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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

PACS fits within a highly complex healthcare delivery organization (HDO) environment that involves interfacing with a range of interconnected systems. PACS may connect with clinical information systems and medical devices and may involve engaging with health professionals who may be both internal and external to the HDO. This complexity may introduce or expose opportunities that allow malicious actors to compromise the confidentiality, integrity, and availability of the PACS ecosystem.

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

Name	Organization
Andy Gray	Forescout
Katherine Gronberg	Forescout
William Canter	Hyland
Kevin Dietz	Hyland
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

Contents

List of Figures

List of Tables

1 Introduction

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

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

1.1 Practice Guide Structure

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate all or parts of the example implementation that was built in the National Cybersecurity Center of Excellence (NCCoE) lab. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

NIST SP 1800-24A: *Executive Summary*

NIST SP 1800-24B: *Approach, Architecture, and Security Characteristics* – what we built and why

NIST SP 1800-24C: *How-To Guides* – instructions for building the example solution **(you are here)**

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

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary,* NIST SP 1800-24A, which describes the following topics:

challenges that enterprises face in securing the picture archiving and communication system (PACS)

example solution built at the NCCoE

benefits of adopting the example solution

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

Section 3.4, Risk Assessment, describes the risk analysis we performed.

Section 3.5, Security Control Map, maps the security characteristics of this example solution to cybersecurity standards and best practices.

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

IT professionals who want to implement an approach like this will find this whole practice guide useful. You can use this How-To portion of the guide, NIST SP 1800-24C, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of PACS security solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

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

Acronyms used in figures can be found in Appendix A.

1.2 Build Overview

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

1.3 Typographic Conventions

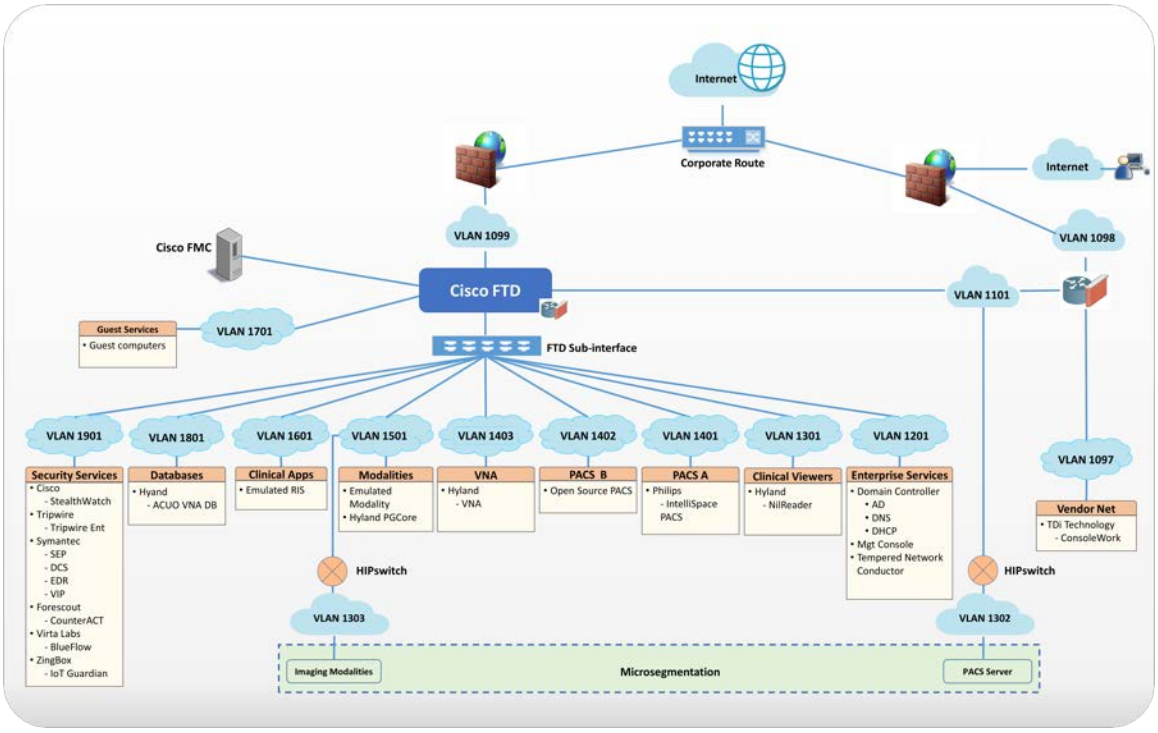
The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
Bold	names of menus, options, command buttons, and fields	Choose **File > Edit.**
`Monospace`	command-line input, onscreen computer output, sample code examples, and status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
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.

1.4 Logical Architecture Summary

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

Figure 1-1 PACS Final Architecture



2 Product Installation Guides

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

The project implemented security capabilities across the laboratory infrastructure, to safeguard the emulated modalities, emulated RIS, viewer workstations, and PACS and VNA systems. Security control

products that align with capabilities were implemented for the environment. Products that align with the security capabilities are enumerated in NIST 1800-24B, Section 3.6, Technologies, Table 3-5.

2.1 Picture Archiving and Communication System (PACS)

This project implemented two separate PACS: Philips IntelliSpace solution and an open source PACS (DCM4CHEE). These PACS systems are used to emulate the case where healthcare delivery organizations (HDOs) may have different PACS vendors installed in their environment.

2.1.1 Philips IntelliSpace PACS

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

System Requirements

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

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

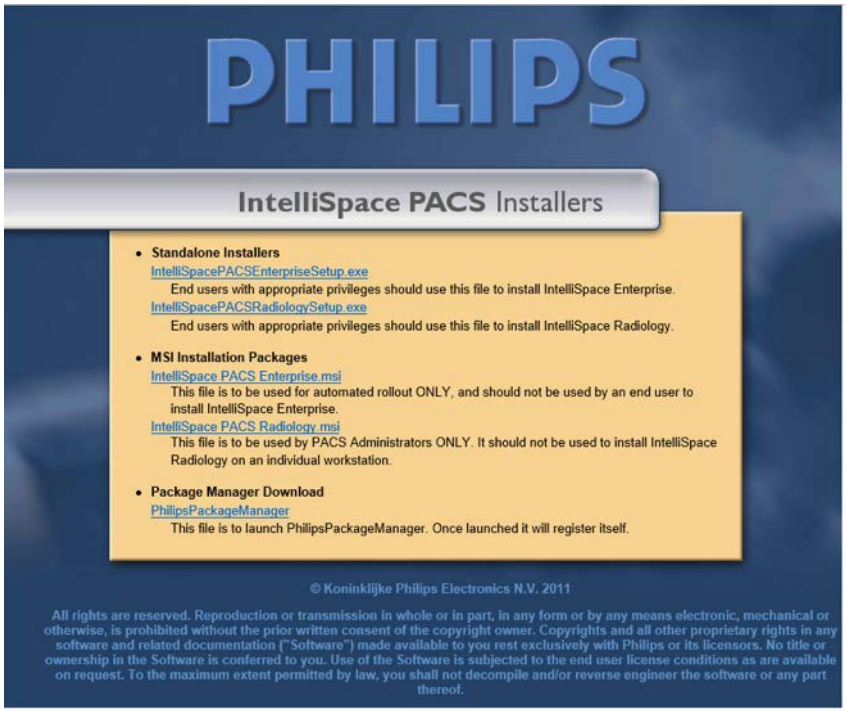
VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
	(DB), Anywhere Viewer (web client)					
UDM	Universal Data Manager (UDM), WEB DICOM services Image Lifecycle Management Image pre fetching from VNA	4	8 GB RAM	200 GB	Microsoft Windows Server 2012	Microsoft SQL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

IntelliSpace PACS Client Installation

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

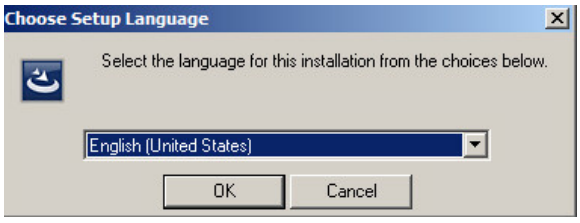
IntelliSpace PACS is a web-based distributed system. Clinicians, referring physicians, nurses, or bioengineers use web-based client application on workstations to view, analyze, and qualify medical images. Once the server components were installed, the web-based client installation was performed using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

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

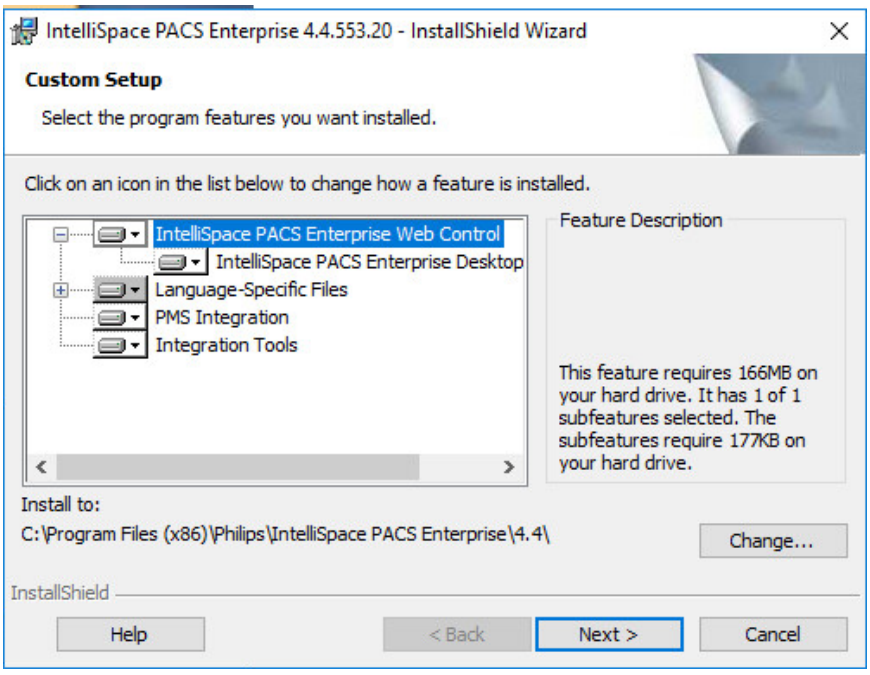


223

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

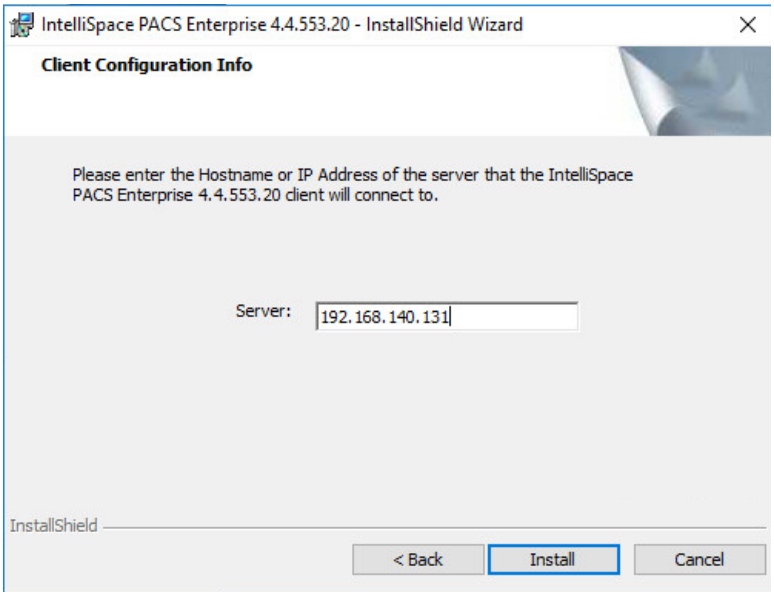
225

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



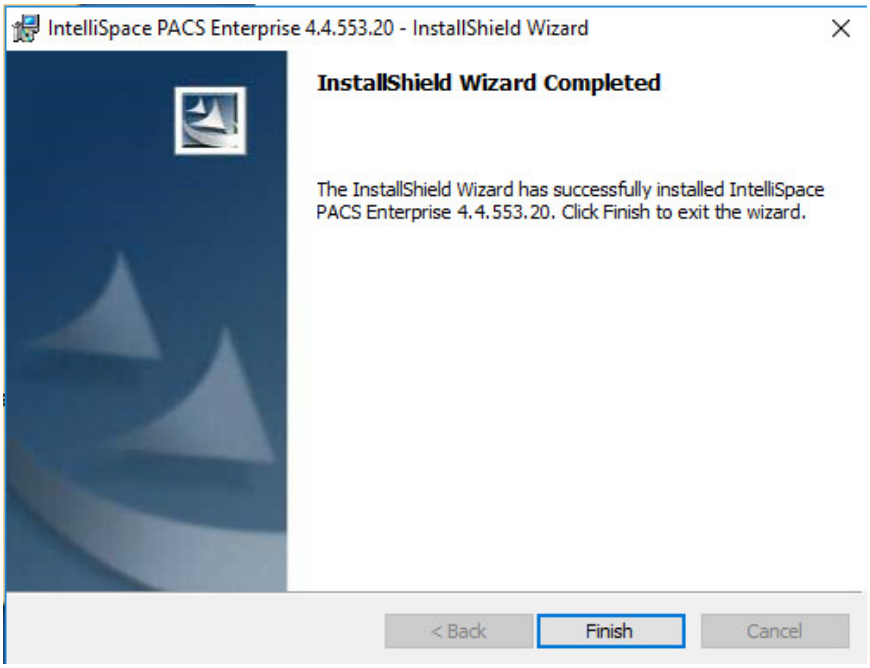
228

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



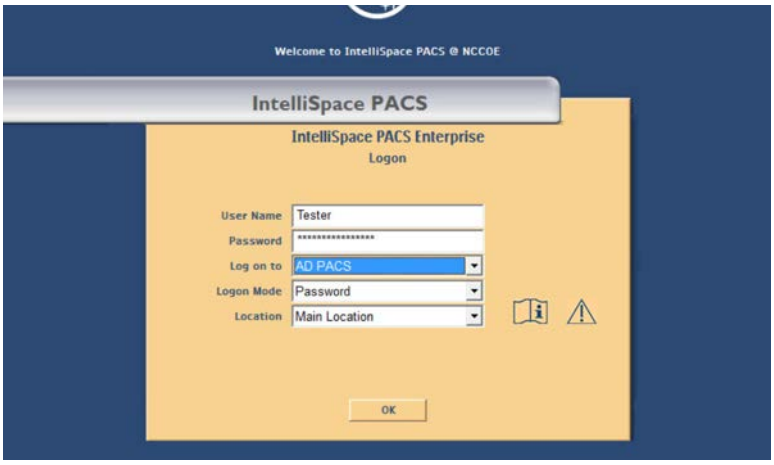
231

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



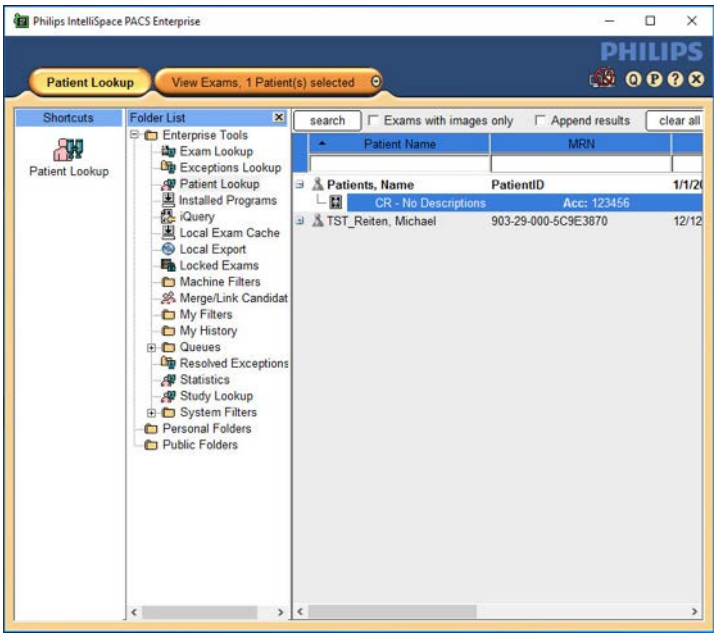
234

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



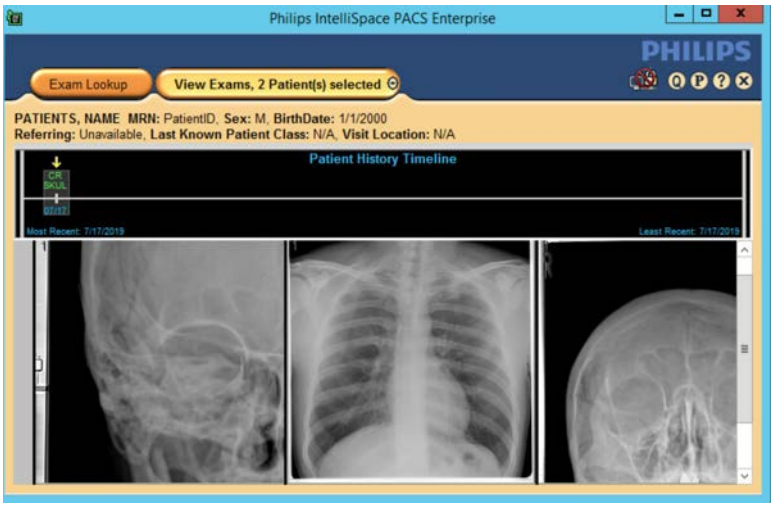
238

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



240

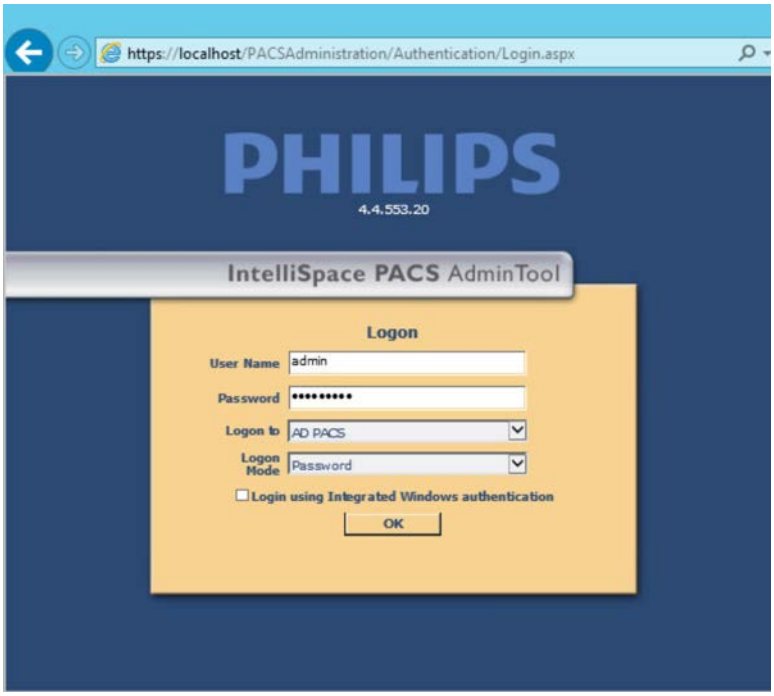
241 10. To view an exam, navigate to **Exam Lookup,** which lists a summary of a patient's exams. Double-
242 click an exam in the list. If the exam has an image, it will be displayed. An example is shown below.



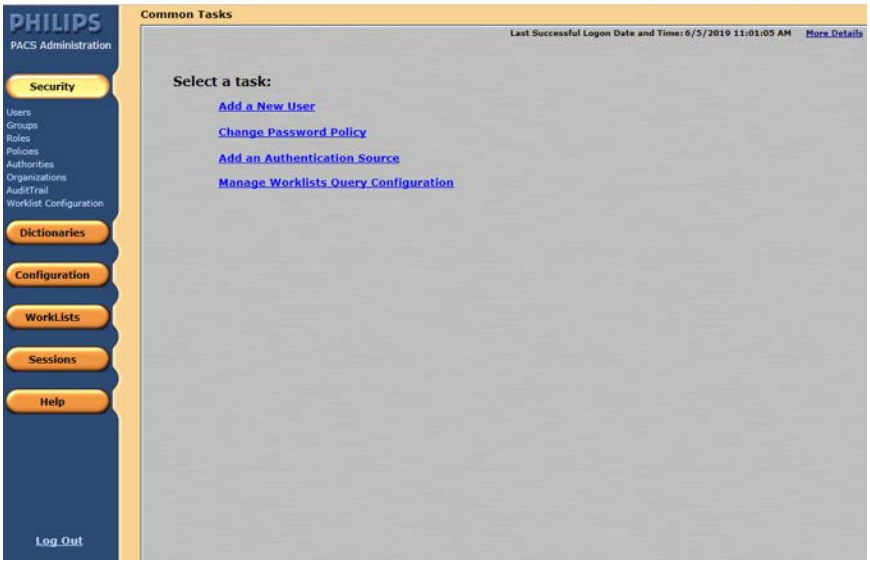
IntelliSpace PACS Client Configuration

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

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



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

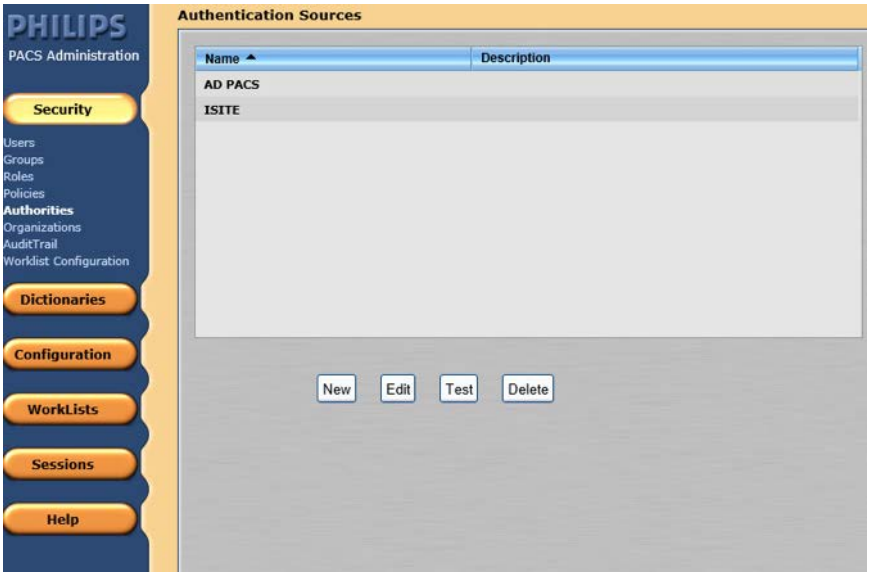


3. To add a new user, navigate to **SECURITY,** found on the far-left column of the Common Tasks screen, and click on **Users**.
   a. Enter the **User ID**.
   b. Enter the user's **First Name**.
   c. Enter the user's **Middle Name** (optional).
   d. Enter the user's **Last Name**.
   e. Enter the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

Configure Sources for User Authentication

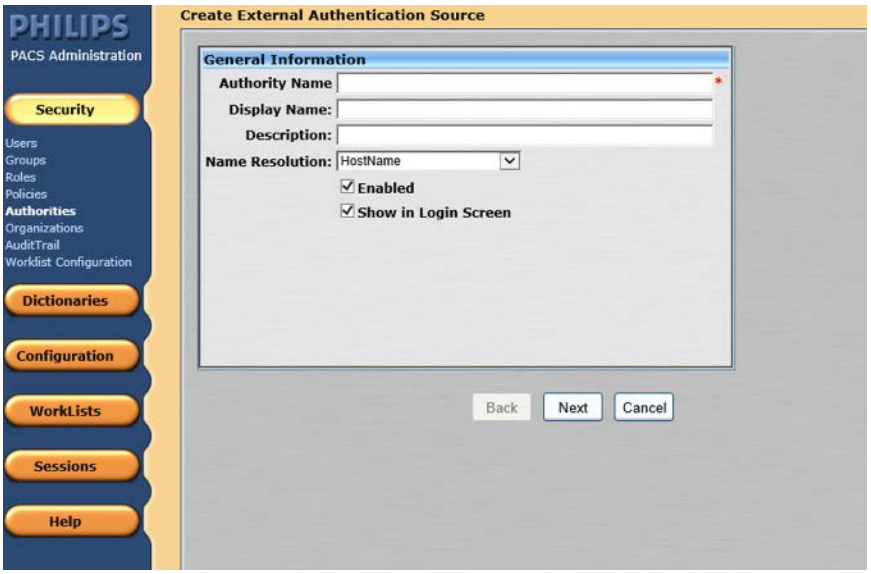
IntelliSpace supports either a locally hosted or an external authentication source. An authentication source provides a directory structure that authenticates and manages user and group accounts. The internal authentication source, called iSite, implements a local database of users and groups. IntelliSpace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

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



271

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



273

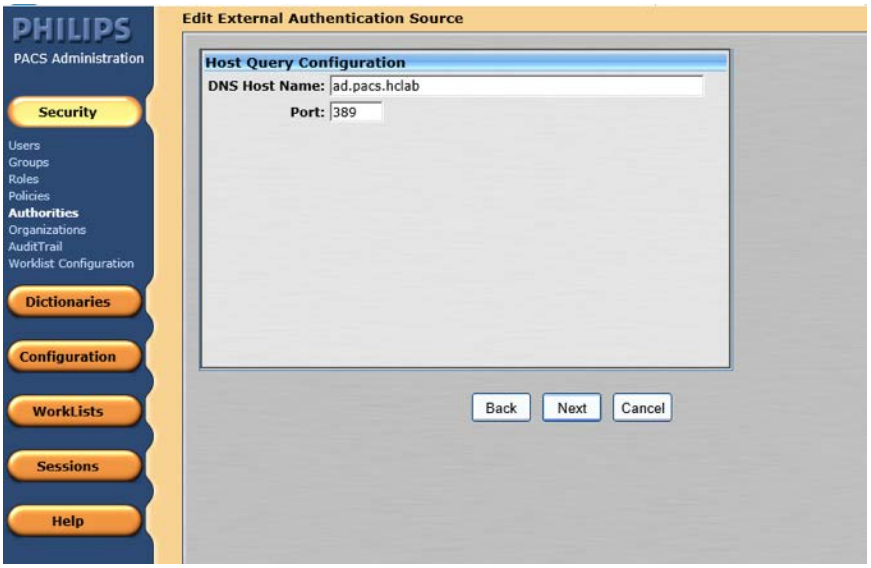
274 3. On the **External Authentication** source page, set the following values and then click **Next**.

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**.

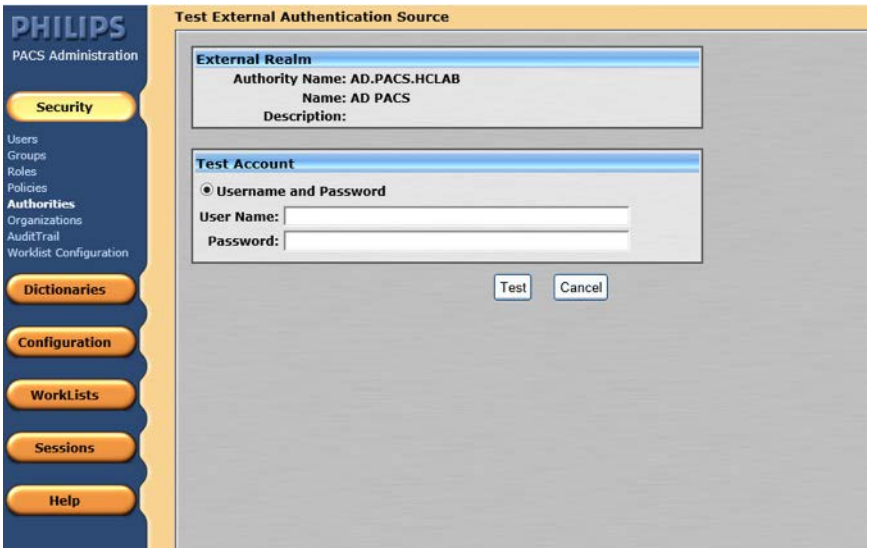


282

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**.

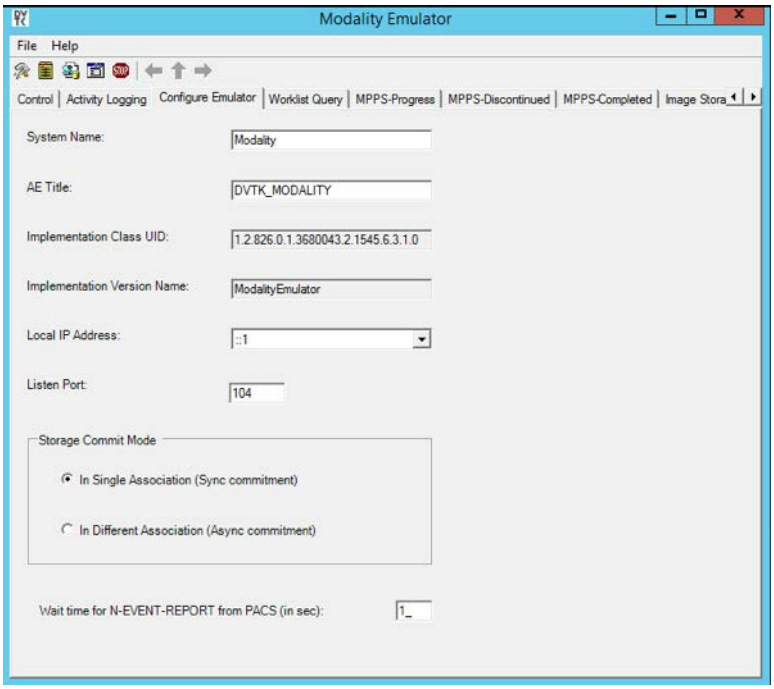


289

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:

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



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

RIS System

- **IP Address:** *192.168.160.201*
- **Remote Port:** 105
- **AE Title:** DVTK_RIS

MPPS Manager

- **IP Address:** *192.168.160.201*
- **Remote Port:** 108
- **AE Title:** DVTK_MPPS

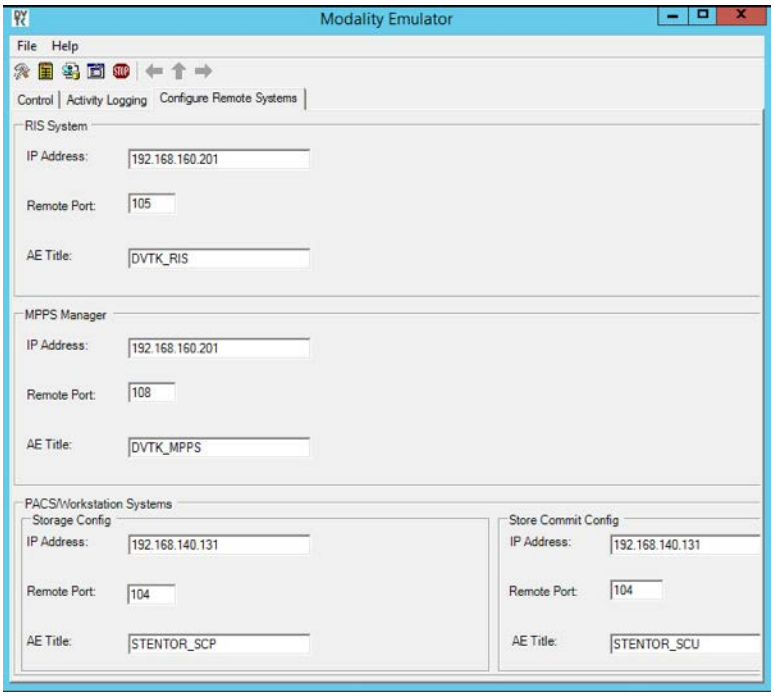
PACS/Workstation Systems–Storage Config

- **IP Address:** *192.168.140.131*

- **Remote Port:** 104
- **AE Title:** STENTOR_SCP

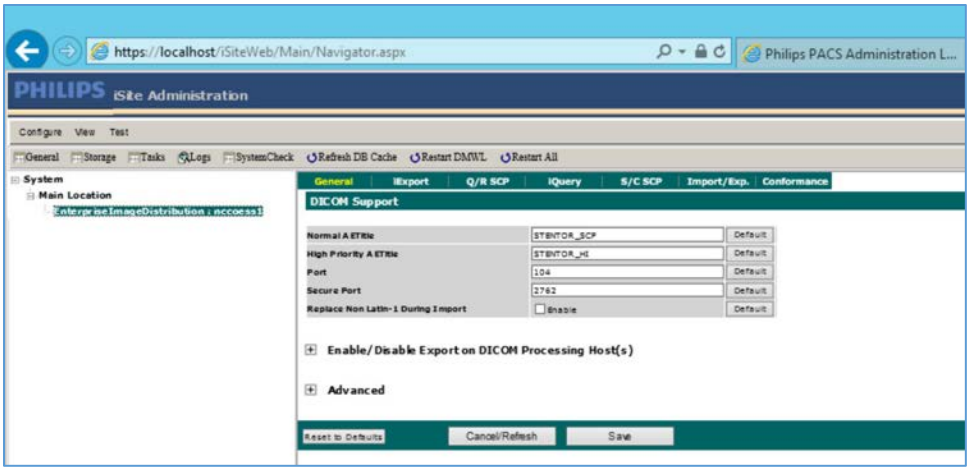
PACS/Workstation Systems–Storage Commit Config

- **IP Address:** *192.168.140.131*
- **Remote Port:** 104
- **AE Title:** STENTOR_SCU

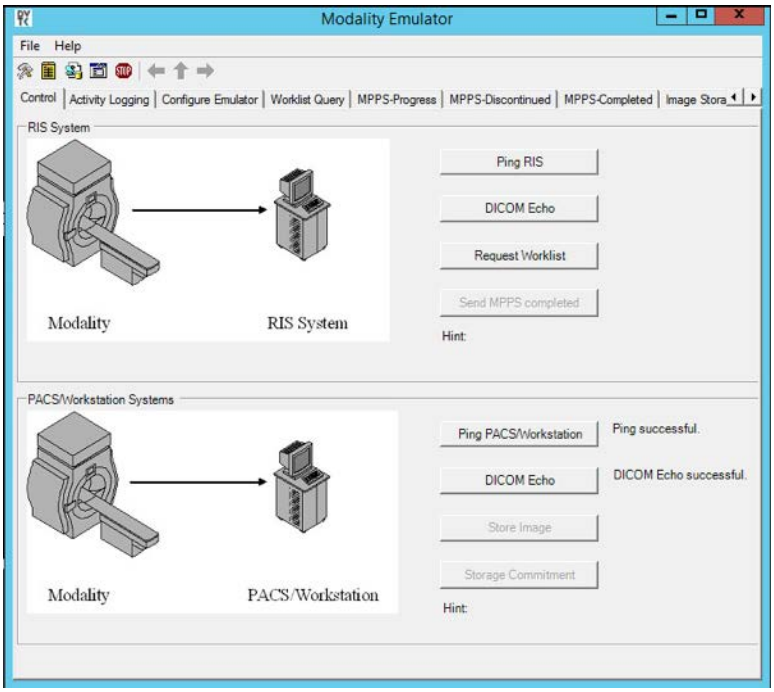


3. To configure the Philips IntelliSpace PACS AE Title and communication port, log on to the iSite Administration web site using the URL *https://192.168.140.131/ iSiteWeb*. Select **Configure > DICOM > General,** set the following values, and then click **Save** to save the settings.

- **Normal AE Title:** STENTOR_SCP
- **High-Priority AE Title:** STENTOR_HI
- **Port:** 104
- **Secure Port:** 2762



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

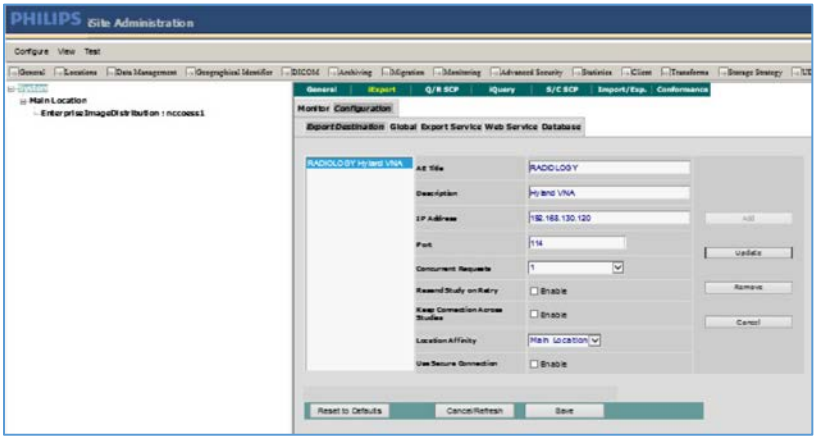


Configure IntelliSpace PACS to Communicate with Hyland VNA

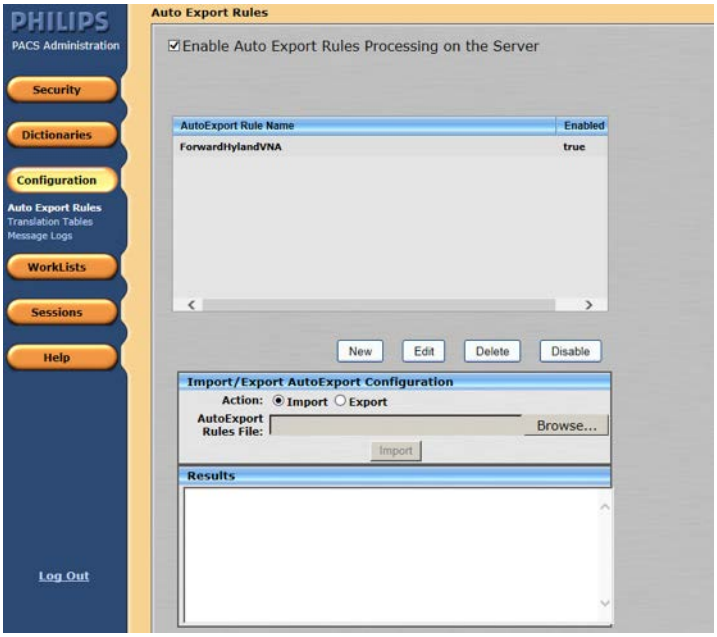
Refer to Section 2.2.2 for detailed installation guidance for Hyland VNA.

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

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

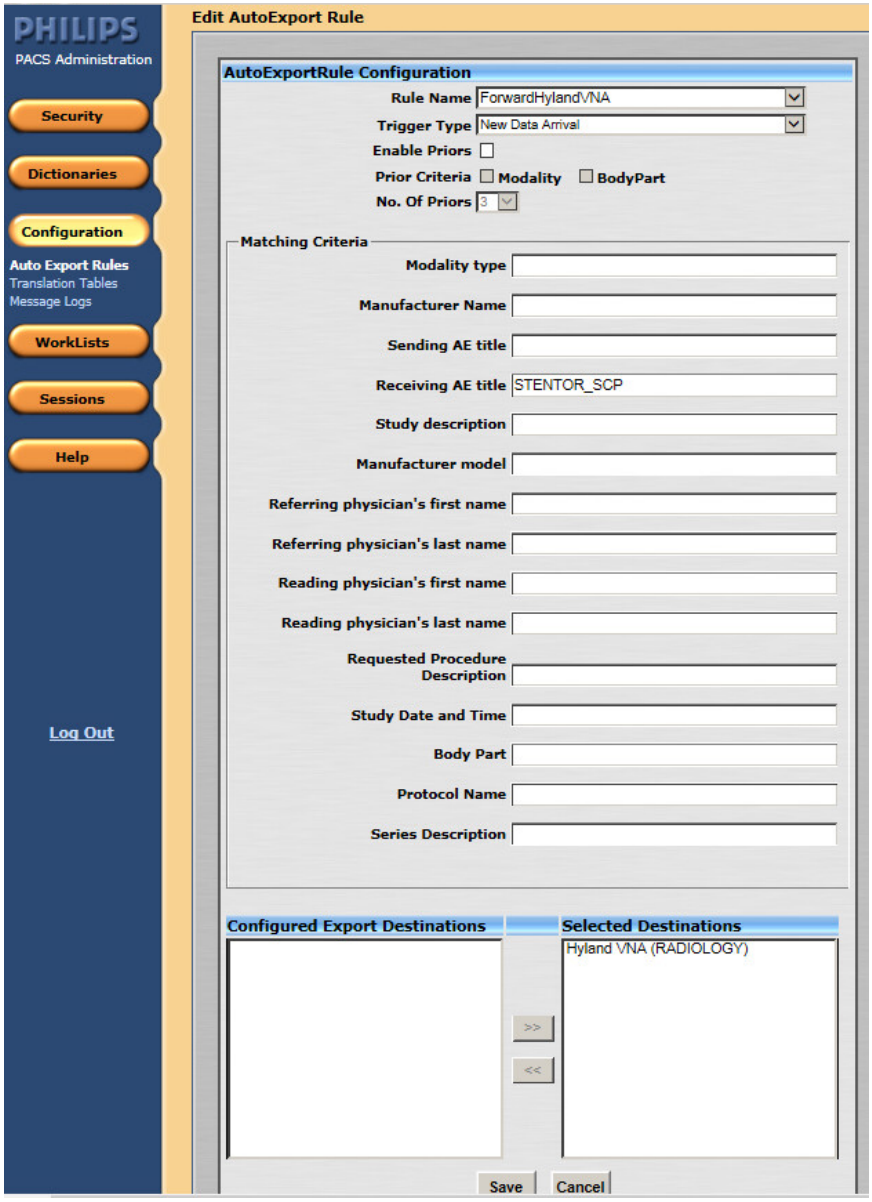


4. Log in to the IntelliSpace PACS Administration page using *https://192.168.140.131/PACSAdministration*.
5. Click the **Configuration** button on the left panel to configure the **Auto Export Rule.**
6. Click the **New** button to create a new rule named **ForwardHylandVNA**.



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

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



2.1.2 DCM4CHEE

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

communicate with DVTk's Modality Emulator to store images in a PostgreSQL database. The JBoss web interface allows an administrator to configure DCM4CHEE to listen for connection requests from specific application entities like DVTk's Modality Emulator. DCM4CHEE also has web-based GUI that displays patient records sent from the Modality Emulator and stored in the PostgreSQL database.

A 32-bit version of Java JDK6 [1], JBoss v4.2.3 [2], and PostgreSQL database v 9.4.23 [3], [4] were installed as the prerequisites for the DCM4CHEE. Refer to each installation guide for the installation procedures.

System Requirements

CPU: 4

Memory: 512 megabyte (MB) RAM

Storage: 200 MB

Operating System: Microsoft Windows Server 2016 Datacenter

Network Adapter: Virtual Local Area Network (VLAN) 1402

DCM4CHEE Installation

The installation guide can be found at [5].

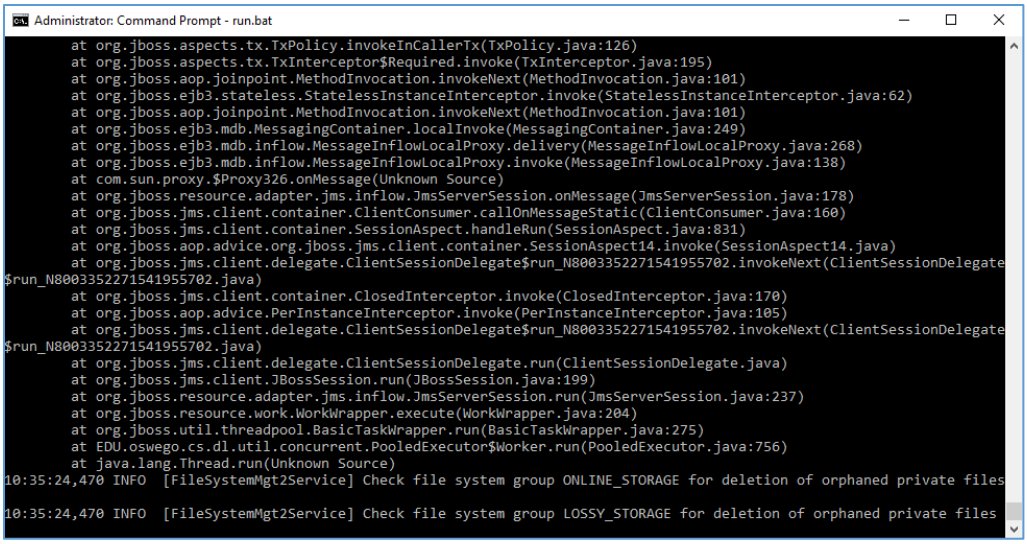
1. Go to https://www.dcm4che.org to download the software.
2. In the left-hand side of the page, click the **Wiki** link under Community.
3. Click the **here** link under **Download Latest Version** nest to **dcm4chee DICOM Archive 2 (includes dcm4che toolkit 1.4)** [6] link on the right-hand side of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

DCM4CHEE Audit Report Repository Installation

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

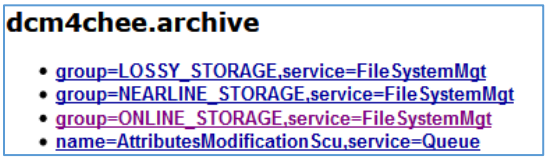
Test the DCM4CHEE Installation

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

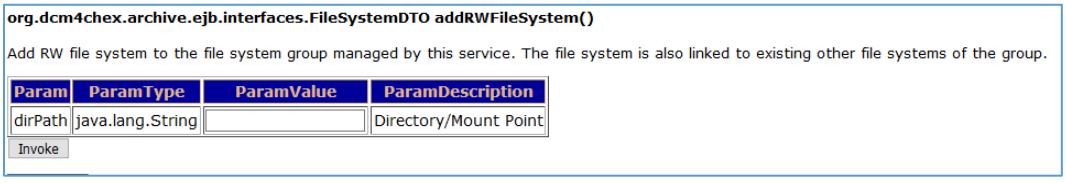


DCM4CHEE Configuration Using the JMX Console

1. Access the JMX Console GUI by navigating to *http://localhost:8080/jmx-console/* and providing the following credentials:
   - **Username**: admin
   - **Password**: *****
2. Click the link **group=ONLINE_STORAGE,service=FileSystemMgt** under the dcmrchee.archive heading.



3. Click the **Invoke** button under the **addRWFileSystem()** section to instantiate where archived data should be stored. If no specific file path is provided as a parameter, the default location is *dcm4chee-2.7.1-psql\server\default\archive.*

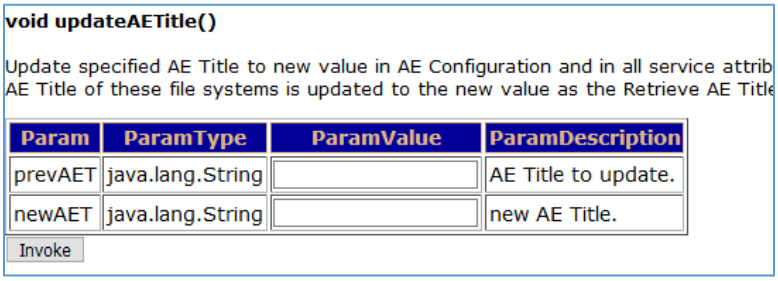


4. Change the default AE Title:

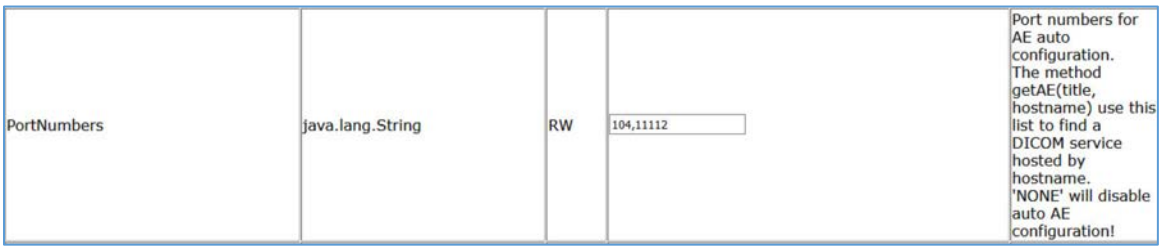
a. The default AE Title is **DCM4CHEE**.

b. Change the title by clicking the **service=AE** link under dcm4chee.archive heading.

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



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

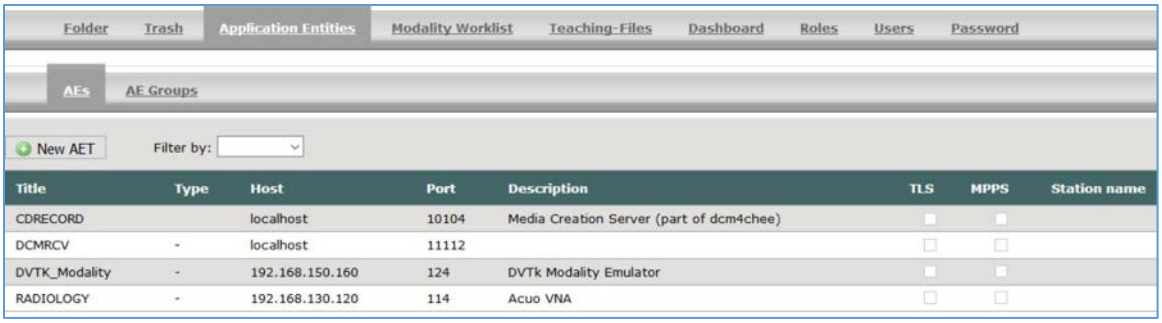


DVTk Modality to DCM4CHEE Configuration

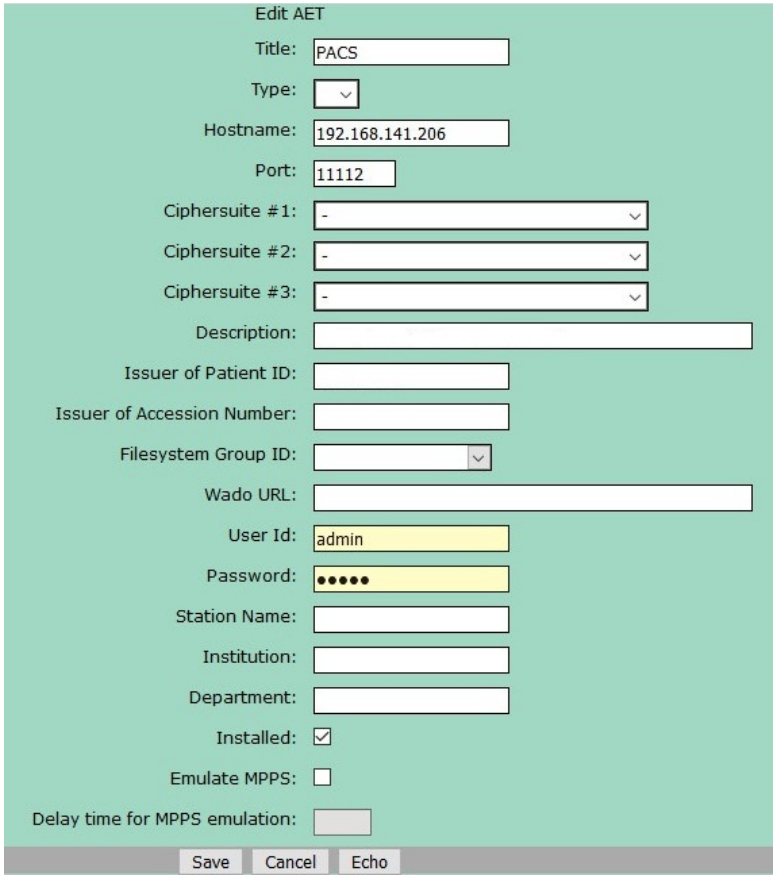
1. Open a web browser to access *http://localhost:8080/dcm4chee-web3/* and provide the following credentials:

   - **Username**: admin
   - **Password**: *****

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

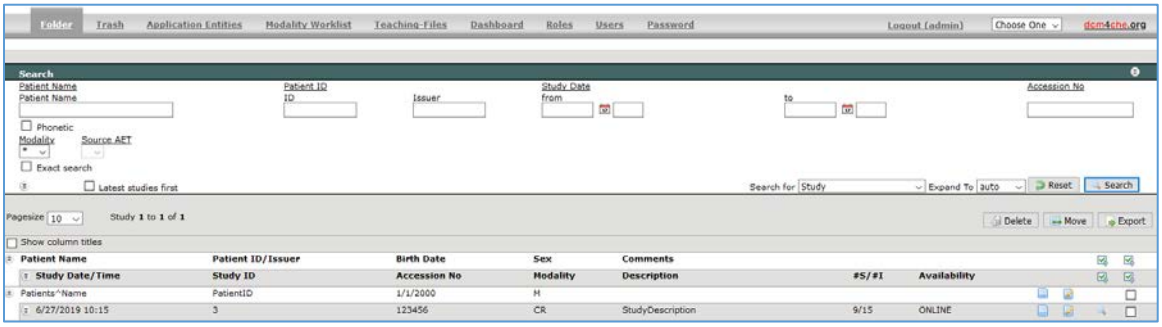


3. Click the **New AET** button in the left-hand side of the AEs page and provide the following information:
   - **Title**: PACS
   - **Type**: -
   - **Hostname**: *192.168.141.206*
   - **Port**: 11112
   - **User Id**: Admin
   - **Password**: *****
4. Click the **Save** button at the bottom center of the screen.



View Stored Data

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



DCM4CHEE to DVTk Modality Configuration

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

RIS System

- **IP Address:** *192.168.160.201*
- **Remote Port:** 105
- **AE Title:** RIS

MPPS Manager

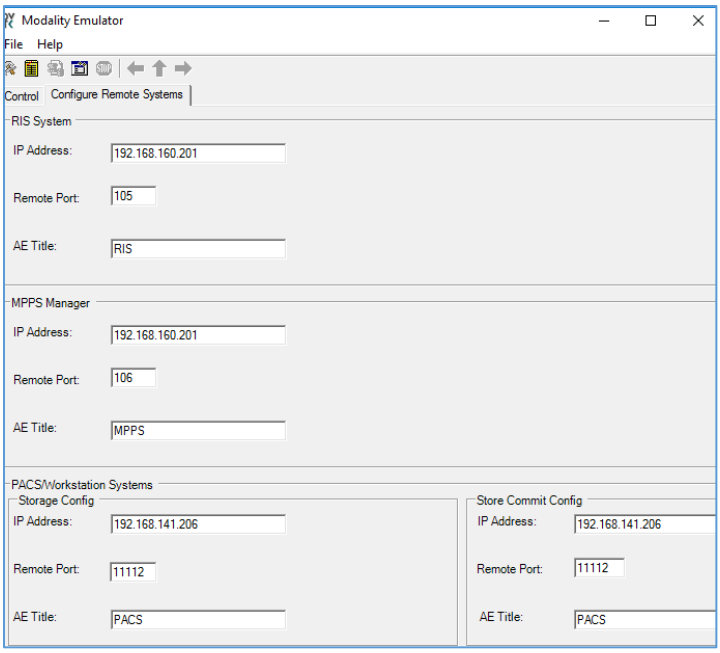
- **IP Address:** *192.168.160.201*
- **Remote Port:** 106
- **AE Title:** MPPS

PACS/Workstation Systems–Storage Config

- **IP Address:** *192.168.141.206*
- **Remote Port:** 11112
- **AE Title:** PACS

PACS/Workstation Systems–Storage Commit Config

- **IP Address:** *192.168.141.206*
- **Remote Port:** 11112
- **AE Title:** PACS



Oviyam Installation

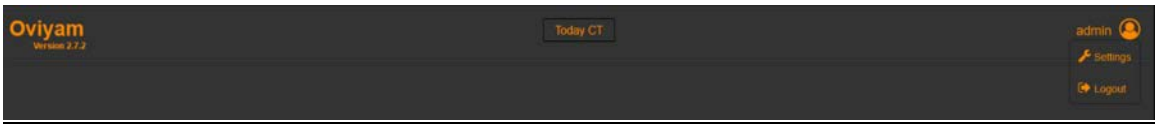
Once downloaded from the SourceForge [8] and unzipped, copy the *oviyam.war* file to the following directory: *dcm4chee-2.7.1\server\default\deploy.* Check if you successfully installed the software by visiting *http://dcm4chee_ip:8080/oviyam2* and accessing a log in screen.

Oviyam Configuration

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

    - **Username**: admin
    - **Password**: *****

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



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

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

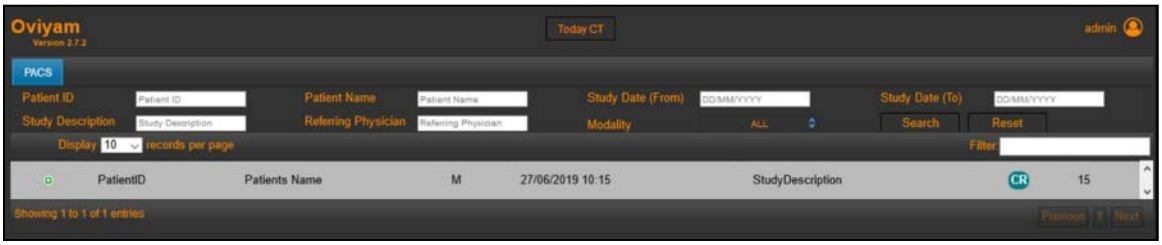
- **Description:** PACS
- **AE Title:** DCM4CHEE
- **Host Name:** localhost
- **Port:** 11112
- **Retrieve Type:** WADO
- **WADO Context:** wado
- **WADO Port:** 8080
- **Image Type:** JPEG

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

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

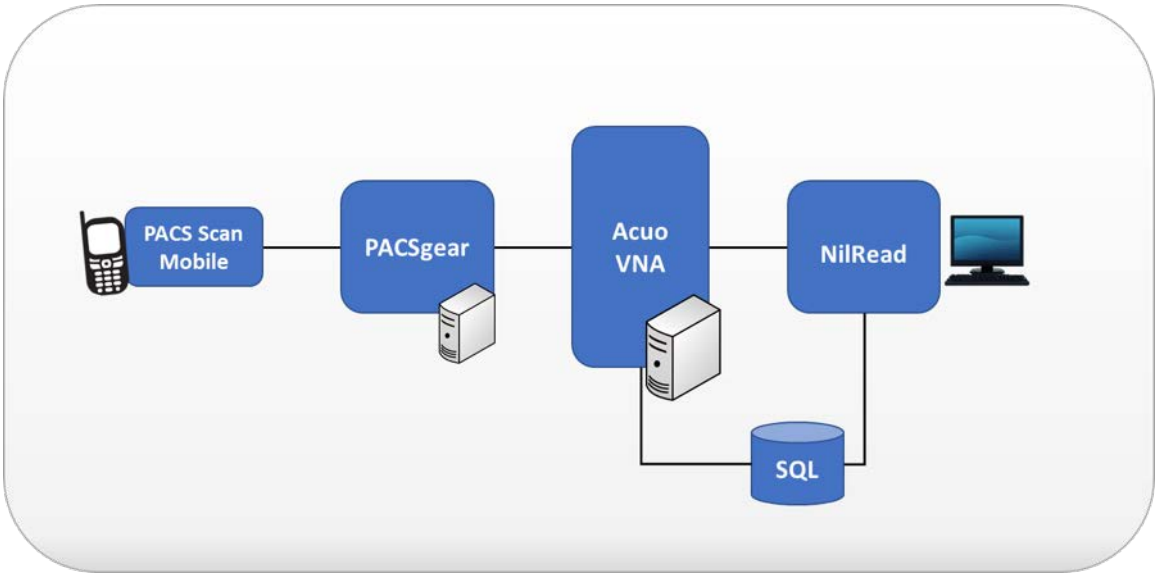
484 **PACSgear Core Server:** image processing and routing server, and back-end services

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

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

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

Figure 2-1 Hyland Systems and Applications Connectivity



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

2.2.1 Hyland Database Server

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

System Requirements

CPU: 4

Memory: 12 GB RAM

Storage:

- Hard Drive (HD)1: 80 GB (Operating System Install)
- HD 2: 20 GB (DB Drives)
- HD 3: 10 GB (Tx Logs)

Operating System: Microsoft Windows Server 2016

Network Adapter: VLAN 1801

Hyland Database Server Installation

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

Hyland Database Configuration

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

2.2.2 Hyland Acuo VNA

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

System Requirements

CPU: 6

Memory: 12 GB RAM

Storage:

- HD 1: 80 GB (OS Install)
- HD 2: 80 GB (Dilib Cache Drive)
- HD 3: 500 GB (Image Cache Drive)

Operating System: Microsoft Windows Server 2016

Network Adapter: VLAN 1301

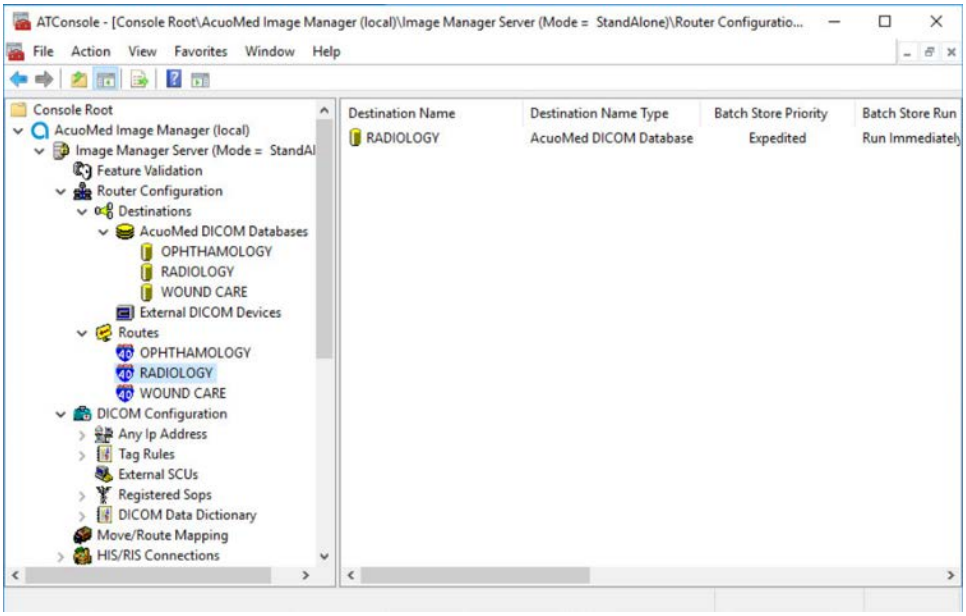
Hyland Acuo VNA Installation

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

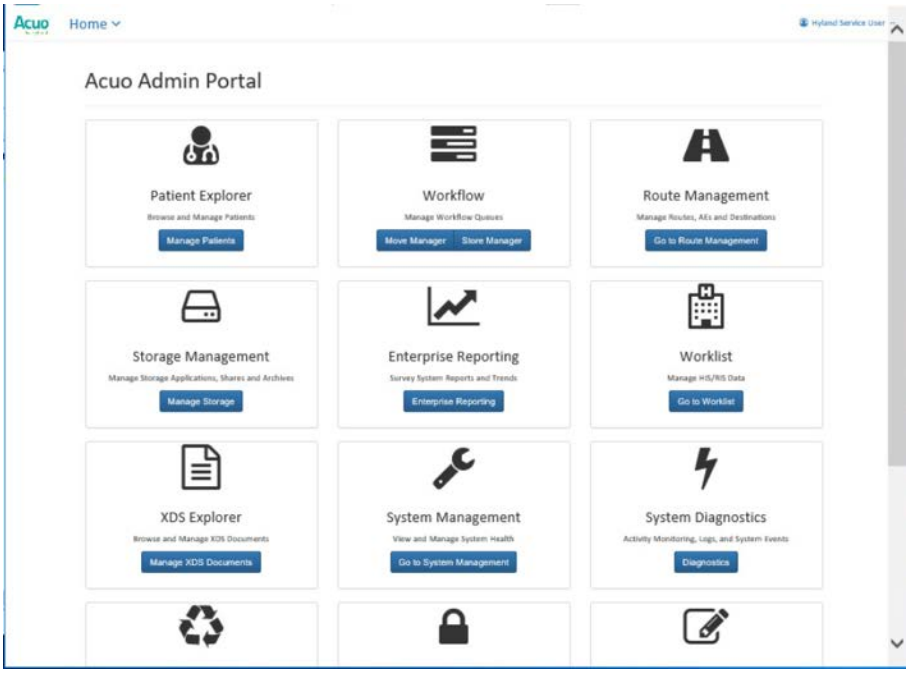
2. Upon completion of the installation, three Windows services were created: AcuoMed, AcuoAudit, and AcuoStore. AcuoMed is associated with a DICOM database containing the patient, study, and series record information that describes the images physically present on the Acuo VNA archive system. The AcuoStore also has its own database for storing information related to the bulk storage of digital images and related data, including information about the shares and about the applications that use those shares.
3. The installation created a web application for the AcuoAdmin Portal, where a Secure Sockets Layer (SSL) certificate signed by DigiCert was created and assigned to the application for hypertext transfer protocol secure (HTTPS) enforcement.

Hyland Acuo VNA Configuration

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



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

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

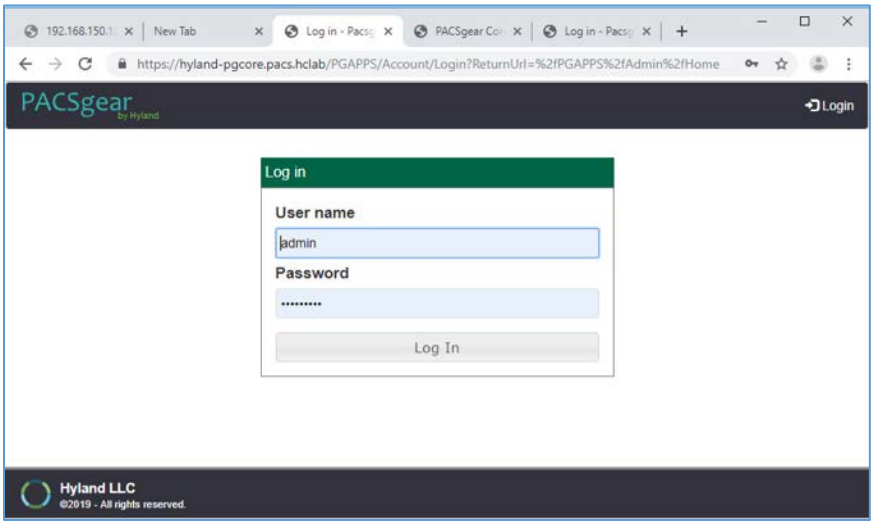
PACSgear Core Server Configuration

Configuration of the PACSgear Core Server was performed by the Hyland engineers. The basic configuration involves managing connection settings to external devices, lookup data sources, and event trace; managing departments for multi tenancy architecture; managing user access; and many more features. Each organization will configure the PACSgear based on its specific needs.

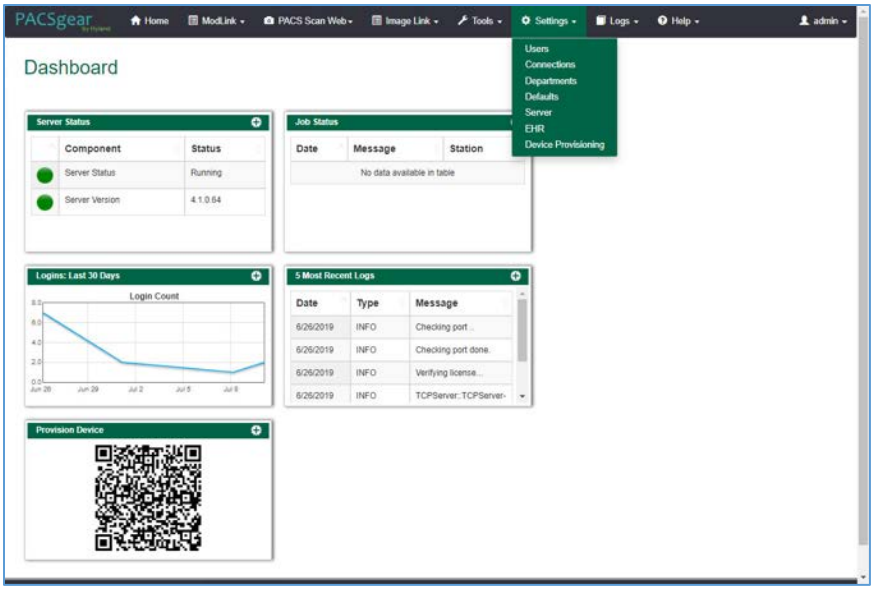
During the database configuration, the Hyland engineers created instances for representative departments (e.g., ophthalmology, radiology, and departments that may see patients who need wound treatment).

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

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

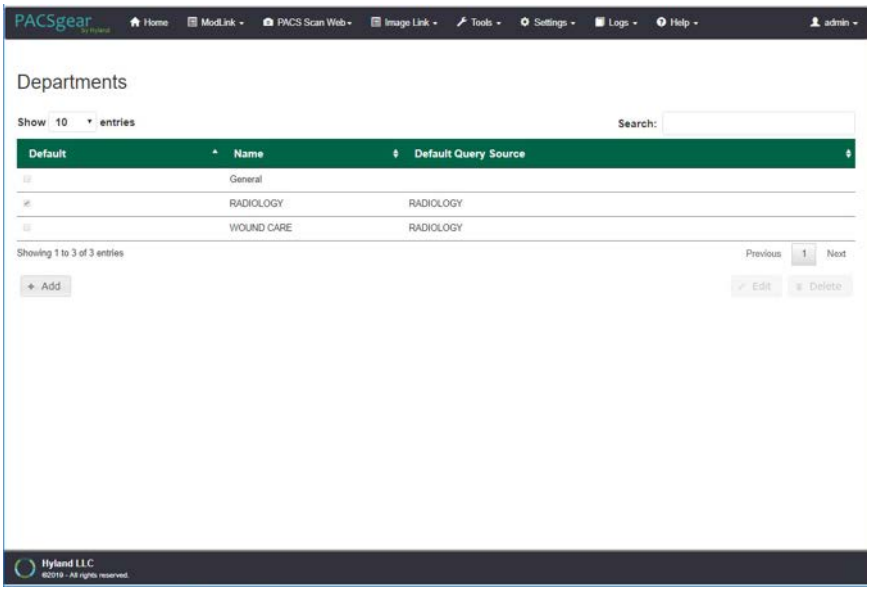


2. On the **Settings** menu, select **Departments.**



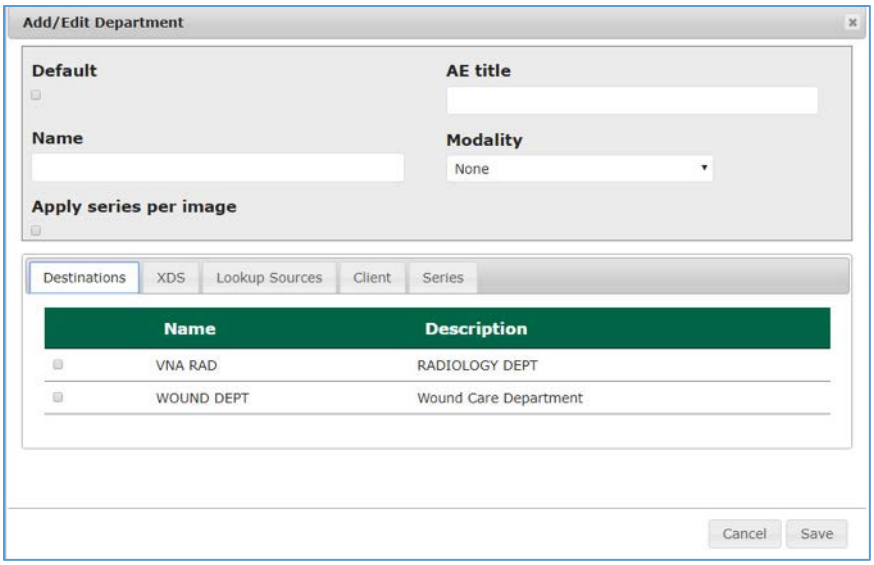
585

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.

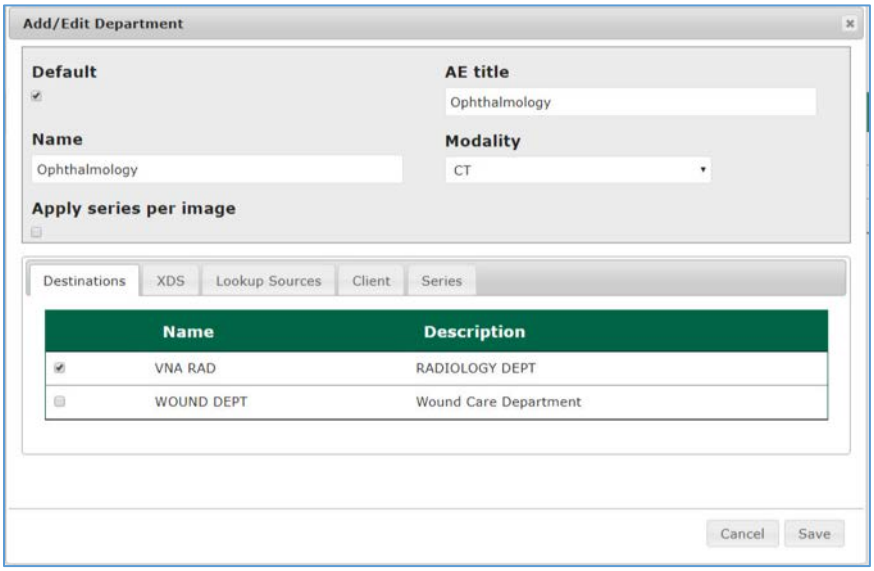


589

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

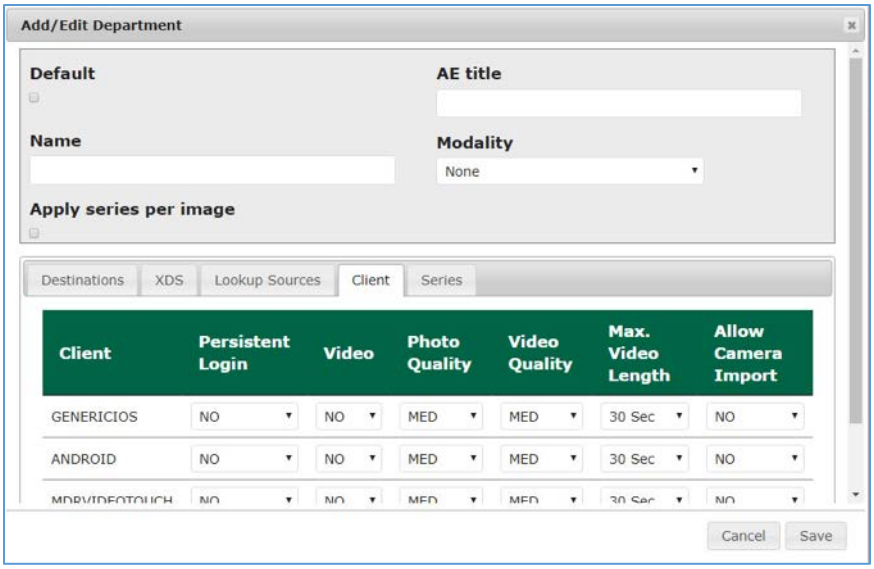


5. In the **Name** text box, the engineers entered **Ophthalmology** to create a department that ties with the Ophthalmology database instance created during database configuration. Engineers also added the **AE title** as **Ophthalmology** and selected a **CT Scan** for the modality.



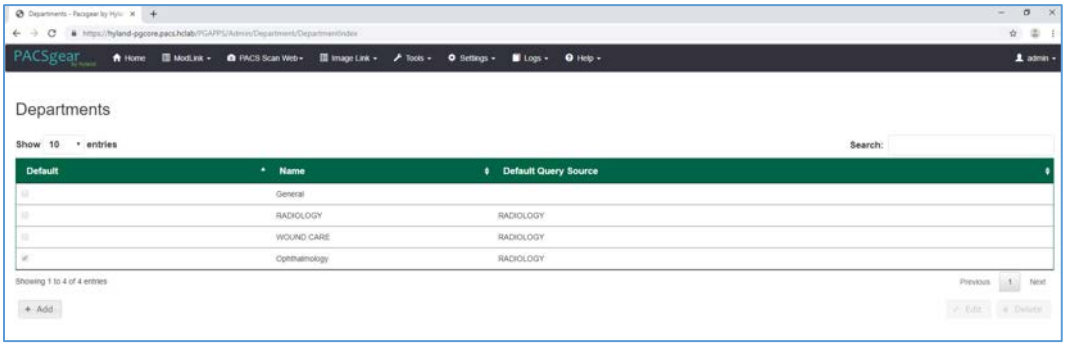
6. On the **Destinations** and **Lookup Sources** tabs, the engineers set up the destination and lookup sources for each department.

