

NIST SPECIAL PUBLICATION 1800-24C

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

Volume C:
How-To Guides

Jennifer Cawthra

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges

Kevin Littlefield

Chris Peloquin

Sue Wang

Ryan Williams

Kangmin Zheng

The MITRE Corporation
McLean, Virginia

December 2020

FINAL

This publication is available free of charge from

<https://doi.org/10.6028/NIST.SP.1800-24>

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

<https://www.nccoe.nist.gov/library/securing-picture-archiving-and-communication-system-nist-sp-1800-24-practice-guide>



DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-24C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-24C, 255 pages, (December 2020), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at 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, 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 with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

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

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

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

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

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

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

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

Contents

1	Introduction	1
1.1	How to Use this Guide.....	1
1.2	Build Overview	2
1.3	Typographic Conventions.....	3
1.4	Logical Architecture Summary	3
2	Product Installation Guides	4
2.1	Picture Archiving and Communication System (PACS)	4
2.1.1	Philips IntelliSpace PACS.....	5
2.1.2	DCM4CHEE	20
2.2	VNA.....	25
2.2.1	Hyland Database Server.....	25
2.2.2	Hyland Acuo VNA.....	26
2.2.3	PACSGear Core Server	28
2.2.4	Hyland NilRead.....	37
2.3	Secure DICOM Communication Between PACS and VNA.....	41
2.3.1	Public Key Infrastructure (PKI) Certificate Creation.....	41
2.3.2	Public Key Infrastructure (PKI) Certification Installation	43
2.3.3	TLS Secure DICOM Configuration	47
2.3.4	PACS and VNA TLS Integration Tests	55
2.4	Modalities.....	55
2.4.1	DVTk Modality Emulator.....	55
2.4.2	DVTk RIS Emulator	60
2.5	Asset and Risk Management	62
2.5.1	Virta Labs BlueFlow.....	62
2.5.2	Tripwire Enterprise	69
2.6	Enterprise Domain Identity Management	95
2.6.1	Domain Controller with AD, DNS, and DHCP	96
2.6.2	DigiCert PKI	115

2.7	Network Control and Security.....	122
2.7.1	Cisco Firepower.....	122
2.7.2	Cisco Stealthwatch.....	147
2.7.3	Tempered Networks Identity Defined Networking (IDN).....	160
2.7.4	Zingbox IoT Guardian.....	166
2.7.5	Forescout CounterACT 8.....	173
2.7.6	Symantec Endpoint Detection and Response (EDR).....	180
2.8	Endpoint Protection and Security	187
2.8.1	Symantec Data Center Security: Server Advanced (DCS:SA)	187
2.8.2	Symantec Endpoint Protection	200
2.9	Data Security	212
2.9.1	Microsoft Azure Cloud Storage.....	213
2.9.2	Hyland VNA Cloud Archive Device.....	233
2.10	Secure Remote Access.....	237
2.10.1	TDi Technologies ConsoleWorks.....	237
2.10.2	Symantec Validation and ID Protection (VIP)	239

Appendix A	List of Acronyms.....	251
-------------------	------------------------------	------------

Appendix B	References	254
-------------------	-------------------------	------------

List of Figures

Figure 1-1	PACS Final Architecture.....	4
Figure 2-1	Hyland Systems and Applications Connectivity	25
Figure 2-2	Architecture of Networks IDN.....	161

List of Tables

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

1 Introduction

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

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

1.1 How to Use this Guide

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

This guide contains three volumes:

- NIST SP 1800-24A: *Executive Summary*
- NIST SP 1800-24B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-24C: *How-To Guides* – instructions for building the example solution (**you are here**)

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

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

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

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

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

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

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

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a PACS security solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, in NIST SP 1800-24B lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to 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 a PACS ecosystem. While the project implemented PACS and vendor neutral archive (VNA) solutions as well as security controls, the environment leveraged modality emulation to simulate medical image acquisition. The project also implemented an emulated radiology information system (RIS), used to generate modality work lists and therefore, support common medical imaging workflows. The project then applied security controls to the lab environment. Refer to NIST Special Publication (SP) 1800-24B, *Approach, Architecture, and Security Characteristics*, for an explanation of why we used each technology.

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

1.4 Logical Architecture Summary

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

2.1.1 Philips IntelliSpace PACS

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

System Requirements

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

Table 2-1 Base VM Configuration Requirements

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

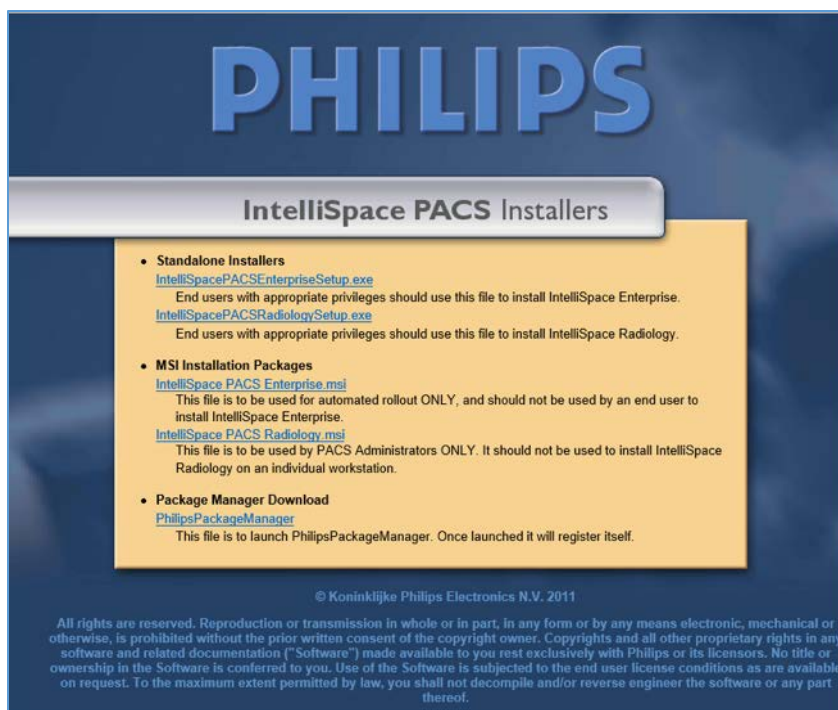
VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
	Image pre-fetching from VNA					

IntelliSpace PACS Client Installation

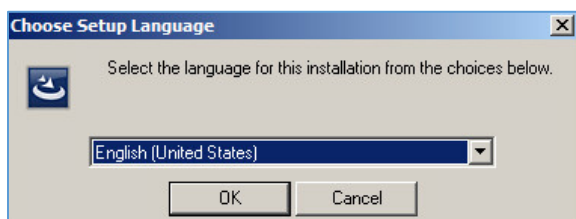
The project team collaborated with a team of Philips Healthcare deployment engineers to install the environment. Based on the base VM configuration requirements, the NCCoE team created the VMs by using the open virtualization format (OVF) files provided by Philips Healthcare. Philips engineers deployed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

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

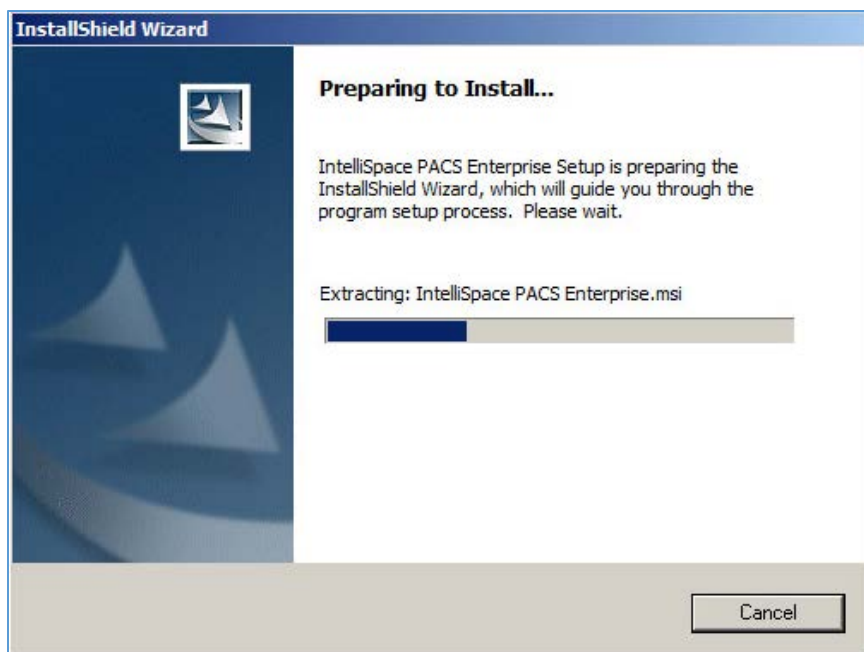
1. Open **Internet Explorer** from a workstation and assign the IntelliSpace server with the internet protocol (IP) address 192.168.140.131. Enter the IntelliSpace server IP address in the address bar by using the following uniform resource locator (URL): <https://192.168.140.131/clientweb/installers>.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



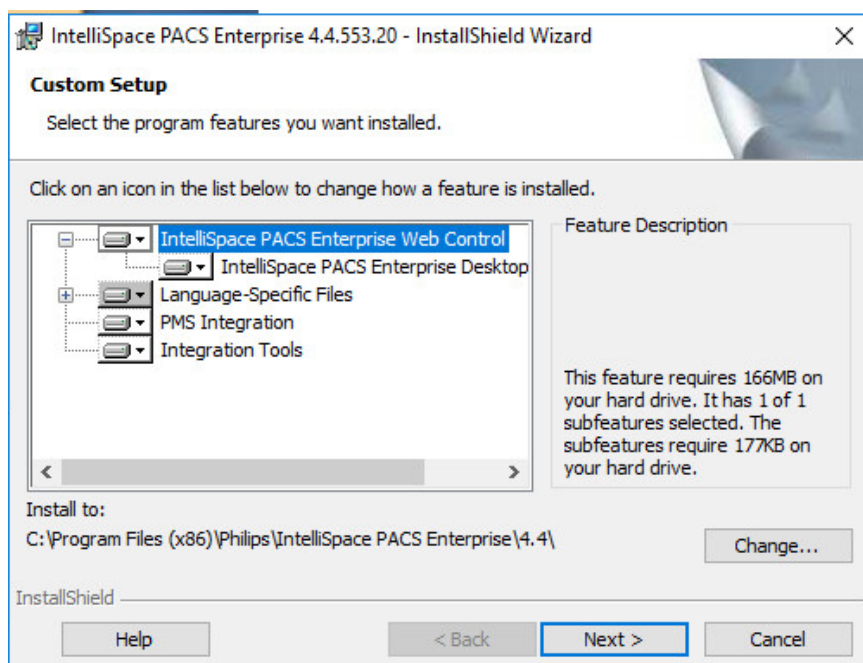
3. An option to choose setup language displays. Select the **English (United States)** from the drop-down and click **OK**.



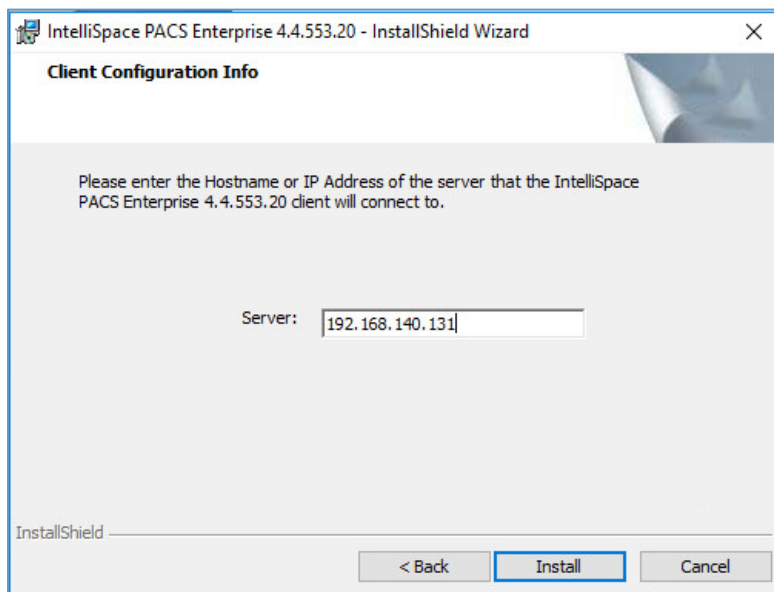
4. After the setup language has been set, the **InstallShield Wizard** begins the installation process.



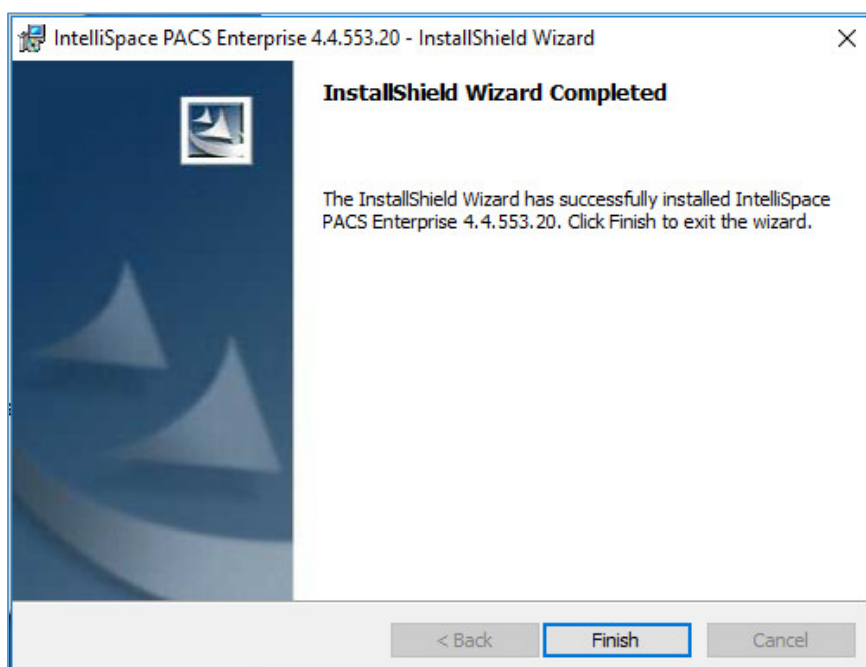
5. Use the default setting for the **Custom Setup** and click the **Next >** button that appears at the bottom of this window.



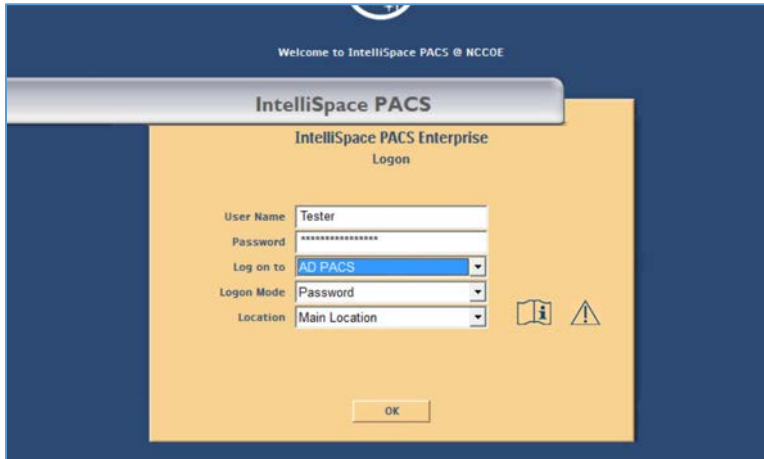
6. On the **Client Configuration Info** window, enter **192.168.140.131** as the Server IP address, and click **Install**.



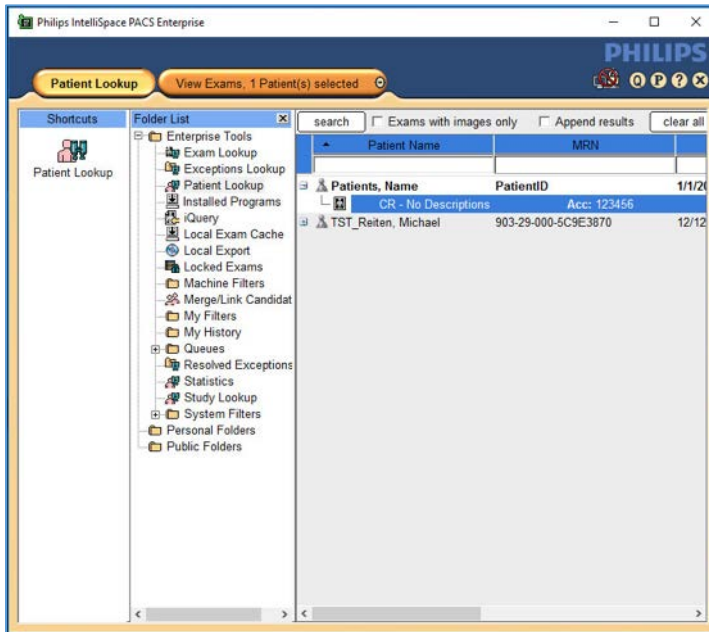
7. When installation is finished, the **InstallShield Wizard** provides a message indicating successful installation. Click **Finish**.



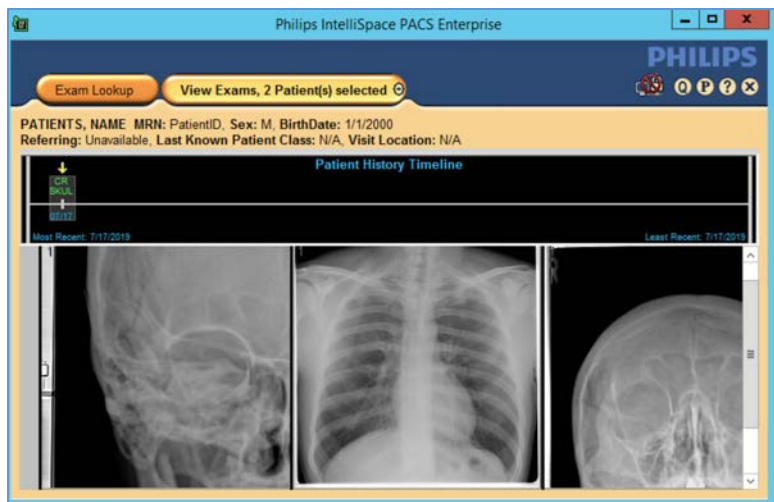
8. Once the installation is done, the installer places an **IntelliSpace PACS Enterprise** icon on the desktop. Type **Tester** in the **User Name** field and the corresponding password in the **Password** field, then click **OK** to log in.



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



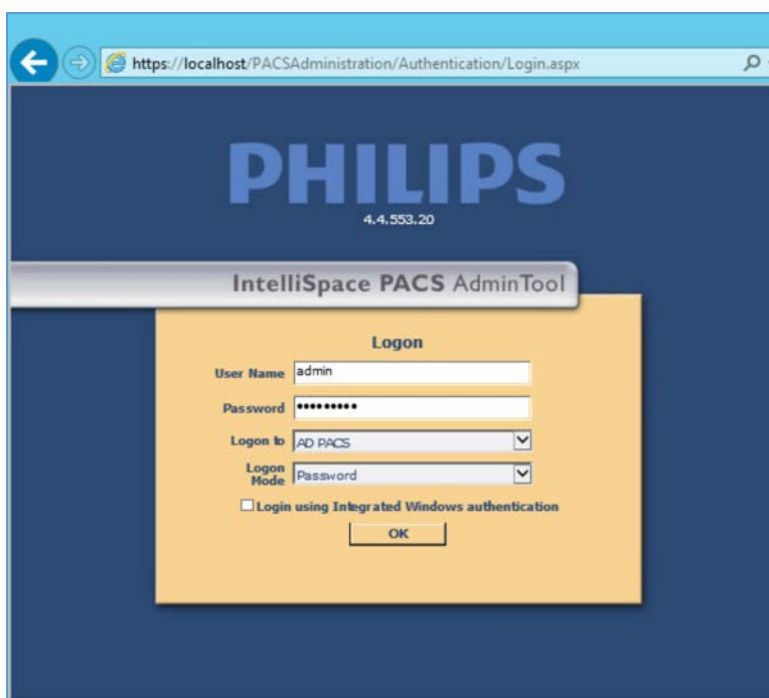
10. To view an exam, navigate to **Exam Lookup**, which lists a summary of a patient's exams. Double-click an exam in the list. If the exam has an image, it will be displayed. An example is below.



IntelliSpace PACS Client Configuration

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

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



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

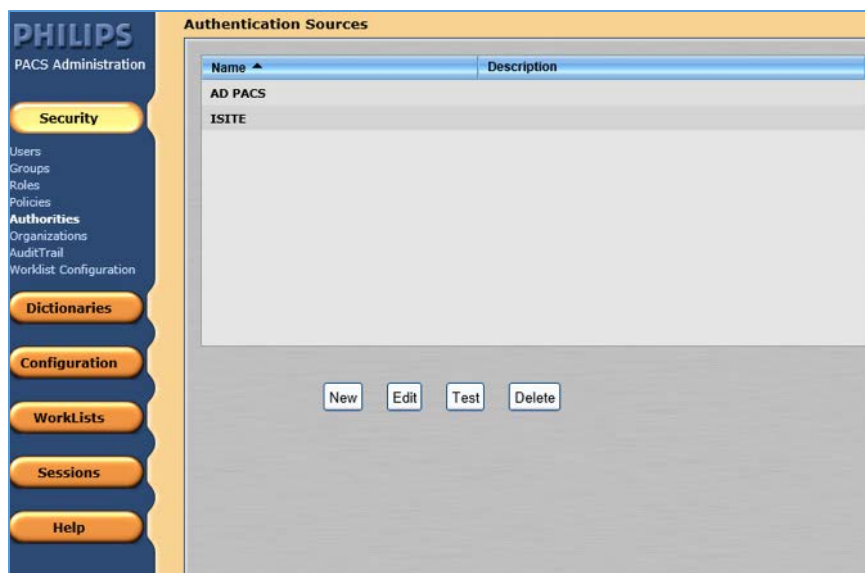


3. To add a new user, navigate to **SECURITY**, found on the far-left column of the Common Tasks screen, and click **Users**.
 - a. Enter the User ID.
 - b. Enter the user's First Name.
 - c. Enter the user's Middle Name (optional).
 - d. Enter the user's Last Name.
 - e. Enter the user's Email Address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

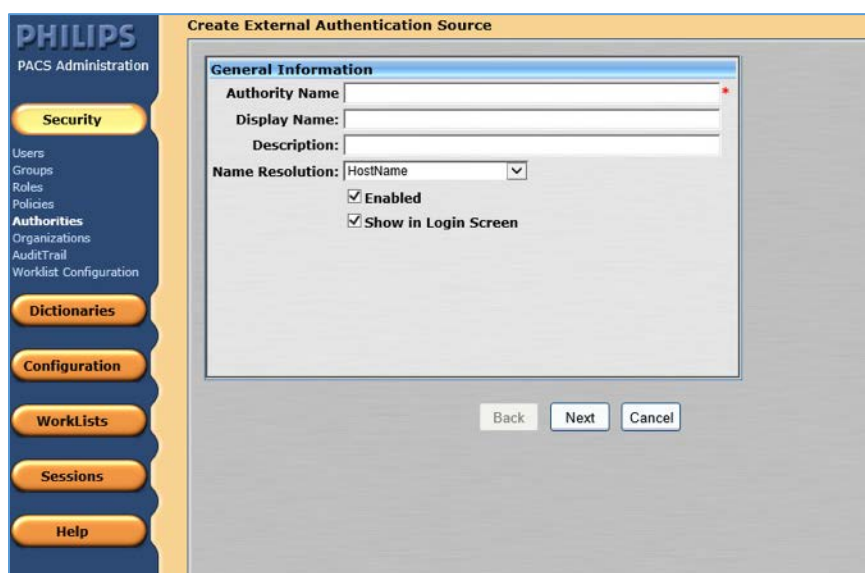
Configure Sources for User Authentication

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

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



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



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

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

The screenshot shows the 'Edit External Authentication Source' window in the PHILIPS PACS Administration interface. The 'General Information' tab is active. The fields are as follows:

- Authority Name:** AD.PACS.HCLAB
- Display Name:** AD PACS
- Description:** (empty)
- Name Resolution:** HostName (dropdown menu)
- Enabled:** ☒
- Show in Login Screen:** ☒

At the bottom of the window are three buttons: Back, Next, and Cancel.

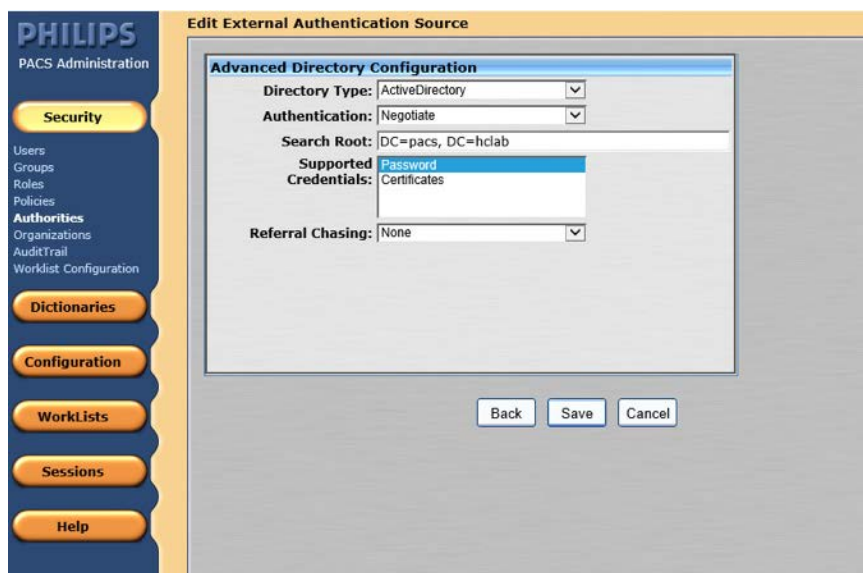
4. In the **Advanced Directory Configuration**, set **DNS Host Name** as **ad.pacs.hclab** and **Port** as **389**.

The screenshot shows the 'Edit External Authentication Source' window in the PHILIPS PACS Administration interface. The 'Host Query Configuration' tab is active. The fields are as follows:

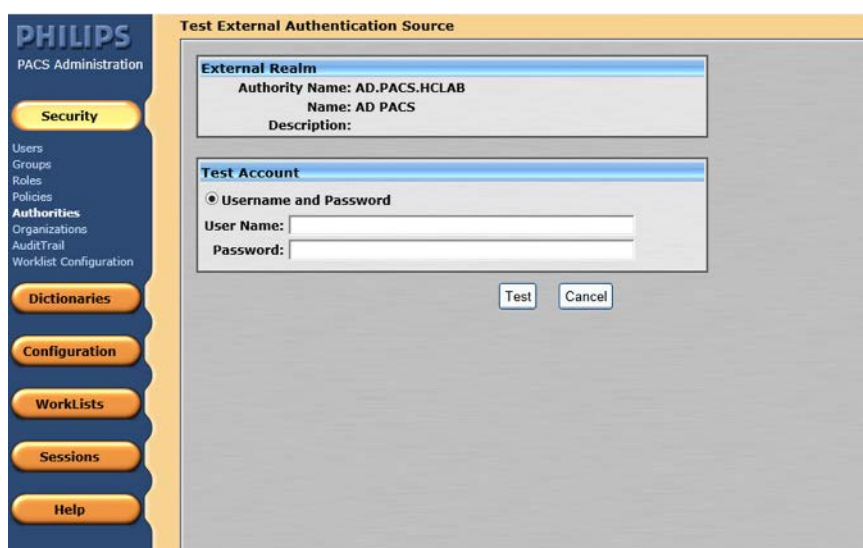
- DNS Host Name:** ad.pacs.hclab
- Port:** 389

At the bottom of the window are three buttons: Back, Next, and Cancel.

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



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

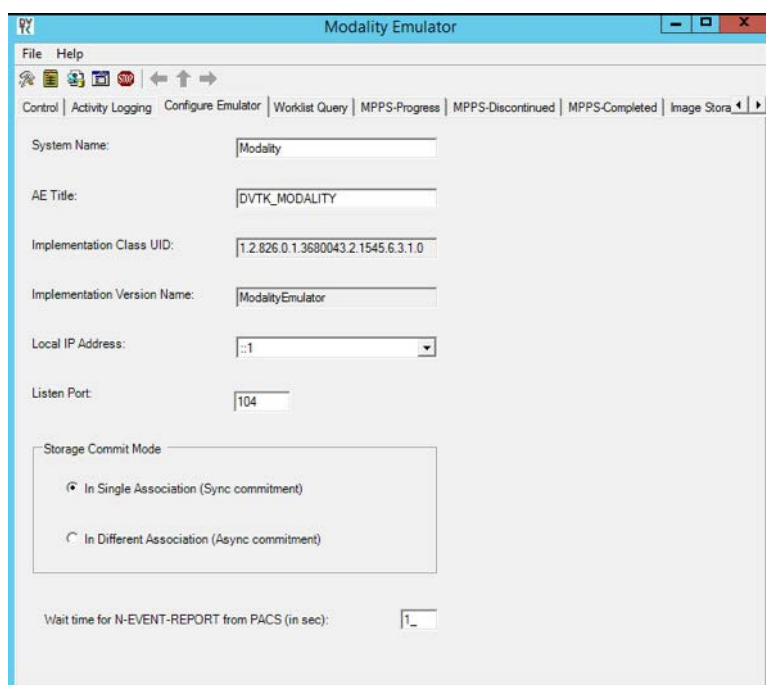


Configure Connection to Modality Emulator

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

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

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



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 is needed. Particularly, the **AE Title** for the Philips IntelliSpace PACS is required for the **AE Title** field. These are the input values:

RIS System

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

MPPS Manager

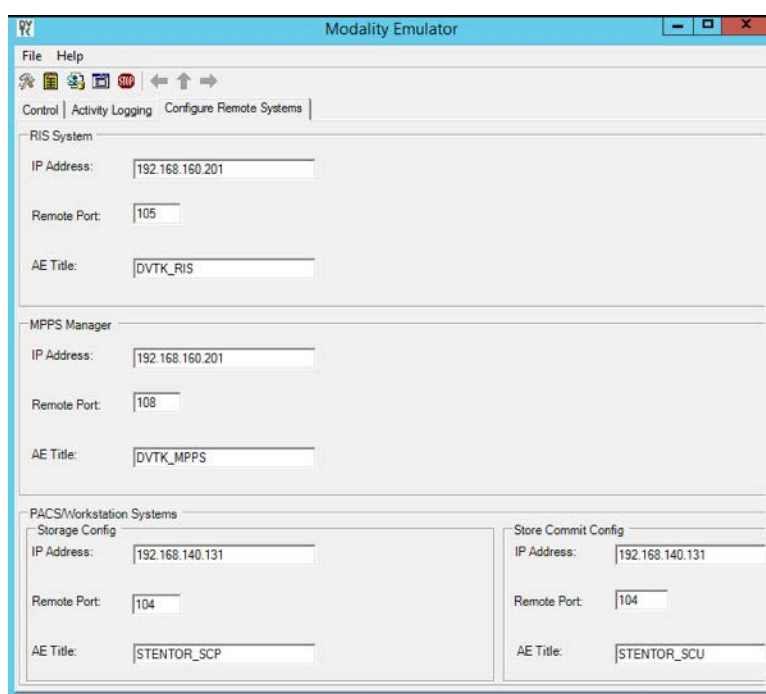
- **IP Address:** 192.168.160.201
- **Remote Port:** 108
- **AE Title:** DVTK_MPPS

PACS/Workstation Systems–Storage Config

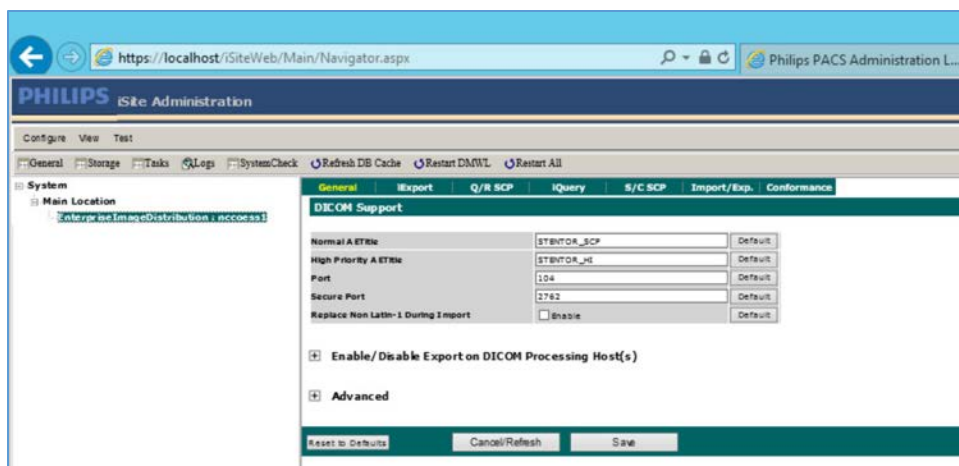
- **IP Address:** 192.168.140.131
- **Remote Port:** 104
- **AE Title:** STENTOR_SCP

PACS/Workstation Systems–Storage Commit Config

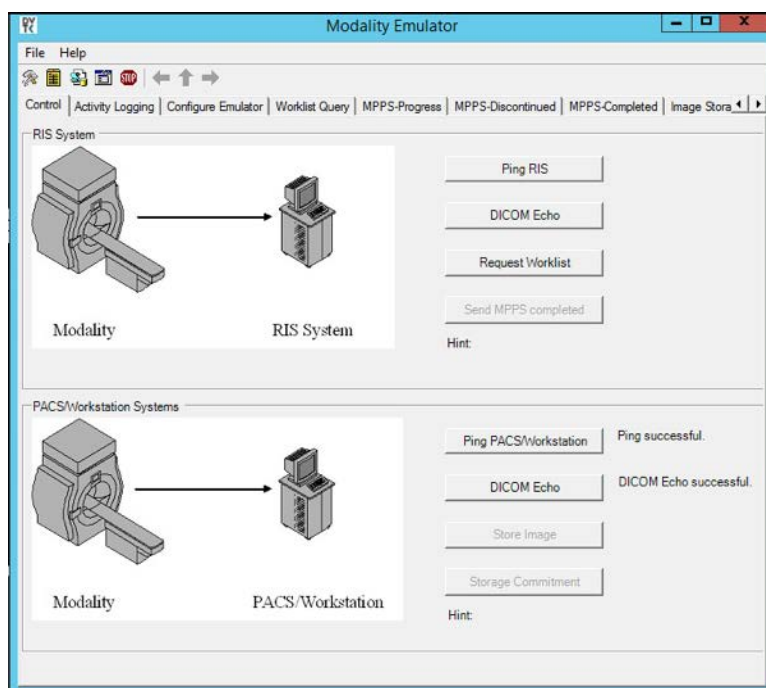
- **IP Address:** 192.168.140.131
- **Remote Port:** 104
- **AE Title:** STENTOR_SCU



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



- 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.

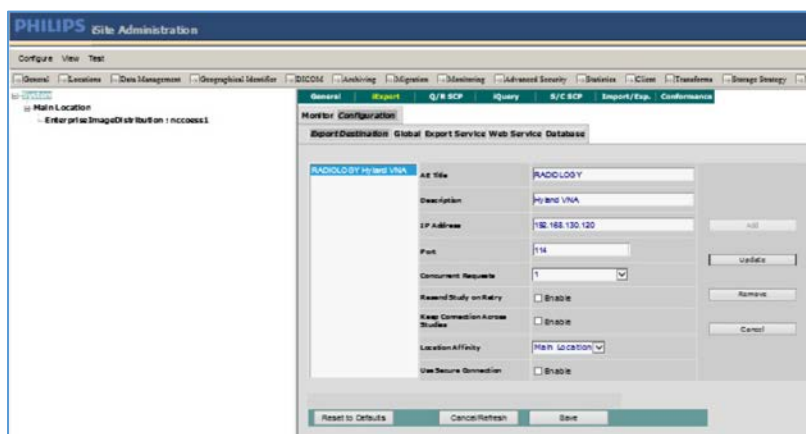


Configure IntelliSpace PACS to Communicate with Hyland VNA

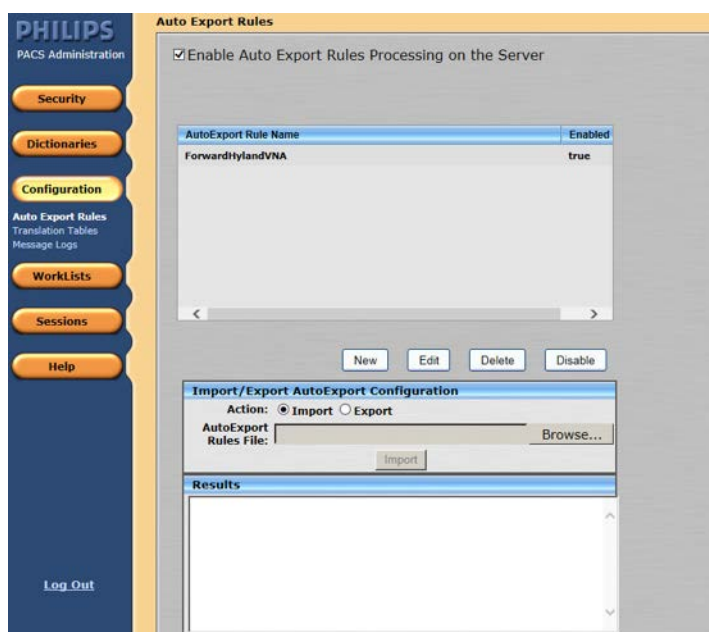
Refer to [Section 2.2.2](#) for detailed installation guidance for Hyland VNA.

- 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 by using <https://192.168.140.131/PACSAdministration>.
5. Click the **Configuration** button on the left panel to configure the **Auto Export Rule**.
6. Click the **New** button to create a new rule named **ForwardHylandVNA**.



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

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

PHILIPS
PACS Administration

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

[Log Out](#)

Edit AutoExport Rule

AutoExportRule Configuration

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

Matching Criteria

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

Configured Export Destinations

Selected Destinations

Hyland VNA (RADIOLOGY)

>>
<<

Save Cancel

2.1.2 DCM4CHEE

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

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

System Requirements

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

DCM4CHEE Installation

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

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



DCM4CHEE to VNA Configuration

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

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

DCM4CHEE to DVTk Modality Configuration

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

RIS System

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

MPPS Manager

- **IP Address:** 192.168.140.160
- **Remote Port:** 108

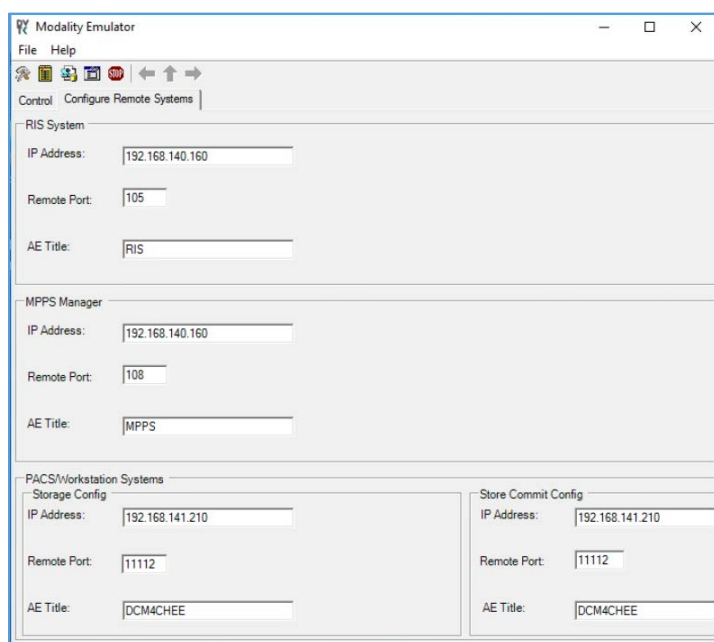
- **AE Title:** MPPS

PACS/Workstation System–Storage Config

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

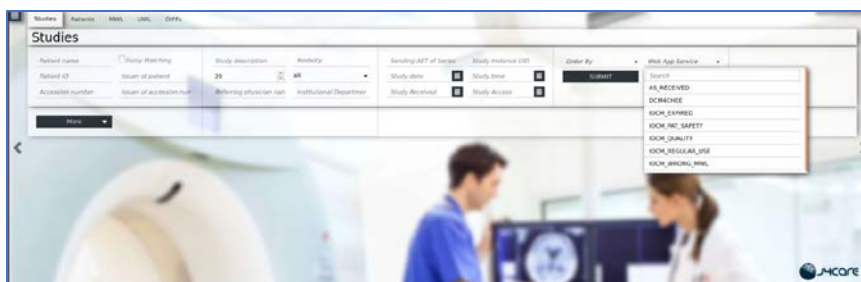
PACS/Workstation System–Storage Commit Config

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

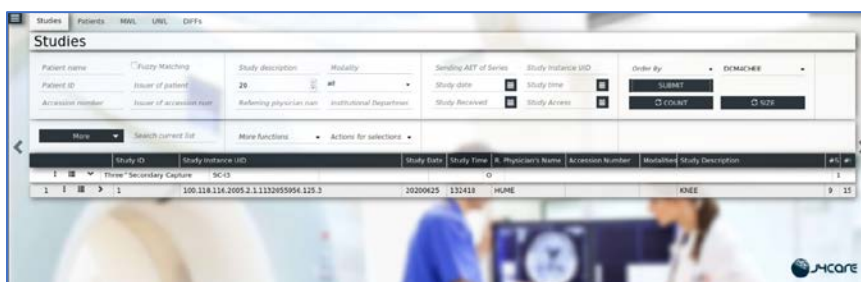


DCM4CHEE View Stored Data and Archive to VNA

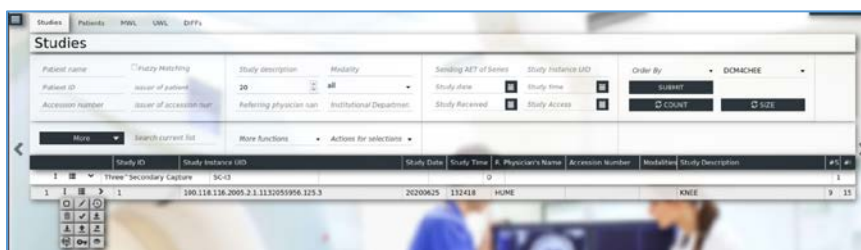
1. Click the dark blue menu dangle (☰) on the left-hand side of the screen.
2. Select **Navigation**.
3. Select **DCM4CHEE** under **Web App Service** on the right-hand side of the screen.



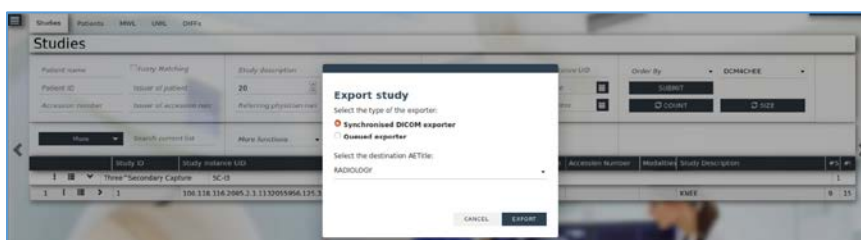
4. Select **Submit** to see stored patient studies.



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



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



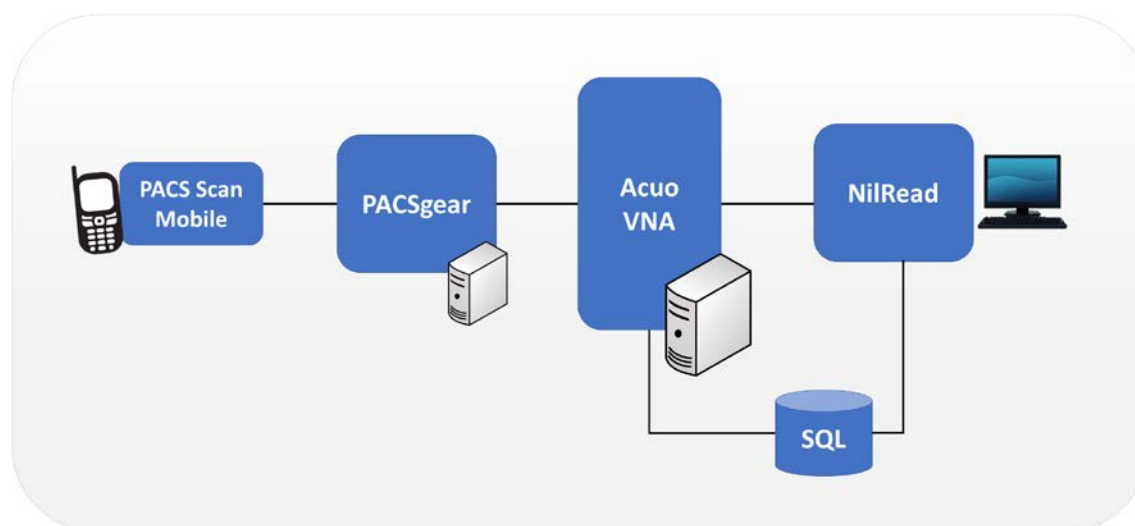
2.2 VNA

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

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

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

Figure 2-1 Hyland Systems and Applications Connectivity



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

2.2.1 Hyland Database Server

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

System Requirements

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

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

Hyland Database Server Installation

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

Hyland Database Configuration

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

2.2.2 Hyland Acuo VNA

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

System Requirements

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

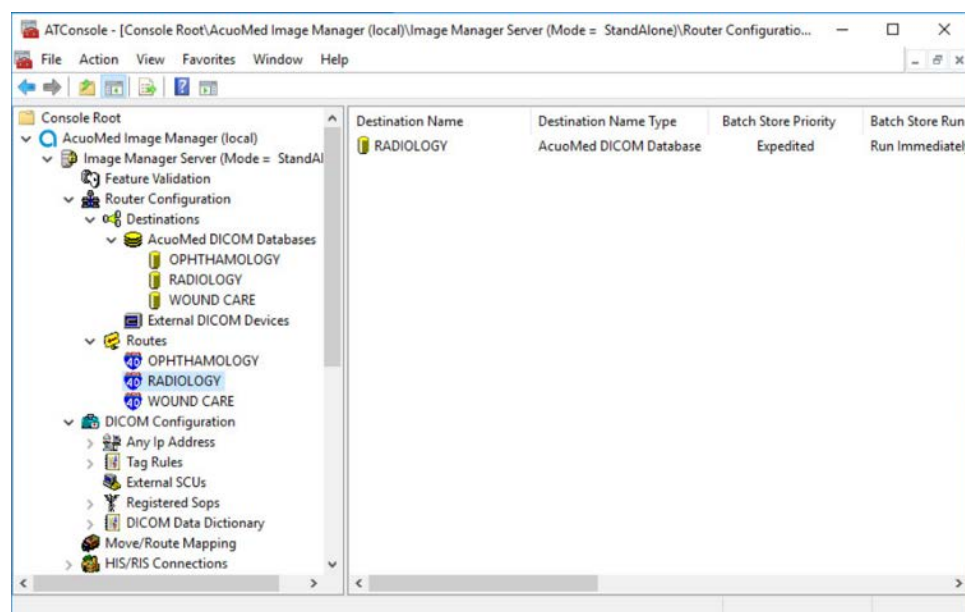
- **Operating System:** Microsoft Windows Server 2016
- **Network Adapter:** VLAN 1301

Hyland Acuo VNA Installation

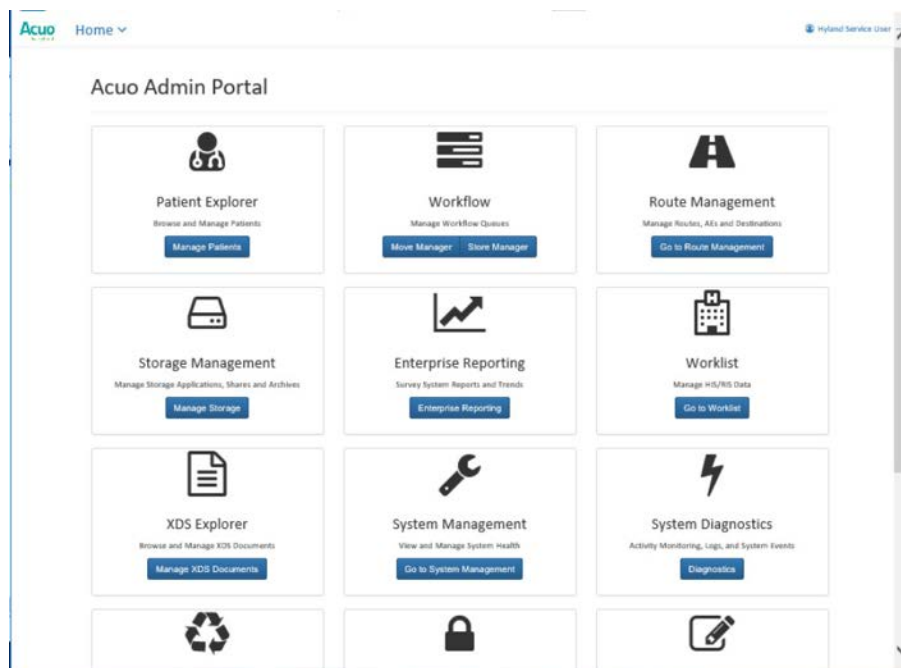
1. In the NCCoE test environment, the Hyland Acuo VNA was installed on a VM preconfigured with the OS and network requirements provided by Hyland. Engineers supplied by Hyland performed the installation.
2. Upon completion of the installation, three Windows services were created: AcuoMed, AcuoAudit,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

Hyland Acuo VNA Configuration

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



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



2.2.3 PACSgear Core Server

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

System Requirements

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

PACSgear Core Server Installation

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

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

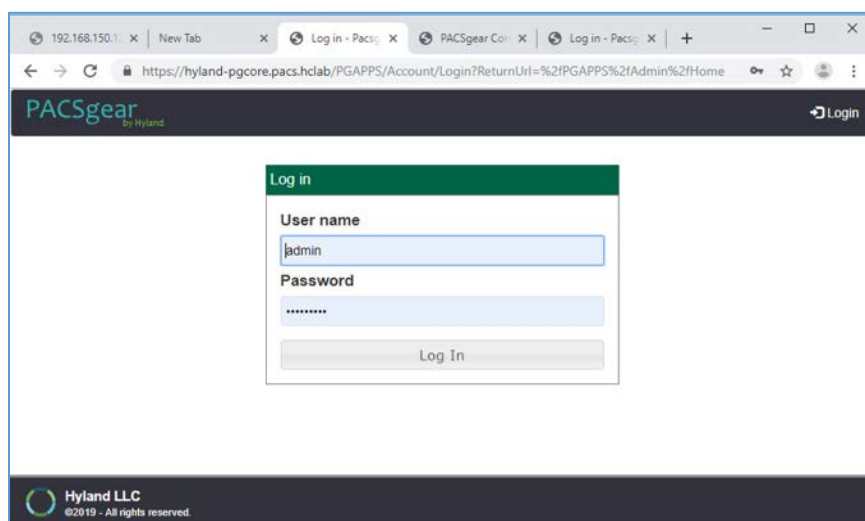
PACSgear Core Server Configuration

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

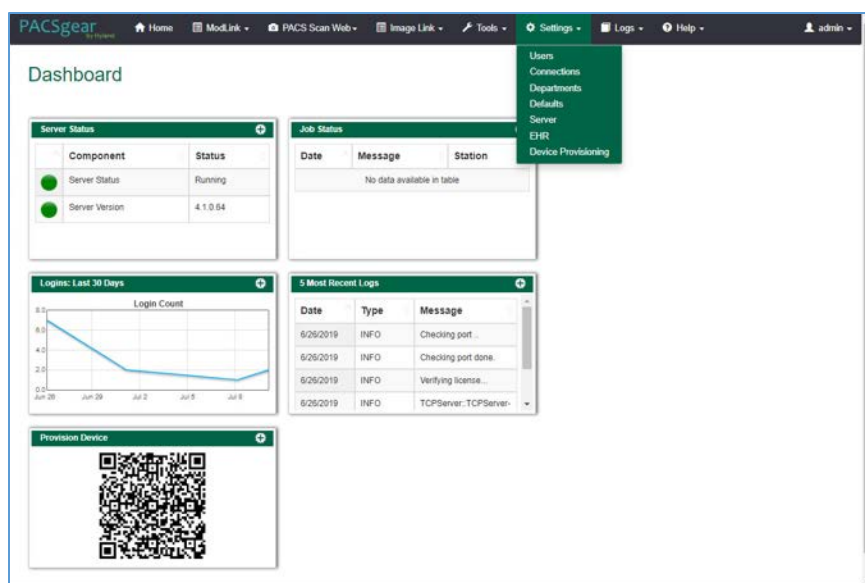
During the DB configuration, the Hyland engineers created instances for representative departments (e.g., ophthalmology, radiology, and departments that may see patients who need wound treatment).

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

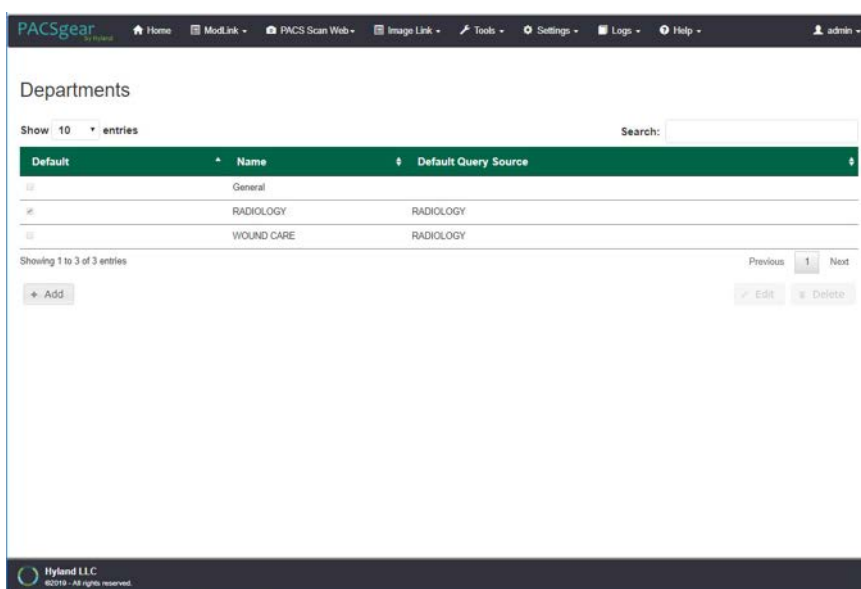
1. The Hyland engineers logged on to the PACSgear Admin portal by using <https://hyland-pgcore.pacs.hclab/PGAPPS/Admin>.



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



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



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

Add/Edit Department

Default ☐

Name

AE title

Modality

Apply series per image ☐

Destinations ☐ XDS ☐ Lookup Sources ☐ Client ☐ Series

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

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

Add/Edit Department

Default ☒

Name

AE title

Modality

Apply series per image ☐

Destinations ☐ XDS ☐ Lookup Sources ☐ Client ☐ Series

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

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.

Add/Edit Department

Default ☐ **AE title**

Name **Modality**

Apply series per image ☐

Destinations XDS Lookup Sources **Client** Series

Client	Persistent Login	Video	Photo Quality	Video Quality	Max. Video Length	Allow Camera Import
GENERICIOS	<input type="text" value="NO"/>	<input type="text" value="NO"/>	<input type="text" value="MED"/>	<input type="text" value="MED"/>	<input type="text" value="30 Sec"/>	<input type="text" value="NO"/>
ANDROID	<input type="text" value="NO"/>	<input type="text" value="NO"/>	<input type="text" value="MED"/>	<input type="text" value="MED"/>	<input type="text" value="30 Sec"/>	<input type="text" value="NO"/>
MRPVINEFOTOUCH	<input type="text" value="NO"/>	<input type="text" value="NO"/>	<input type="text" value="MED"/>	<input type="text" value="MED"/>	<input type="text" value="30 Sec"/>	<input type="text" value="NO"/>

Cancel Save

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.

Departments

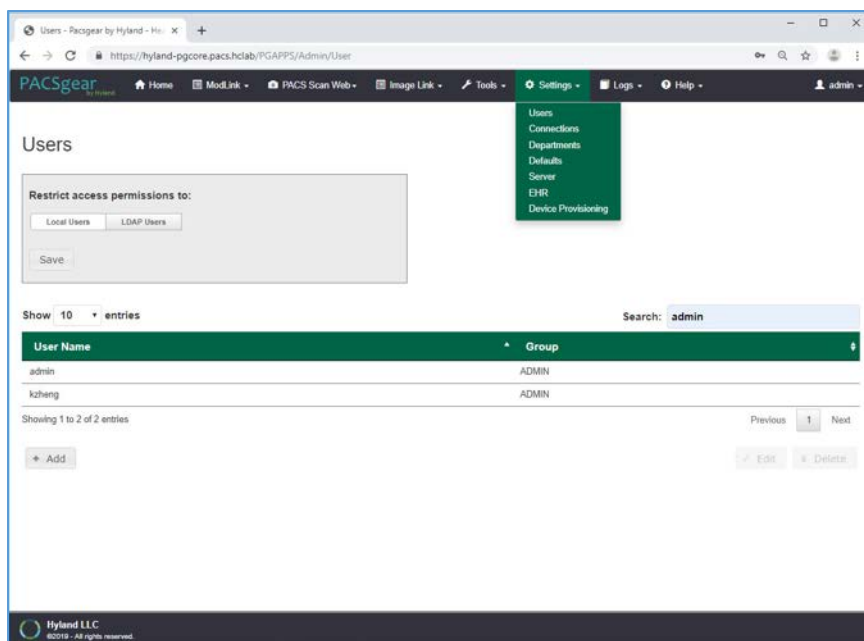
Show 10 entries Search:

Default	Name	Default Query Source
<input type="checkbox"/>	General	
<input type="checkbox"/>	RADIOLOGY	RADIOLOGY
<input type="checkbox"/>	WOUND CARE	RADIOLOGY
<input type="checkbox"/>	Ophthalmology	RADIOLOGY

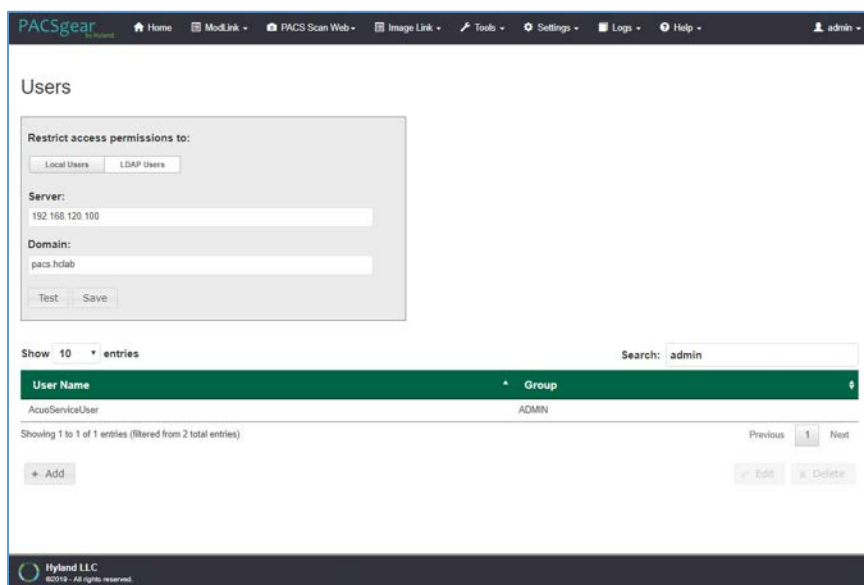
Showing 1 to 4 of 4 entries

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**.



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

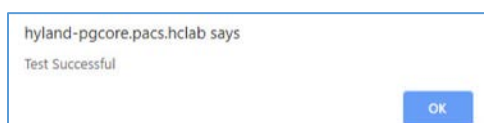


5. Click the **Test** button located under the **Domain** entry box.
6. Enter the **LDAP_User** credentials to verify connectivity to the AD.



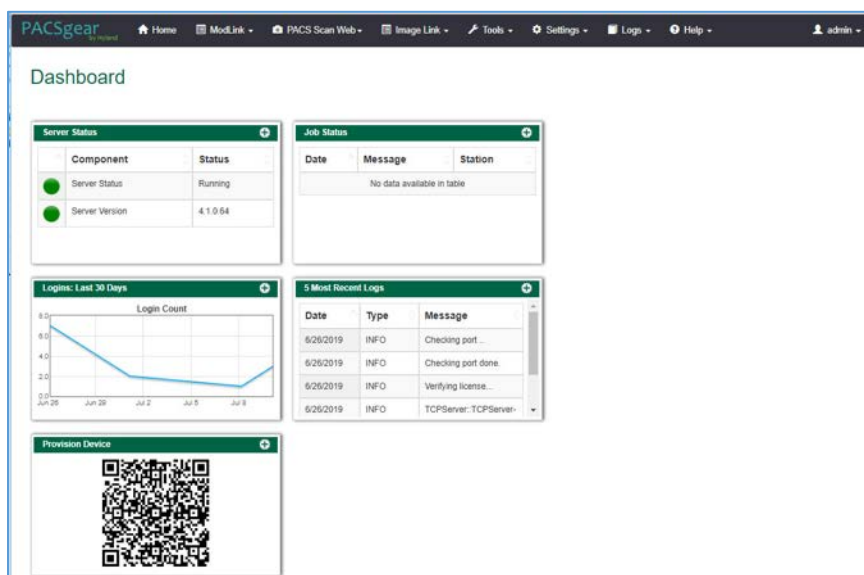
A dialog box titled "Test LDAP Settings" with a close button (X) in the top right corner. It contains two input fields: "Username:" with the text "LDAP_User" and "Password:" with masked characters "*****". Below the fields is a "Test" button.

7. A message box displays 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:

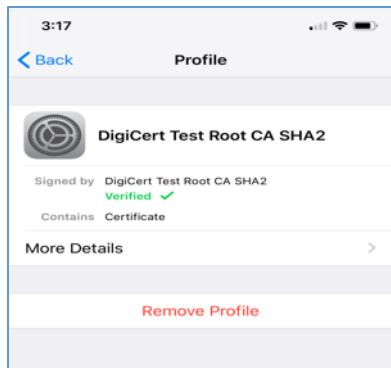
1. On the iPhone, navigate to the **App Store**. Search for PACS Scan Mobile, from Perceptive Software. Perceptive Software is a Hyland business unit. Select the **GET** button to install the software, and then select the **OPEN** button. Select **Allow** to permit the software to send notifications.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



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



4. Point the camera at the **QR code** on the PC screen until a message box appears indicating **Setting Updated Your settings have been updated**. This setting configures the mobile **PACS Scan application** to the address of its **PACSgear Core Server** instance.
5. From a workstation, acquire the trusted root certificate from DigiCert. Further information for using DigiCert is described in [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 certificate profiles.
9. Find the certificate you installed and click to display the detail. An example appears below:



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

2.2.4 Hyland NilRead

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

System Requirements

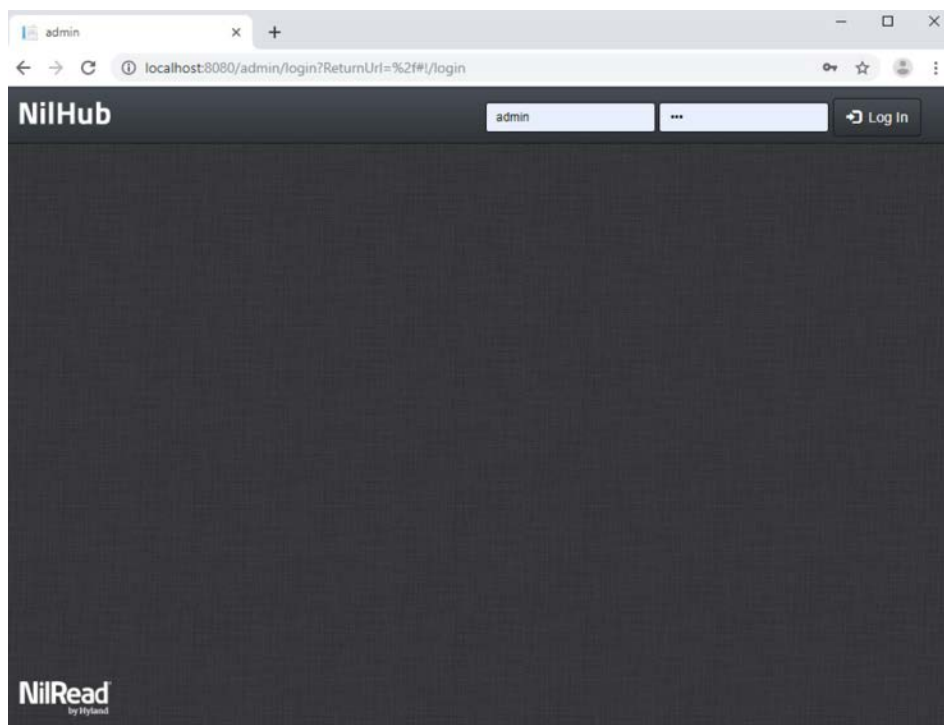
- **CPUs:** 6
- **Memory:** 12 GB RAM
- **Storage:**
 - HD 1: 80 GB (OS installation)
 - HD 2: 200 GB (web application)
 - HD 3: 100 GB (image cache)
- **Operating System:** Microsoft Windows Server 2016
- **Network Adapter:** VLAN 1301

Hyland NilRead Installation

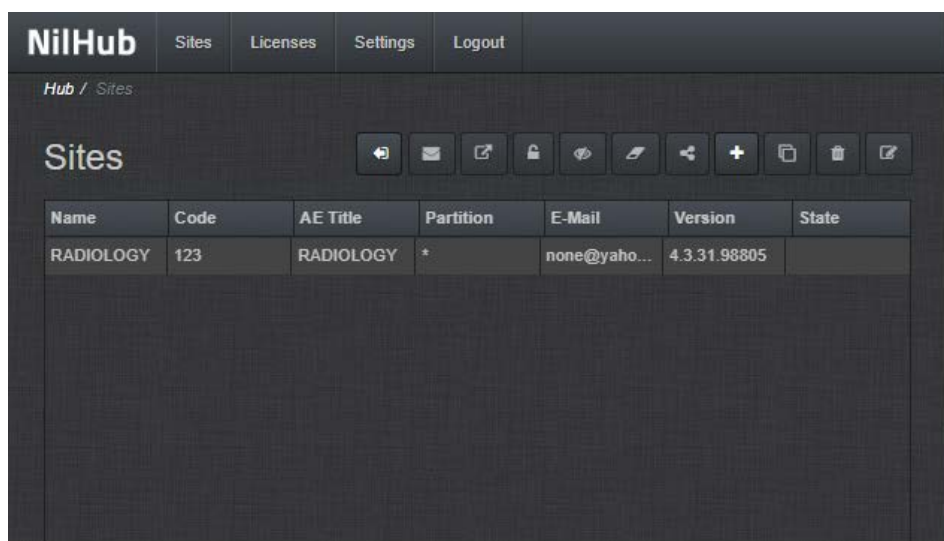
1. Hyland engineers installed Hyland NilRead based on Hyland's proprietary installation package and installation guides. NilRead has three services: Hub Front End service, Nil Back End service, and Nil Front End service. The Hub Front End service provides management service for multitenant configuration.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

Hyland NilRead Configuration

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



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



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

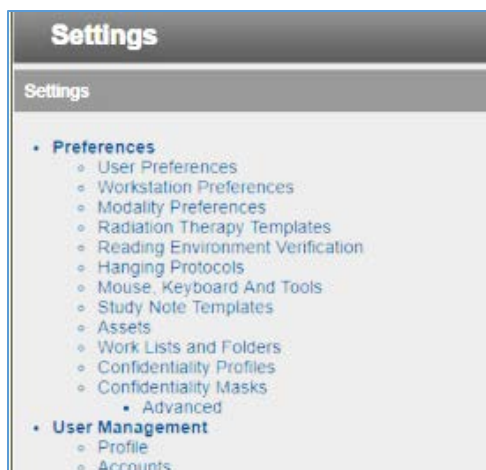
- **Name:** WOUND_CARE
- **Details:** Wound Care Department
- **Code:** 974
- **AE Title:** WOUND_CARE
- **VNA Partition:** WOUND_CARE
- **Database Name:** WOUND_CARE
- **Email:** none@hyland.com

The screenshot shows the 'New' form in the NilHub application. The form is divided into two columns. The left column contains fields for 'NAME' (WOUND_CARE), 'DETAILS' (Wound Care Department), 'CODE' (974), 'AE TITLE' (WOUND_CARE), and 'E MAIL' (none@hyland.com). The right column contains fields for 'UUID' (a long alphanumeric string), 'VNA PARTITION' (WOUND_CARE), 'DATABASE NAME' (WOUND_CARE), 'CACHE PATH' (C:\NilRepository\WOUND_CARE), and 'ENABLE SPORE FEDERATION' (checked). A 'Save' button is located at the bottom right of the form.

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

The screenshot shows the NilRead by Hyland login screen. The 'Site' field is set to 'WOUND_CARE'. The 'User Name' field is set to 'admin'. The 'Password' field is masked with three dots. The 'Domain' field is a dropdown menu. A 'Login' button is located below the fields. Below the login fields, there is a section for 'Test your connection speed' with a 'Connection Type' dropdown set to 'Auto detect' and a 'Waiting Room' button with a globe icon.

