NIST SPECIAL PUBLICATION 1800-30C

Securing Telehealth Remote Patient Monitoring Ecosystem

Volume C:
How-To Guides

Jennifer Cawthra
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.

November 2020

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, 140 pages, (November 2020), 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: November 16, 2020 through December 18, 2020

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
Matthew Hyatt	Cisco

Name	Organization
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
Spike Dog	The MITRE Corporation

Name	Organization
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
Chris Grodzickyj	Onclave Networks
Marianne Meins	Onclave Networks
Christina Phillips	Onclave Networks
James Taylor	Onclave Networks
Chris Jensen	Tenable
Joshua Moll	Tenable
Jeremiah Stallcup	Tenable
Julio C. Cespedes	The University of Mississippi Medical Center
Saurabh Chandra	The University of Mississippi Medical Center
Donald Clark	The University of Mississippi Medical Center
Alan Jones	The University of Mississippi Medical Center
Kristy Simms	The University of Mississippi Medical Center

Name	Organization
Richard Summers	The University of Mississippi Medical Center
Steve Waite	The University of Mississippi Medical Center
Dele Atunrase	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

The 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

Technology Partner/Collaborator	Build Involvement
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
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

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 5
2.1.2 Vivify Health 9
2.2 Security Capabilities 12
2.2.1 Risk Assessment Controls 12
2.2.2 Identity Management, Authentication, and Access Control 30
2.2.3 Security Continuous Monitoring 73
Appendix A List of Acronyms 139
Appendix B References 140

List of Figures

Figure 1-1 Final Architecture 4

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

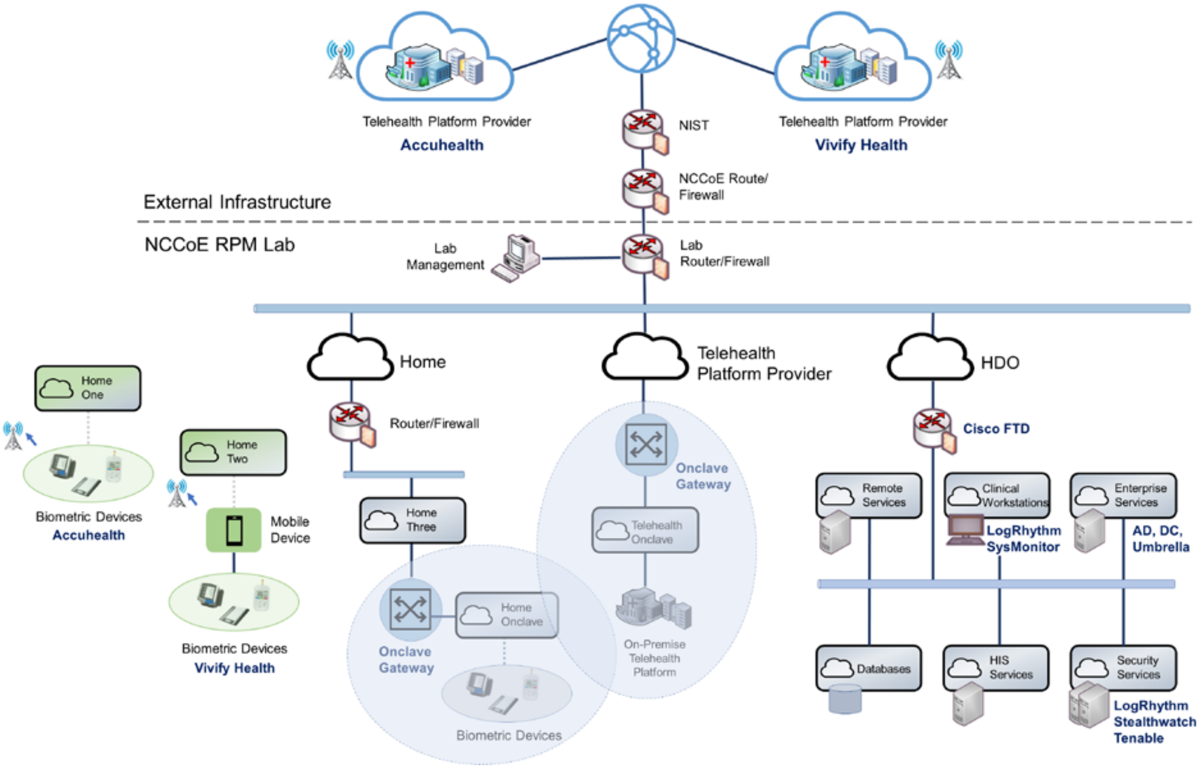
The following table presents typographic conventions used in this volume.

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. This practice guide 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, this practice guide deployed network infrastructure devices to implement network zoning and configure perimeter devices. This practice guide also deployed security capabilities that supported vulnerability management and a security incident event management (SIEM) tool. The following sections detail deployment and configuration of these components.

2.1 Telehealth Platform Provider

This practice guide 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 data 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.

This practice guide 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 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.

2.1.1 Accuhealth

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

2.1.1.1 Patient

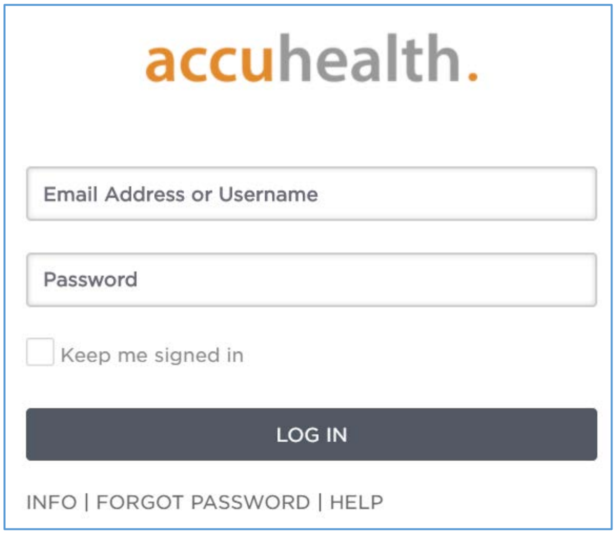
This practice guide assumed that the HDO enrolls the patient in an RPM program. Clinicians would determine when a patient may be enrolled in the program appropriately, and conversations would occur about understanding the roles and responsibilities associated with participating in the RPM program. When clinicians enrolled 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. Biometric devices, thus, were isolated from the patient home network environment. Accuhealth assured device configuration and asset management.

2.1.1.2 HDO

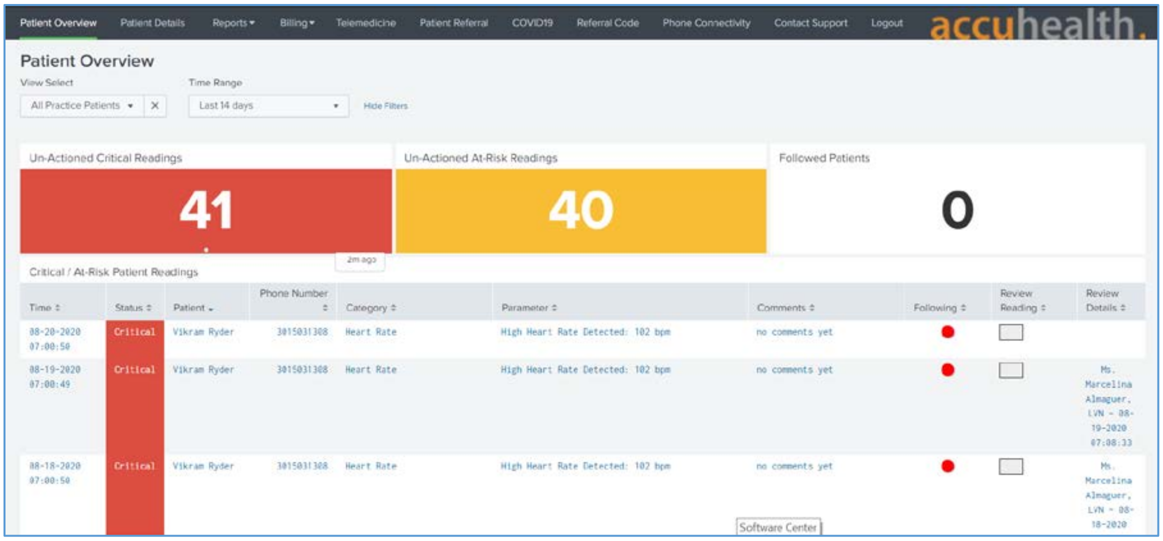
The Accuhealth solution includes installing an application within the HDO environment. Clinicians access a portal hosted by Accuhealth that allows a clinician to view patient biometric data. The application requires unique user accounts and role-based access control. System administrators create accounts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



Patient Overview

View Select: All Practice Patients

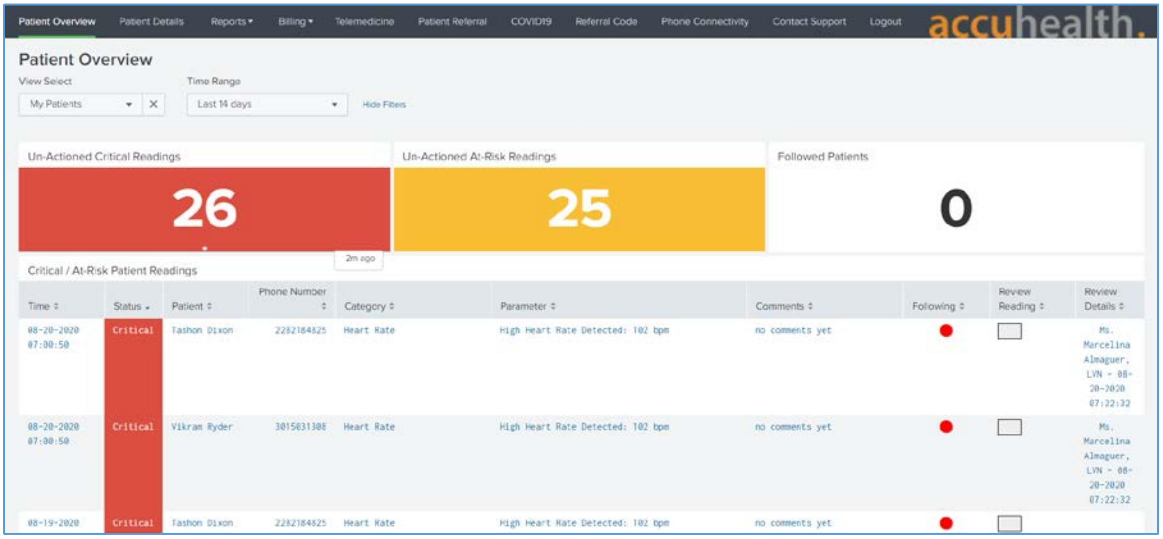
Time Range: Last 14 days

Un-Actioned Critical Readings	Un-Actioned At-Risk Readings	Followed Patients
41	40	0

Critical / At-Risk Patient Readings

Time	Status	Patient	Phone Number	Category	Parameter	Comments	Following	Review Reading	Review Details
08-20-2020 07:00:50	Critical	Vikram Ryder	3015031308	Heart Rate	High Heart Rate Detected: 102 bpm	no comments yet	●	□	
08-19-2020 07:00:49	Critical	Vikram Ryder	3015031308	Heart Rate	High Heart Rate Detected: 102 bpm	no comments yet	●	□	Ms. Marcelina Almaguer, LVN - 08-19-2020 07:08:33
08-18-2020 07:00:50	Critical	Vikram Ryder	3015031308	Heart Rate	High Heart Rate Detected: 102 bpm	no comments yet	●	□	Ms. Marcelina Almaguer, LVN - 08-18-2020

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.**



Patient Overview

View Select: My Patients

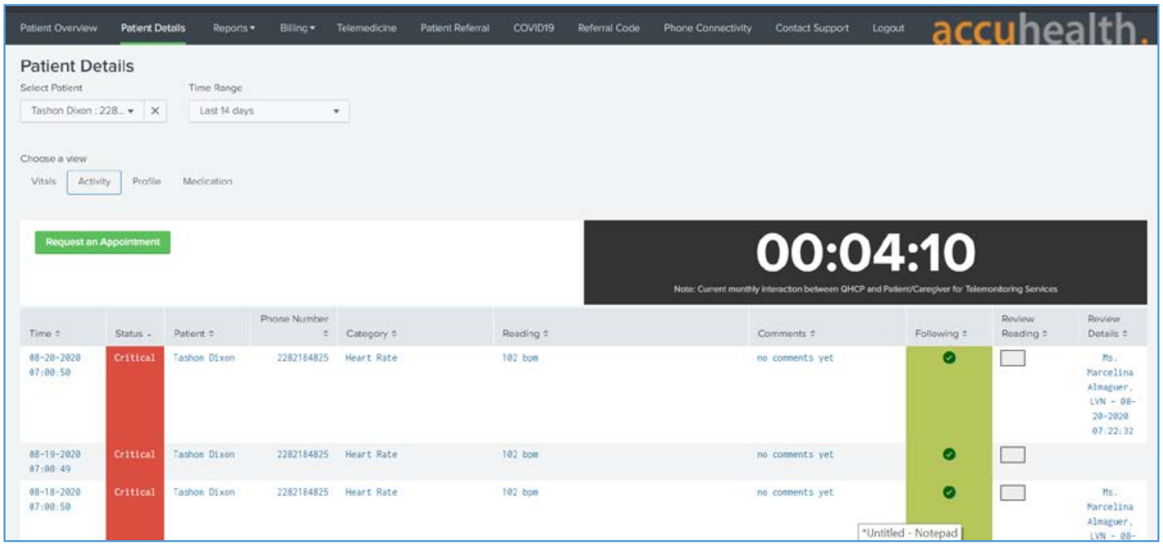
Time Range: Last 14 days

Un-Actioned Critical Readings	Un-Actioned At-Risk Readings	Followed Patients
26	25	0

Critical / At-Risk Patient Readings

Time	Status	Patient	Phone Number	Category	Parameter	Comments	Following	Review Reading	Review Details
08-20-2020 07:00:50	Critical	Tashon Dixon	2232184825	Heart Rate	High Heart Rate Detected: 102 bpm	no comments yet	●	□	Ms. Marcelina Almaguer, LVN - 08-20-2020 07:22:32
08-20-2020 07:00:50	Critical	Vikram Ryder	3015031308	Heart Rate	High Heart Rate Detected: 102 bpm	no comments yet	●	□	Ms. Marcelina Almaguer, LVN - 08-20-2020 07:22:32
08-19-2020	Critical	Tashon Dixon	2232184825	Heart Rate	High Heart Rate Detected: 102 bpm	no comments yet	●	□	

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



Patient Details

Select Patient: Tashon Dixon : 228... ▾ ✕

Time Range: Last 14 days ▾

00:04:10

Note: Current monthly interaction between QHCP and Patient/Caregiver for Telemonitoring Services

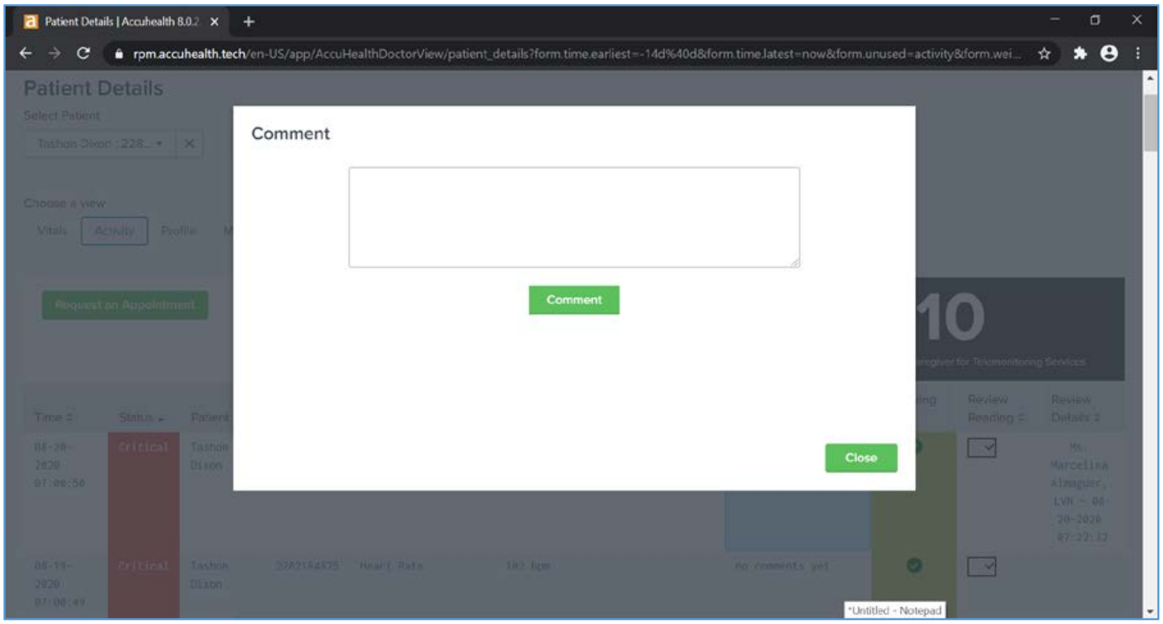
Time	Status	Patient	Phone Number	Category	Reading	Comments	Following	Review Reading	Review Details
08-20-2020 07:00:50	Critical	Tashon Dixon	2282184825	Heart Rate	102 bpm	no comments yet	✓	□	Ms. Marcelina Almaguer, LVN - 08-20-2020 07:22:32
08-19-2020 07:00:49	Critical	Tashon Dixon	2282184825	Heart Rate	102 bpm	no comments yet	✓	□	
08-18-2020 07:00:50	Critical	Tashon Dixon	2282184825	Heart Rate	102 bpm	no comments yet	✓	□	Ms. Marcelina Almaguer, LVN - 08-

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

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

8. Click **Comment**.

9. Click **Close**.

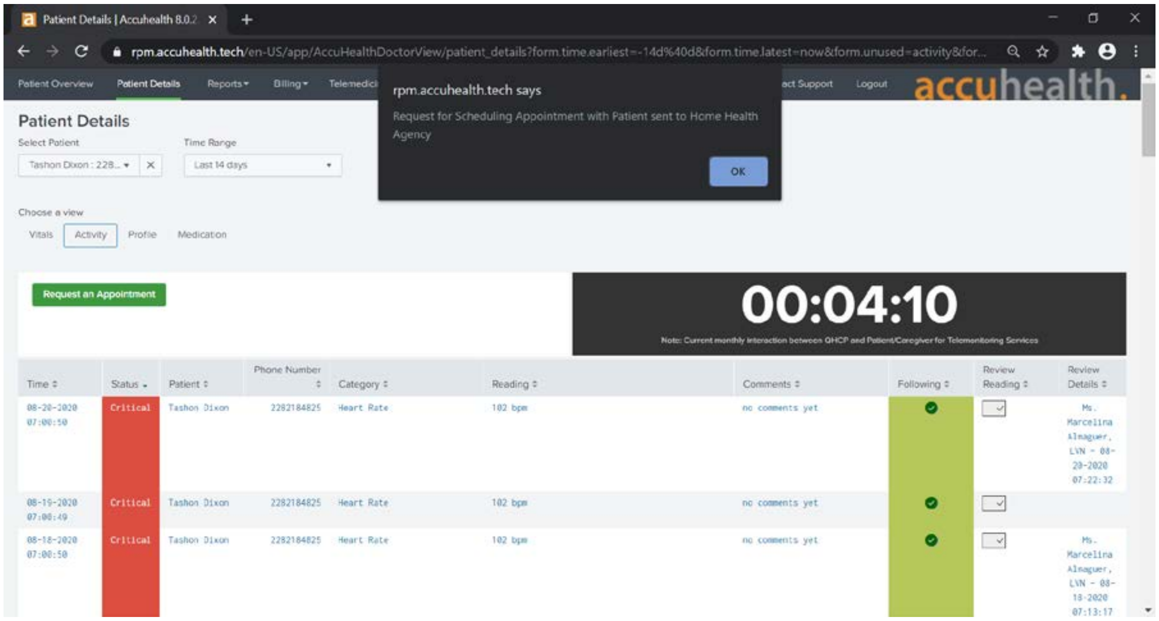


rpm.accuhealth.tech/en-US/app/AccuHealthDoctorView/patient_details?form.time.earliest=-14d%40d&form.time.latest=now&form.unused=activity&form.wei...

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.**



rpm.accuhealth.tech says

Request for Scheduling Appointment with Patient sent to Home Health Agency

00:04:10

Note: Current monthly interaction between QHCP and Patient/Caregiver for Telemonitoring Services

Time	Status	Patient	Phone Number	Category	Reading	Comments	Following	Review Reading	Review Details
08-20-2020 07:00:50	Critical	Tashon Dixon	2282184825	Heart Rate	102 bpm	no comments yet	✓	☑	Ms. Marcelina Almaguer, LVN - 08-20-2020 07:22:32
08-19-2020 07:00:49	Critical	Tashon Dixon	2282184825	Heart Rate	102 bpm	no comments yet	✓	☑	
08-18-2020 07:00:50	Critical	Tashon Dixon	2282184825	Heart Rate	102 bpm	no comments yet	✓	☑	Ms. Marcelina Almaguer, LVN - 08-18-2020 07:13:17

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 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

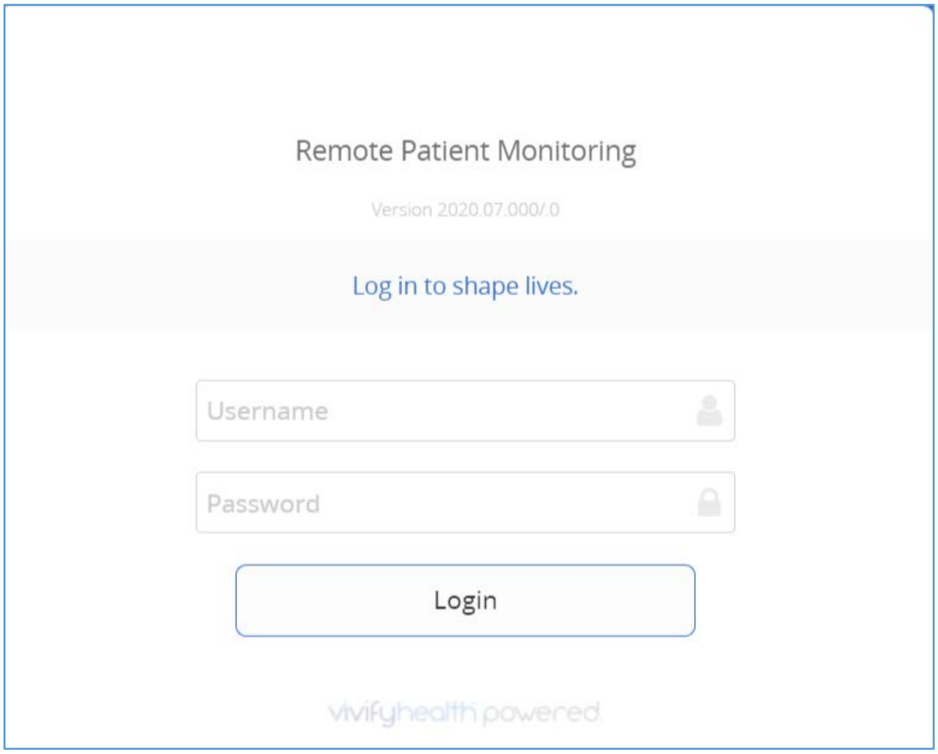
This practice guide assumed that the HDO enrolls the patient in an RPM program. Clinicians would determine when a patient may be enrolled in the program appropriately, and conversations then occur about understanding the roles and responsibilities associated with participating in the RPM program. When 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. Vivify assured device configuration and asset management.

2.1.2.2 HDO

The Vivify solution includes installing an application within the HDO environment. Clinicians access a portal hosted by Vivify 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 https://demonccoerpm.vivifyhealth.com/CaregiverPortal/index.html#/Login and provide 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. Logout of the platform.
12. Login to the platform 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, this practice guide 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. Tenable.sc's dashboard includes vulnerability scoring, enabling engineers to prioritize patching and remediation. This practice guide 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 used the solution for vulnerability management.

System Requirements

Central Processing Unit (CPU): 4

Memory: 8 gigabytes (GB)

Storage: 250 GB

Operating System: CentOS 7

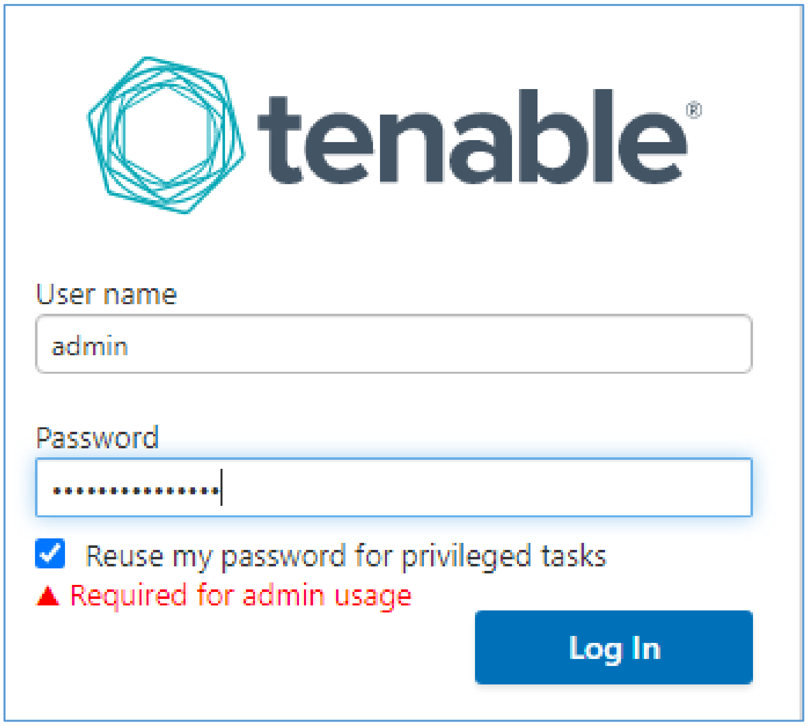
Network Adapter: VLAN 1348

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 virtual local area network (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 popup 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**.



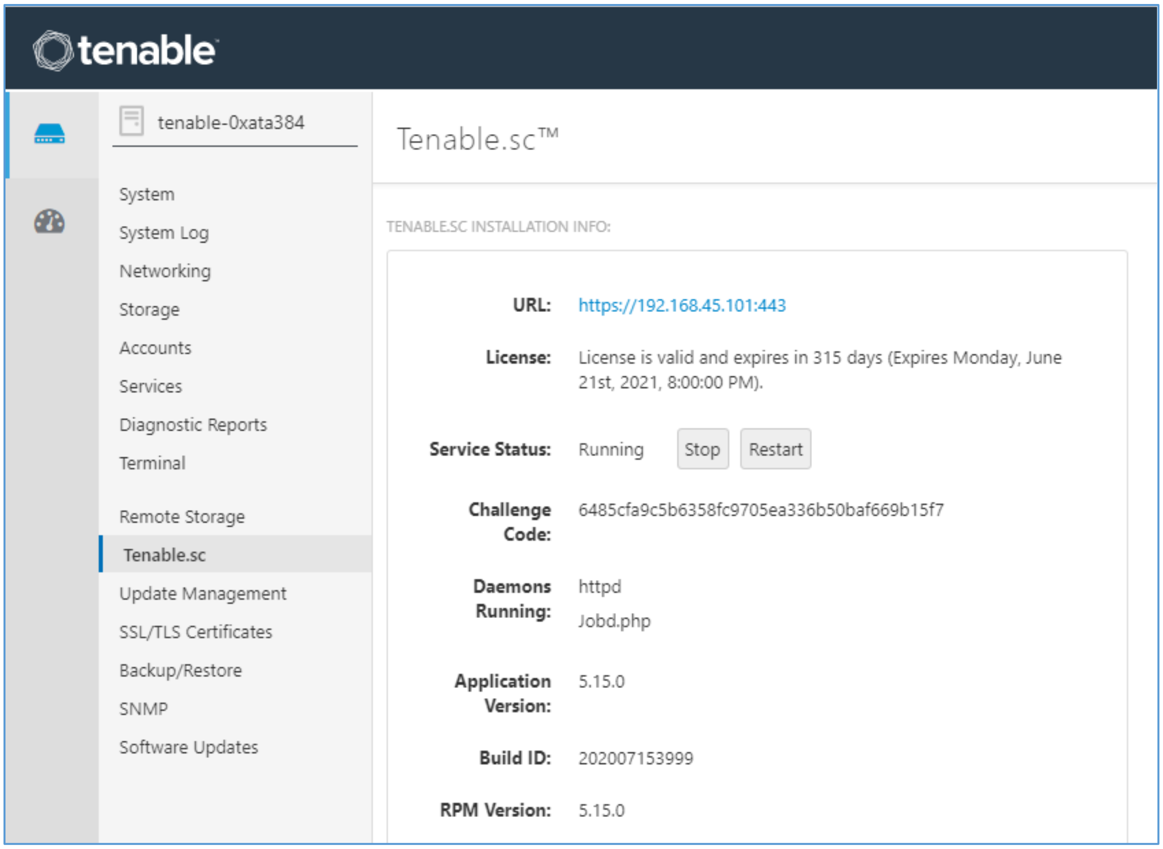
User name: admin

Password: •••••••••••••••

☑ Reuse my password for privileged tasks

▲ Required for admin usage

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.



Tenable.sc™

TENABLE.SC INSTALLATION INFO:

URL: https://192.168.45.101:443

License: License is valid and expires in 315 days (Expires Monday, June 21st, 2021, 8:00:00 PM).

Service Status: Running

Challenge Code: 6485cfa9c5b6358fc9705ea336b50baf669b15f7

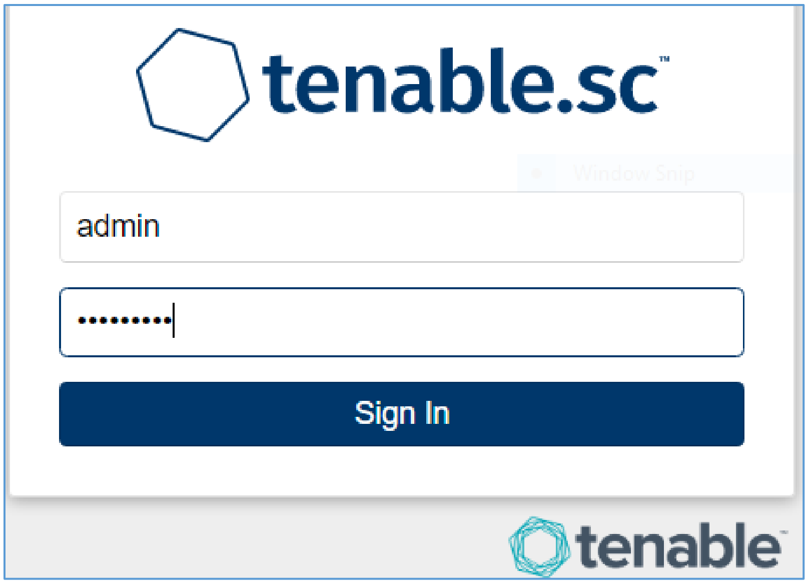
Daemons Running: httpd
Jobd.php

Application Version: 5.15.0

Build ID: 202007153999

RPM Version: 5.15.0

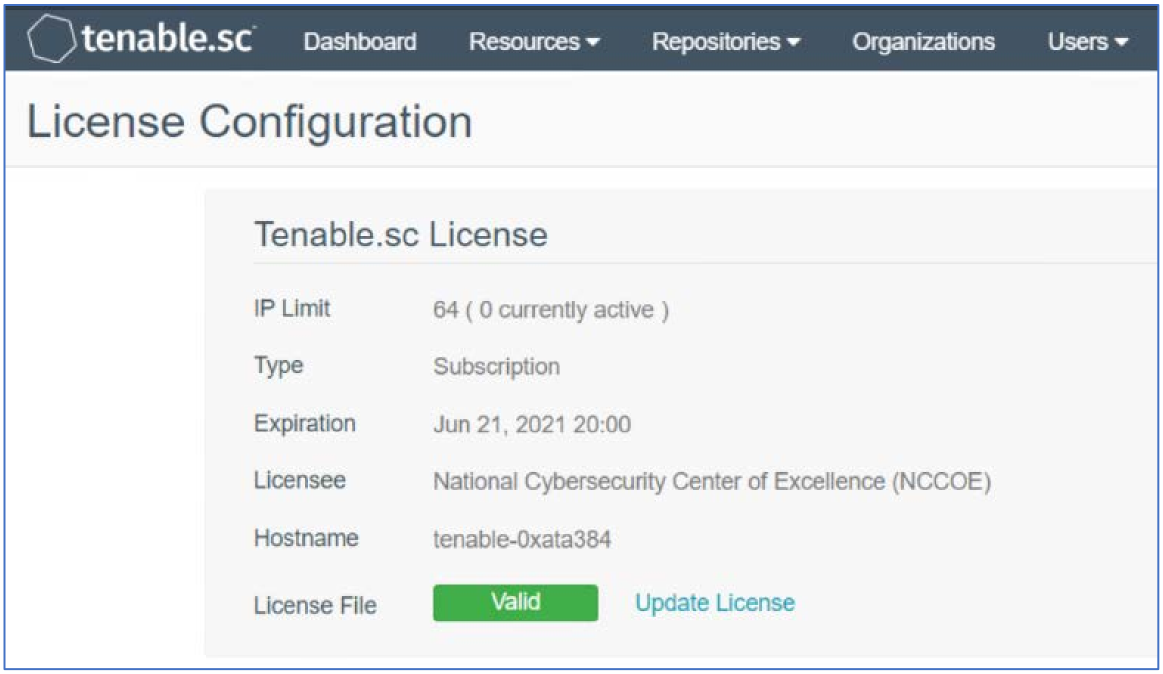
11. Log in to Tenable.sc using the credentials created in previous steps, and click **Sign In.**
    a. **Username:** admin
    b. **Password:** **********



admin

•••••••••

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.



License Configuration

Tenable.sc License

IP Limit 64 (0 currently active)

Type Subscription

Expiration Jun 21, 2021 20:00

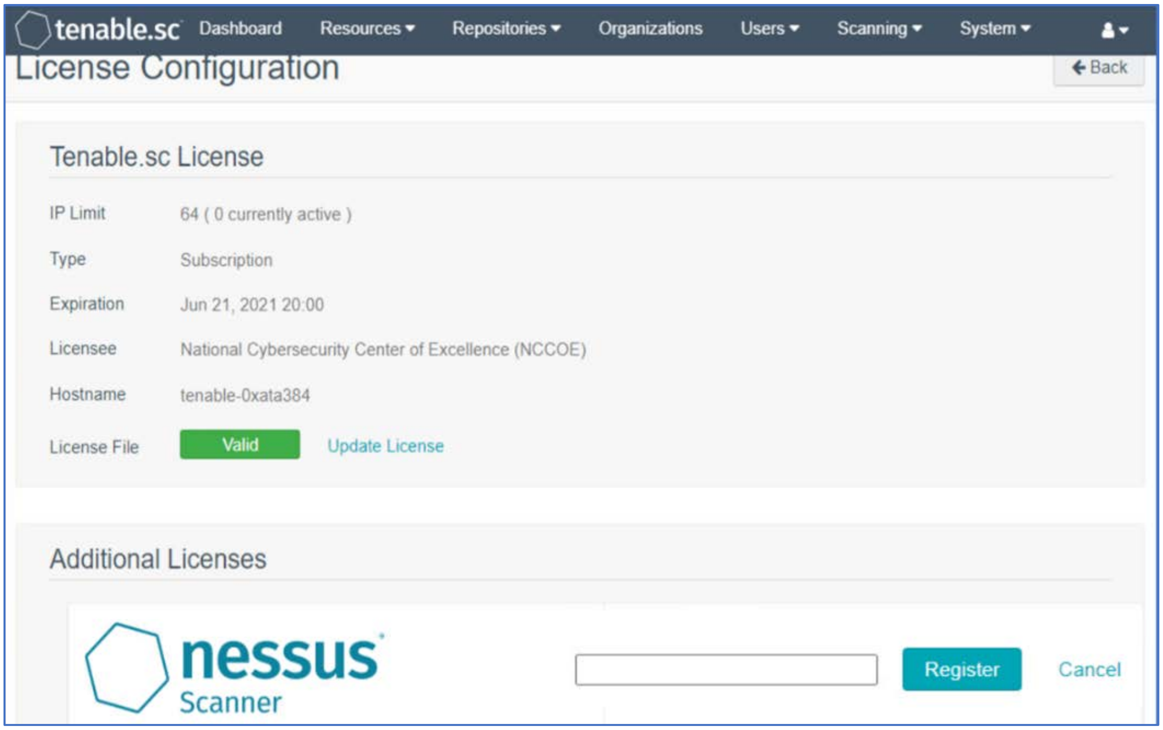
Licensee National Cybersecurity Center of Excellence (NCCOE)

Hostname tenable-0xata384

License File Valid Update License

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

21. Click **Register**.



License Configuration

Tenable.sc License

IP Limit	64 (0 currently active)
Type	Subscription
Expiration	Jun 21, 2021 20:00
Licensee	National Cybersecurity Center of Excellence (NCCOE)
Hostname	tenable-0xata384
License File	Valid

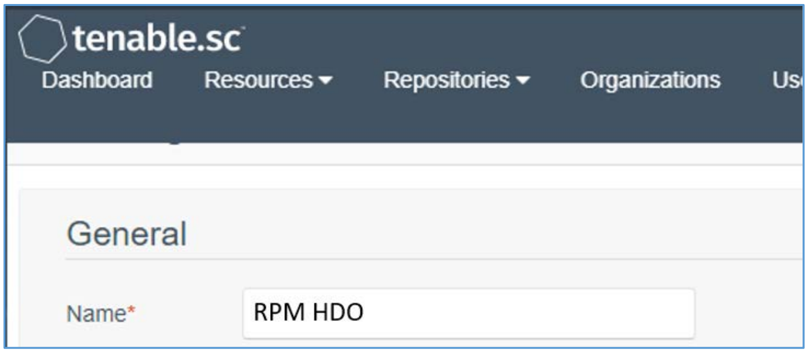
Additional Licenses

<u>Tenable.sc Configuration</u>

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

<u>Add an Organization</u>

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

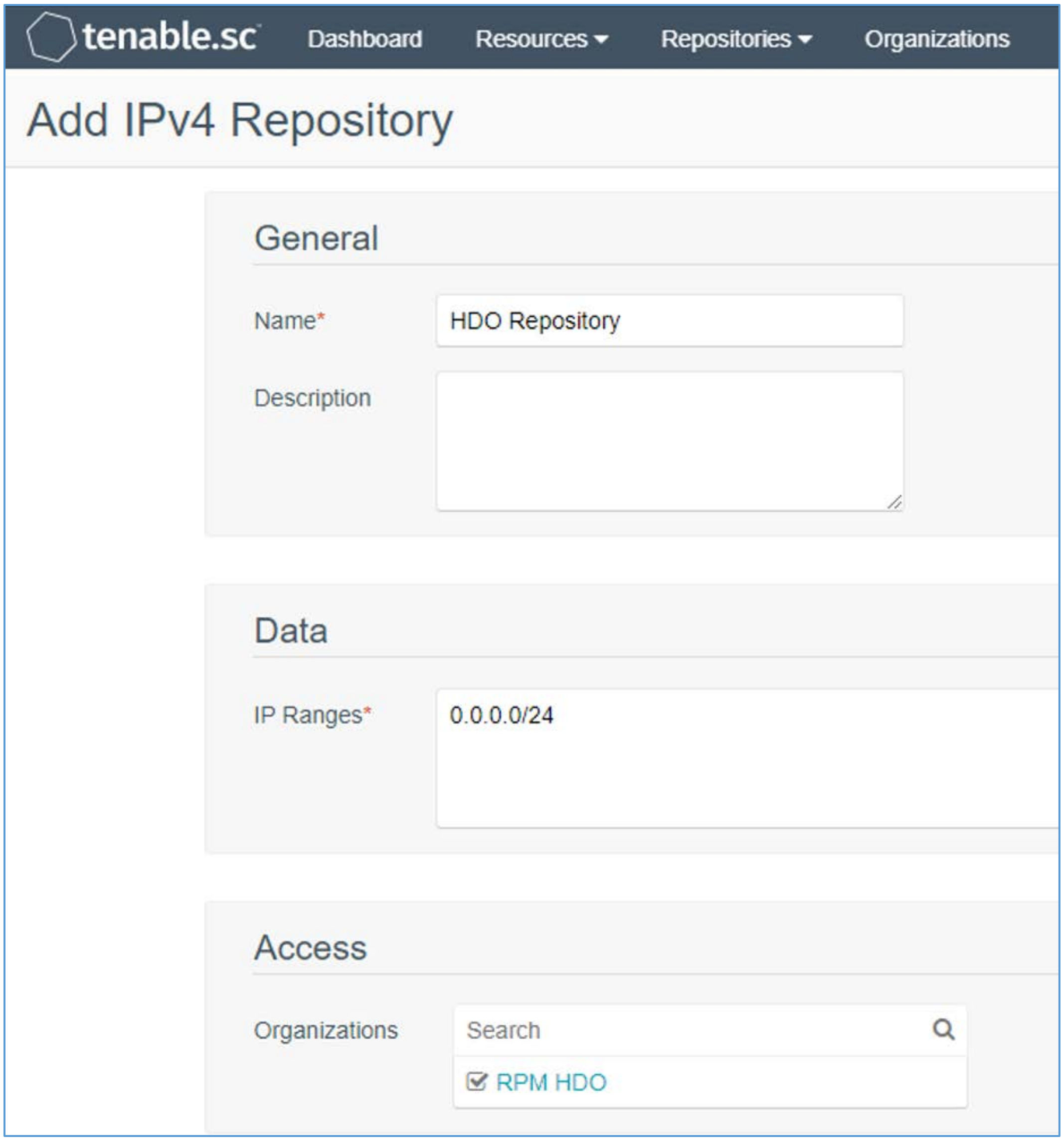


General

Name* RPM HDO

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 IPv4 Repository

General

Name*: HDO Repository

Description

Data

IP Ranges*: 0.0.0.0/24

Access

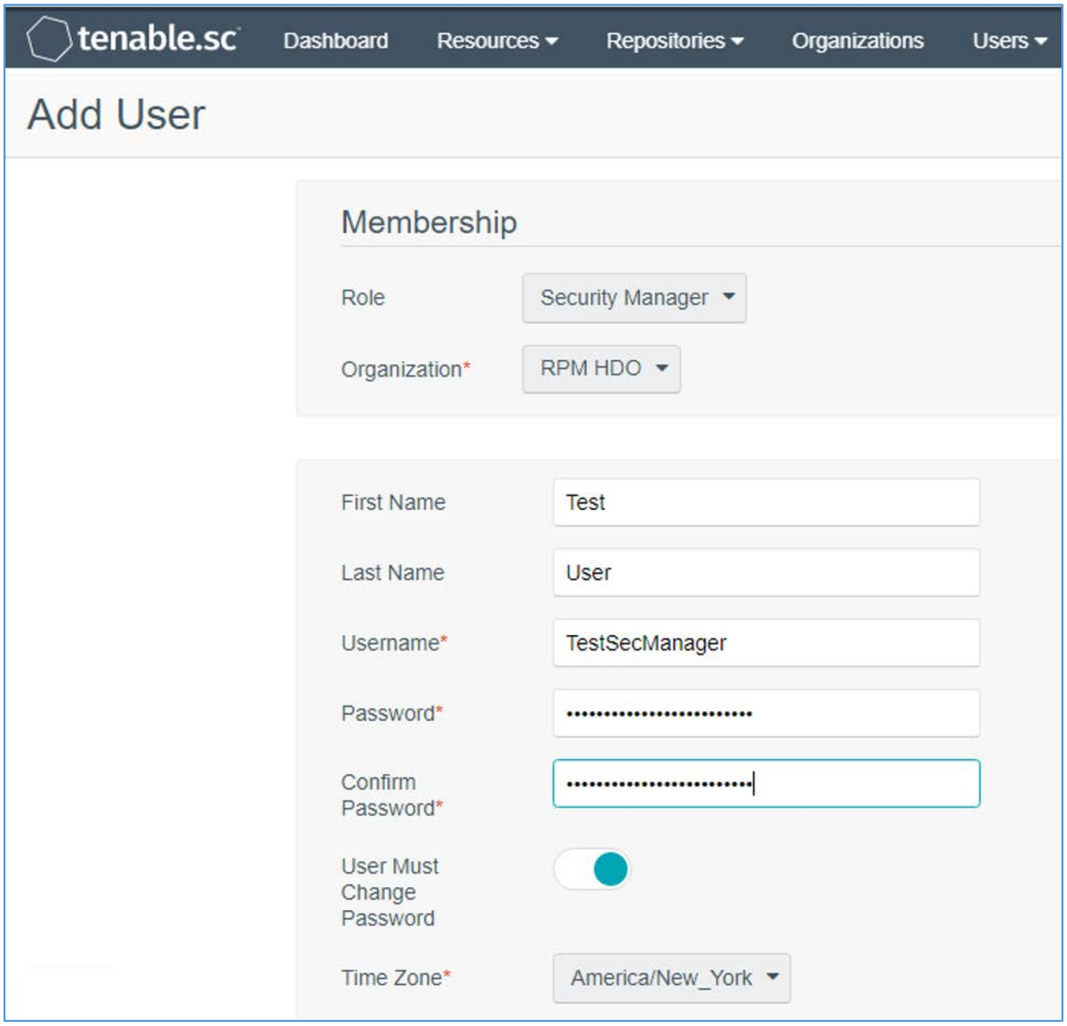
Organizations: Search

☑ RPM HDO

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**.



Add User

Membership

Role: Security Manager

Organization*: RPM HDO

First Name: Test

Last Name: User

Username*: TestSecManager

Password*: ••••••••••••••••••••••••

Confirm Password*: ••••••••••••••••••••••••

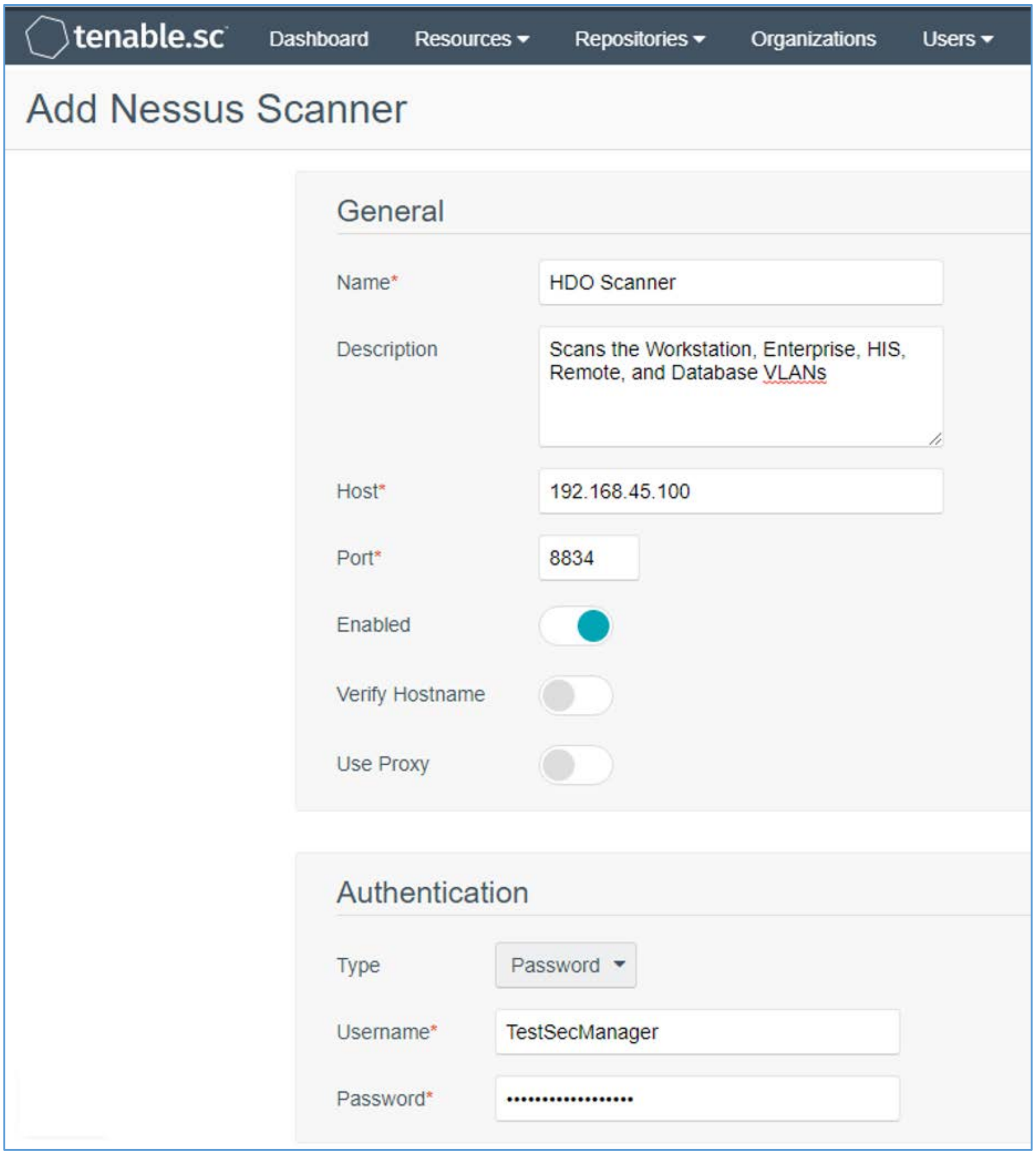
User Must Change Password: ●

Time Zone*: America/New_York

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**.



Add Nessus Scanner

General

Name* HDO Scanner

Description Scans the Workstation, Enterprise, HIS, Remote, and Database VLANs

Host* 192.168.45.100

Port* 8834

Enabled ●

Verify Hostname ○

Use Proxy ○

Authentication

Type Password

Username* TestSecManager

Password* ••••••••••••••••••

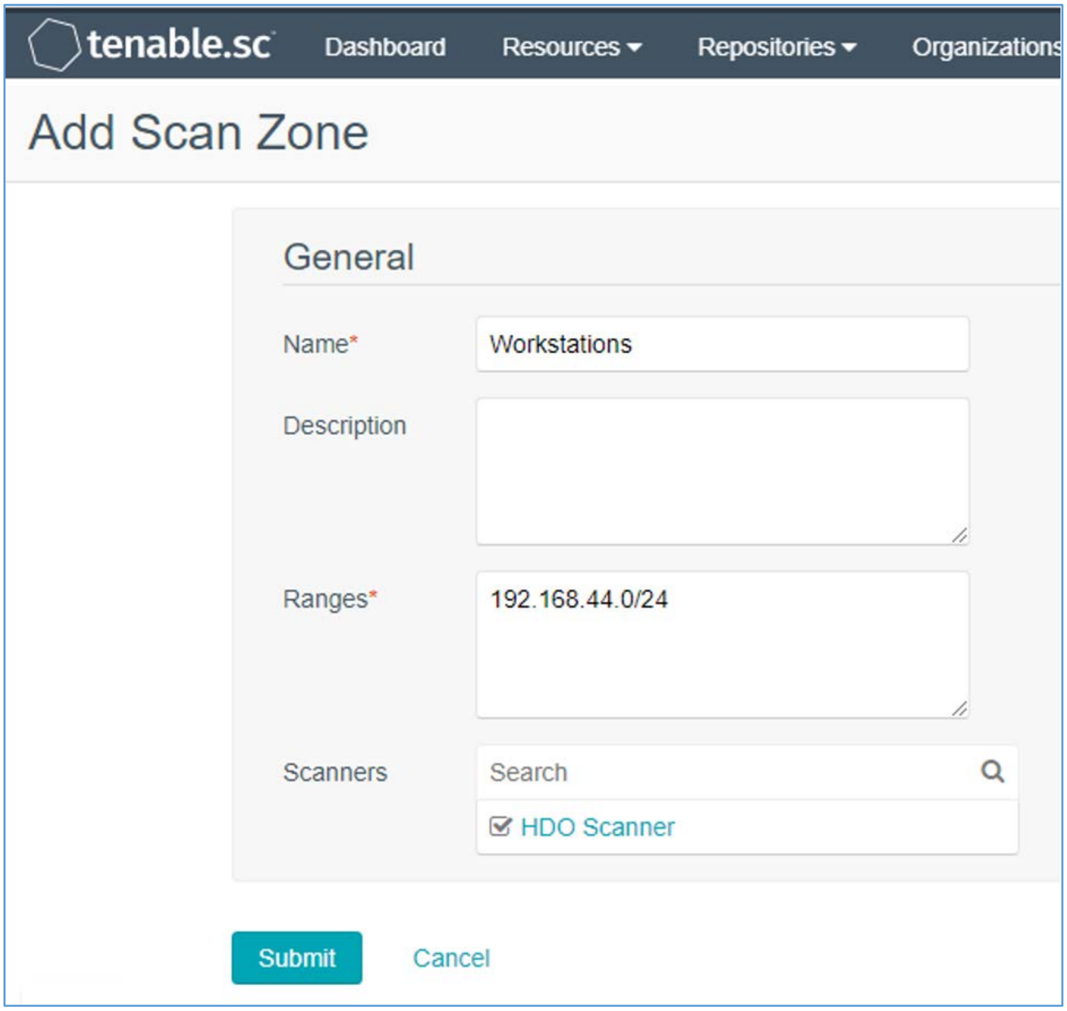
The engineers created a scan zone for each subnet established on the HDO network. The process to create a scan zone is the same for each subnet aside from the IP address range.