7. On the **Client** tab, the engineers set up the client access permissions to this department's resources.



8. On the **Series** tab, click **Add,** type a description, click **Save.**

9. Verify that the department has been added to the list, based on what is displayed.

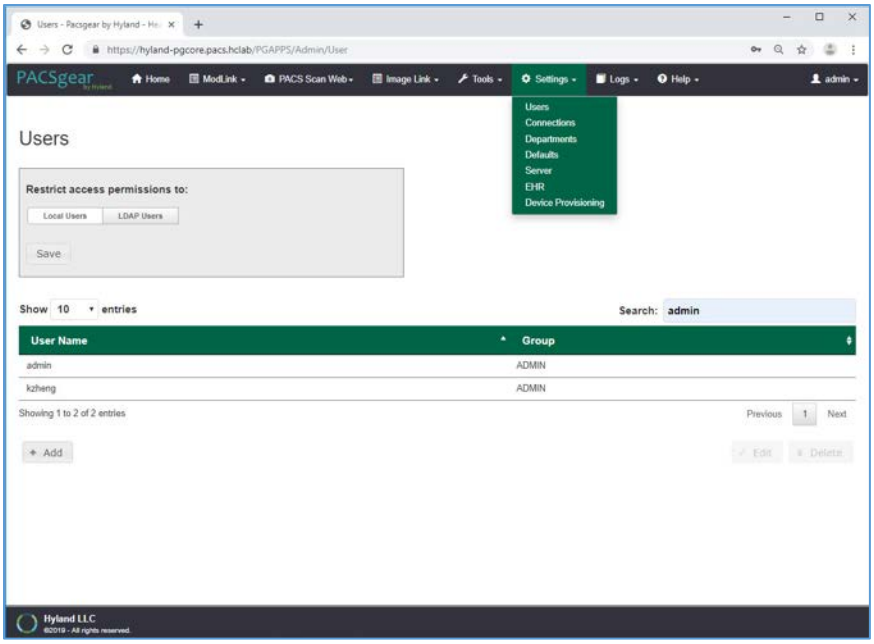


Add LDAP/Active Directory Server: - to use an LDAP/Active Directory server, configure these parameters:

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

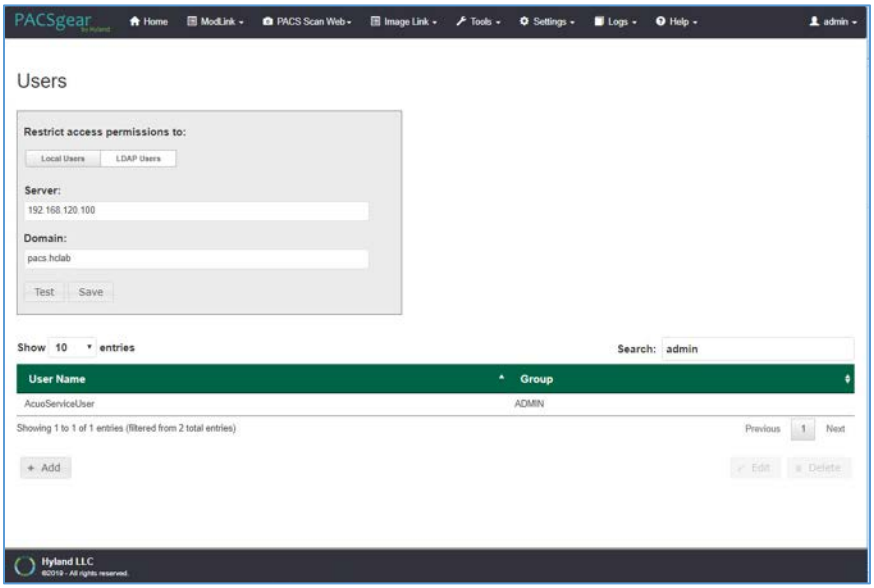
2. Using a browser, log on to the **PACSgear Admin** portal by using *https://hyland-pgcore.pacs.hclab/PGAPPS/Admin*.

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



611

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

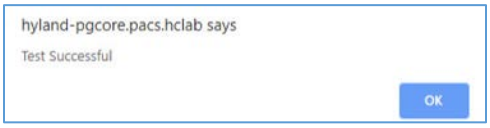


615

616 5. Click the **Test** button located under the **Domain** entry box.

617 6. Enter the **LDAP_User** credentials to verify connectivity to the AD.

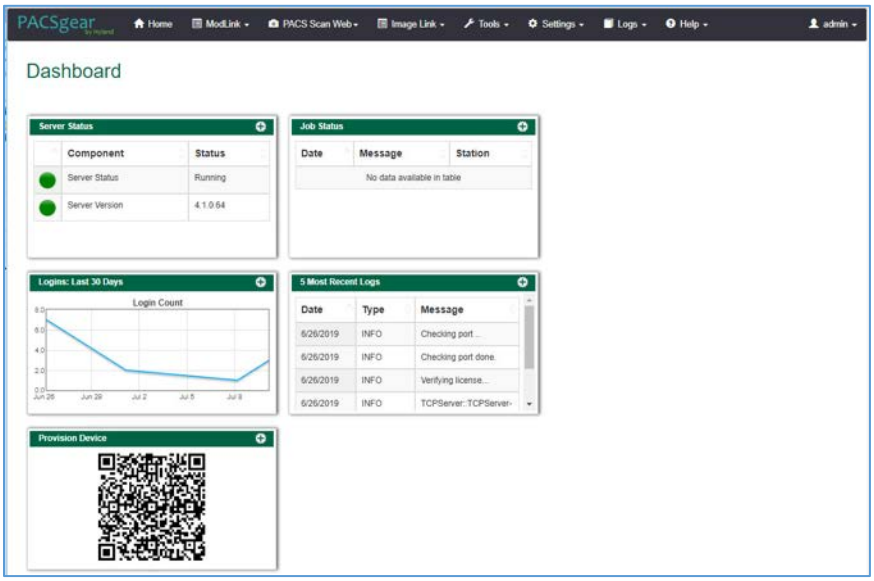
7. A message box appears indicating the test is successful. Click **OK.**



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

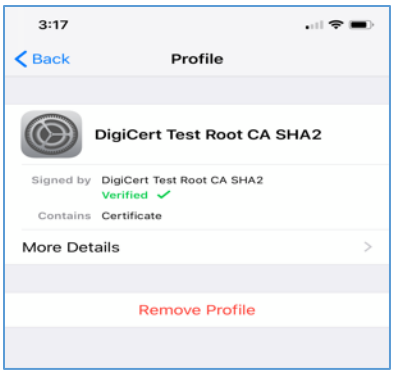
1. On the iPhone, navigate to the **App Store.** Search for PACS Scan Mobile, from Perceptive Software. Perceptive Software is a Hyland business unit. Select the **GET** button to install the software, and then select the **OPEN** button. Select **Allow** to permit the software to send notifications.

2. On a workstation, log in to **PACSgear Core Server** by using the administrator credentials; a dashboard will display and provide a **Provision Device QR code.**



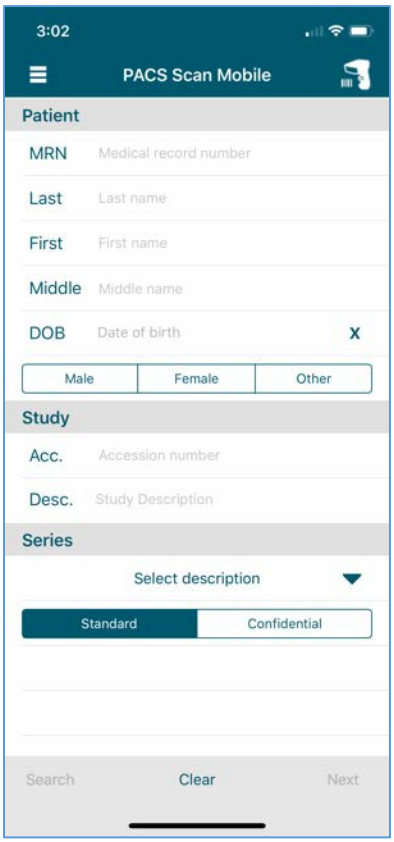
3. On the mobile device **PACS Scan App,** tap the **QR code** icon that appears under the **Log In** button. This will turn on the built-in camera on the iPhone.

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

2.2.4 Hyland NilRead

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

System Requirements

CPU: 6

Memory: 12 GB RAM

Storage:

- HD 1: 80 GB (OS Install)
- HD 2: 200 GB (Web Application)
- HD 3: 100 GB (Image Cache)

Operating System: Microsoft Windows Server 2016

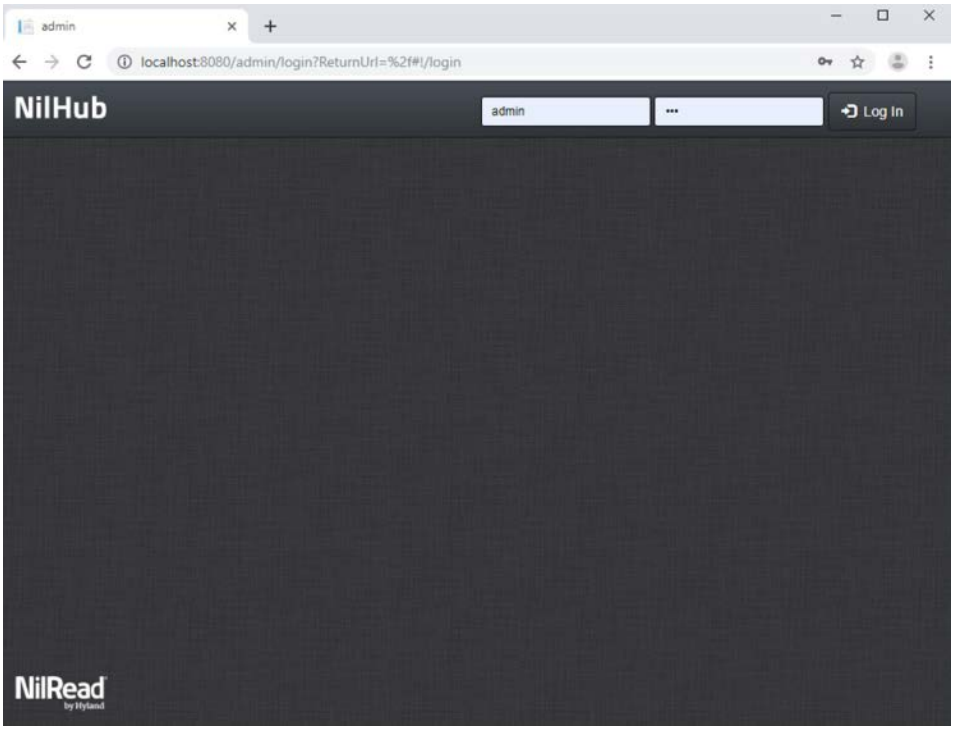
Network Adapter: VLAN 1301

Hyland NilRead Installation

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

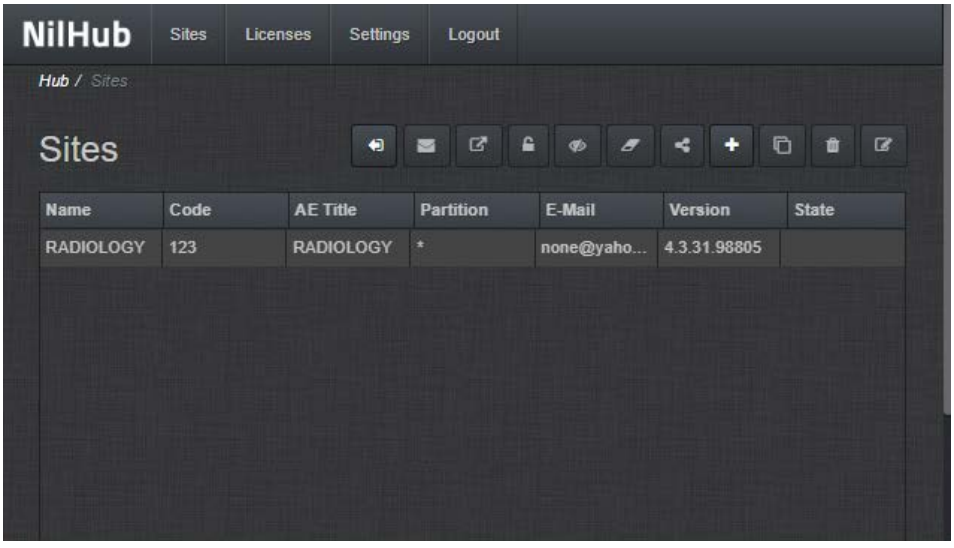
Hyland NilRead Configuration

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



675

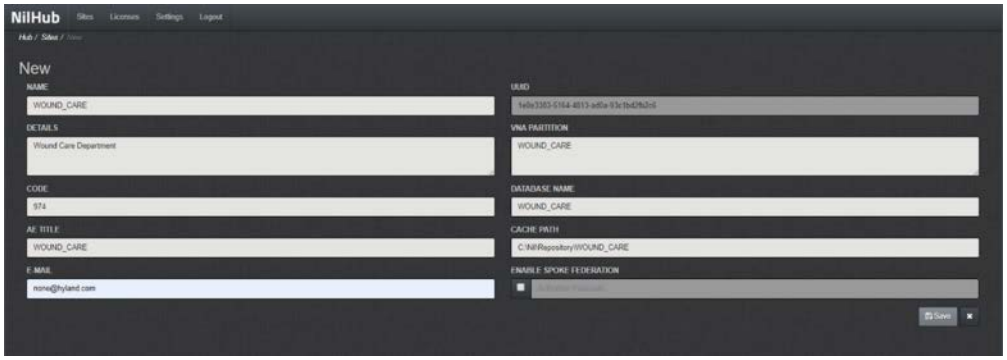
676 1. To add a new site from the **NilHub** home page, click on the Sites tab in the top left-hand side of the
677 screen.



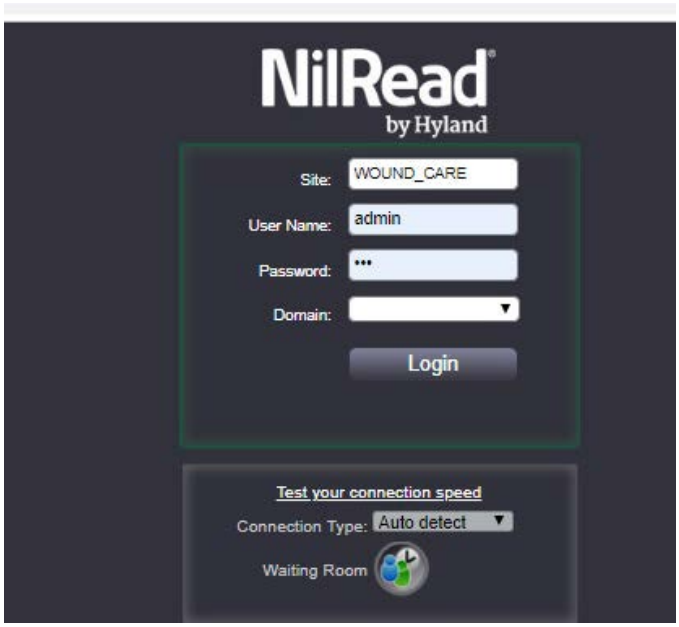
678

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.**

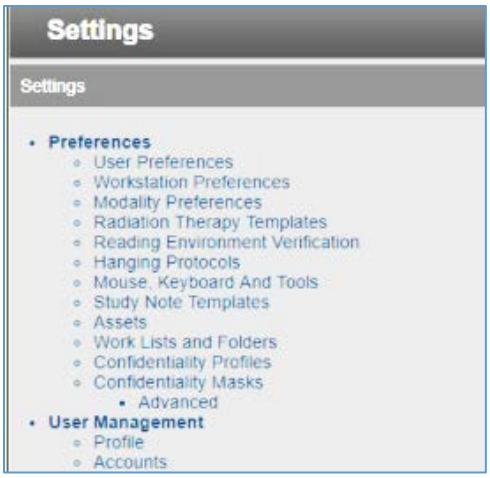
- **Name:** WOUND_CARE
- **Details:** Wound Care Department
- **Code:** 974
- **AE Title:** WOUND_CARE
- **VNA Partition:** WOUND_CARE
- **Database Name:** WOUND_CARE
- **Email:** *none@hyland.com*



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



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.

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

2.3 Secure DICOM Communication Between PACS and VNA

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

2.3.1 Public Key Infrastructure (PKI) Certificate Creation

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

2.3.1.1 Create PKI Certificate for Hyland Acuo VNA

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

2.3.1.2 Create PKI Certificate for Philips IntelliSpace PACS

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

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

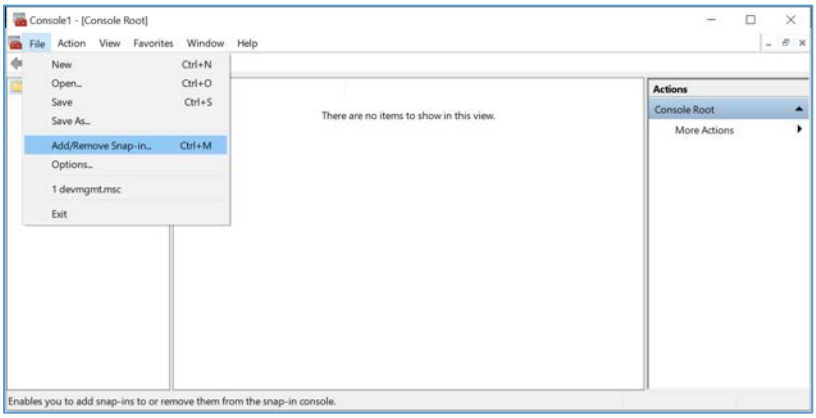
2.3.2 PKI Certification Installation

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

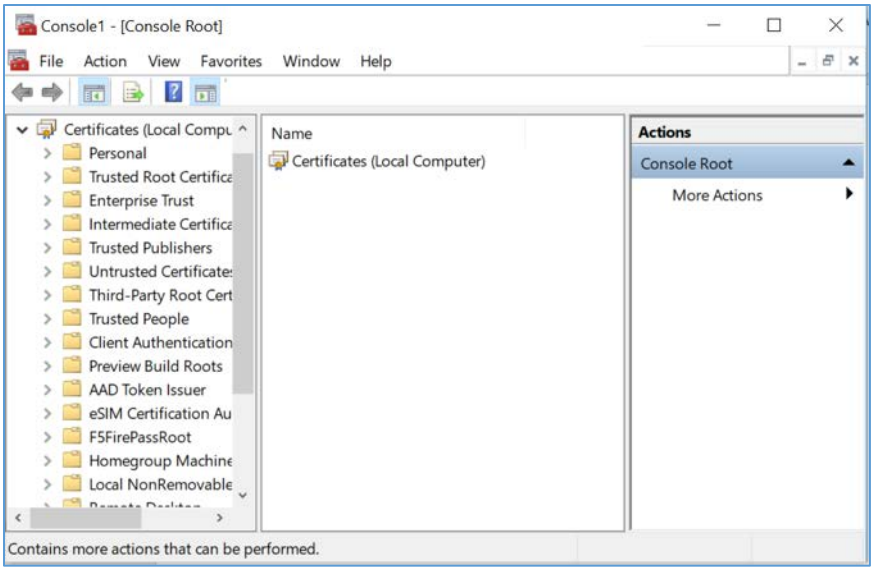
2.3.2.1 Install PKI Certificate for Hyland Acuo VNA

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

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

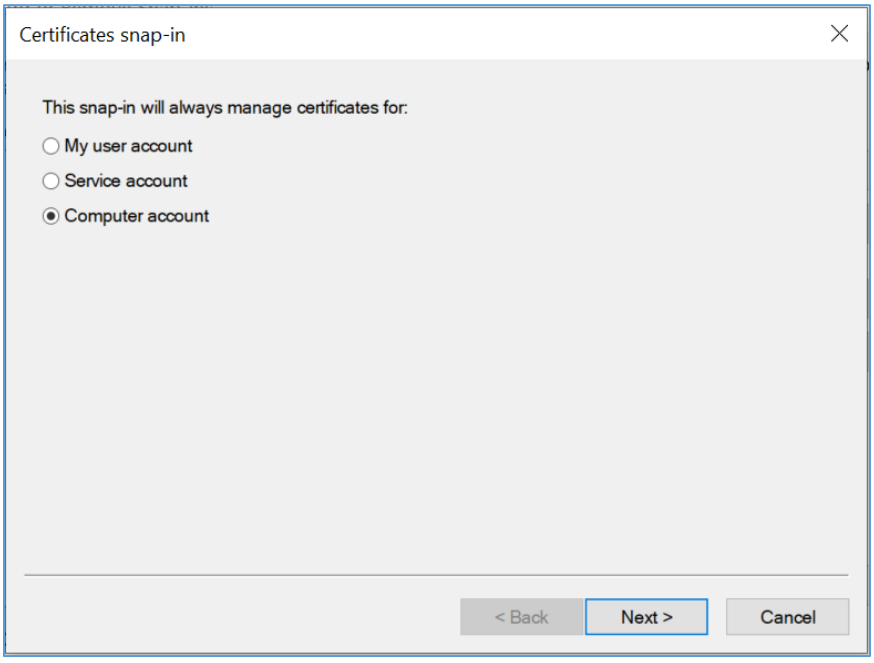


3. Select **Certificates** and click **Add**.
   - Choose **Computer Account**
   - Choose **Local Computer**
4. Click **Finish**, then click **OK**.



762

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

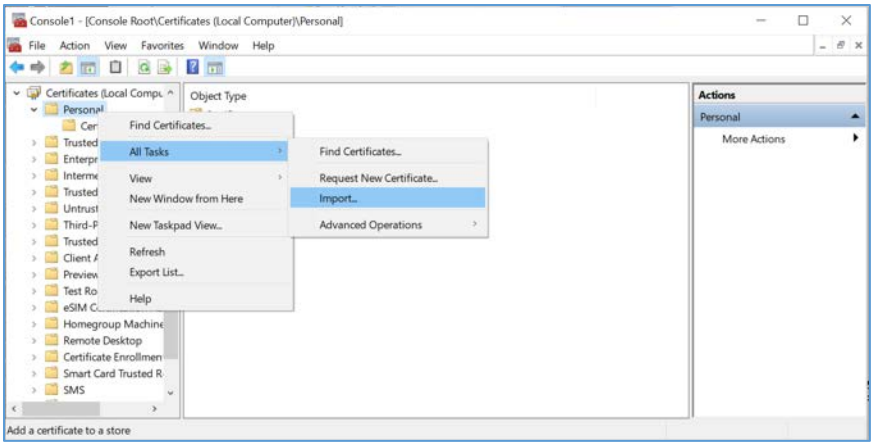


764

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**.

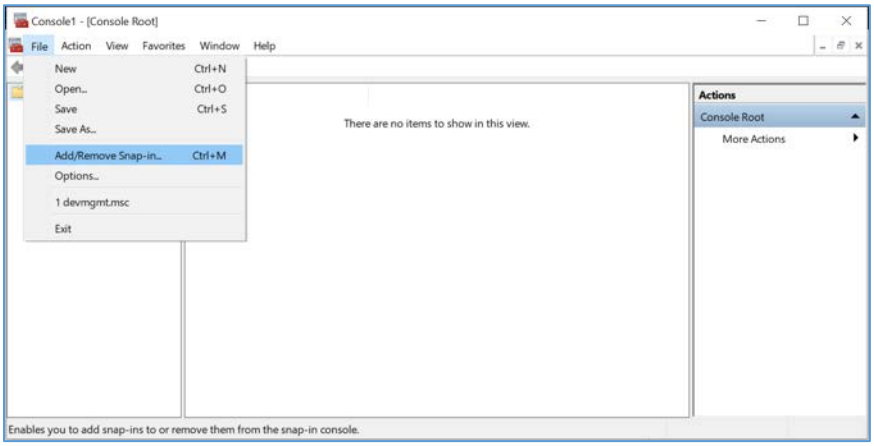
773 This procedure also installs the signing CA Root certificate (**DigiCert Test Root CA SHA2**) and its
774 Intermediate Root certificate (**DigiCert Test Intermediate Root CA SHA2**) into the server computer.

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:

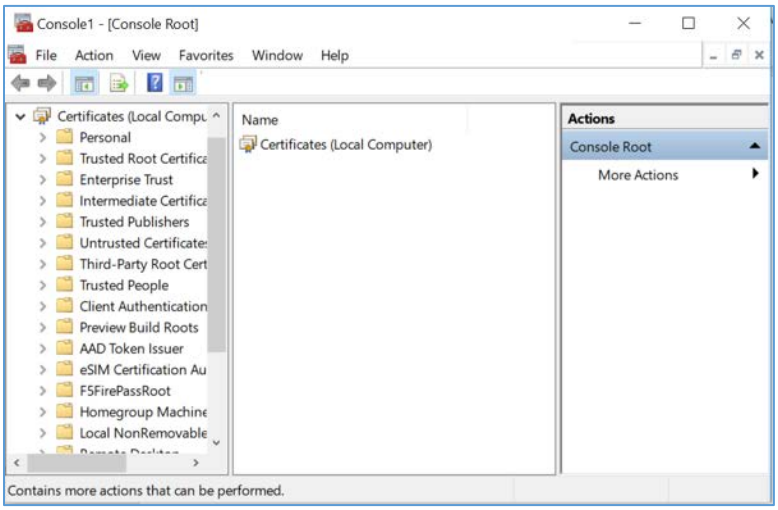
777 1. From the IntelliSpace server, click on **Start** > **Run** > **mmc**.

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

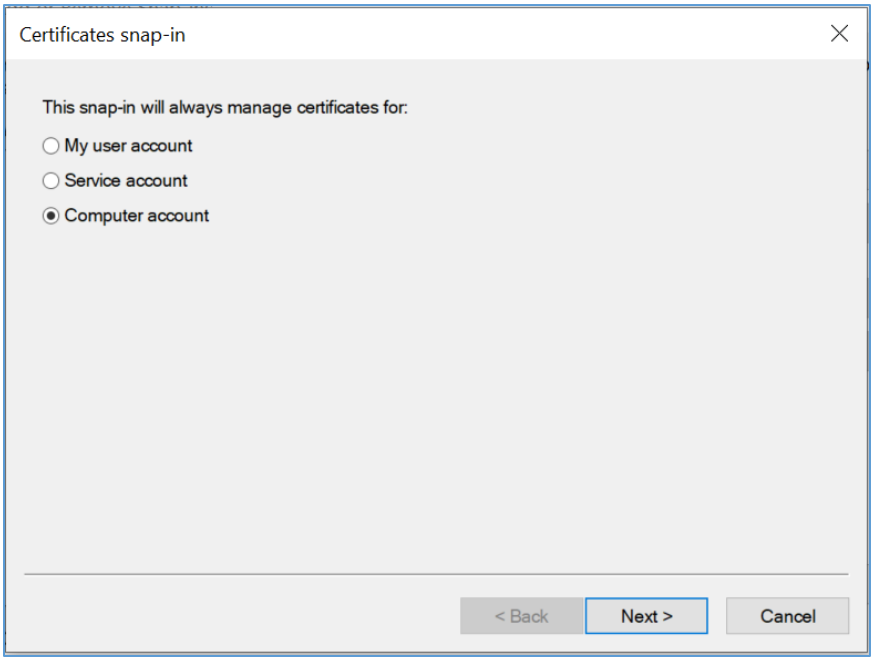


779

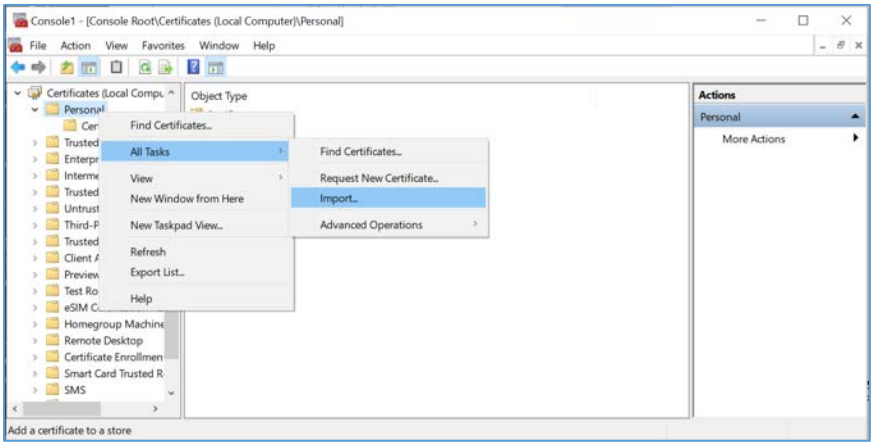
3. Select **Certificates** and click **Add**.
    a. Choose **Computer Account**.
    b. Choose **Local Computer**.
    c. Click **Finish**; click **OK**.



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



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



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

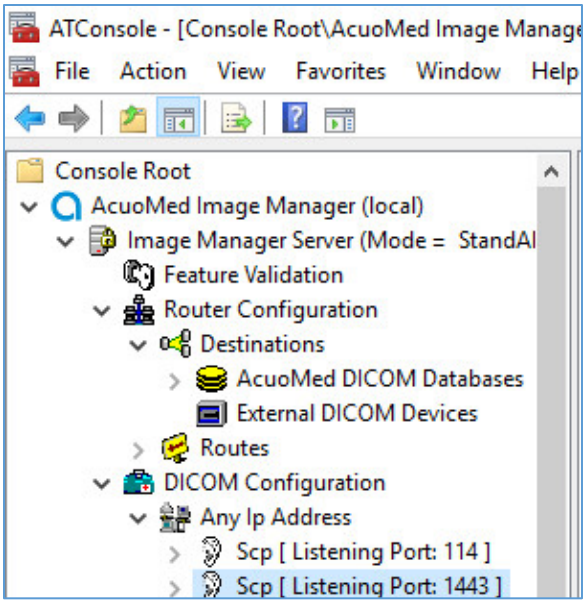
2.3.3 TLS Secure DICOM Configuration

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

2.3.3.1 TLS Configuration for Hyland Acuo VNA

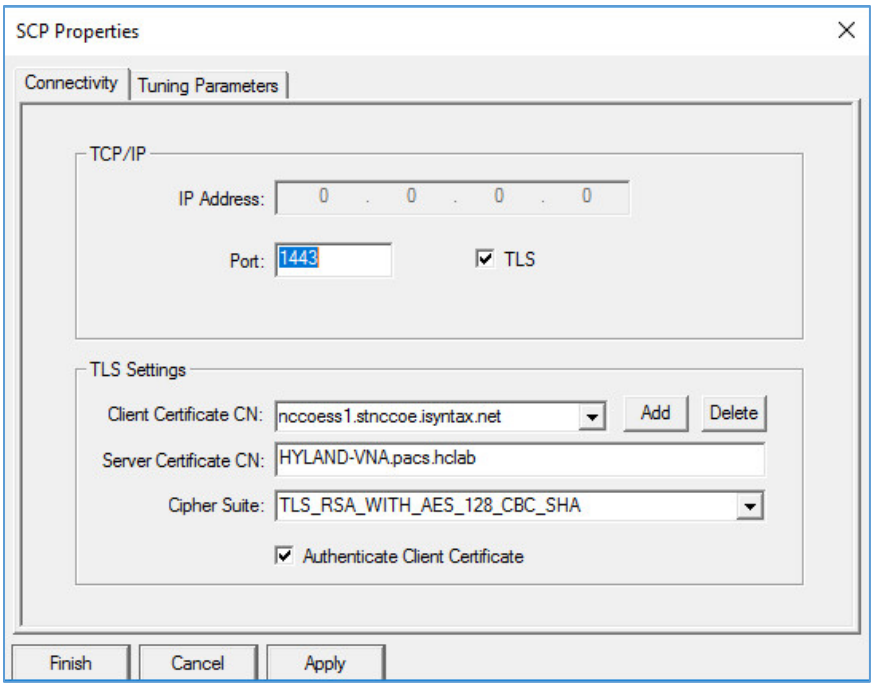
For receiving TLS DICOM message from IntelliSpace PACS, configure a new service-class provider (SCP) in Acuo VNA using Microsoft Windows Console. Configuration is done from the Acuo VNA server.

1. Open Microsoft **MMC** to access the **AcuoMed Image Manager (local):**
2. From the **Console > AcuoMed Image Manager (local) > DICOM Configuration**, right click **Any Ip Address > New Scp …** to create a new SCP for TLS encryption.

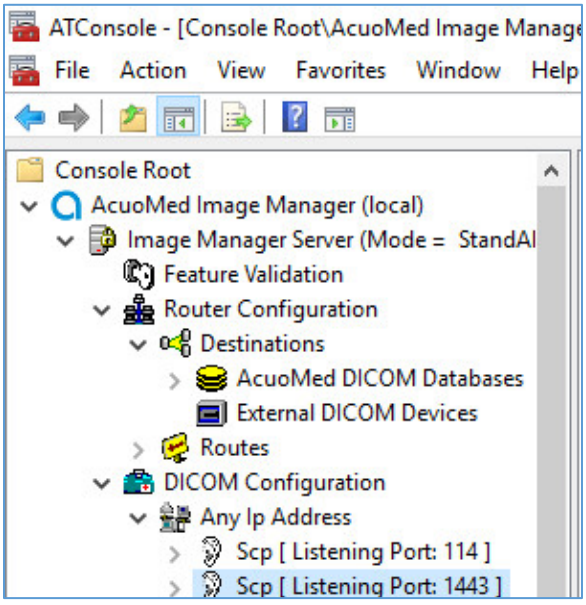


3. On the **Connectivity** tab of the **SCP** Properties page, provide the information below and click **Add**, **Apply,** and then **Finish**:

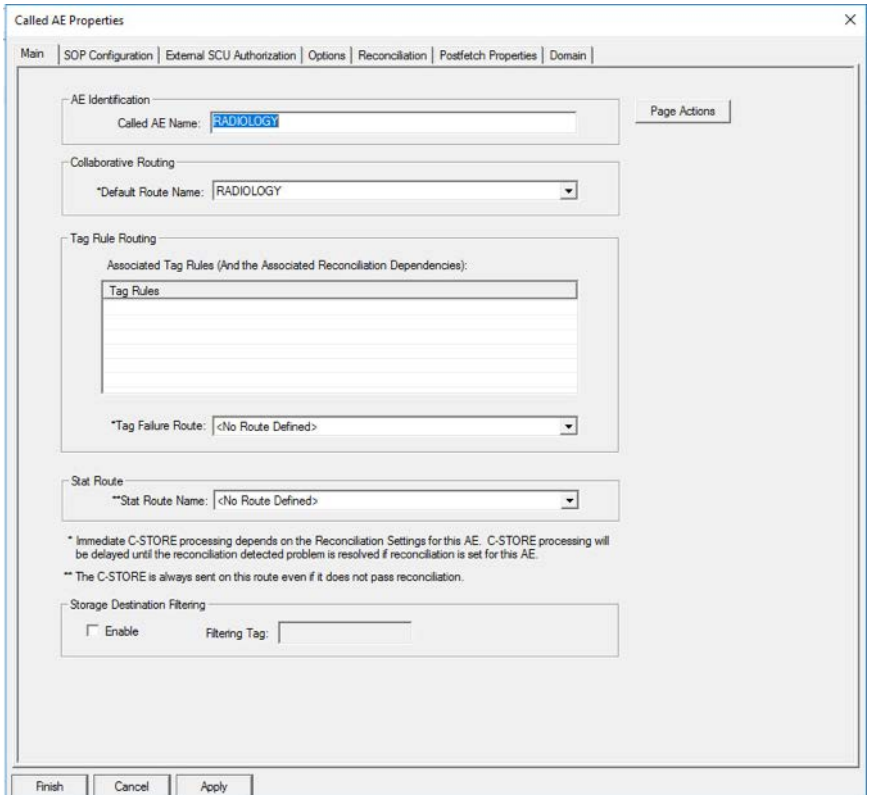
   - **Port**: 1443
   - Check the **TLS** checkbox
   - **Client Certificate CN**: nccoess1.stnccoe.issyntax.net
   - **Server Certificate CN**: HYLAND-VNA.pacs.hclab
   - **Cipher Suite**: TLS_RSA_WITH_AES_128_CBC_SHA
   - Check the **Authenticate Client Certificate** checkbox



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



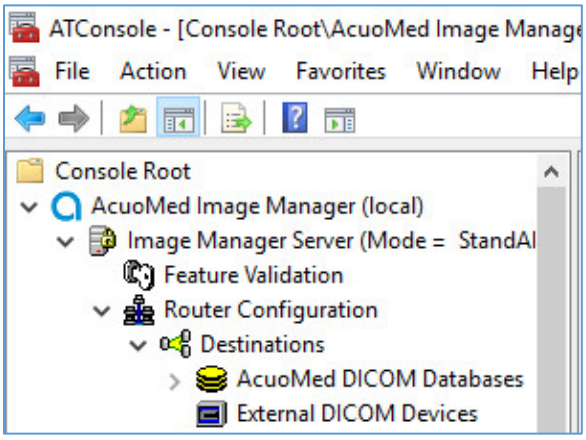
5. Fill in the **Called AE Name**: e.g., **RADIOLOGY** and **Default Route Name**: e.g., **RADIOLOGY**. After populating the information, click **Add.**



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

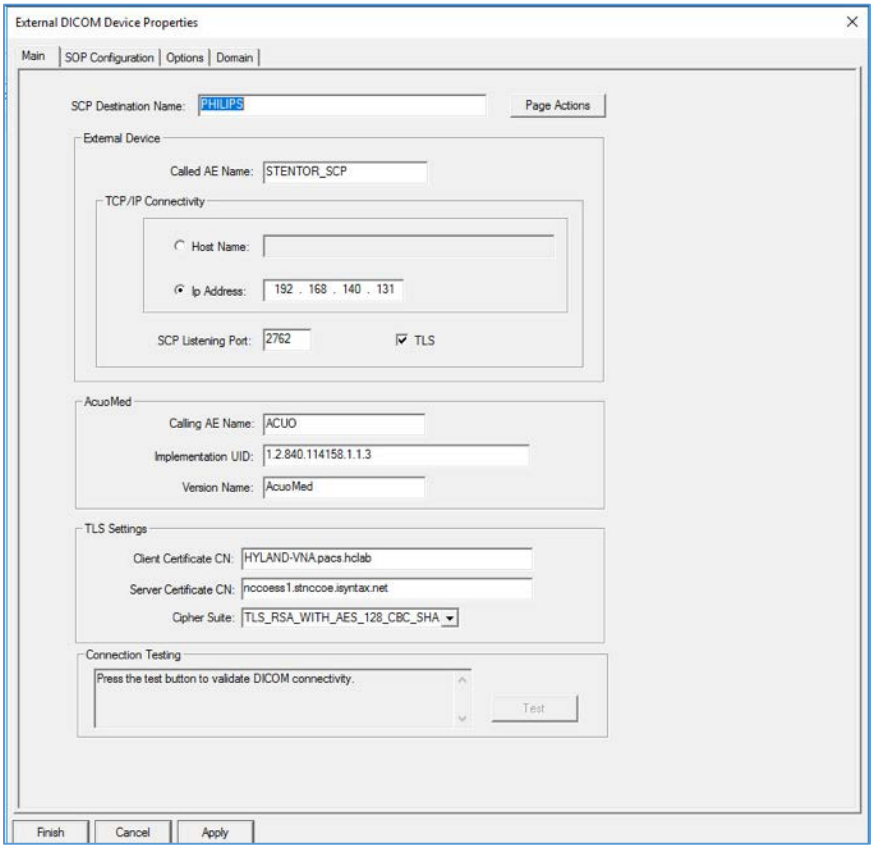
1. Open Microsoft **MMC** to access the **Image Manager Server:**

2. Navigate to **Image Manager Server** > **Router Configuration** > **External DICOM Devices**, right click on **External DICOM Devices** and click **New.**



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

   - **SCP Destination Name**: PHILIPS
   - **Called AE Name**: STENTOR_SCP
   - **IP Address**: 192.168.140.131
   - **SCP Listening Port**: 2762
   - Enable TLS by clicking the **TLS** checkbox next to the listening port number.
   - **Called AE Name**: ACUO
   - **Implementation UID**: 1.2.840.114158.1.1.3
   - **Client Certificate CN**: HYLAND-VNA.pacs.hclab
   - **Server Certificate CN**: nccoess1.stnccoe.isyntax.net
   - **Cipher Suite**: TLS_RSA_WITH_AES_128_CBC_SHA

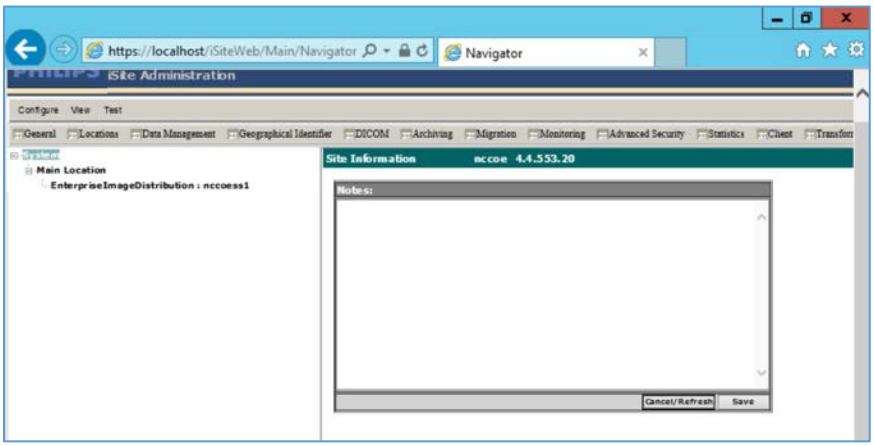


4. Restart the **AcuoMed** service.

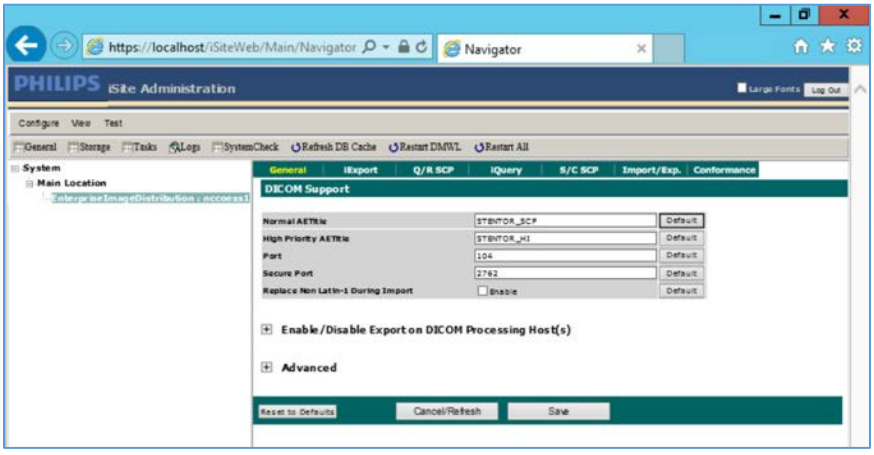
2.3.3.2 TLS Configuration for Philips IntelliSpace PACS

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

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



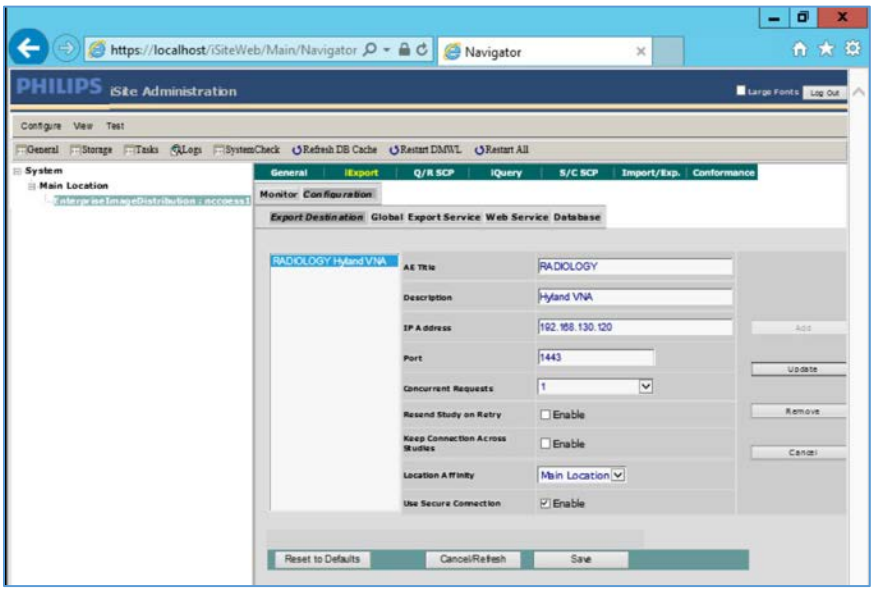
2. Click **Configuration** > **DICOM,** to navigate to DICOM configuration screen.



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

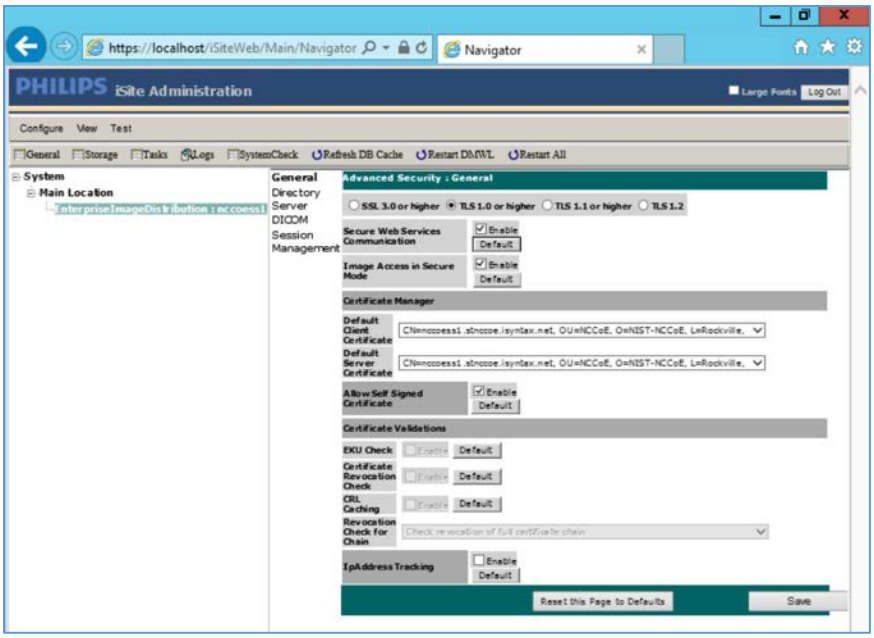
   - **AE Title**: RADIOLOGY
   - **Description**: Hyland VNA
   - **IP Address**: 192.168.130.120

- **Port**: 1443
- **Use Secure Connection**: checked



4. Click **Configuration** > **Advanced Security**, perform these selections:

- **TLS 1.0 or higher**: Selected
- Enable **Secure Web Services Communication**
- Enable **Image Access in Secure Mode**
- **Default Client Certificate**: CN= nccoess1.stnccoe.isyntax.net
- **Default Server Certificate**: CN=HYLAND-VNA.pacs.hclab
- Click **Save** to save the settings



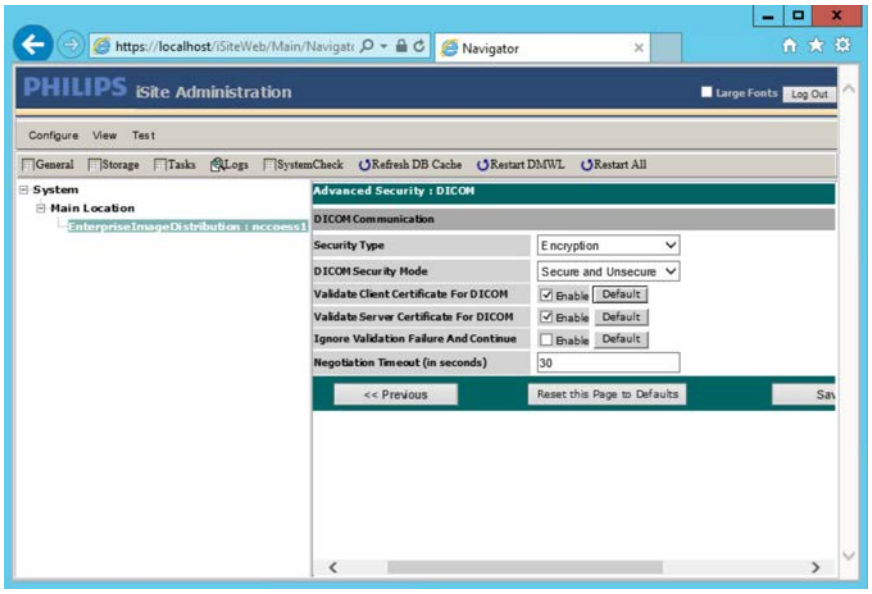
864

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

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

2.3.4 PACS and VNA TLS Integration Tests

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

DICOM communication is still functional.

DICOM communication is encrypted.

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

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

2.4 Modalities

2.4.1 DVTk Modality Emulator

DVTk Modality is a modality emulator that can be used to emulate all the DICOM functions of a modality system. It can simulate a real modality to test and verify communication with all the DICOM services. It uses DICOM files as input for Queries, modality performed procedure step (MPPS), and Storage actions. Consequently, this project chose to use the DVTk Modality as an emulator to test the connectivity, communication, workflow, and interaction between PACS and modality in the lab.

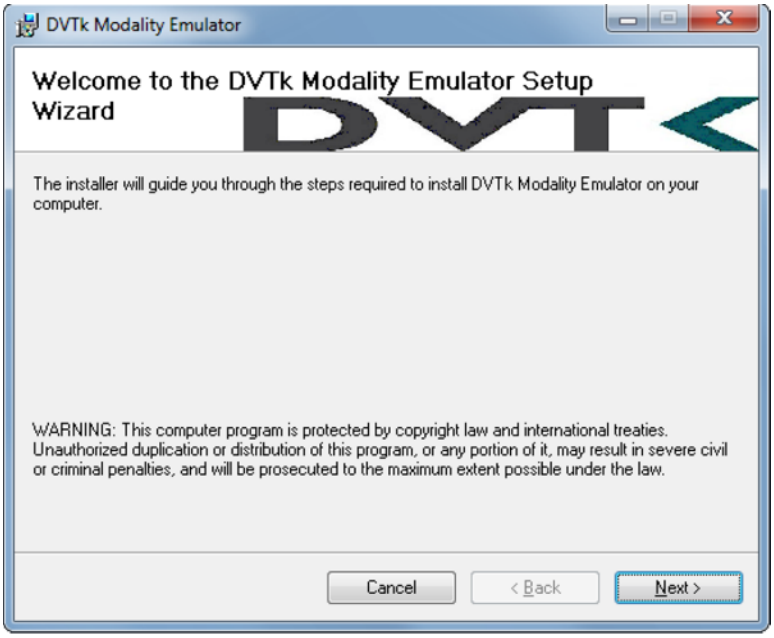
System Requirements

Operating System: Microsoft Window 7 (with Microsoft .NET 4.0 Framework)

Network Adapter: VLAN 1402

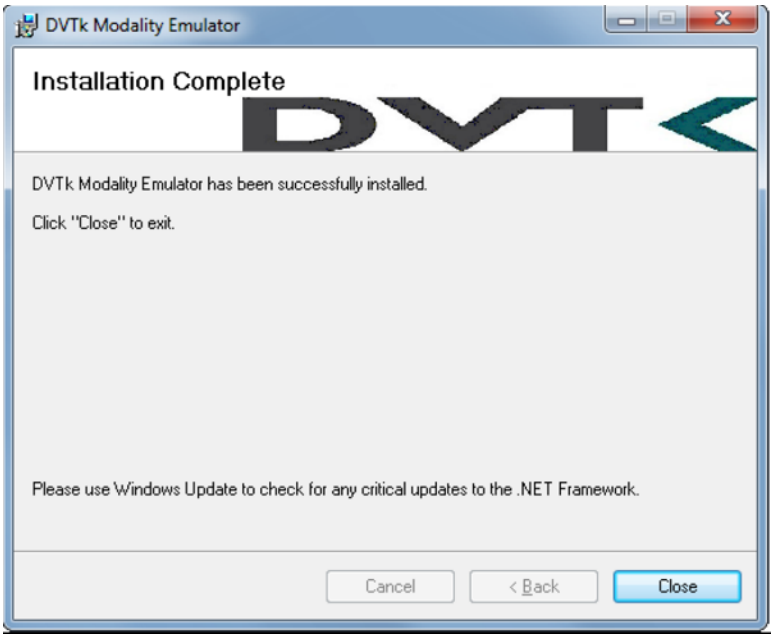
DVTk Modality Installation

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



896

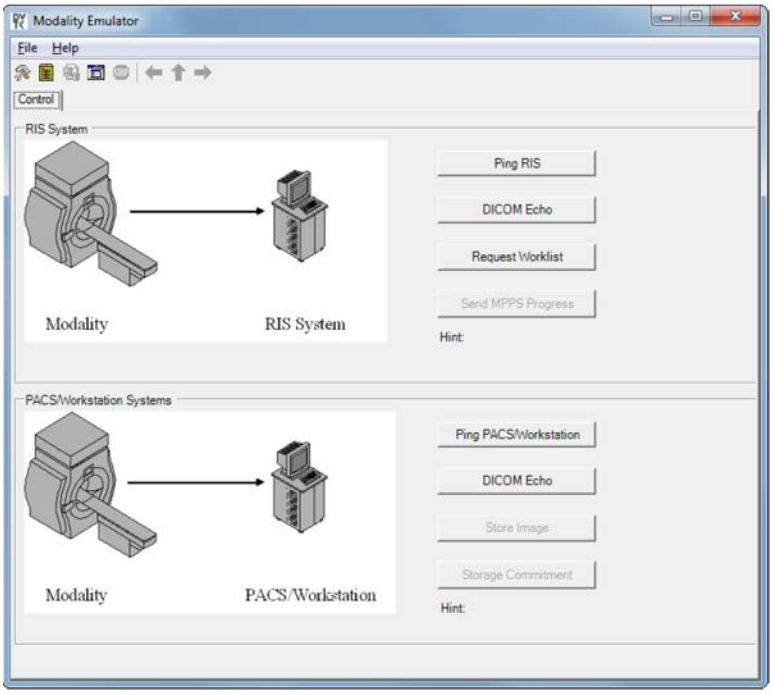
897 3. Follow the wizard instruction to continue the installation until it reaches successful completion.



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.



DVTk Modality Configuration

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

RIS System

- **IP Address**: 192.168.160.201
- **Remote Port**: 105
- **AE Title**: RIS

MPPS Manager

- **IP Address**: localhost
- **Remote Port**: 105
- **AE Title**: RIS

PACS/Workstation Systems–Storage Config

- **IP Address**: localhost

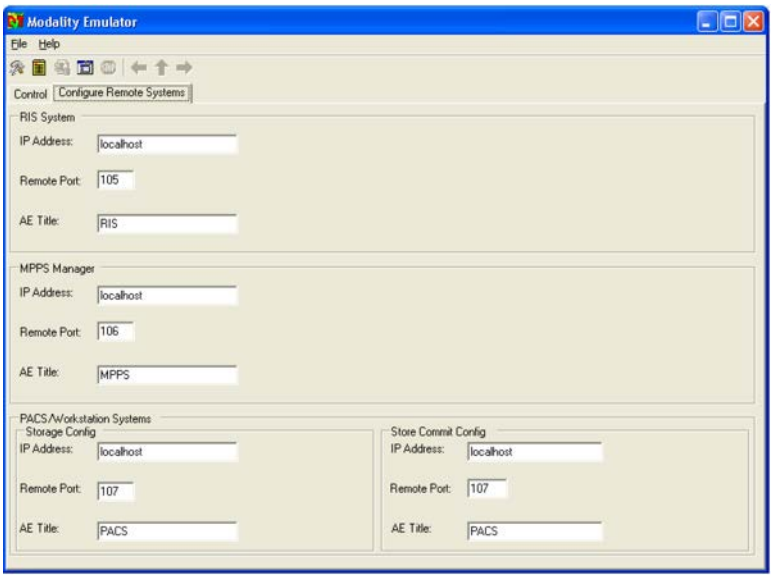
- **Remote Port**: 106
- **AE Title**: MPPS

PACS/Workstation Systems–Storage Commit Config

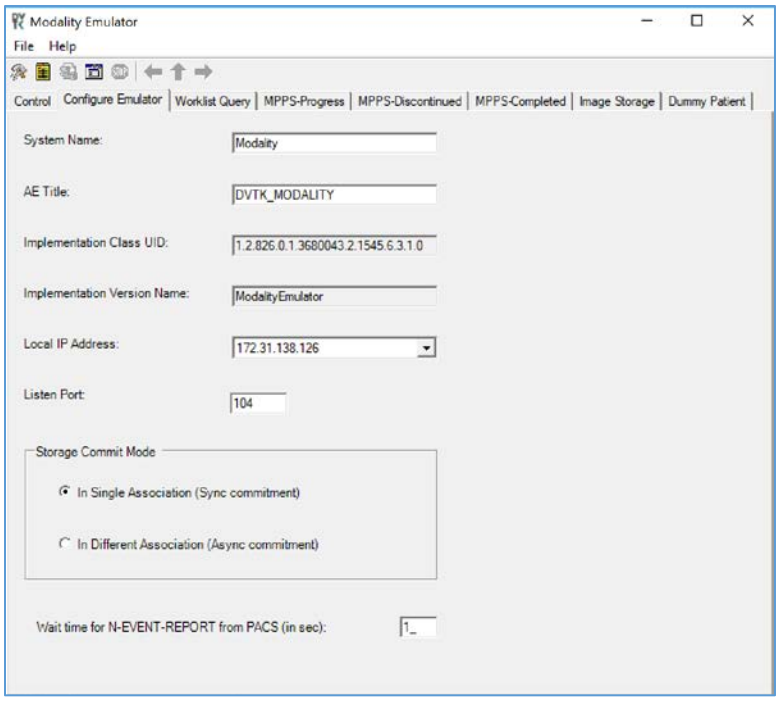
- **IP Address**: localhost
- **Remote Port**: 107
- **AE Title**: PACS

Store Commit Config

- **IP Address**: localhost
- **Remote Port**: 107
- **AE Title**: PACS

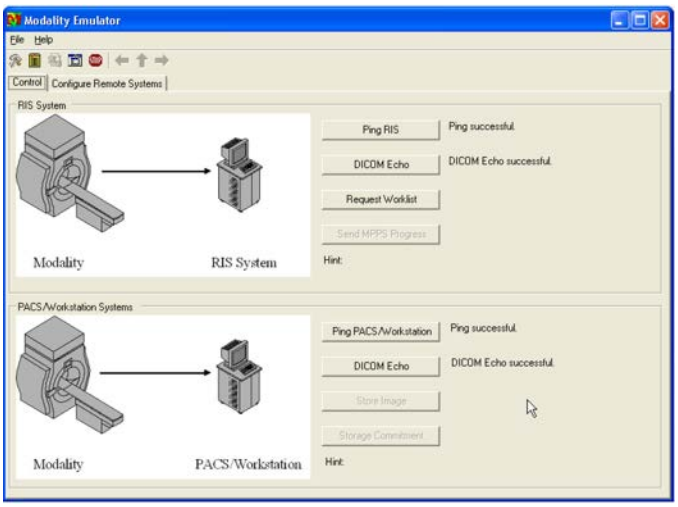


The configuration of the modality itself is also needed to indicate its **AE Title** (e.g., **DVTK_MODALITY**), **Local IP Address** (e.g., **172.31.138.126**), and **Listen Port** (e.g., **104**) to be paired for association negation with other remote systems. The screenshot that follows indicates the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



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

2.4.2 DVTk RIS Emulator

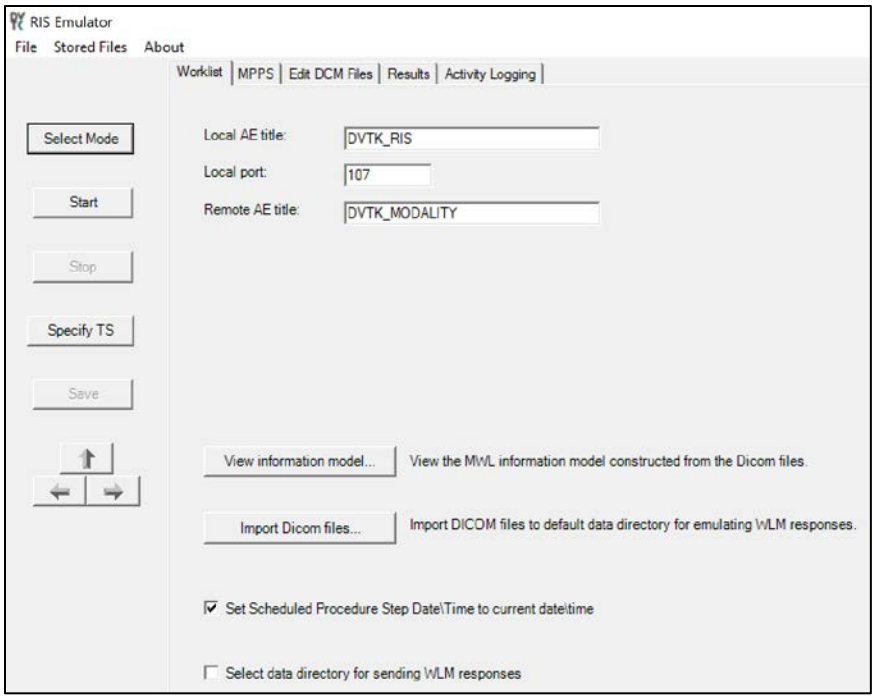
DVTk, the Health Validation Toolkit, is an open-source software. The DVTk RIS Emulator is an application that handles Modality Worklist and Modality Performance Procedure Step requests from remote applications and then responds with the emulated results using the DICOM files specified by the users.

System Requirements

Operating System: Microsoft Windows 7 (Microsoft .NET framework 2.0)

DVTk RIS Emulator Installation

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



DVTk RIS Emulator Configuration

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

2.5 Asset & Risk Management

2.5.1 Virta Labs BlueFlow

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

System Requirements

CPU: 2

Memory: 8 GB RAM

Storage: 100 GB (Thin Provision)

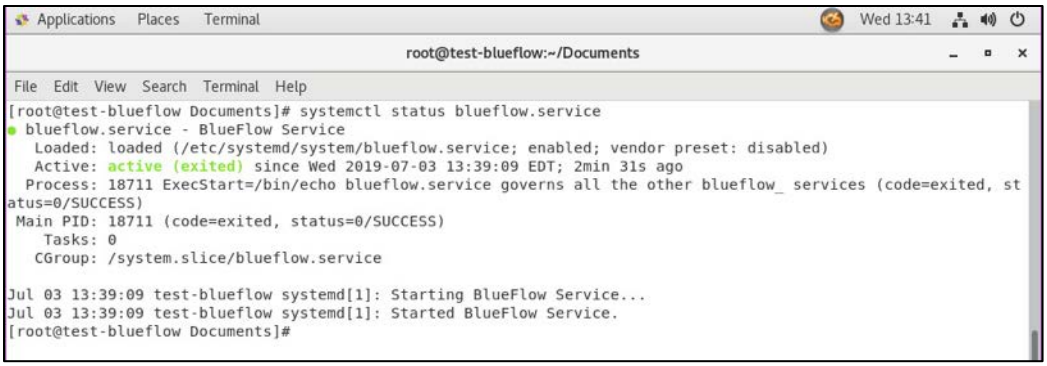
Operating System: CENTOS 7

Network Adapter: VLAN 1201

Virta Labs BlueFlow Installation

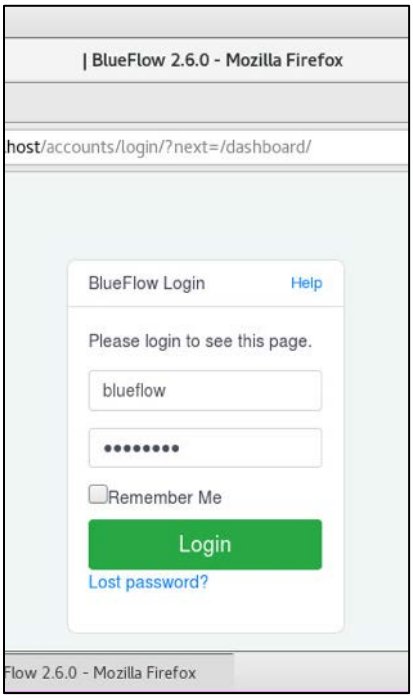
1. Run `rpm -ihv blueflow-2.6.0-1.x86_64.rpm` in the CentOS 7 terminal.
    a. Wait for the package install process to complete.
    b. Depending on your environment, you may need to install some dependencies before the BlueFlow package can be successfully installed.

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



993

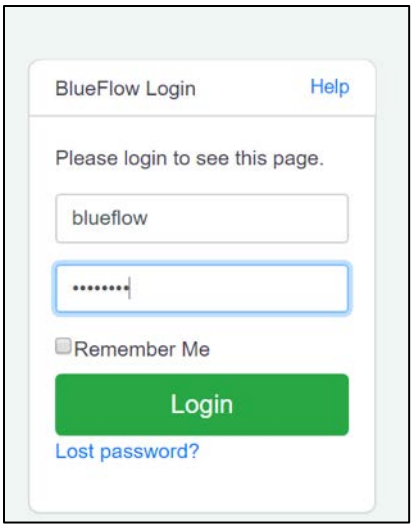
994 4. Visit ***https://localhost*** to verify BlueFlow web service is operating as expected, with a **BlueFlow**
995 **Login page.**



996

997 **Virta Labs BlueFlow Network Groups Configuration**

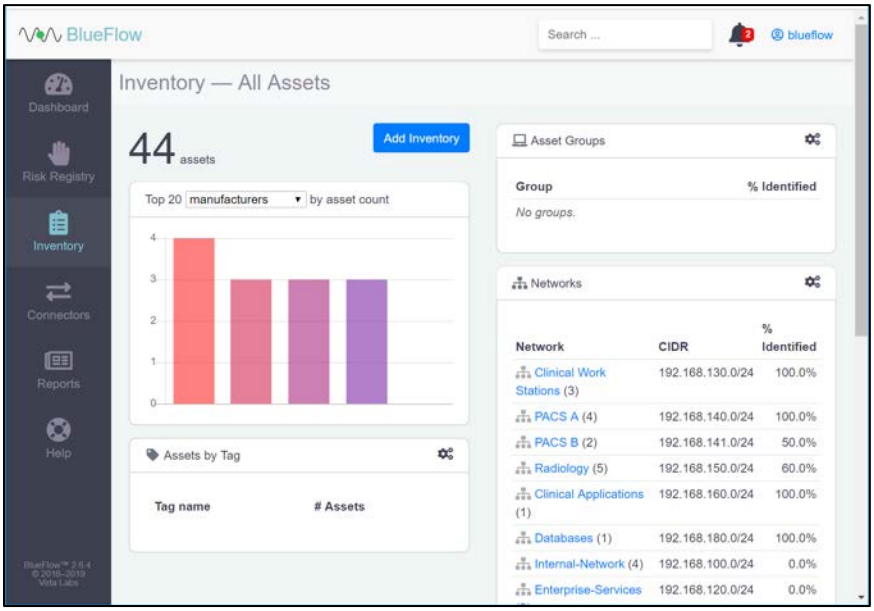
998 1. Log in to the **BlueFlow** web console.



999

1000 2. Navigate to the **Inventory** tab.

1001 3. Under the **Networks** section, click on the **gear** icon.

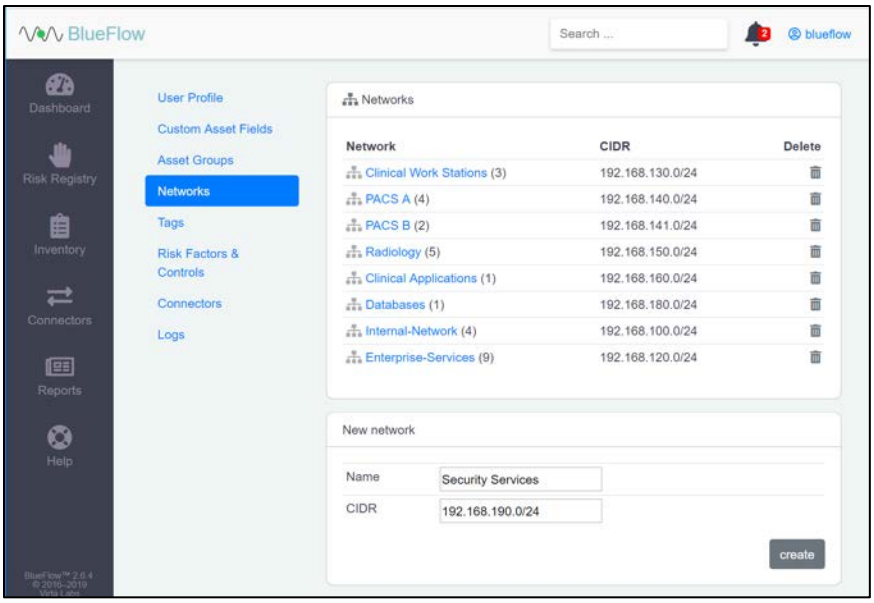


1002

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.**

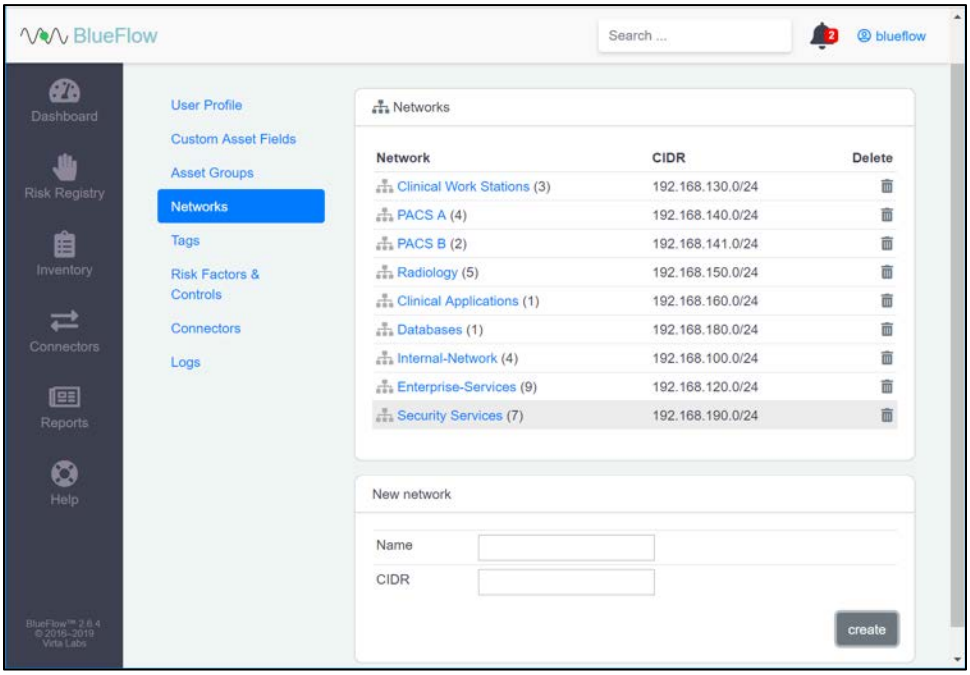
1005 6. Click **create.**



1006

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

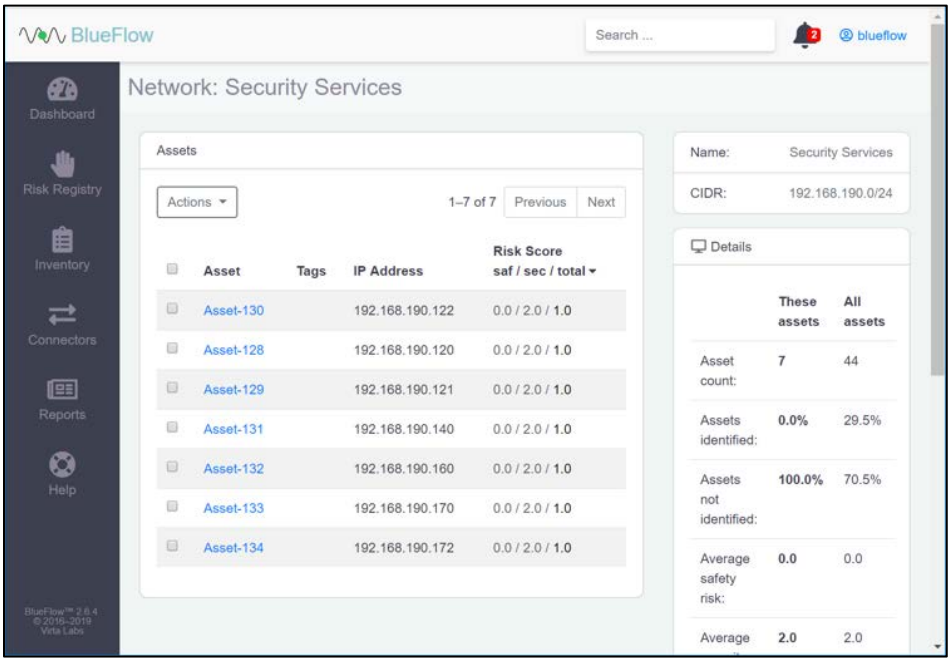
1008 8. Click on the **name** of the new network group.



1009

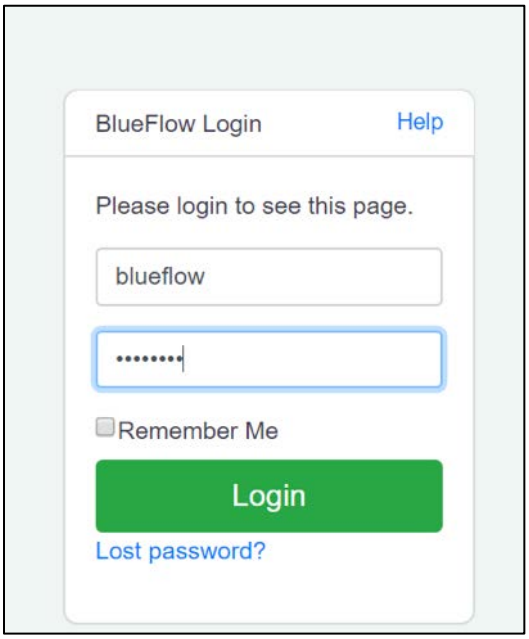
1010 9. **Assets** will be listed on this page if they match the network group's criteria.

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

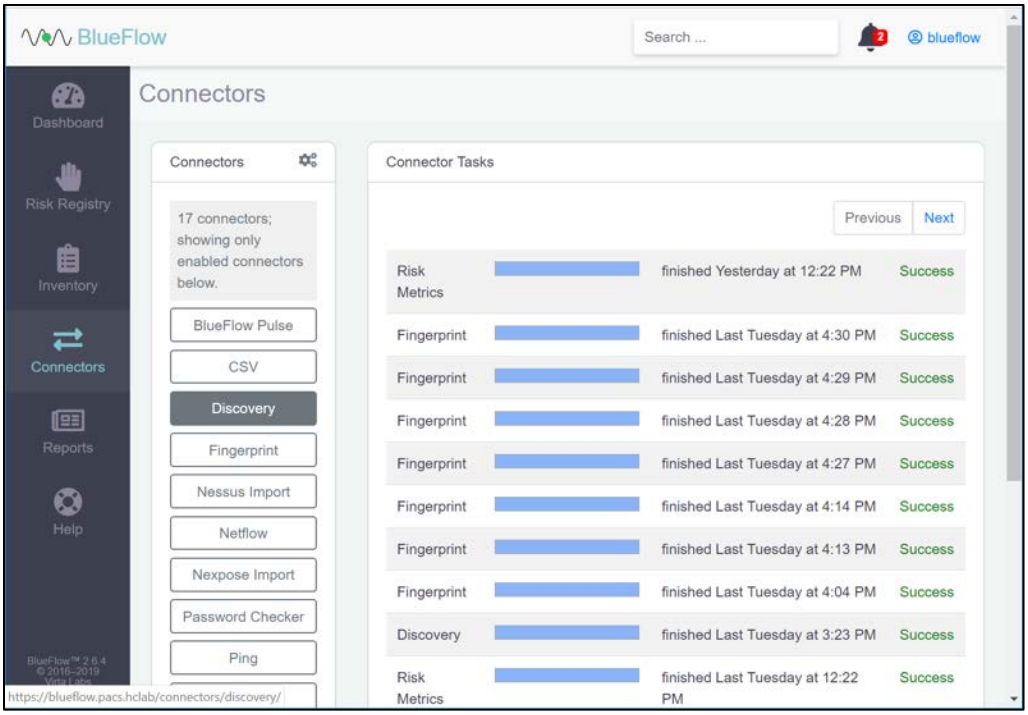


Running an IP Discovery Scan in Virta Labs BlueFlow

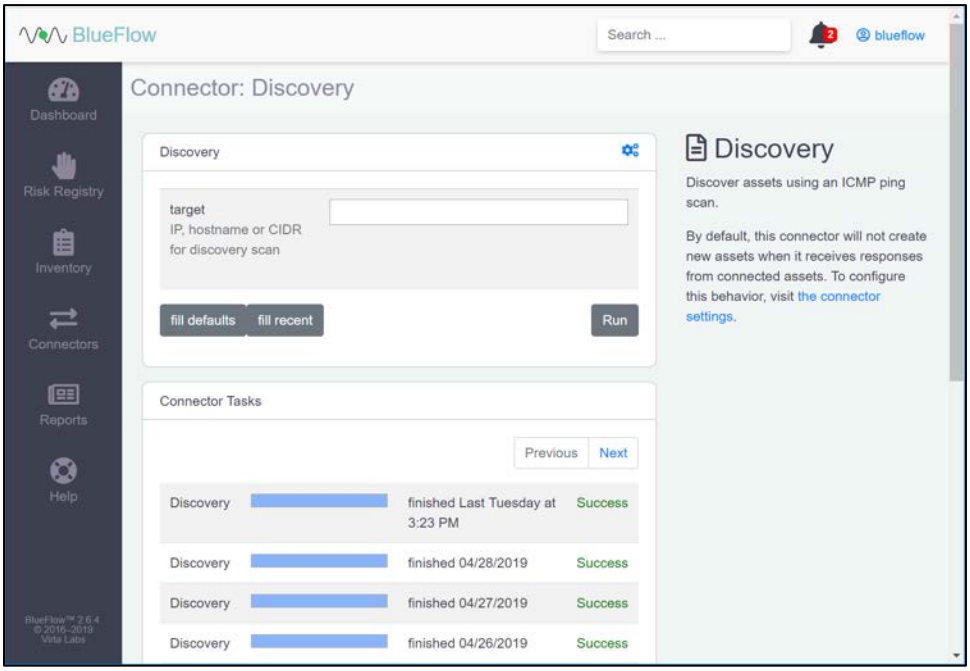
1. Log in to the **BlueFlow** web console.