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



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

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

2.3 Secure DICOM Communication Between PACS and VNA

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

2.3.1 Public Key Infrastructure (PKI) Certificate Creation

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

2.3.1.1 Create PKI Certificate for Hyland Acuo VNA

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

2.3.1.2 Create PKI Certificate for Philips IntelliSpace PACS

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

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

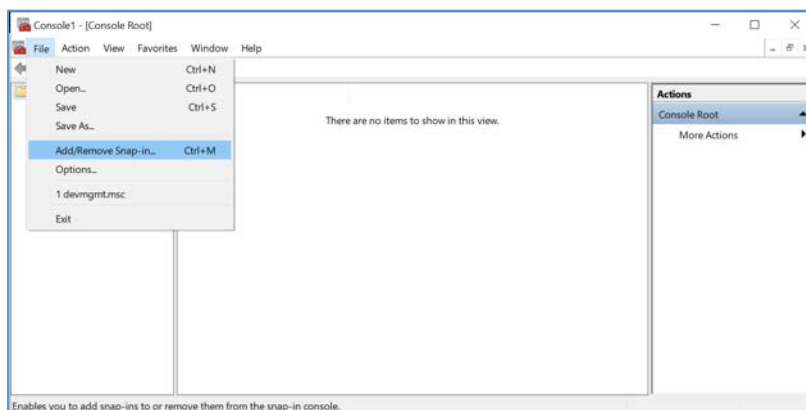
2.3.2 Public Key Infrastructure (PKI) Certification Installation

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

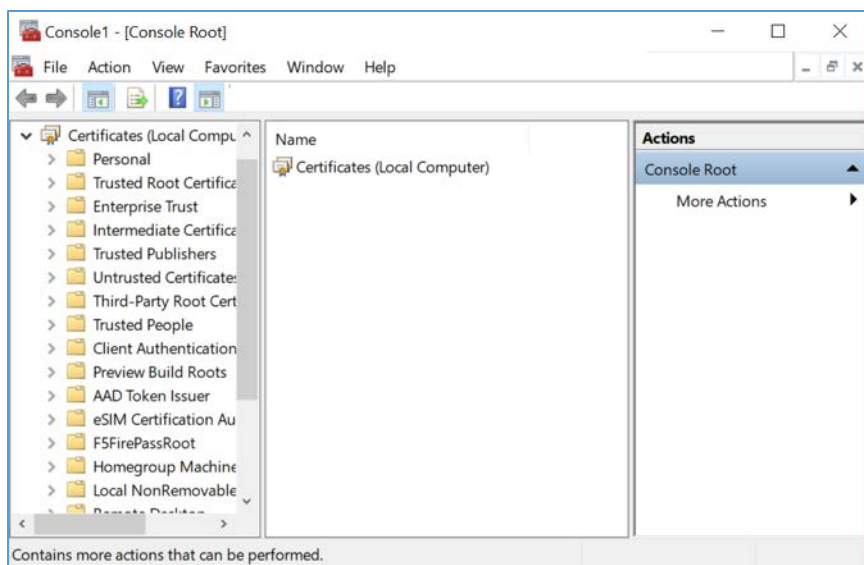
2.3.2.1 Install PKI Certificate for Hyland Acuo VNA

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

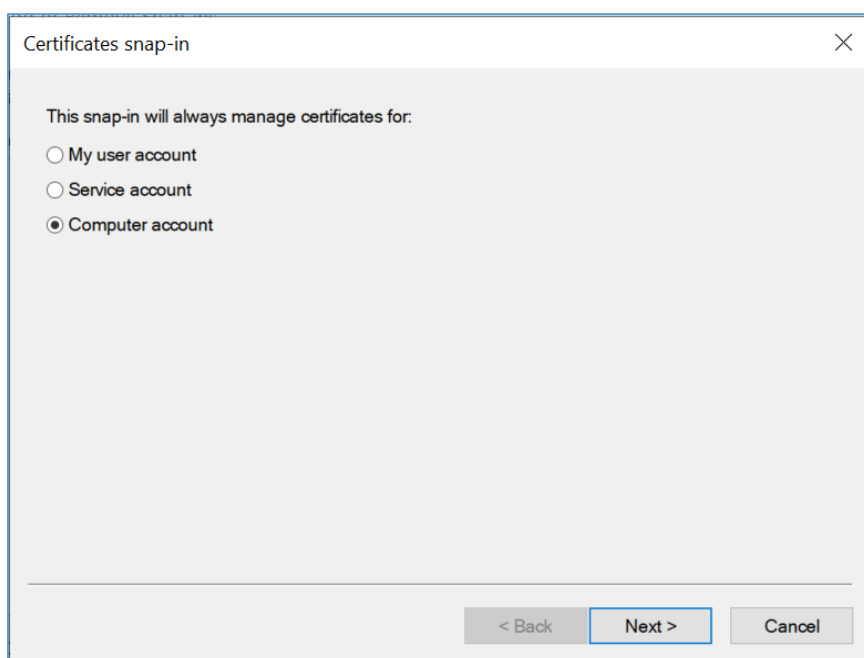
1. From the Acuo server, click **Start > Run > mmc**.
2. Select **File > Add/Remove Snap-in...**



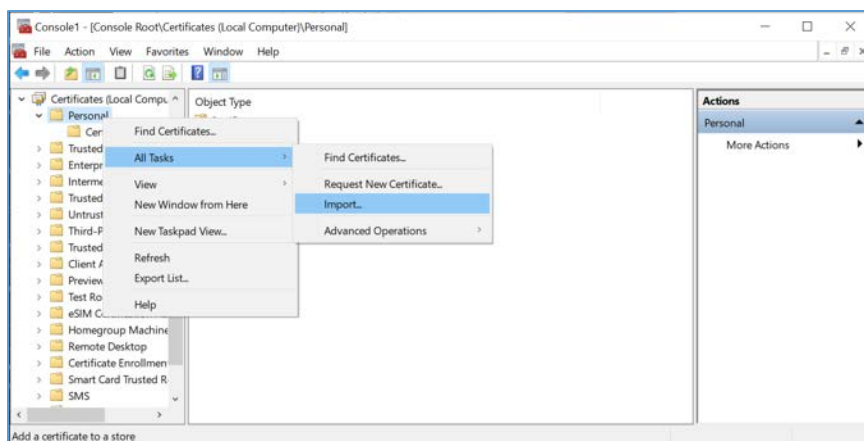
3. Select **Certificates** and click **Add**.
 - a. Choose **Computer Account**.
 - b. Choose **Local Computer**.
4. Click **Finish**, then click **OK**.



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



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



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

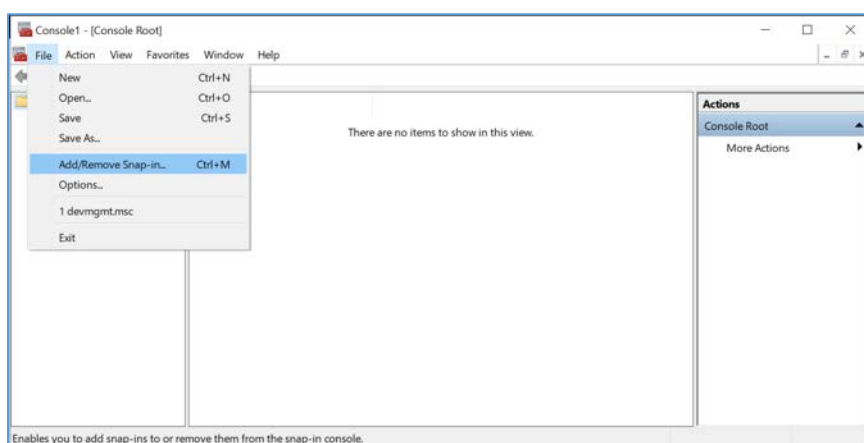
- a. Navigate to **Certificates > Personal > Certificates**.
- b. Right-click the certificate, select **All Tasks > Manage Private Keys...**
- c. Add the **AcuoServiceUser** and grant full control permissions. Click **OK**.

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

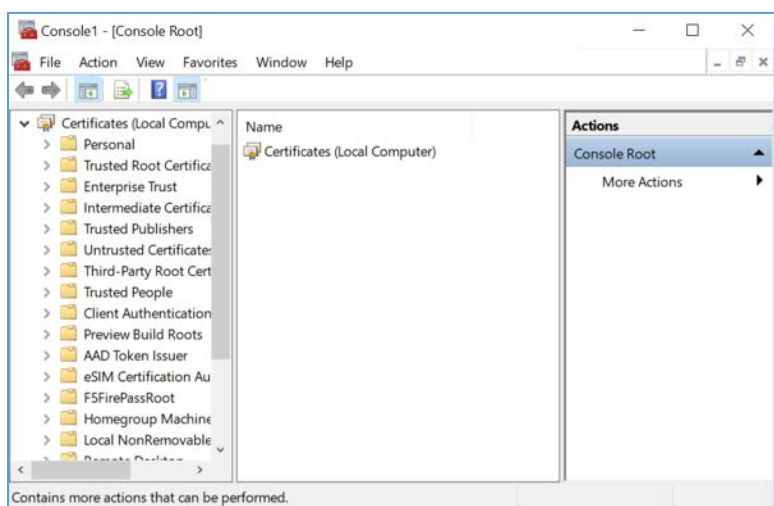
2.3.2.2 Install PKI Certificate for Philips IntelliSpace PACS

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

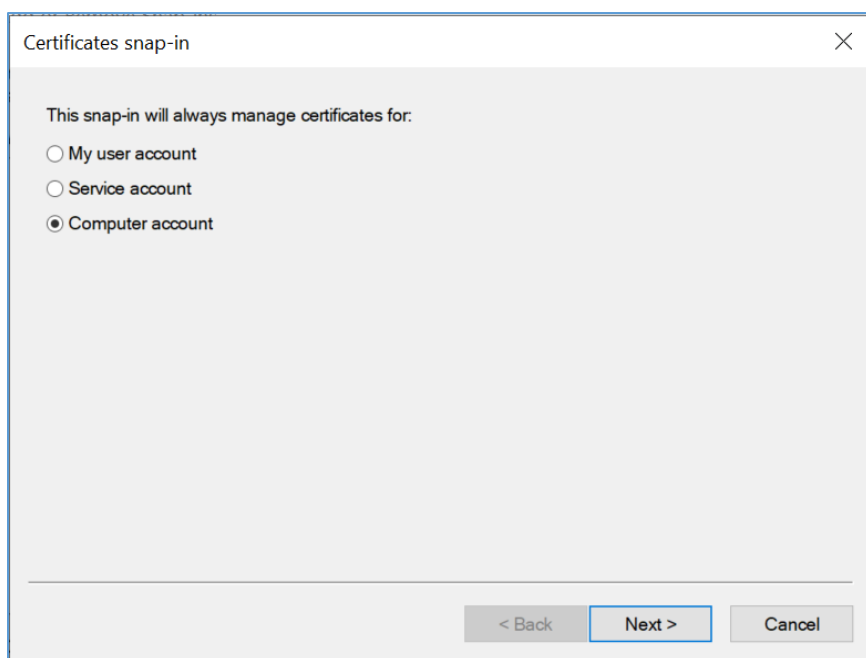
1. From the IntelliSpace server, click **Start > Run > mmc**.
2. Select **File > Add/Remove Snap-in...**



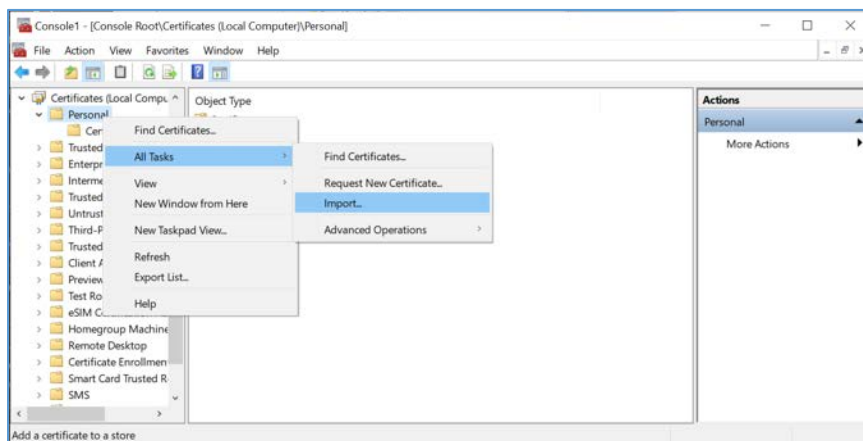
3. Select **Certificates** and click **Add**.
 - a. Choose **Computer Account**.
 - b. Choose **Local Computer**.
 - c. Click **Finish**; click **OK**.



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 root CA certificate (**DigiCert Test Root CA SHA2**) and its Intermediate Root certificate (**DigiCert Test Intermediate Root CA SHA2**) into the server computer.

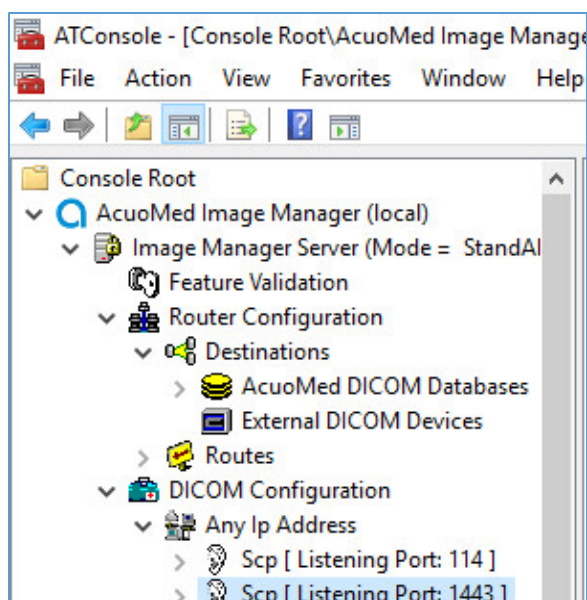
2.3.3 TLS Secure DICOM Configuration

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

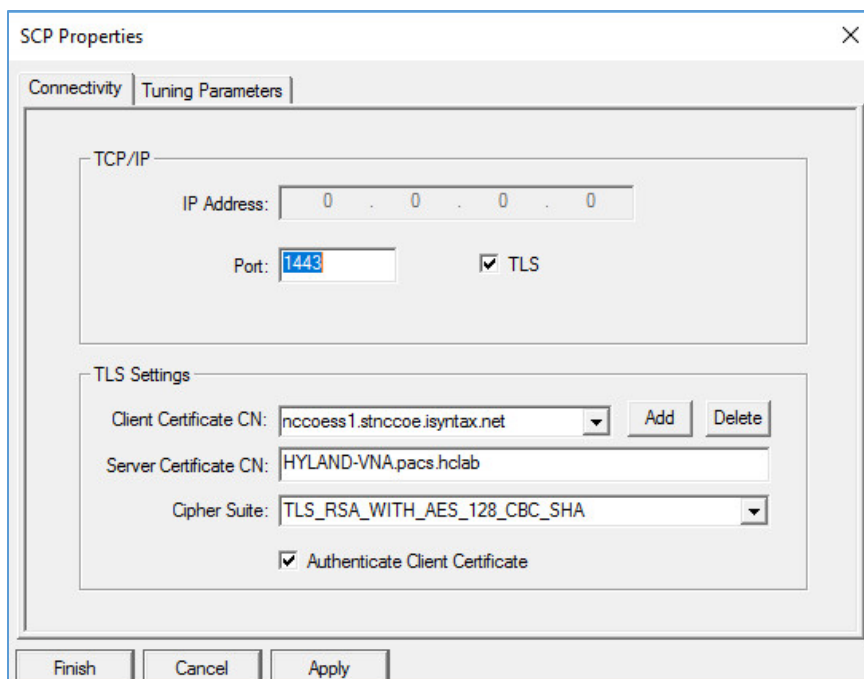
2.3.3.1 TLS Configuration for Hyland Acuo VNA

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

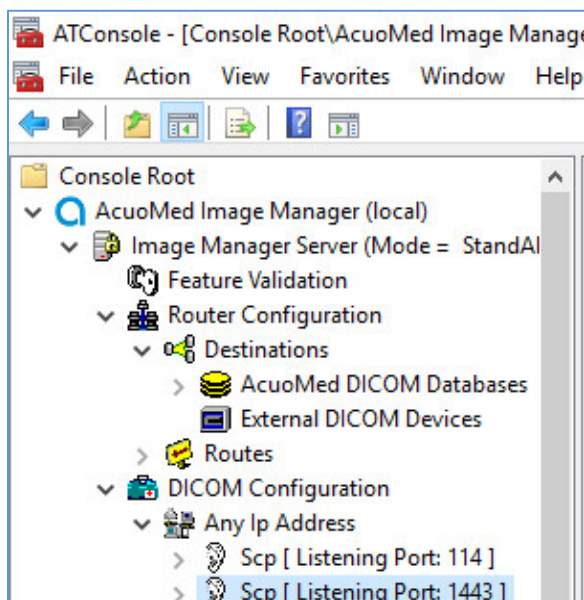
1. Open Microsoft **MMC** to access the **AcuoMed Image Manager (local)**:
2. From the **Console > AcuoMed Image Manager (local) > DICOM Configuration**, right-click **Any IP Address > New SCP ...** to create a new service class provider (SCP) for TLS encryption.



3. On the **Connectivity** tab of the **SCP** Properties page, provide the information below and click **Add**, **Apply**, then **Finish**:
 - **Port:** 1443
 - Check the **TLS** checkbox.
 - **Client Certificate CN:** nccoess1.stnccoe.issyntax.net
 - **Server Certificate CN:** HYLAND-VNA.pacs.hclab
 - **Cipher Suite:** TLS_RSA_WITH_AES_128_CBC_SHA
 - Check the **Authenticate Client Certificate** checkbox.



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**.

Called AE Properties

Main | SOP Configuration | External SCU Authorization | Options | Reconciliation | Postfetch Properties | Domain

AE Identification
Called AE Name:

Collaborative Routing
*Default Route Name:

Tag Rule Routing
Associated Tag Rules (And the Associated Reconciliation Dependencies):

Tag Rules

*Tag Failure Route:

Stat Route
**Stat Route Name:

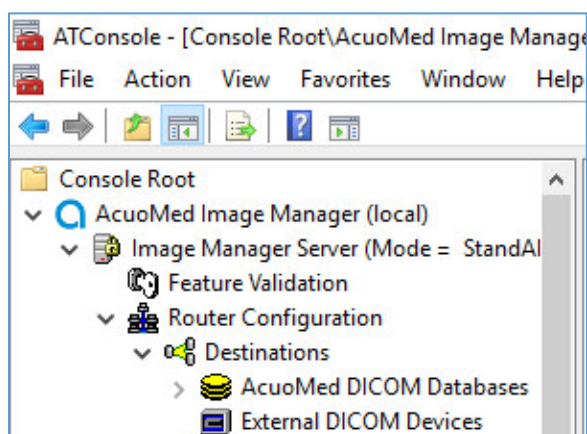
* Immediate C-STORE processing depends on the Reconciliation Settings for this AE. C-STORE processing will be delayed until the reconciliation detected problem is resolved if reconciliation is set for this AE.
 ** The C-STORE is always sent on this route even if it does not pass reconciliation.

Storage Destination Filtering
☐ Enable Filtering Tag:

Finish Cancel Apply

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

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



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

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

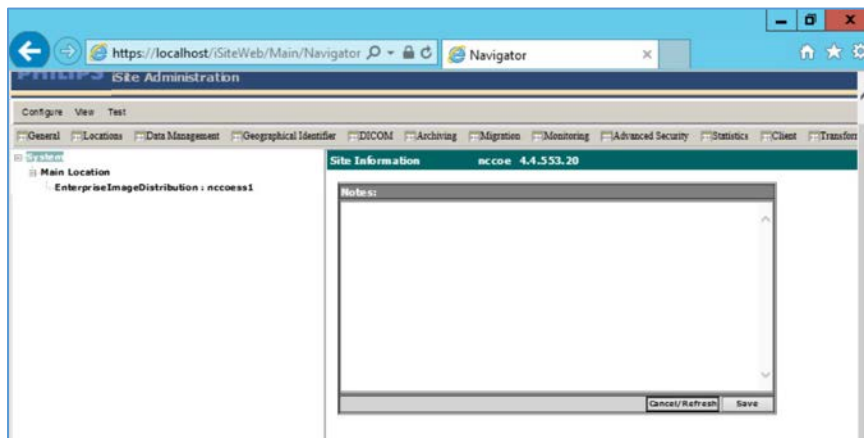
The screenshot shows the 'External DICOM Device Properties' dialog box with the 'Main' tab selected. The 'SCP Destination Name' is 'PHILIPS'. Under 'External Device', 'Called AE Name' is 'STENTOR_SCP'. The 'TCP/IP Connectivity' section shows 'Host Name' as an empty field and 'IP Address' as '192.168.140.131'. 'SCP Listening Port' is '2762' and the 'TLS' checkbox is checked. The 'AcuoMed' section shows 'Calling AE Name' as 'ACUO', 'Implementation UID' as '1.2.840.114158.1.1.3', and 'Version Name' as 'AcuoMed'. The 'TLS Settings' section shows 'Client Certificate CN' as 'HYLAND-VNA.pacs.hclab', 'Server Certificate CN' as 'nccoess1.stnccoe.isyntax.net', and 'Cipher Suite' as 'TLS_RSA_WITH_AES_128_CBC_SHA'. The 'Connection Testing' section has a 'Test' button. At the bottom are 'Finish', 'Cancel', and 'Apply' buttons.

4. Restart the **AcuoMed** service.

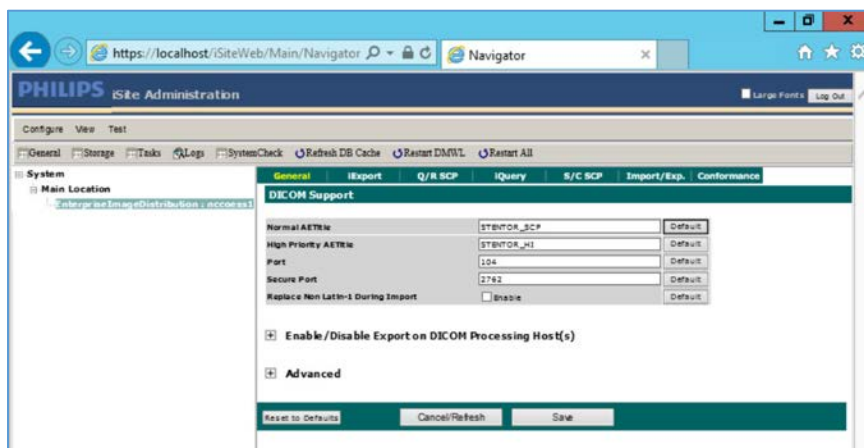
2.3.3.2 TLS Configuration for Philips IntelliSpace PACS

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

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

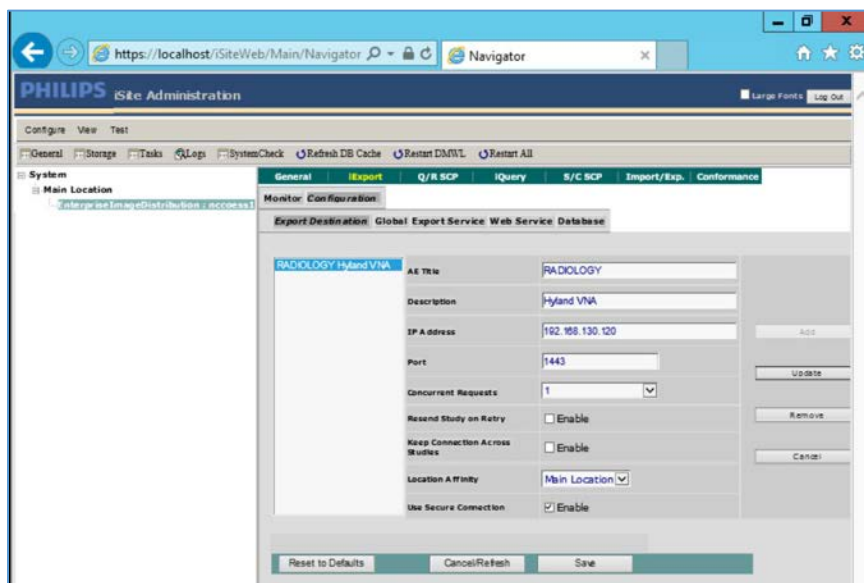


2. Click **Configuration > DICOM** to navigate to the DICOM configuration screen.



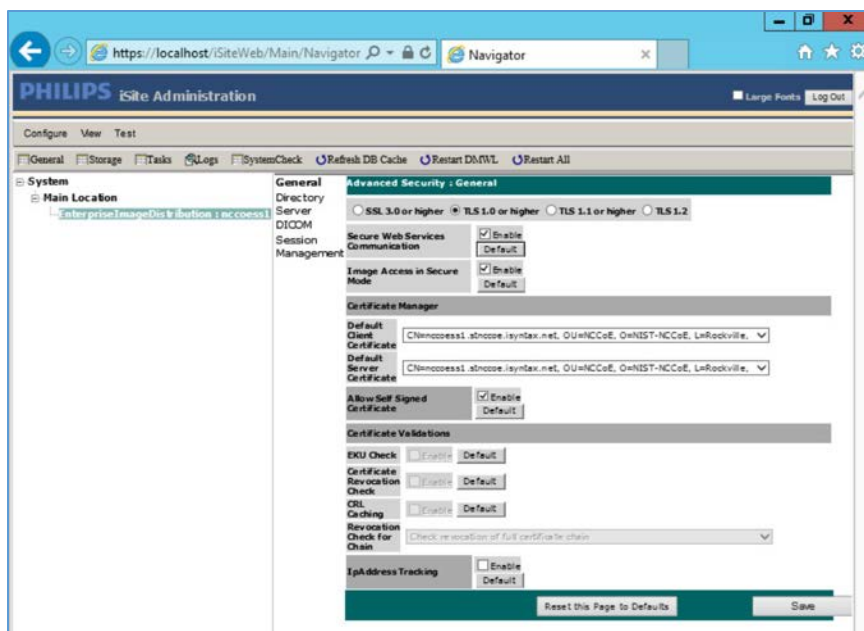
3. On the top menu, click **iExport** to open the **iExport** screen. Provide the information below, and click **Save**:
 - **AE Title:** RADIOLOGY
 - **Description:** Hyland VNA
 - **IP Address:** 192.168.130.120

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

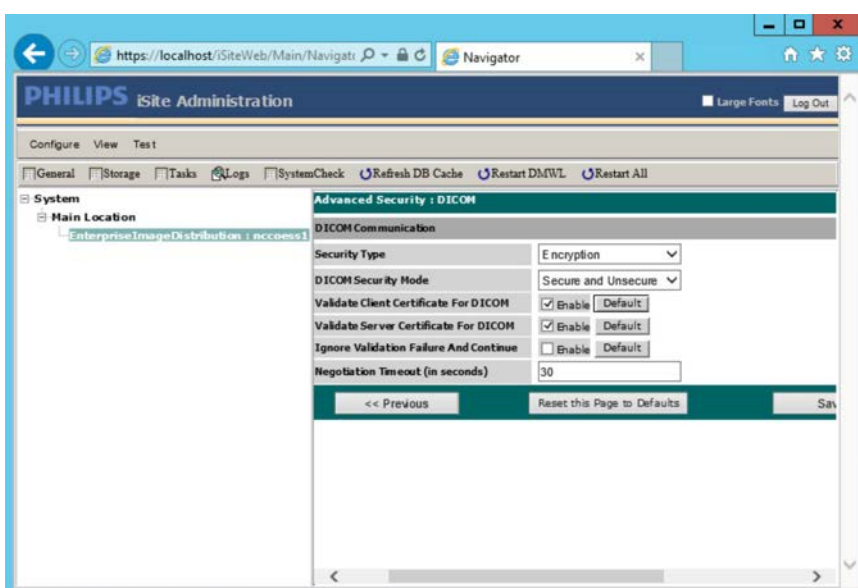


4. Click **Configuration > Advanced Security**, and make these selections:

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



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



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

2.3.4 PACS and VNA TLS Integration Tests

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

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

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

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

2.4 Modalities

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

2.4.1 DVTk Modality Emulator

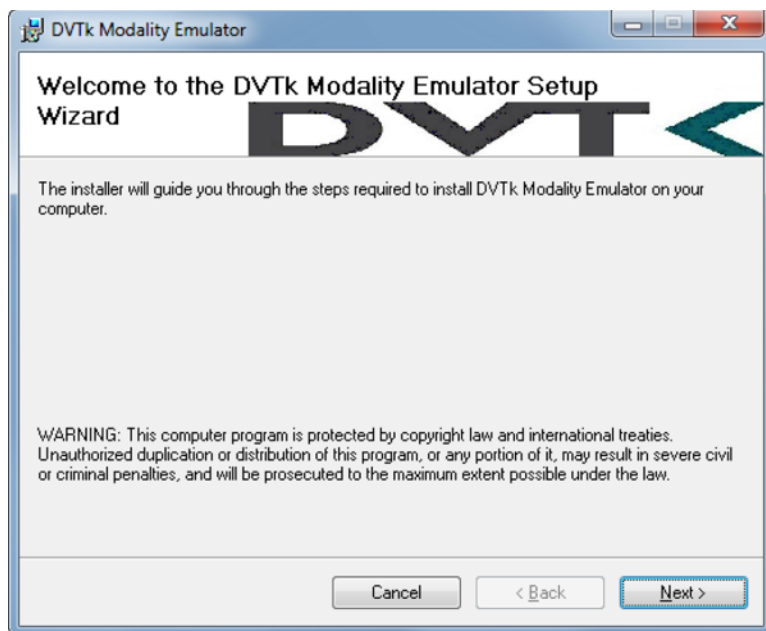
DVTk Modality is a modality emulator that can emulate all the DICOM functions of a modality system. It can simulate a real modality to test and verify communication with all the DICOM services. It uses DICOM files as input for queries, MPPS, and storage actions. Consequently, this project used the DVTk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

System Requirements

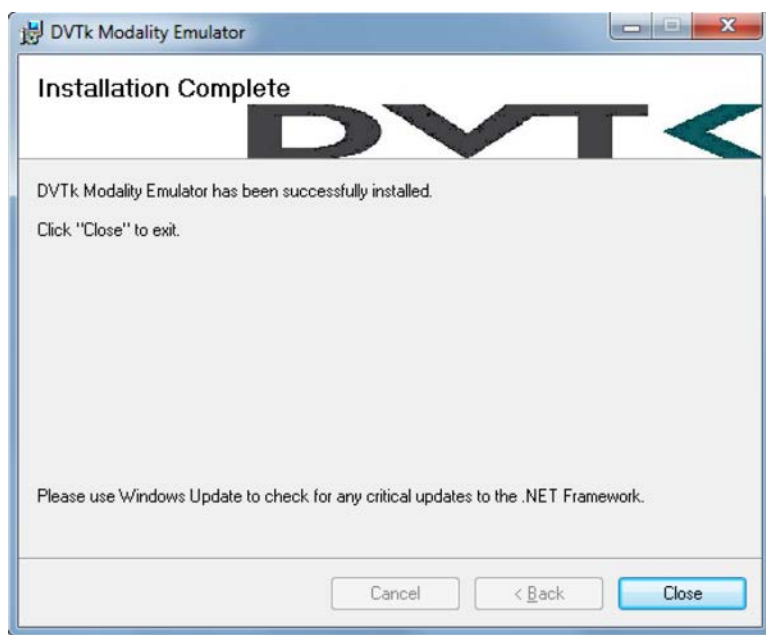
- **Operating System:** Microsoft Windows 7 (with Microsoft .NET 4.0 Framework)
- **Network Adapter:** VLAN 1402

DVTk Modality Installation

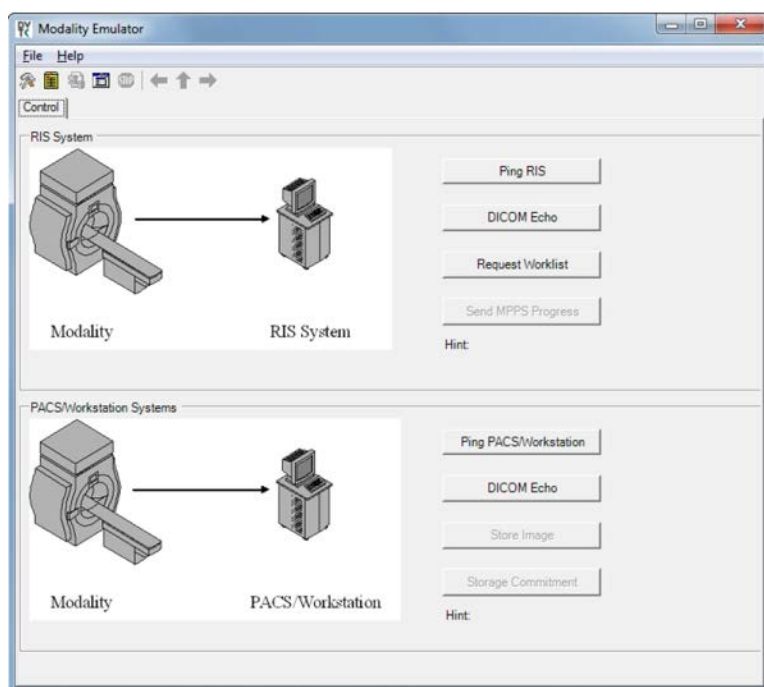
1. Download the installation software from the DVTk site [4].
2. Click the **Modality Installation** file (e.g., *DVTk-Modality-Emulator-5.0.0.msi*) to start the installation process.



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



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

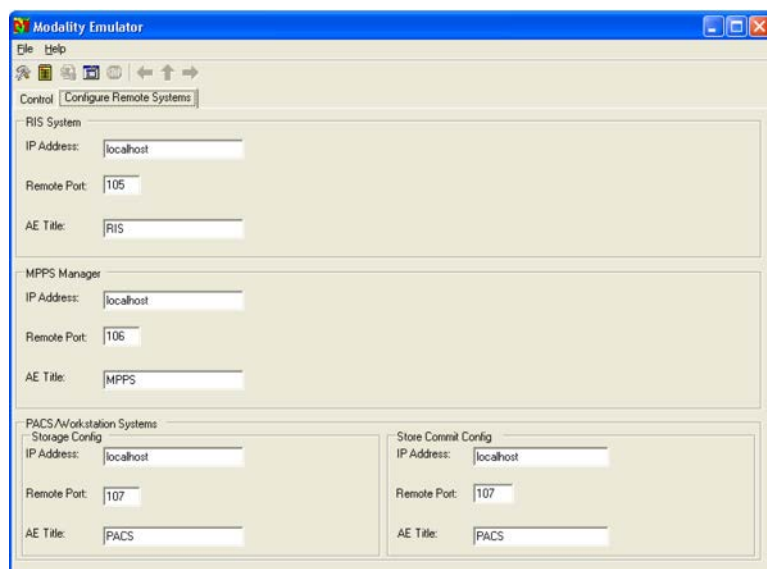


DVTk Modality Configuration

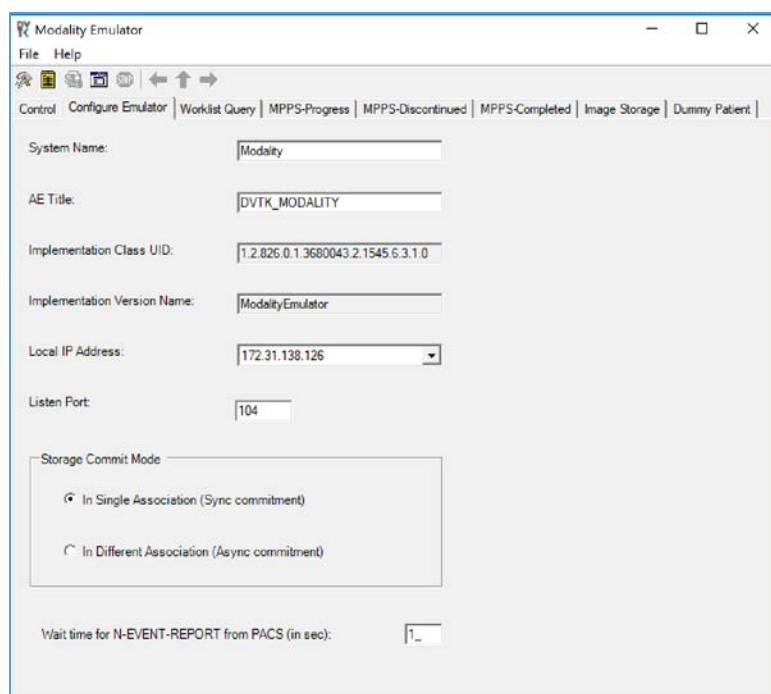
Configuration of the DVTk Modality involves configuration of the communications with different external systems, including the RIS, which is the worklist provider or a work-list broker connected to the RIS; the MPPS manager that handles the MPPS messages for status reporting; and the PACS and its DB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

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

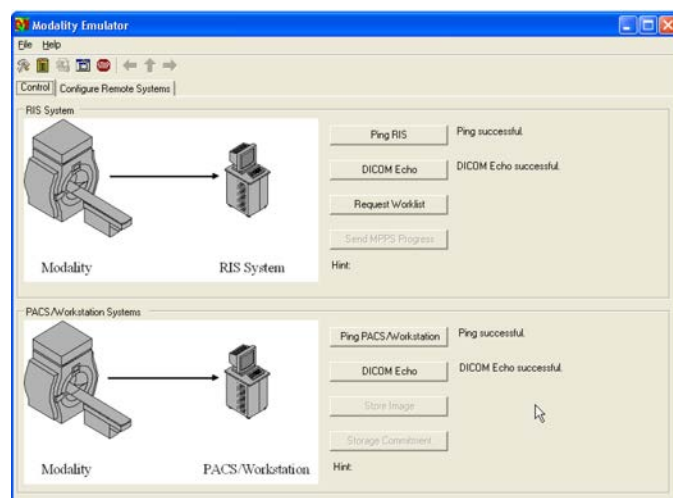
- **Remote Port:** 106
- **AE Title:** MPPS
- **PACS/Workstation Systems–Storage Commit Config**
- **IP Address:** localhost
- **Remote Port:** 107
- **AE Title:** PACS
- **Store Commit Config**
- **IP Address:** localhost
- **Remote Port:** 107
- **AE Title:** PACS



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



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



2.4.2 DVTk RIS Emulator

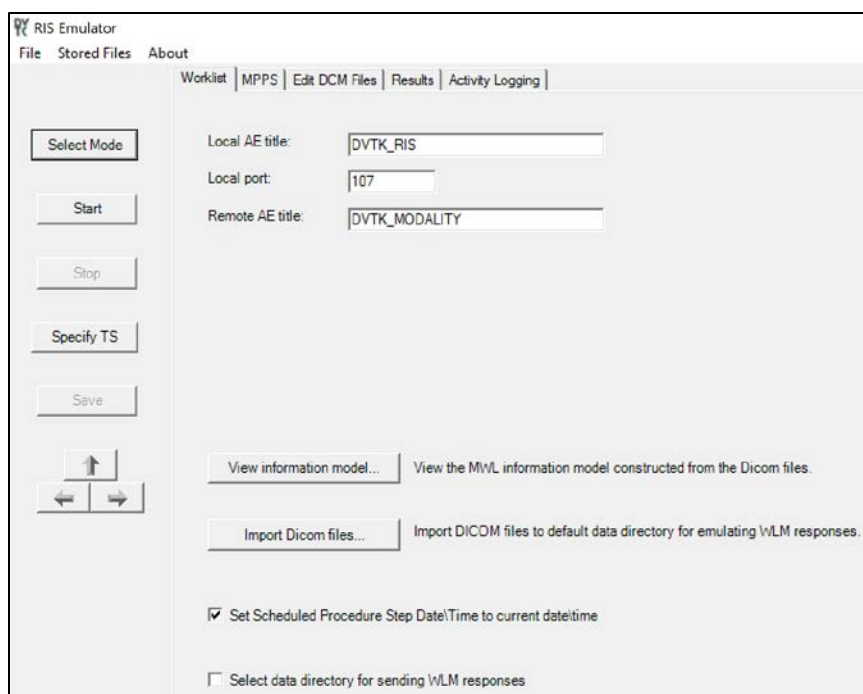
DVTk, the Health Validation Toolkit, is an open-source software. The DVTk RIS Emulator is an application that handles Modality Worklist and Modality Performance Procedure Step requests from remote applications and then responds with the emulated results using the DICOM files specified by the users.

System Requirements

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

DVTk RIS Emulator Installation

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



DVTk RIS Emulator Configuration

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

2.5 Asset and Risk Management

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

2.5.1 Virta Labs BlueFlow

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

System Requirements

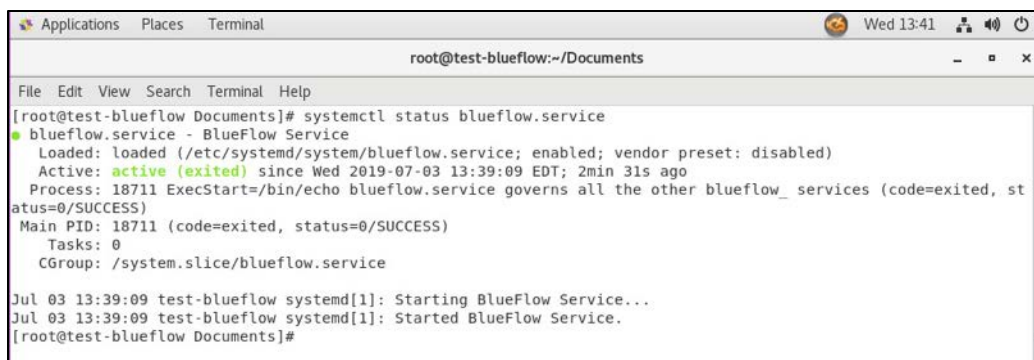
- **CPUs:** 2
- **Memory:** 8 GB RAM
- **Storage:** 100 GB (thin provision)
- **Operating System:** CentOS 7
- **Network Adapter:** VLAN 1201

Virta Labs BlueFlow Installation

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



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



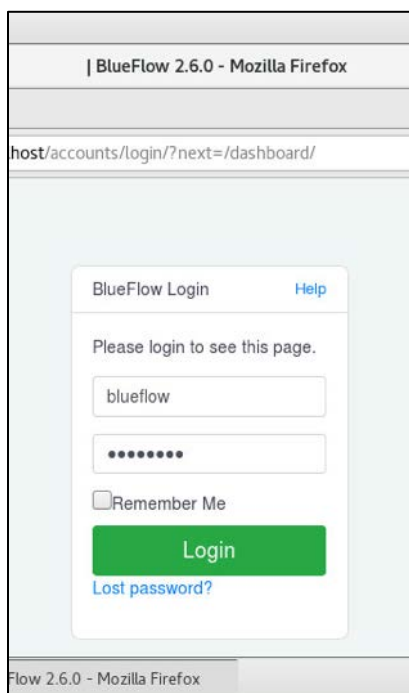
```

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

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

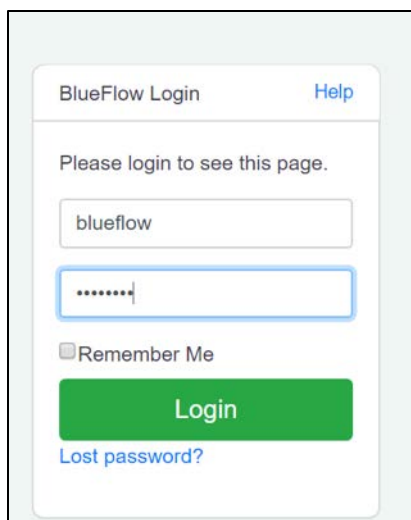
```

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



Virta Labs BlueFlow Network Groups Configuration

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



BlueFlow Login [Help](#)

Please login to see this page.

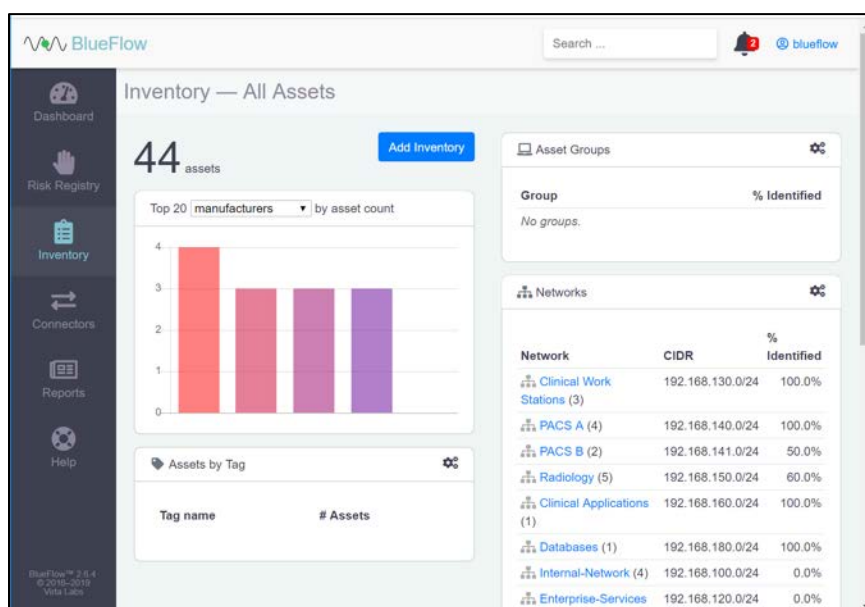
blueflow

☐ Remember Me

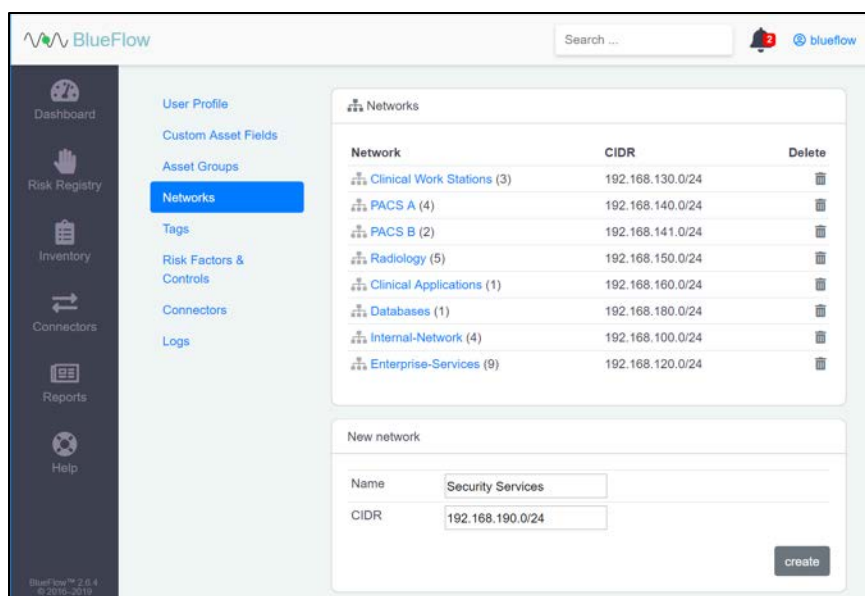
Login

[Lost password?](#)

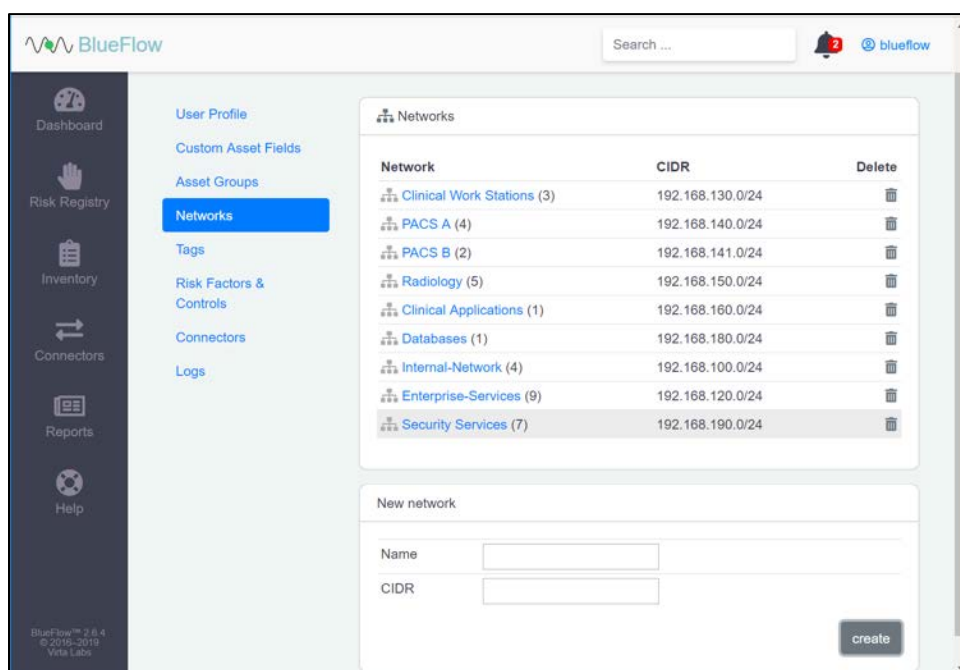
2. Navigate to the **Inventory** tab.
3. Under the **Networks** section, click the **gear** icon.



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

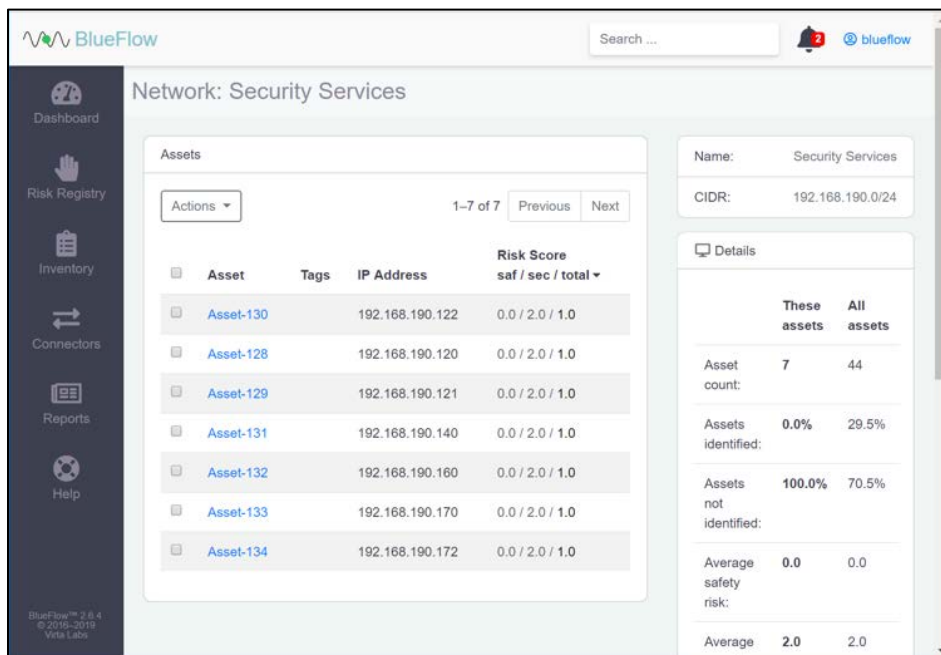


7. Verify that the new **network group (Security Services)** has been created.
8. Click the **name** of the new network group.



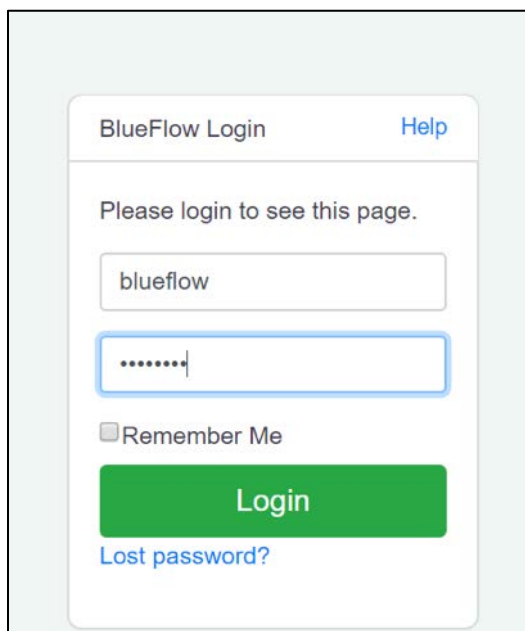
9. **Assets** will be listed on this page if they match the network group's criteria.

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).

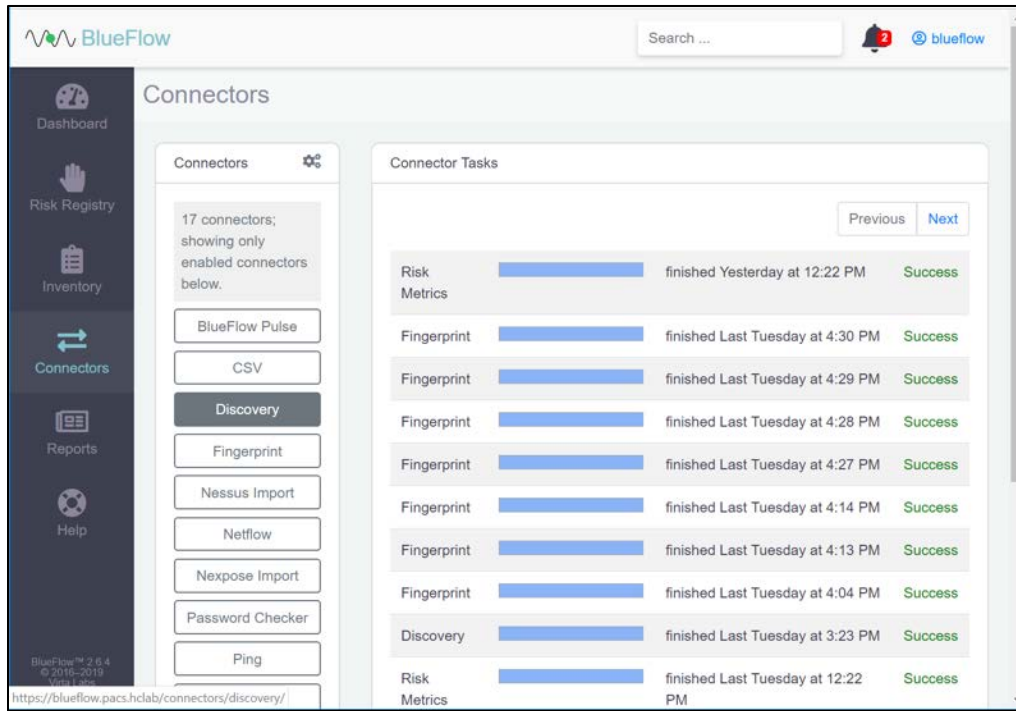


Running an IP Discovery Scan in Virta Labs BlueFlow

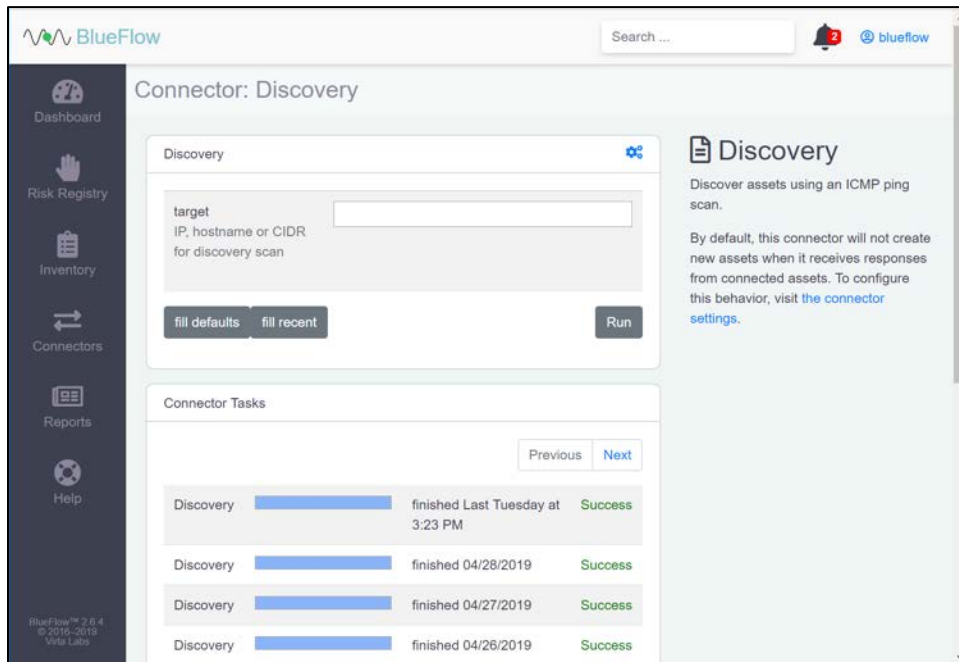
1. Log in to the **BlueFlow** web console.



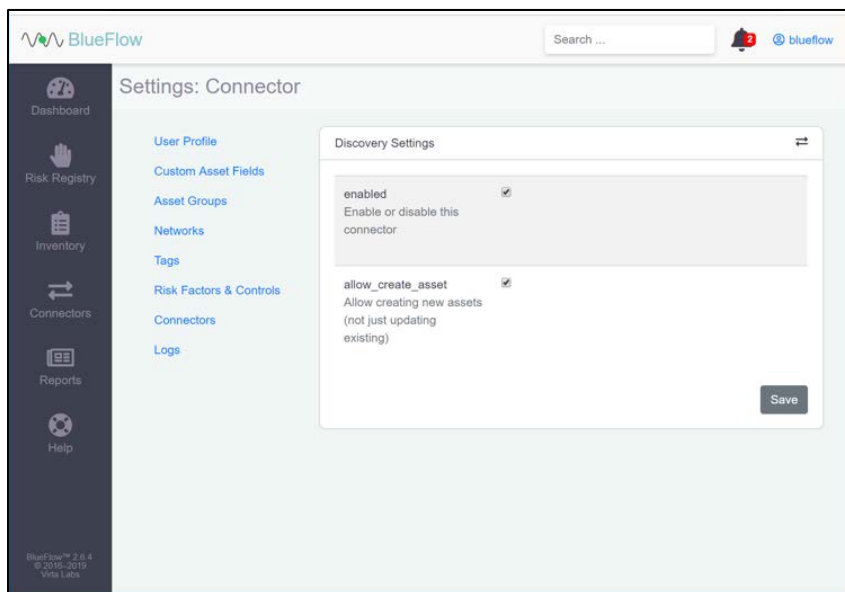
2. Navigate to **Connectors > Discovery**.



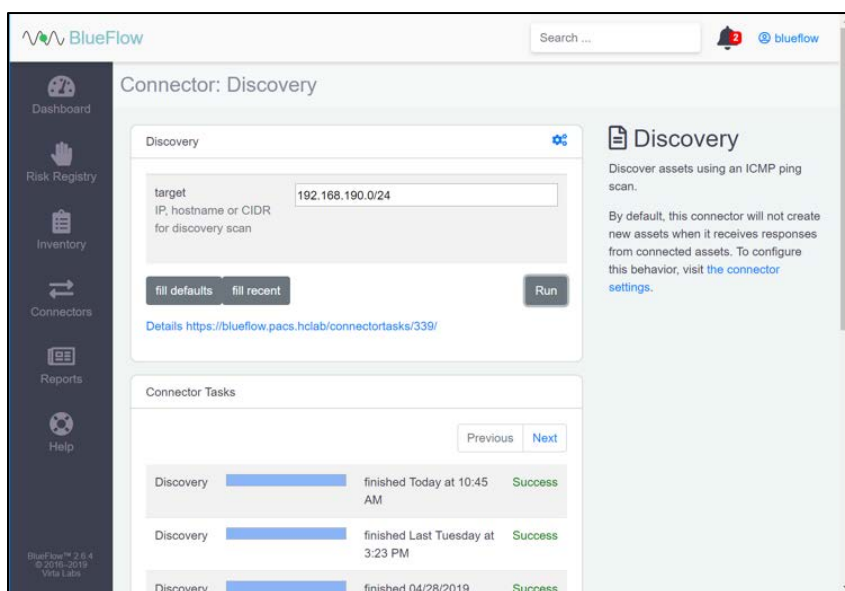
3. Under **Discovery**, click the gear icon.



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

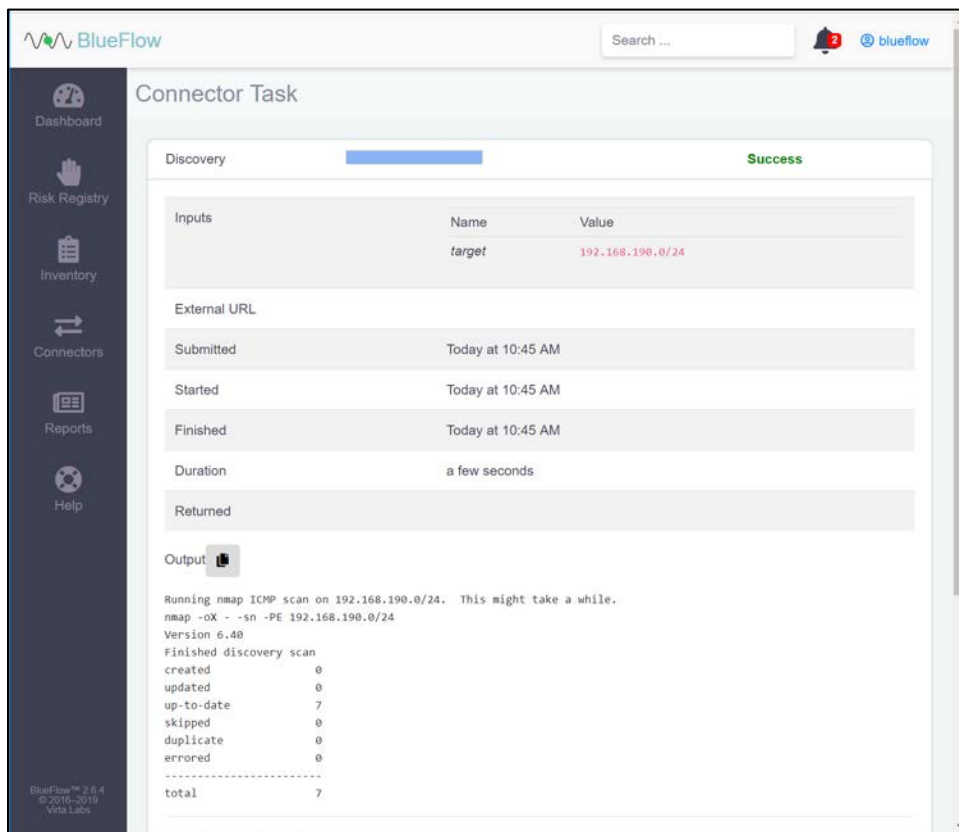


6. Enter an IP (e.g., **192.168.190.0/24**), **host name**, or **CIDR** that you would like to scan.
7. Click **Run**.
8. Wait for the discovery scan to finish.



9. Click 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

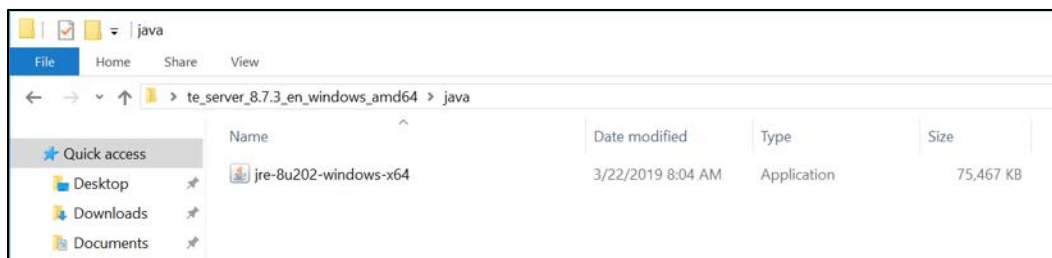
Tripwire Enterprise is a security configuration management software that monitors file integrity through software-based agents. For this project, we used Tripwire Enterprise to monitor file changes on PACS servers and the VNA DB.

System Requirements

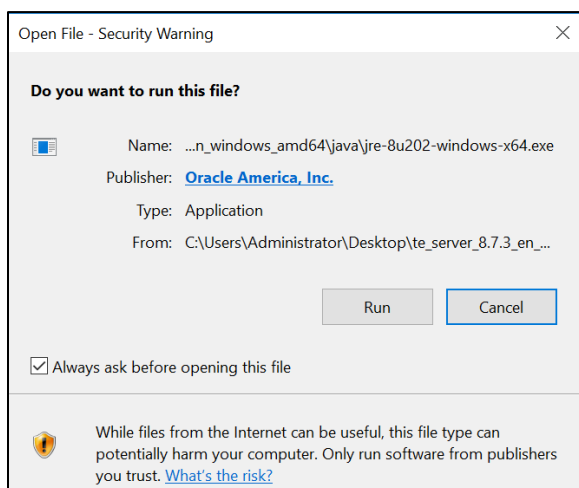
- **CPU:** 1
- **Memory:** 4 GB RAM
- **Storage:** 120 GB (thin provision)
- **Operating System:** Microsoft Windows Server 2016
- **Network Adapter:** VLAN 1201

Tripwire Enterprise Console Installation

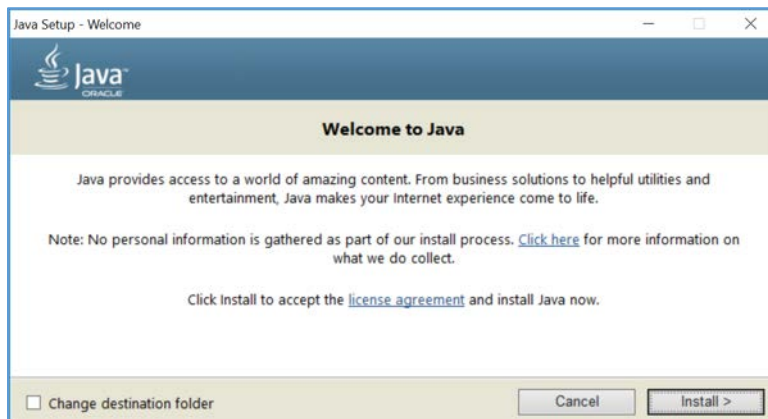
1. In the *tripwire install* folder under java, double-click the *jre-8u202-windows-x64 application* file.



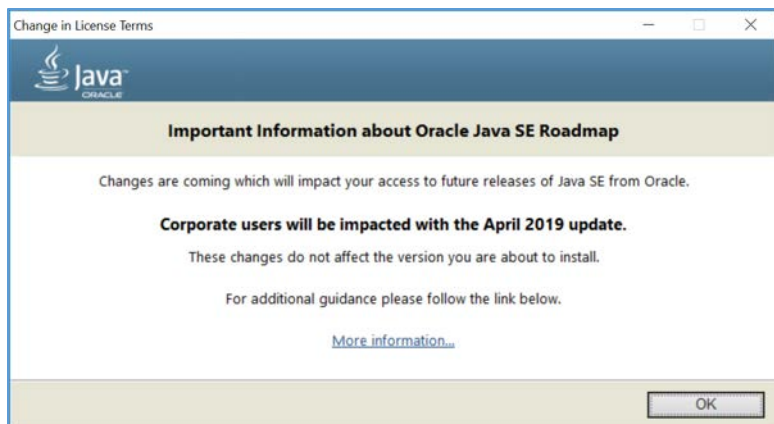
2. Click **Run**.



3. Click **Install >**.



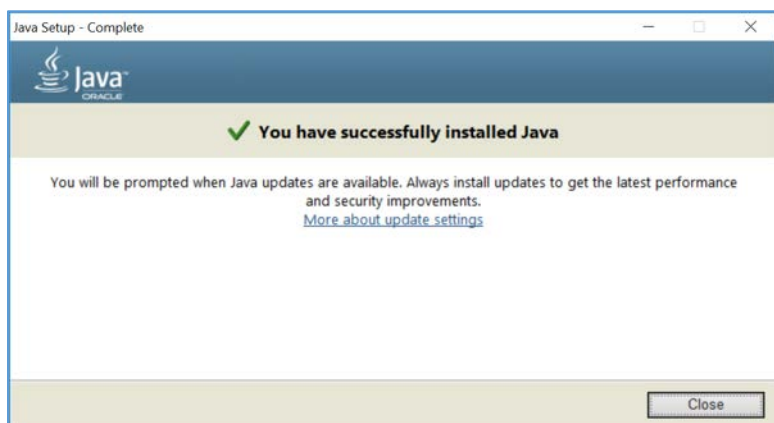
4. Click **OK**.



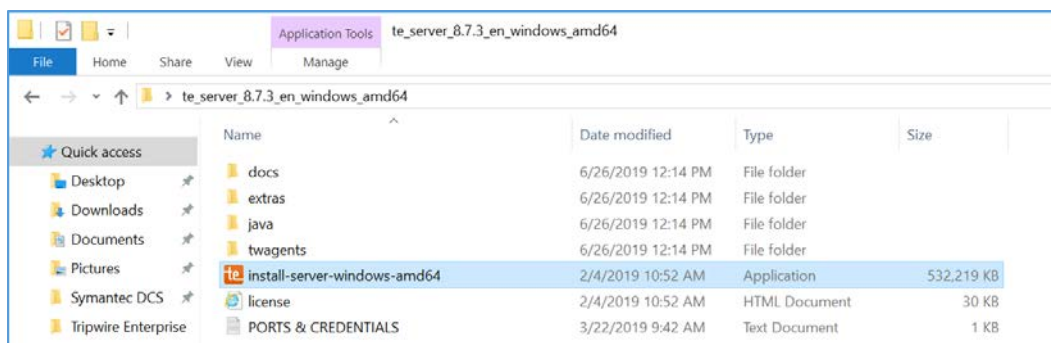
5. Wait for the installation process to complete.



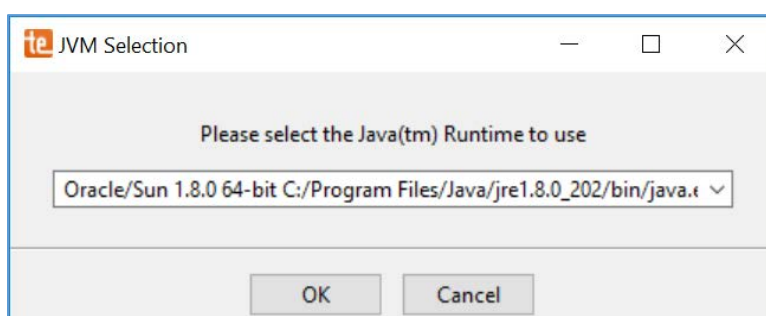
6. Click **Close**.



