NIST SPECIAL PUBLICATION 1800-24

Securing Picture Archiving and Communication System (PACS)

Cybersecurity for the Healthcare Sector

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

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

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs

National Institute of Standards and Technology
U.S. Department of Commerce

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST SPECIAL PUBLICATION 1800-24

Securing Picture Archiving and Communication System (PACS)

Cybersecurity for the Healthcare Sector

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

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

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

DRAFT

September 2019

U.S. Department of Commerce
Wilbur Ross, Secretary

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

NIST SPECIAL PUBLICATION 1800-24A

Securing Picture Archiving and Communication System (PACS)

Cybersecurity for the Healthcare Sector

Volume A:
Executive Summary

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

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

September 2019

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs

Executive Summary

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

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

CHALLENGE

PACS, by its nature, is a system that cannot operate in isolation. The overall PACS ecosystem consists of diverse technologies that include medical imaging devices, patient registry systems, worklist management systems, and systems used to manage and maintain medical image archives. The primary role of PACS is interaction with disparate medical imaging devices, interconnectivity with other clinical systems, and allowing a geographically and organizationally diverse team of healthcare professionals to review medical images to provide quality and timely patient care. Therefore, the threat landscape is broad. If not properly secured, vulnerabilities may be introduced into the PACS ecosystem, either affecting clinical information stored in the PACS environment or allowing malicious actors to leverage components within the ecosystem as pivot points into the integrated healthcare information system.

SOLUTION

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

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

In building the reference architecture, the NCCoE sought existing technologies that provided the following capabilities:

- role-based access control
- authentication
- network access control
- endpoint protection
- network and communication protection
- micro segmentation
- behavioral analytics
- tools that use cyber threat intelligence
- anti-malware
- data security
- segregation of duties
- restoration and recoverability
- cloud storage

While the NCCoE used a suite of commercial products to address security challenges, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Information security experts should identify the products that will best integrate with existing tools and IT system infrastructure. Organizations can adopt this solution or one that adheres to these guidelines in whole, or this guide can be used as a starting point for tailoring and implementing parts of a solution.

BENEFITS

The NCCoE's practice guide to Securing PACS can help an organization:

- improve resilience in the network infrastructure, including limiting a threat actor's ability to leverage components as pivot points to attack other parts of the HDO's environment
- limit unauthorized movement within the HDO environment by authorized system users to address the "insider threat" as well as unauthorized actors once they gain network access
- analyze behavior and detect malware throughout the ecosystem to enable HDOs to determine when components evidence compromise and to enable those organizations to limit the effects of a potential advanced persistent threat such as ransomware
- secure sensitive data (e.g., personally identifiable information or protected health information) at rest and in transit, limiting adversarial ability to exfiltrate or expose that data
- consider and address risks that may be identified as HDOs examine cloud solutions as part of managing their medical imaging infrastructure

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at hit_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Cisco, Clearwater Compliance, DigiCert, Forescout, Hyland, Philips, Symantec, tdi technologies, Tempered Networks, Tripwire, Virta Labs, Zingbox

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 challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

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

NIST SPECIAL PUBLICATION 1800-24B

Securing Picture Archiving and Communication System (PACS)

Cybersecurity for the Healthcare Sector

Volume B:
Approach, Architecture, and Security Characteristics

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

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

September 2019

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-24B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-24B, 96 pages, (September 2019), CODEN: NSPUE2

FEEDBACK

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

Comments on this publication may be submitted to: hit_nccoe@nist.gov.

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

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov .

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

Name	Organization
Andy Gray	Forescout
Katherine Gronberg	Forescout
William Canter	Hyland
Kevin Dietz	Hyland
David Alfonso	Philips Healthcare
Jonathan Bagnall	Philips Healthcare
Julian Castro	Philips Healthcare
Sukanta Das	Philips Healthcare
Jason Dupuis	Philips Healthcare
Michael McNeil	Philips Healthcare
Dwayne Thaele	Philips Healthcare
Steve Kruse	Symantec
Derek Peters	Symantec
Axel Wirth	Symantec
Bill Johnson	TDi Technologies
Pam Johnson	TDi Technologies
Robert Armstrong	Tempered Networks
Nicholas Ringborg	Tempered Networks

Name	Organization
Mehwish Akram	The MITRE Corporation
Steve Edson	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Donald Faatz	The MITRE Corporation
Harry Perper	The MITRE Corporation
Randy Esser	Tripwire
Onyeka Jones	Tripwire
Jim Wachhaus	Tripwire
Sandra Osafo	University of Maryland University College
Henrik Holm	Virta Labs
Michael Holt	Virta Labs
Ben Ransford	Virta Labs
Jun Du	Zingbox
Damon Mosk-Aoyama	Zingbox
David Xiao	Zingbox

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
Philips Healthcare	Philips Enterprise Imaging Domain Controller Philips Enterprise Imaging IntelliSpace PACS Philips Enterprise Imaging Universal Data Manager
Symantec	Symantec Endpoint Detection and Response (EDR) Version 4.1.0 Symantec Data Center Security: Server Advanced (DCS:SA) Version 6.7 Symantec Endpoint Protection (SEP 14) Version 14.2 Symantec Validation and ID Protection Version 9.8.4 Windows
TDi Technologies	TDI Technologies ConsoleWorks Version 5.1-0u1
Tempered Networks	Tempered Networks Identity Defined Networking (IDN) Conductor and HIPSwitch Version 2.1
Tripwire	Tripwire Enterprise Version 8.7
Virta Labs	BlueFlow Version 2.6.4
Zingbox	Zingbox IoT Guardian

Contents

List of Figures

List of Tables

1 Summary

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

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

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory to emulate a medical imaging environment, performed a risk assessment, and developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect the PACS ecosystem. The example implementation, which represents one of many possible solutions and architectures, can be used by any organization that is deploying PACS and medical imaging systems and that is willing to perform its own risk assessment and implement controls based on its risk posture.

For ease of use, the following paragraphs provide a short description of each section of this volume.

Section 1, Summary, presents the challenge addressed by the NCCoE project, with an in-depth look at our approach, the architecture, and the security characteristics we used; the solution demonstrated to address the challenge; benefits of the solution; and the technology partners that participated in building, demonstrating, and documenting the solution. The Summary also explains how to provide feedback on this guide.

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

Section 3, Approach, offers a detailed treatment of the scope of the project and describes the assumptions on which the security platform development was based, the risk assessment that informed platform development, and the technologies and components that industry collaborators gave us to enable platform development.

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

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

Section 6, Functional Evaluation, summarizes the test sequences employed to demonstrate security platform services, the NIST Cybersecurity Framework Functions to which each test sequence is relevant, and the NIST Special Publication (SP) 800-53 Revision 4 controls applicable to the functions being demonstrated.

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

The appendixes provide acronym translations, references, a mapping of the PACS project to the NIST Cybersecurity Framework, and a list of additional informative security references cited in the framework.

1.1 Challenge

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

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

- disruption of the system, leading to
  - inability to render timely diagnosis and treatment
  - inability to access the system for standard use, including inability to schedule procedures
- compromise of image data, leading to incorrect diagnosis and treatment
- compromise of components, allowing malicious actors to use the components as pivot points to attack other parts of the HDO infrastructure

- privacy concerns that may lead to
    - fraudulent or improper use of data
    - patient identity theft

1.2 Solution

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

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

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

1.3 Benefits

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

- improve resilience in the network infrastructure, including limiting a threat actor's ability to leverage components as pivot points to attack other parts of the HDO's environment
- limit unauthorized movement within the HDO enterprise network, to address the potential risk of an "insider threat" or malicious actors who gain network access
- analyze behavior and detect malware throughout the ecosystem to enable HDOs to determine when components evidence compromise and to enable those organizations to limit the effects of a potential threat such as ransomware
- secure sensitive data (e.g., personally identifiable information or protected health information) at rest and in transit, limiting adversarial ability to exfiltrate or expose that data
- consider and address risks that may be identified as HDOs examine cloud solutions as part of managing their medical imaging infrastructure

2 How to Use This Guide

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

This guide contains three volumes:

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

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

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

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

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

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

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

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, NIST SP 1800-24C, to replicate all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not 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 the NCCoE's risk assessment and deployment of a defense-in-depth strategy. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 3.6, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

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

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

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

3 Approach

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

Throughout the PACS project, we collaborated with our NCCoE healthcare Community of Interest and technology and cybersecurity vendors to identify standard medical imaging workflows, identify actors, define interactions between actors and systems, and review risk factors. Based on this analysis, the NCCoE developed an architecture and reference design, identified applicable mitigating security technologies, and designed an example implementation to help better secure the PACS ecosystem. This volume provides the approach used to develop the NCCoE reference solution. Elements include risk assessment and analysis, logical design, build development, test and evaluation, and security control mapping.

To develop the reference solution, we reviewed known vulnerabilities in PACS, the Digital Imaging and Communications in Medicine (DICOM) protocol [2], [3], and medical imaging process flow, leveraging use cases described by Integrating Health Enterprise (IHE) [4]. We examined how the architecture and component integration could be designed to increase the security of the device.

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

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

3.1 Audience

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

3.2 Scope

The NCCoE project focused on securing the environment of the PACS ecosystem but not on reengineering medical devices or altering medical imaging processes themselves. This project has led to a standards-based practice guide that is applicable to the wider healthcare ecosystem. This practice guide has been derived from implementation of a secure PACS in a laboratory environment at the NCCoE that seeks to replicate parts of a typical HDO environment. The project considers PACS users internal to the HDO as well as external users and partners needing access to certain components of the HDO environment.

3.3 Assumptions

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

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

This practice guide identifies controls that may be appropriate for mitigating risks associated with the medical imaging ecosystem made up of PACS and VNA systems. The actual build and example implementation of this architecture occurred in a lab environment at the NCCoE. Although the lab is based on a clinical environment, it does not mirror the complexity of an actual hospital network. It is assumed that any actual clinical environment would represent additional complexity. As such, in addition to the assumptions noted above, we also assume the implementation of pervasive controls, discussed in more detail in Appendix C.

3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [10], states that risk is "a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.”

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations* [11] —publicly available material. The Risk Management Framework (RMF) [9] guidance, as a whole, proved to be invaluable in providing us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

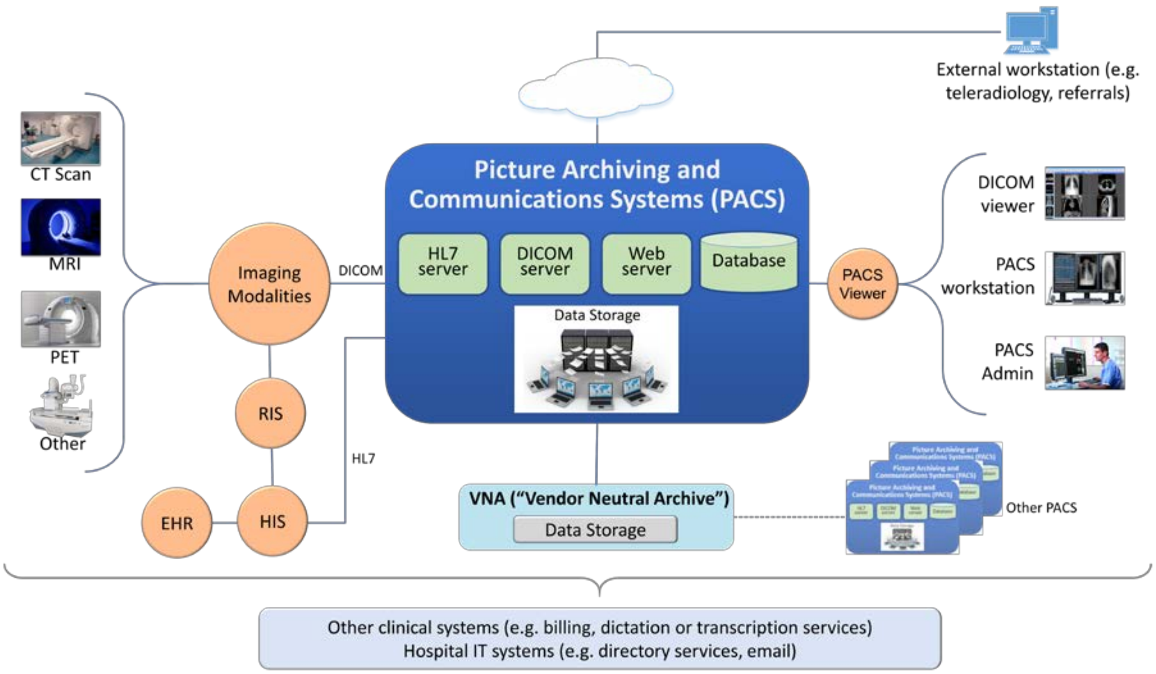
In conducting the risk assessment, this document considers threats and risks grouped under Confidentiality, Integrity, and Availability, commonly referred to as the CIA triad [12].

3.4.1 Establishing the Risk Context

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

Figure 3-1 depicts the notional high-level architecture that bounds the PACS and medical imaging ecosystem [13]. This depiction provides a starting point in understanding the components addressed in this project. Notwithstanding, this project takes a holistic approach in framing the risk context, beyond some of the technology components. This project leverages concepts described in NIST SP 800-160 [5] in defining context for the PACS ecosystem, understanding risk based on context, and selecting appropriate controls when designing the control environment needed to mitigate that contextual risk. NIST SP 800-160, *Systems Security Engineering* [5], identifies concepts of examining system life cycle and components, performing holistic analysis on both technical and nontechnical processes, to deliver “trustworthy” systems. Trustworthiness describes a solution whose objective is to provide “adequate security” related to concerns that may be held by a given stakeholder. “Adequate security” is achieved through considering a system life-cycle process, and it frames the risk context based on processes and interactions with the system and its components [5].

Figure 3-1 Notional High-Level Architecture



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

- workstations used to interact with the medical imaging ecosystem
    - viewer workstations residing within the HDO perimeter
    - viewer workstations residing external to the HDO perimeter, used by remote care specialists
    - workstations used by clinical staff to access peripheral systems, such as Order Entry systems, RIS, HIS, or EHR
- modalities, or medical imaging devices that acquire medical images and forward those to PACS, based on orders typically received from the EHR or HIS and following workflows typically defined by the RIS
- clinical systems that interface with modalities and the PACS environment, supporting medical imaging processes such as scheduling, annotations, or reporting
- interfaces for the PACS that may operate as servers, such as HL7, DICOM, or web
- PACS and VNA application servers

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

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

3.4.2 System Actors

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

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

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

- modalities
- radiology and hospital information systems (RIS and HIS)
- EHRs

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

3.4.3 Use Case Scenarios

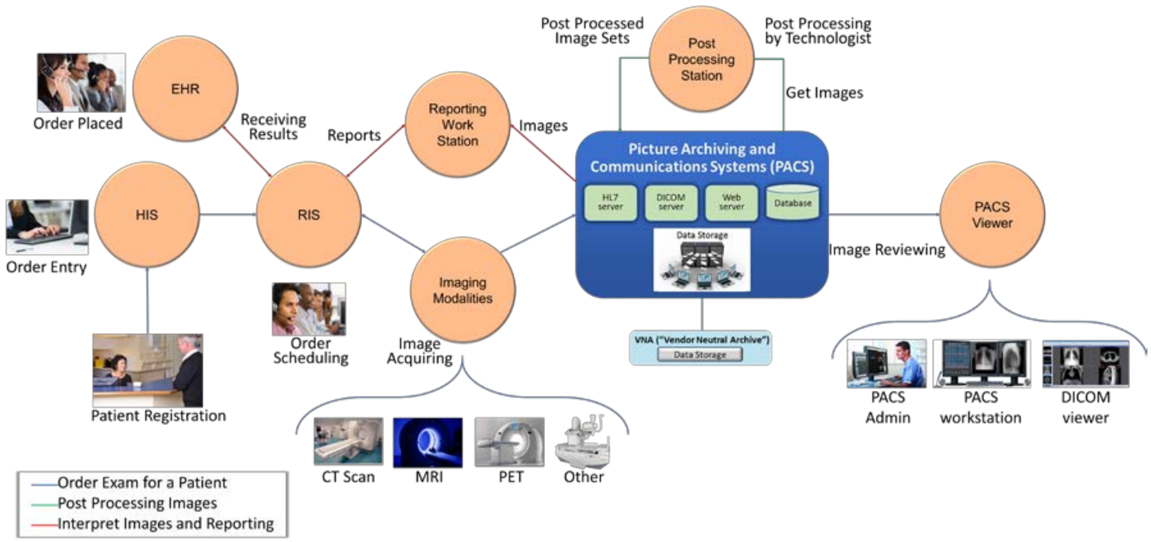
This project assesses risk for the five scenarios [13] described below. Consideration of threats, vulnerabilities, likelihoods, and impacts on medical imaging operations under these scenarios has contributed to the risks documented in Section 3.4.6.

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

3.4.3.1 Sample Radiology Practice Workflows

Scenario One, shown in Figure 3-2, starts with registration of a patient who requires that an imaging procedure be performed [13]. For the purposes of this project, the assumption is that the patient is registered into the EHR, has appropriate identifiers to be admitted as a patient, and is viable to receive procedures. The scenario follows the process flow that begins at scheduling the procedure, having the image acquired, and allowing the care team to analyze and diagnose. The assumption is that all modality devices and clinical staff are on premises, within the boundaries of the HDO. Patient information is conveyed using the Health Level 7 (HL7) [14] protocol (e.g., patient registration and order entry messages). Medical imaging devices would interact with the PACS/VNA by using DICOM [2], [3].

Figure 3-2 Scenario One: Sample Radiology Practice Workflows



The scenario's processes are as follows:

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

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

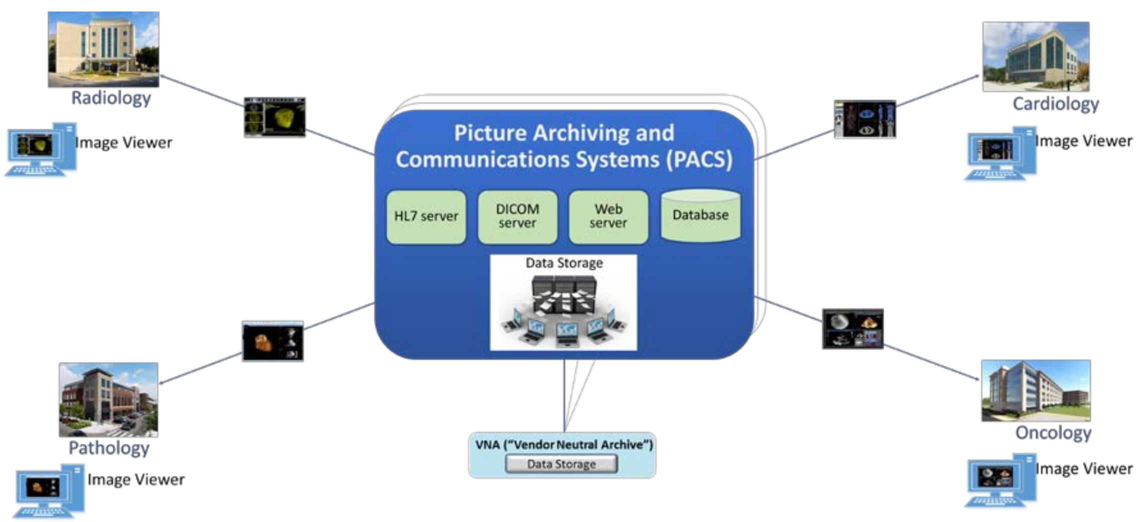
Systems of Interest: order entry, RIS, medical imaging devices, viewer workstations, PACS

Protocols used: DICOM, web (e.g., https), HL7, HIP

3.4.3.2 Image Data Access Across the Enterprise

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

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



In demonstrating that different groups and technologies are involved, this project uses a convention on showing variables as "_a" or "_b." This allows us to show the separation between two components that may be similar in function but are separate, i.e. "component_a" versus "component_b."

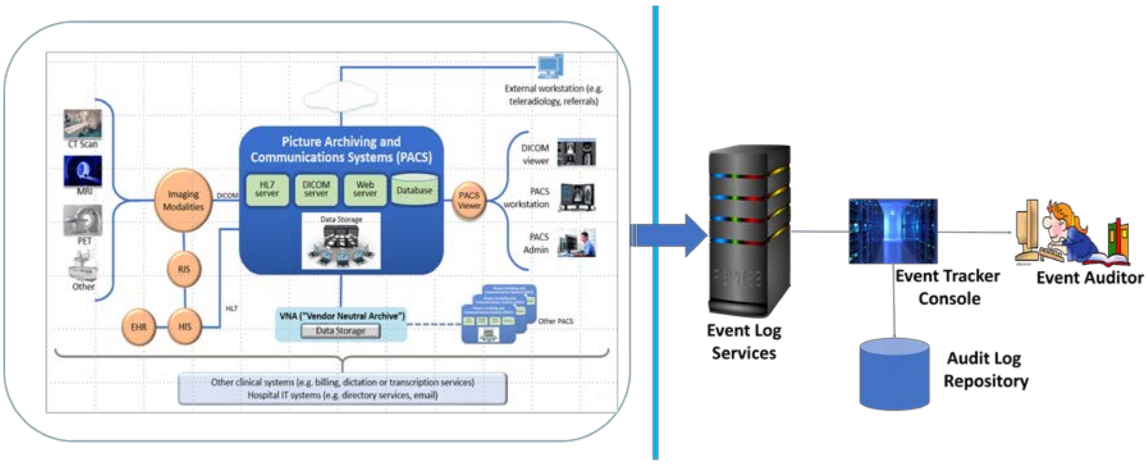
Stakeholders: medical imaging staff_a, medical imaging staff_b, healthcare technology management professionals, PACS_a, PACS_b, VNA

Systems of Interest: image viewer_a, image viewer_b, PACS_a, PACS_b, VNA

3.4.3.3 Accessing, Monitoring, and Auditing

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

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



Identities would be established for users (humans who interact with the system), as well as for devices and systems. Assumptions in this scenario are that individuals have been appropriately identity-proofed and are provisioned accounts with which they may access and use viewer applications. Given that identities and accounts would be provisioned for both human and machine actors, interaction with the system will perform authentication wherein, as actors present credentials to perform actions, challenges must be satisfied. Authentication may involve exchange of passwords, passcodes, biometrics, or use of cryptographic keys to validate the actor. Actions, including presentation of credentials, will be recorded in a log file.

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

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

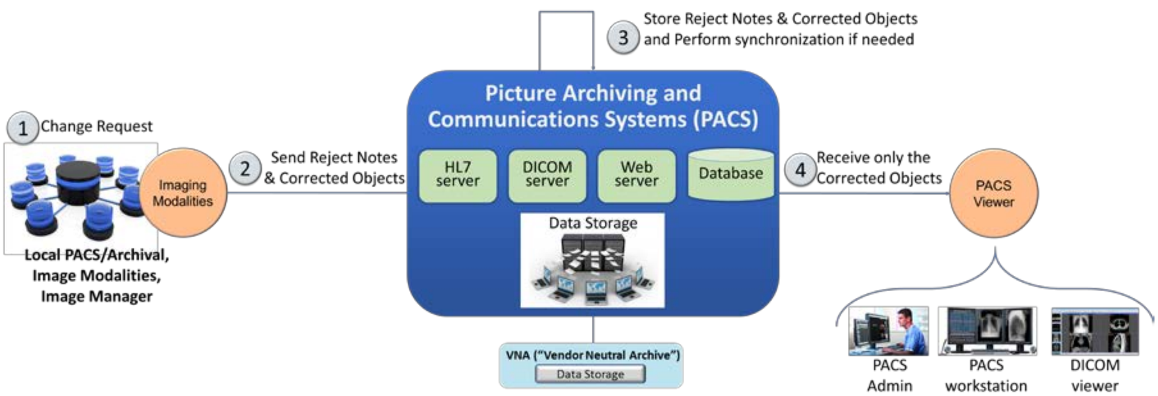
Systems of Interest: directory servers, user account systems, digital certificate servers

Protocols: PKI (associated protocols such as Certificate Management Protocol, http, https), domain name system (DNS), Active Directory

3.4.3.4 Imaging Object Change Management

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

Figure 3-5 Scenario Four: Imaging Object Change Management



<u>Stakeholders</u>: medical imaging clinicians

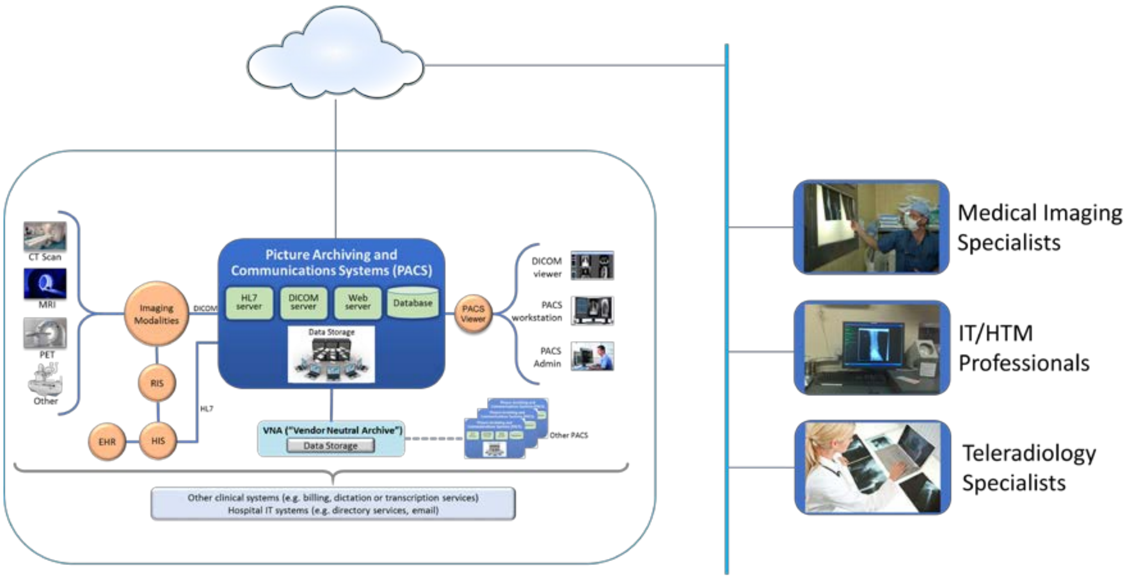
<u>Systems of Interest</u>: PACS, VNA

<u>Protocols</u>: HL7, http, https

3.4.3.5 Remote Access

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

Figure 3-6 Scenario Five: Remote Access



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

Systems of Interest: PACS, VNA

3.4.4 Threats

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

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

Table 3-1 Threats

C/I/A	Threat Event	Description	Unmitigated Likelihood
C	Abuse of credentials or insider threat	Aberrant behavior from an individual who may have legitimate access to the system, however, may leverage granted privileges for unintended purposes.	High

C/I/A	Threat Event	Description	Unmitigated Likelihood
C	Credential compromise	Adversary obtains the means to use credentials provisioned for others. Credentials may involve other users or those used by systems for process or data handling.	High
C	Data exfiltration	The removal of data to an unintended destination. Exfiltration may represent the unauthorized movement of data from one system to uncontrolled physical storage media or may represent movement to uncontrolled virtual destinations such as volatile memory, or to unknown storage such as cloud-hosted or virtual destinations.	High
I	Data in-transit disruption	Distortion or alteration of data in transit that results in information that may not be interpreted as valid information. The attack type seeks to distort or alter data in mid communication stream. Received data may be unintelligible or otherwise unreadable when it arrives at the destination.	Moderate
I	Data alteration	Unauthorized changes to the content of the data. Data alteration may not be superficially detected in that the image may appear legitimate. The attack type seeks to make changes when data are in an at-rest state.	Moderate
I	Time synchronization	System components may rely on synchronizing internal clocks to ensure network session and data integrity. Attacks may seek to alter time stamping or ability for systems to synchronize with an authoritative time source.	Moderate
I	Introduction of malicious software	Introduction of foreign, unauthorized code into a system. Malicious software deployments may affect servers or workstations or both. *Server components:* Unauthorized code may be deployed and run on server components. *Workstations:* Unauthorized code may be deployed and run on workstations connected to PACS ecosystem.	High

C/I/A	Threat Event	Description	Unmitigated Likelihood
I	Unintended use of service	Operating systems may consist of services or processes used to support a system's functionality; however, they may be used to perform unintended functions.	High
A	Data storage disruption	Physical media or file space disruption evidenced by prolonged read/write access times, or corrupted data thereby causing unavailability of service.	High
A	Network disruption	Network disruption attacks may take the form of several different approaches. Below are some disruption approaches that this practice guide will examine: *Denial of service (DoS) or packet flooding:* the introduction of above normal network traffic that saturates network infrastructure components' ability to deliver network communication appropriately *Routing:* inefficient network traffic flow *DNS or name resolution:* Networked hosts are associated with "friendly names" to facilitate interaction; however, name resolution to internet protocol (IP) addressing may be disrupted to make host discovery difficult. Similar or soundalike host and domain names may be introduced to compound confusion. *ARP:* Address Resolution Protocol (ARP) is a localized means by which hosts resolve IP addresses to Media Access Control (MAC) addresses stored in host tables. Corruption of ARP tables may result in network traffic being misdirected or in legitimate devices being unable to connect to the network.	High
	Backup/recovery disruption	Measures that organizations use as a failover or recovery from a prolonged outage may be compromised, e.g., through introduction of malicious software to backup storage media, inability to read and restore from backup media, or introduction of a supply chain compromise	High

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

3.4.5 Vulnerabilities

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

Table 3-2 Vulnerabilities

Vulnerability Description	Vulnerability Severity (Qualitative)	Predisposing Condition	Pervasiveness of Predisposing Condition (Qualitative)
Weak or no system use training	Moderate	Workforce may not be aware or may not have received training on appropriate use or configuration of the system. Users may not have sufficient awareness of action consequences.	High
Weak or no security training	High	Workforce may not be aware of procedures of how to report anomalies. Security teams may not have sufficient training on how to investigate or may not have procedures to address security incidents.	Moderate
Deficient supply chain security controls	High	Organizations may not be aware of third-party practices or downstream suppliers who may implement technology into the healthcare organization’s environment.	High

Vulnerability Description	Vulnerability Severity (Qualitative)	Predisposing Condition	Pervasiveness of Predisposing Condition (Qualitative)
Deficient separation of duties	High	Privileged users may have extended responsibility to ensure system operations. This may be embodied by using “super user” identities that allow escalated access to systems, data, and logging features.	High
Weak or no identity management	High	Organizations may have deficient identity proofing or review processes.	Moderate
Weak or no authentication controls	Very High	This may be evidenced through trivial forms of authentication or using credentials with no authentication requirement. Also found in this category is the use of default credentials that tend to be generally discoverable.	Very High
Permissive privilege	Very High	Credentials may be established without examining the minimum necessary to perform the required function. As such, credentials may exist with access to perform actions outside the work scope. Note that permissive privilege may extend to system services whereby services may run as “root” or “administrator,” granting that credential the ability to perform inappropriate actions.	Very High
Out-of-date or unmanaged services	High	Operating systems, other third-party software, and the PACS application itself include a variety of services, allowing appropriate functionality. Over time, flaws, in the form of bugs (coding errors) or the use of libraries or binaries determined to have security weakness, may be discovered and subsequently addressed, resulting in patches or updates. Systems that do not apply those	Very High

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

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

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

3.4.6 Risk

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* defines risk as “a measure of the extent to which an entity is threatened by potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” [10]. Risk is the adverse impact; that is, risk is the result when a threat (attack) successfully leverages one or more vulnerabilities. As organizations consider risk, they should note that risk is not discrete; that is, a successful attack may involve multiple threats or take advantage of a combination of vulnerabilities. Also, when an organization suffers from an attack campaign, the organization may realize multiple adverse outcomes.

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

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

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

Table 3-3 Risk

C/I/A	Risk	Description	Risk Level
C	Fraudulent use of health-related information	Should unauthorized individuals retrieve protected health information (PHI) that includes health insurance information, those actors may be able to submit fraudulent claims and receive reimbursement from a payer for services not rendered to the patient.	High
C	Identity theft and fraudulent use of PHI	Individuals may receive exfiltrated data to commit identity theft in obtaining healthcare. Fraudulent individuals may receive health services leveraging a victim patient's information and, as a result, introduce false information into a victim patient's medical history. This may result in a patient safety concern, in that treatments performed for the fraudulent individual would be captured in the victim patient's history, potentially leading to future inaccurate diagnoses when that patient seeks legitimate care.	High
I	Patient misdiagnosed based on interpretations made from unauthorized changes to medical images	Patient safety may be affected based on imaging data integrity. Should images be altered, care providers may render inaccurate diagnoses and therefore delay appropriate treatment.	High
A	Patient diagnoses disrupted based on timeliness disruption, leading to patient safety concerns	Patients may have conditions that require timely and accurate diagnosis to achieve optimum mortality rates. Communications disruptions that corrupt or deny data may adversely affect this, so that care teams are not able to make a timely	High

C/I/A	Risk	Description	Risk Level
		diagnosis, and patients may have to repeat imaging processes.	
A	Process disruption due to malware	PACS or other systems within the ecosystem may succumb to ransomware or other forms of malware, rendering those systems and associated data unavailable. Ransomware may render full system unavailability, while other forms of malware may delay processing capability or introduce data integrity risk. As a result, the HDO may not be able to treat patients appropriately or make diagnoses. Delays may result in patient safety concerns.	High
A	Systemic disruption due to component compromise	Individual components within the PACS ecosystem may be compromised and used as pivot points from which other parts of the HDO network may be attacked. This may result in delay in patient care.	High

The project identified the risks above as requirements that needed to be addressed in the lab environment. Organizations should note that the tables offered here are samples and notionally representative. Characterizing threats, vulnerabilities, and risk is contextual. HDOs with different security deficiencies or unique threat situations in their systems and network environments may find their categorization to be different than what was identified for this project. HDOs need to consider their unique profile when categorizing vulnerabilities, threats, and risk. Only then can an adequate set of security controls be determined for their unique environment. This project identified these risk elements and scored them as such, based on the assessment performed on the lab environment.

3.5 Security Control Map

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

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

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

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

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		ID.RA-6: Risk responses are identified and prioritized.	PM-4 PM-9	DTBK SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(B) 164.314(a)(2)(i)(C) 164.314(b)(2)(iv)	Clause 6.1.3
PROTECT (PR)	Identity Management and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	AC-1 AC-2 IA-1 IA-2 IA-3 IA-4 IA-5 IA-6 IA-7 IA-8 IA-9 IA-10 IA-11	ALOF AUTH EMRG NAUT PAUT	45 C.F.R. §§ 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i)	A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.6 A.9.3.1 A.9.4.2 A.9.4.3
		PR.AC-2: Physical access to assets is managed and protected.	PE-2 PE-3 PE-4 PE-5 PE-6 PE-8	PLOK TXCF TXIG	45 C.F.R. §§ 164.308(a)(1)(ii)(B) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.310(a)(1) 164.310(a)(2)(i) 164.310(a)(2)(ii)	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.5 A.11.2.6 A.11.2.7 A.11.2.8

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.AC-3: Remote access is managed.	AC-1 AC-17 AC-19 AC-20 SC-15	ALOF AUTH CSUP EMRG NAUT PAUT	45 C.F.R. §§ 164.308(a)(4)(i) 164.308(b)(1) 164.308(b)(3) 164.310(b) 164.312(e)(1) 164.312(e)(2)(ii)	A.6.2.1 A.6.2.2 A.11.2.6 A.13.1.1 A.13.2.1
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	AC-1 AC-2 AC-3 AC-5 AC-6 AC-14 AC-16 AC-24	ALOF AUTH CNFS EMRG NAUT PAUT	45 C.F.R. §§ 164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i)	A.6.1.2 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	AC-4 AC-10 SC-7	MLDP NAUT	45 C.F.R. §§ 164.308(a)(4)(ii)(B) 164.310(a)(1) 164.310(b) 164.312(a)(1) 164.312(b) 164.312(c)	A.13.1.1 A.13.1.3 A.13.2.1 A.14.1.2 A.14.1.3

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	AC-7 AC-8 AC-9 AC-11 AC-12 AC-14 IA-1 IA-2 IA-3 IA-4 IA-5 IA-8 IA-9 IA-10 IA-11	ALOF AUTH CSUP EMRG NAUT PAUT	45 C.F.R. § 164.308(a)(4)	A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.2 A.9.4.3 A.18.1.4
	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected.	MP-8 SC-12 SC-28	IGAU MLDP NAUT SAHD STCF TXCF	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(b)(1) 164.310(d) 164.312(a)(1) 164.312(a)(2)(iii) 164.312(a)(2)(iv)	A.8.2.3
		PR.DS-2: Data-in-transit is protected.	SC-8 SC-11 SC-12	IGAU NAUT STCF TXCF TXIG	45 C.F.R. §§ 164.308(b)(1) 164.308(b)(2) 164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii) 164.314(b)(2)(i)	A.8.2.3 A.13.1.1 A.13.2.1 A.13.2.3 A.14.1.2 A.14.1.3

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.DS-5: Protections against data leaks are implemented.	AC-4 AC-5 AC-6 PE-19 PS-3 PS-6 SC-7 SC-8 SC-13 SC-31 SI-4	AUTH IGAU MLDP PLOK STCF TXCF TXIG	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.310(b) 164.310(c) 164.312(a)	A.6.1.2 A.7.1.1 A.7.1.2 A.7.3.1 A.8.2.2 A.8.2.3 A.9.1.1 A.9.1.2 A.9.2.3 A.9.4.1 A.9.4.4 A.9.4.5 A.10.1.1 A.11.1.4 A.11.1.5 A.11.2.1 A.13.1.1 A.13.1.3 A.13.2.1 A.13.2.3 A.13.2.4 A.14.1.2 A.14.1.3
		PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity.	SC-16 SI-7	IGAU MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(b) 164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(i)	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3 A.14.2.4

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/ industrial control systems is created and maintained, incorporating security principles (e.g., concept of least functionality).	CM-2 CM-3 CM-4 CM-5 CM-6 CM-7 CM-9 SA-10	CNFS CSUP DTBK NAUT	45 C.F.R. §§ 164.308(a)(8) 164.308(a)(7)(i) 164.308(a)(7)(ii)	A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4
		PR.IP-3: Configuration change control processes are in place.	CM-3 CM-4 SA-10	CNFS CSUP DTBK	45 C.F.R. §§ 164.308(a)(8) 164.308(a)(7)(i) 164.308(a)(7)(ii)	A.12.1.2 A.12.5.1 A.12.6.2 A.14.2.2 A.14.2.3 A.14.2.4
		PR.IP-4: Backups of information are conducted, maintained, and tested.	CP-4 CP-6 CP-9	DTBK PLOK	164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(D) 164.310(a)(2)(i) 164.310(d)(2)(iv)	A.12.3.1 A.17.1.2 A.17.1.3 A.18.1.3
		PR.IP-6: Data is destroyed according to policy.	MP-6	DIDT	45 C.F.R. §§ 164.310(d)(2)(i) 164.310(d)(2)(ii)	A.8.2.3 A.8.3.1 A.8.3.2 A.11.2.7

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

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.PT-4: Communications and control networks are protected.	AC-4 AC-17 AC-18 CP-8 SC-7 SC-19 SC-20 SC-21 SC-22 SC-23 SC-24 SC-25 SC-29 SC-32 SC-36 SC-37 SC-38 SC-39 SC-40 SC-41 SC-43	AUTH MLDP PAUT SAHD	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(a)(1) 164.312(b) 164.312(e)	A.13.1.1 A.13.2.1 A.14.1.3
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	AC-4 CA-3 CM-2 SI-4	CNFS CSUP MLDP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(b)	A.12.1.1 A.12.1.2 A.13.1.1 A.13.1.2

NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 4**	**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	AU-6 CA-7 IR-4 SI-4	AUDT MLDP	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(6)(i) 164.308(a)(6)(i)	A.12.4.1 A.16.1.1 A.16.1.4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	AU-6 CA-7 IR-4 IR-5 IR-8 SI-4	AUDT MLDP SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.308(a)(8) 164.310(d)(2)(iii)	A.12.4.1 A.16.1.7
		DE.AE-5: Incident alert thresholds are established.	IR-4 IR-5 IR-8	DTBK MLDP SGUD	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(6)(i) 164.308(a)(6)(i)	A.16.1.4
	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events.	AC-2 AU-12 CA-7 CM-3 SC-5 SC-7 SI-4	AUDT CNFS CSUP MLDP NAUT	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(2) 164.308(a)(3)(ii)(A)	N/A

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

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

3.6 Technologies

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

Table 3-5 Products and Technologies

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
PACS and VNA	Hyland Acuo Vendor Neutral Archive Version 6.0.4	▪ Provides access to medical images and documents ▪ Stores and retrieves images in a standard format to be accessed by various vendor-neutral systems	PR.AC-1 PR.AC-4 PR.DS-2 PR.IP-4 PR.PT-1
	Hyland NilRead Enterprise Version 4.3.31.98805	▪ Provides medical image viewing and manipulation	PR.AC-1 PR.DS-2 PR.PT-1
	Hyland PACSgear Version 4.1.0.64	▪ Provides ability to capture and share medical images ▪ Provides ability to scan and share medical documents	PR.AC-1 PR.DS-2 PR.PT-1
	Philips Enterprise Imaging Domain Controller	▪ Provides role-based user-access control	PR.AC-1
	Philips Enterprise Imaging IntelliSpace PACS	▪ Provides management of medical images through access and collaboration	PR.DS-2 PR.IP-4 PR.PT-1
	Philips Enterprise Imaging Universal Data Manager	▪ Provides web-based DICOM integration ▪ Provides image lifecycle management	PR.DS-2 PR.IP-4 PR.PT-1
	DCM4CHEE	▪ Open source PACS solution ▪ Allows the lab to demonstrate data-in-transit workflow control	N/A

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
	DVTk Modality Emulator	▪ Open source utility used to demonstrate clinical workflow and interaction with medical imaging devices ▪ Allows the lab to demonstrate data-in-transit workflow between clinical systems and medical devices	N/A
	DVTk RIS Emulator	▪ Open source utility used to demonstrate clinical workflow and interaction with medical imaging devices ▪ Allows the lab to demonstrate data-in-transit workflow between clinical systems and medical devices	N/A
Asset Management	Virta Labs BlueFlow Version 2.6.4	▪ Provides discovery, categorization, grouping, tagging, and identification of medical devices ▪ Provides flexible user-defined risk assessment and scoring ▪ Provides vulnerability management capabilities ▪ Provides reporting on risk and security properties for groups of assets ▪ Provides threat feed for known medical devices	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5 ID.RA-1 ID.RA-5 PR.IP-1
	Clearwater Information Risk Management Analysis	▪ Provides asset inventory management ▪ Provides risk assessment and compliance	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5
	Tripwire Enterprise Version 8.7	▪ Provides security configuration management ▪ Provides file integrity monitoring ▪ Provides patch management	ID.RA-1 ID.RA-5 PR.DS-6 PR.IP-1

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
			PR.IP-3 PR.PT-3
Enterprise Domain and Identity Management	Active Directory	▪ Provides authentication and authorization for users and computers in the domain ▪ Provides authentication and authorization to multiple applications within the environment	PR.AC-1 PR.AC-4 PR.AC-7 PR.PT-3
	DigiCert PKI Platform	▪ Provides SSL/TLS certificates for secure communication between devices ▪ Enables devices to perform data-in-transit encryption ▪ Provides certificate management	PR.AC-1 PR.AC-4 PR.AC-7 PR.DS-2
	Symantec Validation and ID Protection Version 9.8.4 Windows	▪ Integrates with TDi ConsoleWorks using RADIUS ▪ Provides multifactor authentication for remote access	PR.AC-1 PR.AC-3 PR.AC-7
Network Control and Security	Cisco Firepower Management Center (FMC) 6.3.0	▪ Provides console management for Firepower Threat Defense ▪ Provides centralized control over network and communication ▪ Provides network visibility	PR.AC-5 PR.PT-4
	Cisco Firepower Threat Defense (FTD) 6.3.0	▪ Provides intrusion prevention ▪ Provides network segmentation ▪ Provides policy-based network protection	PR.AC-5 PR.PT-4
	Tempered Networks Identity Defined Networking (IDN) Conductor and HIPswitch Version 2.1	▪ Provides network segmentation ▪ Provides end-to-end encryption for device traffic	PR.AC-5 PR.DS-2 PR.PT-4

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
	Zingbox IoT Guardian	▪ Provides passive device discovery and classification ▪ Provides behavioral modeling to identify suspicious behavior ▪ Provides vulnerability assessment	ID.AM-3 ID.RA-1 ID.RA-5 DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-5 DE.CM-1 DE.CM-7
	Forescout CounterACT 8	▪ Provides passive device discovery and profiling ▪ Provides network access control	PR.AC-4 PR.AC-7 PR.PT-4 DE.AE-1 DE.AE-3 DE.CM-1 DE.CM-7
	Symantec Endpoint Detection and Response (EDR) Version 4.1.0	▪ Provides centralized management of threats across endpoint, network, and web traffic	DE.CM-1 DE.CM-4
	Cisco Stealthwatch Version 7.0.0	▪ Provides insight into who and what is on the network ▪ Provides network analysis through machine learning and global threat intelligence ▪ Provides malware detection for encrypted traffic	ID.AM-3 DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-5 DE.CM-1 DE.CM-3 DE.CM-7
Secure Remote Access	TDi Technologies ConsoleWorks Version 5.1-0u1	▪ Provides remote access for external collaborators ▪ Provides logging and monitoring of remote access activities	PR.AC-3 PR.AC-7

Component/ Capability	Product	Function	NIST Cybersecurity Framework Subcategories
Endpoint Protection and Security	Symantec Data Center Security: Server Advanced (DCS:SA) Version 6.7	▪ Provides protection for physical and virtual servers ▪ Provides intrusion detection and prevention ▪ Provides file integrity monitoring	PR.DS-6 PR.IP-3
	Symantec Endpoint Protection (SEP 14) Version 14.2	▪ Provides centralized management of assets through agent-based protection ▪ Provides advanced machine learning and behavioral analysis techniques to identify known and unknown threats ▪ Provides anti-virus (AV) capabilities	DE.CM-4 DE.CM-8

4 Architecture

This practice guide looks at the reference architecture holistically. Food and Drug Administration (FDA) guidance looks at “medical devices that provide functions related to the management of medical images after acquisition, including communication, storage, processing and display (generally known as Picture Archiving and Communications Systems [PACS])” [19]. In addition to the PACS, this project also uses VNA solutions that meet the FDA’s definition of PACS but have other features that HDOs may use to enhance their overall image management ecosystem. This guide understands that healthcare systems interoperate with one another and that the reference architecture needs to accommodate a broad view of the medical imaging ecosystem.

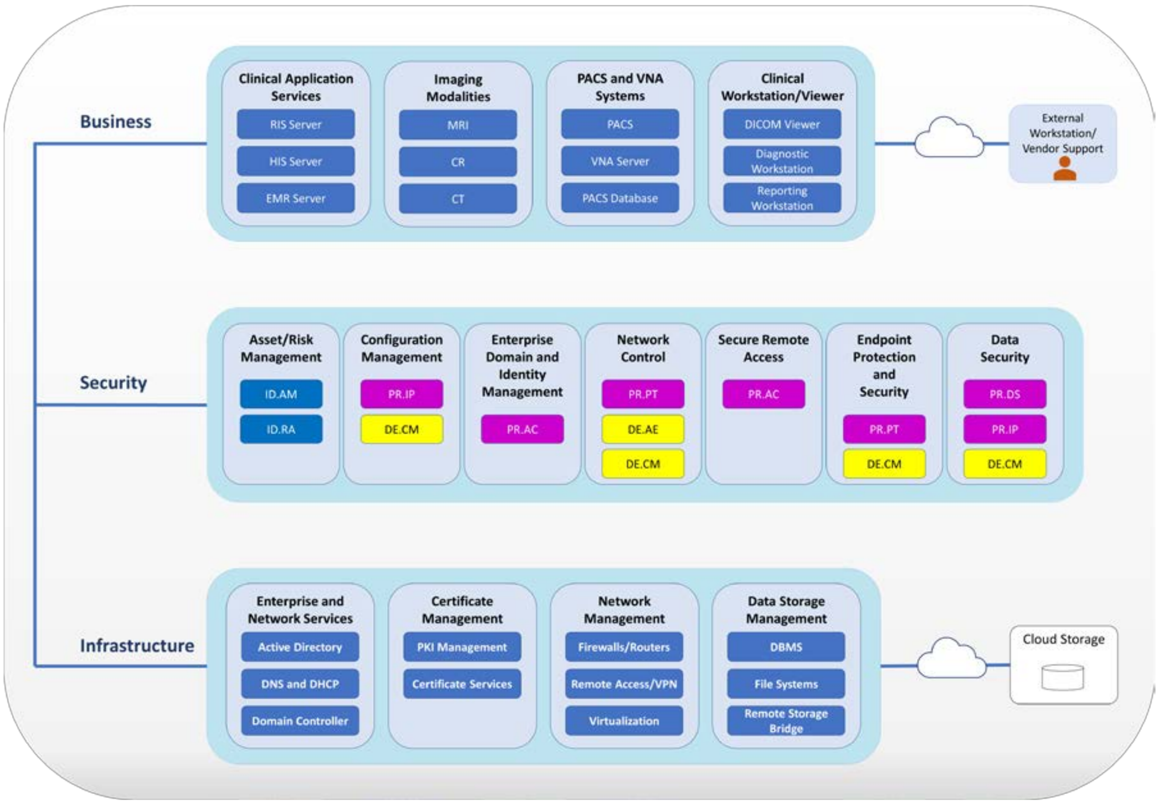
4.1 Architecture Description

Our project’s architecture looks at components from three primary layers:

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

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

Figure 4-1 High-Level PACS Architecture



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

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

In addition to the DICOM standard, PACS uses the HL7 protocol for clinical documentation and image reporting. HL7 defines a markup standard for exchange of health information in a structured format by using a Clinical Document Architecture (CDA) [20].

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

The architecture described for this project implements several zones consisting of:

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

Clinical Workstations are segregated from the standard production network. Clinical workstations are special-purpose devices used to interact with clinical systems. Those devices may use vendor-specified operating systems, applications, and configurations that vary from the HDO standard build. Configuration and patch management may be asynchronous with how the HDO manages its productivity or standard build systems.

Enterprise Network Services are systems used to ensure enterprise operations are segregated into the enterprise network services zone. Services consist of email communications, Active Directory, DNS, and security services such as certificate management.

Modalities: Departments using imaging equipment, generally termed as modalities, would connect those imaging devices to the modalities zone. These devices are medical devices using operating systems that are not consistent with an HDO's baseline. Configuration and patch management are likely asynchronous with how the HDO manages its productivity or standard build systems. For purposes of this project, this zone includes emulated modalities. Images themselves are generated using simulation software.

PACS and VNA Systems: PACS and VNA applications are segregated from clinical applications, general workstations, and storage media. This zone provides the higher-level application functionality to interact with aggregated medical images.

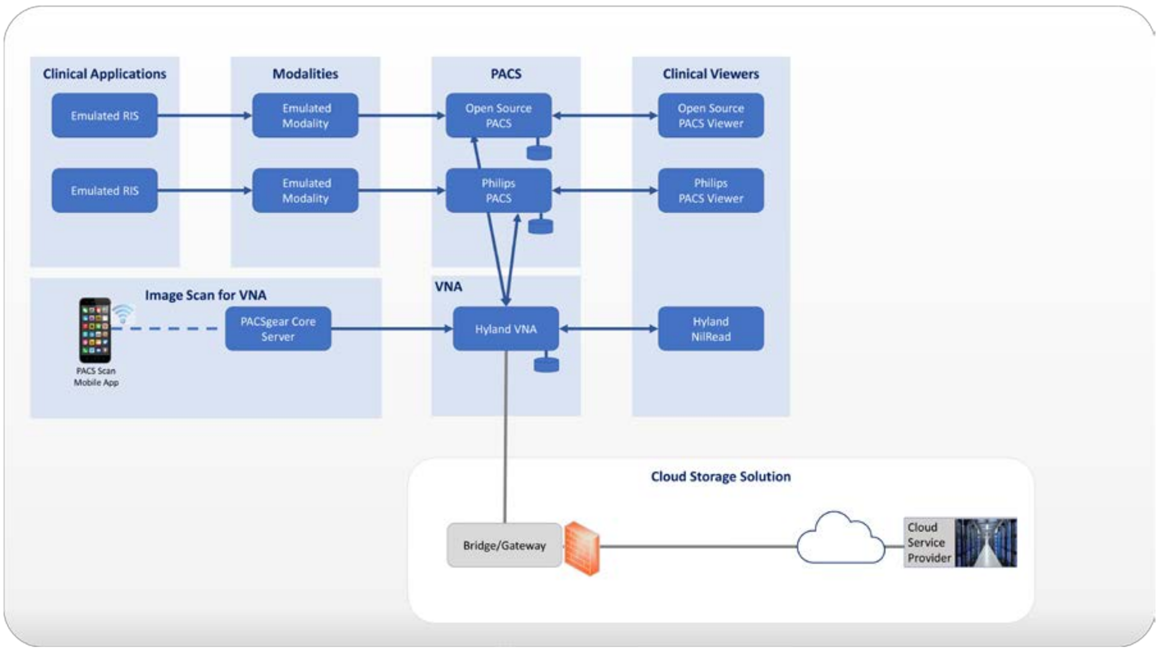
Storage: Large scale storage, such as storage area networks (SANs) or network-attached storage (NAS) devices, would reside in a segregated zone. Data found in this zone may be unstructured, large files and consist of sensitive, personal, or protected health information. Depicted below is the storage zone, which also includes cloud storage, delineated as a separate zone.

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

4.1.1 PACS Ecosystem Components

The PACS ecosystem includes those components that support the clinical processes associated with supporting medical imaging acquisition, review, annotation, and storage. Image acquisition worklists are generated by clinical applications, such as RIS, and applied to associated modalities. Modalities retrieve worklists from the RIS. This practice guide also includes a mobile device used to scan documents and images, and this guide treats this device as a modality. Images are stored and managed by PACS and VNA systems, and images are reviewed and annotated through image viewer applications installed on clinical workstations. In building the lab environment, this practice guide emulated some of the components rather than obtaining full scale solutions. This guide implemented emulated modalities and an emulated RIS. A smartphone device is used for document scanning. The lab environment includes two distinct PACS and a VNA. Also, workstations are deployed that include image viewing software that was provided by the PACS and VNA solutions respectively. Figure 4-2 depicts a high-level view of these components and how we approached implementing them in the lab environment.

Figure 4-2 PACS Ecosystem Components



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

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

4.1.2 Data and Process Flow

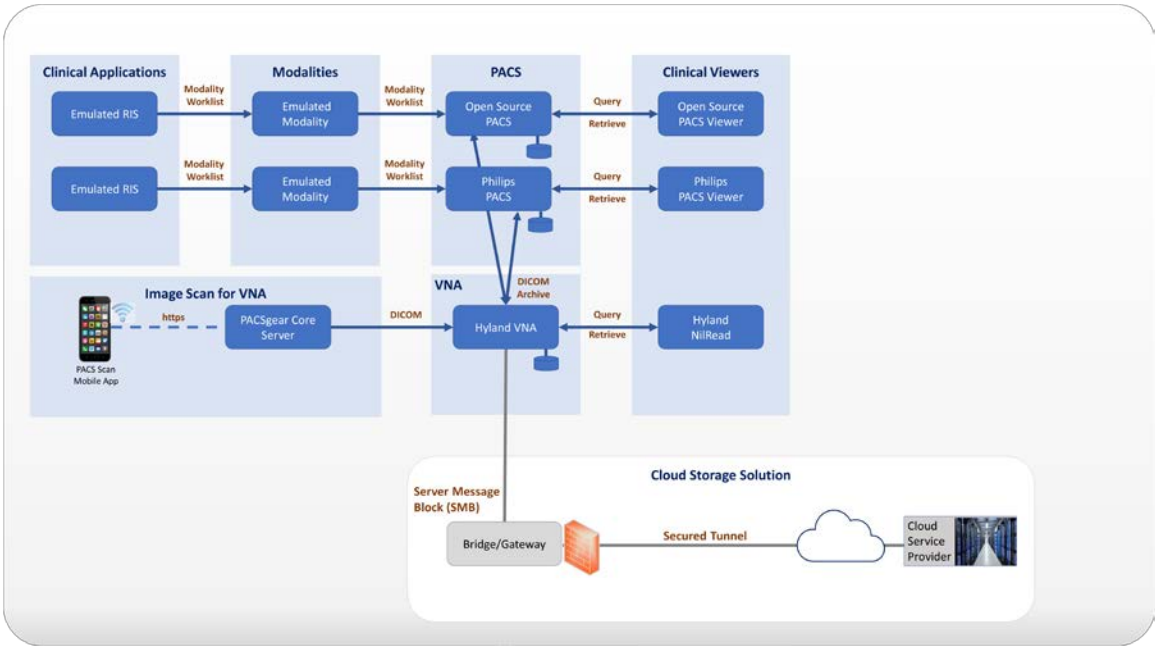
For this project, we examined data and process flows as described in Section 3.4.1, Establishing the Risk Context, that include the following scenarios:

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

The scenarios identify those processes involved when a medical image is acquired, starting with scheduling the patient for a procedure, and follows the life cycle through when the patient interacts with an imaging device to when a medical imaging specialist processes and forwards the annotated image to a clinician for interpretation and diagnosis. Scenarios also examine processes after direct patient interaction, such as when images may be accessed for later review or if images need to be updated.

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

Figure 4-3 PACS Ecosystem Data Communication Flow



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

4.1.3 Security Capabilities

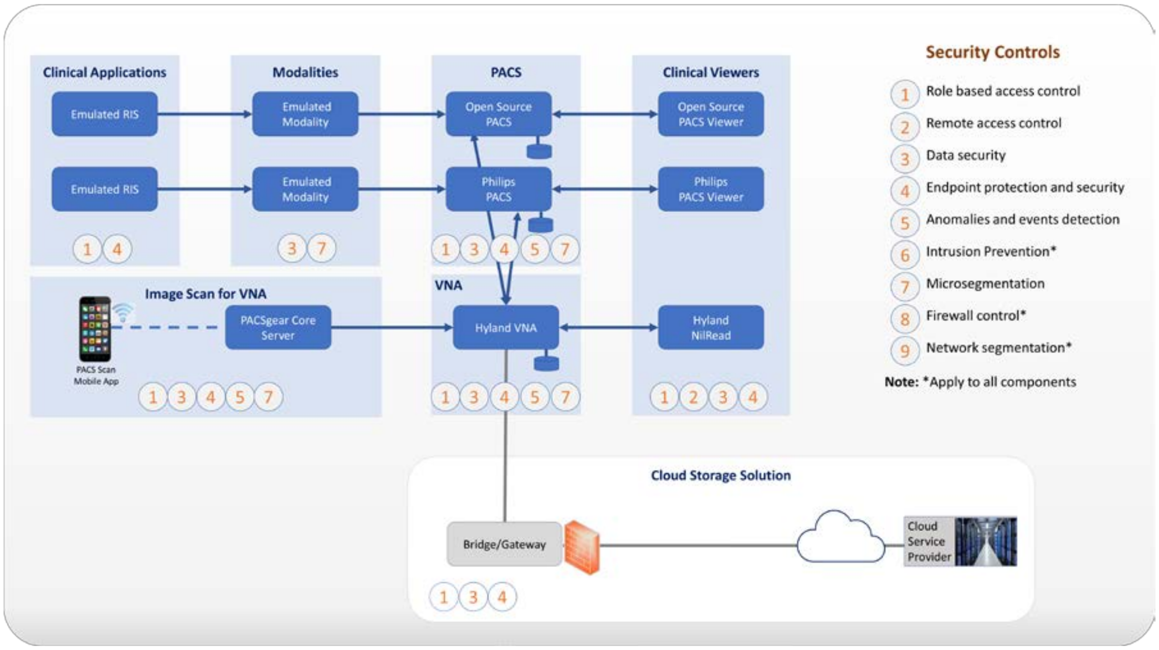
For this project, we build upon the zoned network architecture described in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* [21]. We used the zoning approach as a baseline upon which we could deploy the medical imaging ecosystem infrastructure. On top of the baseline, we selected the following security capabilities that were determined to be relevant to securing our project environment:

- asset and risk management
- enterprise domain and identity management
    - access control
        - privileged access controls

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

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

Figure 4-4 Base Controls on Test Build Components



4.1.4 Asset and Risk Management

Asset management is a critical control that aligns with the Function known as Identify in the NIST Cybersecurity Framework [8]. For this project, IT general assets are assumed to be controlled through a pervasive control such as a governance, risk, and compliance (GRC) solution, e.g., the Clearwater Information Risk Management Analysis tool, addressing the core infrastructure. Medical imaging devices may fall outside the scope of IT general assets for many HDOs. As such, this project implements Virta Labs BlueFlow for asset and inventory management for medical imaging devices. BlueFlow captures inventory, configuration, and patch management information [16], [22], [23].

4.1.5 Enterprise Domain and Identity Management

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

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

Medical devices and systems may also have identities, where authentication is performed using digital certificates or other unique identifiers such as host identifiers or MAC addresses.

4.1.5.1 Access Control

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

4.1.5.1.1 Privileged Access Management

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

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

4.1.5.1.2 User Authentication

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

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

4.1.5.1.3 Device and System Authentication

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

For systems authentication, this project used digital certificates. Digital certificates were deployed to the PACS and VNA servers as well as to a mobile device where we installed software used to scan documents and images that would be added to our medical imaging store.

4.1.5.1.4 Data Access Control

PACS and VNA solutions often support a “multi-tenant” concept to allow for different departments, clinics, or hospitals within a larger healthcare system. These applications may implement or integrate with directory services that allow solutions administrators to provide access based on role or business function. This project used role-based access control capabilities found in the Philips IntelliSpace and Hyland Acuo systems.

4.1.6 Network Control and Security

This project continues with concepts established in NIST SP 1800-8, implements network zoning and segmentation with VLANs, and builds on the concept by implementing several tools to advance protective and detective capabilities. As examples of these enhancements, this project deploys a next-generation firewall, introduces microsegmentation, and implements behavioral analytics in its network control and security in its approach. Subsections below provide additional information on these topics.

4.1.6.1 Network Segmentation and VLANs

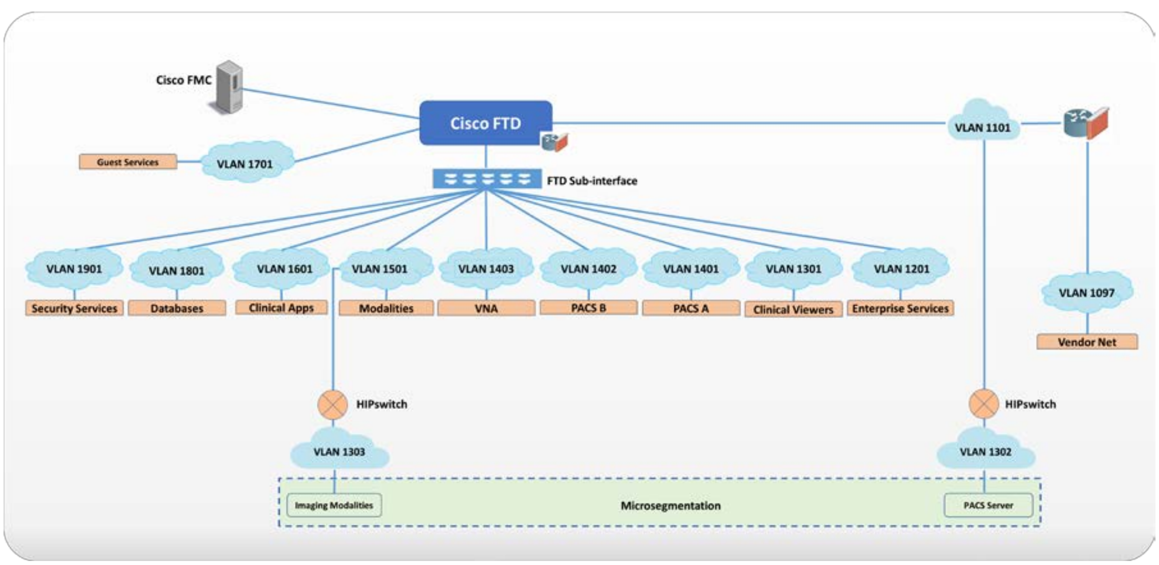
The PACS ecosystem is made up of a variety of different devices with independent requirements to ensure proper functionality. While some devices may require network access to remote services, others may operate effectively with limited connectivity outside their subnet. To meet these needs, we implemented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

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

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

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

Figure 4-5 NCCoE Lab Environment Network Architecture



4.1.6.2 Firewall and Control Policies

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

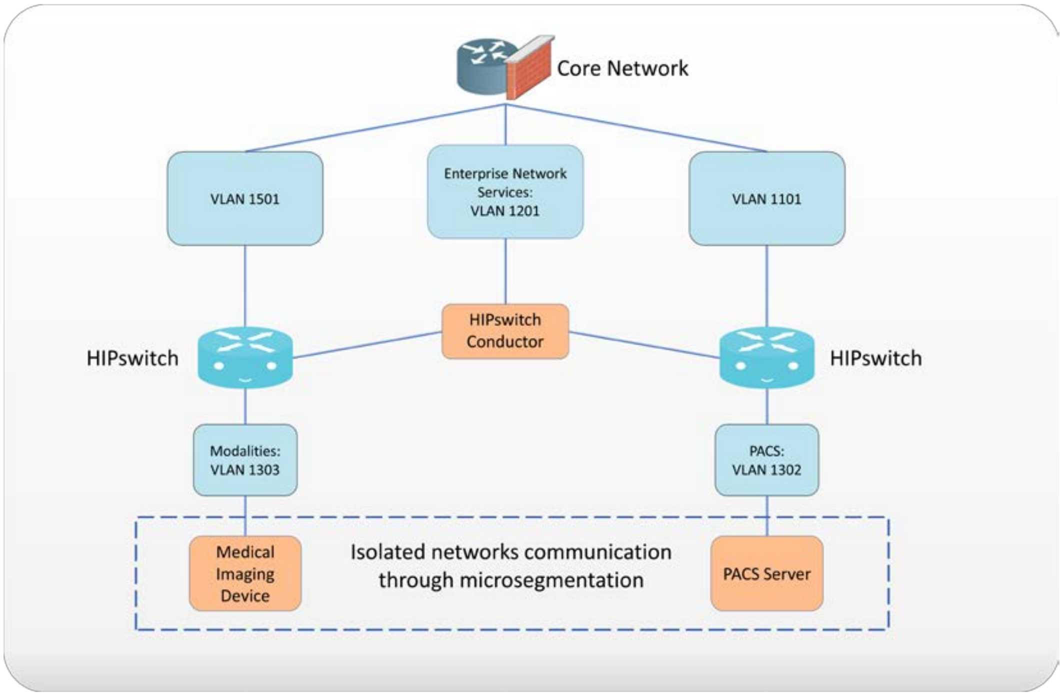
As network and application attacks become more advanced, network controls should be enhanced beyond stateful traffic filtering. NGFW goes beyond ports, protocols, and IP addresses, providing standard policy-based protection, while including more advanced tools such as intrusion prevention systems, application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

4.1.6.3 Microsegmentation

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

Our project implemented microsegmentation through Tempered Networks' HIP solution that includes HIPswitches, implementing HIP, as described in Internet Engineering Task Force Request for Comments (RFC) 4423 [27]. HIP provides a cryptographically defined host identifier bound to endpoints rather than IP addresses. Network traffic between HIP-enabled endpoints traverses a series of HIPswitches deployed in the lab network infrastructure, creating a cloaked network that operates on top of the physical network. The cloaked network uses advanced encryption standard (AES)-256 encryption to secure data in transit and uses secure hash algorithm (SHA)-256 to authenticate data packets from HIP-enabled endpoints [28], [29], [30]. Figure 4-6 below depicts the microsegmentation architecture deployed in the project's test build.

Figure 4-6 Microsegmentation Architecture



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

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

For this project's architecture, it was important to secure this line of communication and ensure these devices were properly protected from potential threats. To accomplish this, the project established two identity-defined perimeters on two separate VLANs. The project then placed a modality behind one perimeter and a PACS behind the other. These perimeters were configured to allow only authorized traffic between them, meaning the modality was allowed to communicate only with the PACS and vice versa. Additionally, all traffic between the two perimeters was encrypted, ensuring the data were secure in-transit.

4.1.6.4 Anomalies and Events Detection (Behavioral Analytics)

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

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

4.1.6.5 Intrusion Detection and Prevention Systems

Components managed through an HDO's IT operations team would implement traditional mechanisms to perform malware detection, vulnerability scanning, and remediation. This project involved several workstations (e.g., image viewing devices), as well as servers that may operate traditional operating systems. Host-based agents are deployed, as appropriate, to permit the IT team to perform regular vulnerability scanning for those non-modality systems. This project implemented Symantec Endpoint Protection on image viewing workstations. Also, the project implemented the Cisco Firepower NGFW that included a network-based intrusion prevention mechanism [31].

4.1.7 Endpoint Protection and Security

This project addressed endpoint protection and security through device hardening and configuration controls and by monitoring for malware. Solutions were deployed to server and workstation endpoints. The project also used a tool to monitor server configurations to assure that only authorized changes were made, therefore maintaining server configuration integrity.

4.1.7.1 Device Hardening and Configuration

Tripwire Enterprise was deployed on server components (e.g., the Hyland Acuo server and the Philips IntelliSpace server) to address device hardening and configuration management, as well as implementing whitelisting.

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

In conjunction with HIPS, critical servers in the reference architecture are protected with a file integrity monitoring (FIM) system. This system monitors file system changes, looking for suspicious changes. The FIM system is also used to do policy compliance evaluation to ensure compliance of the critical servers with the HDO policies.

4.1.7.2 Malware Detection

An endpoint-based malware detection system commonly referred to as antivirus software is used to prevent, detect, and remove malicious software from systems. This function is critical to protecting the systems that healthcare professionals use to interact with the PACS, such as the imaging workstations. The antivirus software implemented in our reference architecture builds upon the traditional role that antivirus software performs by analyzing software for suspicious behavior, performing firewall functions, and allowing custom policy-based enforcement. These added functions enhance the ability for HDOs to respond to the threat of malicious software on healthcare systems. Our project deployed the Symantec Endpoint Protection solution on workstations hosting our DICOM image viewers.

A network-based malware detection system, commonly referred to as an intrusion detection system (IDS), is designed to detect malicious activity over the network. In our reference architecture, the IDS is designed to interface directly with the manager of the endpoint-based malware detection system. This gives the IDS the ability to use data collected from the endpoint to better detect malicious activity on the network [31].

4.1.8 Data Security

This project considered challenges associated with data loss and data alteration. A noted challenge in looking at the medical imaging ecosystem is the diversity of data types that may be prone to varying threat types, with compromise resulting in different adverse outcomes. This project examined data flows between the implemented components and identified a need to secure data in-transit and data at-rest.

4.1.8.1 Data Encryption (at-rest and in-transit)

No specific storage solution was implemented for this project, however, the need for data-at-rest protection was identified. This practice guide recommends referring to NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events* [32], for measures that address backup and recovery. The PACS and VNA solutions used in this project were implemented on Windows servers, and this practice guide recommends implementing secure server message block (SMB) best practices, e.g., as provided by Department of Homeland Security Cyber Infrastructure Security Agency (CISA) [33].

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

Modalities communicating to the PACS and VNA are authenticated using HIP, which also provides for network encryption. HIP employs AES-256 encryption [28], [29], [30] to secure network sessions. By deploying HIP, this project sought to defend against network-borne attacks, including man in the middle attacks where data may be altered in transit.

When multiple PACS data are aggregated into the VNA, the project enabled TLS tunneling. TLS uses DigiCert TLS certificates to implement AES-256 network encryption [29], [30], [34]

Image viewers, as well as mobile devices using Hyland's PACSgear scanning tool, use https/TLS when connecting and communicating to the VNA or PACS respectively [34].

4.1.9 Remote Access

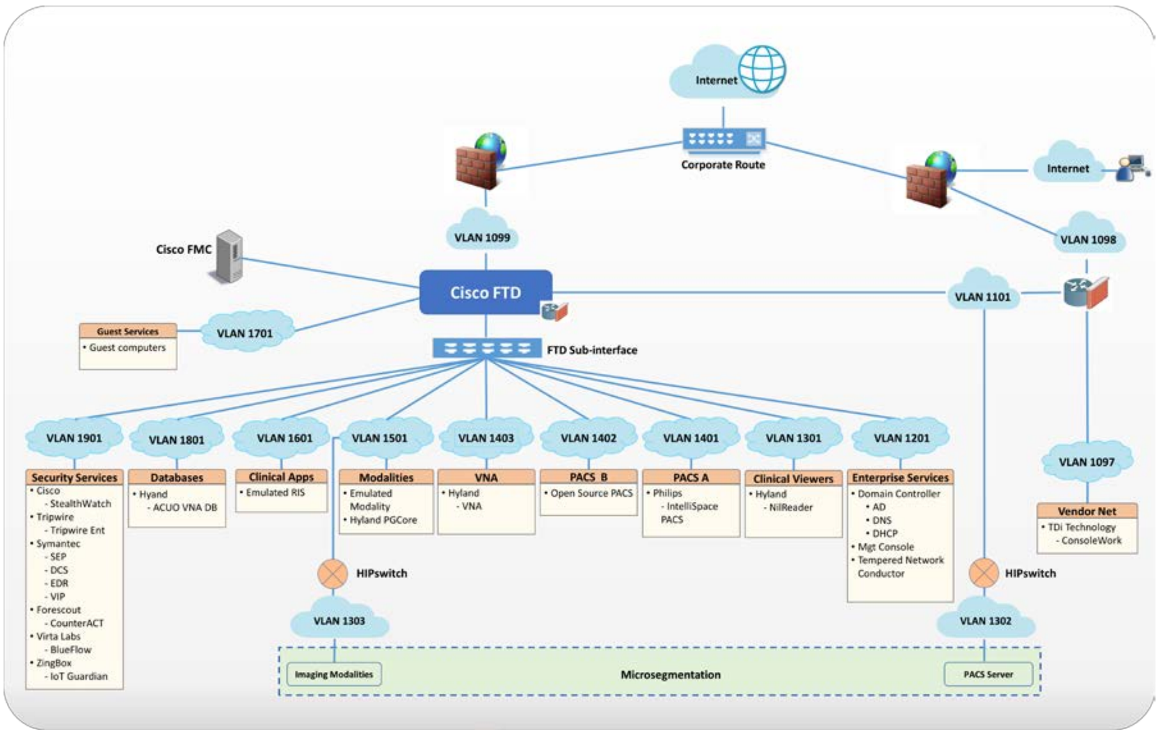
Both healthcare and IT systems require access by vendor support technicians for remote configuration, maintenance, patching, and updates to software and firmware. In our environment, a remote access network segment was designed to provide these external privileged users with privileged access to these components that reside within our reference architecture. A virtual private network (VPN) solution provides a secure way in which an organization can extend its private network across the internet, ensuring that only properly authenticated users can access their organization's private network. The NCCoE VPN in our environment was configured and managed using vendor-recommended practices [35]. This project implemented TDi ConsoleWorks as a remote access mechanism into the infrastructure.

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

4.2 Final Architecture

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

Figure 4-7 PACS Final Architecture



5 Security Characteristic Analysis

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

5.1 Assumptions and Limitations

The security characteristic analysis has the following limitations:

- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.

- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

5.2 Scenarios and Findings

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

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

Using the NIST Cybersecurity Framework Subcategories to organize our analysis also provided additional confidence that the reference design addresses our use case security objectives. The remainder of this subsection discusses how the reference design supports each of the identified Cybersecurity Framework Subcategories [8].

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

5.3.1 Asset Management (ID.AM)

For our project, we considered ID.AM-1, ID.AM-2, ID.AM-4, and ID.AM-5 to address asset management.

The project implemented ID.AM-1 using Virta Labs BlueFlow to address modality asset management. Establishing an asset inventory is a fundamental component in determining appropriate controls for the environment. The ID.AM-1 Subcategory specifies, "[p]hysical devices and systems within the organization are inventoried," and ID.AM-2 specifies, "[s]oftware platforms and applications within the organization are inventoried." For purposes of this document, the ID.AM-1 and ID.AM-2 Subcategories are grouped together, and these Subcategories identify tools to achieve these objectives. Physical devices include workstation, server, and storage components, whereas software assets include those applications that run on the physical components.

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

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

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

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

5.3.2 Risk Assessment (ID.RA)

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

This project used Symantec's Endpoint Protection solution to address threats to image viewer workstations. The project used Tripwire Enterprise for server assets. Virta Labs BlueFlow was applied for medical imaging devices. The project also used Zingbox IoT Guardian to perform NetFlow analysis. Information from these tools can be used when needed to determine risk profile of the HDO environment.

5.3.3 Identity Management and Access Control (PR.AC)

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

5.3.3.1 Identity Management

Human user access to workstations and systems was provisioned by creating accounts in Microsoft Active Directory. This project implemented the Symantec VIP. The Symantec VIP tool gave the project multifactor authentication capability. Table 5-1 describes how different user types are managed and describes some general characteristics of that user type.

Table 5-1 Identity Management Characteristics

User Type	Identity	Tool	Characteristics
Human Users	Active Directory	Active Directory	Human user authentication method dependent on interaction type
Medical Imaging Devices	Host Identifier	Tempered Networks IDN	Imaging devices abstracted from the production network over a cloaked network implementing HIP.
System to System	Certificate	DigiCert Managed PKI	Automated interactions between systems authenticated

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

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

The project augmented device authorization management by limiting PACS accessibility based on workstation zone provisioning. Multifactor authentication was implemented for certain devices through Symantec VIP. Network sessions were secured by TLS using DigiCert issued certificates [34].

5.3.3.2 Access Control

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

This project also took advantage of the network zoning concept and limited access based on firewall policies that restrict traffic between different zones. Image viewer workstation network traffic to the PACS and VNA for image retrieval and interaction are limited to specified network zones.

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

The project implemented PR.AC-3 using TDi Technologies ConsoleWorks to provide remote access to the lab network. The ConsoleWorks environment provided a solution for vendor remote access as well as general user remote VPN, including access by third-party medical imaging services that may need access to patient images [35].

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

5.3.4 Data Security (PR.DS)

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

No specific solution was used for storage. This practice guide recommends HDOs to evaluate NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events* [32], for general guidance for at-rest protection. Further, the PACS and VNA solutions were implemented on a Windows server environment, and therefore it is recommended to review and implement *SMB Security Best Practices* [33], as noted by CISA.

Workstations in this project are protected using Symantec Encryption Platform.

Data in-transit protection is implemented using TLS and HIP. Image viewing workstations connecting to the PACS/VNA environments use TLS encryption to ensure data-in-transit protection [28], [29], [34]. This project also implements microsegmentation with Tempered Networks and ensures data-in-transit protection by HIP-managed encryption between emulated medical imaging devices and the PACS/VNA environment.

The project uses Tripwire Enterprise and Symantec DCS:SA to provide integrity monitoring of system software files. Integrity of system and application software is monitored.

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

5.3.5 Information Protection and Procedures (PR.IP)

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

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

Virta Labs BlueFlow is used to manage medical imaging device configurations. The medical imaging devices deployed in the lab were emulated and do not involve firmware.

5.3.6 Protective Technology (PR.PT)

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

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

Another method this project implemented to ensure traffic was regularly reviewed was implementing the Zingbox IoT Guardian solution. The tool aggregated NetFlow traffic across the lab environment and performed behavioral analytics. HDOs should also consider using a security incident event management (SIEM) system that would aggregate logs from different operating systems, applications, and component types. SIEM tools often can support scripts that may trigger alerting to incident response teams.

To address PR.PT-3, this project implemented operating systems that were configured with the minimum functionality necessary to support PACS and VNA operations, based on guidance from Hyland and Philips respectively. Configuration recommendations from our vendor partners were treated as baseline settings. The project then used Tripwire Enterprise to monitor this baseline.

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

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

External connections were protected using TLS and internet protocol security (IPsec) tunneling where appropriate [34], [35].

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

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

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

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

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

5.4 Security Analysis Summary

Our reference design's implementation of security surrounding the PACS/VNA ecosystem helps reduce risk from the PACS/VNA system, even if a vulnerability is identified in a PACS or VNA system, by creating a more secure environment for the medical devices. The key feature is the multi-layered security capabilities defined in Section 4.1.3. Supporting those security capabilities, our project build follows vendor recommended practices to harden devices and systems; monitor traffic; limit access to only authorized users, devices, and systems; and ensure the data security across the ecosystem. Any organization following this guide must conduct its own analysis of how to employ the elements discussed here, in their own environment. It is essential that organizations follow security best practices to address potential vulnerabilities and to minimize any risk to the operational network.

6 Functional Evaluation

We conducted a functional evaluation of our example implementation to verify that several common provisioning functions used in our laboratory test worked as expected. We also needed to ensure the example solution would not alter normal PACS and VNA functions.

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

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

6.1 PACS Functional Test Plan

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

Table 6-1 Test Case Fields

Test Case Field	Description
Parent Requirement	Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement
Testable Requirement	Drives the definition of the remainder of the test case fields and specifies the capability to be evaluated
Associated Cybersecurity Framework Subcategories	Lists the NIST Cybersecurity Framework Subcategories addressed by the test case
Description	Describes the objective of the test case
Associated Test Cases	In some instances, a test case may be based on the outcome of another test case(s). For example, analysis-based test cases produce a result that is verifiable through various means (e.g., log entries, reports, and alerts).
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple

Test Case Field	Description
	sequences of steps (with delineation) to indicate variations in the test procedure.
Expected Results	The expected results for each variation in the test procedure
Actual Results	The observed results

6.1.1 PACS Functional Evaluation Requirements

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

Table 6-2 Functional Evaluation Requirements

Capability Requirement (CR) ID	Parent Requirement	Subrequirement	Test Case
CR-1	Business workflows that support image acquisition and transfer to archival (e.g., PACS and VNA) are performed.	Simple Radiology Practice Workflows	PACS-1
CR-2	Asset and Inventory Management		PACS-2
CR-3	Enterprise Domain and Identity Management–Access Control		
CR-3.a		Privileged Access Management	PACS-3 PACS-10
CR-3.b		User Authentication	PACS-3 PACS-4 PACS-5 PACS-10
CR-3.c		Device and System Authentication	PACS-3 PACS-4 PACS-5
CR-3.d		Data Access Control	PACS-3 PACS-5
CR-4	Network Control and Security		

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

1265 ### 6.1.2 Test Case: PACS-1

Parent Requirement	(CR-1) Business workflows that support image acquisition and transfer to archival (e.g., PACS and VNA) are performed.
Testable Requirement	(CR-1) Simple Radiology Practice Workflows
Description	Demonstrate that the installed PACS system can be used to acquire images from a simulated modality, store those images based on department, and view those images by using a DICOM viewer.
Associated Test Case	N/A
Associated Cybersecurity Framework Subcategories	N/A

Preconditions	▪ Implement PACS architecture and test that network connections are operational. ▪ Configure DICOM communication between DVTk RIS Emulator and DVTk Modality Emulator. ▪ Load patient studies into the RIS. ▪ Configure DICOM communication between DVTk Modality Emulator and PACS. ▪ Configure the DICOM viewer to connect to the PACS archiving system. ▪ Provision and give proper permissions to user accounts.
Procedure	1. Start the DVTk RIS simulator. 2. Start the Modality Emulator. 3. Click the **Request Worklist** button on the Modality to display the RIS' preinstalled patient studies. 4. Select one of the Patient Names from the given list. 5. Click the enabled **Store Image** button to send the images for the selected patient to the connected PACS server. 6. To verify the archived images stored in the Philips PACS server, run Explorer as a Manager. 7. Log in to the client web by using the URL *https://192.168.140.131/clientweb*. (Alternatively, use a thin client "Philips IntelliSpace PACS Enterprise" to verify the archived images.) 8. From the Folder **List** > **Exam Lookup** press **Search** button to list the patient studies. The image for the patient selected in this test should be listed in the exam lookup view table.
Expected Results	▪ The user should be able to display the image by using the Philips Client Web or the Philips PACS Enterprise client. Note: If you need to repeat the same procedure using the same samples, clear the stored image from the Philips PACS. The cleared image stored in the **Default** folder will be moved to the **Exceptions Lookup** folder. Clear the image from the **Exceptions Lookup** folder as well.
Actual Results	The implemented PACS environment successfully scheduled images by using the RIS, sent and stored the images in the PACS using the Modality, and viewed the stored images using a web client.

6.1.3 Test Case: PACS-2

Parent Requirement	**(CR-2) Asset and Inventory Management**
Testable Requirement	(CR-2) Asset and Inventory Management
Description	Demonstrate how to identify and manage medical assets
Associated Test Case	N/A
Associated Cybersecurity Framework Subcategories	ID.AM-1, ID.AM-2, ID.AM-4, ID.AM-5, ID.RA-1, ID.RA-5, PR.IP-1
Preconditions	▪ PACS network infrastructure is operational. ▪ Virta Labs BlueFlow is deployed in the **Security Services** VLAN. ▪ Network groups are created in the BlueFlow interface to allow automatic organization of discovered devices.
Procedure	1. Open a web browser and navigate to the **Virta Labs BlueFlow** web portal URL and authenticate to the portal. 2. Navigate to **Connectors** > **Discovery.** 3. Enter a **subnet range** (192.168.0.0/16) from which **BlueFlow** will discover devices. 4. Click **Run** and allow the discovery process to populate a network group. 5. Navigate to **Inventory.** Under **Networks,** click on a network object and display a list of discovered devices. 6. Click on a device name and navigate to the **Tools** tab and click on **Fingerprint.** 7. Verify the populated information and click **Run** to perform a scan. 8. Once the scan is complete, navigate back to the device's information page and verify that the **fingerprint** tool has accurately identified information about the device such as Operating System and **Open TCP Ports.** 9. Manually fill in other information about the device if needed.
Expected Results	▪ Devices are discovered within the specified subnets and appear as devices in the network group. ▪ The fingerprint tool identifies device Operating System and open TCP ports. ▪ Device information can be modified manually.

Actual Results	20+ new devices were discovered within the PACS VLANs. These new devices were automatically placed into predefined network segments, and devices that did not fit into a predefined network segment were placed into an Other Assets category. The fingerprint tool populated descriptive information for several discovered devices while all other necessary information was filled in manually.

1267 ### 6.1.4 Test Case: PACS-3

Parent Requirement	**(CR-3) Enterprise Domain and Identity Management–Access Control**
Testable Requirement	(CR-3.a) Privileged Access Management, (CR-3.b) User Authentication, (CR-3.c) Device and System Authentication, (CR-3.d) Data Access Control
Description	Demonstrate the capability authentication to PACS application by using enterprise Active Directory
Associated Test Case	N/A
Associated Cybersecurity Framework Subcategories	PR.AC-1, PR.AC-4, PR.AC-7
Preconditions	▪ Domain controller has been deployed and configured in the **Enterprise Services** VLAN. ▪ Philips PACS has been configured to incorporate the enterprise AD with a display name of **AD PACS.** ▪ Domain groups have been created and assigned proper policies and roles. ▪ A test user with username pacs-user has been set up in the test **AD PACS.**
Procedure	1. Launch the IntelliSpace PACS application on the IntelliSpace PACS Enterprise server. 2. To set the authentication source, select **AD PACS** from the **Log on to** dropdown list. 3. Enter the username and password, and then click on the login button to login.
Expected Results	▪ Authentication via **AD PACS** is successful. ▪ Access to patient data is based on group policy settings.
Actual Results	A user, *pacs-user*, who is in the Active Directory, was used to test the access setup. After entering the username and the correct password to the Philips IntelliSpace PACS Enterprise login page by using the AD PACS as the authentication source, the login was

	successful. The *pacs-user* account was validated to assure that appropriate access control settings were applied. *Pacs-user* authentication was further tested, first by entering an incorrect password and next by incorrectly spelling the username. These attempts failed.

1268
6.1.5 Test Case: PACS-4

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

	To store patient studies on the Philips PACS server by using DVTk Modality Emulator 1. Click the **Store Images** button to send the selected patient study to Philips PACS. To verify that data are encrypted between the modality and PACS 1. Start a packet capture with Cisco Firepower between the HIPswitches associated with the modality and PACS respectively. A new window will appear with attribute text boxes. For the **Source Host,** provide the IP address of the modality's HIPswitch. For the **Destination Host,** provide the IP address of the PACS HIPswitch. 2. Export the produced packet captures to a packet capture (PCAP) file. 3. Import the PCAP file into Wireshark, and try to read the data captured.
Expected Results	▪ RIS establishes a DICOM connection with the modality to schedule patient studies. ▪ DICOM communications channel established between modalities and PACS. ▪ Modality Emulator can send patient studies to PACS. ▪ In-transit data are encrypted.
Actual Results	The RIS, Modality, and PACS succeeded in establishing DICOM connections after microsegmentation was implemented. Data being transferred from Modality to PACS was encrypted through the secured connection.

1269 ### 6.1.6 Test Case: PACS-5

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

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

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

6.1.7 Test Case: PACS-6

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

	client computer accessing the PACS viewer through a web browser. 2. Export the produced packet captures to a PCAP file. 3. Import the PCAP file into Wireshark, and try to read the data captured.
Expected Results	▪ DICOM image web viewer should be accessible and display patient images using https. ▪ Data sent from an archiving server to the DICOM image web viewer should be encrypted.
Actual Results	Web viewer securely connected to the archiving server and transmitted patient images to a client computer over https.

1271 6.1.8 Test Case: PACS-7

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

Procedure	To test that DHCP services are available for Guest network 1. Power on Windows computer on the Guest network and log in. 2. Right-click on **Windows Start button** and select **Network Connections**. 3. Right-click on the **network interface** connected to the Guest network and select **Properties**. 4. Click on **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties** and select **Obtain an IP address automatically**, then click **OK**. 5. Run the **Command Prompt** from the **Windows Start button**. 6. At the **command line** type `ipconfig /all` 7. Ensure **DHCP Enabled** is set to **Yes**. 8. Ensure **IPv4 Address, Subnet Mask, Default Gateway,** and **DHCP Server** are populated according to your DHCP settings. To test that DNS services are available for Guest network 1. Right-click on **Windows Start button** and select **Network Connections**. 2. Right-click on the **network interface** connected to the Guest network and select **Properties**. 3. Click on **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties.** Select **Obtain DNS server address automatically** and click **OK**. 4. Run the **Command Prompt** from the **Windows Start button**. 5. At the **command line** type `ipconfig /all` 6. Ensure **DNS Servers** is populated according to your DHCP settings. 7. At the **command line** type `nslookup` 8. Verify that the **Default Address** and **Address** are populated with the correct **DNS server**. 9. At the prompt, type a URL (`nist.gov`) and ensure an IP address (`129.6.13.49`) is returned by the DNS server. To test that traffic from Guest network to internal VLANs is blocked 1. Open a web browser from the Windows computer connected to the Guest network. 2. Type an IP address (192.168.140.131) that corresponds to a PACS web server from one of the internal PACS VLANs into the

	address bar. The web browser should not be able to retrieve the web page. 3. Right-click on **Windows Start button** and select **Command Prompt**. At the **command** line, attempt to ping the VNA server from one of the internal PACS VLANs by typing `ping 192.168.130.120` 4. Ensure command prompt returns `Request timed out` and no packets are received. To test that only web traffic from Guest network to the WAN is allowed 1. Open a web browser from the Windows computer connected to the Guest network. 2. Type a **URL** (https://www.nist.gov/) into the **address bar**. 3. Wait for website to load properly. 4. Right-click on **Windows Start button** and select **Command Prompt**. 5. At the **command line**, attempt to ping an external web server by typing `ping nist.gov` 6. Ensure command prompt returns `Request timed out` and no packets are received.
Expected Results	▪ Computers with interfaces connected to Guest network will automatically be provisioned an IPv4 address. ▪ Computers with interfaces connected to the Guest network will automatically be provisioned a DNS server address. ▪ All traffic, excluding the exceptions for DNS and DHCP, originating from the Guest network and destined for any internal PACS VLAN will be blocked. ▪ http and https traffic originating from the Guest network and destined for the WAN interface will be allowed.
Actual Results	Upon booting up for the first time, the Windows computer on the Guest network was allocated an IPv4 address within the DHCP scope address pool and provisioned a DNS server address and was successfully able to resolve the IP address of a provided URL. The computer was not able to communicate with other devices in the internal PACS VLANs (192.168.140.131 and 192.168.130.120) using different network protocols (https and internet control message protocol [ICMP]) but was able to communicate with external web servers through a web browser using http and https.