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.**



Add Scan Zone

General

Name*: Workstations

Description:

Ranges*: 192.168.44.0/24

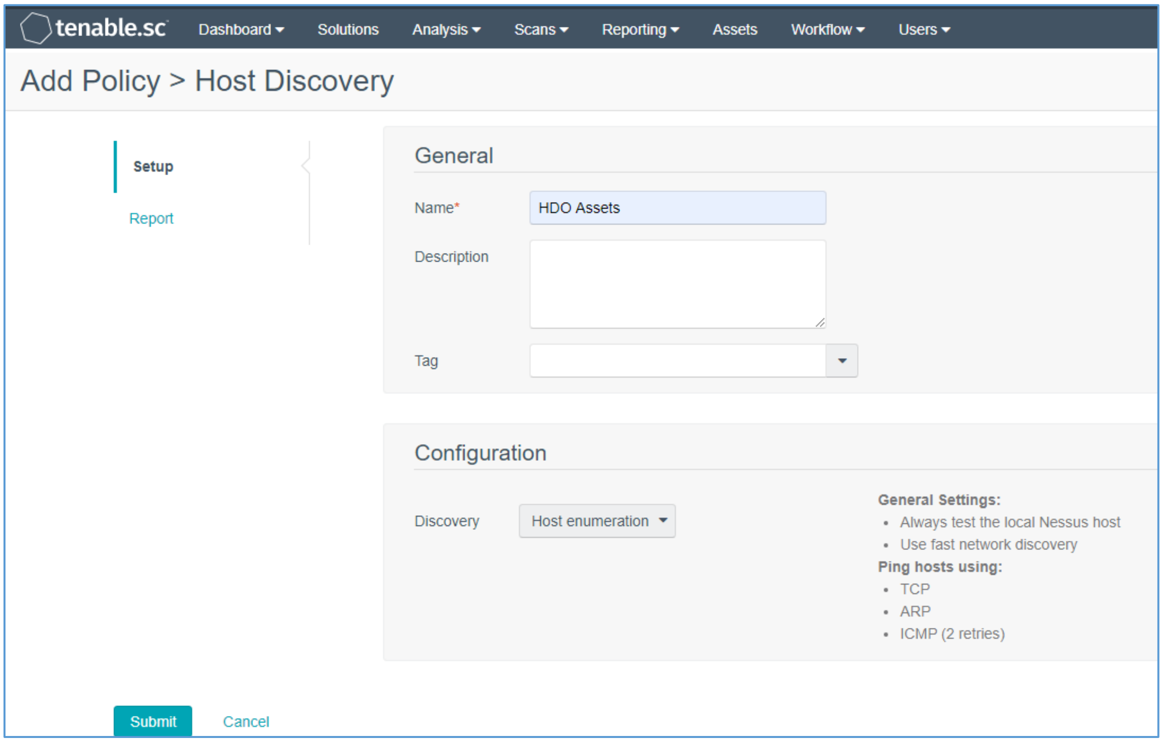
Scanners: ☑ HDO Scanner

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 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.**



Add Policy > Host Discovery

General

Name* HDO Assets

Description

Tag

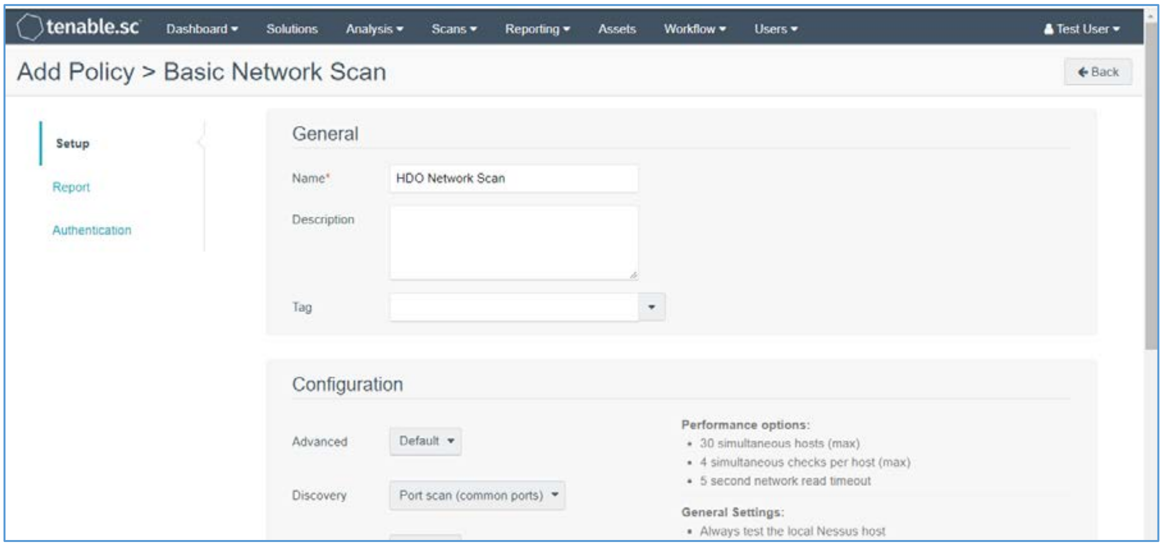
Configuration

Discovery: Host enumeration

General Settings:
- Always test the local Nessus host
- Use fast network discovery

Ping hosts using:
- TCP
- ARP
- ICMP (2 retries)

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**.



Add Policy > Basic Network Scan

General

Name*: HDO Network Scan

Description:

Tag:

Configuration

Advanced: Default

Discovery: Port scan (common ports)

Performance options:
- 30 simultaneous hosts (max)
- 4 simultaneous checks per host (max)
- 5 second network read timeout

General Settings:
- Always test the local Nessus host

<u>Create Active Scans</u>

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

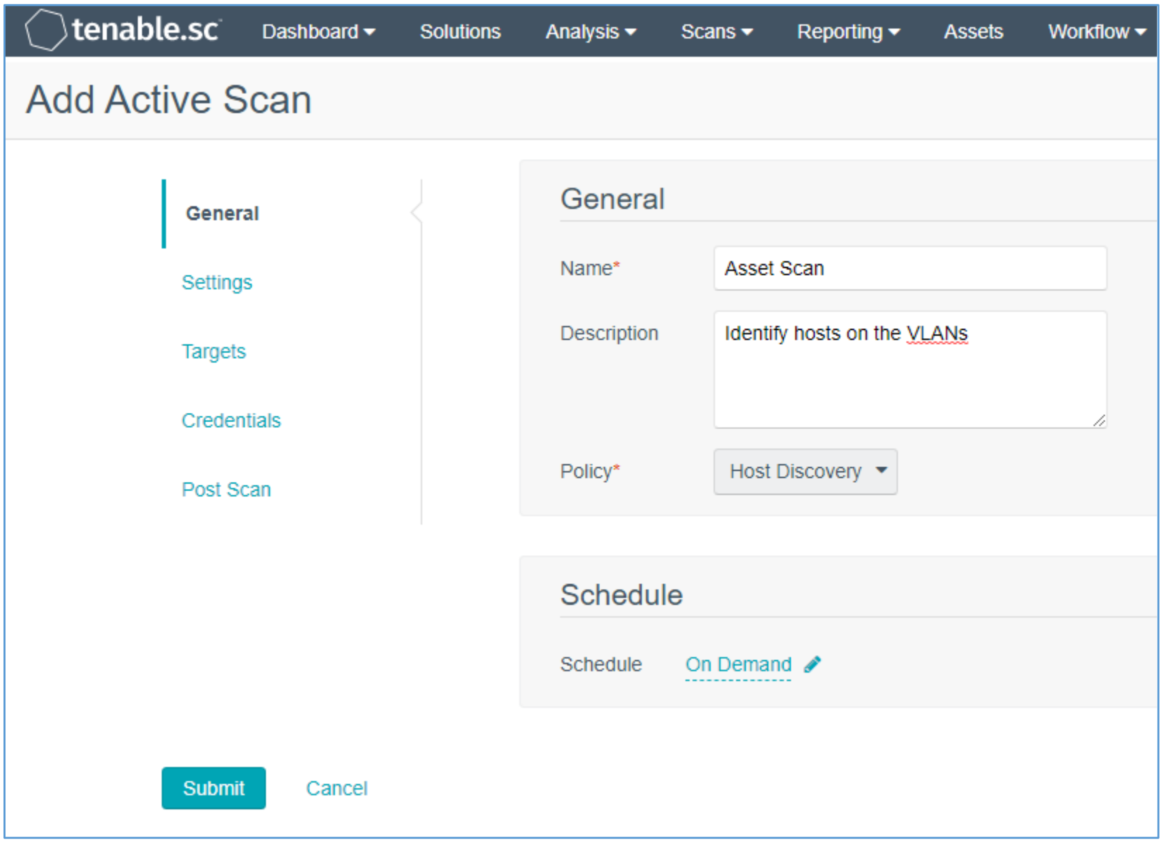
   a. **Name:** Asset Scan
   b. **Description:** Identify hosts on the VLANs
   c. **Policy:** Host Discovery

   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**.



Add Active Scan

General

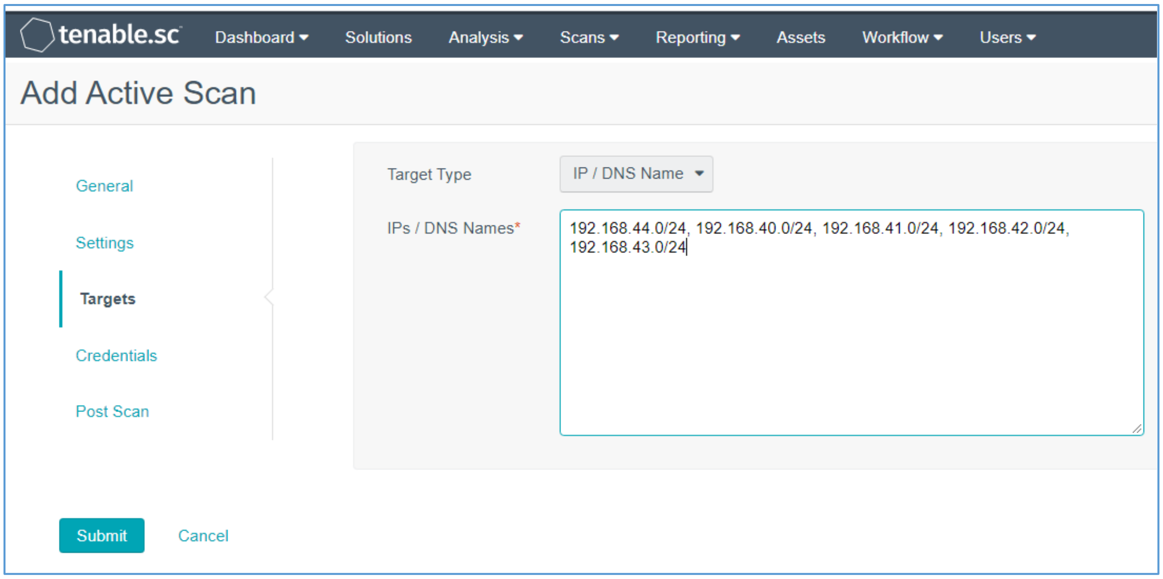
Name* Asset Scan

Description Identify hosts on the VLANs

Policy* Host Discovery

Schedule

Schedule On Demand



Add Active Scan

Target Type: IP / DNS Name

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

Repeat steps in Create Active Scans section for the Basic Network Scan policy. Keep the same value as defined for Active Scan with the exception of 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

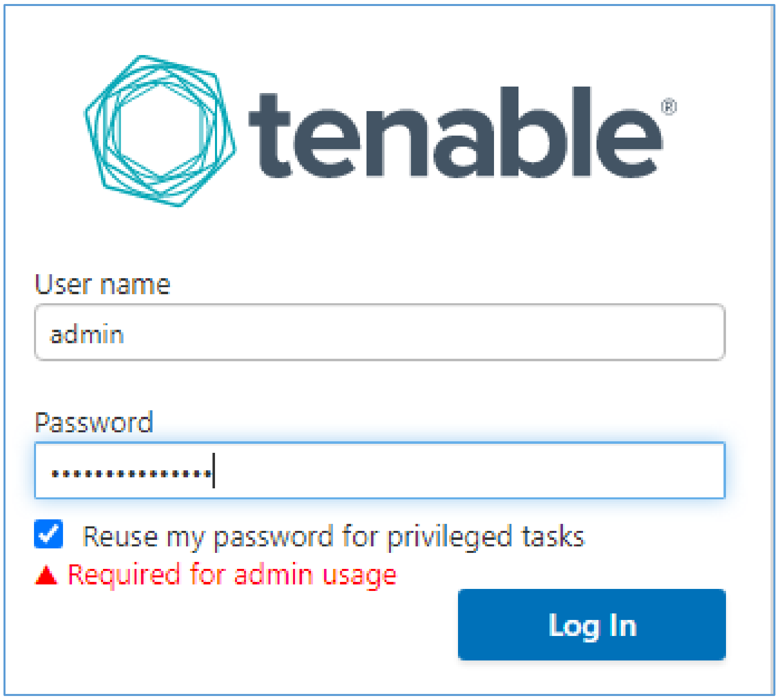
Storage: 82 GB

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.



User name

admin

Password

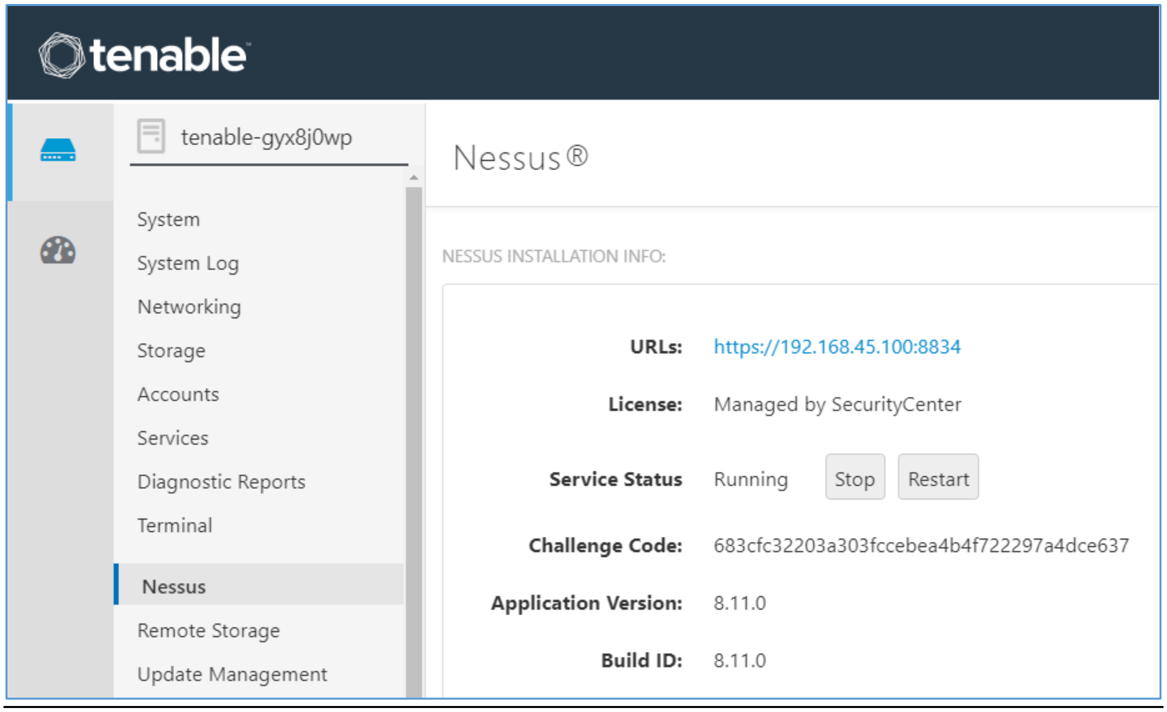
•••••••••••••••

☑ Reuse my password for privileged tasks

▲ Required for admin usage

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

9. To access Tenable.sc, click the **IP address** next to the URL field.



NESSUS INSTALLATION INFO:

URLs: https://192.168.45.100:8834

License: Managed by SecurityCenter

Service Status Running

Challenge Code: 683cfc32203a303fccebea4b4f722297a4dce637

Application Version: 8.11.0

Build ID: 8.11.0

<u>Nessus Configuration</u>

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. This practice guide implemented capabilities in the HDO to address this control category. First, the practice guide implemented Microsoft Active Directory (AD), then installed a domain controller to establish an HDO domain. Next, the practice guide implemented Cisco Firepower as part of its network core infrastructure. The practice guide 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.

<u>Domain Controller Appliance Information</u>

CPU: 4

Random Access Memory (RAM): 8 GB

Storage: 120 GB (Thin Provision)

Network Adapter 1: VLAN 1327

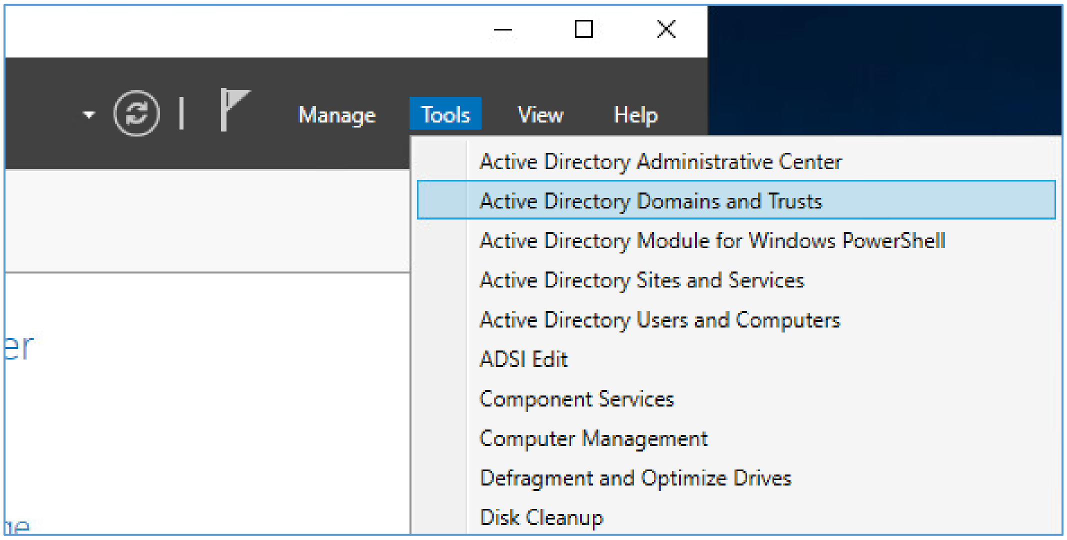
Operating System: Microsoft Windows Server 2019 Datacenter

Domain Controller Appliance Installation Guide

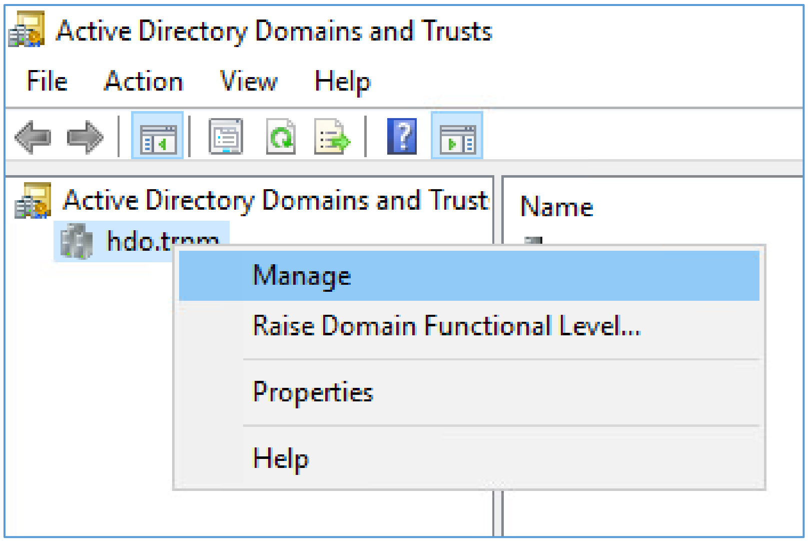
Install the appliance according to the instructions detailed in Microsoft's Install Active Directory Domain Services (Level 100) documentation [4].

Verify Domain Controller Installation

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

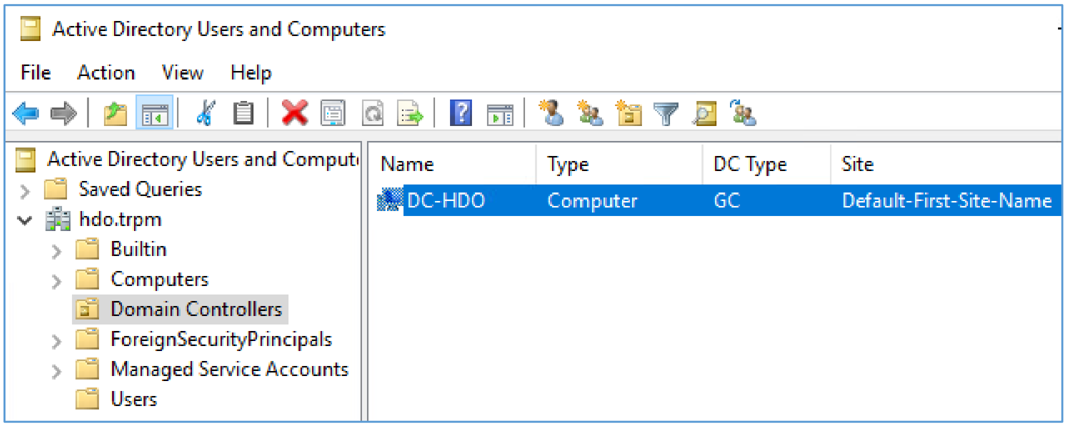

Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup

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


Active Directory Domains and Trusts
File
Action
View
Help
Active Directory Domains and Trust
hdo.trpm
Name
Manage
Raise Domain Functional Level...
Properties
Help

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

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

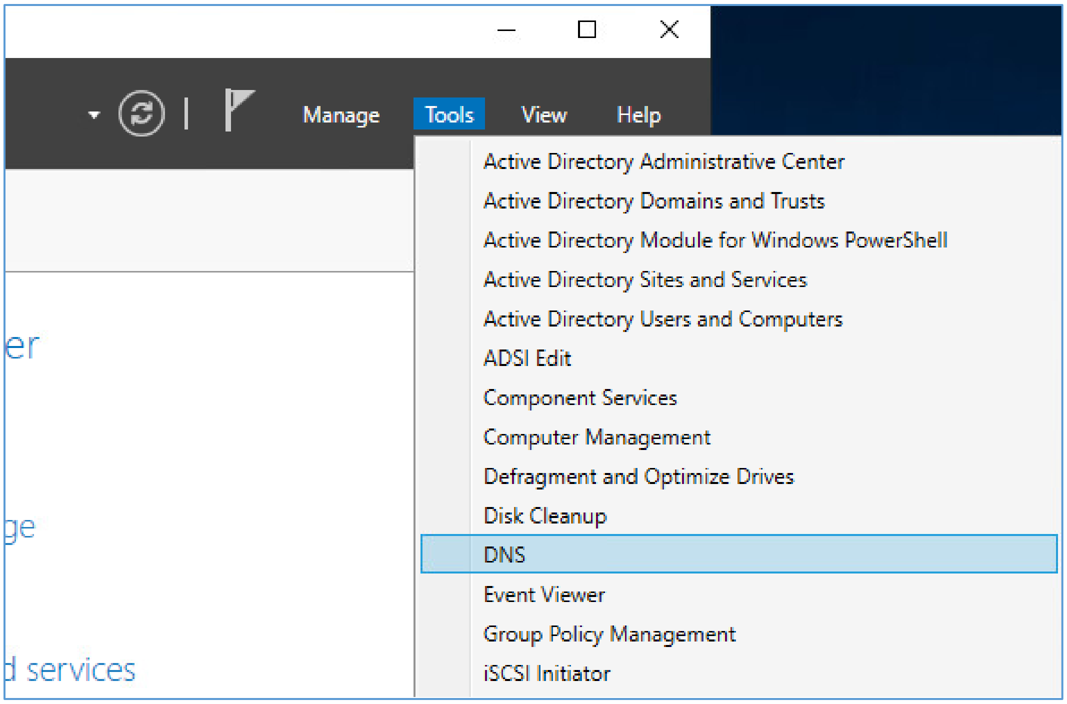


Name	Type	DC Type	Site
DC-HDO	Computer	GC	Default-First-Site-Name

Configure Local DNS

1. Launch Server Manager.

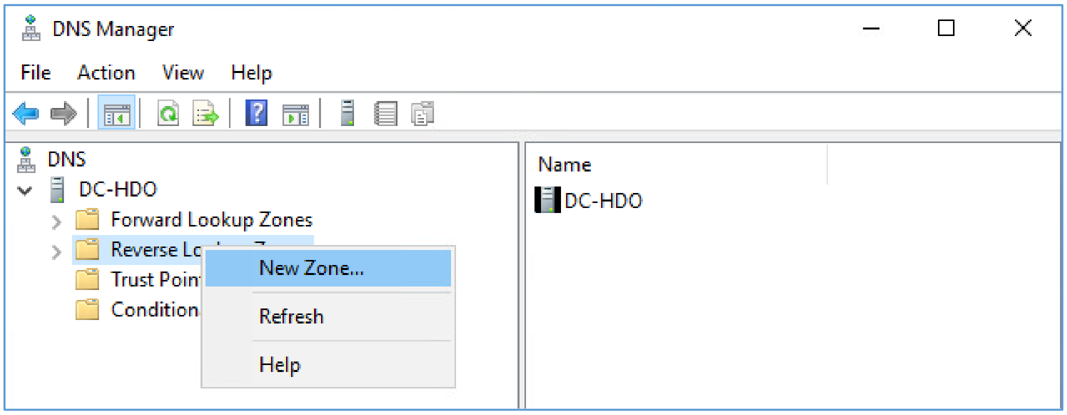
2. Click **Tools > DNS.**


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
er
ge
d services

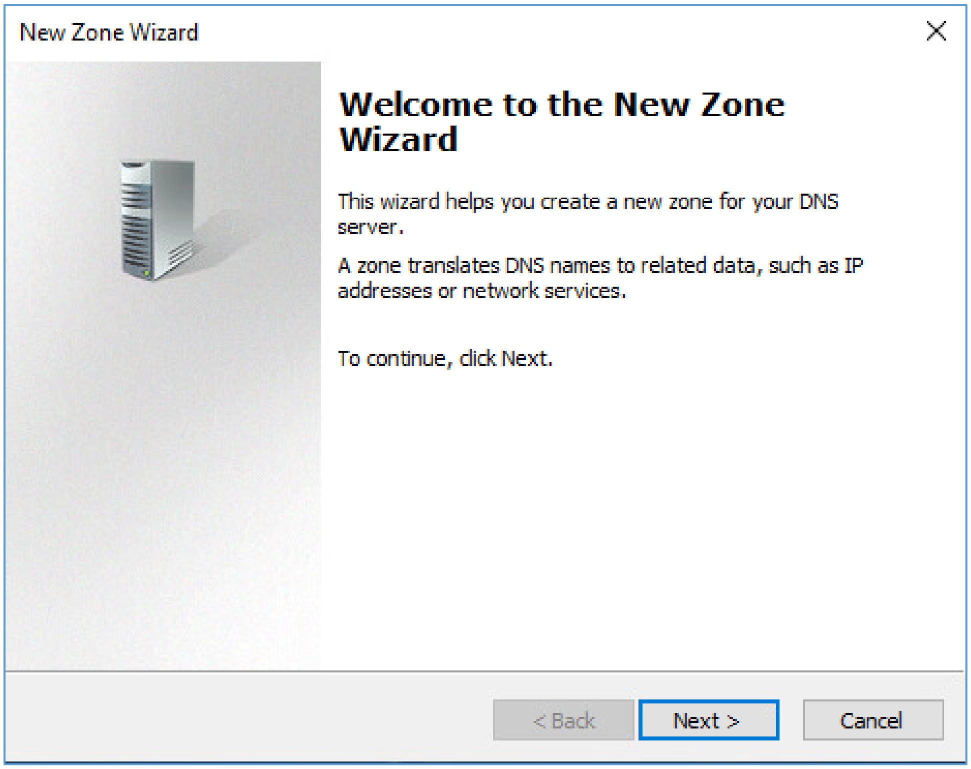
541 3. Click the **arrow symbol** for DC-HDO.

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

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



544 6. Click **Next >**.



New Zone Wizard

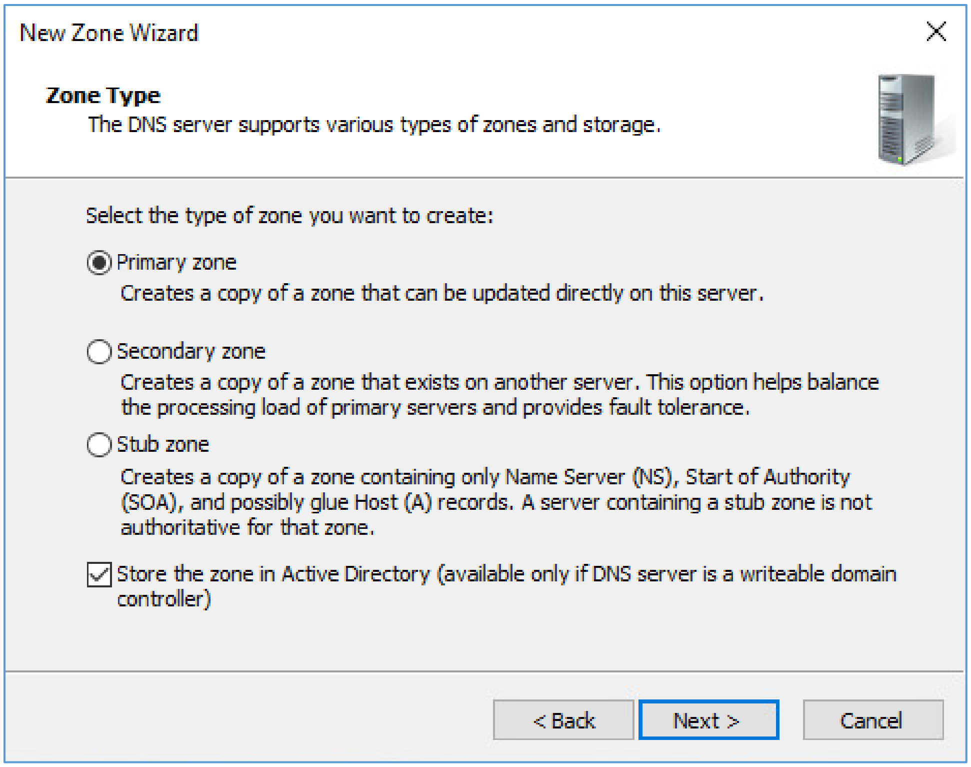
Welcome to the New Zone Wizard

This wizard helps you create a new zone for your DNS server.

A zone translates DNS names to related data, such as IP addresses or network services.

To continue, click Next.

7. Click **Primary zone**.
8. Check **Store the zone in Active Directory**.
9. Click **Next >**.



New Zone Wizard

Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

● Primary zone

Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone

Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

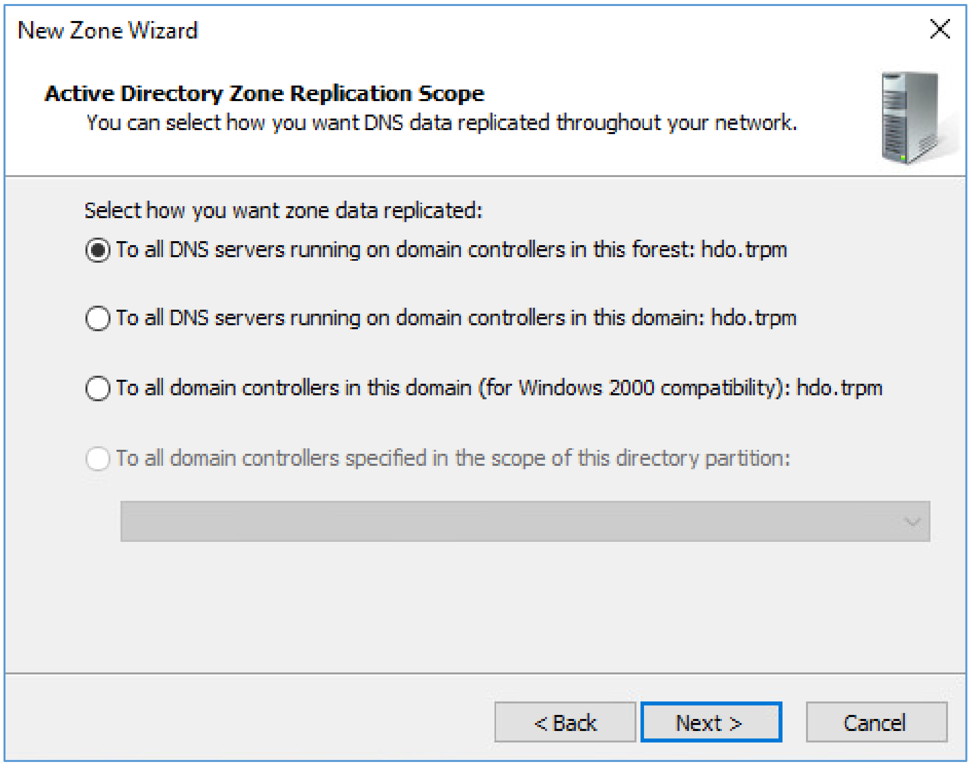
○ Stub zone

Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

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

549 11. Click **Next >**.



New Zone Wizard

Active Directory Zone Replication Scope

You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

● To all DNS servers running on domain controllers in this forest: hdo.trpm

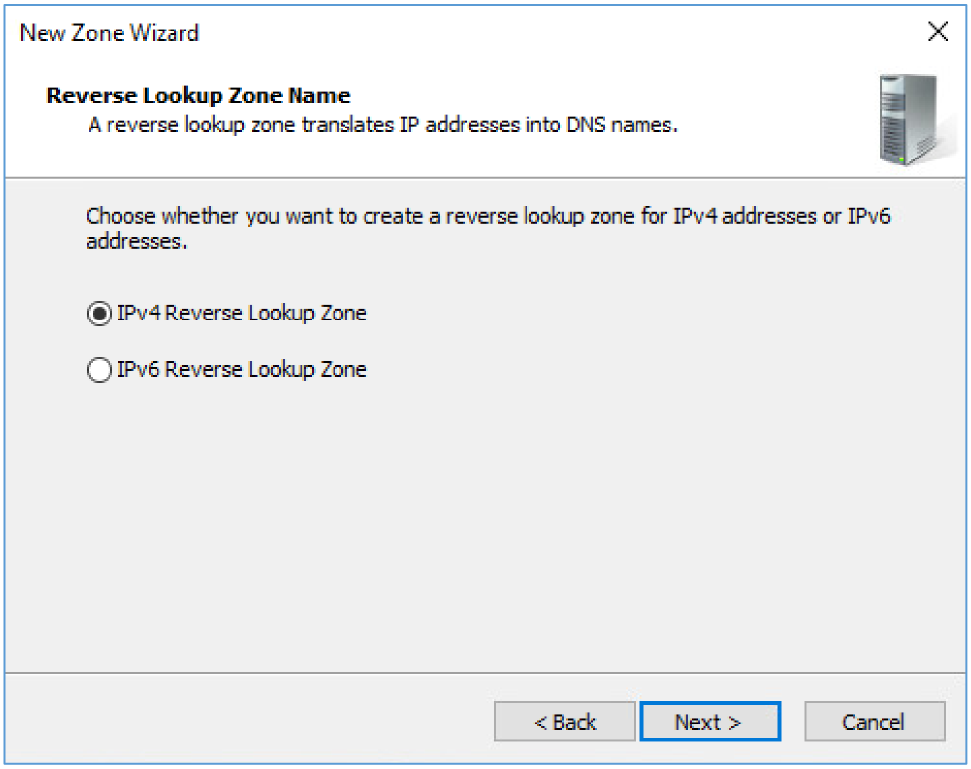
○ To all DNS servers running on domain controllers in this domain: hdo.trpm

○ To all domain controllers in this domain (for Windows 2000 compatibility): hdo.trpm

○ To all domain controllers specified in the scope of this directory partition:

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

551 13. Click **Next >**.



New Zone Wizard

Reverse Lookup Zone Name

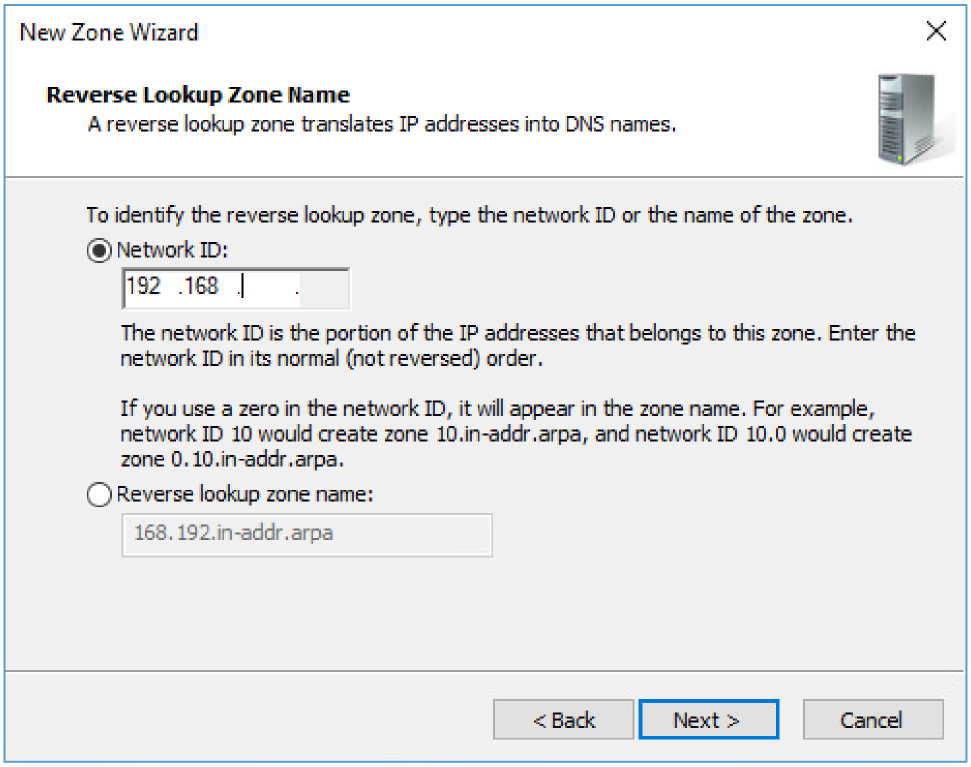
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

● IPv4 Reverse Lookup Zone

○ IPv6 Reverse Lookup Zone

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



New Zone Wizard

Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

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

● Network ID:

192 .168 .

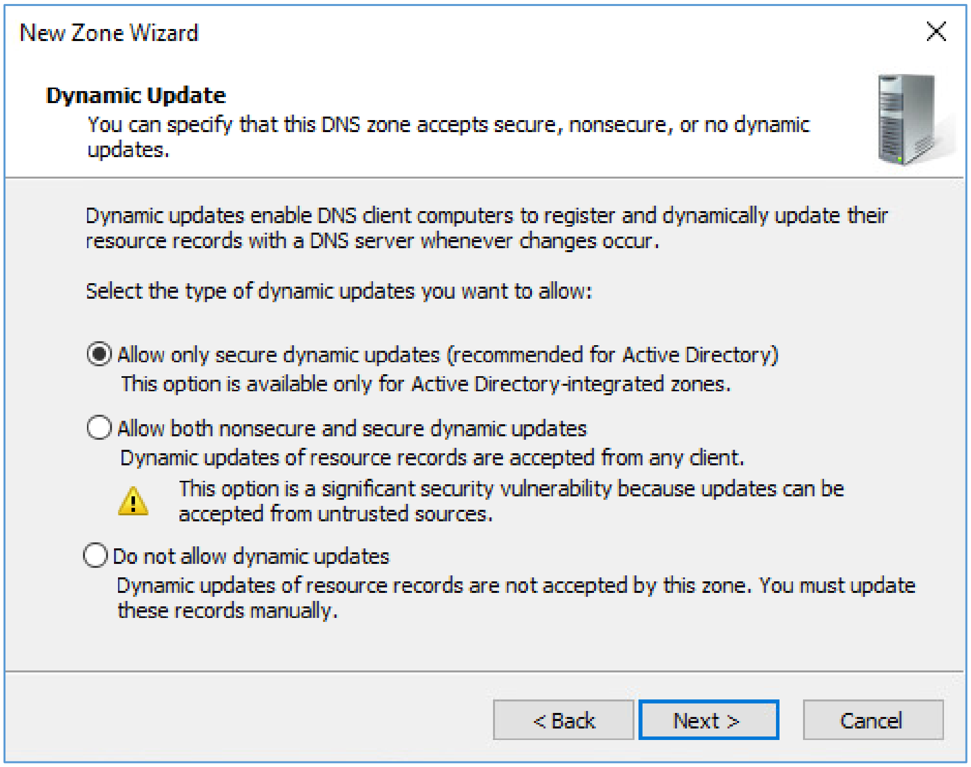
The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

○ Reverse lookup zone name:

168.192.in-addr.arpa

17. Check **Allow only secure dynamic updates**.
18. Click **Next >**.



New Zone Wizard

Dynamic Update

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

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

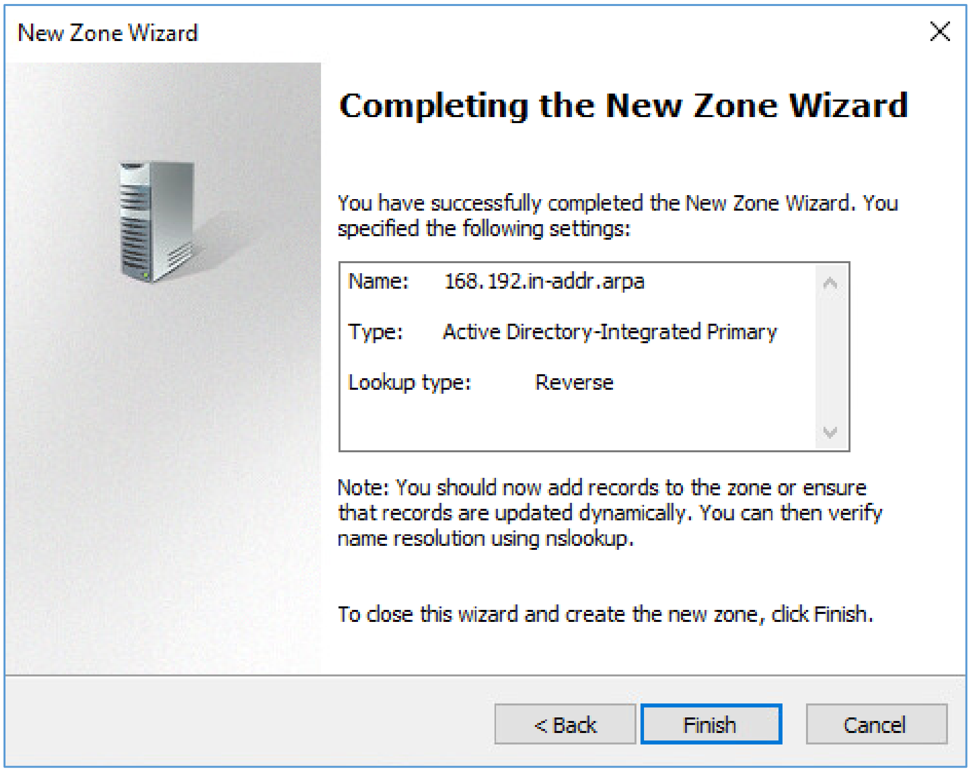
Select the type of dynamic updates you want to allow:

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

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

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

557 19. Click **Finish**.



New Zone Wizard

Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name: 168.192.in-addr.arpa

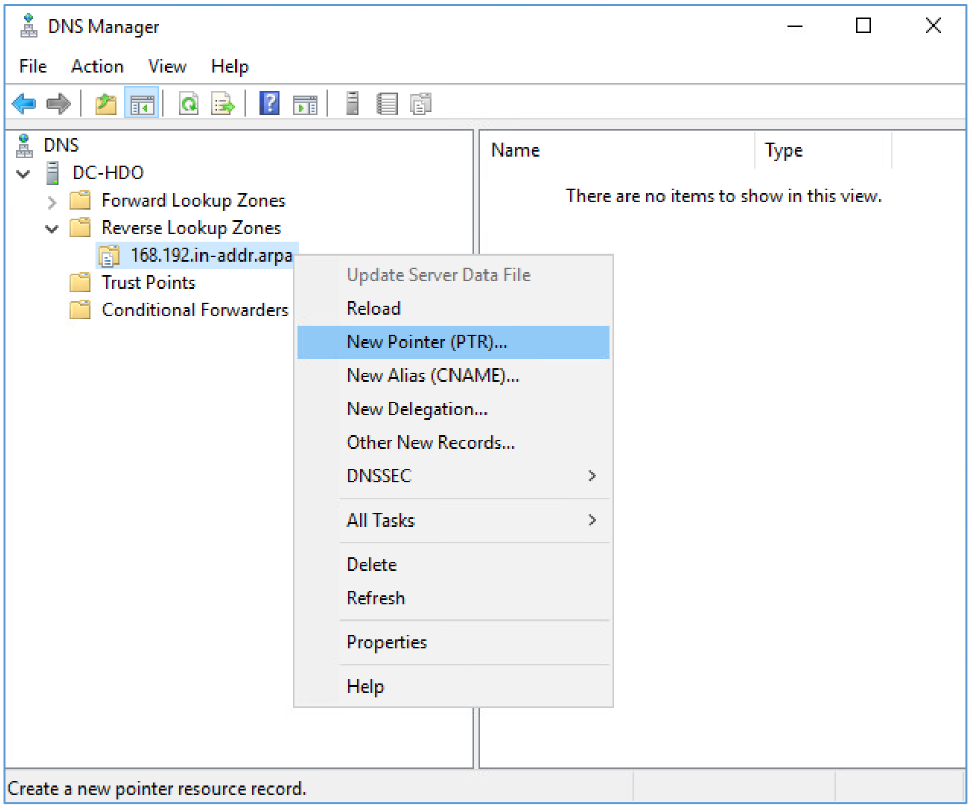
Type: Active Directory-Integrated Primary

Lookup type: Reverse

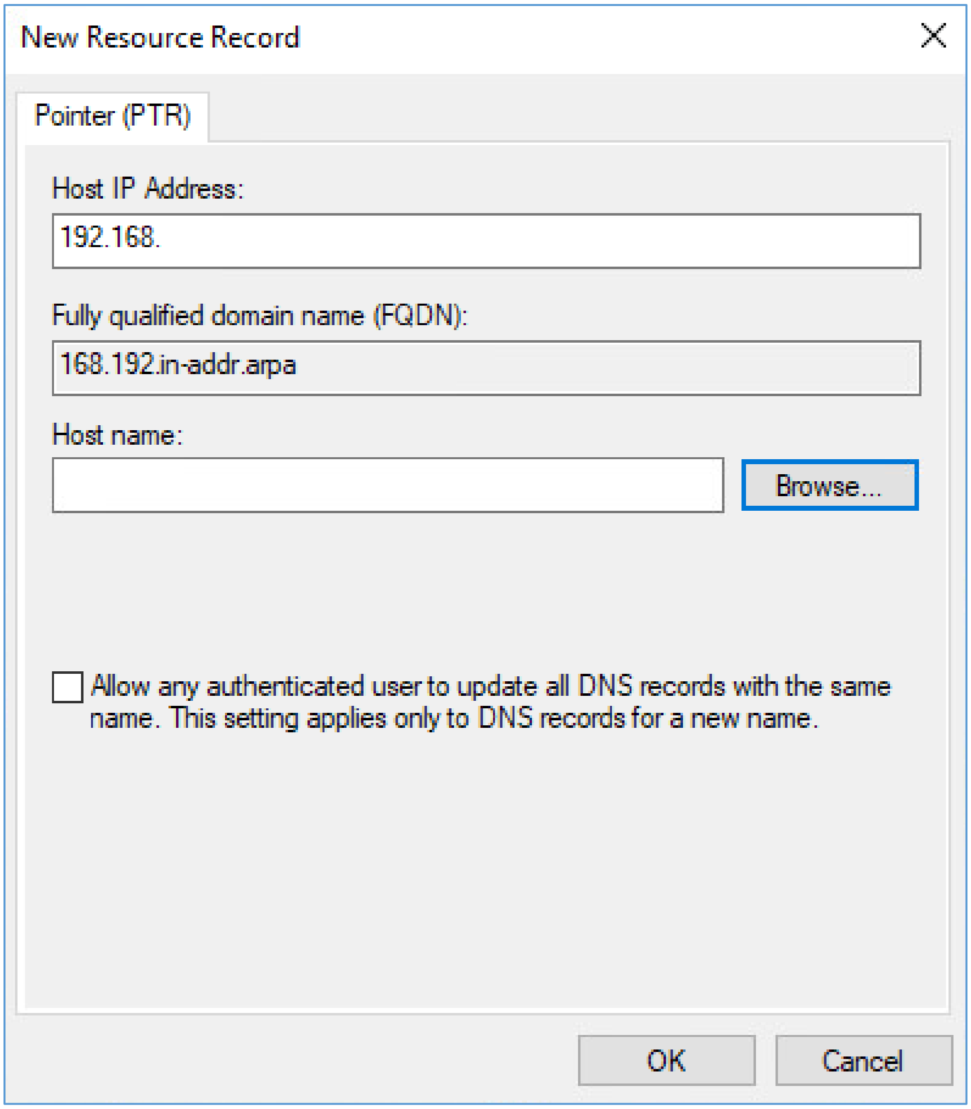
Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

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



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



New Resource Record

Pointer (PTR)

Host IP Address:

192.168.

Fully qualified domain name (FQDN):

168.192.in-addr.arpa

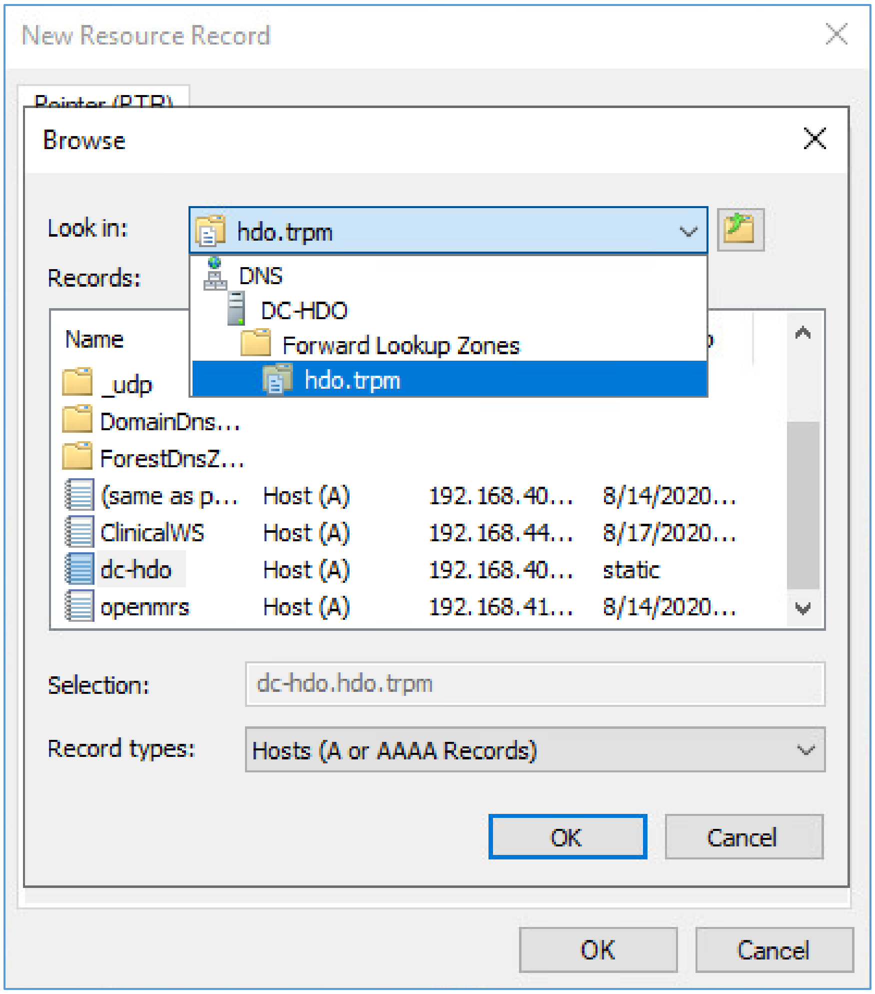
Host name:

☐ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

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

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

564 26. Click **OK**.