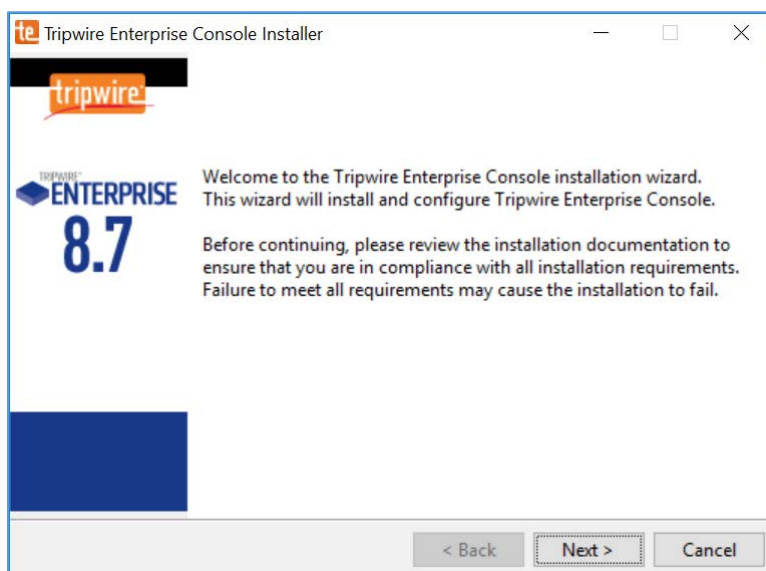
7. With Java installed, double-click the Tripwire install application, *install-server-windows-amd64*.



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

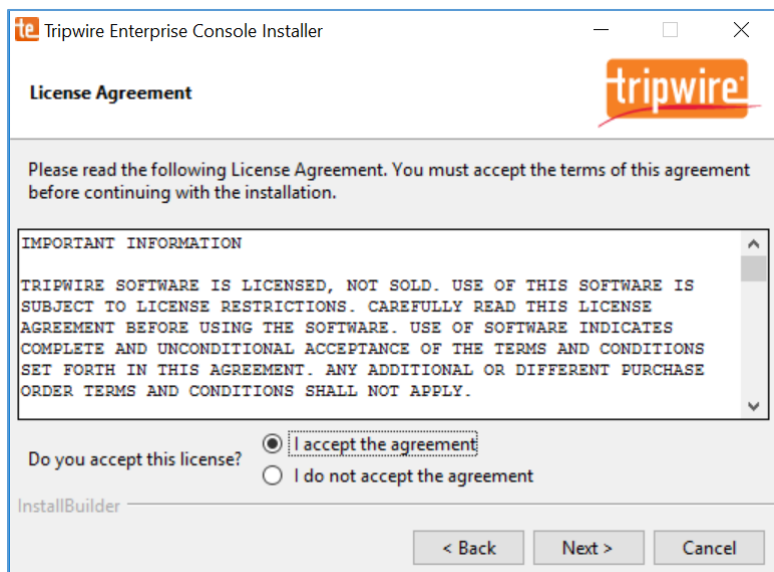


10. Click **Next >**.



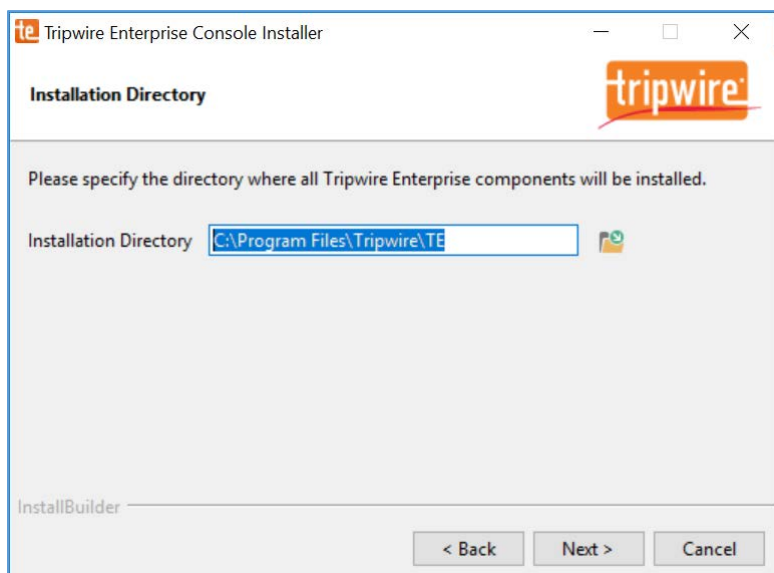
11. Check **I accept the agreement**.

12. Click **Next >**.



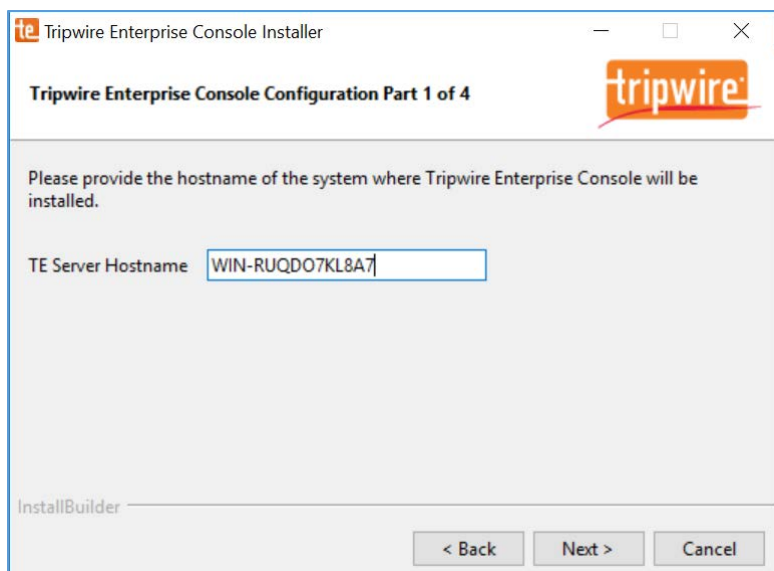
13. Specify an installation directory, *C:\Program Files\Tripwire\TE*, for the Tripwire installation.

14. Click **Next >**.



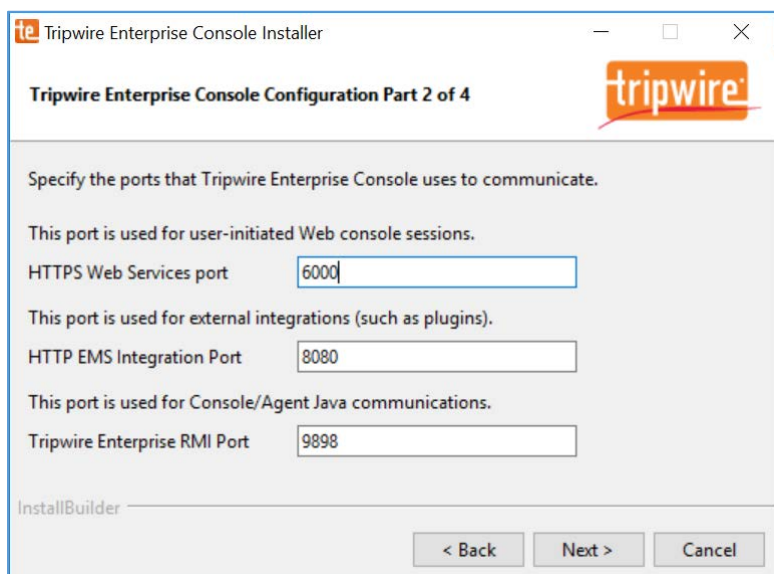
15. Verify the host name for the machine on which you are installing Tripwire (e.g., WIN-RUQDO7KL8A7).

16. Click **Next >**.



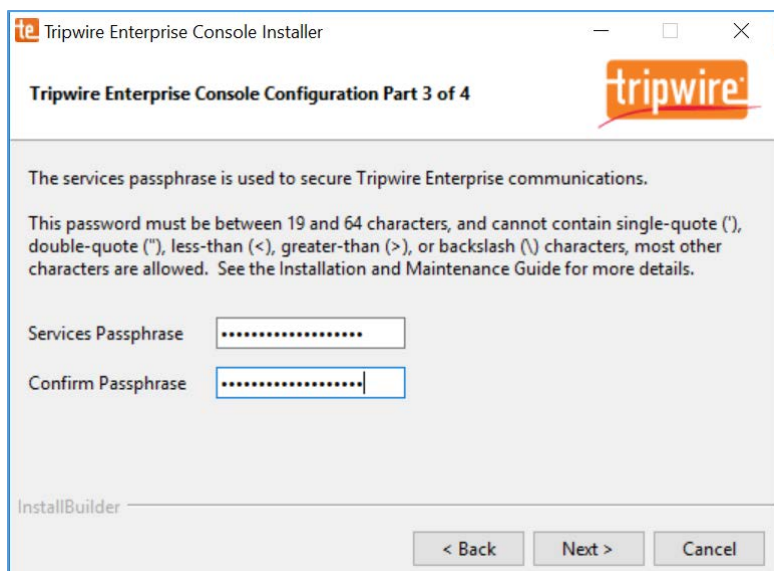
17. Specify the **HTTPS Web Services port** as **6000**, **HTTP EMS Integration Port** as **8080**, and **Tripwire Enterprise RMI Port** as **9898**.

18. Click **Next >**.



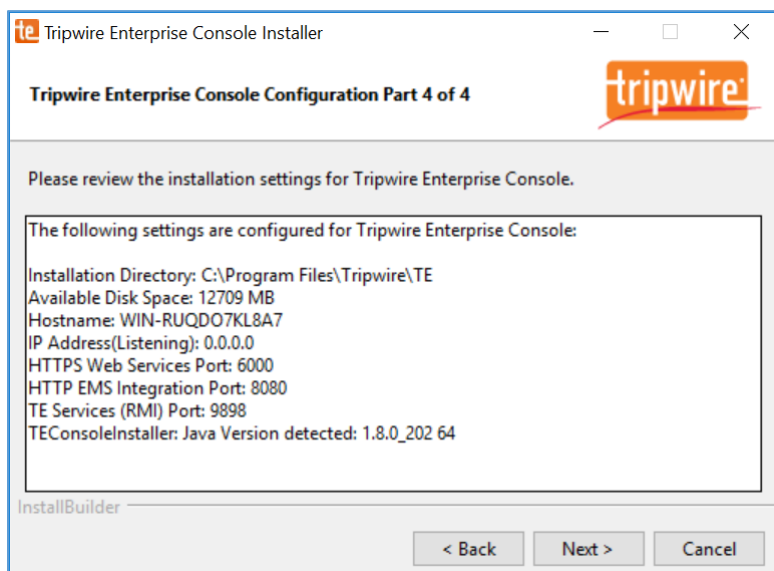
19. Create a password for Tripwire Enterprise services.

20. Click **Next >**.



21. Verify that planned installation settings are correct.

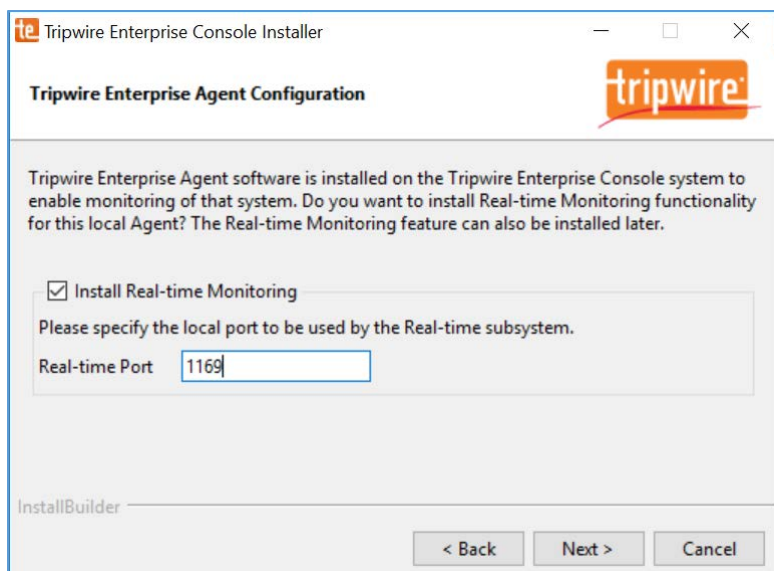
22. Click **Next >**.



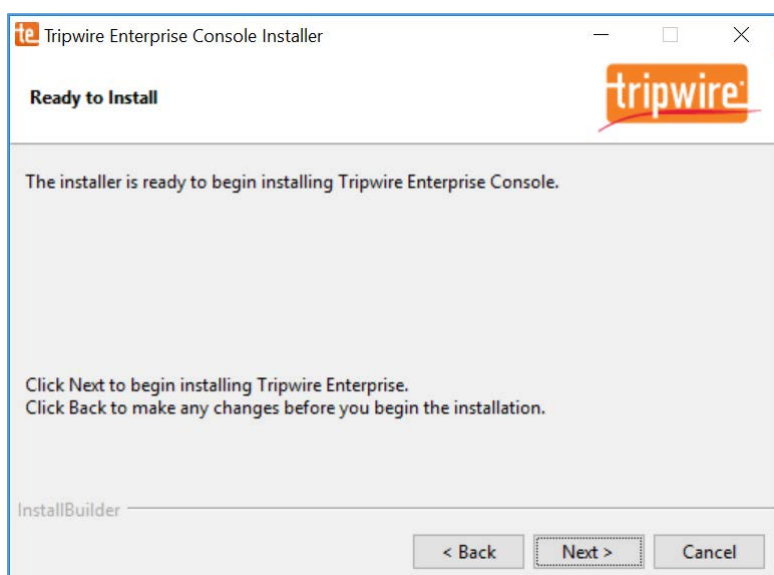
23. Check **Install Real-time Monitoring**.

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

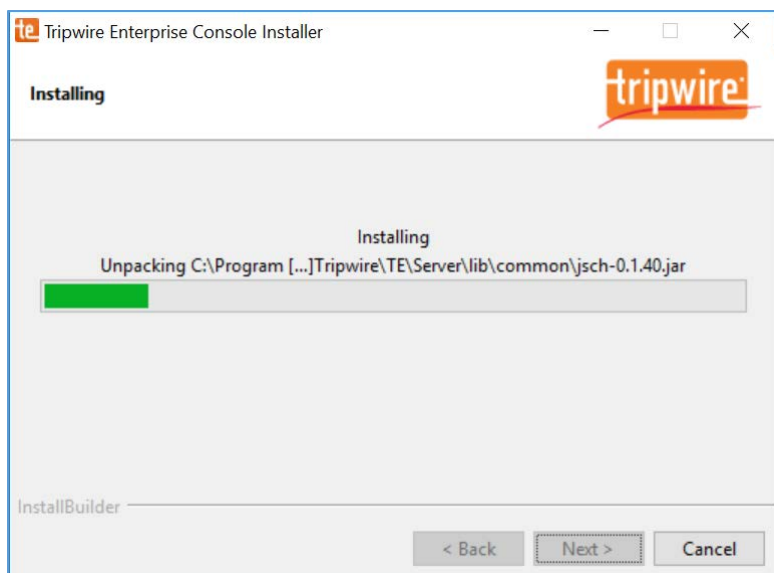
25. Click **Next >**.



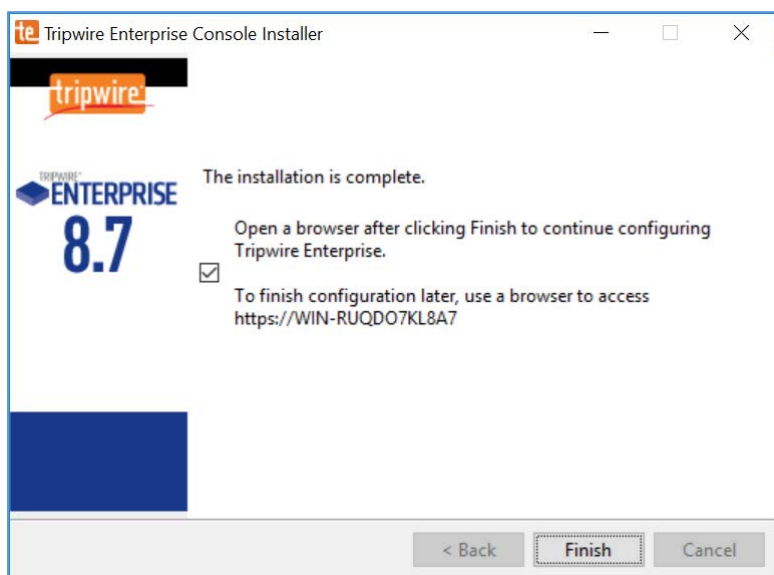
26. Click **Next >**.



27. Wait for Tripwire Enterprise installation to complete.

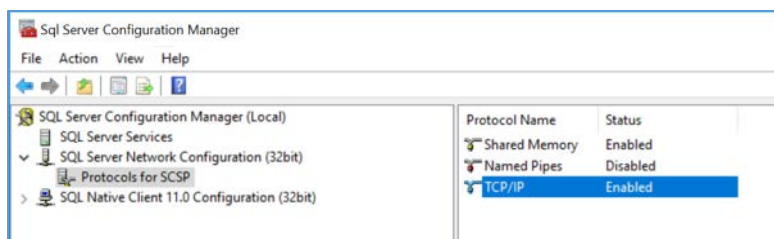


28. Click **Finish**.

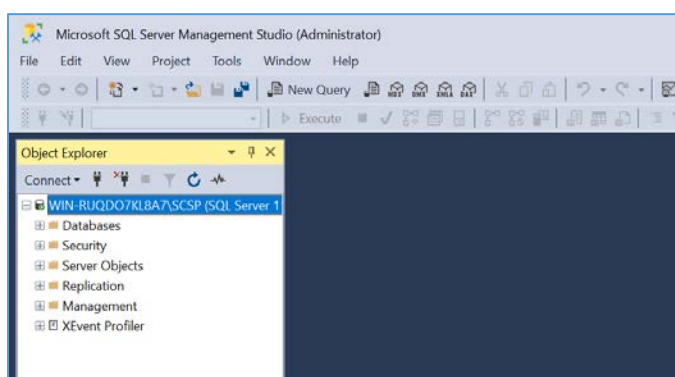


29. Open SQL Server Configuration Manger.

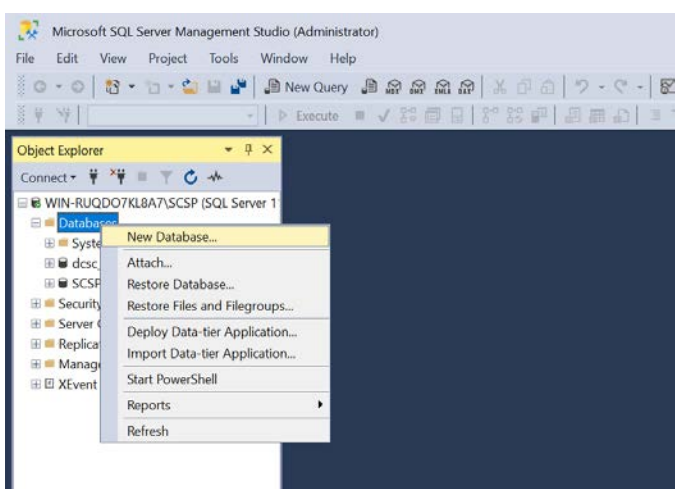
30. Under **SQL Server Network Configuration > Protocols for SQL Server**, ensure that the **TCP/IP protocol** is set to **Enabled**.



31. Open SQL Server Management Studio.



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

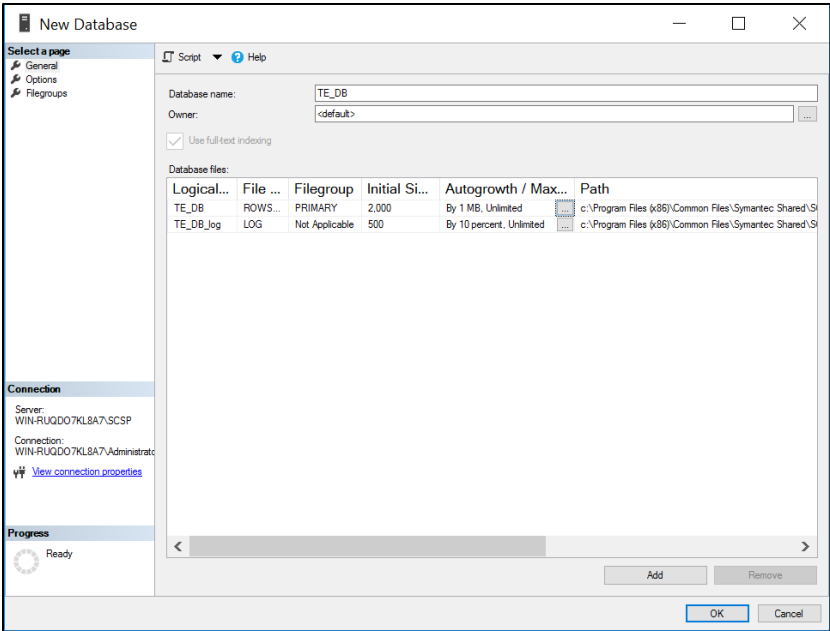


33. On the left, under **Select a page**, select **General**.

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

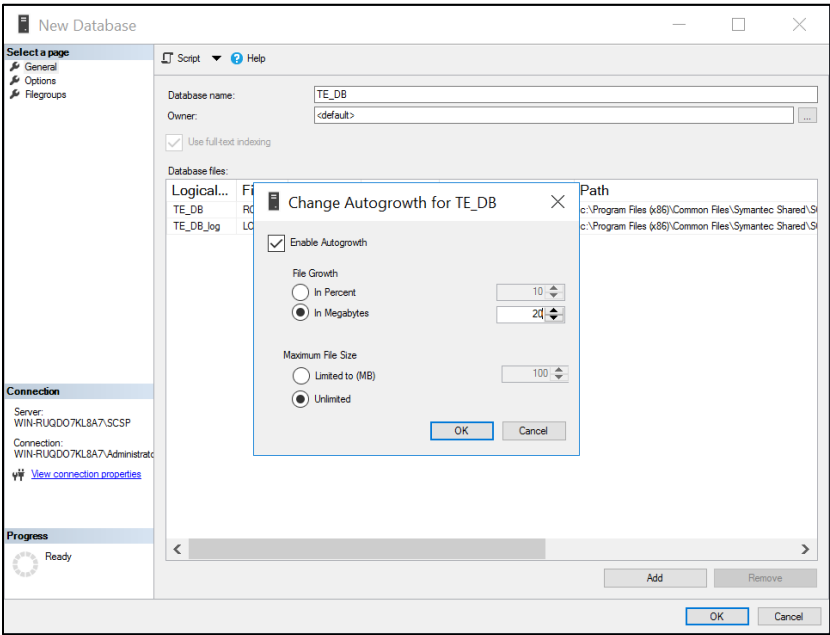
35. Under **Database files**, for the data file, set **Initial Size** to at least **2,000**.

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

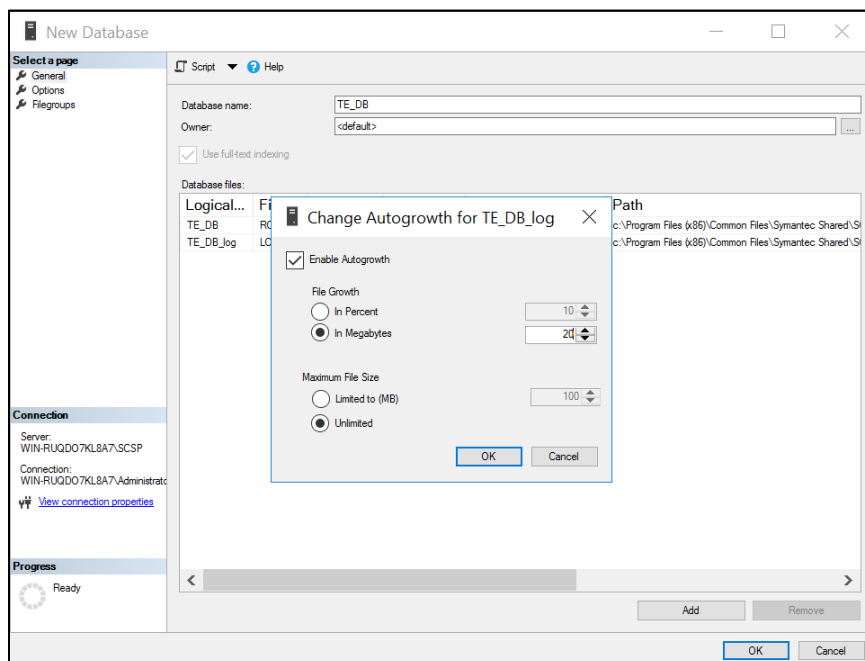


37. Check **Enable Autogrowth**, set **File Growth** to at least **20 MB**, and set **Maximum File Size** to **Unlimited**.

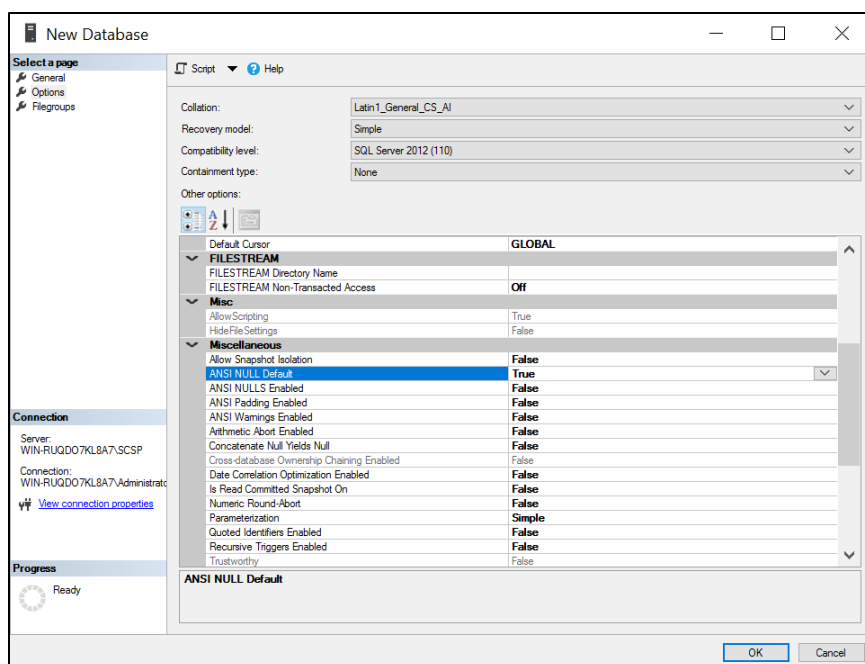
38. Click **OK**.



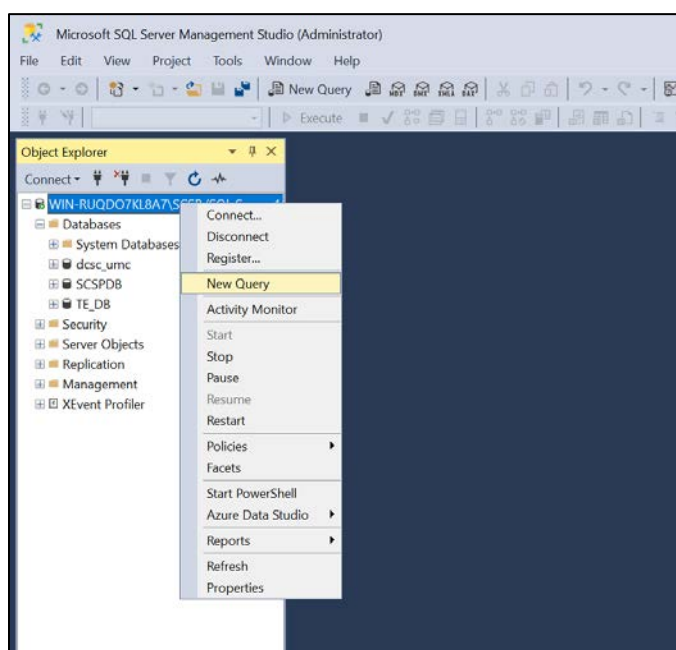
39. Under **Database files**, for the log file, set **Initial Size** to at least **500**.
40. Click the **in Megabytes** button under **Enable Autogrowth**.
41. Check **Enable Autogrowth**, set **File Growth** to at least **20 MB**, and set **Maximum File Size** to **Unlimited**.
42. Click **OK**.



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**.



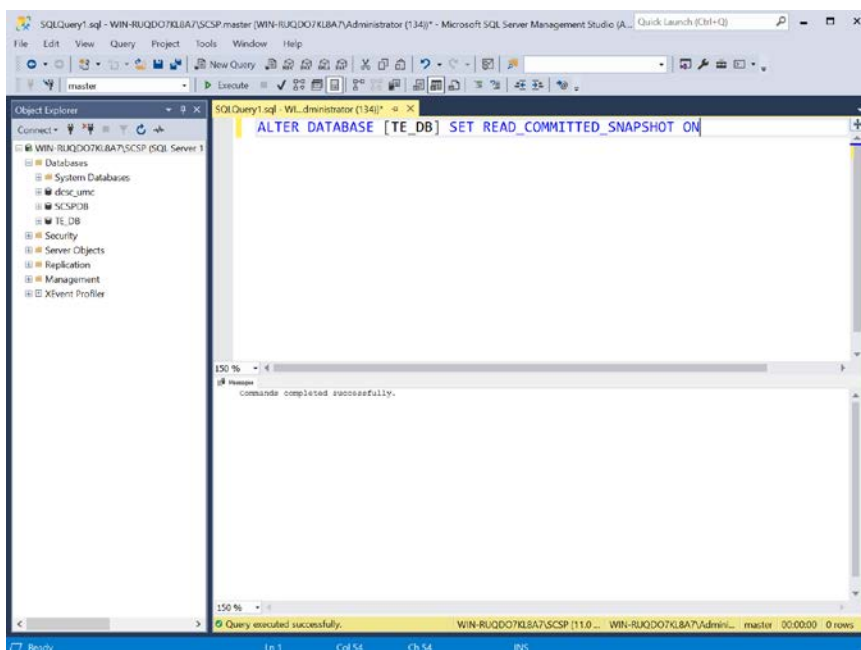
48. In the **Object Explorer**, right-click your DB and select **New Query**.