1272
6.1.9 Test Case: PACS-8

Parent Requirement	**(CR-4) Network Control and Security**
Testable Requirement	(CR-4.d) Anomalies and Events Detection (Behavioral Analytics)
Description	Demonstrate capability to detect abnormal network traffic across the PACS architecture.
Associated Test Case	PACS-7
Associated Cybersecurity Framework Subcategories	DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-5, DE.CM-1, DE.CM-3, and DE.CM-7
Preconditions	▪ PACS architecture is implemented and network connections have been tested and are operational. ▪ Zingbox Inspector is deployed and configured in the **Security Services** VLAN. ▪ Virta Labs BlueFlow is deployed and configured in the **Security Services** VLAN.
Procedure	1. Open a web browser and navigate to the web portal of **Virta Labs BlueFlow**. 2. Enter **credentials** and log in. 3. Navigate to **Connectors > Discovery.** 4. Enter a **subnet range** (192.168.0.0/16) on which BlueFlow will run an IP scan. 5. Click **Run** and wait for discovery process to finish. 6. Open a web browser and navigate to the web portal of **Zingbox Cloud.** 7. Enter **credentials** and log in. 8. Navigate to **Alerts > Security Alerts.** 9. Under **Alerts,** look for an alert named **Suspicious internal IP scans** and an **alert type** of **scanner.** 10. Expand the alert, hover over a subsection, and click on **View Details.** 11. On the **Alert Details** page, verify that the **client IP** that the IP scans originated from corresponds to the **BlueFlow** device.
Expected Results	▪ Zingbox correctly identifies BlueFlow's IP scan and creates a security alert for suspicious activity.
Actual Results	Zingbox identified BlueFlow's IP scan as suspicious activity and created a security alert. Zingbox also created a security alert the second time a BlueFlow IP scan was run but stopped creating alerts

	for subsequent IP scans from the BlueFlow device. While the BlueFlow scan was approved and not malicious, this type of scanning can be performed by malicious devices attempting to discover devices on the network.

1273 ### 6.1.10 Test Case: PACS-9

Parent Requirement	**(CR-4) Network Control and Security** **(CR-5) Endpoint Protection and Security**
Testable Requirement	(CR-4.e) Intrusion Detection and Prevention, (CR-5.a) Device Hardening and Configuration, (CR-5.b) Malware Detection and Prevention
Description	Demonstrate capability to detect threats affecting PACS servers and related endpoints. This test also demonstrates an intrusion detection capability.
Associated Test Case	N/A
Associated Cybersecurity Framework Subcategories	DE.CM-1, DE.CM-4, PR.PT-1, PR.PT-3, PR.PT-4
Preconditions	▪ PACS architecture is implemented and network connections have been tested and are operational. ▪ Symantec Endpoint Protection appliance is deployed and configured in the **Security Services** VLAN. ▪ Symantec Endpoint Protection agent is installed on an endpoint. ▪ The endpoint agent is connected to the Symantec Endpoint Protection Manager.
Procedure	<u>To verify that the endpoint agent is connected to the SEP management server</u> 1. Log in to the SEP management console (*https://192.168.190.172:8443/console/apps/sepm*), click **Clients,** and select the **target group** (e.g., PACS). 2. Click the **Client** tab in the PACS group to list the client information in a table. 3. The endpoint is listed under the **Name** column with a **Health State** of online 4. To verify that the endpoint receives the current policy updates 5. Navigate to the **Client** tab in the SEP management console.

	6. The policy serial number should match the serial number of the endpoint found at **Help** > **Troubleshooting** in the endpoint agent. To verify that the proper protections are enforced on the endpoint 1. Navigate to the **Client** tab in the SEP management console. 2. In the **PACS** group, change the drop-down list selection to **Protection Technology** and review the protection categories status (enabled or disabled). To add a System Lockdown policy to prevent unwanted applications from running 1. Enable the System Lockdown policy from the parent group of PACS. 2. Select the Blacklist Mode, add a test application (e.g., *7zFM.exe*) to the list, and save the policy. 3. From the endpoint, click on the Symantec shield icon and click Update Policy. To verify that the virus and spyware protection policy works 1. Use a browser on the endpoint to download an antivirus test file from the EICAR website (https://www.eicar.org/). 2. Click the image labeled **DOWNLOAD ANTI MALWARE TESTFILE**. 3. Click the eicar.com link under **Download area using the secure, SSL enabled protocol https**. 4. A Symantec notification will appear, informing you that a risk is found.
Expected Results	▪ Files added to the Blacklist are not allowed to be run. ▪ Linking to the test virus file will lead to a warning, and the threat should be locked.
Actual Results	Prior to the lockdown policy enforcement, the *7zFM.exe* file and 7zFM file manager console were able to run on the endpoint. After the lockdown policy enforcement, the *7zFM.exe* file was not able to run, and a warning message appeared stating, “Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.” When accessing the malware test file, the following message appeared: “Symantec Endpoint Protection [SID:24461] Diagnostic: EICAR Standard Anti-Virus Test File detected, Symantec Service Framework.”

1274 ### 6.1.11 Test Case: PACS-10

Parent Requirement	**(CR-3) Enterprise Domain and Identity Management–Access Control** **(CR-7) Remote Access**
Testable Requirement	(CR-3.a) Privileged Access Management, (CR-3.b) User Authentication
Description	Demonstrate capability to provide controlled remote access to PACS systems using the two-factor authentication.
Associated Test Case	PACS-3
Associated Cybersecurity Framework Subcategories	PR.AC-3
Preconditions	▪ TDi Technology ConsoleWorks is installed and configured to use Active Directory for username and password authentication. ▪ Proper access control rules, tags, and profiles are defined to allow access to necessary resources. ▪ User accounts for remote access are set up and linked to profiles set for each remote user who needs to access the PACS servers. ▪ Symantec VIP Enterprise Gateway is installed and integrated with ConsoleWorks by using the RADIUS connection. ▪ To supplement standard username/password logins on a variety of servers and services, the VIP Access smartphone application is installed, and a credential ID has been acquired from Symantec for receiving time sensitive tokens. ▪ Test user credentials are registered in the VIP manager and associated to the account.
Procedure	<u>To verify that username/password are not sufficient to log in</u> 1. Use a web browser to connect to the TDi console (*https://192.168.1.4:5176*) and log in with username/password. 2. Verify that the login is unsuccessful. <u>To verify the two-factor authentication using username/password with a VIP token</u> 1. Use a browser to connect to the TDi console: (*https://192.168.1.4:5176*). 2. Open the VIP Access smartphone application. It should display a security code with a valid time duration. 3. Log in to the TDi console with username/password followed by the VIP security token found in the smartphone application.

	To verify that the user can access only the granted resources 1. Select the **Graphical** menu to open a **Graphical View.** 2. Check the list of graphical connections to ensure that only allowed connections are visible. 3. Check each of the graphical connections by clicking on **Connect** and verifying that the console properly connects.
Expected Results	▪ Logging in to the TDi console with a valid username/password without a 2FA token should fail with the message "Invalid User Credentials." ▪ Logging in to the TDi console with a valid username/password with valid 2FA token should be successful. ▪ Authenticated user should have access to list of approved graphical connections and should be able to connect to these servers.
Actual Results	Using a pre-created Hyland user as an example, the first attempt to log in to the TDi console with only a username and password failed. The second attempt to log in, this time with a 2FA token, was successful. From the dashboard, the Graphical View menu was opened, and only approved graphical connections were visible to the Hyland user (e.g., Hyland VNA, Hyland Database). The user was able to connect to these remote servers and authenticate with a Hyland service account.

7 Future Build Considerations

During this project and development of this practice guide, we did not implement several components; however, these omitted components should be considered. We did not implement an EHR system, and we used simulated medical imaging devices rather than physically deploying them.

Another topic that this practice guide does not implement is the storage tier. An approach to address storage is to examine cloud solutions. Medical images require robust storage media scalability and protection, including data encryption, key management, access control, detection when data are accessed or transported, and recoverability. As HDOs consider using cloud storage providers, organizations need to consider several factors to ensure appropriate information safeguards. Addressing cloud storage for healthcare has data security implications that exceed safeguarding medical images. An update to this practice guide will better address cyber risks associated with cloud storage solutions.

Appendix A List of Acronyms

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AV	Anti-Virus
CDA	Clinical Document Architecture
CIA	Confidentiality, Integrity, and Availability
CIS	Clinical Information System
CISA	Cyber Infrastructure Security Agency
CPOE	Computerized Physician Order Entry
CT	Computed Tomography
DICOM	Digital Imaging and Communications in Medicine
DNS	Domain Name Service
DoS	Denial of Service
EHR	Electronic Health Record
FDA	Food and Drug Administration
FIM	File Integrity Monitoring
FMC	Firepower Management Center
FTD	Firepower Threat Defense
GRC	Governance, Risk, and Compliance
IETF	Internet Engineering Task Force
HDO	Healthcare Delivery Organization
HIP	Host Identity Protocol
HIPPA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System

HIS	Health Information System
HL7	Health Level 7
HTM	Healthcare Technology Management
http	Hypertext Transfer Protocol
https	Hyper Text Transfer Protocol Secure
IDN	Identity Defined Networking
IEC	International Electrotechnical Commission
IDS	Intrusion Detection System
IHE	Integrating Health Enterprise
IoT	Internet of Things
IPSec	Internet Protocol Security
IT	Information Technology
MAC	Media Access Control
MRI	Magnetic Resonance Imaging
NCCoE	National Cybersecurity Center of Excellence
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
PACS	Picture Archiving and Communication System
PAM	Privileged Access Management
PCAP	Packet Capture
PET	Positron Emission Tomography
PHI	Protected Health Information
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
RFC	Request for Comments
RIS	Radiology Information System

RMF	Risk Management Framework
SAN	Storage Area Network
SDN	Software Defined Networking
SHA	Secure Hash Algorithm
SMB	Server Message Block
SP	Special Publication
SSE	Systems Security Engineering
SSL/TLS	Secure Socket Layer/Transport Layer Security
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
VIP	Validation and ID Protection
VLAN	Virtual Local Area Network
VNA	Vendor Neutral Archive
VPN	Virtual Private Network

Appendix B References

[1] Food and Drug Administration, "Display Devices for Diagnostic Radiology, Guidance for Industry and Food and Drug Administration Staff," Oct. 2, 2017. Available: https://www.fda.gov/media/95527/download.

[2] National Electrical Manufacturers Association, *PS3.1: DICOM PS3.1 2019c Introduction and Overview,* 2018. Available: http:/dicom.nema.org/medical/dicom/current/output/pdf/part01.pdf.

[3] DICOM. Digital Imaging and Communications in Medicine. [Website]. Available: https://dicomstandard.org.

[4] Radiology Technical Framework. Integrating the Healthcare Enterprise. [Website]. Available: http://www.ihe.net/Technical_Frameworks/#radiology.

[5] R. Ross et al., *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-160 Volume 1, NIST, Gaithersburg, Md., Nov. 2016. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.

[6] R. Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* NIST SP 800-171 Revision 1, NIST, Gaithersburg, Md., Dec. 2016. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[7] W. Newhouse et al., *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, NIST SP 800-181, NIST, Gaithersburg, Md., Aug. 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[8] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, Gaithersburg, Md., Apr. 16, 2018. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[9] NIST. Risk Management Framework: Quick Start Guides. [Website]. Available: https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides.

[10] Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Revision 1, NIST, Gaithersburg, Md., Sept. 2012. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[11] Joint Task Force Transformation Initiative, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication (SP) 800-37 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[12] NIST. Computer Security Resource Center. [Website]. Available: https://csrc.nist.gov/glossary/term/confidentiality-integrity-availability.

[13] National Cybersecurity Center of Excellence, *Securing Picture Archiving and Communication System (PACS)* Project Description, NIST, Gaithersburg, Md., Jan. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-pacs-project-description-final.pdf.

[14] Health Level 7 International. Introduction to HL7 Standards. [Website]. Available: http://www.hl7.org/implement/standards/index.cfm?ref=nav.

[15] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 4, NIST, Gaithersburg, Md., Apr. 2, 2014. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[16] International Electrotechnical Commission (IEC) Technical Report (TR) 80001-2-2, Edition 1.0 2012-07, Technical Report, "Application of risk management for IT Networks incorporating medical devices–Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls."

[17] The U.S. Department of Health and Human Services Office for Civil Rights, *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, Feb. 2016. Available: https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.

[18] International Organization for Standardization/International Electrotechnical Commission, Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2013, 2013. Available: https://www.itgovernance.co.uk/shop/Product/isoiec-27001-2013-iso-27001-standard-ismsrequirements.

[19] U.S. Food and Drug Administration, *Guidance for the Submission of Premarket Notifications for Medical Image Management Devices–Guidance for Industry*, July 27, 2000. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/guidance-submission-premarket-notifications-medical-image-management-devices-guidance-industry.

[20] Health Level 7 International. *Clinical Document Architecture (CDA®) Release 2.* [Website]. Available: https://www.hl7.org/implement/standards/product_brief.cfm?product_id=7.

[21] G. O'Brien et al., *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations,* NIST SP 1800-8, NIST, Gaithersburg, Md., Aug. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf.

[22] American National Standards Institute (ANSI)/ Association for the Advancement of Medical Instrumentation (AAMI)/IEC 80001-1:2010, "Application of risk management for IT Networks incorporating medical devices–Part 1: Roles, responsibilities and activities."

[23] IECTR 80001-2-1, Edition 1.0 2012-07, Technical Report, "Application of risk management for IT-networks incorporating medical devices–Part 2-1: Step-by-step risk management of medical IT-networks–Practical applications and examples."

[24] K. Waltermire et al., *Privileged Account Management for the Financial Services Sector,* NIST SP 1800-18, NIST, Gaithersburg, Md., Sept. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-pam-nist-sp1800-18-draft.pdf.

[25] NIST. "Easy Ways to Build a Better P@$5w0rd. [Website]. Available: https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd.

[26] M. Grassi et al., *Digital Identity Guidelines,* NIST SP 800-63-3, NIST, Gaithersburg, Md., June 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[27] R. Moskowitz and P. Nikander, *Host Identity Protocol (HIP) Architecture*, Request for Comments 4423, May 2006. Available: https://tools.ietf.org/html/rfc4423.

[28] A. Gurtrov, *Primer on Host Identity Protocol (HIP): A Game Changer in IP Communications*, Tempered Networks, Seattle, Wash. Available: https://www.temperednetworks.com/sites/default/files/resources/whitepapers/Host-Identity-Protocol-Andrei-Gurtov.pdf.

[29] E. Barker et al., *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*, NIST SP 800-56C Revision 1, NIST, Gaithersburg, Md., Apr. 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf.

[30] U.S. Department of Commerce, *Advanced Encryption Standard (AES)*, NIST Federal Information Processing Standards (FIPS) Publication 197, Nov. 26, 2001. Available: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.

[31] K. Scarfone and P. Mell, *Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft)*, NIST SP 800-94 Revision 1 (Draft), NIST, Gaithersburg, Md., July 2012. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf.

[32] T. McBride et al., *Data Integrity: Recovering from Ransomware and Other Destructive Events*, NIST SP 1800-11, NIST, Gaithersburg, Md., Sept. 2017. Available: https://www.nccoe.nist.gov/publication/1800-11/index.html.

[33] U.S. Department of Homeland Security, Cyber Infrastructure Security Agency (CISA). *SMB Security Best Practices*. [Website]. Available: https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices.

[34] K. McKay and D. Cooper, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, NIST SP 800-52 Revision 2, NIST, Gaithersburg, Md., Oct. 2018. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-52/rev-2/draft/documents/sp800-52r2-draft2.pdf.

[35] E. Barker et al., *Guide to IPsec VPNs*, draft NIST SP 800-77 Revision 1, NIST, Gaithersburg, Md., July 2019. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-77r1-draft.pdf.

[36] Securities and Exchange Commission, *Public Company Accounting Oversight Board; Notice of Filing of Proposed Rule on Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with an Audit of Financial Statements, and Related Independence Rule and Conforming Amendments.* June 7, 2007. Available: https://www.sec.gov/rules/pcaob/2007/34-55876.pdf.

Appendix C Pervasive Versus Contextual Controls

This practice guide limits its scope to a defined boundary regarding the scheduling, acquisition, use, and storage of medical imaging and associated information for those images. Conceptually, this is bound in a medical imaging ecosystem and applies contextual controls to that ecosystem. Healthcare delivery organization (HDO) environments, however, feature greater complexity than this practice guide may address. That is, the medical imaging ecosystem resides within an enterprise infrastructure that should implement a pervasive set of controls. The project assumes that an HDO implements pervasive controls that may have material impact on mitigating the HDO's overall cybersecurity risk profile but are not implemented in the lab build. Pervasive controls may be inherited by systems that operate within the HDO infrastructure, but coverage may not be absolute. As such, contextual controls may be implemented to address gaps or to augment pervasive control capabilities. Pervasive controls tend to be organizational in scope, although they may also apply to specific systems and network components within the organization. Pervasive controls may be technical or procedural in nature. The pervasive control concept is borrowed from auditing frameworks that discuss the use of entity controls that have varying degrees of effects that are pervasive or have a widespread effect across an entity or organization [36].

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

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

Table C-1 Pervasive Security Controls

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

Cybersecurity Framework Subcategory	Description	Potential Implementation
		resources required, and milestone dates for realization of tasks. Typical control implementation to address ID.RA-4 and ID.RA-6 would include a GRC suite with an enterprise risk management module. The Clearwater Compliance IRM Analysis tool may be relevant as well.
PR.AC-2	PR.AC-2: Physical access to assets is managed and protected.	Server assets may be hosted in a data center with appropriate physical security and environmental controls.
PR.DS-5	PR.DS-5: Protections against data leaks are implemented.	This control addresses the possibility of data exfiltration and may consider options wherein clinical or other sensitive data are migrated outside the HDO perimeter by using email or web services. Typical controls to be deployed at the internet border may include DLP tools. An example tool may be the Symantec DLP solution.
PR.IP-6	PR.IP-6: Data is destroyed according to policy.	This control addresses the need to destroy data as appropriate should that data reach end of life. PACS and VNA control mechanisms would address objects within their purview, but HDOs should look at pervasive mechanisms to address when data may reside on workstations, endpoint devices, or removable media. In addressing appropriate data destruction measures, HDOs should consult National Institute

Cybersecurity Framework Subcategory	Description	Potential Implementation
		of Standards and Technology Special Publication 800-88 rev. 1, *Guidelines for Media Sanitation.*
PR.IP-9 PR.IP-10	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. PR.IP-10: Response and recovery plans are tested.	These controls pertain to enterprise response and recovery planning, including disaster recovery, and assurance that the plans are regularly tested. Incident response planning may be addressed in several different ways that include establishing an incident response team, capturing data regarding reported or detected security events, and remediation. Inclusive of establishing incident response procedures, organizations may consider developing "play books" that could consist of established procedures based on determining certain threat types that may require courses of action different from standard incident handling. Recovery plans, which may consist of business continuity plans, and disaster recovery plans should be established. Organizations may consider maintaining these plans, including establishing "play books," as maintained out of band, e.g., in physical format or in mechanisms that provide assurance that the plans themselves are inaccessible in case of a security event.

Cybersecurity Framework Subcategory	Description	Potential Implementation
		Management of such plans may be maintained in GRC suites that include modules designed to house such plans and establish regular testing schedules.
RS.RP-1	Response plan is executed during or after an event.	Response plans may be managed through a GRC solution. Physical copies of response plans should be maintained to allow for potential system outages.
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident.	Recovery plans may be managed through a GRC solution. Physical copies of recovery plans should be maintained to allow for potential system outages.

Appendix D Aligning Controls Based on Threats

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

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

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

NIST SPECIAL PUBLICATION 1800-24C

Securing Picture Archiving and Communication System (PACS)

Cybersecurity for the Healthcare Sector

Volume C:
How-To Guides

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

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

September 2019

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs

DISCLAIMER

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

National Institute of Standards and Technology Special Publication 1800-24C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-24C, 236 pages, (September 2019), CODEN: NSPUE2

FEEDBACK

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

Comments on this publication may be submitted to: hit_nccoe@nist.gov.

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

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov .

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

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

Name	Organization
Andy Gray	Forescout
Katherine Gronberg	Forescout
William Canter	Hyland
Kevin Dietz	Hyland
David Alfonso	Philips Healthcare
Jonathan Bagnall	Philips Healthcare
Julian Castro	Philips Healthcare
Sukanta Das	Philips Healthcare
Jason Dupuis	Philips Healthcare
Michael McNeil	Philips Healthcare
Dwayne Thaele	Philips Healthcare
Steve Kruse	Symantec
Derek Peters	Symantec
Axel Wirth	Symantec
Bill Johnson	TDi Technologies
Pam Johnson	TDi Technologies
Robert Armstrong	Tempered Networks
Nicholas Ringborg	Tempered Networks

Name	Organization
Mehwish Akram	The MITRE Corporation
Steve Edson	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Donald Faatz	The MITRE Corporation
Harry Perper	The MITRE Corporation
Randy Esser	Tripwire
Onyeka Jones	Tripwire
Jim Wachhaus	Tripwire
Sandra Osafo	University of Maryland University College
Henrik Holm	Virta Labs
Michael Holt	Virta Labs
Ben Ransford	Virta Labs
Jun Du	Zingbox
Damon Mosk-Aoyama	Zingbox
David Xiao	Zingbox

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
Philips Healthcare	Philips Enterprise Imaging Domain Controller Philips Enterprise Imaging IntelliSpace PACS Philips Enterprise Imaging Universal Data Manager
Symantec	Symantec Endpoint Detection and Response (EDR) Version 4.1.0 Symantec Data Center Security: Server Advanced (DCS:SA) Version 6.7 Symantec Endpoint Protection (SEP 14) Version 14.2 Symantec Validation and ID Protection Version 9.8.4 Windows
TDi Technologies	TDI Technologies ConsoleWorks Version 5.1-0u1
Tempered Networks	Tempered Networks Identity Defined Networking (IDN) Conductor and HIPSwitch Version 2.1
Tripwire	Tripwire Enterprise Version 8.7
Virta Labs	BlueFlow Version 2.6.4
Zingbox	Zingbox IoT Guardian

Contents

List of Figures

List of Tables

1 Introduction

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

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

1.1 Practice Guide Structure

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

This guide contains three volumes:

NIST SP 1800-24A: *Executive Summary*

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

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

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

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

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

example solution built at the NCCoE

benefits of adopting the example solution

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

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

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

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

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

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

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

Acronyms used in figures can be found in Appendix A.

1.2 Build Overview

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

1.3 Typographic Conventions

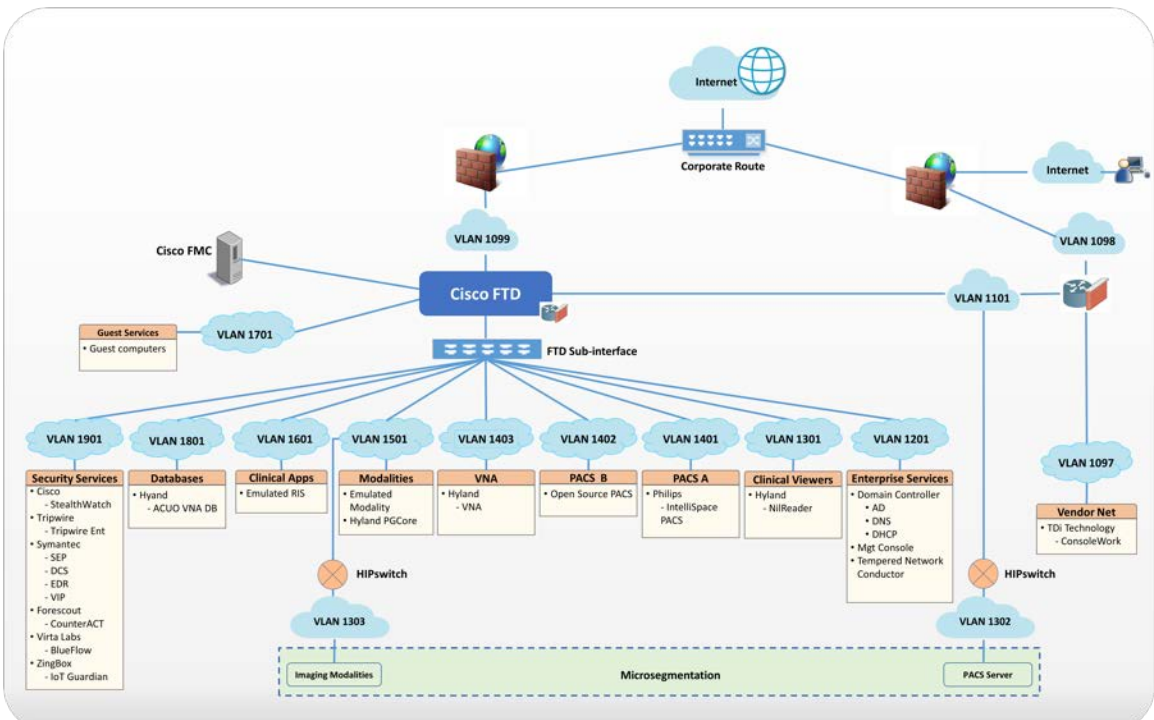
The following table presents typographic conventions used in this volume.

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

1.4 Logical Architecture Summary

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

Figure 1-1 PACS Final Architecture



2 Product Installation Guides

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

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

2.1 Picture Archiving and Communication System (PACS)

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

2.1.1 Philips IntelliSpace PACS

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

System Requirements

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

Table 2-1 Base VM Configuration Requirements

VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
DC1	Domain Controller	4	8 gigabytes (GB) of random access memory (RAM)	200 GB	Microsoft Windows Server 2012	Microsoft Structured Query Language (SQL) 2012, Internet Information Services (IIS) 7
IntelliSpace Server	Infrastructure, Integration, Rhapsody Health Level 7 (HL7), DICOM processor, SQL Database	4	8 GB RAM	200 GB	Microsoft Windows Server 2012	Microsoft SQL 2012, IIS 7

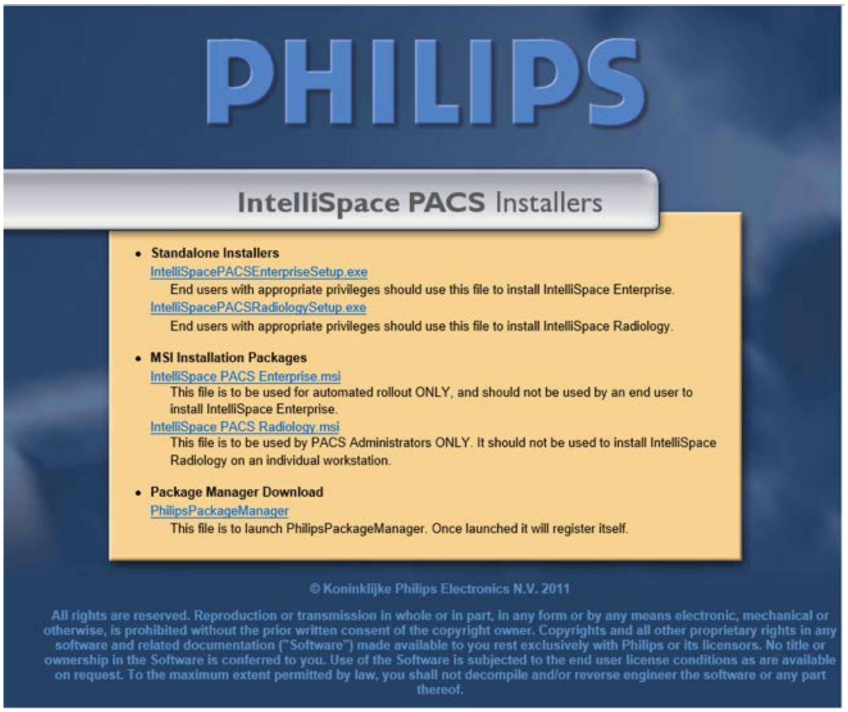
VM Name	Description	Central Processing Unit (CPU)	Memory	Storage	Operating System	Software
	(DB), Anywhere Viewer (web client)					
UDM	Universal Data Manager (UDM), WEB DICOM services Image Lifecycle Management Image pre fetching from VNA	4	8 GB RAM	200 GB	Microsoft Windows Server 2012	Microsoft SQL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

IntelliSpace PACS Client Installation

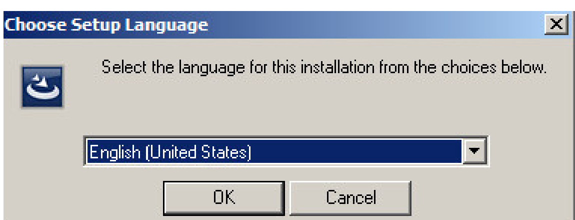
The project team collaborated with a team of Philips Healthcare deployment engineers to install the environment. Based on the base VM configuration requirements, the NCCoE team created the VMs by using the open virtualization format (OVF) files provided by Philips Healthcare. Philips engineers deployed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

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

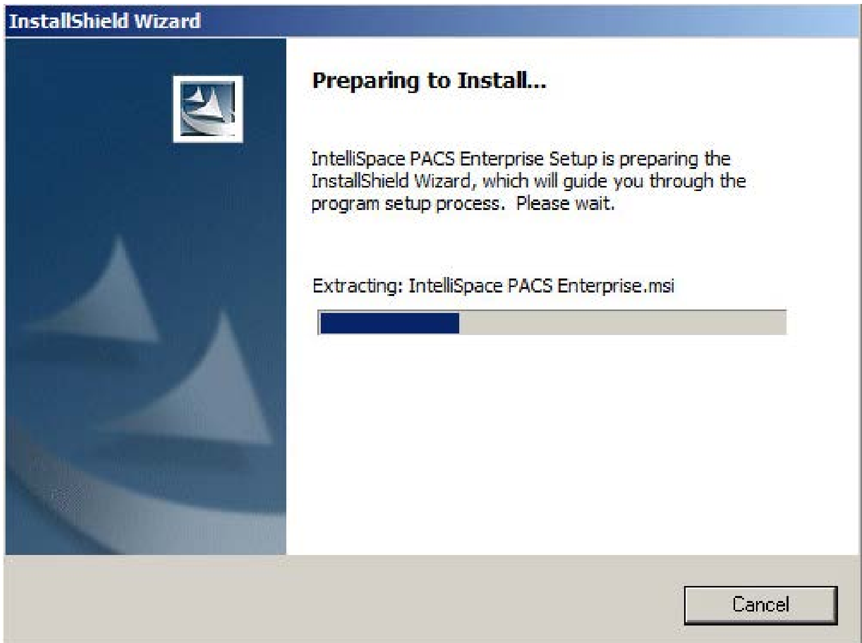
1. Open **Internet Explorer** from a workstation and assign the IntelliSpace server with the internet protocol (IP) address 192.168.140.131. Enter the IntelliSpace server (IP) address in the address bar by using the following URL: *https://192.168.140.131/clientweb/installers*.
2. Select *InstelliSpacePACSEnterpriseSetup.exe*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



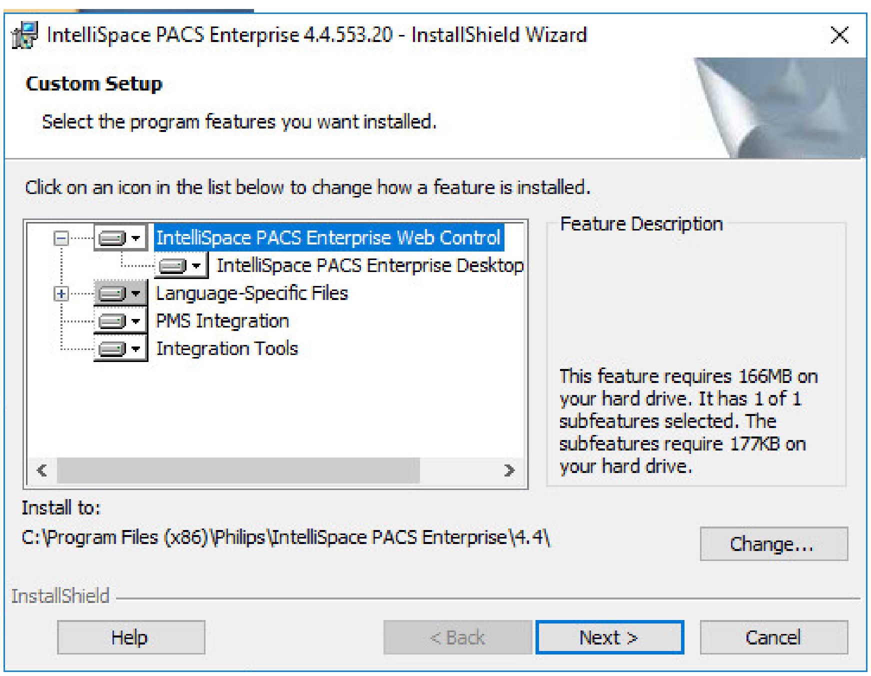
3. An option to choose setup language appears. Select the **English (United States)** from the pull-down and click **OK**.



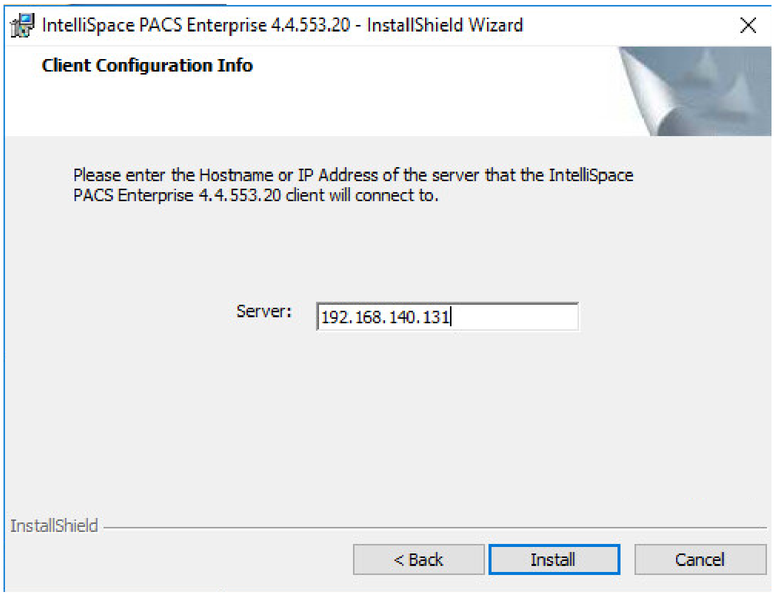
4. After the setup language has been set, the **InstallShield Wizard** begins the installation process.



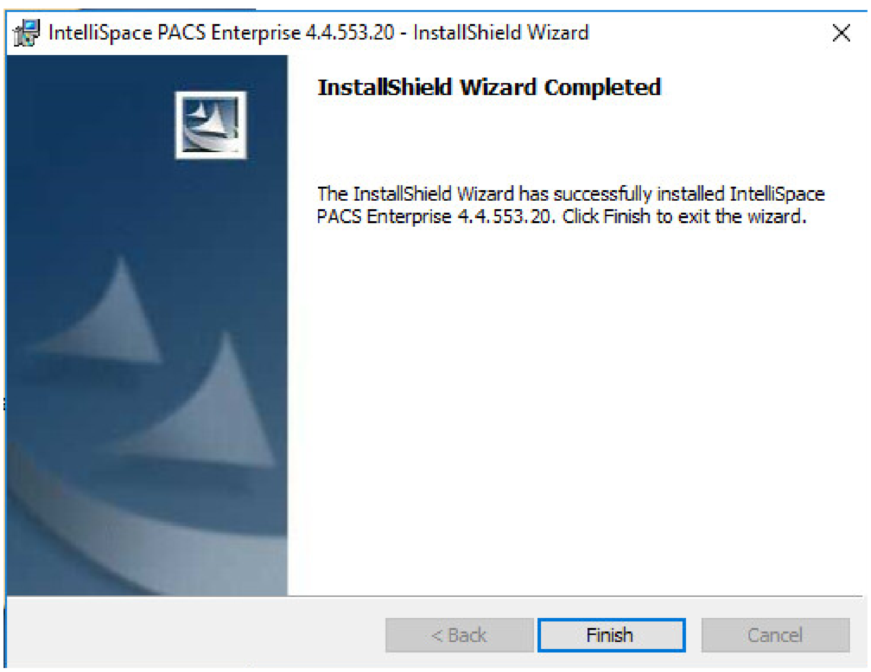
5. Use the default setting for the **Custom Setup** and click on the **Next >** button that appears at the bottom of this window.



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

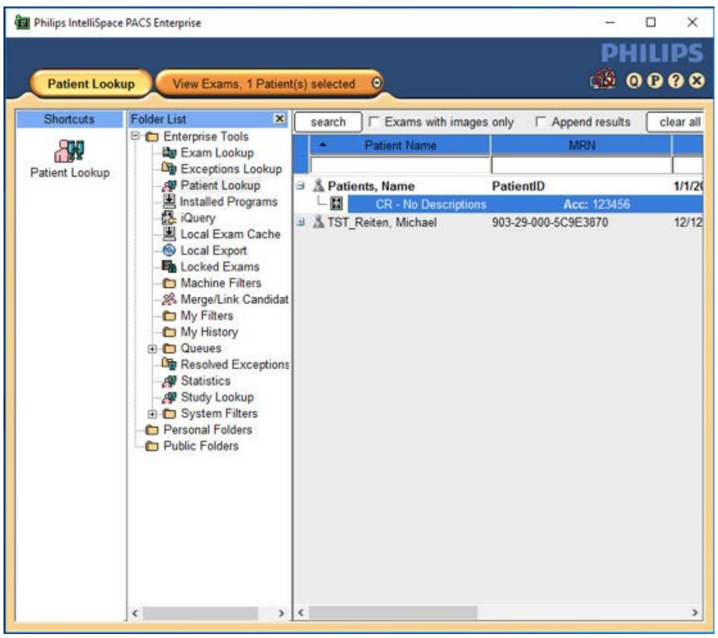


7. When installation is finished, the **InstallShield Wizard** provides a message indicating successful installation. Click **Finish.**

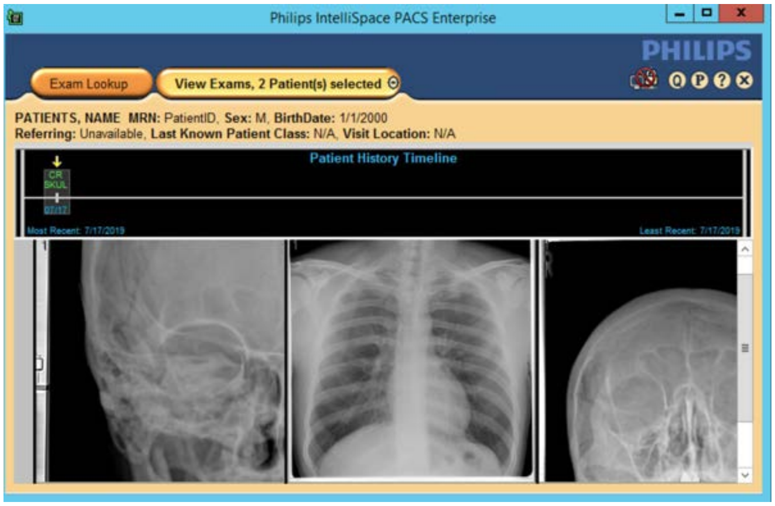


8. Once the installation is done, the installer places an **IntelliSpace PACS Enterprise** icon on the desktop. Type **Tester** in the **User Name** field and the corresponding password in the **Password** field, then click **OK** to log in.

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



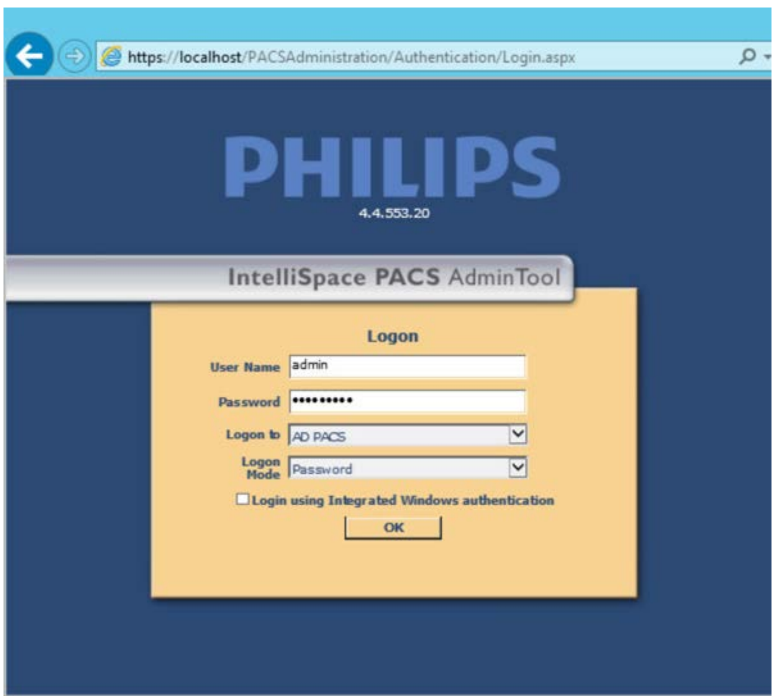
10. To view an exam, navigate to **Exam Lookup,** which lists a summary of a patient's exams. Double-click an exam in the list. If the exam has an image, it will be displayed. An example is shown below.



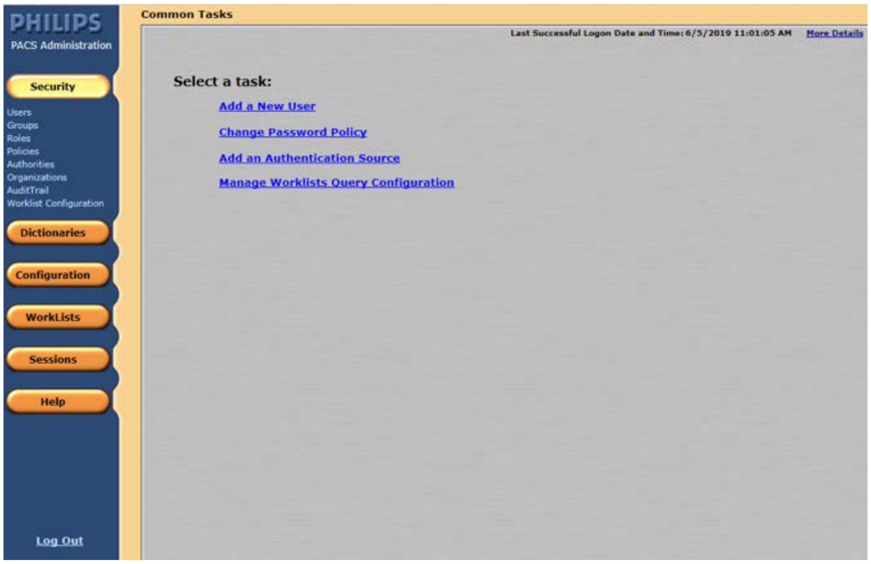
IntelliSpace PACS Client Configuration

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

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



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

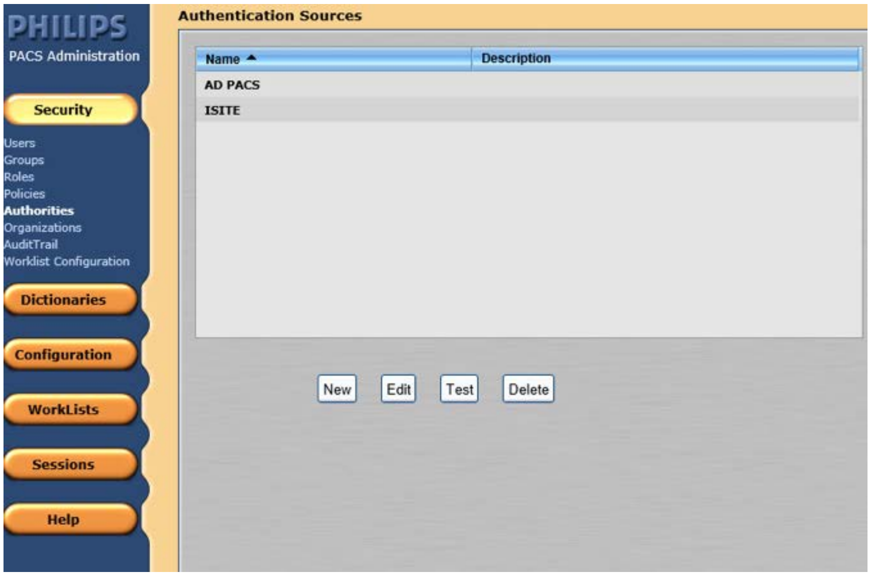


3. To add a new user, navigate to **SECURITY,** found on the far-left column of the Common Tasks screen, and click on **Users**.
   a. Enter the **User ID**.
   b. Enter the user's **First Name**.
   c. Enter the user's **Middle Name** (optional).
   d. Enter the user's **Last Name**.
   e. Enter the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

<u>Configure Sources for User Authentication</u>

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

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

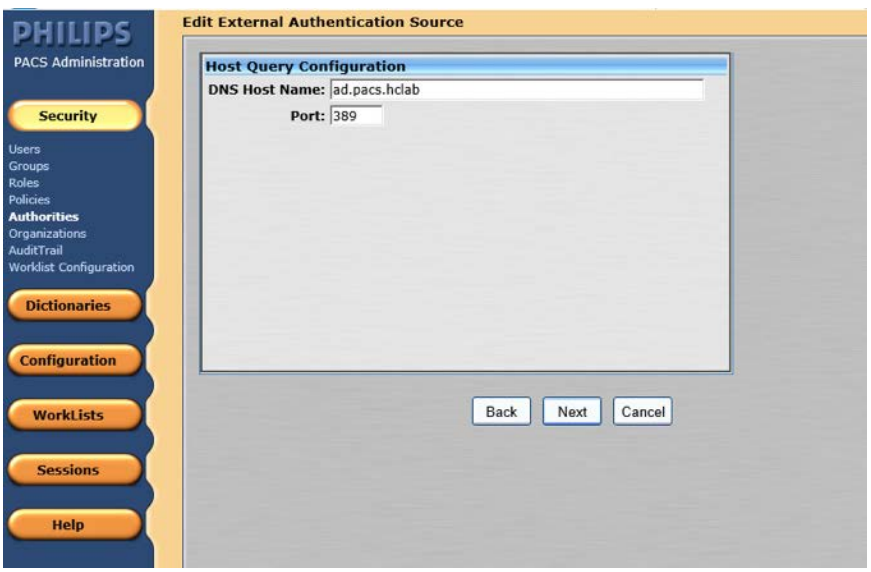


2. Click **New** to open the External Authentication Source wizard.

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

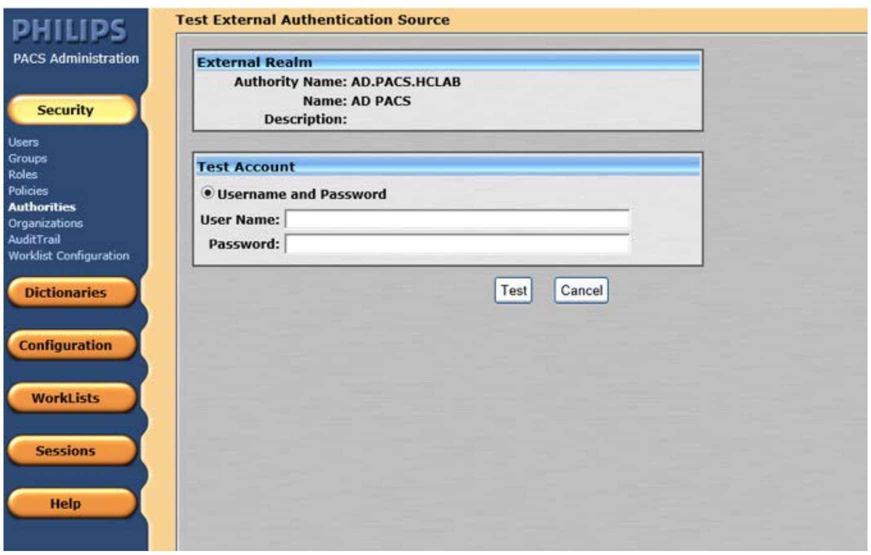
- Check the box next to **Show in Login Screen**

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



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.

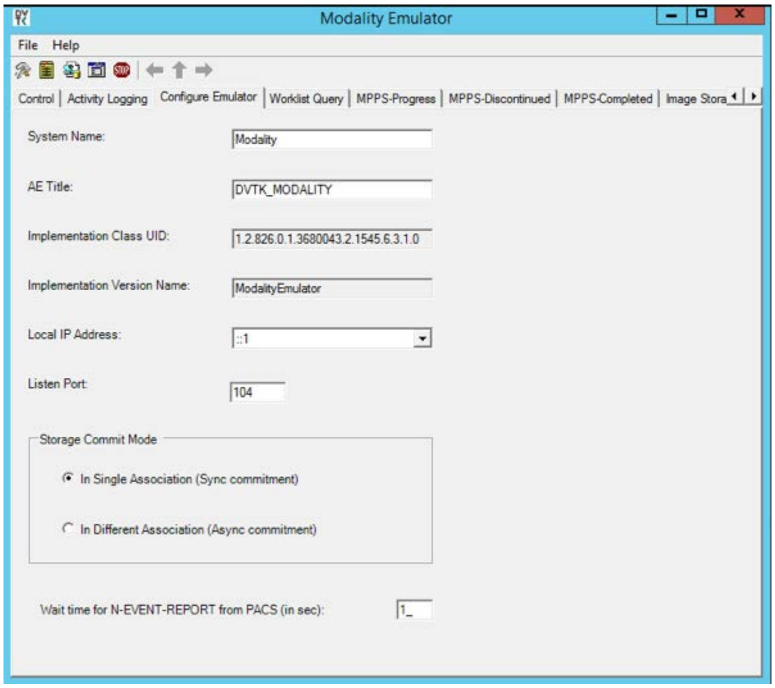
6. The interface provides a test feature to allow engineers to determine connectivity with the external authentication source. From the navigation bar, select the **Security > Authorities**. Click on the name of the **External Authentication Source,** and click **Test**.



__**Configure Connection to Modality Emulator**__

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

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



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

   RIS System

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

   MPPS Manager

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

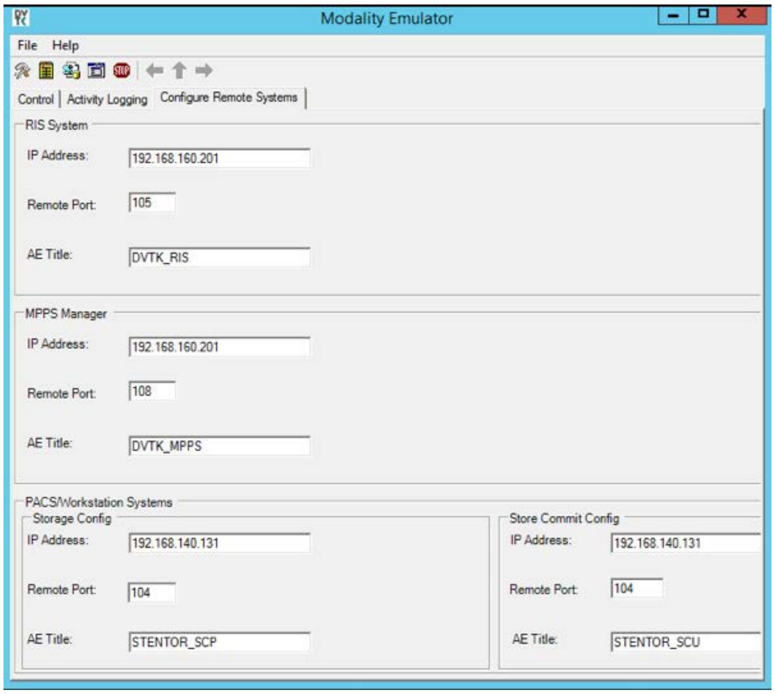
   PACS/Workstation Systems–Storage Config

   - **IP Address:** *192.168.140.131*

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

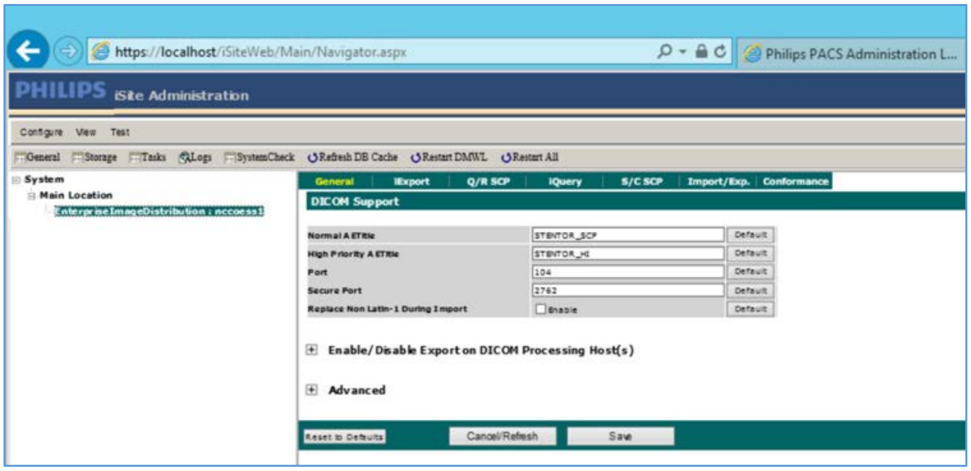
PACS/Workstation Systems–Storage Commit Config

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

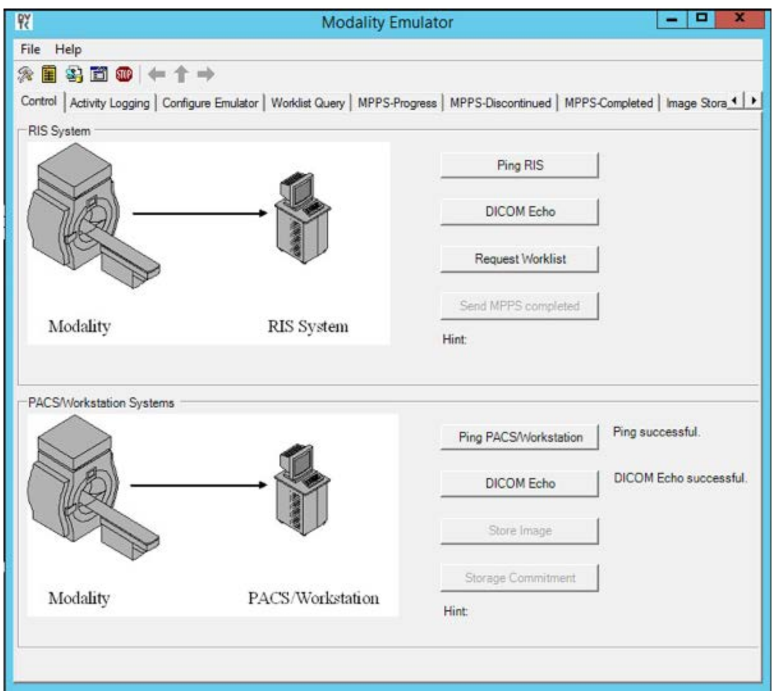


3. To configure the Philips IntelliSpace PACS AE Title and communication port, log on to the iSite Administration web site using the URL *https://192.168.140.131/ iSiteWeb*. Select **Configure > DICOM > General,** set the following values, and then click **Save** to save the settings.

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



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

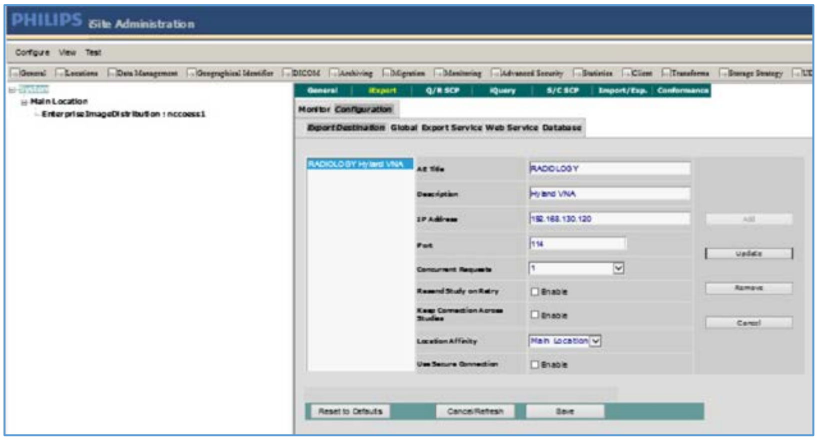


Configure IntelliSpace PACS to Communicate with Hyland VNA

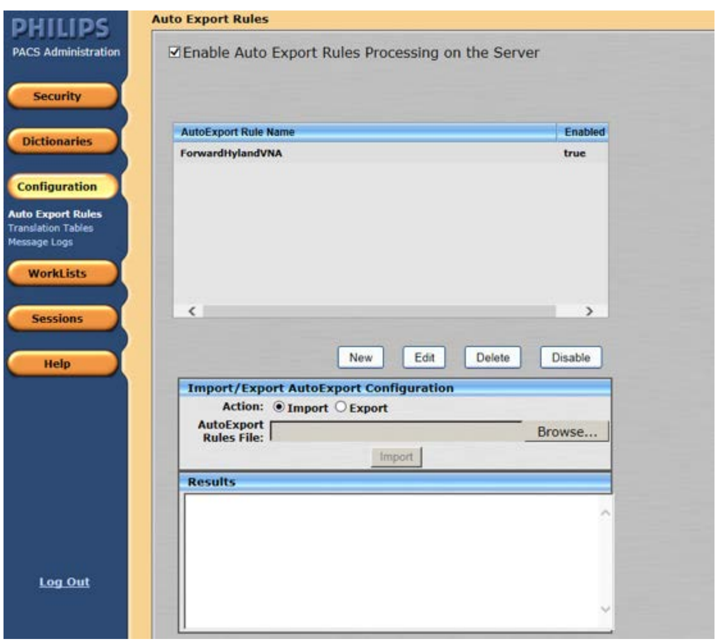
Refer to Section 2.2.2 for detailed installation guidance for Hyland VNA.

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

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

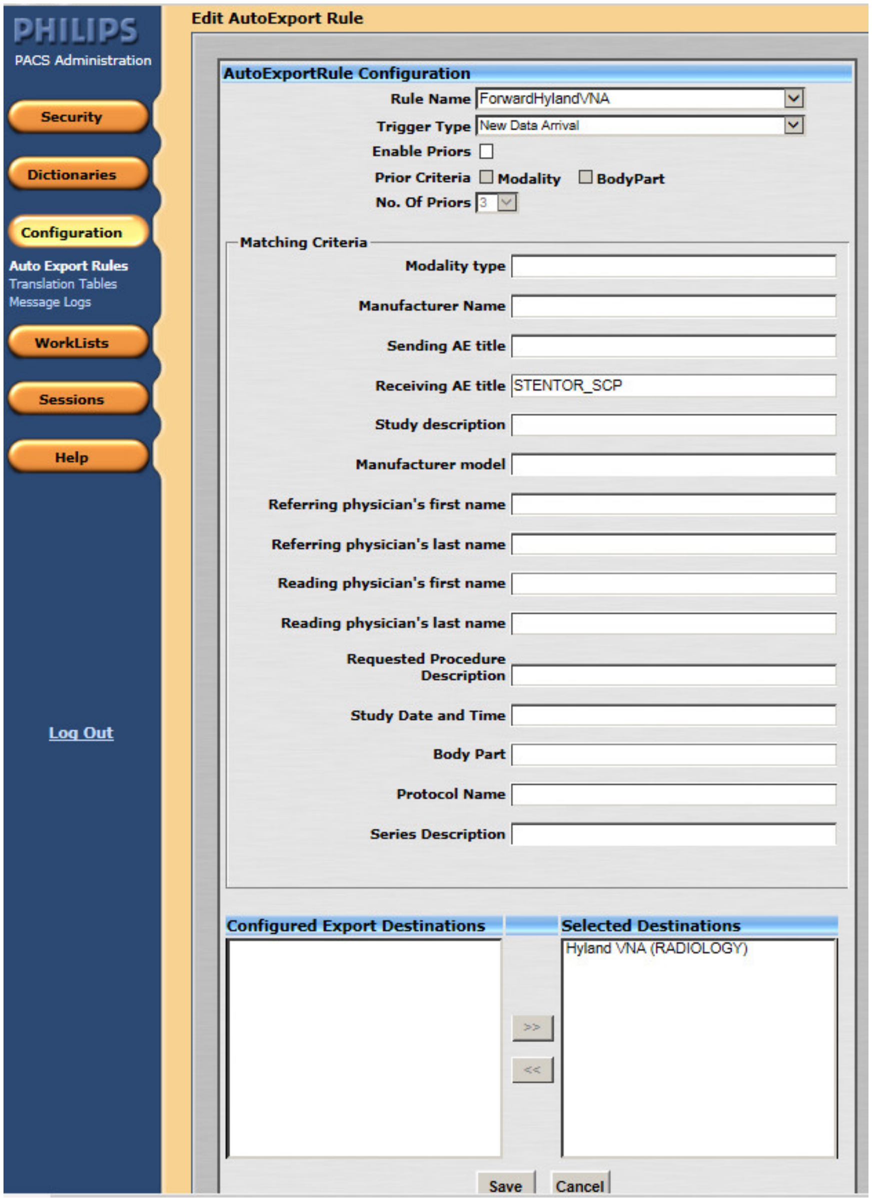


4. Log in to the IntelliSpace PACS Administration page using *https://192.168.140.131/PACSAdministration*.
5. Click the **Configuration** button on the left panel to configure the **Auto Export Rule.**
6. Click the **New** button to create a new rule named **ForwardHylandVNA**.



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

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



2.1.2 DCM4CHEE

DCM4CHEE is a collection of open source applications that communicate with each other using DICOM and HL7 standards for clinical-image management and archiving. In this study, DCM4CHEE has JBoss and a web-based graphical user interface (GUI) application built in. JBoss is used to configure DCM4CHEE to communicate with DVTk's Modality Emulator to store images in a PostgreSQL database. The JBoss web interface allows an administrator to configure DCM4CHEE to listen for connection requests from specific application entities like DVTk's Modality Emulator. DCM4CHEE also has web-based GUI that displays patient records sent from the Modality Emulator and stored in the PostgreSQL database.

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

System Requirements

CPU: 4

Memory: 512 megabyte (MB) RAM

Storage: 200 MB

Operating System: Microsoft Windows Server 2016 Datacenter

Network Adapter: Virtual Local Area Network (VLAN) 1402

DCM4CHEE Installation

The installation guide can be found at [5].

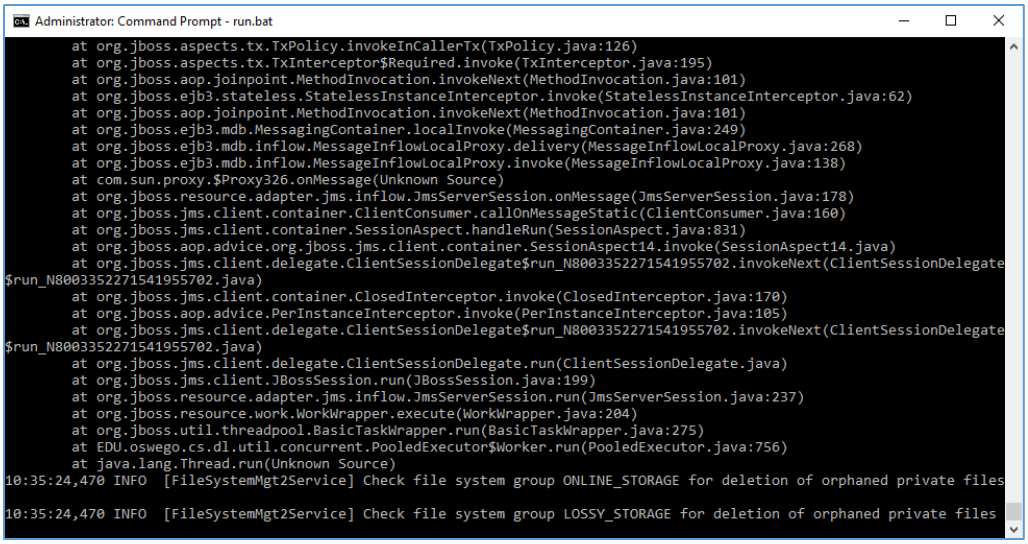
1. Go to https://www.dcm4che.org to download the software.
2. In the left-hand side of the page, click the **Wiki** link under Community.
3. Click the **here** link under **Download Latest Version** nest to **dcm4chee DICOM Archive 2 (includes dcm4che toolkit 1.4)** [6] link on the right-hand side of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

DCM4CHEE Audit Report Repository Installation

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

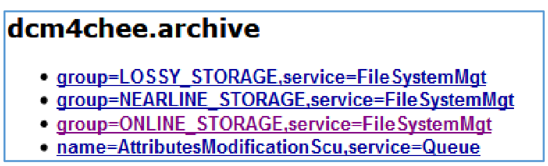
Test the DCM4CHEE Installation

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

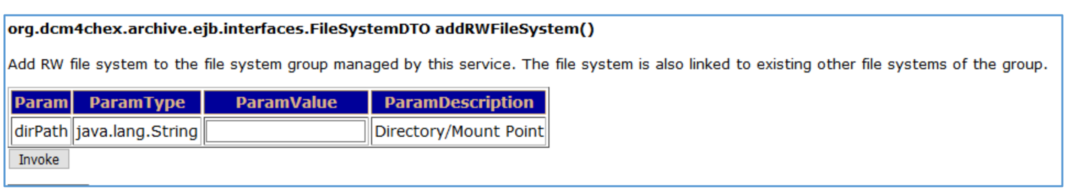


DCM4CHEE Configuration Using the JMX Console

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



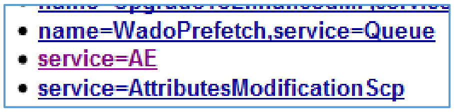
3. Click the **Invoke** button under the **addRWFileSystem()** section to instantiate where archived data should be stored. If no specific file path is provided as a parameter, the default location is *dcm4chee-2.7.1-psql\server\default\archive.*



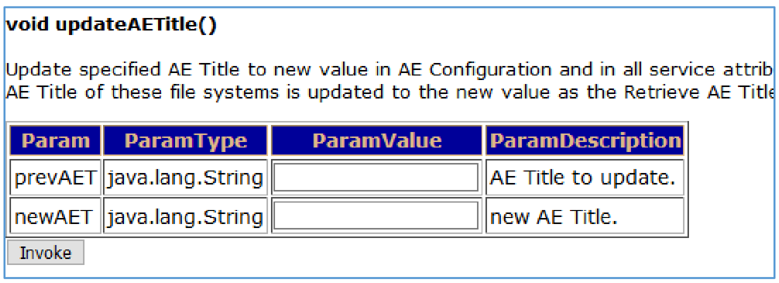
4. Change the default AE Title:

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

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



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

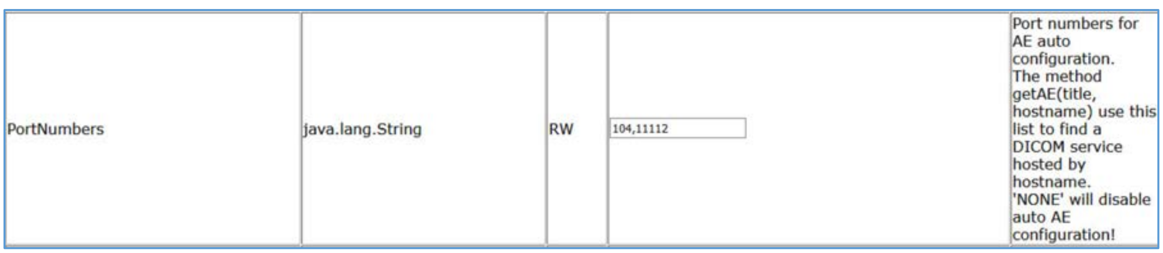

void updateAETitle()

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

Param	ParamType	ParamValue	ParamDescription
prevAET	java.lang.String		AE Title to update.
newAET	java.lang.String		new AE Title.

Invoke

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

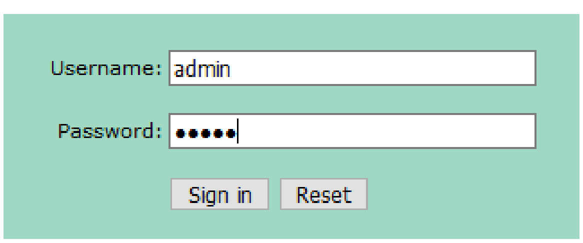


PortNumbers	java.lang.String	RW	104,11112	Port numbers for AE auto configuration. The method getAE(title, hostname) use this list to find a DICOM service hosted by hostname. 'NONE' will disable auto AE configuration!

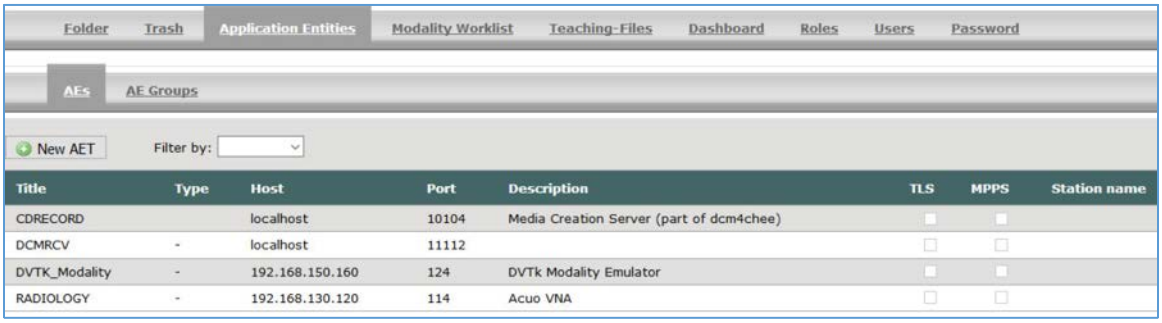
DVTk Modality to DCM4CHEE Configuration

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

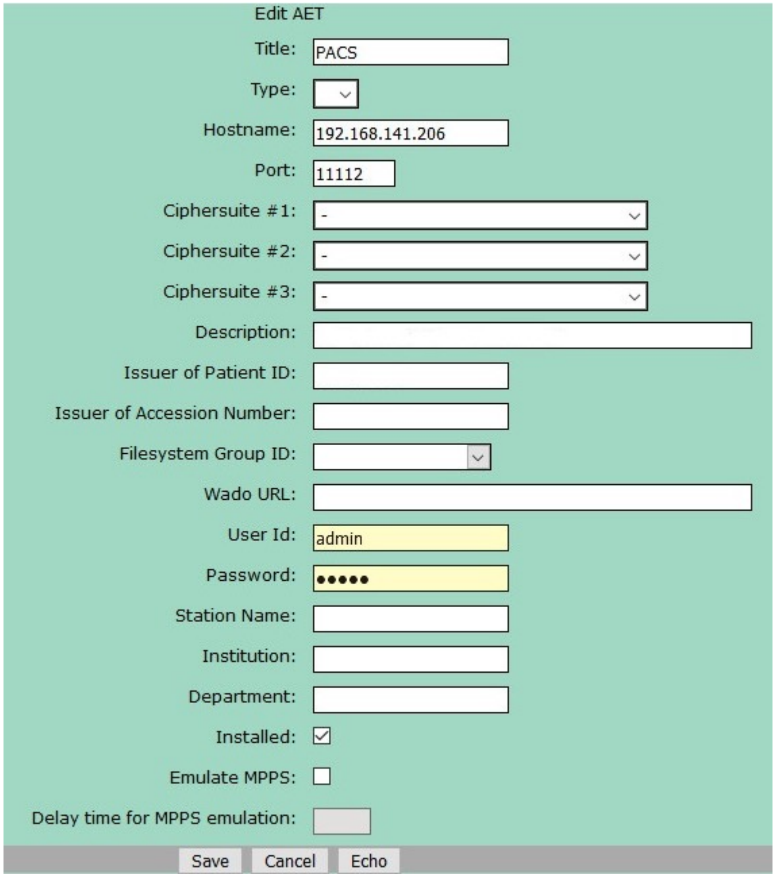
- **Username**: admin
- **Password**: *****



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

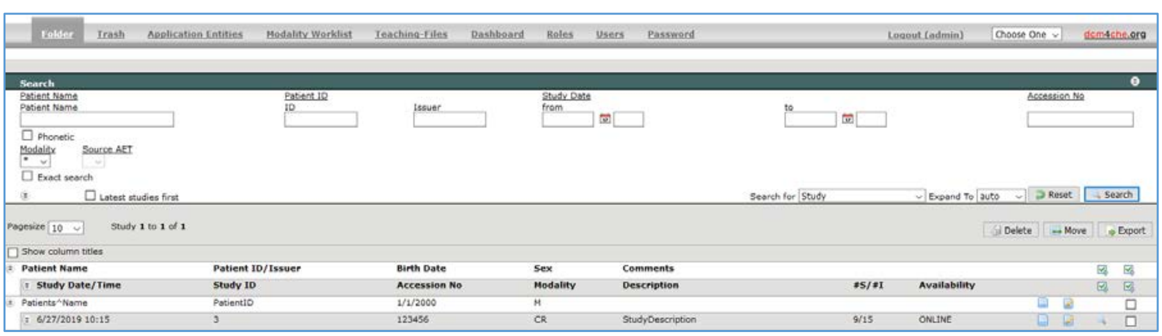


3. Click the **New AET** button in the left-hand side of the AEs page and provide the following information:
   - **Title**: PACS
   - **Type**: -
   - **Hostname**: *192.168.141.206*
   - **Port**: 11112
   - **User Id**: Admin
   - **Password**: *****
4. Click the **Save** button at the bottom center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



View Stored Data

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



DCM4CHEE to DVTk Modality Configuration

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

   RIS System

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

   MPPS Manager

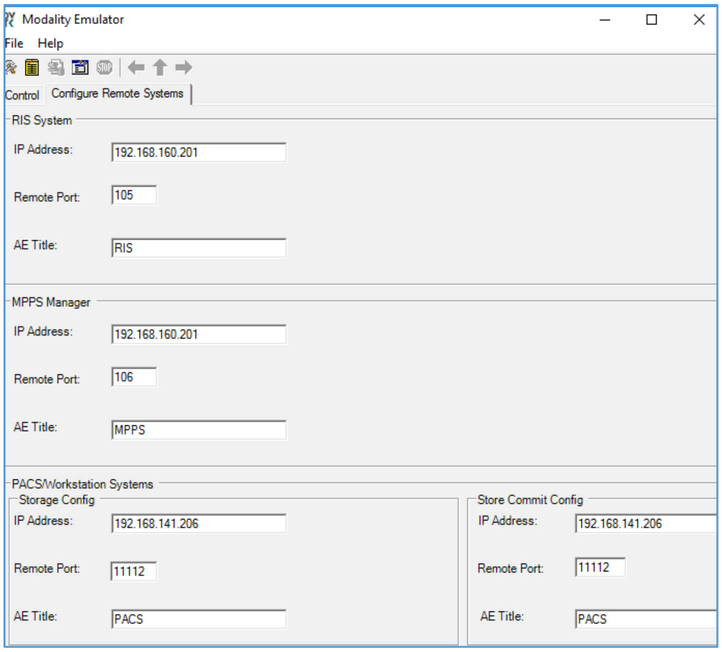
   - **IP Address:** *192.168.160.201*
   - **Remote Port:** 106
   - **AE Title:** MPPS

   PACS/Workstation Systems–Storage Config

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

   PACS/Workstation Systems–Storage Commit Config

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



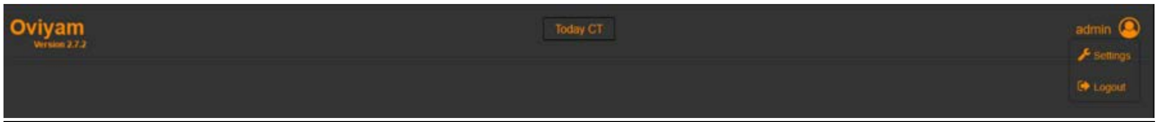
Oviyam Installation

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

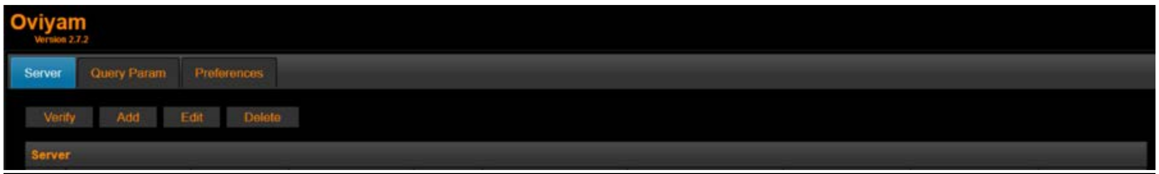
Oviyam Configuration

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

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



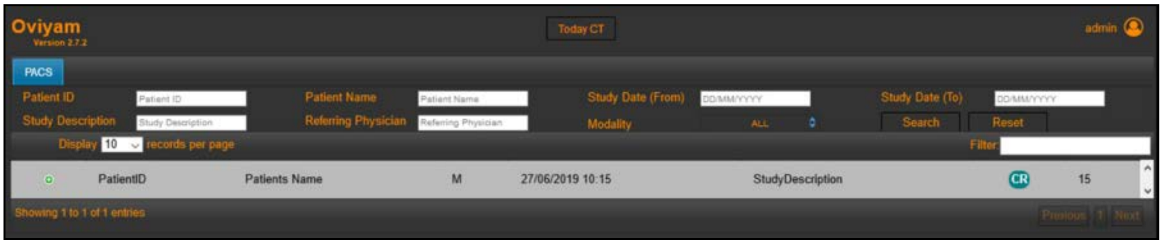
3. Under the **Server** tab, click **Add**.



4. Fill in the PACS server parameters and click the **Save** button located to the far right of the parameters.
   - **Description:** PACS
   - **AE Title:** DCM4CHEE
   - **Host Name:** localhost
   - **Port:** 11112
   - **Retrieve Type:** WADO
   - **WADO Context:** wado
   - **WADO Port:** 8080
   - **Image Type:** JPEG

5. Return to *http://dcm4chee_ip:8080/oviyam2* to see query parameters now available.
6. Click the **Search** button under the parameters on the right-hand side of the screen.

7. Double-click on a patient record.



8. View images related to that patient record.

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

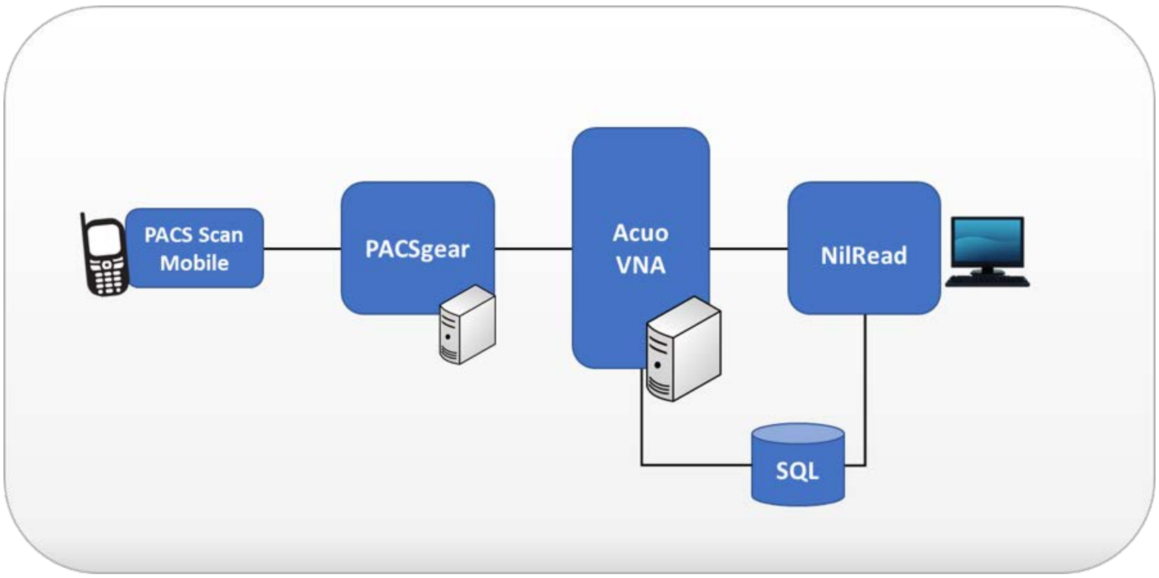
PACSgear Core Server: image processing and routing server, and back-end services

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

NilRead: enterprise image-viewing application

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

Figure 2-1 Hyland Systems and Applications Connectivity



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

2.2.1 Hyland Database Server

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

System Requirements

CPU: 4

Memory: 12 GB RAM

Storage:

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

Operating System: Microsoft Windows Server 2016

Network Adapter: VLAN 1801

Hyland Database Server Installation

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

Hyland Database Configuration

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

2.2.2 Hyland Acuo VNA

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

System Requirements

CPU: 6

Memory: 12 GB RAM

Storage:

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

Operating System: Microsoft Windows Server 2016

Network Adapter: VLAN 1301

Hyland Acuo VNA Installation

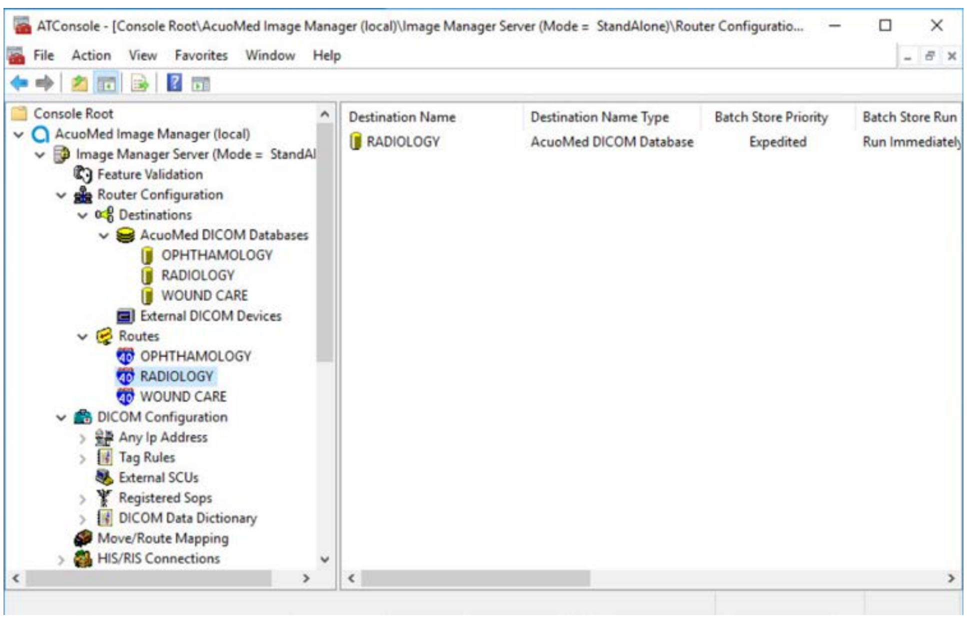
1. In the NCCoE test environment, the Hyland Acuo VNA was installed on a VM preconfigured with the OS and network requirements provided by Hyland. The project leveraged engineers supplied by Hyland to perform the installation.

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

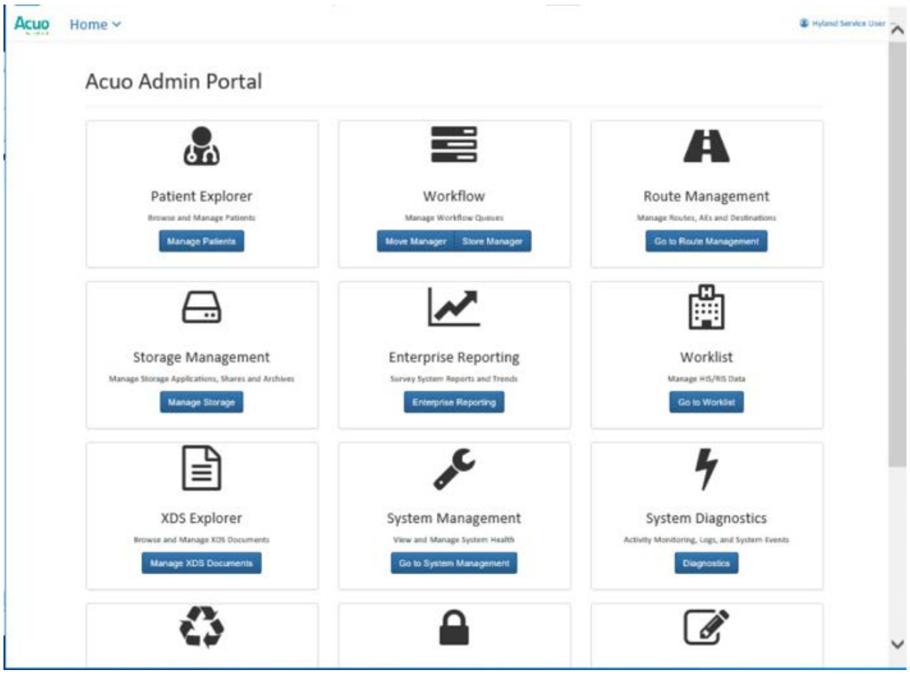
3. The installation created a web application for the AcuoAdmin Portal, where a Secure Sockets Layer (SSL) certificate signed by DigiCert was created and assigned to the application for hypertext transfer protocol secure (HTTPS) enforcement.

<u>Hyland Acuo VNA Configuration</u>

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



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



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

CPU: 4

Memory: 8 GB RAM

Storage:

- HD 1: 80 GB (OS Install)
- HD 2: 170 GB (Application)

Operating System: Microsoft Windows Server 2016

Network Adapter: VLAN 1501

PACSgear Core Server Installation

The installation of Hyland PACSgear Core Server was performed by Hyland engineers as listed below:

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

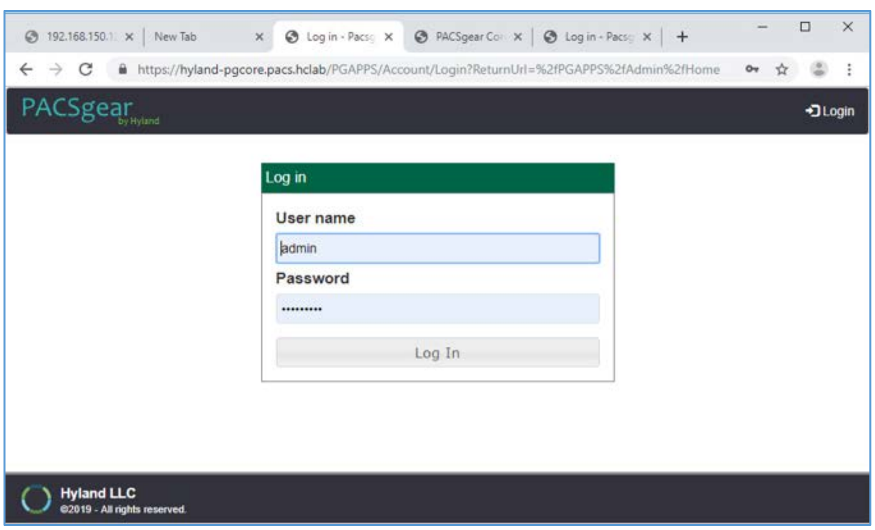
PACSgear Core Server Configuration

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

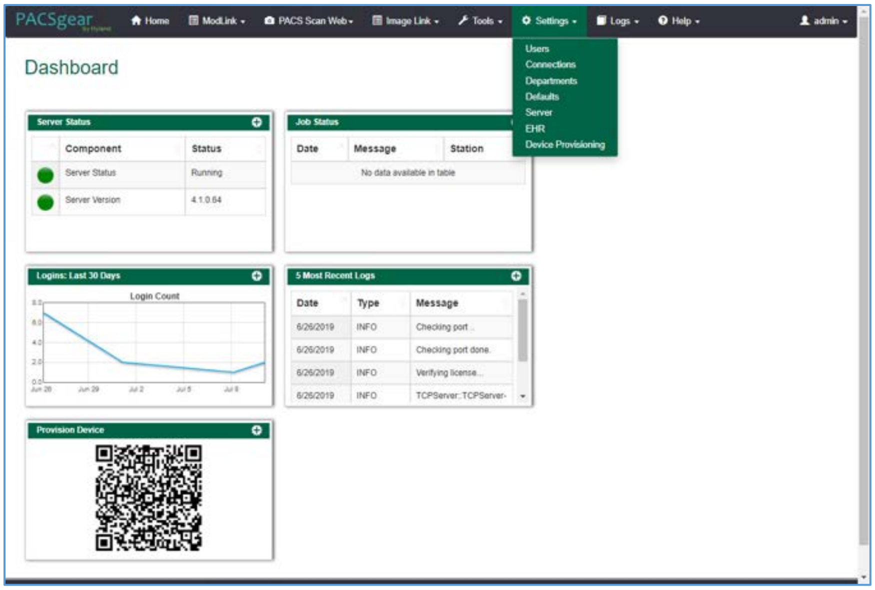
During the database configuration, the Hyland engineers created instances for representative departments (e.g., ophthalmology, radiology, and departments that may see patients who need wound treatment).

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

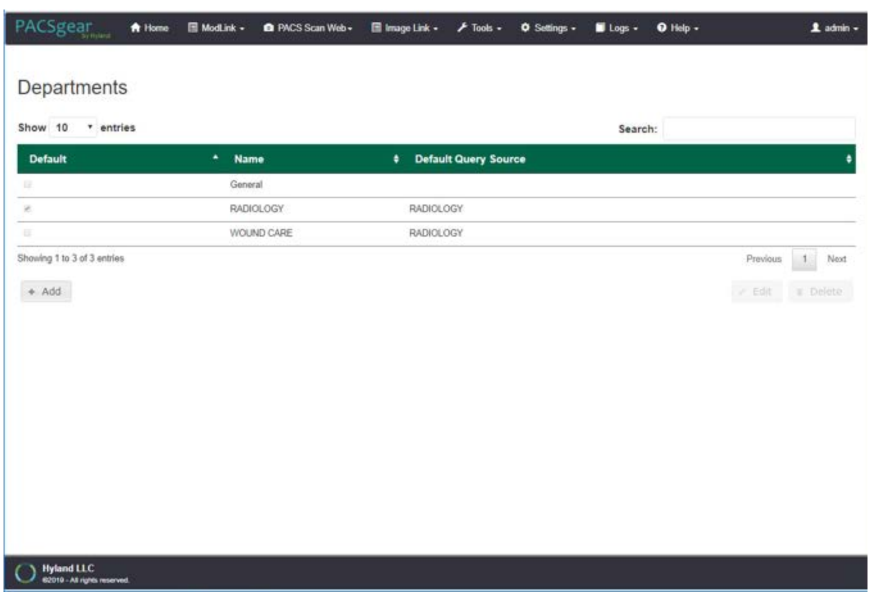
1. The Hyland engineers logged on to the PACSgear Admin portal by using *https:// hyland-pgcore.pacs.hclab/PGAPPS/Admin*.



