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

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.

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

1 Introduction 1
1.1 How to Use this Guide 1
1.2 Build Overview 2
1.3 Typographic Conventions 3
1.4 Logical Architecture Summary 3
2 Product Installation Guides 4
2.1 Telehealth Platform Provider 4
2.1.1 Accuhealth 6
2.1.2 Vivify Health 10
2.2 Security Capabilities 14
2.2.1 Risk Assessment Controls 14
2.2.2 Identity Management, Authentication, and Access Control 32
2.2.3 Security Continuous Monitoring 75
2.2.4 Data Security 142
Appendix A List of Acronyms 159
Appendix B References 160

List of Figures

Figure 1-1 Final Architecture 4
Figure 2-1 RPM Communications Paths 6

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

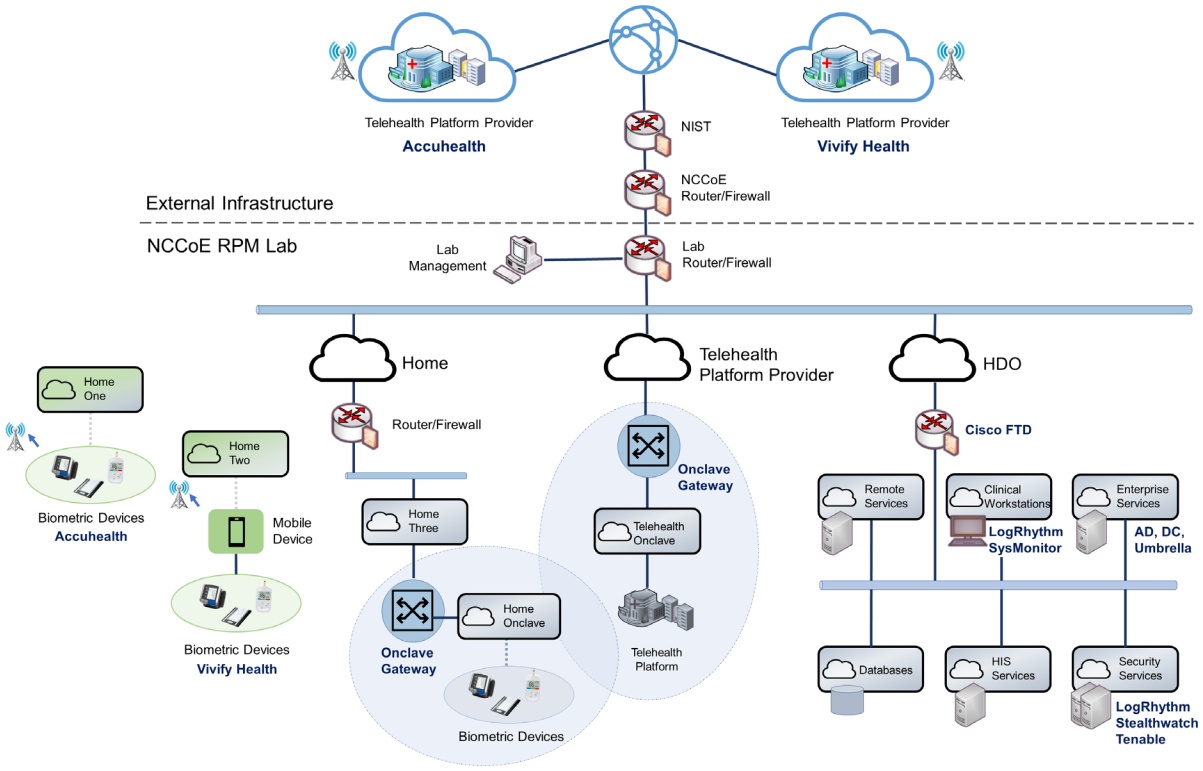
The following table presents typographic conventions used in this volume.

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.

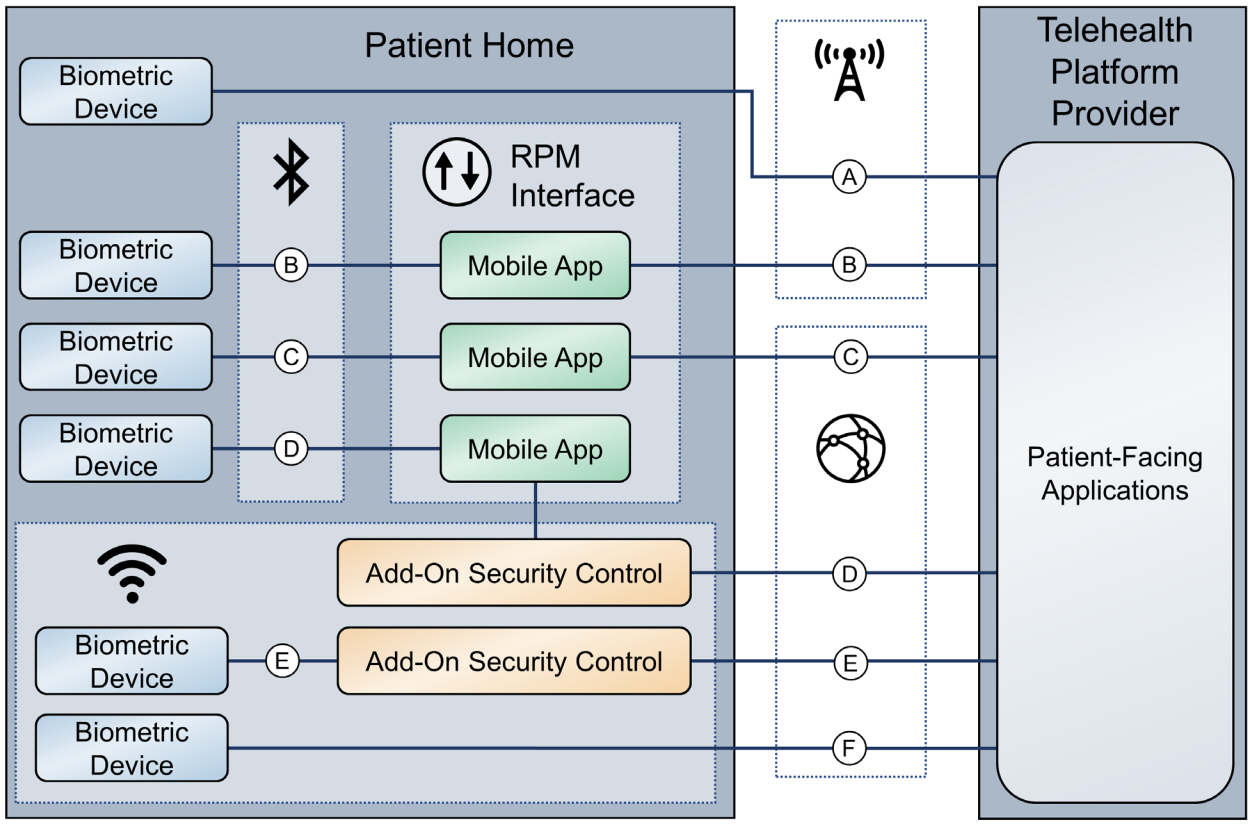
2.1 Telehealth Platform Provider

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.

249 **Figure 2-1 RPM Communications Paths**



250

251 2.1.1 Accuhealth

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

259 *2.1.1.1 Patient Home–Communication Path A*

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

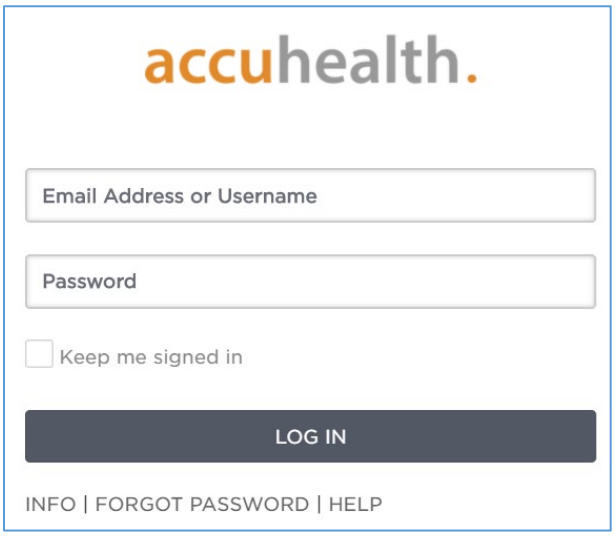
Accuhealth received patient contact information and configured biometric devices appropriate for the RPM program in which the patient was enrolled. Accuhealth configured biometric devices to communicate via cellular data, which is depicted as communication path A of Figure 2-1. Biometric devices, thus,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

2.1.1.2 HDO

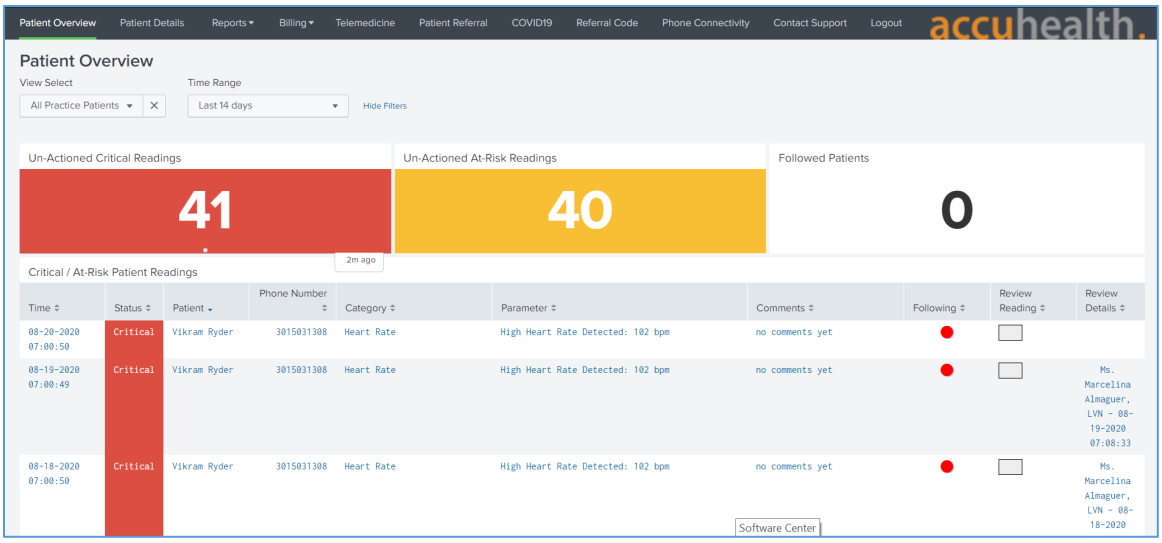
The Accuhealth solution includes installing an application within the HDO environment. Clinicians access a portal hosted by Accuhealth that allows a clinician to view patient biometric data. The application requires unique user accounts and role-based access control. System administrators create accounts 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.

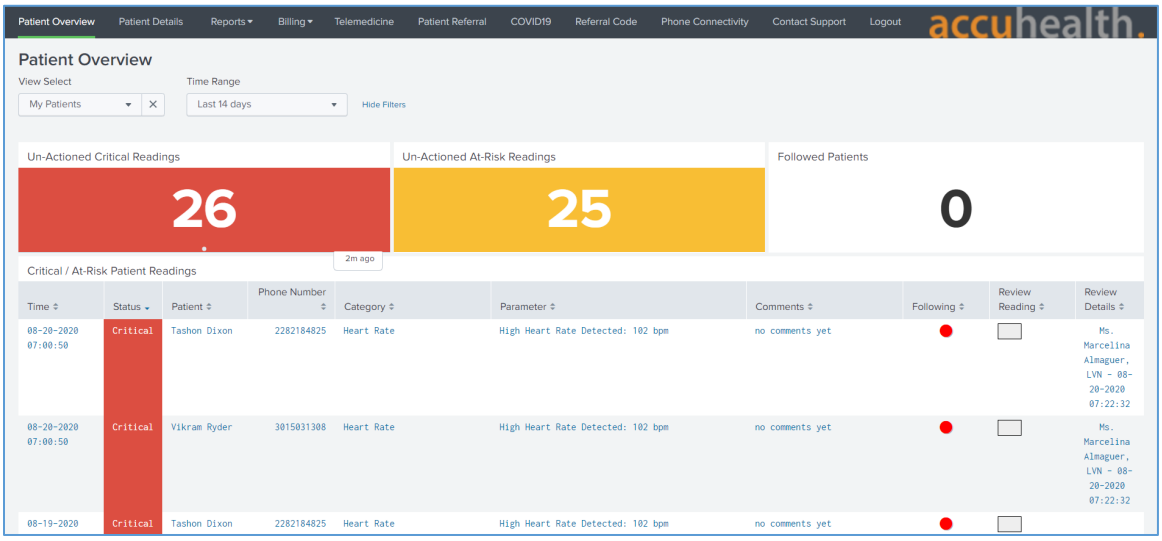
1. Access a device that has a web browser.
2. Navigate to Accuhealth login page, and provide a **Username** and **Password.** The following screenshots show a doctor's point of view in the platform.
3. Click **LOG IN.**



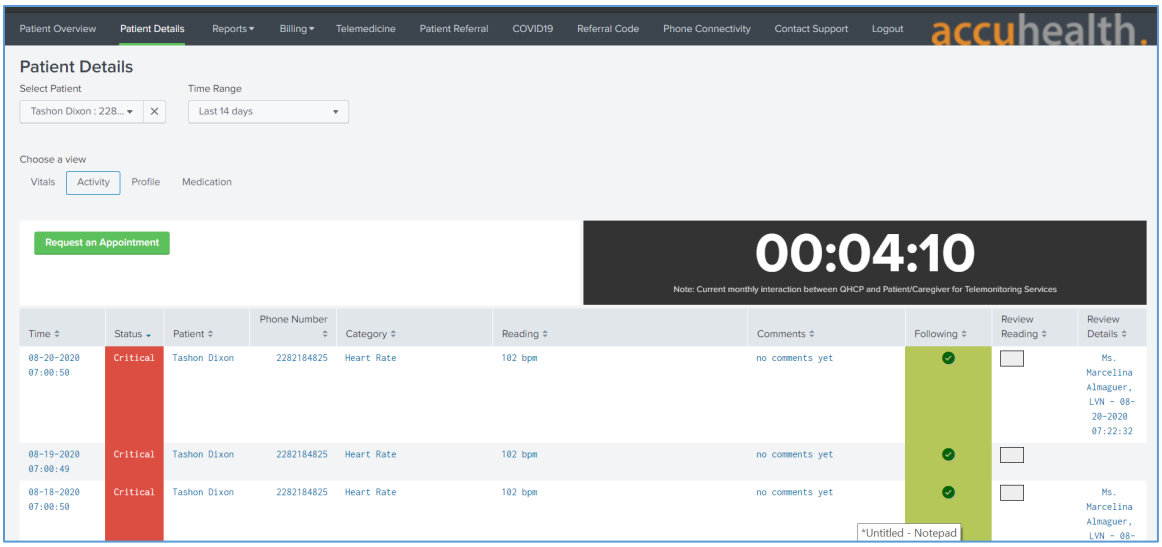
After logging in, the **Patient Overview** screen displays.



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.

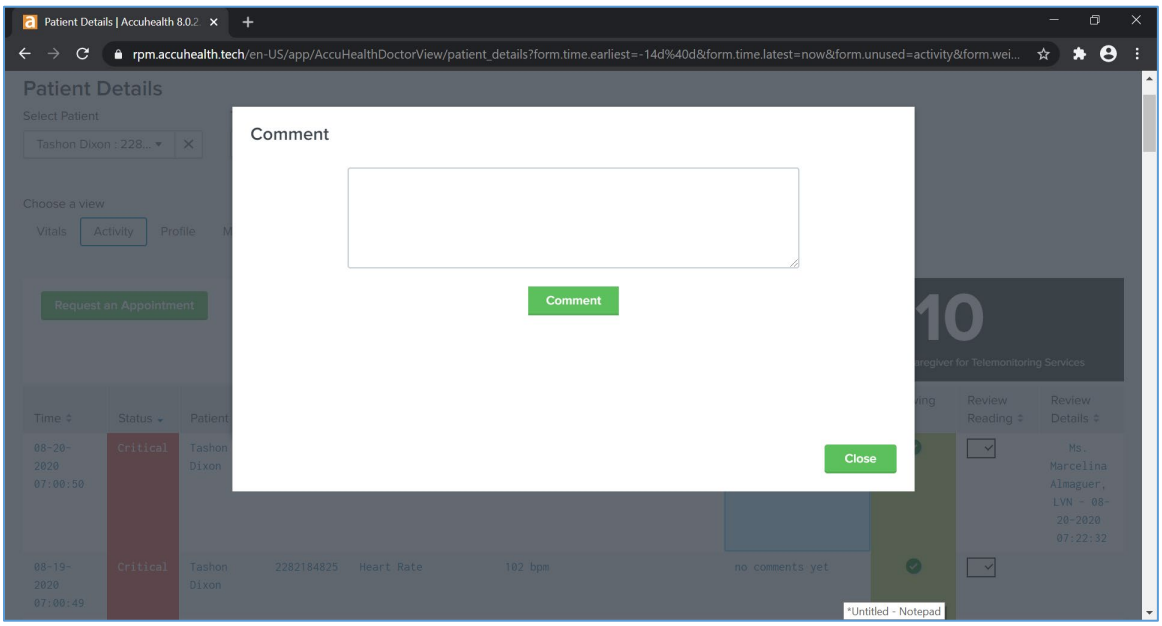


285 6. To leave a comment on a reading, click **no comments yet** under the **Comments** column on the
286 row of the reading to which the comment refers.

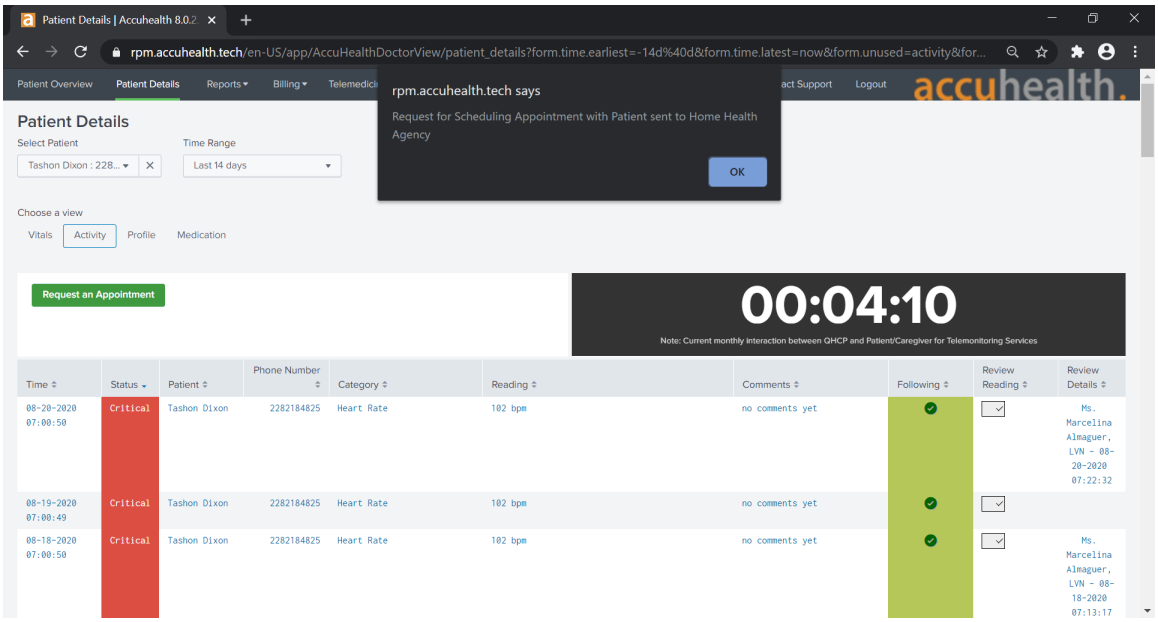
287 7. A **Comment** screen displays that allows free text input.

288 8. Click **Comment.**

289 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.

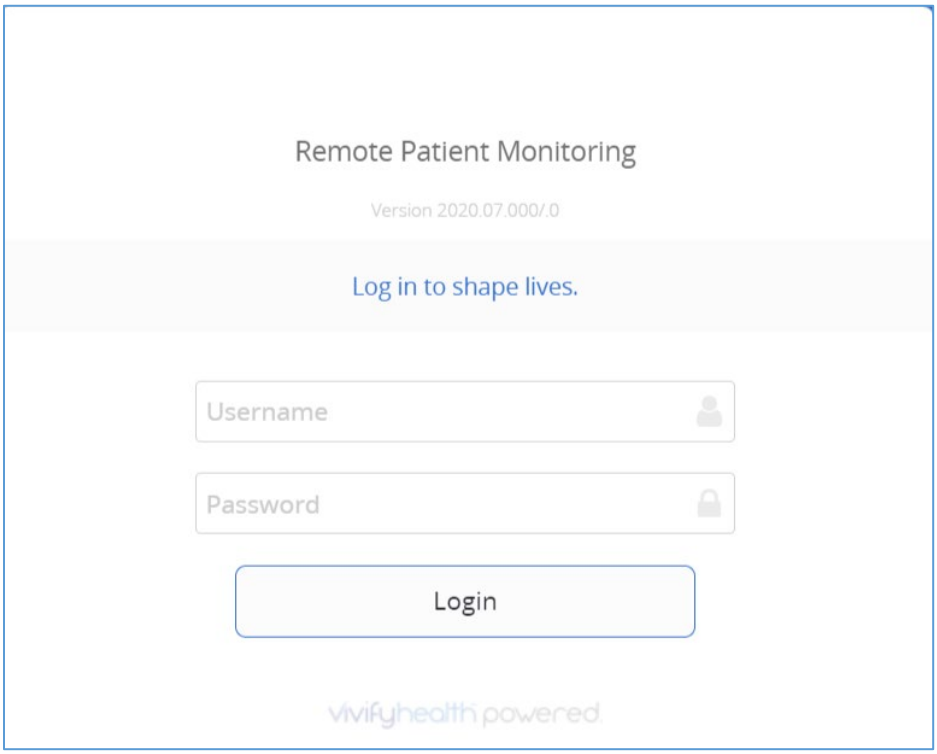
Communication path D required more add-on security controls to be configured in the virtual cloud environment. For this communication pathway, the representative Vivify Pathways Care Team Portal was connected to an Onclave Telehealth Gateway. This gateway accepted data transmissions from the RPM interface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

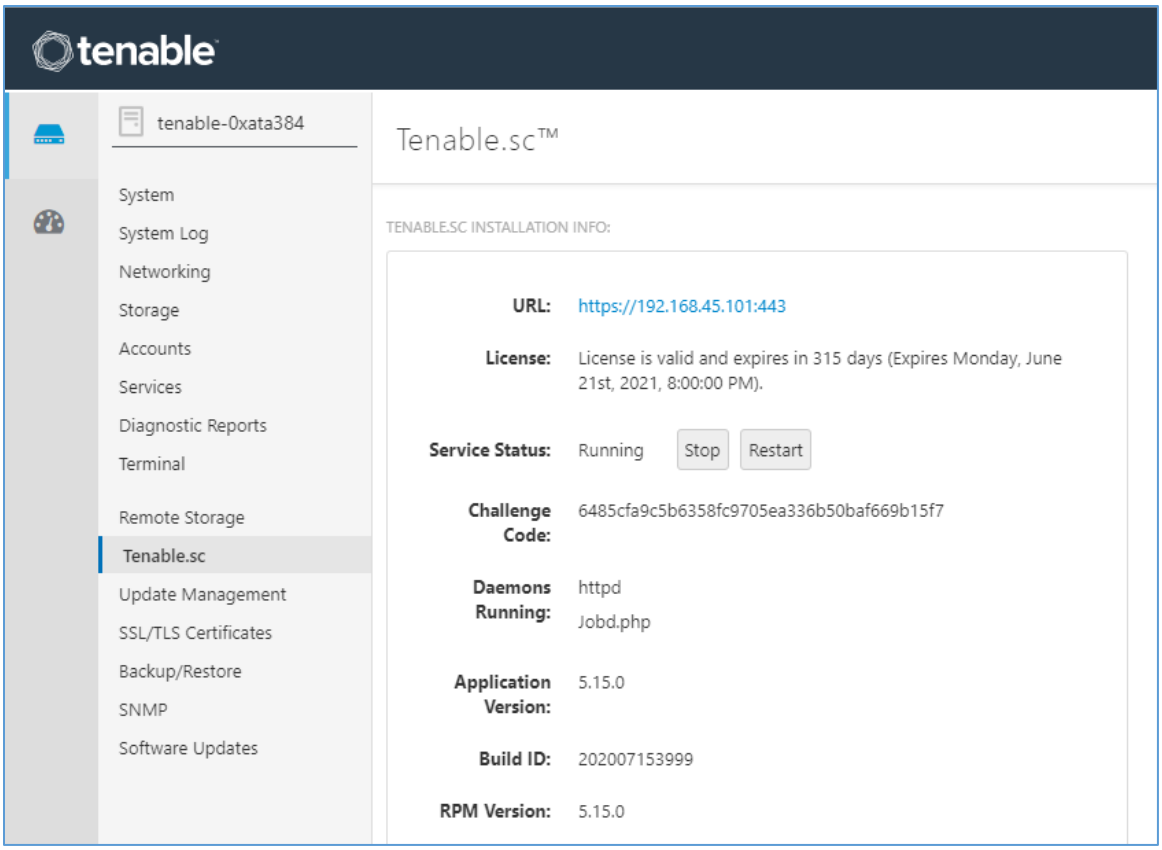
Tenable.sc Installation

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.**

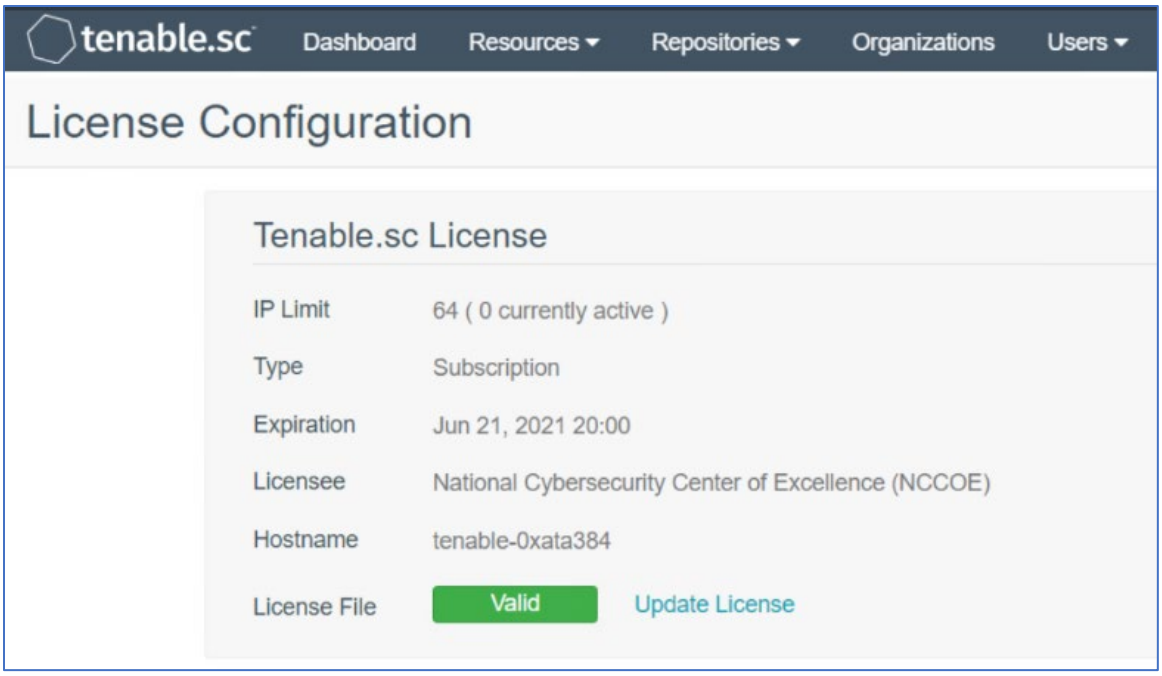
5. For the first login, use **wizard** as the **Username** and **admin** for the **Password.**
6. Tenable.sc prompts a pop-up window for creating a new **admin username** and **password.**
7. Repeat step 5 using the new username and password.
    a. **Username:** admin
    b. **Password:** **********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



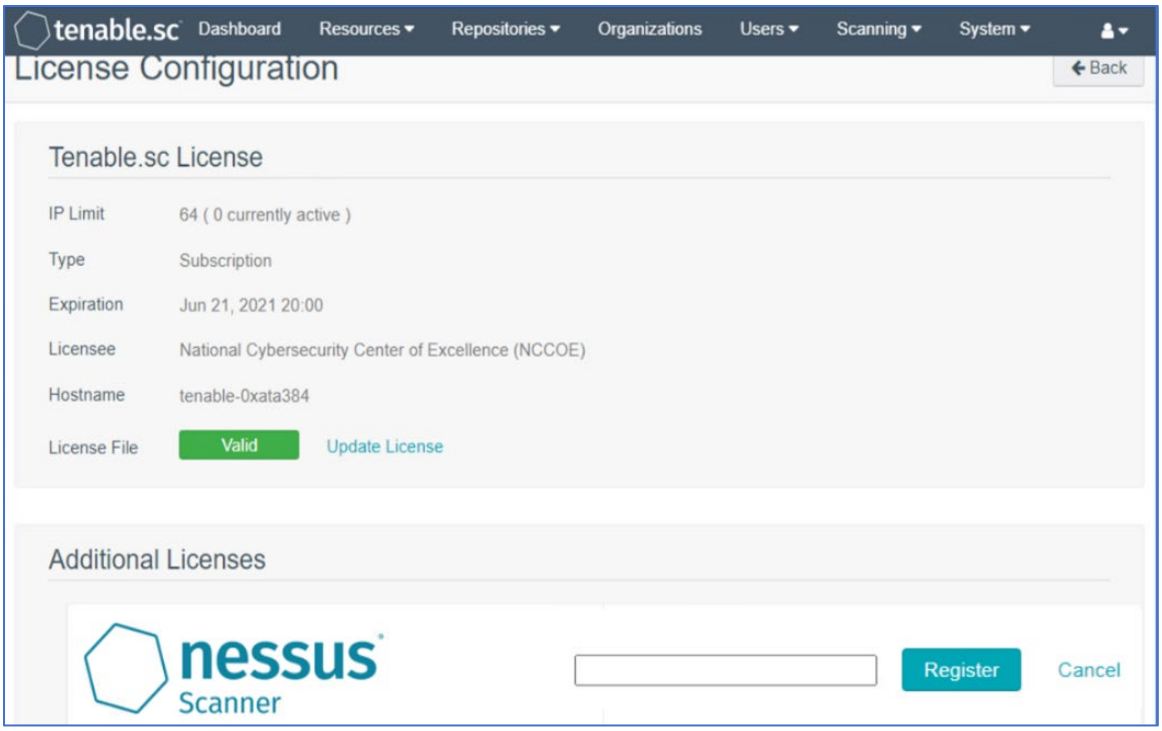
11. Log in to Tenable.sc by using the credentials created in previous steps, and click **Sign In.**
    a. **Username:** admin
    b. **Password:** **********

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.



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

437 21. Click **Register.**

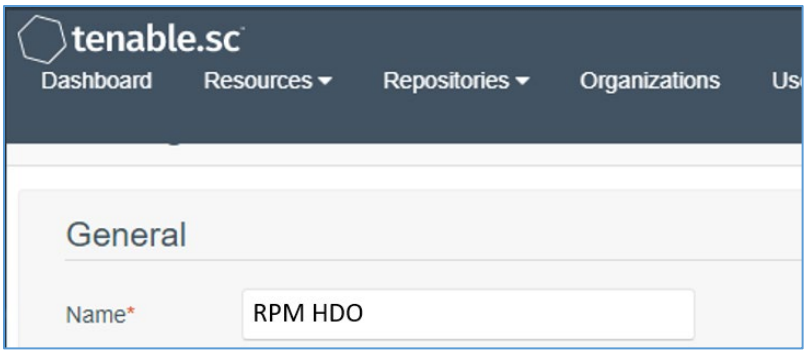


Tenable.sc Configuration

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.

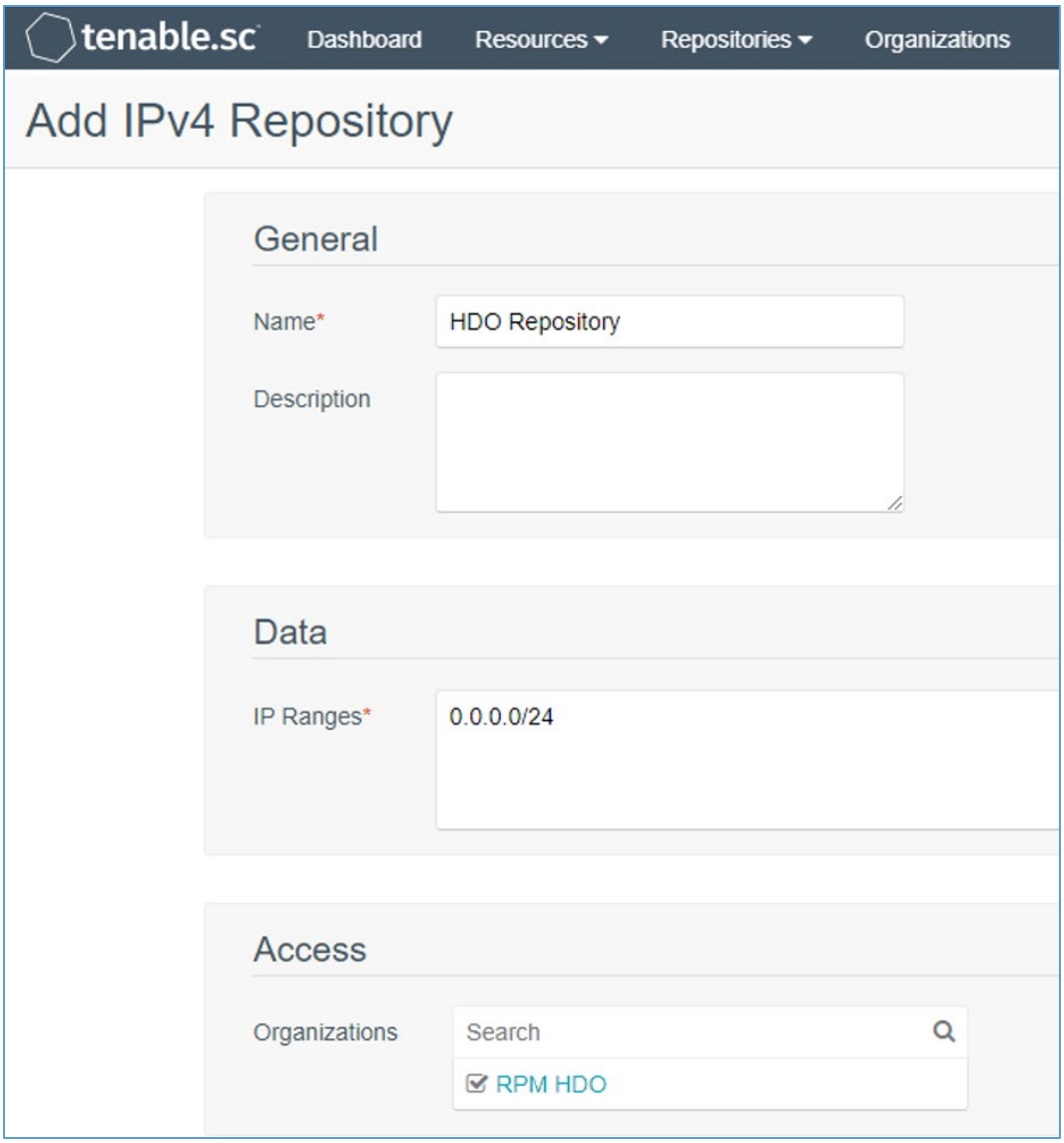
Add an Organization

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.**



Add a User

1. Navigate to the **Users** drop-down list in the menu ribbon.
2. Select **Users.**
3. Click **+Add** in the top right corner. An **Add User** page displays. Provide the following information:
    a. **Role:** Security Manager
    b. **Organization:** RPM HDO

c. **First Name:** Test

d. **Last Name:** User

e. **Username:** TestSecManager

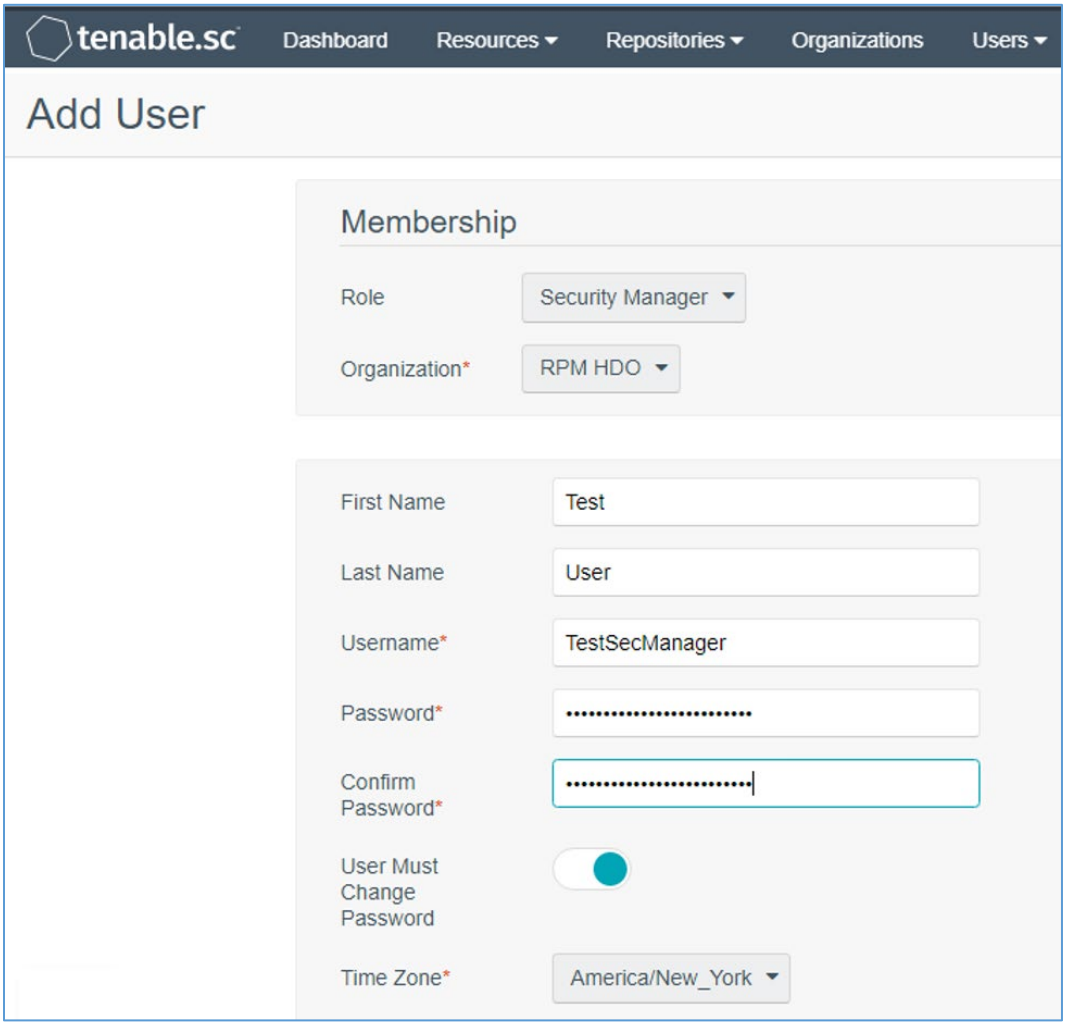
f. **Password:** **********

g. **Confirm Password:** **********

h. Enable **User Must Change Password.**

i. **Time Zone:** America/New York

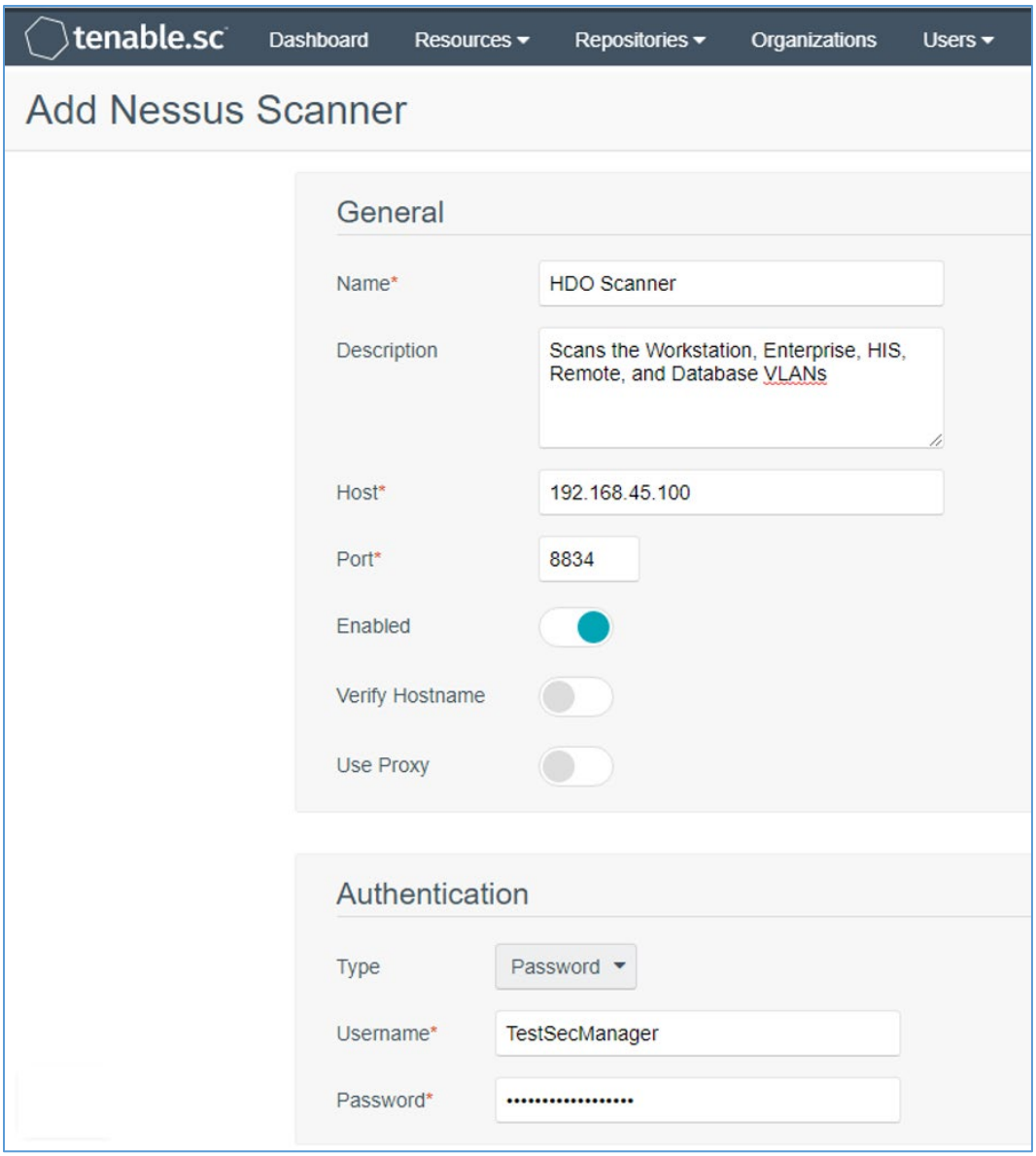
4. Click **Submit.**



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.**



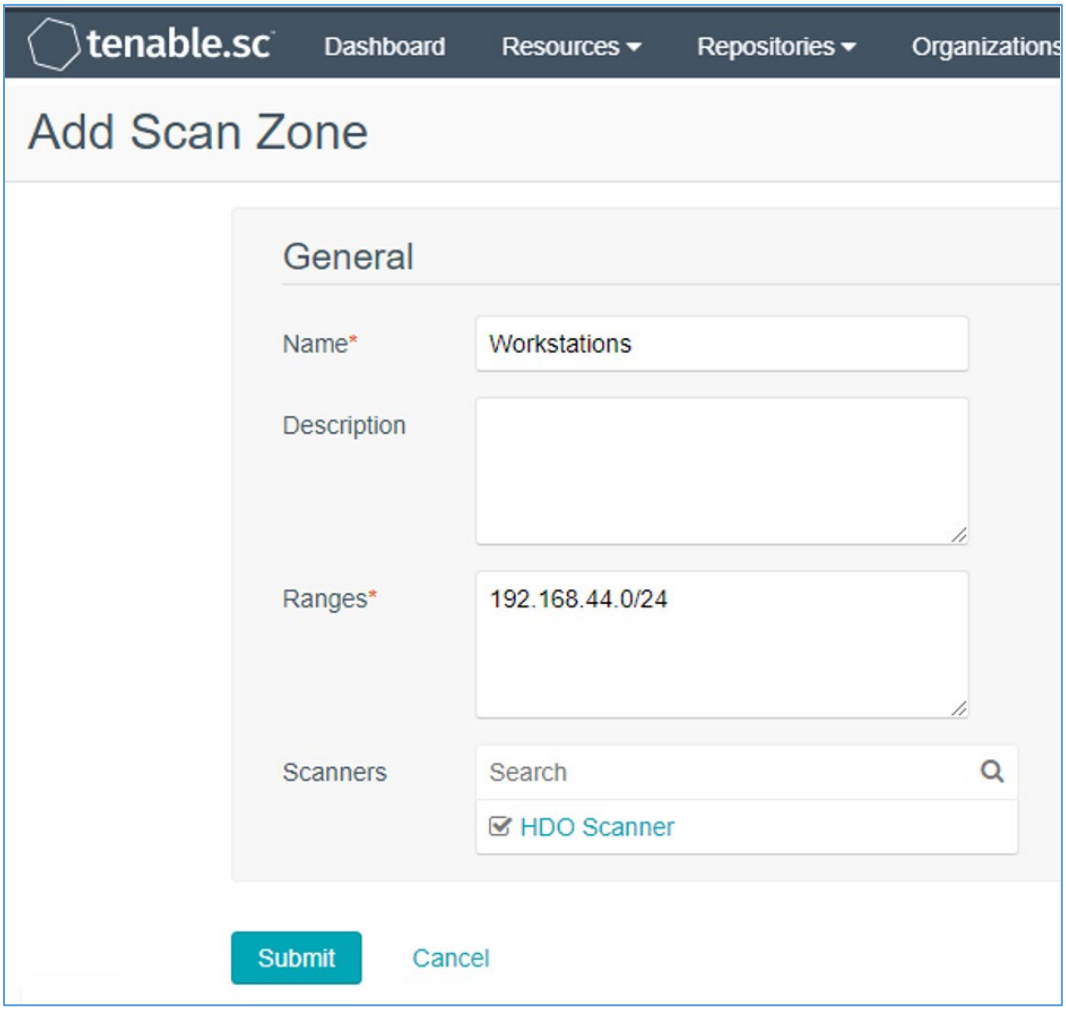
The engineers created a scan zone for each subnet established on the HDO network. The process to create a scan zone is the same for each subnet aside from the IP address range.

