

NIST SPECIAL PUBLICATION 1800-30C

Securing Telehealth Remote Patient Monitoring Ecosystem

**Volume C:
How-To Guides**

Jennifer Cawthra*
Nakia Grayson

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Sue Wang
Ryan Williams
Kangmin Zheng

The MITRE Corporation
McLean, Virginia

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

May 2021

SECOND DRAFT

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



1 **DISCLAIMER**

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

8 National Institute of Standards and Technology Special Publication 1800-30C, Natl. Inst. Stand. Technol.
9 Spec. Publ. 1800-30C, 160 pages, (May 2021), CODEN: NSPUE2

10 **FEEDBACK**

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

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

14 Public comment period: May 6, 2021 through June 7, 2021

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

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

20 National Cybersecurity Center of Excellence
21 National Institute of Standards and Technology
22 100 Bureau Drive
23 Mailstop 2002
24 Gaithersburg, MD 20899
25 Email: nccoe@nist.gov

26 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

42 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

52 **ABSTRACT**

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

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

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

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

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

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

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

78 **KEYWORDS**

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

82 **ACKNOWLEDGMENTS**

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

Name	Organization
Alex Mohseni	Accuhealth
Stephen Samson	Accuhealth
Brian Butler	Cisco

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

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

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

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

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

88

89 **DOCUMENT CONVENTIONS**

90 The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the
 91 publication and from which no deviation is permitted. The terms “should” and “should not” indicate that

92 among several possibilities, one is recommended as particularly suitable without mentioning or
93 excluding others, or that a certain course of action is preferred but not necessarily required, or that (in
94 the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms
95 “may” and “need not” indicate a course of action permissible within the limits of the publication. The
96 terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

97 **CALL FOR PATENT CLAIMS**

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

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

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

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

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

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

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

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

123 **Contents**

124 **1 Introduction 1**

125 1.1 How to Use this Guide..... 1

126 1.2 Build Overview 2

127 1.3 Typographic Conventions..... 3

128 1.4 Logical Architecture Summary 3

129 **2 Product Installation Guides 4**

130 2.1 Telehealth Platform Provider 4

131 2.1.1 Accuhealth 6

132 2.1.2 Vivify Health 10

133 2.2 Security Capabilities 14

134 2.2.1 Risk Assessment Controls 14

135 2.2.2 Identity Management, Authentication, and Access Control 32

136 2.2.3 Security Continuous Monitoring..... 75

137 2.2.4 Data Security..... 142

138 **Appendix A List of Acronyms 159**

139 **Appendix B References 160**

140 **List of Figures**

141 **Figure 1-1 Final Architecture..... 4**

142 **Figure 2-1 RPM Communications Paths..... 6**

143

144 1 Introduction

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

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

152 1.1 How to Use this Guide

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

157 This guide contains three volumes:

- 158 ▪ NIST SP 1800-30A: *Executive Summary*
- 159 ▪ NIST SP 1800-30B: *Approach, Architecture, and Security Characteristics*—what we built and why
- 160 ▪ NIST SP 1800-30C: *How-To Guides*—instructions for building the example solution (**you are here**)

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

162 **Business decision makers, including chief security and technology officers,** will be interested in the
163 *Executive Summary*, NIST SP 1800-30A, which describes the following topics:

- 164 ▪ challenges that enterprises face in securing the remote patient monitoring ecosystem
- 165 ▪ example solution built at the NCCoE
- 166 ▪ benefits of adopting the example solution

167 **Technology or security program managers** who are concerned with how to identify, understand, assess,
168 and mitigate risk will be interested in NIST SP 1800-30B, which describes what we did and why. The
169 following sections will be of particular interest:

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

173 You might share the *Executive Summary*, NIST SP 1800-30A, with your leadership team members to help
174 them understand the importance of adopting standards-based commercially available technologies that
175 can help secure the RPM ecosystem.

