NIST SPECIAL PUBLICATION 1800-30

Securing Telehealth Remote Patient Monitoring Ecosystem

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

Jennifer Cawthra*
Nakia Grayson
Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Julie Snyder
Sue Wang
Ryan Williams
Kangmin Zheng

*Former employee; all work for this publication done while at employer.

SECOND DRAFT

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

NIST SPECIAL PUBLICATION 1800-30

Securing Telehealth Remote Patient Monitoring Ecosystem

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

Jennifer Cawthra*
Nakia Grayson
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Julie Snyder
Sue Wang
Ryan Williams
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

*Former employee; all work for this publication done while at employer.

SECOND DRAFT

May 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Acting NIST Director and Acting Under Secretary of Commerce for Standards and Technology

NIST SPECIAL PUBLICATION 1800-30A

Securing Telehealth Remote Patient Monitoring Ecosystem

Volume A:
Executive Summary

Jennifer Cawthra*
Nakia Grayson
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Sue Wang
Ryan Williams
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

*Former employee; all work for this publication done while at employer.

May 2021

SECOND DRAFT

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

Executive Summary

WHY WE WROTE THIS GUIDE

Increasingly, healthcare delivery organizations (HDOs) are relying on telehealth and remote patient monitoring (RPM) capabilities to treat patients at home. RPM is convenient and cost-effective, and since the onset of the COVID-19 pandemic, its adoption rate has rapidly increased. Without adequate privacy and cybersecurity measures, however, unauthorized individuals may expose sensitive data or disrupt patient monitoring services. In collaboration with industry partners, the National Cybersecurity Center of Excellence (NCCoE) built a laboratory environment to demonstrate how HDOs can implement cybersecurity and privacy controls to enhance telehealth RPM resiliency.

CHALLENGE

RPM solutions engage multiple actors as participants in patients' clinical care—HDOs, telehealth platform providers, and the patients themselves. Each participant uses, manages, and maintains different technology components within an interconnected ecosystem. Each actor must be responsible for safeguarding against unique threats and risks associated with RPM technologies within their purview.

This practice guide assumes that the HDO engages with a telehealth platform provider that is a separate entity from the HDO and patient. The telehealth platform provider manages a distinct infrastructure, applications, and set of services. The telehealth platform provider coordinates with the HDO to provision, configure, and deploy the RPM components to the patient home and assures secure communication between the patient and clinician.

Patients and patient families are involved in this ecosystem. The patient will receive equipment that may include biometric devices, a communications device (tablet or mobile phone), or workstations from the telehealth platform provider. While the telehealth platform provider manages the equipment, the patient may need to provide internet connectivity and be responsible for physically managing the provided equipment.

SOLUTION

The NCCoE collaborated with healthcare, technology, and telehealth partners to build a distributed RPM solution. The RPM solution implemented controls that safeguard the HDO environment and documented approaches that the telehealth platform provider addresses. Telehealth platform providers assure that RPM components are isolated within the patient home environment. The telehealth platform provider assures end-to-end data security between the patient and the HDO.

Technology solutions alone may not be sufficient to maintain privacy and security controls on external environments. This practice guide notes the involvement of people, process, and technology as necessary to implement a holistic risk mitigation strategy.

This practice guide can help your organization:

- assure confidentiality, integrity, and availability of an RPM solution

- enhance patient privacy
- limit HDO risk when implementing an RPM solution

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

HOW TO USE THIS GUIDE

This guide contains three volumes:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-30A: *Executive Summary*—why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-30B: *Approach, Architecture, and Security Characteristics*—what we built and why, including the risk analysis performed and the security/privacy control map
- NIST SP 1800-30C: *How-To Guides*—instructions for building the example implementation, including all the details that would allow one to replicate all or parts of this project

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth. 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.

COLLABORATORS

Collaborators 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). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or 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.

NIST SPECIAL PUBLICATION 1800-30B

Securing Telehealth Remote Patient Monitoring Ecosystem

Volume B:
Approach, Architecture, and Security Characteristics

Jennifer Cawthra*
Nakia Grayson
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Julie Snyder
Sue Wang
Ryan Williams
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

*Former employee; all work for this publication done while at employer.

May 2021

SECOND DRAFT

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DISCLAIMER

National Institute of Standards and Technology Special Publication 1800-30B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-30B, 214 pages, (May 2021), 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: May 6, 2021 through June 7, 2021

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Increasingly, healthcare delivery organizations (HDOs) are relying on telehealth and remote patient monitoring (RPM) capabilities to treat patients at home. RPM is convenient and cost-effective, and its adoption rate has increased. However, without adequate privacy and cybersecurity measures, unauthorized individuals may expose sensitive data or disrupt patient monitoring services.

RPM solutions engage multiple actors as participants in patients' clinical care. These actors include HDOs, telehealth platform providers, and the patients themselves. Each participant uses, manages, and maintains different technology components within an interconnected ecosystem, and each is

responsible for safeguarding their piece against unique threats and risks associated with RPM technologies.

This practice guide assumes that the HDO engages with a telehealth platform provider that is a separate entity from the HDO and patient. The telehealth platform provider manages a distinct infrastructure, applications, and set of services. The telehealth platform provider coordinates with the HDO to provision, configure, and deploy the RPM components to the patient home and assures secure communication between the patient and clinician.

The NCCoE analyzed risk factors regarding an RPM ecosystem by using risk assessment based on the NIST Risk Management Framework. The NCCoE also leveraged the NIST Cybersecurity Framework, *NIST Privacy Framework,* and other relevant standards to identify measures to safeguard the ecosystem. In collaboration with healthcare, technology, and telehealth partners, the NCCoE built an RPM ecosystem in a laboratory environment to explore methods to improve the cybersecurity of an RPM.

Technology solutions alone may not be sufficient to maintain privacy and security controls on external environments. This practice guide notes the application of people, process, and technology as necessary to implement a holistic risk mitigation strategy.

This practice guide's capabilities include helping organizations assure the confidentiality, integrity, and availability of an RPM solution, enhancing patient privacy, and limiting HDO risk when implementing an RPM solution.

KEYWORDS

access control; authentication; authorization; behavioral analytics; cloud storage; data privacy; data security; encryption; HDO; healthcare; healthcare delivery organization; remote patient monitoring; RPM; telehealth; zero trust

ACKNOWLEDGMENTS

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

Name	Organization
Alex Mohseni	Accuhealth
Stephen Samson	Accuhealth
Brian Butler	Cisco

Name	Organization
Matthew Hyatt	Cisco
Kevin McFadden	Cisco
Peter Romness	Cisco
Brad Hoehn	Huntington Ingalls Industries-Mission Driven Innovative Solutions (HII-MDIS)
David Lemire	Huntington Ingalls Industries-Mission Driven Innovative Solutions (HII-MDIS)
Steven Dean	Inova Health System
Zach Furness	Inova Health System
James Carder	LogRhythm
Brian Coulson	LogRhythm
Steven Forsyth	LogRhythm
Jake Haldeman	LogRhythm
Andrew Hollister	LogRhythm
Zack Hollister	LogRhythm
Dan Kaiser	LogRhythm
Sally Vincent	LogRhythm
Vidya Murthy	MedCrypt
Axel Wirth	MedCrypt

Name	Organization
Stephanie Domas	MedSec
Garrett Sipple	MedSec
Nancy Correll	The MITRE Corporation
Spike Dog	The MITRE Corporation
Robin Drake	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Donald Faatz	The MITRE Corporation
Nedu Irrechukwu	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Stuart Shapiro	The MITRE Corporation
Barbara Cuthill	NIST
Jeffrey Marron	NIST
Paul Watrobski	NIST
John Dwyier	Onclave Networks, Inc. (Onclave)
Chris Grodzickyj	Onclave
Marianne Meins	Onclave
Dennis Perry	Onclave
Christina Phillips	Onclave

Name	Organization
Robert Schwendinger	Onclave
James Taylor	Onclave
Chris Jensen	Tenable
Joshua Moll	Tenable
Jeremiah Stallcup	Tenable
Rebecca Herold	The Privacy Professor Consultancy
Julio C. Cespedes	The University of Mississippi Medical Center
Saurabh Chandra	The University of Mississippi Medical Center
Donald Clark	The University of Mississippi Medical Center
Alan Jones	The University of Mississippi Medical Center
Kristy Simms	The University of Mississippi Medical Center
Richard Summers	The University of Mississippi Medical Center
Steve Waite	The University of Mississippi Medical Center
Dele Atunrase	Vivify Health
Aaron Gatz	Vivify Health
Michael Hawkins	Vivify Health
Robin Hill	Vivify Health
Dennis Leonard	Vivify Health

Name	Organization
David Norman	Vivify Health
Bill Paschall	Vivify Health
Eric Rock	Vivify Health
Alan Stryker	Vivify Health
Dave Sutherland	Vivify Health
Michael Tayler	Vivify Health

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
Accuhealth	Accuhealth Evelyn
Cisco	Cisco Firepower Version 6.3.0 Cisco Umbrella Cisco Stealthwatch Version 7.0.0
Inova Health System	subject matter expertise
LogRhythm	LogRhythm XDR Version 7.4.9 LogRhythm NetworkXDR Version 4.0.2
MedCrypt	subject matter expertise
MedSec	subject matter expertise

Technology Partner/Collaborator	Build Involvement
Onclave	Onclave Zero Trust Platform Version 1.1.0
Tenable	Tenable.sc Vulnerability Management Version 5.13.0 with Nessus
The University of Mississippi Medical Center	subject matter expertise
Vivify Health	Vivify Pathways Home Vivify Pathways Care Team Portal

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: hit_nccoe@nist.gov

Contents

List of Figures

List of Tables

1 Summary

This practice guide demonstrates how healthcare delivery organizations (HDOs) can implement cybersecurity and privacy controls to enhance the resiliency of telehealth services. In collaboration with industry partners, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to simulate the telehealth ecosystem and enable remote patient monitoring (RPM) services for patients.

RPM is convenient, cost-effective, and growing, but it comes with security and privacy risks. Patient monitoring systems are often found in healthcare facilities, in controlled environments. RPM is different in that monitoring equipment is deployed in the patient’s home, which may not offer the same level of cybersecurity or physical security control to prevent misuse or compromise. Without privacy or cybersecurity controls in place within the RPM ecosystem, patient data and the ability to communicate with the care providers may be compromised.

This practice guide explores a situation in which a care provider prescribes deploying an RPM device to the patient home. The RPM device captures biometric data on regular intervals, conveys the data to the clinical care team, and allows patient-clinician communication without the patient making an in-person visit to the HDO. RPM enables care based on the patient’s needs, regardless of geographic constraints.

Capturing biometric data at regular intervals allow clinicians to have broader insight into a patient’s condition. With larger data sets, clinicians can monitor the patient’s condition and make diagnosis and treatment decisions with more robust information. RPM solutions allow audio and video communication in addition to utilizing biometric data, and they support the patient-clinician relationship.

Implementing an RPM ecosystem involves multiple parties and environments. In developing the reference architecture for this practice guide, the NCCoE considered components that would be deployed in three distinct domains that encompass the RPM ecosystem: the patient home environment, the telehealth platform provider, and the HDO. The project team engaged with a telehealth platform provider that leveraged cloud services and facilitated audio- and videoconferencing between the patient home and the HDO. The telehealth platform provider provisioned and managed biometric devices that were deployed in the patient home, and routed data and communication between the patient home and the HDO.

The NCCoE built a laboratory environment to simulate the telehealth ecosystem, performed a risk assessment, and developed an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies and collaborate with telehealth platform providers to assure privacy and security biometric devices that are deployed to the patient home.

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 collaborators who participated in building, demonstrating, and documenting the solution.

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

Section 3, Approach, offers a detailed treatment of the scope of the project, 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 RPM 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 and Privacy Characteristic Analysis, provides details about the tools and techniques used to perform risk assessments pertaining to RPM.

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 5 controls demonstrated in the example implementation.

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

The appendixes provide acronym translations, references, a deeper dive into the threats and risks associated with RPM, the review of the NIST Privacy Risk Assessment Methodology (PRAM), and a list of additional informative security references cited in the framework.

1.1 Challenge

HDOs using remote patient monitoring solutions partner with third-party telehealth platform providers. Telehealth platform providers manage biometric devices delivered to and operated by patients. Patients transmit collected biometric data to the telehealth platform provider. The telehealth platform provider presents that data to clinical teams for interpretation and continued patient care. The reliance of external entities and the interaction of devices and data through multiple domains for the effective function of telehealth may expose the HDO and patient to security and privacy risks.

This practice guide addresses a scenario in which the HDO engages with a telehealth platform provider, which manages a distinct infrastructure, applications, and set of services. The telehealth platform provider coordinates with the HDO to provision, configure, and deploy the RPM components to the patient home and assures secure communication between the patient and clinician.

RPM devices are deployed in a networked patient home environment. The patient may have broadband internet connectivity, including Wi-Fi. RPM devices deployed in the patient home may include the biometric monitoring devices, a gateway interface device (tablet or mobile phone), or workstations from the telehealth platform provider. While the telehealth platform provider manages RPM devices, it does not manage the patient home network.

Without privacy or cybersecurity controls in place, patient data and the ability to communicate with the care providers may be compromised.

1.2 Solution

This NIST Cybersecurity Practice Guide, *Securing Telehealth Remote Patient Monitoring Ecosystem*, shows how biomedical engineers, networking engineers, security engineers, and IT professionals can help securely configure and deploy an RPM ecosystem by using commercially available tools and technologies that are consistent with cybersecurity standards.

The NCCoE worked with healthcare, technology, and telehealth collaborators to build a distributed RPM solution. The project team implemented controls, based on the NIST Cybersecurity and Privacy Frameworks, to safeguard the HDO, telehealth platform provider, and patient home environments. This practice guide documents approaches that the telehealth platform provider should consider, including assuring end-to-end data security between the patient and the HDO and that RPM biometric components are isolated within the patient home environment.

Any organization that deploys RPM can use the example implementation, which represents one of many possible solutions and architectures, but those organizations should perform their own risk assessment and implement controls based on their risk posture.

Technology solutions alone may not be sufficient to maintain privacy and security controls on external environments. This practice guide notes the application of people, process, and technology as necessary to implement a holistic risk mitigation strategy.

1.3 Benefits

The NCCoE's practice guide to *Securing Telehealth Remote Patient Monitoring Ecosystem* can help your organization:

- assure the confidentiality, integrity, and availability of an RPM solution
- enhance patient privacy
- limit HDO risk when implementing an RPM solution

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 replicate an RPM environment. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-30A: *Executive Summary*
- NIST SP 1800-30B: *Approach, Architecture, and Security Characteristics*–what we built and why **(you are here)**
- NIST SP 1800-30C: *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 1800-30A, which describes the following topics:

- challenges that enterprises face in securing the RPM ecosystem
- 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 1800-30B, 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 1800-30A, with your leadership team members to help them understand the importance of adopting standards-based commercially available technologies that can help secure the RPM 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 1800-30C, 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 re-create 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 in a distributed RPM 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 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 are in the List of Acronyms appendix.

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

RPM is a telehealth use case wherein healthcare providers can use internet-based technologies to track biometric data from the patient's home. Patients may have chronic or recurring health conditions that require regular clinical monitoring; however, in-person visitation is impractical or undesirable. Technology enables capturing biometric and patient-generated data, having that data relayed to systems that clinicians may use to evaluate a patient; and allows bidirectional communication between the patient and clinician. RPM may be an appropriate means for performing healthcare in pandemic scenarios or to address patients who may live in parts of the country where healthcare settings or practitioners are scarce.

The NCCoE collaborated with a healthcare Community of Interest (COI) that included technology and cybersecurity vendors, healthcare cybersecurity subject matter experts, and healthcare systems to identify RPM use cases, data workflows, ecosystem actor, and general deployment architecture. Further, with the assistance of the COI and external cybersecurity subject matter experts, a risk assessment was performed and reviewed, assuring the measures and outcomes that were determined from the risk assessment activity.

Additionally, this project reviewed NIST SP 800-171 Rev. 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organization*s [1]; as well as NIST SP 800-181 Rev. 1, *Workforce Framework for Cybersecurity (NICE Framework)* [2], 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 on the NIST Cybersecurity Framework [3], the NIST Risk Management Framework [4] and the *NIST Privacy Framework* [5].

3.1 Audience

This guide is intended for professionals implementing an RPM ecosystem for HDOs that use third-party telehealth platform providers. This guide examines scenarios where HDOs partner with a third-party telehealth platform provider where that telehealth platform provider manages devices that are used by the patient in their home setting. The telehealth platform provider implements technology that collects and makes biometric data available to clinicians, thus allowing the HDO to focus on patient care delivery. Approaches and controls focus on securing end-to-end communications and safeguarding assets and data that reside at HDO facilities; and discuss measures that HDOs and telehealth platform providers should implement in the patient home.

3.2 Scope

This RPM practice guide focuses on scenarios where patients with chronic or recurring conditions have biometric devices in their home that enable clinicians to regularly receive biometric data. The scope of this practice guide is limited to remote patient monitoring and does not include remote care. Patients and clinicians may use audio- and videoconferencing. The solution includes a third-party telehealth platform provider that provisions and manages biometric devices and provides means of communication.

3.3 Assumptions

This practice guide makes the following assumptions:

- RPM architecture includes deploying components to three distinct domains: the patient home, the telehealth platform provider, and the HDO.
- HDOs are regulated entities and must comply with federal, state, and local laws and regulations. In complying with laws and regulations, HDOs have implemented adequate privacy and security programs that include activities to address risk to both the organization and individuals when deploying an RPM architecture. Controls that have been implemented in accordance with laws and regulations provide an enterprise scope that this document refers to as pervasive controls.
- The telehealth platform provider maintains an adequate privacy and security control environment.
- The telehealth platform provider manages the configuration of patient home-deployed equipment.
- The patient home may have different communications options such as cellular data connectivity or broadband internet.
- RPM solutions emphasize collaboration. An RPM program's efficacy depends on the patient, the telehealth platform provider, and the HDO to participate in the program and apply adequate privacy and security practices. The HDO does not define the control environments for the telehealth platform provider or the patient home. Each participant needs sufficient awareness and exercises appropriate control over components that operate in their domain.
- Patient engagement activities provide the patient a clear understanding of privacy practices and expectations that address the specifics of the RPM architecture.

For this practice guide, telehealth platform providers deployed biometric devices with cellular data capabilities. Additionally, this practice guide implemented a solution for biometric devices that used patient home Wi-Fi communications.

3.4 Risk Assessment

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, 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, begins with a comprehensive review of [NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*]—material that is available to the public.

The [Risk Management Framework (RMF)] guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

In this practice guide, the NCCoE implements multiple approaches in assessing risk. An RPM environment is composed of multiple domains, with different constituents managing each domain. When analyzing risk, this practice guide contextualizes that risk and selects mitigating controls by disrupting threats. A description of how this practice guide addresses these concepts is in Appendix C, Threats and Risks. The risk assessments included in Appendix C represent how the practice guide examines risks. Organizations may find that the threats, vulnerabilities, and risks that they observe may differ from this practice guide's assessment. The risk assessments in this practice guide serve as examples that may catalyze how organizations perform their own risk assessments.

3.4.1 Threats

NIST SP 800-30 Revision 1 defines a threat as "… 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." Threats are actions that may compromise a system's confidentiality, integrity, or availability [6]. Table 3-1 describes threats that have been evaluated for this project. Threats evolve, and an organization needs to perform its own analysis when evaluating threats and risks that the organization faces.

Table 3-1 below is a sample threat taxonomy as it applies across the entire RPM ecosystem. The threat taxonomy uses a confidentiality (C), integrity (I), and availability (A) categorization; the threat event considered; and a description of the threat event. While the threat taxonomy provides a landscape view of threats, organizations may want to perform threat modeling to determine contextual application of threats. Appendix C, Threats and Risks, describes concepts on how to examine contextualized threats.

Table 3-1 Threat Taxonomy

C, I, A	Threat Event	Description
C	phishing	Phishing attacks are a form of social engineering, where the attacker presents themselves as a trusted party to gain the confidence of the victim.
I, A	malicious software	Malicious software (malware) is unauthorized code that may be introduced to a system. It performs unintended actions that may disrupt normal system function.

C, I, A	Threat Event	Description
		Malware may masquerade as desirable apps or applications.
I, A	command and control	Command and control attacks may begin with deployment of malware. Malware may allow a system to be operated remotely by unauthorized entities. Should a system fall victim to a command and control attack, that system may then be used as a pivot point to attack other components, either within the organization's infrastructure or as a point where attacks may be launched against other organizations.
A	ransomware	Ransomware is a form of malware that disrupts access to system resources. A typical form of ransomware involves the malware employing encryption that disables a legitimate system user from accessing files. Ransomware attacks generally involve a demand for payment to restore files. Payment does not ensure that the attacker will decrypt files, however.
C	credential escalation	Credential escalation attacks seek to take user account capabilities and extend those to a privileged level of capability.
I, A	operating system or application disruption	The operating system or application may be adversely affected by malicious actors who successfully implement malware on the target device. Data may be altered, or the device or application may not function properly.
C	data exfiltration	Malicious actors may be able to retrieve sensitive information from vulnerable devices. Malware may be used for this purpose.
A	denial of service attack	Flooding network connections with high-volume traffic to disrupt communication in patient home, between home and telehealth platform, or between telehealth platform provider and HDO. Such type of attack could also be used to damage a device, e.g., through accelerated battery depletion.
I	transmitted data manipulation	Unauthorized individuals may intercept and alter data transmissions.

3.4.2 Vulnerabilities

This practice guide uses a customized application for identifying vulnerabilities, which aggregates vulnerabilities identified in NIST SP 800-30 Revision 1. As noted in this special publication, a vulnerability is a deficiency or weakness that a threat source may exploit, resulting in a threat event. The document further describes how 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 table in Section C-6 of Appendix C, Threats and Risks, enumerates those vulnerabilities by using a holistic approach and represents those vulnerabilities that this project identified and for which it offers guidance.

3.4.3 Problematic Data Actions for Privacy

This build considered operational activities of the example solution that interact with patient data during RPM processes (“data actions”) and identified those that potentially cause problems to individuals.

The *NIST Privacy Framework* defines a problematic data action as “a data action that could cause an adverse effect for individuals” [5]. Problematic data actions can result in privacy risk to individuals and prevent an organization from developing a solution that meets the privacy engineering objectives of:

- predictability: enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service
- manageability: providing the capability for granular administration of data, including alteration, deletion, and selective disclosure
- disassociability: enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system

Table 3-2 below demonstrates the problematic data action taxonomy identified for the entire RPM ecosystem. This Problematic Data Action Taxonomy uses a predictability (P), manageability (M), and disassociability (D) designation; the problematic data action considered; and the description of the problematic data action. While the Problematic Data Action Taxonomy provides a landscape view of problematic data action, an organization may want to perform a risk assessment to determine contextual application of the problematic data action. The discussion about problematic data actions and risks in Appendix D introduces the PRAM [7] and provides a more detailed analysis.

Table 3-2 Problematic Data Action Taxonomy

P, M, D	Problematic Data Action	Description
P, M	distortion	Inaccurate or misleadingly incomplete data are used or disseminated. Distortion can present users in an

P, M, D	Problematic Data Action	Description
		inaccurate, unflattering, or disparaging manner, opening the door for stigmatization, discrimination, or loss of liberty.
M	insecurity	Lapses in data security can result in various problems, including loss of trust, exposure to economic loss and other identity theft-related harms, and dignity losses.
D, M	re-identification	De-identified data, or data otherwise disassociated from specific individuals, becomes identifiable or associated with specific individuals again. It can lead to problems such as discrimination, loss of trust, and dignity losses.
P, M	unanticipated revelation	Data reveals or exposes an individual or facets of an individual in unexpected ways. Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to dignity losses, discrimination, and loss of trust and autonomy.

The project team used the NIST PRAM [7] and accompanying Catalog of Problematic Data Actions and Problems [8] to conduct this analysis. Table 3-2, Problematic Data Action Taxonomy, provides the results of this analysis. See Appendix D for additional considerations regarding examples of problematic data actions for RPM solutions.

3.4.4 Risk

As noted in Section 3.4, 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” [9].

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, one may realize multiple risks based on a successful attack. Notwithstanding, we consider those risks identified below. In reviewing these risks, please note that we consider unique scenarios that presume certain attack types for the two risks categorized as availability risks, those being ransomware and pivot point attacks.

Table 3-3, Cybersecurity Risk Taxonomy, describes high-level cybersecurity risks that affect the RPM environment. The risk taxonomy table captures key risks, assigning where the risk may impact the organization across a confidentiality, integrity, and availability (CIA) [6] dimension.

Table 3-3 Cybersecurity Risk Taxonomy

C, I, A	Risk	Description	Risk Level
C	fraudulent use of health-related information	Health-related information may be used for several different fraudulent means, such as identity theft, insurance fraud, or extortion.	medium
I	patient diagnoses disrupted based on timeliness interruption, leading to patient safety concerns	Unavailability or significant delay in delivering biometric data may negate the benefits of remote patient monitoring. Clinicians may not be able to provide appropriate care should biometric data transmission be disrupted.	medium
I	incorrect patient diagnosis due to change of data	A critical patient event is missed due to changes in the data stream between device and HDO.	high
A	process disruption due to ransomware	Ransomware may prevent normal device operations. Data may be irretrievable and therefore may prevent clinical care.	high
I, A	systemic disruption due to component compromise	Disruptions to the system that affect its availability or integrity may compromise the benefits derived from remote patient monitoring.	high
I	clinician misdiagnosis	If data are altered inappropriately, clinicians may make inaccurate diagnoses, resulting in patient safety issues.	high

Table 3-4, Privacy Risk Taxonomy, describes high-level privacy risks that affect the RPM environment. Table 3-4 captures key risks, assigning where the risk may impact individuals, in the areas of predictability, manageability, and disassociability [5]. Privacy risk levels to individuals depend on the context of specific RPM solution deployment and are not included. These risks are discussed further in Appendix D.

Table 3-4 Privacy Risk Taxonomy

P, M, D	Risk	Description
M	Storage and movement of data creates multiple points of potential exposure after data is collected from the patient.	Insecurity: Storage and movement of data creates multiple points of potential exposure after it is collected from the patient. RPM context: Biometric data and patient health information flow through various entities in the RPM solution, each of which plays a role in protecting the information.
P, M	Biometric device types can indicate patient health problems that individuals would prefer not to disclose beyond their healthcare provider.	Unanticipated revelation: Biometric device types can indicate patient health problems that individuals would prefer not to disclose beyond their healthcare provider. RPM context: Using one or more biometric devices can indicate—to others beyond the patient's healthcare provider—potential health problems for which a patient is being monitored.
P, M	Incorrect data capture of readings by devices may impact quality of patient care.	Distortion: Device misuse may cause a failure to monitor patients in accordance with their healthcare plan. RPM context: Incorrect or unintended use of biometric devices may introduce data quality issues into the RPM environment, resulting in inaccurate or incomplete data being used to make decisions regarding patient care.
D, M	Aggregated data may expose patient information.	Re-identification: Associating biometric data with patient identifiers can expose health conditions.

P, M, D	Risk	Description
		RPM context: Associating biometric data in a way that exposes information about the patient could cause issues such as embarrassment and discrimination. Disassociated processing is intentionally used during some dataflows within the RPM solution to mitigate the risk of exposing identifiable patient information to vendors, administrators, and other practitioners who are outside the patient's care team.
P, M	Exposure of patient information through multiple providers of system components increases the likelihood of exposure of patient data to unintended recipients.	Unanticipated Revelation: Data processing is handled by multiple parties within the background of the ecosystem and are transparent to the patient. RPM context: Patient health information may be revealed in ways or to parties that the individual may not expect. Additionally, using one or more biometric devices can indicate potential health problems—to others beyond the patient's healthcare provider—for which a patient is being monitored.

3.4.5 Mitigating Risk

As noted above, risk is the adverse outcome when a threat successfully leverages a vulnerability. Mitigating risk may take many different forms. This practice guide addresses risk by performing a threat modeling exercise and by mitigating threats. The previous sections discussed threat from a holistic perspective. That is, the noted threats enumerate a broad survey of attack types that may adversely affect the RPM ecosystem. RPM decomposes to the following three distinct domains: patient home, telehealth platform provider, and HDO. As organizations consider measures to disrupt threats and adverse actions made against the ecosystem, an opportunity exists where organizations examine threats to identify controls that mitigate adverse actions identified by threat modeling.

3.5 Security Control Map

As this practice guide considered RPM ecosystem risks, the team performed a mapping to the NIST Cybersecurity Framework [3]. This mapping established an initial set of appropriate control Functions, Categories, and Subcategories. The mapping demonstrated how selected Cybersecurity Framework Subcategories map to controls in NIST SP 800-53 Revision 5 [10] as well as to the Workforce Framework for Cybersecurity (NICE Framework), NIST SP 800-181 [2]. The table also lists sector-specific standards and best practices (e.g., the International Electrotechnical Commission [IEC] Technical Reports [TR], International Organization for Standardization [ISO]) as well as from the Health Insurance Portability and Accountability Act (HIPAA) [11], [12], [13]. The security control map, shown in Table 3-5, identifies a set of controls, including those specifically implemented in the lab build, as well as the pervasive set of controls as described in Section 5.2, Pervasive Controls, that HDOs should deploy. Practitioners should refer to Appendix C of NIST SP 1800-24, *Securing Picture Archiving and Communication System (PACS)* for further description of pervasive controls [14].

Table 3-5 Security Characteristics and Controls Mapping–NIST Cybersecurity Framework

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		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			45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(7)(ii)(E)	A.8.1.1 A.8.1.2 A.12.5.1
		ID.AM-4: External information systems are catalogued	AC-20 PM-5 SA-9			45 C.F.R. §§ 164.308(a)(4)(ii)(A) 164.308(b) 164.314(a)(1) 164.314(a)(2)(i)(B) 164.314(a)(2)(ii) 164.316(b)(2)	A.11.2.6
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	CP-2RA-2 RA-9 SA-20 SC-6	CO-OPL-001	SGUD	45 C.F.R. §§ 164.308(a)(7)(ii)(E)	A.8.2.1

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**		**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	CA-2 CA-5 CA-7 CA-8 PM-4 PM-15RA-3 RA-5 SA-5 SA-11 SI-2 SI-4 SI-5	AN-ASA-001 AN-ASA-002 AN-TWA-001 CO-CLO-002 CO-OPS-001 SP-ARC-001	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	CP-2 PM-9 PM-11 RA-2 RA-3 RA-9	AN-ASA-001 AN-ASA-002 AN-EXP-001 AN-LNG-001 AN-TGT-001 AN-TGT-002 AN-TWA-001 CO-CLO-001 CO-CLO-002 CO-OPL-001 CO-OPL-002	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

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	CA-2 CA-7 PM-16 PM-28 RA-2 RA-3	SP-SYS-001	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
		ID.RA-6: Risk responses are identified and prioritized	CA-5 PM-4 PM-9 PM-28 RA-7	SP-SYS-001	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, Authentication and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	IA-1 IA-2 IA-3 IA-4 IA-5 IA-7 IA-8 IA-9 IA-10 IA-11 IA-12	OM-ADM-001	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

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**		**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.AC-2: Physical access to assets is managed and protected	PE-1 PE-2 PE-3 PE-4 PE-5 PE-6 PE-8 PE-9	OM-ADM-001	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
		PR.AC-3: Remote access is managed	AC-1 AC-17 AC-19 AC-20 SC-15	OM-ADM-001	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	OM-ADM-001 OM-KMG-001 PR-INF-001	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

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4 AC-10 SC-7 SC-10 SC-20		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
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	AC-16 IA-1 IA-2 IA-4 IA-5 IA-8 IA-12 PE-2 PS-3	SP-RSK-002 OV-PMA-003	AUTH CNFS EMRG NAUT PLOK SGUD	N/A	A.7.1.1 A.9.1.2

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**		**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-14 IA-1 IA-2 IA-3 IA-5 IA-8 IA-9 IA-10 IA-11		ALOF AUTH NAUT PAUT		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-2 MP-3 MP-4 MP-5 MP-6 MP-7 MP-8 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	OM-DTA-002 PR-CDA-001	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				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CM-8 MP-6 PE-16 PE-20		N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv) 164.310(d)(1) 164.310(d)(2)	A.8.2.3 A.8.3.1 A.8.3.2 A.8.3.3 A.11.2.5 A.11.2.7
		PR.DS-4: Adequate capacity to ensure availability is maintained	AU-4 CP-2 PE-11 SC-5		AUDT DTBK	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7) 164.310(a)(2)(i) 164.310(d)(2)(iv) 164.312(a)(2)(ii)	A.12.1.3 A.17.2.1

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		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 AU-13 PE-19 PS-6 SC-7 SI-4	SP-SYS-001	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	SI-7 SI-10		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				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
	Information Protection (PR.IP)	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 SR-12		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
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	CP-1 CP-2 CP-7 CP-10 IR-1 IR-7 IR-8 IR-9		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	OM-NET-001	DTBK SGUD	45 C.F.R. §§ 164.308(a)(7)(ii)(D)	A.17.1.3
		PR.IP-12: A vulnerability management plan is developed and implemented	RA-1 RA-3 RA-5 SI-2	OV-PMA-001	MLDP	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B)	A.12.6.1 A.14.2.3 A.16.1.3 A.18.2.2 A.18.2.3

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
	Maintenance (PR.MA)	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	MA-1 MA-2 MA-3 MA-5 MA-6	OM-ADM-001 PR-INF-001	CSUP RDMP	45 C.F.R. §§ 164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)	A.11.1.2 A.11.2.4 A.11.2.5 A.11.2.6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	MA-4		CSUP	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A) 164.310(d)(1) 164.310(d)(2)(ii) 164.310(d)(2)(iii) 164.312(a) 164.312(a)(2)(ii) 164.312(a)(2)(iv) 164.312(b) 164.312(d) 164.312(e)	A.11.2.4 A.15.1.1 A.15.2.1
	Protective Technology (PR.PT)	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU-1 AU-2 AU-3 AU-6 AU-7 AU-12 AU-13 AU-14 AU-16	OV-PMA-001 OV-PMA-002 OV-PMA-003 OV-PMA-004 OV-PMA-005	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

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
				OV-SPP-001 OV-SPP-002			
		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				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**		**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
		PR.PT-4: Communications and control networks are protected	AC-12 AC-17 AC-18 CP-8 SC-5 SC-7 SC-10 SC-11 SC-20 SC-21 SC-22 SC-23 SC-31 SC-37 SC-38 SC-47		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 SC-16 SI-4	OV-EXL-001 OV-MGT-001	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				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		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 RA-5 IR-4 SI-4	AN-LNG-001 CO-CLO-002 IN-FOR-001 OM-DTA-002 OM-STS-001 PR-CDA-001	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
	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events	AU-12 CA-7 CM-3 SC-5 SC-7 SI-4	AN-ASA-001 AN-ASA-002 AN-EXP-001 AN-TWA-001 CO-CLO-001 OM-DTA-001 OM-KMG-001 OM-NET-001 OV-EXL-001 OV-LGA-002 OV-MGT-001	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
		DE.CM-2: The physical environment is monitored to detect	CA-7 PE-6 PE-20	AN-ASA-001 AN-ASA-002	MLDP	45 C.F.R. §§ 164.310(a)(2)(ii) 164.310(a)(2)(iii)	A.11.1.1 A.11.1.2

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	Category	Subcategory	NIST SP 800-53 Revision 5		IEC TR 80001-2-2	HIPAA Security Rule	ISO/IEC 27001
		potential cybersecurity events		AN-TWA-001			
		DE.CM-4: Malicious code is detected	SC-44 SI-3 SI-4 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-5: Unauthorized mobile code is detected	SC-18 SC-44 SI-4		MLDP SGUD	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)	A.12.5.1 A.12.6.2
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12 CA-7 CM-3 CM-8 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	AN-EXP-001 IN-FOR-002 SP-DEV-002	MLDP PLOK	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(8)	A.12.6.1

NIST Cybersecurity Framework v1.1				NIST NICE Framework (NIST SP 800-181)	Sector-Specific Standards and Best Practices		
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**		**IEC TR 80001-2-2**	**HIPAA Security Rule**	**ISO/IEC 27001**
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
	Improvements (RS.IM)	RS.IM-1: Response plans incorporate lessons learned	CP-2 IR-4 IR-8		DTBK	45 C.F.R. §§ 164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)	A.16.1.6 Clause 10
		RS.IM-2: Response strategies are updated	CP-2 IR-4 IR-8		DTBK	45 C.F.R. §§ 164.308(a)(7)(ii)(D) 164.308(a)(8)	A.16.1.6 Clause 10
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	OM-ADM-001	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

Table 3-6 identifies the *NIST Privacy Framework* v1.0 Functions, Categories, and Subcategories implemented in the lab build that the solution supports and demonstrates how they map to controls in the final published version of NIST SP 800-53, Revision 5 [5], [10]. Practitioners should refer to the Privacy Framework Resource Repository for the comprehensive mapping of the Privacy Framework and Cybersecurity Framework to NIST SP 800-53, Revision 5. HDOs should evaluate controls that align with their identified risks [15] .

Table 3-6 Privacy Characteristics and Controls Mapping–*NIST Privacy Framework*

NIST Privacy Framework v1.0			
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**
Identify—P	Inventory and Mapping (ID.IM-P)	ID.IM-P1: Systems/products/services that process data are inventoried.	CM-8, CM-12, CM-13, PM-5
		ID.IM-P2: Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried.	CM-8(4), CM-13
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	CM-8, CM-12, CM-13
	Risk Assessment (ID.RA-P)	ID.RA-P3: Potential problematic data actions and associated problems are identified.	CM-13, RA-3, RA-8
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	PM-28, RA-2, RA-3, RA-8
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.	CA-5, PM-4, PM-9, PM-28, RA-7, RA-8
Control–P	Data Processing	CT.DM-P5: Data are destroyed according to policy.	MP-6, SI-12(3), SR-12

NIST Privacy Framework v1.0			
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**
	Management (CT.DM-P)	CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16
Protect—P	Data Protection Policies, Processes, and Procedures	PR.PO-P3: Backups of information are conducted, maintained, and tested.	CP-4, CP-6, CP-9
		PR.PO-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9
		PR.PO-P8: Response and recovery plans are tested.	CP-4, IR-3, PM-14
		PR.PO-P10: A vulnerability management plan is developed and implemented.	RA-1, RA-3, RA-5, SI-2
	Identity Management, Authentication, and Access Control	PR.AC-P1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12
		PR.AC-P2: Physical access to data and devices is managed.	PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9
		PR.AC-P3: Remote access is managed.	AC-1, AC-17, AC-19, AC-20, SC-15

NIST Privacy Framework v1.0			
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**
		PR.AC-P4: 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
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	AC-4, AC-10, SC-7, SC-10, SC-20
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	AC-14, AC-16, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11, IA-12, PE-2, PS-3
	Data Security (PR.DS-P)	PR.DS-P1: Data-at-rest are protected.	MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28
		PR.DS-P2: Data-in-transit are protected.	SC-8, SC-11
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	CM-8, MP-6, PE-16, PE-20
		PR.DS-P4: Adequate capacity to ensure availability is maintained.	AU-4, CP-2, PE-11, SC-5
		PR.DS-P5: Protections against data leaks are implemented.	AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4

NIST Privacy Framework v1.0			
Function	**Category**	**Subcategory**	**NIST SP 800-53 Revision 5**
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	SC-16, SI-7, SI-10
	Maintenance (PR.MA-P)	PR.MA-P1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	MA-1, MA-2, MA-3, MA-5, MA-6
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	MA-4
	Protective Technology (PR.PT-P)	PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	AC-3, CM-7
		PR.PT-P3: Communications and control networks are protected.	AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47

3.6 Technologies

Table 3-7 lists all of the technologies used in this project, and provides a mapping among the generic application terms, the specific product used, and the security control(s) that the product provides. Refer to Table 3-5 for an explanation of the NIST Cybersecurity Framework Subcategory codes, and refer to Table 3-6 for an explanation of the *NIST Privacy Framework* Subcategory codes.

While this practice guide notes that the RPM solution is deployed across three domains, HDOs must recognize that the responsibility for risk management remains with the HDO. Risk mitigation may be achieved through tools or practices, where privacy and security measures are applied as appropriate in each of the domains. HDOs may find that deploying privacy and security tools to the patient home involves challenges and that therefore an HDO may collaborate with the telehealth platform provider to provide adequate education and awareness training to patients. Training may address appropriate use of the equipment that is sent to the patient home and awareness that patient data are involved and that the patient needs to assure that data are shared only with authorized individuals.

For this practice guide, the telehealth platform provider is a third-party entity, distinct from the patient and the HDO. Telehealth platform providers should implement an adequate control environment that enables the telehealth platform provider to collaborate with HDOs in delivering RPM solutions. The scope of this practice guide does not discuss all controls that a telehealth platform provider should deploy. Rather, this practice guide focuses on controls that are deployed in the HDO. The telehealth platform provider is a separate entity and should ensure that adequate controls are implemented in its environment. Further, telehealth platform providers must ensure that equipment deployed to the patient home includes appropriate safeguards.

601 **Table 3-7 Products and Technologies**

Component/ Capability	Product	Function	NIST Cybersecurity Framework and Privacy Framework Subcategories	Domain
telehealth platform provider	Accuhealth Evelyn Vivify Pathways Home Vivify Pathways Care Team Portal	▪ Provides role-based user access control. ▪ Performs asset management for the provisioned devices. ▪ Transmits health information to the platform. ▪ Connects patients and physicians.	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5 PR.AC-1 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7 PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-4 PR.DS-6 PR.PT-1 PR.PT-3 PR.PT-4 ID.IM-P1 ID.IM-P2 ID.IM-P7 PR.AC-P1 PR.AC-P4 PR.AC-P5 PR.AC-P6 PR.DS-P1 PR.DS-P2 PR.DS-P3 PR.PT-P2 PR.PT-P3	patient home telehealth platform provider

Component/ Capability	Product	Function	NIST Cybersecurity Framework and Privacy Framework Subcategories	Domain
risk assessment controls	Tenable.sc Vulnerability Management Version 5.13.0 with Nessus	▪ Provides on-premises centralized vulnerability management with multiple scanners. ▪ Provides vulnerability prioritization. ▪ Provides risk scores.	ID.RA-5 ID.RA-P4	HDO
identity management, authentication, and access control	Active Directory (AD)	▪ Authenticates and authorizes users and computers in the domain. ▪ Authenticates and authorizes to multiple applications within the environment.	PR.AC-1 PR.AC-4 PR.AC-P1 PR.AC-P4	HDO
	Cisco Firepower Version 6.3.0	▪ Provides a Firepower management console (FMC) used for Firepower Threat Defense (FTD). ▪ Provides centralized control over network and communication. ▪ Provides network visibility. ▪ Provides intrusion prevention. ▪ Provides network segmentation. ▪ Provides policy-based network protection.	PR.AC-5 PR.PT-4 DE.AE-2 DE.CM-1 DE.CM-4 DE.CM-5 PR.AC-P5 PR.PT-P3	HDO
	Cisco Umbrella	▪ Provides domain name service (DNS) and internet protocol (IP) layer security.	DE.CM-4 DE.CM-5	HDO

Component/ Capability	Product	Function	NIST Cybersecurity Framework and Privacy Framework Subcategories	Domain
		▪ Provides content/application filtering. ▪ Provides advanced malware protection (AMP).		
	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.	PR.DS-5 PR.PT-4 DE.AE-1 DE.CM-1 DE.CM-4 DE.CM-5 PR.DS-P5 PR.PT-P3	HDO
	Onclave Zero Trust Platform Version 1.1.0	▪ Leverages blockchain technology to manage valid endpoints.	PR.AC-1 PR.AC-3 PR.AC-4 PR.PT-4 PR.AC-P1 PR.AC-P3 PR.AC-P4 PR.PT-P3	telehealth platform provider
data security	Accuhealth Vivify Health	▪ Ensures that data-in-transit are protected. ▪ Ensures that data- at-rest are protected.	PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-P1 PR.DS-P2 PR.DS-P3	patient home telehealth platform provider HDO

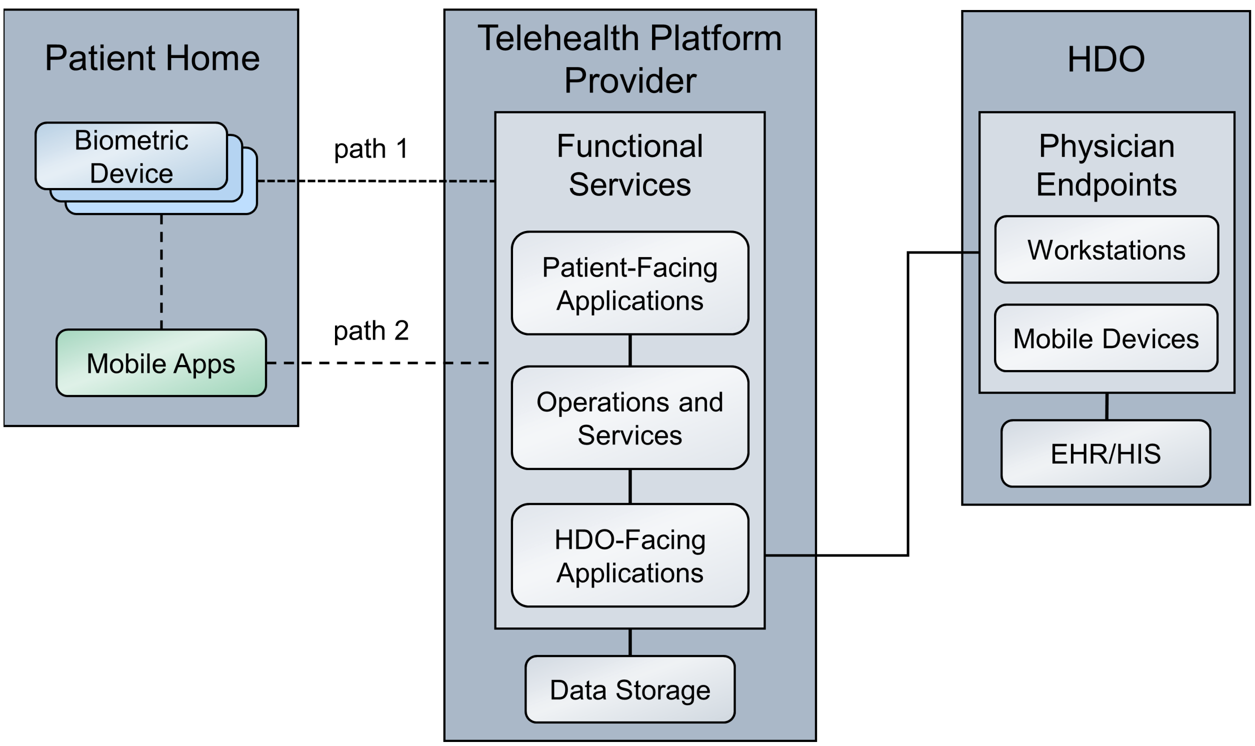
Component/ Capability	Product	Function	NIST Cybersecurity Framework and Privacy Framework Subcategories	Domain
	Onclave Secure IoT Bridge Version 1.1.0	▪ Provides trusted and secure communication between Onclave gateways. ▪ Establishes encrypted layer 2 secure tunnels between Onclave bridges and gateways.	PR.DS-2 PR.DS-P2	telehealth platform provider
	Onclave Secure IoT Gateway Version 1.1.0	▪ Forms the basis of a cryptographically secure enclave. ▪ Establishes encrypted layer 2 secure tunnels between trusted gateways.	PR.AC-5 PR.DS-5 PR.AC-P5 PR.DS-P5	patient home telehealth platform provider
anomalies and events and security continuous monitoring	LogRhythmXDR Version 7.4.9 LogRhythm NetworkXDR Version 4.0.2	▪ Aggregates log files. ▪ Performs behavioral analytics. ▪ Monitors for unauthorized personnel, connections, devices, and software. ▪ Provides dashboards with the analytic results.	ID.RA-5 PR.PT-1 DE.AE-1 DE.AE-2 DE.CM-7 ID.RA-P4 CT.DM-P8	HDO

4 Architecture

This practice guide implements a representative RPM solution as a distributed architecture. The solution deployed components across three domains that consist of the patient home, the telehealth platform provider, and the HDO. The patient home is the environment in which the patient lives and uses RPM components that include biometric monitoring devices, devices that the patient uses to communicate with their care team, and devices that the patient operates for personal use. This practice guide incorporates cloud-hosted telehealth platform providers within the architecture. The telehealth platform provider maintains components that include virtual or physical components with servers to manage, maintain, and receive data communications from either the patient home or the HDO. The HDO maintains its own environment and includes components such as workstations and clinical systems to receive and interpret patient data and record patient interactions in an electronic health record (EHR) system.

Figure 4-1 illustrates a high-level RPM distributed architecture. The depicted architecture notes two primary paths by which network communications traverse. Path 1 shows biometric devices communicating with the telehealth platform provider whereas Path 2 shows the use of a mobile app. The mobile app operates on an interface device (i.e., a provisioned tablet). For Path 2, patients use the tablet to collect data from the biometric devices. Path 2 does not involve data transfer between the biometric device to the telehealth platform provider directly. Rather, patients collect biometric data with the tablet. Patients use the tablet for communications, with data exchanges between the patient home and the telehealth platform provider.

Figure 4-1 RPM Architecture



4.1 Layering the Architecture

The NCCoE healthcare lab stratified the distributed architecture with three layers: business, security, and infrastructure. The business layer focuses on functional capabilities that include biometric readings and patient interactions. The security layer conceptually describes how the NCCoE lab implements security capabilities. The NCCoE also implements an infrastructure layer that represents the network and communications environment.

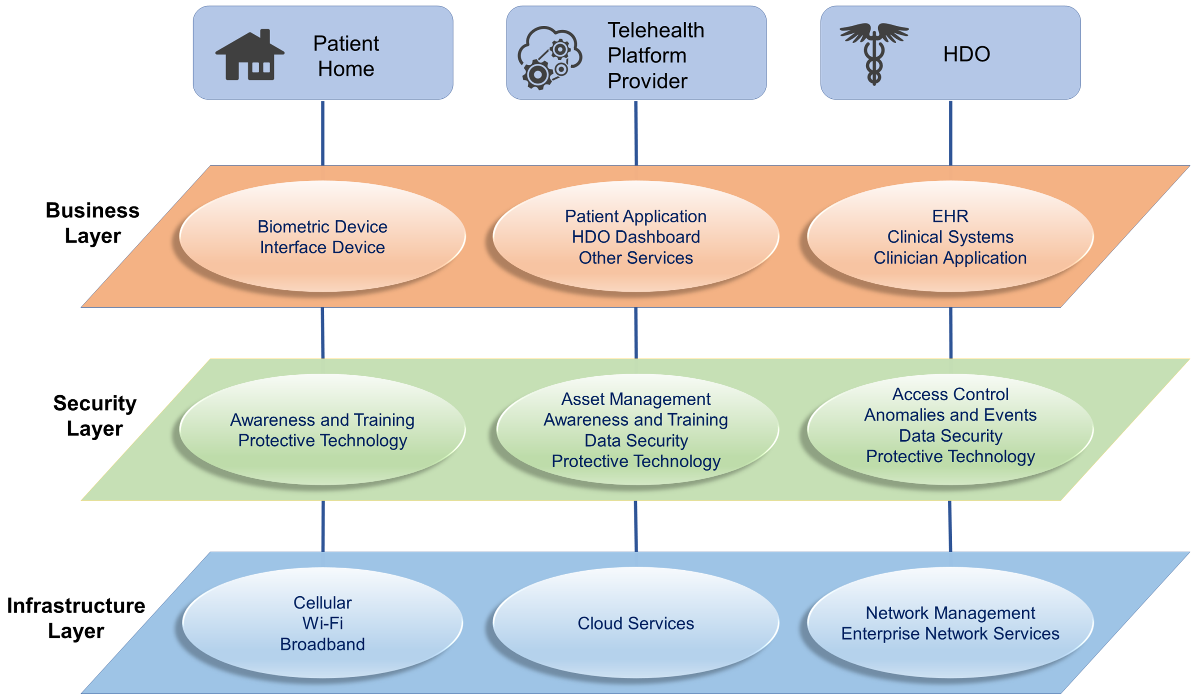
The layers intersect each of the three domains. The patient home domain implements the business layer by using the biometric devices and interface device(s) that capture and relay biometric data from the patient and allow the patient to communicate with the clinical care team, respectively. The patient home may include a security layer component that segregates network traffic between the RPM components and personally owned devices when the RPM devices use the same network infrastructure (e.g., over Wi-Fi) as the personally owned devices. When devices operate and communicate over Wi-Fi, the infrastructure layer would consist of Wi-Fi access points, routers, and switches that the patient operates.

The telehealth platform provider domain also implements three layers. The business layer consists of services that facilitate handling patient data and web- or audioconferencing capabilities. The security layer consists of components used to secure the environment, such as authentication mechanisms, certificate management systems, and security logging capabilities. The infrastructure layer consists of network and server components that may be implemented as cloud services. Practitioners should note that this practice guide does not go into significant detail regarding security or infrastructure layer configurations for telehealth platform providers. As noted in this practice guide's list of assumptions, it is assumed that telehealth platform providers have adequate privacy and security controls. These controls would align with the layer concept. HDOs should evaluate telehealth platform providers to determine control adequacy.

The HDO domain implements the business layer with applications and clinical systems used to support the RPM program. The security layer represents security capability deployment, which includes authentication mechanisms, network monitoring capabilities, and vulnerability scanning for example. The HDO implements the infrastructure layer with fundamental IT services such as AD, DNS, and networking devices.

Figure 4-2 depicts a high-level view of the three layers intersecting each domain of these components and how we approached implementing them in the lab environment.

Figure 4-2 Architecture Layers



4.2 High-Level Architecture Communications Pathways

This practice guide describes an architecture that considers six different communications paths among the patient home, telehealth platform provider, and HDO. Figure 4-3, RPM Communications Paths, shows the different paths labeled A through F. The different communications paths represent the varying modes by which the patient shares data with the clinician. Each path leads to the telehealth platform provider who receives the data and presents the data in an HDO-facing application. The clinician accesses data presented within an HDO-facing application via an app or application.

4.2.1 Cellular Data Pathways

The following communications pathways describe how patients use devices that are preconfigured with cellular data services. Telehealth platform providers may provision devices with cellular data capability to support ease of use and connectivity assurance and to ensure that the device may not be reachable by an untrusted internet connection (e.g., an arbitrary Wi-Fi hot spot).

Path A assumes that the biometric device has cellular communications. The telehealth platform provider deploys the biometric device with a preconfigured subscriber identity module, commonly referred to as a subscriber identity module (SIM) card. Option A does not include an RPM interface, such as a mobile device that may be a laptop, cellular phone, or tablet. The biometric device sends data over cellular data networks, which then route the data to the telehealth platform provider. The telehealth platform provider receives the data and displays it for clinicians to view through a portal or dashboard application. The clinician accesses the data through a clinician-facing app or application.

Path B assumes that the telehealth platform provider has deployed a biometric device and an RPM interface to the patient home. The RPM interface may be a mobile device such as a cellular phone or tablet. For this path, the biometric device forwards data to the RPM interface via Bluetooth. The RPM interface would include a SIM card that enables cellular data communication to the telehealth platform provider. The RPM interface would be deployed with an app to be used by the patient. The app would include an interface that allows the patient to forward the data to the telehealth platform provider.

4.2.2 Broadband Pathways

Telehealth platform providers may provide devices that leverage broadband internet connectivity provisioned at the patient home. Devices may use Wi-Fi or other communications protocols. Devices may transmit data that traverses a patient-provided internet router. The following pathways describe how data may flow when internet broadband is available.

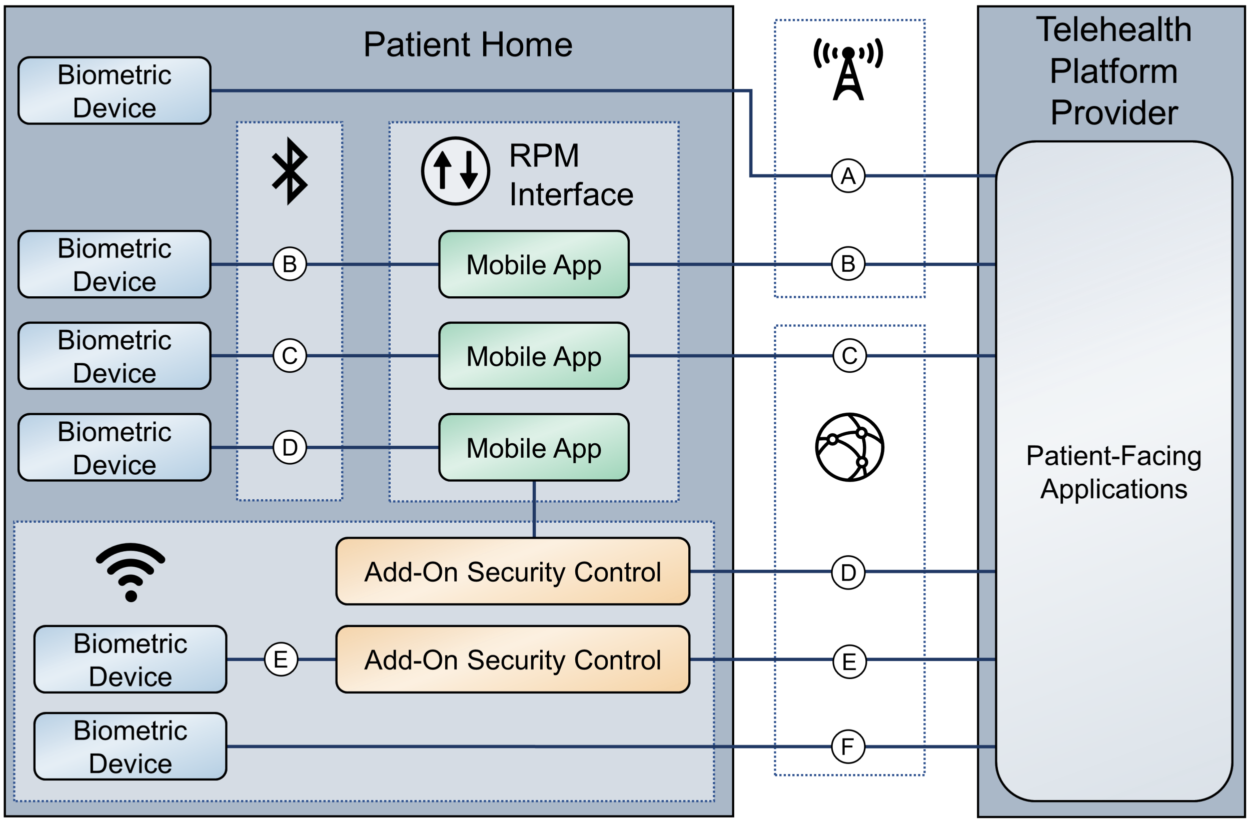
Path C assumes that the telehealth platform provider has deployed a biometric device and an RPM interface to the patient home. The dataflow within the patient home domain is the same as Path B. However, rather than cellular communication, the RPM interface communicates with the telehealth platform provider via a broadband connection provided by the patient.

Path D has the same dataflow as Path C; however, external network transmissions traverse an add-on security device such as a Layer 2 over Layer 3 gateway.

Path E is like Path A; however, rather than cellular data, the path leverages a patient home broadband connection traversing an add-on security device such as a Layer 2 over Layer 3 gateway.

Path F is like Paths A and E. Path F leverages a patient home broadband connection; however, no other gateway is used. Data are sent directly to the telehealth platform provider over the public internet.

695 **Figure 4-3 RPM Communications Paths**



696 ## 4.3 Data and Process Flows

697 To gain a high-level understanding of how RPM programs operate, this practice guide evaluates two use
698 cases: diabetes, and cardiac and pulmonary rehabilitation.

699 The World Health Organization defines diabetes as "a chronic, metabolic disease characterized by
700 elevated levels of blood glucose (or blood sugar), which leads over time to serious damage to the heart,
701 blood vessels, eyes, kidneys, and nerves" [16]. A diabetes RPM program could be beneficial in identifying
702 when a patient's blood glucose levels are higher/lower than normal. Ensuring that a patient's blood
703 glucose levels remain in a normal range helps prevent long-term complications that diabetes could
704 cause [17]. Patients may receive biometric devices such as glucometers, blood pressure monitors,
705 weight scales, and activity trackers. These biometric devices may be enabled with Bluetooth, Wi-Fi, or
706 cellular data communications capabilities that allow patients to share biometric data with physicians.
707 Physicians may continuously monitor patients' biometric data to identify and prevent a potential
708 problem from occurring.

HDOs may enroll patients with chronic heart or lung conditions such as chronic obstructive pulmonary disease or coronary heart disease into cardiac and pulmonary RPM rehabilitation programs. These programs help patients return to a normal life and reduce other risk factors such as high blood pressure, high blood cholesterol, and stress [18], [19].

Telehealth platform providers implement solutions by using biometric devices, services, and applications. While telehealth platform providers may develop and maintain services and applications, they collaborate with manufacturers to procure and manage biometric devices. Conceptually, the device manufacturer operates as an extension of the telehealth platform provider when delivering RPM solutions to patients.

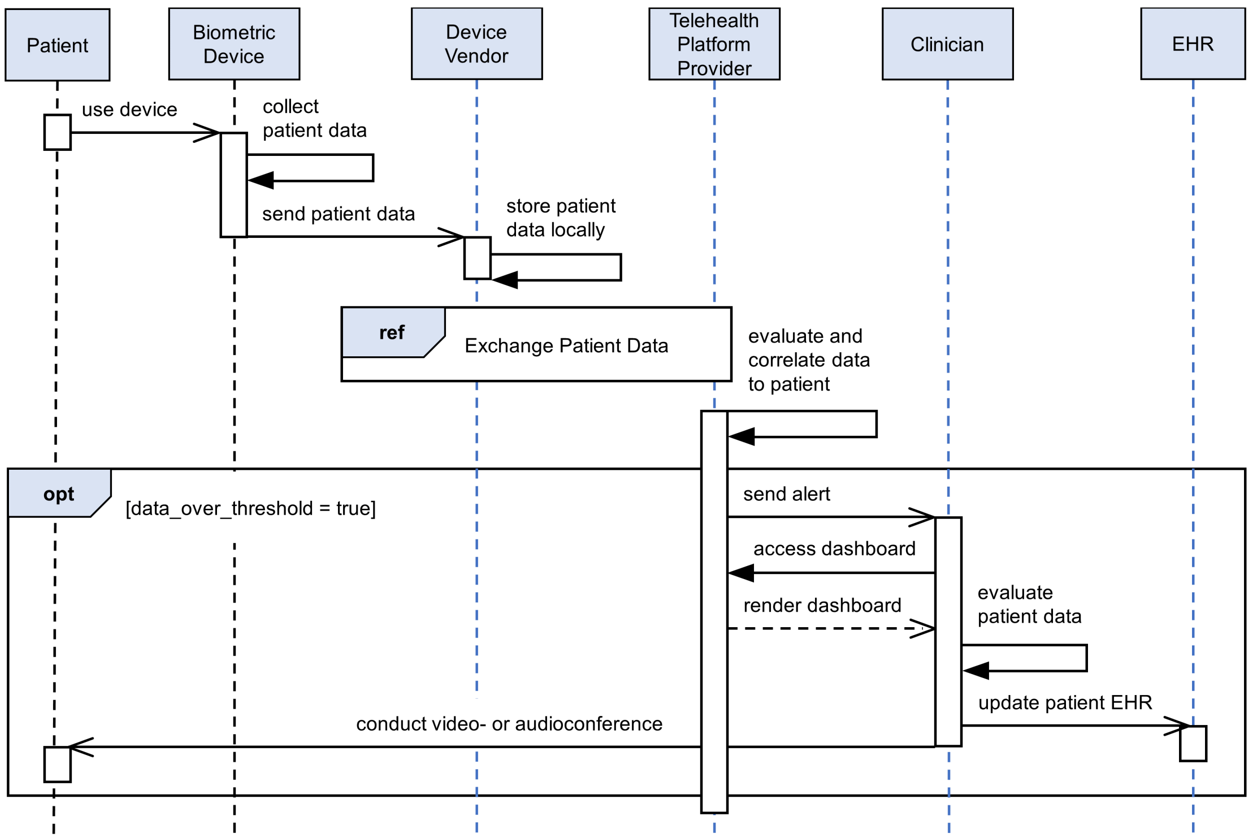
As noted in Section 4.2, High-Level Architecture Communications Pathways, practitioners may implement RPM ecosystems where data communications involve different communications protocols or paths.

This practice guide examines two distinct dataflows. The first dataflow begins when the patient transmits data from the biometric device. The biometric device sends data to the device manufacturer. The telehealth platform provider retrieves the data and presents the data through an HDO-facing application. The clinician views the data from an app or application that interfaces with the patient data residing in the telehealth platform provider HDO-facing application.

The second dataflow begins when the patient transmits the data from the biometric device. A field gateway device, such as a mobile device that may be a tablet, mobile phone, or laptop, pulls the data from the biometric device. The patient uses the field gateway device to transport the data to the telehealth platform provider. The telehealth platform provider receives the data and presents it through an HDO-facing application. The clinician views the data from an app or application that interfaces with the patient data residing in the telehealth platform provider HDO-facing application.

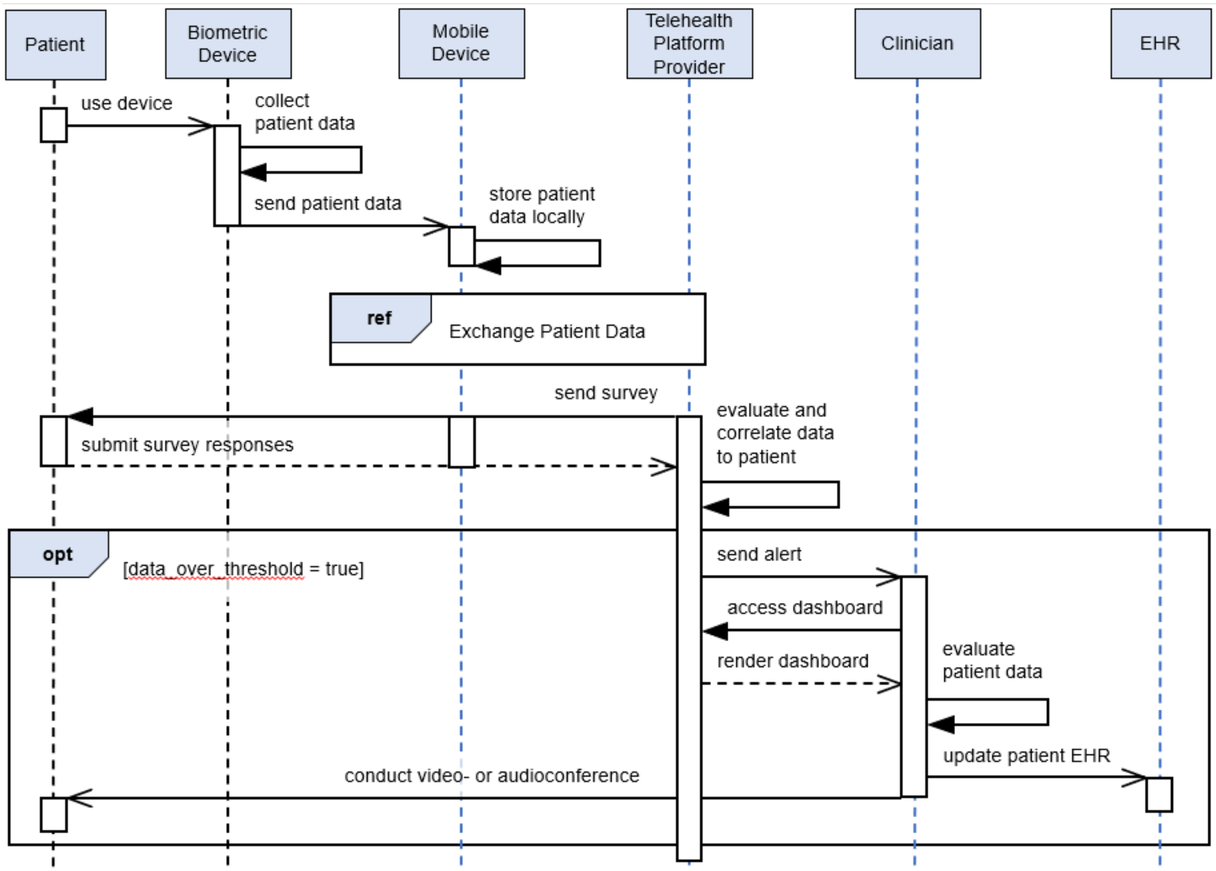
Figure 4-4 depicts the first dataflow sequence. This dataflow sequence demonstrates an RPM implementation that uses device vendor platforms to transmit data from a patient's home to the telehealth platform provider. A patient begins the process by interfacing with the biometric device provided by the third-party platform, which in turn gathers the required medical readings. Once the device gathers the desired readings, the device transmits and stores the data to the device vendor's local storage server. The third-party platform connects to the vendor's storage server and pulls that data into its own local storage server. The platform then evaluates the received data and creates correlations among the retrieved data, the associated patient, and the primary care provider. If the platform identifies any areas of concern (such as high blood glucose readings for a diabetes use case) while evaluating the data, the platform sends an alert to the patient's primary care provider for immediate action. Otherwise, the primary care provider will connect to the third-party platform's web server to view the patient's data on a dashboard. The physician/clinician will evaluate the data, modify the patient's care plan, update the patient's EHR, and contact the patient via video or audio call to update them on their new care plan.

746 **Figure 4-4 RPM Dataflow Option 1**



747 Figure 4-5 depicts the second dataflow sequence. In this dataflow sequence, a patient begins the
748 process by interfacing with the biometric device provided by the telehealth platform provider, which in
749 turn collects the required medical readings. Once the data are collected, the device transmits the data
750 to the mobile device. The patient uses the mobile device to answer survey questions associated with
751 their program, providing a clinician more insight on the patient's health. The patient uses the mobile
752 device to collect data from all biometric devices associated with their RPM regimen. The patient uses
753 the mobile device to transmit the biometric device data and survey results. The mobile device pushes
754 the grouped data to the telehealth platform provider. The telehealth platform provider presents the
755 data to the primary care provider. The clinician connects to the telehealth platform provider's web
756 server to view the patient's data on a dashboard. The clinician evaluates the data and may update the
757 patient's care plan. Then, the clinician may update the patient's EHR and contact the patient via a
758 mobile device to update them on their new care plan.

Figure 4-5 RPM Dataflow Option 2



4.4 Security Capabilities

The project team implemented a lab environment that represented the three domains described in Section 4, Architecture. When building the HDO environment, the team built upon the zoned network architecture described in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* [20]. The team used the network zoning approach as a baseline for the RPM ecosystem infrastructure. On top of the baseline, the team selected relevant security capabilities for appropriate domains. The selected security capabilities are:

- telehealth platform provider
- risk assessment controls
- identity management, authentication, and access control
- data security
- anomalies and events and security continuous monitoring

HDOs bear risk when implementing RPM practices. The RPM environment is distributed across three domains and requires participation of the patient, the telehealth platform provider, and the HDO to assure that risks are adequately mitigated. This practice guide's architecture describes deploying components in three domains, with threats and risks that may affect each domain distinctly. As organizations implement RPM solutions, they must include parties involved in managing the individual domains in recognizing and safeguarding against privacy and cybersecurity events that may occur within the respective domains.

Practitioners will note that the security capability descriptions focus primarily on the HDO domain. Capabilities are deployed to other domains to the extent that the HDO may have influence. HDOs may not authoritatively determine the control environment implemented by the telehealth platform provider. HDOs may obtain assurance that similar controls are implemented by the telehealth platform provider before establishing the relationship with the provider. HDOs should establish questionnaires or audit approaches that they may use in evaluating third parties such as telehealth platform providers. HDOs and telehealth platform providers are subject to regulatory requirements to ensure patient privacy and cybersecurity.

Telehealth platform providers are third parties that may implement security capabilities that do not necessarily use the tools standard to the HDO. Telehealth platform providers may provide services for many HDOs, and implementing the same tools for all HDOs may not be feasible from a technical perspective. Telehealth platform providers apply risk management approaches that are appropriate for their business model. While telehealth platform providers may manage risk by using different tools and techniques from the HDO, these providers should address the risk concerns for the HDO. Telehealth platform providers should apply similar measures, e.g., the NIST Cybersecurity Framework [3] and Risk Management Framework [4], that describe risk and control approaches. When evaluating telehealth platform providers, HDOs should review the privacy and security control policies and other documentation to ensure that the mitigation approaches that the telehealth platform provider implements are consistent with the HDO's requirements.

HDOs and telehealth platform providers may find difficulties when implementing security capabilities on the patient home domain. Patients may find complex controls or practices onerous and therefore, they may be less likely to participate in the RPM program. Telehealth platform providers may implement security capabilities for end-point devices such as biometric sensors or mobile devices that are part of the RPM program. HDOs, in collaboration with telehealth platform providers, may offer education and awareness material to discuss appropriate use of RPM-deployed equipment with the patient.

4.4.1 Telehealth Platform Provider

Telehealth platform providers are discussed in this practice guide as a security capability. HDOs implementing RPM programs will depend on telehealth platform providers to enable communications between patients and clinicians. Also, for this practice guide, telehealth platform providers configure, manage, and maintain biometric devices and potentially other technology provided to the patient. HDOs engaging with telehealth platform providers to enable their RPM programs are responsible for ensuring that they apply due diligence and understand the privacy and security capabilities that the telehealth platform provider maintains. HDOs and partners with whom HDOs engage may be responsible for adhering to regulatory compliance and should ensure that HDOs have implemented measures that address compliance concerns as a baseline. Telehealth platform providers represent a third-party partner, and HDOs should evaluate their partners accordingly.

In addition to safeguarding systems that aggregate patient information, telehealth platform providers are responsible for assuring that the biometric devices that are deployed to the patient home include adequate controls that mitigate privacy and security risk. Biometric devices have characteristics that are similar to Internet of Things (IoTs) architecture. Telehealth platform providers should consider clinical efficacy of the devices as well as assure that devices do not pose privacy or cybersecurity harm to the patient home or the broader RPM ecosystem. Appendix E, Benefits of Device Cybersecurity Requirements, discusses challenges that may be found in biometric devices that may be regarded as IoT. Appendix E's roots are founded in a new set of guidance focused on IoT security. NIST is developing several documents that discuss how IoT device manufacturers may incorporate privacy and security measures in products. Telehealth platform providers may monitor document development in *Defining IoT Cybersecurity Requirements: Draft Guidance for Federal Agencies and IoT Device Manufacturers* (NIST SP 800-213, NIST Interagency or Internal Reports 8259B/C/D) publication series [21]. While NIST SP 800-123 focuses on the federal government's IoT deployment efforts, concepts found in the document may inform telehealth platform providers as they evolve their biometric device acquisition processes.

The NIST Cybersecurity Framework includes risk assessment under the Identify Function. This practice guide implements tools for vulnerability management.

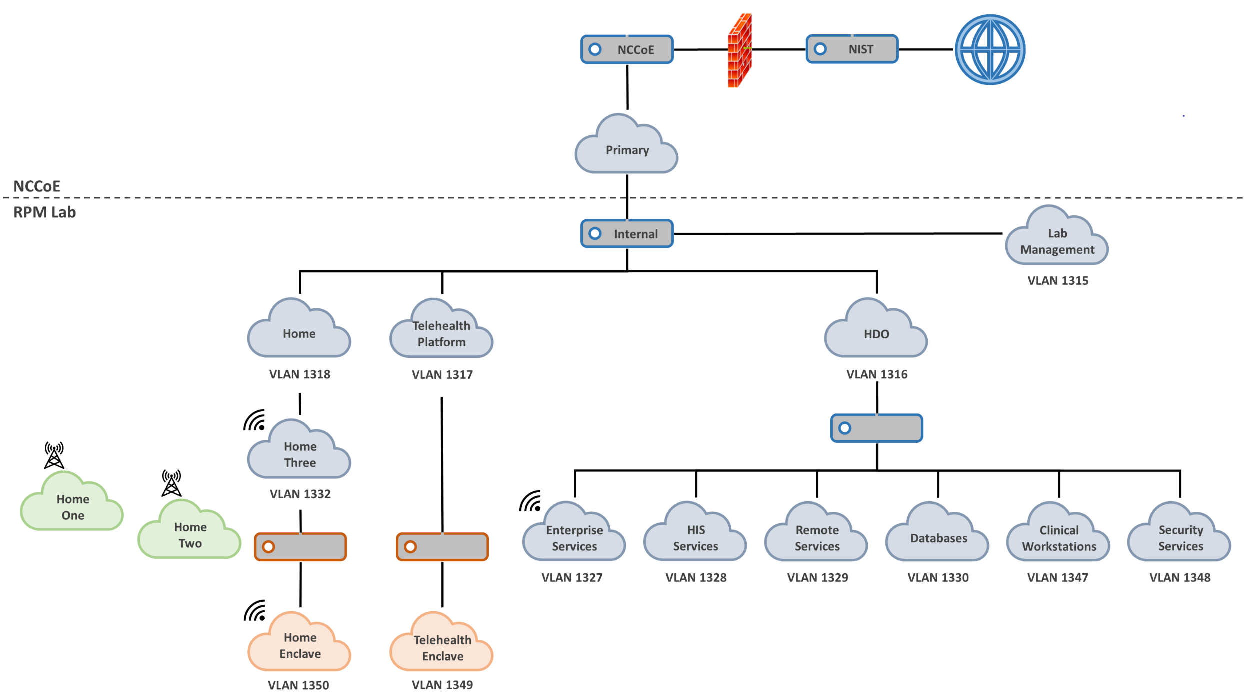
The practice guide uses Tenable.sc with Nessus to perform vulnerability scanning and provide dashboard reports. Vulnerability scanning operates by applying signatures of known vulnerabilities. Components that operate within the HDO domain are subject to regular vulnerability scanning. As vulnerabilities are identified, patching or other mitigating approaches may be applied. Patches or updates to operating systems, apps, or applications may be applied as available.

4.4.2 Identity Management, Authentication, and Access Control

Identity management involves activities that discuss identity proofing and establishing credentials. Authentication for this practice guide provides the mechanisms that assure that authorized entities access the system after telehealth platform providers and HDOs establish respective credentials. Practitioners should refer to NIST SP 1800-24 (reference Section 5.3.3), *Securing Picture Archiving and Communication System (PACS)* [14], which provides more in-depth discussion on identity management and access control. While that practice guide uses different tools and addresses a clinical practice different from RPM, concepts regarding identity management and authentication are relevant for this practice guide.

This practice guide builds upon a network zoning concept that was discussed in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* [20]. Figure 4-6 depicts the lab environment built for this practice guide. The diagram splits the infrastructure between the NCCoE and the RPM lab, with the latter representing the configured simulated environments for this practice guide. Focusing on the HDO cloud depiction, this practice guide simulates the HDO environment that is made up of enterprise services, health information system (HIS) services, remote services, databases, clinical workstations, and security services virtual local area networks (VLANs).

Figure 4-6 Network Segmentation and VLAN Within the RPM Lab



The practice guide extends the network zoning concept between the patient home and the telehealth platform provider. Biometric devices in the patient home using a Wi-Fi communications pathway that traverses a patient-provided broadband connection are secured using a layer 2 over layer 3 solution. In a simulated cloud environment, engineers deployed the layer 2 over layer 3 solution between zones that represent the patient home and a telehealth platform provider. The layer 2 over layer 3 solution segmented the biometric devices from the patient home network into a secured enclave. The enclave assures that network traffic from the patient home is not introduced or have visibility to the biometric devices. The layer 2 over layer 3 solution secures the data in transit communications between the patient home and telehealth platform provider domains respectively and adopts an approach that is consistent with concepts described in NIST SP 800-207, *Zero Trust Architecture* [22].

4.4.3 Data Security

This practice guide examines challenges associated with data loss and data alteration. Communications initiate from the patient home, traversing a public communications channel, and are made accessible to clinicians via internet connectivity. This practice guide addresses the need to provide end-to-end data protection as a vital requirement to ensure RPM viability.

Network sessions are encrypted. Telehealth platform providers implement data security as they manage biometric devices and the dataflow between the patient home and solutions hosted by the telehealth platform provider. Stored data are protected through encryption. The project team examined dataflows and applied a privacy risk assessment that analyzed communications between the implemented components and identified how data-in-transit security controls are implemented.

4.4.4 Anomalies and Events and Security Continuous Monitoring

Managing anomalies and events and performing security continuous monitoring provides a proactive, real-time measure to determine that threats and vulnerabilities are appropriately recognized and mitigated within HDO environments. This practice guide implements several controls that address managing anomalies and events and performing security continuous monitoring. Security engineers require tools and processes to manage anomalies and events that include applying cyber threat intelligence (CTI), collecting and managing log information, and applying behavioral analytics. NIST describes CTI in NIST SP 800-150, *Guide to Cyber Threat Information Sharing* [23]. NIST provides additional detail regarding security continuous monitoring in NIST SP 800-137 [24].

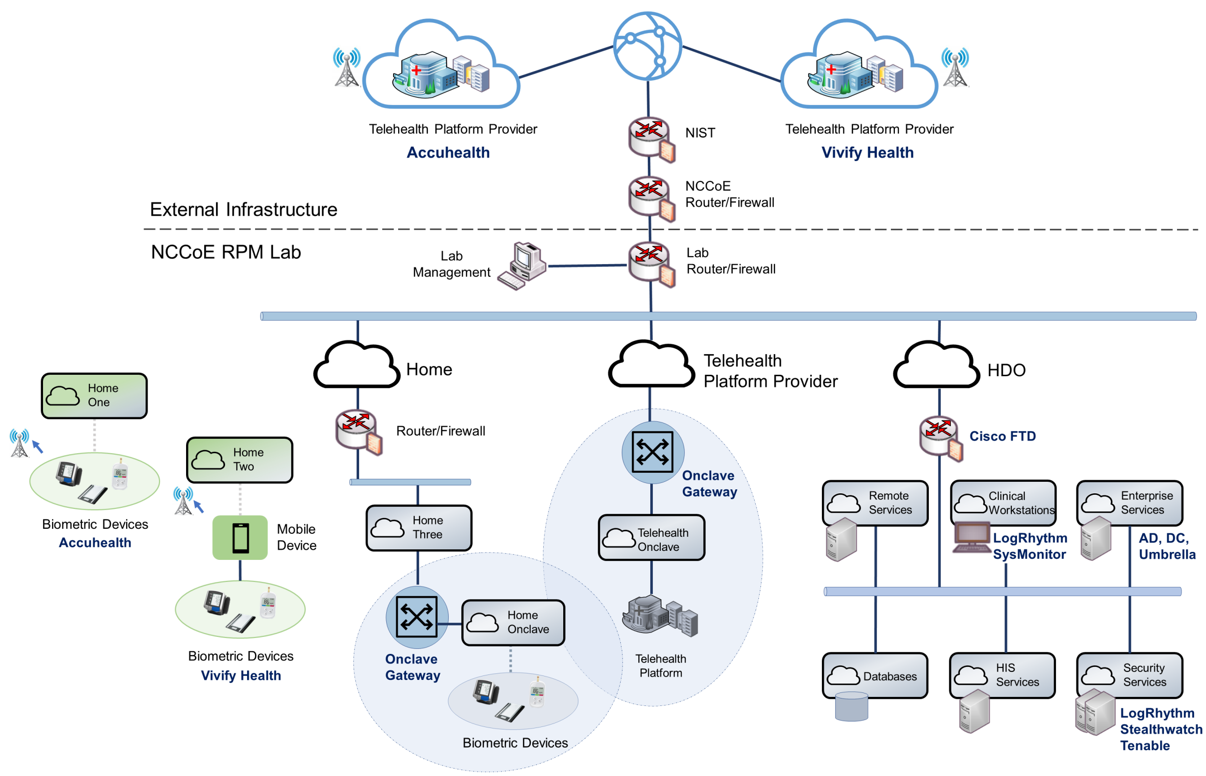
4.5 Final Architecture

The project team built a reference architecture to include two communications pathways for biometric devices. In the first case, biometric devices in the patient home communicated to the telehealth platform provider over cellular data communications. The team built an architecture that addressed communications pathways A and B that were described in Section 4.2, High-Level Architecture Communications Pathways. In the second case, biometric devices communicated to a mobile device, and the mobile device leveraged the patient home Wi-Fi infrastructure. Mobile device communications to the telehealth platform provider are secured by a layer 2 over layer 3 solution through Onclave's Secure IoT platform. Layer 2 over Layer 3 concepts are further described in Appendix F. This scenario aligns with pathway D described in Section 4.2.

Figure 4-7 depicts the final architecture of the lab environment. The two telehealth platform providers, Accuhealth and Vivify, provided cloud-hosted solutions, with biometric devices deployed in respective home environments, described as Home One and Home Two. Biometric devices were provisioned and managed by the telehealth platform providers, with data communications over cellular data. A Home Three environment was provisioned to deploy biometric devices that would communicate over Wi-Fi. The architecture includes a telehealth platform provider hosted in a simulated cloud environment. Engineers implemented a layer 2 over layer 3 solution between Home 3 and the simulated cloud environment.

The architecture also includes an HDO environment with six network zones: Remote Services, Clinical Workstations, Enterprise Services, Databases, HIS Services, and Security Services.

Figure 4-7 Final Architecture



5 Security and Privacy Characteristic Analysis

The purpose of the security and privacy characteristic analysis is to understand the extent to which the project meets its objective of demonstrating the privacy and security capabilities described in the reference architecture in Section 4. In addition, it seeks to understand the security and privacy 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.
- HDOs and telehealth platform providers implement an array of risk mitigation approaches that extend beyond what is discussed in this document. The broader array of controls consists of organizational structures, policies and procedures, and tools to support enterprise privacy and cybersecurity programs that this practice guide refers to as a set of pervasive controls.

5.2 Pervasive Controls

NIST SP 1800-24, *Securing Picture Archiving and Communication System (PACS)* [14], described the use of controls that were termed "pervasive." Subsequent practice guides such as this RPM practice guide discuss implementing controls that narrowly apply to the practice guide's lab construction. Notwithstanding, HDOs and telehealth platform providers are enterprise organizations that may face a broader set of risks, including regulatory requirements, that extend beyond the narrow topic. The pervasive control concept assumes that HDOs and telehealth platform providers have implemented a comprehensive control set to address their risk and regulatory obligation.

For example, onboarding workforce members may involve identity proofing and creating, and managing accounts and credentials. Organizations need to perform these activities to appropriately implement an enterprise risk management program. The requirement is not specific to RPM programs. These functions should be established prior to implementing an RPM program. Other controls, such as performing asset management, having incident response teams, and establishing incident response programs, should also be pervasive across the enterprise.

Another example is asset management. Asset management is a critical control that should be implemented by telehealth platform providers. Telehealth platform providers should maintain accurate inventories and manage configuration settings, patching, updates, and the overall life cycle for devices that are deployed to the patient home. While this is a requirement, the project team partnered with multiple telehealth platform providers. The team did not deploy security or privacy capabilities to the telehealth platform providers. Rather, it relied upon telehealth platform providers to implement an adequate and appropriate set of pervasive controls for their environment and for the services that they provide.