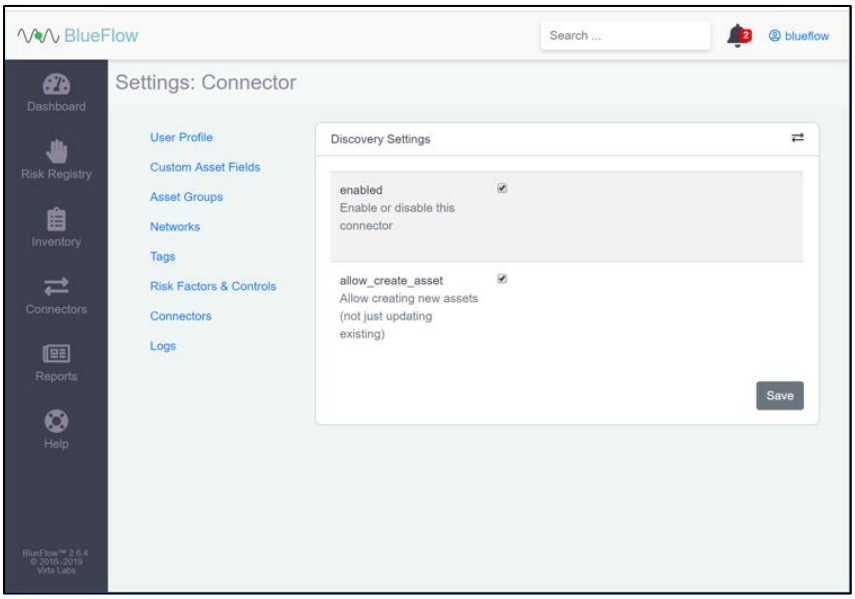
2. Navigate to **Connectors > Discovery**.



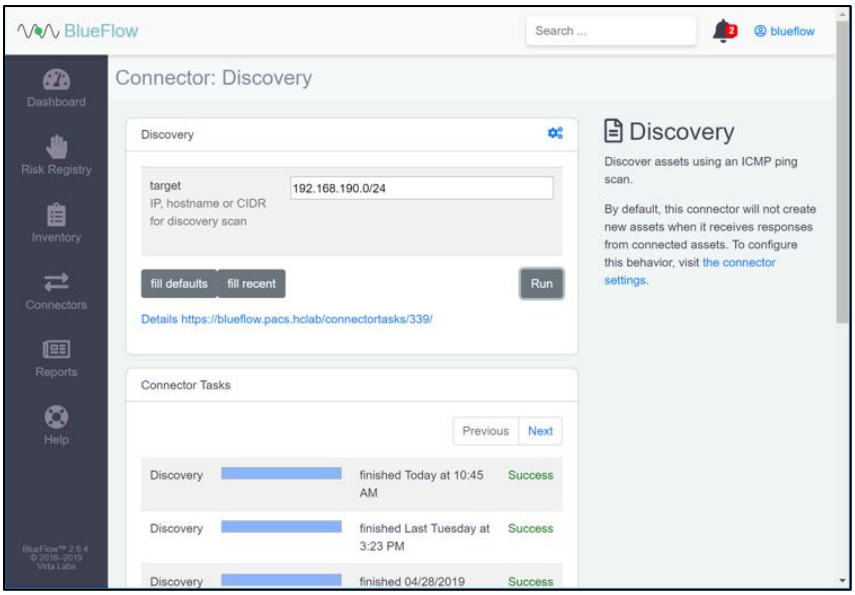
3. Under **Discovery**, click the **gear** icon.



4. Check the box next to **allow_create_asset.**
5. Click **Save**.

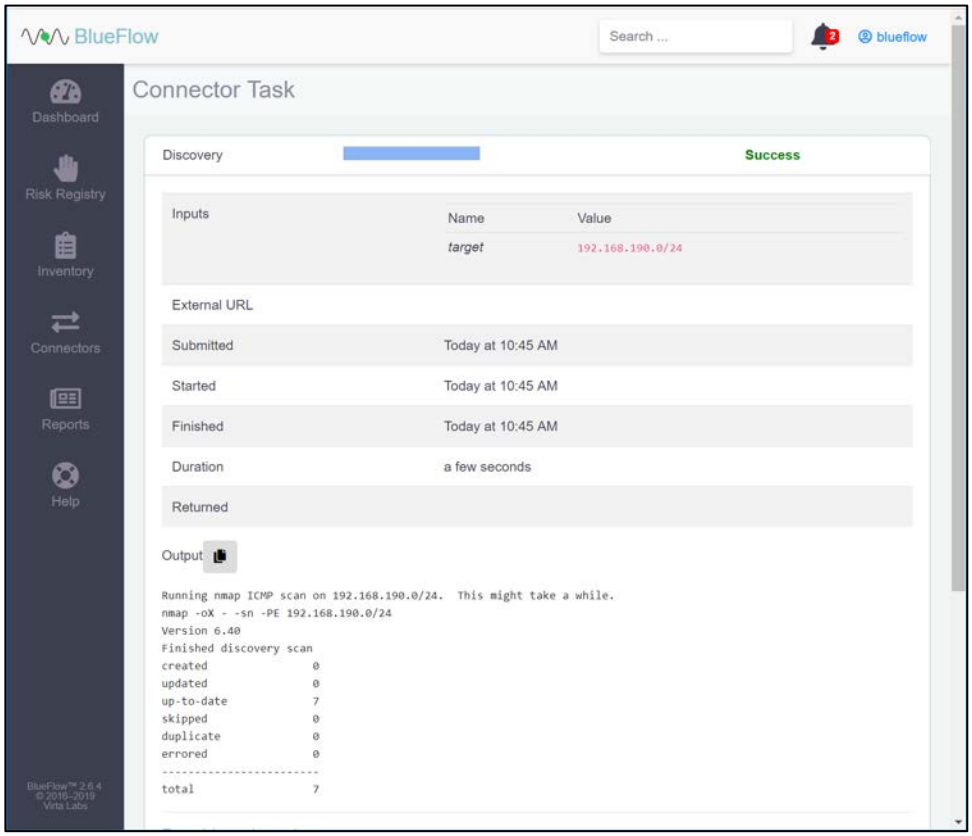


6. Enter an **IP** (e.g., ***192.168.190.0/24***), **host name** or **CIDR** that you would like to scan.
7. Click **Run.**
8. Wait for the discovery scan to finish.



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

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



2.5.2 Tripwire Enterprise

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

System Requirements

CPU: 1

Memory: 4 GB RAM

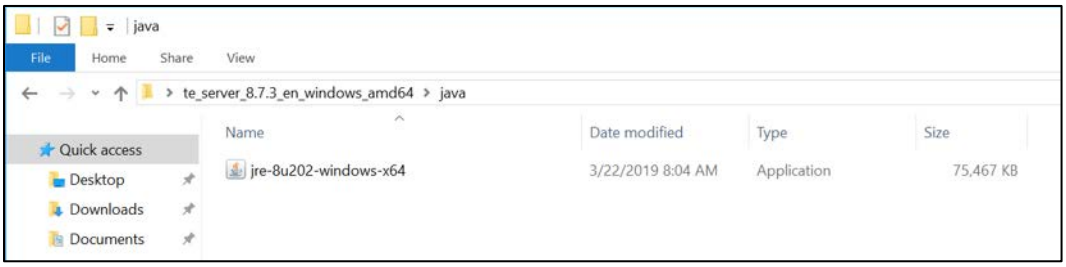
Storage: 120 GB (Thin Provision)

Operating System: Microsoft Windows Server 2016

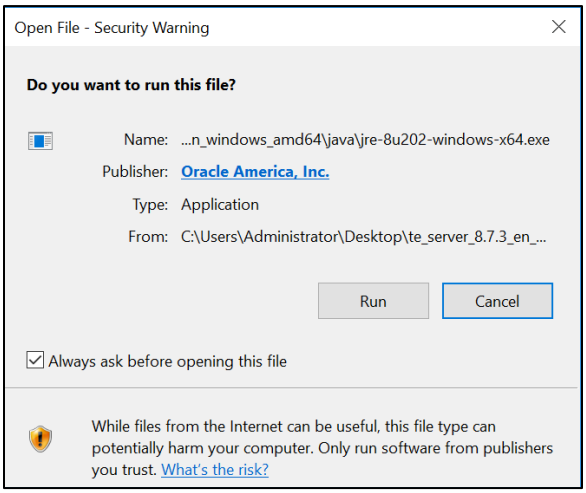
Network Adapter: VLAN 1201

Tripwire Enterprise Console Installation

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

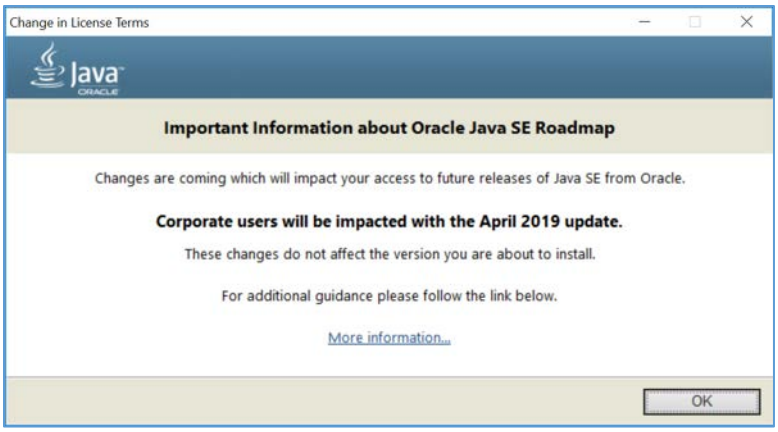


2. Click on **Run**.



3. Click **on Install >**.

4. Click **OK**.

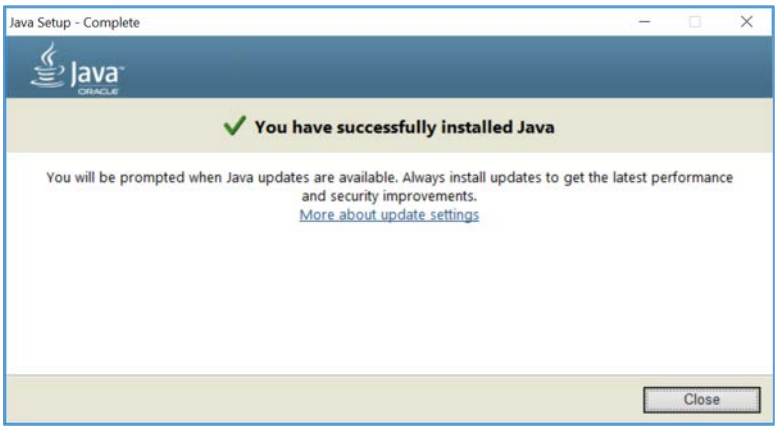


1050

1051 5. Wait for the install process to complete.

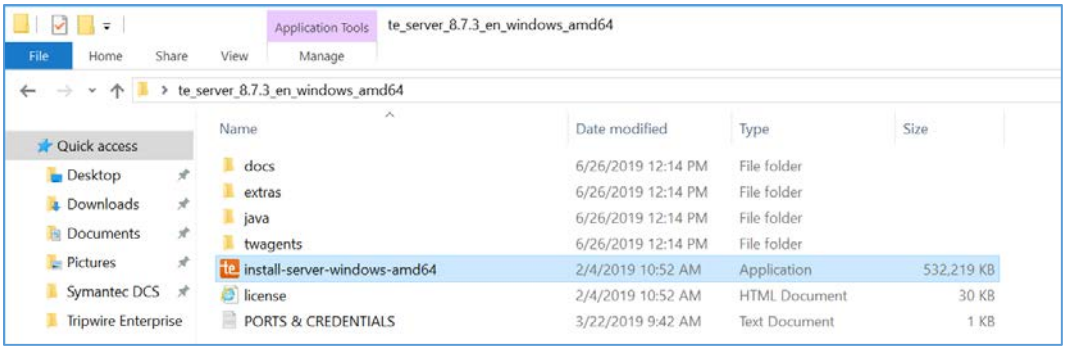
1052

1053 6. Click **Close**.



1054

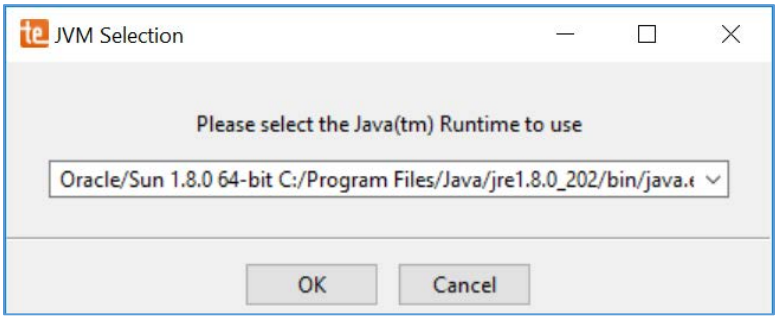
1055 7. With Java installed, double-click on the Tripwire install application, *install-server-windows-amd64.*



1056

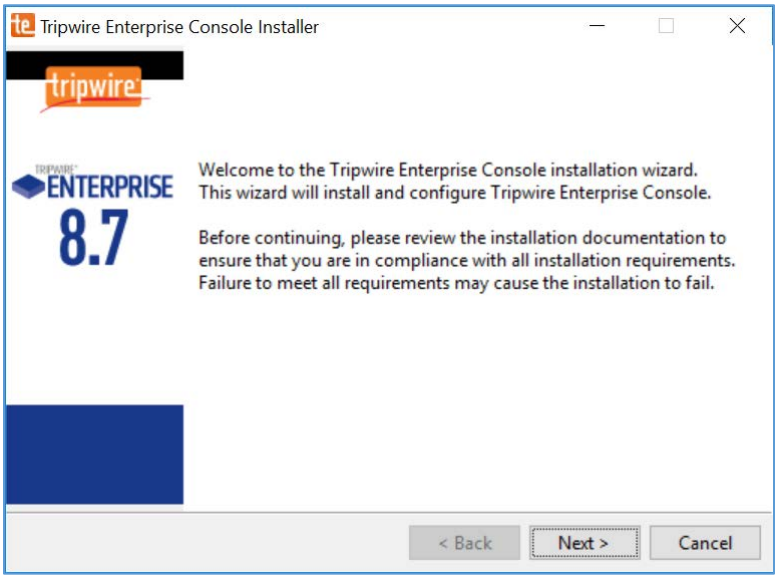
1057 8. Select the version of *Java, Oracle/Sun 1.8.0 64-bit*, that was previously installed.

1058 9. Click **OK**.



1059

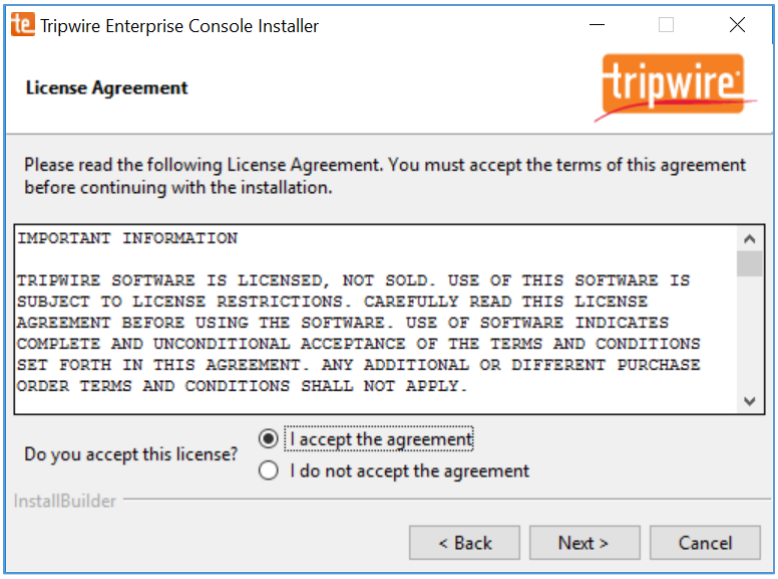
1060 10. Click **Next >**.



1061

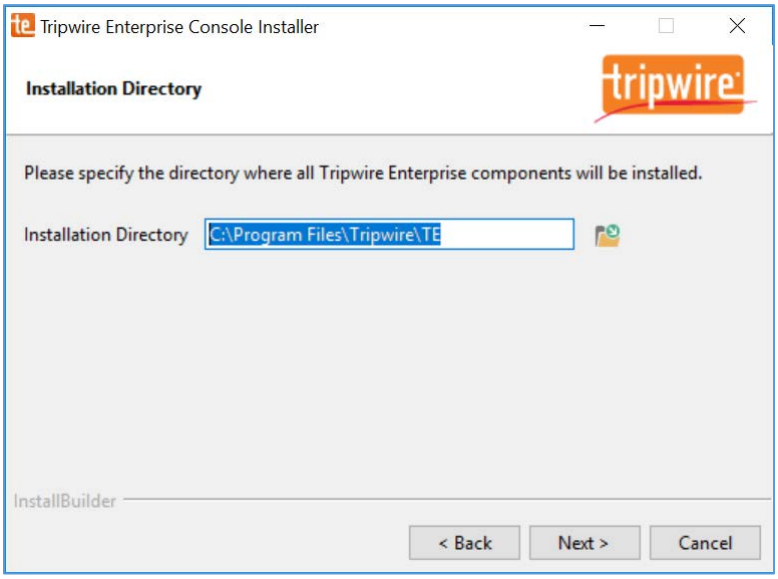
1062 11. Check **I accept the agreement**.

12. Click **Next >**.



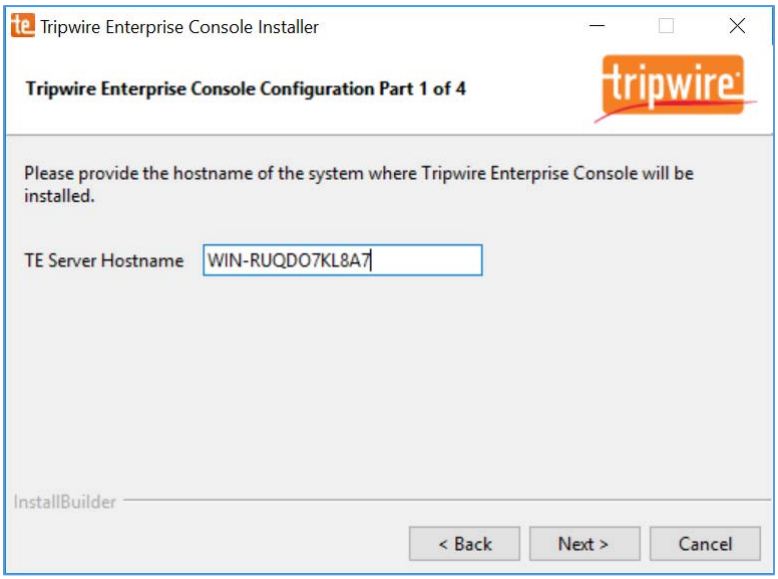
13. Specify an installation directory, *C:\Program Files\Tripwire\TE*, for the Tripwire installation.

14. Click **Next >**.



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

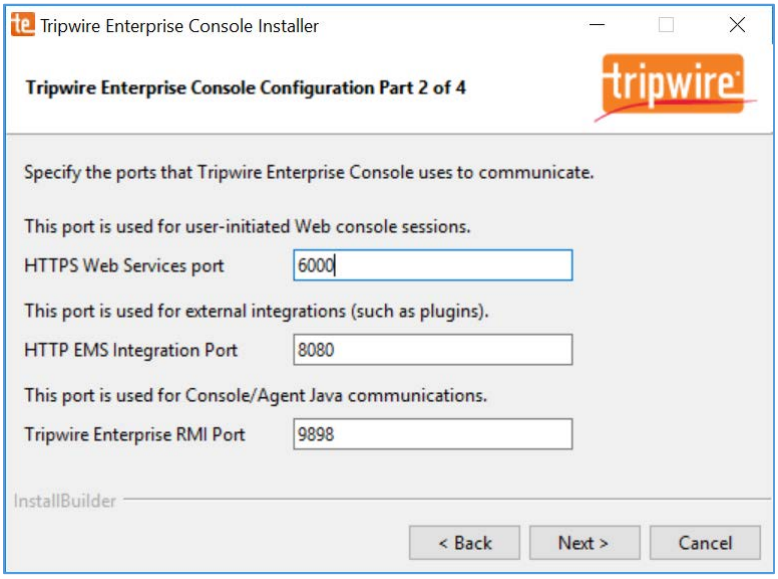
16. Click **Next >.**



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**.

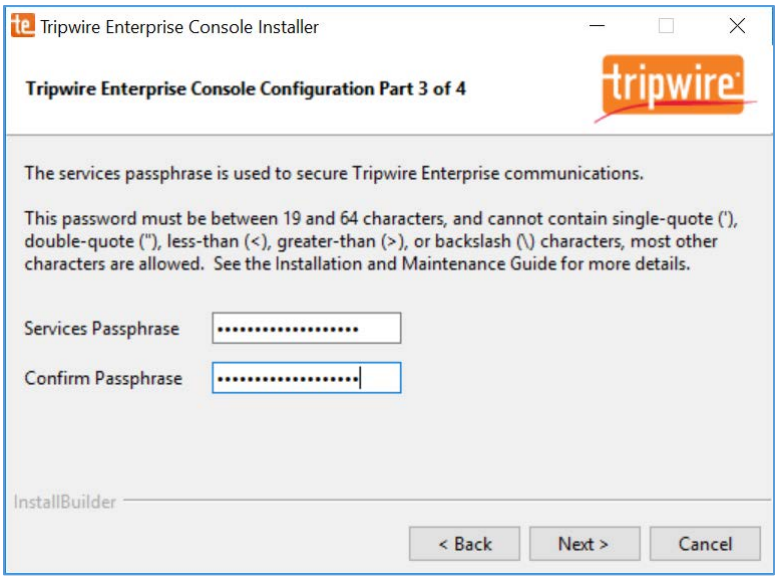
1074 18. Click **Next >**.



1075

1076 19. Create a password for Tripwire Enterprise services.

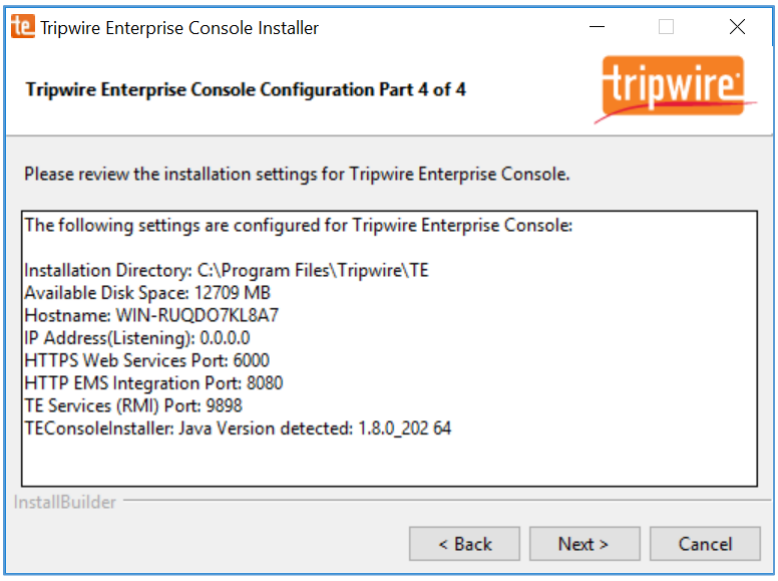
1077 20. Click **Next >.**



1078

1079 21. Verify planned installation settings are correct.

1080 22. Click **Next >**.

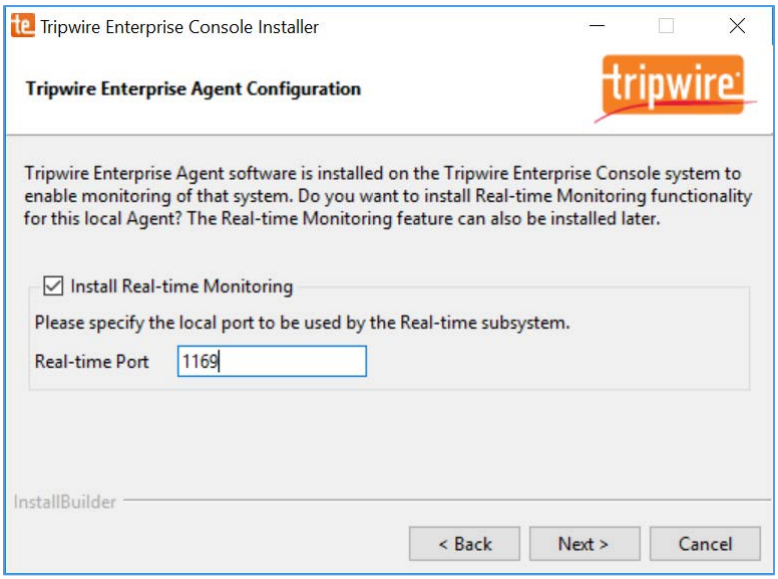


1081

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

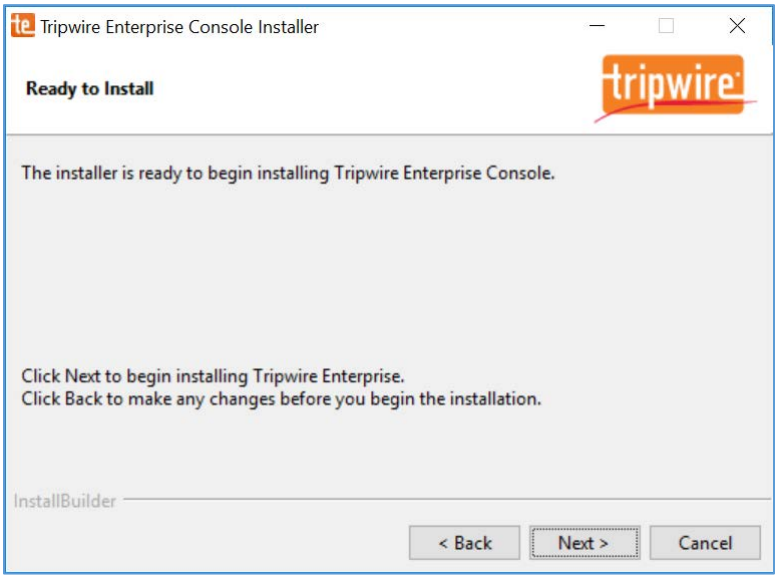
1083 24. Specify **Real-time Port** as **1169** for monitoring.

1084 25. Click **Next >.**



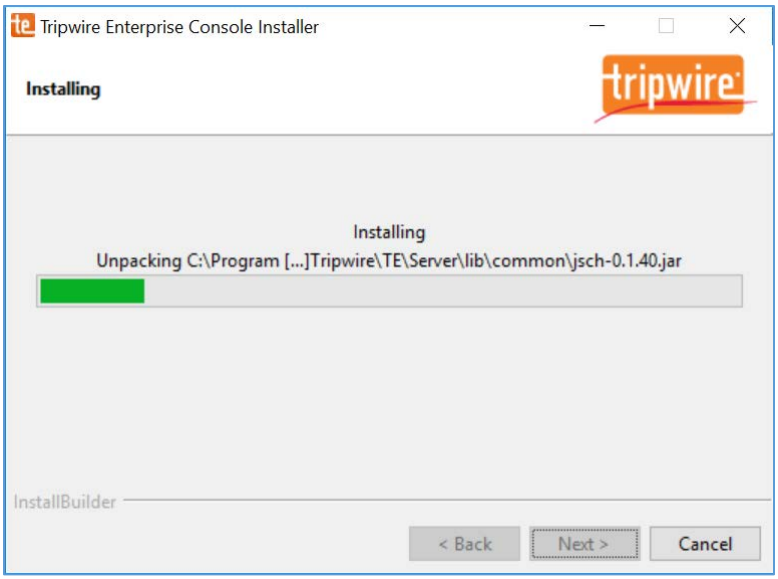
1085

1086 26. Click **Next >**.

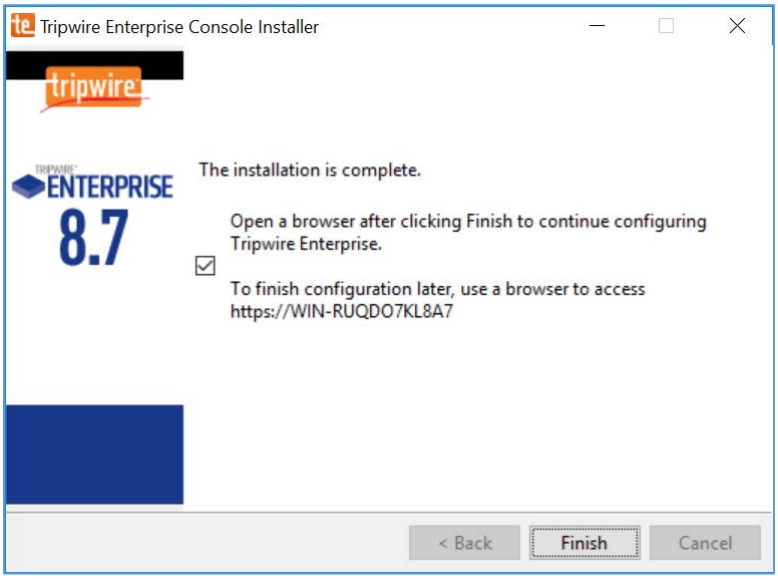


1087

1088 27. Wait for Tripwire Enterprise installation to complete.

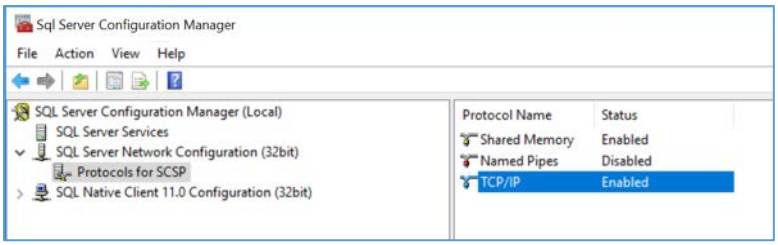


28. Click **Finish**.

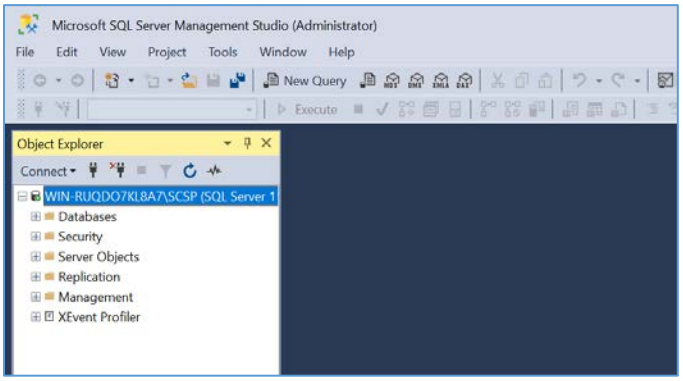


29. Open SQL Server Configuration Manger.

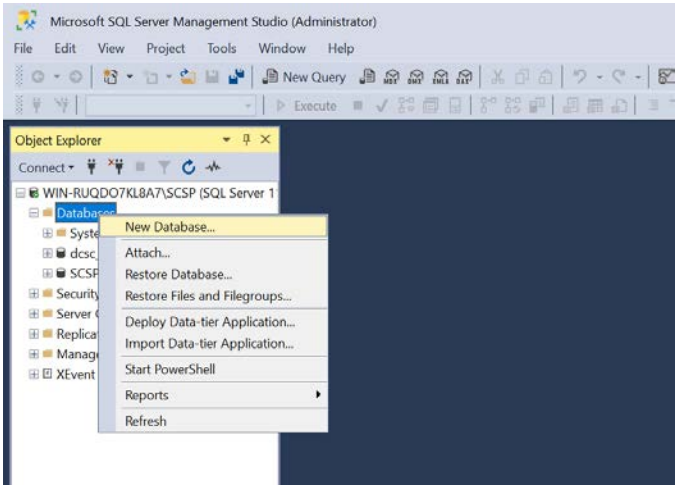
30. Under **SQL Server Network Configuration > Protocols for SQL Server** ensure the **TCP/IP protocol** is set to **Enabled.**



31. Open SQL Server Management Studio.



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

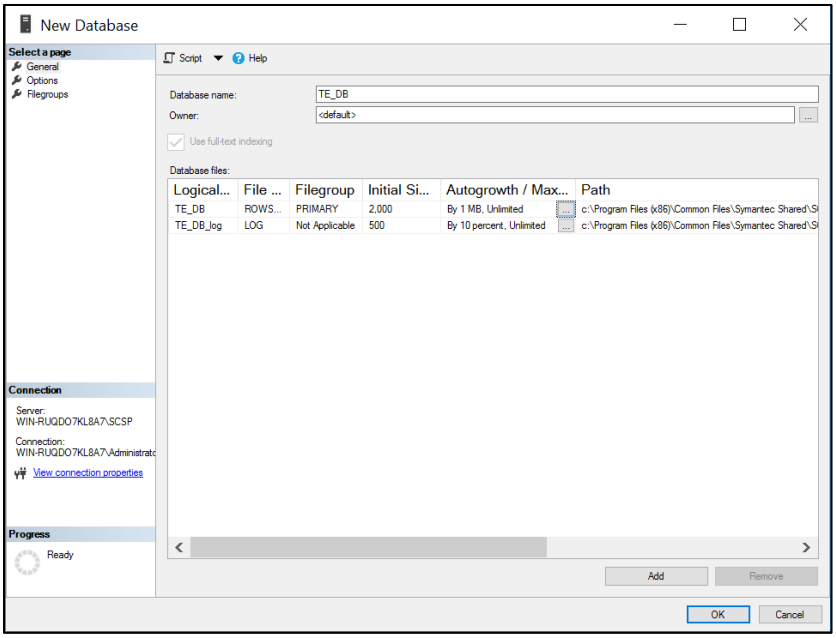


33. On the left, **under Select a page**, select **General**.

34. Enter a **Database name** as **TE_DB**.

35. Under **Database files**, for the data file, set **Initial Size** to at least **2,000**.

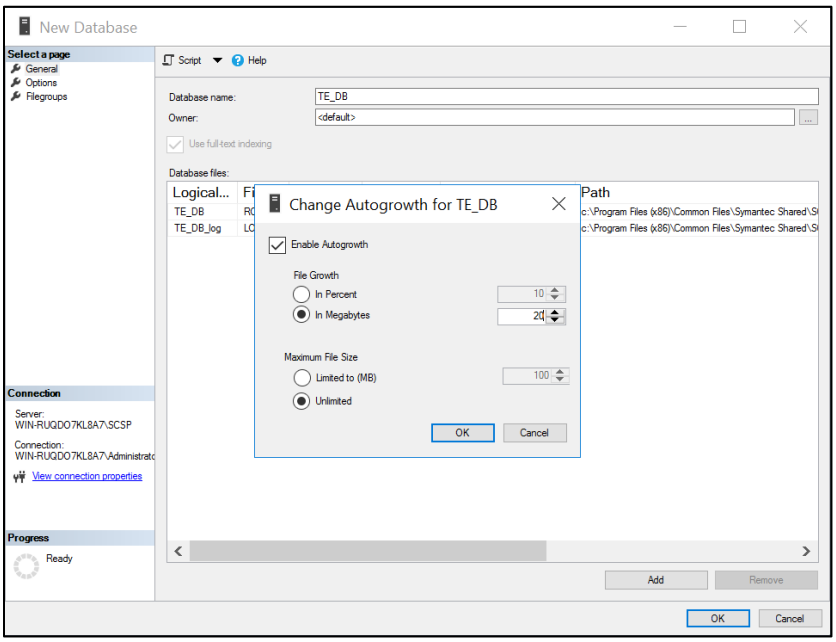
1104 36. Click the **button** under **Autogrowth**.



1105

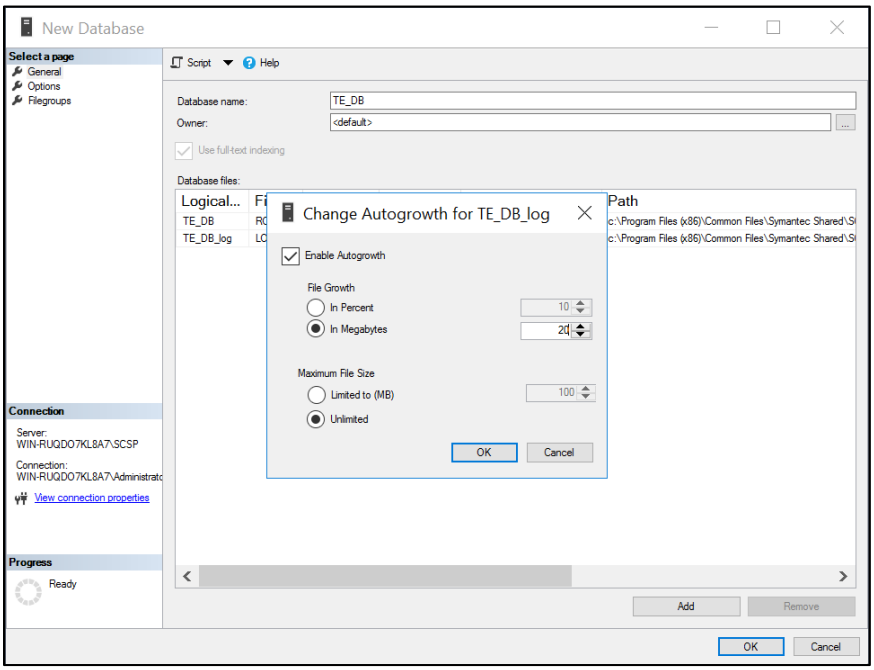
1106 37. Check **Enable Autogrowth**, set **File Growth** to at least **20 MB**, and set **Maximum File Size** to
1107 **Unlimited.**

1108 38. Click **OK**.

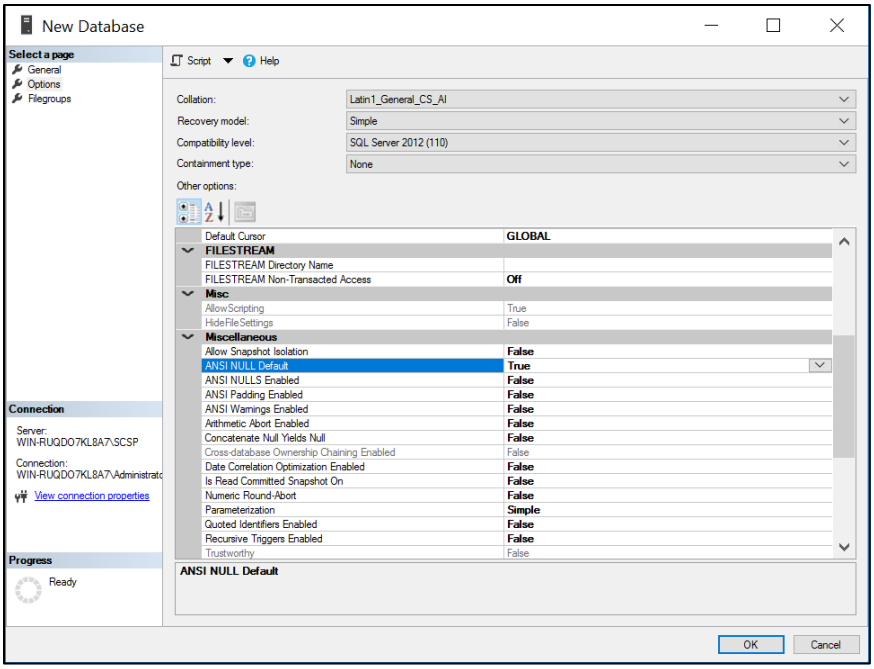


1109

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

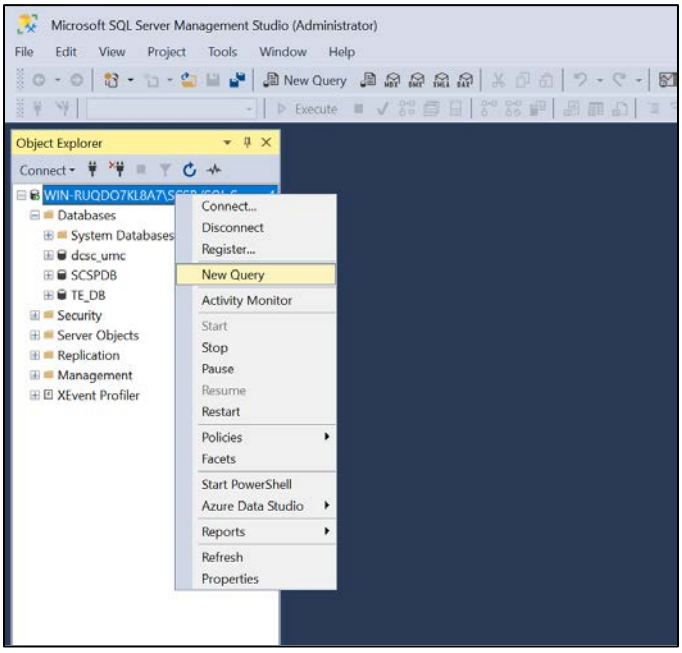


43. On the left, under **select a page**, select **Options**.
44. Set **Collation** to **Latin1_General_CS_AI**.
45. Set **Recovery model** to **Simple**.
46. Under **Other Options > Miscellaneous** set **ANSI NULL Default** to **True**.
47. Click **OK.**



1121

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



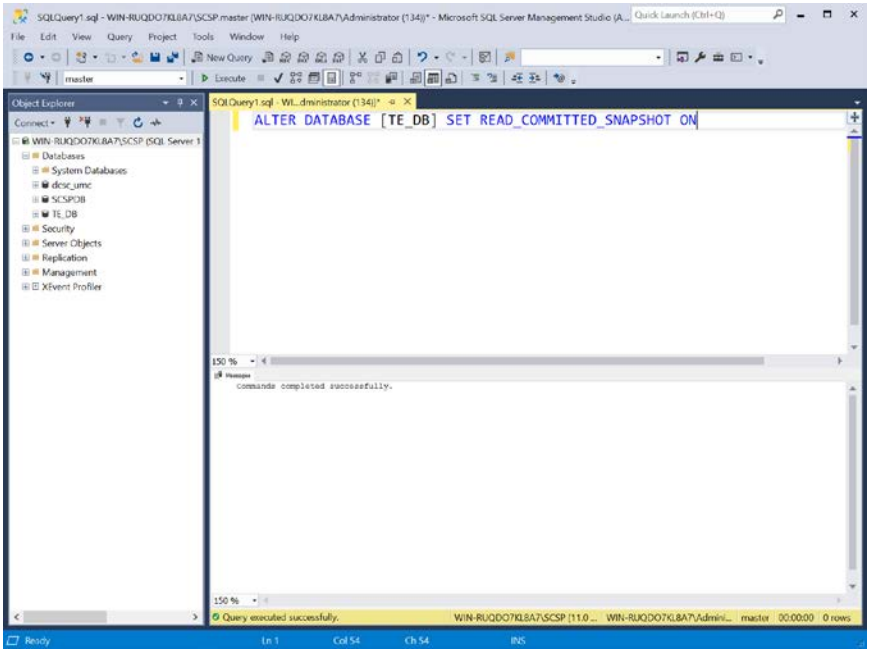
1123

1124 49. Type out the following query:

1125 `ALTER DATABASE [TE_DB] SET READ_COMMITTED_SNAPSHOT ON`

50. Click **Execute** in the toolbar above the **SQL Query** window.

51. Under the **SQL Query** window, in the **Messages** window, verify the command was completed successfully.

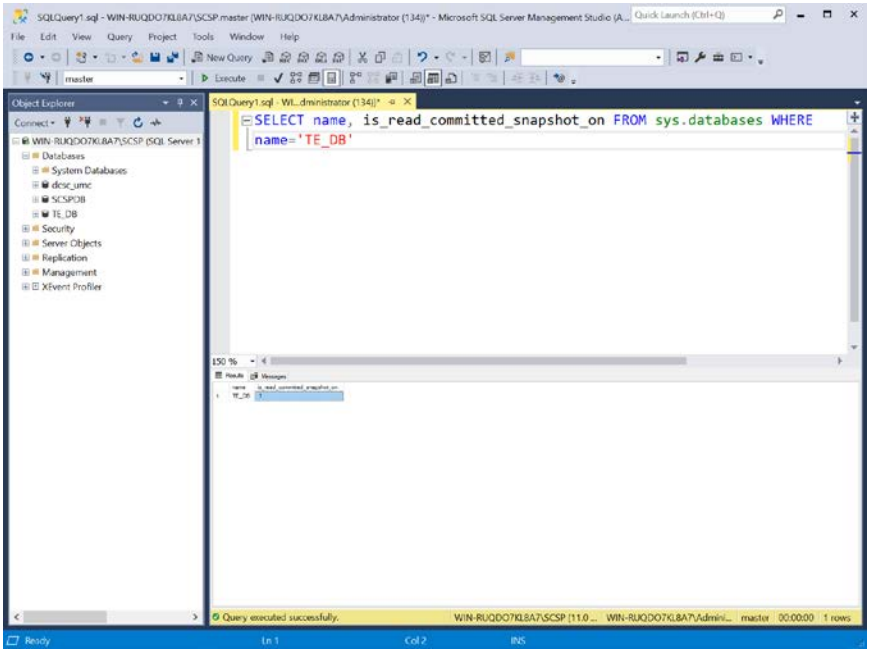


52. Clear the **SQL Query** window, and then type out the following query.

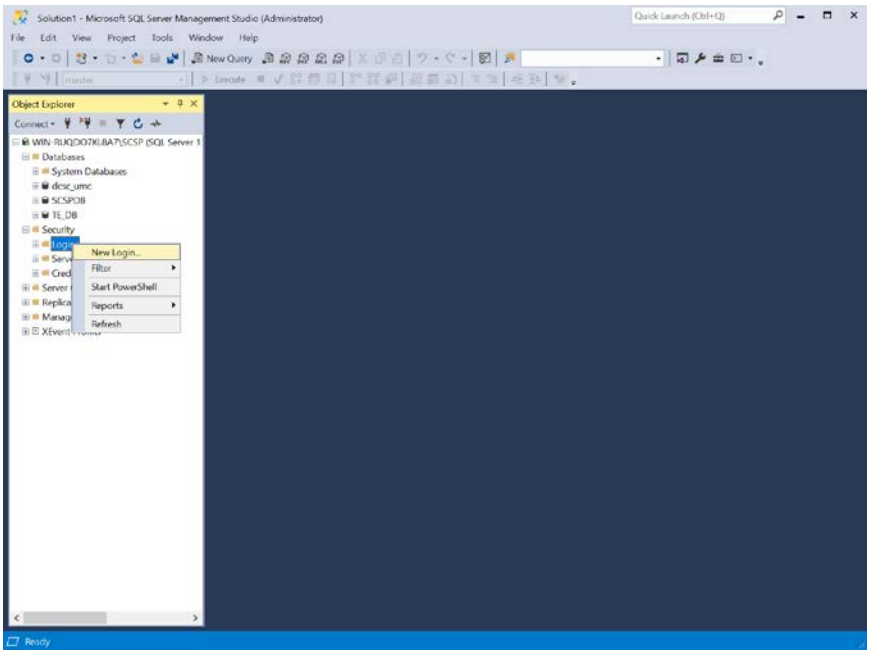
```
SELECT name, is_read_committed_snapshot_on FROM sys.databases WHERE
name='<db_name>'
```

53. Click **Execute** in the toolbar above the **SQL Query** window.

54. Under the **SQL Query** window, in the **Messages** window, verify the **value for is_read_committed_snapshot_on** is set to **1**.



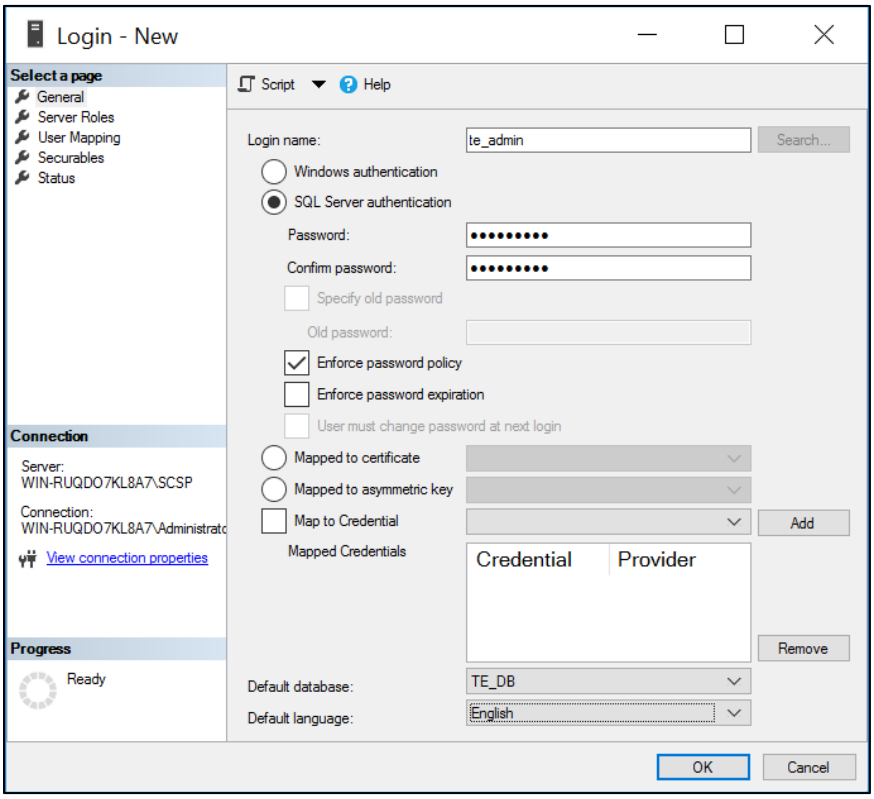
55. In the **Object Explorer**, expand the selection for your database, expand the **Security** section, right click on **Logins**, and select **New Login…**



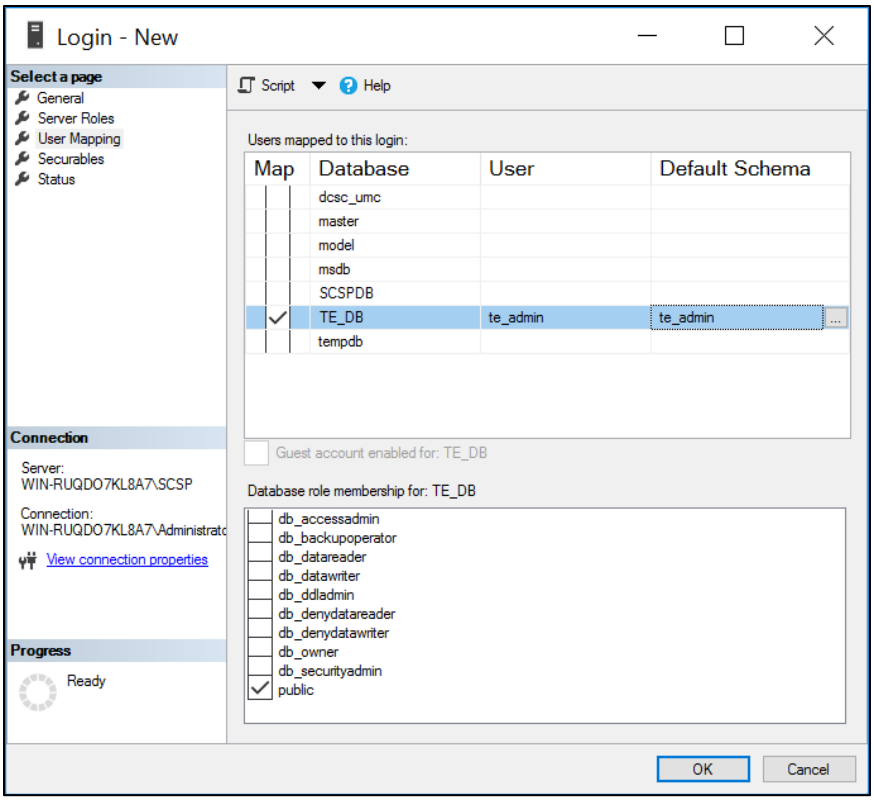
56. On the left, under **Select a page**, select **General**.

57. Create a **Login name**.

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

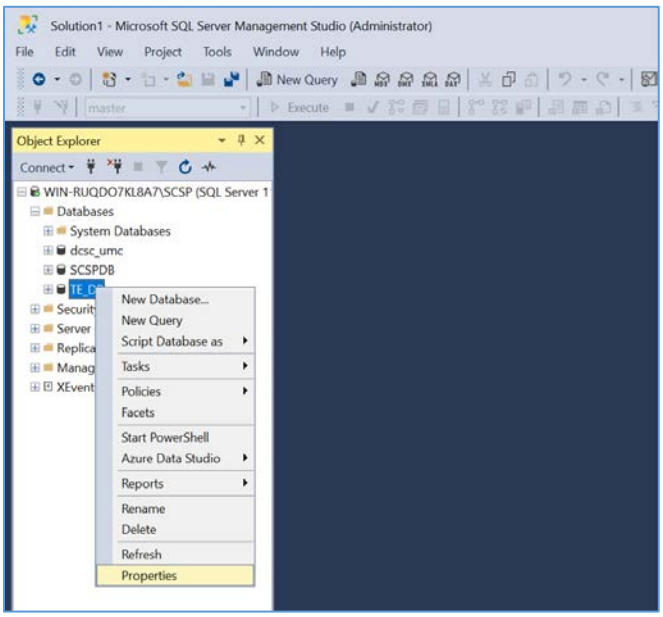


62. On the left, under **Select a page**, select **User Mapping**.
63. Under the **Users mapped to this login** window, perform these actions for the row containing the previously created database:
    a. Check the box in the **Map** column.
    b. In the **Default Schema** column, type the name of the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



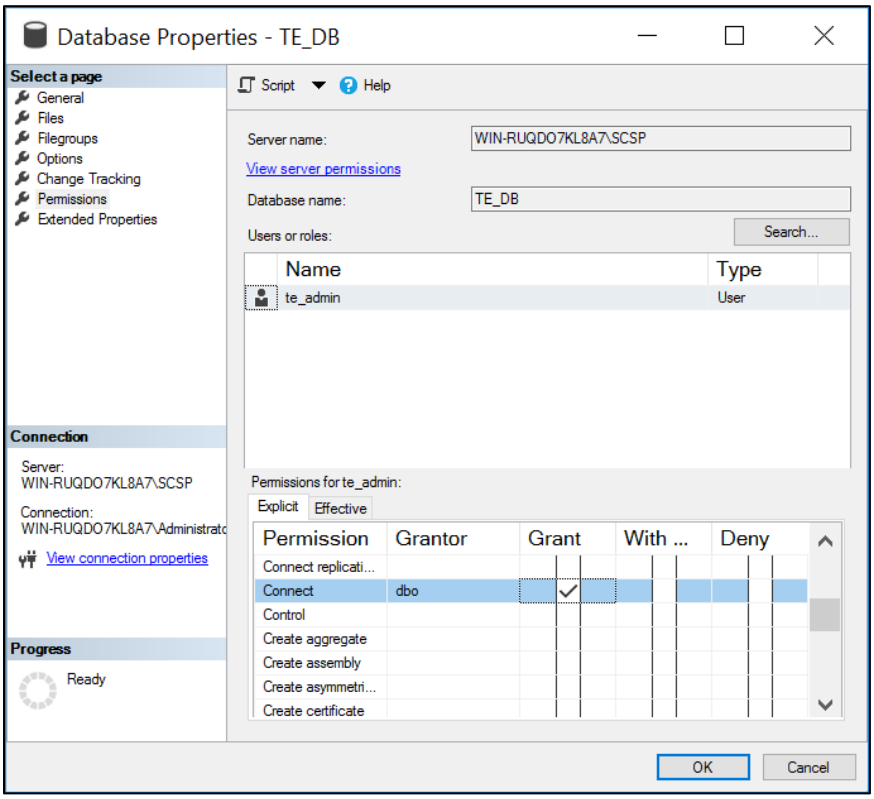
1153

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**.

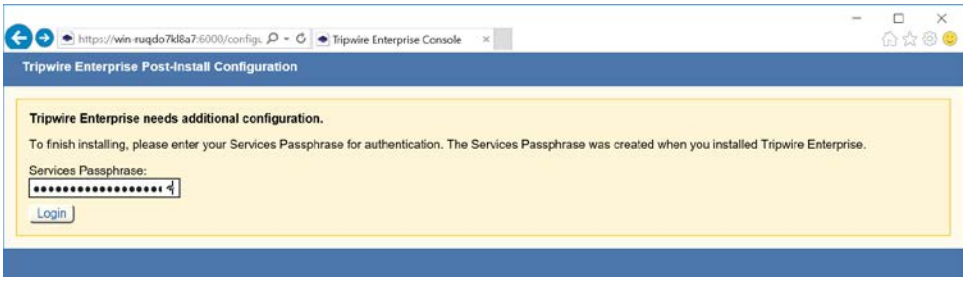


1156

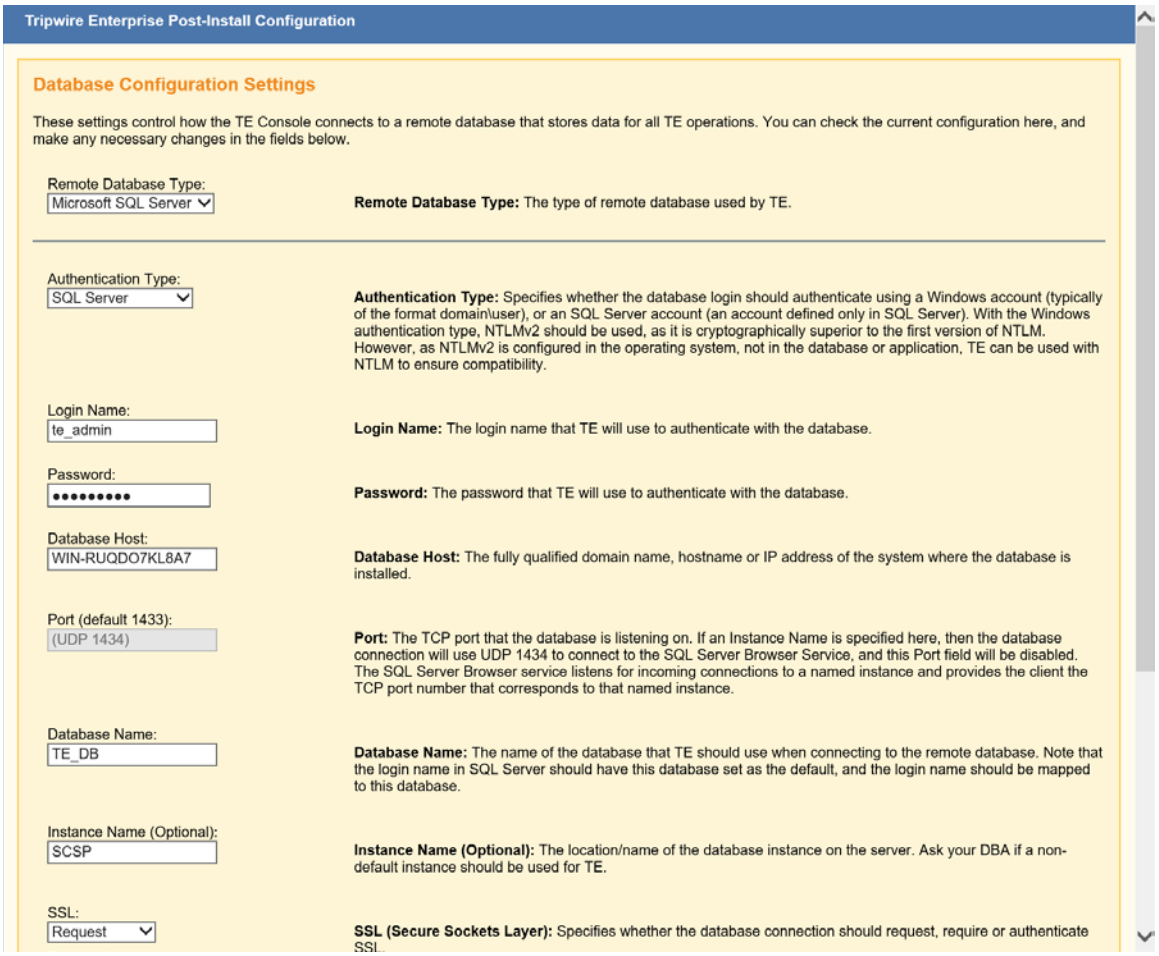
66. On the left, under **select a page**, select **Permissions**.
67. Under **Permissions for user**, check the box in the **Grant** column for the following permissions:
    - **Connect**
    - **Create Function**
    - **Create Procedure**
    - **Create Table**
    - **Create View**
    - **Delete**
    - **Insert**
    - **Select**
    - **Update**
68. Click **OK.**



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

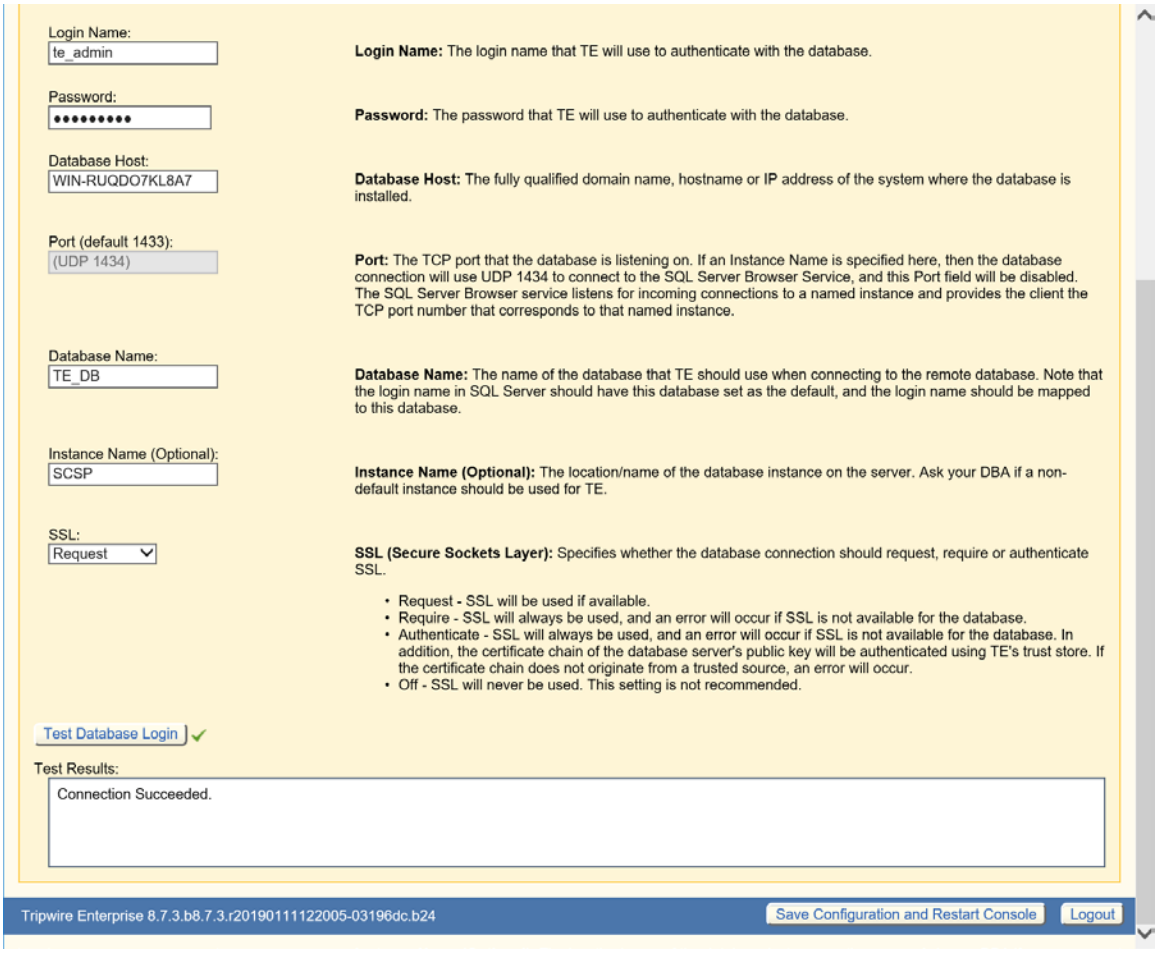


72. Under **Database Configuration Settings**, provide the information that follows:
    - **Remote Database Type**: Microsoft SQL Server
    - **Authentication Type**: SQL Server
    - **Login Name**: te_admin
    - **Password**: *********
    - **Database Host**: WIN-RUQDO7KL8A7
    - **Database Name**: TE_DB
    - **Instance Name**: SCSP (Note: this may not be necessary, depending on how your SQL Server Database is configured)
    - **SSL**: Request



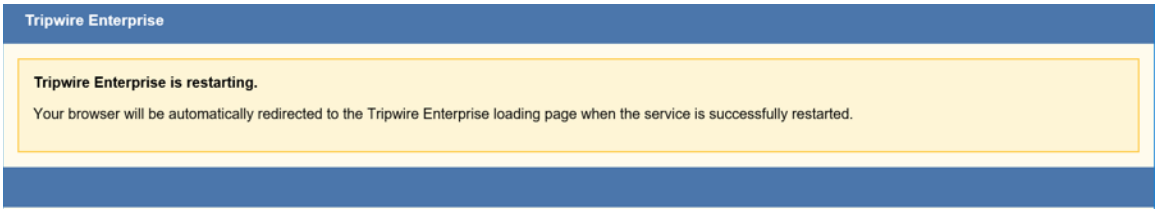
73. Click **Test Database Login** and verify the connection is successful.

74. Click **Save Configuration and Restart Console**.



1188

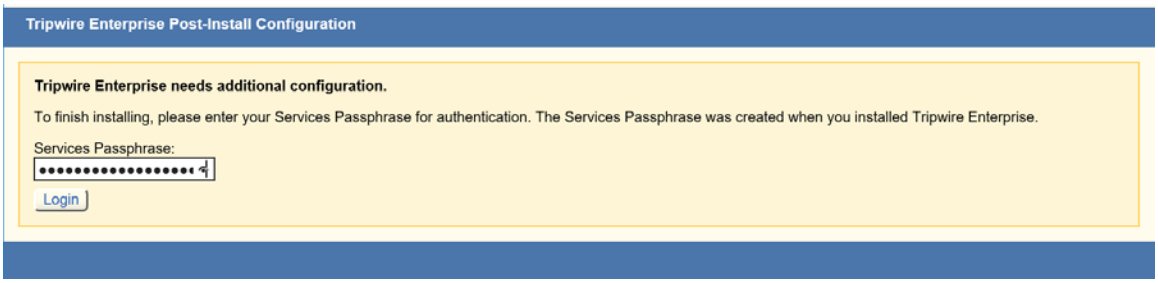
1189 75. Wait for Tripwire Enterprise to restart and redirect you to the log in page.



1190

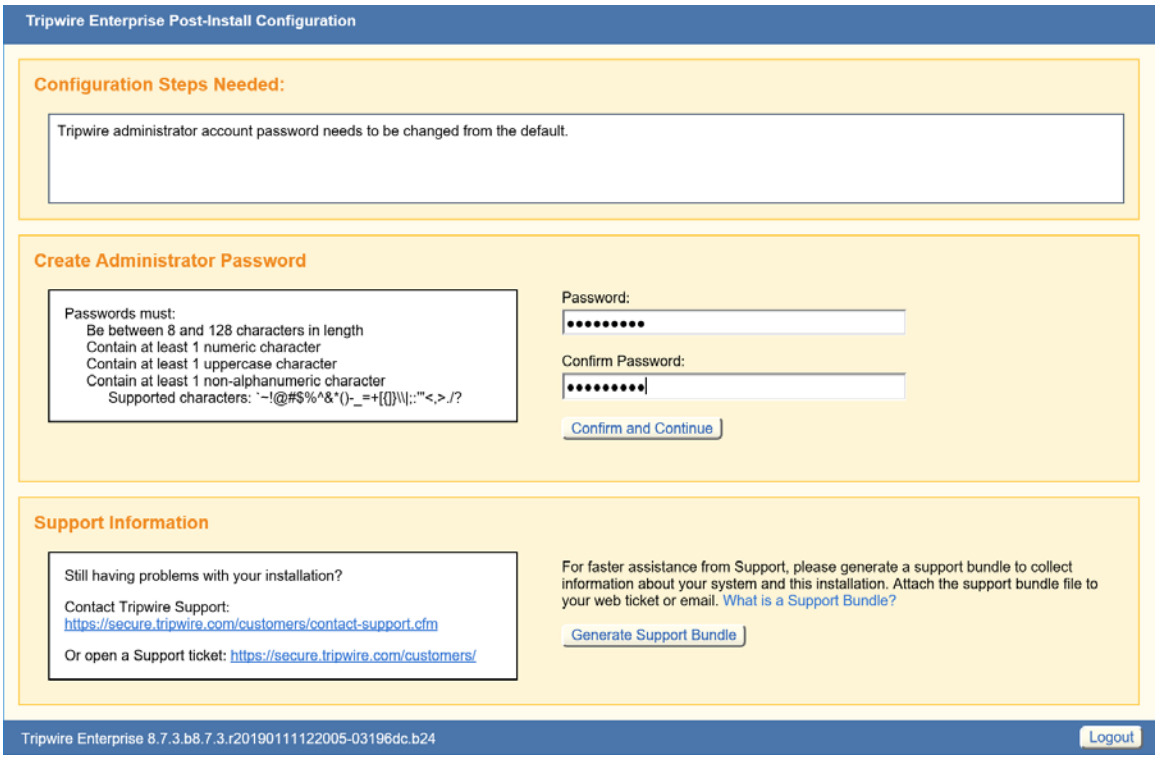
1191 76. Enter the **services password** created during the install process.

1192 77. Click **Login**.



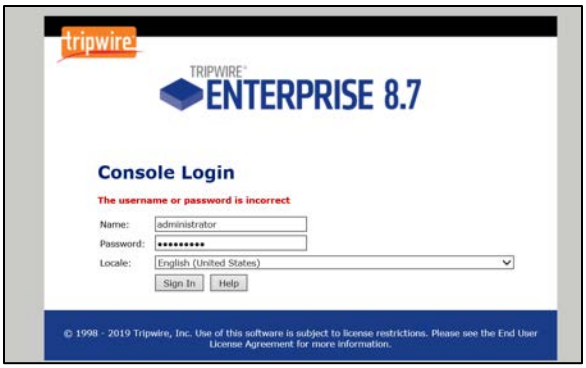
78. Under **Create Administrator Password**, create a password for the Tripwire Enterprise administrator account.

79. Click **Confirm and Continue**.



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

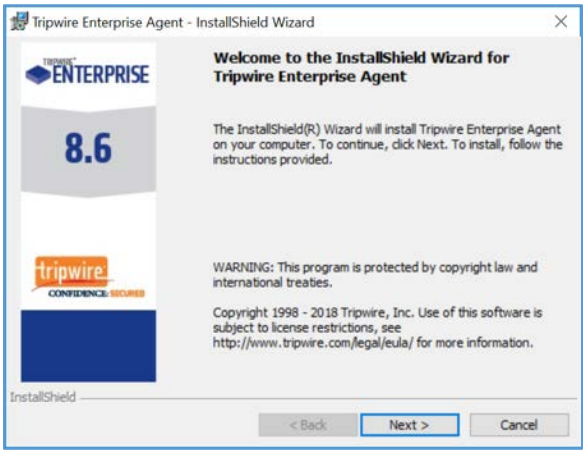
81. Click **Sign In**.



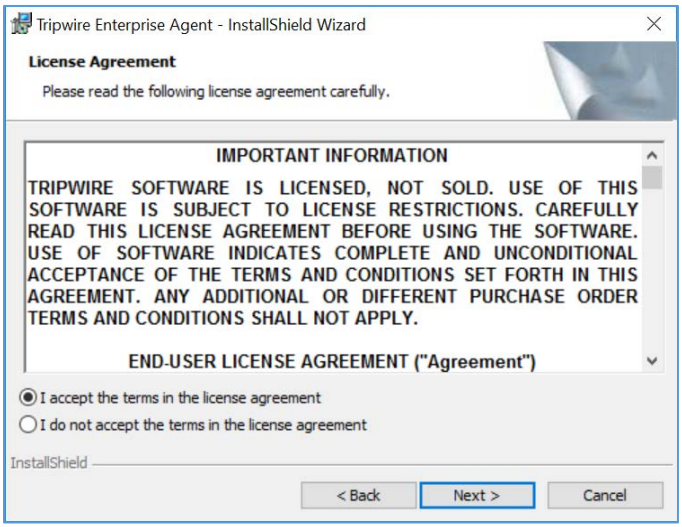
82. Click **Configure Tripwire Enterprise** to begin the configuration process.

Tripwire Enterprise Agent Installation

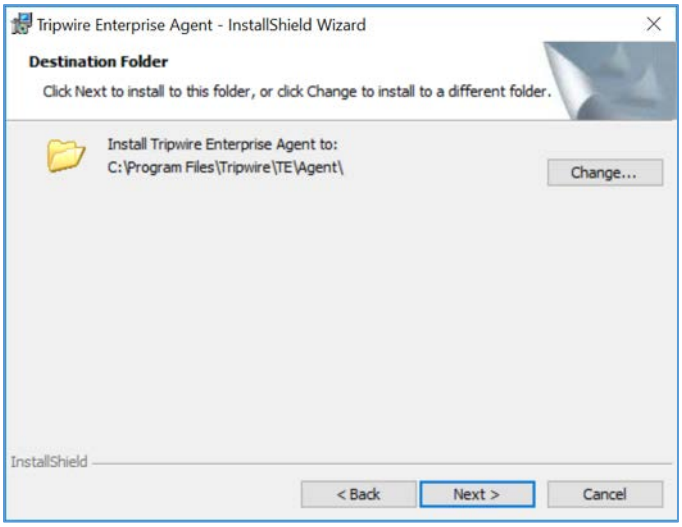
1. **Run** te_agent.msi.
2. Click **Next >**.



3. Check **I accept the terms in the license agreement**.
4. Click **Next >**.

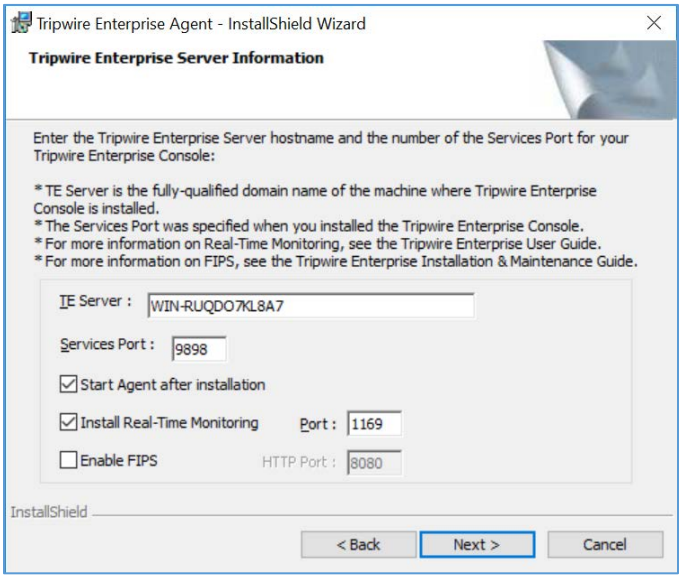


5. Specify an install directory for the Tripwire Enterprise Agent.
6. Click **Next >**.

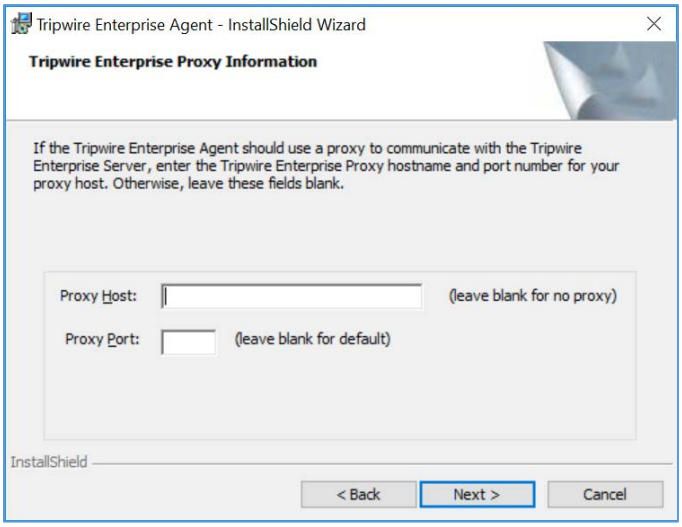


7. Enter the **TE Server** (e.g., **WIN-RUQDO7KL8A7**) of the server where Tripwire Enterprise is installed.
8. Enter **9898** as the **Services Port** established during the installation process of Tripwire Enterprise.
9. Check **Start Agent**, after installation.