176 **IT professionals** who want to implement an approach like this will find this whole practice guide useful.
177 You can use this How-To portion of the guide, NIST SP 1800-30C, to replicate all or parts of the build
178 created in our lab. This How-To portion of the guide provides specific product installation, configuration,
179 and integration instructions for implementing the example solution. We do not recreate the product
180 manufacturers' documentation, which is generally widely available. Rather, we show how we
181 incorporated the products together in our environment to create an example solution.

182 This guide assumes that IT professionals have experience implementing security products within the
183 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
184 not endorse these particular products. Your organization can adopt this solution or one that adheres to
185 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
186 parts of the National Cybersecurity Center of Excellences' (NCCoE's) risk assessment and deployment of
187 a defense-in-depth strategy in a distributed RPM solution. Your organization's security experts should
188 identify the products that will best integrate with your existing tools and IT system infrastructure. We
189 hope that you will seek products that are congruent with applicable standards and best practices.
190 Section 3.6, Technologies, lists the products that we used and maps them to the cybersecurity controls
191 provided by this reference solution.

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

196 Acronyms used in figures are in the List of Acronyms appendix.

197 **1.2 Build Overview**

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

206 1.3 Typographic Conventions

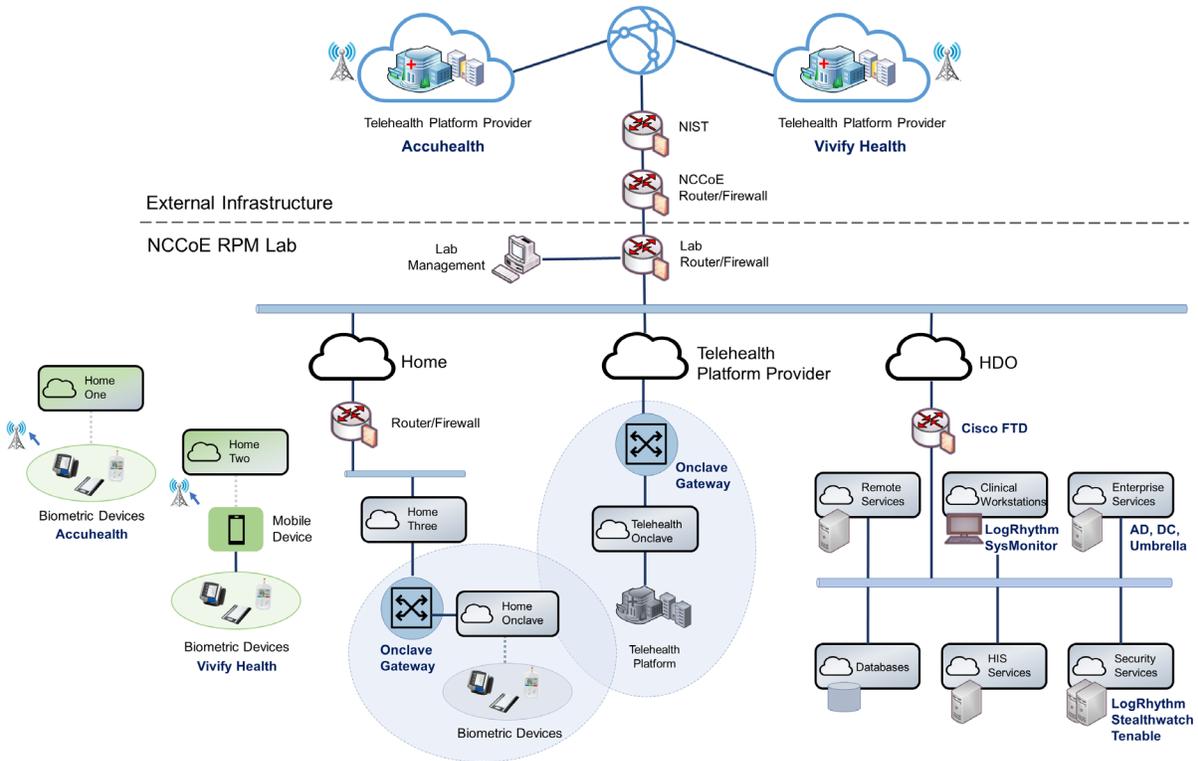
207 The following table presents typographic conventions used in this volume.