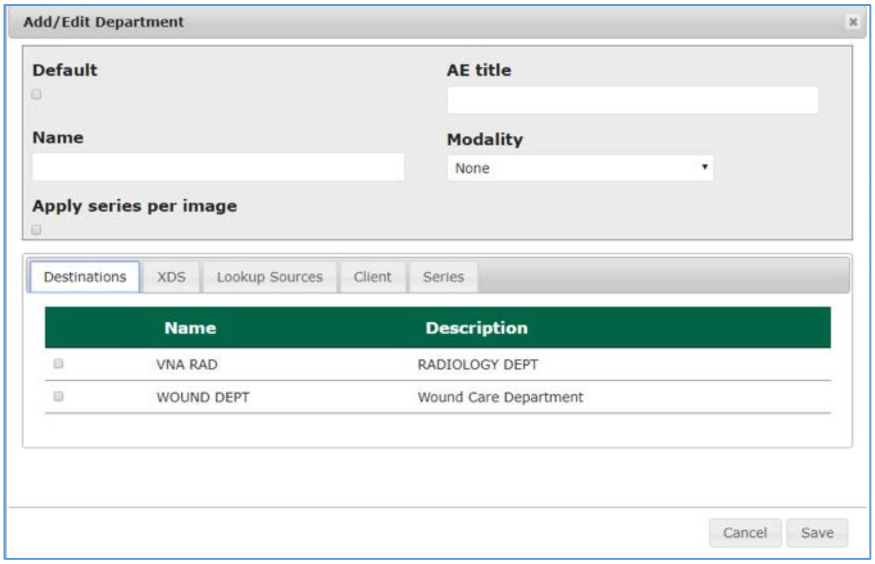
2. On the **Settings** menu, select **Departments.**



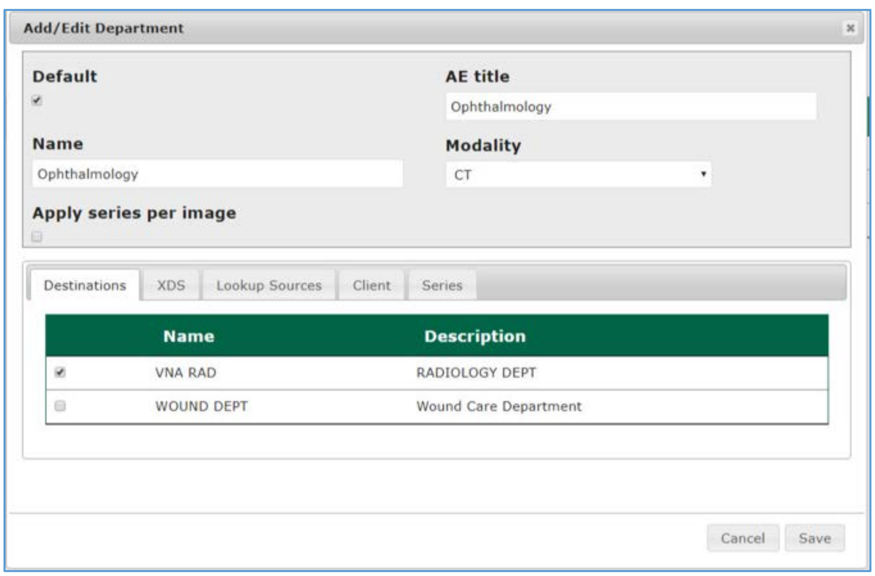
3. After selecting **Departments** from the **Settings** pull-down, the screen advances to a **Departments** screen. The **Departments** screen lists sample hospital departments created during the installation. The project then added a new department by clicking the **+ Add** button.



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

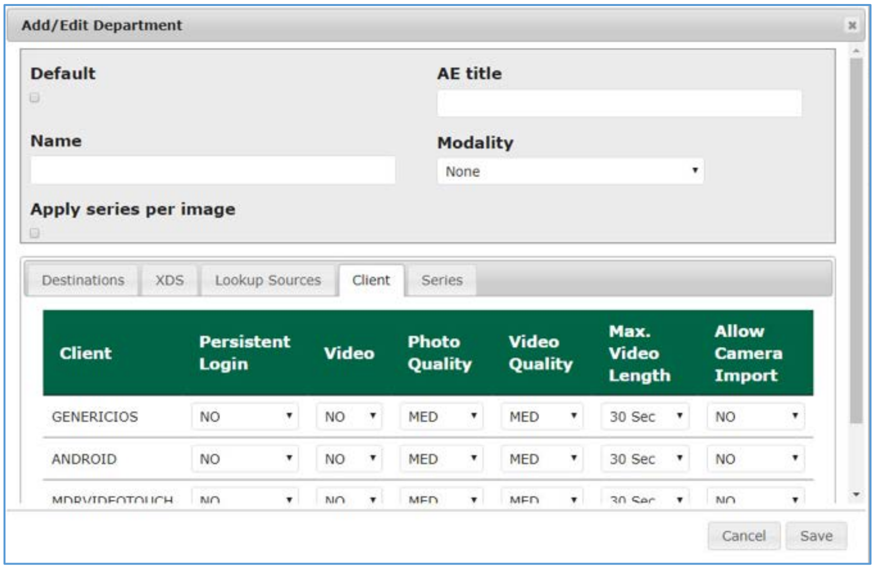


5. In the **Name** text box, the engineers entered **Ophthalmology** to create a department that ties with the Ophthalmology database instance created during database configuration. Engineers also added the **AE title** as **Ophthalmology** and selected a **CT Scan** for the modality.



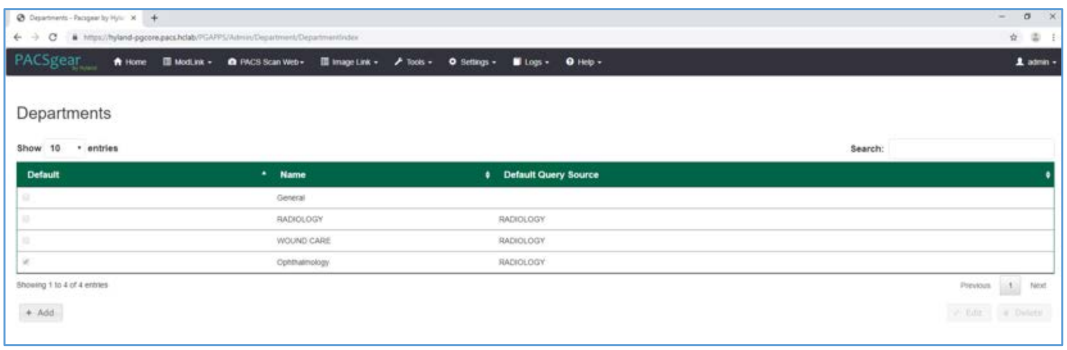
6. On the **Destinations** and **Lookup Sources** tabs, the engineers set up the destination and lookup sources for each department.

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



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

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

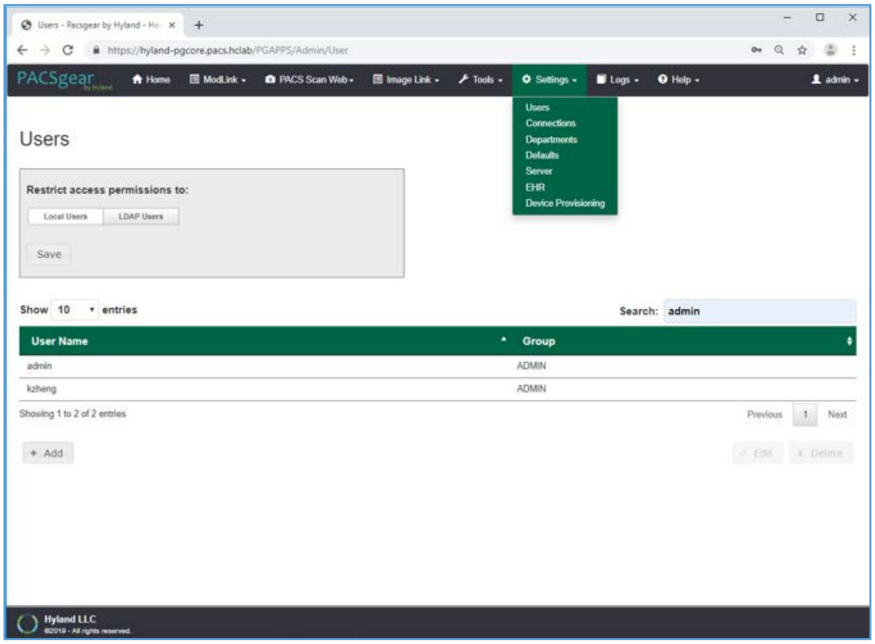


<u>Add LDAP/Active Directory Server: -</u> to use an LDAP/Active Directory server, configure these parameters:

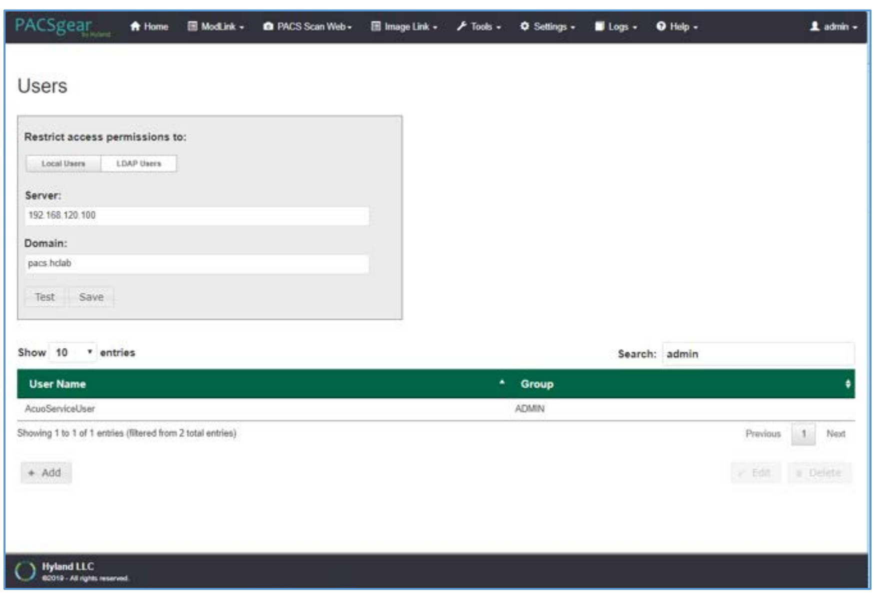
1. Create an **LDAP_User** account in Active Directory before proceeding.

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.**



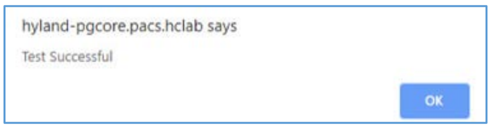
4. On the **Users** screen, navigate to **Restrict access permissions to:** and click on the **LDAP Users** button. Enter **192.168.120.100** to populate the Server text box, and then enter **pacs.hclab** for Domain.



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

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

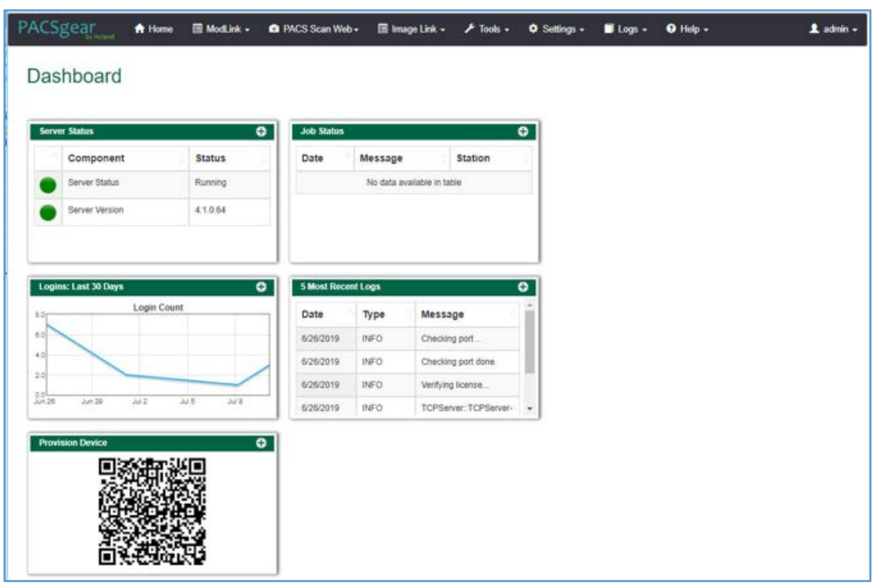
7. A message box appears indicating the test is successful. Click **OK.**



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

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

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



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

4. Point the camera at the **QR code** on the PC screen until a message box appears indicating **Setting Updated Your settings have been updated**. This setting configures the mobile **PACS Scan app** to the address of its **PACSgear Core Server** instance.

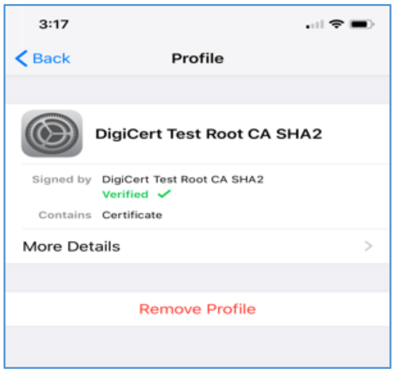
5. From a workstation, acquire the trusted root certificate from DigiCert. Further information for using DigiCert is described in Section 2.6.2.

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

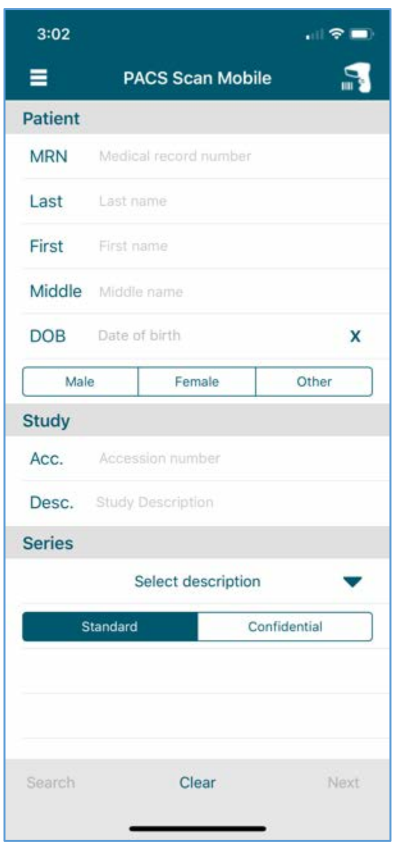
7. The installer opens the email from the iPhone and double-clicks on the attachment to install the certificate to the device.

8. To verify the certificate installation, go to **Settings > General > Profiles & Device Management** to list all the certificates profiles.

9. Find the certificate you installed and click to display the detail. Below is an example:



10. To verify the PACS Scan Mobile App functionality, from the iPhone, double-click the **PACS Scan App.** The log in page will display. Use an account and password that has been associated with a clinical department to log in. Successful log in 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 found below.

System Requirements

CPU: 6

Memory: 12 GB RAM

Storage:

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

Operating System: Microsoft Windows Server 2016

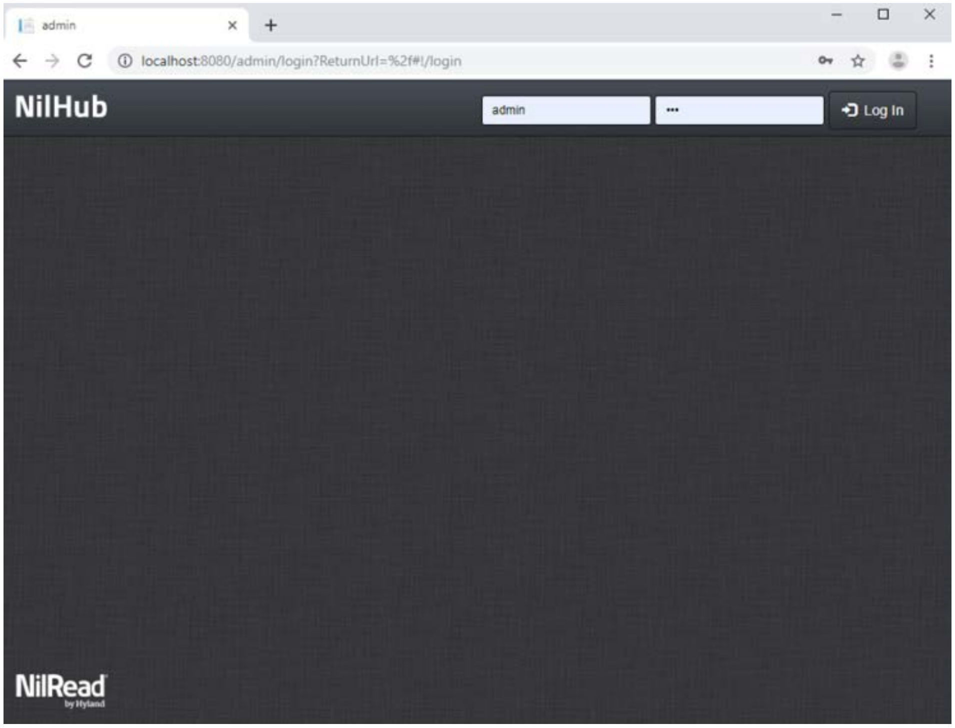
Network Adapter: VLAN 1301

Hyland NilRead Installation

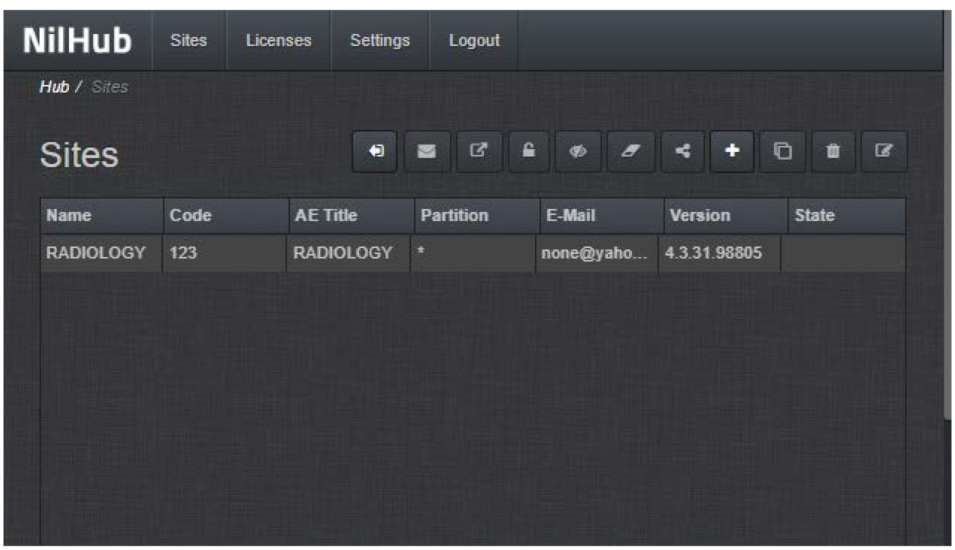
1. The installation of Hyland NilRead was performed by Hyland engineers based on Hyland's proprietary installation package and installation guides. NilRead has three services: the Hub Front End service, Nil Back End service, and Nil Front End service. The Hub Front End service is used to provide management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

Hyland NilRead Configuration

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



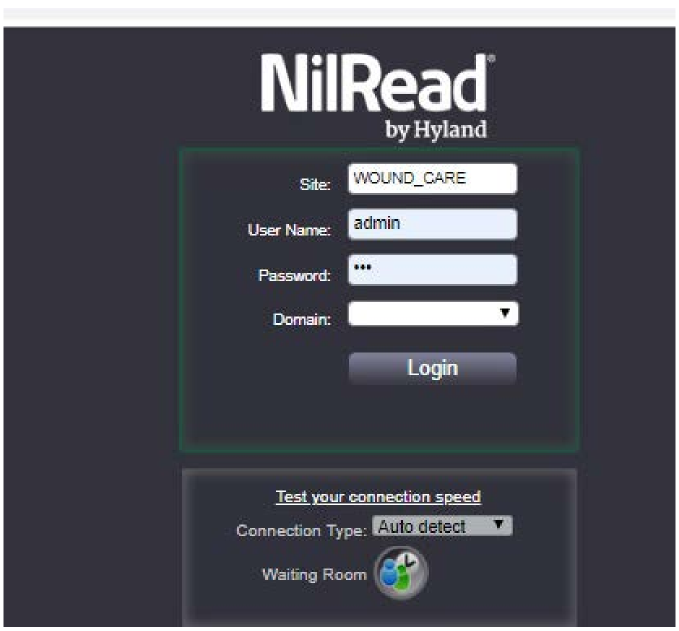
1. To add a new site from the **NilHub** home page, click on the Sites tab in the top left-hand side of the screen.



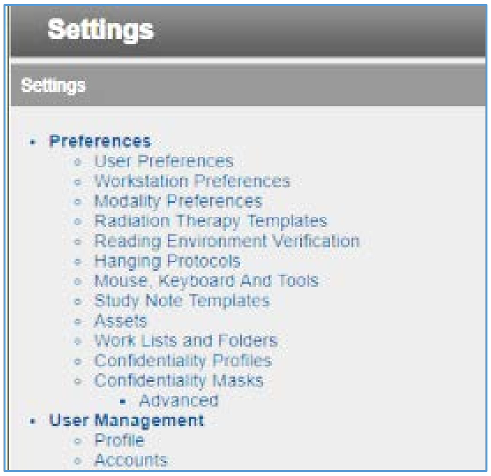
2. Click on the **+** icon on the right-hand side of the screen, to create a new **Site** for **WOUND_CARE** department, and provide the information below, and then click **Save.**

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

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



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



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** the user needs access to and click the **Add** button.
7. Specify the **Granted Privileges** the user needs to have 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 implements DICOM TLS between the Acuo VNA and IntelliSpace PACS via mutual authentication as part of the TLS handshake protocol [10].

2.3.1 Public Key Infrastructure (PKI) Certificate Creation

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

2.3.1.1 Create PKI Certificate for Hyland Acuo VNA

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

2.3.1.2 Create PKI Certificate for Philips IntelliSpace PACS

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

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

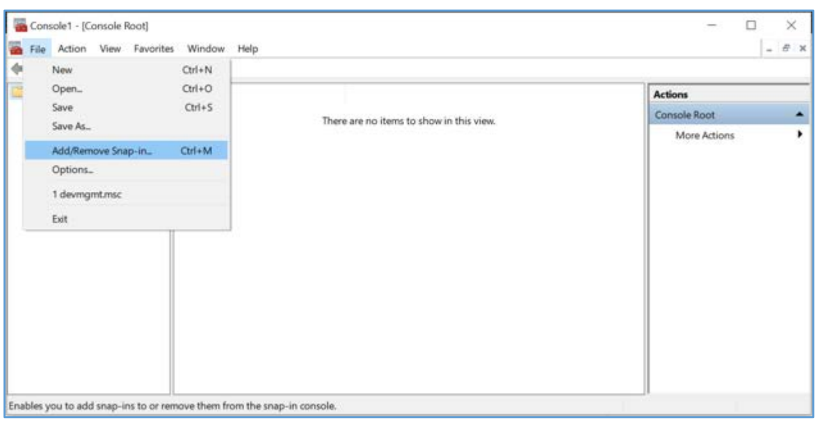
2.3.2 PKI Certification Installation

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

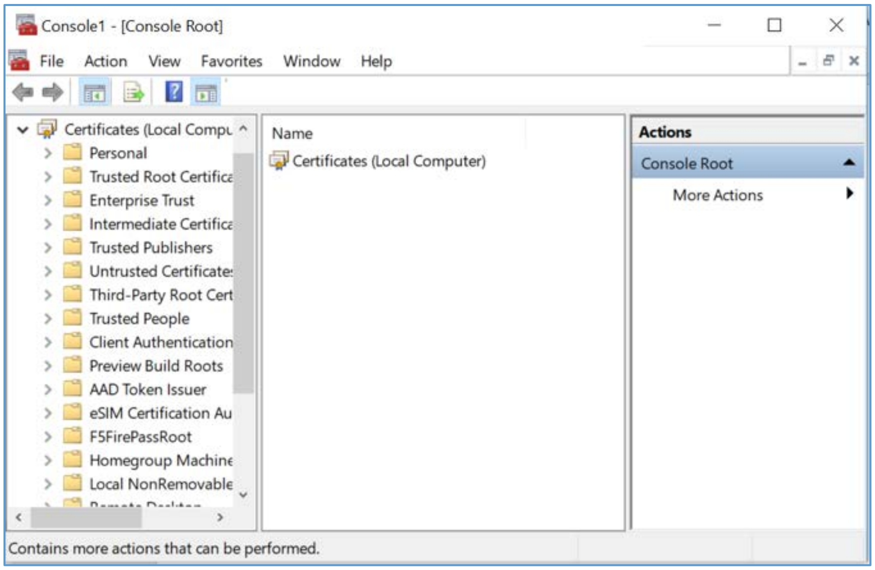
2.3.2.1 Install PKI Certificate for Hyland Acuo VNA

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

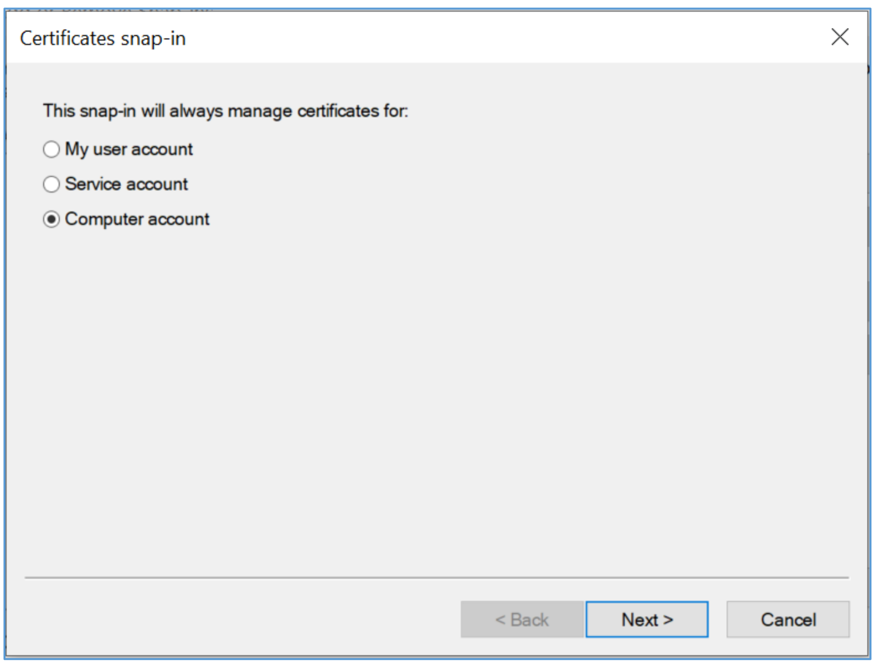
1. From the Acuo server, click on **Start > Run > mmc.**
2. Select **File > Add/Remove Snap-in…**



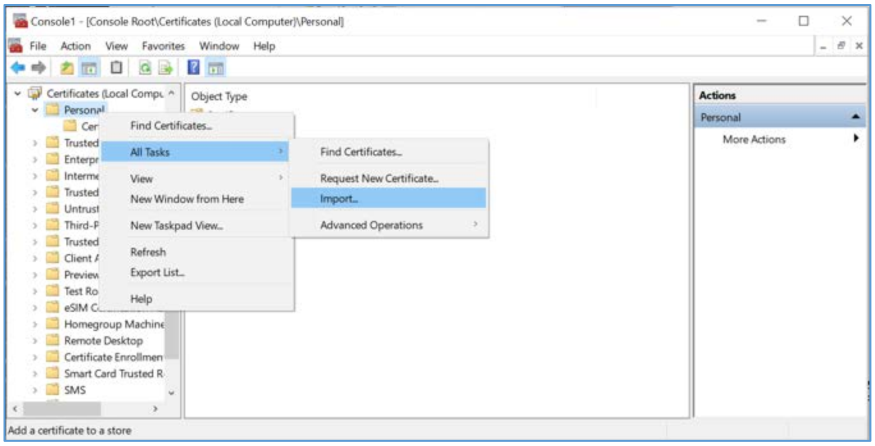
3. Select **Certificates** and click **Add**.
   - Choose **Computer Account**
   - Choose **Local Computer**
4. Click **Finish**, then click **OK**.



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**.



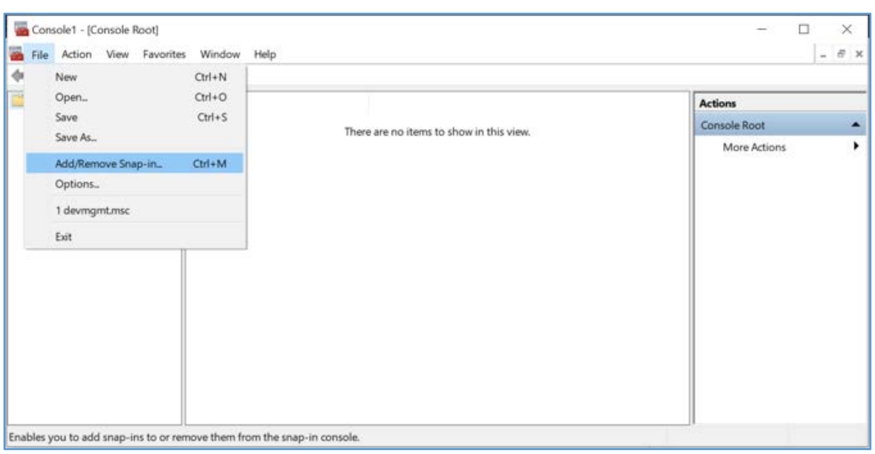
7. Add the appropriate permissions to the newly generated certificate private key.
    a. Navigate to **Certificates > Personal > Certificates**.
    b. Right click on the certificate, select **All Tasks > Manage Private Keys…**
    c. Add the **AcuoServiceUser** and grant full control permissions. Click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

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

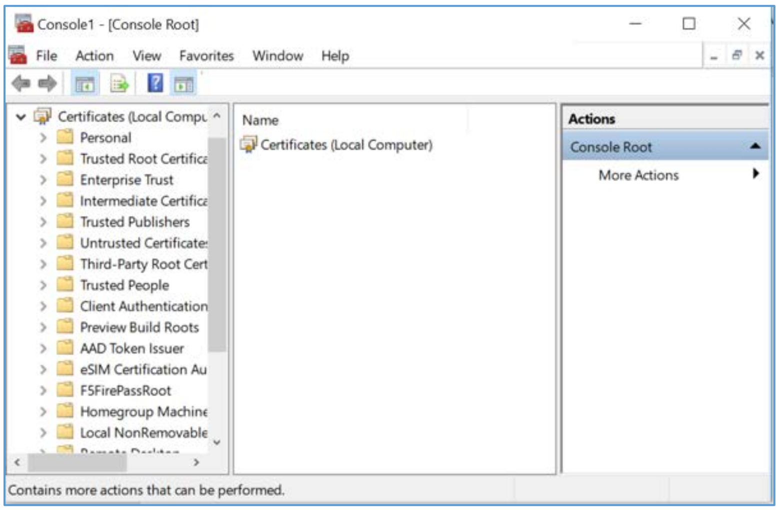
2.3.2.2 Install PKI Certificate for Philips IntelliSpace PACS

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

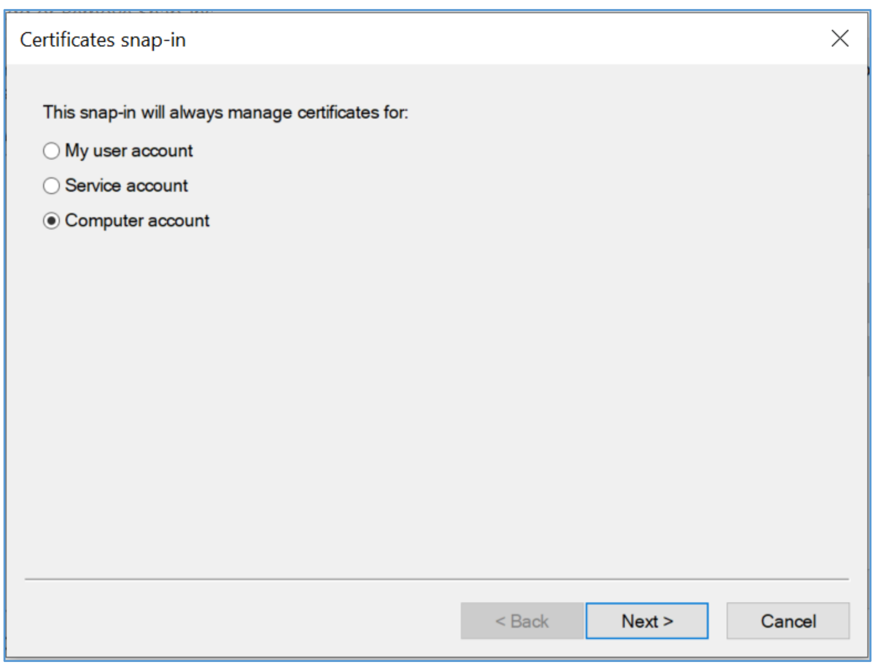
1. From the IntelliSpace server, click on **Start** > **Run** > **mmc**.
2. Select **File** > **Add/Remove Snap-in…**



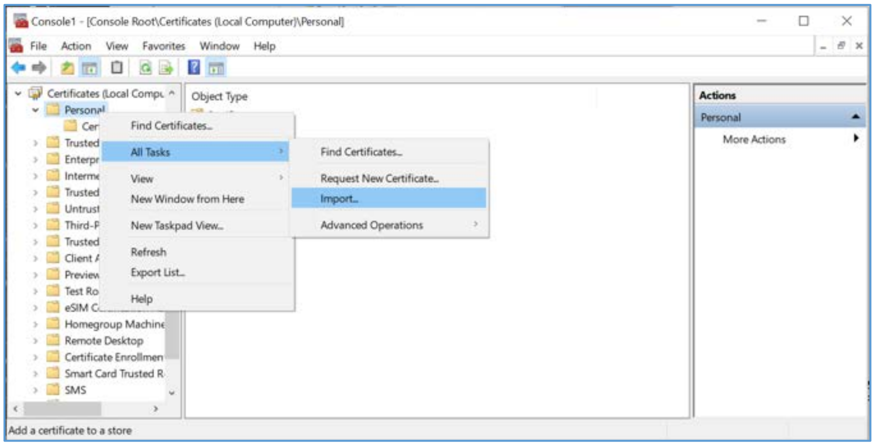
3. Select **Certificates** and click **Add**.
    a. Choose **Computer Account**.
    b. Choose **Local Computer**.
    c. Click **Finish**; click **OK**.



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

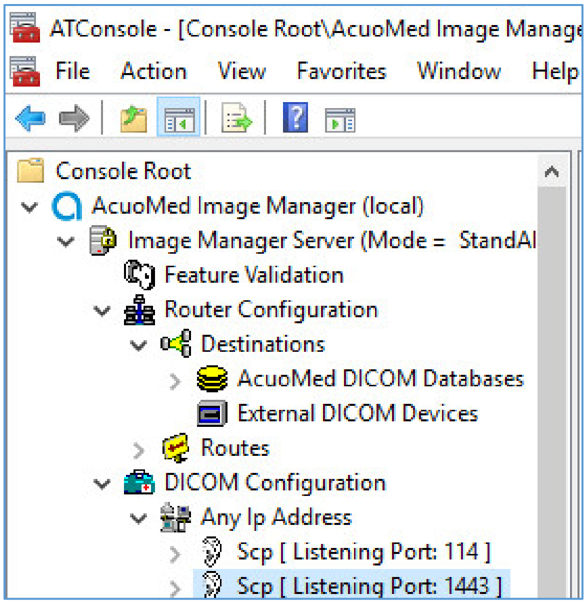
2.3.3 TLS Secure DICOM Configuration

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

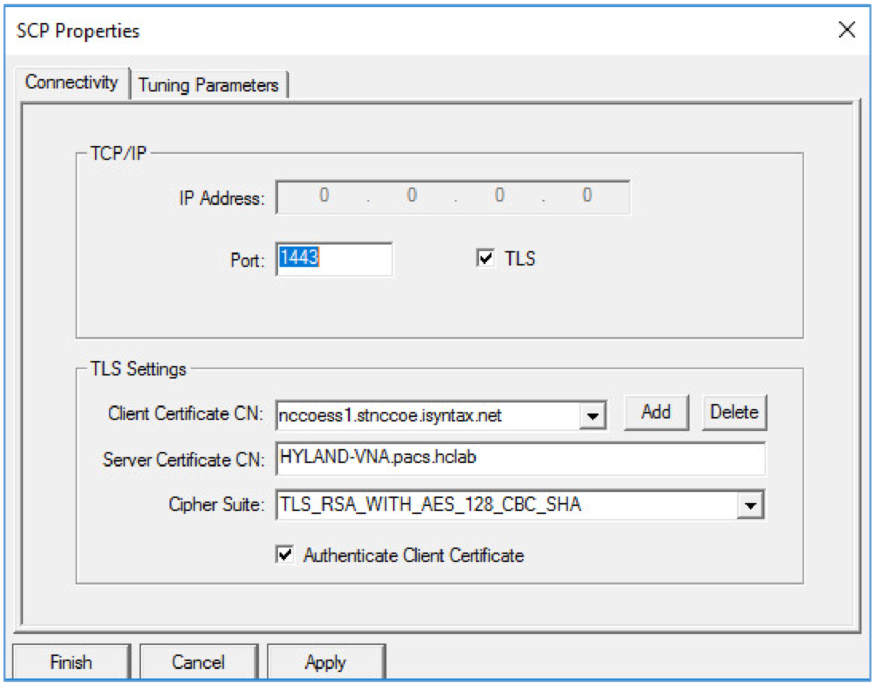
2.3.3.1 TLS Configuration for Hyland Acuo VNA

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

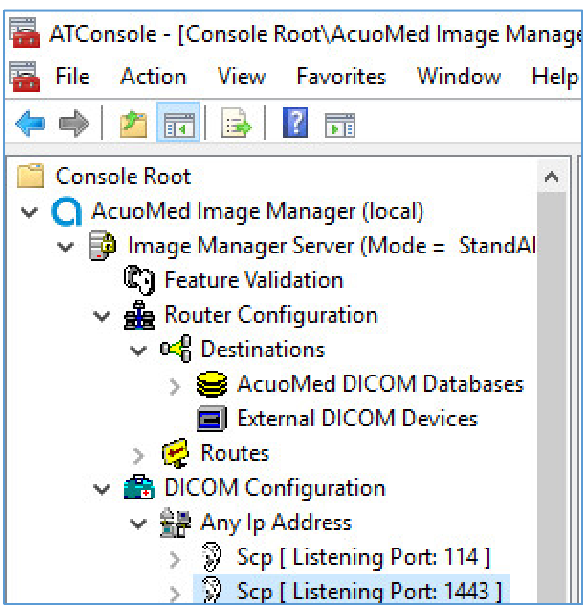
1. Open Microsoft **MMC** to access the **AcuoMed Image Manager (local):**
2. From the **Console > AcuoMed Image Manager (local) > DICOM Configuration**, right click **Any Ip Address > New Scp …** to create a new SCP for TLS encryption.



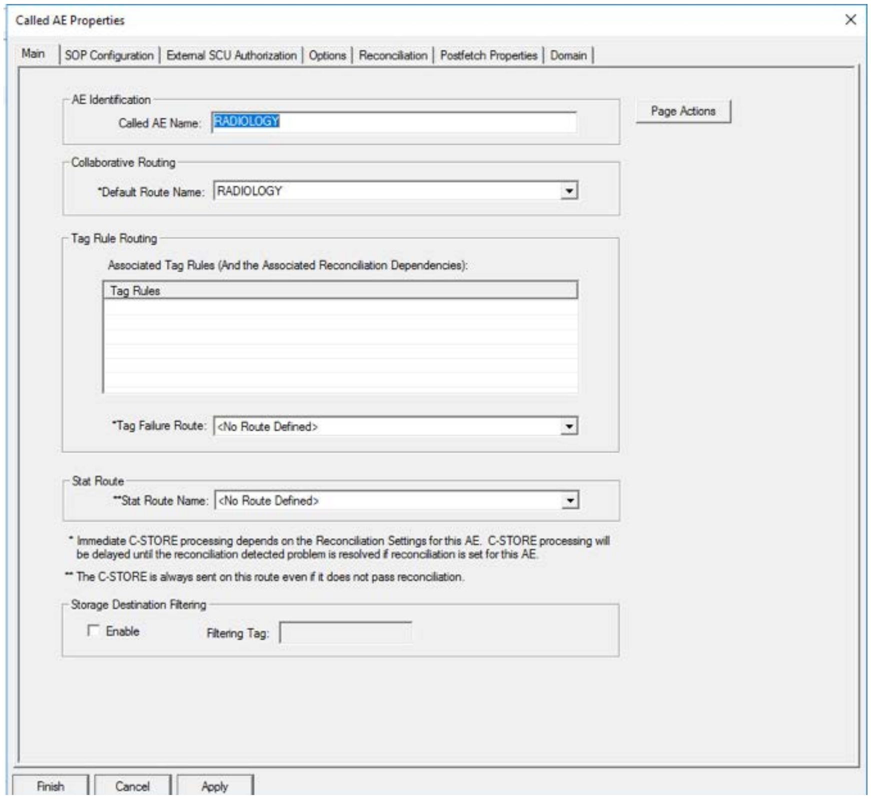
3. On the **Connectivity** tab of the **SCP** Properties page, provide the information below and click **Add**, **Apply,** and then **Finish**:
   - **Port**: 1443
   - Check the **TLS** checkbox
   - **Client Certificate CN**: nccoess1.stnccoe.issyntax.net
   - **Server Certificate CN**: HYLAND-VNA.pacs.hclab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



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

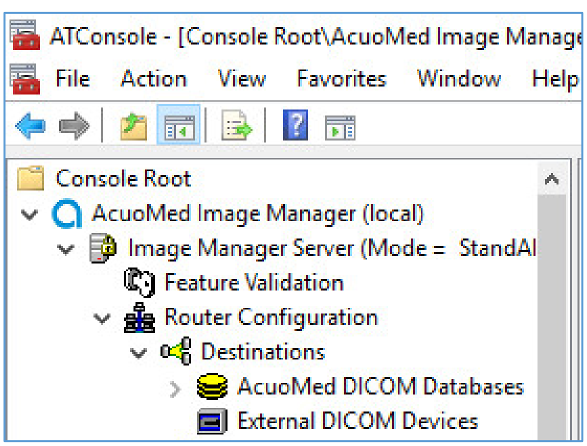


5. Fill in the **Called AE Name**: e.g., **RADIOLOGY** and **Default Route Name**: e.g., **RADIOLOGY**. After populating the information, click **Add.**

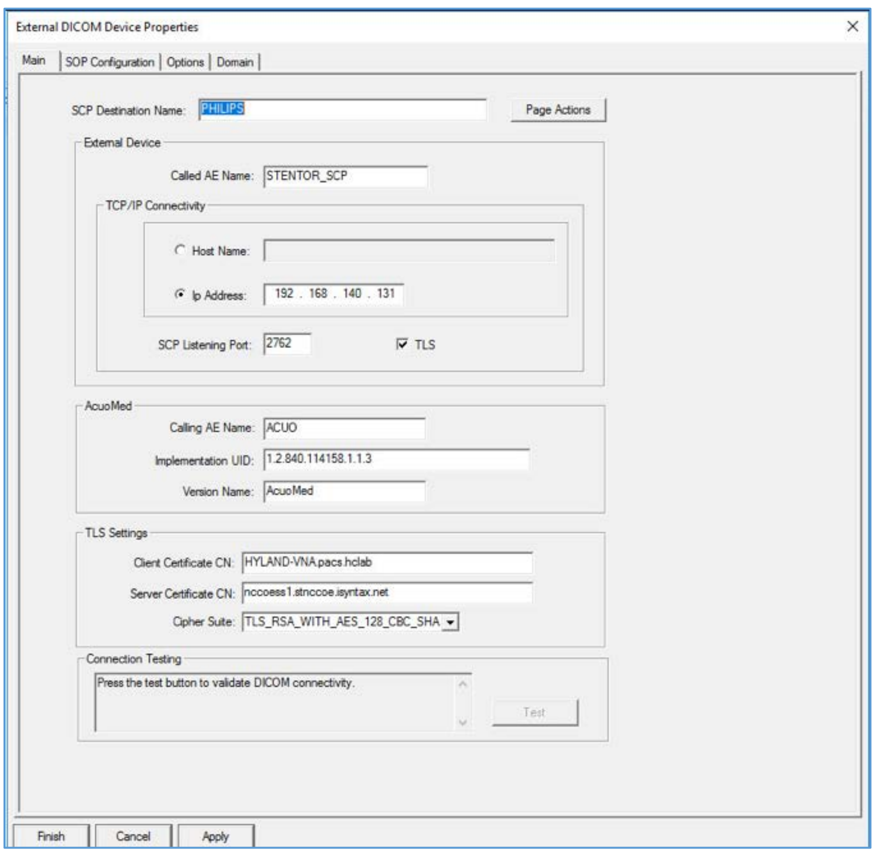


For sending TLS DICOM message to IntelliSpace PACS, configure an External DICOM Device from the Acuo VNA by using Microsoft Windows Console.

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



3. On the **Main** tab of the **External DICOM Devices Properties** page, provide the information below and click **Apply,** and then click **Finish:**
    - **SCP Destination Name**: PHILIPS
    - **Called AE Name**: STENTOR_SCP
    - **IP Address**: 192.168.140.131
    - **SCP Listening Port**: 2762
    - Enable TLS by clicking the **TLS** checkbox next to the listening port number.
    - **Called AE Name**: ACUO
    - **Implementation UID**: 1.2.840.114158.1.1.3
    - **Client Certificate CN**: HYLAND-VNA.pacs.hclab
    - **Server Certificate CN**: nccoess1.stnccoe.isyntax.net
    - **Cipher Suite**: TLS_RSA_WITH_AES_128_CBC_SHA

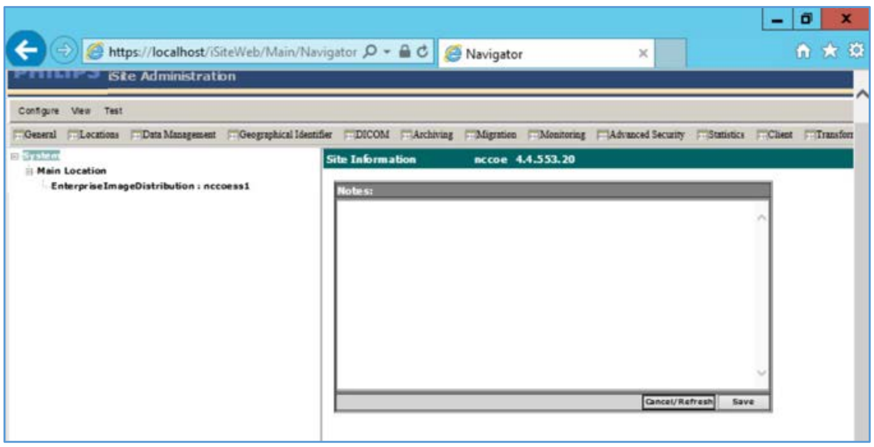


4. Restart the **AcuoMed** service.

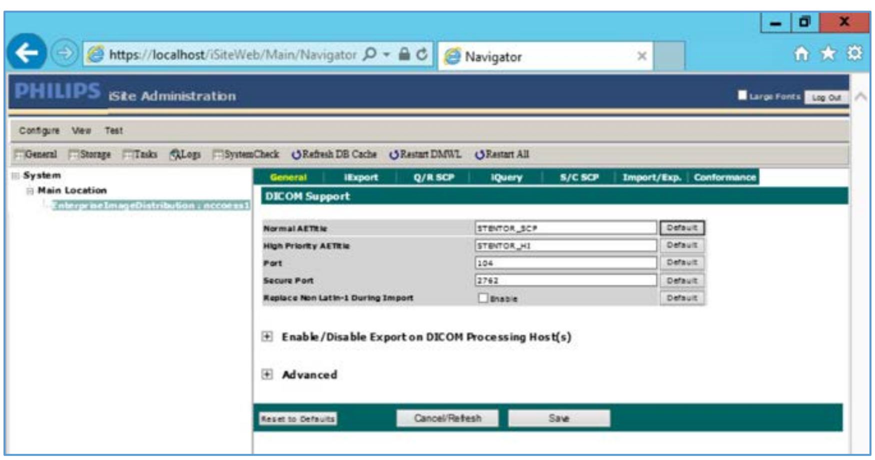
2.3.3.2 TLS Configuration for Philips IntelliSpace PACS

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

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

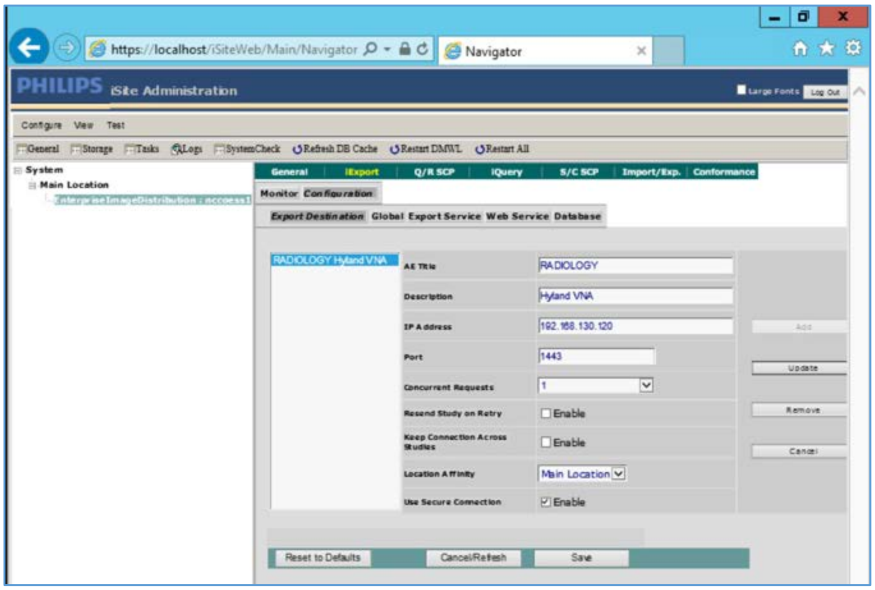


2. Click **Configuration** > **DICOM,** to navigate to DICOM configuration screen.

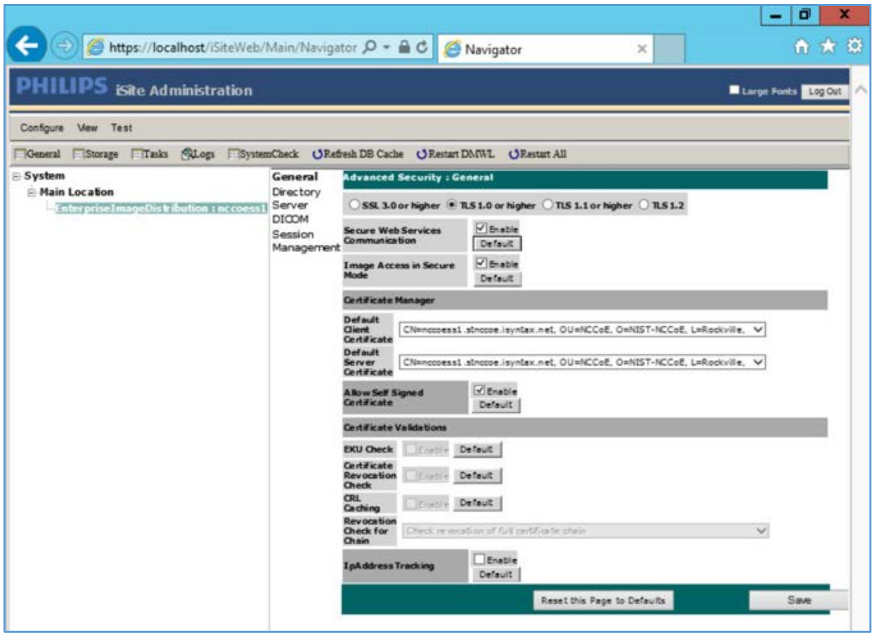


3. On the top menu, click **iExport** to open the **iExport** screen. Provide the information below, and click **Save:**
   - **AE Title**: RADIOLOGY
   - **Description**: Hyland VNA
   - **IP Address**: 192.168.130.120

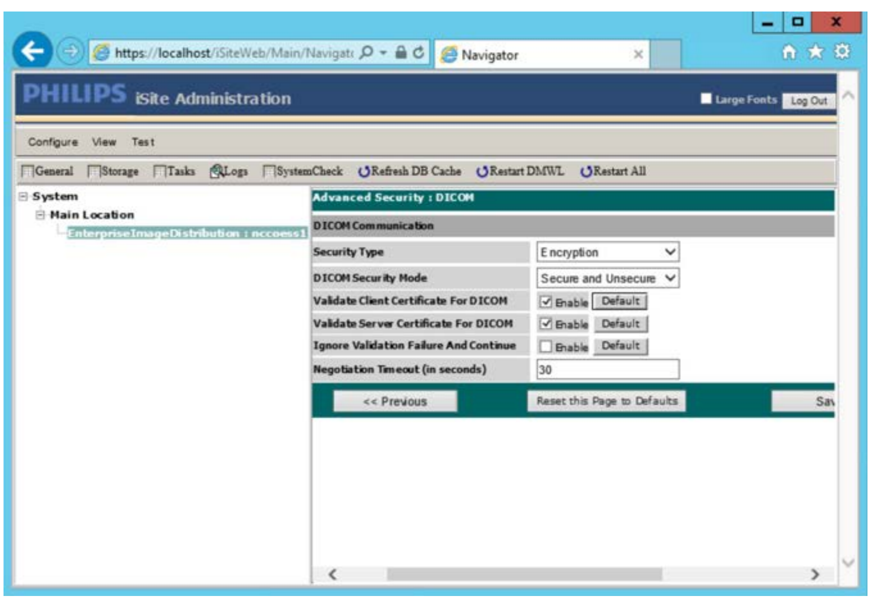
- **Port**: 1443
- **Use Secure Connection**: checked



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



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, both the Acuo VNA and IntelliSpace PACS servers are ready to perform the TLS secure DICOM communication tests. The secure DICOM communication tests were conducted for bi-direction data exchanges between Acuo VNA and IntelliSpace PACS to confirm:

DICOM communication is still functional.

DICOM communication is encrypted.

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

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

2.4 Modalities

2.4.1 DVTk Modality Emulator

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

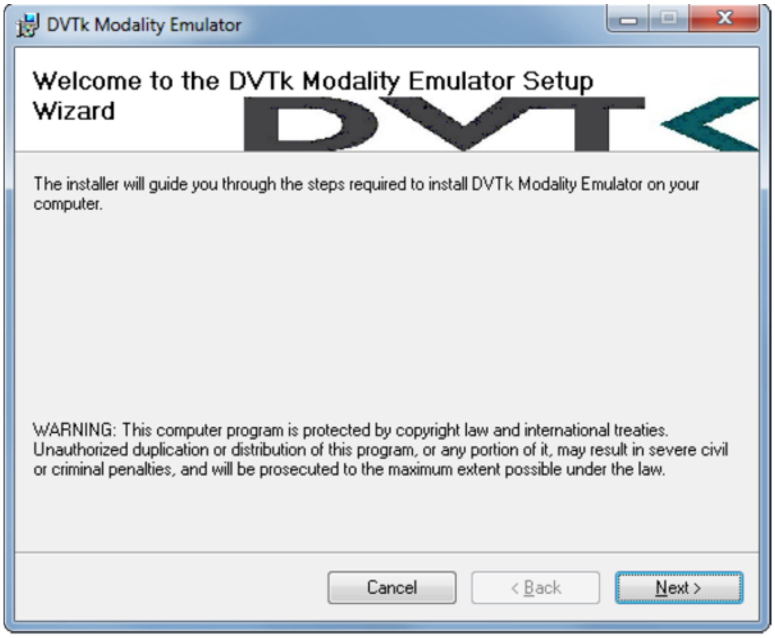
System Requirements

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

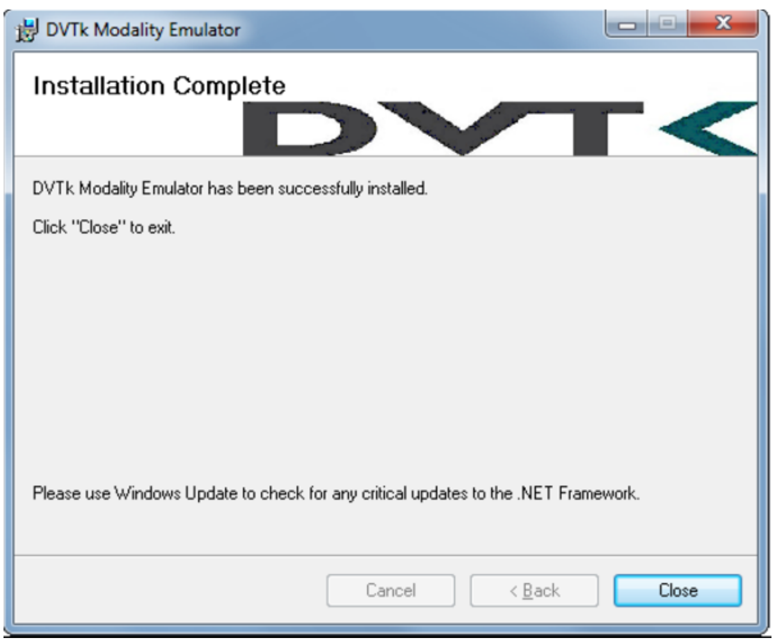
Network Adapter: VLAN 1402

DVTk Modality Installation

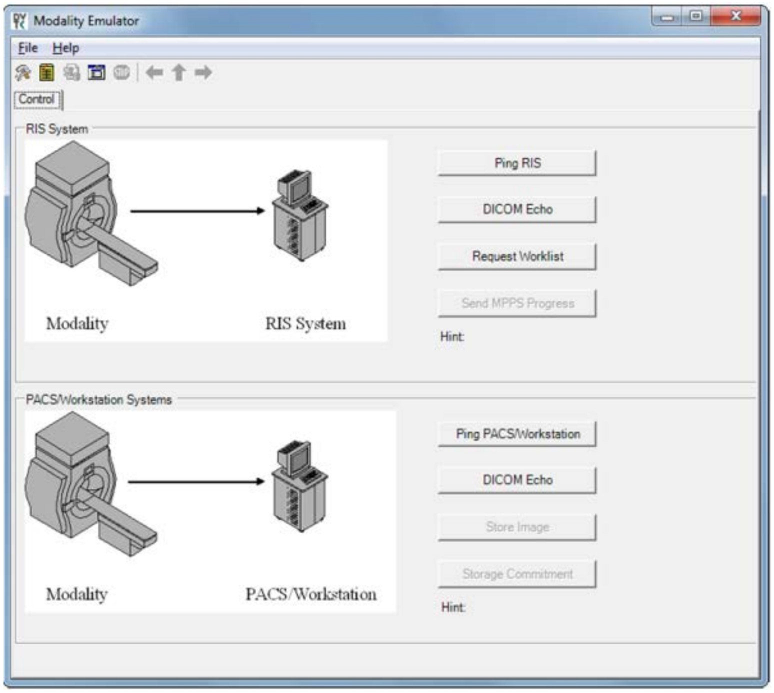
1. Download the installation software from the DVTK site [11].
2. Click the **Modality Installation** file (e.g., *DVTk-Modality-Emulator-5.0.0.msi*) to start the installation process.



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



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



<u>DVTk Modality Configuration</u>

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

RIS System

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

MPPS Manager

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

PACS/Workstation Systems–Storage Config

- **IP Address**: localhost

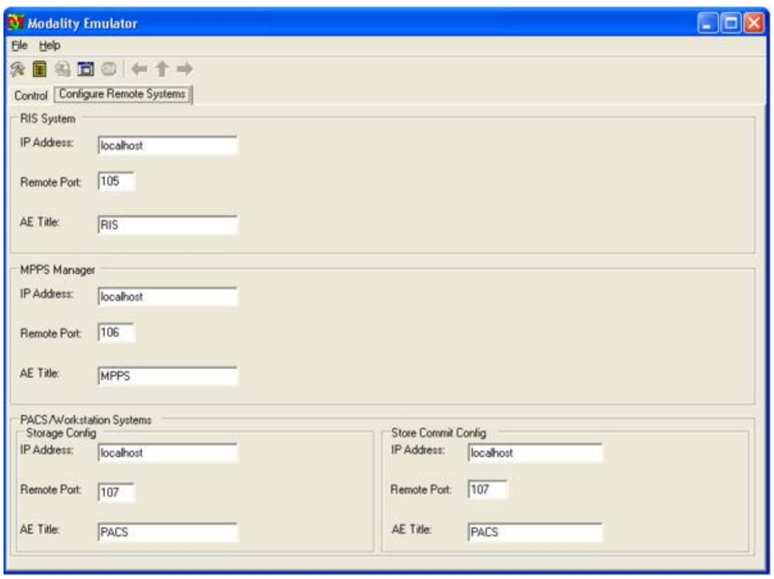
- **Remote Port**: 106
- **AE Title**: MPPS

PACS/Workstation Systems–Storage Commit Config

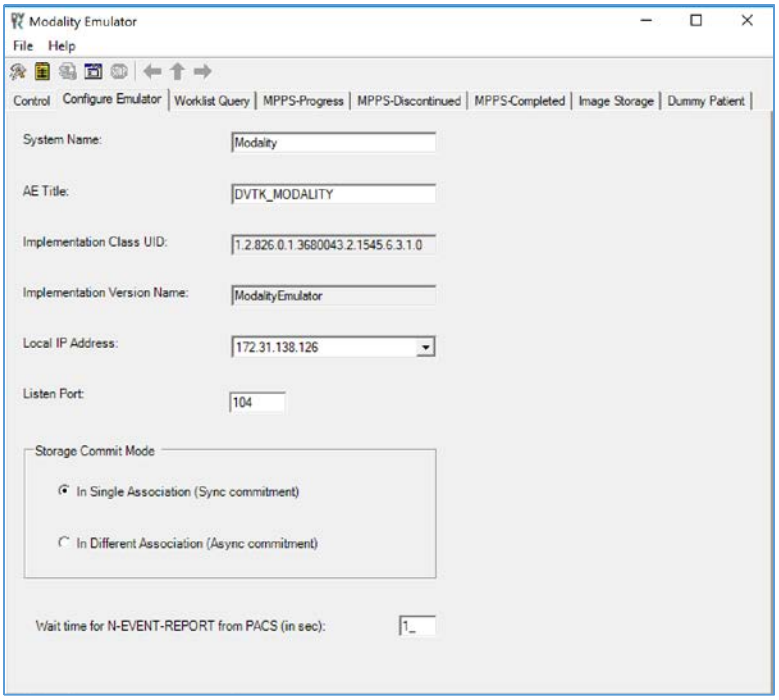
- **IP Address**: localhost
- **Remote Port**: 107
- **AE Title**: PACS

Store Commit Config

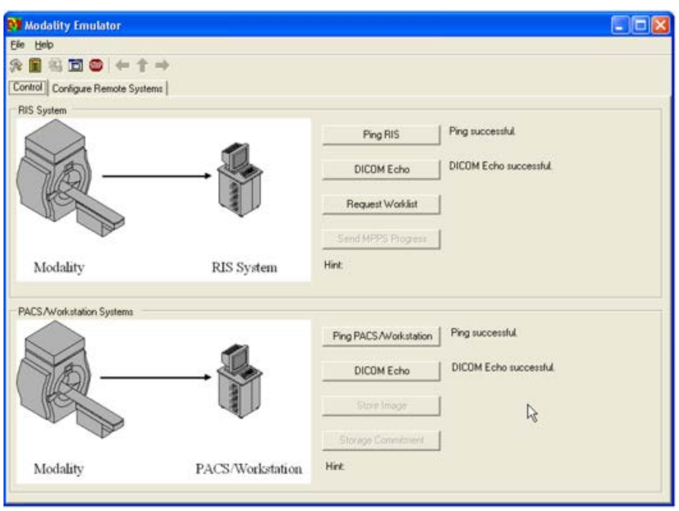
- **IP Address**: localhost
- **Remote Port**: 107
- **AE Title**: PACS



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



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



2.4.2 DVTk RIS Emulator

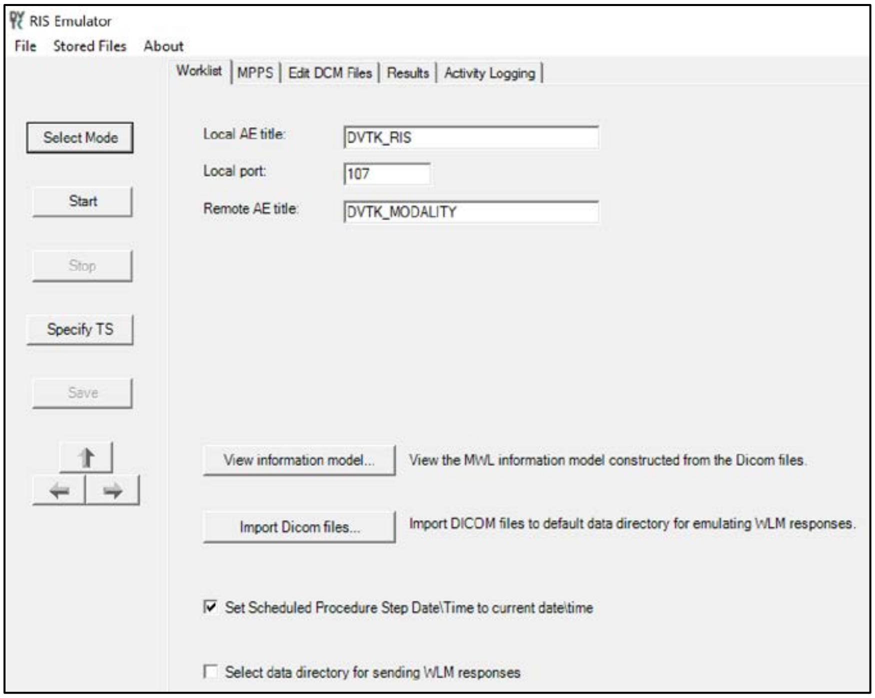
DVTk, the Health Validation Toolkit, is an open-source software. The DVTk RIS Emulator is an application that handles Modality Worklist and Modality Performance Procedure Step requests from remote applications and then responds with the emulated results using the DICOM files specified by the users.

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 instruction to continue the installation until the end of successful installation is displayed.
4. Close the installation window and start to **RIS Emulator**. The User Interface of the **RIS Emulator** tool that follows is shown with the tabs that follow for selecting the modes:
5. Worklist
    - MPPS
    - Edit DCM Files
    - Activity Logging
    - Validation results



<u>DVTk RIS Emulator Configuration</u>

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

2.5 Asset & Risk Management

2.5.1 Virta Labs BlueFlow

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

System Requirements

CPU: 2

Memory: 8 GB RAM

Storage: 100 GB (Thin Provision)

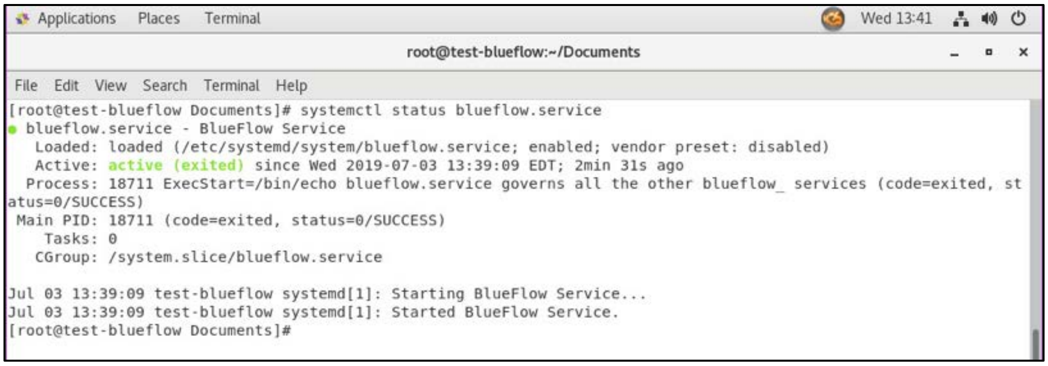
Operating System: CENTOS 7

Network Adapter: VLAN 1201

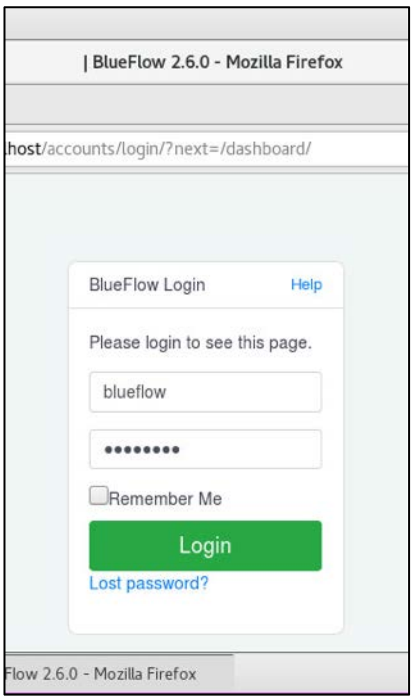
Virta Labs BlueFlow Installation

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

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

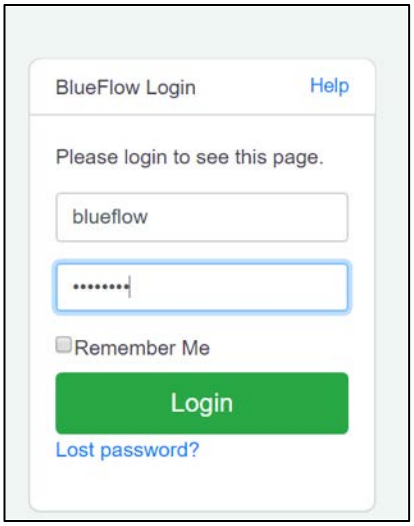


4. Visit ***https://localhost*** to verify BlueFlow web service is operating as expected, with a **BlueFlow Login page.**

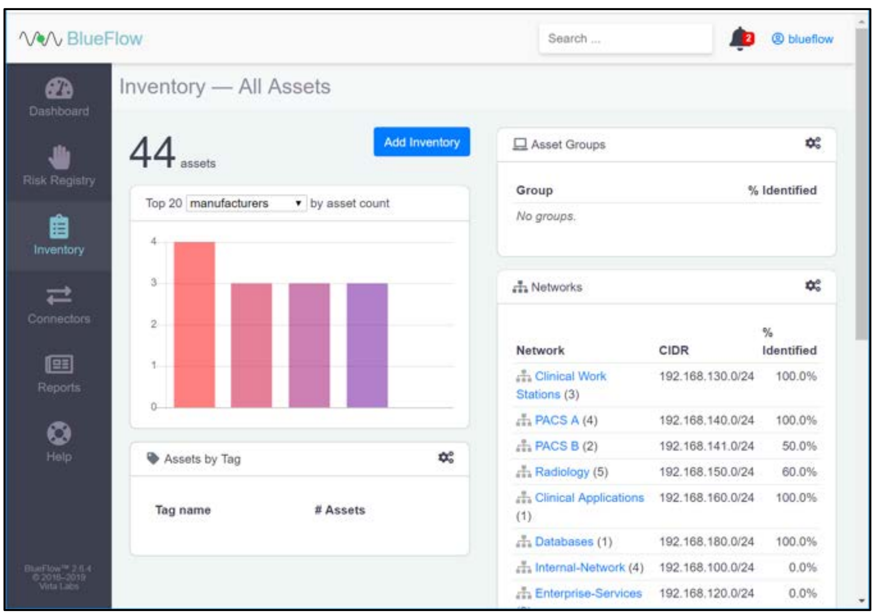


Virta Labs BlueFlow Network Groups Configuration

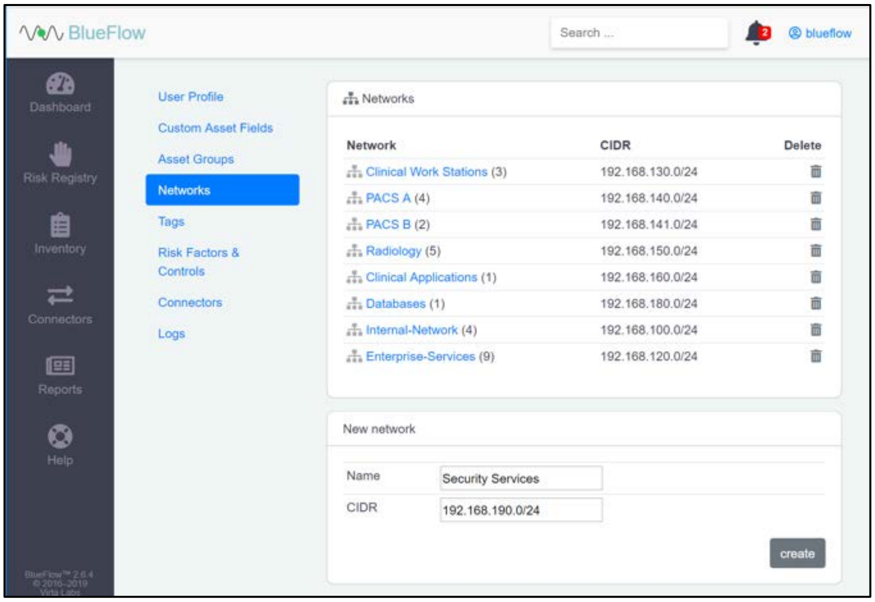
1. Log in to the **BlueFlow** web console.



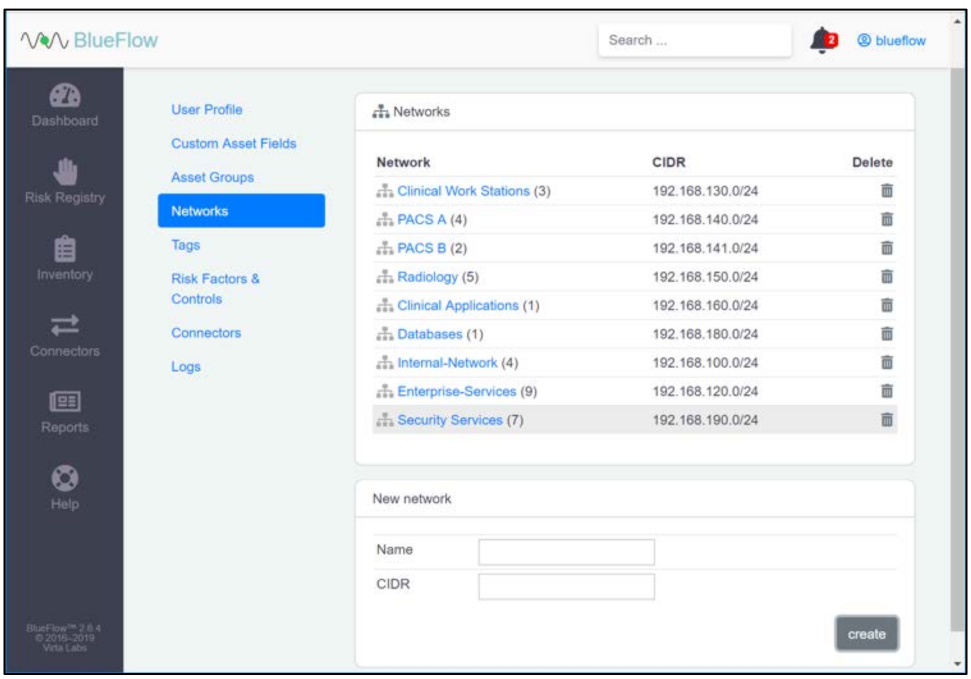
2. Navigate to the **Inventory** tab.
3. Under the **Networks** section, click on the **gear** icon.



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

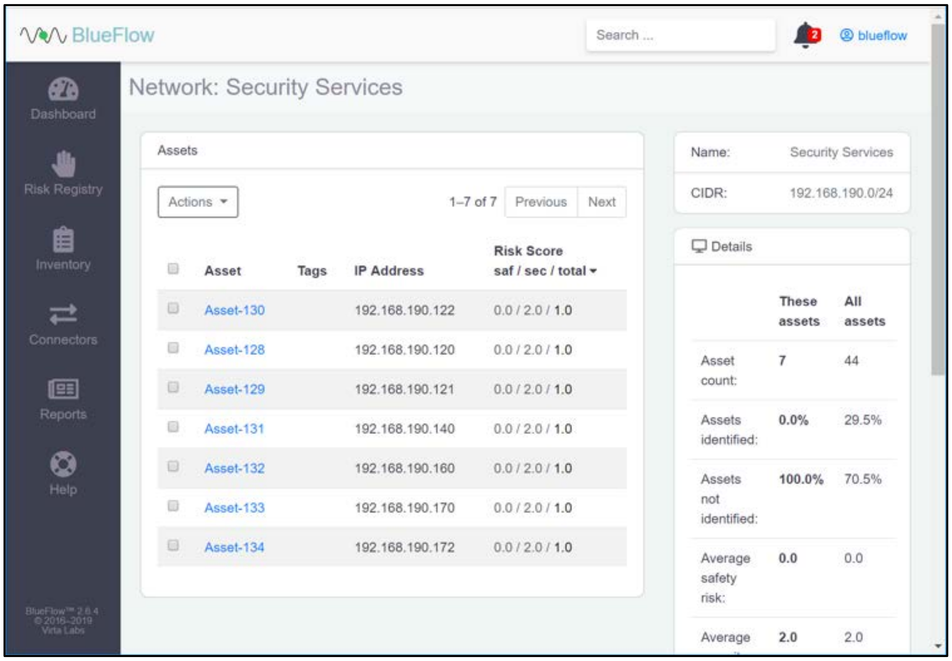


7. Verify that the new **network group (Security Services)** has been created.
8. Click on the **name** of the new network group.



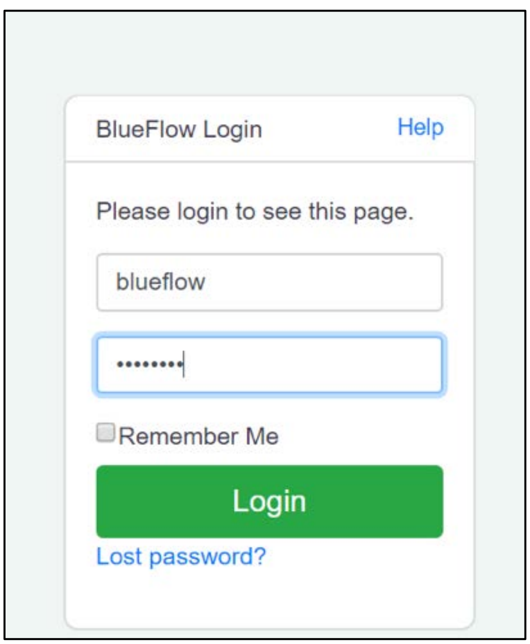
9. **Assets** will be listed on this page if they match the network group's criteria.

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).

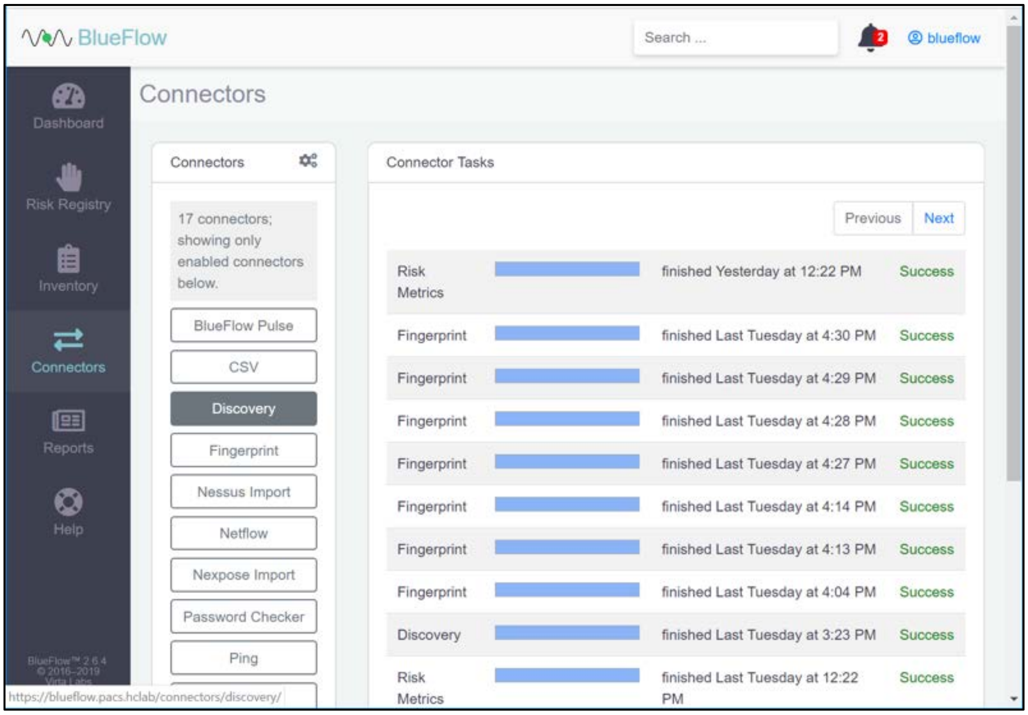


Running an IP Discovery Scan in Virta Labs BlueFlow

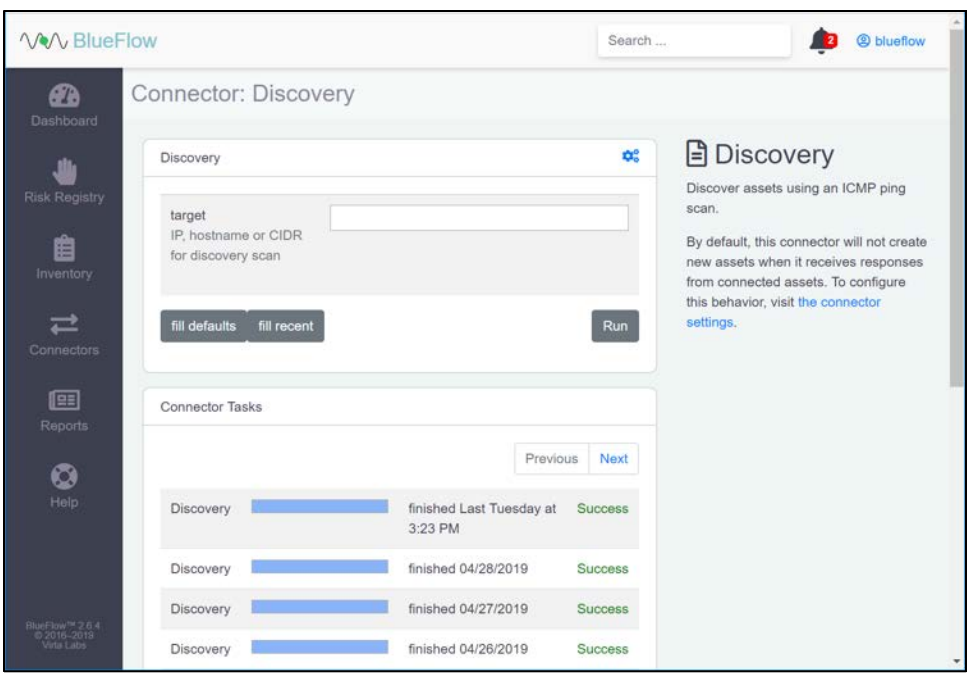
1. Log in to the **BlueFlow** web console.



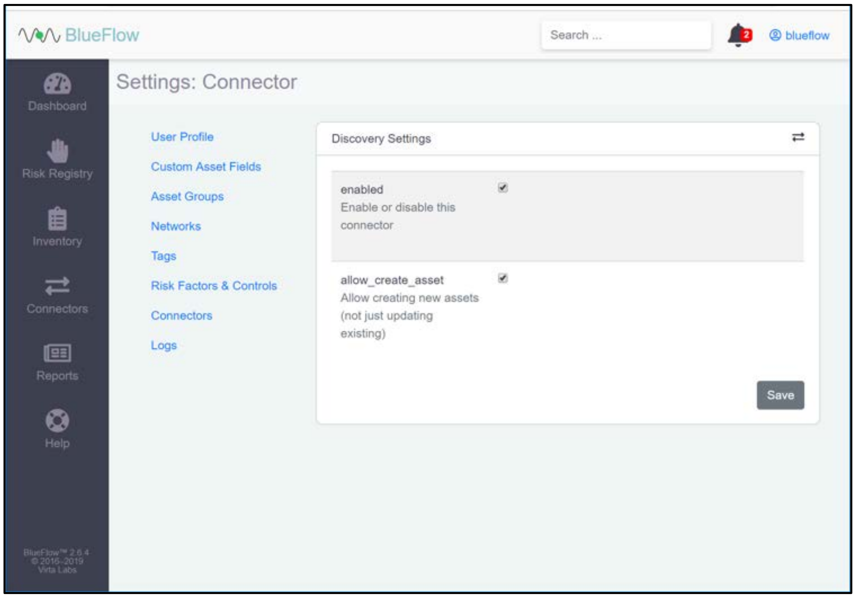
2. Navigate to **Connectors > Discovery**.



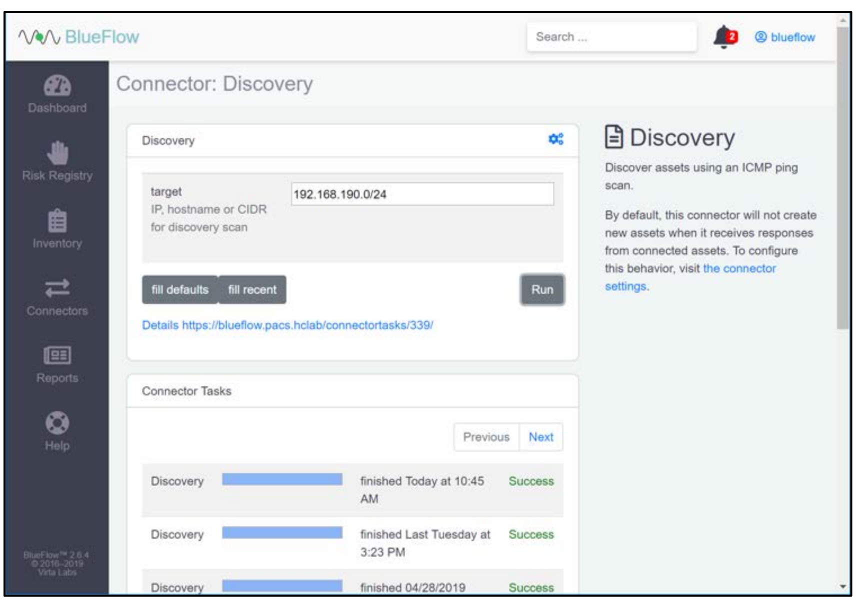
3. Under **Discovery**, click the **gear** icon.



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

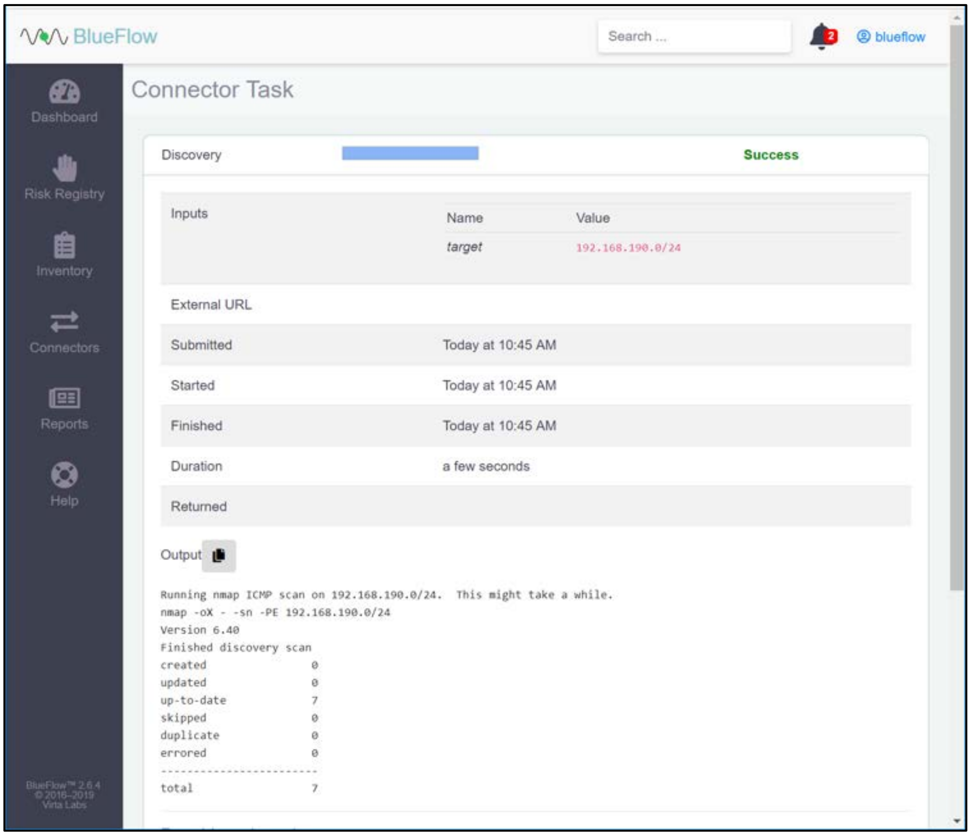


6. Enter an **IP** (e.g., ***192.168.190.0/24***), **host name** or **CIDR** that you would like to scan.
7. Click **Run.**
8. Wait for the discovery scan to finish.