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

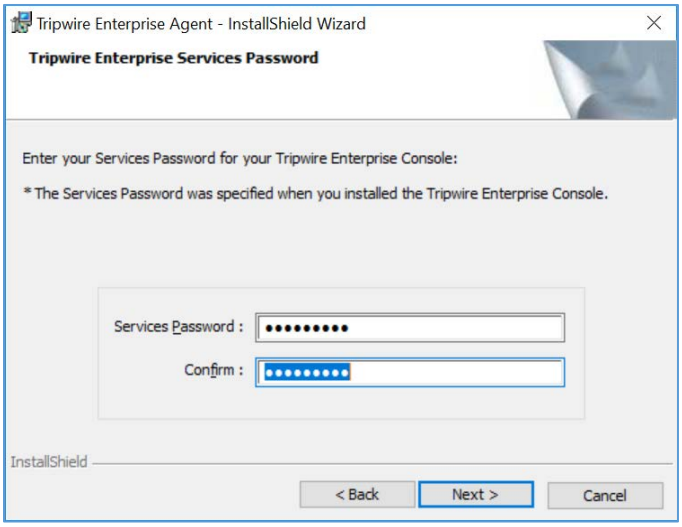


13. Specify a **Proxy Host** and **Proxy Port** if necessary.
14. Click **Next >**.

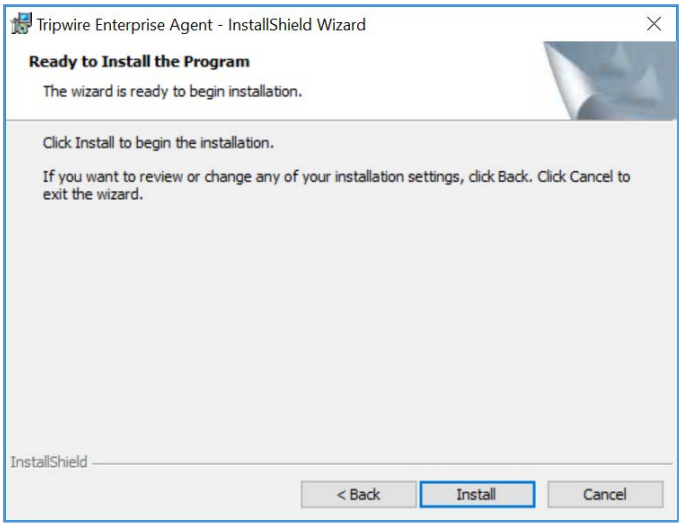


15. Enter the **Services Password** created during the installation process for Tripwire Enterprise.

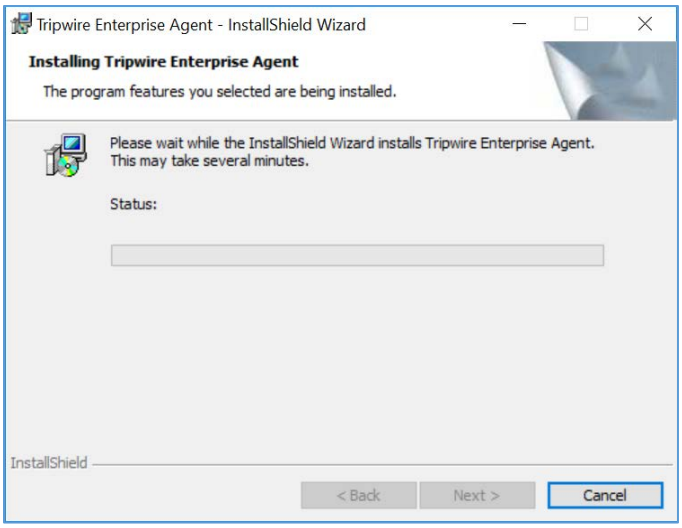
16. Click **Next >**.



17. Click **Install**.

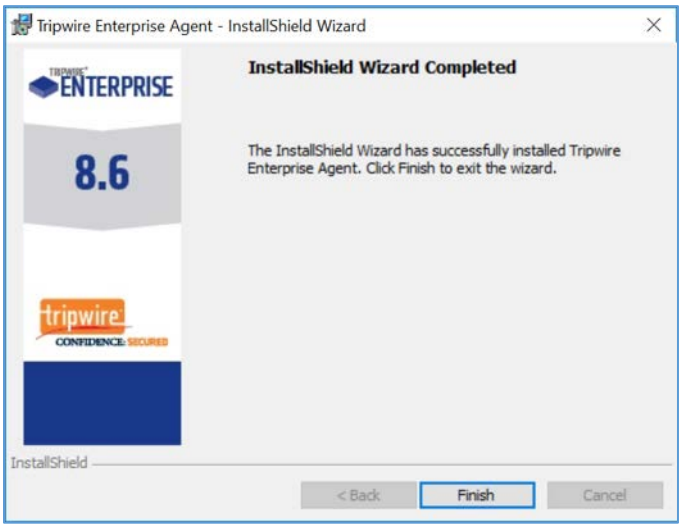


18. Wait for the installation process to complete.



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**

CPU: 1

Memory: 4 GB Ram

Storage: 120 GB (Thin Provision)

Operating System: Microsoft Windows Server 2012 R2

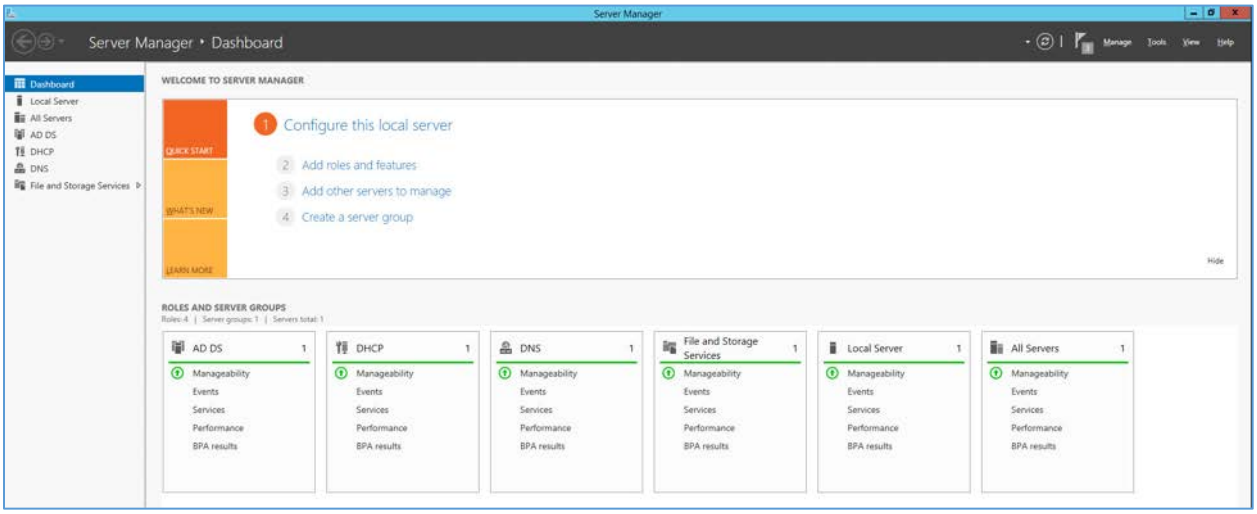
Network Adapter: VLAN 1201

Enterprise Domain Services Installation

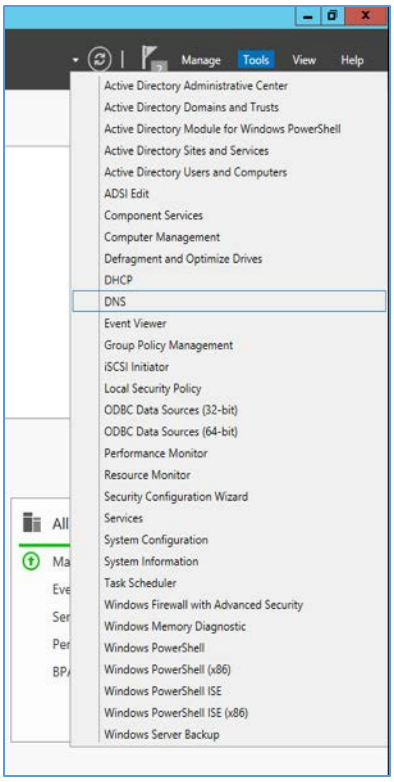
Install the Domain Controller, AD, and DNS appliances according to the instructions detailed in *Building Your First Domain Controller on 2012 R2* [12].

DNS Server Forward Lookup Zone Configuration

1. Open **Server Manager**.

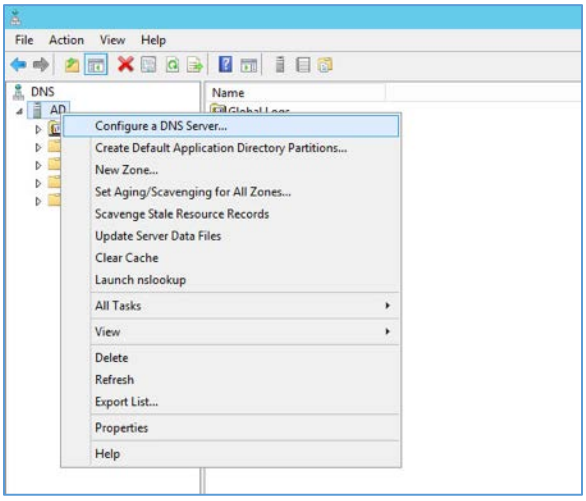


2. In the top right, click on **Tools > DNS**.
3. DNS forward lookup zone should have already been created during the DNS setup process performed previously. If not, follow these instructions:



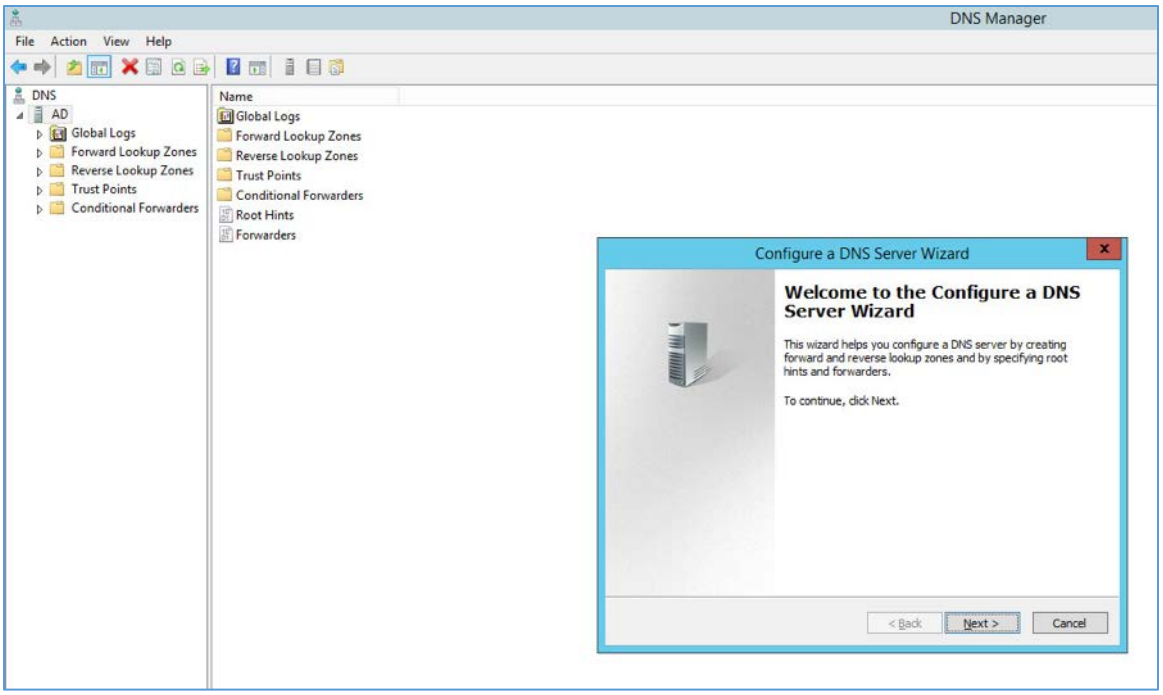
1252

1253 a. Right click on your server's name, and select **Configure a DNS Server…**



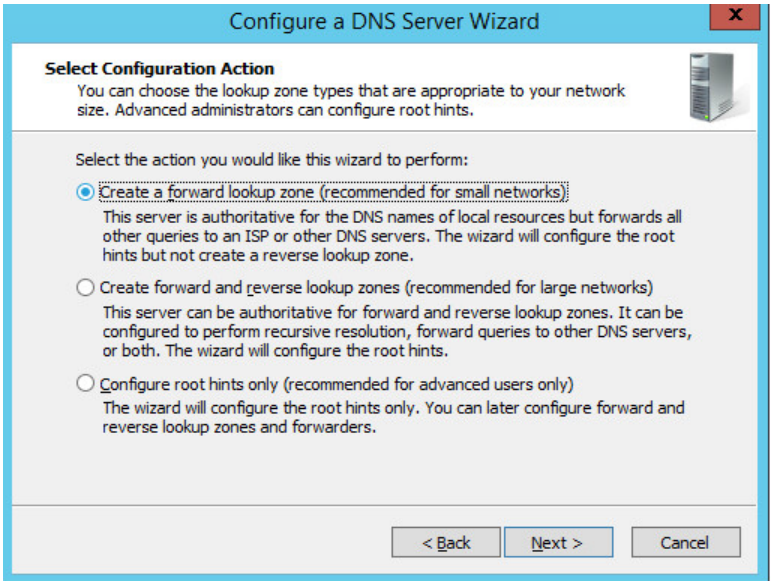
1254

1255 b. Click **Next >**.



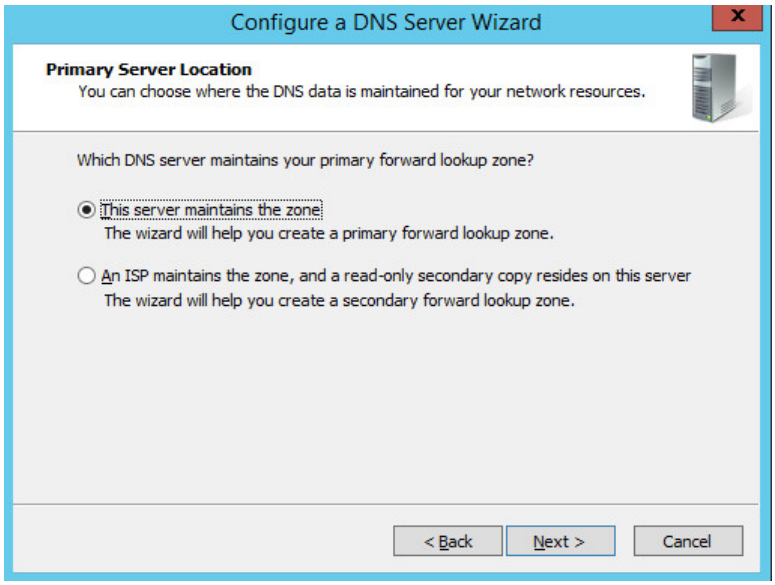
1256

1257 c. Click **Next >**.



1258

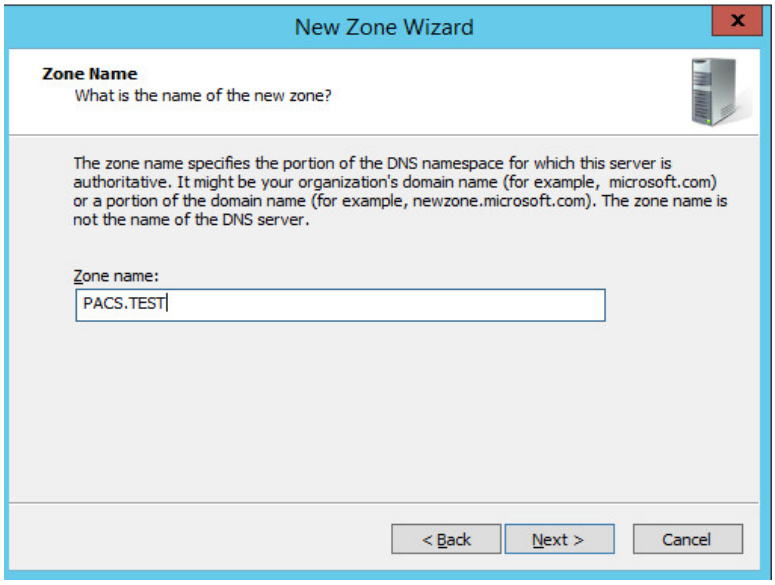
1259 d. Click **Next >**.



1260

1261 e. Enter **PACS.TEST** as the **Zone name**, that was established previously during setup.

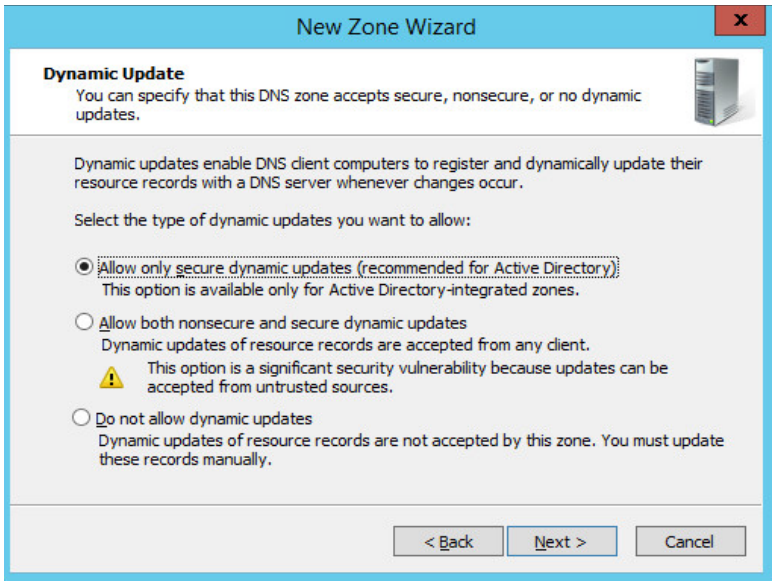
1262 f. Click **Next >**.



1263

1264 g. Select **Allow only secure dynamic updates**.

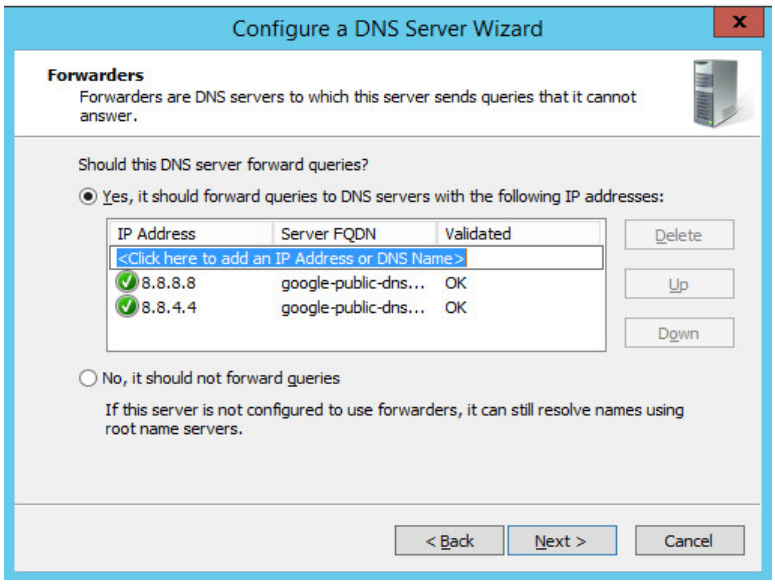
1265 h. Click **Next >**.



1266

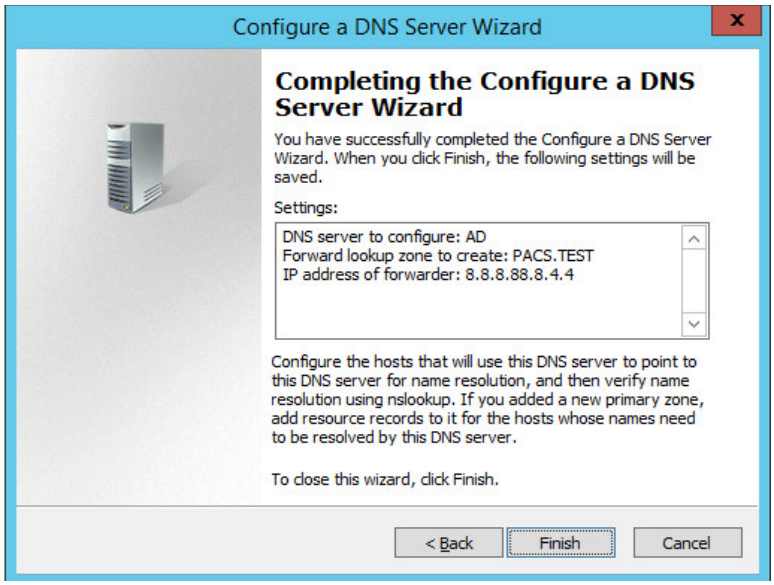
1267 i. Add **Forwarders** (8.8.8.8 and 8.8.4.4 are Google's DNS servers).

1268 j. Click **Next >**.



1269

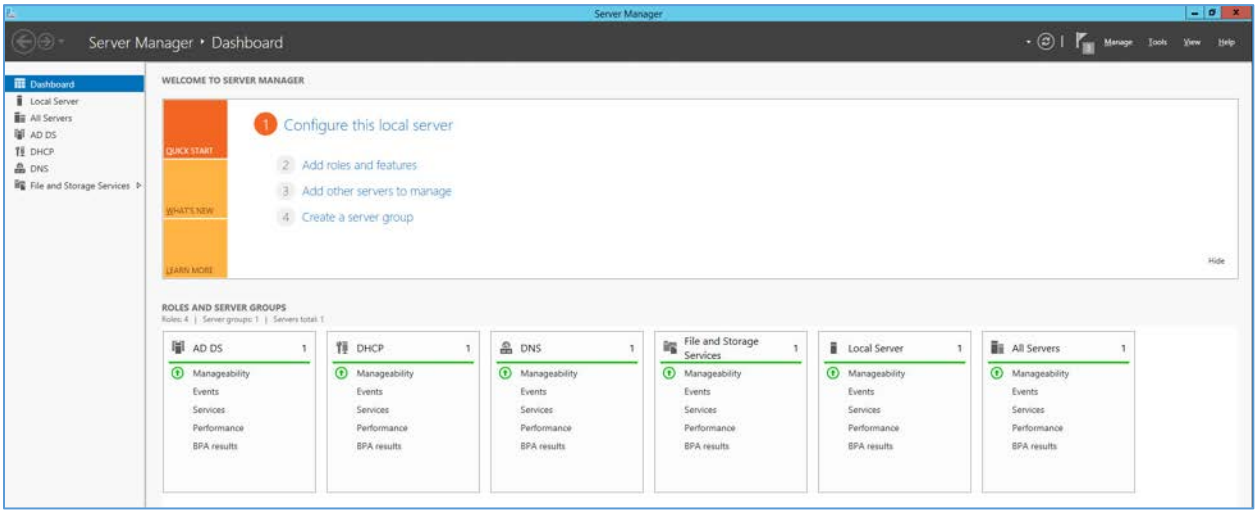
1270 k. Click **Finish**.



1271

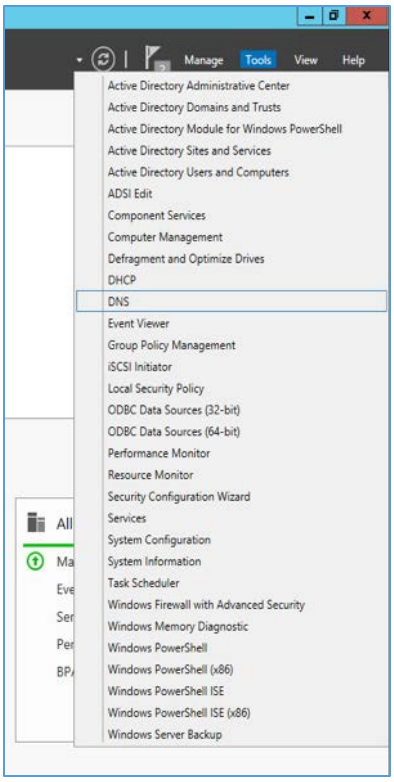
1272 **DNS Server Reverse Lookup Zone Configuration**

1273 1. Open **Server Manager**.



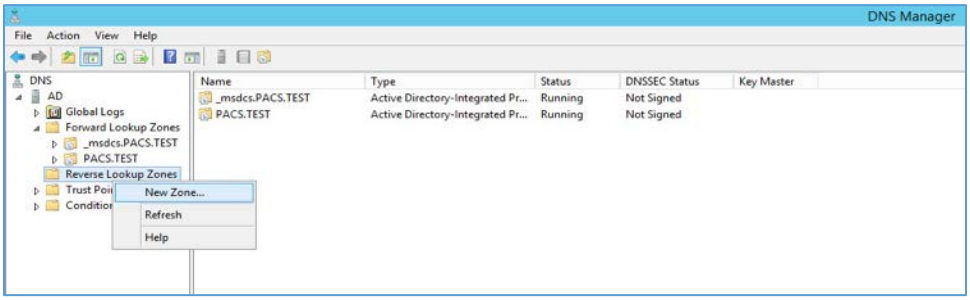
1274

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



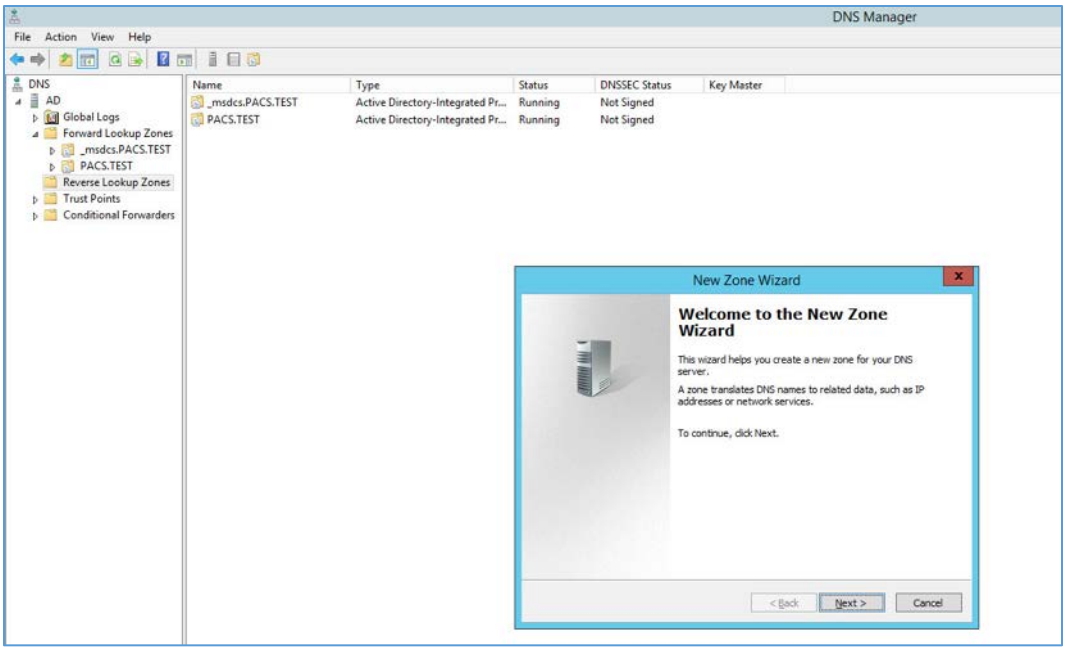
1276

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



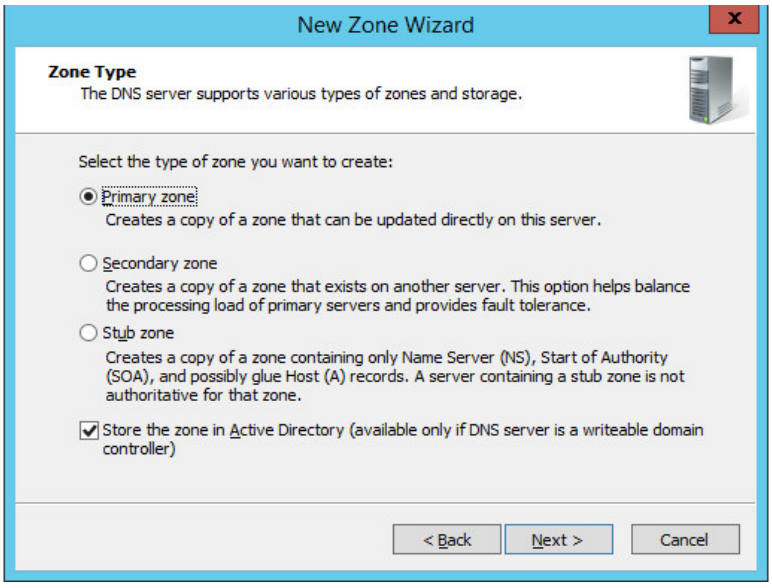
1278

1279 4. Click **Next >**.



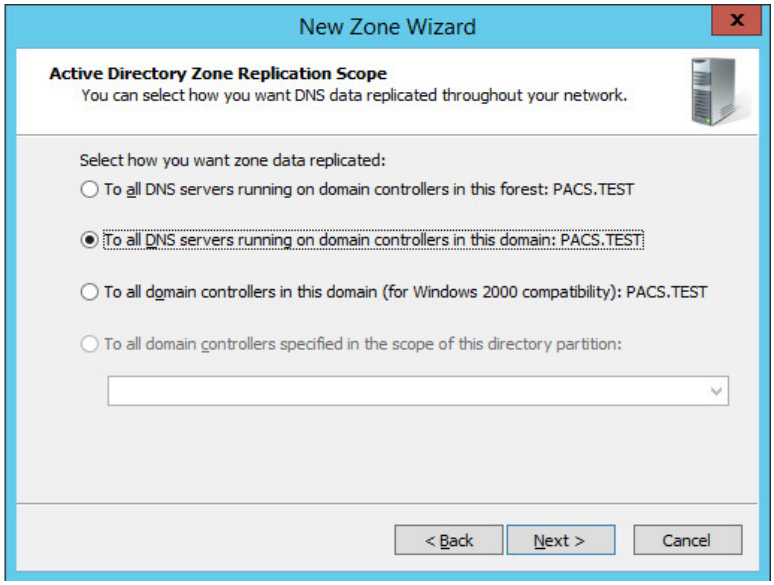
1280

1281 5. Click **Next >**.



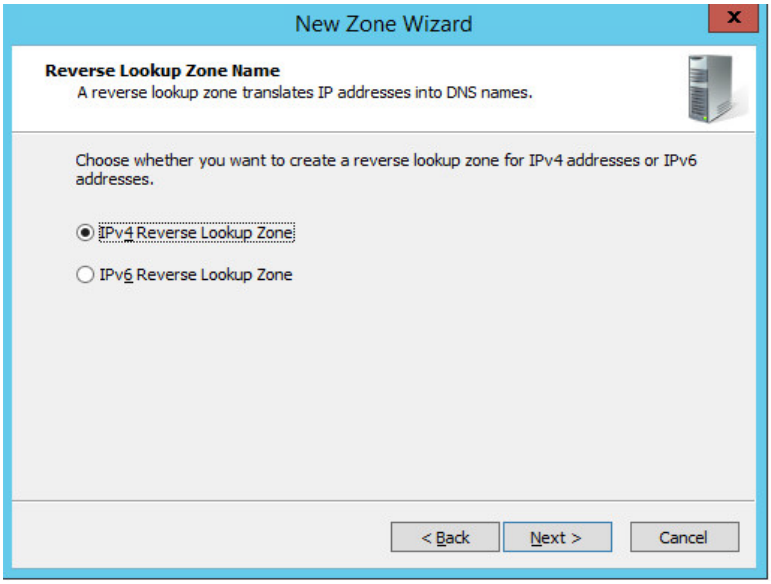
1282

1283 6. Click **Next >**.



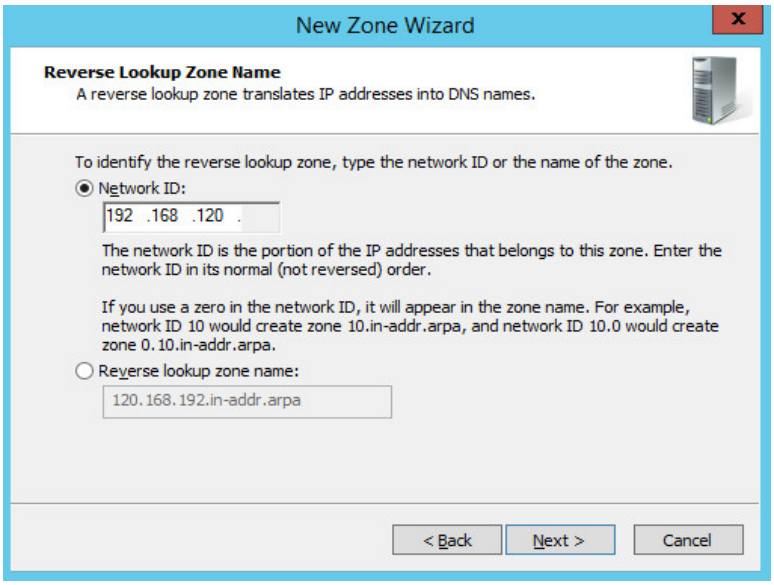
1284

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



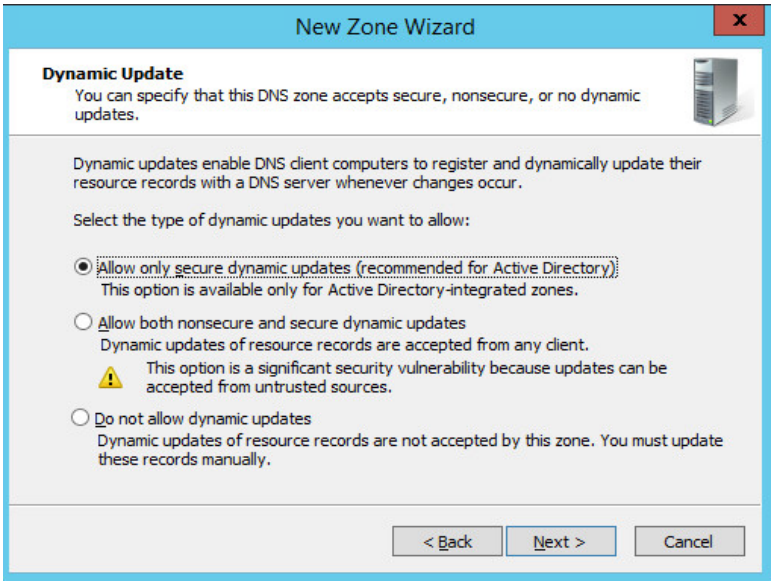
1286

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 >**.



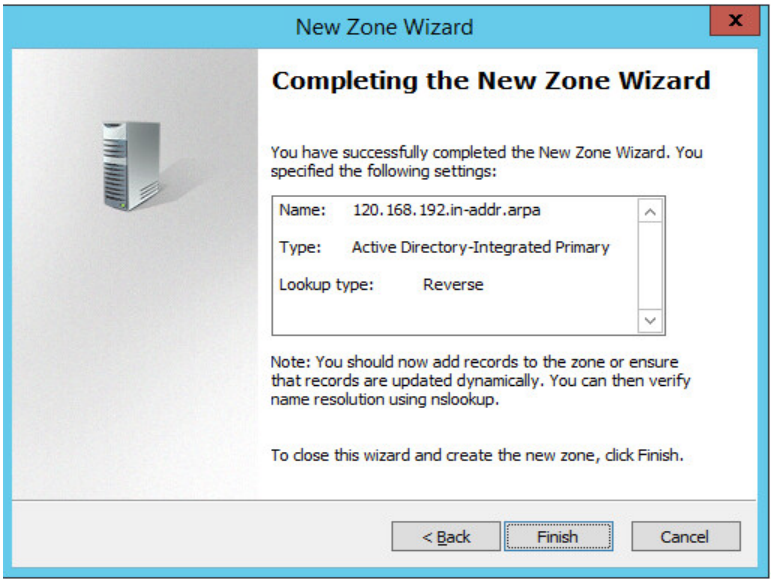
1289

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



1292

1293 10. Click **Finish**.



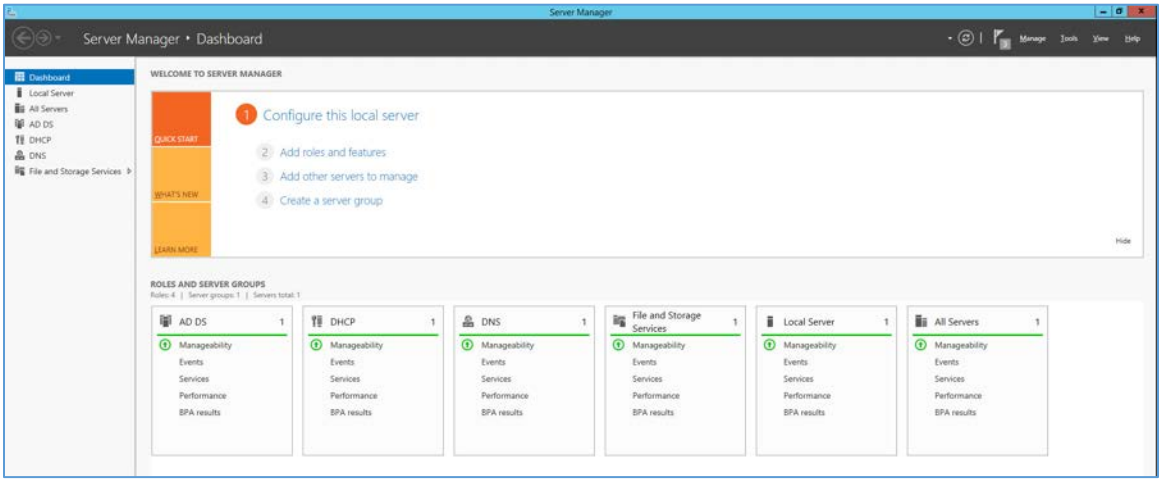
1294

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].

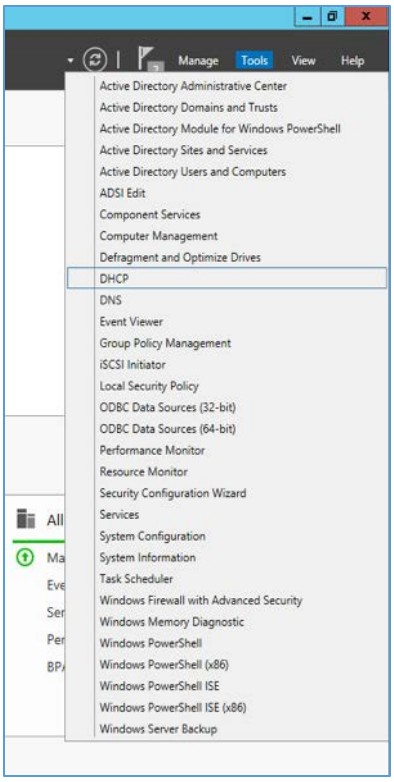
1298 **DHCP Server Configuration**

1299 1. Open **Server Manager**.



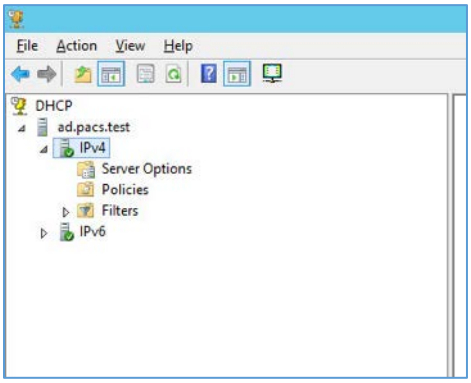
1300

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.

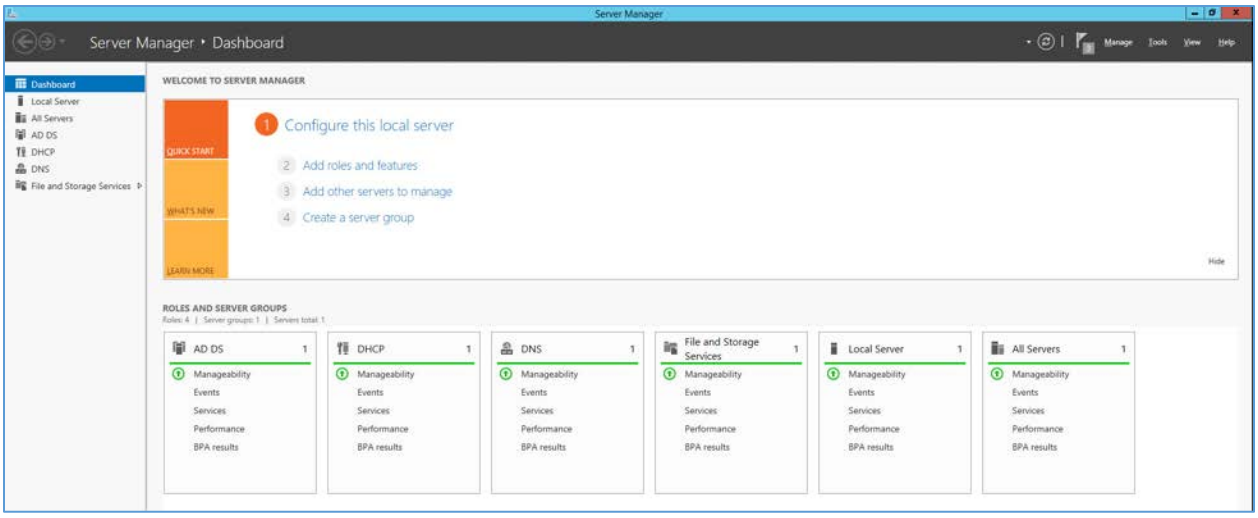


1304

1305 **DHCP Scopes Configuration**

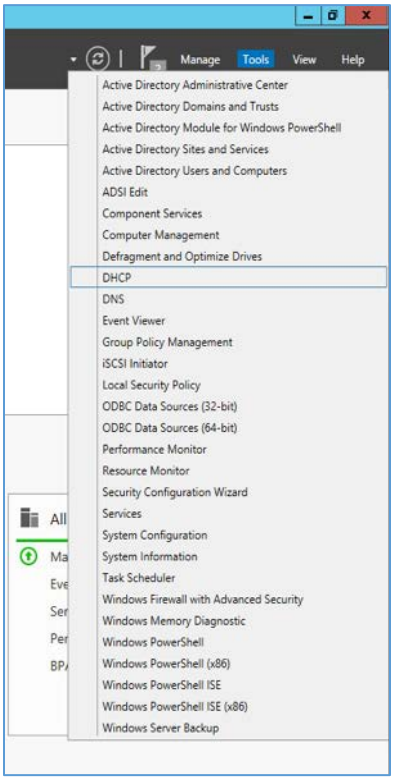
1306 *Performed on Windows Server 2012 R2*.

1307 1. Open **Server Manager**.



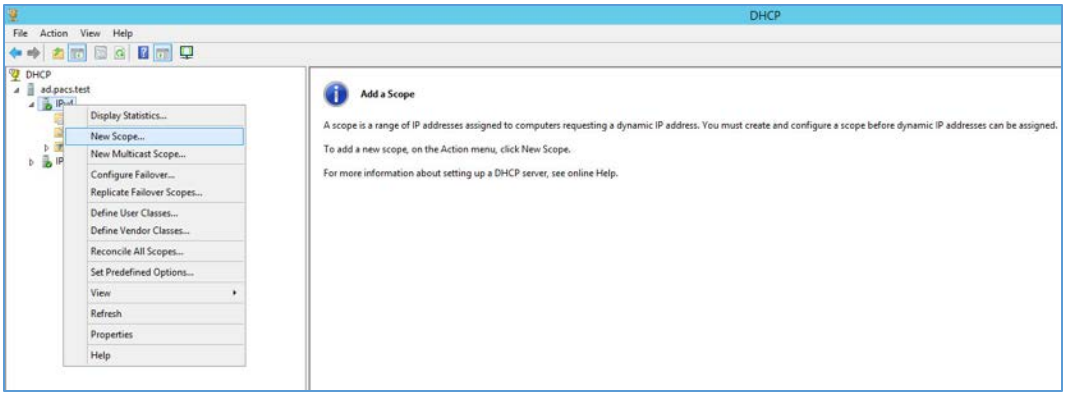
1308

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



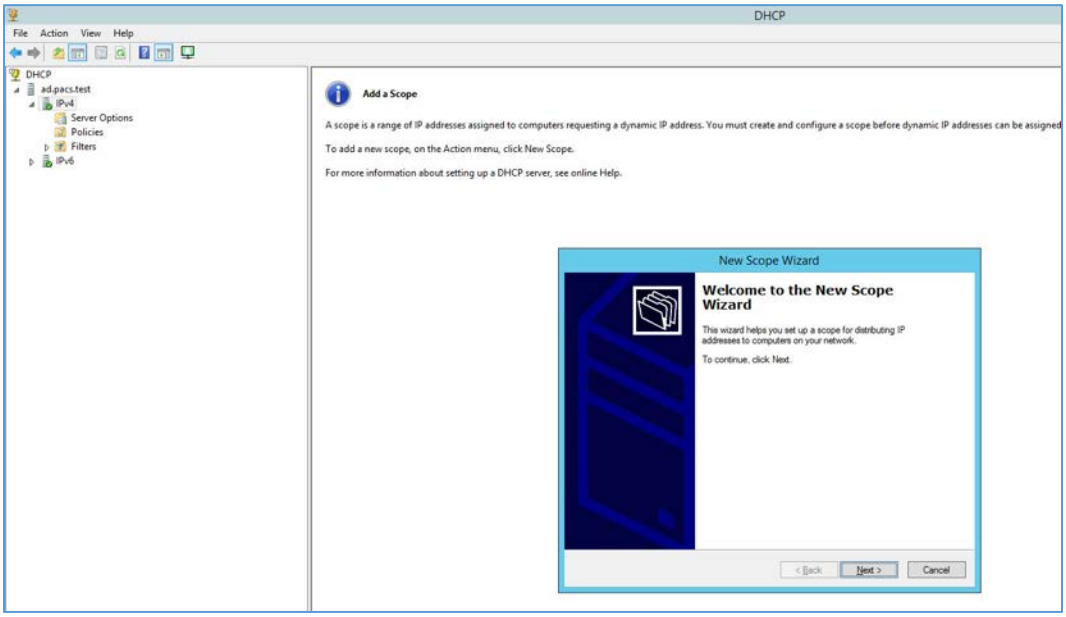
1310

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



1312

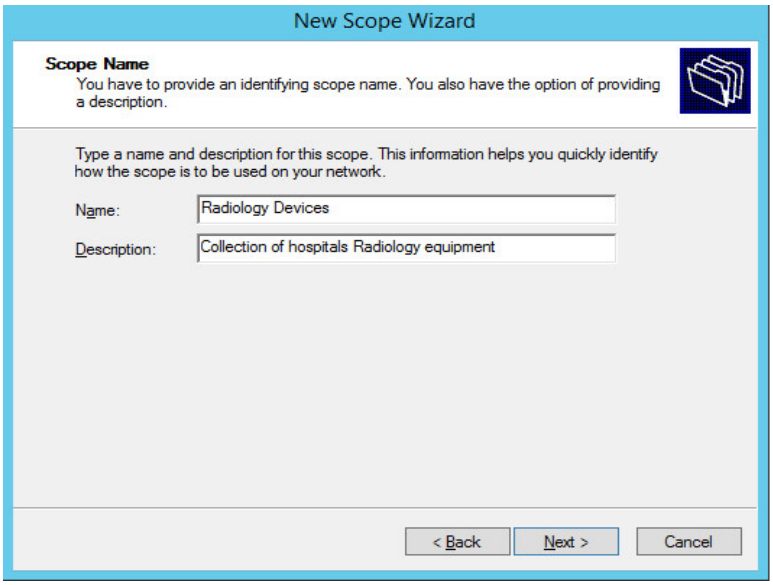
1313 4. **Click Next >**.



1314

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

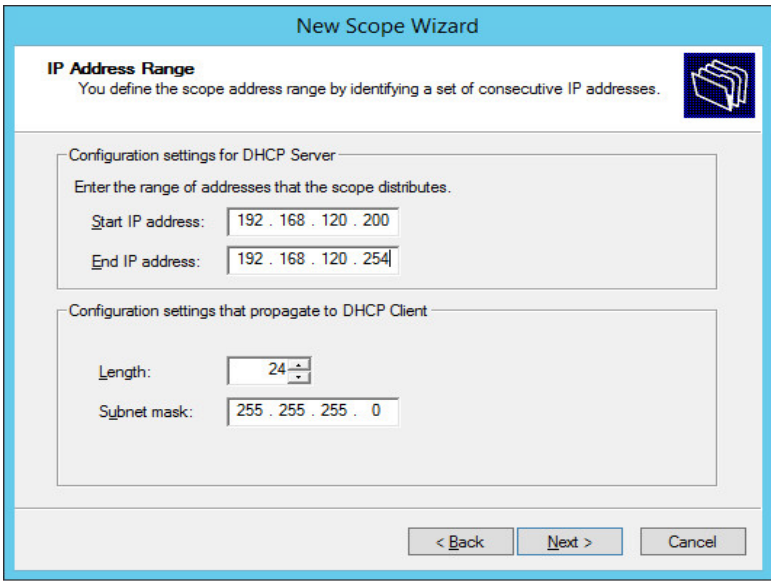
1317 6. Click **Next >**.



1318

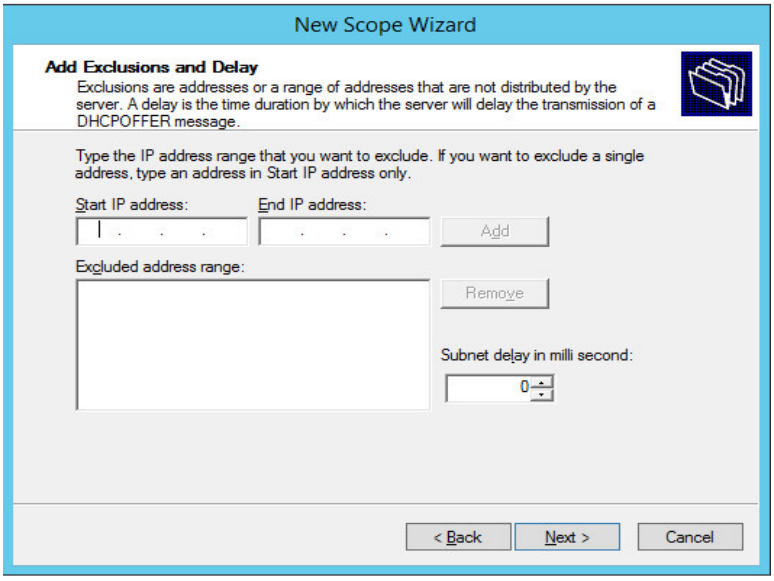
1319 7. Establish the IP range (**192.168.120.200** – **192.168.120.254**) from which the DHCP server should
1320 hand out IPs for devices in this scope.

1321 8. Click **Next >**.



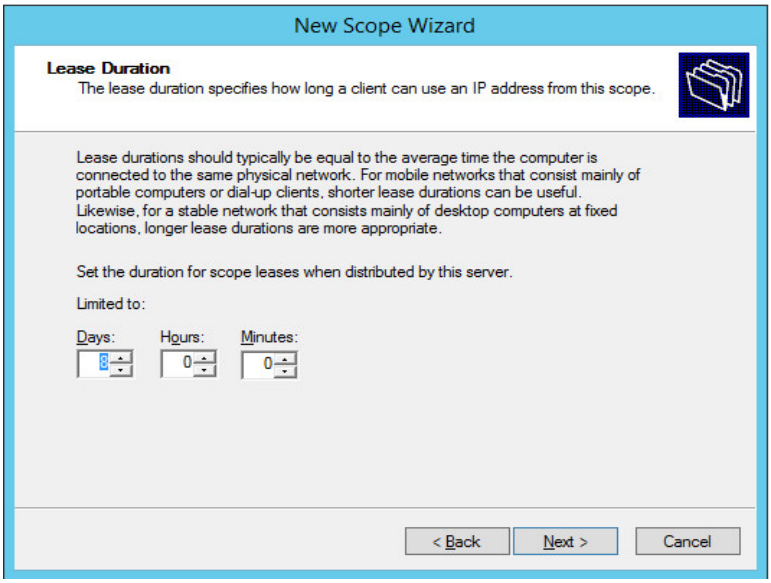
1322

1323 9. Click **Next >**.



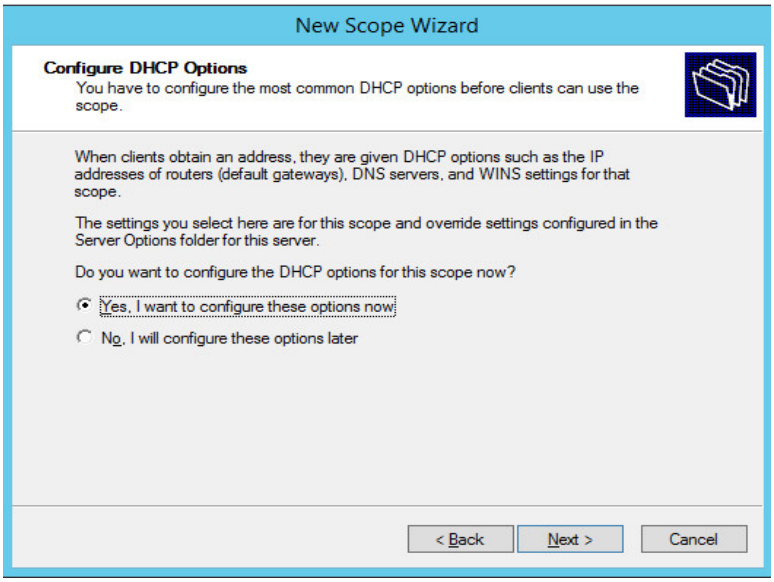
1324

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



1326

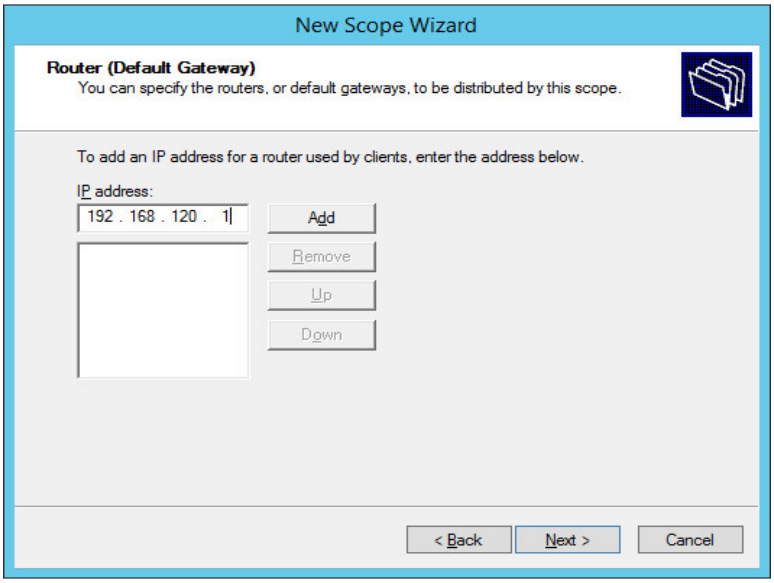
1327 11. Choose **Yes, I want to configure these options now**, and then click **Next >**.



1328

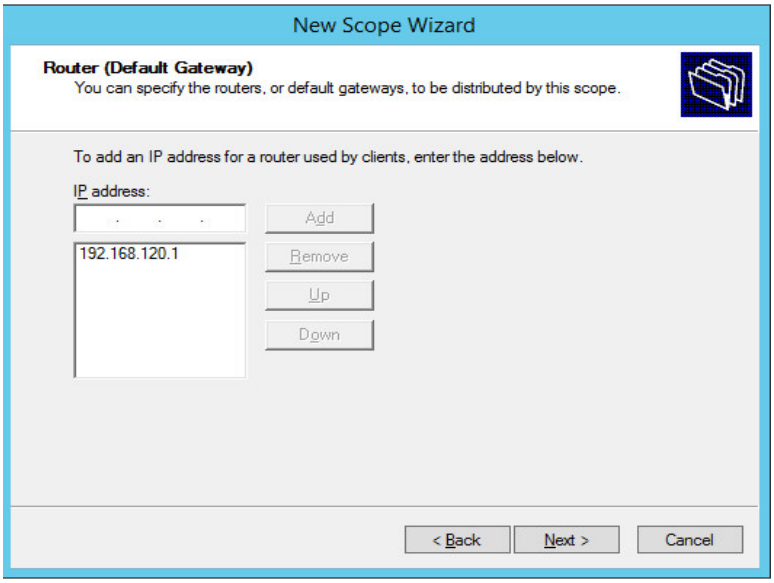
1329 12. Enter the subnet's **Default Gateway** as **192.168.120.1**.

1330 13. Click **Add**.



1331

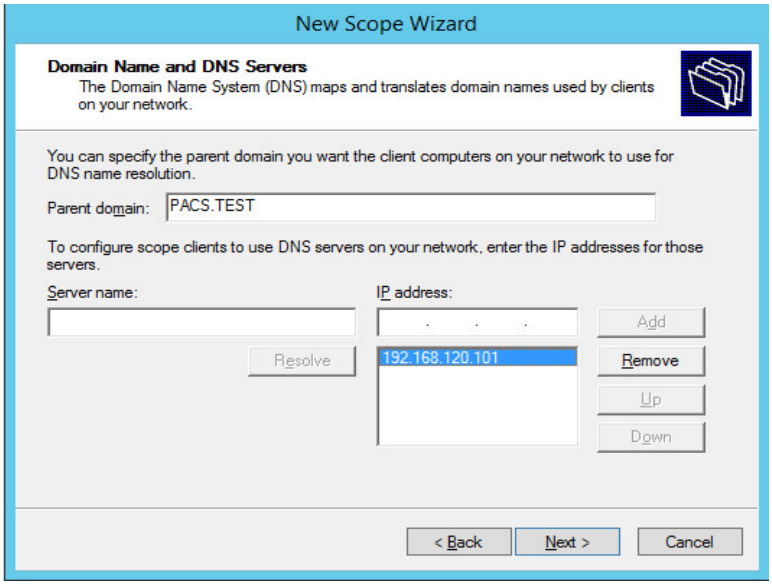
1332 14. Click **Next >**.



1333

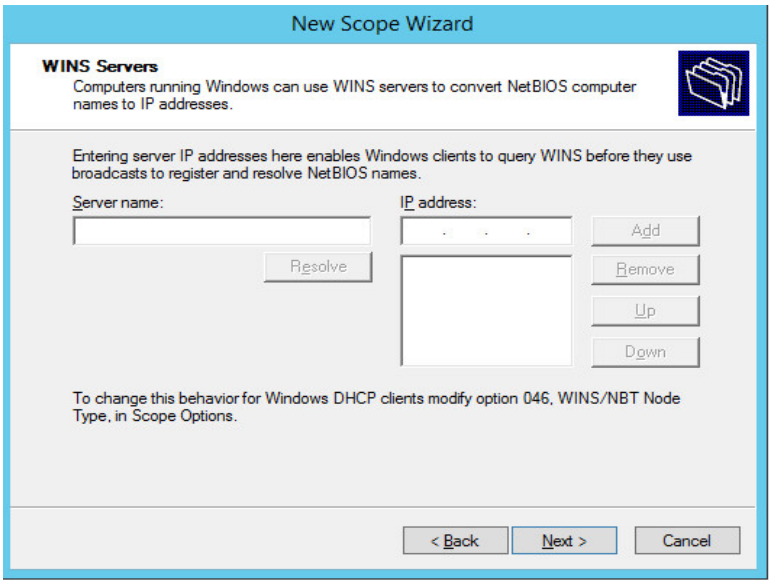
1334 15. Ensure IP address in bottom-right box is the IP address (**192.168.120.101**) for the DNS server
1335 configured earlier.

1336 16. Click **Next >**.



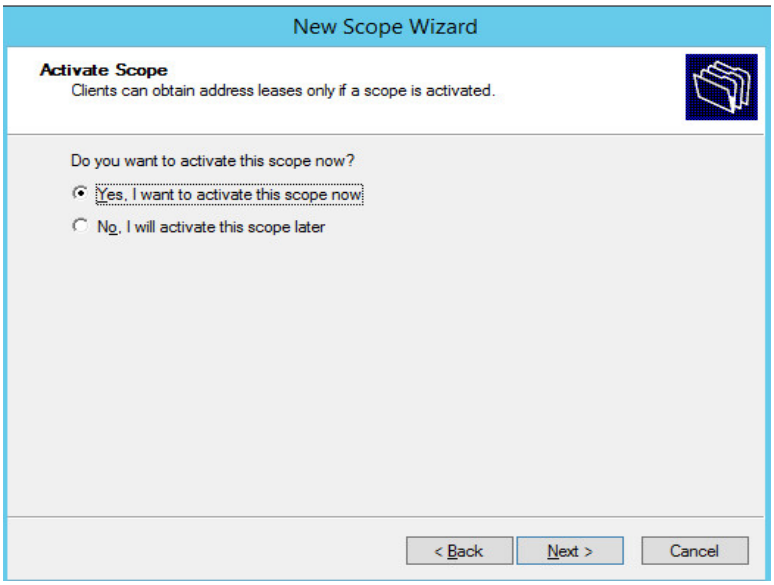
1337

1338 17. Click **Next >**.



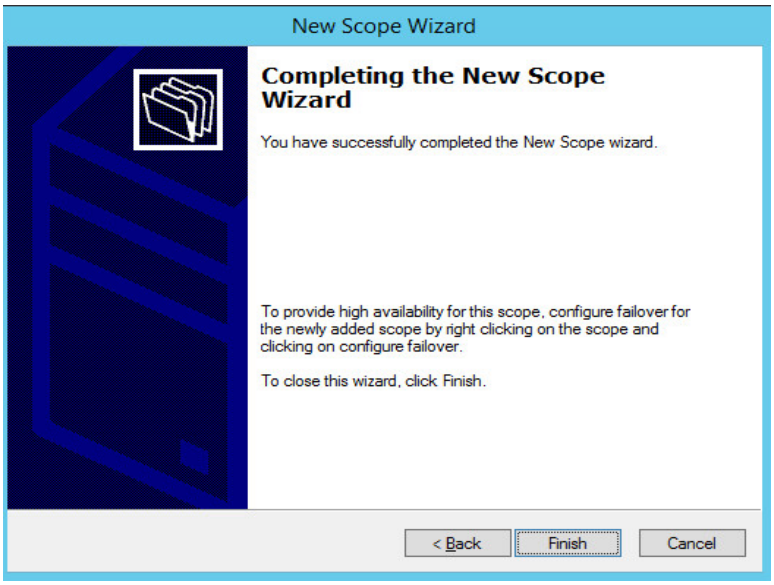
1339

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



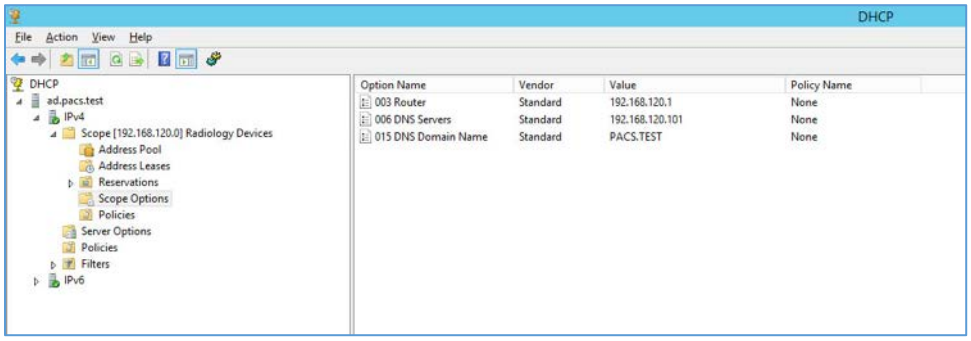
1341

1342 19. Click **Finish**.



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

- **003 Router**: 192.168.120.1
- **006 DNS Servers**: 192.168.120.101
- **015 DNS Domain Name**: PACS.TEST



2.6.2 DigiCert PKI

DigiCert is a cloud-based platform designed to provide a full line of SSL certificates, tools, and platforms, for optimal certificate life-cycle management. To use the service, an account must be established with DigiCert. Once an account is established, access to a DigiCert dashboard is enabled. From the dashboard, DigiCert provides a set of certificate management tools to issue PKI certificates for network authentication and encryption for data-at-rest or data-in-transit as needed.

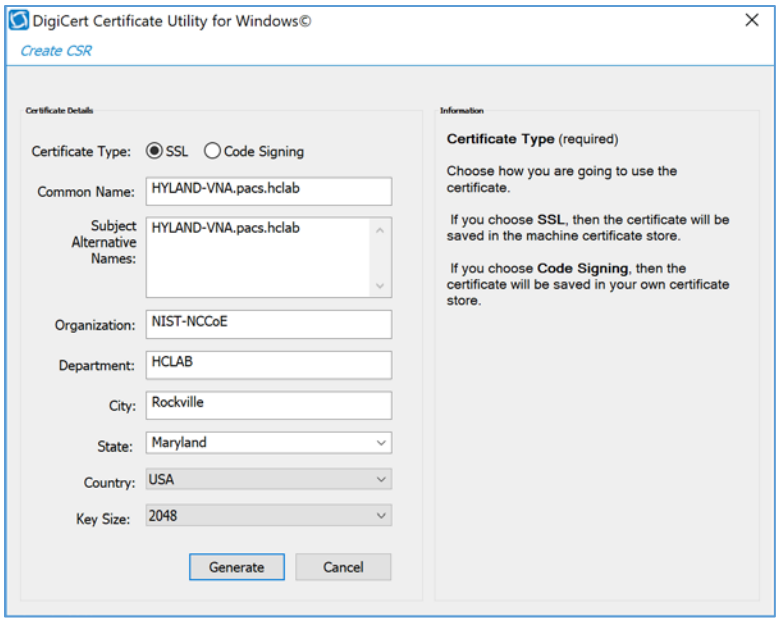
The instructions below describe the process used to obtain an SSL certificate on behalf of medical devices using the DigiCert certificate signing services.

Create CSR

A CSR is represented as a block Base64 encoded PKCS#10 binary format text that will be sent to a CA for digital signature when applying for an SSL Certificate. The CSR identifies the applicant's distinguished common name (domain name), organization name, locality, and country. It also contains the applicant's private key and the public key pair. The CSR is usually generated from the device where the certificate will be installed, but it can also be generated using tools and utilities on behalf the device to generate a CSR. Below is an instruction on how to use the Certificate Utility for Windows (*DigiCertUtil.exe*) provided by DigiCert to generate CSRs for a medical device or a server.

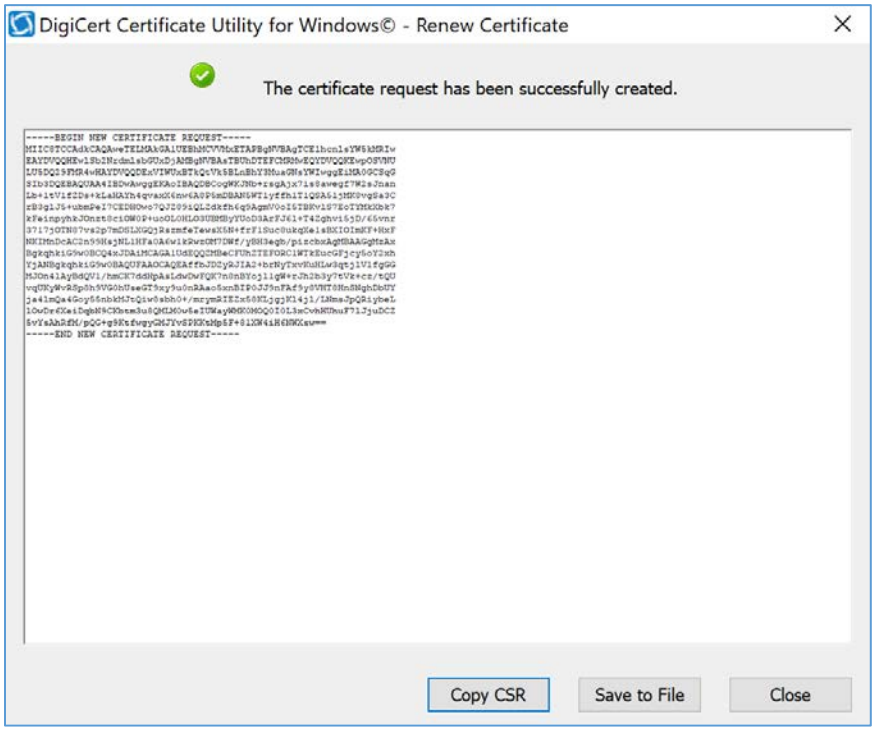
Download and save the *DigiCertUtil.exe* from the DigiCert site [14].

1. Double-click DigiCertUtil.exe to run the utility.
2. Click the **Create CSR** link to open a CSR request window.
3. On the Create CSR window, fill in the key information (some of the information is optional).
   - **Certificate Type**: Select SSL
   - **Common Name**: HYLAND-VNA.pacs.hclab
   - **Subject Alternative Names**: HYLAND-VNA.pacs.hclab
   - **Organization**: NIST-NCCoE
   - **Department**: HCLAB
   - **City**: Rockville
   - **State**: Maryland
   - **Country**: USA
   - **Key Size**: 2048
4. Click **Generate** to create a CSR. This will also generate a corresponding private key in the Windows computer from which the CSR is requested. The Certificate Enrollment Request is stored under *Console Root\Certificates(Local Computer)\Certificate Enrollment Requests\Certificates*.



1382

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



1384

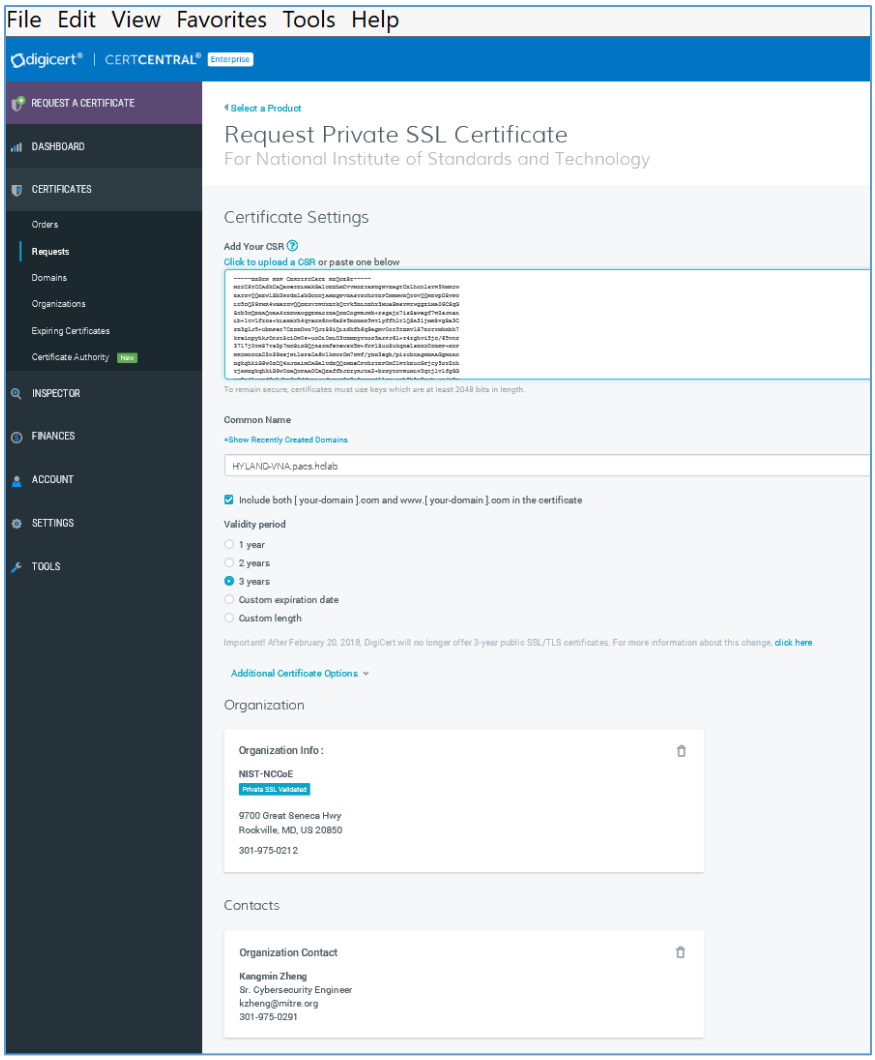
1385 6. Select and copy the certificate contents to the clipboard or save it to an ascii text file. The text
1386 contents will be used to paste into the DigiCert order form.

7. **Issue Signed Certificates**. With a created applicant CSR, request a signed certificate using DigiCert **CertCentral** portal, using these steps:

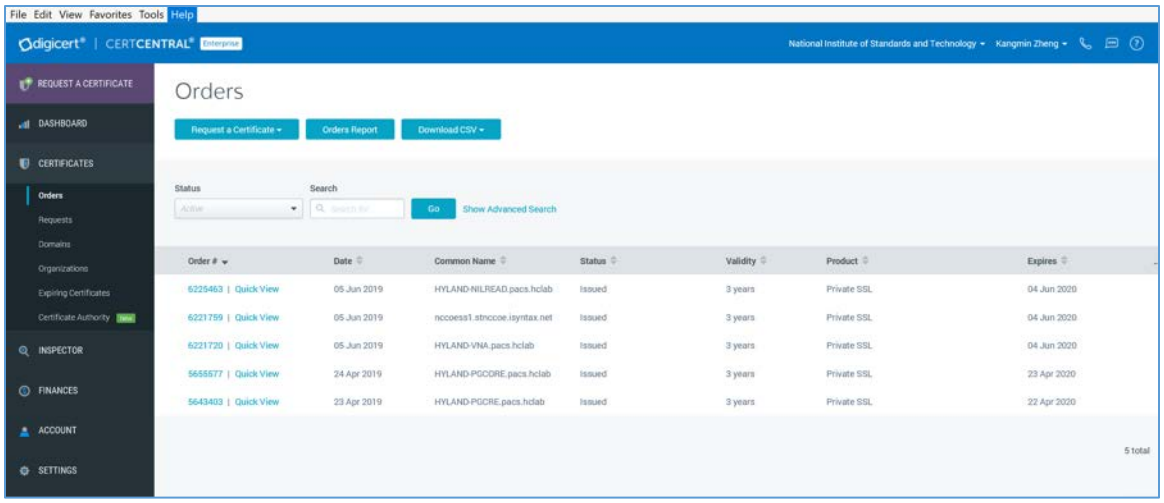
    a. Log in to a DigiCert Dashboard (https://www.digicert.com/account/login.php) with your account username and password. In the portal, select **CERTIFICATES>Requests,** then navigate to **Request a Certificate,** select **Private SSL** to open a certificate request form.

    b. Paste the CSR information to the area called **Add Your CSR**, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags. Once the pasting is done, some of the fields will be populated automatically.

    c. After filling in all the required information, scroll down to the bottom of the page, and select the **I Agree to the Certificate Services Agreement Above** checkbox. Next, click the **Submit Certificate Request** button at the bottom of the form to submit the certificate for signing approval.



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



9. Click a specific order number to display the certificate details with a list of actions that can be performed. Click **Download Certificate As** to download certificates with signed CA and Root CA certificates. A variety of certificate formats can be downloaded, such as .crt, .p7b, .pem, etc.

10. Save the downloaded certificate in a location where it can be used for further processing if needed.

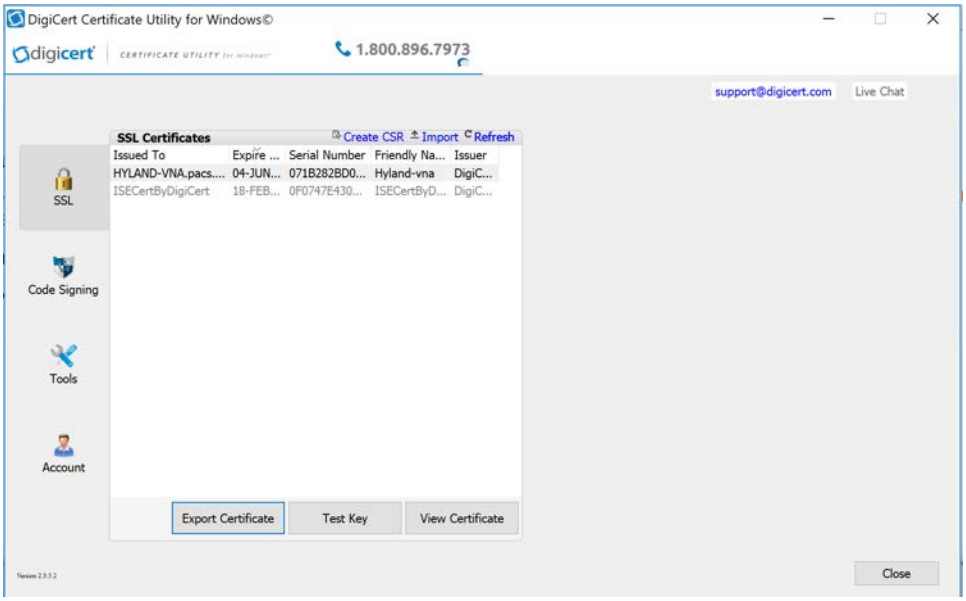
Import and Export the Signed Certification

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

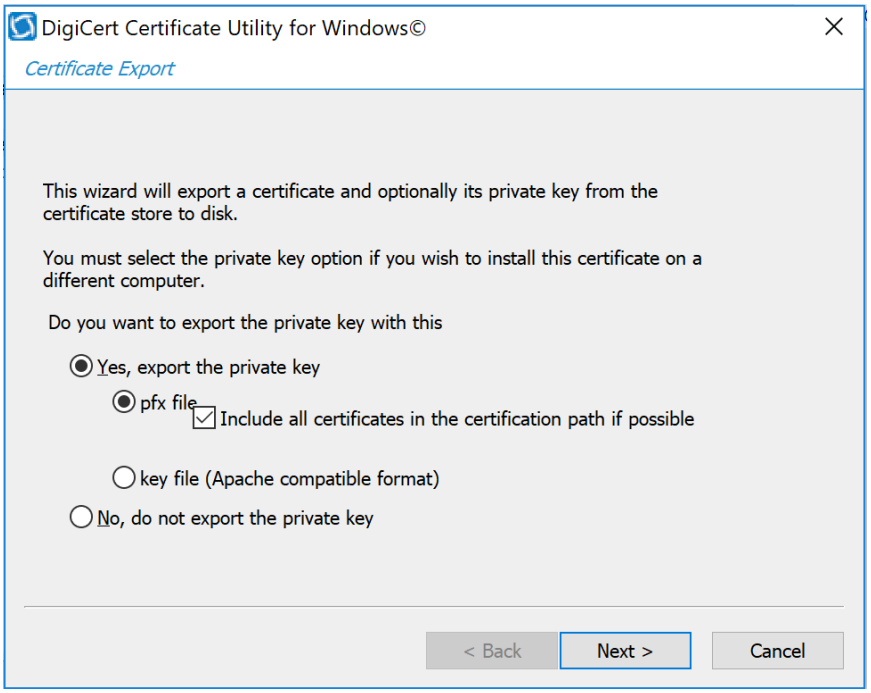
1. From the DigiCert Certificate Utility for Windows, click the **Import** button to load the downloaded signed Certificate file to the utility. The downloaded file was saved in Step 10 of Section 2.6.2. Click the **Next** button to import.

