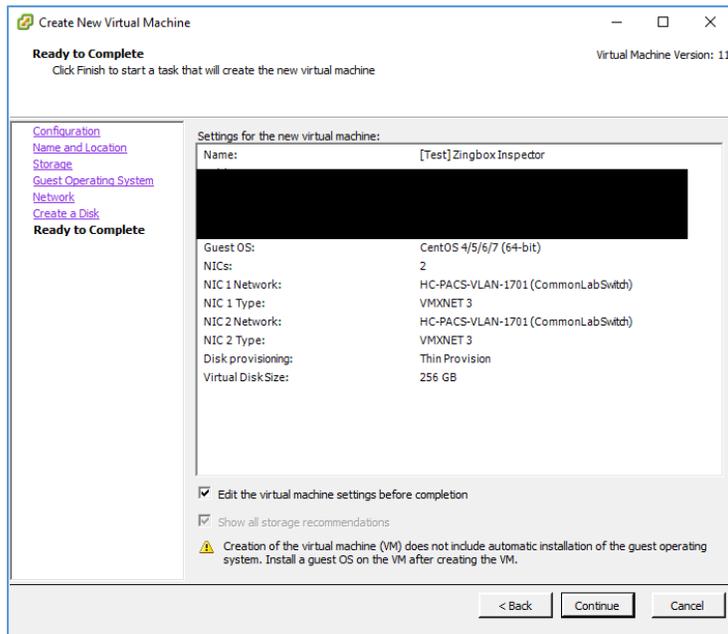


1888

1889 14. Verify virtual machine settings are correct.

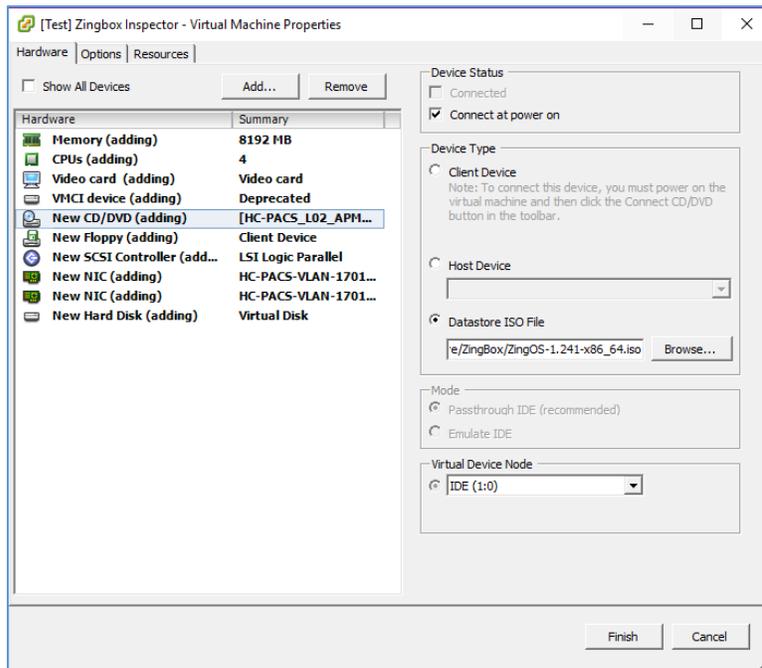
1890 15. Check **Edit the virtual machine settings before completion**.

1891 16. Click **Continue**.



1892

1893 17. Set **memory** to **8 GB**.1894 18. Set **CPUs** to **4**.1895 19. Under **New CD/DVD (adding)**, set these parameters:1896 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**.



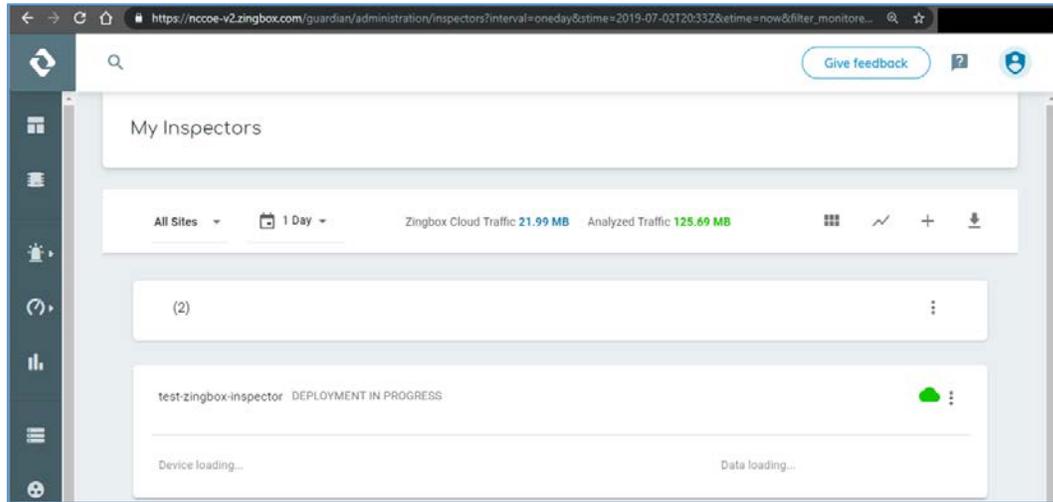
1899

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 connected
1906 (shown by the green cloud icon).



1907

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

- 1921 1. To begin installation, obtain the Forescout ISO. Load the Forescout ISO into the VM's CD/DVD drive.
 1922 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.

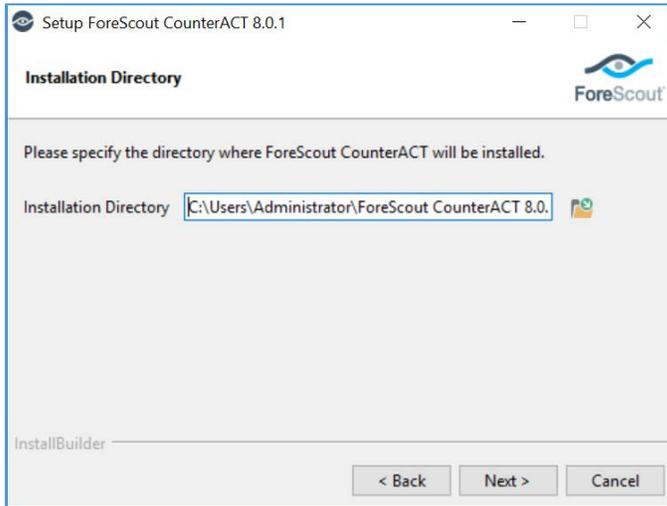
- 1927 6. Select **option 1** for standard installation.
- 1928 7. Press **enter** to proceed.
- 1929 8. Select **option 1** for CounterACT Appliance.
- 1930 9. Select **option 1** for Per Appliance Licensing Mode.
- 1931 10. Enter appliance **description**.
- 1932 11. Give appliance a **password**.
- 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 >**.



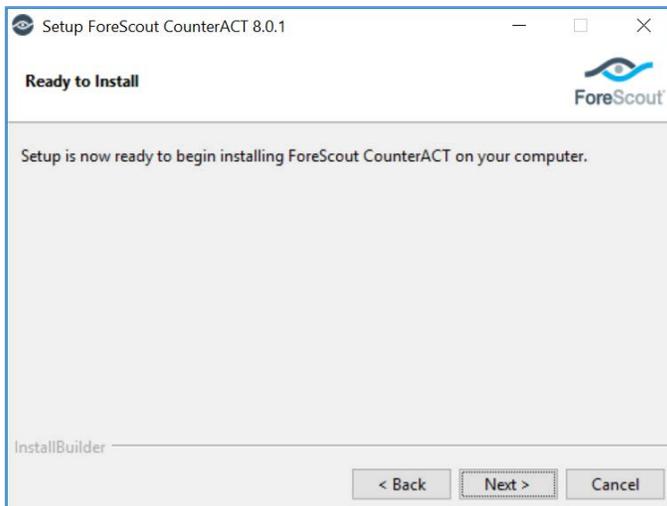
- 1944
- 1945 3. Verify **Installation Directory** as *C:\Users\Administrator\ForeScout CounterACT 8.0.1*; click **Next >**.



1946

1947

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

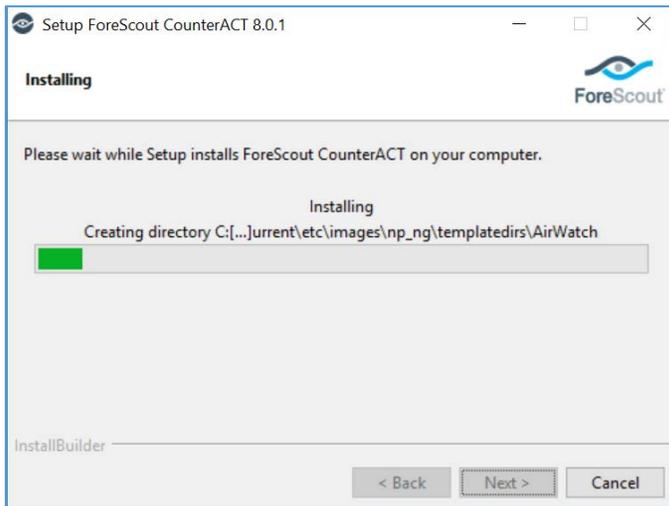


1948

1949

1950

5. 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.



1951

- 1952 6. As the installation nears completion, a screen indicating **Completing the ForeScout 8.0.1 Setup**
1953 **Wizard** appears. Check **Create Desktop shortcut**; click **Finish**.



1954

- 1955 7. Launch **Forescout CounterACT Console** and enter the information that follows, then click **Login**:
1956 a. Enter **192.168.120.160** in the **IP/Name** text box.
1957 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.



1960

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 SNMP
1966 parameters.

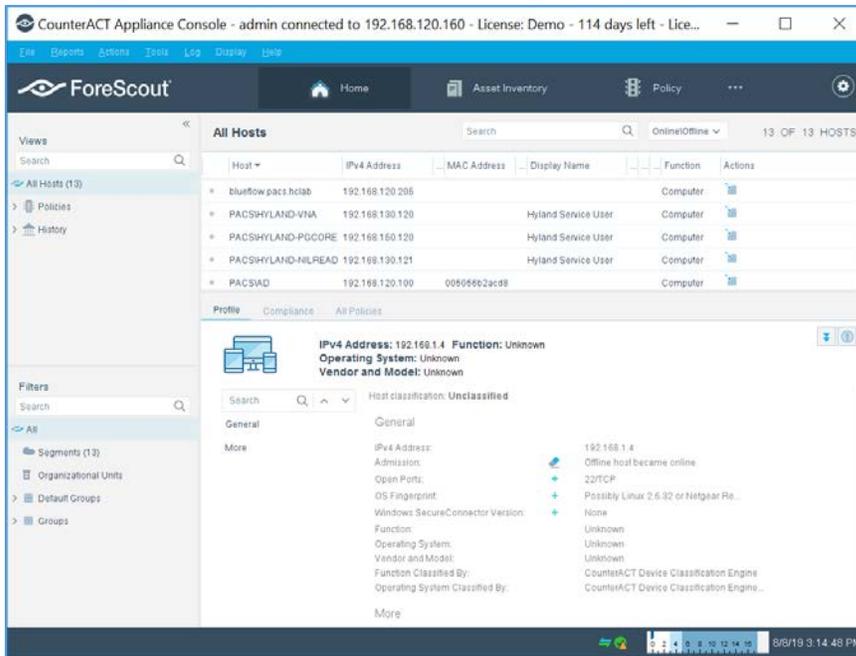
1967 After completing the installation, log in to the CounterACT Console using the steps below:

- 1968 1. Select **the CounterACT** icon from the server on which you installed the **CounterACT Console**. A log
1969 on page appears, as depicted below.



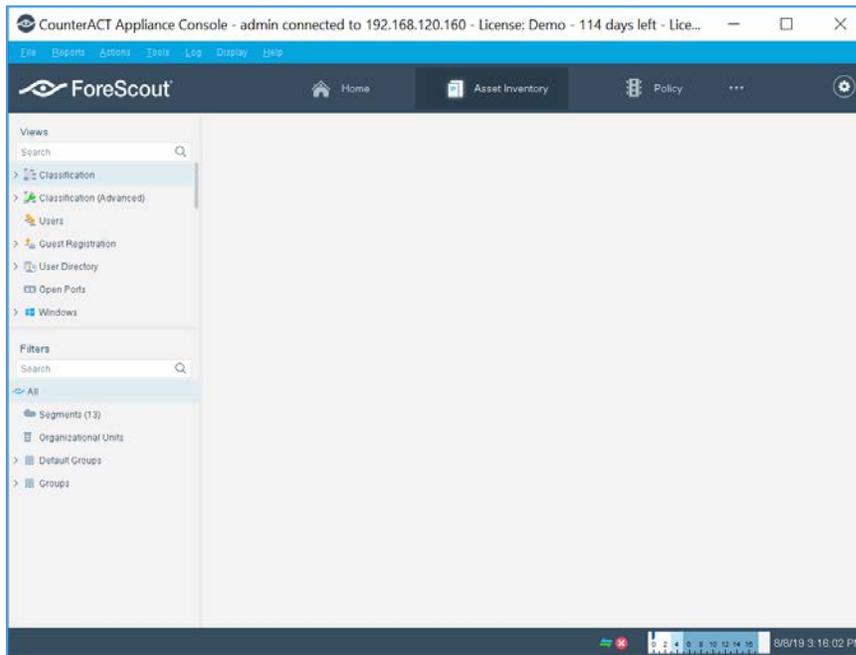
1970

- 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.
- 1973 b. In the **User Name** field, enter **admin**.
- 1974 c. In the **Password** field, enter the admin password which is defined during the installation.



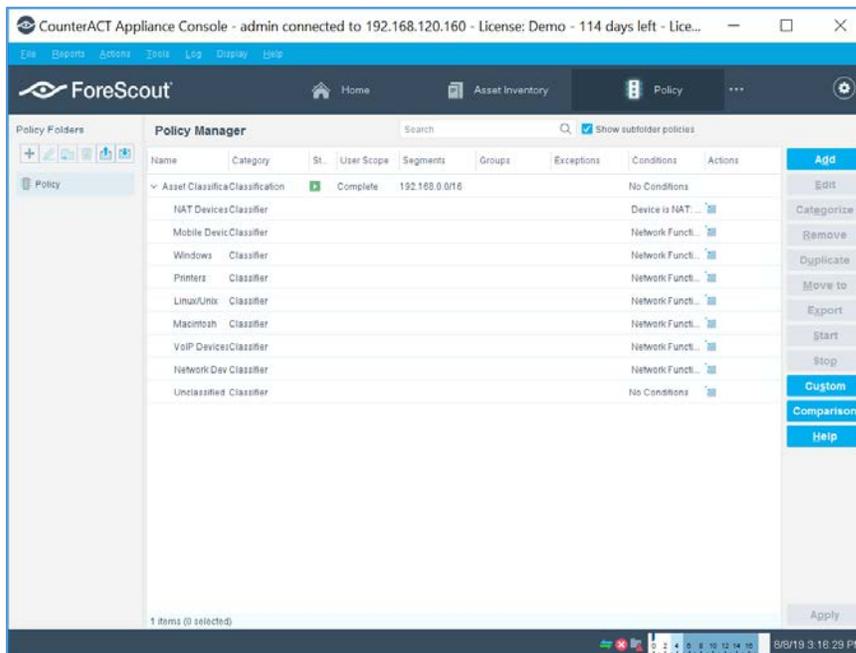
- 1975
- 1976 The console manager can be used to view, track, and analyze network activities detected by the
- 1977 appliance. It can also be used to define the threat protection, firewall, and other policies.
- 1978 The figure below shows the sample asset inventory page. (Further network configuration will be needed
- 1979 for complete inventory information.)

DRAFT



1980

1981 The figure below shows the sample **Policy Manager** page. Further network configuration and policy
1982 definition will be needed for complete policy information.



1983

1984 2.7.6 Symantec Endpoint Detection and Response (EDR)

1985 Symantec Endpoint Detection and Response performs behavioral analytics on endpoint events from
1986 Symantec Endpoint Protection, to identify potentially malicious behavior. It can sandbox impacted
1987 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.

1997 2. Enter default username **admin** and default password. You will be required to change the default
1998 password by entering a new password.