The NIST Cybersecurity Framework [3] describes cybersecurity activities and outcomes that organizations should achieve for establishing or improving enterprise security programs. These activities and outcomes are articulated in the Subcategories of the Cybersecurity Framework Core. The Cybersecurity Framework provides the basis for pervasive controls, whereas this practice guide highlights implementation of selected controls. Readers should not regard the selected controls as the only controls that an HDO must implement. The selected controls that are described in this practice guide are a small subset of controls that HDOs and telehealth platform providers should implement. This practice guide's descriptions of controls indicate how the selected controls were implemented in the lab environment.

5.3 Telehealth Platform Providers

Telehealth platform providers address several controls for the RPM solution. Telehealth platform providers configure, maintain, and manage devices that are deployed to the patient home domain. Telehealth platform providers provision devices to patients who have been enrolled in an RPM program by their HDO. Telehealth platform providers perform asset management for the provisioned devices and thus address ID.AM-1, ID.AM-2, ID.AM-4, ID.AM-5, ID.IM-P1, ID.IM-P2, and ID.IM-P7. Telehealth platform providers are responsible for addressing ID.RA-1.

Telehealth platform providers authenticate sessions based on the device identifier. When patients send or transfer data from biometric devices, data are routed to the telehealth platform provider. The telehealth platform provider receives the data and makes it available to clinicians and system users via a portal. Portals use unique identifiers for credentials (e.g., username/password) and role-based access control and ensure that connections to the portal are protected by using Transport Layer Security (TLS) 1.2.

For this practice guide, telehealth platform providers provisioned two classes of biometric devices: those that used cellular data communications and those that used the patient home-provided Wi-Fi network. In the first category, devices were explicitly not permitted to access Wi-Fi networks. Removing Wi-Fi capability separated RPM communication from network traffic that may have been present in the patient home domain. In the second case that deployed biometric devices that included Wi-Fi capability, those devices leveraged the patient home Wi-Fi environment and used a layer 2 over layer 3 solution to secure connectivity between the RPM devices and the telehealth platform provider.

For biometric devices that focused on cellular data communications, the project team used devices that were equipped to communicate over 4G Long-Term Evolution (LTE), which uses asymmetric encryption between the device and the cellular tower [25]. Further investigation in data-in-transit protection was not determined in this practice guide.

The second case included biometric devices leveraged in the patient home Wi-Fi environment. Network sessions were secured using another product that provided in-transit protection using a layer 2 over layer 3 solution. The project team deployed dedicated gateway devices used to implement a network infrastructure that was consistent with NIST SP 800-207, Zero Trust Architecture[22].

The telehealth platform provider addressed PR.AC-1, PR.AC-4, PR.DS-1, PR.DS-2, PR.DS-4, PR.DS-6, PR.PT-1, PR.PT-3, PR.PT-4, PR.AC-P1, PR.AC-P4, PR.DS-P1, PR.DS-P2, PR.DS-P4, PR.DS-P6, CT.DM-P8, PR.PT-P2, and PR.PT-P3.

The project team implemented telehealth platform provider services with Accuhealth and Vivify Health.

5.4 Risk Assessment (ID.RA and ID.RA-P)

This practice guide implemented tools that address elements of ID.RA-5 (threats, vulnerabilities, likelihoods, and impacts are used to determine risk) and ID.RA-P4. The project team implemented Tenable.sc to address vulnerability management. Tenable includes vulnerability scanning and dashboards that display identified vulnerabilities with scoring and other metrics that enable security engineers to prioritize.

Telehealth platform providers have separate infrastructures and organizational structures that require similar approaches. Telehealth platform providers may host their services with various implementations and may deploy similar solutions for their environments.

5.5 Identity Management, Authentication, and Access Control (PR.AC and PR.AC-P) Protective Technology (PR.PT-P)

The engineers regarded many of the identity management Subcategories as part of a set of pervasive controls that have been discussed in NIST SP 1800-24, *Securing Picture Archiving and Communication System (PACS)* [14]. HDOs and telehealth platform providers should apply similar solutions to address managing human, device, and system identities. Sample solutions are provided in NIST SP 1800-24.

Extending the network zoning concepts that were described in NIST SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations* [20], the project team implemented VLANs with firewall feature sets by using Cisco FTD. This practice guide addresses PR.AC-5 by implementing VLANs that represent network zones found within an HDO. Telehealth platform providers may implement similar measures within their infrastructures.

The NIST Cybersecurity Framework implements identity management, authentication, and access control under the Protect Function by using the PR.AC Category. Within the HDO, the engineers implemented PR.AC-5 by using Cisco FTD to establish network zones as a set of VLANs. The network zones assure that components from each zone do not have implicit trust, and thus compromise on end points found in one zone are limited in their ability to affect devices that operate in other zones.

The Onclave Secure IoT platform creates unique enclaves within the patient home and the telehealth platform provider with their own root of trust for implicit trust.

The engineers implemented three primary Cisco tools for the HDO environment: Cisco Firepower, Cisco Umbrella, and Cisco Stealthwatch. As noted, the project team used Firepower to create and manage VLANs within the environment. Cisco Firepower includes a central management dashboard that allowed security engineers to configure and manage other features within the Cisco suite of tools. Firepower also includes intrusion detection capability and visibility into network traffic and network analytics that enabled engineers to detect and analyze events, monitor the network, and detect malicious code and thus addressed DE.AE-2, DE.CM-1, and DE.CM-4. Cisco Firepower addressed PR.AC-5, PR.PT-4, PR.AC-P5, and PR.PT-P3. The engineers implemented Cisco Umbrella for DNS and IP layer security and provided content and application filtering. Cisco Umbrella addressed DE.CM-4. The team also used Cisco Stealthwatch that implemented behavioral analytics capabilities and provided malware detection. Cisco Stealthwatch addressed PR.DS-5, PR.PT-4, DE.AE-1, DE.CM-1, PR.DS-P5, and PR.PT-P3.

Within the HDO domain, engineers implemented an AD to establish user accounts. AD credentials provided engineers with authentication for several components deployed in the lab. The lab's AD implementation addresses PR.AC-1, PR.AC-4, PR.AC-P1, and PR.AC-P4.

The telehealth platform provider assures that PR.AC-5, PR.AC-6, PR.AC-7, PR.AC-P5, and PR.AC-P6 are met by managing components that are deployed to the patient home. Components that are deployed by the telehealth platform provider are fully managed devices that have been preconfigured and distributed by Accuhealth. The RPM components that Accuhealth provided for the patient home use a cellular communication pathway where unauthorized individuals may not remove or alter SIM cards. The cellular data communication pathway assures that the RPM components are segregated from untrusted devices that may operate in the patient home and thus implements PR.AC-5 and PR.AC-P5.

This practice guide also simulated a use case where a telehealth platform provider provides RPM components that use patient-provided broadband. The simulated test case implements Vivify components; however, it does not reflect how Vivify hosts its services. Biometric devices communicate with an interface device (i.e., the tablet). The simulated environment includes centralized configuration management for interface devices such as the tablet. Management prevents end users from modifying tablet configuration settings or installing unauthorized software. In this use case, biometric devices leverage the patient home Wi-Fi. Engineers secured the devices by leveraging a layer 2 over layer 3 solution to create a secure enclave. The solution segments the biometric devices from the patient home network, with only the biometric devices enabled to communicate over the secure enclave. The secure enclave solution included gateways implemented at the patient home and the simulated telehealth provider. The secure enclave solution supports PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, and PR.PT-4.

RPM-enrolled patients are predetermined by the HDO, and the telehealth platform provider provisions RPM components to an established, known set of patients. HDOs enrolling patients in the RPM program partially addresses PR.AC-1 and PR.AC-P1. Clinicians identifying patients may be regarded as performing an identity-proofing activity, whereas telehealth platform providers may complete PR.AC-1 and PR.AC-

P1 activities by creating accounts or records that relate to the patient and the RPM equipment that the patient receives.

Patient-provided (e.g., "bring your own device") biometric devices were excluded in this practice guide's architecture. The telehealth platform provider manages patient home-deployed components and thus assures that PR.AC-6 and PR.AC-P6 are addressed.

For this practice guide, the telehealth platform provider manages components that it procured and configured. The telehealth platform provider configures the devices to include authenticators that enforce component authentication. For this practice guide, only biometric devices that are managed by telehealth platform providers are provisioned authenticators. This implements PR.AC-7 and PR.AC-P6. Patient homes may include other devices, such as personally owned devices, that are not a part of the RPM ecosystem. Devices that are not managed by telehealth platform providers do not have authentication credentials for the RPM solution. One should note that this practice guide simulated a telehealth platform provider when exploring biometric devices that communicate over broadband.

5.6 Data Security (PR.DS and PR.DS-P)

This practice guide implemented PR.DS-2 and PR.DS-P2 to ensure that data-in-transit are protected. HDOs connecting to cloud-hosted consoles used TLS 1.2 [26]. The telehealth platform provider assured implementation of PR.DS-3 and PR.DS-P3 for RPM biometric devices deployed to the patient home.

For biometric devices that communicate over broadband, the project team secured network sessions using a layer 2 over layer 3 solution that is established using the Onclave Secure IoT platform. The solution segmented biometric devices and their communication from the patient home network. Network sessions between the patient home and the simulated telehealth platform provider used TLS 1.2. The Onclave Secure IoT platform used a key management mechanism that is consistent with guidance from NIST SP 800-57 Part 1, Revision 5, *Recommendation for Key Management: Part 1–General* [27]. The Onclave IoT Platform solution secured sessions using a private blockchain. Data-in-transit used Advanced Encryption Standard (AES)256 encryption [28]. This addresses PR-DS-2 and PR-DS.5 for communications between the patient home and the simulated telehealth platform provider.

Accuhealth and Vivify Health use AES256 encryption [28] for data-at-rest and address PR.DS-1 and PR.DS-P1.

5.7 Anomalies and Events, Security Continuous Monitoring (DE.AE, DE.CM), and Data Processing Management (CT.DM-P)

The project team implemented LogRhythmXDR as a security incident and event management (SIEM) tool. End-point devices that include servers and network infrastructure components generate log data that were aggregated in the SIEM tool for analysis. LogRhythm included two components: LogRhythmXDR and LogRhythm NetworkXDR. SIEM capabilities provide security engineers a baseline of network operations and allow security engineers to determine expected dataflows for users and systems. Engineers can detect events and analyze potential threats. LogRhythmXDR, therefore, is a SIEM that addresses NIST Cybersecurity Framework Subcategories ID.RA-5, PR.PT-1, DE.AE-1, DE.AE-2, ID.RA-P4, and CT.DM-P8. LogRhythm NetworkXDR provides capabilities that assure that the network is monitored for potential cybersecurity threats. It also provides assurance that unauthorized mobile code is detected and thus addresses DE.CM-7. This practice guide assures implementation of a network monitoring capability based on regular log collection and applies the SIEM analytics and automated response capabilities. The project team implemented Cisco Firepower; Cisco Stealthwatch; and Cisco Umbrella, which detects malicious code, detects unauthorized mobile code, and provides continuous network monitoring and analytics. Therefore, the Cisco suite addresses DE.CM-4 and DE.CM-5.

6 Functional Evaluation

This practice guide uses the NIST Cybersecurity Framework. The Cybersecurity Framework includes Category and Subcategory concepts that allowed the project team to develop a reference architecture. The reference architecture reflects use cases and dataflows analyzed by the NCCoE. This practice guide aligns privacy and cybersecurity tools to Cybersecurity Framework Subcategories. The reference architecture depicts where tools were deployed.

6.1 RPM Functional Test Plan

One aspect of our security evaluation involved assessing how well the reference design addresses the security characteristics that it was intended to support. The Cybersecurity Framework Categories and Subcategories were used to provide structure to the security assessment by consulting the specific sections of each standard that are 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.

6.1.1 RPM Functional Evaluation

Table 6-1 identifies the RPM functional evaluation 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 6-1 Functional Evaluation Requirements

Cybersecurity Framework Category	Relevant Cybersecurity Framework Subcategories	Identifier	Requirement	Domain	Test Case
asset management	ID.AM-1 ID.AM-5	CR-1	device management	home telehealth platform provider	RPM-1
risk assessment	ID.RA-1 ID.RA-4 ID.RA-5 ID.RA-6	CR-2	end-point vulnerability scanning	HDO	RPM-2
identity management, authentication, and access control	PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6	CR-3	role-based access	telehealth platform provider	RPM-3
		CR-4	domain user authentication	HDO	RPM-4
		CR-5	domain user authorization	HDO	RPM-4
		CR-6	network segmentation	HDO	RPM-5
		CR-7	access control policy	HDO	RPM-5
security continuous monitoring	DE.CM-1 DE.CM-2 DE.CM-4 DE.CM-7 DE.CM-8	CR-8	malware protection	HDO	RPM-6
		CR-9	anomaly detection	HDO	RPM-7
		CR-10	LogRhythm	HDO	RPM-8
		CR-11	LogRhythm	HDO	RPM-9
data security	PR.DS-2	CR-12	data-in-transit is protected.	home telehealth platform provider	RPM-10
N/A	N/A	CR-13	business workflow	home	RPM-11

Cybersecurity Framework Category	Relevant Cybersecurity Framework Subcategories	Identifier	Requirement	Domain	Test Case
				telehealth platform provider HDO	

1107 ### 6.1.2 Test Case: RPM-1

Cybersecurity Framework Category	**Asset Management**
Testable Requirement(s)	**(CR-1)** device management
Description	Demonstrate the ability to verify that provisioned devices are associated with the intended patient who has enrolled in an RPM program.

Preconditions	▪ A doctor-level Accuhealth account has been provisioned.
	▪ Accuhealth RPM devices have been provisioned and delivered, including the following (obfuscated serial number):
	    o blood pressure monitor (1234567)
	    o blood glucose monitoring system (22334455)
	    o digital scale (987654)
	▪ Accuhealth has enrolled sample patients and associated them with the RPM devices listed above, including:
	    o Regina Houston (1234567)
	    o Regina Houston (987654)
	    o Janelle Kouma (22334455)

Procedure	Verify the patient/device association in the Accuhealth system. 1. Log in to the Accuhealth platform with the doctor-level user account. 2. Click **Patient Details.** 3. Under **Select Patient,** select **Regina Houston.** 4. Under **Choose a view,** select **Profile.** 5. Review the patient info for **Regina Houston.** 6. Navigate to **Device Information.** 7. Check if the **Device ID** field captures the device serial numbers, **1234567** and **987654,** that are associated with **Regina Houston.** 8. Under **Select Patient,** select **Janelle Kouma.** 9. Review the patient information for **Janelle Kouma.** 10. Navigate to **Device Information.**

	11. Check if the **Device ID** field captures the device serial number, **22334455,** associated with **Janelle Kouma.** Verify that data from the RPM devices is being sent to Accuhealth and associated with the correct patient. 12. For the following devices, turn on each device and follow the provided instructions to take a measurement: a. **blood pressure monitor** b. **blood glucose monitoring system** c. **digital scale** 13. Record the time and measurement readings as notes. 14. Log in to the Accuhealth platform with the **doctor-level user account.** 15. Click **Patient Details.** 16. Under **Select Patient,** select **Regina Houston.** 17. Under **Choose a view,** select **Vitals.** 18. Check if the **blood pressure** and **weight measurements** are present. 19. Under **Select Patient,** select **Janelle Kouma.** 20. Under **Choose a view,** select **Vitals.** 21. Check if the **glucose measurement** is present.
Expected Results	▪ Accuhealth can provision the RPM devices and associate them to the intended patient enrolled in an RPM. ▪ Accuhealth can capture the biometric measurements for the correct patient with the assigned RPM devices.
Actual Results	Accuhealth provisioned an instance of its telehealth platform along with doctor-level accounts and sample patients associated with these accounts. We also received three RPM devices from Accuhealth: blood pressure monitor, blood glucose monitor, and digital scale. Accuhealth associated these RPM devices with the sample patients, which we verified by checking the Device ID information for each patient. Once the devices were received, we configured them and recorded sample measurements from each one. With the measurements taken, we logged in to the Accuhealth platform with the doctor-level account and viewed the Vitals information for each patient. As expected, the blood pressure and weight measurements were associated with Regina Houston’s patient record, and the blood glucose measurement was associated with Janelle Kouma’s patient record.

1108
6.1.3 Test Case: RPM-2

Cybersecurity Framework Category	**Risk Assessment**
Testable Requirement(s)	**(CR-2)** end-point vulnerability scanning
Description	Demonstrate the ability to perform vulnerability scans on assets and view results in a dashboard format with risk-scoring evaluations.
Preconditions	▪ Tenable.sc has been configured with the following: o organization o repository o security manager user account o scan zones for each VLAN o host discovery scan policy o basic network scan policy o active scans associated with each scan policy ▪ A Nessus scanner has been deployed to the Security Services VLAN and is being managed by Tenable.sc. ▪ The Nessus scanner has access to each scan zone.
Procedure	Perform scans and view the results. 1. Log in to Tenable.sc with the security manager user account. 2. Navigate to **Scans > Active Scans.** 3. Under **HDO Asset Scan,** click the **run button (▶).** 4. Wait for the HDO Asset Scan to finish. 5. Under **HDO Network Scan,** click the **run button (▶).** 6. Wait for the HDO Network Scan to finish. 7. Click **Dashboard** in the menu ribbon. 8. Check if the risk assessment results are displayed.
Expected Results	▪ Tenable.sc and Nessus scan the HDO VLANs, identify vulnerabilities, and assign risk scores to discovered threats. ▪ Tenable.sc displays risk assessment scan results in the dashboard.
Actual Results	Using Tenable.sc, we ran a host discovery scan followed by a basic network scan. Once both scans were finished, we returned to the Tenable.sc dashboard and were able to view the results. The Nessus scanner was able to identify end points in the scan zones (VLANs) as well as potential vulnerabilities with associated risk scores.

1109
6.1.4 Test Case: RPM-3

Cybersecurity Framework Category	**Identity Management, Authentication, and Access Control**
Testable Requirement(s)	**(CR-3)** role-based access

Description	Demonstrate the ability to limit and disable access to data by implementing role-based access control on the Vivify platform.
Preconditions	▪ Vivify has provisioned a telehealth platform environment. ▪ Vivify has provisioned an administrative user account. ▪ Three test patients have been created in the Vivify platform: o Test Patient 1 o Test Patient 2 o Test Patient 3
Procedure	<u>Create a Clinical Level 1 user account, and test account privileges</u>. 1. Log in to the Vivify platform by using the provisioned admin account. 2. Click **Care Team** in the menu bar. 3. Create a **New User** assigned to the **Clinical Level 1** user group. 4. Access the **Test Patient,** and add the new user into the Care Team for this patient. 5. Log out of the environment. 6. Log in to the environment with the user created in **step 3.** 7. Check if the account has read-only access to patient records associated with that clinician level. <u>Create a Clinical Level 2 user account, and test account privileges</u>. 8. Log in to the Vivify platform by using the provisioned admin account. 9. Click **Care Team** in the menu bar. 10. Create a **New User** assigned to the **Clinical Level 2** and **Clinical Level 1** user groups. 11. Access the **Test Patient 2,** and add the new user into the Care Team for this patient. 12. Log out of the environment. 13. Log in to the environment with the user created in **step 10.** 14. Check if the account has read and write access to patient records associated with that clinician level. <u>Create a Clinical Level 3 user account, and test account privileges</u>. 15. Log in to the Vivify platform by using the provisioned admin account. 16. Click **Care Team** in the menu bar. 17. Create a **New User** assigned to the **Clinical Level 3, Clinical Level 2,** and **Clinical Level 1** user groups. 18. Log out of the environment. 19. Log in to the environment with the user created in **step 17.**

	20. Check if the account has read and write privileges for all patient records.
Expected Results	▪ A user account in the Clinical Level 1 group should be able to read only patient records assigned to that clinician. ▪ A user account in the Clinical Level 2 should be able to read and write only to patient records assigned to that clinician. ▪ A user account in the Clinical Level 3 should be able to read and write to all patient records.
Actual Results	We started by logging in to the provisioned Vivify portal with our admin credentials and creating three new Care Team users, each with their own access levels. The first user was granted Clinical Level 1 and was added as Care Team of the test patient; the second was granted Clinical Levels 1 and 2 and was added as Care Team of the test patient; and the third was granted Clinical Levels 1 through 3. Then we logged in as each new user and tested their privileges. The first user was able to only view patient records that assigned to her. The second user was able to view and modify patient records that associated only with those assigned to her. The third user was able to view and modify all patient records.

1110 ### 6.1.5 Test Case: RPM-4

Cybersecurity Framework Category	**Identity Management, Authentication, and Access Control**
Testable Requirement(s)	**(CR-4)** domain user authentication **(CR-5)** domain user authorization
Description	Demonstrate the ability to create new domain users and enforce restrictions on nonadmin users.
Preconditions	▪ A Windows Server is deployed to the **Enterprise Services** VLAN. ▪ The Windows Server has been configured as an Active Directory Domain Controller for the **hdo.trpm** domain. ▪ A Windows workstation is deployed to the **Enterprise Services** VLAN and has been added to the **hdo.trpm** domain. ▪ A Windows workstation is deployed to the **Clinical Workstations** VLAN and has been added to the **hdo.trpm** domain. ▪ A Cisco Firepower access control policy rule has been created, allowing network traffic from the **Clinical Workstations** VLAN to the **Enterprise Services** VLAN. ▪ The Cisco FTD appliance has been configured to provide Dynamic Host Configuration Protocol (DHCP) services for the **Enterprise Services** and **Clinical Workstations** VLANs.
Procedure	Create a nonadmin domain user.

	1. Power on the Windows Server and log in.
	2. Open the **Server Manager** application.
	3. Navigate to **Tools > Active Directory Users and Computers.**
	4. Navigate to **hdo.trpm > Users.**
	5. Click **Create a new user in the current container.**
	6. Fill out the user's information:
	    a. **First Name:** User
	    b. **Last Name:** Test
	    c. **User logon name:** usertest
	7. Click **Next >.**
	8. Create a password for the user.
	9. Uncheck **User must change the password at next logon.**
	10. Click **Next >.**
	11. Click **Finish.**
	12. Right-click the user's profile, and select **Properties.**
	13. Click **Member Of.**
	14. Ensure that the user is a member of only **Domain Users.**
	
	<u>Create an admin domain user</u>.
	15. Navigate to **hdo.trpm > Users.**
	16. Click **Create a new user in the current container.**
	17. Fill out the user's information:
	    a. **First Name:** Admin
	    b. **Last Name:** Test
	    c. **User logon name:** admintest
	18. Click **Next >.**
	19. Create a password for the user.
	20. Uncheck **User must change the password at next logon.**
	21. Click **Next >.**
	22. Click **Finish.**
	23. Right-click the user's profile, and select **Properties.**
	24. Click **Member Of.**
	25. Click **Add….**
	26. Type **Domain,** and click **Check Names.**
	27. Select **Domain Admins.**
	28. Click **OK.**
	29. Click **OK.**
	
	<u>Create network share folder</u>.
	30. Power on the Windows workstation in the **Enterprise Services** VLAN, and log in with an administrator account.
	31. Right-click the **Windows Start Button.**

	32. Click **Windows PowerShell (Admin).** 33. Run the command `ipconfig` 34. Note the **IP address** (192.168.40.107). 35. Open the **File Explorer** application. 36. Navigate to **This PC > Local Disc (C:).** 37. Under **Home,** click **New Folder.** 38. Name the folder **Share.** 39. Right-click the new folder, and select **Properties.** 40. Under **Sharing,** click **Share….** 41. Click the drop-down, and select **Find people….** 42. Type **Domain,** and click **Check Names.** 43. Select **Domain Admins.** 44. Click **OK.** 45. Click **OK.** 46. Click **Share.** 47. Click **Done.** 48. Create a new text document inside the **Share** folder, and name it **AccessTest.** <u>Test ability to access network share folder with nonadmin user</u>. 49. Power on the Windows workstation in the **Enterprise Services** VLAN. 50. Log in with the nonadmin account, **usertest,** that was created in the previous steps. 51. Right-click the **Windows Start Button.** 52. Click **Run.** 53. Under **Open,** type **\\192.168.40.107\Share.** 54. Click **OK.** 55. Check if a network error is displayed, stating that the user does not have permission to access the network share folder. <u>Test ability to access network share folder with admin user</u>. 56. Log out of the nonadmin account. 57. Log in with the admin account, **admintest,** that was created in the previous steps. 58. Right-click the **Windows Start Button.** 59. Click **Run.** 60. Under **Open,** type **\\192.168.40.107\Share.** 61. Click **OK.** 62. Check if the network share folder is opened and the **AccessTest** text document is visible.

Expected Results	▪ After the nonadmin and admin domain users have been created, they will be able to use their credentials to log in to computers within the domain. ▪ Only the admin domain user will be able to access the network share folder.
Actual Results	Once the user accounts were created and the network share folder was created and configured, we began by logging in to a domain computer with the nonadmin domain user. The user was able to successfully log in. Next, we tested the user's ability to access the network share folder. The nonadmin domain user was not able to access the network share folder, receiving a network error stating that the user did not have the proper permissions. Finally, we were able to successfully log in to a domain computer with the admin domain user's account. With this user, we were also able to successfully access the network share folder and view the files within.

1111 ### 6.1.6 Test Case: RPM-5

Cybersecurity Framework Category	**Identity Management, Authentication, and Access Control**
Testable Requirement(s)	**(CR-6)** network segmentation **(CR-7)** access control policy
Description	Demonstrate the use of network segmentation and an access control policy to allow permitted traffic to selected network devices.
Preconditions	▪ The Cisco FTD appliance's interfaces are configured. ▪ A Windows Server is deployed to the **Clinical Workstations** VLAN. ▪ The Windows Server has been configured with a basic Internet Information Services (IIS) web service. ▪ A Windows workstation is deployed to the **Clinical Workstations** VLAN. ▪ A Windows workstation is deployed to the **Enterprise Services** VLAN. ▪ A Cisco Firepower access control policy has been configured, with a default action of **Block All Traffic,** and applied to the Cisco FTD appliance. ▪ The Cisco FTD appliance has been configured to provide DHCP services for the **HIS Services** and **Clinical Workstations** VLANs.
Procedure	<u>Test connectivity between devices in the same subnet</u>. 1. Power on the Windows workstation, and log in. 2. Power on the Windows Server, and log in. 3. On the Windows workstation, right-click the **Windows Start Button.**

4. Click **Windows PowerShell (Admin).**
5. Run the command `ipconfig`
6. Note the **IP address** (192.168.44.101).
7. On the Windows Server, right-click the **Windows Start Button.**
8. Click **Windows PowerShell (Admin).**
9. Run the command `ipconfig`
10. Ensure that the **IP address** (192.168.44.102) is in the same subnet as the Windows workstation.
11. On the Windows workstation, open an internet browser.
12. In the address bar, type in the address of the Windows Server, **http://192.168.44.102.**
13. Check if the default IIS landing page is displayed.

<u>Test connectivity between devices in separate subnets with no access control policy rules set</u>.

14. Power off the Windows Server.
15. Move it to the **HIS Services** VLAN.
16. Power on the Windows Server, and log in.
17. On the Windows workstation, right-click the **Windows Start Button.**
18. Click **Windows PowerShell (Admin).**
19. Run the command `ipconfig`
20. Note the **IP address** (192.168.41.100).
21. On the Windows workstation, open an internet browser.
22. In the address bar, type in the address of the Windows Server, **http://192.168.41.100.**
23. Check if the connection times out and the IIS web service cannot be reached.

<u>Test connectivity between devices in separate subnets with an access control policy rule set to allow</u>.

24. Power on the Windows workstation in the **Enterprise Services** VLAN, and log in.
25. Open an internet browser.
26. In the address bar, type in the address of the Cisco FMC, **https://192.168.40.100.**
27. Log in to the Cisco FMC with your admin credentials.
28. Navigate to **Policies > Access Control > Access Control.**
29. Select the default access control policy.
30. Click **Add Rule.**
31. Give the rule a name.
32. Set the rule's action to **Allow.**

	33. Under **Networks > Source Networks,** type the IP address of the Windows workstation in the **Clinical Workstations** VLAN (192.168.44.101). 34. Click **Add.** 35. Under **Networks > Destination Networks,** type the IP address of the Windows Server in the **HIS Services** VLAN (192.168.41.100). 36. Click **Add.** 37. Under **Ports > Available Ports,** select **HTTP,** and click **Add to Destination.** 38. Click **Add** to create the rule. 39. Click **Save** and **Deploy** the configuration to the Cisco FTD. 40. On the Windows workstation in the **Clinical Workstations** VLAN, open an internet browser. 41. In the address bar, type in the address of the Windows Server in the **HIS Services** VLAN, **http://192.168.41.100.** 42. Check if the default IIS landing page is displayed.
Expected Results	▪ Devices in separate subnets are not able to communicate with each other until an access control policy rule has been created to allow that communication.
Actual Results	When the workstation and server were both placed inside the Clinical Workstations VLAN, the workstation was able to access the server's web service, successfully displaying the server's default IIS web page. After the server was moved to the HIS Services VLAN, the workstation was no longer able to reach the server's web service. Instead of displaying the default IIS web page, the workstation's internet browser returned an error code and stated that the web service could not be reached. A new access control policy rule was created and applied to the Cisco FTD, allowing hypertext transfer protocol (HTTP) traffic from the workstation to the server. Once the rule was created, the workstation was able to access the server's web service and display the default IIS web page.

1112
6.1.7 Test Case: RPM-6

Cybersecurity Framework Category	**Security Continuous Monitoring**
Testable Requirement(s)	**(CR-8)** malware protection
Description	Demonstrate the ability to protect the network and end points from malicious services by blocking the service before a connection is made.
Preconditions	▪ Two Cisco Umbrella Forwarder appliances have been deployed to the **Enterprise Services** VLAN.

	▪ The domain's DHCP service has been configured to provide the Cisco Umbrella Forwarder appliances as the primary and secondary DNS providers. ▪ A Cisco Umbrella policy has been created, with no malware blocking, and has been applied to the Cisco Umbrella Forwarder appliances. ▪ A Windows workstation is deployed to the **Clinical Workstations** VLAN.
Procedure	Test connectivity to outside malicious service with no Umbrella policy. 1. Power on the Windows workstation, and log in. 2. Right-click the **Windows Start Button.** 3. Click **Windows PowerShell (Admin).** 4. Run the command `ipconfig/all`**.** 5. Under **DNS Servers,** ensure that the IP addresses listed correspond to the deployed Cisco Umbrella Forwarder appliances, **192.168.40.30** and **192.168.40.31.** 6. Open an internet browser. 7. In the address bar, type in the address of Cisco's malware test page, **examplemalwaredomain.com.** 8. Check if the site loads and no block message is displayed. Test connectivity to outside malicious service with Umbrella policy. 9. Open an internet browser. 10. In the address bar, type in the address of the Cisco Umbrella dashboard, **dashboard.umbrella.com.** 11. Log in to the Cisco Umbrella dashboard with your admin credentials. 12. Navigate to **Policies > Management > All Policies.** 13. Open the policy applied to the Cisco Umbrella Forwarder appliances. 14. Under **Security Setting Applied,** click **Edit.** 15. Under **Categories to Block,** click **Edit.** 16. Click the checkbox next to **Malware.** 17. Click **Save.** 18. Click **Proceed** to confirm the changes. 19. Click **Set & Return** to save the default settings. 20. Click **Save** to update the policy applied to the Cisco Umbrella Forwarder appliances. 21. On the Windows workstation in the **Clinical Workstations** VLAN, open an internet browser.

	22. In the address bar, type in the address of Cisco's malware test page, **examplemalwaredomain.com.** 23. Check if the site does not load and a Cisco Umbrella block message is displayed.
Expected Results	▪ When the Cisco Umbrella policy is active, devices within the HDO environment will not be able to access potentially malicious web services outside the HDO.
Actual Results	To start, the Cisco Umbrella policy applied to the Forwarder appliances was not configured to block external sites that have been flagged for potential malware. Using a workstation in the Clinical Workstations VLAN, we navigated to a test malware site hosted by Cisco (examplemalwaredomain.com) to verify Cisco Umbrella's effectiveness. Without the malware policy in place, the workstation was able to successfully reach the test malware site. After this, the Cisco Umbrella policy was configured to block external sites that have been flagged for potential malware. With the policy in place, the workstation was used again to connect to the test malware site, this time receiving a Cisco Umbrella block page notifying us that access to the site was not permitted.

1113
6.1.8 Test Case: RPM-7

Cybersecurity Framework Category	**Security Continuous Monitoring**
Testable Requirement(s)	**(CR-9)** malicious activity detection
Description	Demonstrate the ability to detect anomalous network traffic, and create an alert for further investigation.
Preconditions	▪ Cisco Stealthwatch has been configured and licensed. ▪ A Cisco Stealthwatch Flow Collector has been deployed to the Security Services VLAN and is being managed by the Cisco Stealthwatch Management Console (SMC). ▪ The Cisco FTD has been configured to send NetFlow traffic to the Cisco Stealthwatch Flow Collector for analysis. ▪ A Windows workstation is deployed to the **Security Services** VLAN. ▪ An Ubuntu workstation, with the Nmap tool installed, has been deployed to the **HIS Services** VLAN.
Procedure	Configure Cisco Stealthwatch policy rule. 1. Power on the Ubuntu workstation, and log in. 2. Run the command `ifconfig` 3. Note the **IP address** (192.168.41.10). 4. Power on the Windows workstation, and log in.

	5. Open an internet browser. 6. In the address bar, type in the address of the Cisco SMC, **https://192.168.45.30.** 7. Log in to the Cisco SMC with your admin credentials. 8. Navigate to **Configure > Policy Management.** 9. Click **Create New Policy,** and select **Single Host Policy.** 10. Under **IP Address,** type the IP address of the Ubuntu workstation, **192.168.41.10.** 11. Click **Select Events.** 12. Select **Recon.** 13. Click **Apply.** 14. Under **When Host is Source,** select **On + Alarm.** 15. Click **Save.** Test ability for Cisco Stealthwatch to detect a network discovery scan and create an alert. 16. On the Ubuntu workstation, run the command `nmap 192.168.40.0/24` to perform a host scan of the **Enterprise Services** VLAN. 17. On the Windows workstation, bring up the Cisco Stealthwatch session, and navigate to **Dashboards > Network Security.** 18. Check if the scan from the Ubuntu workstation has triggered one or more alarms.
Expected Results	▪ The network scans from the Ubuntu workstation will trigger some form of alert from Cisco Stealthwatch.
Actual Results	Once the Cisco Stealthwatch policy rule had been created, it took roughly a minute after the Nmap scan had run to begin displaying alerts on the Cisco Stealthwatch dashboard. The Ubuntu workstation from which the scans originated, **192.168.41.10,** was listed on the dashboard under **Top Alarming Hosts** and was also listed in the **Recon** category under **Today's Alarms.** On top of triggering the **Recon** rule that we had created, the scans also triggered a **New Flows Initiated** alarm for exceeding a threshold number of new flows within a set period.

1114 ### 6.1.9 Test Case: RPM-8

Cybersecurity Framework Category	**Security Continuous Monitoring**
Testable Requirement(s)	**(CR-10)** end-point monitoring and protection
Description	Demonstrate the ability to detect unusual authentication behaviors and file integrity changes on protected end points.

Preconditions	▪ LogRhythmXDR has been configured and licensed. ▪ A Windows Server is deployed to the **Clinical Workstations** VLAN. ▪ The Windows Server has a **LogRhythm System Monitor Agent** installed.
Procedure	Enable user activity monitor services on the Clinical Workstation. 1. Power on the LogRhythmXDR host, and log in. 2. Start the **Management Console** application. 3. Click **Deployment Manager.** 4. Click **System Monitors.** 5. Double-click the **Windows Server.** 6. Click **Endpoint Monitoring.** 7. Click **User Activity Monitor.** 8. Click the checkbox next to **Monitor Logon Activity.** 9. Click the checkbox next to **Monitor Network Session Activity.** 10. Click the checkbox next to **Monitor Process Activity.** 11. Click **OK.** Create a file integrity monitor policy for the Clinical Workstation. 12. Power on the Windows Server, and log in with an administrator account. 13. Open the **File Explorer** application. 14. Navigate to **This PC > Local Disc (C:).** 15. Create a new folder, and name it **testdirectory.** 16. Create a new text document inside the **testdirectory** folder and name it **testfile.** 17. On the LogRhythmXDR workstation, open the **Management Console** application. 18. Click **Deployment Manager.** 19. Under **Tools,** select **Administration.** 20. Click **File Integrity Monitor Policy Manager.** 21. In the **dialog box,** right-click and select **New.** 22. Name the policy **NCCoE Testdirectory.** 23. Provide a **Description.** 24. Under **Monitoring Configuration,** right-click and select **New.** 25. Name the policy **testdirectory configuration.** 26. Under **Monitoring Flags,** select **Modify** and **Permission.** 27. Under **Monitored Items,** right-click and select **New.** 28. Under **Type,** select **Directory.** 29. Under **Path,** type **C:\testdirectory.** 30. Click **Apply.** 31. Click **OK.** 32. Click **System Monitors.**

	33. Double-click the **Windows Server.** 34. Click **Endpoint Monitoring.** 35. Click **File Integrity Monitor.** 36. Click the checkbox next to **Enable File Integrity Monitor.** 37. Select **Realtime** mode. 38. Click the checkbox next to **Enable Realtime Mode Anomaly Detection.** 39. Under **Policy,** select **NCCoE Testdirectory.** 40. Click **Apply.** 41. Click **OK.** <u>Create an artificial intelligence (AI) engine rule</u>. 42. Click **Deployment Manager.** 43. Click **AI Engine.** 44. Click **Create a New Rule.** 45. Under **Rule Block Types,** select and drag a **rule block** to the **Rule Block Designer.** 46. Under each tab, fill out the necessary information. 47. Click **Next.** 48. Click **OK.** 49. Create a rule for **Authentication Failure Monitoring.** a. **AI Engine Rule Name:** NCCoE Authentication failure threshold b. **Data Source:** Data Processor Logs c. **Primary Criteria -> Classification:** Authentication Failure d. **Log Sources:** All Log Sources e. **Group By:** Host (Impacted), User (Origin) 50. Create a rule for **File Integrity Monitoring.** a. **AI Engine Rule Name:** NCCoE Use Case File Activity b. **Data Source:** Data Processor Logs c. **Primary Criteria -> Common Event:** File Monitoring Event–Add, File Monitoring Event–Modify d. **Log Sources:** All Log Sources e. **Group By:** User (Origin), Object 51. For both new rules, click the checkbox for **Action.** 52. Under **Actions,** select **Enable.** <u>Test user activity monitoring</u>. 53. Power on the Windows Server. 54. Attempt to log in with a username and invalid password at least five times.

	View user authentication failure alerts. 55. On the LogRhythmXDR host, open an internet browser. 56. In the address bar, type in the address of the LogRhythm Web Console, **https://logrhythm-host:8443,** and log in. 57. Click the **Alarms** tab. 58. Check for alerts coinciding with the user authentication failures. Test file integrity monitoring. 59. On the Windows Server, log in with an administrator account. 60. Open the **File Explorer** application. 61. Navigate to **This PC > Local Disc (C:) > testdirectory.** 62. Open the **testfile** text document. 63. Modify the content of the **testfile** text document. 64. Under **File,** select **Save.** View file integrity monitoring alerts. 65. On the LogRhythmXDR workstation, open an internet browser. 66. In the address bar, type in the address of the LogRhythm Web Console, **https://logrhythm-host:8443,** and log in. 67. Click the **Alarms** tab. 68. Check for alerts coinciding with the file modification.
Expected Results	▪ The unusual authentication behavior will trigger an alarm event that is viewable in the LogRhythm Web Console. ▪ The unauthorized file modification will trigger an alarm event that is viewable in the LogRhythm Web Console, and log files will identify the user who has performed the file modification.
Actual Results	Once LogRhythmXDR was configured to provide user activity monitoring and file integrity monitoring, we began by testing the user activity monitoring. For this test, we powered on the Windows Server in the Clinical Workstations VLAN that had been configured with a LogRhythm System Monitor Agent. We made five consecutive login attempts using an invalid password, which was then detected by LogRhythm, and an alert was created that was visible on the LogRhythm Web Console. Next, we tested the file integrity monitoring. For this test, we logged in to the Windows Server in the Clinical Workstations VLAN and made some modifications to the **testfile** text document in the C:\testdirectory folder. Once the changes had been saved, an alarm was triggered and visible in the LogRhythm Web Console. From the alert, we could also drill down to the event and determine what user had made the modification.

6.1.10 Test Case: RPM-9

Cybersecurity Framework Category	**Security Continuous Monitoring**
Testable Requirement(s)	**(CR-11)** end-point network access monitoring
Associated Test Case(s)	▪ RPM-8
Description	This test case demonstrates the ability to create alarms for unauthorized network traffic.
Preconditions	▪ LogRhythm NetworkXDR has been configured and licensed. ▪ A Windows Server is deployed to the **Clinical Workstations** VLAN. ▪ The Windows Server has a **LogRhythm System Monitor Agent** installed.
Procedure	<u>Enable user network connection monitor on the Clinical Workstation</u>. 1. Power on the LogRhythmXDR host, and log in. 2. Start the **Management Console** application. 3. Click **Deployment Manager.** 4. Click **System Monitors.** 5. Double-click the **Windows Server.** 6. Click **Endpoint Monitoring.** 7. Click **User Activity Monitor.** 8. Click the checkbox next to **Monitor Logon Activity.** 9. Click the checkbox next to **Monitor Network Session Activity.** 10. Click the checkbox next to **Monitor Process Activity.** 11. Click **OK.** 12. Click **Network Connection Monitor.** 13. Click the checkbox next to **Enable Network Connection Monitor.** 14. Click the checkbox next to **Monitor Inbound TCP Connections.** 15. Click the checkbox next to **Monitor Outbound TCP Connections.** 16. Click the checkbox next to **Monitor Listening TCP/UDP Sockets.** 17. Click the checkbox next to **Include User Activity Monitor Data (Required UAM).** 18. Click **OK.** <u>Create an AI engine rule</u>. 19. Click **Deployment Manager.** 20. Click **AI Engine.** 21. Click **Create a New Rule.** 22. Under **Rule Block Types,** select and drag a **rule block** to the **Rule Block Designer.** 23. Under each tab, fill out the necessary information. 24. Click **Next.** 25. Click **OK.**

	26. Create a rule for **Monitoring HTTP Traffic.** a. **AI Engine Rule Name:** NCCoE HTTP traffic from clinical workstation b. **Data Source:** Data Processor Logs c. **Primary Criteria -> Application:** HTTP, Know Host (origin)–Windows Server d. **Log Sources:** All Log Sources e. **Group By:** Host (Origin), Application 27. For the new rule, click the checkbox for **Action.** 28. Under **Actions,** select **Enable.** Test user network connectivity monitoring. 29. Power on the Windows Server, and log in. 30. Open an internet browser. 31. In the address bar, type the address of a web service by using the http protocol, as in **http://www.msn.com/.** View user network connectivity monitoring alerts. 32. On the LogRhythmXDR host, open an internet browser. 33. In the address bar, type in the address of the LogRhythm Web Console, **https://logrhythm-host:8443,** and log in. 34. Click the **Alarms** tab. 35. Check for alerts coinciding with use of the http protocol.
Expected Results	▪ Connecting to a web service using the http protocol will trigger an alarm event that is viewable in the LogRhythm Web Console.
Actual Results	Once LogRhythmXDR and NetworkXDR were configured to provide user network connection monitoring, we powered on the Windows Server in the Clinical Workstations VLAN that had been configured with a LogRhythm System Monitor Agent. After logging in, we opened a web browser and connected to http://www.msn.com/. LogRhythm detected use of the http protocol and created an alert that was visible on the LogRhythm Web Console.

6.1.11 Test Case: RPM-10

Cybersecurity Framework Category	**Data Security**
Testable Requirement(s)	**(CR-12)** data-in-transit is protected
Description	Demonstrate the ability to protect data-in-transit between the patient home and the telehealth platform.

Preconditions	▪ An Onclave environment has been deployed, including the Onclave Telehealth Gateway and Wireless Onclave Home Gateway. ▪ A Vivify Pathways Care Team Portal is deployed behind the Onclave Telehealth Gateway, on the **Telehealth Onclave** VLAN. ▪ Wireshark has been installed and configured on the Vivify Pathways Care Team Portal. ▪ A mobile device has been provided by Vivify and configured to communicate with the Vivify Pathways Care Team Portal. ▪ The mobile device is deployed behind the Wireless Onclave Home Gateway.
Procedure	<u>Verify that the Vivify Pathways Care Team Portal is operational</u>. 1. Power on the Vivify Pathways Care Team Portal. 2. Open an internet browser. 3. In the address bar, type **https://localhost.** 4. Ensure that the Vivify Pathways Care Team Portal landing page is displayed. <u>Test connectivity between the mobile device and Vivify Portal when connected to the Onclave Wireless Home Gateway</u>. 5. On the Vivify Portal system, click on the **Windows Start Button.** 6. Type **Wireshark,** and open the **Wireshark** application. 7. Start a packet capture on the **Ethernet0 network interface.** 8. Using the mobile device, begin a new patient reading. 9. Follow the instructions until the patient reading is complete. 10. On the Vivify Portal system, stop the Wireshark packet capture. 11. Check if there are packets received from the mobile device's IP address, **192.168.50.104.** 12. Check if the packets are obfuscated. 13. Open an internet browser. 14. In the address bar, type **https://localhost.** 15. Log in to the telehealth platform with your admin credentials. 16. Click on the patient for whom the readings were taken. 17. Check if the patient's readings were successfully transmitted from the mobile device to the Vivify Portal. <u>Test connectivity between the mobile device and Vivify Portal when not connected to the Wireless Onclave Home Gateway</u>. 18. On the mobile device, change the device's Wi-Fi to **VLAN 1332.** 19. On the Vivify Portal system, start a new packet capture on the **network interface** using Wireshark. 20. Using the mobile device, begin a new patient reading.

	21. Follow the instructions until the patient reading is complete. 22. On the Vivify Portal, stop the Wireshark packet capture. 23. Check that there are no packets received from the mobile device's IP address, **192.168.50.104.** 24. Open an internet browser. 25. In the address bar, type **https://localhost.** 26. Log in to the telehealth platform with your admin credentials. 27. Click on the patient for whom the readings were taken. 28. Check if the patient's readings were not successfully transmitted from the mobile device to the Vivify Portal.
Expected Results	▪ The mobile device can communicate with the Vivify Portal only when the mobile device is connected to the Wireless Onclave Home Gateway. ▪ Data transmitted from and to the mobile device is encrypted.
Actual Results	The mobile device successfully transmitted data to the Vivify Portal when connected to the Wireless Onclave Home Gateway. The Wireshark packet analysis tool was used to capture network traffic. Captured traffic was observed to be encrypted. When the mobile device was not connected to the Wireless Onclave Home Gateway, data was not transmitted to the Vivify Portal.

1118

1119 ### 6.1.12 Test Case: RPM-11

Cybersecurity Framework Category	N/A
Testable Requirement(s)	**(CR-13)** business workflow
Description	Demonstrate that the telehealth platform provider can receive a patient's biomedical data from the patient home and present this data to the HDO.
Preconditions	▪ Implement an RPM architecture and verify that network connections among the Patient Home, Telehealth Platform Provider, and HDO are functioning. ▪ Place RPM peripherals in the Patient Home environment. ▪ Connect the provided RPM interface to the Patient Home network. ▪ Create accounts for the HDO's clinicians on the Telehealth Platform Provider's platform. ▪ Ensure clinicians are associated with their patients on the third-party platform.
Procedure	Accuhealth–gather biomedical readings from devices with a cellular connection.

	1. Interface with the weight scale provided by Accuhealth, and record the measurement. 2. Interface with the blood glucose monitor provided by Accuhealth, and record the measurement. 3. Interface with the blood pressure monitor provided by Accuhealth, and record the measurement. <u>Accuhealth–view and verify that patient data was stored in the telehealth platform from the HDO network</u>. 4. Log in to Accuhealth's platform by using the credentials that it provided from a workstation connected to the HDO network. 5. Navigate to the patient account associated with the provided peripheral devices. 6. Verify that the biomedical readings taken in steps 1-3 are listed. <u>Vivify—gather biomedical readings from devices with a broadband connection</u>. 1. Interface with the RPM tablet provided by Vivify, and answer the presented survey questions. 2. Interface with the blood pressure monitor provided by Vivify, and verify that the tablet has the correct reading. 3. Interface with the oximeter provided by Vivify, and verify that the tablet has the correct reading. 4. Interface with the weight scale provided by Vivify, and verify that the tablet has the correct reading. 5. Interface with the blood glucose monitoring system provided by Vivify, and verify that the tablet has the correct reading. <u>Vivify–view and verify that patient data was stored in the telehealth platform from the HDO network</u>. 6. Log in to Vivify's platform by using the credentials that it provided from a workstation connected to the HDO network. 7. Navigate to the patient account associated with the provided peripheral devices. 8. Verify that the biomedical readings and survey answers provided in steps 1-5 are listed.
Expected Results	▪ The biomedical readings gathered from the provided RPM devices should be transmitted to a patient account on the appropriate telehealth platform provider platforms. ▪ Clinicians should be able to access these readings from the HDO network by logging in to the platforms and using the credentials provided to them by the third-party platform.

Actual Results	Biomedical readings were transmitted from the patient's home to the telehealth platform provider. Clinicians were also able to access and view the patient's biomedical readings from the HDO network by logging in to the third party's platform and using their provided credentials.

7 Future Build Considerations

This practice guide implemented biometric devices that used cellular data communications. This guide also addressed biometric devices using broadband communications. The practice guide implemented Onclave Networks as a proof-of-concept solution that provides layer 2 over layer 3 protection in a zero trust architecture model. This practice guide simulated a telehealth platform provider and deployed the Onclave solution to demonstrate how data communications between the patient home and telehealth platform provider may be secured. The solution assures that biometric devices are segmented from other devices that may appear in a patient home network.

A future build may also implement an EHR system that would receive automated data from the telehealth platform provider. Patient-initiated messages from RPM components deployed to the patient home were contained within the RPM systems hosted within an application to which HDOs connected for review and analysis. The future build may include direct messaging from the RPM systems to the EHR.

Appendix A List of Acronyms

AD	Active Directory
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMP	Advanced Malware Protection
CIA	Confidentiality, Integrity, and Availability
COI	Community of Interest
CTI	Cyber Threat Intelligence
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EHR	Electronic Health Record
FTD	Firepower Threat Defense
HDO	Healthcare Delivery Organization
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information System
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IIS	Internet Information Services
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
IoT	Internet of Things
LAN	Local Area Network
LTE	Long-Term Evolution

MAC	Media Access Control
NCCoE	National Cybersecurity Center of Excellence
NFC	Near Field Communication
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OS	Operating System
OSI	Open Systems Interconnection
PACS	Picture Archiving and Communication System
PAN	Personal Area Network
PRAM	Privacy Risk Assessment Methodology
RMF	Risk Management Framework
RPM	Remote Patient Monitoring
SaaS	Software as Service
SC	Security Categorization
SD	Secure Digital
SIEM	Security Incident and Event Management
SIM	Subscriber Identity Module
SMC	Stealthwatch Management Console
SP	Special Publication
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
ZTA	Zero Trust Architecture

Appendix B References

[1] R. Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 2, NIST, Gaithersburg, Md., Feb. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[2] R. Petersen et al., *Workforce Framework for Cybersecurity (NICE Framework)*, NIST SP 800-181 Revision 1, NIST, Gaithersburg, Md., Nov. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

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

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

[5] NIST. *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management,* Version 1.0 (Privacy Framework). Jan. 16, 2020. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf.

[6] NIST. Computer Security Resource Center. Available: https://csrc.nist.gov/glossary/term/confidentiality_integrity_availability.

[7] NIST. *NIST Privacy Risk Assessment Methodology (PRAM)*. Jan. 16, 2020. Available: https://www.nist.gov/privacy-framework/nist-pram.

[8] NIST. Privacy Engineering Program: *Privacy Risk Assessment Methodology (PRAM), Catalog of Problematic Data Actions and Problems.* Available: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources.

[9] 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.

[10] Joint Task Force, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 5, NIST, Gaithersburg, Md., Sept. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[11] *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,* International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Technical Report (TR) 80001-2-2, Edition 1.0 2012-07, International Electrotechnical Commission.

[12] 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.

[13] ISO/IEC, *Information technology–Security techniques–Information security management systems–Requirements,* ISO/IEC 27001:2013, 2013.

[14] J. Cawthra et al., *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.

[15] NIST. NIST Privacy Framework*, NIST Privacy Framework and Cybersecurity Framework to NIST Special Publication 800-53, Revision 5 Crosswalk*, Dec. 2020. Available: https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-nist-special-publication-800-53.

[16] World Health Organization. Health Topics. Diabetes. Available: https://www.who.int/health-topics/diabetes#tab=tab_1.

[17] P. Lee et al., *The impact of telehealth remote patient monitoring on glycemic control in type 2 diabetes: a systematic review and meta-analysis of systematic reviews of randomised controlled trials*, U.S. National Library of Medicine, National Institutes of Health. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6019730/.

[18] U.S. National Library of Medicine. Cardiac Rehabilitation. Available: https://medlineplus.gov/cardiacrehabilitation.html#summary.

[19] U.S. National Library of Medicine. Pulmonary Rehabilitation. Available: https://medlineplus.gov/pulmonaryrehabilitation.html.

[20] 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.

[21] NIST. *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*, Dec. 2020. Available: https://csrc.nist.gov/News/2020/draft-guidance-for-defining-iot-cyber-requirements.

[22] S. Rose et al., *Zero Trust Architecture*, NIST SP 800-207, NIST, Gaithersburg, Md., Aug. 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[23] C. Johnson et al., *Guide to Cyber Threat Information Sharing*, NIST SP 800-150, NIST, Gaithersburg, Md., Oct. 2016. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf.

[24] K. Dempsey et al., *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* Information Security, NIST SP 800-137, NIST, Gaithersburg, Md., Sept. 2011. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf.

[25] J. Cichonski et al., *Guide to LTE Security*, NIST SP 800-187, NIST, Gaithersburg, Md., Dec. 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf.

[26] 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., Aug. 2019. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf.

[27] E. Barker, *Recommendation for Key Management: Part 1–General*, NIST SP 800-57 Part 1 Revision 5, NIST, Gaithersburg, Md., May 2020. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

[28] 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.

[29] U.S. Department of Commerce, *Standards for Security Categorization of Federal Information and Information Systems*, NIST Federal Information Processing Standards Publication 199, Feb. 2004. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[30] K. Stine et al., *Guide for Mapping Types of Information and Information Systems to Security Categories Volume I*, NIST SP 800-60 Volume I Revision 1, NIST, Gaithersburg, Md., Aug. 2008. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.

[31] K. Stine et al., *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories Volume II,* NIST SP 800-60 Volume II Revision 1, NIST, Gaithersburg, Md., Aug. 2008. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf.

[32] U.S. Department of Commerce, *Minimum Security Requirements for Federal Information and Information Systems*, NIST Federal Information Processing Standards Publication 200, Mar. 2006. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

[33] S. Quinn et al., *National Checklist Program for IT Products–Guidelines for Checklist Users and Developers*, NIST SP 800-70 Revision 4, NIST, Gaithersburg, Md., Feb. 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf.

[34] Joint Task Force Transformation Initiative, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, NIST SP 800-53A Revision 4, NIST, Gaithersburg, Md., Dec. 2014. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

[35] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37 Revision 2, NIST, Gaithersburg, Md., Dec. 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[36] S. Brooks et al., *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, NIST Internal Report 8062, NIST, Gaithersburg, Md., Jan. 2017. Available: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf.

[37] J. Padgette et al., *Guide to Bluetooth Security,* NIST SP 800-121 Revision 2, NIST, Gaithersburg, Md., May 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf.

[38] NIST Cybersecurity for IoT Program, Feb. 2021. Available: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.

[39] International Organization for Standardization/International Electrotechnical Commission, *Information technology–Open Systems Interconnection–Basic Reference Model: The Basic Model*, ISO/IEC 7498-1, 1994.

Appendix C Threats and Risks

Organizations need to understand risks associated with systems they deploy. The National Institute of Standards and Technology (NIST) provides two bodies of work that enable organizations to examine risk and determine how risks may be mitigated. The National Cybersecurity Center of Excellence (NCCoE) uses the NIST Cybersecurity Framework as guidance for managing risks in healthcare technology. Dovetailing with the Cybersecurity Framework is the NIST Risk Management Framework (RMF). This appendix discusses how the Cybersecurity Framework and the RMF may be applied when managing risks for the remote patient monitoring (RPM) environment.

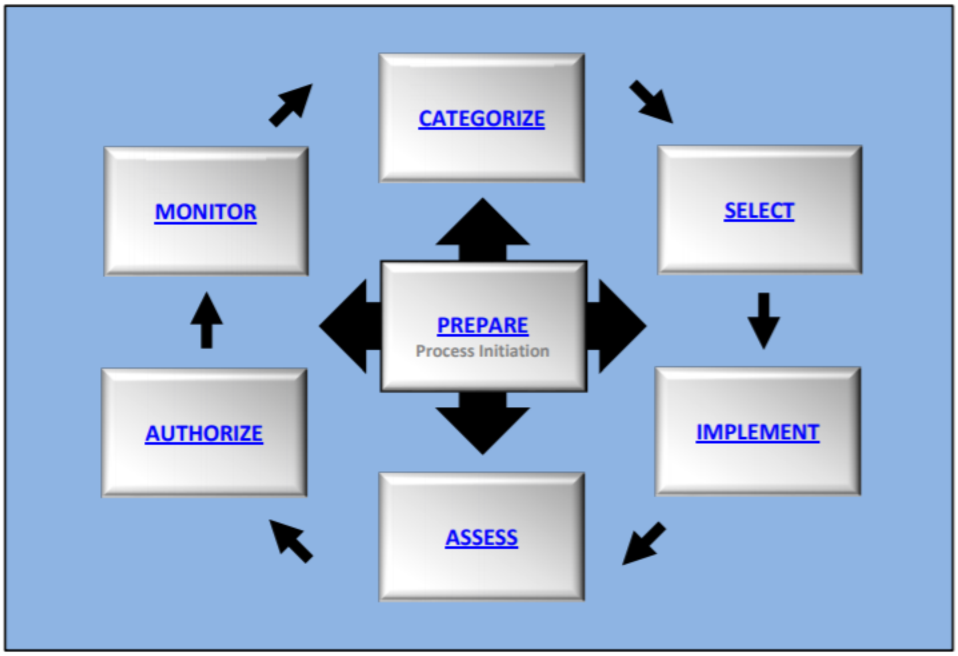
C-1 Discussion on the Risk Management Framework

This practice guide implements concepts in the NIST RMF [4]. The NIST RMF consists of a series of documents that may be applied in categorizing systems, selecting controls, assessing controls, and monitoring the security state of the overall architecture. The RMF captures this concept by describing a six-step process.

The RMF security life cycle can be described as follows:

Step	Description	Guidance Document(s)
1	categorize	Federal Information Processing Standards (FIPS) 199 [29]; NIST Special Publication (SP) 800-60 [30], [31]
2	select	FIPS 200 [32]; NIST SP 800-53 [10]
3	implement	NIST SP 800-70 [33]
4	assess	NIST SP 800-53A [34]
5	authorize	NIST SP 800-37 [35]
6	monitor	NIST SP 800-37 [35]; NIST SP 800-53A [34]

Figure C-1 Risk Management Framework [35]



Note that this practice guide does not apply the RMF sequentially as described. The NIST RMF, in this stepped approach, applies to new systems as they are evaluated for their suitability to transition from development to production environments. For this RPM practice guide, components are already developed. The approach that the project team uses in applying the RMF is first categorizing the system, then assessing risk and understanding threats that may result in risk. The team then selects controls to disrupt threats.

C-2 Information and Information System Categorization

An initial step in performing a system risk assessment and then selecting and applying appropriate controls is to perform an information and information system categorization exercise. A method to categorize is described in NIST SP 800-60 Volumes I and II [30], [31], as well as in FIPS 199 [29]. These documents are a foundational step in the NIST Risk Management Framework. The NIST SP 800-60 volumes provide guidance on identifying information categories and provide recommended categorization, based on confidentiality (C), integrity (I), and availability (A) security objectives.

In reviewing information types described in NIST SP 800-60 Volume II [31], the engineers selected two information types as relevant for the representative build: C.2.8.9, personal identity and authentication; and D.14.1, access to care. The two information types were recorded in Table C-1, Information Types and Categorizations, and provisional impact levels were captured, with the category levels corresponding to the recommended value found in NIST SP 800-60 Volume II [31].

Table C-1 Information Types and Categorizations

Information Type	NIST SP 800-60 Volume II Reference (e.g., C.2.8.9)	Confidentiality	Integrity	Availability	Justification (to change an impact level)
personal identity and authentication	C.2.8.9	moderate	moderate	moderate	N/A
access to care	D.14.1	low	moderate	low	N/A
Overall Rating		moderate	moderate	moderate	N/A

After identifying the information categories, one may determine the security objectives. Security objectives use a scale of low, medium, and high. FIPS 199 provides guidance in applying security categorization (SC). This practice guide identifies two information types: personal identity and authentication, as well as access to care. RPM's SC may be expressed as {(**confidentiality,** MODERATE), (**integrity,** MODERATE),(**availability,** MODERATE)} [29]. The SC provides a base guide for security controls selection.

C-3 Risk Context

This practice guide describes risk from a systemic perspective while contextualizing risk. The RPM system for this practice guide consists of three domains. For this document, a domain is a group of assets whose maintenance and underlying infrastructure are the responsibility of discrete entities. In RPM, this practice guide implements a reference architecture that uses the patient home, the telehealth platform provider, and the healthcare delivery organization (HDO) as domains.

Because each domain is managed and used by different entities, risks and threats may manifest differently in each domain. While HDOs and telehealth platform providers are corporate entities that are subject to regulatory obligations, the patient home tends to be managed by individuals. For RPM, HDOs and telehealth platform providers should provide guidance to patients in safeguarding their systems and information. Controls may be implemented on provisioned devices managed by HDOs or telehealth platform providers; however, other controls may need to be addressed through education and awareness.

Despite how controls may be implemented, this practice guide examines the contextualized risks and threats and describes how the NCCoE implemented mitigating controls. Organizations that implement RPM practices should ensure that they apply due diligence by examining their own risk scenarios, including legal and regulatory obligations that may apply to their locale. Risks and threats should be analyzed based on their context. This practice guide applies contextualized controls to disrupt threats as its strategy to mitigate risk.

C-4 Threats

In this practice guide, the NCCoE identified a threat taxonomy for the entire system. Threats may manifest differently to the system depending on the domain in which they appear. Environments that may have resources to maintain security tools and procedures may have mitigating circumstances that reduce the likelihood of attack and minimize impact based on pervasive controls. This practice guide considers scenarios where patient homes may have less resource and capability to minimize threats when compared with telehealth platform providers and HDOs. Also, for the purposes of this practice guide, some threats may target HDOs to a greater extent than patient homes or telehealth platform providers, given a more target-rich data set that may attract threat actors.

The following tables describe events and consider the likelihood of variation based on this context. Note that the assigned values are notional. Practitioners who perform similar exercises may determine different assignments. For purposes of this exercise, likelihood is categorized using a range that extends from very low to very high, consistent with a model described in Appendix G of NIST 800-30 [9]. An abstract of the table appears below. The qualitative values from the Table C-2 describes threat likelihood.

Table C-2 Assessment Scale: Likelihood of Threat Event Initiation

Qualitative Values	Frequency (derived from nonadversarial table)	Description (derived from adversarial table)
very high	Error, accident, or act of nature **is almost certain** to occur or occurs **more than 100 times per year.**	Adversary is **almost certain** to initiate the threat event.
high	Error, accident, or act of nature **is highly likely** to occur or occurs **10-100 times per year.**	Adversary is **highly likely** to initiate the threat event.
moderate	Error, accident, or act of nature **is somewhat likely** to occur or occurs **1-10 times per year.**	Adversary is **somewhat likely** to initiate the threat event.
low	Error, accident, or act of nature **is unlikely** to occur or occurs **less than once a year** but **more than every ten years.**	Adversary is **unlikely** to initiate the threat event.
very low	Error, accident, or act of nature **is highly unlikely** to occur or occurs **less than once every ten years.**	Adversary is **highly unlikely** to initiate the threat event.

The patient home may include technology and network infrastructure that offer malicious actors the opportunity to introduce disruption. Patients and individuals in the patient home come from different walks of life and may have varying degrees of experience in ensuring that privacy and cybersecurity are appropriately implemented for the devices that they may use. Malicious actors may opportunistically leverage a lack of robust controls in the patient home. While the patient home environment may have limited data to exfiltrate and data that pertains to a few individuals, the ability to compromise a patient home environment may pose fewer challenges than better resourced companies and hospital systems.

Table C-3 Threats Applied to the Patient Home

C, I, A	Threat Event	Description	Likelihood
C	phishing	Patients and individuals in the patient home may be susceptible to phishing attempts.	high

C, I, A	Threat Event	Description	Likelihood
I, A	malicious software	Patients and individuals in the patient home may be susceptible to permitting or introducing malicious software into the patient home environment.	moderate
I, A	command and control	Patients and individuals in the patient home may be susceptible to enabling malware that gives threat actors the ability to exercise command and control on devices.	moderate
A	ransomware	Ransomware may be introduced into the patient home environment either as links or attachments found in phishing emails or may be introduced through local media.	moderate
C	credential escalation	Malware may be introduced to the patient home environment that allows threat actors to execute arbitrary code and perform privileged functions.	low
I, A	operating system (OS) or application disruption	Malware may be introduced into the patient home environment that disrupts the operating system or applications. Libraries or subsystems may be affected.	moderate
C	data exfiltration	Sensitive data may be exposed to unauthorized individuals, e.g., via social engineering disclosure or malware that allows threat actors to retrieve data arbitrarily. Malware may be used for this purpose.	moderate

Using the same threat matrix, an examination is made of the telehealth platform provider. In general, the threat table considers when threat actors target workforce members who may have privileged access. The assumption is that telehealth platform providers may implement pervasive controls and have privacy and cybersecurity resources deployed that mitigate likelihood. The caveat in these assumptions is that HDOs that engage with telehealth platform providers should be provided assurance that third parties that they engage deploy mature privacy and cybersecurity programs.

1346 **Table C-4 Threats Applied to the Telehealth Platform Provider**

C, I, A	Threat Event	Description	Likelihood
C	phishing	Telehealth platform provider workforce with privileged access may be susceptible to spear phishing attacks.	high
I, A	malicious software	Telehealth platform provider workforce with privileged access to permitting allows malicious software to be introduced into the telehealth platform environment.	moderate
I, A	command and control	Telehealth platform provider workforce with privileged access to permitting allows threat actors to execute arbitrary code and perform privileged functions.	low
A	ransomware	Ransomware may be introduced into the telehealth platform provider environment either as links or attachments found in phishing emails or may be introduced through local media.	moderate
C	credential escalation	Malware may be introduced to the telehealth platform provider environment that allows threat actors to execute arbitrary code and perform privileged functions.	moderate
I, A	OS or application disruption	Malware may be introduced into the telehealth platform provider environment that disrupts the operating system or applications. Libraries or subsystems may be affected.	low
C	data exfiltration	Sensitive data may be exposed to unauthorized individuals, e.g., via social engineering disclosure or malware that allows threat actors to retrieve data arbitrarily.	moderate

1347 The table below represents a notional HDO model. As with the telehealth platform provider above,
1348 many assumptions have been made about implementing pervasive controls.

1349 **Table C-5 Threats Applied to the HDO**

C, I, A	Threat Event	Description	Likelihood
C	phishing	HDO workforce with privileged access may be susceptible to spear phishing attacks.	high
I, A	malicious software	HDO workforce with privileged access to permitting allows malicious software to be introduced into the HDO environment.	moderate
I, A	command and control	HDO workforce with privileged access to permitting allows threat actors to execute arbitrary code and perform privileged functions.	moderate
A	ransomware	Ransomware may be introduced into the HDO environment either as links or attachments found in phishing emails or may be introduced through local media.	moderate
C	credential escalation	Malware may be introduced to the HDO environment that allows threat actors to execute arbitrary code and perform privileged functions.	moderate
I, A	OS or application disruption	Malware may be introduced into the HDO environment that disrupts the operating system or applications. Libraries or subsystems may be affected.	moderate
C	data exfiltration	Sensitive data may be exposed to unauthorized individuals, e.g., via social engineering disclosure or malware that allows threat actors to retrieve data arbitrarily.	high
A	denial of service attack	Flooding network connection with high-volume traffic to disrupt communication in patient home,	high

C, I, A	Threat Event	Description	Likelihood
		between home and telehealth platform, or between telehealth platform provider and HDO. Such type of attack could also be used to damage a device, e.g., through accelerated battery depletion.	

C-5 Threat Sources

Threat sources describe those groups or individuals that may expose weaknesses to the RPM infrastructure. Threat sources may take actions that expose or leverage vulnerabilities either through unintentional actions or by actively attacking components within the RPM infrastructure. The following table lists the threat sources identified for this risk assessment. The table is derived from one referenced in NIST Special Publication 800-30 revision 1 (page D-2) [9].

Table C-6 Taxonomy of Threat Sources

Type of Threat Source	Description	Characteristics
unintentional–patient	The patient has physical access to biometric devices, workstations, and mobile devices that may be used as part of the RPM patient home environment.	▪ able to access components in patient home domain ▪ intend to access components ▪ patient may be targeted by malicious actors.
unintentional–care provider (e.g., family member, friend, or others with relationship to the patient)	Care providers or other trusted individuals that may have physical access to biometric devices, workstations, and mobile devices that may be used as part of the RPM patient home environment	▪ able to access components in patient home domain ▪ intend to access components ▪ individuals may be targeted by malicious actors.
unintentional–other actors	Other actors may include clinical or technical staff who may be involved in deploying the RPM infrastructure in the patient's home and may have local or remote access to data or systems used as part of the overall RPM system. Other actors may interact with	▪ able to access components or data as part of the RPM system ▪ intend to access the system (e.g., through maintenance or data review) ▪ individuals may be targeted by malicious actors or may represent insider threats

Type of Threat Source	Description	Characteristics
	components at the software as a service (SaaS) provider or at the HDO location.	where actors have legitimate access; however, component use or data access is not aligned with providing patient care.
intentional—domestic—criminal	Criminal actors may be domestic and are motivated primarily by financial interest. Criminal actors may disrupt RPM deployments either directly or by affecting other devices. Threat actions may be direct or through a chain of attacks.	▪ ability to access components is not initially provisioned. Criminal actors may perform discovery to identify vulnerable components and may seek means to deploy malicious software that would allow them access and control of the components. ▪ intent often is driven by financial motivation. Criminal elements may seek to obtain information that allows them to obtain funds directly (e.g., credit or bank account numbers) or indirectly (e.g., personal information that would allow criminals to fraudulently obtain financial accounts, to commit insurance fraud, or to sell sensitive information).
intentional–nation-state	Some foreign nation-states may want to disrupt another nation's critical infrastructure. A malicious nation-state's intent may be difficult to discern as it pertains to an individual. Attacks may be sophisticated and challenging to attribute definitively to a specific attacker.	▪ ability to access components is not initially provisioned. Nation-state actors may perform discovery to identify vulnerable components, may try to obtain user or administrator credentials, or may seek to deploy malicious software that would allow them access to

Type of Threat Source	Description	Characteristics
		and control of the components. ▪ nation-states may obfuscate their identity, posing as legitimate users, other nation-states, criminals, or activists. ▪ nation-states have significant resources to implement complex or advanced attacks. ▪ nation-states may act to disrupt critical infrastructure to either do physical damage or cause sociopolitical discord. ▪ nation-state actors may seek to obtain intellectual property (e.g., designs, formularies, clinical research).
domestic or international–non-nation-state actors (e.g., hacktivists or terrorists)	Non-nation-state actors include those parties that operate as large, disparate organizations that are not necessarily tethered to a government entity. Non-nation-state actors implement attacks based on political or social motivations.	▪ ability to access components is not initially provisioned. Non-nation-state actors may perform discovery to identify vulnerable components and may seek to deploy malicious software that would allow them access to and control of the components. ▪ non-nation-state actors primarily seek to further a social or political agenda. ▪ attacks may seek to disrupt critical infrastructure to either do physical damage or cause sociopolitical discord.

C-5.1 Business Processes

Several functions are performed with the RPM system, with those functions performed in the respective scopes. Patient data are gathered and stored, and patients interact from the patient home; communications between patients and care teams are routed through the telehealth platform provider, which is cloud hosted; and clinicians receive and interact with patient data from the HDO. Table C-7 identifies these and other business processes that support the RPM functions.

Table C-7 RPM Functions and Processes

Function	Description	Components Used	Domain
interface with biometric devices	Patients may connect biometric devices to their bodies. Physical contact occurs between the device and the patient to allow the device to capture health data. Physical interface is a continuous process in that patients may make physical contact with the biometric device on a daily or more frequent basis.	biometric device	patient home
store biometric data	Biometric data are stored to physical media. Physical media are nonvolatile media types, meaning that data are recorded to the media and available for retrieval after a device has been power cycled. Physical media may consist of flash memory, secure digital (SD) cards, or hard drives associated with the biometric device or a device hosting a healthcare app or application (e.g., a	biometric device mobile device laptop desktop dedicated device gateway	patient home

Function	Description	Components Used	Domain
	mobile device, laptop, desktop, or other workstation-type device).		
connect to cloud environment	Biometric devices may connect to a local device that uses a telehealth app or application, or the devices may connect to a cloud-hosted telehealth platform provider directly. Connections originate from the patient home connected to the cloud-hosted telehealth platform.	biometric device mobile device laptop desktop dedicated device gateway cloud-hosted components	patient home telehealth platform
connect to HDO environment	The telehealth platform provider serves as a routing mechanism that connects communications between the patient home and the HDO. The telehealth platform provider handles in-transit data as well as manages the underlying technology to enable RPM.	telehealth platform provider gateway or end-point devices at the HDO	telehealth platform provider HDO
conduct video- or audioconferencing	Patients may initiate video or audio communication with the clinical care team through the telehealth app or application. Communications will route through the telehealth platform	mobile device laptop desktop cloud-hosted components HDO mobile devices HDO workstations	patient home telehealth platform provider HDO

Function	Description	Components Used	Domain
	provider and be routed to the HDO.		
remote configuration or settings updates	HDOs may periodically push configuration or other settings updates to biometric devices. The connection initiates from the HDO and connects to the biometric device located in the patient home.	HDO-hosted servers biometric devices	HDO patient home
review patient biometric data	Physicians access patient biometric data and review and analyze it.	HDO workstation HDO mobile device	HDO
add biometric data to clinical notes	Biometric data may not ingest directly to an electronic health record (EHR) system. A physician may need to manually enter information based on the biometric data to the EHR.	HDO workstation EHR	HDO

C-6 Vulnerabilities

Below is a customized application on identifying vulnerabilities that aggregates vulnerabilities identified in NIST SP 800-30 Revision 1 [9]. 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, readers should reference NIST SP 800-30 Revision 1 [9].

1373 **Table C-8 Vulnerability Taxonomy**

Vulnerability Description	Vulnerability Severity	Predisposing Condition	Pervasiveness of Predisposing Condition
out-of-date software	high	Systems may not have patches deployed in a timely fashion, or software may not be validated to assure that applications may operate appropriately should the underlying operating system receive new updates.	high
permissive configuration settings	high	Underlying operating systems or security components (e.g., firewall) may have configuration settings that allow actions that exceed the minimum necessary to operate the application.	high
unmanaged or improperly managed credentials	high	Applications may use service or other privileged accounts to operate, or operating systems may have privileged accounts that have expansive access to the host system(s). These access privileges may exceed the minimum necessary to operate applications.	high
unprotected data	high	Data on systems may lack restrictions that limit accessibility.	high
failing or missing integrity or	high	Data path may lack end-to-end data	high

Vulnerability Description	Vulnerability Severity	Predisposing Condition	Pervasiveness of Predisposing Condition
authenticity verification		integrity or authenticity verification.	

C-7 Threat Modeling

Thus far, this practice guide has discussed several elements that make up an attack. Threats involve threat actors that may leverage vulnerabilities found in components. Components represent end-point devices found in the overall system. Components are made up of several subcomponents. The threat-modeling exercise described below identifies adverse actions that may expose vulnerabilities at the subcomponent level.

This practice guide considers that threats may include multiple actions taken that ultimately result in risk. These multiple actions are described herein as adverse actions. A threat may involve one or more adverse actions leveraging vulnerabilities at the subcomponent level that then result in risk.

The patient home environment is used as a representative domain by which the threat-modeling exercise is applied. Practitioners may wish to perform a similar, granular level of analysis for other domains in their deployment.

For the RPM solution, components are identified in three distinct domains: the patient home, the telehealth platform provider, and the HDO. This section describes a means by which threats may occur contextually. Adverse actions that align with threats may target specific subcomponents, with different risk outcomes based on the domain within which the threat actor executes the attack. Practitioners should note that while this practice guide does not apply any particular threat-modeling methodology, several are available that provide guidance for performing similar exercises for an organization's environment.

C-7.1 Modeling Threats to the Patient Home

The patient home domain poses several challenges when considering threats. For example, patients or care providers may not have the resources or technology background to address these threats independently. Telehealth platform providers and HDOs may not have the ability to manage the patient home environment entirely. Patients may have devices that are unrelated to RPM operating in their home environment. Other individuals within the patient home may have physical access to RPM devices.

Components that may be present in the RPM system's environment are outlined in Table C-9.

1400 **Table C-9 Components in the Patient Home Environment**

Component	Description	Communicates with	Provisioned by
biometric device	A sensor device that interfaces with the patient and captures biometric data that is conveyed to the clinician	patient (direct, tactile interface) interface device wireless personal area network (PAN) (Bluetooth, Wi-Fi) telehealth platform provider (Wi-Fi)	telehealth platform HDO
interface device	A device that potentially retrieves data from biometric devices and is used as a communications device by which patient-clinician communications may occur. The device may be a mobile device such as a tablet or a connected phone running a dedicated application, may be a full-feature device such as a laptop or desktop workstation, or may be a purpose-designed device.	biometric device (e.g., near-field communication[NFC], Bluetooth, Wi-Fi) telehealth platform provider	telehealth platform provider HDO
Wi-Fi access point	A device that provides the RPM environment a wireless means to communicate with devices by using internet protocols	biometric device interface device unrelated equipment	telehealth platform provider HDO patient

Component	Description	Communicates with	Provisioned by
internet router	A device that allows computing devices in the home to communicate via the internet over broadband infrastructure (e.g., cable, fiber-optic, telephone)	biometric device interface device unrelated equipment	patient
personally owned device	A device that is not part of the RPM solution; however, it may have communications capabilities to components. These devices may include patient-owned devices such as personal computers, mobile devices, or connected home devices	biometric device interface device internet router Wi-Fi access point	patient
unknown device	A device belonging to individuals other than the patient. This may include guests or unknown individuals.	unknown biometric device interface device internet router Wi-Fi access point	unknown individuals

The RPM solution deployed in the patient home is not a closed system. Elements that may be provisioned by the patient include Wi-Fi or cellular access points and the internet router. Further, the patient may have other devices on the home network. These may include connected home devices, personal computers, mobile devices, and gaming and entertainment systems.

The biometric device may consist of several subcomponents. Biometric devices may have PAN interfaces that support short-distance communication (e.g., Bluetooth). Biometric devices may also support Wi-Fi connectivity. A biometric device has a tactile interface that makes physical contact with an individual. There may be a display that acts as a user interface, and there may be storage media embedded in the device. There may be onboard storage. Physical external interfaces are ports for data communication (e.g., Universal Serial Bus [USB]), acceptance of removable media (e.g., SD card), and power.

Threats may be introduced based on the proximity of the subcomponent, as described in Table C-10. Threats that involve physical interaction with the subcomponent may be regarded as "local." Threats that originate from an external network may be regarded as "remote." Threats that use communications that are contained within the local environment may be described as "near remote."

Table C-10 Biometric Device Subcomponent Breakdown

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
tactile interface	An individual other than the patient attaches the biometric device and introduces nonpatient data.	local	I	biometric data would be false; does not pertain to the patient.	high
display	An individual other than the patient may be able to navigate the user interface and view patient biometric data.	local	C	unauthorized individuals may have access to biometric data.	high
display	The display may be damaged so that navigation is not possible.	local	A	biometric device usage degraded	high
onboard storage	Storage media that maintains biometric device system files may be damaged or made unavailable.	local	A	biometric device rendered inoperative	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
data communication port	An individual may access the biometric device and expose a subsystem (e.g., operating system).	local	I, A	exposing a subsystem such as an OS may enable a malicious actor to escalate privileges and modify, install, or execute arbitrary code.	low
personal area network	An individual may retrieve communications between the biometric device and the interface device.	near remote	C	unauthorized individuals may have access to biometric data.	low
removable media	An individual may be able to leverage removable media and extract data from the biometric device.	local	C	unauthorized individuals may have access to biometric data.	moderate
removable media	An individual may be able to introduce removable media to convey malicious software.	local	I, A	unauthorized individuals may introduce unauthorized or malicious software to the biometric device and alter functionality or render the device inoperative.	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
cellular communications	Cellular communications may be damaged.	local; remote	A	cellular communications may be inoperative.	low
cellular communications	Cellular communications may become compromised.	local; remote	A	cellular data may be exposed to unauthorized individuals.	low
Wi-Fi communications	Wi-Fi communications may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Wi-Fi communications	Wi-Fi communications may be compromised.	local; remote	C	data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate

The interface device may be a connected phone, tablet, laptop, or desktop device. Depending on the device type and manufacturer, subcomponents may vary. The first threat model profile offered below assumes that the interface device is a connected phone or tablet. Connected phones and tablets are assumed to have similar characteristics for the purposes of developing the threat model considered in this practice guide.

1416 **Table C-11 Interface Device Subcomponent Breakdown**

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
display	Display may become damaged.	local	A	device may be inoperable or unusable.	high
display	An unauthorized individual who has access to the display may be able to obtain biometric	local	A	biometric data lost	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
	data (e.g., fingerprint).				
data access port	An individual may access the mobile device and expose a subsystem (e.g., operating system).	local	I, A	unauthorized code may be introduced that compromises the device integrity or renders the device inoperable for intended purposes.	low
operating system	The operating system may be susceptible to known vulnerability exposure.	local; remote	C, I, A	vulnerability exposure may allow unauthorized removal of data, allow introduction of unauthorized code that could compromise the device operational integrity, or render the device inoperable.	moderate
RPM app	The RPM app may not be patched to current versions and may allow known vulnerability exposure.	local; remote	C, I, A	apps on the device may include flaws or vulnerabilities that result in unauthorized data exposure or compromise to an app or to device	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
				operational integrity or that render the app or device inoperable.	
other apps	Apps may be installed on the device that include unauthorized code.	local; remote	C	unauthorized actors may exfiltrate data from the device.	moderate
other apps	Apps may be installed on the device that include unauthorized code.	local; remote	I, A	unauthorized actors may disrupt the device's functionality.	moderate
onboard storage media	Onboard storage media may become damaged.	local	A	device may become inoperative or unable to obtain or transmit biometric data.	low
removable media	A device that allows removable media may enable a means by which files may be moved or copied.	local	C	data may be exfiltrated.	low
removable media	A device that allows removable media may allow code installation.	local	C, I, A	unauthorized software is introduced on the device.	low
camera	The camera may become damaged, rendering videoconferencing inoperative.	local		images and videos may not be obtained.	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
camera	Malicious actors may be able to compromise subsystems and allow unauthorized control of camera functions.	remote	C	sensitive video data may be exposed.	moderate
audio microphone	Audio microphone may become damaged.	local	C	audio communication may not function appropriately.	low
cellular communications	Cellular communications may be damaged.	local	A	cellular communications may be inoperative.	low
cellular communications	Cellular communications may become compromised.	local; remote	C	cellular data may be exposed to unauthorized individuals.	low
Wi-Fi communications	Wi-Fi communications may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Wi-Fi communications	Wi-Fi communications may be compromised.	local; remote	C	data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate

1417 **Table C-12 Laptop Subcomponent Breakdown**

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
data access port	An individual may access the mobile device and expose	local	I, A	unauthorized code may be introduced that	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
	a subsystem (e.g., operating system).			compromises the device integrity or renders the device inoperable for intended purposes.	
display	An unauthorized individual who has access to the display may be able to obtain biometric data (e.g., fingerprint).	local	A	biometric data lost	low
operating system	The operating system may not be patched to current versions and may allow known vulnerability exposure.	local; remote	C, I, A	vulnerability exposure may allow unauthorized removal of data, allow introduction of unauthorized code that could compromise the device operational integrity, or render the device inoperable.	moderate
RPM application	The RPM application may not be patched to current versions and may allow known vulnerability exposure.	local; remote	C, I, A	applications on the device may include flaws or vulnerabilities that result in unauthorized data exposure, compromise the	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
				app or device operational integrity, or render the application or device inoperable.	
other applications	Applications may be installed on the device that include unauthorized code.	local; remote	C	unauthorized actors may exfiltrate data from the device.	moderate
other applications	Applications may be installed on the device that include unauthorized code.	local; remote	C	unauthorized actors may exfiltrate data from the device.	moderate
onboard storage media	Onboard storage media may become damaged.	local	A	device may become inoperative or unable to obtain or transmit biometric data.	low
removable media	A device that allows removable media may allow code installation.	local		unauthorized software is introduced on the device.	low
camera	The camera may become damaged, rendering videoconferencing inoperative.	local		images and videos may not be obtained.	moderate
camera	Unauthorized actors may be able to compromise	remote	C	sensitive video data may be exposed.	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
	subsystems and allow unauthorized control of camera functions.				
audio microphone	Audio microphone may become damaged.	local	A	audio communication may not function appropriately.	low
Wi-Fi communications	Wi-Fi communications may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Wi-Fi communications	Wi-Fi communications may be compromised.	local; remote	C	data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate

1418 **Table C-13 Desktop Subcomponent Breakdown**

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
data access port	An unintended device may obtain communications channels by using data access ports (e.g., USB).	local	I, A	unauthorized code may be conveyed via the data access port and expose or corrupt subsystem libraries (e.g., operating system).	low
display port	The display port may become	local	A	information may not be displayed; interaction with	low

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
	physically damaged.			the system may be prevented.	
operating system	The operating system may not be patched to current versions.	local; remote	C, I, A	vulnerabilities may persist.	moderate
RPM application	The RPM application may not be patched.	local; remote	C, I, A	vulnerabilities may persist.	moderate
other applications	Applications may be installed on the device that include malicious code.	local; remote	C	unauthorized actors may exfiltrate data from the device.	moderate
other applications	Applications may be installed on the device that include malicious code.	local; remote	C	unauthorized actors may exfiltrate data from the device.	moderate
onboard storage media	Onboard storage media may become damaged.	local	A	device may become inoperative or unable to obtain or transmit biometric data.	low
removable media	A device that allows removable media may allow code installation.	local	C	unauthorized software is introduced on the device.	low
camera	The camera may become damaged, rendering videoconferencing inoperative.	local	A	images and videos may not be obtained.	moderate
camera	Unauthorized actors may be able to	remote	C	sensitive video data may be exposed.	moderate

Subcomponent	Adverse Action	Proximity	C, I, A	Adverse Outcome	Unmitigated Likelihood
	compromise subsystems and allow unauthorized control of camera functions.				
audio microphone	Audio microphone may become damaged.	local		audio communication may not function appropriately.	low
Ethernet network port	Ethernet port may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Ethernet network port	Ethernet communications may be compromised.	local; remote	C	data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate
Wi-Fi communications	Wi-Fi communications may be damaged.	local	A	Wi-Fi communications may be inoperative.	low
Wi-Fi communications	Wi-Fi communications may be compromised.	local; remote	C	data carried over Wi-Fi may be exposed to unauthorized individuals.	moderate

C-7.2 Linking Threats to Adverse Actions

For the threat-modeling exercise, this practice guide examines concepts at a granular level. The exercise examined the concept that threats may be evaluated at the subcomponent level through introduction of adverse actions. The adverse actions that the threat-modeling exercise included in themselves do not represent the enterprise threat environment but rather events that may occur that, in combination, may be how threats are found in the three domains that the practice guide describes as composing the RPM architecture.