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

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



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



2.7 Network Control & Security

2.7.1 Cisco Firepower

Cisco Firepower, consisting of Cisco Firepower Management Center and Cisco Firepower Threat Defense, is a network management solution that provides firewall, intrusion prevention, and other networking services. For this project, Firepower was used to provide network segmentation and both internal and external routing. Access control and intrusion prevention policies were also implemented.

Cisco Firepower Management Center Appliance Information

CPU: 8

RAM: 16 GB

Storage: 250 GB (Thin Provision)

Network Adapter 1: VLAN 1201

Operating System: Cisco Fire Linux

Cisco Firepower Management Center Virtual Installation Guide

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

Cisco Firepower Threat Defense Appliance Information

CPU: 8

RAM: 16 GB

Storage: 48.5 GB (Thin Provision)

Network Adapter 1: VLAN 1201

Network Adapter 2: VLAN 1201

Network Adapter 3: VLAN 1099

Network Adapter 4: VLAN 1099

Network Adapter 5: Trunk Port

Network Adapter 6: Trunk Port

Network Adapter 7: VLAN 1101

Network Adapter 8: VLAN 1101

Network Adapter 9: VLAN 1701

Operating System: Cisco Fire Linux

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

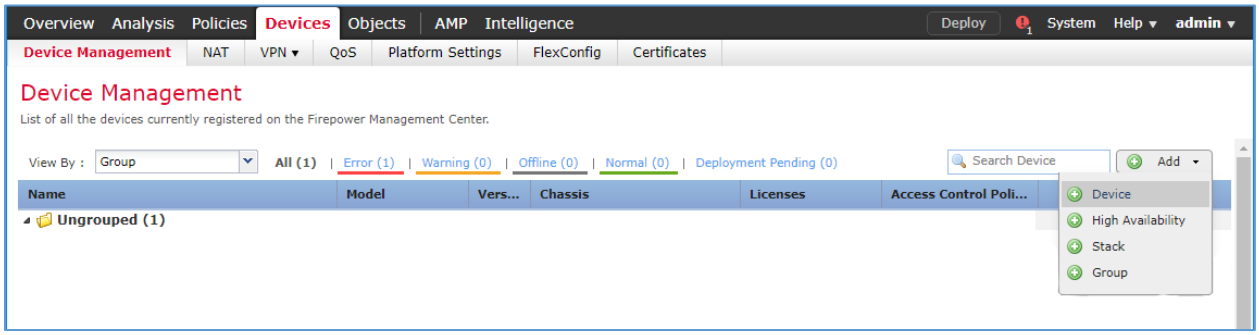
1452 Install the Cisco Firepower Threat Defense Virtual appliance, according to the instructions detailed at
1453 Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide [16].

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.

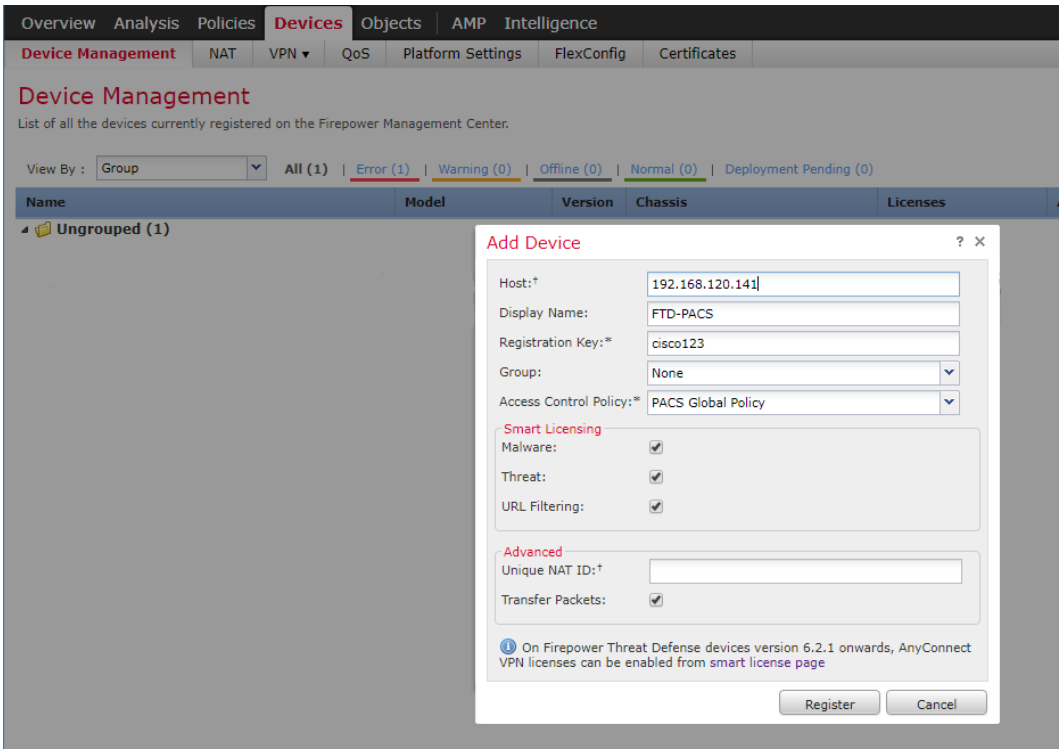
1464 b. Select Block All Traffic.

1465 c. Click Save.

1466 8. Under **Smart Licensing**, check the boxes next to **Malware**, **Threat**, and **URL**.

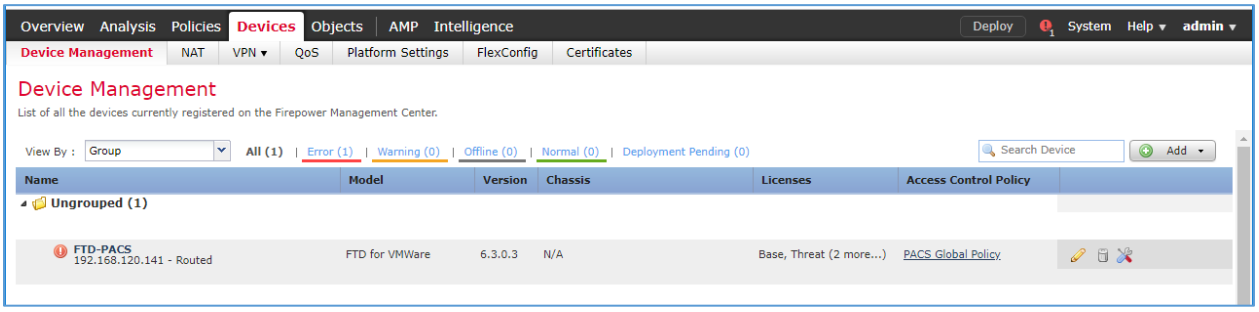
1467 9. Under **Advanced** check the box next to **Transfer Packets**.

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**

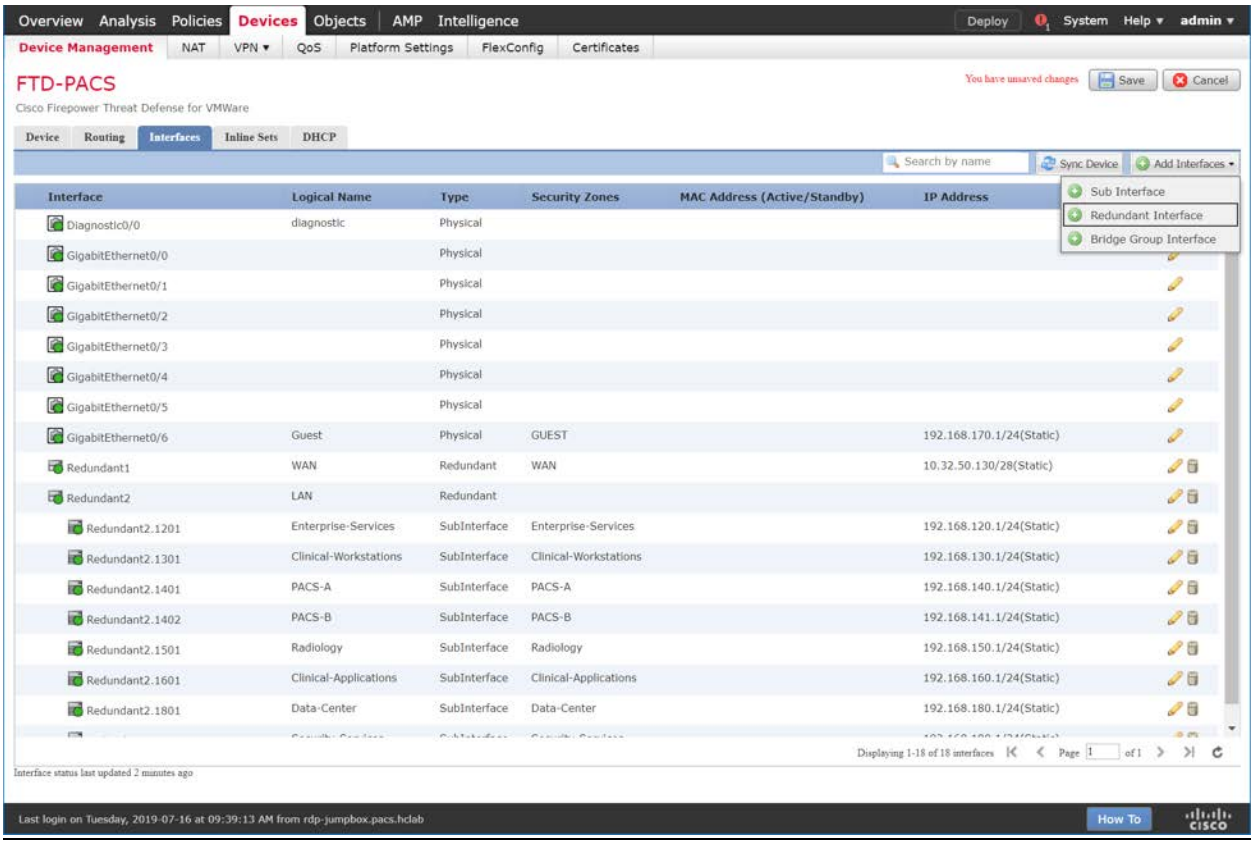
1473 Each physical interface connected to the Cisco FTD will appear in the FMC device management section
1474 under the interface tab. In order to configure the eight subnets needed for the PACS architecture while
1475 also allowing for management, diagnostic, and Wide Area Network (WAN) traffic, we 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.

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**.



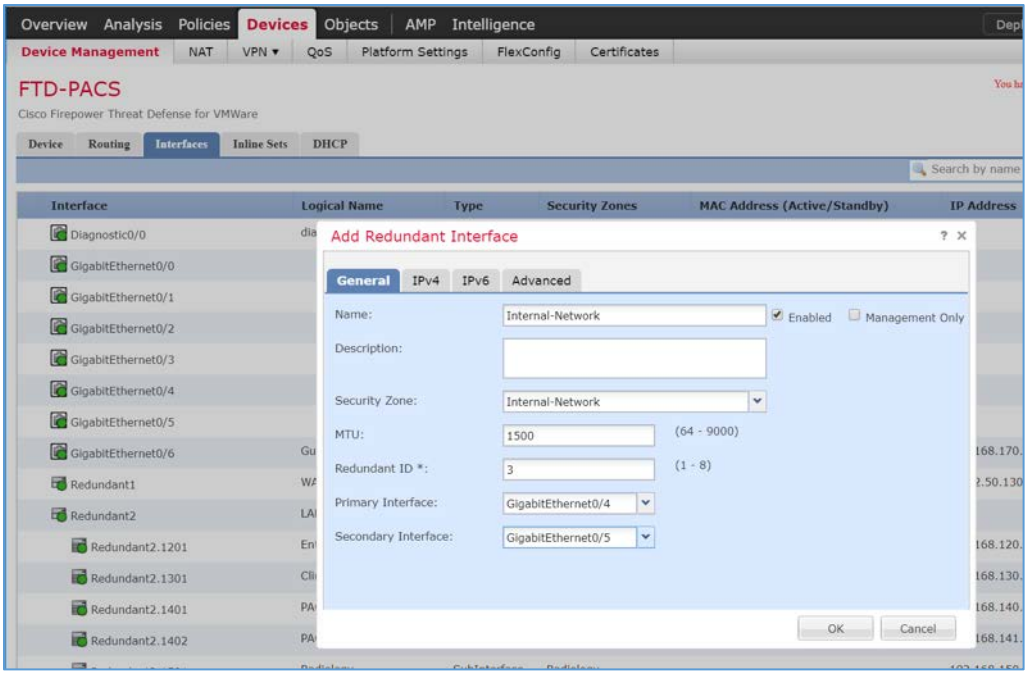
1484

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.

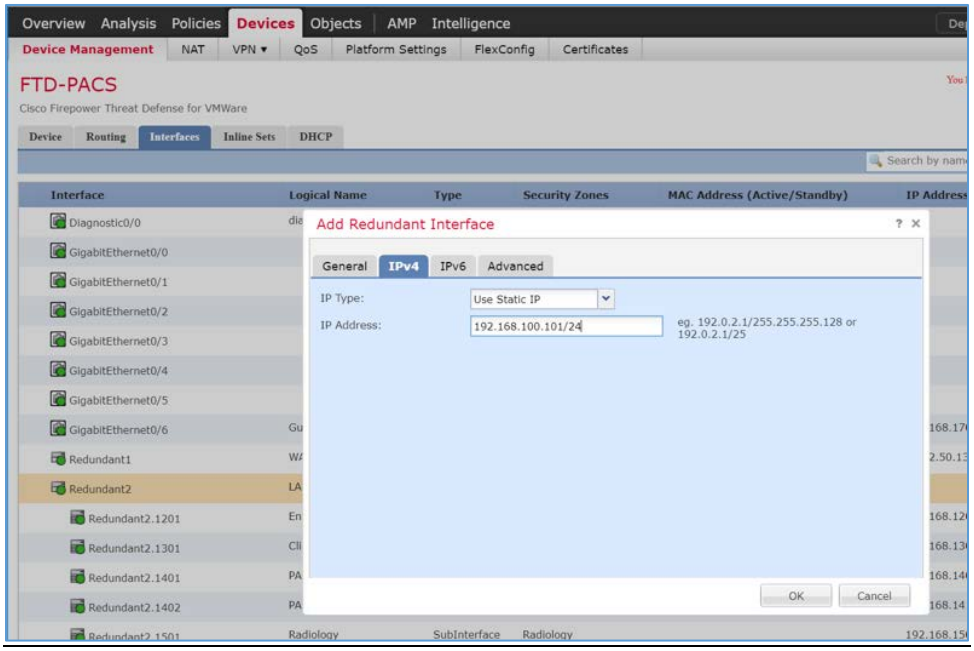


1489

1490 9. Navigate to the **IPv4** tab.

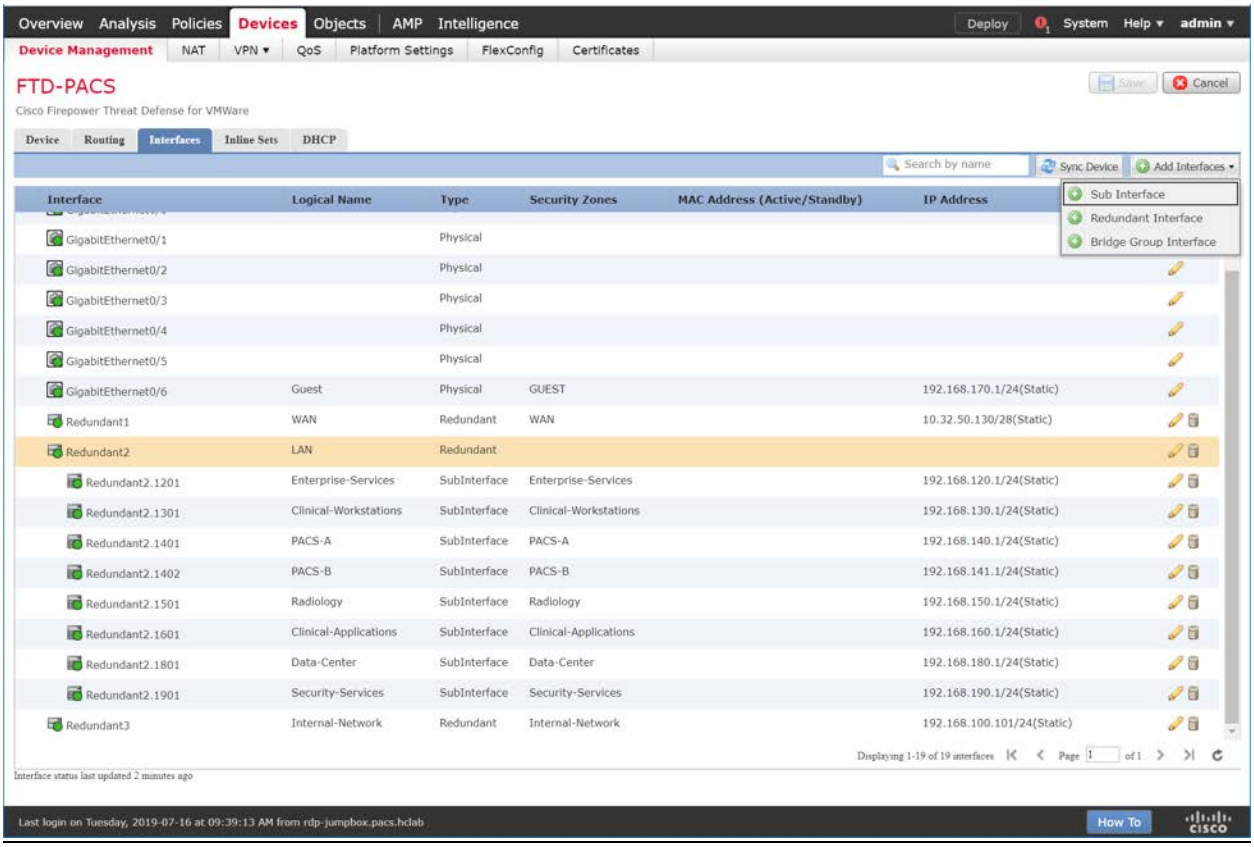
1491 10. Assign an **IP address** and **netmask** (e.g., **192.168.100.101/24**) to the interface.

1492 11. Click **OK**.



1493

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



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

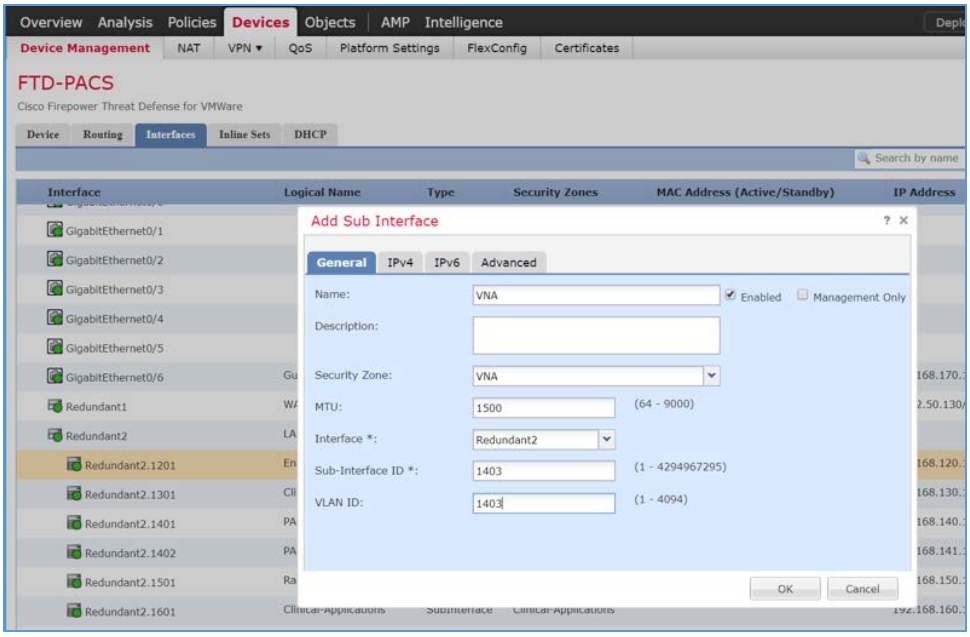
14. Create and/or add a **security zone**, **VNA**, to the sub interface.

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

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

16. Assign **1403** as the **Sub Interface ID** to the sub interface.

17. Assign **1403** as the **VLAN ID** to the sub interface.

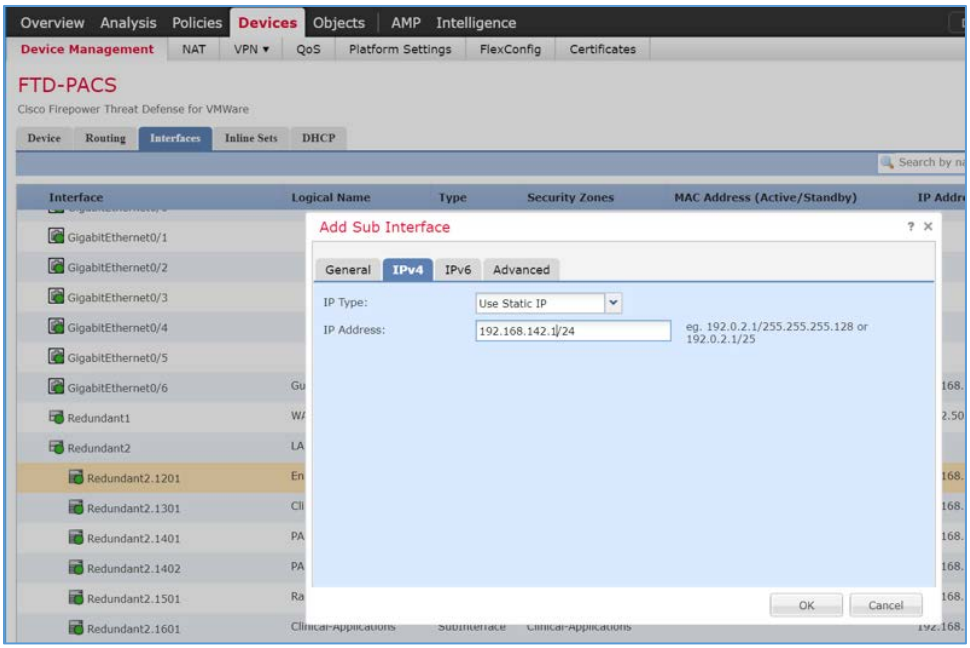


1504

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

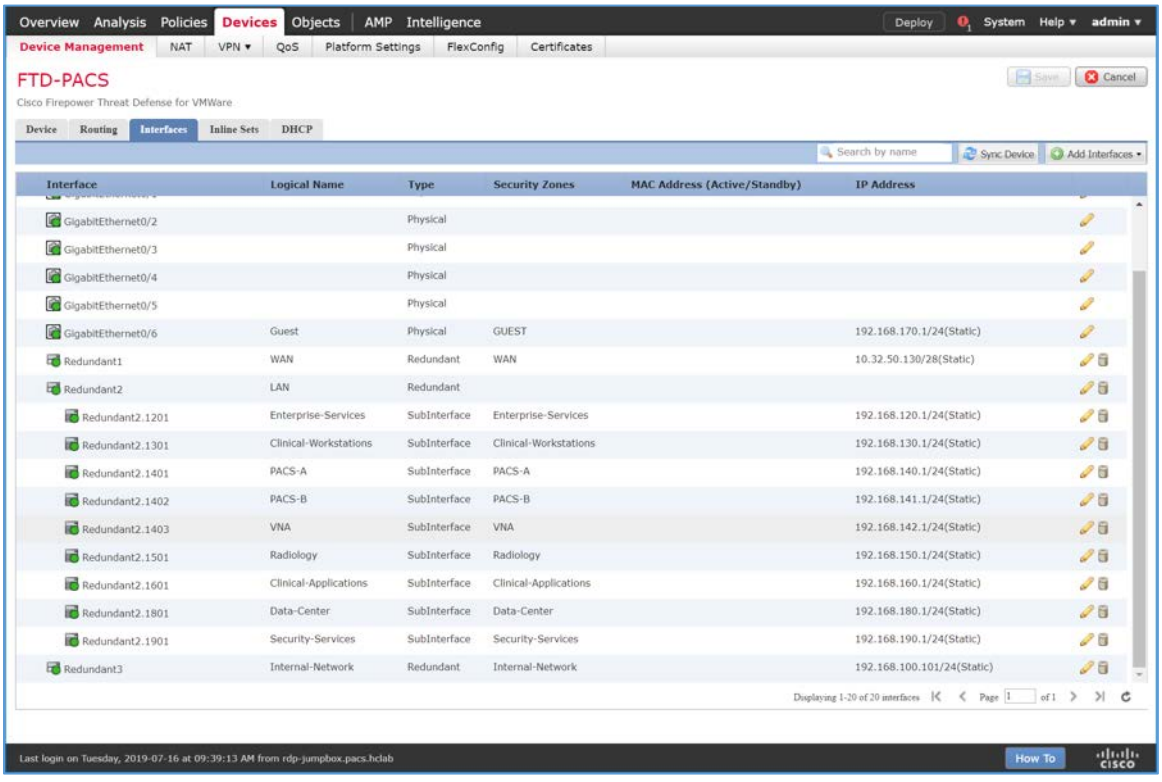
1506 19. Assign an **IP address** and **netmask** (e.g., **192.168.142.1/24**) to the sub interface.

1507 20. Click **OK**.



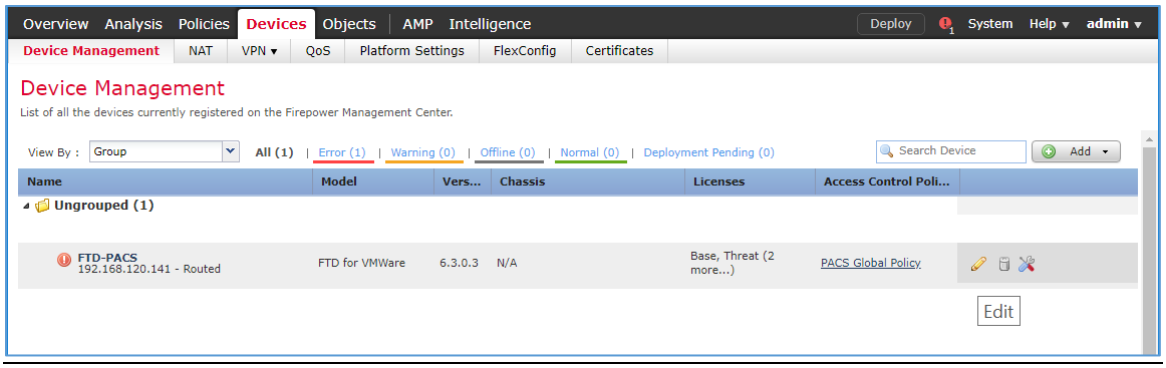
1508

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



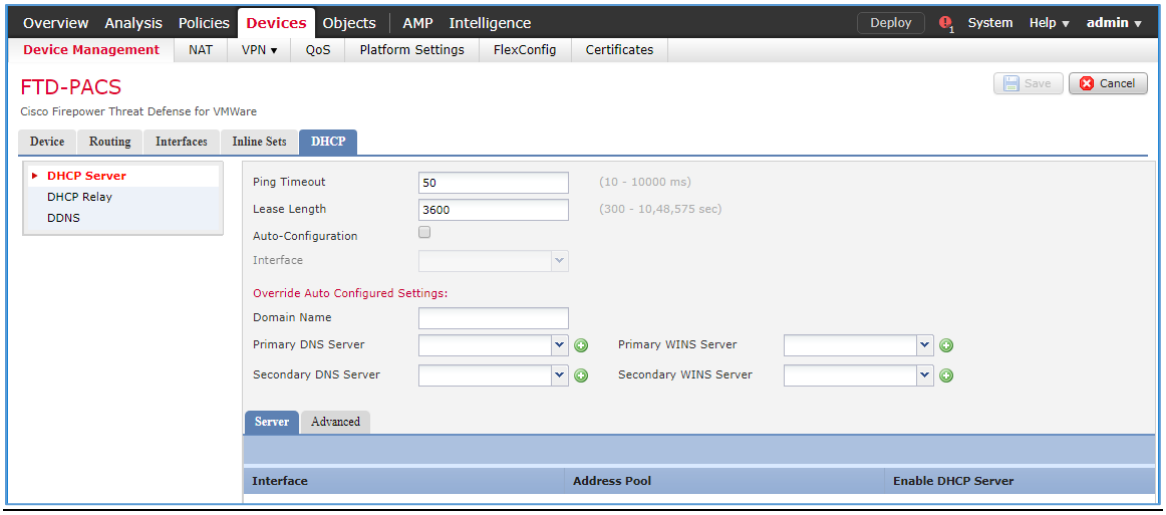
DHCP Relay Through Cisco Firepower Management Center Configuration

1. Log in to the **FMC Console**.
2. Navigate to **Devices > Device Management**.
3. Find your FTD device and click the **edit** icon.



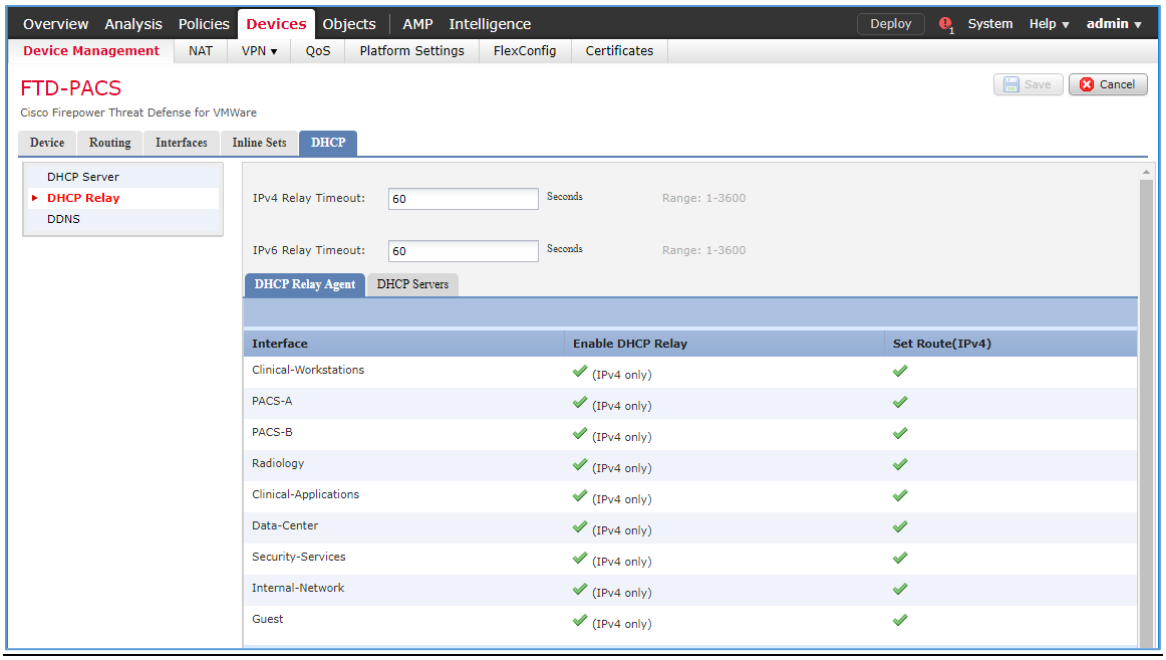
1518

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



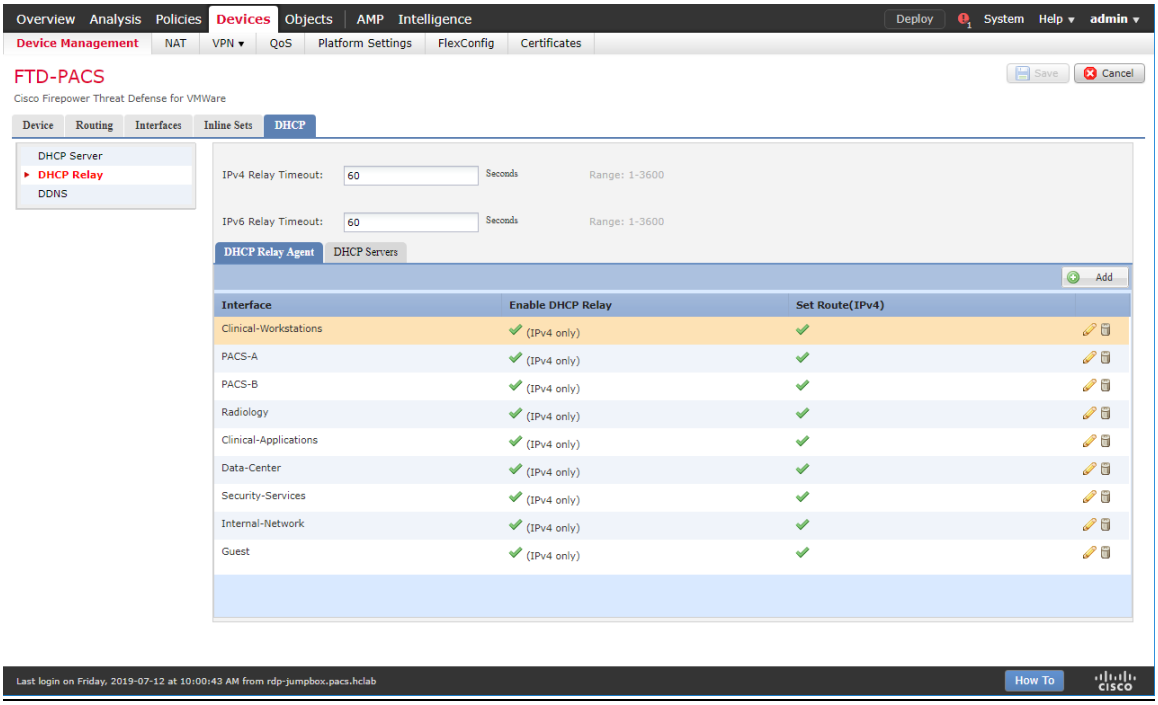
1520

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



1522

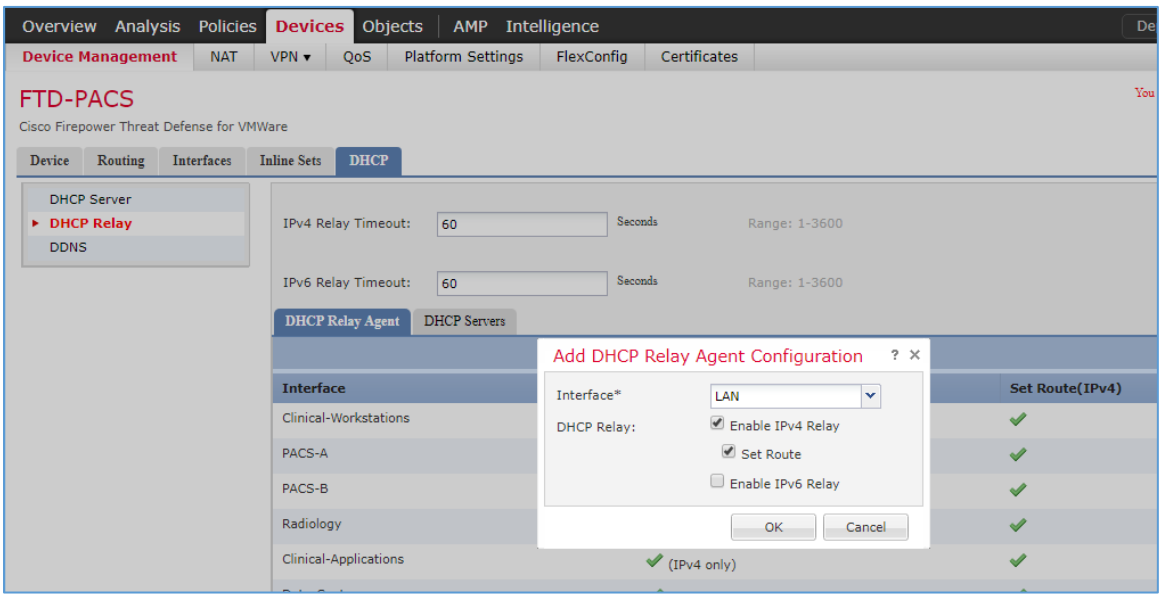
1523 6. Under **DHCP Relay Agent**, click **Add**.



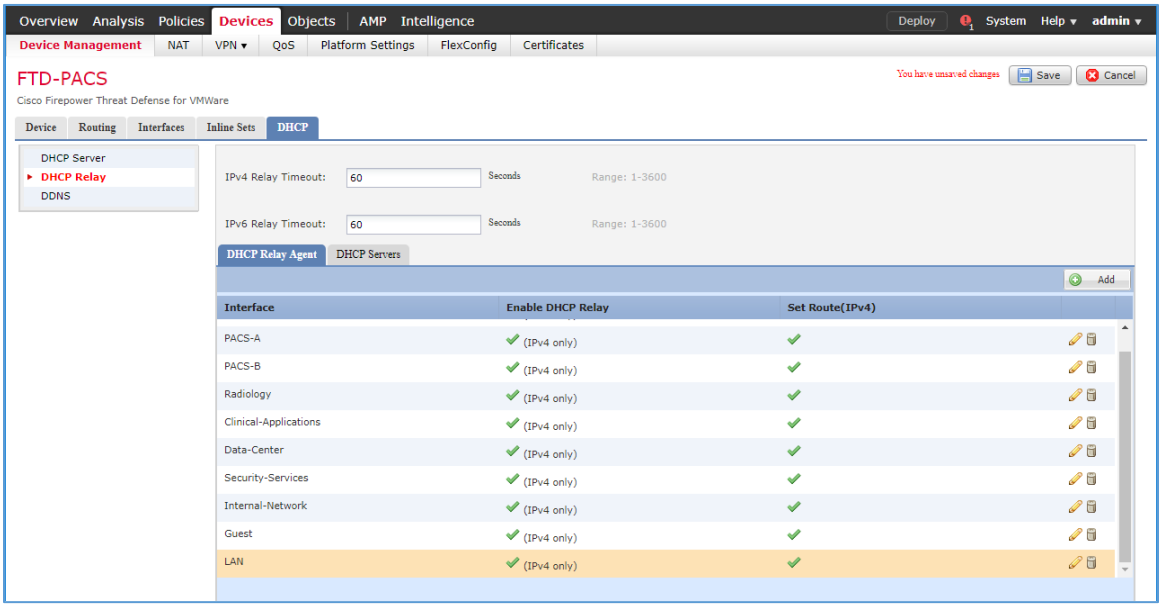
1524

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

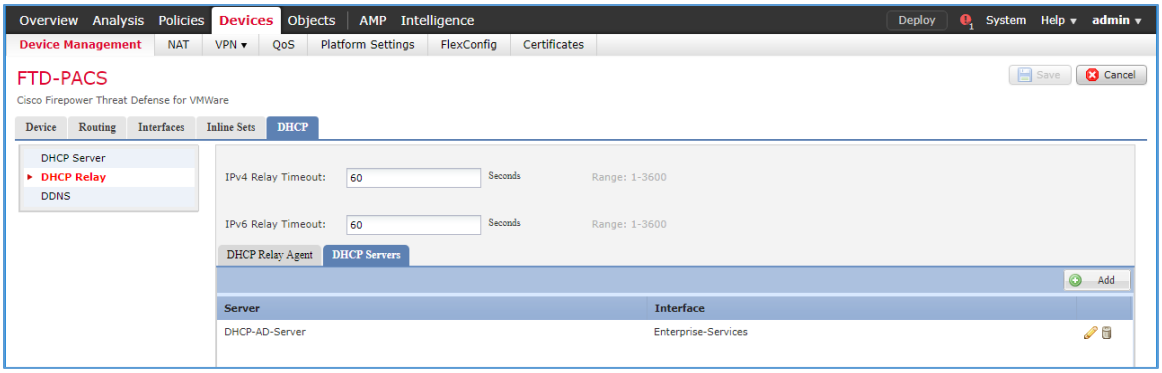
8. Check the box next to **Enable IPv4 Relay**.
9. Check the box next to **Set Route**.
10. Click **OK**.



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

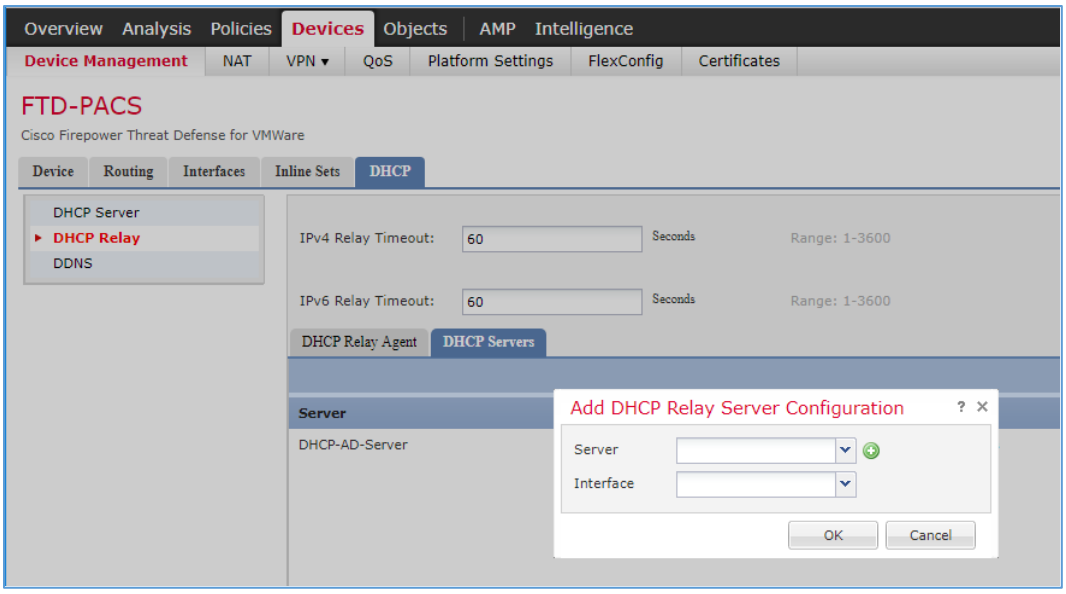


12. Under **DHCP Servers**, click **Add**.



1533

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

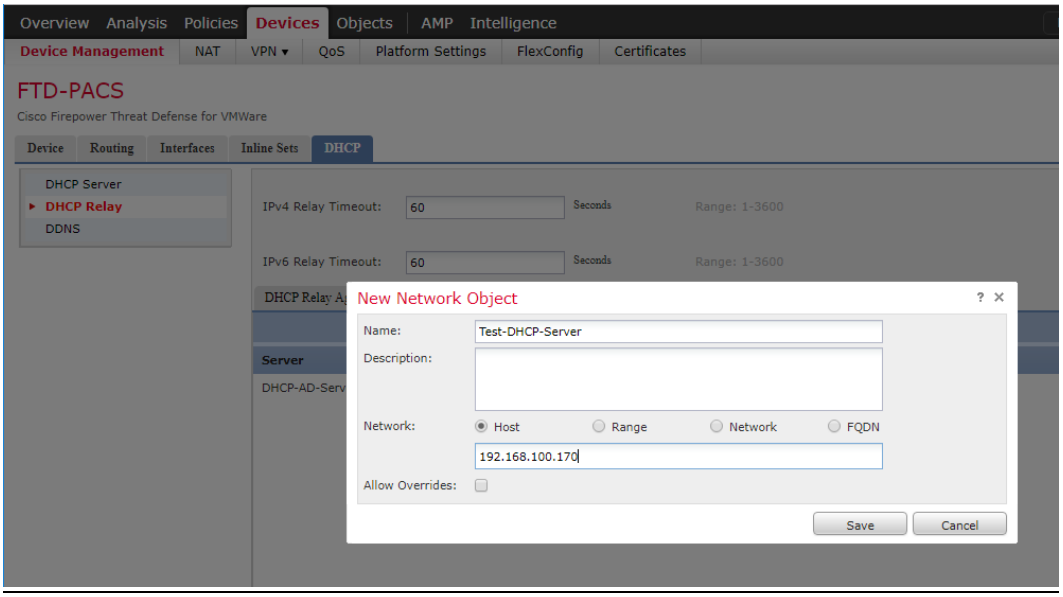


1535

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**.

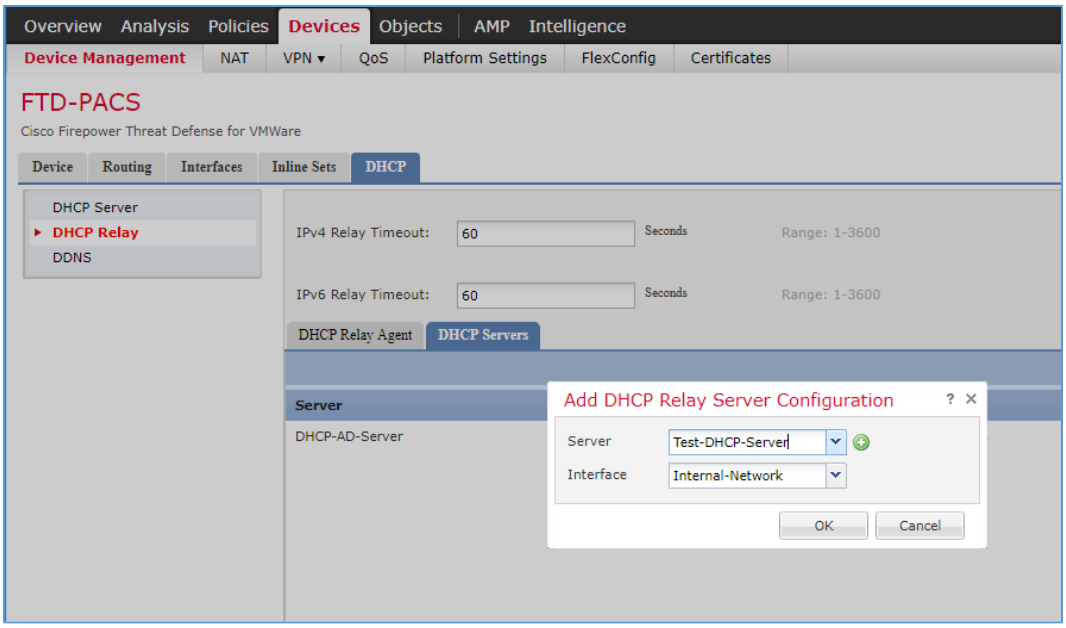


1539

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**.

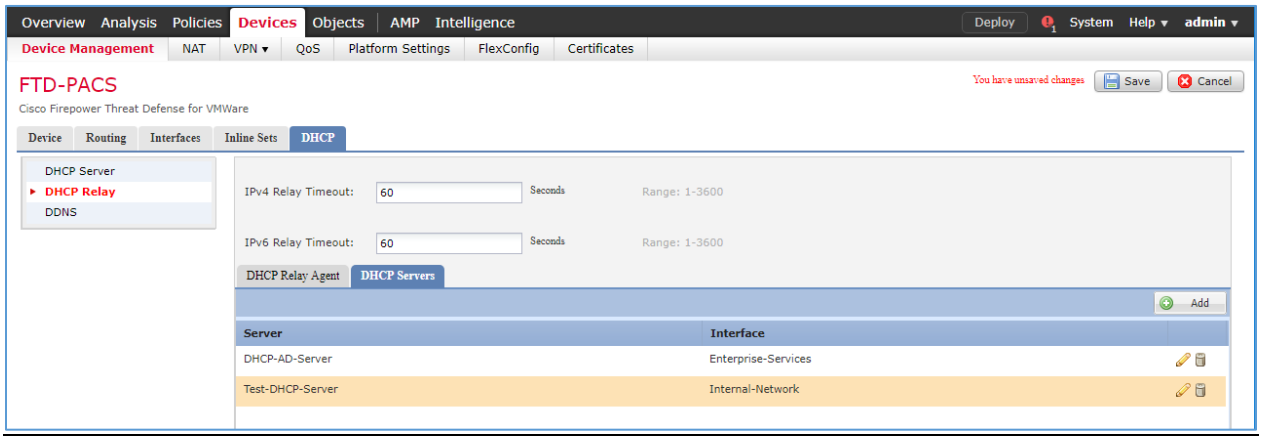


1543

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

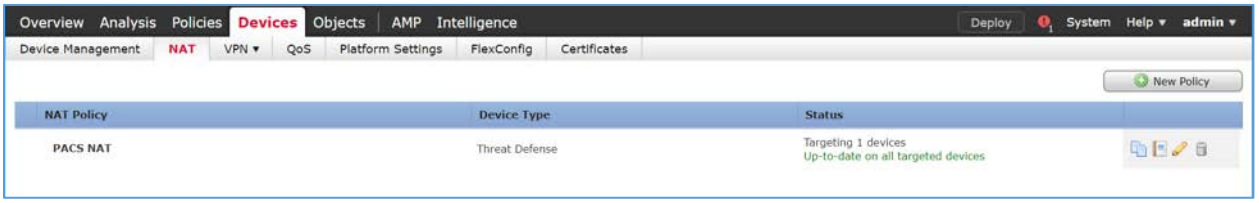
21. Click **Save**.

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

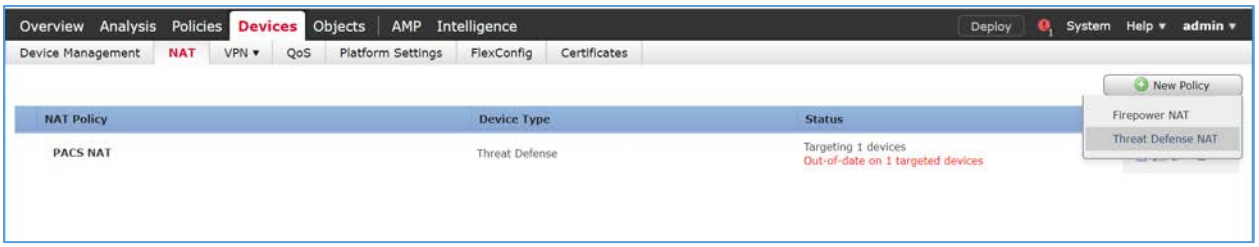


Network Address Translation (NAT) Rules Configuration

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



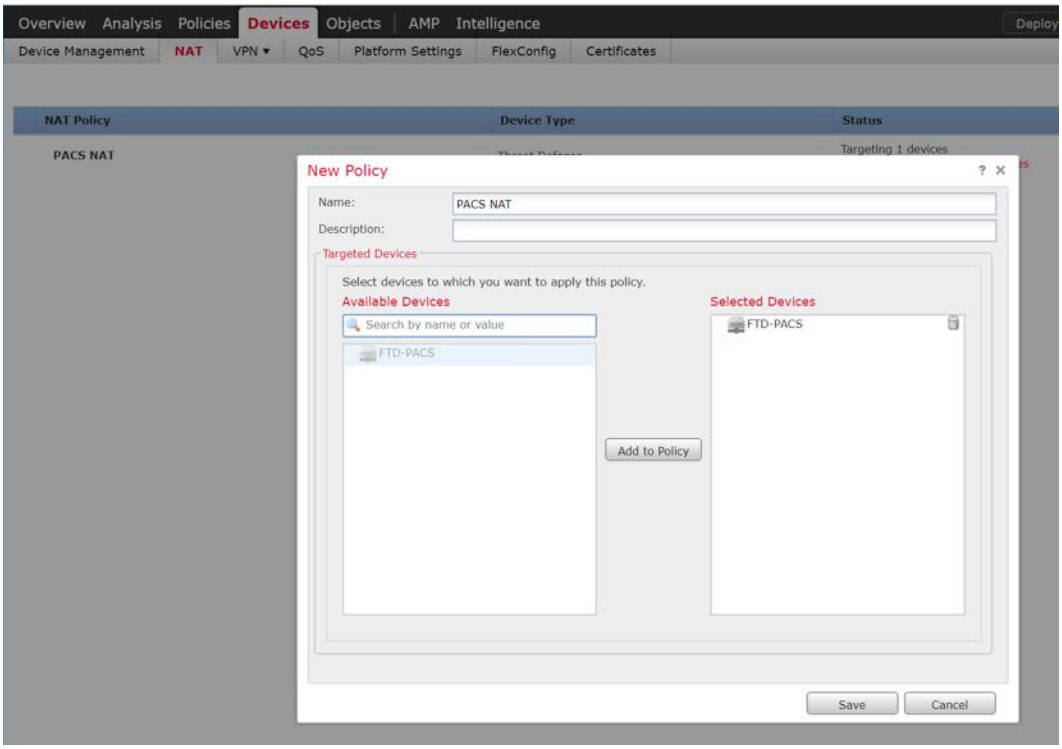
2. Click **New Policy > Threat Defense NAT**.



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

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

5. Click **Save**.



1556

1557 6. Click on the NAT policy's **edit** icon.

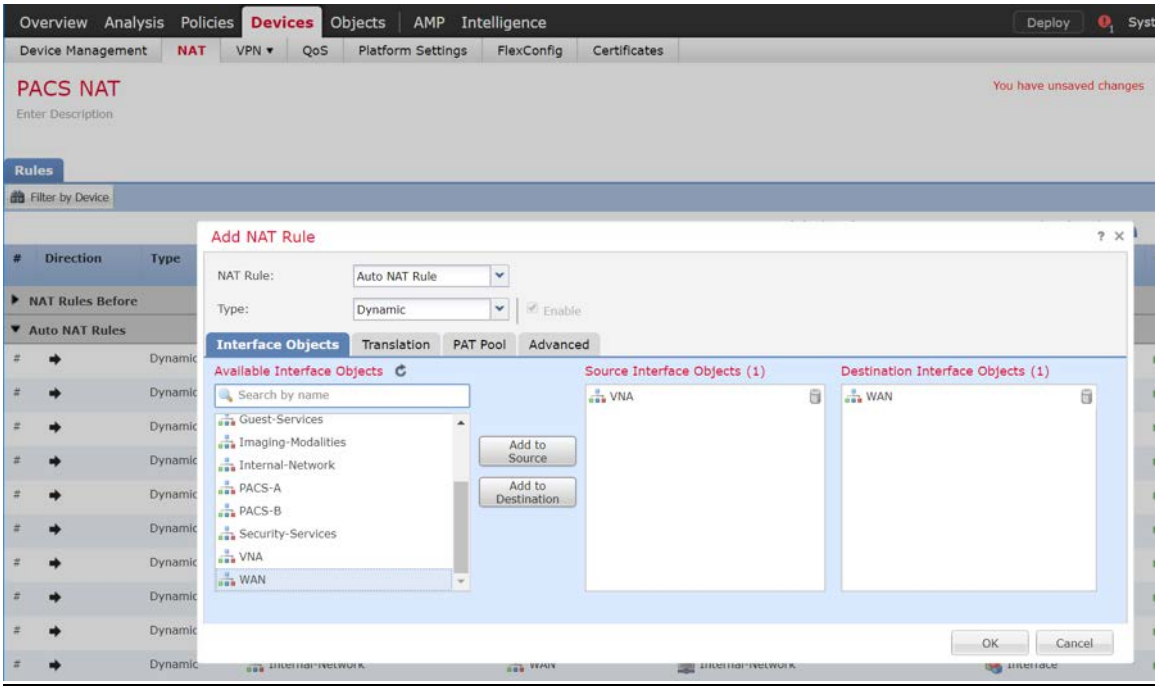
1558 7. Click **Add Rule**.

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**.

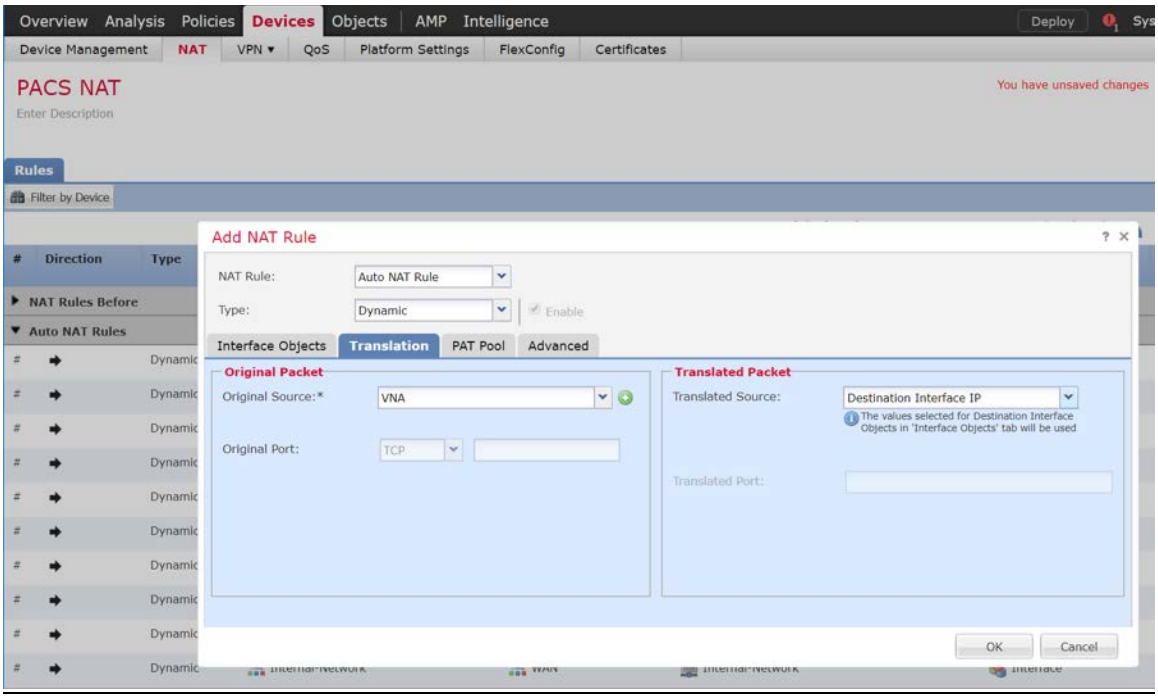


1563

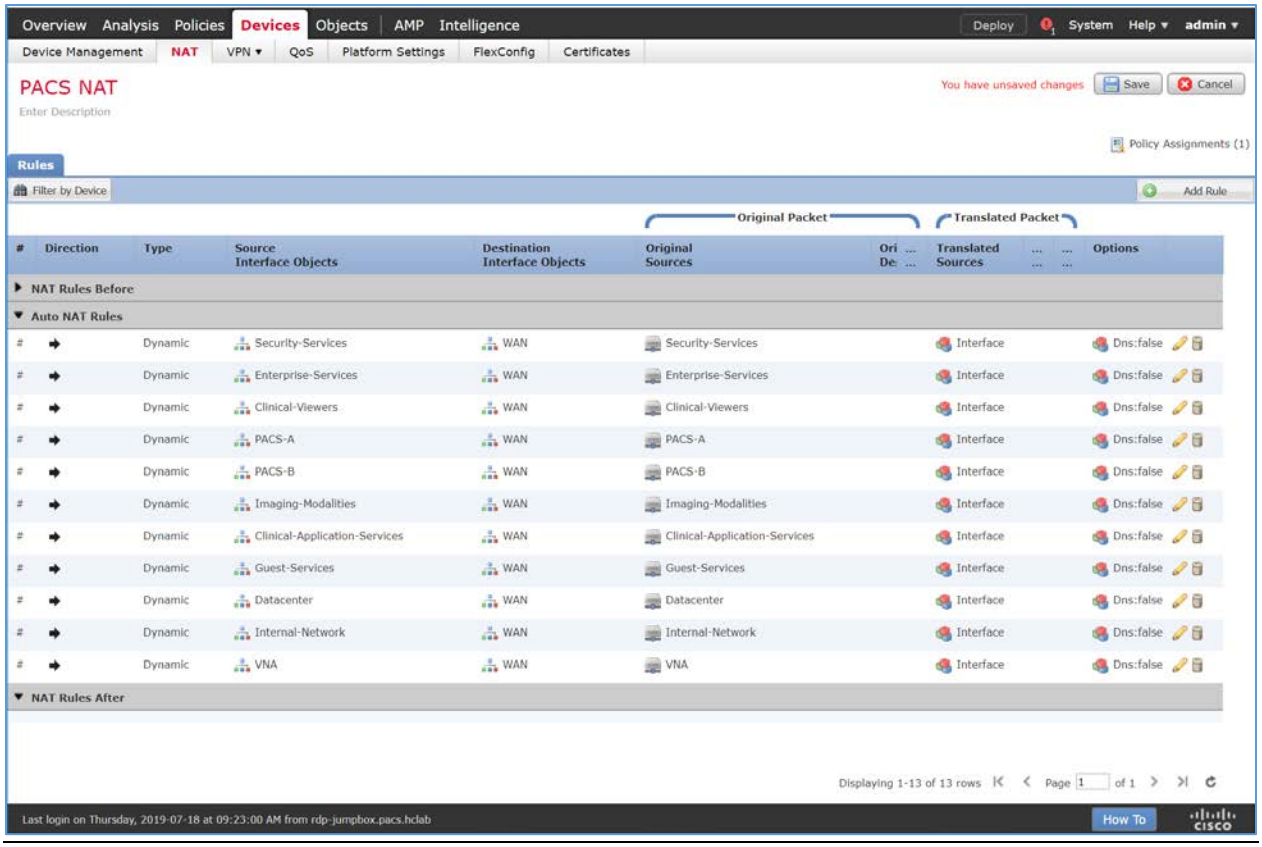
1564 12. Under **Translation**, set **Original Source** to the **network** that corresponds with the source interface
1565 object established in the previous step.

1566 13. Set **Translated Source** to **Destination Interface IP**.

1567 14. Click **OK**.



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

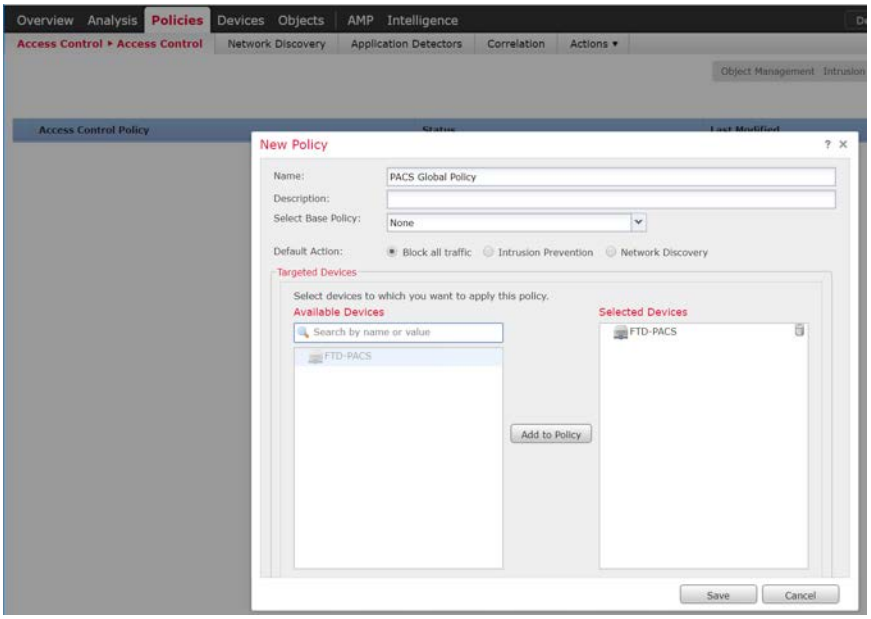


Access Control Policy Through Firepower Management Center Configuration

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

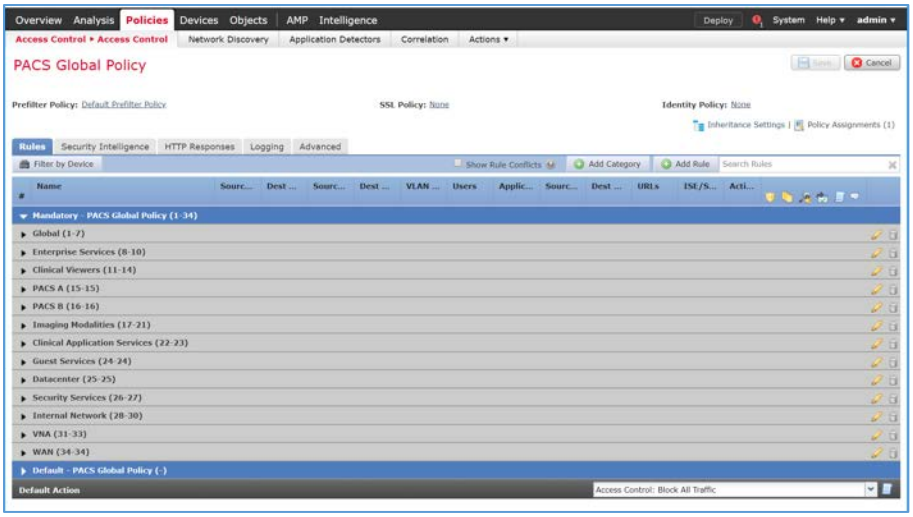
1. Navigate to **Policies > Access Control > Access Control**.

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



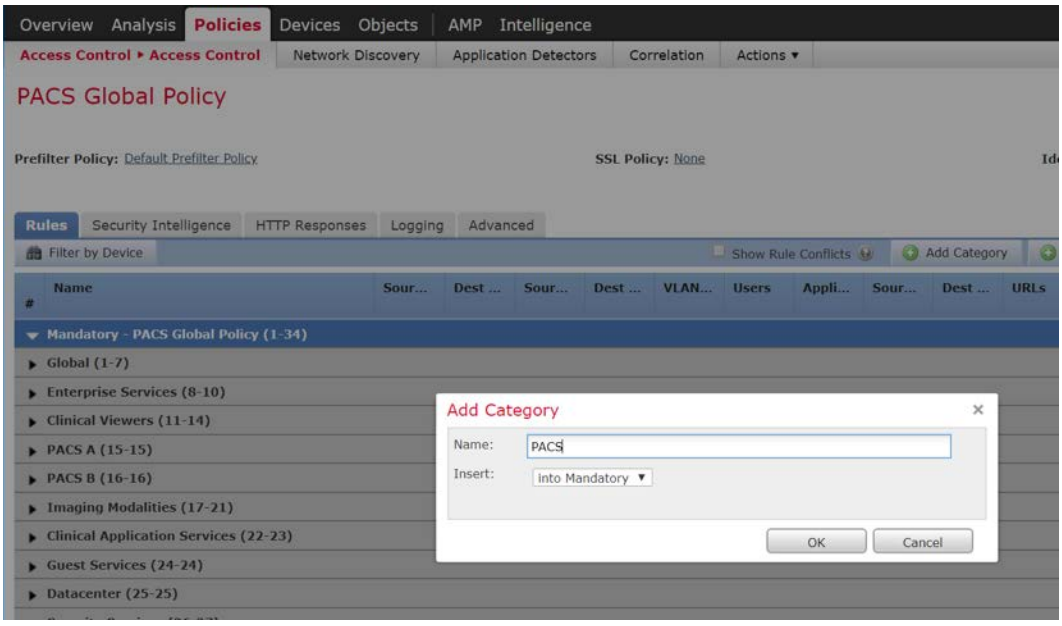
8. Click the access-control policy's **edit** icon.

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



Creating a category:

1. Click **Add Category**.
2. Enter **PACS** as the name for the category.
3. Insert the category into the **Mandatory** section.
4. Click **OK**.



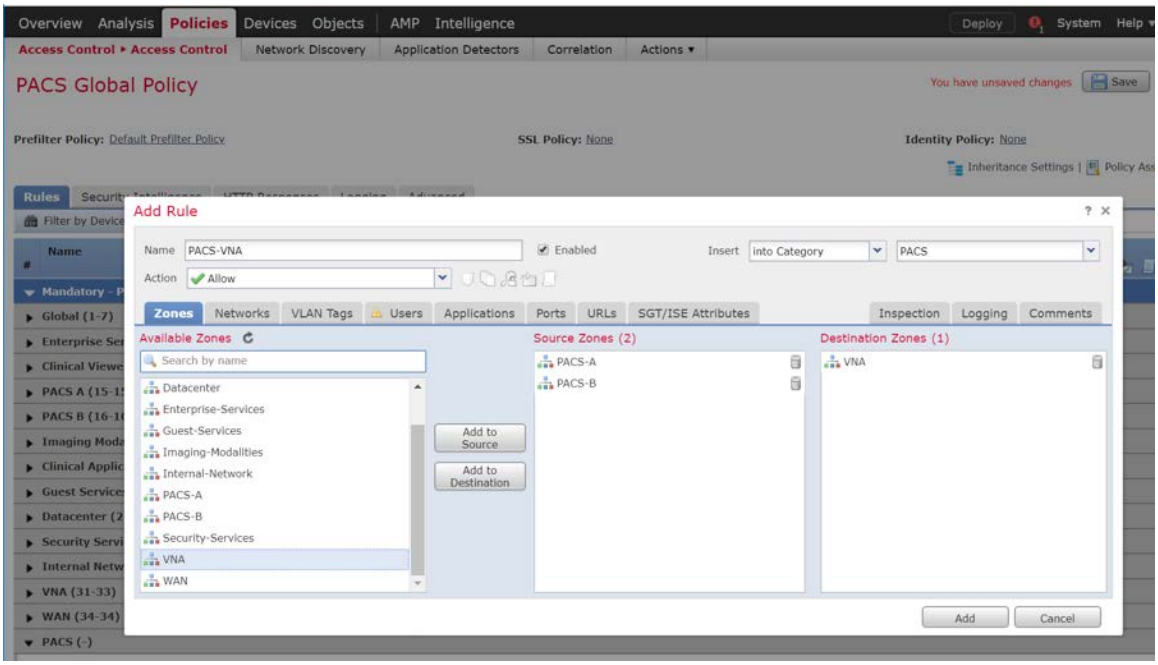
Create a rule that allows application traffic between security zones

1. Click **Add Rule.**
2. Enter **PACS-VNA** as the name for the rule.
3. Insert the rule into the category created in the previous step.
4. Set **Action** to **Allow.**

   Note: Because we set the default action to **block all traffic** when creating the policy, all of the rules we created were set to **Allow.**

5. Add security zone(s) to the **Source Zone,** and also add security zone(s) to the **Destination Zone.**

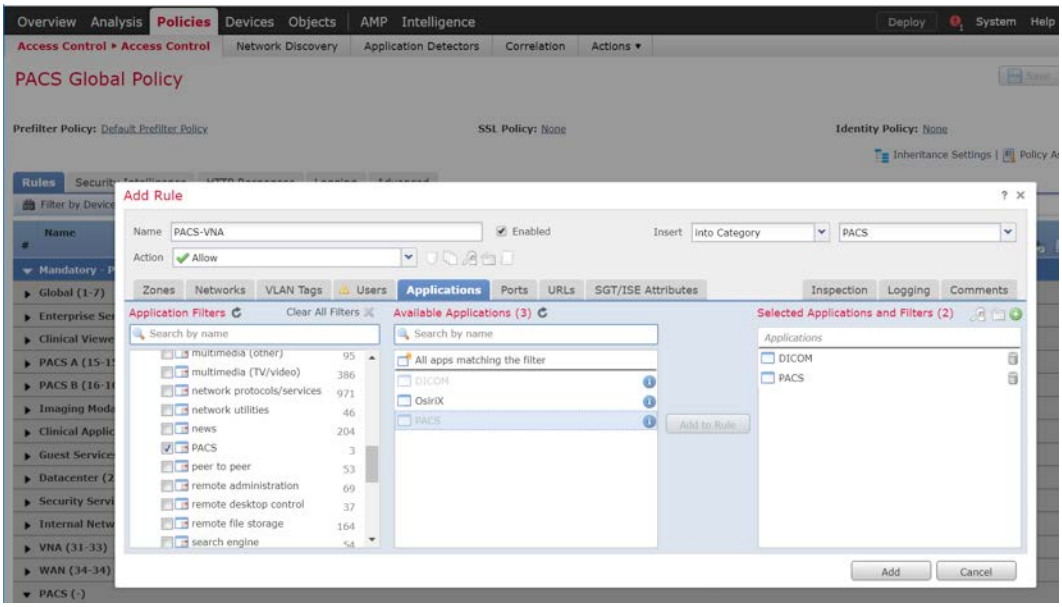
   Note: The two primary methods for adding source and destination networks to an access control rule are through security zones or networks. Security zones are objects that can contain multiple FTD interfaces. Networks can be different types of network objects, including network segments (**192.168.1.0/24**)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



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

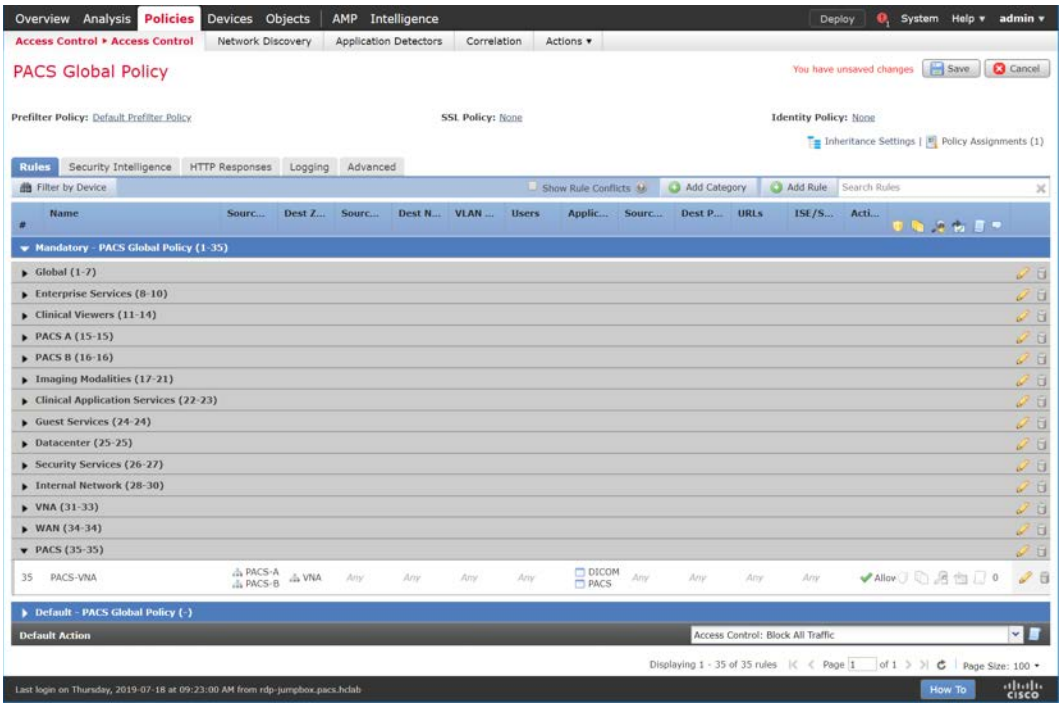
   Note: This can also be accomplished by specifying the **port** you would like to allow under the **Ports** tab. By specifying a specific port, this will open the port to all traffic regardless the type of traffic (e.g., DICOM) being sent.

7. Click **Add**.



1620

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

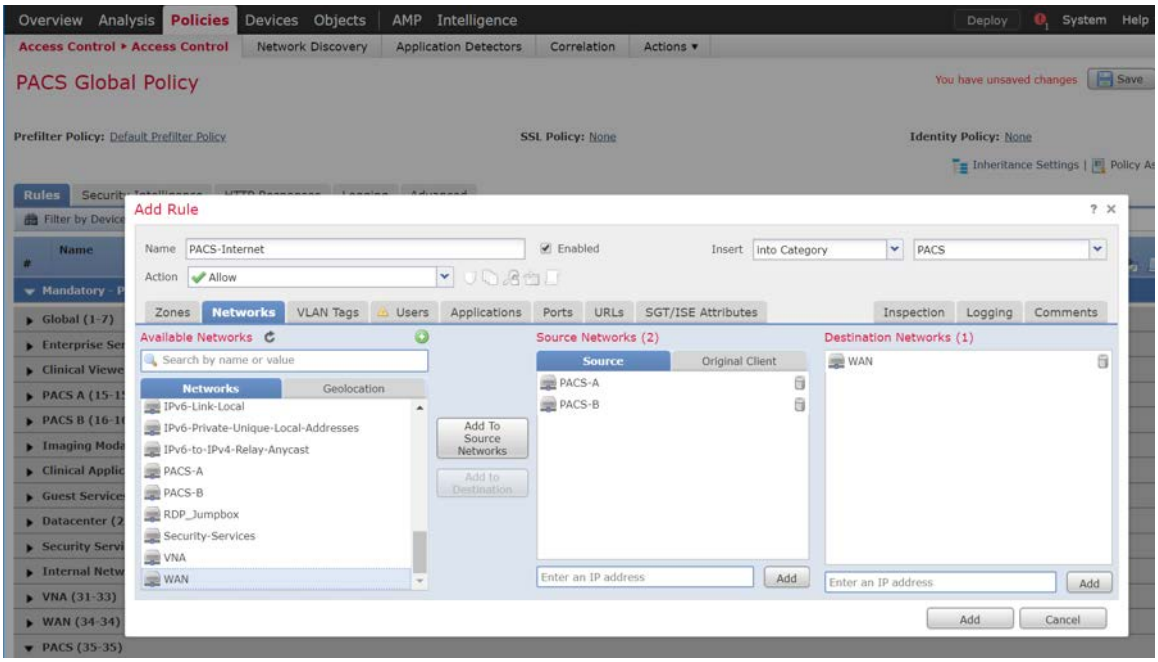


1622

1623 **<u>Create a rule that allows traffic on a specific port between networks</u>**

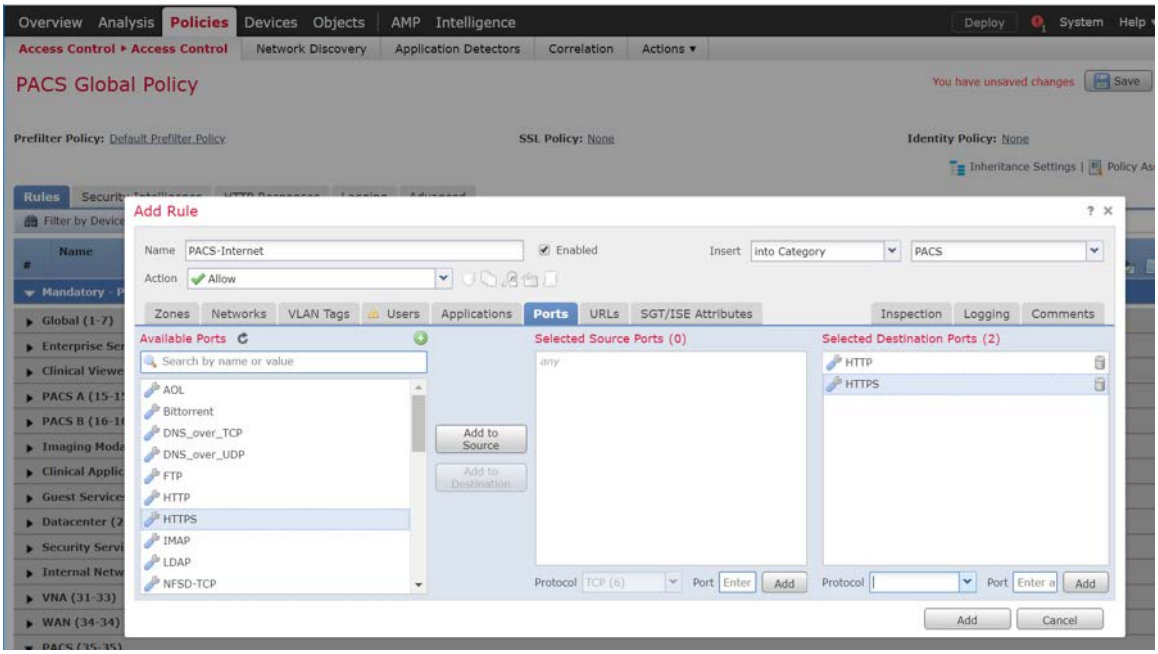
1624 1. Click **Add Rule**.