49. Type the following query:

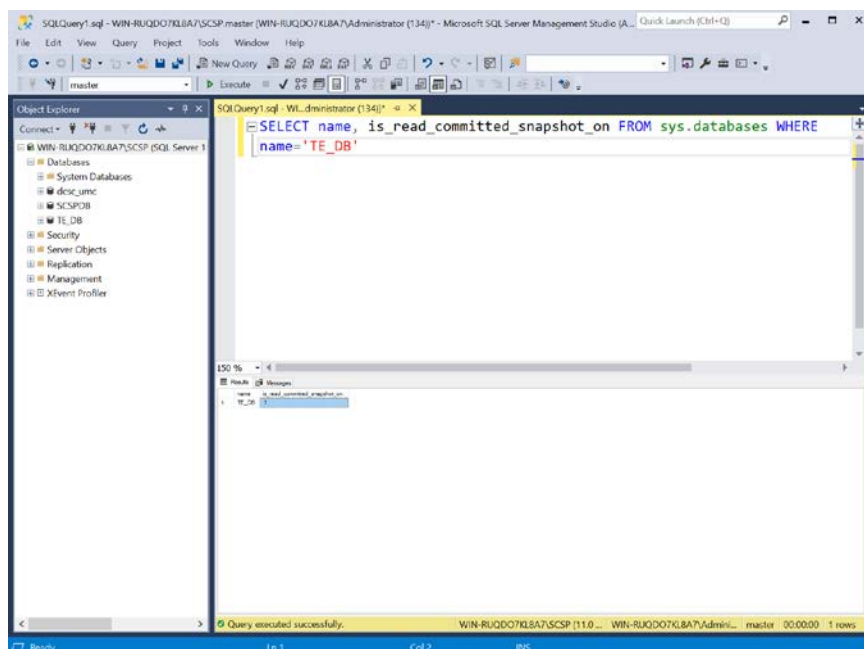
```
ALTER DATABASE [TE_DB] SET READ_COMMITTED_SNAPSHOT ON
```

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

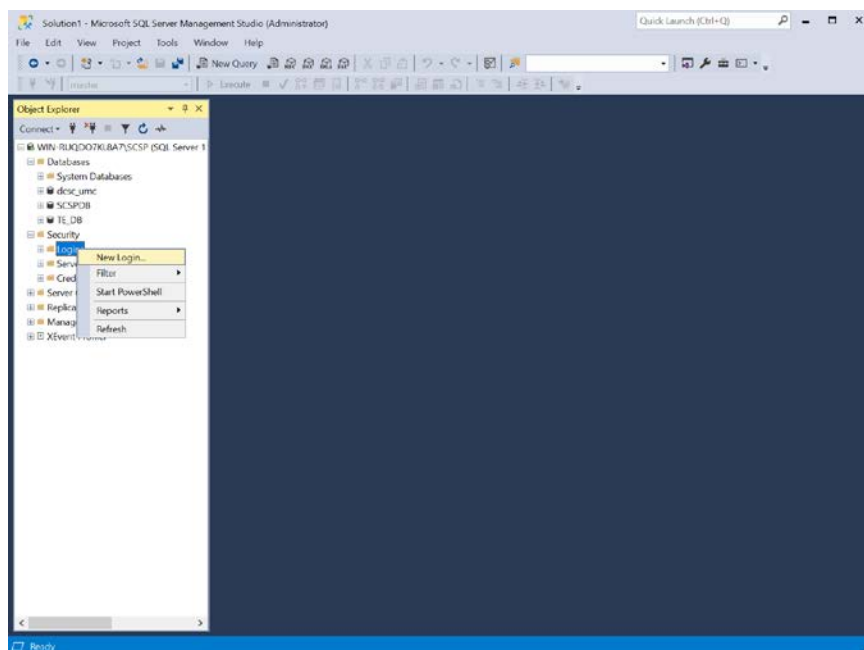


52. Clear the **SQL Query** window, then type the following query:


```
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**.



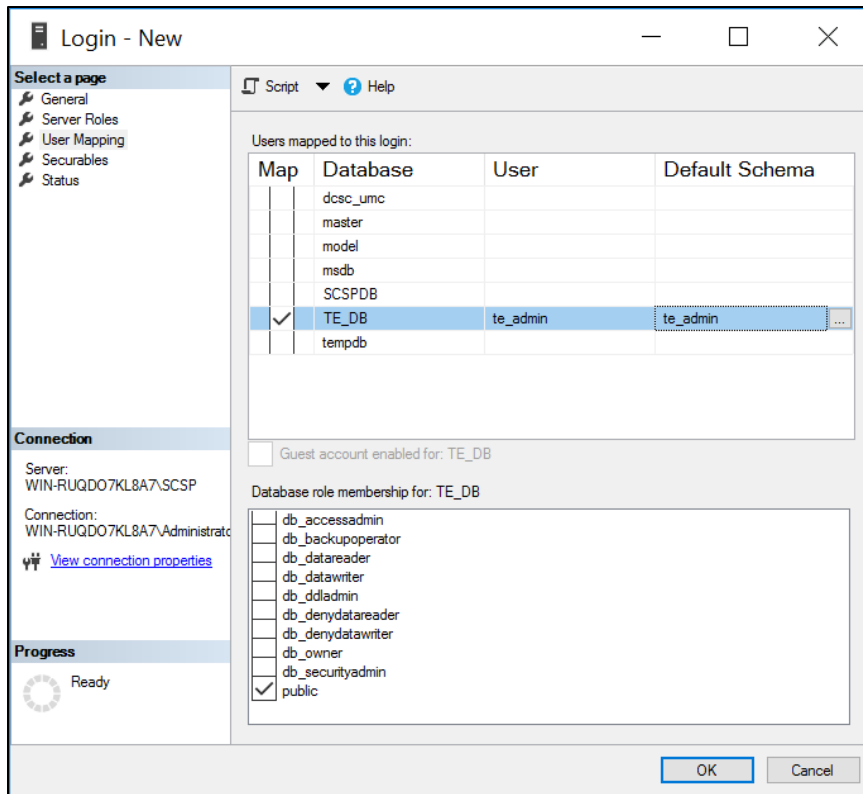
55. In the **Object Explorer**, expand the selection for your DB, expand the **Security** section, right-click **Logins**, and select **New Login...**



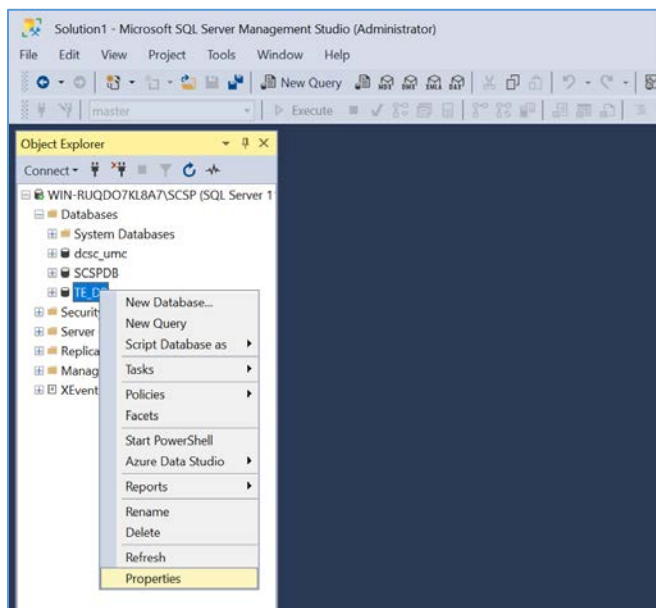
56. On the left, under **Select a page**, select **General**.
57. Create a **Login name**.

58. Select **SQL Server authentication**.
59. Create a **password**.
60. For **Default database**, select the DB 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 DB:
 - a. Check the box in the **Map** column.
 - b. In the **Default Schema** column, type the name of the new user being created.
64. Click **OK**.



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

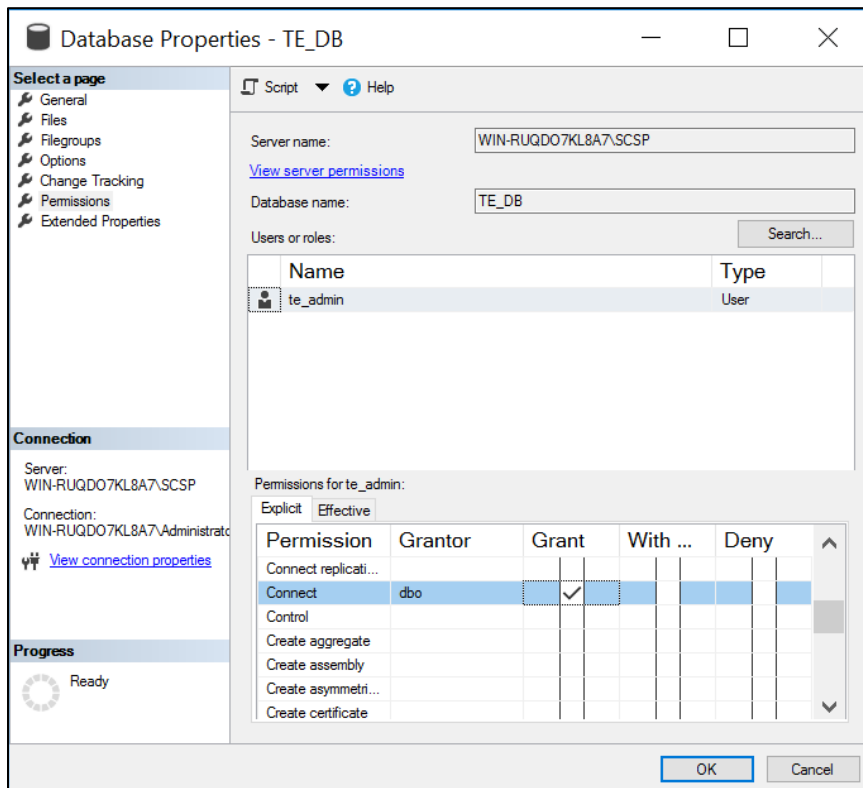


66. On the left, under **select a page**, select **Permissions**.

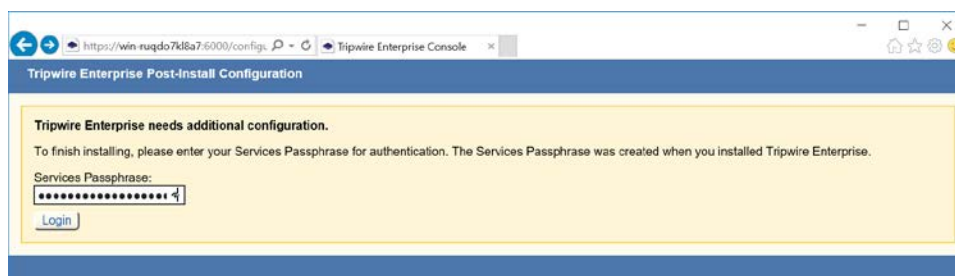
67. Under **Permissions for user**, check the box in the **Grant** column for the following permissions:

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

68. Click **OK**.



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



72. Under **Database Configuration Settings**, provide the information that follows:
 - **Remote Database Type:** Microsoft SQL Server
 - **Authentication Type:** SQL Server
 - **Login Name:** *****
 - **Password:** *****
 - **Database Host:** WIN-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

Tripwire Enterprise Post-Install Configuration

Database Configuration Settings

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

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

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

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

Login Name: <input type="text" value="te_admin"/>	Login Name: The login name that TE will use to authenticate with the database.
Password: <input type="password" value="*****"/>	Password: The password that TE will use to authenticate with the database.
Database Host: <input type="text" value="WIN-RUQDO7KL8A7"/>	Database Host: The fully qualified domain name, hostname or IP address of the system where the database is installed.
Port (default 1433): <input type="text" value="(UDP 1434)"/>	Port: The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.
Database Name: <input type="text" value="TE_DB"/>	Database Name: The name of the database that TE should use when connecting to the remote database. Note that the login name in SQL Server should have this database set as the default, and the login name should be mapped to this database.
Instance Name (Optional): <input type="text" value="SCSP"/>	Instance Name (Optional): The location/name of the database instance on the server. Ask your DBA if a non-default instance should be used for TE.
SSL: <input type="button" value="Request"/>	SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL. <ul style="list-style-type: none"> • Request - SSL will be used if available. • Require - SSL will always be used, and an error will occur if SSL is not available for the database. • Authenticate - SSL will always be used, and an error will occur if SSL is not available for the database. In addition, the certificate chain of the database server's public key will be authenticated using TE's trust store. If the certificate chain does not originate from a trusted source, an error will occur. • Off - SSL will never be used. This setting is not recommended.
<input type="button" value="Test Database Login"/> ✓	
Test Results: <div style="border: 1px solid black; padding: 5px; min-height: 40px;"> Connection Succeeded. </div>	

Tripwire Enterprise 8.7.3.b8.7.3.r20190111122005-03196dc.b24

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

Tripwire Enterprise

Tripwire Enterprise is restarting.

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

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

77. Click **Login**.

Tripwire Enterprise Post-Install Configuration

Tripwire Enterprise needs additional configuration.

To finish installing, please enter your Services Passphrase for authentication. The Services Passphrase was created when you installed Tripwire Enterprise.

Services Passphrase:

[Login](#)

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

79. Click **Confirm and Continue**.

Tripwire Enterprise Post-Install Configuration

Configuration Steps Needed:

Tripwire administrator account password needs to be changed from the default.

Create Administrator Password

Passwords must:

- Be between 8 and 128 characters in length
- Contain at least 1 numeric character
- Contain at least 1 uppercase character
- Contain at least 1 non-alphanumeric character
- Supported characters: `~!@#%&*'()-_+={}|\\;:~" '<>./?`

Password:

Confirm Password:

[Confirm and Continue](#)

Support Information

Still having problems with your installation?

Contact Tripwire Support:
<https://secure.tripwire.com/customers/contact-support.cfm>

Or open a Support ticket: <https://secure.tripwire.com/customers/>

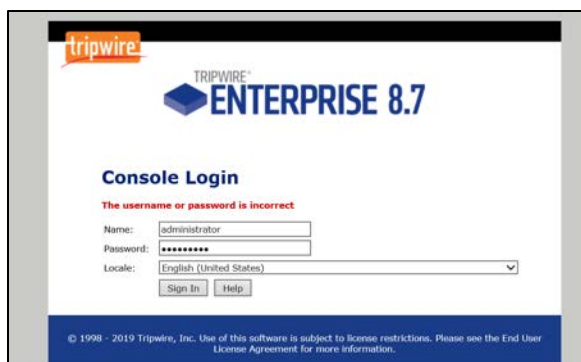
For faster assistance from Support, please generate a support bundle to collect information about your system and this installation. Attach the support bundle file to your web ticket or email. [What is a Support Bundle?](#)

[Generate Support Bundle](#)

Tripwire Enterprise 8.7.3.b8.7.3.r20190111122005-03196dc.b24 [Logout](#)

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

81. Click **Sign In**.

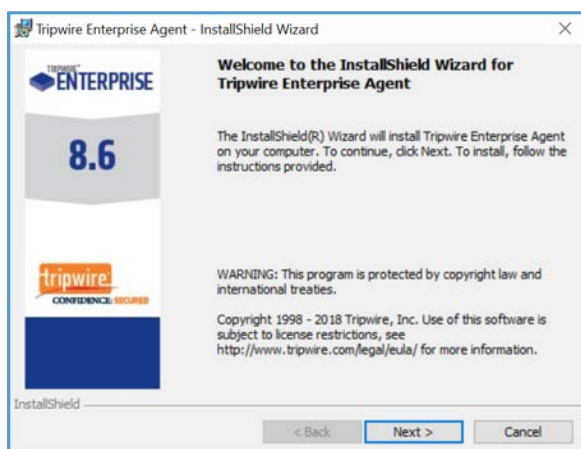


82. Click **Configure Tripwire Enterprise** to begin the configuration process.

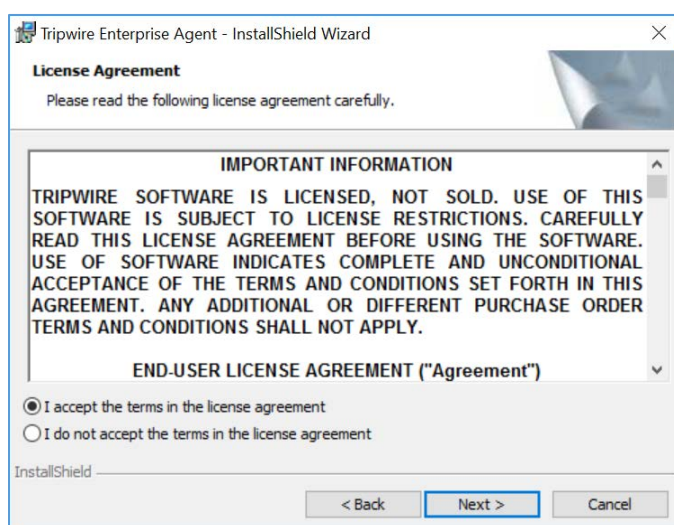


Tripwire Enterprise Agent Installation

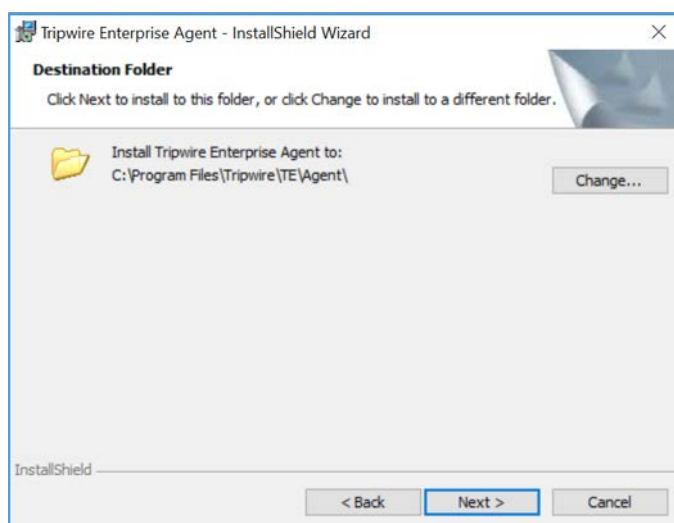
1. Run `te_agent.msi`.
2. Click **Next >**.



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



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



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

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

Tripwire Enterprise Agent - InstallShield Wizard

Tripwire Enterprise Server Information

Enter the Tripwire Enterprise Server hostname and the number of the Services Port for your Tripwire Enterprise Console:

* TE Server is the fully-qualified domain name of the machine where Tripwire Enterprise Console is installed.
 * The Services Port was specified when you installed the Tripwire Enterprise Console.
 * For more information on Real-Time Monitoring, see the Tripwire Enterprise User Guide.
 * For more information on FIPS, see the Tripwire Enterprise Installation & Maintenance Guide.

IE Server :

Services Port :

☒ Start Agent after installation

☒ Install Real-Time Monitoring Port :

☐ Enable FIPS HTTP Port :

InstallShield

< Back Next > Cancel

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

Tripwire Enterprise Agent - InstallShield Wizard

Tripwire Enterprise Proxy Information

If the Tripwire Enterprise Agent should use a proxy to communicate with the Tripwire Enterprise Server, enter the Tripwire Enterprise Proxy hostname and port number for your proxy host. Otherwise, leave these fields blank.

Proxy Host: (leave blank for no proxy)

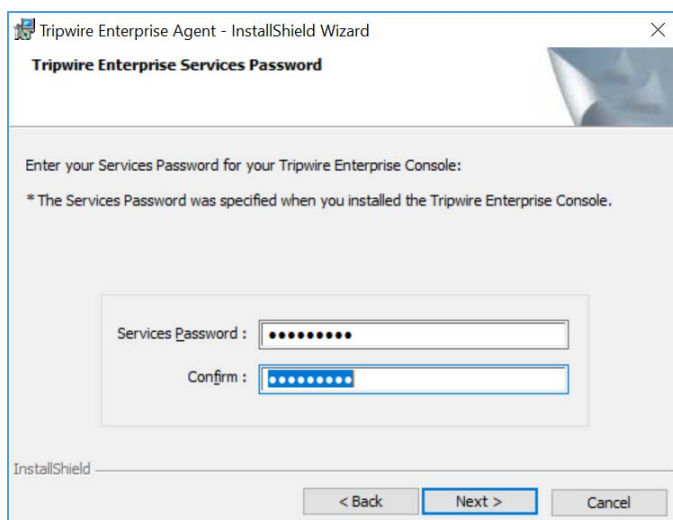
Proxy Port: (leave blank for default)

InstallShield

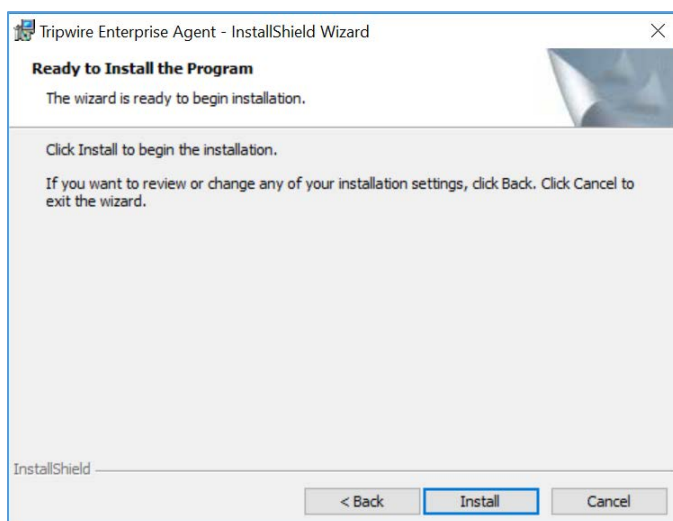
< Back Next > Cancel

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

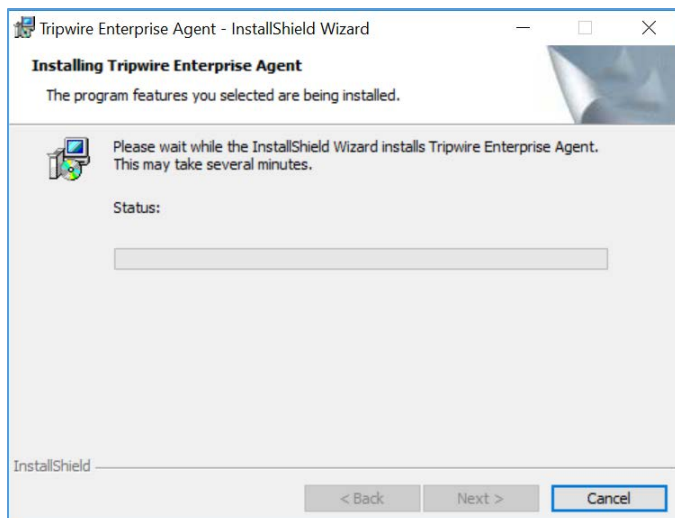
16. Click **Next >**.



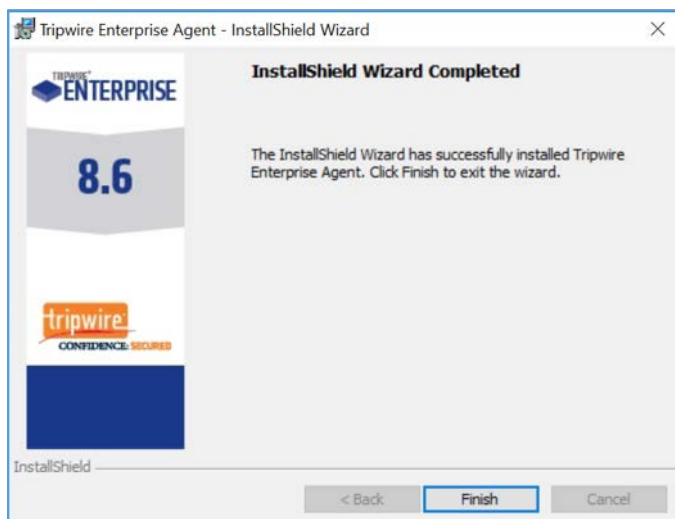
17. Click **Install**.



18. Wait for the installation process to complete.



19. Click **Finish**.



2.6 Enterprise Domain Identity Management

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

2.6.1 Domain Controller with AD, DNS, and DHCP

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

System Requirements

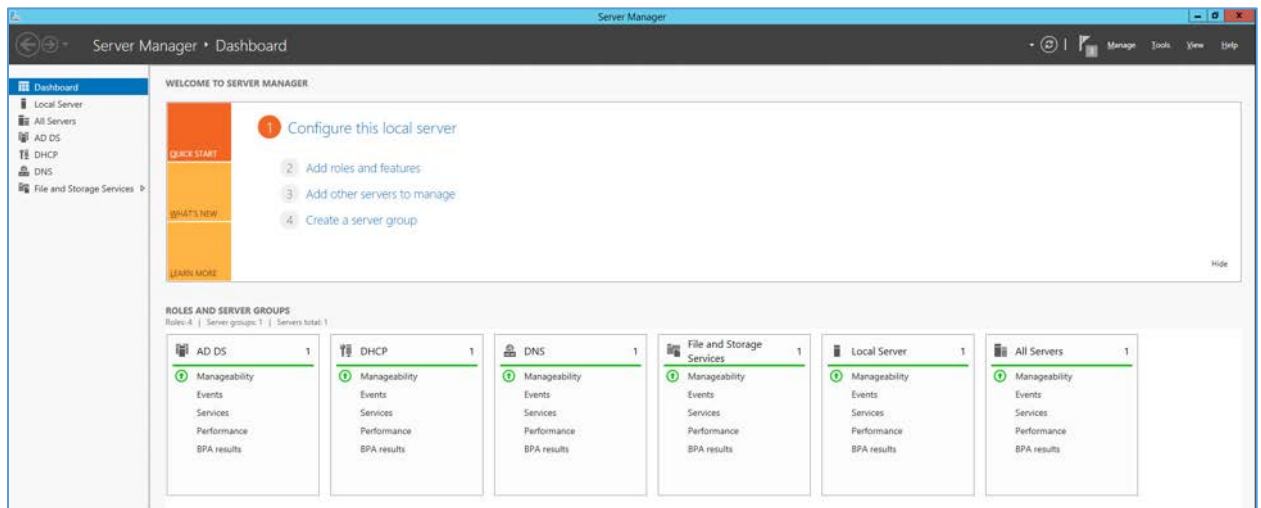
- **CPU:** 1
- **Memory:** 4 GB RAM
- **Storage:** 120 GB (thin provision)
- **Operating System:** Microsoft Windows Server 2012 R2
- **Network Adapter:** VLAN 1201

Enterprise Domain Services Installation

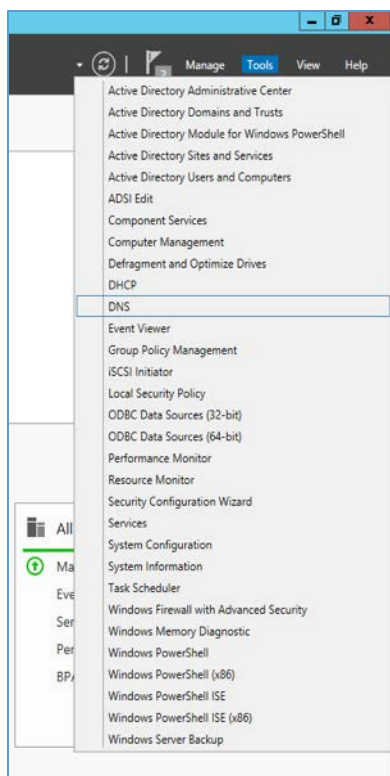
Install the DC, AD, and DNS appliances according to the instructions detailed in *Building Your First Domain Controller on 2012 R2* [5].

DNS Server Forward Lookup Zone Configuration

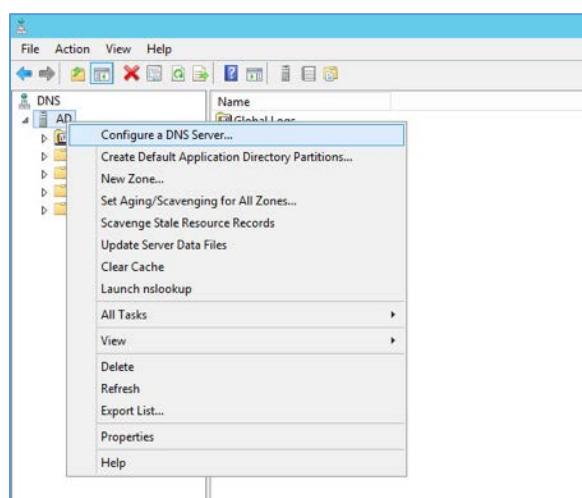
1. Open **Server Manager**.



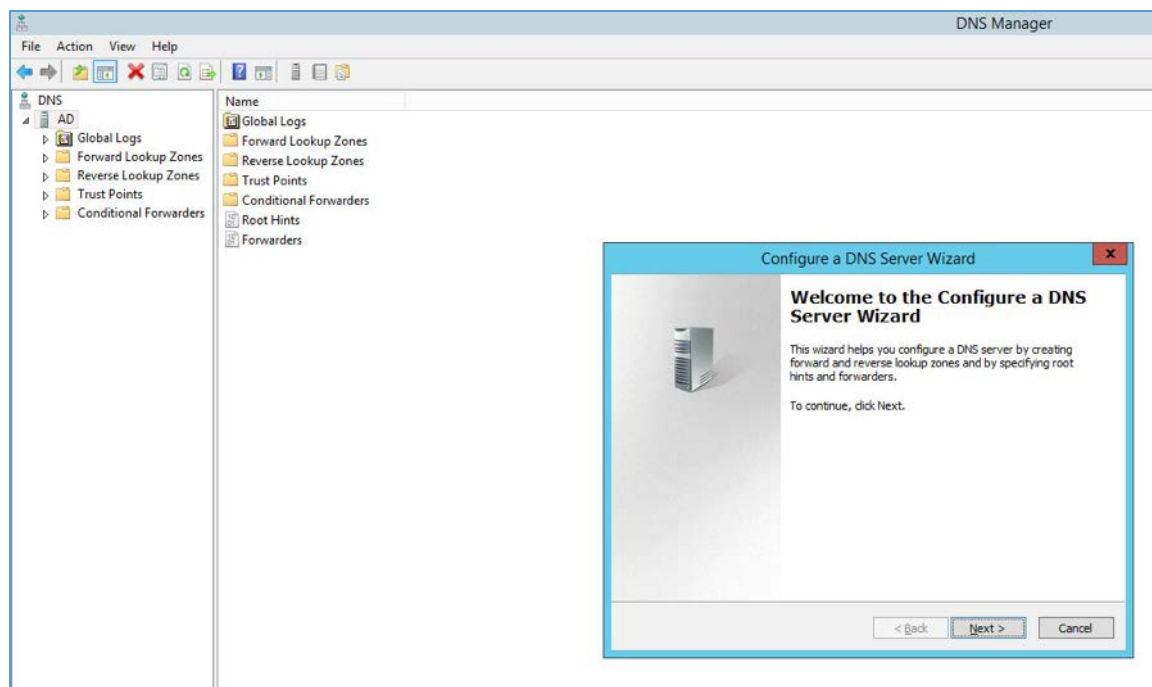
2. In the top right, click **Tools > DNS**.
3. The DNS forward lookup zone should have already been created during the DNS setup process performed previously. If not, follow these instructions:



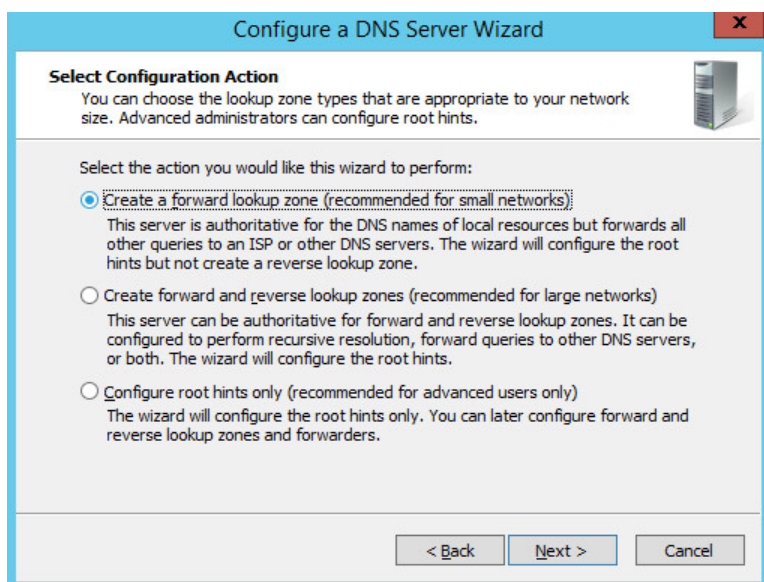
- a. Right-click your server's name, and select **Configure a DNS Server...**



- b. Click **Next >**.

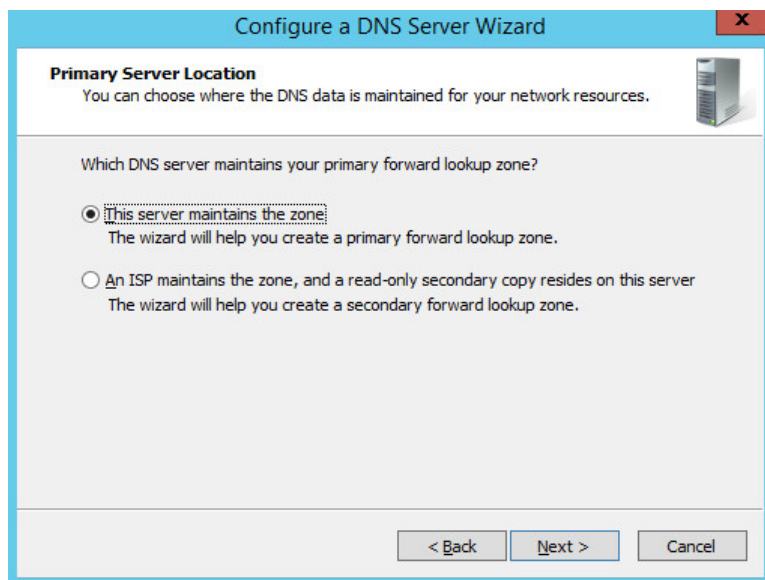


- c. Click **Next >**.
- d. Under **Select Configuration Action**, select **Create a forward loading zone...**

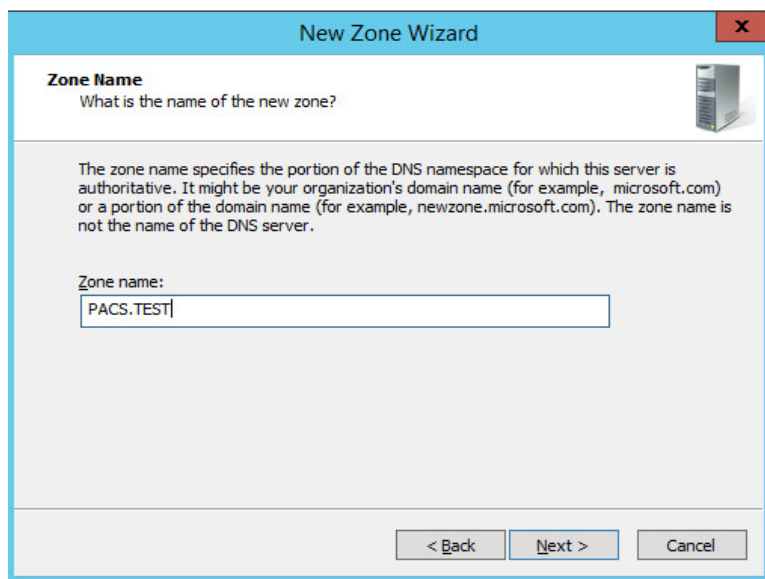


- e. Click **Next >**.

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

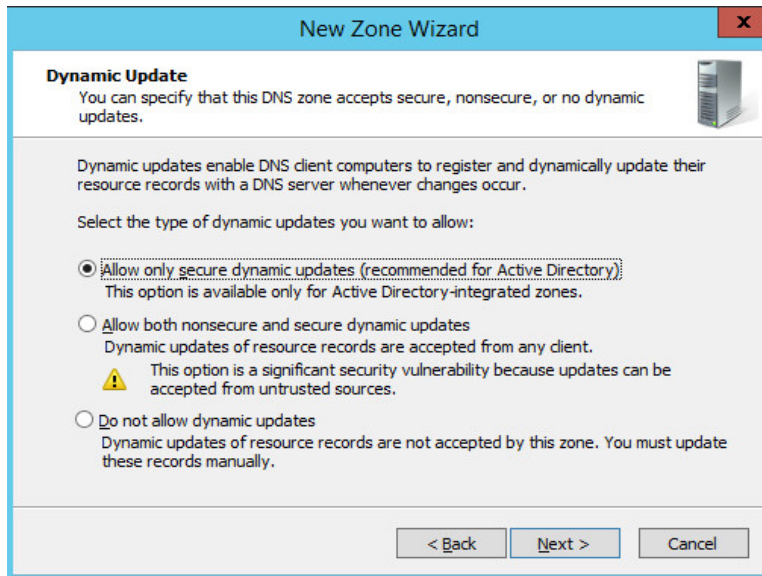


- h. Enter **PACS.TEST** as the **Zone name** that was established previously during setup.
- i. Click **Next >**.



- j. Select **Allow only secure dynamic updates**.

- k. Click **Next >**.




New Zone Wizard

Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

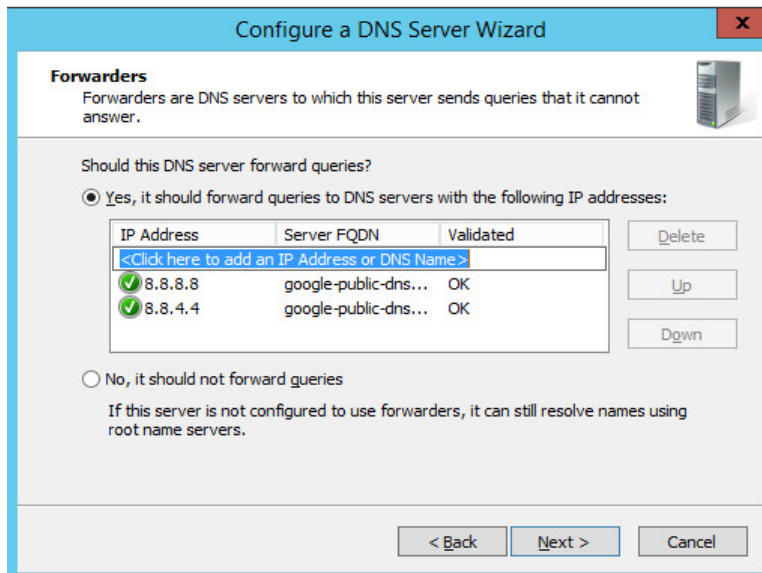
Select the type of dynamic updates you want to allow:

- ☒ **Allow only secure dynamic updates (recommended for Active Directory)**
This option is available only for Active Directory-integrated zones.
- ☐ **Allow both nonsecure and secure dynamic updates**
Dynamic updates of resource records are accepted from any client.
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- ☐ **Do not allow dynamic updates**
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

- l. Add **Forwarders** (8.8.8.8 and 8.8.4.4 are Google's DNS servers).

- m. Click **Next >**.



Configure a DNS Server Wizard

Forwarders
Forwarders are DNS servers to which this server sends queries that it cannot answer.

Should this DNS server forward queries?

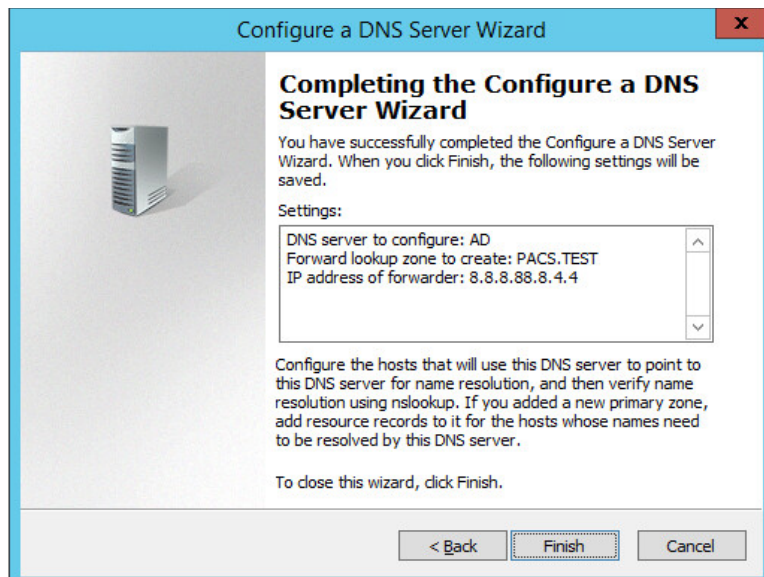
- ☒ **Yes, it should forward queries to DNS servers with the following IP addresses:**

IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
8.8.8.8	google-public-dns...	OK
8.8.4.4	google-public-dns...	OK

Buttons: Delete, Up, Down
- ☐ **No, it should not forward queries**
If this server is not configured to use forwarders, it can still resolve names using root name servers.

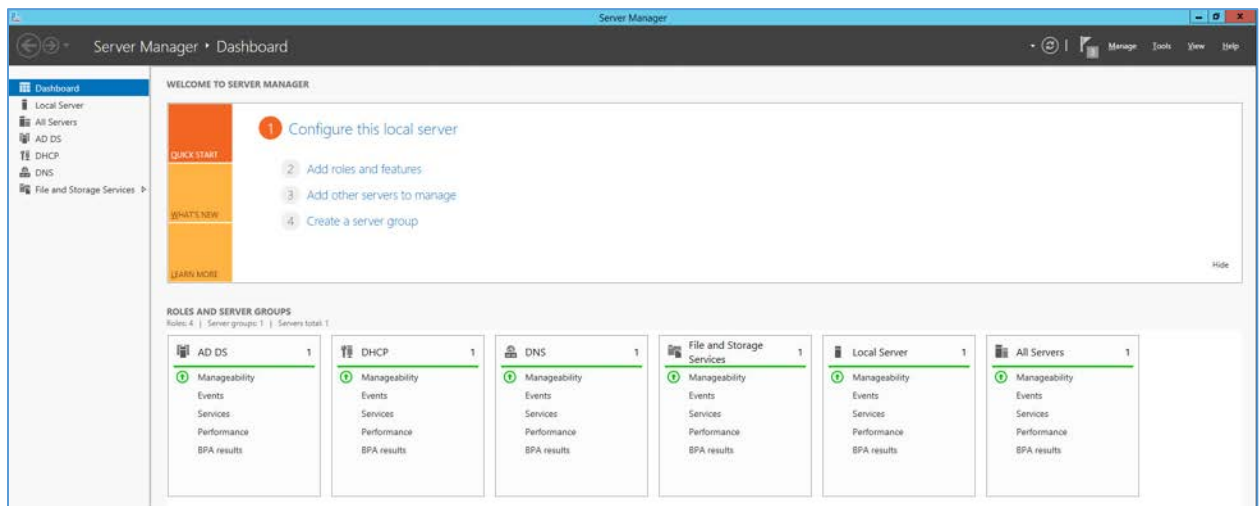
< Back Next > Cancel

- n. Click **Finish**.

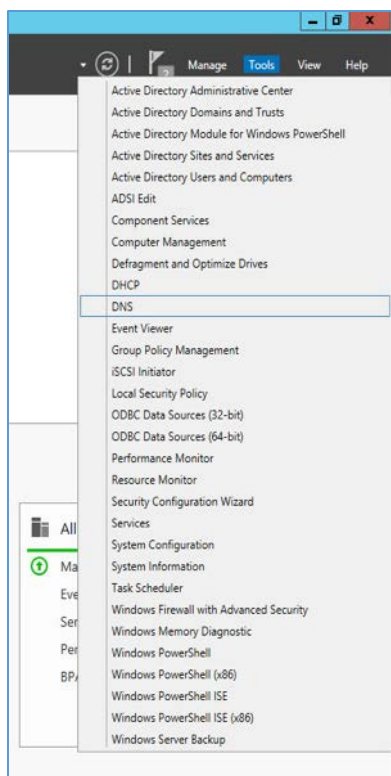


DNS Server Reverse Lookup Zone Configuration

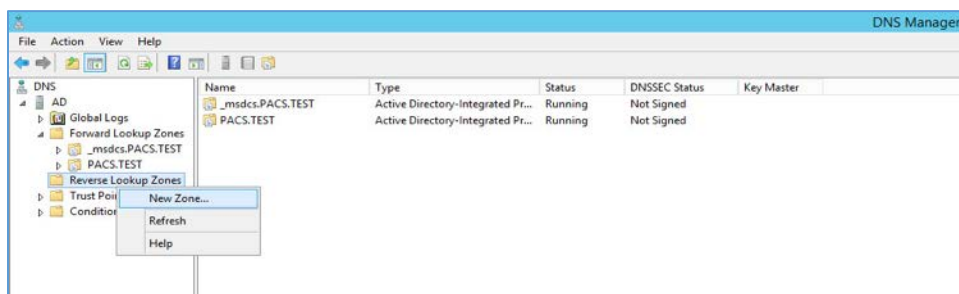
1. Open **Server Manager**.



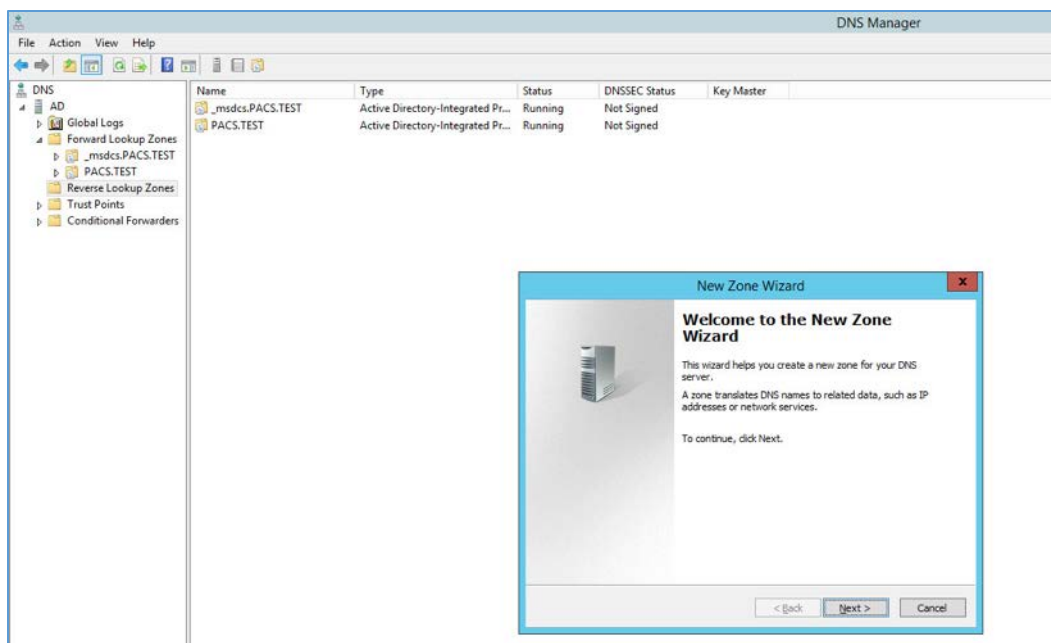
2. In the top right, click **Tools > DNS**.



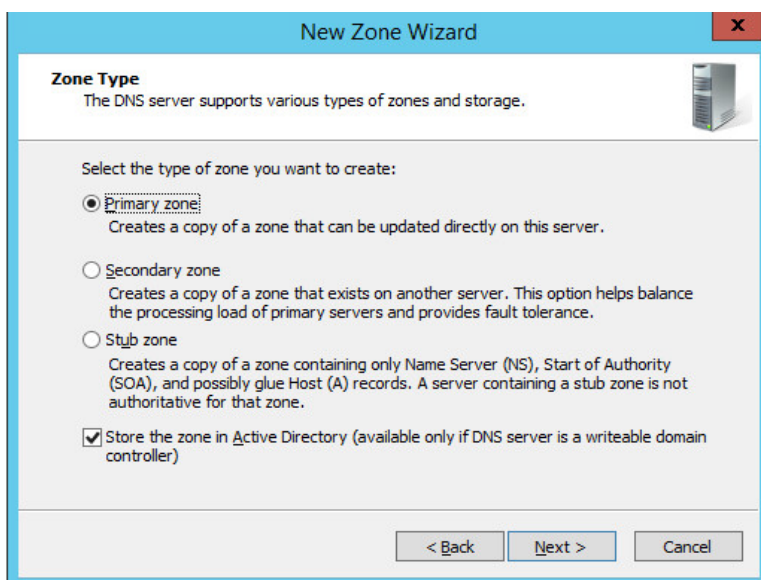
3. Right-click **Reverse Lookup Zones** folder, and select **New Zone...**



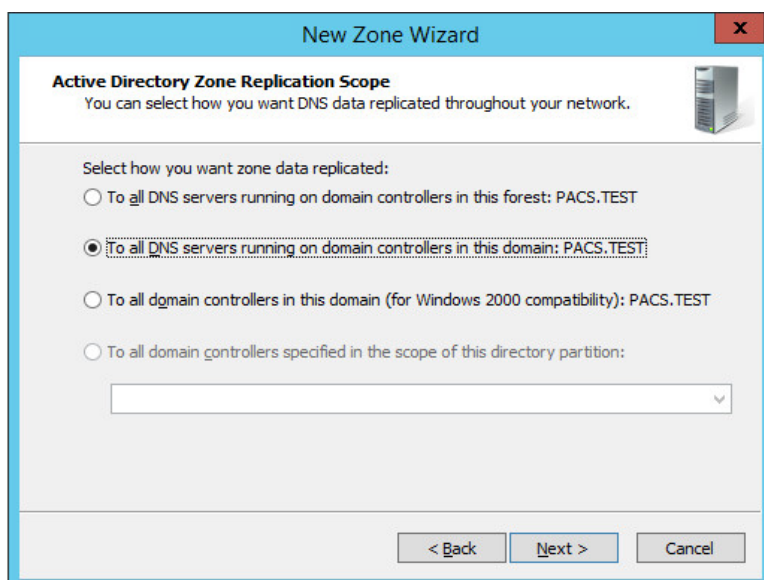
4. Click **Next >**.



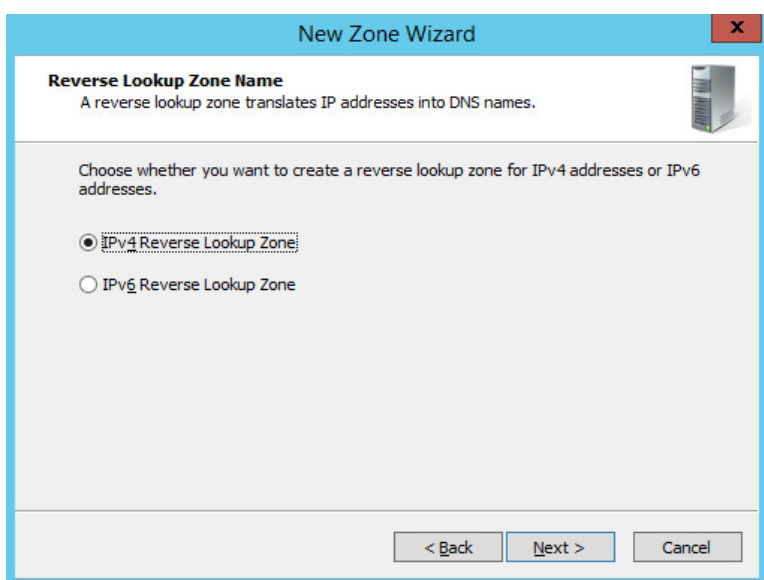
5. Click **Next >**.
6. Under **Zone Type**, select **Primary zone**.
7. Select the **Store the zone in Active Directory...** checkbox.
8. Click **Next >**.



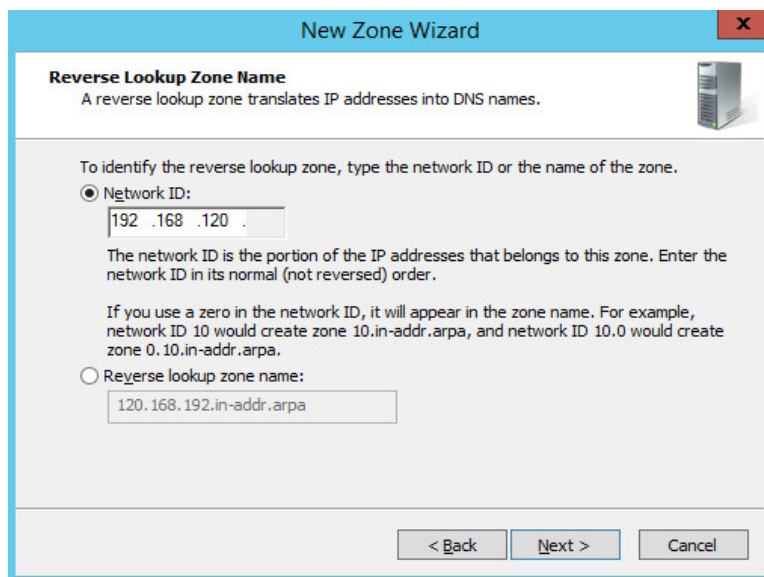
9. Click **Next >**.
10. Under **Active Directory Zone Replication Scope**, Select **To all DNS servers running...**
11. Click **Next>**.



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



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



New Zone Wizard

Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

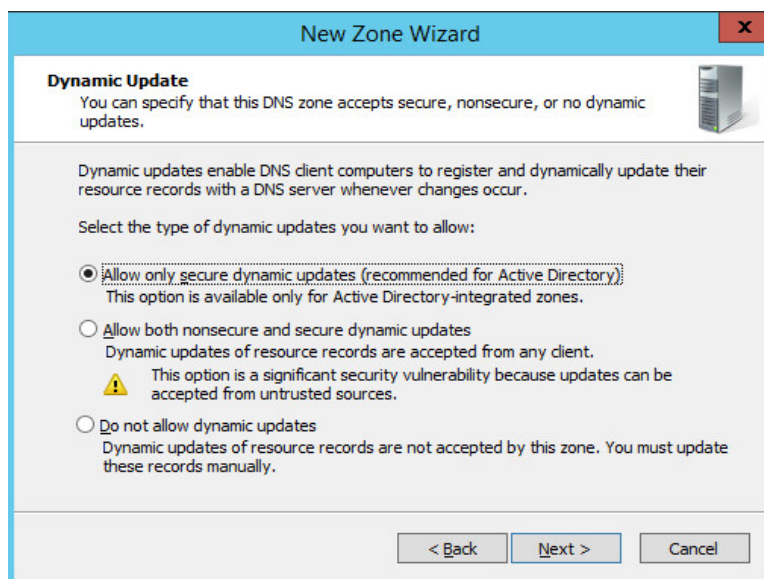
☒ **Network ID:**

 The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.
 If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ **Reverse lookup zone name:**

< Back Next > Cancel

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



New Zone Wizard

Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

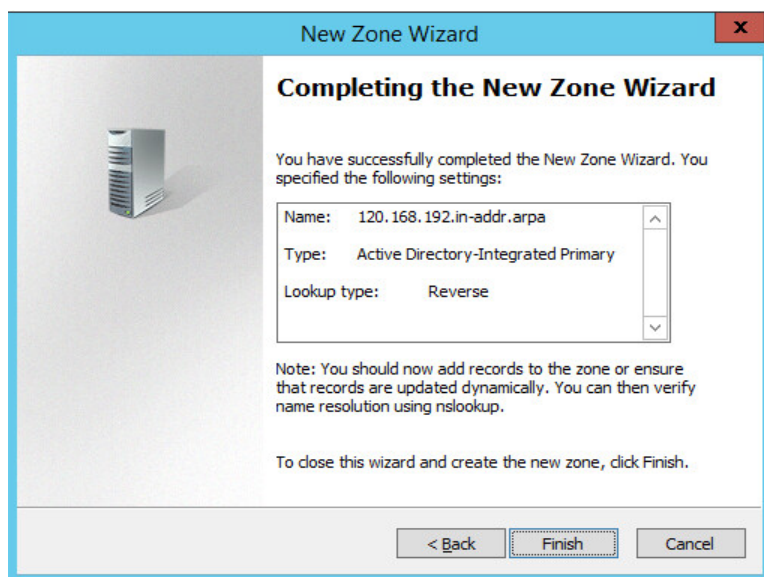
☒ **Allow only secure dynamic updates (recommended for Active Directory)**
 This option is available only for Active Directory-integrated zones.

☐ **Allow both nonsecure and secure dynamic updates**
 Dynamic updates of resource records are accepted from any client.
 ⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

☐ **Do not allow dynamic updates**
 Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back Next > Cancel

15. Click **Finish**.

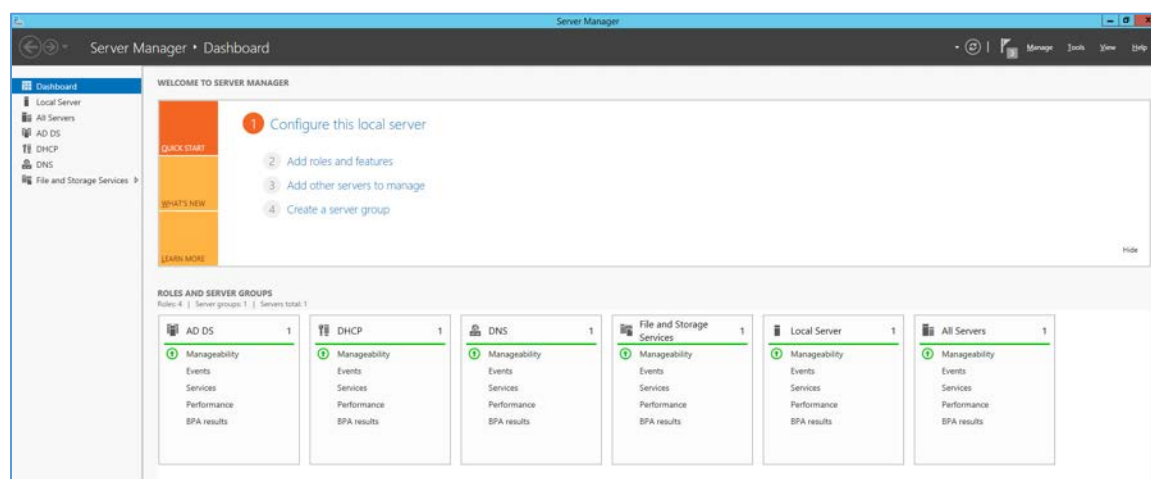


DHCP Server Installation

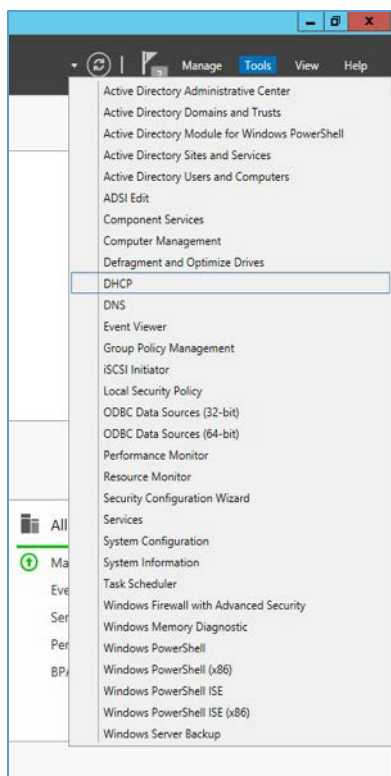
Install the DHCP server according to the instructions detailed in *Installing and Configuring DHCP Role on Windows Server 2012* [6].

DHCP Server Configuration

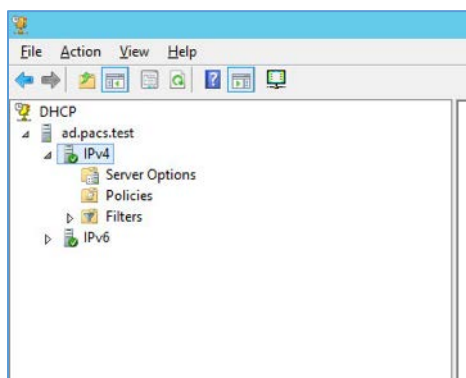
1. Open **Server Manager**.



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



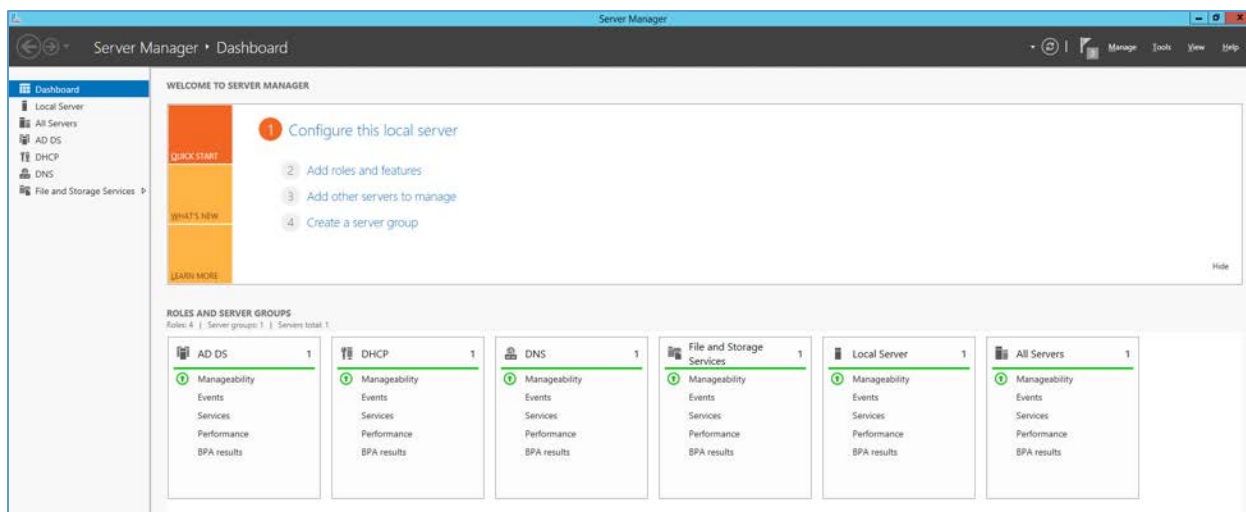
3. If you see a green check mark on the **IPv4** server, the DHCP server is up and running.



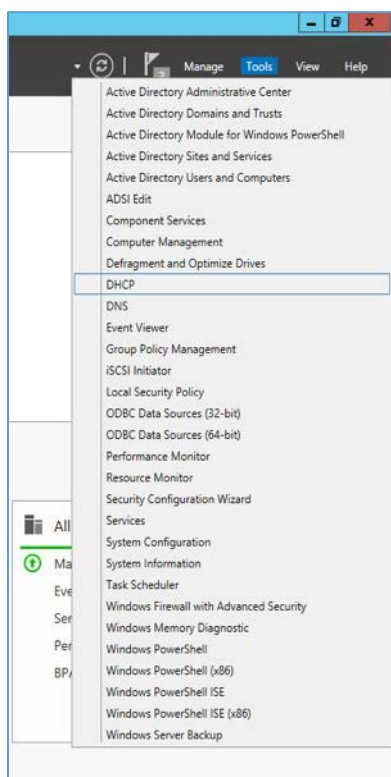
DHCP Scopes Configuration

Performed on Windows Server 2012 R2

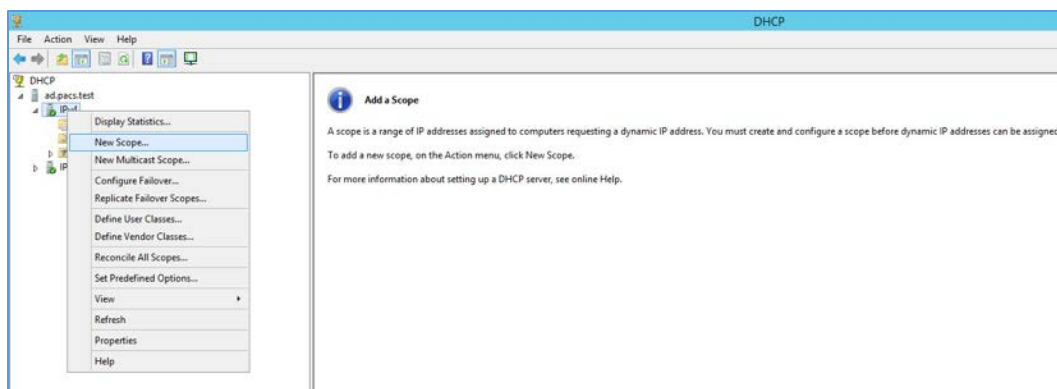
1. Open **Server Manager**.



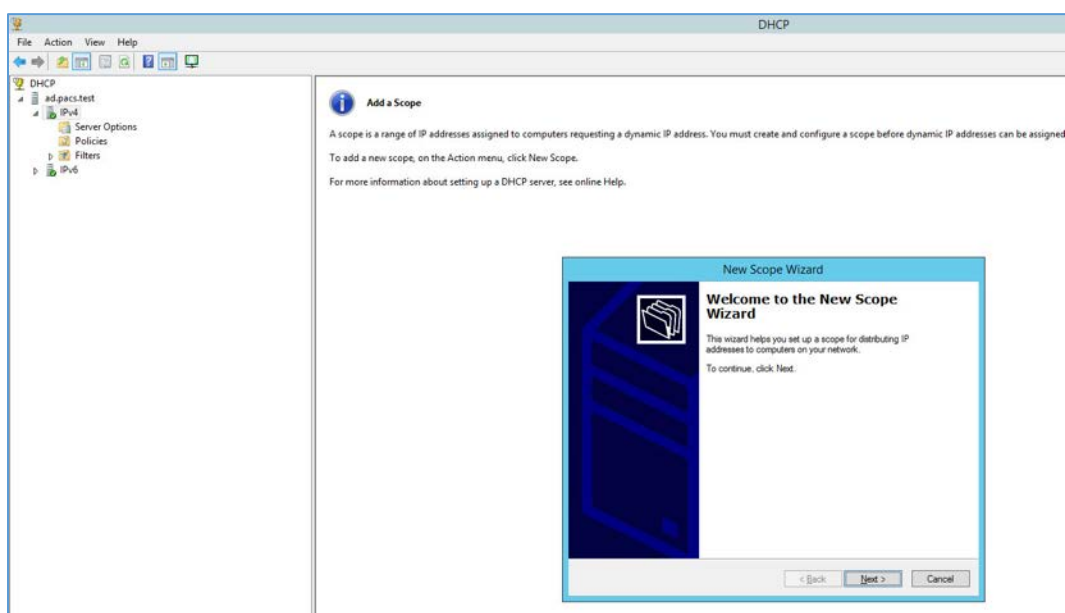
2. In the top right, click **Tools > DHCP**.



3. Right-click **IPv4**, and select **New Scope...**

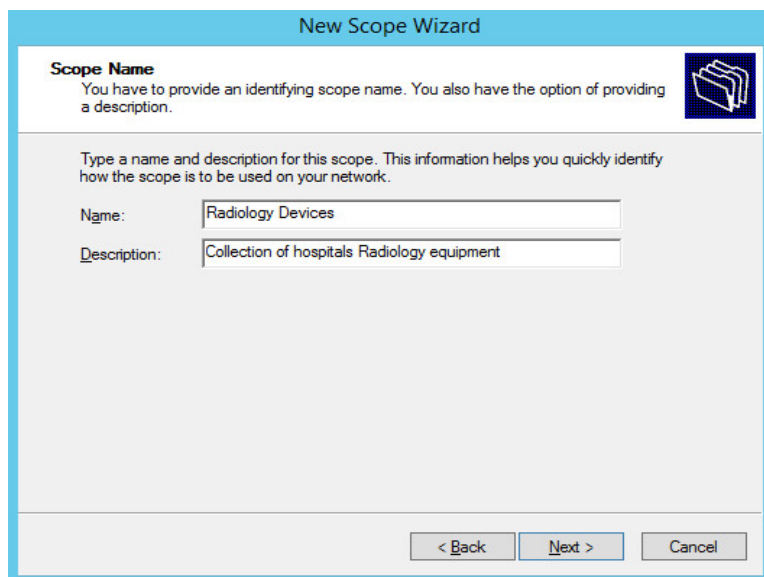


4. Click **Next >**.



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

6. Click **Next >**.



New Scope Wizard

Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

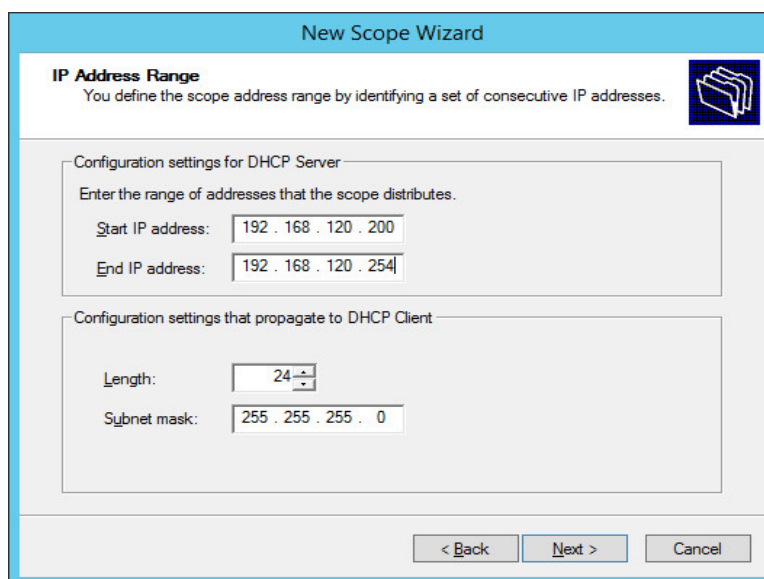
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back Next > Cancel

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



New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

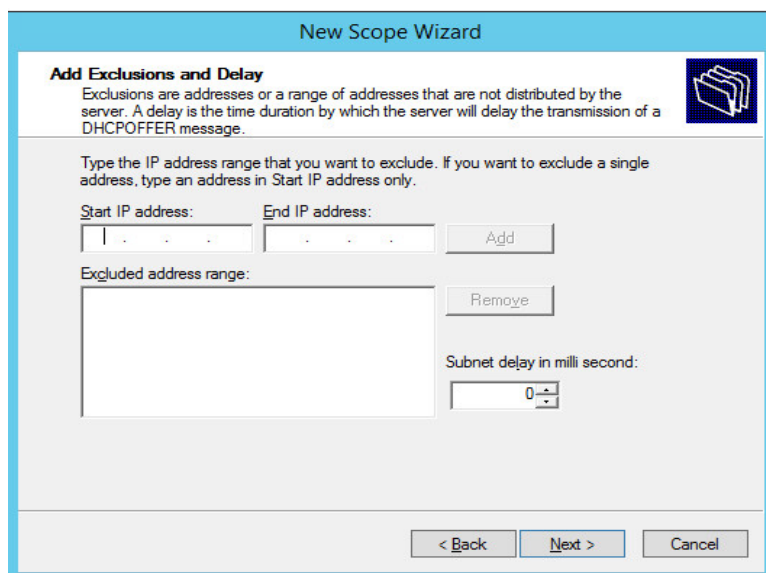
Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back Next > Cancel

9. Click **Next >**.



New Scope Wizard

Add Exclusions and Delay
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

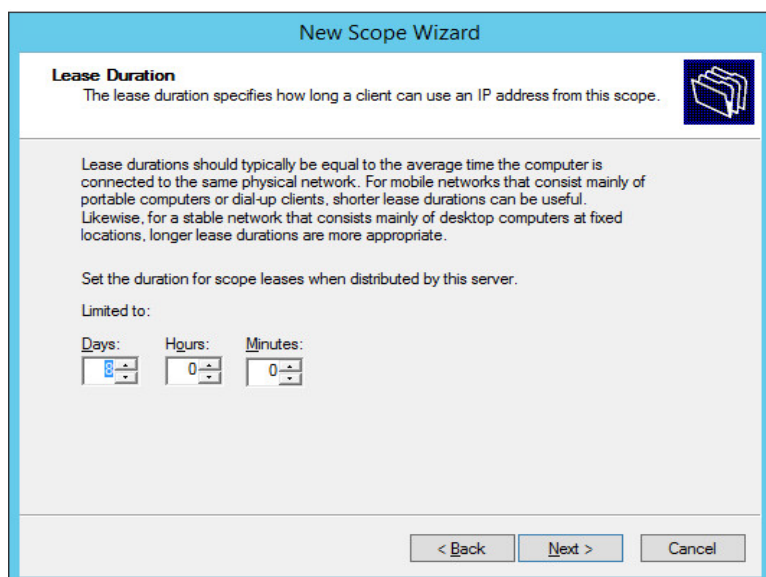
Start IP address: End IP address:

Excluded address range:

Subnet delay in milli second:

< Back Next > Cancel

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



New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

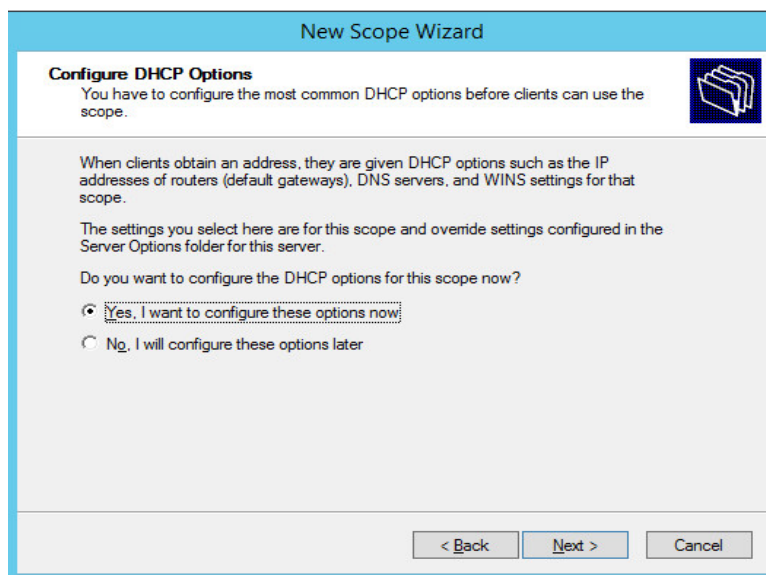
Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back Next > Cancel

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



New Scope Wizard

Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

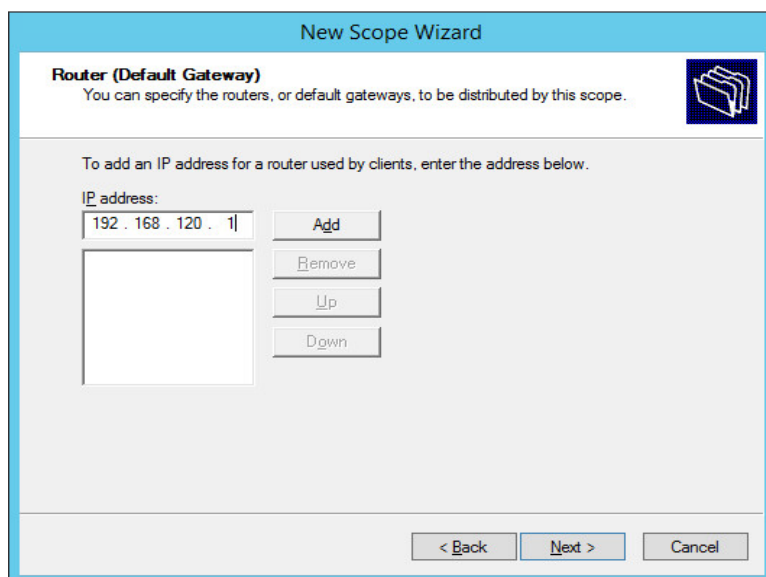
☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back Next > Cancel

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

13. Click **Add**.



New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:
192 . 168 . 120 . 1

Add

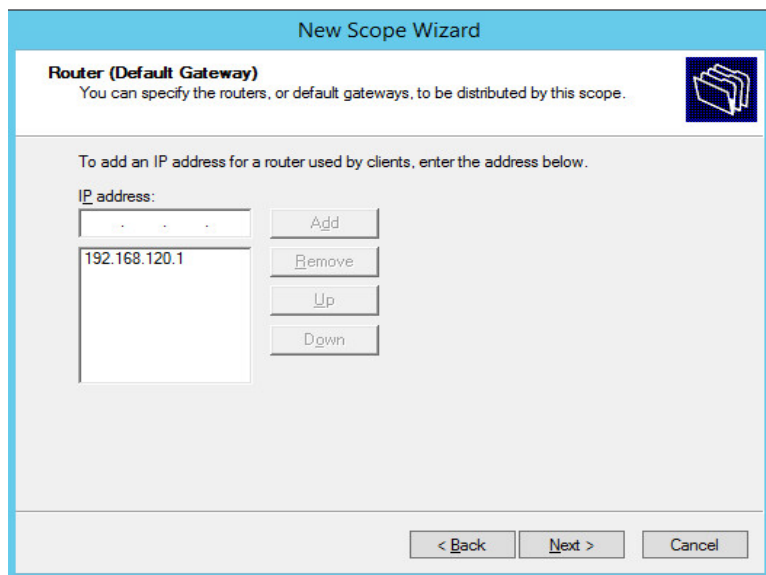
Remove

Up

Down

< Back Next > Cancel

14. Click **Next >**.



New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

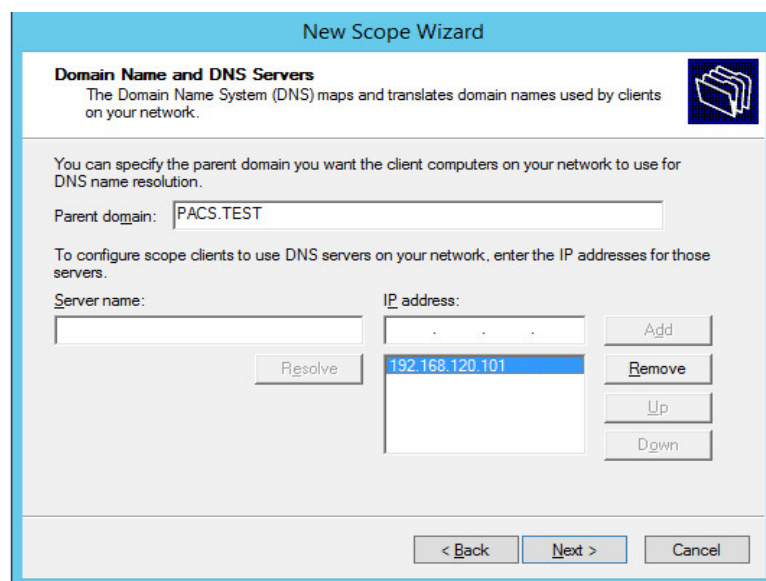
IP address:

	Add
192.168.120.1	Remove
	Up
	Down

< Back Next > Cancel

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

16. Click **Next >**.



New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

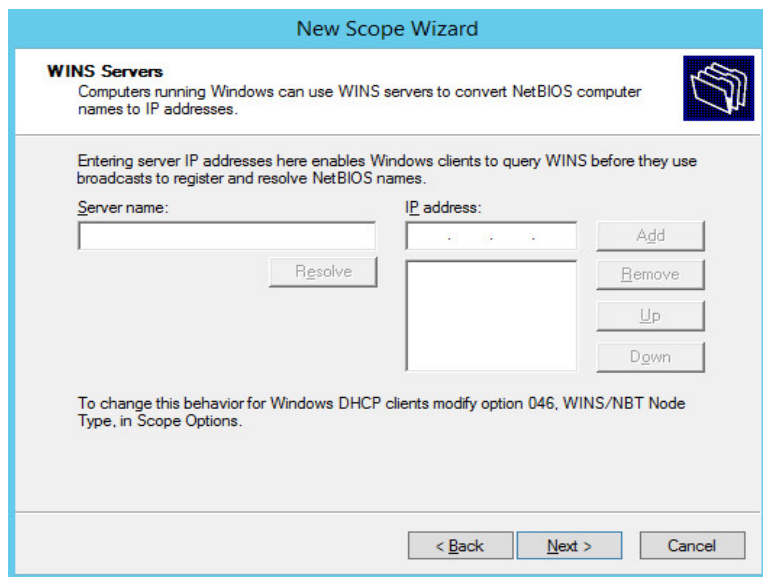
Parent domain: PACS.TEST

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:	IP address:	Add
	192.168.120.101	Remove
Resolve		Up
		Down

< Back Next > Cancel

17. Click **Next >**.



New Scope Wizard

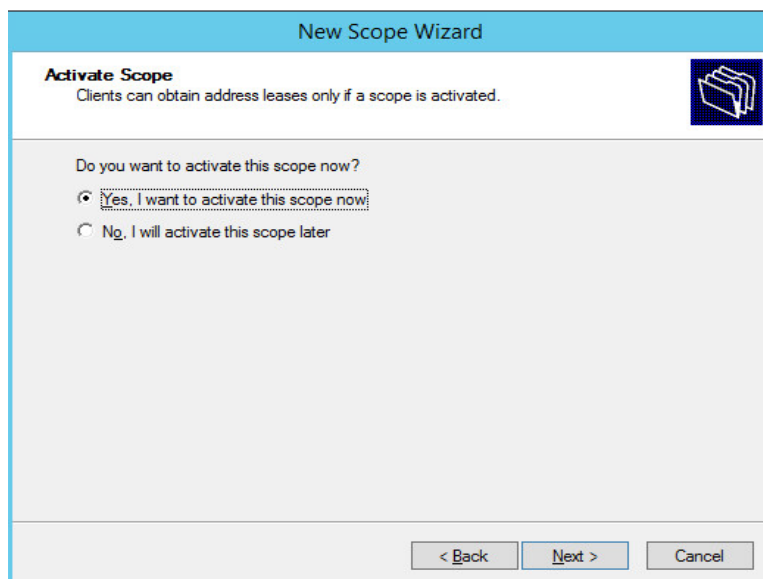
WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name: IP address:

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

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



New Scope Wizard

Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

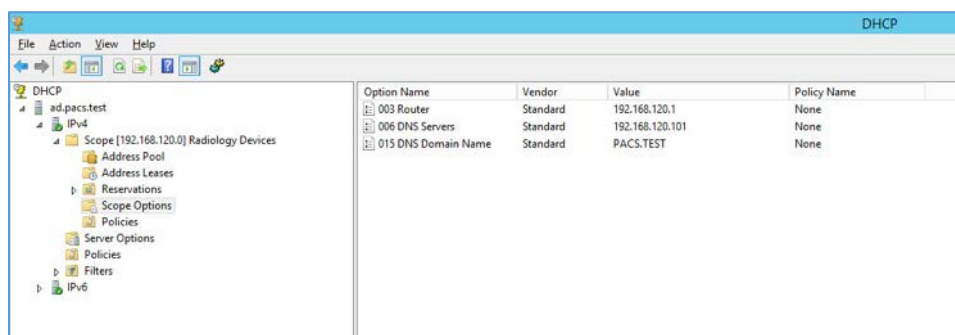
☒ **Yes, I want to activate this scope now**
☐ No, I will activate this scope later

19. Click **Finish**.



20. Scope should appear under the **IPv4** drop-down. Ensure **Scope Options** are correctly established with these values:

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



2.6.2 DigiCert PKI

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

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

Create CSR

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

Download and save the *DigiCertUtil.exe* from the DigiCert site [7].

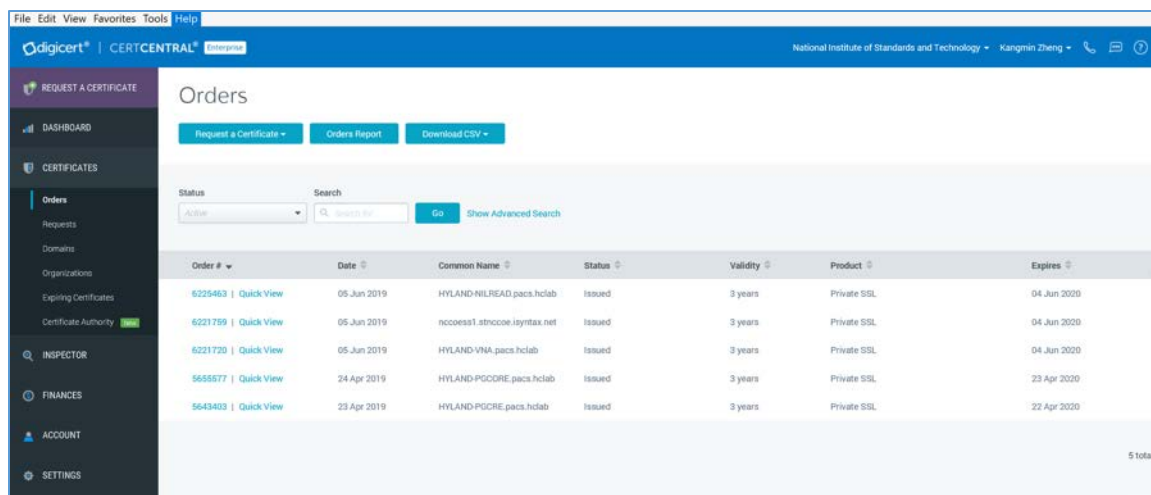
1. Double-click ***DigiCertUtil.exe*** to run the utility.
2. Click the **Create CSR** link to open a CSR request window.
3. On the Create CSR window, fill in the key information (some of the information is optional).
 - **Certificate Type:** Select SSL
 - **Common Name:** HYLAND-VNA.pacs.hclab
 - **Subject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

- The screenshot shows the 'Digicert Certificate Utility for Windows' window. At the top, a green checkmark icon and the text 'The certificate request has been successfully created.' are displayed. Below this, a text area contains a long, base64-encoded string representing the CSR request. The string is enclosed in '-----BEGIN NEW CERTIFICATE REQUEST-----' and '-----END NEW CERTIFICATE REQUEST-----' markers. At the bottom of the window, there are three buttons: 'Copy CSR', 'Save to File', and 'Close'.

- 117

7. **Issue Signed Certificates.** With a created applicant CSR, request a signed certificate using DigiCert **CertCentral** portal by following 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**, and 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.

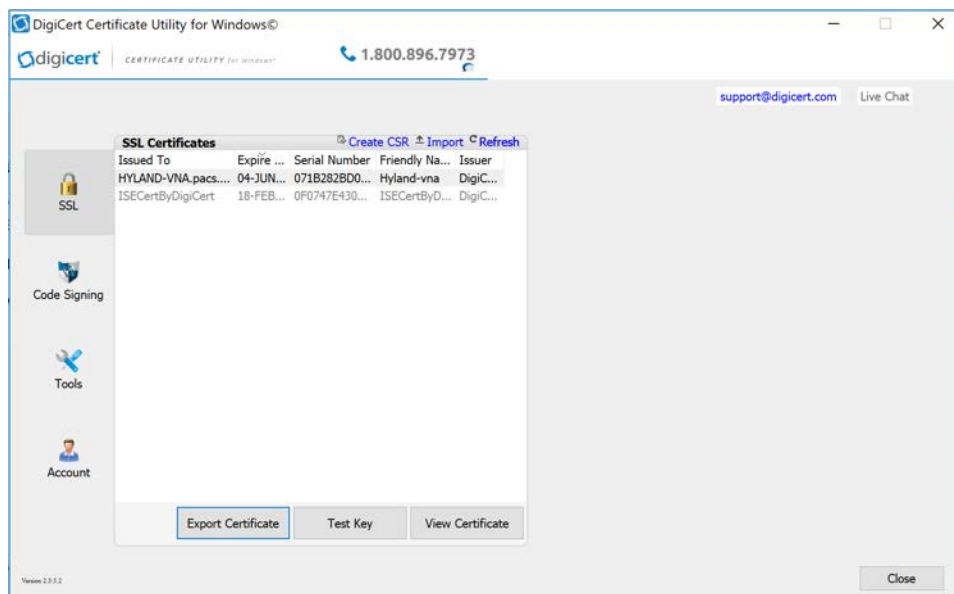


9. Click a specific order number to display the certificate details with a list of actions that can be performed. Click **Download Certificate As** to download certificates with signed CA and Root CA certificates. A variety of certificate formats can be downloaded, such as .crt, .p7b, .pem.
10. Save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



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



2.7 Network Control and Security

Network control and security was implemented throughout the network infrastructure. The build features perimeter security that includes firewall feature sets and network traffic monitoring. The internal lab environment implements VLANs to establish network zones. Modality devices are further isolated by using micro-segmentation. The build also includes behavioral analysis tools that alert upon anomalous activity.

2.7.1 Cisco Firepower

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

Cisco Firepower Management Center Appliance Information

- **CPUs:** 8
- **RAM:** 16 GB
- **Storage:** 250 GB (thin provision)
- **Network Adapter 1:** VLAN 1201
- **Operating System:** Cisco Fire Linux

Cisco Firepower Management Center Virtual Installation Guide

Install the Cisco Firepower Management Center Virtual appliance according to the instructions detailed in *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide* [8].