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

Add a Scan Zone

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.**



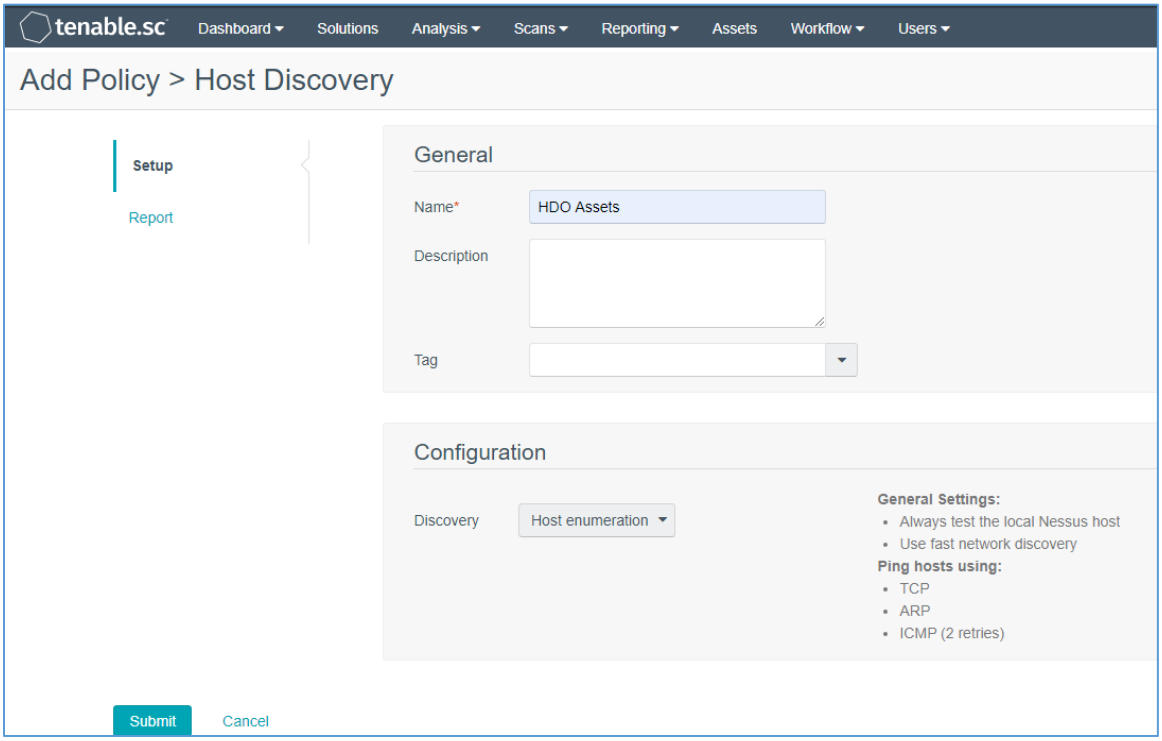
Repeat steps in Add a Scan Zone section for each VLAN.

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

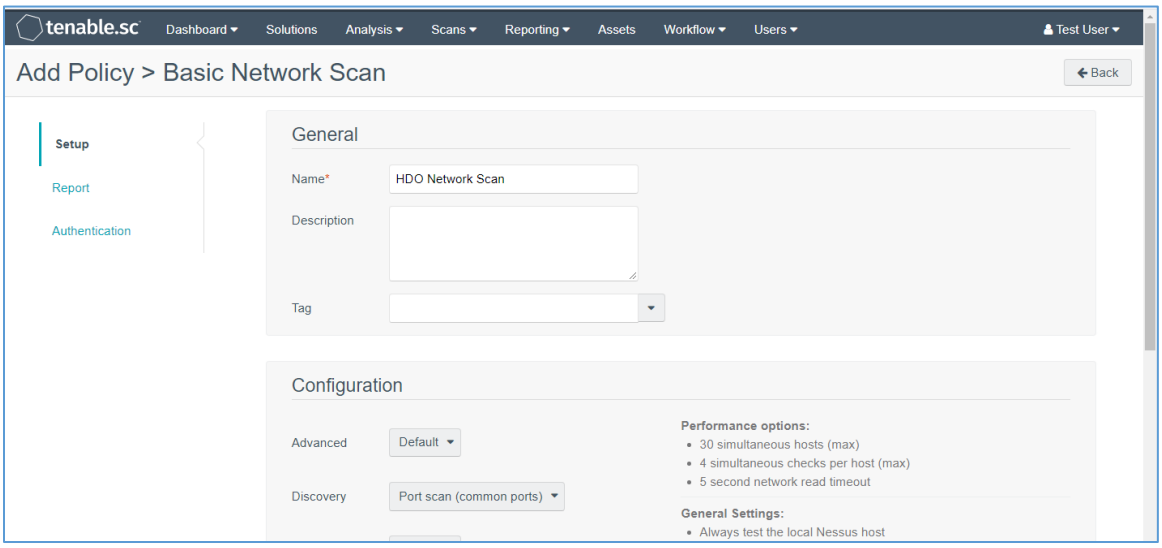
on each of the HDO VLANs. Once Tenable identifies the assets, Tenable.sc executes a basic network scan to identify any vulnerabilities on these assets.

Create Scan Policies

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

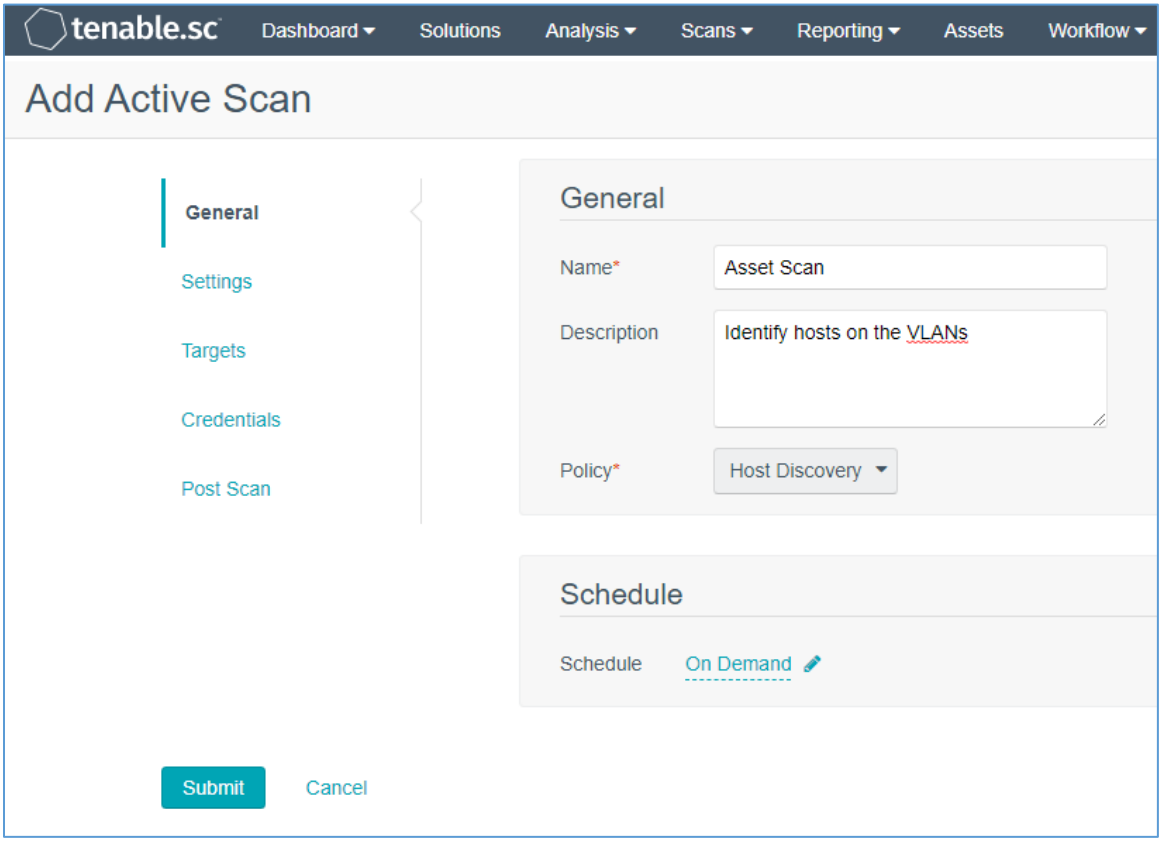
c. **Policy:** Host Discovery

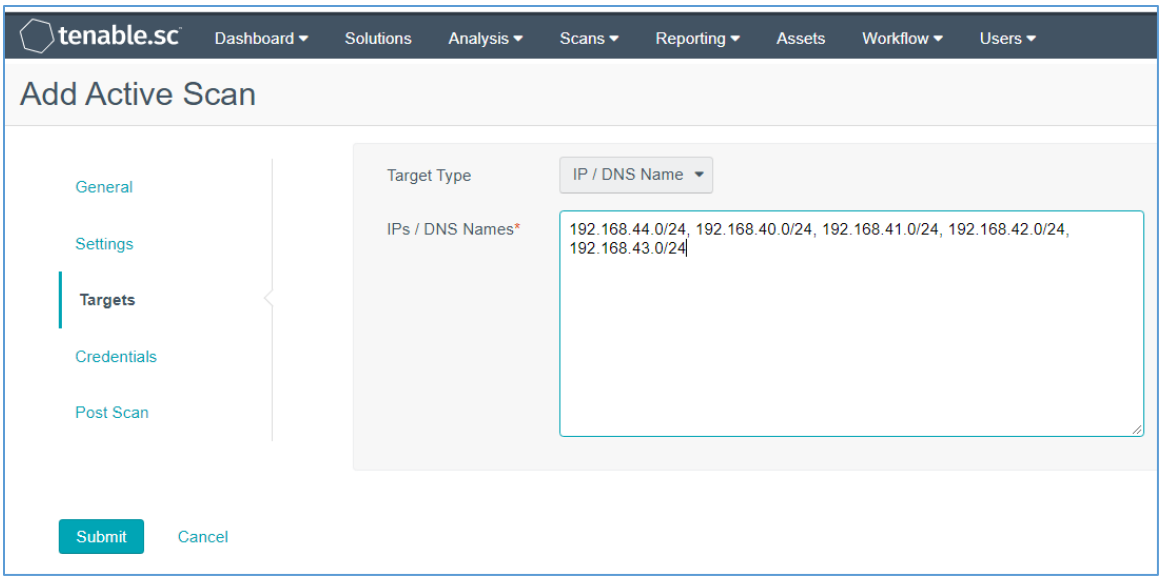
Targets

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.

Execute Active Scans

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.**

View Active Scan Results in the Dashboard

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

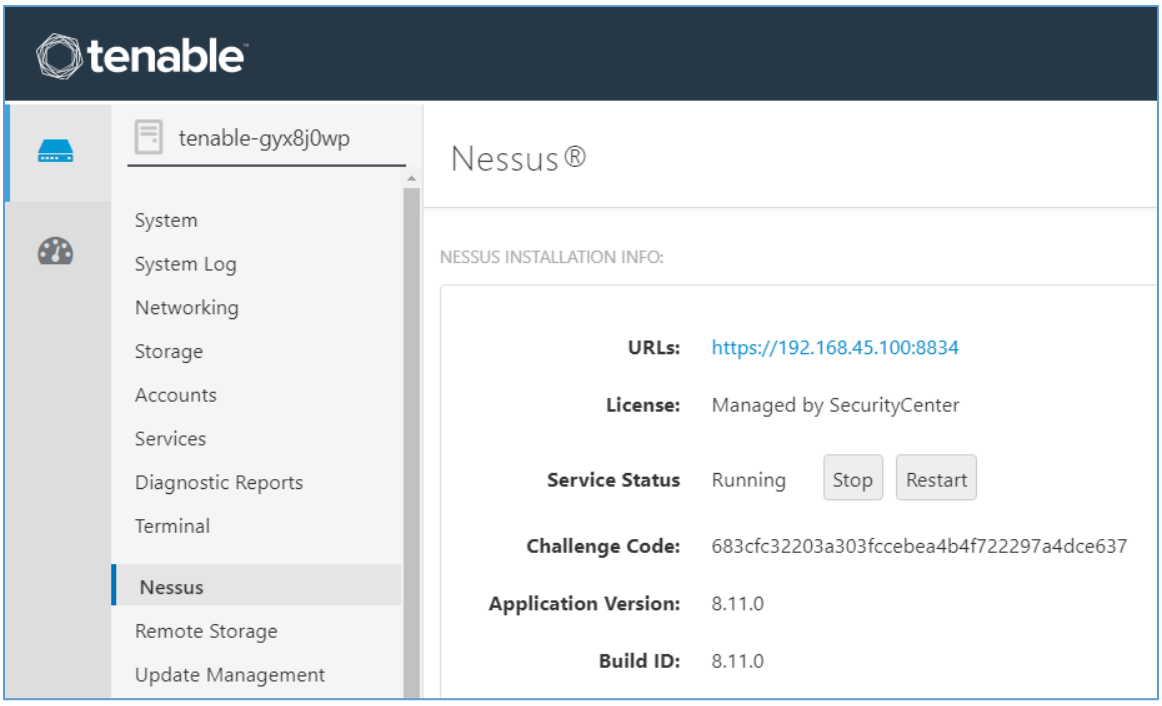
Network Adapter: VLAN 1348

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.**

576 8. Click **Tenable.sc** on the left side of the screen.

577 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

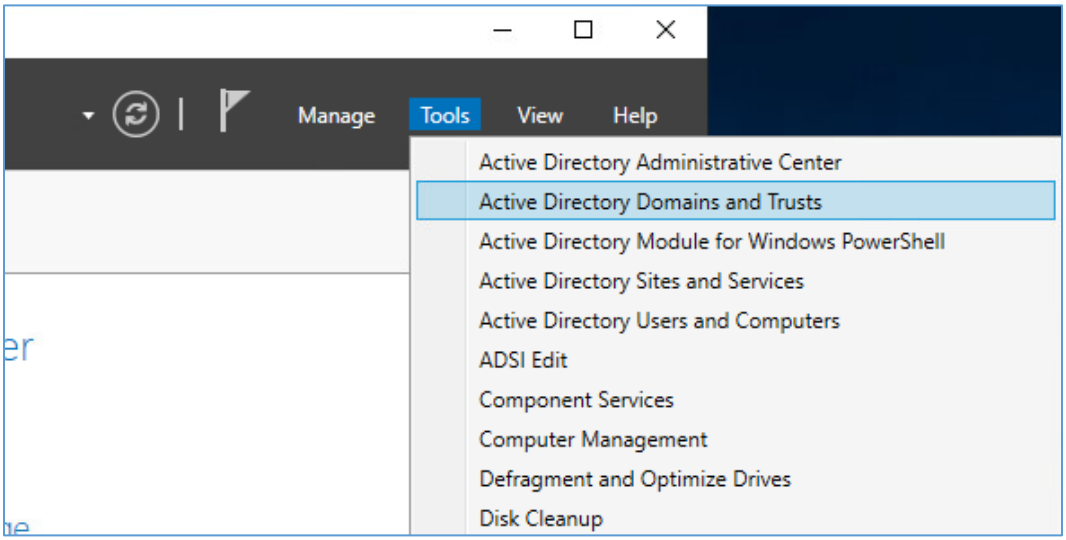
Operating System: Microsoft Windows Server 2019 Datacenter

Domain Controller Appliance Installation Guide

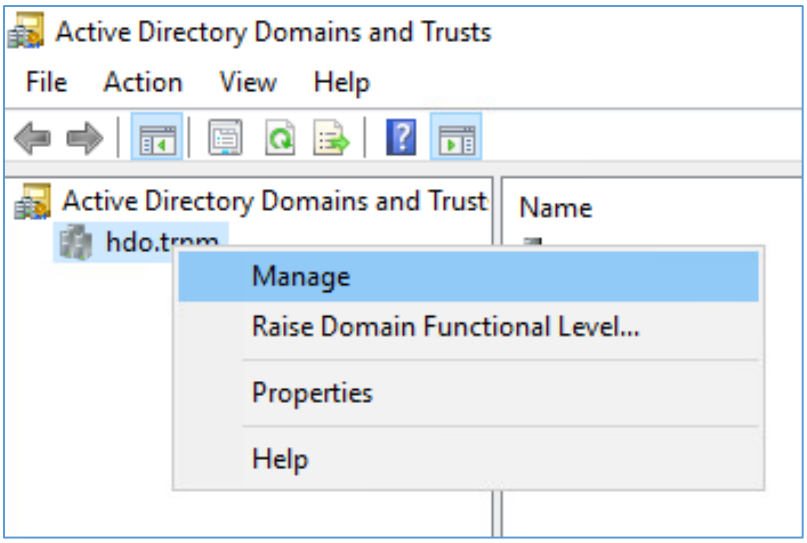
Install the appliance according to the instructions detailed in Microsoft's Install Active Directory Domain Services (Level 100) documentation [4].

Verify Domain Controller Installation

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



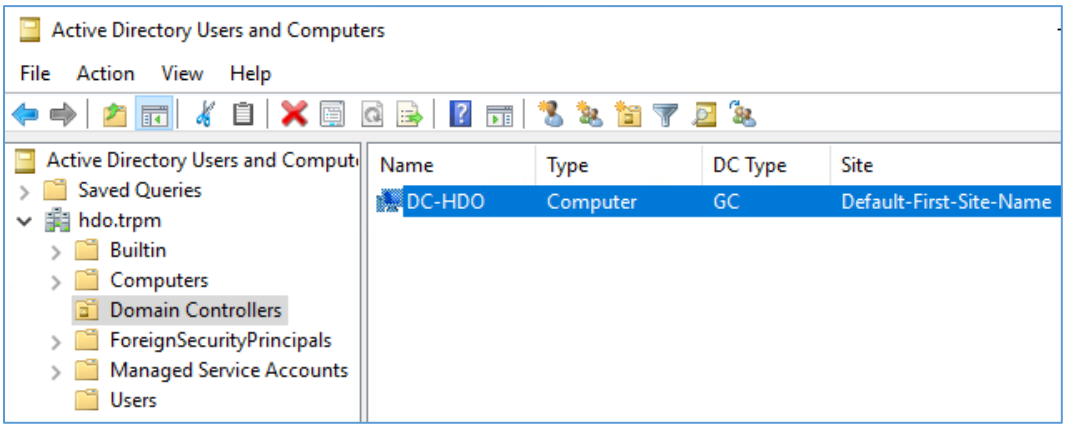
3. Right-click **hdo.trpm.**
4. Click **Manage.**



607

608 5. Click **hdo.trpm > Domain Controllers.**

609 6. Check that the Domain Controllers directory lists the new domain controller.

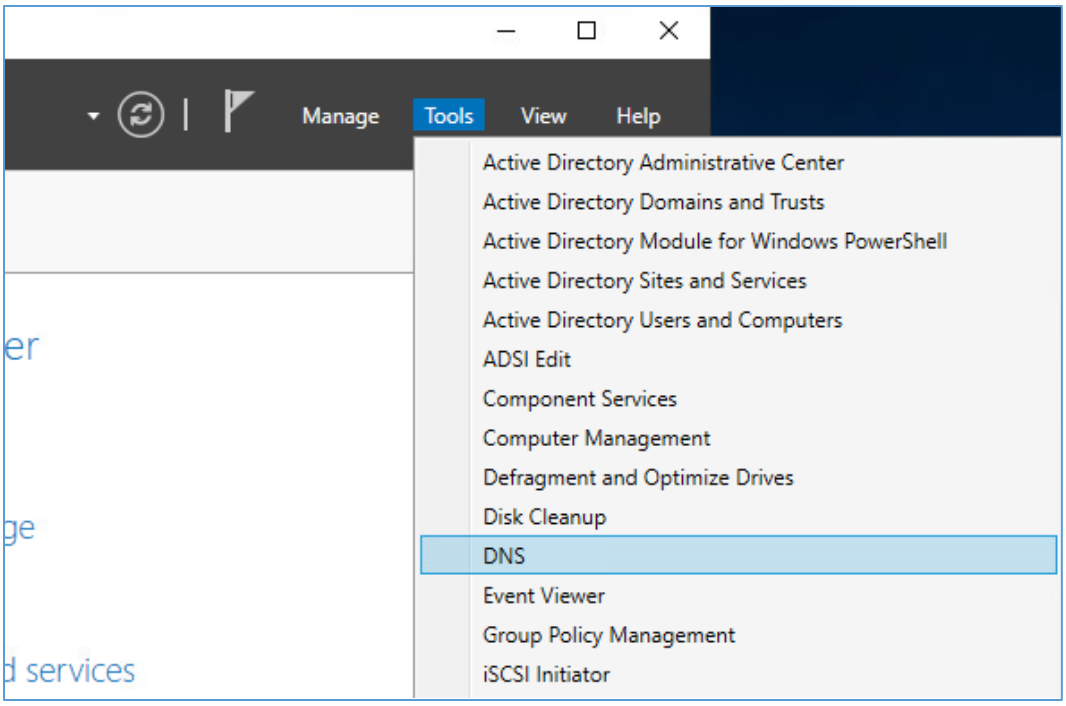


610

611 **Configure Local DNS**

612 1. Launch **Server Manager.**

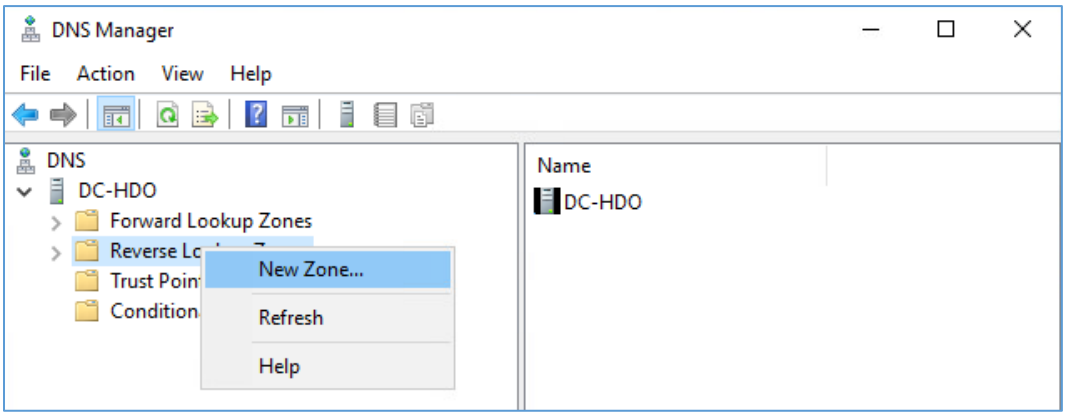
613 2. Click **Tools > DNS.**



614 3. Click the **arrow symbol** for DC-HDO.

615 4. Right-click **Reverse Lookup Zones.**

616 5. Click **New Zone….** The New Zone Wizard displays.

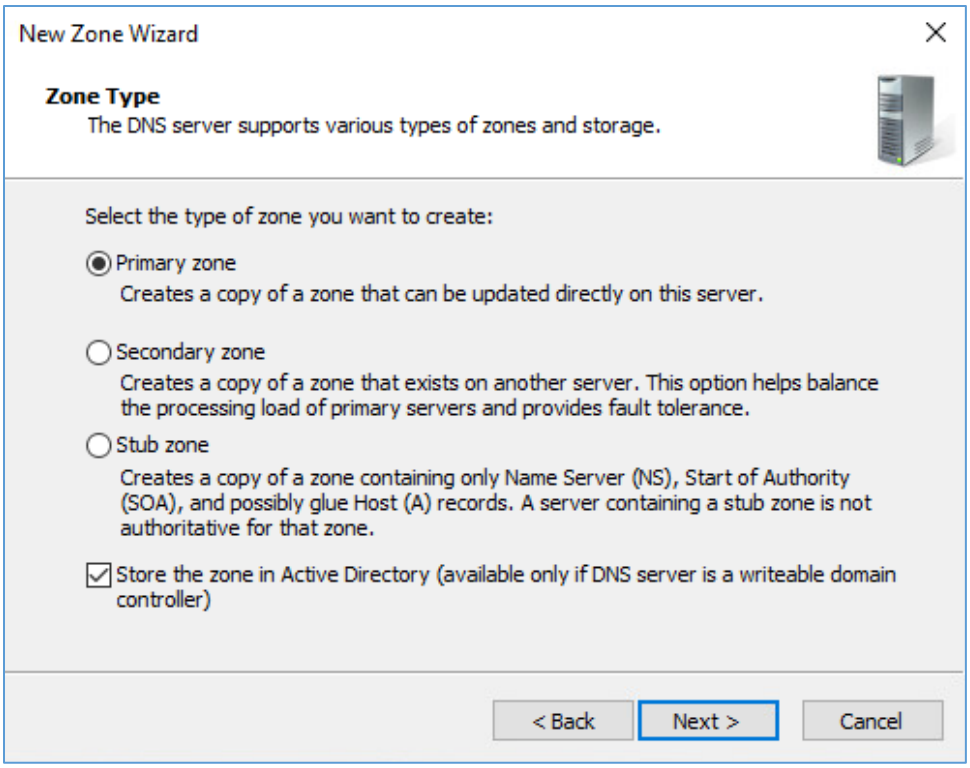


617 6. Click **Next >.**

618 7. Click **Primary zone.**

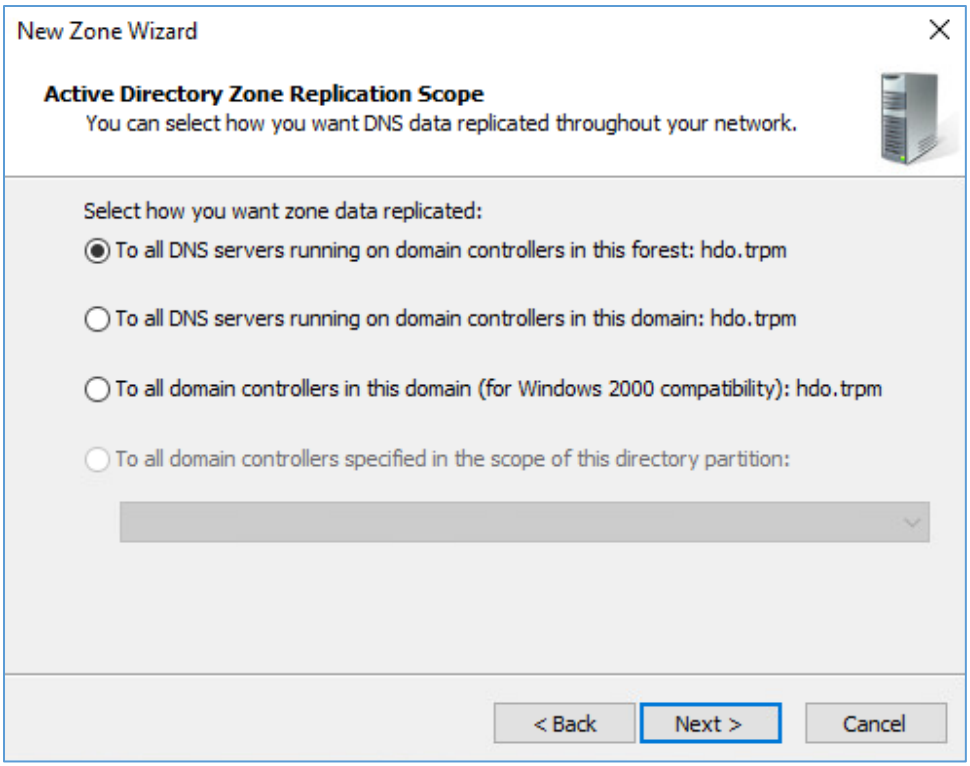
619 8. Check **Store the zone in Active Directory.**

620 9. Click **Next >.**



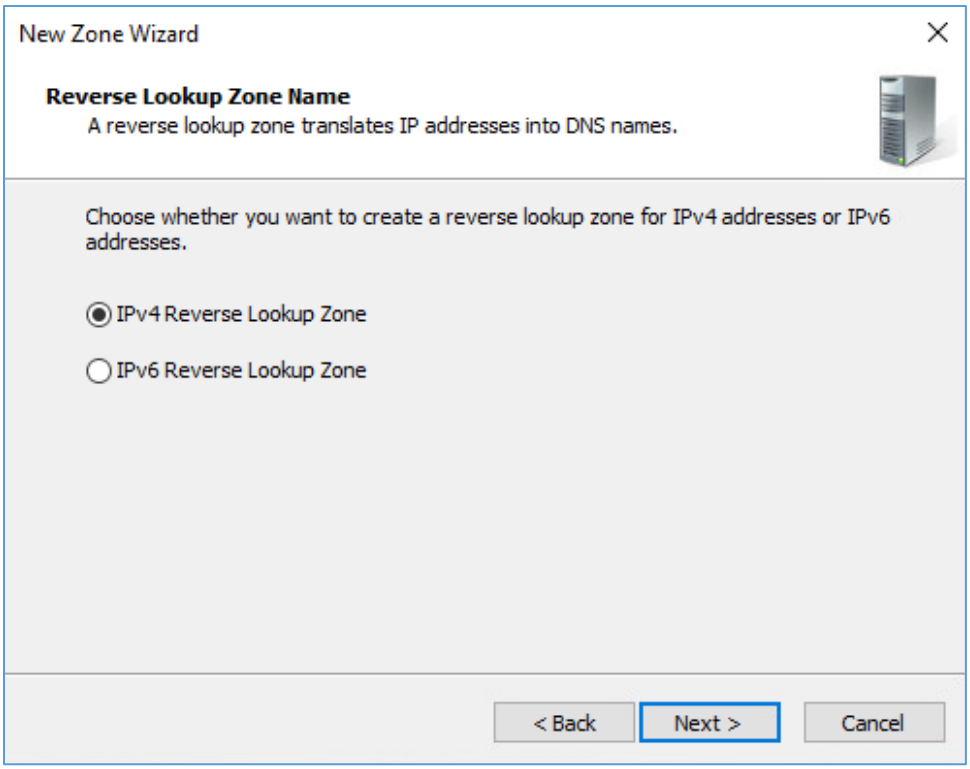
621 10. Check **To all DNS servers running on domain controllers in this forest: hdo.trpm.**

622 11. Click **Next >.**



623 12. Check **IPv4 Reverse Lookup Zone.**

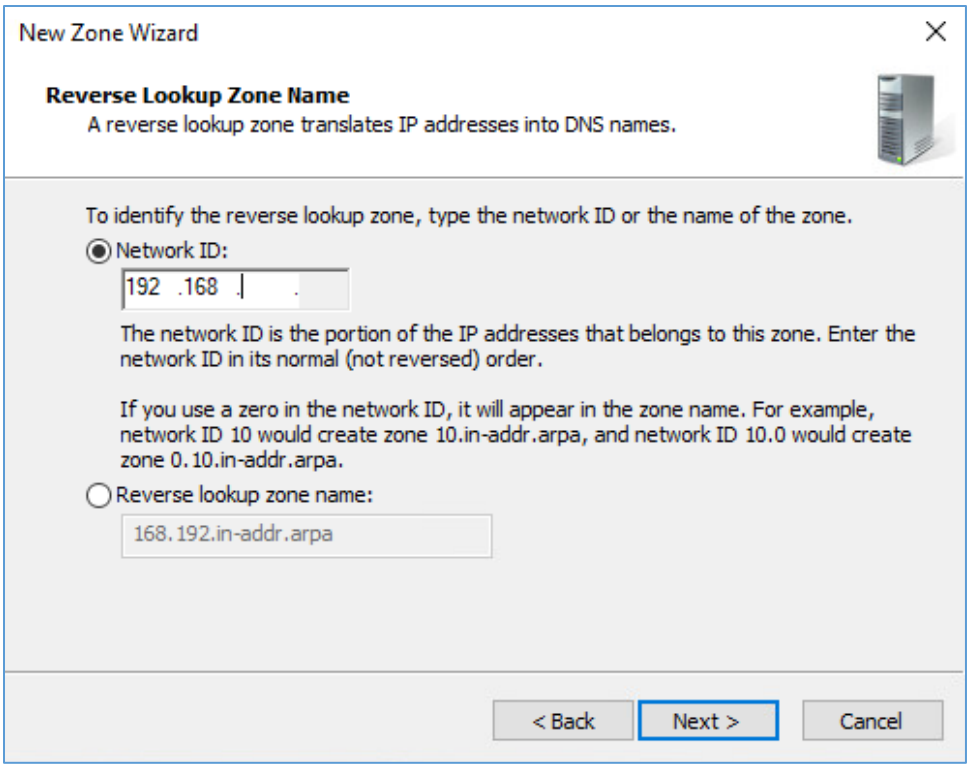
624 13. Click **Next >.**



625 14. Check **Network ID.**

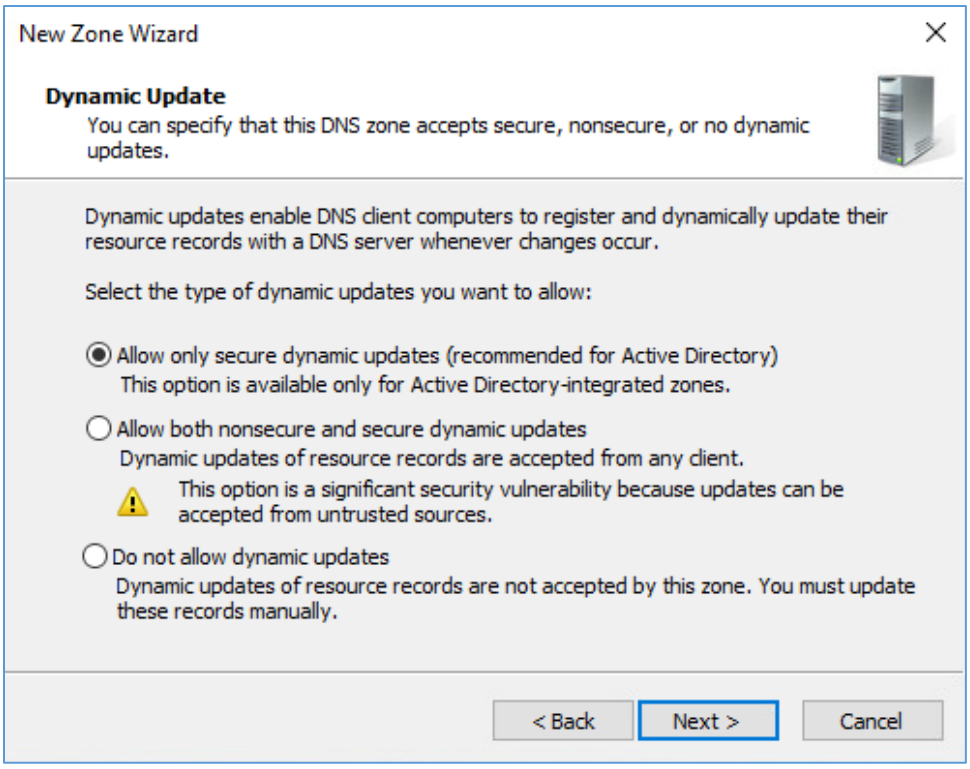
626 15. Under **Network ID,** type **192.168.**

627 16. Click **Next >.**

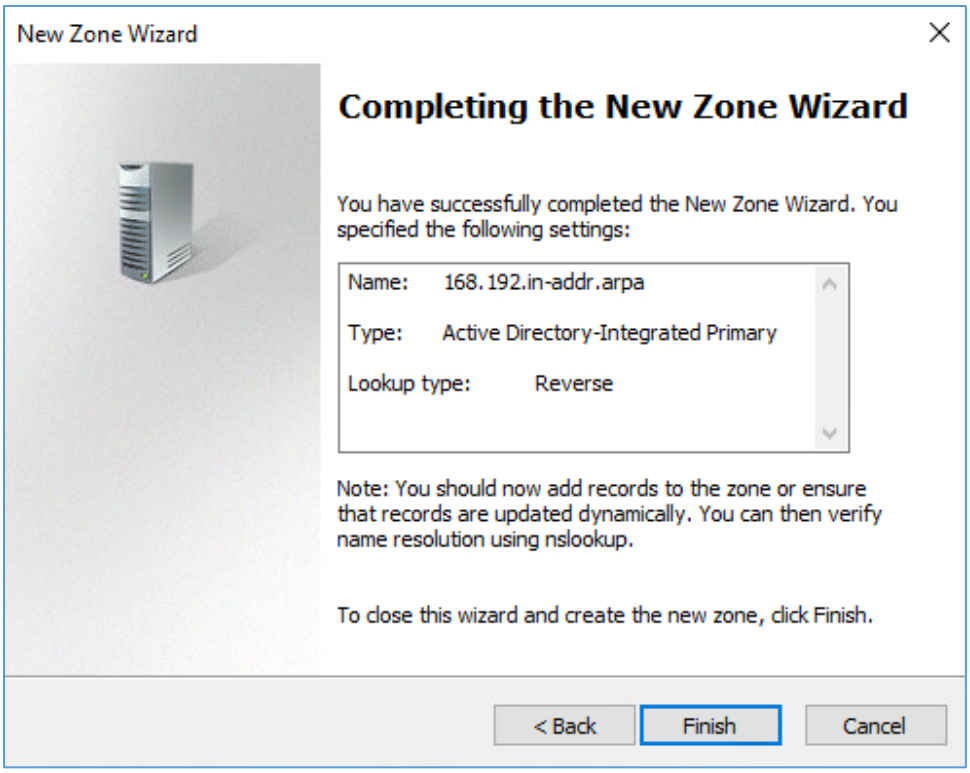


628 17. Check **Allow only secure dynamic updates.**

629 18. Click **Next >.**



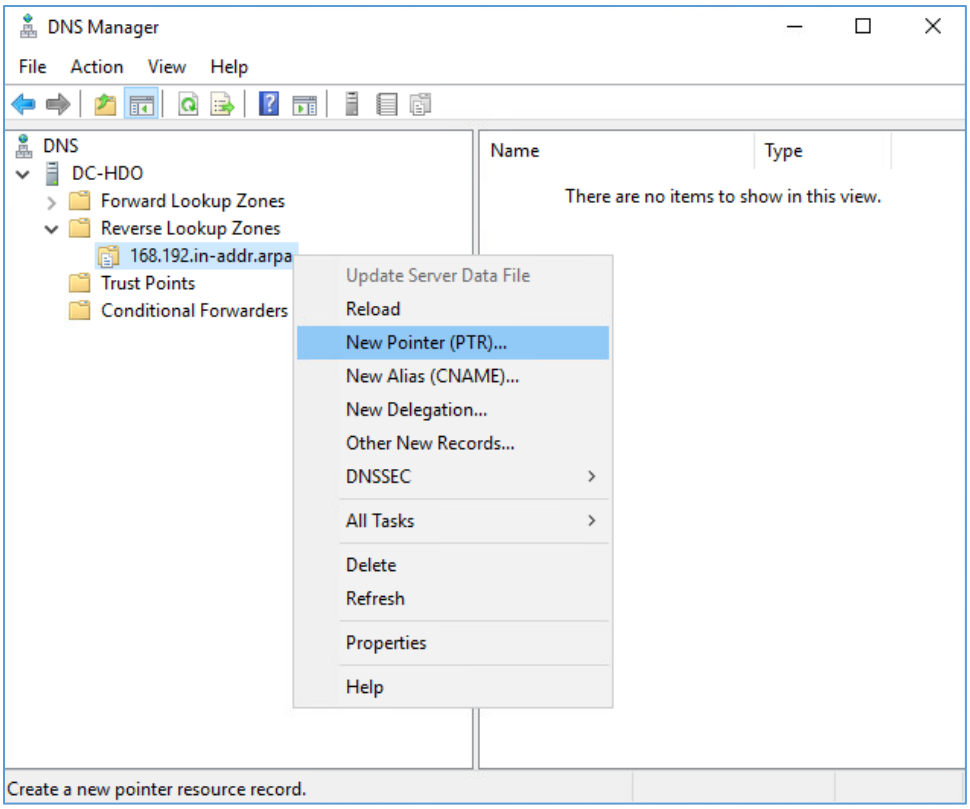
630 19. Click **Finish.**



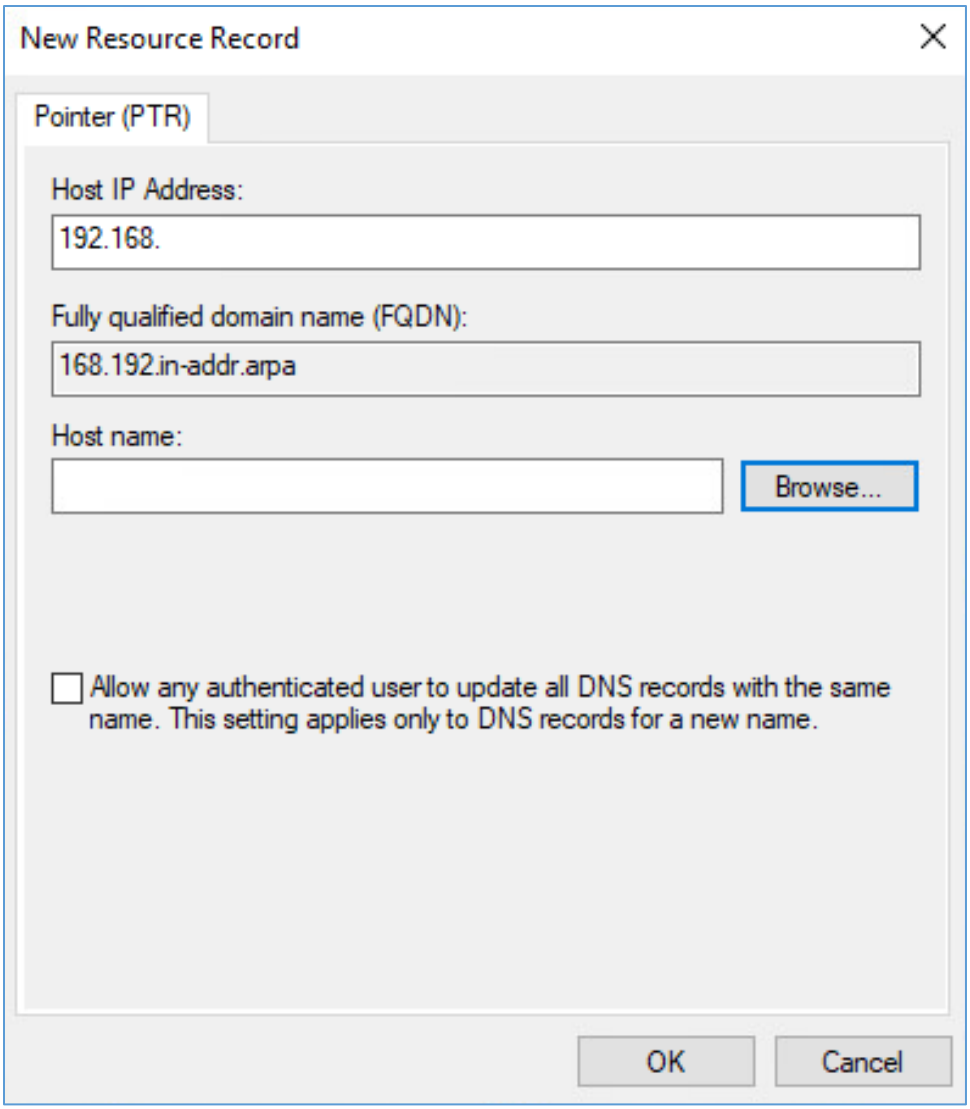
631 20. Click the arrow symbol for **Reverse Lookup Zones.**

632 21. Right-click **168.192.in-addr.arpa.**

633 22. Click **New Pointer (PTR)….**



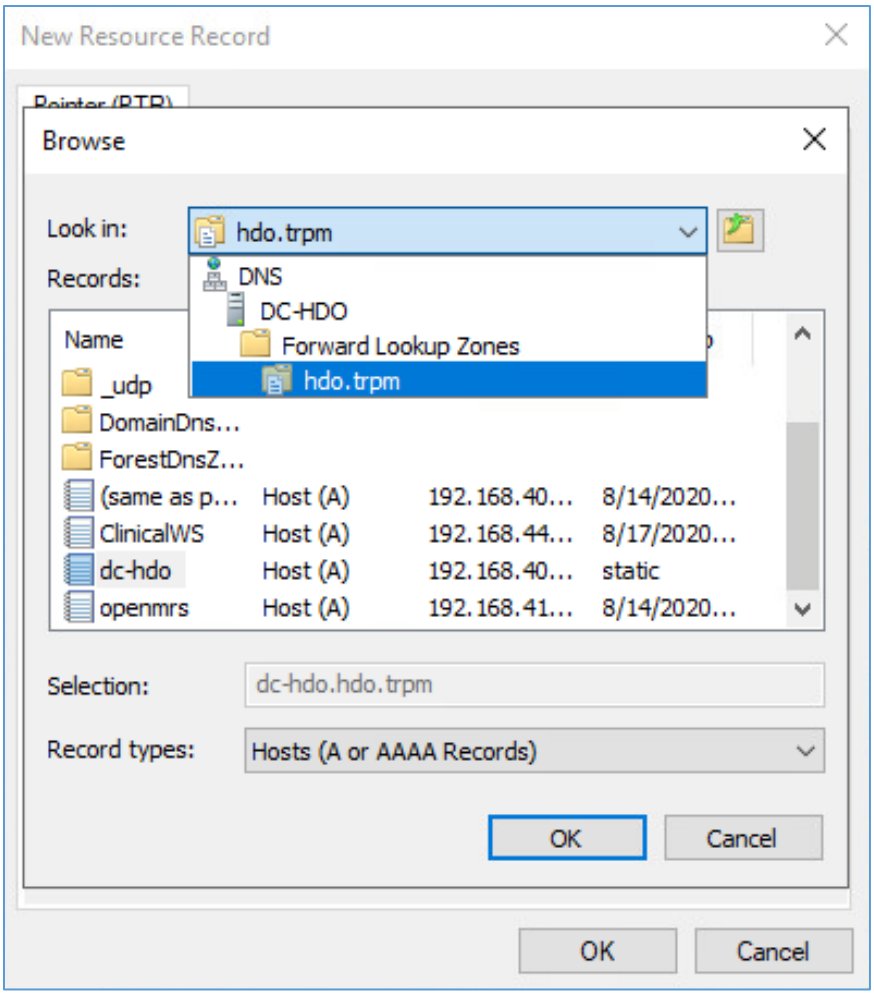
634 23. Under **Host name,** click **Browse….**



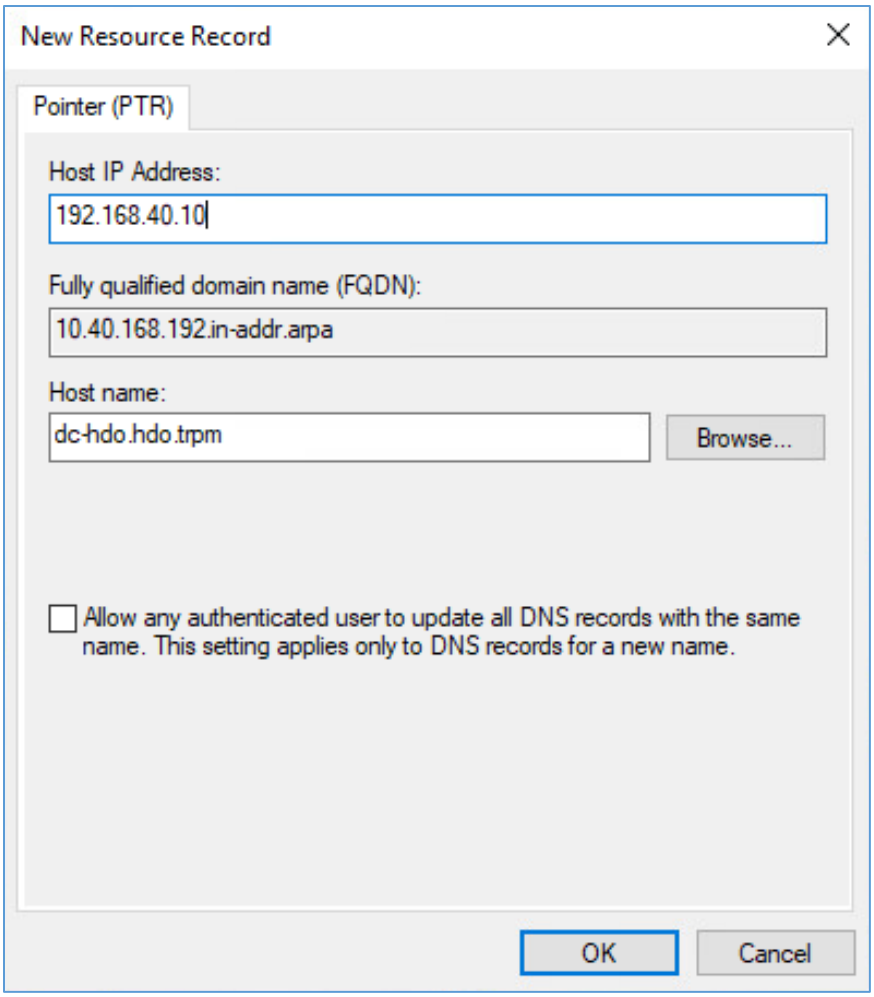
635 24. Under Look in, select **hdo.trpm.**

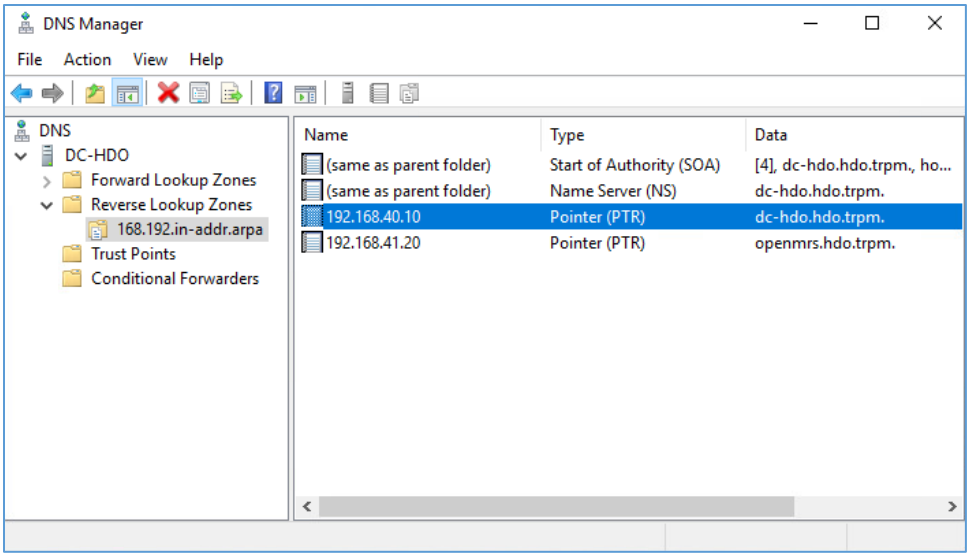
636 25. Under Records, select **dc-hdo.**

637 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

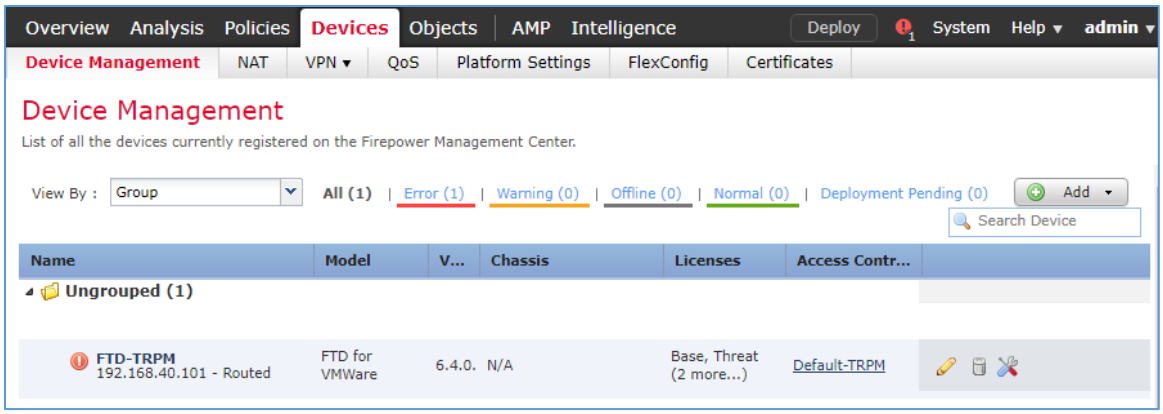
Cisco FTD Installation Guide

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].