1999 3. After changing the default password, the bootstrap will automatically launch. Enter the following
2000 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

```

# If you have logged on to this system in error,      #
# please log off now.                                #
# Unauthorized access will be prosecuted.            #
#####
Change the admin password.

New password:
Re-enter new password:
Select one of the following appliance roles:
1) Management platform - The appliance acts as a management platform. In this
   role, network scanners can point to this appliance.
2) Network scanner - The appliance acts as a network scanner. In this role, the
   appliance must point to an existing management platform appliance.
3) All-in-one - Provides full Symantec EDR functionality,
   including the management platform and a network scanner. In this role, other
   network scanners cannot point to this appliance.
[]? 3
Configure the management port.

IPv4 address []: 192.168.190.170
IPv4 netmask []: 255.255.255.0
Gateway []: 192.168.190.1
Name server (IPv4) []: 192.168.120.100
Configure another nameserver? [y/n] n
Configure IPv4 static routes? [y/n] n
What do you want to call this device? EDR
Set NTP server []: ██████████

Role = 3 (All-in-one)
IPv4 address = 192.168.190.170
Netmask = 255.255.255.0
Gateway = 192.168.190.1
Nameserver1 = 192.168.120.100
Device name = EDR
NTP server = ██████████
Save changes? [y/n] y
-

```

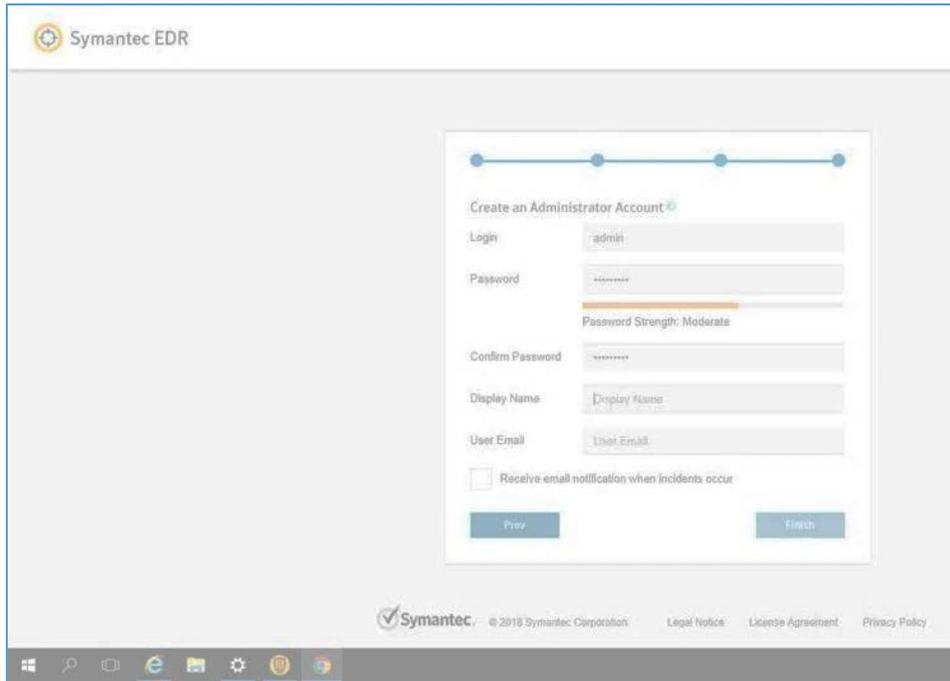
2012

2013

2014

2015

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



2016

2017

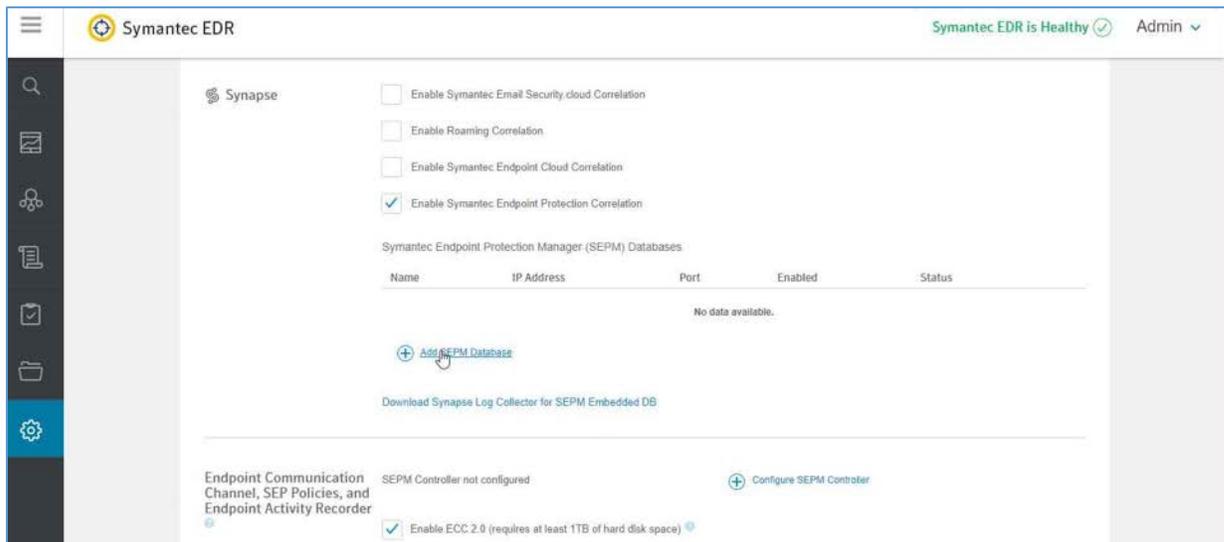
7. Select the **Settings** menu, and then select the **Global** sub-menu.

2018

8. Ensure **Enable Symantec Endpoint Protection Correlation** is checked.

2019

9. Select **Add SEPM Database** and enter the following options.

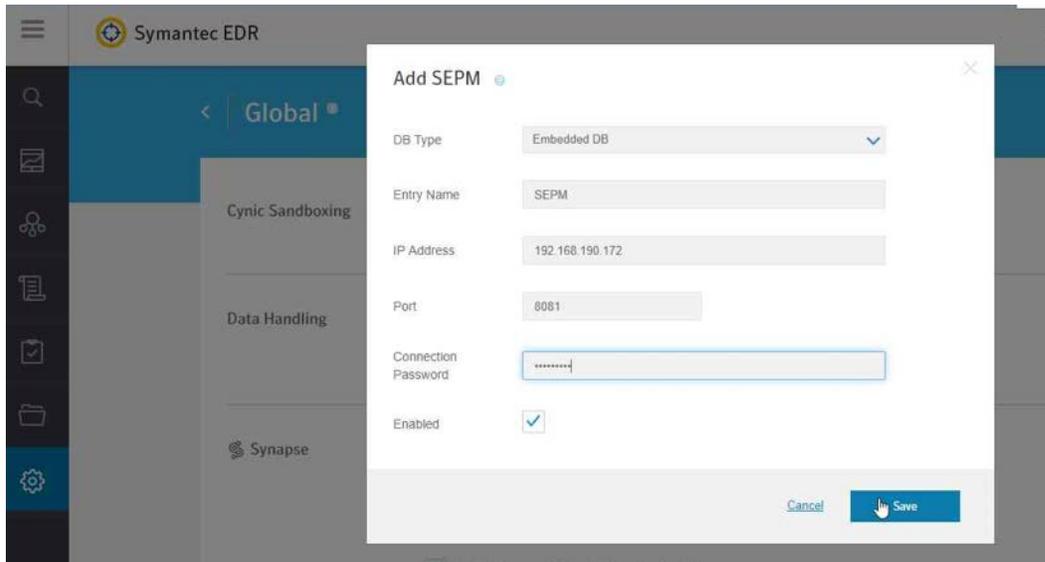


2020

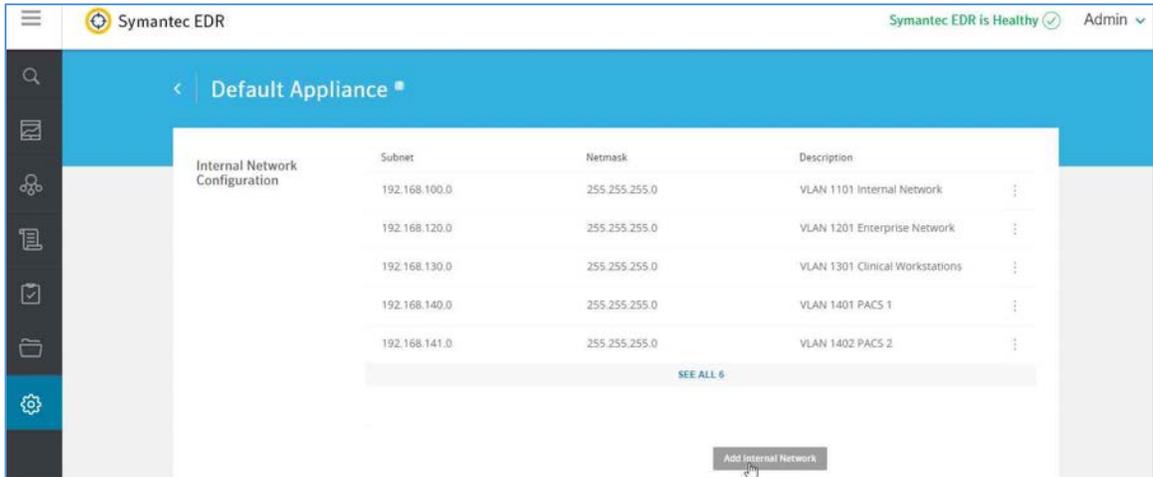
2021

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***
- 2027 ■ **Enabled: *Checked***



- 2028
- 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.



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**

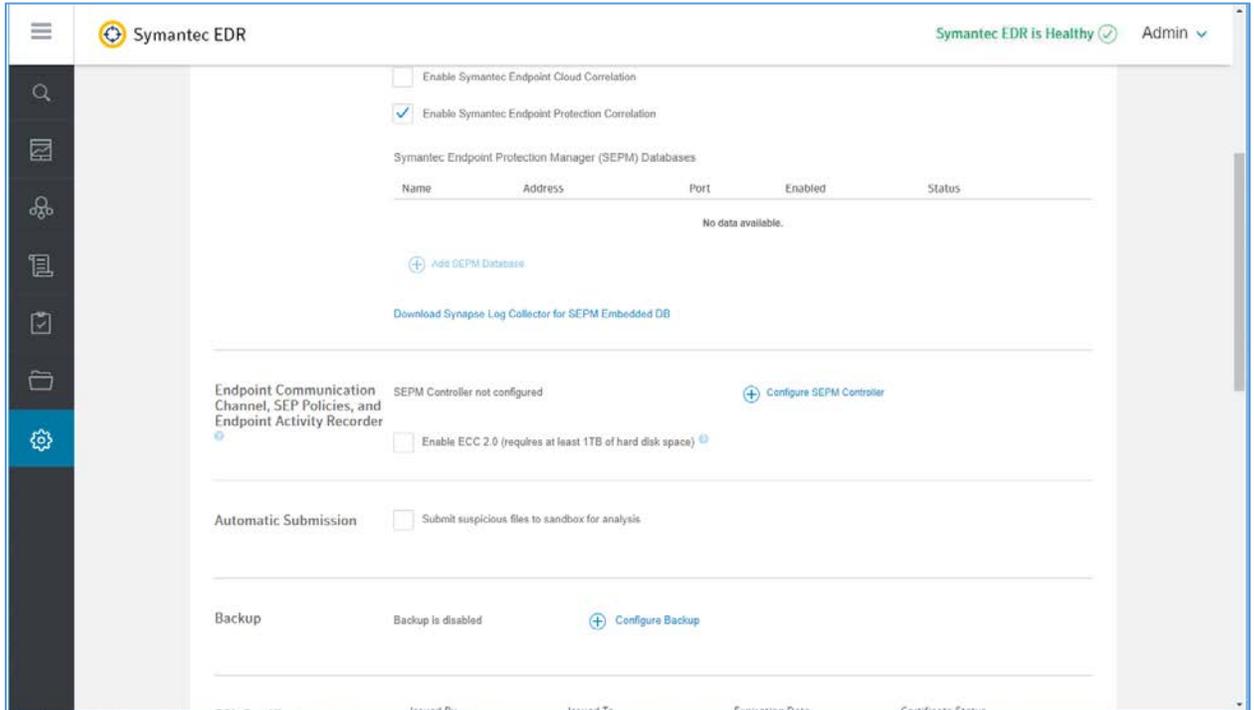
The screenshot shows a detailed view of the 'Internal Network Configuration' table. The table has three columns: 'Subnet', 'Netmask', and 'Description'. The rows in the table are:

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
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
192.168.160.0	255.255.255.0	VLAN 1601 Clinical Application Services

2044

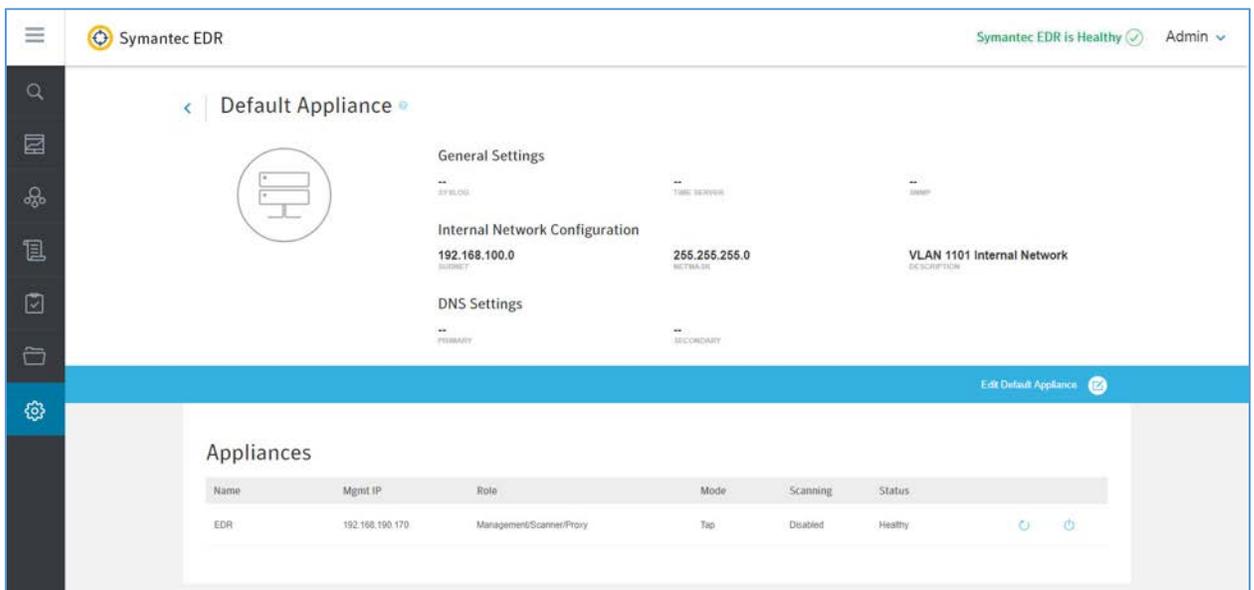
2045 14. Select **Settings** and then **Global**.

- 2046 15. Uncheck **Enable ECC 2.0** under **Endpoint Communication Channel, SEP Policies and Endpoint**
2047 **Activity Recorder**.



2048

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



2050

2051 17. Select **EDR** from the appliances list.

2052 18. Turn **Scanning** on under the **Network Interface Settings**.

2053 **Symantec EDR and SEP Correlation**

2054 1. Open a web browser and travel to the virtual appliance at *https://192.168.190.170*. Log in with
2055 your administrator account.

2056 2. From the settings menu, select **global settings**.

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 **Next** to use the default settings.

2061 7. After installation is complete, launch the **Log Collection** for **SEPM** embedded database
2062 configuration utility, and enter the values below:

2063 ■ **Service Hostname (optional):** *Leave blank*

2064 ■ **Service IP address:** **192.168.190.172**

2065 ■ **Service port:** **8082**

2066 ■ **Log Collector connection password:** *enter connection password*

2067 ■ **Confirm connection password:** *enter connection password again*

2068 ■ **SEPM embedded database configuration password:** *enter embedded database password*

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

Log Collector for SEPM embedded database configuration utility

Log Collector service settings:

Service Hostname (optional):

Service IP address: 192.168.190.172

Service port: 8081

Log Collector connection password:

Confirm connection password:

SEPM embedded database configuration:

Password:

Configuration Status:

2070

2071 2.8 Endpoint Protection & Security

2072 2.8.1 Symantec Data Center Security: Server Advanced (DCS:SA)

2073 Symantec DCS:SA utilizes a software agent to provide various server protections, including application
 2074 whitelisting, intrusion prevention, and file integrity monitoring. For this project, a DCS:SA agent was
 2075 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**.

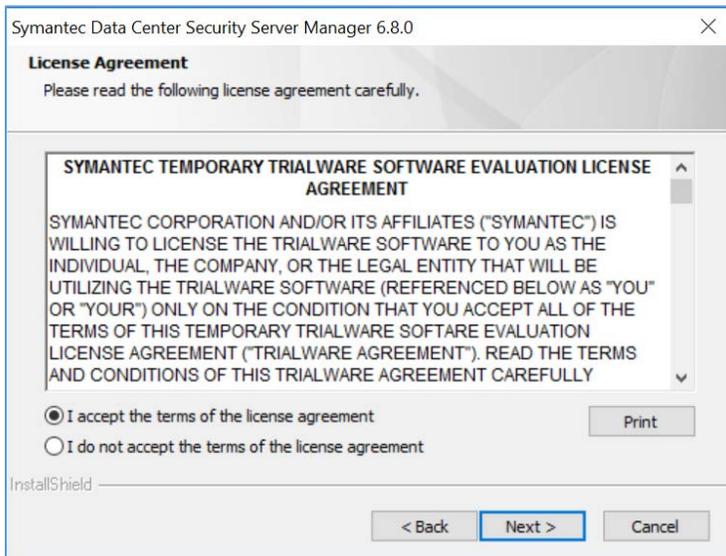
2084 2. Click **Next >**.



2085

2086 3. Check **I accept the terms of the license agreement**.