Cisco Firepower Threat Defense Appliance Information

- **CPUs:** 8
- **RAM:** 16 GB
- **Storage:** 48.5 GB (thin provision)
- **Network Adapter 1:** VLAN 1201
- **Network Adapter 2:** VLAN 1201
- **Network Adapter 3:** VLAN 1099
- **Network Adapter 4:** VLAN 1099
- **Network Adapter 5:** Trunk Port
- **Network Adapter 6:** Trunk Port

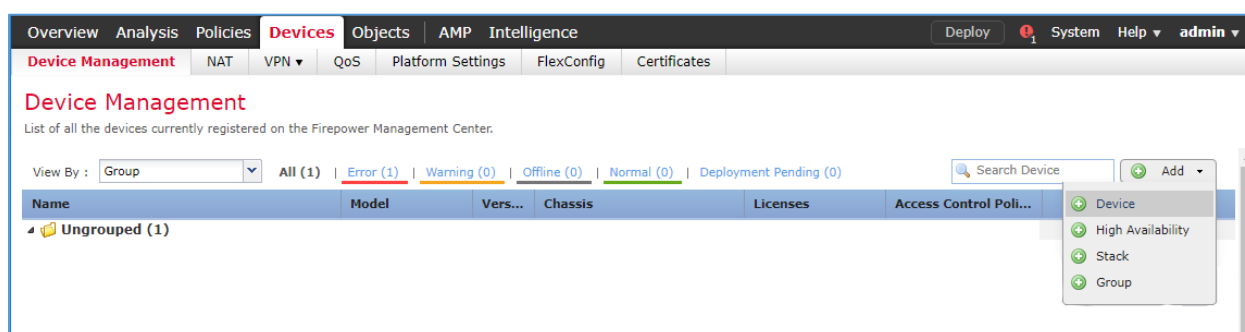
- **Network Adapter 7:** VLAN 1101
- **Network Adapter 8:** VLAN 1101
- **Network Adapter 9:** VLAN 1701
- **Operating System:** Cisco Fire Linux

Cisco Firepower Threat Defense Virtual Installation Guide

Install the Cisco Firepower Threat Defense Virtual appliance, according to the instructions detailed at *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide* [9].

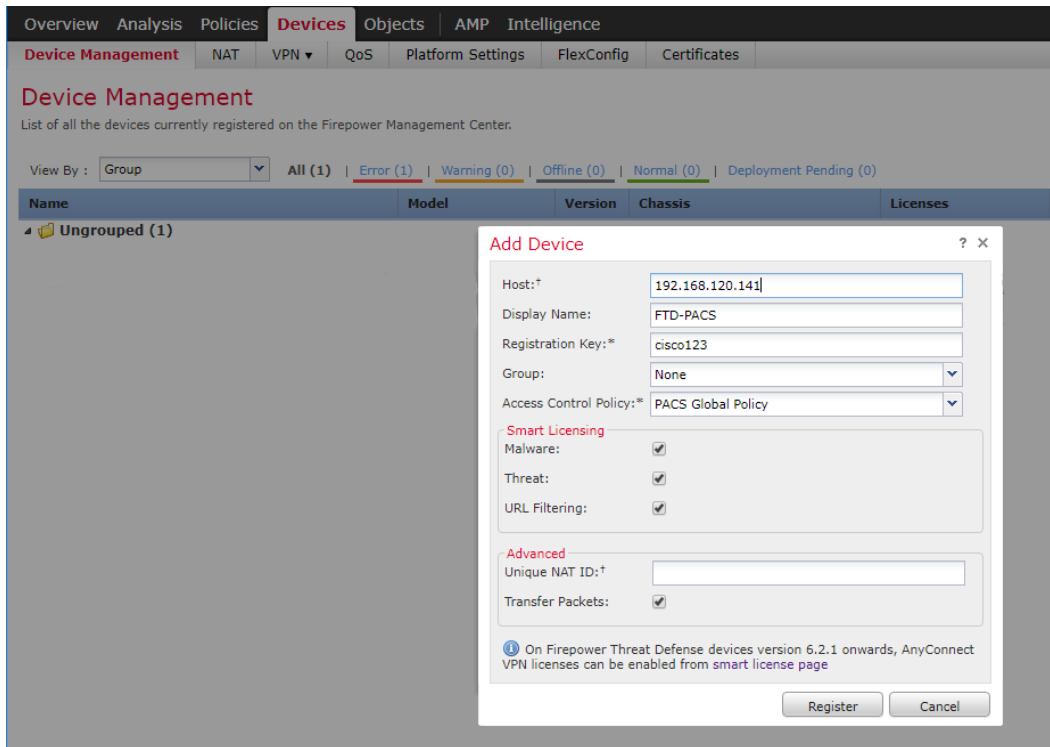
Adding Firepower Threat Defense (FTD) Appliance to Firepower Management Center (FMC)

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

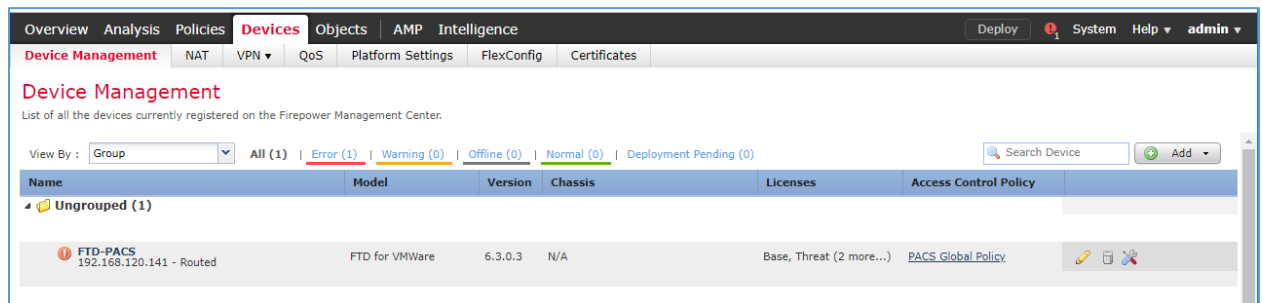


4. Enter **192.168.120.141** as the **IP address** of the FTD appliance.
5. Enter **FTD-PACS** as a **display name** to identify the FTD appliance.
6. Enter the **manager key** created when configuring the manager on the FTD appliance.
7. Click the **Access Control Policy** drop-down and select **Create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

10. Click **Register**.



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

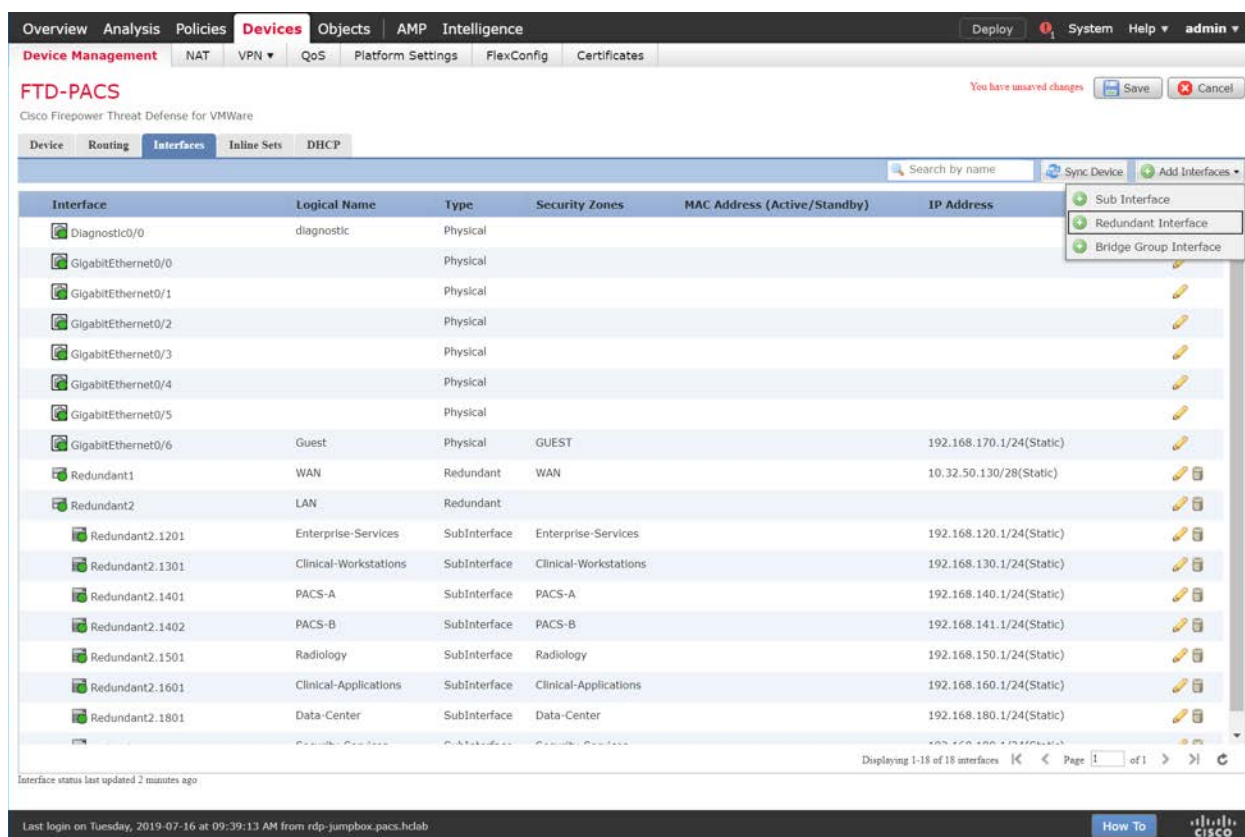


FTD Interfaces for PACS Architecture Configuration

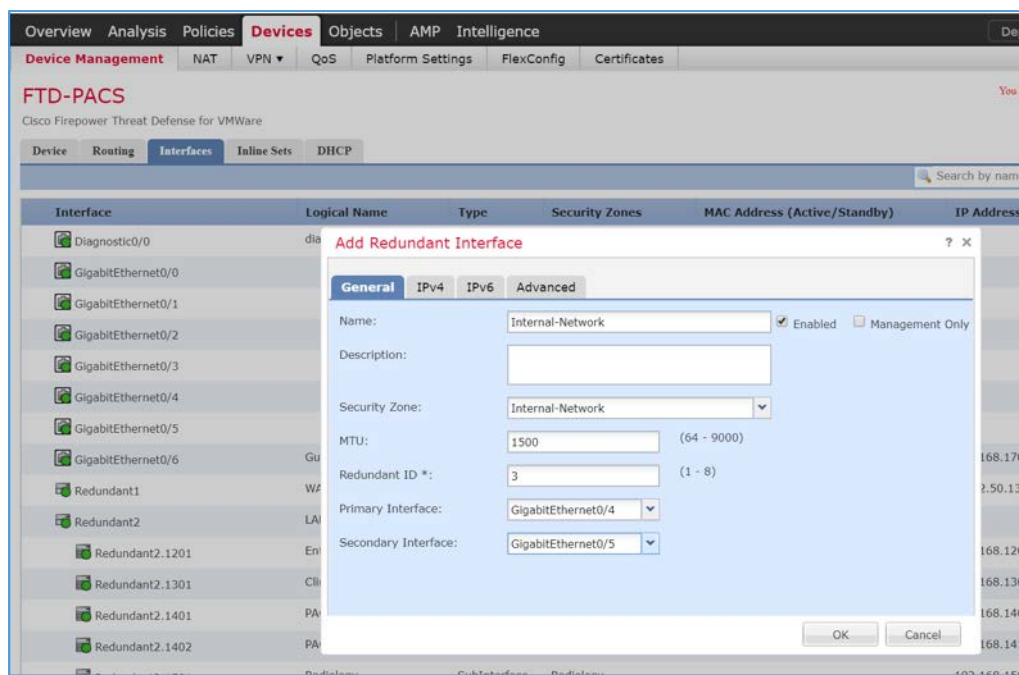
Each physical interface connected to the Cisco FTD will appear in the FMC device management section under the interface tab. To configure the eight subnets needed for the PACS architecture while also allowing management, diagnostic, and wide area network (WAN) traffic, we dedicated two interfaces set up as a redundant pair for all internal subnet traffic. To accomplish this, a sub-interface was created for each of the eight PACS subnets (e.g., Enterprise Services, Imaging Modalities, Security Services) and

established redundant interfaces for WAN traffic and traffic on VLAN 1101. The following guidance describes how the redundant interfaces and sub-interfaces were created.

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



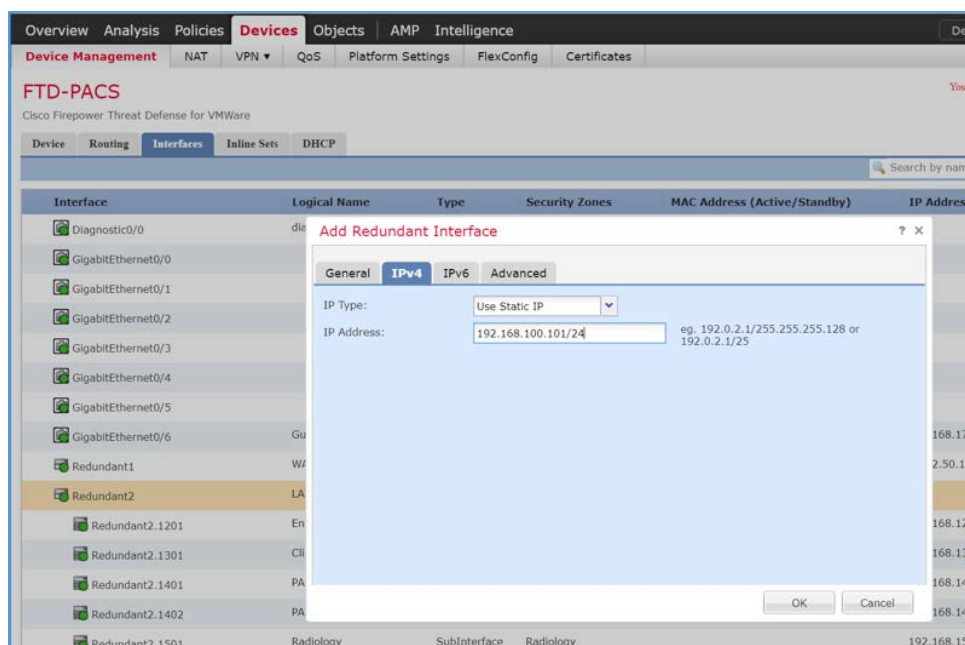
5. Enter **Internal-Network** as the **name** for the redundant interface.
6. Create and/or add a **security zone** to the redundant interface.
7. Assign a **Redundant ID** (e.g., **Internal-Network**) to the redundant interface.
8. Select a **primary interface** and **secondary interface** for the redundant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



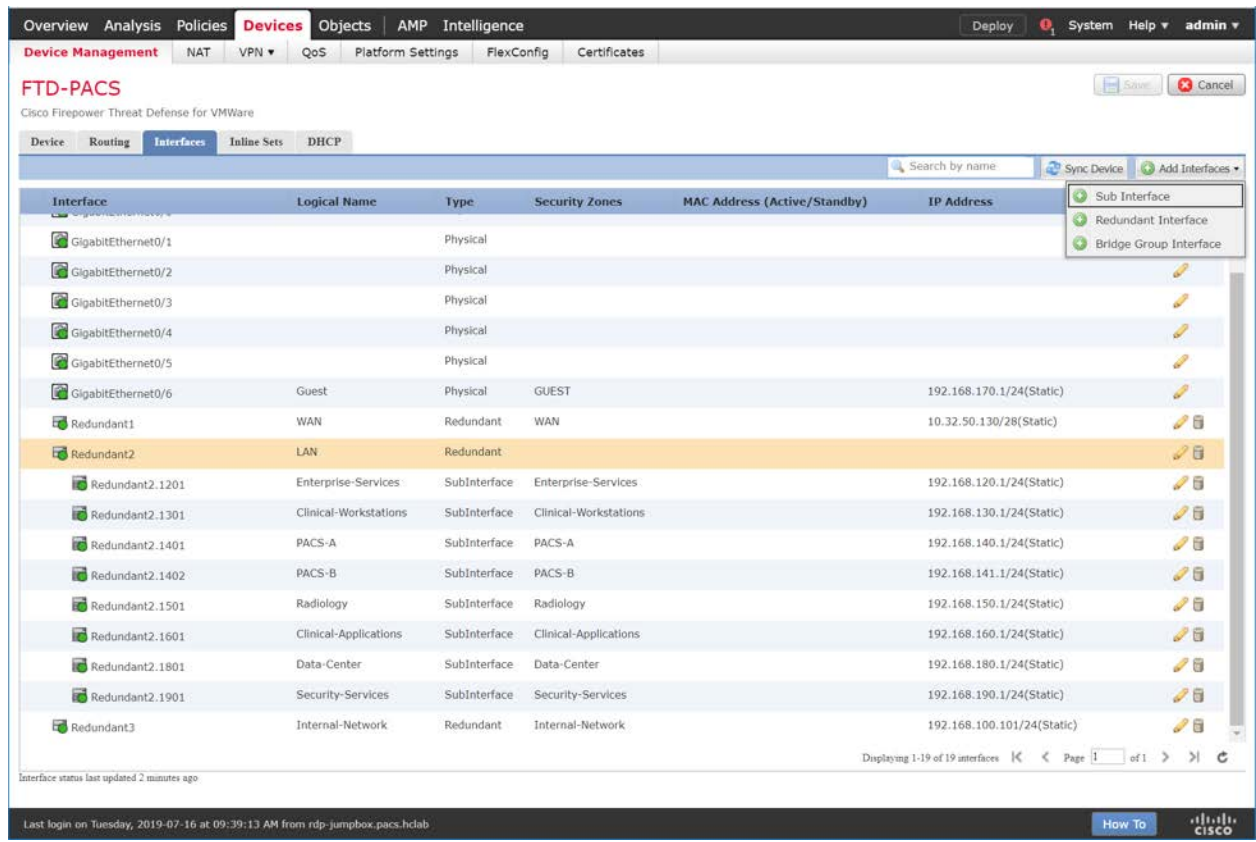
9. Navigate to the **IPv4** tab.

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

11. Click **OK**.



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



13. Enter **VNA** as the **name** for the subinterface.

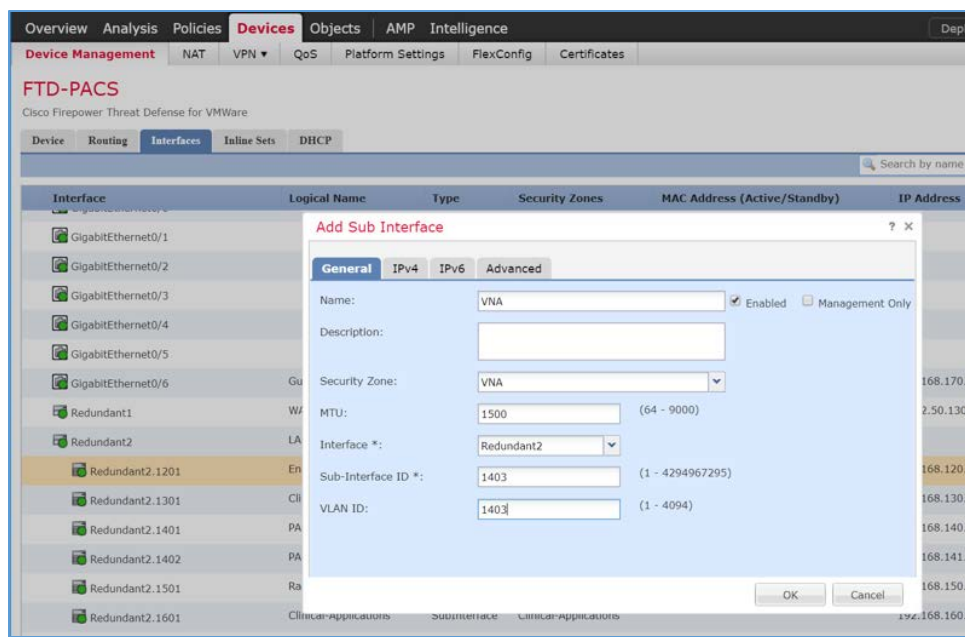
14. Create and/or add a **security zone, VNA**, to the subinterface.

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

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

16. Assign **1403** as the **Sub Interface ID** to the subinterface.

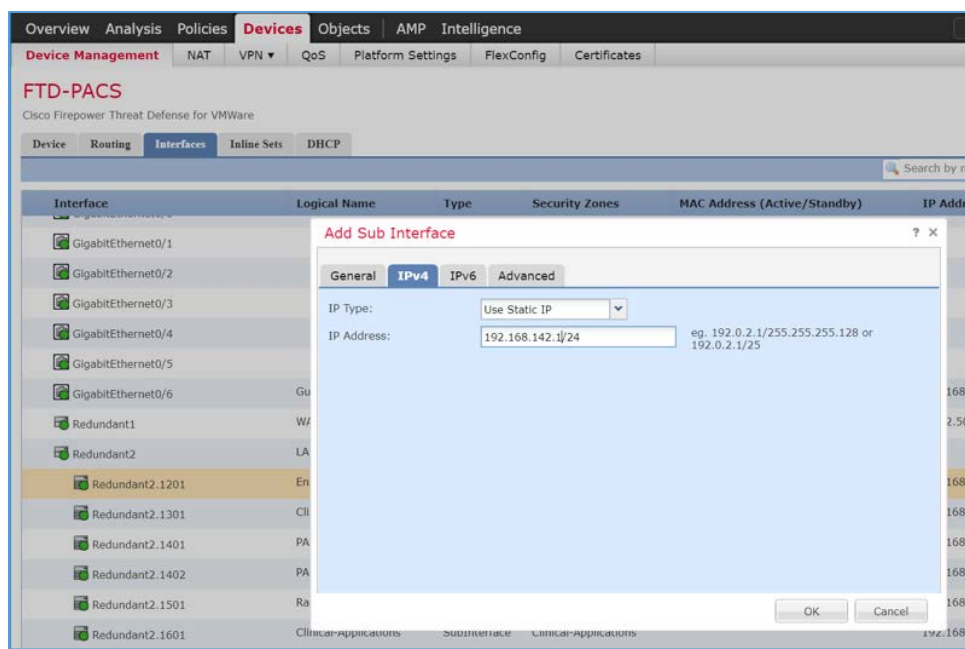
17. Assign **1403** as the **VLAN ID** to the subinterface.



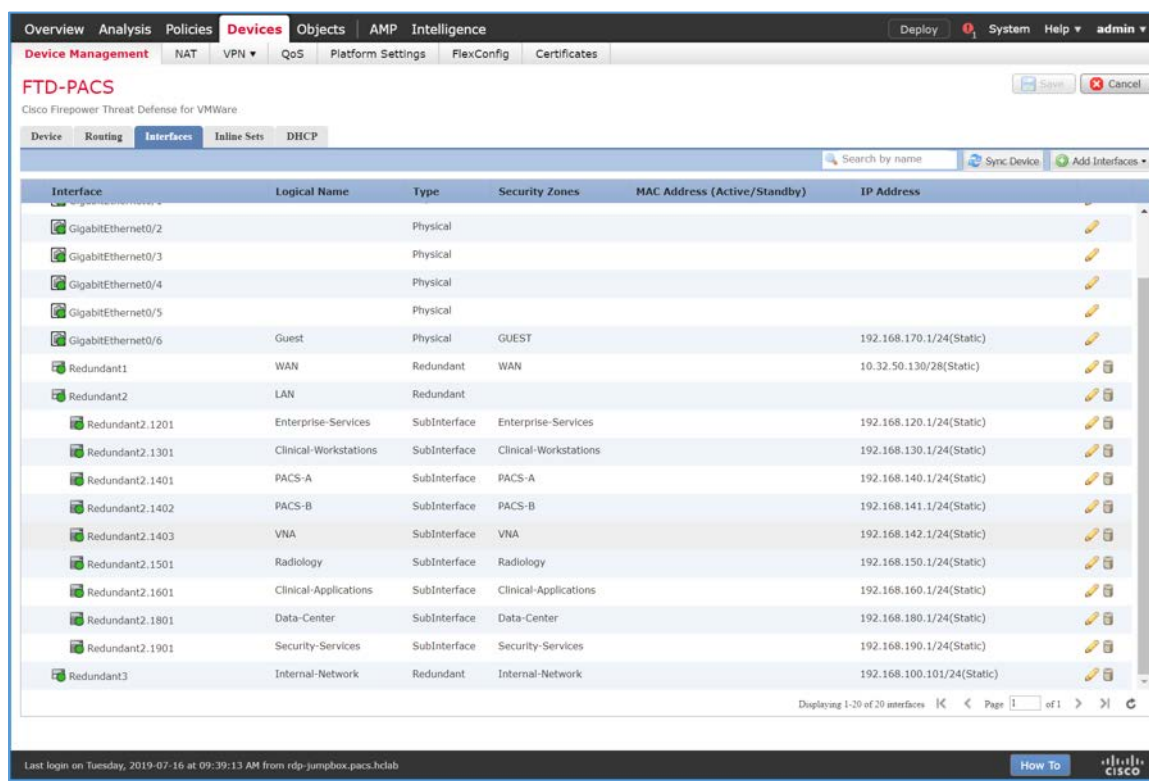
18. Navigate to the **IPv4** tab.

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

20. Click **OK**.

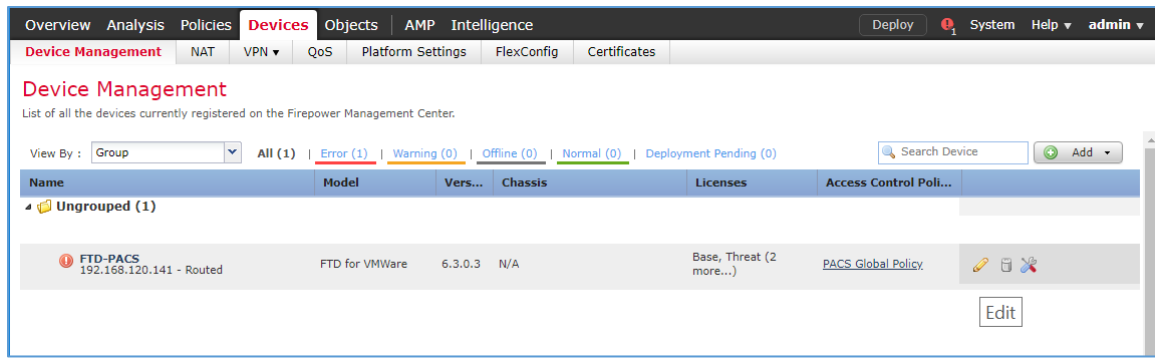


21. Click **Save**.
22. Click **Deploy** and wait for deployment to FTD to complete.
23. Refresh the page and confirm that the redundant interface and subinterface are running (shown with a green dot on the interface's icon).

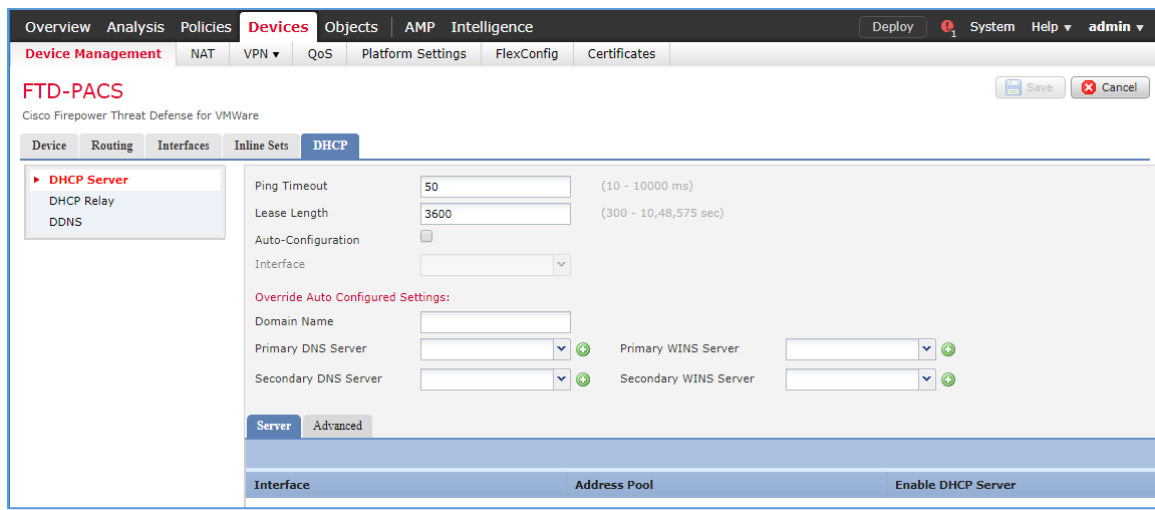


DHCP Relay Through Cisco Firepower Management Center Configuration

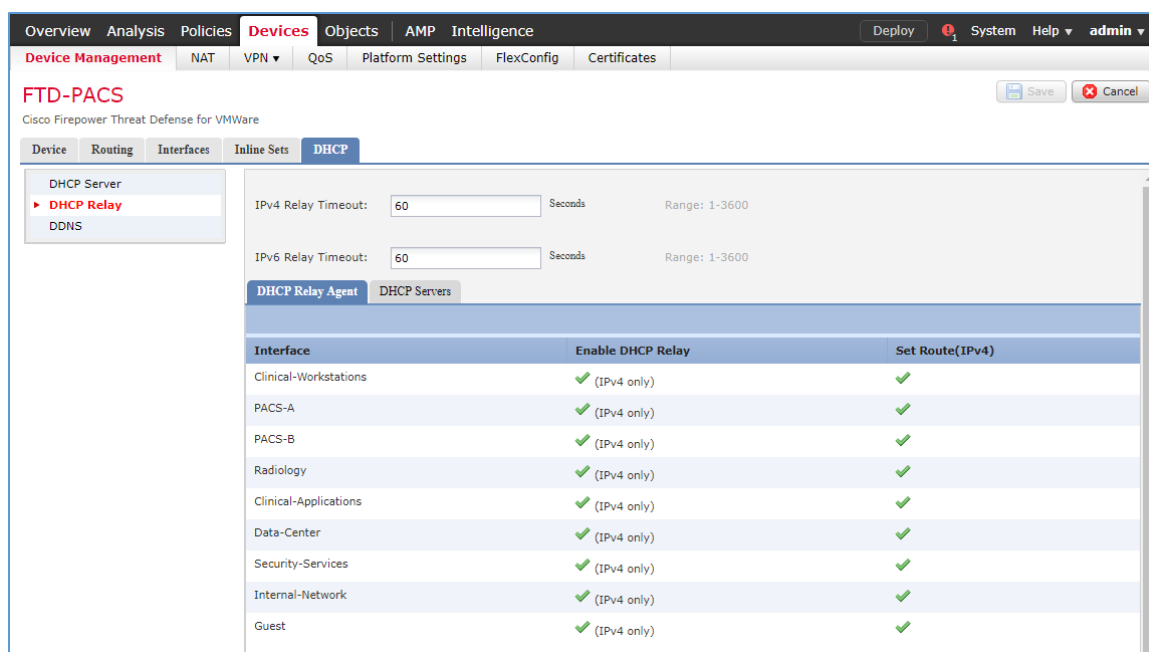
1. Log in to the **FMC Console**.
2. Navigate to **Devices > Device Management**.
3. Find your FTD device and click the **edit** icon.



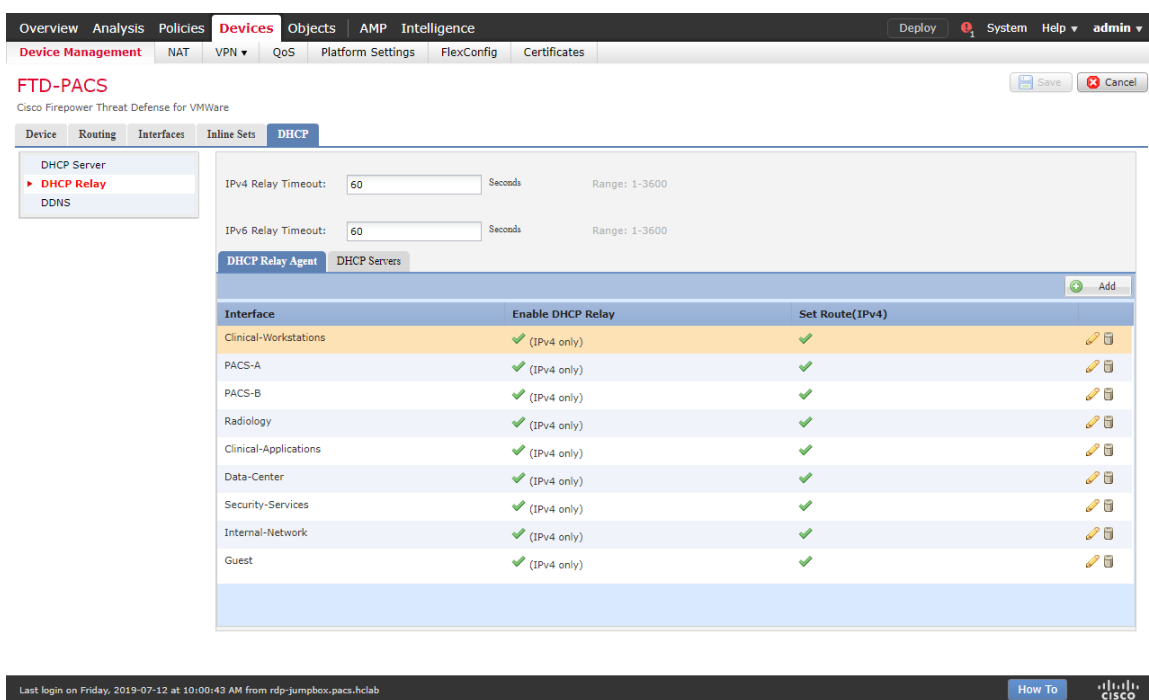
4. Navigate to the **DHCP** tab.



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

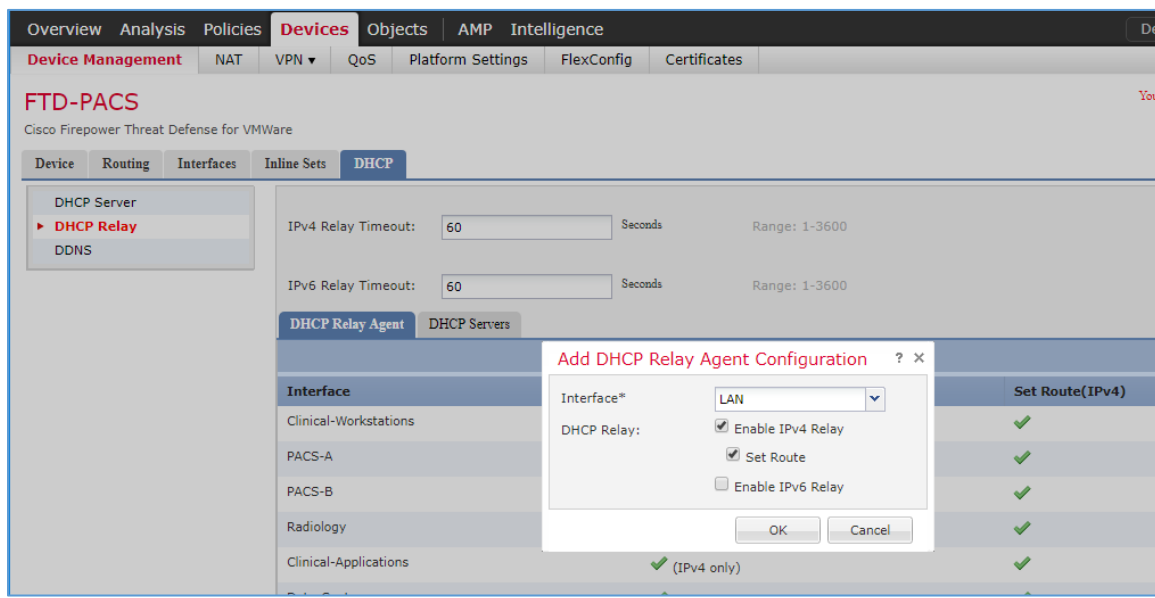


6. Under DHCP Relay Agent, click Add.

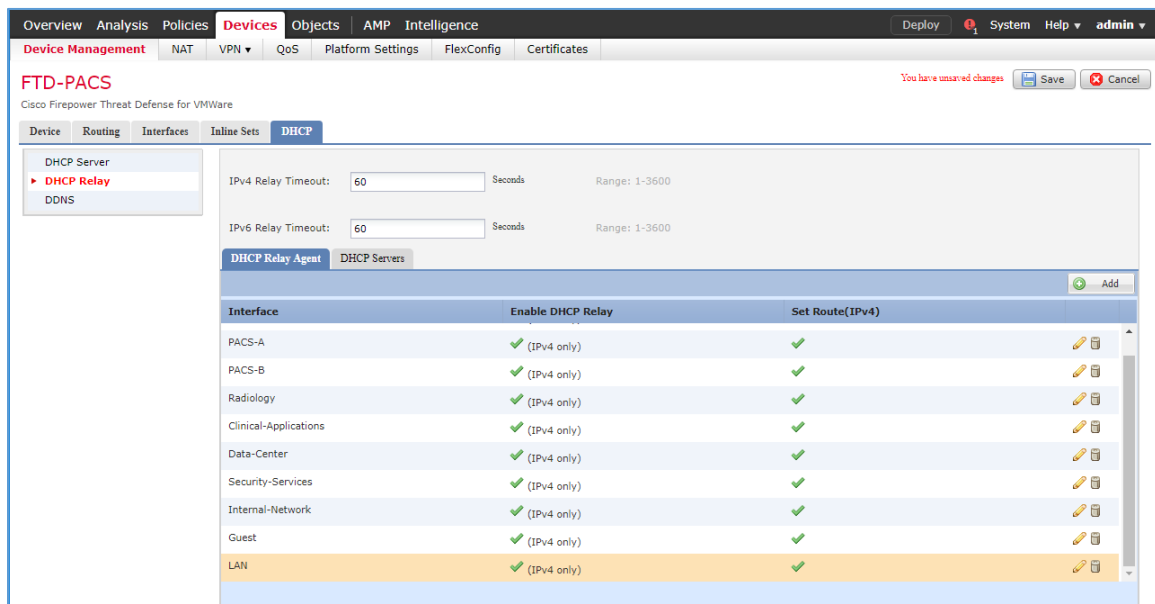


7. Assign an FTD interface as LAN.

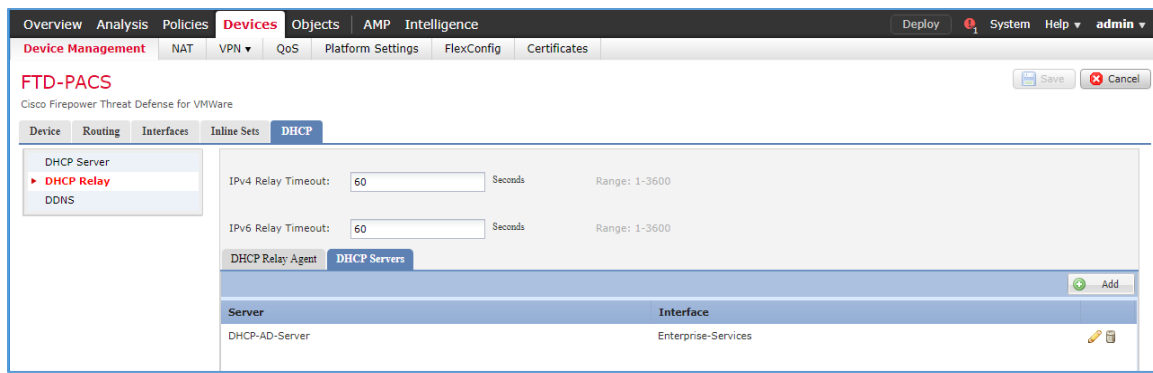
8. Check the box next to **Enable IPv4 Relay**.
9. Check the box next to **Set Route**.
10. Click **OK**.



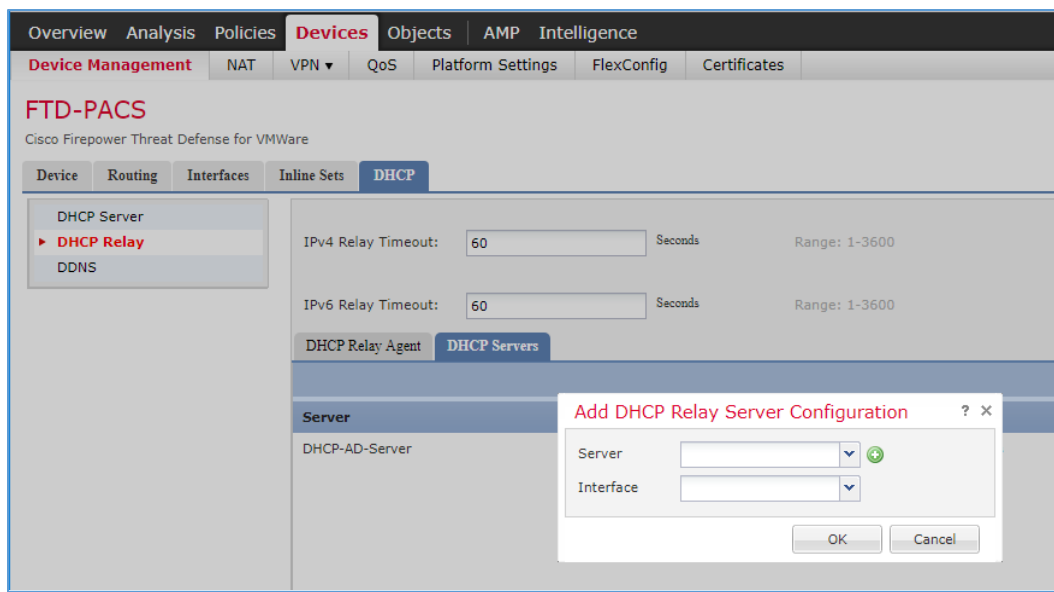
11. Ensure that the new relay, **LAN**, is in the **DHCP Relay Agent** list.



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



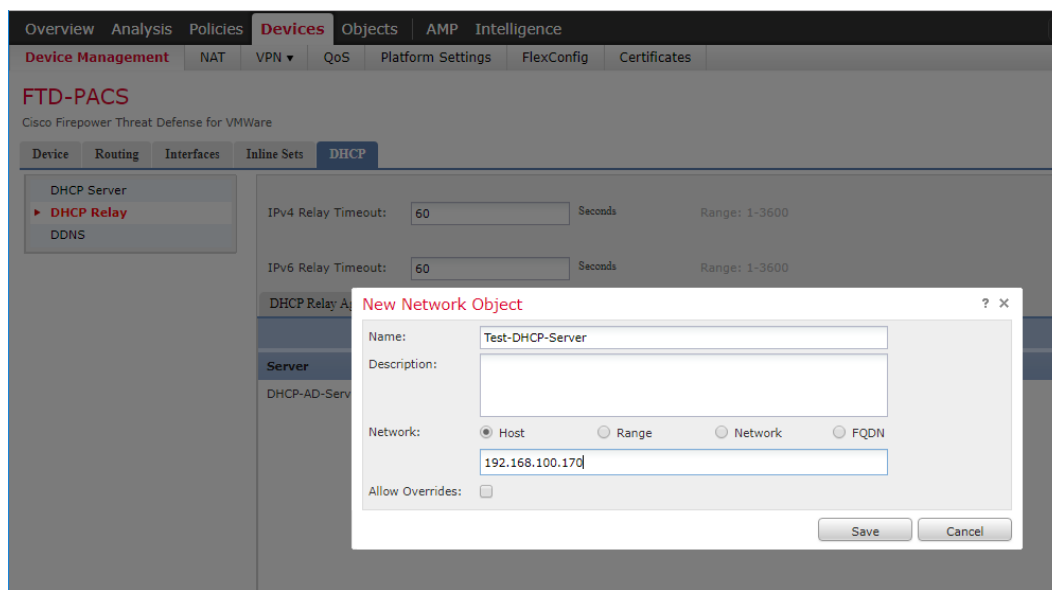
13. Click the green + button to create a new object for the DHCP server.



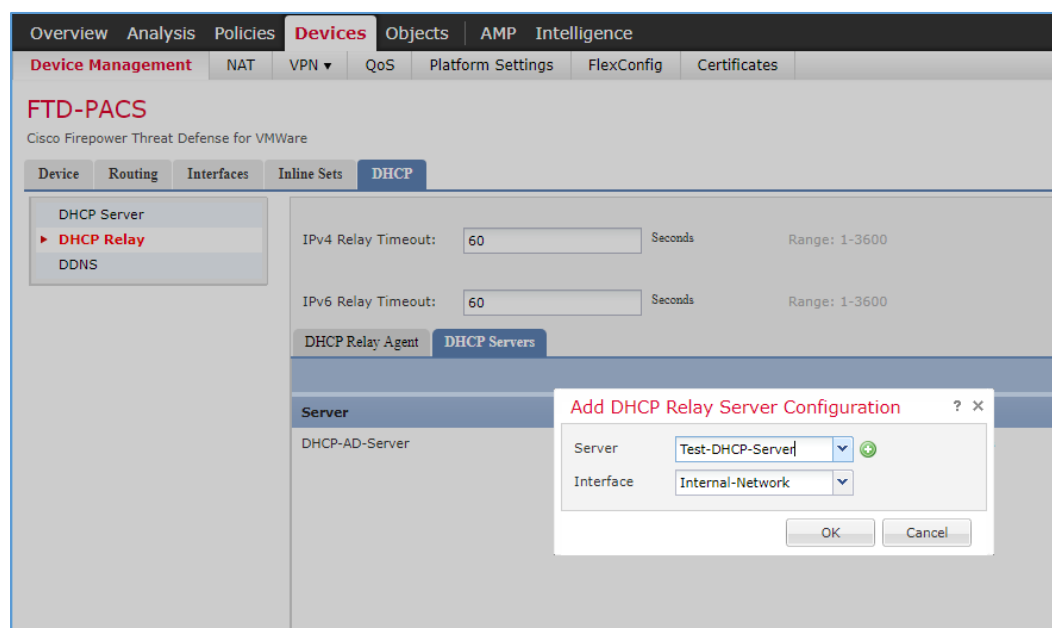
14. Enter **Test-DHCP-Server** as a **name** for the DHCP server.

15. Enter **192.168.100.170** as an **IP address** for the DHCP server.

16. Click **Save**.



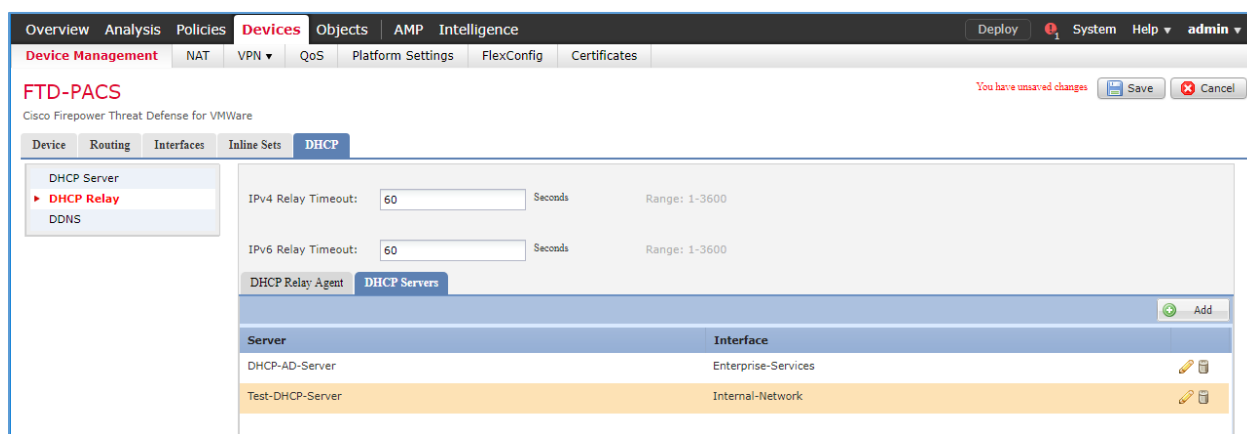
17. Select the newly created **DHCP server**.
18. Select an **FTD interface** through which the **DHCP server** can be connected.
19. Click **OK**.



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

21. Click **Save**.

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

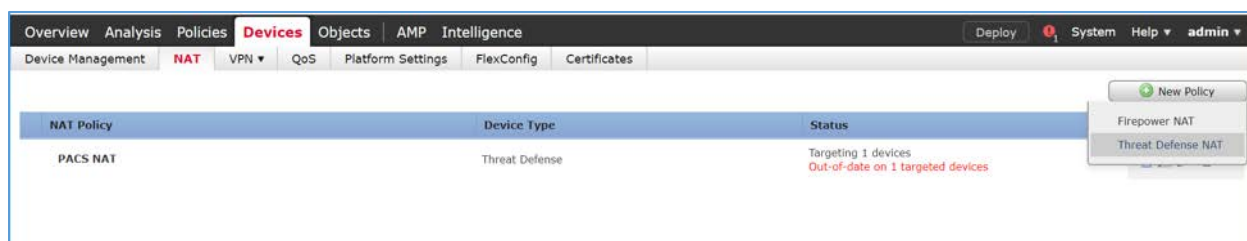


Network Address Translation (NAT) Rules Configuration

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



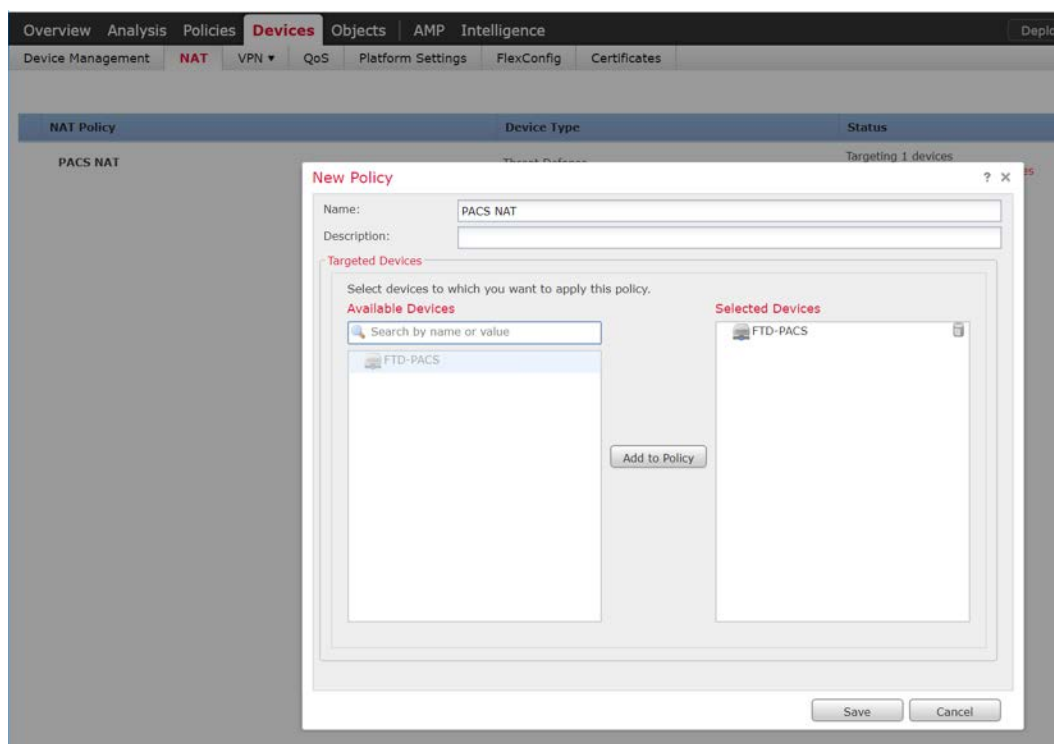
2. Click **New Policy > Threat Defense NAT**.



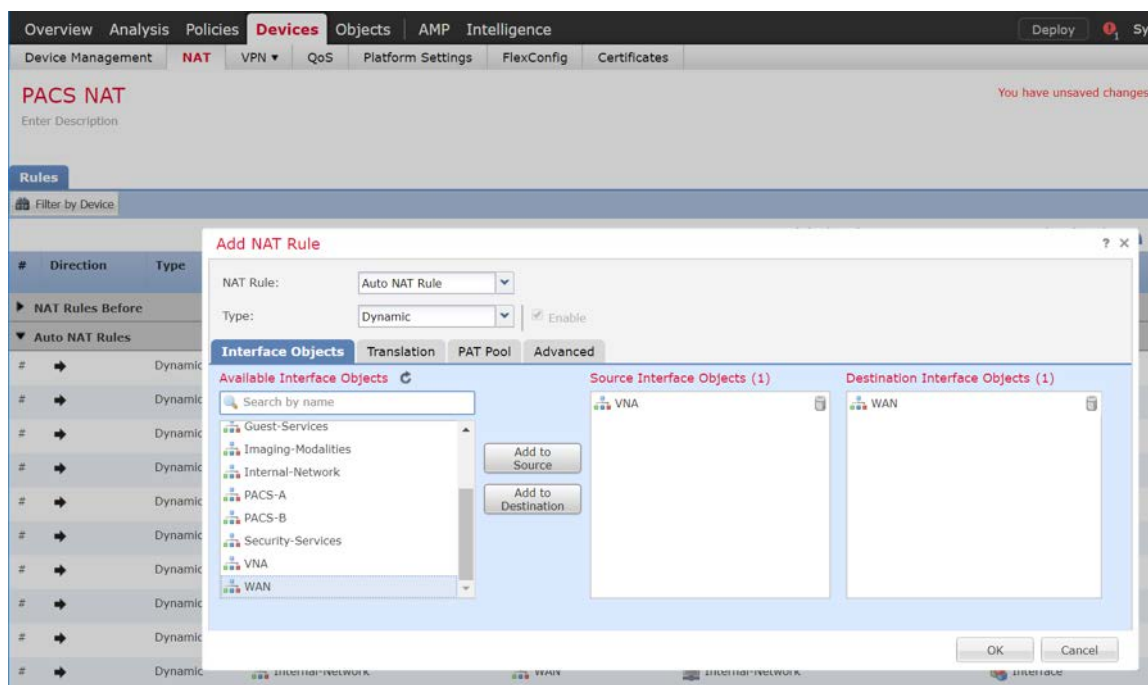
3. Give the new policy a **Name** as **PACS NAT**.

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

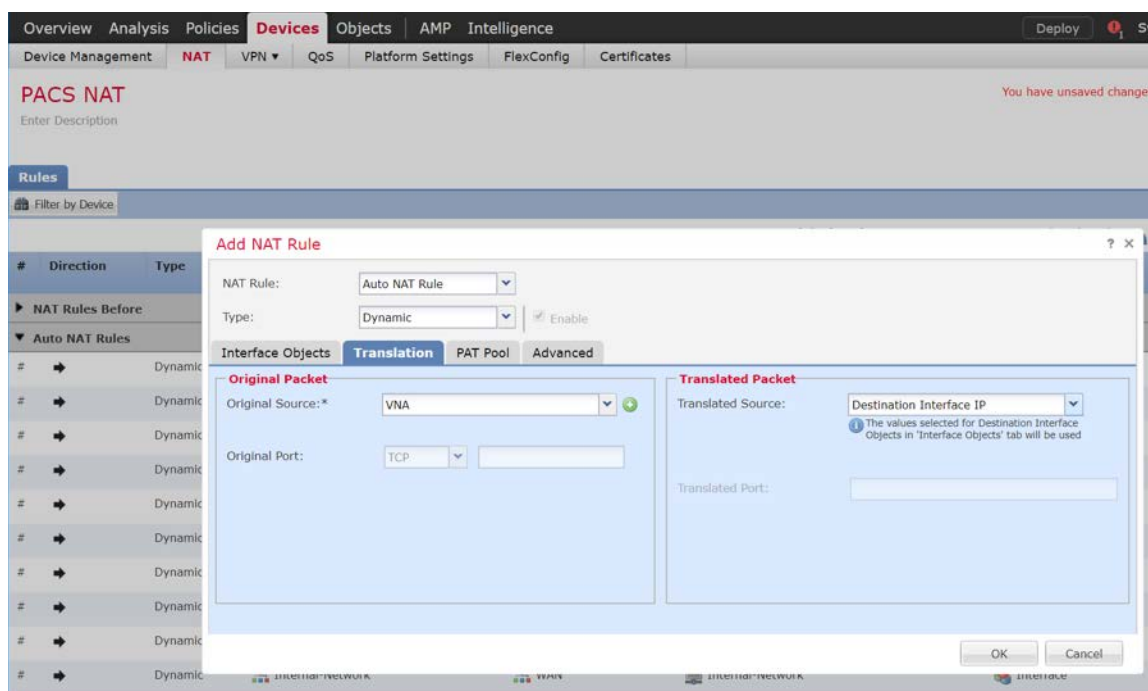
5. Click **Save**.



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



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



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

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

PACS NAT

Enter Description

You have unsaved changes Save Cancel

Policy Assignments (1)

Rules

Filter by Device Add Rule

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Translated Sources	Options
NAT Rules Before							
Auto NAT Rules							
#	→	Dynamic	Security-Services	WAN	Security-Services	Interface	Dns:false
#	→	Dynamic	Enterprise-Services	WAN	Enterprise-Services	Interface	Dns:false
#	→	Dynamic	Clinical-Viewers	WAN	Clinical-Viewers	Interface	Dns:false
#	→	Dynamic	PACS-A	WAN	PACS-A	Interface	Dns:false
#	→	Dynamic	PACS-B	WAN	PACS-B	Interface	Dns:false
#	→	Dynamic	Imaging-Modalities	WAN	Imaging-Modalities	Interface	Dns:false
#	→	Dynamic	Clinical-Application-Services	WAN	Clinical-Application-Services	Interface	Dns:false
#	→	Dynamic	Guest-Services	WAN	Guest-Services	Interface	Dns:false
#	→	Dynamic	Datacenter	WAN	Datacenter	Interface	Dns:false
#	→	Dynamic	Internal-Network	WAN	Internal-Network	Interface	Dns:false
#	→	Dynamic	VNA	WAN	VNA	Interface	Dns:false
NAT Rules After							

Displaying 1-13 of 13 rows Page 1 of 1

Last login on Thursday, 2019-07-18 at 09:23:00 AM from rdp-jumpbox.pacs.hclab

How To Cisco

Access Control Policy Through Firepower Management Center Configuration

The Firepower Management Center allows configuration of access-control policies that can then be applied to individual FTD appliances. The purpose of the access-control policy is to create rules that specify how traffic is managed within the network. Each access-control policy contains multiple rules followed by a default action established when the policy is created. For the PACS architecture, one access-control policy was established to manage the traffic on each FTD interface. The steps below describe how the policy and rules were created, as well as how to utilize an intrusion policy with the access-control policy. Additional information on the Cisco Firepower access control list and intrusion prevention configuration is available [10].

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

Overview Analysis **Policies** Devices Objects AMP Intelligence

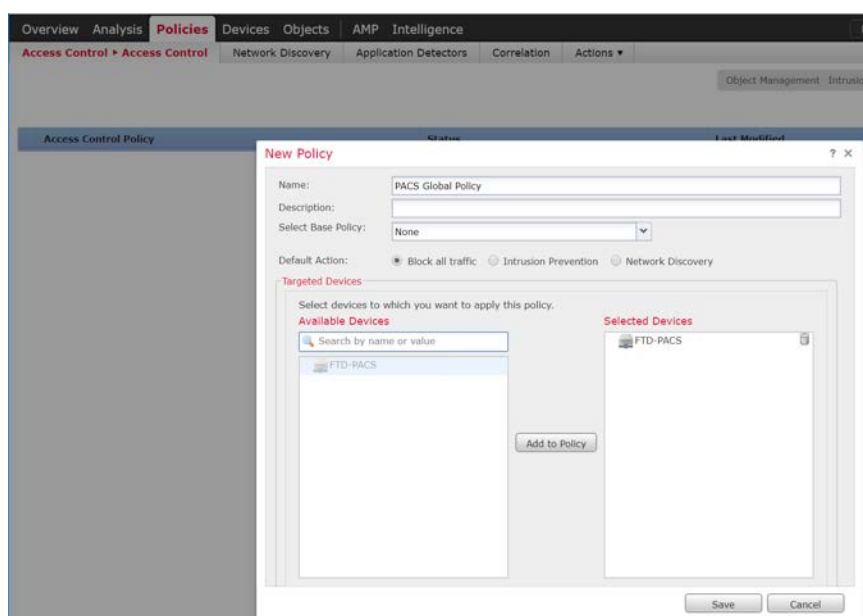
Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export

New Policy

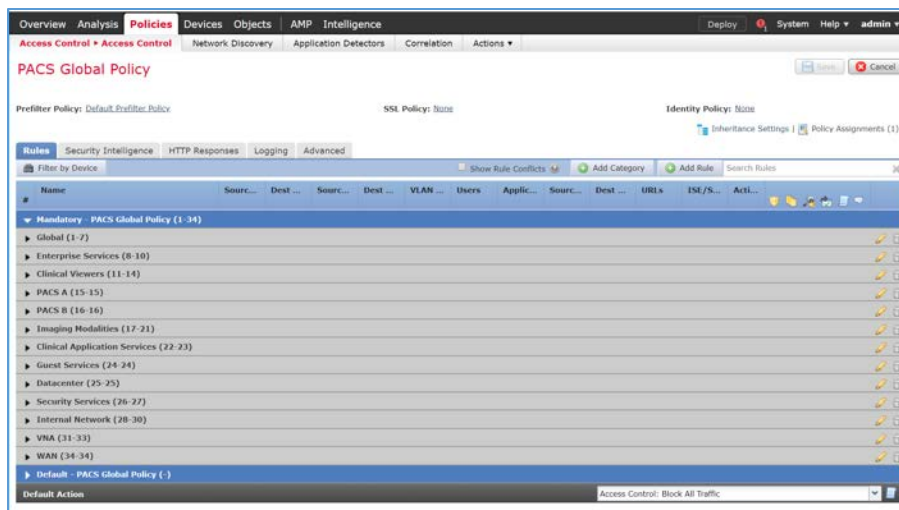
Access Control Policy	Status	Last Modified
-----------------------	--------	---------------

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



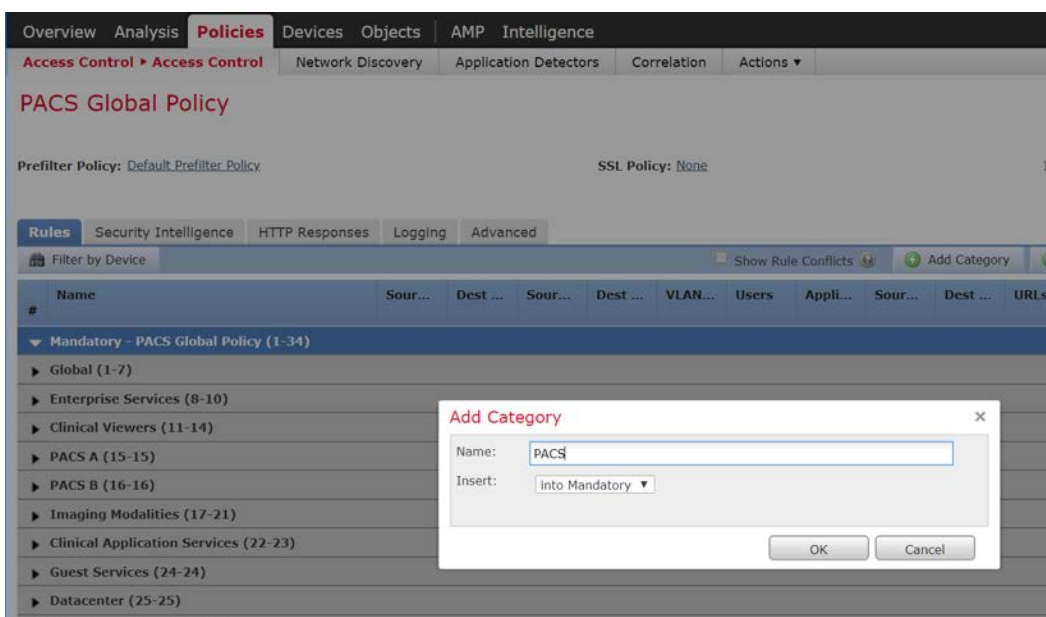
8. Click the access-control policy's **edit** icon.

Note: The policy in the screenshots that follow contains categories created during the process of building the PACS architecture. These categories are not preconfigured.



Create a Category

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



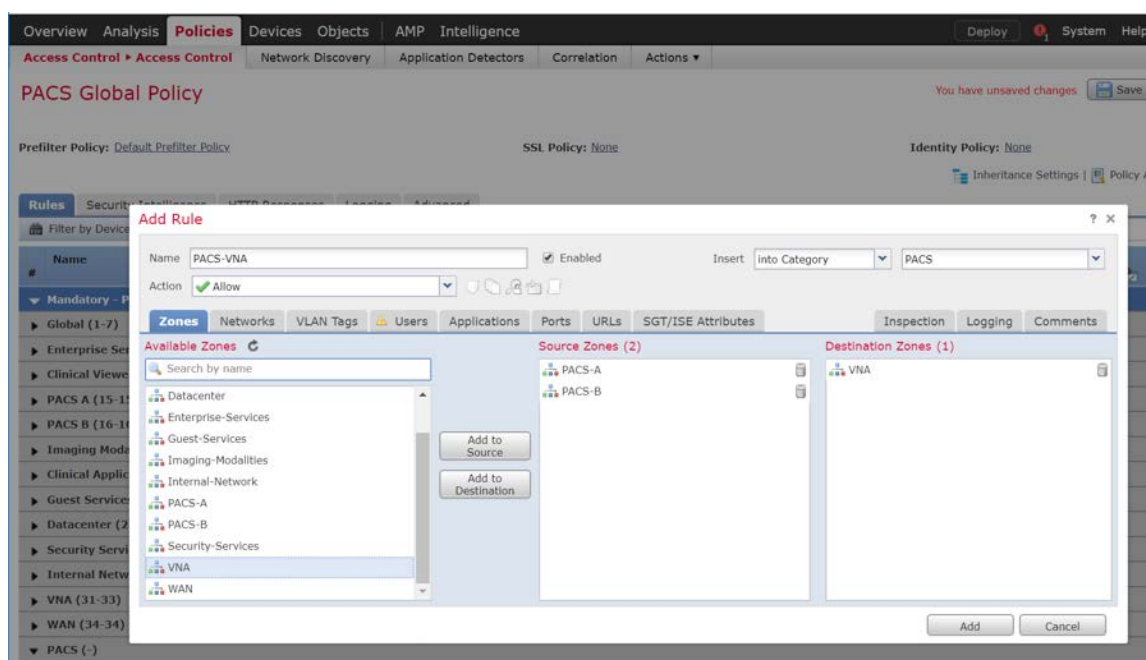
Create a Rule that Allows Application Traffic Between Security Zones

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

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

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

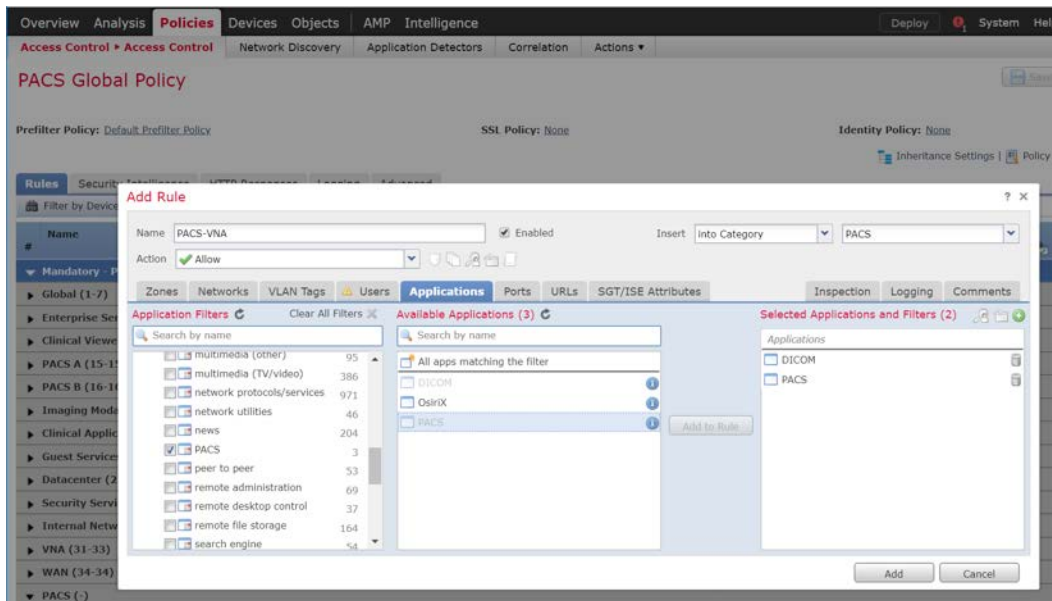
Note: The two primary methods for adding source and destination networks to an access control rule are through security zones or networks. Security zones are objects that can contain multiple FTD interfaces. Networks can be different types of network objects, including network segments (**192.168.1.0/24**)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



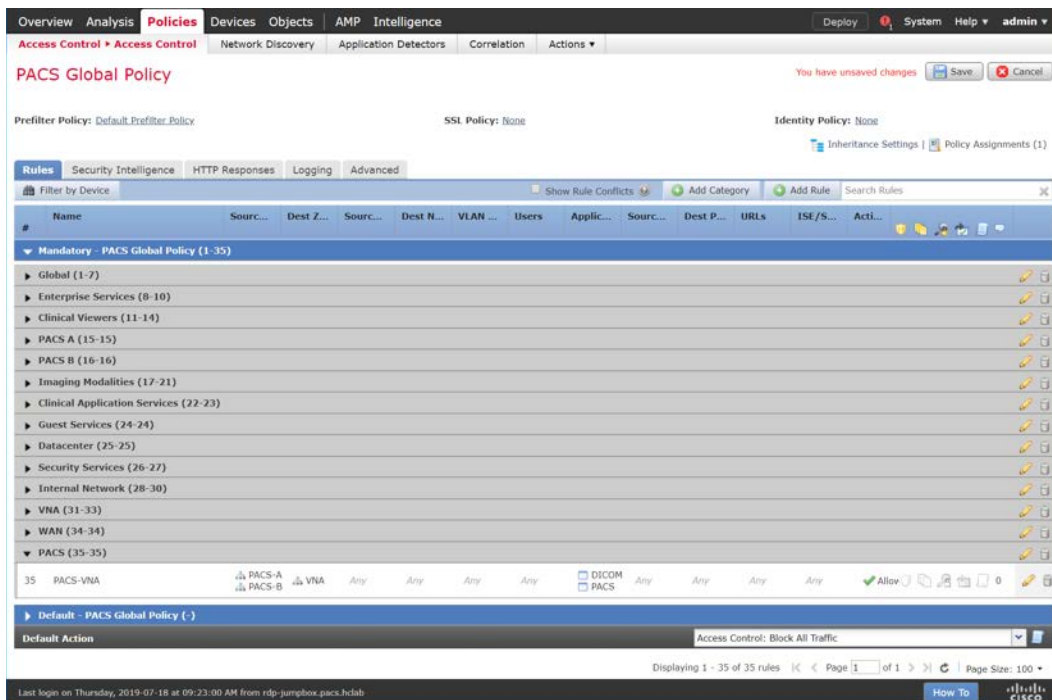
6. Under **Applications**, add the application(s) you would like to **allow** between the specified zones.

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

7. Click **Add**.



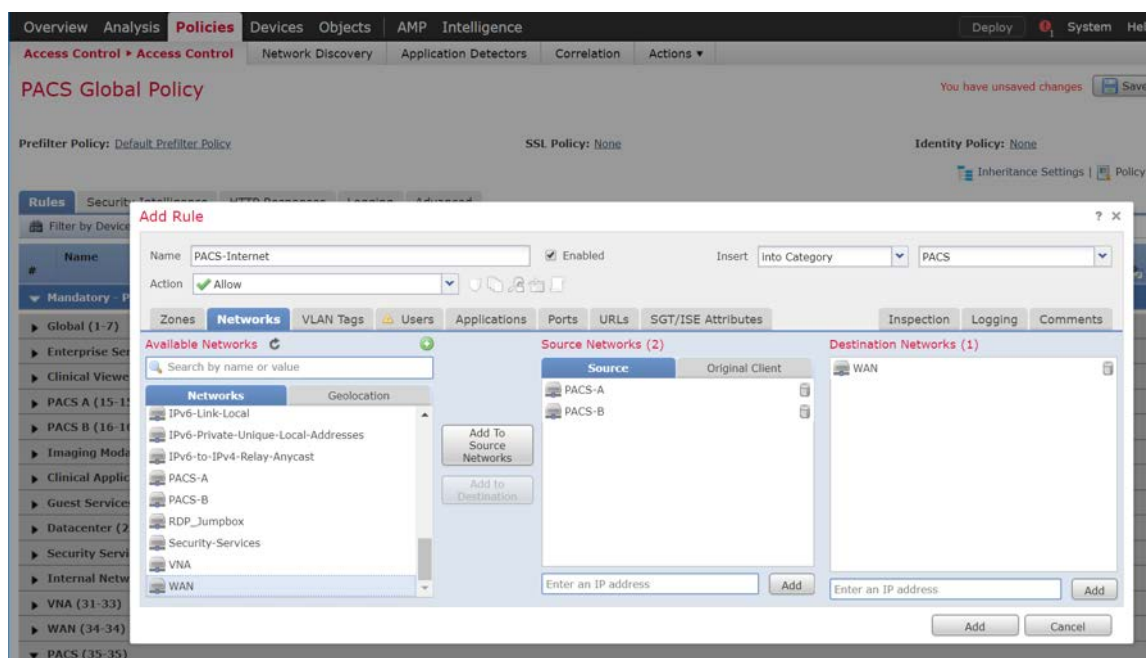
8. Verify that the Rule has been created.



Create a Rule that Allows Traffic on a Specific Port Between Networks

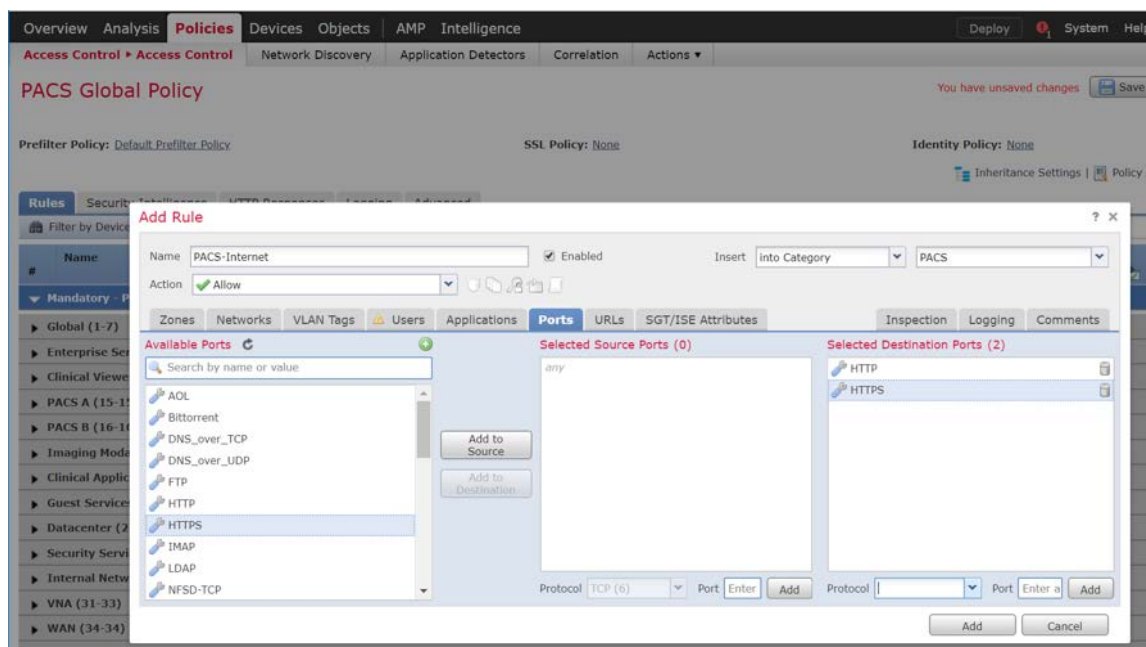
1. Click Add Rule.

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



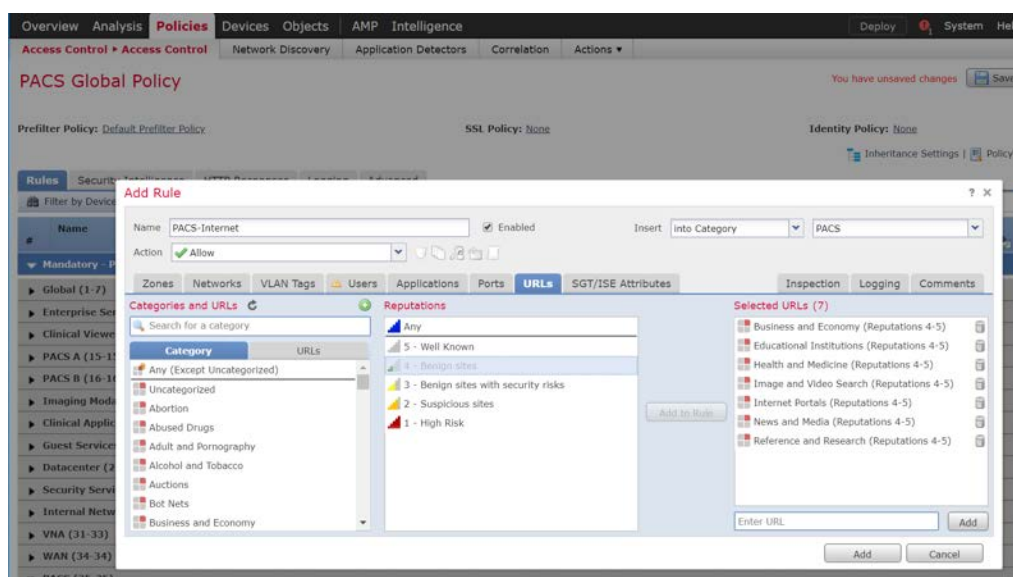
6. Under **Ports**, add (a) port(s) to the **Selected Destination Ports**.

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.



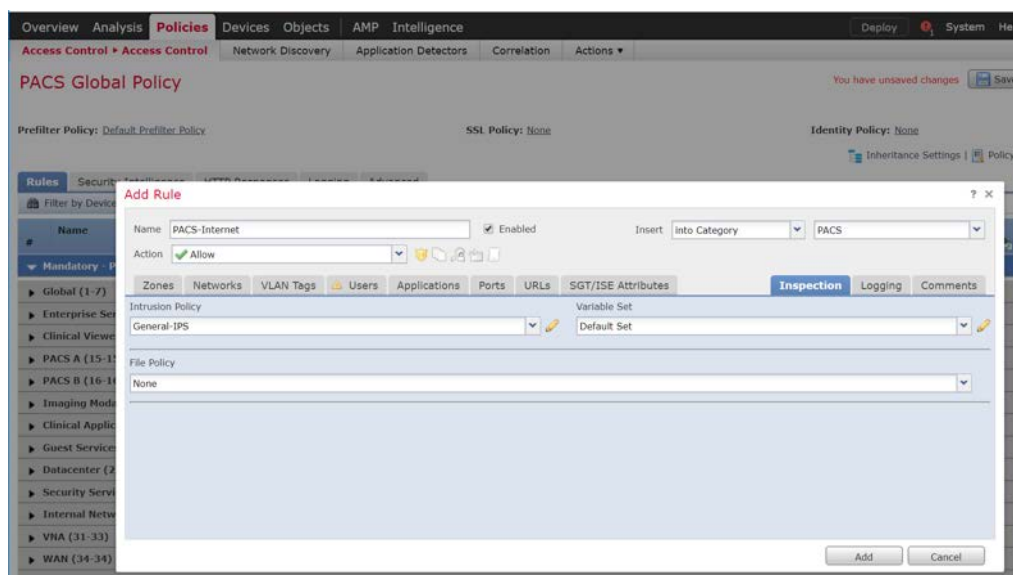
7. Under **URLs**, add **URL categories** that will be allowed (or leave this section blank).

Note: Cisco Firepower generates the URL categories and updates them regularly. Within each URL category, you can specify the reputation level that the URL must meet for the rule to match.



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

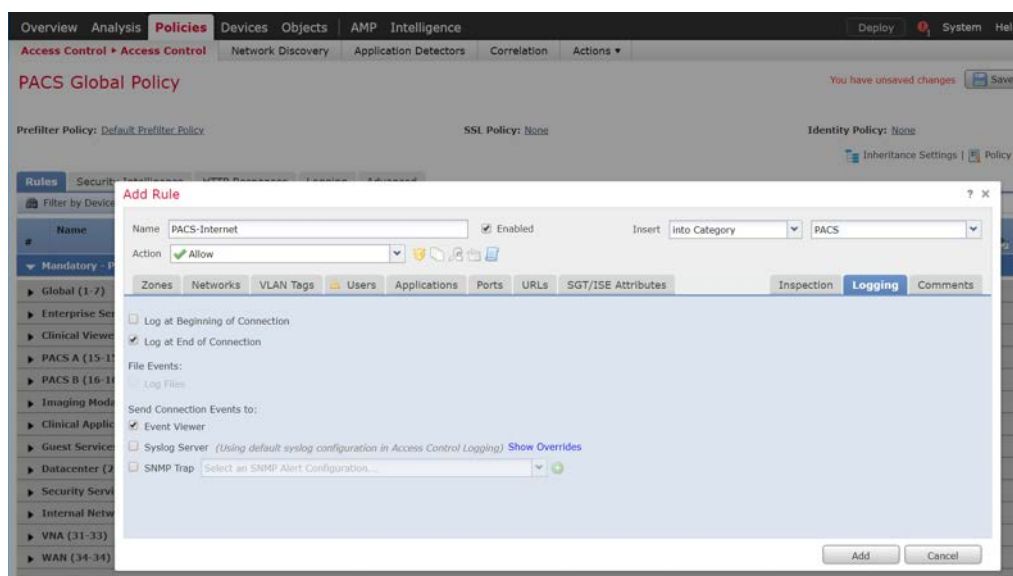
Note: Intrusion policies are created separately from the access-control policy. Once created, an intrusion policy can be applied to a specific access-control rule or an entire access-control policy. See the link posted [10] at the beginning of this section for more information on how to create and use intrusion policies in Cisco Firepower.



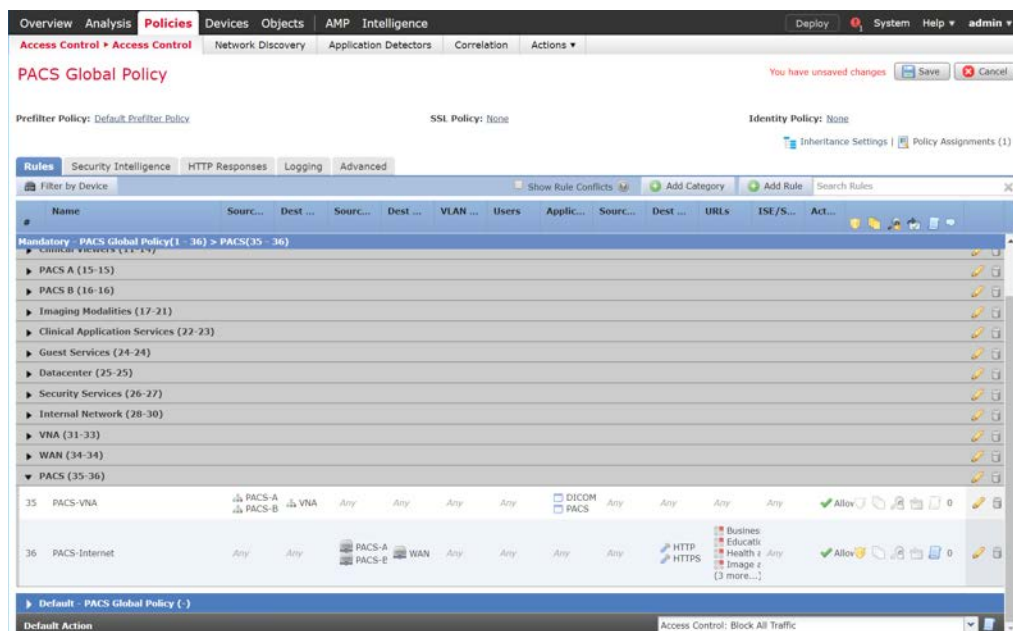
9. Under **Logging**, select **Log at End of Connection**, or leave this section blank.

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

10. Click **Add**.



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



2.7.2 Cisco Stealthwatch

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

Cisco Stealthwatch Management Console Appliance Information

- **CPUs:** 3
- **RAM:** 16 GB
- **Storage:** 60 GB (thin provision)
- **Network Adapter 1:** VLAN 1901
- **Operating System:** Linux

Cisco Stealthwatch Management Console Virtual Edition Installation Guide

Install the Cisco Stealthwatch Management Console appliance according to the instructions detailed in the Cisco installation guide [11].

Cisco Stealthwatch User Datagram Protocol (UDP) Director Appliance Information

- **CPU:** 1
- **RAM:** 4 GB
- **Storage:** 60 GB (thin provision)
- **Network Adapter 1:** VLAN 1901
- **Network Adapter 2:** VLAN 1901
- **Operating System:** Linux

Cisco Stealthwatch UDP Director Virtual Edition Installation Guide

Install the Cisco Stealthwatch UDP Director appliance according to the instructions provided in the Cisco installation guide [\[11\]](#).

Cisco Stealthwatch Flow Collector Appliance Information

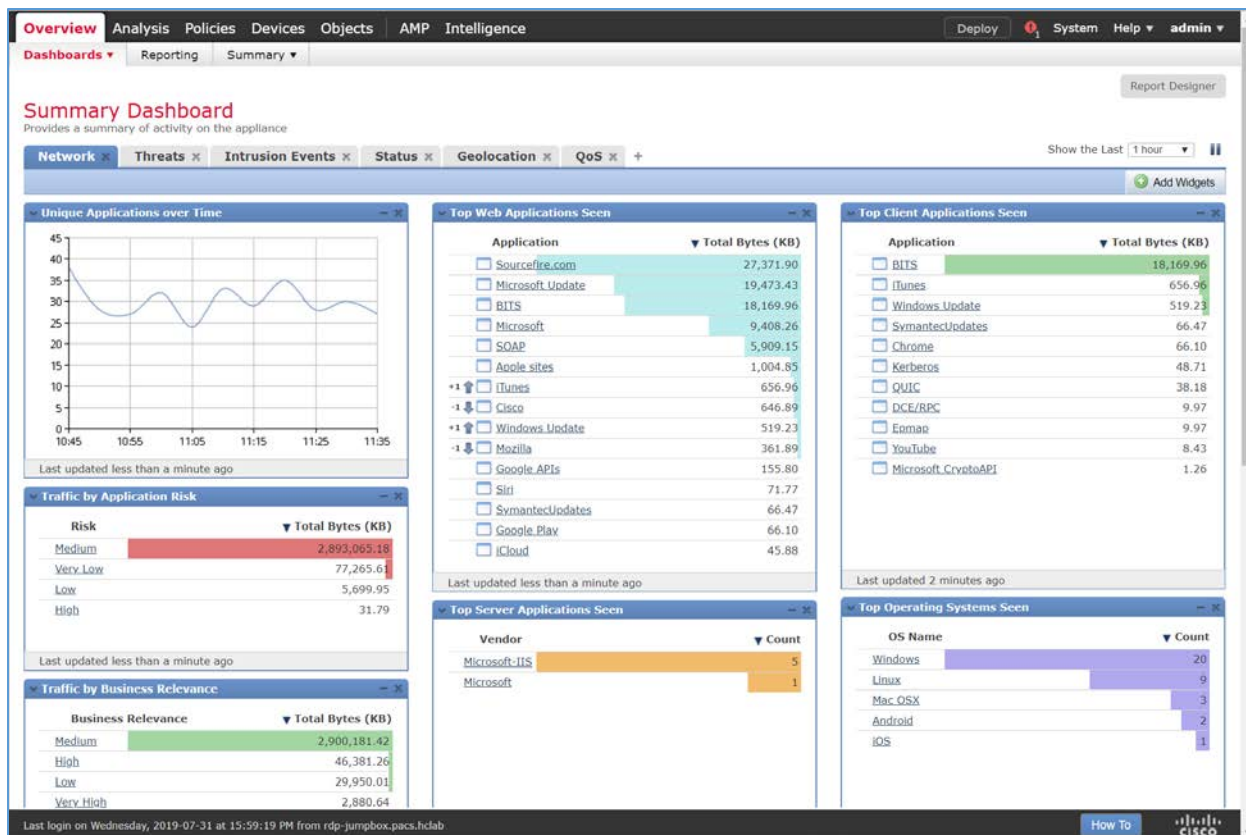
- **CPUs:** 2
- **RAM:** 16 GB
- **Storage:** 60 GB (thin provision)
- **Network Adapter 1:** VLAN 1901
- **Operating System:** Linux

Cisco Stealthwatch Flow Collector Virtual Edition Installation Guide

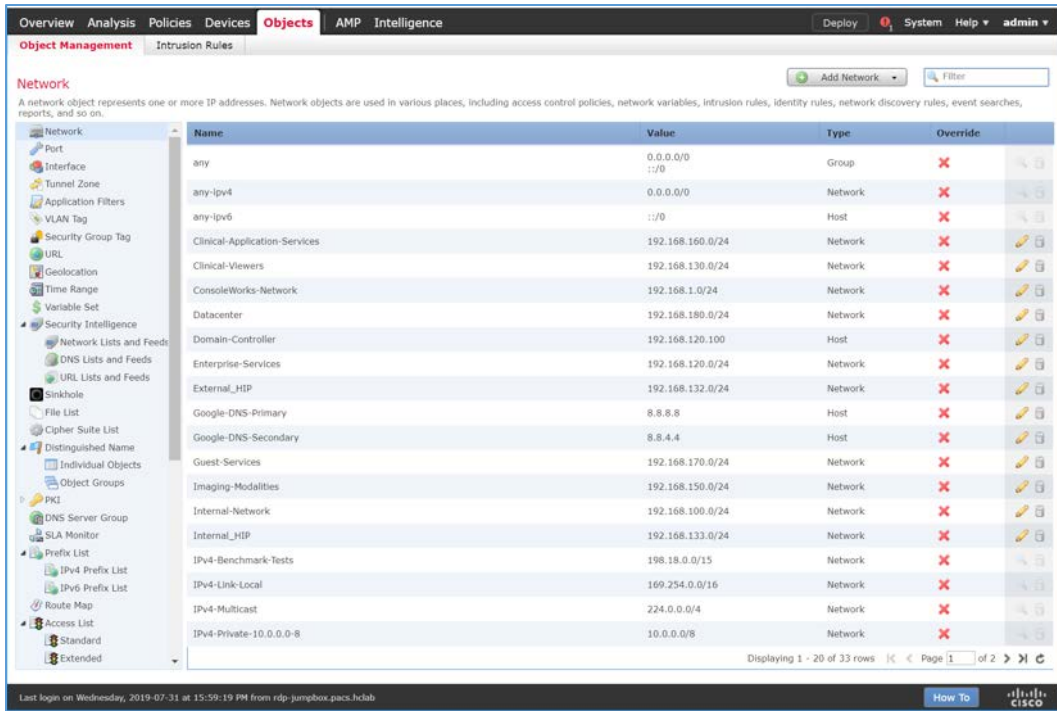
Install the Cisco Stealthwatch Flow Collector appliance according to the instructions provided in the Cisco installation guide [\[11\]](#).

Configure NetFlow Parameters for Cisco Firepower

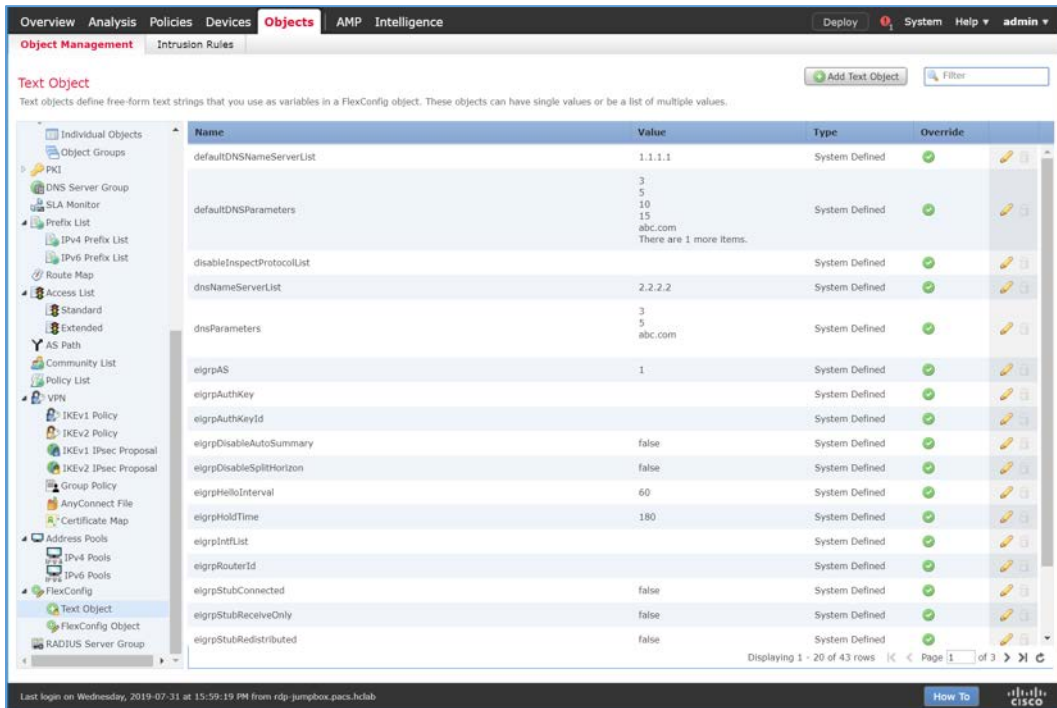
1. Log in to the Cisco Firepower Management Console.



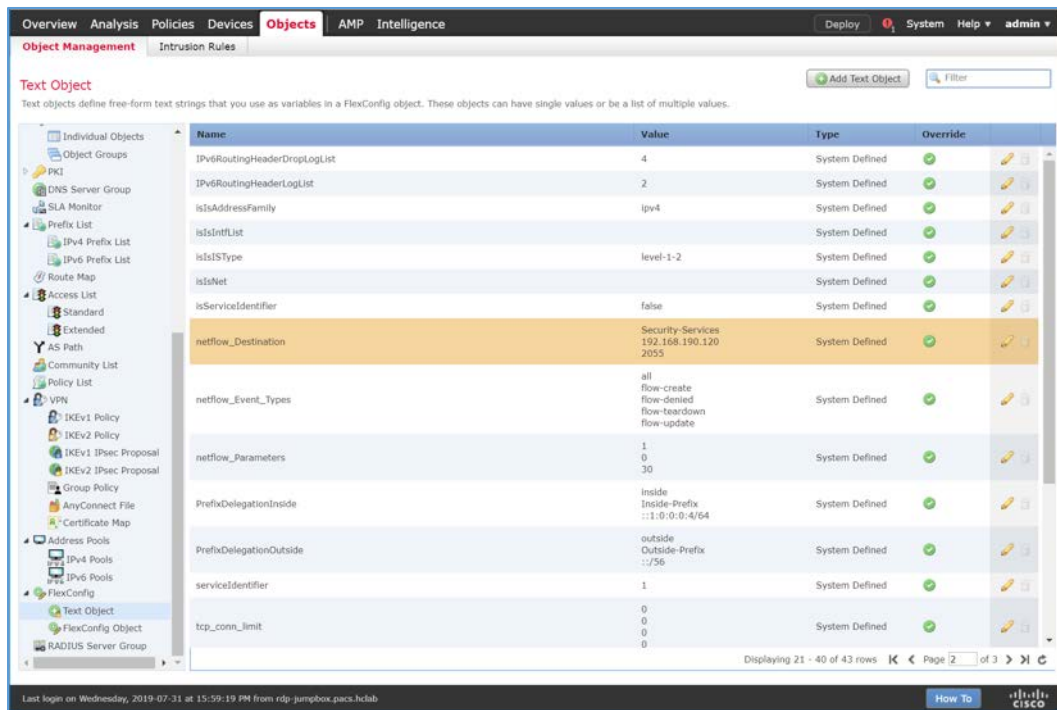
2. Navigate to **Objects**.



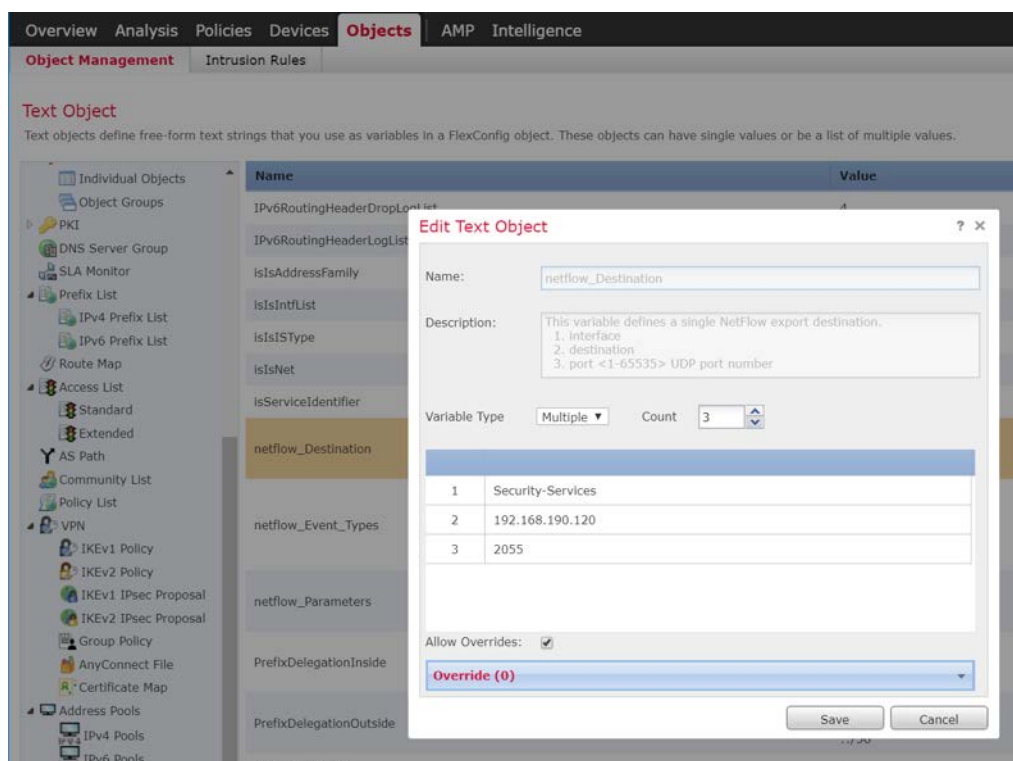
3. Navigate to **FlexConfig > Text Object**.



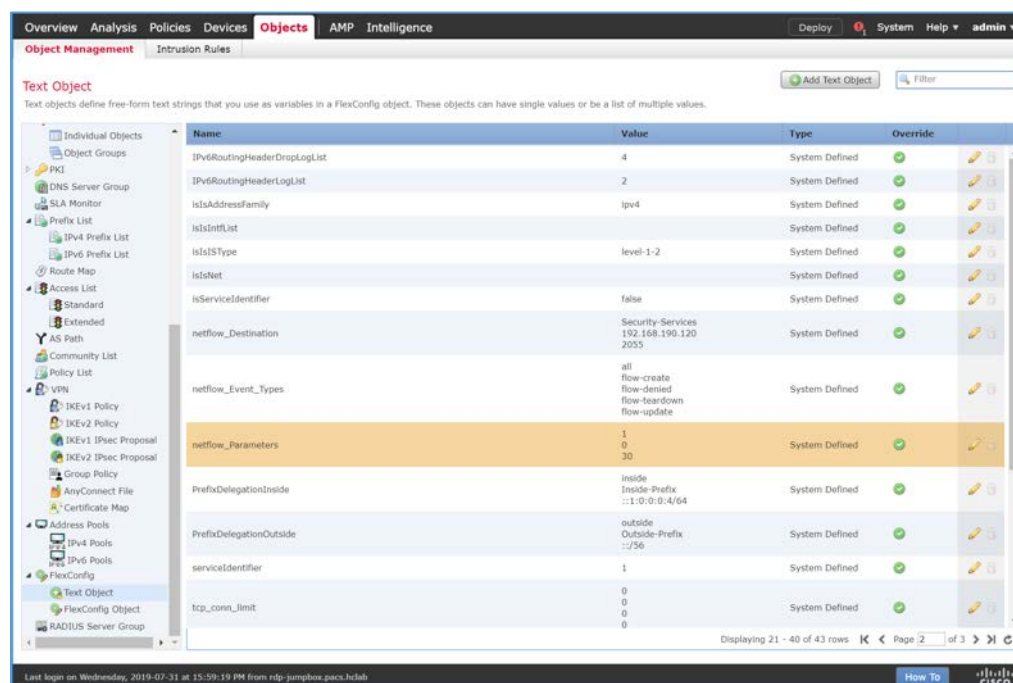
- Under the **Name** column, find **netflow_Destination**.



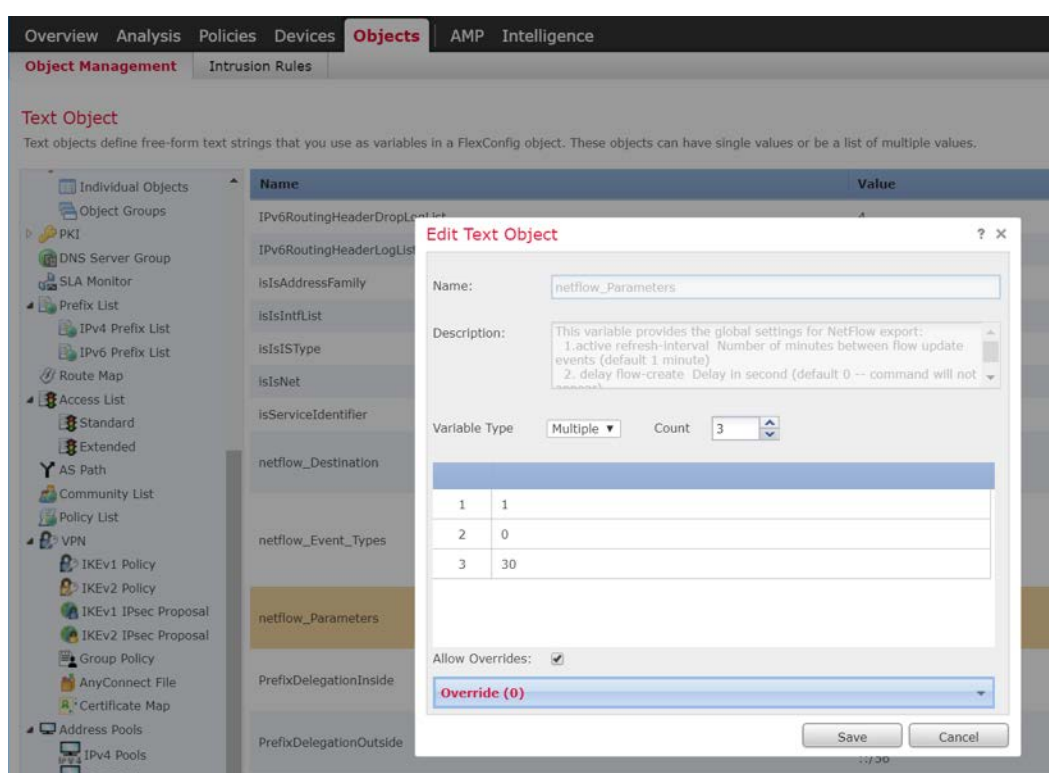
- Click the **edit** icon for **netflow_Destination**.
- Set **Variable Type** to **Multiple**.
- Set **Count** to **3**.
- For **Row 1**, enter **Security-Service** to set the name of the Cisco FTD interface to which the Cisco Stealthwatch UDP appliance is connected.
- For **Row 2**, enter **192.168.190.120**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



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



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

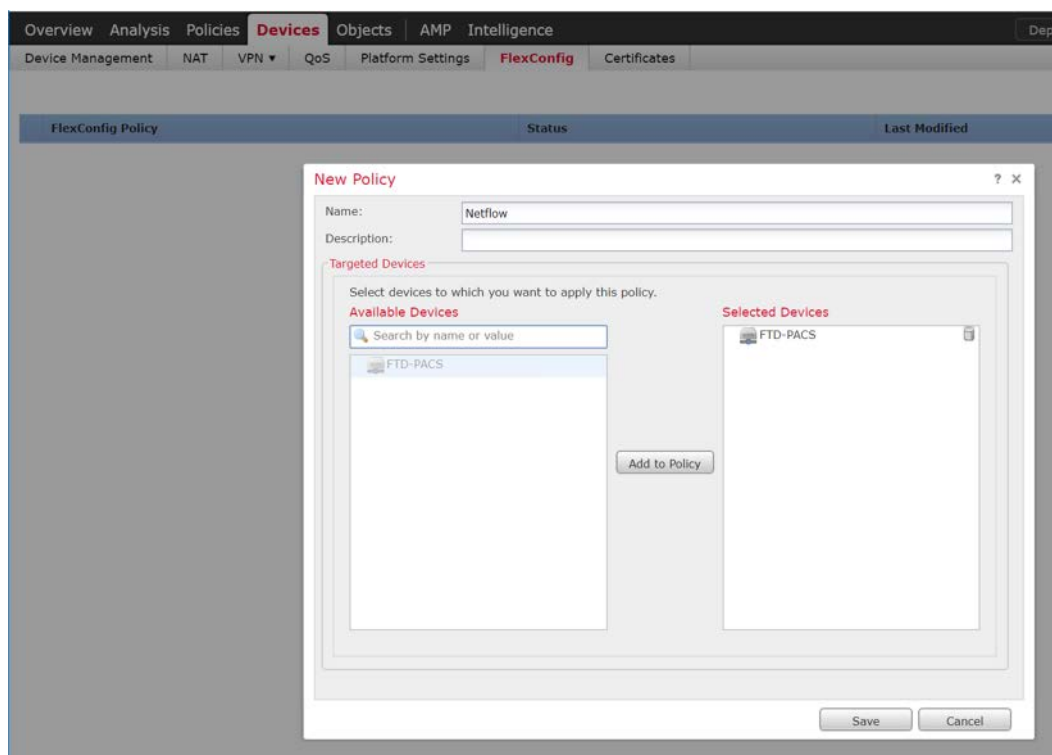


20. Navigate to **Devices > FlexConfig**.



21. Click **New Policy**.

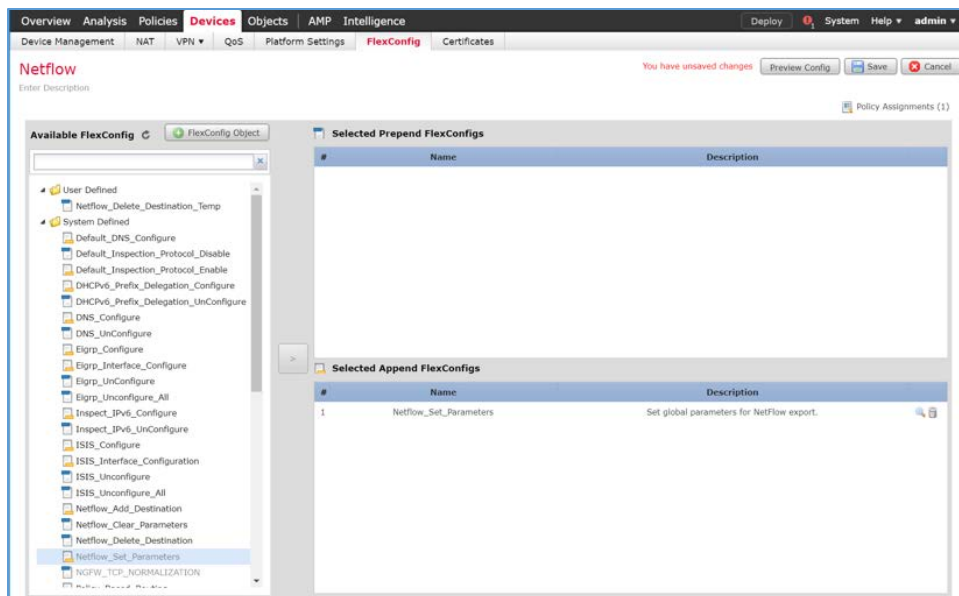
22. Enter a **Name** (e.g., **Netflow**) for the policy.
23. Under **Selected Devices**, add the Cisco FTD.
24. Click **Save**.



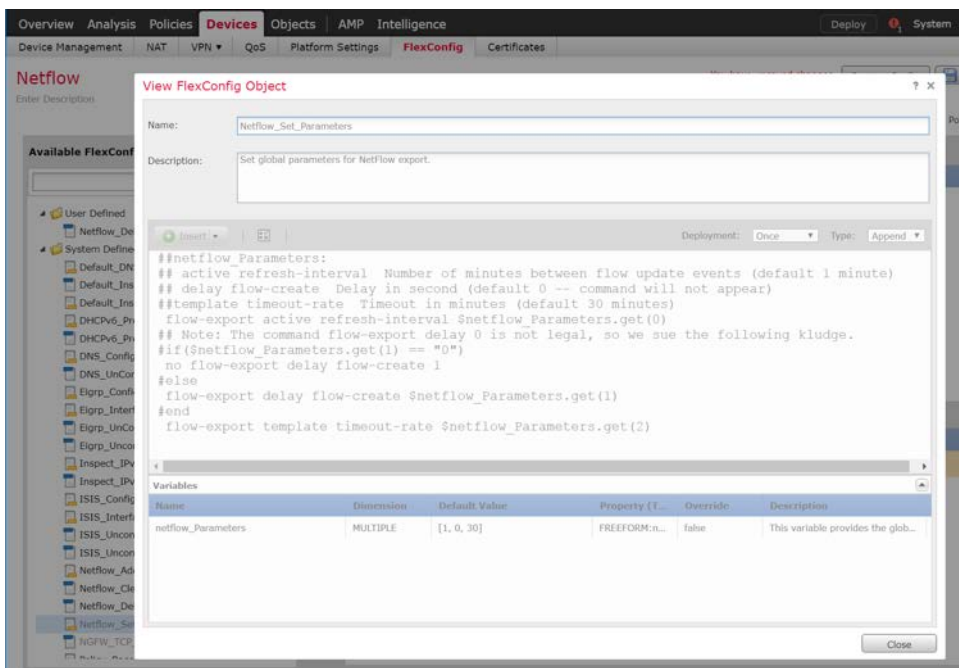
25. Click the **edit** icon for the new policy.



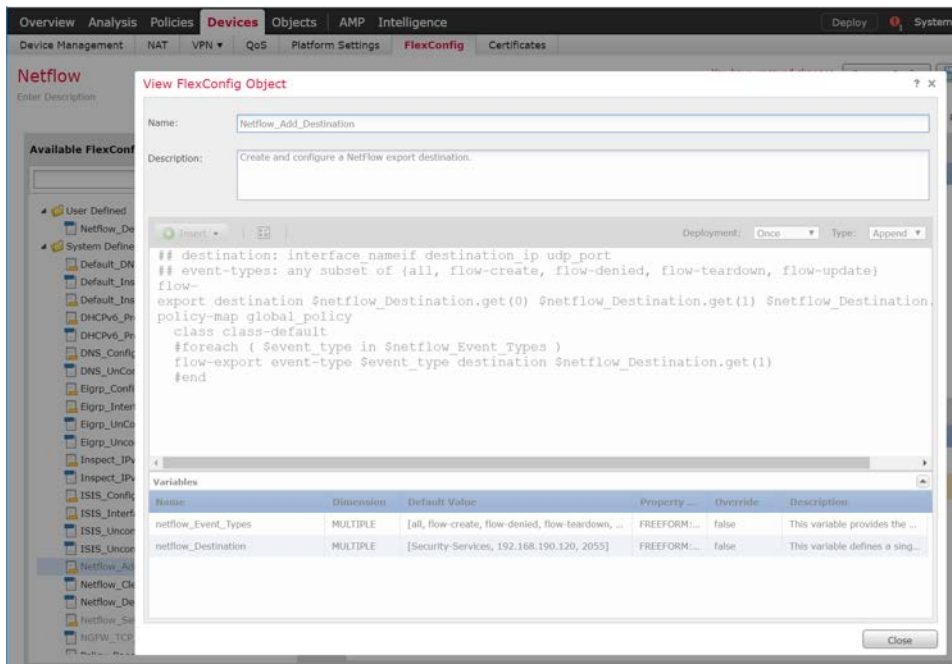
26. Under **Available FlexConfig**, find **Netflow_Set_Parameters**, and add it to **Selected Append FlexConfigs**.



27. Click the **magnifier** icon for **Netflow_Set_Parameters**.
28. Under **Variables > Default Value**, verify the minutes between flow data events, seconds to delay flow create, and minutes for template time-out rate that were set for **netflow_Parameters**.
29. Click **Close**.



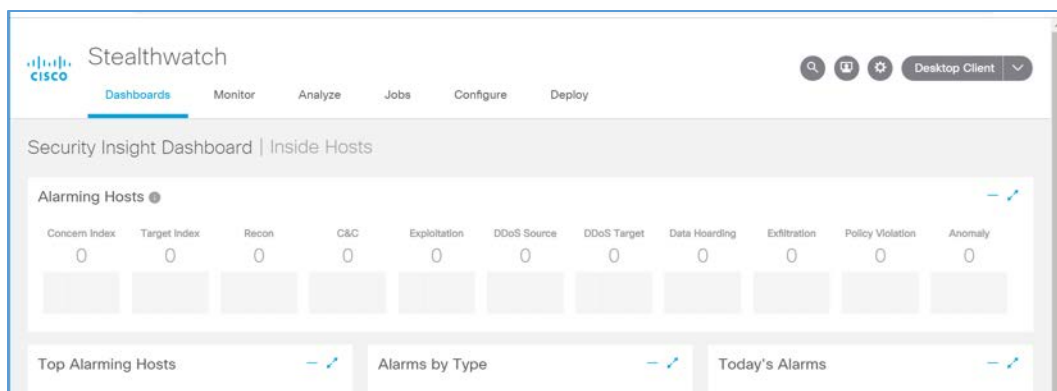
30. Under **Available FlexConfig**, find **Netflow_Add_Destination**, and add it to **Selected Append FlexConfigs**.
31. Click the **magnifier** icon for **Netflow_Add_Destination**.
32. Under **Variables > Default Value**, verify the Cisco FTD interface name, IP address of the Cisco Stealthwatch, and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



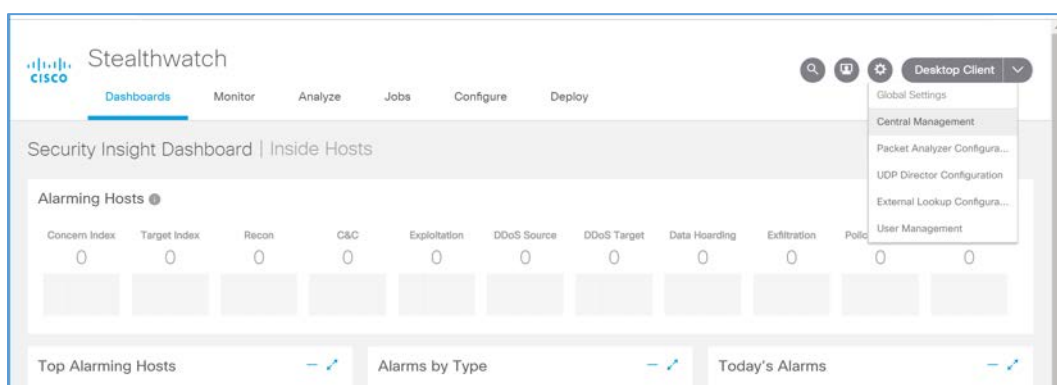
34. Click **Save**.
35. Deploy changes to the Cisco FTD.

Forwarding Rules for Cisco Stealthwatch UDP Configuration

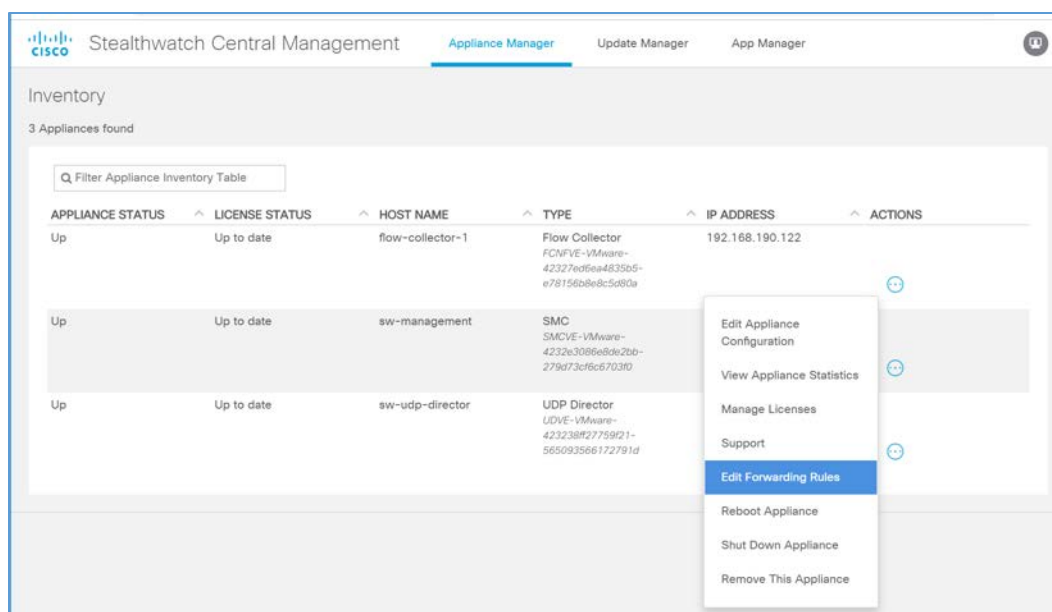
1. Log in to the web dashboard of the Cisco Stealthwatch Management Console.



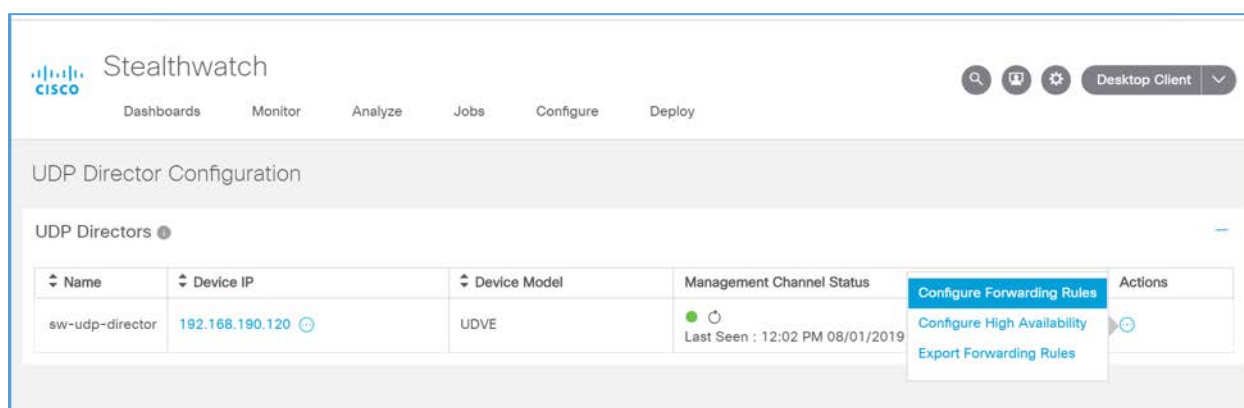
2. Navigate to **Settings > Central Management**.



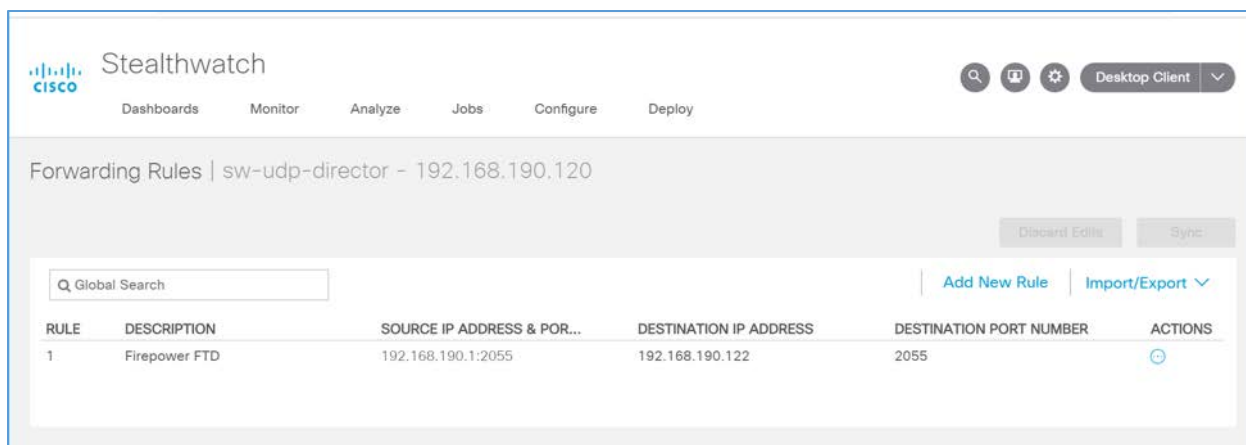
3. Click the **ellipsis** for the Cisco Stealthwatch UDP appliance and select **Edit Forwarding Rules**.



- Click the **ellipsis** for the Cisco Stealthwatch UDP appliance, select **Configure Forwarding Rules**.



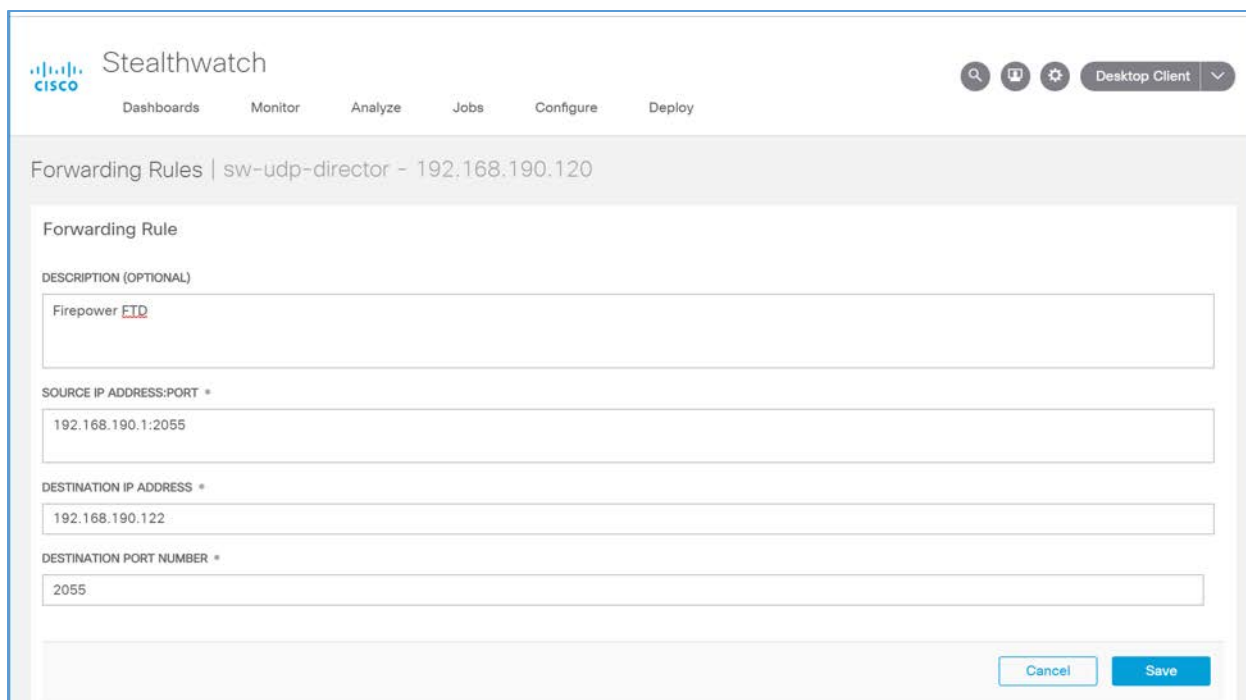
- Under **Forwarding Rules**, select **Add New Rule**.



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 setup of the Flow Collector.



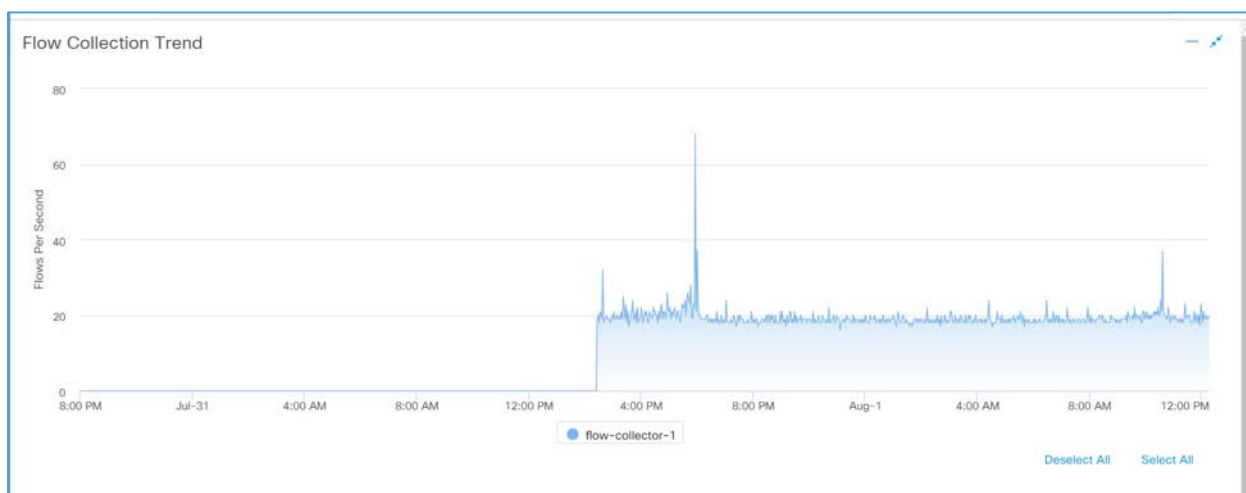
The screenshot shows the Cisco Stealthwatch Management Console interface. At the top, there is a navigation bar with the Cisco logo and the word "Stealthwatch". Below this, there are tabs for "Dashboards", "Monitor", "Analyze", "Jobs", "Configure", and "Deploy". On the right side of the navigation bar, there are icons for search, help, settings, and a "Desktop Client" dropdown menu.

The main content area is titled "Forwarding Rules | sw-udp-director - 192.168.190.120". Below this title, there is a form for configuring a "Forwarding Rule". The form has the following fields:

- DESCRIPTION (OPTIONAL):** A text area containing the text "Firepower FTD".
- SOURCE IP ADDRESS:PORT *:** A text field containing the value "192.168.190.1:2055".
- DESTINATION IP ADDRESS *:** A text field containing the value "192.168.190.122".
- DESTINATION PORT NUMBER *:** A text field containing the value "2055".

At the bottom right of the form, there are two buttons: "Cancel" and "Save".

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

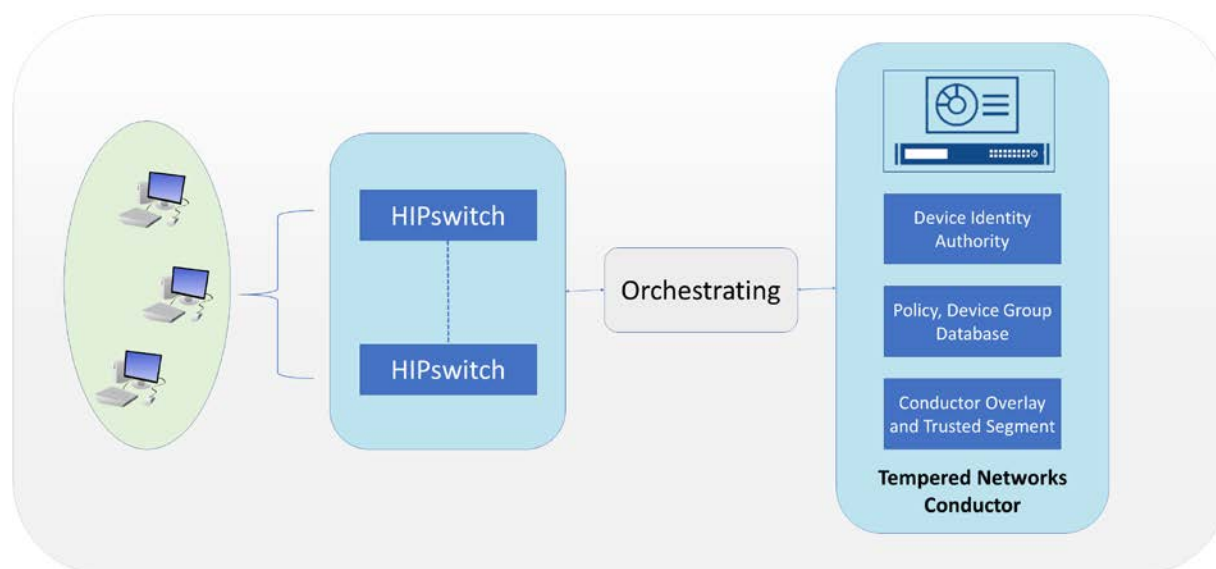


2.7.3 Tempered Networks Identity Defined Networking (IDN)

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

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

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 to the IDN end points that enforce explicit trust relationships through device-based allow-listing.

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

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

2.7.3.1 Conductor Installation

System Requirements

- **CPUs:** 4
- **Memory:** 4 GB RAM
- **Storage:** 120 GB

- **Operating System:** Linux Red Hat
- **Network Adapter:** VLAN 1201

Tempered Networks Conductor Installation

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

2.7.3.2 HIPswitch Installation

System Requirements

- **CPUs:** 4
- **Memory:** 1 GB RAM
- **Storage:** 1 GB
- **Operating System:** Linux Red Hat
- **Network Adapter:** VLAN 1201

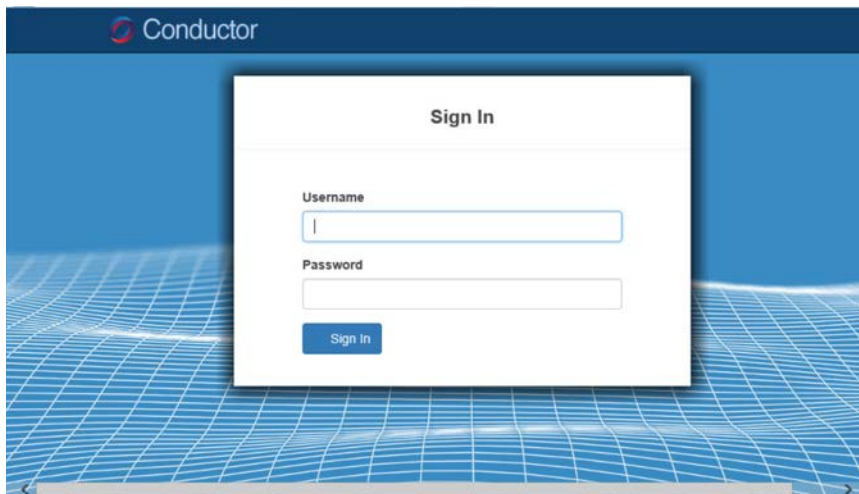
HIPswitch Installation

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

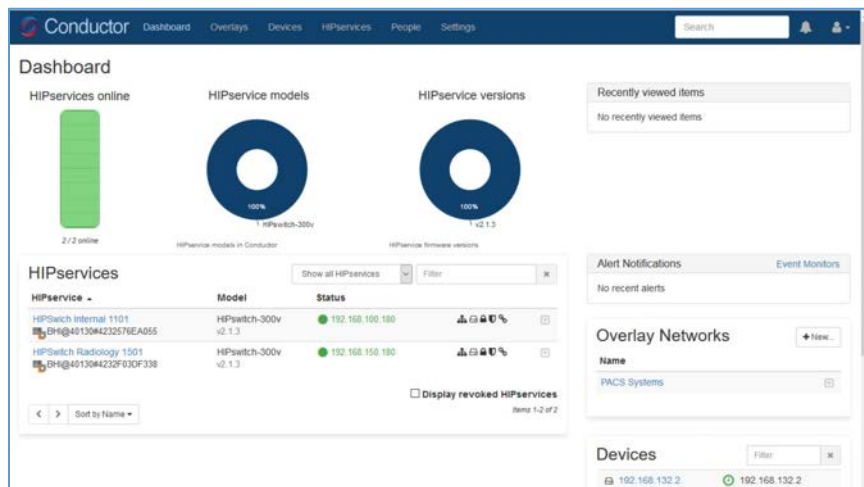
Tempered Networks Conductor and HIPswitch Configuration

Configuration for the Conductor and HIPswitches is done through the browser connected to the Conductor <https://ConductorIP>. The login page appears below.

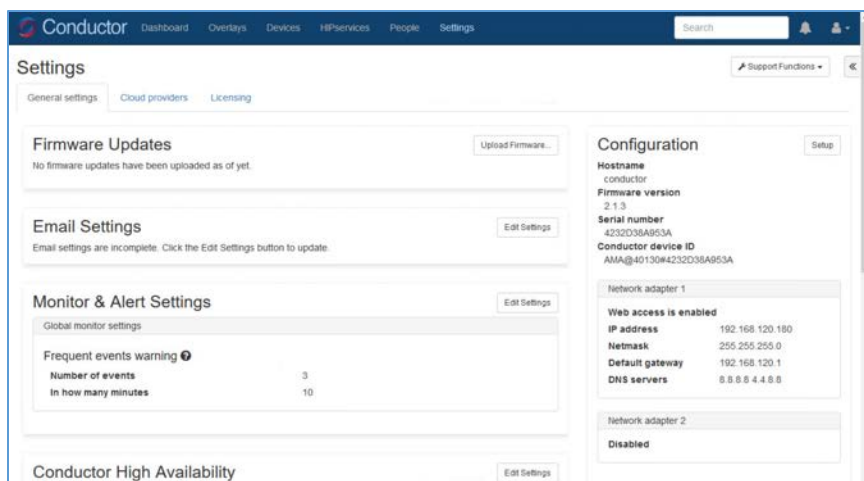
1. Enter the **username** and **password** to open the dashboard.



2. Click the **Settings** tab.



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



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

System Configuration

Host name

conductor

Domain name

Network adapter 1

Network adapter 2

☒ Enable network adapter

☒ Enable web access to Conductor

Network configuration

Static IP

IP address

192.168.120.180

Netmask

255.255.255.0

Default gateway

192.168.120.1

DNS1

8.8.8.8

DNS2

4.4.8.8

Static Routes

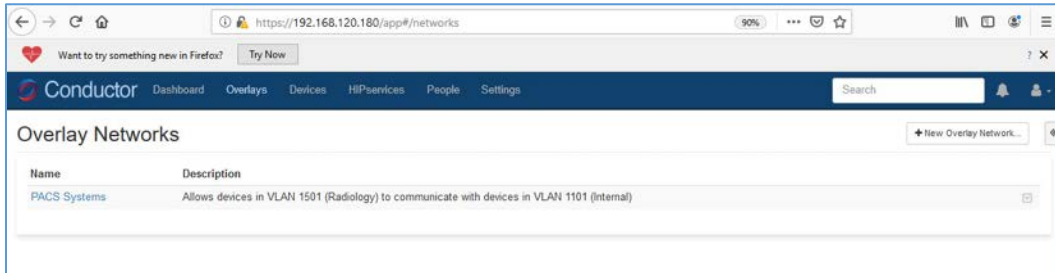
+

No static routes defined

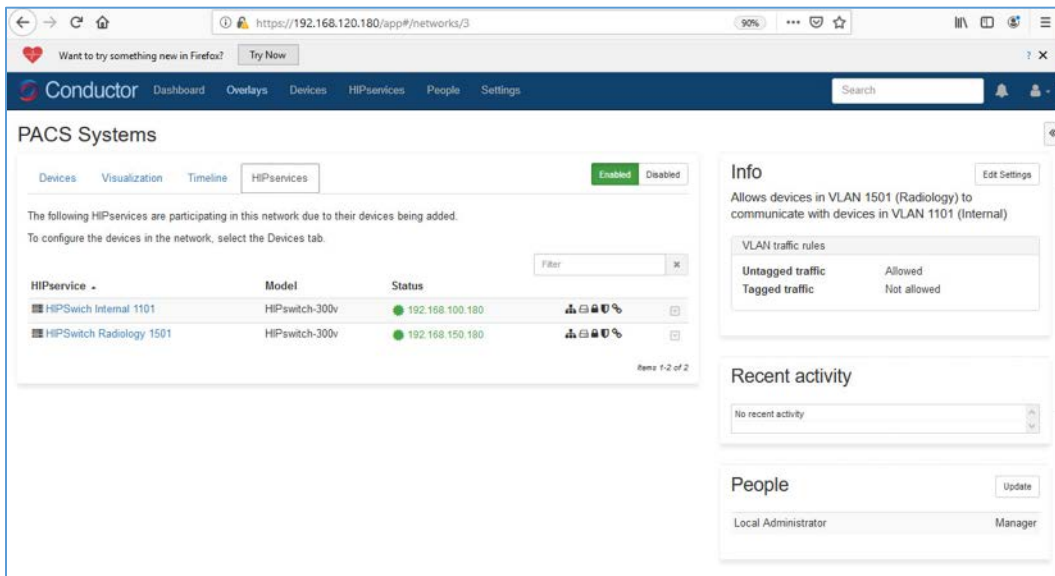
Configure

Cancel

5. An overlay is configured to support the micro-segmentation. Click the **Overlay** tab to open the following page and add a new overlay by clicking the **+ New Overlay Network...** The screenshot below shows a configured overlay called **PACS Systems**.



6. Two HIPswitches were installed to test for this project. These two HIPswitches are Model HIPswitch-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

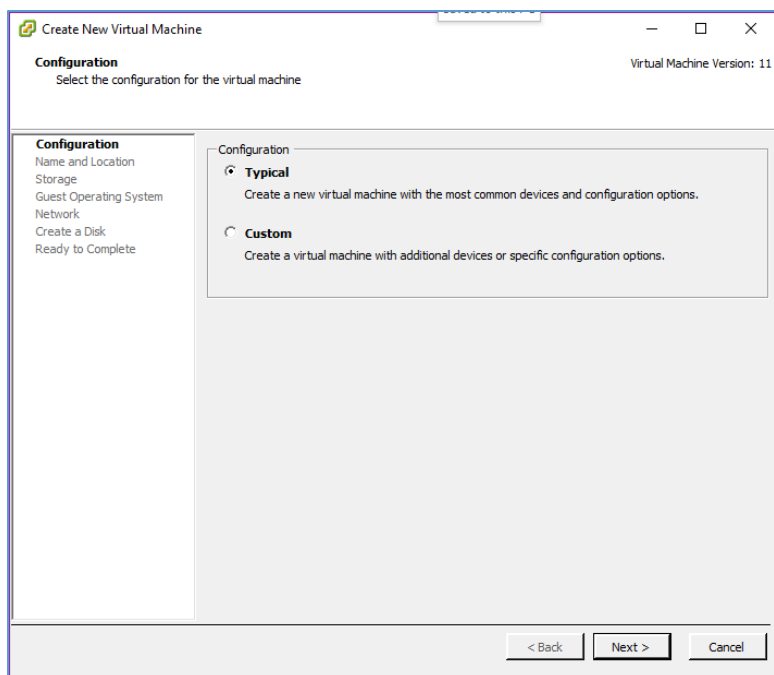
1. Visit <https://zingbox.com> and register for an account.
2. Log in to the Zingbox console and navigate to **Administration > My Inspectors > Download Inspector**.