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

208 1.4 Logical Architecture Summary

209 Figure 1-1 illustrates the reference network architecture implemented in the NCCoE virtual
 210 environment, initially presented in NIST SP 1800-30B, Section 4.5, Final Architecture. The HDO
 211 environment utilizes network segmenting similar to the architecture segmentation used in NIST SP 1800-
 212 24, *Securing Picture Archiving and Communication System (PACS)* [1]. The telehealth platform provider is
 213 a vendor-managed cloud environment that facilitates data transmissions and communications between
 214 the patient home and the HDO. Patient home environments have a minimalistic structure, which
 215 incorporates the devices provided by the telehealth platform provider.

216 **Figure 1-1 Final Architecture**



217 **2 Product Installation Guides**

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

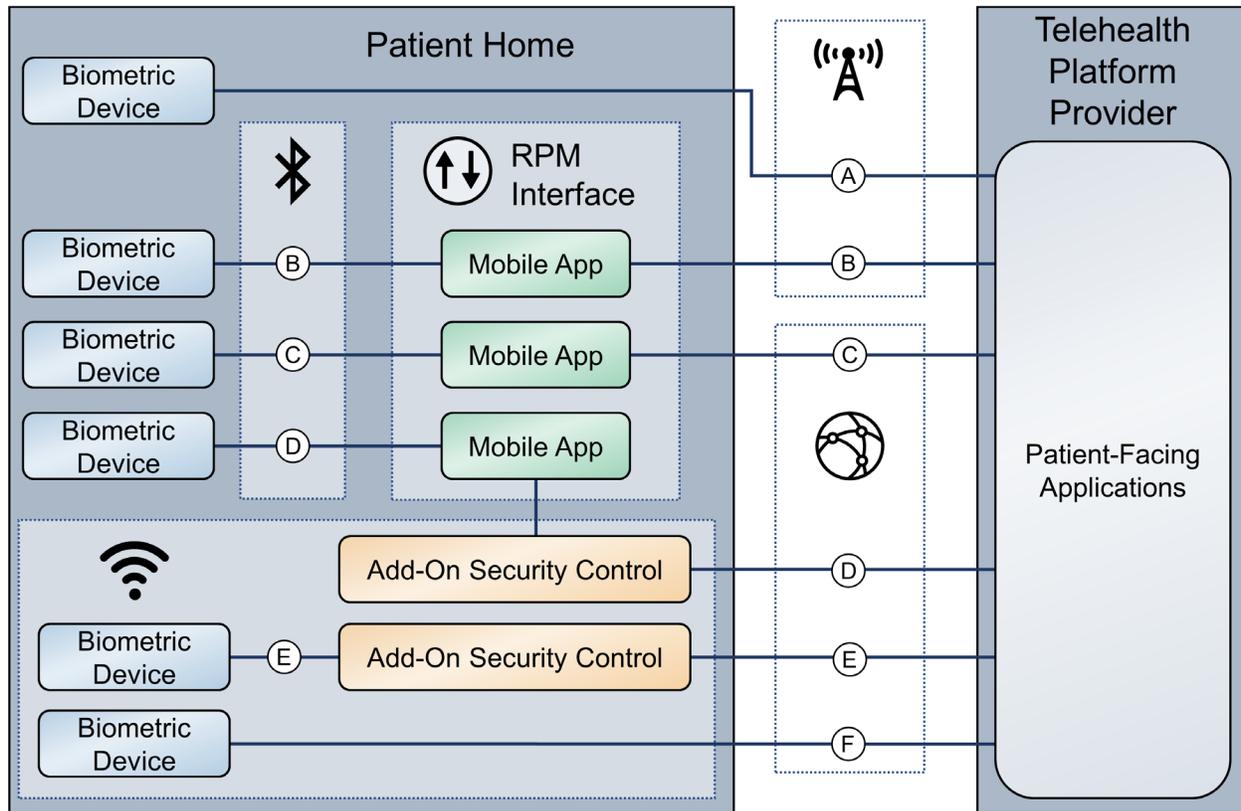
227 **2.1 Telehealth Platform Provider**