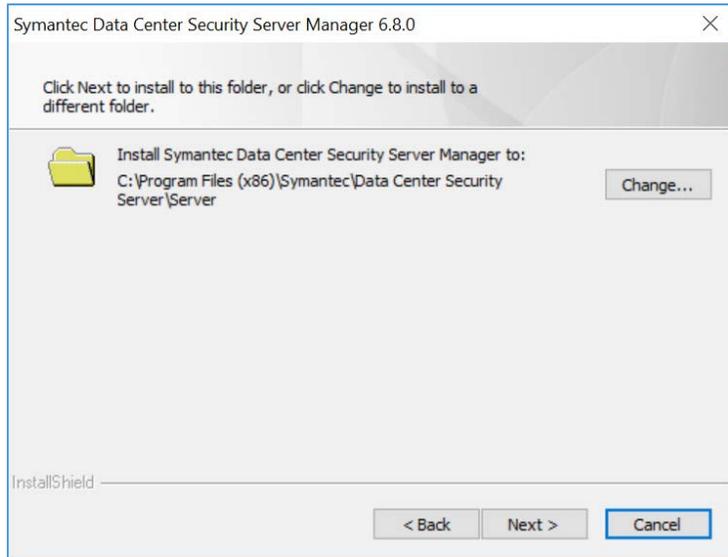
2087 4. Click **Next >**.



2088

2089 5. Verify install location.

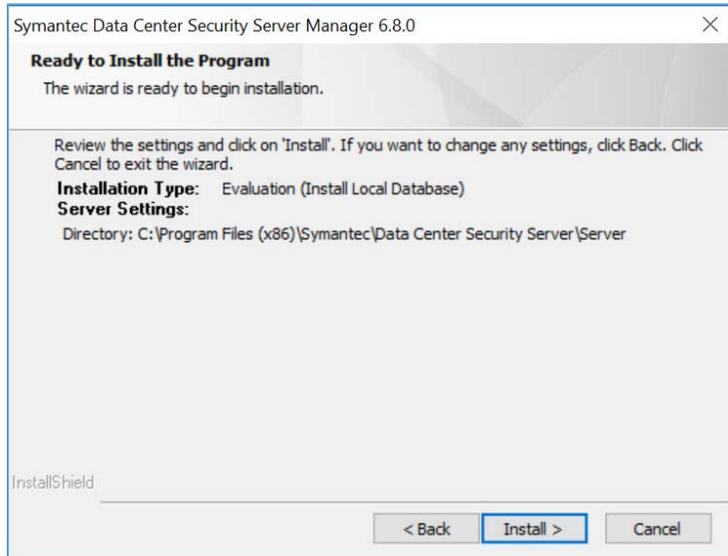
2090 6. Click **Next >**.



2091

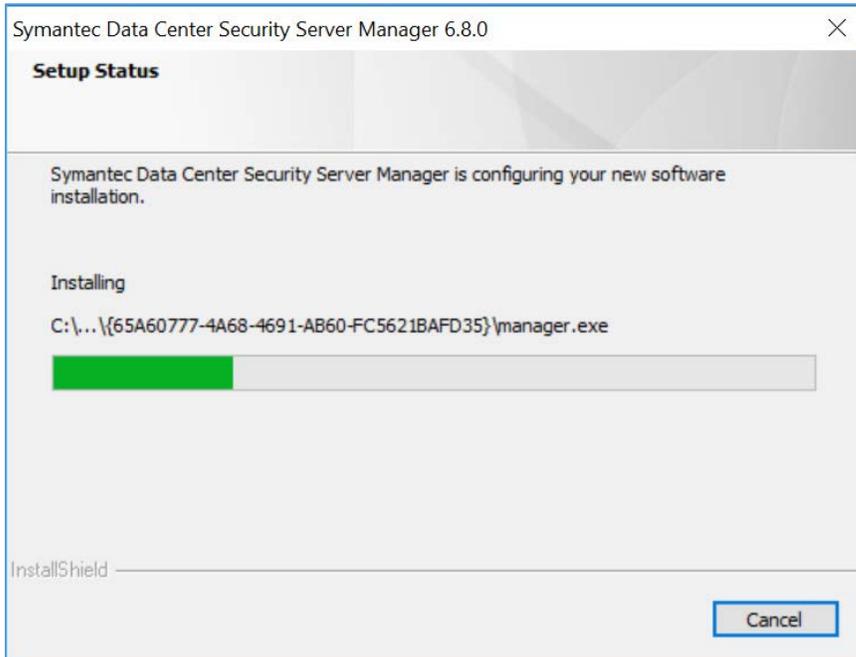
2092 7. Review settings.

2093 8. Click **Install >**.



2094

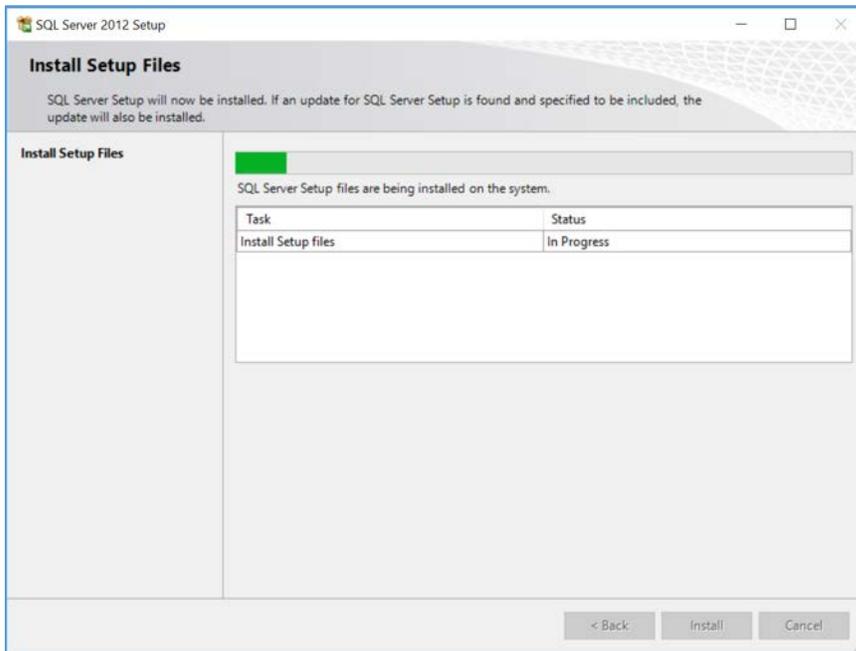
2095 9. Wait for setup and install process to complete.



2096

2097

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



2098

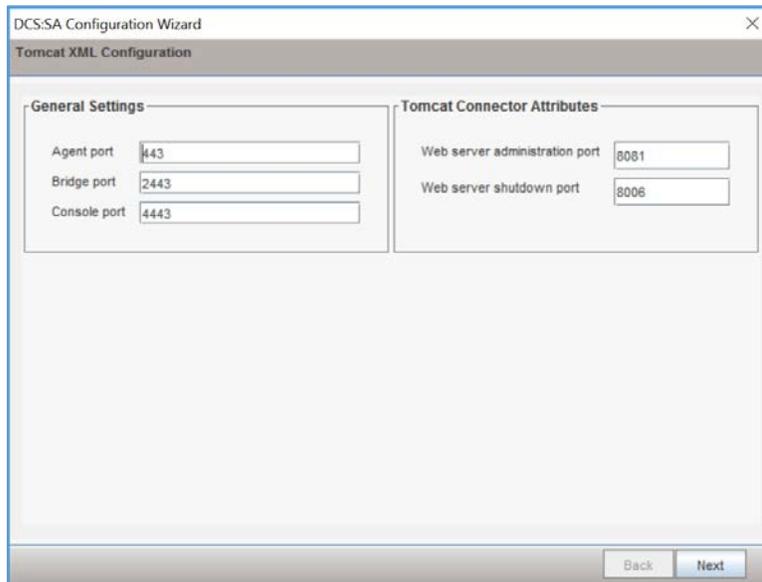
2099

11. Provide the information below, and click on **Next**:

2100

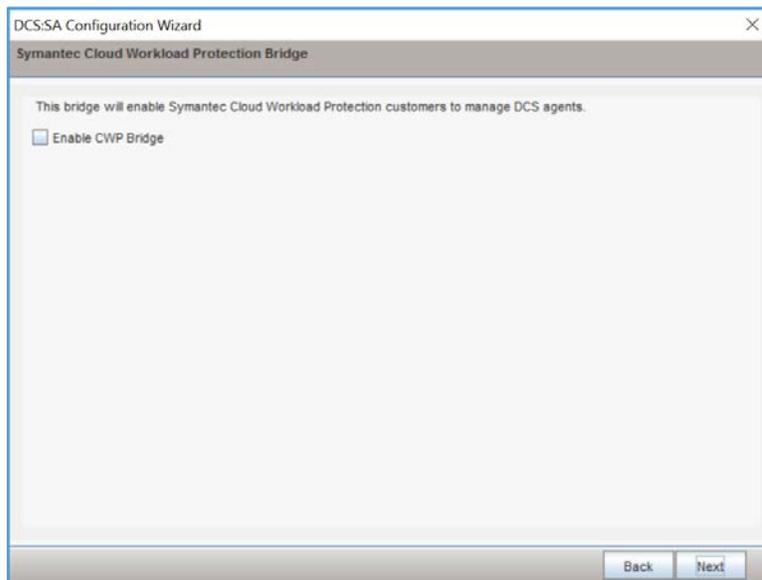
- **Agent port: 443**

- 2101 ▪ **Bridge port:** 2443
- 2102 ▪ **Console port:** 4443
- 2103 ▪ **Web server administration port:** 8081
- 2104 ▪ **Web server shutdown port:** 8006



2105

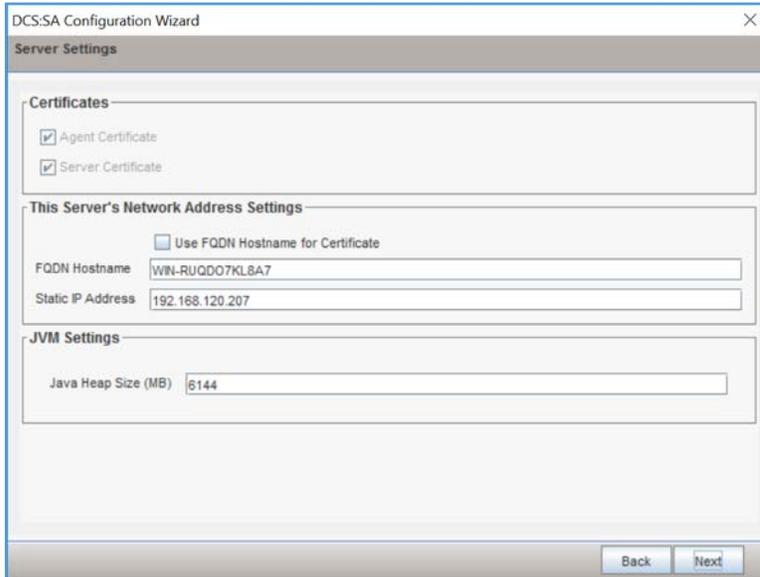
2106 12. Uncheck **Enable CWP Bridge** and click **Next**.



2107

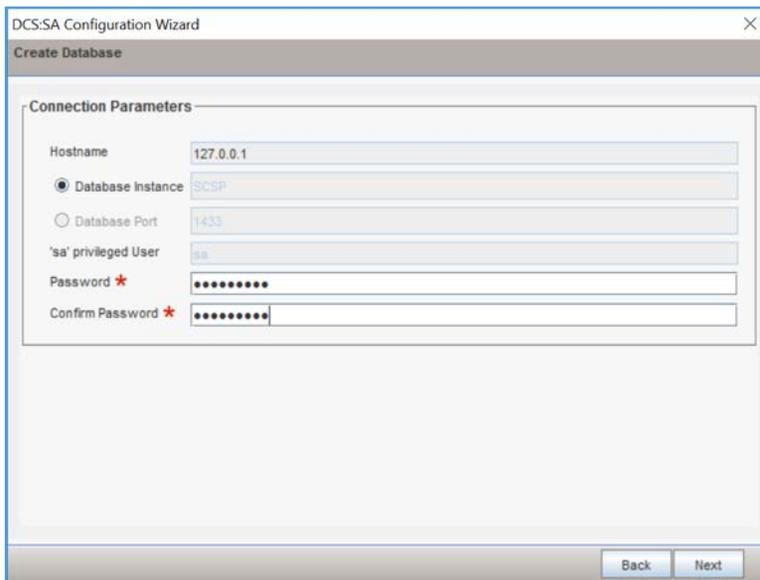
DRAFT

- 2108 13. Verify settings for **FQDN Hostname** as **WIN-RUQDO7KL8A7**, **Static IP Address** as **192.168.120.207**,
2109 and **Java Heap Size** as **6144** and then click **Next**.



The screenshot shows the 'Server Settings' window of the DCS:SA Configuration Wizard. It is divided into three sections: 'Certificates', 'This Server's Network Address Settings', and 'JVM Settings'. In the 'Certificates' section, both 'Agent Certificate' and 'Server Certificate' are checked. In the 'Network Address Settings' section, the 'Use FQDN Hostname for Certificate' checkbox is unchecked, the 'FQDN Hostname' field contains 'WIN-RUQDO7KL8A7', and the 'Static IP Address' field contains '192.168.120.207'. In the 'JVM Settings' section, the 'Java Heap Size (MB)' field contains '6144'. At the bottom right, there are 'Back' and 'Next' buttons.

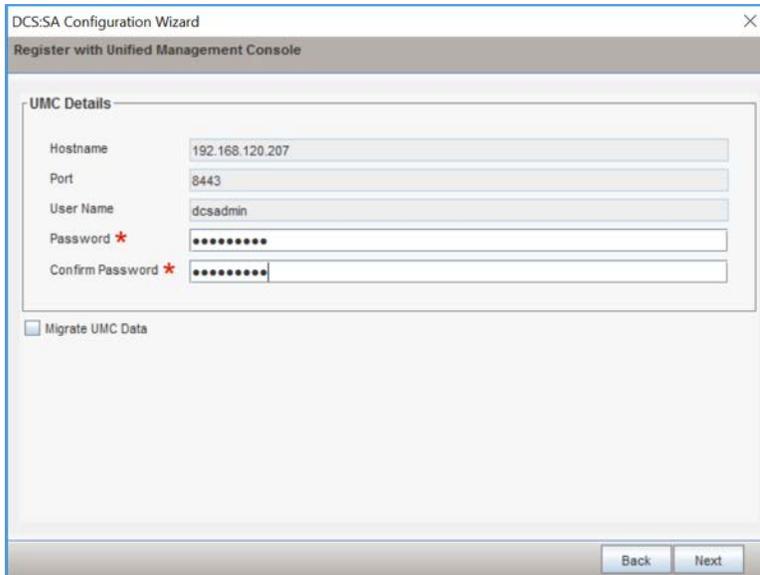
- 2110
2111 14. Create a **password** for the database connection.
2112 15. Click **Next**.



The screenshot shows the 'Create Database' window of the DCS:SA Configuration Wizard. It is titled 'Connection Parameters' and contains several input fields: 'Hostname' with '127.0.0.1', 'Database Instance' with 'SCSP' (selected with a radio button), 'Database Port' with '1433', ''sa' privileged User' with 'sa', 'Password' with masked characters, and 'Confirm Password' with masked characters. At the bottom right, there are 'Back' and 'Next' buttons.

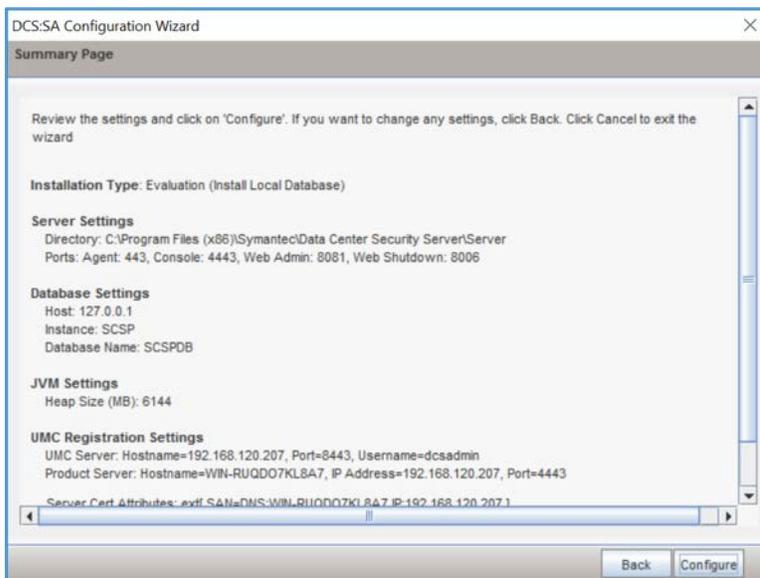
- 2113
2114 16. Verify **Unified Management Console** connection settings.
2115 17. Create a password for **Unified Management Console** connection.

2116 18. Click **Next**.