Look in: hdo.trpm

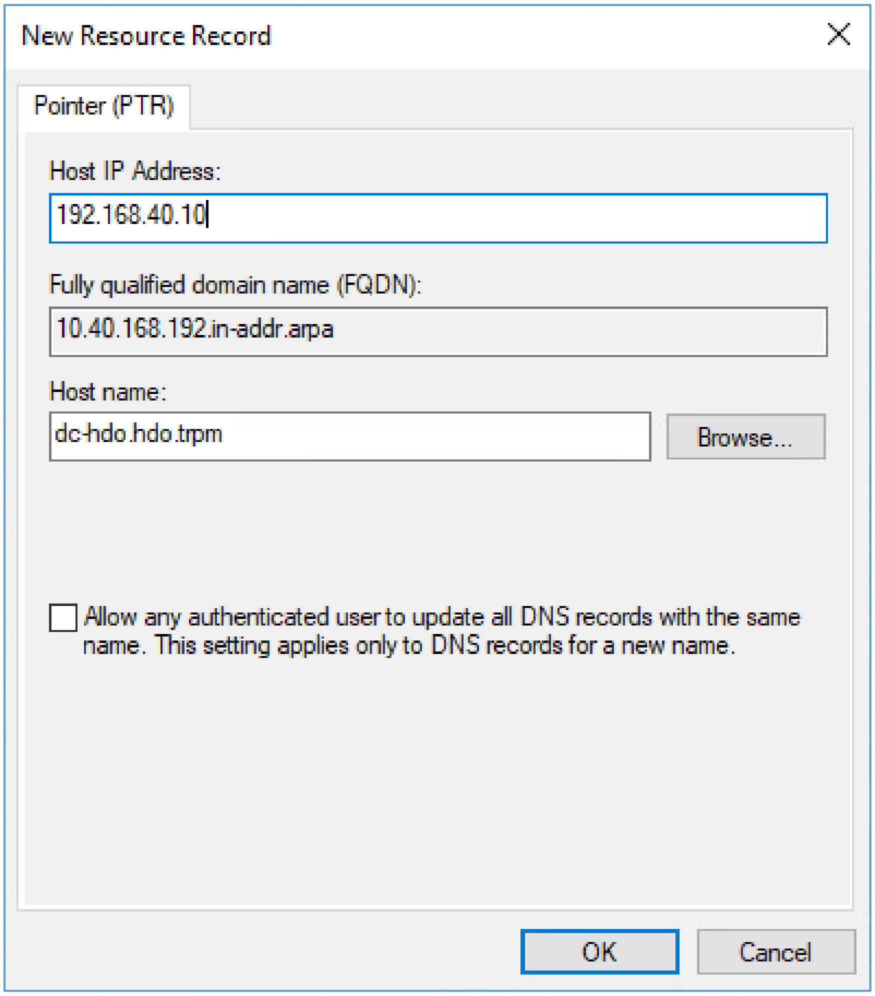
Records:

Name			
_udp			
DomainDns...			
ForestDnsZ...			
(same as p...	Host (A)	192.168.40...	8/14/2020...
ClinicalWS	Host (A)	192.168.44...	8/17/2020...
dc-hdo	Host (A)	192.168.40...	static
openmrs	Host (A)	192.168.41...	8/14/2020...

Selection: dc-hdo.hdo.trpm

Record types: Hosts (A or AAAA Records)

565 27. Click **OK**.



New Resource Record

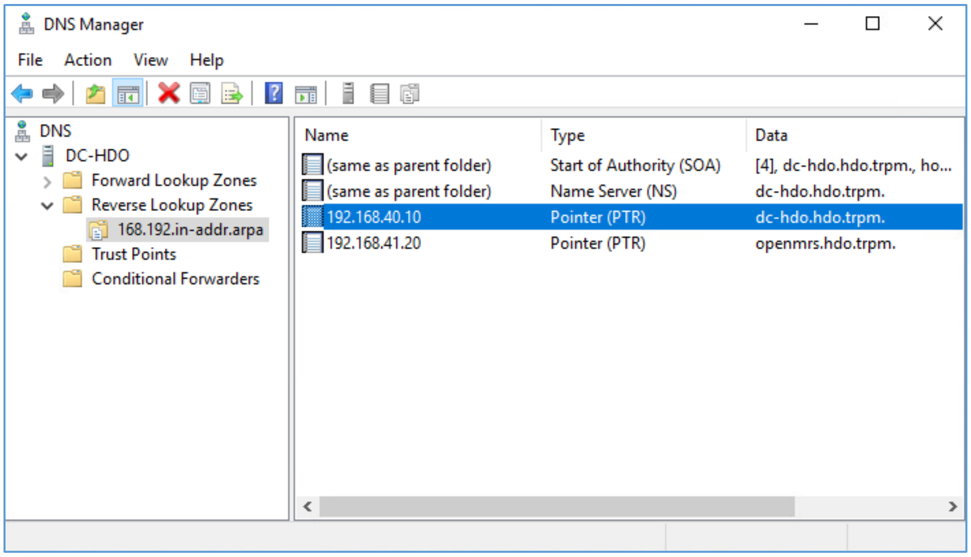
Pointer (PTR)

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

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[4], dc-hdo.hdo.trpm., ho...
(same as parent folder)	Name Server (NS)	dc-hdo.hdo.trpm.
192.168.40.10	Pointer (PTR)	dc-hdo.hdo.trpm.
192.168.41.20	Pointer (PTR)	openmrs.hdo.trpm.

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

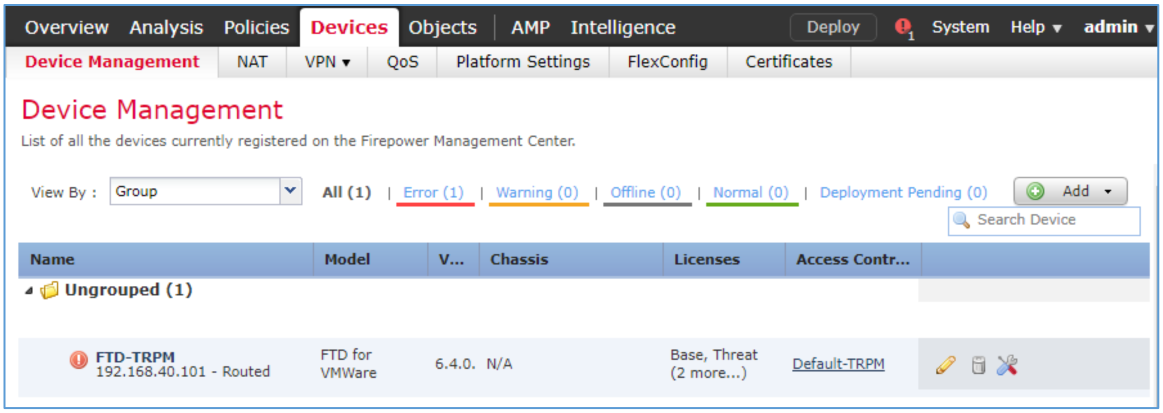
Cisco FTD Installation Guide

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.



Device Management

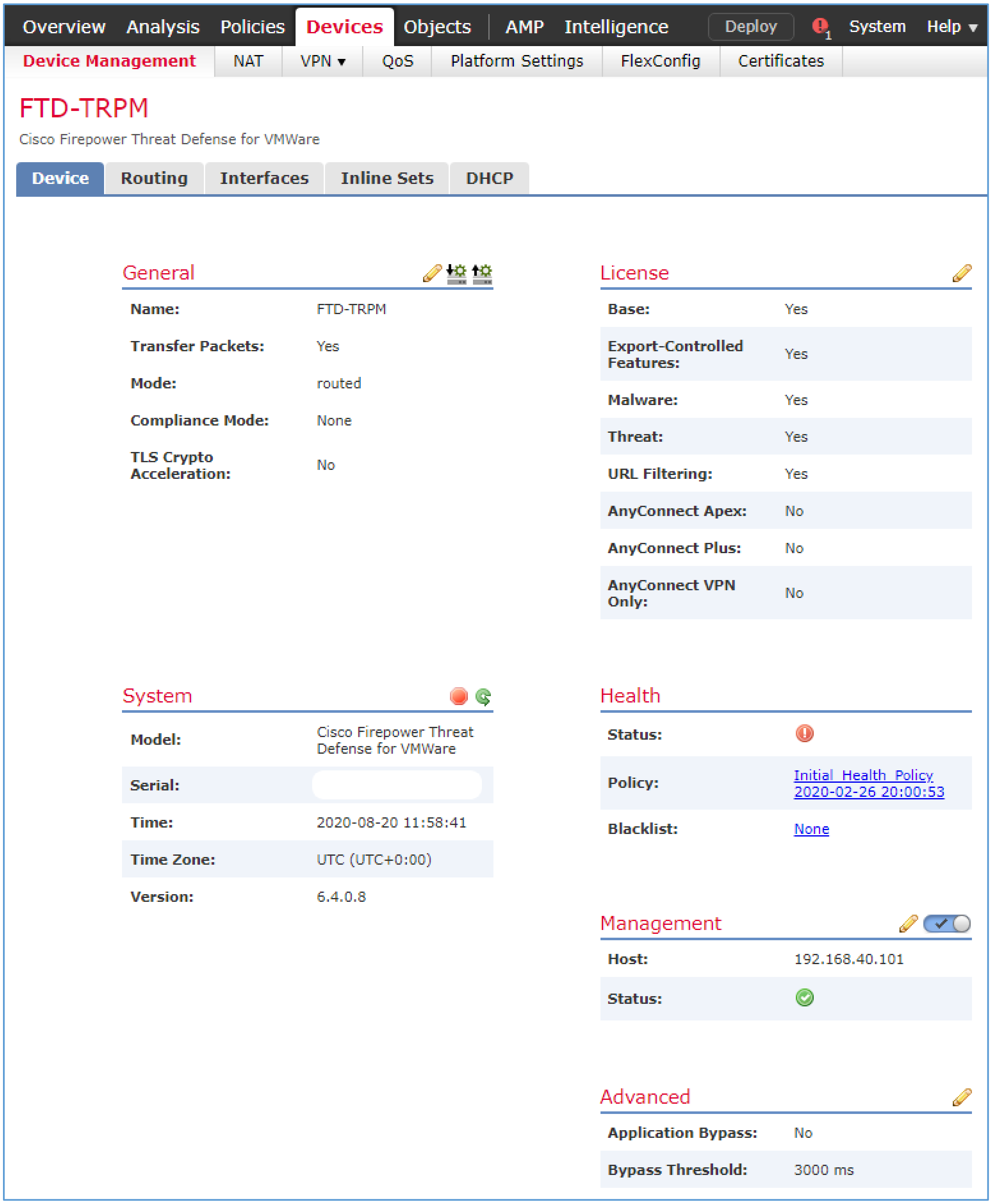
List of all the devices currently registered on the Firepower Management Center.

View By : Group

All (1) | Error (1) | Warning (0) | Offline (0) | Normal (0) | Deployment Pending (0)

Name	Model	V...	Chassis	Licenses	Access Contr...
Ungrouped (1)					
FTD-TRPM 192.168.40.101 - Routed	FTD for VMWare	6.4.0.	N/A	Base, Threat (2 more...)	Default-TRPM

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**.



FTD-TRPM

Cisco Firepower Threat Defense for VMWare

General

Name: FTD-TRPM

Transfer Packets: Yes

Mode: routed

Compliance Mode: None

TLS Crypto Acceleration: No

License

Base: Yes

Export-Controlled Features: Yes

Malware: Yes

Threat: Yes

URL Filtering: Yes

AnyConnect Apex: No

AnyConnect Plus: No

AnyConnect VPN Only: No

System

Model: Cisco Firepower Threat Defense for VMWare

Serial:

Time: 2020-08-20 11:58:41

Time Zone: UTC (UTC+0:00)

Version: 6.4.0.8

Health

Status: ❗

Policy: Initial_Health_Policy 2020-02-26 20:00:53

Blacklist: None

Management

Host: 192.168.40.101

Status: ✓

Advanced

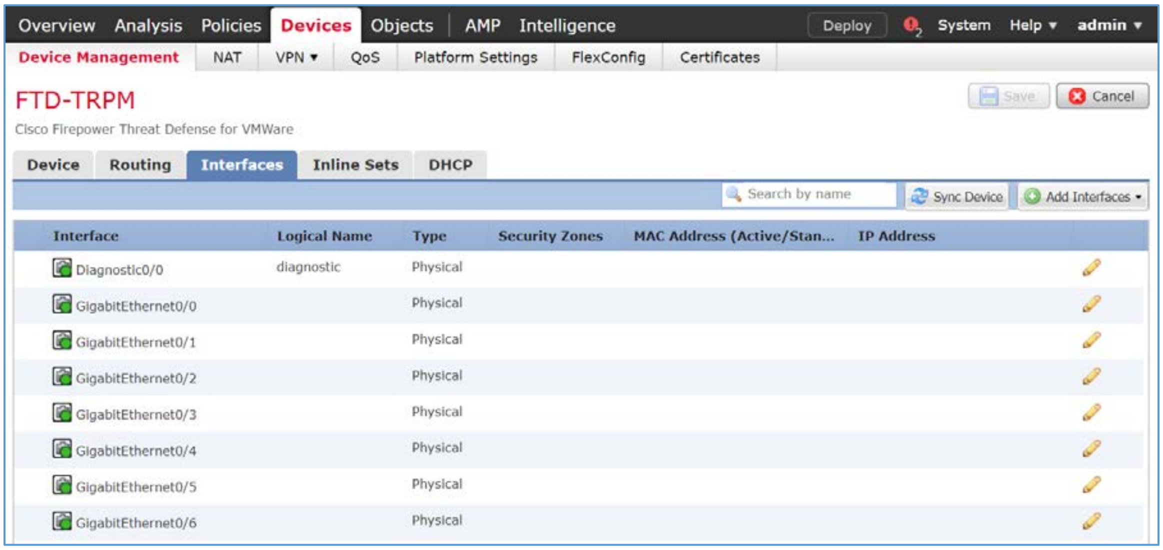
Application Bypass: No

Bypass Threshold: 3000 ms

Configure Cisco FTD Interfaces for the RPM Architecture

By default, each of the Interfaces are defined as GigabitEthernet, and are denoted as 0 through 6.

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

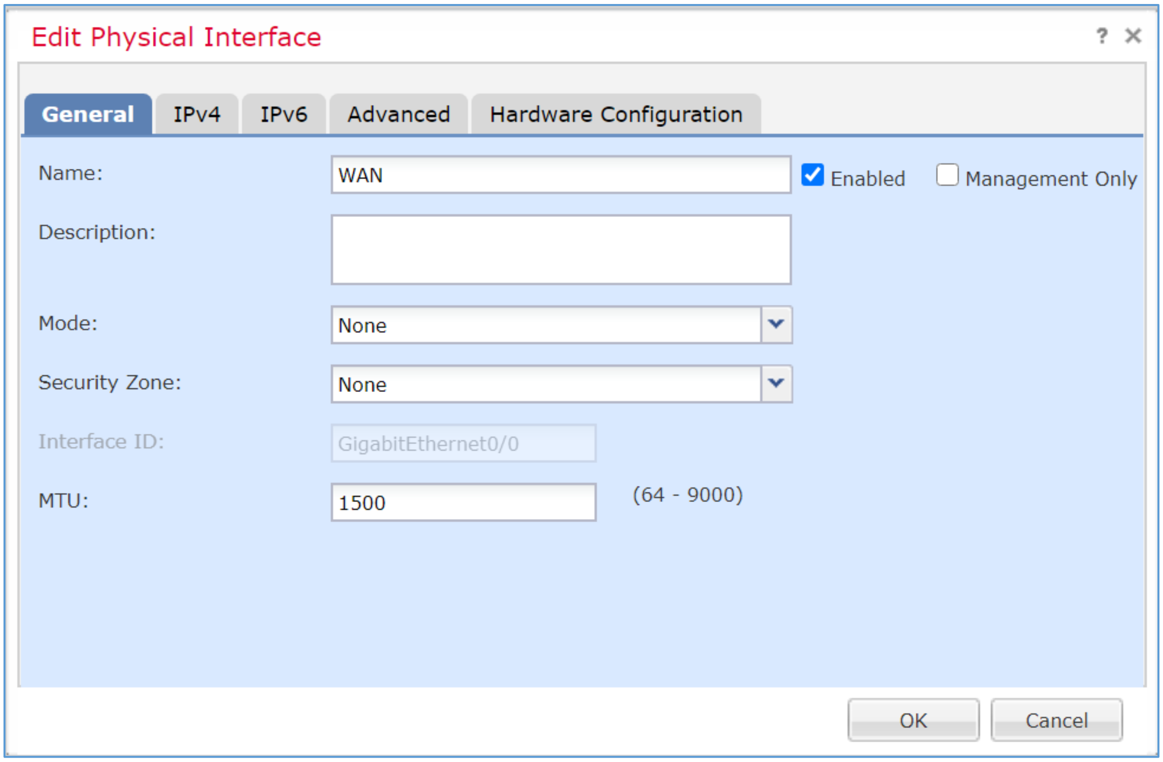


FTD-TRPM

Cisco Firepower Threat Defense for VMWare

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stan...	IP Address	
Diagnostic0/0	diagnostic	Physical				✎
GigabitEthernet0/0		Physical				✎
GigabitEthernet0/1		Physical				✎
GigabitEthernet0/2		Physical				✎
GigabitEthernet0/3		Physical				✎
GigabitEthernet0/4		Physical				✎
GigabitEthernet0/5		Physical				✎
GigabitEthernet0/6		Physical				✎

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



Edit Physical Interface

Name: WAN ☑ Enabled □ Management Only

Description:

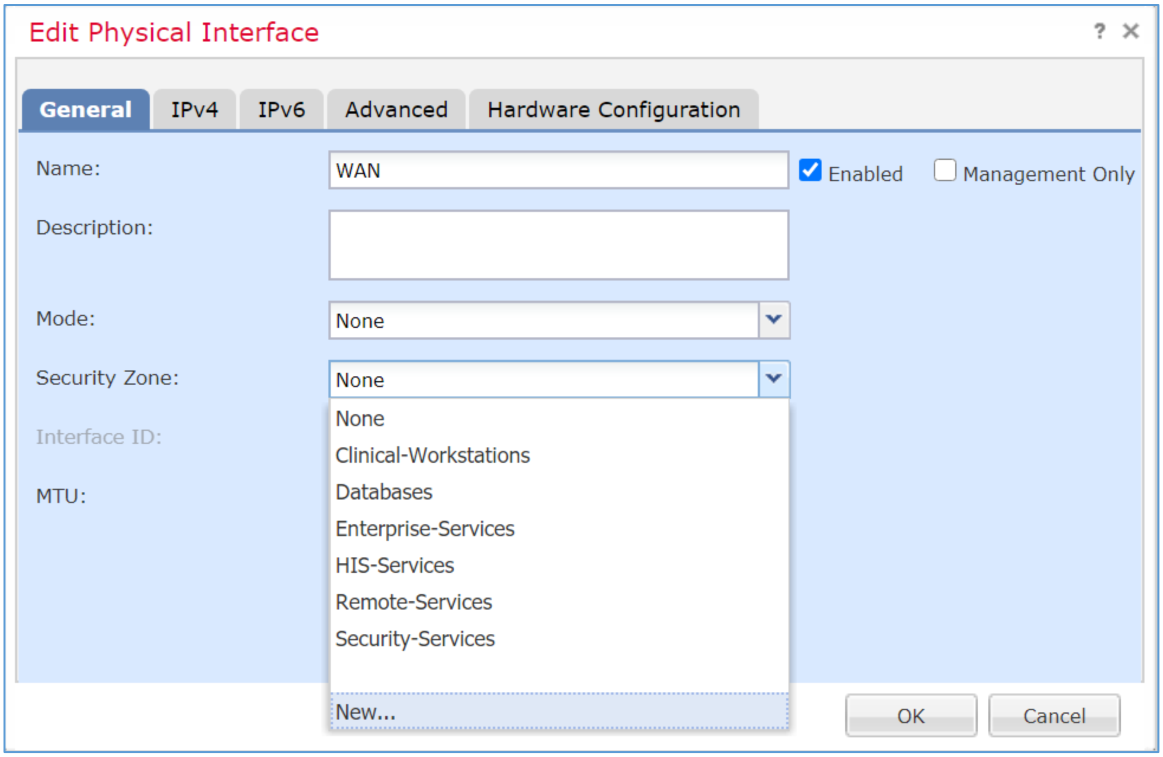
Mode: None

Security Zone: None

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

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



Name: WAN ☑ Enabled □ Management Only

Description:

Mode: None

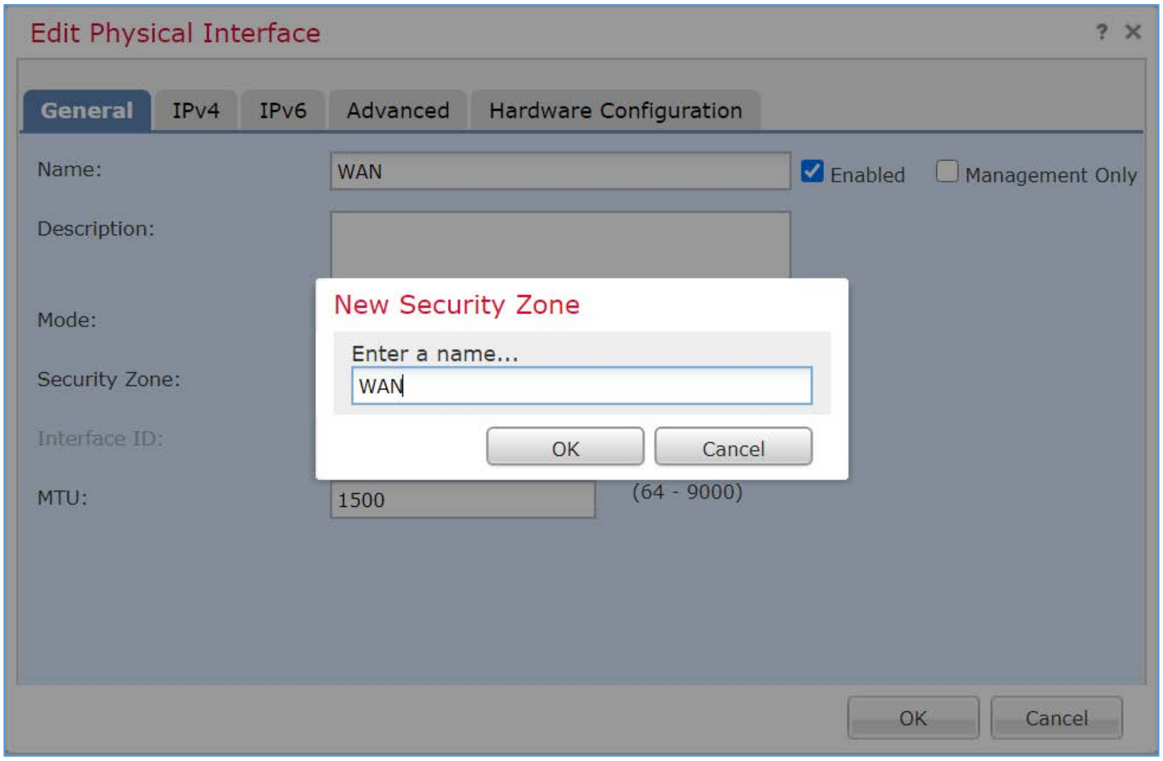
Security Zone: None

Interface ID:

MTU:

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

6. Click **OK**.



Edit Physical Interface

Name: WAN ☑ Enabled □ Management Only

Description:

Mode:

Security Zone:

Interface ID:

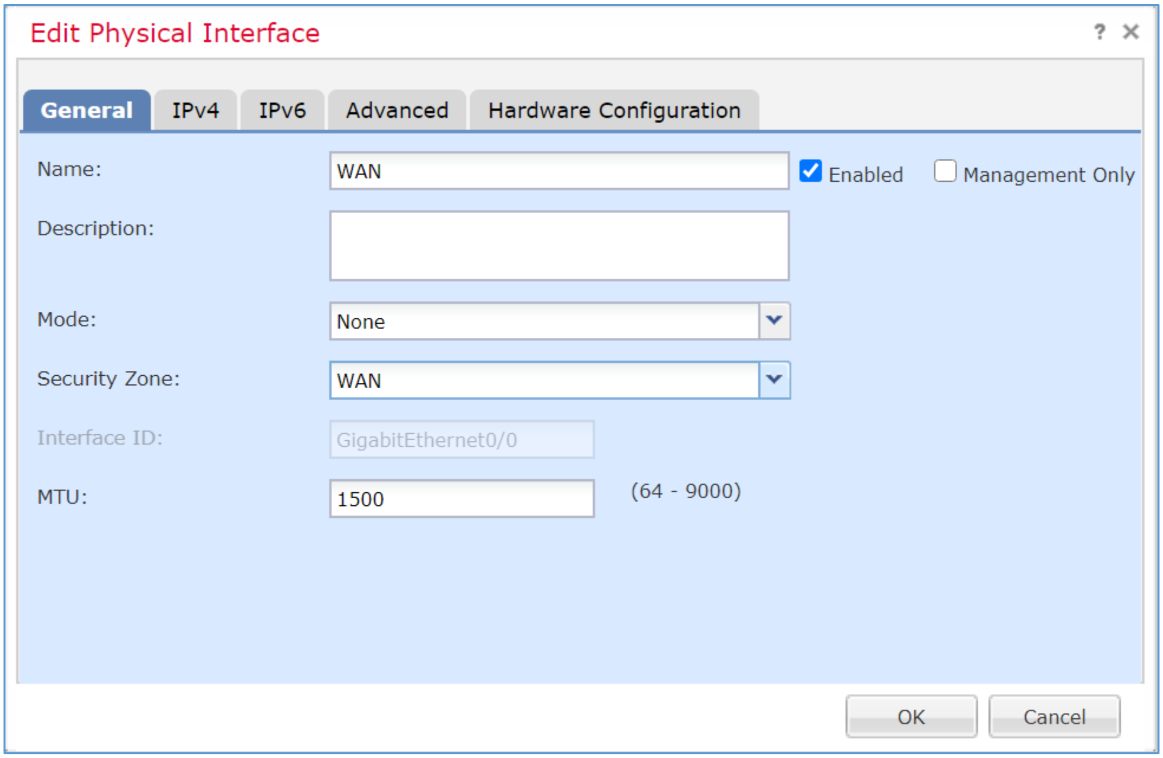
MTU: 1500 (64 - 9000)

New Security Zone

Enter a name...

WAN

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



Name: WAN ☑ Enabled ☐ Management Only

Description:

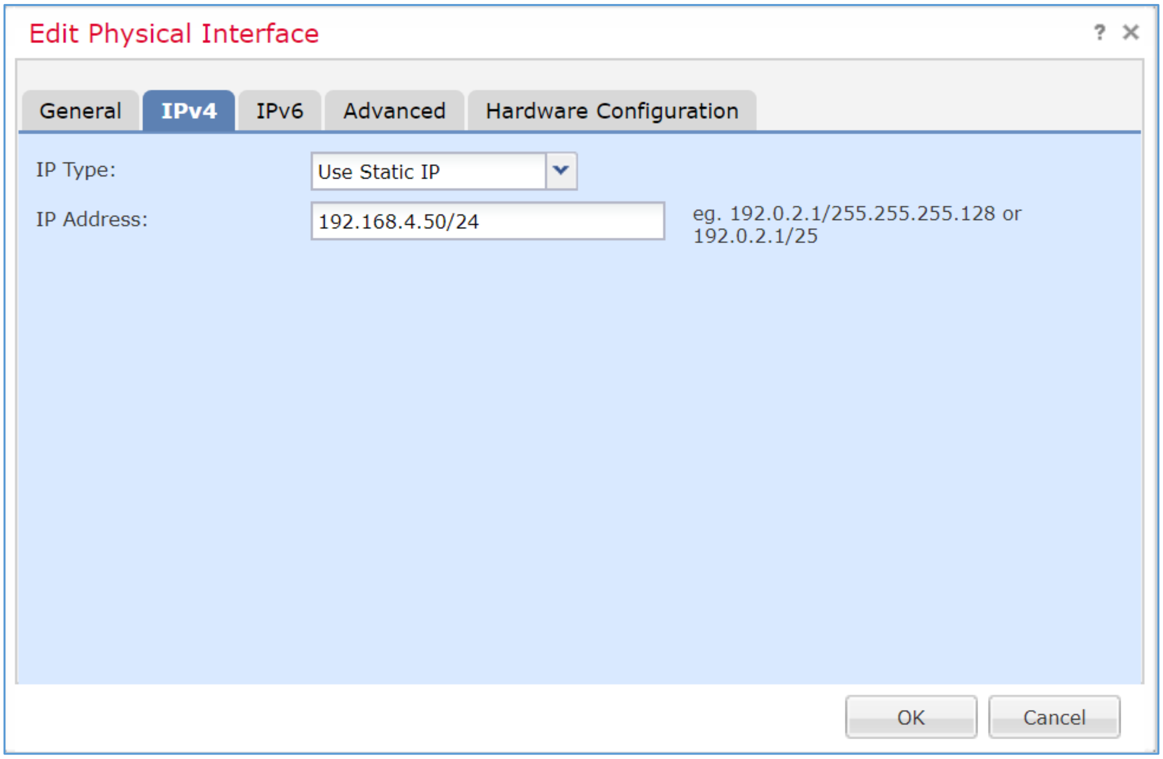
Mode: None

Security Zone: WAN

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

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



IP Type: Use Static IP

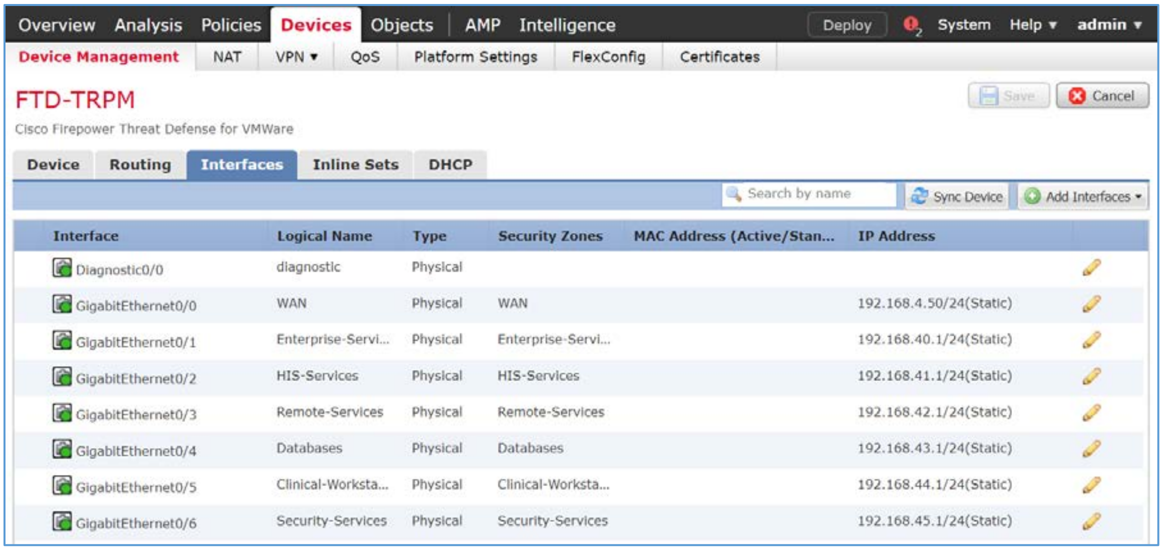
IP Address: 192.168.4.50/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

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

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


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy
System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
Save
Cancel
Device Routing Interfaces Inline Sets DHCP
Search by name
Sync Device
Add Interfaces ▾

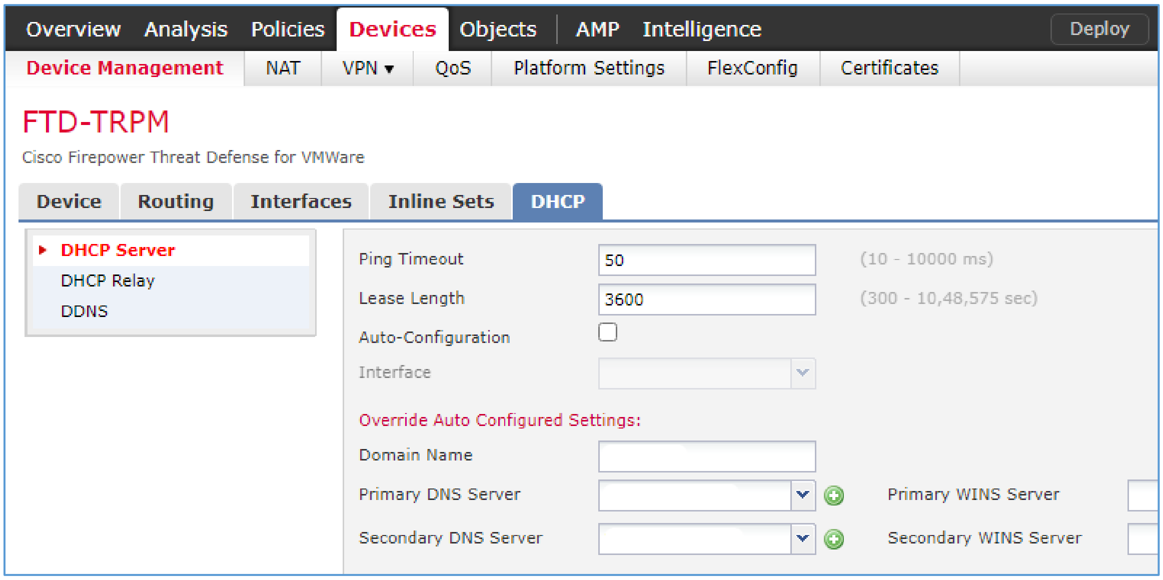
FTD-TRPM

Cisco Firepower Threat Defense for VMWare

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Stan...	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	WAN	Physical	WAN		192.168.4.50/24(Static)
GigabitEthernet0/1	Enterprise-Servi...	Physical	Enterprise-Servi...		192.168.40.1/24(Static)
GigabitEthernet0/2	HIS-Services	Physical	HIS-Services		192.168.41.1/24(Static)
GigabitEthernet0/3	Remote-Services	Physical	Remote-Services		192.168.42.1/24(Static)
GigabitEthernet0/4	Databases	Physical	Databases		192.168.43.1/24(Static)
GigabitEthernet0/5	Clinical-Worksta...	Physical	Clinical-Worksta...		192.168.44.1/24(Static)
GigabitEthernet0/6	Security-Services	Physical	Security-Services		192.168.45.1/24(Static)

Configure Cisco FTD DHCP

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


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
Device Routing Interfaces Inline Sets DHCP
DHCP Server
DHCP Relay
DDNS

FTD-TRPM

Cisco Firepower Threat Defense for VMWare

Ping Timeout: 50 (10 - 10000 ms)

Lease Length: 3600 (300 - 10,48,575 sec)

Auto-Configuration: □

Interface:

Override Auto Configured Settings:

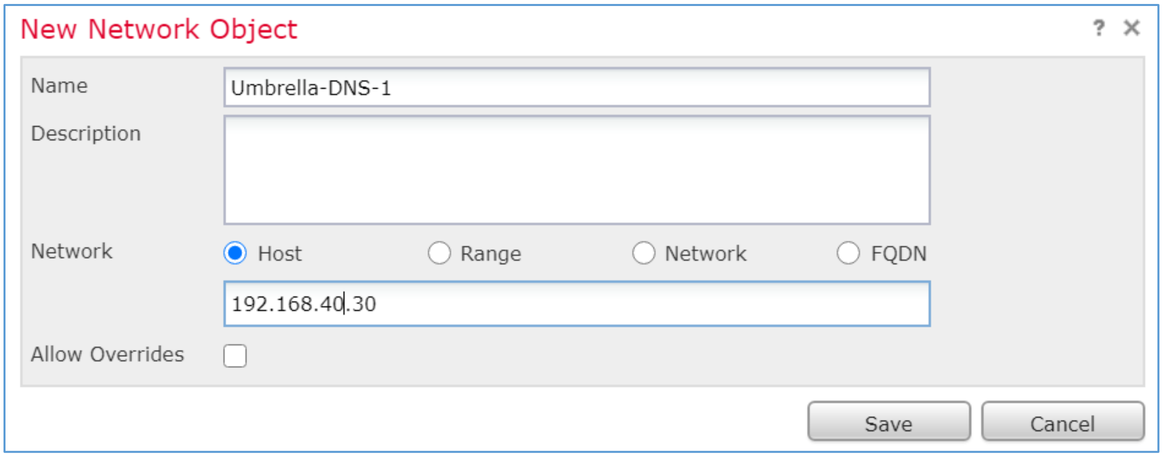
Domain Name:

Primary DNS Server: Primary WINS Server:

Secondary DNS Server: Secondary WINS Server:

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

4. Click **Save.**



New Network Object

Name: Umbrella-DNS-1

Description:

Network: ● Host ○ Range ○ Network ○ FQDN

192.168.40.30

Allow Overrides □

5. Click the **plus symbol** next to **Secondary DNS Server**.

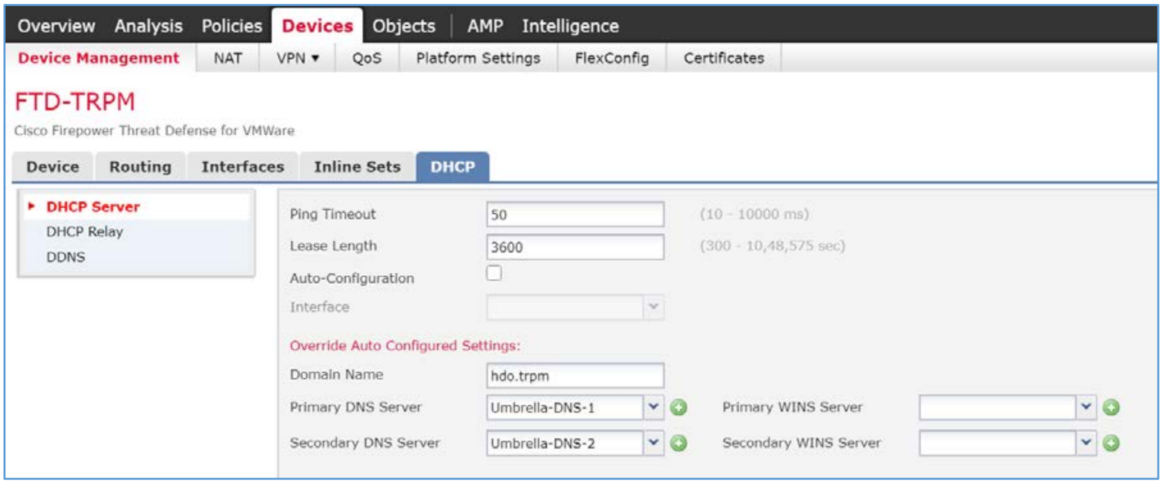
6. The New Network Object popup window appears. Fill out the following information:

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

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

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

8. Click **Add Server**.



FTD-TRPM

Cisco Firepower Threat Defense for VMWare

Ping Timeout: 50 (10 - 10000 ms)

Lease Length: 3600 (300 - 10,48,575 sec)

Auto-Configuration □

Interface

Override Auto Configured Settings:

Domain Name: hdo.trpm

Primary DNS Server: Umbrella-DNS-1

Secondary DNS Server: Umbrella-DNS-2

Primary WINS Server:

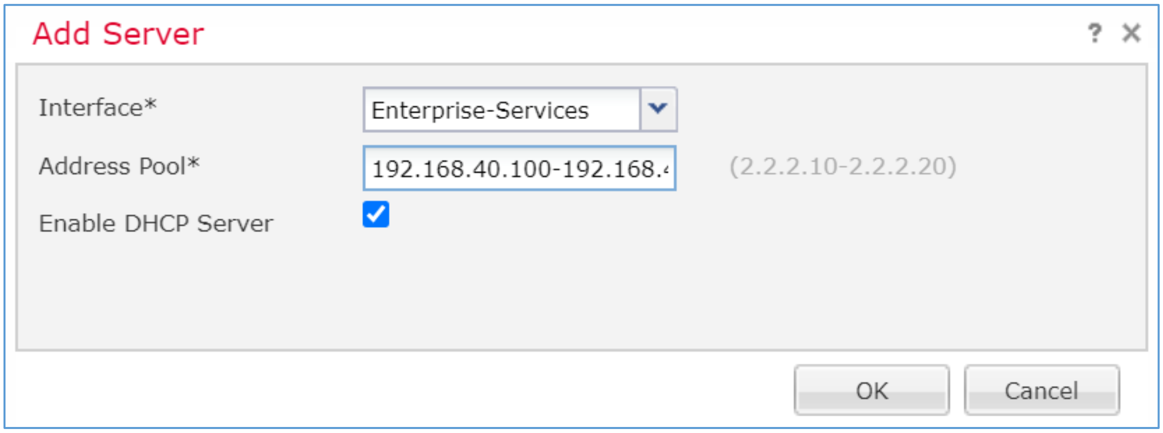
Secondary WINS Server:

9. The Add Server popup 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**.



Add Server

Interface* Enterprise-Services

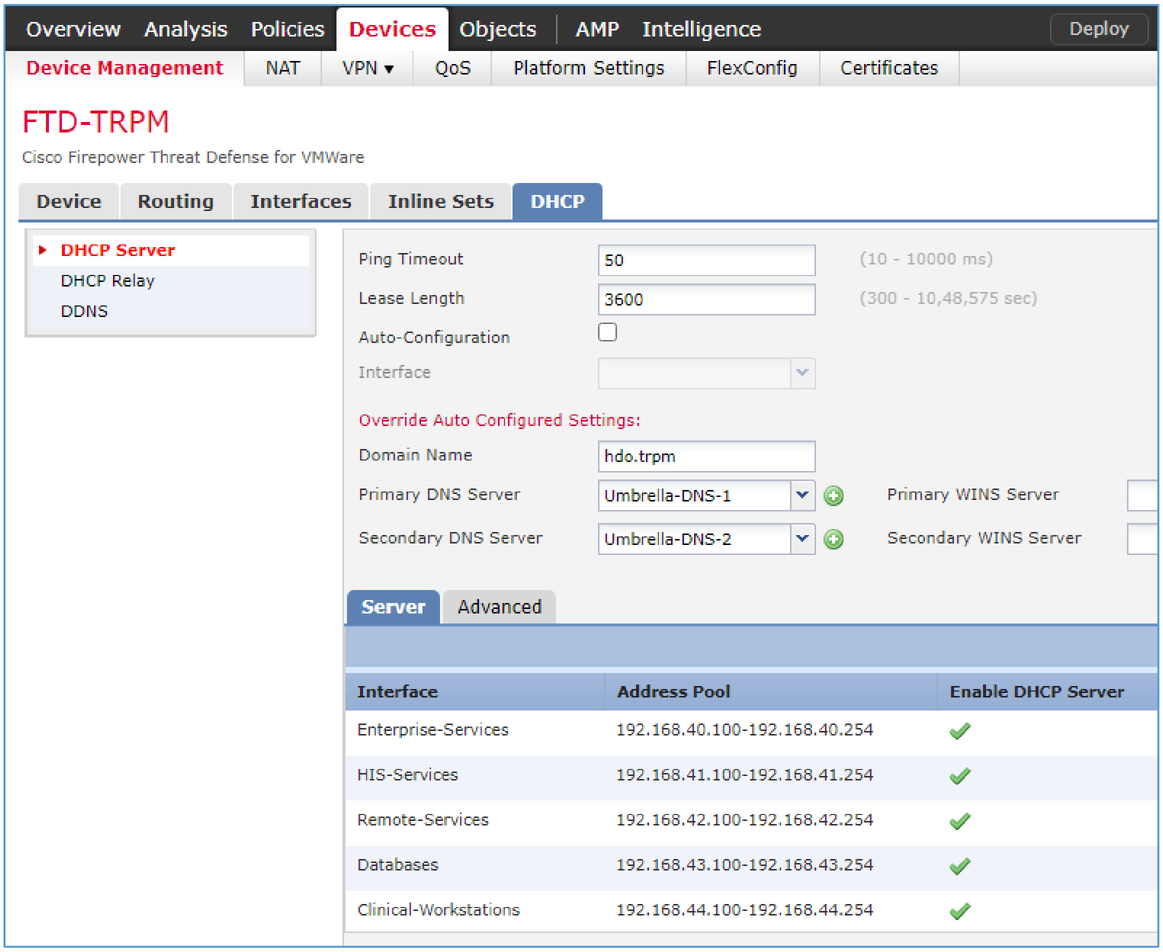
Address Pool* 192.168.40.100-192.168.4 (2.2.2.10-2.2.2.20)

Enable DHCP Server ☑

11. Add additional servers following the same pattern described above, populating the respective Interface, Address Pool and check the Enable DHCP Server that correspond 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 which 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, one should 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.