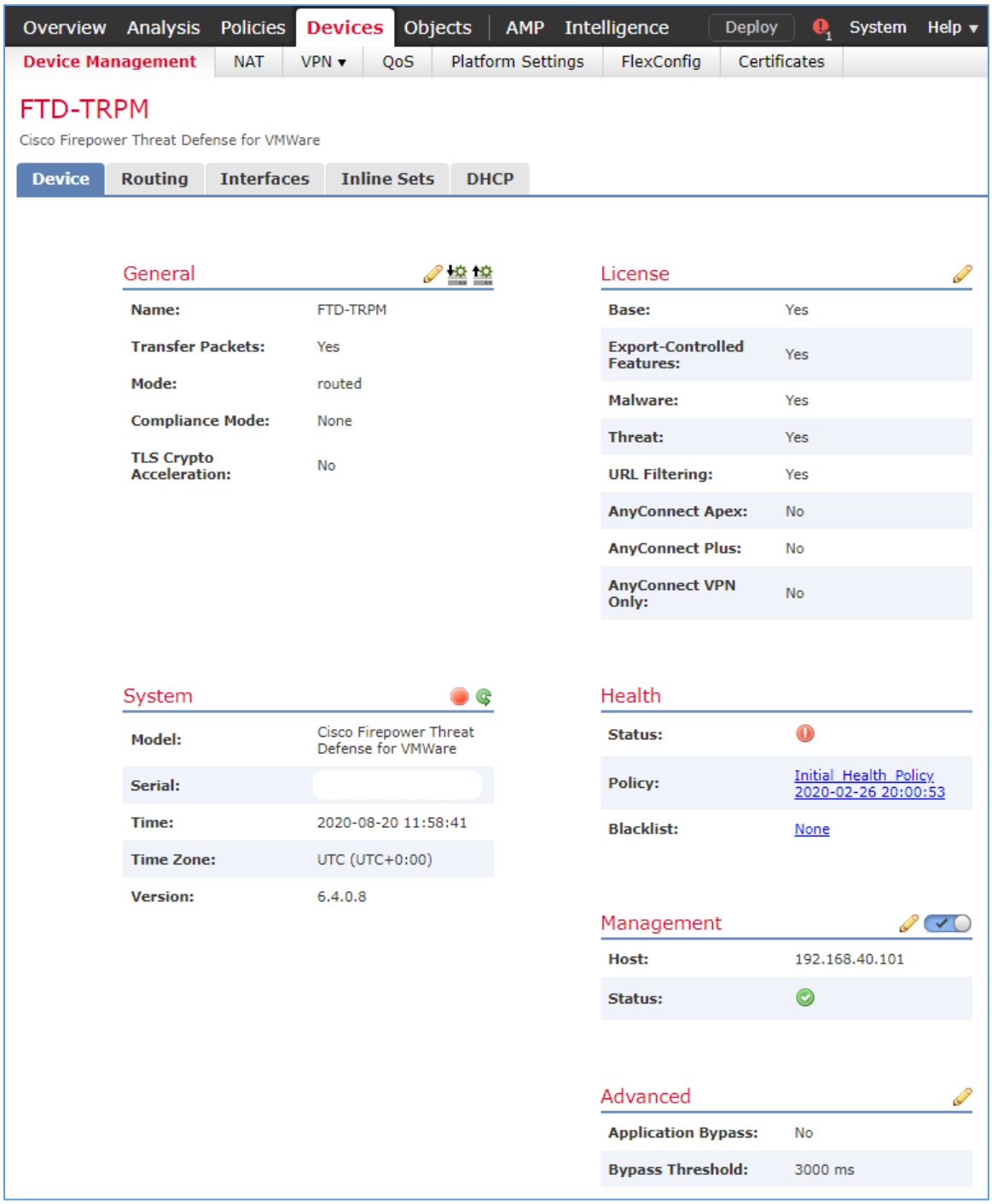
Configure FMC Management of FTD

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.**

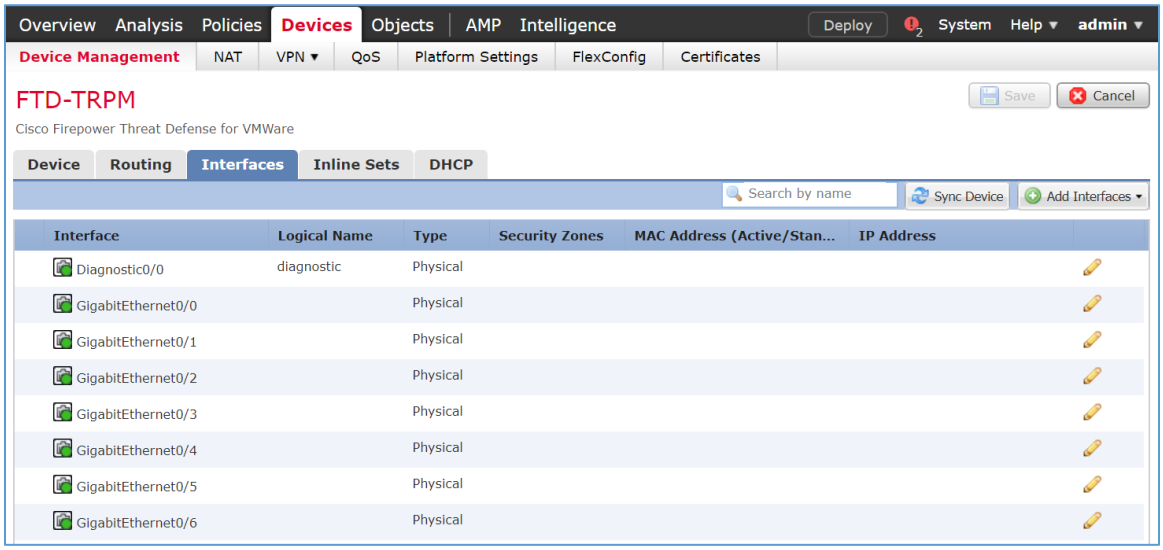


Configure Cisco FTD Interfaces for the RPM Architecture

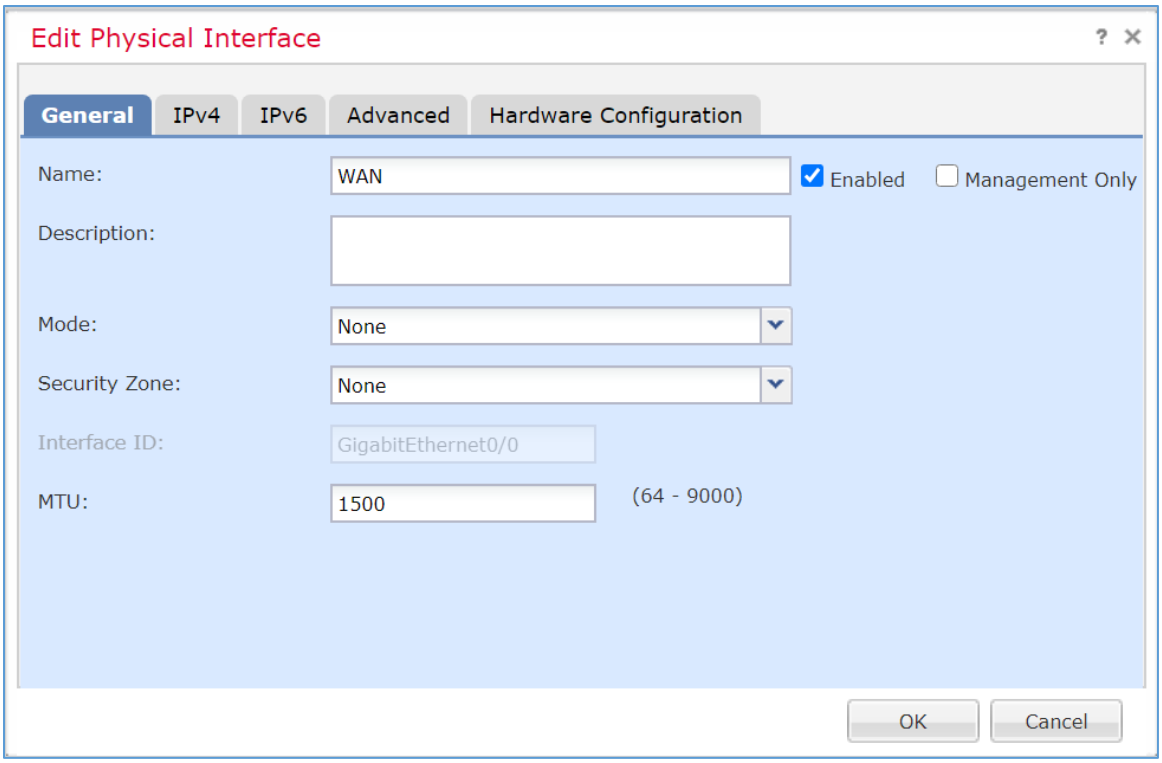
By default, each of the interfaces is defined as GigabitEthernet and is denoted as 0 through 6.

683 1. From **Devices > Device Management > FTD-TRPM > Device,** click **Interfaces.**

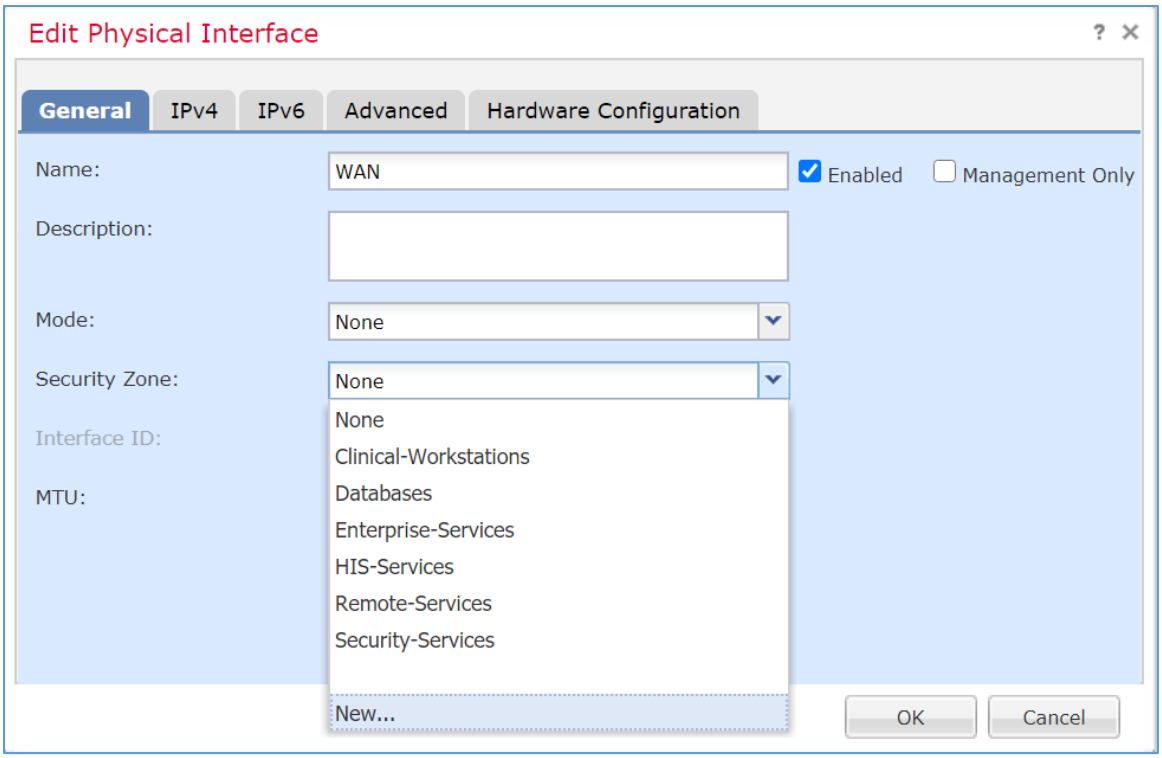
684 2. On the Cisco FTD Interfaces window, an Edit icon appears on the far right. The first
685 GigabitEthernet interface configured is GigabitEthernet0/0. Click the Edit icon to configure the
686 GigabitEthernet interface.



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

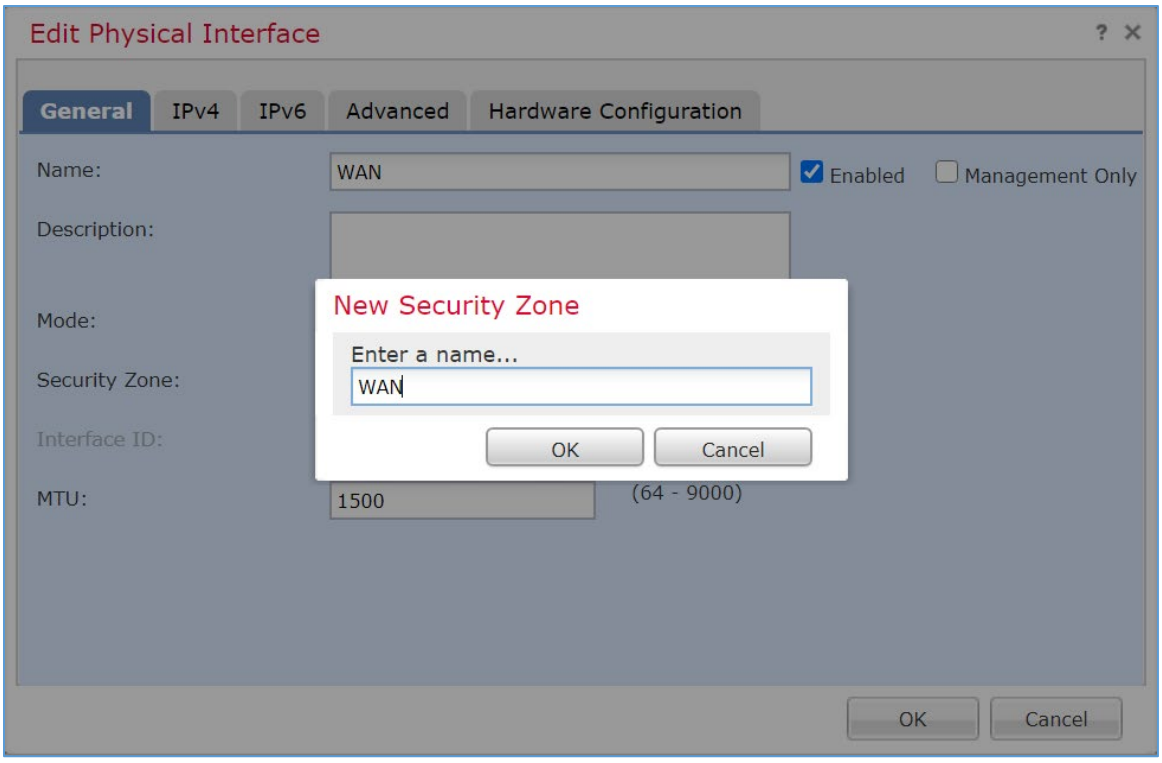


689 4. Under **Security Zone,** click the drop-down arrow and select **New….**

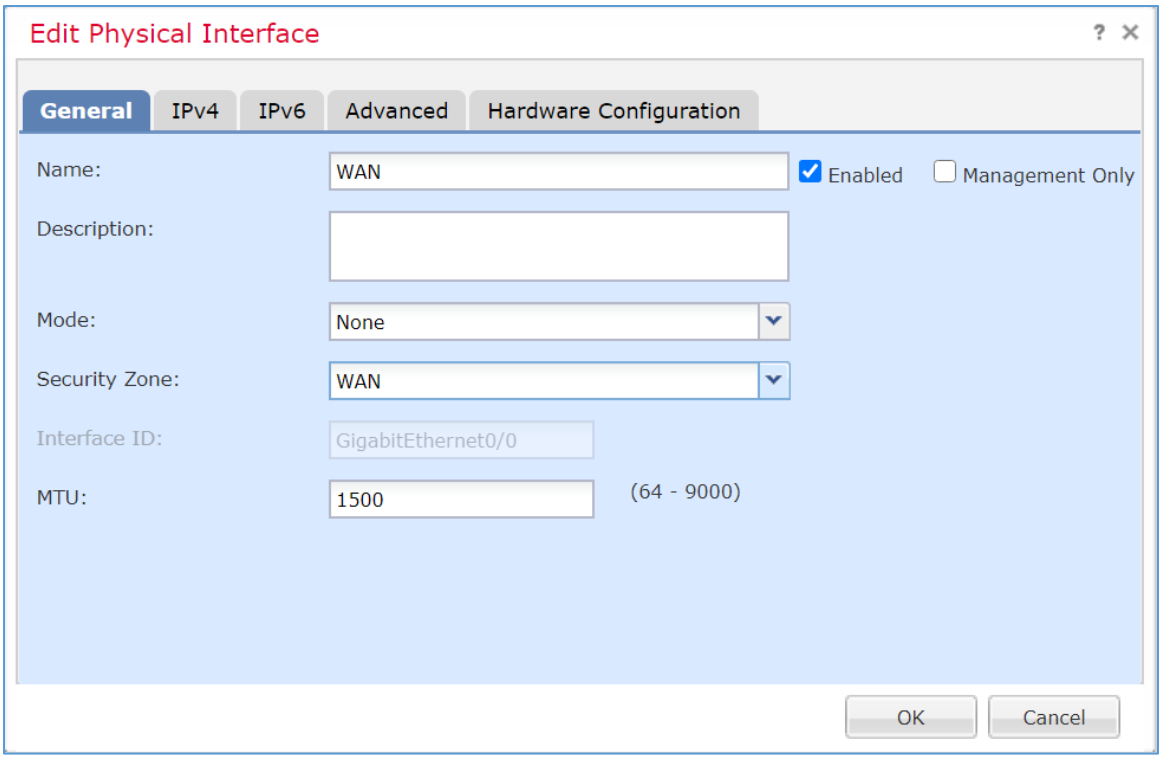


690 5. The New Security Zone pop-up box appears. Enter **WAN** in the **Enter a name…** field.

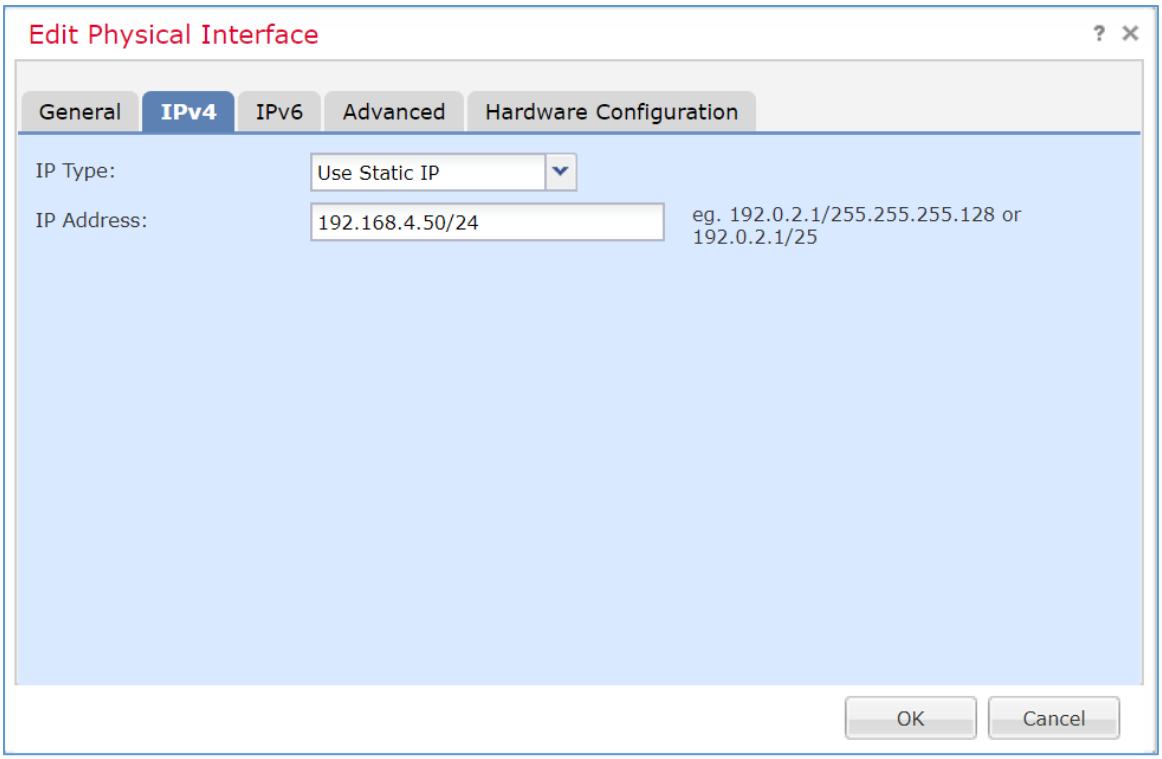
691 6. Click **OK.**



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



8. Fill out the following information:
    a. **IP Type:** Use Static IP
    b. **IP Address:** 192.168.4.50/24
    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

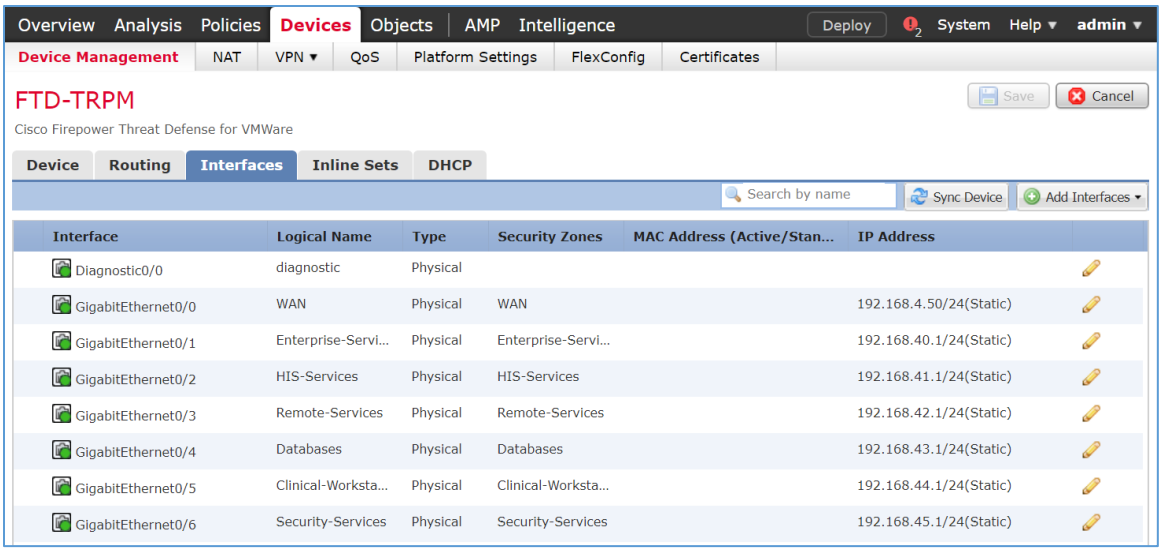
    c. GigabitEthernet0/2 (VLAN 1328)

        i. **Name:** HIS-Services

710 ii. **Security Zone:** HIS-Services
711 iii. **IP Address:** 192.168.41.1/24
712 d. GigabitEthernet0/3 (VLAN 1329)
713 i. **Name:** Remote-Services
714 ii. **Security Zone:** Remote-Services
715 iii. **IP Address:** 192.168.42.1/24
716 e. GigabitEthernet0/4 (VLAN 1330)
717 i. **Name:** Databases
718 ii. **Security Zone:** Databases
719 iii. **IP Address:** 192.168.43.1/24
720 f. GigabitEthernet0/5 (VLAN 1347)
721 i. **Name:** Clinical-Workstations
722 ii. **Security Zone:** Clinical-Workstations
723 iii. **IP Address:** 192.168.44.1/24
724 g. GigabitEthernet0/6 (VLAN 1348)
725 i. **Name:** Security-Services
726 ii. **Security Zone:** Security-Services
727 iii. **IP Address:** 192.168.45.1/24

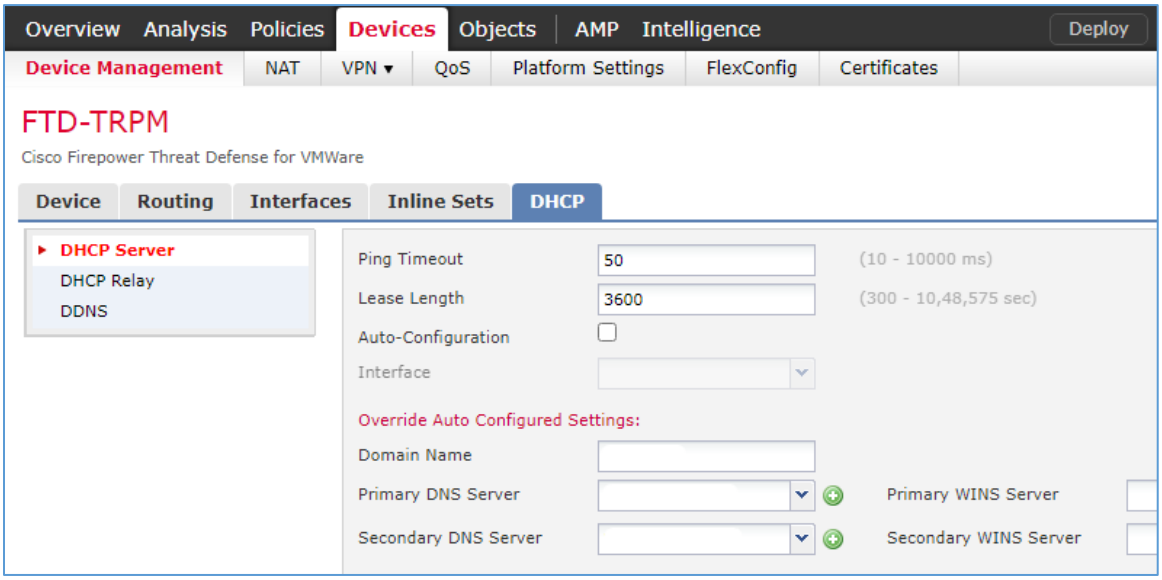
728 10. Click **Save.**

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



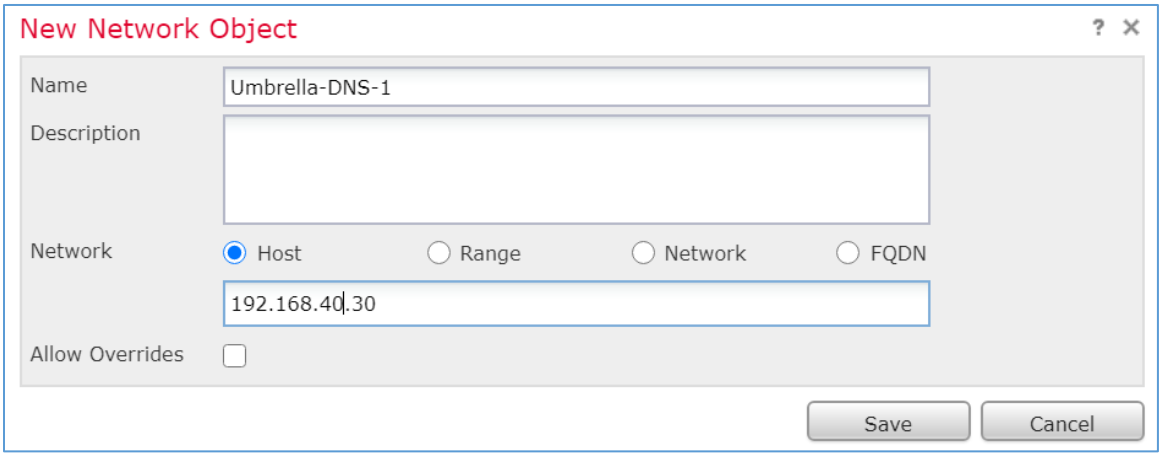
Configure Cisco FTD DHCP

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.**

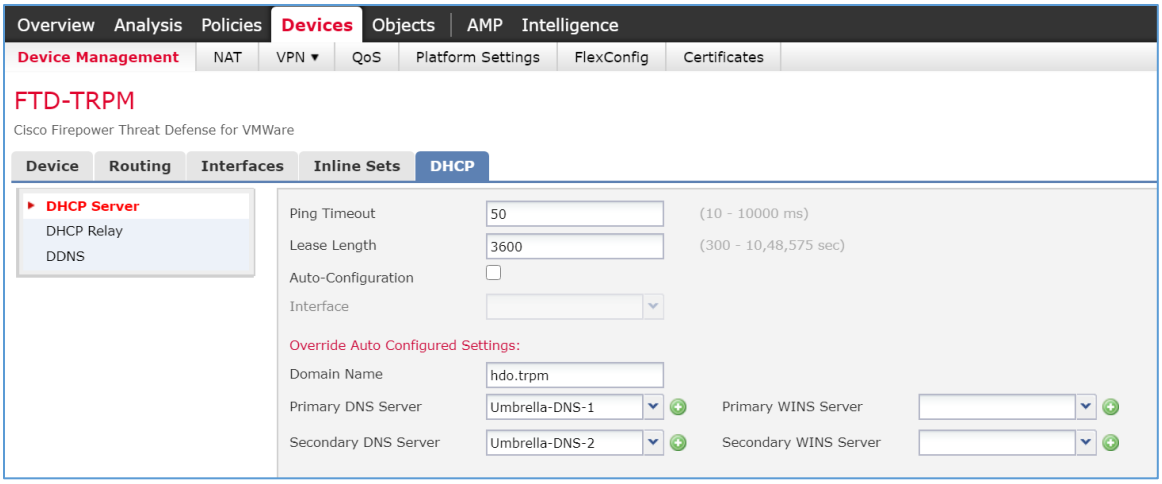
6. The New Network Object pop-up window appears. Fill out the following information:

    a. **Name:** Umbrella-DNS-2

    b. **Network (Host):** 192.168.40.31

7. Under **Domain Name,** add **hdo.trpm.**

8. Click **Add Server.**



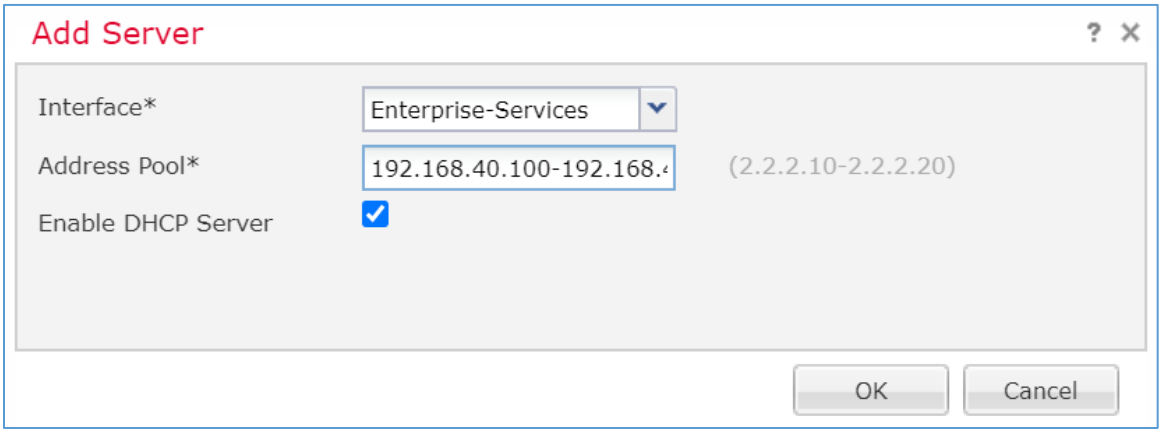
9. The Add Server pop-up window appears. Fill out the following information:

    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

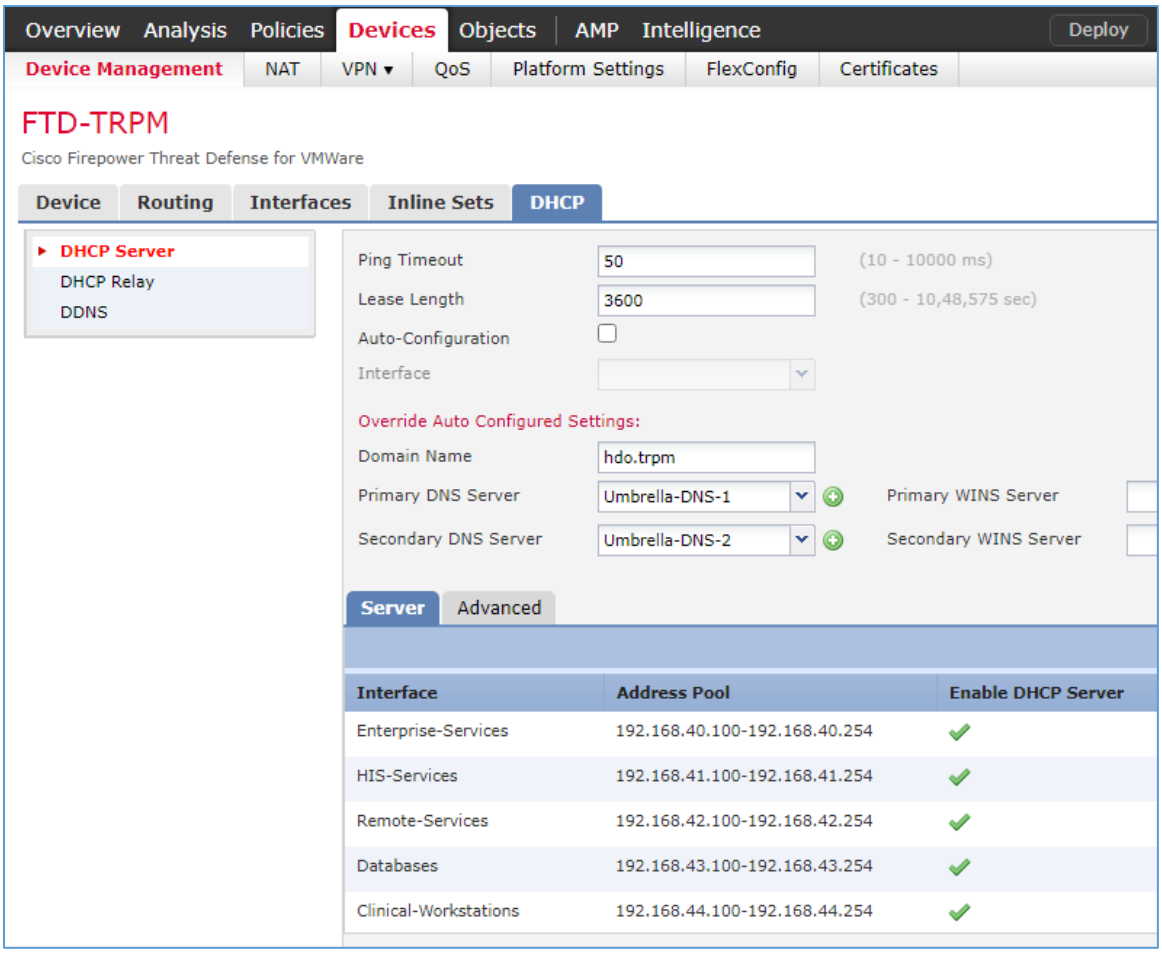
f. **Interface:** Security-Services

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

ii. **Enable DHCP Server:** checked

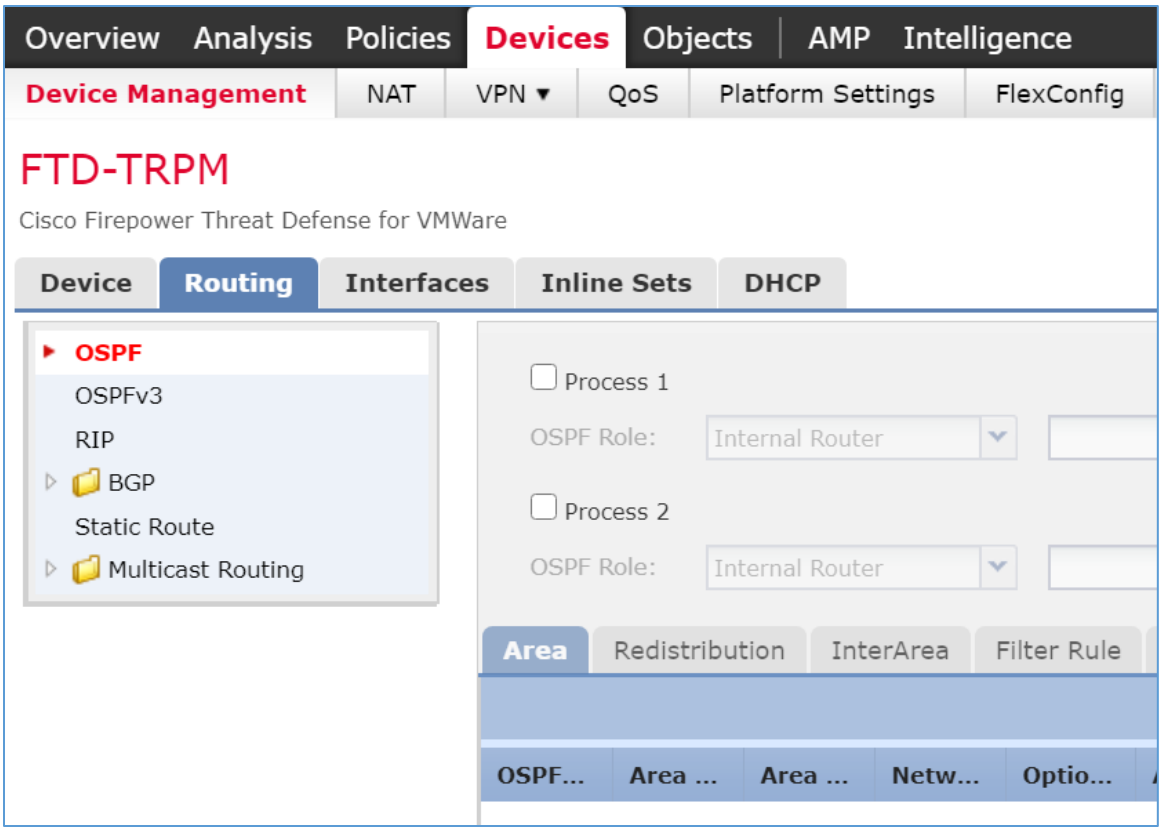
12. Click **Save.**

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.