2117

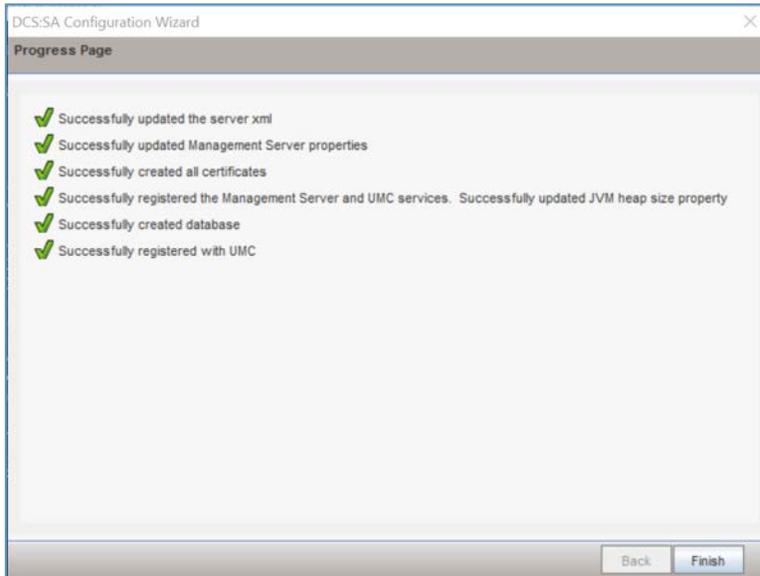
2118 19. Verify configuration settings and click **Next**.



2119

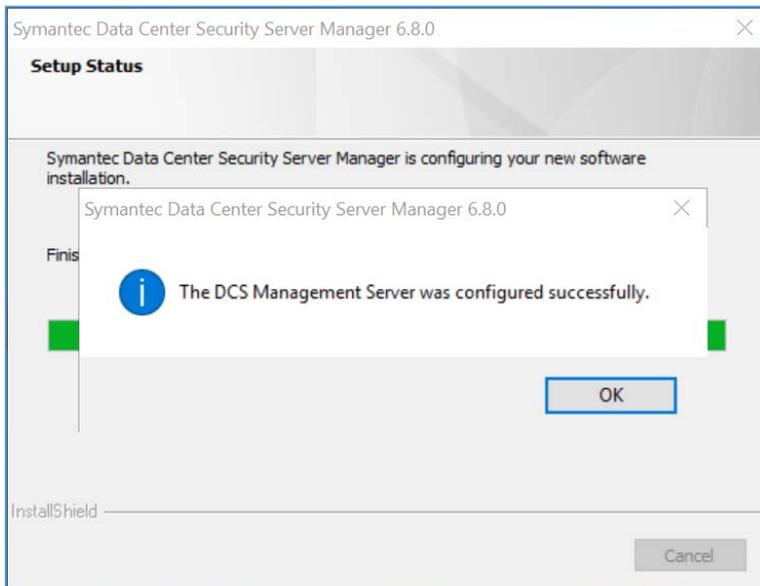
2120 20. Wait for configuration process to complete.

2121 21. Click **Finish**.



2122

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



2124

2125 **Symantec Datacenter Security Windows Agent Install**

2126 1. Run **agent.exe**.

2127 2. Click **Next >**.



2128

2129 3. Check **I accept the terms in the license agreement.**

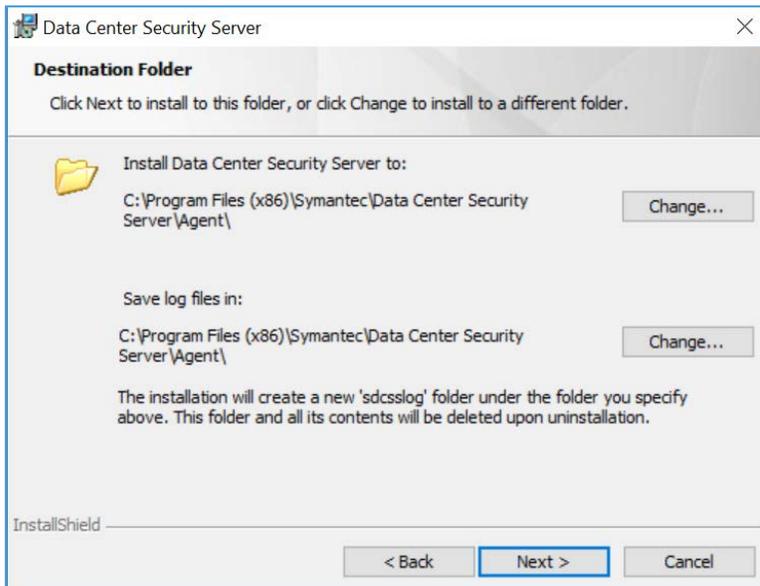
2130 4. Click **Next >**.



2131

2132 5. Verify installation and log files directories.

2133 6. Click **Next >**.



2134

2135 7. Provide the information below, and click on **Next>**:

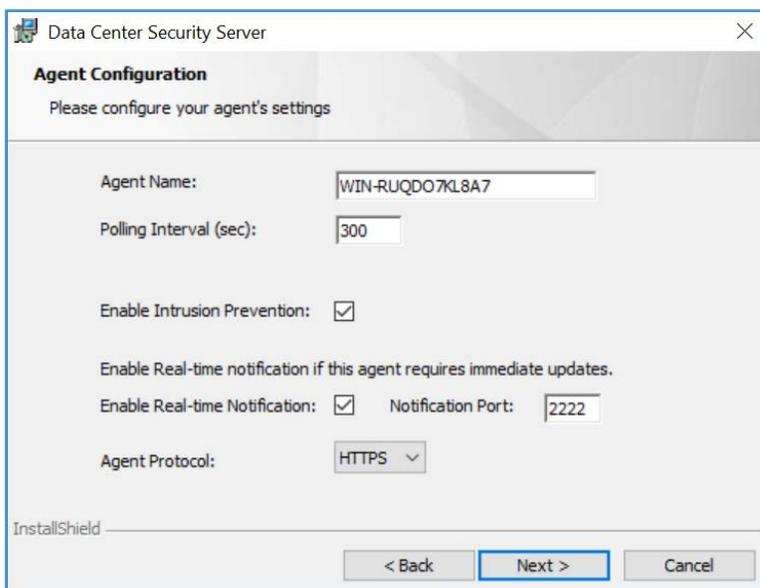
2136 ■ **Agent Name:** WIN-RUQDO7KL8A

2137 ■ **Polling Interval (sec):** 300

2138 ■ Check **Enable Intrusion Prevention**

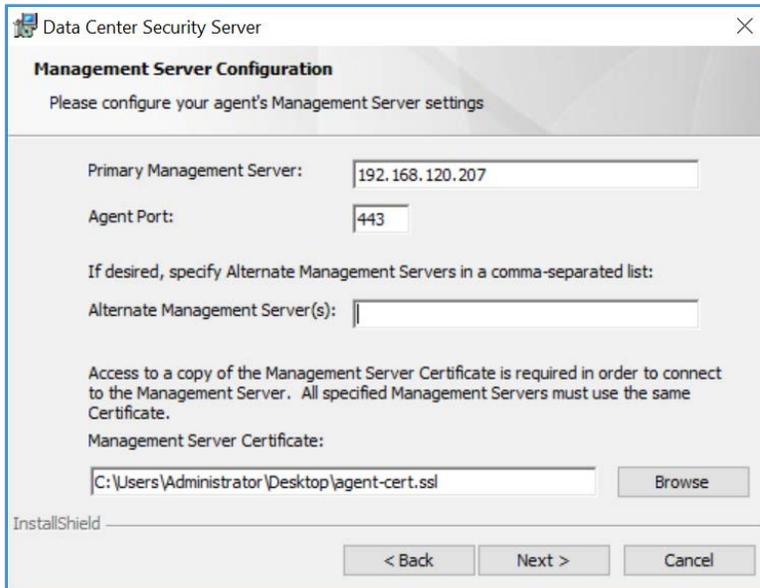
2139 ■ **Notification Port:** 2222

2140 ■ **Agent Protocol:** HTTPS

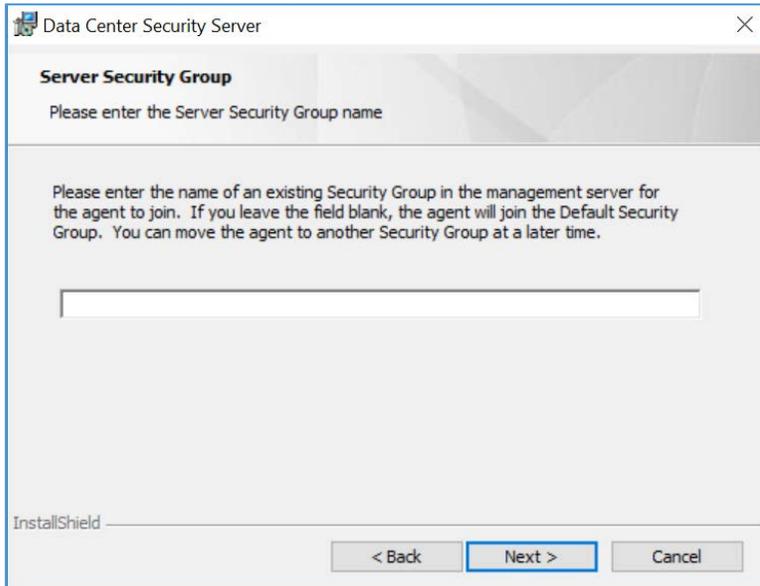


2141

- 2142 8. Provide the information below and click **Next**:
- 2143 ▪ **Primary Management Server:** 192.168.120.207
- 2144 ▪ **Agent Port:** 443
- 2145 ▪ **Alternate Management Servers:**
- 2146 ▪ **Management Server Certificate:** *C:\User\Administrator\Desktop\agent-cert.ssh*

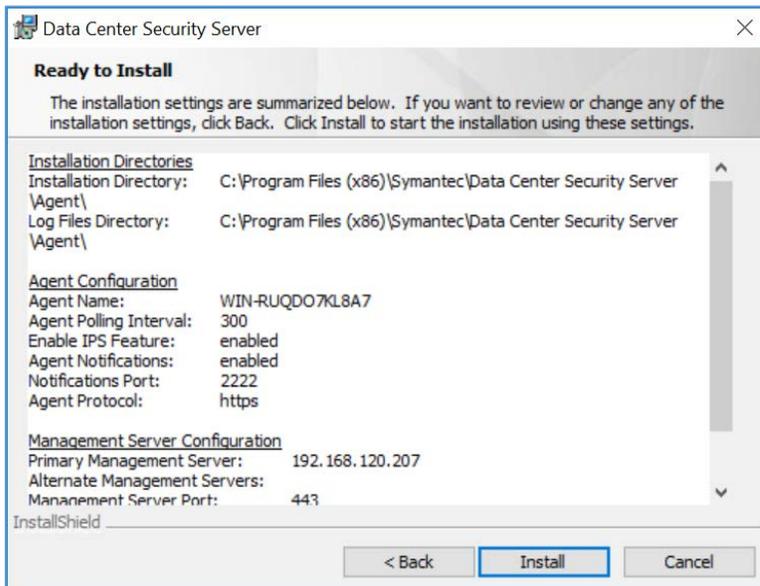


- 2147
- 2148 9. Specify a **Server Security Group** created through Symantec Datacenter Security Server or leave it
- 2149 blank to use the default security group.
- 2150 10. Click **Next >**.



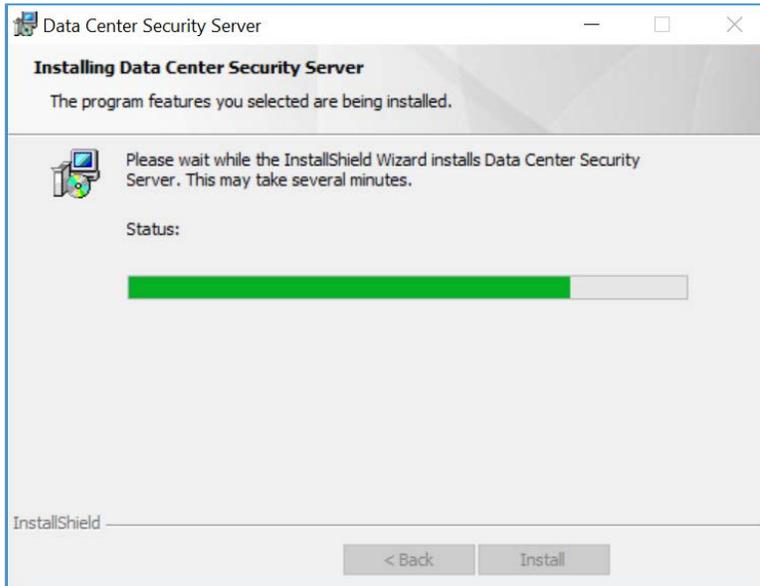
2151

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



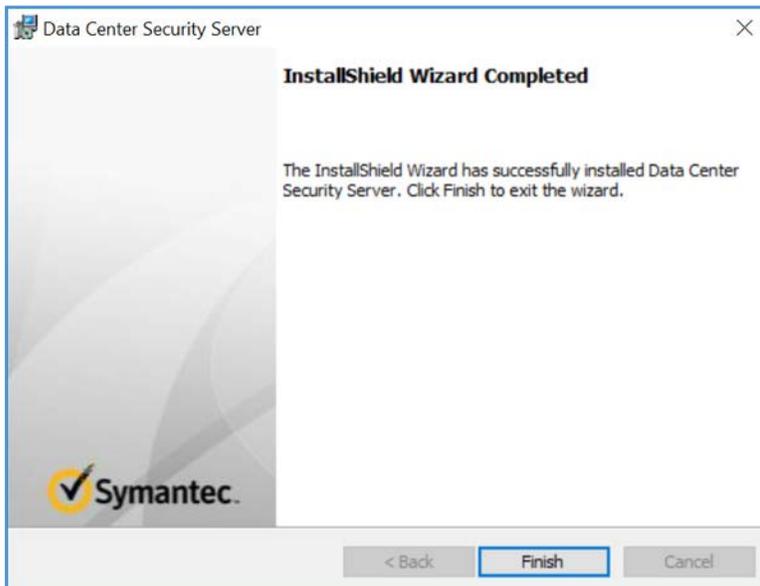
2153

2154 12. Wait for the installation process to complete.



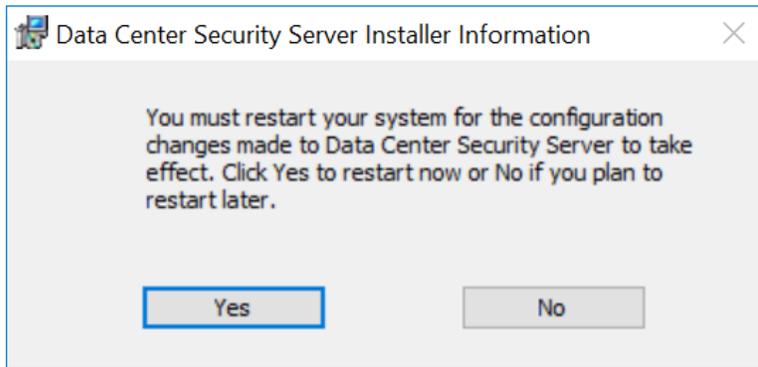
2155

2156 13. Click **Finish**.



2157

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



2159

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

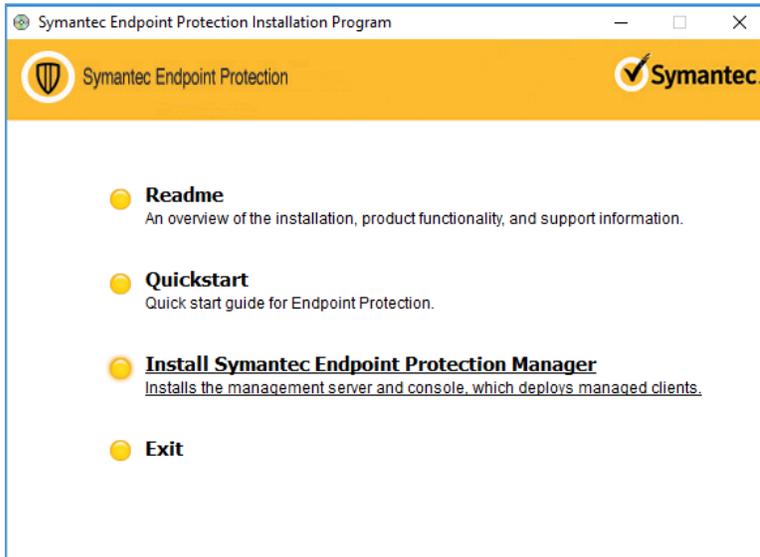
2168 **Storage:** 240GB (thin provisioned)

2169 **Operating System:** Microsoft Windows Server 2016

2170 **Network Adapter:** VLAN 1901

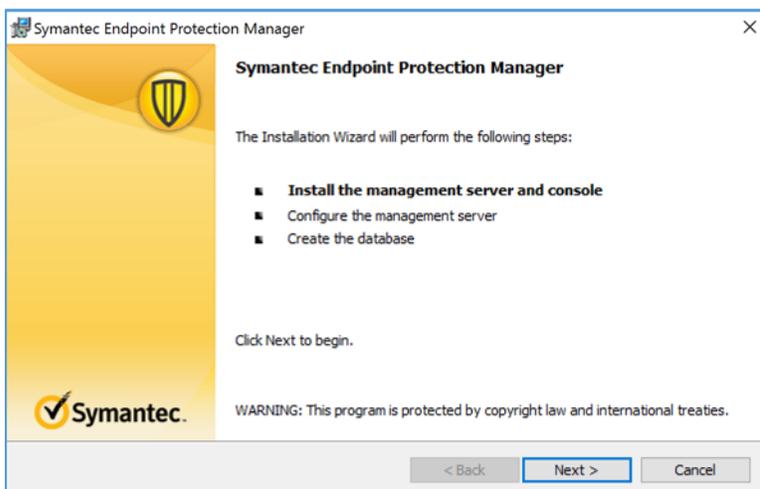
2171 Symantec Endpoint Protection Manager Installation

- 2172 1. Launch *Symantec_Endpoint_Protection_14.2.0.MP1_Part1_Trialware_EN.exe* file.
- 2173 2. Select **Install Symantec Protection Endpoint Manager** option.