Ping Timeout	50	(10 - 10000 ms)
Lease Length	3600	(300 - 10,48,575 sec)
Auto-Configuration	□	
Interface		

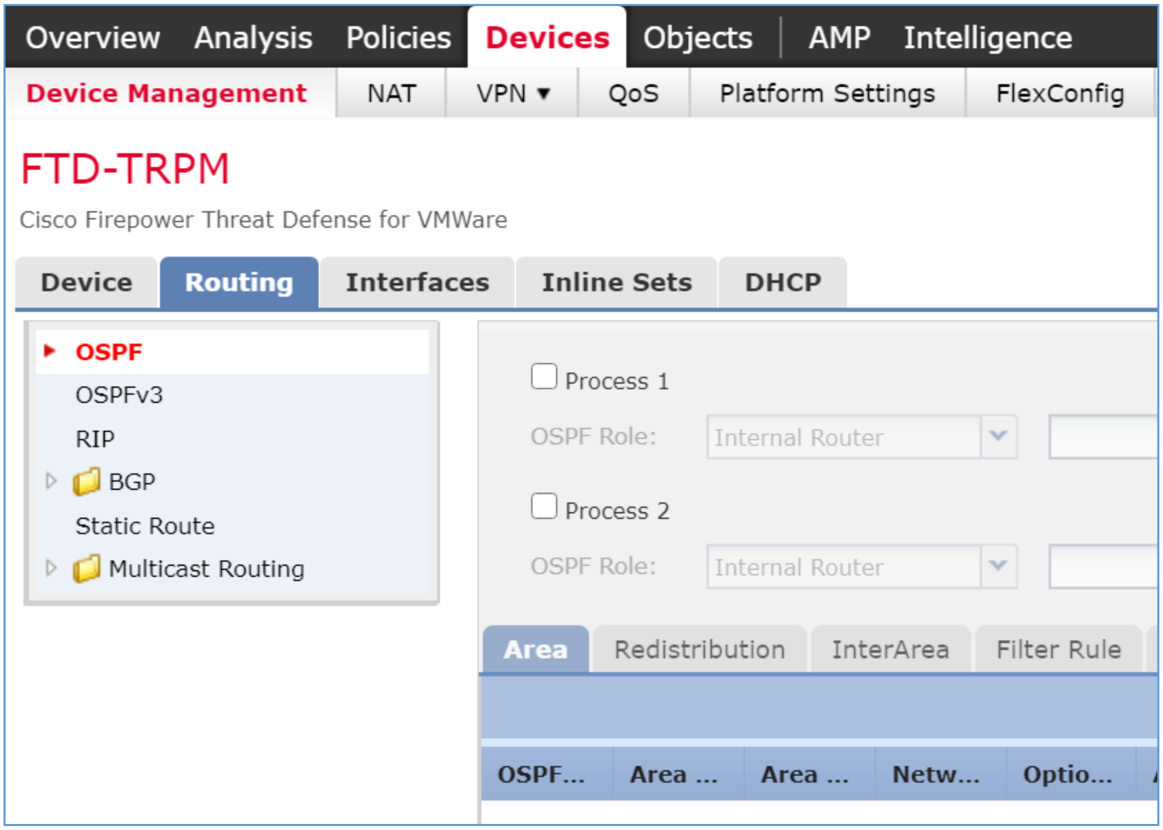
Override Auto Configured Settings:

Domain Name	hdo.trpm		
Primary DNS Server	Umbrella-DNS-1	Primary WINS Server	
Secondary DNS Server	Umbrella-DNS-2	Secondary WINS Server	

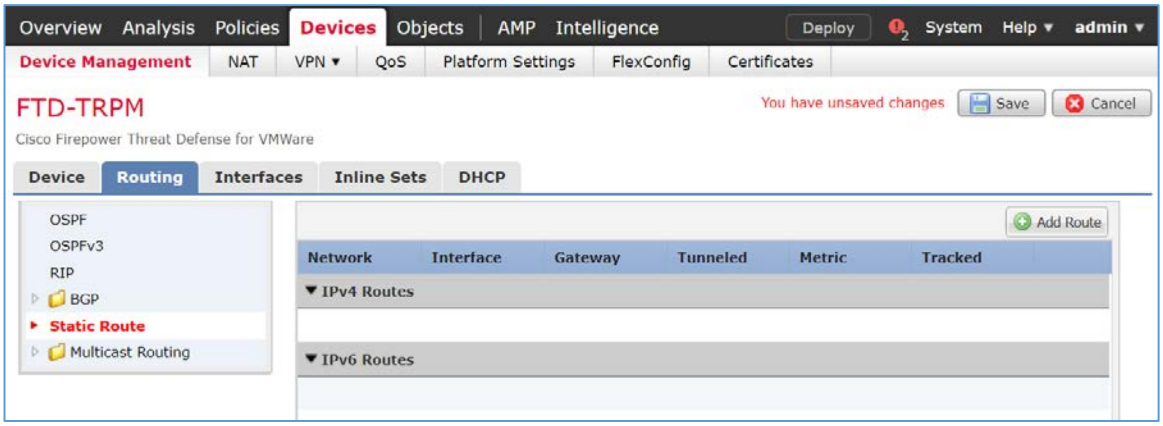
Interface	Address Pool	Enable DHCP Server
Enterprise-Services	192.168.40.100-192.168.40.254	✓
HIS-Services	192.168.41.100-192.168.41.254	✓
Remote-Services	192.168.42.100-192.168.42.254	✓
Databases	192.168.43.100-192.168.43.254	✓
Clinical-Workstations	192.168.44.100-192.168.44.254	✓

Configure Cisco FTD Static Route

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



3. Click **Add Route.**

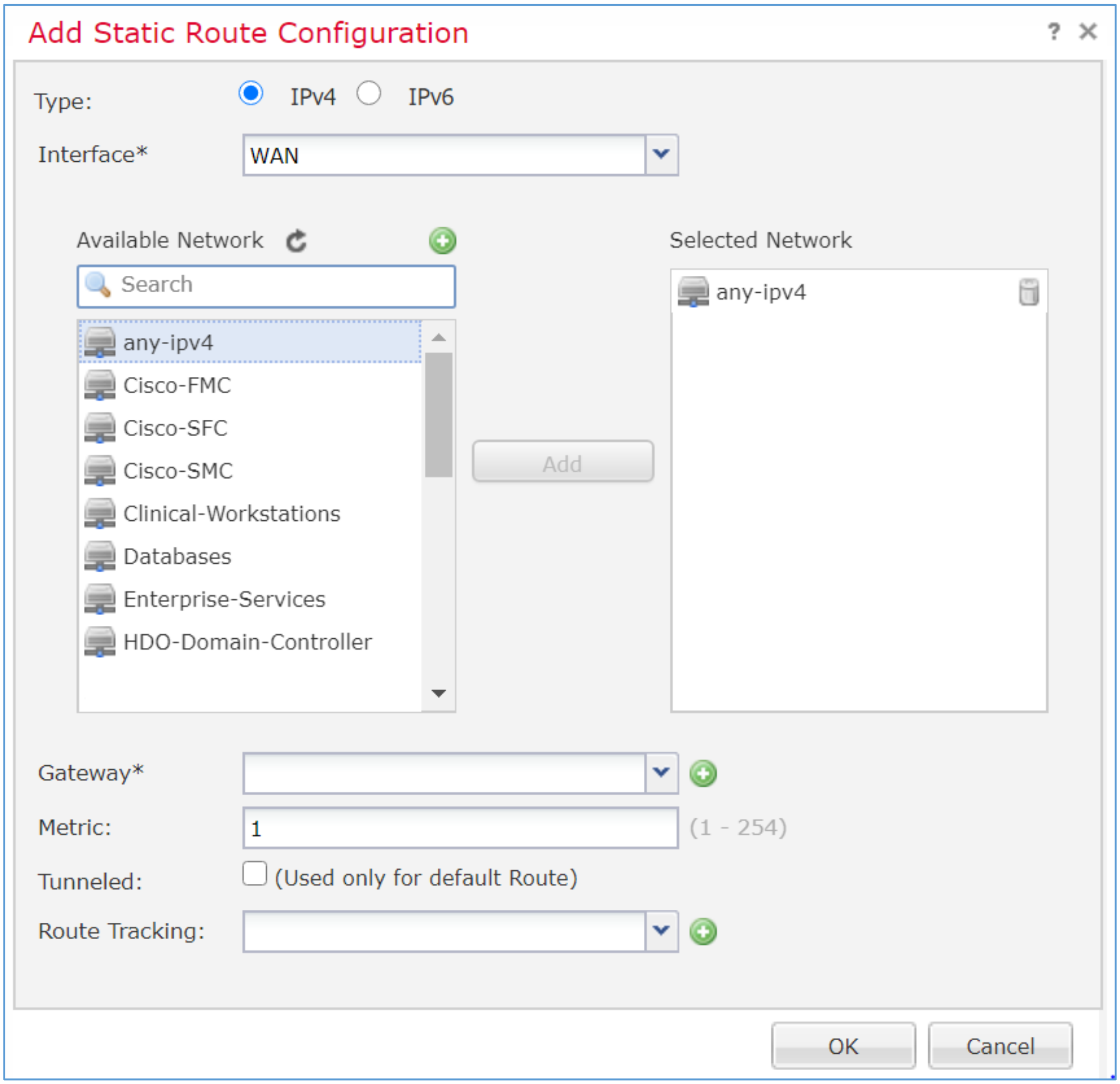


4. The Add Static Route Configuration popup window appears. Fill out the following information:

   a. **Interface:** WAN

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

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



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface* WAN

Available Network

Selected Network

any-ipv4

Gateway*

Metric: 1 (1 - 254)

Tunneled: □ (Used only for default Route)

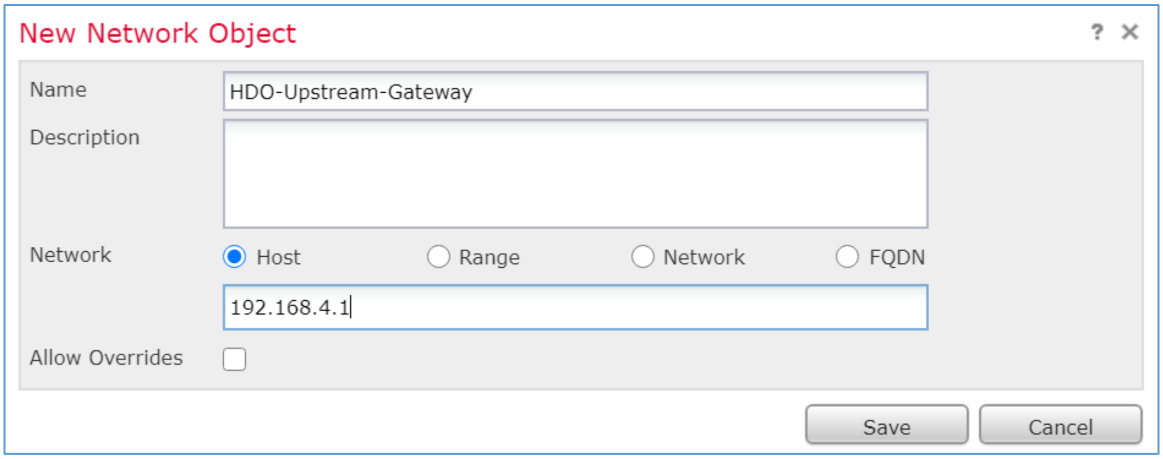
Route Tracking:

6. The New Network Object popup window appears. Fill out the following information:

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

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

7. Click **Save**.



New Network Object

Name: HDO-Upstream-Gateway

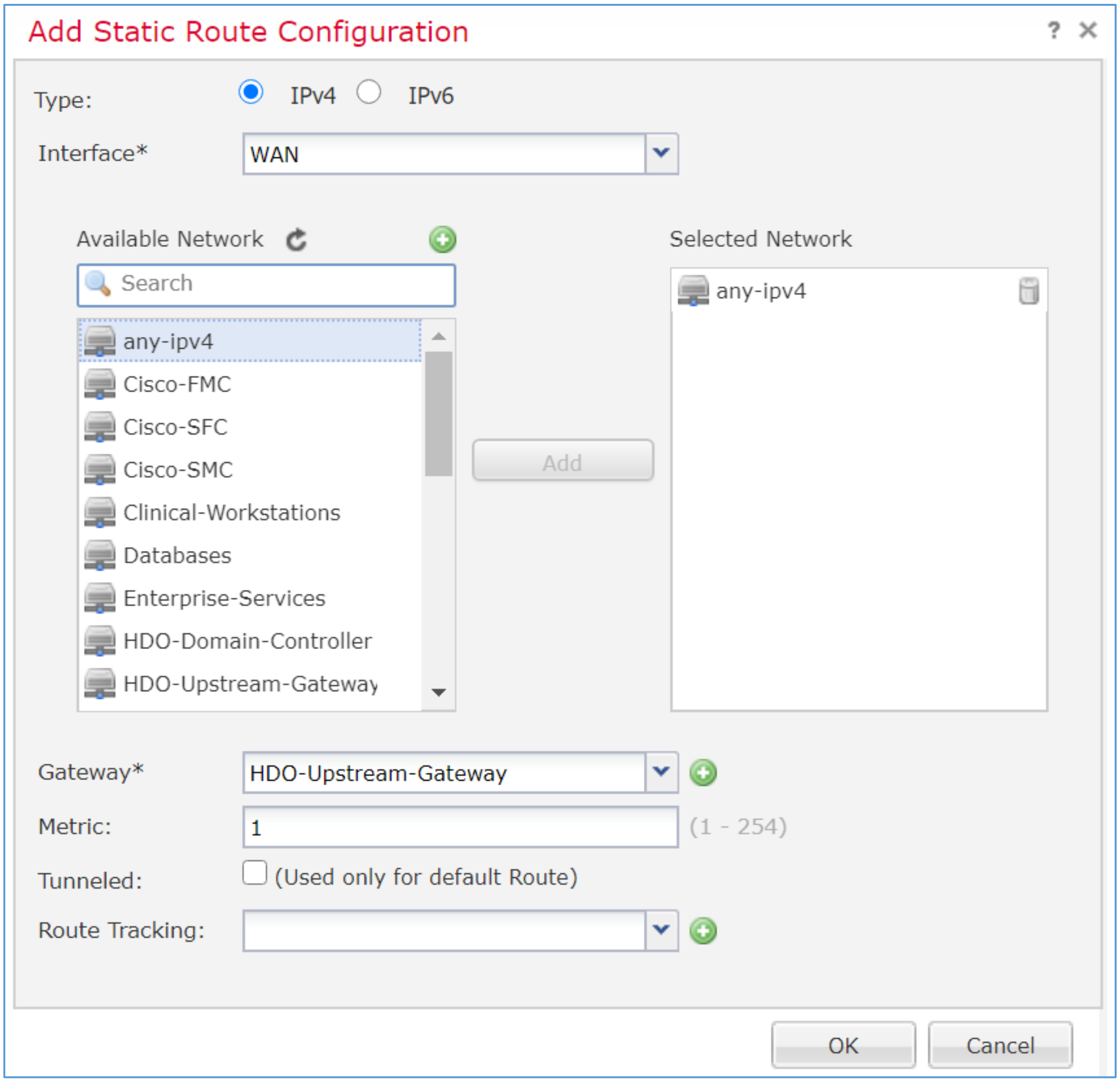
Description:

Network: ● Host ○ Range ○ Network ○ FQDN

192.168.4.1

Allow Overrides □

720 8. Click **OK**.



Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: WAN

Selected Network: any-ipv4

Gateway*: HDO-Upstream-Gateway

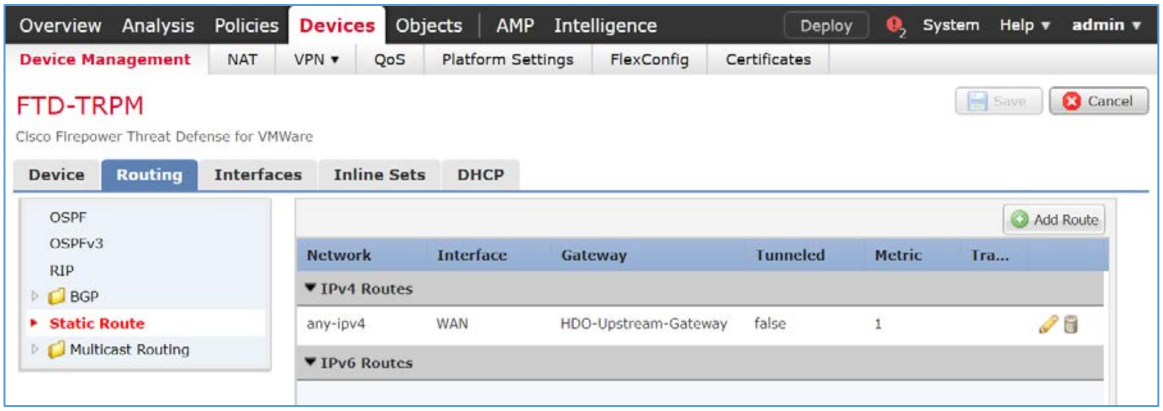
Metric: 1 (1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:

9. Click **Save**.

10. Click **Deploy**. Verify that the static route has been set correctly. From **Devices**, 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.


Overview Analysis Policies Devices Objects AMP Intelligence
Deploy System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
Save Cancel
Device Routing Interfaces Inline Sets DHCP
OSPF
OSPFv3
RIP
BGP
Static Route
Multicast Routing
Add Route

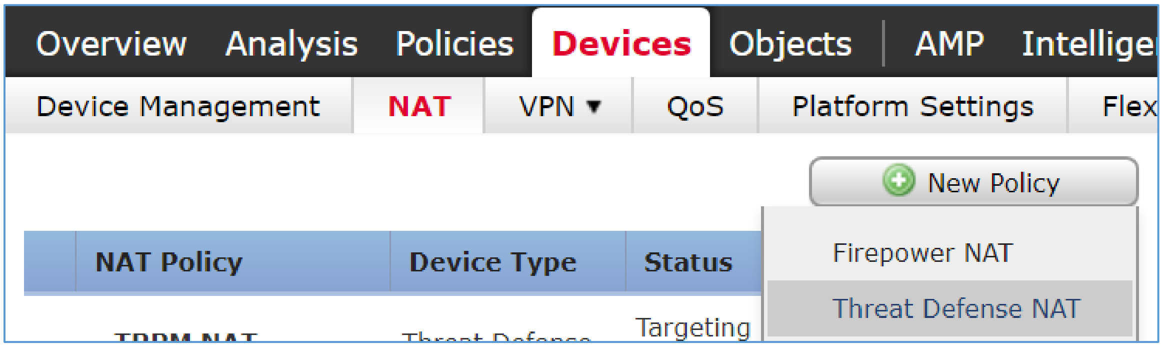
FTD-TRPM

Cisco Firepower Threat Defense for VMWare

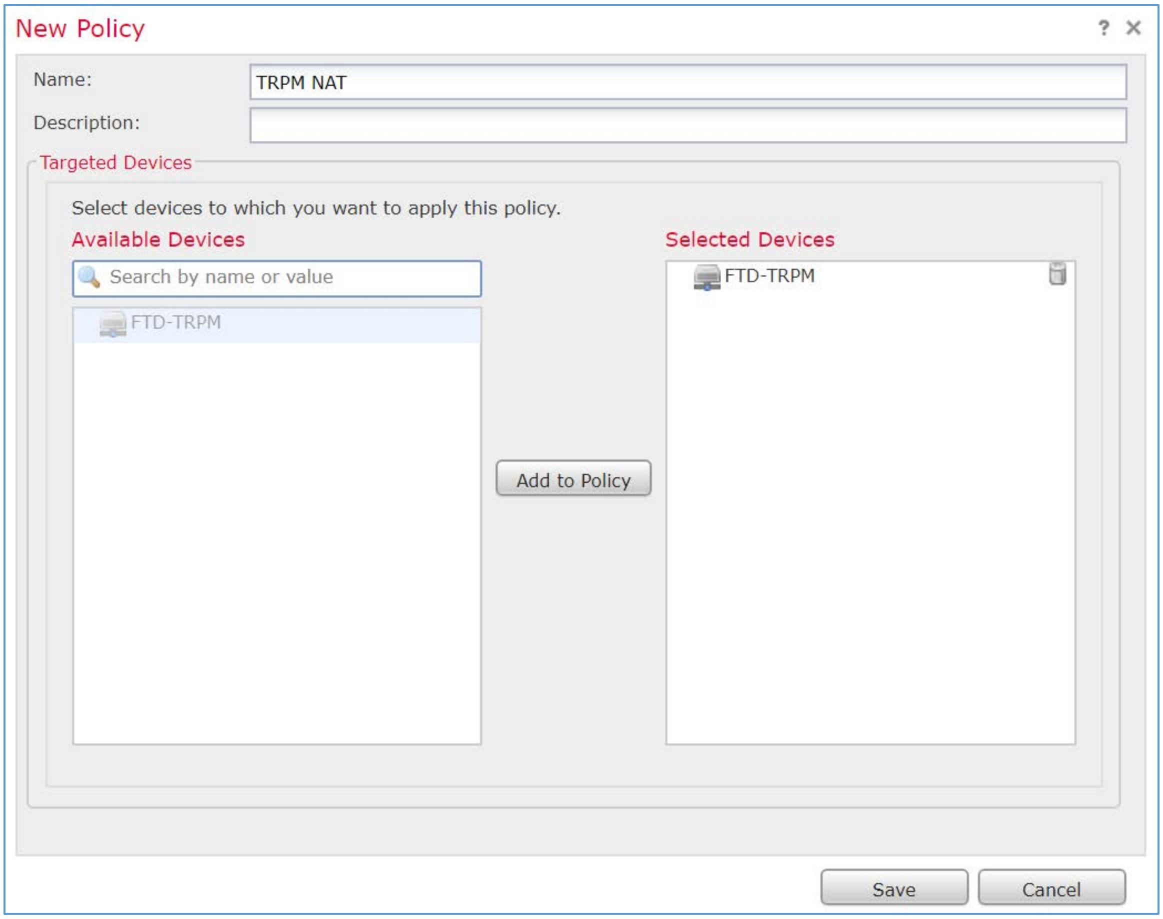
Network	Interface	Gateway	Tunneled	Metric	Tra...
▼ IPv4 Routes					
any-ipv4	WAN	HDO-Upstream-Gateway	false	1	
▼ IPv6 Routes					

Configure Cisco FTD Network Address Translation (NAT)

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


Overview Analysis Policies Devices Objects AMP Intellige
Device Management NAT VPN ▾ QoS Platform Settings Flex
New Policy
Firepower NAT
Threat Defense NAT
NAT Policy
Device Type
Status
TRPM NAT
Threat Defense
Targeting

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



New Policy

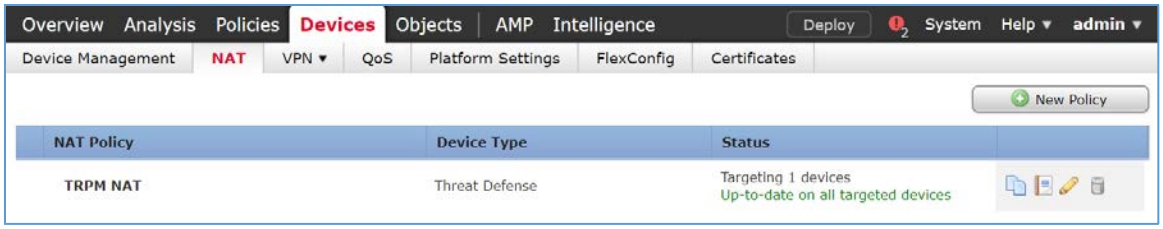
Name: TRPM NAT

Description:

Targeted Devices

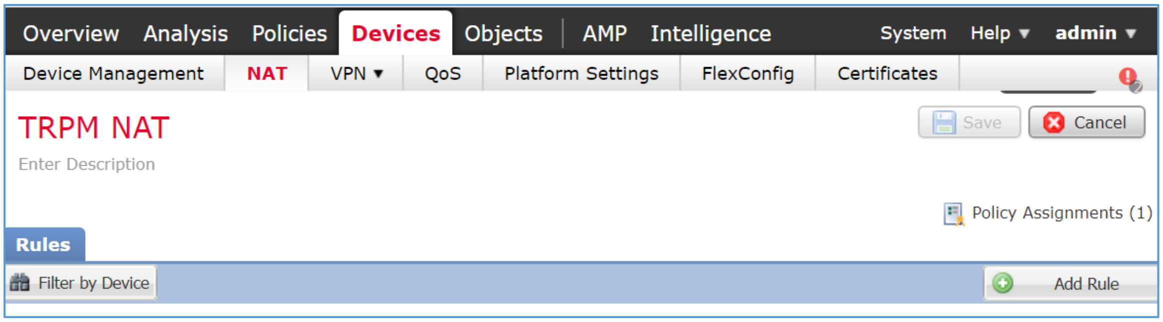
Select devices to which you want to apply this policy.

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

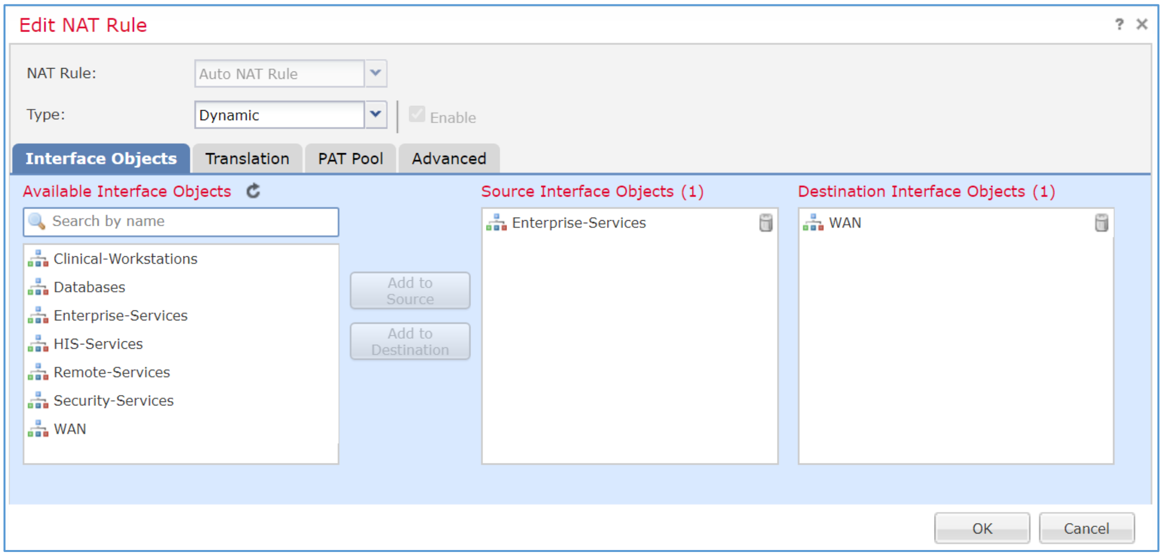


NAT Policy	Device Type	Status
TRPM NAT	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

736 6. Click **Add Rule**.


Overview Analysis Policies Devices Objects AMP Intelligence System Help ▾ admin ▾
Device Management NAT VPN ▾ QoS Platform Settings FlexConfig Certificates
TRPM NAT
Enter Description
Save
Cancel
Policy Assignments (1)
Rules
Filter by Device
Add Rule

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



NAT Rule: Auto NAT Rule

Type: Dynamic ☑ Enable

Available Interface Objects

- Clinical-Workstations
- Databases
- Enterprise-Services
- HIS-Services
- Remote-Services
- Security-Services
- WAN

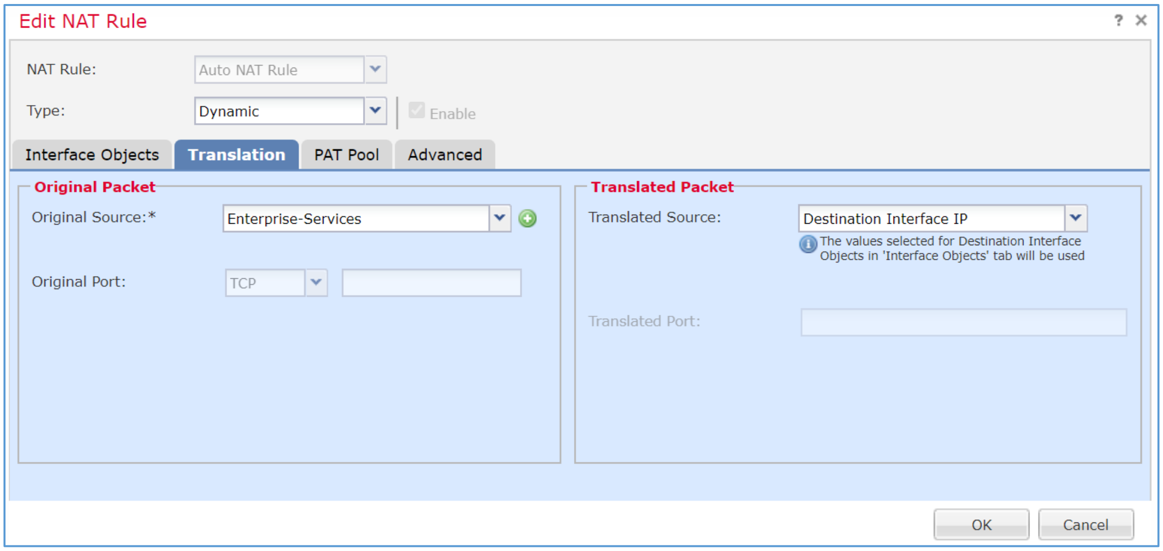
Source Interface Objects (1)

- Enterprise-Services

Destination Interface Objects (1)

- WAN

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



Edit NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

☑ Enable

Original Packet

Original Source:* Enterprise-Services

Original Port: TCP

Translated Packet

Translated Source: Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

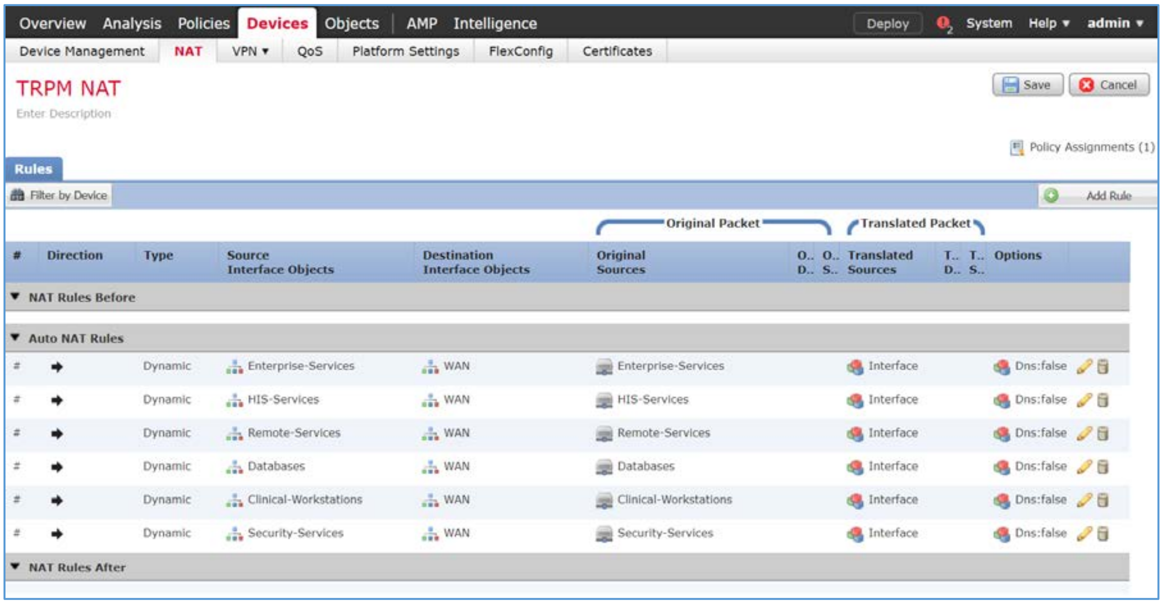
Translated Port:

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

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

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

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



TRPM NAT

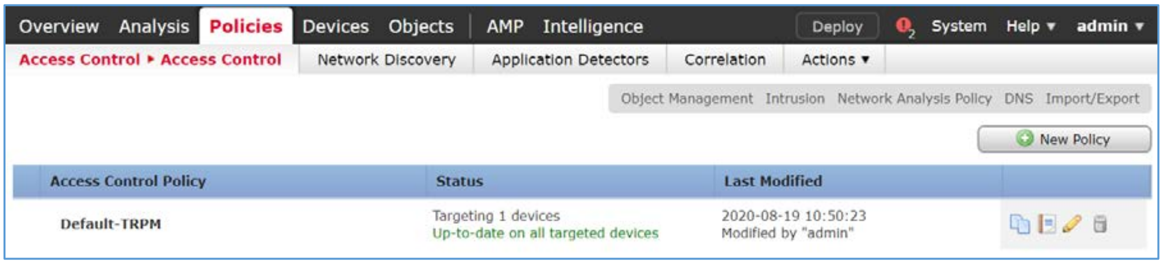
Enter Description

					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	O.. D..	O.. S..	Translated Sources	T.. D..	T.. S..	Options
▼ NAT Rules Before											
▼ Auto NAT Rules											
#	➔	Dynamic	Enterprise-Services	WAN	Enterprise-Services			Interface			Dns:false
#	➔	Dynamic	HIS-Services	WAN	HIS-Services			Interface			Dns:false
#	➔	Dynamic	Remote-Services	WAN	Remote-Services			Interface			Dns:false
#	➔	Dynamic	Databases	WAN	Databases			Interface			Dns:false
#	➔	Dynamic	Clinical-Workstations	WAN	Clinical-Workstations			Interface			Dns:false
#	➔	Dynamic	Security-Services	WAN	Security-Services			Interface			Dns:false
▼ NAT Rules After											

Configure Cisco FTD Access Control Policy

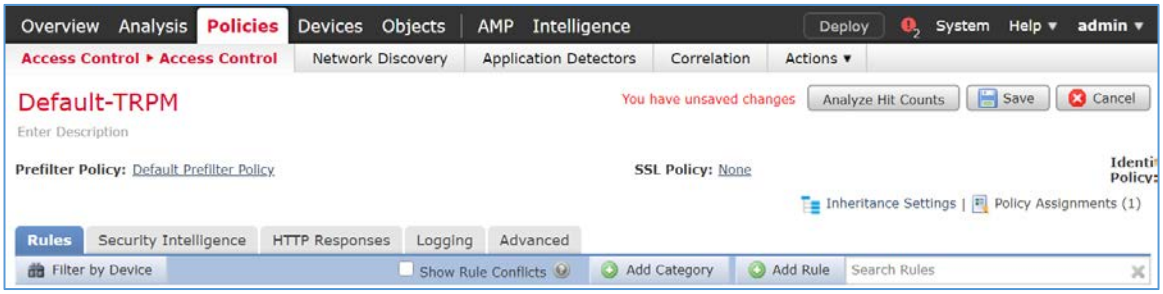
1. Click **Polices > Access Control > Access Control**.

2. Click the **edit symbol** for **Default-TRPM**.



Access Control Policy	Status	Last Modified
Default-TRPM	Targeting 1 devices Up-to-date on all targeted devices	2020-08-19 10:50:23 Modified by "admin"

3. Click **Add Category.**



Default-TRPM

You have unsaved changes

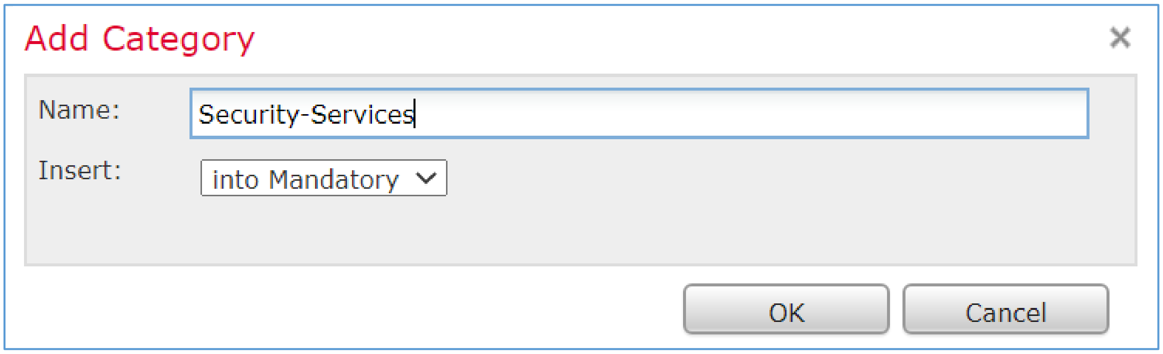
Enter Description

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

Identi Policy:

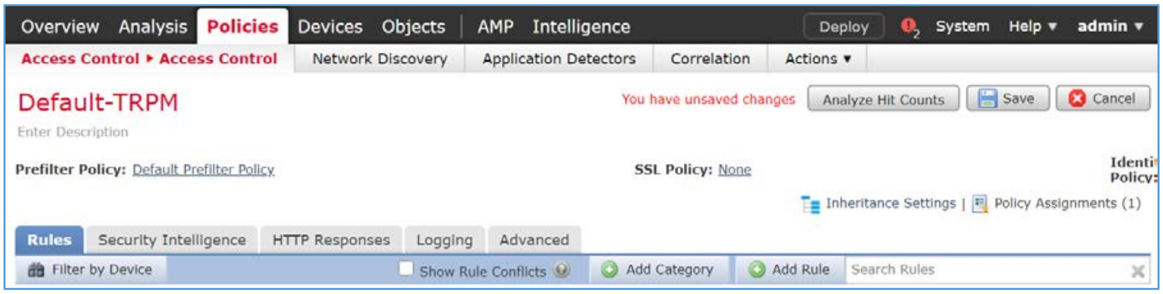
4. Fill out the following information:
    a. **Name:** Security Services
    b. **Insert:** into Mandatory
5. Click **OK**.



Name: Security-Services

Insert: into Mandatory

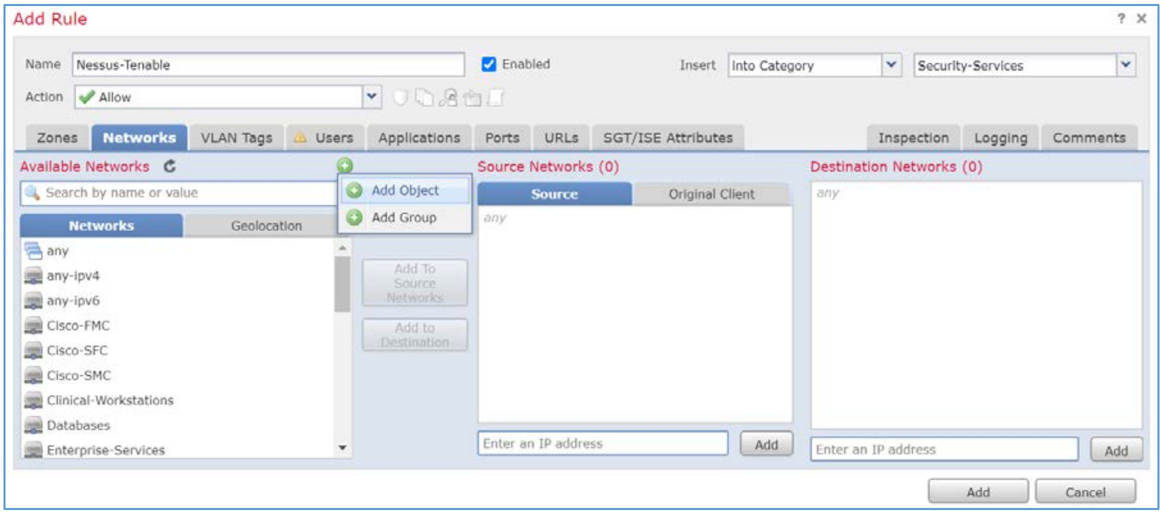
6. Repeat the previous steps of **Add Category** section for each network segment in the architecture.
7. Click **Add Rule**.



Prefilter Policy: Default Prefilter Policy

SSL Policy: None

8. 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.**



Name: Nessus-Tenable

☑ Enabled

Insert: Into Category | Security-Services

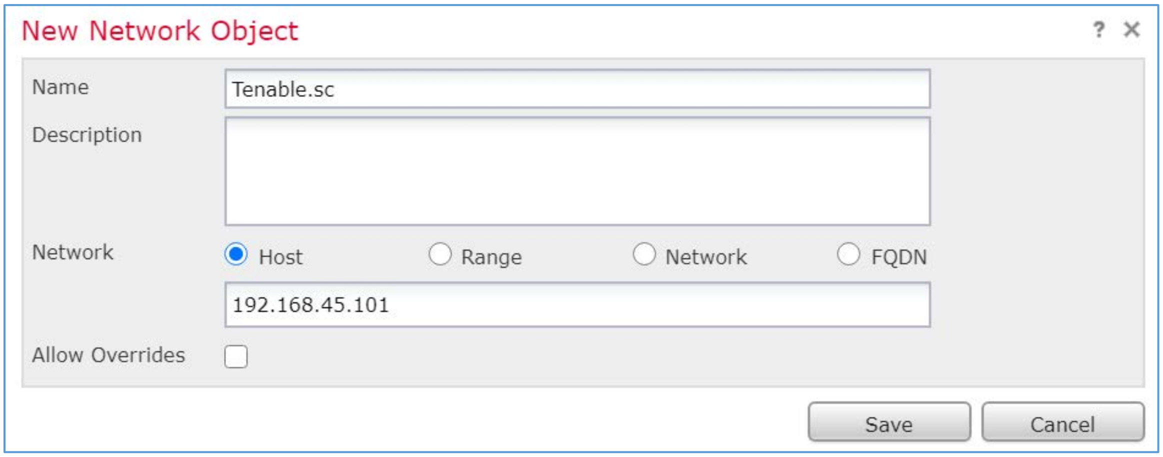
Action: ✓ Allow

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

   a. **Name:** Tenable.sc

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

10. Click **Save**.



Name: Tenable.sc

Description:

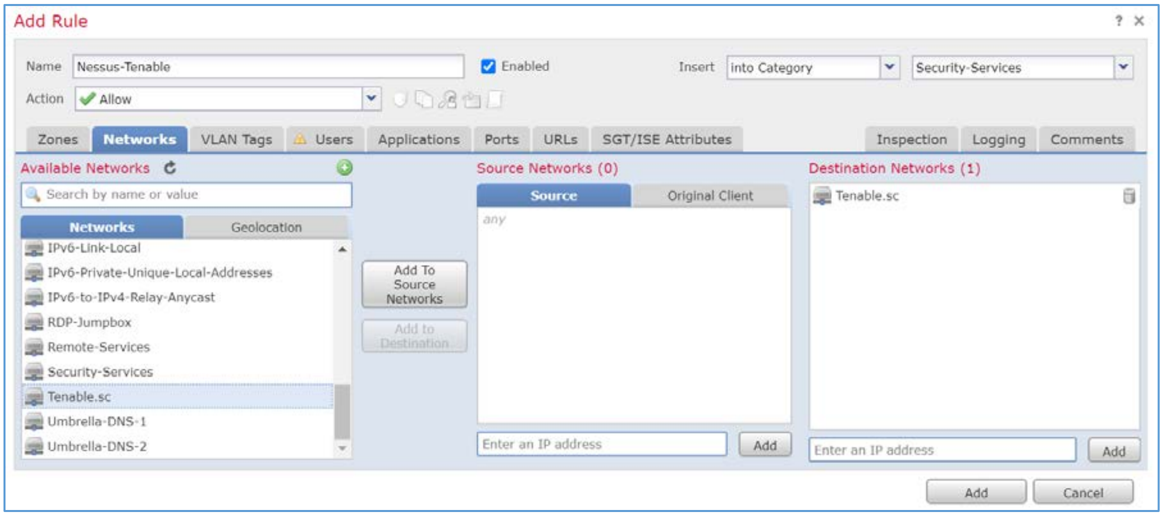
Network: ● Host ○ Range ○ Network ○ FQDN

192.168.45.101

Allow Overrides ☐

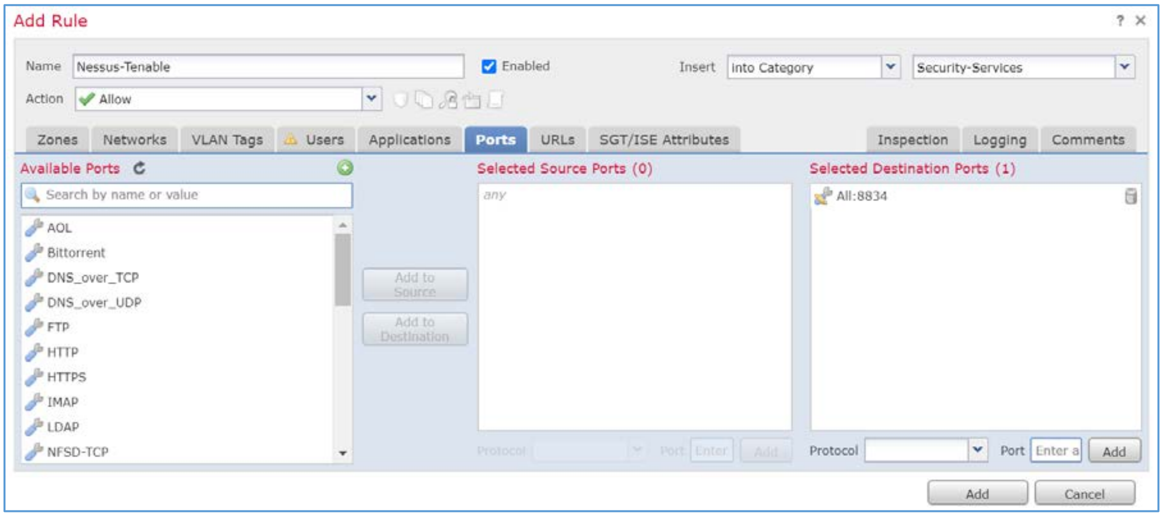
11. In the Add Rule screen, under the **Networks** tab, set **Destination Networks** to Tenable.sc.

12. Click **Ports.**



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

14. Click **Add.**



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

16. Click **Save.**

17. Click **Deploy**.

2.2.3 Security Continuous Monitoring

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

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

2.2.3.1 Cisco Stealthwatch

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

Cisco Stealthwatch Management Center (SMC) Appliance Information

CPU: 4

RAM: 16 GB

Storage: 200 GB (Thick Provision)

Network Adapter 1: VLAN 1348

Operating System: Linux

Cisco SMC Appliance Installation Guide

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

Cisco SFC Appliance Information

CPU: 4

RAM: 16 GB

Storage: 300 GB (Thick Provision)

Network Adapter 1: VLAN 1348

Operating System: Linux

Cisco SFC Appliance Installation Guide

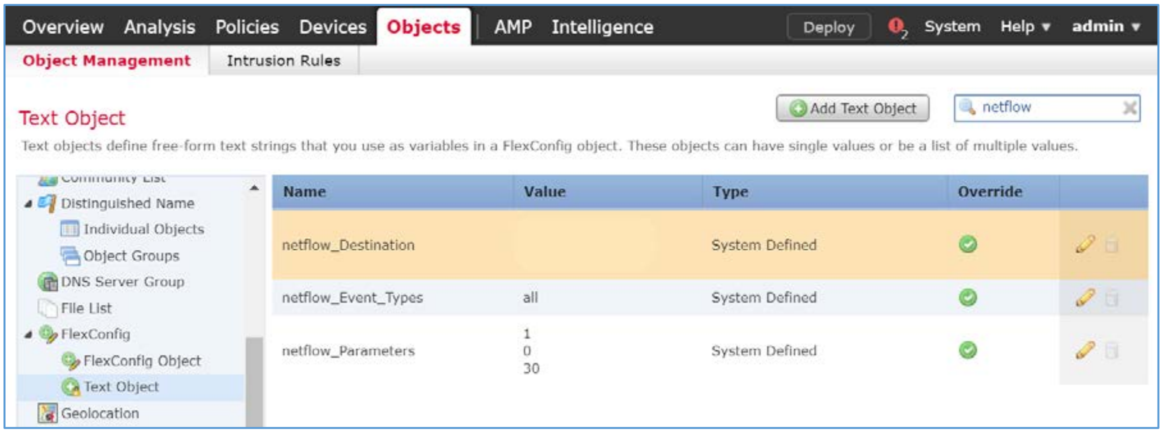
Install the appliance according to the instructions detailed in the *Cisco Stealthwatch Installation and Configuration Guide 7.1* [8].

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

Configure Cisco FTD NetFlow for Cisco SFC

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

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

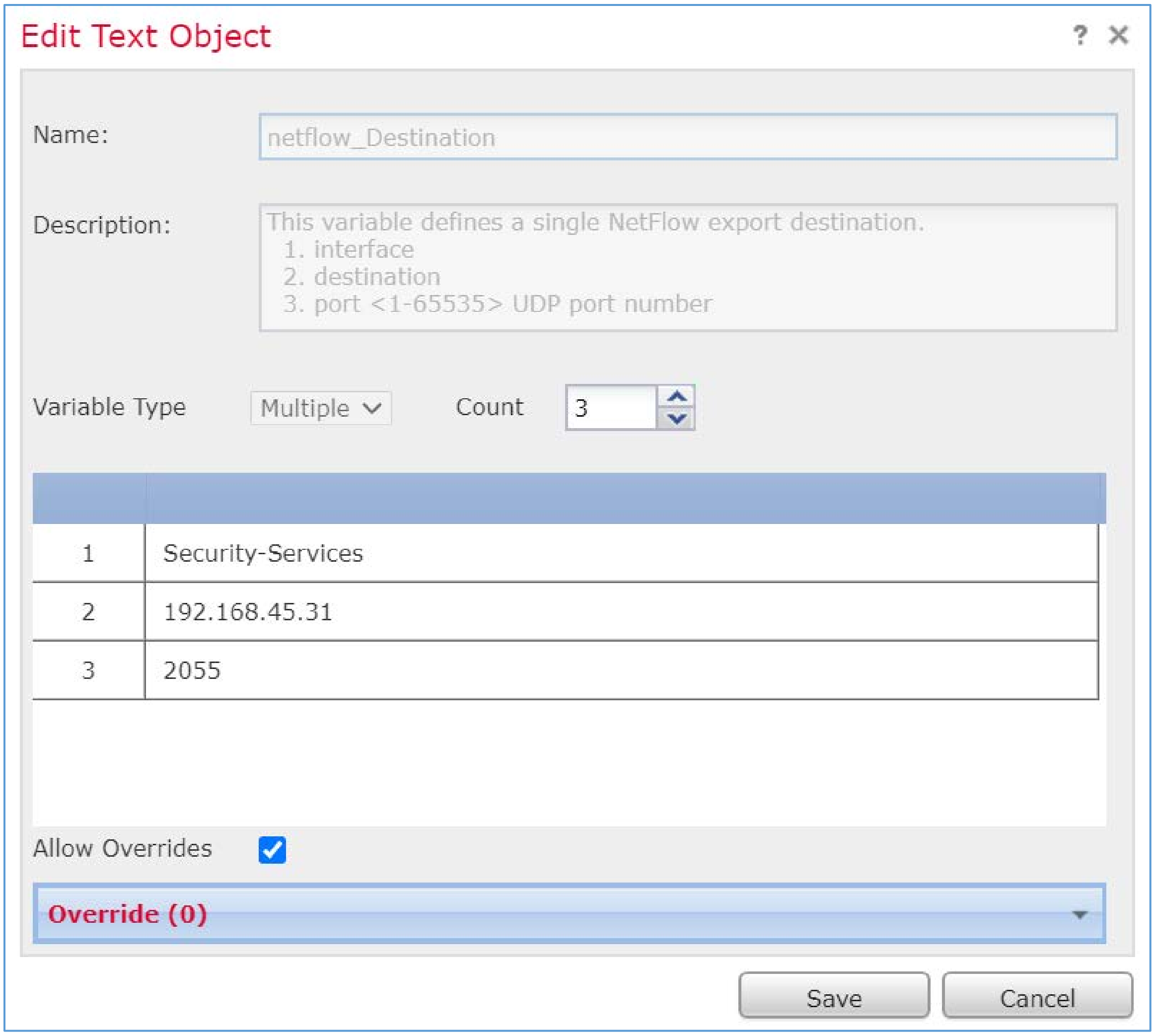


Text Object

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Name	Value	Type	Override
netflow_Destination		System Defined	✓
netflow_Event_Types	all	System Defined	✓
netflow_Parameters	1 0 30	System Defined	✓

4. The Edit Text Object popup 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.**



Name: netflow_Destination

Description: This variable defines a single NetFlow export destination.
1. interface
2. destination
3. port <1-65535> UDP port number

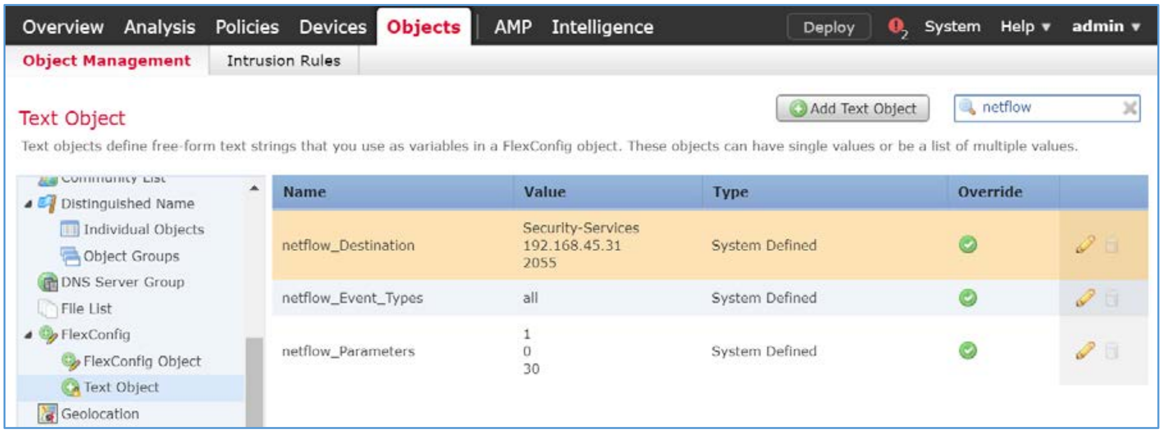
Variable Type: Multiple

Count: 3

1	Security-Services
2	192.168.45.31
3	2055

Allow Overrides ☑

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

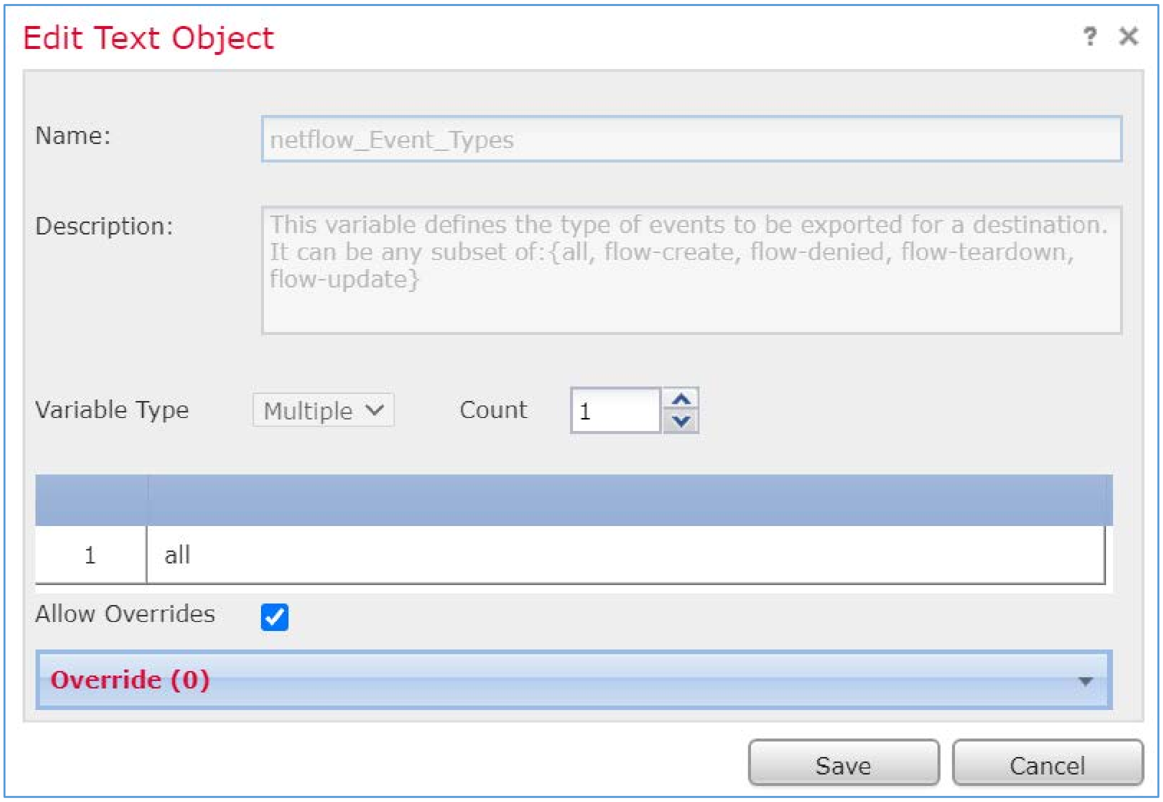


Text Object

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Name	Value	Type	Override
netflow_Destination	Security-Services 192.168.45.31 2055	System Defined	✓
netflow_Event_Types	all	System Defined	✓
netflow_Parameters	1 0 30	System Defined	✓

7. The Edit Text Object popup window appears, fill out the following information:
   a. **Count:** 1
   b. **1:** All
   c. **Allow Overrides:** Checked
8. Click **Save.**



Edit Text Object

Name: netflow_Event_Types

Description: This variable defines the type of events to be exported for a destination. It can be any subset of:{all, flow-create, flow-denied, flow-teardown, flow-update}