3. Download either the .ova or the .iso file, depending on your environment's requirements.

System Requirements

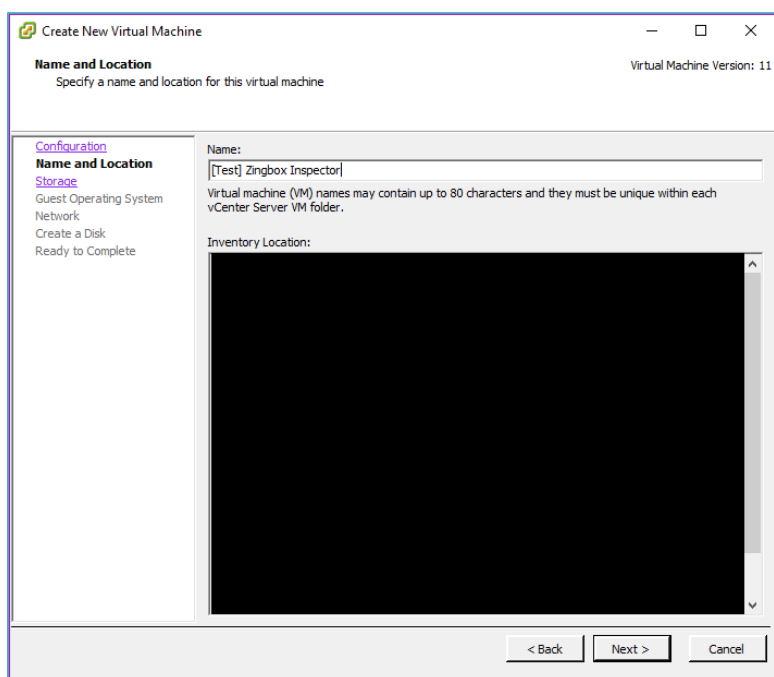
- **CPUs:** 4
- **Memory:** 8 GB RAM
- **Storage:** 256 GB (thin provision)
- **Operating System:** CentOS 7
- **Network Adapter 1:** VLAN 1101
- **Network Adapter 2:** Trunk Port

Zingbox Inspector Installation

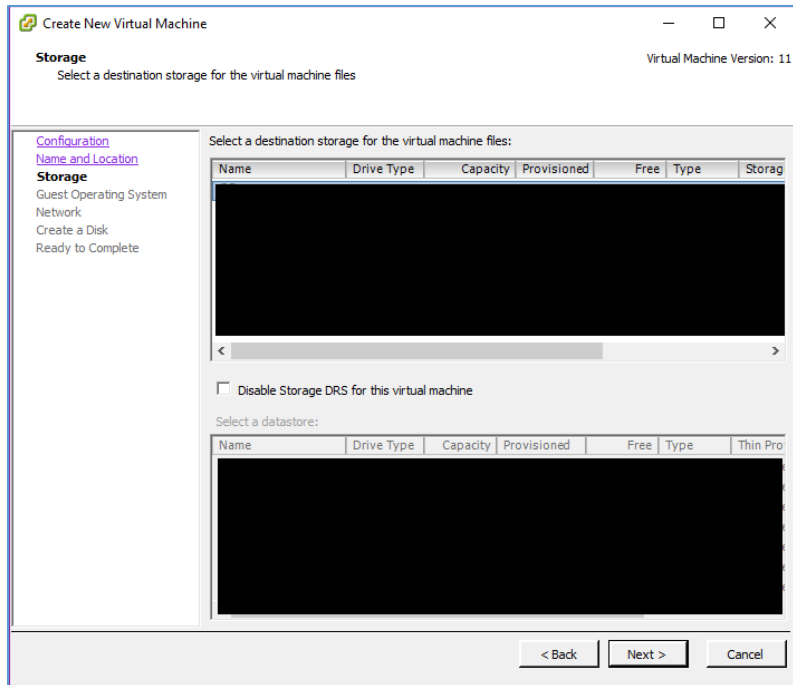
1. Create a new virtual machine, and under **configuration**, select **Typical**.
2. Click **Next >**.



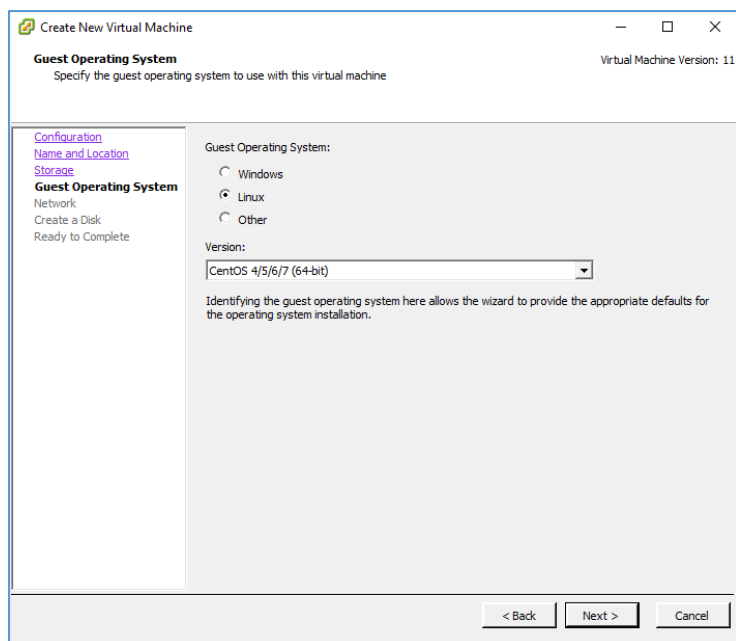
3. Create a **Name** for the virtual machine and assign it an **Inventory Location**.
4. Click **Next >**.



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



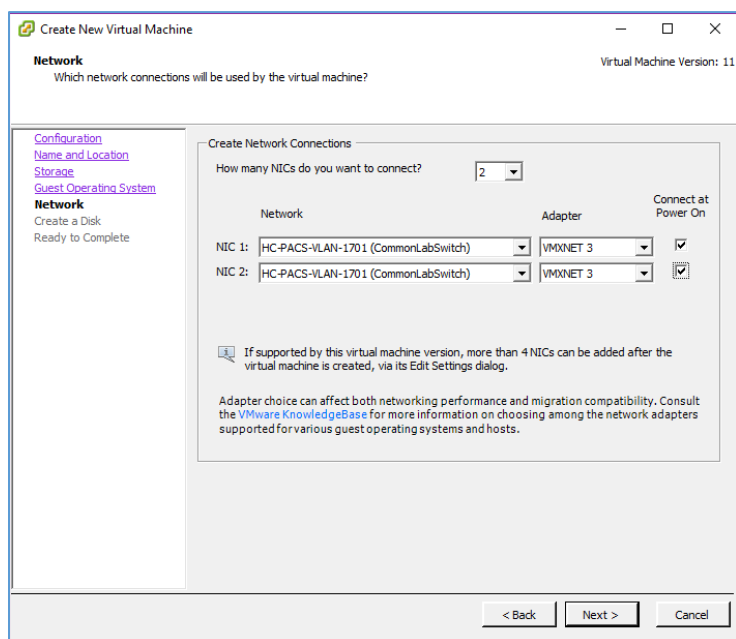
7. Check **Linux** and set the version to **CentOS 4/5/6/7 (64-bit)**.
8. Click **Next >**.



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

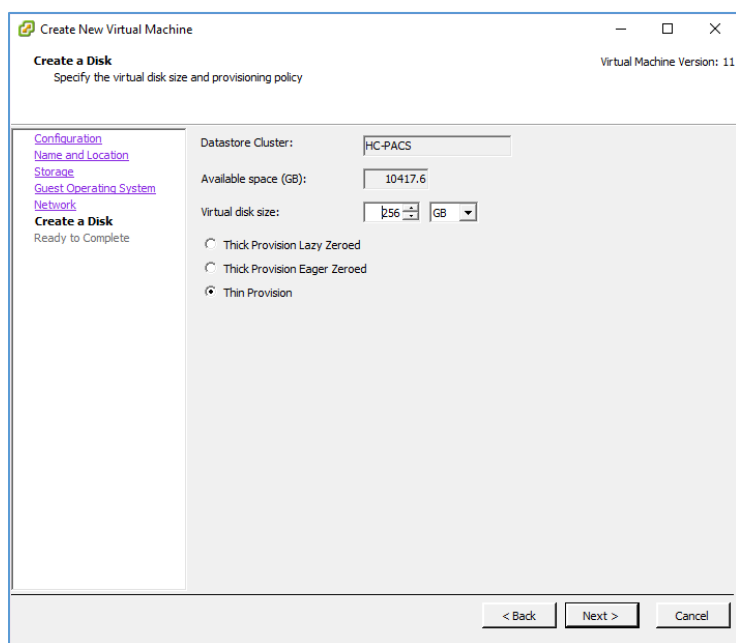
10. Check **Connect at Power On** for both NICs.

11. Click **Next >**.



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

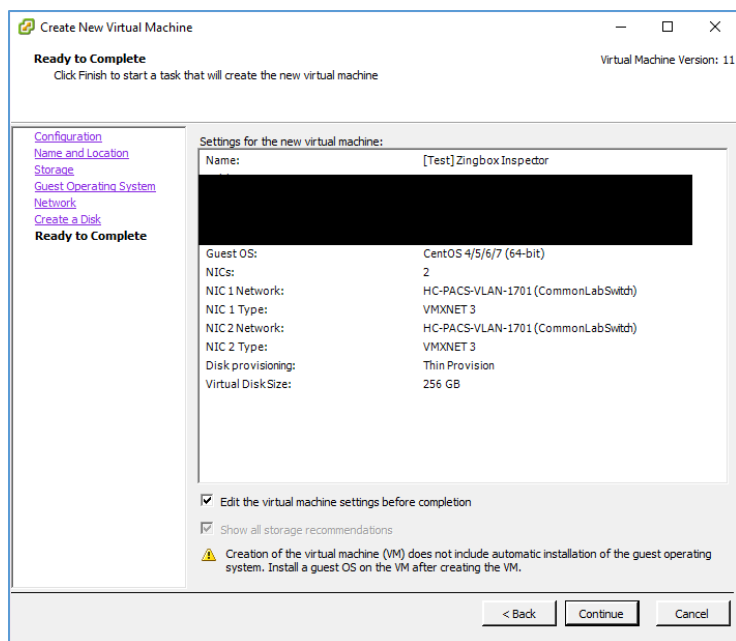
13. Click **Next >**.



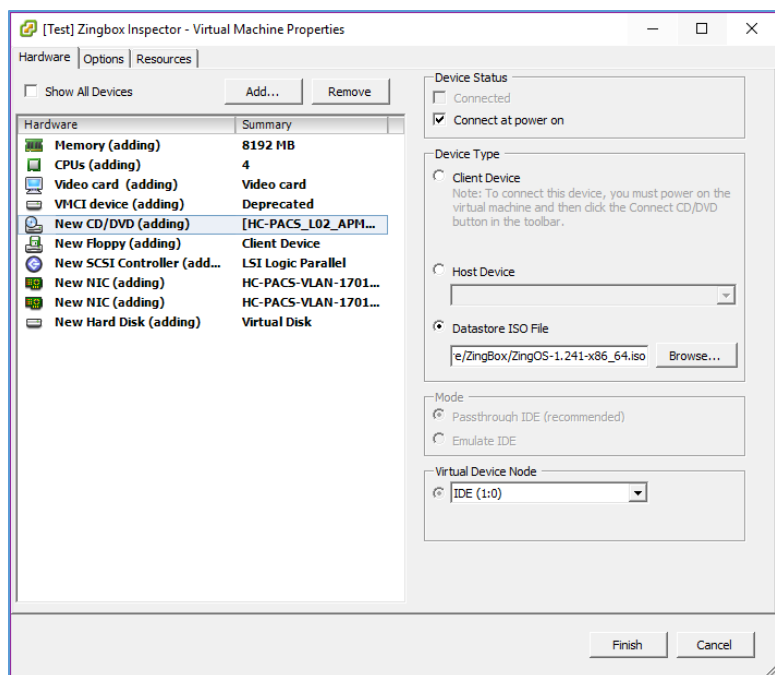
14. Verify that virtual machine settings are correct.

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

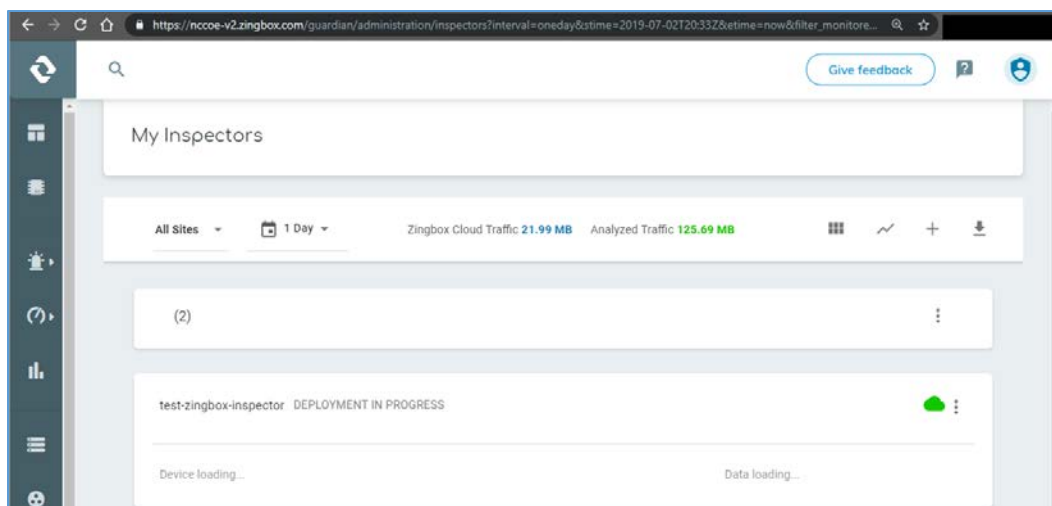
16. Click **Continue**.



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



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



2.7.5 Forescout CounterACT 8

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

System Requirements

- **CPUs:** 2
- **Memory:** 8 GB RAM
- **Storage:** 80 GB (thin provision)
- **Operating System:** Linux Kernel 3.10
- **Network Adapter 1:** VLAN 1201
- **Network Adapter 2:** Trunk Port

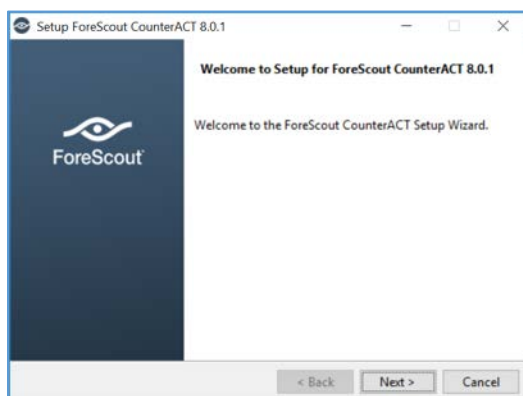
Forescout Appliance Installation

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

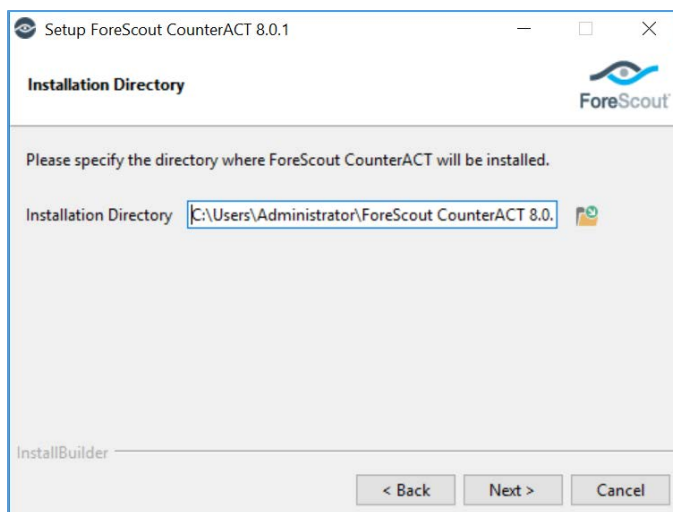
5. Select **option 1** to configure CounterACT.
6. Select **option 1** for standard installation.
7. Press **enter** to proceed.
8. Select **option 1** for CounterACT Appliance.
9. Select **option 1** for Per Appliance Licensing Mode.
10. Enter appliance **description**.
11. Give appliance a **password**.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

Forescout CounterACT Console Installation

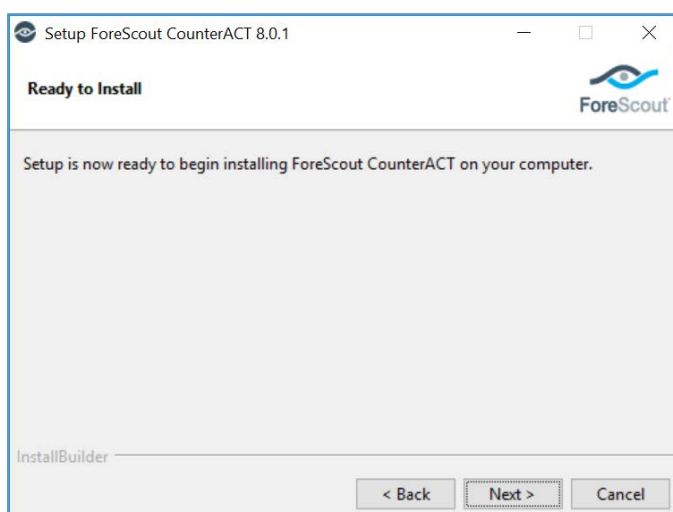
1. Run **Install_Management.exe**.
2. Click **Next >**.



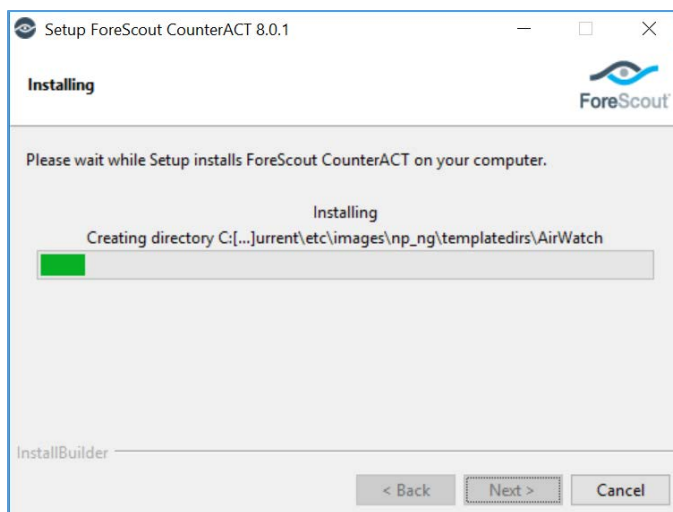
3. Verify **Installation Directory** as *C:\Users\Administrator\ForeScout CounterACT 8.0.1*; click **Next >**.



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



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



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



7. Launch **Forescout CounterACT Console**, and enter the information that follows, then click **Login**:
 - a. Enter **192.168.120.160** in the **IP/Name** text box.
 - b. Select **Password** as the **Login Method**.
 - c. Enter **Administrator** in the **User Name** text box.
 - d. Enter the password in the **Password** box.



Forescout CounterACT Configuration

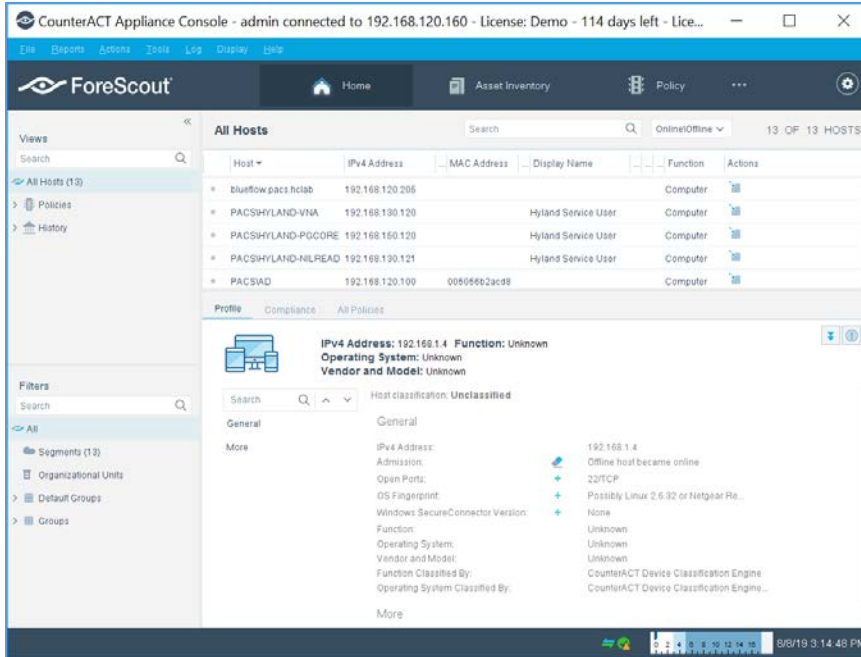
To use the full function offered by the Forescout CounterACT, proper network configuration is required, which may include the monitor and response interface assignments at the data center, the network VLAN and segmentation information, the IP address range that the CounterACT appliance will protect,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

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

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

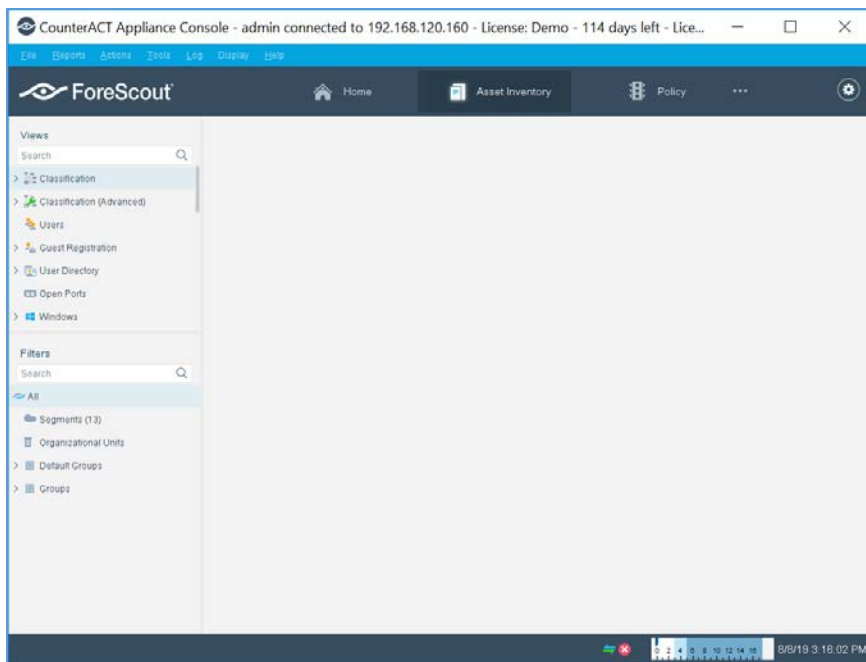


2. Provide the following information, and select **Login** to open the console:
 - a. Enter the IP address **192.168.120.160** in the **IP/Name** field.
 - b. In the **User Name** field, enter **admin**.
 - c. In the **Password** field, enter the admin password, which is defined during the installation.

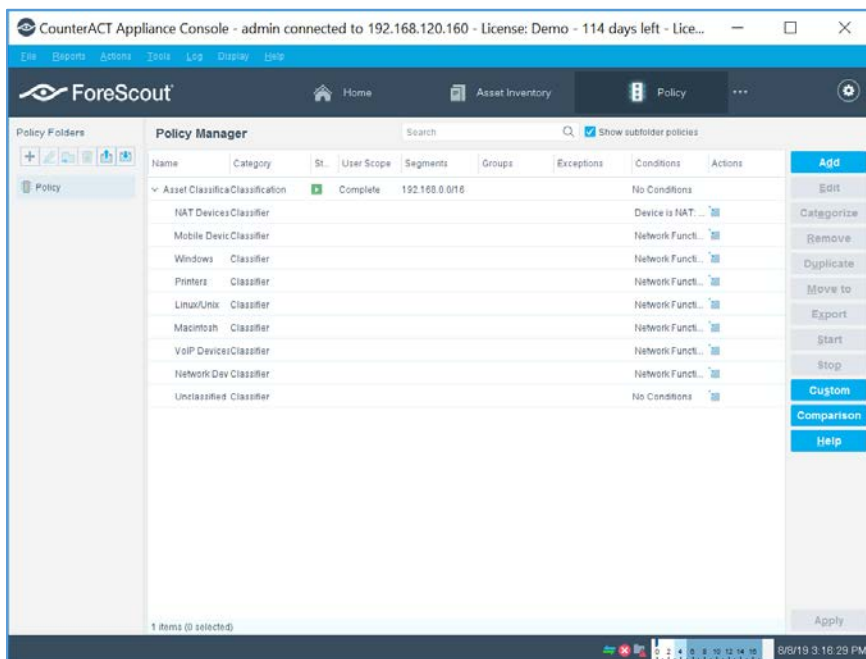


The console manager can be used to view, track, and analyze network activities detected by the appliance. It can also be used to define the threat protection, firewall, and other policies.

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



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



2.7.6 Symantec Endpoint Detection and Response (EDR)

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

System Requirements

- **CPUs:** 12
- **Memory:** 5 GB RAM
- **Storage:** 500 GB (thin provision)
- **Operating System:** CentOS 7
- **Network Adapter 1:** VLAN 1901
- **Network Adapter 2:** SPAN_PACS

Symantec EDR Installation

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

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

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

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

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

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

Symantec EDR

Create an Administrator Account

Login: admin

Password: [password]

Password Strength: Moderate

Confirm Password: [password]

Display Name: Display Name

User Email: User Email

☐ Receive email notification when incidents occur

Prev Finish

Symantec © 2018 Symantec Corporation Legal Notice License Agreement Privacy Policy

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

Symantec EDR Symantec EDR is Healthy Admin

Synapse

☐ Enable Symantec Email Security cloud Correlation

☐ Enable Roaming Correlation

☐ Enable Symantec Endpoint Cloud Correlation

☒ Enable Symantec Endpoint Protection Correlation

Symantec Endpoint Protection Manager (SEPM) Databases

Name	IP Address	Port	Enabled	Status
No data available.				

+ Add SEPM Database

Download Synapse Log Collector for SEPM Embedded DB

Endpoint Communication Channel, SEP Policies, and Endpoint Activity Recorder

SEPM Controller not configured

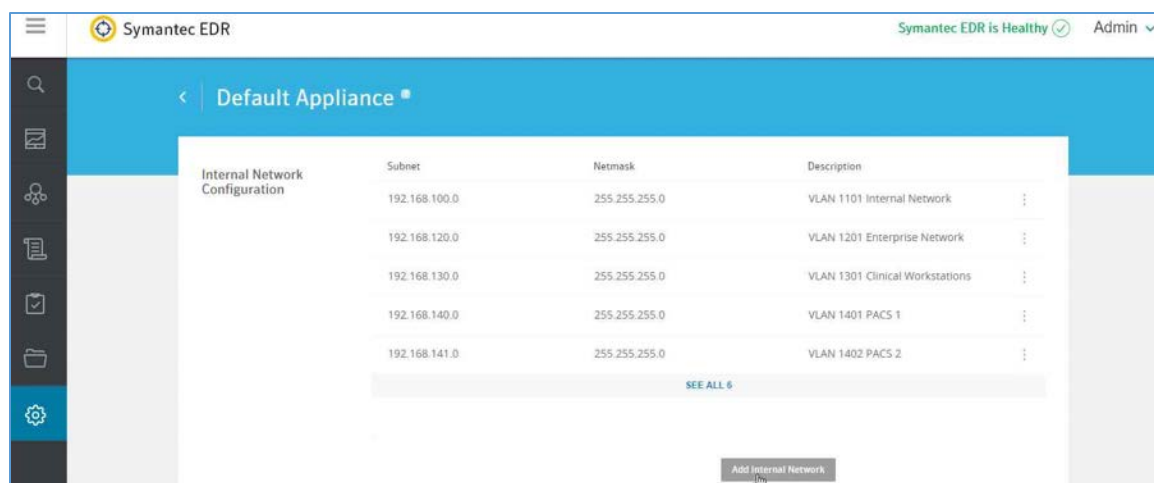
+ Configure SEPM Controller

☒ Enable ECC 2.0 (requires at least 1TB of hard disk space)

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** submenu.
12. Select **Edit Default Appliance**.
13. Select **Add Internal Network** to create and add a **Subnet**, **Netmask**, and **Description** for each internal network listed below. Make sure to save after entering the network details.

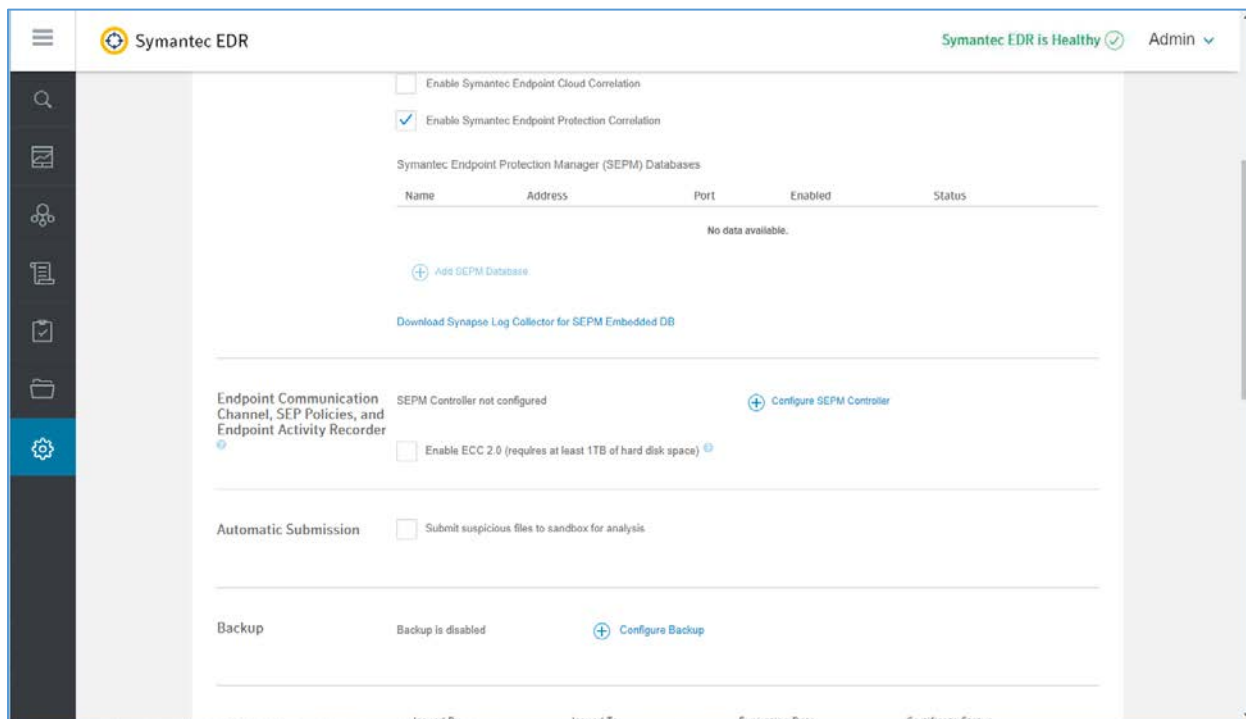


- **Subnet:** 192.168.100.0 **Netmask:** 255.255.255.0 **Description:** VLAN 1101
- **Subnet:** 192.168.120.0 **Netmask:** 255.255.255.0 **Description:** VLAN 1201
- **Subnet:** 192.168.130.0 **Netmask:** 255.255.255.0 **Description:** VLAN 1301
- **Subnet:** 192.168.140.0 **Netmask:** 255.255.255.0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

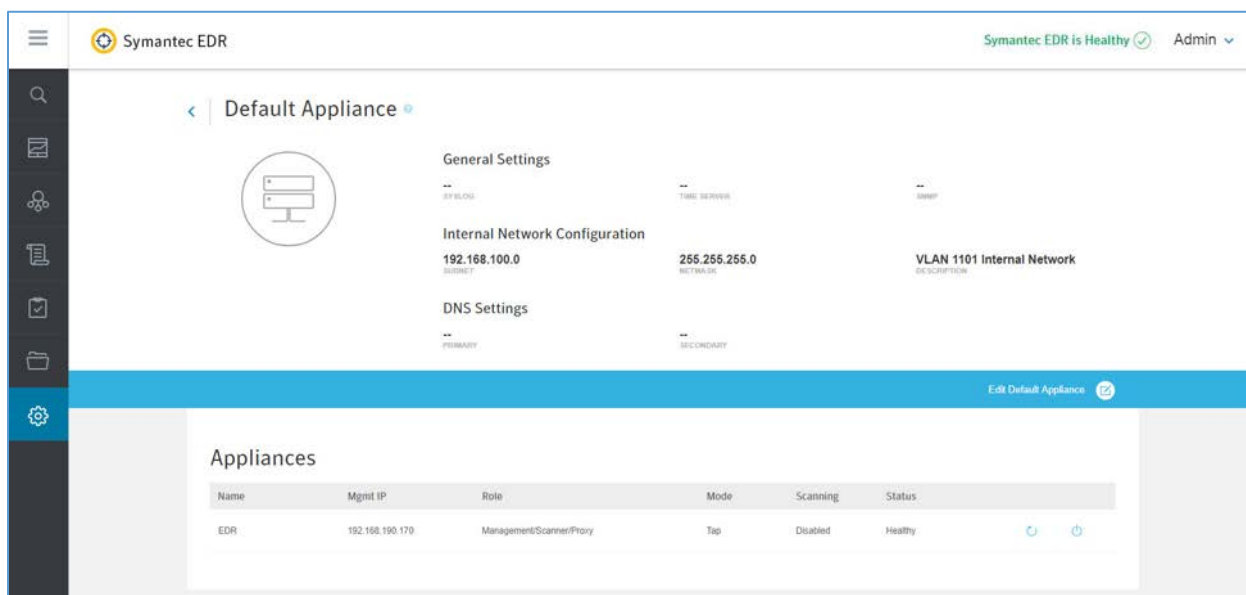
Subnet	Netmask	Description
192.168.100.0	255.255.255.0	VLAN 1101 Internal Network
192.168.120.0	255.255.255.0	VLAN 1201 Enterprise Network
192.168.130.0	255.255.255.0	VLAN 1301 Clinical Workstations
192.168.140.0	255.255.255.0	VLAN 1401 PACS 1
192.168.141.0	255.255.255.0	VLAN 1402 PACS 2
192.168.150.0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

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 on **Scanning** under the **Network Interface Settings**.

Symantec EDR and SEP Correlation

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

The screenshot shows a Windows-style dialog box titled "Log Collector for SEPM embedded database configuration utility". It contains two main sections: "Log Collector service settings" and "SEPM embedded database configuration".

Log Collector service settings:

- Service Hostname (optional): An empty text input field.
- Service IP address: A dropdown menu showing "192.168.190.172".
- Service port: A text input field containing "8081".
- Log Collector connection password: A password input field with 10 dots.
- Confirm connection password: A password input field with 10 dots.

SEPM embedded database configuration:

- Password: A password input field with 10 dots.
- Below the password field is a button labeled "Test Database Connection".

At the bottom of the dialog, there is a "Configuration Status:" label followed by a greyed-out status bar. Below the status bar are three buttons: "Confirm", "Close", and "Help".

2.8 Endpoint Protection and Security

Endpoint protection and security measures are deployed to workstation end points to further emphasize defense in depth. The build includes an agent-based endpoint protection solution that is centrally managed within the enterprise. Endpoint protection provides anti-malware features with centralized servers assuring that managed assets receive regular updates.

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

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

System Requirements

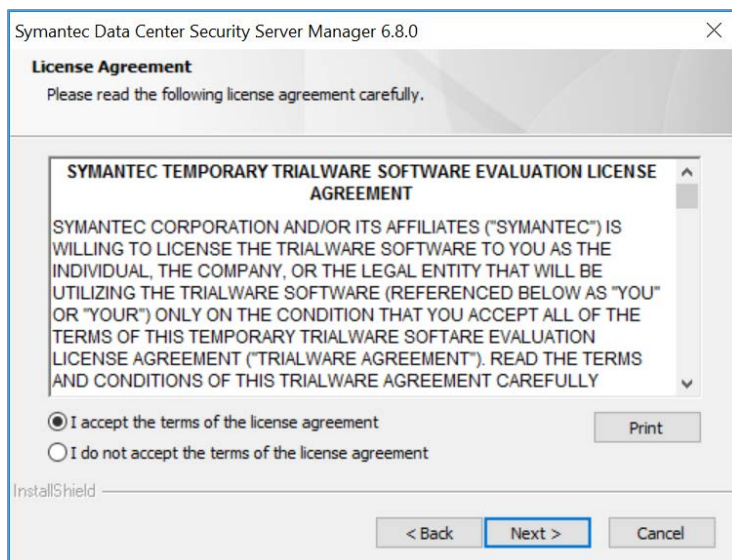
- **CPUs:** 4
- **Memory:** 8 GB RAM
- **Storage:** 120 GB (thin provision)
- **Operating System:** Microsoft Windows Server 2016 Datacenter
- **Network Adapter:** VLAN 1901

Symantec Data Center Security Installation

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

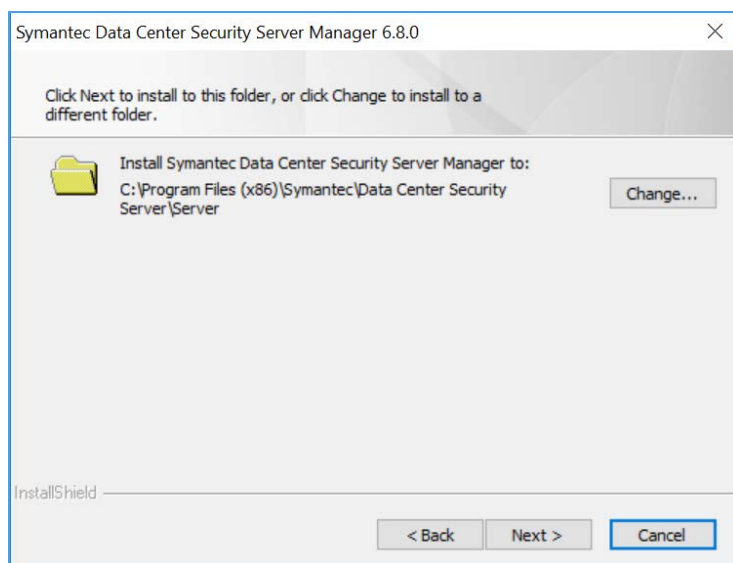


3. Check **I accept the terms of the license agreement**.
4. Click **Next >**.

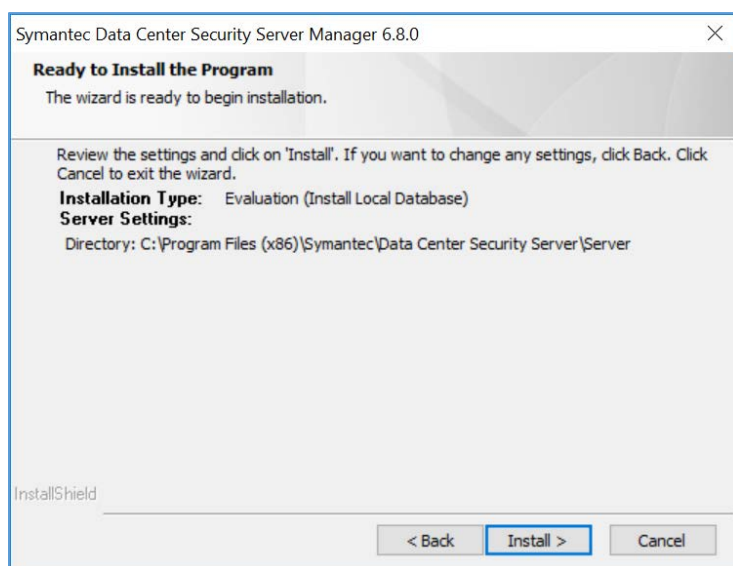


5. Verify installation location.

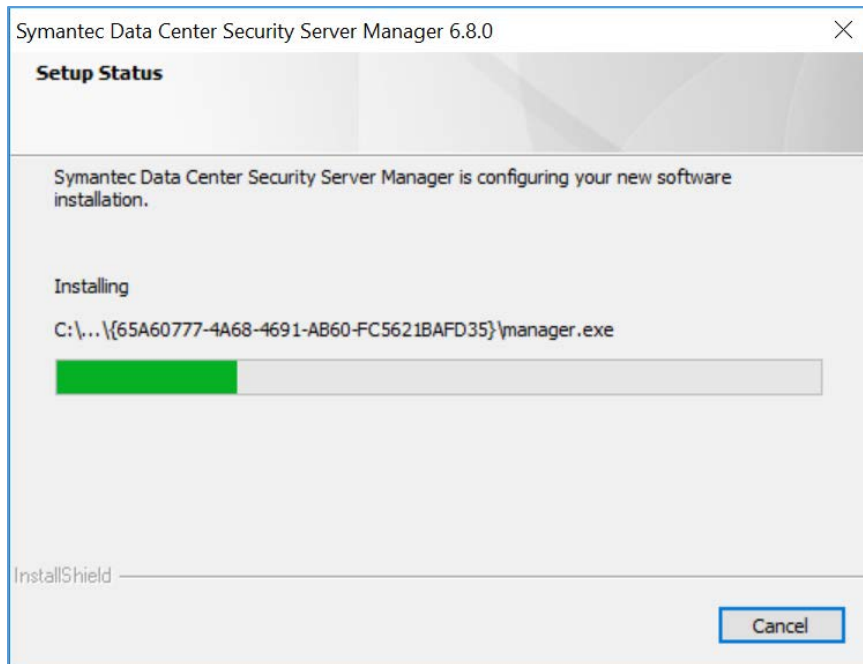
6. Click **Next >**.



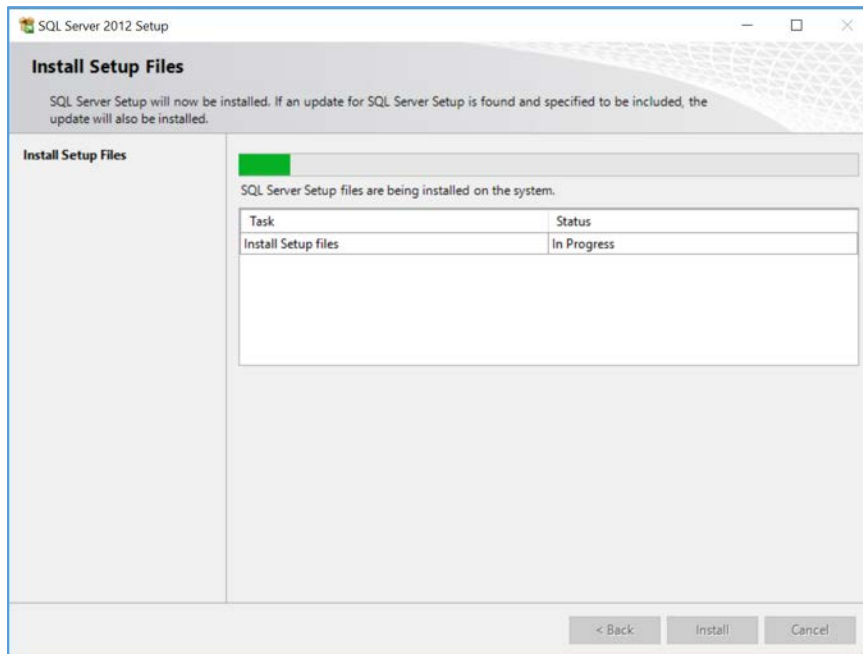
7. Review settings.
8. Click **Install >**.



9. Wait for the setup and installation process to complete.



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



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

- **Agent port: 443**

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

The screenshot shows the 'Tomcat XML Configuration' window of the 'DCS:SA Configuration Wizard'. It is divided into two main sections: 'General Settings' and 'Tomcat Connector Attributes'. In the 'General Settings' section, there are three input fields: 'Agent port' with the value '443', 'Bridge port' with the value '2443', and 'Console port' with the value '4443'. In the 'Tomcat Connector Attributes' section, there are two input fields: 'Web server administration port' with the value '8081' and 'Web server shutdown port' with the value '8006'. At the bottom right of the window, there are 'Back' and 'Next' buttons.

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

The screenshot shows the 'Symantec Cloud Workload Protection Bridge' window of the 'DCS:SA Configuration Wizard'. It contains a text box stating: 'This bridge will enable Symantec Cloud Workload Protection customers to manage DCS agents.' Below this text is a checkbox labeled 'Enable CWP Bridge', which is currently unchecked. At the bottom right of the window, there are 'Back' and 'Next' buttons.

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

DCS:SA Configuration Wizard

Server Settings

Certificates

☒ Agent Certificate

☒ Server Certificate

This Server's Network Address Settings

☐ Use FQDN Hostname for Certificate

FQDN Hostname: WIN-RUQDO7KL8A7

Static IP Address: 192.168.120.207

JVM Settings

Java Heap Size (MB): 6144

Back Next

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

15. Click **Next**.

DCS:SA Configuration Wizard

Create Database

Connection Parameters

Hostname: 127.0.0.1

☒ Database Instance: SCSP

☐ Database Port: 1433

'sa' privileged User: sa

Password *: [masked]

Confirm Password *: [masked]

Back Next

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

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

18. Click **Next**.

DCS:SA Configuration Wizard

Register with Unified Management Console

UMC Details

Hostname: 192.168.120.207

Port: 8443

User Name: dcsadmin

Password: *

Confirm Password: *

☐ Migrate UMC Data

Back Next

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

DCS:SA Configuration Wizard

Summary Page

Review the settings and click on 'Configure'. If you want to change any settings, click Back. Click Cancel to exit the wizard

Installation Type: Evaluation (Install Local Database)

Server Settings

Directory: C:\Program Files (x86)\Symantec\Data Center Security Server\Server

Ports: Agent: 443, Console: 4443, Web Admin: 8081, Web Shutdown: 8006

Database Settings

Host: 127.0.0.1

Instance: SCSP

Database Name: SCSPDB

JVM Settings

Heap Size (MB): 6144

UMC Registration Settings

UMC Server: Hostname=192.168.120.207, Port=8443, Username=dcsadmin

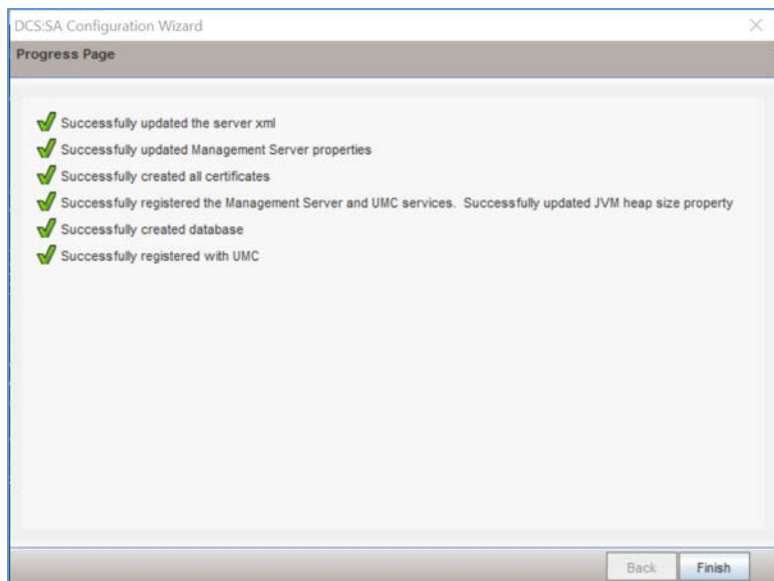
Product Server: Hostname=WIN-RUQD07KL8A7, IP Address=192.168.120.207, Port=4443

Server Cert Attributes: exif.SAN=DNS=WIN-RUQD07KL8A7,IP=192.168.120.207.1

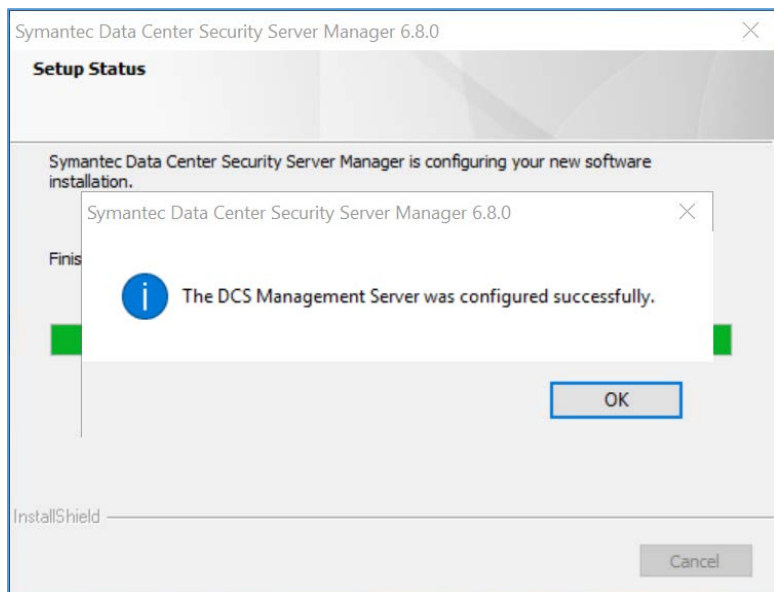
Back Configure

20. Wait for the configuration process to complete.

21. Click **Finish**.



22. Wait for the installation to complete and click **OK**.



Symantec Datacenter Security Windows Agent Install

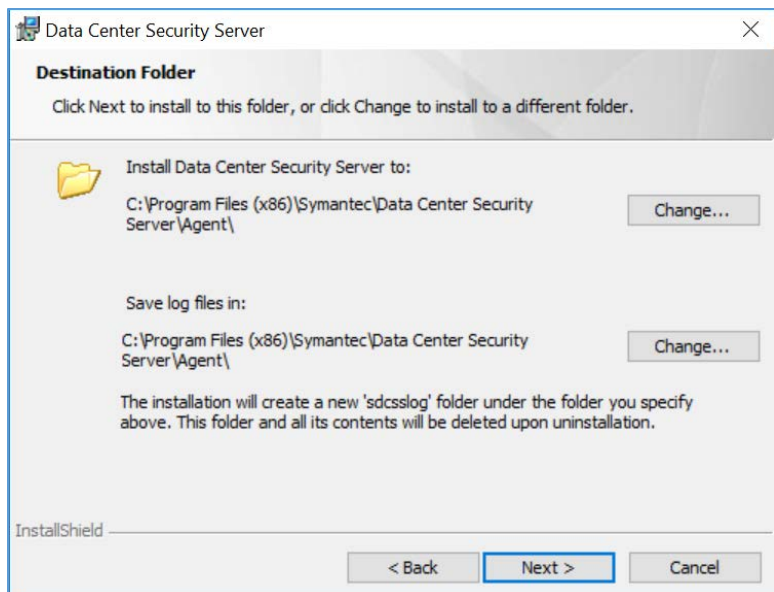
1. Run **agent.exe**.
2. Click **Next >**.



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

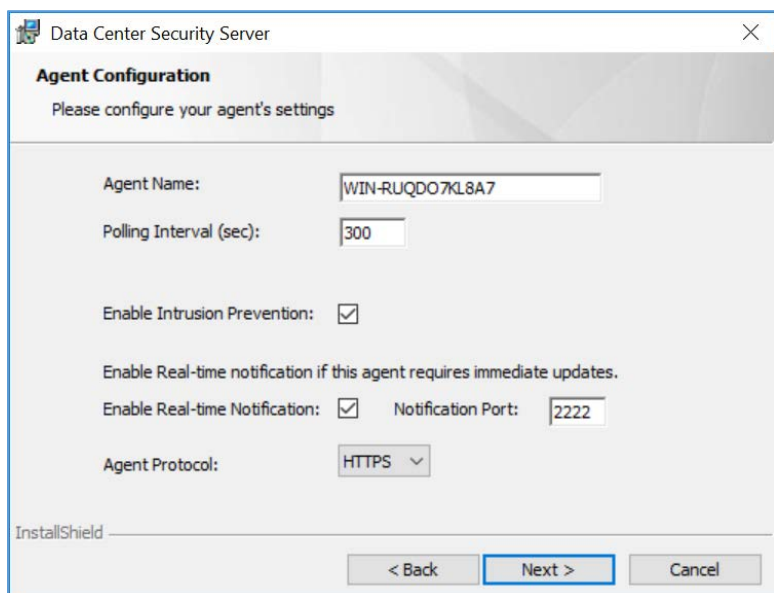


5. Verify the installation and log files directories.
6. Click **Next >**.



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

- **Agent Name:** WIN-RUQDO7KL8A
- **Polling Interval (sec):** 300
- Check **Enable Intrusion Prevention**.
- **Notification Port:** 2222
- **Agent Protocol:** HTTPS

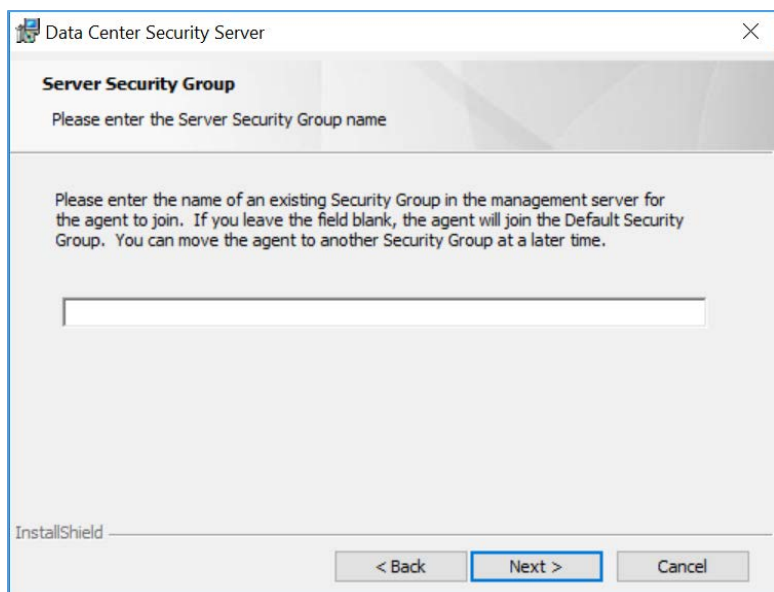


8. Provide the information below, and click **Next**:

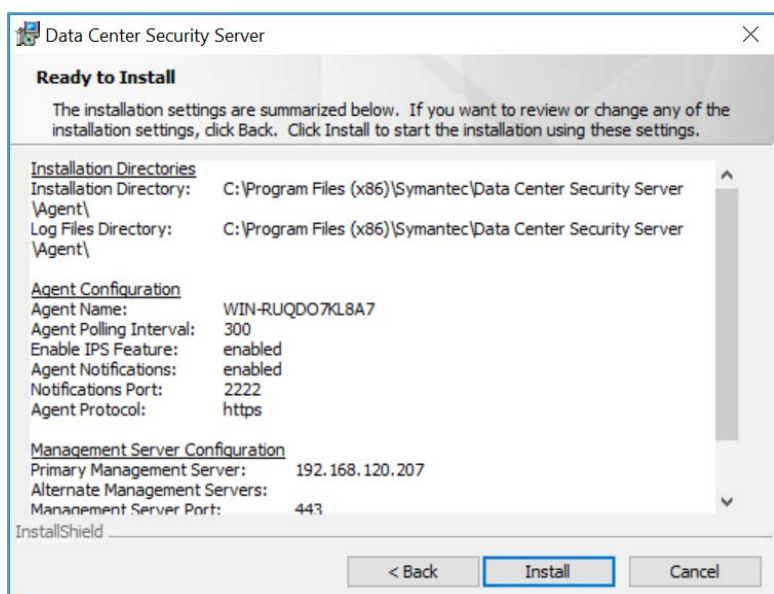
- **Primary Management Server:** 192.168.120.207
- **Agent Port:** 443
- **Alternate Management Servers:**
- **Management Server Certificate:** *C:\User\Administrator\Desktop\agent-cert.ssh*

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

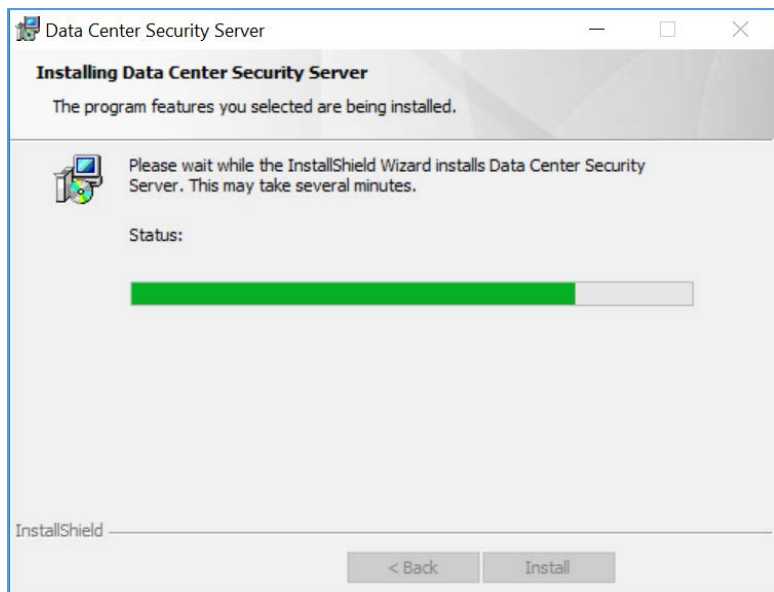
10. Click **Next >**.



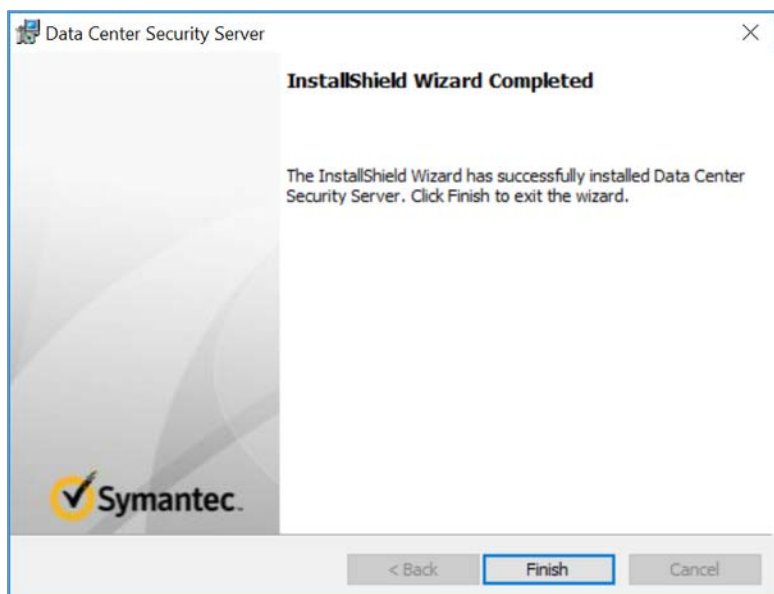
11. Verify installation and configuration settings and click **Install**.



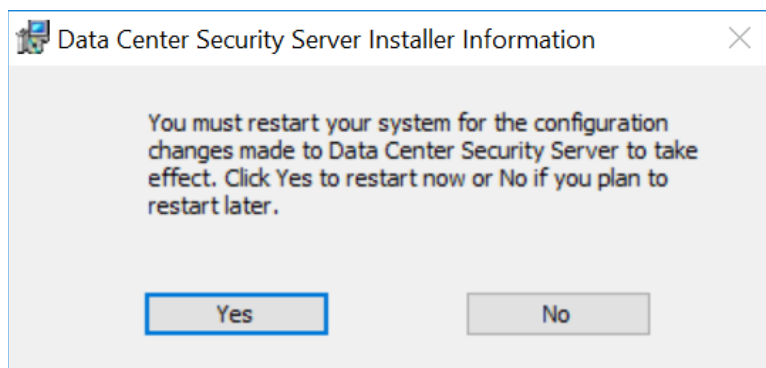
12. Wait for the installation process to complete.



13. Click **Finish**.



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



2.8.2 Symantec Endpoint Protection

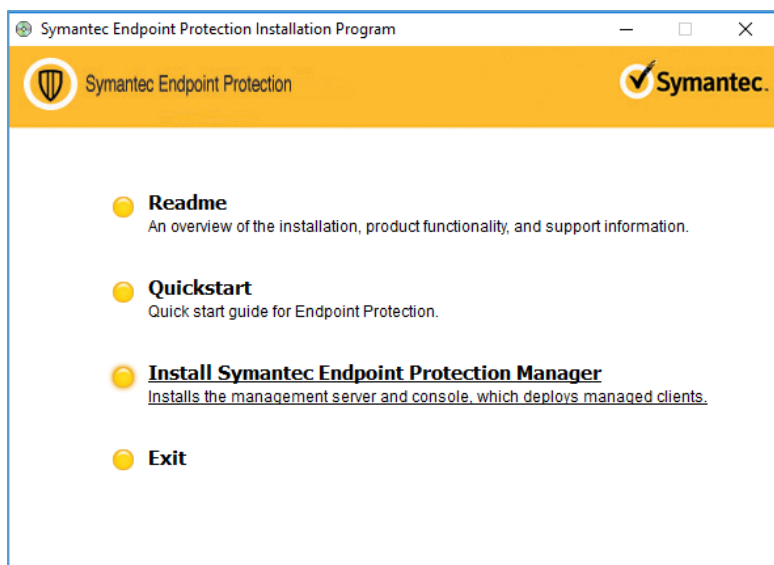
Symantec Endpoint Protection is an agent-based security solution that provides anti-virus, intrusion prevention, application allow-listing, and other capabilities. For this project, Symantec SEP protects endpoints from malicious software and integrates with Symantec Endpoint Detection and Response to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

System Requirements

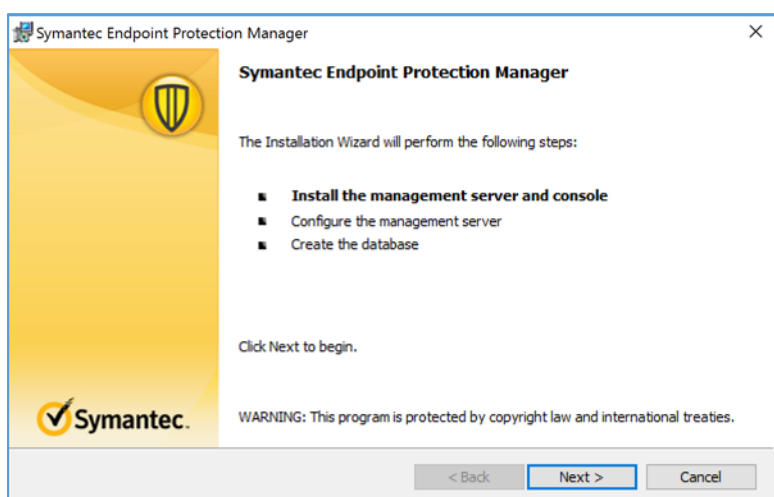
- **CPUs:** 4
- **Memory:** 8GB RAM
- **Storage:** 240 GB (thin provision)
- **Operating System:** Microsoft Windows Server 2016
- **Network Adapter:** VLAN 1901

Symantec Endpoint Protection Manager Installation

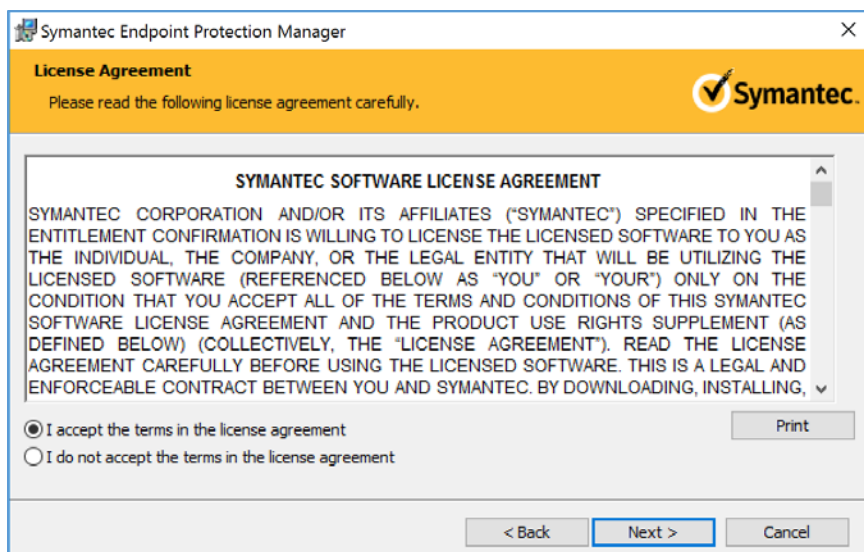
1. Launch *Symantec_Endpoint_Protection_14.2.0.MP1_Part1_Trialware_EN.exe* file.
2. Select the **Install Symantec Protection Endpoint Manager** option.



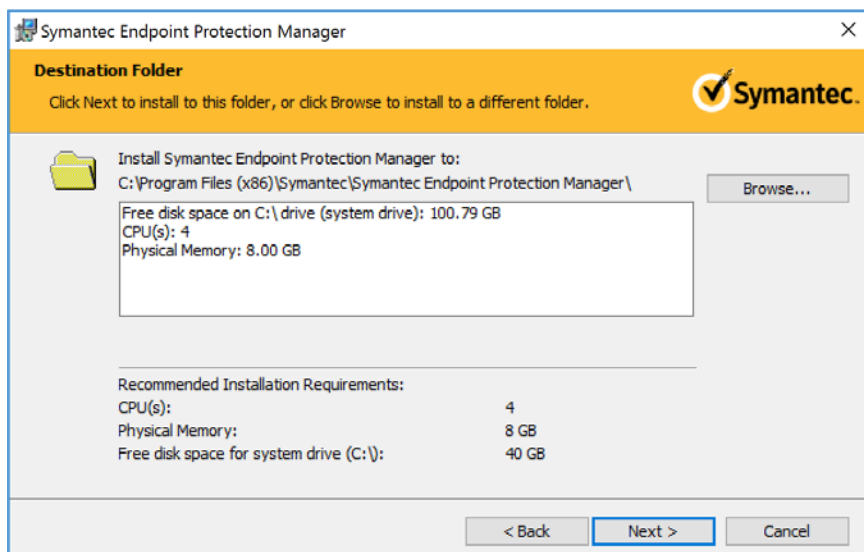
3. Proceed through the installation wizard by clicking **Next >**.



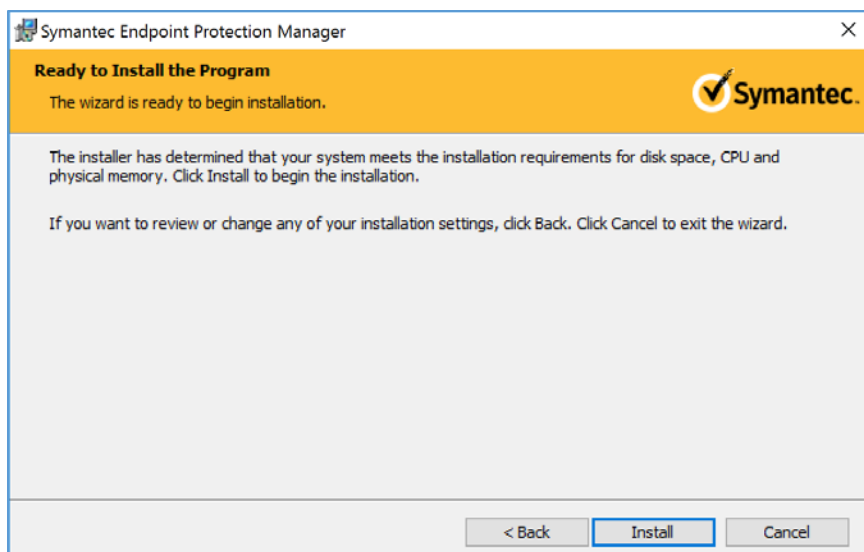
4. Check **I accept the terms in the license agreement**.
5. Click **Next >**.



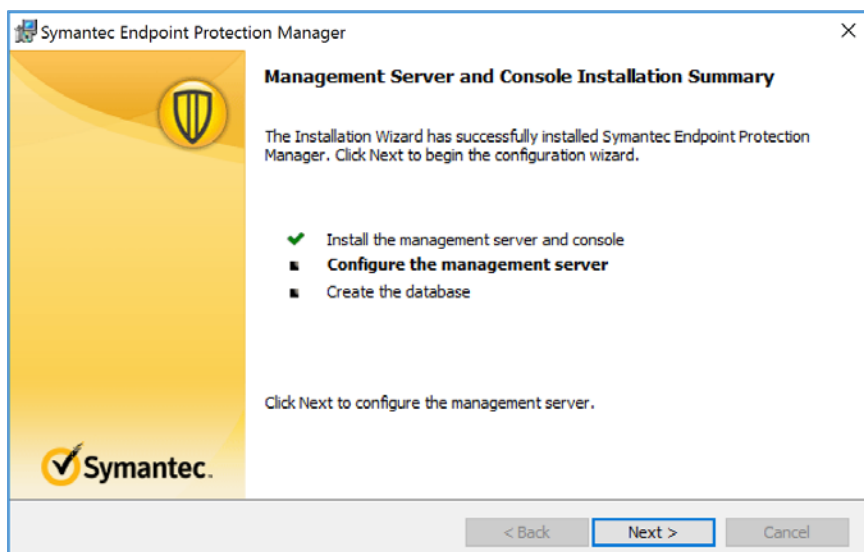
6. Select the location you want to install Symantec Endpoint Protection Manager and click **Next >**. Keep the default location of *C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager*.



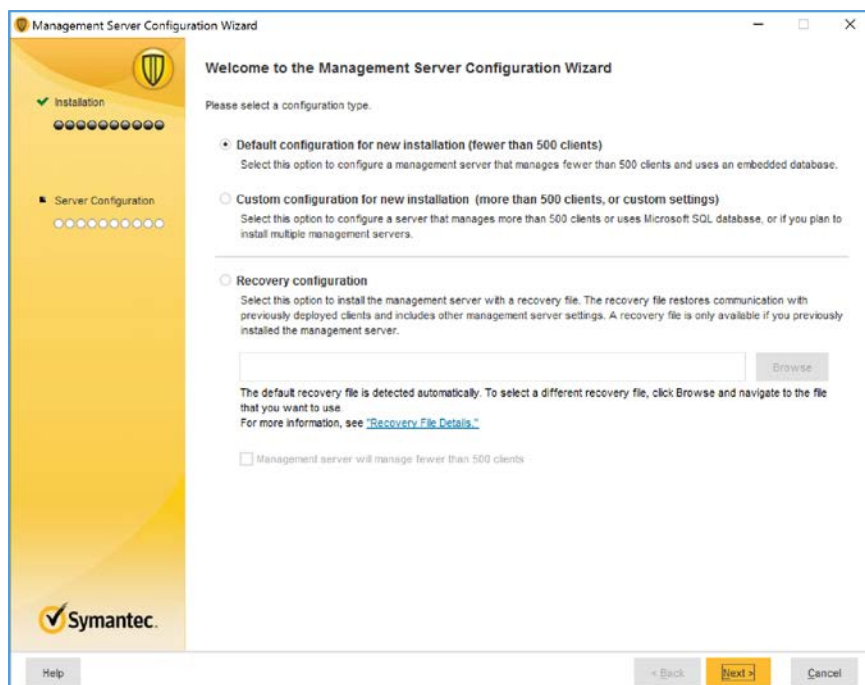
7. Select **Install**.



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

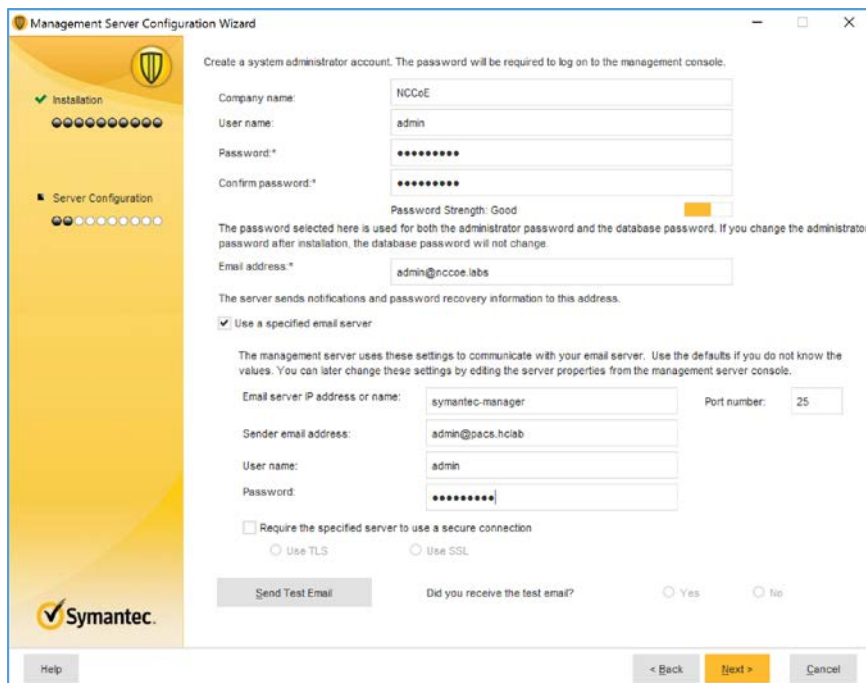


9. Select **Default configuration for new installation...**; then click **Next >**.



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

- **Company Name:** *****
- **User name:** *****
- **Password:** *****
- **Confirm password:** *****
- **Email address:** *****



Management Server Configuration Wizard

Create a system administrator account. The password will be required to log on to the management console.

Company name: NCCoE
 User name: admin
 Password: *****
 Confirm password: *****

Password Strength: Good

The password selected here is used for both the administrator password and the database password. If you change the administrator password after installation, the database password will not change.

Email address: admin@nccoe.labs

The server sends notifications and password recovery information to this address.

☒ Use a specified email server

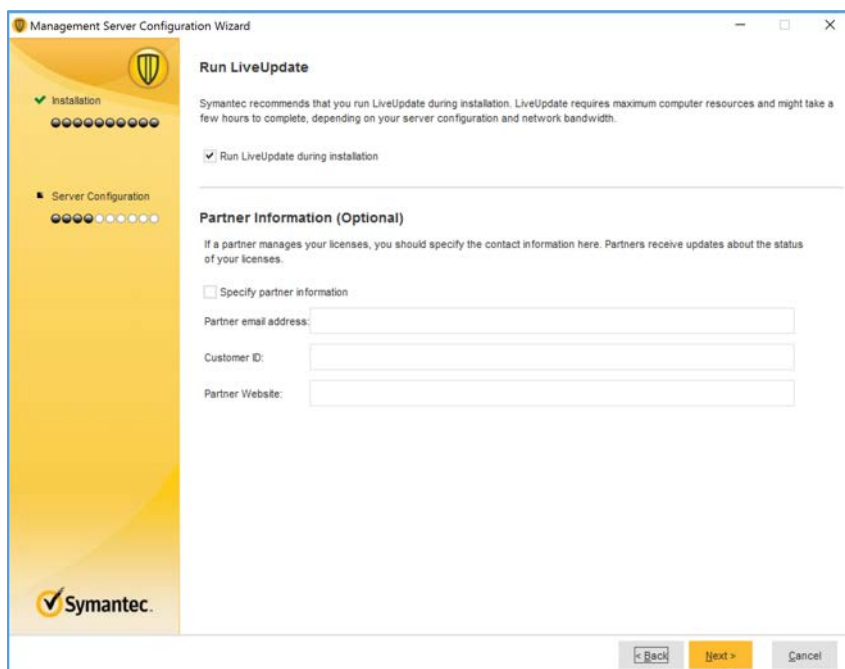
The management server uses these settings to communicate with your email server. Use the defaults if you do not know the values. You can later change these settings by editing the server properties from the management server console.

Email server IP address or name: symantec-manager Port number: 25
 Sender email address: admin@pacs.hclab
 User name: admin
 Password: *****

☐ Require the specified server to use a secure connection
☐ Use TLS ☐ Use SSL

Did you receive the test email? ☐ Yes ☐ No

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



Management Server Configuration Wizard

Run LiveUpdate

Symantec recommends that you run LiveUpdate during installation. LiveUpdate requires maximum computer resources and might take a few hours to complete, depending on your server configuration and network bandwidth.

☒ Run LiveUpdate during installation

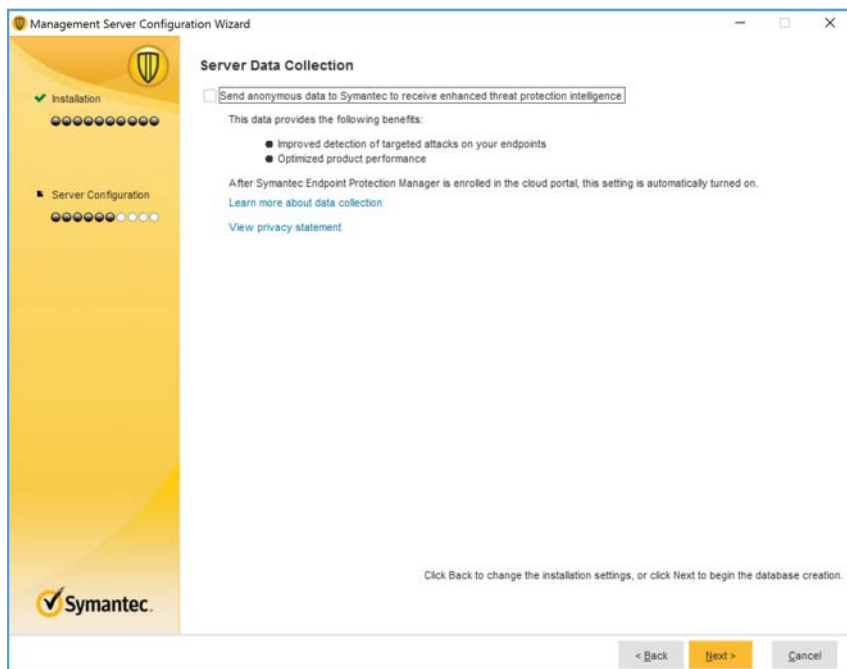
Partner Information (Optional)

If a partner manages your licenses, you should specify the contact information here. Partners receive updates about the status of your licenses.

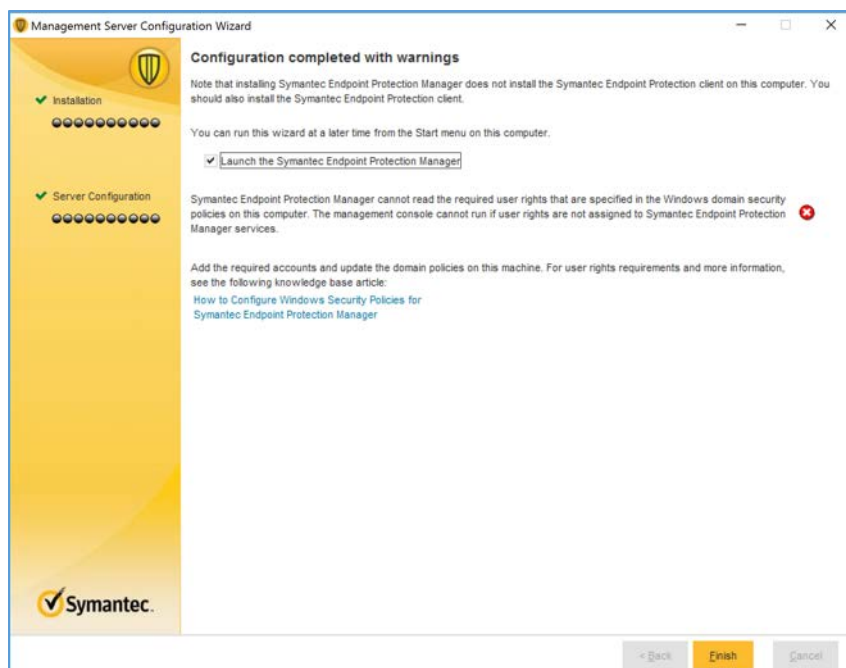
☐ Specify partner information

Partner email address:
 Customer ID:
 Partner Website:

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

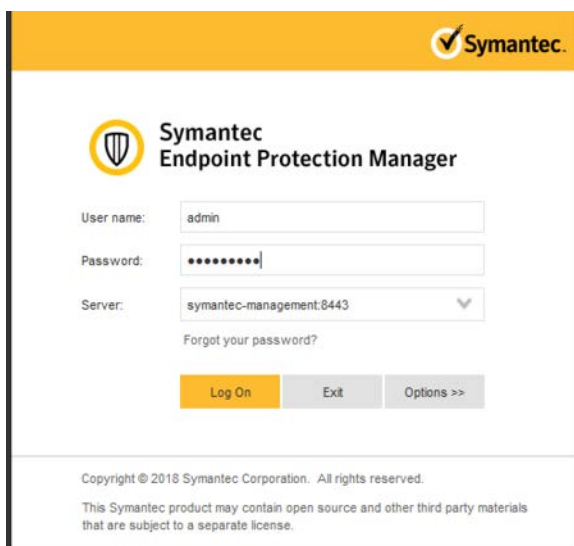


13. After installation is completed, check **Launch the Symantec Endpoint Protection Manager** to configure your hosts; click **Finish**.

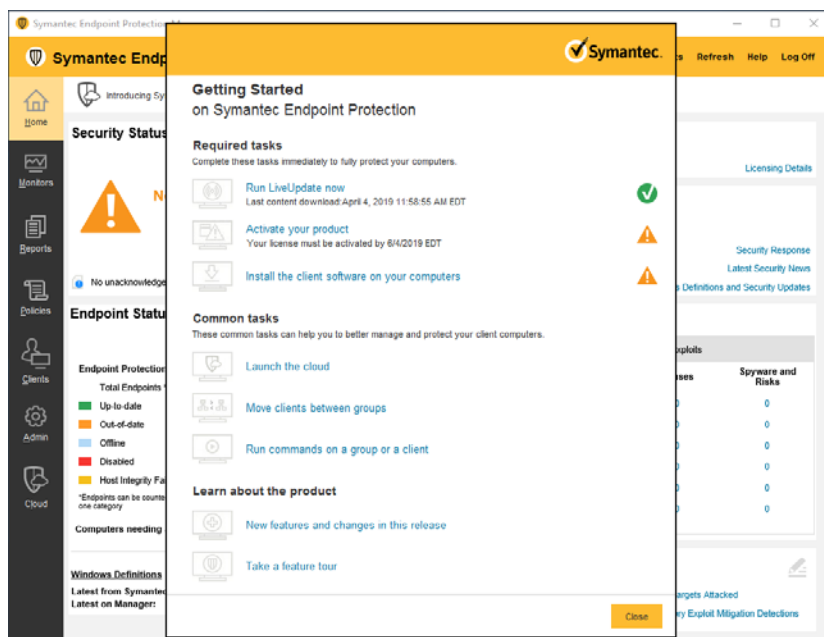


Symantec Endpoint Protection Host Windows Installation

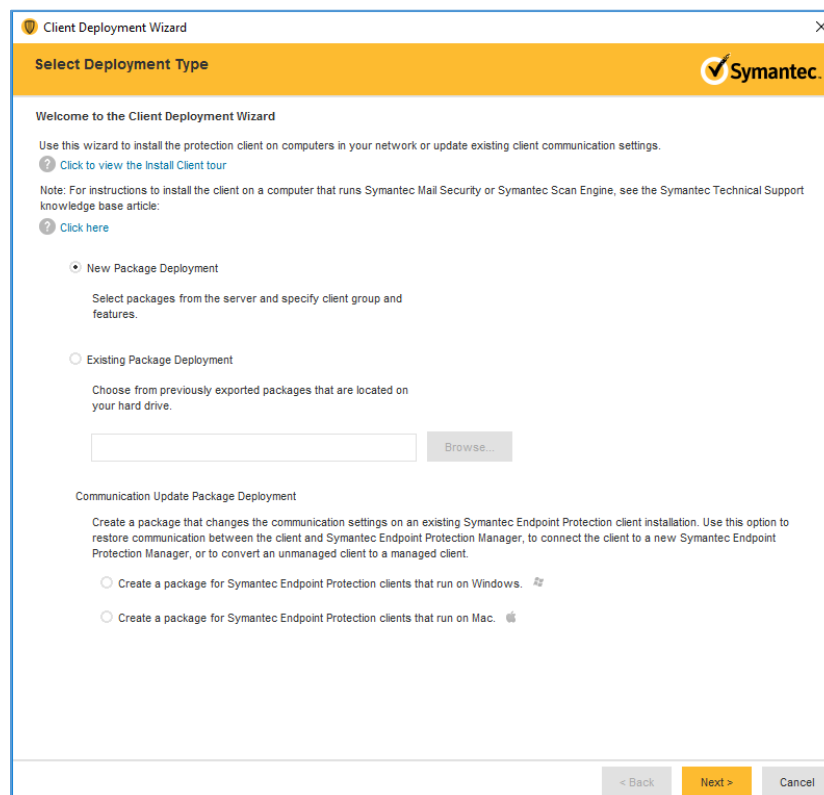
1. Launch the **Symantec Endpoint Protection Manager**, and log in as the **admin**.



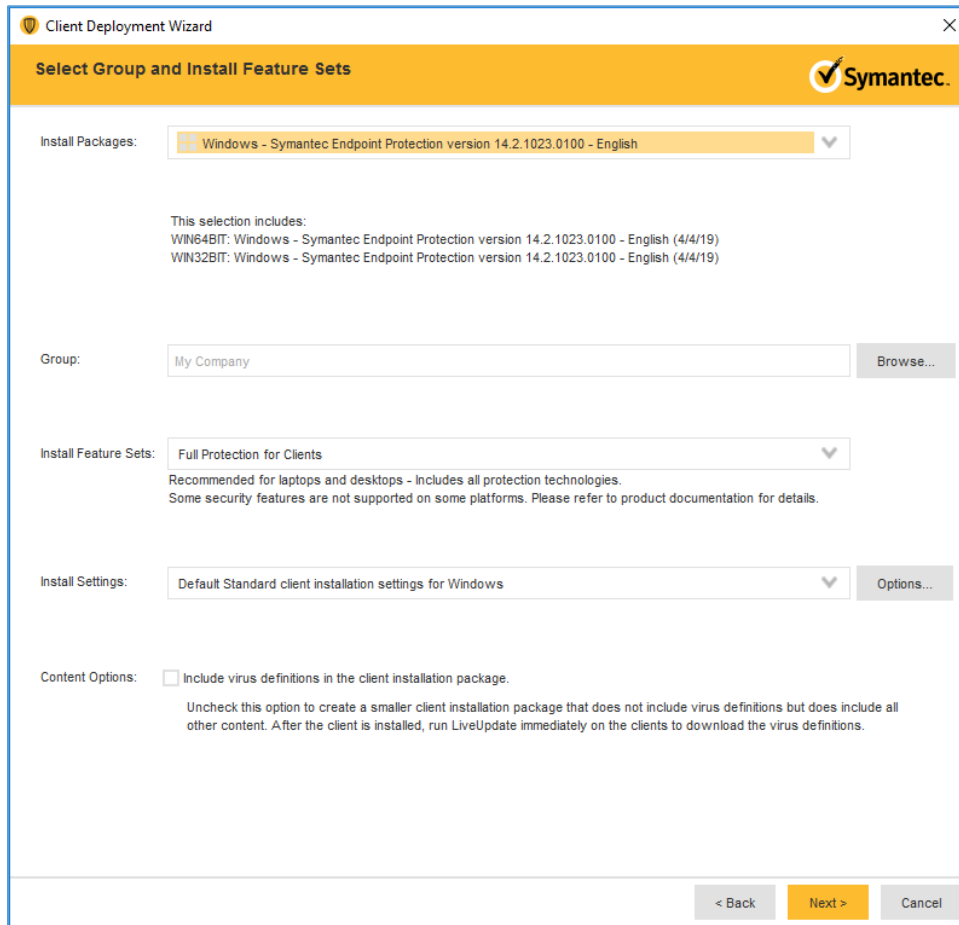
2. Select **Install the client software on your computers** from the **Getting Started** screen.



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

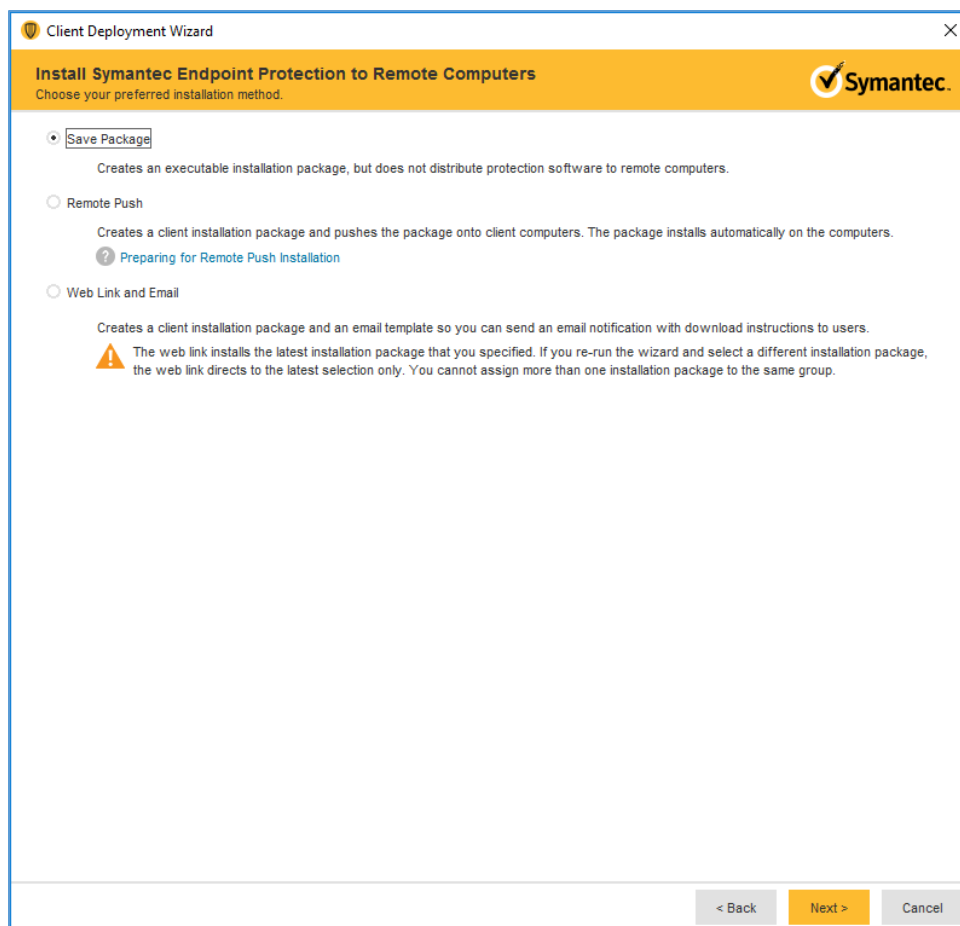


4. Confirm the settings for the Install Packages: **Windows—Symantec Endpoint Protection version 14.2.1023.0100—English**, Group: **My Company**, Install Feature Sets: **Full Protection for Clients**, Install Settings: **Default Standard client installation settings for Windows**. Click **Next >**.

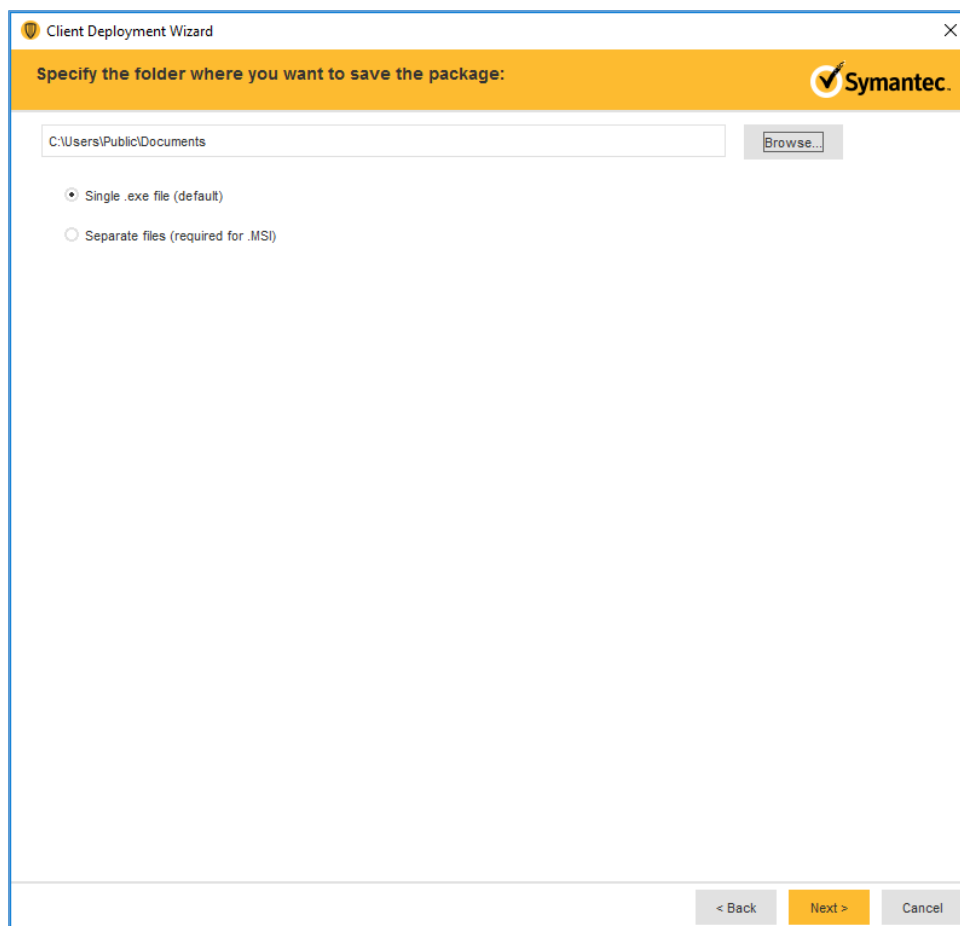