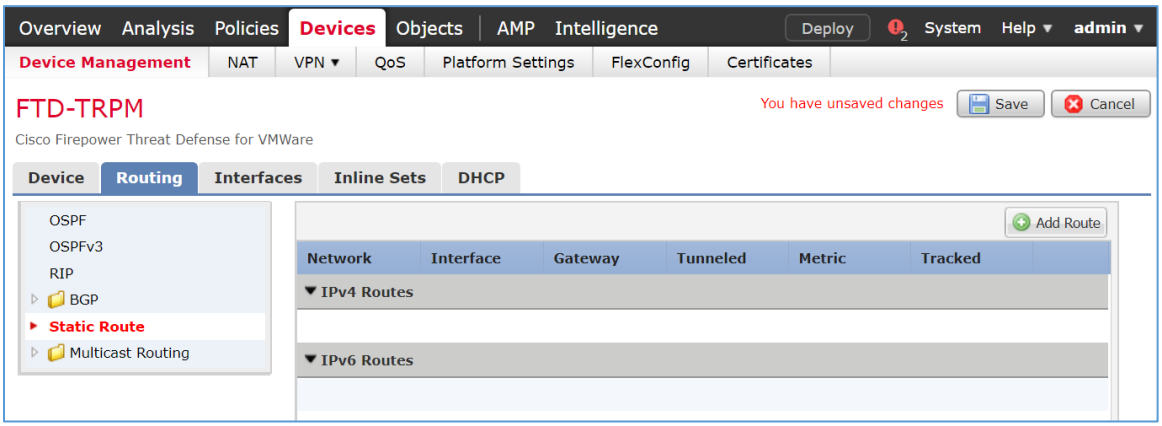


Configure Cisco FTD Static Route

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



783 3. Click **Add Route.**

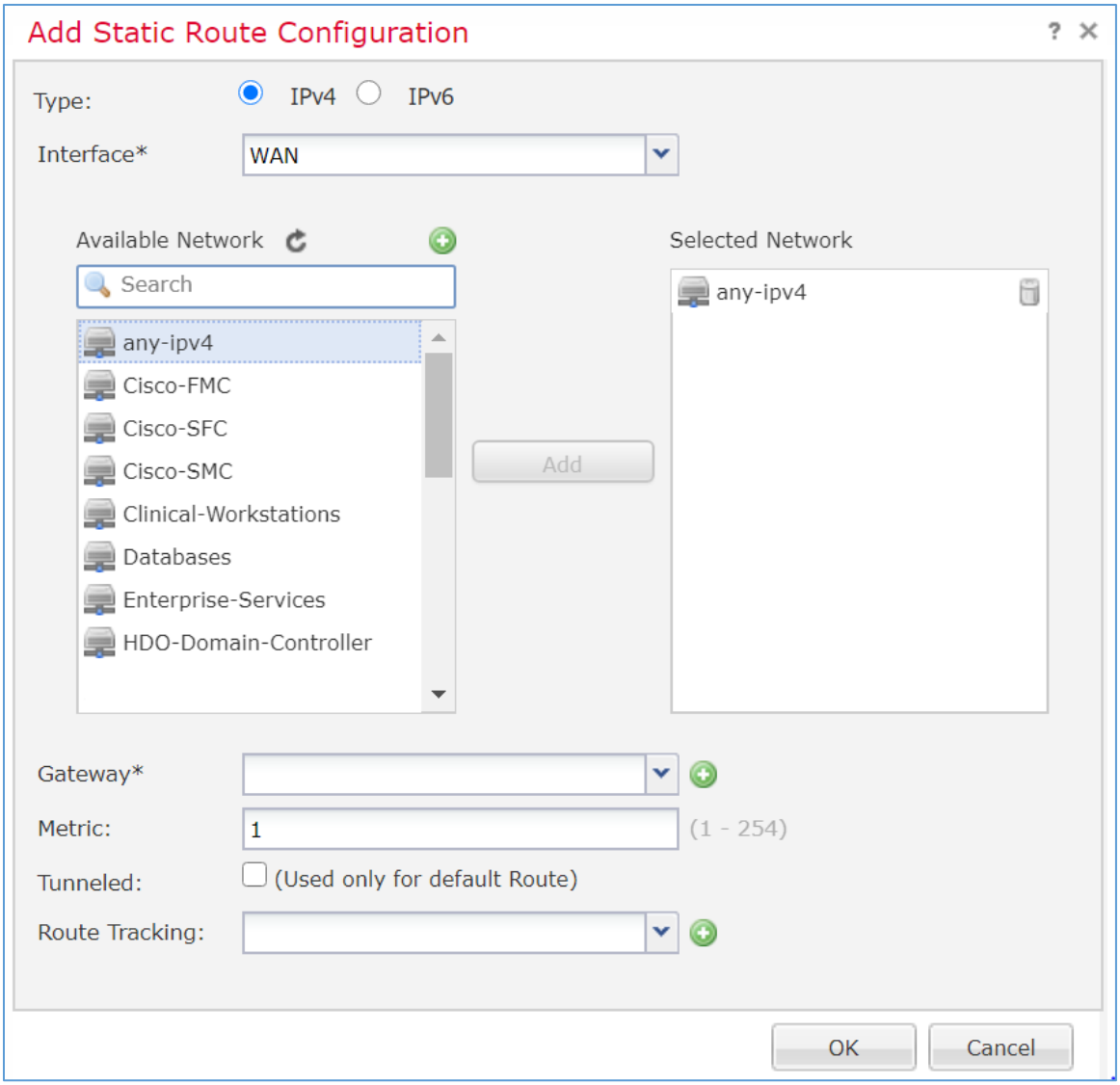


784 4. The Add Static Route Configuration pop-up window appears. Fill out the following information:

785 a. **Interface:** WAN

786 b. **Selected Network:** any-ipv4

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

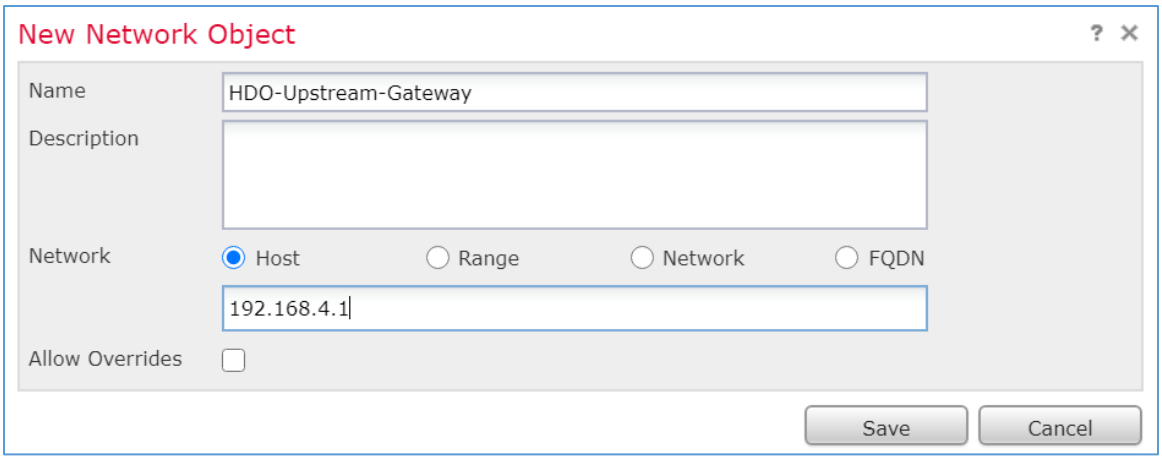


788 6. The New Network Object pop-up window appears. Fill out the following information:

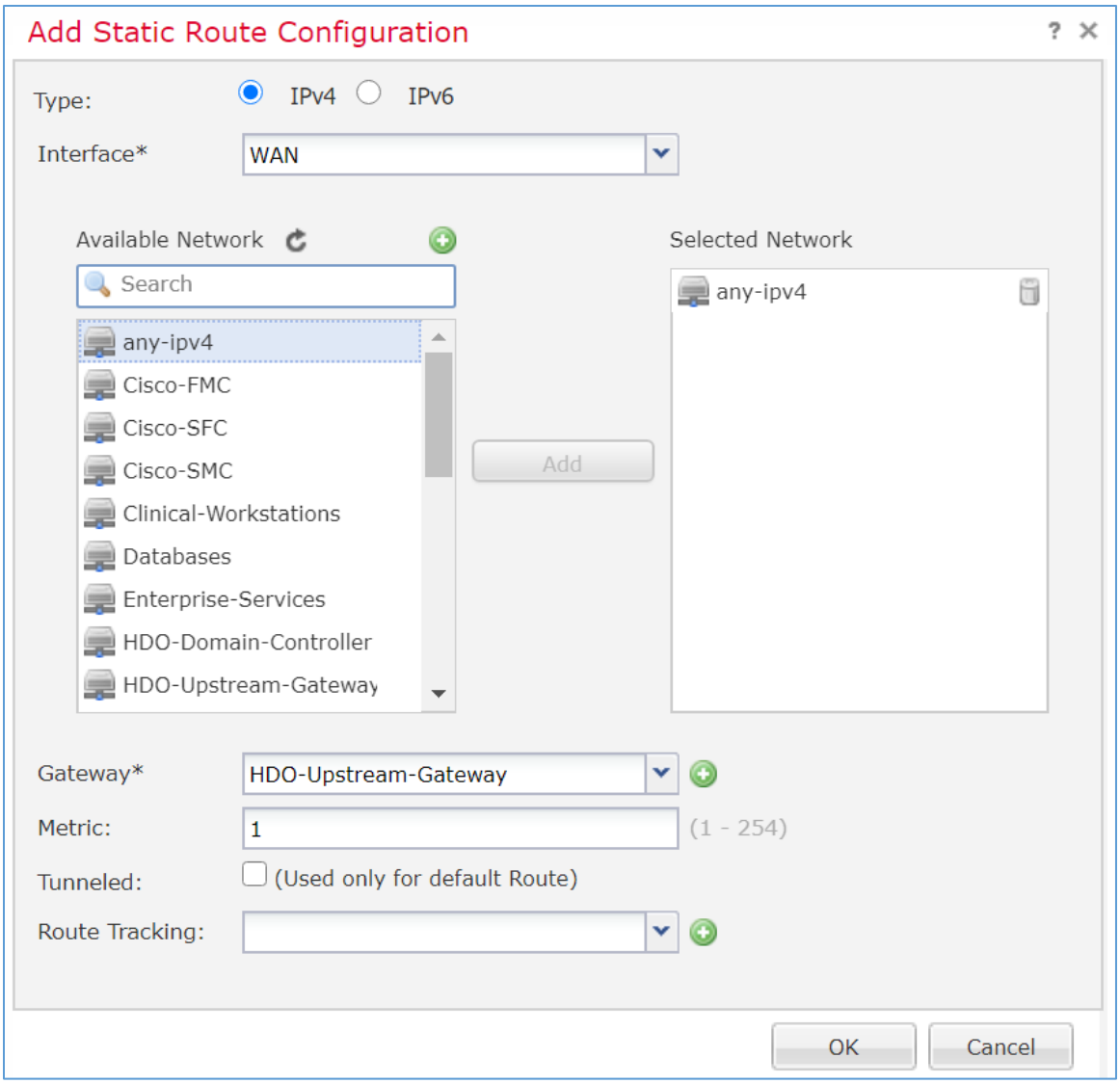
789 a. **Name:** HDO-Upstream-Gateway

790 b. **Network (Host):** 192.168.4.1

791 7. Click **Save.**

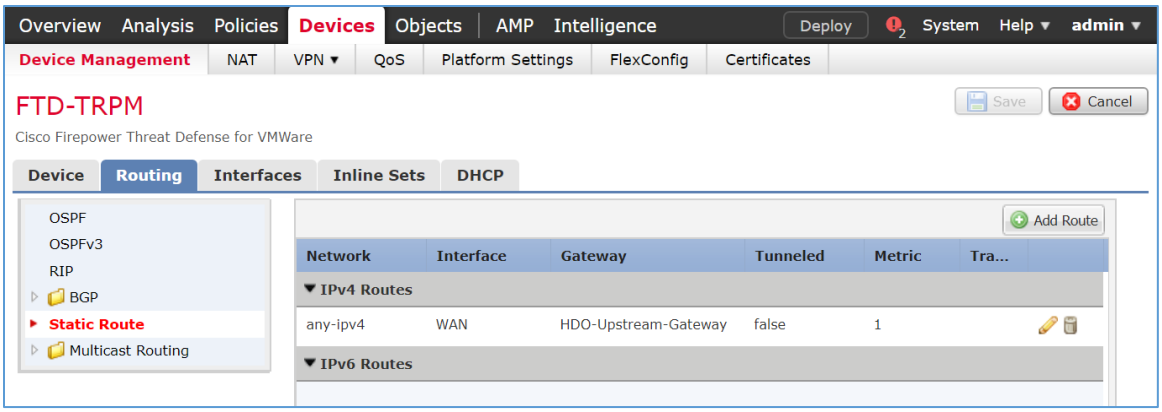

New Network Object
Name
HDO-Upstream-Gateway
Description
Network
Host
Range
Network
FQDN
192.168.4.1
Allow Overrides
Save
Cancel

8. Click **OK.**



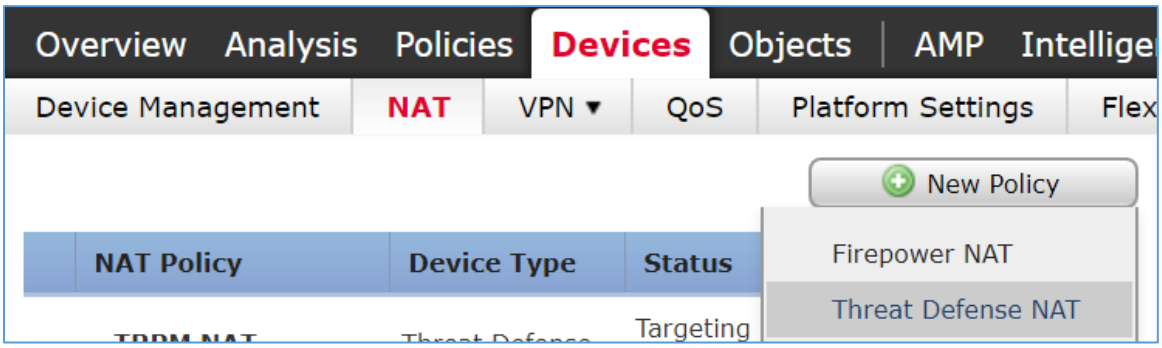
9. Click **Save.**

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.

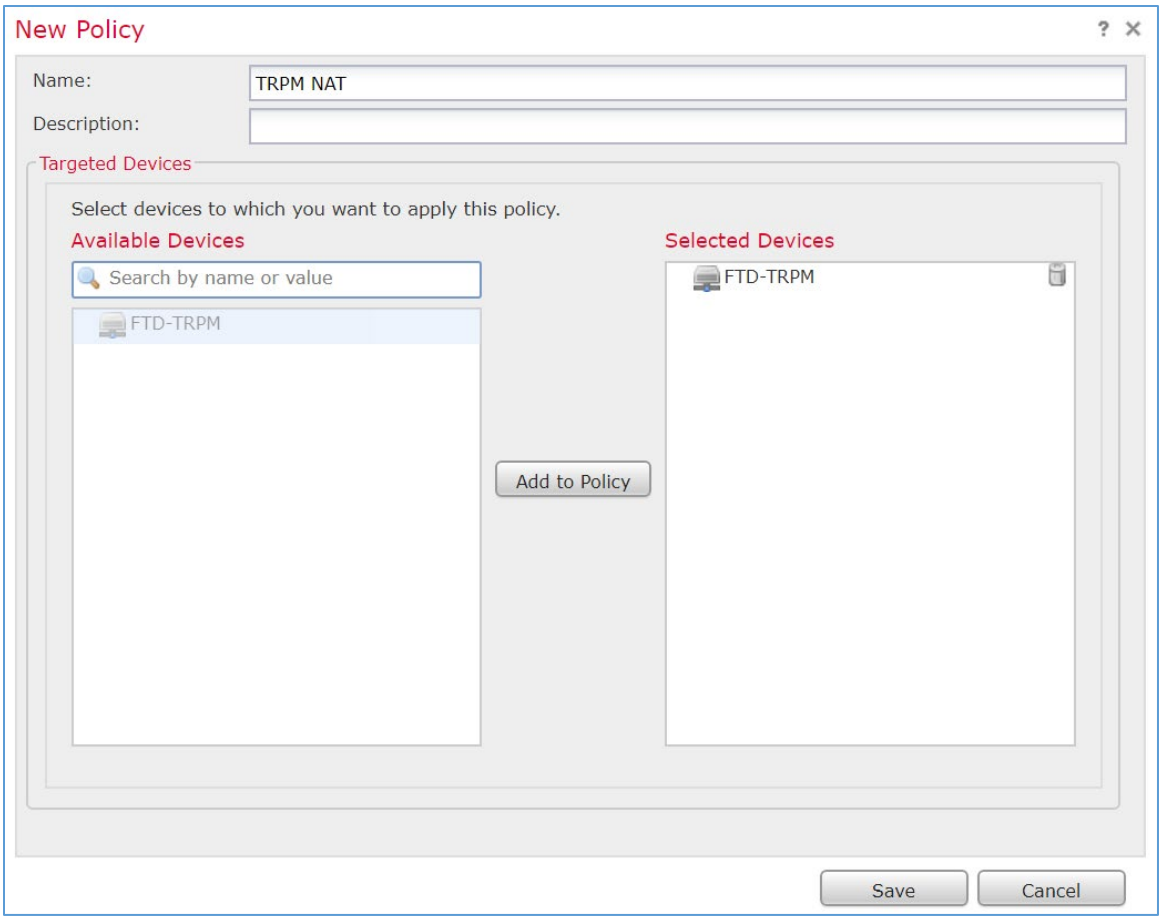


Configure Cisco FTD Network Address Translation (NAT)

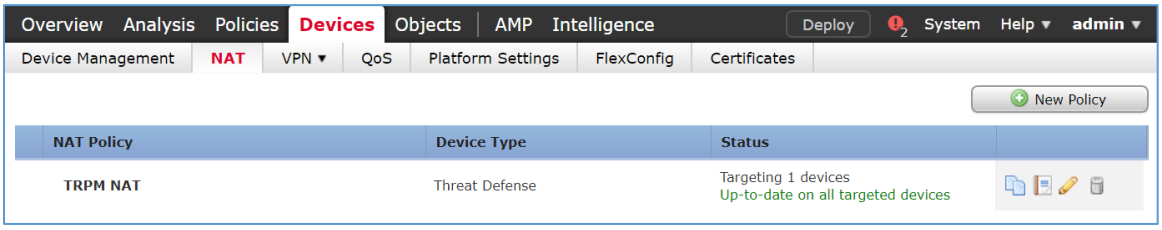
1. Click **Devices > NAT.**
2. Click **New Policy > Threat Defense NAT.**



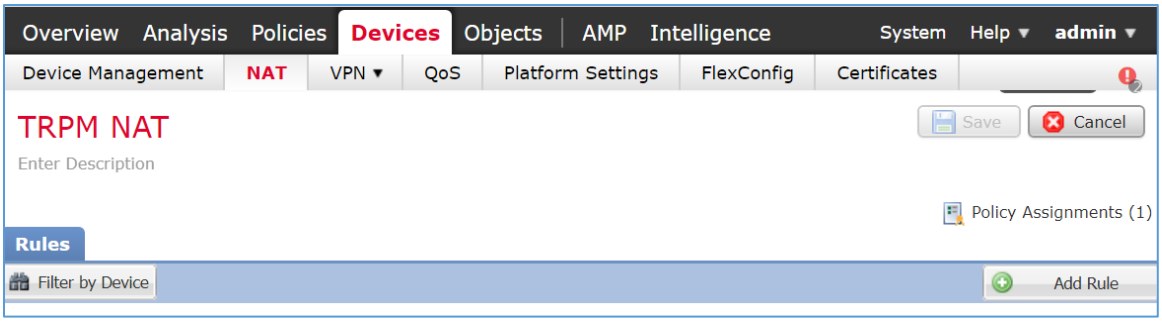
3. The New Policy pop-up window appears. Fill out the following information:
    a. **Name:** TRPM NAT
    b. **Selected Devices:** FTD-TRPM
4. Click **Save.**



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



808 6. Click **Add Rule.**



809 7. The Edit NAT Rule pop-up window appears. Under **Interface Objects,** fill out the following
810 information:

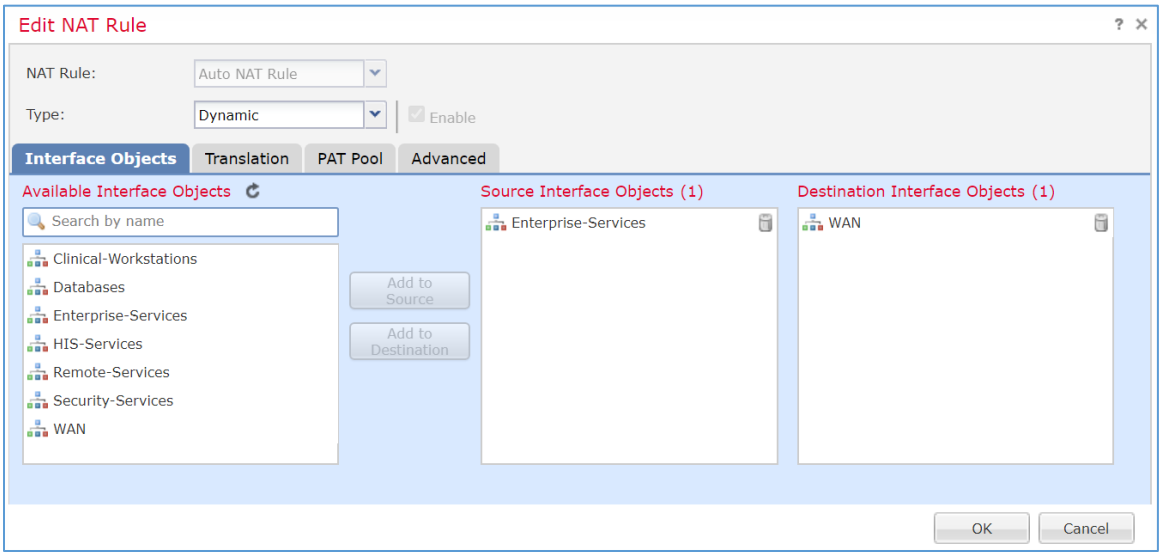
811 a. **NAT Rule:** Auto NAT Rule

812 b. **Type:** Dynamic

813 c. **Source Interface Objects:** Enterprise-Services

814 d. **Destination Interface Objects:** WAN

815 8. Click **Translation.**

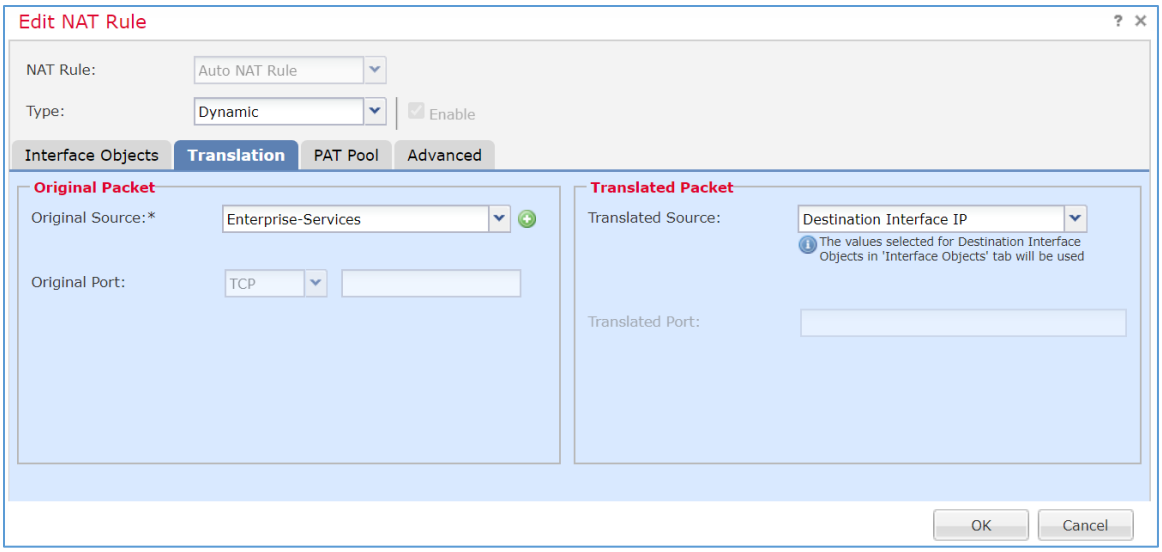


816 9. Under **Translation,** fill out the following information:

817 a. **Original Source:** Enterprise-Services

818 b. **Translated Source:** Destination Interface IP

819 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

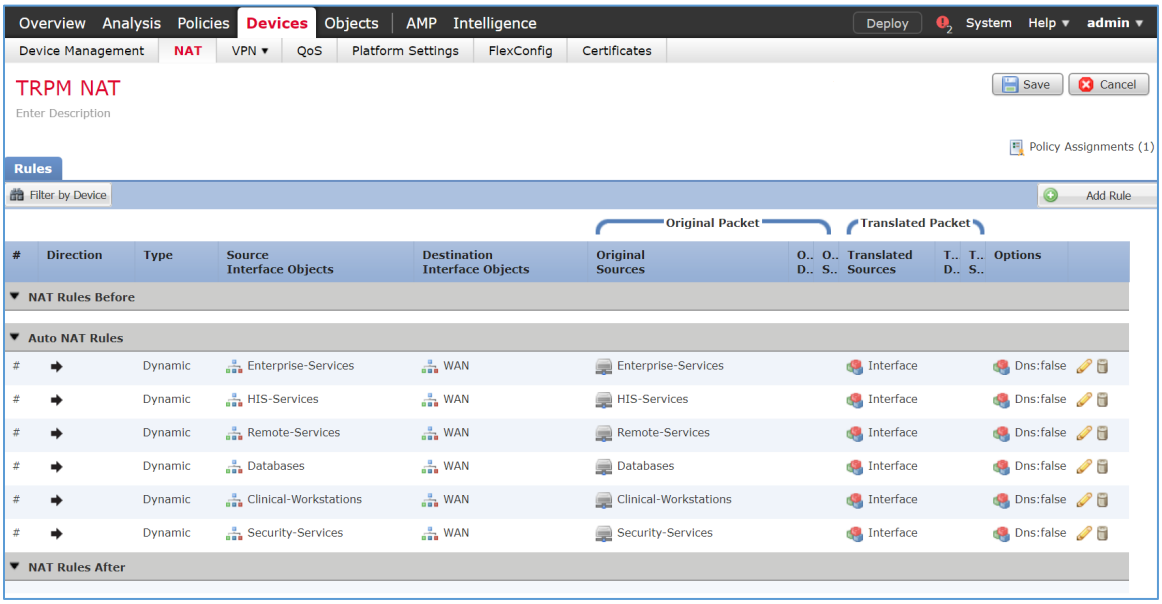
        vi. **Translated Source:** Destination Interface IP

836 c. Databases
837 i. **NAT Rule:** Auto NAT Rule
838 ii. **Type:** Dynamic
839 iii. **Source Interface Objects:** Databases
840 iv. **Destination Interface Objects:** WAN
841 v. **Original Source:** Databases
842 vi. **Translated Source:** Destination Interface IP
843 d. Clinical-Workstations
844 i. **NAT Rule:** Auto NAT Rule
845 ii. **Type:** Dynamic
846 iii. **Source Interface Objects:** Clinical-Workstations
847 iv. **Destination Interface Objects:** WAN
848 v. **Original Source:** Clinical-Workstations
849 vi. **Translated Source:** Destination Interface IP
850 e. Security-Services
851 i. **NAT Rule:** Auto NAT Rule
852 ii. **Type:** Dynamic
853 iii. **Source Interface Objects:** Security-Services
854 iv. **Destination Interface Objects:** WAN
855 v. **Original Source:** Security-Services
856 vi. **Translated Source:** Destination Interface IP

857 12. Click **Save.**

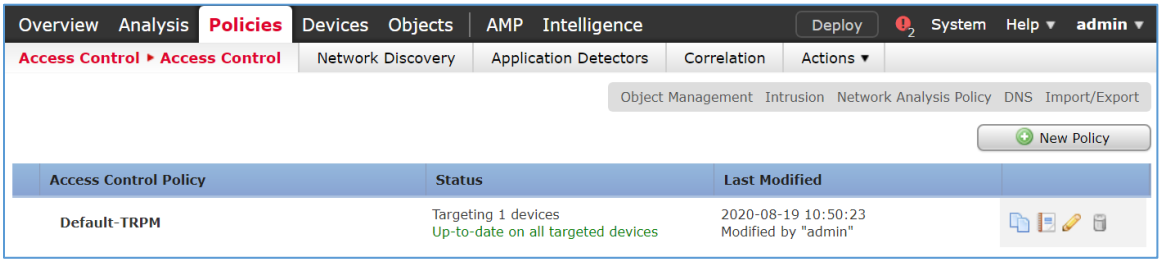
858 13. Click **Deploy.** Verify the NAT settings through the **Devices** screen. The **NAT** rules are displayed in
859 a table format. The table includes values for **Direction** of the NAT displayed as a directional
860 arrow, the **NAT Type,** the **Source Interface Objects** (i.e., the security zone IP networks), the
861 **Destination Interface Objects,** the **Original Sources** (i.e., these addresses correspond to the IP
862 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.

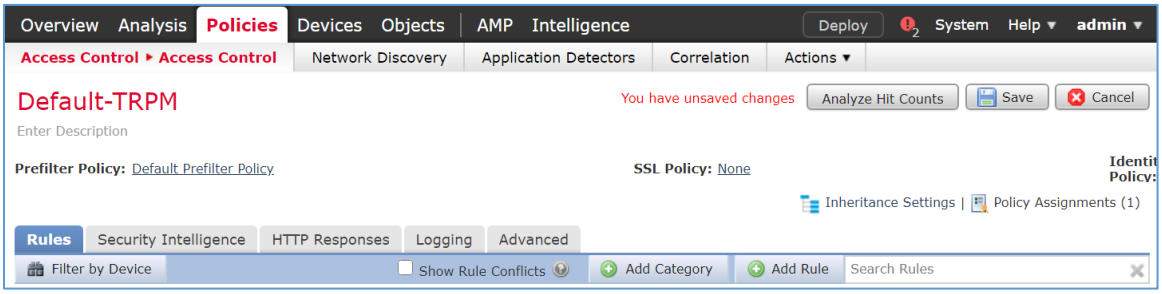


Configure Cisco FTD Access Control Policy

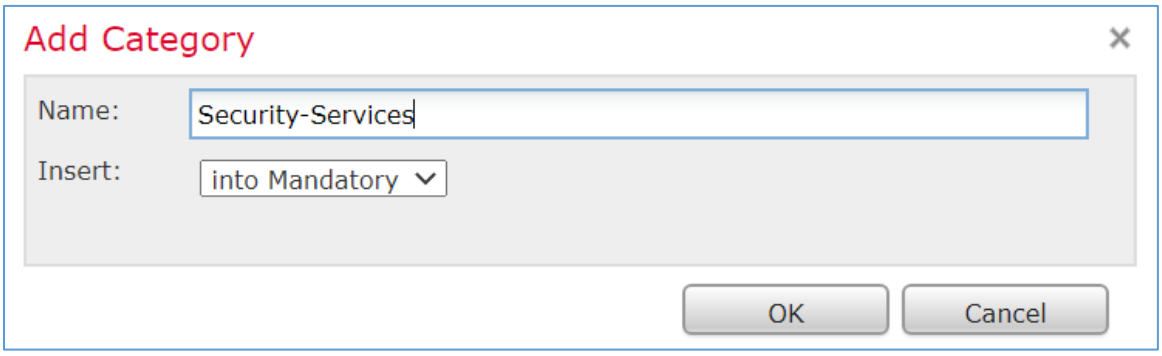
1. Click **Polices > Access Control > Access Control.**
2. Click the **edit symbol** for **Default-TRPM.**



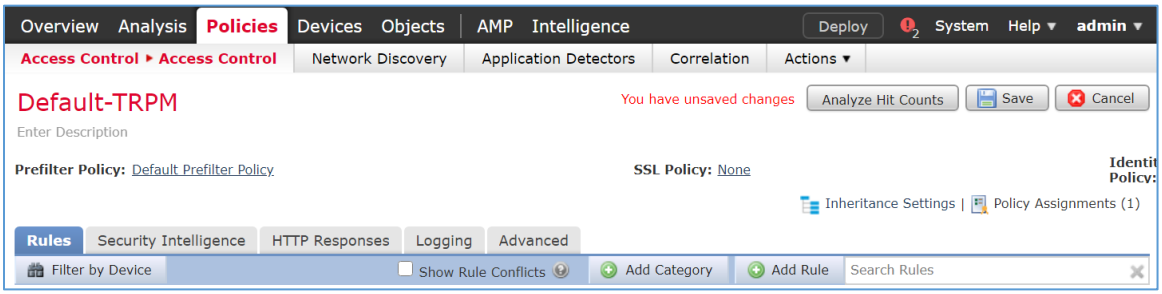
3. Click **Add Category.**



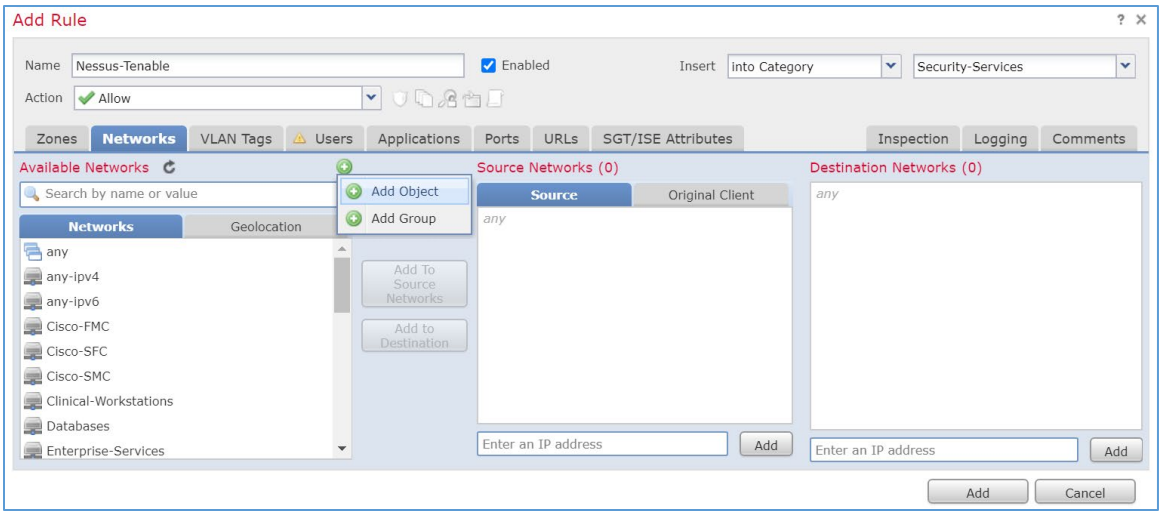
4. Fill out the following information:
    a. **Name:** Security Services
    b. **Insert:** into Mandatory
5. Click **OK.**



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.**

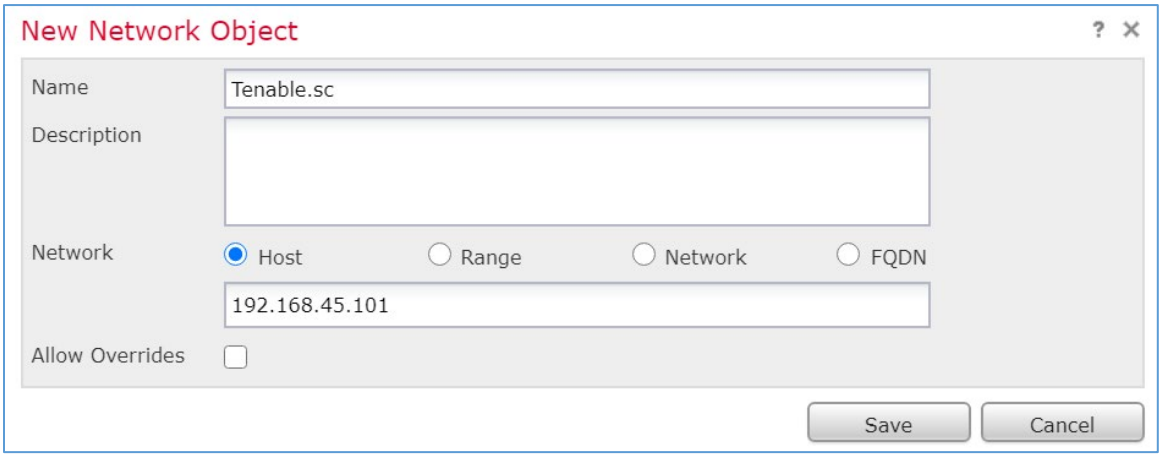


882 9. When the New Network Object pop-up window appears, fill out the following information:

883 a. **Name:** Tenable.sc

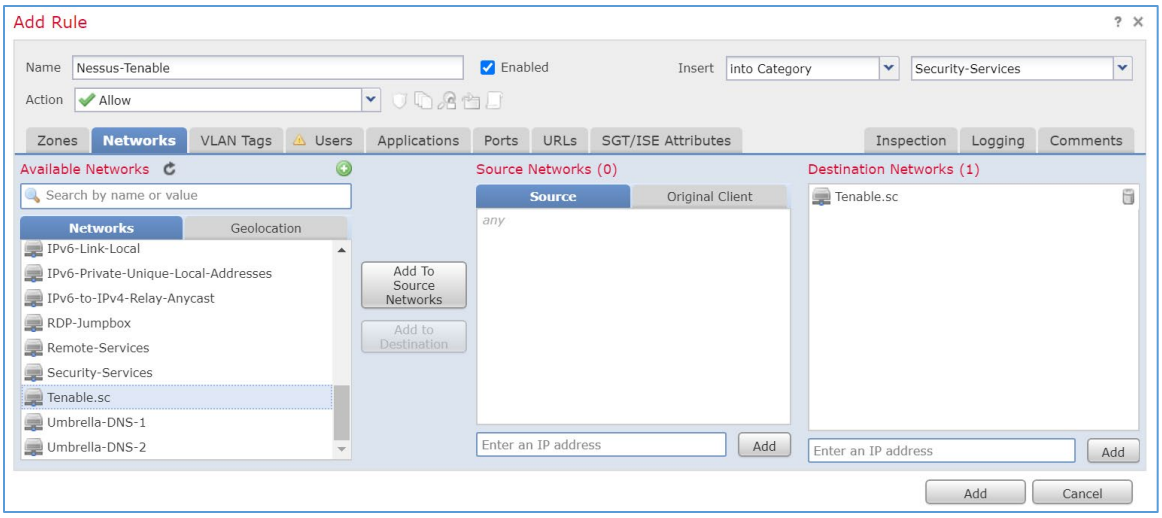
884 b. **Network (Host):** 192.168.45.101

885 10. Click **Save.**



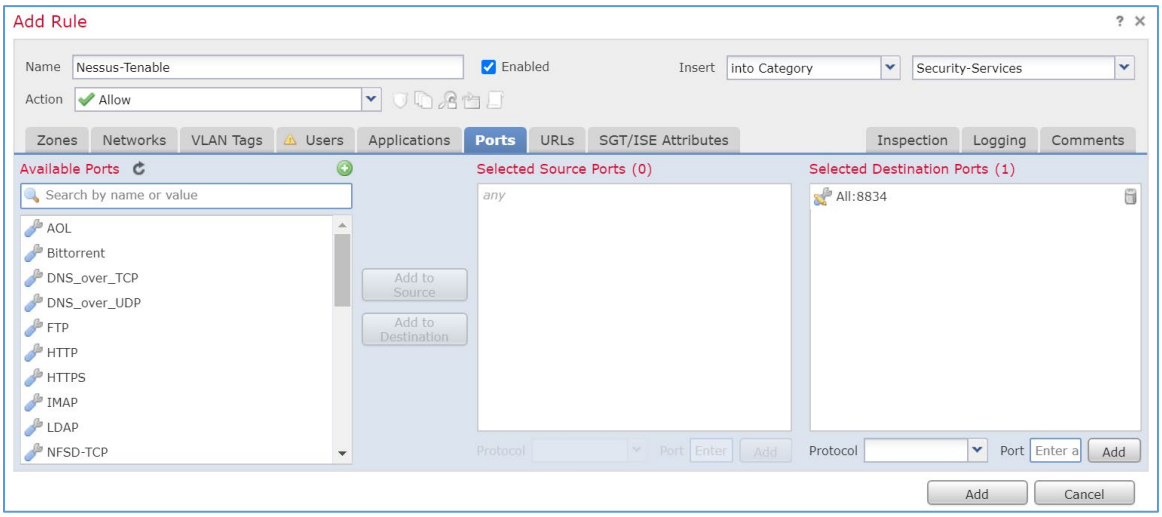
886 11. In the Add Rule screen, under the **Networks** tab, set **Destination Networks** to **Tenable.sc.**

887 12. Click **Ports.**



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

889 14. Click **Add.**



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

891 16. Click **Save.**

892 17. Click **Deploy.**

893 2.2.3 Security Continuous Monitoring

894 The project team implemented a set of tools that included Cisco Stealthwatch, Cisco Umbrella, and
895 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

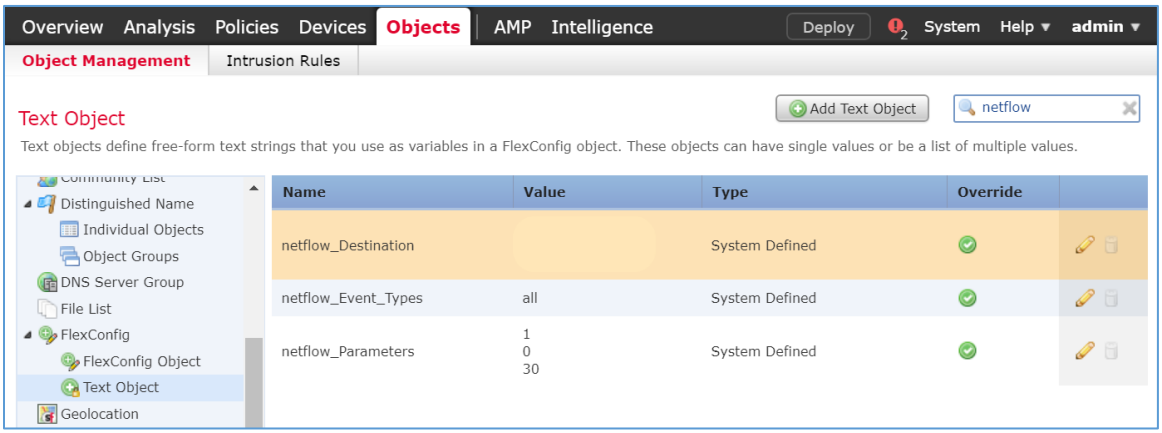
Install the appliance according to the instructions detailed in the *Cisco Stealthwatch Installation and Configuration Guide 7.1* [8].