Variable Type: Multiple

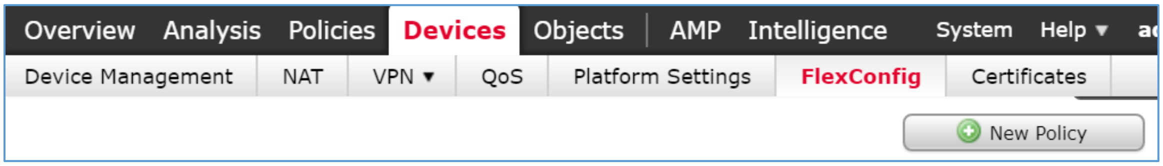
Count: 1

1	all

Allow Overrides ☑

9. Click **Devices > FlexConfig.**

10. Click **New Policy.**

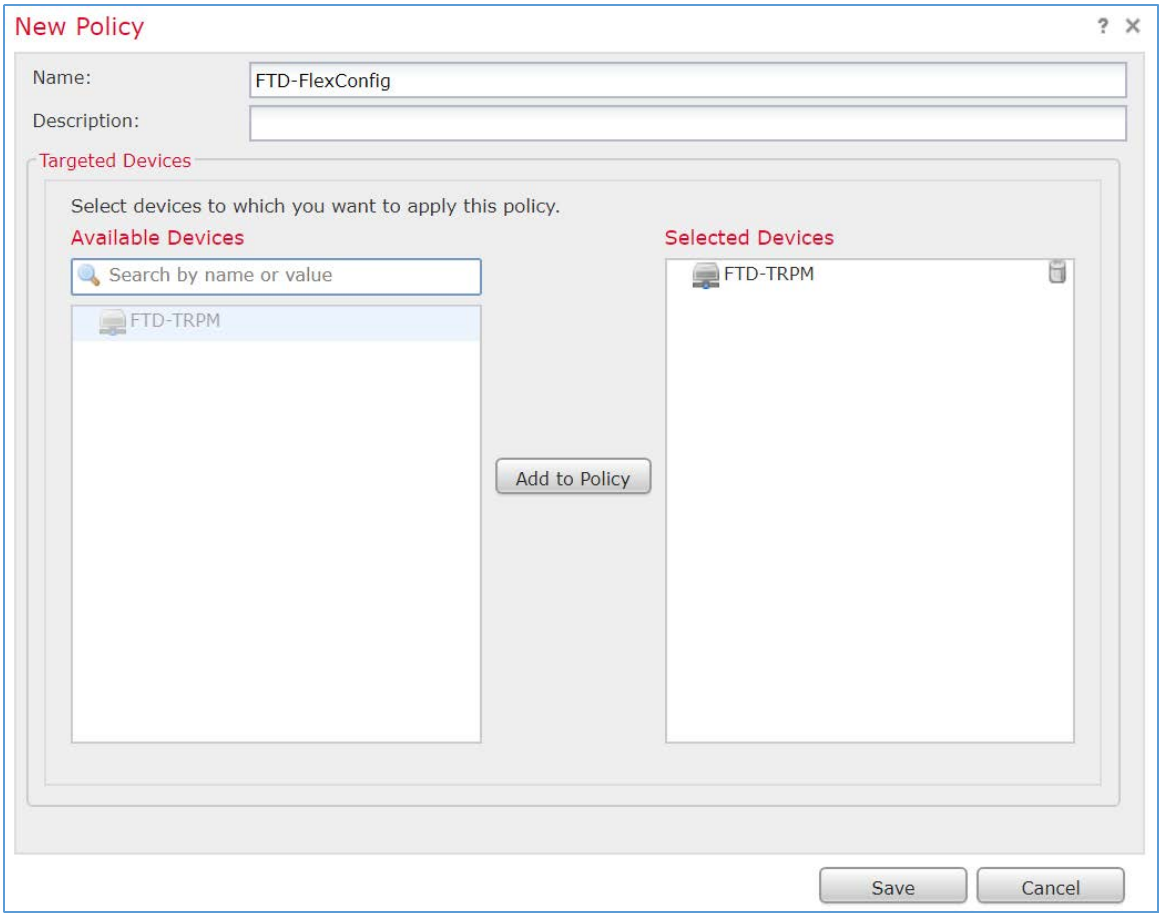


11. The New Policy screen appears, fill out the following information:

    a. **Name:** FTD-FlexConfig

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

12. Click **Save.**



Name: FTD-FlexConfig

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

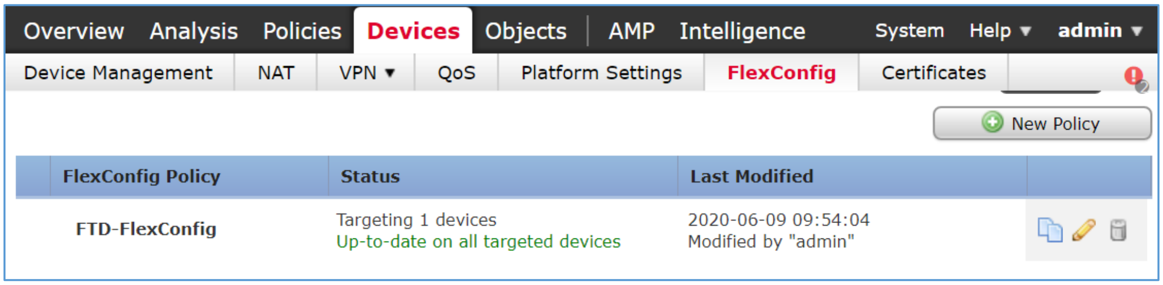
Search by name or value

FTD-TRPM

Selected Devices

FTD-TRPM

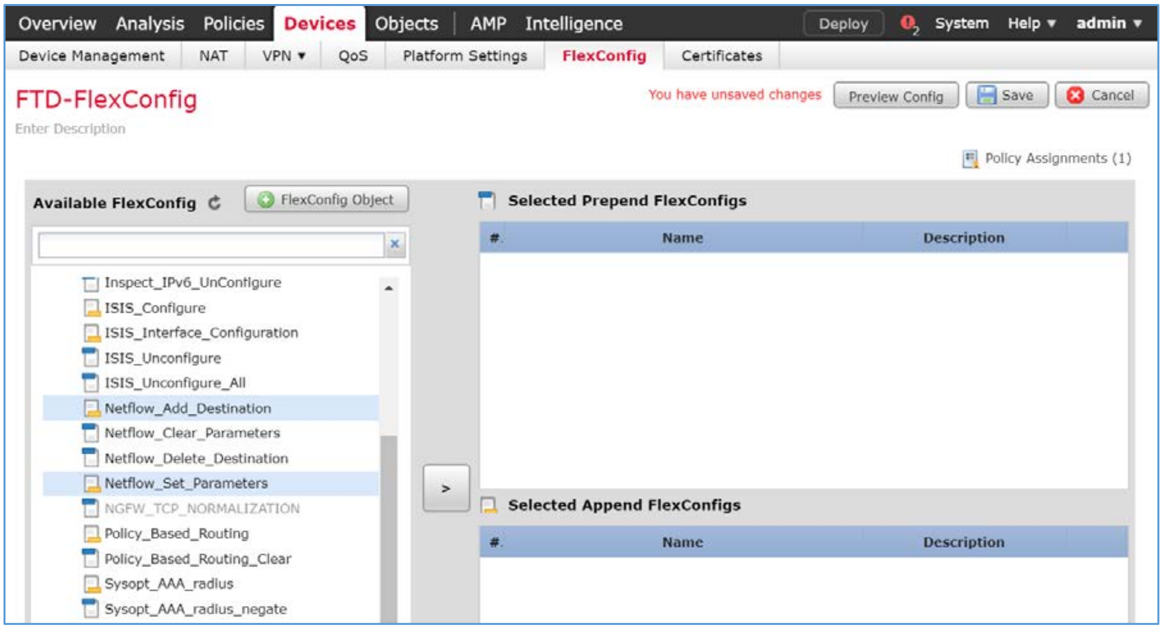
13. Click the **edit symbol** for **FTD-FlexConfig.**



FlexConfig Policy	Status	Last Modified
FTD-FlexConfig	Targeting 1 devices Up-to-date on all targeted devices	2020-06-09 09:54:04 Modified by "admin"

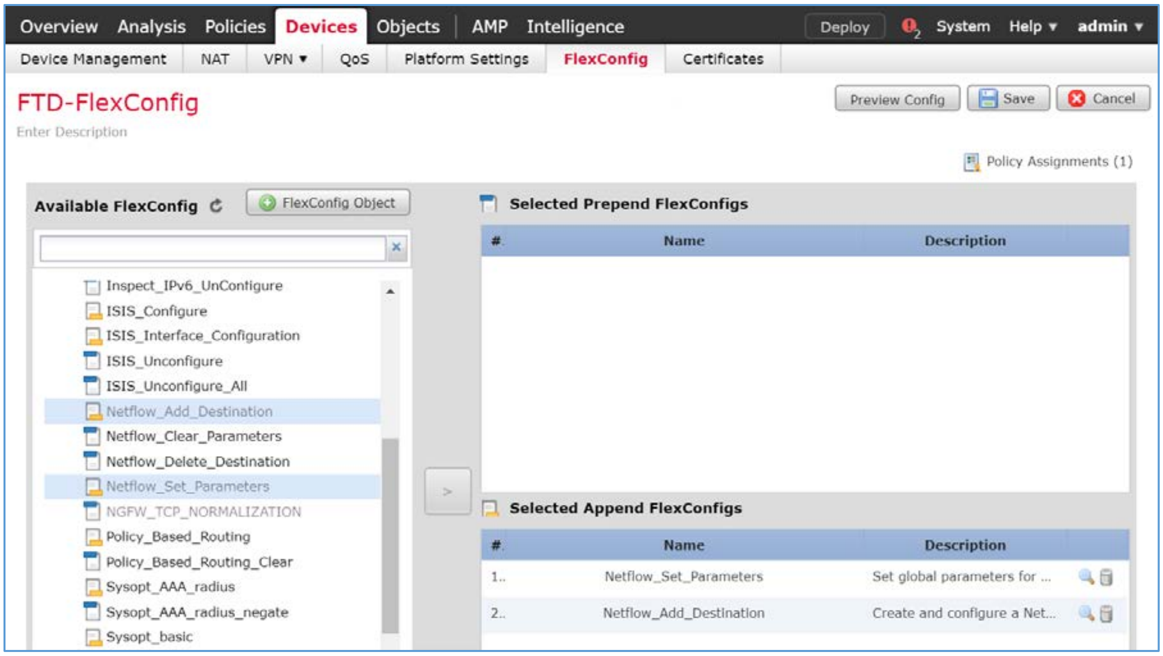
14. Under the **Device**s tab, select **Netflow_Add_Destination** and **Netflow_Set_Parameters.**

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



16. Click **Save**.

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

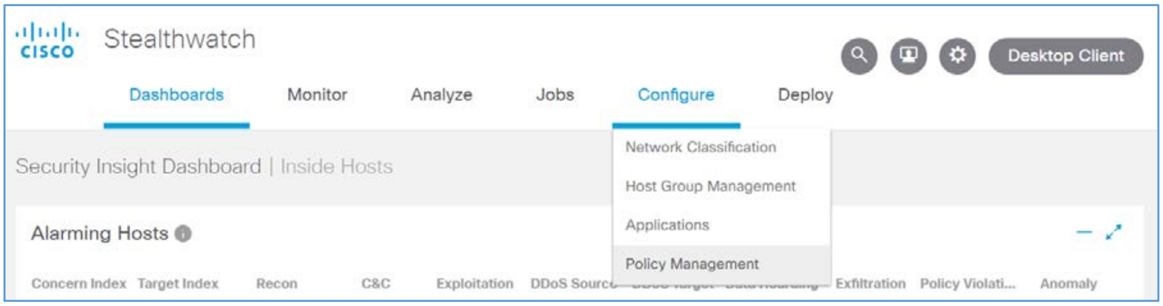


#	Name	Description

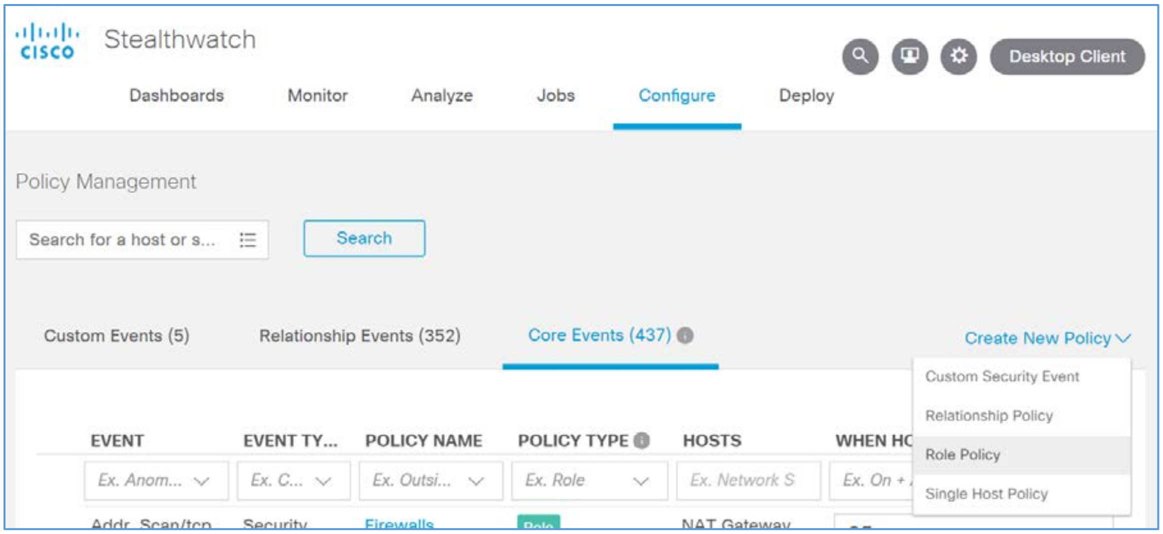
#	Name	Description
1..	Netflow_Set_Parameters	Set global parameters for ...
2..	Netflow_Add_Destination	Create and configure a Net...

881 <u>**Creating a Custom Policy Management Rule**</u>

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

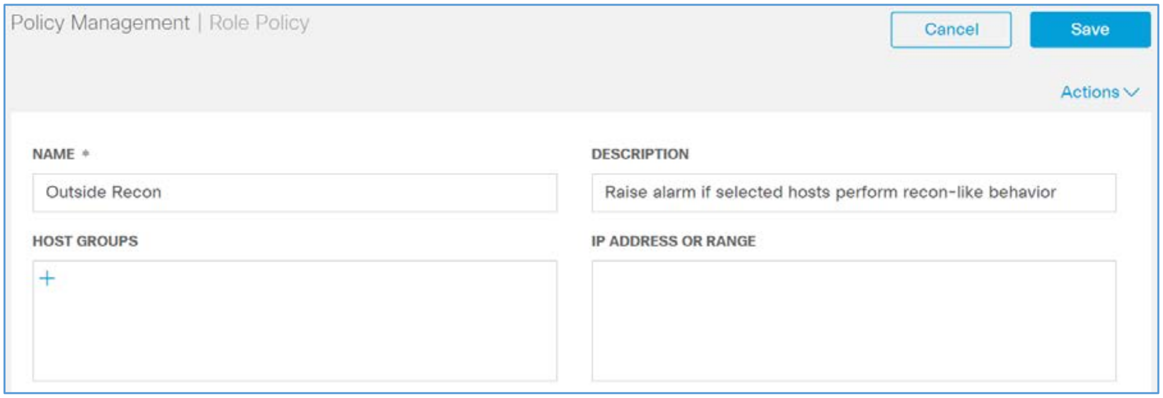


883 2. Click **Create New Policy > Role Policy.**



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

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



NAME *

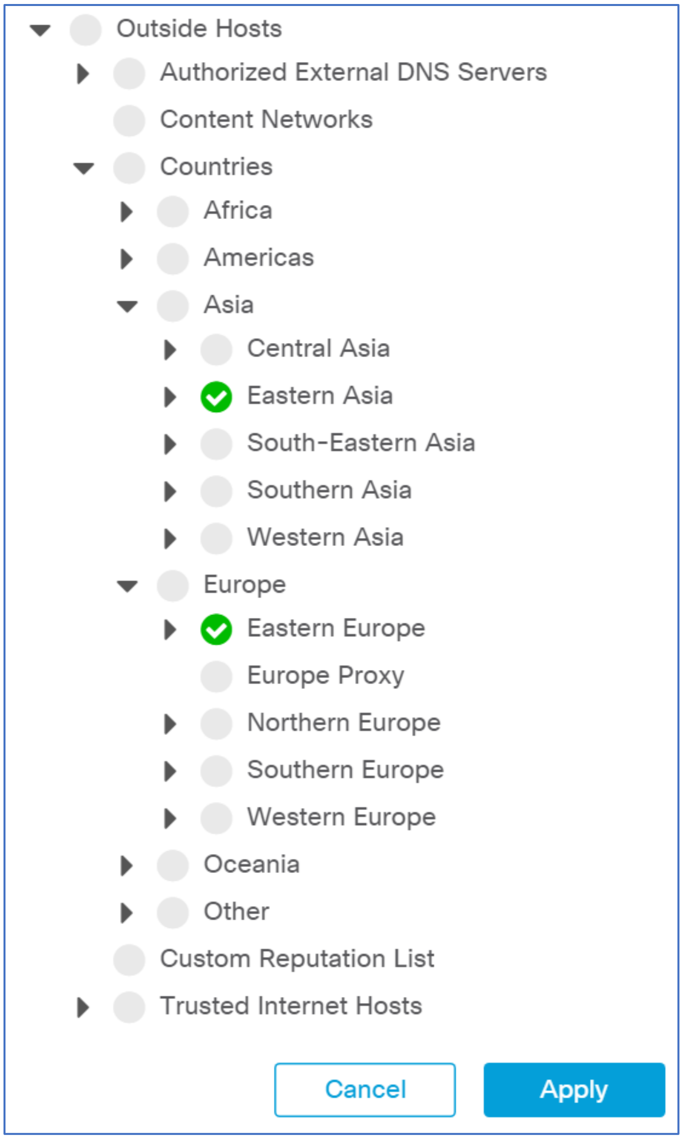
Outside Recon

DESCRIPTION

Raise alarm if selected hosts perform recon-like behavior

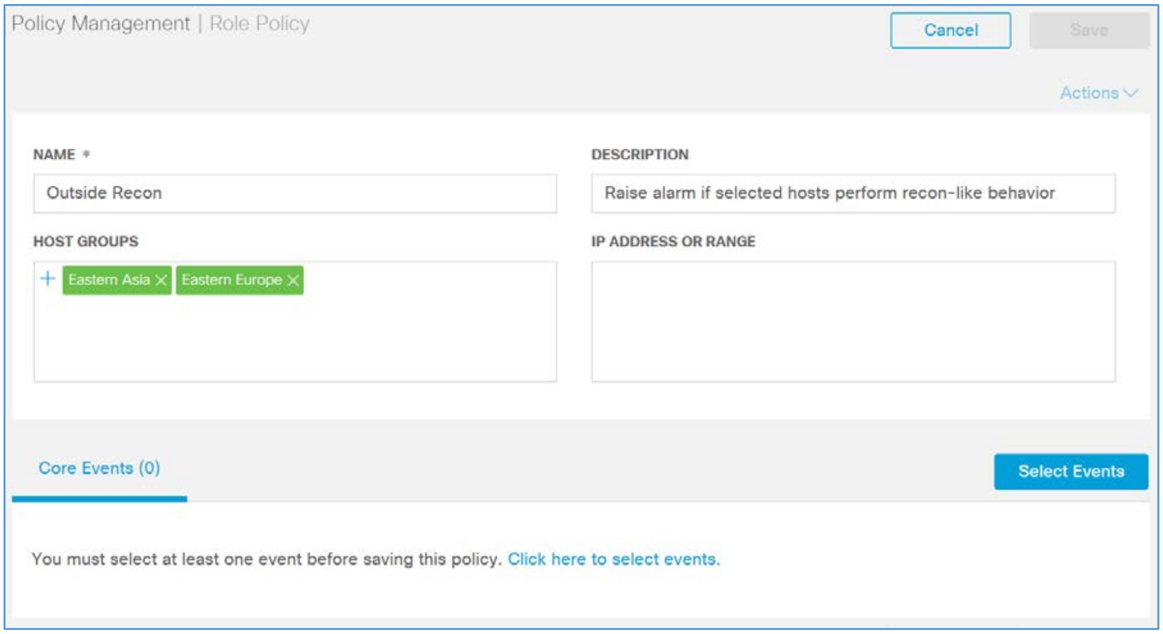
886 5. Under **Outside** Hosts, select **Eastern Asia** and **Eastern Europe.**

887 6. Click **Apply.**



- ○ Outside Hosts
  - ○ Authorized External DNS Servers
  - ○ Content Networks
  - ○ Countries
    - ○ Africa
    - ○ Americas
    - ○ Asia
      - ○ Central Asia
      - ✓ Eastern Asia
      - ○ South-Eastern Asia
      - ○ Southern Asia
      - ○ Western Asia
    - ○ Europe
      - ✓ Eastern Europe
      - ○ Europe Proxy
      - ○ Northern Europe
      - ○ Southern Europe
      - ○ Western Europe
    - ○ Oceania
    - ○ Other
  - ○ Custom Reputation List
  - ○ Trusted Internet Hosts

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



NAME *

Outside Recon

DESCRIPTION

Raise alarm if selected hosts perform recon-like behavior

HOST GROUPS

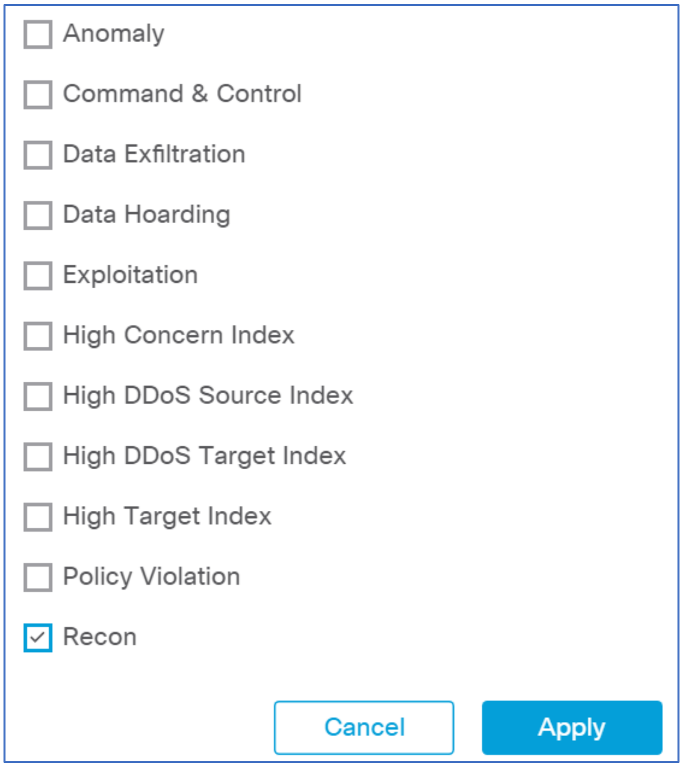
Eastern Asia, Eastern Europe

IP ADDRESS OR RANGE

You must select at least one event before saving this policy. Click here to select events.

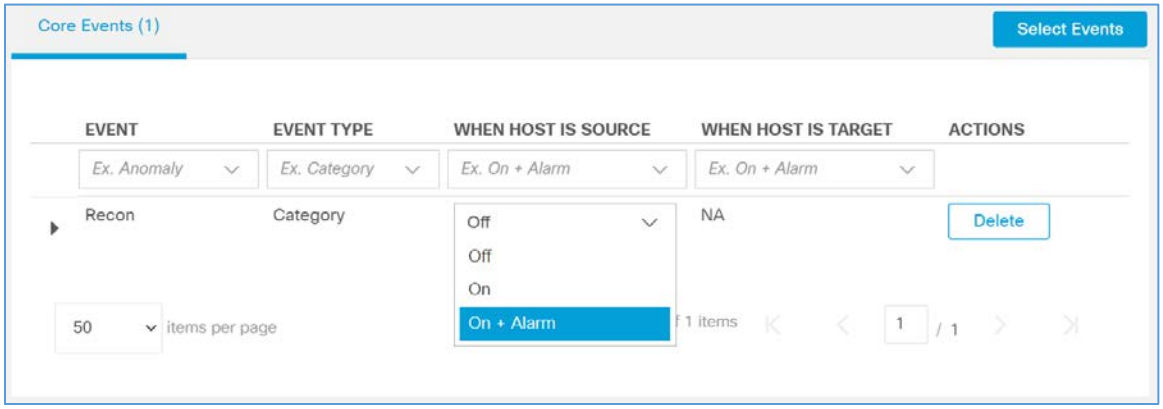
889 8. Select **Recon.**

890 9. Click **Apply.**



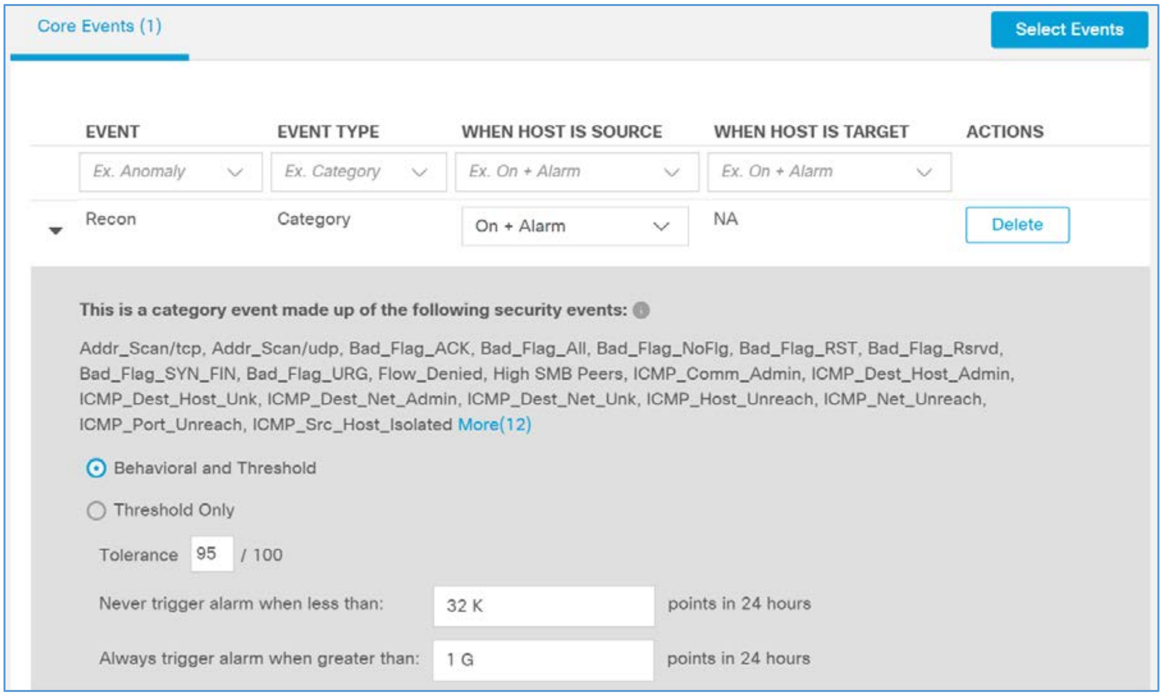
☐ Anomaly
☐ Command & Control
☐ Data Exfiltration
☐ Data Hoarding
☐ Exploitation
☐ High Concern Index
☐ High DDoS Source Index
☐ High DDoS Target Index
☐ High Target Index
☐ Policy Violation
☑ Recon

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



EVENT	EVENT TYPE	WHEN HOST IS SOURCE	WHEN HOST IS TARGET	ACTIONS
Ex. Anomaly	Ex. Category	Ex. On + Alarm	Ex. On + Alarm	
Recon	Category	Off Off On On + Alarm	NA	Delete

12. Select **Behavioral and Threshold.**



EVENT	EVENT TYPE	WHEN HOST IS SOURCE	WHEN HOST IS TARGET	ACTIONS
Ex. Anomaly	Ex. Category	Ex. On + Alarm	Ex. On + Alarm	
Recon	Category	On + Alarm	NA	Delete

This is a category event made up of the following security events:

Addr_Scan/tcp, Addr_Scan/udp, Bad_Flag_ACK, Bad_Flag_All, Bad_Flag_NoFlg, Bad_Flag_RST, Bad_Flag_Rsrvd, Bad_Flag_SYN_FIN, Bad_Flag_URG, Flow_Denied, High SMB Peers, ICMP_Comm_Admin, ICMP_Dest_Host_Admin, ICMP_Dest_Host_Unk, ICMP_Dest_Net_Admin, ICMP_Dest_Net_Unk, ICMP_Host_Unreach, ICMP_Net_Unreach, ICMP_Port_Unreach, ICMP_Src_Host_Isolated More(12)

● Behavioral and Threshold

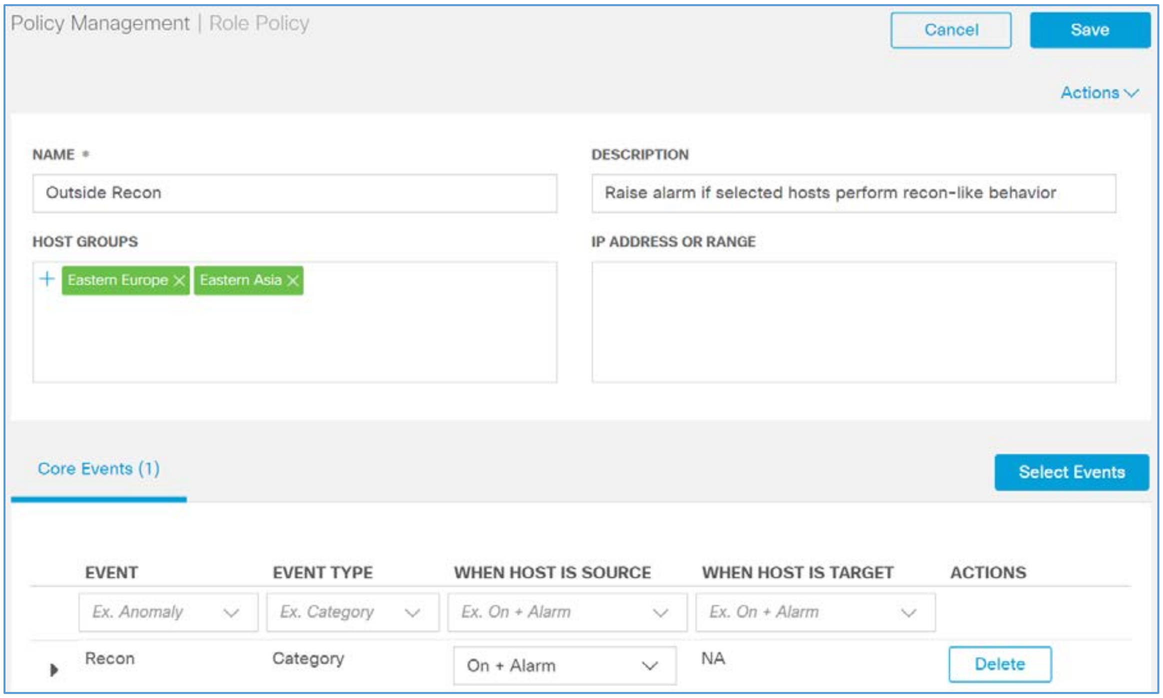
○ Threshold Only

Tolerance 95 / 100

Never trigger alarm when less than: 32 K points in 24 hours

Always trigger alarm when greater than: 1 G points in 24 hours

13. Click **Save.**



NAME *

Outside Recon

DESCRIPTION

Raise alarm if selected hosts perform recon-like behavior

HOST GROUPS

Eastern Europe, Eastern Asia

IP ADDRESS OR RANGE

EVENT	EVENT TYPE	WHEN HOST IS SOURCE	WHEN HOST IS TARGET	ACTIONS
Ex. Anomaly	Ex. Category	Ex. On + Alarm	Ex. On + Alarm	
Recon	Category	On + Alarm	NA	Delete

2.2.3.2 Cisco Umbrella

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

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

CPU: 1

RAM: 0.5 GB

Storage: 6.5 GB (Thick Provision)

Network Adapter 1: VLAN 1327

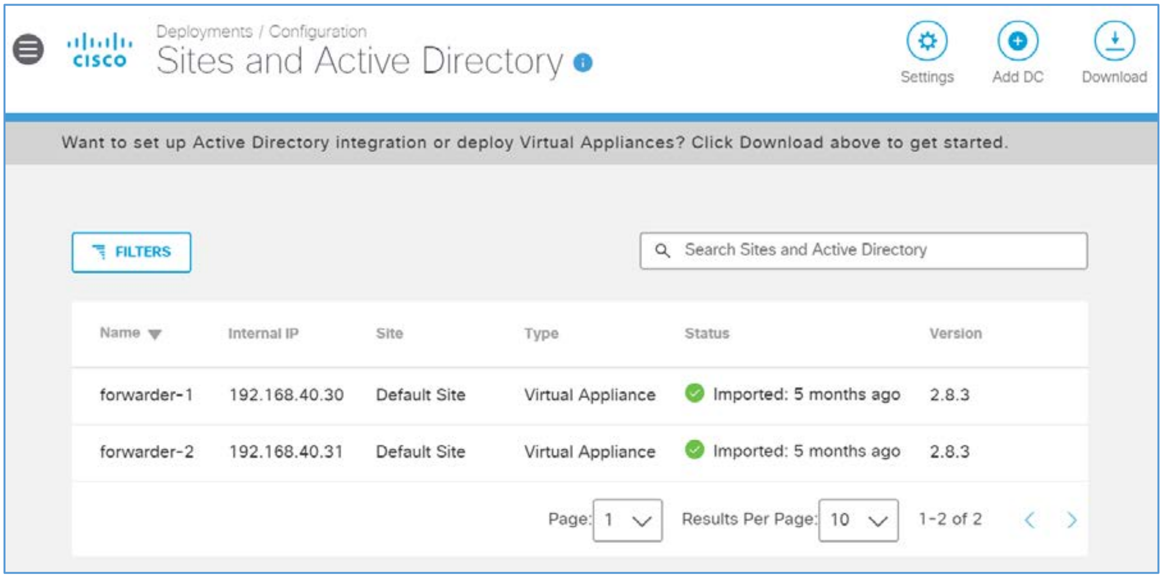
Operating System: Linux

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

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

<u>**Create an Umbrella Site**</u>

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



Deployments / Configuration
Sites and Active Directory
Settings
Add DC
Download

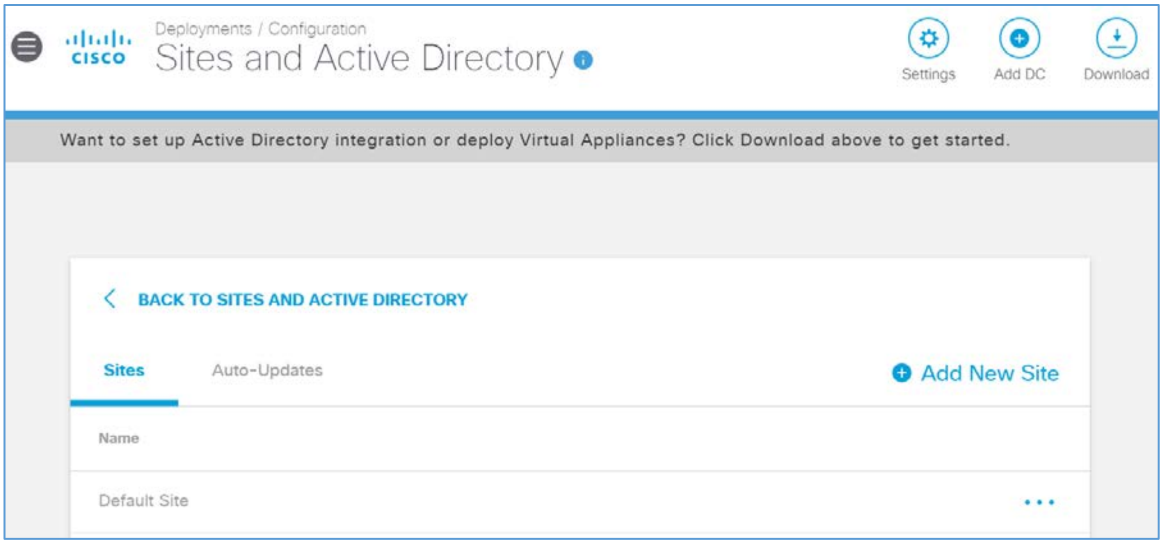
Want to set up Active Directory integration or deploy Virtual Appliances? Click Download above to get started.

FILTERS
Search Sites and Active Directory

Name	Internal IP	Site	Type	Status	Version
forwarder-1	192.168.40.30	Default Site	Virtual Appliance	✓ Imported: 5 months ago	2.8.3
forwarder-2	192.168.40.31	Default Site	Virtual Appliance	✓ Imported: 5 months ago	2.8.3

Page: 1 Results Per Page: 10 1-2 of 2

3. Click **Add New** Site.

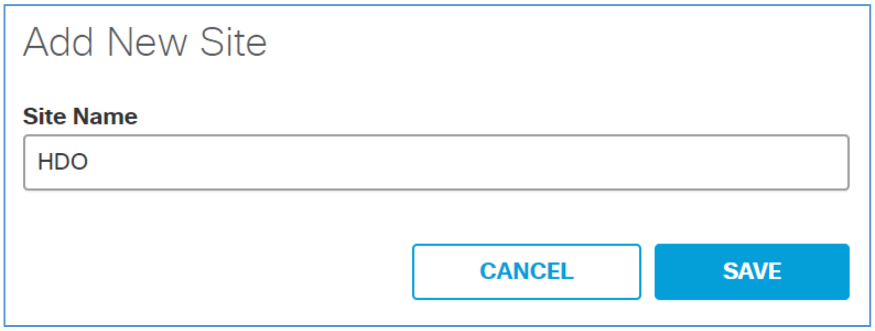

Deployments / Configuration
Sites and Active Directory
Settings
Add DC
Download
BACK TO SITES AND ACTIVE DIRECTORY
Sites
Auto-Updates
Add New Site
Name

Want to set up Active Directory integration or deploy Virtual Appliances? Click Download above to get started.

Default Site

911 4. In the Add New Site popup window, set **Name** to **HDO**.

912 5. Click **Save.**


Add New Site

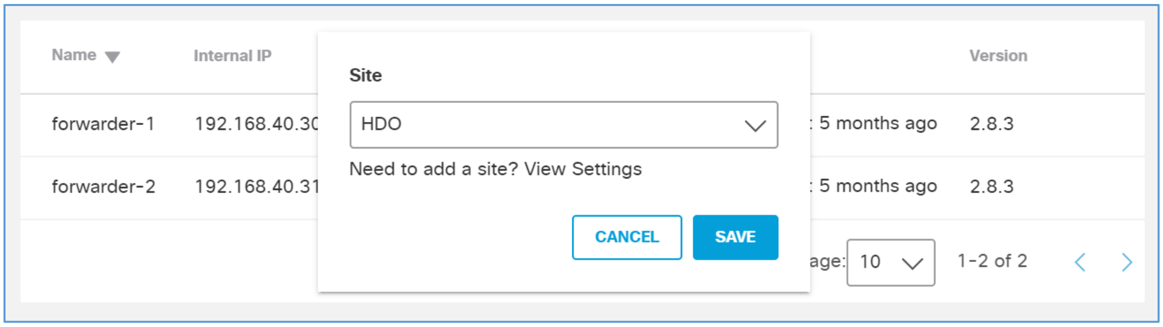
Site Name: HDO

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

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

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

916 9. Click **Save.**



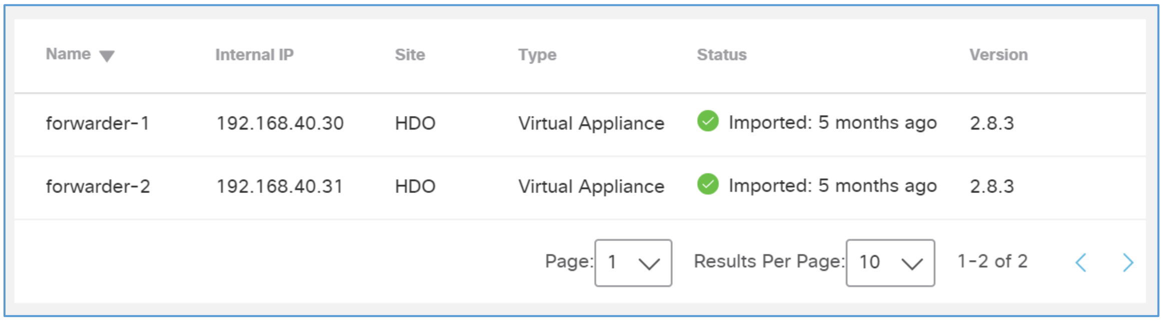
Name ▼	Internal IP		Version
forwarder-1	192.168.40.30	: 5 months ago	2.8.3
forwarder-2	192.168.40.31	: 5 months ago	2.8.3

Site

HDO

Need to add a site? View Settings

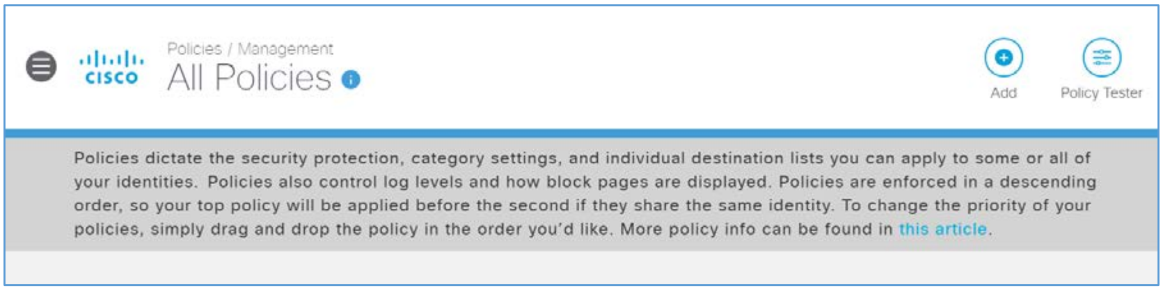
10. Repeat the previous steps for **forwarder-2.**



Name ▼	Internal IP	Site	Type	Status	Version
forwarder-1	192.168.40.30	HDO	Virtual Appliance	✓ Imported: 5 months ago	2.8.3
forwarder-2	192.168.40.31	HDO	Virtual Appliance	✓ Imported: 5 months ago	2.8.3

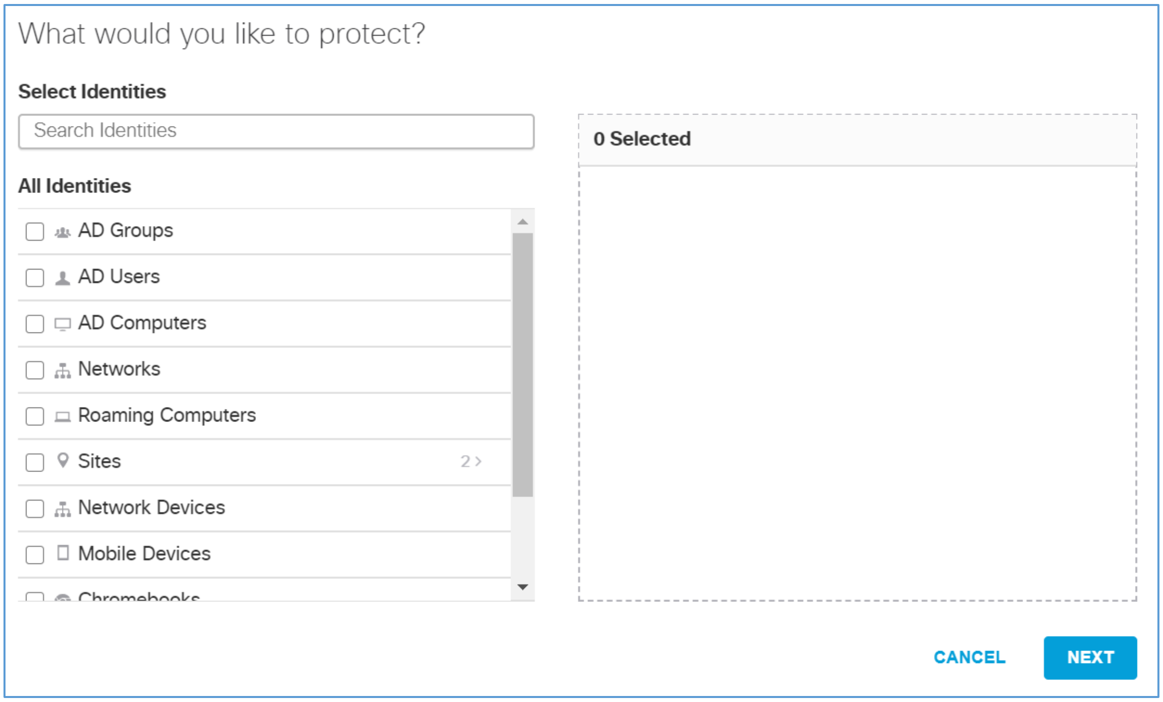
Configure an Umbrella Policy

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



Policies dictate the security protection, category settings, and individual destination lists you can apply to some or all of your identities. Policies also control log levels and how block pages are displayed. Policies are enforced in a descending order, so your top policy will be applied before the second if they share the same identity. To change the priority of your policies, simply drag and drop the policy in the order you'd like. More policy info can be found in this article.

3. Expand the **Sites** identity.



What would you like to protect?

Select Identities

Search Identities

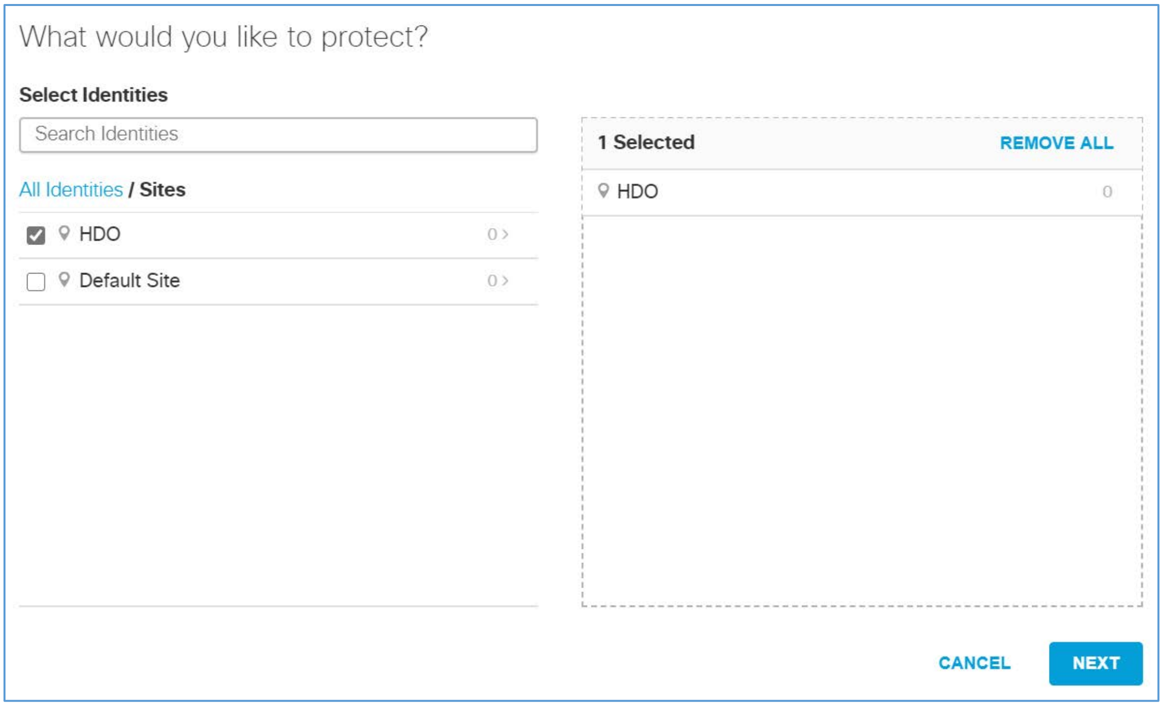
All Identities

- □ AD Groups
- □ AD Users
- □ AD Computers
- □ Networks
- □ Roaming Computers
- □ Sites 2 >
- □ Network Devices
- □ Mobile Devices
- □ Chromebooks

0 Selected

922 4. Select **HDO.**

923 5. Click **Next.**



What would you like to protect?

Select Identities

Search Identities

All Identities / Sites

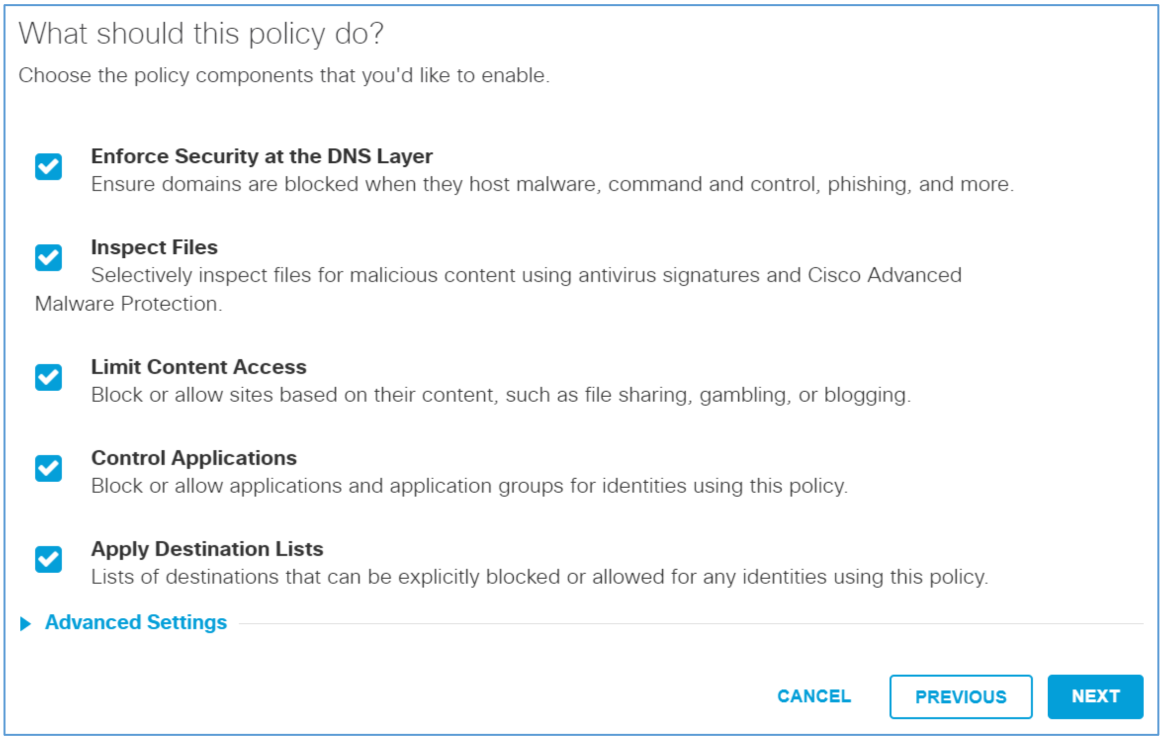
☑ HDO 0 >

□ Default Site 0 >

1 Selected REMOVE ALL

HDO 0

924 6. Click **Next.**



What should this policy do?

Choose the policy components that you'd like to enable.

☑ **Enforce Security at the DNS Layer**
Ensure domains are blocked when they host malware, command and control, phishing, and more.