2174

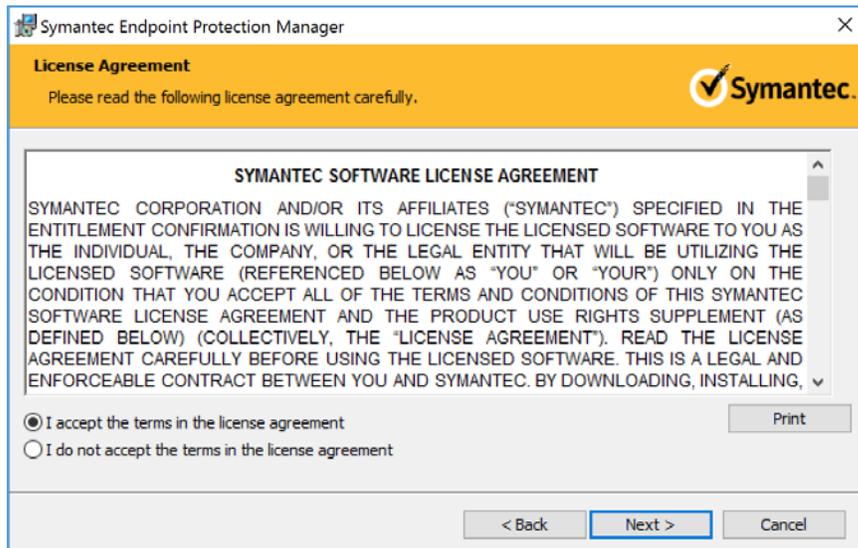
2175 3. Proceed through the install wizard by clicking **Next >**.



2176

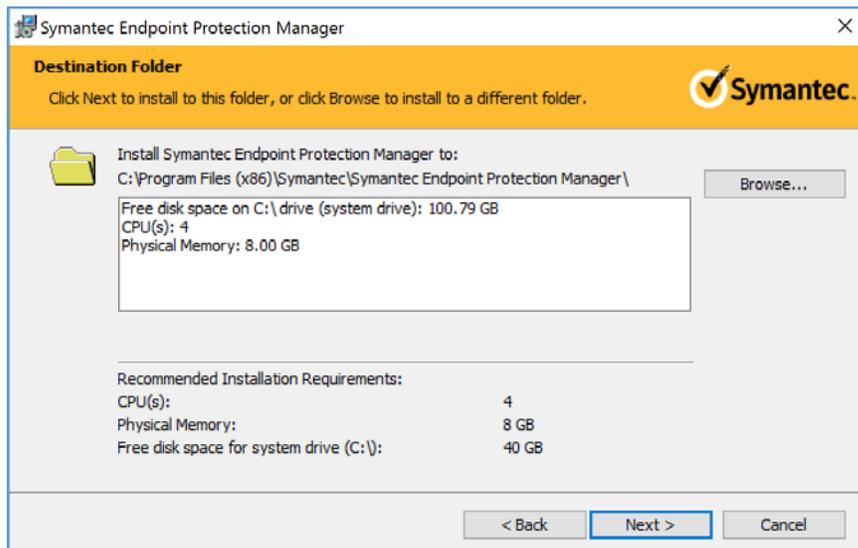
2177 4. Check **I accept the terms in the license agreement.**

2178 5. Click **Next >**.



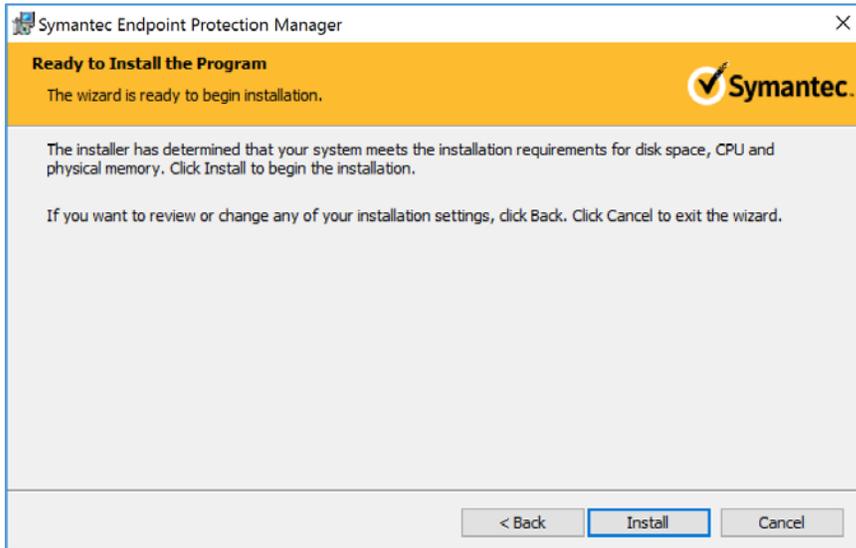
2179

- 2180 6. Select the location you want to install Symantec Endpoint Protection Manger and click **Next >**. Keep
2181 the default location of *C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager*.



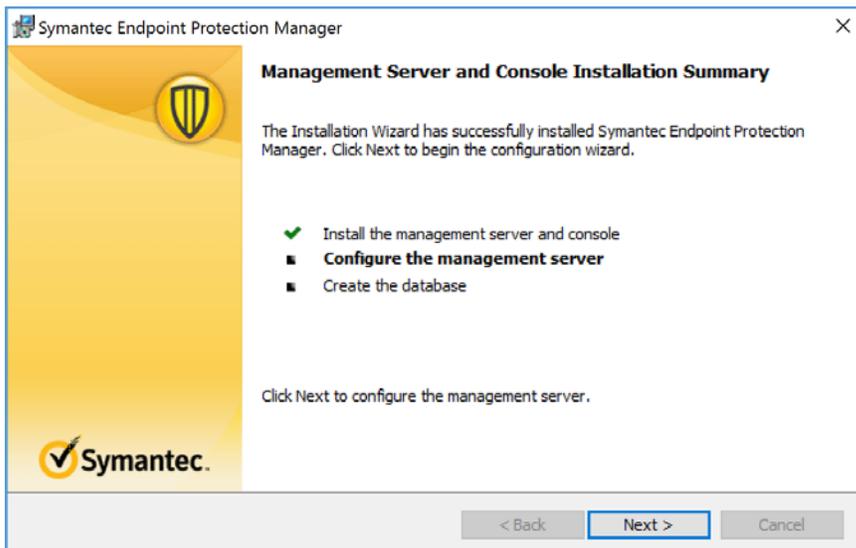
2182

- 2183 7. Select **Install**.



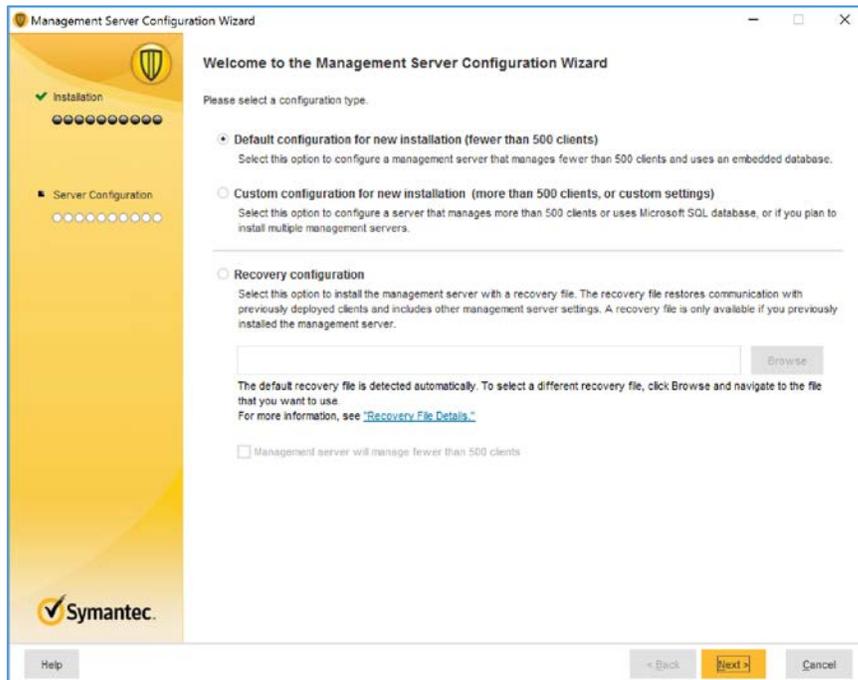
2184

- 2185 8. After installation is complete, click **Next >** to continue with configuration of the management
2186 server.



2187

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



2189

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

2191

- **Company Name:** NCCoE

2192

- **User name:** admin

2193

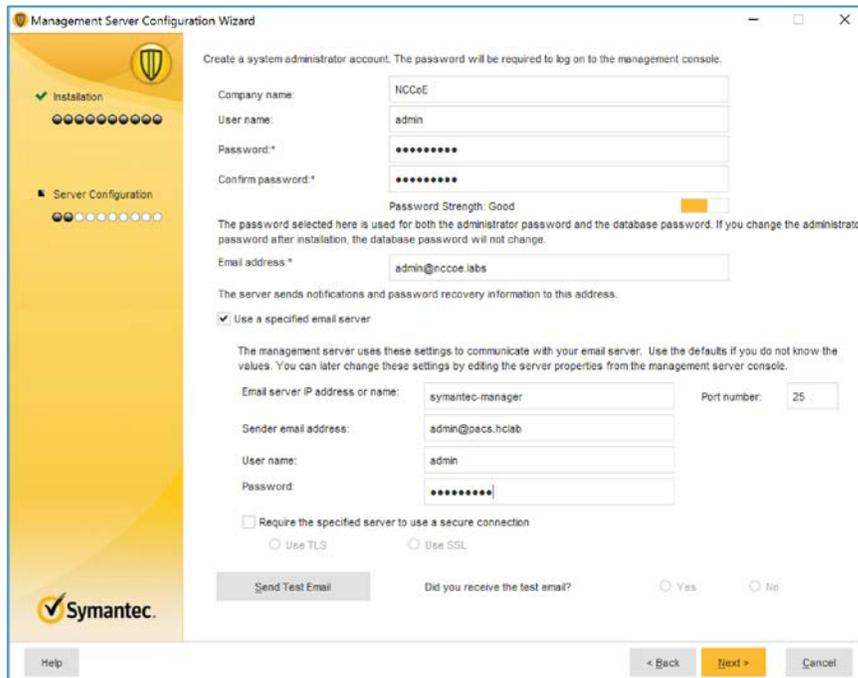
- **Password:** *****

2194

- **Confirm password:** *****

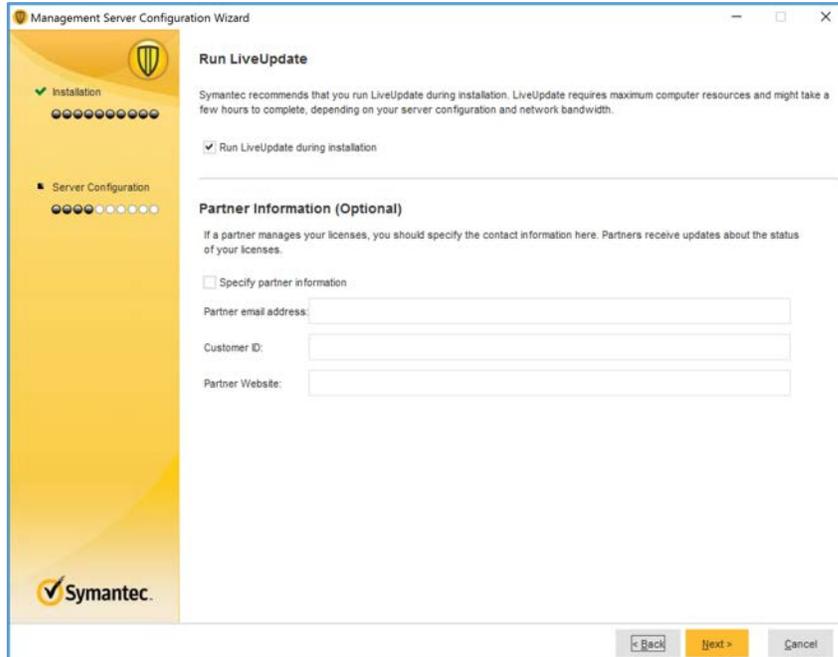
2195

- **Email address:** admin@nccoe.labs



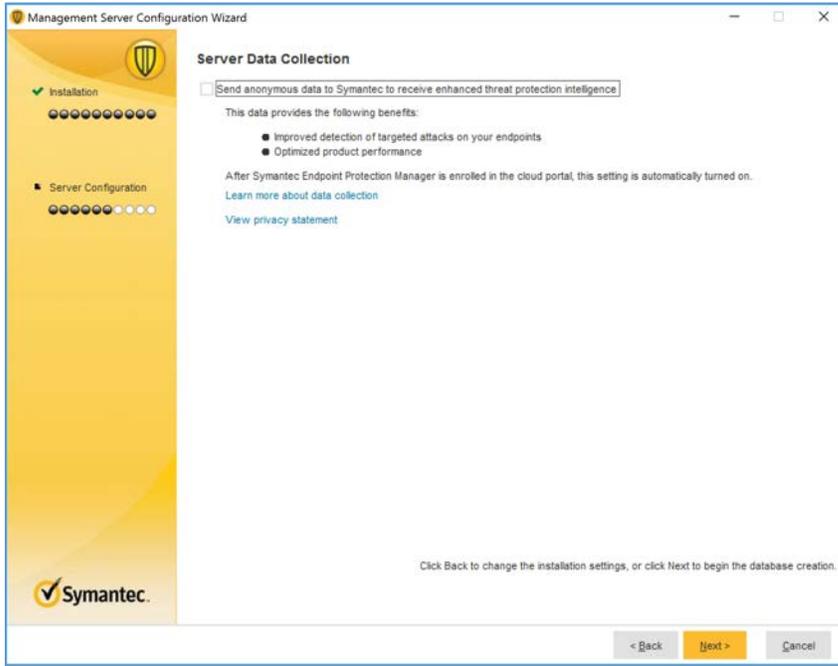
2196

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

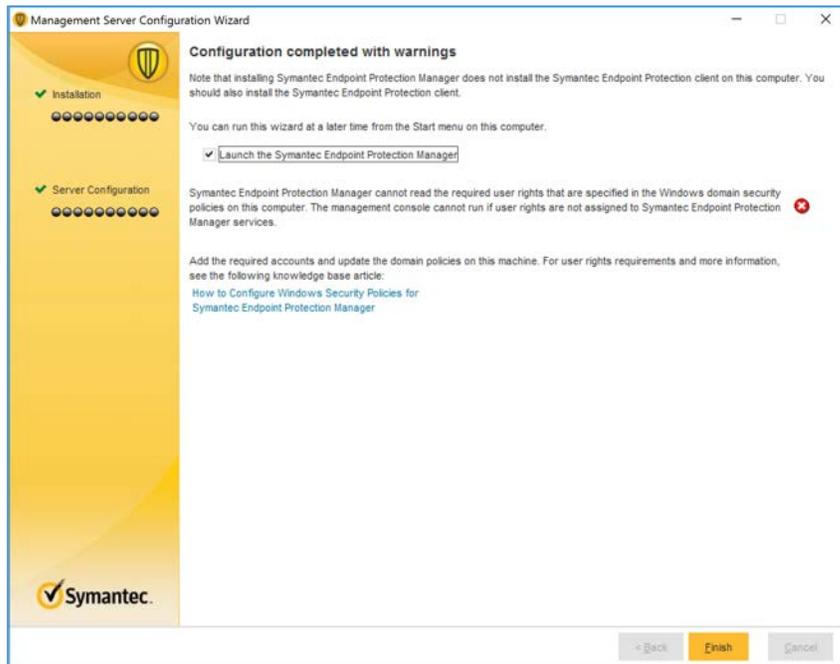


2198

- 2199 12. Uncheck **Send anonymous data to Symantec to receive enhanced threat protection intelligence**
2200 and click **Next >**.



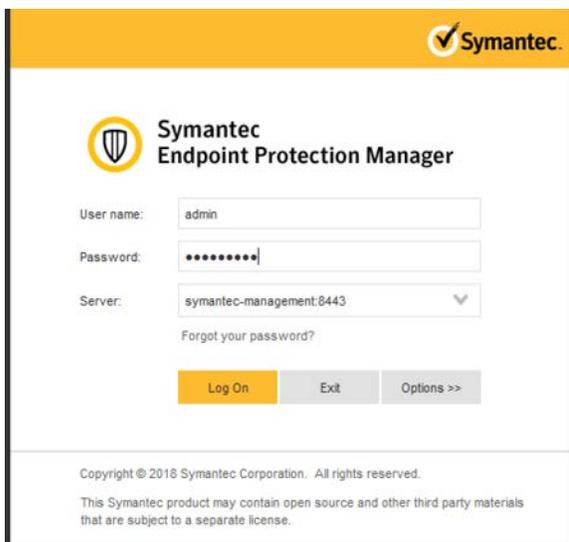
- 2201
2202 13. After installation is completed, check **Launch the Symantec Endpoint Protection Manager** to
2203 configure your hosts; click **Finish**.