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



6. Under **Ports**, add a port(s) to the **Selected Destination Ports**.

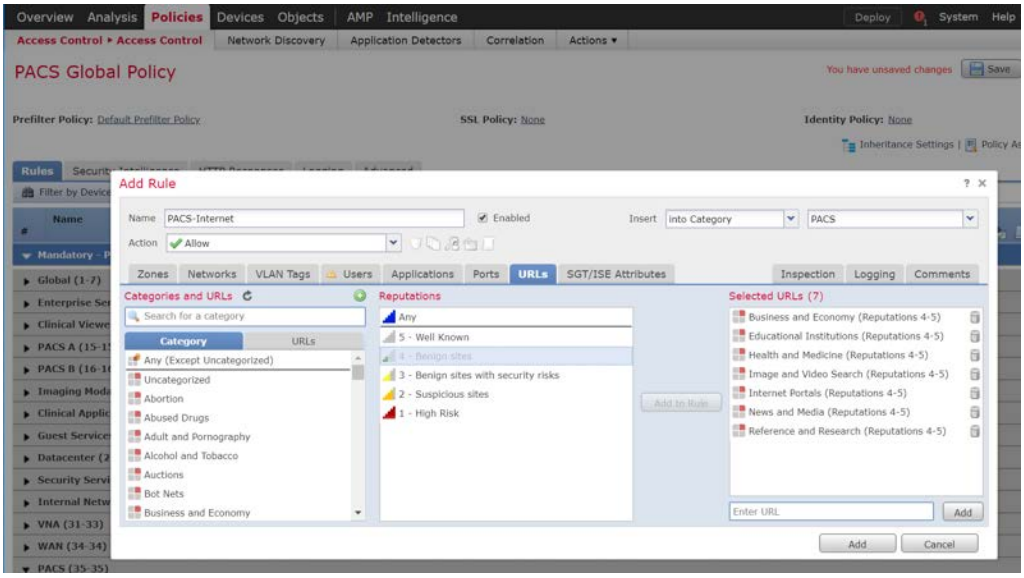
Note: Select from a group of pre-created ports or add your own port by filling out the **protocol** and **port** boxes, then click **Add** under the selected destination ports.



1633

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

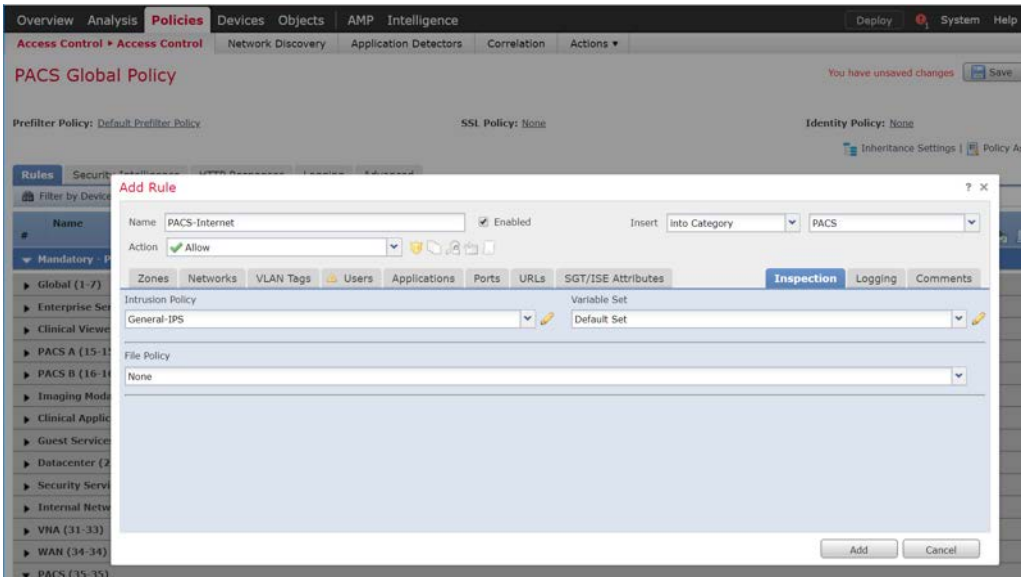
1635 Note: The URL categories are generated by Cisco Firepower and updated regularly. Within each
1636 URL category, you can specify the reputation level the URL must meet in order for the rule to
1637 match.



1638

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

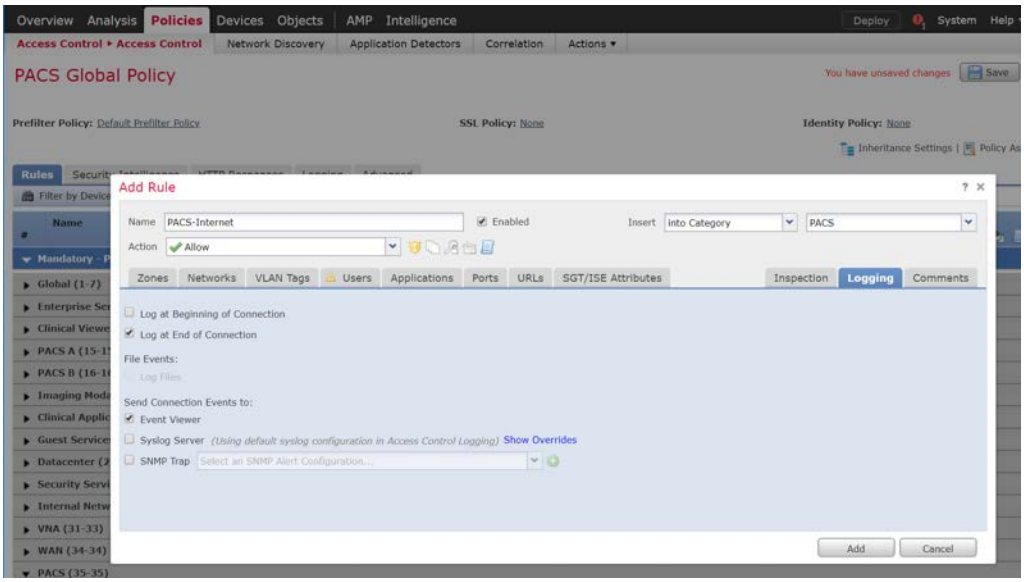
Note: Intrusion policies are created separately from the access-control policy. Once created, an intrusion policy can be applied to a specific access-control rule or an entire access-control policy. See the link posted [17] at the beginning of this section for more information on how to create and use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



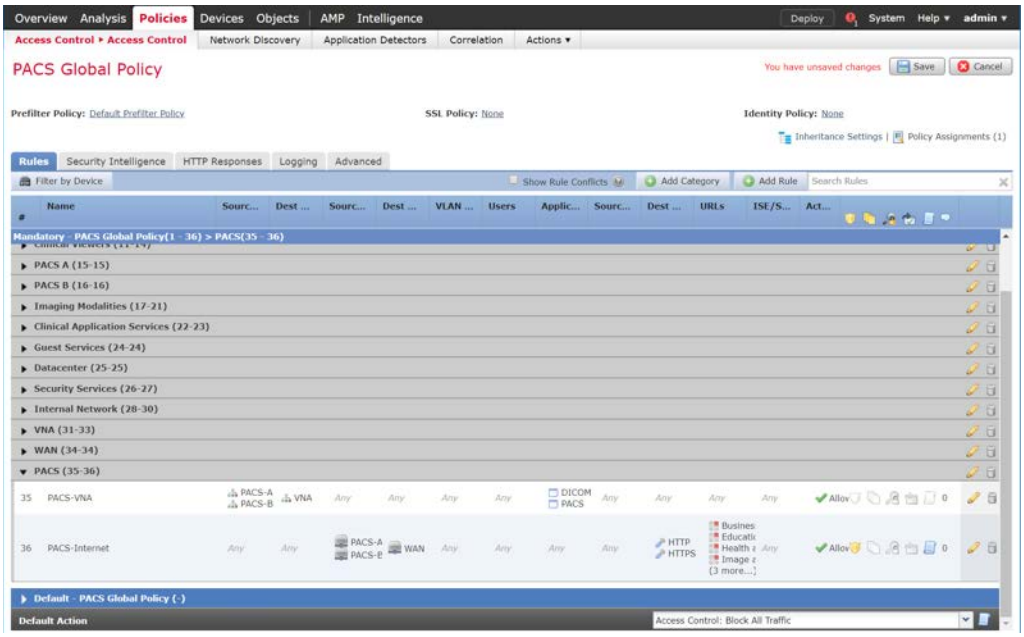
9. Under **Logging**, select **Log at End of Connection**, or leave this section blank.

Note: If logging is enabled, select **Event Viewer**.

10. Click **Add**.



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



2.7.2 Cisco Stealthwatch

Cisco Stealthwatch provides network visibility and analysis through the use of network telemetry. It provides threat detection and remediation as well as network segmentation using machine learning and behavioral modeling. This project integrates Cisco Stealthwatch with Cisco Firepower to allow Cisco FTD to send NetFlow directly to Stealthwatch for analysis.

Cisco Stealthwatch Management Console Appliance Information

CPU: 3

RAM: 16 GB

Storage: 60 GB (Thin Provision)

Network Adapter 1: VLAN 1901

Operating System: Linux

Cisco Stealthwatch Management Console Virtual Edition Installation Guide

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

Cisco Stealthwatch UDP Director Appliance Information

CPU: 1

RAM: 4 GB

Storage: 60 GB (Thin Provision)

Network Adapter 1: VLAN 1901

Network Adapter 2: VLAN 1901

Operating System: Linux

Cisco Stealthwatch UDP Director Virtual Edition Installation Guide

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

Cisco Stealthwatch Flow Collector Appliance Information

CPU: 2

RAM: 16 GB

Storage: 60 GB (Thin Provision)

Network Adapter 1: VLAN 1901

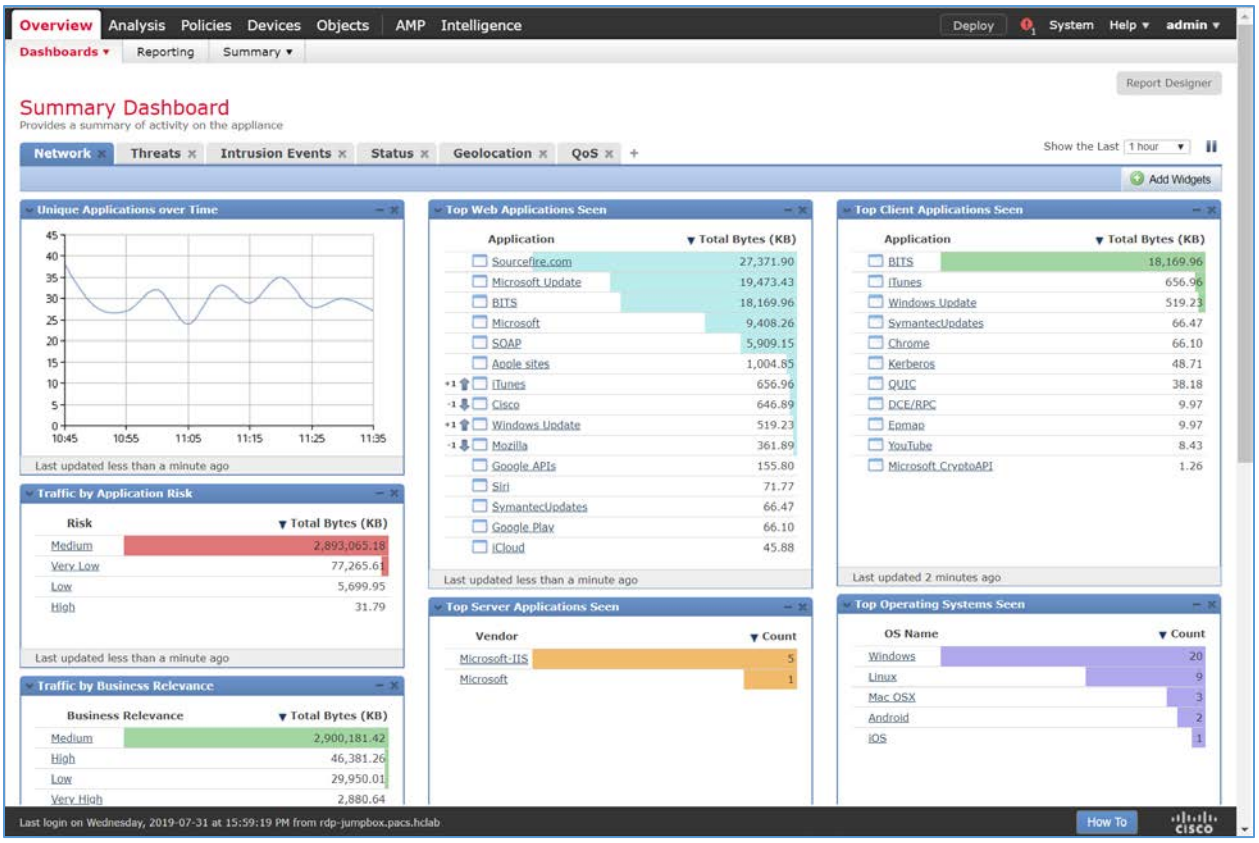
Operating System: Linux

Cisco Stealthwatch Flow Collector Virtual Edition Installation Guide

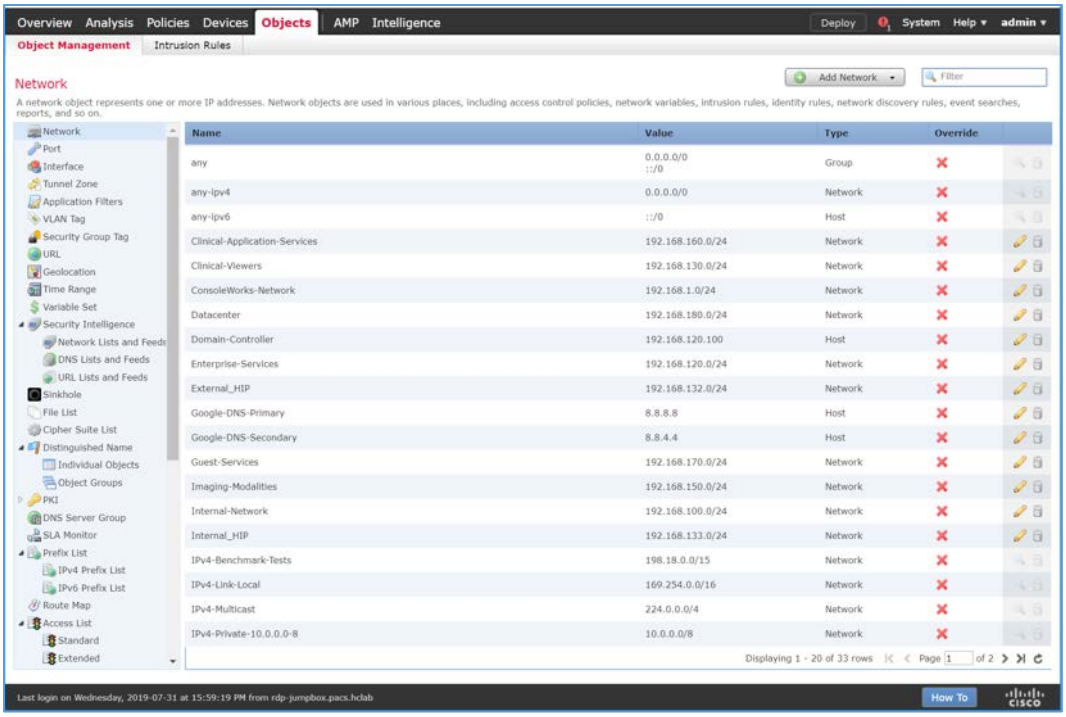
Install the Cisco Stealthwatch Flow Collector appliance according to the instructions provided at the Cisco installation guide [18].

Configure NetFlow Parameters for Cisco Firepower

1. Log in to the Cisco Firepower Management Console.

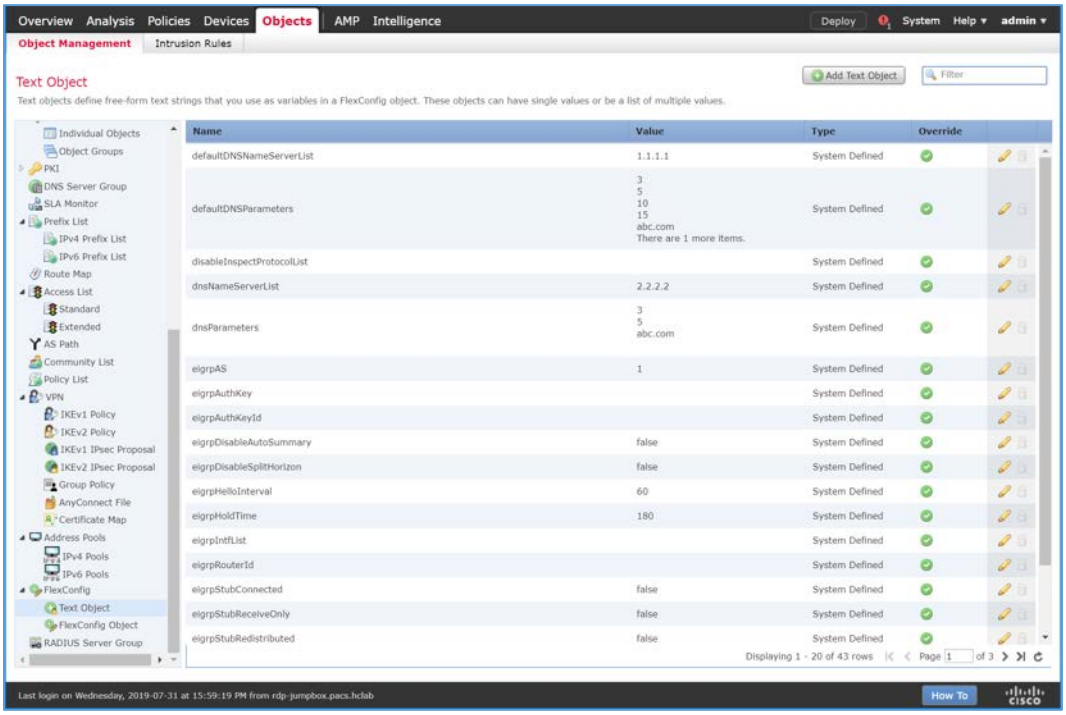


2. Navigate to **Objects**.



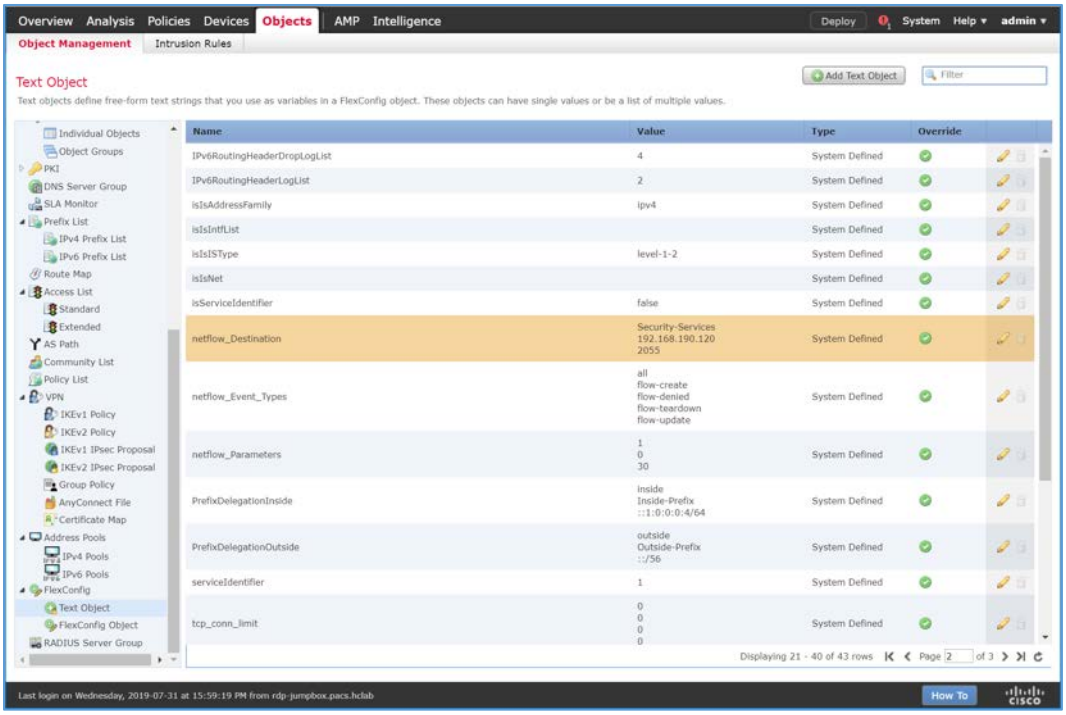
1690

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

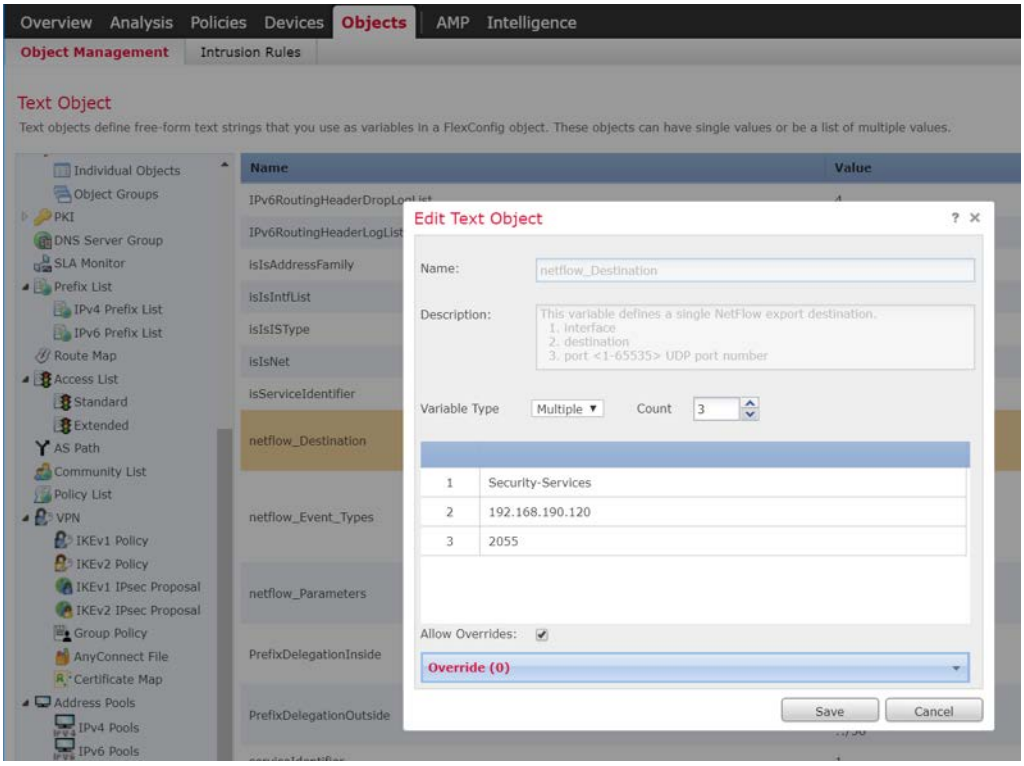


1692

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

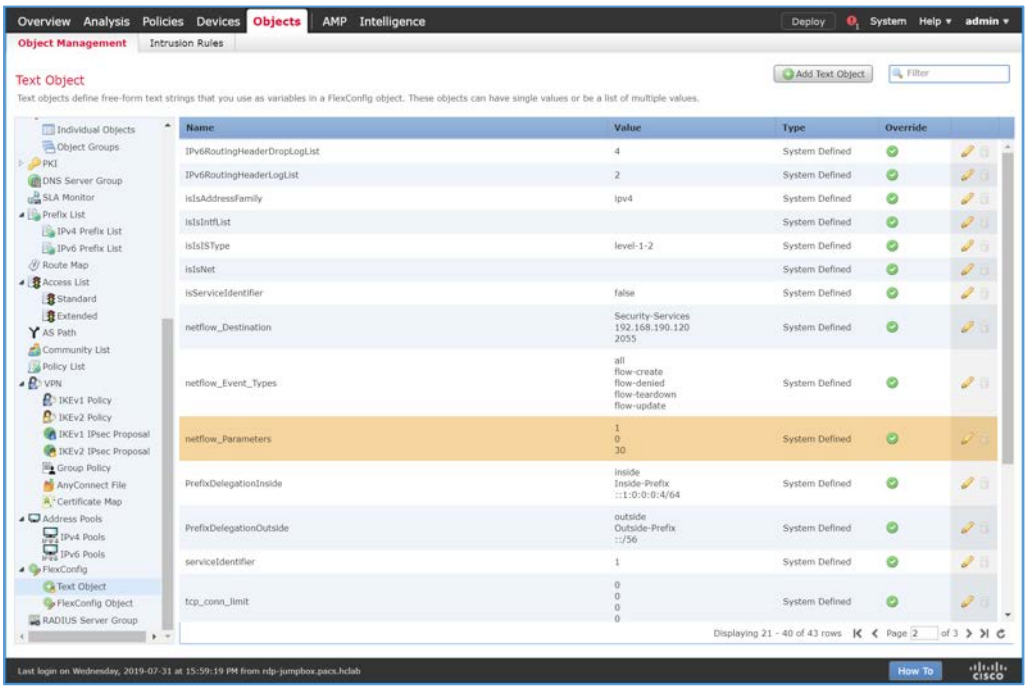


5. Click the **edit** icon for **netflow_Destination**.
6. Set **Variable Type** to **Multiple**.
7. Set **Count** to **3**.
8. For **Row 1**, enter **Security-Service** to set the name of the Cisco FTD interface to which the Cisco Stealthwatch UDP appliance is connected.
9. For **Row 2**, enter **192.168.190.120** to set the IP address of the Cisco Stealthwatch UDP appliance.
10. For **Row 3**, enter **2055** to set a port from which the Cisco Stealthwatch UDP appliance will receive NetFlow traffic.
11. Click **Save**.



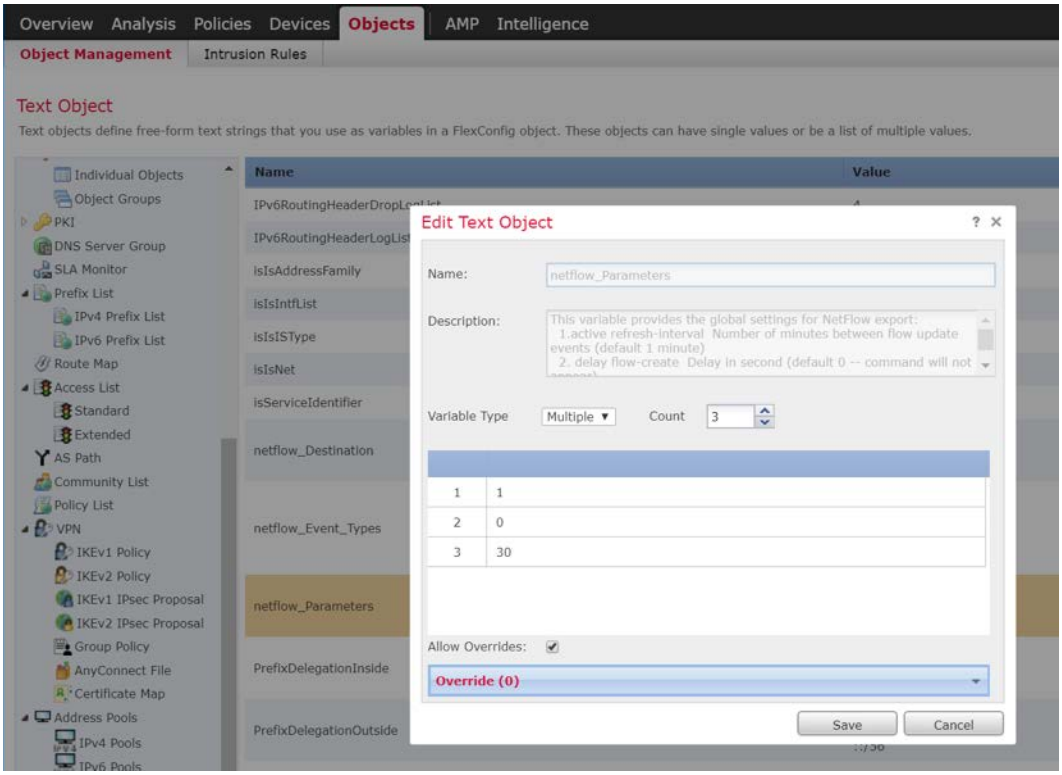
1704

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

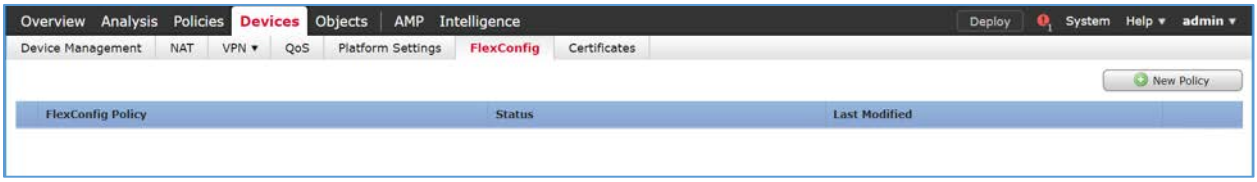


1706

13. Click the **edit** icon for **netflow_Parameters**.
14. Set **Variable Type** to **Multiple**.
15. Set **Count** to **3**.
16. For **Row 1**, enter **1** as a number for minutes between flow update events.
17. For **Row 2**, enter **0** as a number for seconds to delay flow create.
18. For **Row 3**, enter **30** as a number for minutes for template timeout rate.
19. Click **Save**.

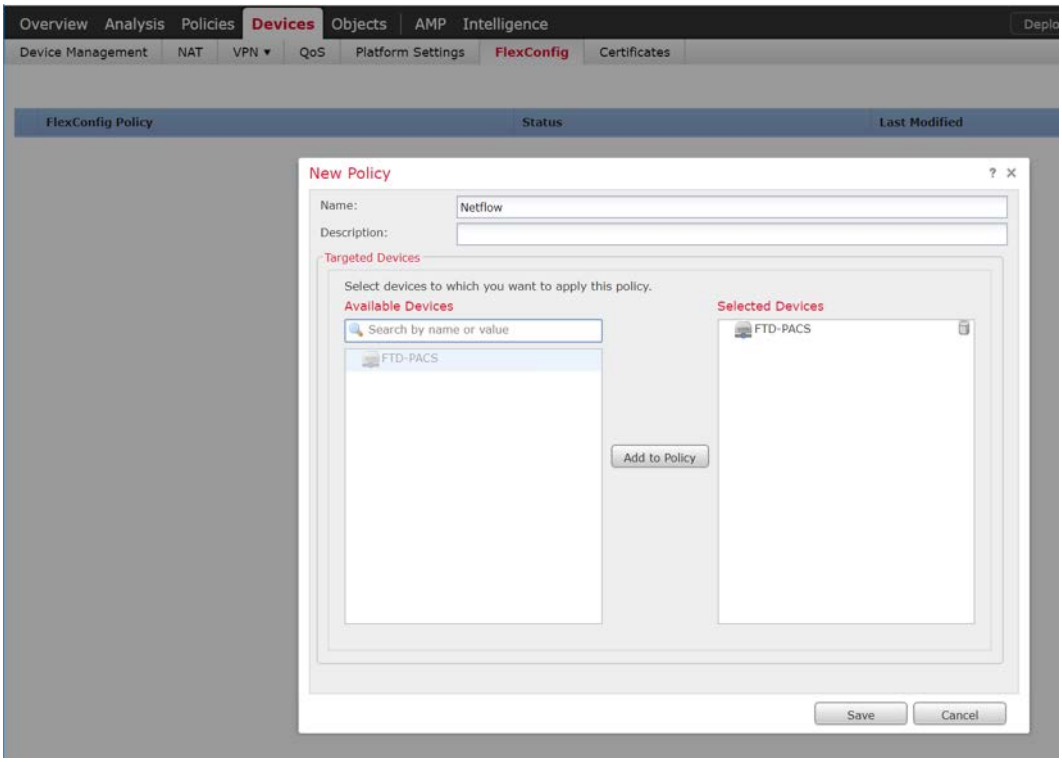


20. Navigate to **Devices > FlexConfig**.



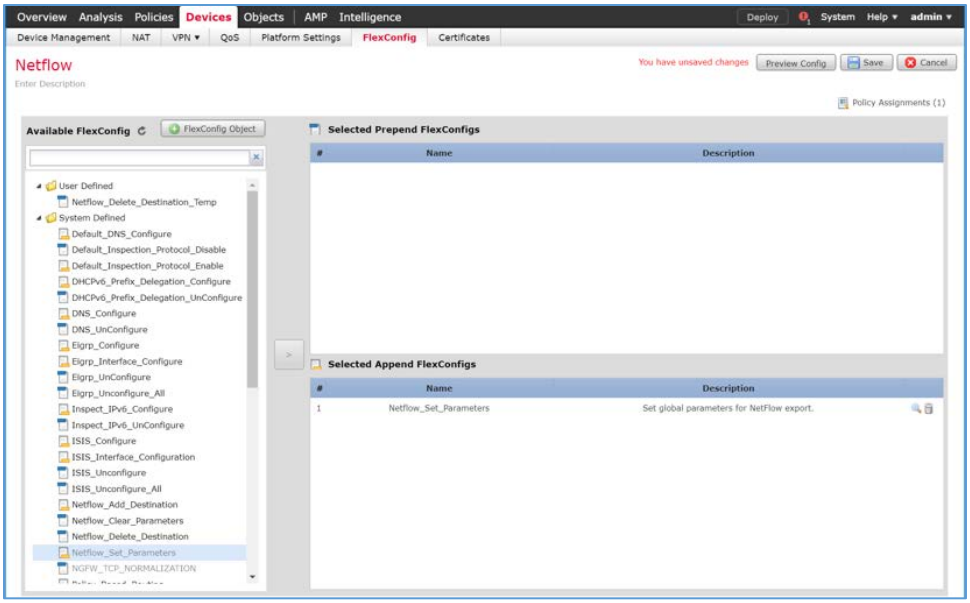
21. Click **New Policy**.

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



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

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

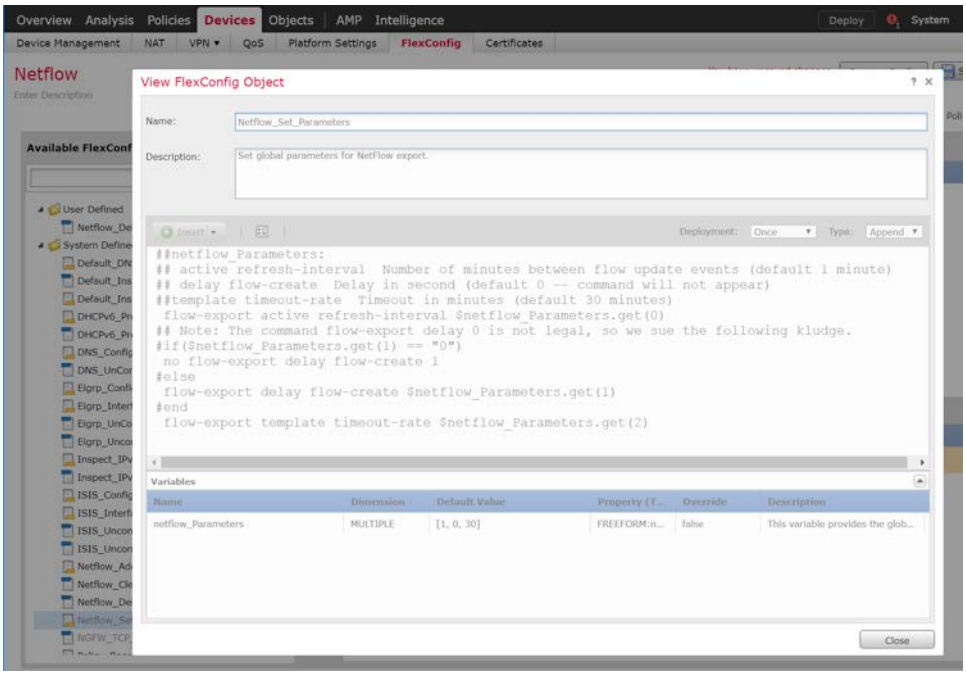


1726

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

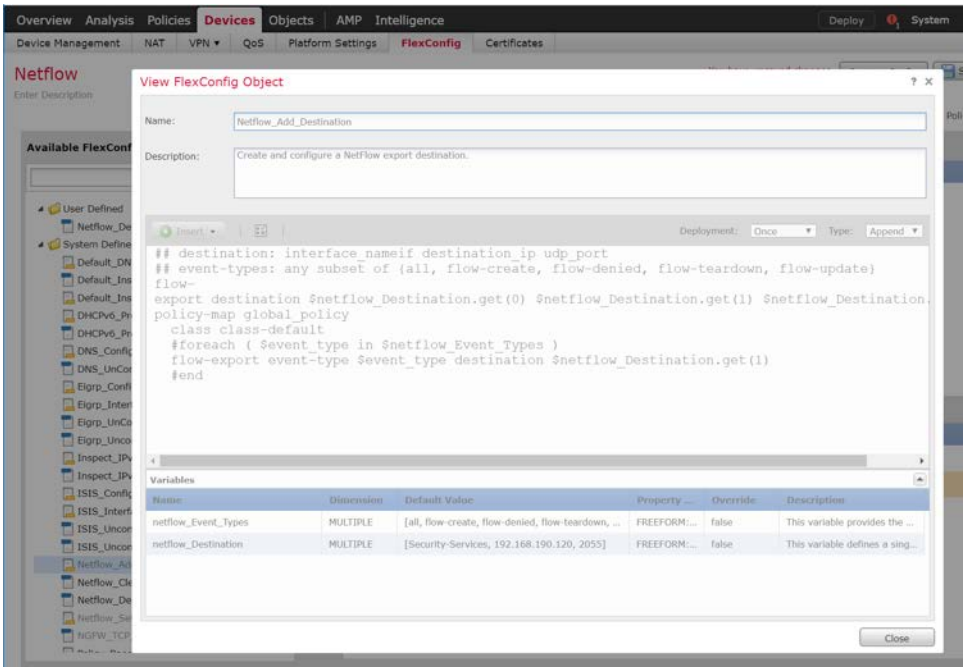
1728 28. Under **Variables > Default Value**, verify the minutes between flow data events, seconds to delay
1729 flow create, and minutes for template timeout rate that were set for **netflow_Parameters**.

1730 29. Click **Close**.



1731

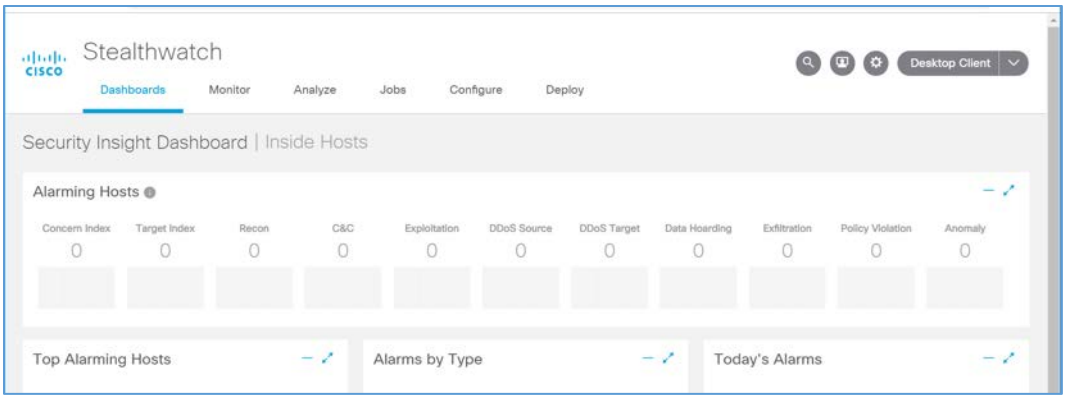
30. Under **Available FlexConfig**, find **Netflow_Add_Destination,** and add it to **Selected Append FlexConfigs**.
31. Click the **magnifier** icon for **Netflow_Add_Destination**.
32. Under **Variables > Default Value**, verify the Cisco FTD interface name, IP address of the Cisco Stealthwatch, and the NetFlow traffic port.
33. Click **Close**.



34. Click **Save**.
35. Deploy changes to the Cisco FTD.

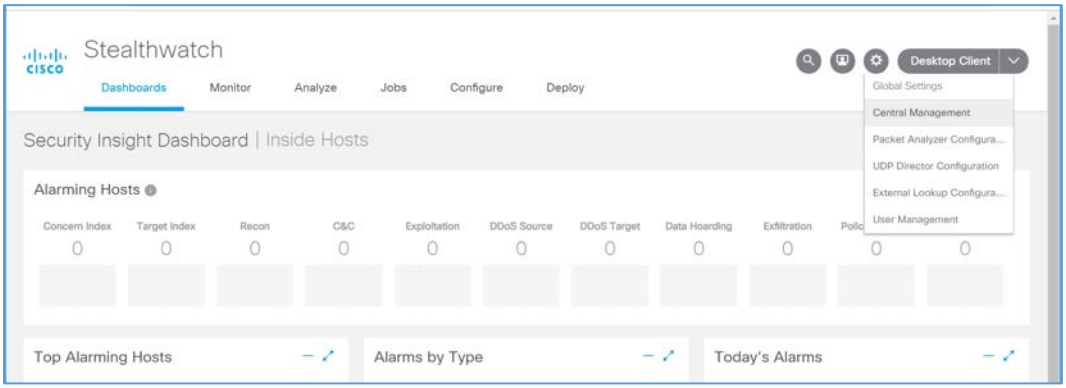
Forwarding Rules for Cisco Stealthwatch UDP Configuration

1. Log in to the web dashboard of the Cisco Stealthwatch Management Console.



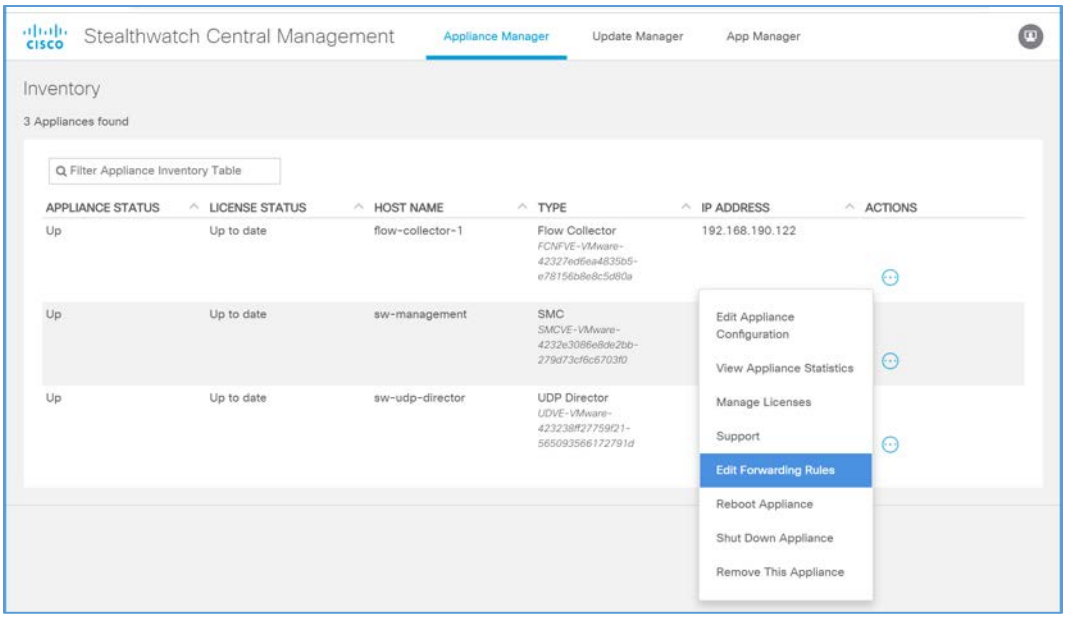
1743

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



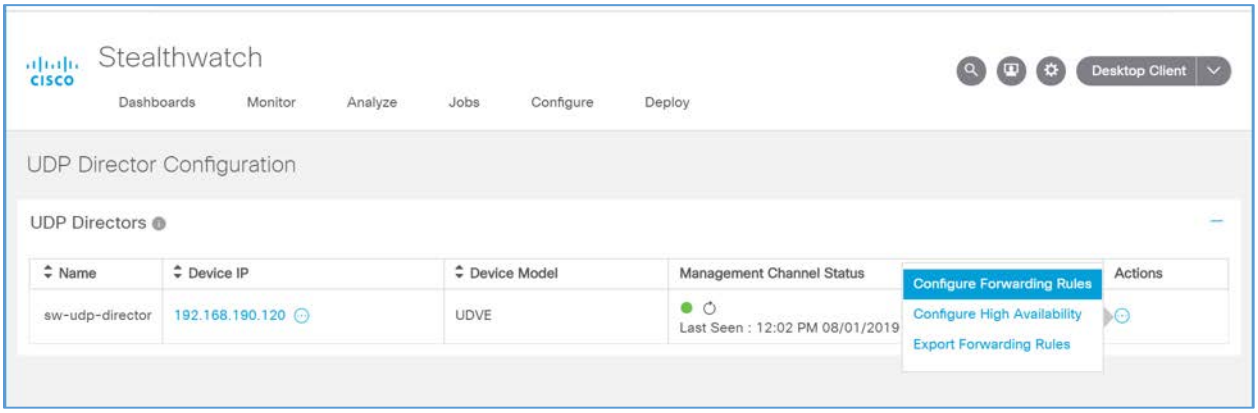
1745

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



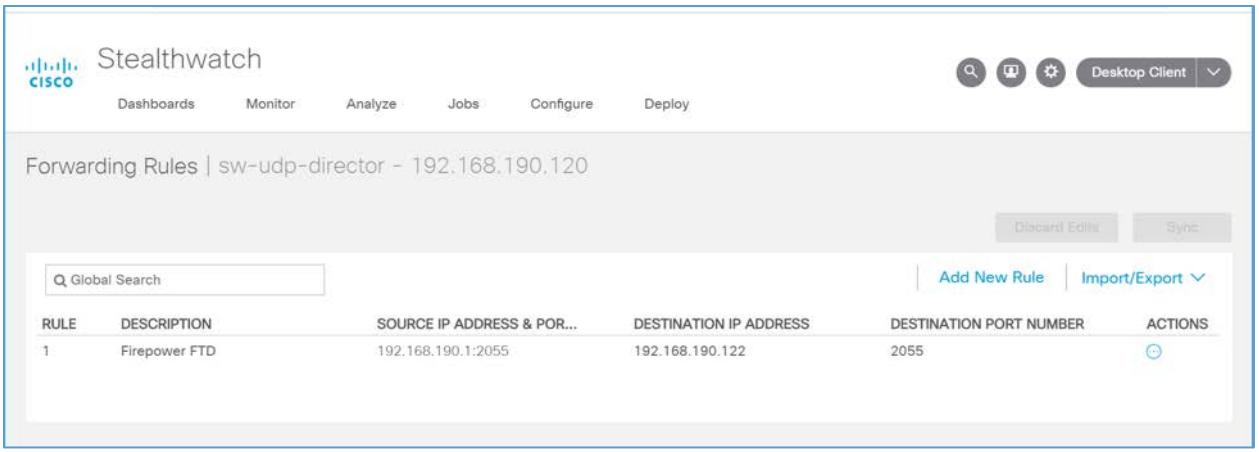
1747

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



1749

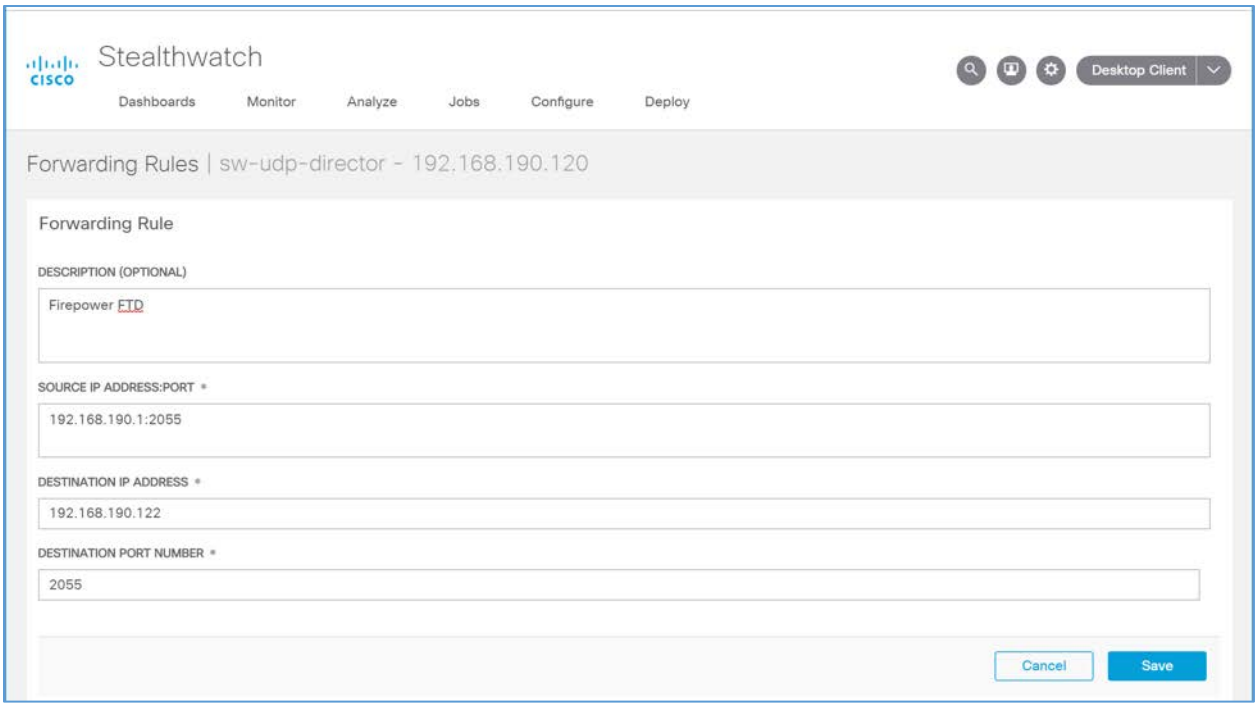
1750 5. Under **Forwarding Rules**, select **Add New Rule**.



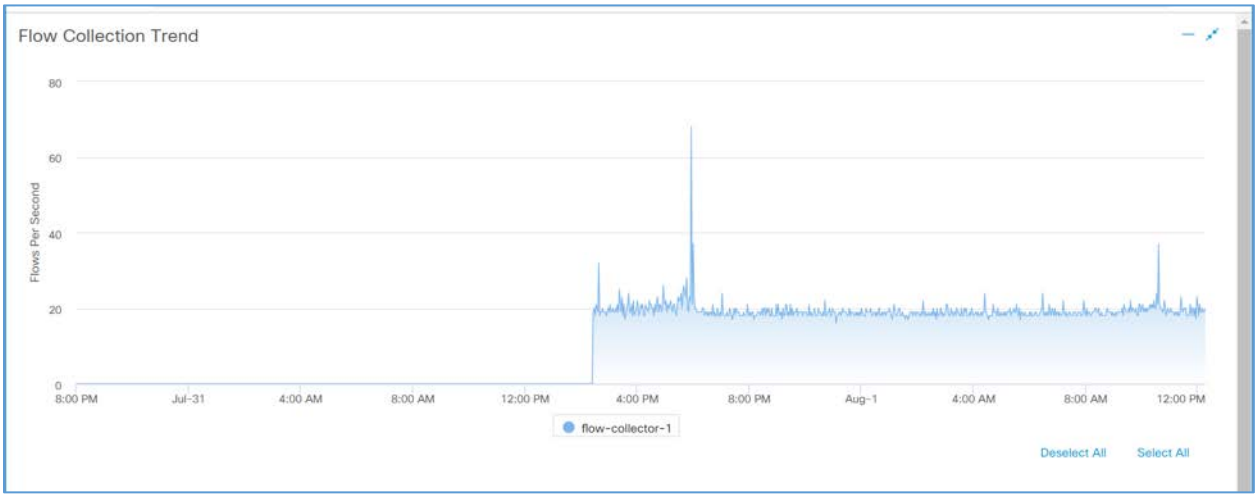
6. Enter a description (e.g., **Firepower FTD**) for the rule.
7. For **source IP address** and **source port**, enter the IP address, and port (e.g., **192.168.190.1:2055**) of the Cisco FTD interface sending the NetFlow traffic.

   Note: These parameters were established in Cisco FTD, found in the previous section, for the netflow_Destination object.
8. For **destination IP address**, enter the IP address (e.g., **192.168.190.122**) of the Cisco Stealthwatch Flow Collector.
9. For **destination port**, enter the port (e.g., **2055**) of the Cisco Stealthwatch Flow Collector.

   Note: This port was configured during the setup of the Flow Collector.



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

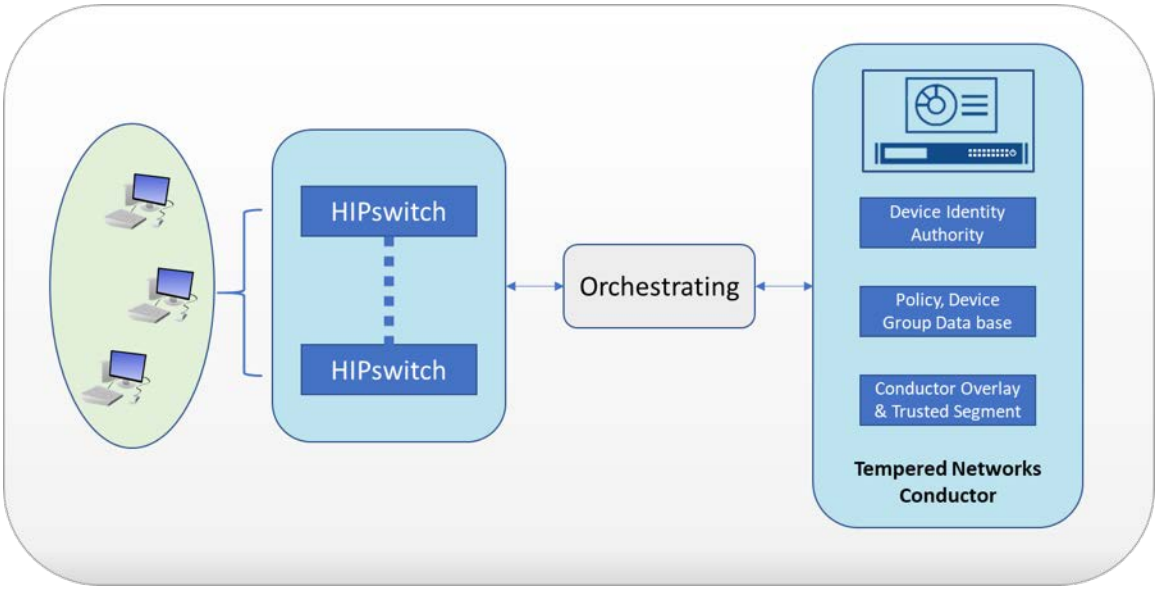


2.7.3 Tempered Networks Identity Defined Networking (IDN)

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

effectively cloak that traffic from the production network. A notional architecture is depicted in Figure 2-2 below.

Figure 2-2 Architecture of Networks IDN



Tempered Networks Conductor is the orchestration engine and intelligence behind an IDN. As shown in the above figure, the Conductor is responsible for creating and executing security policies and overlays. It is also responsible for issuing unique Cryptographic IDs (CIDs) to the IDN endpoints that enforce explicit trust relationships through device-based whitelisting.

HIPswitches are typically deployed in front of devices or hosts that cannot protect themselves, like medical devices such as modalities and other legacy systems and machines, or when customers are unable to install the proper endpoint-protection applications.

Installation involves the deployments of the Tempered Networks Conductor and HIPswitches. A Conductor open virtual appliance or application (OVA) file and a HIPswitches OVA file were provided by Tempered Networks.

2.7.3.1 Conductor Installation

System Requirements

CPU: 4

Memory: 4 GB RAM

Storage: 120 GB

Operating System: Linux Red Hat

Network Adapter: VLAN 1201

Tempered Networks Conductor Installation

1. Log in to the vSphere Client.
2. Select **File** > **Deploy OVF Template**.
3. Respond to the prompts with information specific to your deployment, including the ova package location, name and location, storage, networking and provisioning, etc.
4. Click **Power On After Deployment,** and click **Finish**.
5. Once the installation is done, power on the Conductor server and log in with username **macinfo** and the corresponding password to set up the necessary Mac address and IP address.

2.7.3.2 HIPswitch Installation

System Requirements

CPU: 4

Memory: 1 GB RAM

Storage: 1 GB

Operating System: Linux Red Hat

Network Adapter: VLAN 1201

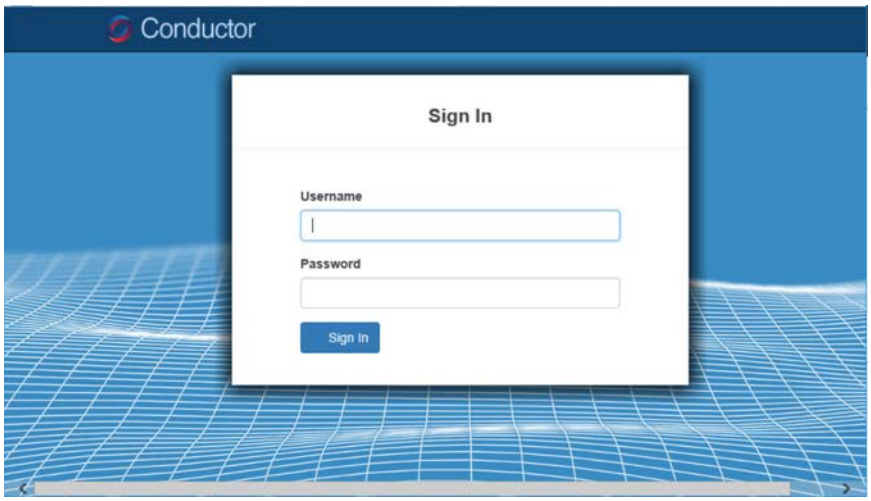
HIPswitch Installation

1. Log in to the vSphere Client.
2. Select **File** > **Deploy OVF Template**.
3. Respond to the prompts with information specific to your deployment, including the ova package location, name and location, storage, networking and provisioning, etc.
4. Click **Power On After Deployment**, and click **Finish**.
5. After the installation, use the username **mapconfig** and the corresponding password to connection the HIPswitch the conductor.
6. Use the username **underlayaddress** and its corresponding password to setup the IP address, netmask, gateway, and DNS for the HIPswitch.
7. Repeat the above installation procedures to install additional HIPswitches.

Tempered Networks Conductor and HIPswitch Configuration

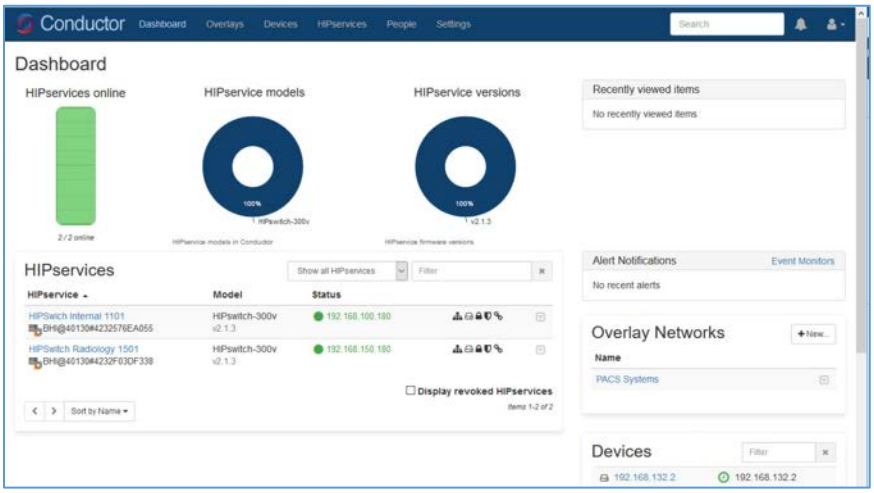
1817 The configuration for the Conductor and HIPswitches is done through the browser connected to the
1818 Conductor *https://ConductorIP*. Below is the log in page.

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



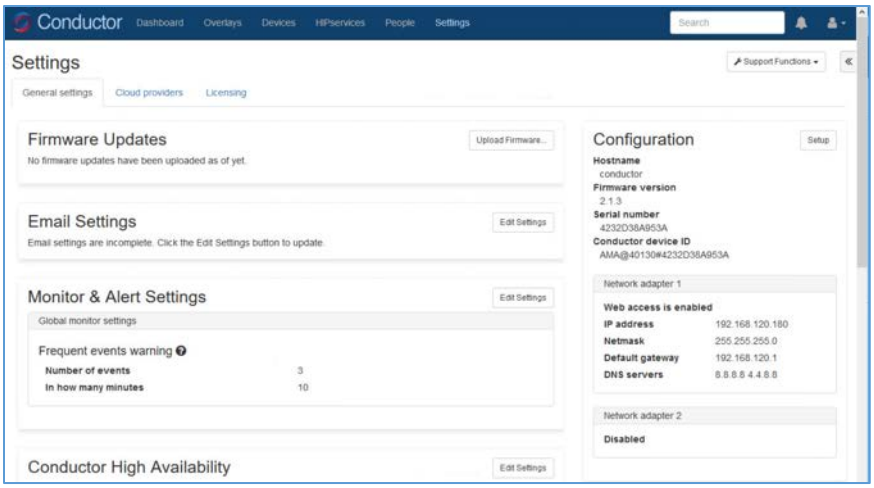
1820

1821 2. Click **Settings** tab.



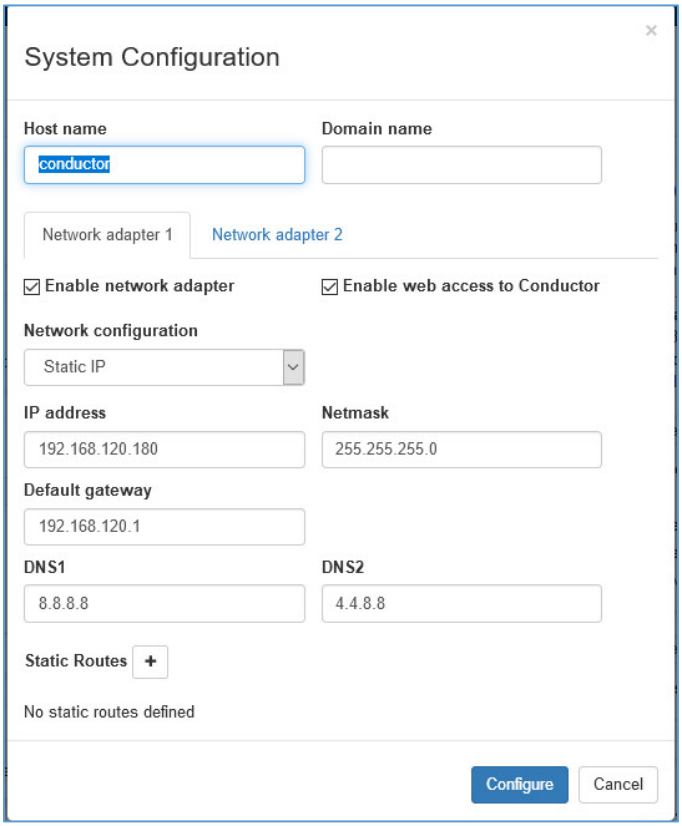
1822

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.



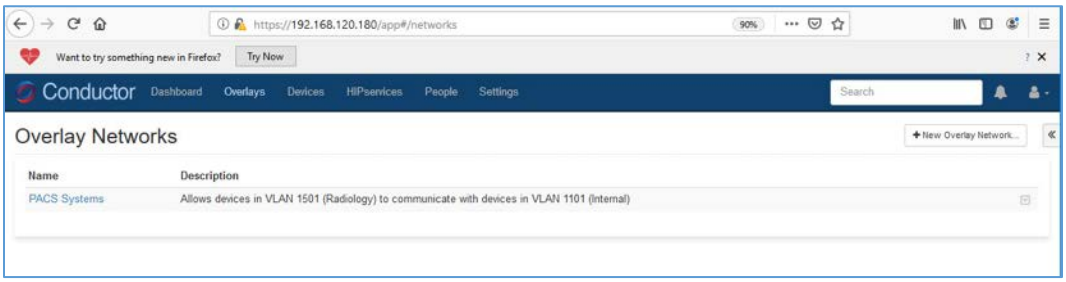
1825

1826 4. Enter the proper network parameters for the **Conductor,** including the **IP address** (e.g.,
1827 **192.168.120.180**), **Netmask** (e.g., **255.255.255.0**), **Default gateway** (e.g., **192.168.120.1**), and **DNS**
1828 (e.g., **8.8.8.8**, **4.4.8.8**), then click **Configure**.

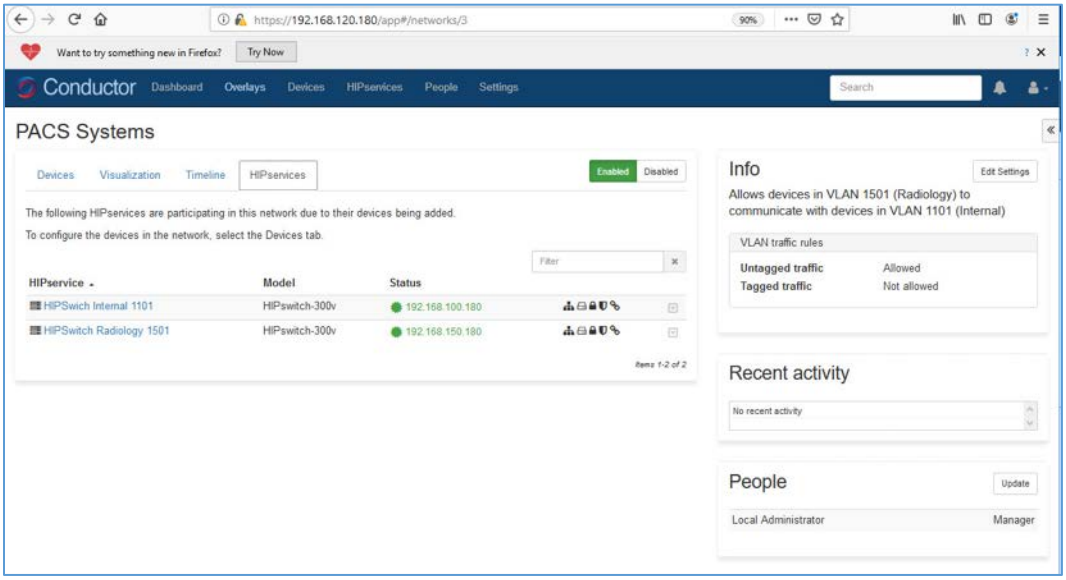


1829

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



6. Two HIPswitches were installed to test for this project. These two HIPswitches are Model HIPswtich-300v, and they are named **HIPswitch Internal** and **HIPswitch Radiology**. Both were configured to participate in the **PACS Systems** overlay network.



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

After creating a secure layer in the Conductor and adding those medical imaging devices and PACS servers to that layer, the medical imaging device and PACS server can be set up as trusted, by selecting the Enable button on the overlay page. Once they are trusted, communication between those medical imaging devices and PACS servers will be established. All the communication will be encrypted.

The microsegmentation is achieved by using the HIPswitch. Other VMs will not be able to communicate with these two devices unless they are configured to do so.

2.7.4 Zingbox IoT Guardian

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

Zingbox Cloud Setup

1. Visit https://zingbox.com and register for an account.
2. Log in to the Zingbox console and navigate to **Administration > My Inspectors > Download Inspector**.
3. Download either the .ova or the .iso file, depending on your environment's requirements.

System Requirements

CPU: 4

Memory: 8 GB RAM

Storage: 256 GB (Thin Provision)

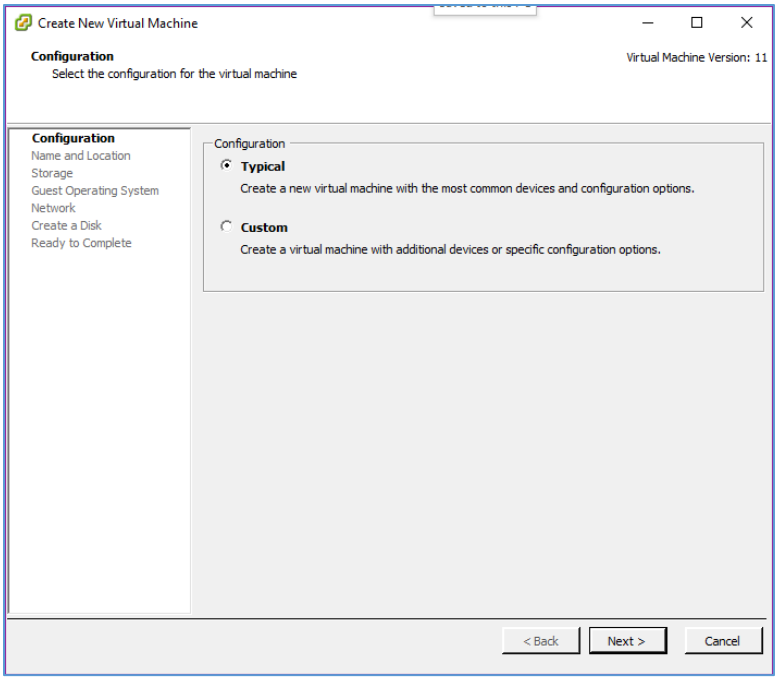
Operating System: CentOS 7

Network Adapter 1: VLAN 1101

Network Adapter 2: Trunk Port

Zingbox Inspector Installation

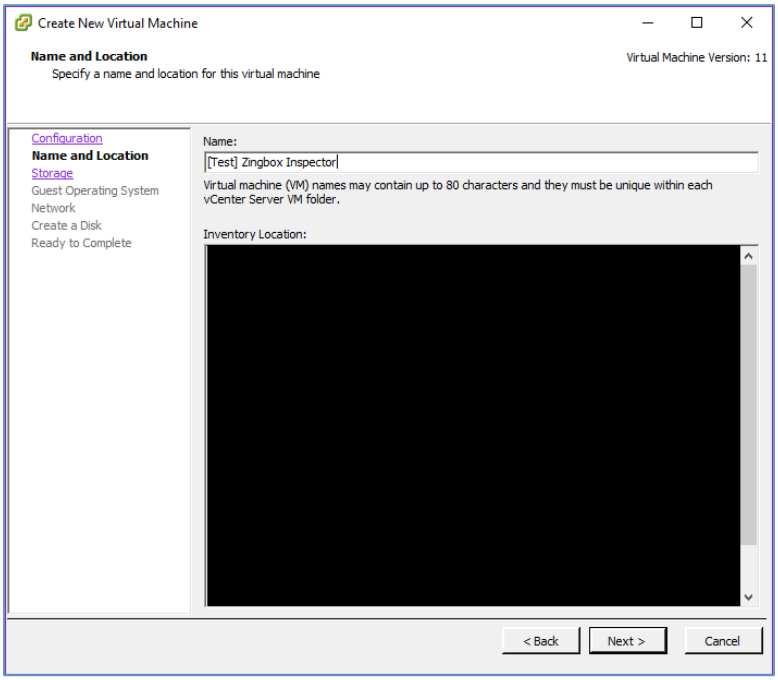
1. Create a new virtual machine, and under **configuration** select **Typical**.
2. Click **Next >**.



1872

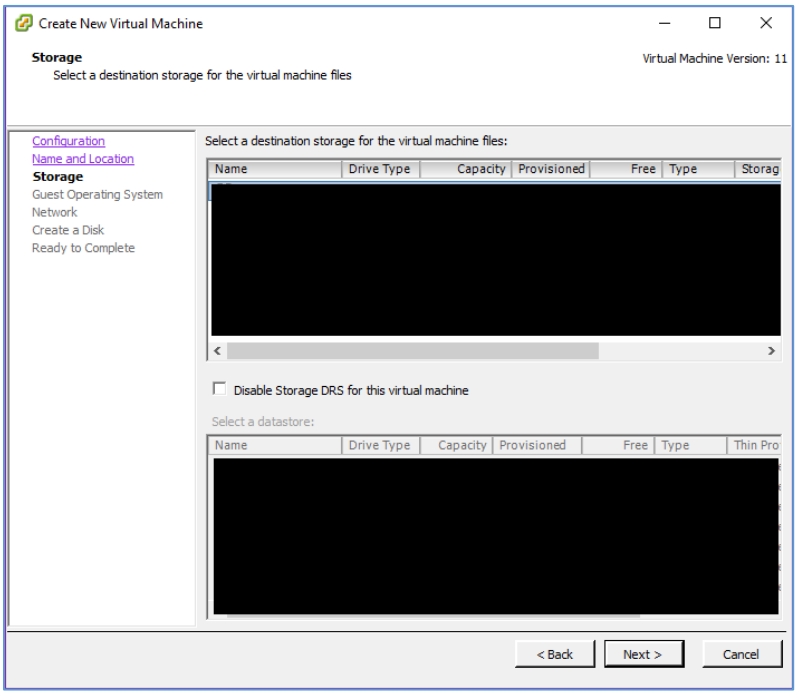
1873 3. Create a **Name** for the virtual machine and assign it an **Inventory Location**.

1874 4. Click **Next >**.

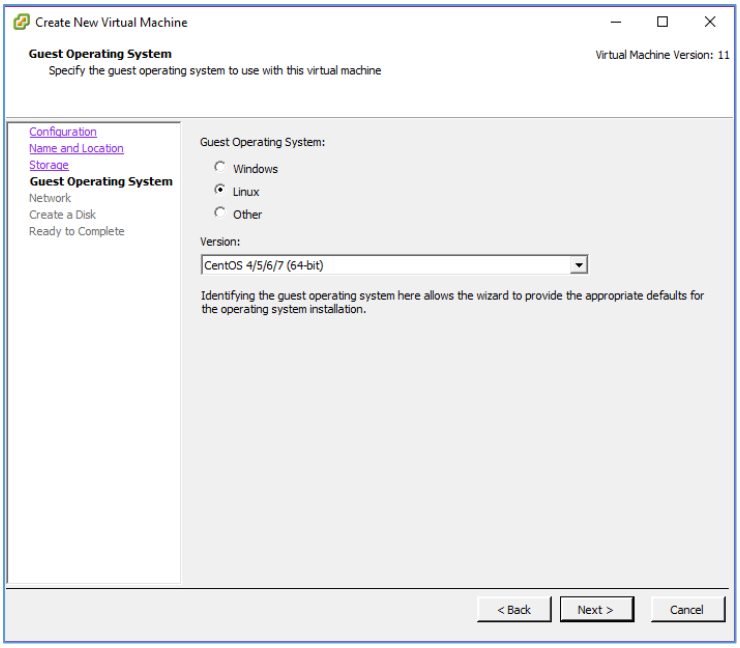


1875

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



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

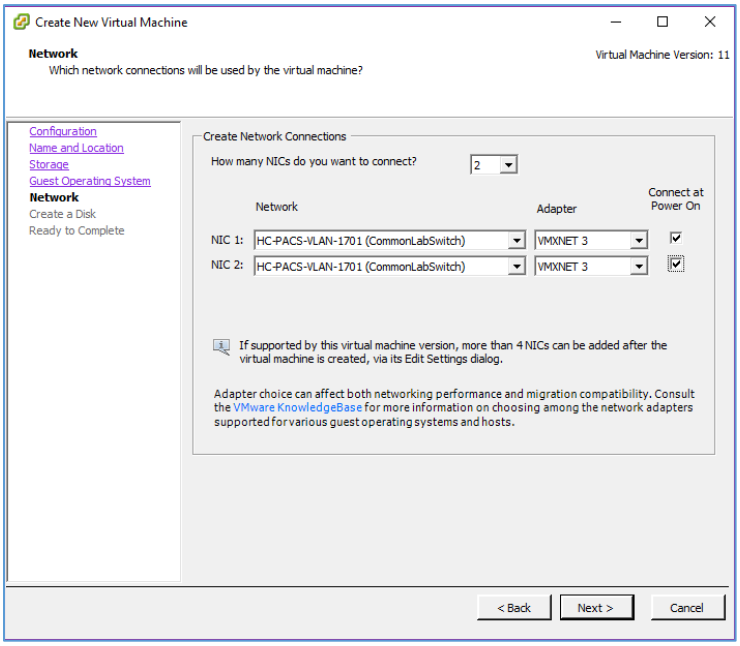


1881

1882 9. Connect **2 NICs** to the virtual machine and assign them to a **network**.