228 The project team implemented a model where an HDO partners with telehealth platform providers to
 229 enable RPM programs. Telehealth platform providers are third parties that, for this practice guide,

230 configured, deployed, and managed biometric devices and mobile devices (e.g., tablets) that were sent
231 to the patient home. The telehealth platform provider managed data communications over cellular and
232 broadband where patients send biometric data to the telehealth platform provider. The telehealth
233 platform provider implemented an application that allowed clinicians to access the biometric data.

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

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



250

251 **2.1.1 Accuhealth**

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

259 **2.1.1.1 Patient Home—Communication Path A**

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

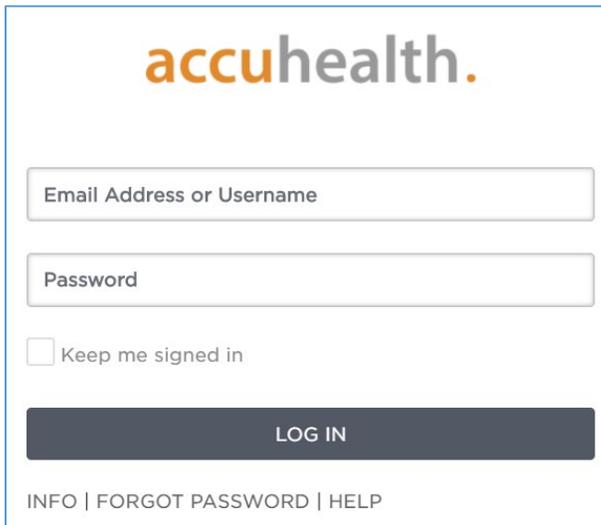
264 Accuhealth received patient contact information and configured biometric devices appropriate for the
265 RPM program in which the patient was enrolled. Accuhealth configured biometric devices to
266 communicate via cellular data, which is depicted as communication path A of [Figure 2-1](#). Biometric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

269 [2.1.1.2 HDO](#)

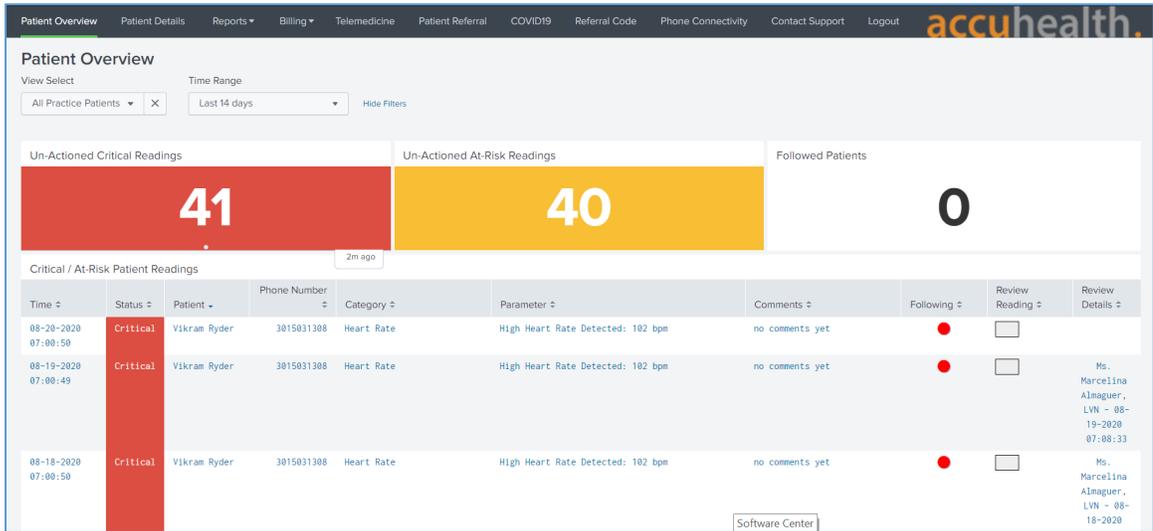
270 The Accuhealth solution includes installing an application within the HDO environment. Clinicians access
271 a portal hosted by Accuhealth that allows a clinician to view patient biometric data. The application
272 requires unique user accounts and role-based access control. System administrators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