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

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



2.5.2 Tripwire Enterprise

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

System Requirements

CPU: 1

Memory: 4 GB RAM

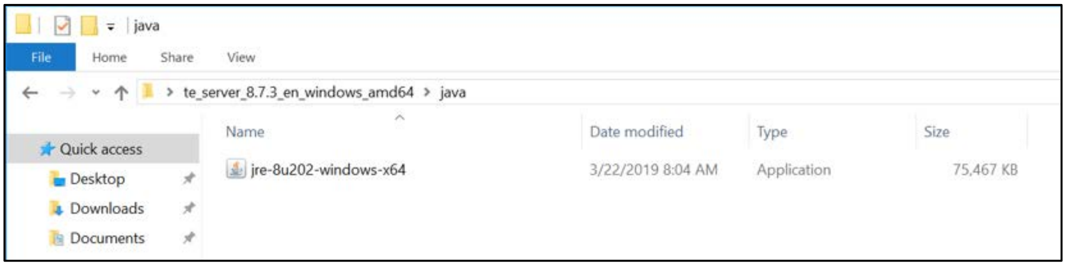
Storage: 120 GB (Thin Provision)

Operating System: Microsoft Windows Server 2016

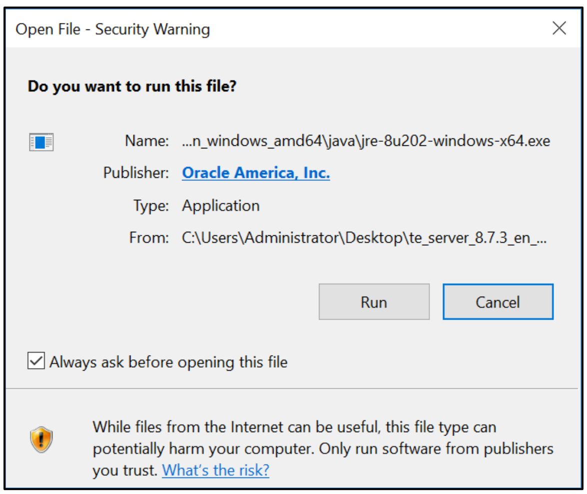
Network Adapter: VLAN 1201

Tripwire Enterprise Console Installation

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

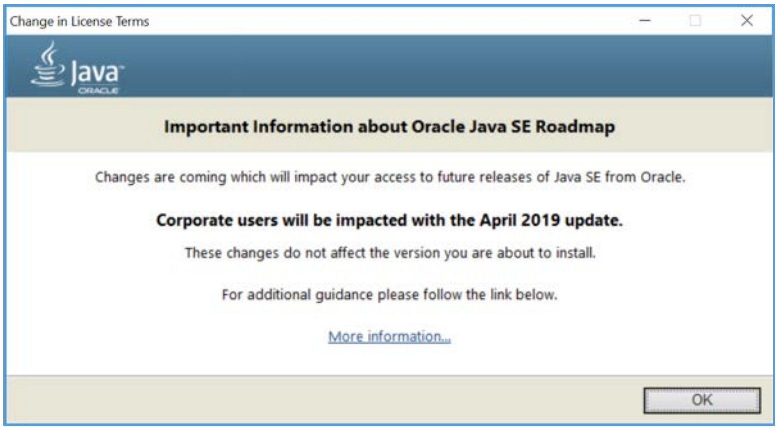


2. Click on **Run**.



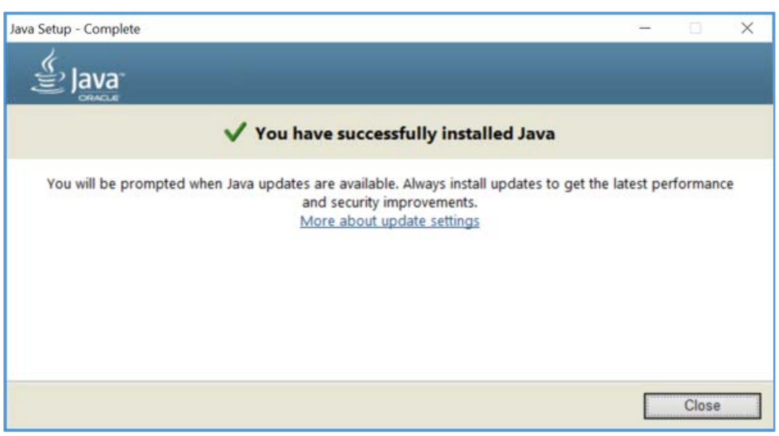
3. Click **on Install >**.

4. Click **OK**.

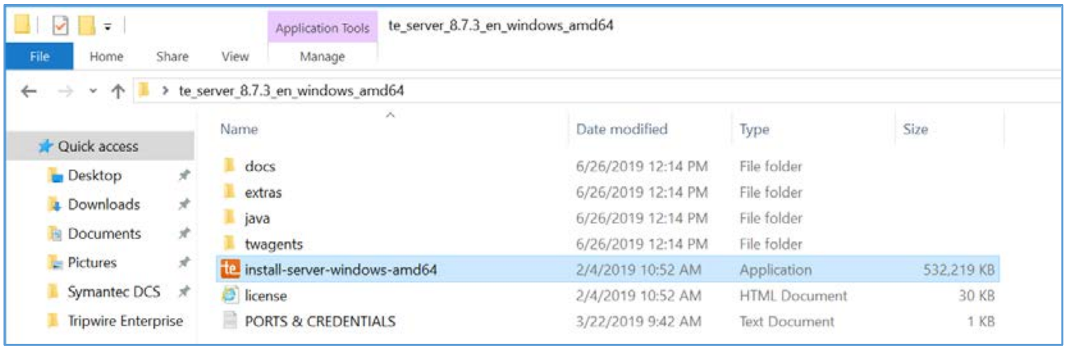


5. Wait for the install process to complete.

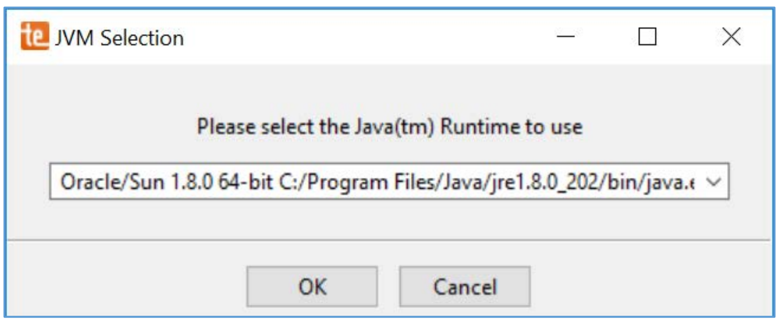
6. Click **Close**.



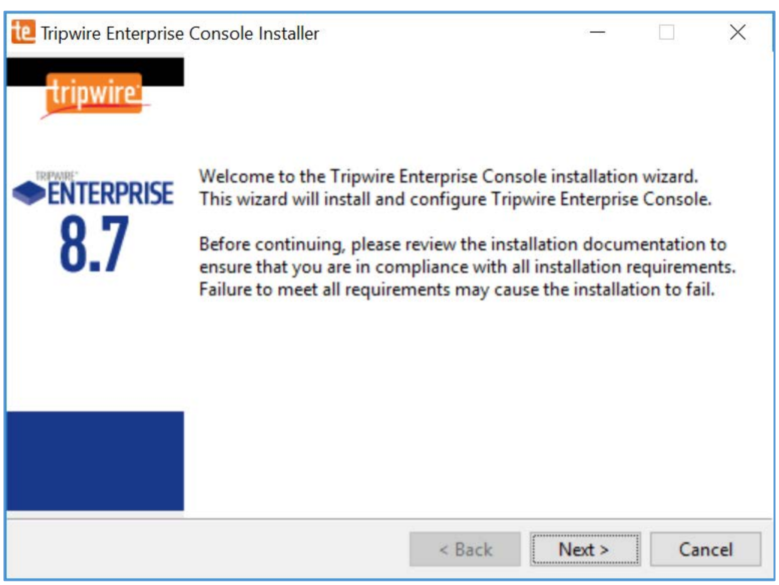
7. With Java installed, double-click on the Tripwire install application, *install-server-windows-amd64.*



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

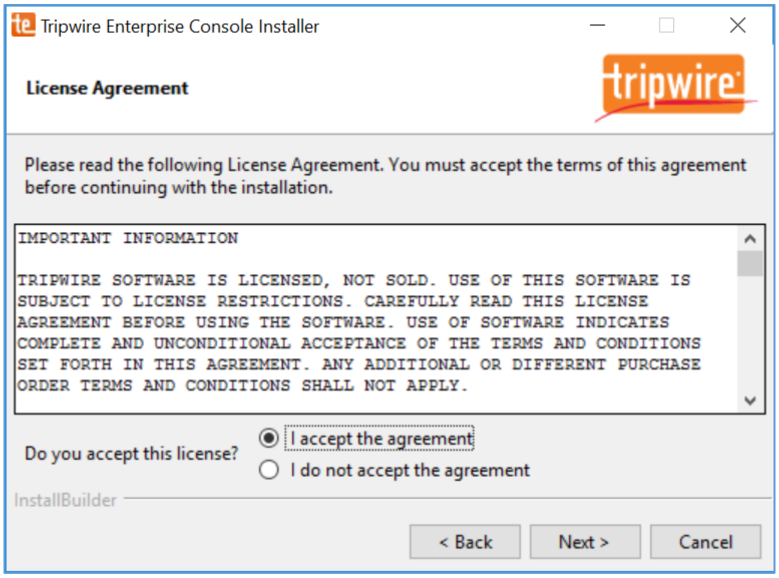


10. Click **Next >**.



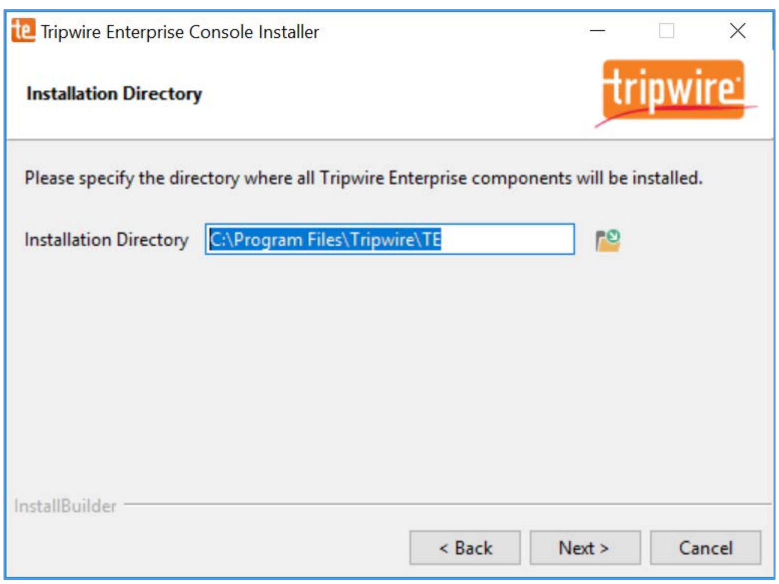
11. Check **I accept the agreement**.

12. Click **Next >**.



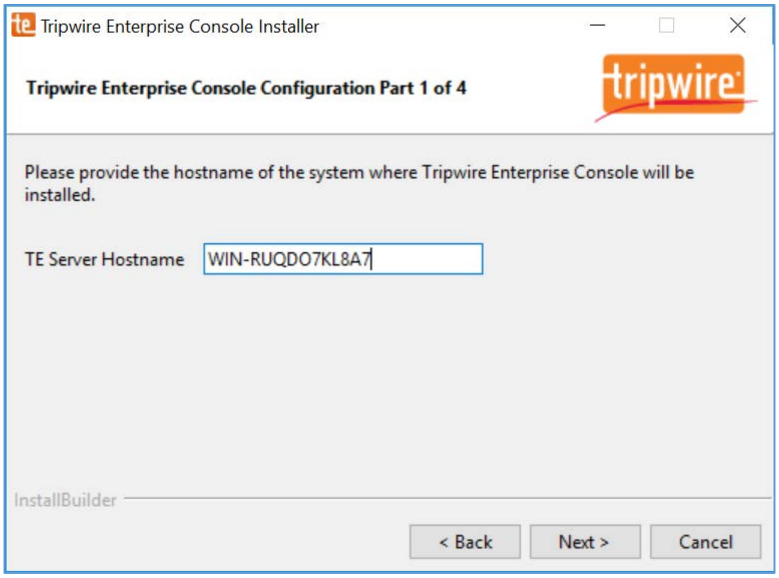
13. Specify an installation directory, *C:\Program Files\Tripwire\TE*, for the Tripwire installation.

14. Click **Next >**.



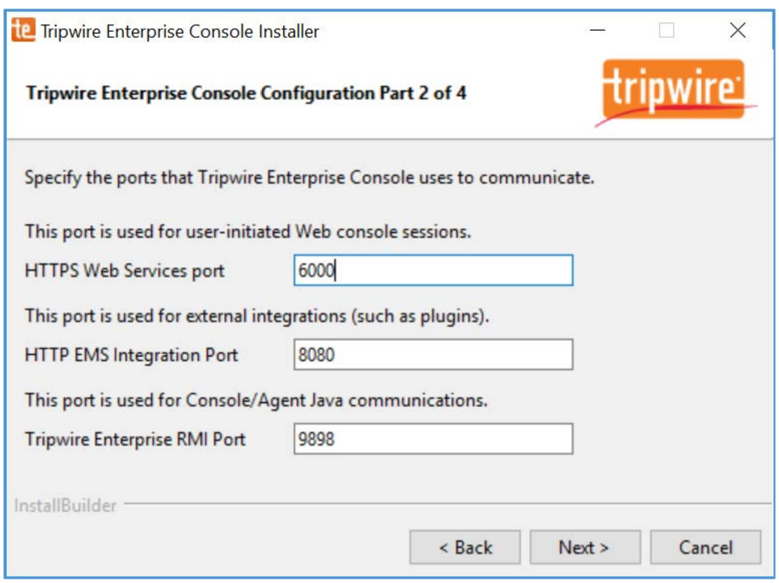
15. Verify the host name for the machine on which you're installing Tripwire (e.g., WIN-RUQDO7KL8A7).

16. Click **Next >.**



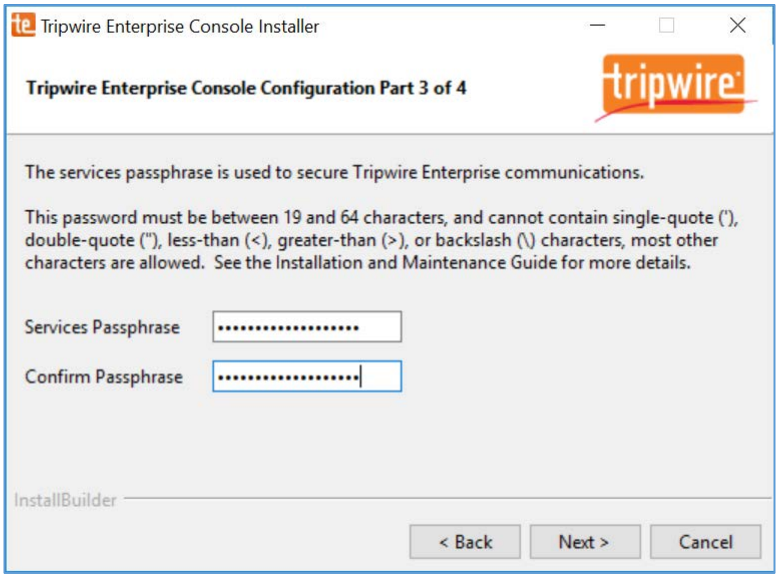
17. Specify the **HTTPS Web Services port** as **6000**, **HTTP EMS Integration Port** as **8080**, and **Tripwire Enterprise RMI Port** as **9898**.

18. Click **Next >**.

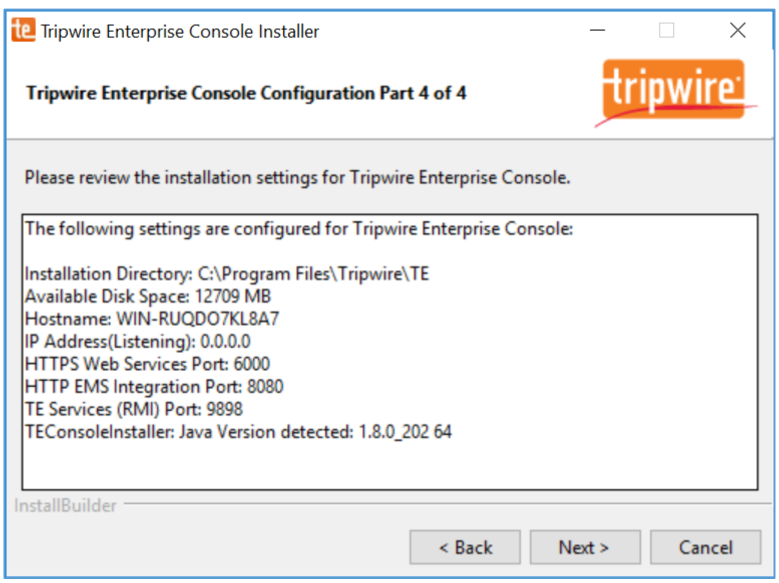


19. Create a password for Tripwire Enterprise services.

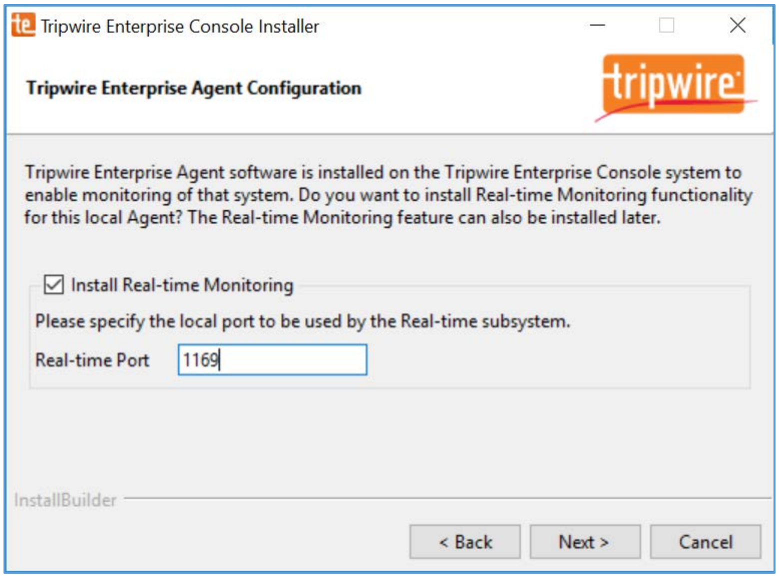
20. Click **Next >.**



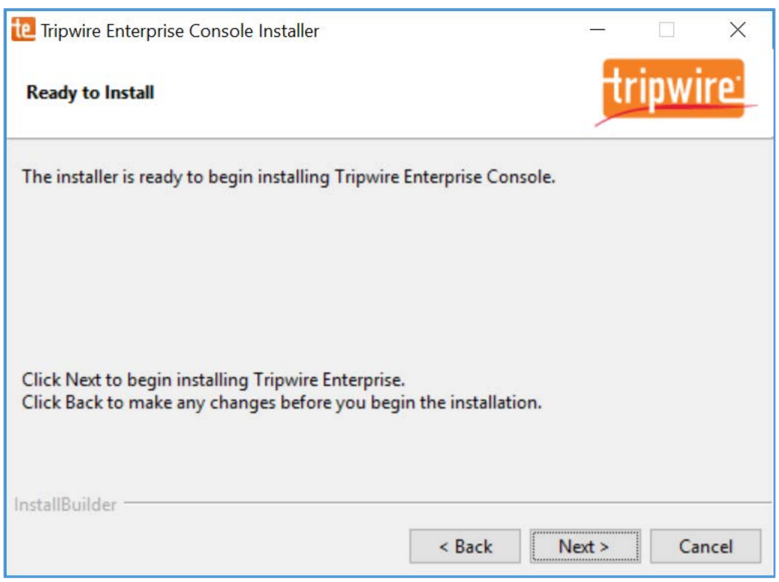
21. Verify planned installation settings are correct.
22. Click **Next >**.



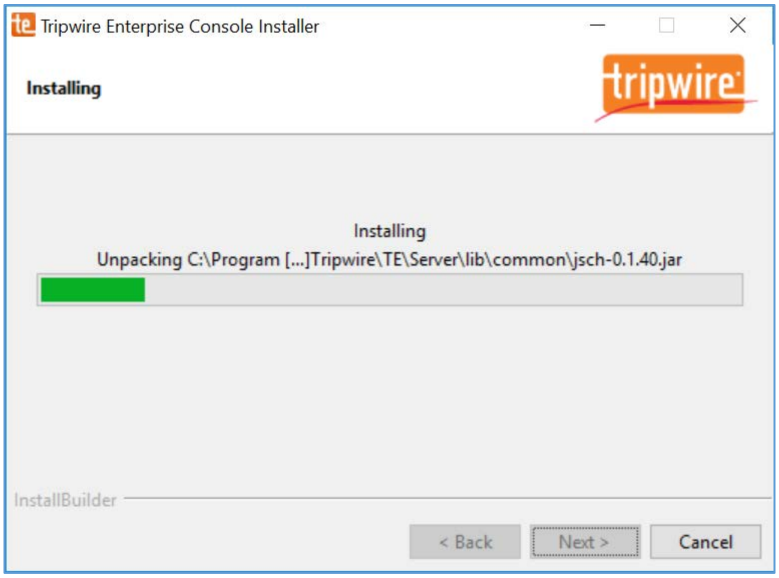
23. Check **Install Real-time Monitoring**.
24. Specify **Real-time Port** as **1169** for monitoring.
25. Click **Next >.**



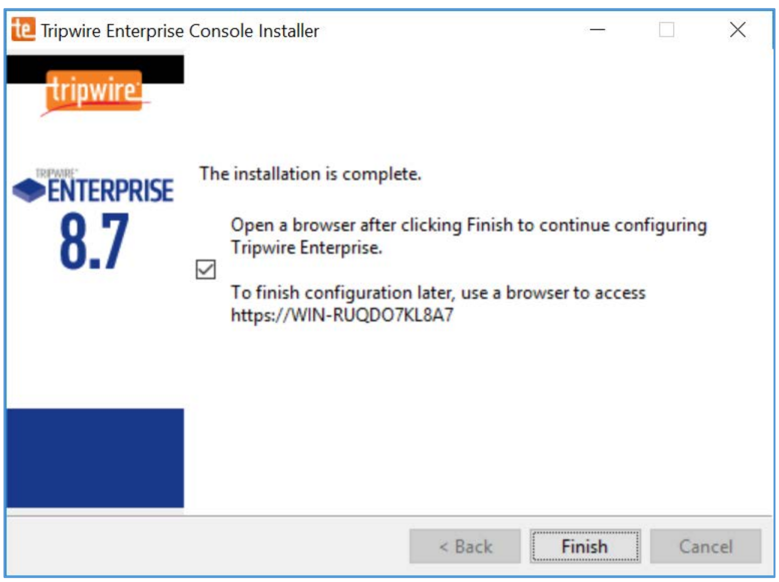
26. Click **Next >**.



27. Wait for Tripwire Enterprise installation to complete.

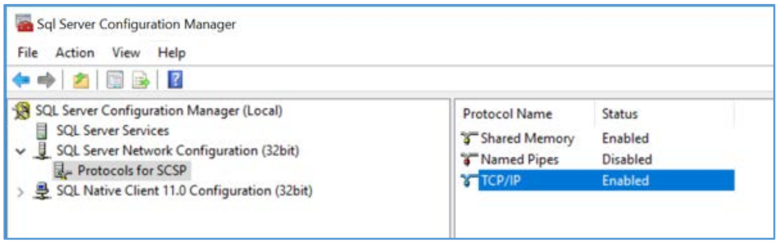


28. Click **Finish**.

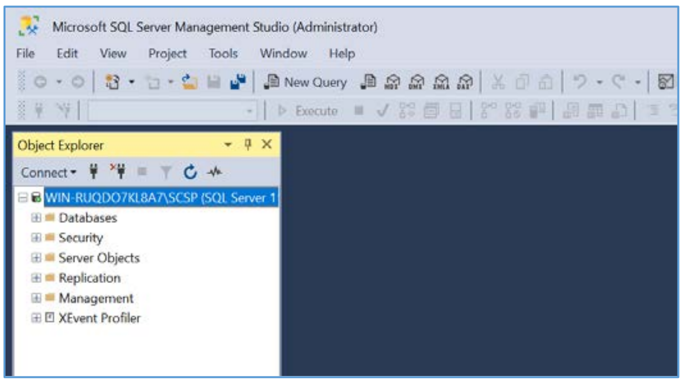


29. Open SQL Server Configuration Manger.

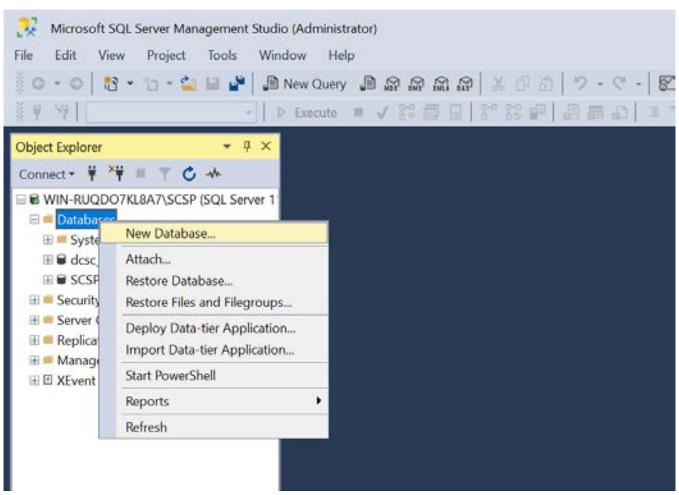
30. Under **SQL Server Network Configuration > Protocols for SQL Server** ensure the **TCP/IP protocol** is set to **Enabled.**



31. Open SQL Server Management Studio.



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

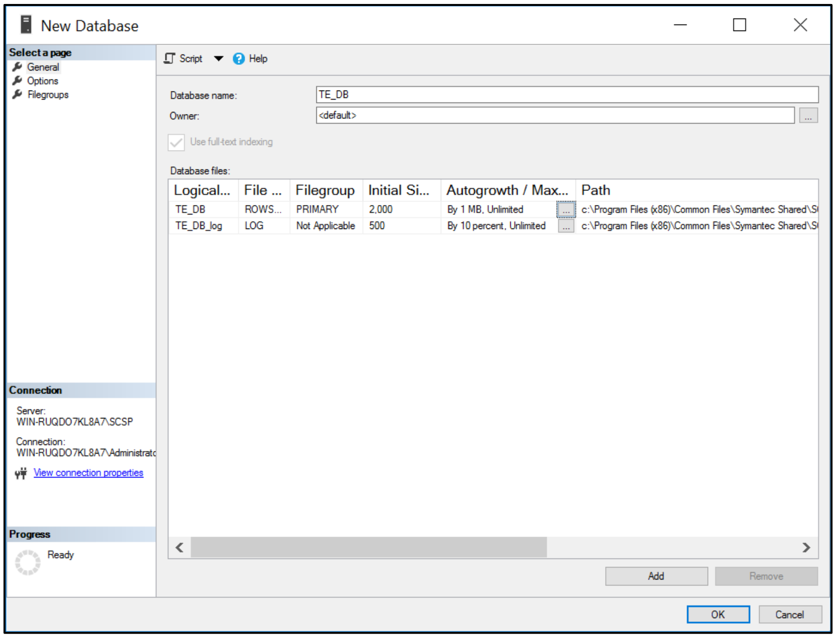


33. On the left, **under Select a page**, select **General**.

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

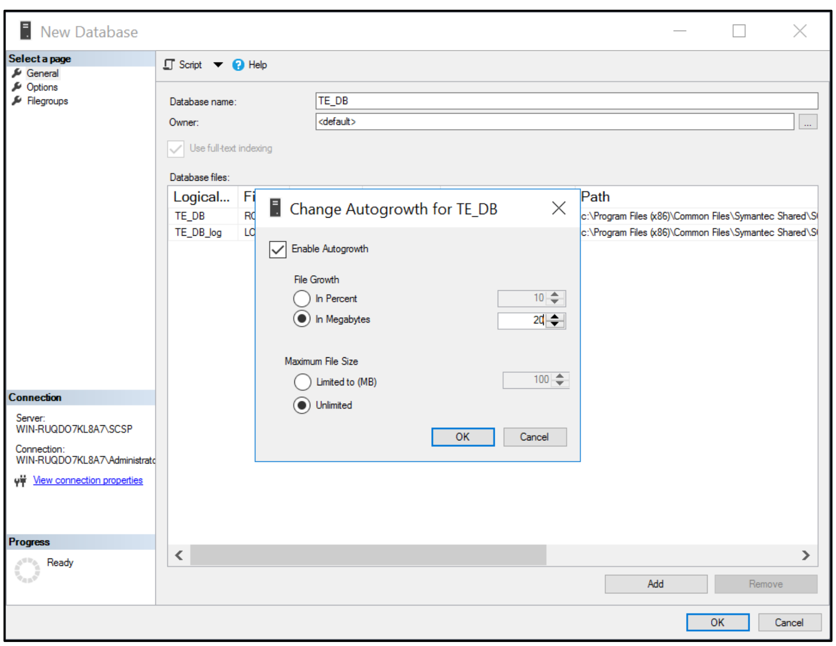
35. Under **Database files**, for the data file, set **Initial Size** to at least **2,000**.

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

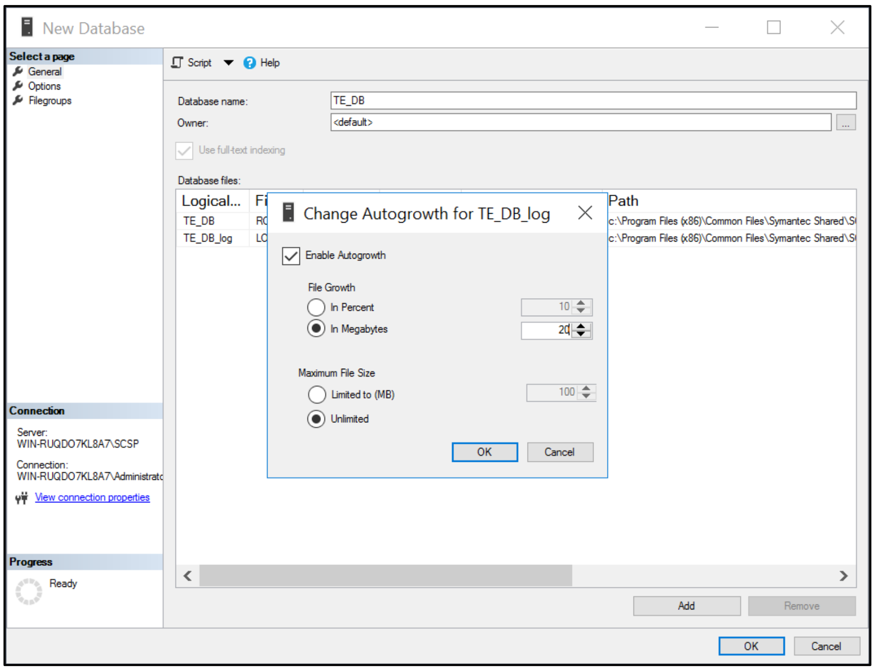


37. Check **Enable Autogrowth**, set **File Growth** to at least **20 MB**, and set **Maximum File Size** to **Unlimited.**

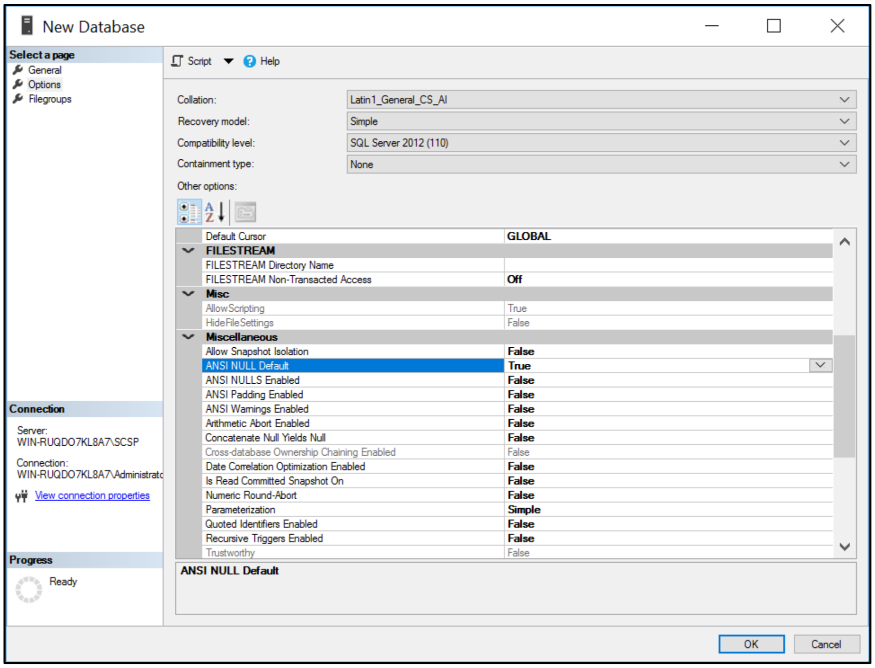
38. Click **OK**.



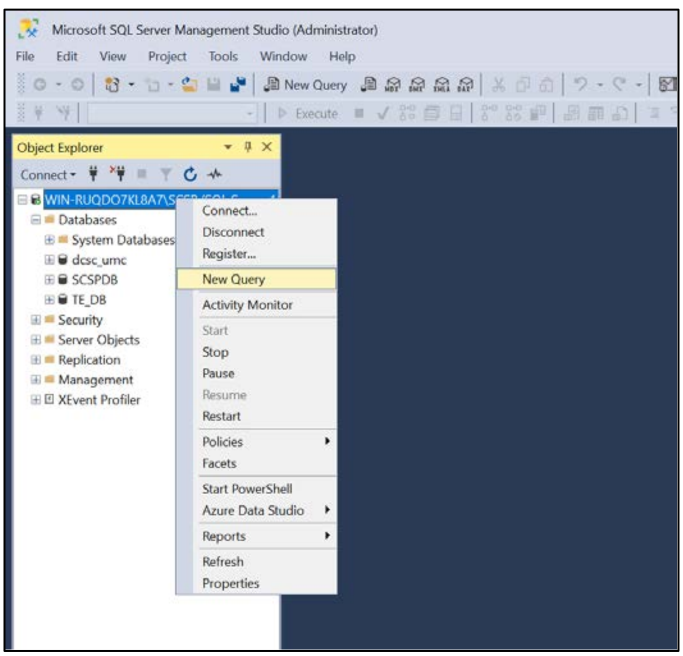
39. Under **Database files**, for the log file, set **Initial Size** to at least **500**.
40. Click the **button** under Autogrowth.
41. Check **Enable Autogrowth**, set **File Growth** to at least **20 MB**, and set **Maximum File Size** to **Unlimited.**
42. Click **OK**.



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



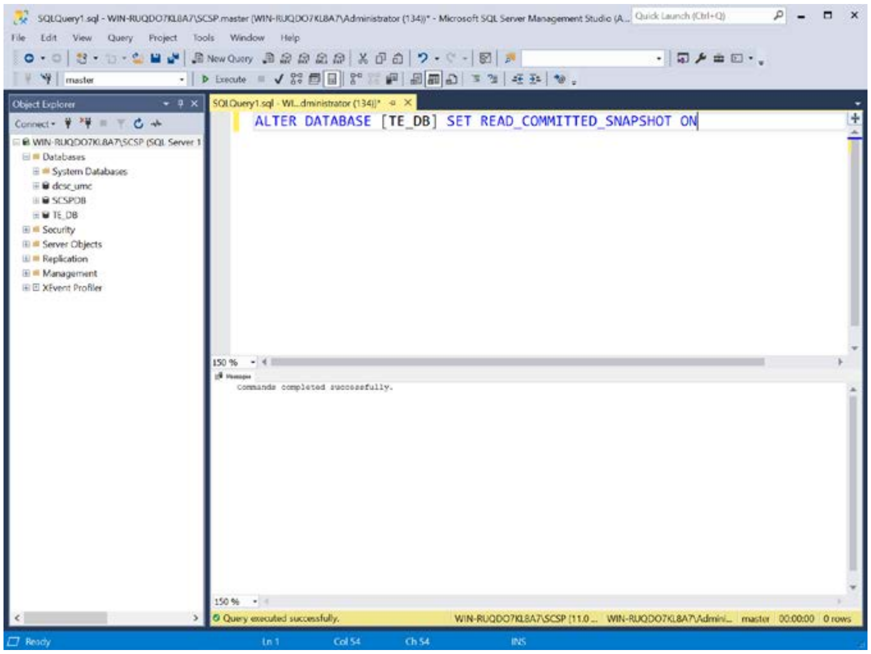
48. In the **Object Explorer**, right click on your database and select **New Query**.



49. Type out the following query:

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

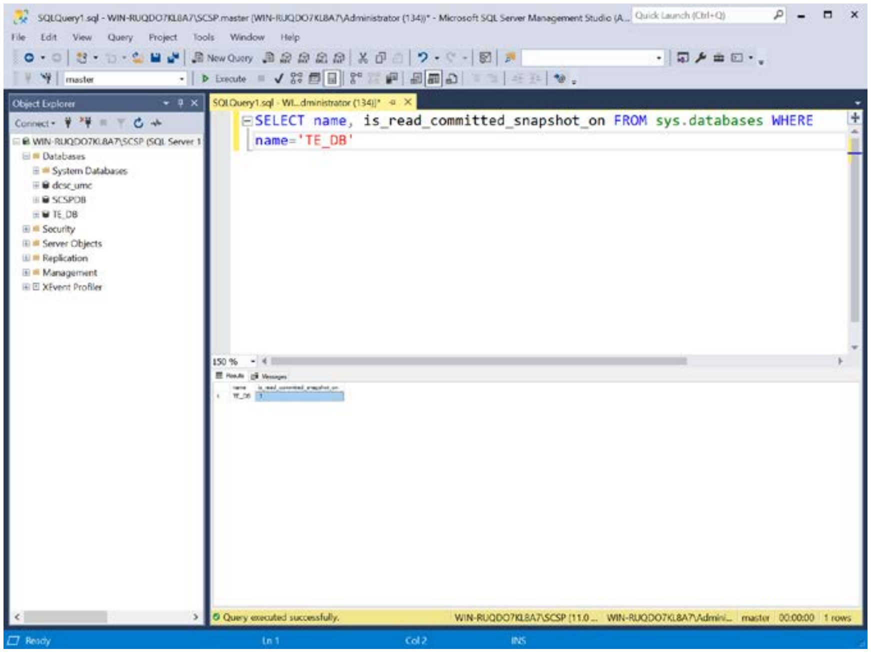
50. Click **Execute** in the toolbar above the **SQL Query** window.
51. Under the **SQL Query** window, in the **Messages** window, verify the command was completed successfully.



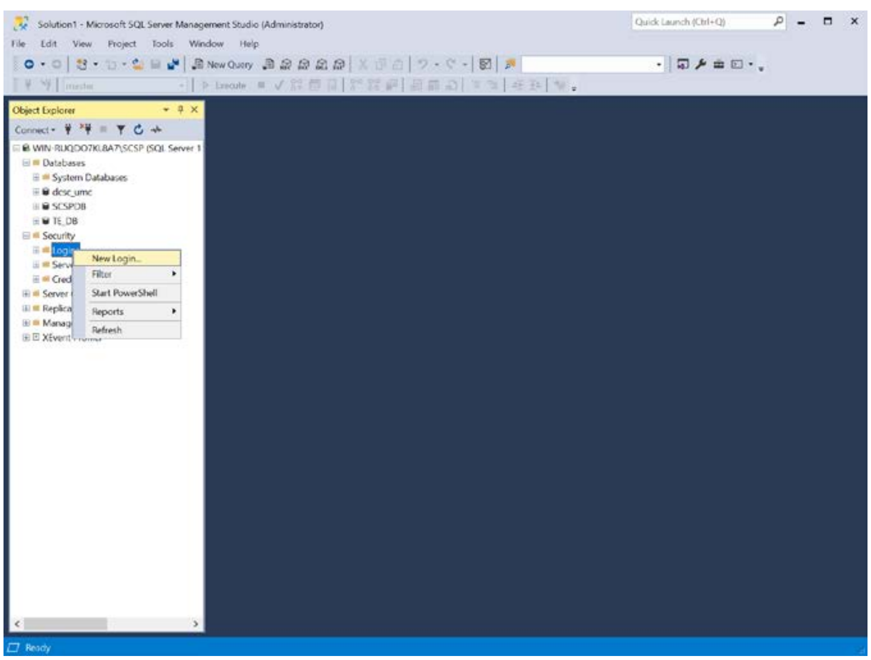
52. Clear the **SQL Query** window, and then type out the following query.

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

53. Click **Execute** in the toolbar above the **SQL Query** window.
54. Under the **SQL Query** window, in the **Messages** window, verify the **value for is_read_committed_snapshot_on** is set to **1**.



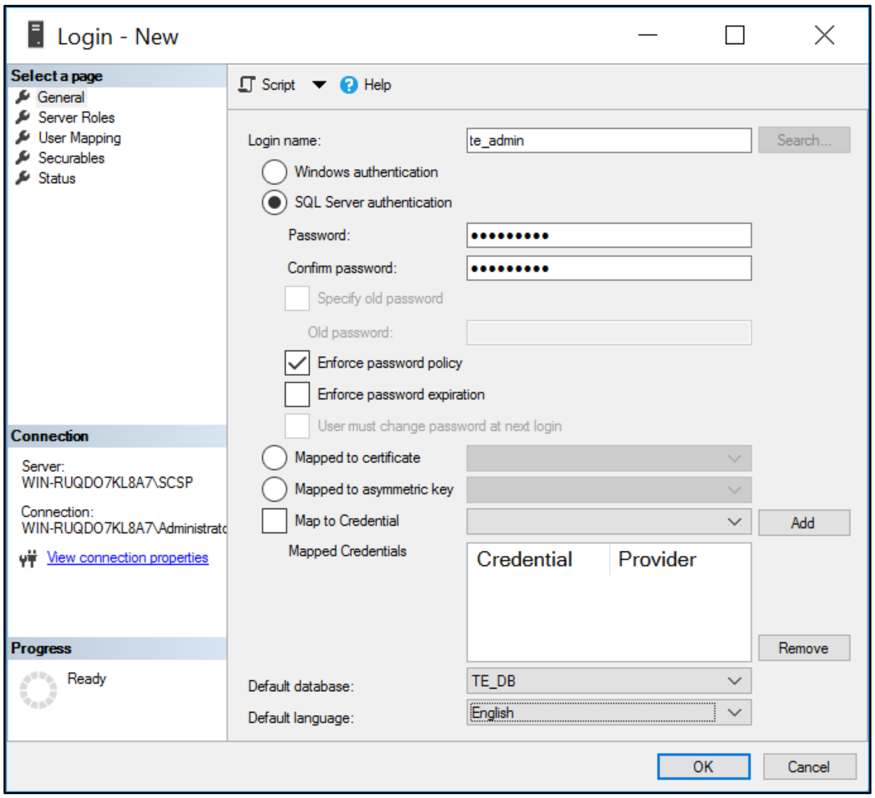
55. In the **Object Explorer**, expand the selection for your database, expand the **Security** section, right click on **Logins**, and select **New Login…**



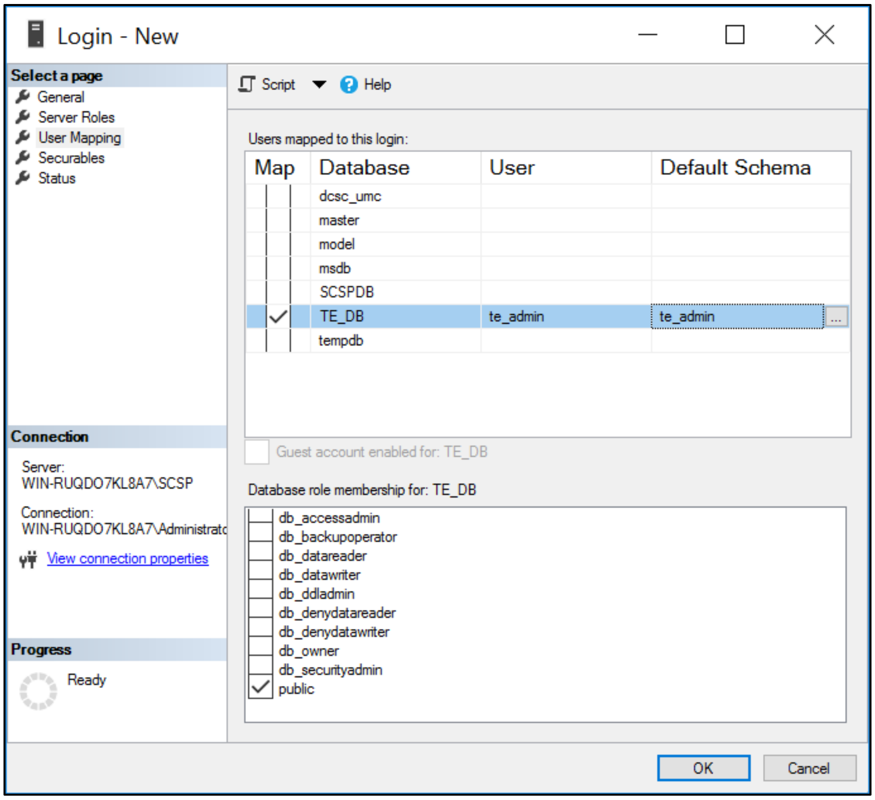
56. On the left, under **Select a page**, select **General**.

57. Create a **Login name**.

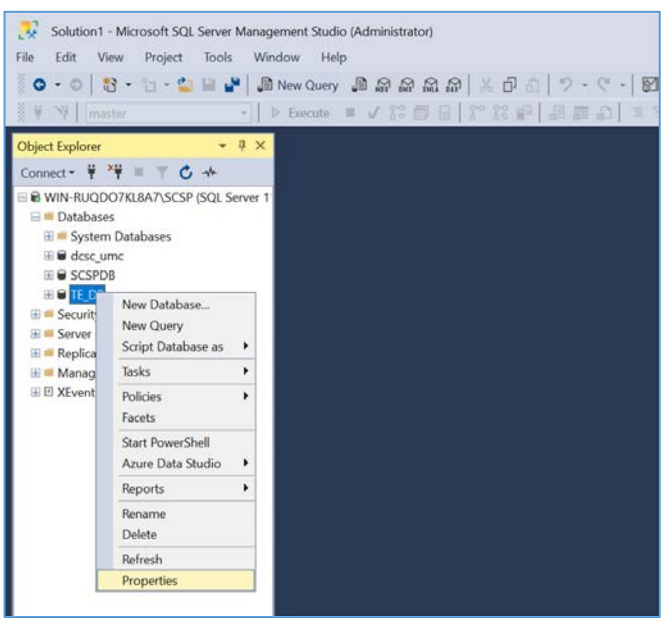
58. Select **SQL Server authentication**.
59. Create a **password**.
60. For **Default database**, select the database previously created.
61. For **Default language**, select **English**.



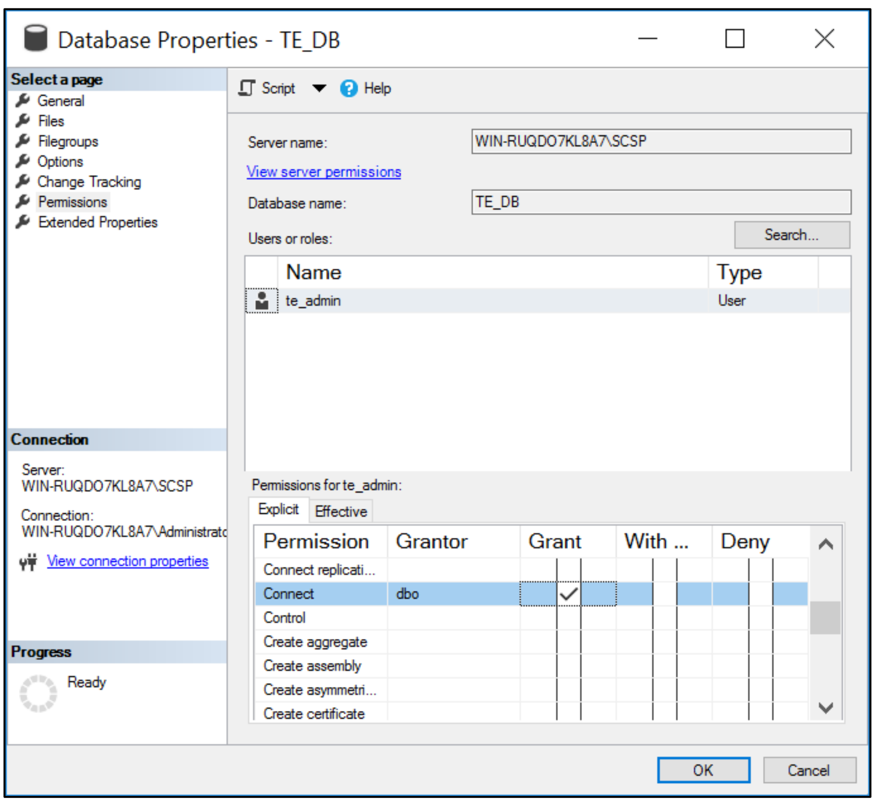
62. On the left, under **Select a page**, select **User Mapping**.
63. Under the **Users mapped to this login** window, perform these actions for the row containing the previously created database:
    a. Check the box in the **Map** column.
    b. In the **Default Schema** column, type the name of the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



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



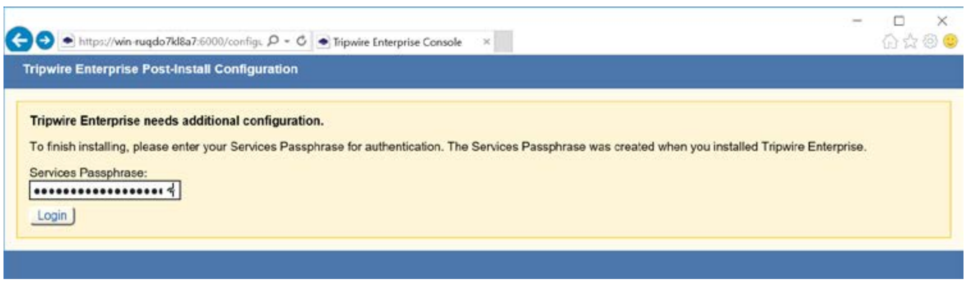
66. On the left, under **select a page**, select **Permissions**.
67. Under **Permissions for user**, check the box in the **Grant** column for the following permissions:
    - **Connect**
    - **Create Function**
    - **Create Procedure**
    - **Create Table**
    - **Create View**
    - **Delete**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



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

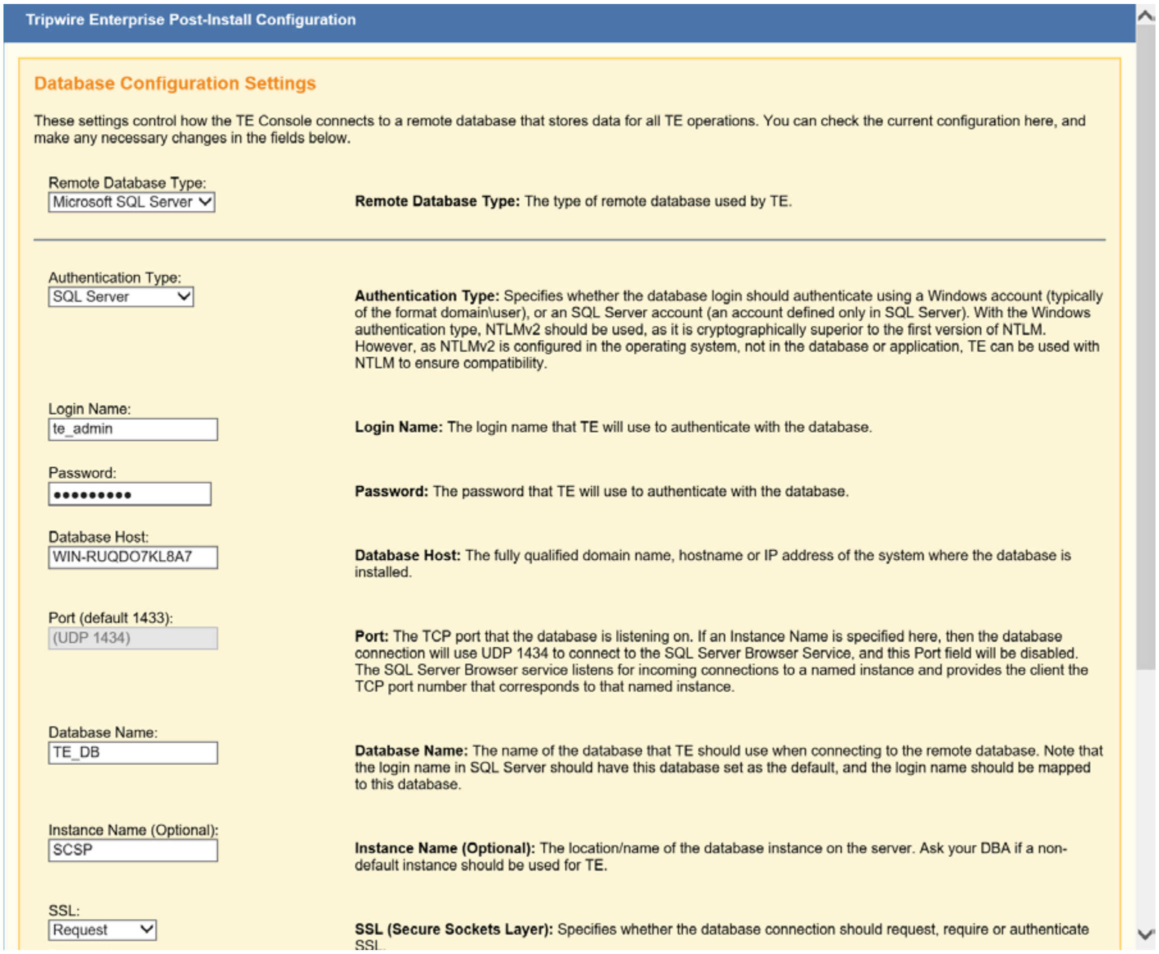
70. Enter the **services password** created during the install process.

71. Click **Login**.

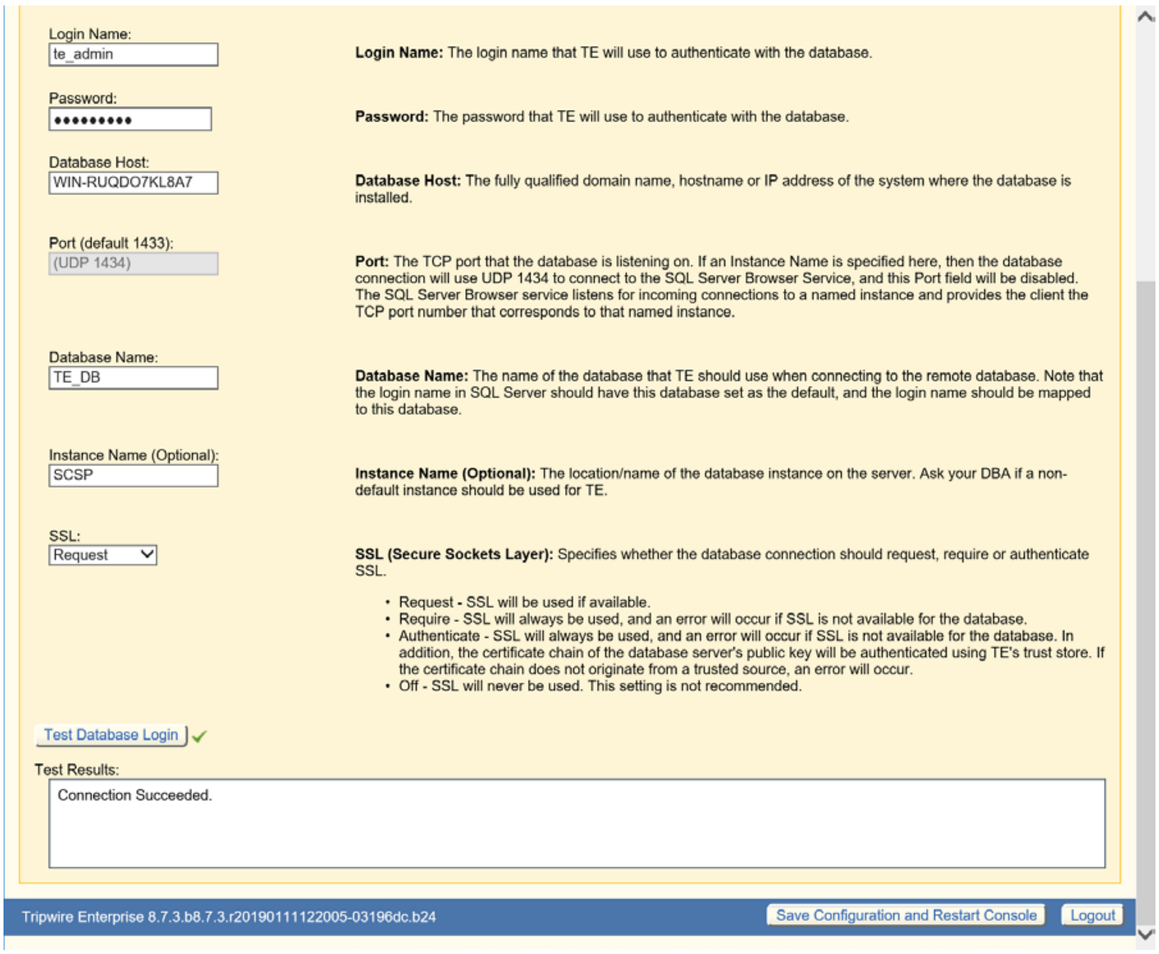


72. Under **Database Configuration Settings**, provide the information that follows:

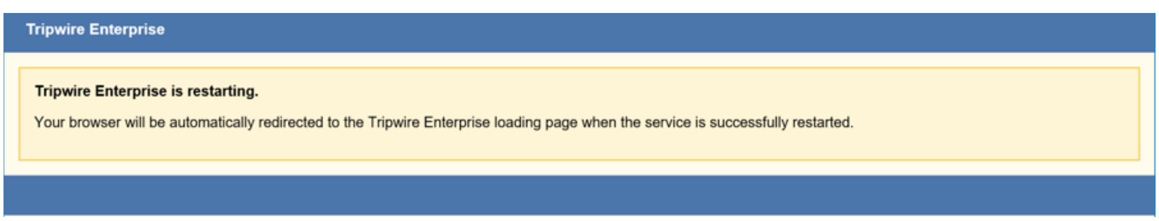
- **Remote Database Type**: Microsoft SQL Server
- **Authentication Type**: SQL Server
- **Login Name**: te_admin
- **Password**: *********
- **Database Host**: WIN-RUQDO7KL8A7
- **Database Name**: TE_DB
- **Instance Name**: SCSP (Note: this may not be necessary, depending on how your SQL Server Database is configured)
- **SSL**: Request



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

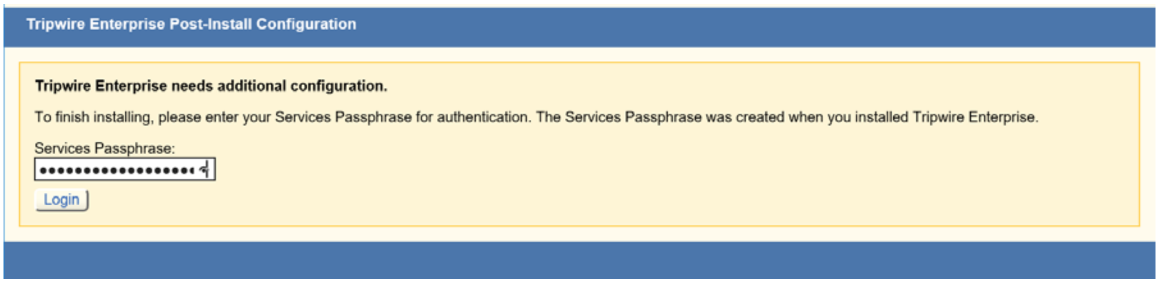


75. Wait for Tripwire Enterprise to restart and redirect you to the log in page.



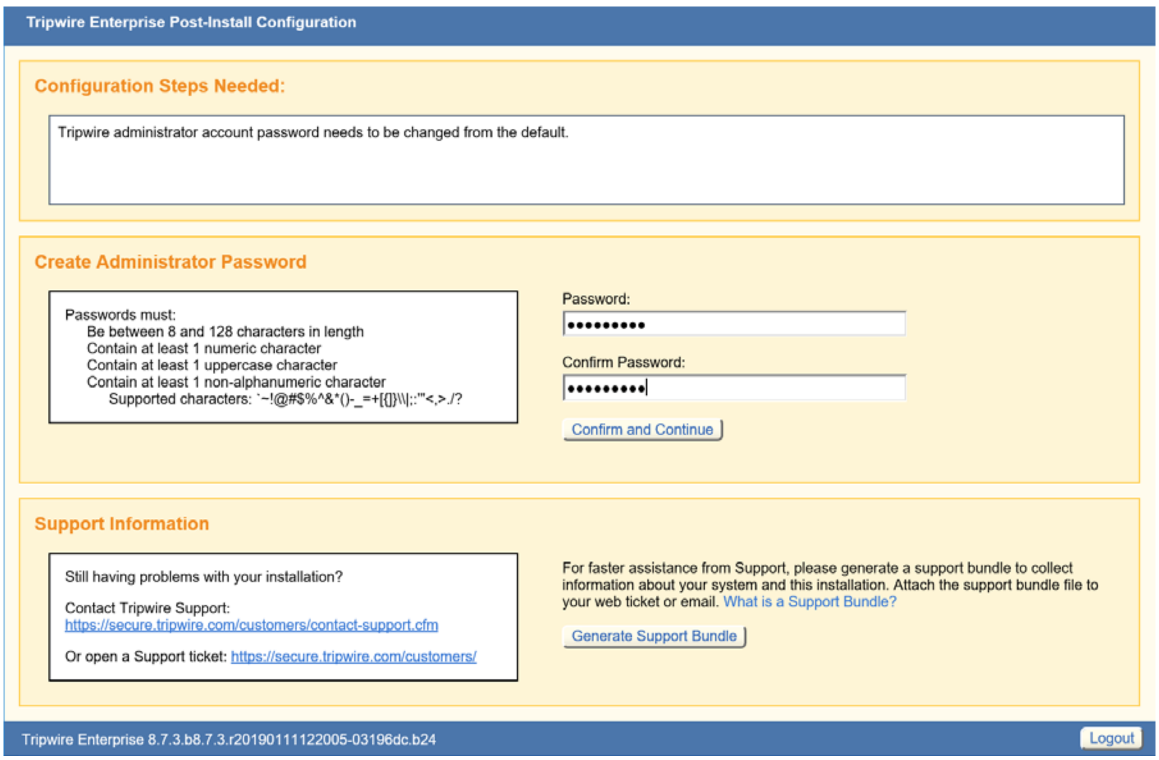
76. Enter the **services password** created during the install process.

77. Click **Login**.



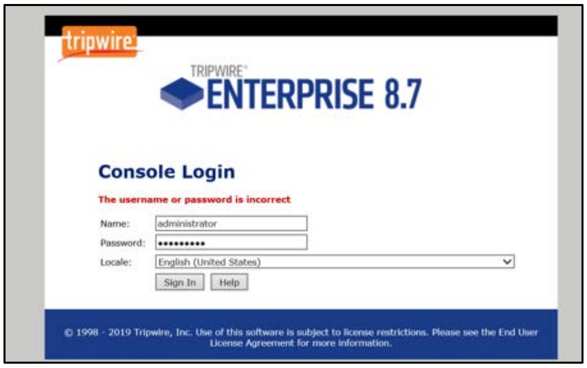
78. Under **Create Administrator Password**, create a password for the Tripwire Enterprise administrator account.

79. Click **Confirm and Continue**.



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

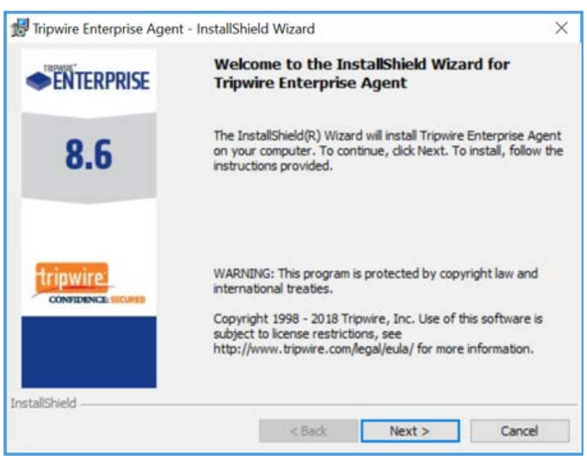
81. Click **Sign In**.



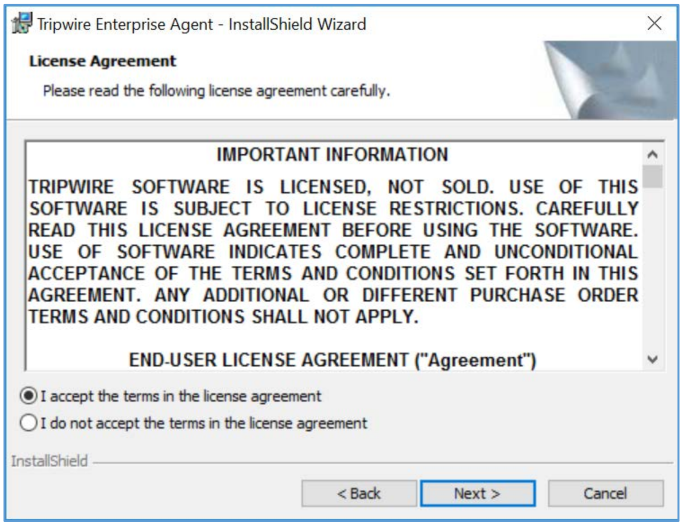
82. Click **Configure Tripwire Enterprise** to begin the configuration process.

Tripwire Enterprise Agent Installation

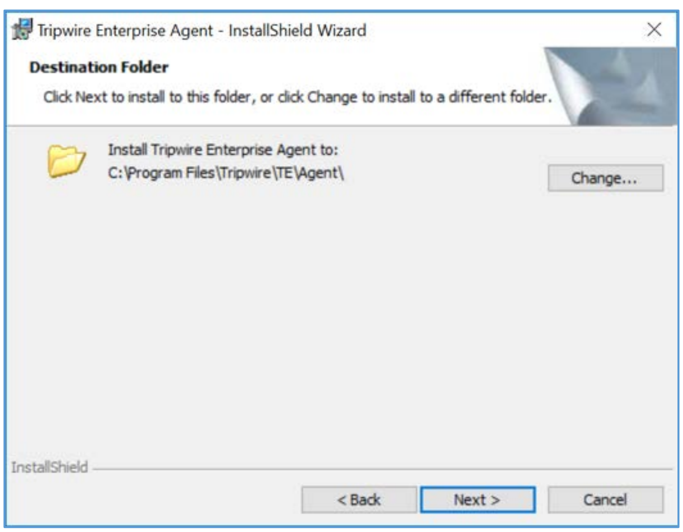
1. **Run** te_agent.msi.
2. Click **Next >**.



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

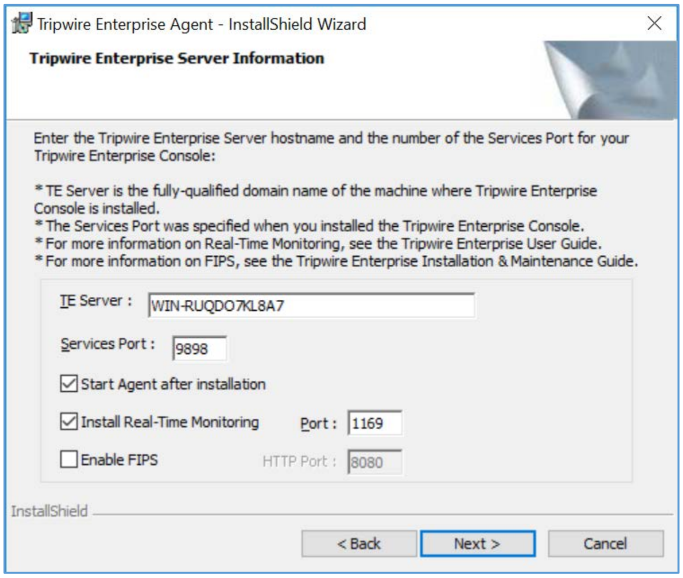


5. Specify an install directory for the Tripwire Enterprise Agent.
6. Click **Next >**.

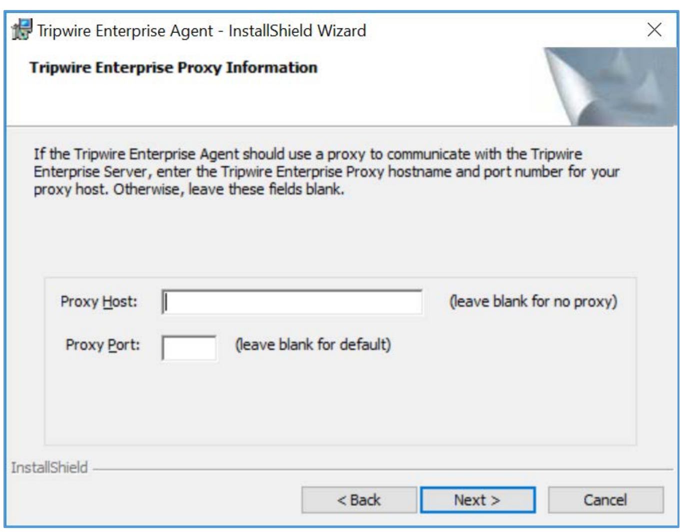


7. Enter the **TE Server** (e.g., **WIN-RUQDO7KL8A7**) of the server where Tripwire Enterprise is installed.
8. Enter **9898** as the **Services Port** established during the installation process of Tripwire Enterprise.
9. Check **Start Agent**, after installation.

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

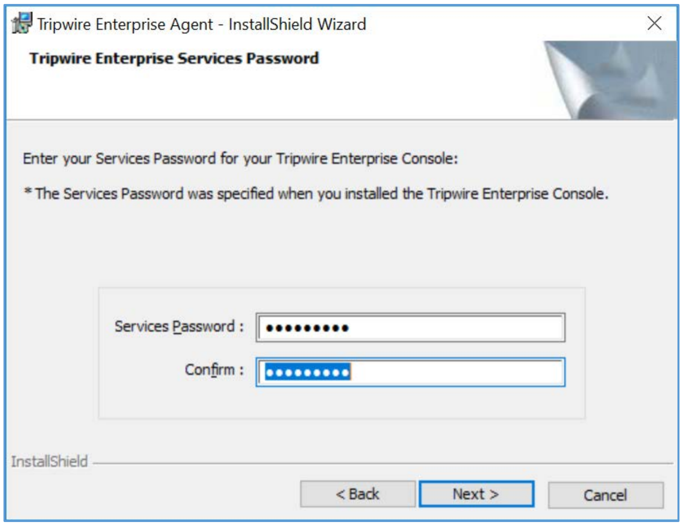


13. Specify a **Proxy Host** and **Proxy Port** if necessary.
14. Click **Next >**.

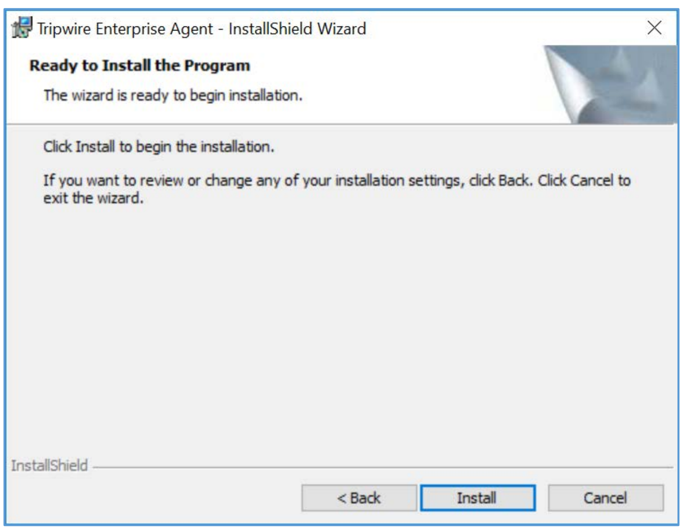


15. Enter the **Services Password** created during the installation process for Tripwire Enterprise.

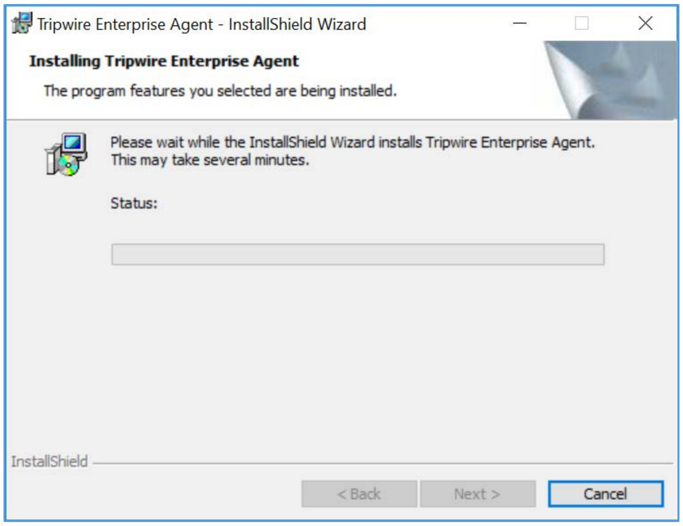
16. Click **Next >**.



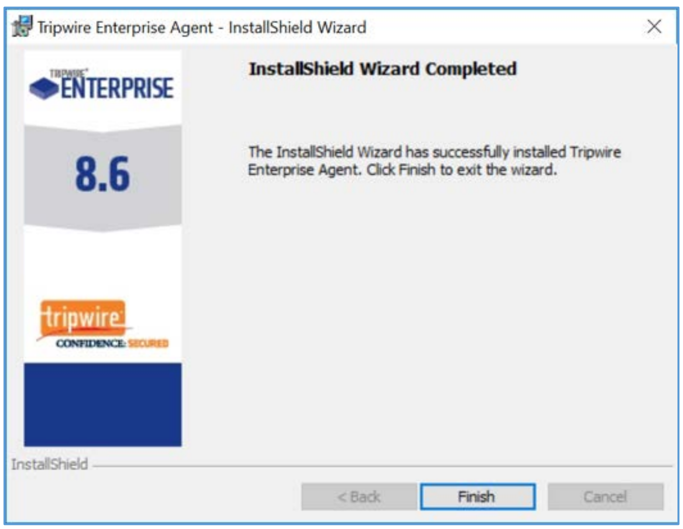
17. Click **Install**.



18. Wait for the installation process to complete.



19. Click **Finish**.



2.6 Enterprise Domain Identity Management

2.6.1 Domain Controller with AD, DNS, & DHCP

Within the PACS architecture, we established a Windows Server 2012 R2 Domain Controller to manage AD, DNS, and Dynamic Host Configuration Protocol (DHCP) services for the enterprise. The 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

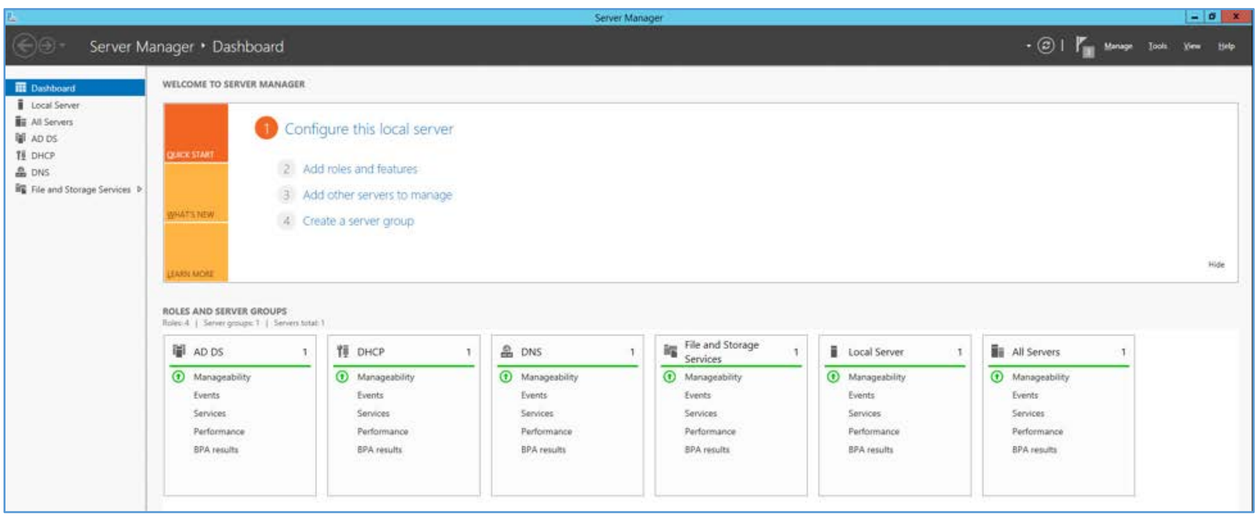
Network Adapter: VLAN 1201

Enterprise Domain Services Installation

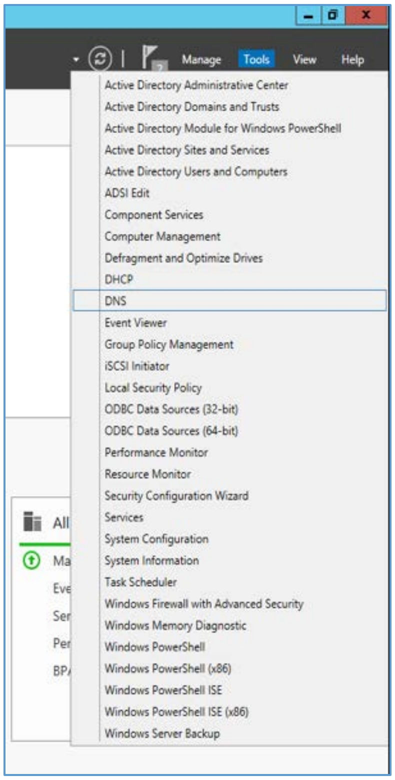
Install the Domain Controller, AD, and DNS appliances according to the instructions detailed in *Building Your First Domain Controller on 2012 R2* [12].

DNS Server Forward Lookup Zone Configuration

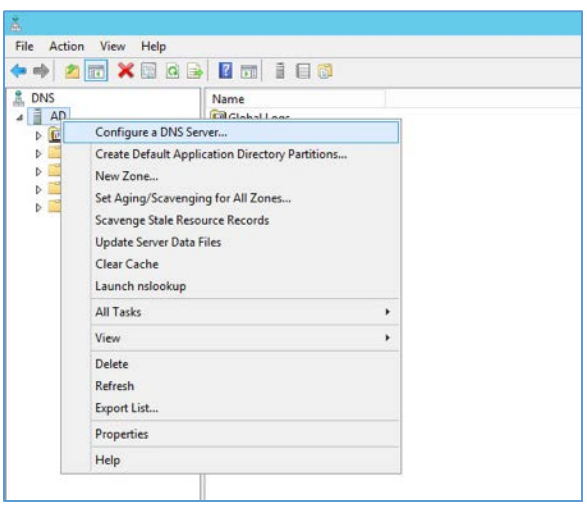
1. Open **Server Manager**.



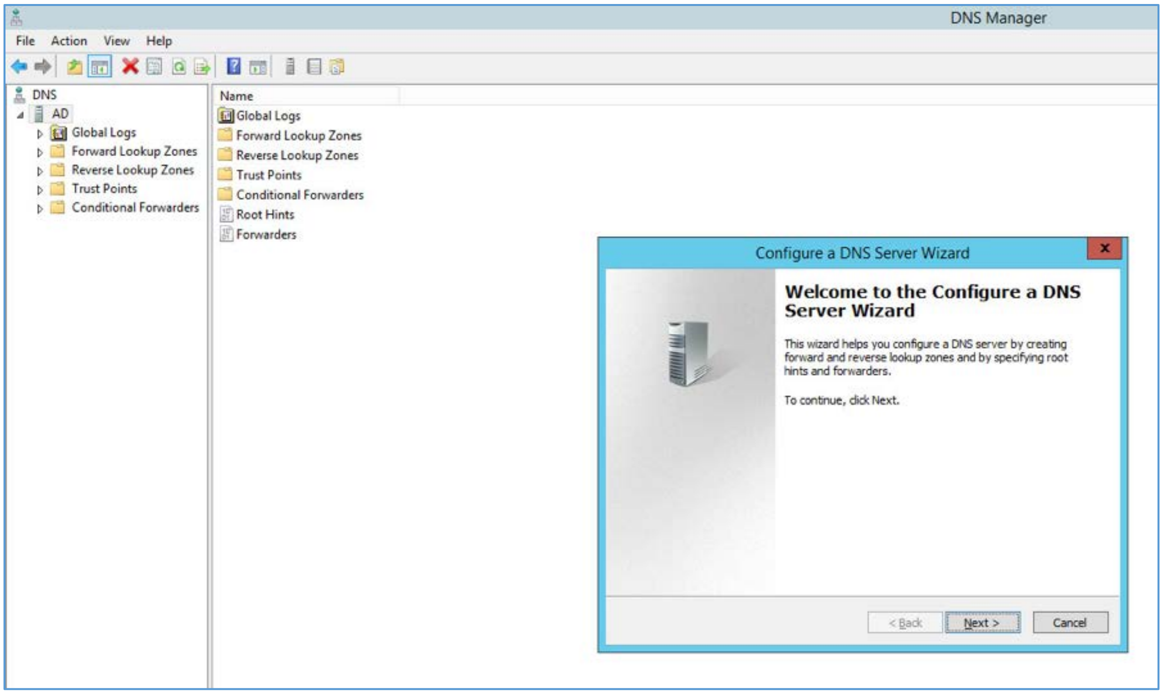
2. In the top right, click on **Tools > DNS**.
3. DNS forward lookup zone should have already been created during the DNS setup process performed previously. If not, follow these instructions:



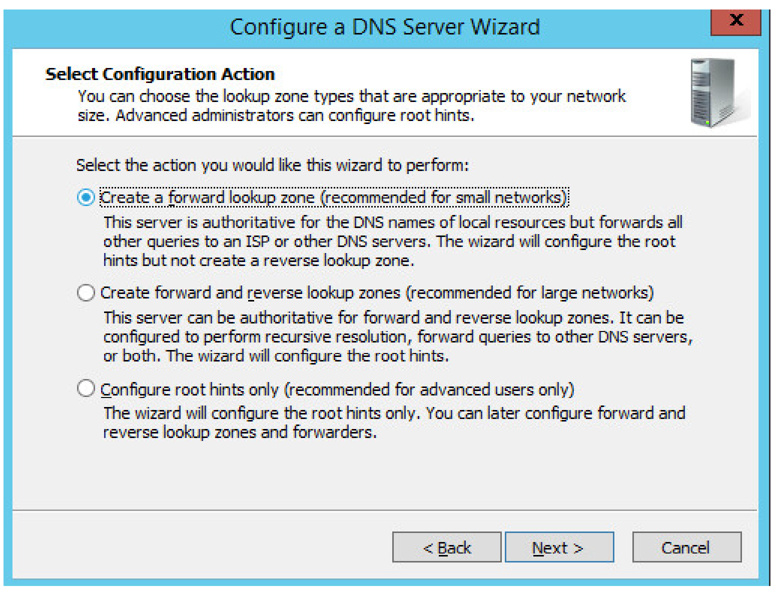
a. Right click on your server's name, and select **Configure a DNS Server…**



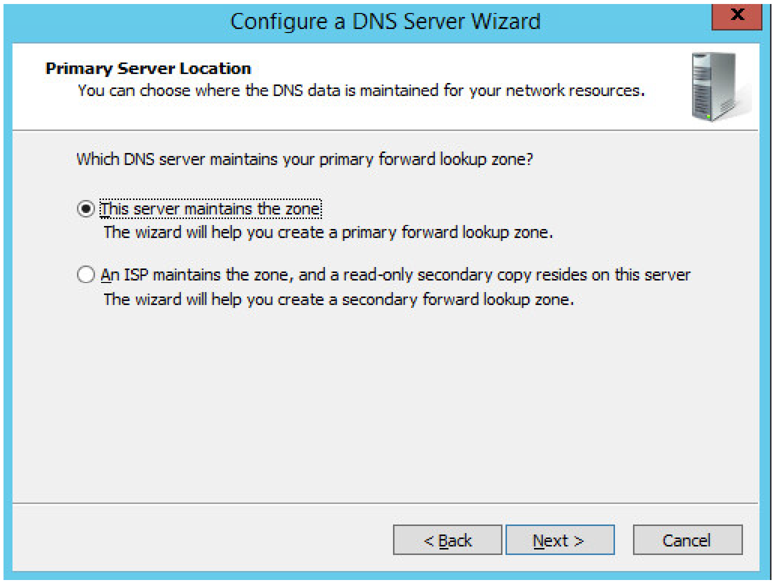
b. Click **Next >**.



c. Click **Next >**.

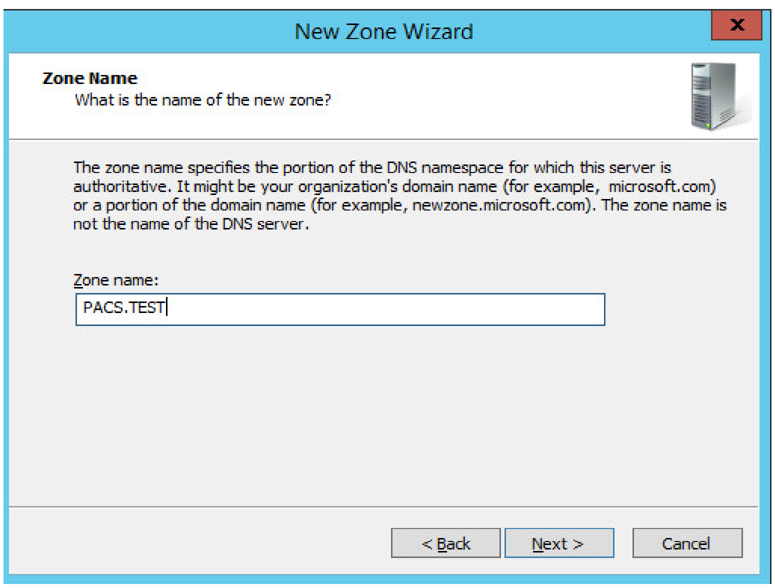


d. Click **Next >**.



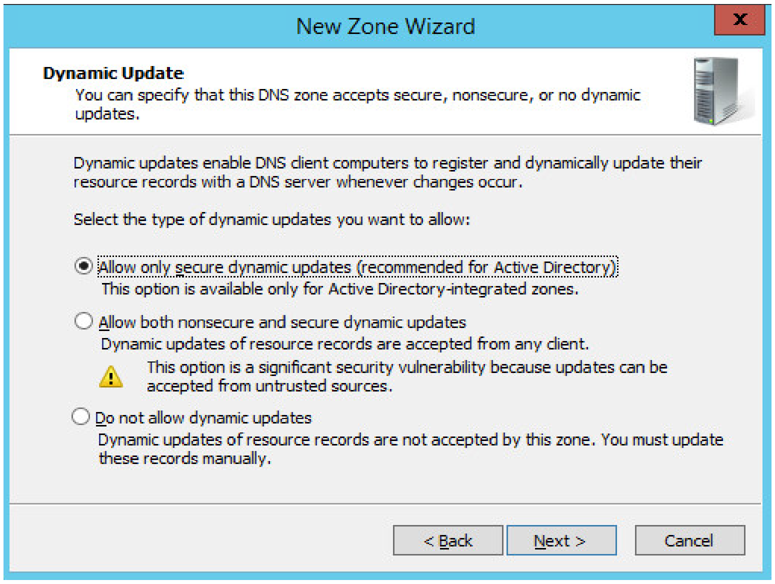
e. Enter **PACS.TEST** as the **Zone name**, that was established previously during setup.

f. Click **Next >**.



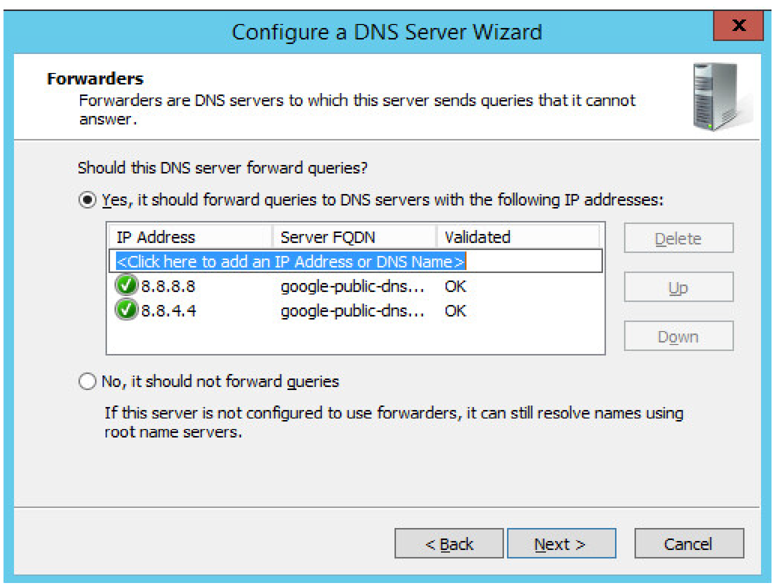
g. Select **Allow only secure dynamic updates**.

h. Click **Next >**.

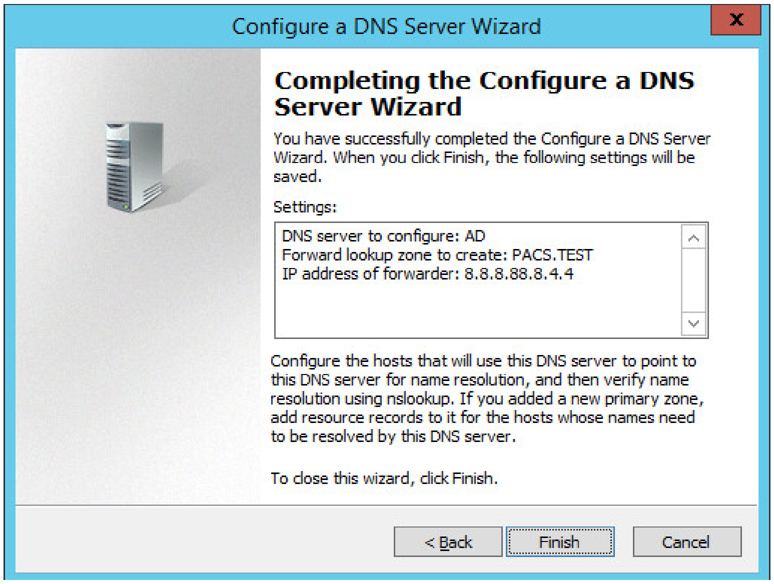


i. Add **Forwarders** (8.8.8.8 and 8.8.4.4 are Google's DNS servers).

j. Click **Next >**.