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

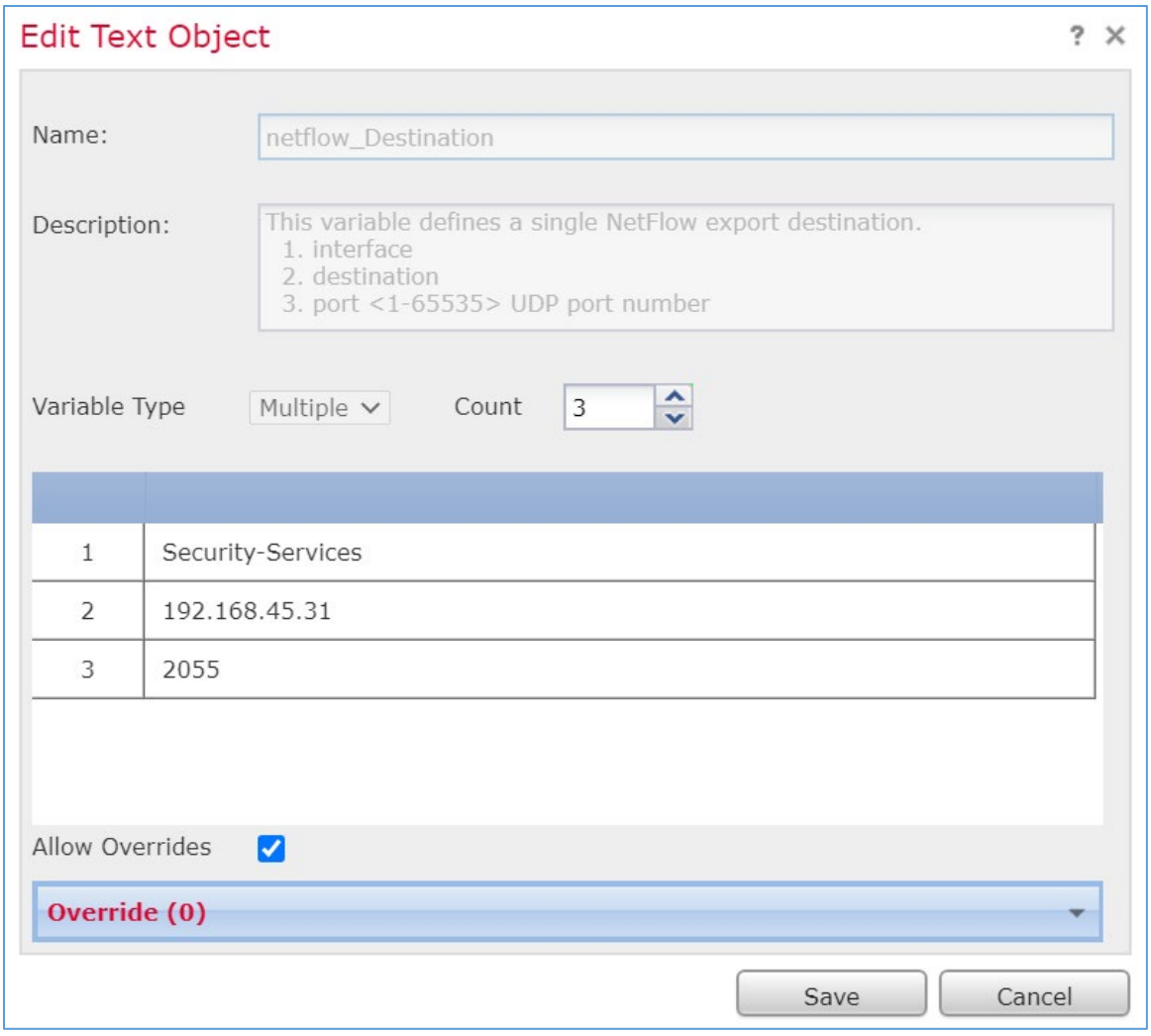
Configure Cisco FTD NetFlow for Cisco SFC

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

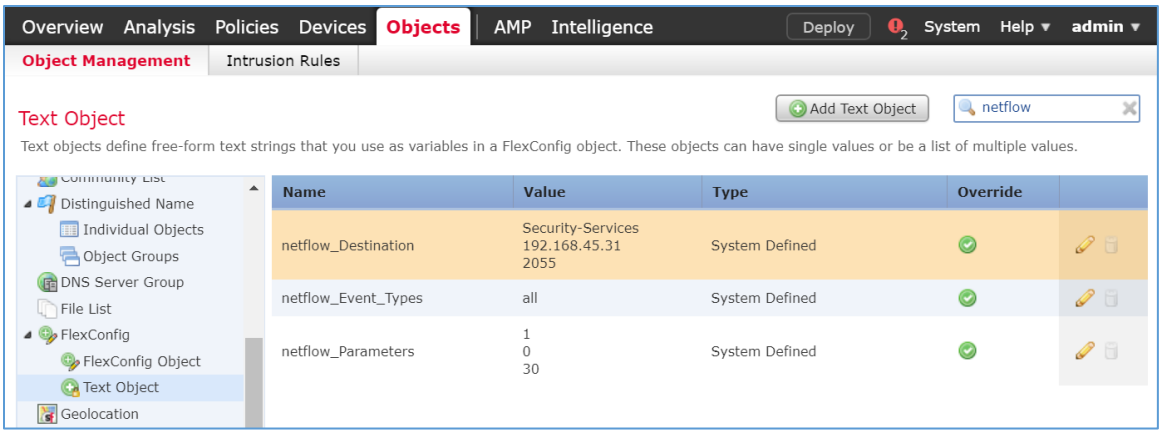
2. In the **search box,** type `netflow`.
3. Click the **edit symbol** for **netflow_Destination.**



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.**



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



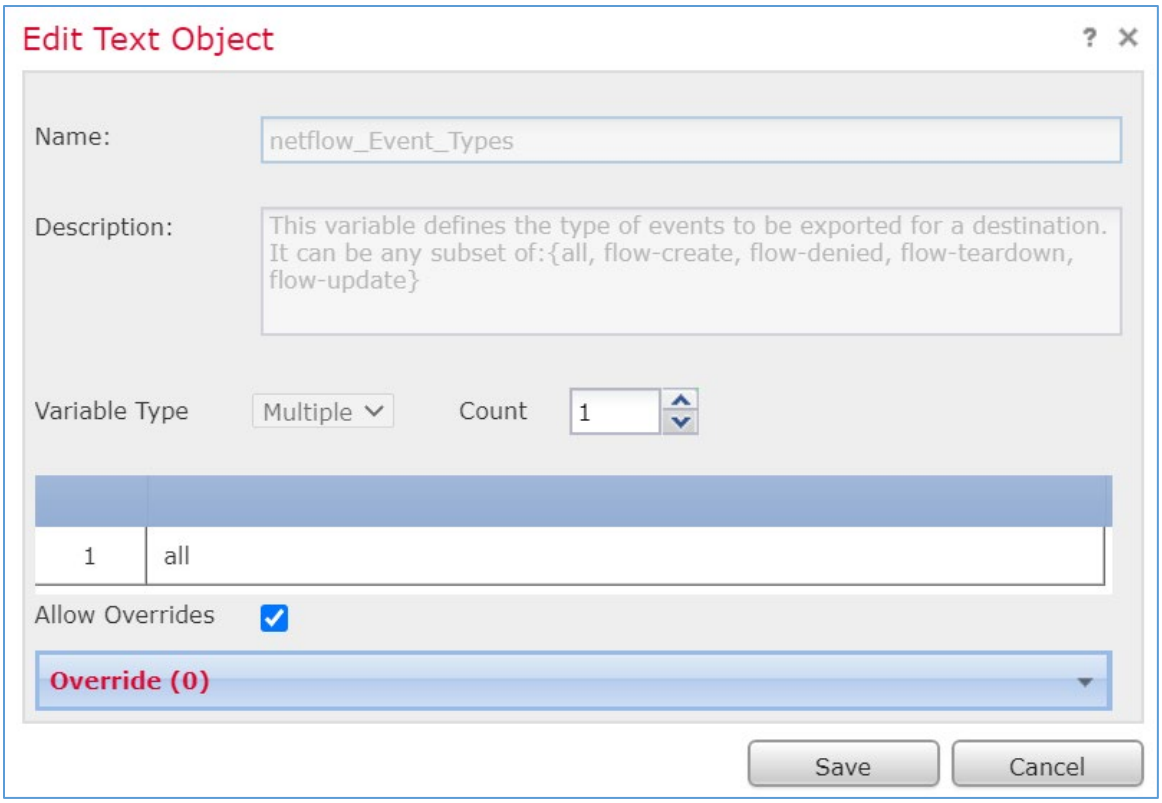
933 7. When the Edit Text Object pop-up window appears, fill out the following information:

934 a. **Count:** 1

935 b. **1:** All

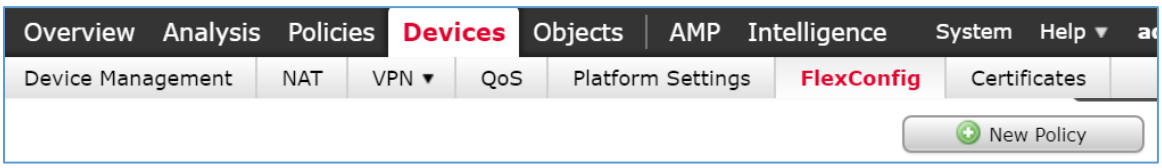
936 c. **Allow Overrides:** checked

937 8. Click **Save.**



938 9. Click **Devices > FlexConfig.**

939 10. Click **New Policy.**

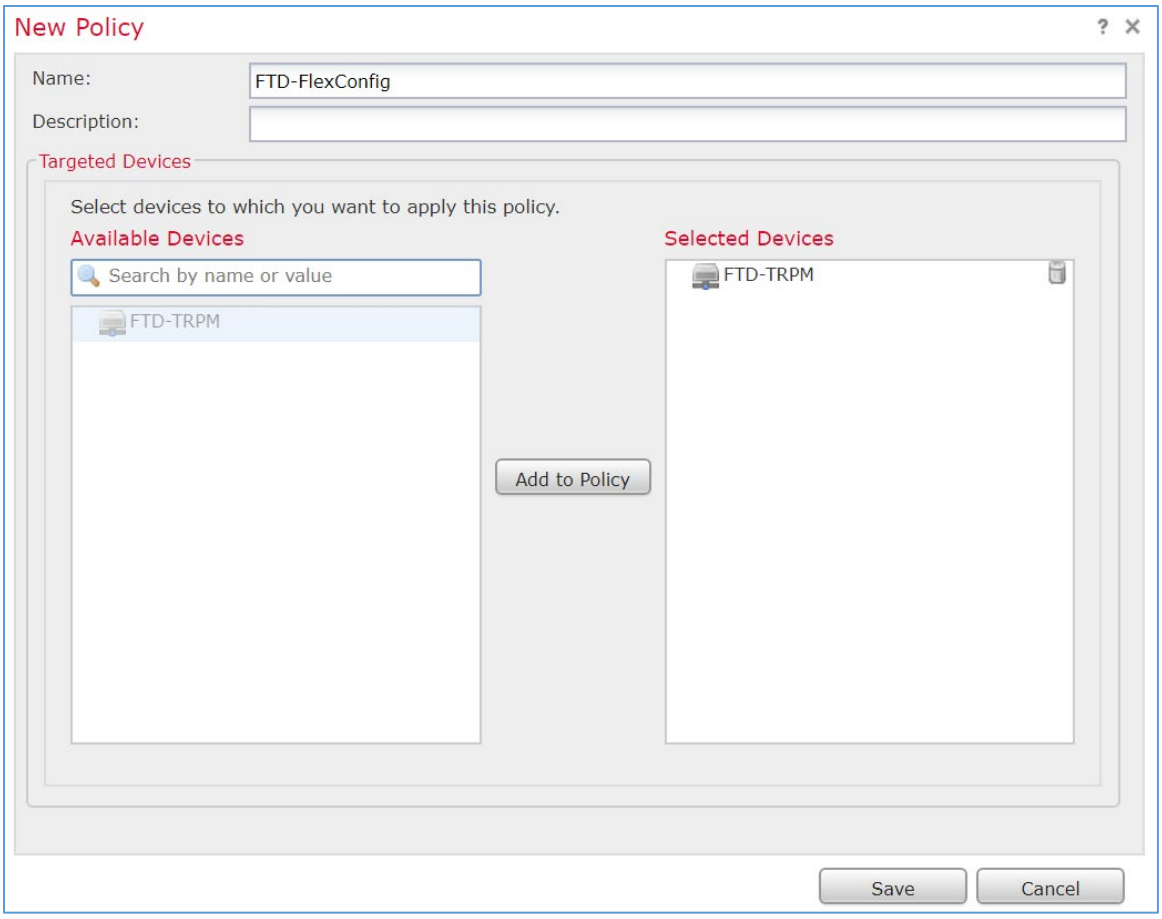


940 11. When the New Policy screen appears, fill out the following information:

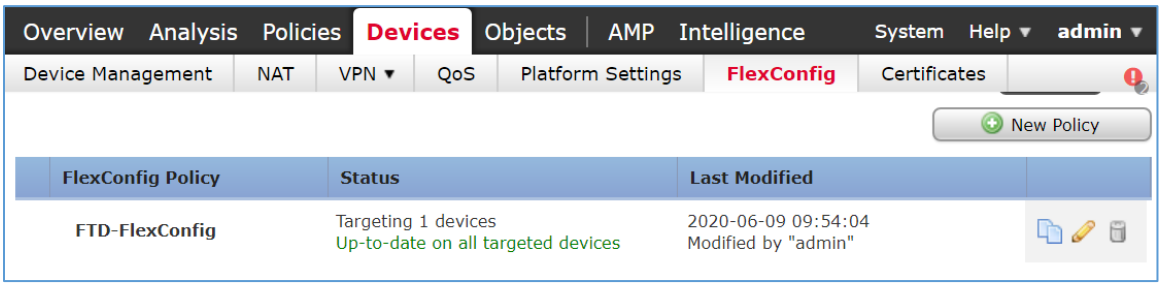
941 a. **Name:** FTD-FlexConfig

942 b. **Selected Devices:** FTD-TRPM

943 12. Click **Save.**

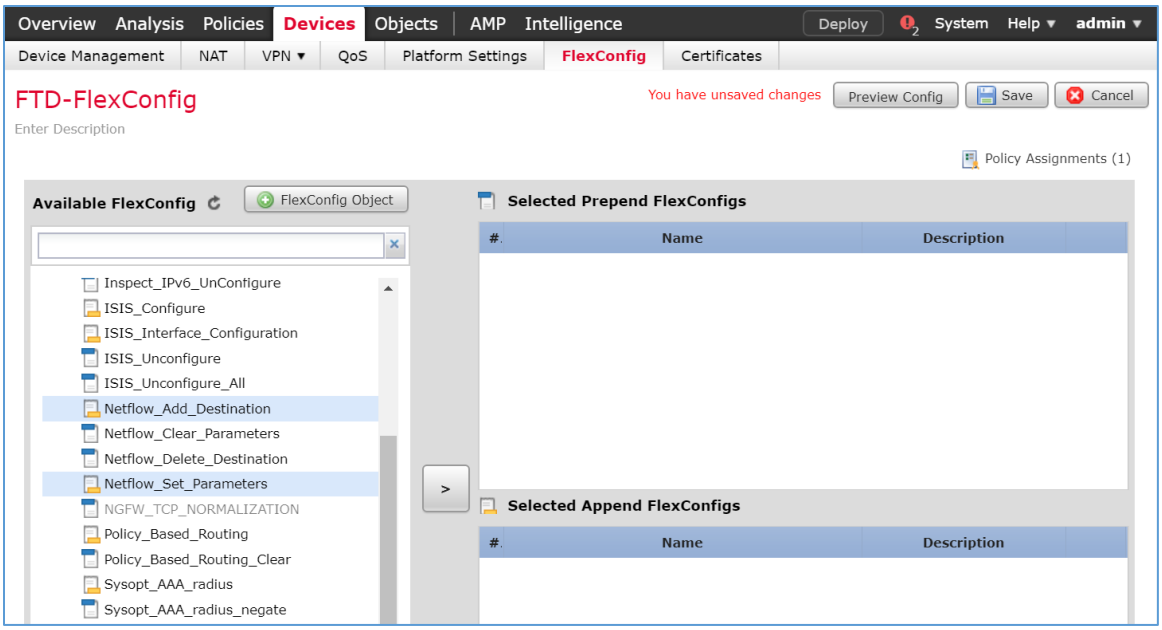


944 13. Click the **edit symbol** for **FTD-FlexConfig.**



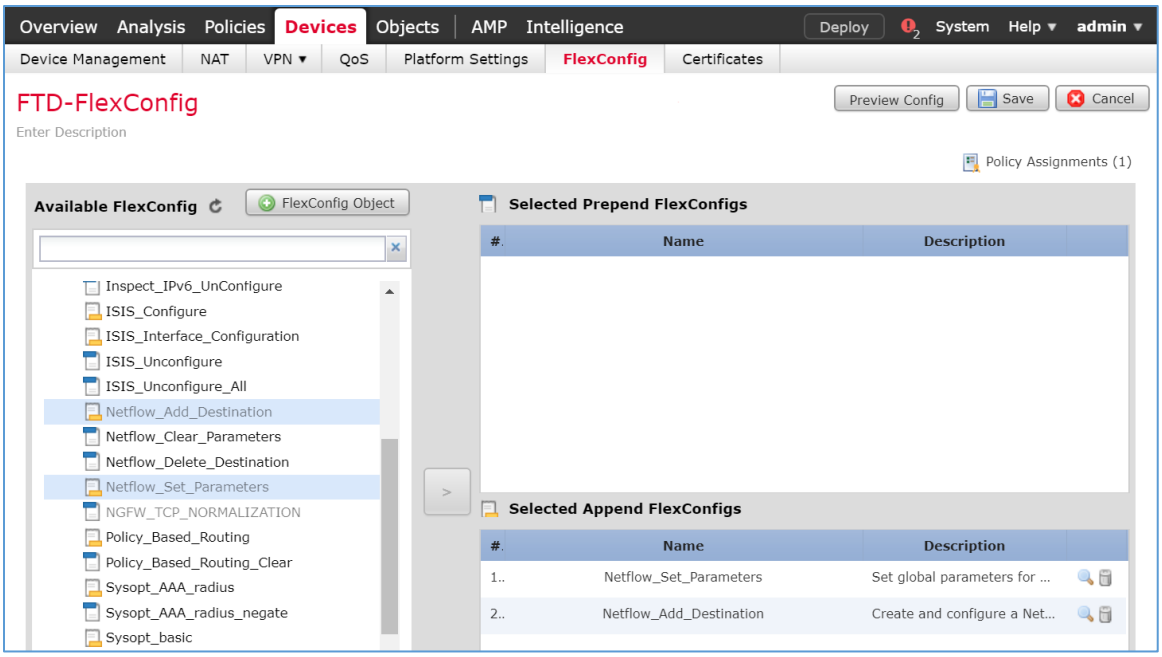
945 14. Under the **Devices** tab, select **Netflow_Add_Destination** and **Netflow_Set_Parameters.**

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



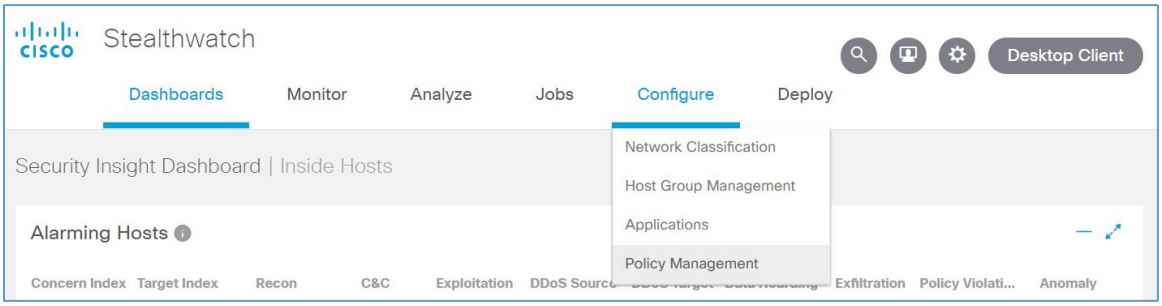
16. Click **Save.**

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.**

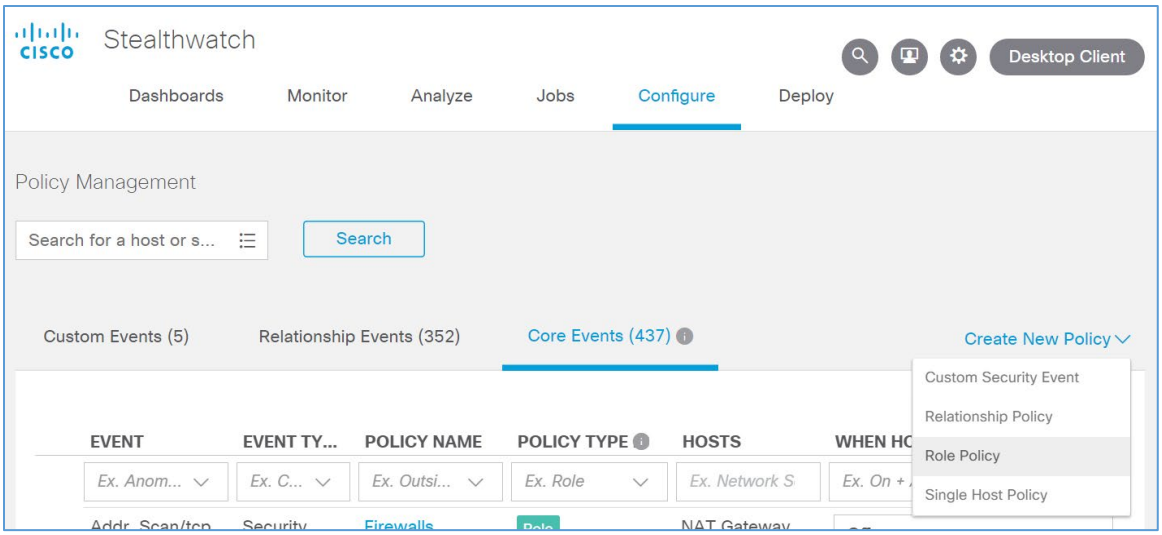


953 **Create a Custom Policy Management Rule**

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

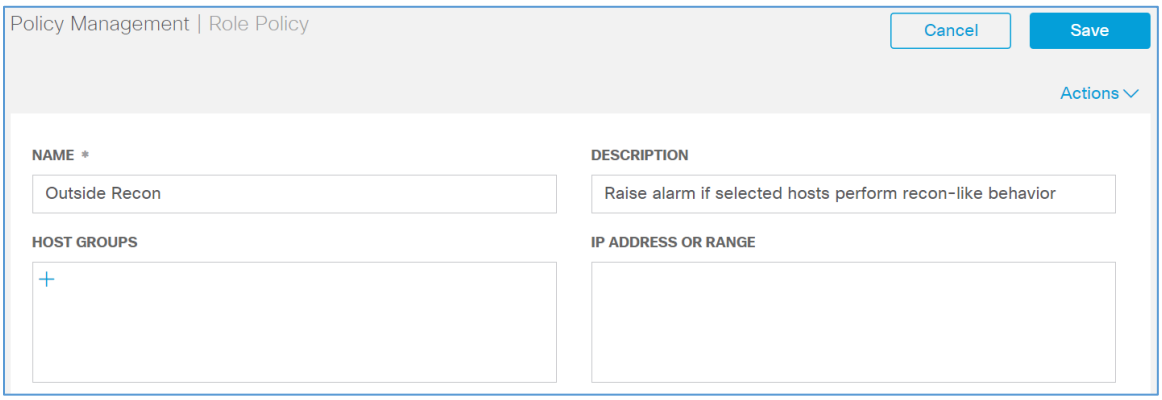


955 2. Click **Create New Policy > Role Policy.**



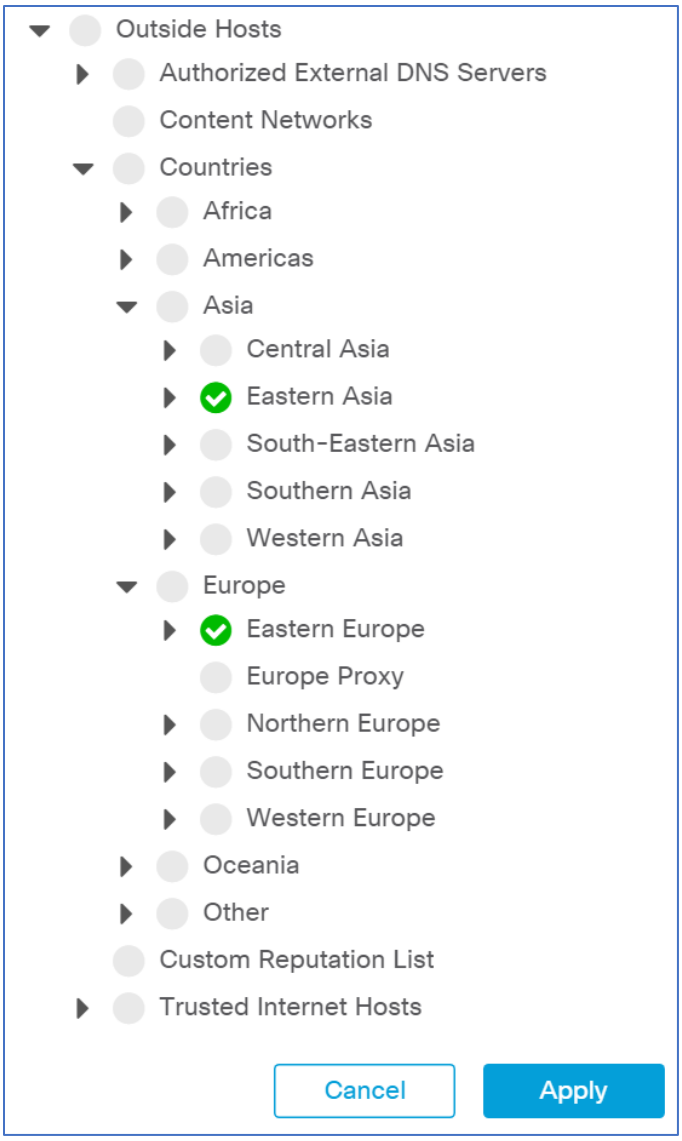
956 3. Give the policy a **name** and **description.**

957 4. Under **Host Groups,** click the **plus symbol.**

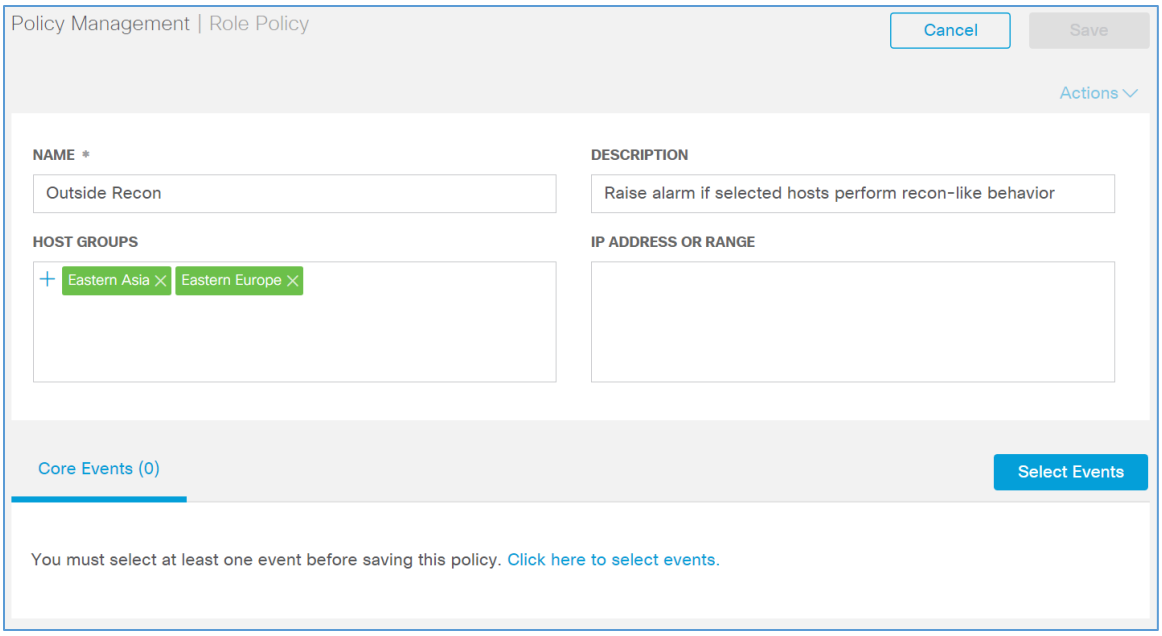


958 5. Under **Outside** Hosts, select **Eastern Asia** and **Eastern Europe.**

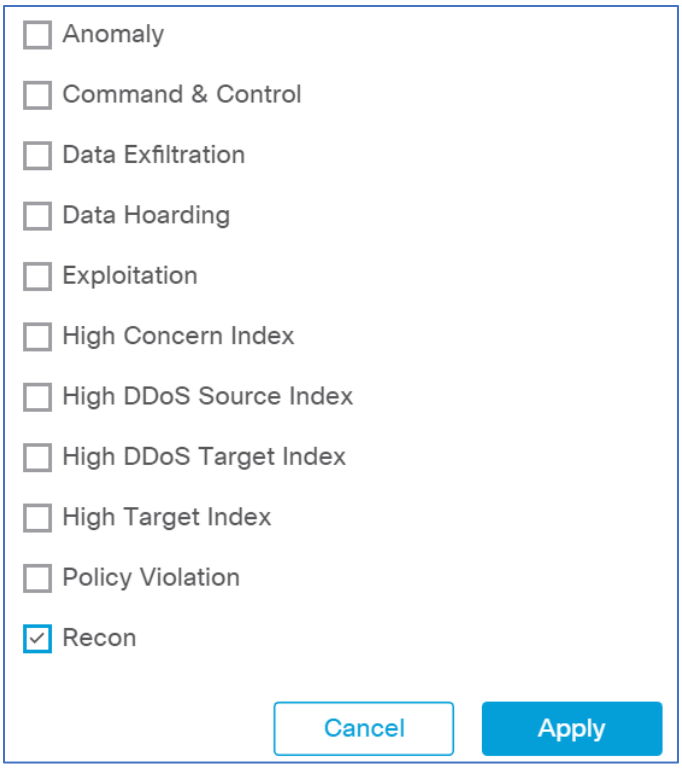
959 6. Click **Apply.**



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

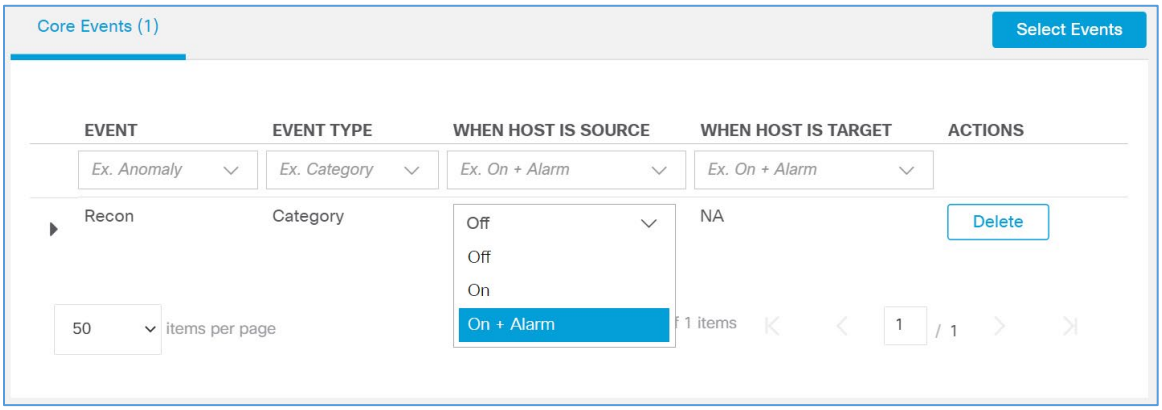


961 8. Select **Recon.**
962 9. Click **Apply.**

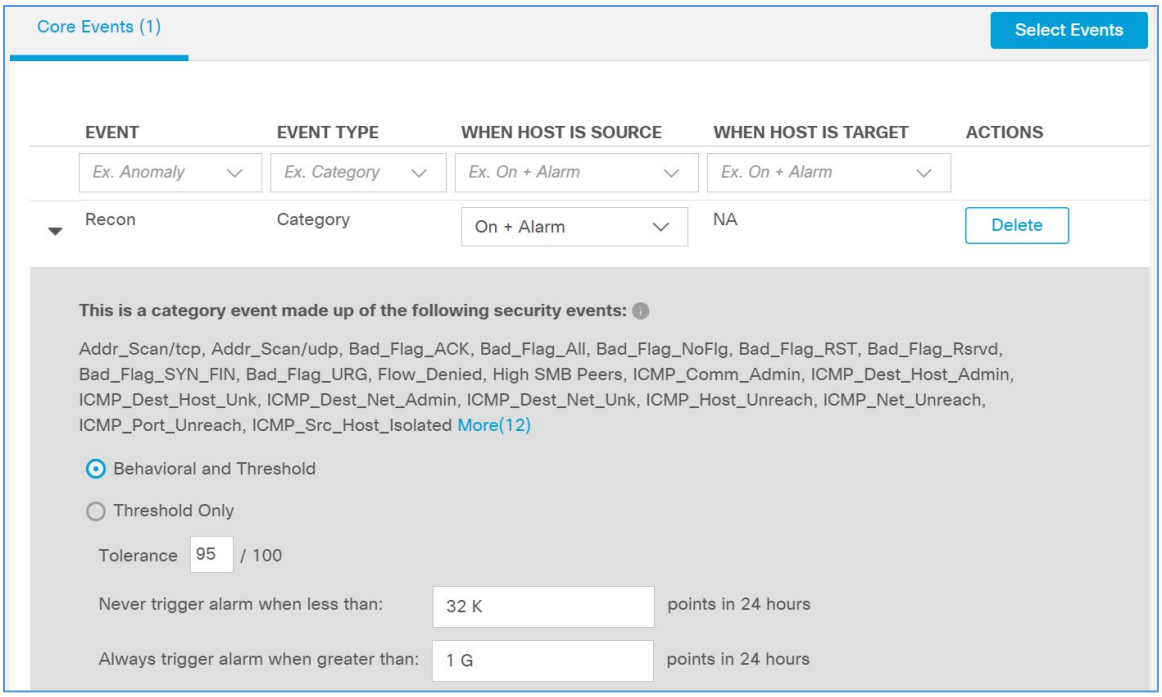


963 10. Under **Core Events > Recon** > **When Host is Source**, select **On + Alarm.**

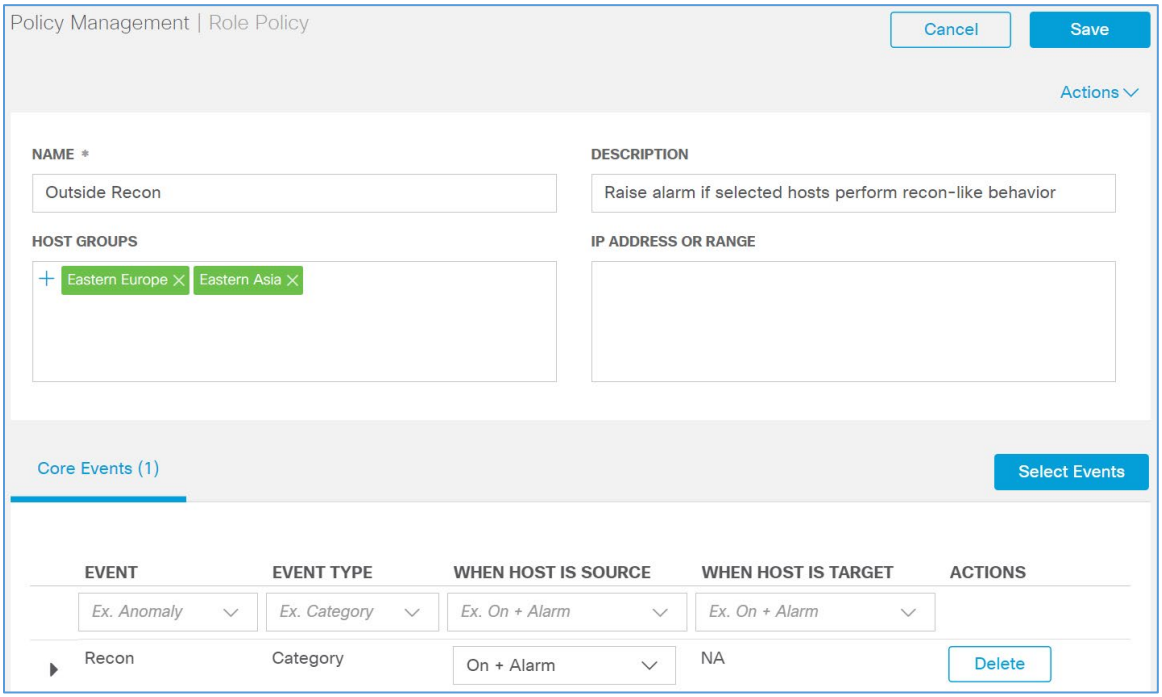
964 11. Click the **expand arrow** next to **Recon.**



965 12. Select **Behavioral and Threshold.**



966 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.

Cisco Umbrella Forwarder Appliance Information

CPU: 1

RAM: 0.5 GB

Storage: 6.5 GB (Thick Provision)

Network Adapter 1: VLAN 1327

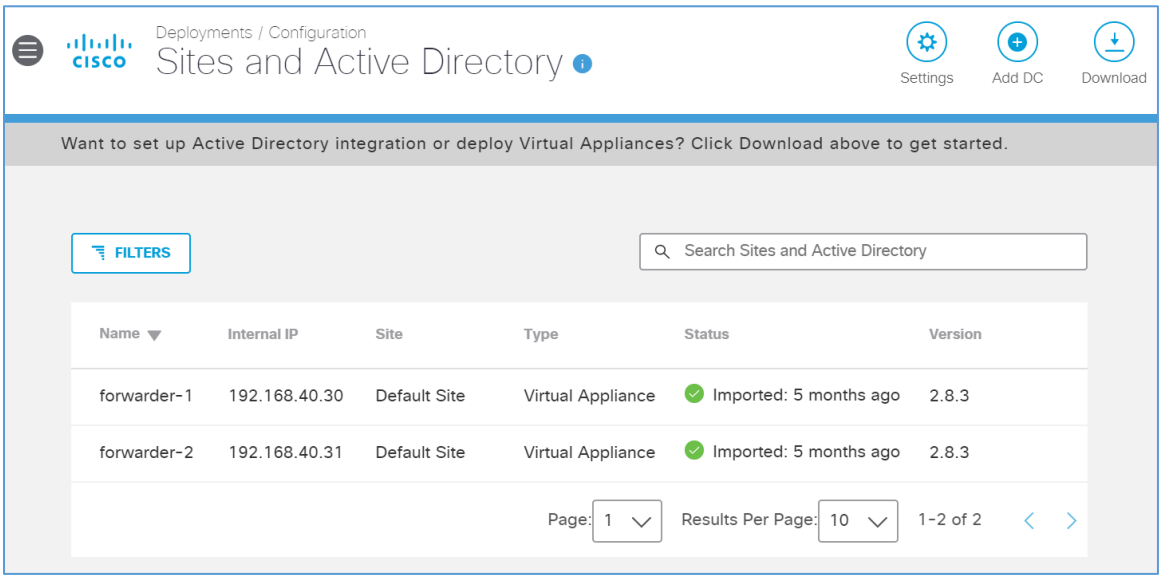
Operating System: Linux

Cisco Umbrella Forwarder Appliance Installation Guide

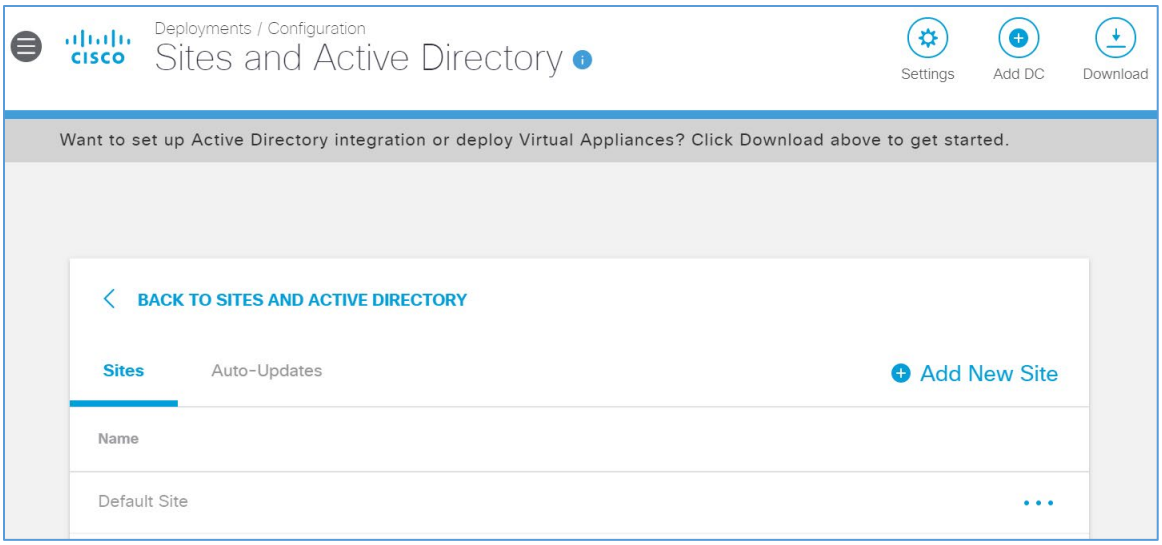
Install the appliance according to the instructions detailed in Cisco's Deploy VAs in VMware guidance [9].

Create an Umbrella Site

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

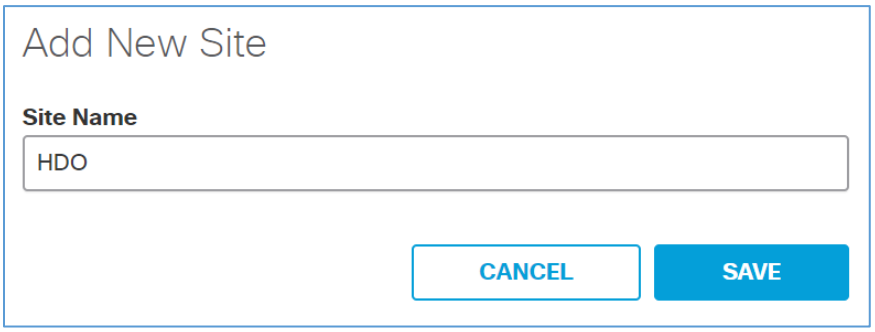


3. Click **Add New Site.**



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

984 5. Click **Save.**

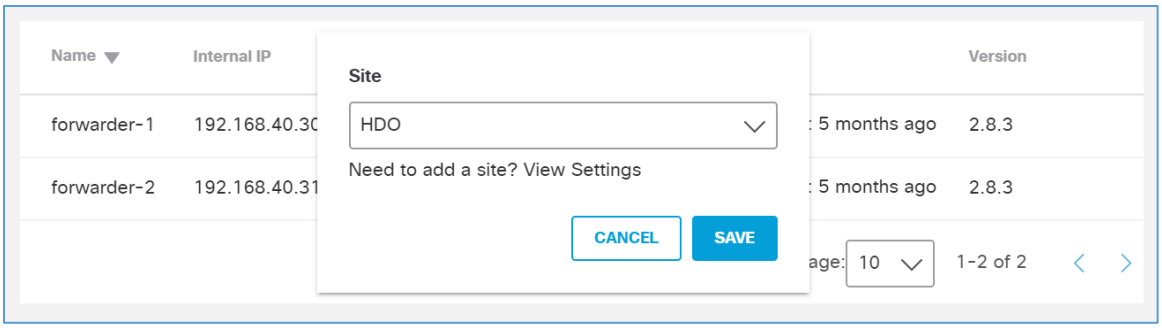


985 6. Click **Deployments > Configuration > Sites and Active Directory.**

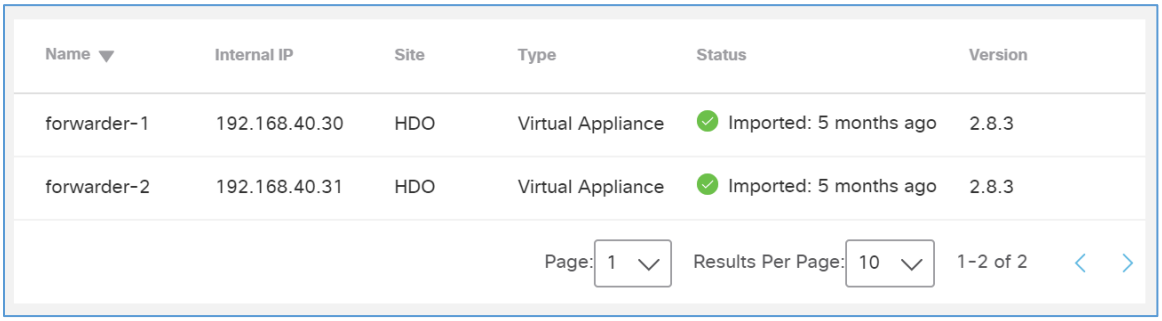
986 7. Click the **edit symbol** for the Site of **forwarder-1.**

987 8. Under Site, select **HDO.**

988 9. Click **Save.**



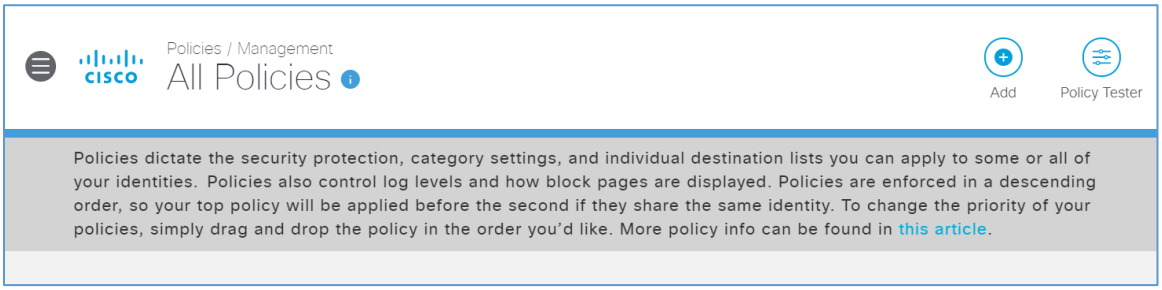
989 10. Repeat the previous steps for **forwarder-2.**



990 **Configure an Umbrella Policy**

991 1. Click **Policies > Management > All Policies.**

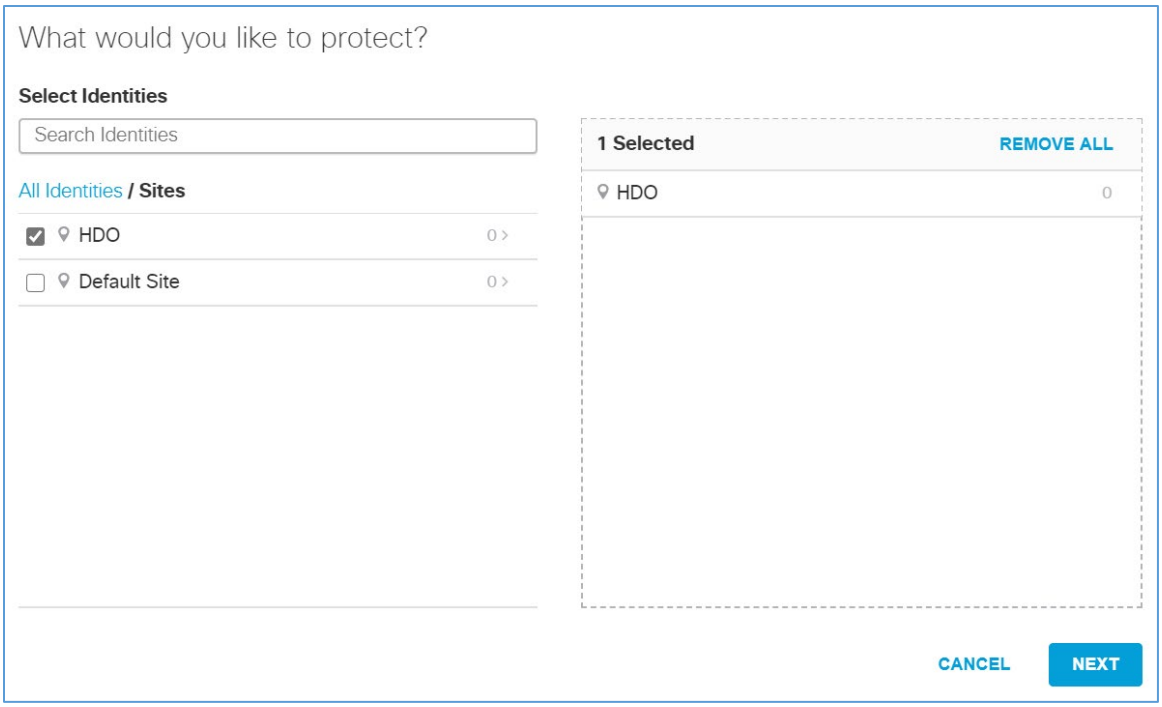
992 2. Click **Add.**



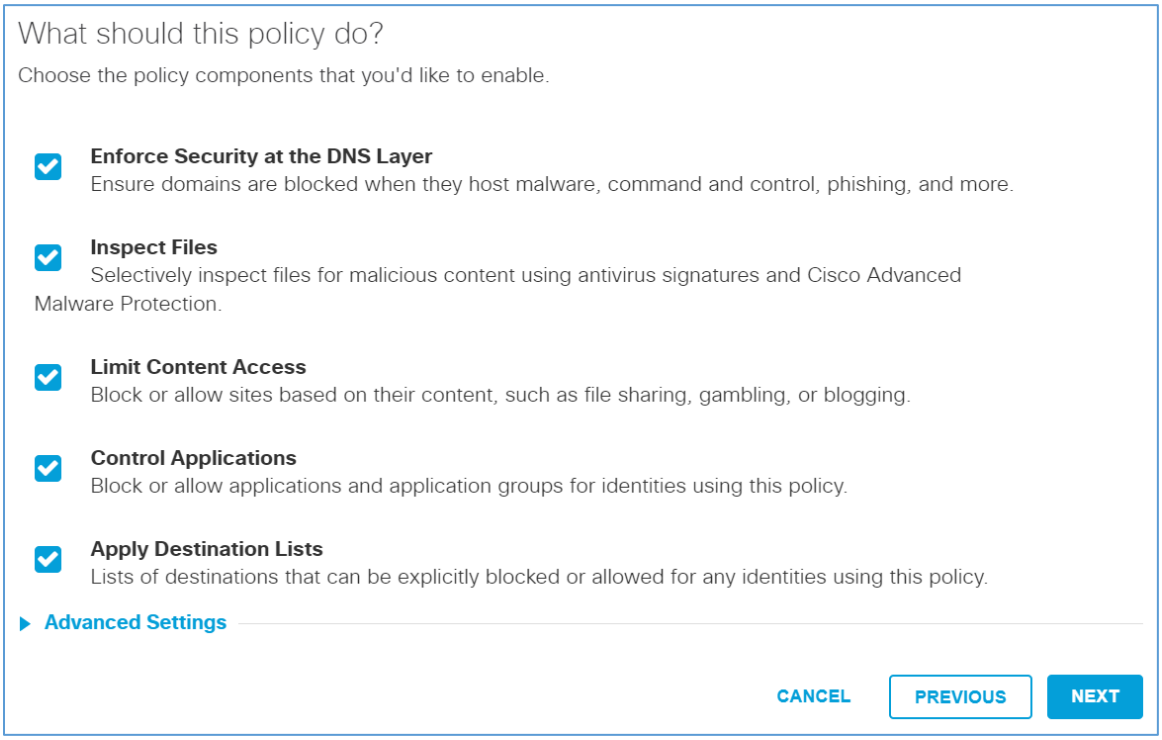
993 3. Expand the **Sites** identity.