Table C-14 Threat Event to Adverse Action Mapping

C, I, A	Threat Event	Attack Description	Target Component	Adverse Action
C	phishing	A social engineering attack that solicits an authorized user to perform an action that is beyond intended function. Phishing typically is delivered via an email that falsely claims authenticity. A phishing email may contain payloads such as attachments or links that then run arbitrary code.	interface device mobile device laptop desktop	escalation of privilege
I, A	unauthorized software	Unauthorized software may include arbitrary code that compromises system integrity or system stability.	biometric device interface device laptop desktop	system integrity compromise: system availability degraded
I, A	command and control	Unauthorized software is introduced that allows unintended actors to initiate connections to the target device.	biometric device interface device laptop desktop	system integrity compromise: system availability degraded
A	ransomware	A form of unauthorized software that prevents legitimate access to the system and resources	interface device laptop desktop	system availability degraded
C	credential escalation	Unauthorized individuals can leverage credentials and view sensitive data.	interface device laptop desktop	information exposure
I, A	OS or application disruption	Resource requests or application of unauthorized software may compromise the	interface device laptop desktop	system integrity compromise: system availability degraded

C, I, A	Threat Event	Attack Description	Target Component	Adverse Action
		integrity or stability of the RPM application.		
C	data exfiltration	Unauthorized users may be able to remove sensitive data from the device.	biometric device interface device laptop desktop	information exposure

Appendix D Problematic Data Actions and Risks

While the project team was writing this practice guide, the National Institute of Standards and Technology (NIST) published the *NIST Privacy Framework,* Version 1.0 [5]. Privacy concerns should be addressed particularly in healthcare environments. The project team examined the *NIST Privacy Framework* and included approaches that lead toward better understanding and managing the privacy risks that may be present in remote patient monitoring (RPM) deployments.

Structurally, the *NIST Privacy Framework* is like the NIST Cybersecurity Framework. Both frameworks should be applied when evaluating enterprise programs and developing mitigation strategies. Applying the Privacy Framework does not supersede the NIST Cybersecurity Framework. Rather, the Privacy Framework provides organizations with information to understand privacy-specific risks. For more information about the NIST Privacy Framework, healthcare delivery organizations (HDOs) should review *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management,* Version 1.0 [5].

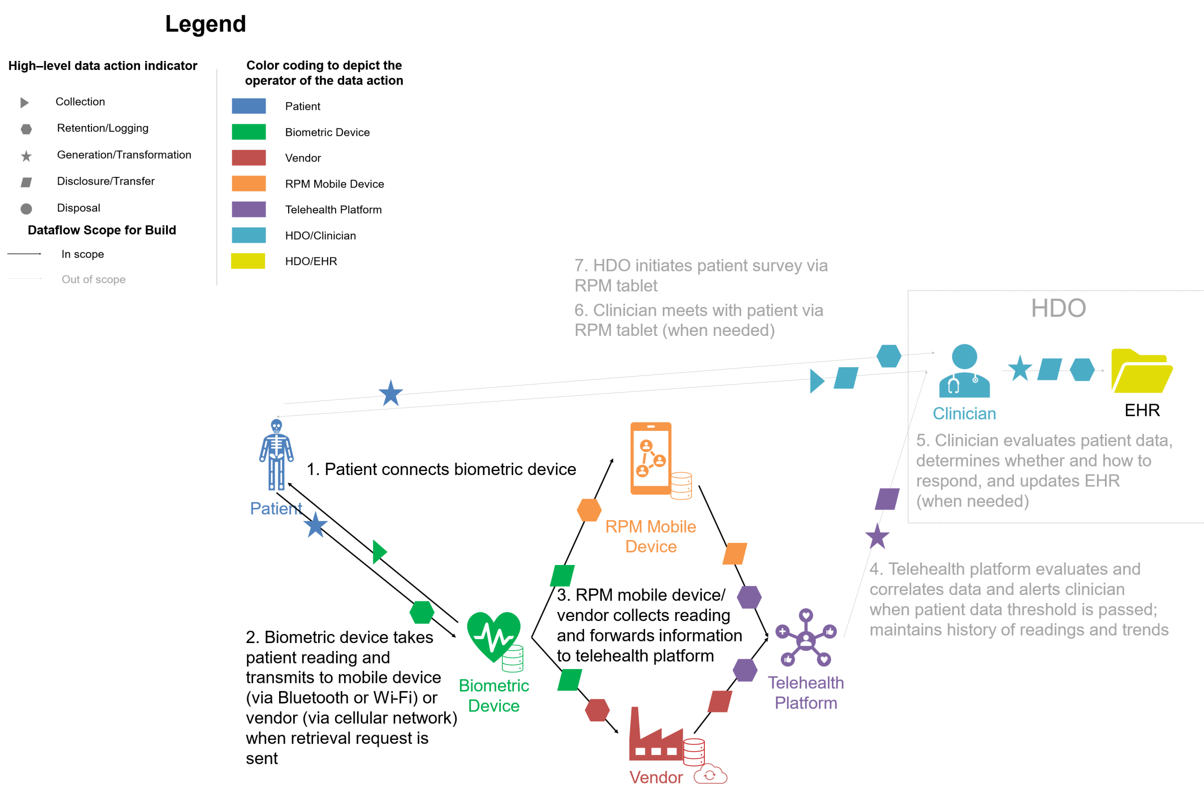
D-1 Privacy Risk Assessment Methodology

The project team applied the NIST Privacy Risk Assessment Methodology (PRAM) to conduct a privacy risk assessment for the RPM architecture. The PRAM helps an organization analyze privacy risks and facilitates communication regarding how it is managing privacy risks to achieve business/mission objectives. Processing can include collection, retention, logging, analysis, generation, transformation, merging, disclosure, transfer, and disposal of data. The PRAM also uses the privacy risk model and privacy engineering objectives described in NIST Internal Report 8062 [36] to analyze data processing for problematic data actions. A problematic data action is any data processing operation that could lead to an adverse effect, or problem, for individuals.

The occurrence or potential occurrence of problematic data actions is a privacy event. For this RPM solution, the PRAM helped elucidate how RPM solutions can present privacy concerns for individuals. The PRAM, being a risk assessment, also supports the risk assessment task in the Prepare step of the NIST Risk Management Framework as discussed in Section C-1 of this guide. The privacy events identified are discussed in Section C-2. A blank version of the PRAM is available for download on NIST's website [7]. When conducting the PRAM for this RPM solution, metadata was not assessed as it is out of scope for this project; therefore, this practice guide does not provide guidance to help an organization with securing any possible metadata if it may be leaked on devices within the telehealth ecosystem. An organization should consider the risk that could result from this incident occurring in its telehealth ecosystem.

Figure D-1 depicts the privacy view of the RPM solution dataflow and was used to conduct the privacy risk assessment.

Figure D-1 Privacy View of RPM Solution Dataflow



D-2 Problematic Data Actions and Mitigations

The *NIST Privacy Framework* refers to the concept of problematic data actions, which derives from the NIST PRAM. Problematic data actions are discovered by conducting a privacy risk assessment and analyzing the likelihood that an operation performed by a system would create a problem for individuals when processing data and the impact of the problematic data action should it occur. This section provides representative problematic data actions identified in the RPM architecture and the mitigations that an organization may use to reduce or prevent potential risk.

The discussion of problematic data actions is structured as follows:

- Privacy Risk: descriptive name for the issue that can arise in the RPM solution from data processing
- Data Action: a data life-cycle operation in the RPM solution, including collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal

- Problematic Data Action: a data action in the RPM solution that could cause an adverse effect for individuals (based on the NIST Catalog of Problematic Data Actions and Problems)
- Potential Problems for Individuals: discussion regarding the nature of the problematic data action and the specific privacy problems that can arise for patients (based on the NIST Catalog of Problematic Data Actions and Problems)
- Mitigations: examples of mitigations for the problematic data action, including those that this RPM solution addresses as well as other mitigations that organizations may wish to consider beyond the direct capabilities built into their RPM solution

D-2.1 Privacy Risk 1: Storage and movement of data creates multiple points of potential exposure after data is collected from the patient

Data Action: Patients' readings are taken from the biometric device and forwarded to the telehealth platform.

Problematic Data Action: Insecurity

Potential Problems for Individuals:
Data shared between devices in the RPM data ecosystem may not be protected at rest or in transit. Data may include sensitive information. Unauthorized data disclosure may result in patient harm. For example, disclosure could lead to dignity loss or embarrassment or may cause patients to distrust the RPM system.

The solution relies on communication between the patient's biometric device(s) and the HDO. Biometric devices forward the information to the HDO via the telehealth platform provider. In this solution, dataflow from the biometric device either directly to the telehealth platform provider or are routed via an RPM mobile device via Bluetooth, Wi-Fi, or over the cellular network. Each device, system, and dataflow in the process introduces an exposure point, several of which would not arise in a traditional healthcare setting, such as a doctor's appointment (e.g., if the patient's reading is taken in a doctor's office). Any failure to protect data stored on the biometric and RPM mobile devices and forwarded may allow unauthorized individuals to view sensitive information. In this event, someone other than a patient-approved individual can access data that is unencrypted on the biometric device or RPM mobile device or during forwarding. The patient may experience dignity loss due to their health information being exposed and may also experience loss of trust for the HDO and RPM mobile device.

Mitigation(s):

RPM Solution Mitigation:

Physical device security is out of scope for this lab solution.

Protect data at rest and in transit between devices and telehealth platforms.

Protecting data on the biometric device, e.g., by using encryption, prior to moving it to the telehealth platform and using encrypted connections to protect the contents of data in transit reduces the risk of exposure. Robust network security controls should be in place to help protect data in transit. For example, firewalls and network access control will help secure the data against ransomware, malware, and other attacks. If data are not encrypted, unauthorized individuals may be able to retrieve the data, which can lead to inappropriate use of information. Encryption methods should be used in preventing health information disclosure.

Additional Privacy Mitigations for Organizations to Consider:

Develop and adopt enterprise encryption policies.

Policies should be created, developed, and adopted for systematically categorizing and classifying all healthcare data, including metadata, no matter where the data is stored.

D-2.2 Privacy Risk 2: Biometric device types can indicate patient health problems that individuals would prefer not to disclose beyond their healthcare provider

Data Action: Patients are provided one or more biometric devices that monitor biometric data, which helps healthcare providers assess the physical health condition of the patient between visits with the provider.

Problematic Data Action: Unanticipated Revelation

Potential Problems for Individuals: Patients with given medical conditions may use certain biometric devices. Knowledge of the biometric devices that a patient is using, alone or in combination, can indicate a particular health problem. For example, a glucometer can indicate that a patient is being monitored for diabetes. This assumption could be more obvious if that same patient is also known to be using a blood pressure monitor, weight scale, and activity tracker.

Patient sensitivities regarding their health status can vary widely. Unauthorized individuals may be able to determine a patient’s medical condition based on knowing a combination of factors. For example, knowledge of the device type and the biometric data may enable individuals to conclude the patient’s health condition. Revealing a health condition that a patient would prefer not to disclose or disclosure of a patient’s medical treatment and their course of treatment outside their healthcare provider can lead to dignity loss, such as embarrassment, emotional distress, and loss of trust in the HDO and RPM system. This could damage the relationship with a patient, including losing the opportunity for the HDO to continue providing care. Intercepting communications sessions may have a lower likelihood of occurrence than aggregated data compromise.

Mitigation(s):

RPM Solution Mitigation(s):

Protect data transmitted between parties and in storage.

Data-in-transit protection, e.g., by encrypting communications channels, reduces the risk of compromise of information transmitted between parties. Reducing the risk of compromise and any resulting exposures reduces the risk of unintentional exposure of the information. Biometric devices communicate through a mobile device that uses a Bluetooth connection, and the RPM solution assumes that these devices are deployed using an appropriate encryption mode [25], [37]. The RPM solution uses devices that are equipped to communicate over 4G long-term evolution (LTE), which uses asymmetric encryption between the device and the cellular tower. Additionally, all data at rest is protected with AES256 encryption [28].

Limit or disable access to data.

Conduct a system-specific privacy risk assessment to determine how access to data in the telehealth platform provider can be limited. Using access controls to limit staff access to biometric and patient data can be important in preventing associating health conditions with specific individuals.

D-2.3 Privacy Risk 3: Incorrect data capture of readings by devices may impact quality of patient care

Data Action: The RPM solution relies on the patient to take readings by using the patient's assigned biometric device(s) when required according to their care plan.

Problematic Data Action: Distortion

Potential Problems for Individuals: Devices may be inaccurately applied by the patient (e.g., not properly using or inadvertently changing settings), which can impact the ability of a biometric device to take proper readings. Anomalies may also be introduced by other individuals who may have physical access to the device (e.g., allowing someone other than the patient to use the device), which may introduce biometric readings other than the patient's into the system. Data integrity may be compromised, causing confusion regarding the patient's actual health and possibly leading to physical harm to the patient.

Mitigation(s):

RPM Solution Mitigation(s):

Physical device security is out of scope for this lab solution. Ultimately, responsibility for monitoring patient data, including identifying anomalies, falls on the clinician.

Additional Privacy Mitigations for Organizations to Consider:

Educate patients regarding practices for handling biometric device(s) and the importance of following their monitoring plan.

Educating patients regarding how their interactions with the biometric devices assigned to them affect the quality of the data provided to the telehealth platform provider, HDO, healthcare provider, and ultimately the quality of care they receive and their health safety will encourage them to use the biometric devices as designed and intended.

D-2.4 Privacy Risk 4: Aggregated data may expose patient information

Data Action: Patients use one or more biometric devices to monitor the condition of their health. The biometric data generated is transmitted through multiple entities, including cellular or broadband internet providers, biometric device vendors, telehealth platform providers, cloud service providers, and HDOs before reaching the healthcare provider.

Problematic Data Action: Re-identification

Potential Problems for Individuals: The RPM architecture integrates data from multiple organizations, each of which may have different data that pertains to the patient. The biometric data generated by the solution indicates an individual's health status. Aggregation of biometric data with patient identifiers associates information about the patient that, if revealed to an entity other than their healthcare provider and care team, may result in dignity losses, such as embarrassment or emotional distress, as well as loss of trust in the HDO and provider.

Mitigation(s):

RPM Solution Mitigation(s):

Combine biometric data with patient identifiers only when operationally required.

The device manufacturer may aggregate data received from patients. Biometric data do not include patient identifiers, however, will include device identifiers. The telehealth platform provider may associate the biometric data to patients by using device identifiers. In this RPM solution, the telehealth platform provider does not combine this data until the point at which it is necessary to perform patient analytics that enable the healthcare delivery organization to manage the patient's care. The telehealth platform provider uses a biometric device identifier to correlate a patient with the biometric data that a device transmits.

Protect data transmitted between parties and in storage.

Data protection, e.g., by using encryption, reduces the risk that compromised data can be easily used and combined with other data to re-identify patients. Biometric devices communicate through a mobile device that uses Bluetooth connections, and the RPM solution assumes that these devices are deployed using an appropriate encryption mode [25], [37]. The RPM solution uses devices that are equipped to communicate over 4G LTE, which uses asymmetric encryption between the device and the cellular tower. Additionally, all data at rest is protected with AES256 encryption.

D-2.5 Privacy Risk 5: Exposure of patient information through multiple providers of system components increases the likelihood of exposure of patient data to unintended recipients

Data Action: Data about individuals and their devices flows between various applications and analytical tools, some of which are managed by third parties.

Problematic Data Action: Unanticipated Revelation

Potential Problems for Individuals: Multiple organizations work together to provide individual components of the RPM solution, and each organization that plays a role in data processing represents an exposure point for patient information. Patient biometric data from devices travels to the HDO through device vendors and telehealth platform providers over cellular and broadband networks. Some of the data also flows through cloud solutions. These third parties beyond the HDO and patient's provider may conduct system monitoring, analytics, and other operational activities as part of the solution. System administrators have access to otherwise private healthcare information through knowledge of biometric device types and the data they generate, which may reveal information about patients that results in dignity losses, such as embarrassment or emotional distress.

Data transmission about patients and their biometric devices among a variety of different parties could be confusing for patients who might not know who has access to information about them. This transmission could reveal personal information about the patient to parties they would not expect to have such information. This lack of patient visibility and awareness of data-sharing practices may also cause patient loss of trust in the provider.

Additionally, the communications between RPM devices and systems generate metadata that may pose additional risk of exposure. For example, device identifiers in some contexts may indicate the type of device that is communicating, which can provide insights into a patient's condition even without viewing the data transmitted. Metadata was not evaluated as part of this solution; however, organizations planning to implement RPM solutions should include an evaluation of metadata in their risk assessment.

Mitigation(s):

RPM Solution Mitigation(s):

Combine biometric data with patient identifiers only when operationally required.

The device manufacturer may aggregate data received from patients. Biometric data do not include patient identifiers, however, will include device identifiers. The telehealth platform provider may associate the biometric data to patients by using device identifiers. In this RPM solution, the telehealth platform provider does not combine this data until the point at which it is necessary to perform patient analytics that enable the healthcare delivery organization to manage the patient's care. The telehealth platform provider uses a biometric device identifier to correlate the biometric data with a patient.

Protect data transmitted between parties and in storage.

Data protection, e.g., using encryption, reduces the risk of compromise of information transmitted between parties. Biometric devices communicate through a mobile device that uses Bluetooth connections, and the RPM solution assumes that these devices are deployed using an appropriate encryption mode. The RPM solution uses devices that are equipped to communicate over 4G LTE, which uses asymmetric encryption between the device and the cellular tower [25], [37]. Additionally, all data at rest is protected with AES256 encryption.

Limit or disable collection of specific data elements.

Conduct a system-specific privacy risk assessment to determine what elements can be limited. The RPM solution sends only biometric and device data from the device to the RPM interface and vendors and excludes identifying information about the patient. This would limit insight into patient health status by outsiders or telehealth platform provider administrators if the security of the information is compromised.

Additional Privacy Mitigations for Organizations to Consider:

Limit or disable access to data.

Conduct a system-specific privacy risk assessment to determine how access to data can be limited. Using access controls to limit staff access to compliance information, especially when associated with patients, can be important in preventing association of specific biometric data with individuals.

Use contracts to limit third-party data processing.

Establish contractual policies to limit data processing by third parties to only the processing that facilitates delivery of security services and to no data processing beyond those explicit purposes.

D-3 Additional Program Mitigations Applicable Across Various Data Actions

Organizations that deploy RPM solutions will conduct their own risk assessment and determine what mitigations are most appropriate for their environment, including organizational activities outside the direct control of their RPM solution. This section includes several examples of mitigations that may be common across the organization and is not intended to be all-encompassing.

Mitigations:

Ensure that privacy notices address end-to-end dataflows in the RPM solution between patient and provider.

RPM solutions empower patients as active participants in their healthcare. Privacy notices—information such as the data collected about the patient, the reason it is collected, how it is processed by an organization, how it is protected, and how long an organization plans to use it—are one way that HDOs can help patients understand their relationship and expectations with an organization. Privacy notices are also a precursor to requesting consent so that patients understand what agreements they are making. Effective notices that cover the RPM solution should be specific enough to help patients understand the PRM solution and should be written in clear terms that are easily understood by any individuals (i.e., individuals do not need healthcare, RPM, or privacy expertise to interpret the privacy notice). Patients may not be aware of or easily able to discern what is happening with the information generated by their biometric device(s), such as analytics and trend analyses that telehealth platform providers can conduct and how a provider may use this information for their care. Information regarding the RPM solution that includes a discussion of privacy helps patients better understand how the system processes their data, which enhances predictability. One example of providing an effective RPM privacy notice would be to create an RPM website or pamphlet, separate from the overall operational privacy notice that an HDO may have, that explains the RPM program.

Provide a support point of contact.

Providing patients with a point of contact in the organization who can respond to privacy inquiries and concerns regarding the RPM solution helps patients better understand how the system processes their data, which enhances predictability.

Define and communicate clear retention policies.

To minimize security and privacy risk to patients (e.g., deciding based on aged data that could impact the quality of care provided through an RPM solution), HDOs should use the results of their risk assessment to determine how each solution component impacts their retention policies for each step in the dataflow process. When an HDO relies on other entities to support data processing activities, the HDO should clearly communicate its data retention and privacy risk management needs to those entities.

Implement program-specific privacy and security training and awareness activities.

Privacy and security may be compromised while performing business functions if employees do not understand how to incorporate security and privacy practices into their operational activities. Each organization that plays a role in healthcare RPM solutions must evaluate its role in the data ecosystem, the privacy and security risks that arise in the context of that role, and the training and awareness activities that will be most impactful for addressing those risks.

Appendix E Benefits of IoT Device Cybersecurity Requirements

The National Institute of Standards and Technology's (NIST's) Cybersecurity for the Internet of Things (IoT) program [38] supports development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

Computing devices that integrate physical and/or sensing capabilities and network interface capabilities are being designed, developed, and deployed at an ever-increasing pace. These devices are fulfilling customer needs in all sectors of the economy. Many of these computing devices are connected to the internet. IoT devices combine network connectivity with the ability to sense or affect the physical world. Individuals may find challenges with applying privacy and cybersecurity controls as devices include greater functionality.

NIST's Cybersecurity for IoT program has defined a baseline set of device cybersecurity capabilities that manufacturers should consider integrating into their IoT devices and that consumers should consider enabling/configuring in those devices. **Device cybersecurity capabilities** are cybersecurity features or functions that IoT devices provide through their own technical means (i.e., device hardware and software). **Nontechnical supporting capabilities** are actions that a manufacturer or third-party organization performs in support of the cybersecurity of an IoT device. Examples of nontechnical support include providing information about software updates, instructions for configuration settings, and supply chain information.

Used together, **device cybersecurity capabilities** and **nontechnical supporting capabilities** can help mitigate cybersecurity risks related to the use of IoT devices while assisting customers in achieving their goals. Device cybersecurity capabilities and nontechnical supporting capabilities—if properly defined and integrated into the RPM devices and RPM architectural environment—can assist in securely deploying and configuring an RPM ecosystem.

E-1 Device Capabilities Mapping

Table E-1 below builds on the Security Control Map in Section 3.5 of this document. The table lists both device cybersecurity capabilities and nontechnical supporting capabilities that map to NIST Cybersecurity Framework Subcategories that were considered relevant to RPM ecosystem risks. Selecting devices and/or third parties that provide these capabilities can support the secure deployment and configuration of the RPM ecosystem. The column listing mapping from Cybersecurity Framework Subcategories to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule is included as an important sector-specific standard.

Note: In the table below, the HIPAA Security Rule elements listed in the last column were previously mapped to the Cybersecurity Framework Subcategories. The device cybersecurity capabilities and nontechnical supporting capabilities listed were mapped to the Cybersecurity Framework Subcategories, not to the HIPAA Security Rule elements. In this sense, the Cybersecurity Framework Subcategories served as the central element joining the device cybersecurity capabilities and nontechnical supporting capabilities with the HIPAA Security Rule elements.

Table E-1 Mapping of Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities to NIST Cybersecurity Framework Subcategories of the RPM Project

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
ID.AM-1: Physical devices and systems within the organization are inventoried.	▪ Ability to detect unauthorized hardware and software components.	▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing IoT device customers with the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing IoT device customers with the details necessary to require unique identifiers for each IoT device associated with the system and critical system components within which it is used.	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)
ID.AM-2: Software platforms and applications within the organization are inventoried.	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to detect unauthorized hardware and software components.	N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(7)(ii)(E)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
ID.AM-4: External information systems are catalogued.	N/A	▪ Providing documentation detailing all the cloud services used to support the IoT device. ▪ Providing a detailed description of all logical interfaces to the IoT device and documenting the interfaces used by the manufacturer's third parties, and the purposes for such uses.	45 C.F.R. §§ 164.308(a)(4)(ii)(A) 164.308(b) 164.314(a)(1) 164.314(a)(2)(i)(B) 164.314(a)(2)(ii) 164.316(b)(2)
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	N/A	N/A	45 C.F.R. §§ 164.308(a)(7)(ii)(E)
ID.RA-1: Asset vulnerabilities are identified and documented.	N/A	▪ Providing details for performing the tests necessary for IoT device and related system software updates, for	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(4)(ii)(A) 164.308(a)(7)(ii)(E)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		effectiveness and to identify potential side effects, before installation. ▪ Providing communications describing the types of security and privacy tests necessary for the IoT device and software before installation. ▪ Providing training and awareness information to IoT device customers that describe newly identified vulnerabilities and threats (such as zero-day malware) for the associated IoT device.	164.308(b) 164.310(d) 164.310(d)(2)(iii)
ID.RA-4: Potential business impacts and likelihoods are identified.	N/A	▪ Providing the details necessary for the installation of IoT devices and associated systems security-relevant software updates within an organizationally defined time period from the vendor release of the updates. ▪ Providing education describing the operational impacts of the anti-malware activities on mission critical processes in the system where the IoT device is used.	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	N/A	▪ Providing education explaining the responsibilities of IoT device customers to perform their own risk assessments, using information provided by the manufacturer, to determine the risks the IoT device will bring into the IoT device customer's systems.	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)
ID.RA-6: Risk responses are identified and prioritized.	▪ Ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state.	▪ Providing the details necessary for the installation of IoT devices and associated systems security-relevant software updates within an organizationally defined time period from the vendor release of the updates.	45 C.F.R. §§ 164.308(a)(1)(ii)(B) 164.314(a)(2)(i)(C) 164.314(b)(2)(iv)
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.	▪ Ability to uniquely identify the IoT device logically. ▪ Ability to uniquely identify a remote IoT device. ▪ Ability for the device to support a unique device ID (e.g., to allow it to be linked to the person or process assigned to use the IoT device). ▪ Ability to configure IoT device access control policies using IoT device identity.	▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to verify the identity of an IoT device. ▪ Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access. ▪ Ability for the IoT device to hide or mask authentication information during authentication process. ▪ Ability to set and change authentication configurations, policies and limitations settings for the IoT device. ▪ Ability to revoke access to the device. ▪ Ability to create unique IoT device user accounts. ▪ Ability to identify unique IoT device user accounts. ▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions. ▪ Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface. ▪ Ability to enable automation and reporting of account management activities.	capabilities, or through supporting systems and/or tools. ▪ Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing the details necessary to require unique identifiers for each IoT device associated with the system and critical system components within which it is used. ▪ Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources. ▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	◦ Ability to assign access to IoT device audit controls to specific roles or organizationally defined personnel. ◦ Ability to control access to IoT device audit data. ◦ Ability to identify the user, process or device requesting access to the audit/accountability information (i.e., to ensure only authorized users and/or devices have access). ▪ Ability to establish conditions for shared/group accounts on the IoT device. ▪ Ability to administer conditions for shared/group accounts on the IoT device. ▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions.	▪ Providing education explaining how to enforce authorized access at the system level.	
PR.AC-2: Physical access to assets is managed and protected.	N/A	▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device based upon the	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		determined risk level that the device brings to the IoT customer's system. ▪ Providing descriptions of the physical access security procedures the manufacturer recommends for limiting physical access to the device and to associated device controls. ▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted or is occurring.	164.310(a)(2)(i) 164.310(a)(2)(ii)
PR.AC-3: Remote access is managed.	▪ Ability to configure IoT device access control policies using IoT device identity. ○ Ability to hide IoT device identity from non-authorized entities. ○ Ability for the IoT device to differentiate between authorized and unauthorized remote users. ○ Ability for the IoT device to differentiate between authorized and unauthorized physical device users.	N/A	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to authenticate external users and systems. ▪ Ability to securely interact with authorized external, third-party systems. ▪ Ability to identify when an external system meets the required security requirements for a connection. ▪ Ability to establish secure communications with internal systems when the device is operating on external networks. ▪ Ability to establish requirements for remote access to the IoT device and/or IoT device interface, including: o usage restrictions o configuration requirements o connection requirements o manufacturer established requirement ▪ Ability to enforce the established local and remote access requirements. ▪ Ability to prevent external access to the IoT device management interface. ▪ Ability to control the IoT device's logical interface (e.g., locally or remotely).		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera). ▪ Ability to detect remote activation of sensors.		
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	▪ Ability to revoke access to the device. ▪ Ability to establish access to the IoT device to perform organizationally defined user actions without identification or authentication. ▪ Ability to assign roles to IoT device user accounts. ▪ Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary) ○ Ability to establish user accounts to support role-based logical access privileges.	▪ Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device. ▪ Providing details about the specific types of manufacturer's needs to access the IoT device interfaces; such as for specific support, updates, ongoing maintenance, and other purposes. ▪ Providing documentation with instructions for the IoT device customer to follow for how to restrict interface connections that enable specific activities.	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	◦ Ability to administer user accounts to support role-based logical access privileges. ◦ Ability to use organizationally defined roles to define each user account's access and permitted device actions. ◦ Ability to support multiple levels of user/process account functionality and roles for the IoT device. ▪ Ability to apply least privilege to user accounts (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions) ◦ Ability to create additional processes, roles (e.g., admin, emergency, temporary) and accounts as necessary to achieve least privilege. ◦ Ability to apply least privilege settings within the device (i.e., to ensure that the processes operate	▪ Providing descriptions of the types of access to the IoT device that the manufacturer will require on an ongoing or regular basis. ▪ Providing detailed instructions for how to implement management and operational controls based on the role of the IoT device user, and not on an individual basis. ▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing a detailed description of the other types of devices and systems that will access the IoT device during customer use of the device, and how they will access it. ▪ Providing communications and detailed instructions for implementing a hierarchy of privilege levels to use with	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	at privilege levels no higher than necessary to accomplish required functions). o Ability to limit access to privileged device settings that are used to establish and administer authorization requirements. o Ability for authorized users to access privileged settings. ▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions. ▪ Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface. ▪ Ability to enable automation and reporting of account management activities. o Ability to assign access to IoT device audit controls to specific roles or organizationally defined personnel. o Ability to control access to IoT device audit data.	the IoT device and/or necessary associated information systems. ▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools. ▪ Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources. ▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems. ▪ Providing education explaining how to enforce authorized access at the system level. ▪ Providing education and supporting materials explaining how to establish roles and responsibilities for IoT device data security, using the device	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	○ Ability to identify the user, process or device requesting access to the audit/accountability information (i.e., to ensure only authorized users and/or devices have access). ▪ Ability to establish conditions for shared/group accounts on the IoT device. ▪ Ability to administer conditions for shared/group accounts on the IoT device. ▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions. ▪ Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on: ○ run-time access control decisions facilitated by dynamic privilege management. ○ organizationally defined actions to access/use device ▪ Ability to allow information sharing capabilities based upon the type and/or role of user attempting to share the information.	capabilities and/or other services that communicate or interface with the device. ▪ Providing education and supporting materials describing the IoT device capabilities for role-based controls, and how to establish different roles within the IoT device. ▪ Providing education and supporting materials for how to establish roles to support IoT device policies, procedures and associated documentation.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization. ▪ Ability to establish pre-defined restrictions for information searches within the device. ▪ Ability to establish limits on authorized concurrent device sessions for: ○ user accounts ○ roles ○ groups ○ dates ○ times ○ locations ○ manufacturer-established parameters ▪ Ability to restrict updating actions to authorized entities. ▪ Ability to restrict access to the cybersecurity state indicator to authorized entities.		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to enforce the established local and remote access requirements. ▪ Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means. ▪ Ability to store and process session identifiers. ▪ Ability to identify and track sessions with identifiers. ▪ Ability to enforce access to memory space through the kernel. ▪ Ability to prevent a process from accessing memory space of another process.		
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	N/A	N/A	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)
PR.AC-6: Identities are proofed and	▪ Ability to obtain and validate certificates.	N/A	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
bound to credentials and asserted in interactions.	▪ Ability to identify unique users interacting with the device (to allow for user session monitoring).		
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).	▪ Ability to configure IoT device access control policies using IoT device identity. ○ Ability to hide IoT device identity from non-authorized entities. ○ Ability for the IoT device to differentiate between authorized and unauthorized remote users. ○ Ability for the IoT device to differentiate between authorized and unauthorized physical device users. ▪ Ability for the IoT device to identify itself as an authorized entity to other devices. ▪ Ability for the IoT device to require authentication prior to connecting to the device. ▪ Ability for the IoT device to support a second, or more, authentication	▪ Providing detailed instructions and guidance for establishing activities performed by the IoT device that do not require identification or authentication. ▪ Providing documentation describing the specific IoT platforms used with the device to support required IoT authentication control techniques. ▪ Providing documentation with details describing external authentication by IoT platforms and associated authentication methods that can be used with the IoT device.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	method(s) through an out-of-band path such as: ○ temporary passwords or other one-use log-on credentials ○ third-party credential checks ○ biometrics ○ text messages ○ hard tokens ○ manufacturer proprietary method ▪ Ability to set the time period for how long the device will remain locked after an established configurable limit of unsuccessful login attempts has been met. ▪ Ability to disable or lock access to the device after an established number of unsuccessful login attempts. ▪ Ability to display and/or report the previous date and time of the last successful login authentication. ▪ Ability to automatically disable accounts for the IoT device after an established period of inactivity. ○ Ability to support automatic logout of inactive accounts after a		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory

	configurable established time period.
	  ○ Ability to support automatic removal of temporary, emergency and other special use accounts after an established time period.
	▪ Ability to authenticate external users and systems.
	▪ Ability to display to IoT device users an organizationally defined system use notification message or banner prior to successful IoT device authentication.
	▪ Ability to create an organizationally defined system use notification message or banner to be displayed on the IoT device.
	  ○ Ability to edit an existing IoT device display.
	  ○ Ability to establish the maximum size (e.g., in characters, bytes) of the available device display.
	▪ Ability to keep the notification message or banner on the device screen until the		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	device user actively acknowledges and agrees to the usage conditions. ▪ Ability to identify authorized users and processes. ▪ Ability to differentiate between authorized and unauthorized users (physical and remote). ▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions. ▪ Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface. ▪ Ability to enable automation and reporting of account management activities. ○ Ability to assign access to IoT device audit controls to specific roles or organizationally defined personnel. ○ Ability to control access to IoT device audit data. ○ Ability to identify the user, process or device requesting access to the audit/accountability information		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	(i.e., to ensure only authorized users and/or devices have access). ▪ Ability to establish conditions for shared/group accounts on the IoT device. ▪ Ability to administer conditions for shared/group accounts on the IoT device. ▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions. ▪ Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization. ▪ Ability to establish secure communications with internal systems when the device is operating on external networks. ▪ Ability to verify and authenticate any update before installing it.		
PR.DS-1: Data-at-rest is protected.	▪ Ability to execute cryptographic mechanisms of appropriate strength and performance. ▪ Ability to obtain and validate certificates.	▪ Providing detailed instructions for how to implement management and operational controls for securely handling and retaining IoT device data,	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(b)(1) 164.310(d)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to perform authenticated encryption algorithms. ▪ Ability to change keys securely. ▪ Ability to generate key pairs. ▪ Ability to store encryption keys securely. ▪ Ability to cryptographically store passwords at rest, as well as device identity and other authentication data. ▪ Ability to support data encryption and signing to prevent data from being altered in device storage. ▪ Ability to secure data stored locally on the device. ▪ Ability to secure data stored in remote storage areas (e.g., cloud, server). ▪ Ability to utilize separate storage partitions for system and user data. ▪ Ability to protect the audit information through: ○ encryption ○ digitally signing audit files ○ securely sending audit files to another device	associated systems data, and data output from the IoT device. ▪ Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements.	164.312(a)(1) 164.312(a)(2)(iii) 164.312(a)(2)(iv)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	○ other protections created by the device manufacturer		
PR.DS-2: Data-in-transit is protected.	▪ Ability to execute cryptographic mechanisms of appropriate strength and performance. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to change keys securely. ▪ Ability to store encryption keys securely. ▪ Ability to secure data stored in remote storage areas (e.g., cloud, server). ▪ Ability to support trusted data exchange with a specified minimum-strength cryptography algorithm. ▪ Ability to support data encryption and signing to prevent data from being altered in transit. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to use cryptographic means to validate the integrity of data transmitted. ▪ Ability to protect the audit information through:	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet requirements of the IoT device customers' organizational security policies, contractual requirements, applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements.	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	○ encryption ○ digitally signing audit files ○ securely sending audit files to another device ○ other protections created by the device manufacturer		
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	N/A	N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv) 164.310(d)(1) 164.310(d)(2)
PR.DS-4: Adequate capacity to ensure availability is maintained.	▪ Ability to enforce configured disk quotas. ▪ Ability to provide sufficient resources to store and run the operating environment (e.g., operating systems, firmware, applications). ▪ Ability to utilize file compression technologies (e.g., to protect against denial of service).	N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7) 164.310(a)(2)(i) 164.310(d)(2)(iv) 164.312(a)(2)(ii)
PR.DS-5: Protections against	▪ Ability to control device responses to device input.	N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(D)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
data leaks are implemented.	▪ Ability to control output from the device.		164.308(a)(3) 164.308(a)(4) 164.310(b) 164.310(c) 164.312(a)
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	▪ Ability to identify software loaded on the IoT device based on IoT device identity. ▪ Ability to verify digital signatures. ▪ Ability to run hashing algorithms. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to compute and compare hashes. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification. ▪ Ability to use cryptographic means to validate the integrity of data transmitted. ▪ Ability to verify software updates come from valid sources by using an effective method (e.g., digital signatures, checksums, certificate validation). ▪ Ability to verify and authenticate any update before installing it.	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing communications to IoT device customers describing how to implement management and operational controls to protect IoT device data integrity and associated systems data integrity. ▪ Providing IoT device customers with the details necessary to support secure implementation of the IoT device and associated systems data integrity controls. ▪ Providing IoT device customers with documentation describing the data	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).	integrity controls built into the IoT device and how to use them. If there are no data integrity controls built into the IoT device, include documentation explaining to IoT device customers the ways to achieve IoT device data integrity. ▪ Providing details for how to review and update the IoT device and associated systems while preserving data integrity.	
PR.IP-4: Backups of information are conducted, maintained, and tested.	N/A	▪ Providing education to IoT device customers covering the instructions and details necessary for them to create accurate backups and to recover the backups when necessary. ▪ Providing education to IoT device customers that includes instructions describing how to back up data from systems where IoT device data is stored. ▪ Providing awareness reminders and tips to IoT device customers (e.g., directly in person, in videos, in an online webinar) for various aspects involved with backing up the IoT device data.	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
PR.IP-6: Data is destroyed according to policy.	▪ Ability to sanitize or purge specific or all data in the device.	▪ Providing documentation describing how to irreversibly delete data from the IoT device. ▪ Providing IoT device customers the details necessary for them to know when and how to remove all data from IoT devices prior to removing the devices from facilities for offsite maintenance or repairs. ▪ Providing information describing how to use the IoT device capabilities to remove all data from the device. ▪ Providing education that explains and/or demonstrates how to securely and irreversibly delete data from the IoT device and any associated data storage locations.	45 C.F.R. §§ 164.310(d)(2)(i) 164.310(d)(2)(ii)
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans	N/A	N/A	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
(Incident Recovery and Disaster Recovery) are in place and managed.			
PR.IP-10: Response and recovery plans are tested.	N/A	N/A	45 C.F.R. §§ 164.308(a)(7)(ii)(D)
PR.IP-12: A vulnerability management plan is developed and implemented.	N/A	▪ Providing communications and documentation detailing the manufacturer's recommended vulnerability and patch management plan.	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B)
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	N/A	▪ Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home. ▪ Providing instructions and documentation describing the physical and logical access capabilities necessary	45 C.F.R. §§ 164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		to the IoT device to perform each type of maintenance activity. ▪ Providing other information and actions as necessary for physically securing, and securely using, the IoT device based upon the IoT device use, purpose, and other contextual factors related to the digital ecosystem(s) within which they are intended to be used. ▪ Providing the details necessary for IoT device customers to implement only organizationally approved IoT device diagnostic tools within their system. ▪ Providing detailed documentation describing the tools manufacturers require for IoT device diagnostics activities. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		manufacturer and the manufacturer's supporting entities. ▪ Providing communications and comprehensive documentation describing maintenance operations that the IoT device customer is required to perform. If such comprehensive IoT device maintenance operations documentation does not exist, the manufacturer should clearly communicate to IoT device customers that the user must perform these operations themselves. ▪ Providing communications that include details for the recommended events that will trigger IoT device system reviews and/or maintenance by the manufacturer. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities. ▪ Providing the details necessary to enable IoT device customers to monitor	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		onsite and offsite IoT device maintenance activities. ▪ Providing the details necessary to implement management and operational controls for IoT device maintenance personnel and associated authorizations, and record-keeping of maintenance organizations and personnel. ▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization. ▪ Providing IoT device customers with the details necessary to implement management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally defined personnel or roles to follow.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks. ▪ Providing the details necessary for customers to document attempts to obtain IoT device components or IoT device information system service documentation when such documentation is either unavailable or nonexistent, and documenting the appropriate response for manufacturer employees, or supporting entities, to follow. ▪ Following procedures to obtain input from IoT device customers about the breadth and depth of the technical documentation provided with the IoT device to determine if it is acceptable to support customer needs. ▪ Providing a process for IoT device customers to contact the manufacturer to ask questions or obtain help related to the IoT device configuration settings.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		▪ Providing information to allow for in-house support from within the IoT device customer organization. ▪ Providing education explaining how to inspect IoT device and/or use maintenance tools to ensure the latest software updates and patches are installed. ▪ Providing education for how to scan for critical software updates and patches. ▪ Providing education that explains the legal requirements governing IoT device maintenance responsibilities or how to meet specific types of legal requirements when using the IoT device.	
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents	N/A	▪ Providing details about the types of, and situations that trigger, local and/or remote maintenance activities required once the device is purchased and deployed in the organization's digital ecosystem or within an individual consumer's home. ▪ Providing instructions and documentation describing the physical	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A) 164.310(d)(1) 164.310(d)(2)(ii) 164.310(d)(2)(iii) 164.312(a) 164.312(a)(2)(ii)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
unauthorized access.		and logical access capabilities necessary to the IoT device to perform each type of maintenance activity. ▪ Providing other information and actions as necessary for physically securing, and securely using, the IoT device based upon the IoT device use, purpose, and other contextual factors related to the digital ecosystem(s) within which they are intended to be used. ▪ Providing the details and instructions to perform necessary IoT device maintenance activities and repairs. ▪ Providing communications and comprehensive documentation describing the IoT device maintenance operations performed by the manufacturer and the manufacturer's supporting entities. ▪ Providing communications and documentation detailing how to perform recommended local and/or remote maintenance activities.	164.312(a)(2)(iv) 164.312(b) 164.312(d) 164.312(e)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		▪ Providing the details necessary to enable IoT device customers to monitor onsite and offsite IoT device maintenance activities. ▪ Providing the details necessary for maintaining records for nonlocal IoT device maintenance and diagnostic activities. ▪ Providing the details necessary to implement management and operational controls for IoT device maintenance personnel and associated authorizations, and record-keeping of maintenance organizations and personnel. ▪ Providing communications describing the type and nature of the local and/or remote maintenance activities that will involve and require manufacturer personnel, or their contractors, once the device is purchased and deployed in the IoT device customer's organization. ▪ Providing IoT device customers with the details necessary to implement	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		management and operational controls in support of their security policies and legal requirements for IoT device maintenance for assigned organizationally defined personnel or roles to follow. ▪ Providing documented descriptions of the specific maintenance procedures for defined maintenance tasks.	
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	▪ Ability to preserve system state information. ▪ Ability to support a list of events that are necessary for auditing purposes (to support the organizational auditing policy). ▪ Ability to identify and capture organizationally defined events using a persistent method. ▪ Ability to capture information from organizationally defined cybersecurity events (e.g., cybersecurity state, time) through organizationally defined means (e.g., logs).	▪ Providing the details requested by IoT device customers to perform periodic checks and/or audits to ensure IoT device security controls are functioning as intended following maintenance and repairs. ▪ Providing IoT device customers, upon their request, with the tools, assistance, instructions, and other support for the IoT device to perform audit and log maintenance and repairs.	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to create audit logs within the device for organizationally defined and auditable events (e.g., account creation, modification, enabling, disabling, removal actions, notifications). ▪ Ability to track users interacting with the device, the time they interacted with the device, the time the user logged out of the device, and to list this information in an audit log. ▪ Ability to log information pertaining to: o the type of event that occurred o the time that the event occurred o where the event occurred o the source of the event o the outcome of the event o the identity of users/processes associated with the event ▪ Ability to support auditing of configuration actions such as: o Current configuration state. o History of configuration changes. o When changes in configuration occurred.		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	○ Which account made the configuration change. ▪ Ability to provide information as to why the device captured a particular event or set of events. ▪ Ability to capture organizationally defined information to support examination of security incidents. ▪ Ability to record stored data access and usage. ▪ Ability to comply with organizational policy for storing persistent audit logs up to a predefined size. ▪ Ability to comply with organizational policy for audit log retention period. ▪ Ability to delete audit logs in accordance with organizational policy. ▪ Ability to send alerts when the logs are too big for the device to continue to store (if the predefined amount of time has not yet passed to delete them). ▪ Ability to support organizationally defined granularity in device timing measurements.		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to use synchronization with a verified time source to determine the validity of a time stamp. ▪ Ability to record timestamps convertible to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) to support a standardized representation of timing. ▪ Ability to log timing measurements outside a threshold value (e.g., enabling alerts if the device's system time is not reliable). ▪ Ability to run audit scans (automated or otherwise) to provide specific information (e.g., requested for an external process to audit the device). ▪ Ability to send requested audit logs to an external audit process or information system (e.g., where its auditing information can be checked to allow review, analysis, and reporting). ▪ Ability to keep an accurate internal system time.		

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	▪ Ability to restrict use of IoT device components (e.g., ports, functions, microphones, video). ▪ Ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device. ▪ Ability to restrict use of IoT device services. ▪ Ability to execute code in confined virtual environments. ▪ Ability to separate IoT device processes into separate execution domains. ▪ Ability to separate the levels of IoT device user functionality. ▪ Ability to authorize various levels of IoT device functionality. ▪ Ability to restrict components/features of the IoT device (e.g., ports, functions, protocols, services) in accordance with organizationally defined policies.	N/A	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)
PR.PT-4: Communications	▪ Ability to support wireless technologies needed by the organization (e.g., microwave, packet radio, ultrahigh	N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(D)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
and control networks are protected.	frequency/very high frequency]), Bluetooth, manufacturer defined). ▪ Ability to support communications technologies (including but not limited to): ○ IEEE 802.11 ○ Bluetooth ○ Ethernet ○ Manufacturer defined ▪ Ability to establish and configure IoT device settings for wireless technologies, including authentication protocols (e.g., Extensible Authentication Protocol [EAP]/TLS, Protected Extensible Authentication Protocol [PEAP]). ▪ Ability to enforce traffic flow policies. ▪ Ability to utilize standardized protocols. ▪ Ability to establish network connections. ▪ Ability to terminate network connections (e.g., automatically based on organizationally defined parameters). ▪ Ability to de-allocate Transmission Control Protocol/Internet Protocol (TCP/IP) address/port pairings.		164.312(a)(1) 164.312(b) 164.312(e)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to establish communications channels. ▪ Ability to secure the communications channels. ▪ Ability to interface with Domain Name System (DNS)/DNS Security Extensions (DNSSEC).		
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	N/A	▪ Providing documentation describing how to implement and securely deploy monitoring devices and tools for IoT devices and associated systems.	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.312(b)
DE.AE-2: Detected events are analyzed to understand attack targets and methods.	▪ Ability to identify organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device.	▪ Providing documentation describing IoT device behavior indicators that could occur when an attack is being launched.	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
DE.CM-1: The network is monitored to detect potential cybersecurity events.	▪ Ability to monitor specific actions based on the IoT device identity. ▪ Ability to access information about the IoT device's cybersecurity state and other necessary data. ▪ Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check). ▪ Ability to monitor communications traffic.	▪ Providing information that describes the types of system monitoring information generated from, or associated with, the IoT device and instructions for obtaining that information. ▪ Providing documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing how to perform monitoring activities.	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)
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	N/A	▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device. ▪ Providing descriptions of the physical access security procedures the	45 C.F.R. §§ 164.310(a)(2)(ii) 164.310(a)(2)(iii)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		manufacturer recommends for limiting physical access to the device and to associated device controls. ▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted or is occurring.	
DE.CM-4: Malicious code is detected.	N/A	▪ Providing education for how to implement malicious code protection in the IoT device and associated systems as well as how to detect and eradicate malicious code. ▪ Providing education for how to update the IoT device and related systems malicious code protection mechanisms when new releases are available, in accordance with organizational configuration management policy and procedures. ▪ If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, the	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
		manufacturer should provide education to IoT device customers describing how to use and/or configure malicious code protection mechanisms in IoT devices, supporting anti-malware tools, and related systems. ▪ Providing education that include the details necessary to implement management and operational controls for malicious code detection and eradication.	
DE.CM-5: Unauthorized mobile code is detected.	N/A	N/A	45 C.F.R. §§ 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check). ▪ Ability to monitor changes to the configuration settings.	▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity.	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)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
	▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera). ▪ Ability to detect remote activation of sensors. ▪ Ability to define the characteristics of unapproved content. ▪ Ability to scan files for unapproved content. ▪ Ability to prevent download of unapproved content. ▪ Ability to delete unapproved content. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.	

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
DE.CM-8: Vulnerability scans are performed.	N/A	N/A	45 C.F.R. §§ 164.308(a)(1)(i) 164.308(a)(8)
RS.RP-1: Response plan is executed during or after an event.	▪ Ability to respond to alerts according to predefined responses. ▪ Ability to respond following an auditing failure (either by the device or an external auditing process).	▪ Providing education describing the options and recommended responses to malicious code identification within the IoT device.	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)
RS.IM-1: Response plans incorporate lessons learned.	N/A	N/A	45 C.F.R. §§ 164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)
RS.IM-2: Response strategies are updated.	N/A	N/A	45 C.F.R. §§ 164.308(a)(7)(ii)(D) 164.308(a)(8)
RC.RP-1: Recovery plan is executed during or after a	N/A	N/A	45 C.F.R. §§ 164.308(a)(7) 164.308(a)(7)(i) 164.308(a)(7)(ii)

Cybersecurity Framework v1.1 Subcategory	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities	HIPAA Security Rule Mapping to Cybersecurity Framework Subcategory
cybersecurity incident.			164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)

1748

E-2 Device Capabilities Supporting Functional Evaluations

Table E-2 below builds on the functional evaluations included in Section 6 of this document. The table lists both device cybersecurity capabilities and nontechnical supporting capabilities that map to each of the functional test cases. Selecting devices and/or third parties that provide these capabilities can help achieve the respective functional requirements.

Table E-2 Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities that Map to Each of the Functional Test Cases

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
RPM-1 Asset Management: Device Management Demonstrate the ability to verify that provisioned devices are associated with the intended patient who has enrolled in an RPM program. **ID.AM-1** **ID.AM-5**	▪ Ability to detect unauthorized hardware and software components.	▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing IoT device customers with the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing IoT device customers with the details necessary to require unique identifiers for each IoT device associated with the system and critical system components within which it is used.
RPM-2 Risk Assessment: End-Point Vulnerability Scanning Demonstrate the ability to perform vulnerability	▪ Ability to differentiate between when a device will likely operate as expected from when it may be in a degraded cybersecurity state.	▪ Providing details for performing the tests necessary for IoT device and related system software updates, for effectiveness and to identify potential side effects, before installation.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
scans on assets and view results in a dashboard format with risk-scoring evaluations. **ID.RA-1** **ID.RA-4** **ID.RA-5** **ID.RA-6**		▪ Providing communications describing the types of security and privacy tests necessary for the IoT device and software before installation. ▪ Providing training and awareness information to IoT device customers that describe newly identified vulnerabilities and threats (such as zero-day malware) for the associated IoT device. ▪ Providing the details necessary for the installation of IoT devices and associated systems security-relevant software updates within an organizationally defined time period from the vendor release of the updates. ▪ Providing education describing the operational impacts of the anti-malware activities on mission critical processes in the system where the IoT device is used. ▪ Providing education explaining the responsibilities of IoT device customers to perform their own risk assessments, using information provided by the

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		manufacturer, to determine the risks the IoT device will bring into the IoT device customer's systems.

RPM-3 Identity Management, Authentication, and Access Control: Role-based Access
Demonstrate the ability to limit and disable access to data by implementing role-based access control on the Vivify platform.
PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AC-5
PR.AC-6
	▪ Ability to uniquely identify the IoT device logically.
	▪ Ability to uniquely identify a remote IoT device.
	▪ Ability for the device to support a unique device ID (e.g., to allow it to be linked to the person or process assigned to use the IoT device).
	▪ Ability to configure IoT device access control policies using IoT device identity.
	  ○ Ability to hide IoT device identity from non-authorized entities.
	  ○ Ability for the IoT device to differentiate between authorized and unauthorized remote users.
	  ○ Ability for the IoT device to differentiate between authorized and unauthorized physical device users.
	▪ Ability to verify the identity of an IoT device.
	▪ Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.
	▪ Ability for the IoT device to hide or mask authentication information during authentication process.
		▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used.
		▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.
		▪ Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used.
		▪ Providing the details necessary to require unique identifiers for each IoT device associated with the system and critical

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to set and change authentication configurations, policies and limitations settings for the IoT device. ▪ Ability to revoke access to the device. ▪ Ability to create unique IoT device user accounts. ▪ Ability to identify unique IoT device user accounts. ▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions. ▪ Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface. ▪ Ability to enable automation and reporting of account management activities. ○ Ability to assign access to IoT device audit controls to specific roles or organizationally defined personnel. ○ Ability to control access to IoT device audit data. ○ Ability to identify the user, process or device requesting access to the audit/accountability information (i.e., to ensure only authorized users and/or devices have access). ▪ Ability to establish conditions for shared/group accounts on the IoT device.	system components within which it is used. ▪ Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources. ▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems. ▪ Providing education explaining how to enforce authorized access at the system level. ▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device based upon the determined risk level that the device brings to the IoT customer's system. ▪ Providing descriptions of the physical access security procedures the

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to administer conditions for shared/group accounts on the IoT device. ▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions. ▪ Ability to authenticate external users and systems. ▪ Ability to securely interact with authorized external, third-party systems. ▪ Ability to identify when an external system meets the required security requirements for a connection. ▪ Ability to establish secure communications with internal systems when the device is operating on external networks. ▪ Ability to establish requirements for remote access to the IoT device and/or IoT device interface, including: o usage restrictions o configuration requirements o connection requirements o manufacturer established requirement ▪ Ability to enforce the established local and remote access requirements. ▪ Ability to prevent external access to the IoT device management interface.	manufacturer recommends for limiting physical access to the device and to associated device controls. ▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted or is occurring. ▪ Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device. ▪ Providing details about the specific types of manufacturer's needs to access the IoT device interfaces; such as for specific support, updates, ongoing maintenance, and other purposes. ▪ Providing documentation with instructions for how to restrict interface connections that enable specific activities.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities

	▪ Ability to control the IoT device's logical interface (e.g., locally or remotely).
	▪ Ability to detect remote activation attempts.
	▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera).
	▪ Ability to detect remote activation of sensors.
	▪ Ability to establish access to the IoT device to perform organizationally defined user actions without identification or authentication.
	▪ Ability to assign roles to IoT device user accounts.
	▪ Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary)
	    ○ Ability to establish user accounts to support role-based logical access privileges.
	    ○ Ability to administer user accounts to support role-based logical access privileges.
	    ○ Ability to use organizationally defined roles to define each user account's access and permitted device actions.
	▪ Ability to support multiple levels of user/process account functionality and roles for the IoT device.
		▪ Providing descriptions of the types of access to the IoT device that the manufacturer will require on an ongoing or regular basis.
		▪ Providing detailed instructions for how to implement management and operational controls based on the role of the IoT device user, and not on an individual basis.
		▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion.
		▪ Providing a detailed description of the other types of devices and systems that will access the IoT device during customer use of the device, and how they will access it.
		▪ Providing communications and detailed instructions for implementing a hierarchy

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to apply least privilege to user accounts (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions) ○ Ability to create additional processes, roles (e.g., admin, emergency, temporary) and accounts as necessary to achieve least privilege. ○ Ability to apply least privilege settings within the device (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions). ○ Ability to limit access to privileged device settings that are used to establish and administer authorization requirements. ○ Ability for authorized users to access privileged settings. ▪ Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on: ○ run-time access control decisions facilitated by dynamic privilege management. ○ Organizationally defined actions to access/use device	of privilege levels to use with the IoT device and/or necessary associated information systems. ▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools. ▪ Providing education and supporting materials explaining how to establish roles and responsibilities for IoT device data security, using the device capabilities and/or other services that communicate or interface with the device. ▪ Providing education and supporting materials describing the IoT device capabilities for role-based controls, and how to establish different roles within the IoT device. ▪ Providing education and supporting materials for how to establish roles to

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to allow information sharing capabilities based upon the type and/or role of user attempting to share the information. ▪ Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization. ▪ Ability to establish pre-defined restrictions for information searches within the device. ▪ Ability to establish limits on authorized concurrent device sessions for: ○ user accounts ○ roles ○ groups ○ dates ○ times ○ locations ○ manufacturer-established parameters ▪ Ability to restrict updating actions to authorized entities. ▪ Ability to restrict access to the cybersecurity state indicator to authorized entities. ▪ Ability to enforce the established local and remote access requirements.	support IoT device policies, procedures and associated documentation.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means. ▪ Ability to store and process session identifiers. ▪ Ability to identify and track sessions with identifiers. ▪ Ability to enforce access to memory space through the kernel. ▪ Ability to prevent a process from accessing memory space of another process. ▪ Ability to obtain and validate certificates. ▪ Ability to identify unique users interacting with the device (to allow for user session monitoring).	
RPM-4 Identity Management, Authentication, and Access Control: Domain User Authentication and Authorization Demonstrate the ability to create new domain users and enforce restrictions on nonadmin users.	▪ Ability to uniquely identify the IoT device logically. ▪ Ability to uniquely identify a remote IoT device. ▪ Ability for the device to support a unique device ID (e.g., to allow it to be linked to the person or process assigned to use the IoT device). ▪ Ability to configure IoT device access control policies using IoT device identity. ○ Ability to hide IoT device identity from non-authorized entities. ○ Ability for the IoT device to differentiate between authorized and unauthorized remote users.	▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
PR.AC-1 **PR.AC-2** **PR.AC-3** **PR.AC-4** **PR.AC-5** **PR.AC-6**	○ Ability for the IoT device to differentiate between authorized and unauthorized physical device users. ▪ Ability to verify the identity of an IoT device. ▪ Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access. ▪ Ability for the IoT device to hide or mask authentication information during authentication process. ▪ Ability to set and change authentication configurations, policies and limitations settings for the IoT device. ▪ Ability to revoke access to the device. ▪ Ability to create unique IoT device user accounts. ▪ Ability to identify unique IoT device user accounts. ▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions. ▪ Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface. ▪ Ability to enable automation and reporting of account management activities.	▪ Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used. ▪ Providing the details necessary to require unique identifiers for each IoT device associated with the system and critical system components within which it is used. ▪ Providing education explaining how to establish and enforce approved authorizations for logical access to IoT device information and system resources. ▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems. ▪ Providing education explaining how to enforce authorized access at the system level.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	○ Ability to assign access to IoT device audit controls to specific roles or organizationally defined personnel. ○ Ability to control access to IoT device audit data. ○ Ability to identify the user, process or device requesting access to the audit/accountability information (i.e., to ensure only authorized users and/or devices have access). ▪ Ability to establish conditions for shared/group accounts on the IoT device. ▪ Ability to administer conditions for shared/group accounts on the IoT device. ▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions. ▪ Ability to authenticate external users and systems. ▪ Ability to securely interact with authorized external, third-party systems. ▪ Ability to identify when an external system meets the required security requirements for a connection. ▪ Ability to establish secure communications with internal systems when the device is operating on external networks.	▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device based upon the determined risk level that the device brings to the IoT customer's system. ▪ Providing descriptions of the physical access security procedures the manufacturer recommends for limiting physical access to the device and to associated device controls. ▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted or is occurring. ▪ Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to establish requirements for remote access to the IoT device and/or IoT device interface, including: ○ usage restrictions ○ configuration requirements ○ connection requirements ○ manufacturer established requirement ▪ Ability to enforce the established local and remote access requirements. ▪ Ability to prevent external access to the IoT device management interface. ▪ Ability to control the IoT device's logical interface (e.g., locally or remotely). ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera). ▪ Ability to detect remote activation of sensors. ▪ Ability to establish access to the IoT device to perform organizationally defined user actions without identification or authentication. ▪ Ability to assign roles to IoT device user accounts.	▪ Providing details about the specific types of manufacturer's needs to access the IoT device interfaces; such as for specific support, updates, ongoing maintenance, and other purposes. ▪ Providing documentation with instructions for how to restrict interface connections that enable specific activities. ▪ Providing descriptions of the types of access to the IoT device that the manufacturer will require on an ongoing or regular basis. ▪ Providing detailed instructions for how to implement management and operational controls based on the role of the IoT device user, and not on an individual basis. ▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary) ○ Ability to establish user accounts to support role-based logical access privileges. ○ Ability to administer user accounts to support role-based logical access privileges. ○ Ability to use organizationally defined roles to define each user account's access and permitted device actions. ▪ Ability to support multiple levels of user/process account functionality and roles for the IoT device. ▪ Ability to apply least privilege to user accounts (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions) ○ Ability to create additional processes, roles (e.g., admin, emergency, temporary) and accounts as necessary to achieve least privilege. ○ Ability to apply least privilege settings within the device (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions).	unauthorized access, modification, and deletion. ▪ Providing a detailed description of the other types of devices and systems that will access the IoT device during customer use of the device, and how they will access it. ▪ Providing communications and detailed instructions for implementing a hierarchy of privilege levels to use with the IoT device and/or necessary associated information systems. ▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools. ▪ Providing education and supporting materials explaining how to establish roles and responsibilities for IoT device data security, using the device capabilities and/or other services that

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	○ Ability to limit access to privileged device settings that are used to establish and administer authorization requirements. ○ Ability for authorized users to access privileged settings. ▪ Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on: ○ run-time access control decisions facilitated by dynamic privilege management. ○ Organizationally defined actions to access/use device ▪ Ability to allow information sharing capabilities based upon the type and/or role of user attempting to share the information. ▪ Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization. ▪ Ability to establish pre-defined restrictions for information searches within the device. ▪ Ability to establish limits on authorized concurrent device sessions for: ○ user accounts	communicate or interface with the device. ▪ Providing education and supporting materials describing the IoT device capabilities for role-based controls, and how to establish different roles within the IoT device. ▪ Providing education and supporting materials for how to establish roles to support IoT device policies, procedures and associated documentation.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	○ roles ○ groups ○ dates ○ times ○ locations ○ manufacturer-established parameters ▪ Ability to restrict updating actions to authorized entities. ▪ Ability to restrict access to the cybersecurity state indicator to authorized entities. ▪ Ability to enforce the established local and remote access requirements. ▪ Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means. ▪ Ability to store and process session identifiers. ▪ Ability to identify and track sessions with identifiers. ▪ Ability to enforce access to memory space through the kernel. ▪ Ability to prevent a process from accessing memory space of another process. ▪ Ability to obtain and validate certificates. ▪ Ability to identify unique users interacting with the device (to allow for user session monitoring).	

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities

RPM-5 Identity Management, Authentication, and Access Control: Network Segmentation and Access Control Policy
Demonstrate the use of network segmentation and an access control policy to allow permitted traffic to selected network devices.
PR.AC-1
PR.AC-2
PR.AC-3
PR.AC-4
PR.AC-5
PR.AC-6
	▪ Ability to uniquely identify the IoT device logically.
	▪ Ability to uniquely identify a remote IoT device.
	▪ Ability for the device to support a unique device ID (e.g., to allow it to be linked to the person or process assigned to use the IoT device).
	▪ Ability to configure IoT device access control policies using IoT device identity.
	  ○ Ability to hide IoT device identity from non-authorized entities.
	  ○ Ability for the IoT device to differentiate between authorized and unauthorized remote users.
	  ○ Ability for the IoT device to differentiate between authorized and unauthorized physical device users.
	▪ Ability to verify the identity of an IoT device.
	▪ Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.
	▪ Ability for the IoT device to hide or mask authentication information during authentication process.
	▪ Ability to set and change authentication configurations, policies and limitations settings for the IoT device.
	▪ Ability to revoke access to the device.
		▪ Providing details for how to establish unique identification for each IoT device associated with the system and critical system components within which it is used.
		▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools.
		▪ Providing the details necessary to establish and implement unique identification for each IoT device associated with the system and critical system components within which it is used.
		▪ Providing the details necessary to require unique identifiers for each IoT device associated with the system and critical system components within which it is used.
		▪ Providing education explaining how to establish and enforce approved

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities

	▪ Ability to create unique IoT device user accounts.
	▪ Ability to identify unique IoT device user accounts.
	▪ Ability to create organizationally defined accounts that support privileged roles with automated expiration conditions.
	▪ Ability to establish organizationally defined user actions for accessing the IoT device and/or device interface.
	▪ Ability to enable automation and reporting of account management activities.
	    ○ Ability to assign access to IoT device audit controls to specific roles or organizationally defined personnel.
	    ○ Ability to control access to IoT device audit data.
	    ○ Ability to identify the user, process or device requesting access to the audit/accountability information (i.e., to ensure only authorized users and/or devices have access).
	▪ Ability to establish conditions for shared/group accounts on the IoT device.
	▪ Ability to administer conditions for shared/group accounts on the IoT device.
		authorizations for logical access to IoT device information and system resources.
		▪ Providing education explaining how to control access to IoT devices implemented within IoT device customer information systems.
		▪ Providing education explaining how to enforce authorized access at the system level.
		▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device based upon the determined risk level that the device brings to the IoT customer's system.
		▪ Providing descriptions of the physical access security procedures the manufacturer recommends for limiting physical access to the device and to associated device controls.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities

	▪ Ability to restrict the use of shared/group accounts on the IoT device according to organizationally defined conditions.
	▪ Ability to authenticate external users and systems.
	▪ Ability to securely interact with authorized external, third-party systems.
	▪ Ability to identify when an external system meets the required security requirements for a connection.
	▪ Ability to establish secure communications with internal systems when the device is operating on external networks.
	▪ Ability to establish requirements for remote access to the IoT device and/or IoT device interface, including:
	  ○ usage restrictions
	  ○ configuration requirements
	  ○ connection requirements
	  ○ manufacturer established requirement
	▪ Ability to enforce the established local and remote access requirements.
	▪ Ability to prevent external access to the IoT device management interface.
	▪ Ability to control the IoT device's logical interface (e.g., locally or remotely).
		▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted or is occurring.
		▪ Providing the tools, assistance, instructions, and other types of information to support establishing a hierarchy of role-based privileges within the IoT device.
		▪ Providing details about the specific types of manufacturer's needs to access the IoT device interfaces; such as for specific support, updates, ongoing maintenance, and other purposes.
		▪ Providing documentation with instructions for how to restrict interface connections that enable specific activities.
		▪ Providing descriptions of the types of access to the IoT device that the manufacturer will require on an ongoing or regular basis.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera). ▪ Ability to detect remote activation of sensors. ▪ Ability to establish access to the IoT device to perform organizationally defined user actions without identification or authentication. ▪ Ability to assign roles to IoT device user accounts. ▪ Ability to support a hierarchy of logical access privileges for the IoT device based on roles (e.g., admin, emergency, user, local, temporary) ○ Ability to establish user accounts to support role-based logical access privileges. ○ Ability to administer user accounts to support role-based logical access privileges. ○ Ability to use organizationally defined roles to define each user account's access and permitted device actions. ▪ Ability to support multiple levels of user/process account functionality and roles for the IoT device.	▪ Providing detailed instructions for how to implement management and operational controls based on the role of the IoT device user, and not on an individual basis. ▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing a detailed description of the other types of devices and systems that will access the IoT device during customer use of the device, and how they will access it. ▪ Providing communications and detailed instructions for implementing a hierarchy of privilege levels to use with the IoT device and/or necessary associated information systems.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to apply least privilege to user accounts (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions) ○ Ability to create additional processes, roles (e.g., admin, emergency, temporary) and accounts as necessary to achieve least privilege. ○ Ability to apply least privilege settings within the device (i.e., to ensure that the processes operate at privilege levels no higher than necessary to accomplish required functions). ○ Ability to limit access to privileged device settings that are used to establish and administer authorization requirements. ○ Ability for authorized users to access privileged settings. ▪ Ability to implement dynamic access control approaches (e.g., service-oriented architectures) that rely on: ○ run-time access control decisions facilitated by dynamic privilege management. ○ Organizationally defined actions to access/use device	▪ Providing communications and documentation detailing how to perform account management activities, using the technical IoT device capabilities, or through supporting systems and/or tools. ▪ Providing education and supporting materials explaining how to establish roles and responsibilities for IoT device data security, using the device capabilities and/or other services that communicate or interface with the device. ▪ Providing education and supporting materials describing the IoT device capabilities for role-based controls, and how to establish different roles within the IoT device. ▪ Providing education and supporting materials for how to establish roles to support IoT device policies, procedures and associated documentation.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities

	▪ Ability to allow information sharing capabilities based upon the type and/or role of user attempting to share the information.
	▪ Ability to restrict access to IoT device software, hardware, and data based on user account roles, used with proper authentication of the identity of the user to determine type of authorization.
	▪ Ability to establish pre-defined restrictions for information searches within the device.
	▪ Ability to establish limits on authorized concurrent device sessions for:
	    ○ user accounts
	    ○ roles
	    ○ groups
	    ○ dates
	    ○ times
	    ○ locations
	    ○ manufacturer-established parameters
	▪ Ability to restrict updating actions to authorized entities.
	▪ Ability to restrict access to the cybersecurity state indicator to authorized entities.
	▪ Ability to enforce the established local and remote access requirements.	

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to update the device's software through remote (e.g., network download) and/or local (e.g., removable media) means. ▪ Ability to store and process session identifiers. ▪ Ability to identify and track sessions with identifiers. ▪ Ability to enforce access to memory space through the kernel. ▪ Ability to prevent a process from accessing memory space of another process. ▪ Ability to obtain and validate certificates. ▪ Ability to identify unique users interacting with the device (to allow for user session monitoring).	
RPM-6 Security Continuous Monitoring: Malware Protection Demonstrate the ability to protect the network and end points from malicious services by blocking the service before a connection is made. **DE.CM-1**	▪ Ability to monitor specific actions based on the IoT device identity. ▪ Ability to access information about the IoT device's cybersecurity state and other necessary data. ▪ Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check	▪ Providing information that describes the types of system monitoring information generated from, or associated with, the IoT device and instructions for obtaining that information. ▪ Providing documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
DE.CM-2 **DE.CM-4** **DE.CM-7** **DE.CM-8**	itself or provide the information necessary for an external process to check). ▪ Ability to monitor communications traffic. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera). ▪ Ability to detect remote activation of sensors. ▪ Ability to define the characteristics of unapproved content. ▪ Ability to scan files for unapproved content. ▪ Ability to prevent download of unapproved content. ▪ Ability to delete unapproved content. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing how to perform monitoring activities. ▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device. ▪ Providing descriptions of the physical access security procedures the manufacturer recommends for limiting physical access to the device and to associated device controls. ▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted or is occurring. ▪ Providing education for how to implement malicious code protection in

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		the IoT device and associated systems as well as how to detect and eradicate malicious code. ▪ Providing education for how to update the IoT device and related systems malicious code protection mechanisms when new releases are available, in accordance with organizational configuration management policy and procedures. ▪ If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, the manufacturer should provide education to IoT device customers describing how to use and/or configure malicious code protection mechanisms in IoT devices, supporting anti-malware tools, and related systems. ▪ Providing education that include the details necessary to implement management and operational controls

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		for malicious code detection and eradication. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.
RPM-7 Security Continuous Monitoring: Malicious Activity Detection Demonstrate the ability to detect anomalous network traffic and	▪ Ability to monitor specific actions based on the IoT device identity. ▪ Ability to access information about the IoT device's cybersecurity state and other necessary data. ▪ Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device.	▪ Providing information that describes the types of system monitoring information generated from, or associated with, the IoT device and instructions for obtaining that information. ▪ Providing documentation describing the types of monitoring tools with which the

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
create an alert for further investigation. **DE.CM-1** **DE.CM-2** **DE.CM-4** **DE.CM-7** **DE.CM-8**	▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check). ▪ Ability to monitor communications traffic. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera). ▪ Ability to detect remote activation of sensors. ▪ Ability to define the characteristics of unapproved content. ▪ Ability to scan files for unapproved content. ▪ Ability to prevent download of unapproved content. ▪ Ability to delete unapproved content. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing how to perform monitoring activities. ▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device. ▪ Providing descriptions of the physical access security procedures the manufacturer recommends for limiting physical access to the device and to associated device controls. ▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		IoT device was or is attempted or is occurring. ▪ Providing education for how to implement malicious code protection in the IoT device and associated systems as well as how to detect and eradicate malicious code. ▪ Providing education for how to update the IoT device and related systems malicious code protection mechanisms when new releases are available, in accordance with organizational configuration management policy and procedures. ▪ If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, the manufacturer should provide education to IoT device customers describing how to use and/or configure malicious code protection mechanisms in IoT devices,

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		supporting anti-malware tools, and related systems. ▪ Providing education that include the details necessary to implement management and operational controls for malicious code detection and eradication. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer’s supporting entity. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.
RPM-8	▪ Ability to monitor specific actions based on the IoT device identity.	▪ Providing information that describes the types of system monitoring information

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
Security Continuous Monitoring: End-Point Monitoring and Protection Demonstrate the ability to detect unusual authentication behaviors and file integrity changes on protected end points. **DE.CM-1** **DE.CM-2** **DE.CM-4** **DE.CM-7** **DE.CM-8**	▪ Ability to access information about the IoT device's cybersecurity state and other necessary data. ▪ Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check). ▪ Ability to monitor communications traffic. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera). ▪ Ability to detect remote activation of sensors. ▪ Ability to define the characteristics of unapproved content. ▪ Ability to scan files for unapproved content. ▪ Ability to prevent download of unapproved content. ▪ Ability to delete unapproved content.	generated from, or associated with, the IoT device and instructions for obtaining that information. ▪ Providing documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing how to perform monitoring activities. ▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used to prevent unauthorized physical access to the IoT device. ▪ Providing descriptions of the physical access security procedures the manufacturer recommends for limiting

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	physical access to the device and to associated device controls. ▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted or is occurring. ▪ Providing education for how to implement malicious code protection in the IoT device and associated systems as well as how to detect and eradicate malicious code. ▪ Providing education for how to update the IoT device and related systems malicious code protection mechanisms when new releases are available, in accordance with organizational configuration management policy and procedures. ▪ If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, the

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		manufacturer should provide education to IoT device customers describing how to use and/or configure malicious code protection mechanisms in IoT devices, supporting anti-malware tools, and related systems. ▪ Providing education that include the details necessary to implement management and operational controls for malicious code detection and eradication. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the monitoring service of the manufacturer's supporting entity. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems.

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		▪ Providing documentation that describes indicators of unauthorized use of the IoT device.
RPM-9 Security Continuous Monitoring: End-Point Network Access Monitoring This test case demonstrates the ability to create alarms for unauthorized network traffic. **DE.CM-1** **DE.CM-2** **DE.CM-4** **DE.CM-7** **DE.CM-8**	▪ Ability to monitor specific actions based on the IoT device identity. ▪ Ability to access information about the IoT device's cybersecurity state and other necessary data. ▪ Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device. ▪ Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check). ▪ Ability to monitor communications traffic. ▪ Ability to monitor changes to the configuration settings. ▪ Ability to detect remote activation attempts. ▪ Ability to detect remote activation of a collaborative computing device/component (e.g., microphone, camera). ▪ Ability to detect remote activation of sensors.	▪ Providing information that describes the types of system monitoring information generated from, or associated with, the IoT device and instructions for obtaining that information. ▪ Providing documentation describing the types of monitoring tools with which the IoT device is compatible, and recommendations for how to configure the IoT device to best work with such monitoring tools. ▪ Providing the details necessary to monitor IoT devices and associated systems. ▪ Providing documentation describing how to perform monitoring activities. ▪ Providing descriptions of the types of physical access practices, and manufacturer suggested hardware or other types of devices, that can be used

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to define the characteristics of unapproved content. ▪ Ability to scan files for unapproved content. ▪ Ability to prevent download of unapproved content. ▪ Ability to delete unapproved content. ▪ Ability to take organizationally defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a Universal Serial Bus [USB] port is present).	to prevent unauthorized physical access to the IoT device. ▪ Providing descriptions of the physical access security procedures the manufacturer recommends for limiting physical access to the device and to associated device controls. ▪ Providing details of indications, and recommendations for how to determine, when unauthorized physical access to the IoT device was or is attempted or is occurring. ▪ Providing education for how to implement malicious code protection in the IoT device and associated systems as well as how to detect and eradicate malicious code. ▪ Providing education for how to update the IoT device and related systems malicious code protection mechanisms when new releases are available, in accordance with organizational

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		configuration management policy and procedures. ▪ If the IoT device manufacturer provides anti-malware for the associated IoT device, or if the IoT device has built-in anti-malware capabilities, the manufacturer should provide education to IoT device customers describing how to use and/or configure malicious code protection mechanisms in IoT devices, supporting anti-malware tools, and related systems. ▪ Providing education that include the details necessary to implement management and operational controls for malicious code detection and eradication. ▪ Providing appropriate tools, assistance, instructions, or other details describing the capabilities for monitoring the IoT device and/or for the IoT device customer to report actions to the

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
		monitoring service of the manufacturer's supporting entity. ▪ Providing documentation describing details necessary to identify unauthorized use of IoT devices and their associated systems. ▪ Providing documentation that describes indicators of unauthorized use of the IoT device.
RPM-10 Data Security: Data in Transit Is Protected Demonstrate the ability to protect data in transit between the patient home and the telehealth platform. **PR.DS-2**	▪ Ability to execute cryptographic mechanisms of appropriate strength and performance. ▪ Ability to perform authenticated encryption algorithms. ▪ Ability to change keys securely. ▪ Ability to store encryption keys securely. ▪ Ability to secure data stored in remote storage areas (e.g., cloud, server). ▪ Ability to support trusted data exchange with a specified minimum-strength cryptography algorithm. ▪ Ability to support data encryption and signing to prevent data from being altered in transit. ▪ Ability to utilize one or more capabilities to protect transmitted data from unauthorized access and modification.	▪ Providing documentation and/or other communications describing how to implement management and operational controls to protect data obtained from IoT devices and associated systems from unauthorized access, modification, and deletion. ▪ Providing education describing how to securely handle and retain IoT device data, associated systems data, and data output from the IoT device to meet requirements of the IoT device customers' organizational security policies, contractual requirements,

Test Case Identification (ID) and Description with Relevant Cybersecurity Framework Subcategories	Device Cybersecurity Capabilities	Manufacturer Nontechnical Supporting Capabilities
	▪ Ability to use cryptographic means to validate the integrity of data transmitted. ▪ Ability to protect the audit information through: ○ encryption ○ digitally signing audit files ○ securely sending audit files to another device ○ other protections created by the device manufacturer	applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and other legal requirements.

1756

Appendix F Applying the OSI Model in Understanding Zero Trust Architecture

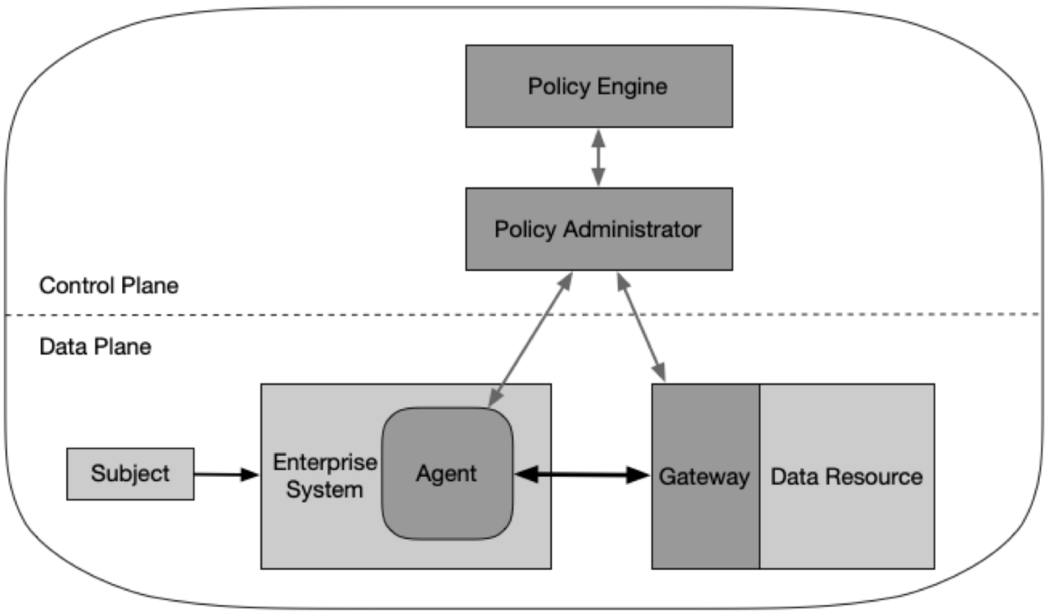
Networking professionals often refer to the Open Systems Interconnection (OSI) model when implementing network protocols. The International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) describe the OSI model as consisting of seven layers called Application, Presentation, Session, Transport, Network, Data Link, and Physical, where layers are numerically ordered in reverse. That is, the Application Layer is regarded as Layer 7, whereas the Physical Layer is regarded as Layer 1, a proof of concept to secure network sessions between the patient home and the telehealth platform provider [39].

Layer 2 aligns with the OSI model's Data link layer. Devices operating at Layer 2 have media access control (MAC) addresses by which devices, such as biometric devices, may communicate across a local area network (LAN) segment. Layer 3 aligns with the OSI model's Network layer. Devices implement the Network layer with Internet Protocol (IP) addresses. Layer 2 over Layer 3 solutions enable devices that do not implement the Network layer to have broader interconnectivity. Layer 2 over Layer 3 solutions provide security by limiting access to devices and securing the data-in-transit communications, e.g., with encryption. Layer 2 over Layer 3 solutions may be used to create secure enclaves, grouping small numbers of devices that may require enhanced network security. Creating secure enclaves aligns with the concept of micro-segmentation.

Organizations may consider Layer 2 over Layer 3 solutions for devices that may be prone to internet threats. Biometric devices may implement Layer 2 and Layer 3 interconnectivity; however, they do not have robust controls that prevent unauthorized remote access. Secure enclaves may be created that encapsulate biometric devices with other devices when secure cross communication is required. This practice guide deployed a Layer 2 over Layer 3 solution as part of a proof of concept within the healthcare lab.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, *Zero Trust Architecture* [22], describes an enclave gateway model that may be applied to a telehealth remote patient monitoring (RPM) architecture. In the enclave gateway model, a zero trust solution operates in two conceptual planes: a control and a data plane. Micro-segmentation management devices operate in a control plane. These management devices provide administrative and policy capabilities to support secure enclaves. Operational components, such as biometric devices, telehealth platform provider services, and devices hosted by healthcare delivery organizations, may operate in the data plane. Figure F-1 depicts the enclave gateway model.

Figure F-1 Enclave Gateway Model [25]



The Layer 2 over Layer 3 solution used in this practice guide brings principles on zero trust architecture (ZTA) to telehealth RPM. Managed biometric devices may be subject to threats that may be present in the patient home network. The Layer 2 over Layer 3 approach segments the RPM components from other devices that may operate in the patient home. Devices not associated with the deployed RPM components do not have a communication pathway to the RPM devices. ZTA allows the biometric devices to authenticate into the Layer 2 over Layer 3 security solution so that only traffic from the RPM components traverses the Layer 2 over Layer 3 network. Practitioners should refer to NIST SP 800-207, *Zero Trust Architecture,* for guidance [22].

NIST SPECIAL PUBLICATION 1800-30C

Securing Telehealth Remote Patient Monitoring Ecosystem

Volume C:
How-To Guides

Jennifer Cawthra*
Nakia Grayson
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Sue Wang
Ryan Williams
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

*Former employee; all work for this publication done while at employer.

May 2021

SECOND DRAFT

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

DISCLAIMER

National Institute of Standards and Technology Special Publication 1800-30C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-30C, 160 pages, (May 2021), 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: May 6, 2021 through June 7, 2021

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

Increasingly, healthcare delivery organizations (HDOs) are relying on telehealth and remote patient monitoring (RPM) capabilities to treat patients at home. RPM is convenient and cost-effective, and its adoption rate has increased. However, without adequate privacy and cybersecurity measures, unauthorized individuals may expose sensitive data or disrupt patient monitoring services.

RPM solutions engage multiple actors as participants in a patient's clinical care. These actors include HDOs, telehealth platform providers, and the patients themselves. Each participant uses, manages, and maintains different technology components within an interconnected ecosystem, and each is

responsible for safeguarding their piece against unique threats and risks associated with RPM technologies.

This practice guide assumes that the HDO engages with a telehealth platform provider that is a separate entity from the HDO and patient. The telehealth platform provider manages a distinct infrastructure, applications, and set of services. The telehealth platform provider coordinates with the HDO to provision, configure, and deploy the RPM components to the patient home and assures secure communication between the patient and clinician.

The NCCoE analyzed risk factors regarding an RPM ecosystem by using risk assessment based on the NIST Risk Management Framework. The NCCoE also leveraged the NIST Cybersecurity Framework, *NIST Privacy Framework,* and other relevant standards to identify measures to safeguard the ecosystem. In collaboration with healthcare, technology, and telehealth partners, the NCCoE built an RPM ecosystem in a laboratory environment to explore methods to improve the cybersecurity of an RPM.

Technology solutions alone may not be sufficient to maintain privacy and security controls on external environments. This practice guide notes the application of people, process, and technology as necessary to implement a holistic risk mitigation strategy.

This practice guide's capabilities include helping organizations assure the confidentiality, integrity, and availability of an RPM solution, enhancing patient privacy, and limiting HDO risk when implementing an RPM solution.