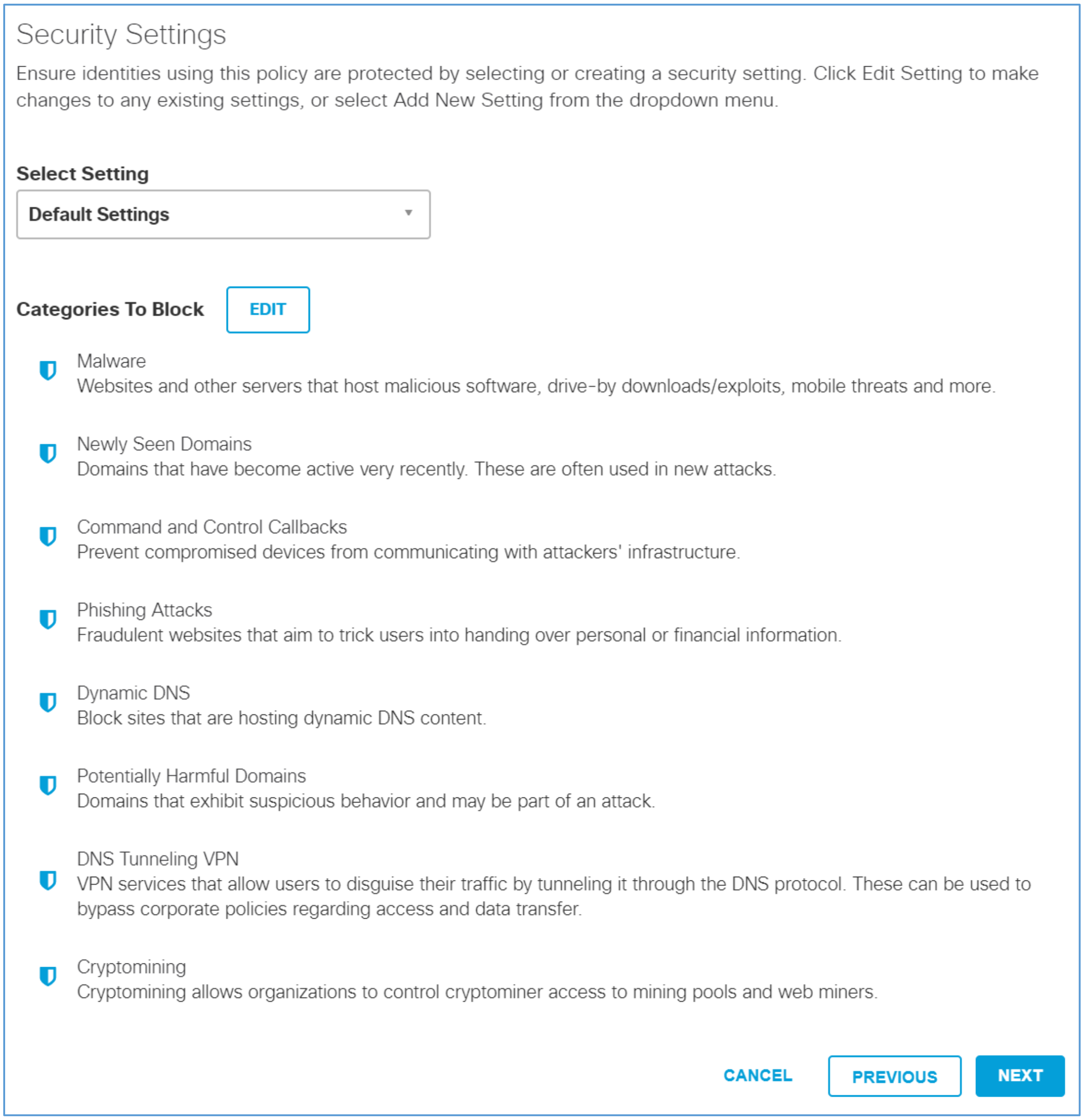
☑ **Inspect Files**
Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.

☑ **Limit Content Access**
Block or allow sites based on their content, such as file sharing, gambling, or blogging.

☑ **Control Applications**
Block or allow applications and application groups for identities using this policy.

☑ **Apply Destination Lists**
Lists of destinations that can be explicitly blocked or allowed for any identities using this policy.

925 7. Click **Next.**



Security Settings

Ensure identities using this policy are protected by selecting or creating a security setting. Click Edit Setting to make changes to any existing settings, or select Add New Setting from the dropdown menu.

Select Setting

Default Settings

Categories To Block

Malware
Websites and other servers that host malicious software, drive-by downloads/exploits, mobile threats and more.

Newly Seen Domains
Domains that have become active very recently. These are often used in new attacks.

Command and Control Callbacks
Prevent compromised devices from communicating with attackers' infrastructure.

Phishing Attacks
Fraudulent websites that aim to trick users into handing over personal or financial information.

Dynamic DNS
Block sites that are hosting dynamic DNS content.

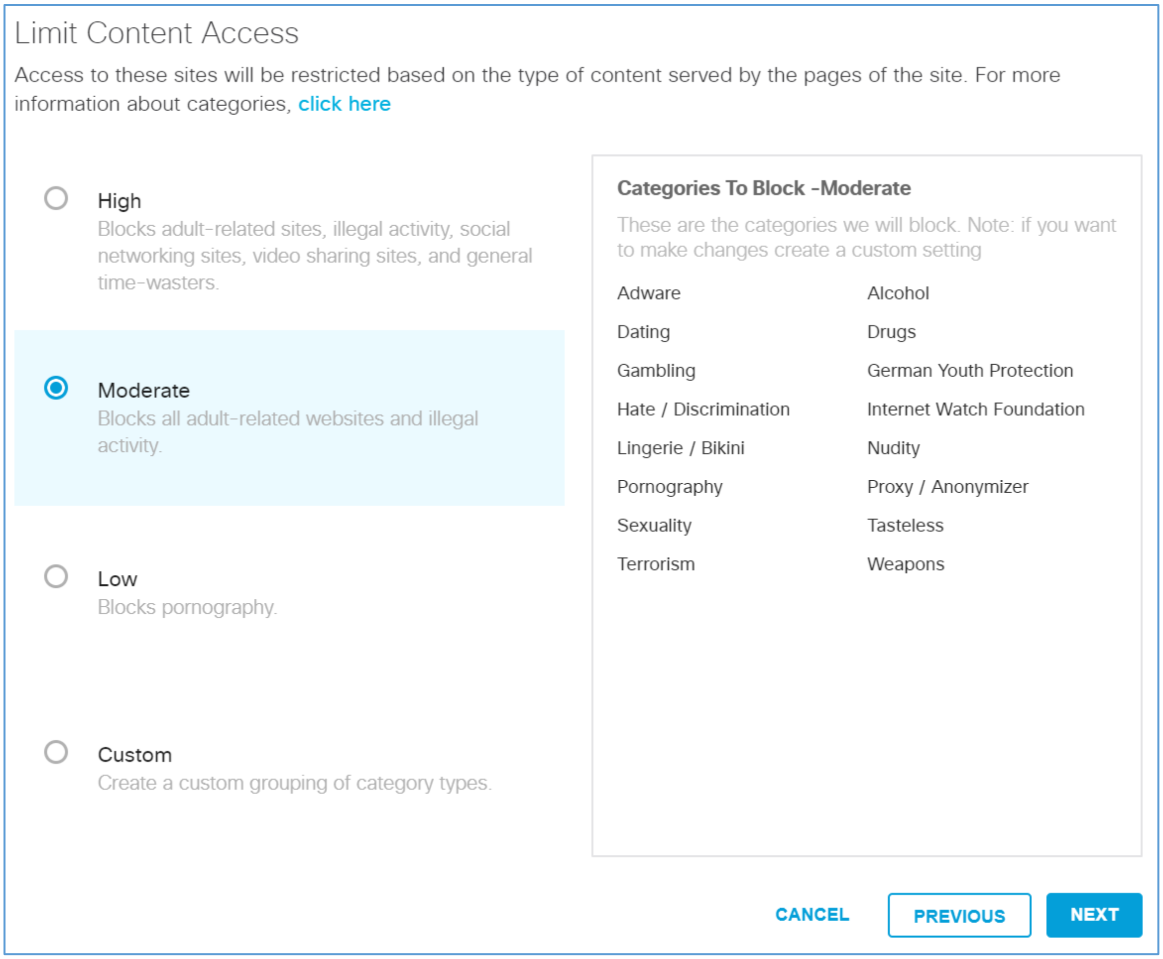
Potentially Harmful Domains
Domains that exhibit suspicious behavior and may be part of an attack.

DNS Tunneling VPN
VPN services that allow users to disguise their traffic by tunneling it through the DNS protocol. These can be used to bypass corporate policies regarding access and data transfer.

Cryptomining
Cryptomining allows organizations to control cryptominer access to mining pools and web miners.

926 8. Select **Moderate**.

927 9. Click **Next.**



Limit Content Access

Access to these sites will be restricted based on the type of content served by the pages of the site. For more information about categories, click here

○ High
Blocks adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters.

● Moderate
Blocks all adult-related websites and illegal activity.

○ Low
Blocks pornography.

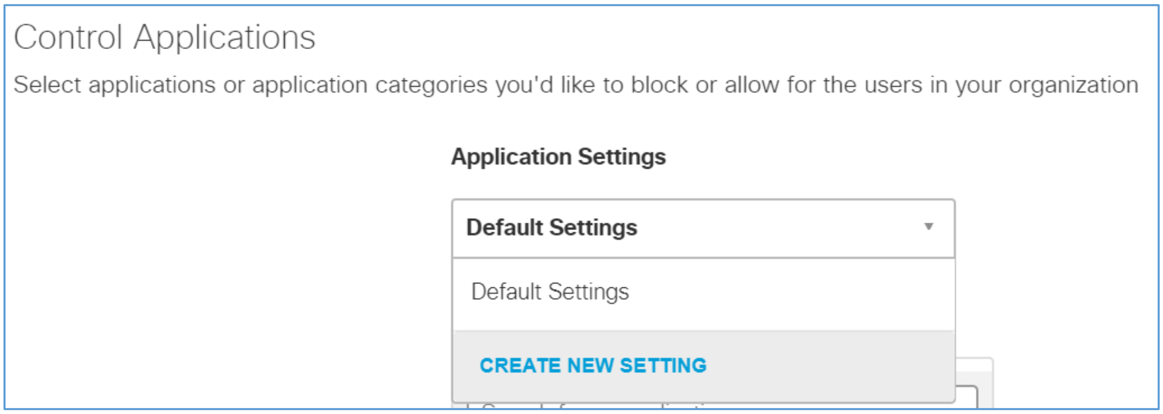
○ Custom
Create a custom grouping of category types.

Categories To Block -Moderate

These are the categories we will block. Note: if you want to make changes create a custom setting

Adware	Alcohol
Dating	Drugs
Gambling	German Youth Protection
Hate / Discrimination	Internet Watch Foundation
Lingerie / Bikini	Nudity
Pornography	Proxy / Anonymizer
Sexuality	Tasteless
Terrorism	Weapons

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



Control Applications

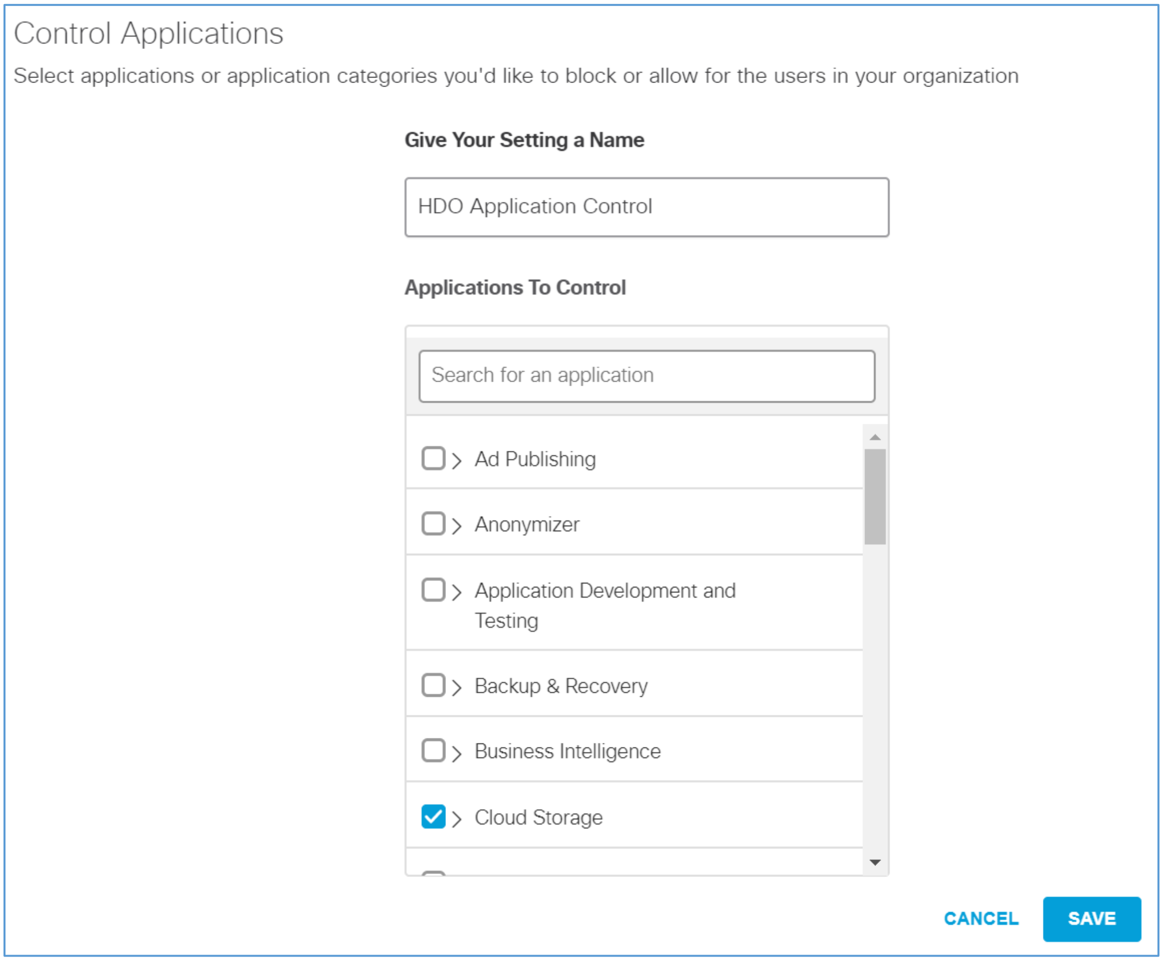
Select applications or application categories you'd like to block or allow for the users in your organization

Application Settings

929 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.**



Control Applications

Select applications or application categories you'd like to block or allow for the users in your organization

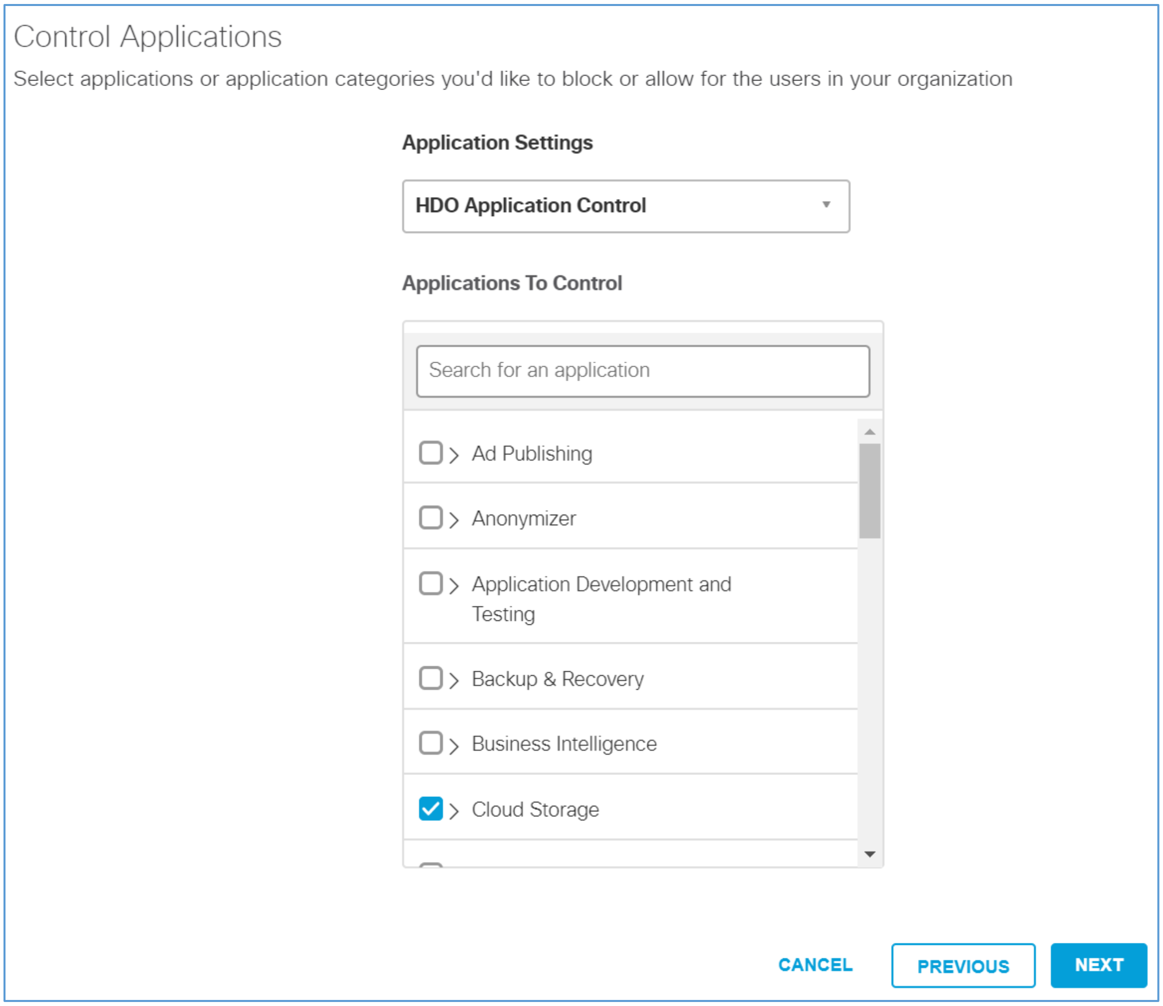
Give Your Setting a Name: HDO Application Control

Applications To Control

Search for an application

- □ > Ad Publishing
- □ > Anonymizer
- □ > Application Development and Testing
- □ > Backup & Recovery
- □ > Business Intelligence
- ☑ > Cloud Storage

13. Click **Next.**



Control Applications

Select applications or application categories you'd like to block or allow for the users in your organization

Application Settings

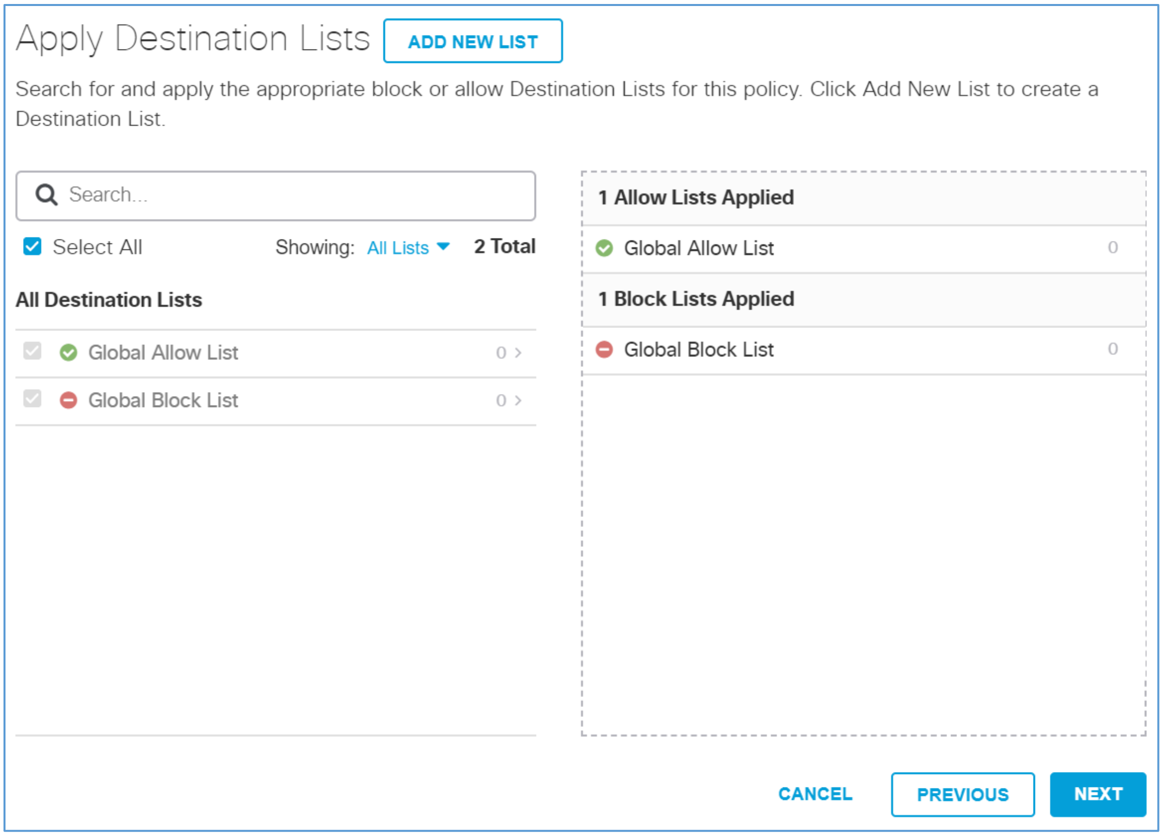
HDO Application Control

Applications To Control

Search for an application

- □ Ad Publishing
- □ Anonymizer
- □ Application Development and Testing
- □ Backup & Recovery
- □ Business Intelligence
- ☑ Cloud Storage

934 14. Click **Next.**



Apply Destination Lists

Search for and apply the appropriate block or allow Destination Lists for this policy. Click Add New List to create a Destination List.

☑ Select All Showing: All Lists 2 Total

All Destination Lists

- ☑ Global Allow List 0
- ☑ Global Block List 0

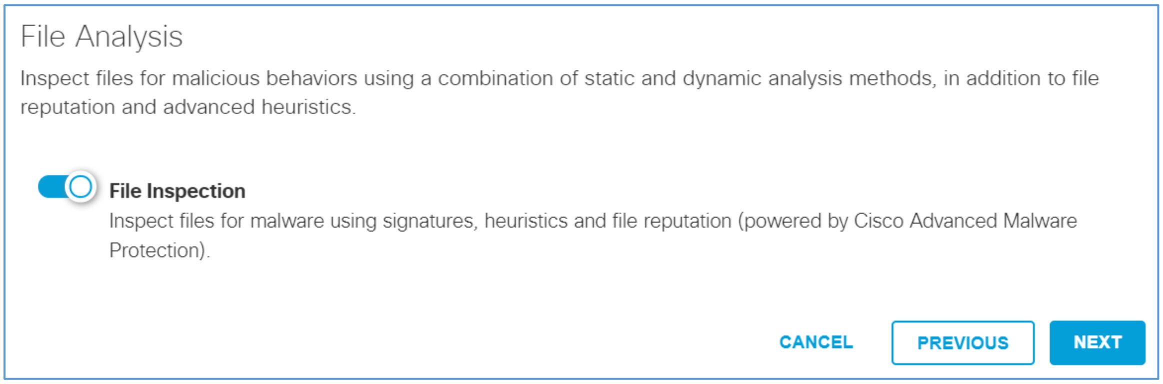
1 Allow Lists Applied

- Global Allow List 0

1 Block Lists Applied

- Global Block List 0

935 15. Click **Next.**



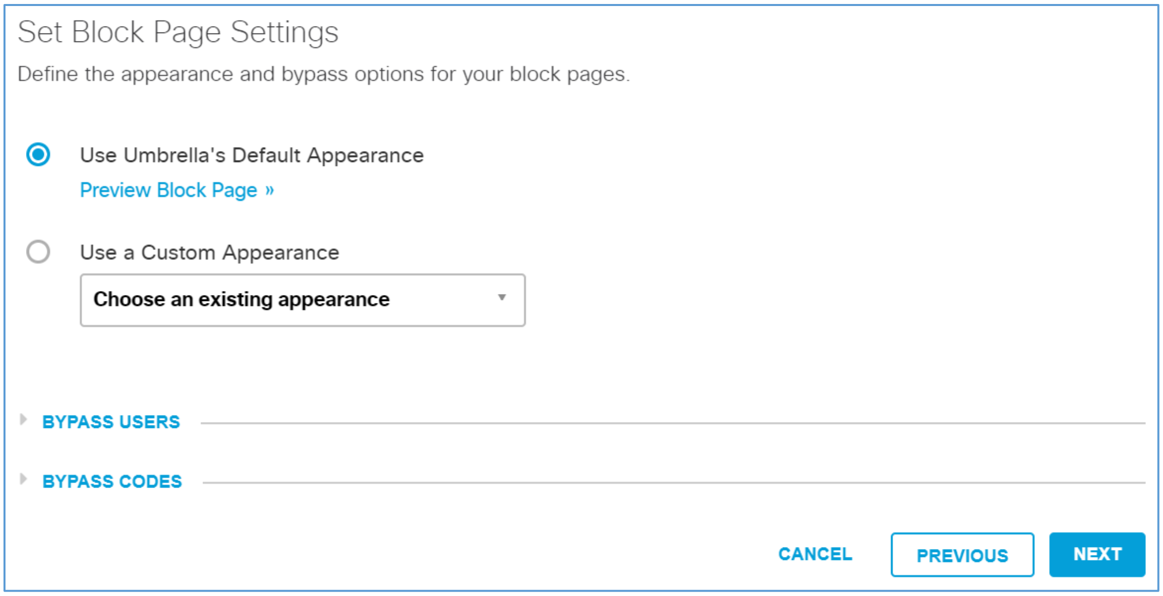
File Analysis

Inspect files for malicious behaviors using a combination of static and dynamic analysis methods, in addition to file reputation and advanced heuristics.

File Inspection

Inspect files for malware using signatures, heuristics and file reputation (powered by Cisco Advanced Malware Protection).

936 16. Click **Next.**



Set Block Page Settings

Define the appearance and bypass options for your block pages.

● Use Umbrella's Default Appearance

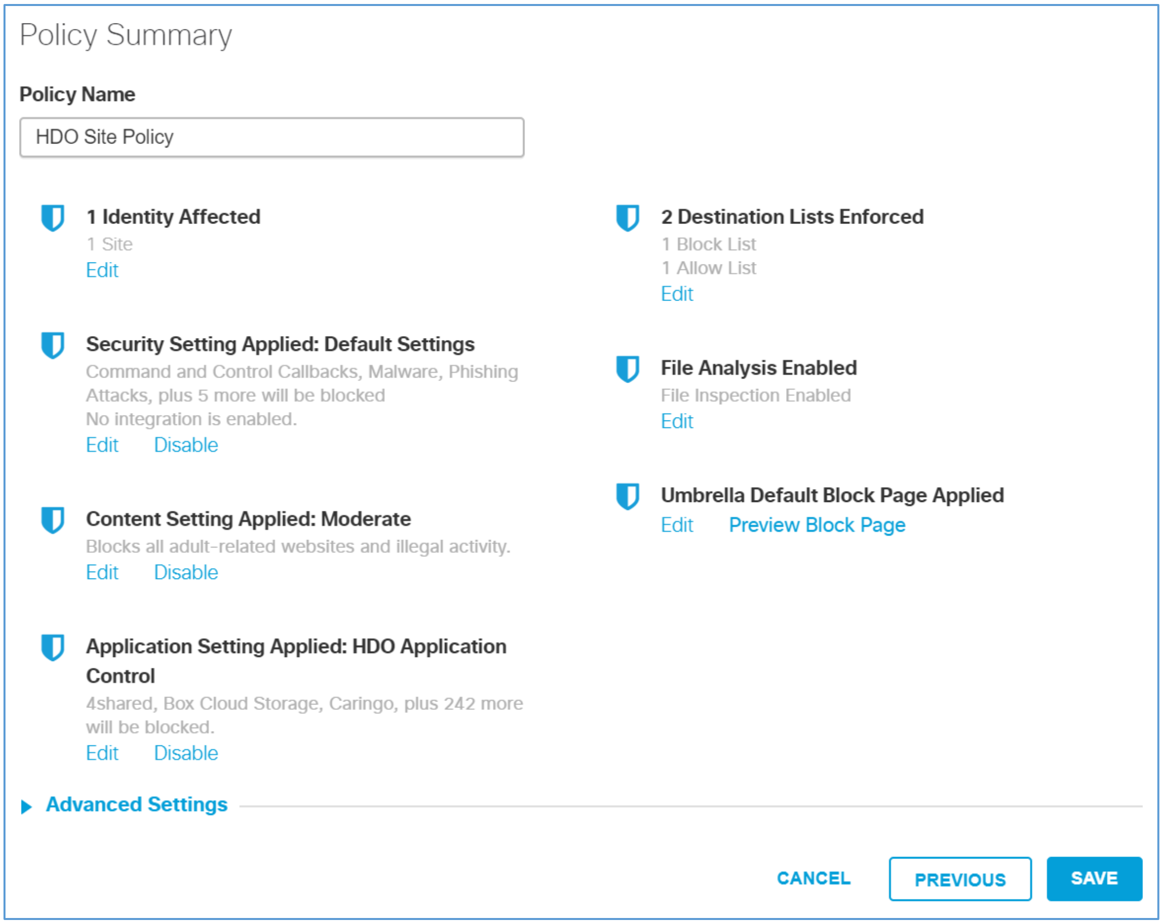
Preview Block Page »

○ Use a Custom Appearance

Choose an existing appearance

937 17. In the Policy Summary screen, set the **Name** to **HDO Site Policy**.

938 18. Click **Save.**



Policy Summary

Policy Name

HDO Site Policy

1 Identity Affected
1 Site
Edit

2 Destination Lists Enforced
1 Block List
1 Allow List
Edit

Security Setting Applied: Default Settings
Command and Control Callbacks, Malware, Phishing Attacks, plus 5 more will be blocked
No integration is enabled.
Edit Disable

File Analysis Enabled
File Inspection Enabled
Edit

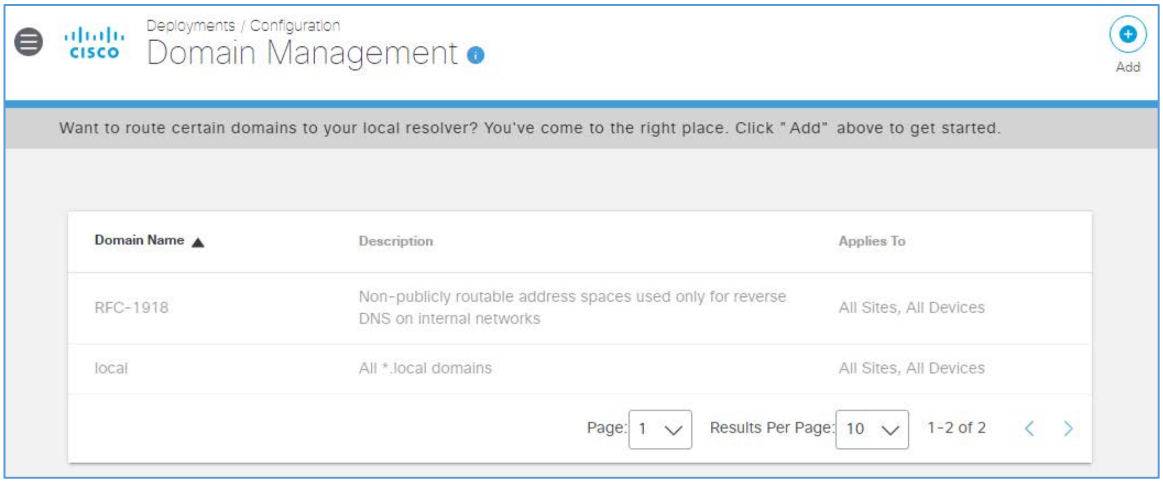
Umbrella Default Block Page Applied
Edit Preview Block Page

Content Setting Applied: Moderate
Blocks all adult-related websites and illegal activity.
Edit Disable

Application Setting Applied: HDO Application Control
4shared, Box Cloud Storage, Caringo, plus 242 more will be blocked.
Edit Disable

Configure Windows Domain Controller as the Local DNS Provider

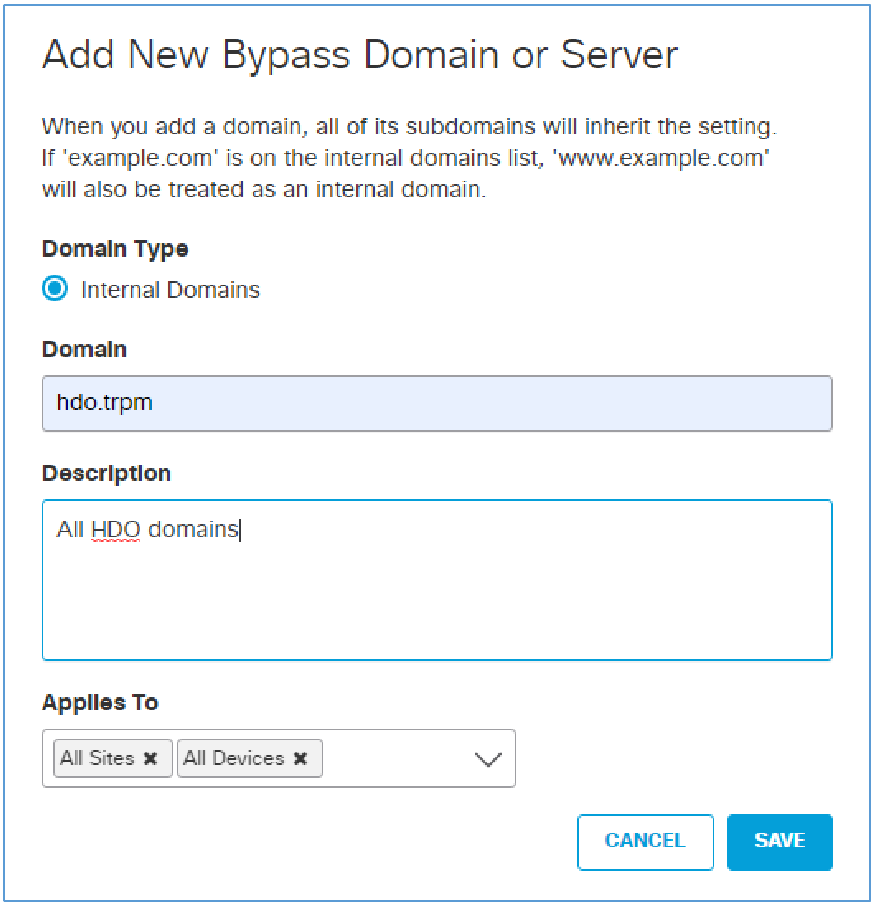
1. Click **Deployments > Configuration > Domain Management**.
2. Click **Add.**



Want to route certain domains to your local resolver? You've come to the right place. Click " Add" above to get started.

Domain Name ▲	Description	Applies To
RFC-1918	Non-publicly routable address spaces used only for reverse DNS on internal networks	All Sites, All Devices
local	All *.local domains	All Sites, All Devices

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



Add New Bypass Domain or Server

When you add a domain, all of its subdomains will inherit the setting. If 'example.com' is on the internal domains list, 'www.example.com' will also be treated as an internal domain.

Domain Type

● Internal Domains

Domain

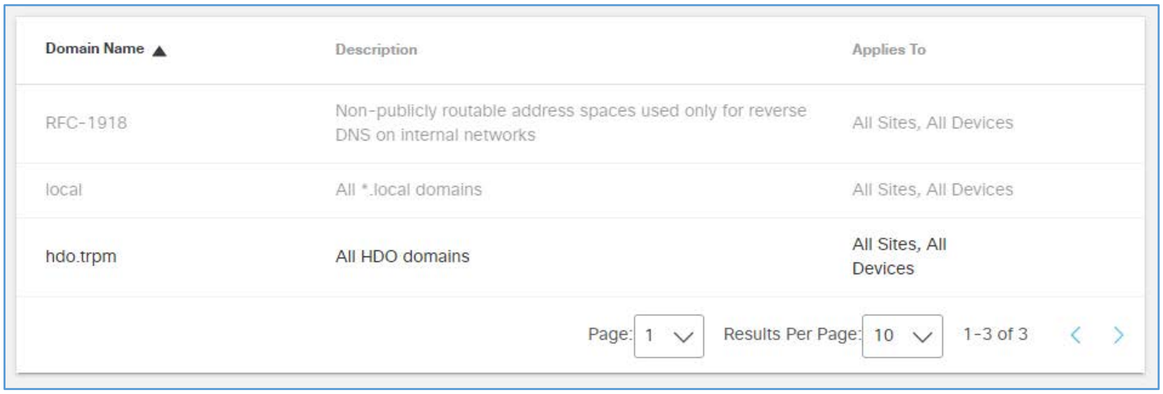
hdo.trpm

Description

All HDO domains

Applies To

All Sites ✖ All Devices ✖



Domain Name ▲	Description	Applies To
RFC-1918	Non-publicly routable address spaces used only for reverse DNS on internal networks	All Sites, All Devices
local	All *.local domains	All Sites, All Devices
hdo.trpm	All HDO domains	All Sites, All Devices

Page: 1 Results Per Page: 10 1-3 of 3

2.2.3.3 LogRhythm XDR (Extended Detection and Response)

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

System Requirements

CPU: 20 virtual central processing unit (vCPU)

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.

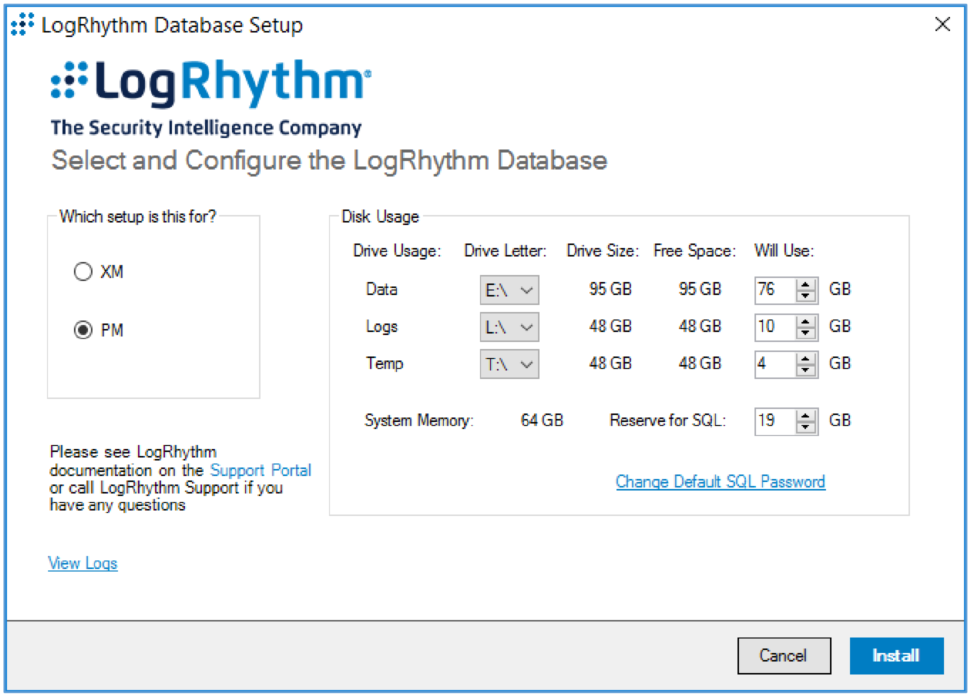
Download Installation Packages

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. Provide the following information:
    a. Which setup is this for?: PM
    b. Disk Usage:

Data: E:\
Logs: L:\
Temp: T:\



LogRhythm Database Setup

LogRhythm
The Security Intelligence Company
Select and Configure the LogRhythm Database

Which setup is this for?

○ XM
● PM

Disk Usage

Drive Usage:	Drive Letter:	Drive Size:	Free Space:	Will Use:	
Data	E:\	95 GB	95 GB	76	GB
Logs	L:\	48 GB	48 GB	10	GB
Temp	T:\	48 GB	48 GB	4	GB

System Memory: 64 GB Reserve for SQL: 19 GB

Change Default SQL Password

Please see LogRhythm documentation on the Support Portal or call LogRhythm Support if you have any questions

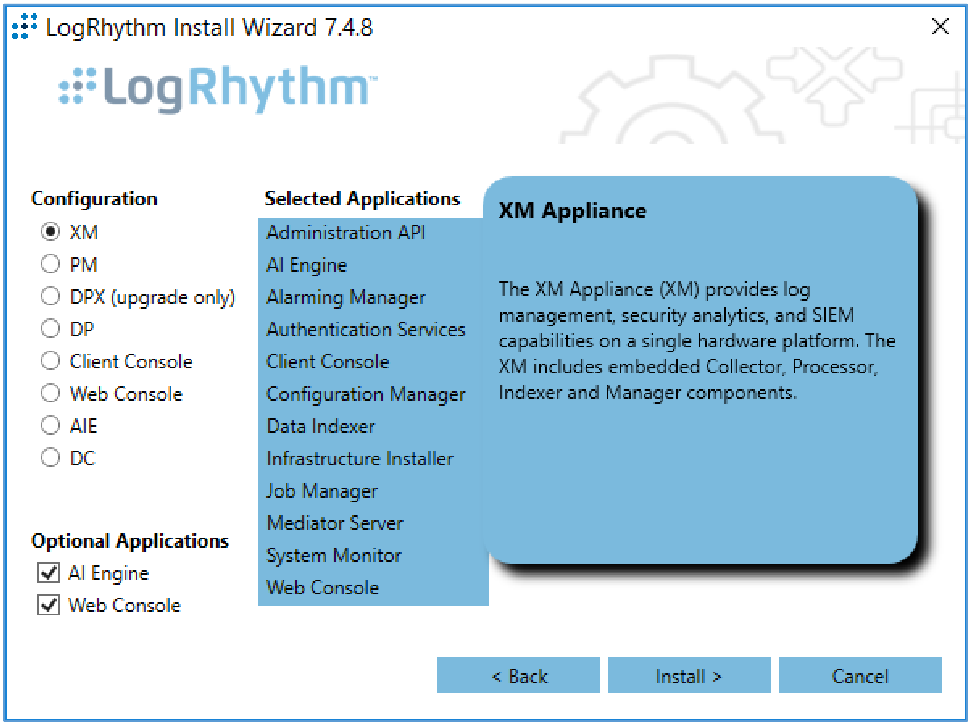
View Logs

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.**



Configuration
● XM
○ PM
○ DPX (upgrade only)
○ DP
○ Client Console
○ Web Console
○ AIE
○ DC

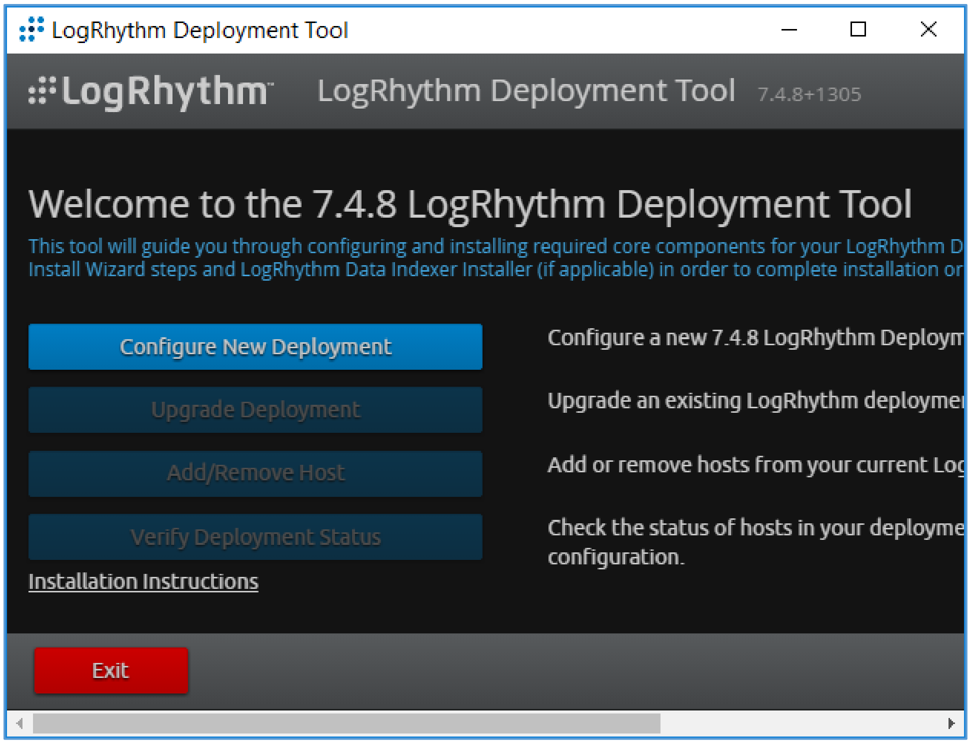
Optional Applications
☑ AI Engine
☑ Web Console

Selected Applications
Administration API
AI Engine
Alarming Manager
Authentication Services
Client Console
Configuration Manager
Data Indexer
Infrastructure Installer
Job Manager
Mediator Server
System Monitor
Web Console

XM Appliance

The XM Appliance (XM) provides log management, security analytics, and SIEM capabilities on a single hardware platform. The XM includes embedded Collector, Processor, Indexer and Manager components.

11. A **LogRhythm Deployment Tool** window displays.
12. Click **Configure New Deployment.**



LogRhythm Deployment Tool

LogRhythm Deployment Tool 7.4.8+1305

Welcome to the 7.4.8 LogRhythm Deployment Tool

This tool will guide you through configuring and installing required core components for your LogRhythm D
Install Wizard steps and LogRhythm Data Indexer Installer (if applicable) in order to complete installation or

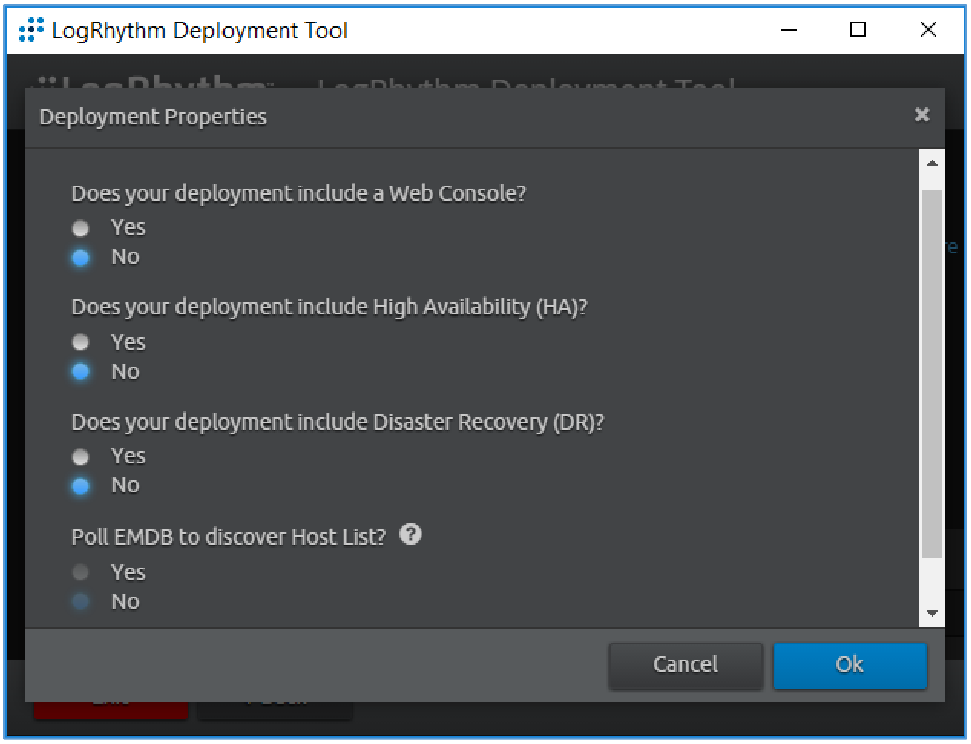
Configure a new 7.4.8 LogRhythm Deploym

Upgrade an existing LogRhythm deployme

Add or remove hosts from your current Log

Check the status of hosts in your deployme
configuration.

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



Deployment Properties

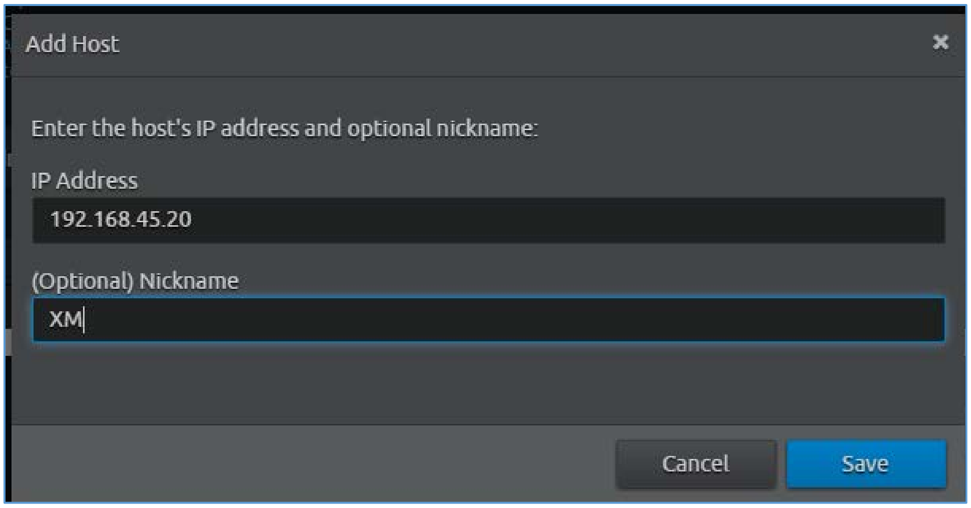
Does your deployment include a Web Console?
○ Yes
● No

Does your deployment include High Availability (HA)?
○ Yes
● No

Does your deployment include Disaster Recovery (DR)?
○ Yes
● No

Poll EMDB to discover Host List?
○ Yes
● No

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.**

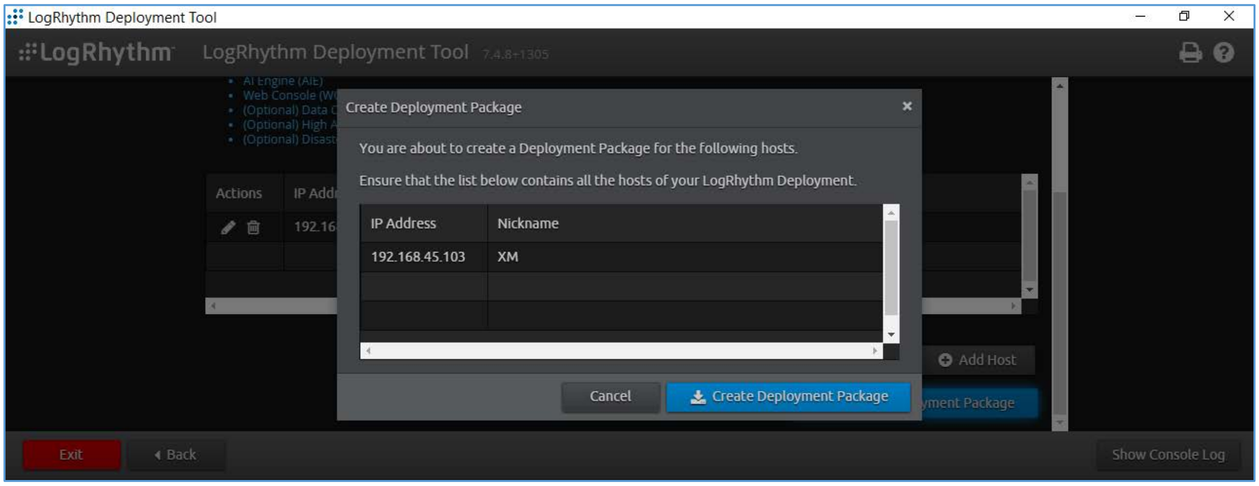


Enter the host's IP address and optional nickname:

IP Address: 192.168.45.20

(Optional) Nickname: XM

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.**

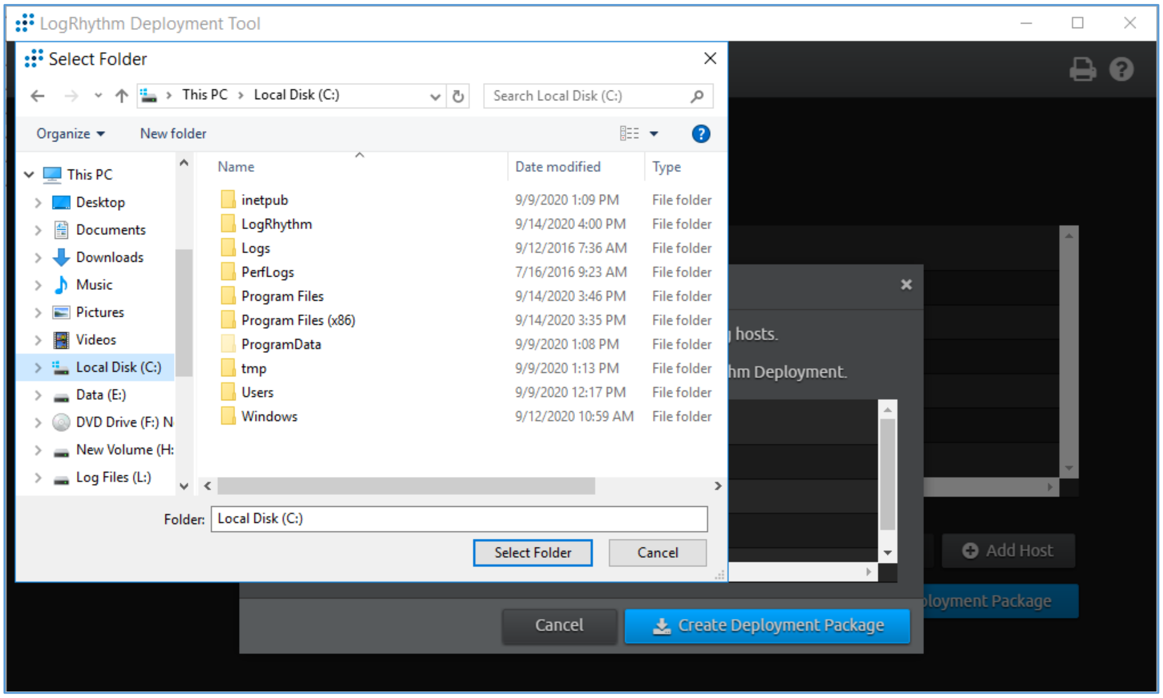


You are about to create a Deployment Package for the following hosts.