994 4. Select **HDO.**

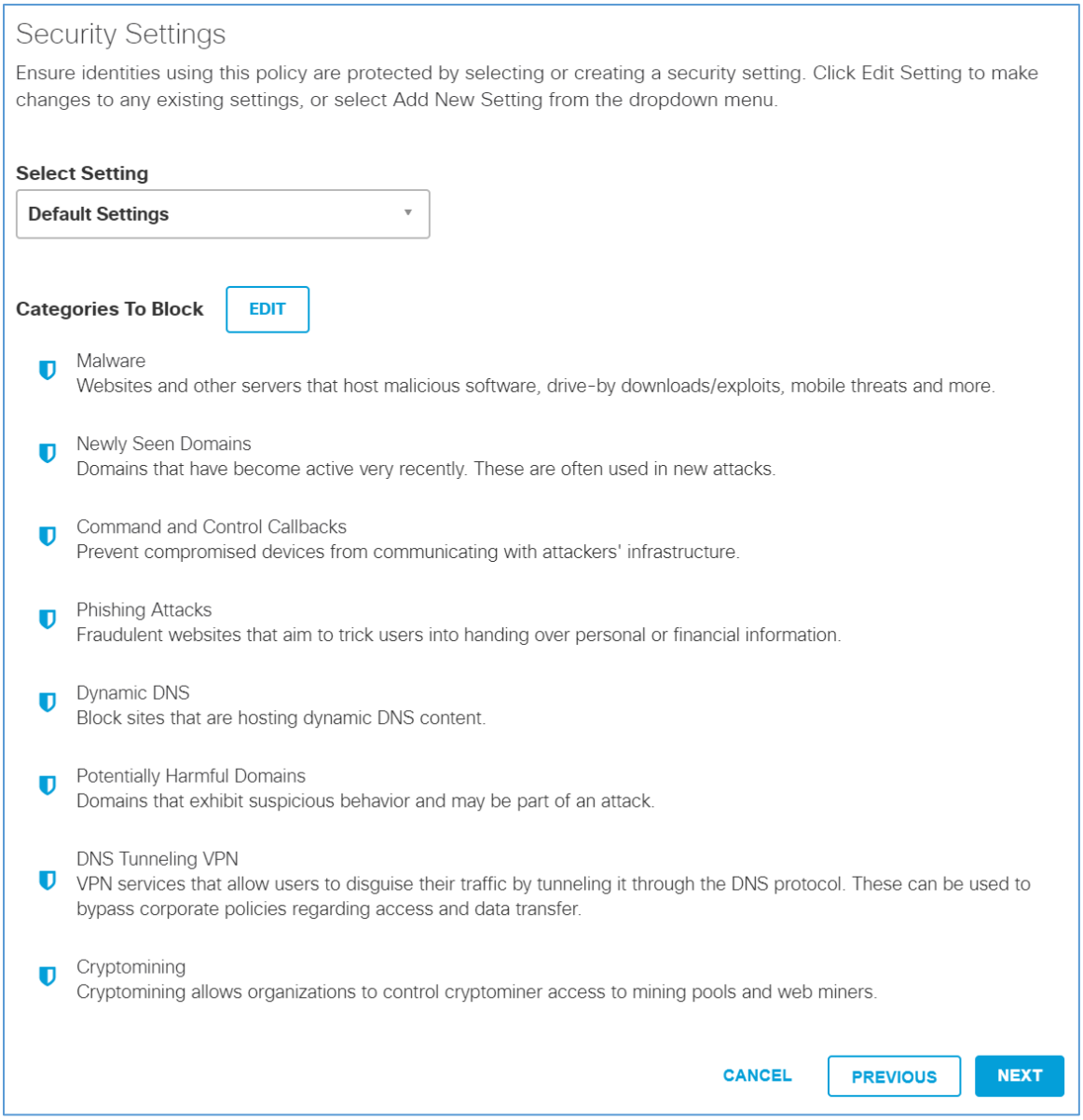
995 5. Click **Next.**



996 6. Click **Next.**

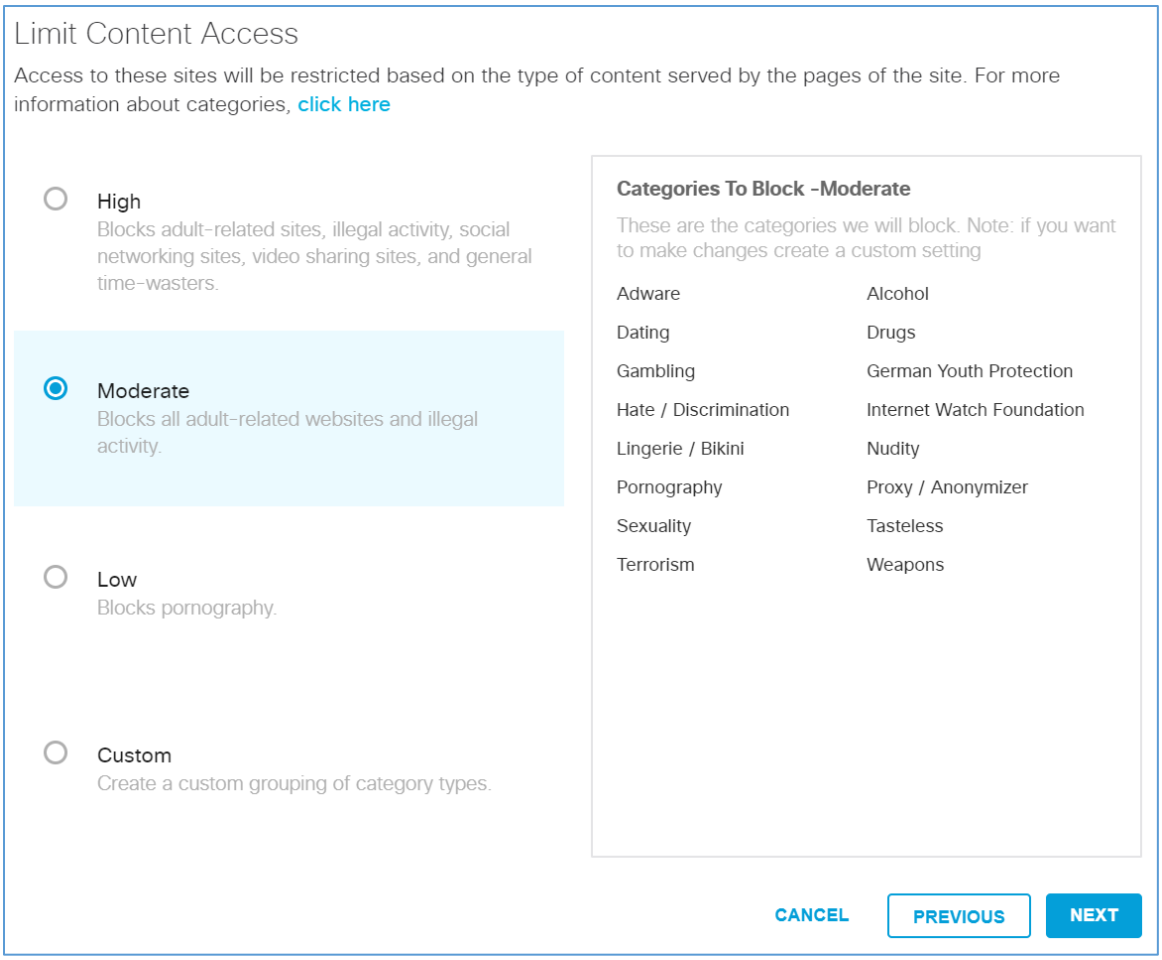


997 7. Click **Next.**

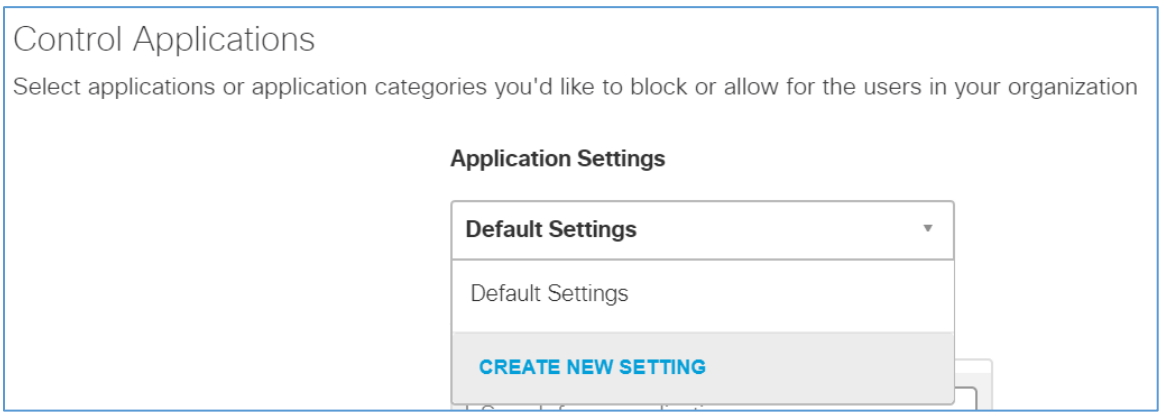


998 8. Select **Moderate.**

999 9. Click **Next.**



1000 10. Under Application Settings, use the drop-down menu to select **Create New Setting.**

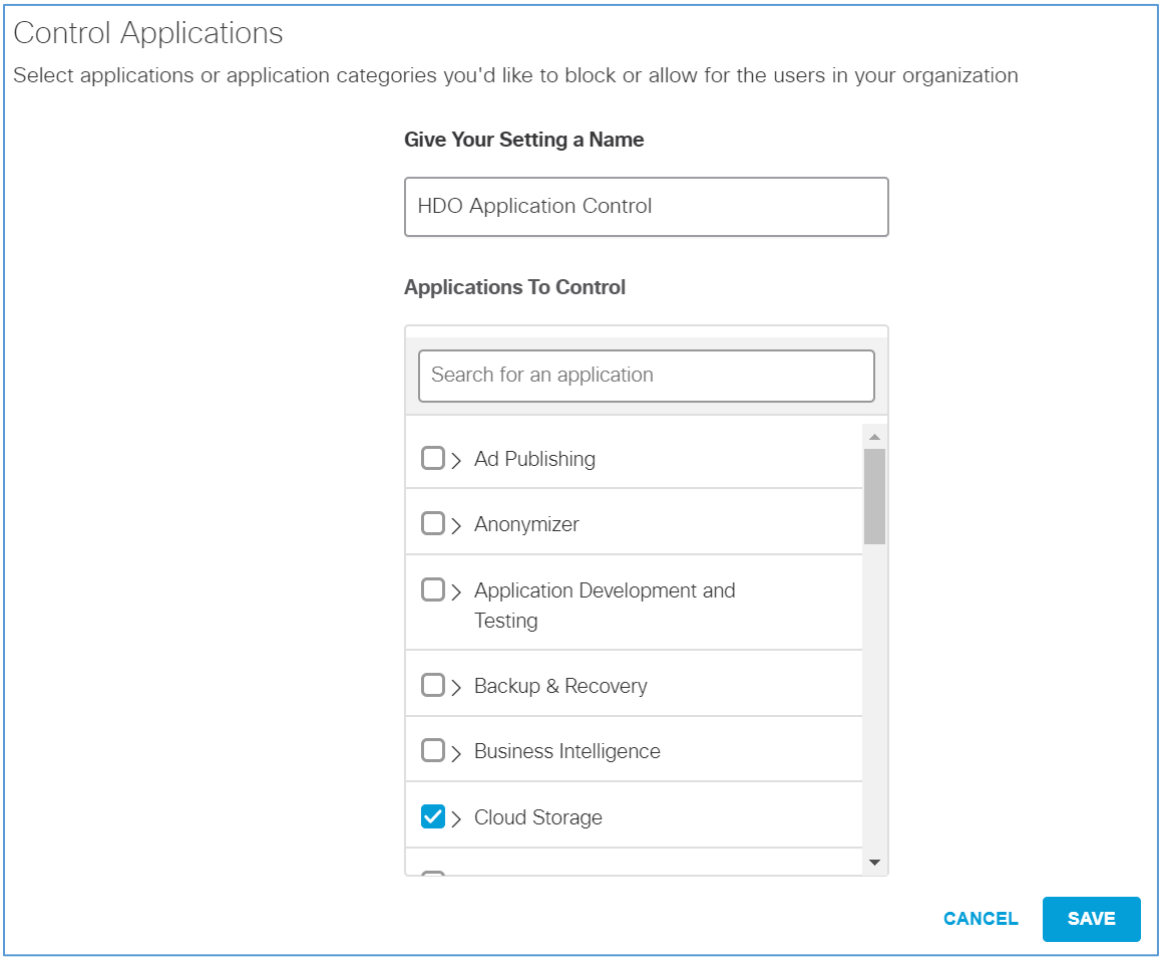


1001 11. Under the Control Applications screen, fill out the following information:

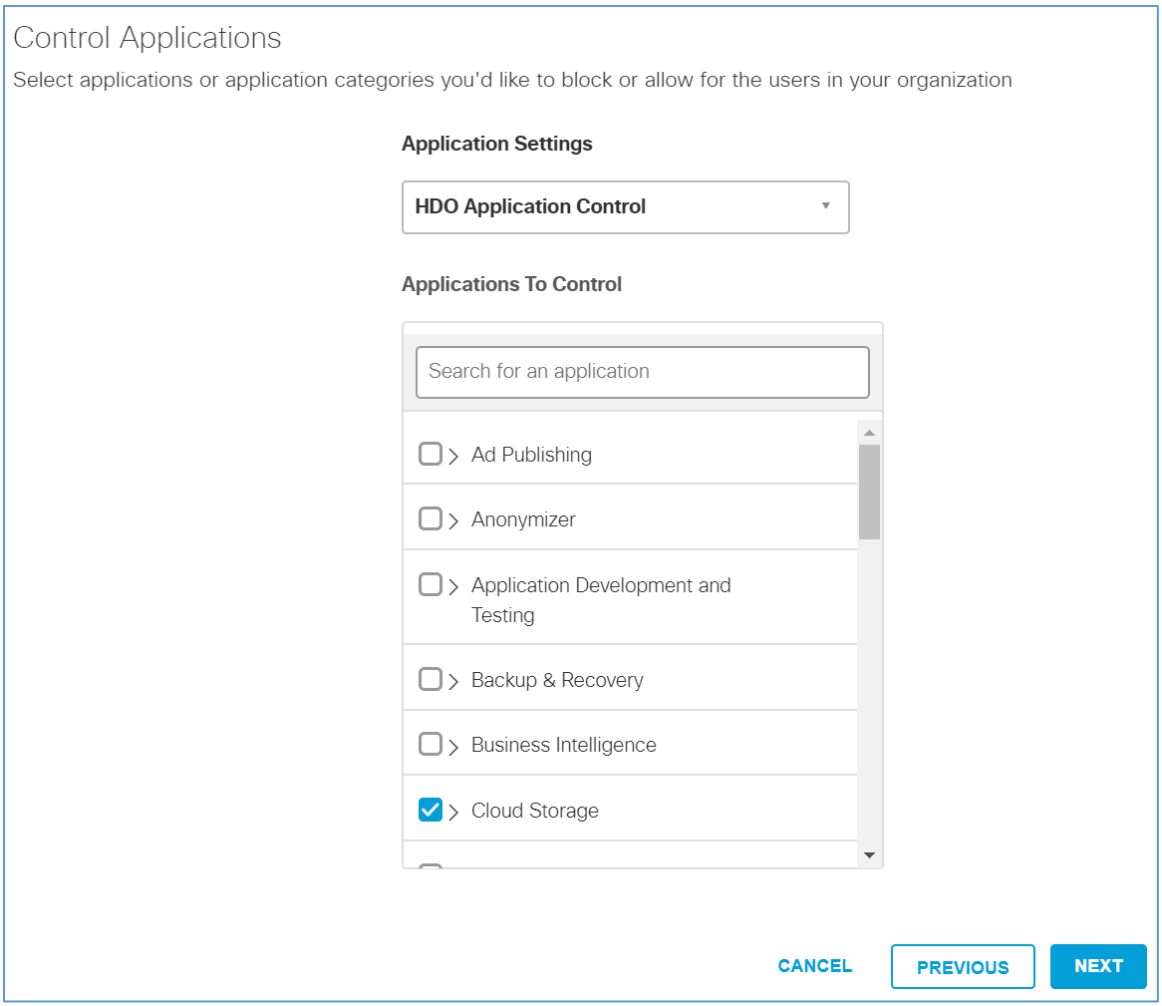
a. **Name:** HDO Application Control

b. **Applications to Control:** Cloud Storage

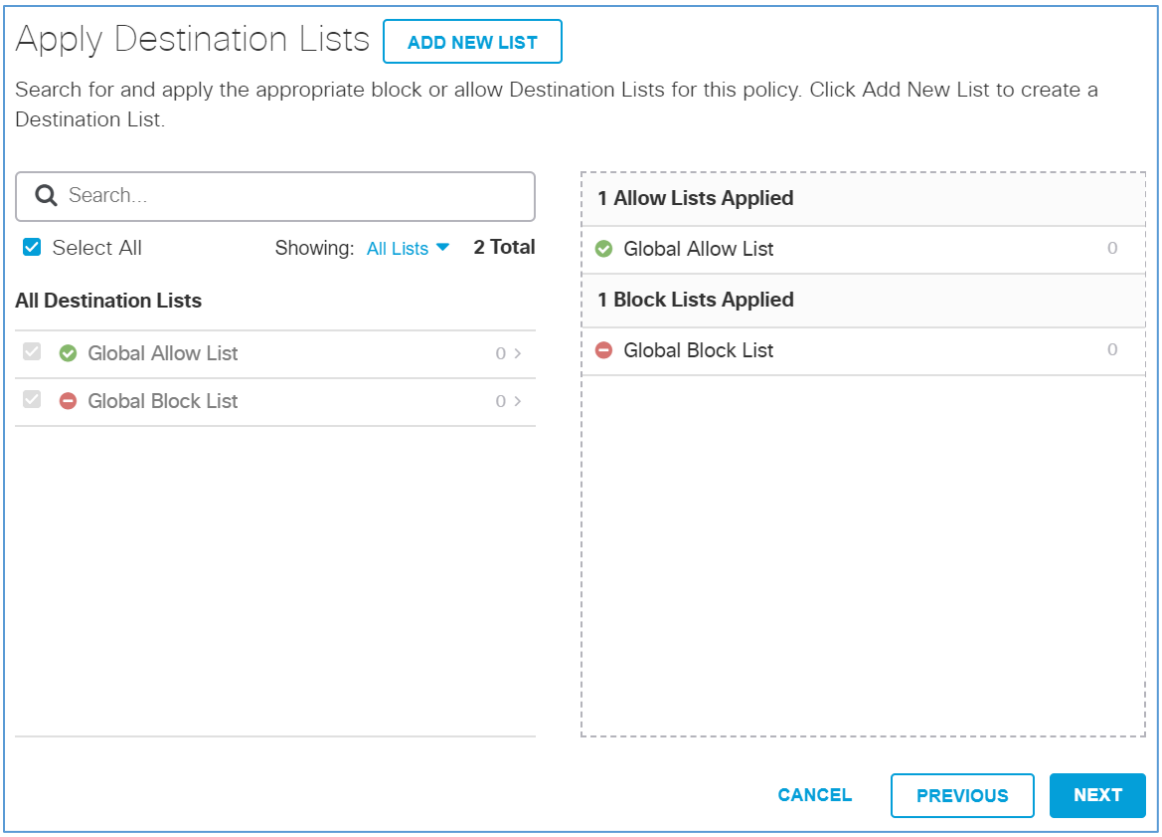
12. Click **Save.**



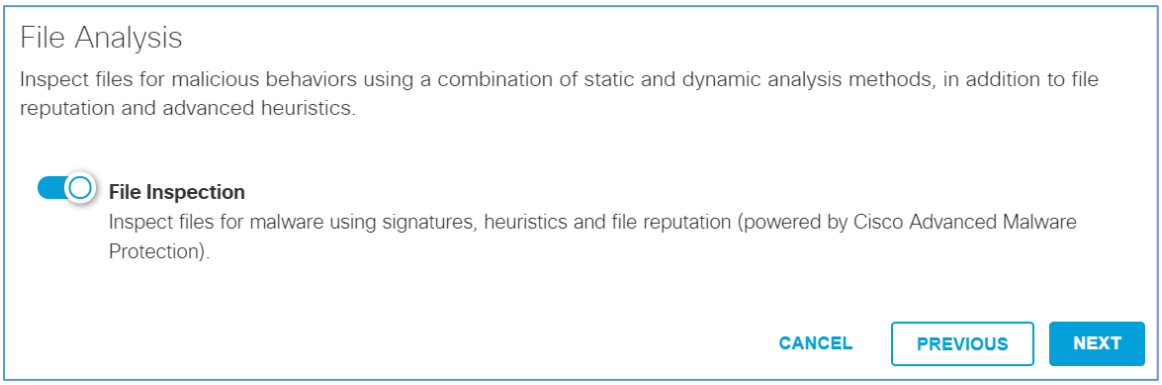
13. Click **Next.**



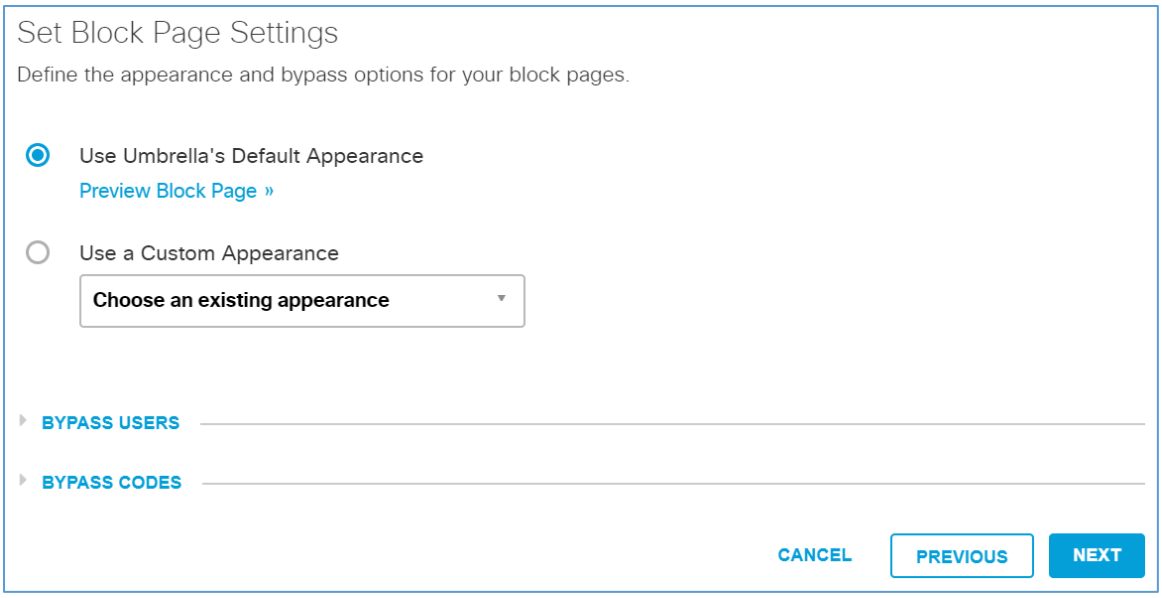
14. Click **Next.**



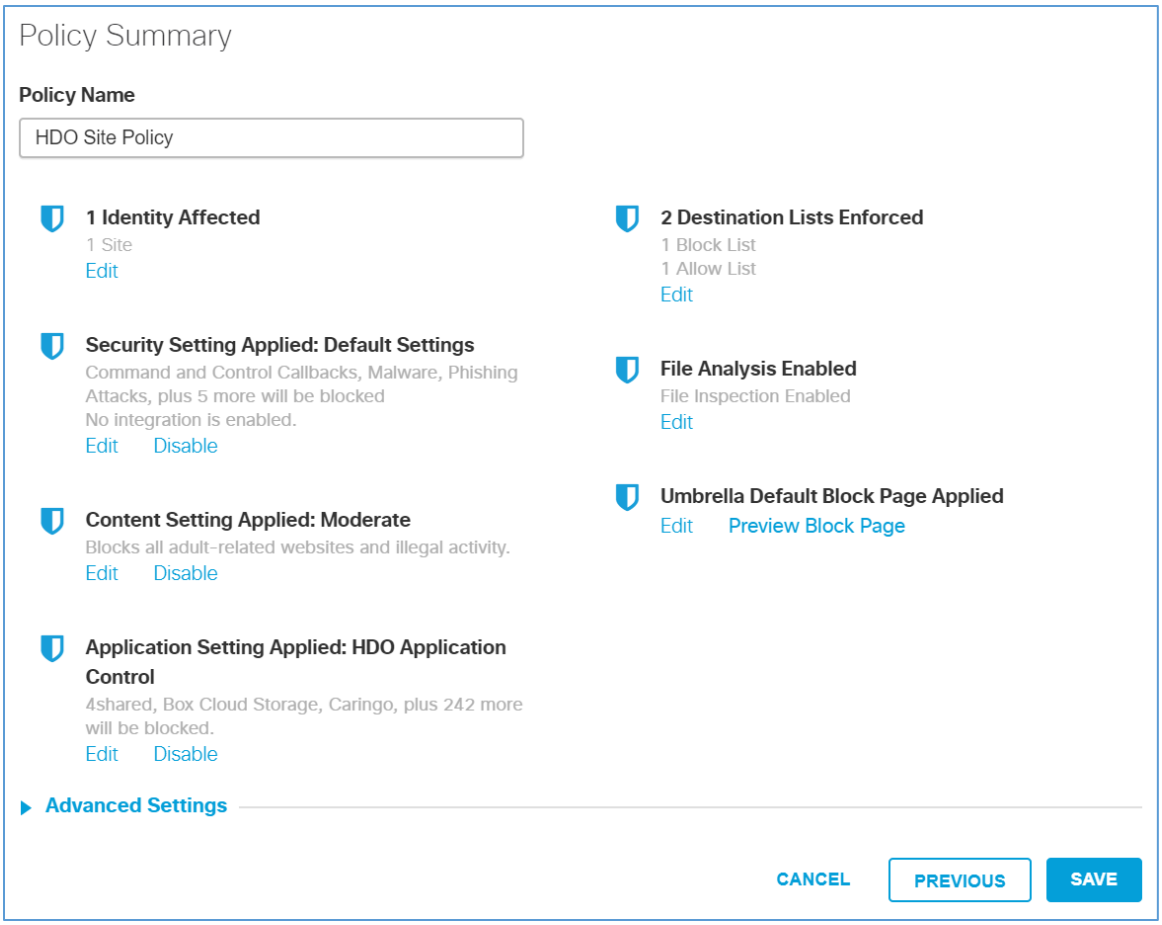
1007 15. Click **Next.**



1008 16. Click **Next.**

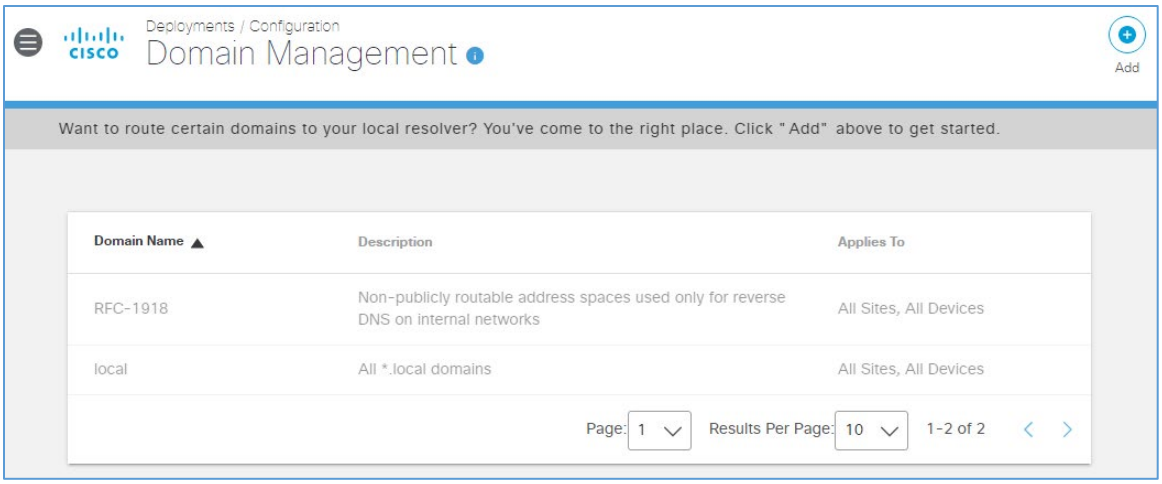


17. In the Policy Summary screen, set the **Name** to **HDO Site Policy.**
18. Click **Save.**

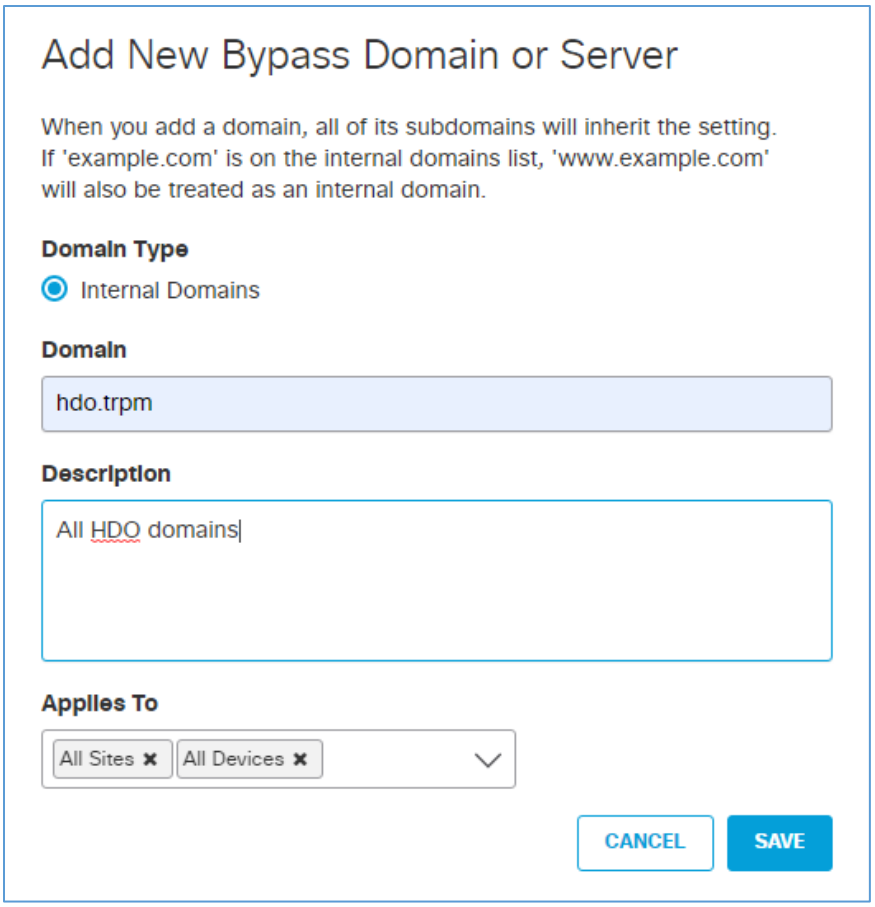


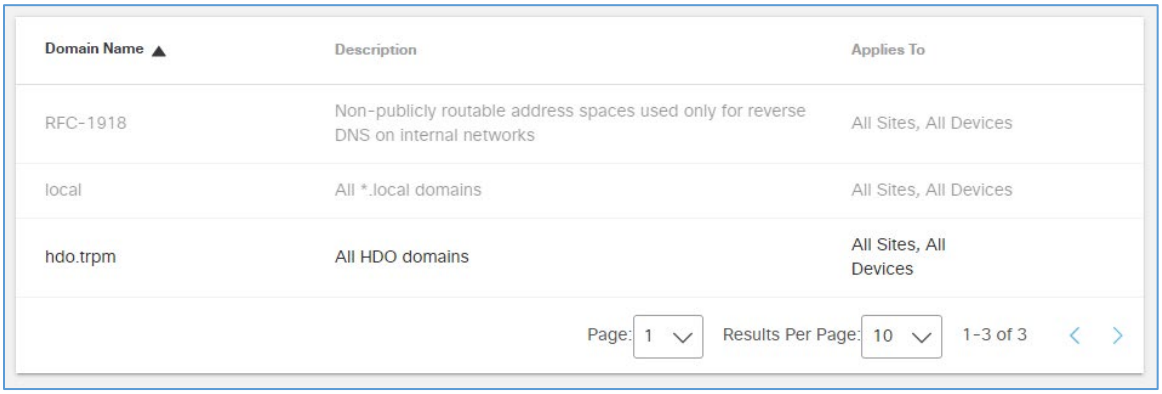
Configure Windows Domain Controller as the Local DNS Provider

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.





1018 *2.2.3.3 LogRhythm XDR (Extended Detection and Response)*

1019 LogRhythm XDR is a SIEM system that receives log and machine data from multiple end points and
1020 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

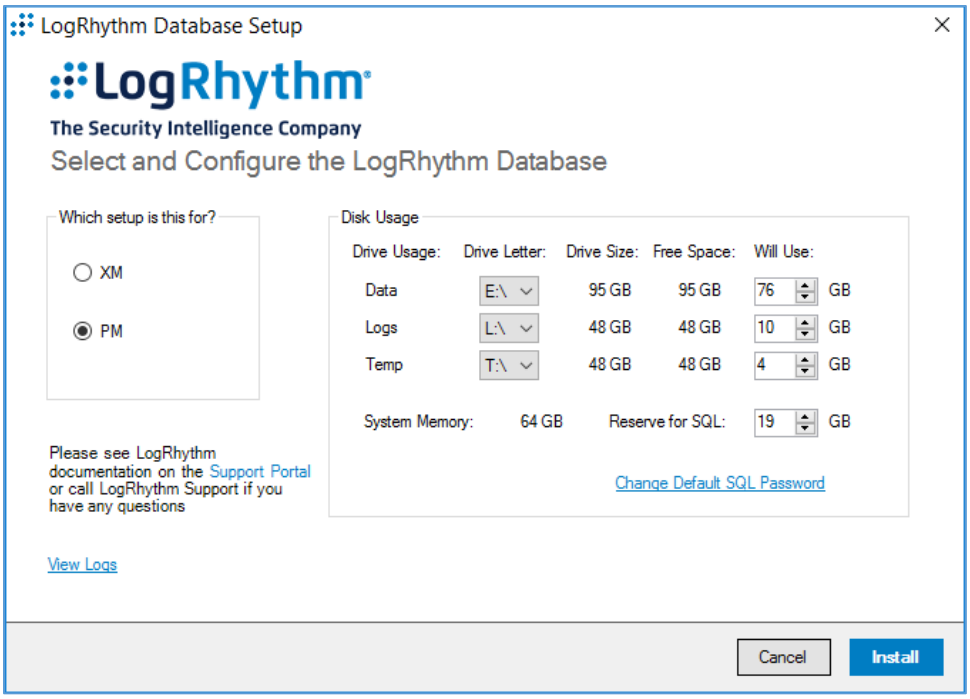
This section describes LogRhythm installation processes.

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**.



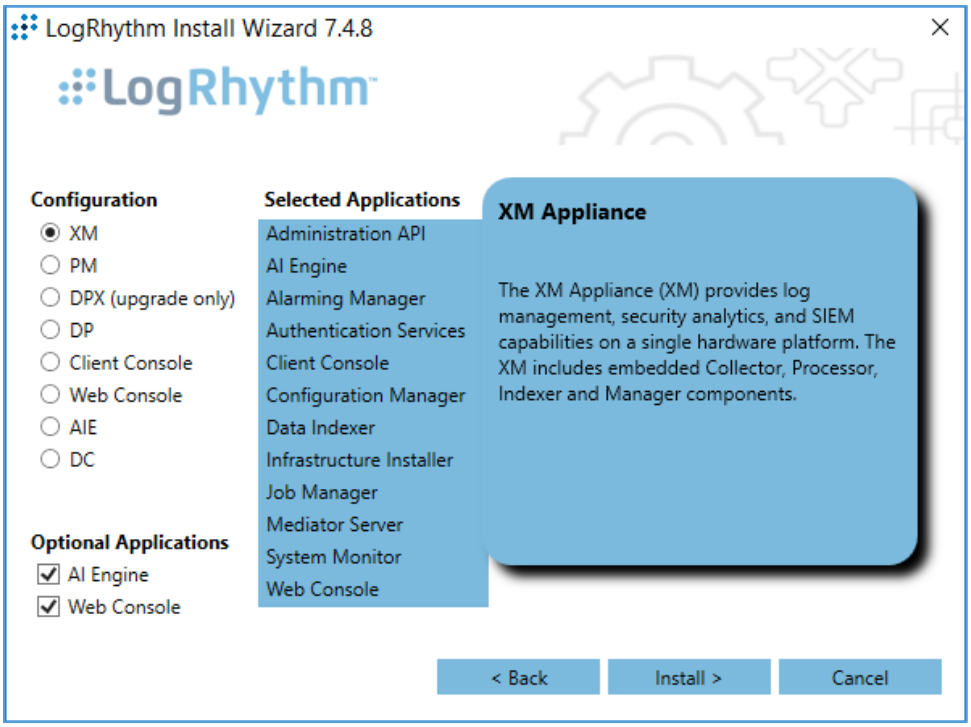
5. The remaining fields will automatically populate with the appropriate values. Click **Install.**
6. Click **Done** to close the **LogRhythm Database Setup** window.

Install LogRhythm XDR

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.

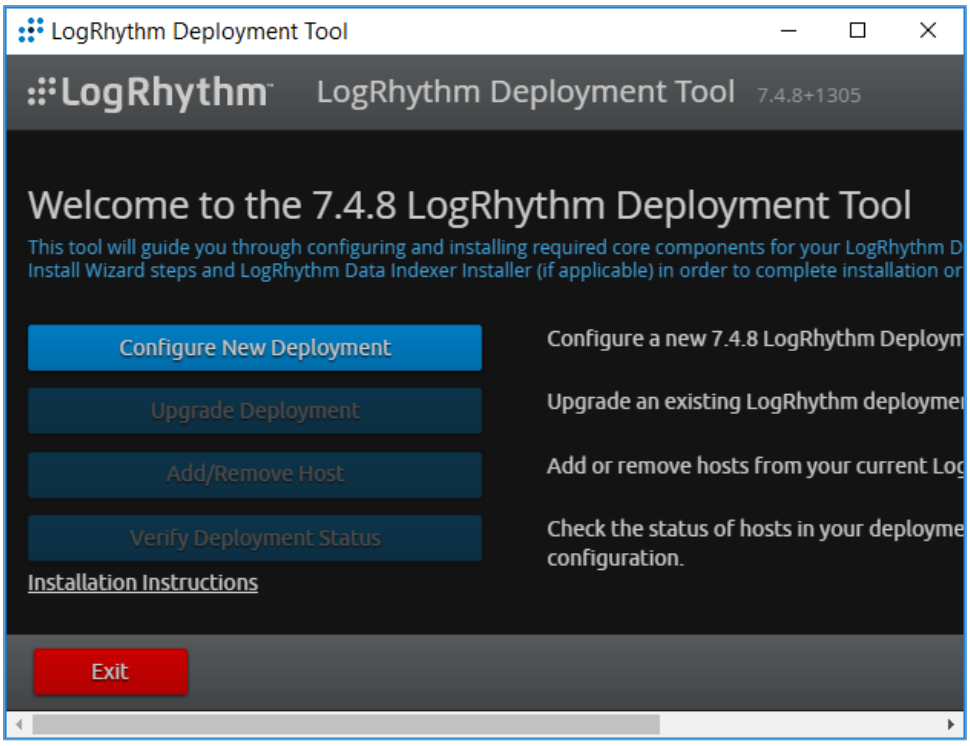
b. **Optional Applications:** Check both **AI Engine** and **Web Console** boxes.

10. Click **Install.**

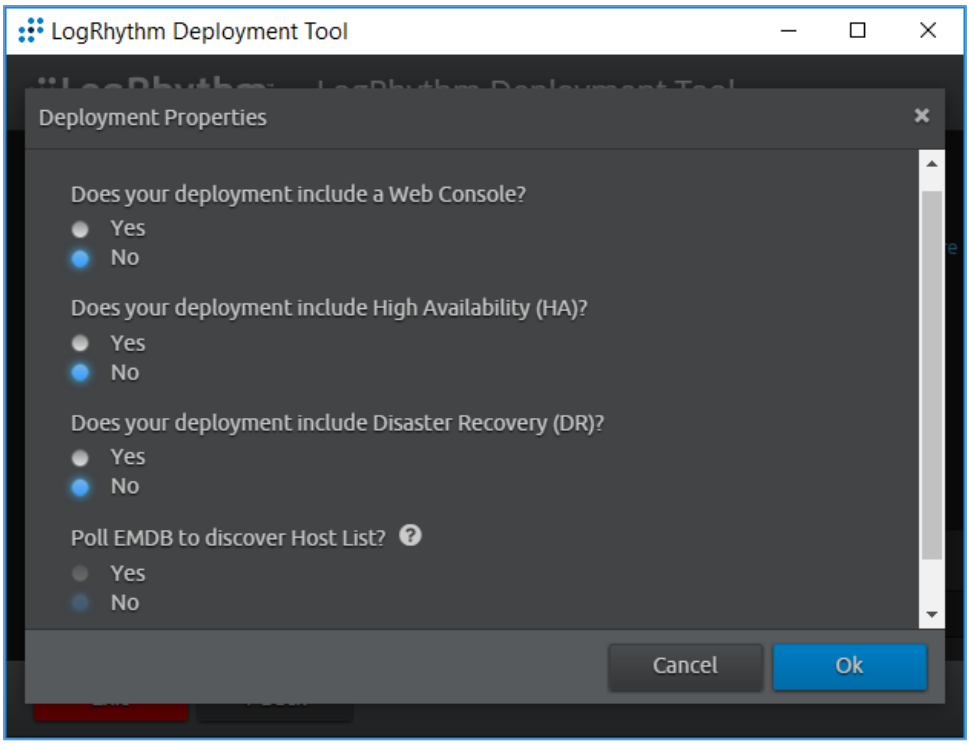


11. A **LogRhythm Deployment Tool** window displays.

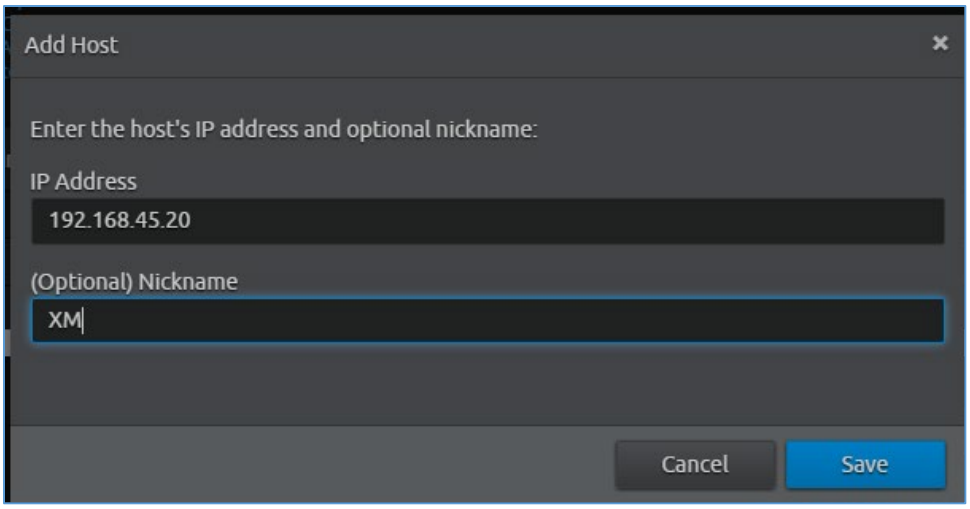
12. Click **Configure New Deployment.**



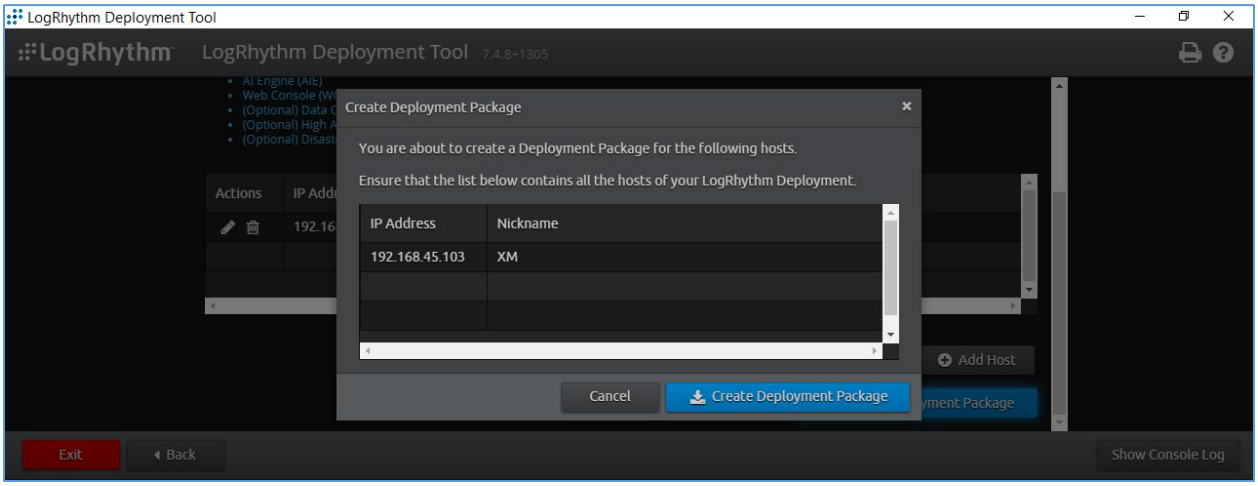
1065 13. In the **Deployment Properties window,** keep the default configurations and click **Ok.**



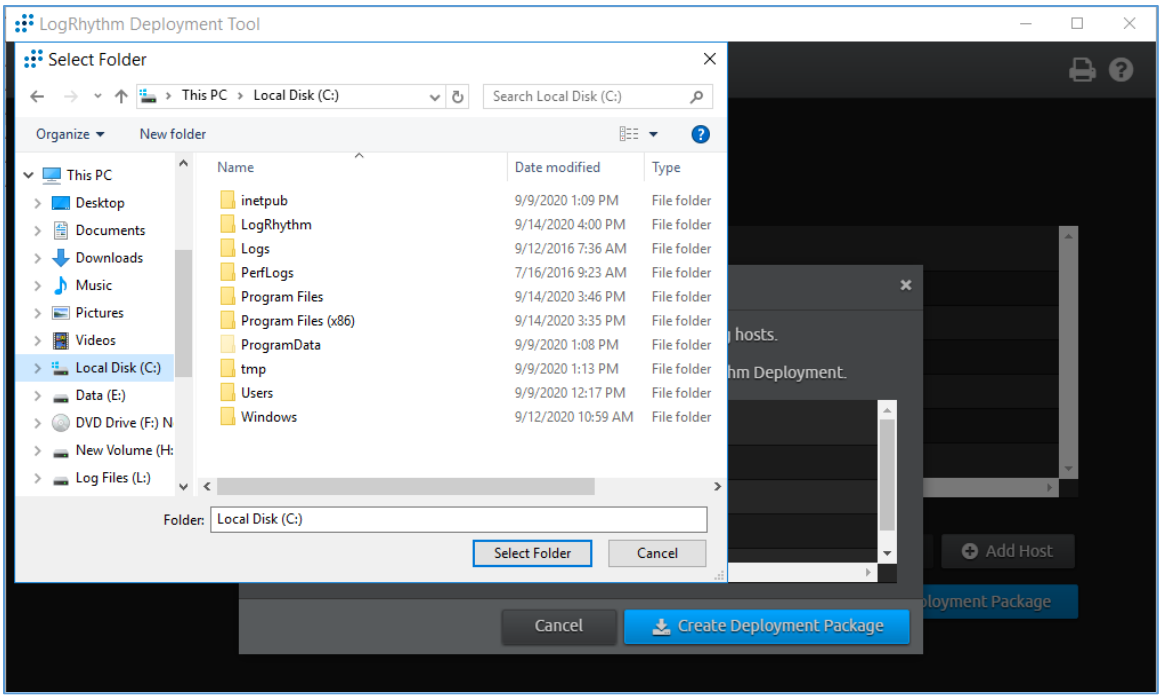
14. Click **+Add Host IP** in the bottom right corner of the screen, and provide the following information:
    a. **IP Address:** 192.168.45.20
    b. **Nickname:** XM
15. Click **Save.**