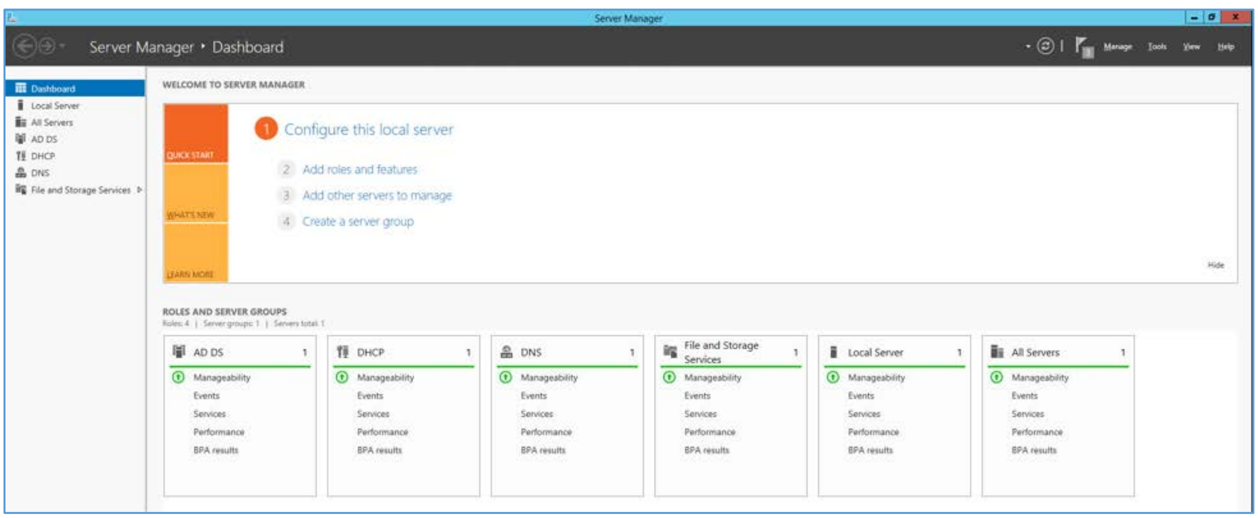


k. Click **Finish**.

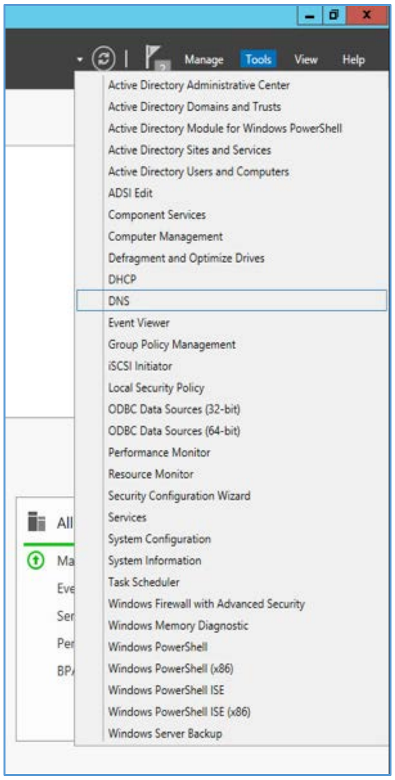


DNS Server Reverse Lookup Zone Configuration

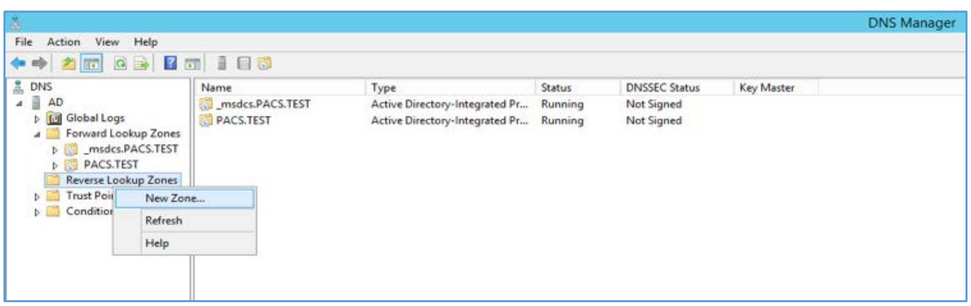
1. Open **Server Manager**.



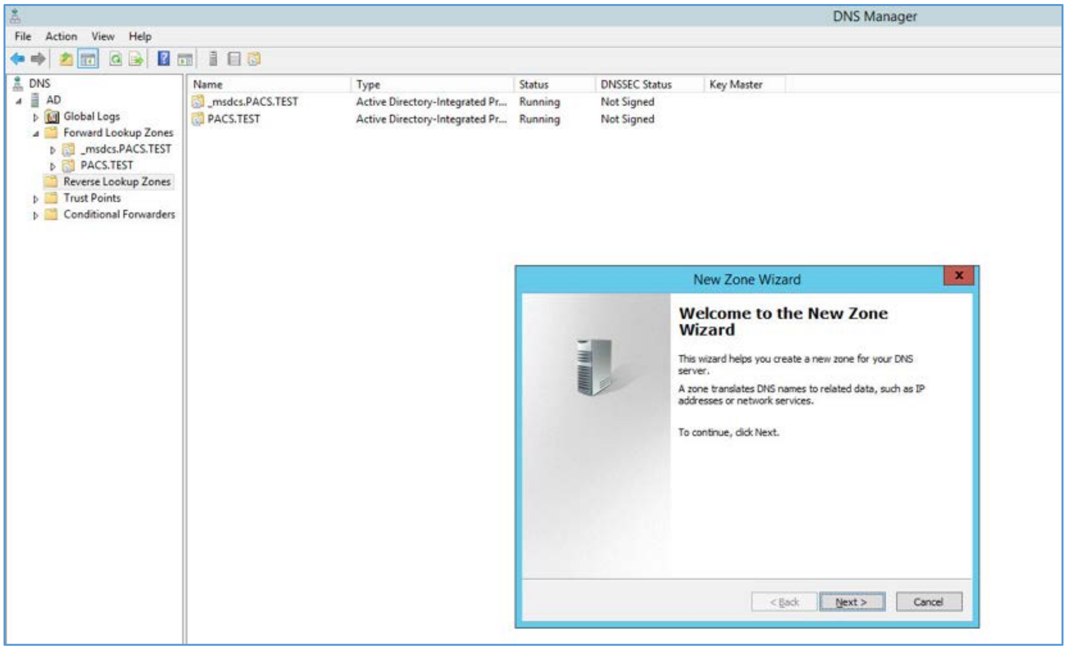
2. In the top right, click on **Tools** > **DNS**.



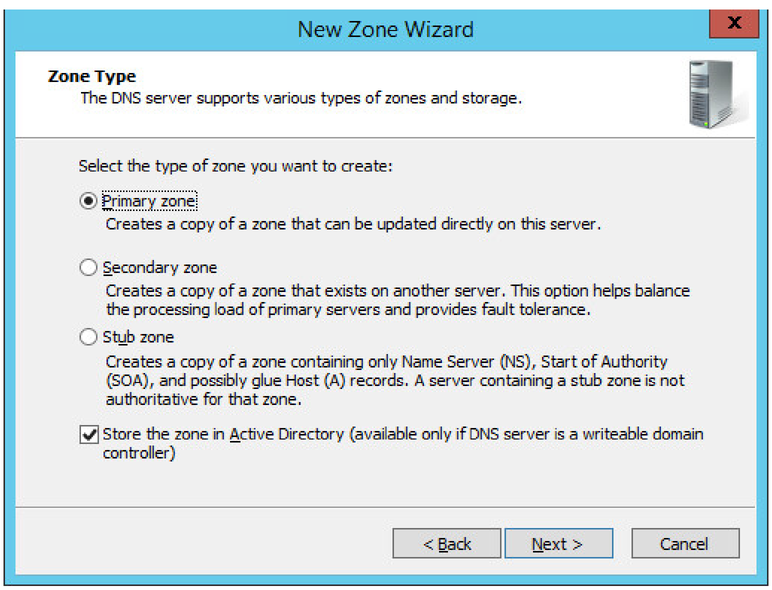
3. Right click on **Reverse Lookup Zones** folder and select **New Zone…**



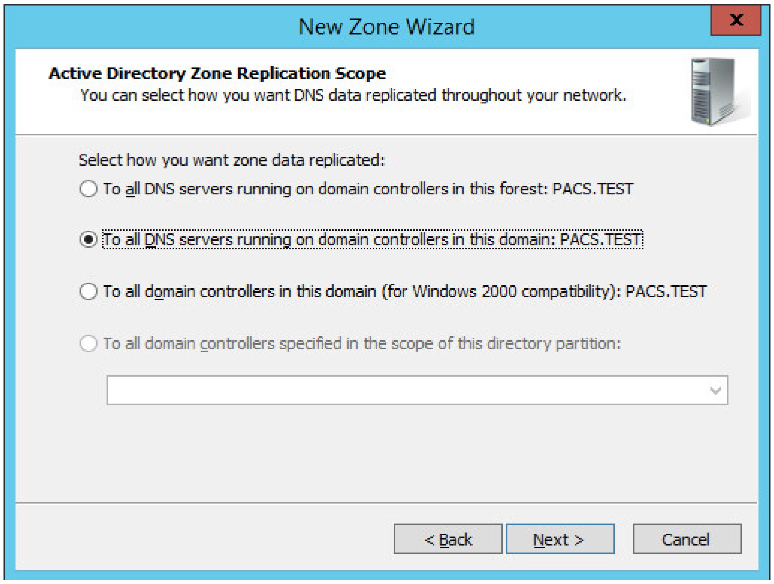
4. Click **Next >**.



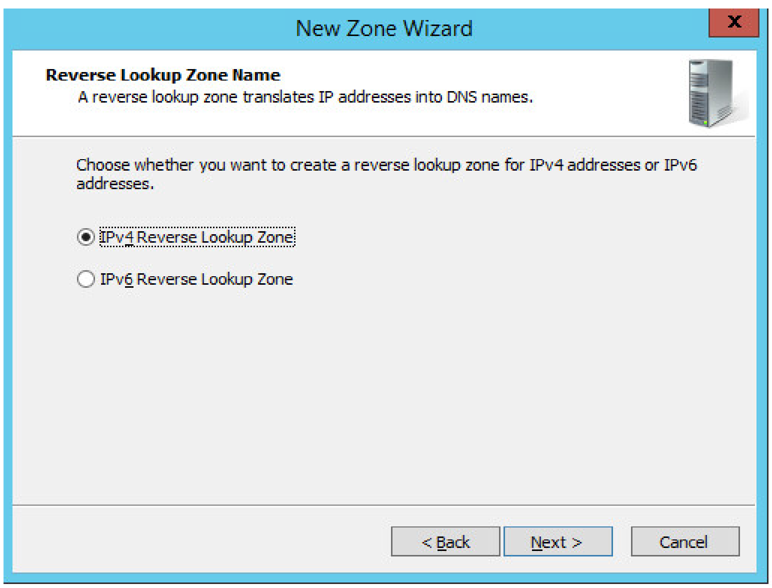
5. Click **Next >**.



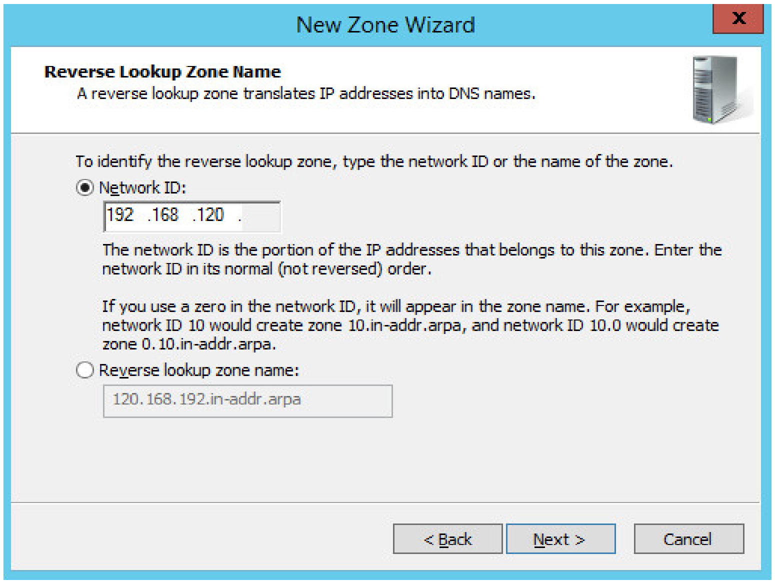
6. Click **Next >**.



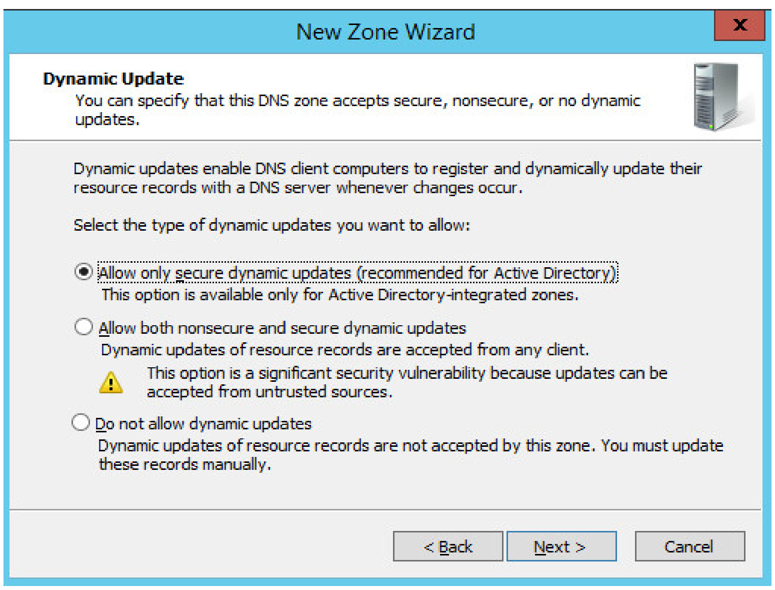
7. Choose Internet Protocol version 4 (IPv4), **IPv4 reverse Lookup Zone** option and click **Next >**.



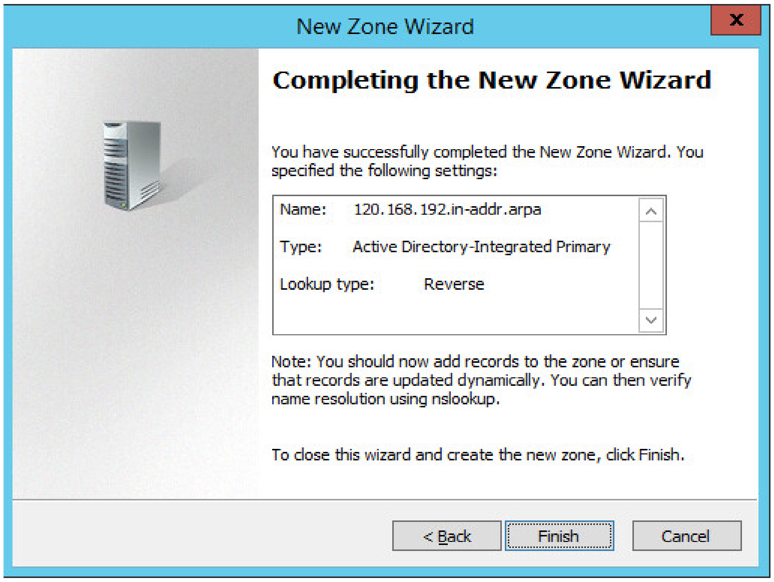
8. Establish which IP addresses should be included in reverse lookup (the example above encompasses all devices in the **192.168.120.0/24** subnet), then click **Next >**.



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



10. Click **Finish**.

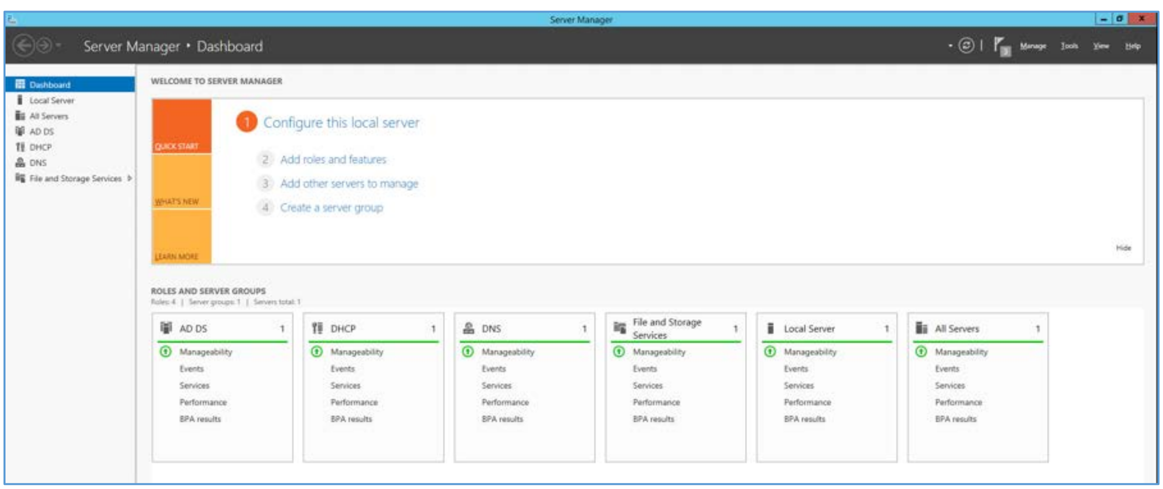


DHCP Server Installation

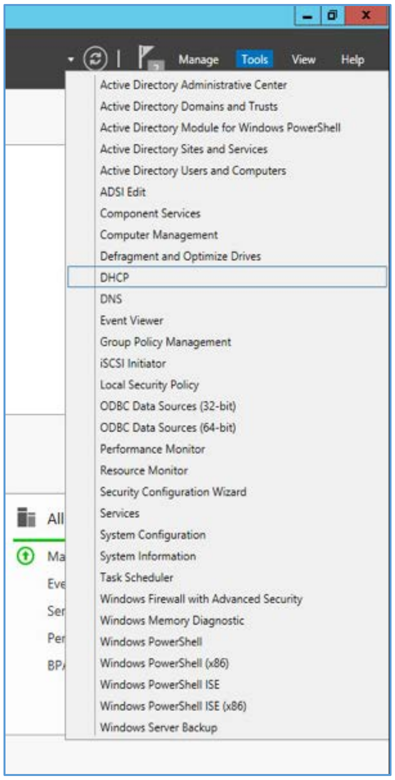
Install the DHCP server according to the instructions detailed in *Installing and Configuring DHCP Role on Windows Server 2012* [13].

DHCP Server Configuration

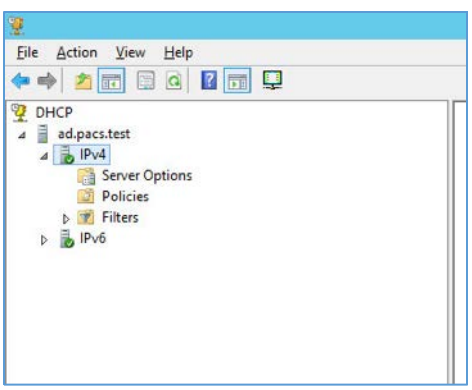
1. Open **Server Manager**.



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



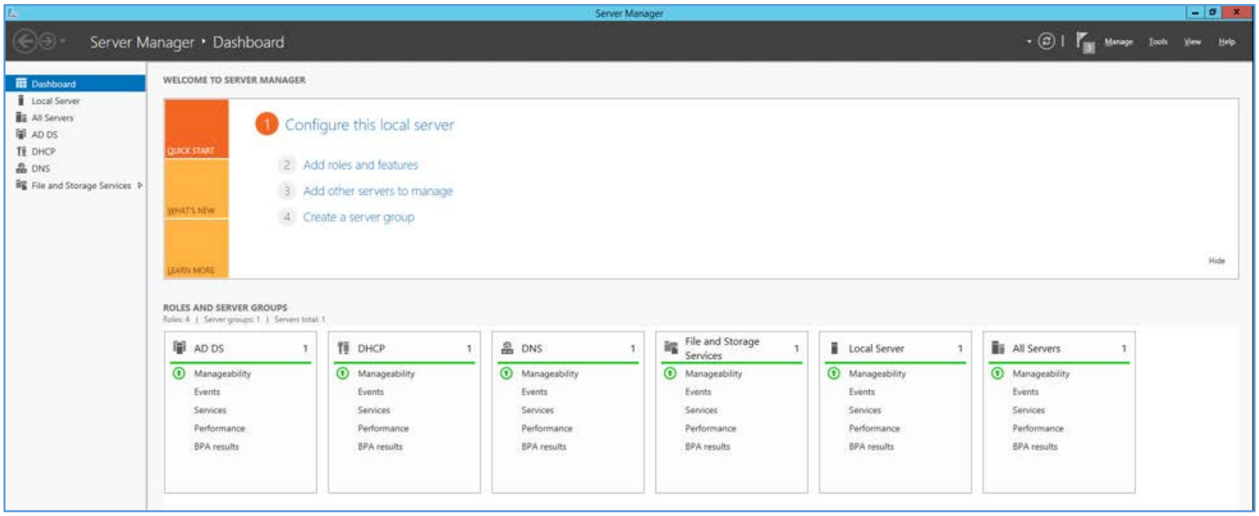
3. If you see a green checkmark on the **IPv4** server, the DHCP server is up and running.



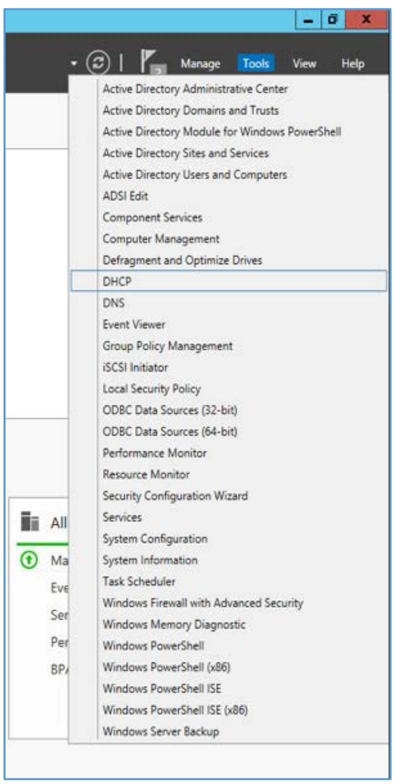
DHCP Scopes Configuration

Performed on Windows Server 2012 R2.

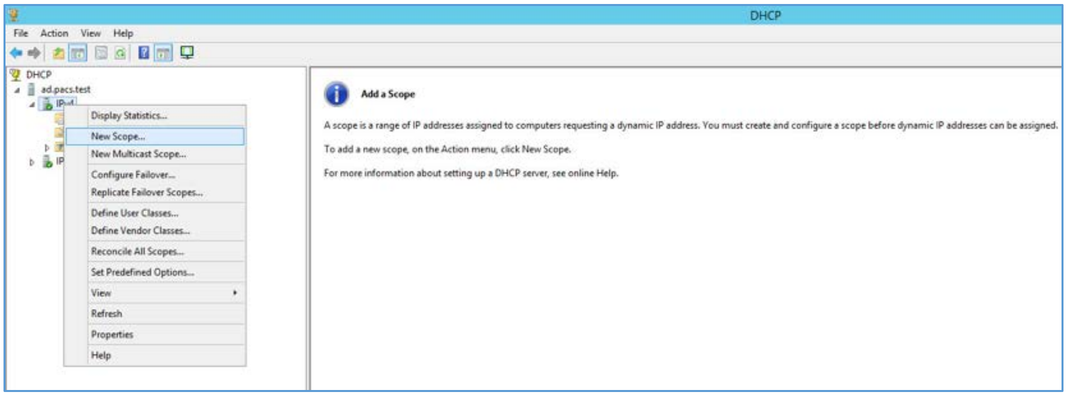
1. Open **Server Manager**.



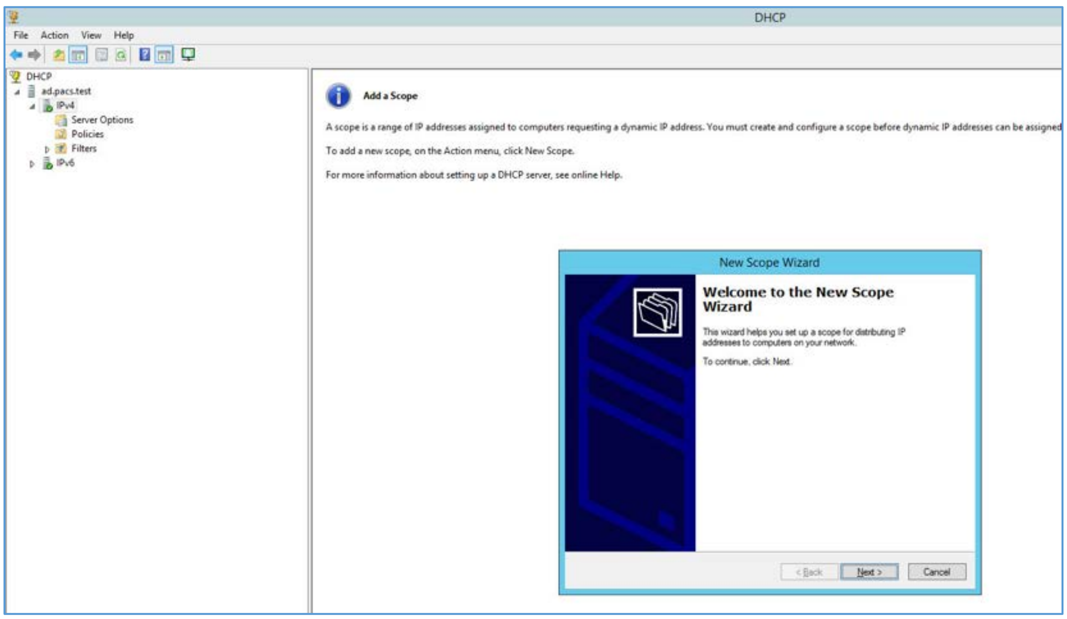
2. In the top right, click on **Tools > DHCP**.



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

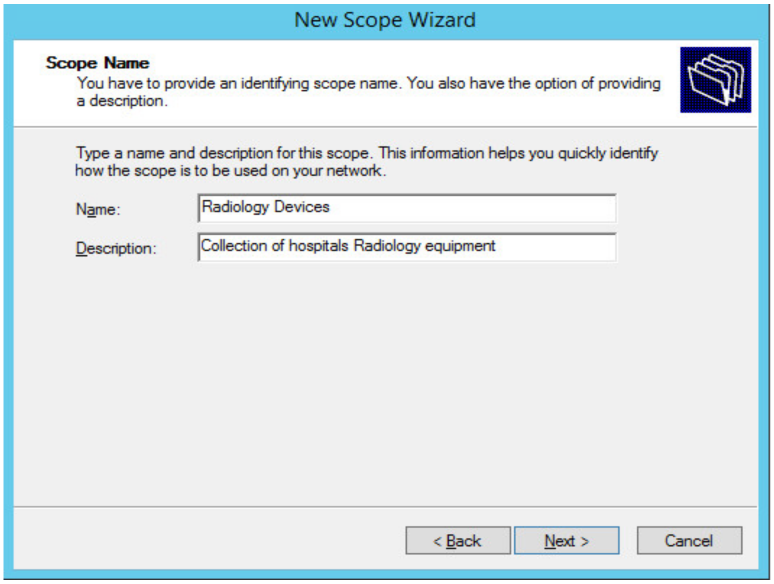


4. **Click Next >**.



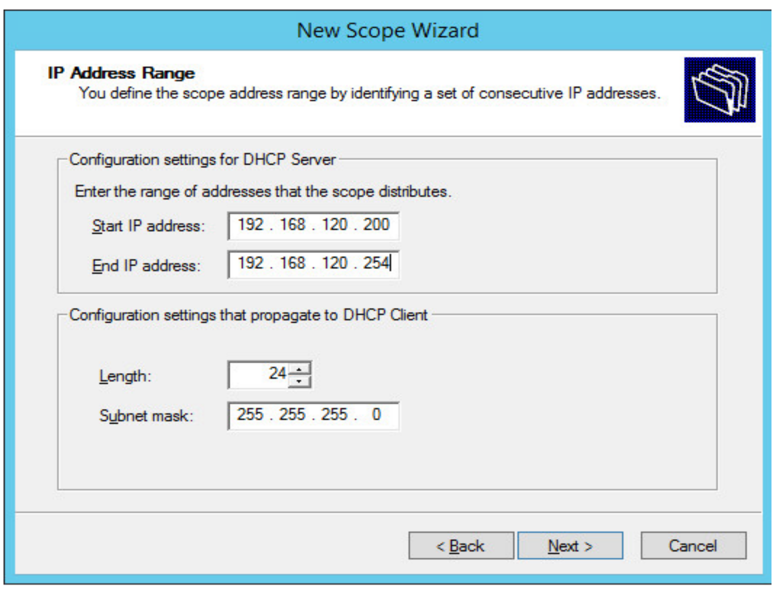
5. Provide a **Name** as **Radiology Devices** and a **Description** as **Collection of hospitals Radiology equipment** in the **New Scope Wizard**.

6. Click **Next >**.

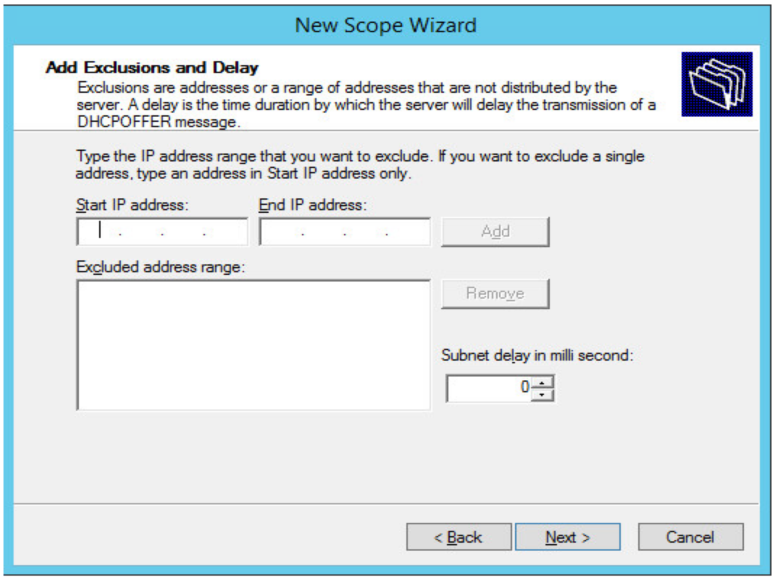


7. Establish the IP range (**192.168.120.200** – **192.168.120.254**) from which the DHCP server should hand out IPs for devices in this scope.

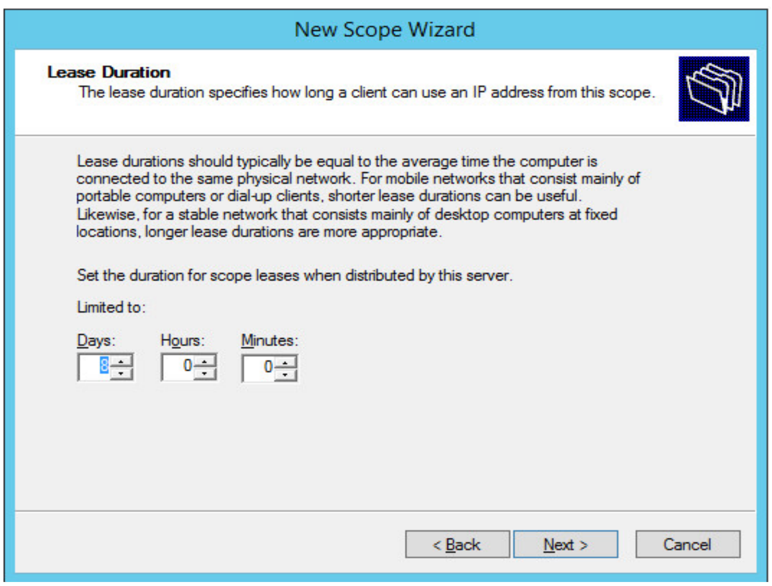
8. Click **Next >**.



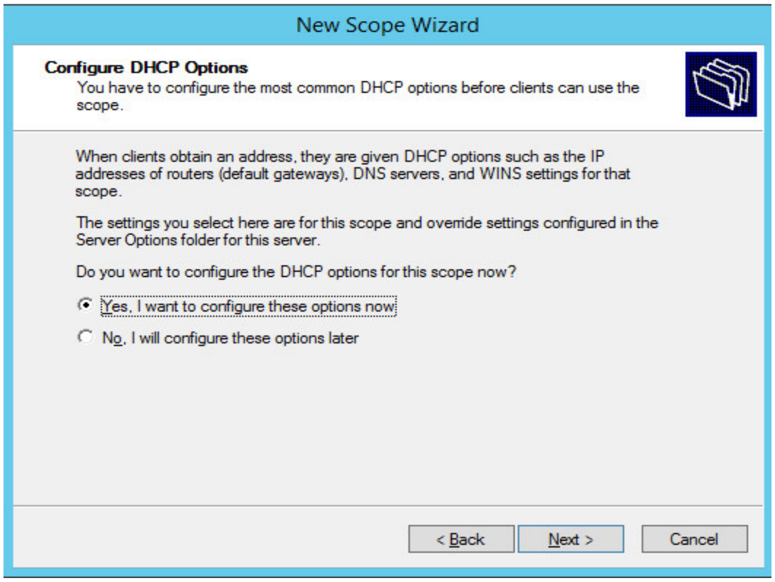
9. Click **Next >**.



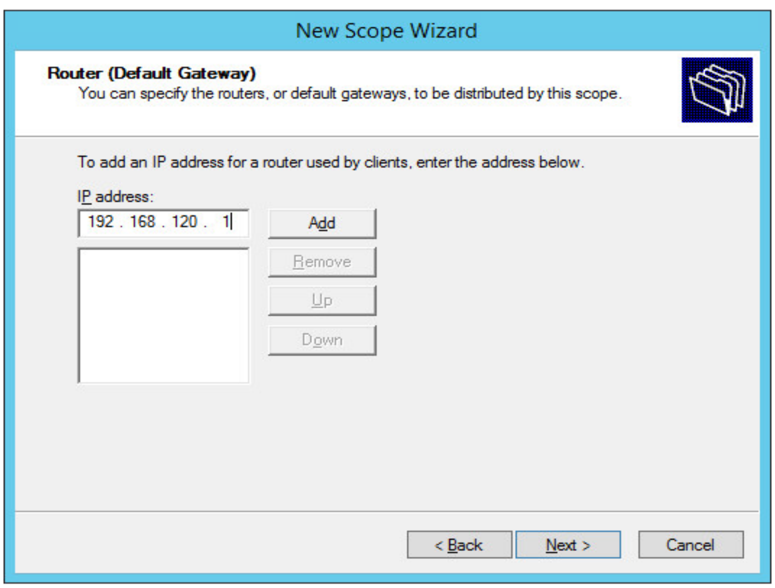
10. Configure preferred **Lease Duration** (e.g., **8 days**), and click **Next >**.



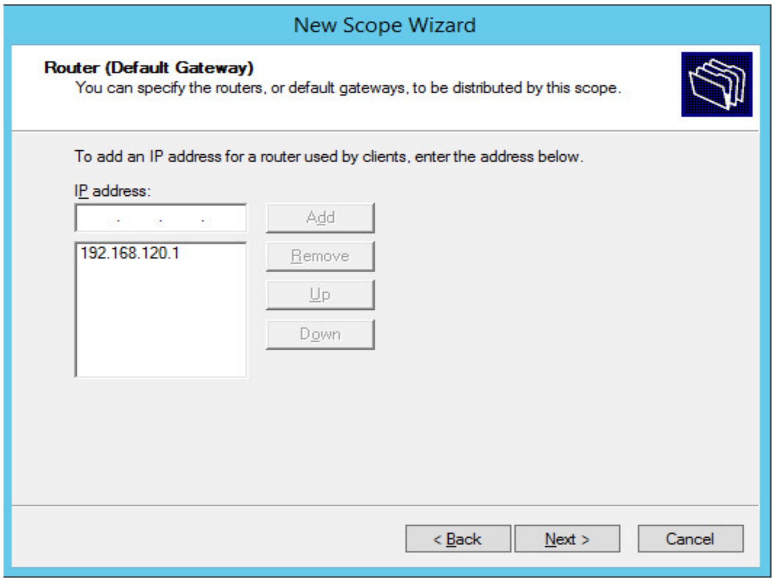
11. Choose **Yes, I want to configure these options now**, and then click **Next >**.



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

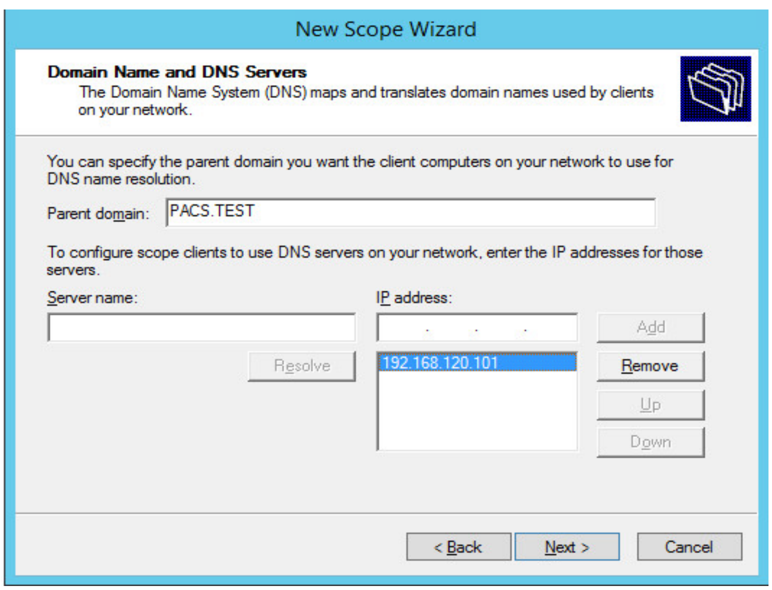


14. Click **Next >**.

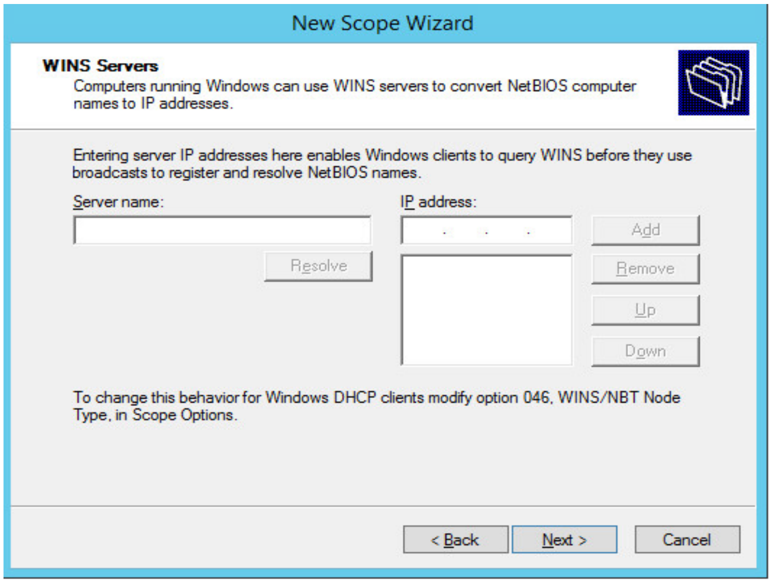


15. Ensure IP address in bottom-right box is the IP address (**192.168.120.101**) for the DNS server configured earlier.

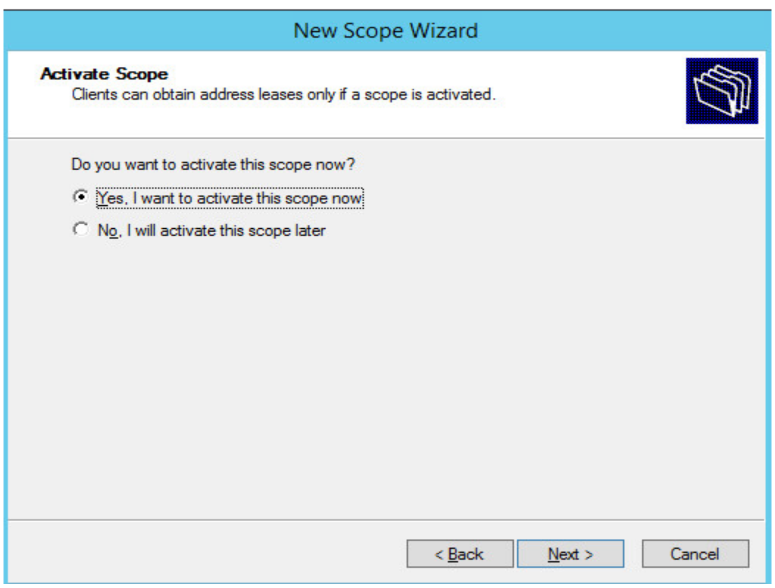
16. Click **Next >**.



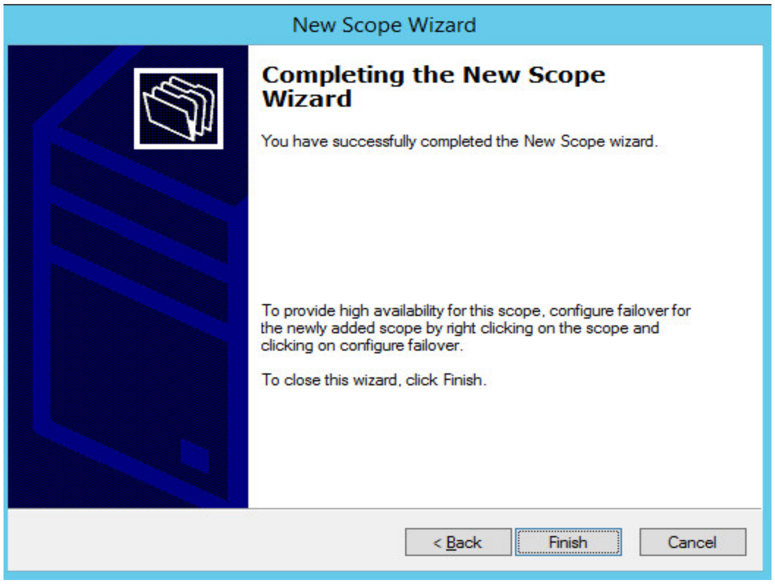
17. Click **Next >**.



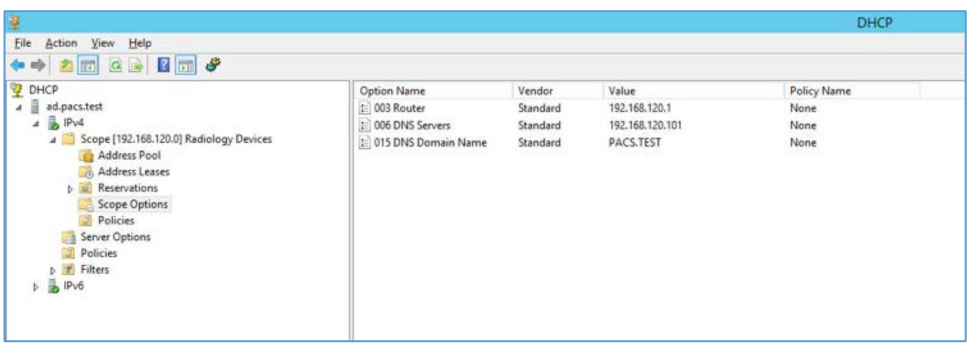
18. Choose **Yes, I want to activate this scope now** option and then click **Next >**.



19. Click **Finish**.



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



2.6.2 DigiCert PKI

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

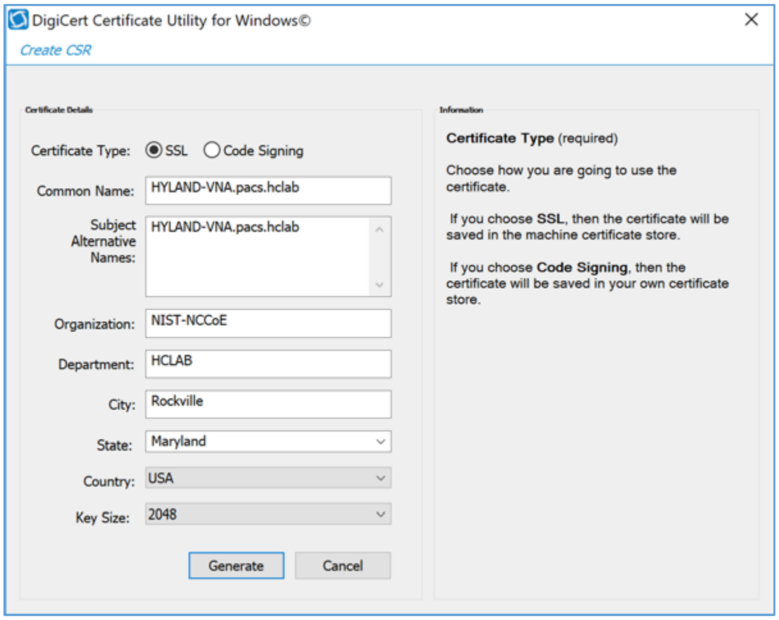
The instructions below describe the process used to obtain an SSL certificate on behalf of medical devices using the DigiCert certificate signing services.

Create CSR

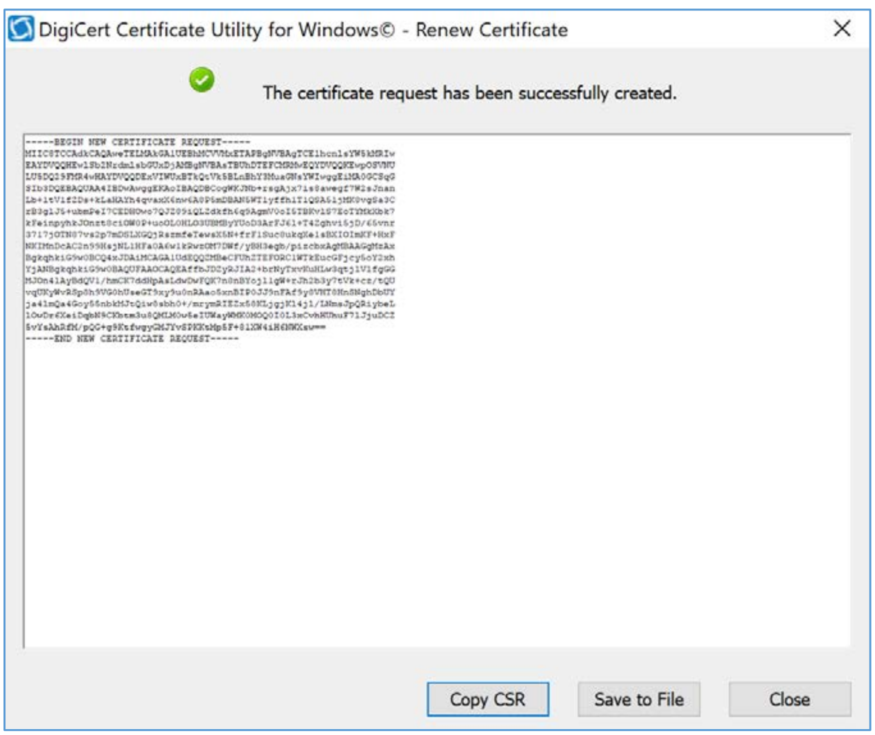
A CSR is represented as a block Base64 encoded PKCS#10 binary format text that will be sent to a CA for digital signature when applying for an SSL Certificate. The CSR identifies the applicant's distinguished common name (domain name), organization name, locality, and country. It also contains the applicant's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

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

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



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



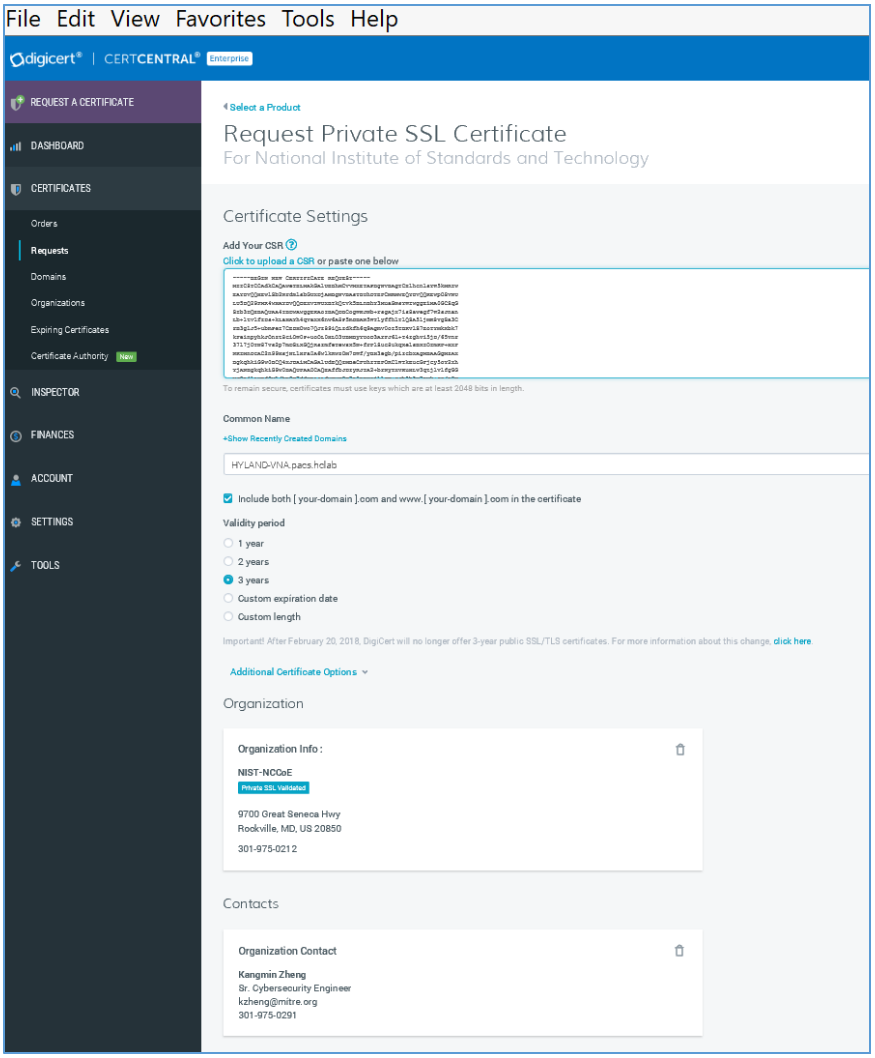
6. Select and copy the certificate contents to the clipboard or save it to an ascii text file. The text contents will be used to paste into the DigiCert order form.

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

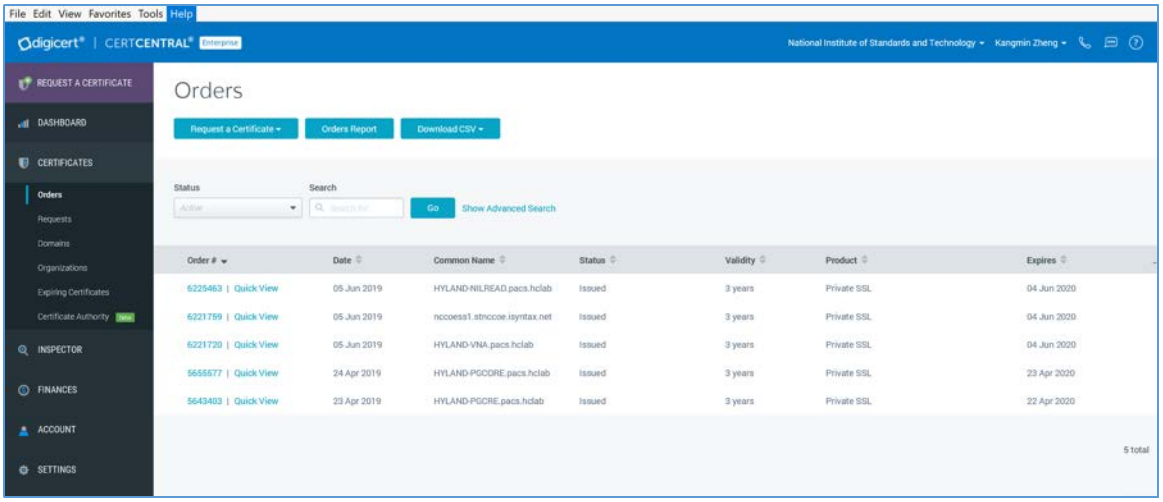
    a. Log in to a DigiCert Dashboard (https://www.digicert.com/account/login.php) with your account username and password. In the portal, select **CERTIFICATES>Requests,** then navigate to **Request a Certificate,** select **Private SSL** to open a certificate request form.

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

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



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

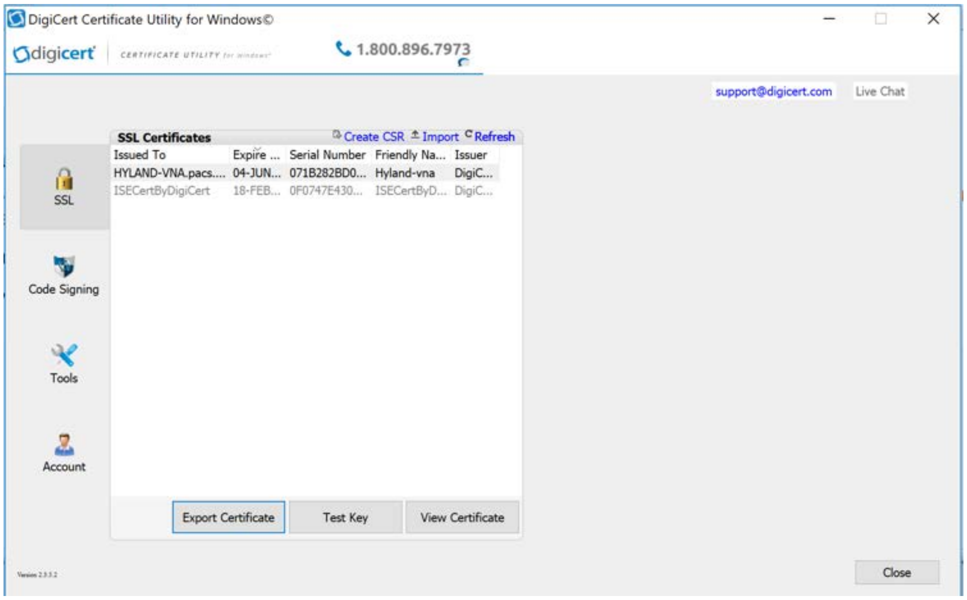


9. Click a specific order number to display the certificate details with a list of actions that can be performed. Click **Download Certificate As** to download certificates with signed CA and Root CA certificates. A variety of certificate formats can be downloaded, such as .crt, .p7b, .pem, etc.
10.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

Import and Export the Signed Certification

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

1. From the DigiCert Certificate Utility for Windows, click the **Import** button to load the downloaded signed Certificate file to the utility. The downloaded file was saved in Step 10 of Section 2.6.2. Click the **Next** button to import.
2. From the DigiCert Certificate Utility for Windows, click **SSL** to list all the imported files.
3. To export the certificate, select the certificate you want to export as a combined certificate file and key file in a .pfx file, or separated as a certificate file and key file, and then click **Export Certificate**.



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

2.7 Network Control & Security

2.7.1 Cisco Firepower

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

Cisco Firepower Management Center Appliance Information

CPU: 8

RAM: 16 GB

Storage: 250 GB (Thin Provision)

Network Adapter 1: VLAN 1201

Operating System: Cisco Fire Linux

Cisco Firepower Management Center Virtual Installation Guide

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

Cisco Firepower Threat Defense Appliance Information

CPU: 8

RAM: 16 GB

Storage: 48.5 GB (Thin Provision)

Network Adapter 1: VLAN 1201

Network Adapter 2: VLAN 1201

Network Adapter 3: VLAN 1099

Network Adapter 4: VLAN 1099

Network Adapter 5: Trunk Port

Network Adapter 6: Trunk Port

Network Adapter 7: VLAN 1101

Network Adapter 8: VLAN 1101

Network Adapter 9: VLAN 1701

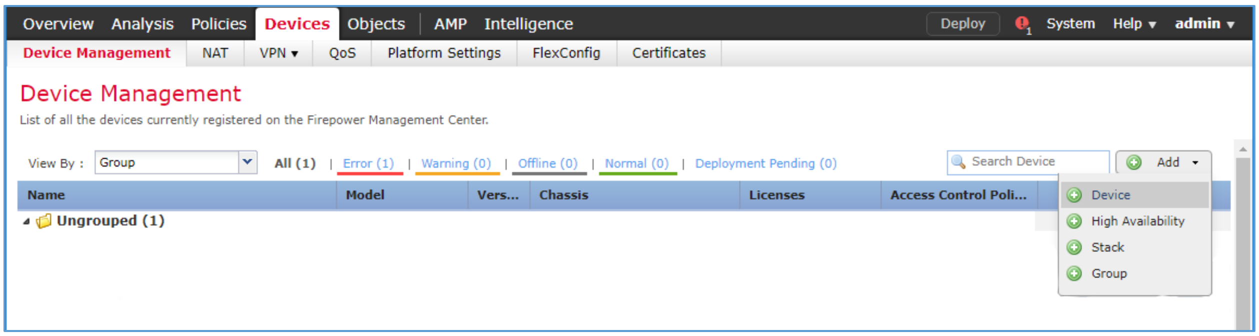
Operating System: Cisco Fire Linux

Cisco Firepower Threat Defense Virtual Installation Guide

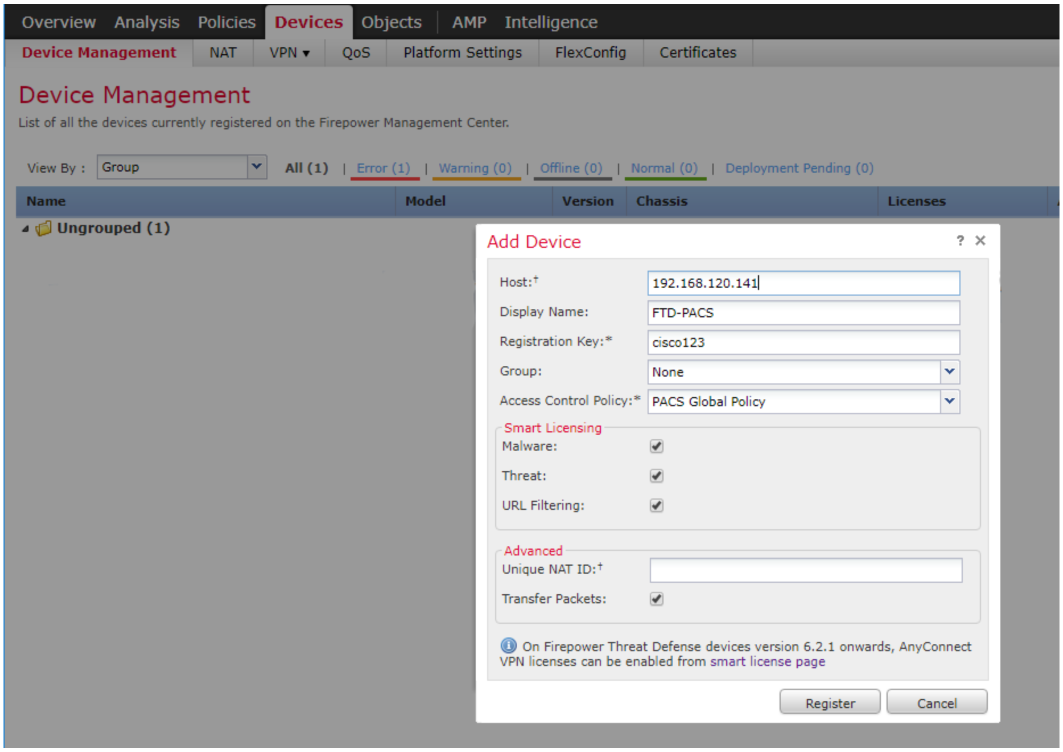
Install the Cisco Firepower Threat Defense Virtual appliance, according to the instructions detailed at Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide [16].

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

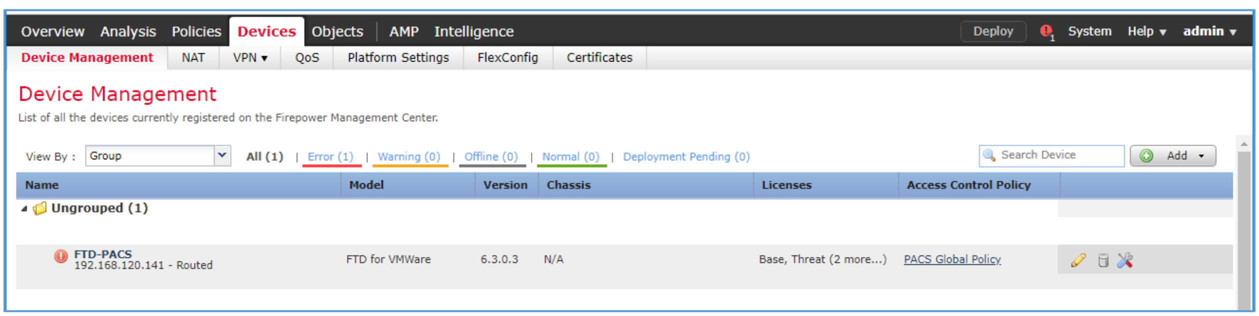
1. Log in to the **FMC Console**.
2. Navigate to **Devices > Device Management**.
3. Click the **Add drop-down** button and select **Add Device**.



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**.



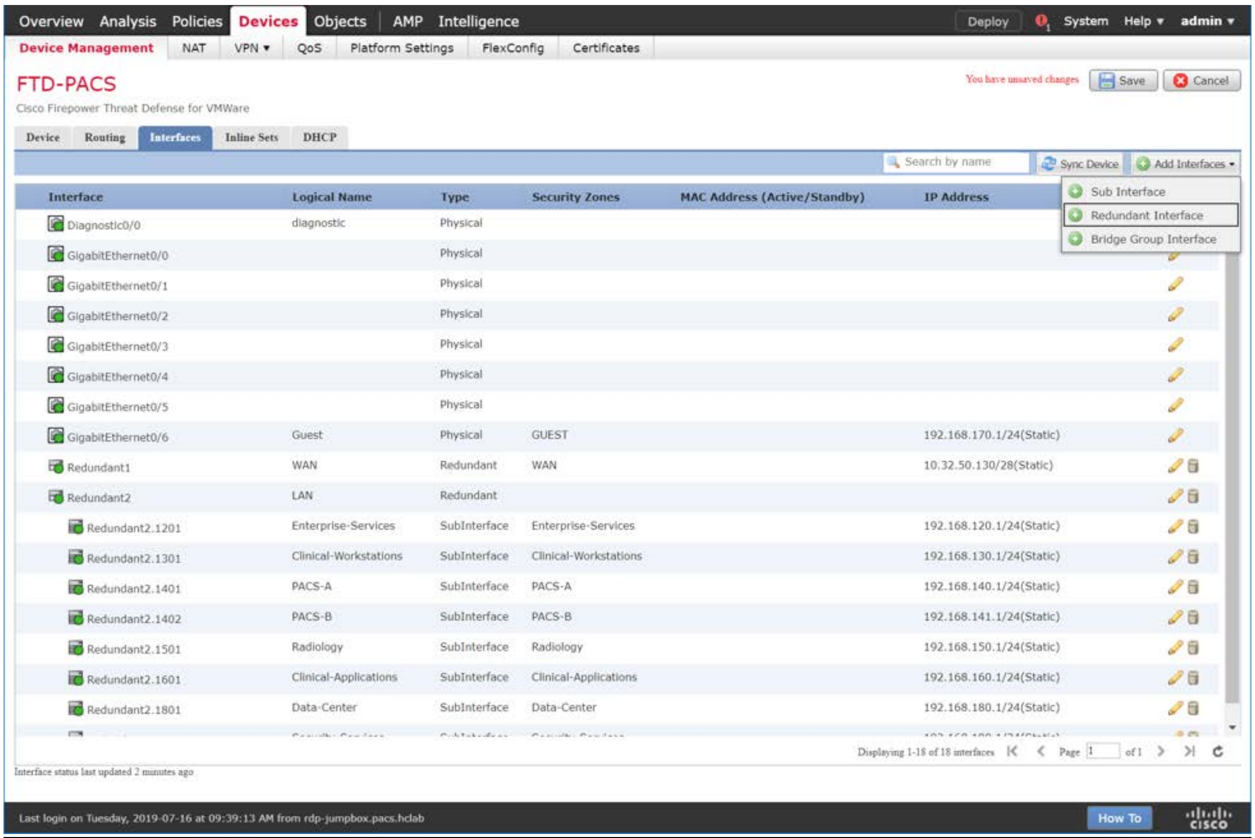
11. The FTD appliance will be added to the FMC's **device list**.



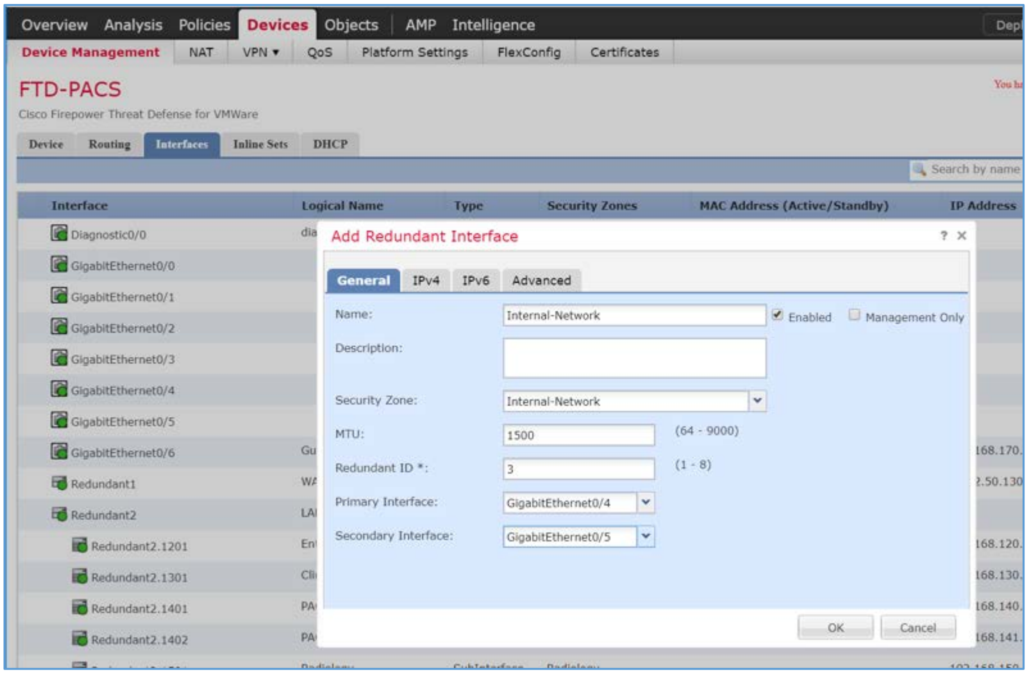
FTD Interfaces for PACS Architecture Configuration

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

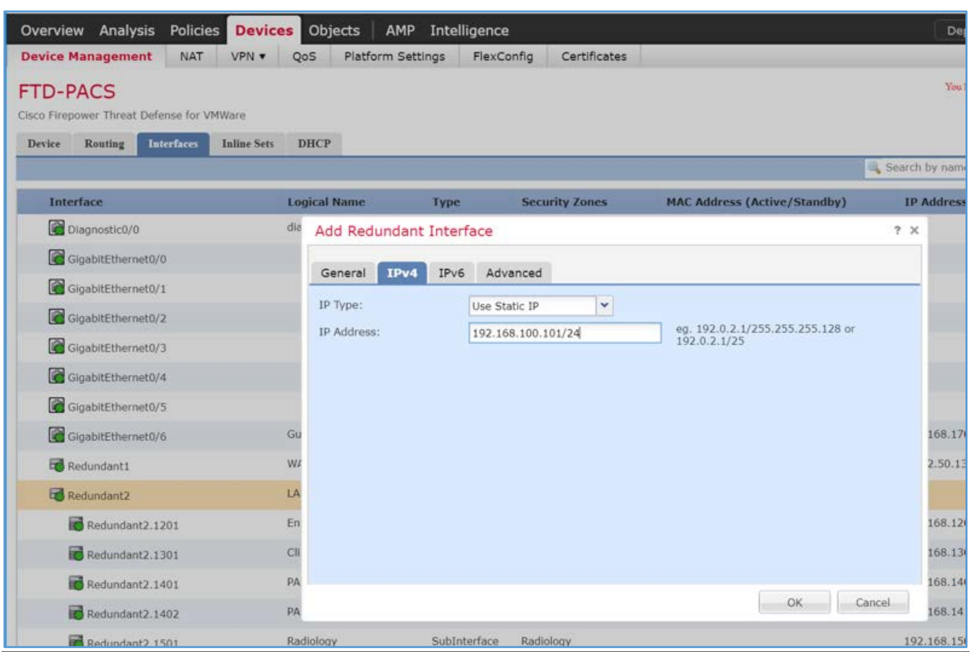
1. Log in to the **FMC Console**.
2. Navigate to **Devices > Device Management**.
3. Find your FTD device and click the **edit** icon.
4. Navigate to **Add Interfaces > Redundant Interface**.



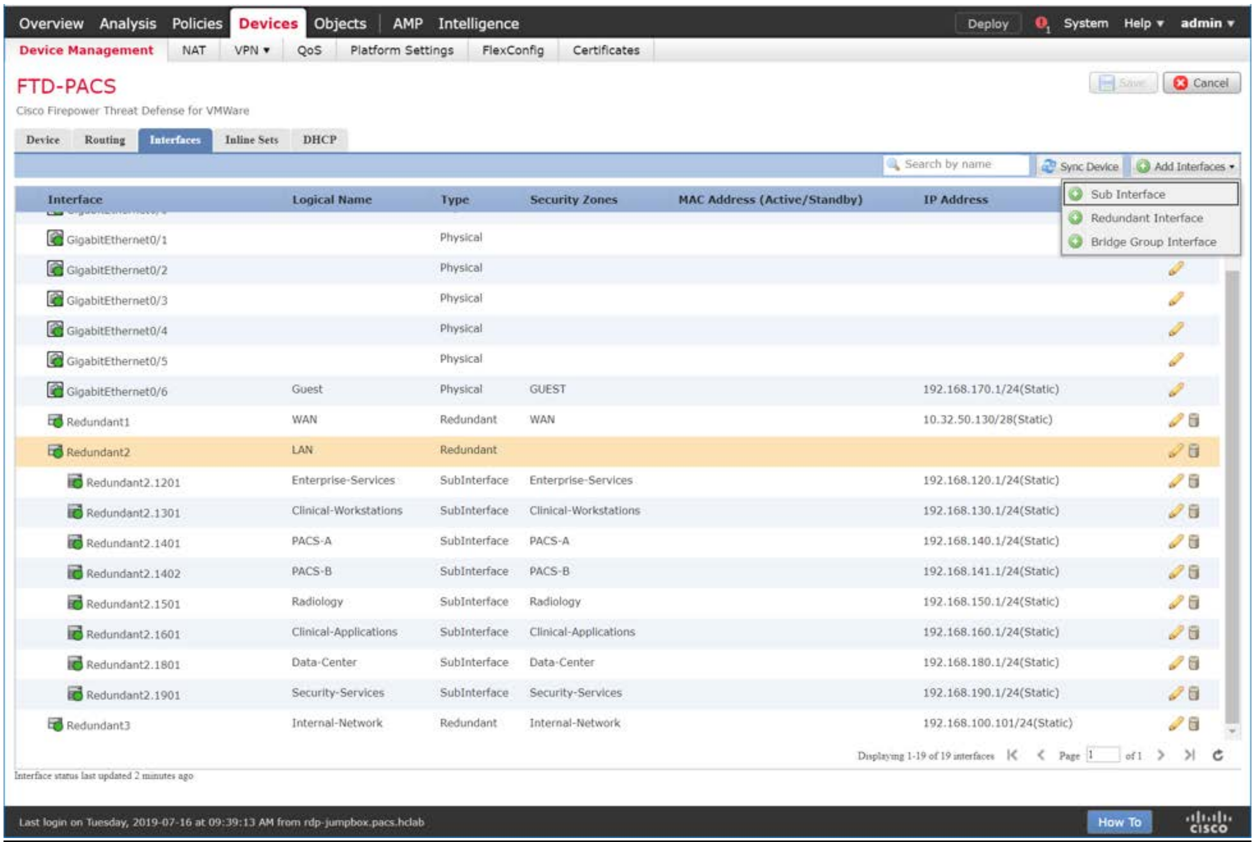
5. Enter **Internal-Network** as the **name** for the redundant interface.
6. Create and/or add a **security zone** to the redundant interface.
7. Assign a **Redundant ID** (e.g., **Internal-Network**) to the redundant interface.
8. Select a **primary interface** and **secondary interface** for the redundant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



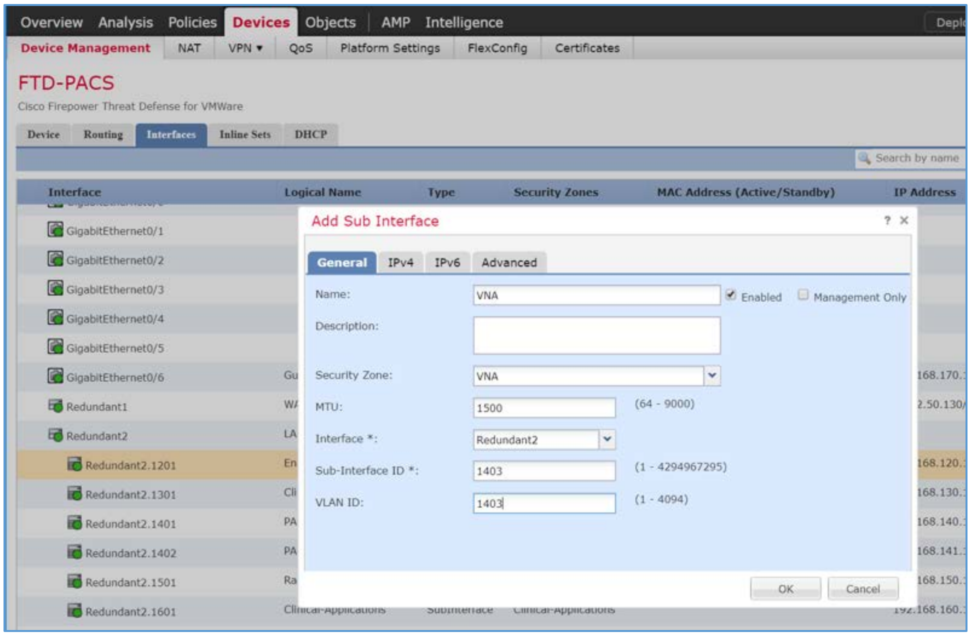
12. Navigate to **Add Interfaces > Sub Interface**.



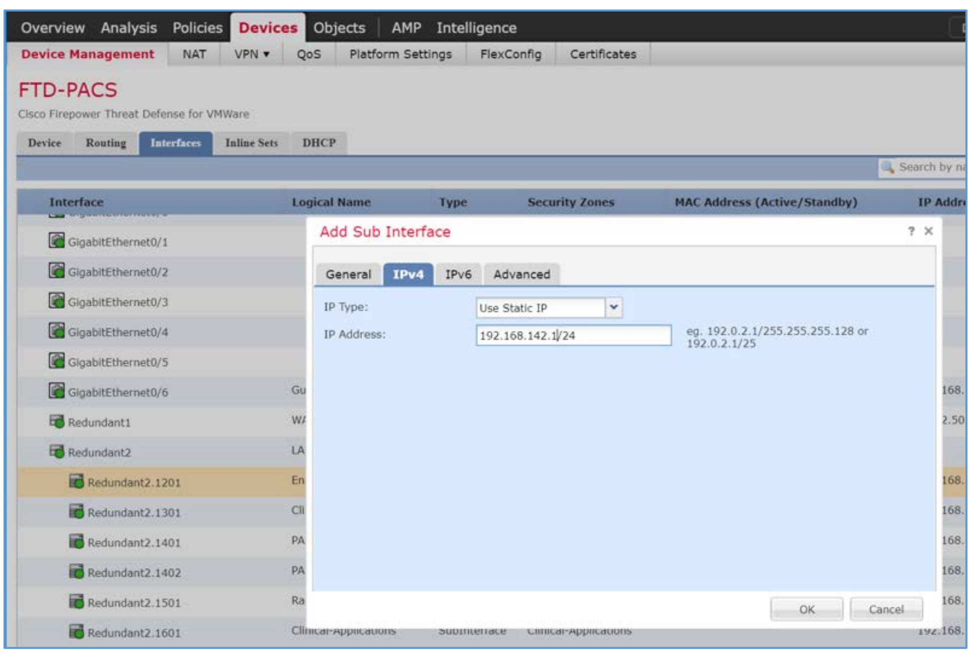
13. Enter **VNA** as the **name** for the sub interface.
14. Create and/or add a **security zone**, **VNA**, to the sub interface.
15. Select an **interface** under which the sub interface will operate.

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

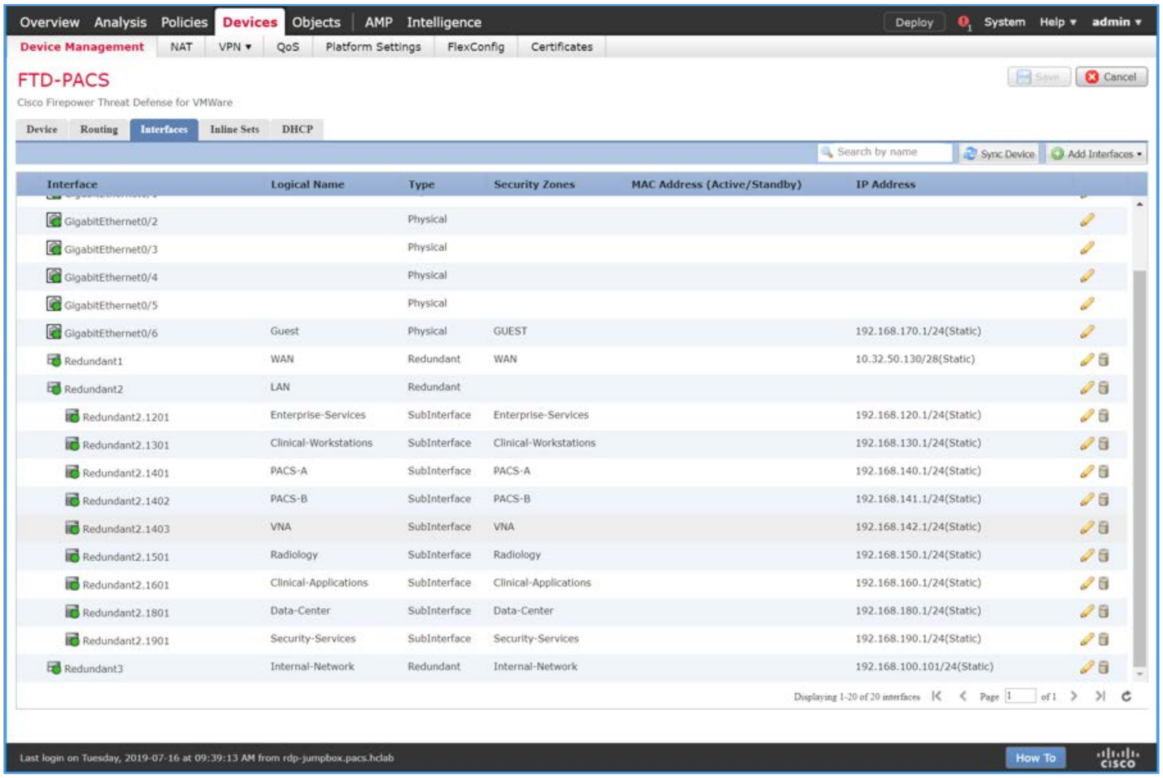
16. Assign **1403** as the **Sub Interface ID** to the sub interface.
17. Assign **1403** as the **VLAN ID** to the sub interface.



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

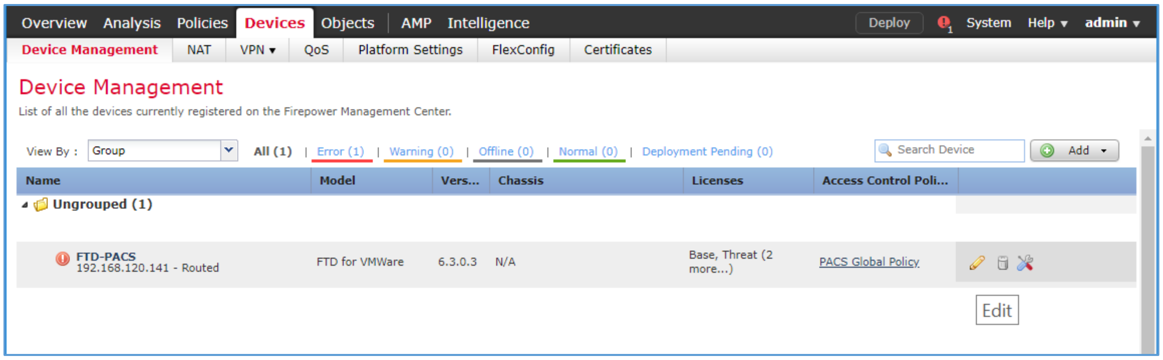


21. Click **Save**.
22. Click **Deploy** and wait for deployment to FTD to complete.
23. Refresh the page and confirm that the redundant interface and sub-interface are running (shown with a green dot on the interface's icon).

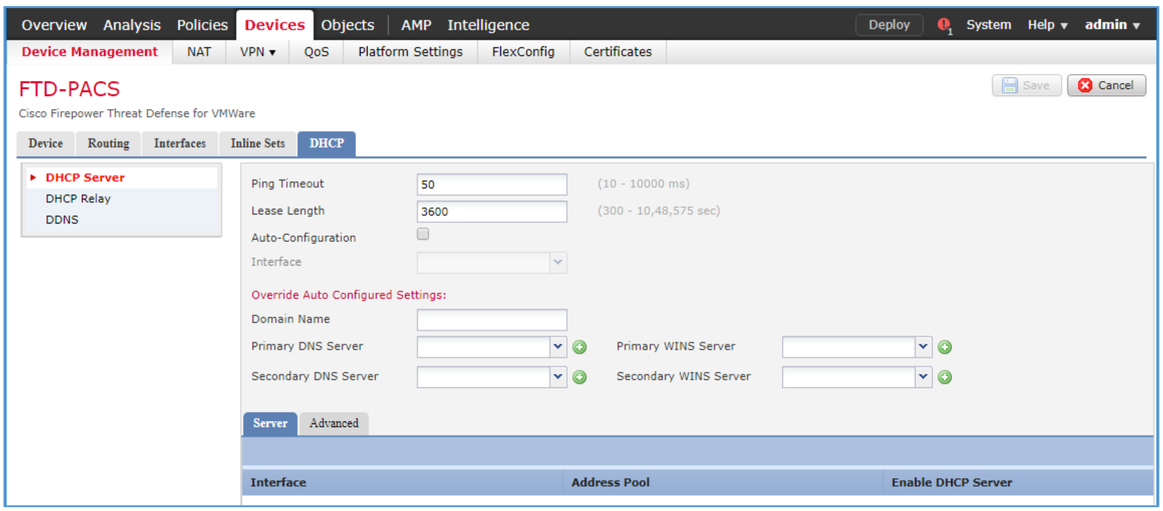


DHCP Relay Through Cisco Firepower Management Center Configuration

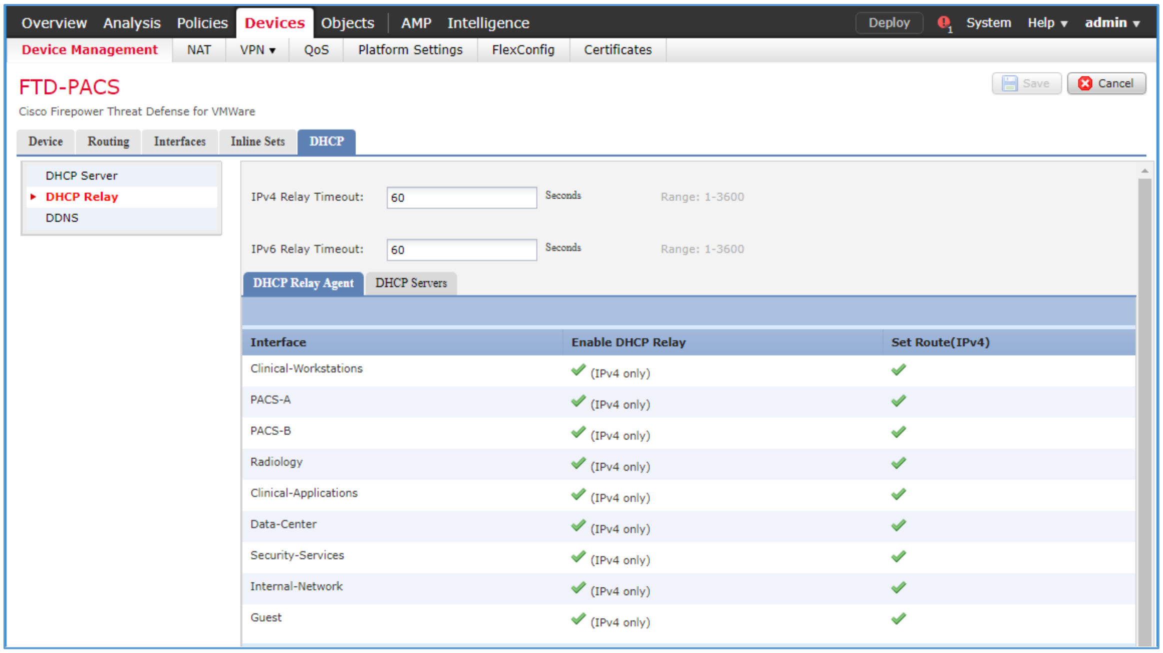
1. Log in to the **FMC Console**.
2. Navigate to **Devices > Device Management**.
3. Find your FTD device and click the **edit** icon.



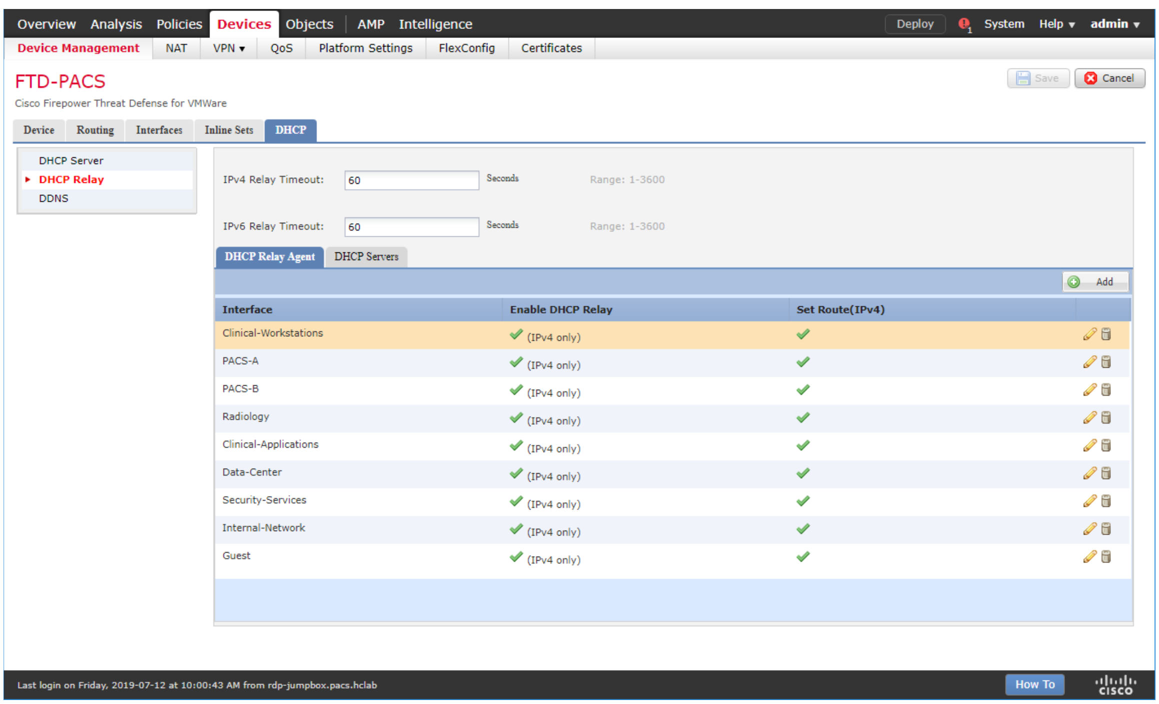
4. Navigate to the **DHCP** tab.