2204

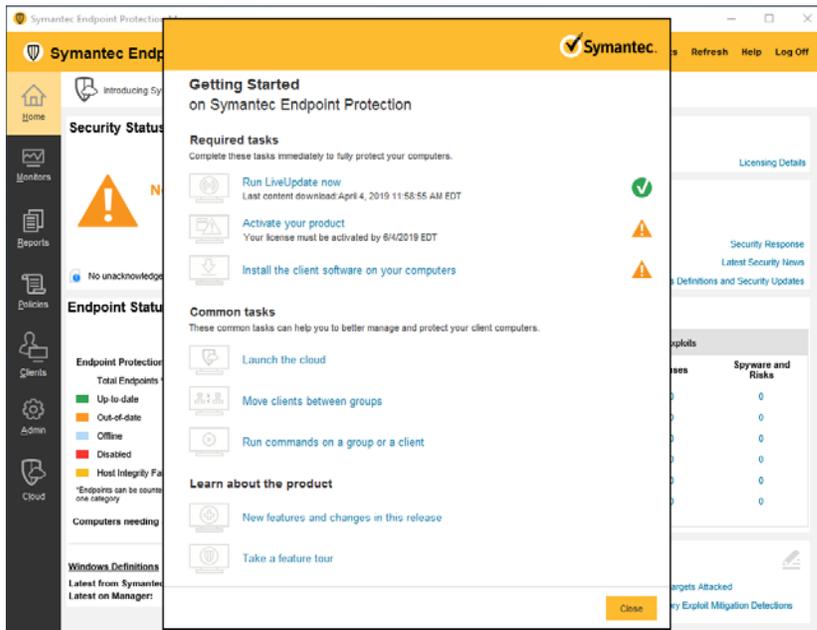
2205 **Symantec Endpoint Protection Host Windows Installation**

- 2206 1. Launch the **Symantec Endpoint Protection Manager** and log in as the **admin**.



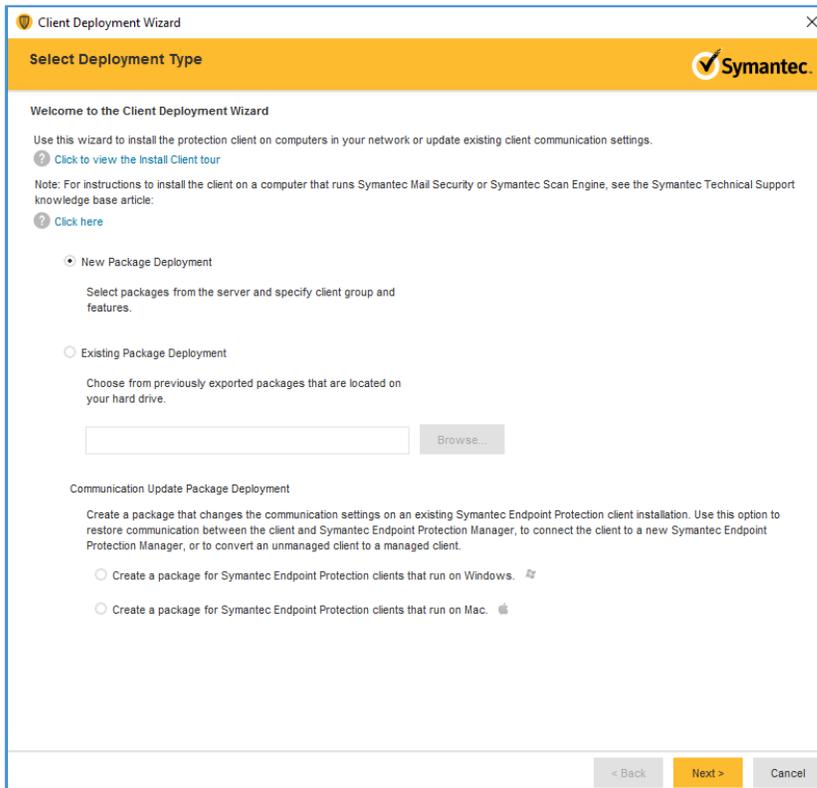
2207

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



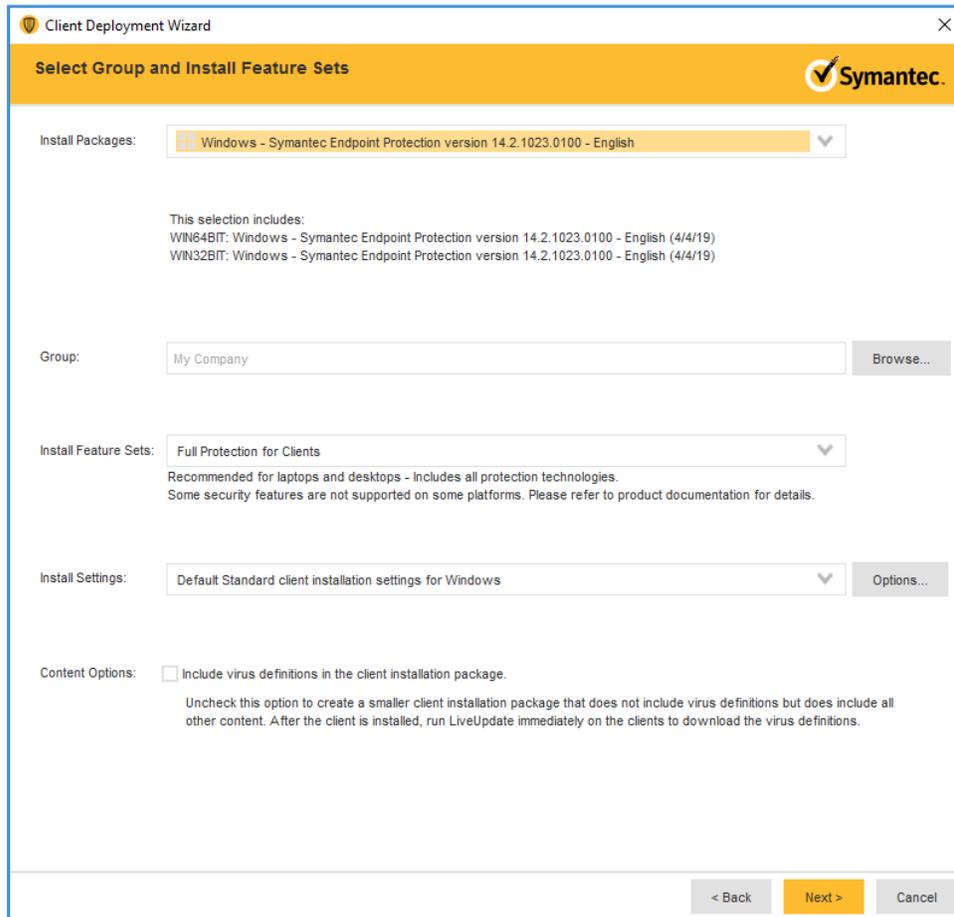
2209

2210 3. Confirm that **New Package Deployment** is checked and click **Next >**.



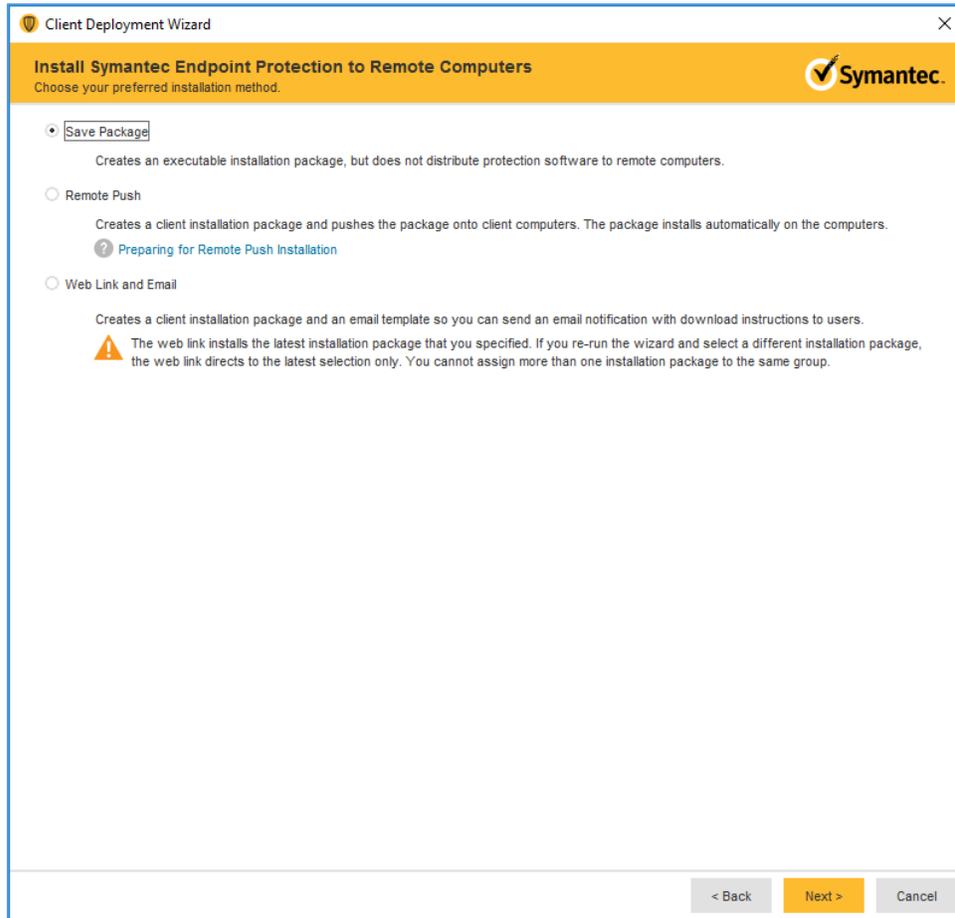
2211

- 2212 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 >**.



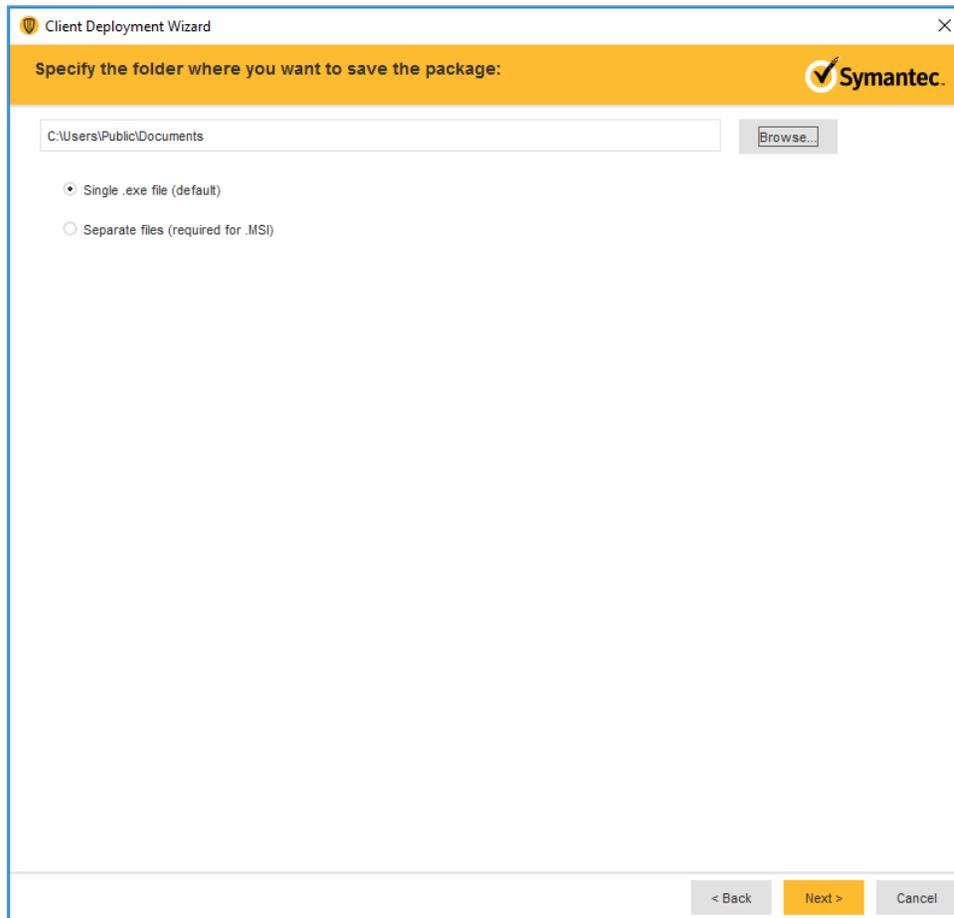
2215

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



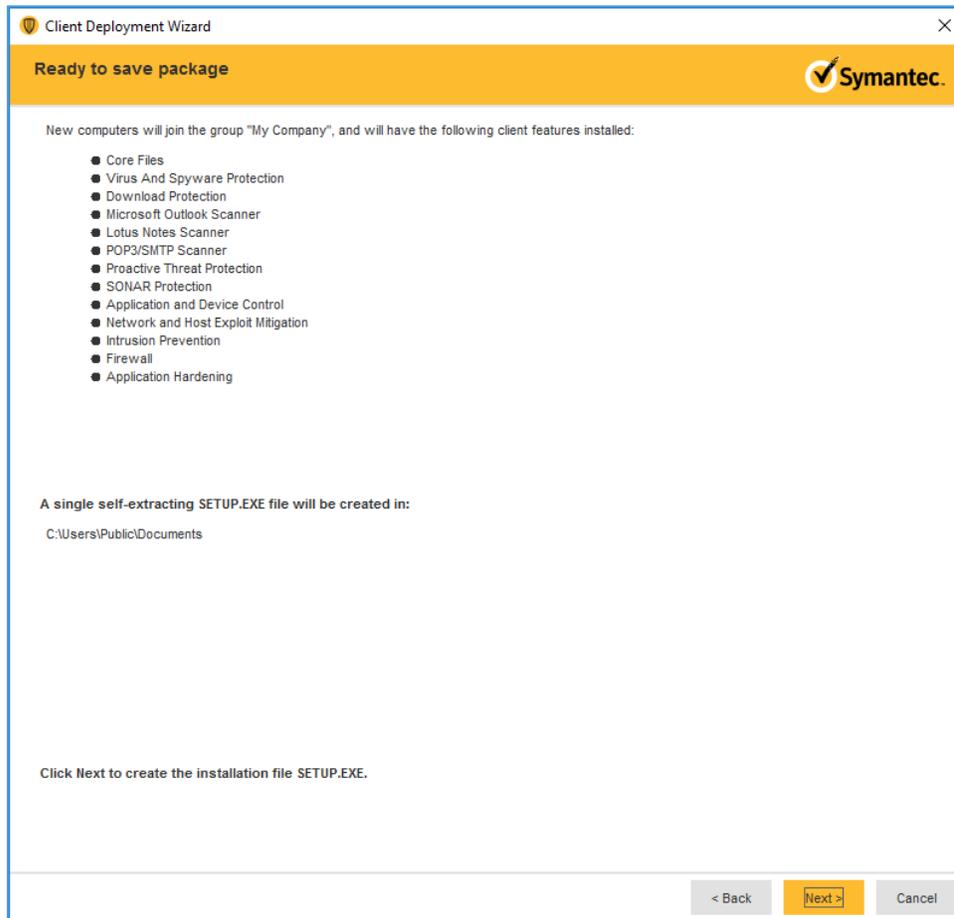
2217

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



2219

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



2221

2222 8. Move the installation package to the Operating System on which you want to install Symantec
 2223 Endpoint Protection.

2224 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 [Section 2.6.2](#), 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 [Section](#)
 2230 [2.7.3](#), Tempered Networks Identity Defined Networking (IDN).

2231 2.10 Secure Remote Access

2232 2.10.1 TDi Technologies ConsoleWorks

2233 The NCCoE lab implemented a VendorNet using TDi ConsoleWorks, which is a browser interface that
2234 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

2246 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.

- 2249 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.
- 2251 3. Restart ConsoleWorks by executing *cw_stop* and *cw_start* scripts located in the
2252 */opt/ConsoleWorks/bin* directory.
- 2253 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.

External Authentication Record

Record Name: RADIUS

Enabled

Library: radius

Parameter 1: 192.168.120.190:1812/*****

Parameter 2: 30

Parameter 3:

Parameter 4:

Parameter 5:

Parameter 6: 15

Required Profile:

Template User: CONSOLE_MANAGER

Cancel Next

- 2264
- 2265 8. Ensure that **Enable External Authentication** is checked.

SECURITY: External Authentication

Enable External Authentication

External Authentication assumed for pre-existing User accounts

External Authentication	Library	Enabled	Param 1
<input type="checkbox"/> RADIUS	radius	Y	192.168.120.190:1812/...

Up Down Delete Add Rename Edit Save

2266

2267 2.10.2 Symantec Validation and ID Protection (VIP)

2268 Symantec Validation and ID Protection is an authentication service that provides various forms of
2269 authentication such as push, SMS, and biometric. For this project, Symantec VIP is used as a second form
2270 of authentication for remote access to the PACS architecture through TDi Technologies ConsoleWorks.