Ensure that the list below contains all the hosts of your LogRhythm Deployment.

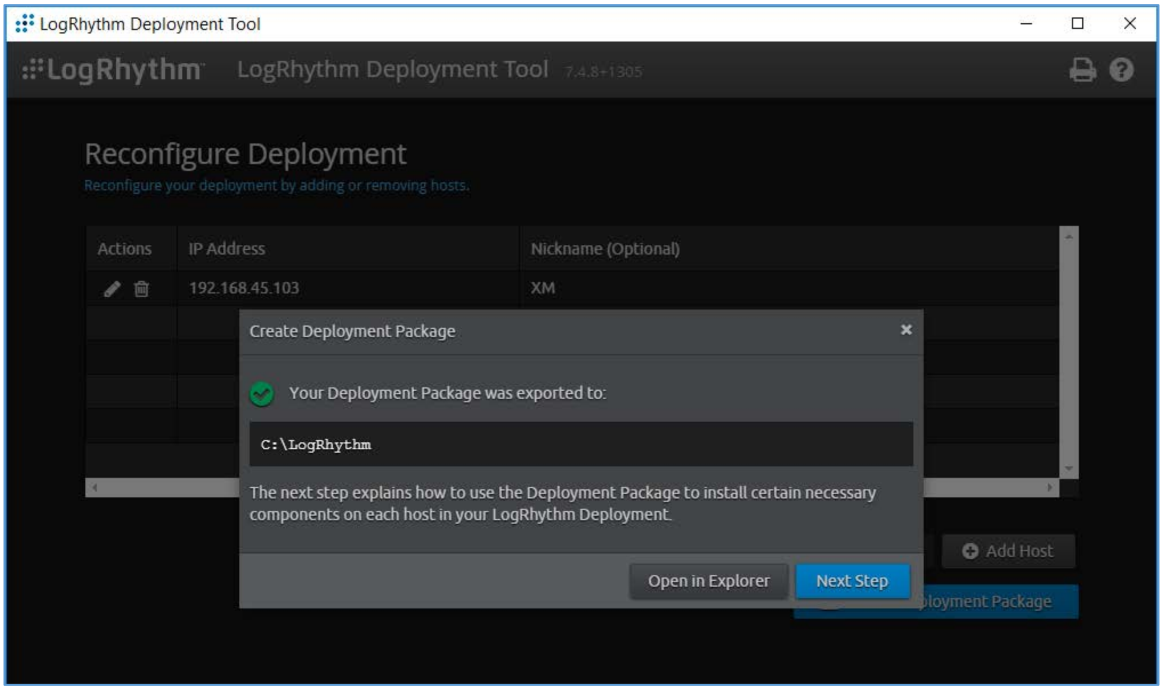
IP Address	Nickname
192.168.45.103	XM

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



Name	Date modified	Type
inetpub	9/9/2020 1:09 PM	File folder
LogRhythm	9/14/2020 4:00 PM	File folder
Logs	9/12/2016 7:36 AM	File folder
PerfLogs	7/16/2016 9:23 AM	File folder
Program Files	9/14/2020 3:46 PM	File folder
Program Files (x86)	9/14/2020 3:35 PM	File folder
ProgramData	9/9/2020 1:08 PM	File folder
tmp	9/9/2020 1:13 PM	File folder
Users	9/9/2020 12:17 PM	File folder
Windows	9/12/2020 10:59 AM	File folder

1009 22. Click **Next Step.**


LogRhythm Deployment Tool
LogRhythm
LogRhythm Deployment Tool 7.4.8+1305
Reconfigure Deployment
Reconfigure your deployment by adding or removing hosts.
Actions
IP Address
Nickname (Optional)
Create Deployment Package
Open in Explorer
Next Step
Add Host

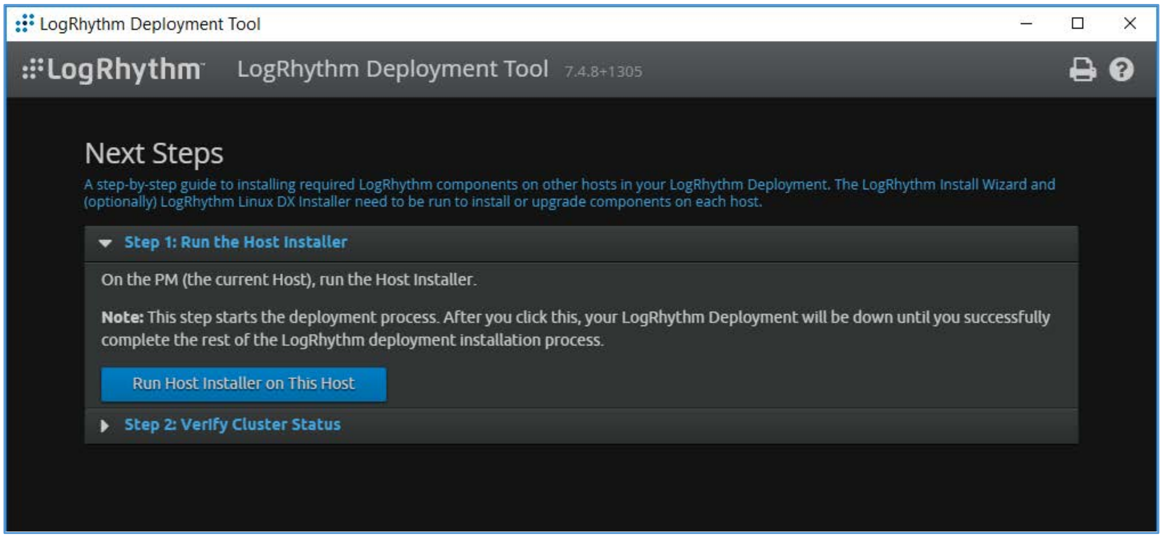
Actions	IP Address	Nickname (Optional)
	192.168.45.103	XM

Your Deployment Package was exported to:

```
C:\LogRhythm
```

The next step explains how to use the Deployment Package to install certain necessary components on each host in your LogRhythm Deployment.

1010 23. Click **Run Host Installer on this Host.**



LogRhythm Deployment Tool
LogRhythm
LogRhythm Deployment Tool 7.4.8+1305

Next Steps

A step-by-step guide to installing required LogRhythm components on other hosts in your LogRhythm Deployment. The LogRhythm Install Wizard and (optionally) LogRhythm Linux DX Installer need to be run to install or upgrade components on each host.

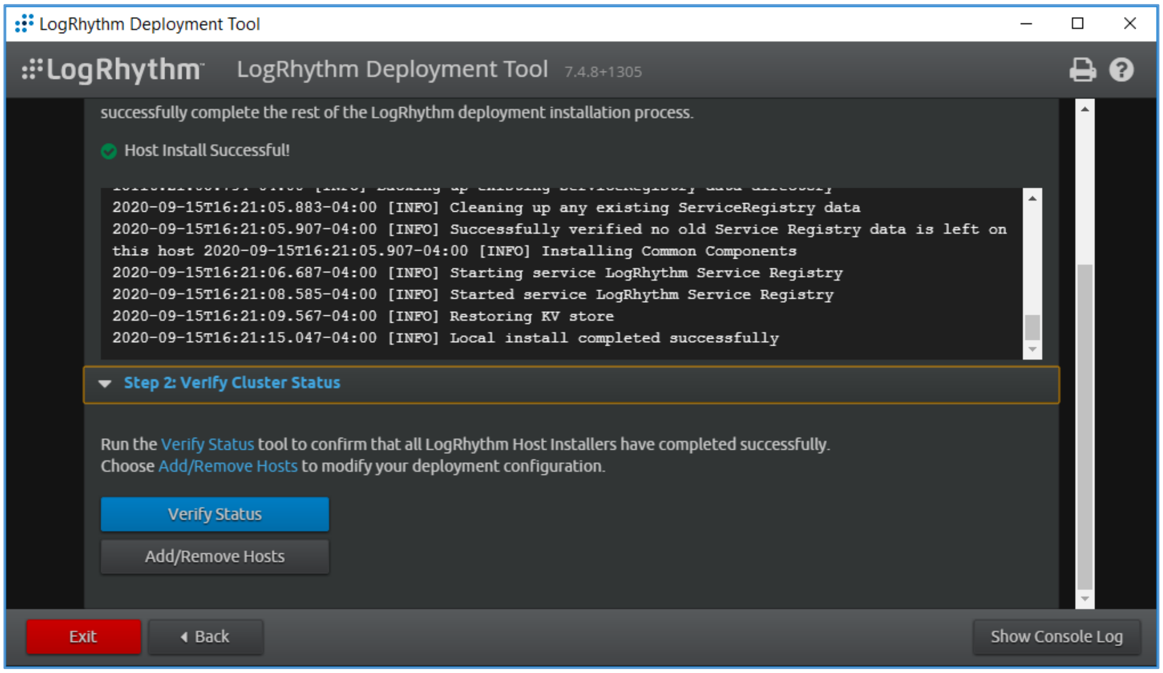
Step 1: Run the Host Installer

On the PM (the current Host), run the Host Installer.

Note: This step starts the deployment process. After you click this, your LogRhythm Deployment will be down until you successfully complete the rest of the LogRhythm deployment installation process.

Step 2: Verify Cluster Status

1011 24. After the Host Installer has finished, click **Verify Status.**



LogRhythm Deployment Tool
LogRhythm
LogRhythm Deployment Tool 7.4.8+1305

successfully complete the rest of the LogRhythm deployment installation process.

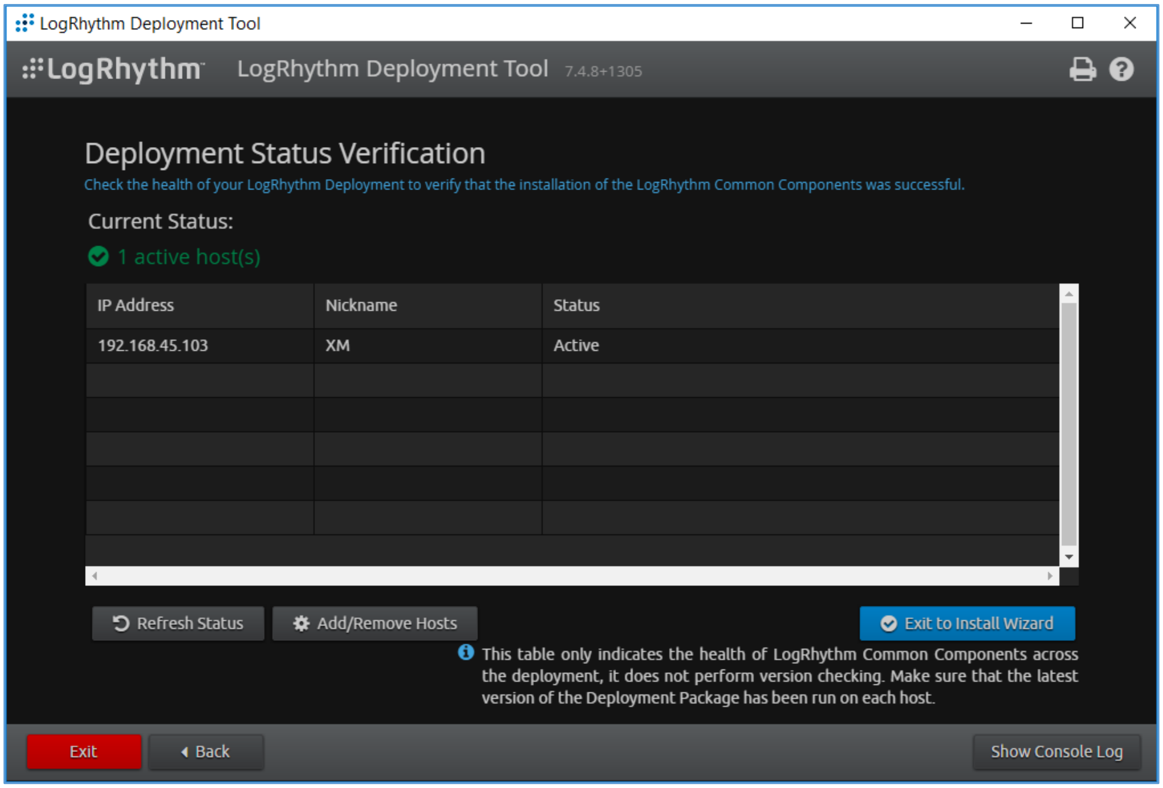
Host Install Successful!

```
2020-09-15T16:21:05.883-04:00 [INFO] Cleaning up any existing ServiceRegistry data
2020-09-15T16:21:05.907-04:00 [INFO] Successfully verified no old Service Registry data is left on
this host 2020-09-15T16:21:05.907-04:00 [INFO] Installing Common Components
2020-09-15T16:21:06.687-04:00 [INFO] Starting service LogRhythm Service Registry
2020-09-15T16:21:08.585-04:00 [INFO] Started service LogRhythm Service Registry
2020-09-15T16:21:09.567-04:00 [INFO] Restoring KV store
2020-09-15T16:21:15.047-04:00 [INFO] Local install completed successfully
```

Step 2: Verify Cluster Status

Run the Verify Status tool to confirm that all LogRhythm Host Installers have completed successfully.
Choose Add/Remove Hosts to modify your deployment configuration.

1012 25. Click **Exit to Install Wizard.**



Deployment Status Verification

Check the health of your LogRhythm Deployment to verify that the installation of the LogRhythm Common Components was successful.

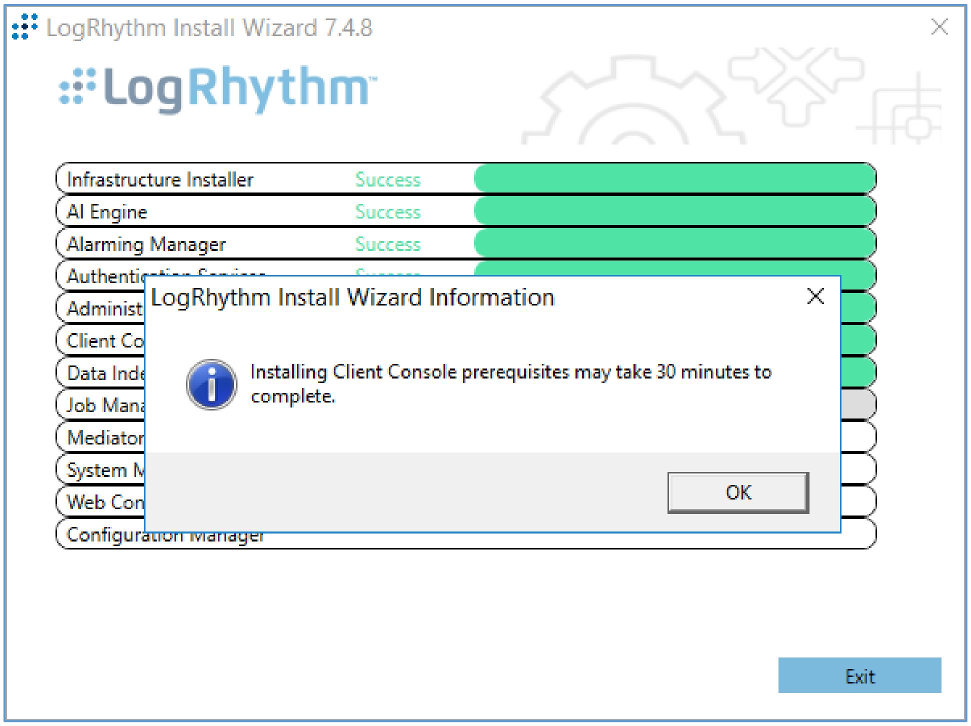
Current Status:

1 active host(s)

IP Address	Nickname	Status
192.168.45.103	XM	Active

This table only indicates the health of LogRhythm Common Components across the deployment, it does not perform version checking. Make sure that the latest version of the Deployment Package has been run on each host.

26. A notification window displays stating the installation could take up to 30 minutes. Click **OK.**



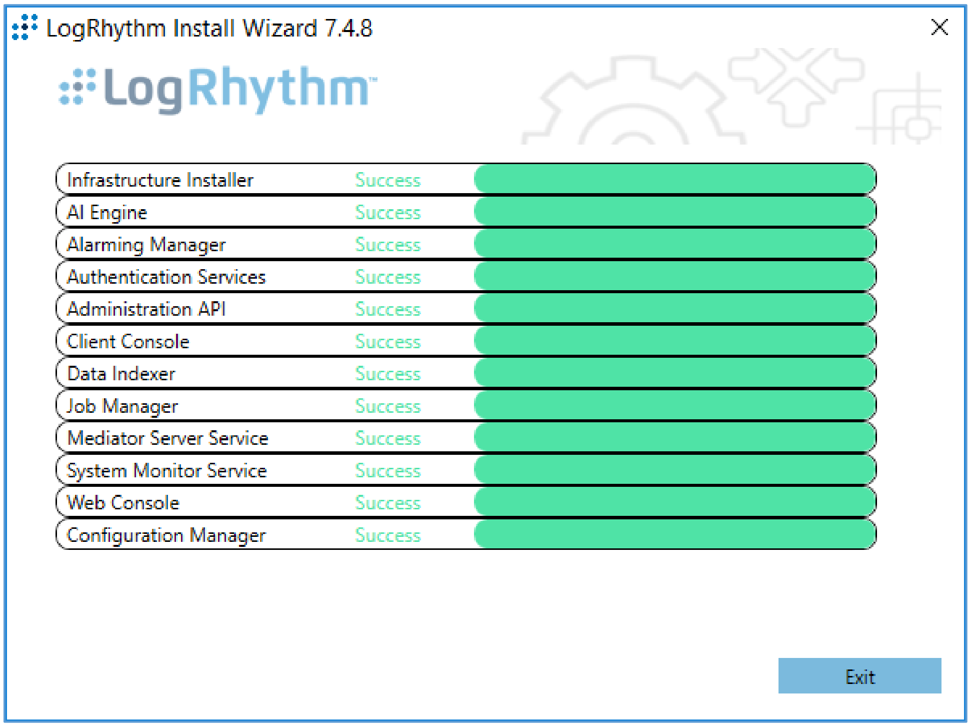
LogRhythm Install Wizard 7.4.8

Infrastructure Installer	Success
AI Engine	Success
Alarming Manager	Success
Authentic	
Administ	
Client Co	
Data Inde	
Job Mana	
Mediator	
System M	
Web Con	
Configuration Manager	

LogRhythm Install Wizard Information

Installing Client Console prerequisites may take 30 minutes to complete.

1014 27. After the Install Wizard has successfully installed the services, click **Exit.**



LogRhythm Install Wizard 7.4.8

Infrastructure Installer	Success
AI Engine	Success
Alarming Manager	Success
Authentication Services	Success
Administration API	Success
Client Console	Success
Data Indexer	Success
Job Manager	Success
Mediator Server Service	Success
System Monitor Service	Success
Web Console	Success
Configuration Manager	Success

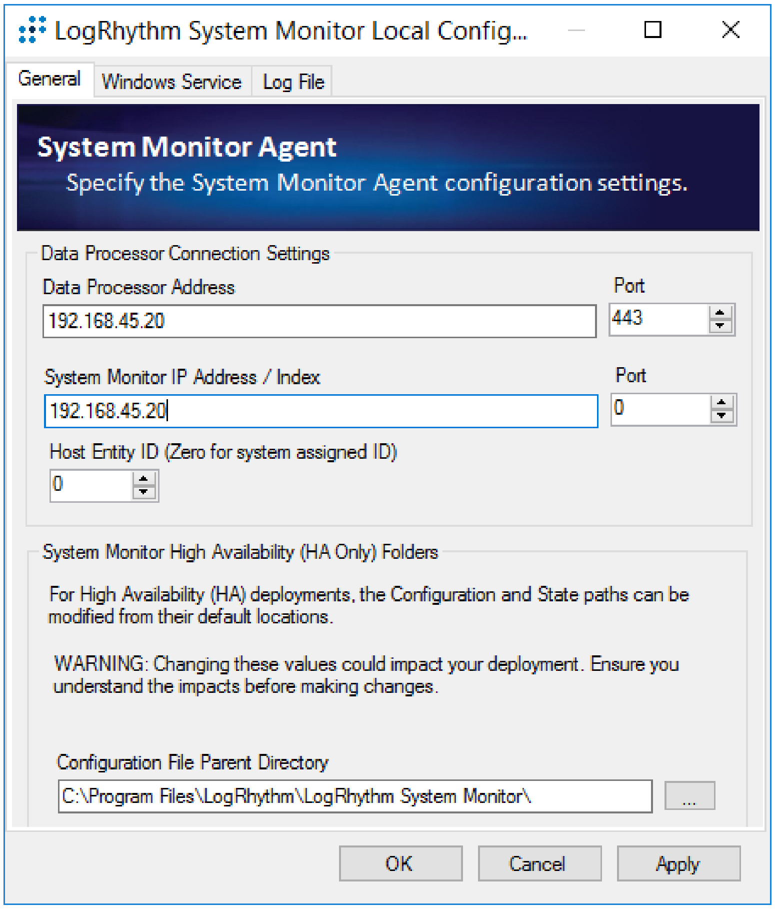
LogRhythm XDR Configuration

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.**



System Monitor Agent

Specify the System Monitor Agent configuration settings.

Data Processor Connection Settings

Data Processor Address: 192.168.45.20

Port: 443

System Monitor IP Address / Index: 192.168.45.20

Port: 0

Host Entity ID (Zero for system assigned ID): 0

System Monitor High Availability (HA Only) Folders

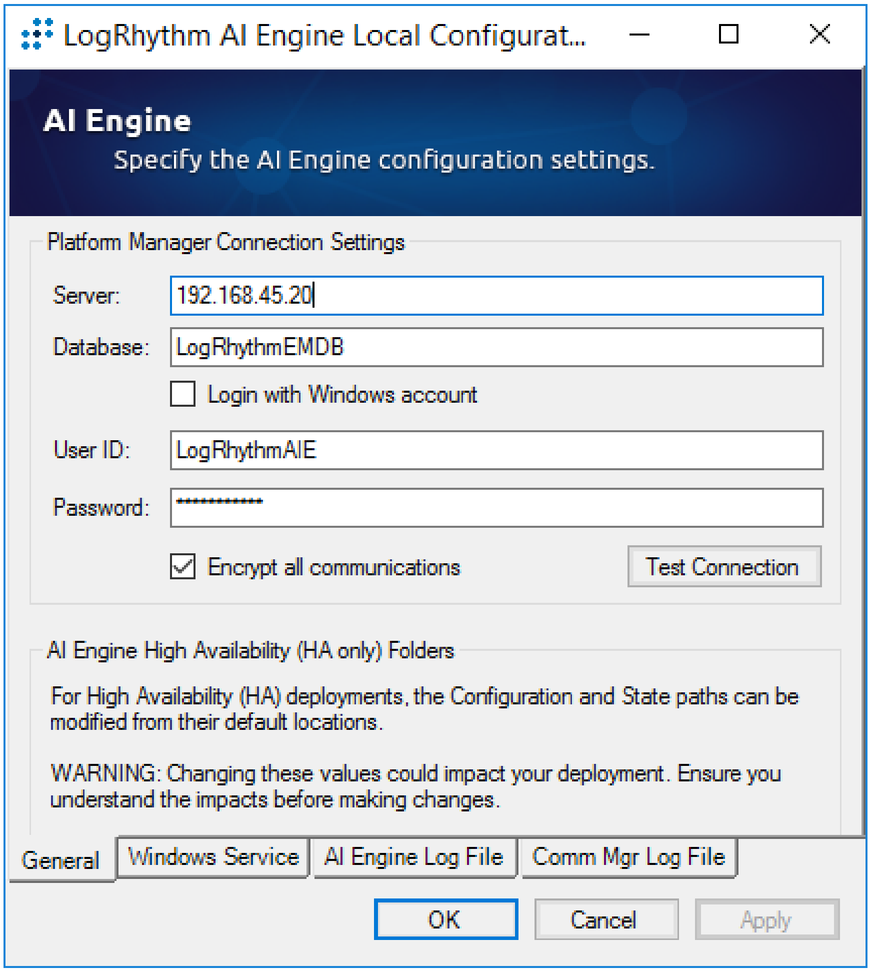
For High Availability (HA) deployments, the Configuration and State paths can be modified from their default locations.

WARNING: Changing these values could impact your deployment. Ensure you understand the impacts before making changes.

Configuration File Parent Directory: C:\Program Files\LogRhythm\LogRhythm System Monitor\

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.**



AI Engine

Specify the AI Engine configuration settings.

Platform Manager Connection Settings

Server: 192.168.45.20

Database: LogRhythmEMDB

☐ Login with Windows account

User ID: LogRhythmAIE

Password: ************

☑ Encrypt all communications

AI Engine High Availability (HA only) Folders

For High Availability (HA) deployments, the Configuration and State paths can be modified from their default locations.

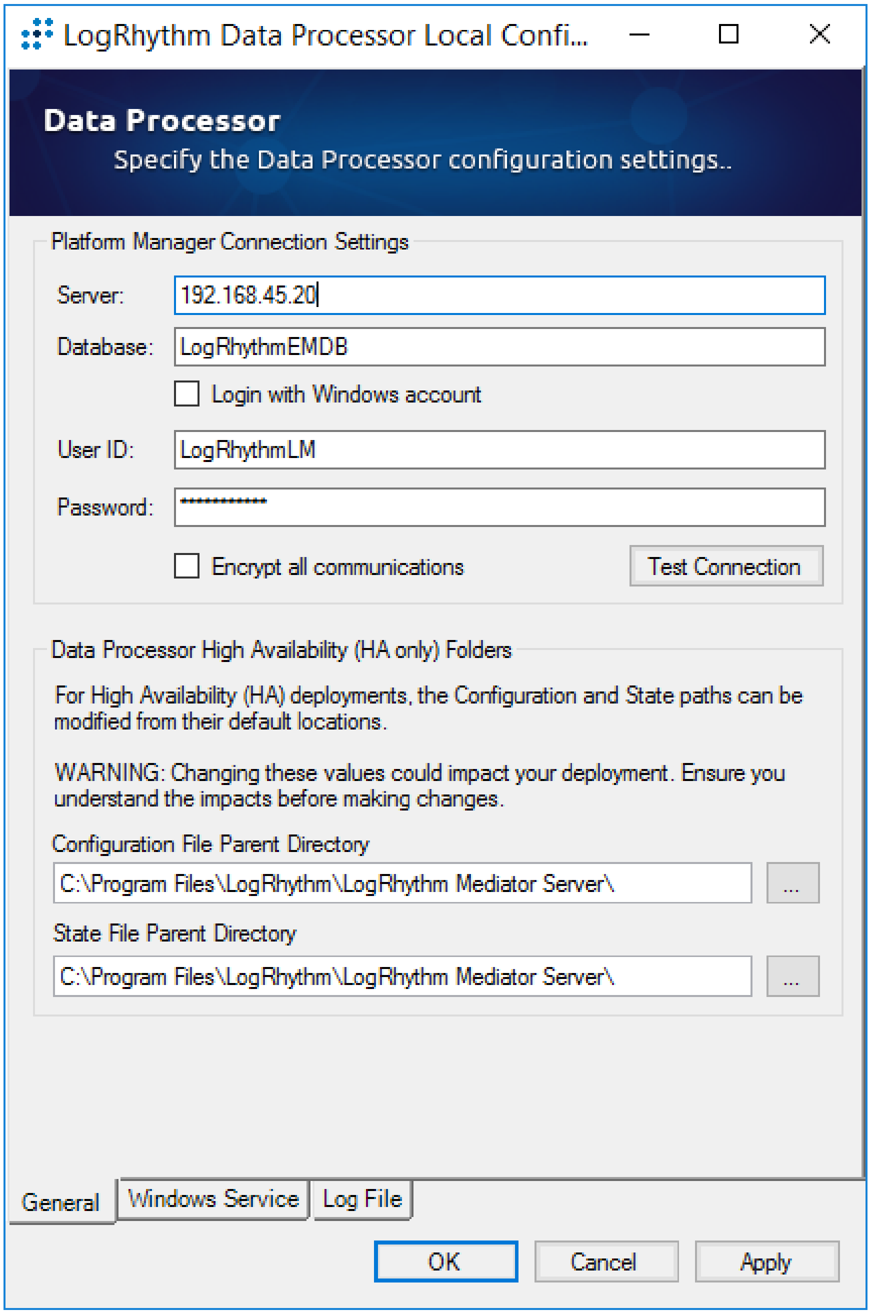
WARNING: Changing these values could impact your deployment. Ensure you understand the impacts before making changes.

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.**



LogRhythm Data Processor Local Confi...

Data Processor

Specify the Data Processor configuration settings..

Platform Manager Connection Settings

Server: 192.168.45.20

Database: LogRhythmEMDB

□ Login with Windows account

User ID: LogRhythmLM

Password: ************

□ Encrypt all communications

Data Processor High Availability (HA only) Folders

For High Availability (HA) deployments, the Configuration and State paths can be modified from their default locations.

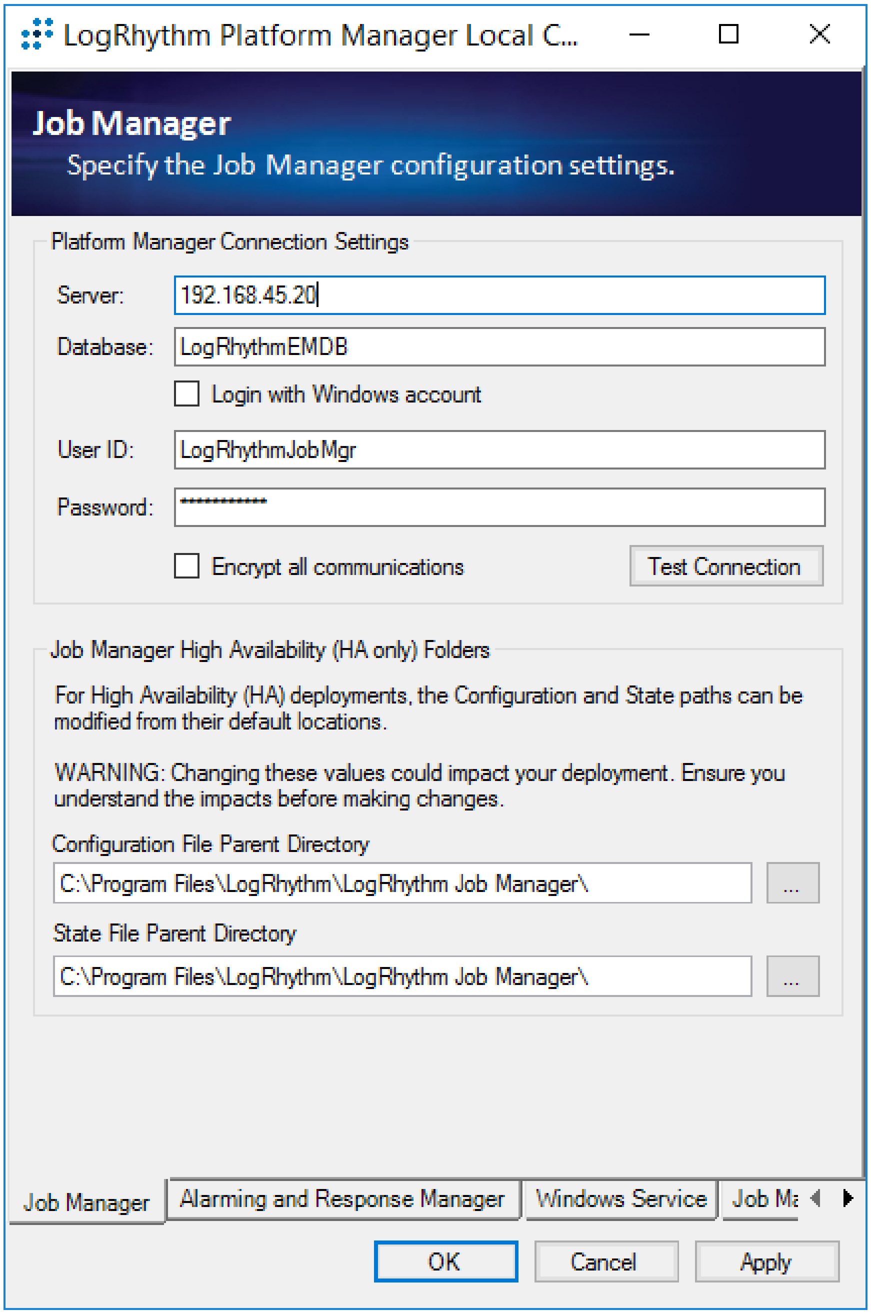
WARNING: Changing these values could impact your deployment. Ensure you understand the impacts before making changes.

Configuration File Parent Directory: C:\Program Files\LogRhythm\LogRhythm Mediator Server\

State File Parent Directory: C:\Program Files\LogRhythm\LogRhythm Mediator Server\

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.**



LogRhythm Platform Manager Local C...

Job Manager

Specify the Job Manager configuration settings.

Platform Manager Connection Settings

Server: 192.168.45.20

Database: LogRhythmEMDB

□ Login with Windows account

User ID: LogRhythmJobMgr

Password: ************

□ Encrypt all communications

Job Manager High Availability (HA only) Folders

For High Availability (HA) deployments, the Configuration and State paths can be modified from their default locations.

WARNING: Changing these values could impact your deployment. Ensure you understand the impacts before making changes.

Configuration File Parent Directory: C:\Program Files\LogRhythm\LogRhythm Job Manager\

State File Parent Directory: C:\Program Files\LogRhythm\LogRhythm Job Manager\

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

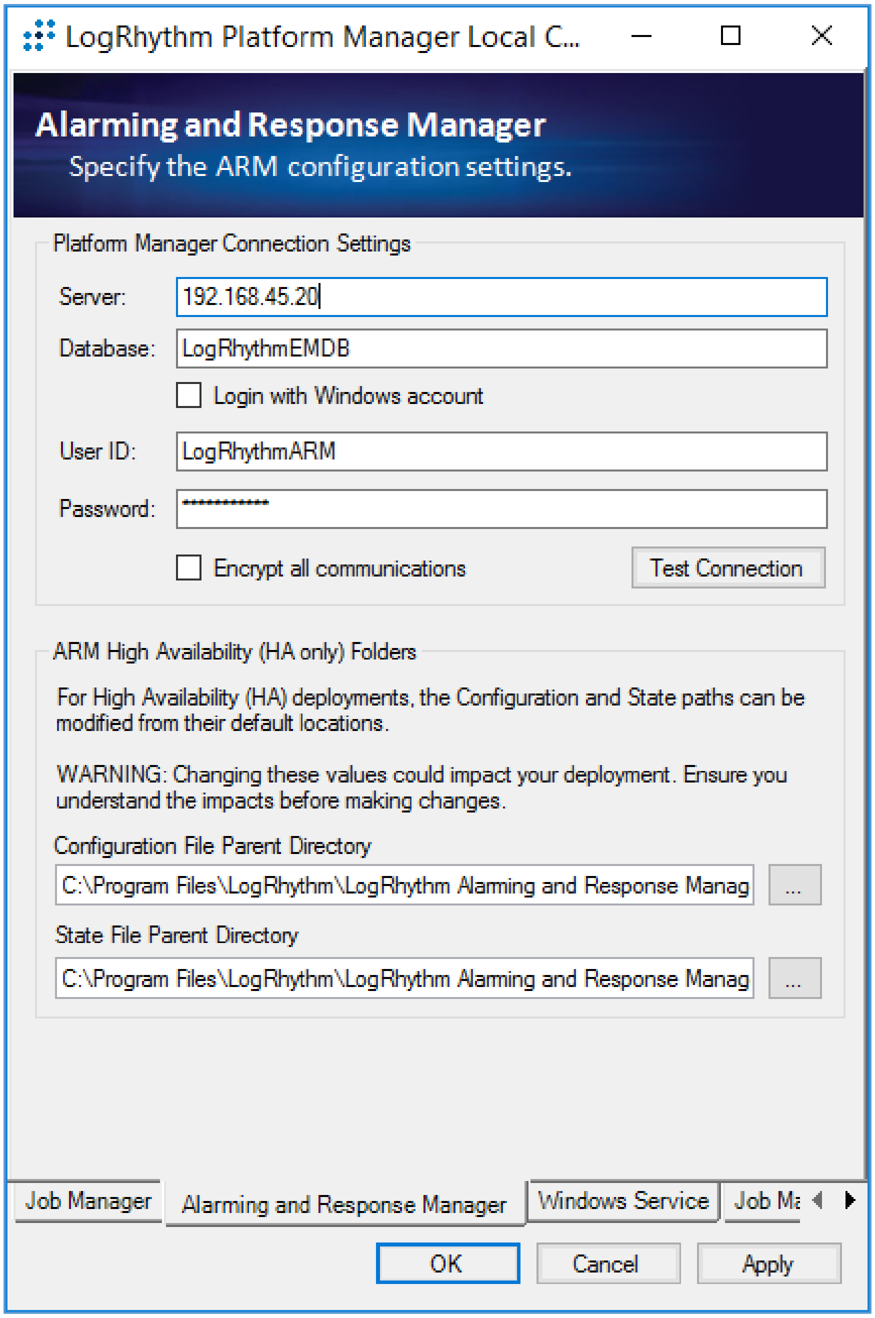
8. In the **Alarming and Response Manager** window, provide the following information, and leave the remaining fields as their default values:

    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.**



Alarming and Response Manager

Specify the ARM configuration settings.

Platform Manager Connection Settings

Server: 192.168.45.20

Database: LogRhythmEMDB

□ Login with Windows account

User ID: LogRhythmARM

Password: ************

□ Encrypt all communications

ARM High Availability (HA only) Folders

For High Availability (HA) deployments, the Configuration and State paths can be modified from their default locations.

WARNING: Changing these values could impact your deployment. Ensure you understand the impacts before making changes.

Configuration File Parent Directory: C:\Program Files\LogRhythm\LogRhythm Alarming and Response Manag

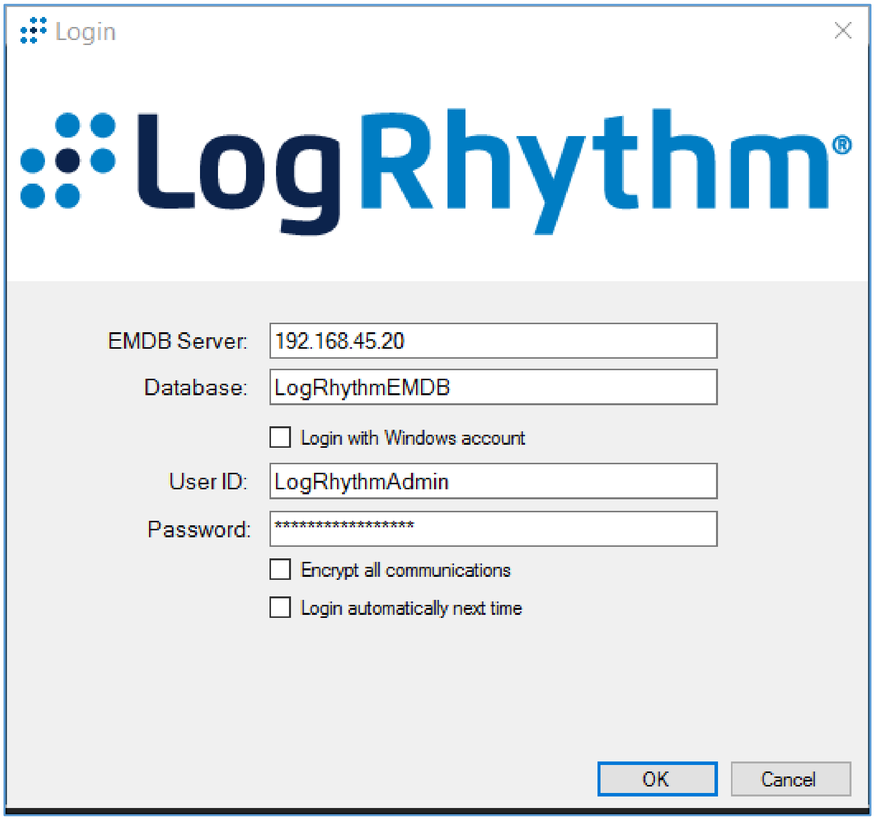
State File Parent Directory: C:\Program Files\LogRhythm\LogRhythm Alarming and Response Manag

1073 **<u>Configure LogRhythm Console</u>**

1074 1. Open File Explorer and navigate to ***C:\Program Files\LogRhythm.***

1075 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**.



EMDB Server: 192.168.45.20

Database: LogRhythmEMDB

☐ Login with Windows account

User ID: LogRhythmAdmin

Password: *******************

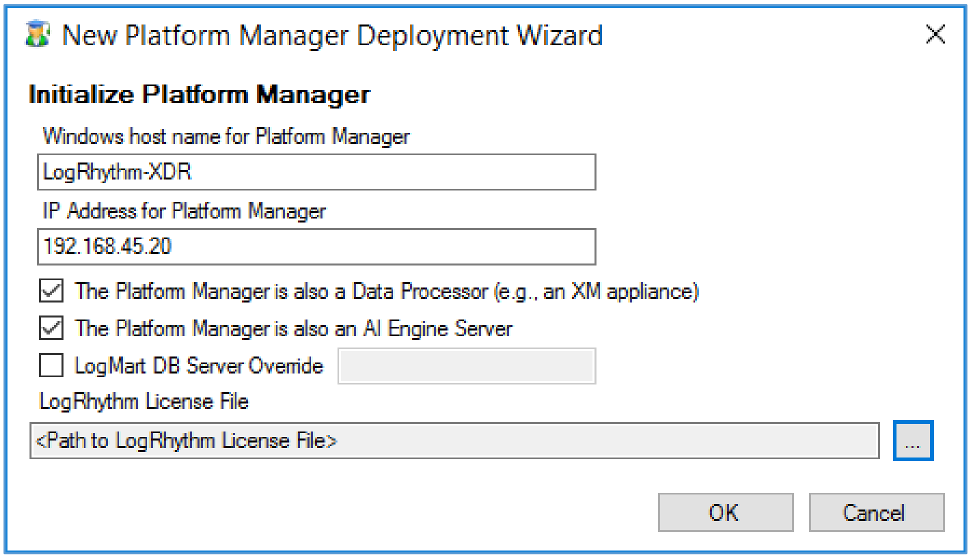
☐ Encrypt all communications

☐ Login automatically next time

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.



New Platform Manager Deployment Wizard

Initialize Platform Manager

Windows host name for Platform Manager: LogRhythm-XDR

IP Address for Platform Manager: 192.168.45.20

☑ The Platform Manager is also a Data Processor (e.g., an XM appliance)

☑ The Platform Manager is also an AI Engine Server

☐ LogMart DB Server Override

LogRhythm License File: <Path to LogRhythm License File>

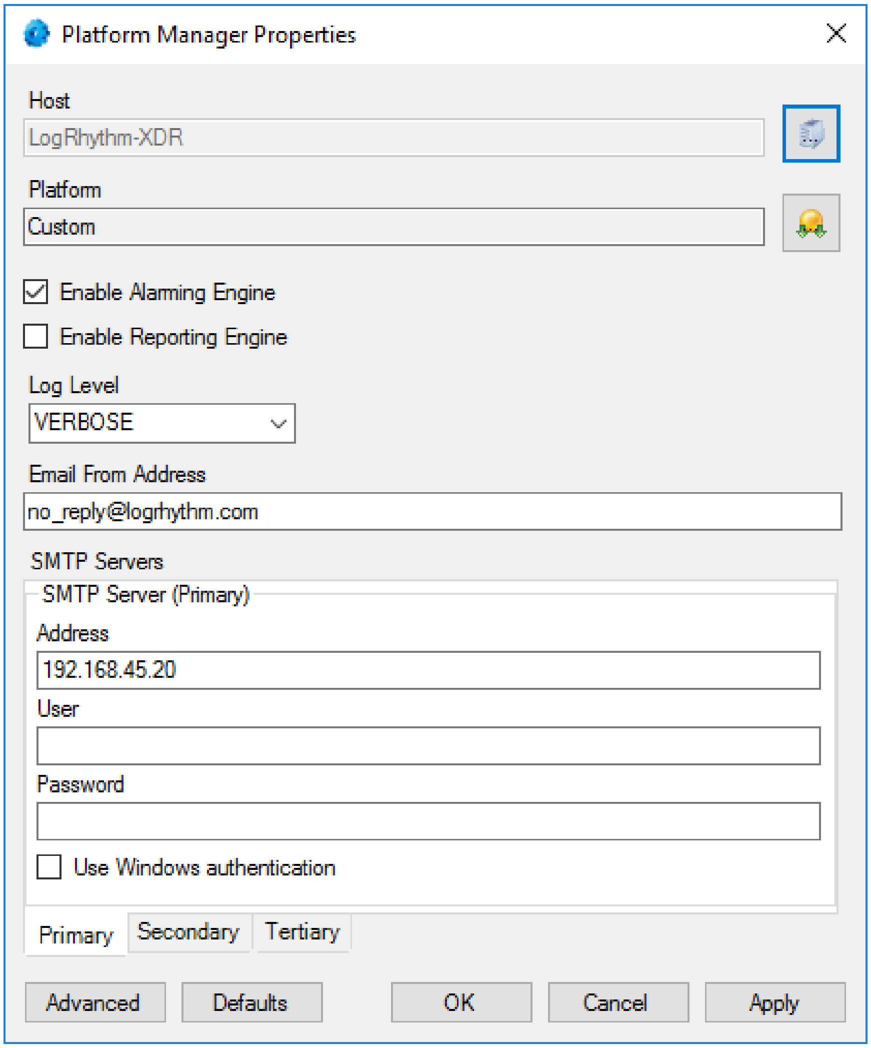
8. The New Knowledge Base Deployment Wizard window displays and shows the import progress status. Once LogRhythm has successfully imported the file, a message window will appear stating more configurations need to be made for optimum performance. Click **OK** to open the **Platform Manager Properties**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



Platform Manager Properties

Host: LogRhythm-XDR

Platform: Custom

☑ Enable Alarming Engine

☐ Enable Reporting Engine

Log Level: VERBOSE

Email From Address: no_reply@logrhythm.com

SMTP Servers

SMTP Server (Primary)

Address: 192.168.45.20

User

Password

☐ Use Windows authentication

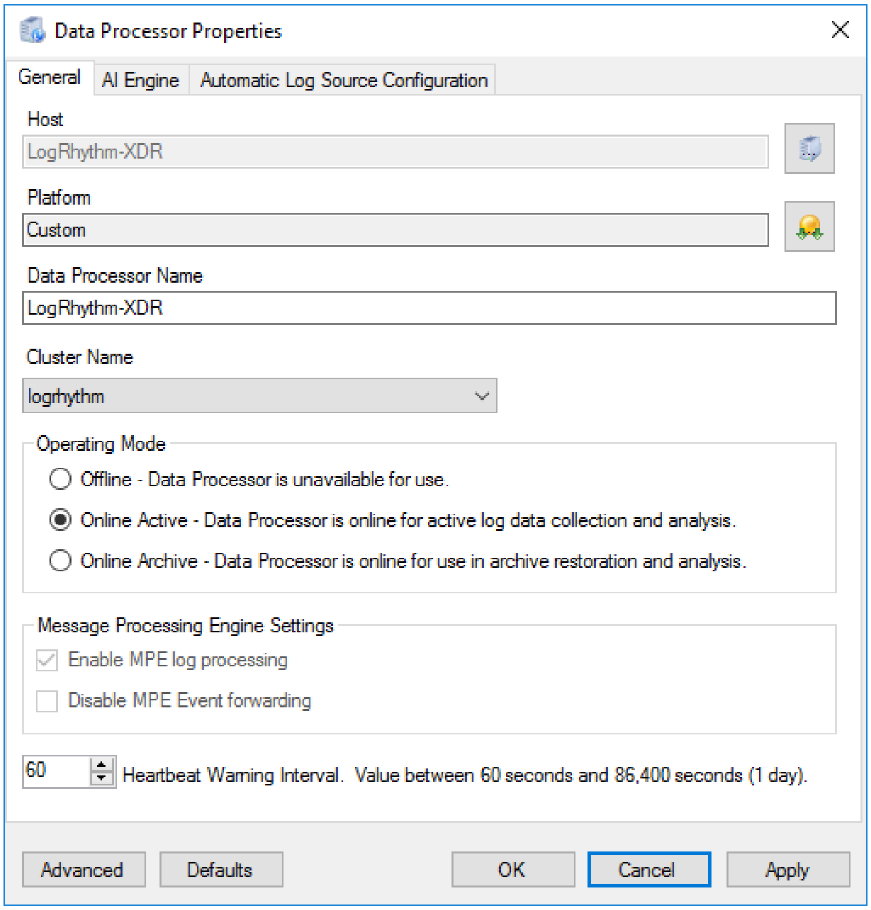
11. After the Platform Manager Properties window closes, a message window displays for configuring the Data Processor. Click **OK** to open the **Data Processor Properties** window.

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**.**



Host: LogRhythm-XDR

Platform: Custom

Data Processor Name: LogRhythm-XDR

Cluster Name: logrhythm

Operating Mode

○ Offline - Data Processor is unavailable for use.

● Online Active - Data Processor is online for active log data collection and analysis.

○ Online Archive - Data Processor is online for use in archive restoration and analysis.

Message Processing Engine Settings

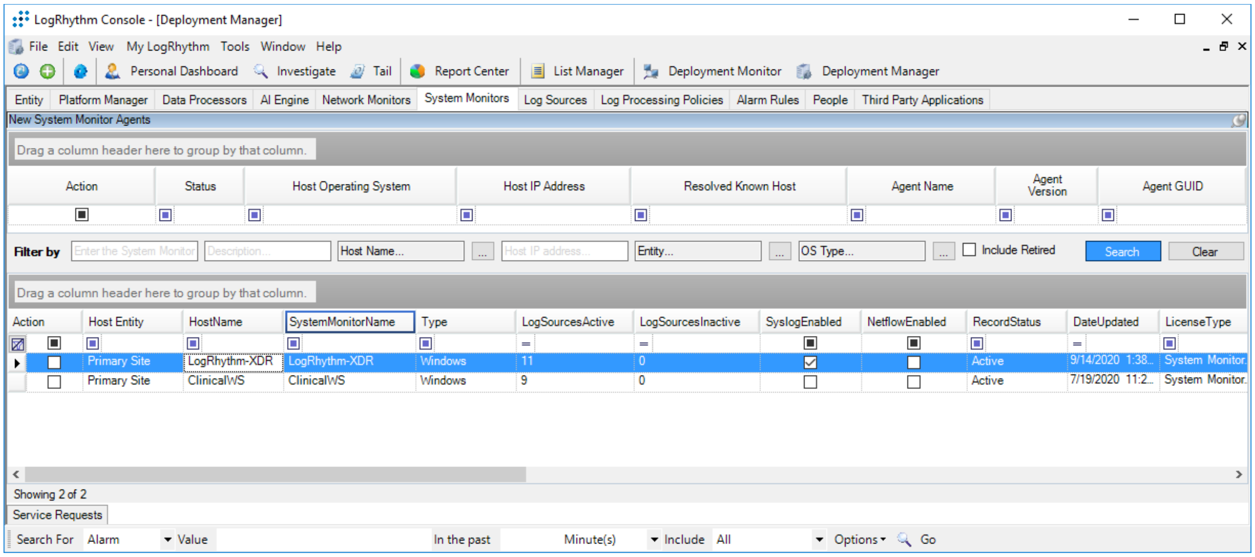
☑ Enable MPE log processing

☐ Disable MPE Event forwarding

60 Heartbeat Warning Interval. Value between 60 seconds and 86,400 seconds (1 day).

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.**


LogRhythm Console - [Deployment Manager]
File Edit View My LogRhythm Tools Window Help
Personal Dashboard Investigate Tail Report Center List Manager Deployment Monitor Deployment Manager
Entity Platform Manager Data Processors AI Engine Network Monitors System Monitors Log Sources Log Processing Policies Alarm Rules People Third Party Applications
New System Monitor Agents
Drag a column header here to group by that column.
Action Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent Version Agent GUID
Filter by Enter the System Monitor Description... Host Name... Host IP address... Entity... OS Type... Include Retired Search Clear
Drag a column header here to group by that column.