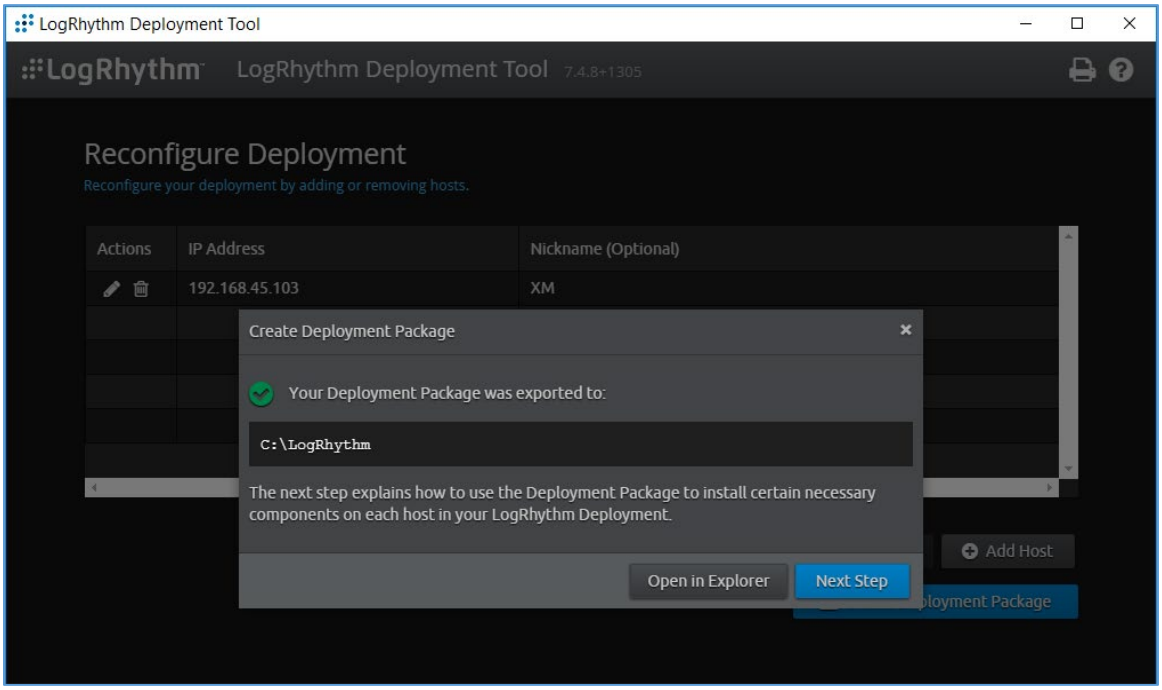
16. Click **Create Deployment Package** in the bottom right corner of the screen.
17. A **Create Deployment Package** window displays.
18. Click **Create Deployment Package.**



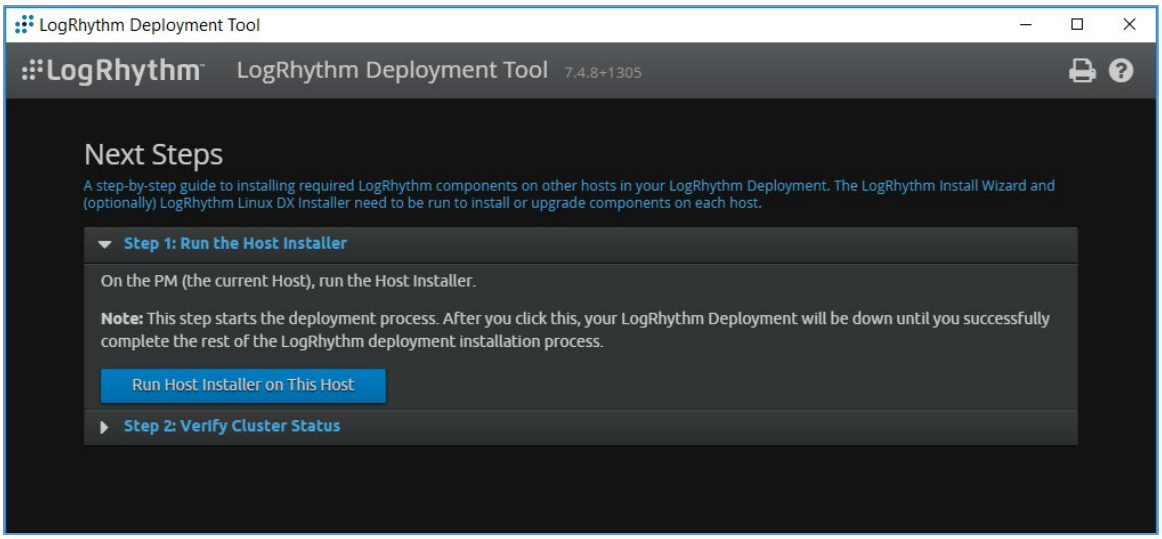
19. A Select Folder window appears.
20. Navigate to ***C:\LogRhythm.***
21. Click **Select Folder.**



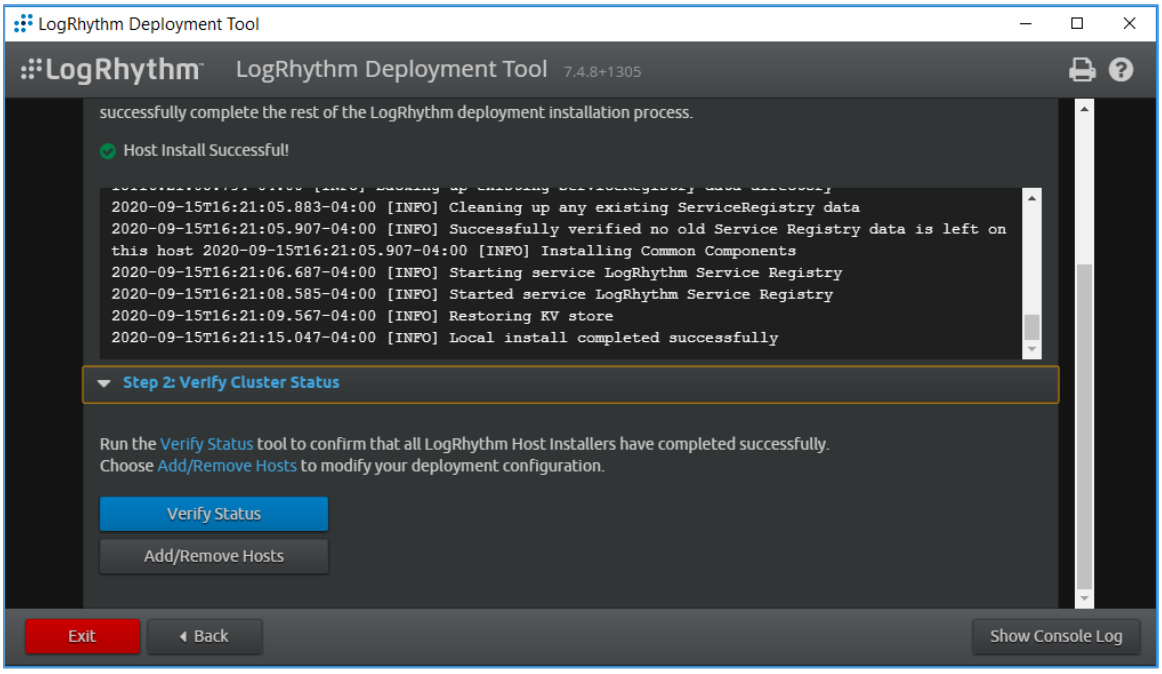
1077 22. Click **Next Step.**



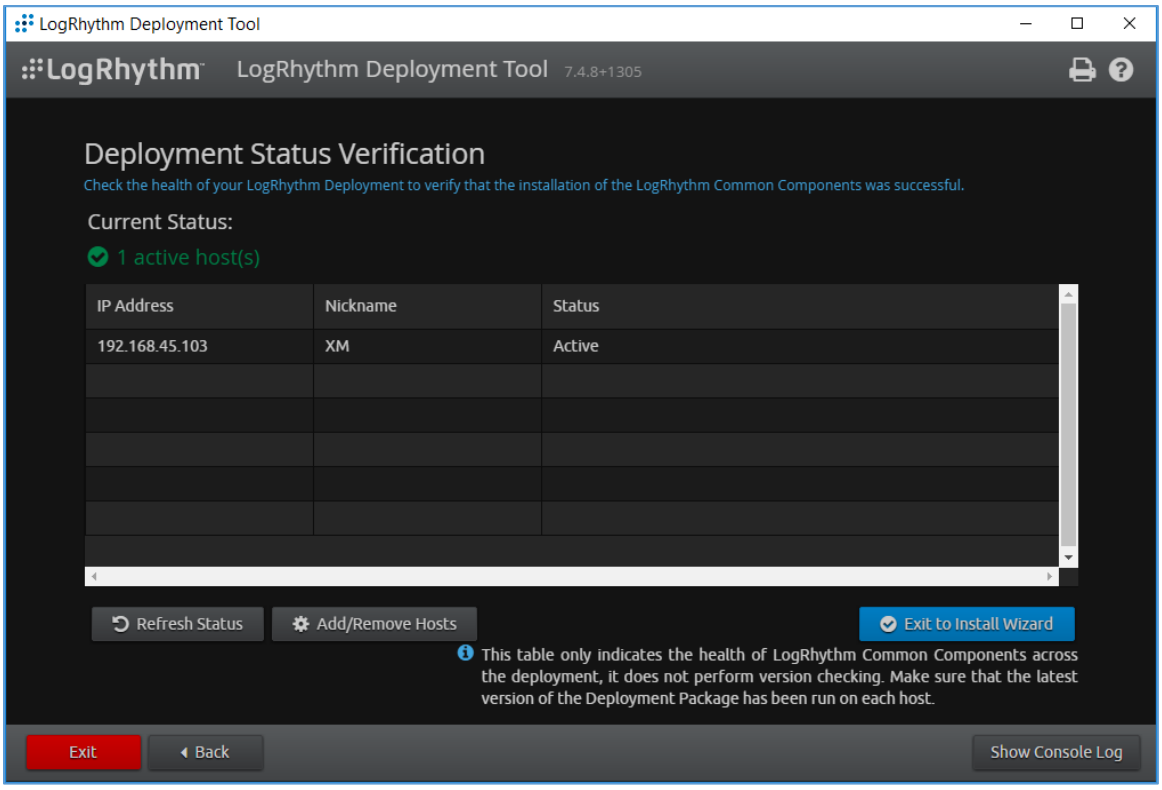
1078 23. Click **Run Host Installer on this Host.**



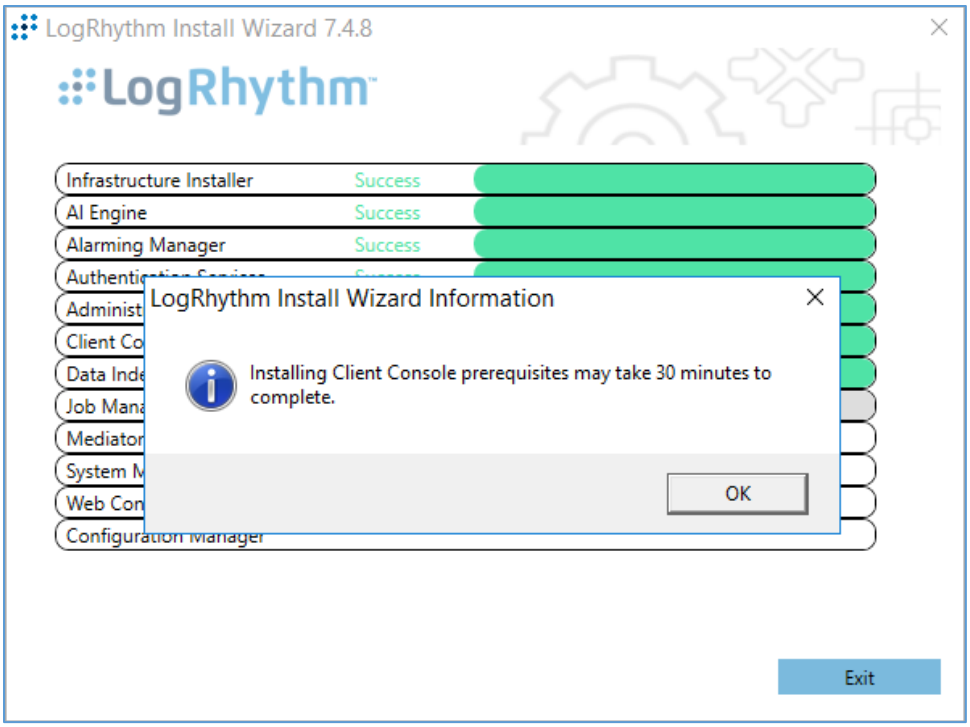
1079 24. After the Host Installer has finished, click **Verify Status.**



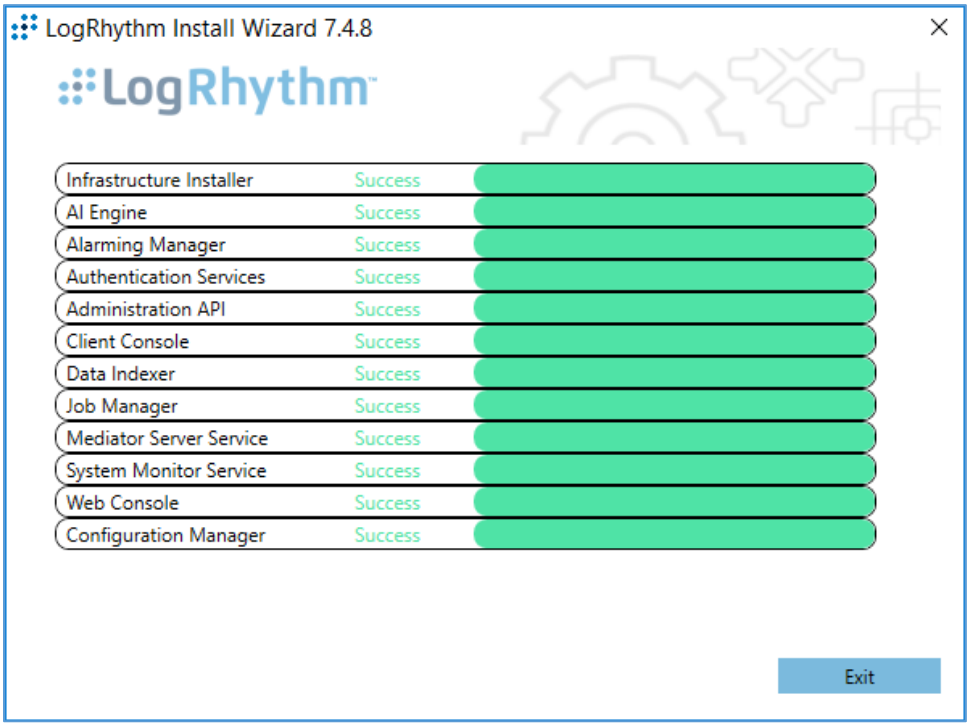
1080 25. Click **Exit to Install Wizard.**



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.**



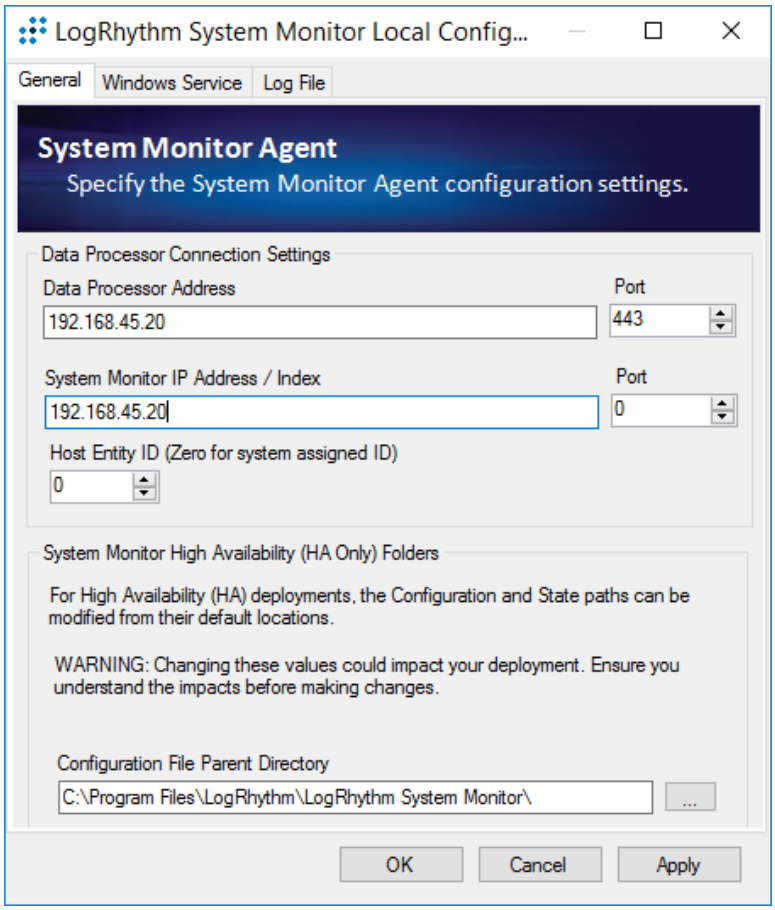
LogRhythm XDR Configuration

The LogRhythm XDR configuration includes multiple related components:

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

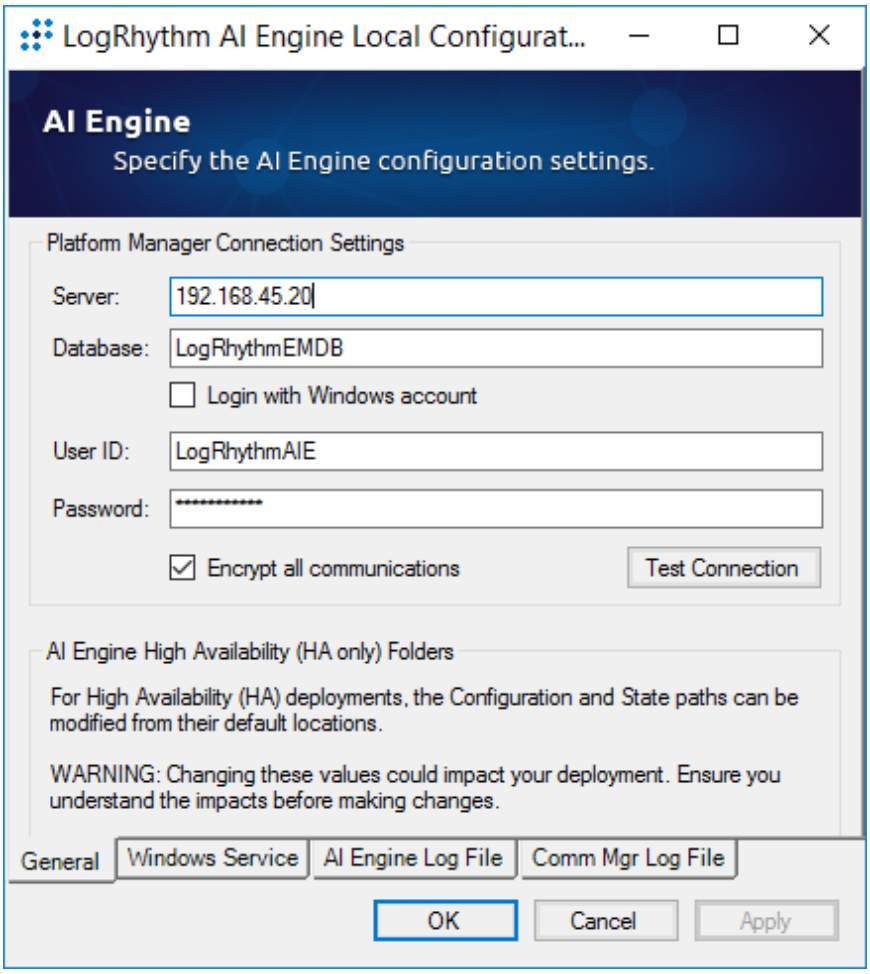
Configure System Monitor

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.**



Configure LogRhythm AI Engine

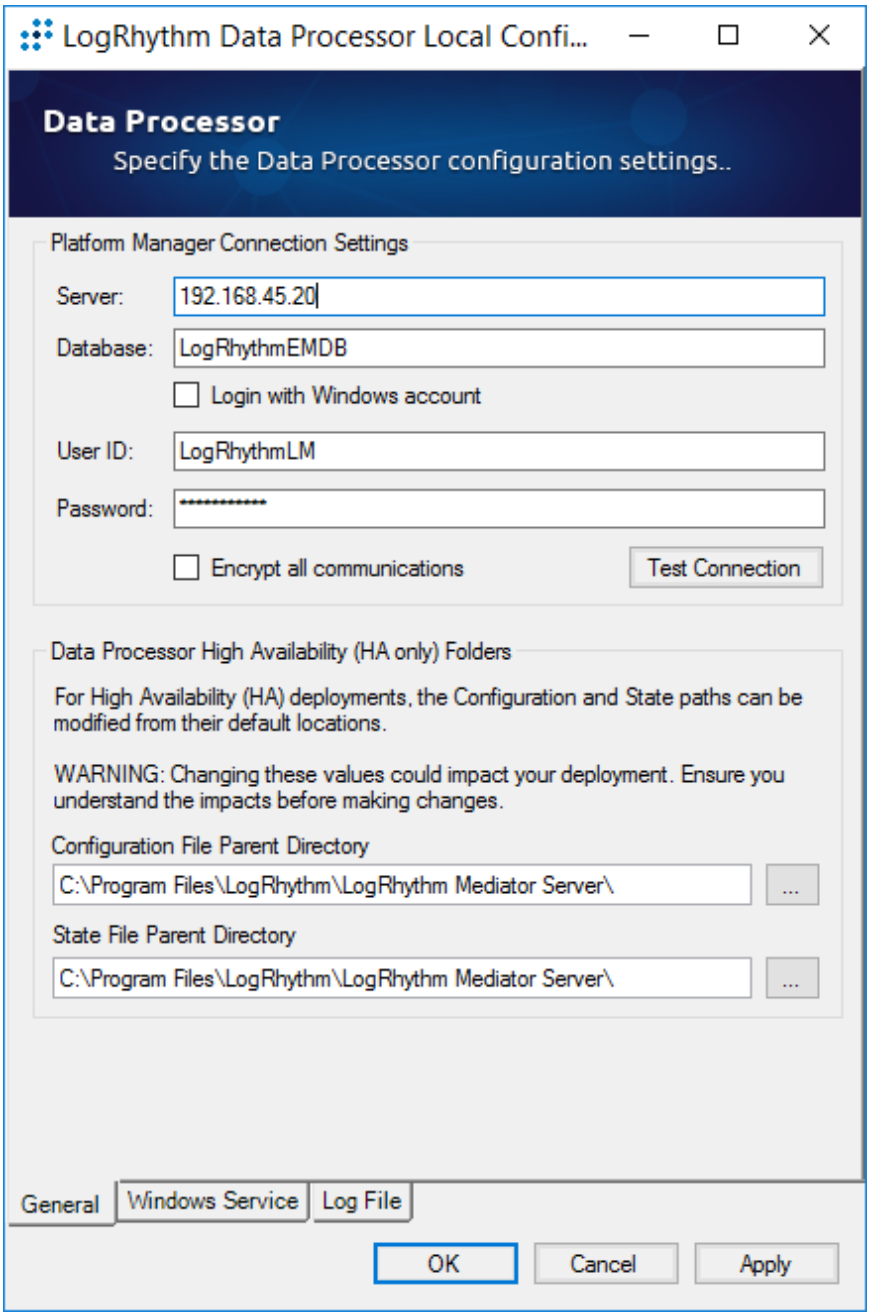
1. Open **File Explorer,** and navigate to ***C:\Program Files\LogRhythm.***
2. Navigate to **LogRhythm AI Engine.**
3. Double-click the ***lrconfig*** application file.
4. In the **LogRhythm AI Engine Local Configuration Manager** window, provide the following information, and leave the remaining fields 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.**



Configure Mediator Server

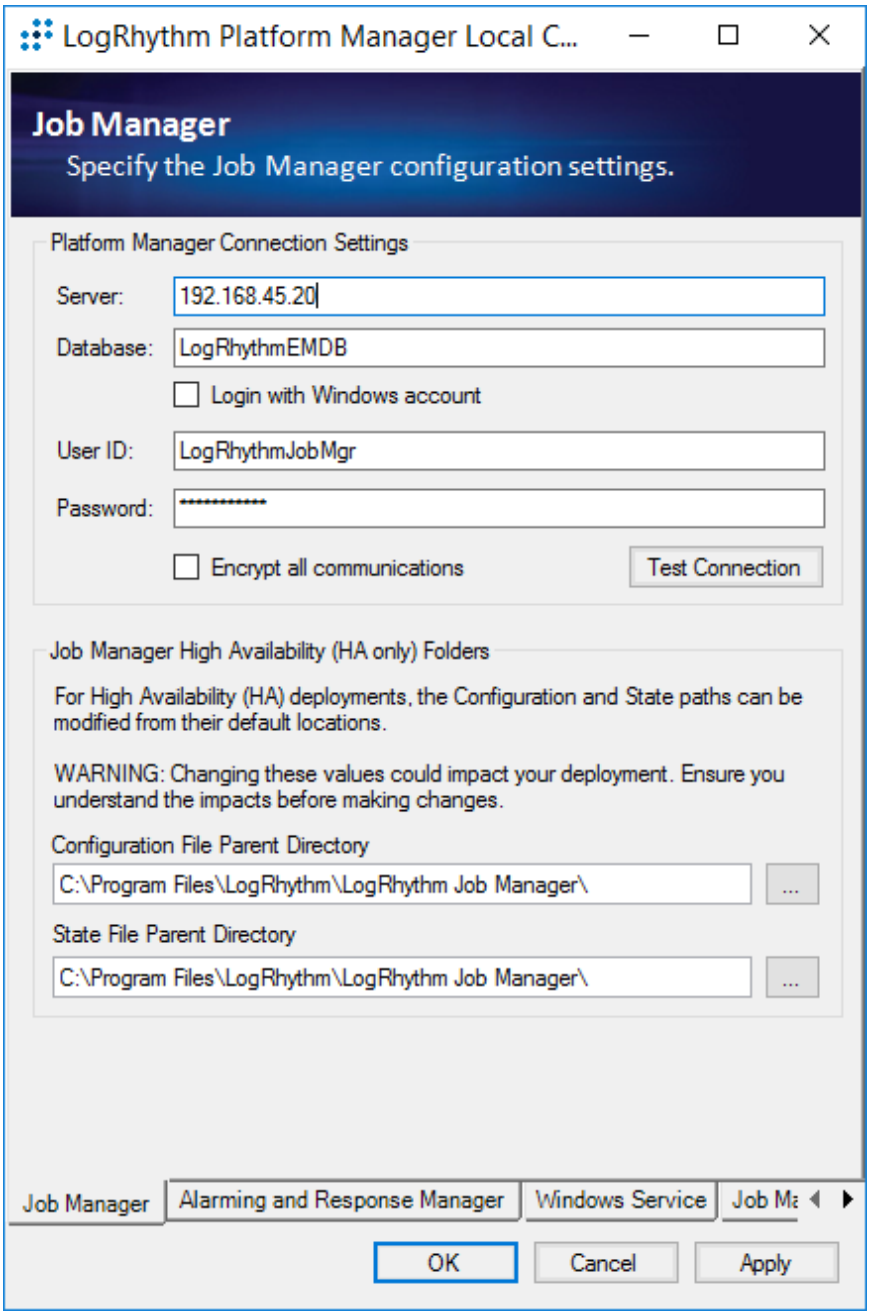
1. Open File Explorer, and navigate to ***C:\Program Files\LogRhythm.***
2. Navigate to **Mediator Server.**
3. Double-click ***lrconfig*** application file.
4. In the **LogRhythm Data Processor Local Configuration Manager** window, provide the following information, and leave the remaining fields as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

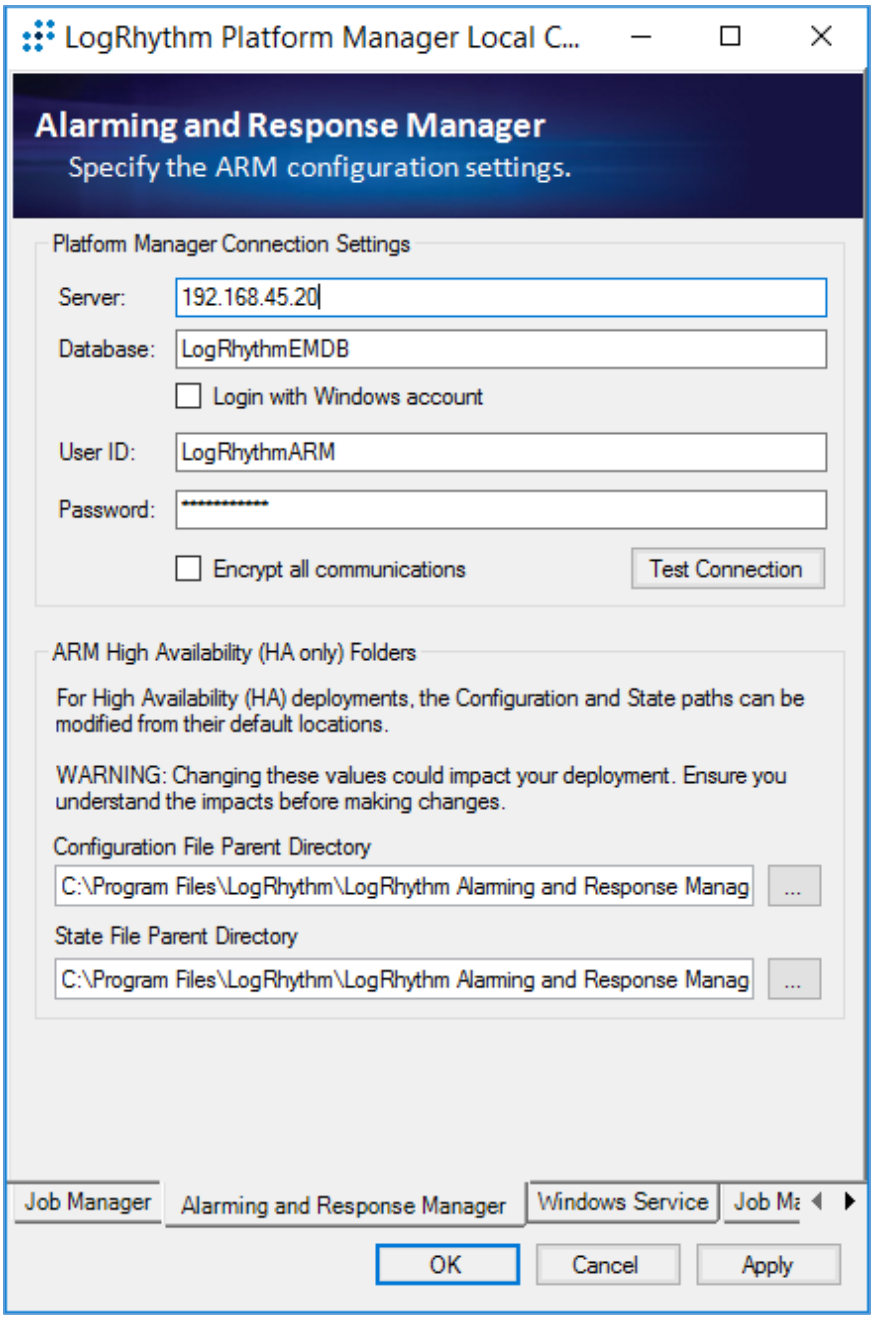


7. Navigate to the **Alarming and Response Manager** tab in the bottom menu ribbon.
8. In the **Alarming and Response Manager** window, provide the following information, and leave the remaining fields as their default values:
    a. **Server:** 192.168.45.20

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

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

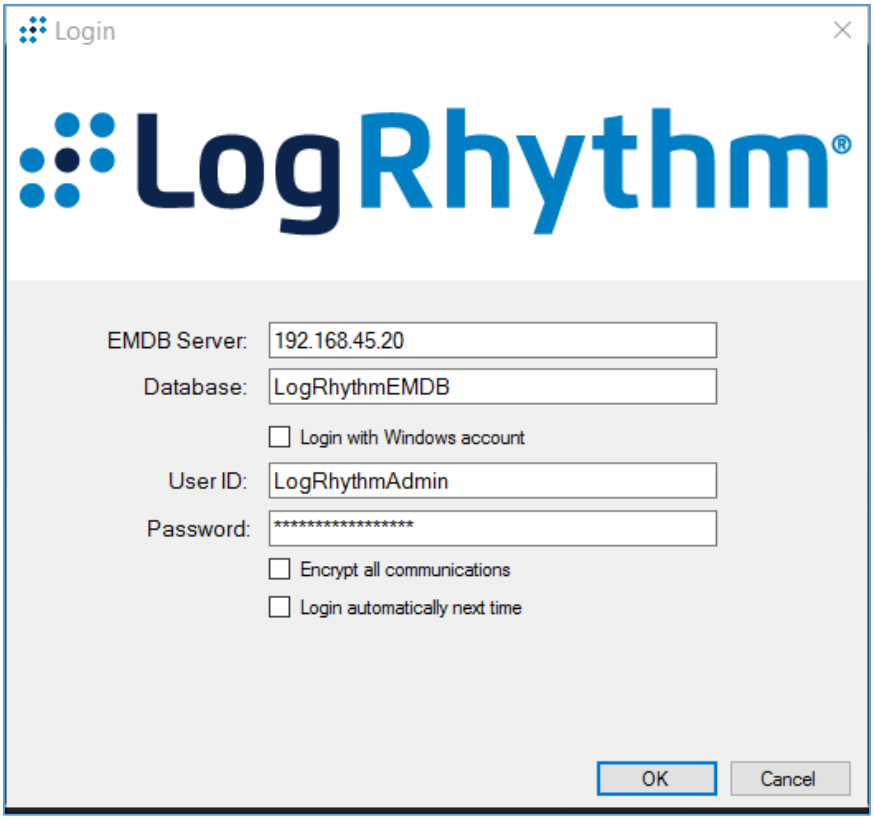
10. Click **Apply,** and then click **OK.**



Configure LogRhythm Console

1. Open File Explorer and navigate to ***C:\Program Files\LogRhythm.***
2. Navigate to **LogRhythm Console.**

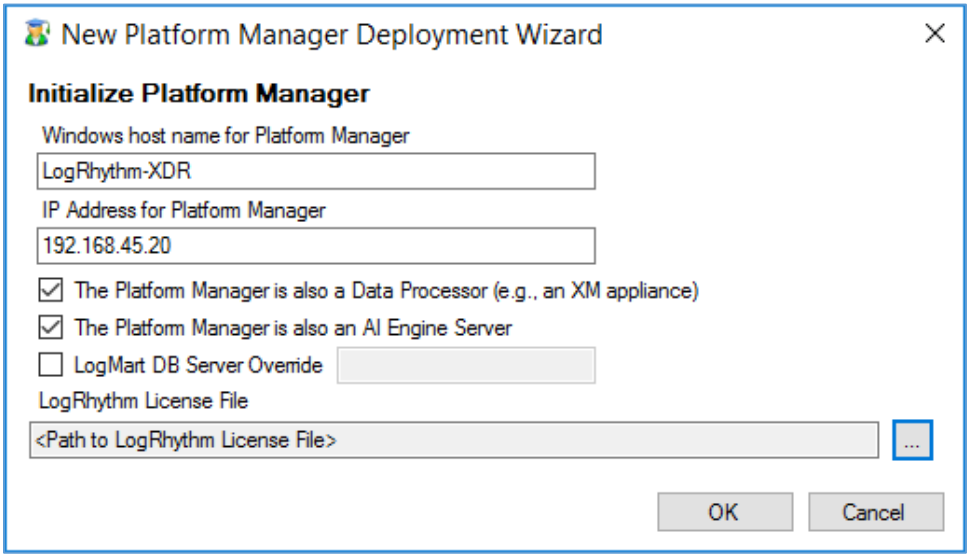
3. Double-click ***lrconfig*** application file.
4. In the LogRhythm Login window, provide the following information:
    a. **EMDB Server:** 192.168.45.20
    b. **UserID:** LogRhythmAdmin
    c. **Password:** ********
5. Click **OK.**



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.



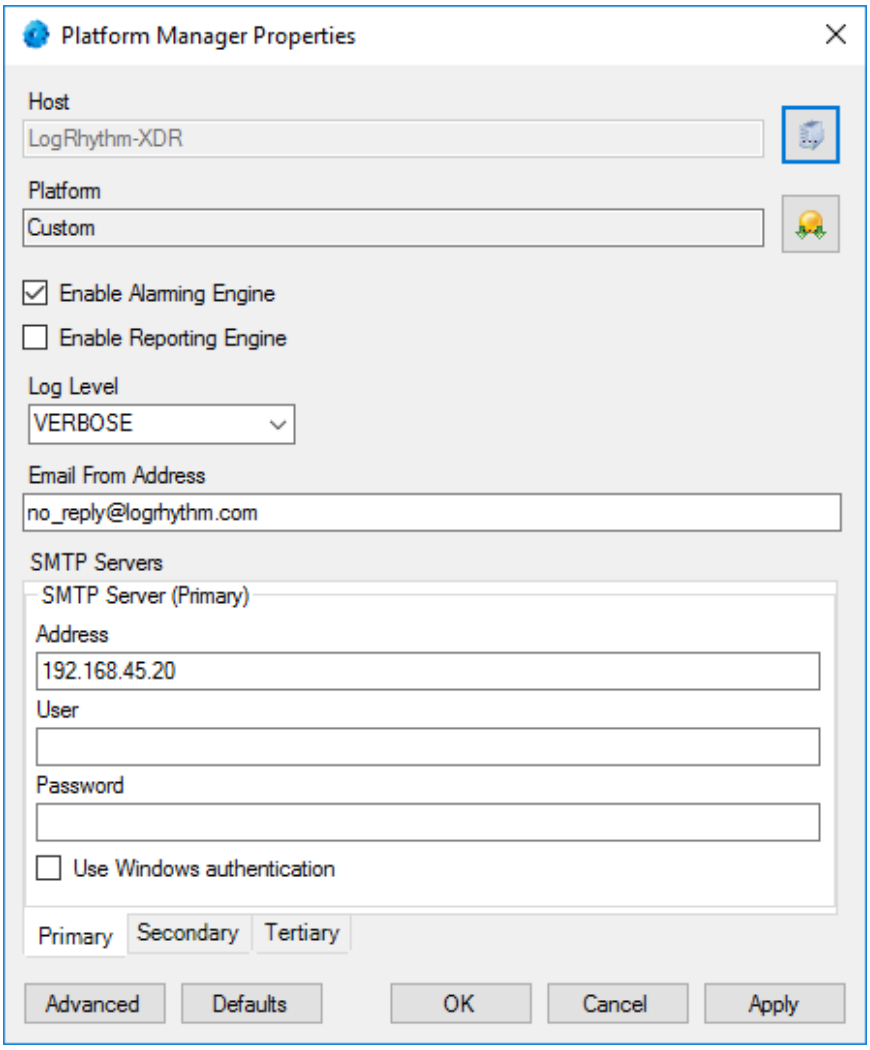
8. The New Knowledge Base Deployment Wizard window displays and shows the import progress status. Once LogRhythm has successfully imported the file, a message window will appear stating more configurations need to be made for optimum performance. Click **OK** to open the **Platform Manager Properties**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

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

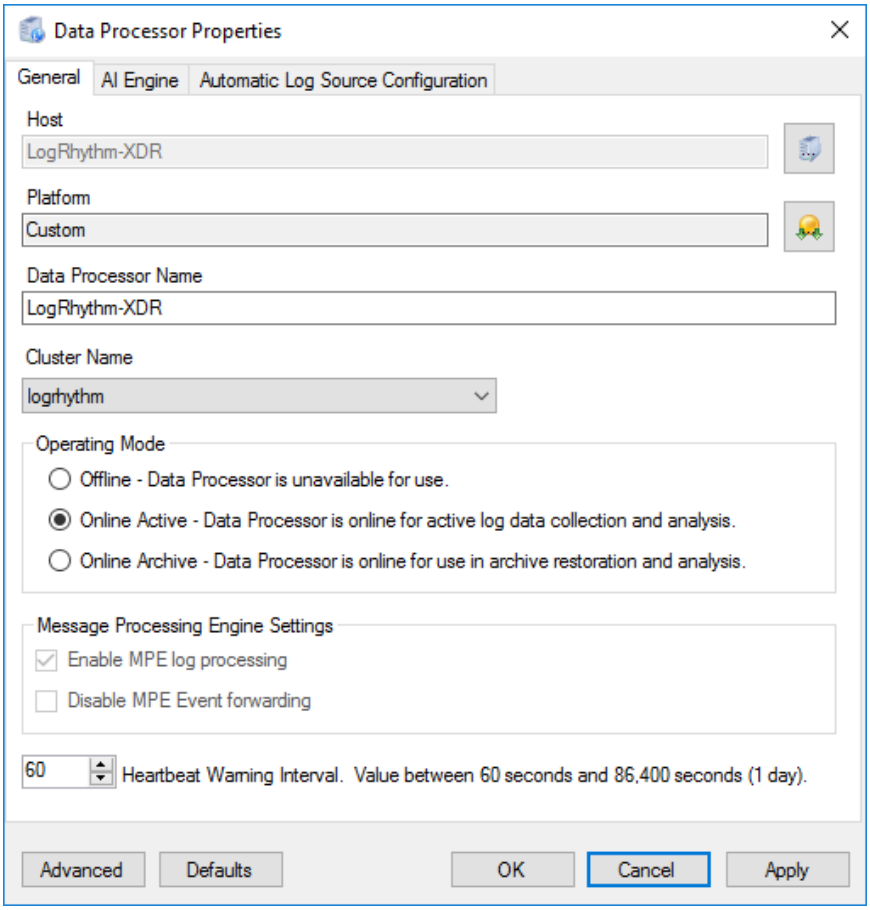
   a. **Email address:** no_reply@logrhythm.com

   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.**

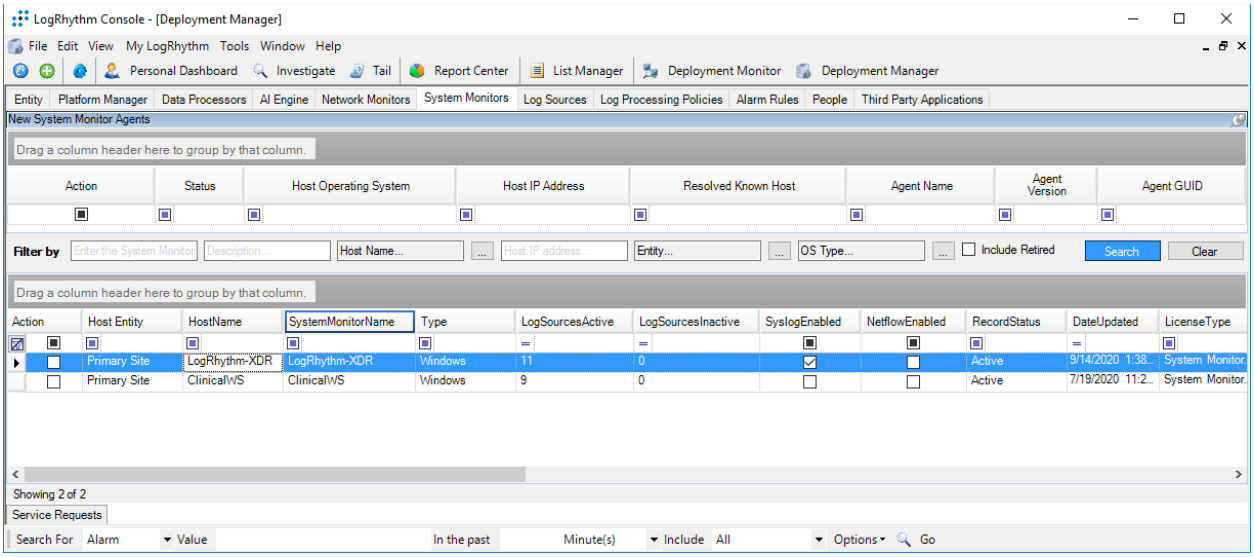


11. After the Platform Manager Properties window closes, a message window displays for configuring the Data Processor. Click **OK** to open the **Data Processor Properties** window.
12. Click the button next to **Platform,** and enable the **Custom Platform** radio button.
13. Click **OK.**
14. Leave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



Set LogRhythm-XDR for System Monitor

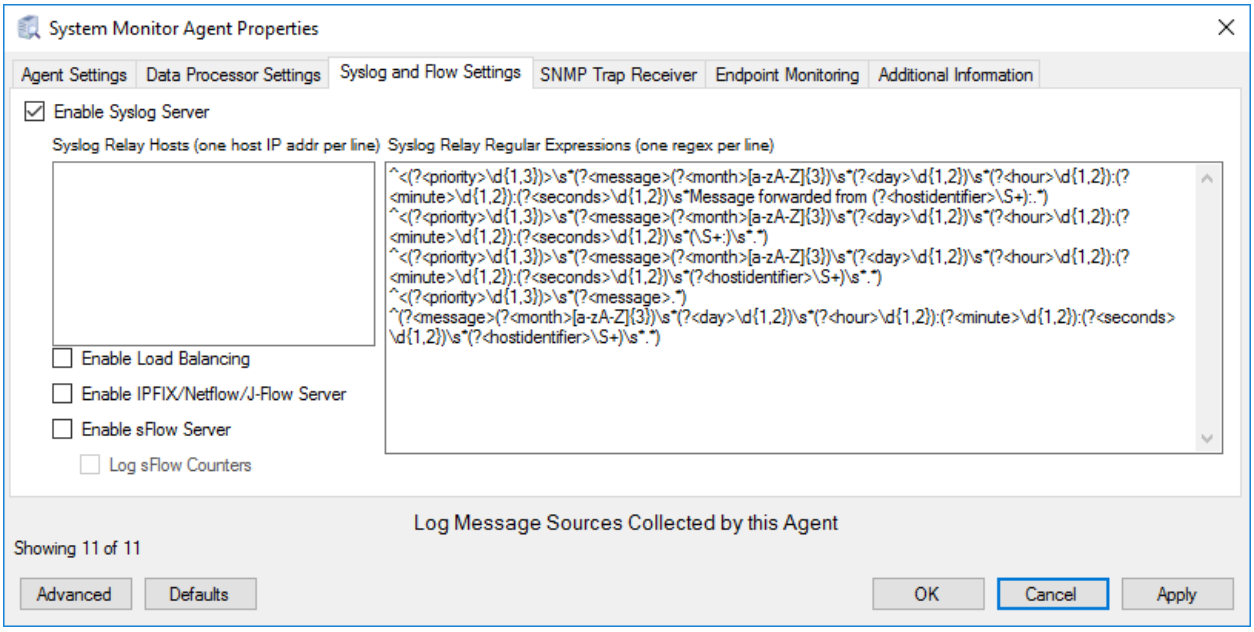
1. Back in the LogRhythm console, navigate to the **Deployment Manager** tab in the menu ribbon.
2. Navigate to **System Monitors** on the Deployment Manager menu ribbon.
3. Double-click **LogRhythm-XDR.**



1179 4. In the **System Monitor Agent Properties** window, navigate to **Syslog and Flow Settings.**

1180 5. Click the checkbox beside **Enable Syslog Server.**

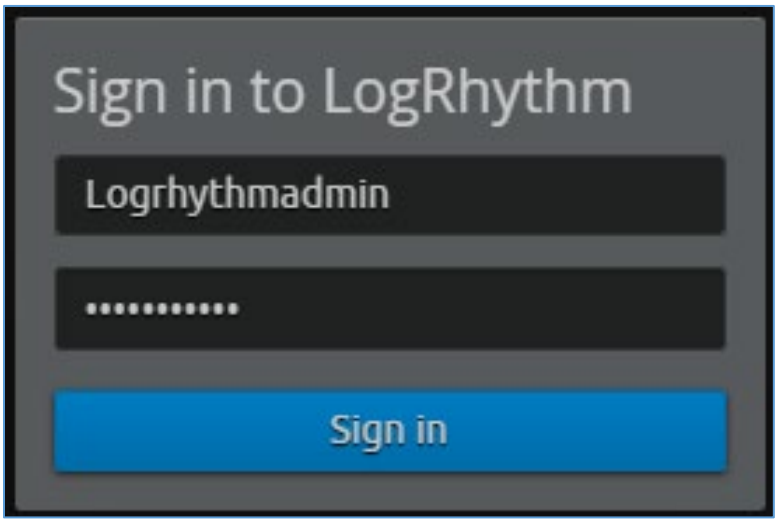
1181 6. Click **OK** to close the System Monitor Agent Properties window.