275 This section discusses the HDO application installation and configuration procedures.

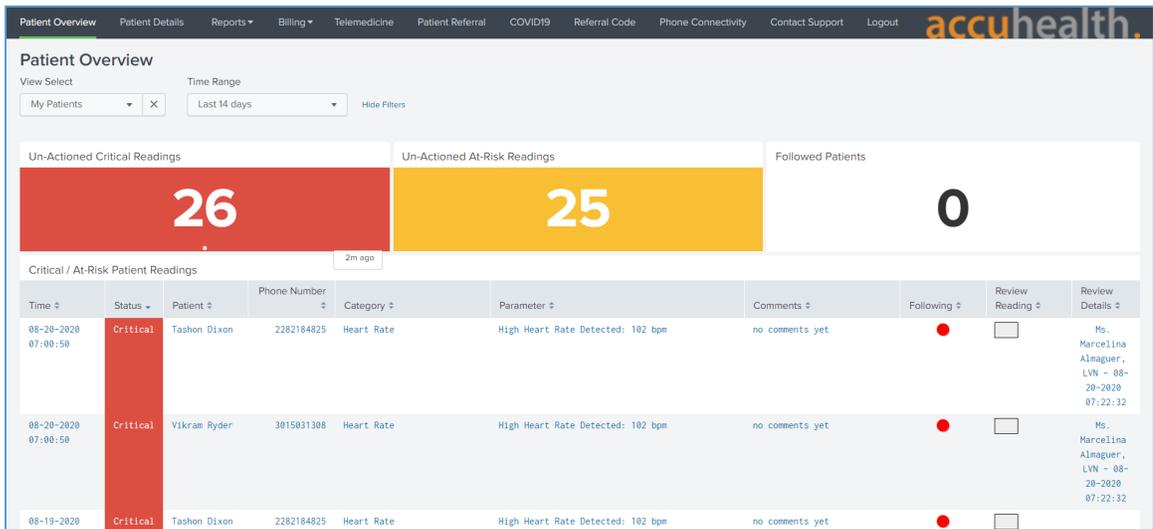
- 276 1. Access a device that has a web browser.
- 277 2. Navigate to Accuhealth login page, and provide a **Username** and **Password**. The following
278 screenshots show a doctor's point of view in the platform.
- 279 3. Click **LOG IN**.