2271 System Requirements

2272 **CPU:** 4

2273 **Memory:** 8192MB RAM

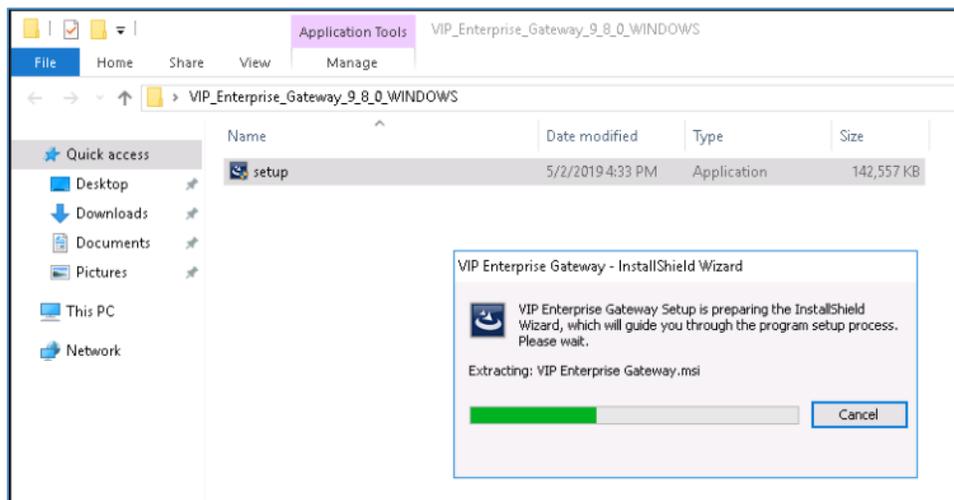
2274 **Storage:** 240GB (thin provisioned)

2275 **Operating System:** Microsoft Windows Server 2016

2276 **Network Adapter:** VLAN 1201

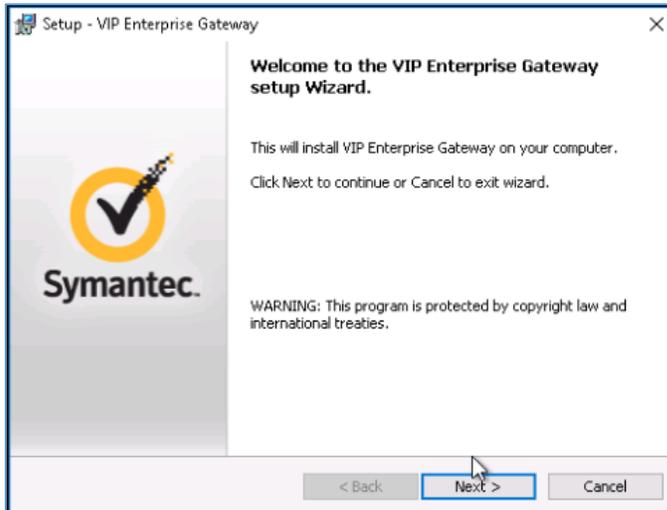
2277 Symantec VIP Installation

2278 1. Right click on the *setup.exe* file for VIP Enterprise Gateway 9.8.0; select **Run as administrator**.



2279

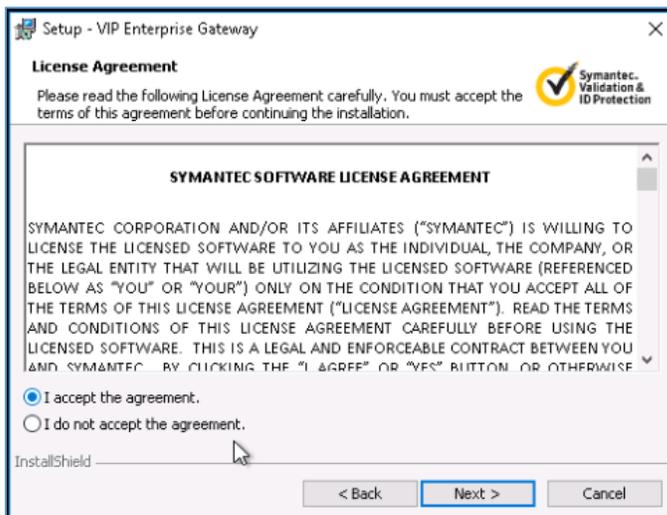
2280 2. Proceed through the install wizard by clicking **Next >**.



2281

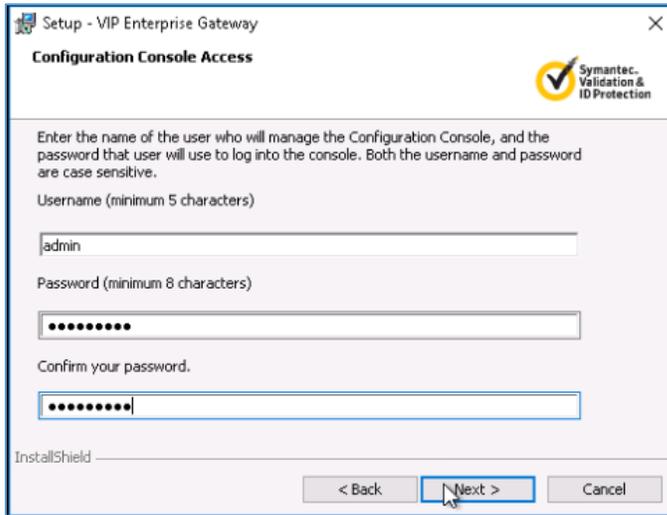
2282 3. Check **I accept the agreement.**

2283 4. Click **Next >**.



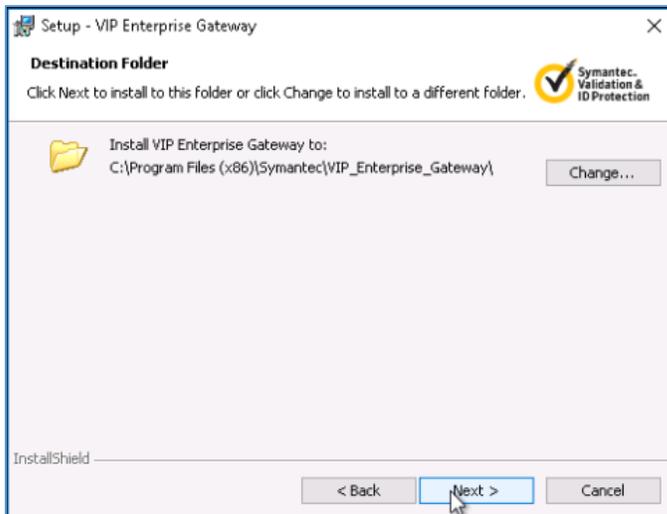
2284

2285 5. Create a **username** as **admin** and **password** and click **Next >**.



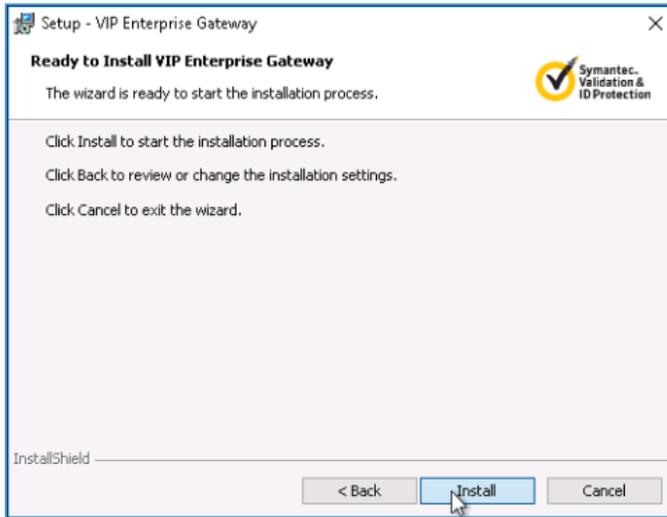
2286

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



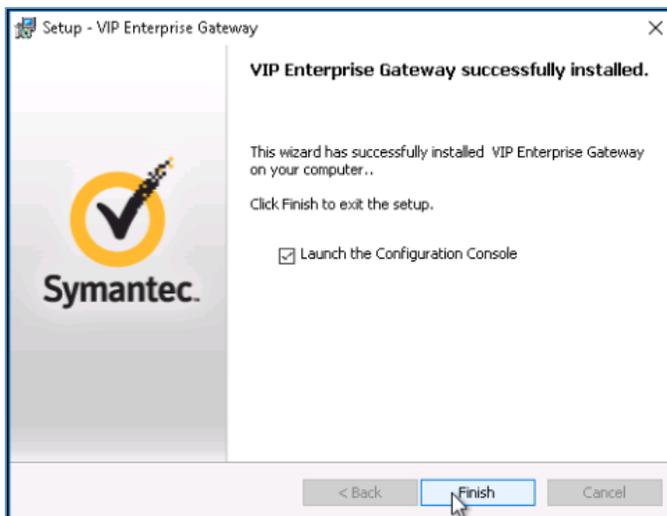
2288

2289 7. Click **Install**.



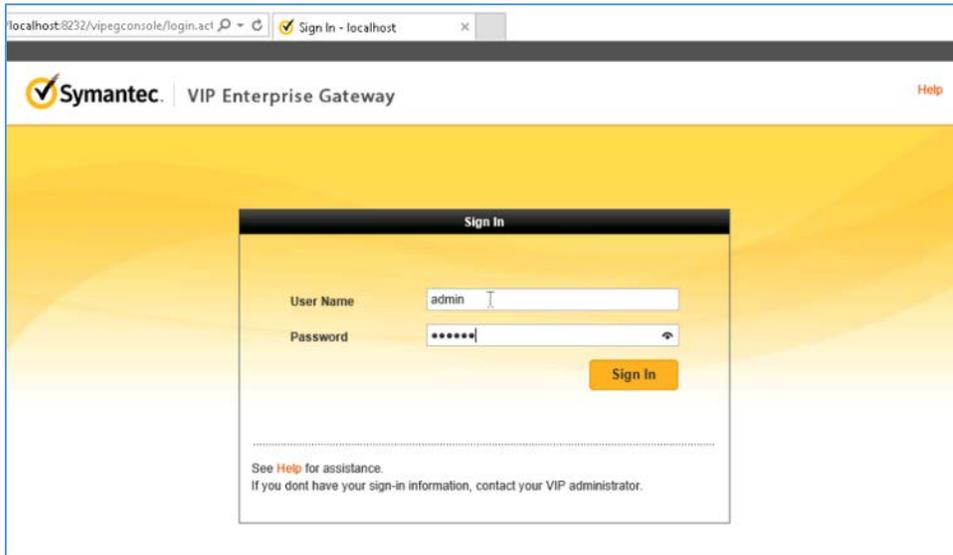
2290

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



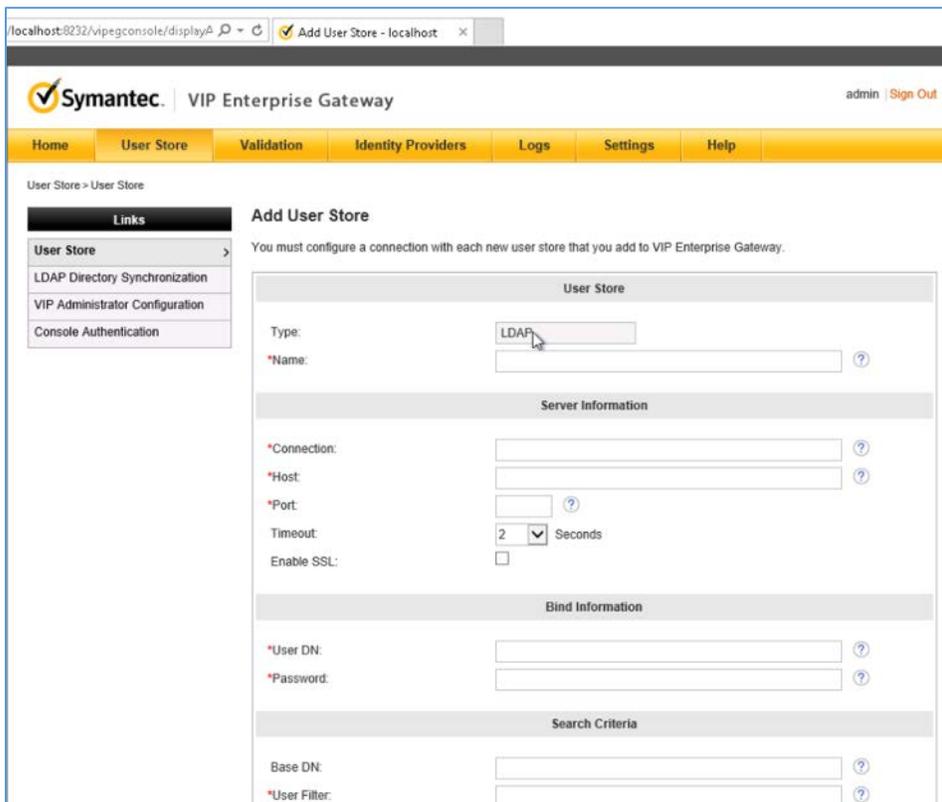
2292

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.



2295

2296 10. Select **User Store** from the menu bar.

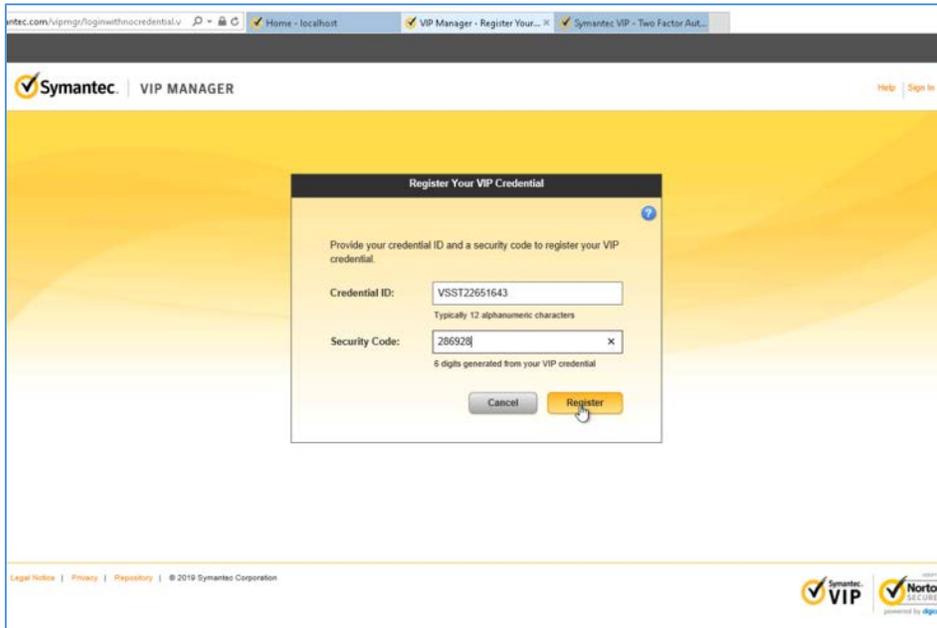


2297

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

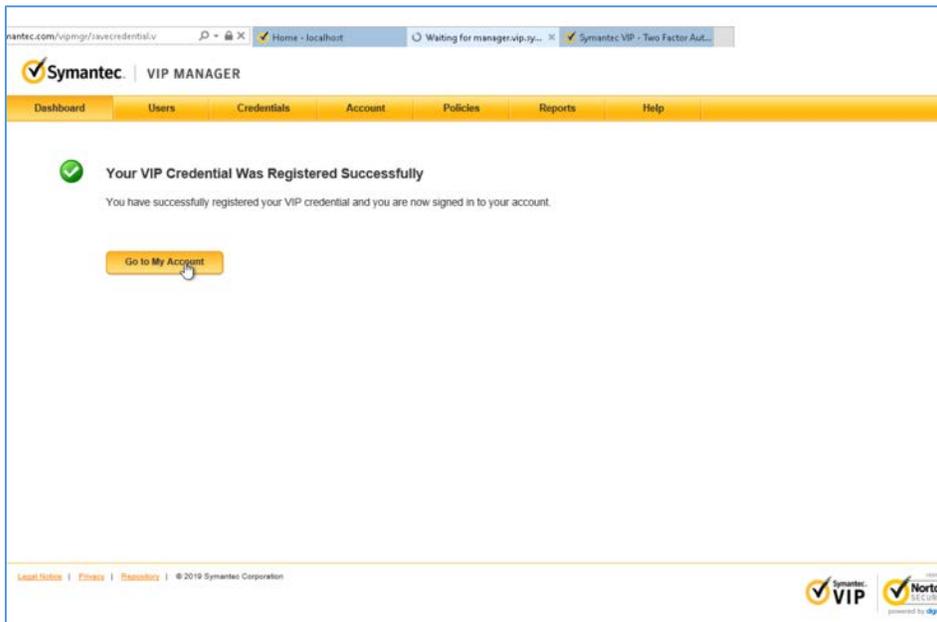
- 2299 ▪ **Name:** AD PACS
- 2300 ▪ **Connection:** ad-main
- 2301 ▪ **Host:** ad.pacs.hclab
- 2302 ▪ **Port:** 389
- 2303 ▪ **User DN:** CN=symantec, DC=pacs, DC=hclab
- 2304 ▪ **Password:** *****
- 2305 ▪ **Base DN:** DC=pacs, DC=hclab
- 2306 ▪ **User Filter:** (&(&objectClass=user)(objectCategory=person))(sAMAccountName=%s)

- 2307
- 2308 12. Log into VIP Manager by navigating to <https://manager.vip.symantec.com/vipmgr>. Use the account
- 2309 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 <https://vip.symantec.com/>.