The screenshot shows the 'Client Deployment Wizard' window with the title bar 'Client Deployment Wizard' and a close button. The main header is 'Select Group and Install Feature Sets' with the Symantec logo on the right. The 'Install Packages:' section shows a dropdown menu with 'Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English' selected. Below this, it states 'This selection includes:' followed by 'WIN64BIT: Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English (4/4/19)' and 'WIN32BIT: Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English (4/4/19)'. The 'Group:' section has a text box with 'My Company' and a 'Browse...' button. The 'Install Feature Sets:' section has a dropdown menu with 'Full Protection for Clients' selected, with a note: 'Recommended for laptops and desktops - Includes all protection technologies. Some security features are not supported on some platforms. Please refer to product documentation for details.' The 'Install Settings:' section has a dropdown menu with 'Default Standard client installation settings for Windows' selected and an 'Options...' button. The 'Content Options:' section has a checkbox labeled 'Include virus definitions in the client installation package.' which is unchecked, with a note: 'Uncheck this option to create a smaller client installation package that does not include virus definitions but does include all other content. After the client is installed, run LiveUpdate immediately on the clients to download the virus definitions.' At the bottom, there are three buttons: '< Back', 'Next >' (highlighted in orange), and 'Cancel'.

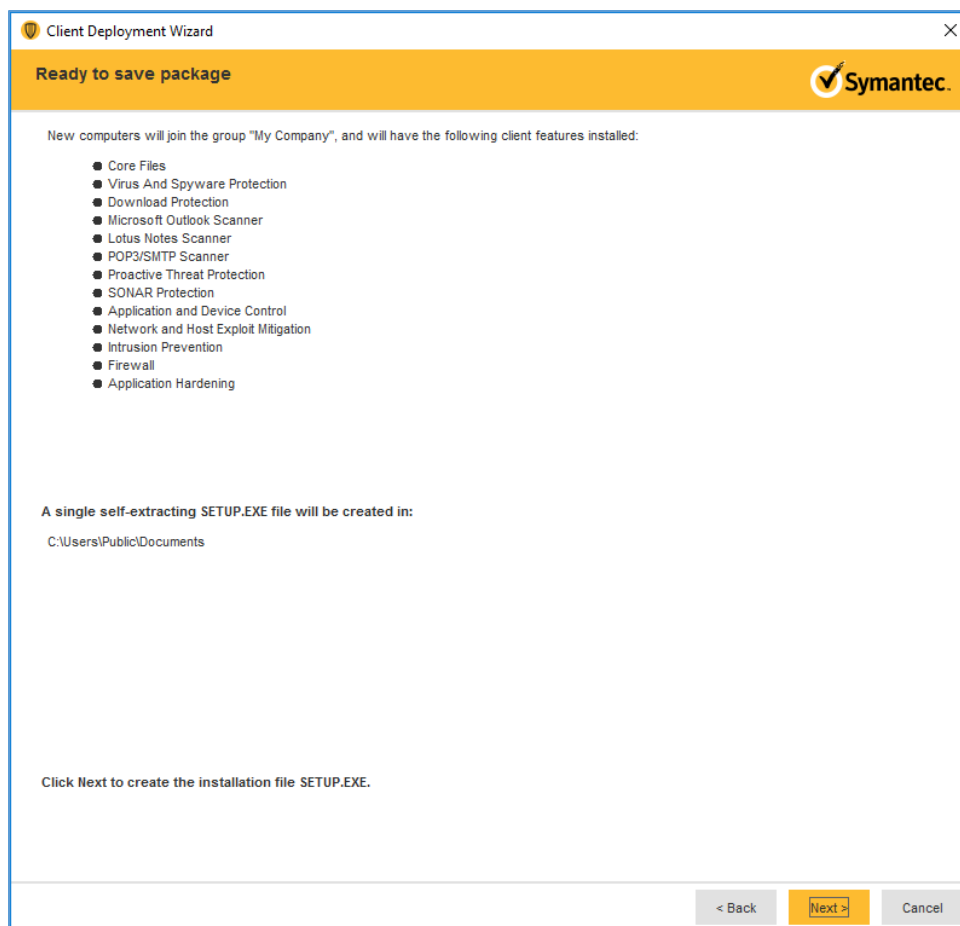
5. Confirm that **Save Package** is selected and click **Next >**.



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



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



8. Move the installation package to the operating system where you want to install Symantec Endpoint Protection.
9. Launch the executable file and follow the prompts to install Symantec Endpoint Protection.

2.9 Data Security

A cloud storage solution, Microsoft Azure, was used to provide data security safeguards for medical images. The Azure solution provides data-at-rest encryption and, through a combination of access control and encryption, provides data security assurance.

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

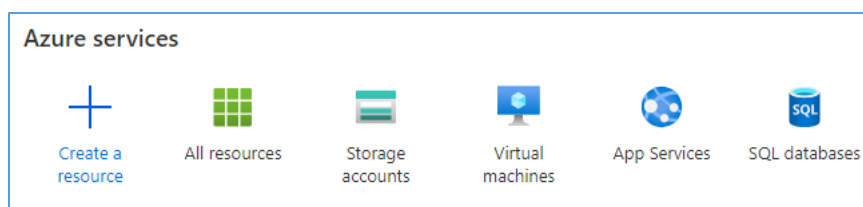
2.9.1 Microsoft Azure Cloud Storage

Microsoft Azure is a cloud service provider that provides storage and encryption for unstructured data in a remote location separate from the HDO environment. This project used an Azure blob storage account as a remote archive for medical images managed by the VNA. For more information on configuring Azure Storage accounts, including recommended security practices, visit *Microsoft's Azure Blob Storage Documentation* [13].

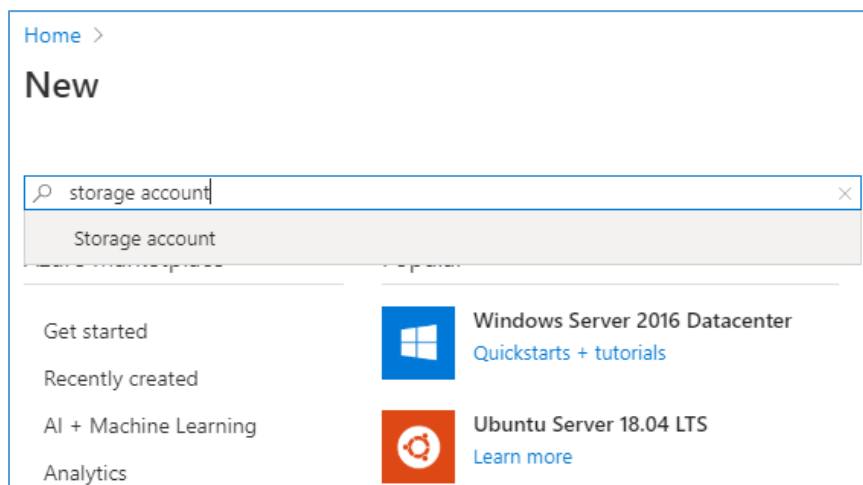
Microsoft Azure Blob Storage Creation

To proceed with the following steps, a Microsoft Storage account needs to be established.

1. From a web browser, navigate to <https://portal.azure.com/>.
2. Log in to the Microsoft account.
3. On the **home screen**, click **Create a resource**.

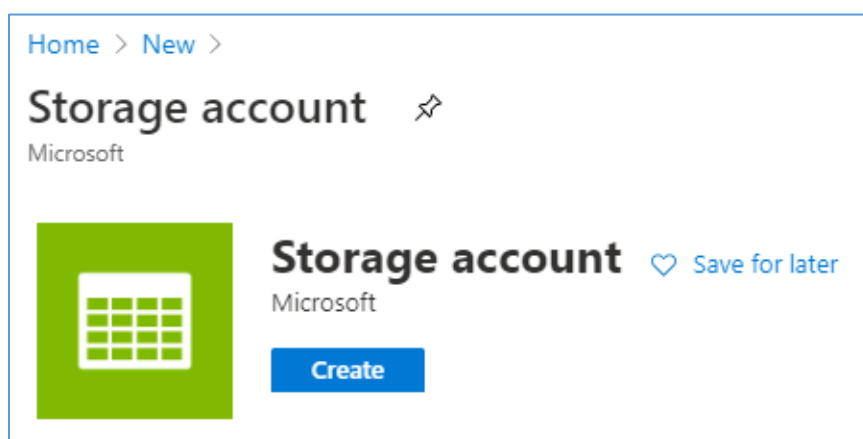


4. Type **storage account** into the search bar, then click **Storage account**.



5. On the Storage Account screen, click the **Create** button. A new screen will appear that requires information to be populated, found in the **Basics** tab. When complete, click the **Next: Networking** button. Populate the **Basics** information using the following values:

- a. On the **Subscription** field, select **Enterprise** from the pull-down menu.
- b. Navigate to the **Resource Group** field. Select the corresponding resource group. If one is not available, create a new resource group.
- c. Navigate to the **Storage Account Name** field. From the pull-down menu, select the storage account name that had previously been created.
- d. Navigate to the **Location** field. From the pull-down menu, select **(US) East US**.
- e. Navigate to the **Performance** field and select **Standard**.
- f. Navigate to the **Account Kind** field. From the pull-down menu, select **StorageV2**.
- g. Navigate to the **Replication** field. From the pull-down menu, select **Geo-redundant storage (GRS)**.
- h. Navigate to the **Access Tier** field and select **Hot**.



Home > New > Storage account >

Create storage account

Basics Networking Data protection Advanced Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Visual Studio Enterprise Subscription

Resource group * [Create new](#)

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

Storage account name * ①

Location * (US) East US

Performance ① ☒ Standard ☐ Premium

Account kind ① StorageV2 (general purpose v2)

Replication ① Geo-redundant storage (GRS)

Access tier (default) ① ☐ Cool ☒ Hot

[Review + create](#) < Previous Next : Networking >

6. Select the **Networking** tab. This will display a form with a series of fields that need to be populated. Fill out the **Networking** information using the following respective values.
 - a. Navigate to the **Connectivity Method** field and select **Public endpoint (all network)**.
 - b. Navigate to the **Network Routing Preference** field and select **Microsoft network routing**.

Home > New > Storage account >

Create storage account

Basics **Networking** Data protection Advanced Tags Review + create

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method *

☒ Public endpoint (all networks)
☐ Public endpoint (selected networks)
☐ Private endpoint
☒ All networks will be able to access this storage account.
[Learn more about connectivity methods](#)

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference * ⓘ

☒ Microsoft network routing (default)
☐ Internet routing

[Review + create](#) [< Previous](#) [Next: Data protection >](#)

7. After supplying the values above, click the **Next: Data Protection** button.
8. Select the **Data Protection** tab, and populate the information as follows:
 - a. Navigate to the **Blob Soft Delete** field and select **Enabled**.
 - b. Navigate to the **Blob Retainment Period in Days** field and enter **60**.
 - c. Navigate to the **File Share Soft Delete** field and select **Disabled**.

Home > New > Storage account >

Create storage account

Basics Networking **Data protection** Advanced Tags Review + create

Blob soft delete ⓘ

☐ Disabled ☒ Enabled

Blob retainment period in days ⓘ

60 days

File share soft delete ⓘ

☒ Disabled ☐ Enabled

Versioning ⓘ

☒ Disabled ☐ Enabled

i The current combination of subscription, storage account kind, performance, replication and location does not support versioning.

[Review + create](#) [< Previous](#) [Next: Advanced >](#)

9. Click the **Next: Advanced** button.
10. Populate the **Advanced** information as follows:

- a. Navigate to the **Secure Transfer Required:** field and select **Enabled**.
- b. Navigate to the **Blob Public Access** field and select **Disabled**.
- c. Navigate to the **Minimum TLS Version** pull-down menu and select **Version 1.2**.

11. Click **Next: Tags** button.

Home > New > Storage account >

Create storage account

Basics Networking Data protection **Advanced** Tags Review + create

Security

Secure transfer required ⓘ ☐ Disabled ☒ Enabled

Blob public access ⓘ ☒ Disabled ☐ Enabled

Minimum TLS version ⓘ Version 1.2 ▼

Azure Files

Large file shares ⓘ ☒ Disabled ☐ Enabled

ⓘ The current combination of storage account kind, performance, replication and location does not support large file shares.

Data Lake Storage Gen2

Hierarchical namespace ⓘ ☒ Disabled ☐ Enabled

ⓘ Data protection and hierarchical namespace cannot be enabled simultaneously.

NFS v3 ⓘ ☒ Disabled ☐ Enabled

ⓘ Sign up is currently required to utilize the NFS v3 feature on a per-subscription basis. [Sign up for NFS v3](#) ↗

[Review + create](#) [< Previous](#) [Next : Tags >](#)

12. Fill out the **Tags** information, then click **Next: Review + create**.

Home > New > Storage account >

Create storage account

Basics Networking Data protection Advanced **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ	Resource
<input type="text"/>	: <input type="text"/>	Storage account

Review + create < Previous Next : Review + create >

- Review the **Create storage account** configuration page, verify the configuration information, then click **Create**.

Basics

- **Subscription:** Visual Studio Enterprise Subscription
- **Resource group:** *****
- **Location:** East US
- **Storage account name:** *****
- **Deployment model:** Resource manager
- **Account kind:** StorageV2 (general purpose v2)
- **Replication:** Geo-redundant storage (GRS)
- **Performance:** Standard
- **Access tier (default):** Hot

Networking

- **Connectivity method:** Public endpoint (all networks)
- **Default routing tier:** Microsoft network routing (default)

Data protection

- **Blob soft delete:** Enabled
- **Blob Retainment Period in Days:** 60

- **File share soft delete:** Disabled
- **Blob change feed:** Disabled
- **Versioning:** Disabled

Advanced

- **Secure transfer required:** Enabled
- **Blob public access:** Disabled
- **Minimum TLS version:** TLS 1.2
- **Large File Shares:** Disabled
- **Hierarchical namespace:** Disabled
- **NSF v3:** Disabled

Home > New > Storage account >

Create storage account

✔ Validation passed

BasicsNetworkingData protectionAdvancedTagsReview + create

Basics

Subscription	Visual Studio Enterprise Subscription
Resource group	
Location	East US
Storage account name	
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Geo-redundant storage (GRS)
Performance	Standard
Access tier (default)	Hot

Networking

Connectivity method	Public endpoint (all networks)
Default routing tier	Microsoft network routing (default)

Data protection

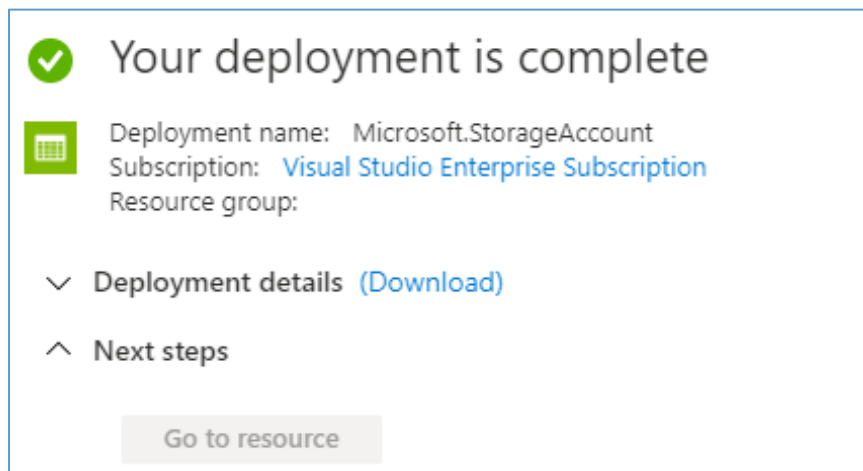
Blob soft delete	Enabled
Blob retainment period in days	60 days
File share soft delete	Disabled
Blob change feed	Disabled
Versioning	Disabled

Advanced

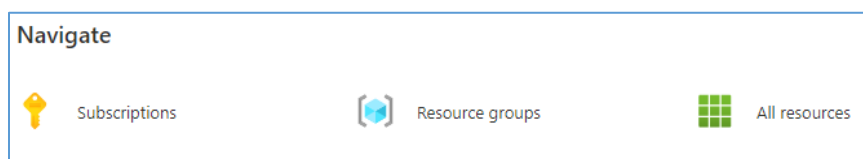
Secure transfer required	Enabled
Blob public access	Disabled
Minimum TLS version	Version 1.2
Large file shares	Disabled
Hierarchical namespace	Disabled
NFS v3	Disabled

Create< PreviousNext >Download a template for

14. Wait for the deployment process to finish. When the deployment is ready, a screen will announce that the deployment has been created.



15. Navigate to the **home screen** and click **All resources**.



16. Click the newly created **storage account**.
17. Navigate to **Firewalls and virtual networks** on the left.
18. Make the following modifications, then click **Save**:
 - **Allow access from:** Selected networks
 - **Address range:** *****

Save

Discard

Refresh

Firewall settings allowing access to storage services will remain in effect for up to a minute.

Allow access from

☐ All networks
 ☒ Selected networks

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)

Virtual Network	Subnet	Address range
No network selected.		

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#)

☐ Add your client IP address (' ')

Address range

✓

IP address or CIDR

19. Navigate to **Encryption** on the left.
20. Under **Encryption type**, select **Customer-managed keys**.
21. Under **Encryption key**, select **Select from key vault**.
22. Under **Key vault and key**, click **Select a key vault and key**.

Encryption Encryption scopes

Save Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters and decrypts it when you access it.

By default, data in the storage account is encrypted using Microsoft-managed keys. You may choose to bring your own keys.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in the storage account will be encrypted by a background encryption process. [Learn more about Azure Storage encryption](#)

Encryption type

☐ Microsoft-managed keys

☒ Customer-managed keys

i The storage account named 'nccoepacstest' will be granted access to protection will be enabled on the key vault and cannot be disabled.

Encryption key

☐ Enter key URI

☒ Select from key vault

Key vault and key *****

Select a key vault and key

23. Under **Key Vault**, click **Create New**.

Home > All resources > Encryption >

Select key from Azure Key Vault

Subscription ***** Visual Studio Enterprise Subscription

Key vault *****

Create new

Key

Create new

24. On the **Create key vault** screen, select the **Basics** tab, and populate the information as follows:

- Navigate to the **Resource Group** field, select the corresponding resource group.
- Navigate to the **Key Vault Name** field, select the corresponding key vault name.
- Navigate to the **Pricing Tier** field; select **Premium**.
- Navigate to the **Soft-Delete** field; select **Enabled**.
- Navigate to the **Days to Retain Deleted Vaults** field; enter 60.
- Navigate to the **Purge Protection** field; select **Allow purging**.

Home > | Encryption > Select key from Azure Key Vault >

Create key vault

Basics Access policy Networking Tags Review + create

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription Visual Studio Enterprise Subscription

Resource group * [Create new](#)

Instance details

Key vault name * ✓

Region East US

Pricing tier * Premium (includes support for HSM backed keys)

Recovery options
Soft delete allows you to recover a deleted key vault and its objects within the retention period you specify. Purging triggers immediate and irrecoverable deletion of the key vault. When purge protection is enabled, vault and its object in the deleted state cannot be purged until the retention period has passed. [Learn more](#)

Soft-delete ☒ Enable recovery of this vault and its objects
☐ Disable recovery of this vault and its objects
 ⓘ Once enabled, this option cannot be disabled

Days to retain deleted vaults * 60 ✓

Purge protection ☒ Allow purging of this vault and its objects during retention period
☐ Enable purge protection of this vault and its objects during retention period

[Review + create](#) < Previous Next : Access policy >

25. Click the **Next: Access Policy** button.

26. Fill out the **Access Policy** information, then click **Next: Networking**.

- a. Navigate to the **Enable Access to** group, and set the following checkboxes:
 - **Azure Virtual Machines for deployment:** Unchecked
 - **Azure Resource Manager for template deployment:** Unchecked
 - **Azure Disk Encryption for volume encryption:** Unchecked
- b. Navigate to the **Current Access Policies:** group and keep the Default User Permissions.

27. On the **Create key vault** screen, under the **Networking** tab, navigate to the line labelled **Connectivity method** and select **Public endpoint(all networks)** and then click on **Next:Tags>**.

28. Fill out the **Tags** information, then click **Next: Review + create**.

Home > | Encryption > Select key from Azure Key Vault >

Create key vault

Basics Access policy Networking **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more](#)

Name ⓘ	Value ⓘ	Resource
<input type="text"/>	:	Key vault

[Review + create](#) < Previous Next : Review + create >

29. Review the **Create key value** configuration page, verify the configuration information, then click **Create**.

Basics

- **Subscription:** Visual Studio Enterprise Subscription
- **Resource group:** *****
- **Key vault name:** *****
- **Region:** East US
- **Pricing tier:** Premium
- **Soft-Delete:** Enabled
- **Purge Protection During Retention Period:** Disabled
- **Retention period (days):** 60 days

Access policy

- **Azure Virtual Machines for deployment:** Disabled
- **Azure Resource Manager for template deployment:** Disabled
- **Azure Disk Encryption for volume encryption:** Disabled
- **Permission model:** Access control list
- **Access policies:** 1

Networking

- **Connectivity method:** Public endpoint (all networks)

[Home](#) > [Encryption](#) > [Select key from Azure Key Vault](#) >

Create key vault

✔ Validation passed

Basics

Access policy

Networking

Tags

Review + create

Review + create

Basics

Subscription

Visual Studio Enterprise Subscription

Resource group

Key vault name

Region

East US

Pricing tier

Premium

Soft-delete

Enabled

Purge protection during retention period

Disabled

Days to retain deleted vaults

60 days

Access policy

Azure Virtual Machines for deployment

Disabled

Azure Resource Manager for template deployment

Disabled

Azure Disk Encryption for volume encryption

Disabled

Permission model

Access control list

Access policies

1

Networking

Connectivity method

Public endpoint (all networks)

Create

< Previous

Next >

Download a

30. Wait for the creation process to finish.
31. Navigate to the **Key** field and click **Create New**.

Home > | Encryption >

Select key from Azure Key Vault

Subscription *

Key vault *

[Create new](#)

Key *

[Create new](#)

32. Fill out the form with the following information, then click **Create**:

- **Options:** Generate
- **Name:** *****
- **Key Type:** RSA
- **RSA Key Size:** 2048
- **Enabled?:** Yes

[Home](#) >
 [Encryption](#) >
[Select key from Azure Key Vault](#) >

Create a key

Options

Generate

Name * ⓘ

Key Type ⓘ

RSA

EC

RSA Key Size

2048

3072

4096

Set activation date? ⓘ ☐

Set expiration date? ⓘ ☐

Enabled?

Yes

No

Create

33. Once the key has been successfully created, ensure the values for **Subscription**, **Key Vault**, and **Key** are correct as follows, then click **Select**:

- **Subscription:** Visual Studio Enterprise Subscription
- **Key vault:** *****
- **Key:** *****

Home > | Encryption >

Select key from Azure Key Vault

i The key ' ' has been successfully created.

Subscription *

Key vault * [Create new](#)

Key * [Create new](#)

[Select](#)

34. Verify the following **Encryption** information, then click **Save**:

- **Encryption type:** Customer-managed keys
- **Encryption key:** Select from key vault
- **Key vault:** *****
- **Key:** *****

Encryption | Encryption scopes

[Save](#) [Discard](#)

Encryption type ☐ Microsoft-managed keys ☒ Customer-managed keys

i The storage account named ' ' protection will be enabled on the key vault

Encryption key ☐ Enter key URI ☒ Select from key vault

Key vault and key *

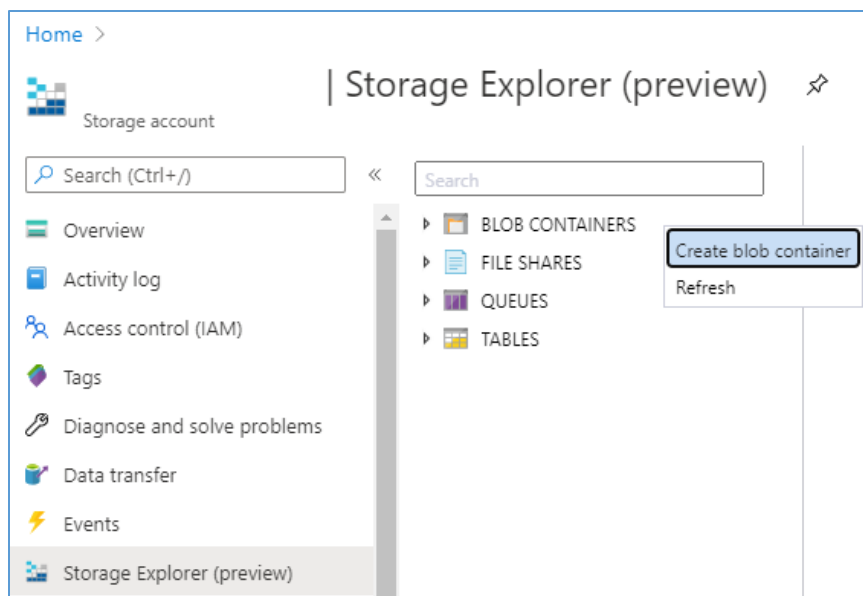
Key vault:
Key:
[Select a key vault and key](#)

35. Take note of the key strings. These will be used to authenticate the VNA's requests to the storage account:

- **Storage account name:** *****
- **Key:** *****
- **Connection string:** *****

36. Navigate to **Storage Explorer** on the left of the **Storage Explorer (preview)** page.

37. Right-click **BLOB CONTAINERS**, then click **Create blob container**.



38. Fill out value of the **Name** field for the **New container**, then click **Create**.

New container ×

Name *

Public access level ⓘ

Private (no anonymous access) ▼

i The public access level is set to private because public access is disabled on this storage account.

▼ Advanced

Create
Discard

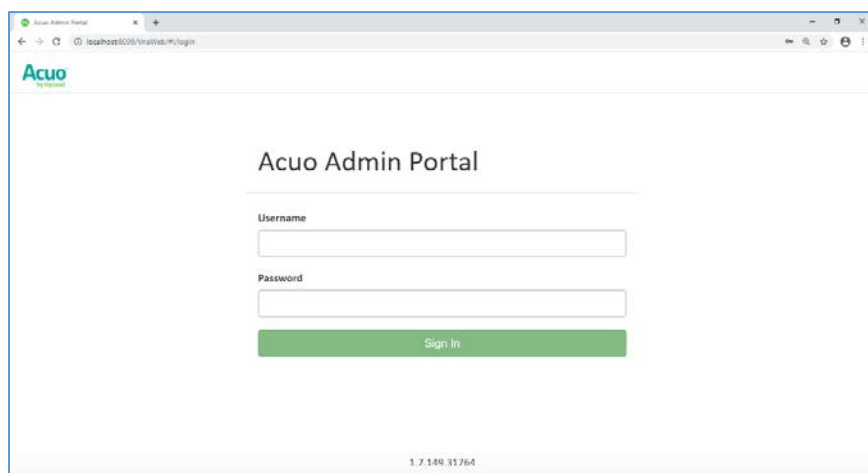
39. The established storage account is ready for use, and the VNA can be configured to send and receive medical images to and from the storage account container.

2.9.2 Hyland VNA Cloud Archive Device

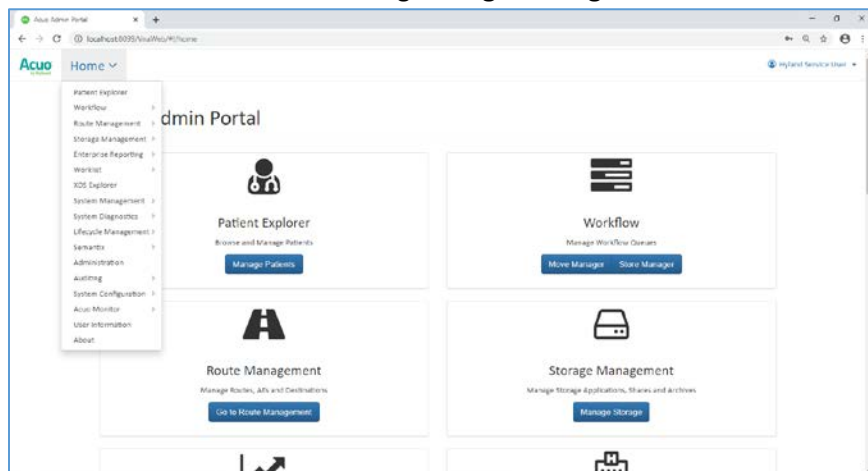