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

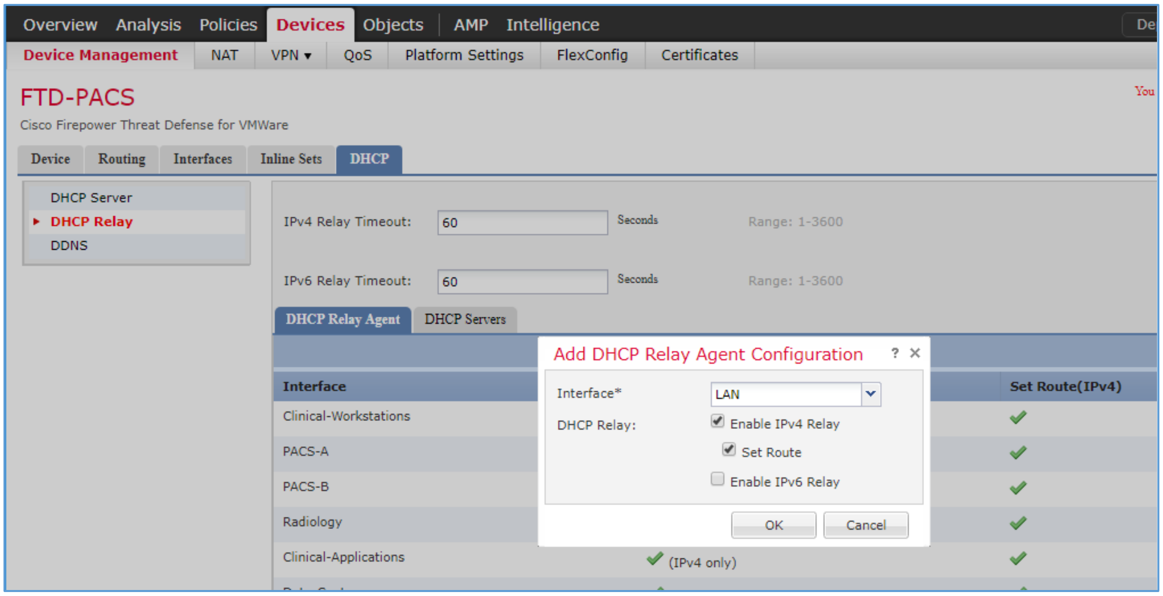


6. Under **DHCP Relay Agent**, click **Add**.

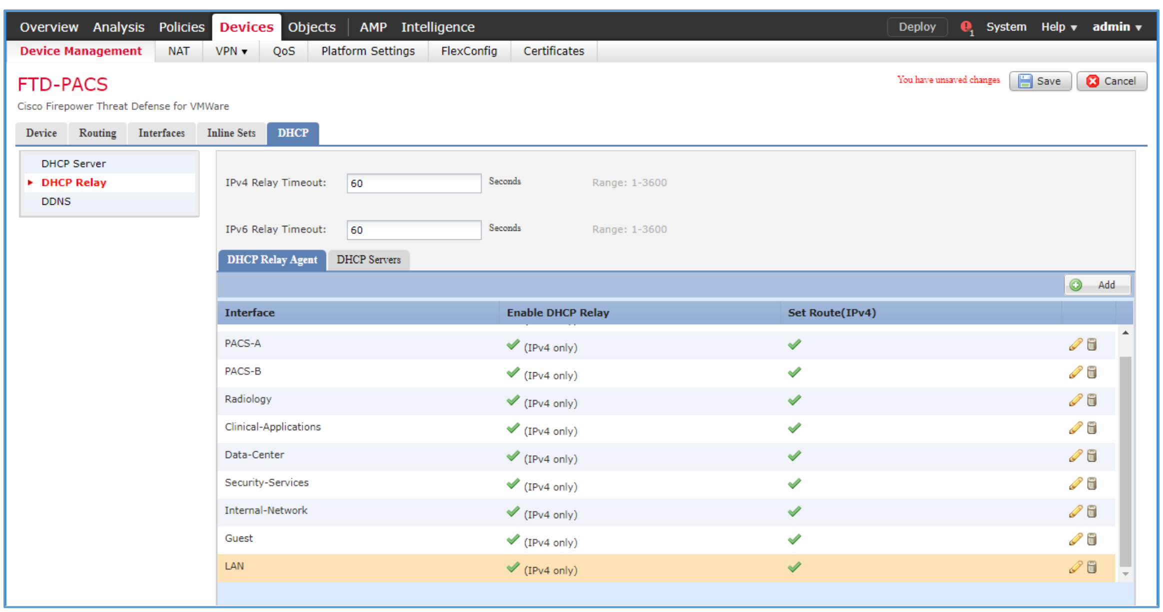


7. Assign an **FTD interface** as **LAN**.

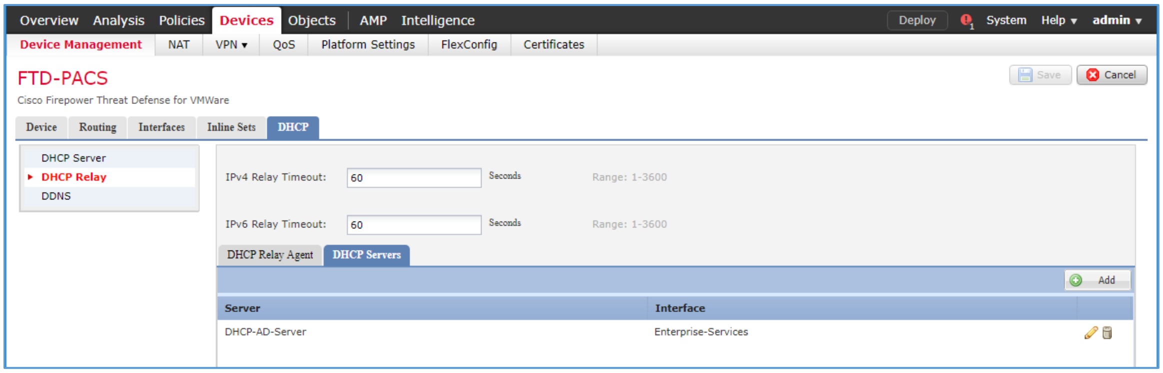
8. Check the box next to **Enable IPv4 Relay**.
9. Check the box next to **Set Route**.
10. Click **OK**.



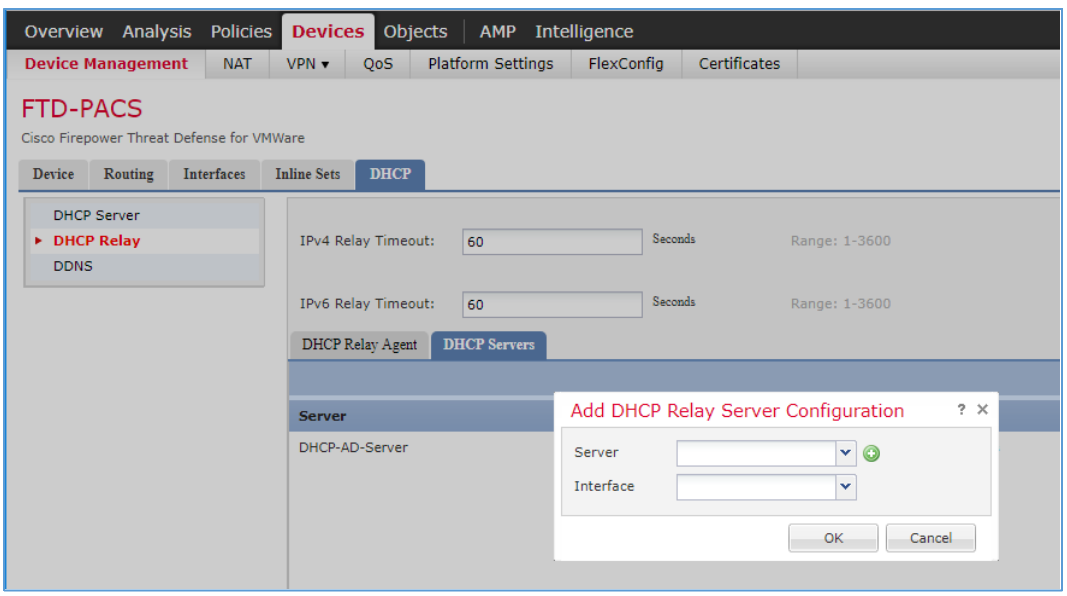
11. Ensure the new relay, **LAN**, is shown in the **DHCP Relay Agent** list.



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



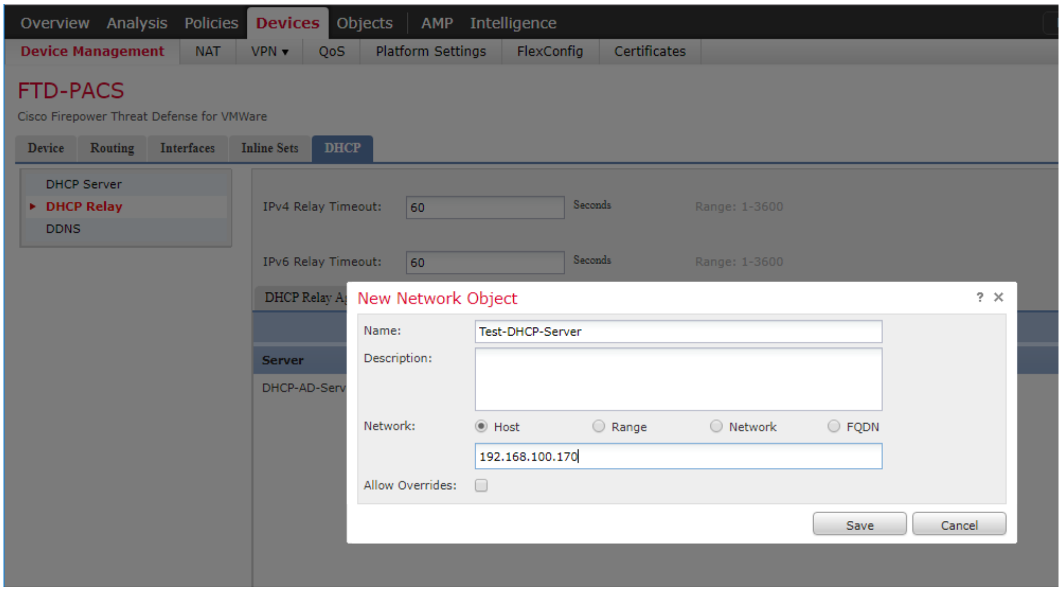
13. Click the green **+** button to create a new object for the DHCP server.



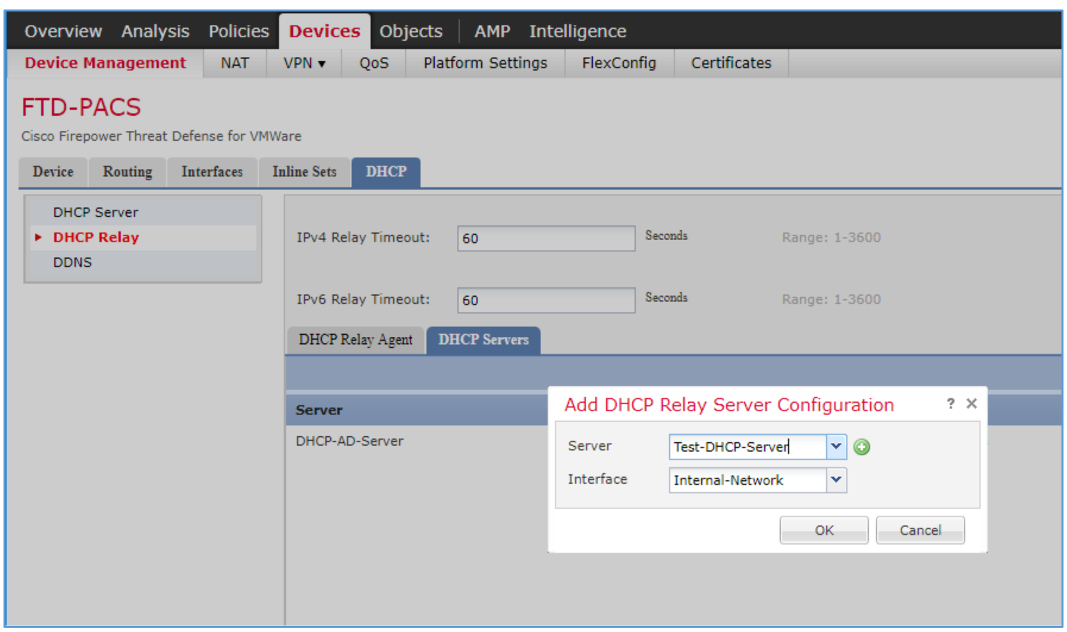
14. Enter **Test-DHCP-Server** as a **name** for the DHCP server.

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

16. Click **Save**.

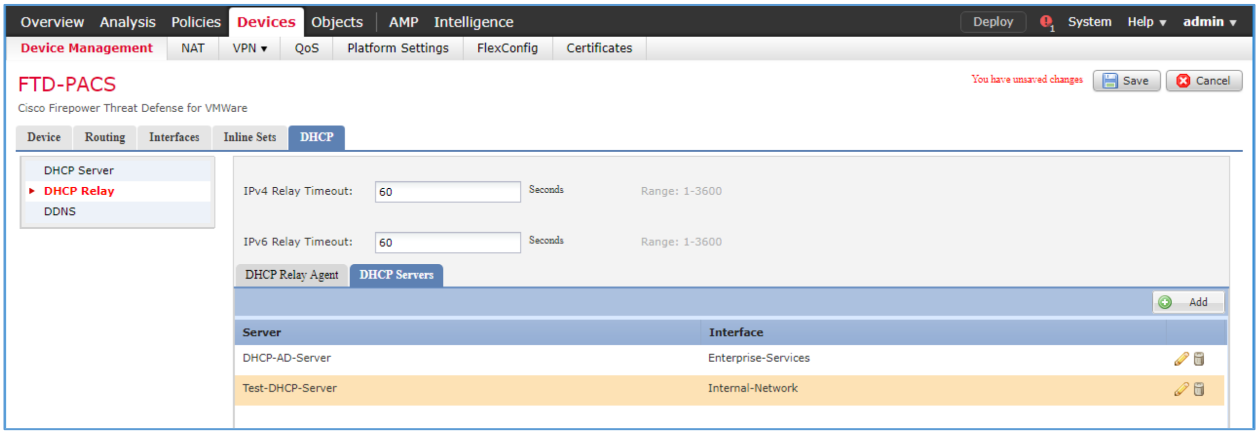


17. Select the newly created **DHCP server**.
18. Select an **FTD interface** through which the **DHCP server** can be connected.
19. Click **OK**.



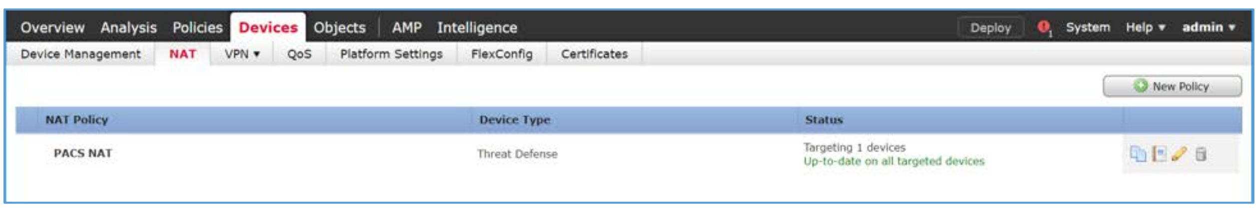
20. Ensure the new server is shown in the **DHCP Server** list.

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

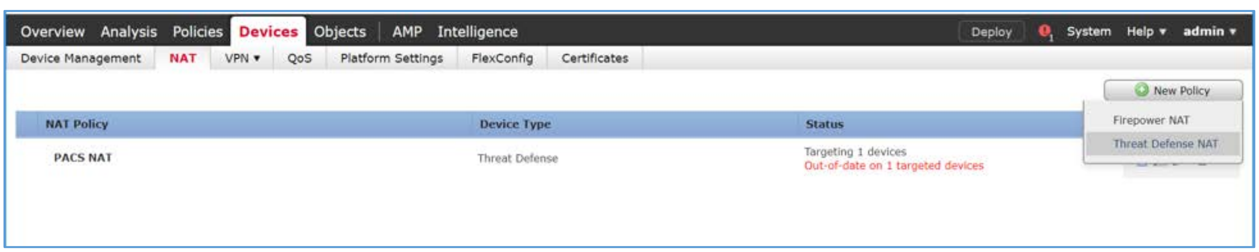


Network Address Translation (NAT) Rules Configuration

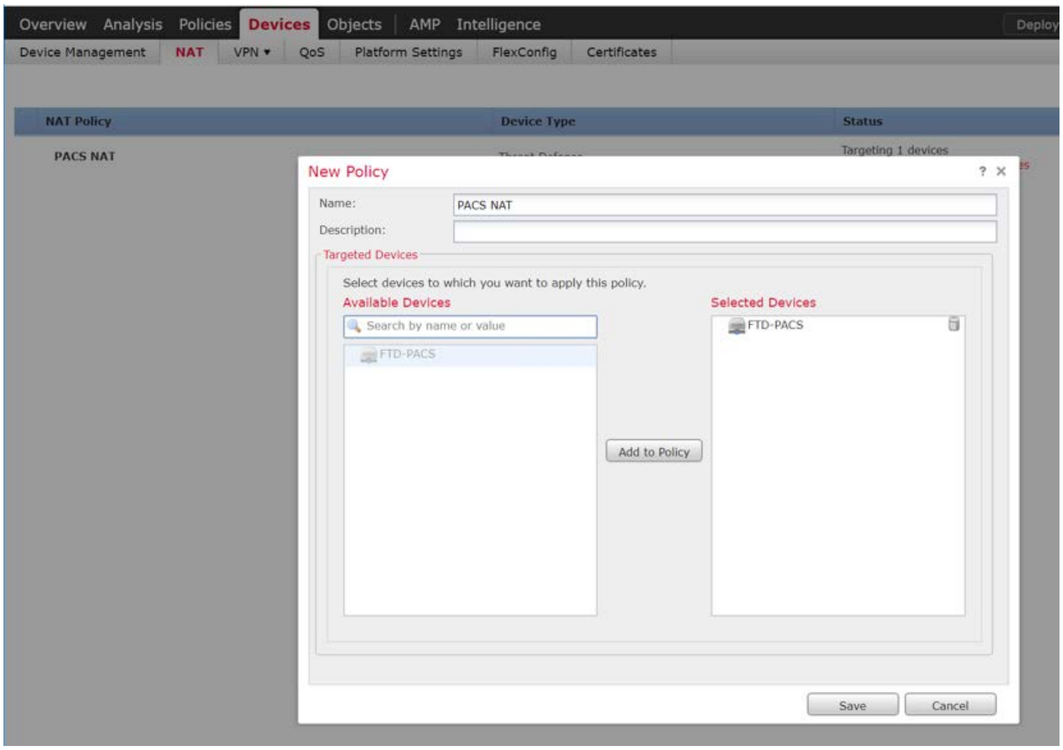
1. Navigate to **Devices** > **NAT**.



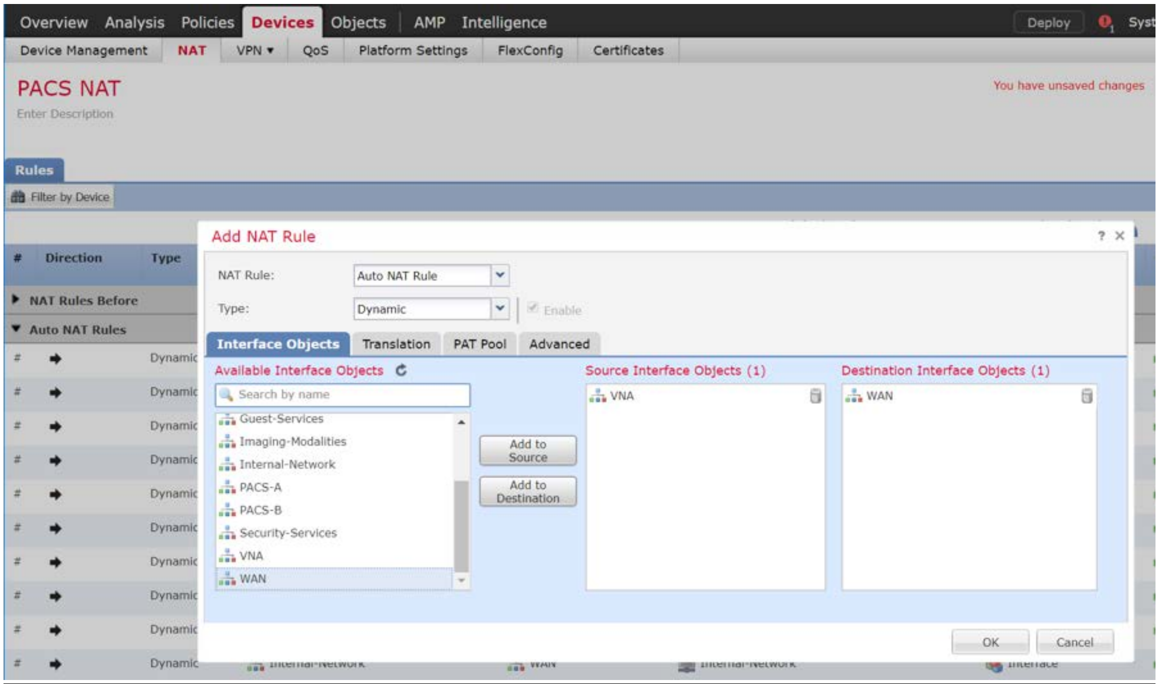
2. Click **New Policy > Threat Defense NAT**.



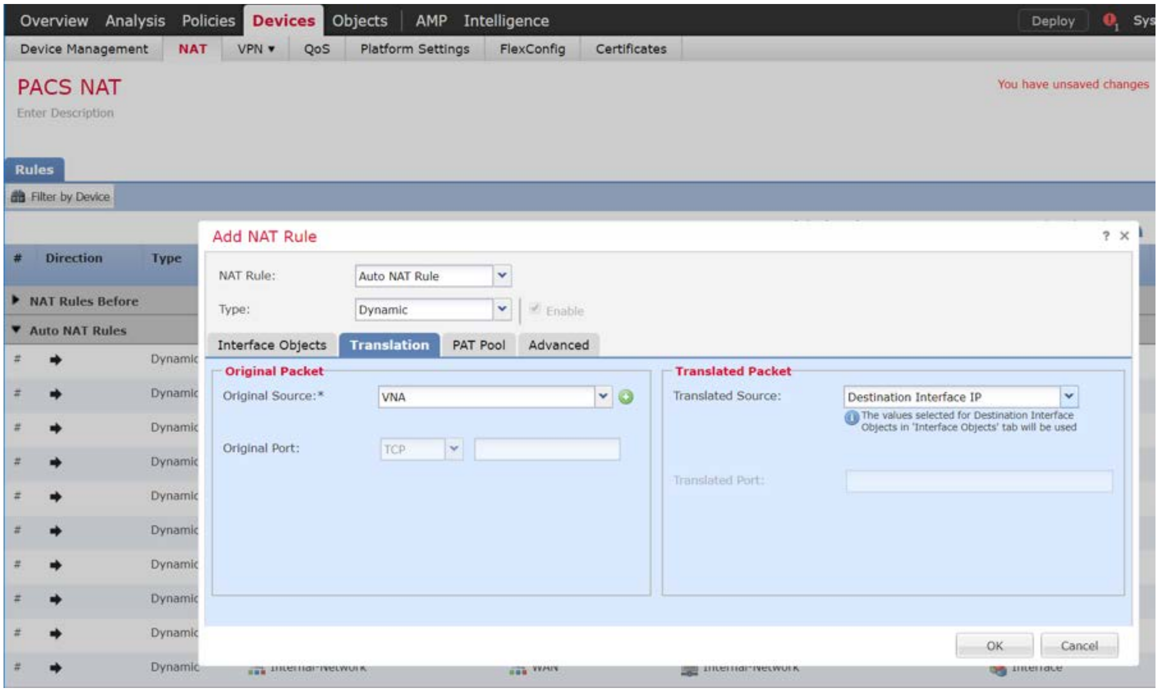
3. Give the new policy a **Name** as **PACS NAT**.
4. Assign the **FTD appliance** to the new NAT policy.
5. Click **Save**.



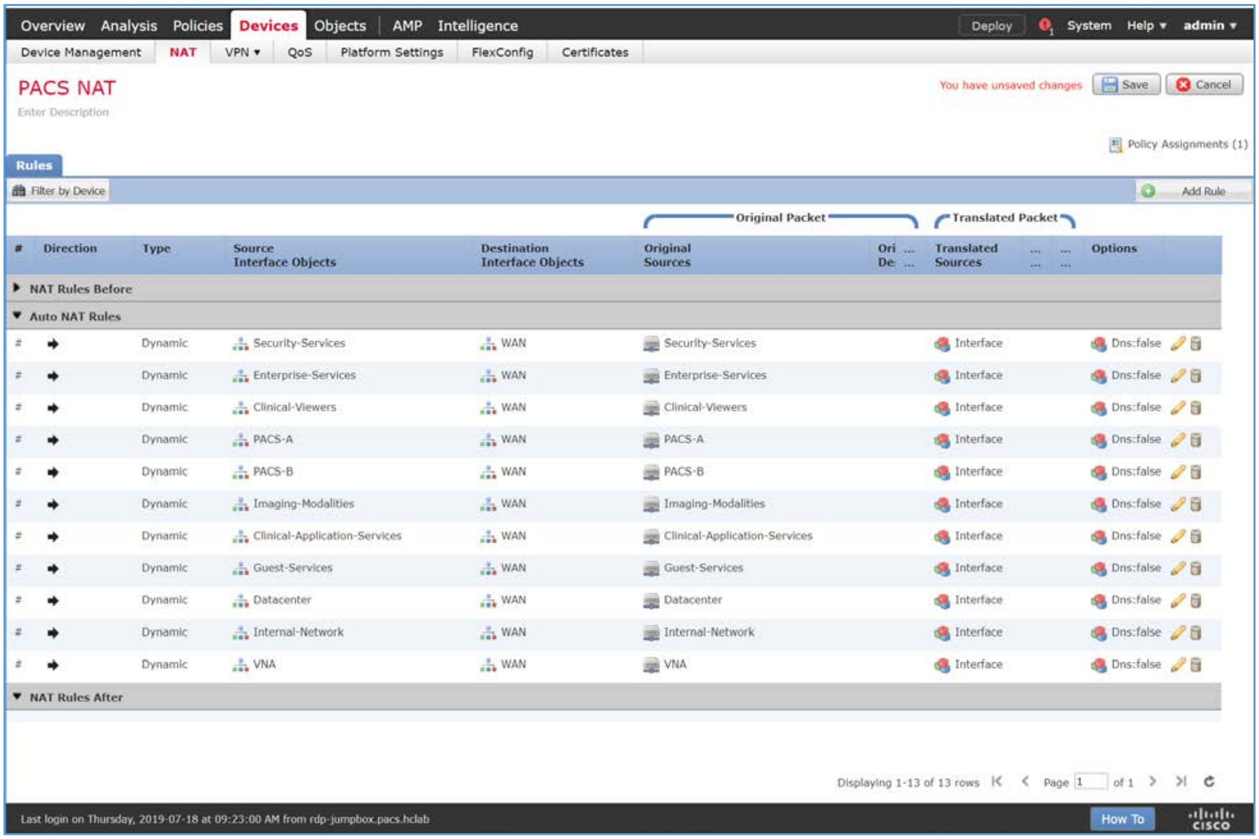
6. Click on the NAT policy's **edit** icon.
7. Click **Add Rule**.
8. Set **NAT Rule** to **Auto NAT Rule**.
9. Set **Type** to **Dynamic**.
10. Under **Interface Objects** set **Source Interface Object** to one of the FTD appliance's **LAN interfaces**.
11. Set **Destination Interface Object** to the 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 the new **NAT Rule** has been created.
16. Repeat these steps if needed for each **LAN interface** attached to FTD appliance.
17. Click **Save**.
18. **Deploy** changes to FTD appliance.

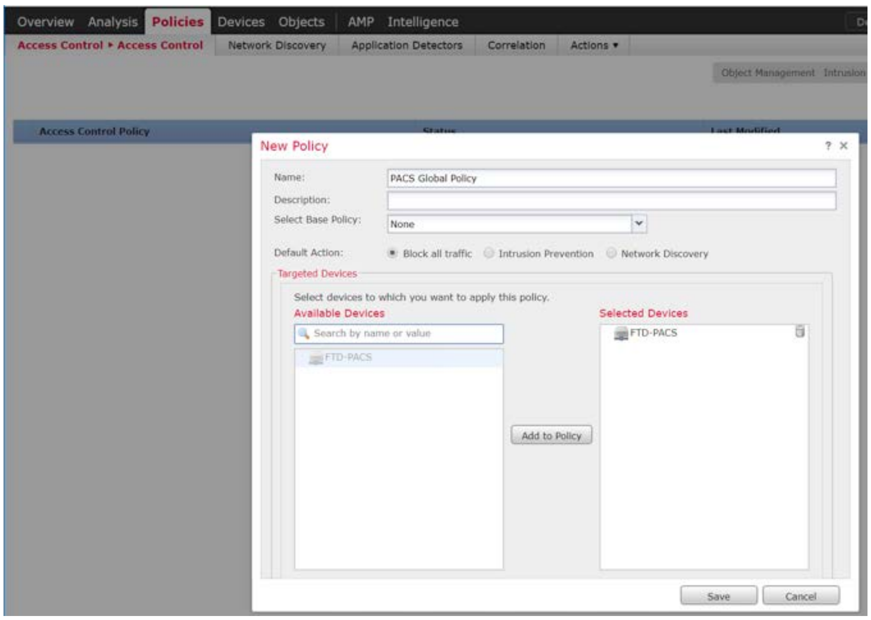


Access Control Policy Through Firepower Management Center Configuration

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

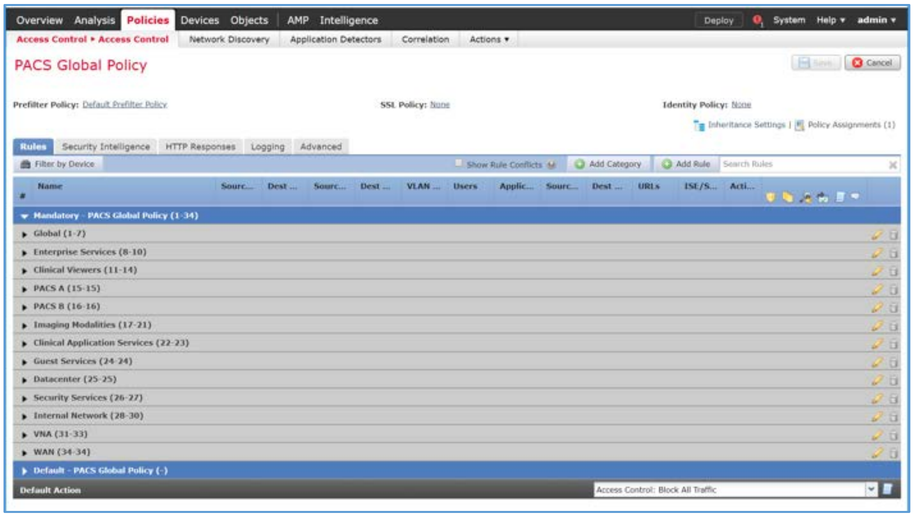
1. Navigate to **Policies > Access Control > Access Control**.

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



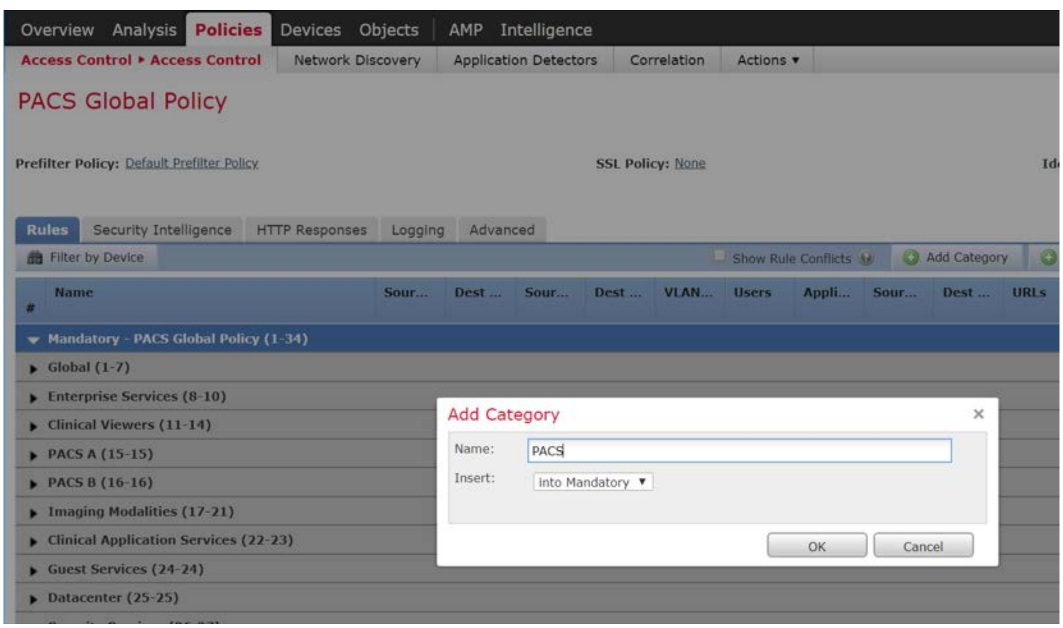
8. Click the access-control policy’s **edit** icon.

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



Creating a category:

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



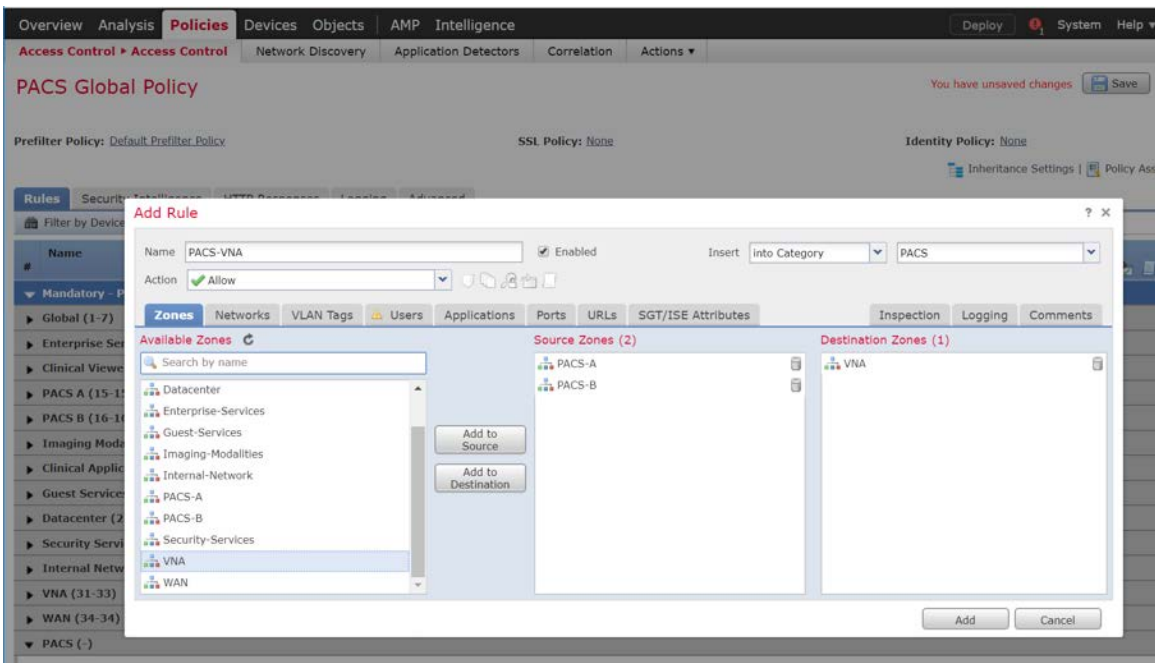
Create a rule that allows application traffic between security zones

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

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

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

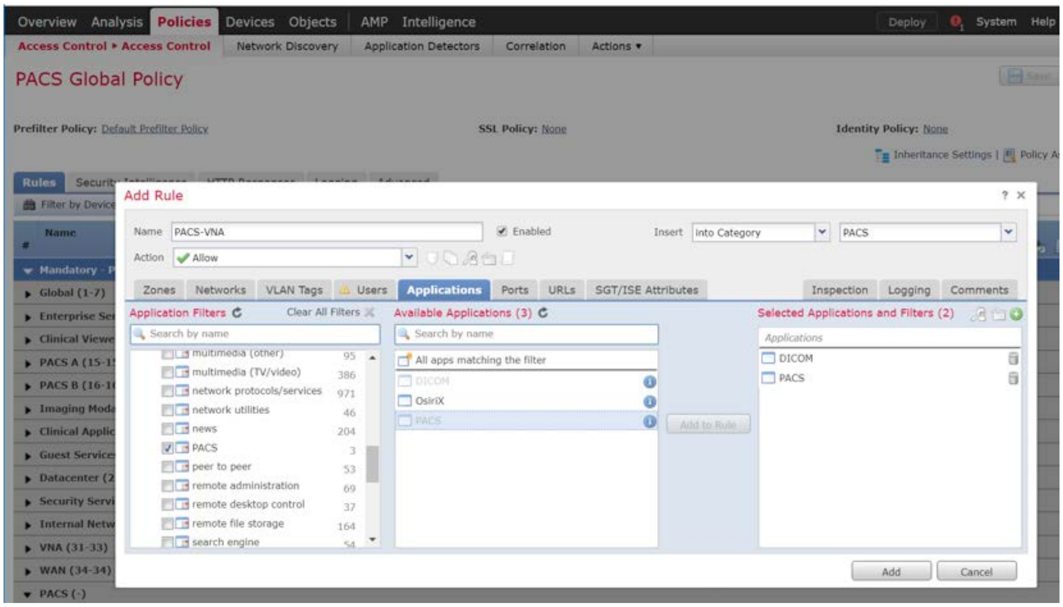
   Note: The two primary methods for adding source and destination networks to an access control rule are through security zones or networks. Security zones are objects that can contain multiple FTD interfaces. Networks can be different types of network objects, including network segments (**192.168.1.0/24**)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



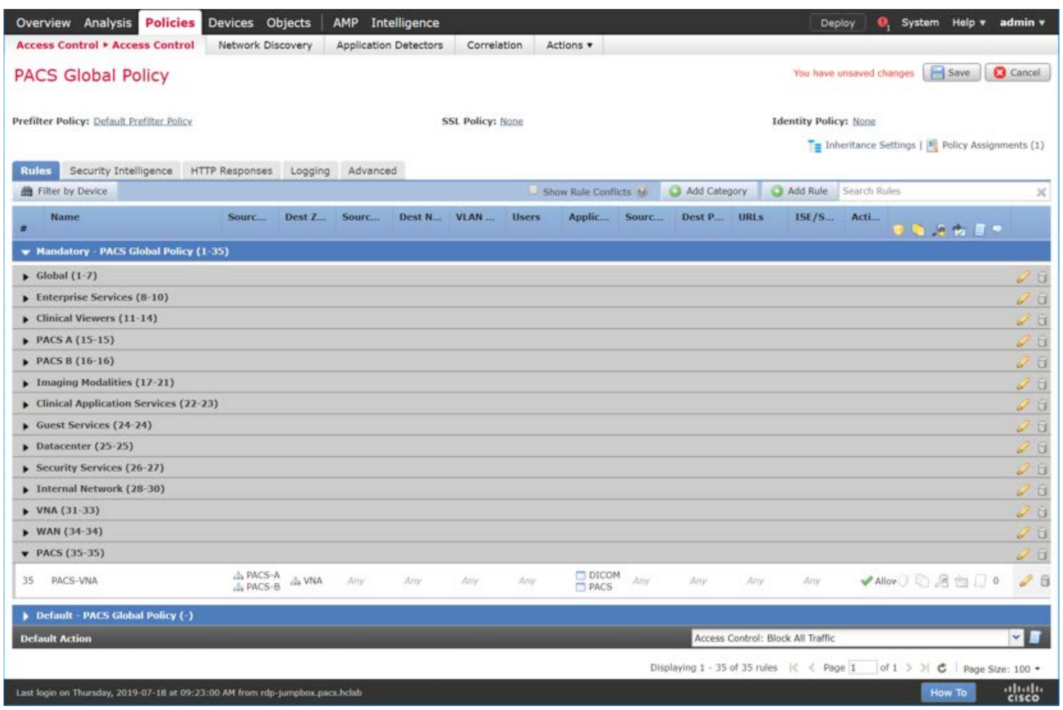
6. Under **Applications**, add the application(s) you would like to **allow** between the specified zones.

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

7. Click **Add**.



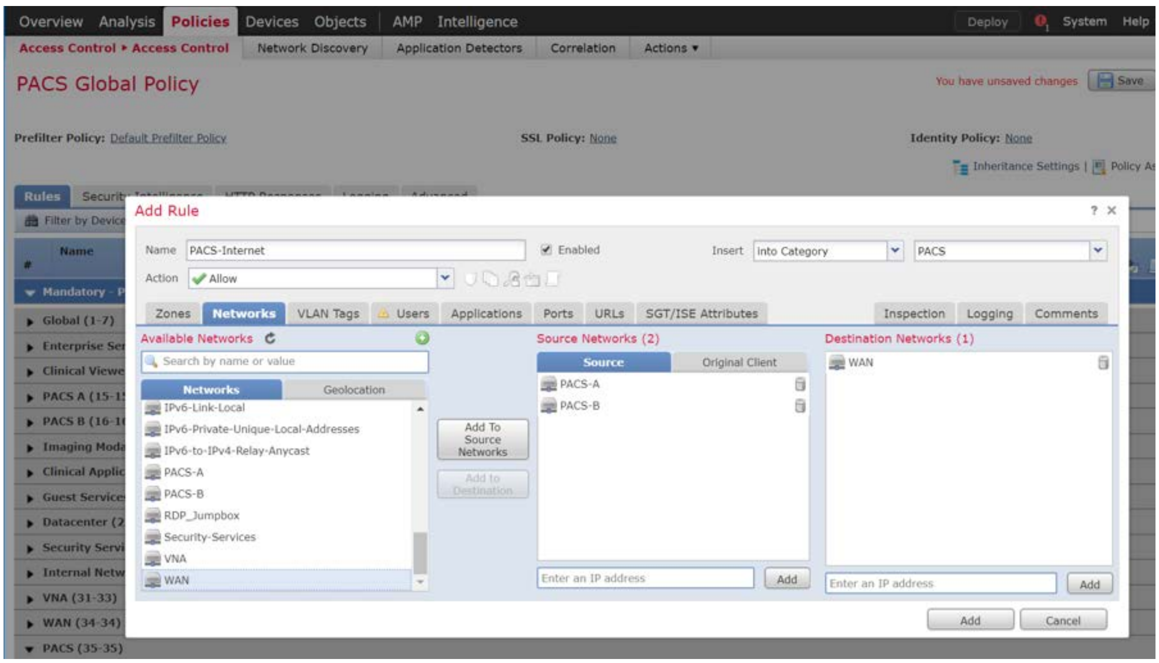
8. Verify that the **rule** has been created.



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

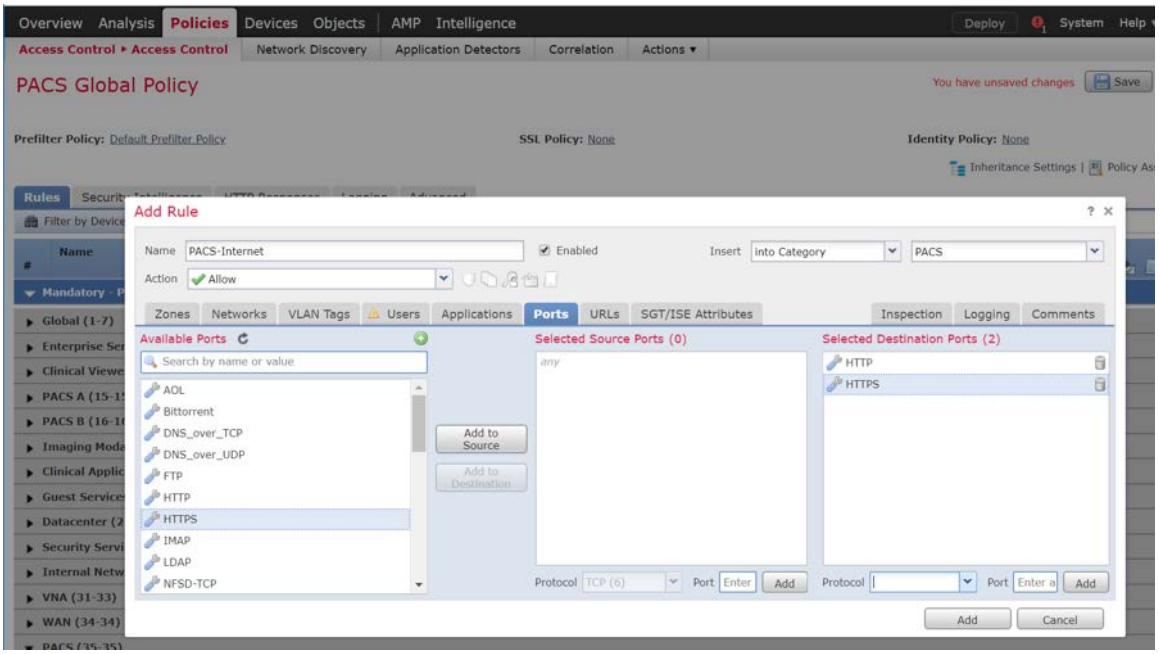
1. Click **Add Rule**.

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)**.



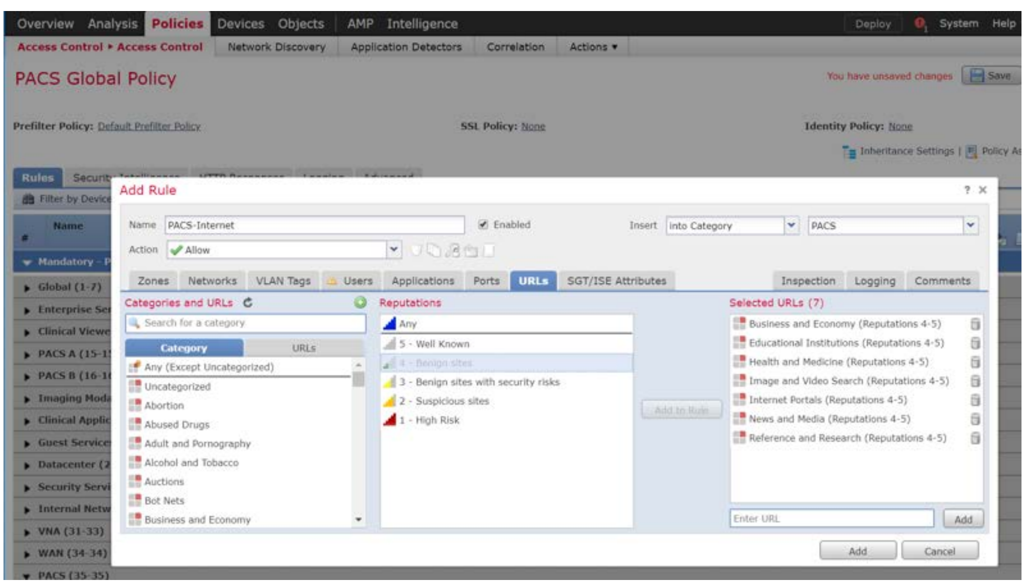
6. Under **Ports**, add a port(s) to the **Selected Destination Ports**.

   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.



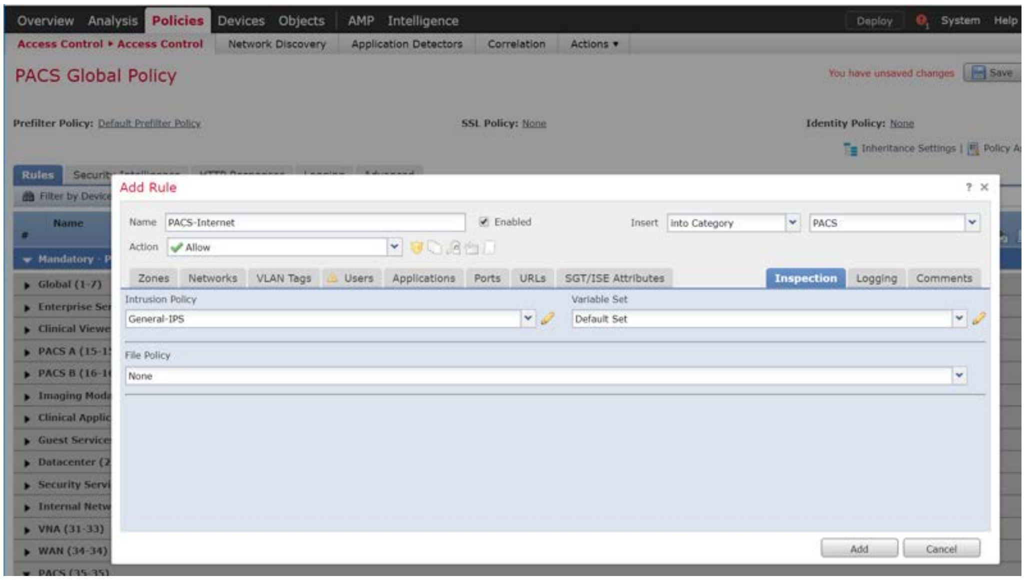
7. Under **URLs**, add **URL categories** that will be allowed (or leave this section blank).

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



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

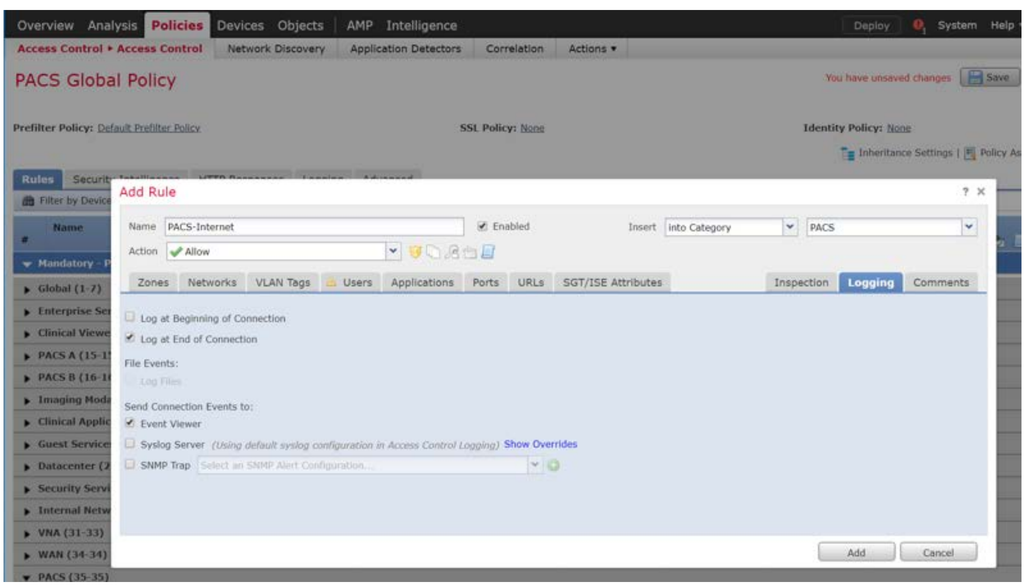
Note: Intrusion policies are created separately from the access-control policy. Once created, an intrusion policy can be applied to a specific access-control rule or an entire access-control policy. See the link posted [17] at the beginning of this section for more information on how to create and use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



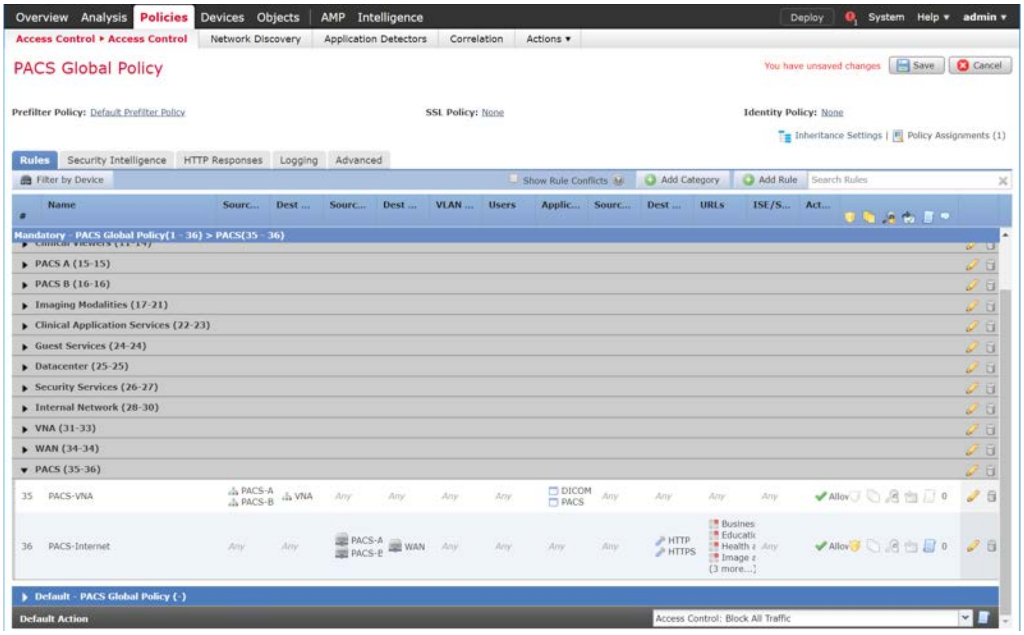
9. Under **Logging**, select **Log at End of Connection**, or leave this section blank.

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

10. Click **Add**.



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



2.7.2 Cisco Stealthwatch

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

Cisco Stealthwatch Management Console Appliance Information

CPU: 3

RAM: 16 GB

Storage: 60 GB (Thin Provision)

Network Adapter 1: VLAN 1901

Operating System: Linux

Cisco Stealthwatch Management Console Virtual Edition Installation Guide

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

Cisco Stealthwatch UDP Director Appliance Information

CPU: 1

RAM: 4 GB

Storage: 60 GB (Thin Provision)

Network Adapter 1: VLAN 1901

Network Adapter 2: VLAN 1901

Operating System: Linux

Cisco Stealthwatch UDP Director Virtual Edition Installation Guide

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

Cisco Stealthwatch Flow Collector Appliance Information

CPU: 2

RAM: 16 GB

Storage: 60 GB (Thin Provision)

Network Adapter 1: VLAN 1901

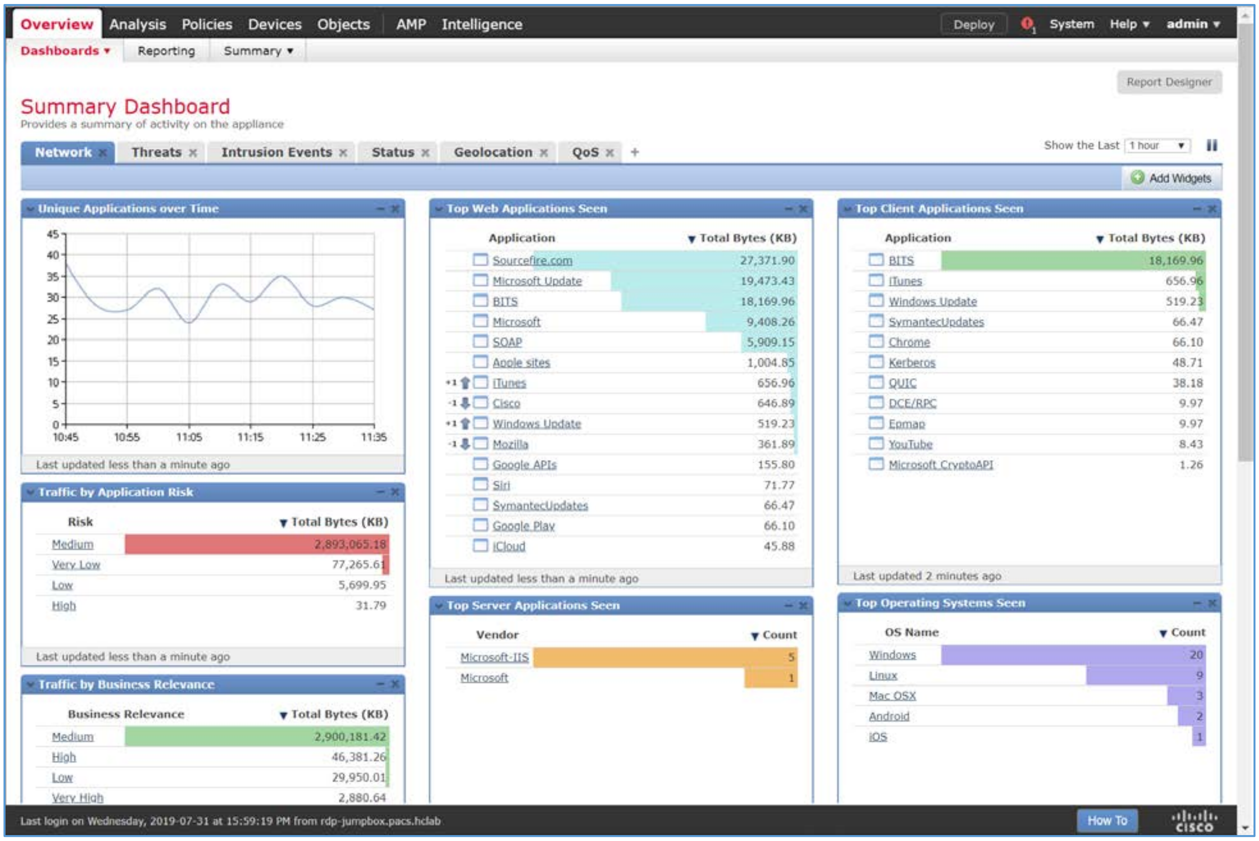
Operating System: Linux

Cisco Stealthwatch Flow Collector Virtual Edition Installation Guide

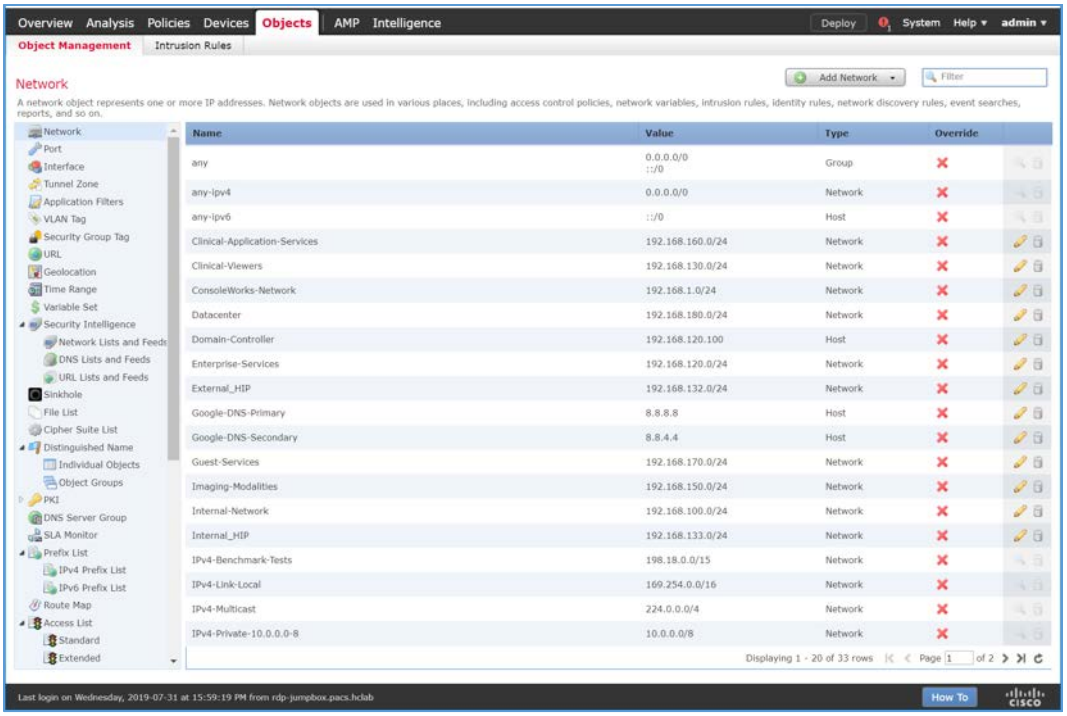
Install the Cisco Stealthwatch Flow Collector appliance according to the instructions provided at the Cisco installation guide [18].

Configure NetFlow Parameters for Cisco Firepower

1. Log in to the Cisco Firepower Management Console.

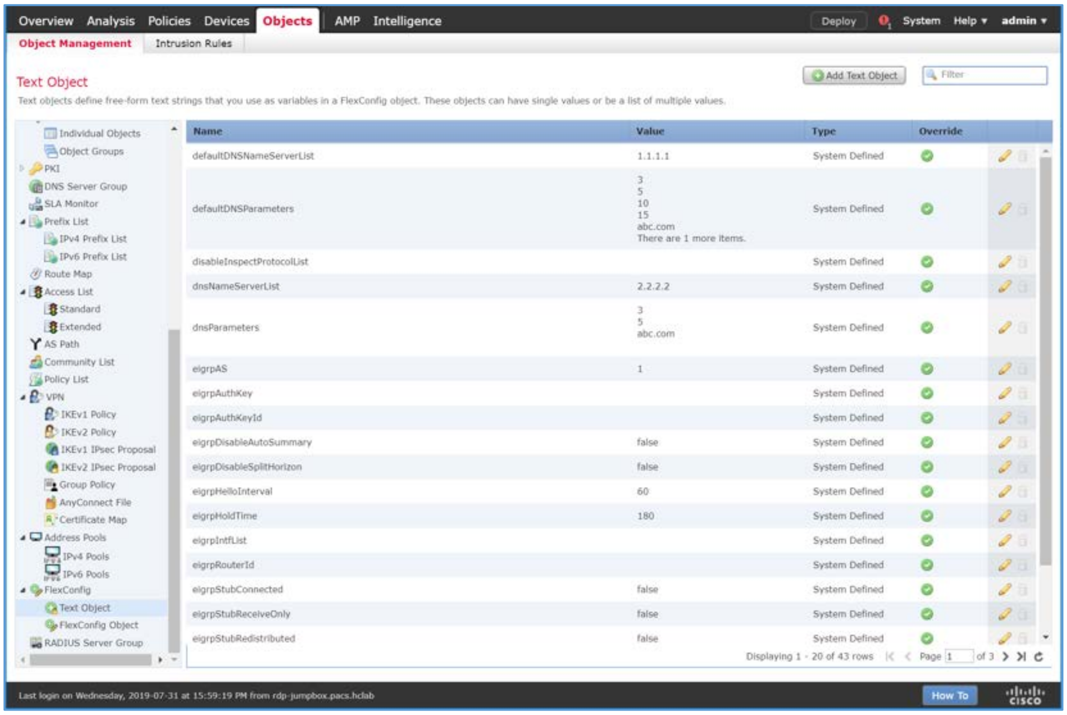


2. Navigate to **Objects**.



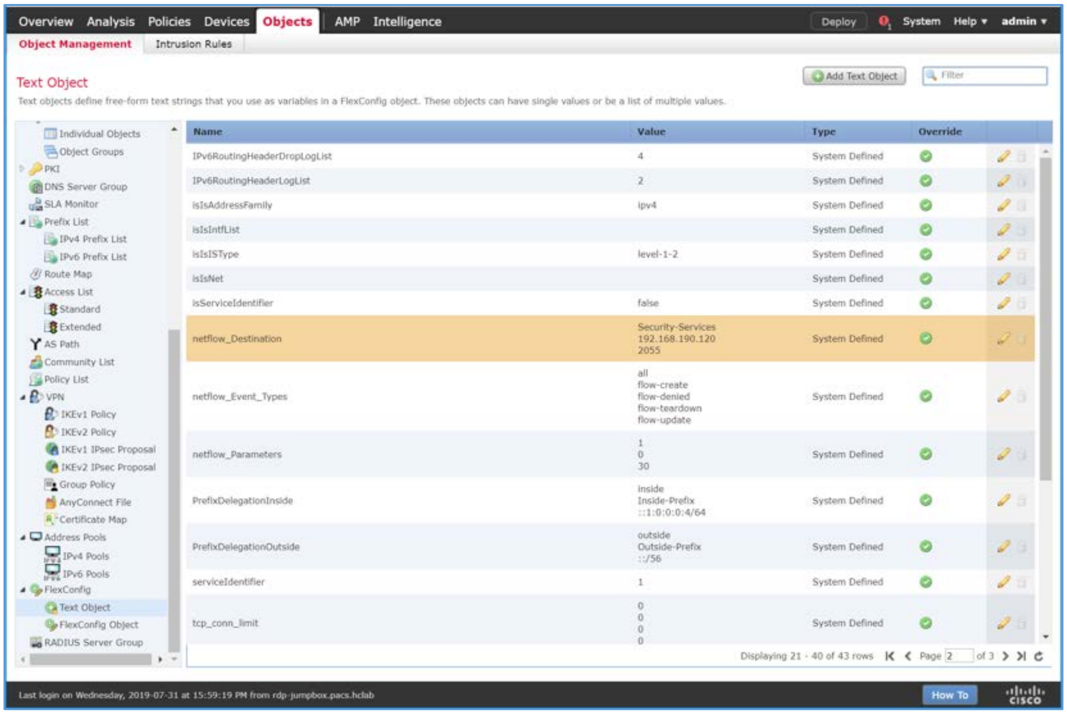
1690

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

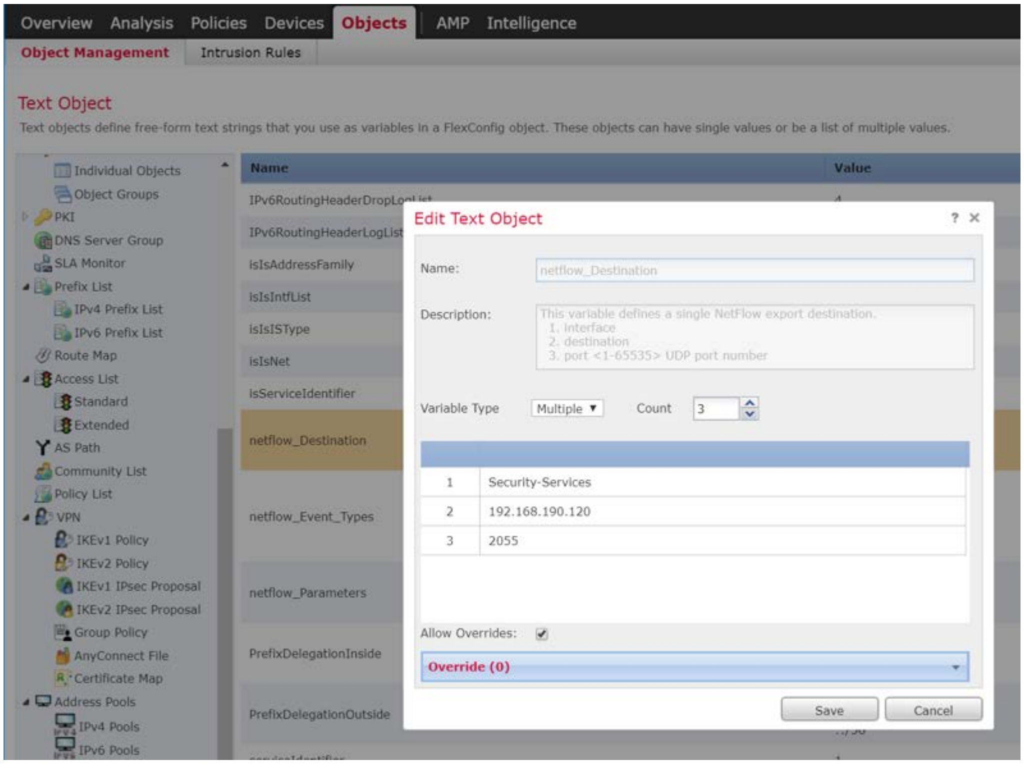


1692

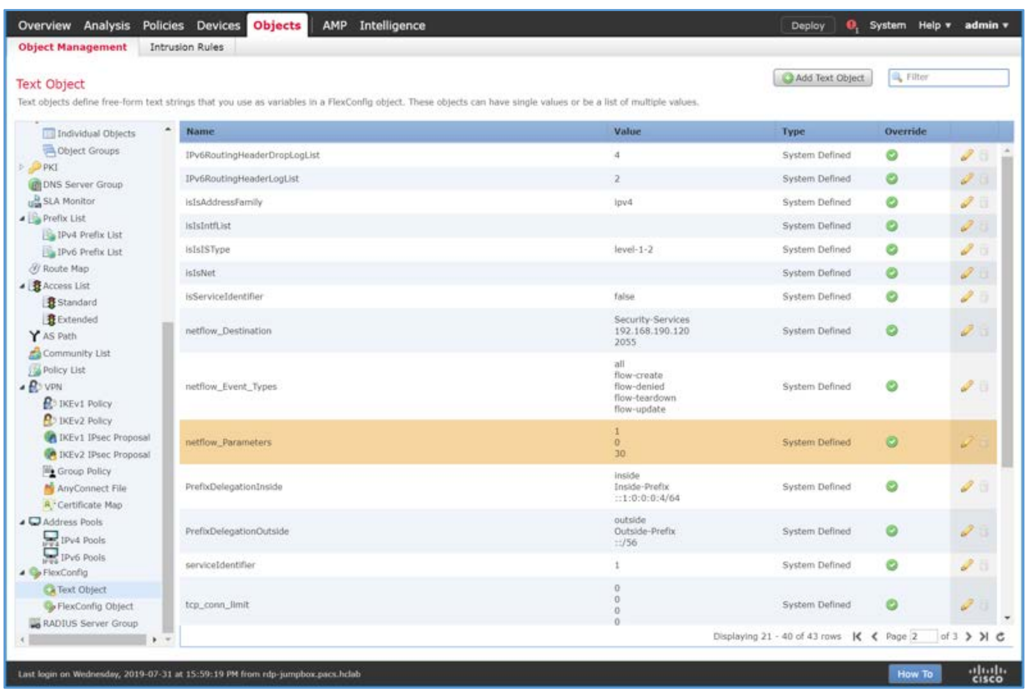
4. Under the **Name** column, find **netflow_Destination**.



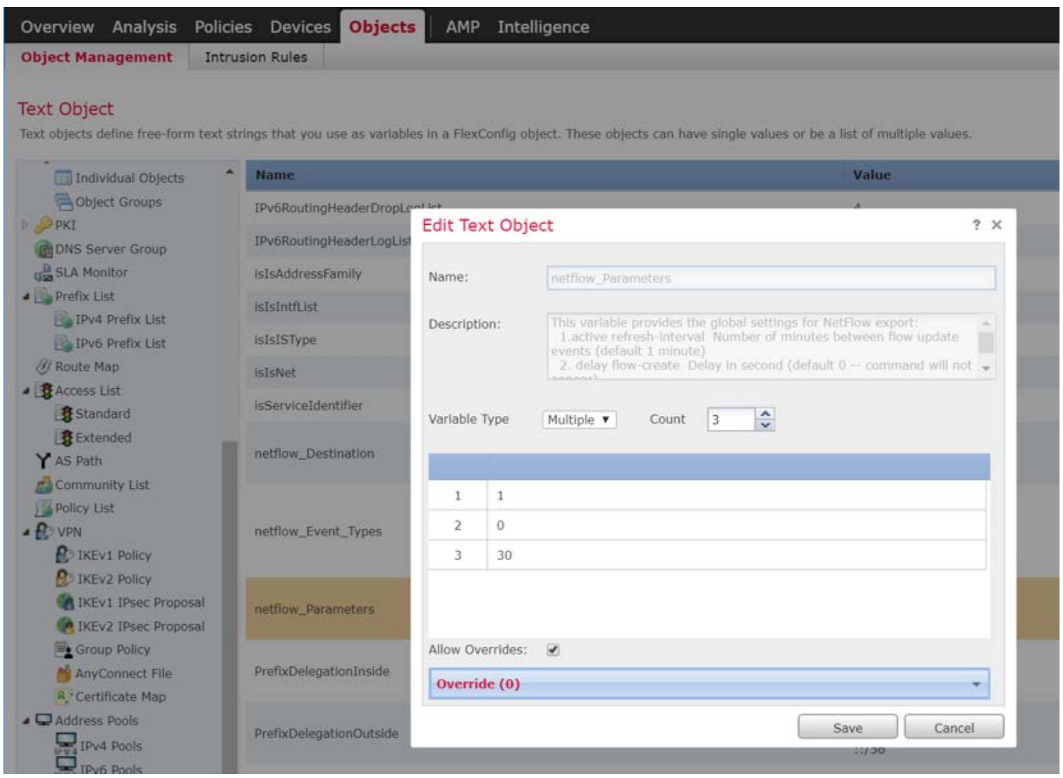
5. Click the **edit** icon for **netflow_Destination**.
6. Set **Variable Type** to **Multiple**.
7. Set **Count** to **3**.
8. For **Row 1**, enter **Security-Service** to set the name of the Cisco FTD interface to which the Cisco Stealthwatch UDP appliance is connected.
9. For **Row 2**, enter **192.168.190.120**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



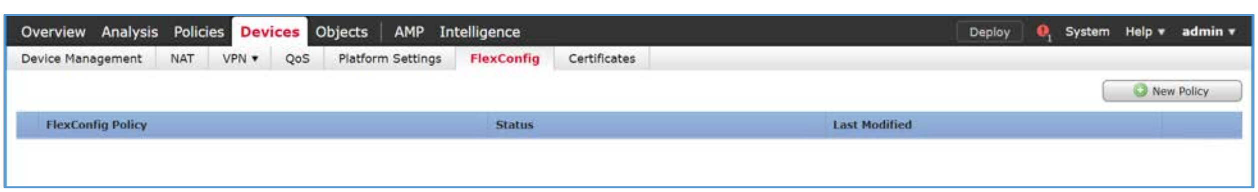
12. Under the **Name** column, find **netflow_Parameters**.



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 timeout rate.
19. Click **Save**.

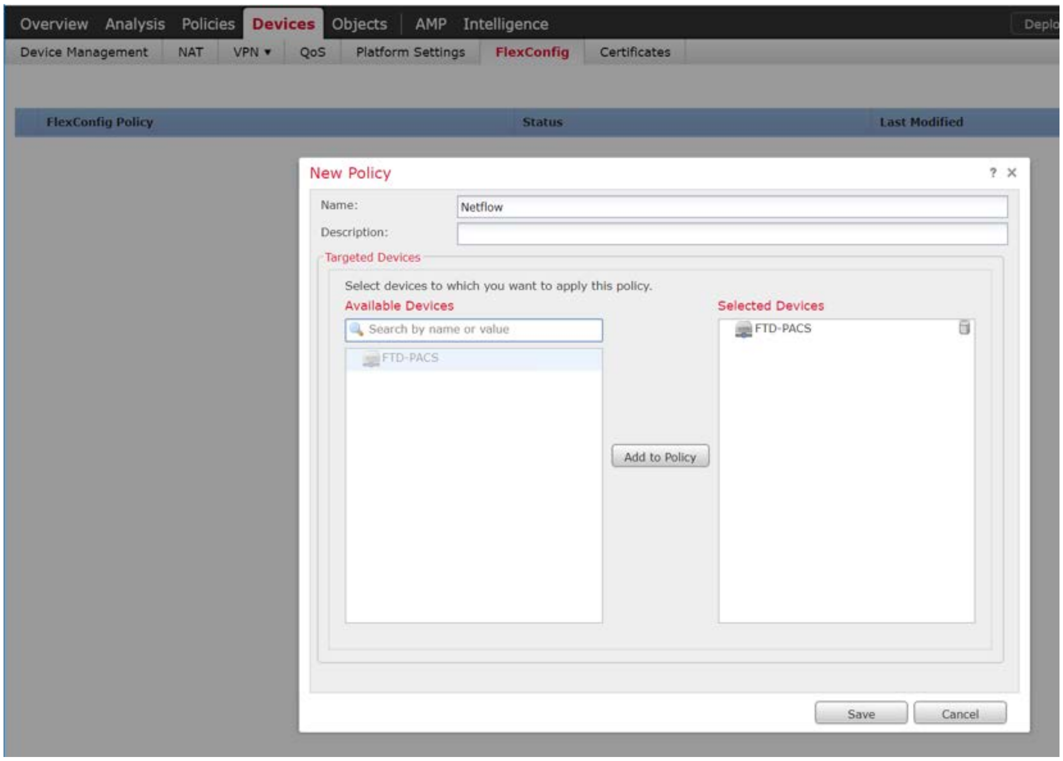


20. Navigate to **Devices > FlexConfig**.

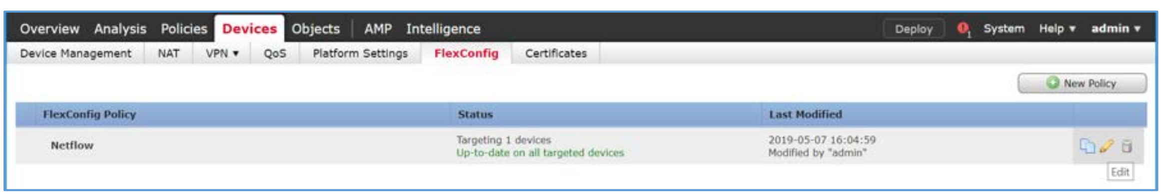


21. Click **New Policy**.

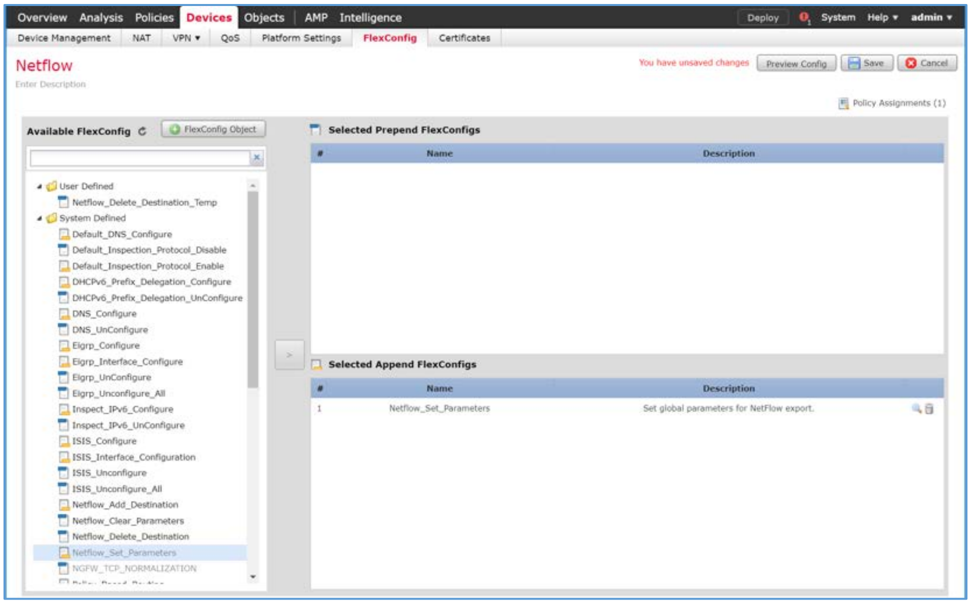
22. Enter a **Name** (e.g., **Netflow**) for the policy.
23. Under **Selected Devices**, add the Cisco FTD.
24. Click **Save**.



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



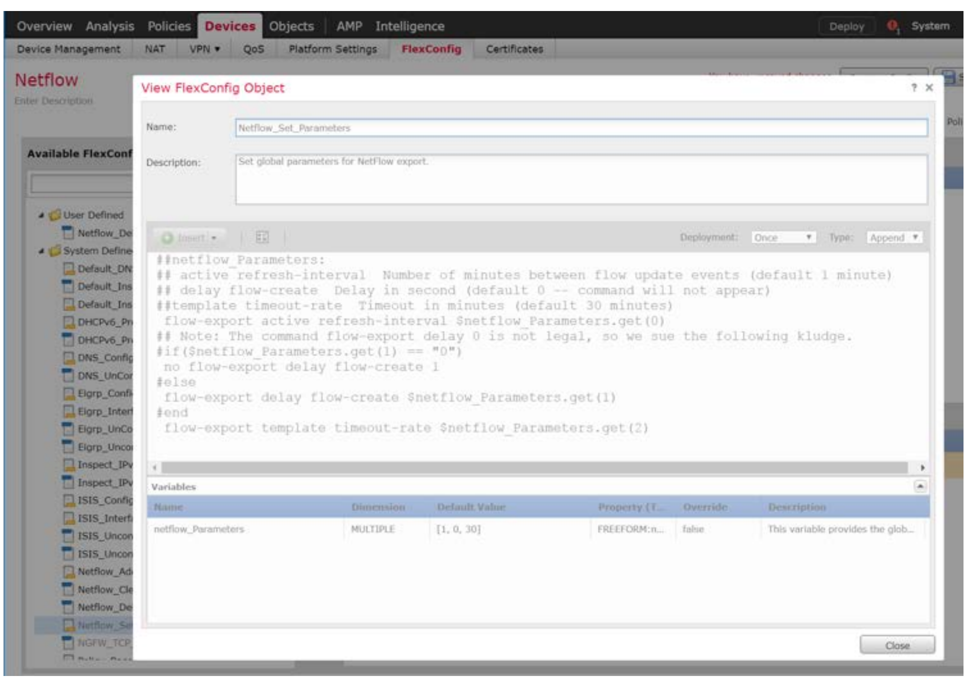
26. Under **Available FlexConfig**, find **Netflow_Set_Parameters**, and add it to **Selected Append FlexConfigs**.



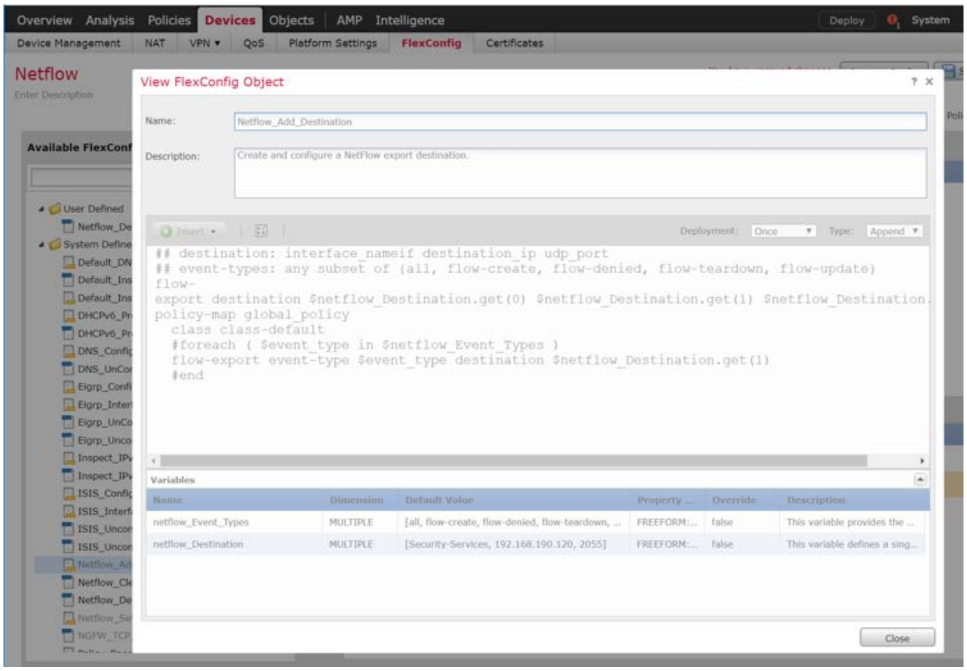
27. Click the **magnifier** icon for **Netflow_Set_Parameters**.

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

29. Click **Close**.



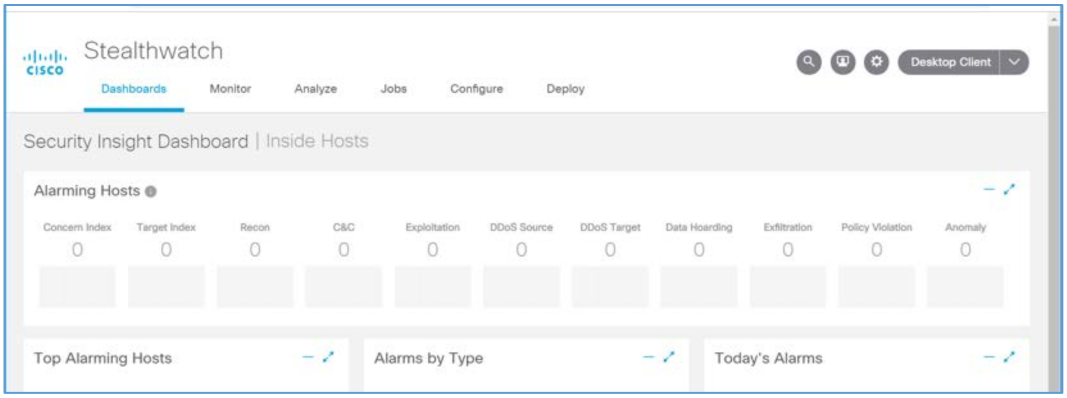
30. Under **Available FlexConfig**, find **Netflow_Add_Destination,** and add it to **Selected Append FlexConfigs**.
31. Click the **magnifier** icon for **Netflow_Add_Destination**.
32. Under **Variables > Default Value**, verify the Cisco FTD interface name, IP address of the Cisco Stealthwatch, and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



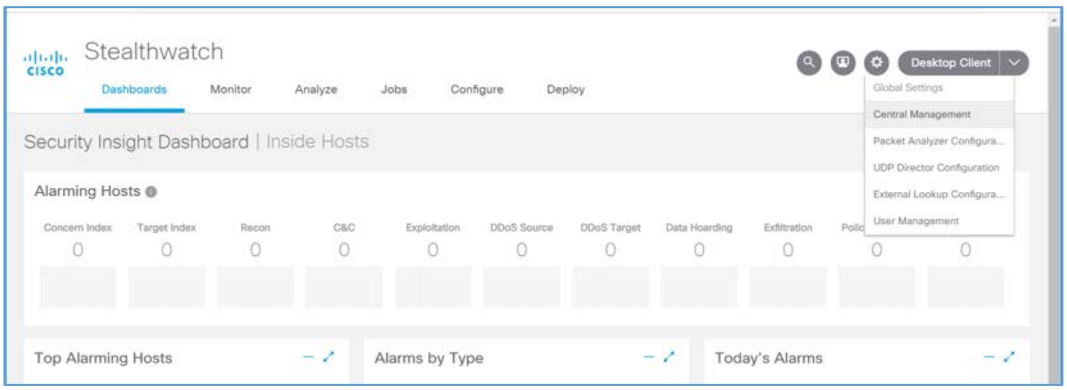
34. Click **Save**.
35. Deploy changes to the Cisco FTD.

Forwarding Rules for Cisco Stealthwatch UDP Configuration

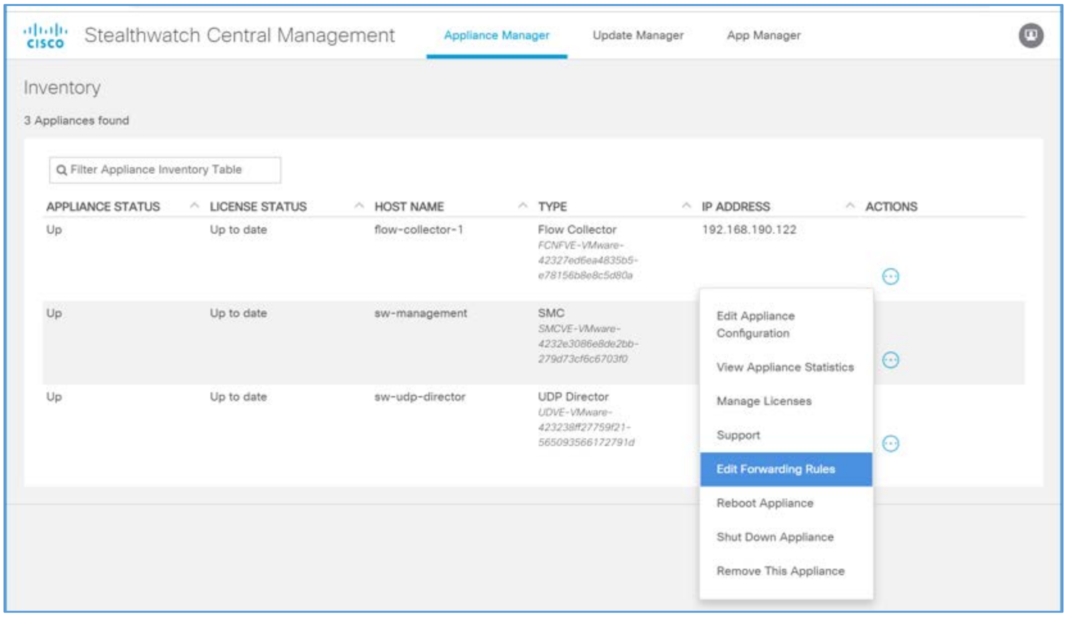
1. Log in to the web dashboard of the Cisco Stealthwatch Management Console.



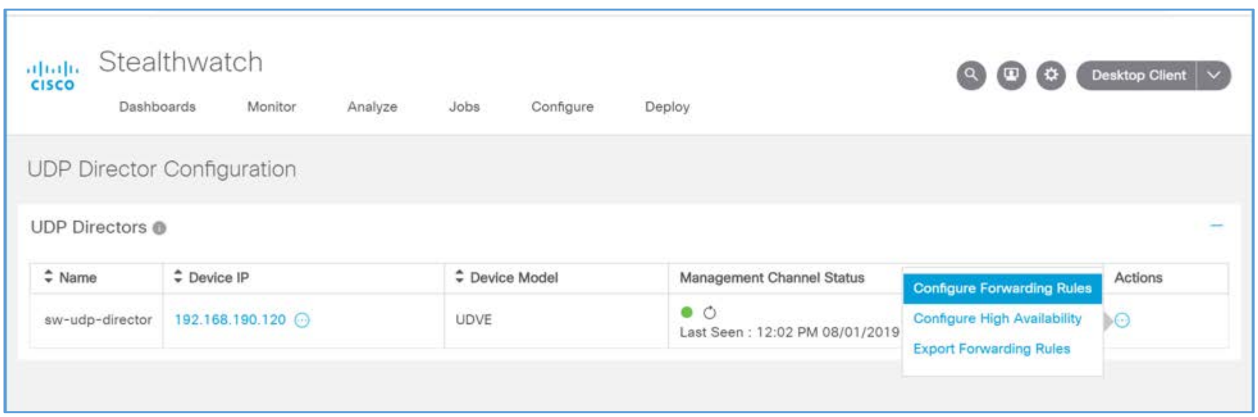
2. Navigate to **Settings** > **Central Management**.



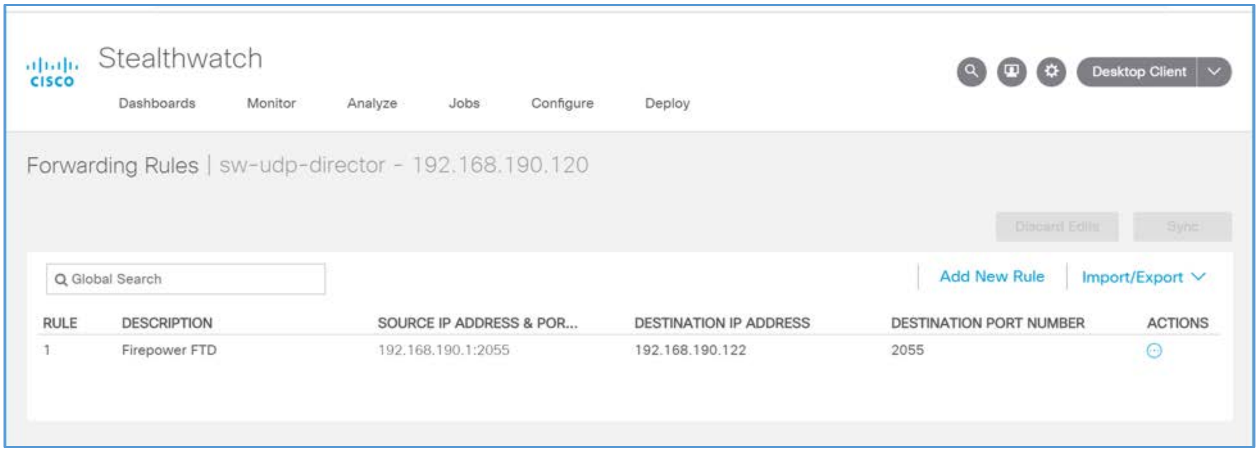
3. Click on the **ellipsis** for the Cisco Stealthwatch UDP appliance and select **Edit Forwarding Rules**.