KEYWORDS

access control; authentication; authorization; behavioral analytics; cloud storage; data privacy; data security; encryption; HDO; healthcare; healthcare delivery organization; remote patient monitoring; RPM; telehealth

ACKNOWLEDGMENTS

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

Name	Organization
Alex Mohseni	Accuhealth
Stephen Samson	Accuhealth
Brian Butler	Cisco

Name	Organization
Matthew Hyatt	Cisco
Kevin McFadden	Cisco
Peter Romness	Cisco
Steven Dean	Inova Health System
Zach Furness	Inova Health System
James Carder	LogRhythm
Brian Coulson	LogRhythm
Steven Forsyth	LogRhythm
Jake Haldeman	LogRhythm
Andrew Hollister	LogRhythm
Zack Hollister	LogRhythm
Dan Kaiser	LogRhythm
Sally Vincent	LogRhythm
Vidya Murthy	MedCrypt
Axel Wirth	MedCrypt
Stephanie Domas	MedSec
Garrett Sipple	MedSec
Nancy Correll	The MITRE Corporation

Name	Organization
Spike Dog	The MITRE Corporation
Robin Drake	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Donald Faatz	The MITRE Corporation
Nedu Irrechukwu	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Stuart Shapiro	The MITRE Corporation
John Dwyier	Onclave Networks, Inc. (Onclave)
Chris Grodzickyj	Onclave
Marianne Meins	Onclave
Dennis Perry	Onclave
Christina Phillips	Onclave
Robert Schwendinger	Onclave
James Taylor	Onclave
Chris Jensen	Tenable
Joshua Moll	Tenable
Jeremiah Stallcup	Tenable
Julio C. Cespedes	The University of Mississippi Medical Center

Name	Organization
Saurabh Chandra	The University of Mississippi Medical Center
Donald Clark	The University of Mississippi Medical Center
Alan Jones	The University of Mississippi Medical Center
Kristy Simms	The University of Mississippi Medical Center
Richard Summers	The University of Mississippi Medical Center
Steve Waite	The University of Mississippi Medical Center
Dele Atunrase	Vivify Health
Aaron Gatz	Vivify Health
Michael Hawkins	Vivify Health
Robin Hill	Vivify Health
Dennis Leonard	Vivify Health
David Norman	Vivify Health
Bill Paschall	Vivify Health
Eric Rock	Vivify Health
Alan Stryker	Vivify Health
Dave Sutherland	Vivify Health
Michael Tayler	Vivify Health

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
Accuhealth	Accuhealth Evelyn
Cisco	Cisco Firepower Version 6.3.0 Cisco Umbrella Cisco Stealthwatch Version 7.0.0
Inova Health System	subject matter expertise
LogRhythm	LogRhythm XDR Version 7.4.9 LogRhythm NetworkXDR Version 4.0.2
MedCrypt	subject matter expertise
MedSec	subject matter expertise
Onclave Networks, Inc. (Onclave)	Onclave Zero Trust Platform Version 1.1.0
Tenable	Tenable.sc Vulnerability Management Version 5.13.0 with Nessus
The University of Mississippi Medical Center	subject matter expertise
Vivify Health	Vivify Pathways Home Vivify Pathways Care Team Portal

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms "may" and "need not" indicate a course of action permissible within the limits of the publication. The terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: hit_nccoe@nist.gov

Contents

List of Figures

1 Introduction

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

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

1.1 How to Use this Guide

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the telehealth remote patient monitoring (RPM) environment. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-30A: *Executive Summary*
- NIST SP 1800-30B: *Approach, Architecture, and Security Characteristics*–what we built and why
- NIST SP 1800-30C: *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 1800-30A, which describes the following topics:

- challenges that enterprises face in securing the remote patient monitoring ecosystem
- 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 1800-30B, 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 1800-30A, with your leadership team members to help them understand the importance of adopting standards-based commercially available technologies that can help secure the RPM 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 1800-30C, 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 the National Cybersecurity Center of Excellences' (NCCoE's) risk assessment and deployment of a defense-in-depth strategy in a distributed RPM 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 are in the List of Acronyms appendix.

1.2 Build Overview

The NCCoE constructed a virtual lab environment to evaluate ways to implement security capabilities across an RPM ecosystem, which consists of three separate domains: patient home, telehealth platform provider, and healthcare delivery organization (HDO). The project implements virtual environments for the HDO and patient home while collaborating with a telehealth platform provider to implement a cloud-based telehealth RPM environment. The telehealth environments contain simulated patient data that portray relevant cases that clinicians could encounter in real-world scenarios. The project then applies security controls to the virtual environments. Refer to NIST Special Publication (SP) 1800-30B, Section 5, Security Characteristic Analysis, for an explanation of why we used each technology.

1.3 Typographic Conventions

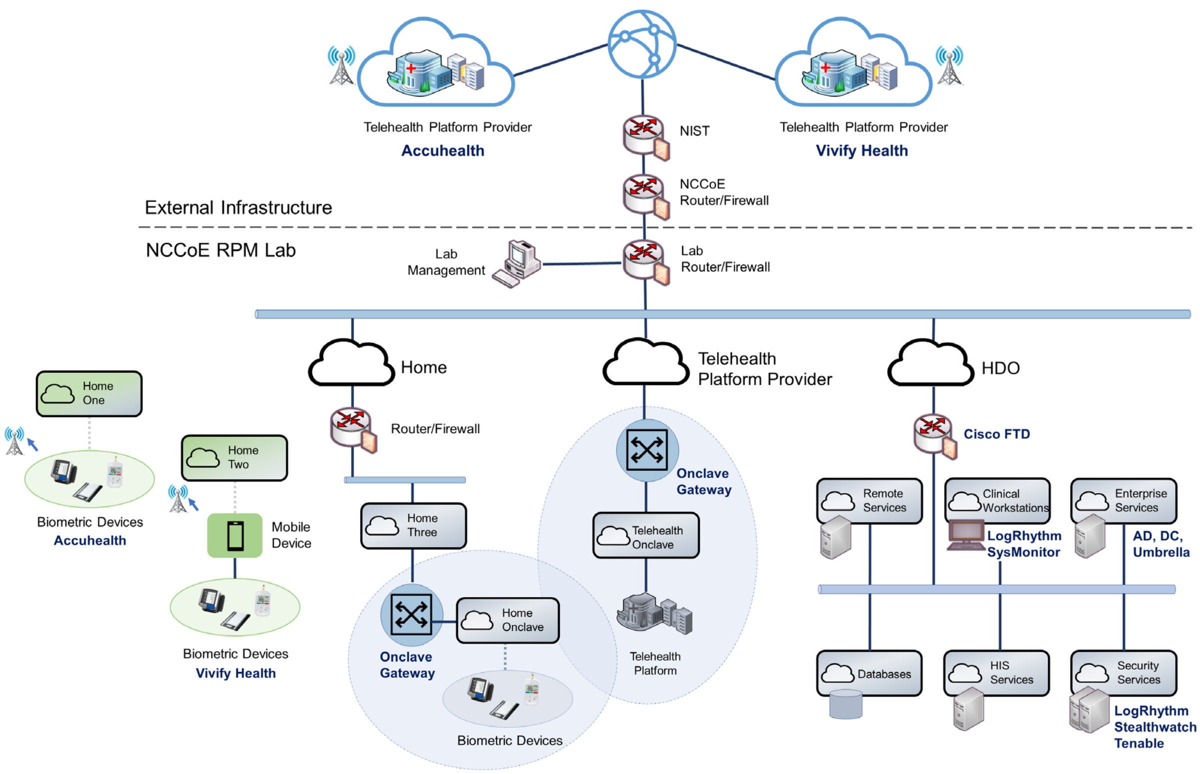
The following table presents typographic conventions used in this volume.

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 illustrates the reference network architecture implemented in the NCCoE virtual environment, initially presented in NIST SP 1800-30B, Section 4.5, Final Architecture. The HDO environment utilizes network segmenting similar to the architecture segmentation used in NIST SP 1800-24, *Securing Picture Archiving and Communication System (PACS)* [1]. The telehealth platform provider is a vendor-managed cloud environment that facilitates data transmissions and communications between the patient home and the HDO. Patient home environments have a minimalistic structure, which incorporates the devices provided by the telehealth platform provider.

Figure 1-1 Final Architecture



2 Product Installation Guides

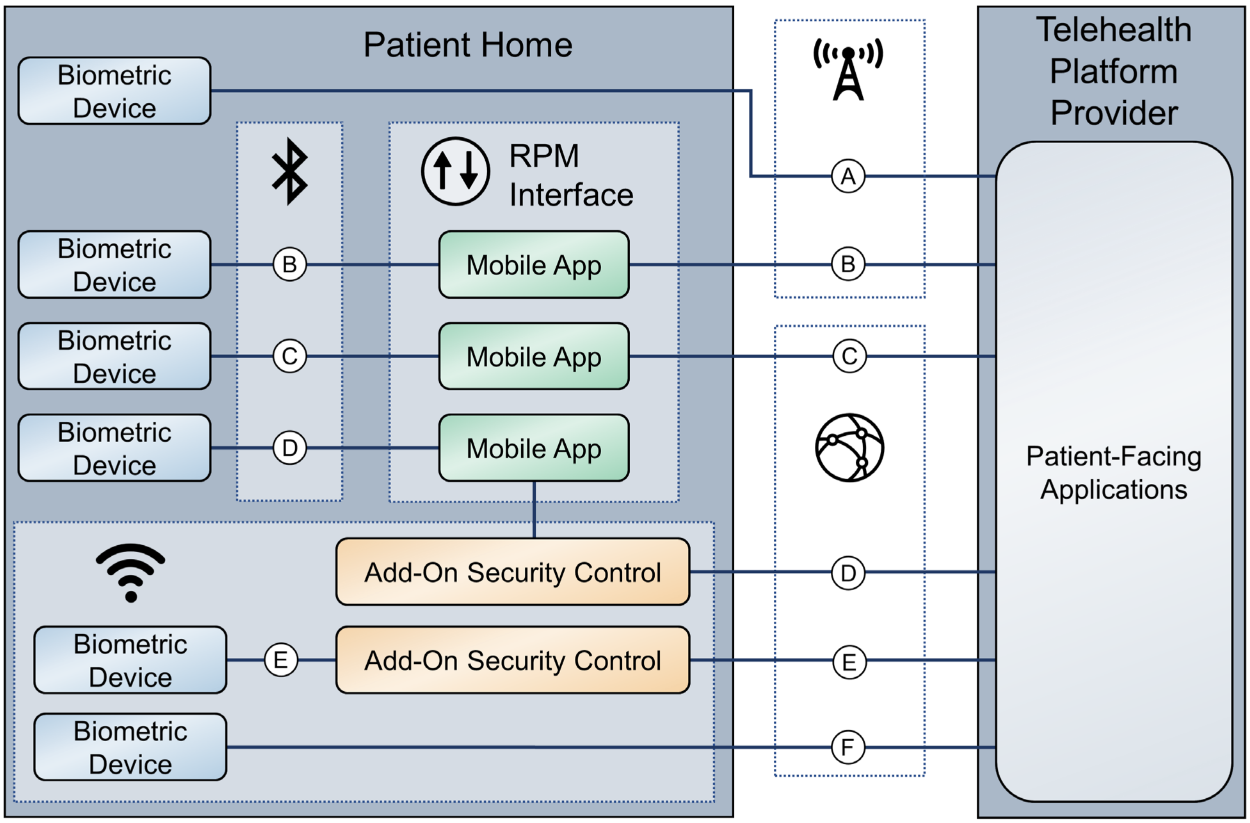
This section of the practice guide contains detailed instructions for installing and configuring all the products used to build an instance of the example solution. The project team implemented several capabilities that included deploying components received from telehealth platform providers and components that represent the HDO. The telehealth platform providers provisioned biometric devices that were deployed to a patient home environment. Within the HDO, the engineers deployed network infrastructure devices to implement network zoning and configure perimeter devices. The engineers also deployed security capabilities that supported vulnerability management and a security incident and event management (SIEM) tool. The following sections detail deployment and configuration of these components.

2.1 Telehealth Platform Provider

The project team implemented a model where an HDO partners with telehealth platform providers to enable RPM programs. Telehealth platform providers are third parties that, for this practice guide, configured, deployed, and managed biometric devices and mobile devices (e.g., tablets) that were sent to the patient home. The telehealth platform provider managed data communications over cellular and broadband where patients send biometric data to the telehealth platform provider. The telehealth platform provider implemented an application that allowed clinicians to access the biometric data.

The team collaborated with two independent telehealth platform providers. Collaborating with two unique platforms enabled the team to apply NIST's Cybersecurity Framework [2] to multiple telehealth platform implementations. One platform provides biomedical devices enabled with cellular data. These devices transmitted biometric data to the cloud-based telehealth platform. The second platform provider deployed biometric devices enabled with Bluetooth wireless technology. Biometric devices communicated with an interface device (i.e., a tablet). The telehealth platform provider configured the interface device by using a mobile device management solution, limiting the interface device's capabilities to those services required for RPM participation. The patient transmitted biometric data to the telehealth platform provider by using the interface device. The interface device transmitted data over cellular or broadband data communications. Both telehealth platform providers allowed HDOs to access patient data by using a web-based application. Both platforms implemented unique access control policies for access control, authentication, and authorization. Figure 2-1 depicts the different communication pathways tested in this practice guide. A detailed description of each communications pathway is provided in NIST SP 1800-30B, Section 4.2, High-Level Architecture Communications Pathways.

Figure 2-1 RPM Communications Paths



2.1.1 Accuhealth

Accuhealth provided biometric devices that included cellular data communication. Accuhealth also included a cloud-hosted application for HDOs to access patient-sent biometric data. Accuhealth provisioned biomedical devices with subscriber identity module (SIM) cards that enabled biomedical devices to transmit data via cellular data communications to the Accuhealth telehealth platform. Accuhealth stored patient-transmitted data in an application. Individuals assigned with clinician roles accessed transmitted data hosted in the Accuhealth application. The biomedical data displayed in the following screen captures are notional in nature and do not relate to an actual patient.

2.1.1.1 Patient Home–Communication Path A

This practice guide assumes that the HDO enrolls the patient in an RPM program. Clinicians would determine when a patient may be enrolled in the program appropriately, and conversations would occur about understanding the roles and responsibilities associated with participating in the RPM program. When clinicians enroll patients in the RPM program, the HDO would collaborate with Accuhealth.

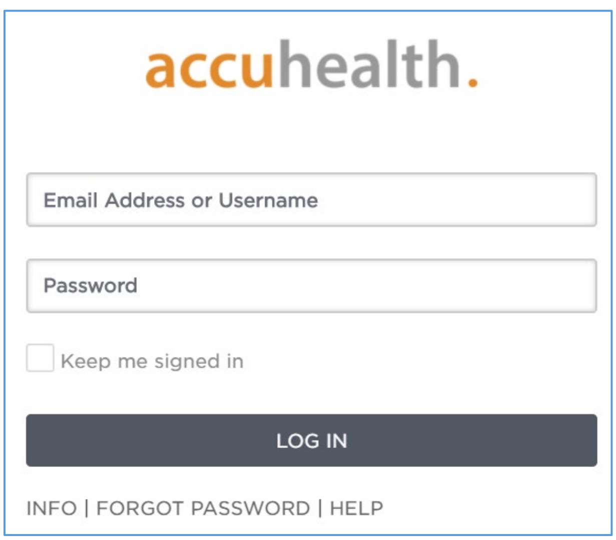
Accuhealth received patient contact information and configured biometric devices appropriate for the RPM program in which the patient was enrolled. Accuhealth configured biometric devices to communicate via cellular data, which is depicted as communication path A of Figure 2-1. Biometric devices, thus, were isolated from the patient home network environment. Accuhealth assured device configuration and asset management.

2.1.1.2 HDO

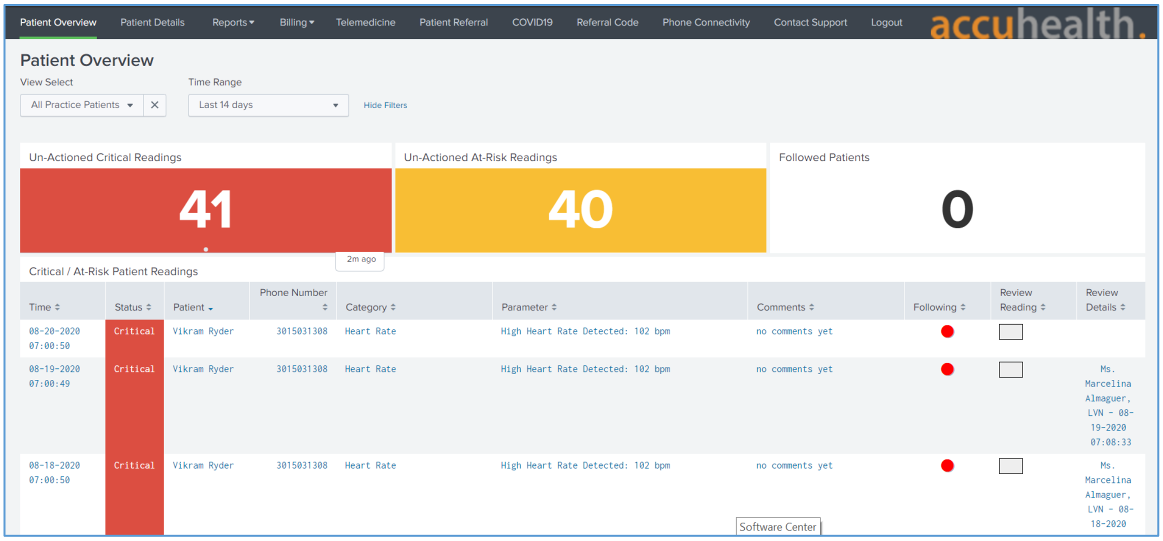
The Accuhealth solution includes installing an application within the HDO environment. Clinicians access a portal hosted by Accuhealth that allows a clinician to view patient biometric data. The application requires unique user accounts and role-based access control. System administrators create accounts and assign roles through an administrative console. Sessions from the clinician to the hosted application use encryption to ensure data-in-transit protection.

This section discusses the HDO application installation and configuration procedures.

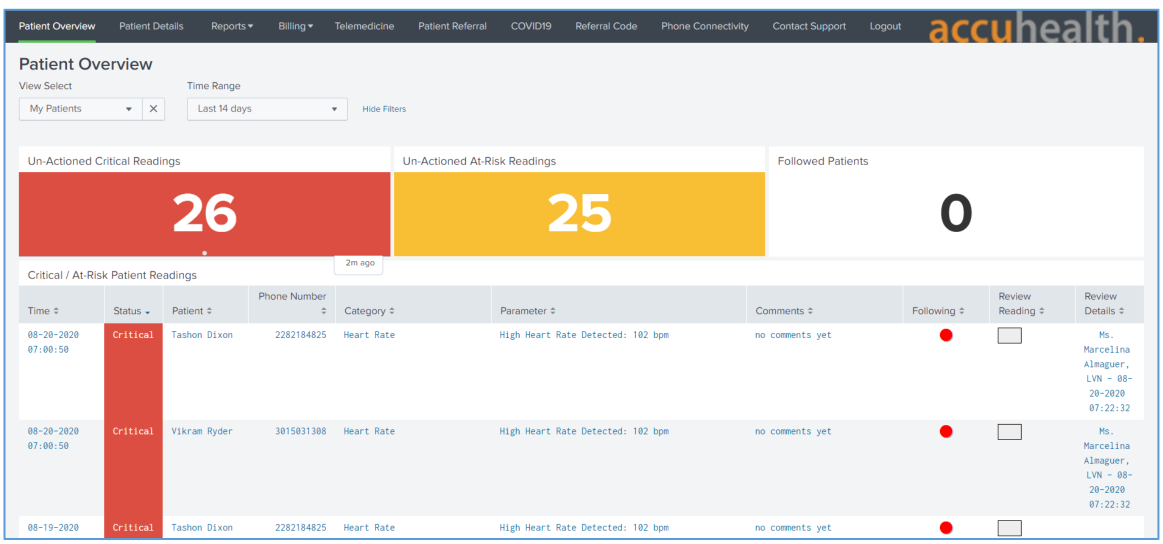
1. Access a device that has a web browser.
2. Navigate to Accuhealth login page, and provide a **Username** and **Password.** The following screenshots show a doctor's point of view in the platform.
3. Click **LOG IN.**



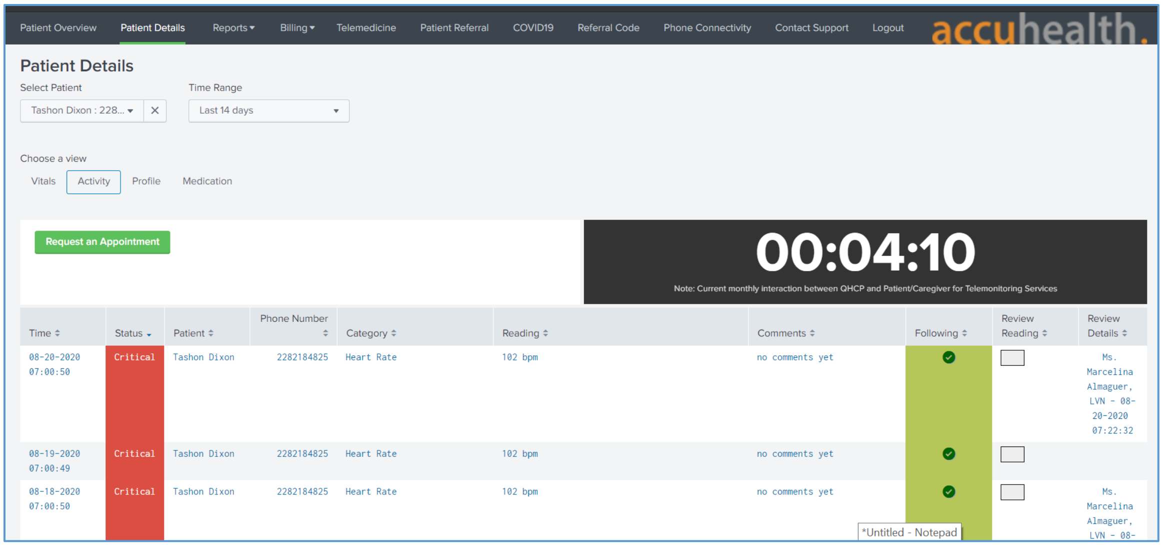
After logging in, the **Patient Overview** screen displays.



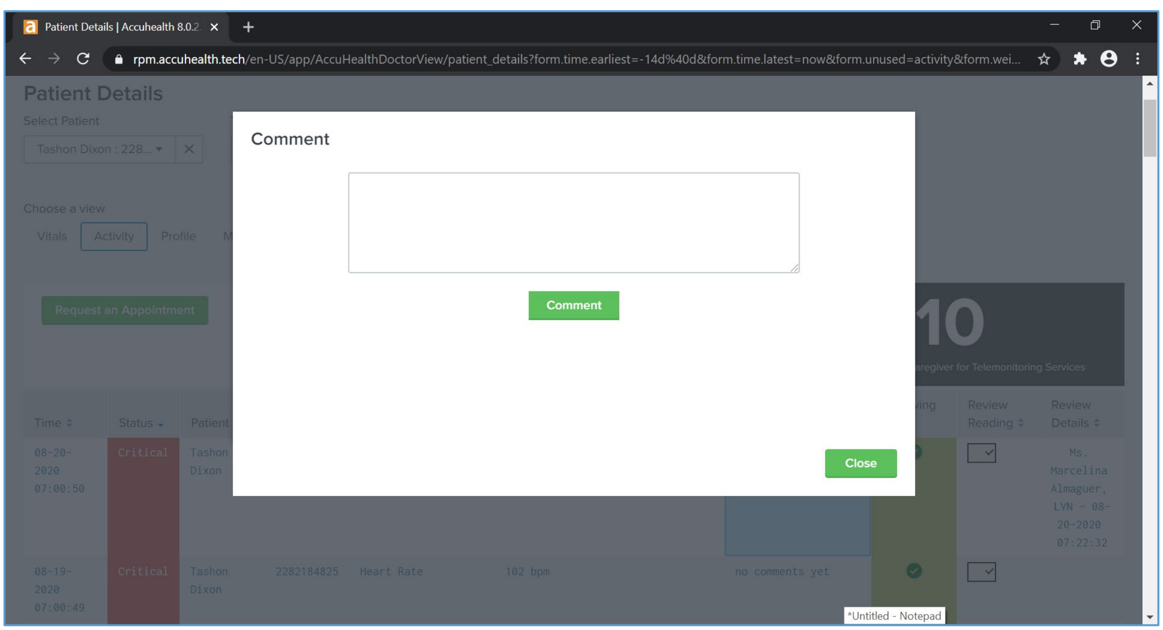
4. To view patients associated with the account used to log in, navigate to the **View Select** drop-down list in the top left corner of the screen, and select **My Patients.**



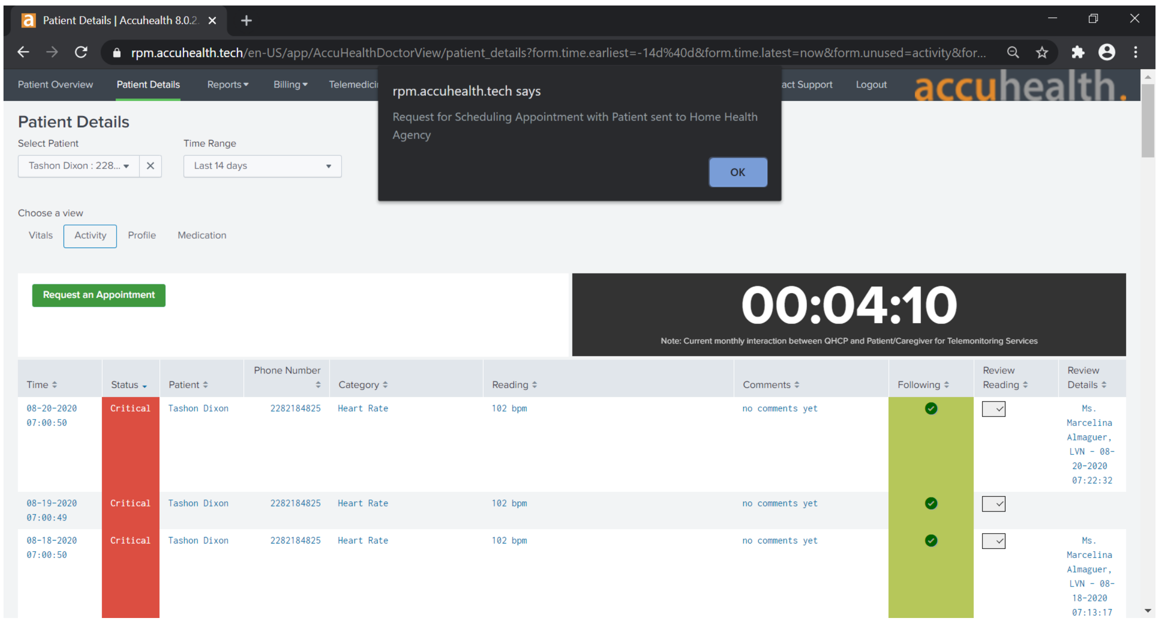
5. Click a **Patient** to display the **Patient Details** page, which displays all patient biomedical readings.



6. To leave a comment on a reading, click **no comments yet** under the **Comments** column on the row of the reading to which the comment refers.
7. A **Comment** screen displays that allows free text input.
8. Click **Comment.**
9. Click **Close.**



10. To have a call with a patient, click **Request an Appointment** in the top left of the **Patient Details** page.
11. A notification box displays, asking if the Home Health Agency needs to schedule an appointment with the patient.
12. Click **OK.**



2.1.2 Vivify Health

Vivify provided biometric and interface devices (i.e., Vivify provisioned a tablet device) and a cloud-hosted platform. Vivify enabled biometric devices with Bluetooth communication and provisioned interface devices with SIM cards. Individuals provisioned with patient roles used the interface device to retrieve data from the biometric devices via Bluetooth. Individuals acting as patients then used the interface device to transmit data to Vivify by using cellular data. Vivify's application presented the received data. Individuals provisioned with clinician roles accessed the patient-sent data stored in the Vivify application via a web interface.

2.1.2.1 Patient Home–Communication Path B

This practice guide assumes that the HDO enrolls the patient in an RPM program. Clinicians would determine when a patient may be enrolled in the program appropriately, and conversations then occur about understanding the roles and responsibilities associated with participating in the RPM program. When clinicians enroll patients in the RPM program, the HDO would collaborate with Vivify. Vivify received patient contact information and configured biometric devices and an interface device (i.e., tablet) appropriate for the RPM program in which the patient was enrolled. These devices were configured to transmit data via cellular through the interface device, which is depicted as communication path B in Figure 2-1. Vivify assured device configuration and asset management.

2.1.2.2 Patient Home–Communication Paths C and D

To evaluate communication path C in Figure 2-1, the project team implemented another instance of the Vivify Pathways Care Team Portal in a simulated cloud environment. The simulated cloud environment represented how a telehealth platform provider may operate; however, it does not reflect how any specific telehealth platform provider hosts its components. The simulated cloud environment deployed Vivify-provided software, but note that the simulated cloud environment does not represent how Vivify implements its service offering. The NCCoE implemented the simulated cloud environment as a test case where telehealth platforms may incorporate layer 2 over layer 3 solutions as part of their architecture. A Vivify Pathways Home kit was hosted in a patient home network, which included peripherals as well as an RPM interface. Engineers connected the RPM interface (mobile device) to the patient home network to enable broadband communications with the new simulated cloud instance. The RPM interface collected patient data from the provided peripherals via Bluetooth and then transmitted this data to the simulated cloud environment through the broadband connection.

After implementing communication path C and the Onclave Network Solution, the RPM interface connected to an add-on security control, Onclave Home Gateway, inside the patient home environment. Once the RPM interface was connected to the Onclave Home Gateway, patient data were transmitted to the simulated cloud environment through the Onclave Telehealth Gateway. These connections enabled the project team to implement communication path D as depicted in Figure 2-1. Details on how engineers installed and configured Onclave tools are described in section 2.2.4.1, Onclave SecureIoT.

2.1.2.3 Telehealth Platform–Communication Paths C and D

For communication paths C and D, a simulated cloud environment was created to represent a telehealth platform provider that supports broadband-capable biometric devices. A sample Vivify Pathways Care Team Portal was obtained to demonstrate how patient data could be transmitted via broadband communications. Practitioners should note, however, that Vivify as an entity may not support this use case. Vivify engineers facilitated deploying the Vivify Pathways Care Team Portal as representative of how a telehealth platform provider may support the communications pathway. Communication paths A and B used telehealth platform providers that were located outside the NCCoE lab, and data were transmitted via cellular communications.

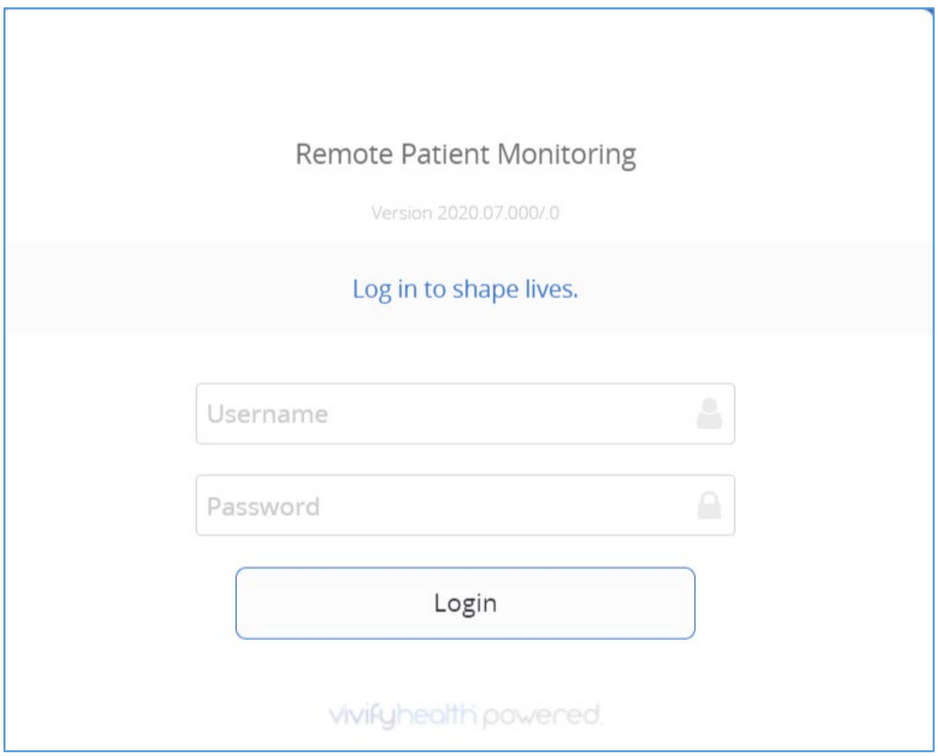
Communication path D required more add-on security controls to be configured in the virtual cloud environment. For this communication pathway, the representative Vivify Pathways Care Team Portal was connected to an Onclave Telehealth Gateway. This gateway accepted data transmissions from the RPM interface connected to the Onclave Home Gateway housed in the patient home environment.

2.1.2.4 HDO

Using a web browser interface, clinicians access a portal hosted by Vivify that allows access to view patient biometric data. Portal interaction requires unique user accounts and role-based access control. System administrators create accounts and assign roles through an administrative console. Sessions from the clinician to the hosted application use encryption to ensure data-in-transit protection.

This section discusses the HDO application installation and configuration procedures.

1. Access a device that has a web browser.
2. Navigate to https://<vivifyhealth site>/CaregiverPortal/Login and give the **Username** and **Password** of the administrative account provided by Vivify.
3. Click **Login.**



4. Navigate to the **Care Team** menu item on the left-hand side of the screen.

   Click **+ New User.**
5. In the **New User** screen, provide the following information:
   a. **First Name:** Test

    b. **Last Name:** Clinician
    c. **User Name:** TClinician1
    d. **Password:** **********
    e. **Confirm Password:** **********
    f. **Facilities:** Vivify General
    g. **Sites:** Default
    h. **Roles:** Clinical Level 1, Clinical Level 2
    i. **Email Address:** **********
    j. **Mobile Phone:** *********
6. Click **Save Changes.**
7. Navigate to **Patients** in the left-hand menu bar.
8. Select the **NCCoE, Patient** record.
9. Under **Care Team,** click the **notepad and pencil** in the top right of the box.
10. In the **Care Team** window, select **Clinician, Test** and click **Ok.**
11. Log out of the platform.
12. Log in to the platform by using the **Test Clinician** credentials, and click **Login.**
13. Click the **NCCoE, Patient** record.
14. Navigate to the **Monitoring** tab to review patient readings.
15. Based on the patient's data, the clinician needs to consult the patient.
16. Click the ellipsis in the **NCCoE, Patient** menu above the green counter.
17. Select **Call Patient.**
18. In the **Respond to Call Request** screen, select **Phone Call Now.**
19. After the consultation, record the action items performed during the call.
20. In the **Monitoring** window, click **Accept All** under the **Alerts** tab to record intervention steps.
21. In the **Select Intervention** window, select the steps performed to address any patient alerts.
22. Click **Accept.**

23. Navigate to **Notes** to review recorded interventions or add other clinical notes.

2.2 Security Capabilities

The following instruction and configuration steps depict how the NCCoE engineers along with project collaborators implemented provided cybersecurity tools to achieve the desired security capabilities identified in NIST SP 1800-30B, Section 4.4, Security Capabilities.

2.2.1 Risk Assessment Controls

Risk assessment controls align with the NIST Cybersecurity Framework's ID.RA category. For this practice guide, the Tenable.sc solution was implemented as a component in an HDO's risk assessment program. While Tenable.sc includes a broad functionality set, the project team leveraged Tenable.sc's vulnerability scanning and management capabilities.

2.2.1.1 Tenable.sc

Tenable.sc is a vulnerability management solution. Tenable.sc includes vulnerability scanning and configuration checking, which displays information through a dashboard graphical user interface (GUI). Tenable.sc's dashboard includes vulnerability scoring, enabling engineers to prioritize patching and remediation. The engineers used Tenable.sc to manage a Nessus scanner, which performed vulnerability scanning against HDO domain-hosted devices. While the Tenable.sc solution includes configuration-checking functionality, this practice guide uses the solution for vulnerability management.

System Requirements

Central Processing Unit (CPU): 4

Memory: 8 gigabytes (GB)

Storage: 250 GB

Operating System: CentOS 7

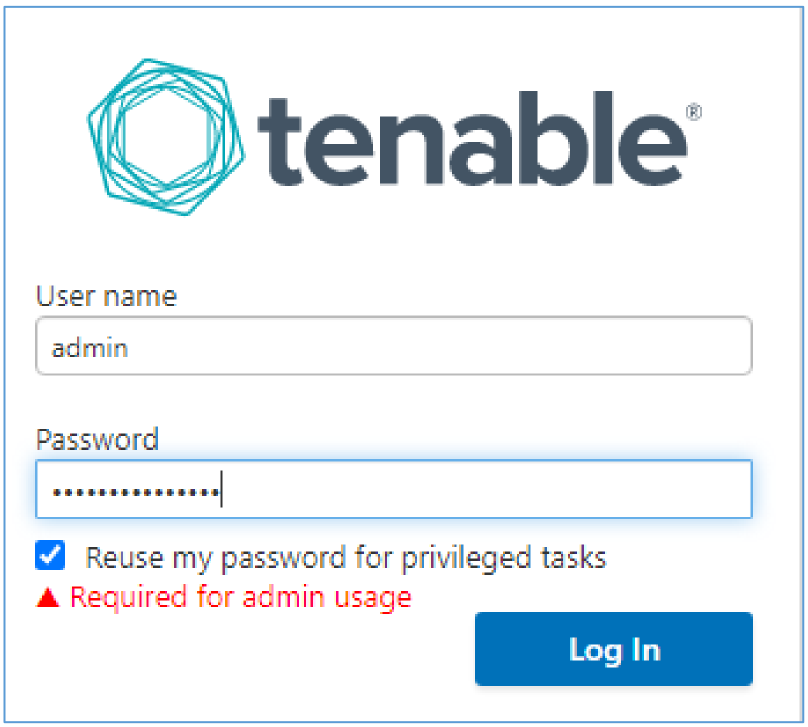
Network Adapter: virtual local area network (VLAN) 1348

Tenable.sc Installation

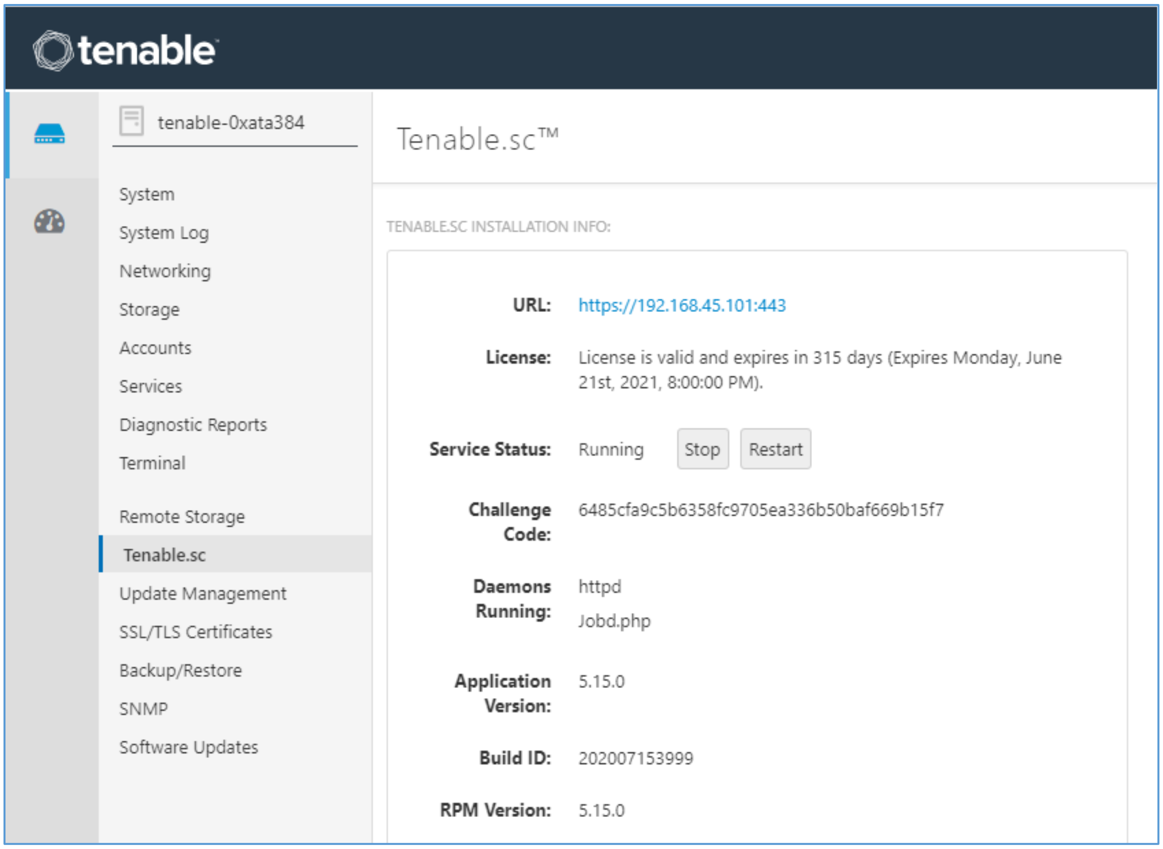
This section discusses installation of the Tenable.sc vulnerability management solution.

1. Import the Tenable.sc **open virtual appliance or appliance (OVA) file** to the virtual environment.
2. Assign the virtual machine (VM) to **VLAN 1348.**
3. Start the VM, and document the associated **internet protocol (IP) address.**
4. Open a web browser that can talk to VLAN 1348, and navigate to the VM's **IP address.**

5. For the first login, use **wizard** as the **Username** and **admin** for the **Password.**
6. Tenable.sc prompts a pop-up window for creating a new **admin username** and **password.**
7. Repeat step 5 using the new username and password.
    a. **Username:** admin
    b. **Password:** **********
    c. Check the box beside **Reuse my password for privileged tasks.**

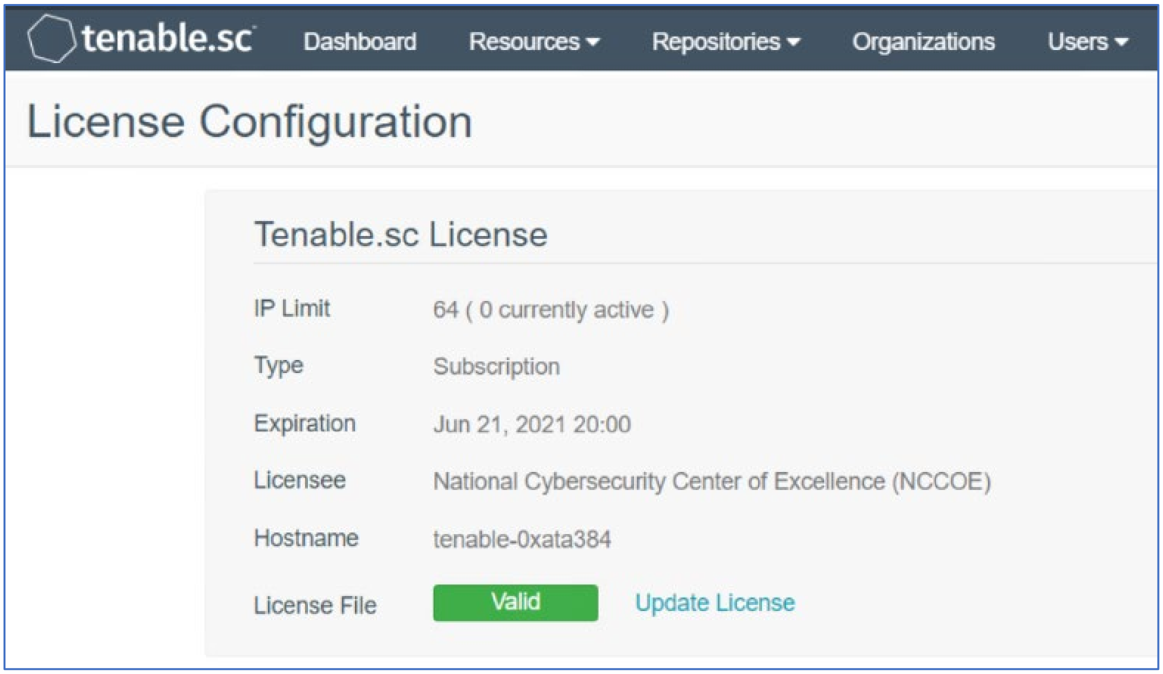


8. After logging in, the Tenable Management Console page displays.
9. Click the **Tenable.sc** menu option on the left side of the screen.
10. To access Tenable.sc, click the **IP address** next to the uniform resource locator (URL) field.



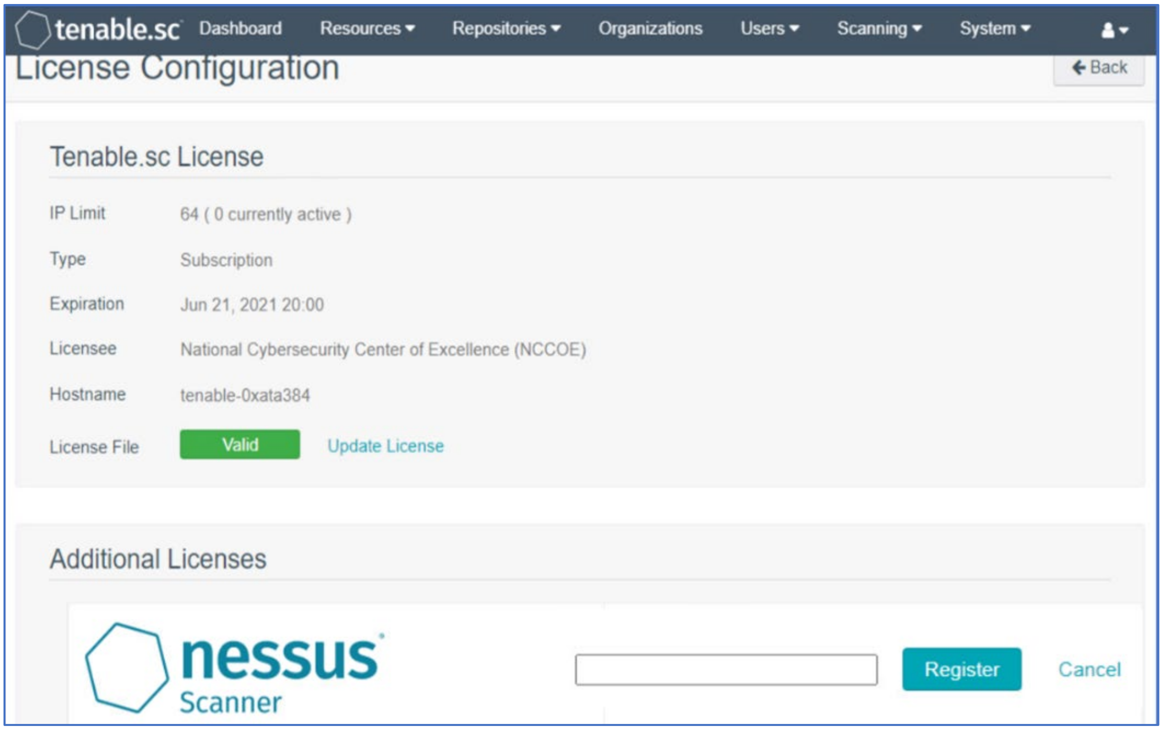
11. Log in to Tenable.sc by using the credentials created in previous steps, and click **Sign In.**
    a. **Username:** admin
    b. **Password:** **********

12. After signing in, Tenable.sc's web page displays.
13. Navigate to the **System** drop-down list in the menu ribbon.
14. Click **Configuration.**
15. Under Tenable.sc License, click **Upload** next to License File.
16. Navigate to the storage location of the Tenable.sc license key obtained from a Tenable representative, and select the **key file.**
17. Click **OK.**
18. Click **Validate.**
19. When Tenable.sc accepts the key, a green Valid label will display next to License File.



20. Under Additional Licenses, input the Nessus **license key** provided by a Tenable representative next to Nessus Scanner.

21. Click **Register.**

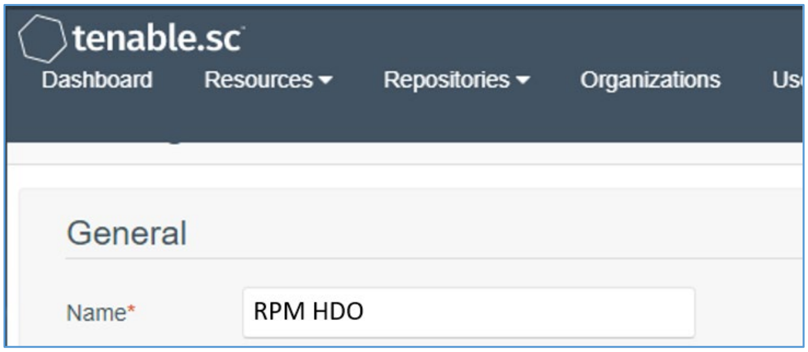


<u>Tenable.sc Configuration</u>

The project team leveraged support from Tenable engineers. Collectively, engineers installed Tenable.sc and validated license keys for Tenable.sc and Nessus. Engineers created Organization, Repository, User, Scanner, and Scan Zones instances for the HDO lab environment. The configuration steps are below.

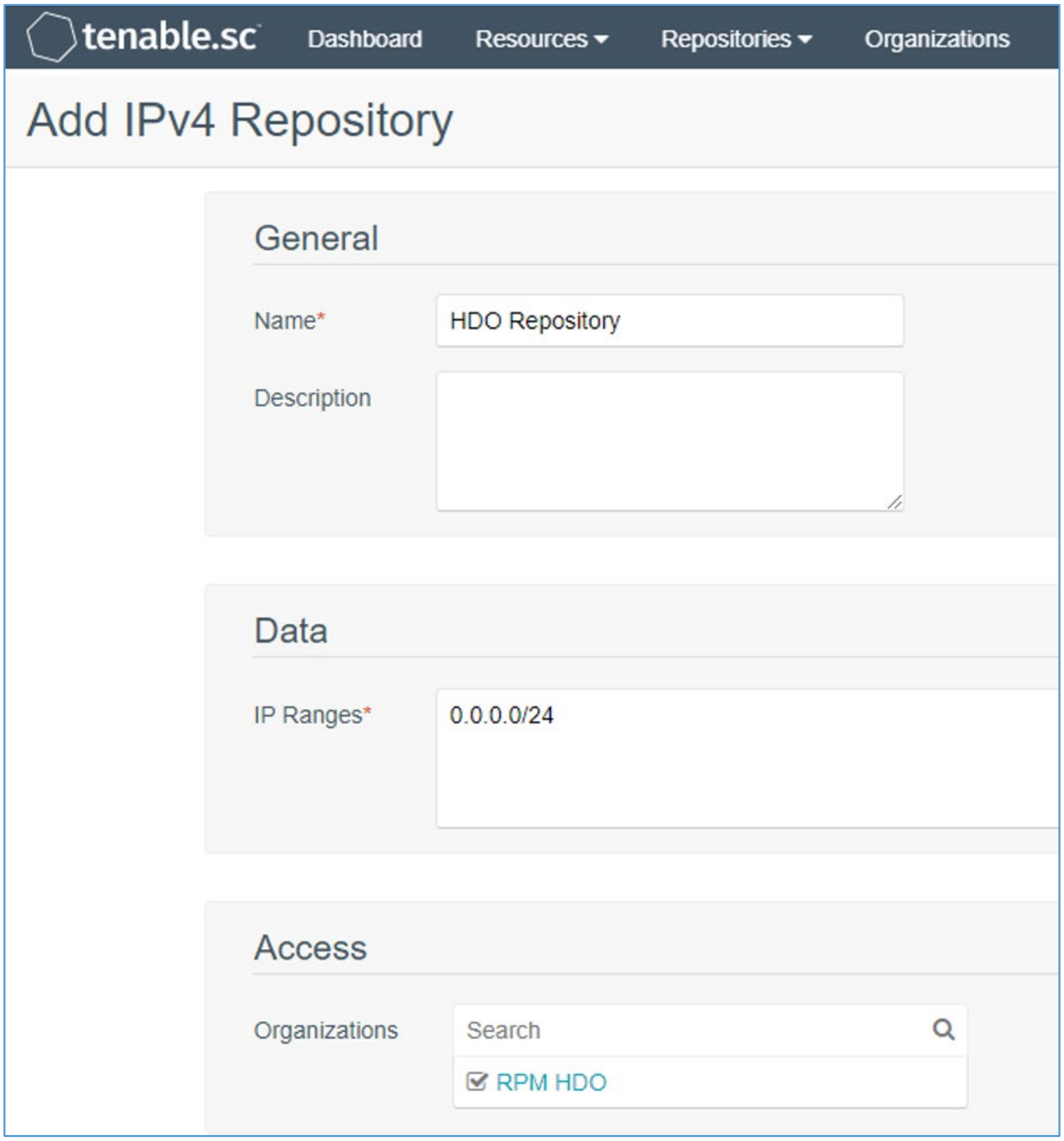
<u>Add an Organization</u>

1. Navigate to **Organizations** in the menu ribbon.
2. Click **+Add** in the top right corner of the screen**.** An **Add Organization** page will appear.
3. Name the Organization **RPM HDO** and leave the remaining fields as their default values.
4. Click **Submit.**



Add a Repository

1. Navigate to the **Repositories** drop-down list in the menu ribbon.
2. Click **+Add** in the top right corner of the screen. An **Add Repository** screen displays.
3. Under Local, click **IPv4.** An **Add IPv4 Repository** page displays. Provide the following information:
    a. **Name:** HDO Repository
    b. **IP Ranges:** 0.0.0.0/24
    c. **Organizations:** RPM HDO
4. Click **Submit.**



456 <u>Add a User</u>

457 1. Navigate to the **Users** drop-down list in the menu ribbon.

458 2. Select **Users.**

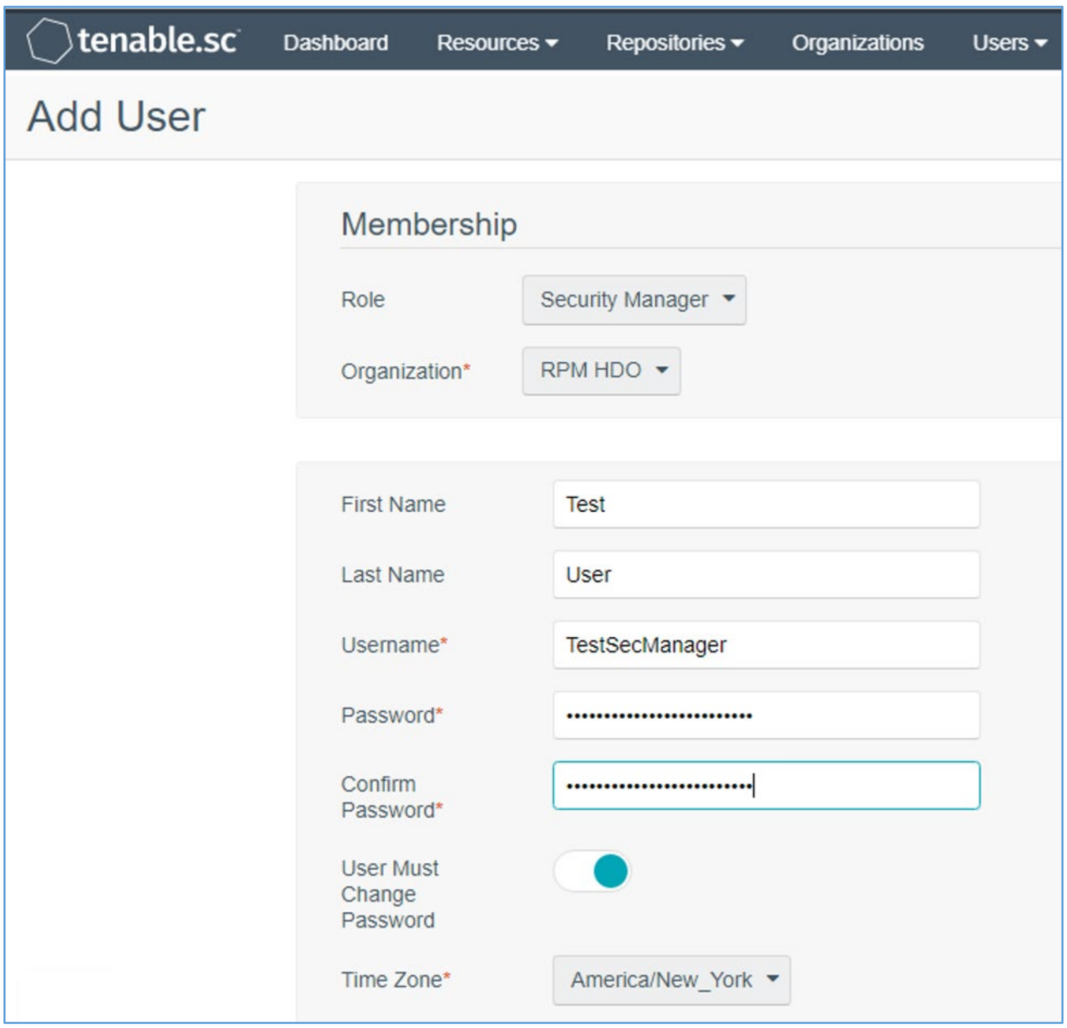
459 3. Click **+Add** in the top right corner. An **Add User** page displays. Provide the following information:

460 a. **Role:** Security Manager

461 b. **Organization:** RPM HDO

  c. **First Name:** Test
  d. **Last Name:** User
  e. **Username:** TestSecManager
  f. **Password:** **********
  g. **Confirm Password:** **********
  h. Enable **User Must Change Password.**
  i. **Time Zone:** America/New York

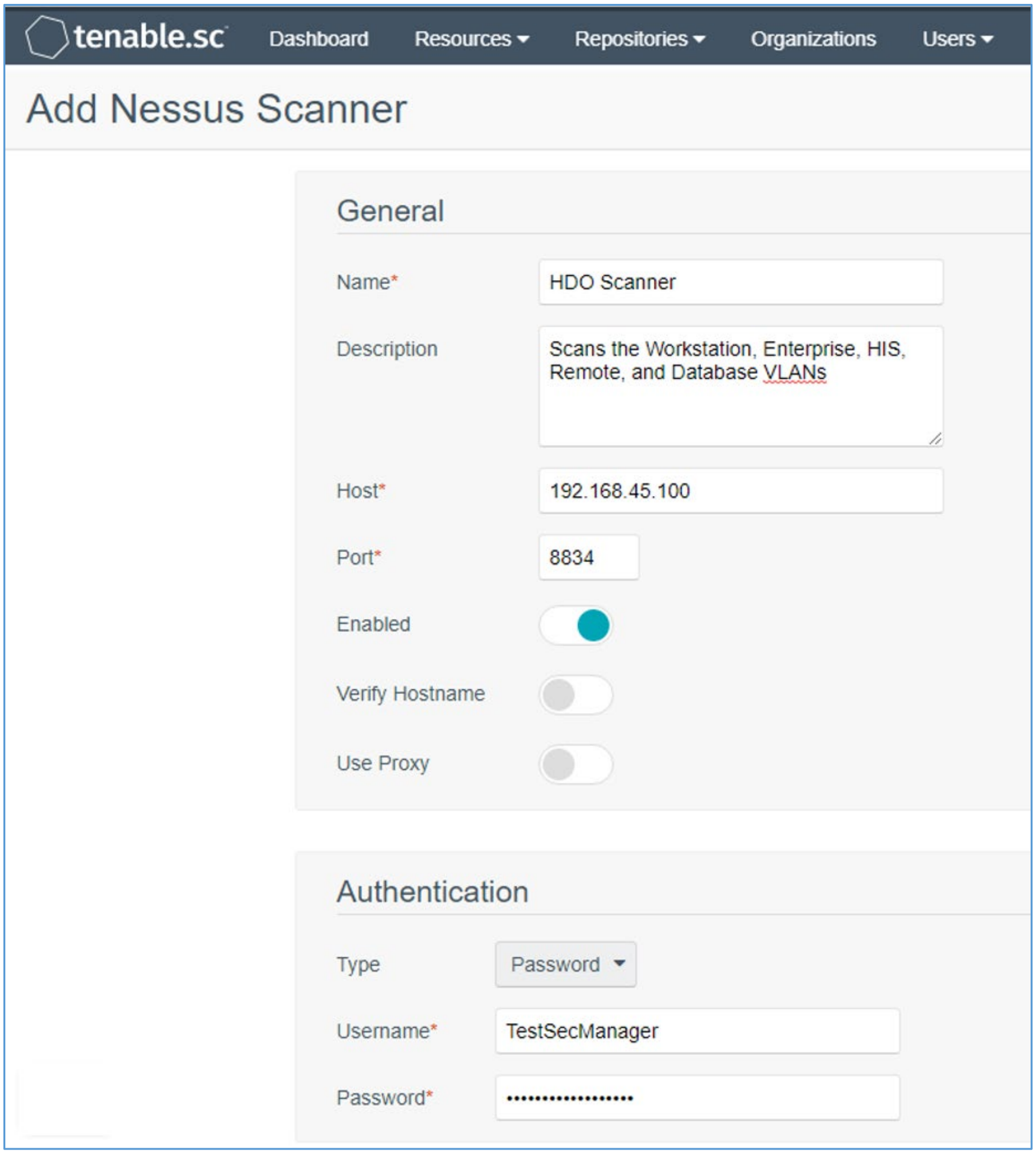
4. Click **Submit.**



For the lab deployment of Tenable.sc, the engineers instantiated one Nessus scanner in the Security Services subnet that has access to every subnet in the HDO environment.

Add a Scanner

1. Navigate to the **Resources** drop-down list in the menu ribbon.
2. Select **Nessus Scanners.**
3. Click **+Add** in the top right corner**.** An **Add Nessus Scanner** page displays. Fill in the following information:
    a. **Name:** HDO Scanner
    b. **Description:** Scans the Workstation, Enterprise, HIS, Remote, and Database VLANs
    c. **Host:** 192.168.45.100
    d. **Port:** 8834
    e. **Enabled:** on
    f. **Type:** Password
    g. **Username:** TestSecManager
    h. **Password:** **********
4. Click **Submit.**



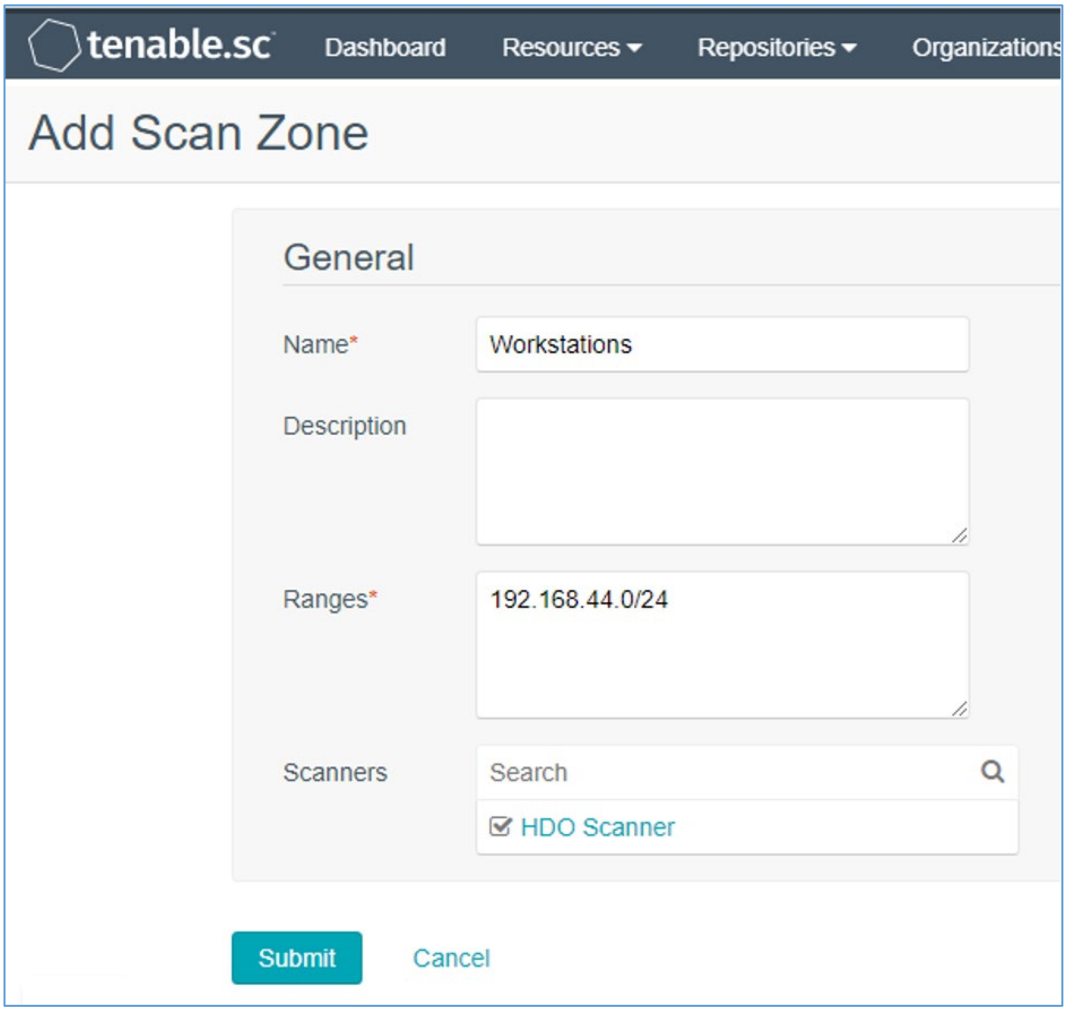
The engineers created a scan zone for each subnet established on the HDO network. The process to create a scan zone is the same for each subnet aside from the IP address range.

As an example, the steps for creating the Workstation scan zone are as follows:

<u>Add a Scan Zone</u>

1. Navigate to the **Resources** drop-down list in the menu ribbon.
2. Select **Scan Zones.**

3. Click **+Add.** An **Add Scan Zone** page will appear. Provide the following information:
    a. **Name:** Workstations
    b. **Ranges:** 192.168.44.0/24
    c. **Scanners:** HDO Scanner
4. Click **Submit.**

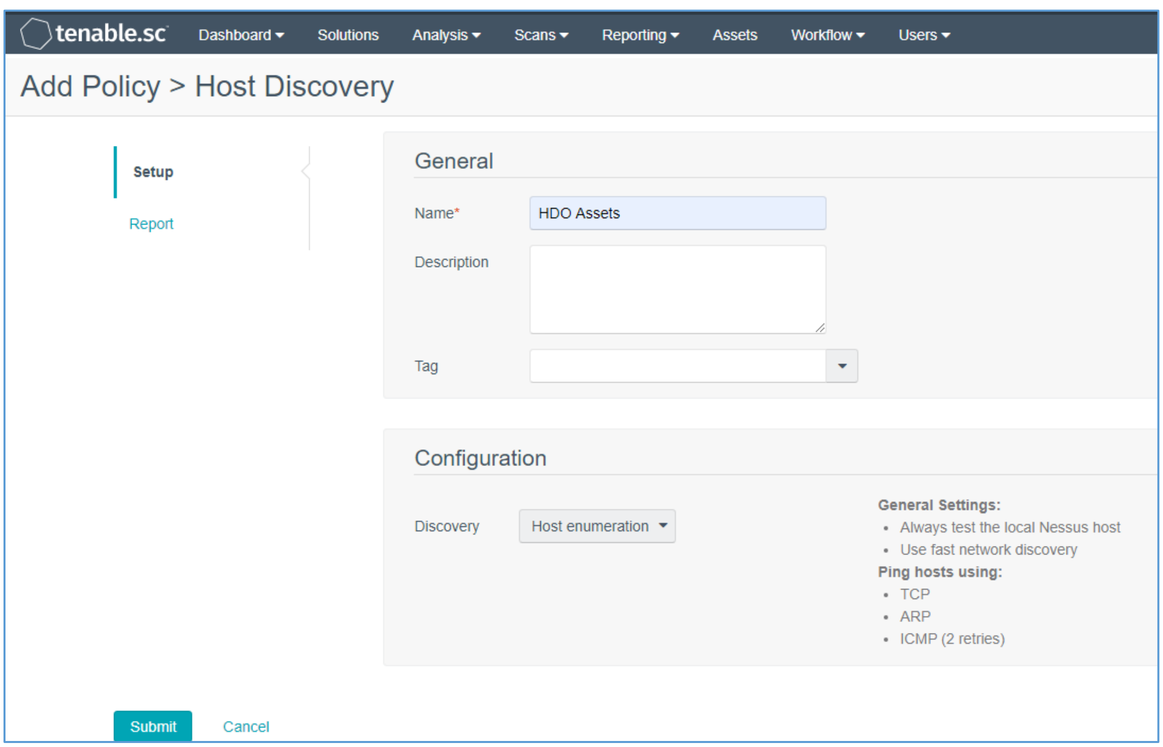


Repeat steps in Add a Scan Zone section for each VLAN.

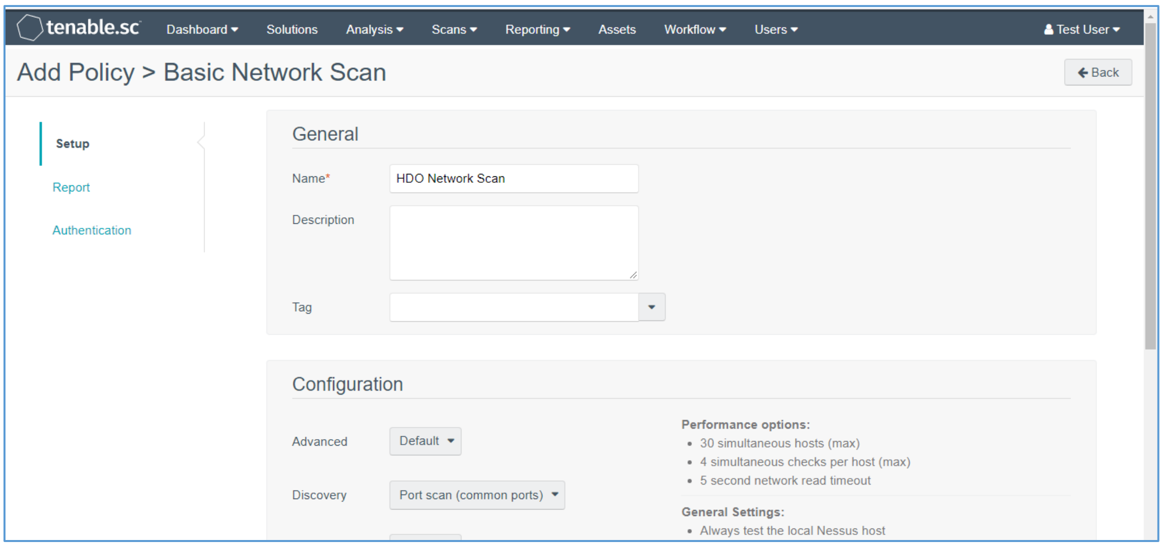
To fulfil the identified NIST Cybersecurity Framework Subcategory requirements, the engineers utilized Tenable's host discovery and vulnerability scanning capabilities. The first goal was to identify the hosts on each of the HDO VLANs. Once Tenable identifies the assets, Tenable.sc executes a basic network scan to identify any vulnerabilities on these assets.

<u>Create Scan Policies</u>

1. Engineers created a **Security Manager** account in a previous step when adding users. Log in to Tenable.sc by using the **Security Manager** account.
2. Navigate to the **Scans** drop-down list in the menu ribbon.
3. Select **Policies.**
4. Click **+Add** in the top right corner.
5. Click **Host Discovery** in the **Add Policy** page. An **Add Policy > Host Discovery** page will appear. Provide the following information:
    a. **Name:** HDO Assets
    b. **Discovery:** Host enumeration
    c. Leave the remaining options as their default values.
6. Click **Submit.**



7. Click **+Add** in the top right corner.
8. Click **Basic Network Scan** in the **Add Policy** page. An **Add Policy > Basic Network Scan** page displays.
9. Name the scan **HDO Network Scan** and leave the remaining options to their default settings.
10. Click **Submit.**



Create Active Scans

1. Navigate to the **Scans** drop-down list in the menu ribbon.
2. Select **Active Scans.**
3. Click **+Add** in the top right corner. An **Add Active Scan** page will appear. Provide the following information for General and Target Type sections.

   General

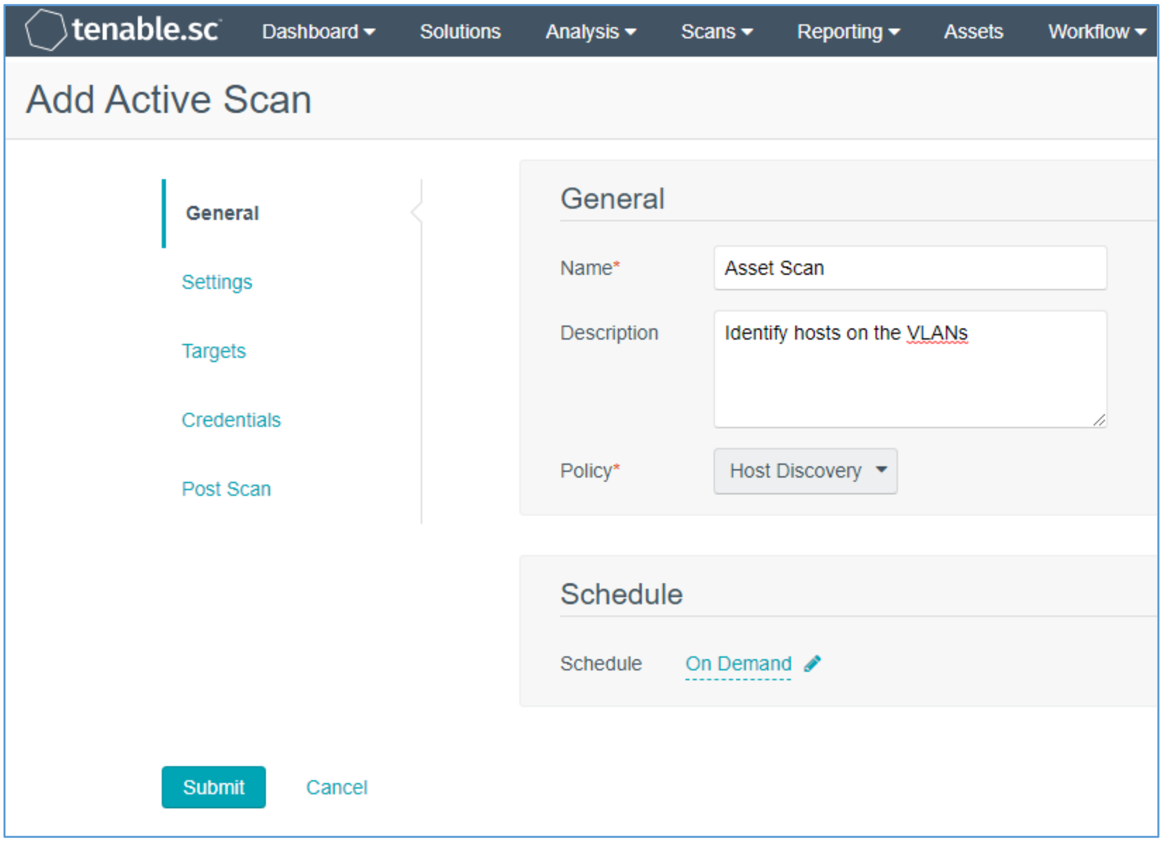
   a. **Name:** Asset Scan
   b. **Description:** Identify hosts on the VLANs
   c. **Policy:** Host Discovery

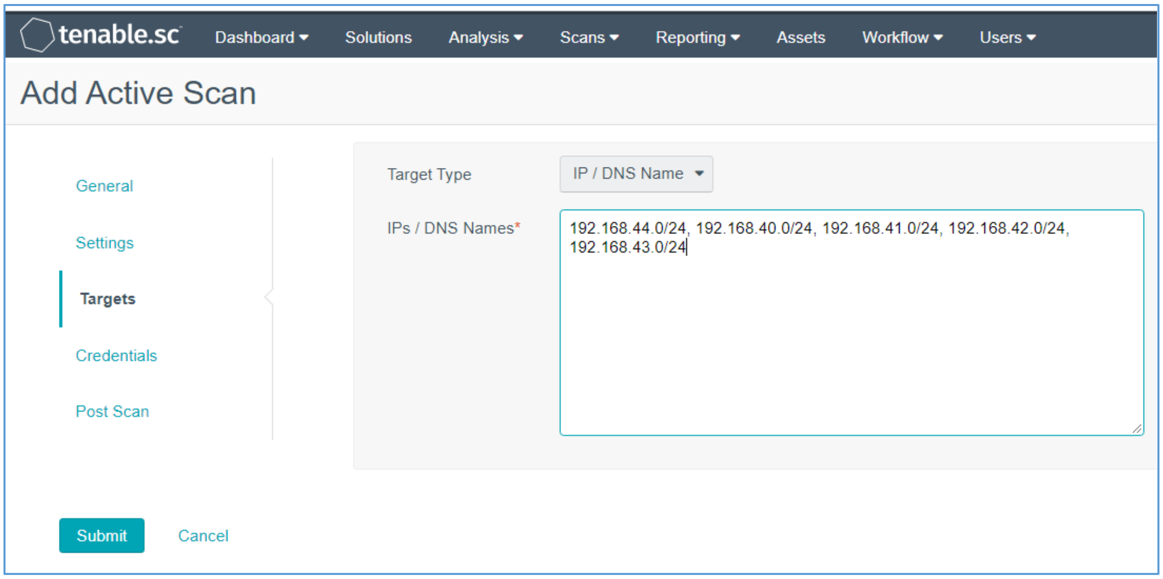
   Targets

   a. **Target Type:** IP/DNS Name

b. **IPs/DNS Names:** 192.168.44.0/24, 192.168.40.0/24, 192.168.41.0/24, 192.168.42.0/24, 192.168.43.0/24

4. Click **Submit.**





Repeat steps in Create Active Scans section for the Basic Network Scan policy. Keep the same value as defined for Active Scan except the following:

a. Name the scan **HDO Network Scan.**

b. Set Policy to **HDO Network Scan.**

After the engineers created and correlated the Policies and Active Scans to each other, they executed the scans.

<u>Execute Active Scans</u>

1. Navigate to the **Scans** drop-down list in the menu ribbon.
2. Select **Active Scans.**
3. Next to **HDO Asset Scan** click **▶.**
4. Navigate to the **Scan Results** menu option shown at the top of the screen under the menu ribbon to see the status of the scan.
5. Click **HDO Asset Scan** to see the scan results.
6. Repeat the above steps for **HDO Network Scan.**

<u>View Active Scan Results in the Dashboard</u>

1. Navigate to the **Dashboard** drop-down list in the menu ribbon.
2. Select **Dashboard.**

3. In the top right, click **Switch Dashboard.**
4. Click **Vulnerability Overview.** A screen will appear that displays a graphical representation of the vulnerability results gathered during the HDO Host Scan and HDO Network Scan.

2.2.1.2 Nessus

Nessus is a vulnerability scanning engine that evaluates a host's operating system and configuration to determine the presence of exploitable vulnerabilities. This project uses one Nessus scanner to scan each VLAN created in the HDO environment to identify hosts on each VLAN and the vulnerabilities associated with those hosts. Nessus sends the results back to Tenable.sc, which graphically represents the results in dashboards.

System Requirements

CPU: 4

Memory: 8 GB

Storage: 82 GB

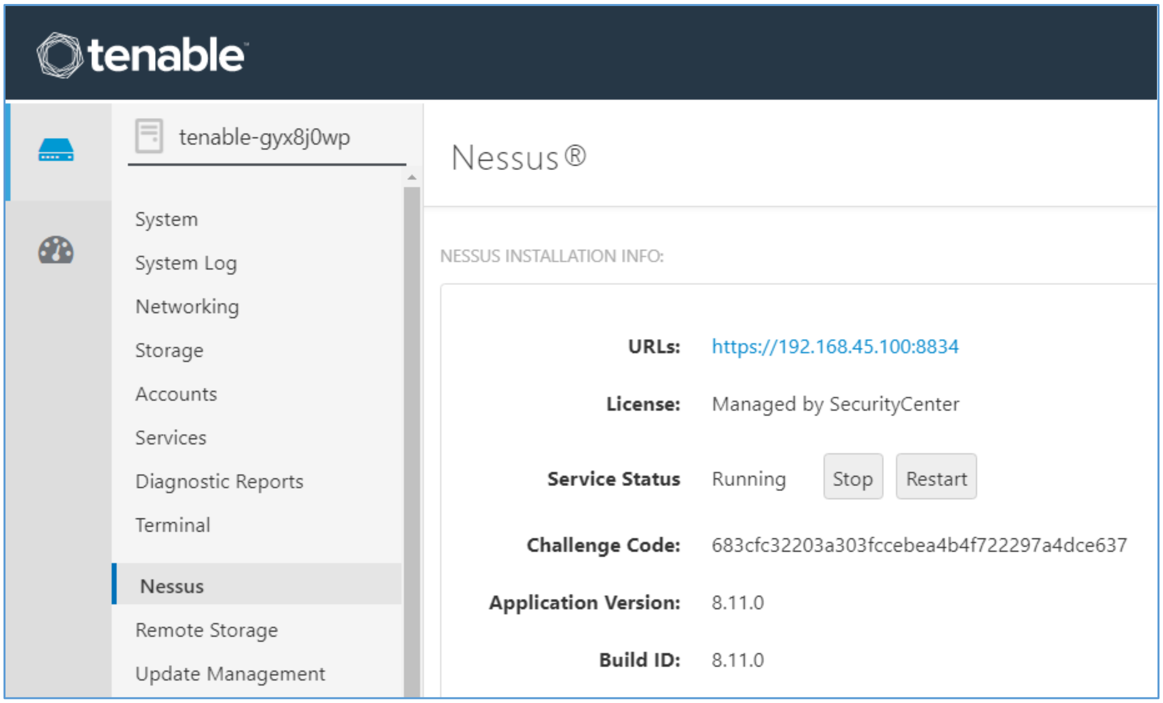
Operating System: CentOS 7

Network Adapter: VLAN 1348

Nessus Installation

1. Import the **OVA file** to the virtual lab environment.
2. Assign the VM to **VLAN 1348.**
3. Start the VM, and document the associated **IP address.**
4. Open a web browser that can talk to VLAN 1348, and navigate to the VM's **IP address.**
5. Log in using **wizard** as the **Username** and **admin** for the **Password.**
6. Create a new **admin username** and **password.**
7. Log in using the new username and password.
    a. **Username:** admin
    b. **Password:** **********
    c. Enable **Reuse my password for privileged tasks.**

8. Click **Tenable.sc** on the left side of the screen.
9. To access Tenable.sc, click the **IP address** next to the URL field.



Nessus Configuration

The engineers utilized Tenable.sc to manage Nessus. To configure Nessus as managed by Tenable.sc, follow Tenable's Managed by Tenable.sc guide [3].

2.2.2 Identity Management, Authentication, and Access Control

Identity management, authentication, and access control align with the NIST Cybersecurity Framework PR.AC control. The engineers implemented capabilities in the HDO to address this control category. First, they implemented Microsoft Active Directory (AD), then installed a domain controller to establish an HDO domain. Next, the engineers implemented Cisco Firepower as part of its network core infrastructure. They used Cisco Firepower to build VLANs that aligned to network zones. Cisco Firepower also was configured to provide other network services. Details on installation are included in the following sections.

2.2.2.1 Domain Controller

The engineers installed a Windows Server domain controller within the HDO to manage AD and local domain name service (DNS) for the enterprise. The following section details how the engineers installed the services.

Domain Controller Appliance Information

CPU: 4

Random Access Memory (RAM): 8 GB

Storage: 120 GB (Thin Provision)

Network Adapter 1: VLAN 1327

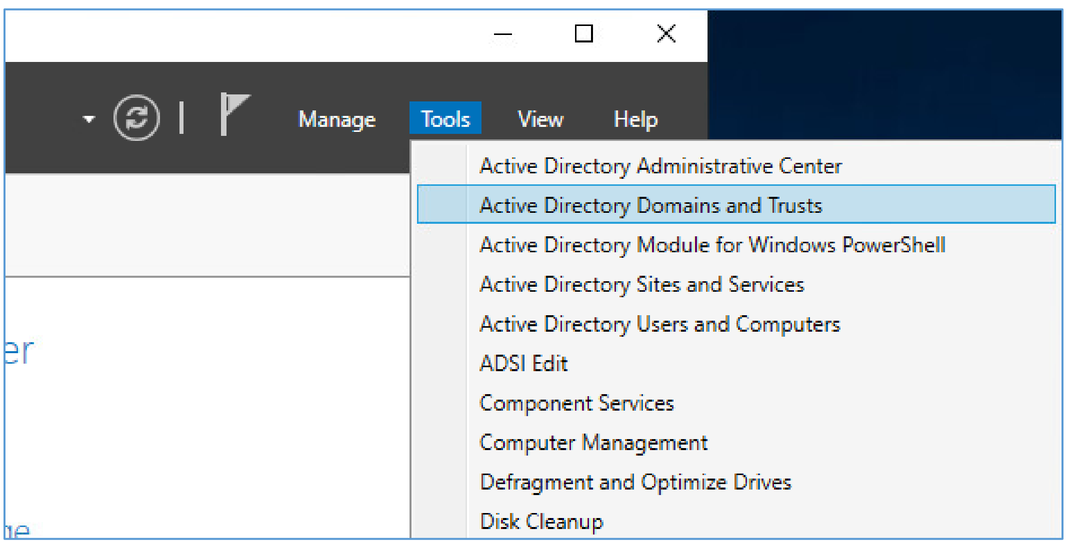
Operating System: Microsoft Windows Server 2019 Datacenter

Domain Controller Appliance Installation Guide

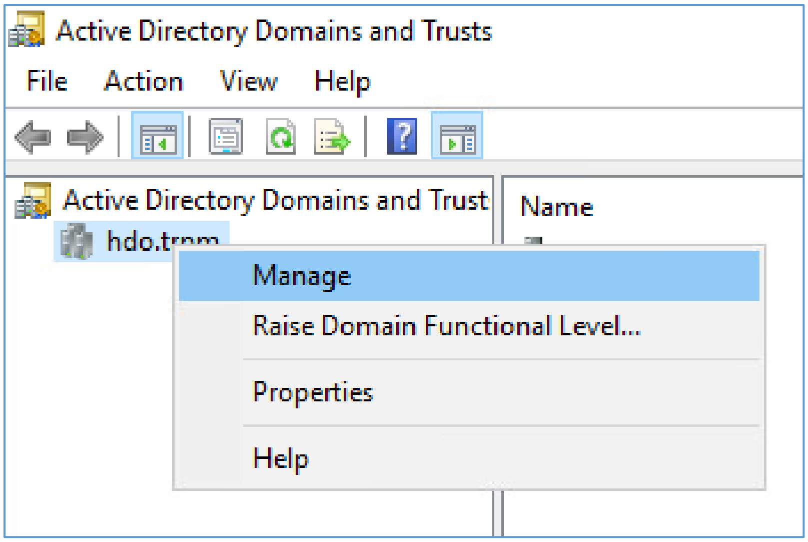
Install the appliance according to the instructions detailed in Microsoft's Install Active Directory Domain Services (Level 100) documentation [4].