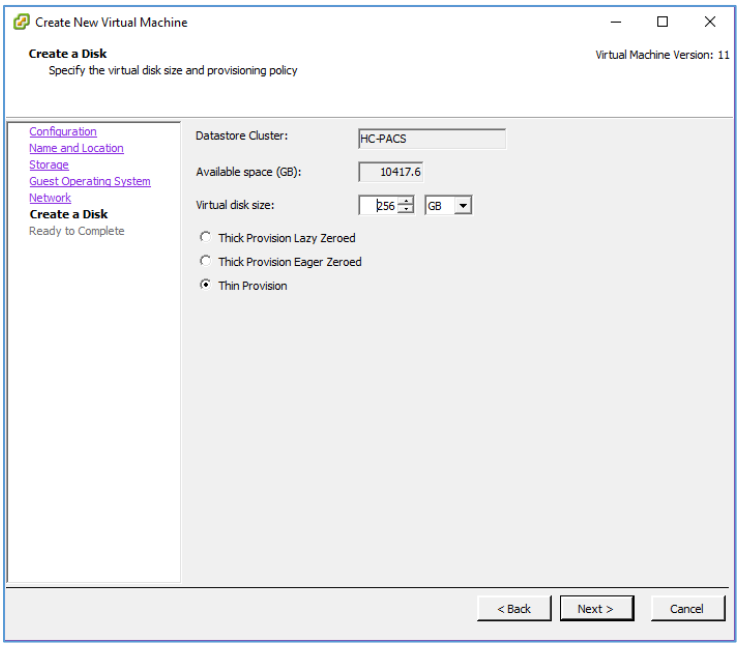
1883 10. Check **Connect at Power On** for both NICs.

1884 11. Click **Next >**.

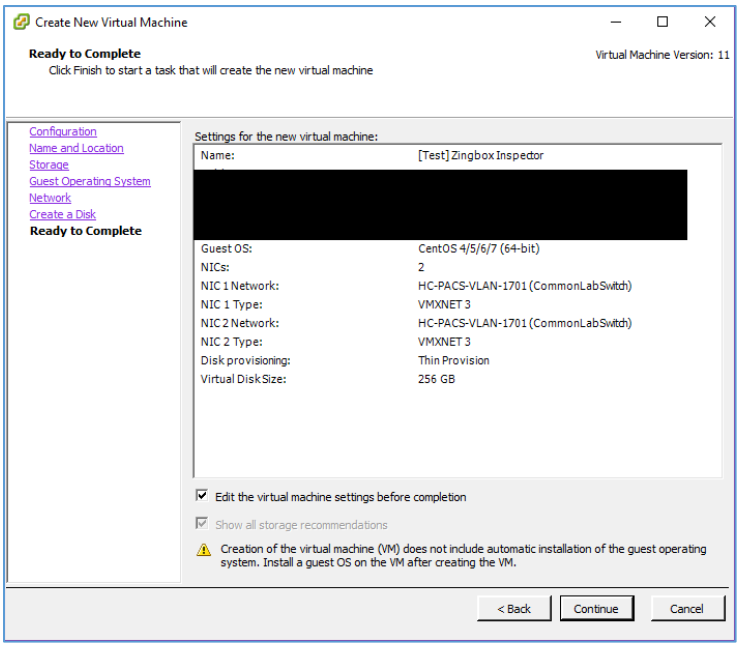


1885

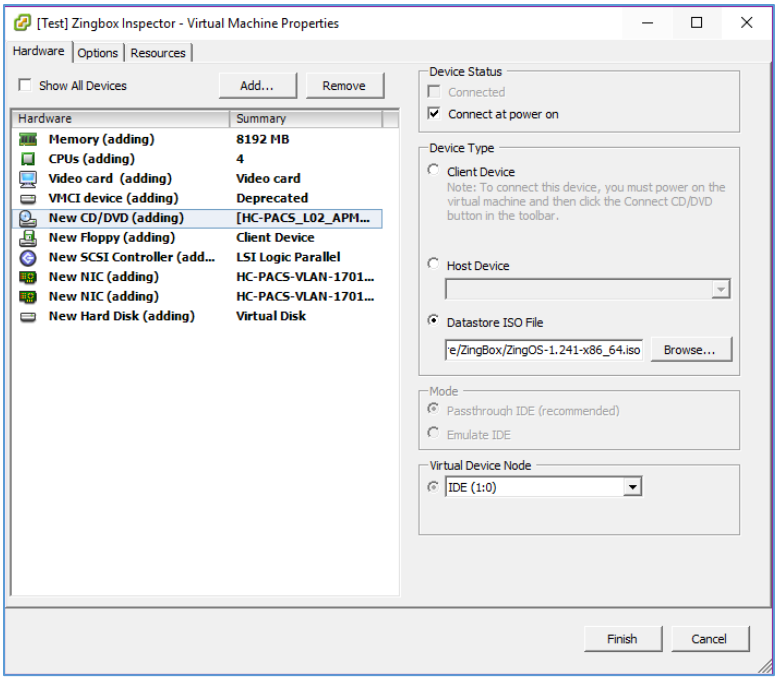
12. Set a **Virtual disk size** and **Provisioning method**.
13. Click **Next >**.



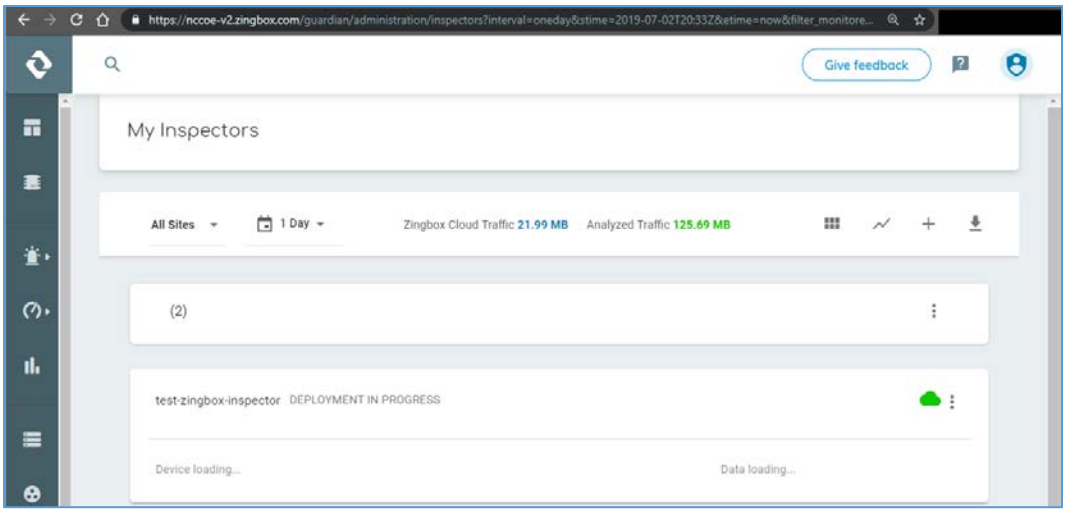
14. Verify virtual machine settings are correct.
15. Check **Edit the virtual machine settings before completion**.
16. Click **Continue**.



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



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



2.7.5 Forescout CounterACT 8

Forescout CounterACT is a network access control tool that can perform device discovery and classification, risk assessment, and control automation through passive and active techniques. For this project, the intended use of Forescout is to manage device compliance and perform necessary remediation when devices fall out of compliance.

System Requirements

CPU: 2

Memory: 8 GB RAM

Storage: 80 GB (Thin Provision)

Operating System: Linux Kernel 3.10

Network Adapter 1: VLAN 1201

Network Adapter 2: Trunk Port

Forescout Appliance Installation

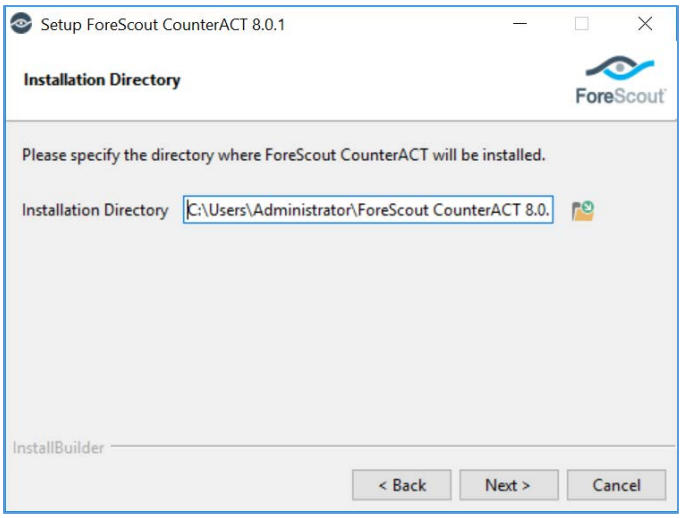
1. To begin installation, obtain the Forescout ISO. Load the Forescout ISO into the VM's CD/DVD drive. Make sure the CD/DVD drive is set to **Connect at Power On**.
2. Boot up the VM and begin the installation process.
3. Select **Install CounterACT**.
4. Press **Enter** to reboot.
5. Select **option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

6. Select **option 1** for standard installation.
7. Press **enter** to proceed.
8. Select **option 1** for CounterACT Appliance.
9. Select **option 1** for Per Appliance Licensing Mode.
10. Enter appliance **description**.
11. Give appliance a **password**.
12. Enter **forescoutCA** and apply this as the appliance host name.
13. Assign the appliance an IP address **192.168.120.160**.
14. Assign appliance a network mask **255.255.255.0**.
15. Enter **192.168.120.1** as the appliance's gateway.
16. Enter domain name *pacs.hclab*.
17. Enter DNS server address **192.168.120.100**.
18. Review configuration and run test.
19. Once the test passes, select **done**.

Forescout CounterACT Console Installation

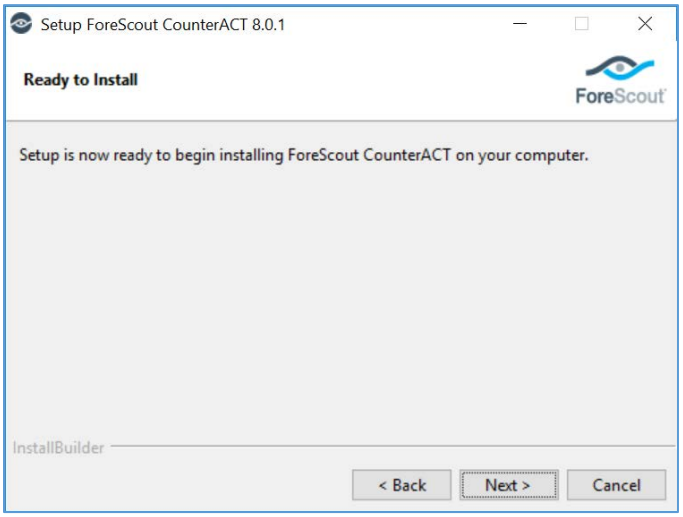
1. Run **Install_Management.exe**.
2. Click **Next >**.

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



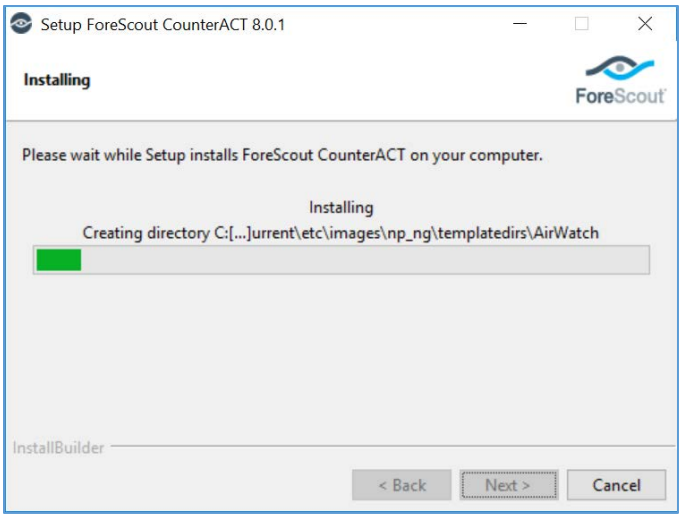
1946

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



1948

1949 5. An **Installing** screen will appear that provides a status bar indicating degree of installation
1950 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.

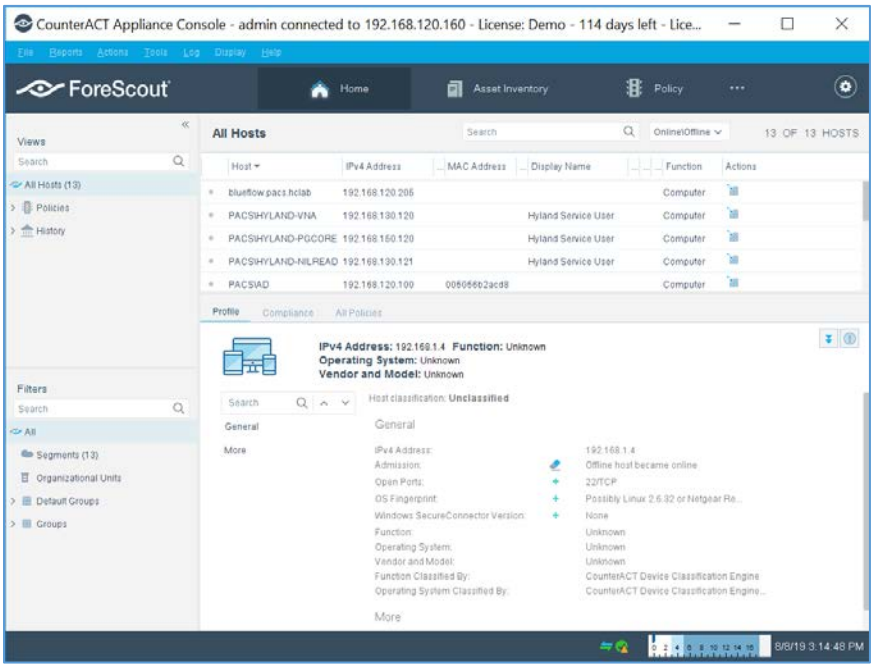
Forescout CounterACT Configuration

To use the full function offered by the Forescout CounterACT, proper network configuration is required, which may include the monitor and response interface assignments at the data center, the network VLAN and segmentation information, IP address range that the CounterACT appliance will protect, user Directory account information, domain credentials, core switch IP address, and vendor and SNMP parameters.

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

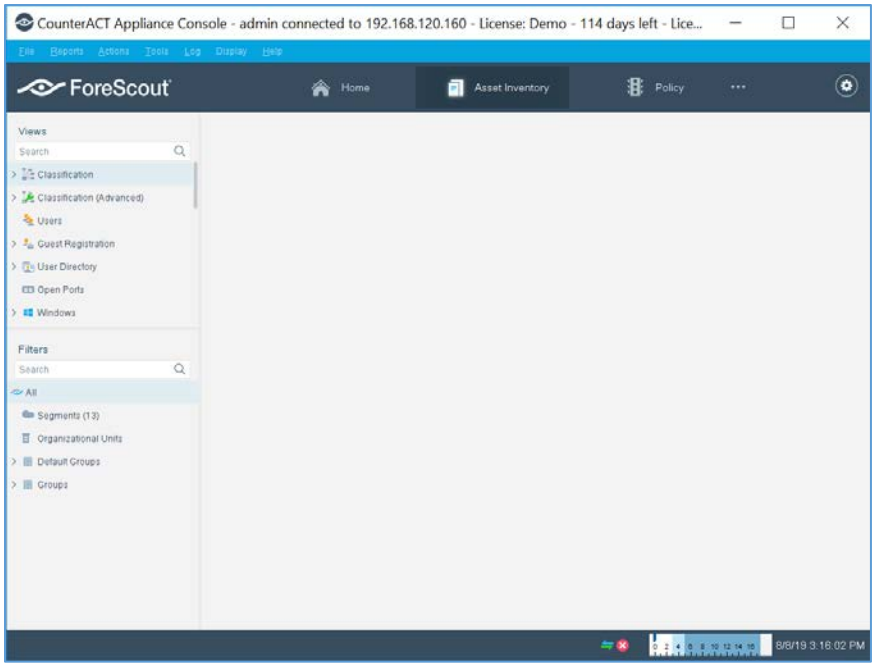
1. Select **the CounterACT** icon from the server on which you installed the **CounterACT Console**. A log on page appears, as depicted below.

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



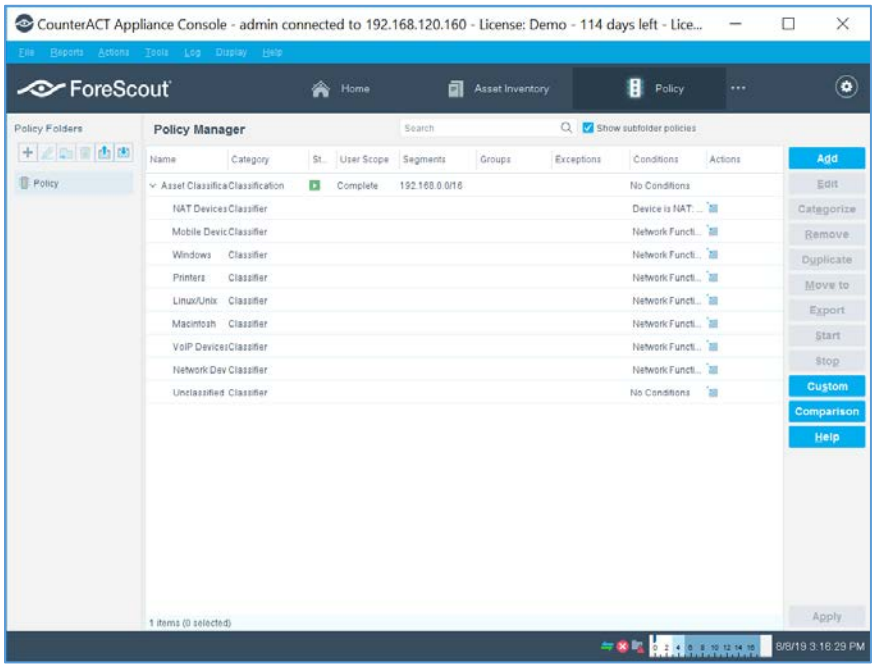
The console manager can be used to view, track, and analyze network activities detected by the appliance. It can also be used to define the threat protection, firewall, and other polices.

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



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

2.7.6 Symantec Endpoint Detection and Response (EDR)

Symantec Endpoint Detection and Response performs behavioral analytics on endpoint events from Symantec Endpoint Protection, to identify potentially malicious behavior. It can sandbox impacted endpoints, prioritize risks, and provide tailored remediation guides.

System Requirements

CPU: 12

Memory: 5 GB RAM

Storage: 500 GB (thin provisioned)

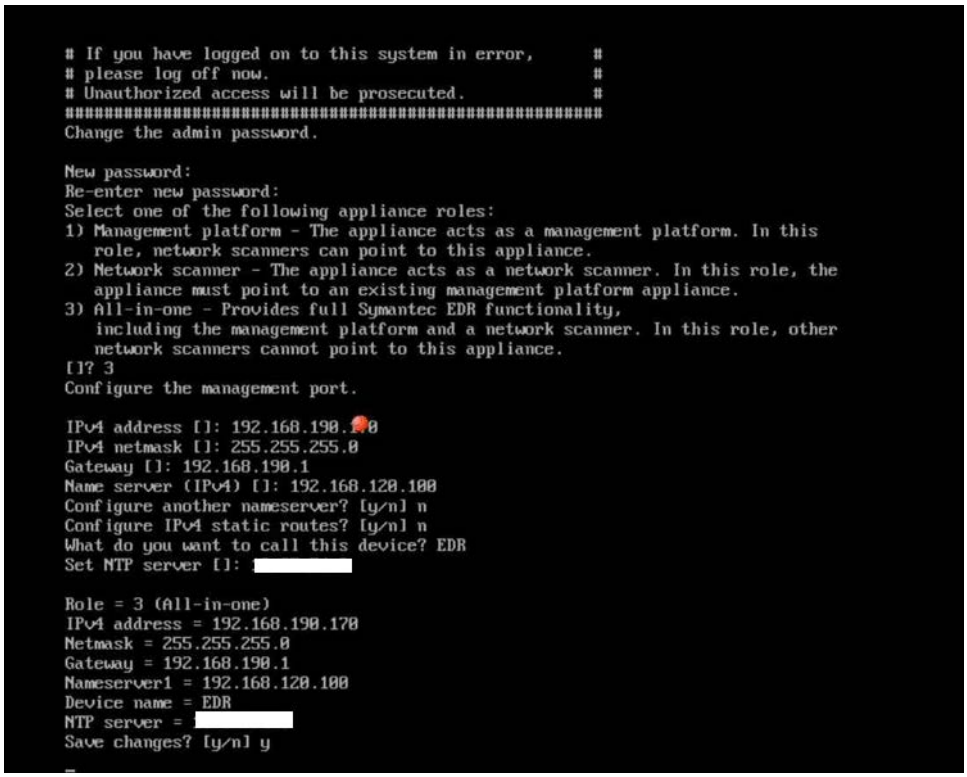
Operating System: CentOS 7

Network Adapter 1: VLAN 1901

Network Adapter 2: SPAN_PACS

Symantec EDR Installation

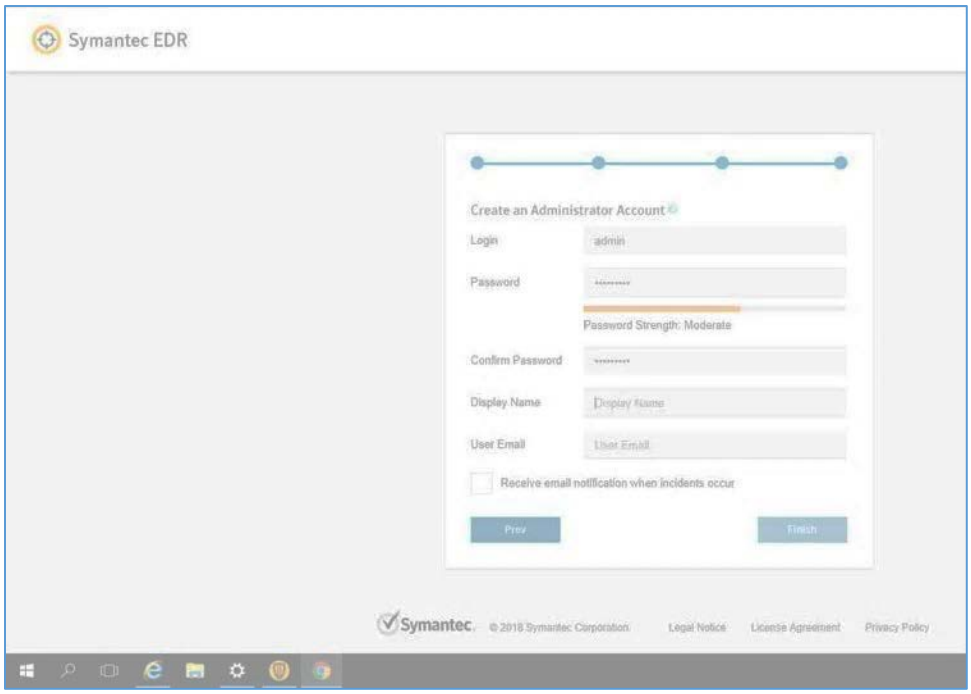
1. Launch the virtual appliance after deployment of the vendor-provided *SEDR-4.0.0-483-VE.ova* file.
2. Enter default username **admin** and default password. You will be required to change the default password by entering a new password.
3. After changing the default password, the bootstrap will automatically launch. Enter the following options during the bootstrap:
    - **IPv4 address []: 192.168.190.17**
    - **IPv4 netmask []: 255.255.255.0**
    - **Gateway []: 192.168.190.1**
    - **Name server (IPv4) []: 192.168.120.100**
    - **Configure another nameserver? [y/n]: n**
    - **Configure IPv4 static routes? [y/n]: n**
    - **What do you want to call this device?: EDR**
    - **Set NTP server []: *X.X.X.X***
4. After verifying the correct details, enter **Y** to save changes. The appliance will restart.



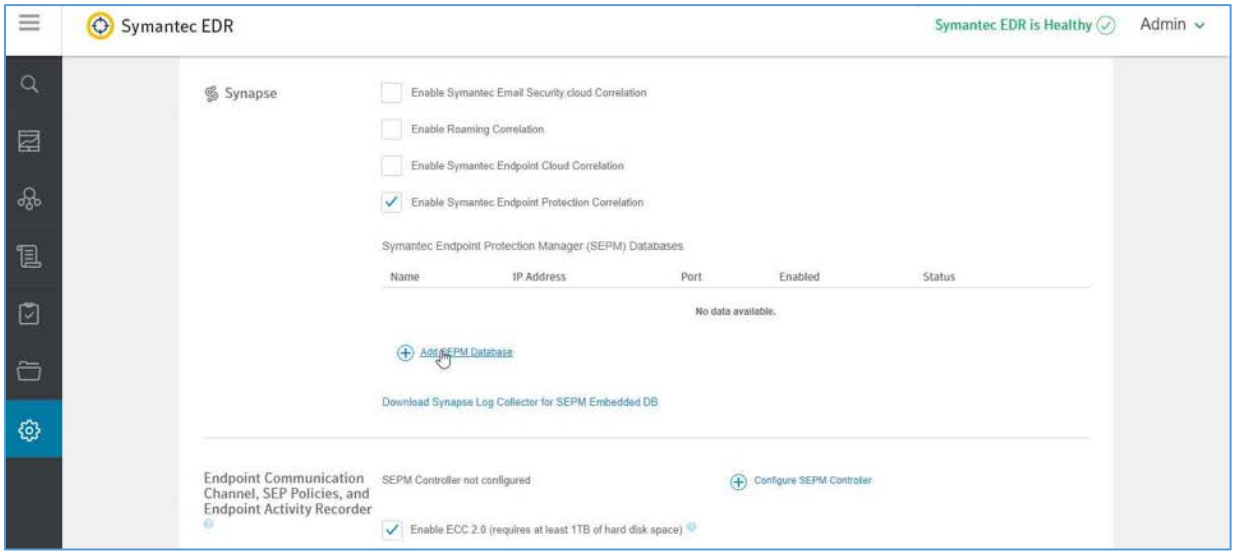
2012

2013 5. Open a web browser and travel to the virtual appliance at *https://192.168.190.170*. Enter the
2014 username setup and password *******.

2015 6. Follow the prompts to create the initial admin account.

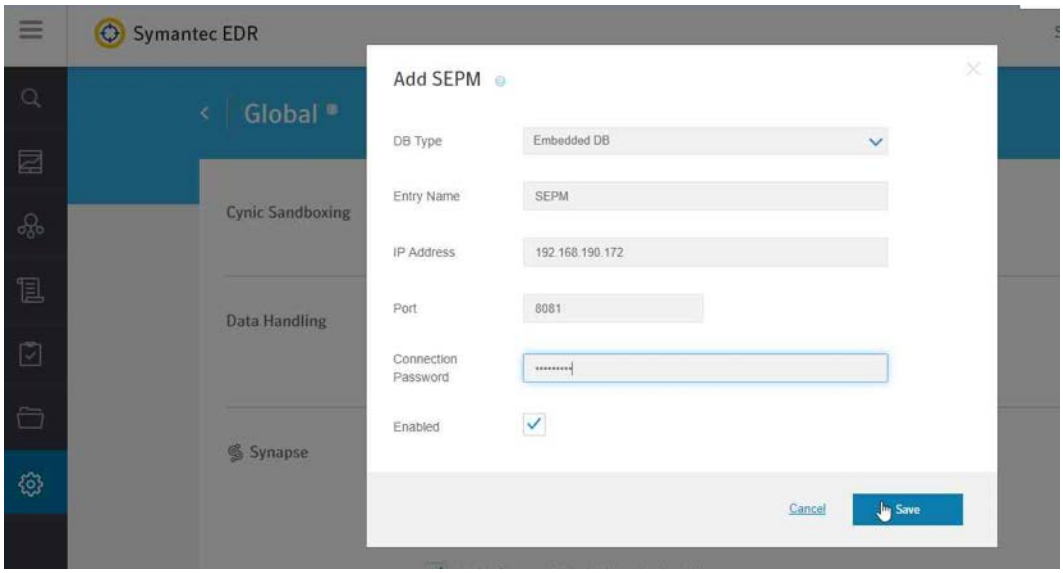


7. Select the **Settings** menu, and then select the **Global** sub-menu.
8. Ensure **Enable Symantec Endpoint Protection Correlation** is checked.
9. Select **Add SEPM Database** and enter the following options.

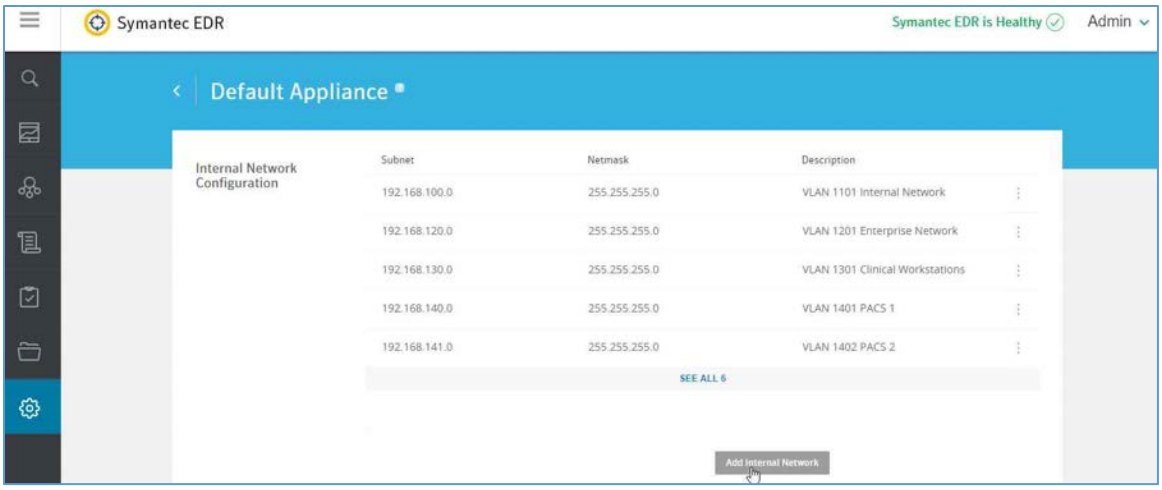


10. Provide the information that follows, and click **Save**:

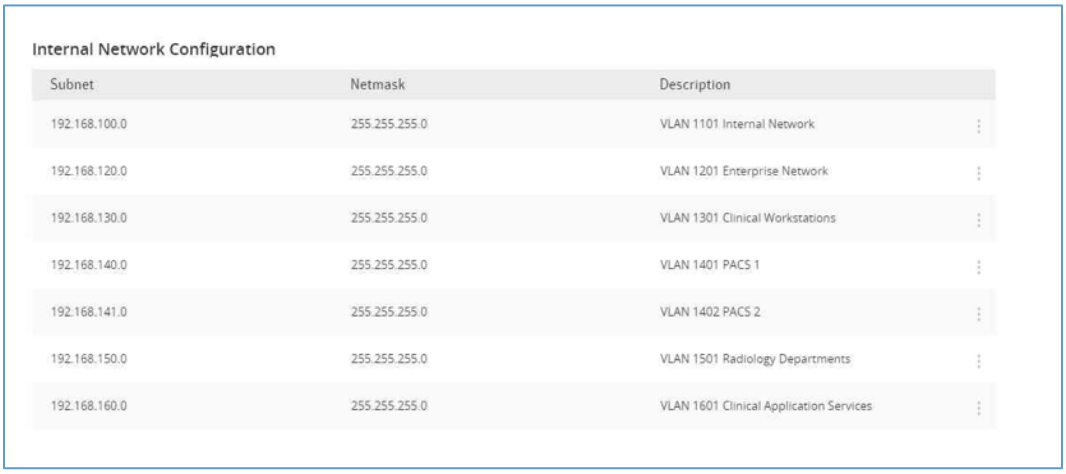
- **DB Type: Embedded DB**
- **Entry Name: SEPM**
- **Address: 192.168.190.172**
- **Port: 8081**
- **Connection Password:** *enter your connection password*
- **Enabled:** *Checked*



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

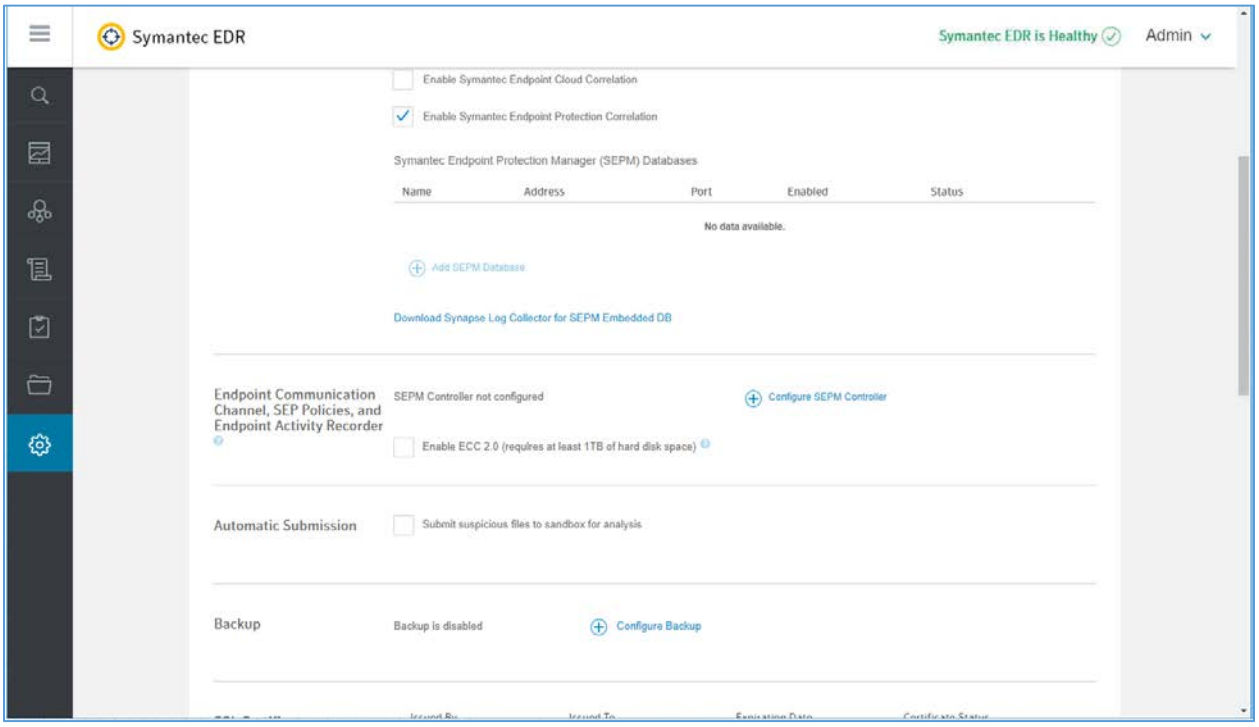


- **Subnet: 192.168.100.0 Netmask: 255.255.255.0 Description: VLAN 1101**
- **Subnet: 192.168.120.0 Netmask: 255.255.255.0 Description: VLAN 1201**
- **Subnet: 192.168.130.0 Netmask: 255.255.255.0 Description: VLAN 1301**
- **Subnet: 192.168.140.0 Netmask: 255.255.255.0 Description: VLAN 1401**
- **Subnet: 192.168.141.0 Netmask: 255.255.255.0 Description: VLAN1402**
- **Subnet: 192.168.150.0 Netmask: 255.255.255.0 Description: VLAN 1501**
- **Subnet: 192.168.160.0 Netmask: 255.255.255.0 Description: VLAN 1601**
- **Subnet: 192.168.180.0 Netmask: 255.255.255.0 Description: VLAN 1801**
- **Subnet: 192.168.190.0 Netmask: 255.255.255.0 Description: VLAN 1901**

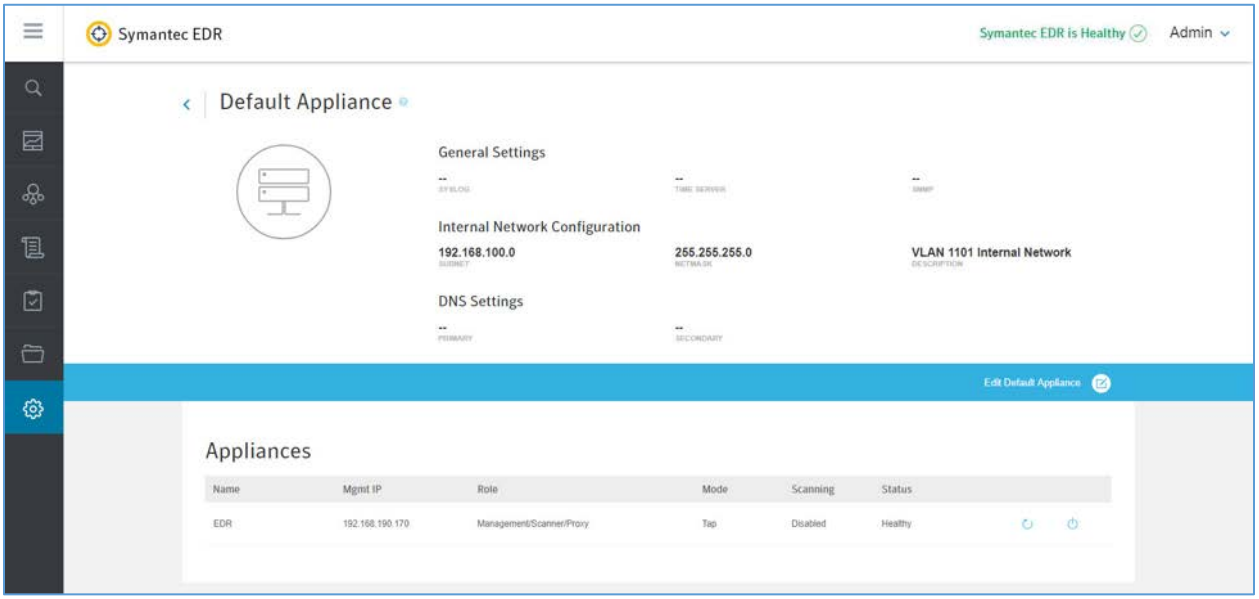


14. Select **Settings** and then **Global**.

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



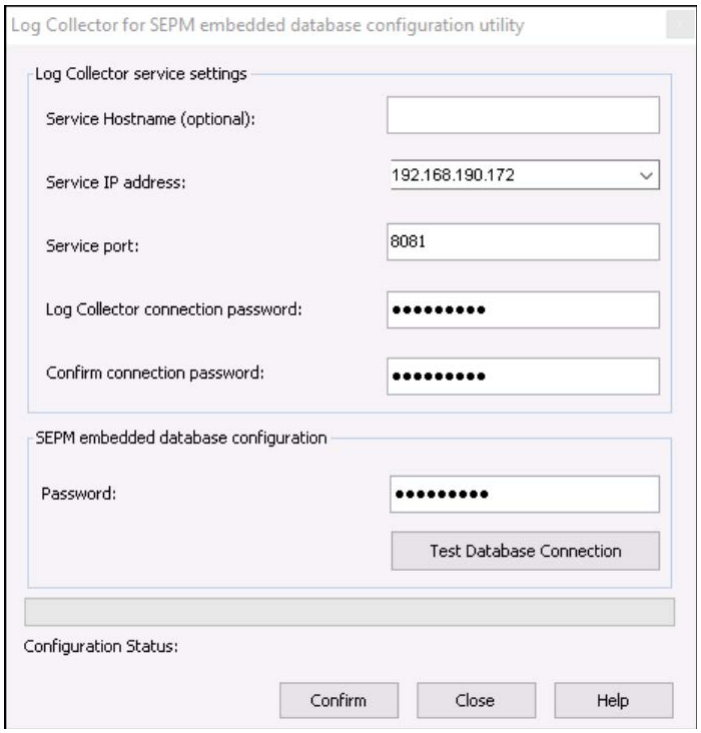
16. Select **Settings** and then **Appliances**.



17. Select **EDR** from the appliances list.
18. Turn **Scanning** on under the **Network Interface Settings**.

Symantec EDR and SEP Correlation

1. Open a web browser and travel to the virtual appliance at *https://192.168.190.170*. Log in with your administrator account.
2. From the settings menu, select **global settings**.
3. Select **Download Synapse Log Collector** for SEPM Embedded DB.
4. After the *SEPMLogCollector.msi* finishes downloading move to the **SEP Manager (SEPM)**.
5. Launch the *SEPMLogCollector.msi* file from **SEPM**.
6. Continue through the setup wizard prompts by clicking **Next** to use the default settings.
7. After installation is complete, launch the **Log Collection** for **SEPM** embedded database configuration utility, and enter the values below:
   - **Service Hostname (optional):** *Leave blank*
   - **Service IP address: 192.168.190.172**
   - **Service port: 8082**
   - **Log Collector connection password:** *enter connection password*
   - **Confirm connection password:** *enter connection password again*
   - **SEPM embedded database configuration password:** *enter embedded database password*
8. After entering values into configuration utility, click **Confirm**.



2.8 Endpoint Protection & Security

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

Symantec DCS:SA utilizes a software agent to provide various server protections, including application whitelisting, intrusion prevention, and file integrity monitoring. For this project, a DCS:SA agent was installed on both PACS servers in our architecture.

System Requirements

CPU: 4

Memory: 8 GB RAM

Storage: 120 GB (Thin Provision)

Operating System: Microsoft Windows Server 2016 Datacenter

Network Adapter: VLAN 1901

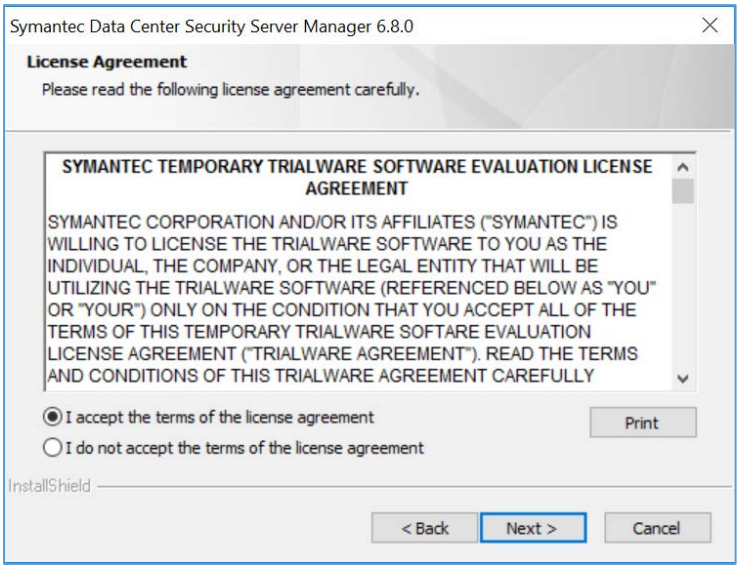
Symantec Data Center Security Installation

1. Launch **server.exe**.
2. Click **Next >**.

2085

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

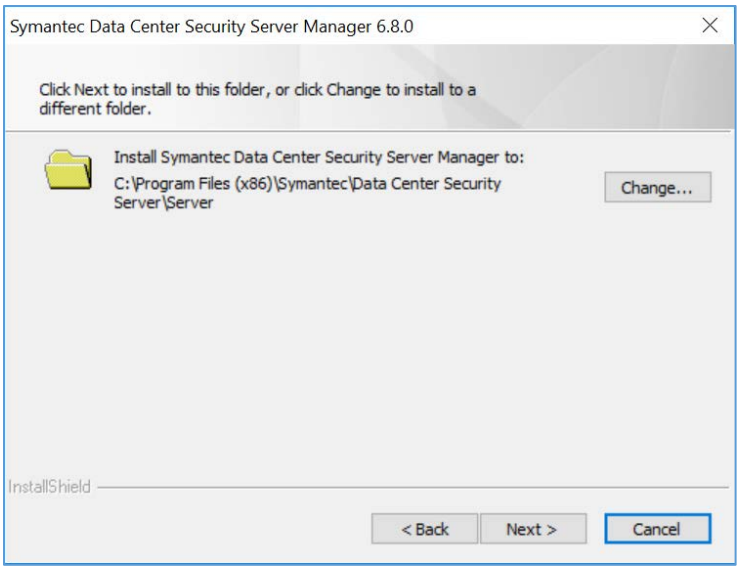
2087 4. Click **Next >**.



2088

2089 5. Verify install location.

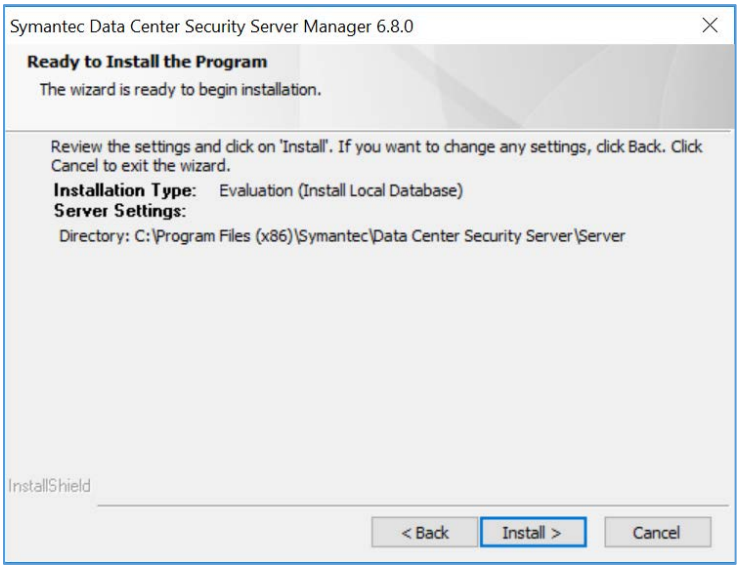
2090 6. Click **Next >**.



2091

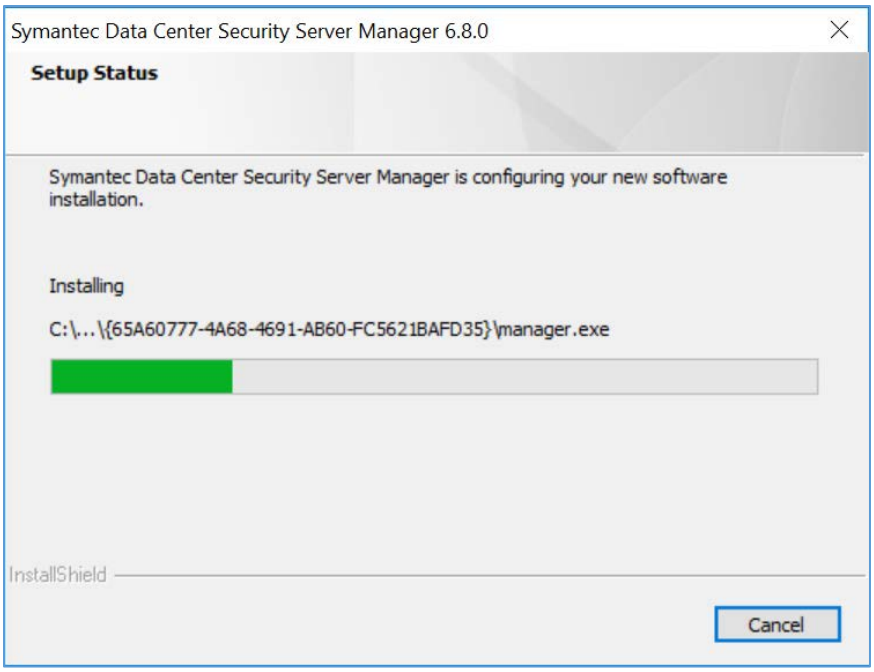
2092 7. Review settings.

2093 8. Click **Install >**.



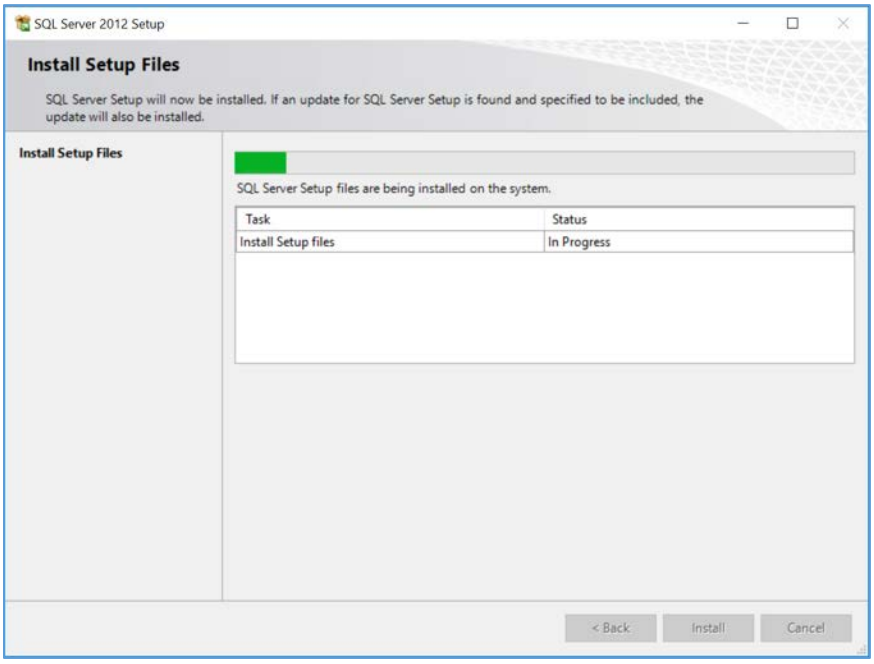
2094

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



2096

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

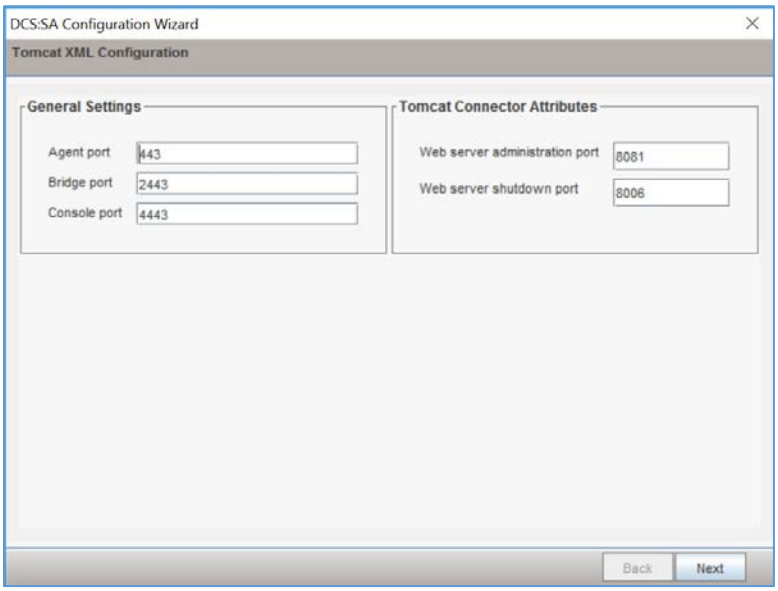


2098

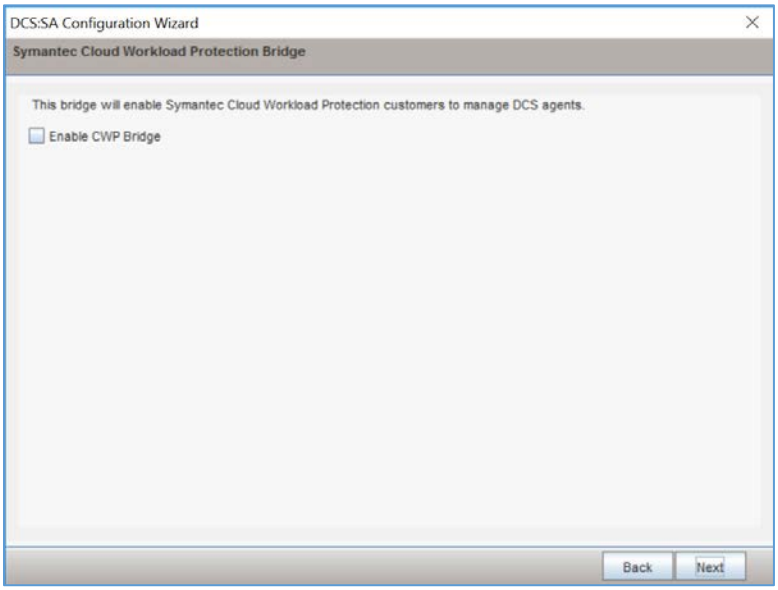
2099 11. Provide the information below, and click on **Next**:

2100 - **Agent port**: 443

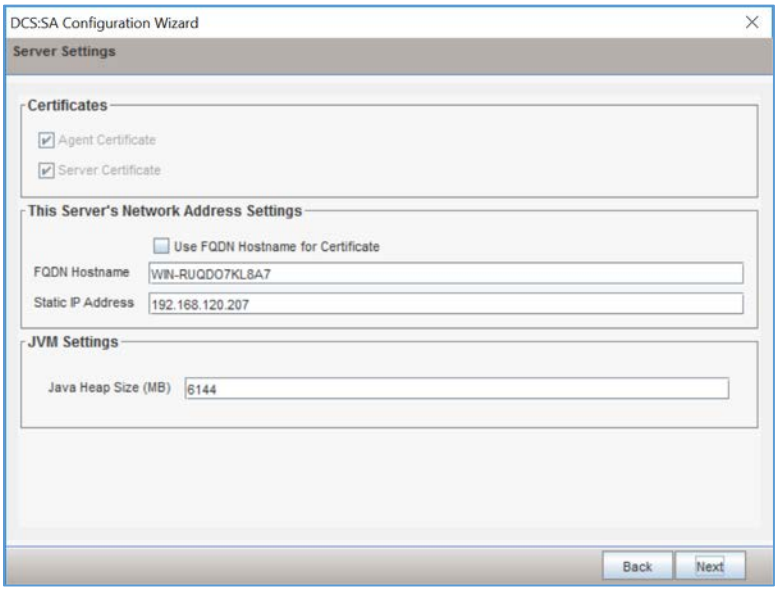
- **Bridge port**: 2443
- **Console port**: 4443
- **Web server administration port**: 8081
- **Web server shutdown port**: 8006



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

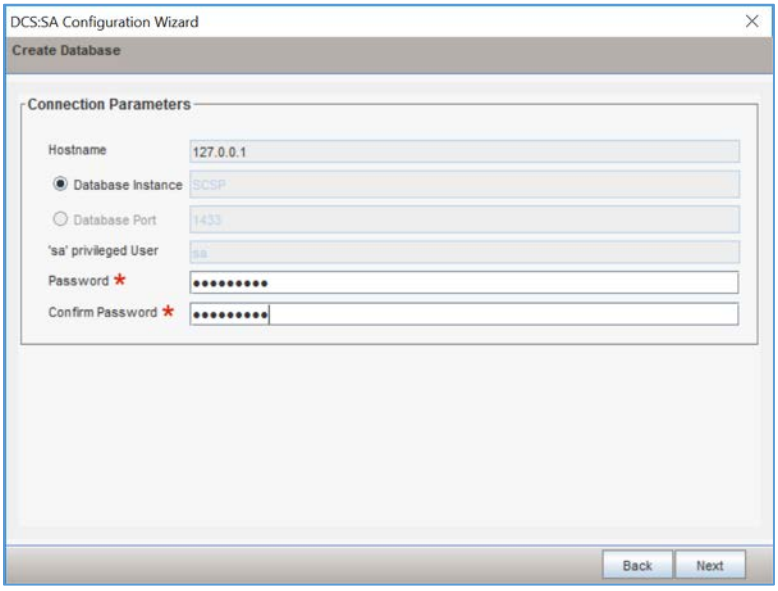


13. Verify settings for **FQDN Hostname** as **WIN-RUQDO7KL8A7**, **Static IP Address** as **192.168.120.207**, and **Java Heap Size** as **6144** and then click **Next**.



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

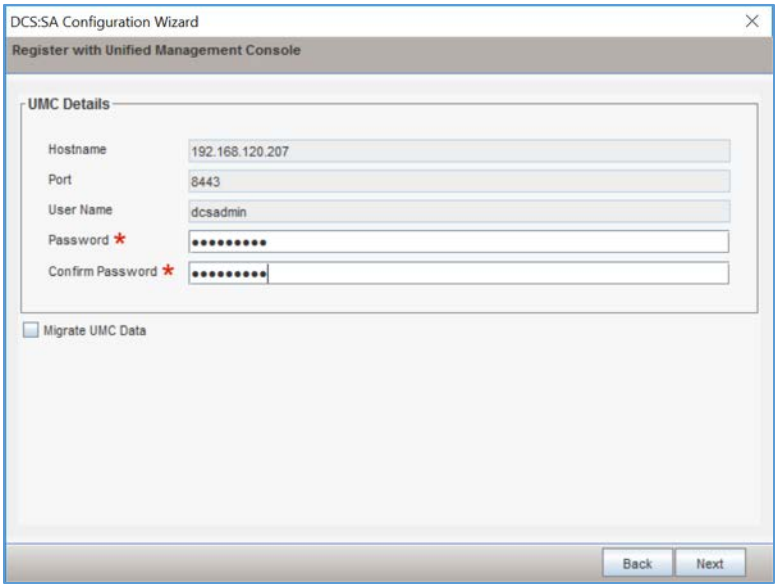
15. Click **Next**.



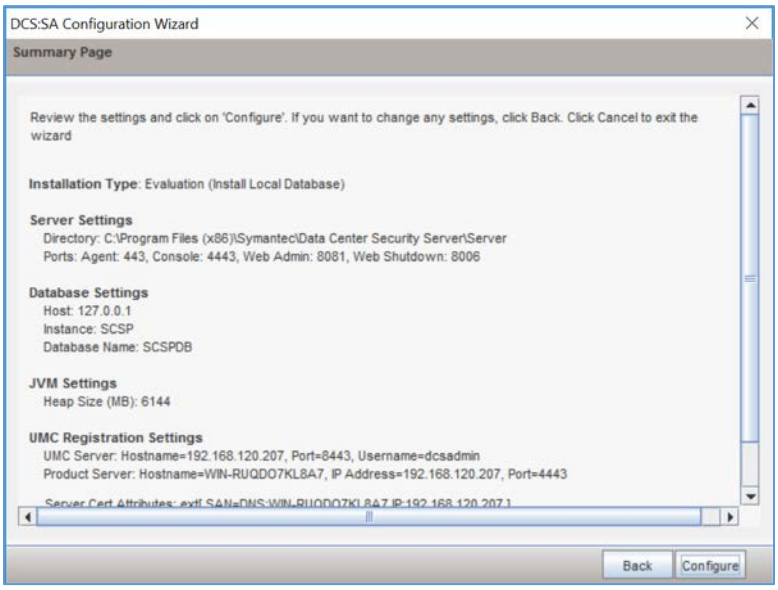
16. Verify **Unified Management Console** connection settings.

17. Create a password for **Unified Management Console** connection.

18. Click **Next**.

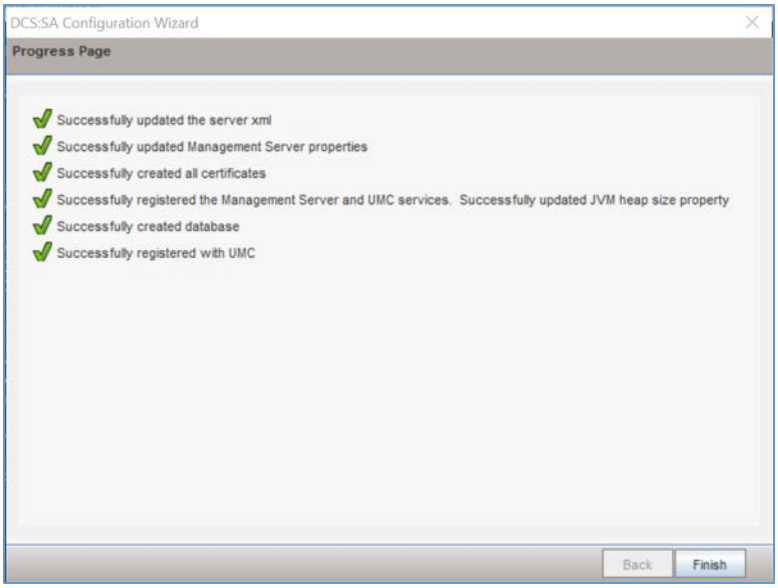


19. Verify configuration settings and click **Next**.

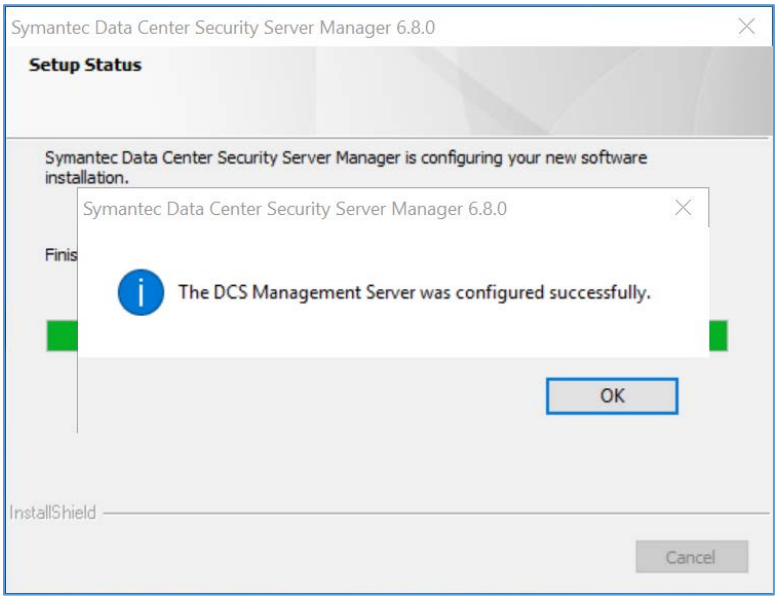


20. Wait for configuration process to complete.

21. Click **Finish**.

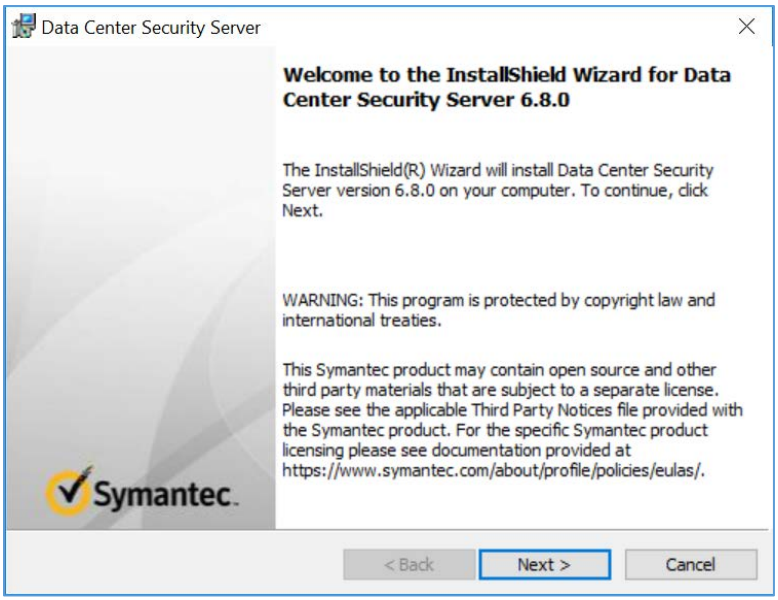


22. Wait for install to complete and click **OK**.



Symantec Datacenter Security Windows Agent Install

1. Run **agent.exe**.
2. Click **Next >**.



2128

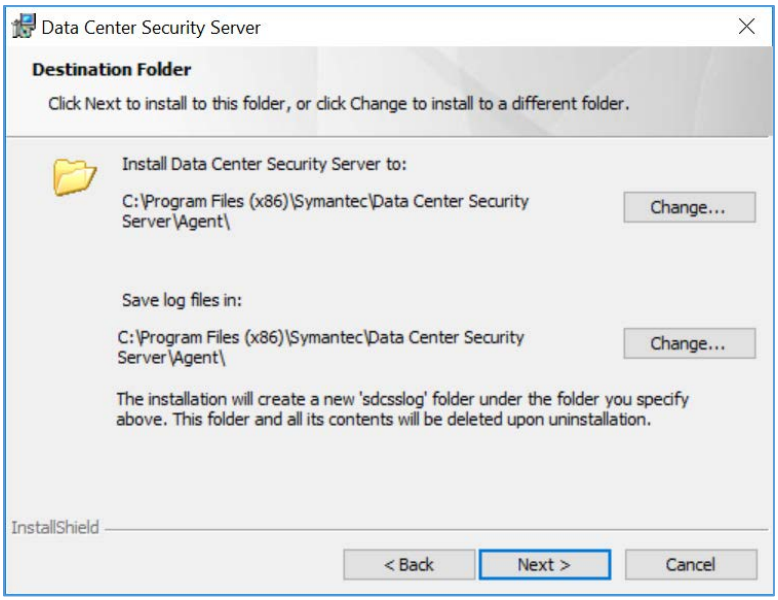
2129 3. Check **I accept the terms in the license agreement**.

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>**:

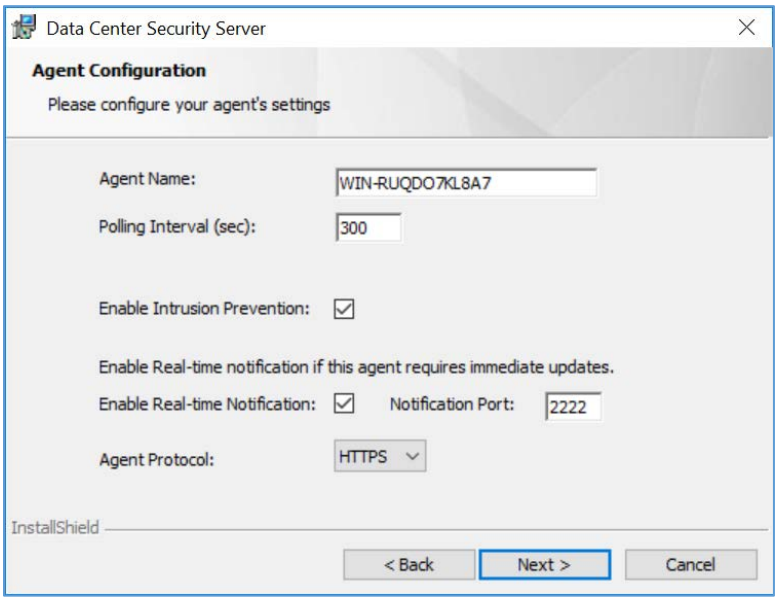
2136 - **Agent Name**: WIN-RUQDO7KL8A

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

2138 - Check **Enable Intrusion Prevention**

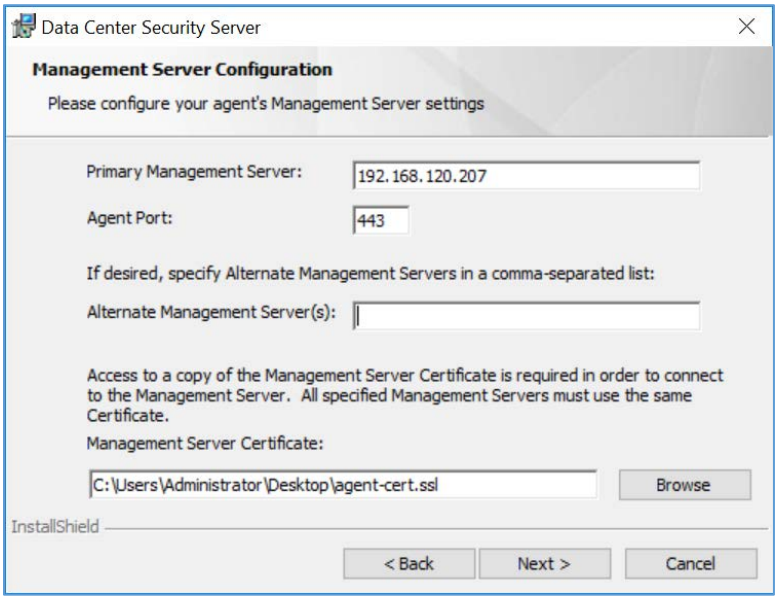
2139 - **Notification Port:** 2222

2140 - **Agent Protocol:** HTTPS

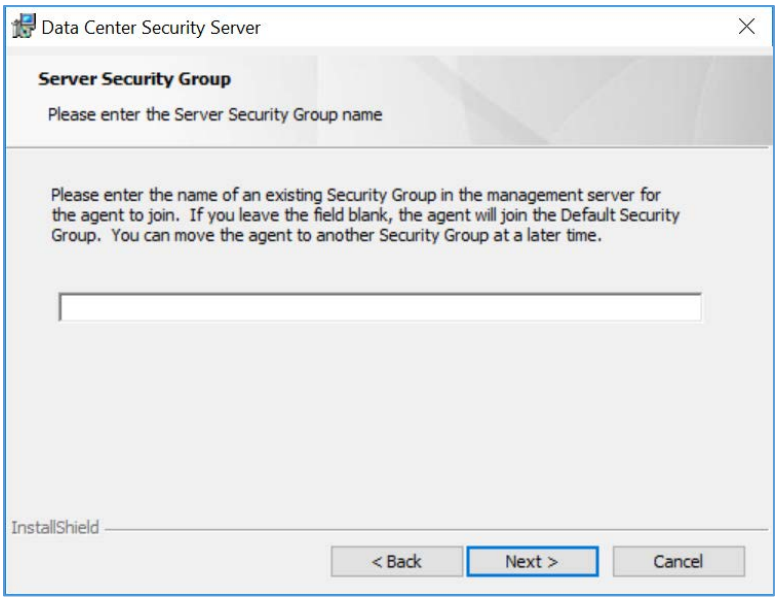


2141

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

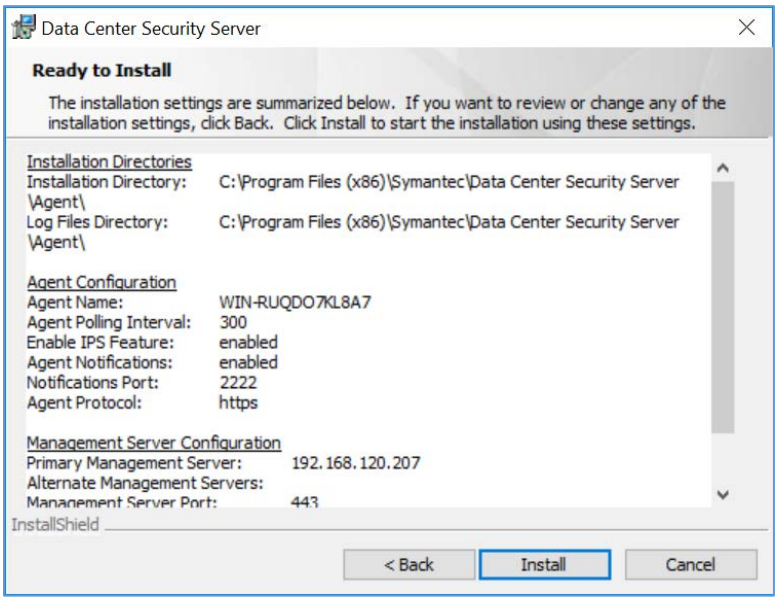


9. Specify a **Server Security Group** created through Symantec Datacenter Security Server or leave it blank to use the default security group.
10. Click **Next >**.



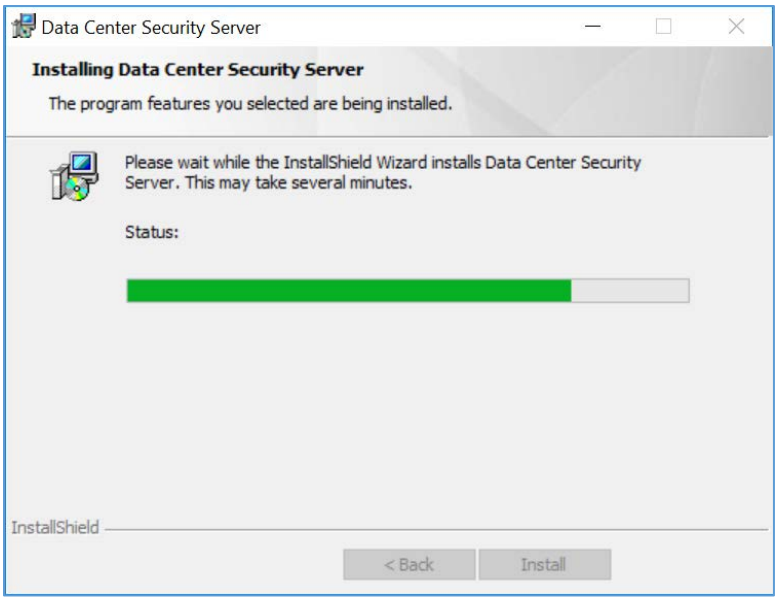
2151

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



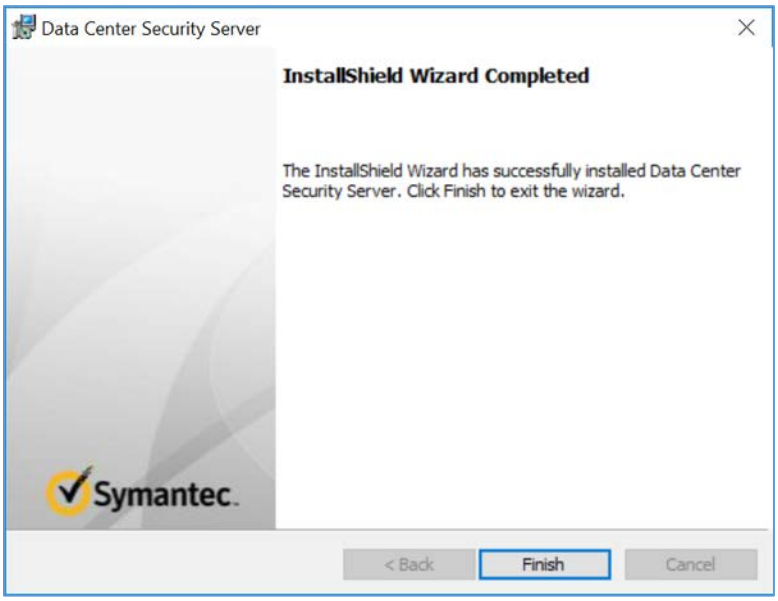
2153

2154 12. Wait for the installation process to complete.



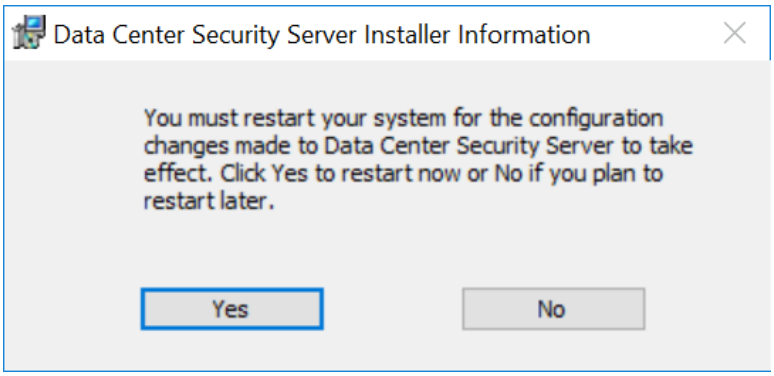
2155

2156 13. Click **Finish**.



2157

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



2.8.2 Symantec Endpoint Protection

Symantec Endpoint Protection is an agent-based security solution that provides antivirus, intrusion prevention, application whitelisting, and other capabilities. For this project Symantec SEP is used to protect endpoints from malicious software and integrates with Symantec Endpoint Detection and Response to detect suspicious behavior.