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



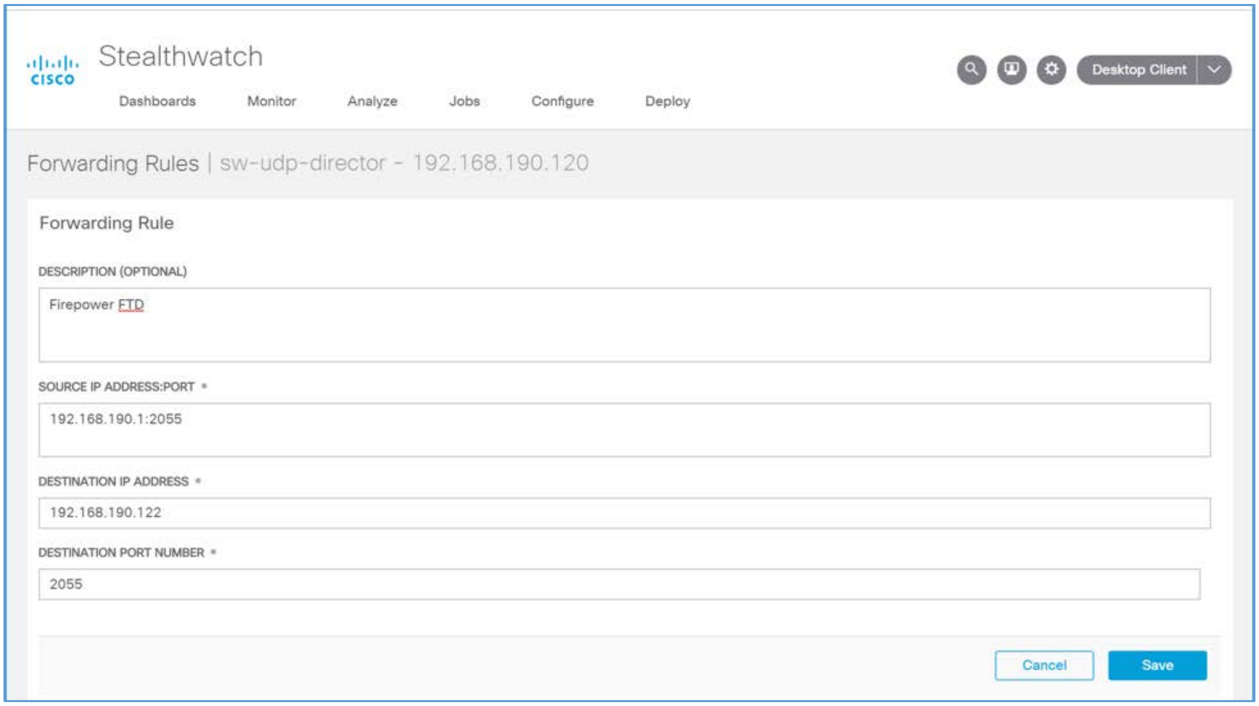
5. Under **Forwarding Rules**, select **Add New Rule**.



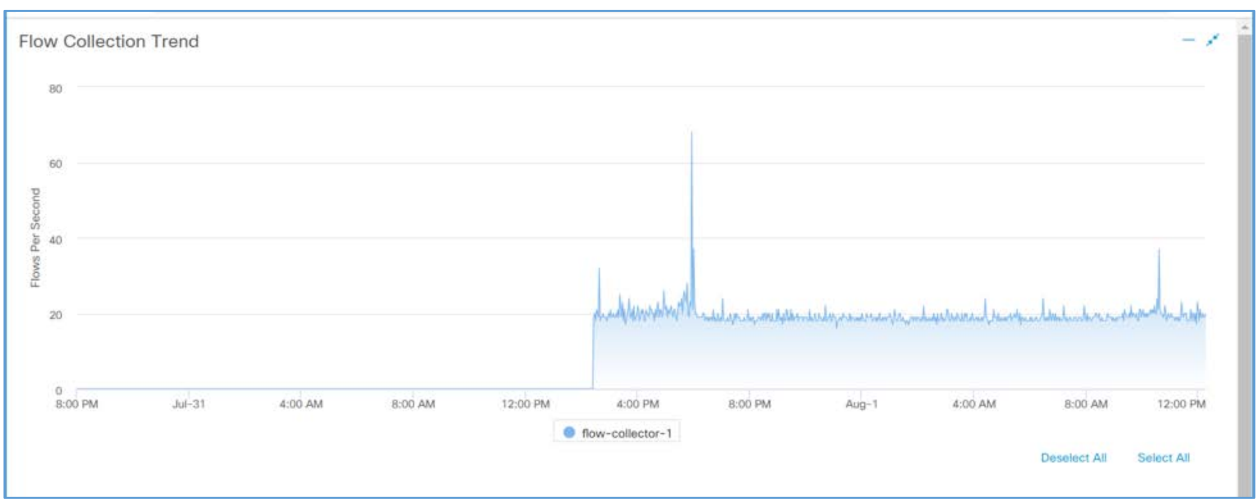
6. Enter a description (e.g., **Firepower FTD**) for the rule.
7. For **source IP address** and **source port**, enter the IP address, and port (e.g., **192.168.190.1:2055**) of the Cisco FTD interface sending the NetFlow traffic.

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

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



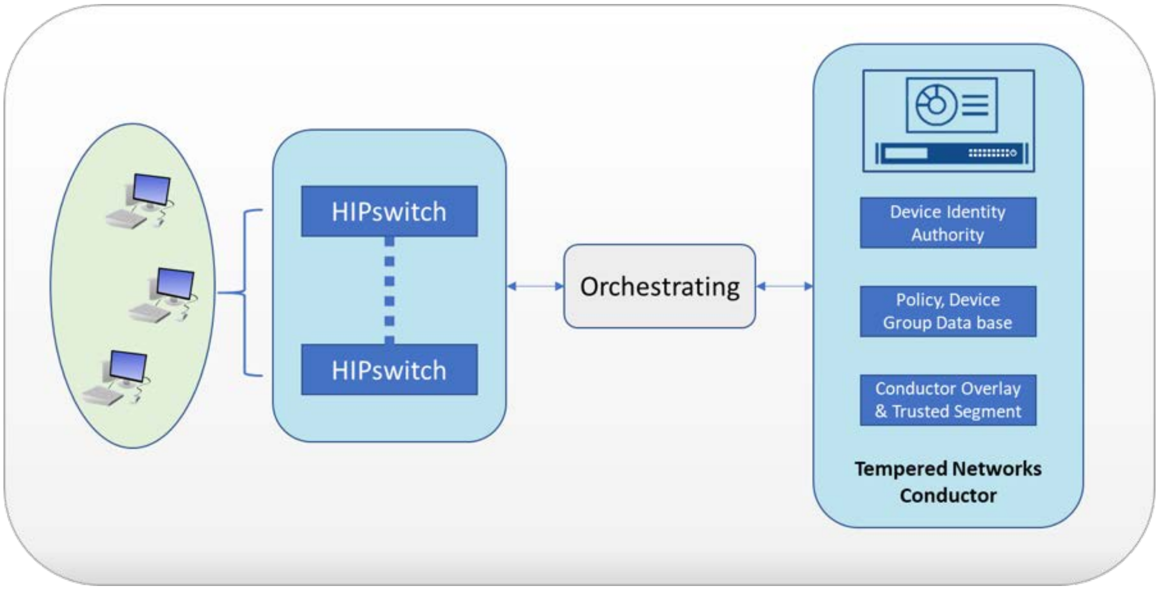
10. On the Cisco Stealthwatch Management Console dashboard, view the **Flow Collection Trend** graph to verify that the Cisco Stealthwatch Flow Collector is receiving packets from the Cisco Stealthwatch UDP.



2.7.3 Tempered Networks Identity Defined Networking (IDN)

Tempered Networks IDN provides cryptographically defined host identifiers using the HIP protocol rather than using IP addressing. Network traffic traverses an overlay network using HIP switches that effectively cloak that traffic from the production network. A notional architecture is depicted in Figure 2-2 below.

Figure 2-2 Architecture of Networks IDN



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

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

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

2.7.3.1 Conductor Installation

System Requirements

CPU: 4

Memory: 4 GB RAM

Storage: 120 GB

Operating System: Linux Red Hat

Network Adapter: VLAN 1201

Tempered Networks Conductor Installation

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

2.7.3.2 HIPswitch Installation

System Requirements

CPU: 4

Memory: 1 GB RAM

Storage: 1 GB

Operating System: Linux Red Hat

Network Adapter: VLAN 1201

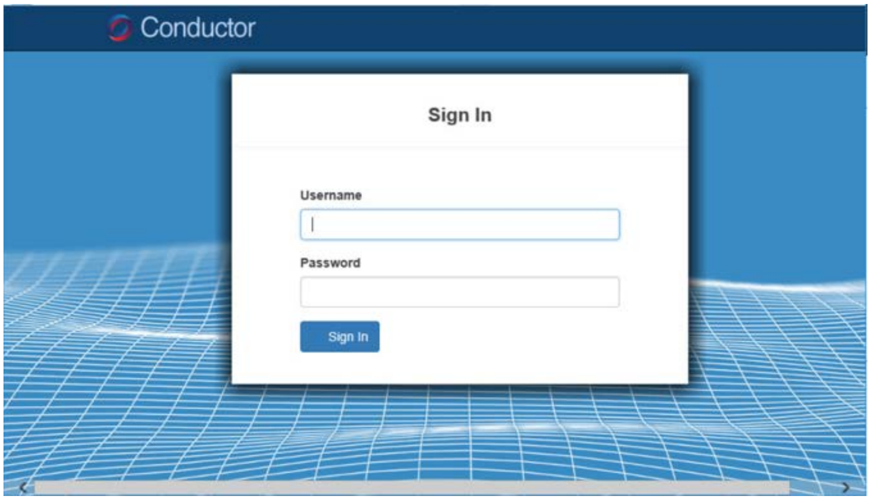
HIPswitch Installation

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

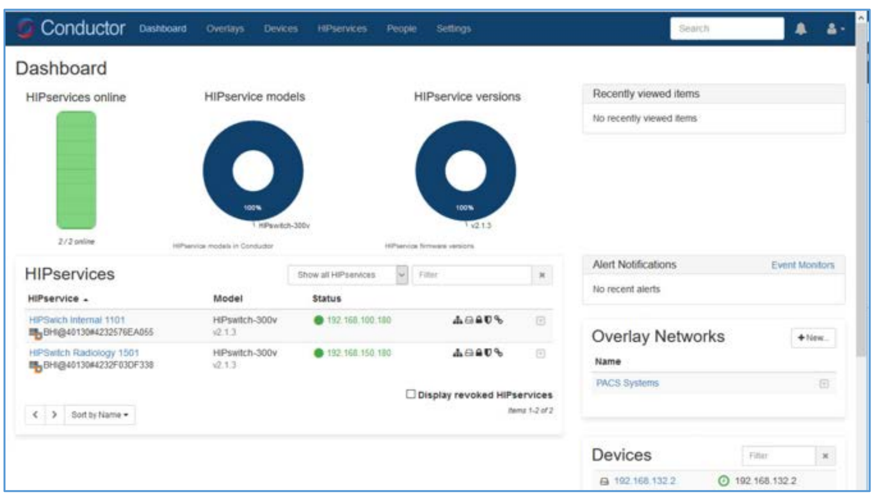
Tempered Networks Conductor and HIPswitch Configuration

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

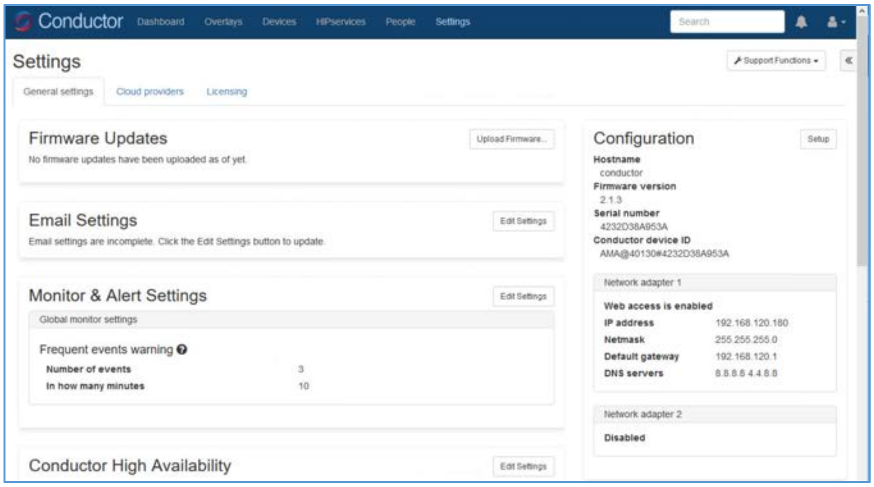
1. Enter the **username** and **password** to open the Dashboard.



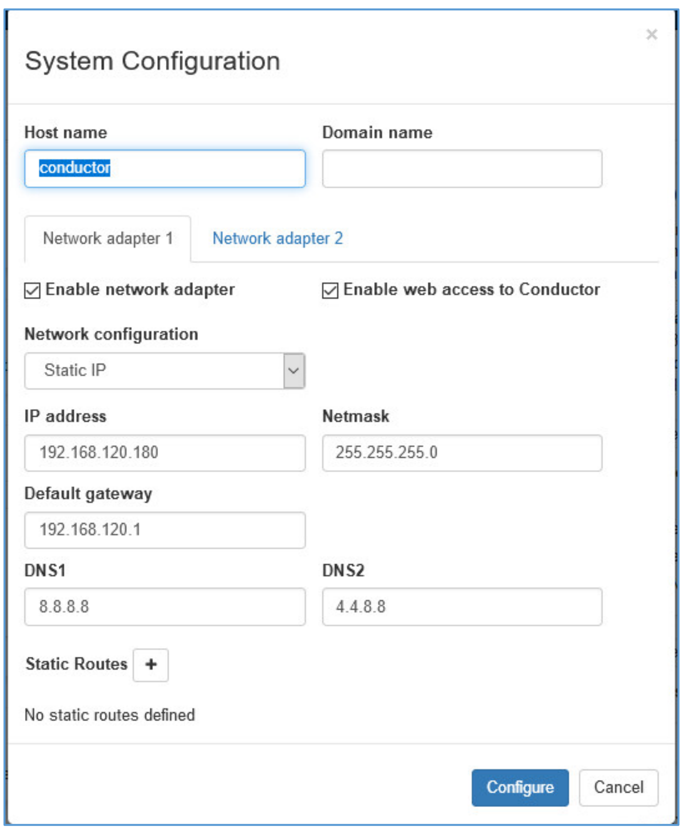
2. Click **Settings** tab.



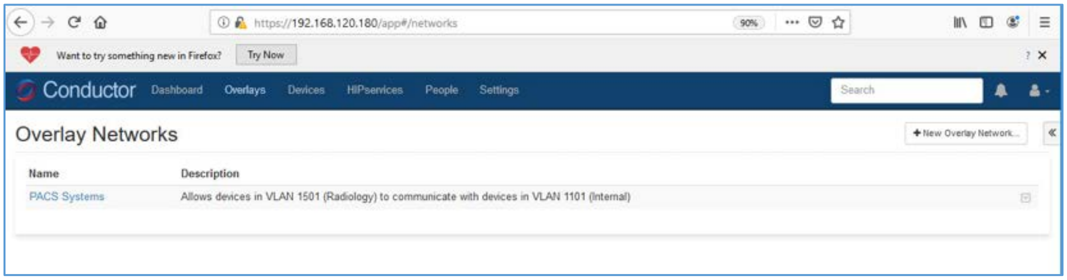
3. From this page, you can set up license and perform the system setup. Click the **Setup** button to enter the system setup.



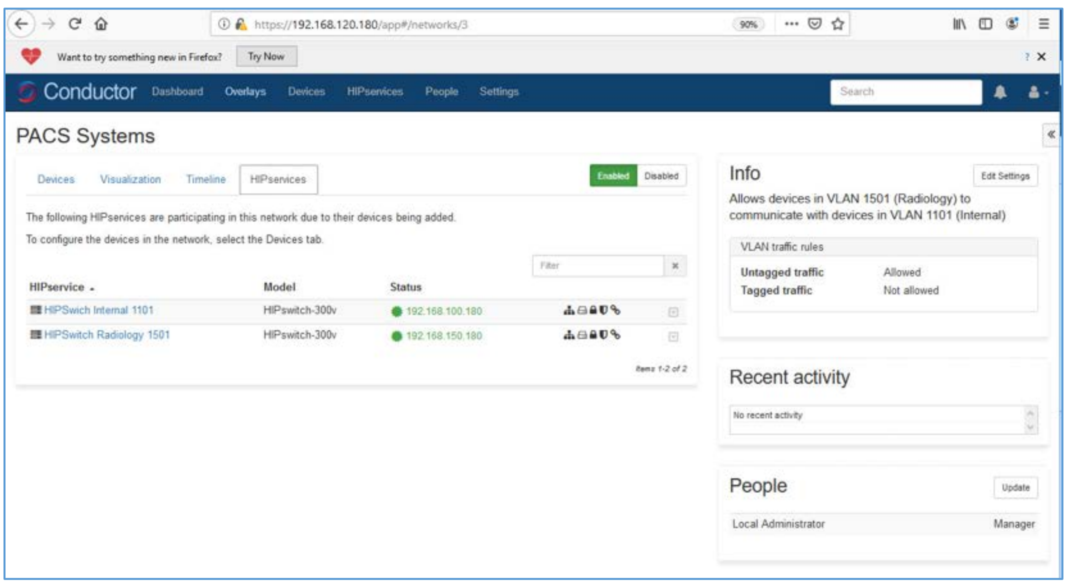
4. Enter the proper network parameters for the **Conductor,** including the **IP address** (e.g., **192.168.120.180**), **Netmask** (e.g., **255.255.255.0**), **Default gateway** (e.g., **192.168.120.1**), and **DNS** (e.g., **8.8.8.8**, **4.4.8.8**), then click **Configure**.



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



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



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

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

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

2.7.4 Zingbox IoT Guardian

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

Zingbox Cloud Setup

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

System Requirements

CPU: 4

Memory: 8 GB RAM

Storage: 256 GB (Thin Provision)

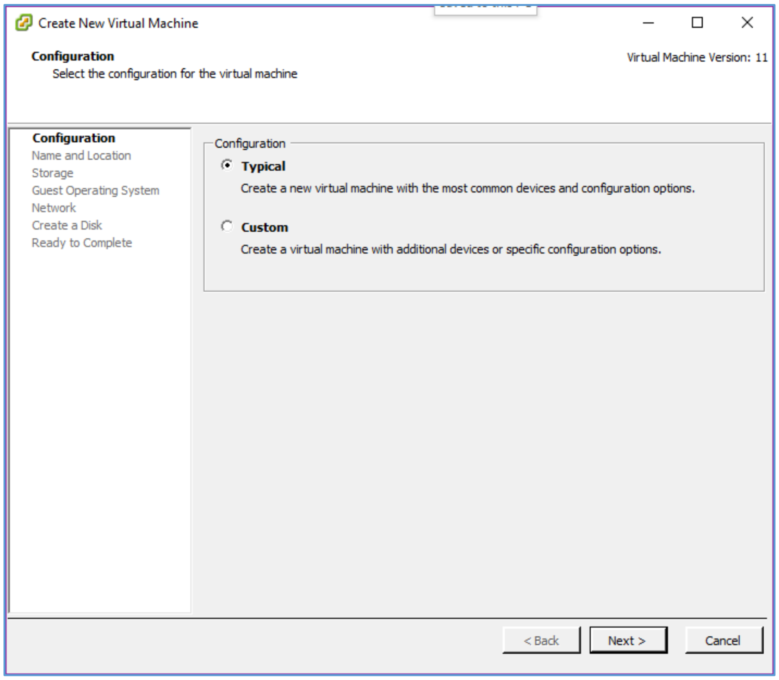
Operating System: CentOS 7

Network Adapter 1: VLAN 1101

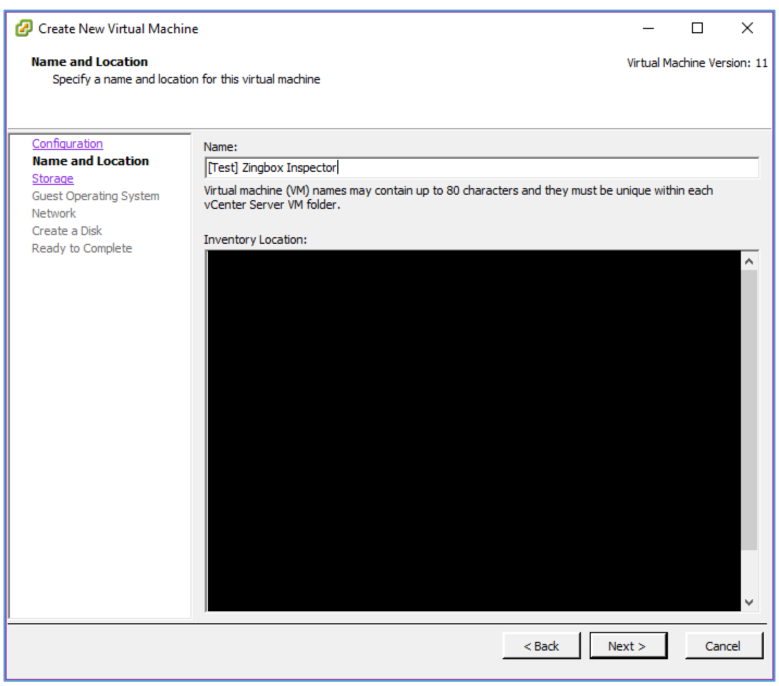
Network Adapter 2: Trunk Port

Zingbox Inspector Installation

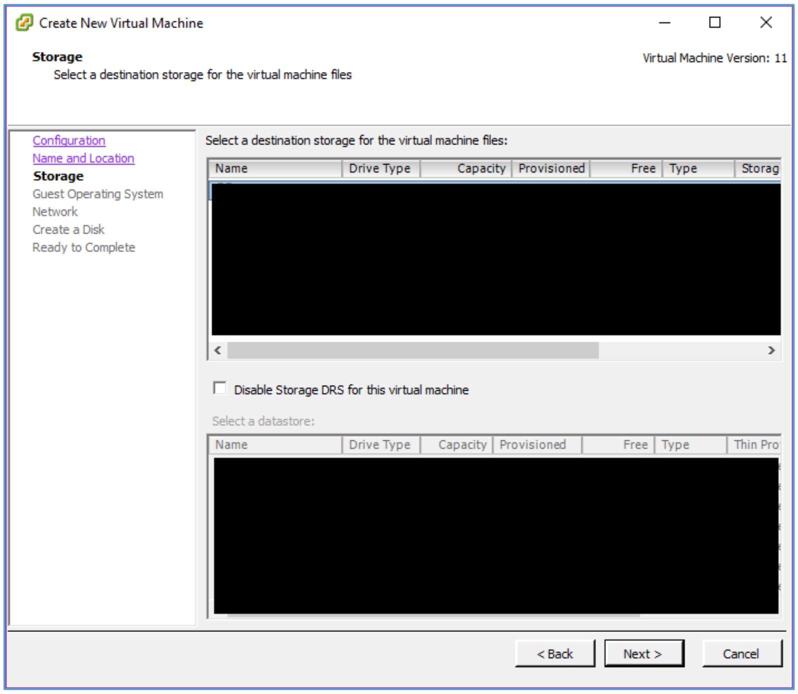
1. Create a new virtual machine, and under **configuration** select **Typical**.
2. Click **Next >**.



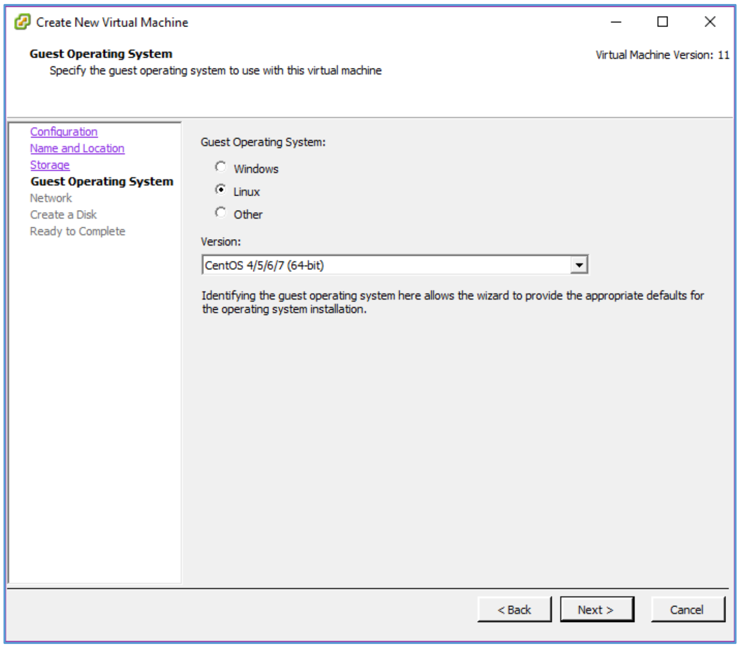
3. Create a **Name** for the virtual machine and assign it an **Inventory Location**.
4. Click **Next >**.



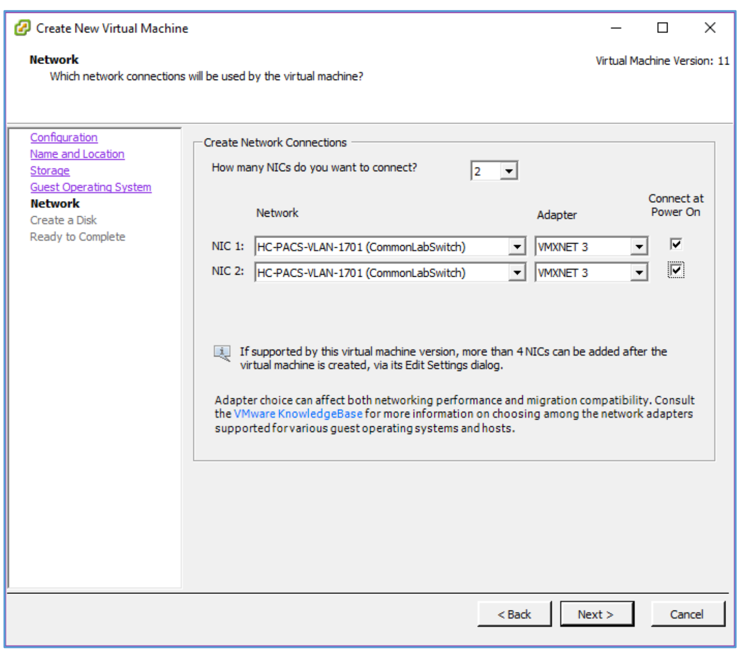
5. Select a **destination storage** for the VM.
6. Click **Next >**.



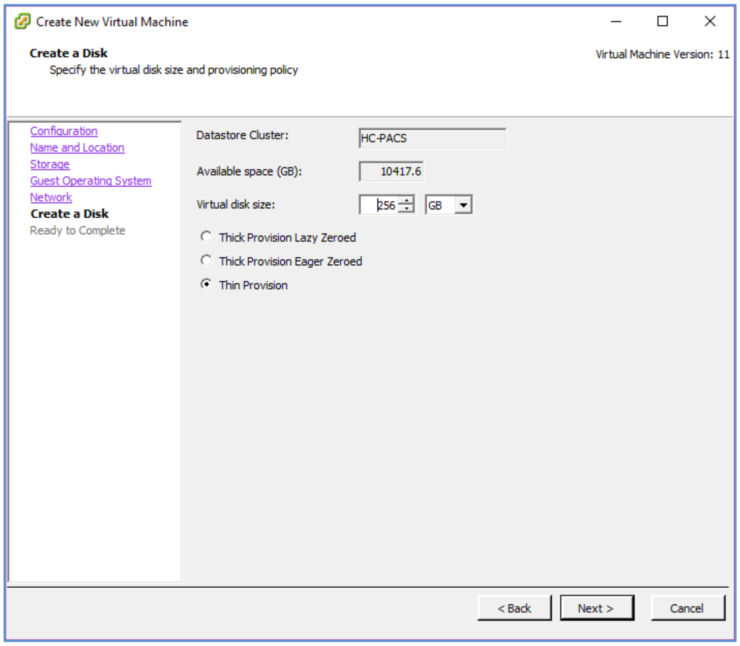
7. Check **Linux** and set version to **CentOS 4/5/6/7 (64-bit)**.
8. Click **Next >**.



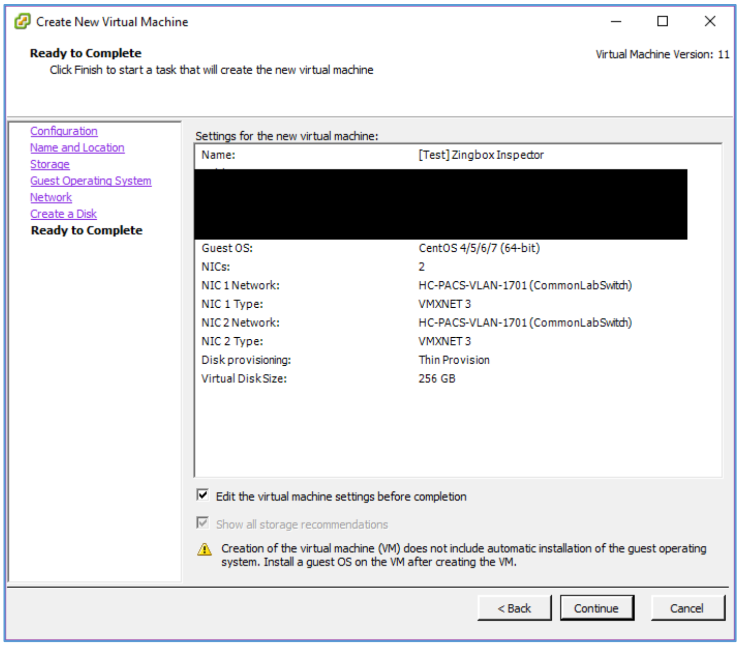
9. Connect **2 NICs** to the virtual machine and assign them to a **network**.
10. Check **Connect at Power On** for both NICs.
11. Click **Next >**.



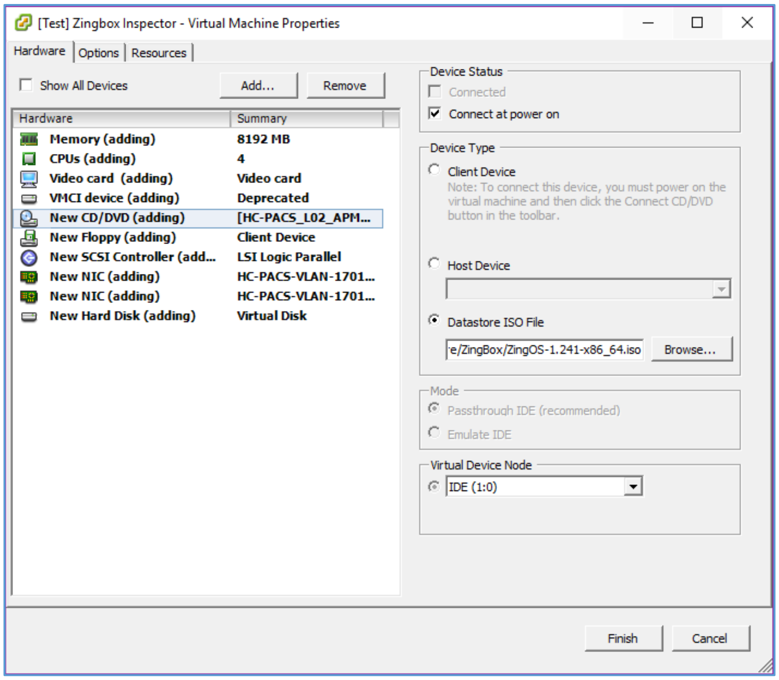
12. Set a **Virtual disk size** and **Provisioning method**.
13. Click **Next >**.



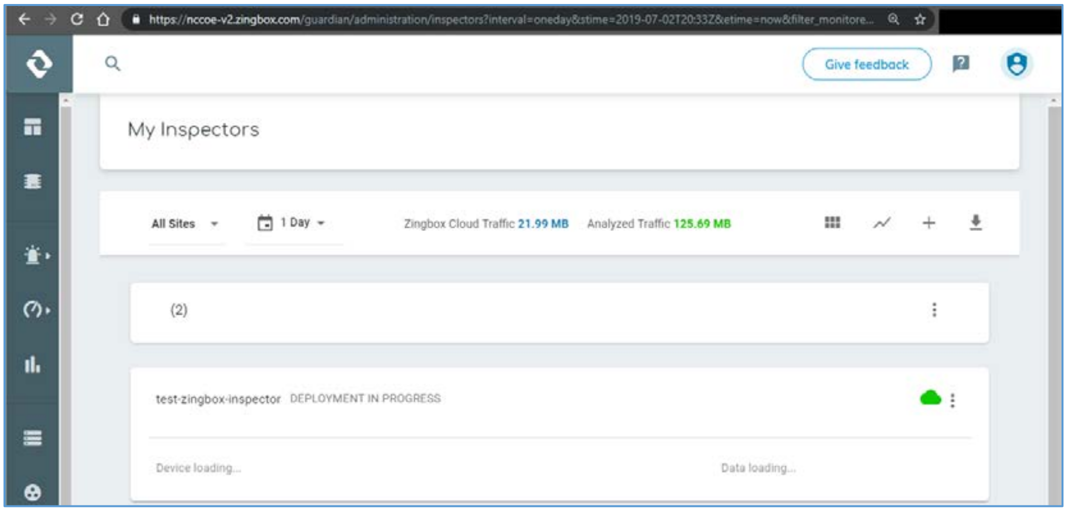
14. Verify virtual machine settings are correct.
15. Check **Edit the virtual machine settings before completion**.
16. Click **Continue**.



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



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



2.7.5 Forescout CounterACT 8

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

System Requirements

CPU: 2

Memory: 8 GB RAM

Storage: 80 GB (Thin Provision)

Operating System: Linux Kernel 3.10

Network Adapter 1: VLAN 1201

Network Adapter 2: Trunk Port

Forescout Appliance Installation

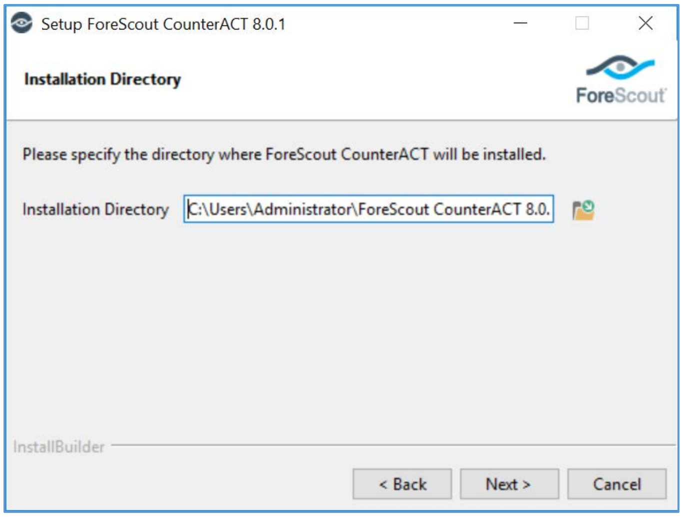
1. To begin installation, obtain the Forescout ISO. Load the Forescout ISO into the VM's CD/DVD drive. Make sure the CD/DVD drive is set to **Connect at Power On**.
2. Boot up the VM and begin the installation process.
3. Select **Install CounterACT**.
4. Press **Enter** to reboot.
5. Select **option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

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

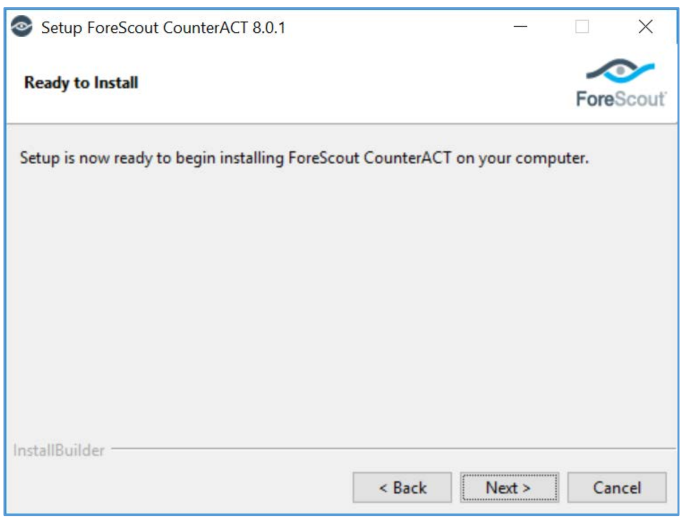
<u>**Forescout CounterACT Console Installation**</u>

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

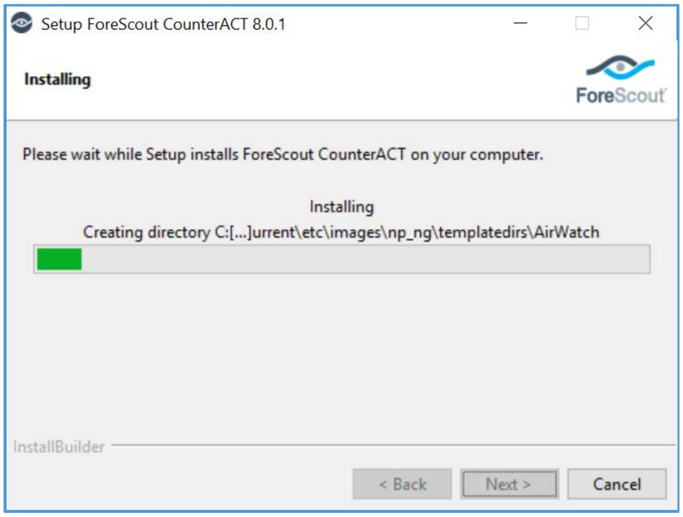
3. Verify **Installation Directory** as C*:\Users\Administrator\ForeScout CounterACT 8.0.1*; click **Next >**.



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 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** appears. Check **Create Desktop shortcut**; 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.

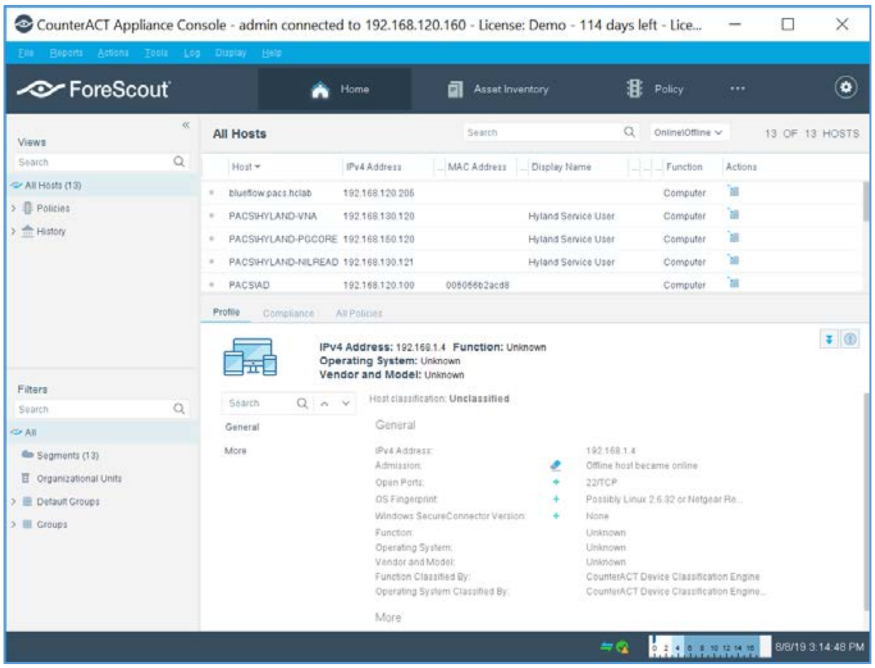
<u>Forescout CounterACT Configuration</u>

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

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

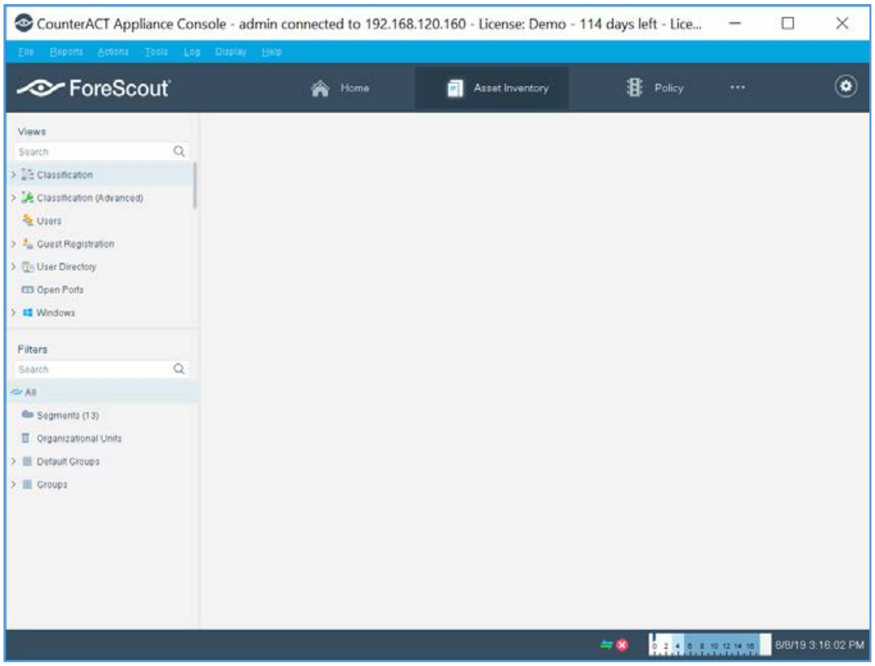
1. Select **the CounterACT** icon from the server on which you installed the **CounterACT Console**. A log on page appears, as depicted below.

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

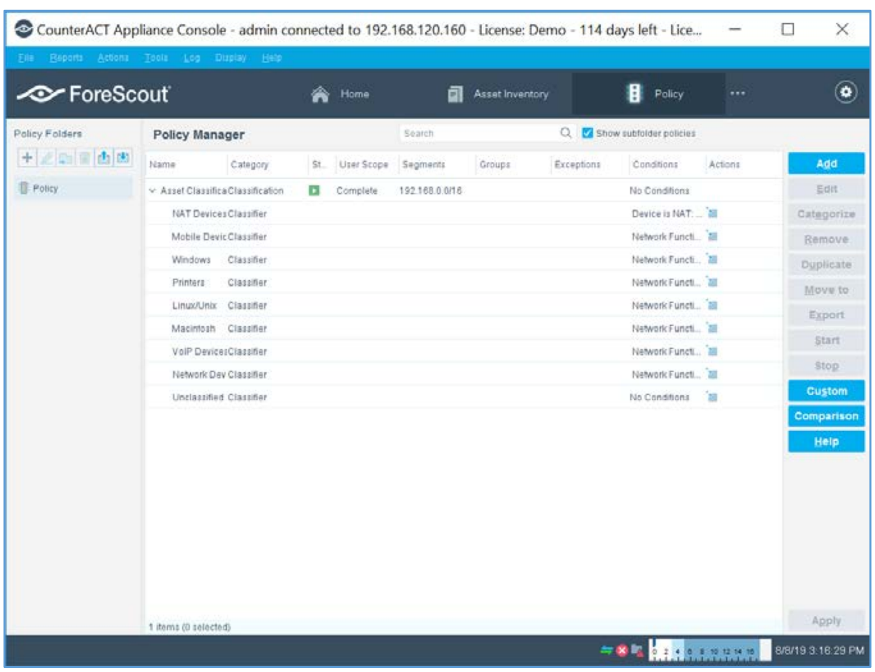


The console manager can be used to view, track, and analyze network activities detected by the appliance. It can also be used to define the threat protection, firewall, and other polices.

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



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

CPU: 12

Memory: 5 GB RAM

Storage: 500 GB (thin provisioned)

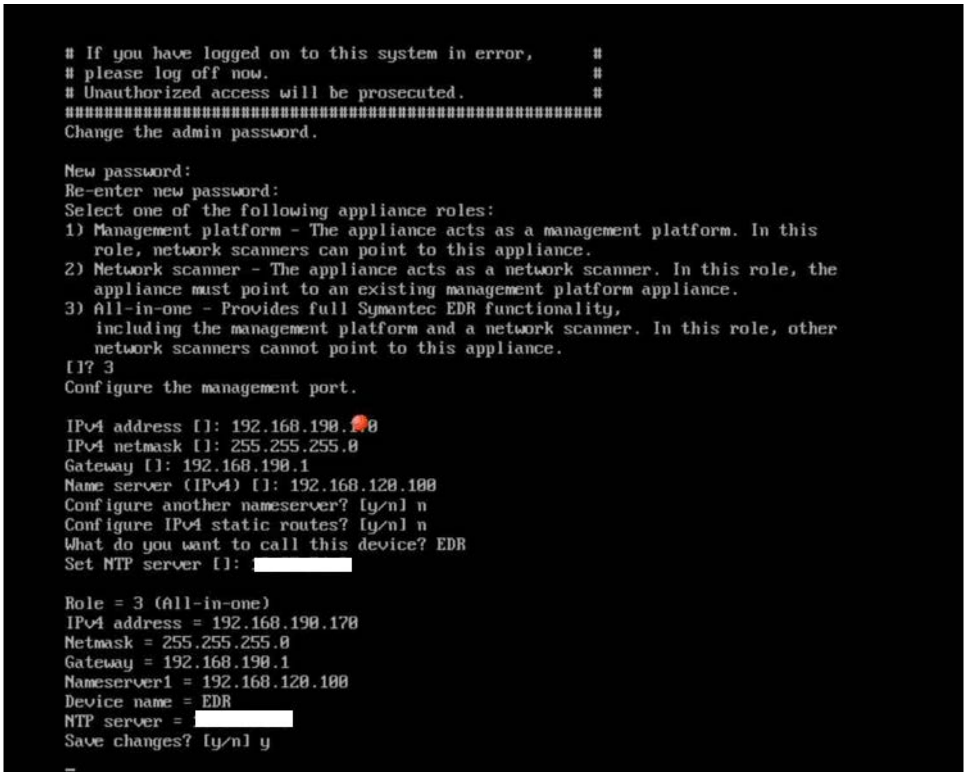
Operating System: CentOS 7

Network Adapter 1: VLAN 1901

Network Adapter 2: SPAN_PACS

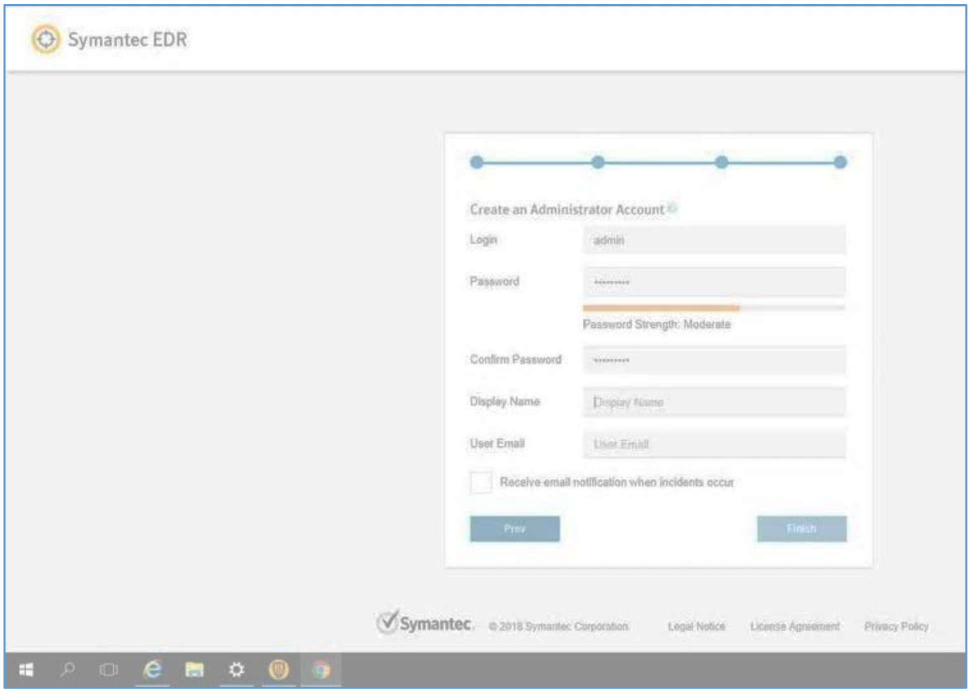
Symantec EDR Installation

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

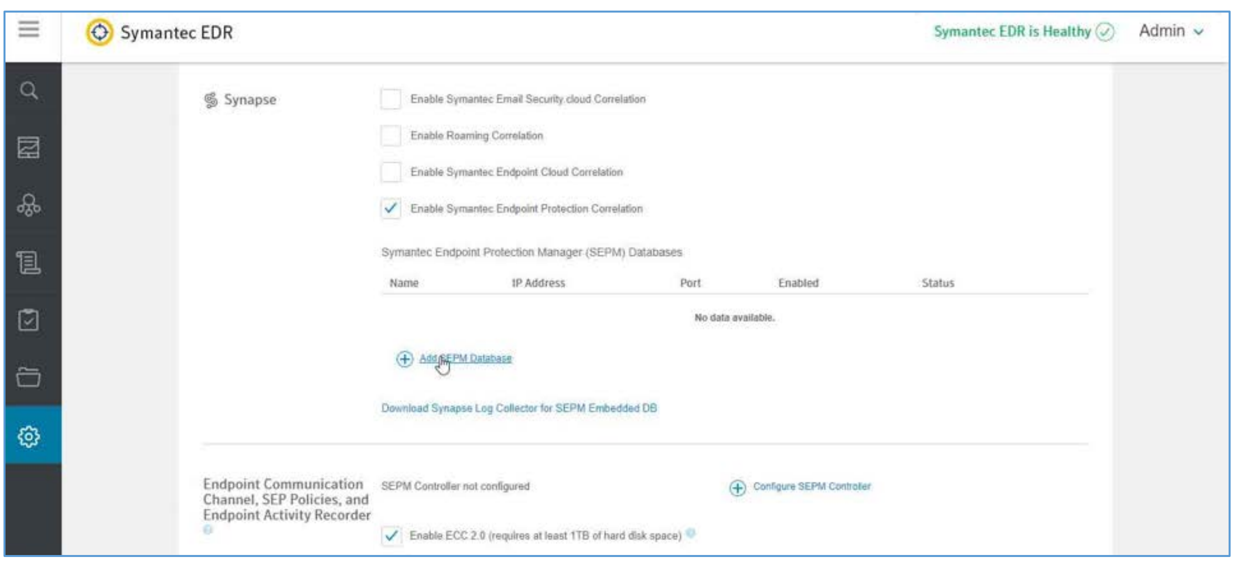


5. Open a web browser and travel to the virtual appliance at *https://192.168.190.170*. Enter the username setup and password *******.

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

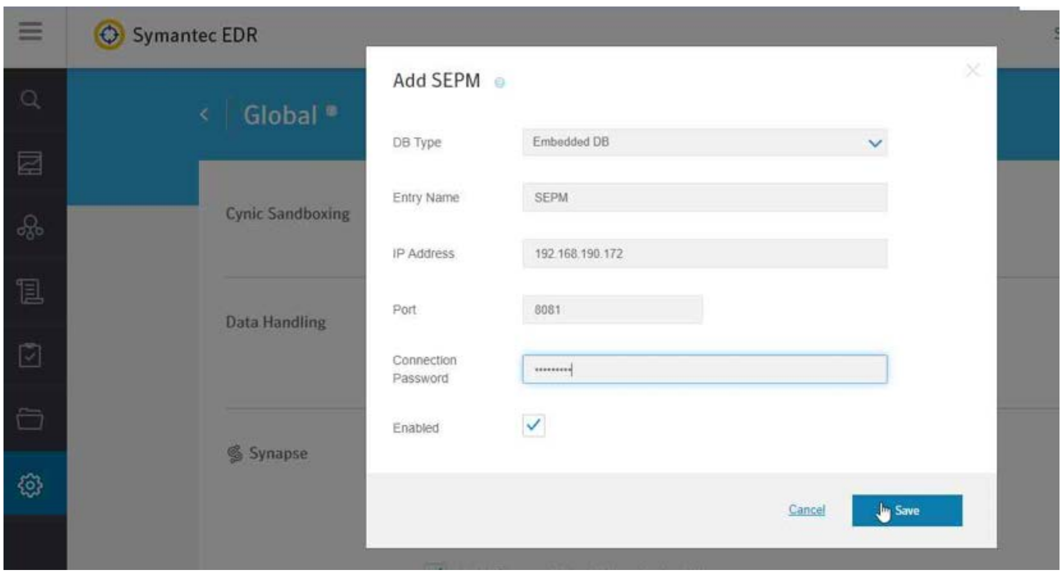


7. Select the **Settings** menu, and then select the **Global** sub-menu.
8. Ensure **Enable Symantec Endpoint Protection Correlation** is checked.
9. Select **Add SEPM Database** and enter the following options.

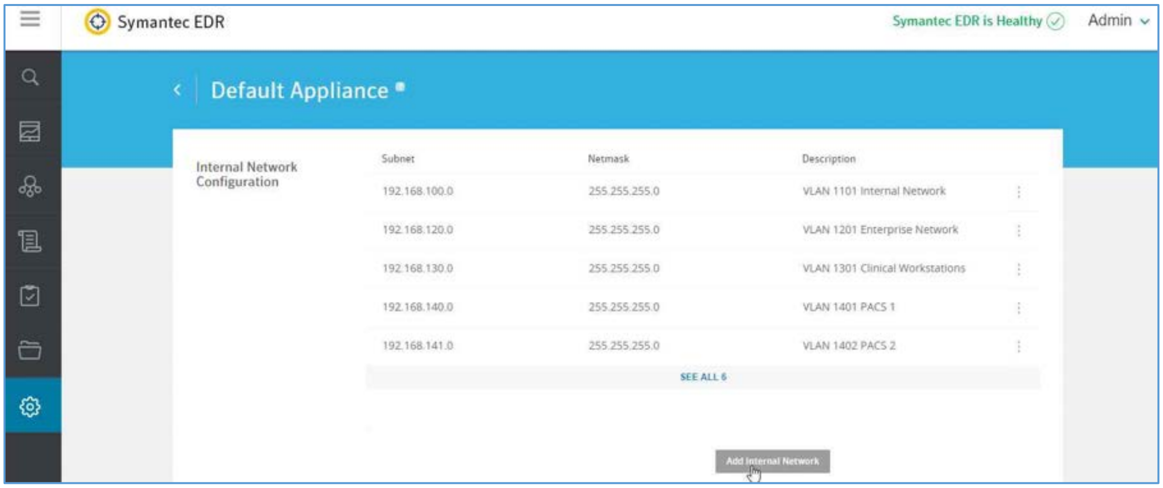


10. Provide the information that follows, and click **Save**:

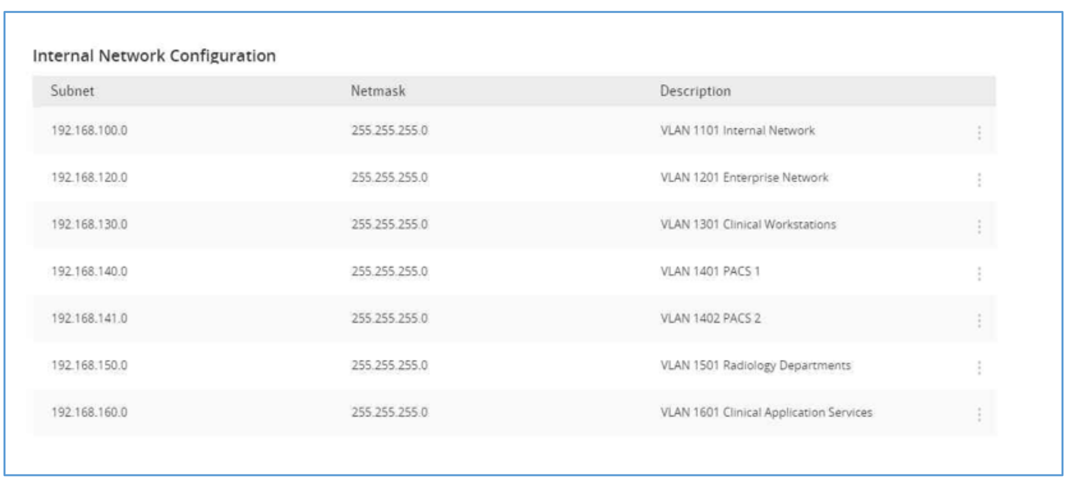
- **DB Type: Embedded DB**
- **Entry Name: SEPM**
- **Address: 192.168.190.172**
- **Port: 8081**
- **Connection Password:** *enter your connection password*
- **Enabled:** *Checked*



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



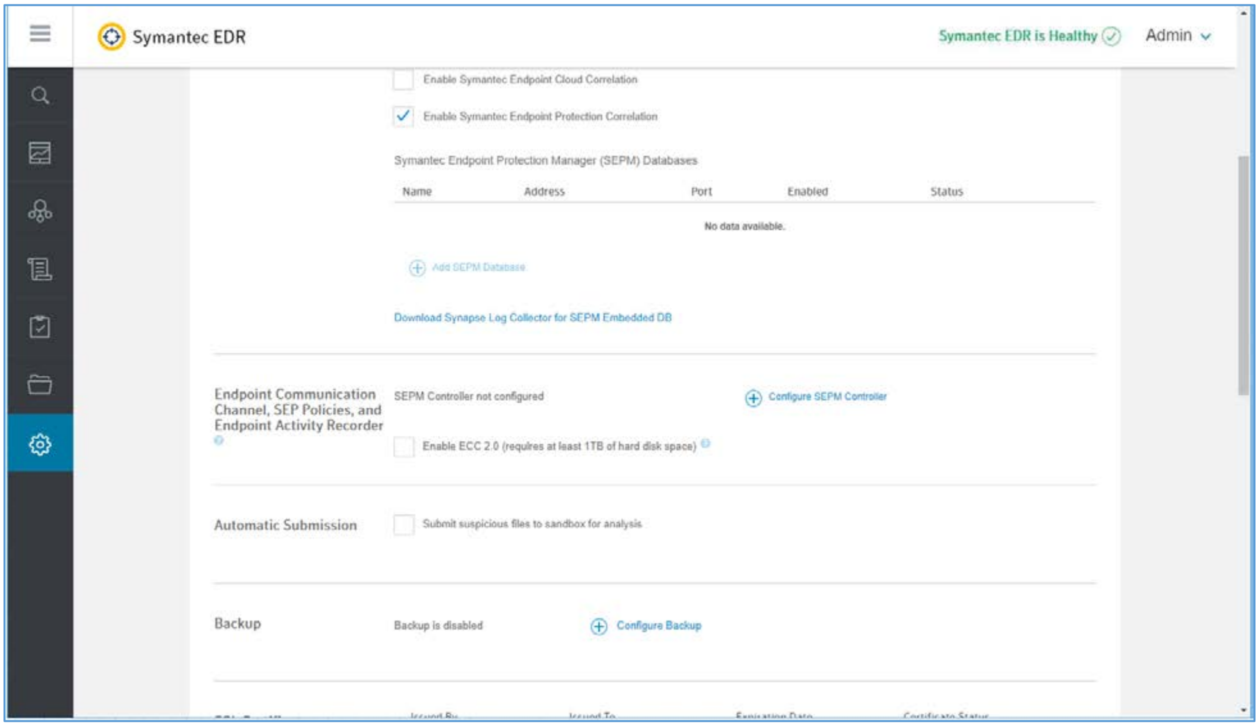
- **Subnet: 192.168.100.0 Netmask: 255.255.255.0 Description: VLAN 1101**
- **Subnet: 192.168.120.0 Netmask: 255.255.255.0 Description: VLAN 1201**
- **Subnet: 192.168.130.0 Netmask: 255.255.255.0 Description: VLAN 1301**
- **Subnet: 192.168.140.0 Netmask: 255.255.255.0 Description: VLAN 1401**
- **Subnet: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


Internal Network Configuration

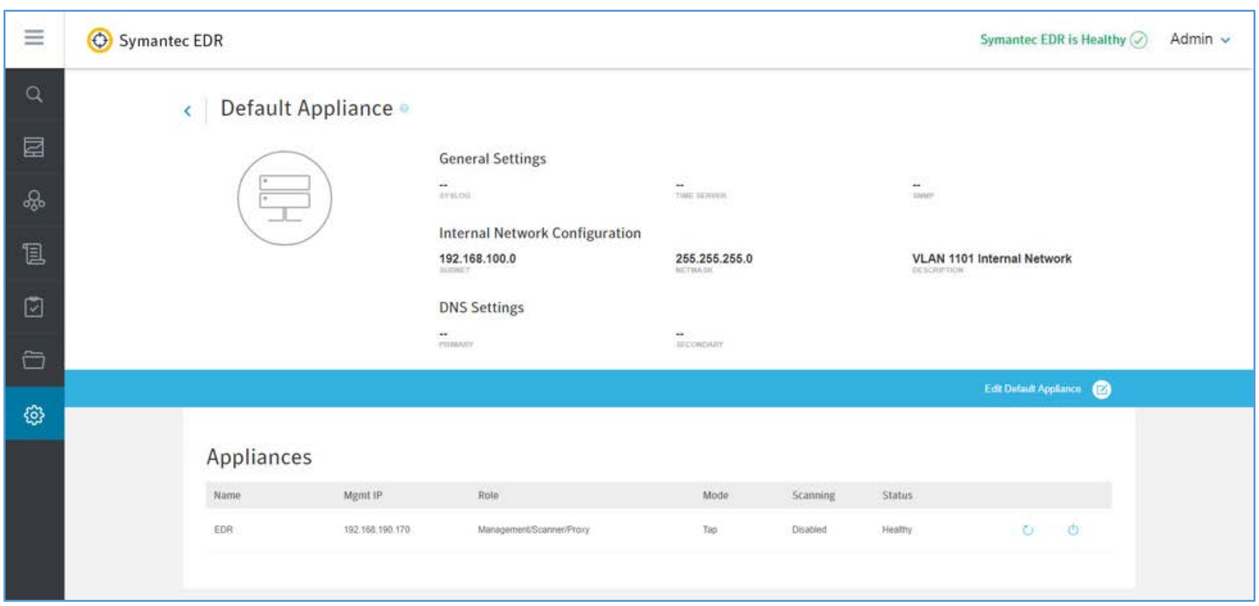
Subnet	Netmask	Description
192.168.100.0	255.255.255.0	VLAN 1101 Internal Network
192.168.120.0	255.255.255.0	VLAN 1201 Enterprise Network
192.168.130.0	255.255.255.0	VLAN 1301 Clinical Workstations
192.168.140.0	255.255.255.0	VLAN 1401 PACS 1
192.168.141.0	255.255.255.0	VLAN 1402 PACS 2
192.168.150.0	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**.



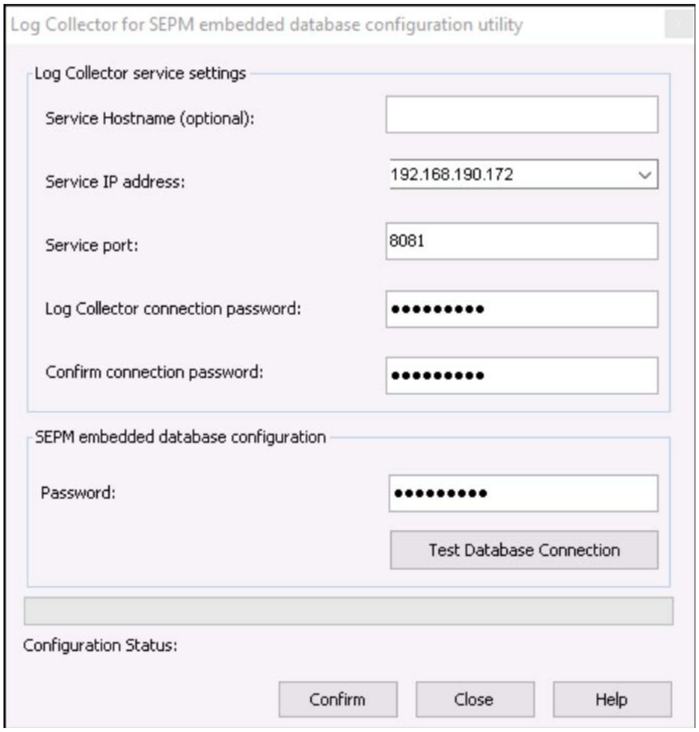
16. Select **Settings** and then **Appliances**.



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

Symantec EDR and SEP Correlation

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



2.8 Endpoint Protection & Security

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

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

System Requirements

CPU: 4

Memory: 8 GB RAM

Storage: 120 GB (Thin Provision)

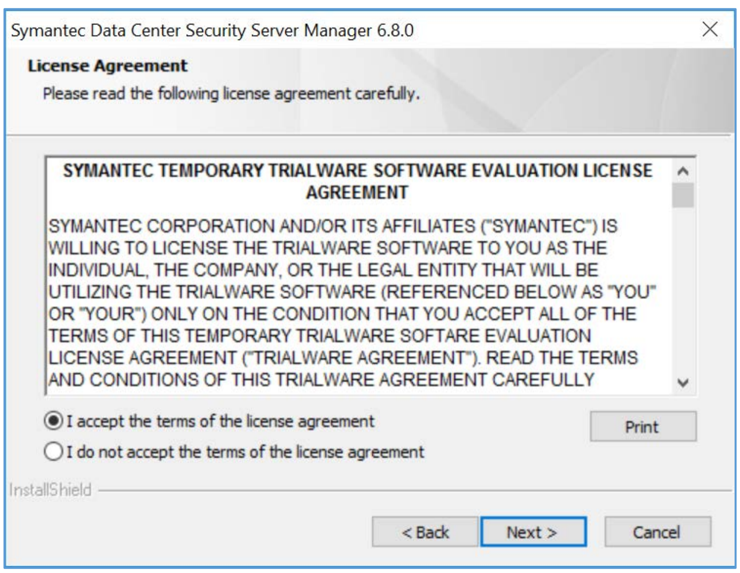
Operating System: Microsoft Windows Server 2016 Datacenter

Network Adapter: VLAN 1901

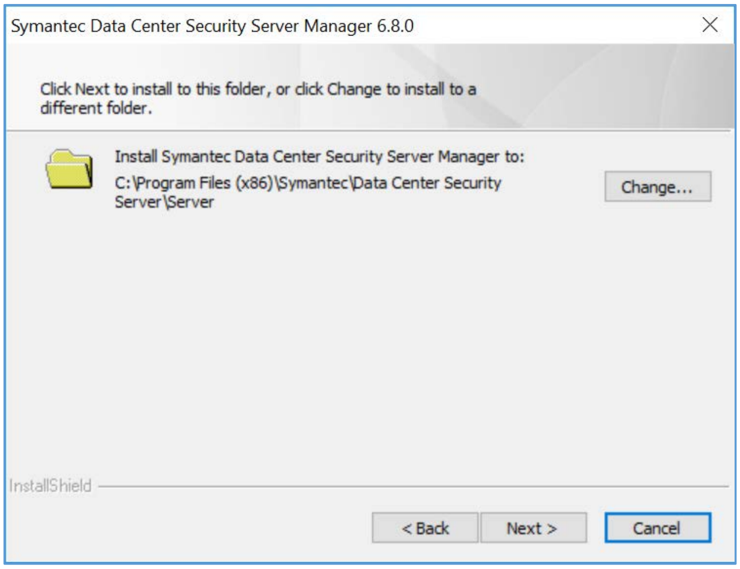
Symantec Data Center Security Installation

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

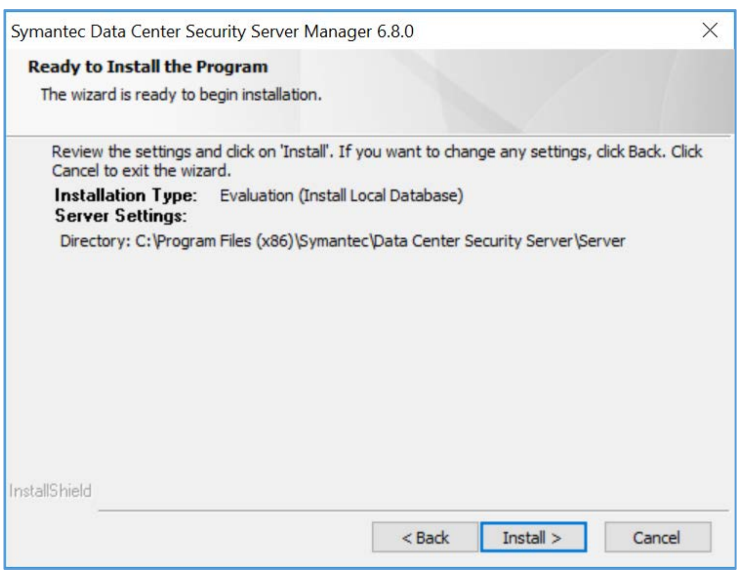
3. Check **I accept the terms of the license agreement**.
4. Click **Next >**.



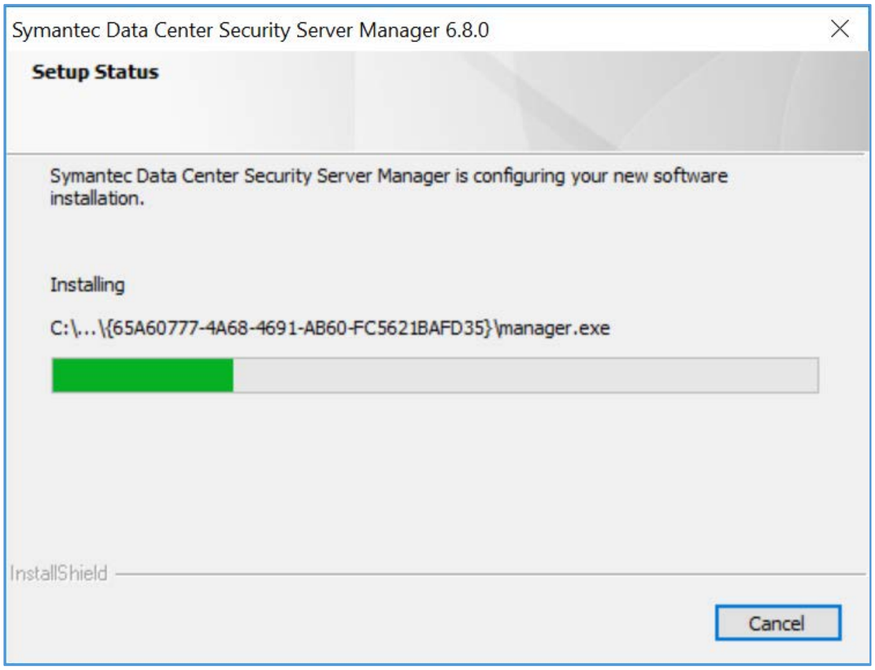
5. Verify install location.
6. Click **Next >**.



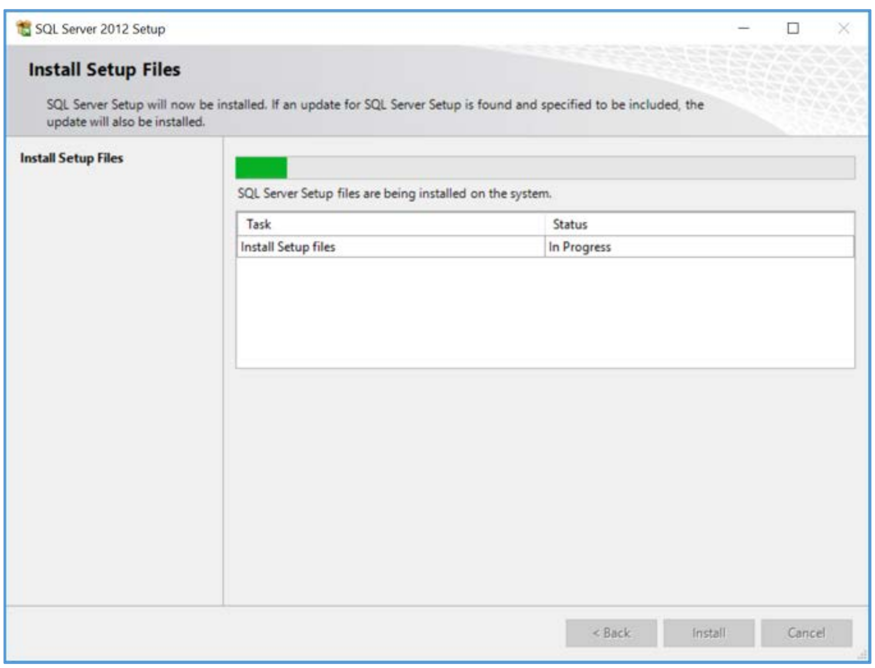
7. Review settings.
8. Click **Install >**.



9. Wait for setup and install process to complete.

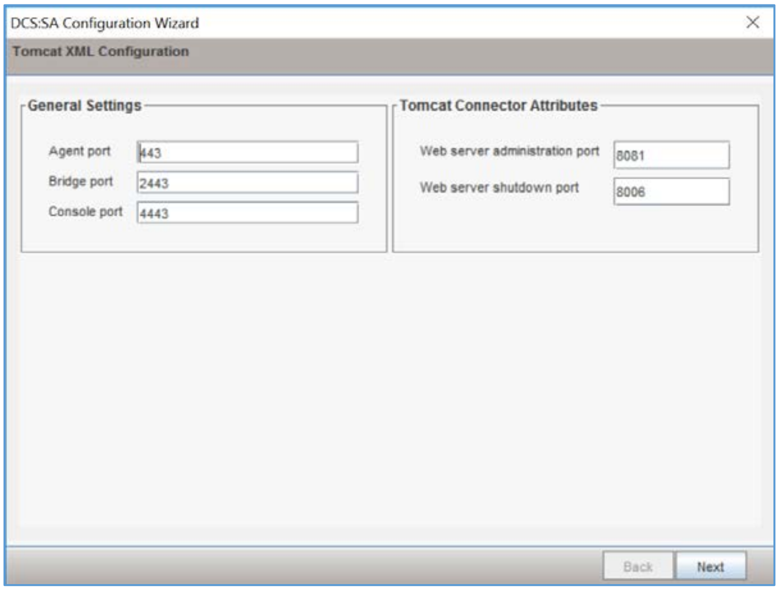


10. SQL Server will automatically be installed during the setup process.

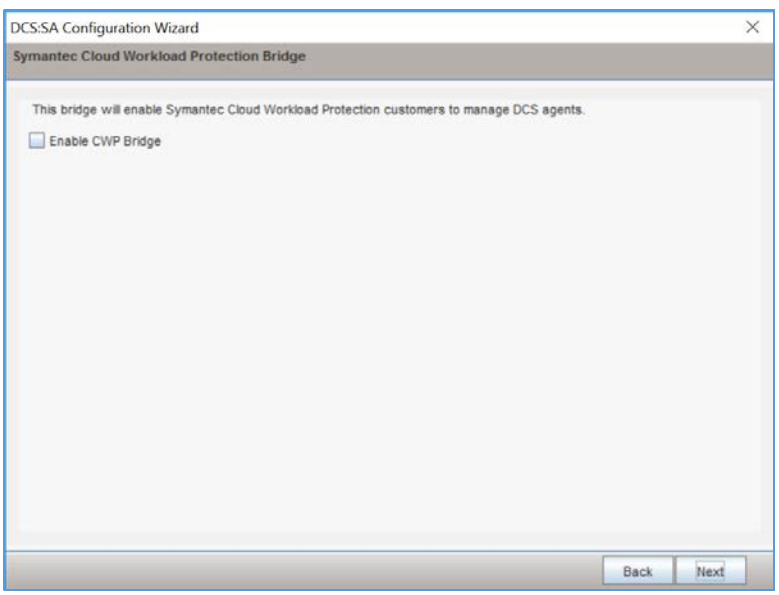


11. Provide the information below, and click on **Next**:
    - **Agent port**: 443

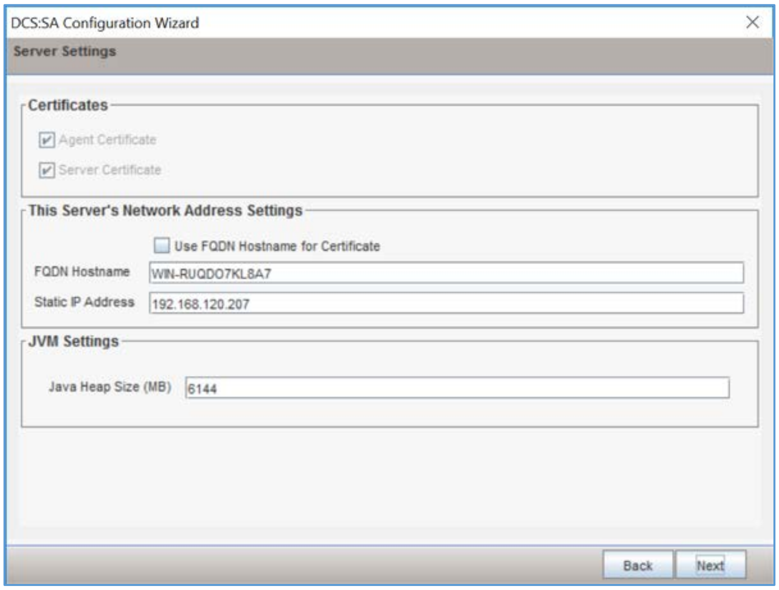
- **Bridge port**: 2443
- **Console port**: 4443
- **Web server administration port**: 8081
- **Web server shutdown port**: 8006



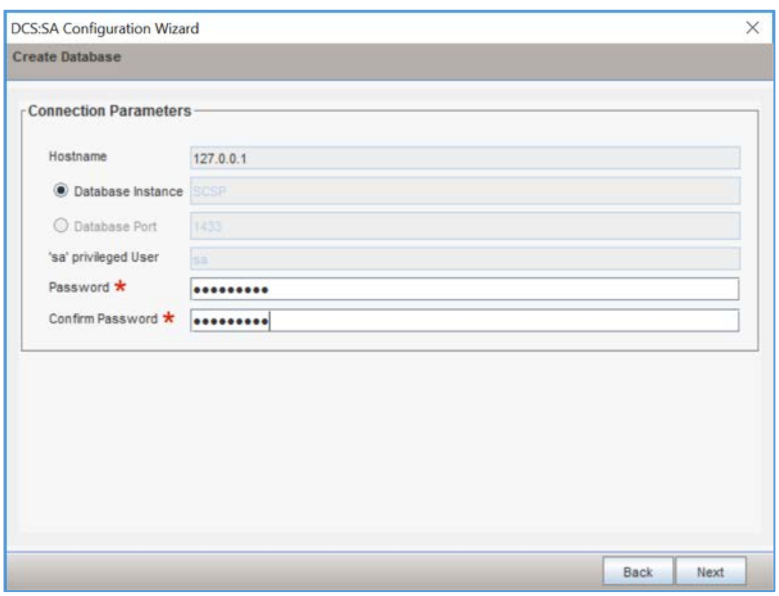
12. Uncheck **Enable CWP Bridge** and click **Next**.



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

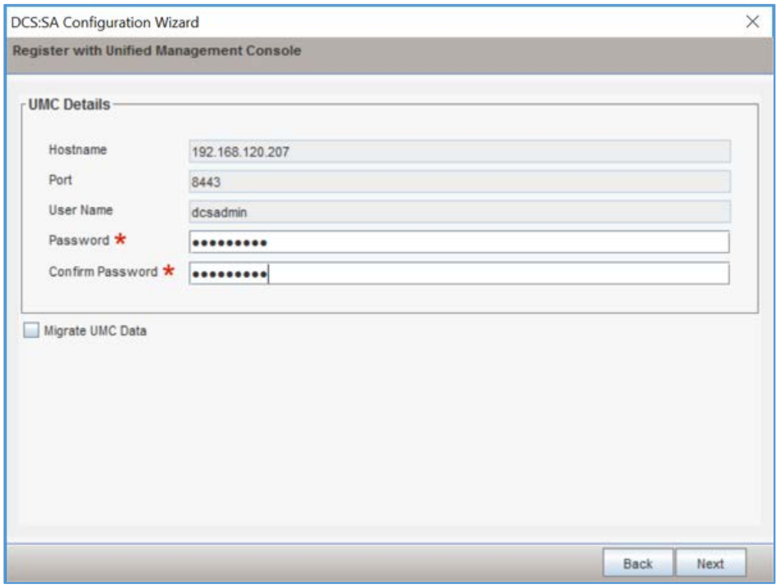


14. Create a **password** for the database connection.
15. Click **Next**.

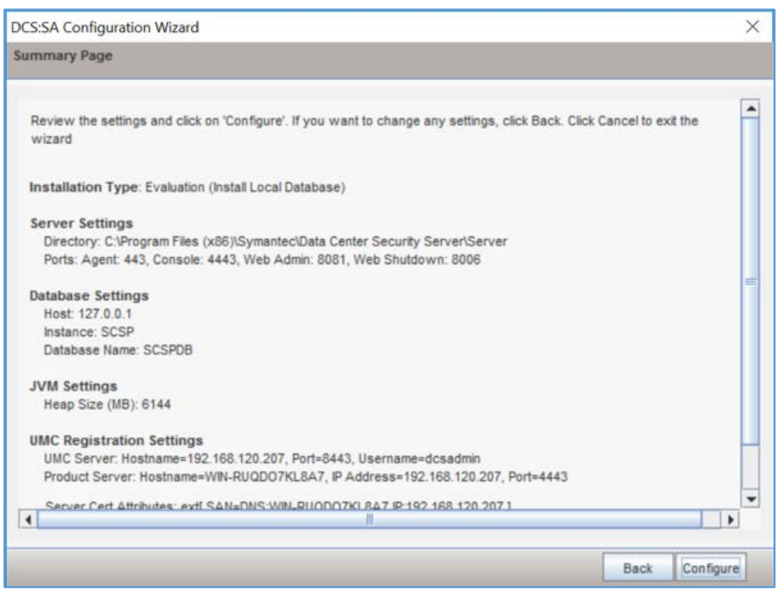


16. Verify **Unified Management Console** connection settings.
17. Create a password for **Unified Management Console** connection.

18. Click **Next**.

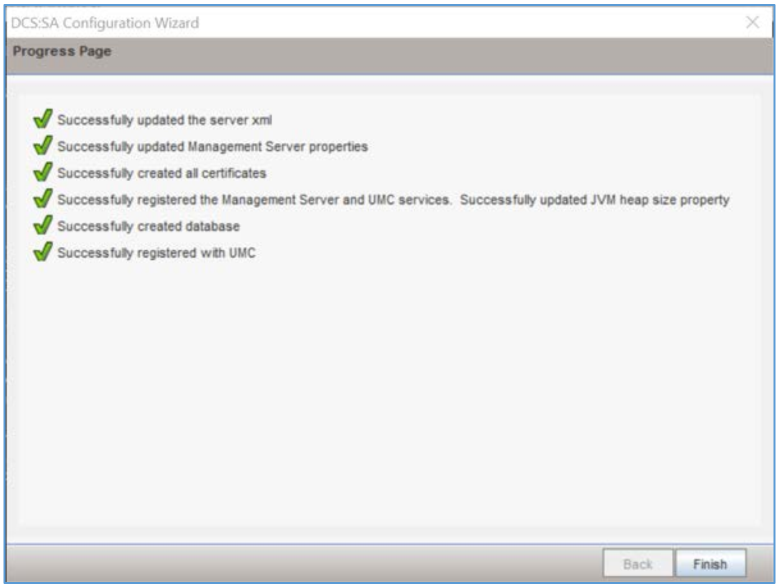


19. Verify configuration settings and click **Next**.

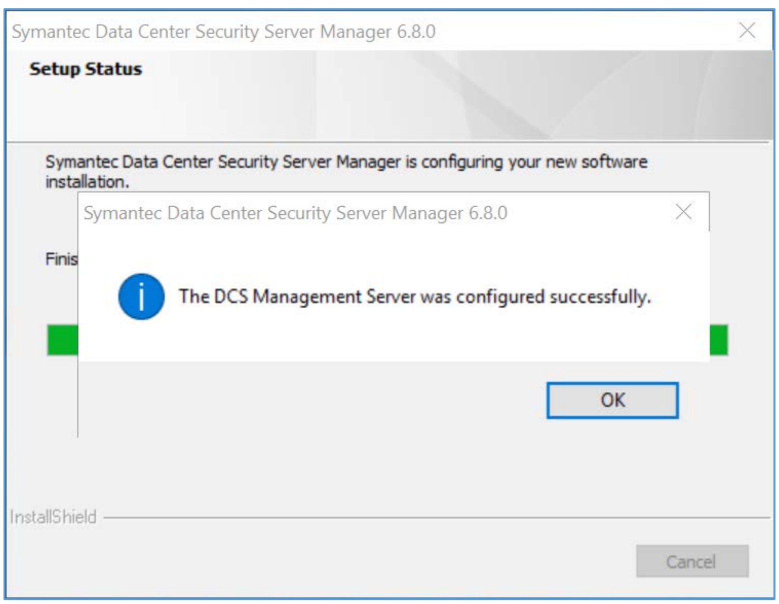


20. Wait for configuration process to complete.

21. Click **Finish**.

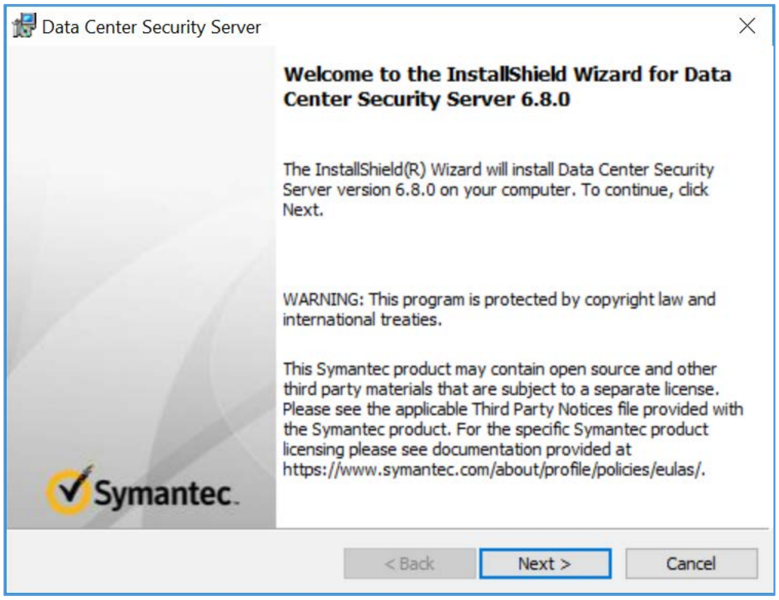


22. Wait for install to complete and click **OK**.

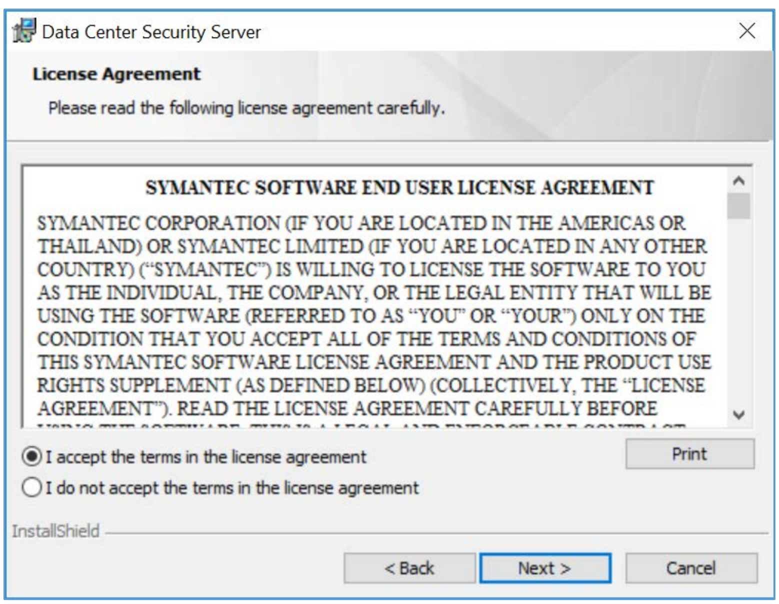


Symantec Datacenter Security Windows Agent Install

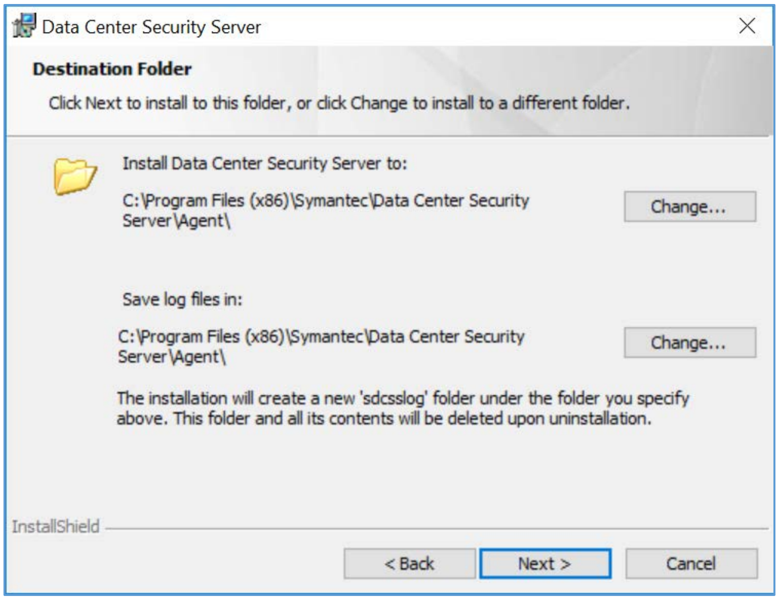
1. Run **agent.exe**.
2. Click **Next >**.



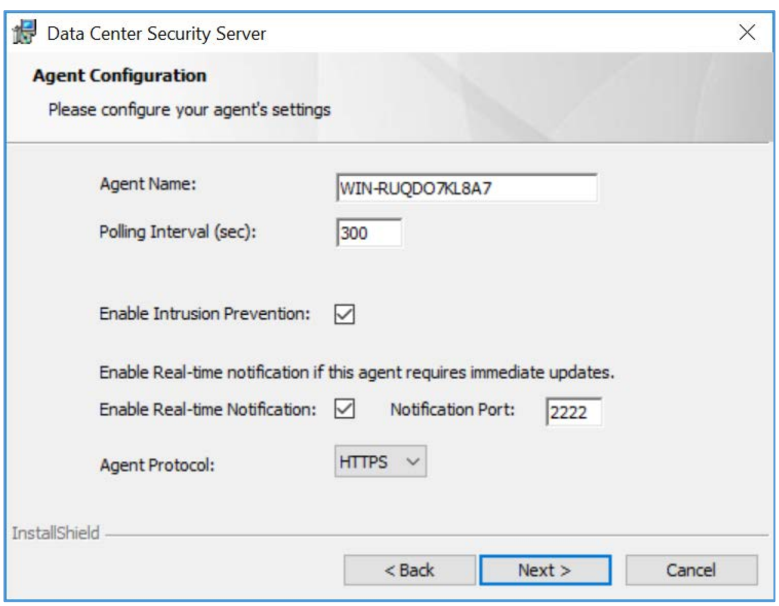
3. Check **I accept the terms in the license agreement**.
4. Click **Next >**.



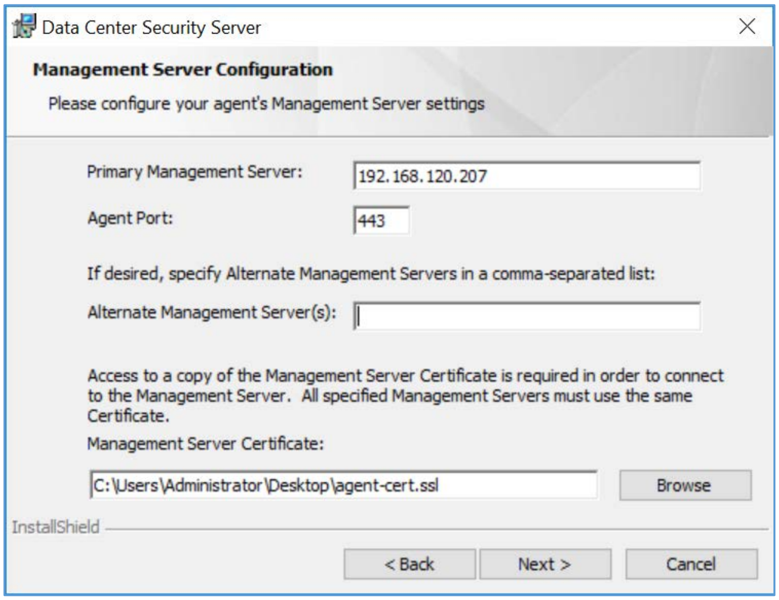
5. Verify installation and log files directories.
6. **Click Next >**.