1182 **Use the LogRhythm Web Console**

1183 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

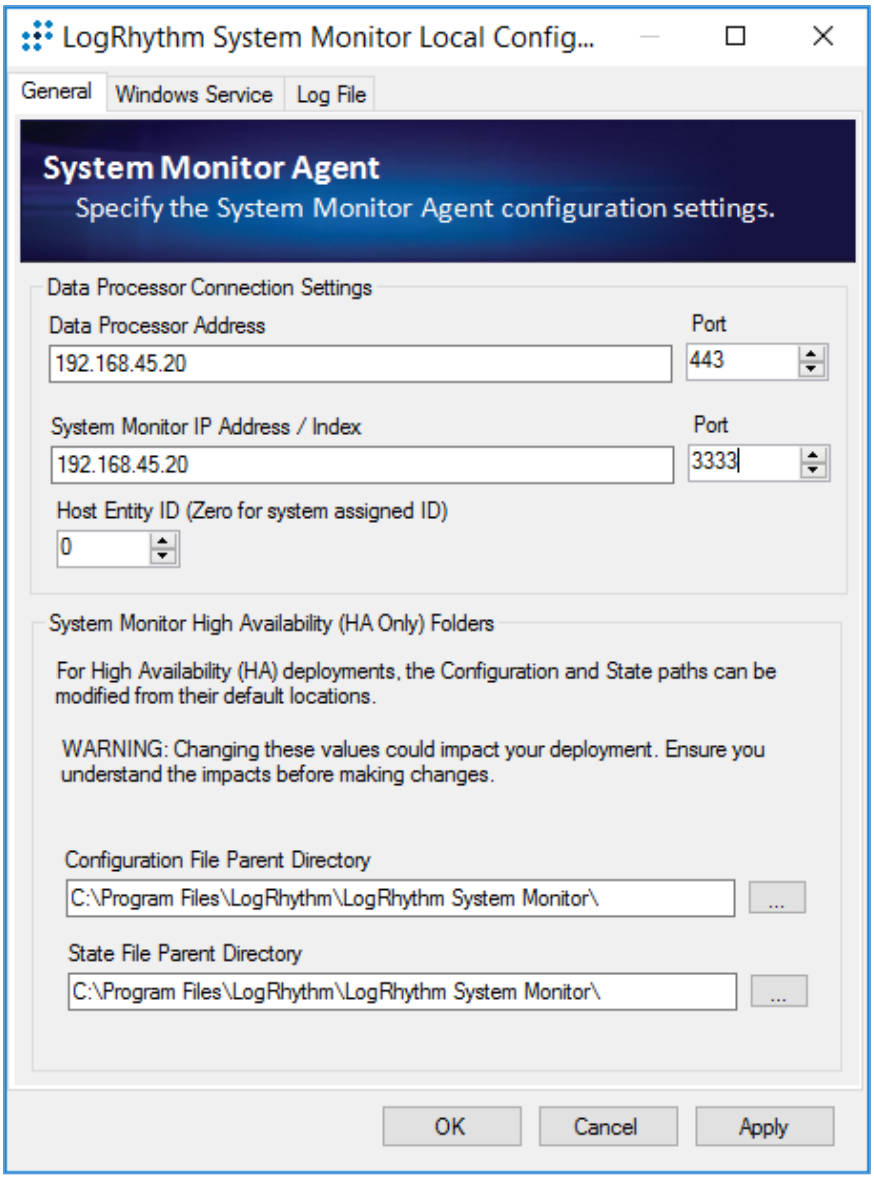
1. Open a new tab in the web browser, and navigate to https://community.logrhythm.com.
2. Log in using the appropriate credentials.
3. Click **LogRhythm Community.**
4. Navigate to **Documentation & Downloads.**
5. Register a **Username.**
6. Click **Accept.**
7. Click **Submit.**
8. Navigate to **NetMon.**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

Install LogRhythm NetworkXDR

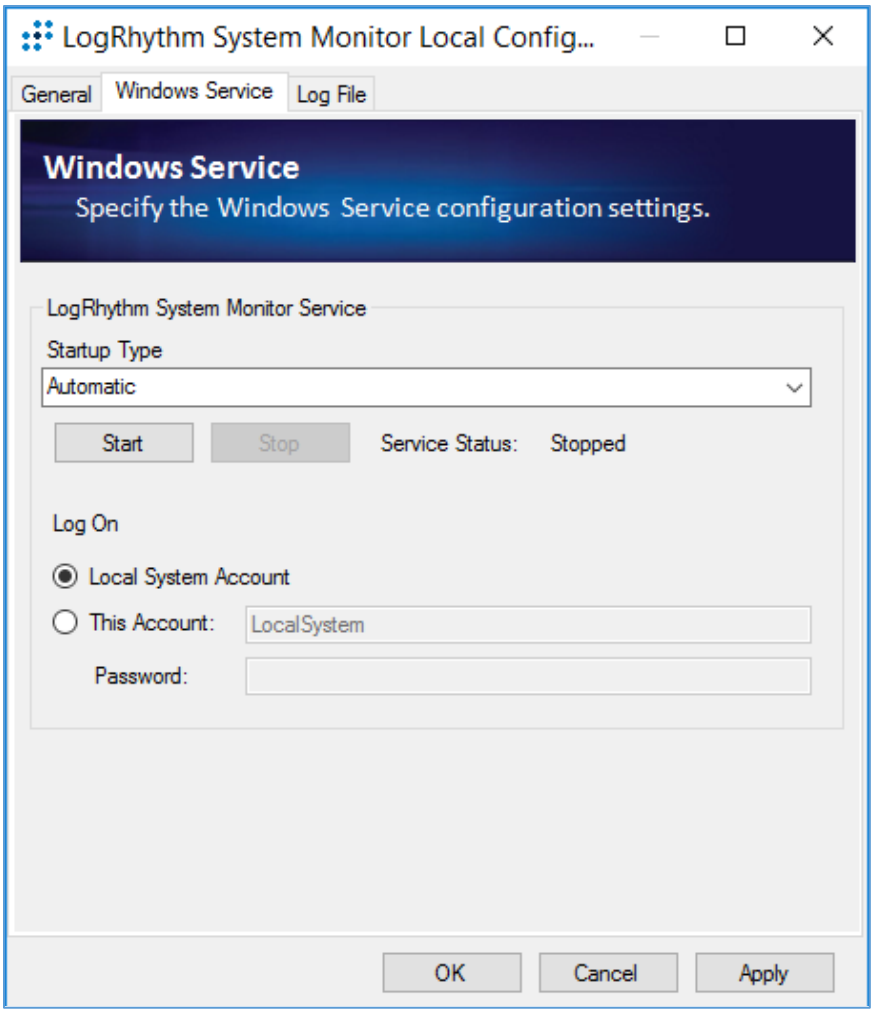
1. In the host server, mount the *.iso* for the installation.
2. Start the VM with the mounted *.iso*.
3. When the welcome screen loads, select **Install LogRhythm Network Monitor.**
4. The installer completes the installation, and the system reboots.
5. When the system reboots, log in to the console 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

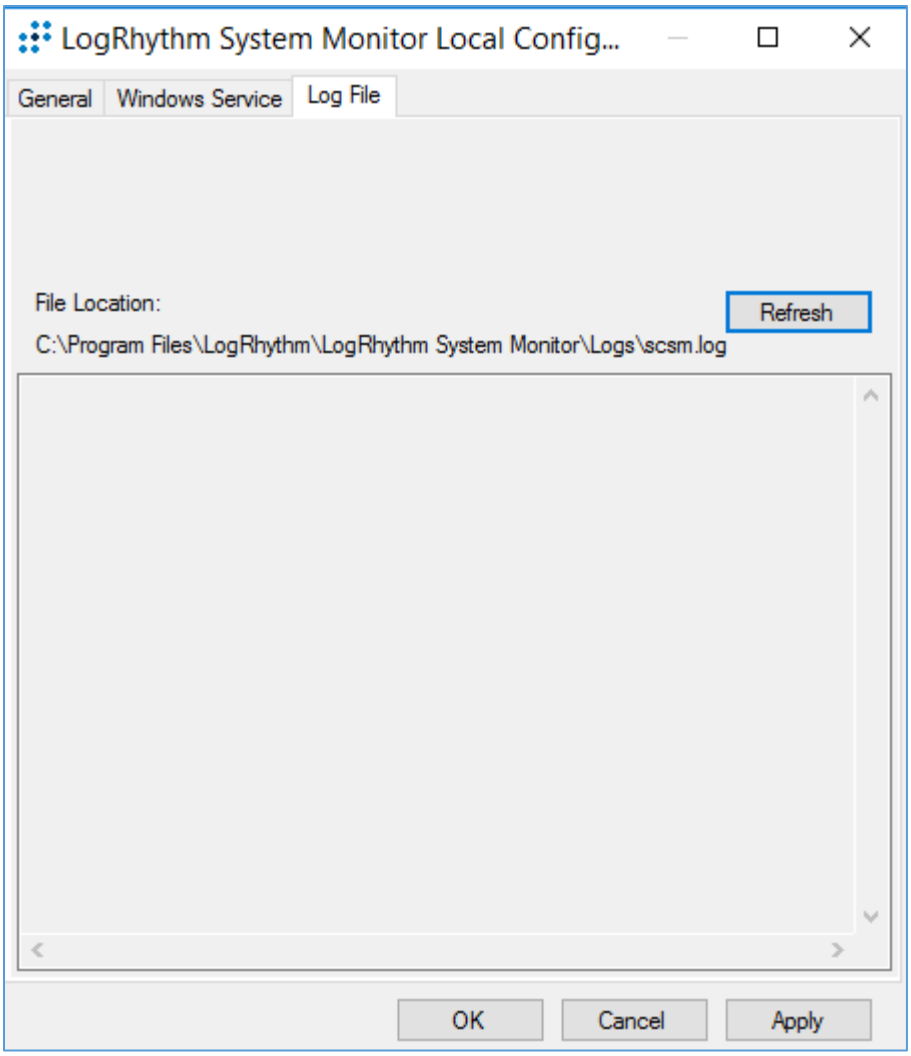
1. **Data Process Address:** 192.168.45.20
2. Click **Apply.**



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



6. Click the **Log File** tab.
7. Click **Refresh** to ensure NetworkXDR log collection.
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.

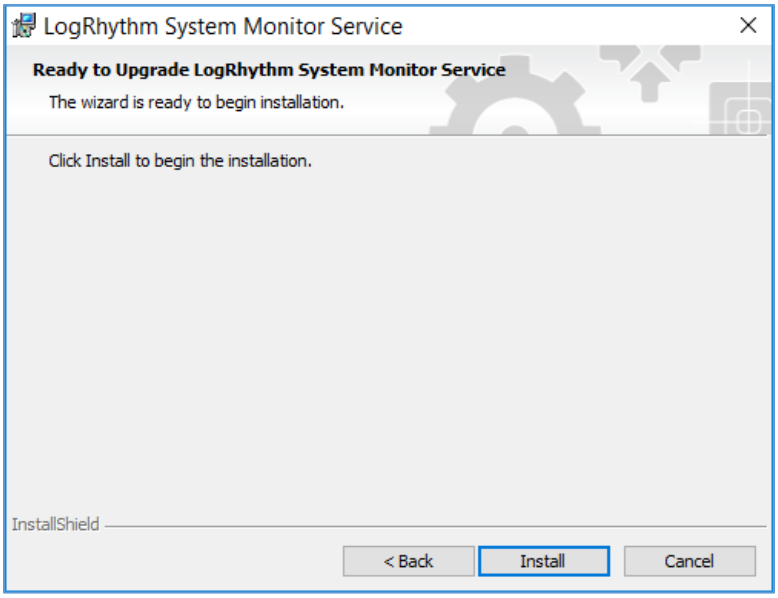
Download Installation Packages

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.

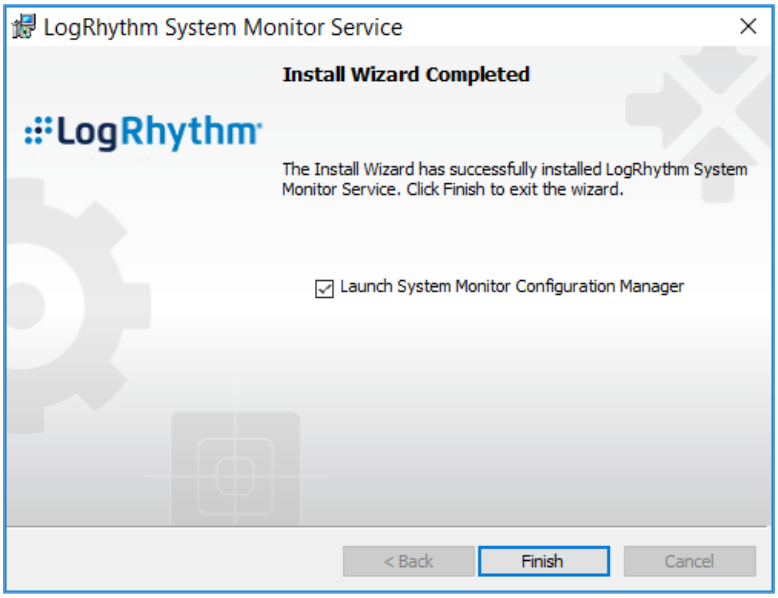
Install System Monitor Agent

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.**



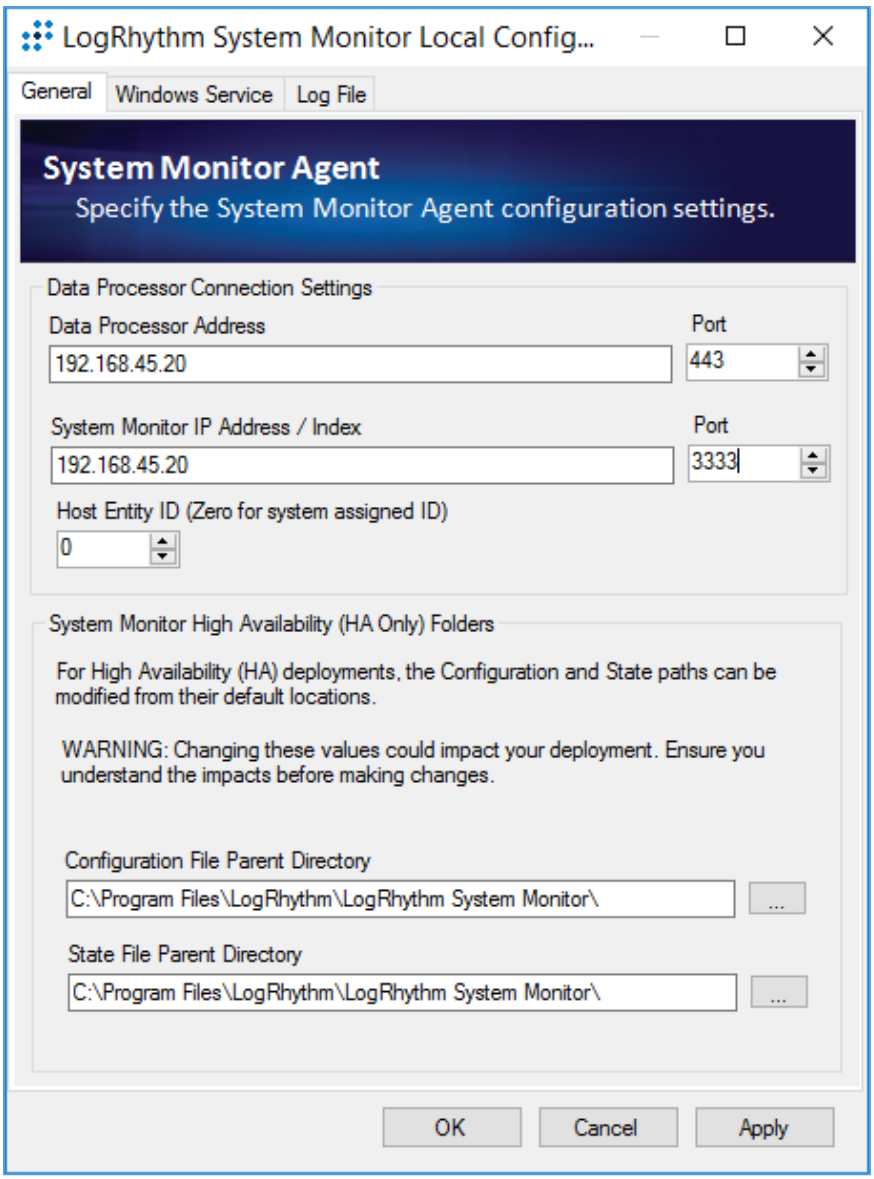
System Monitor Agent Configuration

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

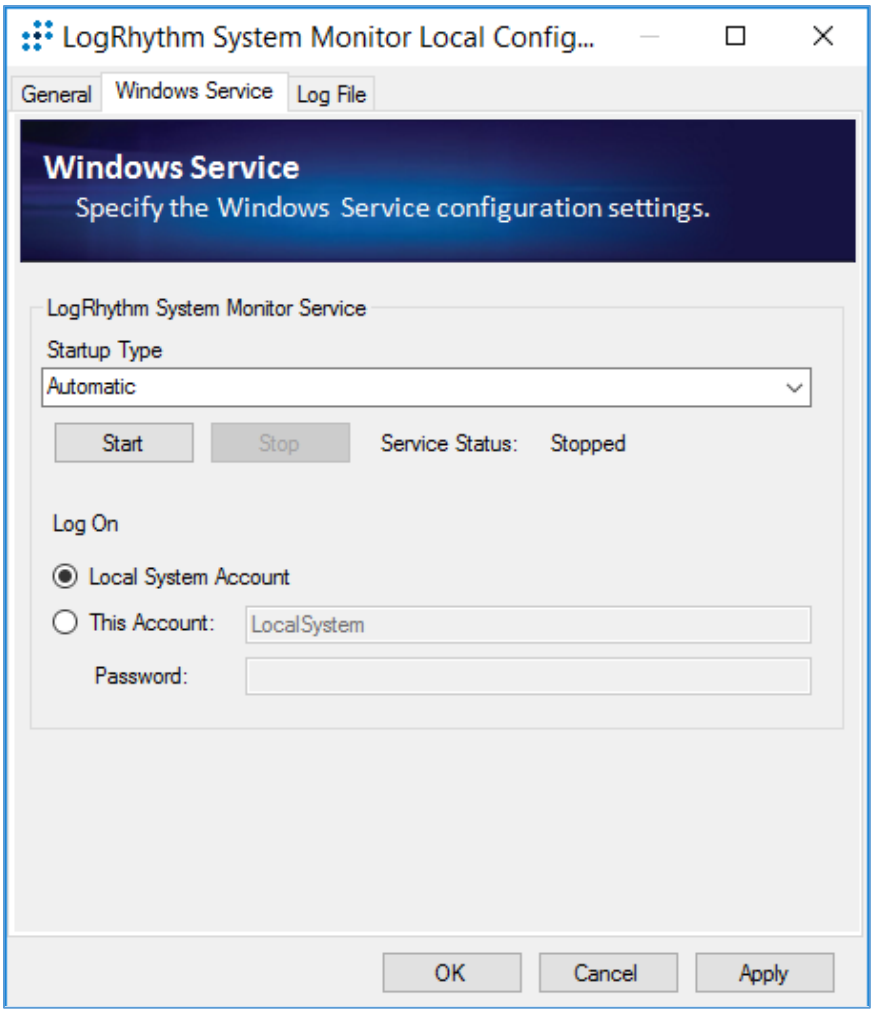
2. Click **Apply.**



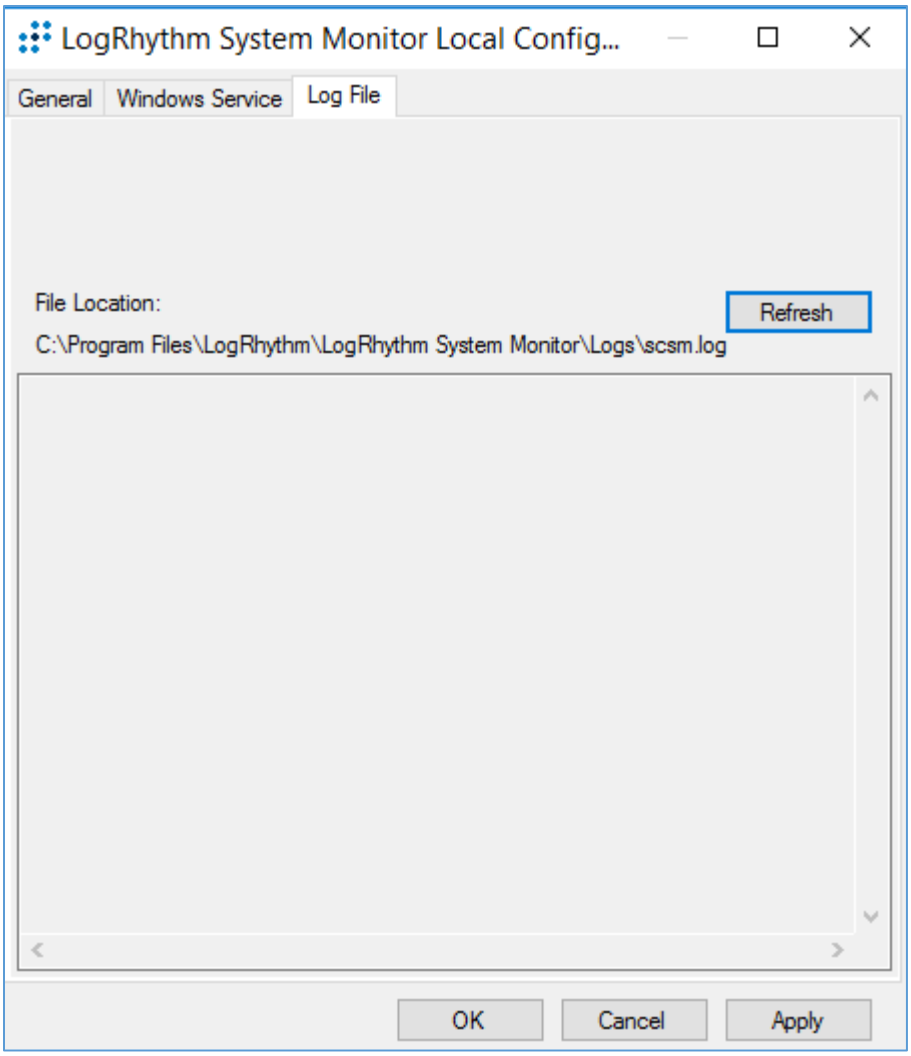
3. Click the **Windows Service** tab.

4. Change the **Service Type** to **Automatic.**

5. Click **Apply.**



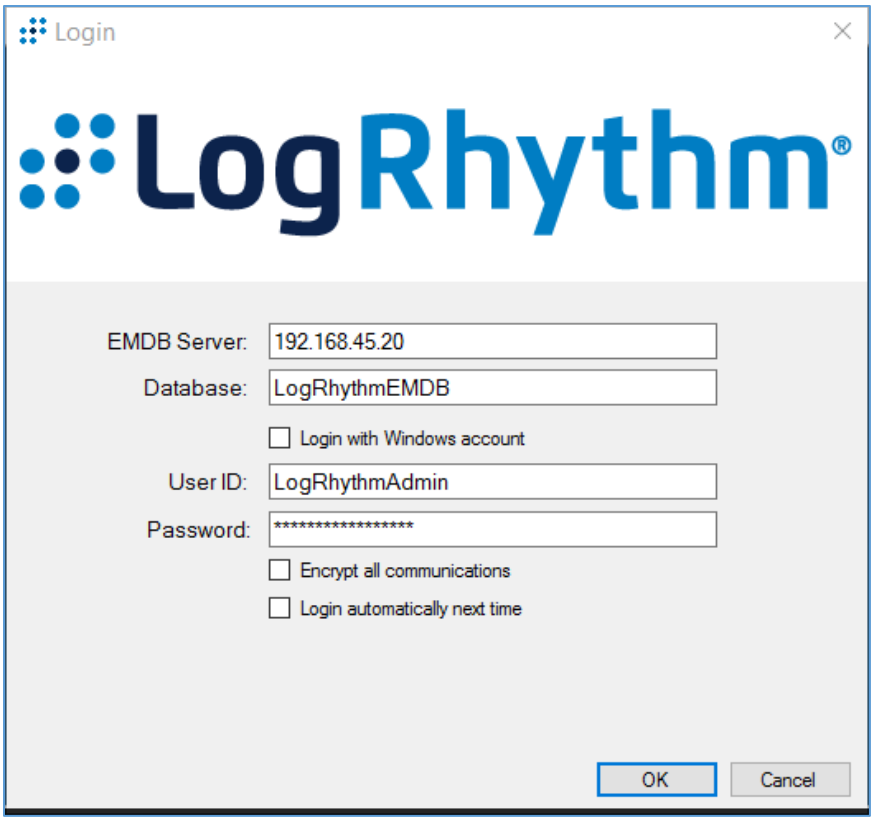
6. Click the **Log File** tab.
7. Click **Refresh** to ensure NetworkXDR log collection.
8. Click **OK** to exit the **Local Configuration Manager.**



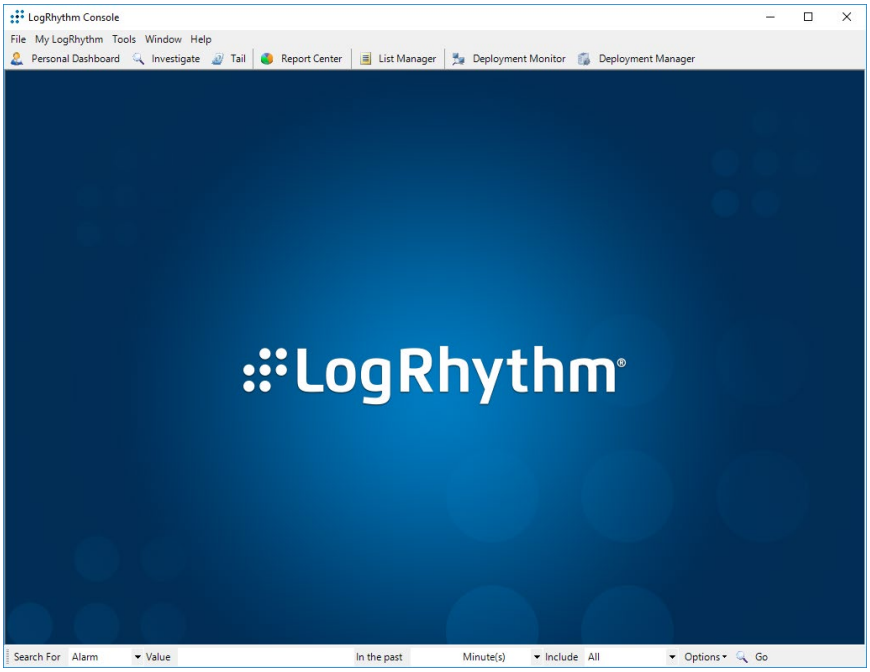
Add Workstation for System Monitor

Engineers added Clinical Workstation for System Monitor and Set Its Message Source Types in the LogRhythm Deployment Manager.

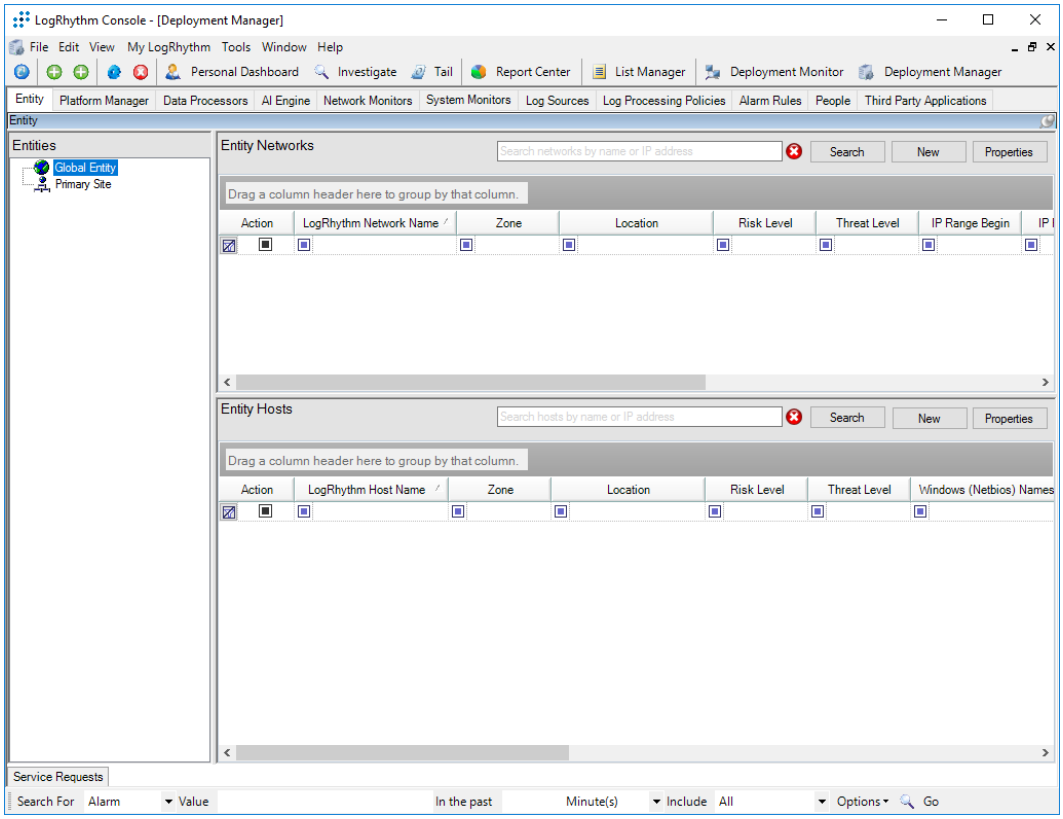
1. Log in to the **LogRhythm Console.**
    a. **User ID:** LogRhythmAdmin
    b. **Password:** **********



2. Navigate to the **Deployment Manager** in the menu ribbon.



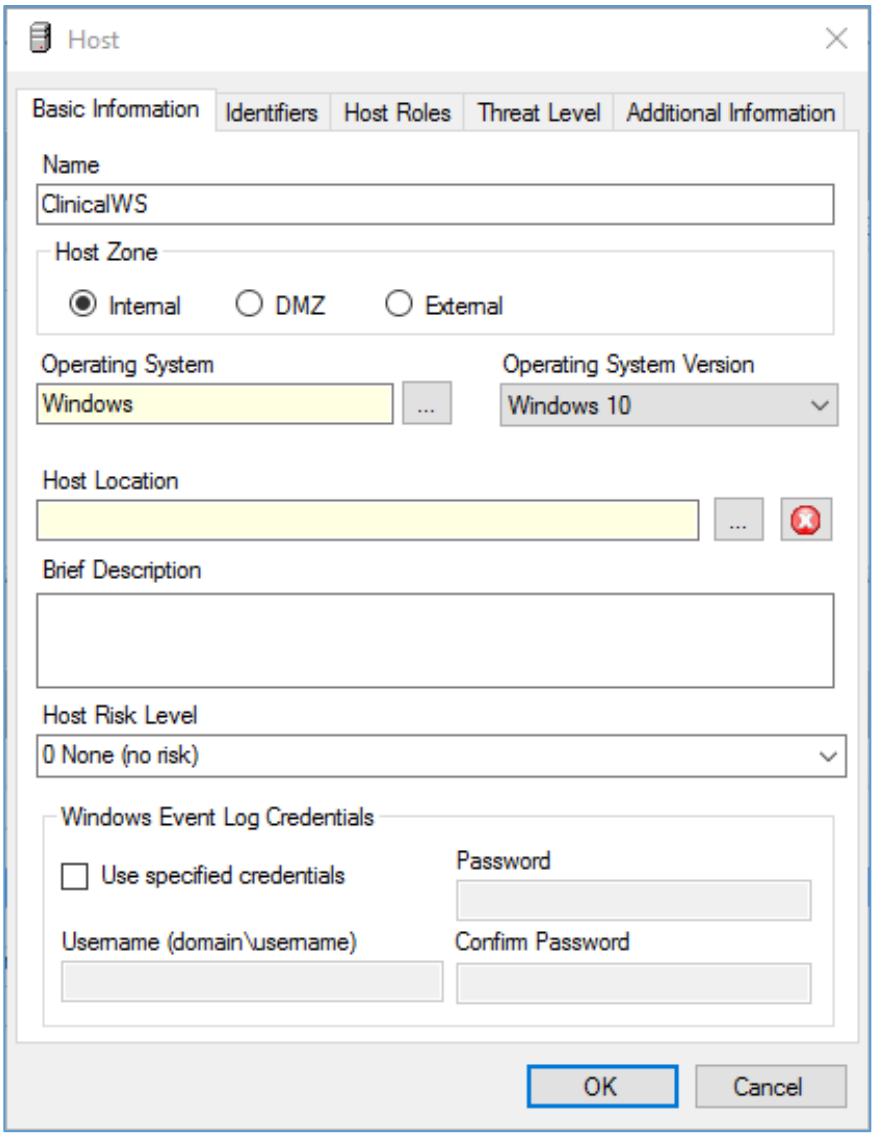
3. Under **Entity Hosts,** click on **New.**



4. Click **New** to open the **Host** pop-up window, and enter the following under the **Basic Information** tab**:**

    a. **Name:** ClinicalWS

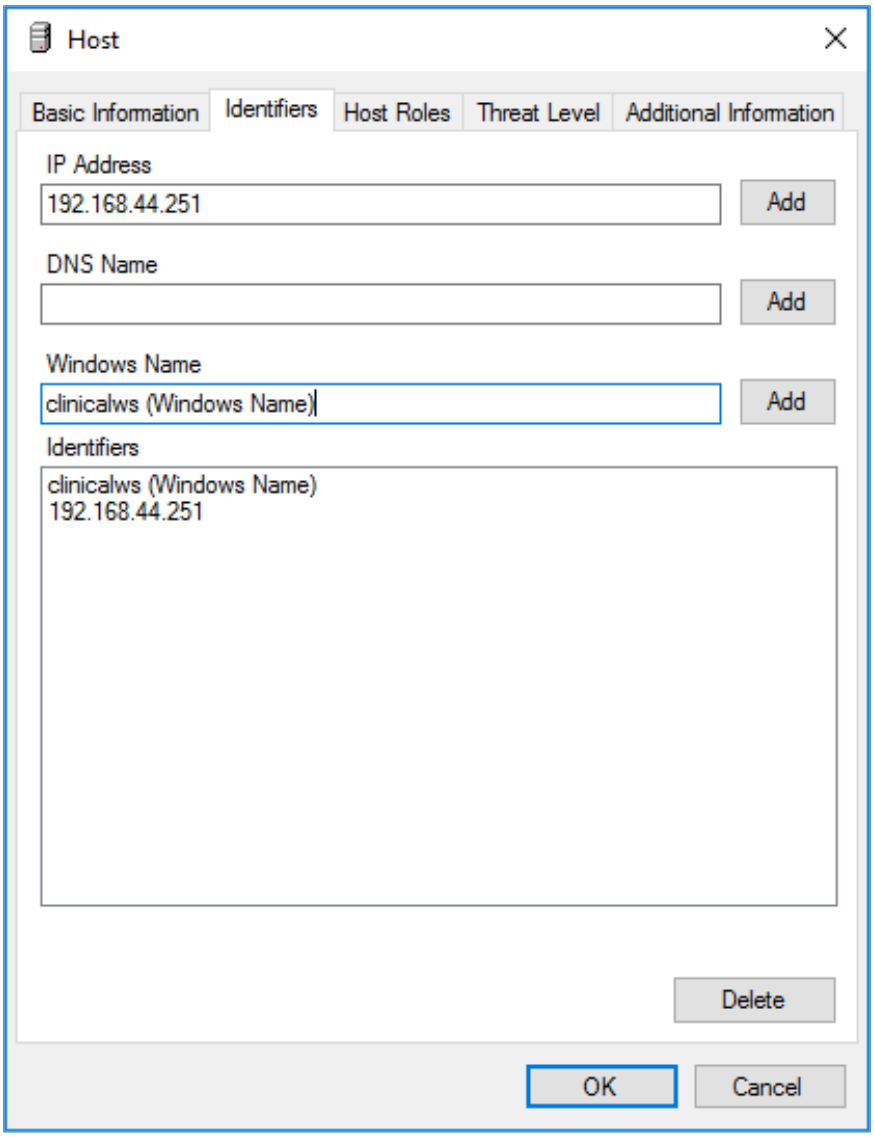
    b. **Host Zone:** Internal



1287 5. Navigate to the **Identifiers** tab, provide the following information in the appropriate fields, and
1288 click **Add**.

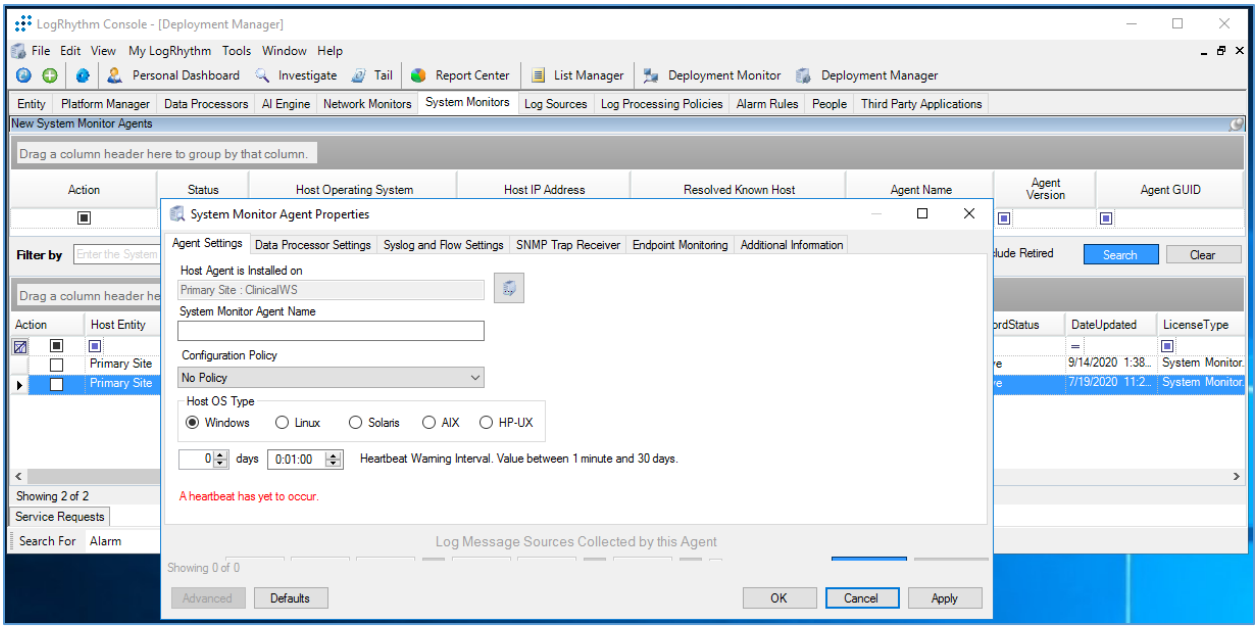
1289 a. **IP Address:** 192.168.44.251

1290 b. **Windows Name:** clinicalws (Windows Name)

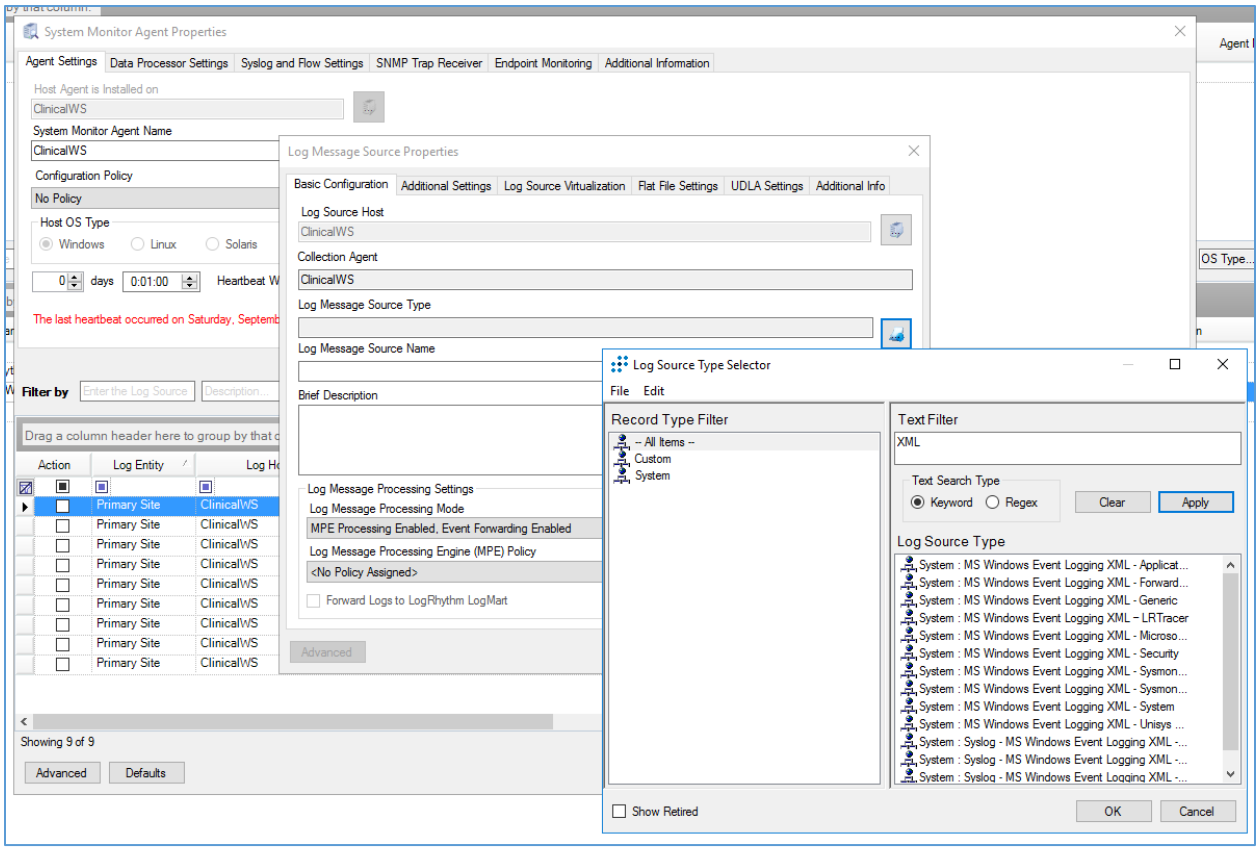


6. Add the **ClinicalWS** as a new system monitor agent by navigating to the **System Monitors** tab, right-clicking in the empty space, and selecting **New.**

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.**

Onclave SecureIoT Blockchain Appliance Information

CPU: 4

RAM: 8 GB

Storage: 120 GB (Thick Provision)

Network Adapter 1: VLAN 1317

Operating System: Debian Linux 9.11

Onclave SecureIoT Blockchain Appliance Configuration Guide

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.

Onclave SecureIoT Administrator Console Appliance Information

CPU: 4

RAM: 8 GB

Storage: 32 GB (Thick Provision)

Network Adapter 1: VLAN 1317

Operating System: Debian Linux 9.11

Onclave SecureIoT Administrator Console Appliance Configuration Guide

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`

Administrator Console Initialization and Bundle Creation

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.**

Transfer Ownership of Onclave Devices to the Orchestrator

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.**

Onclave SecureIoT Orchestrator Appliance Information

CPU: 4

RAM: 8 GB

Storage: 32 GB (Thick Provision)

Network Adapter 1: VLAN 1317

Operating System: Debian Linux 9.11

Onclave SecureIoT Orchestrator Appliance Configuration Guide

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

Create a Customer in the Orchestrator

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.**

Create a Secure Enclave

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.**

Onclave SecureIoT Bridge Appliance Information

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

Onclave SecureIoT Bridge Appliance Configuration Guide

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.**

Onclave SecureIoT Telehealth Gateway Appliance Information

CPU: 2

RAM: 8 GB

Storage: 16 GB

Network Adapter 1: VLAN 1317

Network Adapter 2: VLAN 1349

Operating System: Debian Linux 9.11

Onclave SecureIoT Telehealth Gateway Appliance Configuration Guide

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.**

Onclave SecureIoT Home Wi-Fi Gateway Appliance Information

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

Onclave SecureIoT Home Wi-Fi Gateway Appliance Configuration Guide

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.