Action	Host Entity	HostName	SystemMonitorName	Type	LogSourcesActive	LogSourcesInactive	SyslogEnabled	NetflowEnabled	RecordStatus	DateUpdated	LicenseType
□	Primary Site	LogRhythm-XDR	LogRhythm-XDR	Windows	11	0	☑	□	Active	9/14/2020 1:38...	System Monitor.
□	Primary Site	ClinicalWS	ClinicalWS	Windows	9	0	□	□	Active	7/19/2020 11:2...	System Monitor.

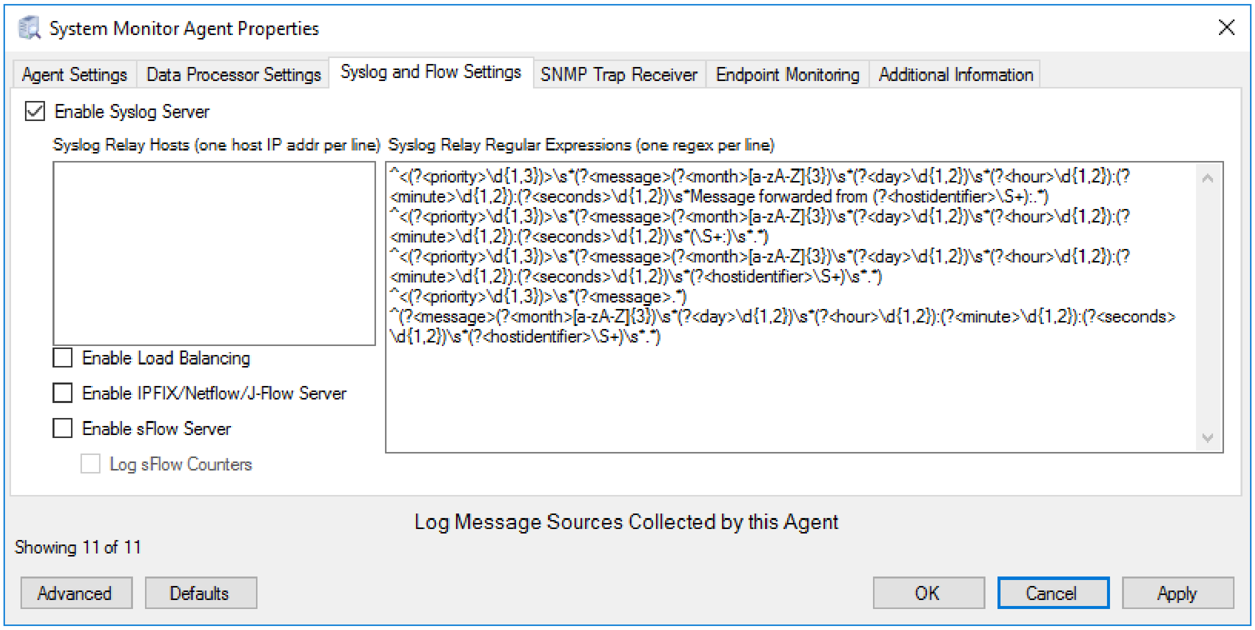
Showing 2 of 2

Service Requests
Search For Alarm Value In the past Minute(s) Include All Options Go

1111 4. In the **System Monitor Agent Properties** window, navigate to **Syslog and Flow Settings**.

1112 5. Click the checkbox beside **Enable Syslog Server**.

1113 6. Click **OK** to close the System Monitor Agent Properties window.


System Monitor Agent Properties
Agent Settings Data Processor Settings Syslog and Flow Settings SNMP Trap Receiver Endpoint Monitoring Additional Information

☑ Enable Syslog Server

Syslog Relay Hosts (one host IP addr per line)

Syslog Relay Regular Expressions (one regex per line)

```
^<(?<priority>\d{1,3})>\s*(?<message>(?<month>[a-zA-Z]{3})\s*(?<day>\d{1,2})\s*(?<hour>\d{1,2}):(?<minute>\d{1,2}):(?<seconds>\d{1,2})\s*Message forwarded from (?<hostidentifier>\S+):.*)
^<(?<priority>\d{1,3})>\s*(?<message>(?<month>[a-zA-Z]{3})\s*(?<day>\d{1,2})\s*(?<hour>\d{1,2}):(?<minute>\d{1,2}):(?<seconds>\d{1,2})\s*(\S+:)\s*.*)
^<(?<priority>\d{1,3})>\s*(?<message>(?<month>[a-zA-Z]{3})\s*(?<day>\d{1,2})\s*(?<hour>\d{1,2}):(?<minute>\d{1,2}):(?<seconds>\d{1,2})\s*(?<hostidentifier>\S+)\s*.*)
^<(?<priority>\d{1,3})>\s*(?<message>.*)
^(?<message>(?<month>[a-zA-Z]{3})\s*(?<day>\d{1,2})\s*(?<hour>\d{1,2}):(?<minute>\d{1,2}):(?<seconds>\d{1,2})\s*(?<hostidentifier>\S+)\s*.*)
```

□ Enable Load Balancing

□ Enable IPFIX/Netflow/J-Flow Server

□ Enable sFlow Server

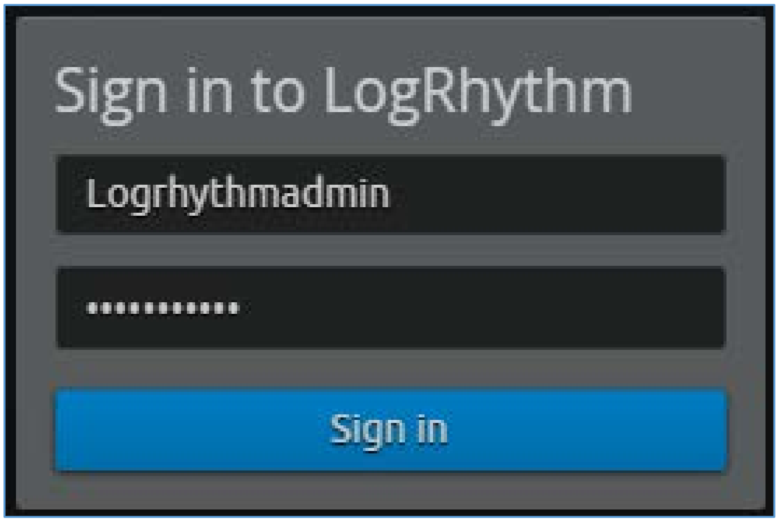
□ Log sFlow Counters

Log Message Sources Collected by this Agent
Showing 11 of 11
Advanced Defaults OK Cancel Apply

1114 Use the LogRhythm Web Console

1115 1. Open a web browser and navigate to https://localhost:8443.

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



Sign in to LogRhythm

Logrhythmadmin

••••••••••••

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 vCPU

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.

Create a New Firewall Rule

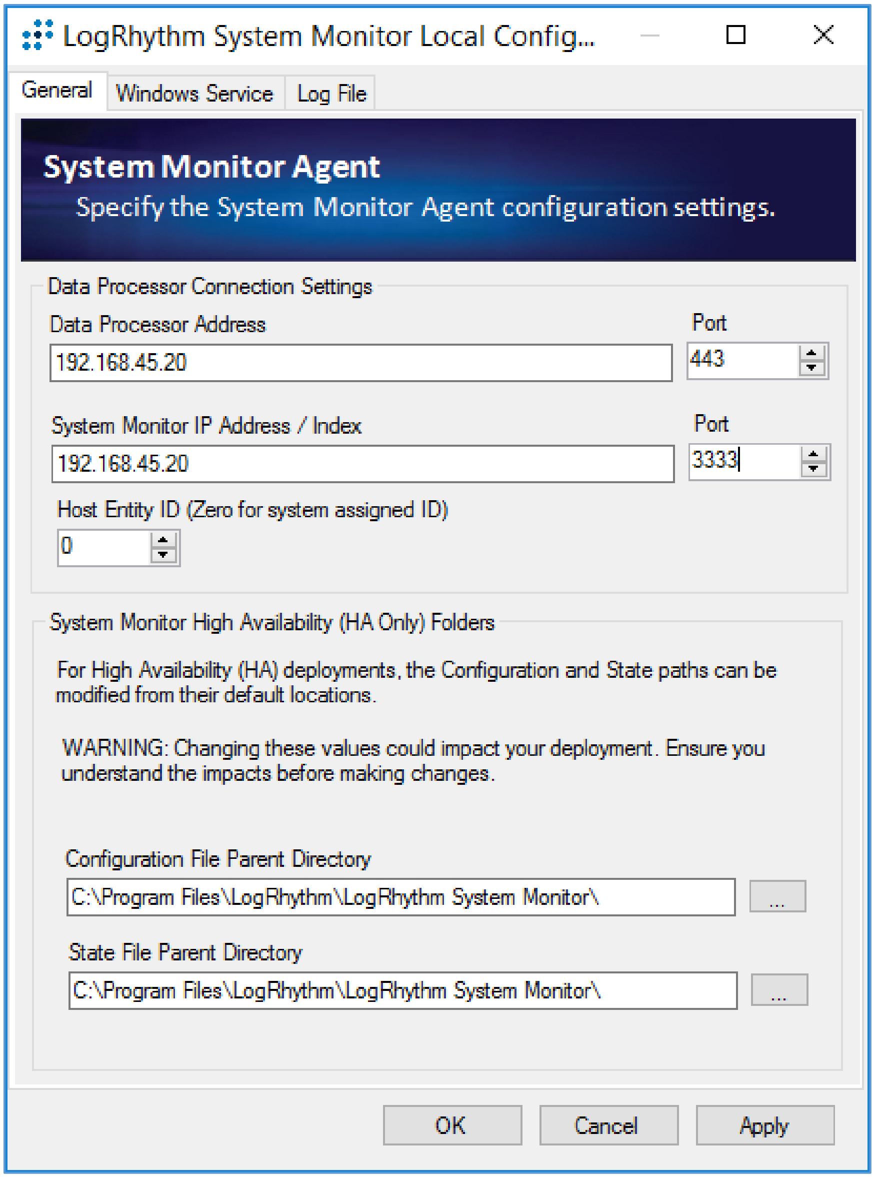
NetMon communicates over TCP 443. The lab environment was configured to allow network sessions connecting to the LogRhythm agent.

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.**



LogRhythm System Monitor Local Config...

System Monitor Agent

Specify the System Monitor Agent configuration settings.

Data Processor Connection Settings

Data Processor Address: 192.168.45.20 Port: 443

System Monitor IP Address / Index: 192.168.45.20 Port: 3333

Host Entity ID (Zero for system assigned ID): 0

System Monitor High Availability (HA Only) Folders

For High Availability (HA) deployments, the Configuration and State paths can be modified from their default locations.

WARNING: Changing these values could impact your deployment. Ensure you understand the impacts before making changes.

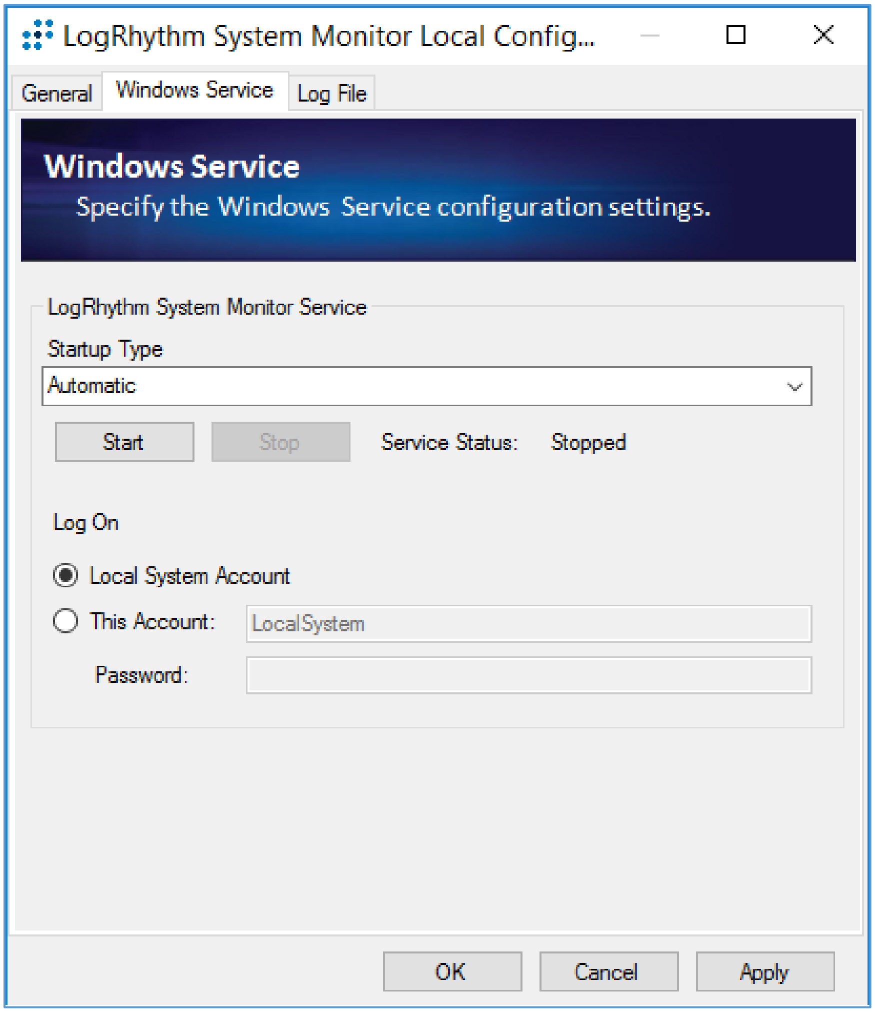
Configuration File Parent Directory: C:\Program Files\LogRhythm\LogRhythm System Monitor\

State File Parent Directory: C:\Program Files\LogRhythm\LogRhythm System Monitor\

1163 3. Click the **Windows Service** tab.

1164 4. Change the **Service Type** to **Automatic**.

1165 5. Click **Apply**.



LogRhythm System Monitor Local Config...

Windows Service

Specify the Windows Service configuration settings.

LogRhythm System Monitor Service

Startup Type: Automatic

Service Status: Stopped

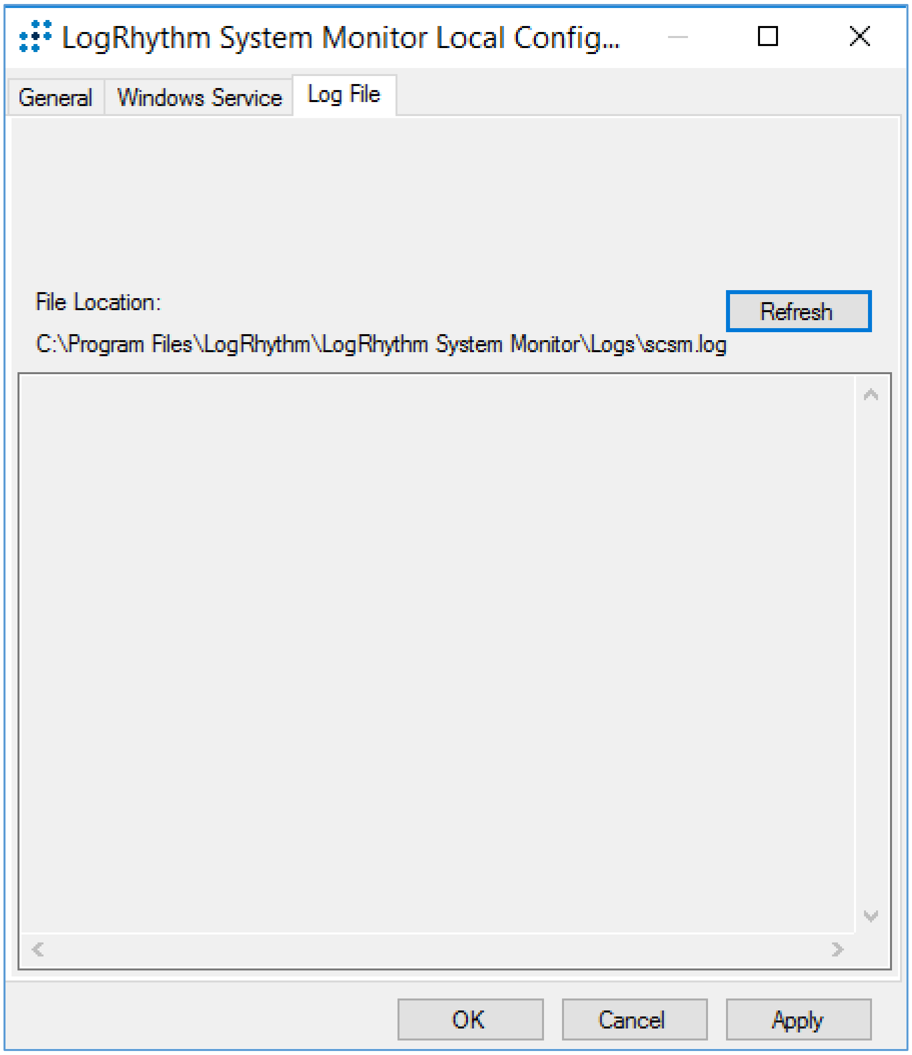
Log On

● Local System Account

○ This Account: LocalSystem

Password:

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



File Location:
C:\Program Files\LogRhythm\LogRhythm System Monitor\Logs\scsm.log

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

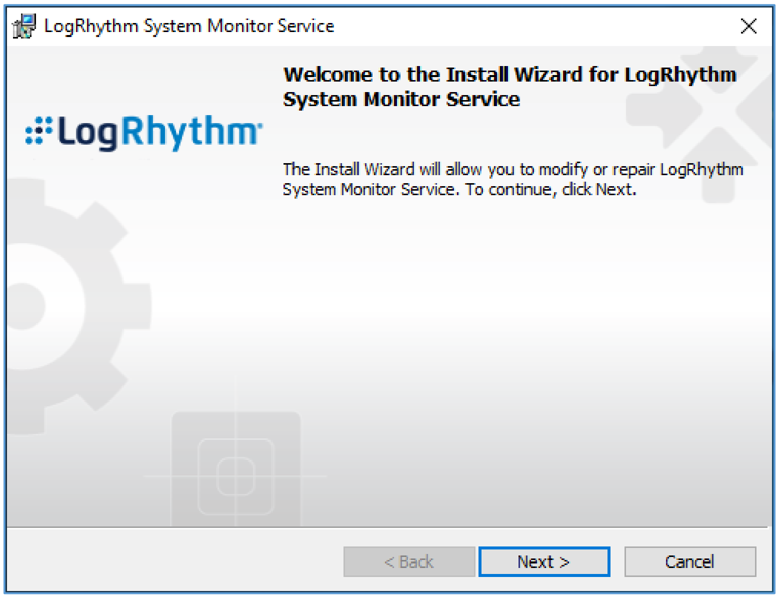
This section describes installation of the system monitor agent.

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…**

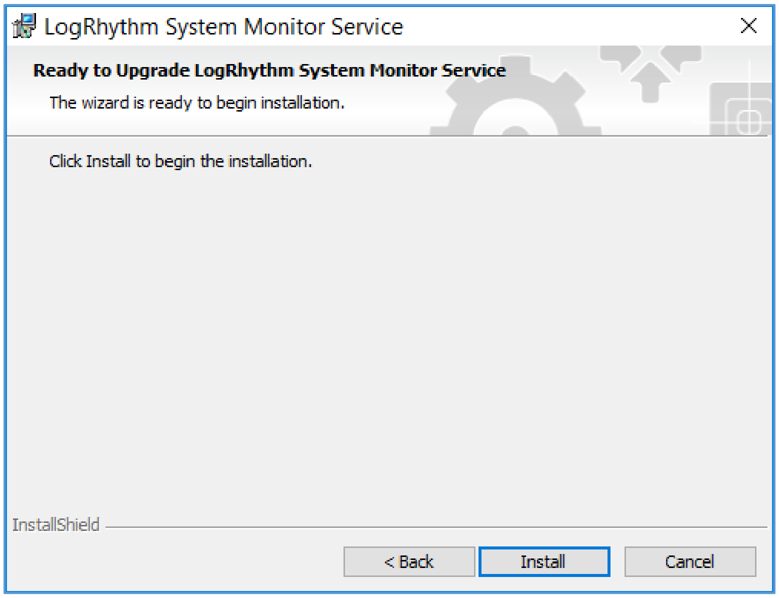


LogRhythm System Monitor Service

Welcome to the Install Wizard for LogRhythm System Monitor Service

The Install Wizard will allow you to modify or repair LogRhythm System Monitor Service. To continue, click Next.

5. On the ready to begin installation page, click **Install**.



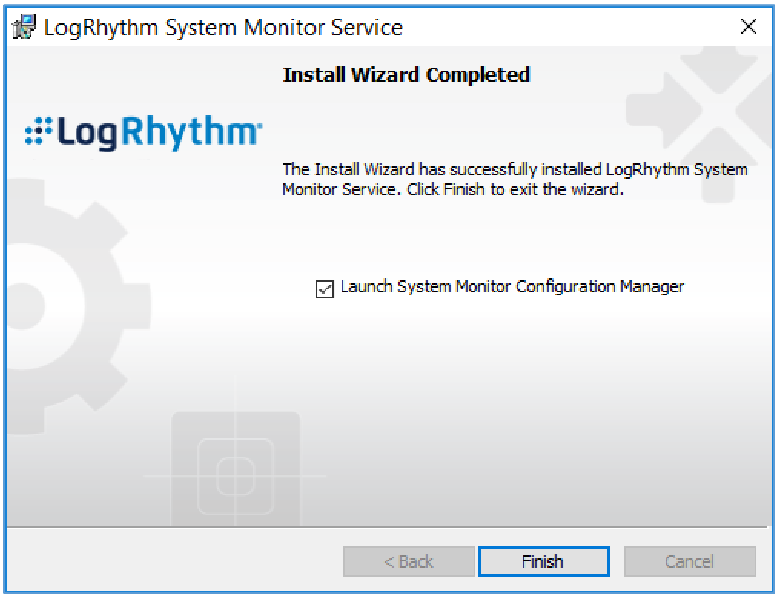
LogRhythm System Monitor Service

Ready to Upgrade LogRhythm System Monitor Service

The wizard is ready to begin installation.

Click Install to begin the installation.

6. Click **Finish.**



LogRhythm System Monitor Service

Install Wizard Completed

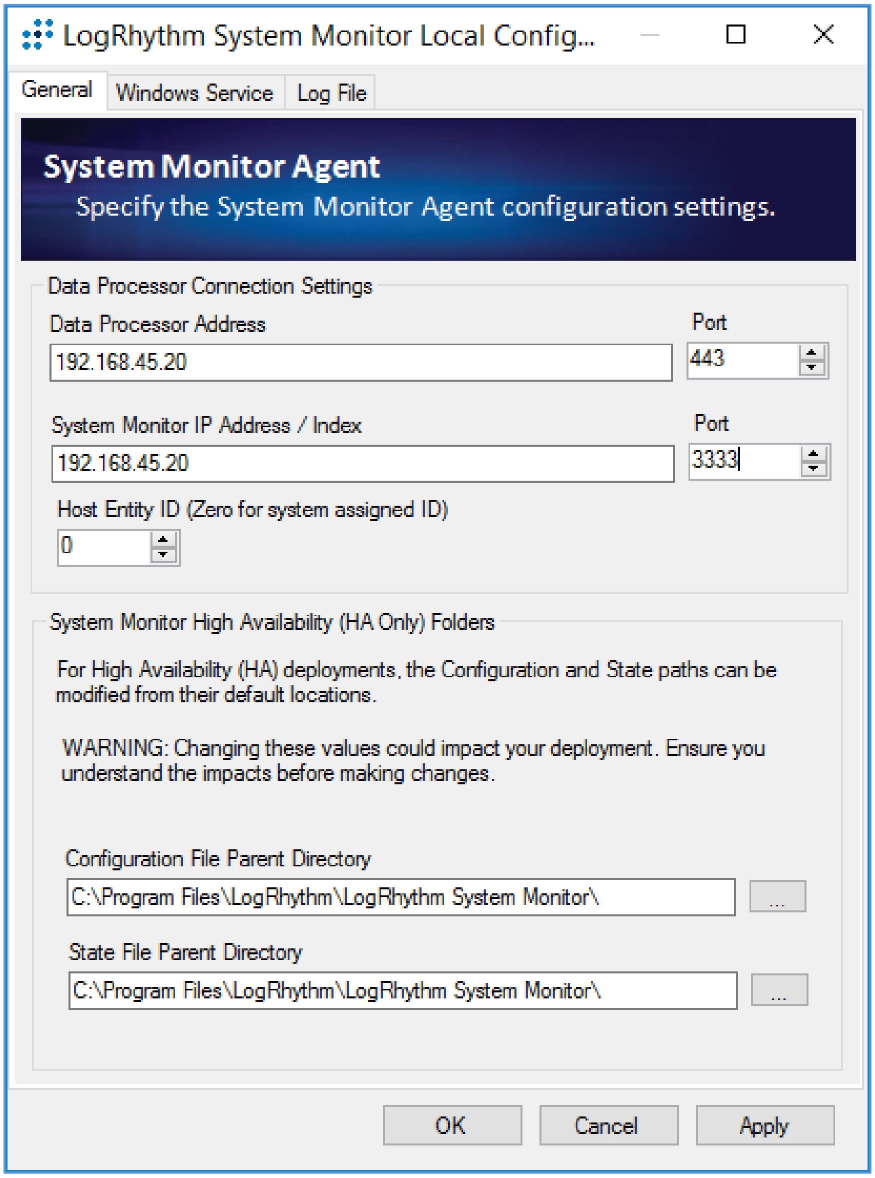
The Install Wizard has successfully installed LogRhythm System Monitor Service. Click Finish to exit the wizard.

☑ Launch System Monitor Configuration Manager

<u>System Monitor Agent Configuration</u>

1. After exiting the **LogRhythm System Monitor Service Install Wizard,** a LogRhythm System Monitor Local Configuration window displays. Under the **General** tab, provide the following information:

   a. **Data Process Address:** 192.168.45.20
   b. **System Monitor IP Address/Index:** 192.168.45.20
2. Click **Apply**.



System Monitor Agent
Specify the System Monitor Agent configuration settings.

Data Processor Connection Settings

Data Processor Address: 192.168.45.20 Port: 443

System Monitor IP Address / Index: 192.168.45.20 Port: 3333

Host Entity ID (Zero for system assigned ID): 0

System Monitor High Availability (HA Only) Folders

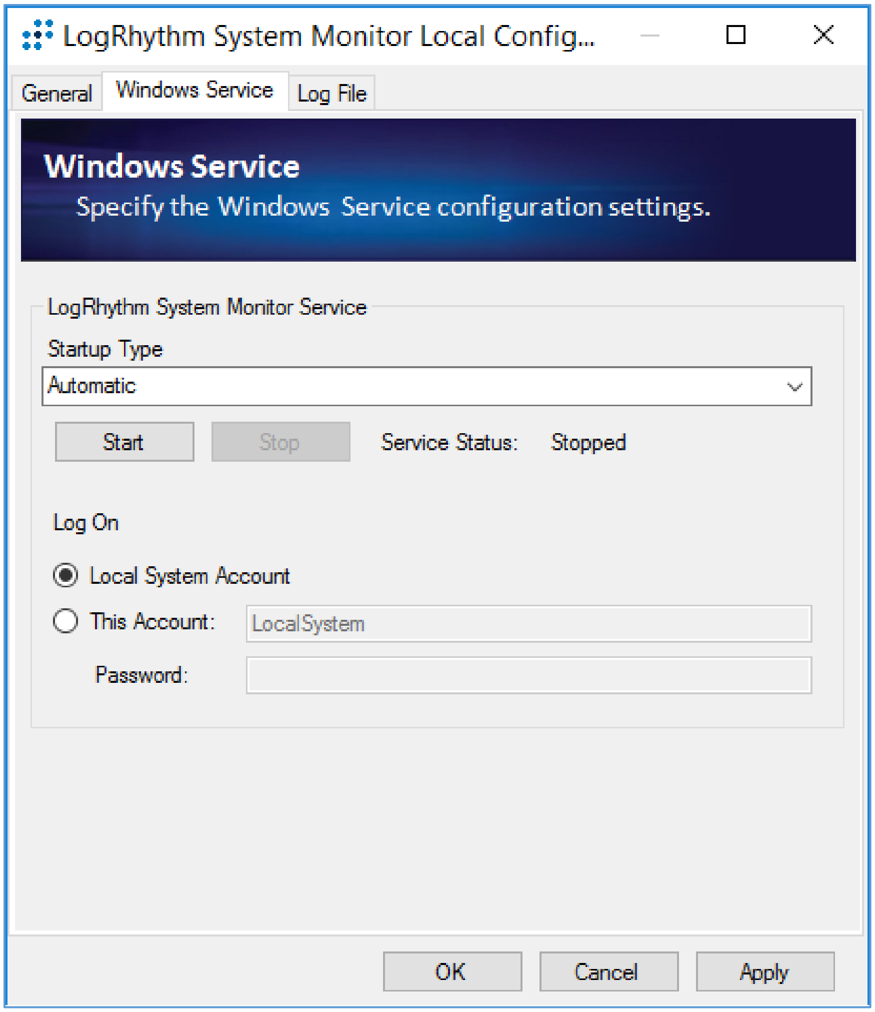
For High Availability (HA) deployments, the Configuration and State paths can be modified from their default locations.

WARNING: Changing these values could impact your deployment. Ensure you understand the impacts before making changes.

Configuration File Parent Directory: C:\Program Files\LogRhythm\LogRhythm System Monitor\

State File Parent Directory: C:\Program Files\LogRhythm\LogRhythm System Monitor\

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



LogRhythm System Monitor Local Config...

Windows Service

Specify the Windows Service configuration settings.

LogRhythm System Monitor Service

Startup Type: Automatic

Service Status: Stopped

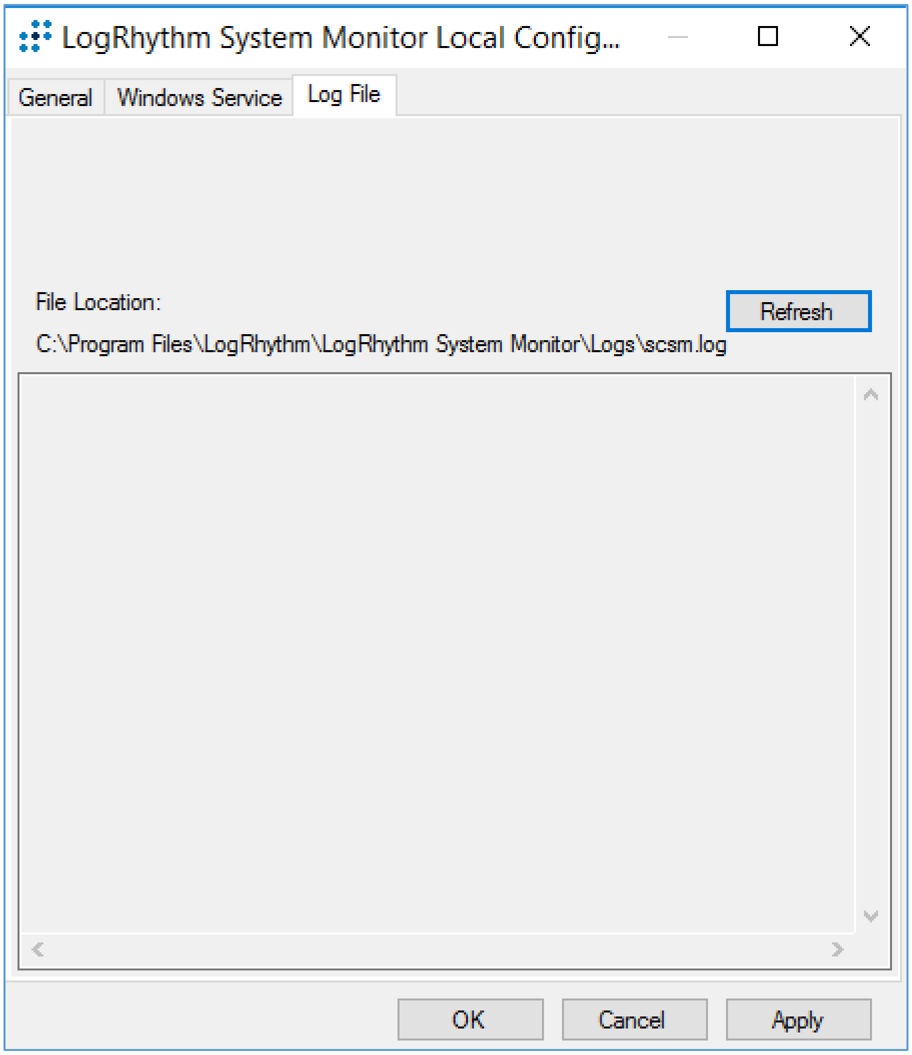
Log On

● Local System Account

○ This Account: LocalSystem

Password:

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



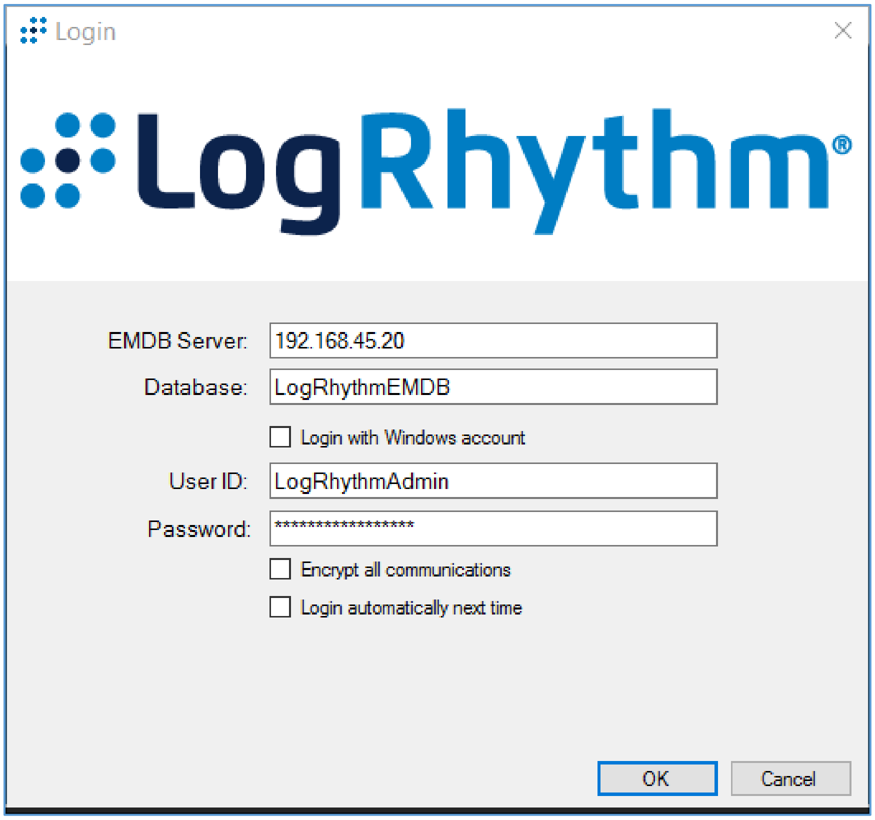
File Location:

C:\Program Files\LogRhythm\LogRhythm System Monitor\Logs\scsm.log

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:** **********



EMDB Server: 192.168.45.20

Database: LogRhythmEMDB

□ Login with Windows account

User ID: LogRhythmAdmin

Password: *****************

□ Encrypt all communications

□ Login automatically next time

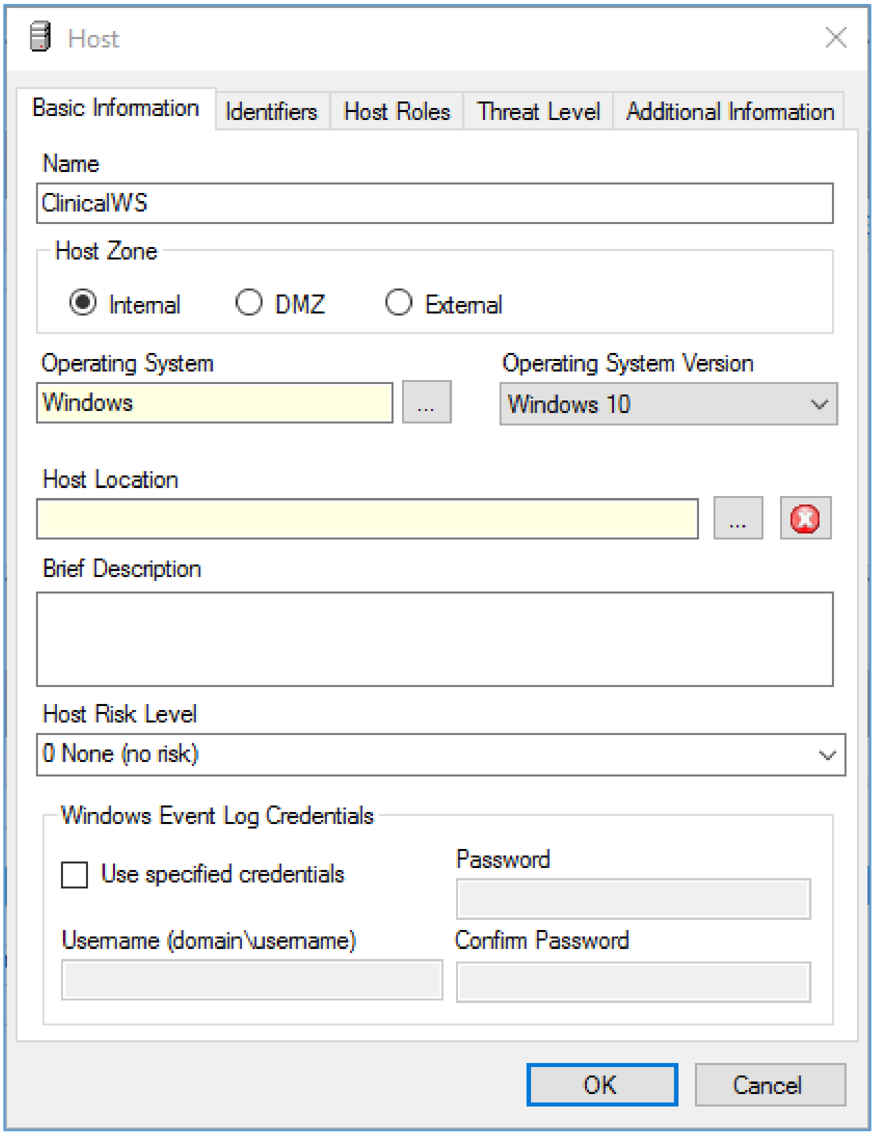
2. Navigate to the **Deployment Manager** in the menu ribbon.

3. Under the **Entity** tab on the **Deployment Manager** menu ribbon.

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



Name: ClinicalWS

Host Zone: ● Internal ○ DMZ ○ External

Operating System: Windows

Operating System Version: Windows 10

Host Location:

Brief Description:

Host Risk Level: 0 None (no risk)

Windows Event Log Credentials

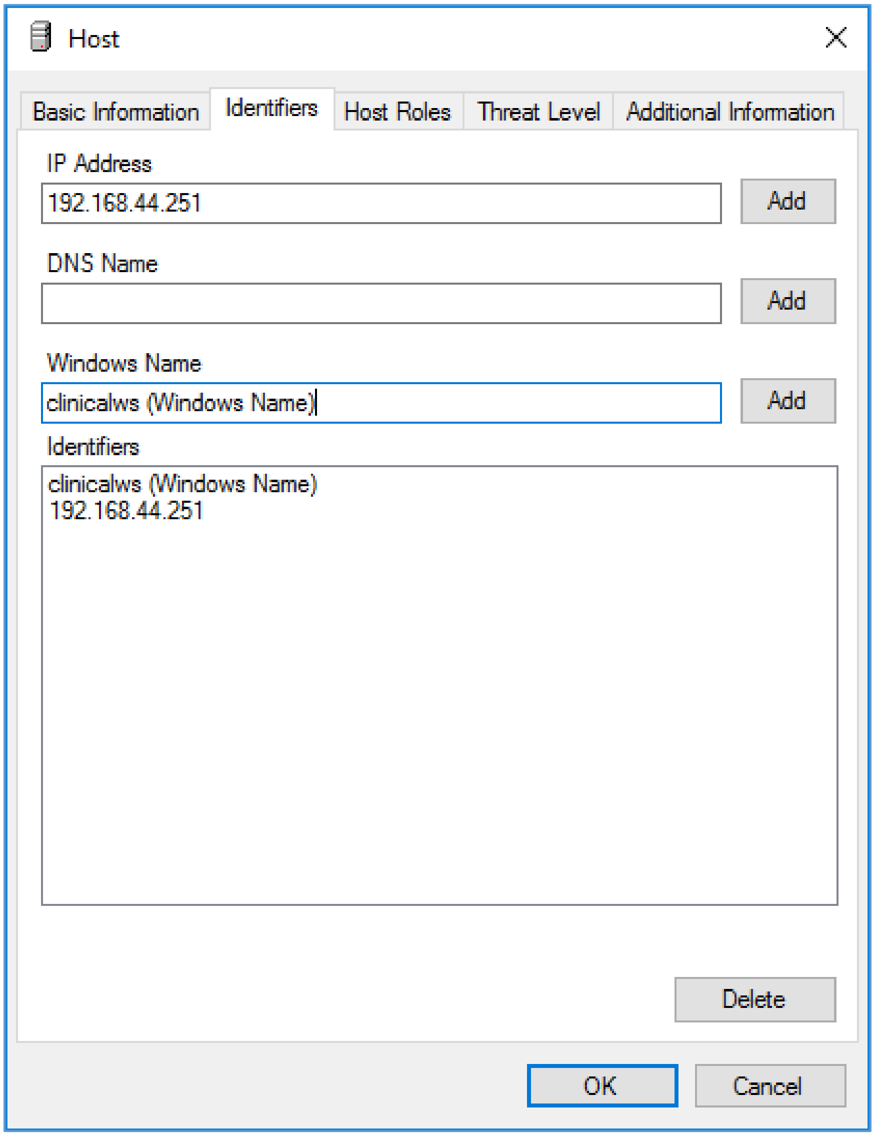
□ Use specified credentials

Password:

Username (domain\username):

Confirm Password:

5. Navigate to the **Identifiers** tab, provide the following information in the appropriate fields, and click **Add**.
    a. **IP Address:** 192.168.44.251
    b. **Windows Name:** clinicalws (Windows Name)



IP Address

192.168.44.251

DNS Name

Windows Name

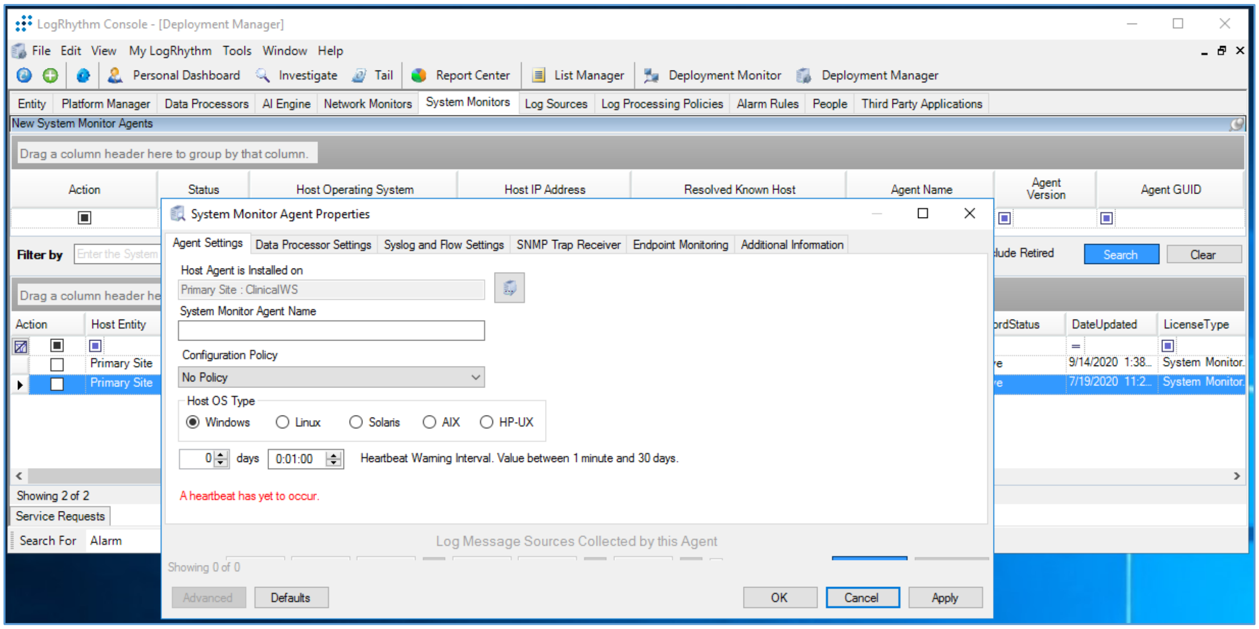
clinicalws (Windows Name)

Identifiers

clinicalws (Windows Name)
192.168.44.251

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**.


LogRhythm Console - [Deployment Manager]
File Edit View My LogRhythm Tools Window Help
Personal Dashboard Investigate Tail Report Center List Manager Deployment Monitor Deployment Manager
Entity Platform Manager Data Processors AI Engine Network Monitors System Monitors Log Sources Log Processing Policies Alarm Rules People Third Party Applications
New System Monitor Agents
Drag a column header here to group by that column.
Action Status Host Operating System Host IP Address Resolved Known Host Agent Name Agent Version Agent GUID
Filter by
Enter the System
Include Retired
Search
Clear
Action Host Entity
ordStatus DateUpdated LicenseType
Showing 2 of 2
Service Requests
Search For Alarm
System Monitor Agent Properties
Agent Settings Data Processor Settings Syslog and Flow Settings SNMP Trap Receiver Endpoint Monitoring Additional Information
Advanced Defaults OK Cancel Apply

Host Entity	DateUpdated	LicenseType
Primary Site	9/14/2020 1:38...	System Monitor...
Primary Site	7/19/2020 11:2...	System Monitor...

Host Agent is Installed on: Primary Site : ClinicalWS

System Monitor Agent Name:

Configuration Policy: No Policy

Host OS Type: ● Windows ○ Linux ○ Solaris ○ AIX ○ HP-UX

0 days 0:01:00 Heartbeat Warning Interval. Value between 1 minute and 30 days.

A heartbeat has yet to occur.

Log Message Sources Collected by this Agent

Showing 0 of 0

8. Go to **System Monitors.**

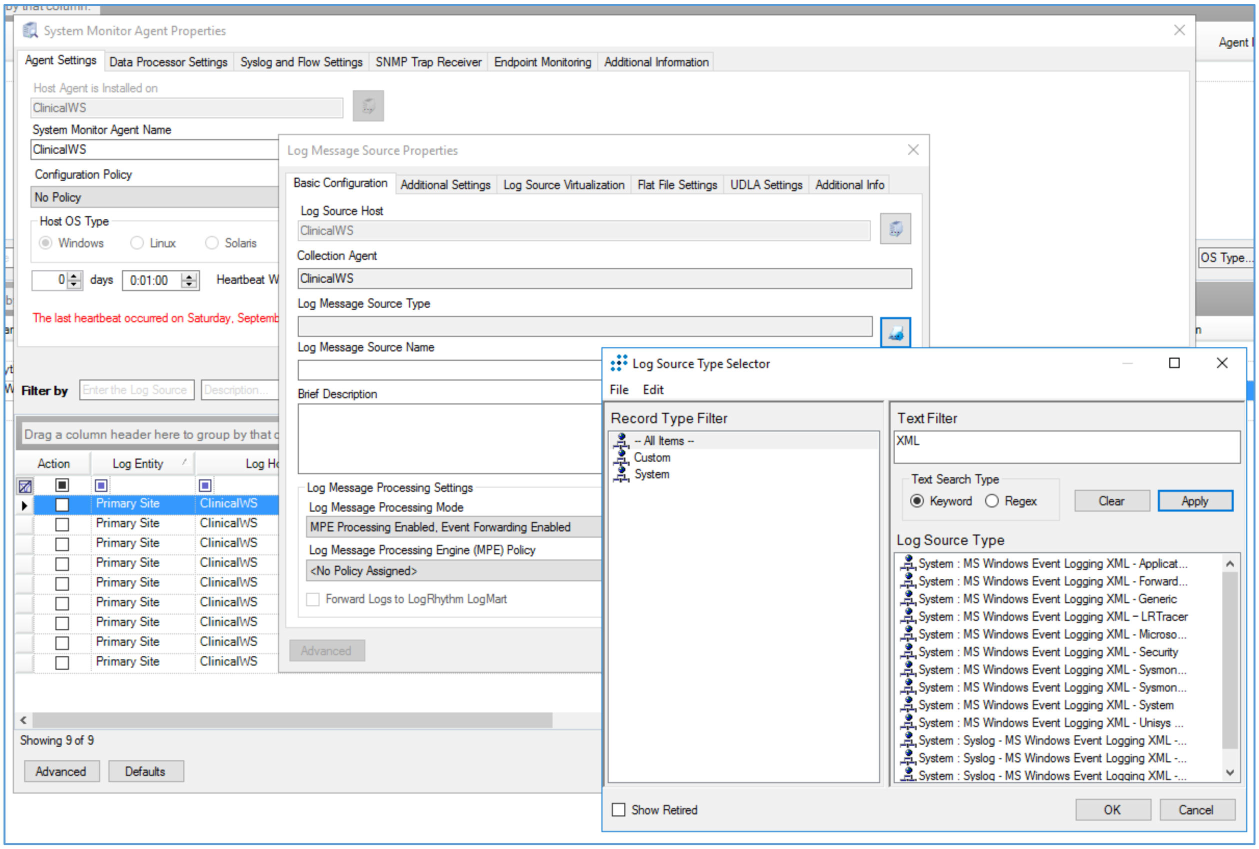
9. Double-click **ClinicalWS.**

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**.



System Monitor Agent Properties

Agent Settings | Data Processor Settings | Syslog and Flow Settings | SNMP Trap Receiver | Endpoint Monitoring | Additional Information

Host Agent is Installed on: ClinicalWS

System Monitor Agent Name: ClinicalWS

Configuration Policy: No Policy

Host OS Type: ● Windows ○ Linux ○ Solaris

0 days 0:01:00 Heartbeat W

The last heartbeat occured on Saturday, Septemb

Filter by: Enter the Log Source | Description...

Drag a column header here to group by that c

	Action	Log Entity	Log Ho
▶	□	Primary Site	ClinicalWS
	□	Primary Site	ClinicalWS
	□	Primary Site	ClinicalWS
	□	Primary Site	ClinicalWS
	□	Primary Site	ClinicalWS
	□	Primary Site	ClinicalWS
	□	Primary Site	ClinicalWS
	□	Primary Site	ClinicalWS
	□	Primary Site	ClinicalWS

Showing 9 of 9

Log Message Source Properties

Basic Configuration | Additional Settings | Log Source Virtualization | Flat File Settings | UDLA Settings | Additional Info

Log Source Host: ClinicalWS

Collection Agent: ClinicalWS

Log Message Source Type:

Log Message Source Name:

Brief Description:

Log Message Processing Settings

Log Message Processing Mode: MPE Processing Enabled, Event Forwarding Enabled

Log Message Processing Engine (MPE) Policy: <No Policy Assigned>

□ Forward Logs to LogRhythm LogMart

Log Source Type Selector

Record Type Filter

- -- All Items --
- Custom
- System

Text Filter: XML

Text Search Type: ● Keyword ○ Regex

Log Source Type

- System : MS Windows Event Logging XML - Applicat...
- System : MS Windows Event Logging XML - Forward...
- System : MS Windows Event Logging XML - Generic
- System : MS Windows Event Logging XML – LRTracer
- System : MS Windows Event Logging XML - Microso...
- System : MS Windows Event Logging XML - Security
- System : MS Windows Event Logging XML - Sysmon...
- System : MS Windows Event Logging XML - Sysmon...
- System : MS Windows Event Logging XML - System
- System : MS Windows Event Logging XML - Unisys ...
- System : Syslog - MS Windows Event Logging XML -...
- System : Syslog - MS Windows Event Logging XML -...
- System : Syslog - MS Windows Event Logging XML -...

□ Show Retired

Appendix A List of Acronyms

AD	Active Directory
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
FMC	Firepower Management Center
FTD	Firepower Threat Defense
GB	Gigabyte
HDO	Healthcare Delivery Organization
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 (SP) 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.