7. Provide the information below, and click on **Next>**:
   - **Agent Name**: WIN-RUQDO7KL8A
   - **Polling Interval (sec)**: 300
   - Check **Enable Intrusion Prevention**
   - **Notification Port:** 2222
   - **Agent Protocol:** HTTPS

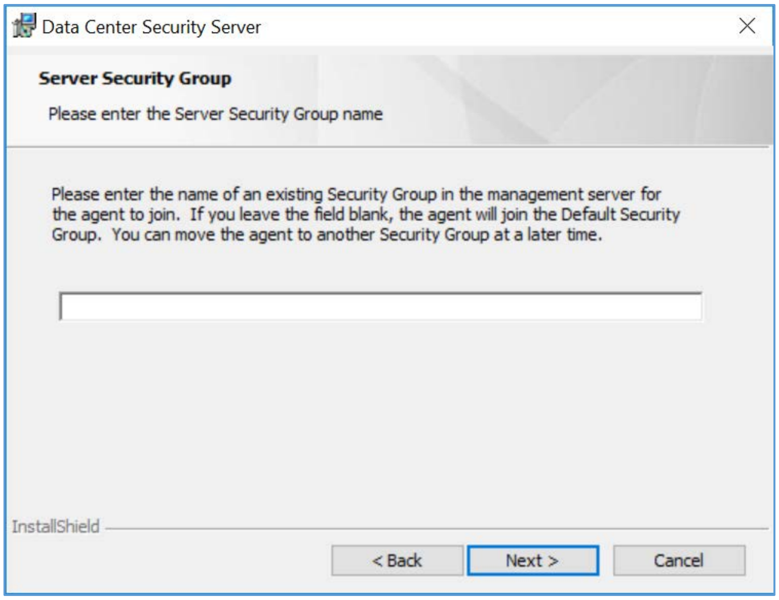


8. Provide the information below and click **Next**:
   - **Primary Management Server**: 192.168.120.207
   - **Agent Port**: 443
   - **Alternate Management Servers**:
   - **Management Server Certificate**: *C:\User\Administrator\Desktop\agent-cert.ssh*

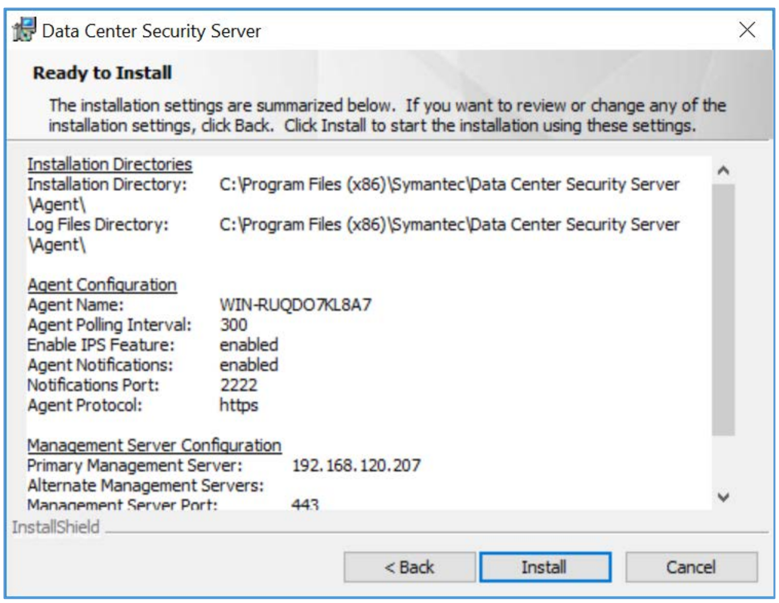


9. Specify a **Server Security Group** created through Symantec Datacenter Security Server or leave it blank to use the default security group.

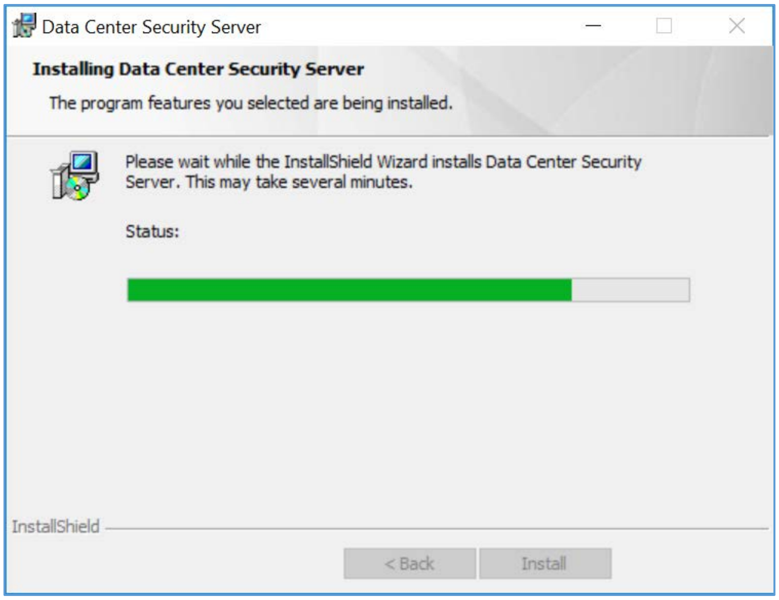
10. Click **Next >**.



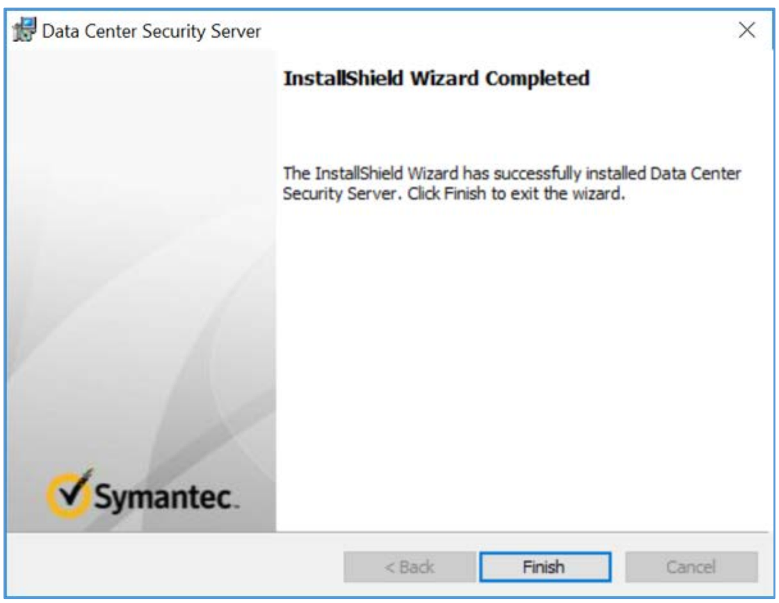
11. Verify installation and configuration settings and click **Install**.



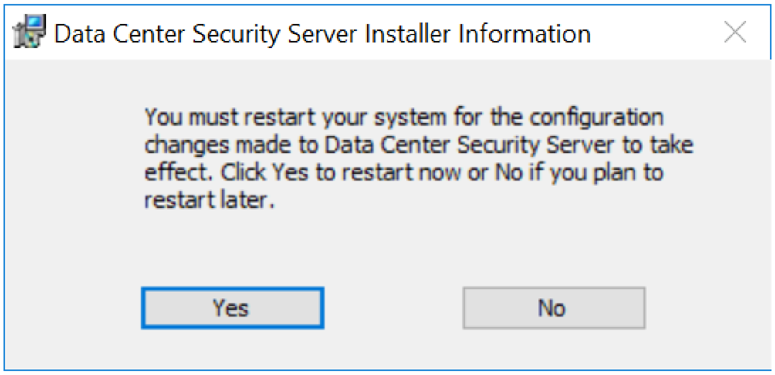
12. Wait for the installation process to complete.



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 antivirus, intrusion prevention, application whitelisting, and other capabilities. For this project Symantec SEP is used to protect endpoints from malicious software and integrates with Symantec Endpoint Detection and Response to detect suspicious behavior.

System Requirements

CPU: 4

Memory: 8GB RAM

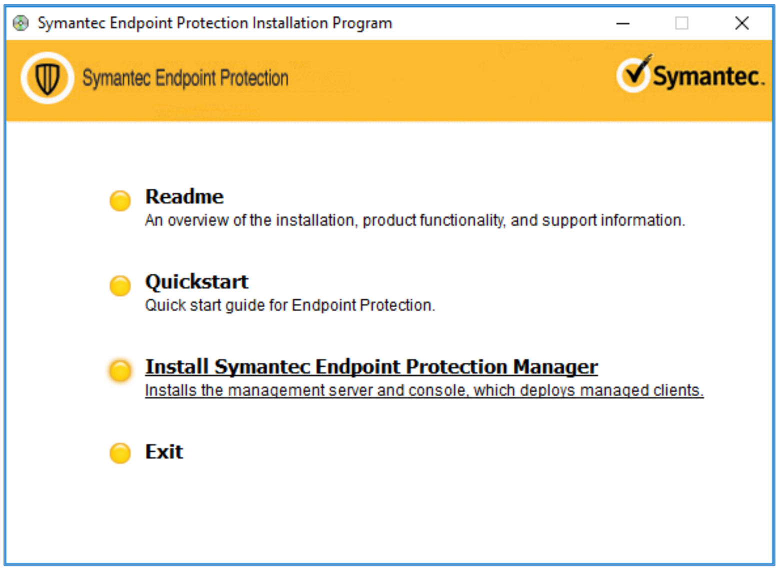
Storage: 240GB (thin provisioned)

Operating System: Microsoft Windows Server 2016

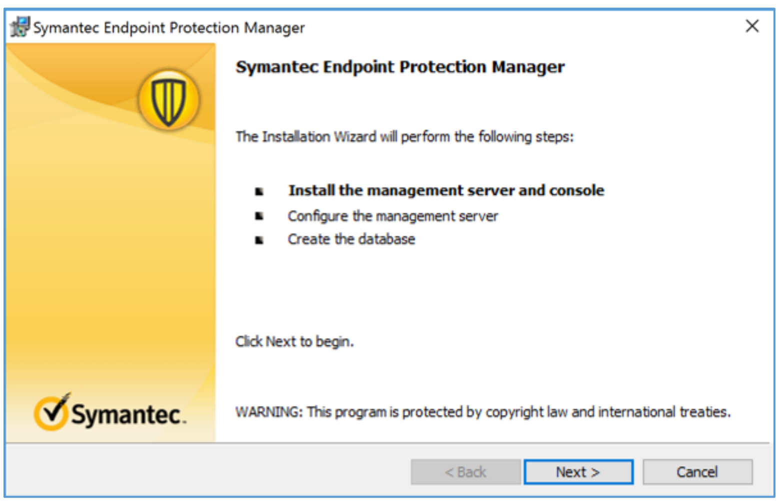
Network Adapter: VLAN 1901

Symantec Endpoint Protection Manager Installation

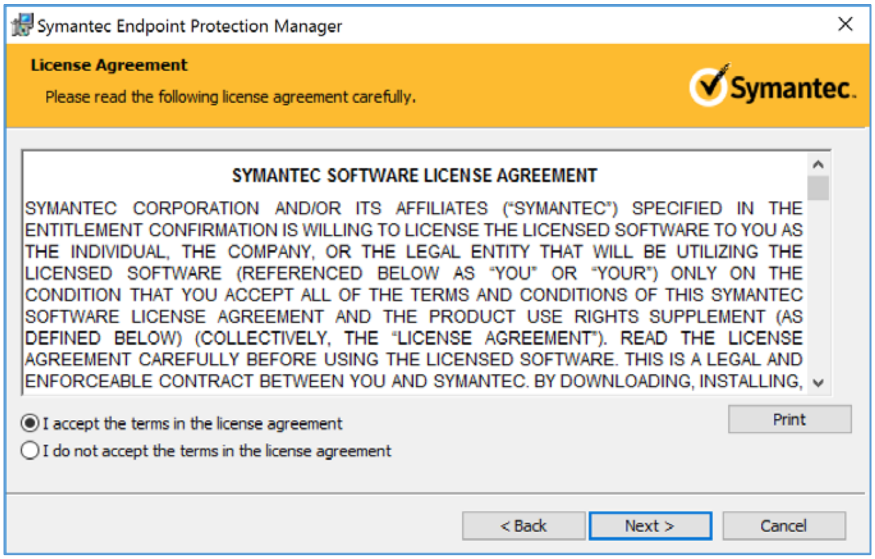
1. Launch *Symantec_Endpoint_Protection_14.2.0.MP1_Part1_Trialware_EN.exe* file.
2. Select **Install Symantec Protection Endpoint Manager** option.



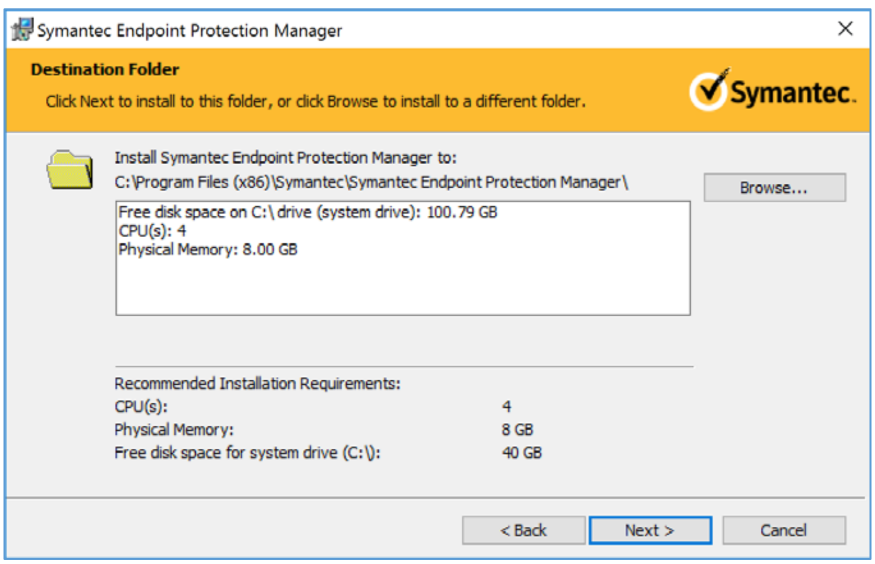
3. Proceed through the install wizard by clicking **Next >.**



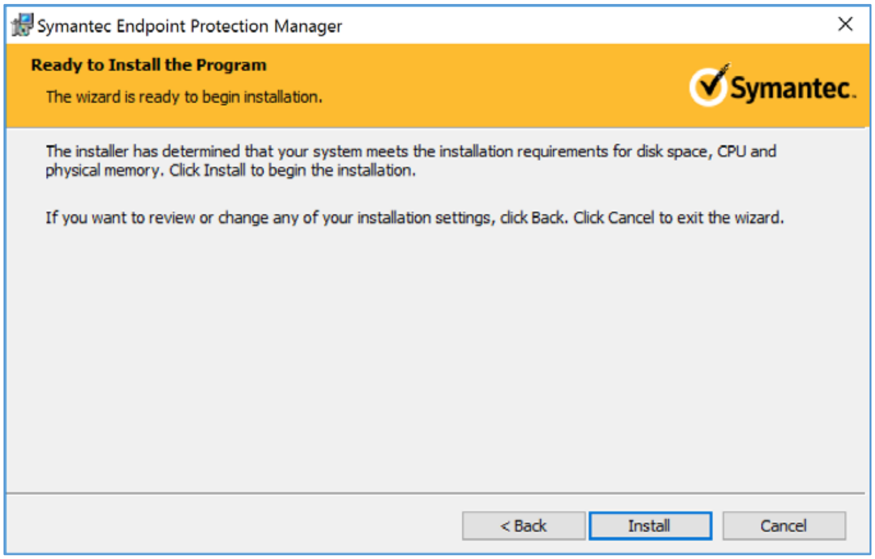
4. Check **I accept the terms in the license agreement**.
5. Click **Next >**.



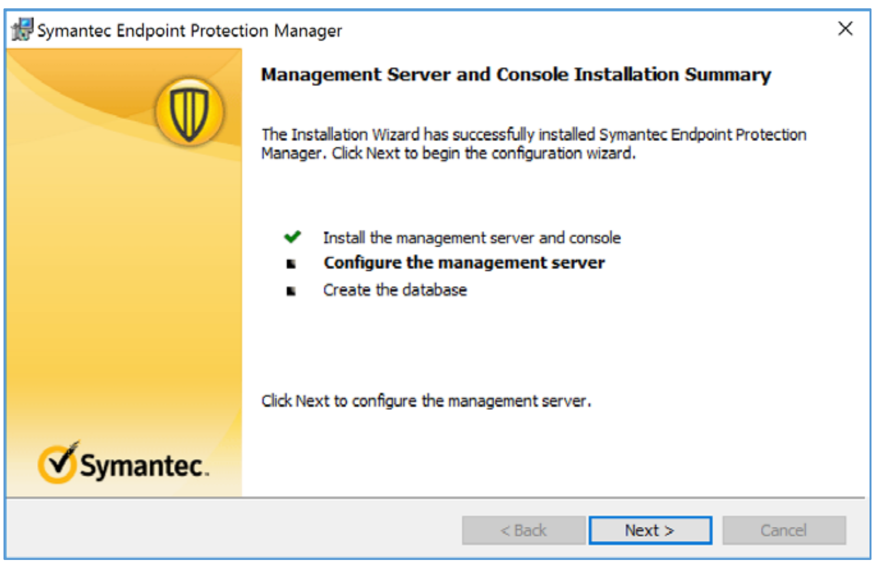
6. Select the location you want to install Symantec Endpoint Protection Manger and click **Next >**. Keep the default location of *C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager*\.



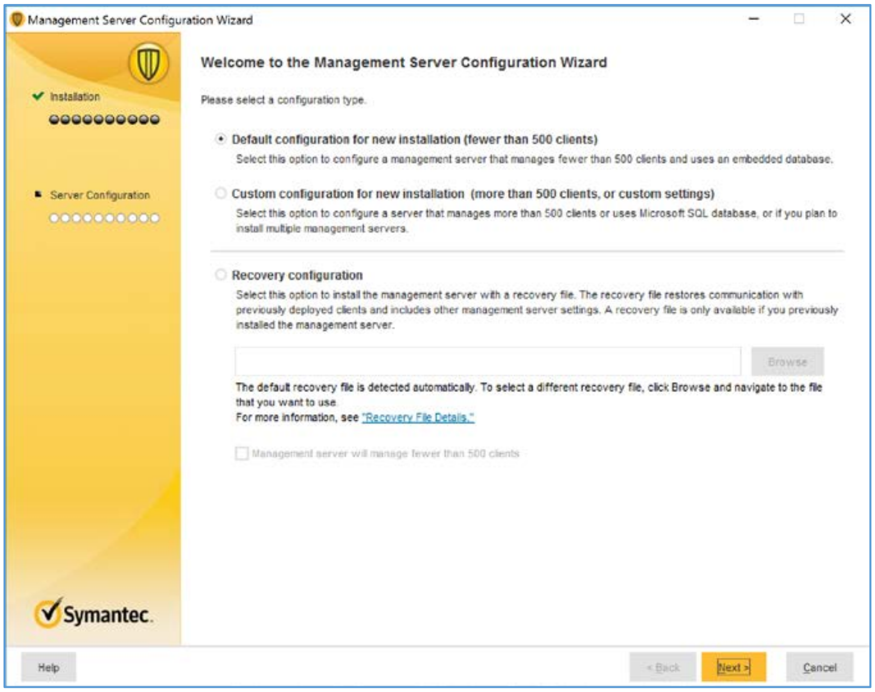
7. Select **Install**.



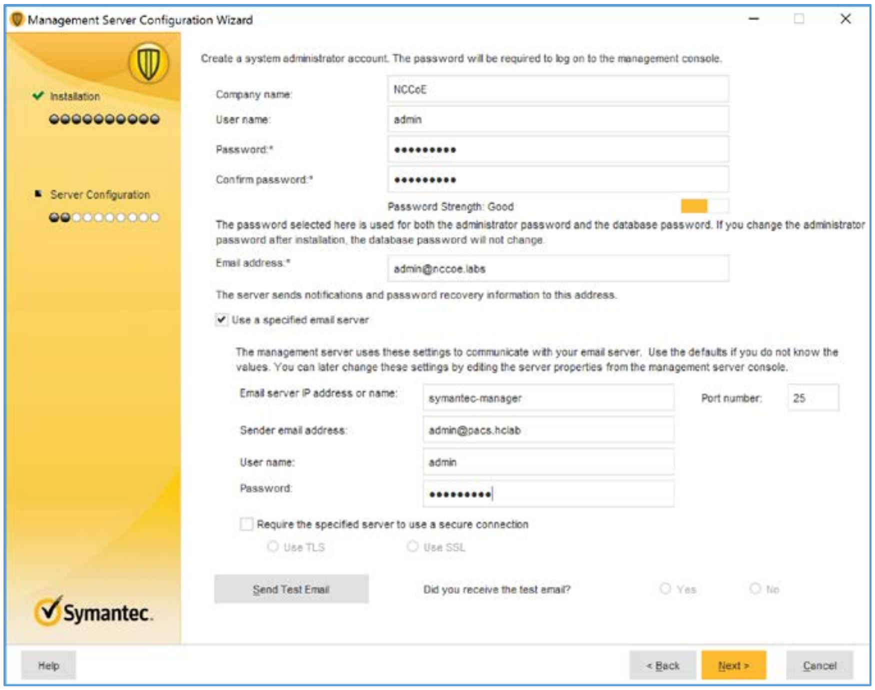
8. After installation is complete, click **Next >** to continue with configuration of the management server.



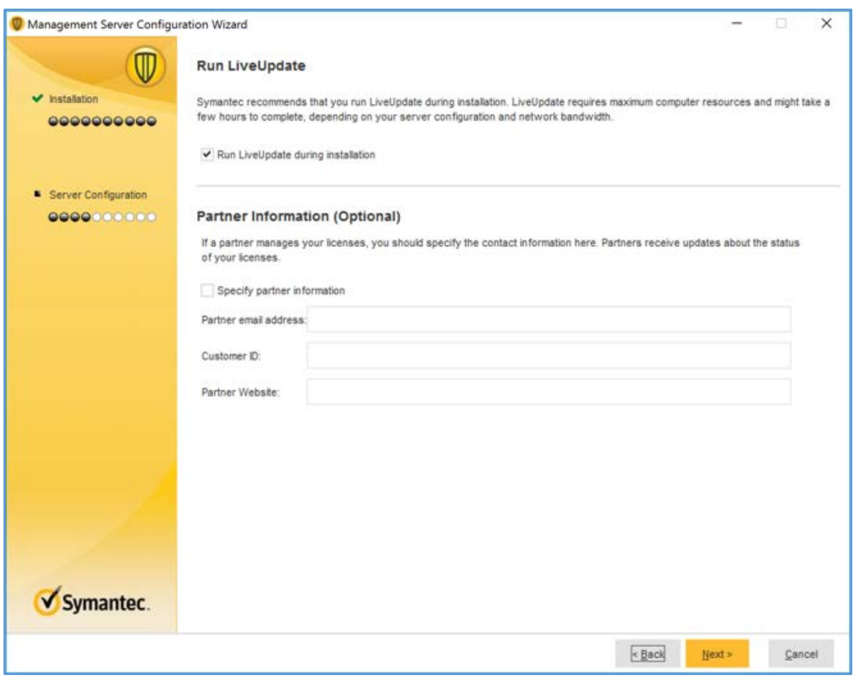
9. Select **Default configuration** for new installation; click **Next >**.



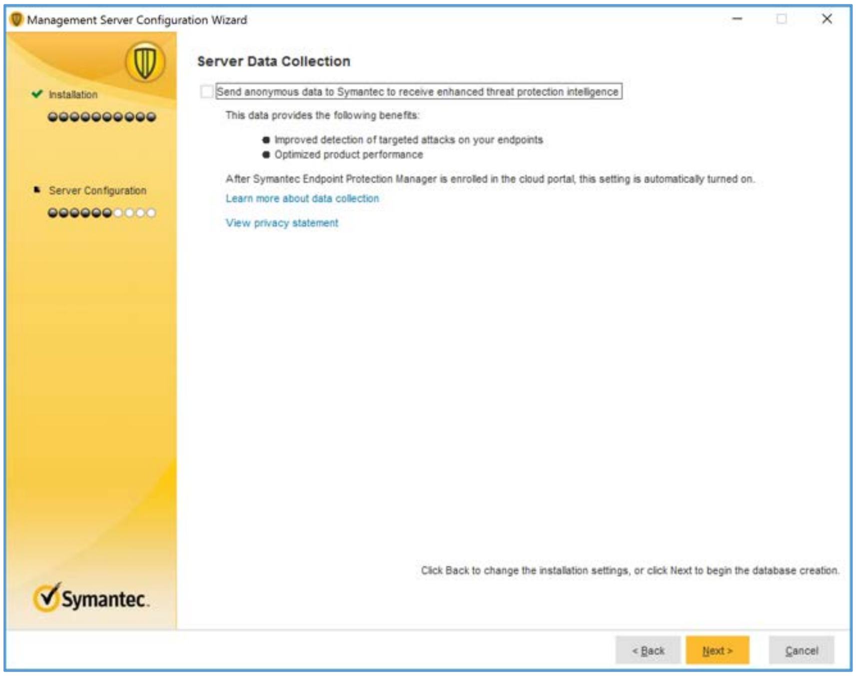
10. Provide the following information and click **Next>**.
    - **Company Name**: NCCoE
    - **User name**: admin
    - **Password**: ********
    - **Confirm password**: ********
    - **Email address**: admin@nccoe.labs



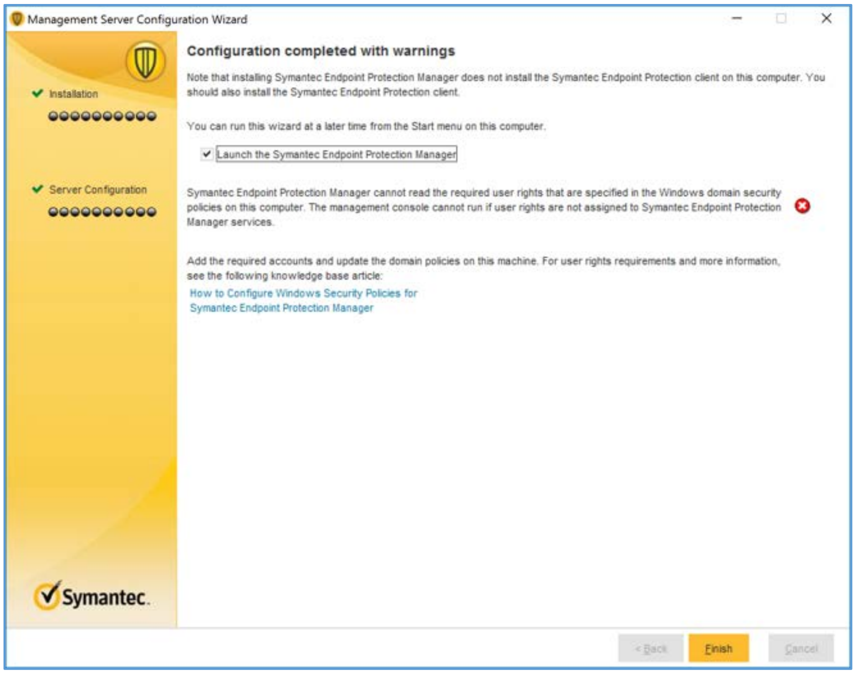
11. Confirm that **Run LiveUpdate** during installation is checked; click **Next >**.



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

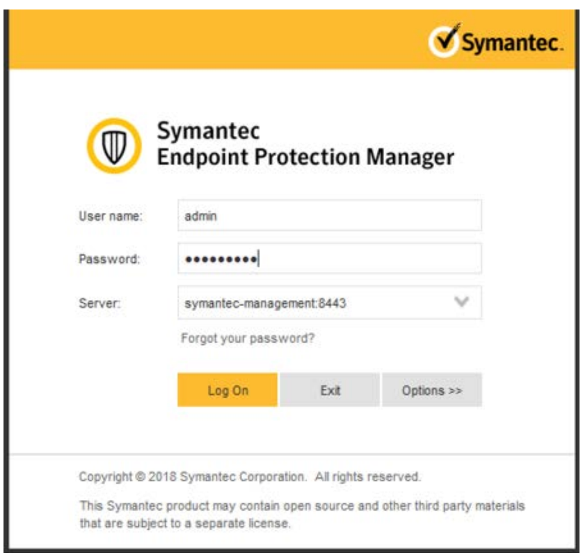


13. After installation is completed, check **Launch the Symantec Endpoint Protection Manager** to configure your hosts; click **Finish**.

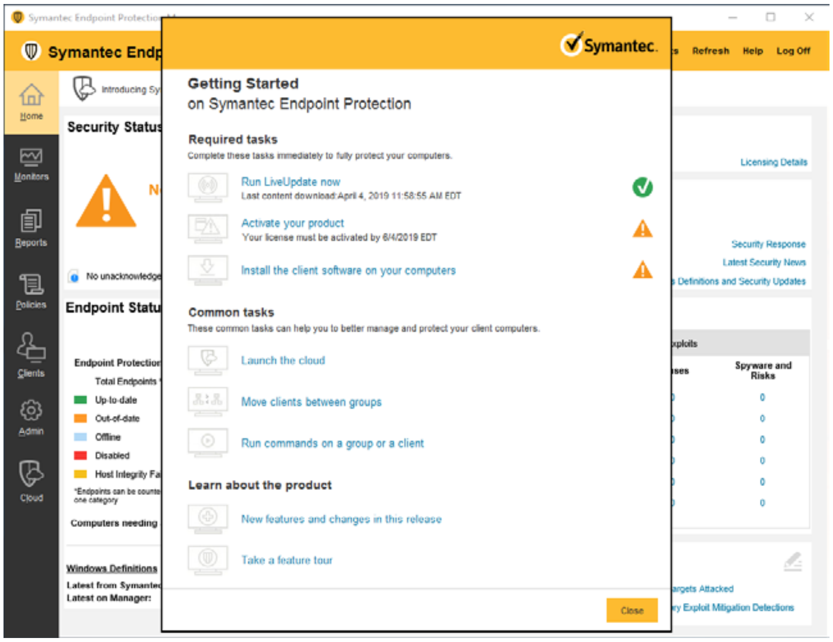


Symantec Endpoint Protection Host Windows Installation

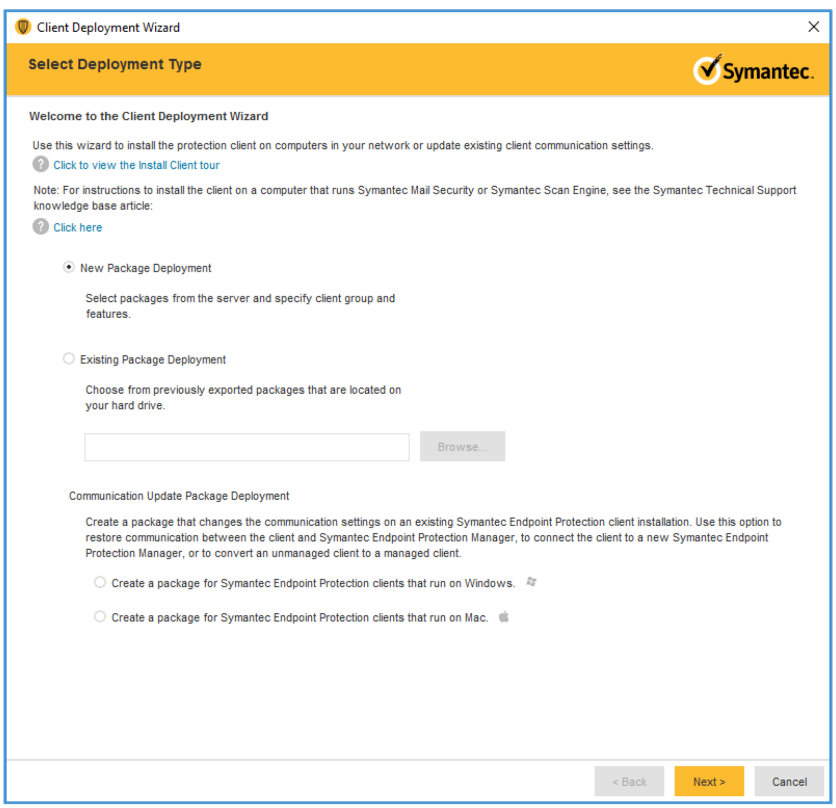
1. Launch the **Symantec Endpoint Protection Manager** and log in as the **admin**.



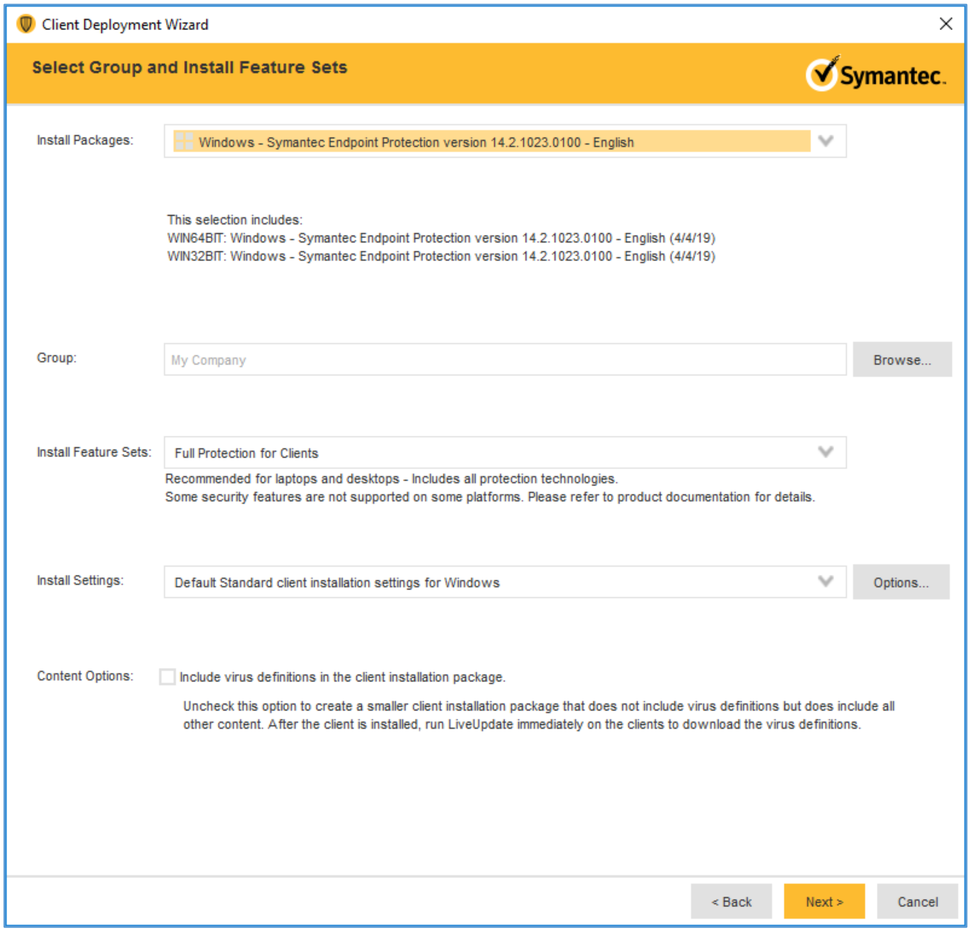
2. Select **Install the client software on your computers** from the **Getting Started** screen.



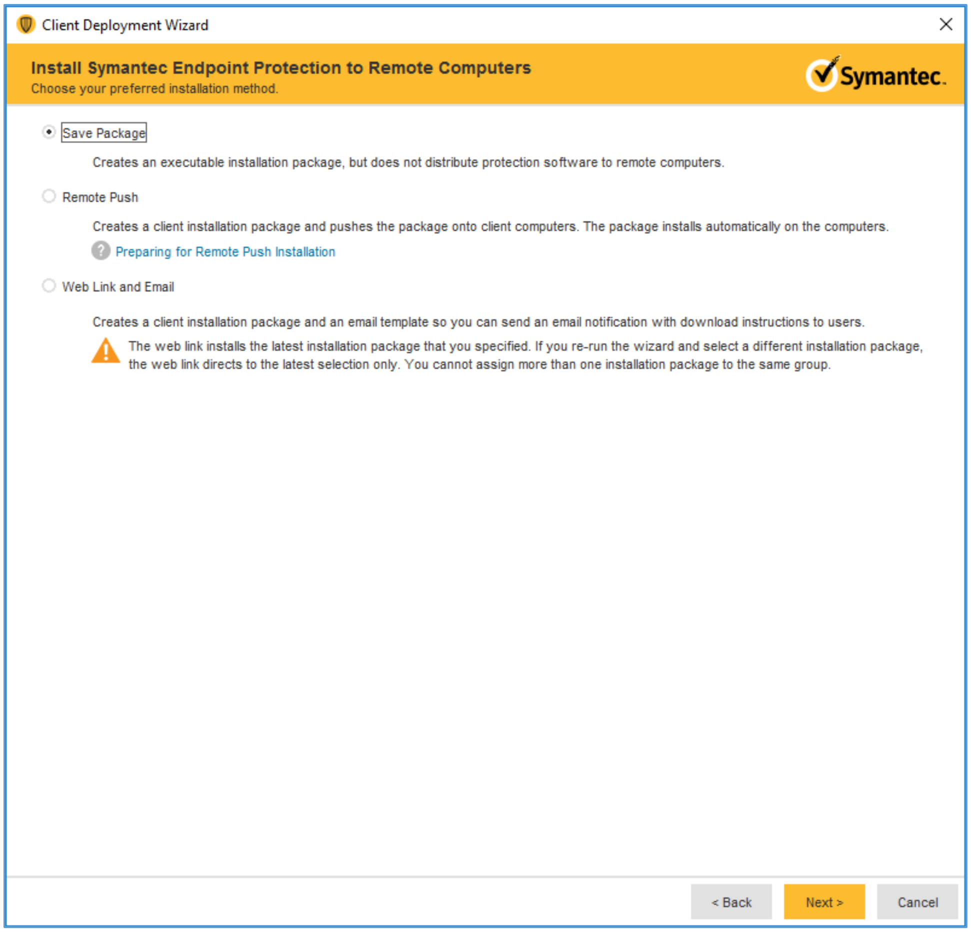
3. Confirm that **New Package Deployment** is checked and click **Next >**.



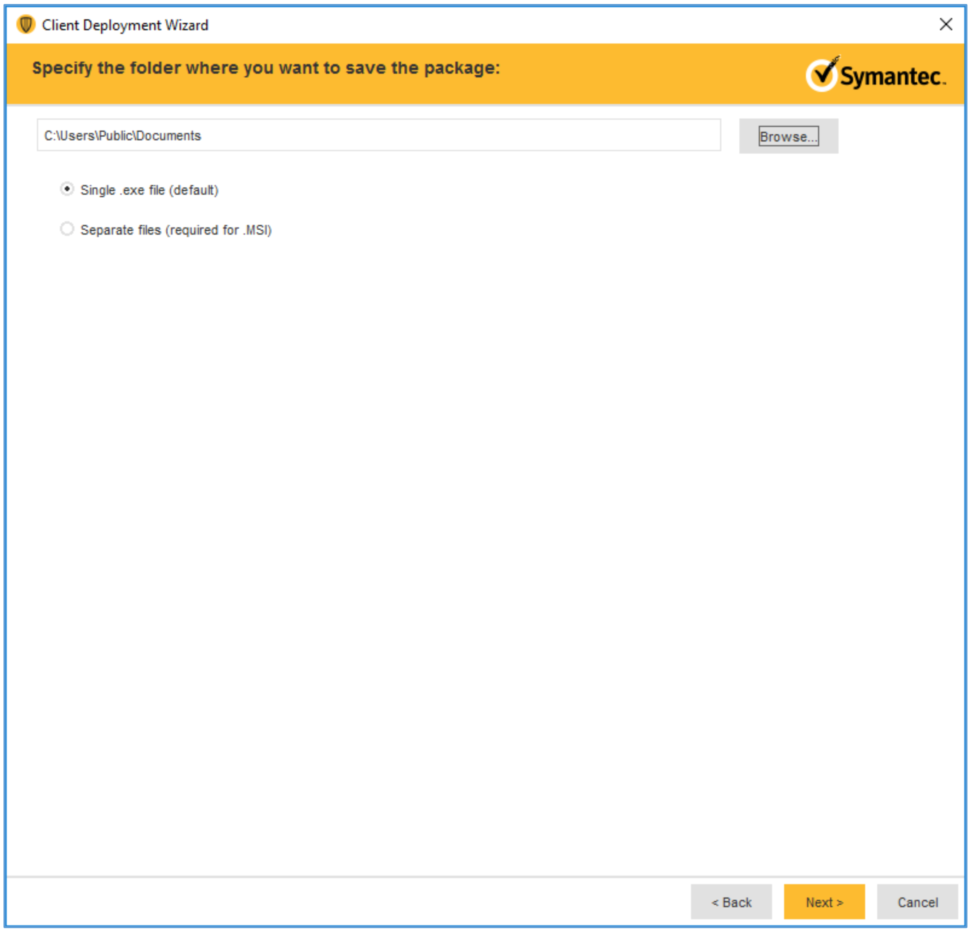
4. Confirm the settings Install Packages: **Windows - Symantec Endpoint Protection version 14.2.1023.0100 - English**, Group: **My Company**, Install Feature Sets: **Full Protection for Clients**, Install Settings: **Default Standard client installation settings for Windows**. Click **Next >**.



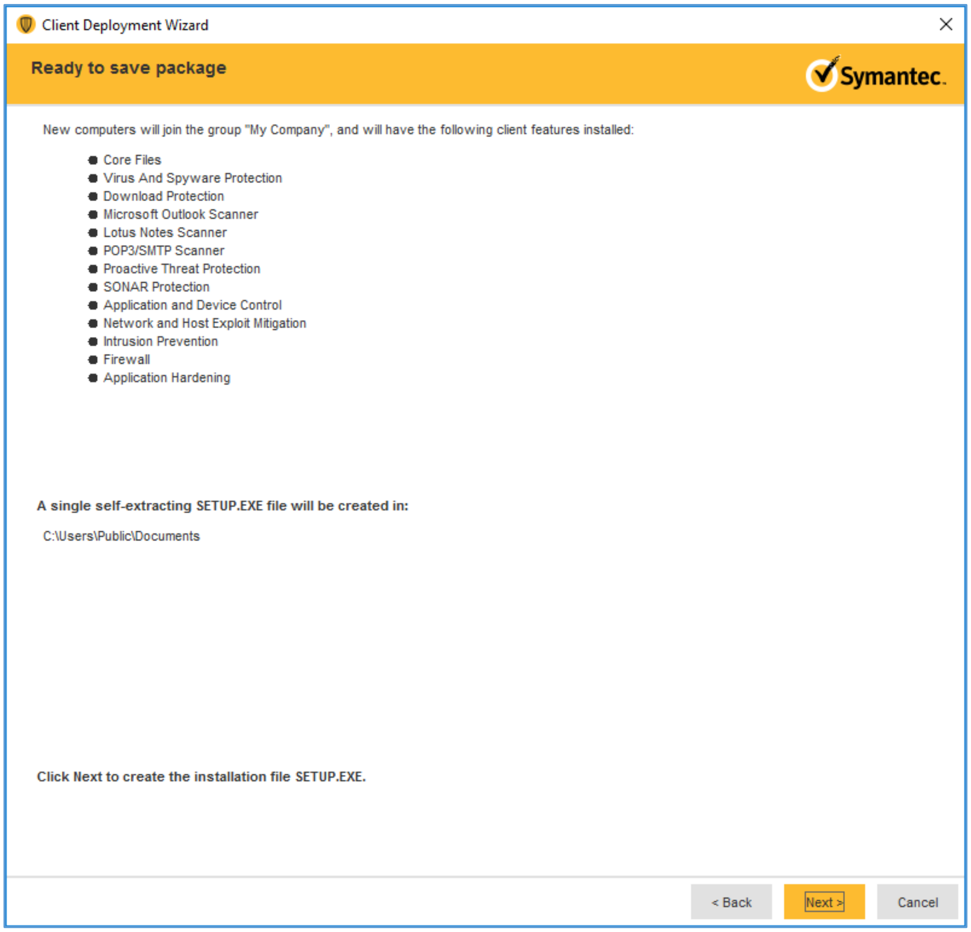
5. Confirm that **Save Package** is selected and click **Next >**.



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



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



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

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

2.9 Data Security

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

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

2.10 Secure Remote Access

2.10.1 TDi Technologies ConsoleWorks

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

System Requirements

CPU: 1

Memory: 8 GB RAM

Storage: 40 GB

Operating System: CentOS 7

Network Adapter: VLAN 1097

TDi ConsoleWorks Installation

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

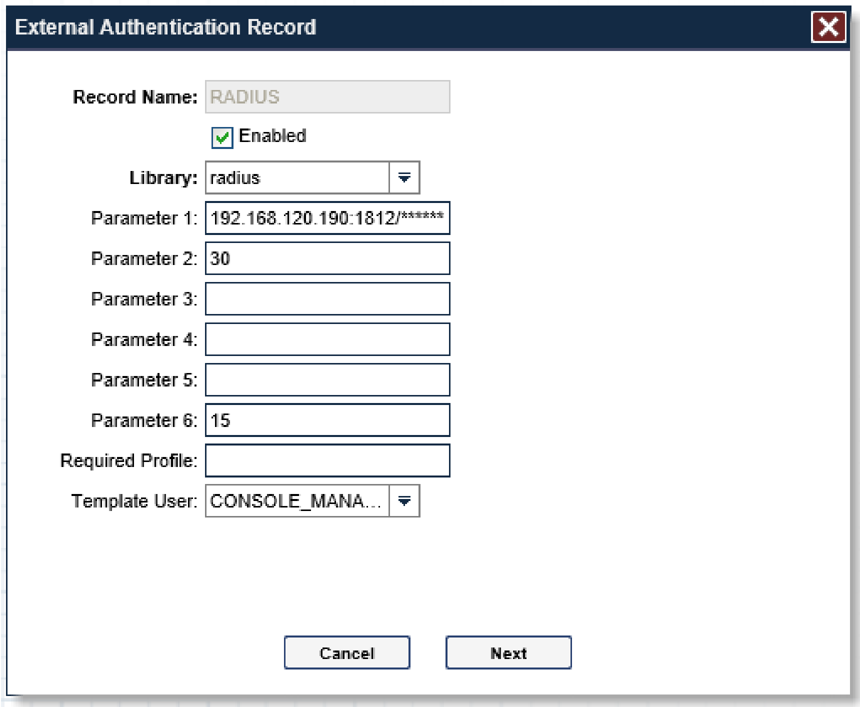
TDi ConsoleWorks Radius Authentication Configuration

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

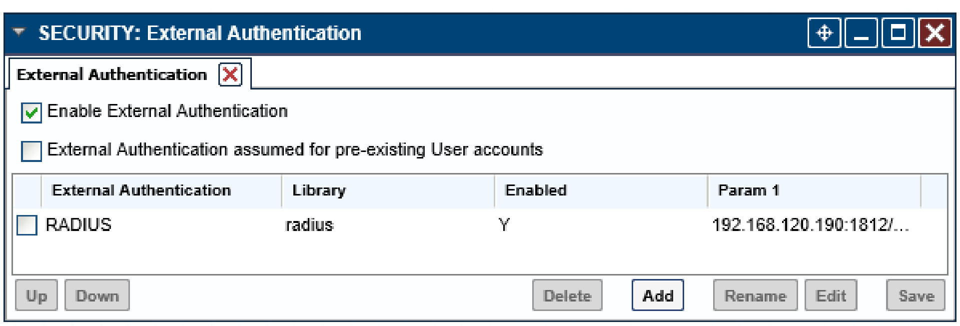
1. Download *extern_auth_radius.so* file from ConsoleWorks support site [20].
2. Move *extern_auth_radius.so* file to */opt/ConsoleWorks/bin* directory.
3. Restart ConsoleWorks by executing *cw_stop* and *cw_start* scripts located in the */opt/ConsoleWorks/bin* directory.
4. From the ConsoleWorks web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

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

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



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



2.10.2 Symantec Validation and ID Protection (VIP)

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

System Requirements

CPU: 4

Memory: 8192MB RAM

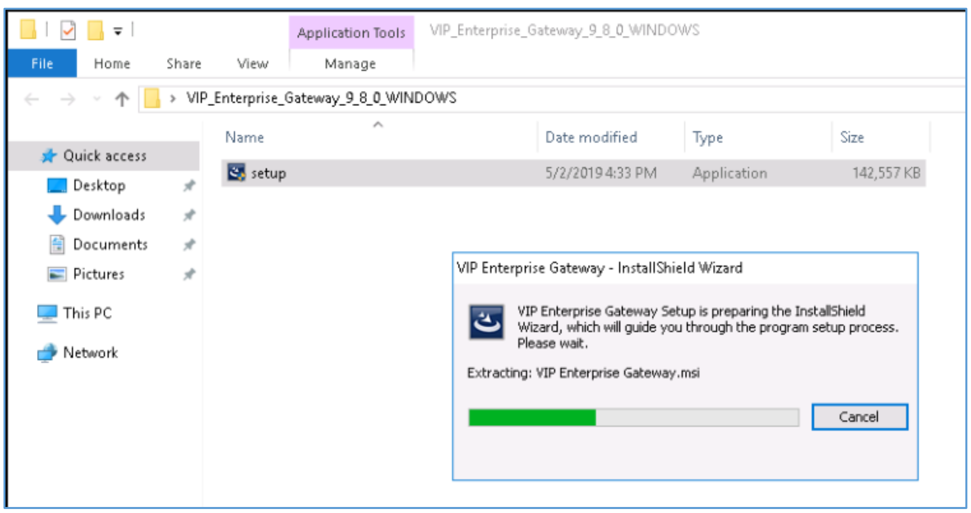
Storage: 240GB (thin provisioned)

Operating System: Microsoft Windows Server 2016

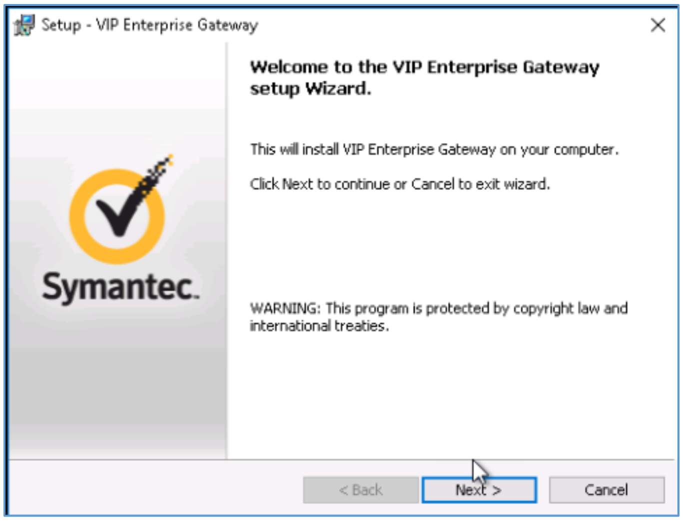
Network Adapter: VLAN 1201

Symantec VIP Installation

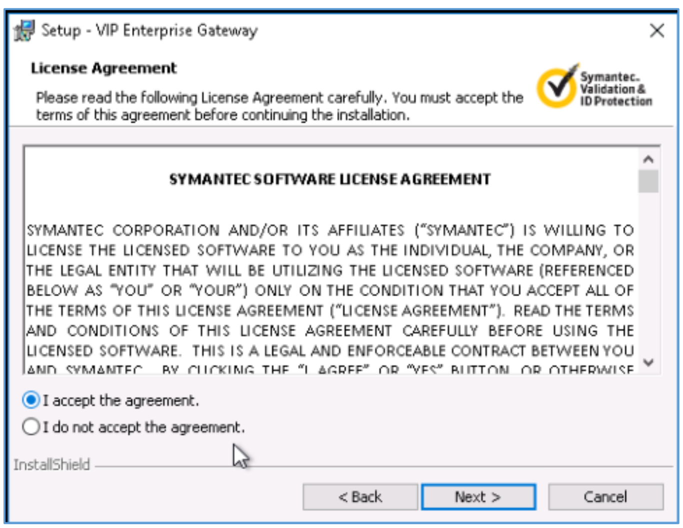
1. Right click on the *setup.exe* file for VIP Enterprise Gateway 9.8.0; select **Run as administrator**.



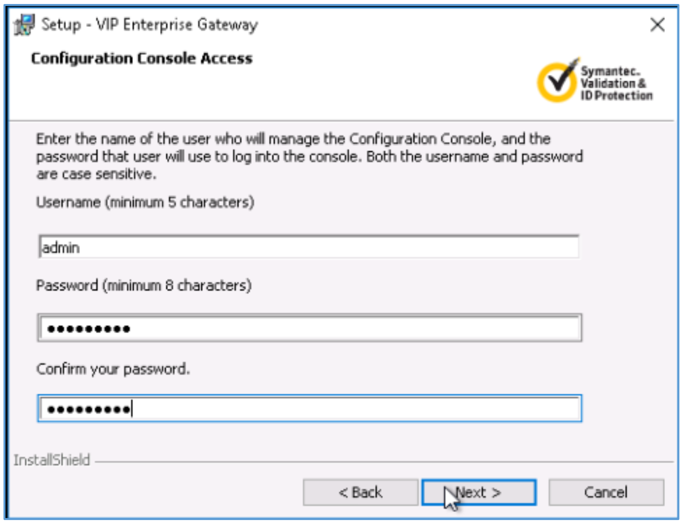
2. Proceed through the install wizard by clicking **Next >**.



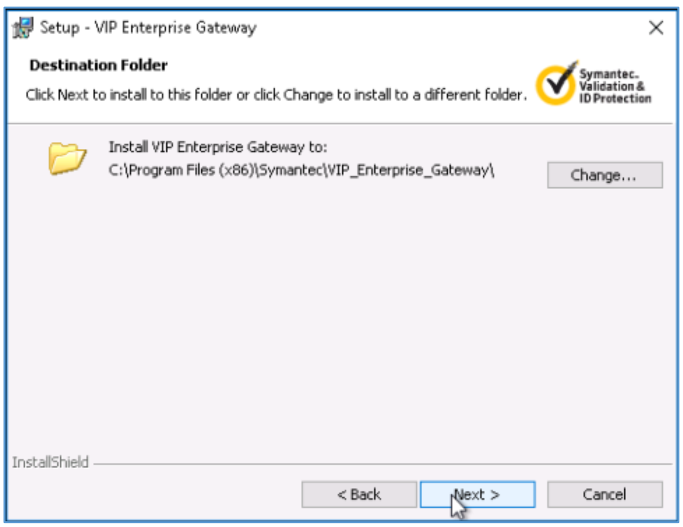
3. Check **I accept the agreement**.
4. Click **Next >**.



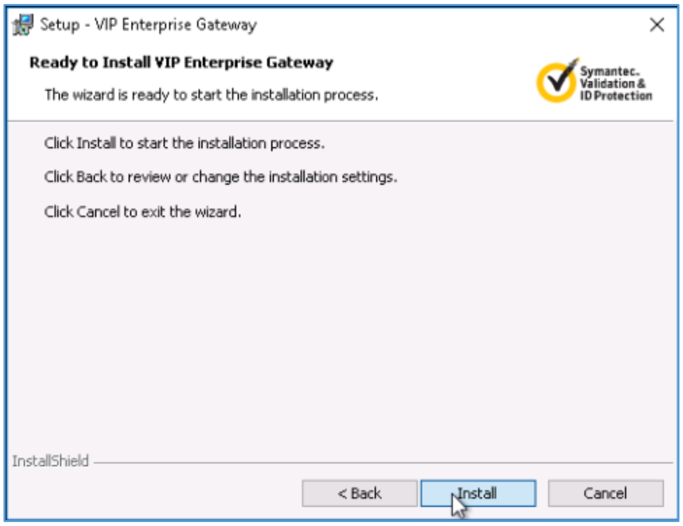
5. Create a **username** as **admin** and **password** and click **Next >**.



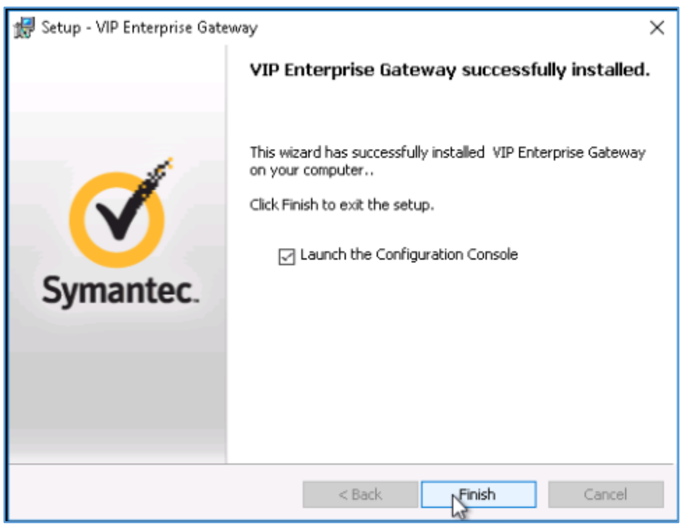
6. Keep the default installation location by clicking **Next >**.



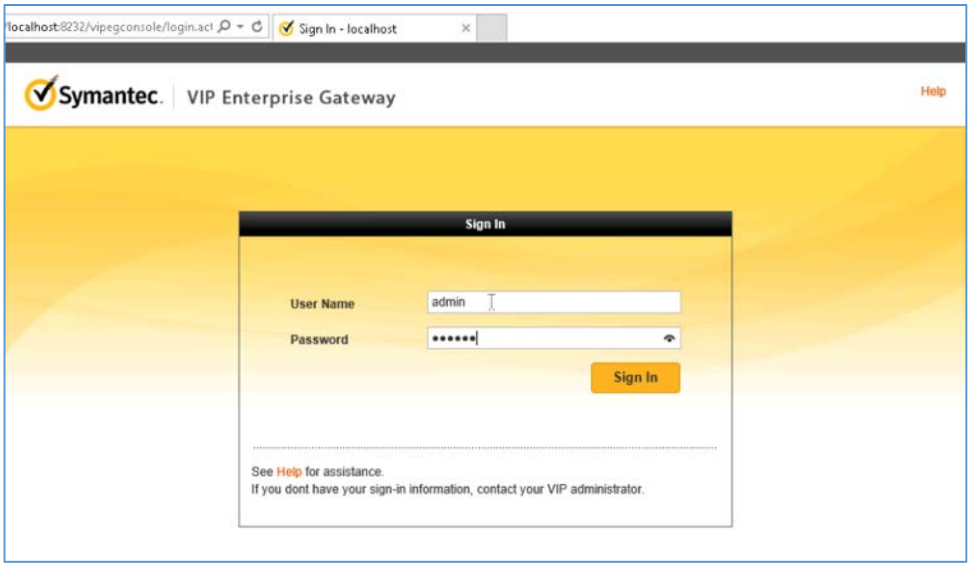
7. Click **Install**.



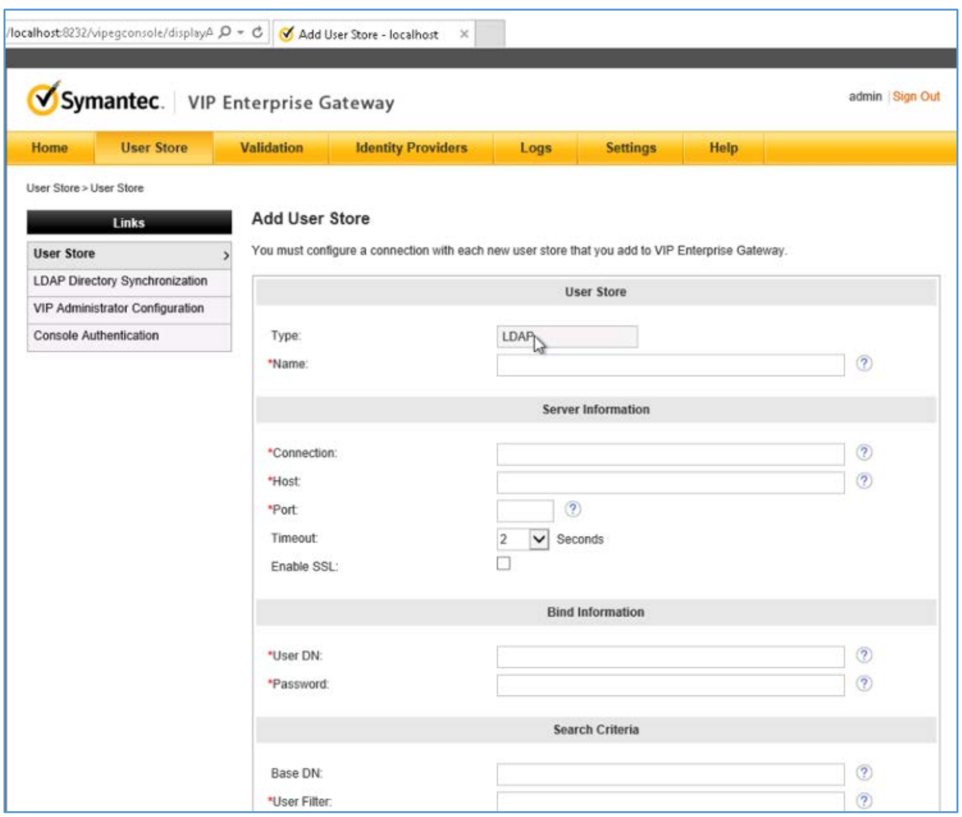
8. Click **Finish** after installer is complete.



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.

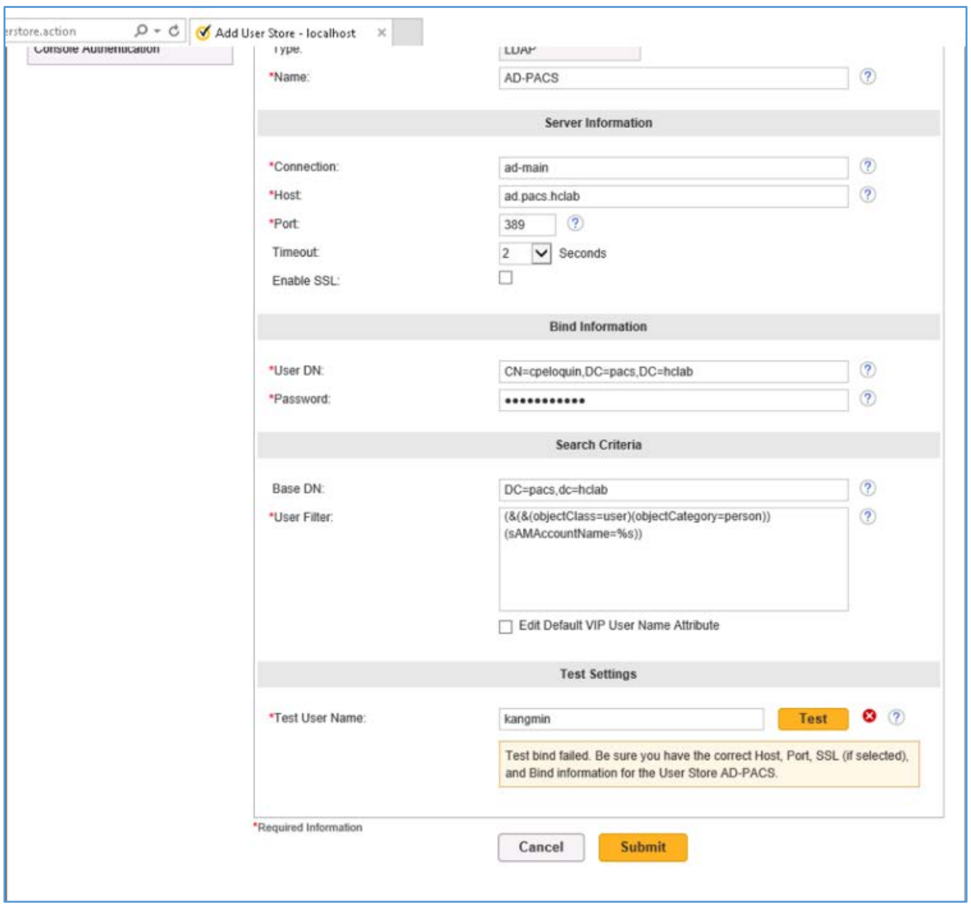


10. Select **User Store** from the menu bar.



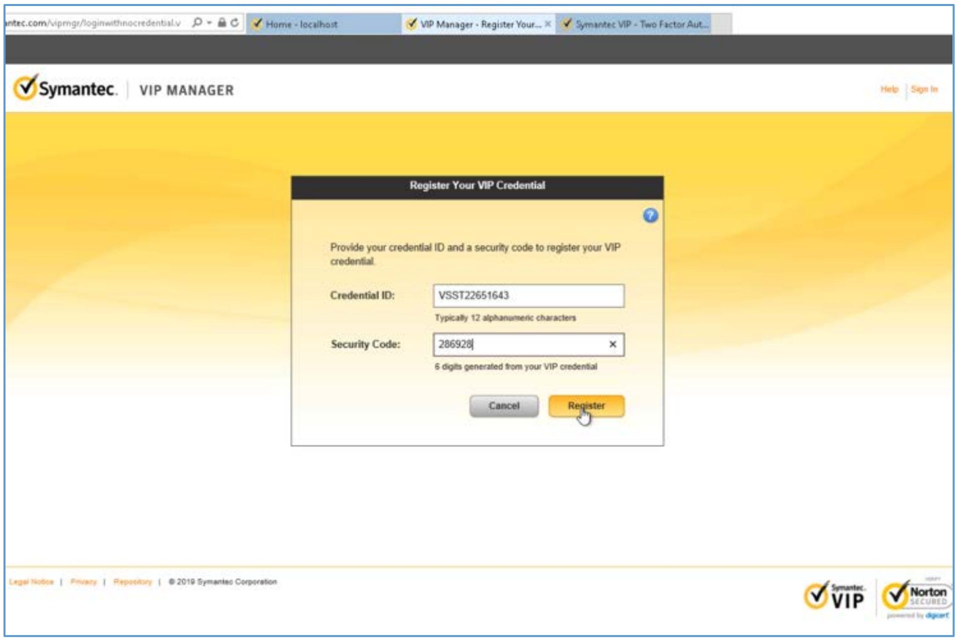
11. Add a user store with the following information:

- **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))(sAMAcountName=%s))

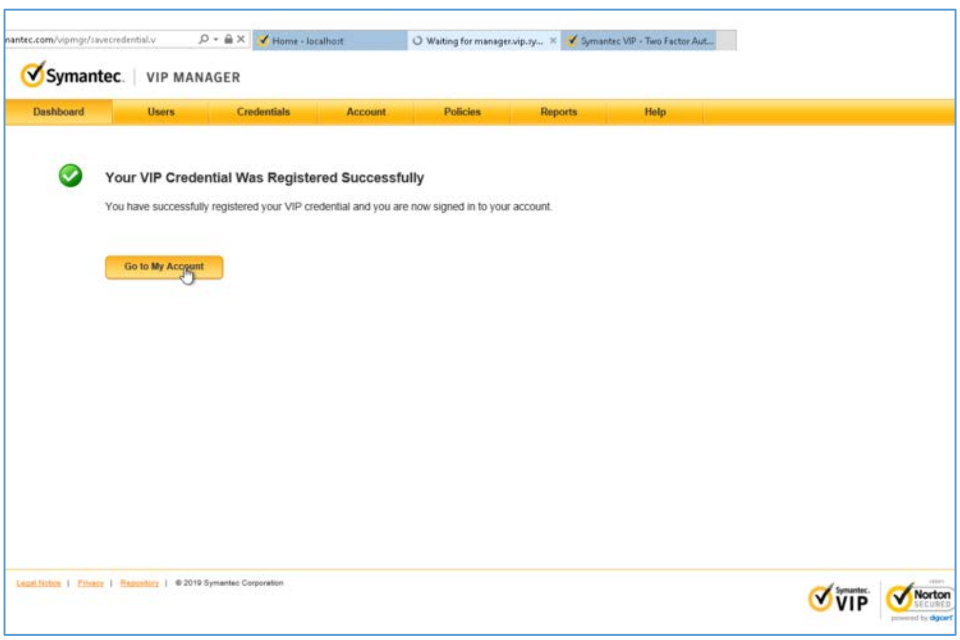


12. Log into VIP Manager by navigating to *https://manager.vip.symantec.com/vipmgr*. Use the account provided by Symantec.

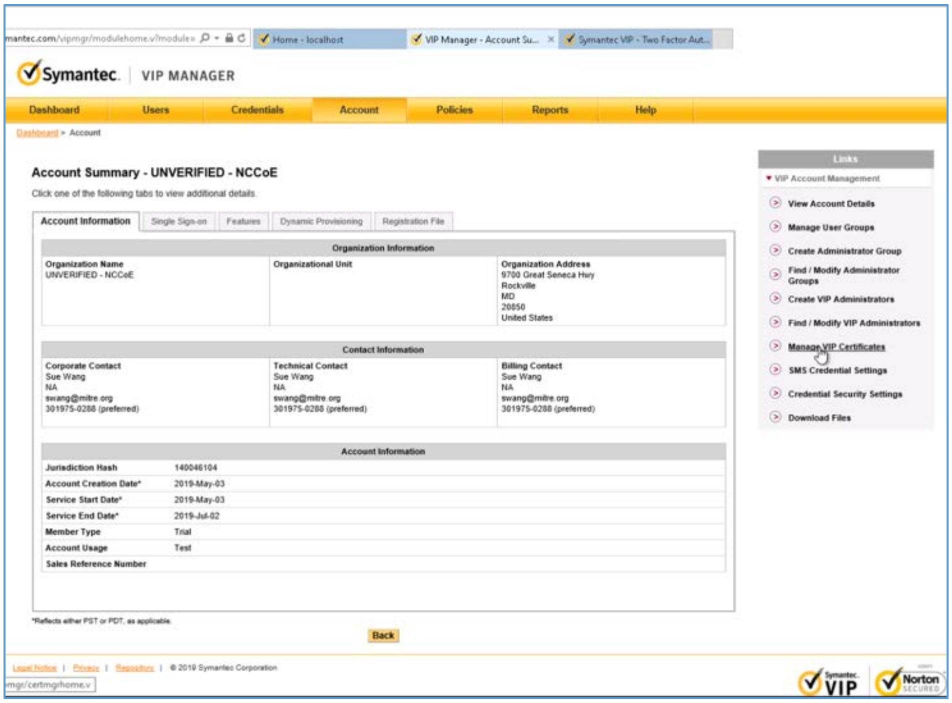
13. Select **Register Your VIP Credential**. Provide **the Credential ID** and **Security Code** of your credentials. Credentials can be downloaded by navigating to https://vip.symantec.com/.



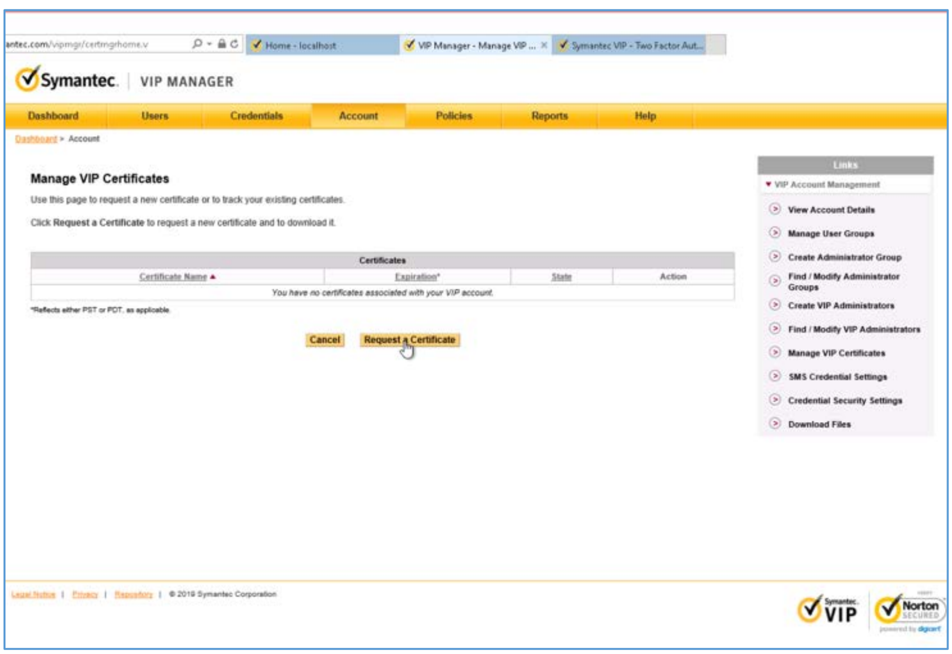
14. After registering the credential, select **Go to My Account**.



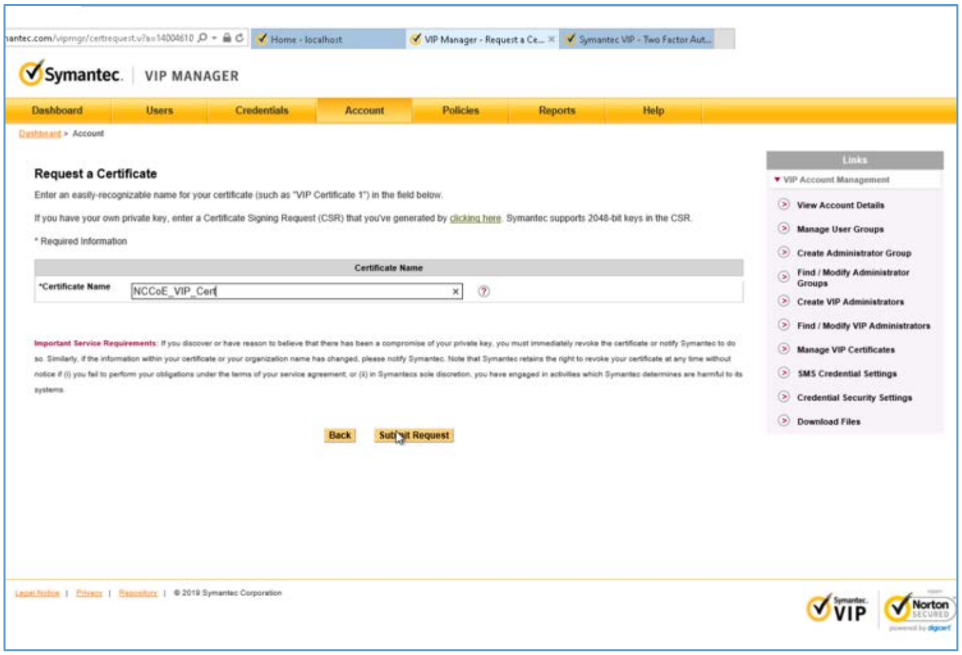
15. Select **Account** from menu bar, then select **Manage VIP Credentials**.



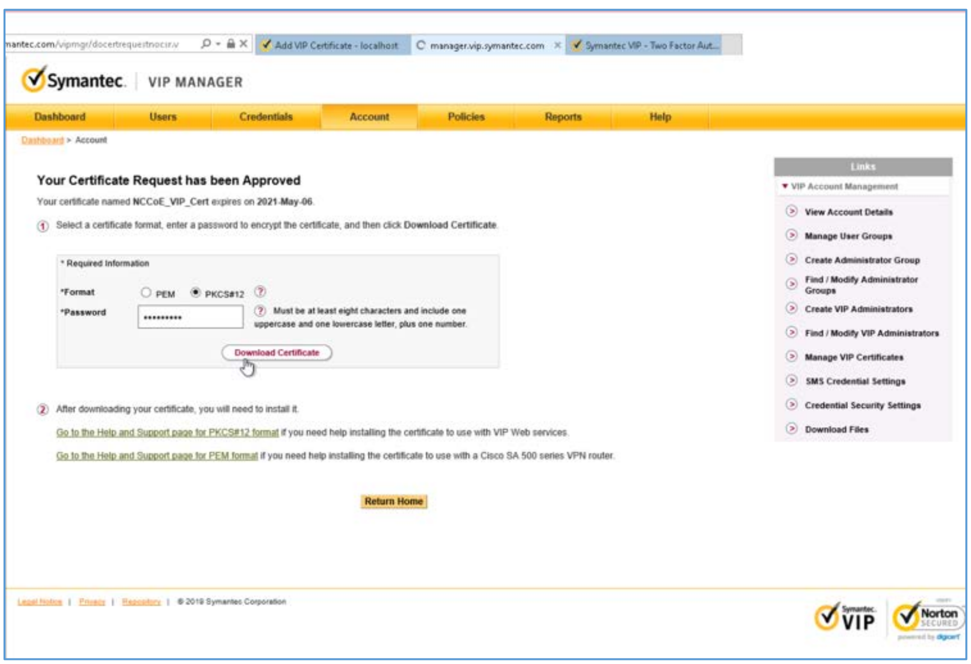
16. Select **Request a Certificate**.



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

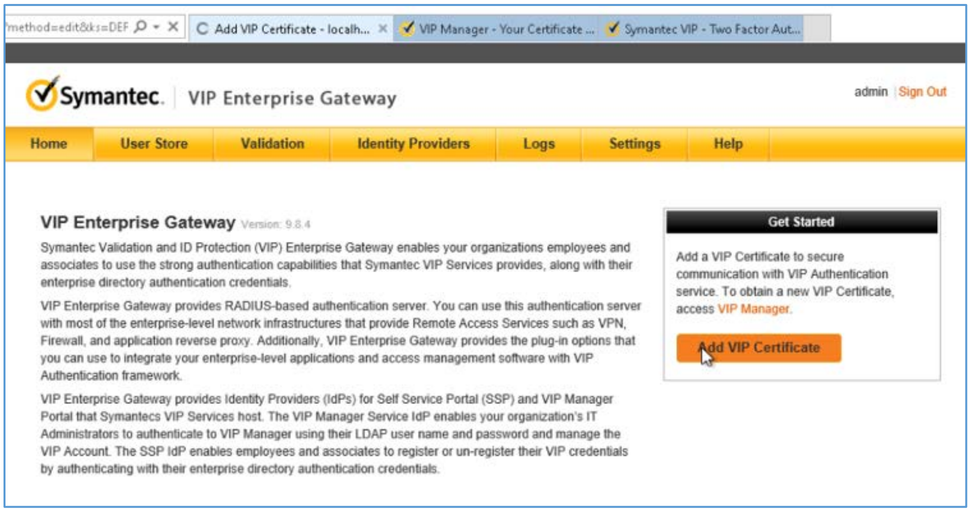


18. Select **PKCS#12 format** and create a password for the requested certificate. Then select **Download Certificate**.

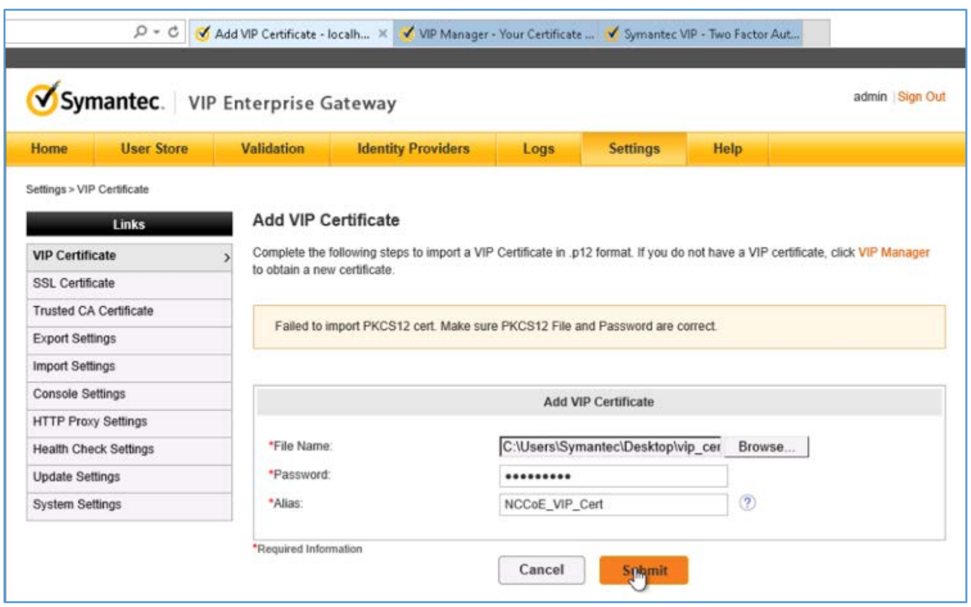


19. Save the certificate on the Symantec VIP local machine.

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



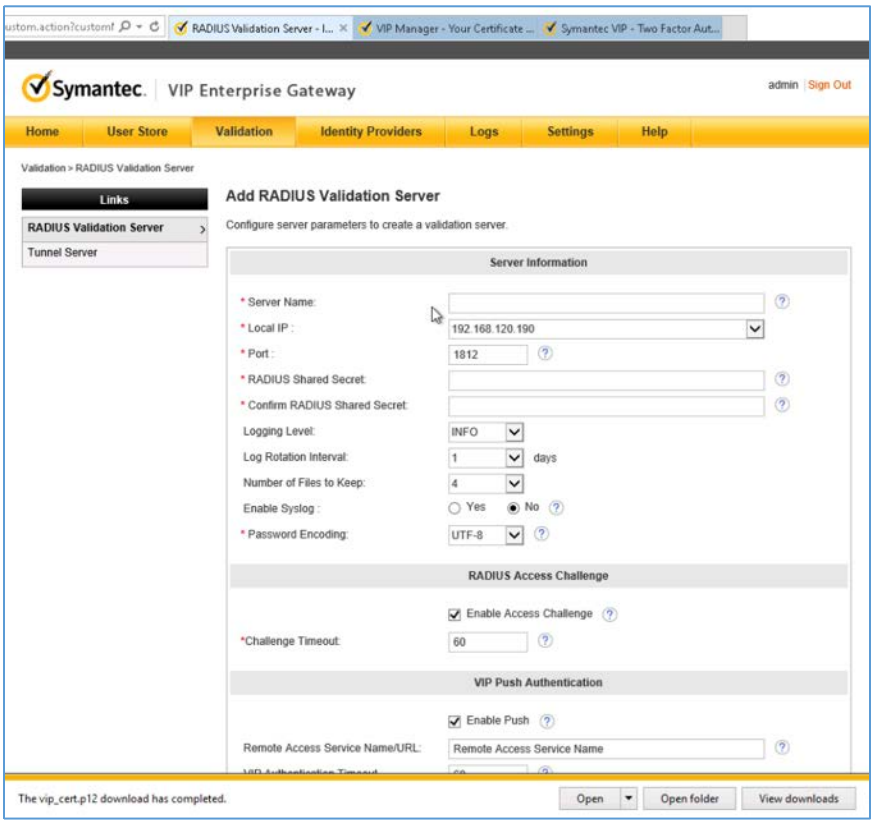
21. Select **Browse** and upload the certificate from the previous step. Enter the correct password and alias for the certificate, then click **Submit**.



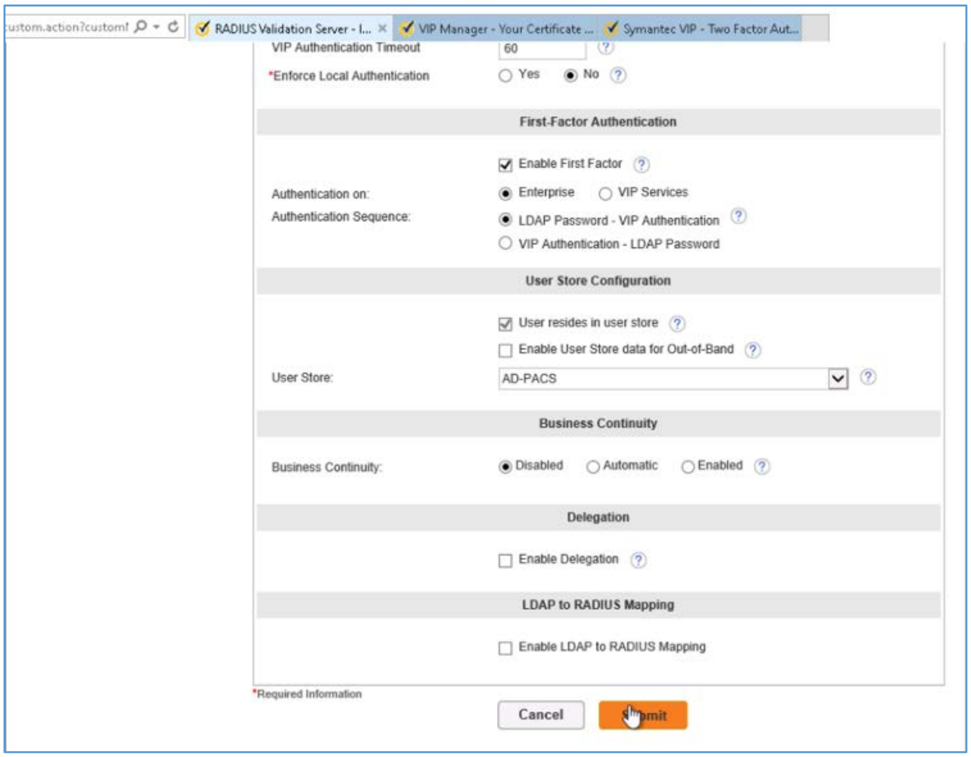
22. Select Validation from the menu bar, select Custom configuration, and provide the information that follows:

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

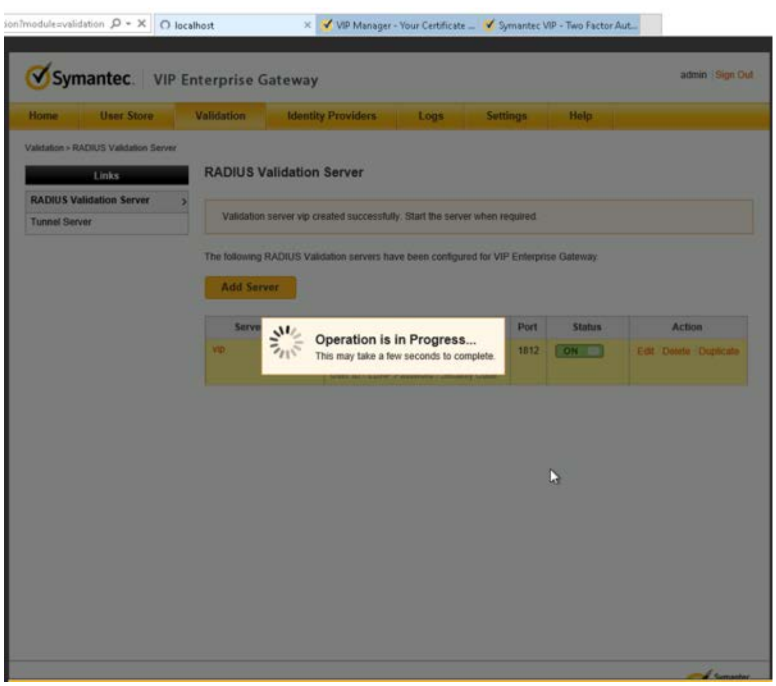
- **Port**: 1812
- **RADIUS Shared Secret**: *****
- **Confirm RADIUS Shared Secret:** *****
- **Enable First Factor:** *Checked*
- **Authentication on:** Enterprise
- **Authentication Sequence:** *LDAP Password – VIP Authentication*
- **User Store:** AD PACS



23. Click **Submit**.



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



Appendix A List of Acronyms

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

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

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

Appendix B References

[1] ORACLE. Java SE 6 Downloads. [Website]. Available: https://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html

[2] Red Hat. JBoss Application Server Downloads. [Website]. Available: https://jbossas.jboss.org/downloads.

[3] dcm4che.org Wiki. PostgreSQL Installation. [Website]. Available: https://dcm4che.atlassian.net/wiki/spaces/ee2/pages/2556071/PostgreSQL.

[4] EDB POSTGRES. PostgreSQL Database Download. [Website]. Available: https://www.enterprisedb.com/downloads/postgres-postgresql-downloads.

[5] Dcm4che.org Wiki. Installation. [Website]. Available: https://dcm4che.atlassian.net/wiki/spaces/ee2/pages/2555918/Installation.

[6] SourceForge. dcm4che, a DICOM Implementation in JAVA. [Website]. Available: https://sourceforge.net/projects/dcm4che/files/dcm4chee/.

[7] SourceForge. dcm4che, a DICOM Implementation in JAVA. [Website]. Available: https://sourceforge.net/projects/dcm4che/files/dcm4chee-arr/3.0.11.

[8] SourceForge. dcm4che, a DICOM Implementation in JAVA. [Website]. Available: https://sourceforge.net/projects/dcm4che/files/Oviyam/.

[9] Microsoft Docs. Install SQL Server from the Installation Wizard (Setup). [Website]. Available: https://docs.microsoft.com/en-us/sql/database-engine/install-windows/install-sql-server-from-the-installation-wizard-setup?view=sql-server-2017.

[10] T. Polk et al., *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Revision 1, NIST, Gaithersburg, Md., Apr. 2014. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf.

[11] DVTk. DVTk open source project main contributors ICT Group and Philips. [Website]. Available: https://www.dvtk.org/.

[12] Microsoft TechNet. *Building Your First Domain Controller on 2012 R2*. [Website]. Available: https://social.technet.microsoft.com/wiki/contents/articles/22622.building-your-first-domain-controller-on-2012-r2.aspx.

[13] Microsoft TechNet. *Installing and Configuring DHCP role on Windows Server 2012*. [Website]. Available: https://blogs.technet.microsoft.com/teamdhcp/2012/08/31/installing-and-configuring-dhcp-role-on-windows-server-2012/.

[14] *DigiCert.* CSR Creation Instructions for Microsoft Servers. [Website]. Available: https://www.digicert.com/util/csr-creation-microsoft-servers-using-digicert-utility.htm.

[15] Cisco. *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*. [Website]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/fmcv/FMCv-quick.html.

[16] *Cisco. Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide*. [Website]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg.html.

[17] Cisco Systems, Inc. *Basic Policy Creation for Firepower*. Jan. 30, 2019 [Online]. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/firepower/Self-Help/Basic_Policy_Creation_on_Cisco_Firepower_Devices.pdf.

[18] Cisco Systems, Inc. *Cisco Stealthwatch Installation and Configuration Guide 7.0*. 2019 [Online]. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_0_0_Installation_and_Configuration_Guide_DV_3_1.pdf.

[19] G. O'Brien et al., *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations,* NIST SP 1800-8, NIST, Gaithersburg, Md., Aug. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-wip-nist-sp1800-8.pdf.

[20] *External Authentication libraries*, ConsoleWorks Cybersecurity Operations Platform [Website]. Available: https://support.tditechnologies.com/content/external-authentication-libraries.