For this project, a Hyland engineer upgraded the Hyland Acuo VNA v6.0.4 and NilRead Enterprise v4.3.31.98805 to Acuo VNA v6.0.4.2798_H2_P2 and NilRead Enterprise v4.4.32.103830. These upgrades enabled the Hyland VNA to store patient studies in a Microsoft Azure storage account. When configuring the connection to the Azure account, the VNA allowed an engineer to determine the number of days that patient studies were held in the cache. For testing purposes, this project kept studies in the VNA cache for three days and immediately stored these studies in the Azure storage. When configuring for production, identify time frames for cache and cloud storage that coincide with an HDO's business practices.

Hyland NilRead Archive Device Configuration

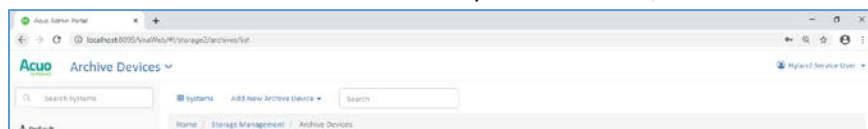
1. Open a web browser and navigate to the Acuo Admin Portal created in [Section 2.2.2](#), Hyland Acuo VNA.
2. Enter the **Username** and **Password** for the **Admin Portal**, and click **Sign In**.



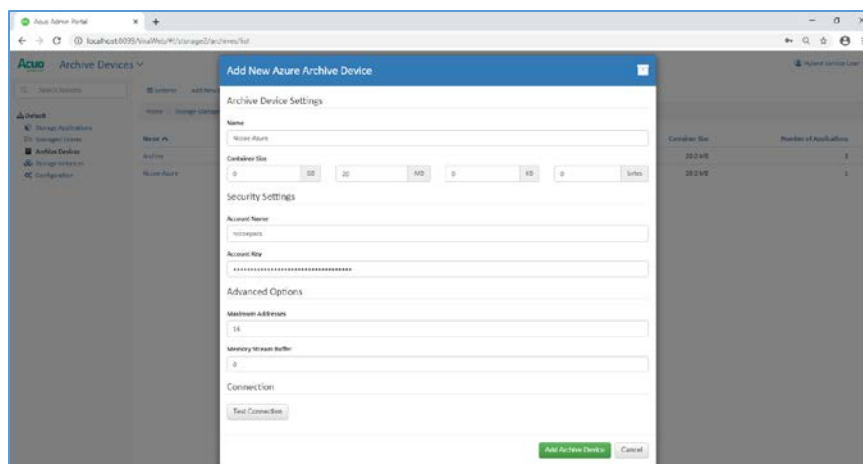
3. Navigate to the Archive Devices section of the portal by clicking the drop-down list on the top left corner of the screen and selecting **Storage Management** and then **Archive Devices**.



4. Click **Add New Archive Device** in the top of the screen, then select **Azure**.

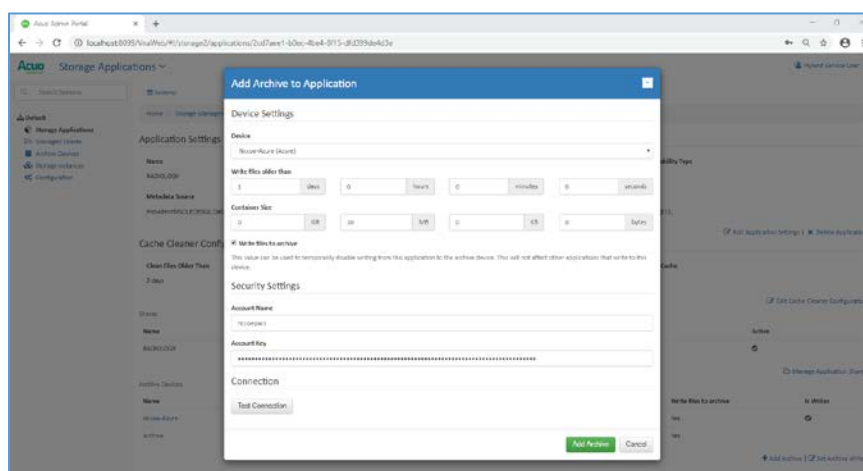


5. In the Add New Azure Archive Device window, provide the following Azure account information:
 - **Name:** *****
 - **Container Size:** 20 MB
 - **Account Name:** *****
 - **Account Key:** *****
6. Click **Add Archive Device**.



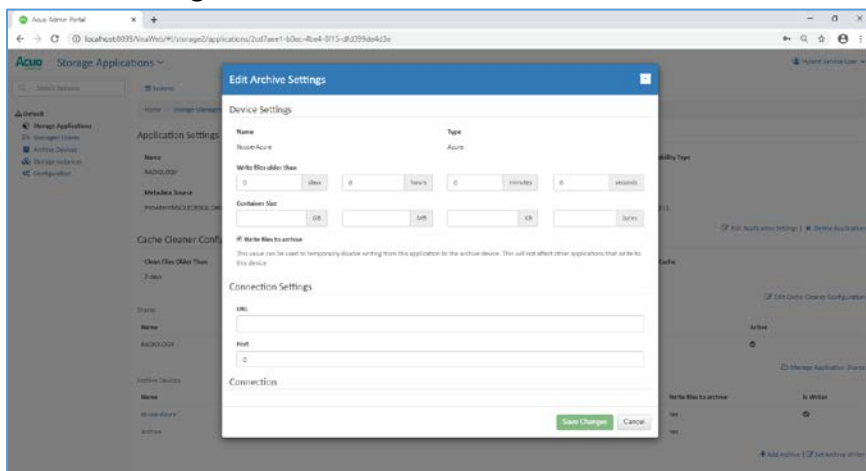
Connect Microsoft Azure Archive Device to the RADIOLOGY Storage Application

1. Click **Storage Applications** on the left-hand side of the screen.
2. Click **RADIOLOGY**.
3. Scroll down and click **Add Archive**.
 - **Device:** *****
 - **Write files older than:** 1 day(s)
 - **Enable Write files to archive.**
4. Click **Add Archive**.



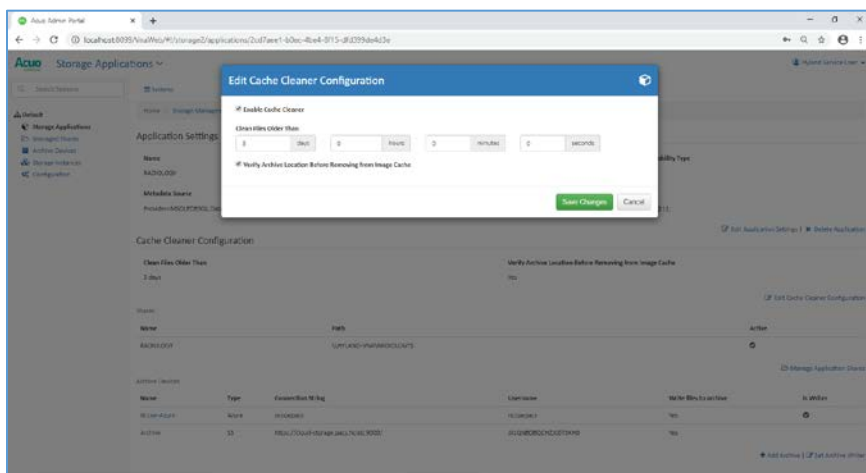
Set Parameters for Image Archival to Microsoft Azure

1. Select **Nccoe-Azure** under Archive Devices at the bottom of the screen.
2. Set **Write files older than** to **0 days**.
3. Click **Save Changes**.



Set Parameters for Storing Images in the VNA's Cache

1. Click **Edit Cache Cleaner Configuration**.
2. Set **Clean Files Older Than** to **3 days**.
3. Click **Save Changes**.



2.10 Secure Remote Access

Both healthcare and IT systems require access by vendor support technicians for remote configuration, maintenance, patching, and updates to software and firmware. This project implemented secure remote access by integrating Symantec Validation and ID Protection (VIP) into the ConsoleWorks authentication mechanism. This implementation enforced two-factor authentication with username, password, and a onetime passcode.

2.10.1 TDi Technologies ConsoleWorks

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

System Requirements

- **CPUs:** 1
- **Memory:** 8 GB RAM
- **Storage:** 40 GB
- **Operating System:** CentOS 7
- **Network Adapter:** VLAN 1097

TDi ConsoleWorks Installation

The TDi ConsoleWorks installation in this PACS environment replicates the installation in the Wireless Infusion Pumps Project. For detailed installation guidance, please refer to Section 2.1.8, TDi ConsoleWorks External Remote Access, in NIST SP 1800-8C, *Securing Wireless Infusion Pumps* [12].

TDi ConsoleWorks Radius Authentication Configuration

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

1. Download *extern_auth_radius.so* file from ConsoleWorks support site [14].
2. Move *extern_auth_radius.so* file to */opt/ConsoleWorks/bin* directory.
3. Restart ConsoleWorks by executing *cw_stop* and *cw_start* scripts located in the */opt/ConsoleWorks/bin* directory.
4. From the ConsoleWorks web interface, navigate to **Security**, and click **External Authentication**.
5. Click **add** to create a new external authentication source.

6. Fill out the required fields. The setup we used is below:

- **Record Name:** Radius
- Ensure **Enable** is checked.
- For **Library**, select **radius**.
- **Parameter 1:** 192.168.120.190:1812/*****
- **Parameter 2:** 30
- **Parameter 6:** 15
- **Template User:** CONSOLE_MANAGER

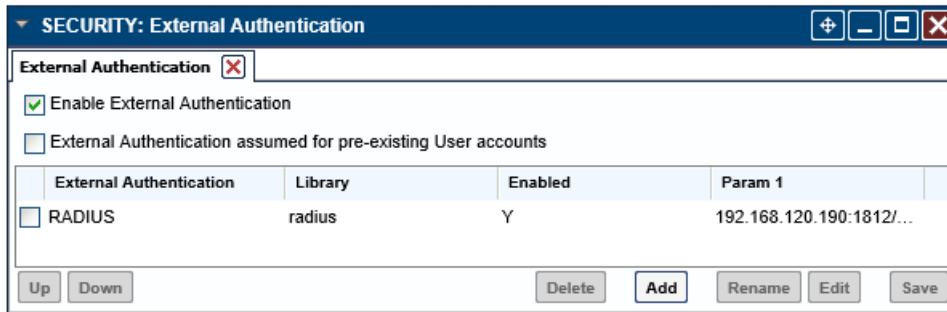
7. Continue through the prompt by clicking **Next**; click **Save** on the final prompt.

The screenshot shows a window titled "External Authentication Record". It contains the following fields and values:

- Record Name:** RADIUS
- Enabled:** ☒
- Library:** radius
- Parameter 1:** 192.168.120.190:1812/*****
- Parameter 2:** 30
- Parameter 3:** (empty)
- Parameter 4:** (empty)
- Parameter 5:** (empty)
- Parameter 6:** 15
- Required Profile:** (empty)
- Template User:** CONSOLE_MANA...

At the bottom of the window are two buttons: "Cancel" and "Next".

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



2.10.2 Symantec Validation and ID Protection (VIP)

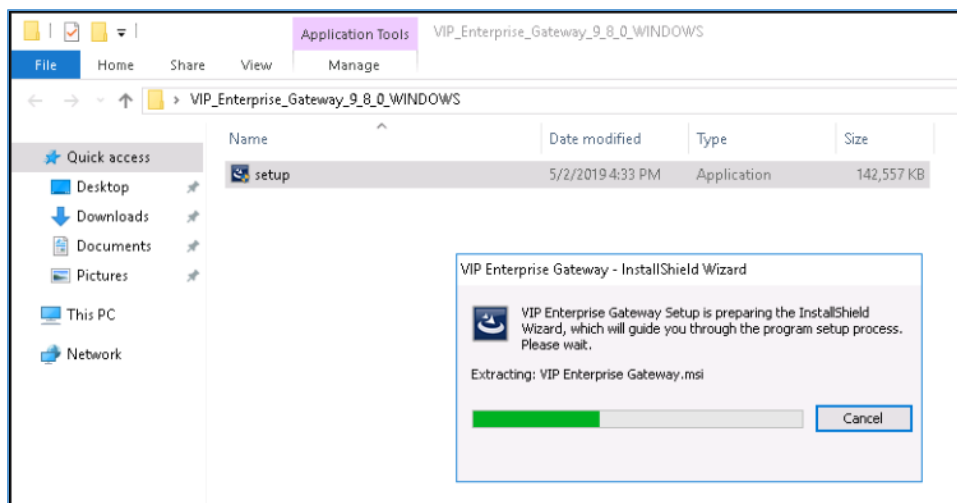
Symantec Validation and ID Protection is an authentication service that provides various forms of authentication such as push, short message service (SMS), and biometric. This project used Symantec VIP as a second form of authentication for remote access to the PACS architecture through TDi Technologies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

System Requirements

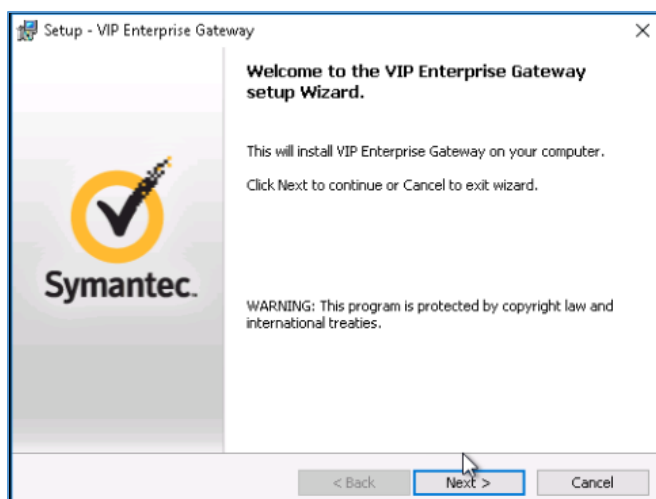
- **CPUs:** 4
- **Memory:** 8192 MB RAM
- **Storage:** 240 GB (thin provision)
- **Operating System:** Microsoft Windows Server 2016
- **Network Adapter:** VLAN 1201

Symantec VIP Installation

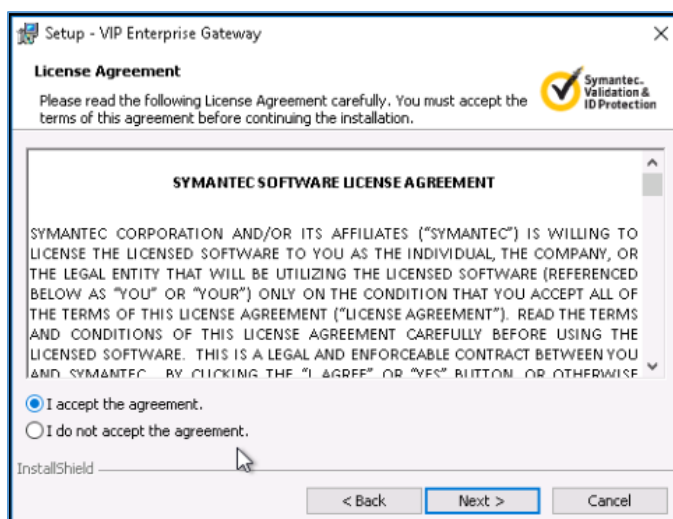
1. Right-click on *setup.exe* file for VIP Enterprise Gateway 9.8.0; select **Run as administrator**.



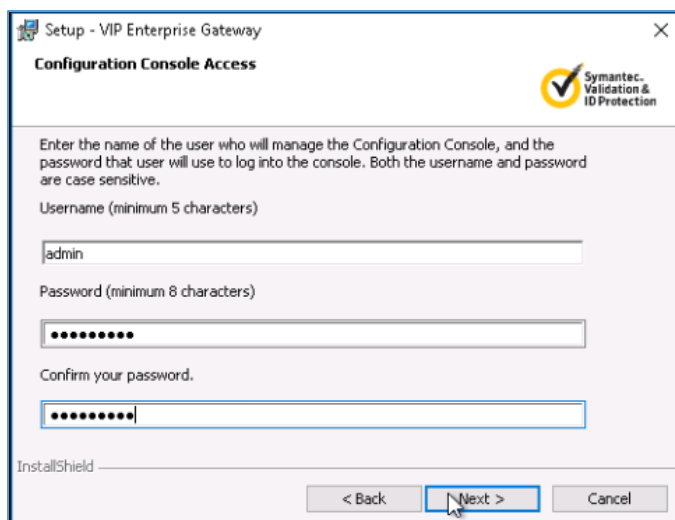
2. Proceed through the installation wizard by clicking **Next >**.



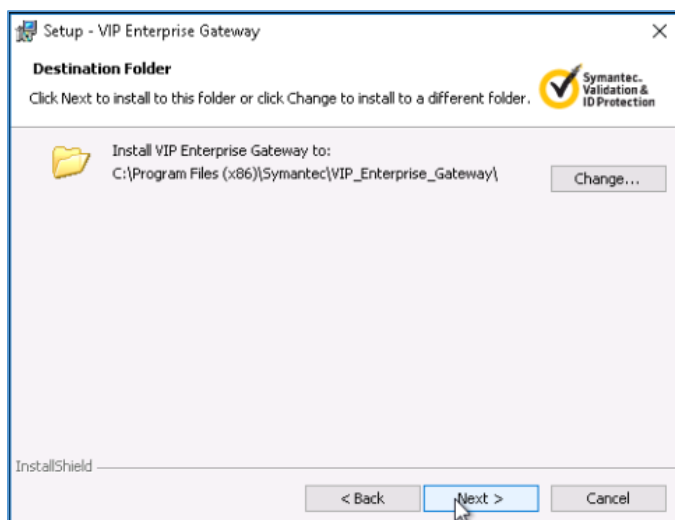
3. Check **I accept the agreement**.
4. Click **Next >**.



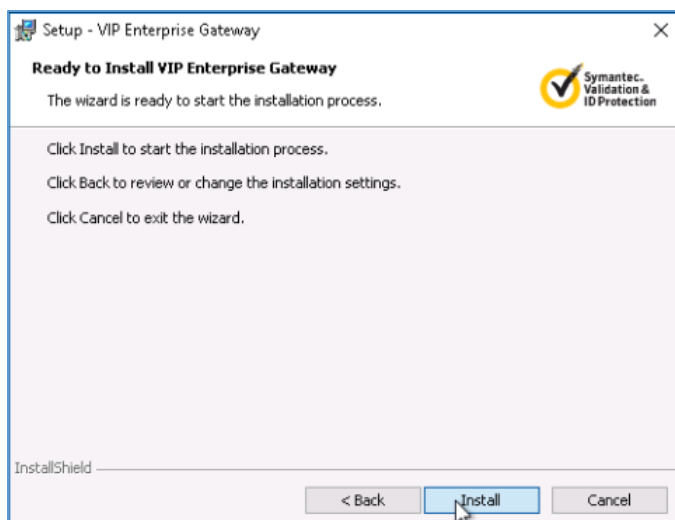
5. Create a **username** as **admin** and a **password** and click **Next >**.



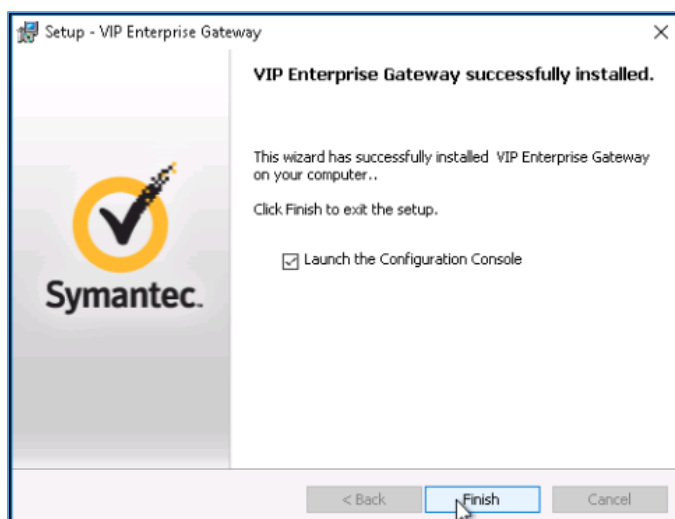
6. Keep the default installation location by clicking **Next >**.



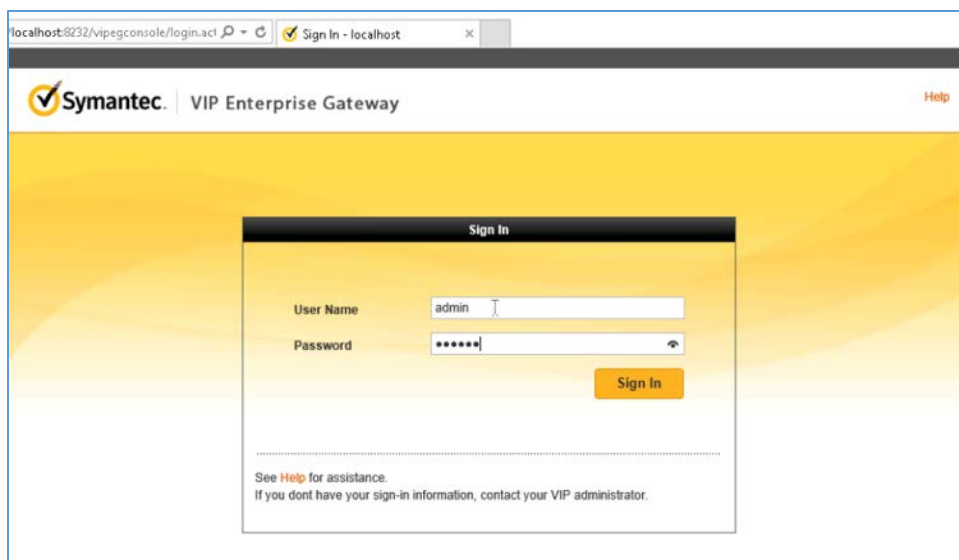
7. Click **Install**.



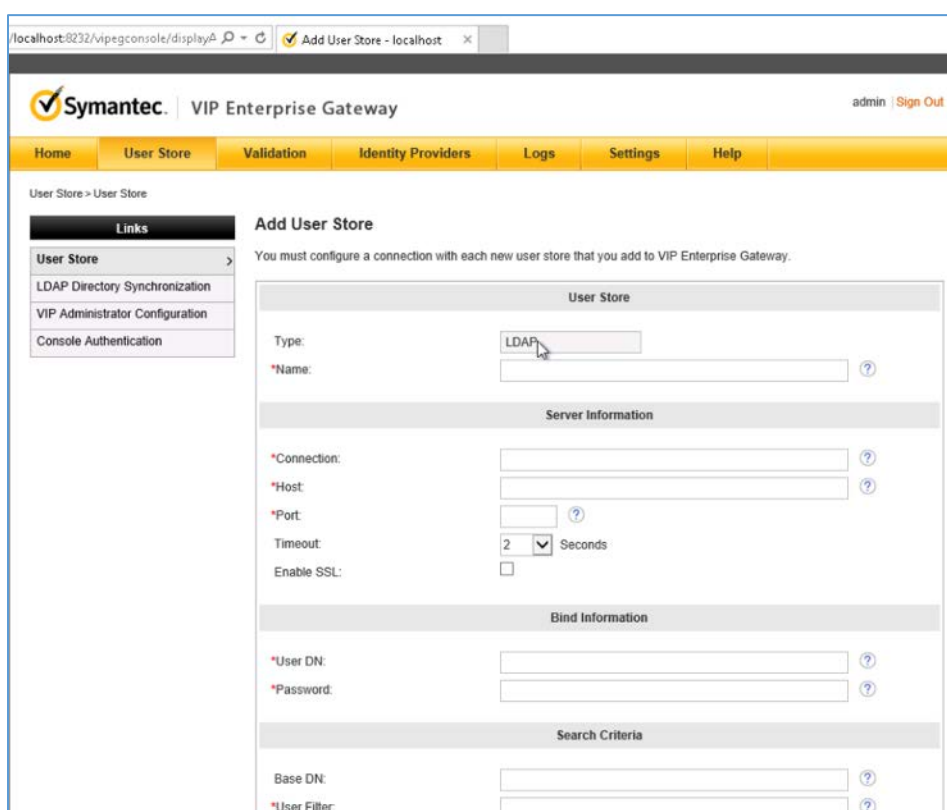
8. Click **Finish** after installer is complete.



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



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



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))(sAMAccountName=%s))

The screenshot shows a configuration window titled "Add User Store - localhost". The window is divided into several sections:

- Name:** AD-PACS
- Server Information:**
 - Connection:** ad-main
 - Host:** ad.pacs.hclab
 - Port:** 389
 - Timeout:** 2 Seconds
 - Enable SSL:** ☐
- Bind Information:**
 - User DN:** CN=cpeloquin,DC=pacs,DC=hclab
 - Password:** *****
- Search Criteria:**
 - Base DN:** DC=pacs,dc=hclab
 - User Filter:** (&(&objectClass=user)(objectCategory=person))(sAMAccountName=%s))
 - ☐ Edit Default VIP User Name Attribute
- Test Settings:**
 - Test User Name:** kangmin
 - Test:** [Button]
 - Message:** Test bind failed. Be sure you have the correct Host, Port, SSL (if selected), and Bind information for the User Store AD-PACS.

At the bottom, there are "Cancel" and "Submit" buttons, and a note: "*Required Information".

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/>.

ntec.com/vipmgr/loginwithnocredential.v

Home - localhost

VIP Manager - Register Your... X

Symantec VIP - Two Factor Aut...

Symantec | VIP MANAGER

Help | Sign In

Register Your VIP Credential

Provide your credential ID and a security code to register your VIP credential.

Credential ID: VSST22651643
Typically 12 alphanumeric characters

Security Code: 286928 X
6 digits generated from your VIP credential

Cancel Register

Legal Notice | Privacy | Repository | © 2019 Symantec Corporation

Symantec VIP

Norton SECURED
powered by digiart

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

ntec.com/vipmgr/savecredential.v

Home - localhost

Waiting for manager.vip.s... X

Symantec VIP - Two Factor Aut...

Symantec | VIP MANAGER

Dashboard Users Credentials Account Policies Reports Help

✓ **Your VIP Credential Was Registered Successfully**

You have successfully registered your VIP credential and you are now signed in to your account.

Go to My Account

Legal Notice | Privacy | Repository | © 2019 Symantec Corporation

Symantec VIP

Norton SECURED
powered by digiart

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

Account Summary - UNVERIFIED - NCCoE

Click one of the following tabs to view additional details:

- Account Information
- Single Sign-on
- Features
- Dynamic Provisioning
- Registration File

Organization Information		
Organization Name UNVERIFIED - NCCoE	Organizational Unit	Organization Address 9700 Great Seneca Hwy Rockville MD 20850 United States

Contact Information		
Corporate Contact Sue Wang NA swang@nbtire.org 301975-0288 (preferred)	Technical Contact Sue Wang NA twang@nbtire.org 301975-0288 (preferred)	Billing Contact Sue Wang NA swang@nbtire.org 301975-0288 (preferred)

Account Information	
Jurisdiction Hash	140046104
Account Creation Date*	2019-May-03
Service Start Date*	2019-May-03
Service End Date*	2019-Jul-02
Member Type	Trial
Account Usage	Test
Sales Reference Number	

*Reflects either PST or PDT, as applicable.

[Back](#)

Links

- VIP Account Management
 - View Account Details
 - Manage User Groups
 - Create Administrator Group
 - Find / Modify Administrator Groups
 - Create VIP Administrators
 - Find / Modify VIP Administrators
 - Manage VIP Certificates
 - SMS Credential Settings
 - Credential Security Settings
 - Download Files

16. Select **Request a Certificate**.

Manage VIP Certificates

Use this page to request a new certificate or to track your existing certificates.

Click **Request a Certificate** to request a new certificate and to download it.

Certificate Name	Expiration*	State	Action
You have no certificates associated with your VIP account.			

*Reflects either PST or PDT, as applicable.

[Cancel](#) [Request a Certificate](#)

Links

- VIP Account Management
 - View Account Details
 - Manage User Groups
 - Create Administrator Group
 - Find / Modify Administrator Groups
 - Create VIP Administrators
 - Find / Modify VIP Administrators
 - Manage VIP Certificates
 - SMS Credential Settings
 - Credential Security Settings
 - Download Files

17. Provide a **Certificate Name** as **NCCoE_VIP_Cert**. Click **Submit Request**.

Request a Certificate

Enter an easily-recognizable name for your certificate (such as "VIP Certificate 1") in the field below.

If you have your own private key, enter a Certificate Signing Request (CSR) that you've generated by [clicking here](#). Symantec supports 2048-bit keys in the CSR.

* Required Information

Certificate Name

*Certificate Name NCCoE_VIP_Cert

Important Service Requirements: If you discover or have reason to believe that there has been a compromise of your private key, you must immediately revoke the certificate or notify Symantec to do so. Similarly, if the information within your certificate or your organization name has changed, please notify Symantec. Note that Symantec retains the right to revoke your certificate at any time without notice if (i) you fail to perform your obligations under the terms of your service agreement, or (ii) in Symantec's sole discretion, you have engaged in activities which Symantec determines are harmful to its systems.

Back Submit Request

Links

- VIP Account Management
 - View Account Details
 - Manage User Groups
 - Create Administrator Group
 - Find / Modify Administrator Groups
 - Create VIP Administrators
 - Find / Modify VIP Administrators
 - Manage VIP Certificates
 - SMS Credential Settings
 - Credential Security Settings
 - Download Files

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

Your Certificate Request has been Approved

Your certificate named NCCoE_VIP_Cert expires on 2021 May-06.

1 Select a certificate format, enter a password to encrypt the certificate, and then click Download Certificate.

* Required Information

*Format ☐ PEM ☒ PKCS#12

*Password ***** Must be at least eight characters and include one uppercase and one lowercase letter, plus one number.

Download Certificate

2 After downloading your certificate, you will need to install it.

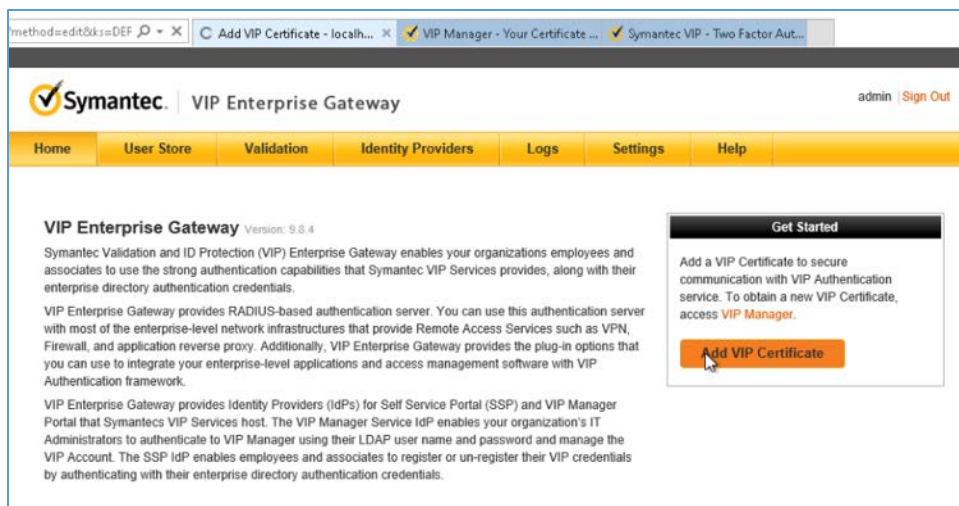
[Go to the Help and Support page for PKCS#12 format](#) if you need help installing the certificate to use with VIP Web services.

[Go to the Help and Support page for PEM format](#) if you need help installing the certificate to use with a Cisco SA 500 series VPN router.

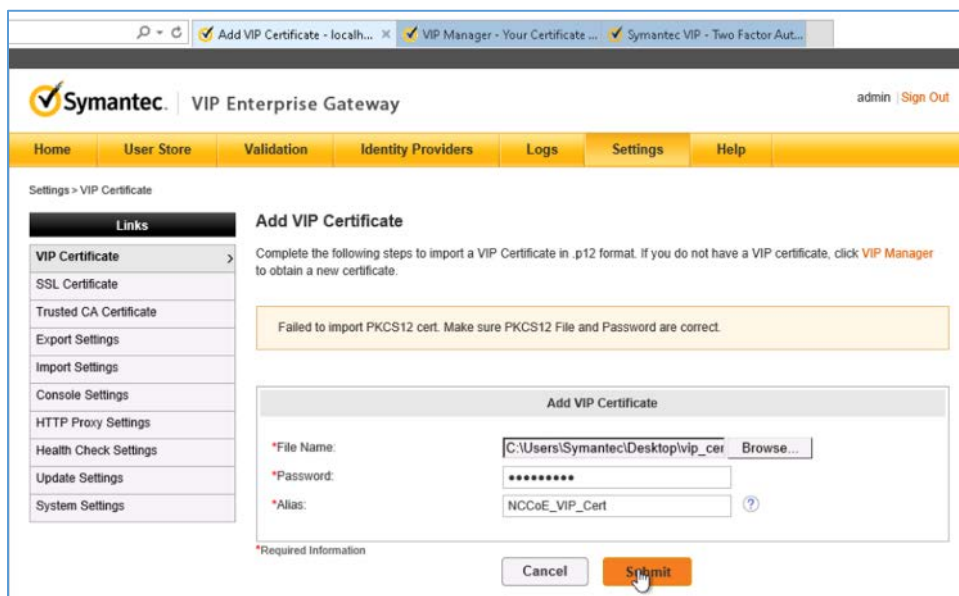
Return Home

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

20. Navigate to <http://localhost: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

The screenshot shows the 'Add RADIUS Validation Server' configuration page in the Symantec VIP Enterprise Gateway. The page is titled 'Validation > RADIUS Validation Server' and includes a 'Links' sidebar with 'RADIUS Validation Server' and 'Tunnel Server'. The main content area is titled 'Add RADIUS Validation Server' and contains the following fields and sections:

- Server Information:**
 - * Server Name: [Text Field]
 - * Local IP: [Dropdown Menu] (192.168.120.190)
 - * Port: [Text Field] (1812)
 - * RADIUS Shared Secret: [Text Field]
 - * Confirm RADIUS Shared Secret: [Text Field]
 - Logging Level: [Dropdown Menu] (INFO)
 - Log Rotation Interval: [Text Field] (1) days
 - Number of Files to Keep: [Text Field] (4)
 - Enable Syslog: [Radio Buttons] (Yes/No) (No selected)
 - * Password Encoding: [Dropdown Menu] (UTF-8)
- RADIUS Access Challenge:**
 - ☒ Enable Access Challenge
 - * Challenge Timeout: [Text Field] (60)
- VIP Push Authentication:**
 - ☒ Enable Push
 - Remote Access Service Name/URL: [Text Field] (Remote Access Service Name)

At the bottom, a status message states 'The vip_cert.p12 download has completed.' with buttons for 'Open', 'Open folder', and 'View downloads'.

23. Click **Submit**.

ustom.action?customf

RADIUS Validation Server - I... VIP Manager - Your Certificate ... Symantec VIP - Two Factor Aut...

VIP Authentication Timeout: 60

*Enforce Local Authentication: ☐ Yes ☒ No

First-Factor Authentication

☒ Enable First Factor

Authentication on: ☒ Enterprise ☐ VIP Services

Authentication Sequence: ☒ LDAP Password - VIP Authentication ☐ VIP Authentication - LDAP Password

User Store Configuration

☒ User resides in user store

☐ Enable User Store data for Out-of-Band

User Store: AD-PACS

Business Continuity

Business Continuity: ☒ Disabled ☐ Automatic ☐ Enabled

Delegation

☐ Enable Delegation

LDAP to RADIUS Mapping

☐ Enable LDAP to RADIUS Mapping

*Required Information

Cancel Submit

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

Symantec | VIP Enterprise Gateway

admin | Sign Out

Home User Store Validation Identity Providers Logs Settings Help

Validation > RADIUS Validation Server

Links

RADIUS Validation Server

Tunnel Server

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

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

Add Server

Server	Port	Status	Action
VIP	1812	ON	Edit Delete Duplicate

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

Appendix A List of Acronyms

AD	Active Directory
AES	Advanced Encryption Standard
AE Title	Application Entity Title
CA	Certificate Authority
CIDR	Classless Inter-Domain Routing
CPU	Central Processing Unit
CSR	Certificate Signing Request
DB	Database
DC	Domain Controller
DCS:SA	Data Center Security: Server Advanced
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine
DNS	Domain Name System
EDR	Endpoint Detection and Response
FMC	Firepower Management Center
FTD	Firepower Threat Defense
GB	gigabyte
GUI	Graphical User Interface
HD	Hard Drive
HDO	Healthcare Delivery Organization
HIP	Host Identity Protocol
HL7	Health Level 7
http	Hypertext Transfer Protocol
https	Hyper Text Transfer Protocol Secure

IDN	Identity Defined Networking
IIS	Internet Information Services
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MPPS	Modality Performed Procedure Step
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
OVA	Open Virtual Appliance or Application
OVF	Open Virtualization Format
PACS	Picture Archiving and Communication System
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
QR Code	Quick Response Code
RAM	Random Access Memory
RIS	Radiology Information System
SCP	Service Class Provider
SEP	Symantec Endpoint Protection
SEPM	Symantec Endpoint Protection Manager

SMS	Short Message Service
SP	Special Publication
SQL	Structured Query Language
SSL/TLS	Secure Sockets Layer/Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol
UDM	Universal Data Manager
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VIP	Validation and ID Protection
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNA	Vendor Neutral Archive
WAN	Wide Area Network
WLM	Workload Management

Appendix B References

- [1] Docker. Install Docker Desktop on Windows. Available: <https://docs.docker.com/docker-for-windows/install/>.
- [2] Microsoft Docs. Install SQL Server from the Installation Wizard (Setup). Available: <https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server-from-the-installation-wizard-setup?view=sql-server-2017>.
- [3] K. McKay and D. Cooper, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Revision 2, NIST, Gaithersburg, Md., Aug. 2019. Available: <https://doi.org/10.6028/NIST.SP.800-52r2>.
- [4] DVTk. DVTk open source project main contributors ICT Group and Philips. Available: <https://www.dvtk.org/>.
- [5] Microsoft TechNet. Building Your First Domain Controller on 2012 R2. Available: <https://social.technet.microsoft.com/wiki/contents/articles/22622-building-your-first-domain-controller-on-2012-r2.aspx>.
- [6] Microsoft TechNet. Installing and Configuring DHCP role on Windows Server 2012. Available: <https://blogs.technet.microsoft.com/teamdhcp/2012/08/31/installing-and-configuring-dhcp-role-on-windows-server-2012/>.
- [7] DigiCert. CSR Creation Instructions for Microsoft Servers. Available: <https://www.digicert.com/util/csr-creation-microsoft-servers-using-digicert-utility.htm>.
- [8] Cisco. *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/fmcv/FMCv-quick.html.
- [9] Cisco. *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide*. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg.html.
- [10] Cisco Systems, Inc. *Basic Policy Creation for Firepower*. Jan. 30, 2019. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/Basic_Policy_Creation_on_Cisco_Firepower_Devices.pdf.
- [11] Cisco Systems, Inc. *Cisco Stealthwatch: Installation and Configuration Guide 7.0*. 2019. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_0_Installation_and_Configuration_Guide_DV_3_1.pdf.

- [12] G. O'Brien et al., *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*, NIST SP 1800-8, NIST, Gaithersburg, Md., Aug. 2018. Available: <https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf>.
- [13] Microsoft. Storage Account Overview. Available: <https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview?toc=/azure/storage/blobs/toc.json>.
- [14] TDi Technologies, External Authentication libraries, ConsoleWorks Cybersecurity Operations Platform. Available: <https://support.tditechnologies.com/content/external-authentication-libraries>.