Verify Domain Controller Installation

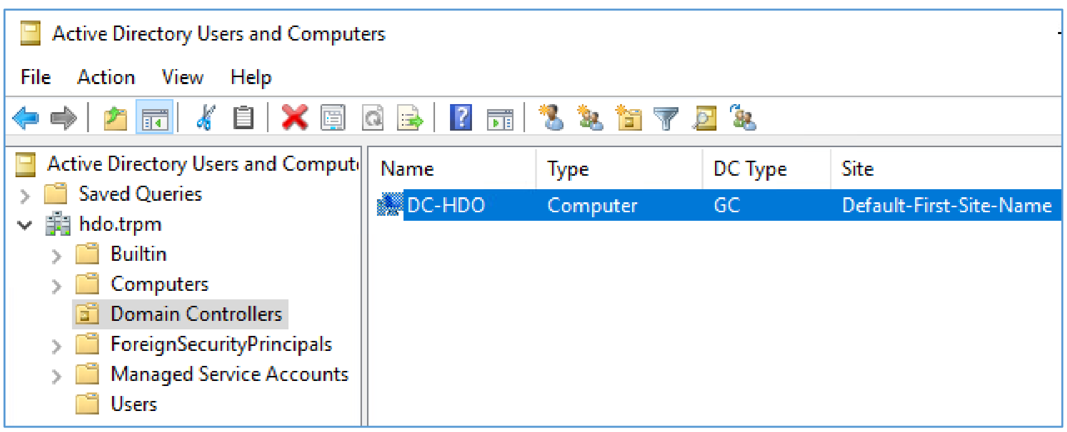
1. Launch **Server Manager.**
2. Click **Tools > Active Directory Domains and Trusts.**



3. Right-click **hdo.trpm.**
4. Click **Manage.**

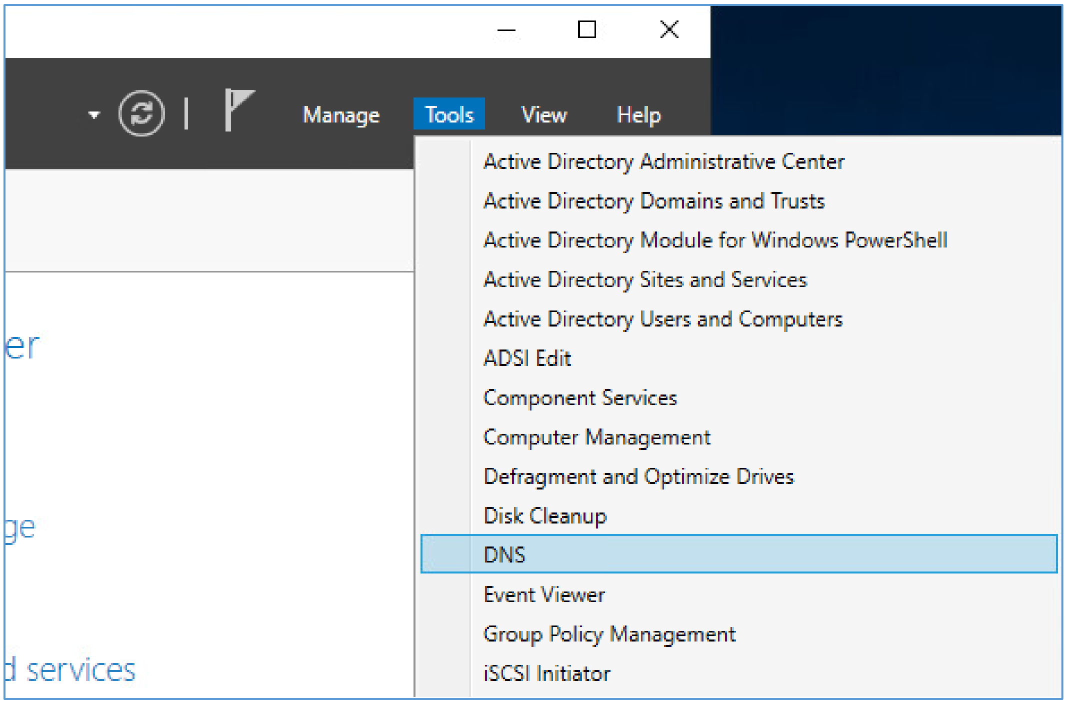


5. Click **hdo.trpm > Domain Controllers.**
6. Check that the Domain Controllers directory lists the new domain controller.

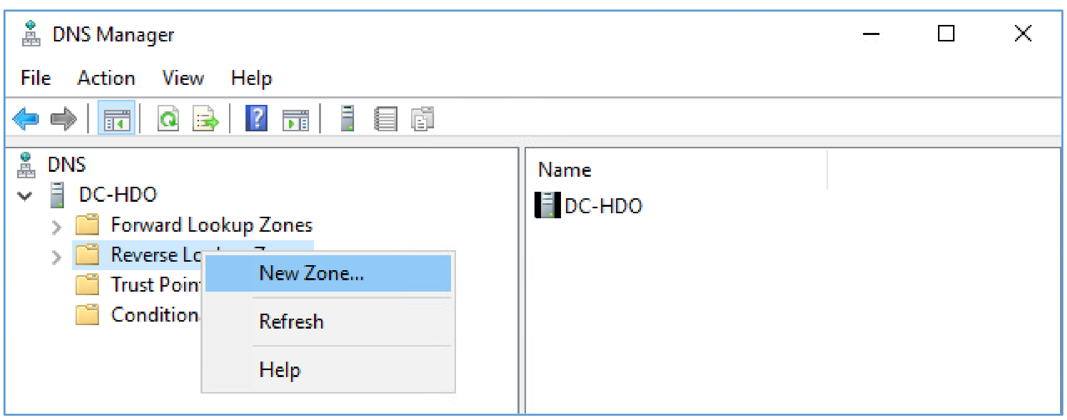


<u>Configure Local DNS</u>

1. Launch **Server Manager.**
2. Click **Tools > DNS.**



3. Click the **arrow symbol** for DC-HDO.
4. Right-click **Reverse Lookup Zones.**
5. Click **New Zone….** The New Zone Wizard displays.

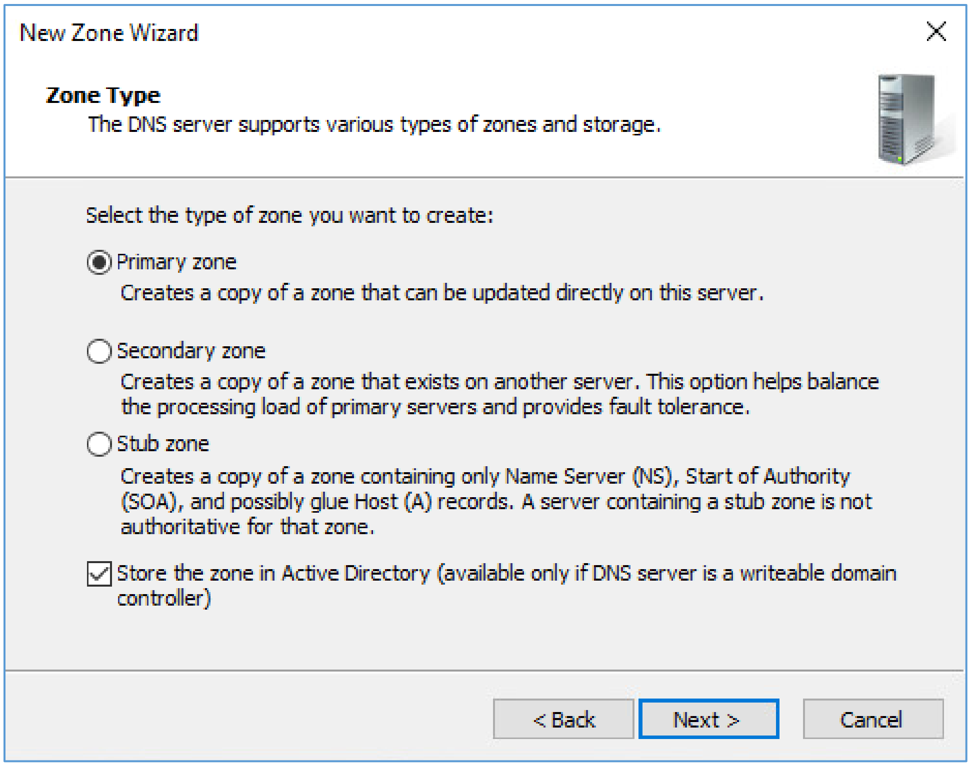


6. Click **Next >.**

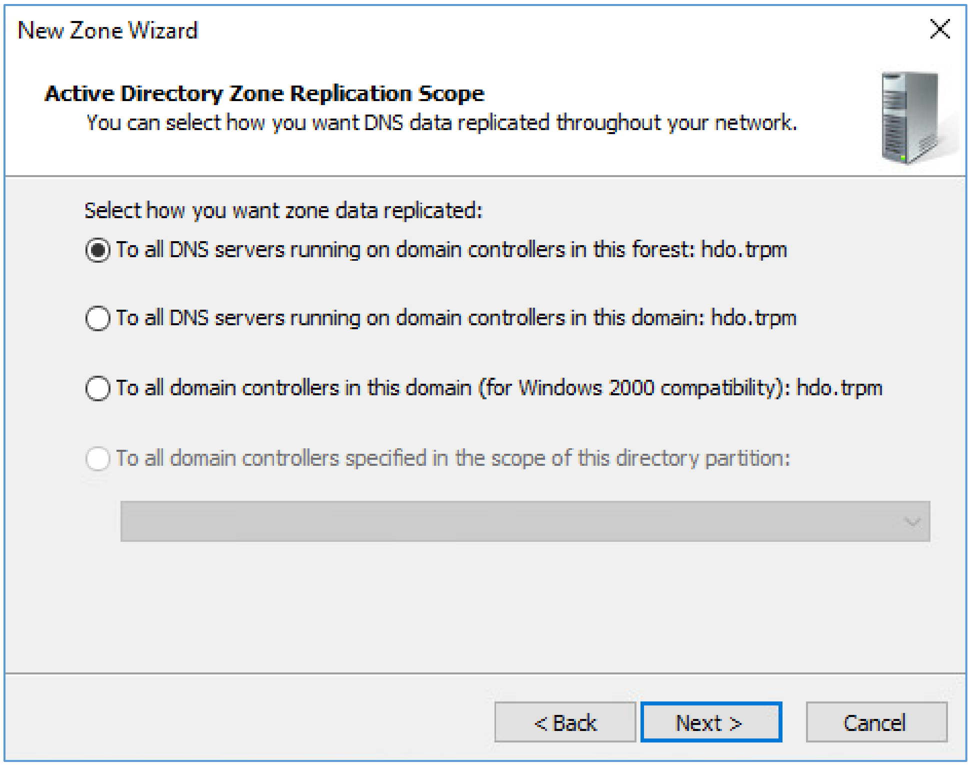
618 7. Click **Primary zone.**

619 8. Check **Store the zone in Active Directory.**

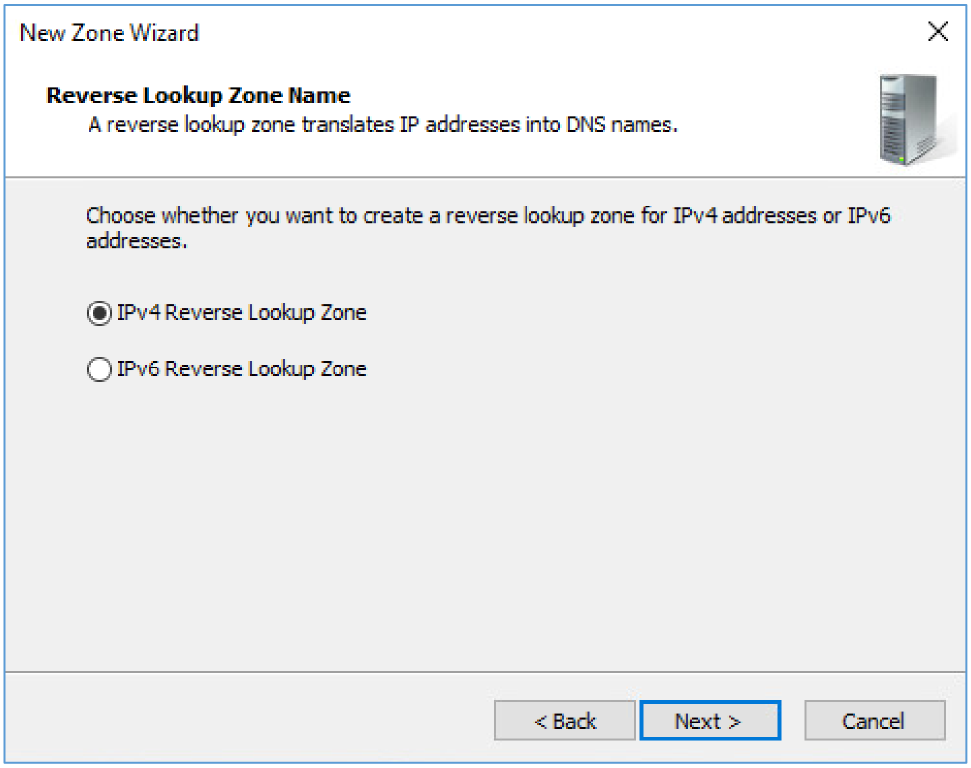
620 9. Click **Next >.**



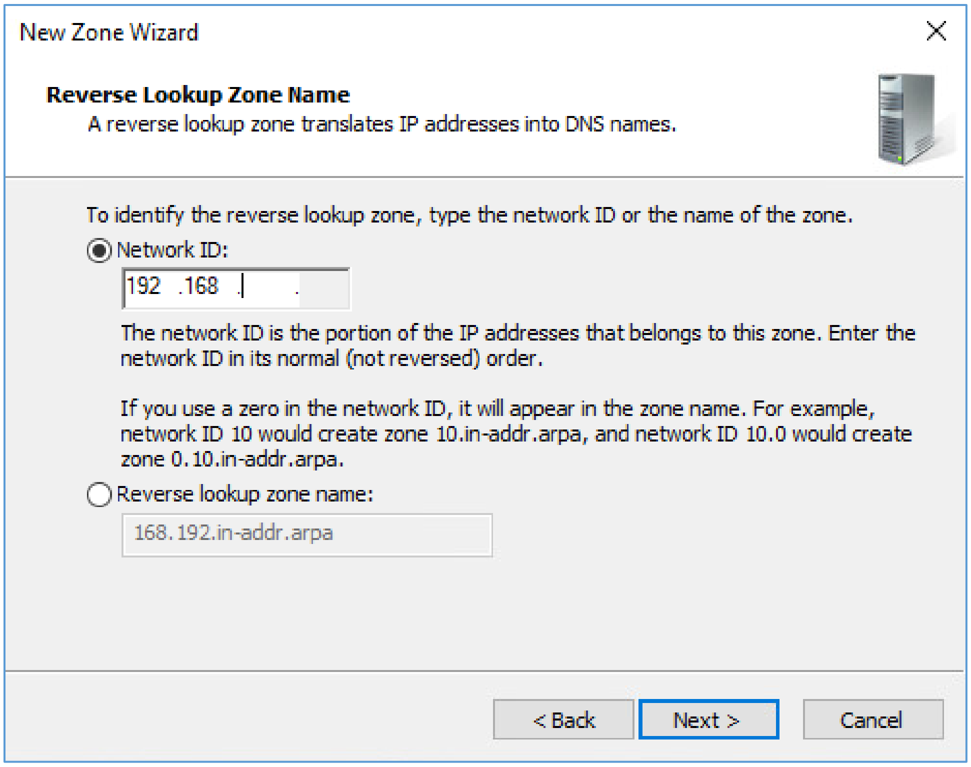
10. Check **To all DNS servers running on domain controllers in this forest: hdo.trpm.**
11. Click **Next >.**



12. Check **IPv4 Reverse Lookup Zone.**
13. Click **Next >.**

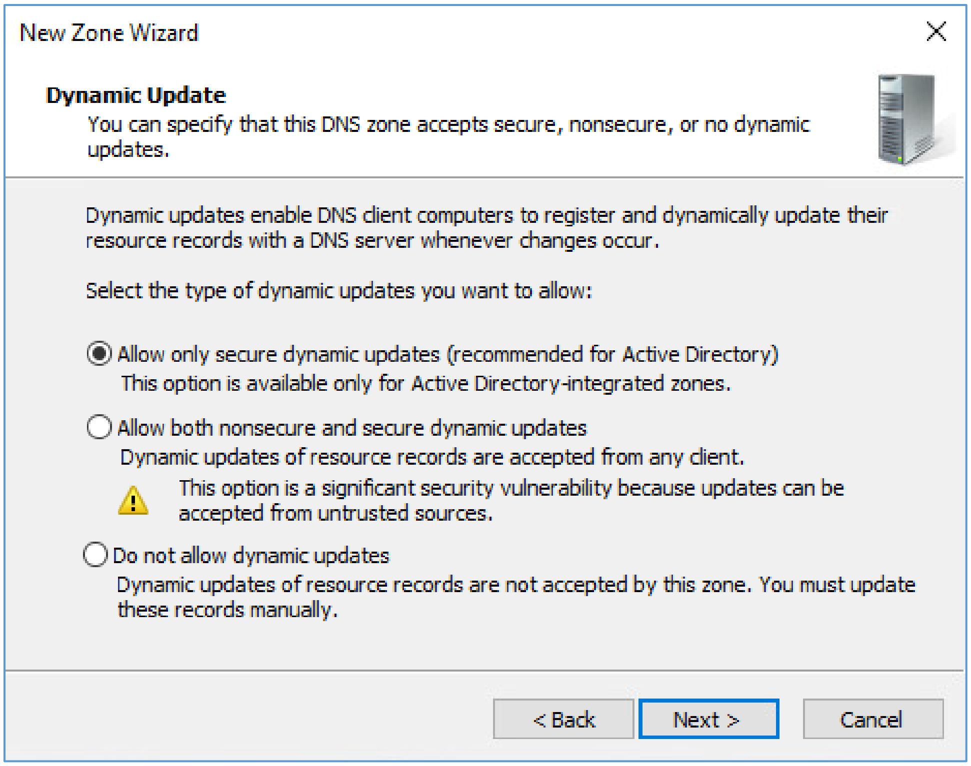


14. Check **Network ID.**
15. Under **Network ID,** type **192.168.**
16. Click **Next >.**

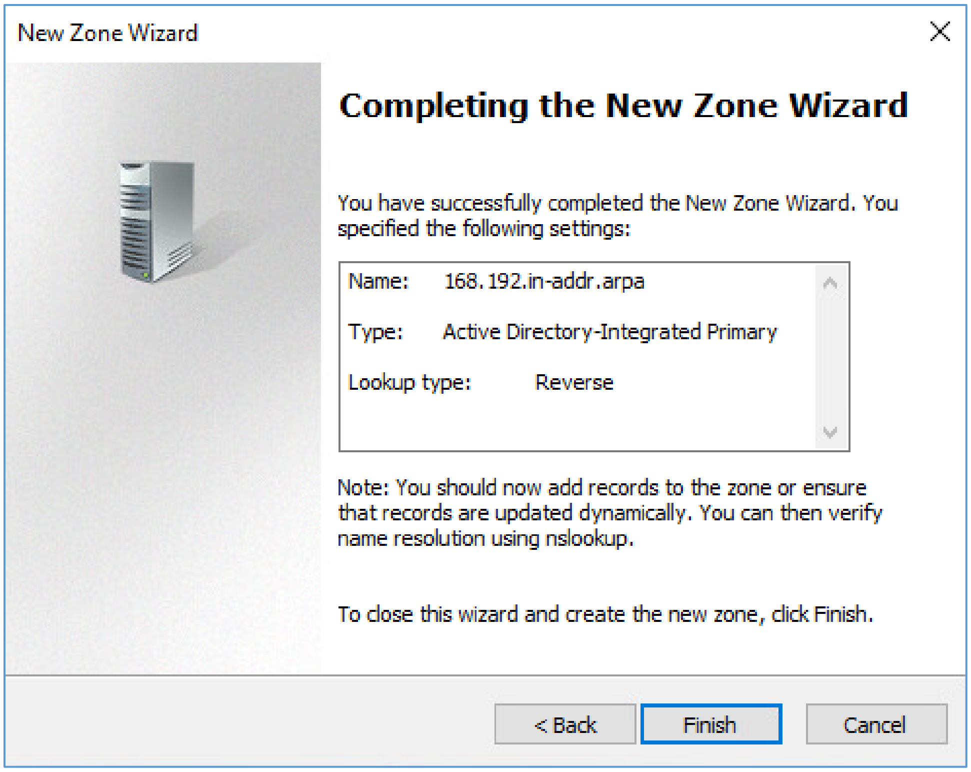


628 17. Check **Allow only secure dynamic updates.**

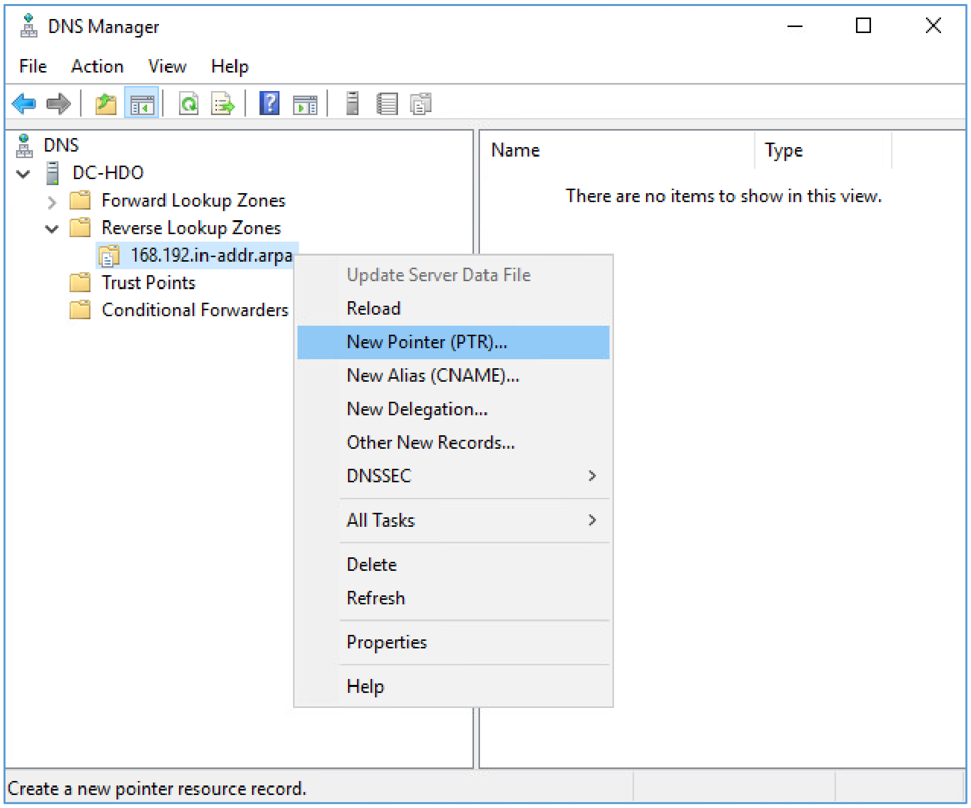
629 18. Click **Next >.**



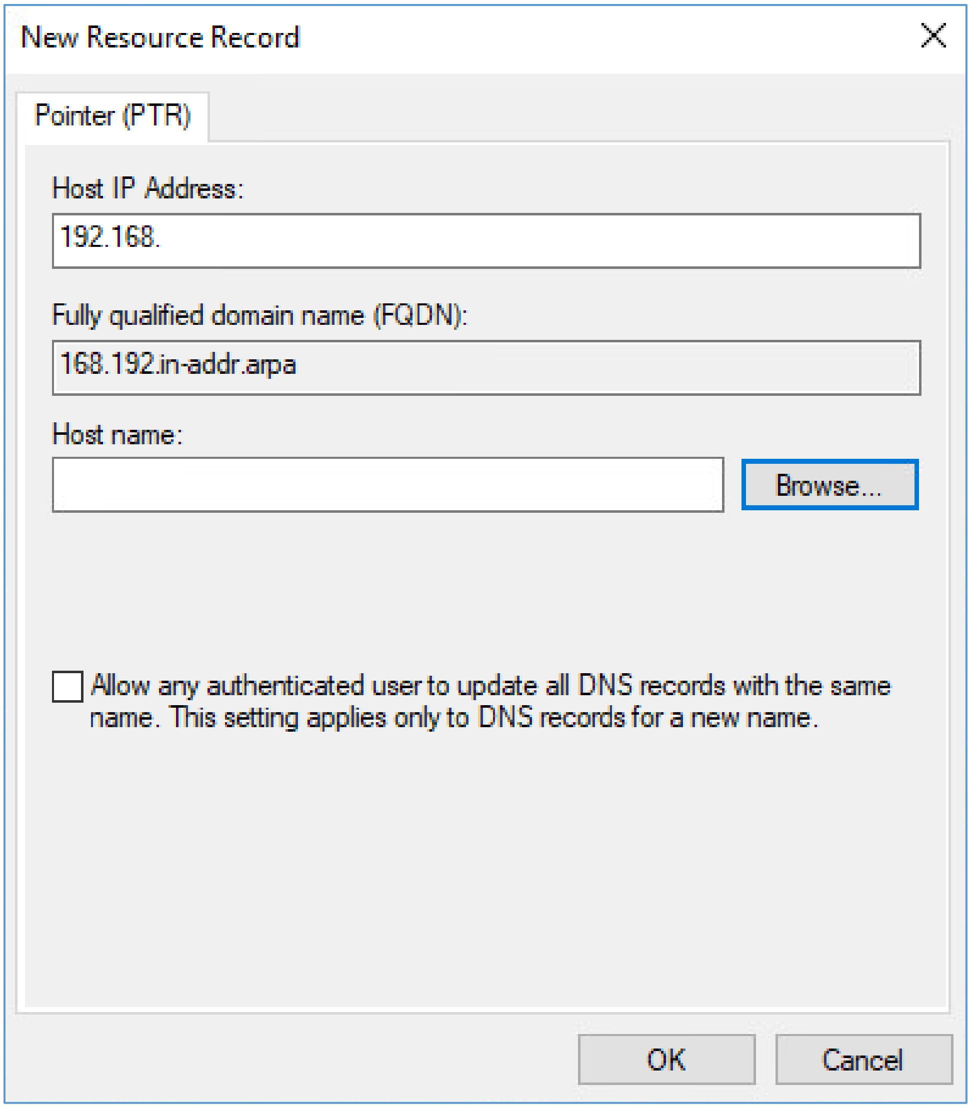
19. Click **Finish.**



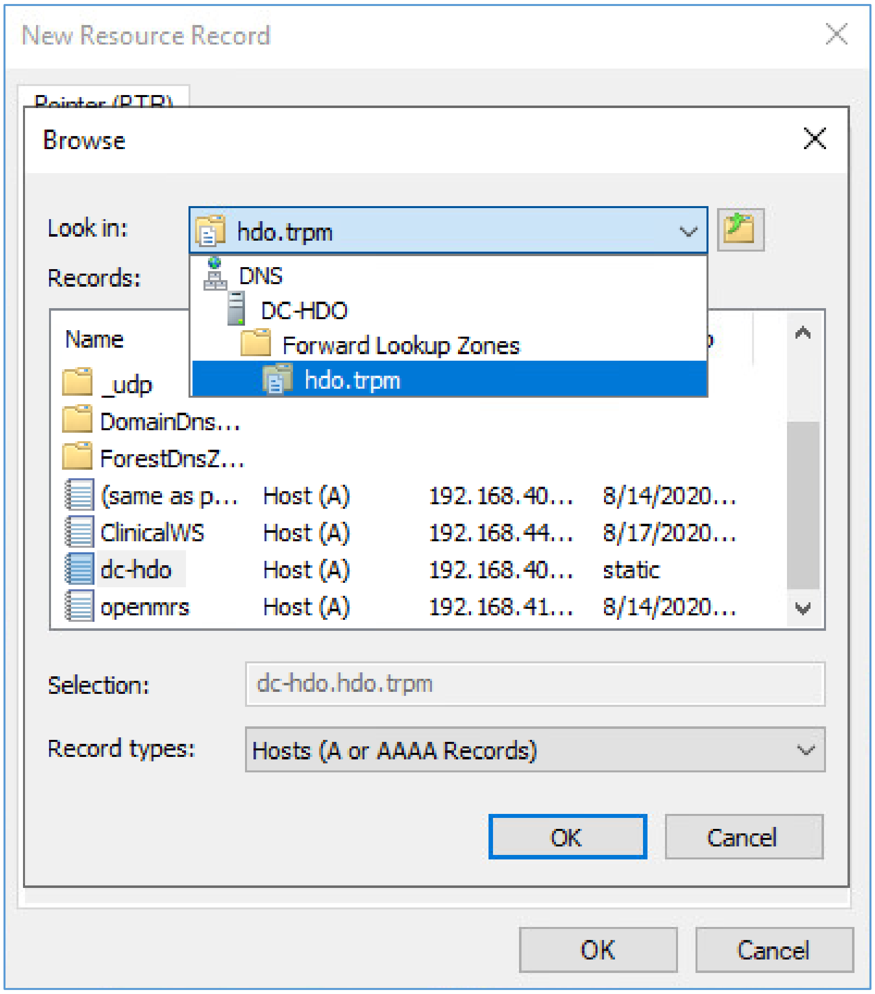
20. Click the arrow symbol for **Reverse Lookup Zones.**
21. Right-click **168.192.in-addr.arpa.**
22. Click **New Pointer (PTR)….**



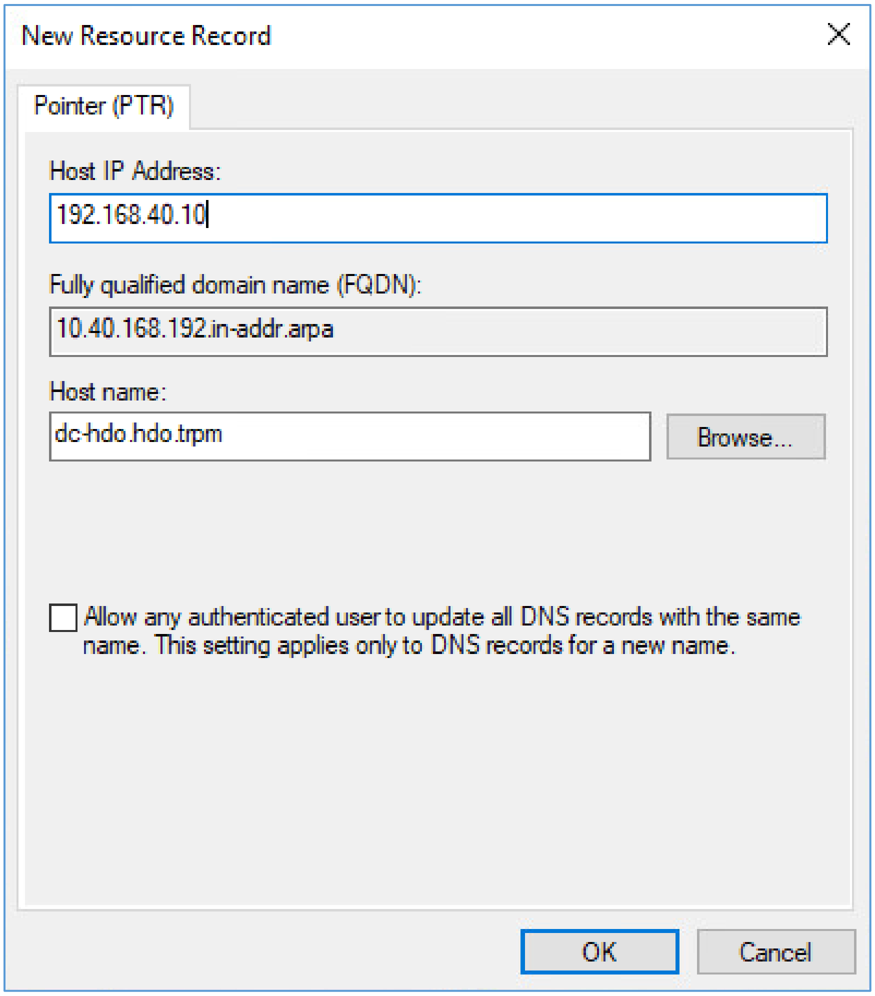
634 23. Under **Host name,** click **Browse….**

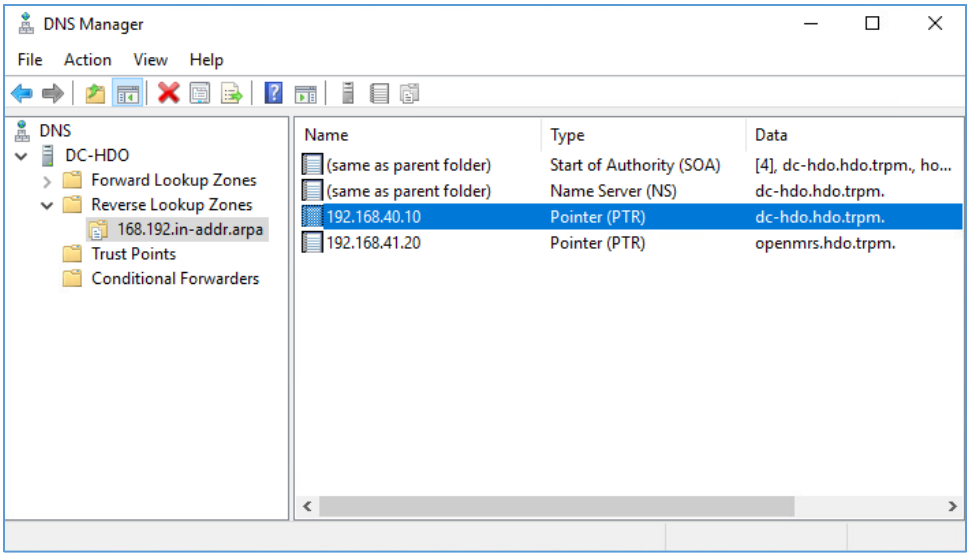


24. Under Look in, select **hdo.trpm.**
25. Under Records, select **dc-hdo.**
26. Click **OK.**



638 27. Click **OK.**


New Resource Record
Pointer (PTR)
Host IP Address:
192.168.40.10
Fully qualified domain name (FQDN):
10.40.168.192.in-addr.arpa
Host name:
dc-hdo.hdo.trpm
Browse...
Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.
OK
Cancel



2.2.2.2 Cisco Firepower

Cisco Firepower consists of two primary components: Cisco Firepower Management Center and Cisco Firepower Threat Defense (FTD). Cisco Firepower provides firewall, intrusion prevention, and other networking services. This project used Cisco Firepower to implement VLAN network segmentation, network traffic filtering, internal and external routing, applying an access control policy, and Dynamic Host Configuration Protocol (DHCP). Engineers deployed Cisco Firepower as a core component for the lab's network infrastructure.

Cisco Firepower Management Center (FMC) Appliance Information

CPU: 4

RAM: 8 GB

Storage: 250 GB (Thick Provision)

Network Adapter 1: VLAN 1327

Operating System: Cisco Fire Linux 6.4.0

Cisco Firepower Management Center Installation Guide

Install the appliance according to the instructions detailed in the *Cisco Firepower Management Center Virtual Getting Started Guide* [5].

Cisco FTD Appliance Information

CPU: 8

RAM: 16 GB

Storage: 48.5 GB (Thick Provision)

Network Adapter 1: VLAN 1327

Network Adapter 2: VLAN 1327

Network Adapter 3: VLAN 1316

Network Adapter 4: VLAN 1327

Network Adapter 5: VLAN 1328

Network Adapter 6: VLAN 1329

Network Adapter 7: VLAN 1330

Network Adapter 8: VLAN 1347

Network Adapter 9: VLAN 1348

Operating System: Cisco Fire Linux 6.4.0

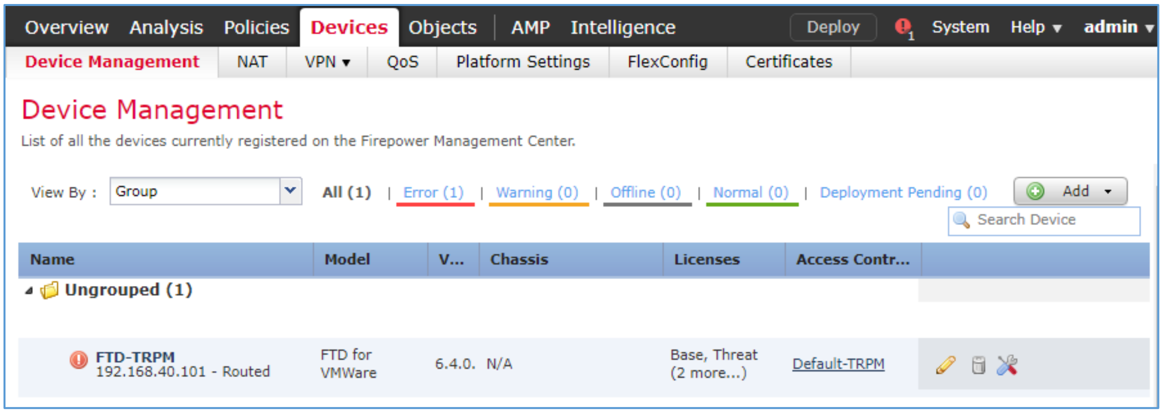
Cisco FTD Installation Guide

Install the appliance according to the instructions detailed in the *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide* in the Deploy the Firepower Threat Defense Virtual chapter [6].

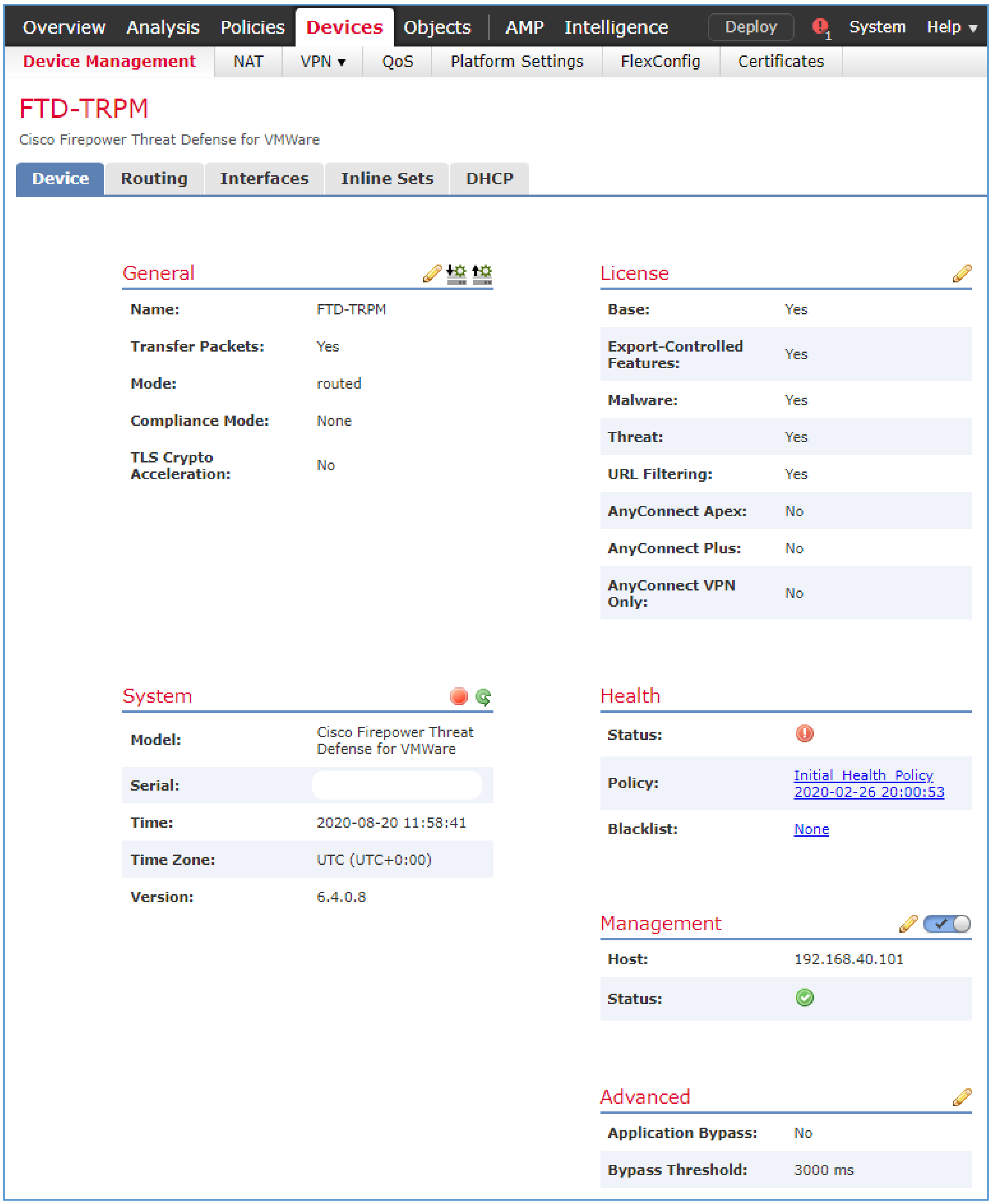
Configure FMC Management of FTD

The *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide'*s Managing the Firepower Threat Defense Virtual with the Firepower Management Center (FMC) chapter covers how we registered the FTD appliance with the FMC [7].

Once the FTD successfully registers with the FMC, it will appear under **Devices > Device Management** in the FMC interface.



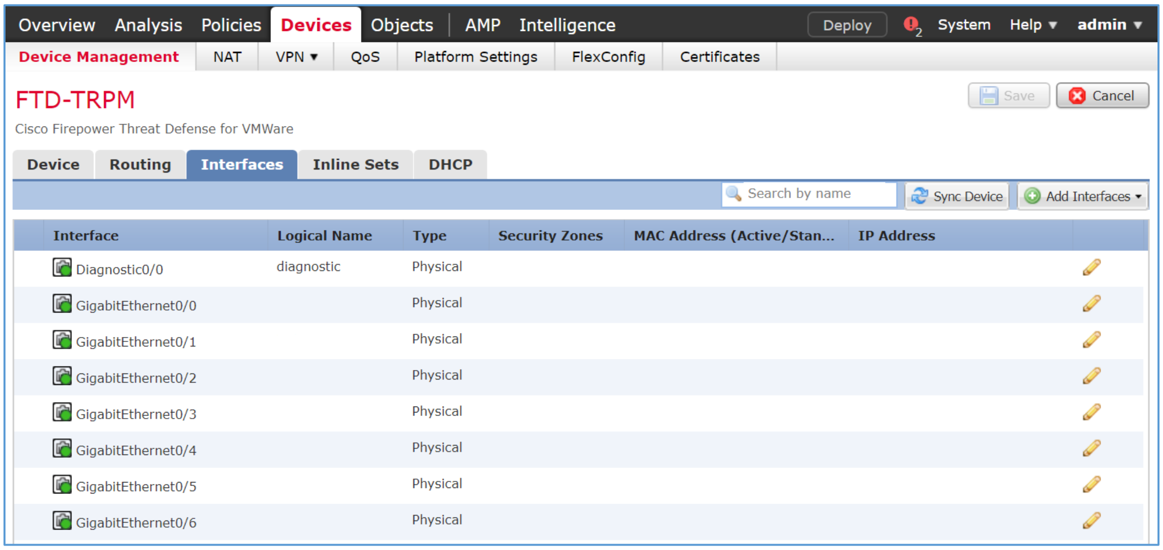
From the Device Management section, the default routes, interfaces, and DHCP settings can be configured. To view general information for the FTD appliance, navigate to **Devices > Device Management > FTD-TRPM > Device.**



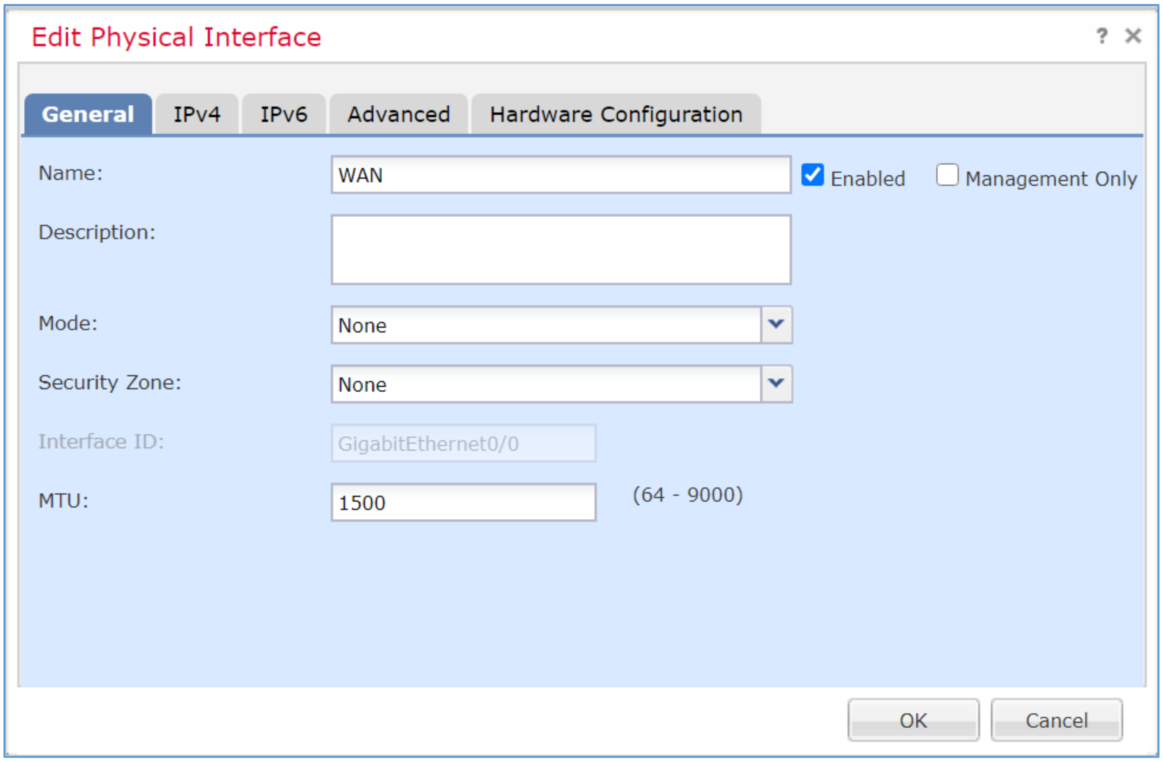
Configure Cisco FTD Interfaces for the RPM Architecture

By default, each of the interfaces is defined as GigabitEthernet and is denoted as 0 through 6.

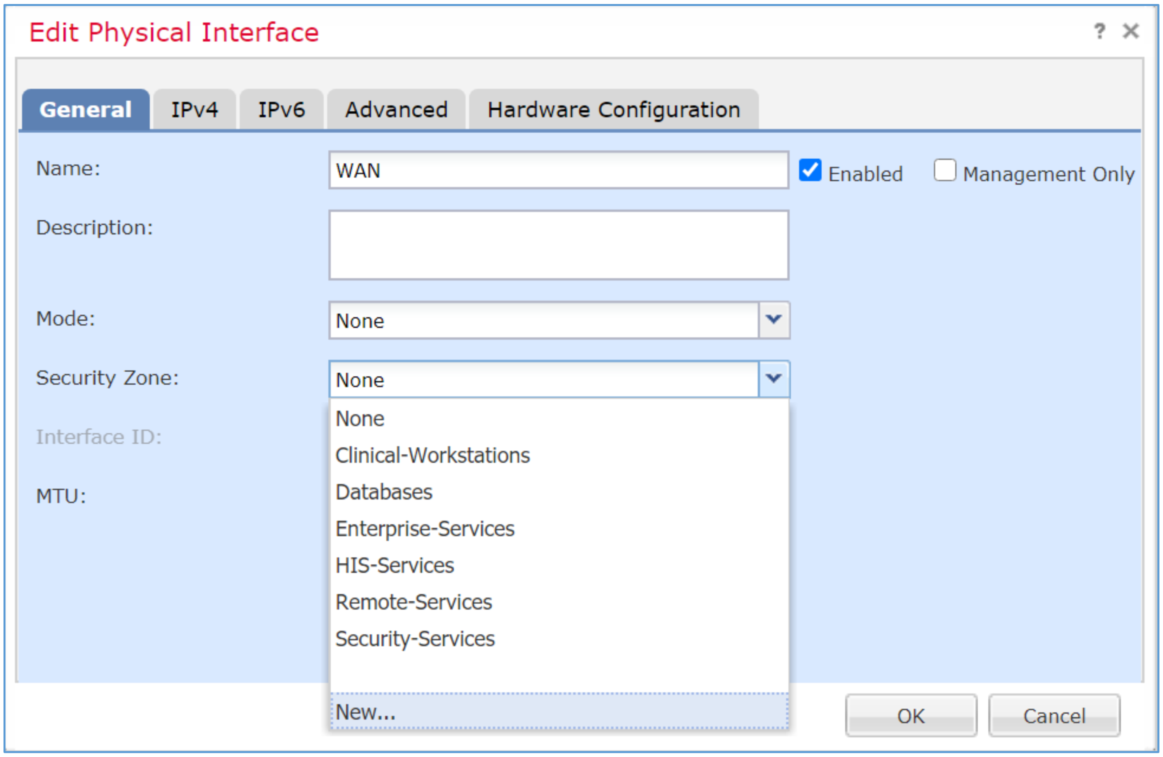
1. From **Devices > Device Management > FTD-TRPM > Device,** click **Interfaces.**
2. On the Cisco FTD Interfaces window, an Edit icon appears on the far right. The first GigabitEthernet interface configured is GigabitEthernet0/0. Click the Edit icon to configure the GigabitEthernet interface.



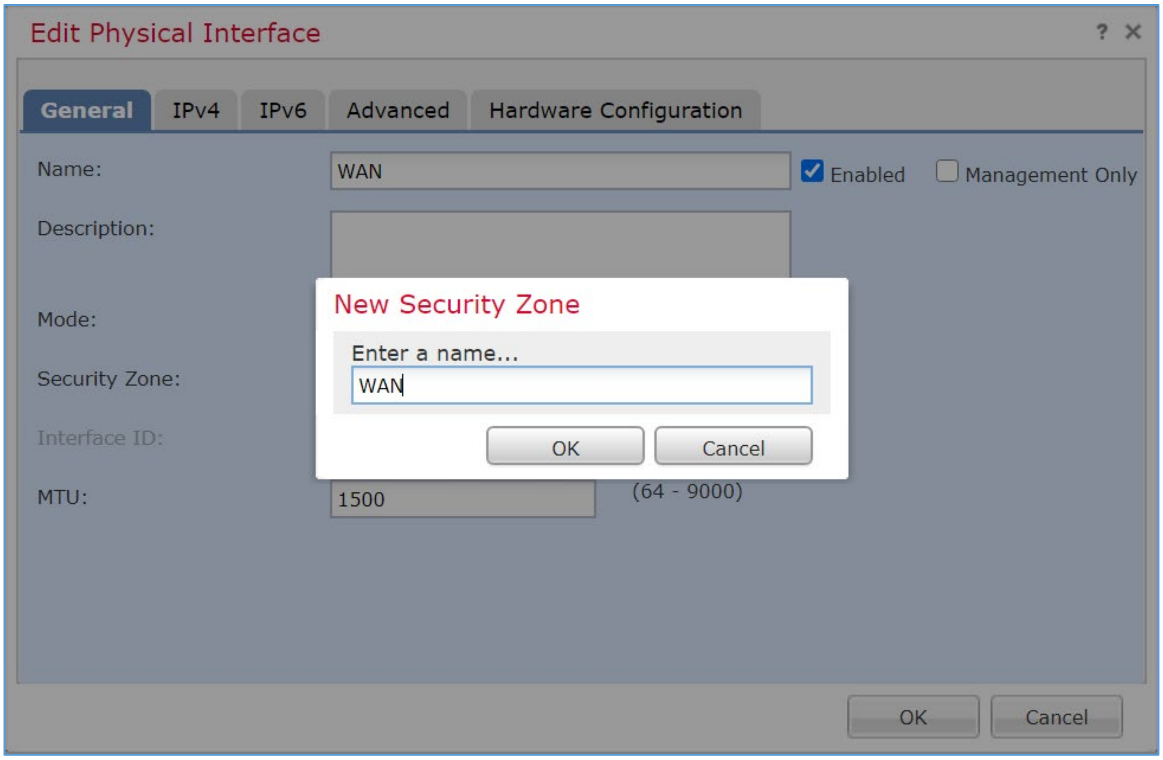
3. The Edit Physical Interface group box displays. Under the General tab, enter **WAN** in the **Name** field.



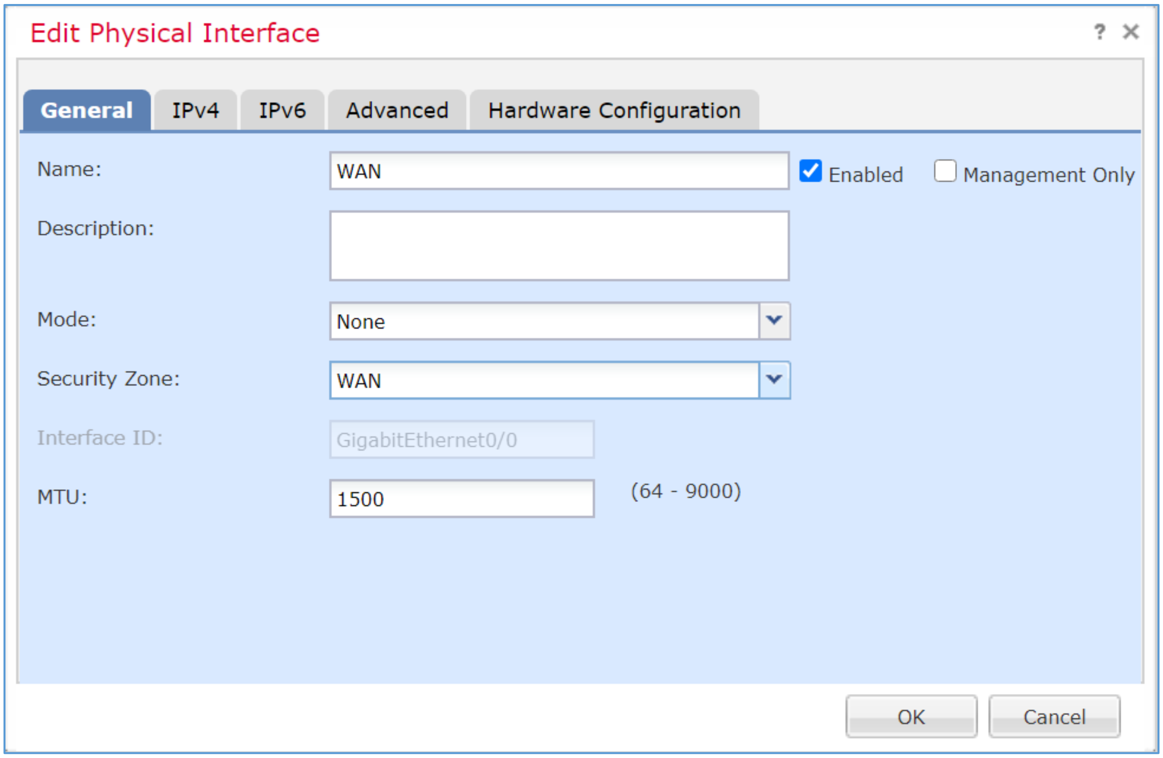
689 4. Under **Security Zone,** click the drop-down arrow and select **New….**



5. The New Security Zone pop-up box appears. Enter **WAN** in the **Enter a name…** field.
6. Click **OK.**



692 7. On the Edit Physical Interface page group box, click the **IPv4** tab.

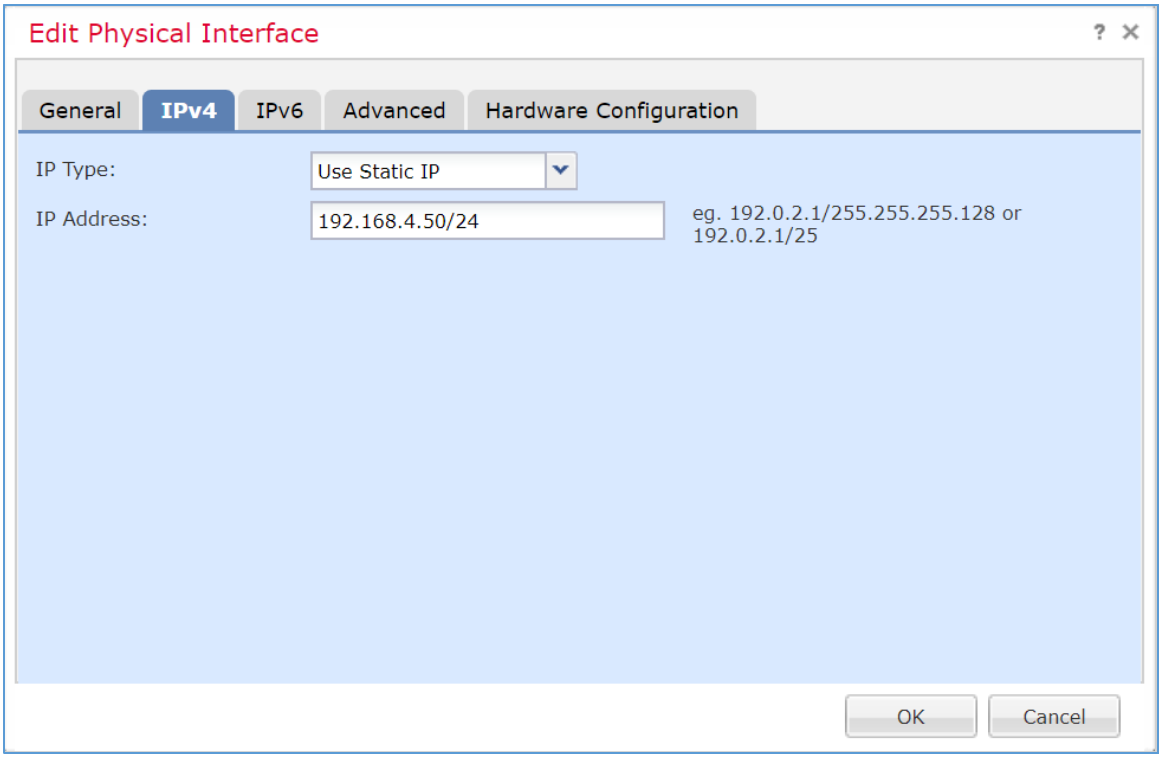


693 8. Fill out the following information:

694 a. **IP Type:** Use Static IP

695 b. **IP Address:** 192.168.4.50/24

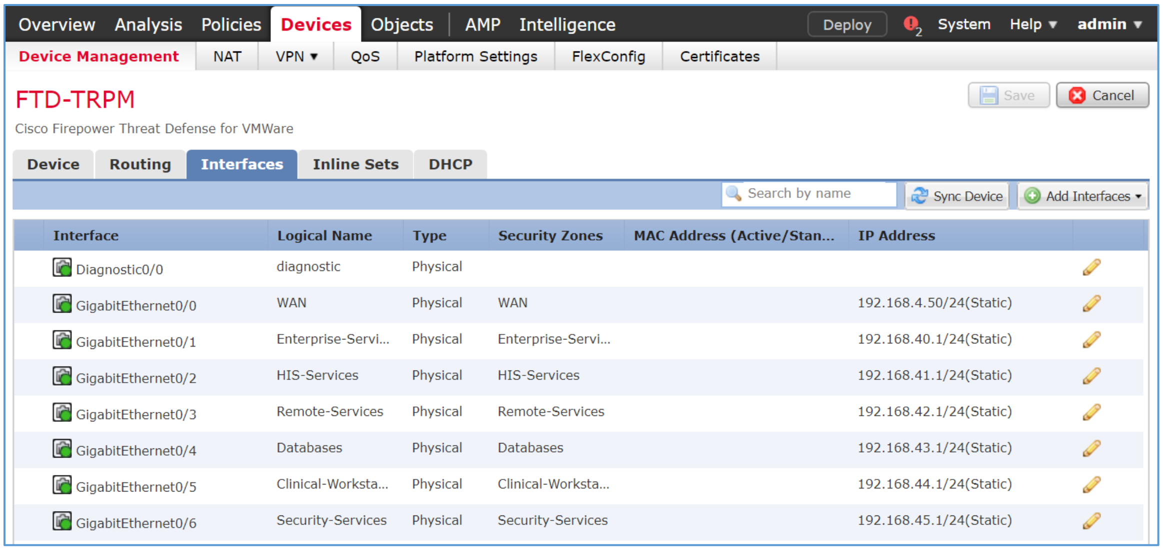
696 c. Click **OK.**



9. Configure each of the other GigabitEthernet interfaces following the same pattern described above, populating the respective IP addresses that correspond to the appropriate VLAN. Values for each VLAN are described below:
    a. GigabitEthernet0/0 (VLAN 1316)
        i. **Name:** WAN
        ii. **Security Zone:** WAN
        iii. **IP Address:** 192.168.4.50/24
    b. GigabitEthernet0/1 (VLAN 1327)
        i. **Name:** Enterprise-Services
        ii. **Security Zone:** Enterprise-Services
        iii. **IP Address:** 192.168.40.1/24
    c. GigabitEthernet0/2 (VLAN 1328)
        i. **Name:** HIS-Services

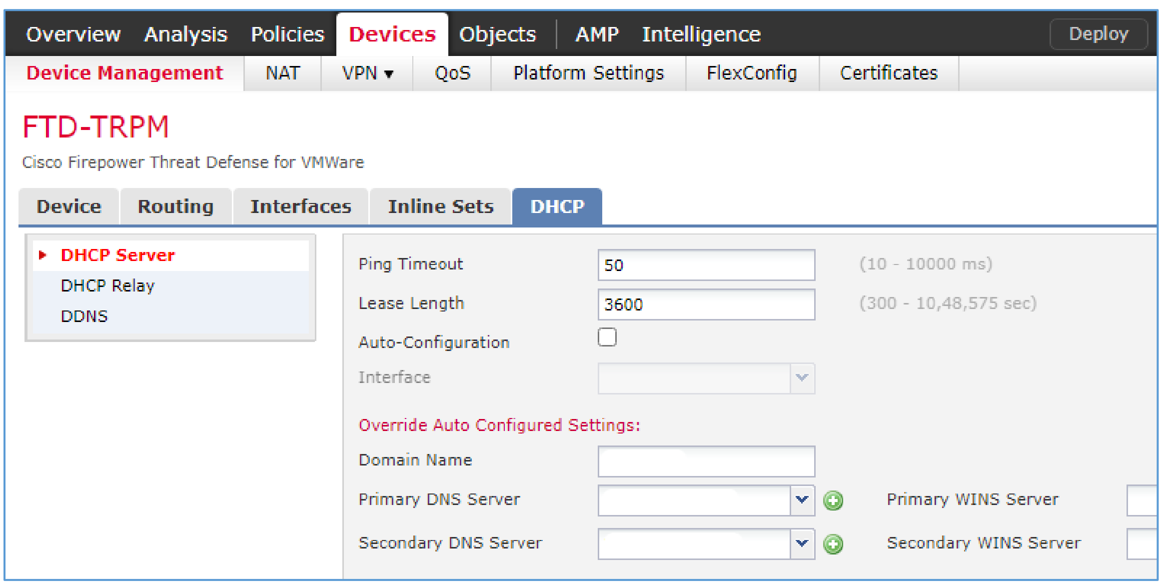
        ii. **Security Zone:** HIS-Services
        iii. **IP Address:** 192.168.41.1/24
    d. GigabitEthernet0/3 (VLAN 1329)
        i. **Name:** Remote-Services
        ii. **Security Zone:** Remote-Services
        iii. **IP Address:** 192.168.42.1/24
    e. GigabitEthernet0/4 (VLAN 1330)
        i. **Name:** Databases
        ii. **Security Zone:** Databases
        iii. **IP Address:** 192.168.43.1/24
    f. GigabitEthernet0/5 (VLAN 1347)
        i. **Name:** Clinical-Workstations
        ii. **Security Zone:** Clinical-Workstations
        iii. **IP Address:** 192.168.44.1/24
    g. GigabitEthernet0/6 (VLAN 1348)
        i. **Name:** Security-Services
        ii. **Security Zone:** Security-Services
        iii. **IP Address:** 192.168.45.1/24

10. Click **Save.**
11. Click **Deploy.** Verify that the interfaces have been configured properly. Selecting the Devices tab, the Device Management screen displays the individual interfaces, assigned logical names, type of interface, security zone labeling, and assigned IP address network that corresponds to the VLANs that are assigned per security zone.



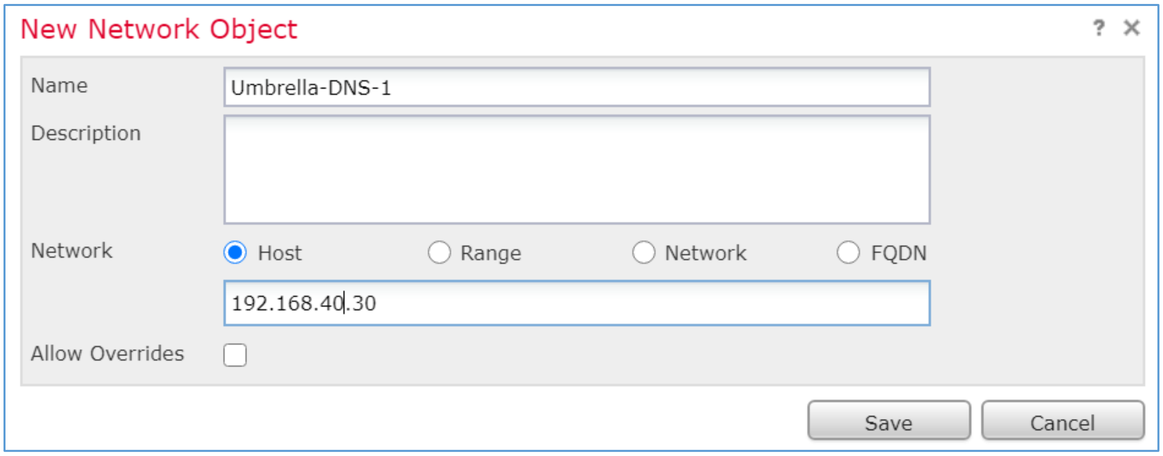
Configure Cisco FTD DHCP

1. From **Devices > Device Management > FTD-TRPM > Interfaces,** click **DHCP.**
2. Click the **plus symbol** next to **Primary DNS Server.**

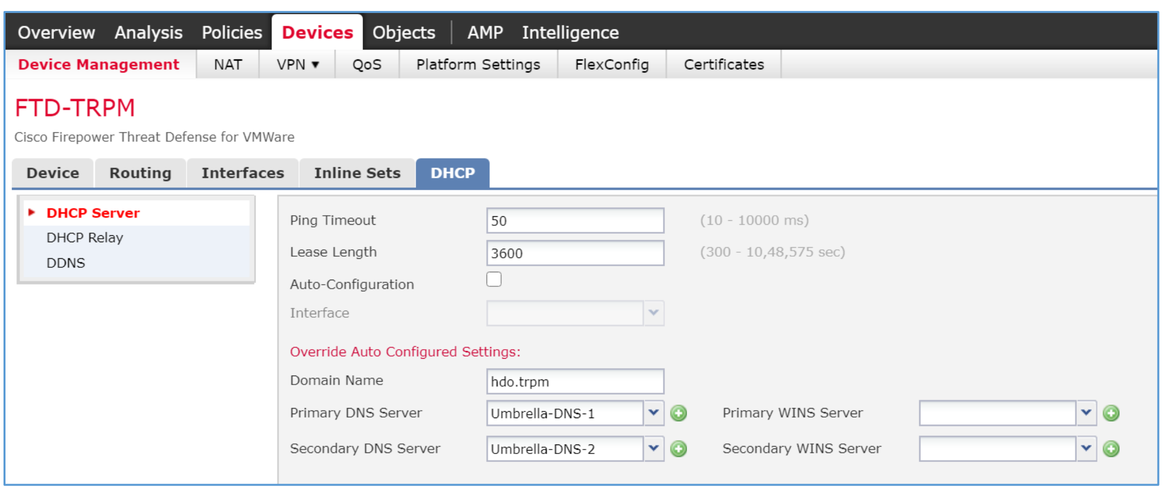


3. The New Network Object pop-up window appears. Fill out the following information:
   a. **Name:** Umbrella-DNS-1
   b. **Network (Host):** 192.168.40.30

4. Click **Save.**

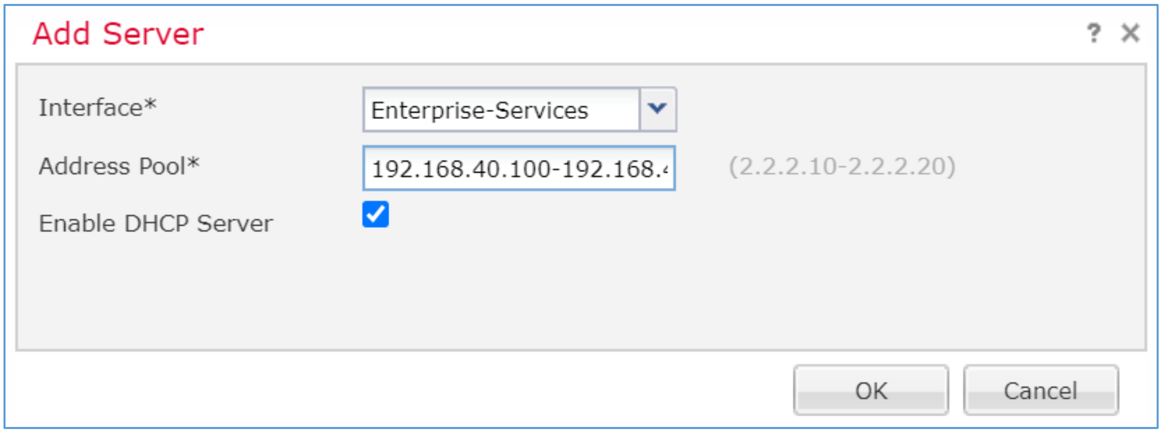


5. Click the **plus symbol** next to **Secondary DNS Server.**
6. The New Network Object pop-up window appears. Fill out the following information:
    a. **Name:** Umbrella-DNS-2
    b. **Network (Host):** 192.168.40.31
7. Under **Domain Name,** add **hdo.trpm.**
8. Click **Add Server.**



9. The Add Server pop-up window appears. Fill out the following information:
    a. **Interface:** Enterprise-Services

   b. **Address Pool:** 192.168.40.100-192.168.40.254
   c. **Enable DHCP Server:** checked
10. Click **OK.**



11. Add additional servers by following the same pattern described above, populating the respective Interface and Address Pool, and check the **Enable DHCP Server** that corresponds to the appropriate server. Values for each server are described below:
   a. **Interface:** Enterprise-Services
      i. **Address Pool:** 192.168.40.100-192.168.40.254
      ii. **Enable DHCP Server:** checked
   b. **Interface:** HIS-Services
      i. **Address Pool:** 192.168.41.100-192.168.41.254
      ii. **Enable DHCP Server:** checked
   c. **Interface:** Remote-Services
      i. **Address Pool:** 192.168.42.100-192.168.42.254
      ii. **Enable DHCP Server:** checked
   d. **Interface:** Databases
      i. **Address Pool:** 192.168.43.100-192.168.43.254
      ii. **Enable DHCP Server:** checked
   e. **Interface:** Clinical-Workstations

i. **Address Pool:** 192.168.44.100-192.168.44.254

ii. **Enable DHCP Server:** checked

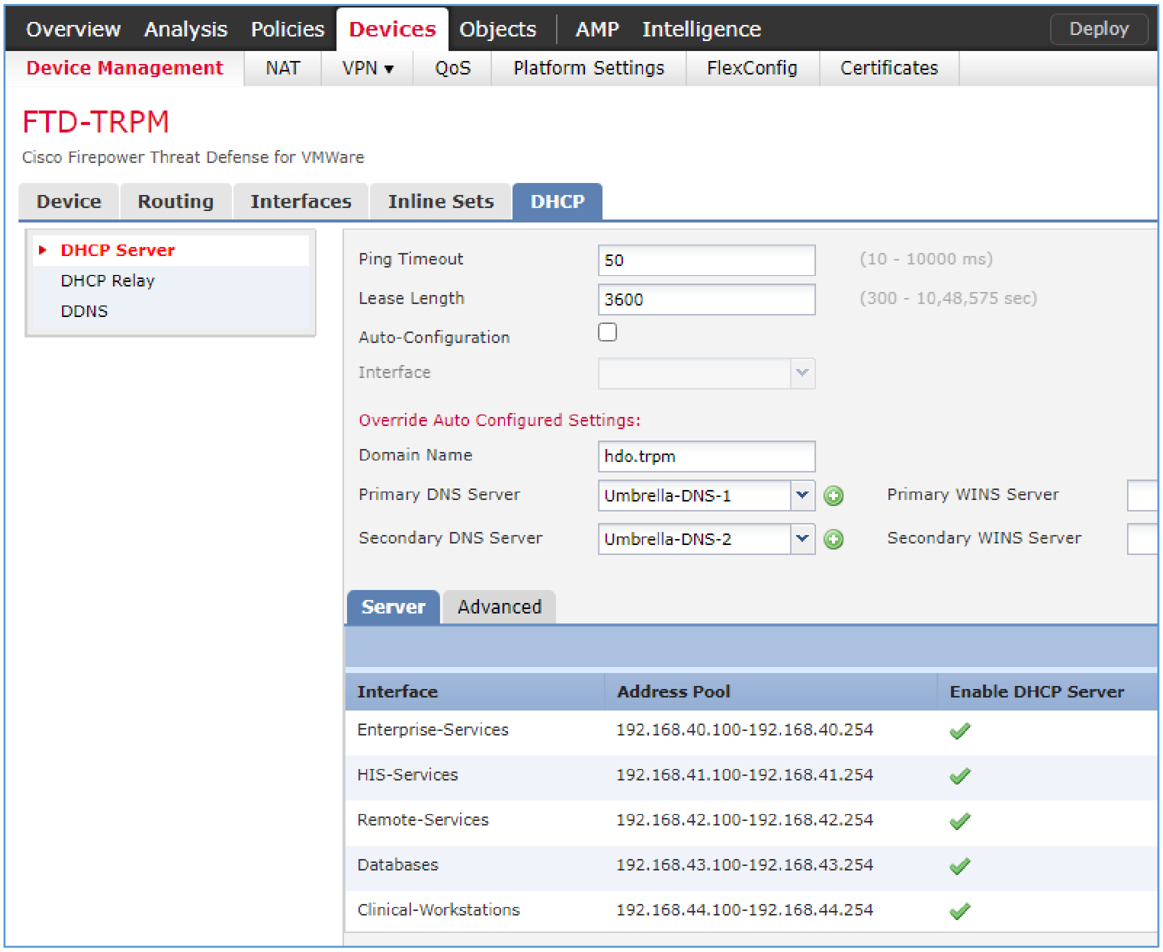
f. **Interface:** Security-Services

i. **Address Pool:** 192.168.45.100-192.168.45.254

ii. **Enable DHCP Server:** checked

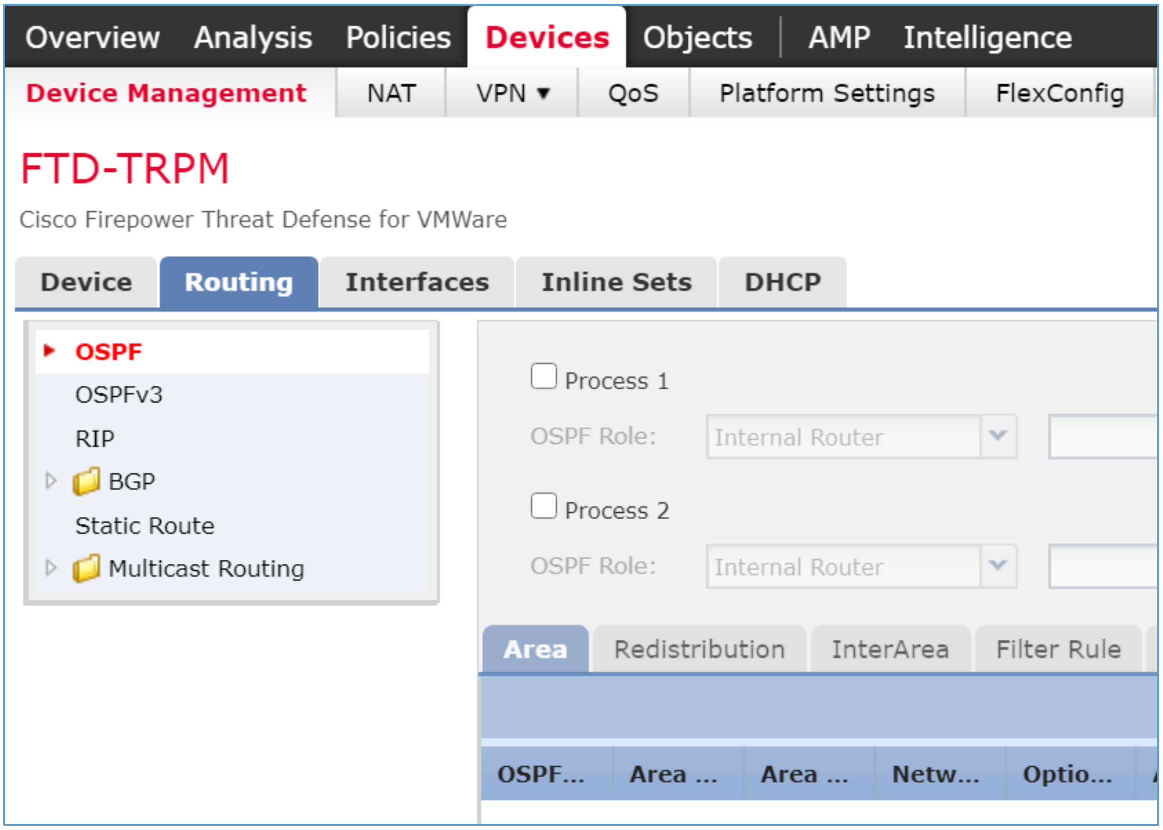
12. Click **Save.**

13. Click **Deploy.** Verify that the DHCP servers have been configured properly. Select the **Devices** tab, and review the DHCP server configuration settings. Values for **Ping Timeout** and **Lease Length** correspond to default values that were not altered. The **Domain Name** is set to **hdo.trpm,** with values that were set for the primary and secondary DNS servers. Below the DNS server settings, a **Server** tab displays the DHCP address pool that corresponds to each security zone. Under the **Interface** heading, view each security zone label that aligns to the assigned **Address Pool,** and review that the **Enable DHCP Server** setting appears as a green check mark.

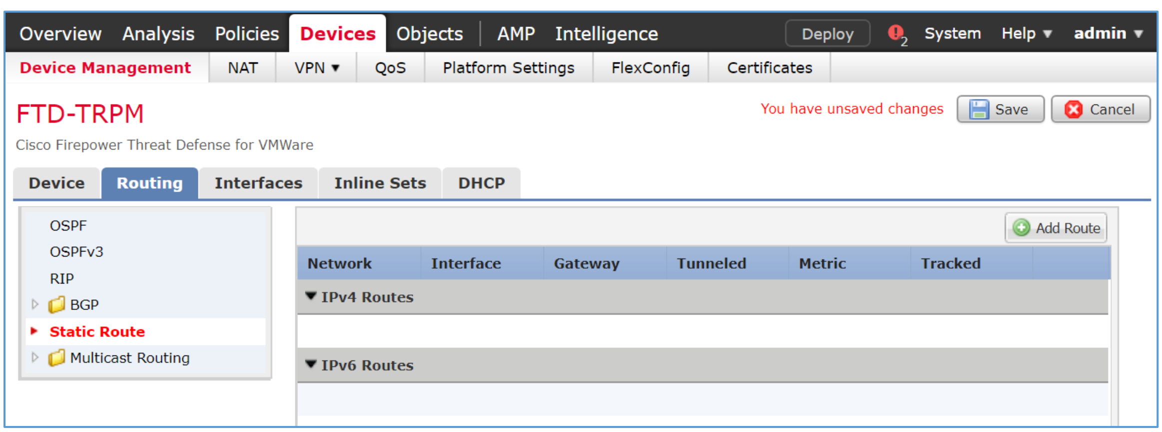


Configure Cisco FTD Static Route

1. From **Devices > Device Management > FTD-TRPM > DHCP,** click **Routing.**
2. Click **Static Route.**

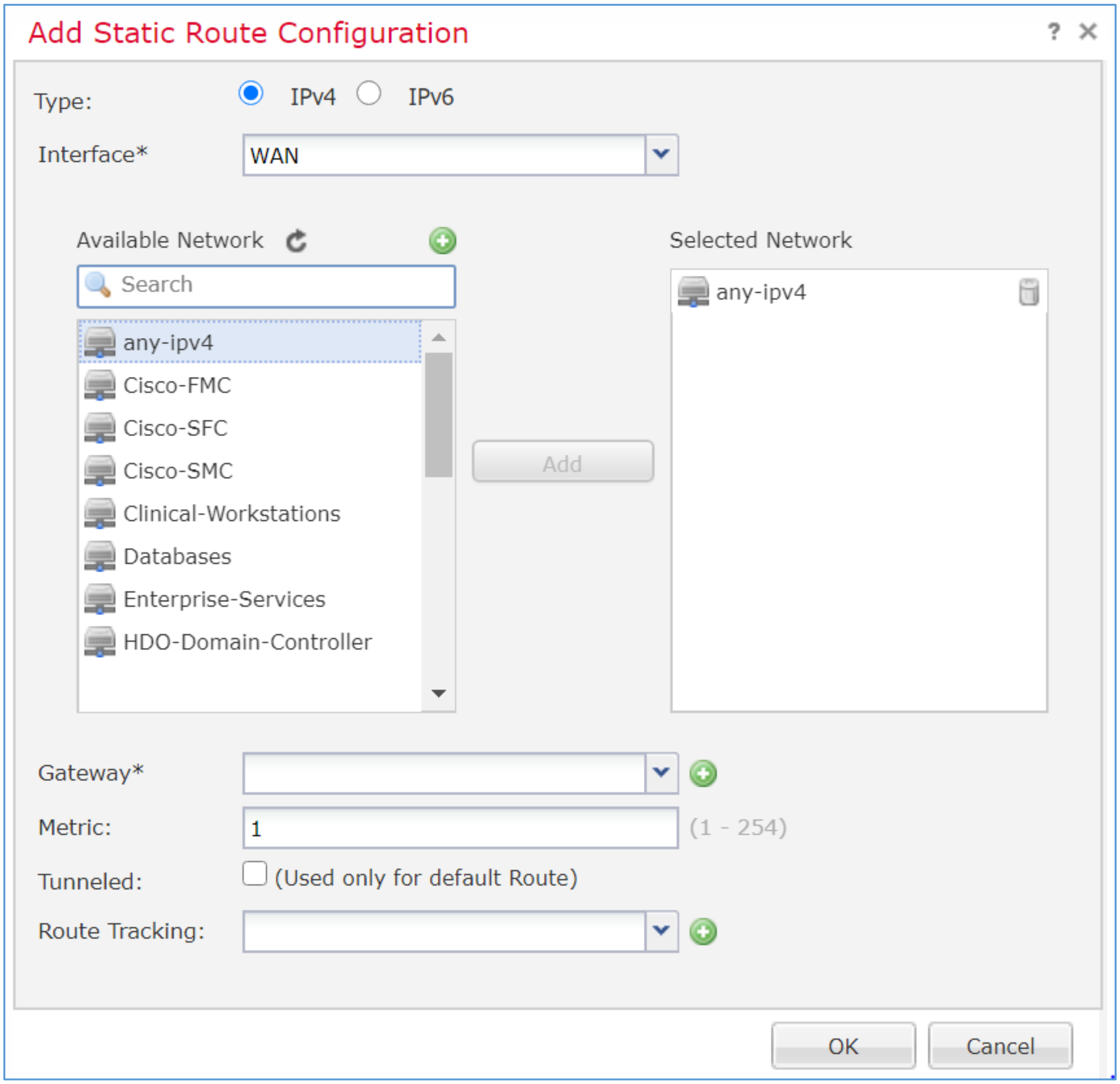


3. Click **Add Route.**

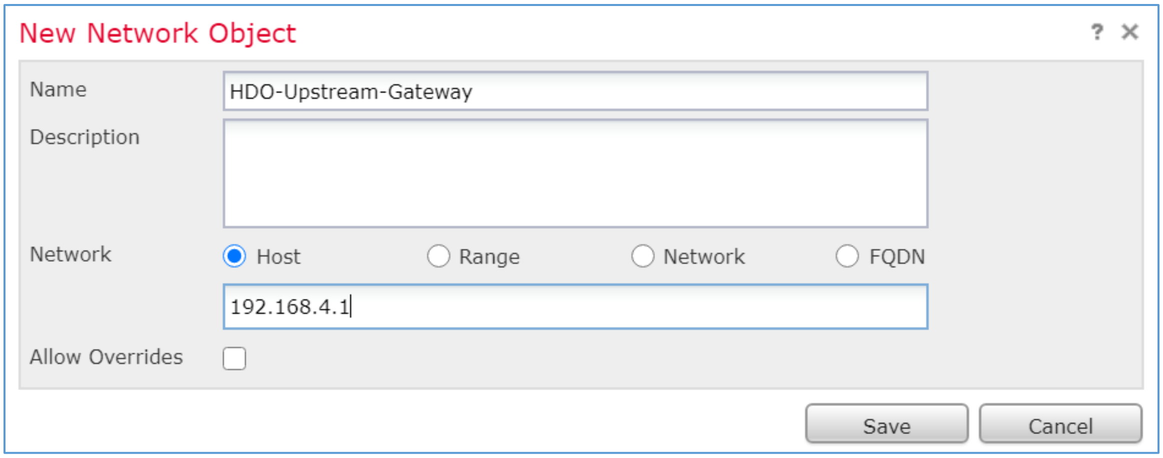


4. The Add Static Route Configuration pop-up window appears. Fill out the following information:
   a. **Interface:** WAN
   b. **Selected Network:** any-ipv4

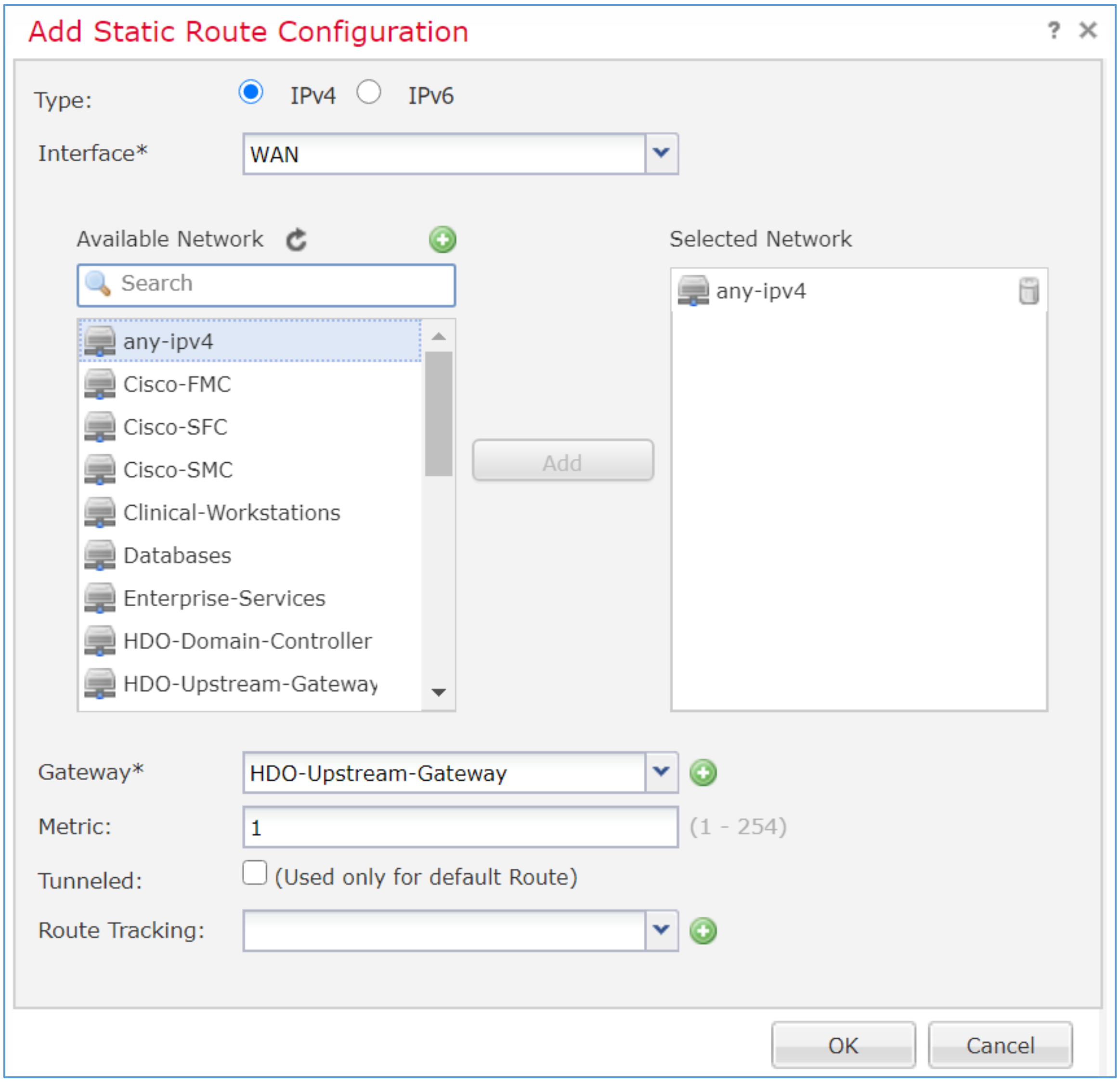
5. Click the **plus symbol** next to **Gateway.**



6. The New Network Object pop-up window appears. Fill out the following information:
   a. **Name:** HDO-Upstream-Gateway
   b. **Network (Host):** 192.168.4.1
7. Click **Save.**

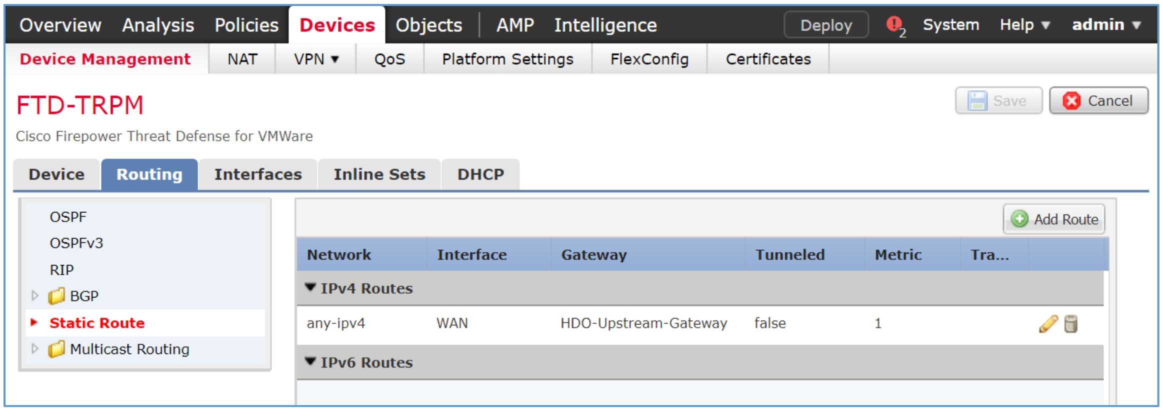


792 8. Click **OK.**



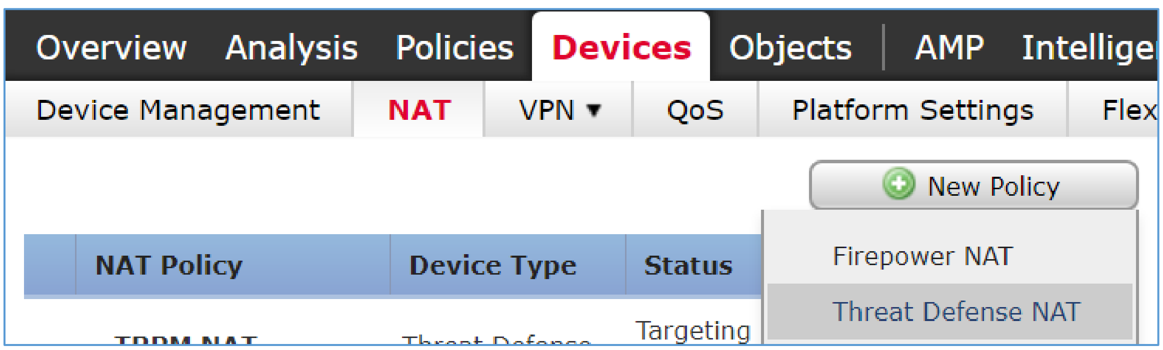
9. Click **Save.**

10. Click **Deploy.** Verify that the static route has been set correctly. From **Devices,** when selecting the **Routing** tab, the **Static Route** will indicate the network routing settings. The screen displays the static route settings in a table format that includes values for **Network, Interface, Gateway, Tunneled,** and **Metric.** The static route applies to the IP addressing that has been specified, where network traffic traverses the interface. Note the **Gateway** value. The **Tunneled** and **Metric** values display the default value.