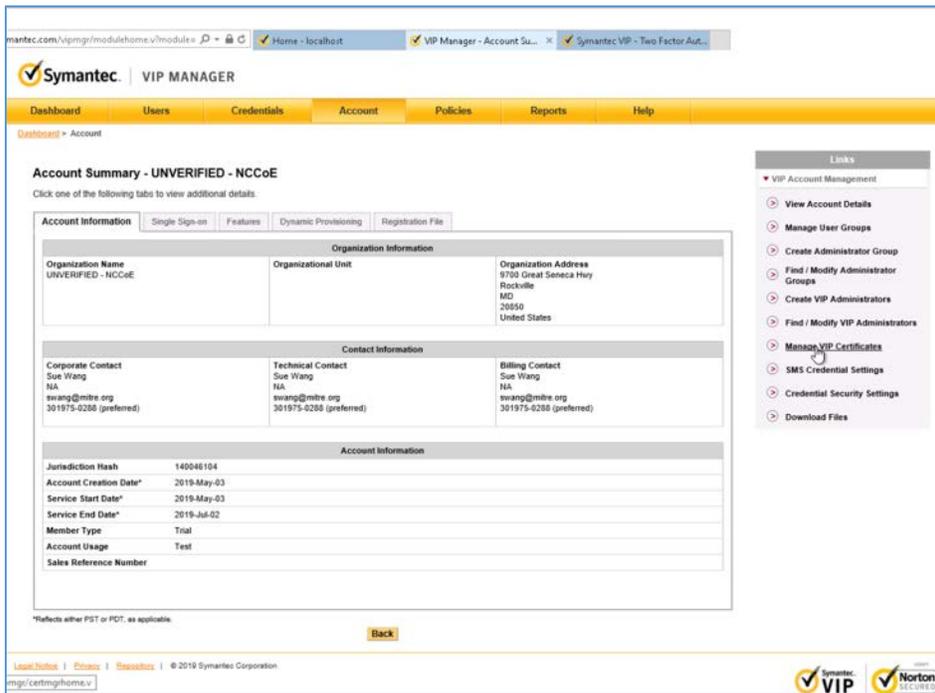
2312

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



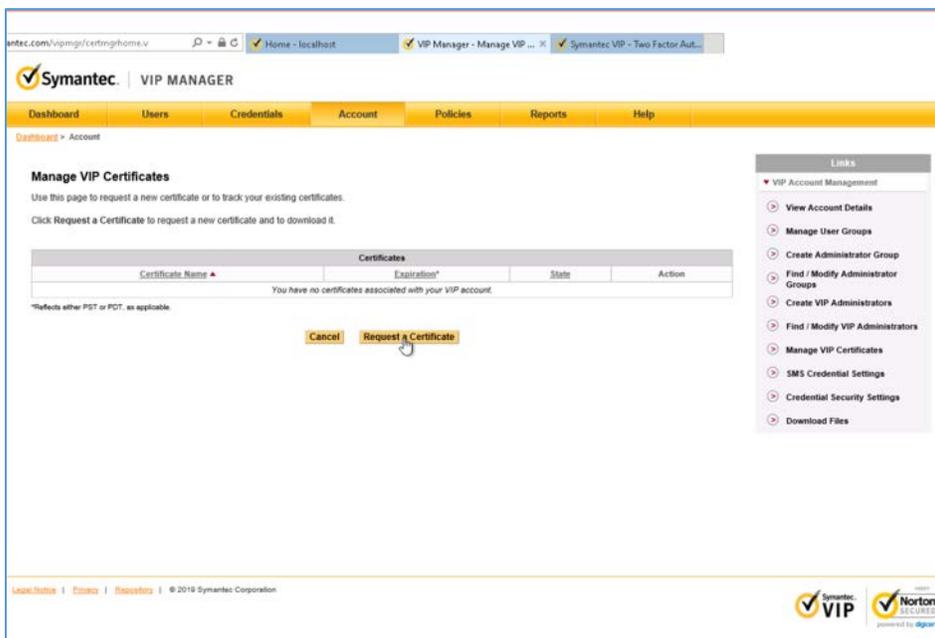
2314

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



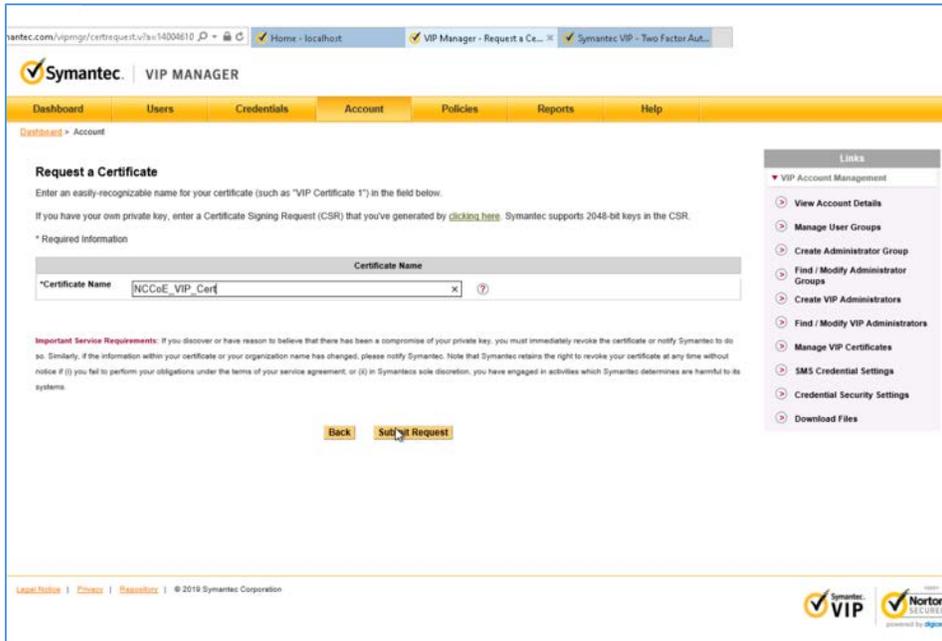
2316

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



2318

2319 17. Provide a **Certificate Name** as **NCCoE_VIP_Cert**; click **Submit Request**.

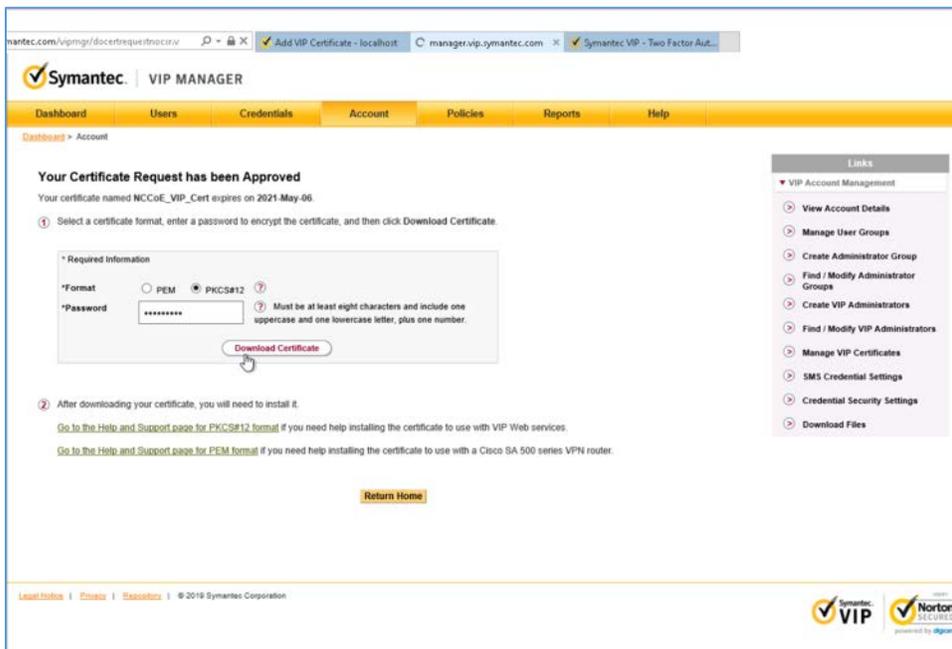


2320

2321

2322

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

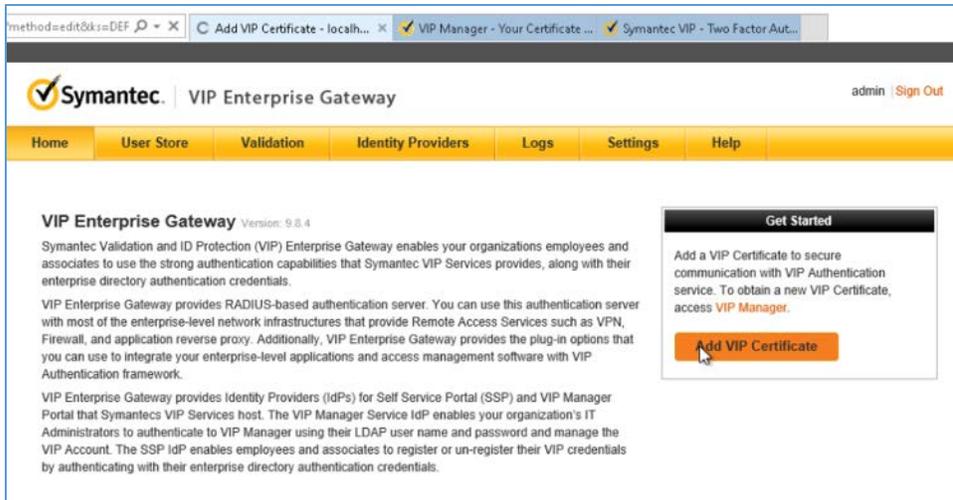


2323

2324

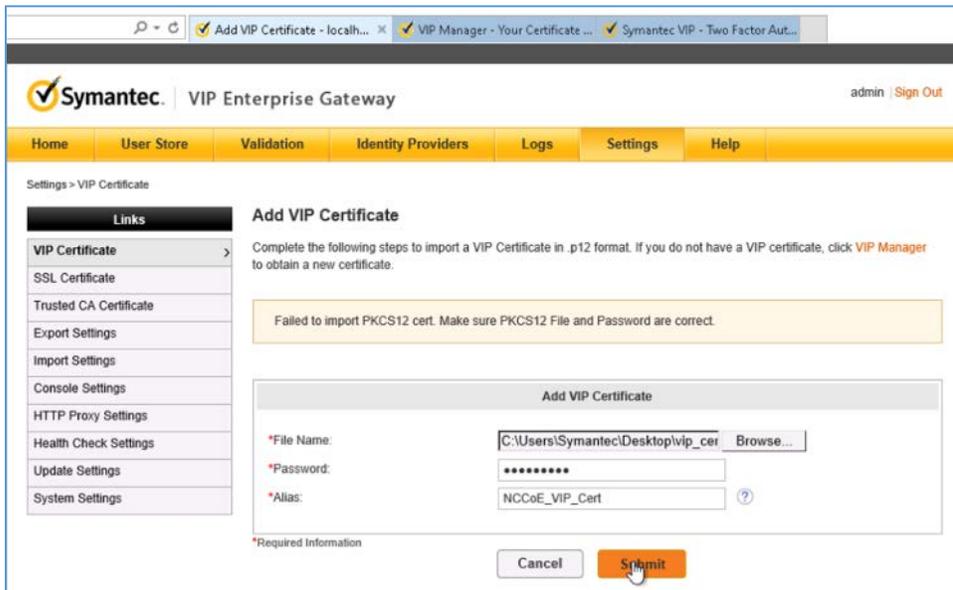
19. Save the certificate on the Symantec VIP local machine.

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



2326

2327 21. Select **Browse** and upload the certificate from the previous step. Enter the correct password and
 2328 alias for the certificate, then click **Submit**.

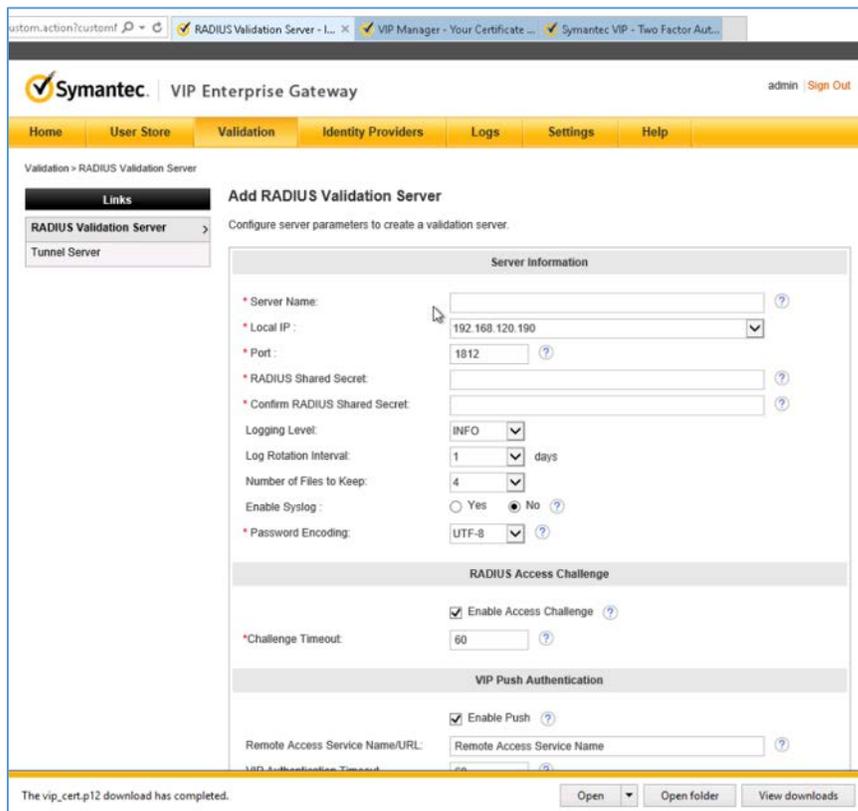


2329

2330 22. Select Validation from the menu bar, select Custom configuration, and provide the information that
 2331 follows:

- 2332 ■ **Server Name:** vip
- 2333 ■ **Local IP:** 192.168.120.190

- 2334 ■ **Port:** 1812
- 2335 ■ **RADIUS Shared Secret:** *****
- 2336 ■ **Confirm RADIUS Shared Secret:** *****
- 2337 ■ **Enable First Factor:** *Checked*
- 2338 ■ **Authentication on:** Enterprise
- 2339 ■ **Authentication Sequence:** *LDAP Password – VIP Authentication*
- 2340 ■ **User Store:** AD PACS



- 2341
- 2342 23. Click **Submit**.

VIP Authentication Timeout: 60

*Enforce Local Authentication: Yes No

First-Factor Authentication

Enable First Factor:

Authentication on: Enterprise VIP Services

Authentication Sequence: LDAP Password - VIP Authentication 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 Submit

2343

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

Symantec | VIP Enterprise Gateway

admin | Sign Out

Home User Store Validation Identity Providers Logs Settings Help

Validation > RADIUS Validation Server

Links

RADIUS Validation Server

Tunnel Server

Validation server vip created successfully. Start the server when required.

The following RADIUS Validation servers have been configured for VIP Enterprise Gateway

Add Server

Server	Port	Status	Action
VIP	1812	ON	Edit Delete Duplicate

Operation is in Progress... This may take a few seconds to complete.

2345

Appendix A List of Acronyms

AD	Active Directory
AES	Advanced Encryption Standard
AE Title	Application Entity Title
CA	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
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure

ICMP	Internet Control Message Protocol
IDN	Identity Defined Networking
IHE	Integrating Health Enterprise
IIS	Internet Information Services
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
ISO	International Standards Organization
IT	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
PKI	Public Key Infrastructure
QR Code	Quick Response Code
RAM	Random Access Memory
RIS	Radiology Information System

DRAFT

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: <https://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html>
- [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: <https://dcm4che.atlassian.net/wiki/spaces/ee2/pages/2555918/Installation>.
- [6] SourceForge. dcm4che, a DICOM Implementation in JAVA. [Website]. Available: <https://sourceforge.net/projects/dcm4che/files/dcm4chee/>.
- [7] SourceForge. dcm4che, a DICOM Implementation in JAVA. [Website]. Available: <https://sourceforge.net/projects/dcm4che/files/dcm4chee-arr/3.0.11>.
- [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: <https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server-from-the-installation-wizard-setup?view=sql-server-2017>.
- [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: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf>.
- [11] DVTK. DVTK open source project main contributors ICT Group and Philips. [Website]. Available: <https://www.dvtk.org/>.
- [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-domain-controller-on-2012-r2.aspx>.
- [13] Microsoft TechNet. *Installing and Configuring DHCP role on Windows Server 2012*. [Website]. Available: <https://blogs.technet.microsoft.com/teamdhcp/2012/08/31/installing-and-configuring-dhcp-role-on-windows-server-2012/>.

- [14] *DigiCert*. CSR Creation Instructions for Microsoft Servers. [Website]. Available: <https://www.digicert.com/util/csr-creation-microsoft-servers-using-digicert-utility.htm>.
- [15] Cisco. *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*. [Website]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/fmfv/FMCv-quick.html.
- [16] Cisco. *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide*. [Website]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg.html.
- [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: 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.
- [19] G. O'Brien et al., *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*, NIST SP 1800-8, NIST, Gaithersburg, Md., Aug. 2018. Available: <https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf>.
- [20] *External Authentication libraries*, ConsoleWorks Cybersecurity Operations Platform [Website]. Available: <https://support.tditechnologies.com/content/external-authentication-libraries>.