System Requirements

CPU: 4

Memory: 8GB RAM

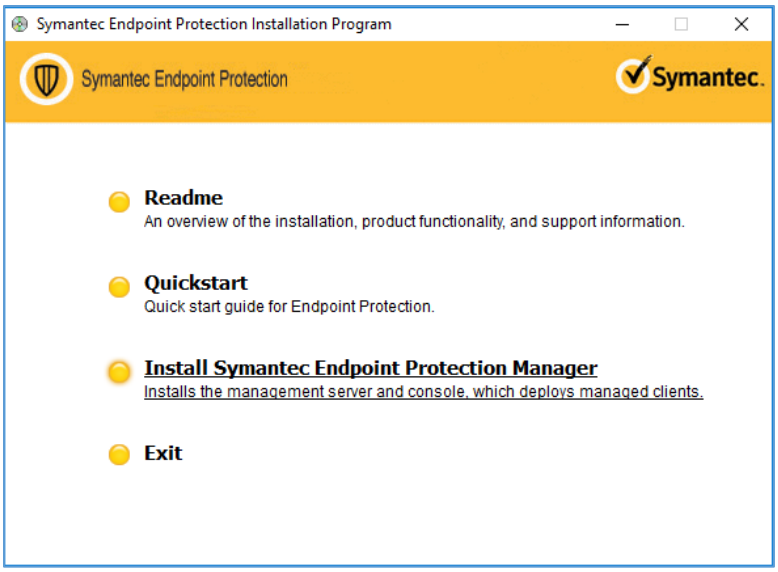
Storage: 240GB (thin provisioned)

Operating System: Microsoft Windows Server 2016

Network Adapter: VLAN 1901

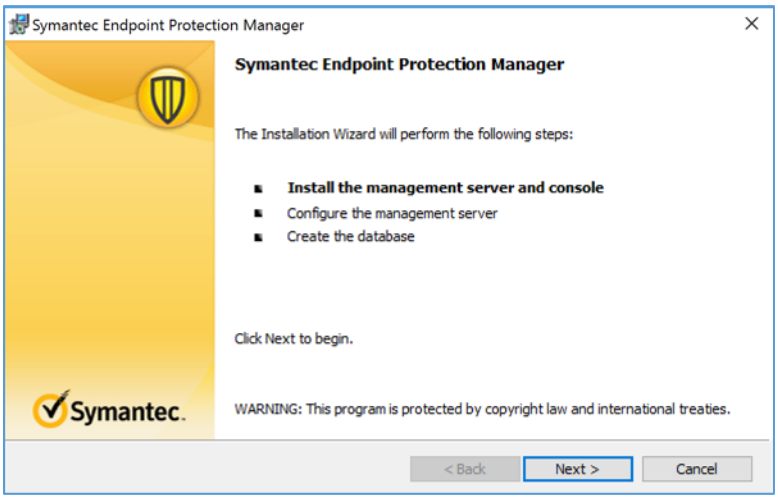
Symantec Endpoint Protection Manager Installation

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



2174

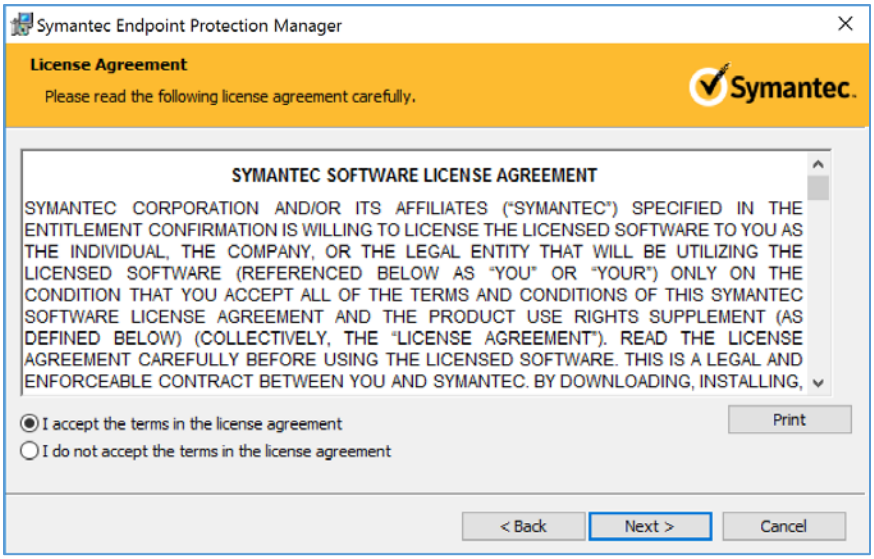
2175 3. Proceed through the install wizard by clicking **Next >.**



2176

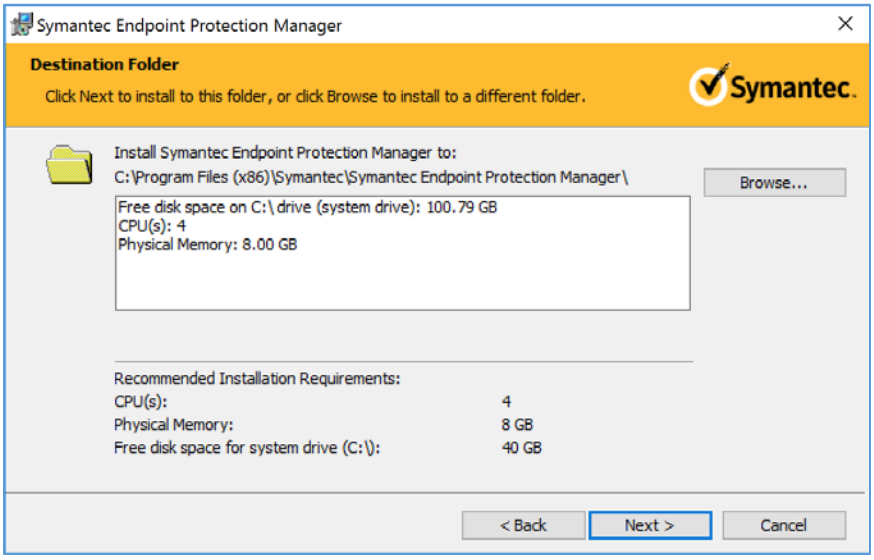
2177 4. Check **I accept the terms in the license agreement**.

2178 5. Click **Next >**.



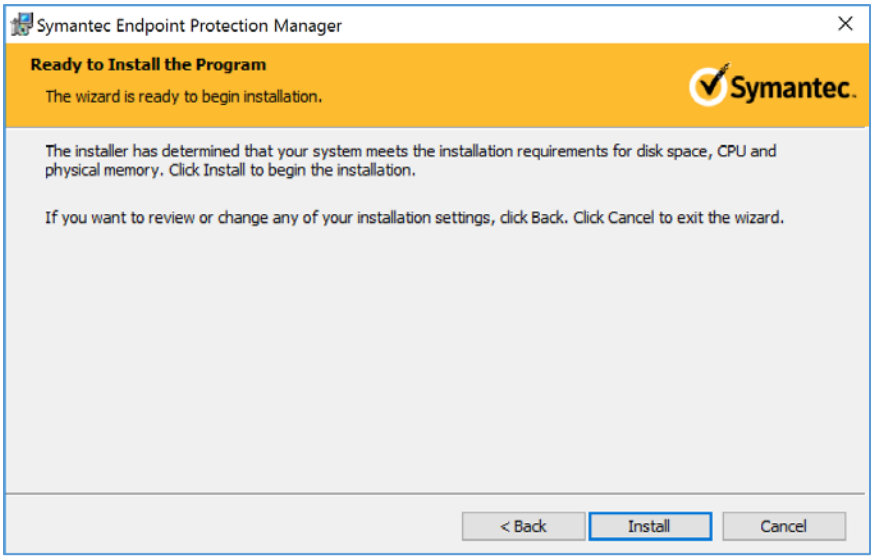
2179

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*.



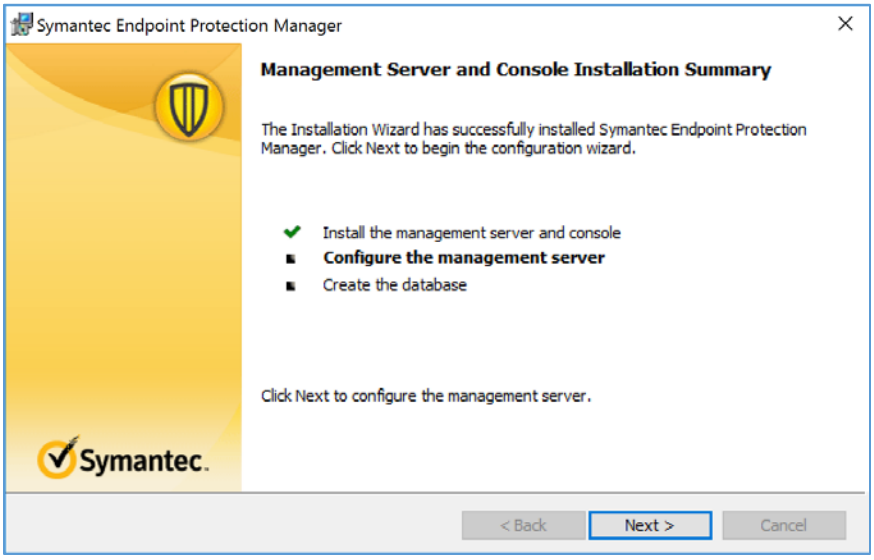
2182

2183 7. Select **Install**.



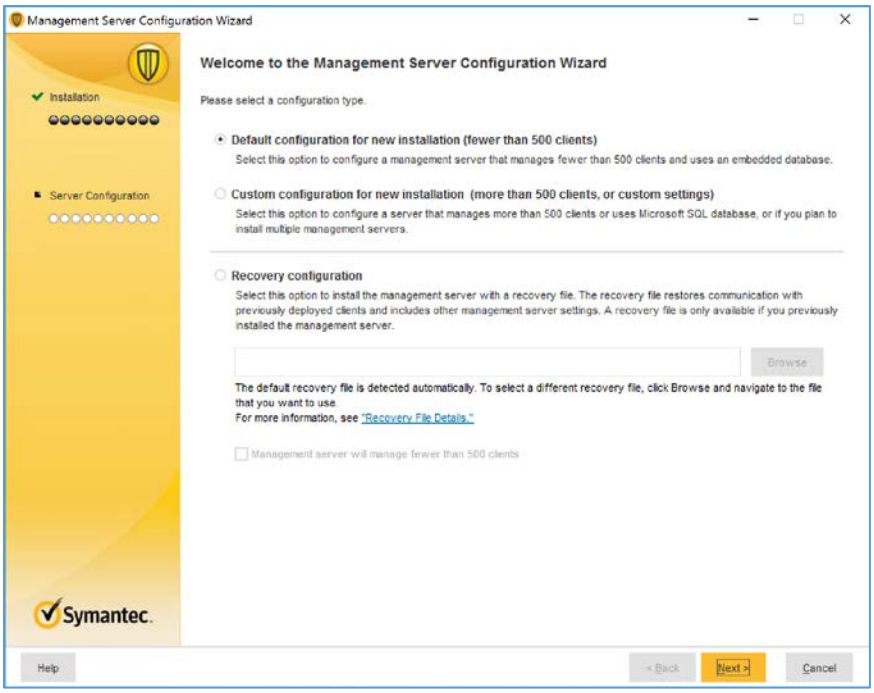
2184

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

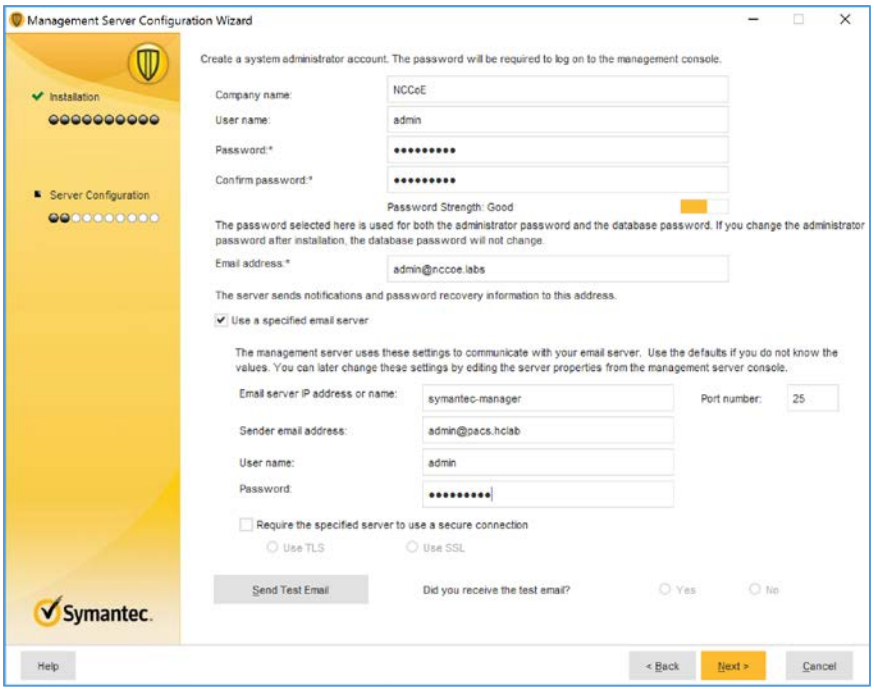


2187

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

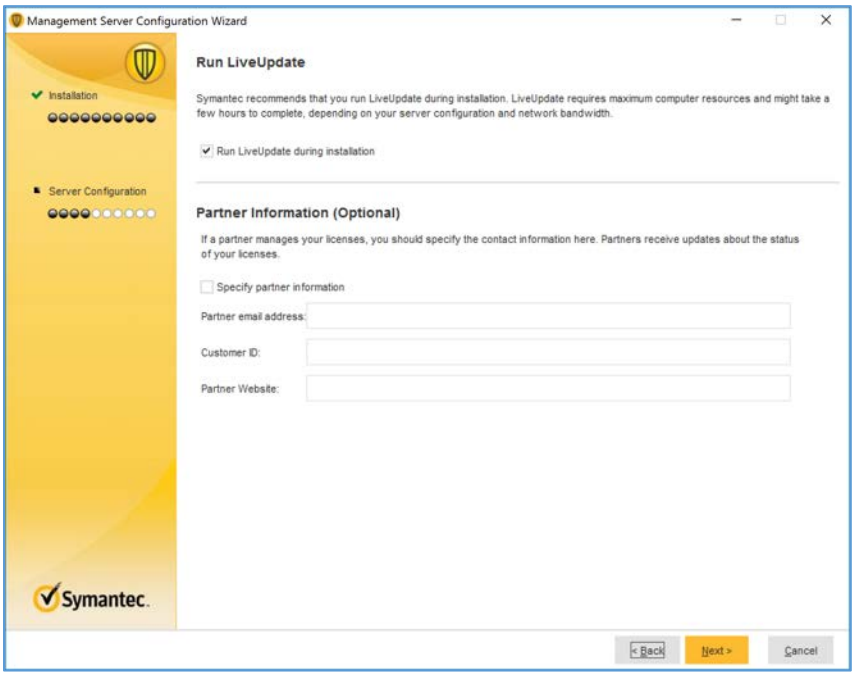


10. Provide the following information and click **Next>**.
    - **Company Name**: NCCoE
    - **User name**: admin
    - **Password**: ********
    - **Confirm password**: ********
    - **Email address**: admin@nccoe.labs



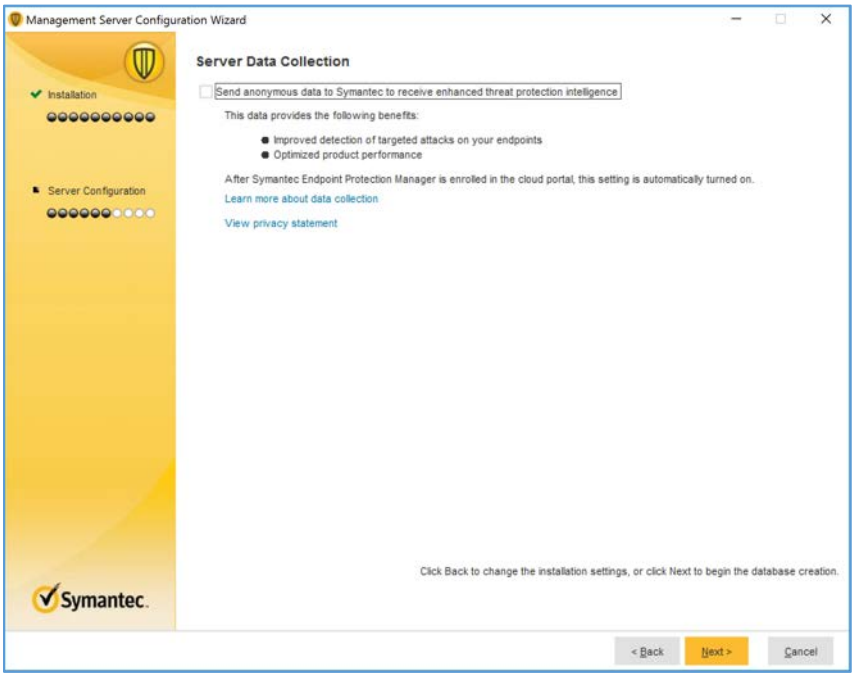
2196

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

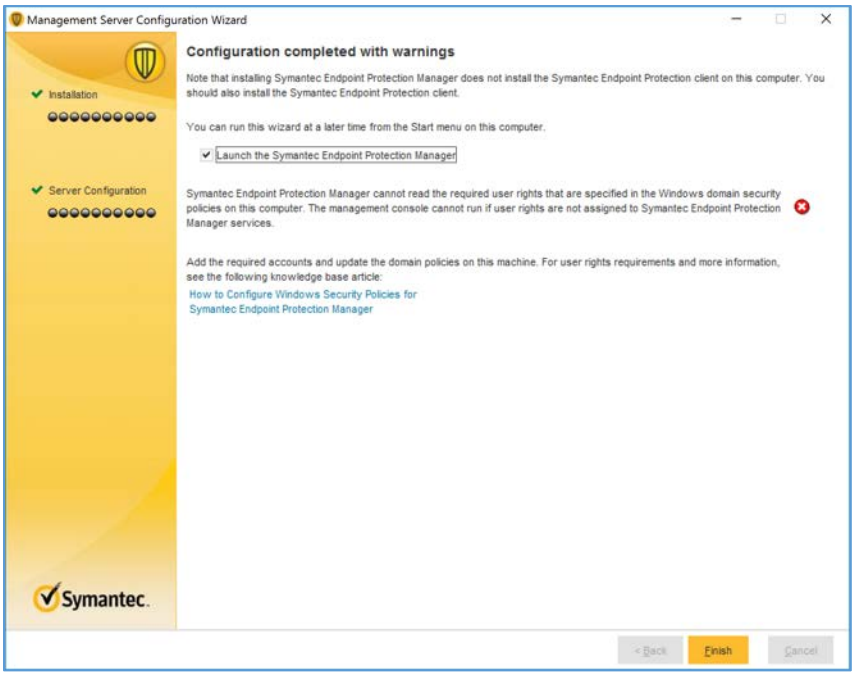


2198

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



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



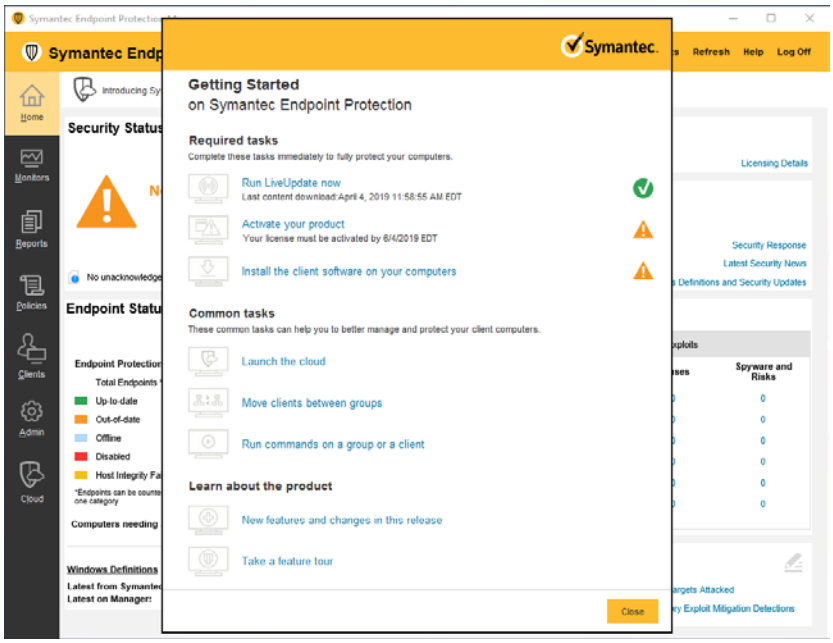
2204

2205 **Symantec Endpoint Protection Host Windows Installation**

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

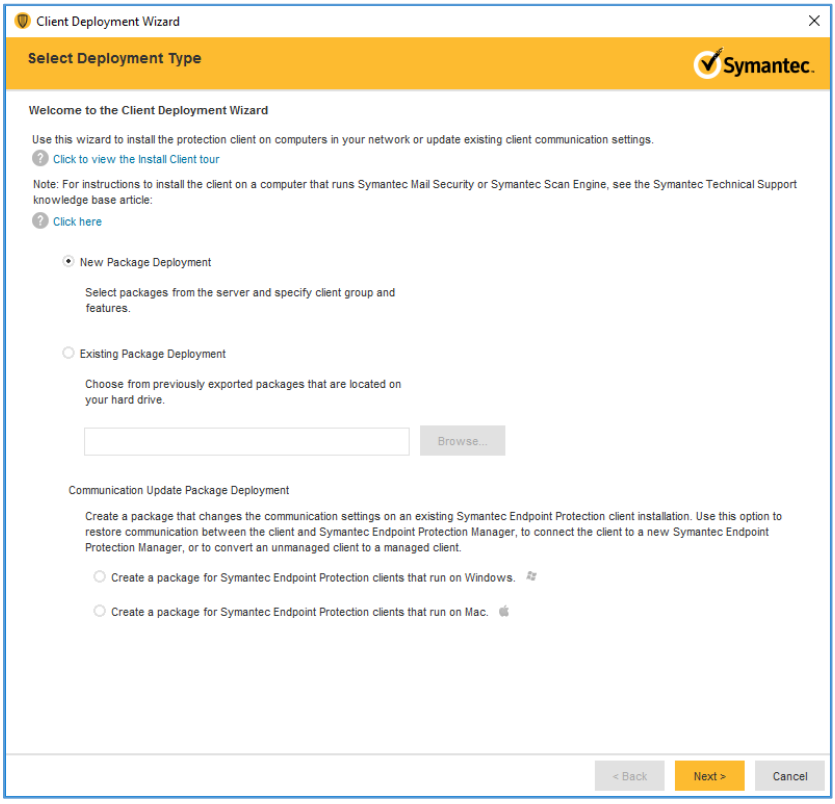
2207

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



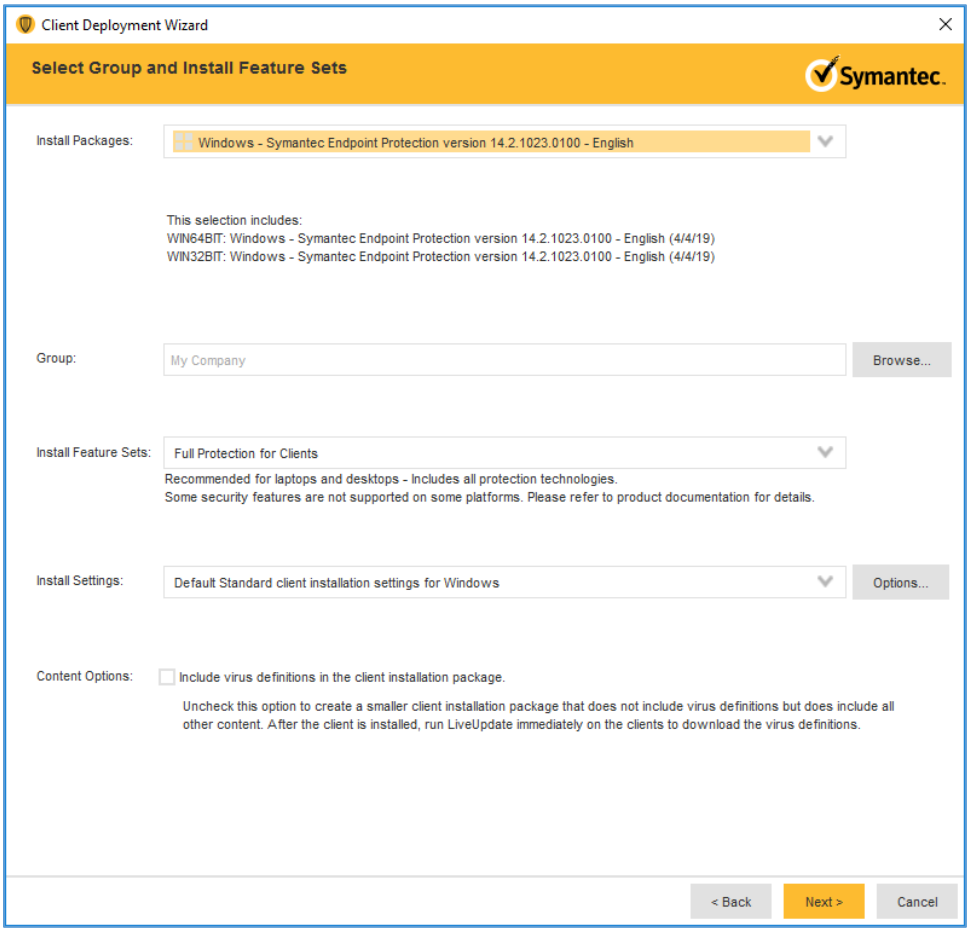
2209

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

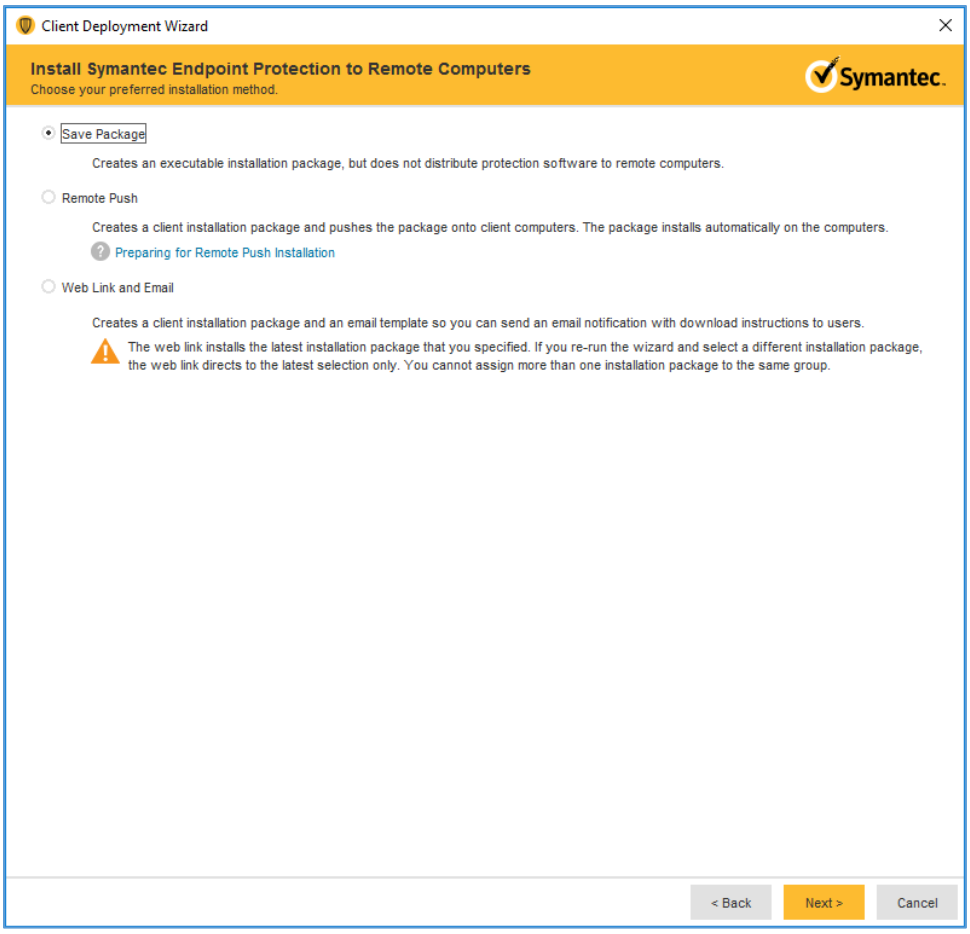


2211

4. Confirm the settings Install Packages: **Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English**, Group: **My Company**, Install Feature Sets: **Full Protection for Clients**, Install Settings: **Default Standard client installation settings for Windows**. Click **Next >**.

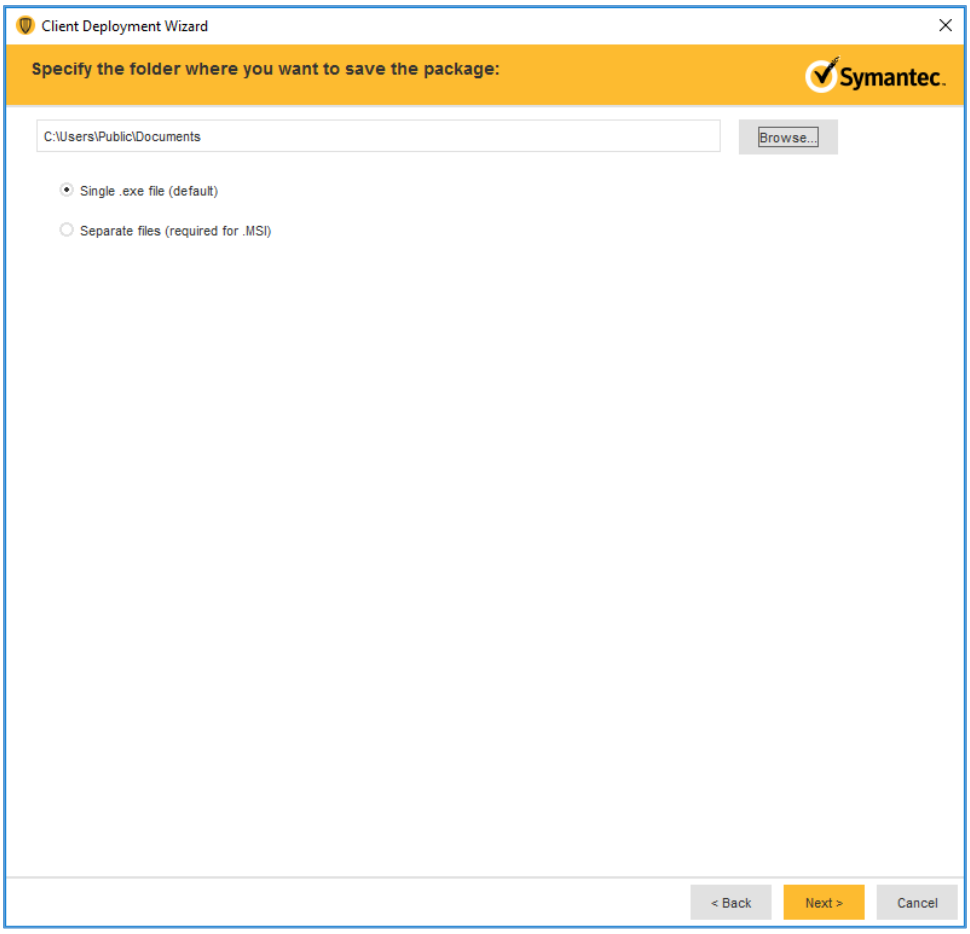


5. Confirm that **Save Package** is selected and click **Next >**.



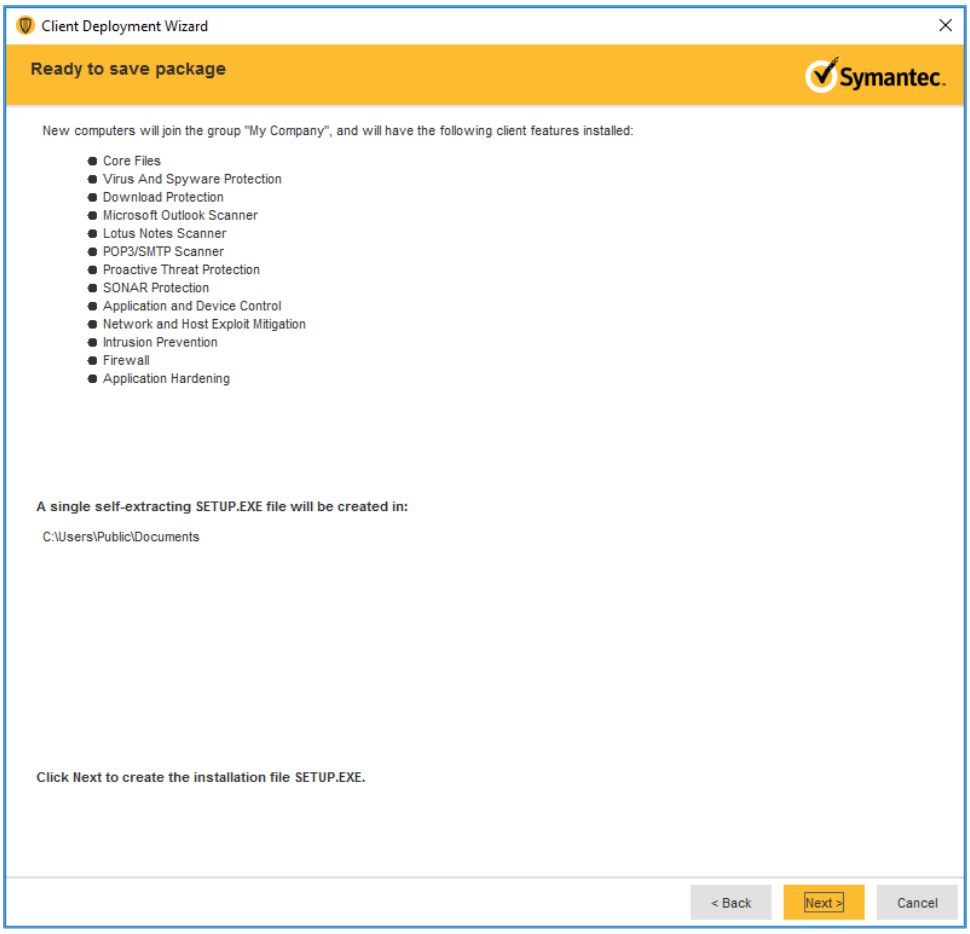
2217

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 >**.



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

9. Launch the executable file and follow the prompts to install Symantec Endpoint Protection.

2.9 Data Security

No specific solution was implemented in the NCCoE lab to address data-at-rest encryption.

The NCCoE lab used several different solutions to address data-in-transit encryption. As described in Section 2.6.2, DigiCert PKI, the lab implements SSL/TLS encryption using DigiCert-issued certificates. Communications between modalities and clinical systems are secured using HIP, as described in Section 2.7.3, Tempered Networks Identity Defined Networking (IDN).

2.10 Secure Remote Access

2.10.1 TDi Technologies ConsoleWorks

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

System Requirements

CPU: 1

Memory: 8 GB RAM

Storage: 40 GB

Operating System: CentOS 7

Network Adapter: VLAN 1097

TDi ConsoleWorks Installation

The TDi ConsoleWorks installation in this PACS environment replicates the installation in the Wireless Infusion Pumps project. For detailed installation guidance, please refer to the Section 2.1.8 *TDi ConsoleWorks External Remote Access* in NIST SP 1800-8C, *Securing Wireless Infusion Pumps* [19].

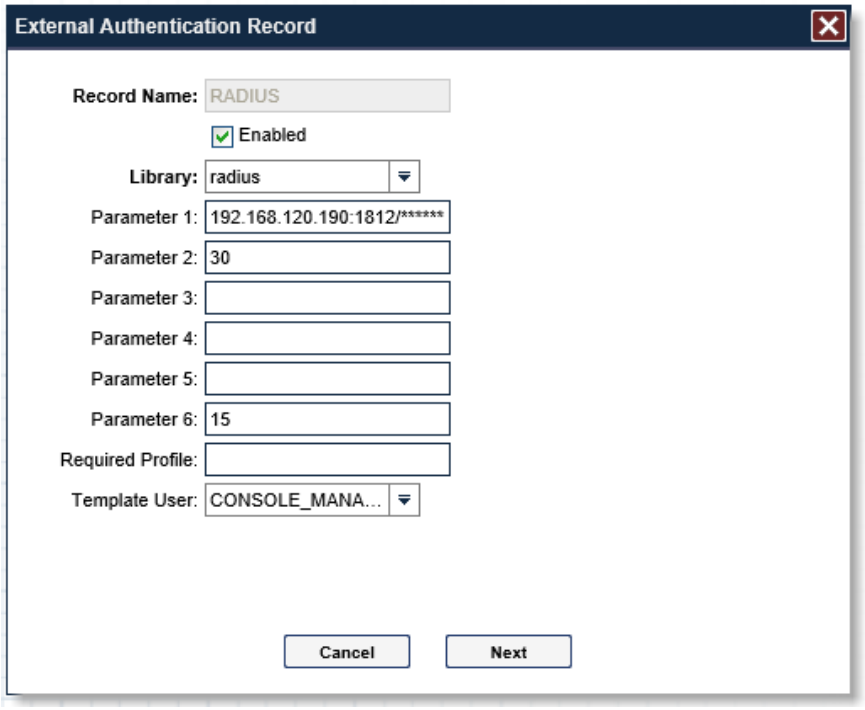
TDi ConsoleWorks Radius Authentication Configuration

In our project, we integrated TDi ConsoleWorks with the Symantec VIP, for two-factor authentication. This section explains how to enable external authentications for ConsoleWorks. In the next section we explain how we configured Symantec VIP to integrate with ConsoleWorks.

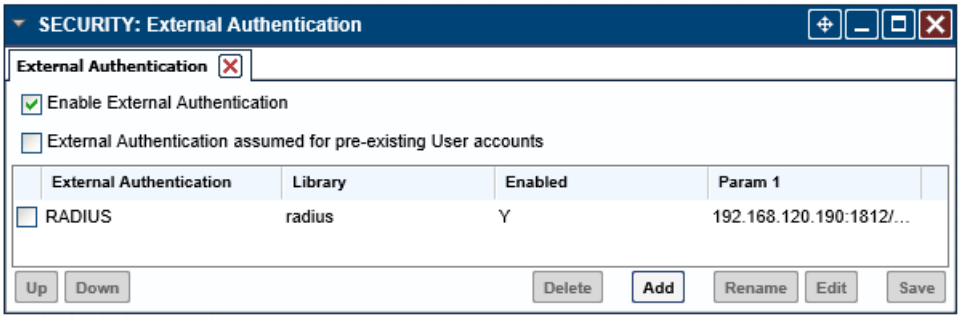
1. Download *extern_auth_radius.so* file from ConsoleWorks support site [20].
2. Move *extern_auth_radius.so* file to */opt/ConsoleWorks/bin* directory.
3. Restart ConsoleWorks by executing *cw_stop* and *cw_start* scripts located in the */opt/ConsoleWorks/bin* directory.
4. From the ConsoleWorks web interface, navigate to **Security** and click **External Authentication**.
5. Click **add** to create a new external authentication source.
6. Fill out the required fields. Below is the setup we used:
   - **Record Name**: Radius
   - Ensure **Enable** is checked
   - For **Library** select **radius**

- **Parameter 1**: 192.168.120.190:1812/*******
- **Parameter 2**: 30
- **Parameter 6**: 15
- **Template User**: CONSOLE_MANAGER

7. Continue through the prompt by clicking **Next**; click **Save** on the final prompt.



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



2.10.2 Symantec Validation and ID Protection (VIP)

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

System Requirements

CPU: 4

Memory: 8192MB RAM

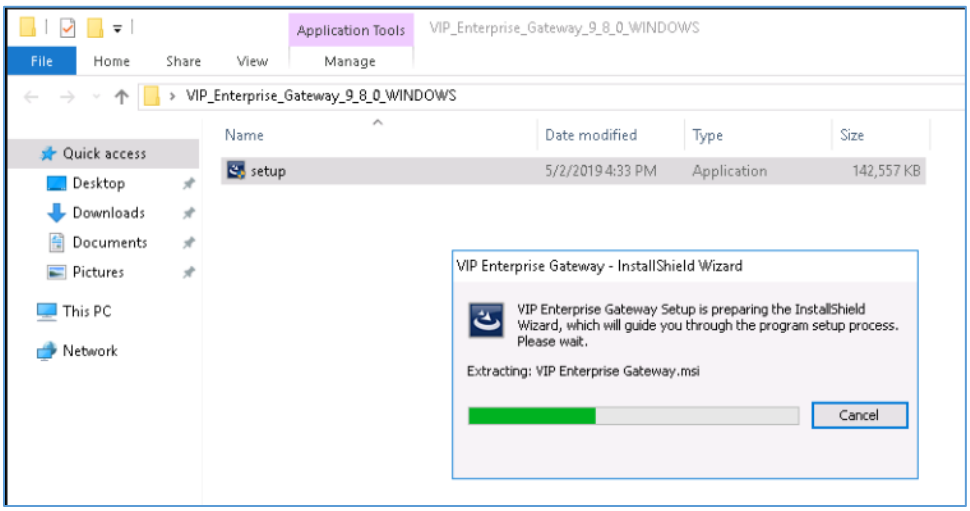
Storage: 240GB (thin provisioned)

Operating System: Microsoft Windows Server 2016

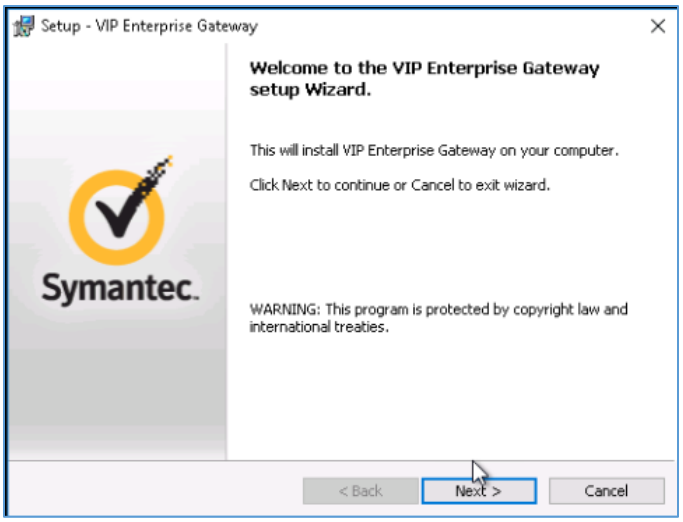
Network Adapter: VLAN 1201

Symantec VIP Installation

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



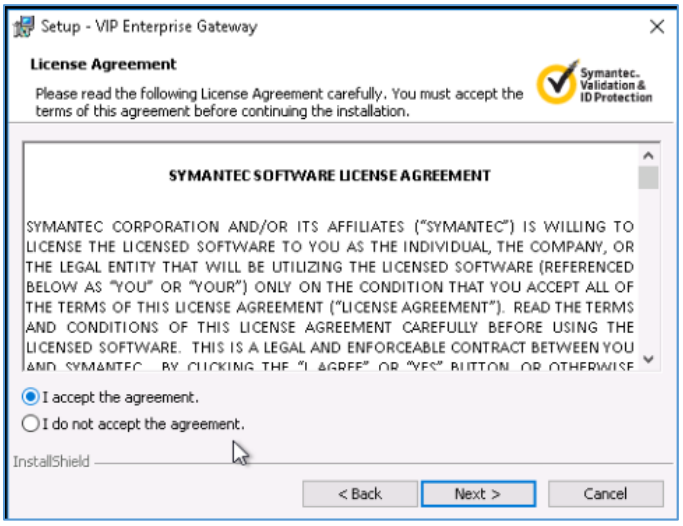
2. Proceed through the install wizard by clicking **Next >**.



2281

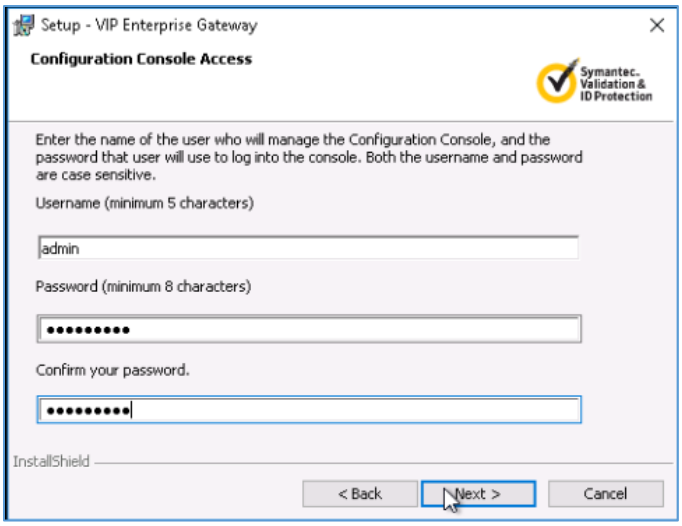
2282 3. Check **I accept the agreement**.

2283 4. Click **Next >**.



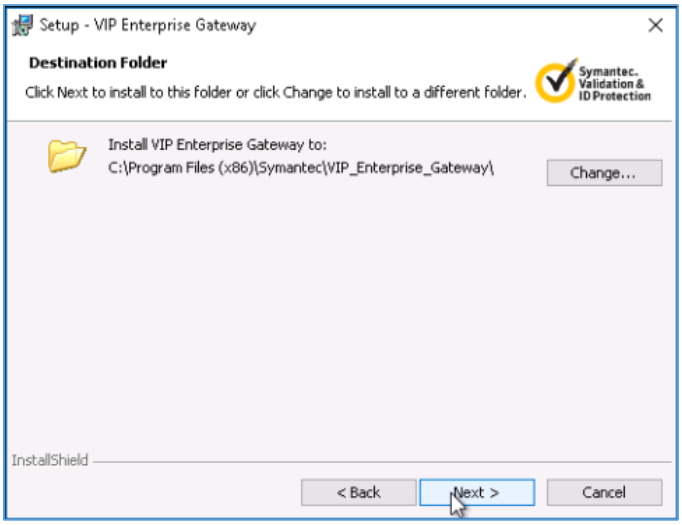
2284

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



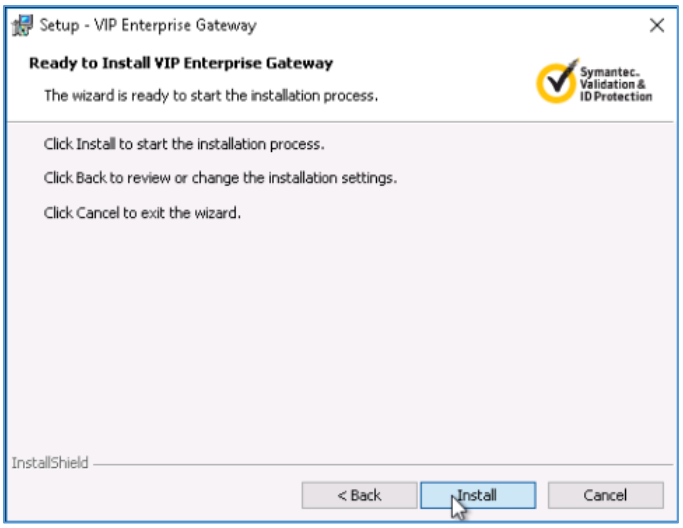
2286

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



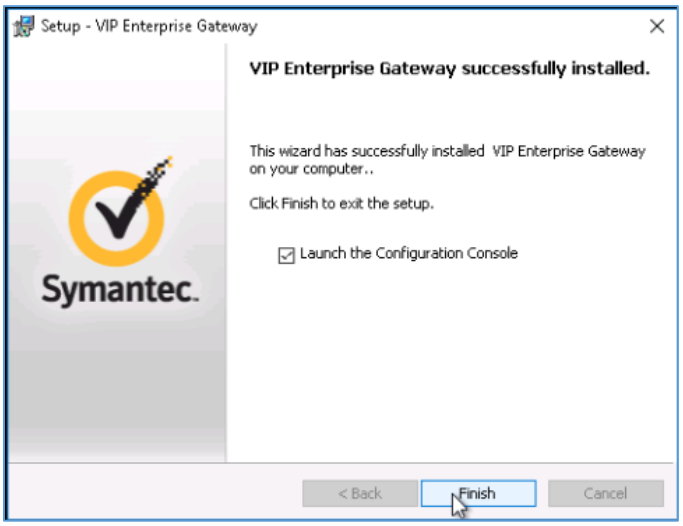
2288

2289 7. Click **Install**.



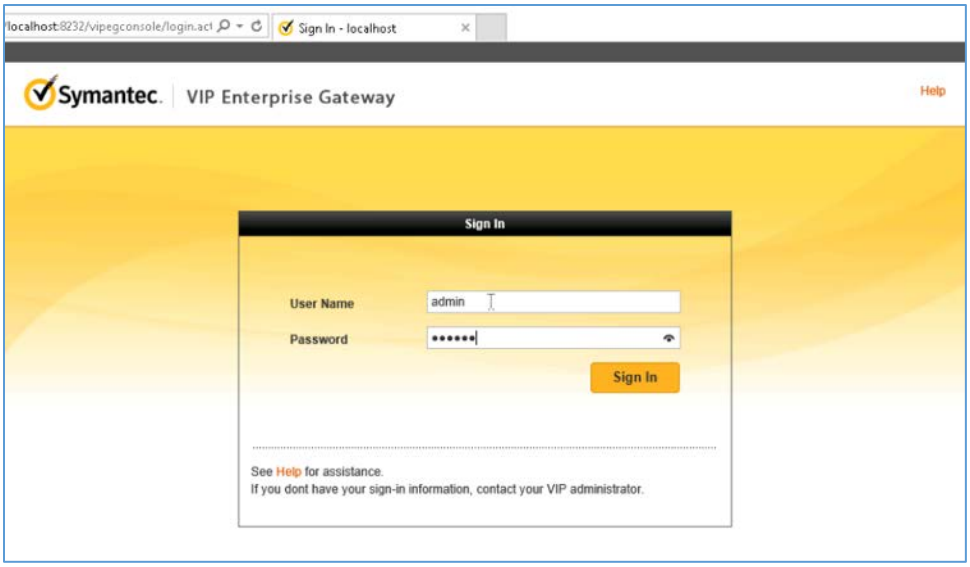
2290

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



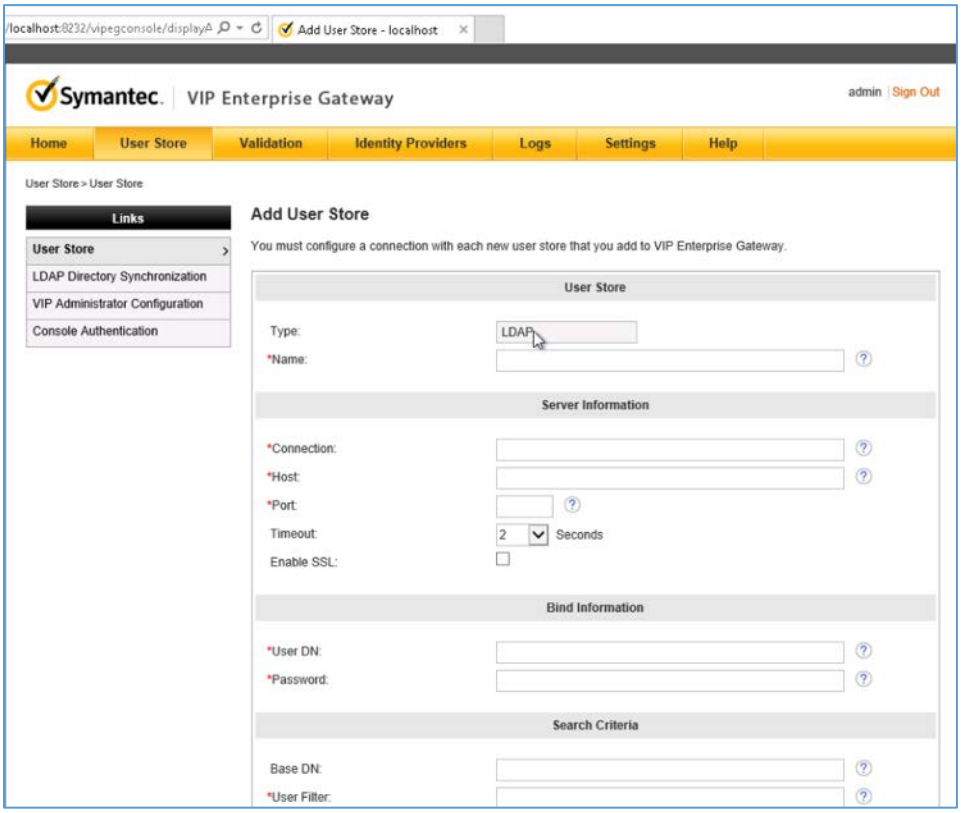
2292

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

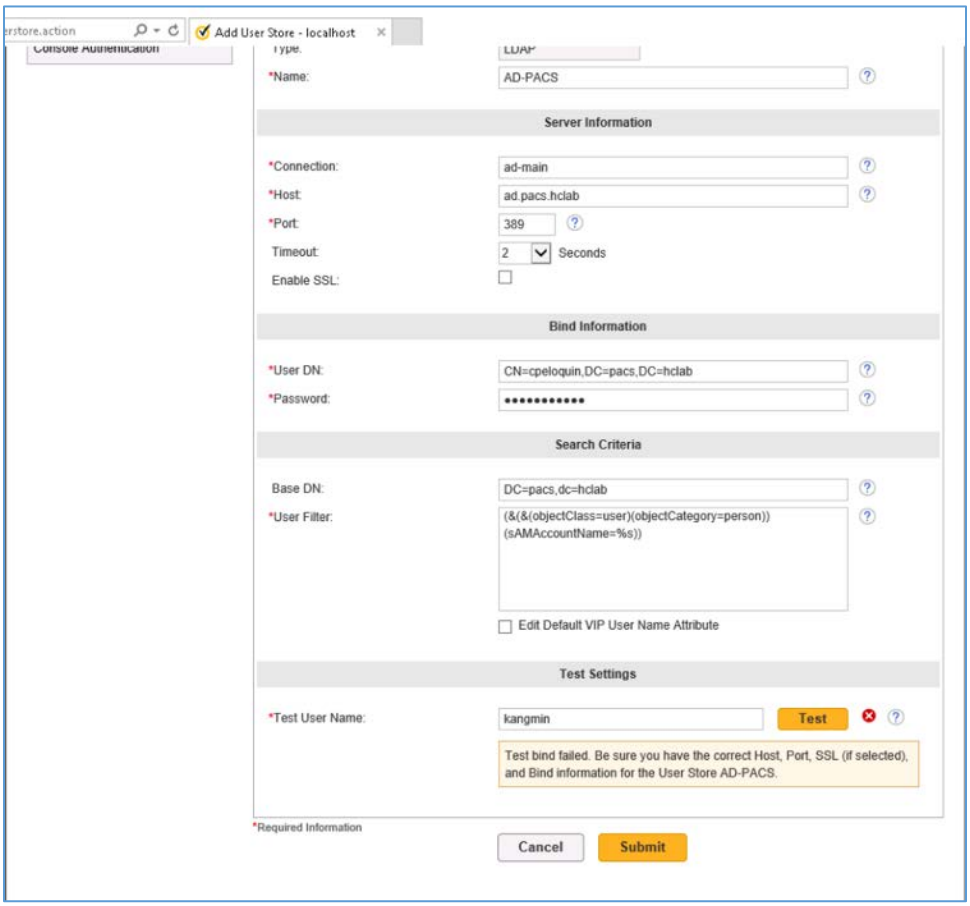
2296 10. Select **User Store** from the menu bar.



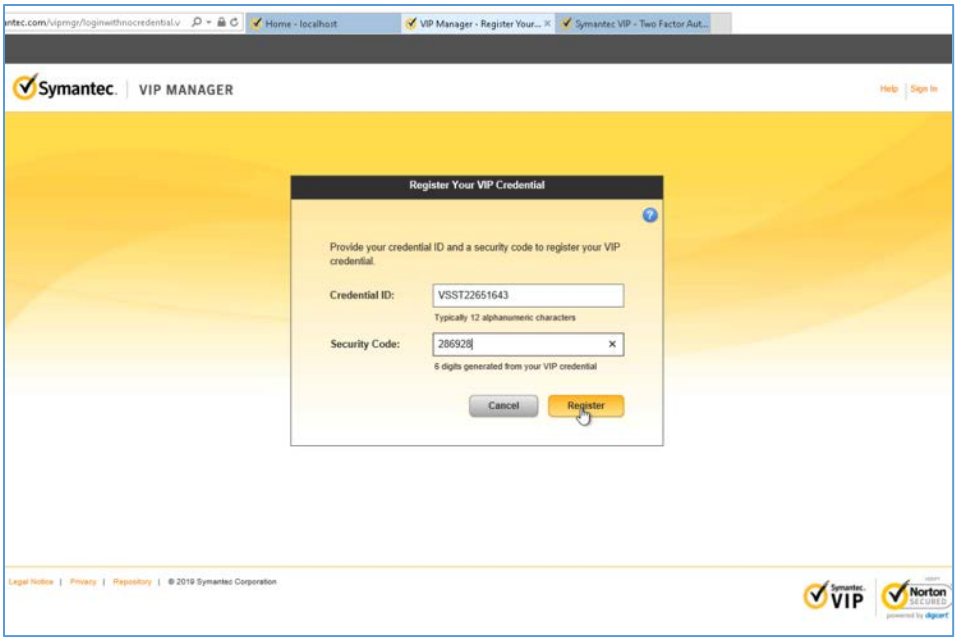
2297

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

- **Name**: AD PACS
- **Connection**: ad-main
- **Host**: ad.pacs.hclab
- **Port**: 389
- **User DN**: CN=symantec, DC=pacs, DC=hclab
- **Password**: *********
- **Base DN**: DC=pacs, DC=hclab
- **User Filter**: (&(&objectClass=user)(objectCategory=person))(sAMAcountName=%s))

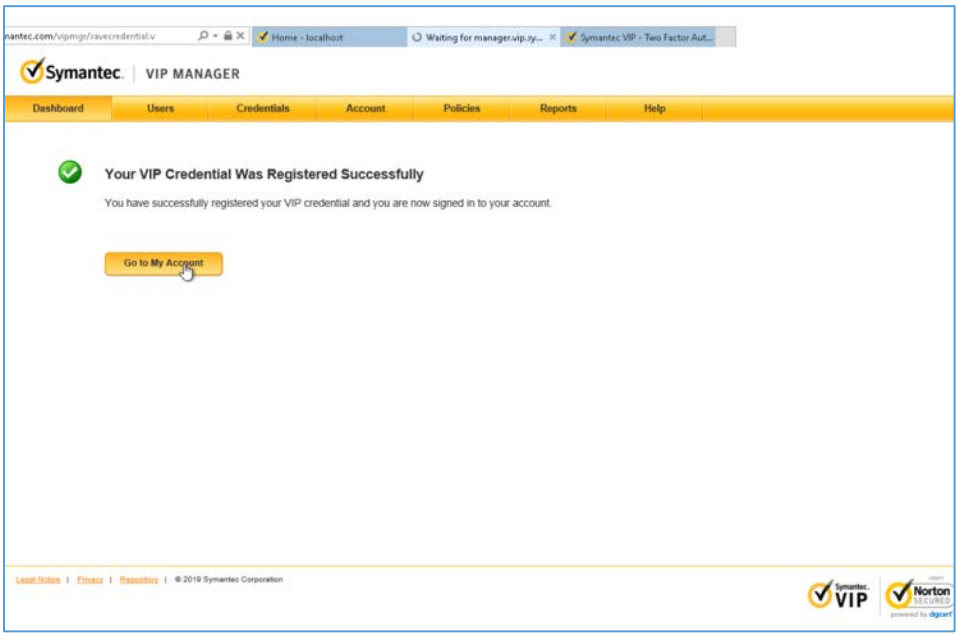


12. Log into VIP Manager by navigating to *https://manager.vip.symantec.com/vipmgr*. Use the account provided by Symantec.
13. Select **Register Your VIP Credential**. Provide **the Credential ID** and **Security Code** of your credentials. Credentials can be downloaded by navigating to https://vip.symantec.com/.



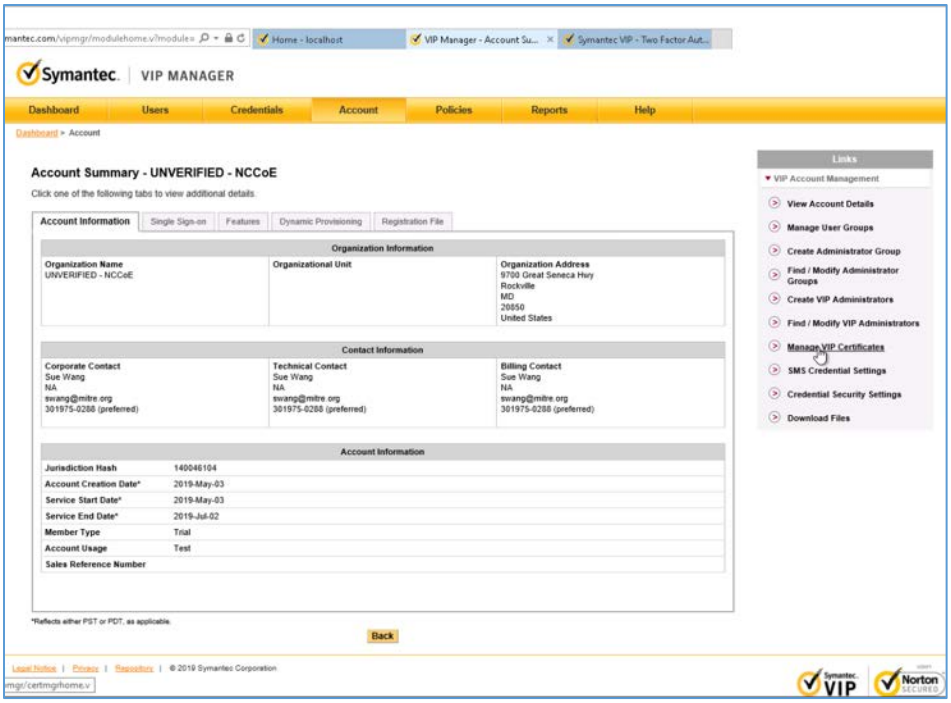
2312

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



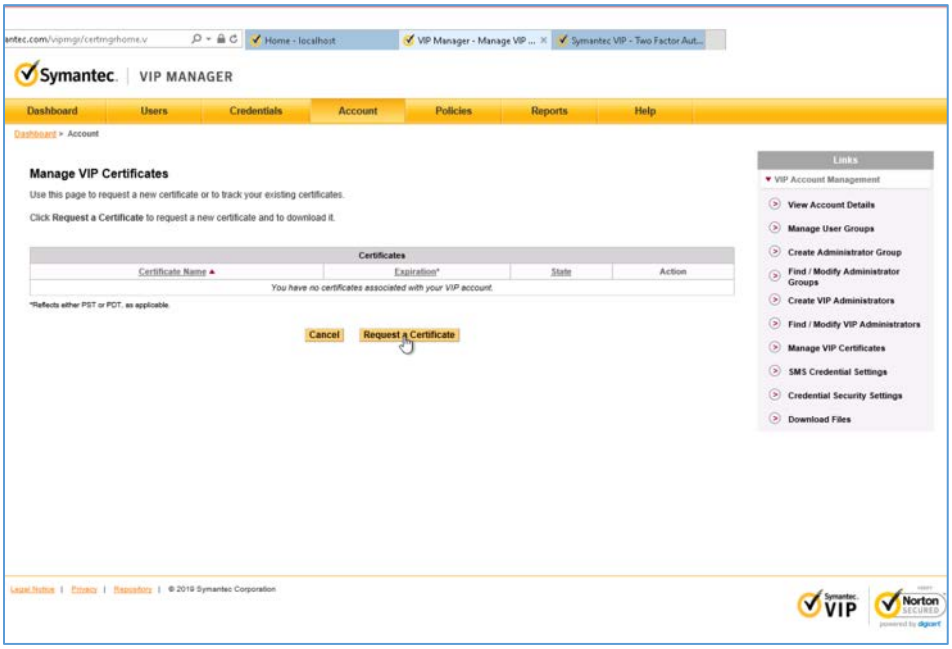
2314

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



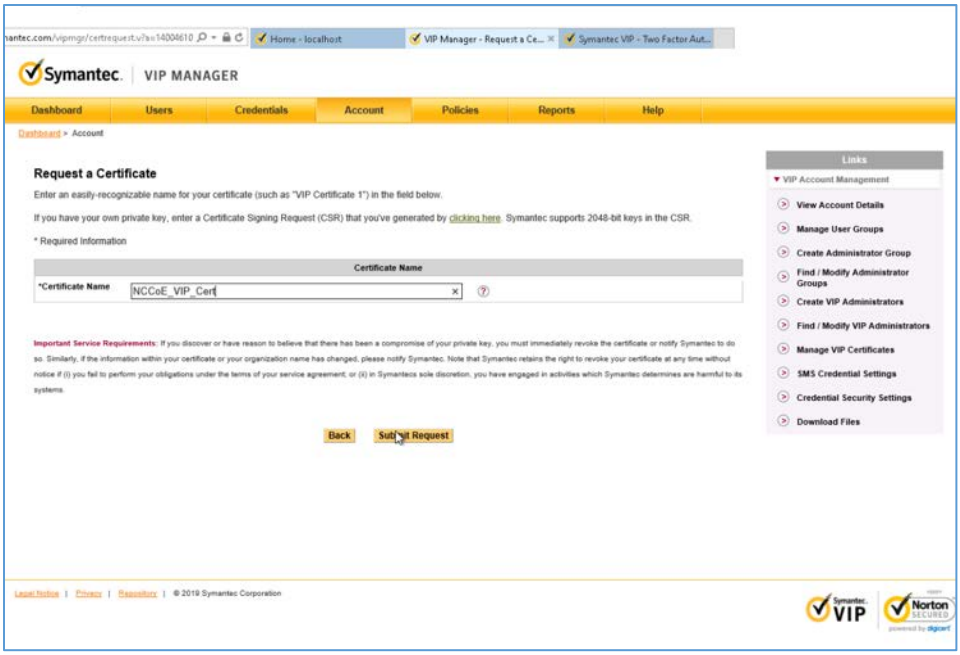
2316

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



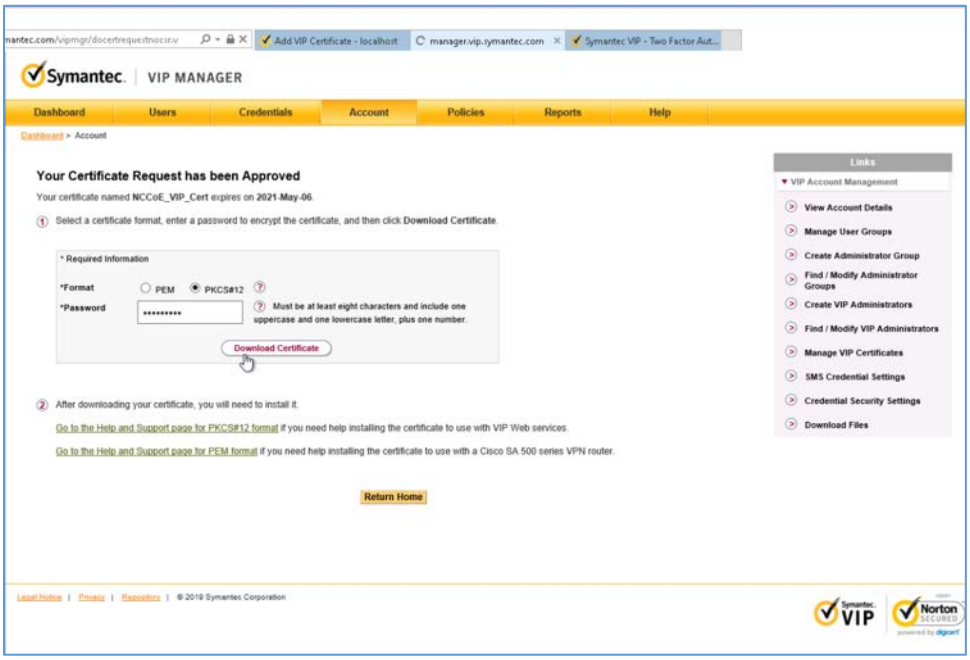
2318

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



2320

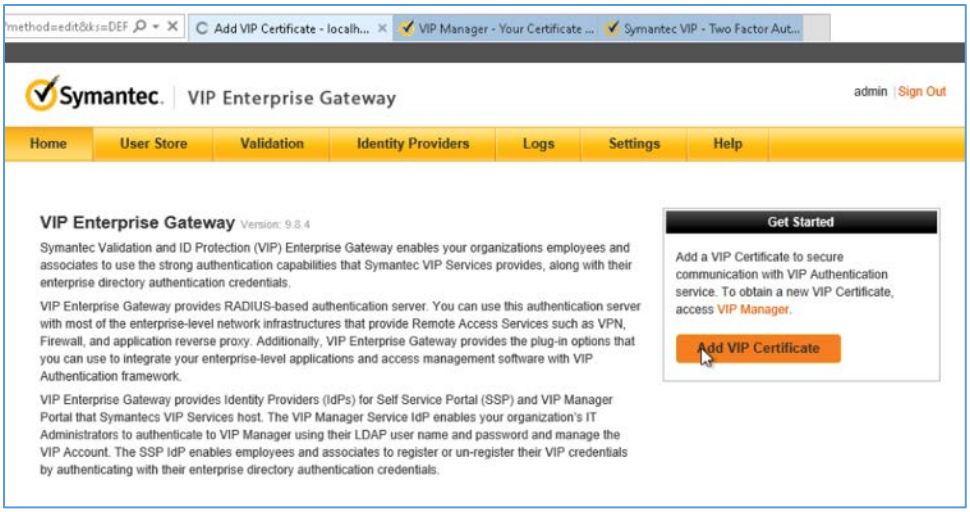
2321 18. Select **PKCS#12 format** and create a password for the requested certificate. Then select **Download**
2322 **Certificate**.



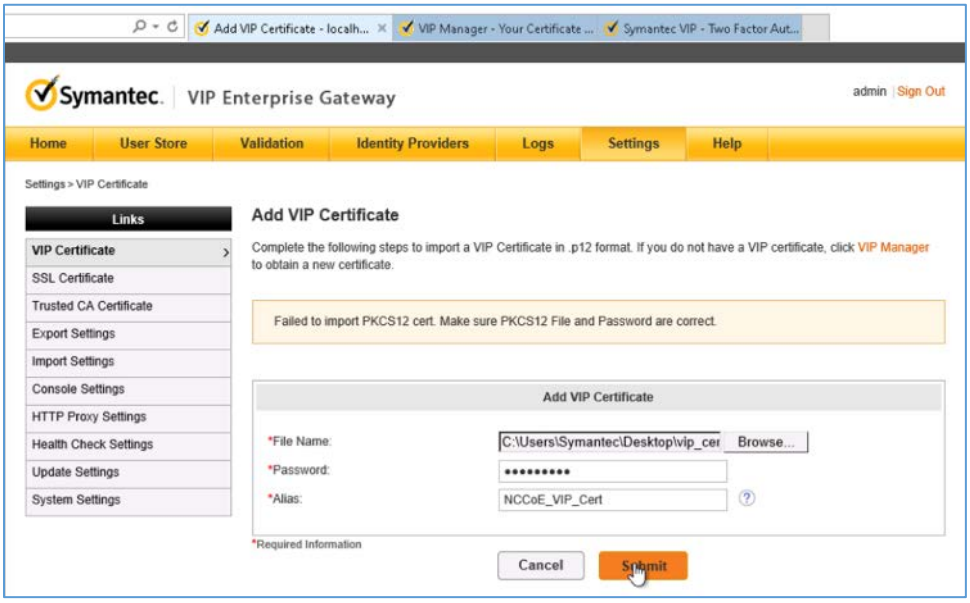
2323

2324 19. Save the certificate on the Symantec VIP local machine.

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



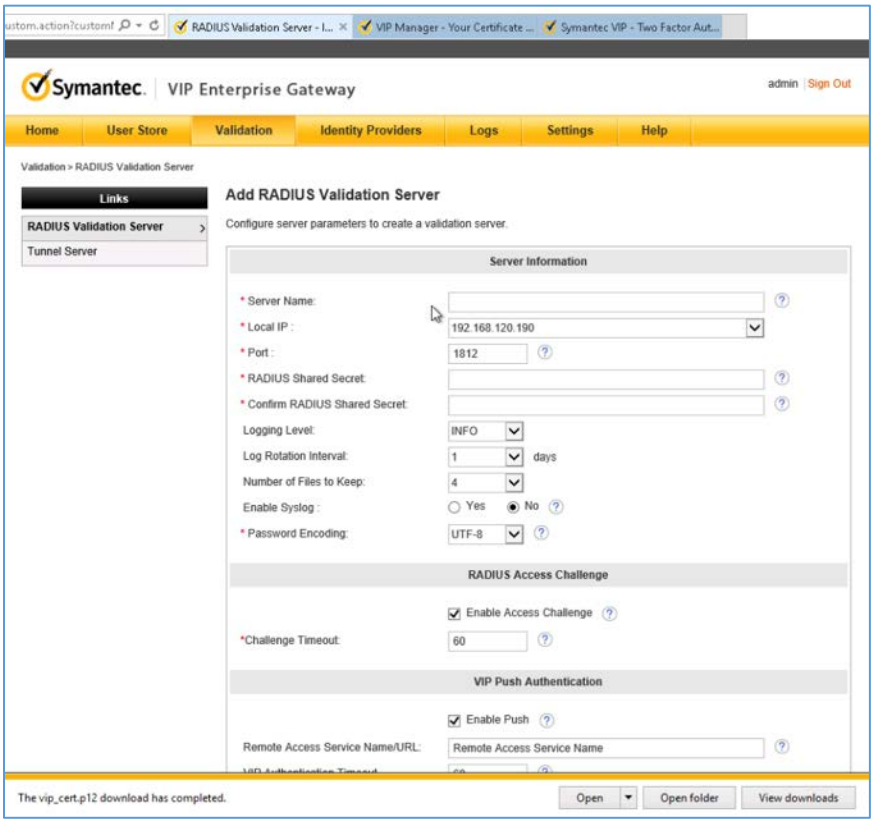
21. Select **Browse** and upload the certificate from the previous step. Enter the correct password and alias for the certificate, then click **Submit**.



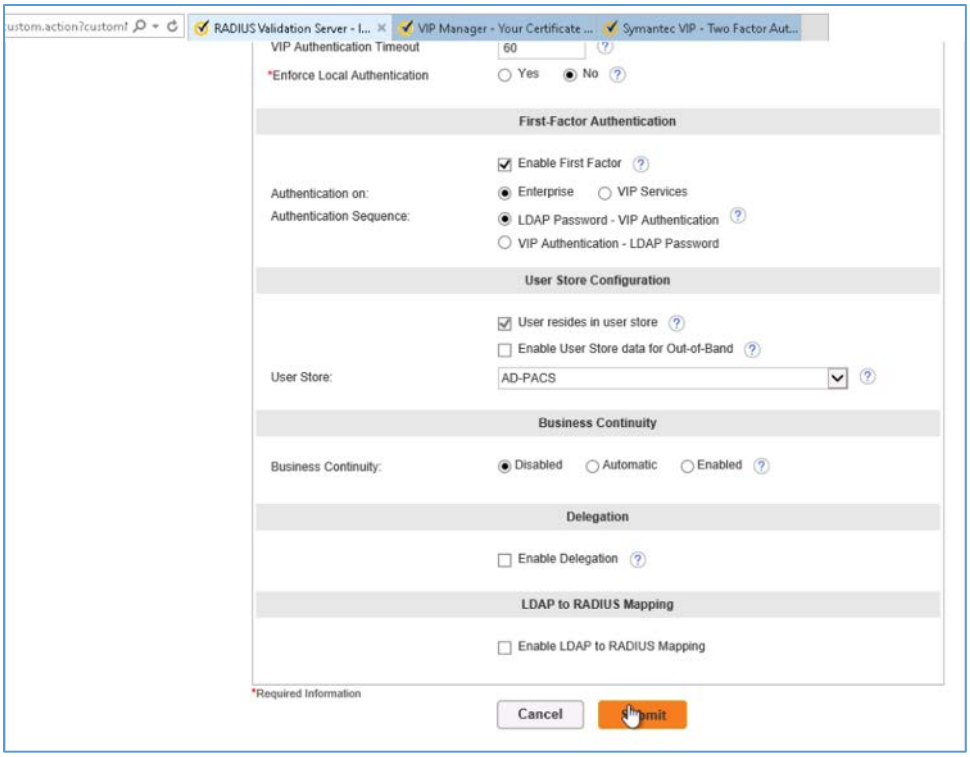
22. Select Validation from the menu bar, select Custom configuration, and provide the information that follows:

- **Server Name**: vip
- **Local IP**: 192.168.120.190

- **Port**: 1812
- **RADIUS Shared Secret**: *****
- **Confirm RADIUS Shared Secret:** *****
- **Enable First Factor:** *Checked*
- **Authentication on:** Enterprise
- **Authentication Sequence:** *LDAP Password – VIP Authentication*
- **User Store:** AD PACS

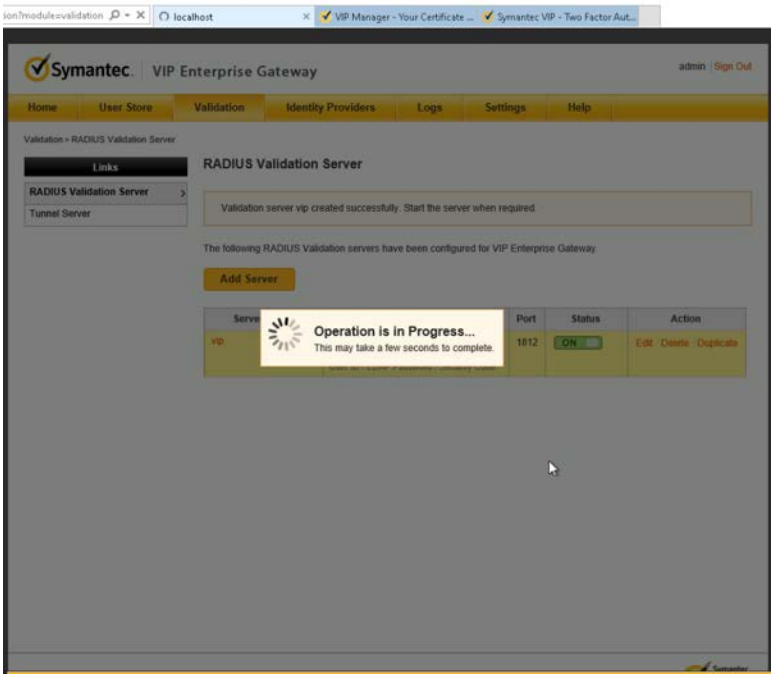


23. Click **Submit**.



2343

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



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

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/fmcv/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.