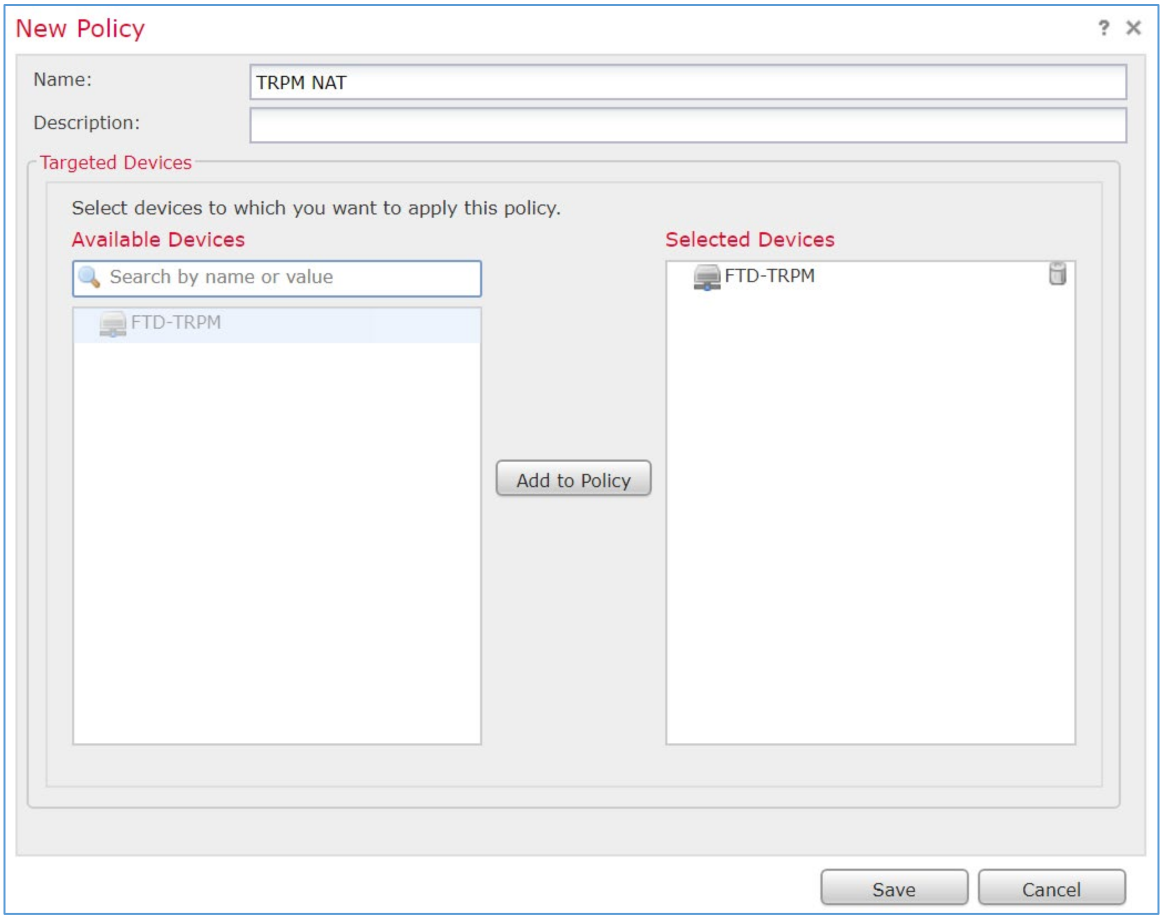


Configure Cisco FTD Network Address Translation (NAT)

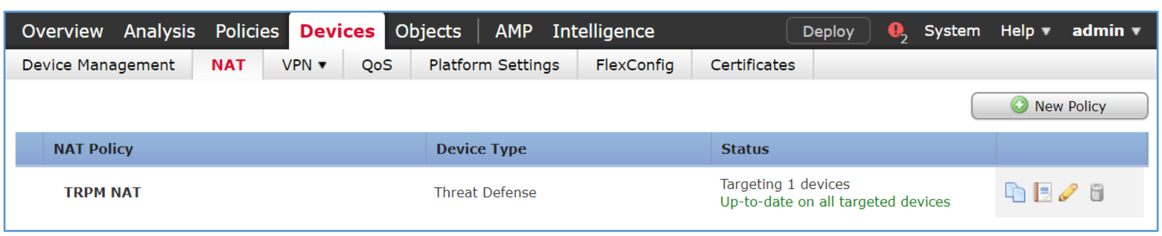
1. Click **Devices > NAT.**
2. Click **New Policy > Threat Defense NAT.**



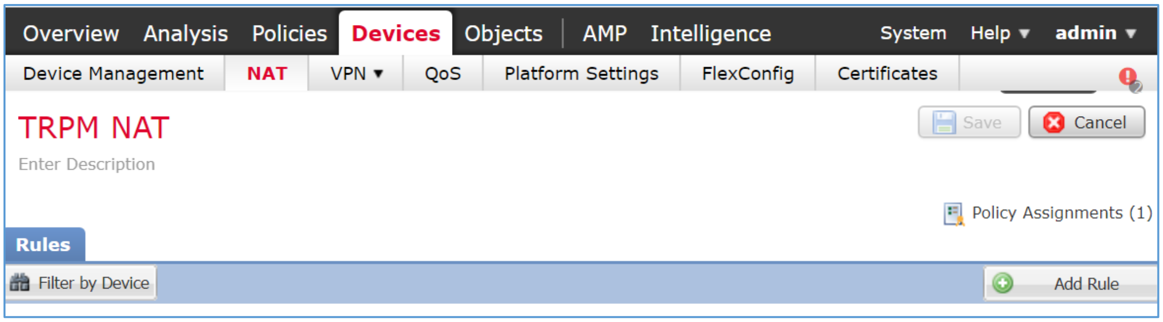
3. The New Policy pop-up window appears. Fill out the following information:
   a. **Name:** TRPM NAT
   b. **Selected Devices:** FTD-TRPM
4. Click **Save.**



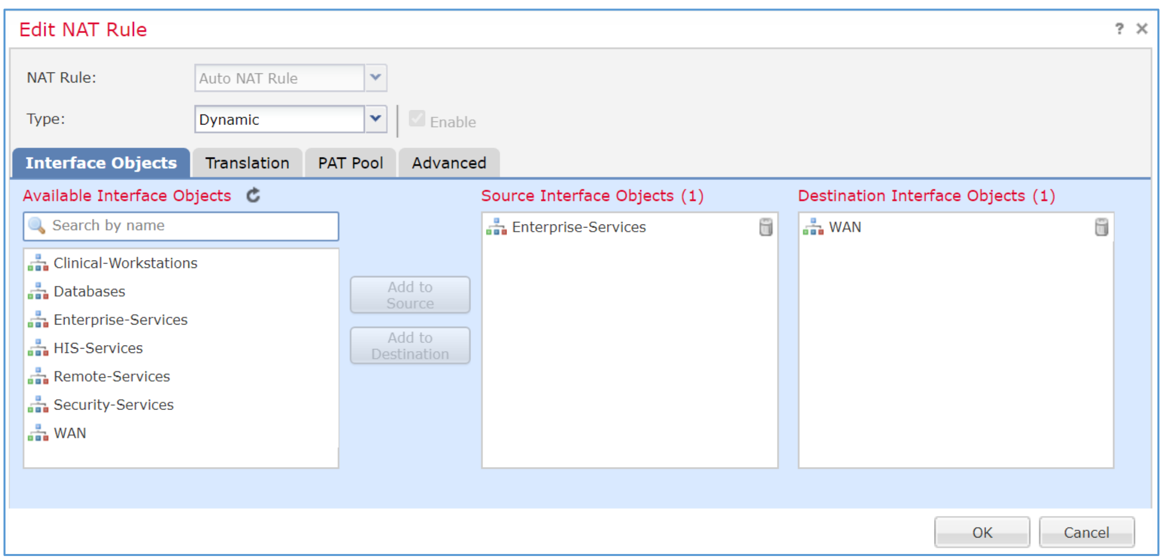
807 5. Click the **edit symbol** for **TRPM NAT.**



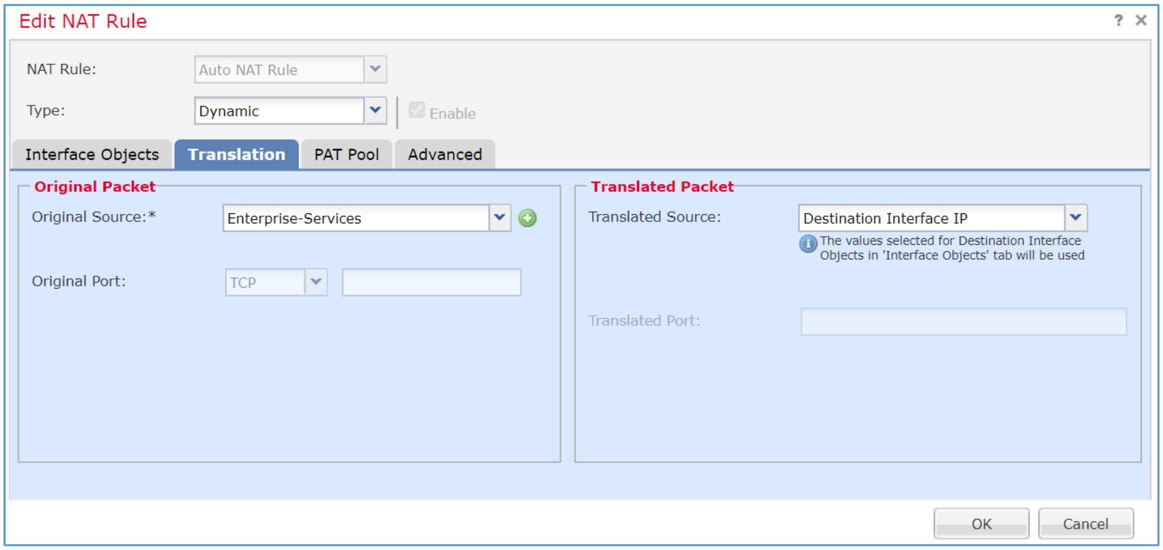
808 6. Click **Add Rule.**



7. The Edit NAT Rule pop-up window appears. Under **Interface Objects,** fill out the following information:
    a. **NAT Rule:** Auto NAT Rule
    b. **Type:** Dynamic
    c. **Source Interface Objects:** Enterprise-Services
    d. **Destination Interface Objects:** WAN
8. Click **Translation.**



9. Under **Translation,** fill out the following information:
    a. **Original Source:** Enterprise-Services
    b. **Translated Source:** Destination Interface IP
10. Click **OK.**

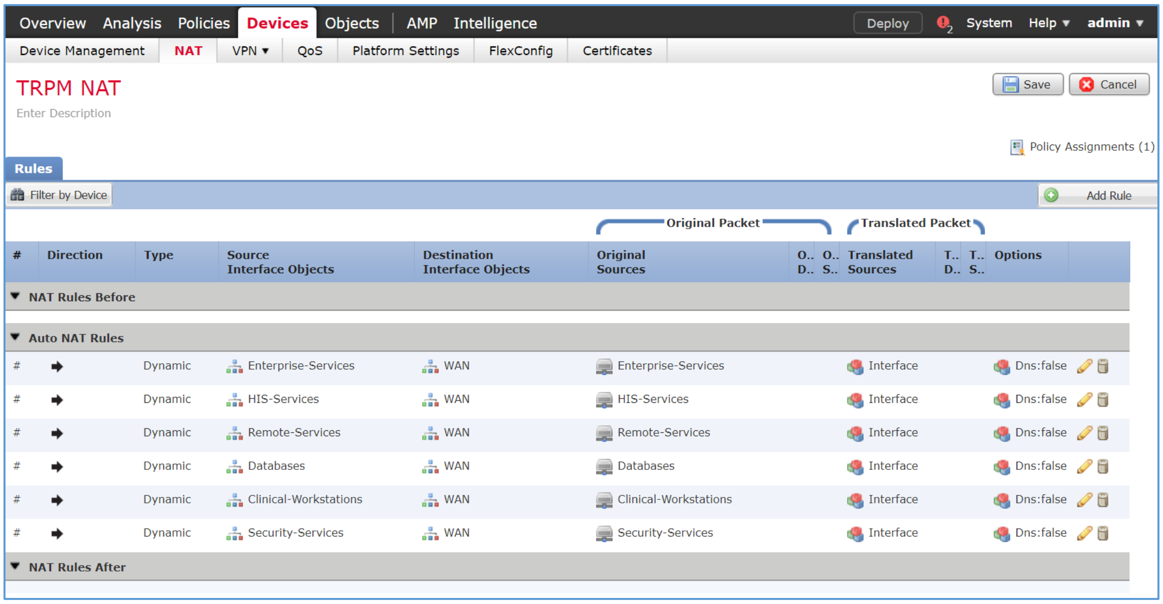


11. Create additional rules following the same pattern described above, populating the respective information for each rule. Values for each rule are described below:
    a. HIS-Services
        i. **NAT Rule:** Auto NAT Rule
        ii. **Type:** Dynamic
        iii. **Source Interface Objects:** HIS-Services
        iv. **Destination Interface Objects:** WAN
        v. **Original Source:** HIS-Services
        vi. **Translated Source:** Destination Interface IP
    b. Remote-Services
        i. **NAT Rule:** Auto NAT Rule
        ii. **Type:** Dynamic
        iii. **Source Interface Objects:** Remote-Services
        iv. **Destination Interface Objects:** WAN
        v. **Original Source:** Remote-Services
        vi. **Translated Source:** Destination Interface IP

c. Databases
   i. **NAT Rule:** Auto NAT Rule
   ii. **Type:** Dynamic
   iii. **Source Interface Objects:** Databases
   iv. **Destination Interface Objects:** WAN
   v. **Original Source:** Databases
   vi. **Translated Source:** Destination Interface IP
d. Clinical-Workstations
   i. **NAT Rule:** Auto NAT Rule
   ii. **Type:** Dynamic
   iii. **Source Interface Objects:** Clinical-Workstations
   iv. **Destination Interface Objects:** WAN
   v. **Original Source:** Clinical-Workstations
   vi. **Translated Source:** Destination Interface IP
e. Security-Services
   i. **NAT Rule:** Auto NAT Rule
   ii. **Type:** Dynamic
   iii. **Source Interface Objects:** Security-Services
   iv. **Destination Interface Objects:** WAN
   v. **Original Source:** Security-Services
   vi. **Translated Source:** Destination Interface IP

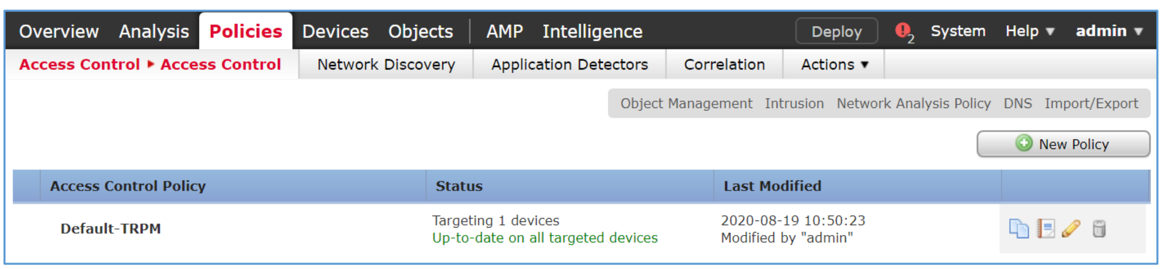
12. Click **Save.**
13. Click **Deploy.** Verify the NAT settings through the **Devices** screen. The **NAT** rules are displayed in a table format. The table includes values for **Direction** of the NAT displayed as a directional arrow, the **NAT Type,** the **Source Interface Objects** (i.e., the security zone IP networks), the **Destination Interface Objects,** the **Original Sources** (i.e., these addresses correspond to the IP network from where the network traffic originates), the **Translated Sources,** and **Options.** The

settings indicate that IP addresses from the configured security zones are translated behind the Interface IP address.

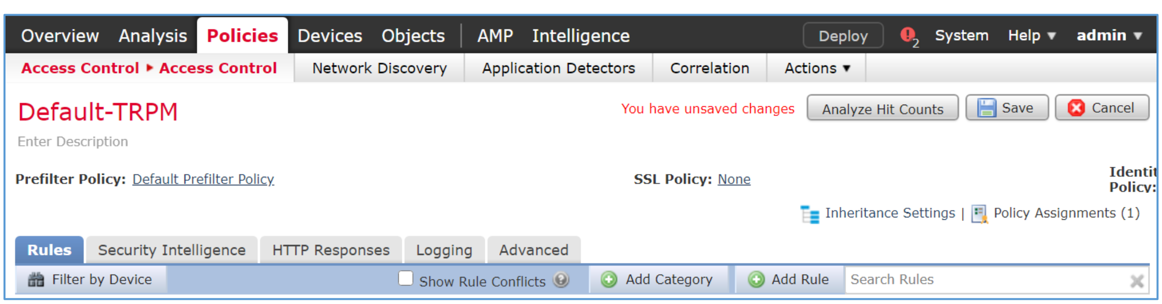


Configure Cisco FTD Access Control Policy

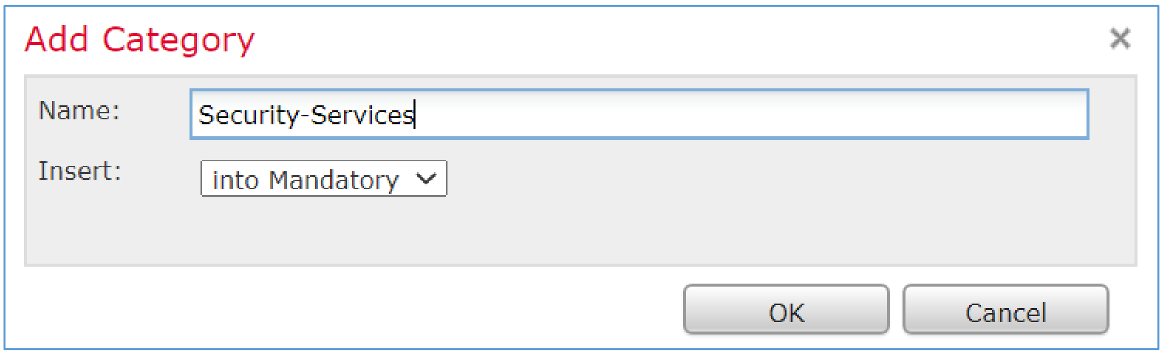
1. Click **Polices > Access Control > Access Control.**
2. Click the **edit symbol** for **Default-TRPM.**



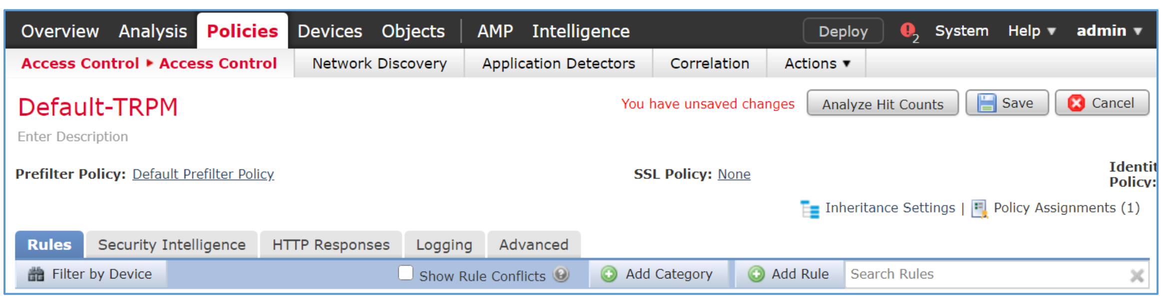
3. Click **Add Category.**



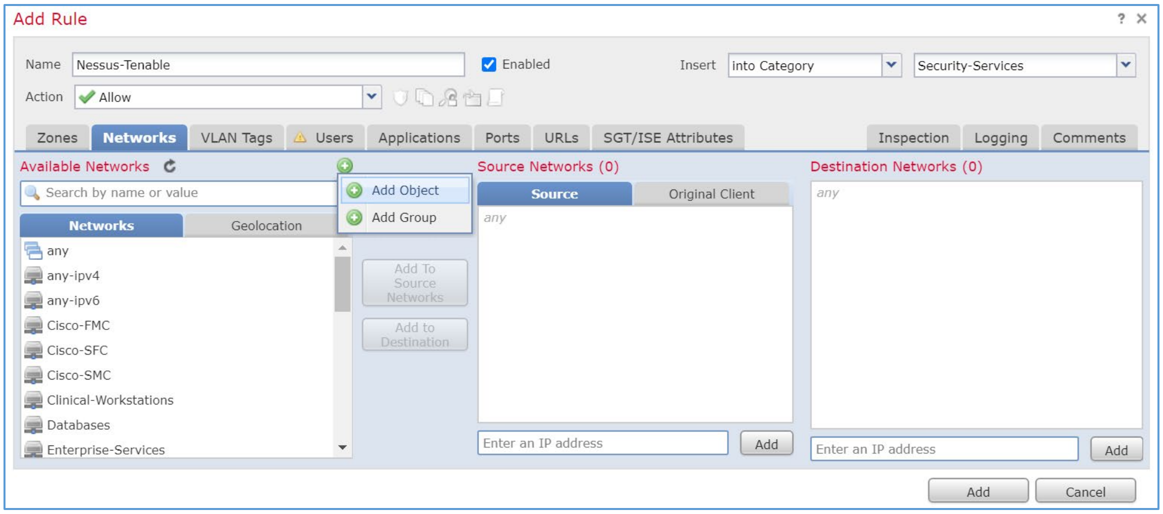
4. Fill out the following information:
    a. **Name:** Security Services
    b. **Insert:** into Mandatory
5. Click **OK.**



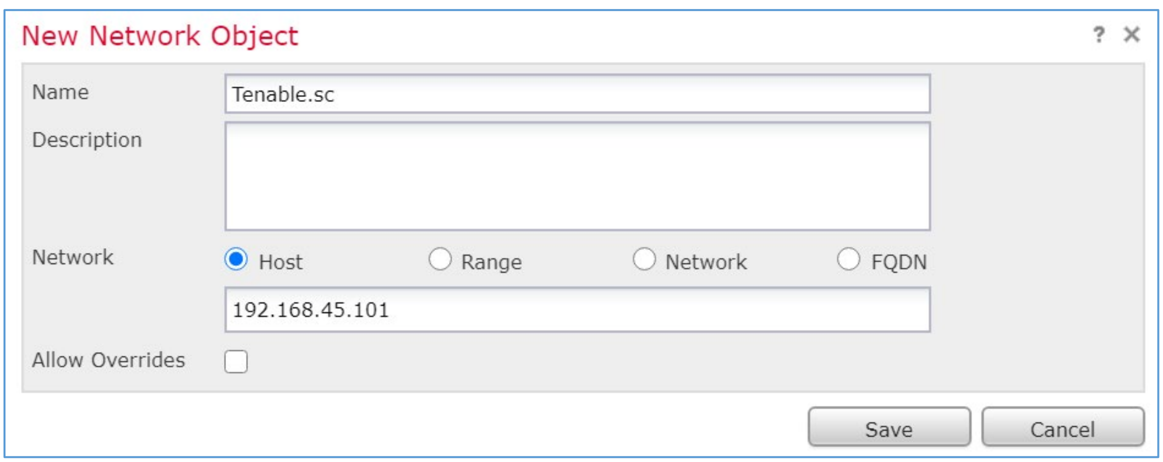
6. Repeat the previous steps of **Add Category** section for each network segment in the architecture.
7. Click **Add Rule.**



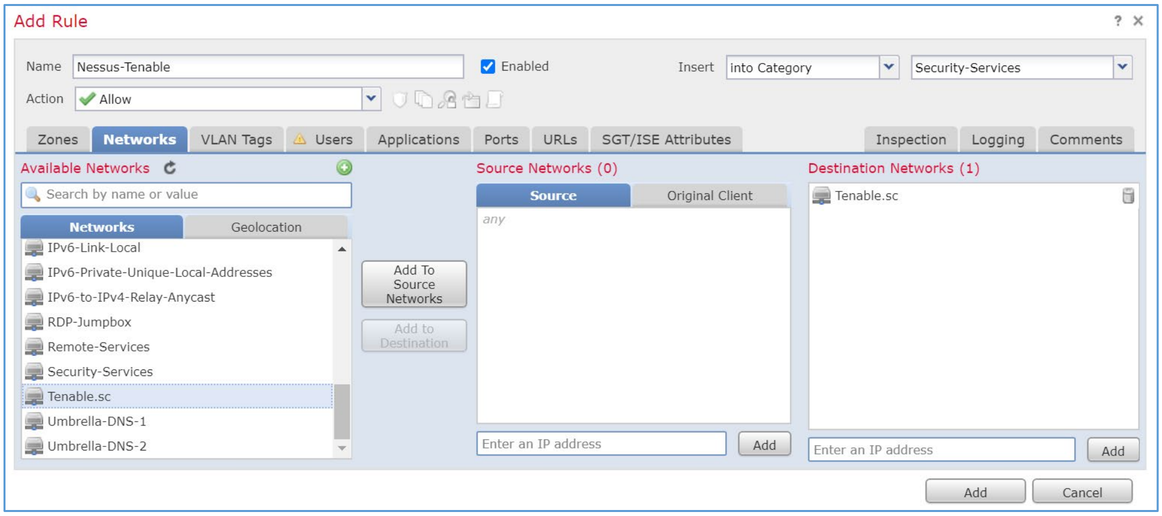
8. When the Add Rule screen appears, fill out the following information:
    a. **Name:** Nessus-Tenable
    b. **Action:** Allow
    c. **Insert:** into Category, Security Services
    d. Under **Networks,** click the **plus symbol** next to **Available Networks,** and select **Add Object.**



9. When the New Network Object pop-up window appears, fill out the following information:
    a. **Name:** Tenable.sc
    b. **Network (Host):** 192.168.45.101
10. Click **Save.**

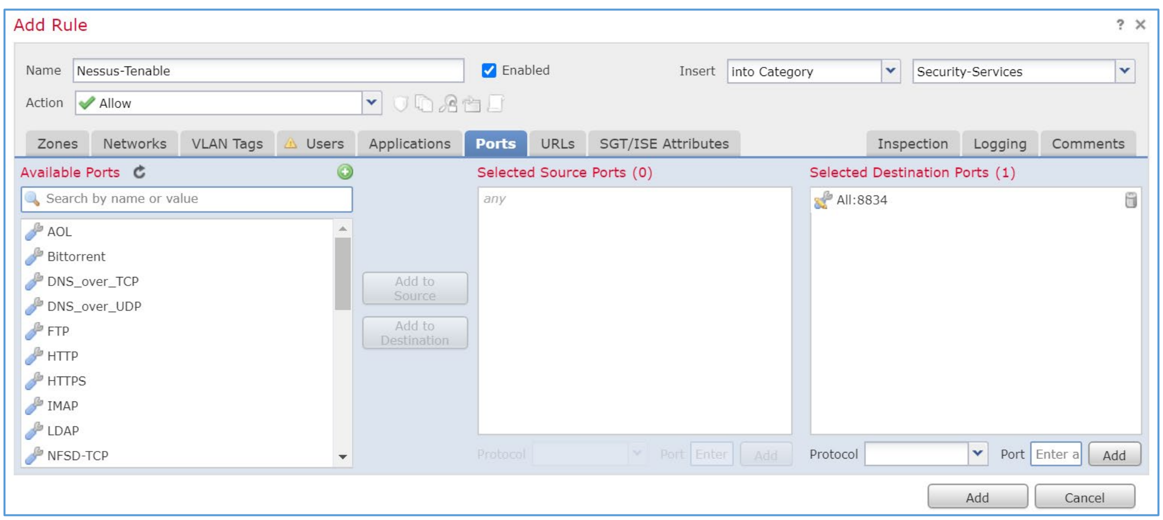


11. In the Add Rule screen, under the **Networks** tab, set **Destination Networks** to **Tenable.sc.**
12. Click **Ports.**



13. In the Add Rule screen, under the **Ports** tab, set **Selected Destination Ports** to **8834.**

14. Click **Add.**



15. Repeat the previous steps for any network requirement rules if necessary.

16. Click **Save.**

17. Click **Deploy.**

2.2.3 Security Continuous Monitoring

The project team implemented a set of tools that included Cisco Stealthwatch, Cisco Umbrella, and LogRhythm to address security continuous monitoring. This practice guide uses Cisco Stealthwatch for

NetFlow analysis. Cisco Umbrella is a service used for DNS-layer monitoring. The LogRhythm tools aggregate log file information from across the HDO infrastructure and allow behavioral analytics.

2.2.3.1 Cisco Stealthwatch

Cisco Stealthwatch provides network visibility and analysis through network telemetry. This project integrates Cisco Stealthwatch with Cisco Firepower, sending NetFlow directly from the Cisco FTD appliance to a Stealthwatch Flow Collector (SFC) for analysis.

Cisco Stealthwatch Management Center (SMC) Appliance Information

CPU: 4

RAM: 16 GB

Storage: 200 GB (Thick Provision)

Network Adapter 1: VLAN 1348

Operating System: Linux

Cisco SMC Appliance Installation Guide

Install the appliance according to the instructions detailed in the *Cisco Stealthwatch Installation and Configuration Guide 7.1* [8].

Cisco SFC Appliance Information

CPU: 4

RAM: 16 GB

Storage: 300 GB (Thick Provision)

Network Adapter 1: VLAN 1348

Operating System: Linux

Cisco SFC Appliance Installation Guide

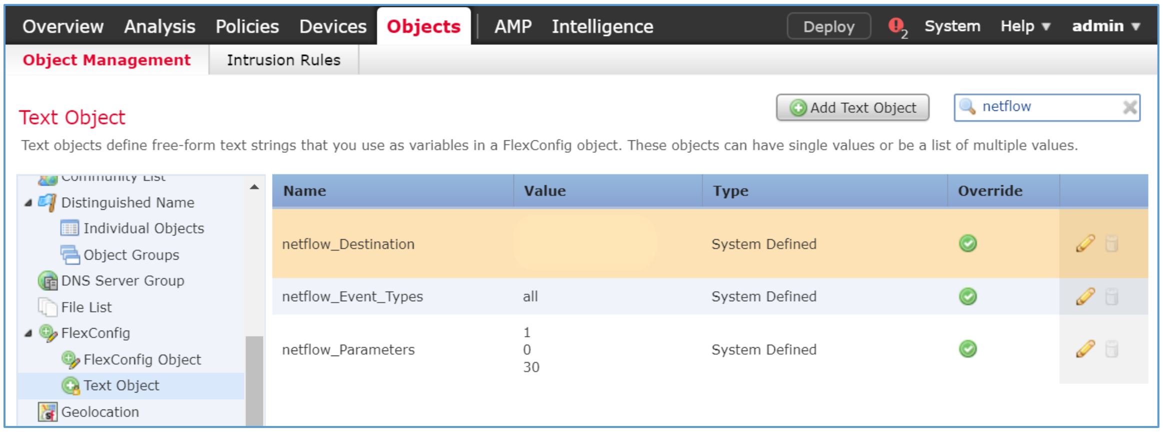
Install the appliance according to the instructions detailed in the *Cisco Stealthwatch Installation and Configuration Guide 7.1* [8].

Accept the default port value **2055** for NetFlow.

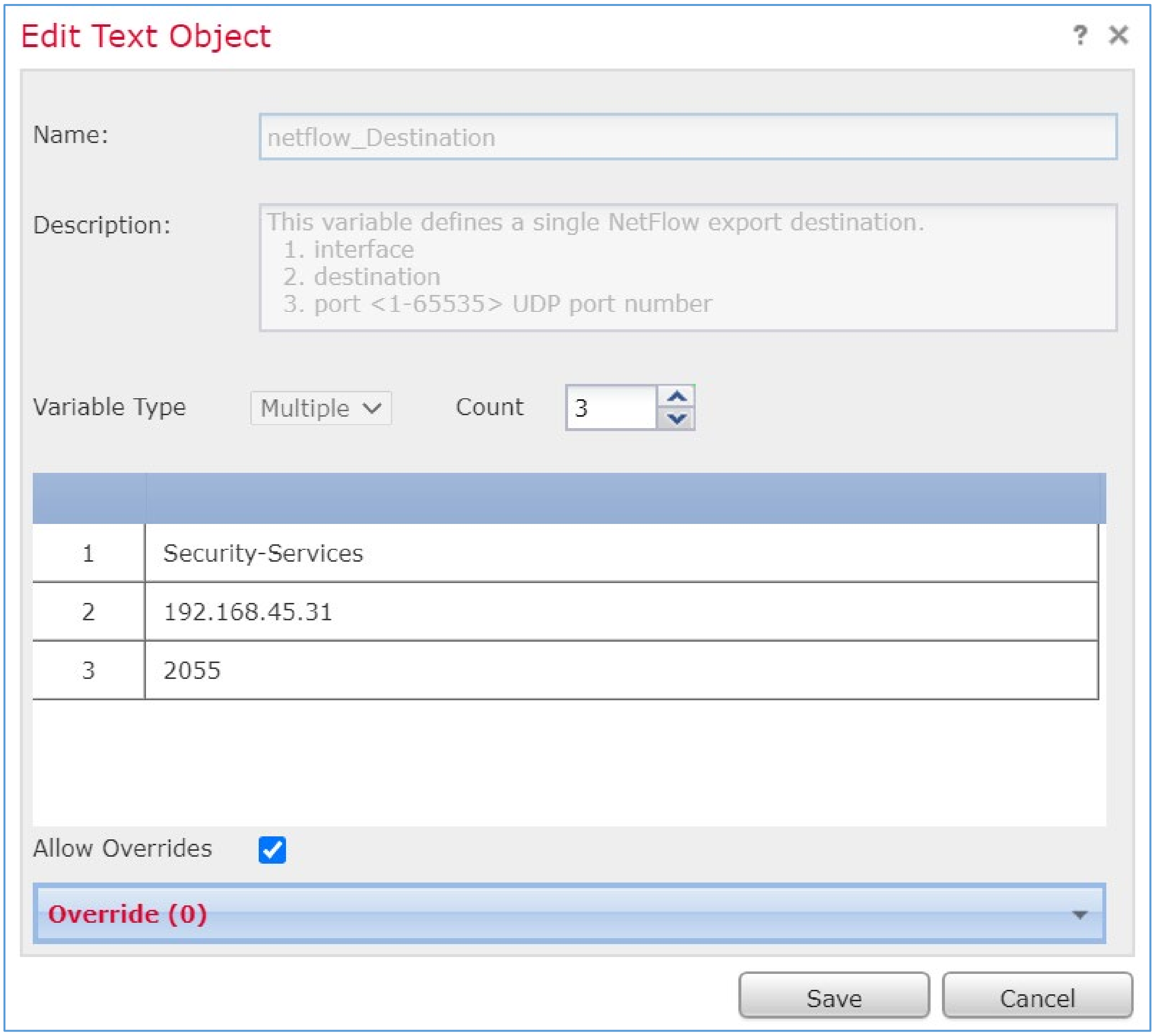
Configure Cisco FTD NetFlow for Cisco SFC

1. Click **Objects > Object Management > FlexConfig > Text Object.**

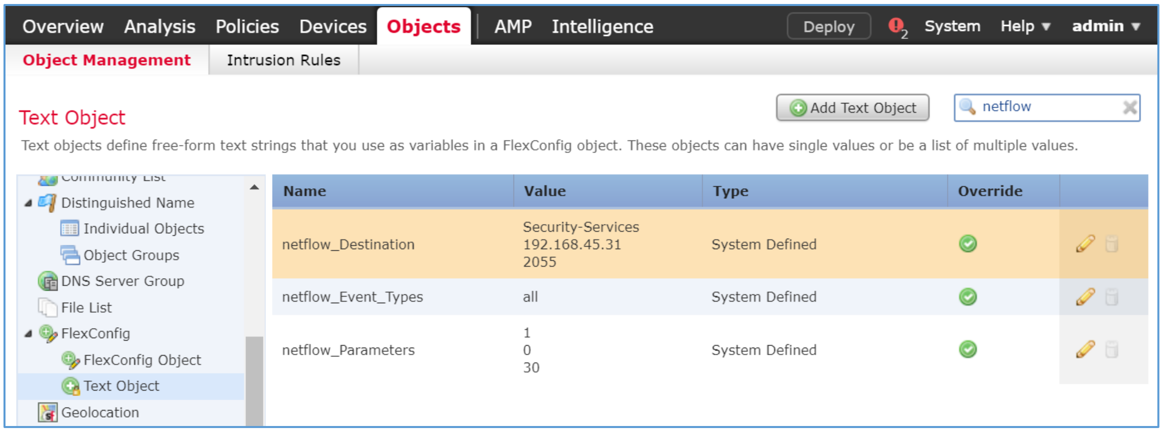
2. In the **search box,** type `netflow`.
3. Click the **edit symbol** for **netflow_Destination.**



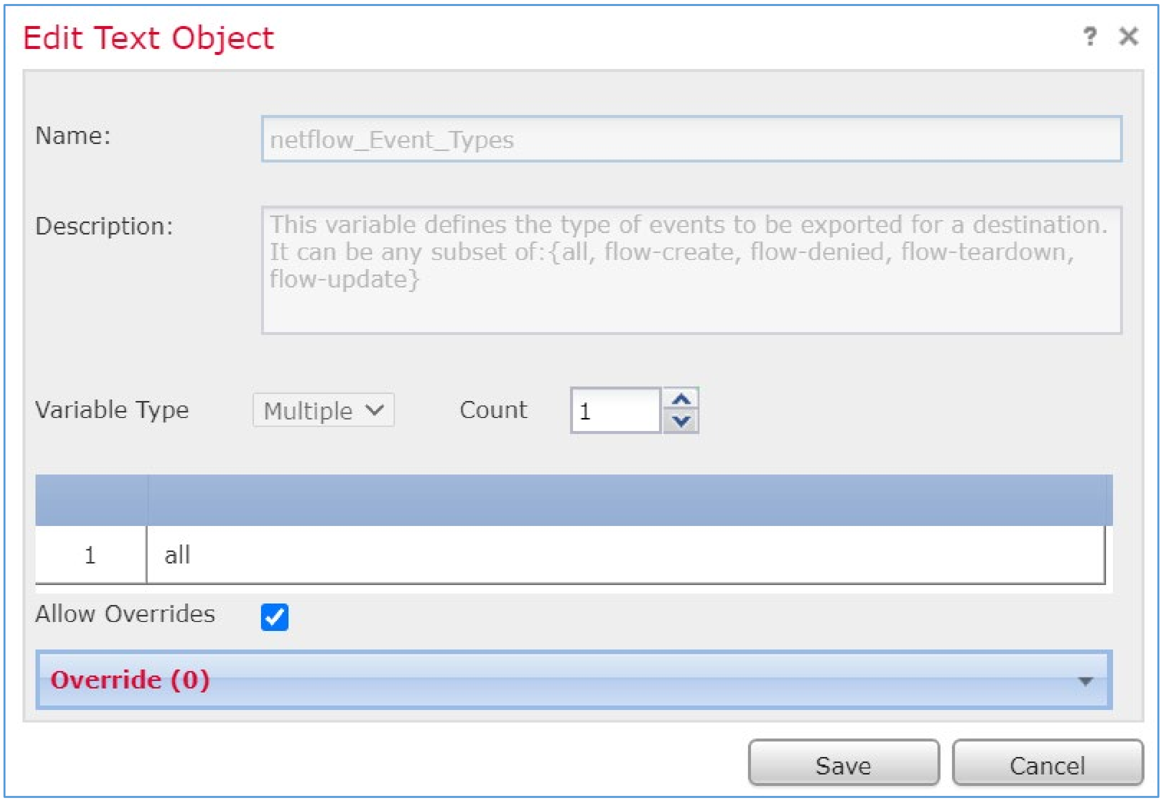
4. When the Edit Text Object pop-up window appears, fill out the following information:
   a. **Count:** 3
   b. **1:** Security Services
   c. **2:** 192.168.45.31
   d. **3:** 2055
   e. **Allow Overrides:** checked
5. Click **Save.**



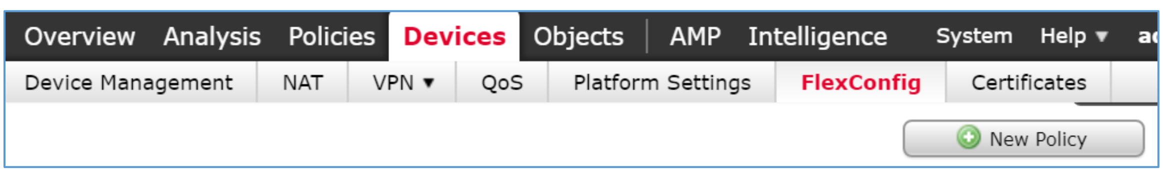
6. Click the **edit symbol** for **netflow_Event_Types.**



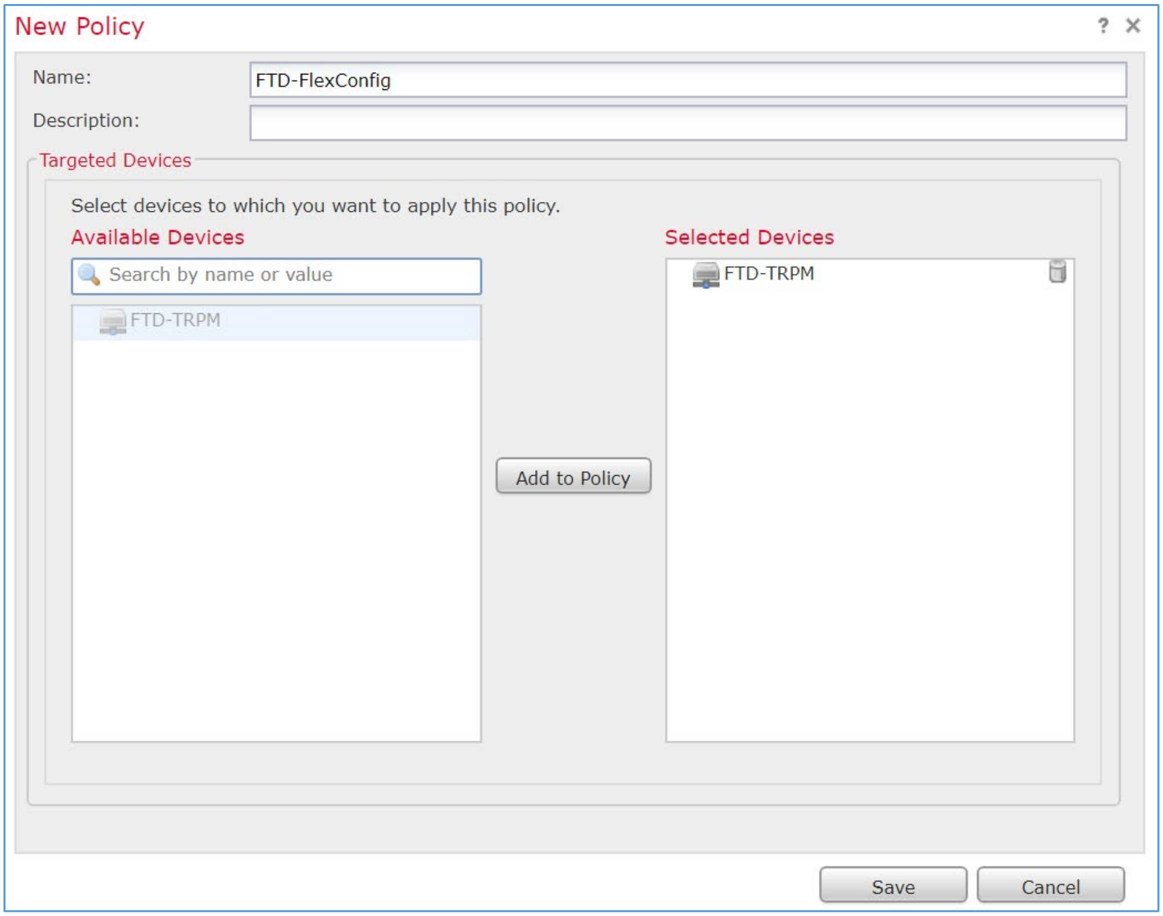
7. When the Edit Text Object pop-up window appears, fill out the following information:
    a. **Count:** 1
    b. **1:** All
    c. **Allow Overrides:** checked
8. Click **Save.**



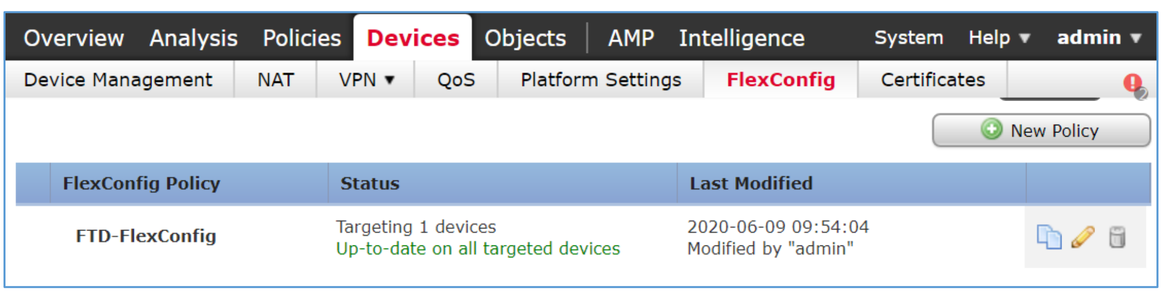
9. Click **Devices > FlexConfig.**
10. Click **New Policy.**



11. When the New Policy screen appears, fill out the following information:
    a. **Name:** FTD-FlexConfig
    b. **Selected Devices:** FTD-TRPM
12. Click **Save.**

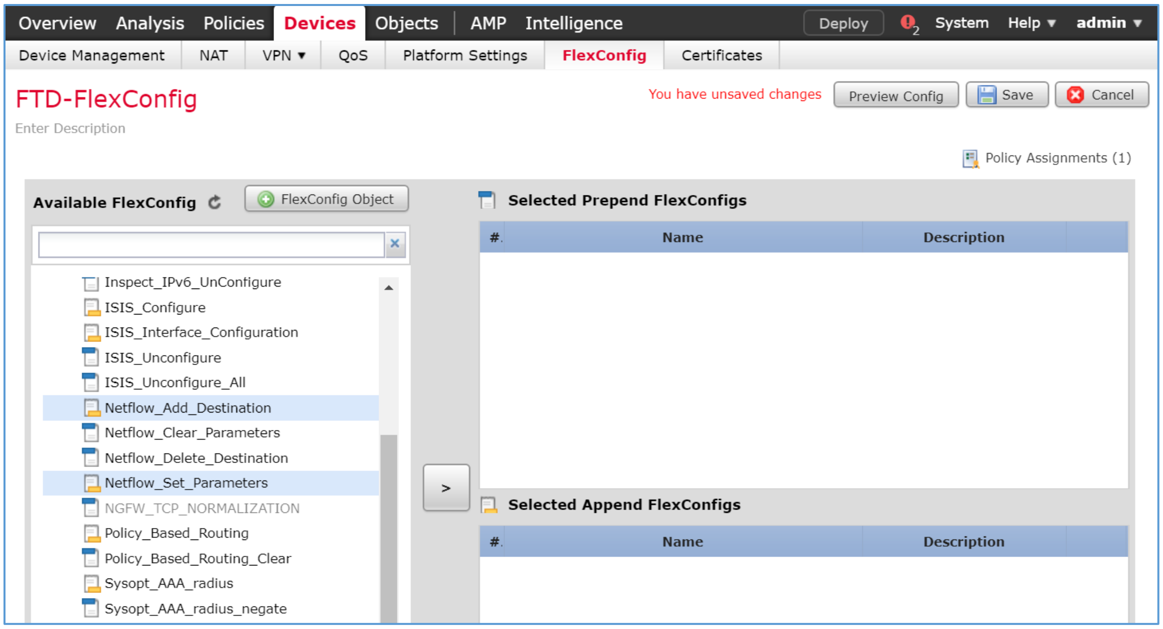


13. Click the **edit symbol** for **FTD-FlexConfig.**



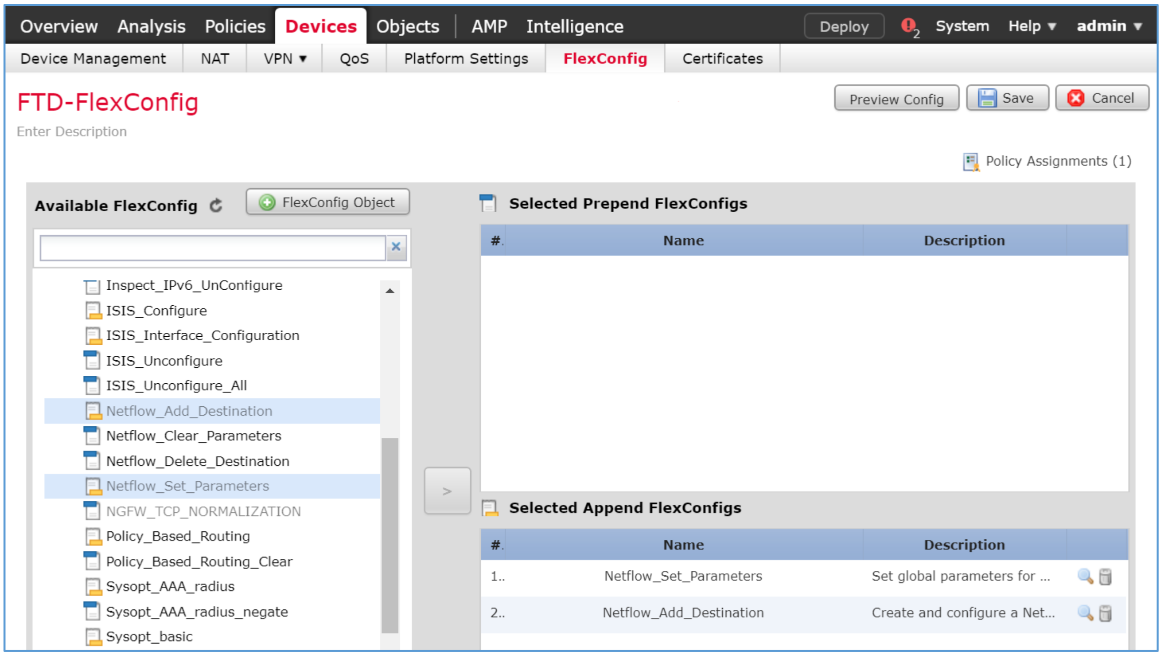
14. Under the **Devices** tab, select **Netflow_Add_Destination** and **Netflow_Set_Parameters.**

15. Click the **right-arrow symbol** to move the selections to the **Selected Append FlexConfigs** section.



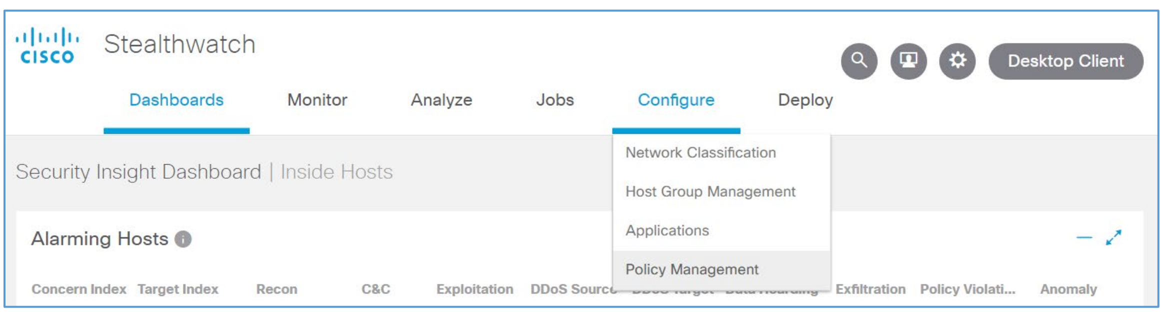
16. Click **Save.**

17. Click **Deploy.** From the **Devices** screen, verify the **FlexConfig** settings. Select the **FlexConfig** tab. The **NetFlow** configurations appear in the lower right of the screen as a table. Under **Selected Append FlexConfigs,** the table includes columns labeled **#** which corresponds to the number of configurations that have been made: **Name** and **Description.**

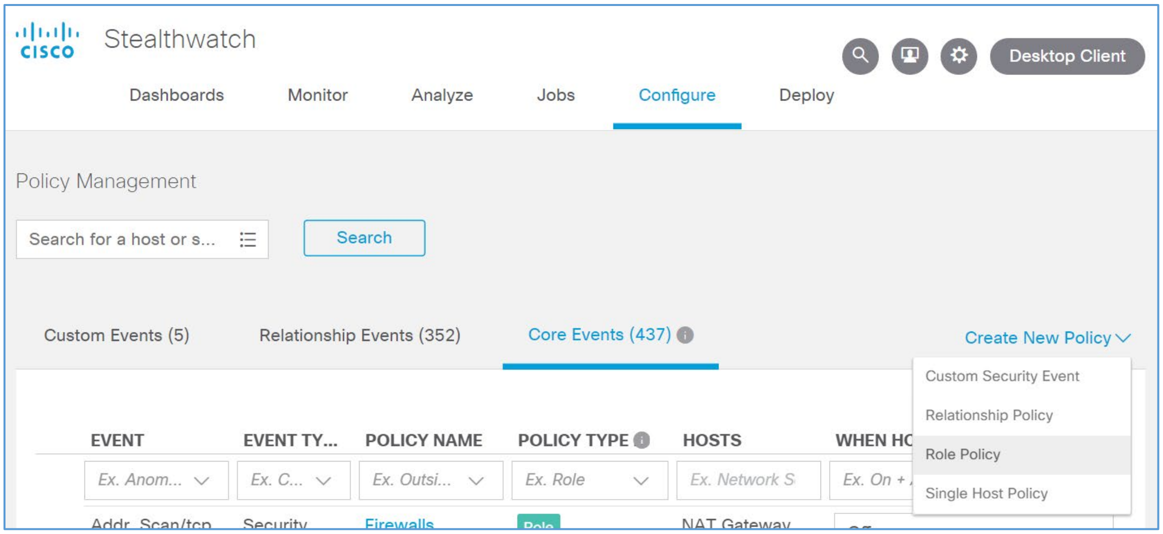


Create a Custom Policy Management Rule

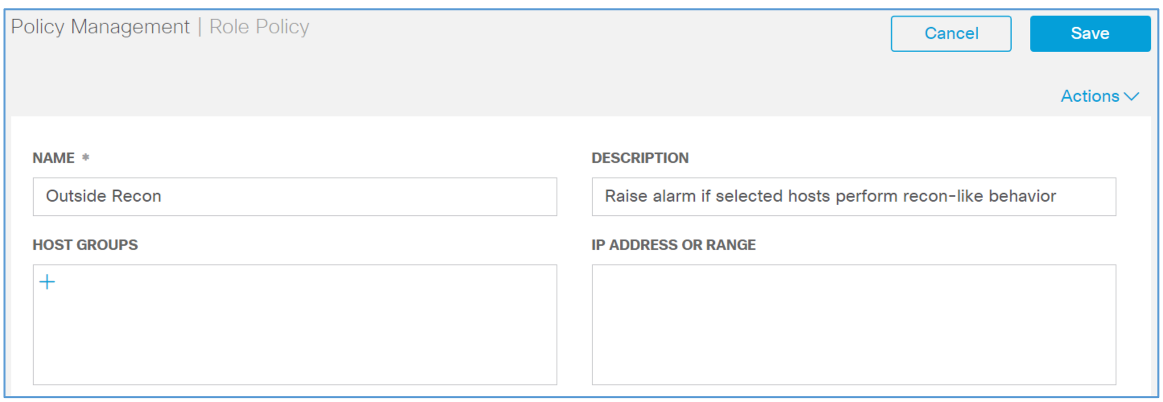
1. Click **Configure > Policy Management.**



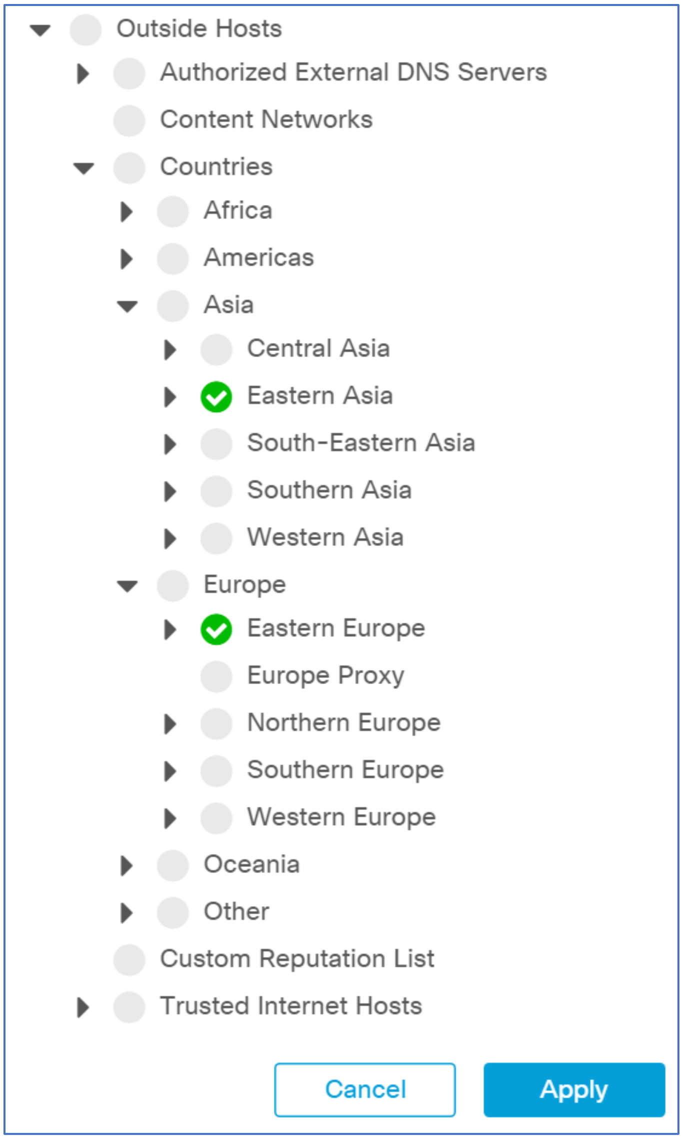
2. Click **Create New Policy > Role Policy.**



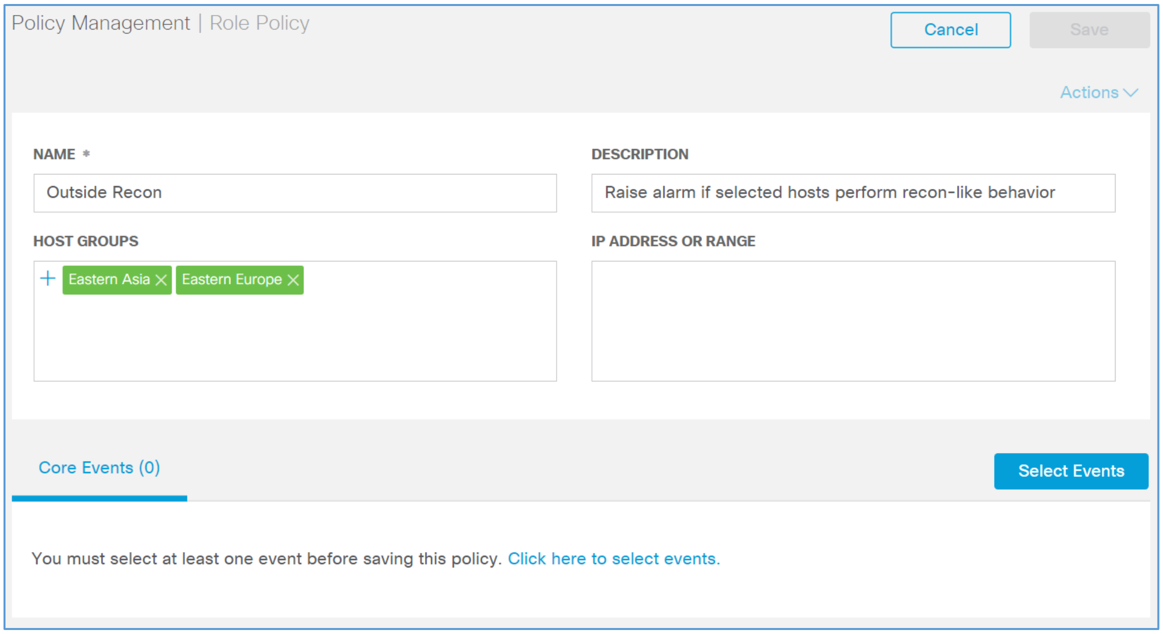
3. Give the policy a **name** and **description.**
4. Under **Host Groups,** click the **plus symbol.**



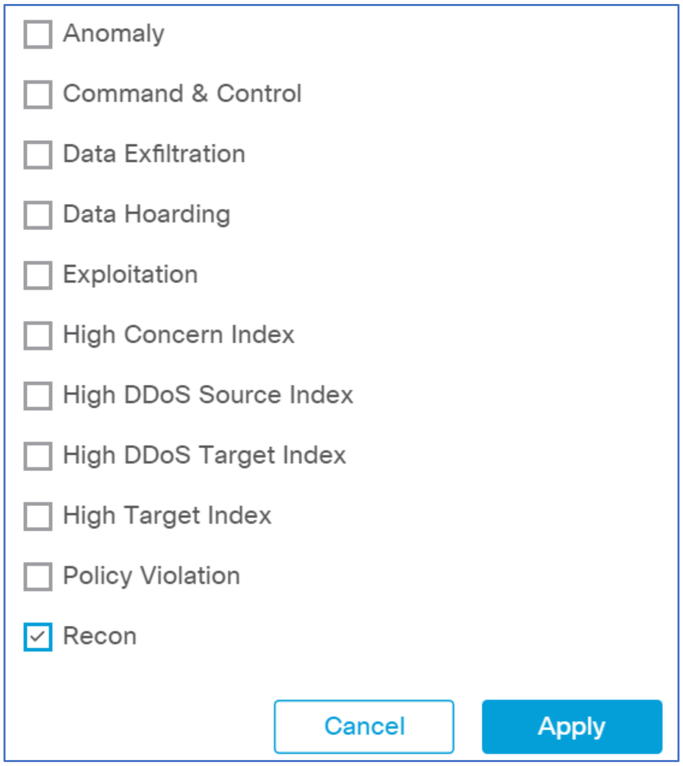
5. Under **Outside** Hosts, select **Eastern Asia** and **Eastern Europe.**
6. Click **Apply.**



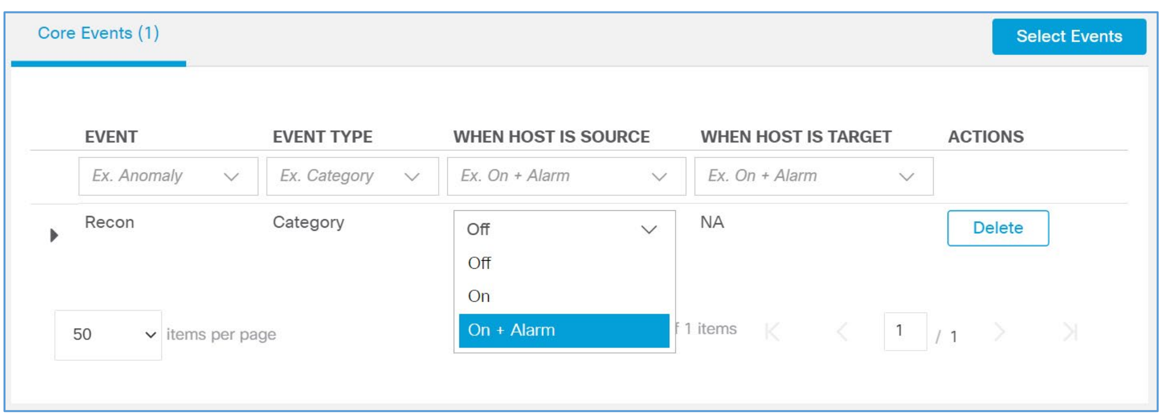
7. Under **Core Events,** click **Select Events.**



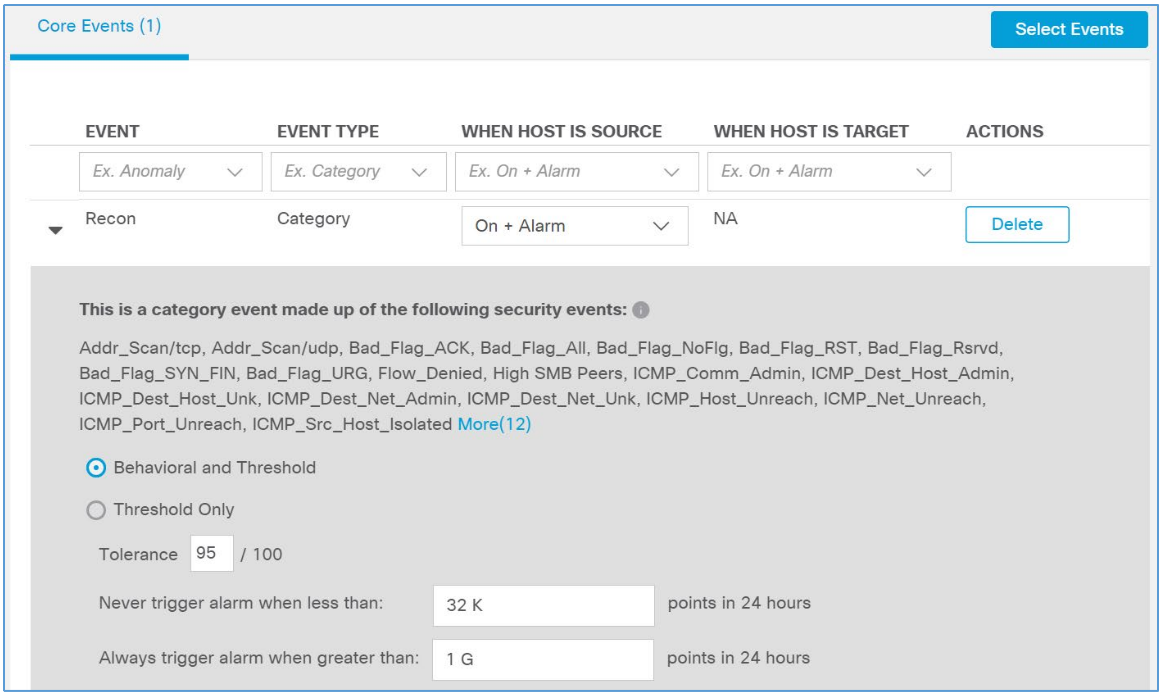
8. Select **Recon.**
9. Click **Apply.**



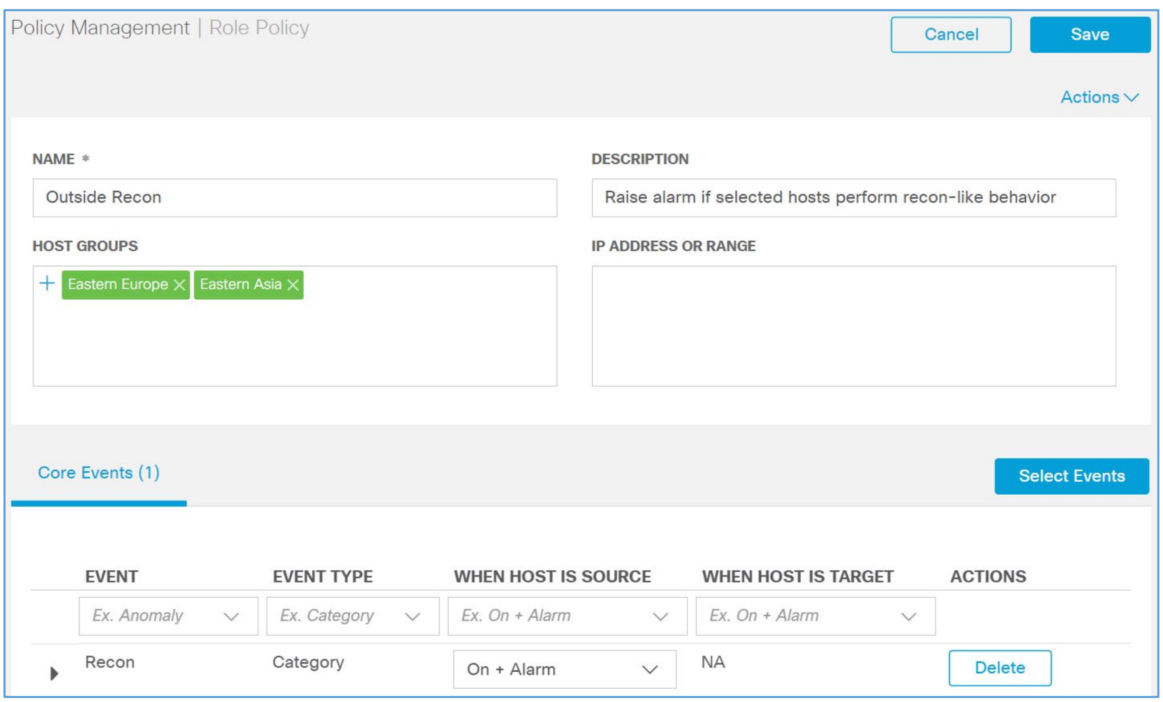
10. Under **Core Events > Recon** > **When Host is Source**, select **On + Alarm.**
11. Click the **expand arrow** next to **Recon.**



12. Select **Behavioral and Threshold.**



13. Click **Save.**



2.2.3.2 Cisco Umbrella

Cisco Umbrella is a cloud service that provides protection through DNS-layer security. Engineers deployed two Umbrella virtual appliances in the HDO to provide DNS routing and protection from malicious web services.

<u>Cisco Umbrella Forwarder Appliance Information</u>

CPU: 1

RAM: 0.5 GB

Storage: 6.5 GB (Thick Provision)

Network Adapter 1: VLAN 1327

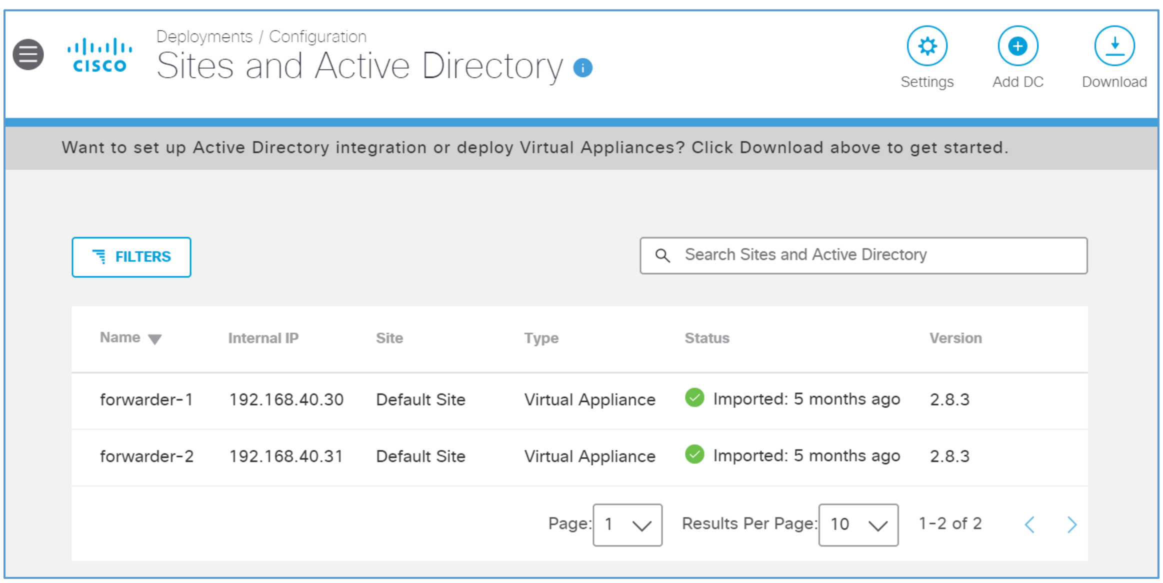
Operating System: Linux

<u>Cisco Umbrella Forwarder Appliance Installation Guide</u>

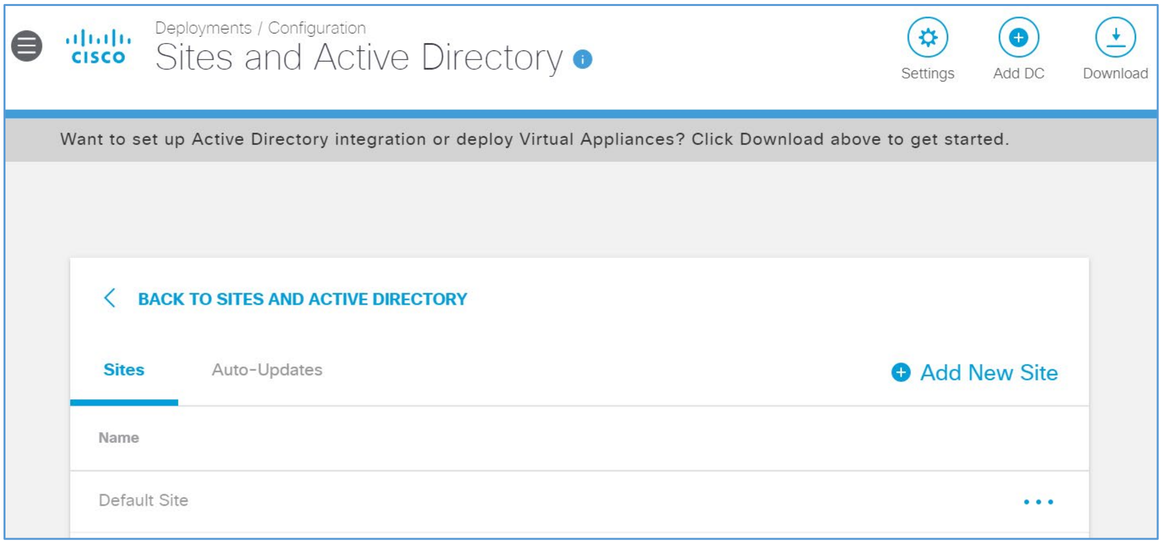
Install the appliance according to the instructions detailed in Cisco's Deploy VAs in VMware guidance [9].

<u>Create an Umbrella Site</u>

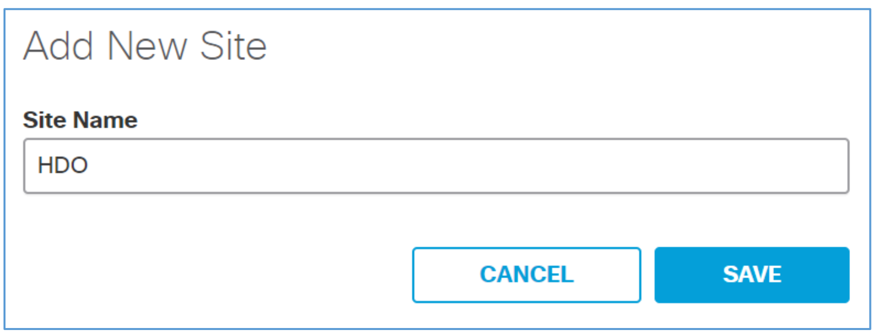
1. Click **Deployments > Configuration > Sites and Active Directory.**
2. Click **Settings.**



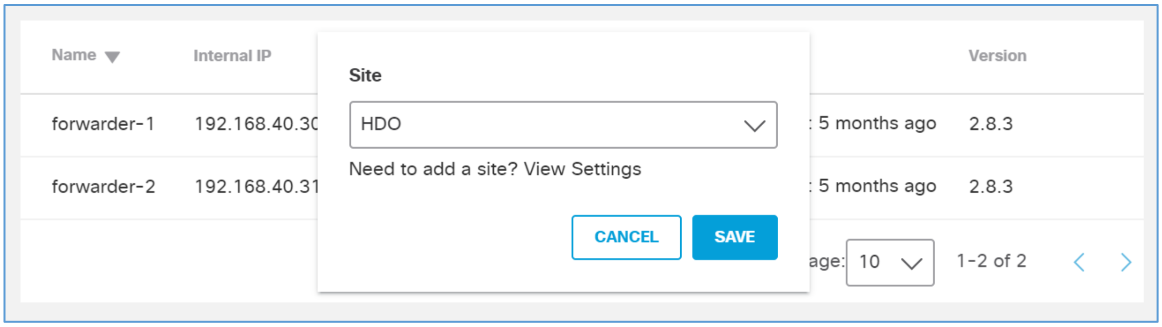
3. Click **Add New Site.**



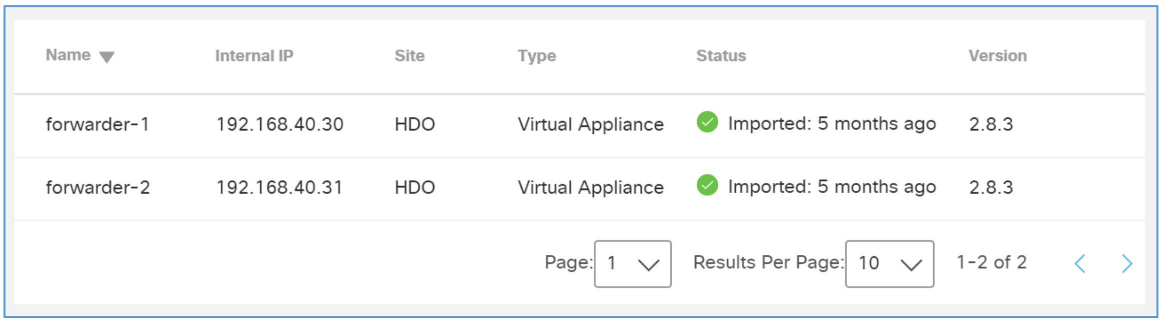
4. In the Add New Site pop-up window, set **Name** to **HDO.**
5. Click **Save.**



6. Click **Deployments > Configuration > Sites and Active Directory.**
7. Click the **edit symbol** for the Site of **forwarder-1.**
8. Under Site, select **HDO.**
9. Click **Save.**

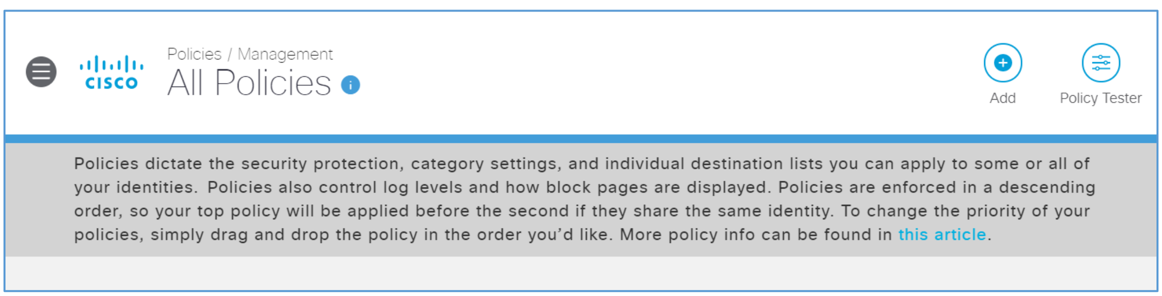


10. Repeat the previous steps for **forwarder-2.**



Configure an Umbrella Policy

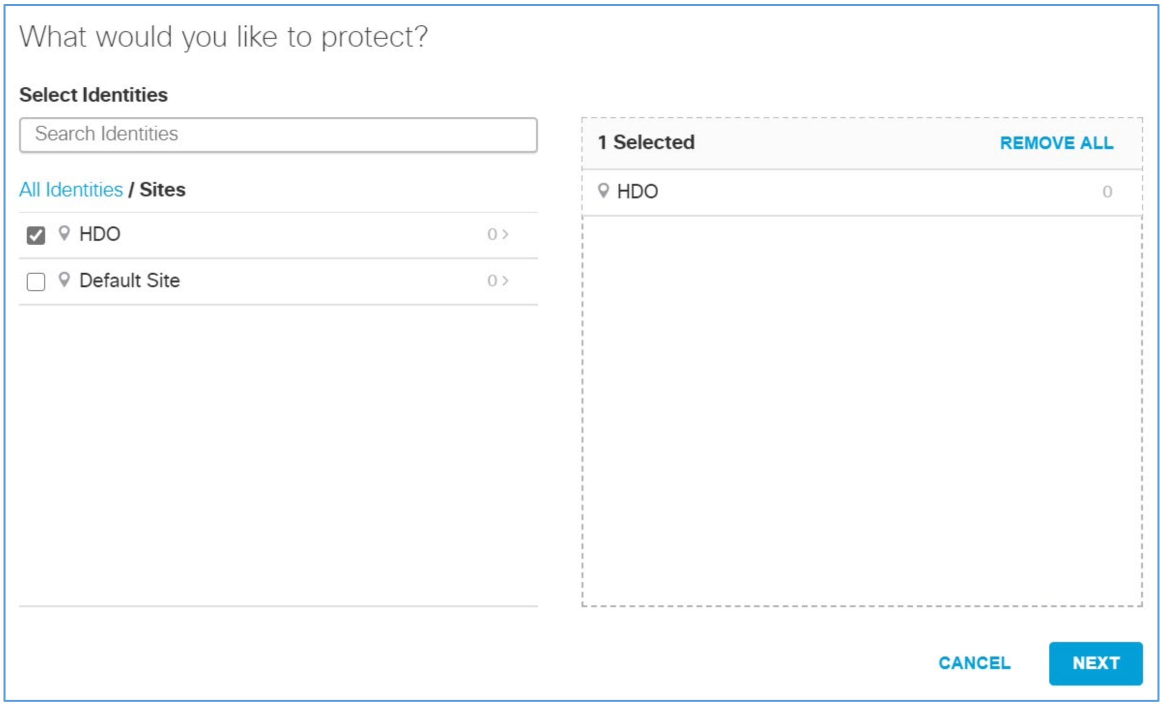
1. Click **Policies > Management > All Policies.**
2. Click **Add.**



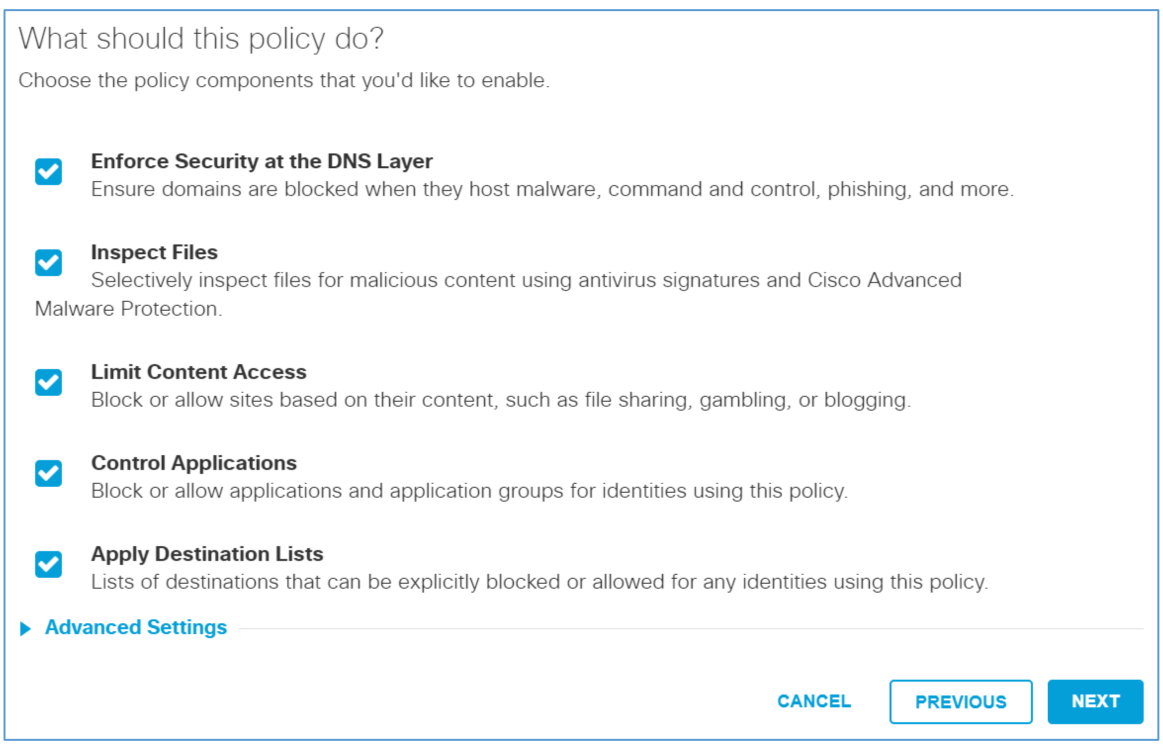
3. Expand the **Sites** identity.

994 4. Select **HDO.**

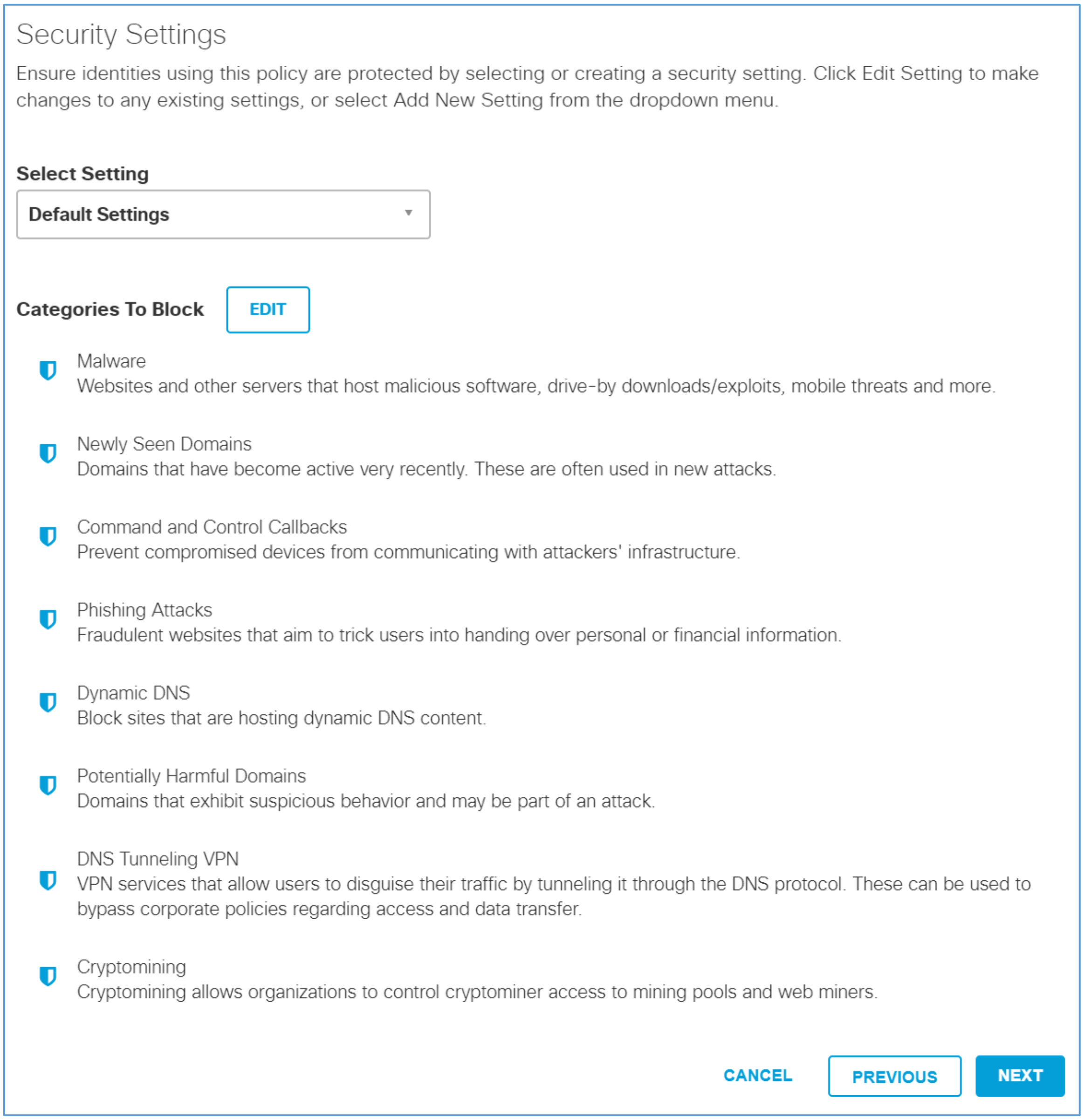
995 5. Click **Next.**


What would you like to protect?
Select Identities
Search Identities
All Identities / Sites
HDO
Default Site
1 Selected
REMOVE ALL
HDO
CANCEL
NEXT

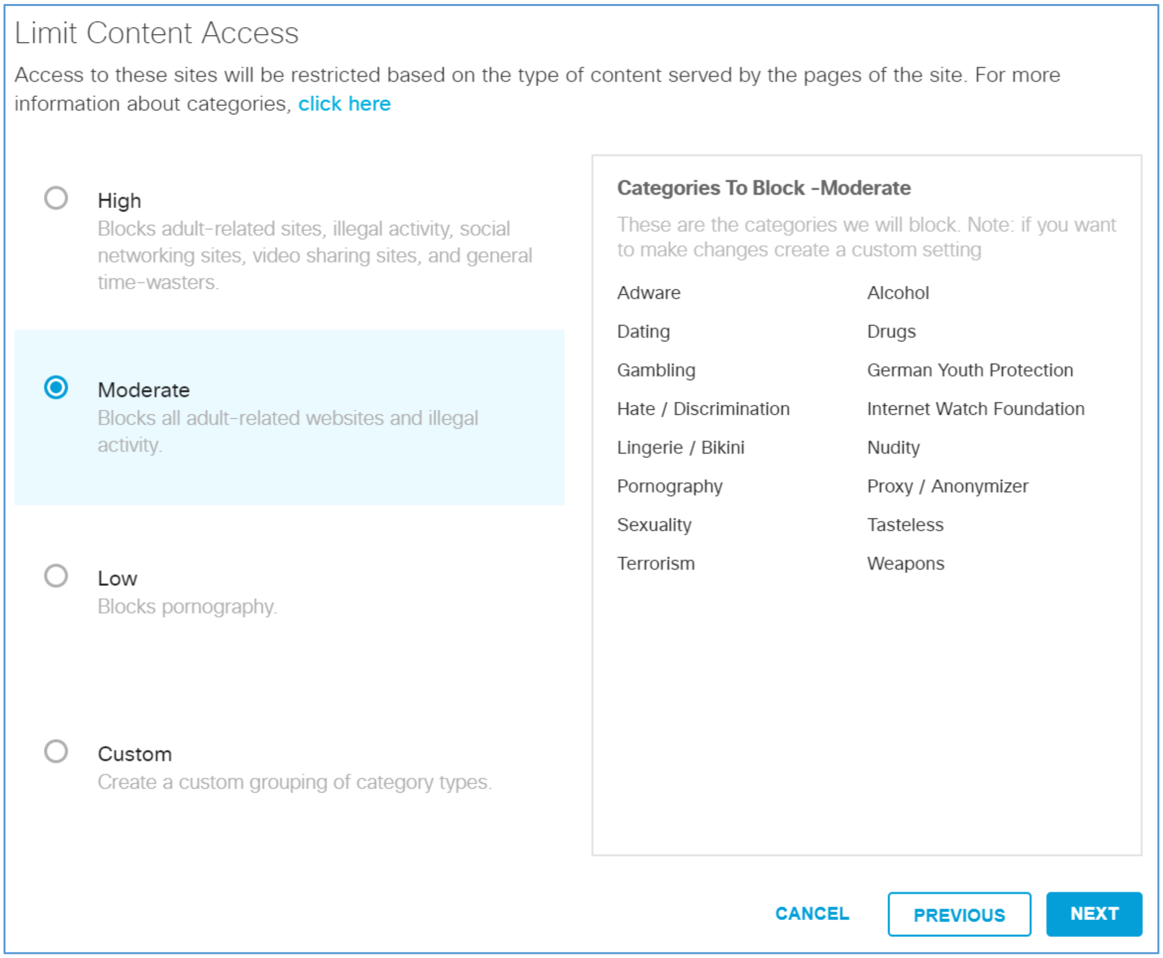
6. Click **Next.**


What should this policy do?
Choose the policy components that you'd like to enable.
Enforce Security at the DNS Layer
Ensure domains are blocked when they host malware, command and control, phishing, and more.
Inspect Files
Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.
Limit Content Access
Block or allow sites based on their content, such as file sharing, gambling, or blogging.
Control Applications
Block or allow applications and application groups for identities using this policy.
Apply Destination Lists
Lists of destinations that can be explicitly blocked or allowed for any identities using this policy.
Advanced Settings
CANCEL
PREVIOUS
NEXT

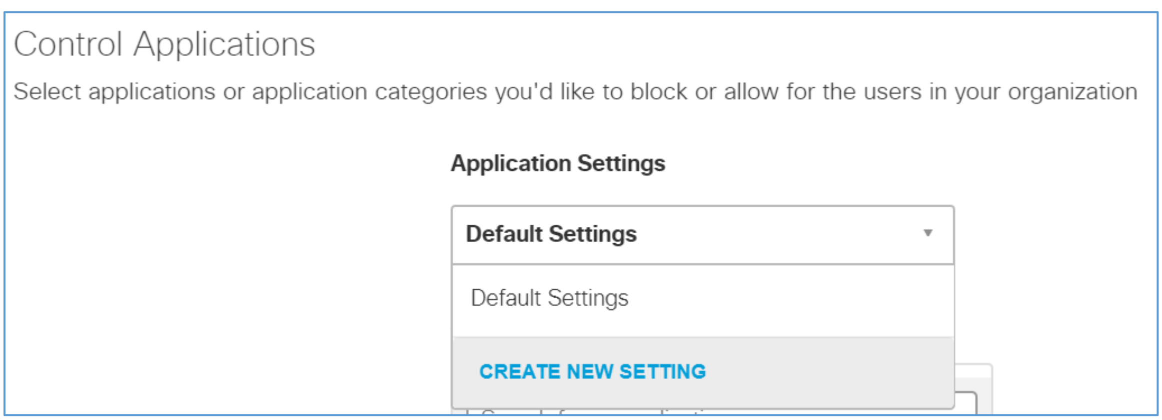
7. Click **Next.**



8. Select **Moderate.**
9. Click **Next.**



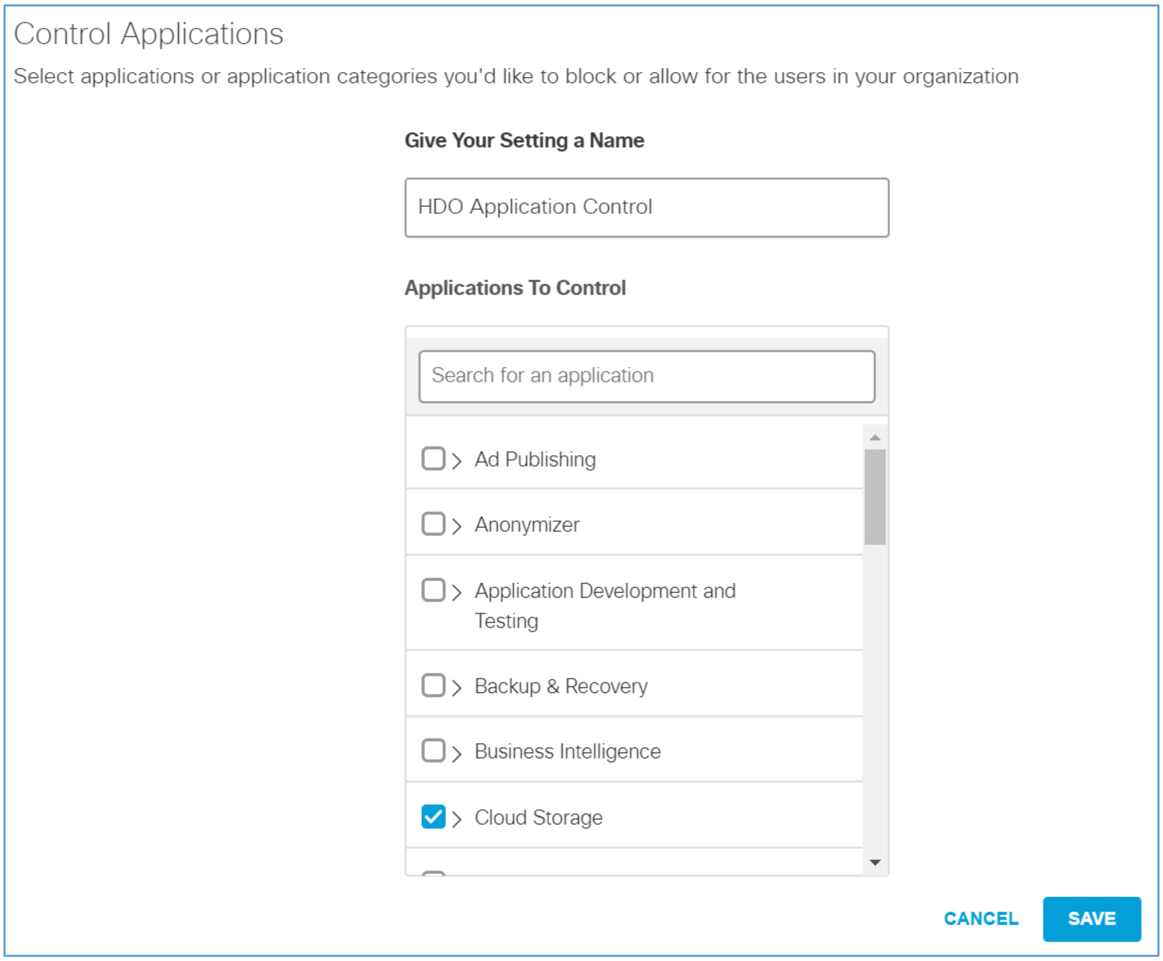
10. Under Application Settings, use the drop-down menu to select **Create New Setting.**



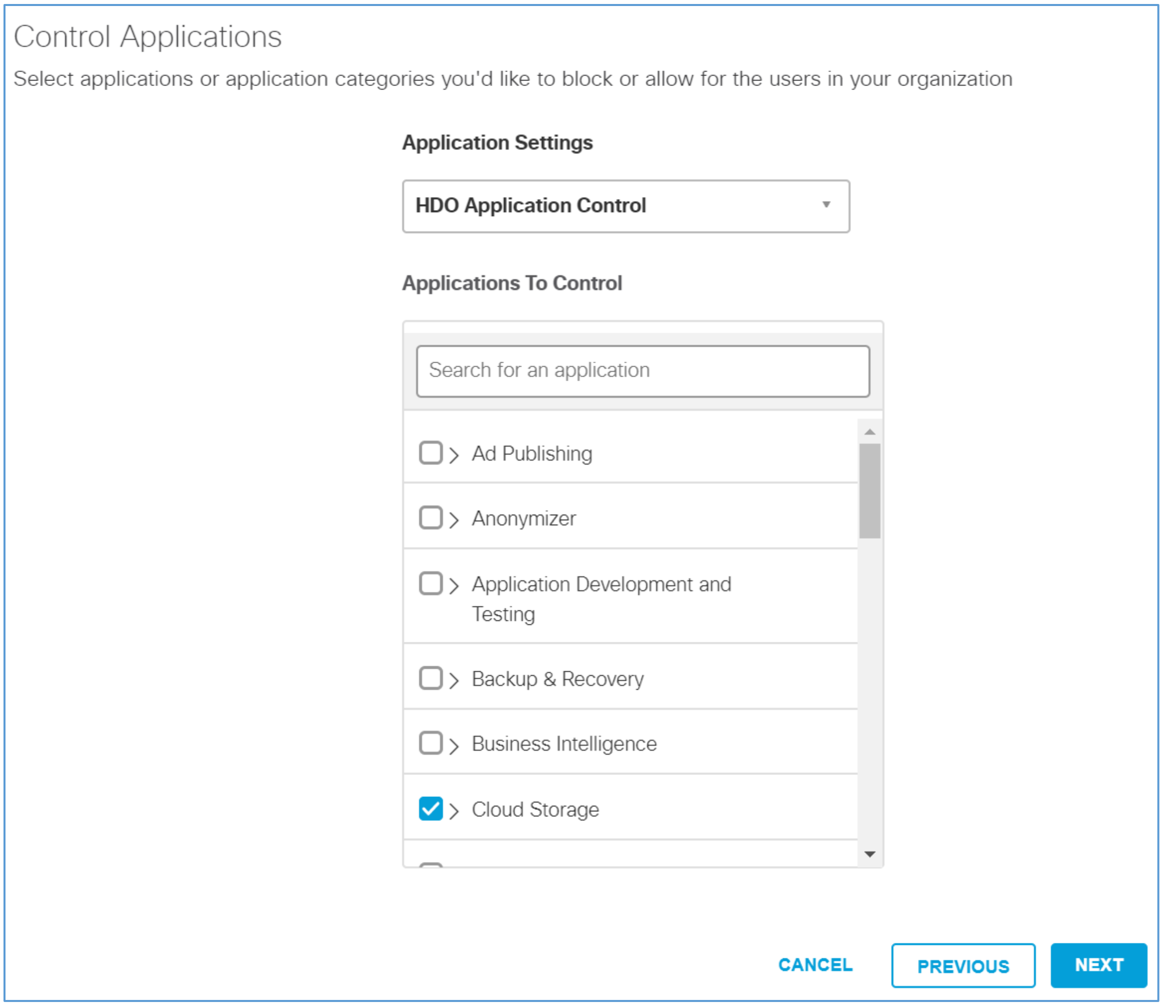
11. Under the Control Applications screen, fill out the following information:

   a. **Name:** HDO Application Control
   b. **Applications to Control:** Cloud Storage

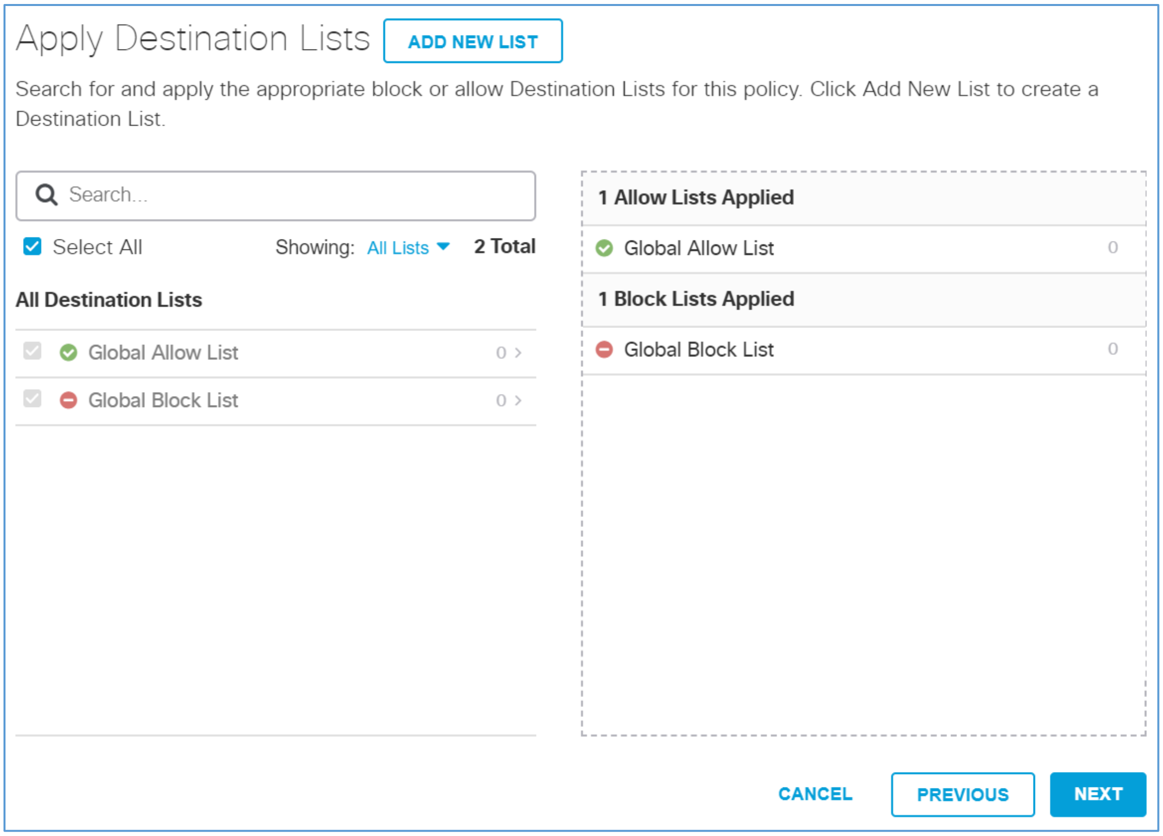
12. Click **Save.**



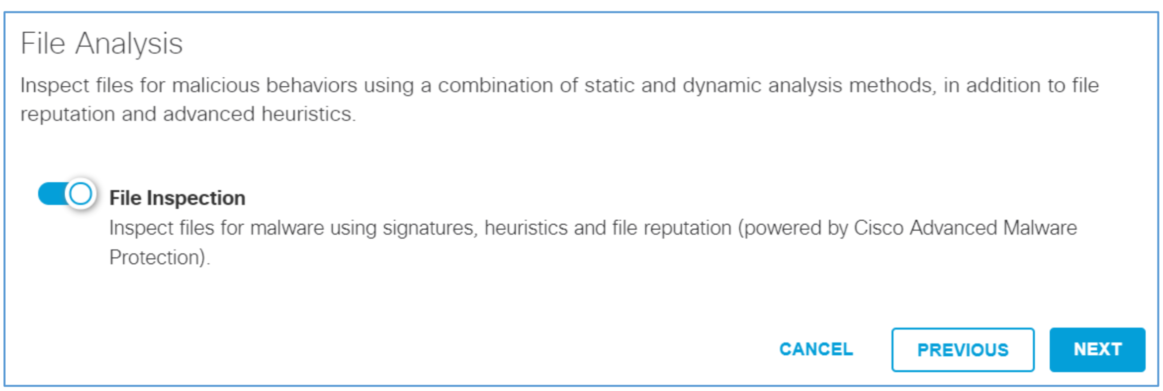
13. Click **Next.**



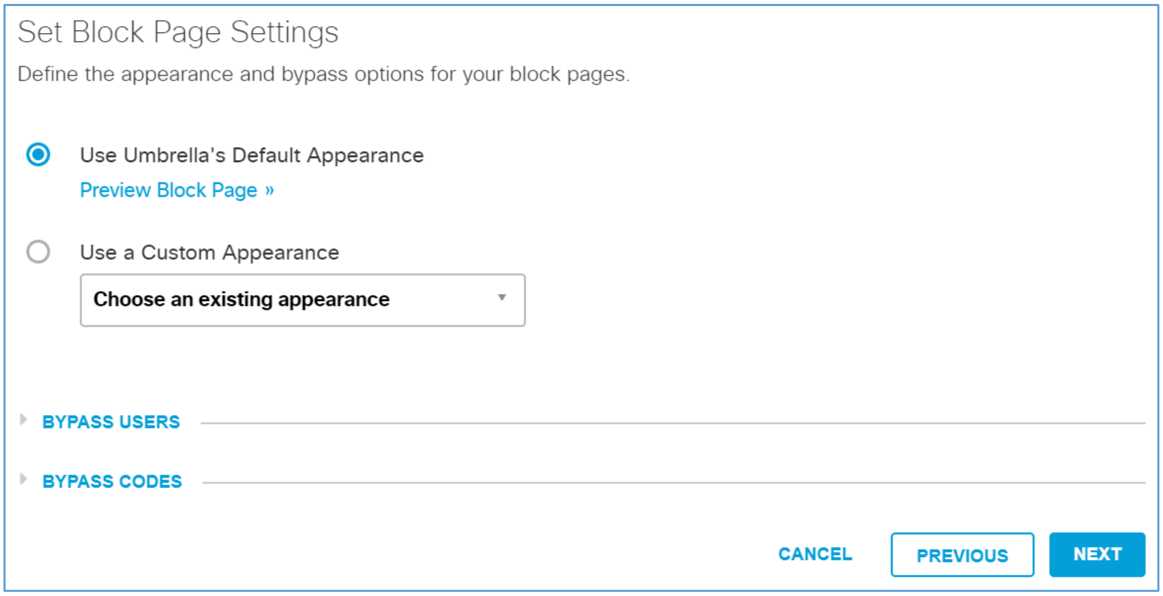
14. Click **Next.**



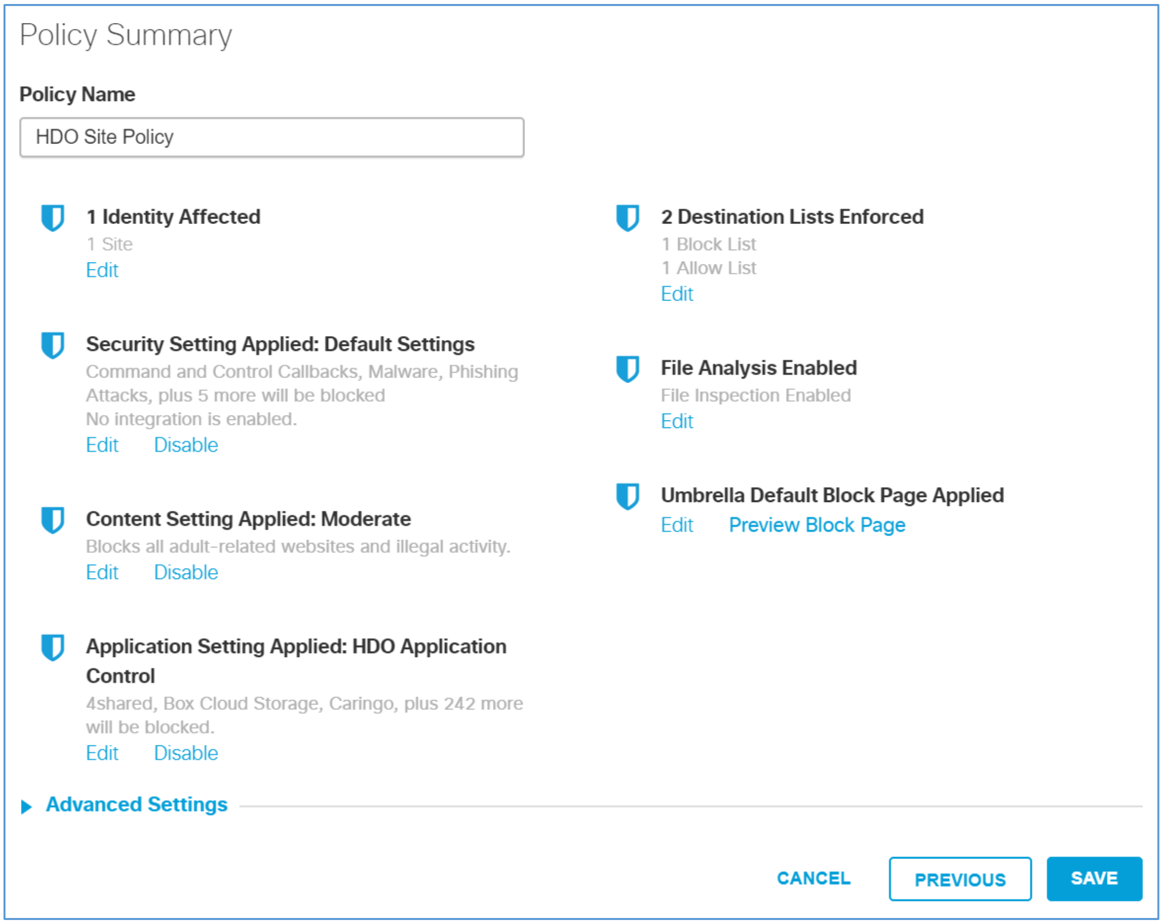
15. Click **Next.**



16. Click **Next.**

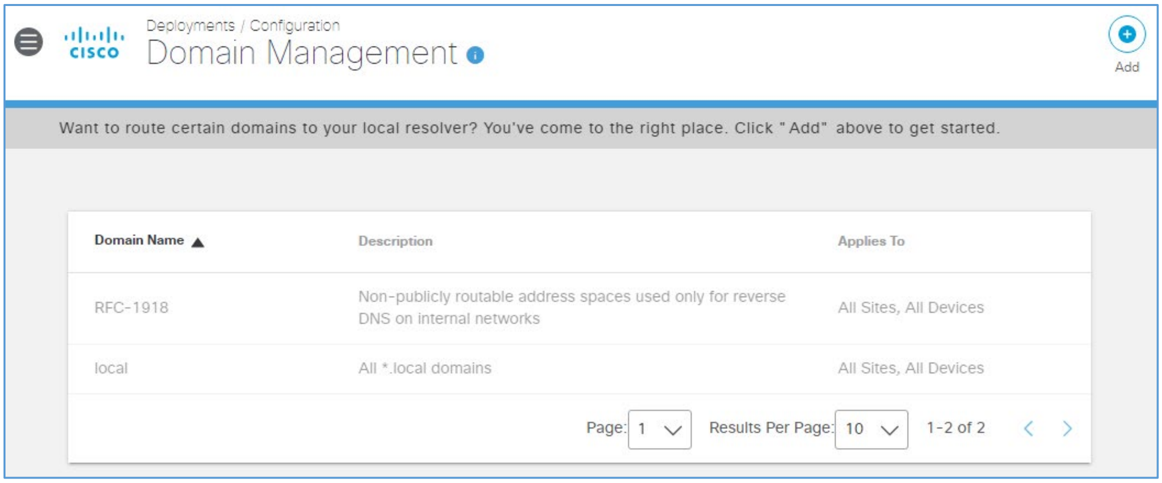


17. In the Policy Summary screen, set the **Name** to **HDO Site Policy.**
18. Click **Save.**

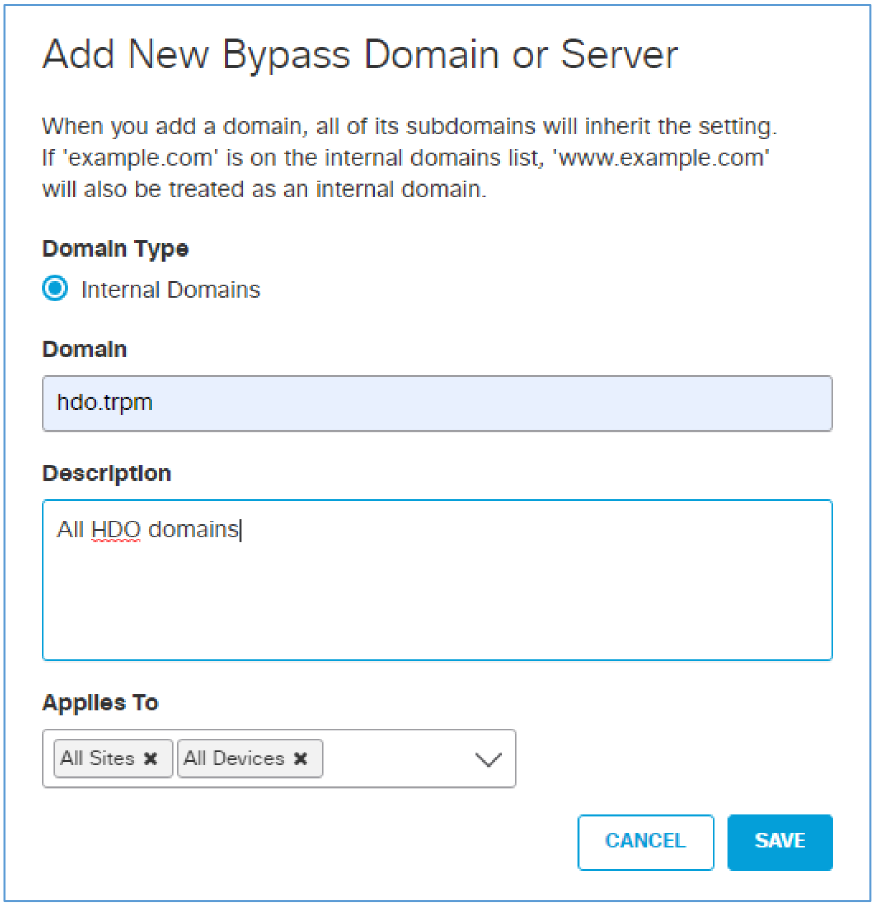


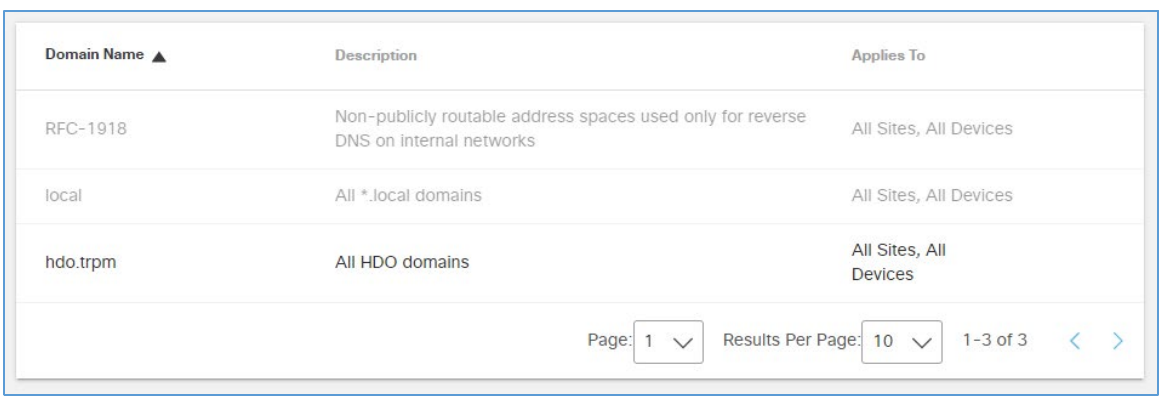
<u>Configure Windows Domain Controller as the Local DNS Provider</u>

1. Click **Deployments > Configuration > Domain Management.**
2. Click **Add.**



3. In the **Add New Bypass Domain or Server** popup window, fill out the following information:
    a. **Domain:** hdo.trpm
    b. **Applies To:** All Sites, All Devices
4. Click **Save.** Verify that the rule for the **hdo.trpm** has been added.





2.2.3.3 LogRhythm XDR (Extended Detection and Response)

LogRhythm XDR is a SIEM system that receives log and machine data from multiple end points and evaluates the data to determine when cybersecurity events occur. The project utilizes LogRhythm XDR in the HDO environment to enable a continuous view of business operations and detect cyber threats on assets.

System Requirements

CPU: 20 virtual central processing units (vCPUs)

Memory: 96 GB RAM

Storage:

- **hard drive C:** 220 GB
- **hard drive D:** 1 terabyte (TB)
- **hard drive L:** 150 GB

Operating System: Microsoft Windows Server 2016 X64 Standard Edition

Network Adapter: VLAN 1348

LogRhythm XDR Installation

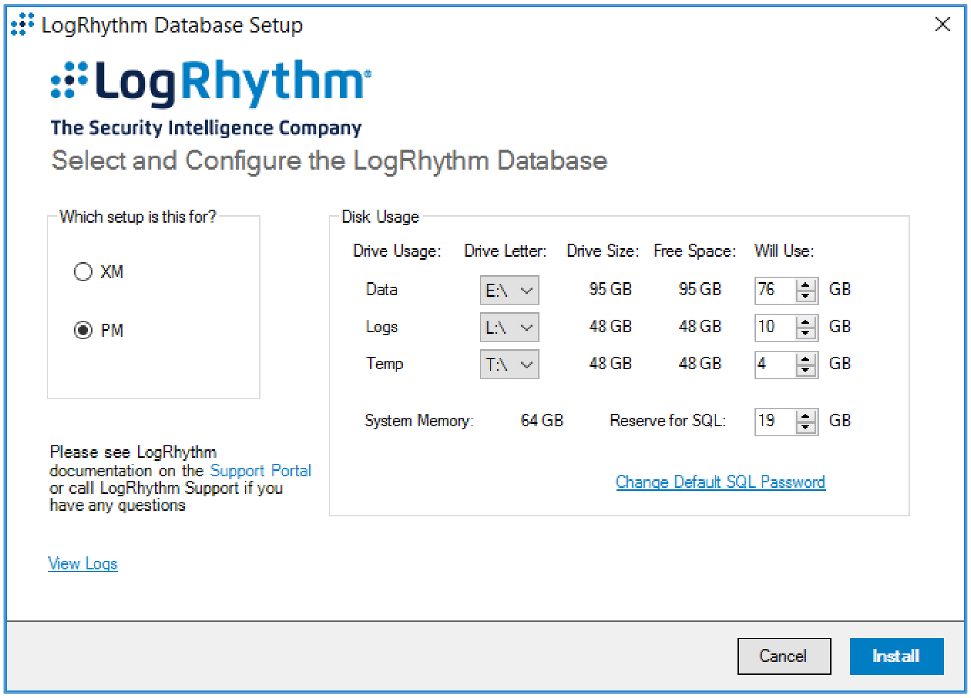
This section describes LogRhythm installation processes.

Download Installation Packages

1. Acquire the installation packages from LogRhythm, Inc.
2. Prepare a virtual Windows Server per the system requirements.
3. Create three new drives.
4. Create a new folder from C:\ on the Platform Manager server, and name the folder **LogRhythm.**
5. Extract the provided Database Installer tool and LogRhythm XDR Wizard from the installation package in *C:\LogRhythm.*

Install Database

1. Open *LogRhythmDatabaseInstallTool* folder.
2. Double-click ***LogRhythmDatabaseInstallTool*** application file.
3. Click **Run.**
4. A **LogRhythm Database Setup** window will appear. Set the **Which setup is this for?** to **PM** and use the default values for **Disk Usage**.



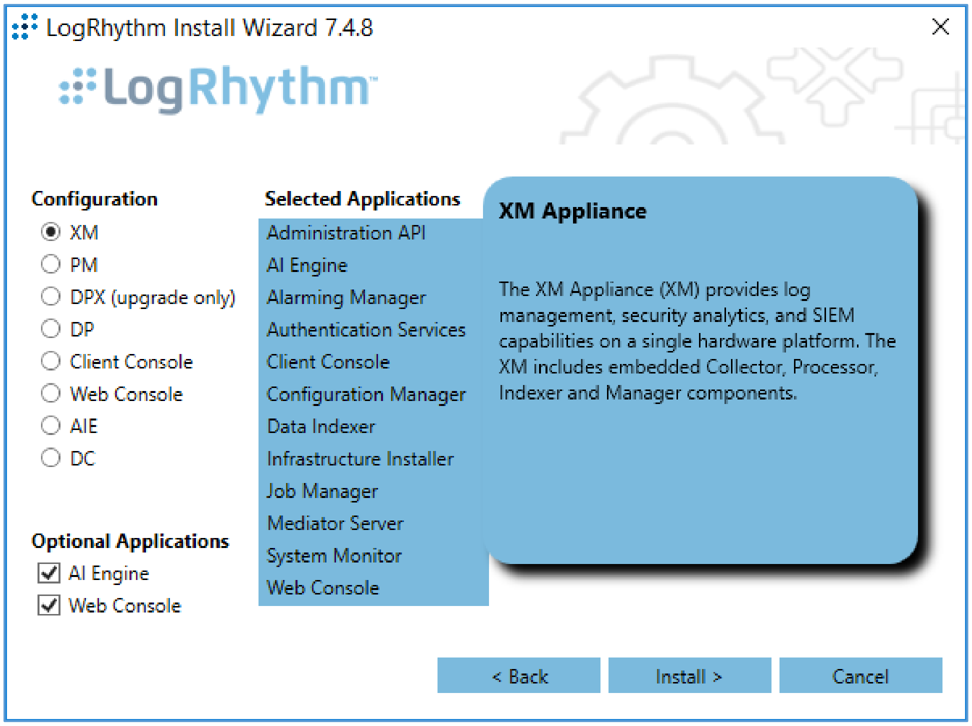
5. The remaining fields will automatically populate with the appropriate values. Click **Install.**
6. Click **Done** to close the **LogRhythm Database Setup** window.

<u>Install LogRhythm XDR</u>

1. Navigate to ***C:*** and open **LogRhythm XDR Wizard** folder.
2. Double-click the ***LogRhythmInstallerWizard*** application file.
3. The LogRhythm Install Wizard 7.4.8 window will appear.
4. Click **Next.**
5. A **LogRhythm Install Wizard Confirmation** window will appear.
6. Click **Yes** to continue.
7. Check the box beside **I accept the terms in the license agreement** to accept the License Agreement.
8. Click **Next.**
9. In the **Selected Applications** window, select the following attributes:
    a. **Configuration:** Select the XM radio button.

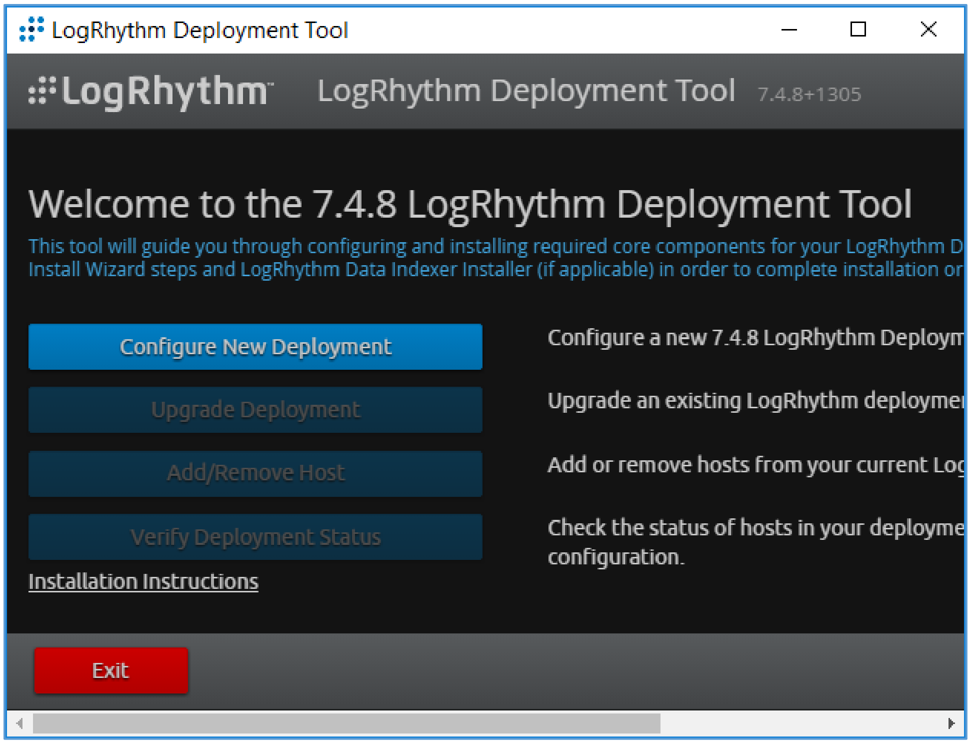
    b. **Optional Applications:** Check both **AI Engine** and **Web Console** boxes.

10. Click **Install.**

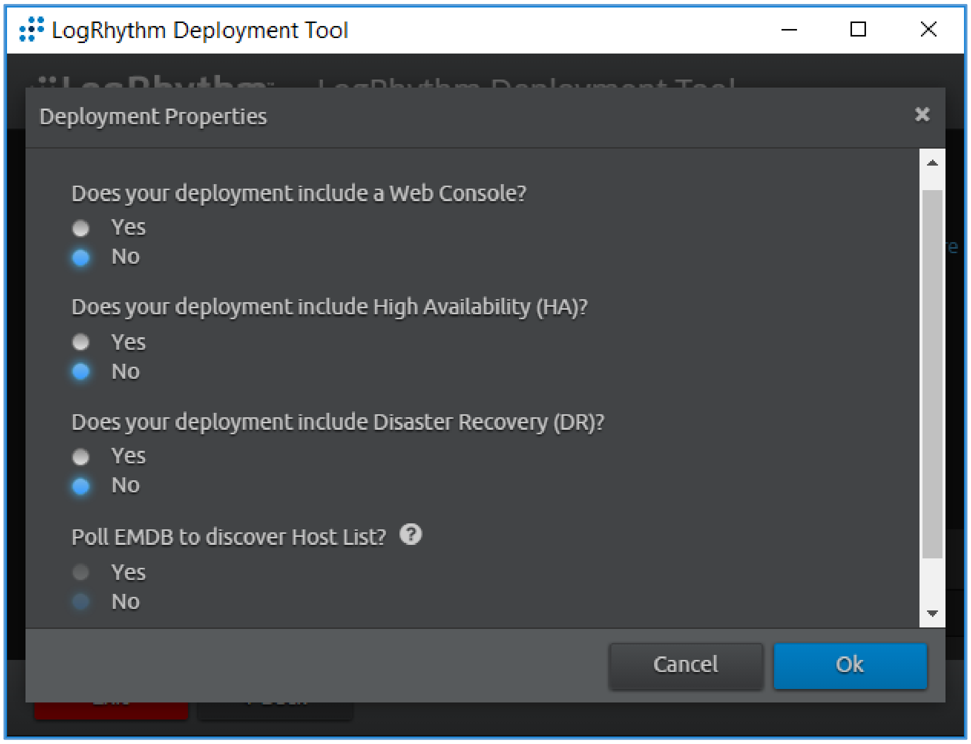


11. A **LogRhythm Deployment Tool** window displays.

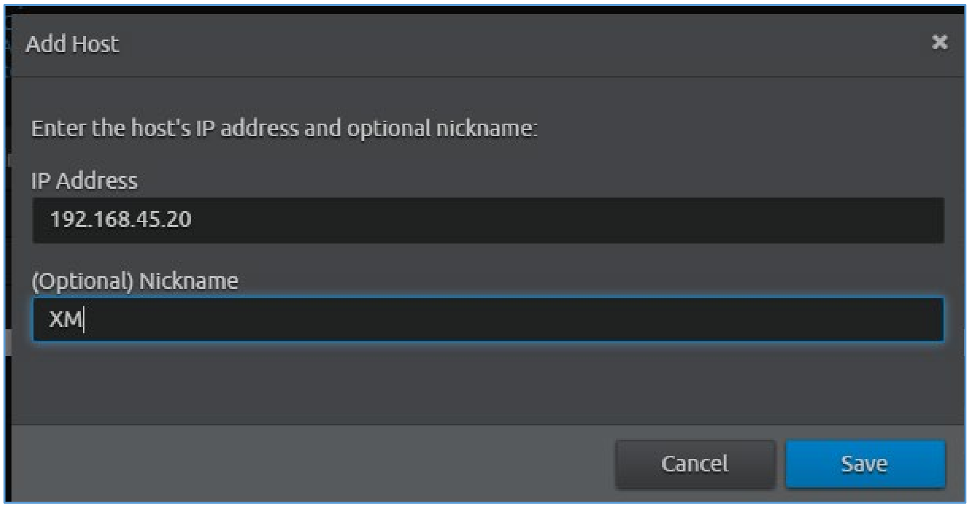
12. Click **Configure New Deployment.**



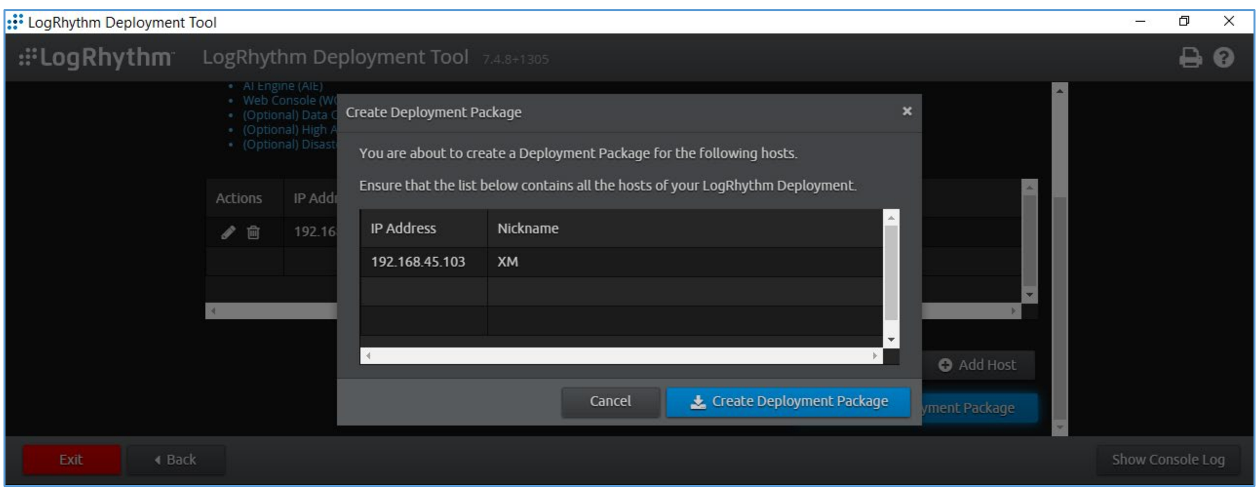
1065 13. In the **Deployment Properties window,** keep the default configurations and click **Ok.**



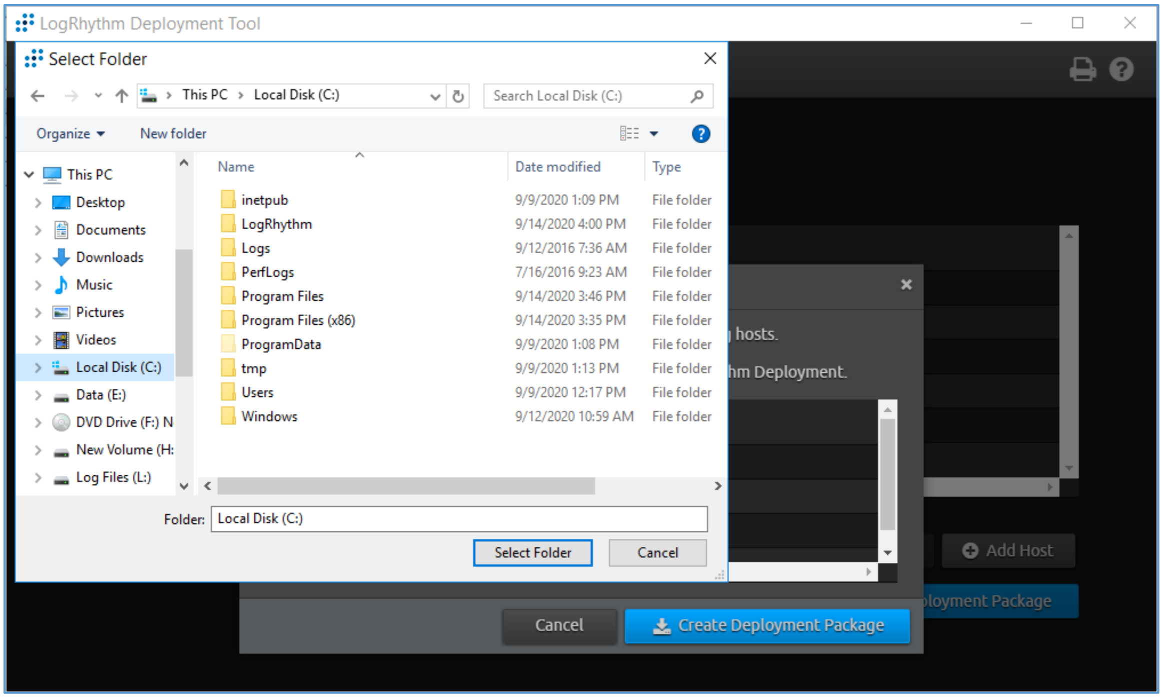
14. Click **+Add Host IP** in the bottom right corner of the screen, and provide the following information:
    a. **IP Address:** 192.168.45.20
    b. **Nickname:** XM
15. Click **Save.**



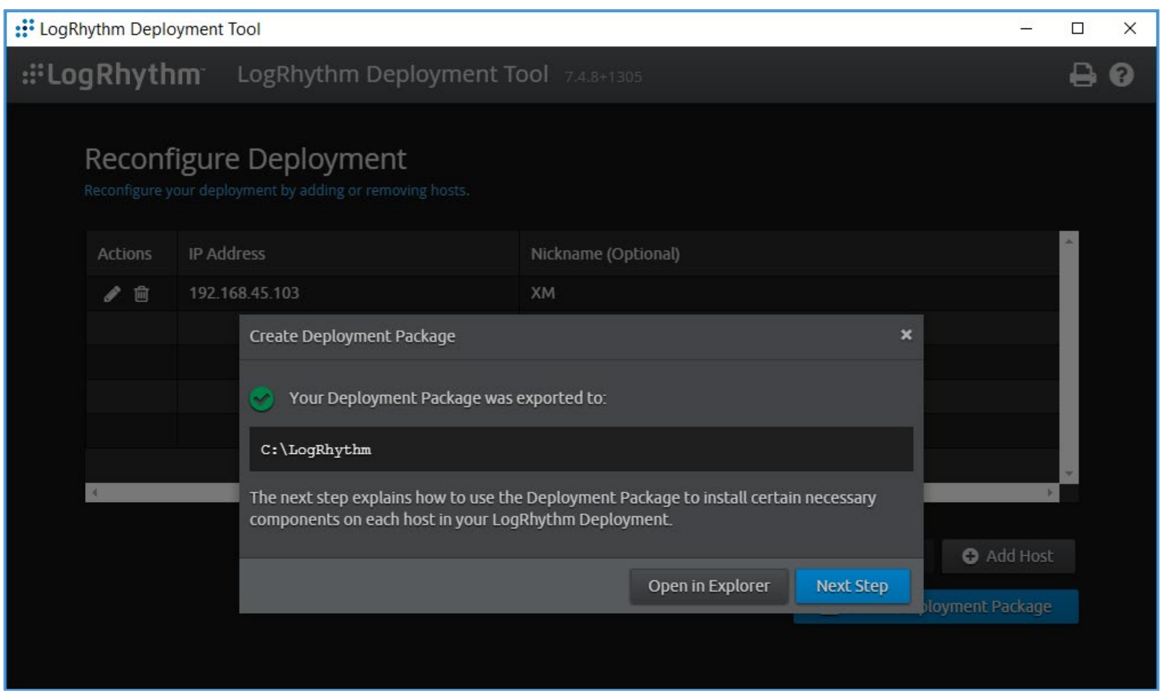
16. Click **Create Deployment Package** in the bottom right corner of the screen.
17. A **Create Deployment Package** window displays.
18. Click **Create Deployment Package.**



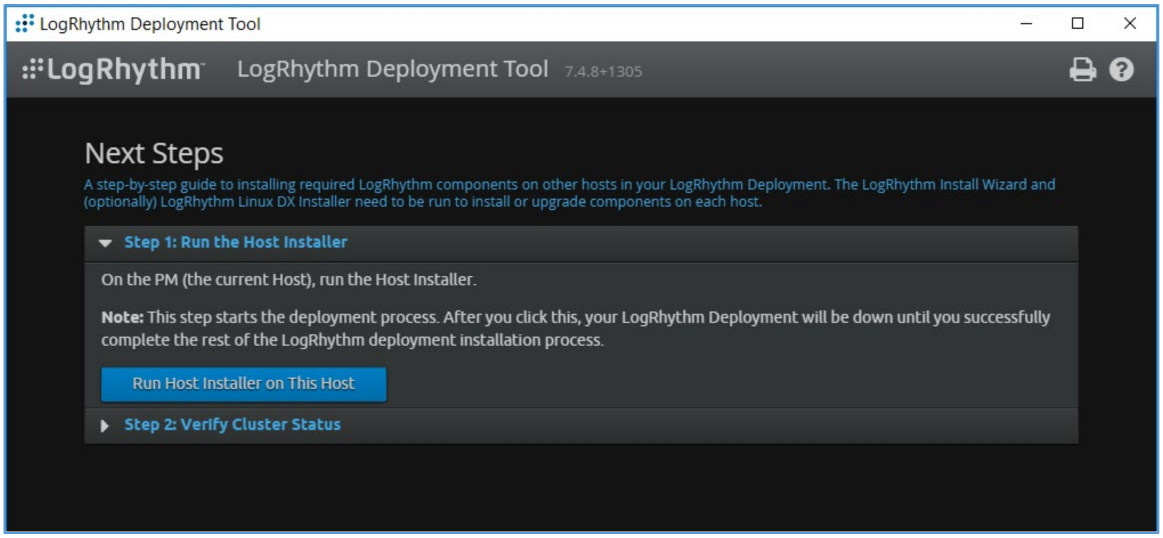
19. A Select Folder window appears.
20. Navigate to ***C:\LogRhythm.***
21. Click **Select Folder.**



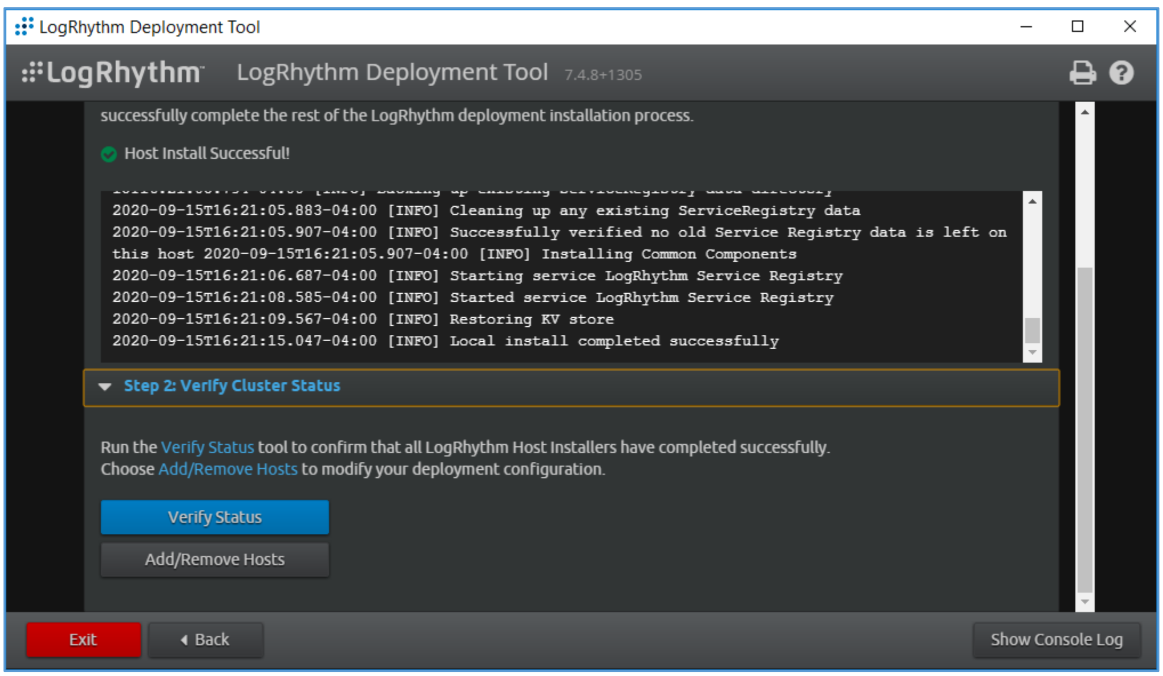
22. Click **Next Step.**



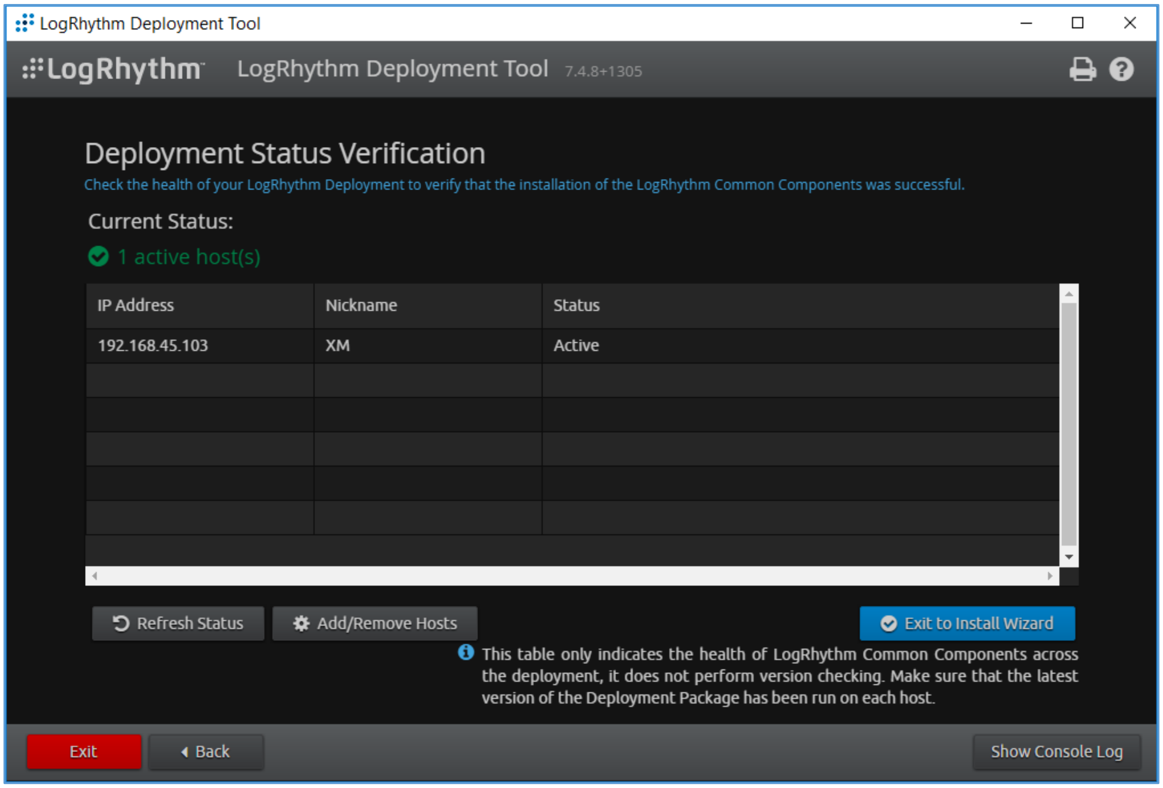
23. Click **Run Host Installer on this Host.**



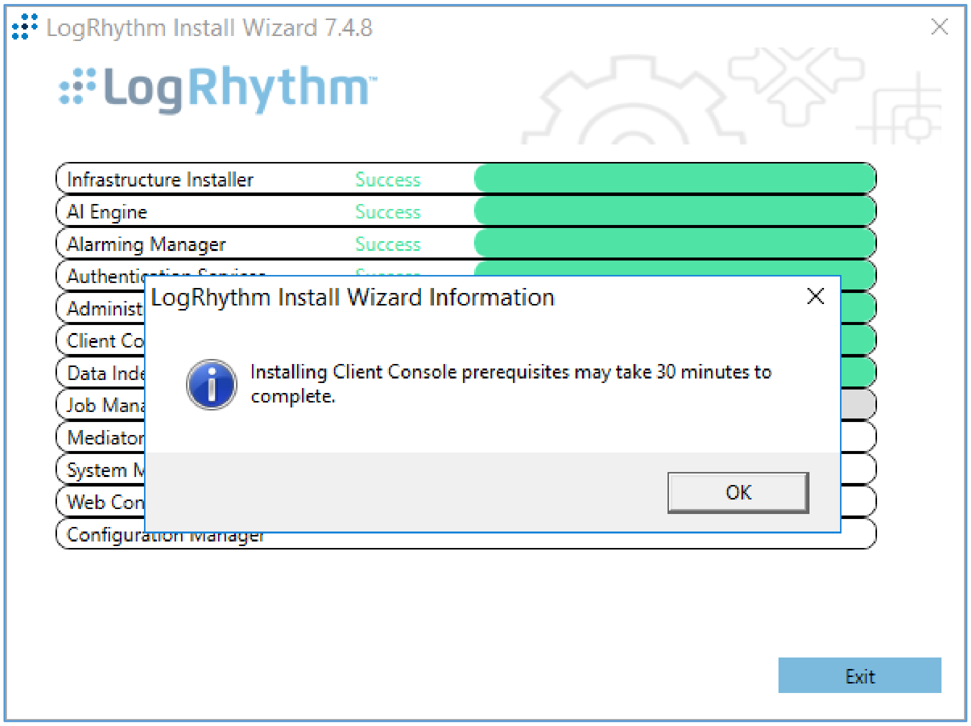
24. After the Host Installer has finished, click **Verify Status.**



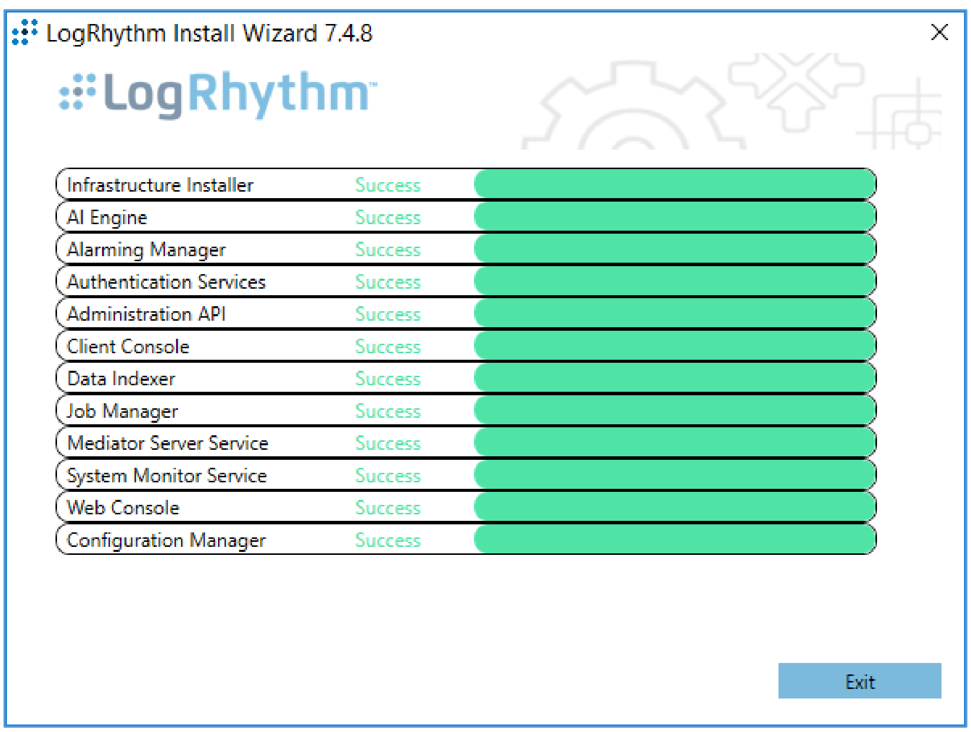
25. Click **Exit to Install Wizard.**



1081 26. A notification window displays stating the installation could take as long as 30 minutes. Click **OK.**



1082 27. After the Install Wizard has successfully installed the services, click **Exit.**



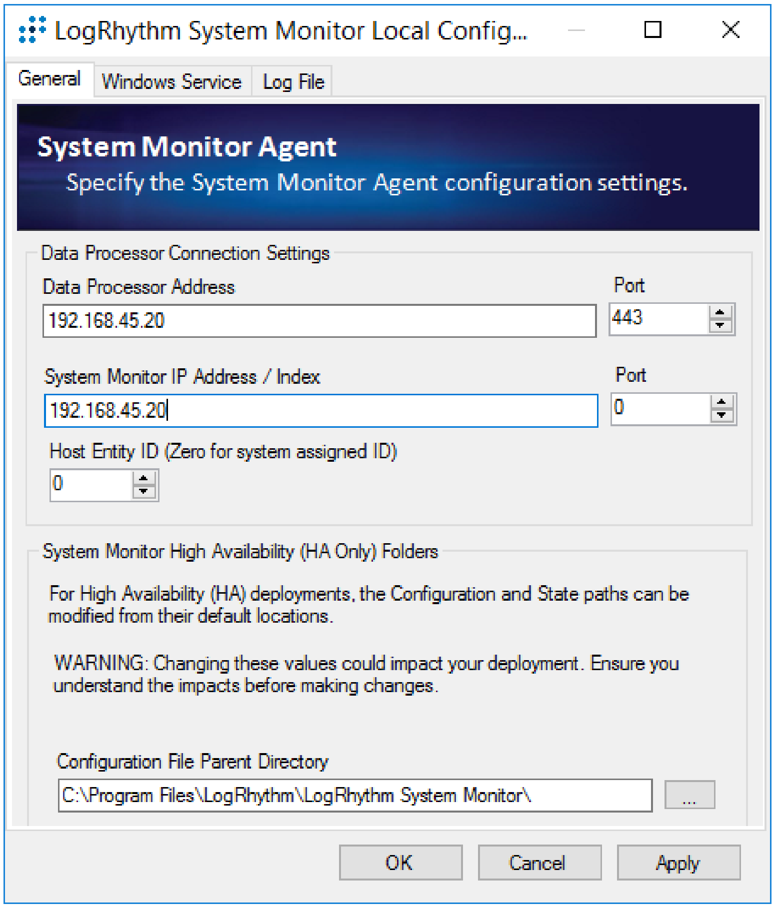
LogRhythm XDR Configuration

The LogRhythm XDR configuration includes multiple related components:

- System Monitor
- LogRhythm Artificial Intelligence (AI) Engine
- Mediator Server
- Job Manager
- LogRhythm Console

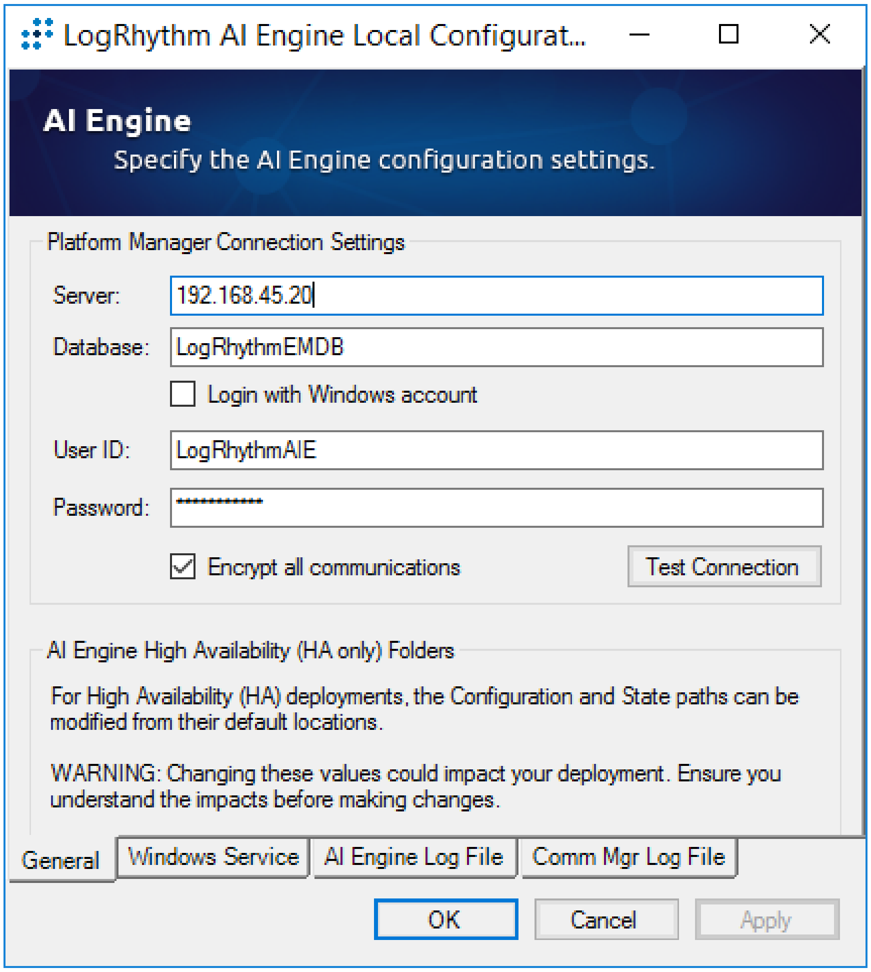
Configure System Monitor

1. Open **File Explorer,** and navigate to ***C:\Program Files\LogRhythm.***
2. Navigate to **LogRhythm System Monitor.**
3. Double-click the ***lrconfig*** application file.
4. In the **LogRhythm System Monitor Local Configuration Manager** window, provide the following information, and leave the remaining fields as their default values:
    a. **Data Processor Address:** 192.168.45.20
    b. **System Monitor IP Address/Index:** 192.168.45.20
5. Click **Apply,** and then click **OK.**



<u>**Configure LogRhythm AI Engine**</u>

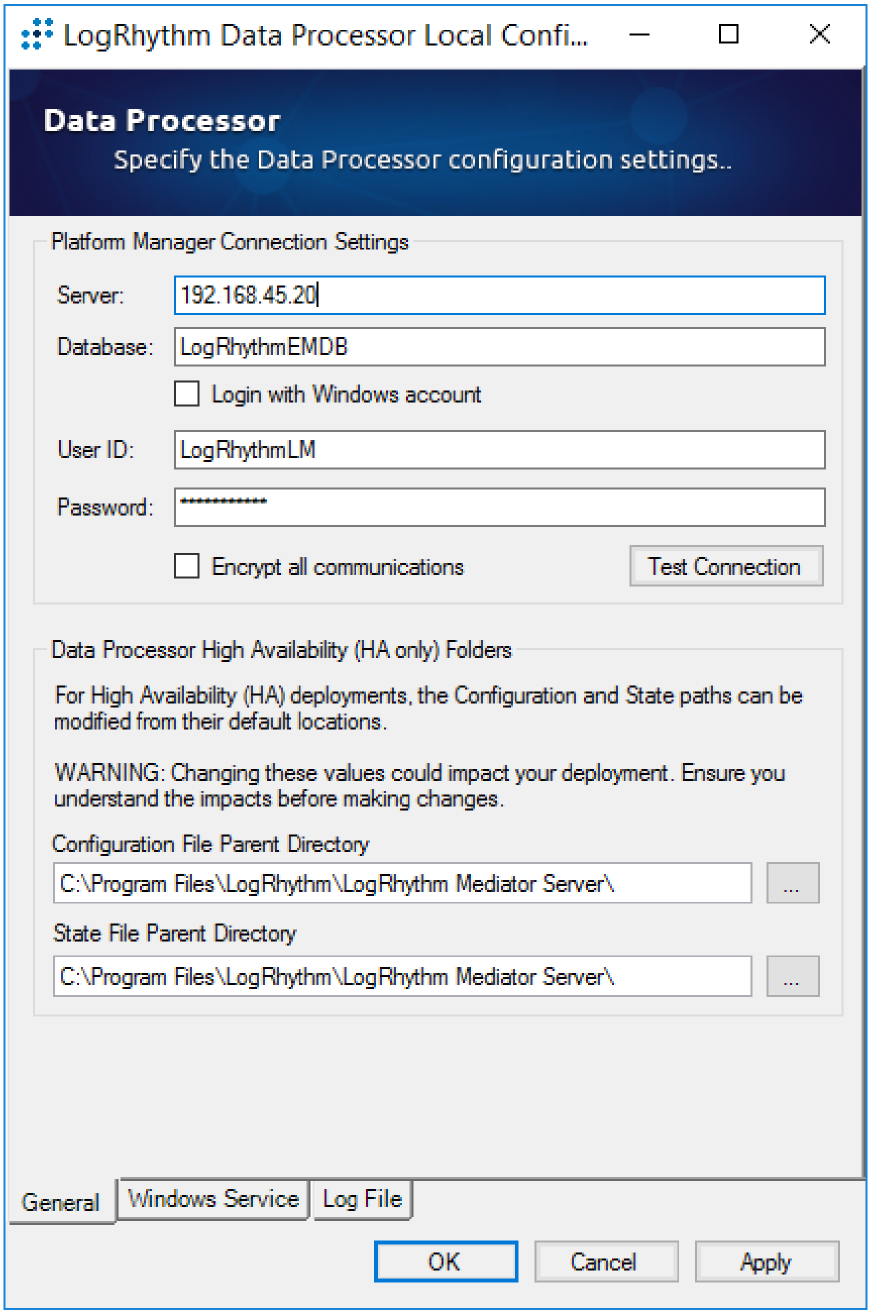
1. Open **File Explorer,** and navigate to ***C:\Program Files\LogRhythm.***
2. Navigate to **LogRhythm AI Engine.**
3. Double-click the ***lrconfig*** application file.
4. In the **LogRhythm AI Engine Local Configuration Manager** window, provide the following information, and leave the remaining fields as their default values:
    a. **Server:** 192.168.45.20
    b. **Password:** **********
5. Click **Test Connection,** then follow the instruction of the alert window to complete the test connection.
6. Click **Apply,** and then click **OK.**



<u>**Configure Mediator Server**</u>

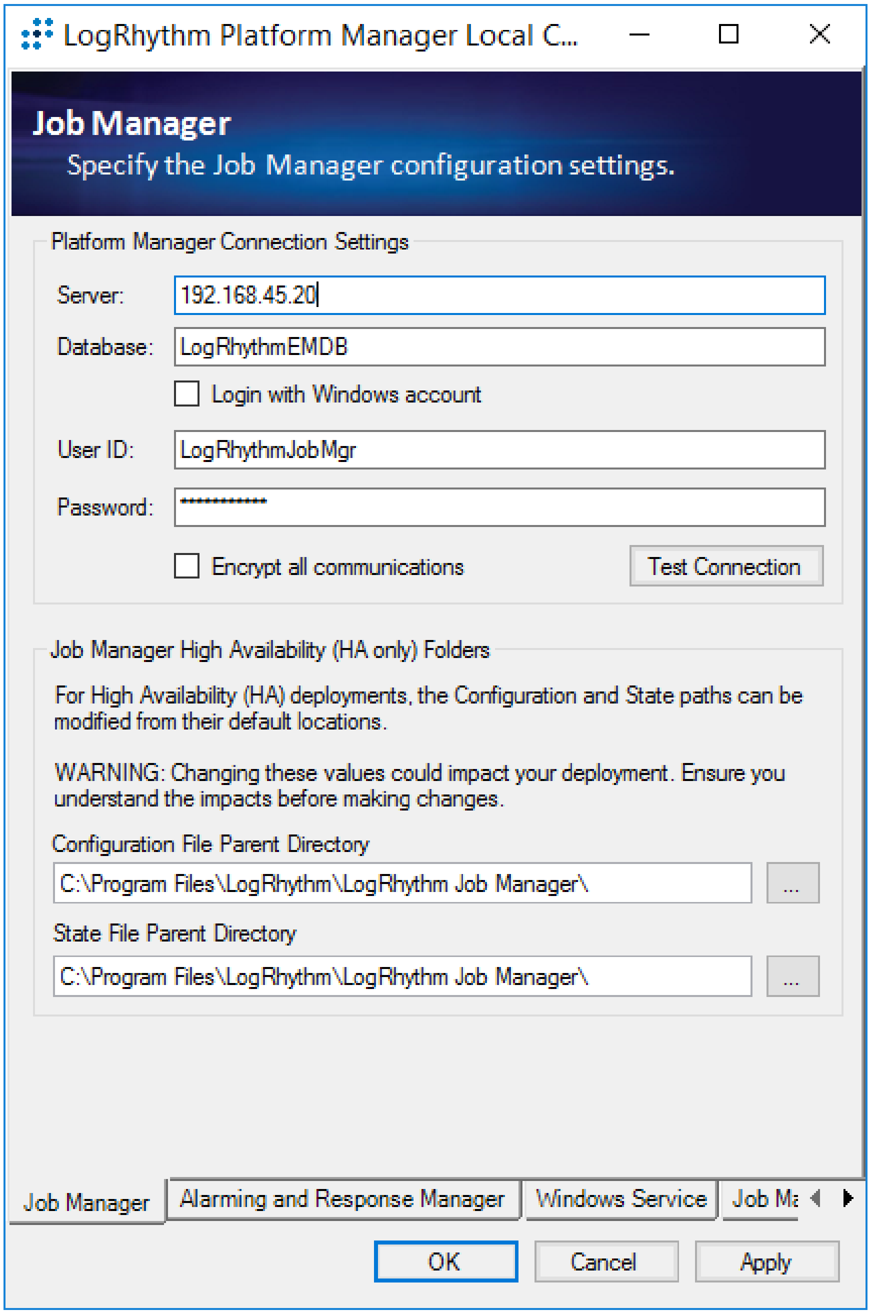
1. Open File Explorer, and navigate to ***C:\Program Files\LogRhythm.***
2. Navigate to **Mediator Server.**
3. Double-click ***lrconfig*** application file.
4. In the **LogRhythm Data Processor Local Configuration Manager** window, provide the following information, and leave the remaining fields as their default values:
    a. **Server:** 192.168.45.20
    b. **Password:** **********

5. Click **Test Connection,** then follow the instruction of the alert window to complete the test connection.
6. Click **Apply,** and then click **OK.**



Configure Job Manager

1. Open File Explorer and navigate to ***C:\Program Files\LogRhythm.***
2. Navigate to **Job Manager.**
3. Double-click the ***lrconfig*** application file.
4. In the **LogRhythm Platform Manager Local Configuration Manager** window, provide the following information, and leave the remaining fields as their default values:
    a. **Server:** 192.168.45.20
    b. **Password:** **********
5. Click **Test Connection,** then follow the instruction of the alert window to complete the test connection.
6. Click **Apply,** and then click **OK.**



7. Navigate to the **Alarming and Response Manager** tab in the bottom menu ribbon.

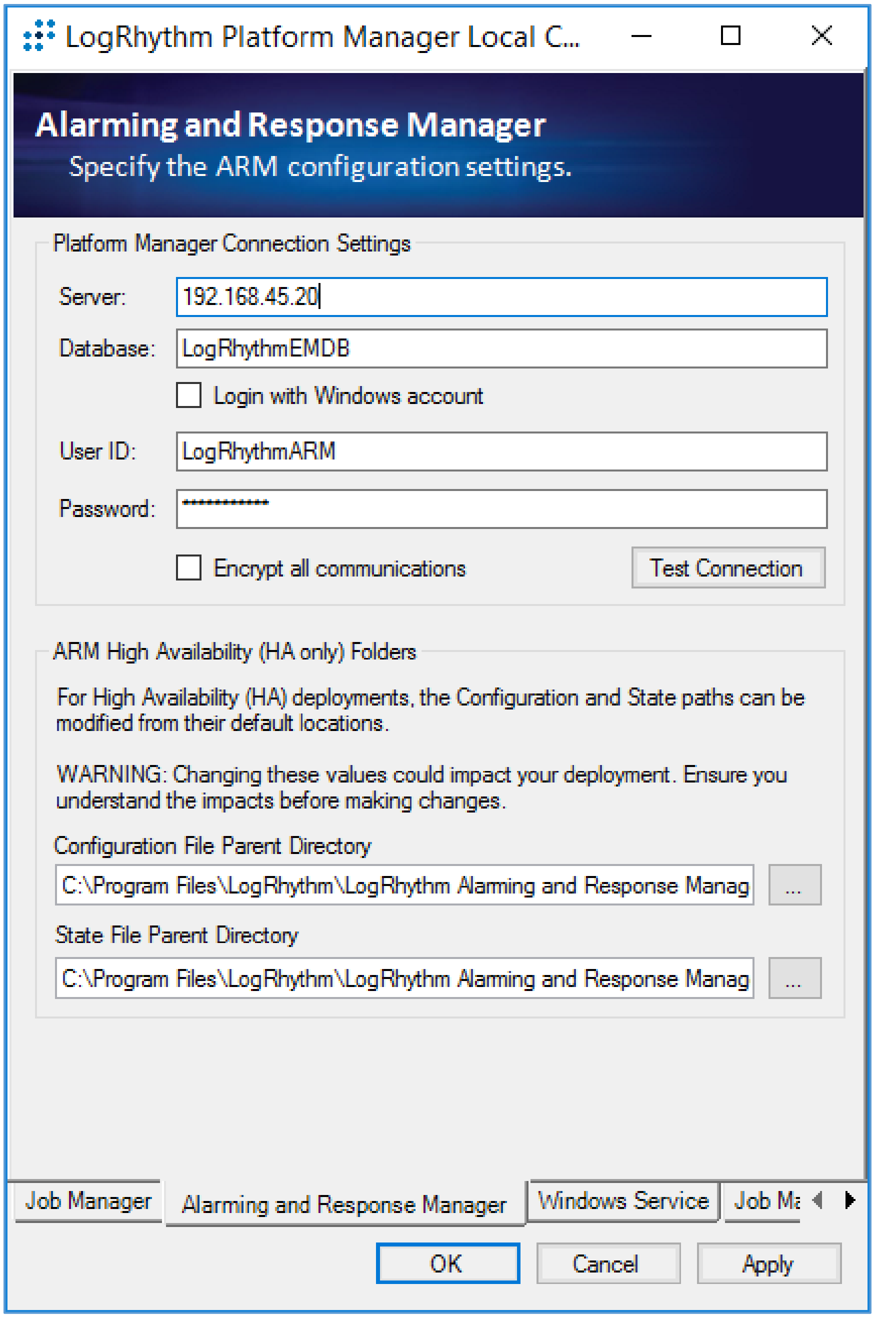
8. In the **Alarming and Response Manager** window, provide the following information, and leave the remaining fields as their default values:

    a. **Server:** 192.168.45.20

   b. **Password:** **********

9. Click **Test Connection,** then follow the instruction of the alert window to complete the test connection.

10. Click **Apply,** and then click **OK.**

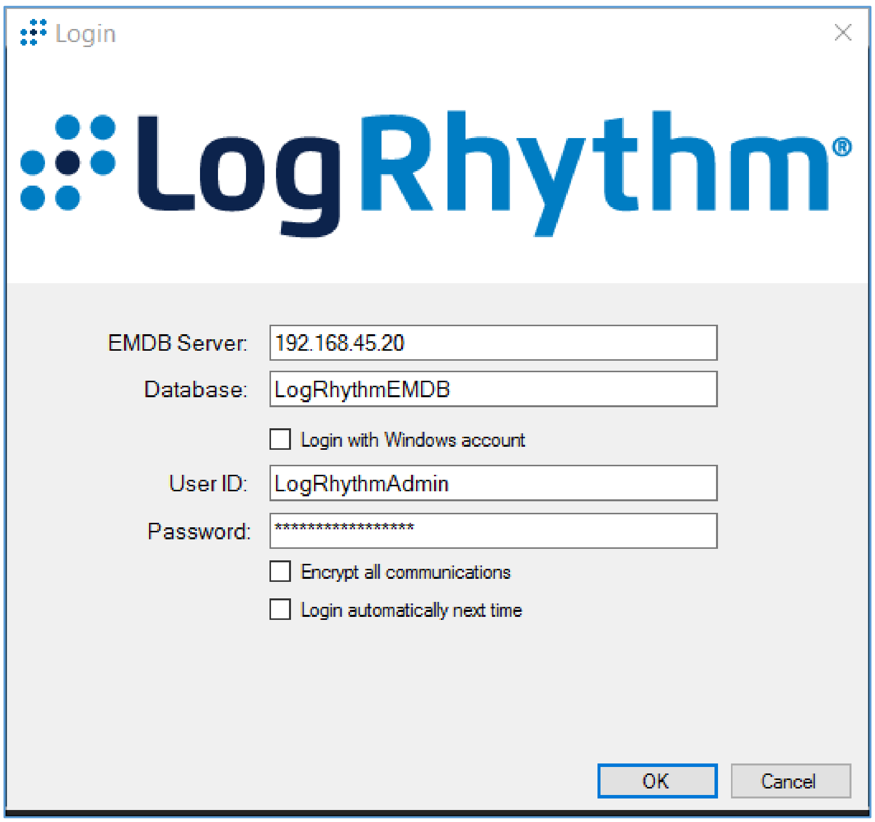


1141 **Configure LogRhythm Console**

1142 1. Open File Explorer and navigate to ***C:\Program Files\LogRhythm.***

1143 2. Navigate to **LogRhythm Console.**

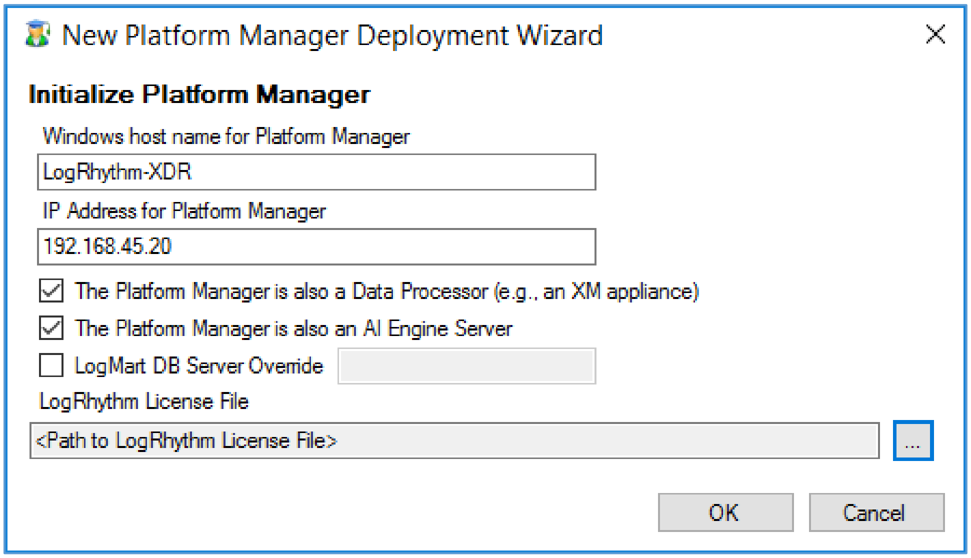
3. Double-click ***lrconfig*** application file.
4. In the LogRhythm Login window, provide the following information:
    a. **EMDB Server:** 192.168.45.20
    b. **UserID:** LogRhythmAdmin
    c. **Password:** ********
5. Click **OK.**



6. A New Platform Manager Deployment Wizard window displays. Provide the following information:
    a. **Windows host name for Platform Manager:** LogRhythm-XDR
    b. **IP Address for Platform Manager:** 192.168.45.20
    c. Check the box next to **The Platform Manager is also a Data Processor (e.g., an XM appliance).**

   d. Check the box next to **The Platform Manager is also an AI Engine Server.**

7. Click the **ellipsis button** next to **<Path to LogRhythm License File>,** and navigate to the location of the LogRhythm License File.



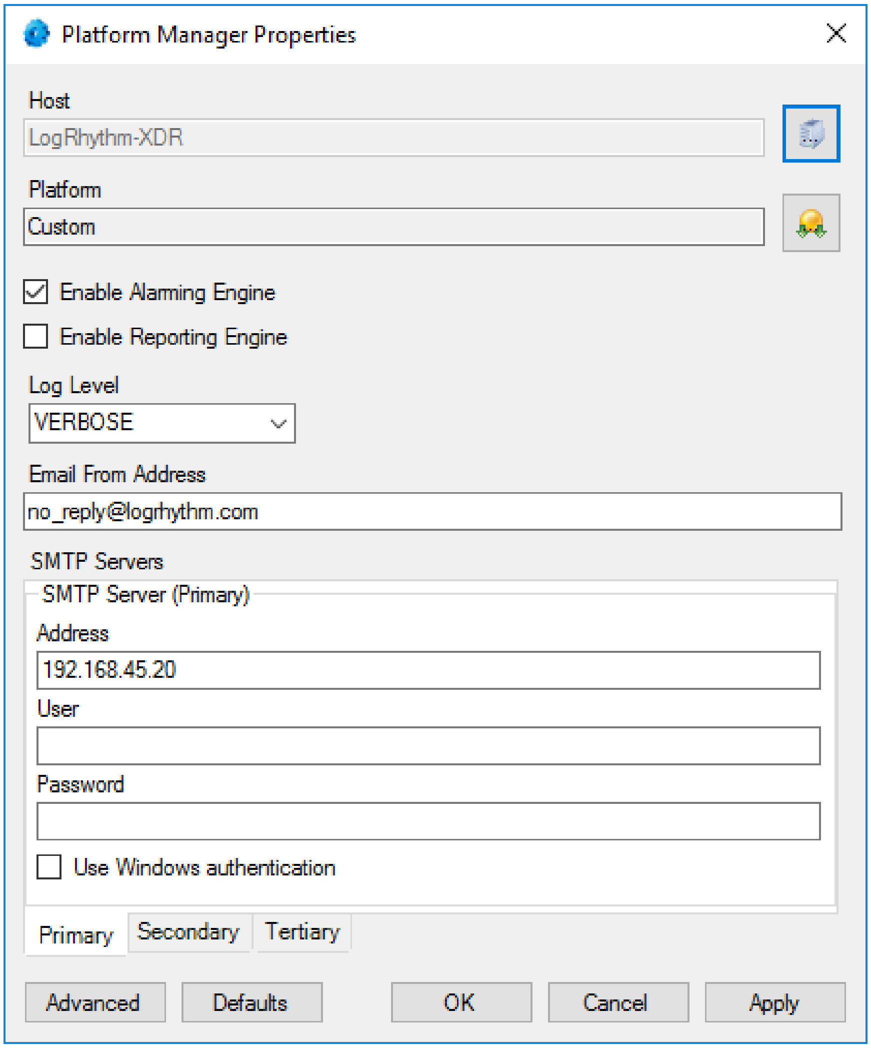
8. The New Knowledge Base Deployment Wizard window displays and shows the import progress status. Once LogRhythm has successfully imported the file, a message window will appear stating more configurations need to be made for optimum performance. Click **OK** to open the **Platform Manager Properties** window.

9. In the Platform Manager Properties window, provide the following information:

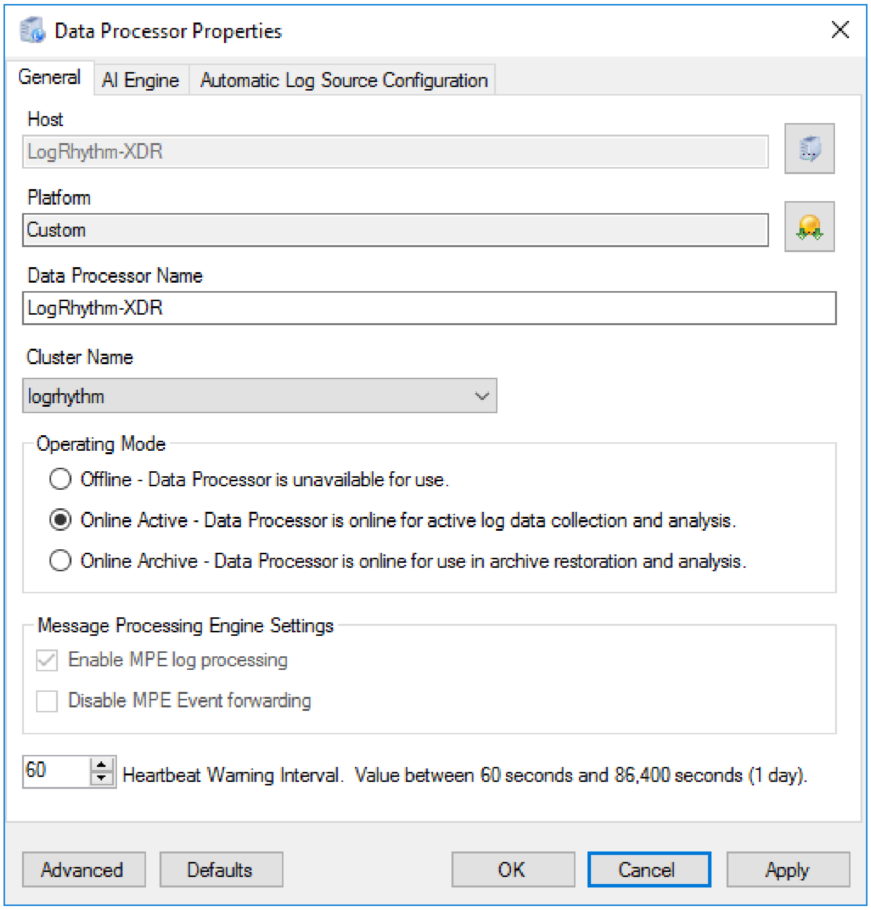
   a. **Email address:** no_reply@logrhythm.com

   b. **Address:** 192.168.45.20

10. Click the button next to **Platform,** enable the **Custom Platform** radio button, and complete the process by clicking **Apply,** followed by clicking **OK.**

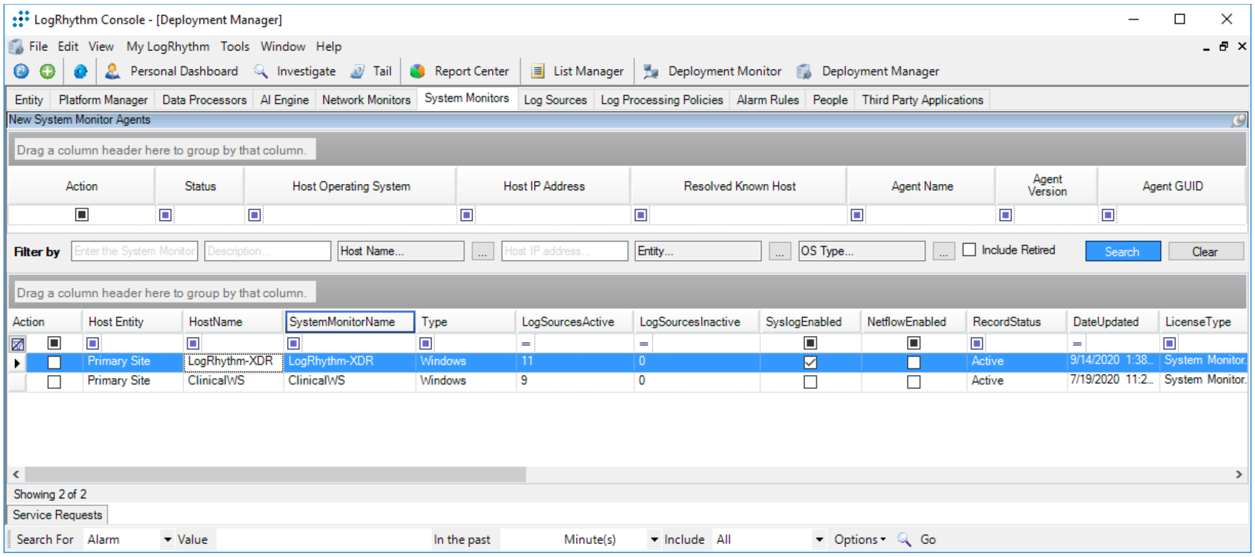


11. After the Platform Manager Properties window closes, a message window displays for configuring the Data Processor. Click **OK** to open the **Data Processor Properties** window.
12. Click the button next to **Platform,** and enable the **Custom Platform** radio button.
13. Click **OK.**
14. Leave the remaining fields in the Data Processor Properties window as their default values, and click **Apply.**
15. Click **OK** to close the window**.**



<u>Set LogRhythm-XDR for System Monitor</u>

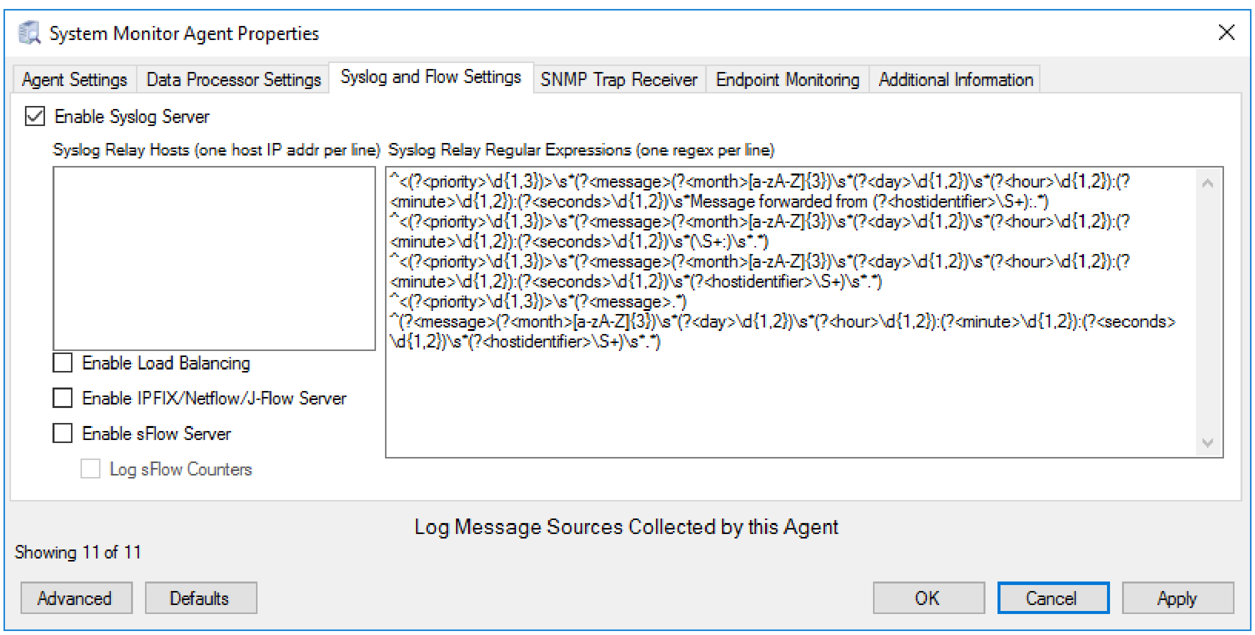
1. Back in the LogRhythm console, navigate to the **Deployment Manager** tab in the menu ribbon.
2. Navigate to **System Monitors** on the Deployment Manager menu ribbon.
3. Double-click **LogRhythm-XDR.**



4. In the **System Monitor Agent Properties** window, navigate to **Syslog and Flow Settings.**

5. Click the checkbox beside **Enable Syslog Server.**

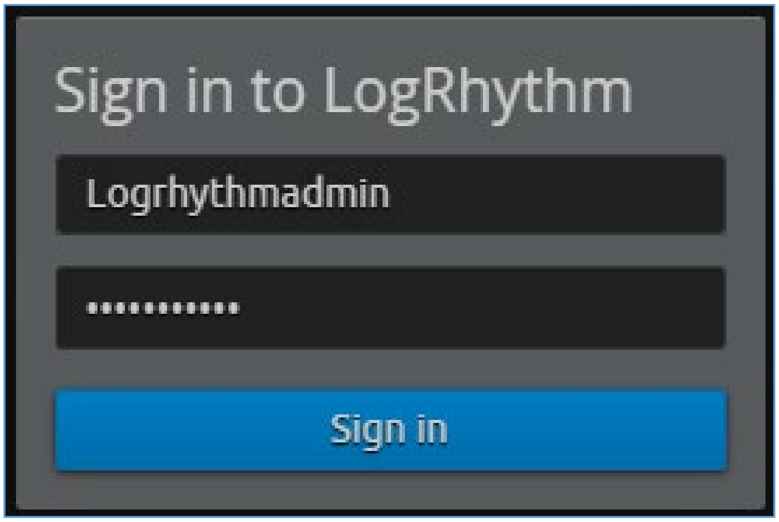
6. Click **OK** to close the System Monitor Agent Properties window.



Use the LogRhythm Web Console

1. Open a web browser, and navigate to **https://localhost:8443.**

2. Enter the **Username:** logrhythmadmin
3. Enter the **Password:** **********



2.2.3.4 LogRhythm NetworkXDR

LogRhythm NetworkXDR paired with LogRhythm XDR enables an environment to monitor network traffic between end points and helps suggest remediation techniques for identified concerns. This project utilizes NetworkXDR for continuous visibility on network traffic between HDO VLANs and incoming traffic from the telehealth platform provider.

System Requirements

CPU: 24 vCPUs

Memory: 64 GB RAM

Storage:
- Operating System Hard Drive: 220 GB
- Data Hard Drive: 3 TB
- Operating System: CentOS 7

Network Adapter: VLAN 1348

LogRhythm NetworkXDR Installation

LogRhythm provides an International Organization for Standardization (.iso) disk image to simplify installation of NetMon. The .iso is a bootable image that installs CentOS 7.7 Minimal and NetMon. Note: Because this is an installation on a Linux box, there is no need to capture the screenshots.

Download the Installation Software

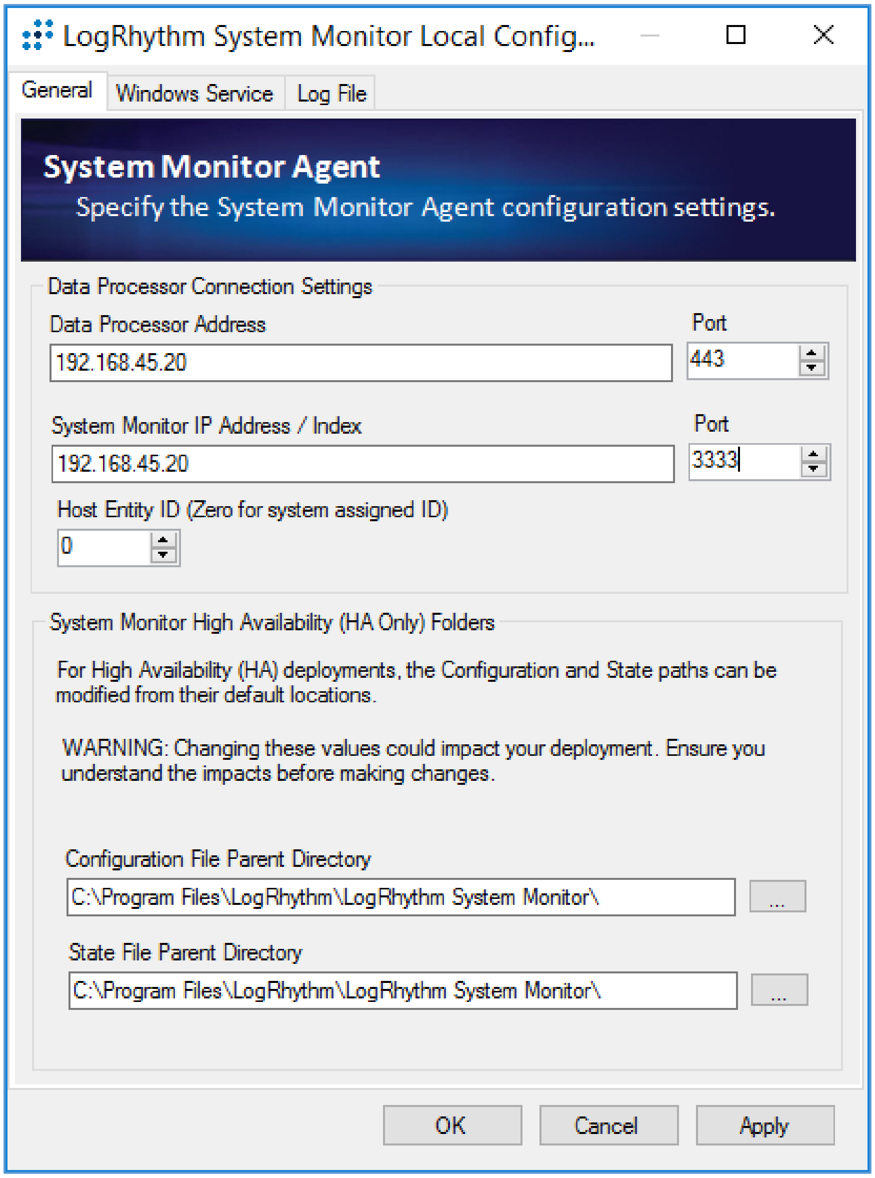
1. Open a new tab in the web browser, and navigate to https://community.logrhythm.com.
2. Log in using the appropriate credentials.
3. Click **LogRhythm Community.**
4. Navigate to **Documentation & Downloads.**
5. Register a **Username.**
6. Click **Accept.**
7. Click **Submit.**
8. Navigate to **NetMon.**
9. Click **downloads: netmon4.0.2.**
10. Select **NetMon ISO** under Installation Files.

Install LogRhythm NetworkXDR

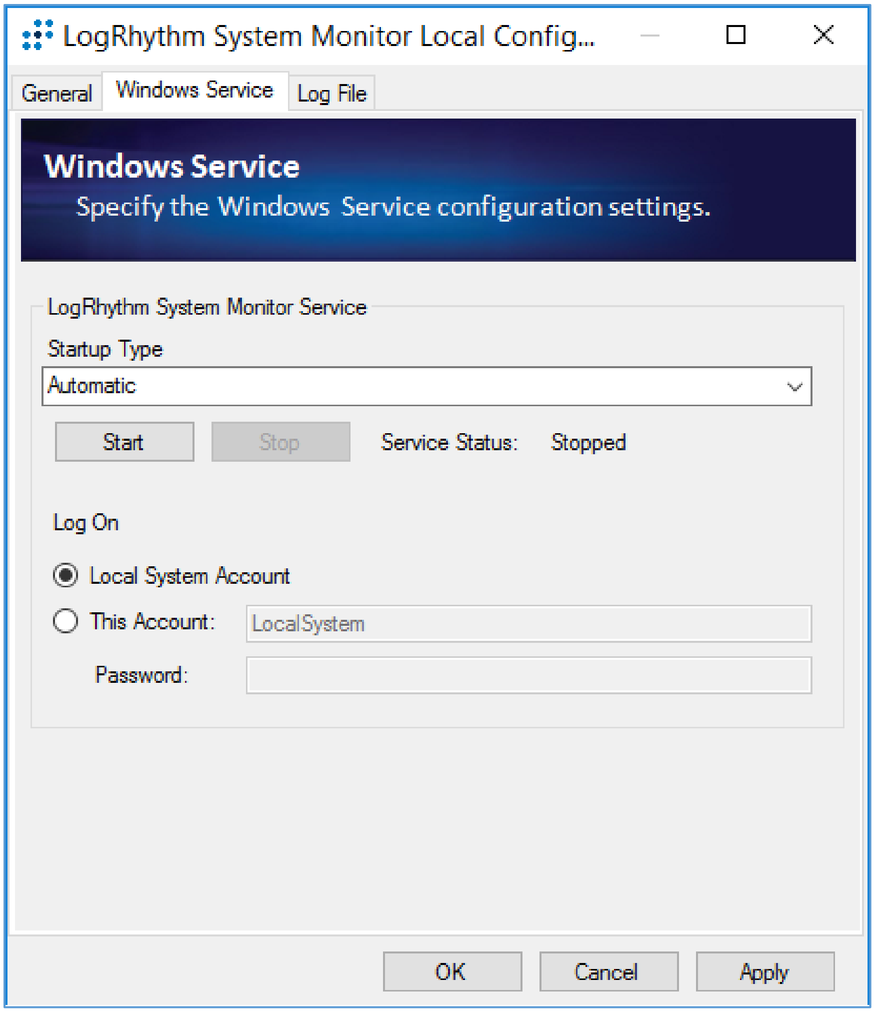
1. In the host server, mount the *.iso* for the installation.
2. Start the VM with the mounted *.iso*.
3. When the welcome screen loads, select **Install LogRhythm Network Monitor.**
4. The installer completes the installation, and the system reboots.
5. When the system reboots, log in to the console by using **logrhythm** as the login and ********** as the password.
6. Then change the password by typing the command **`passwd`,** type the default **password,** and then type and verify the **new password.**

LogRhythm NetworkXDR Configuration

1. **Data Process Address:** 192.168.45.20
2. Click **Apply.**



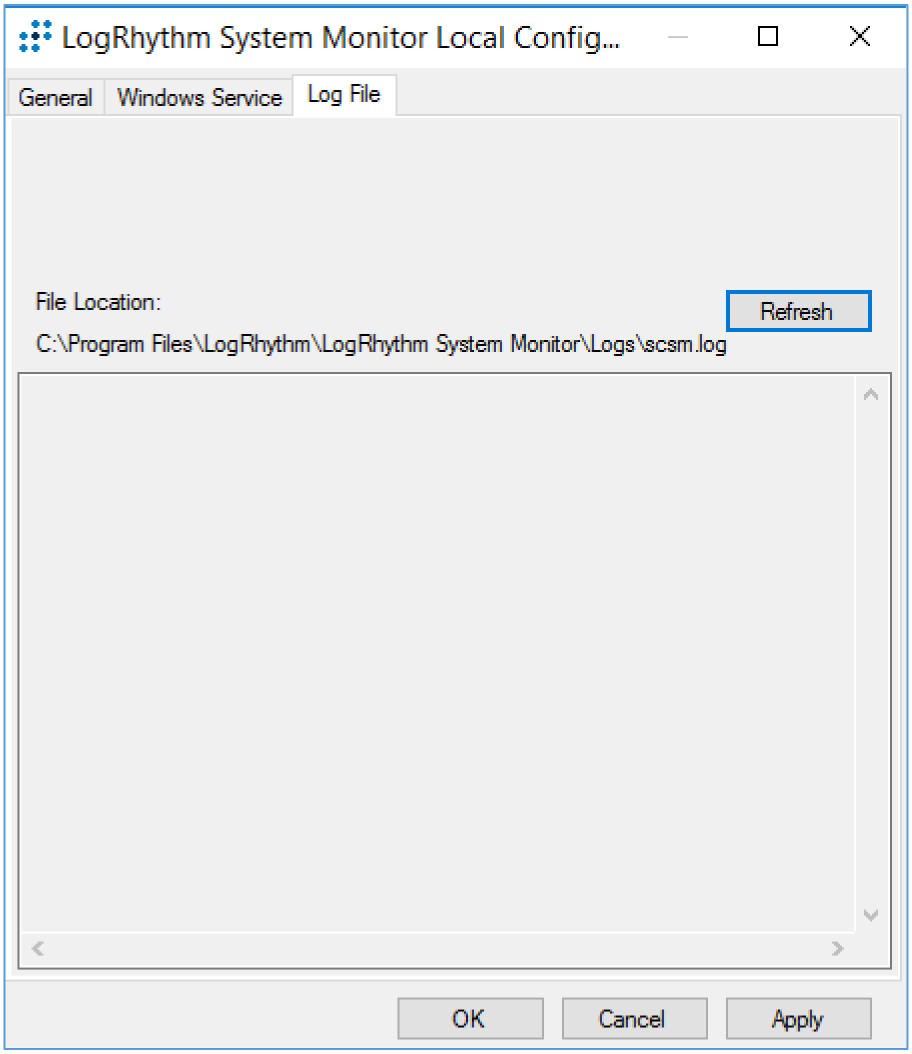
3. Click the **Windows Service** tab.
4. Change the **Service Type** to **Automatic.**
5. Click **Apply.**



1231 6. Click the **Log File** tab.

1232 7. Click **Refresh** to ensure NetworkXDR log collection.

1233 8. Click **OK** to exit the **Local Configuration Manager.**



2.2.3.5 LogRhythm System Monitor Agent

LogRhythm System Monitor Agent is a component of LogRhythm XDR that receives end-point log files and machine data in an IT infrastructure. The system monitor transmits ingested data to LogRhythm XDR where a web-based dashboard displays any identified cyber threats. This project deploys LogRhythm's System Monitor Agents on end points in each identified VLAN.

Install the LogRhythm System Monitor Agent on one of the end points (e.g., Clinical Workstation) in the HDO environment so that the LogRhythm XDR can monitor the logs, such as syslog and eventlog, of this workstation.

System Monitor Agent Installation

This section describes installation of the system monitor agent.

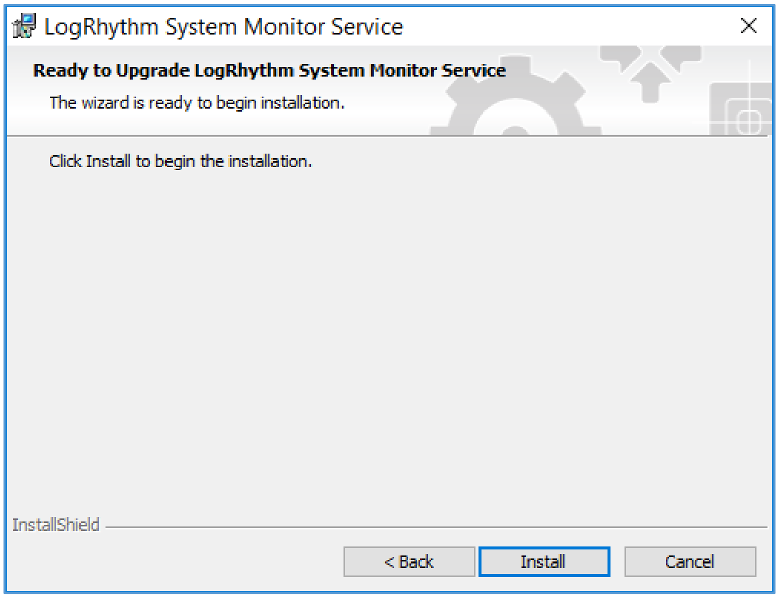
<u>Download Installation Packages</u>

1. Using a Clinical Workstation, open a web browser.
2. Navigate to https://community.logrhythm.com.
3. Log in using the credentials made when installing and configuring LogRhythm XDR.
4. Navigate to **LogRhythm Community.**
5. Click **Documents & Downloads.**
6. Click **SysMon.**
7. Click **SysMon – 7.4.10.**
8. Click **Windows System Monitor Agents,** and save to the **Downloads** folder on the Workstation.

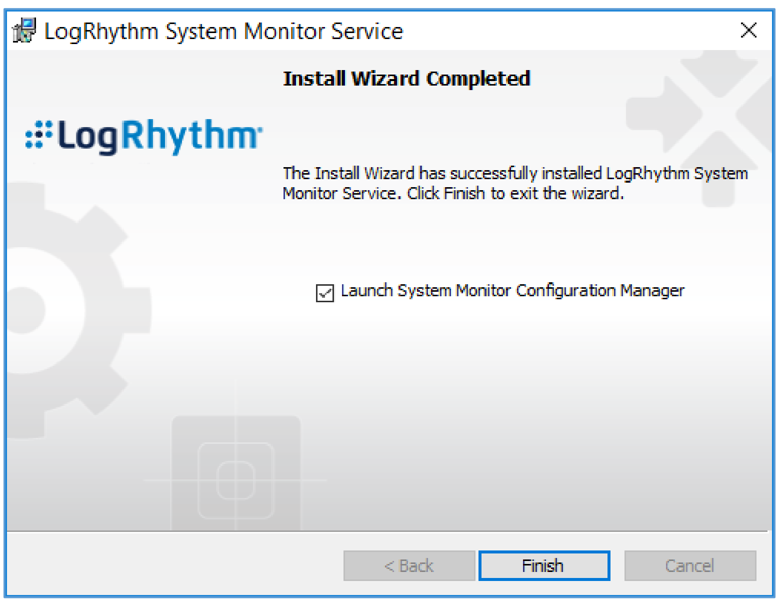
<u>Install System Monitor Agent</u>

1. On the Workstation, navigate to **Downloads** folder.
2. Click **LRWindowsSystemMonitorAgents.**
3. Click **LRSystemMonitor_64_7.**
4. On the Welcome page, follow the Wizard, and click **Next….**

5. On the ready to begin installation page, click **Install.**



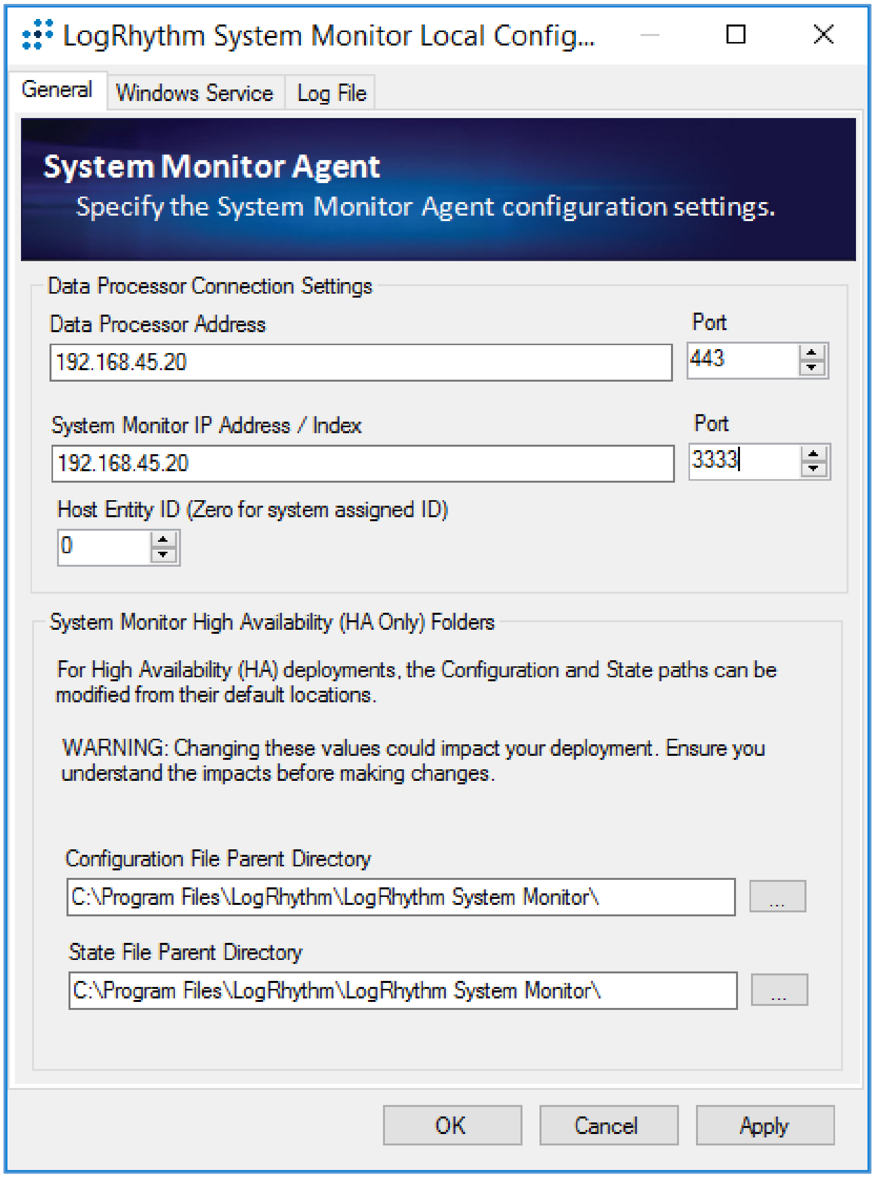
6. Click **Finish.**



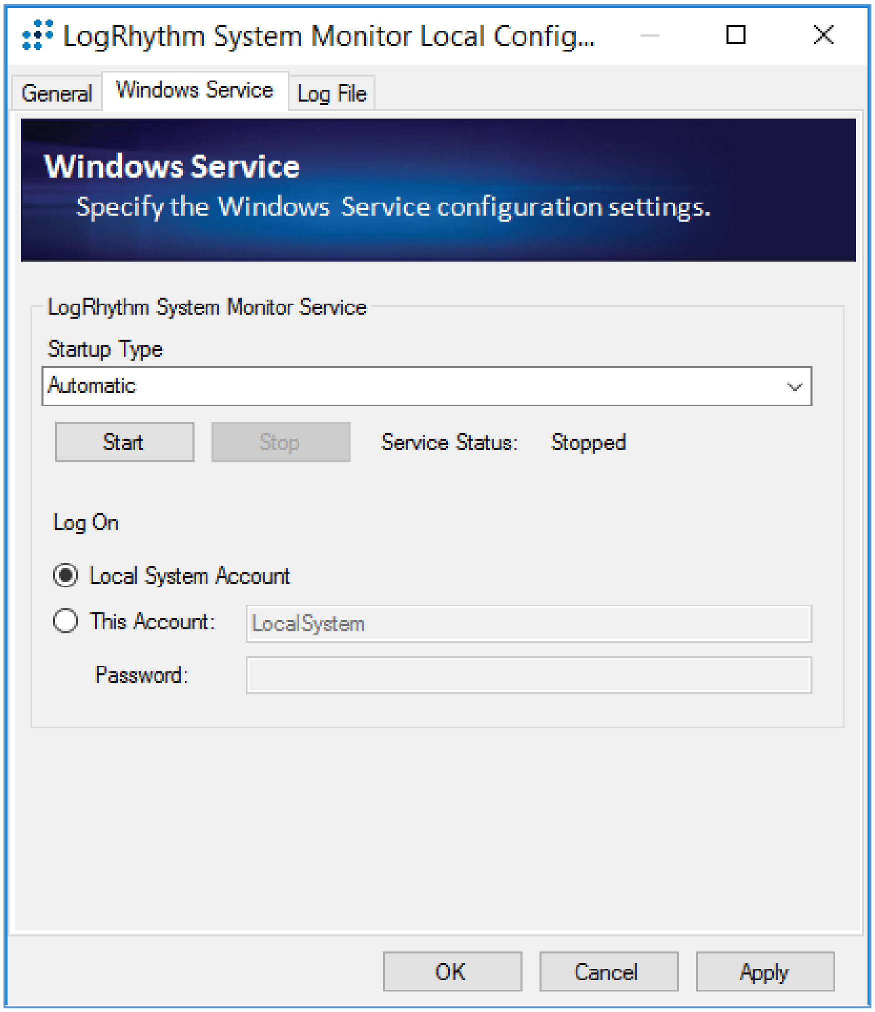
<u>**System Monitor Agent Configuration**</u>

1. After exiting the **LogRhythm System Monitor Service Install Wizard,** a LogRhythm System Monitor Local Configuration window displays. Under the **General** tab, provide the following information:

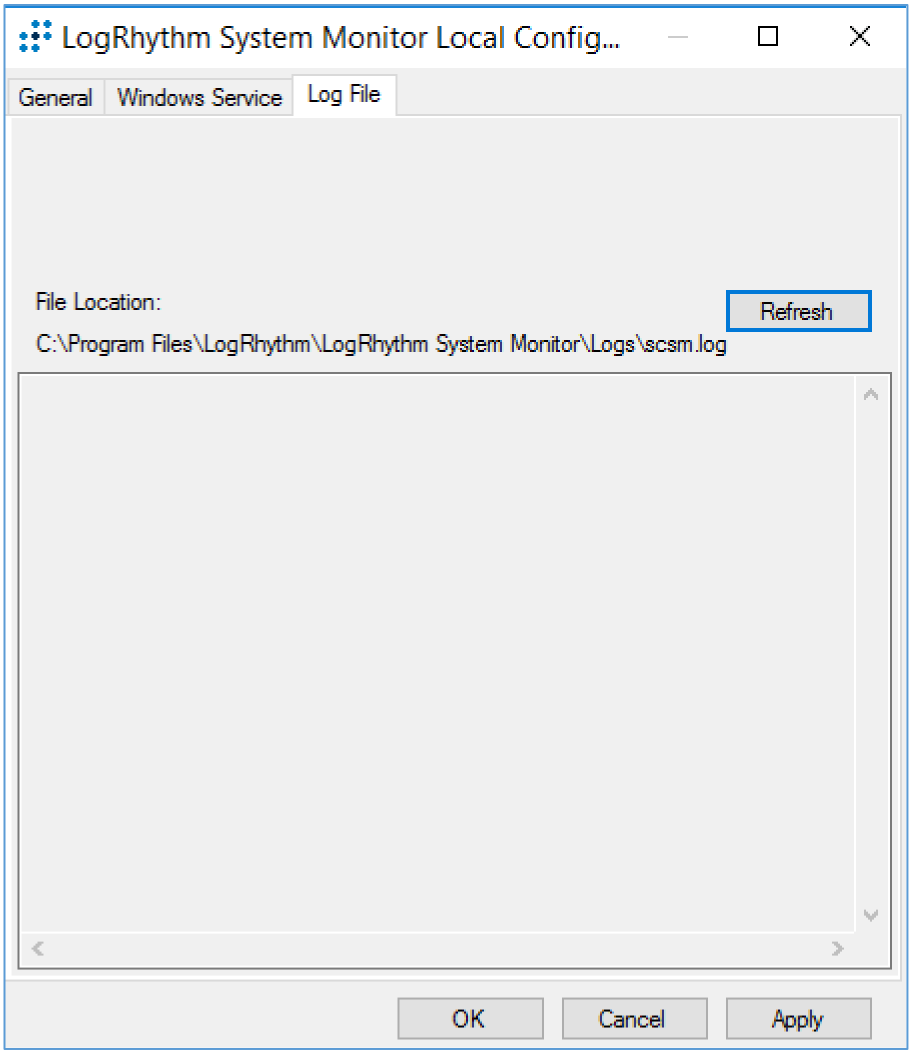
   a. **Data Process Address:** 192.168.45.20
   b. **System Monitor IP Address/Index:** 192.168.45.20
2. Click **Apply.**



3. Click the **Windows Service** tab.
4. Change the **Service Type** to **Automatic.**
5. Click **Apply.**



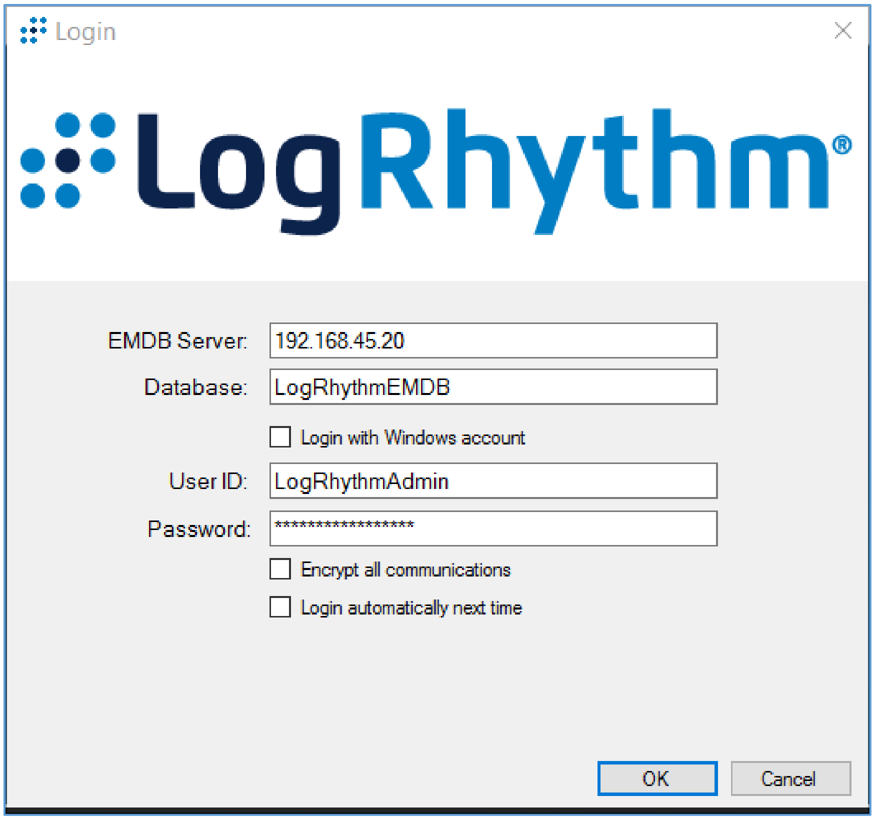
6. Click the **Log File** tab.
7. Click **Refresh** to ensure NetworkXDR log collection.
8. Click **OK** to exit the **Local Configuration Manager.**



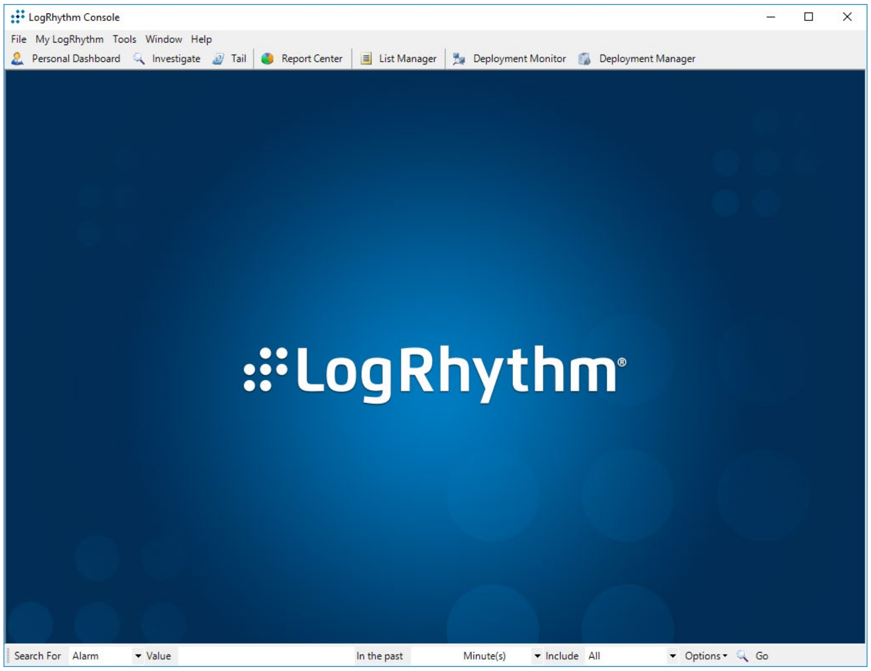
Add Workstation for System Monitor

Engineers added Clinical Workstation for System Monitor and Set Its Message Source Types in the LogRhythm Deployment Manager.

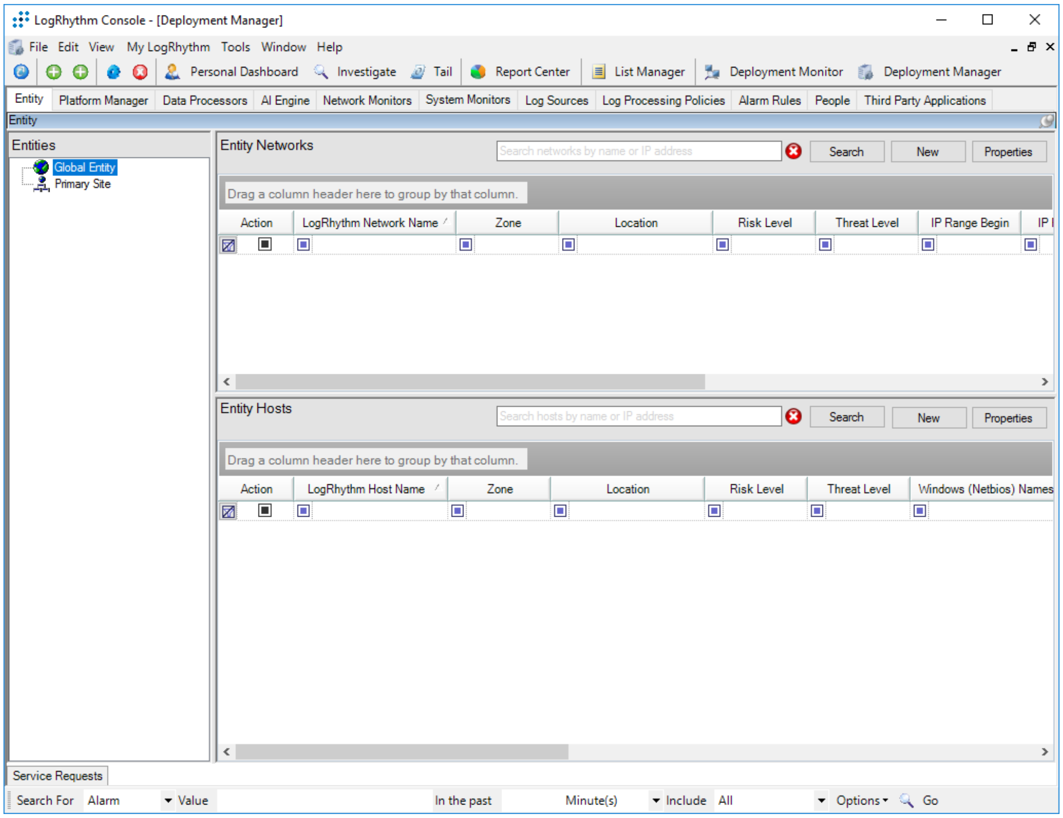
1. Log in to the **LogRhythm Console.**
    a. **User ID:** LogRhythmAdmin
    b. **Password:** **********



2. Navigate to the **Deployment Manager** in the menu ribbon.



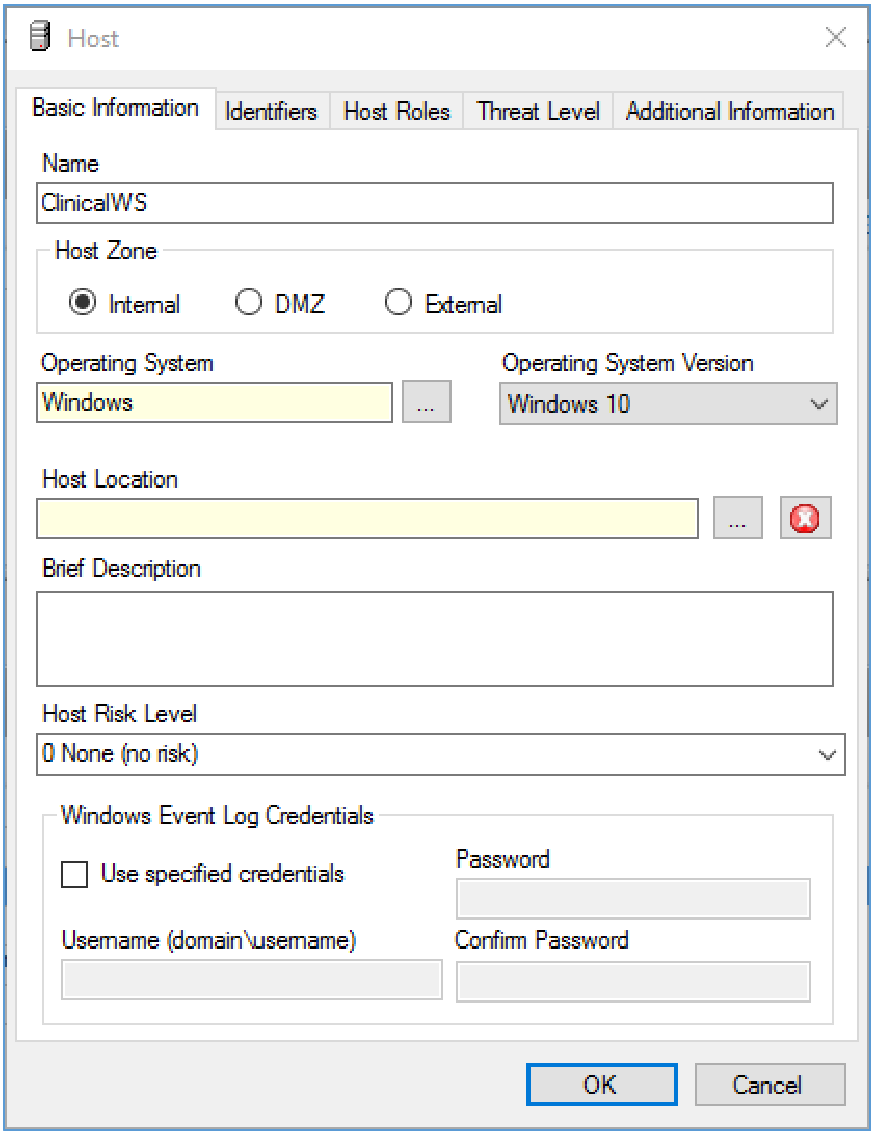
3. Under **Entity Hosts,** click on **New.**



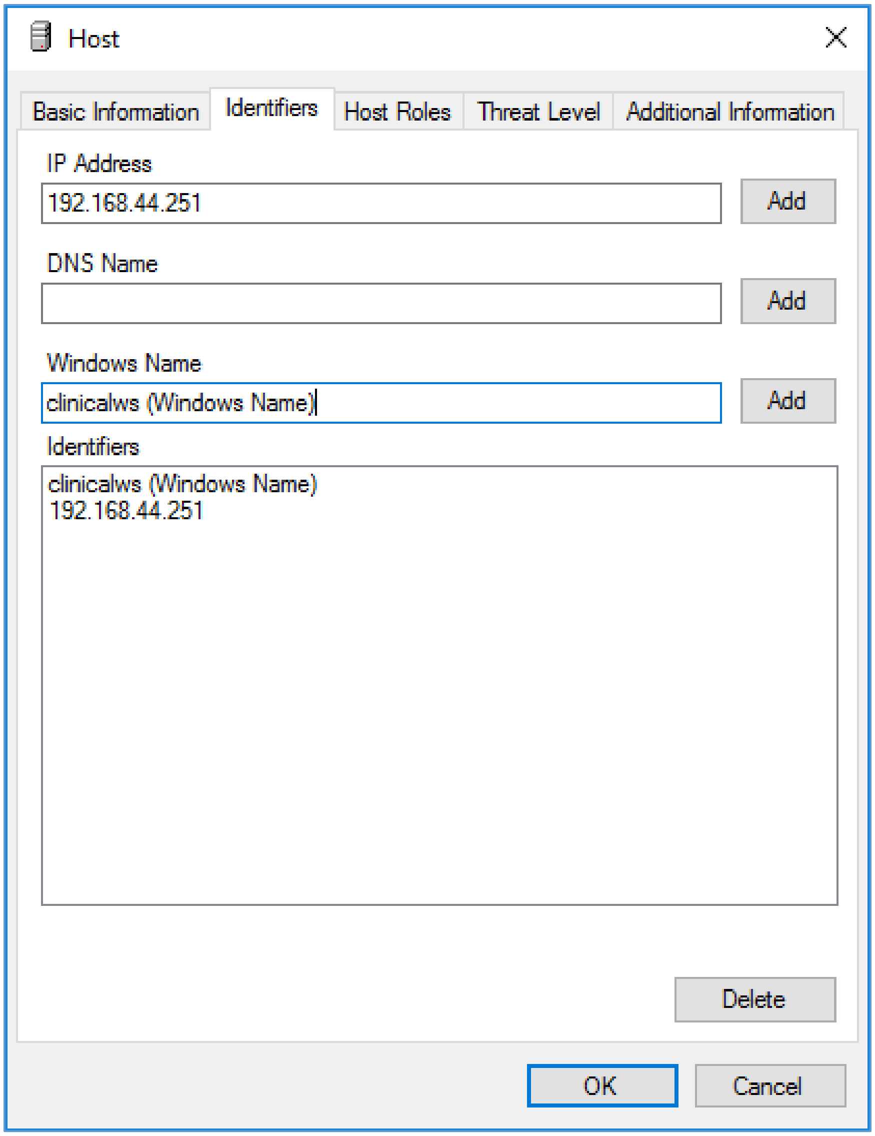
4. Click **New** to open the **Host** pop-up window, and enter the following under the **Basic Information** tab:

   a. **Name:** ClinicalWS

   b. **Host Zone:** Internal

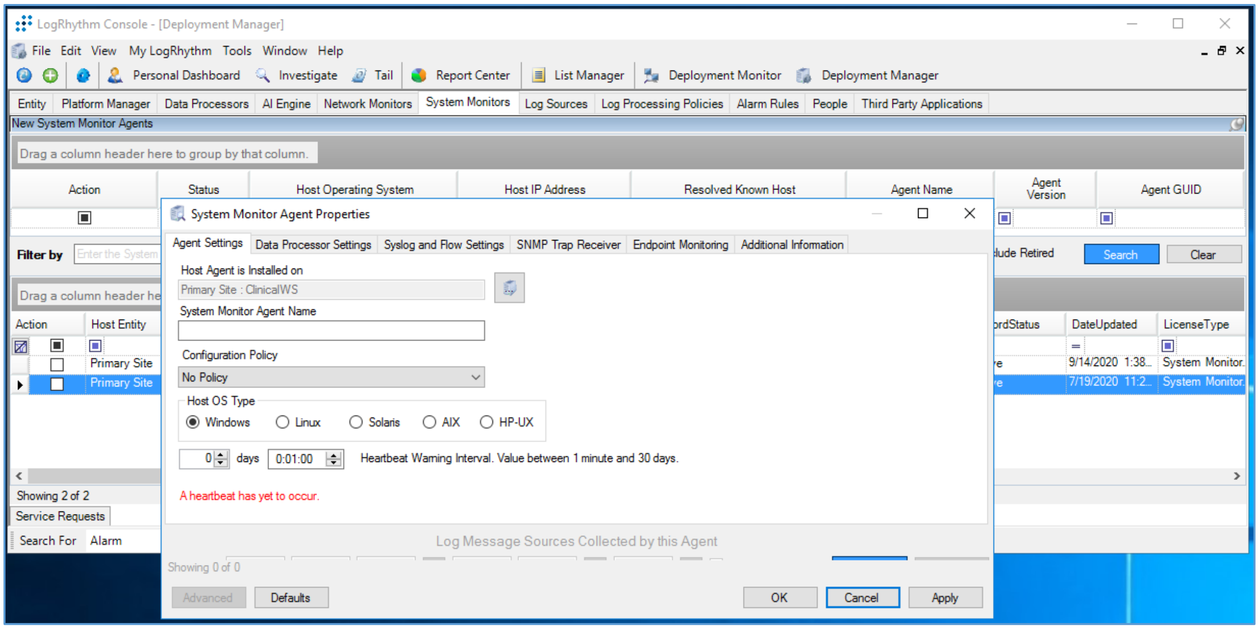


5. Navigate to the **Identifiers** tab, provide the following information in the appropriate fields, and click **Add**.
    a. **IP Address:** 192.168.44.251
    b. **Windows Name:** clinicalws (Windows Name)

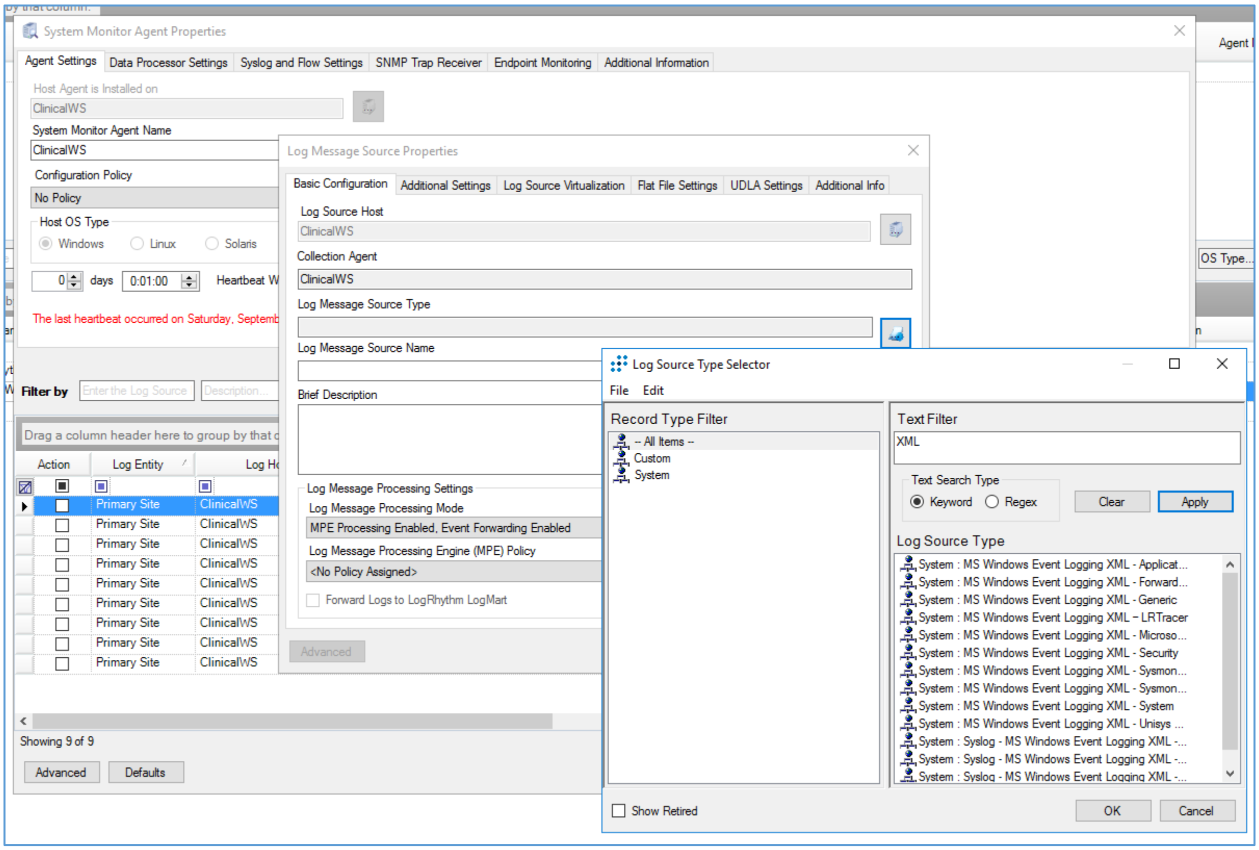


6. Add the **ClinicalWS** as a new system monitor agent by navigating to the **System Monitors** tab, right-clicking in the empty space, and selecting **New.**

7. In the System Monitor Agent Properties window, click the button next to **Host Agent is Installed on,** and select **Primary Site: ClinicalWS.**



8. Go to **System Monitors.**
9. Double-click **ClinicalWS.**
10. Under **LogSource** of the **System Monitor Agent Property** window, right-click in the empty space, and select **New.** The **Log Message Source Property** window will open.
11. Under the **Log Message Source Property** window, click the button associated with **Log Message Source Type.** It will open the **Log Source Selector** window.
12. In the text box to the right of the **Log Source Selector** window, type **XML,** and click **Apply.**
13. Select the **Log Source Type,** and click **OK.**



2.2.4 Data Security

Data security controls align with the NIST Cybersecurity Framework's PR.DS category. For this practice guide, the Onclave Networks solution was implemented as a component in the simulated patient home and simulated telehealth platform provider cloud environment. The Onclave Networks suite of tools provides secure communication between the two simulated environments when using broadband communications to exchange data.

2.2.4.1 Onclave SecureIoT

The Onclave SecureIoT deployment consists of six components: Onclave Blockchain, Onclave Administrator Console, Onclave Orchestrator, Onclave Bridge, and two Onclave Gateways. These components work together to provide secure network sessions between the deployed gateways.

Onclave SecureIoT Virtual Appliance Prerequisites

All Onclave devices require Debian 9.9/9.11/9.13. In addition, please prepare the following:

1. GitHub account.

2. Request an invitation to the Onclave Github account.

Once the GitHub invitation has been accepted and a Debian VM has been installed in the virtual environment, download and run the installation script to prepare the VM for configuration.

1. Run the command `sudo apt-get update`
2. Run the command `apt install git -y`
3. Run the command `sudo apt install openssh-server`
4. Run the command `git clone https://readonly:Sh1bboleth45@gitlab.onclave.net/onclave/build/install.git`
5. Navigate to the **/home/onclave/install** directory.
6. Run the command `chmod +x *.sh`

This process can be repeated for each virtual appliance that is deployed. The following guidance assumes the system user is named **onclave.**

<u>Onclave SecureIoT Blockchain Appliance Information</u>

CPU: 4

RAM: 8 GB

Storage: 120 GB (Thick Provision)

Network Adapter 1: VLAN 1317

Operating System: Debian Linux 9.11

<u>Onclave SecureIoT Blockchain Appliance Configuration Guide</u>

Before starting the installation script, prepare an answer for each question. The script will configure the server, assign a host name, create a self-signed certificate, and start the required services.

1. Run the command `nano/etc/hosts`
    a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device, as well as Onclave's docker server. This will include:
        i. 192.168.5.11 tele-adco.trpm.hclab
        ii. 192.168.5.12 tele-orch.trpm.hclab
        iii. 192.168.5.13 tele-bg.trpm.hclab

        iv. 192.168.5.14 tele-gw1.trpm.hclab
        v. 192.168.21.10 tele-gw2.trpm.hclab
        vi. 38.142.224.131 docker.onclave.net

2. Save the **file** and **exit.**
3. Navigate to the **/home/onclave/install** directory.
4. Run the command `./go.sh` and fill out the following information:
    a. **What type of device is being deployed?:** bci
    b. **Enter device hostname (NOT FQDN):** tele-bci
    c. **Enter device DNS domain name:** trpm.hclab
    d. **Enter the public NIC:** ens192
    e. **Enter the private NIC, if does not exist type in NULL:** NULL
    f. **Enter the IP Settings (DHCP or Static):** PUBLIC NIC (Static)
        i. address 192.168.5.10
        ii. netmask 255.255.255.0
        iii. gateway 192.168.5.1
        iv. dns-nameservers 192.168.1.10
    g. **What is the BCI FQDN for this environment?:** tele-bci.trpm.hclab
    h. **Enter the Docker Service Image Path:** NULL
    i. **Will system need TPM Emulator? (yes/no):** no
    j. **Keystore/Truststore password to be used?:** Onclave56
    k. **GitLab Username/Password (format username:password):** readonly:Sh1bboleth45
5. Wait for the **Blockchain server** to reboot.
6. Login to the appliance.
7. Run the command `su root` and enter the password.
8. Wait for the configuration process to finish.

<u>Onclave SecureIoT Administrator Console Appliance Information</u>

CPU: 4

RAM: 8 GB

Storage: 32 GB (Thick Provision)

Network Adapter 1: VLAN 1317

Operating System: Debian Linux 9.11

<u>Onclave SecureIoT Administrator Console Appliance Configuration Guide</u>

1. Run the command `scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-bci.trpm.hclab.crt /root/certs`
2. Run the command `nano/etc/hosts`
    a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device, as well as Onclave's docker server. This will include:
        i. 192.168.5.10 tele-bci.trpm.hclab
        ii. 192.168.5.12 tele-orch.trpm.hclab
        iii. 192.168.5.13 tele-bg.trpm.hclab
        iv. 192.168.5.14 tele-gw1.trpm.hclab
        v. 192.168.21.10 tele-gw2.trpm.hclab
        vi. 38.142.224.131 docker.onclave.net
    b. Save the **file** and **exit.**
3. Navigate to the **/home/onclave/install** directory.
4. Run the command `chmod +x *.sh`
5. Run the command `./go.sh` and fill out the following information:
    a. **What type of device is being deployed?:** adco
    b. **Enter device hostname (NOT FQDN):** tele-adco
    c. **Enter device DNS domain name:** trpm.hclab
    d. **Enter the public NIC:** ens192
    e. **Enter the private NIC, if does not exist type in NULL:** NULL

   f. **Enter the IP Settings (DHCP or Static):** PUBLIC NIC (Static)
      i. address 192.168.5.11
      ii. netmask 255.255.255.0
      iii. gateway 192.168.5.1
      iv. dns-nameservers 192.168.1.10
   g. **What is the BCI FQDN for this environment?:** tele-bci.trpm.hclab
   h. **Enter the Docker Service Image Path:** NULL
   i. **Will system need TPM Emulator? (yes/no):** yes
   j. **Keystore/Truststore password to be used?:** Onclave56
   k. **GitLab Username/Password (format username:password):** readonly:Sh1bboleth45

6. Wait for the **Administrator Console server** to reboot.
7. Login to the appliance.
8. Run the command `su root` and enter the password.
9. Wait for the configuration process to finish.
10. Navigate to the **/home/onclave** directory.
11. Run the command `docker pull docker.onclave.net/orchestrator-service:1.1.0`
12. Run the command `docker pull docker.onclave.net/bridge-service:1.1.0`
13. Run the command `docker pull docker.onclave.net/gateway-service:1.1.0`

<u>**Administrator Console Initialization and Bundle Creation**</u>

1. Using a web browser, navigate to **https://tele-adco.trpm.hclab.**
2. Click **Verify.**
3. Provide the following information:
   a. **Software ID** (provided by Onclave)
   b. **Password** (provided by Onclave)
   c. **PIN** (provided by Onclave)
4. Provide the following information to create a superuser account:

   a. **First Name:** *****
   b. **Last Name:** *****
   c. **Username:** *****@email.com
   d. **Password:** ********
   e. **Organization Name:** NCCoEHC
5. Click **Software Bundles.**
6. Click the **plus symbol** (top right), and provide the following information:
   a. **Bundle name:** nccoe-tele-orch
   b. **Bundle type:** Orchestrator
   c. **Owned by:** NCCoEHC
   d. **Orchestrator owner name:** HCLab
   e. **PIN:** ****
   f. **Password:** ********
7. Click **Create.**
8. Click the **plus symbol** (top right), and provide the following information:
   a. **Bundle name:** nccoe-tele-bg
   b. **Bundle type:** Bridge
   c. **Owned by:** NCCoEHC
9. Click **Create.**
10. Click the **plus symbol** (top right), and provide the following information:
    a. **Bundle name:** nccoe-tele-gw
    b. **Bundle type:** Gateway
    c. **Owned by:** NCCoEHC
11. Click **Create.**

<u>Transfer Ownership of Onclave Devices to the Orchestrator</u>

Once each Onclave device has been created and provisioned, it will show up in the Admin Console's web GUI. From here, the devices can be transferred to the Orchestrator with the following steps:

1. Using a web browser, navigate to **https://tele-adco.trpm.hclab.**
2. Click **Devices.**
3. Select the **checkbox** next to **tele-bg, tele-gw1,** and **tele-gw2.**
4. Click **Transfer ownership.**
5. Under **Select a new owner,** select **HCLab.**
6. Click **Transfer ownership.**

<u>Onclave SecureIoT Orchestrator Appliance Information</u>

CPU: 4

RAM: 8 GB

Storage: 32 GB (Thick Provision)

Network Adapter 1: VLAN 1317

Operating System: Debian Linux 9.11

<u>Onclave SecureIoT Orchestrator Appliance Configuration Guide</u>

1. Run the command **`scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-bci.trpm.hclab.crt /root/certs`**
2. Run the command **`nano/etc/hosts`**
    a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device, as well as Onclave's docker server. This will include:
        i. 192.168.5.10 tele-bci.trpm.hclab
        ii. 192.168.5.11 tele-adco.trpm.hclab
        iii. 192.168.5.13 tele-bg.trpm.hclab
        iv. 192.168.5.14 tele-gw1.trpm.hclab
        v. 192.168.21.10 tele-gw2.trpm.hclab
        vi. 38.142.224.131 docker.onclave.net
    b. Save the **file** and **exit.**

3. Run the command `nano /etc/network/interfaces`
    a. Edit the **Interfaces** file to include:
        i. iface ens192 inet static
            1. address 192.68.5.12
            2. netmask 255.255.255.0
            3. gateway 192.168.5.1
            4. dns-nameservers 192.168.1.10
    b. Save the **file** and **exit.**
4. Run the command `git clone https://github.com/Onclave-Networks/orch.git`
5. Navigate to the **/home/onclave/orch** directory.
6. Run the command `chmod +x *.sh`
7. Run the command `./go.sh` and fill out the following information:
    a. **What will be the hostname for your orchestrator?:** tele-orch
    b. **What will be the domain name for your orchestrator?:** trpm.hclab
    c. **Enter the device's public NIC:** ens192
    d. **What is the Blockchain environment?:** tele-bci
    e. **Will system need TPM Emulator? (yes/no):** yes
    f. **What is the docker image for the Orchestrator Service?:** docker.onclave.net/orchestrator-service:1.1.0- nccoe-tele-orch
8. Reboot the **Orchestrator server.**
9. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
10. Click **Verify.**
11. Provide the following information (created when making the bundle in the Admin Console):
    a. **Software ID**
    b. **Password**
    c. **PIN**

12. Provide the following information to create a superuser account:
    a. **First Name:** *****
    b. **Last Name:** *****
    c. **Username:** *****@email.com
    d. **Password:** ********
    e. **Organization Name:** Telehealth Lab

<u>Create a Customer in the Orchestrator</u>

1. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
2. Click **Customers.**
3. Click the **plus symbol.**
4. Under **Attributes > Customer Name,** enter **Telehealth Lab.**
5. Click **Create.**

<u>Create a Secure Enclave</u>

Once each Onclave device has been transferred to the Orchestrator, it will show up in the Orchestrator's web GUI. From here, the secure enclave can be created with the following steps:

1. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
2. Click **Secure Enclaves.**
3. Click the **plus symbol.**
4. Under **General,** provide the following information:
    a. **Secure Enclave name:** TeleHealth Secure Enclave
    b. **Customer:** Telehealth Lab
    c. **Sleeve ID:** 51
5. Under **Subnets**, provide a **Network Address (CIDR notation)** of **192.168.50.0/24.**
6. Under **Session Key**, provide a **Lifespan (minutes)** of **60.**

7. Click **Create.**

Prepare the Bridge for Inclusion in the Secure Enclave

1. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
2. Click **Devices.**
3. Select the **bridge,** and provide the following information:
    a. **Device Name:** tele-bg
    b. **Customer:** Telehealth Lab
    c. **Secure Enclaves:** Not assigned to any Secure Enclave
    d. **State:** Orchestrator Acquired
    e. **Secure tunnel port number:** 820
    f. **Private interface IP address undefined:** checked
4. Click **Save.**

Prepare the Telehealth Gateway for Inclusion in the Secure Enclave

1. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
2. Click **Devices.**
3. Select the **bridge,** and provide the following information:
    a. **Device Name:** tele-gw1
    b. **Customer:** Telehealth Lab
    c. **Secure Enclaves:** Not assigned to any Secure Enclave
    d. **State:** Orchestrator Acquired
    e. **Secure tunnel port number:** 820
    f. **Private interface IP address undefined:** checked
4. Click **Save.**

Prepare the Home Gateway for Inclusion in the Secure Enclave

1. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
2. Click **Devices.**
3. Select the **bridge,** and provide the following information:

   a. **Device Name:** tele-gw2
   b. **Customer:** Telehealth Lab
   c. **Secure Enclaves:** Not assigned to any Secure Enclave
   d. **State:** Orchestrator Acquired
   e. **Secure tunnel port number:** 820
   f. **Private interface IP address undefined:** checked
4. Click **Save.**

Establish the Secure Enclave

Once the secure enclave has been created and each Onclave device has been configured with a name and customer, the secure enclave can be established with the following steps:

1. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
2. Click **Secure Enclaves.**
3. Click the **edit symbol** for the previously created secure enclave.
4. Under **Topology,** click **Add a Bridge.**
5. Select **tele-bg.**
6. Click **Add.**
7. Click **Add a Gateway.**
8. Select **tele-gw1.**
9. Click **Add.**
10. Click **Add a Gateway.**
11. Select **tele-gw2.**
12. Click **Add.**
13. Under **Topology Controls,** toggle on **Approve topology.**
14. Click **Save Changes.**
15. Click **Devices.**
16. Refresh the **Devices** page until each device is labeled as **Topology Approved.**

17. Click **Secure Enclaves.**
18. Click the **edit symbol** for the previously created secure enclave.
19. Under **Topology,** toggle on **Trust All Devices.**
20. Click **Save Changes.**
21. Click **Devices.**
22. Refresh the **Devices** page until each device is labeled as **Secured.**

<u>Onclave SecureIoT Bridge Appliance Information</u>

CPU: 4

RAM: 8 GB

Storage: 32 GB (Thick Provision)

Network Adapter 1: VLAN 1317

Network Adapter 2: VLAN 1319

Operating System: Debian Linux 9.11

<u>Onclave SecureIoT Bridge Appliance Configuration Guide</u>

1. Run the command `scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-bci.trpm.hclab.crt /root/certs`
2. Run the command `nano /etc/hosts`
    a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device, as well as Onclave's docker server. This will include:
        i. 192.168.5.10 tele-bci.trpm.hclab
        ii. 192.168.5.11 tele-adco.trpm.hclab
        iii. 192.168.5.12 tele-orch.trpm.hclab
        iv. 192.168.5.14 tele-gw1.trpm.hclab
        v. 192.168.21.10 tele-gw2.trpm.hclab
        vi. 38.142.224.131 docker.onclave.net
3. Run the command `nano /etc/network/interfaces`

   a. Edit the **Interfaces** file to include:
      i. iface ens192 inet static
         1. address 192.68.5.13
         2. netmask 255.255.255.0
         3. gateway 192.168.5.1
         4. dns-nameservers 192.168.1.10
      ii. iface ens224 inet static
   b. Save the **file** and **exit.**
4. Run the command `git clone https://github.com/Onclave-Networks/bridge.git`
5. Navigate to the **/home/onclave/bridge** directory.
6. Run the command `chmod +x *.sh`
7. Run the command `./go.sh`
   a. **What will be the hostname for your bridge?:** tele-bg
   b. **What will be the domain name for your bridge?:** trpm.hclab
   c. **Enter the device's public NIC:** ens192
   d. **Enter the device's private NIC:** ens224
   e. **What is the Blockchain environment?:** tele-bci
   f. **Will system need TPM Emulator? (yes/no):** yes
   g. **What is the docker image for the Bridge Service?:** docker.onclave.net/bridge-service:1.1.0- nccoe-tele-bg
8. Reboot the **Bridge server.**

<u>Onclave SecureIoT Telehealth Gateway Appliance Information</u>

CPU: 2

RAM: 8 GB

Storage: 16 GB

Network Adapter 1: VLAN 1317

Network Adapter 2: VLAN 1349

Operating System: Debian Linux 9.11

<u>**Onclave SecureIoT Telehealth Gateway Appliance Configuration Guide**</u>

1. Run the command `scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-bci.trpm.hclab.crt /root/certs`
2. Run the command `nano /etc/hosts`
    a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device, as well as Onclave's docker server. This will include:
        i. 192.168.5.10 tele-bci.trpm.hclab
        ii. 192.168.5.11 tele-adco.trpm.hclab
        iii. 192.168.5.12 tele-orch.trpm.hclab
        iv. 192.168.5.13 tele-bg.trpm.hclab
        v. 192.168.21.10 tele-gw2.trpm.hclab
        vi. 38.142.224.131 docker.onclave.net
3. Run the command `nano /etc/network/interfaces`
    a. Edit the **Interfaces** file to include:
        i. iface enp3s0 inet static
            1. address 192.168.5.14
            2. netmask 255.255.255.0
            3. gateway 192.168.5.1
            4. dns-nameservers 192.168.1.10
        ii. iface ens224 inet dhcp
    b. Save the **file** and **exit.**
4. Run the command `git clone https://github.com/Onclave-Networks/gateway.git`
5. Navigate to the **/home/onclave/gateway** directory.
6. Run the command `chmod +x *.sh`

7. Run the command **`./go.sh`**
    a. **What will be the hostname for your gateway?:** tele-gw1
    b. **What will be the domain name for your gateway?:** trpm.hclab
    c. **Enter the device's public NIC:** enp3s0
    d. **Enter the device's private NIC:** enp2s0
    e. **What is the Blockchain environment?:** tele-bci
    f. **Will system need TPM Emulator? (yes/no):** no
    g. **What is the docker image for the Gateway Service?:** docker.onclave.net/ gateway-service:1.1.0- nccoe-tele-gw
8. Reboot the **Gateway server.**

<u>**Onclave SecureIoT Home Wi-Fi Gateway Appliance Information**</u>

CPU: 1

RAM: 4 GB

Storage: 16 GB

Network Adapter 1: VLAN 1332

Network Adapter 2: VLAN 1350 (Wi-Fi)

Operating System: Debian Linux 9.11

<u>**Onclave SecureIoT Home Wi-Fi Gateway Appliance Configuration Guide**</u>

1. Run the command **`scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-bci.trpm.hclab.crt /root/certs`**
2. Run the command **`nano /etc/hosts`**
    a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device, as well as Onclave's docker server. This will include:
        i. 192.168.5.10 tele-bci.trpm.hclab
        ii. 192.168.5.11 tele-adco.trpm.hclab
        iii. 192.168.5.12 tele-orch.trpm.hclab
        iv. 192.168.5.13 tele-bg.trpm.hclab

            v. 192.168.5.14 tele-gw1.trpm.hclab
            vi. 38.142.224.131 docker.onclave.net

3. Run the command `nano /etc/network/interfaces`
    a. Edit the **Interfaces** file to include:
        i. iface enp3s0 inet static
            1. address 192.168.21.10
            2. netmask 255.255.255.0
            3. gateway 192.168.21.1
            4. dns-nameservers 192.168.1.10
        ii. iface br0 inet static
            1. bridge_ports br51 wlp5s0
        iii. iface wlp5s0 inet manual
    b. Save the **file** and **exit.**
4. Run the command `git clone https://github.com/Onclave-Networks/hostapd-29.git`
5. Navigate to the **/home/onclave/hostapd-29** directory.
6. Run the command `chmod +x *.sh`
7. Run the command `./hostapd-29.sh`
8. Navigate to the **/home/onclave** directory.
9. Run the command `git clone https://github.com/Onclave-Networks/hostapd-client.git`
10. Navigate to the **/home/onclave/hostapd-client** directory.
11. Run the command `chmod +x *.sh`
12. Run the command `./hostapd-client.sh`
13. Navigate to the **/home/onclave** directory.
14. Run the command `git clone https://github.com/Onclave-Networks/gateway.git`
15. Navigate to the **/home/onclave/gateway** directory.
16. Run the command `chmod +x *.sh`

17. Run the command `./go.sh`
    a. **What will be the hostname for your gateway?:** tele-gw2
    b. **What will be the domain name for your gateway?:** trpm.hclab
    c. **Enter the device's public NIC:** enp3s0
    d. **Enter the device's private NIC:** wlp5s0
    e. **What is the Blockchain environment?:** tele-bci
    f. **Will system need TPM Emulator? (yes/no):** no
    g. **What is the docker image for the Gateway Service?:** docker.onclave.net/ gateway-service:1.1.0- nccoe-tele-gw
18. Reboot the **Gateway server.**

Appendix A List of Acronyms

AD	Active Directory
CPU	Central Processing Unit
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
FMC	Firepower Management Center
FTD	Firepower Threat Defense
GB	Gigabyte
HDO	Healthcare Delivery Organization
HIS	Health Information System
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OVA	Open Virtual Appliance or Application
PACS	Picture Archiving and Communication System
RAM	Random Access Memory
RPM	Remote Patient Monitoring
SFC	Stealthwatch Flow Collector
SIEM	Security Incident Event Management
SMC	Stealthwatch Management Center
SP	Special Publication
TB	Terabyte
URL	Uniform Resource Locator
vCPU	Virtual Central Processing Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
XDR	Extended Detection and Response

Appendix B References

[1] J. Cawthra et al., *Securing Picture Archiving and Communication System (PACS)*, National Institute of Standards and Technology (NIST) Special Publication 1800-24, NIST, Gaithersburg, Md., Sep. 2019. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-pacs-nist-sp1800-24-draft.pdf.

[2] *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.

[3] Tenable. Managed by Tenable.sc. [Online]. Available: https://docs.tenable.com/nessus/8_10/Content/ManagedbyTenablesc.htm.

[4] Microsoft. Install Active Directory Domain Services (Level 100). [Online]. Available: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-#to-install-ad-ds-by-using-server-manager.

[5] Cisco. *Cisco Firepower Management Center Virtual Getting Started Guide.* [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcv/fpmc-virtual/fpmc-virtual-vmware.html.

[6] Cisco. *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide:* Deploy the Firepower Threat Defense Virtual. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg/ftdv-vmware-deploy.html.

[7] Cisco. *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide:* Managing the Firepower Threat Defense Virtual with the Firepower Management Center. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg/ftdv-vmware-fmc.html.

[8] Cisco. *Cisco Stealthwatch Installation and Configuration Guide 7.1*. [Online]. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation_configuration/SW_7_1_Installation_and_Configuration_Guide_DV_1_0.pdf.

[9] Cisco. Deploy VAs in VMware. [Online]. Available: https://docs.umbrella.com/deployment-umbrella/docs/deploy-vas-in-vmware.