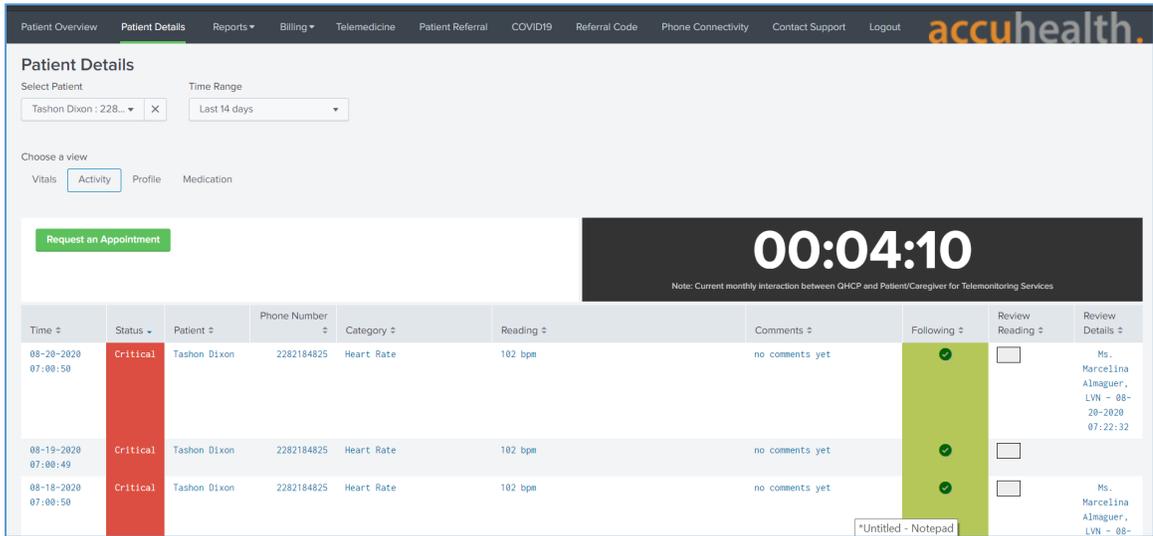
280 After logging in, the **Patient Overview** screen displays.



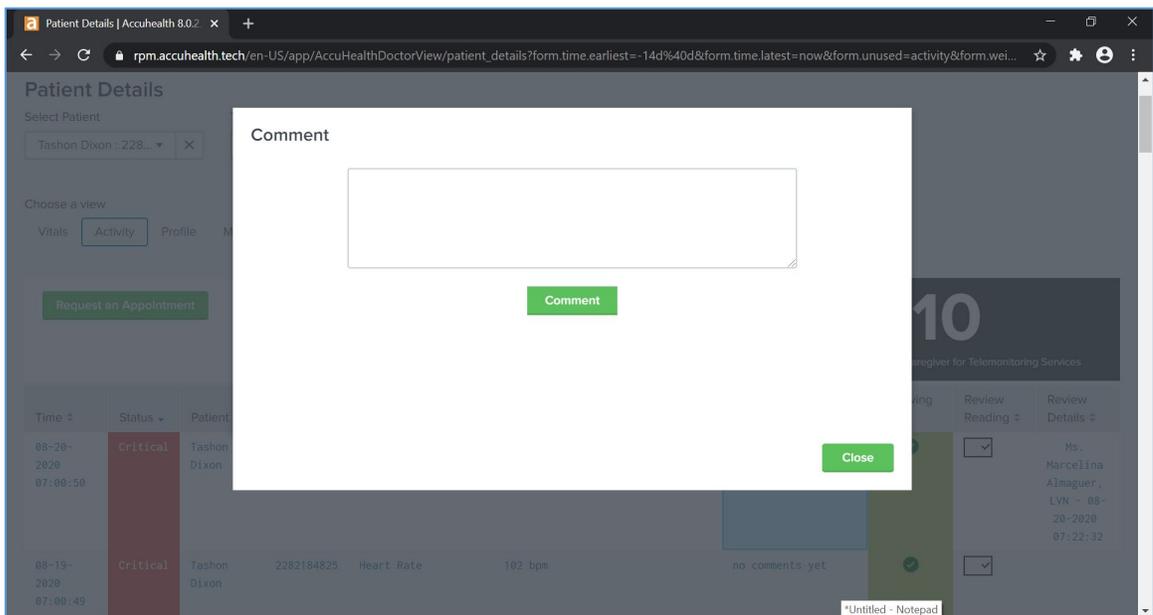
- 281 4. To view patients associated with the account used to log in, navigate to the **View Select** drop-
 282 down list in the top left corner of the screen, and select **My Patients**.



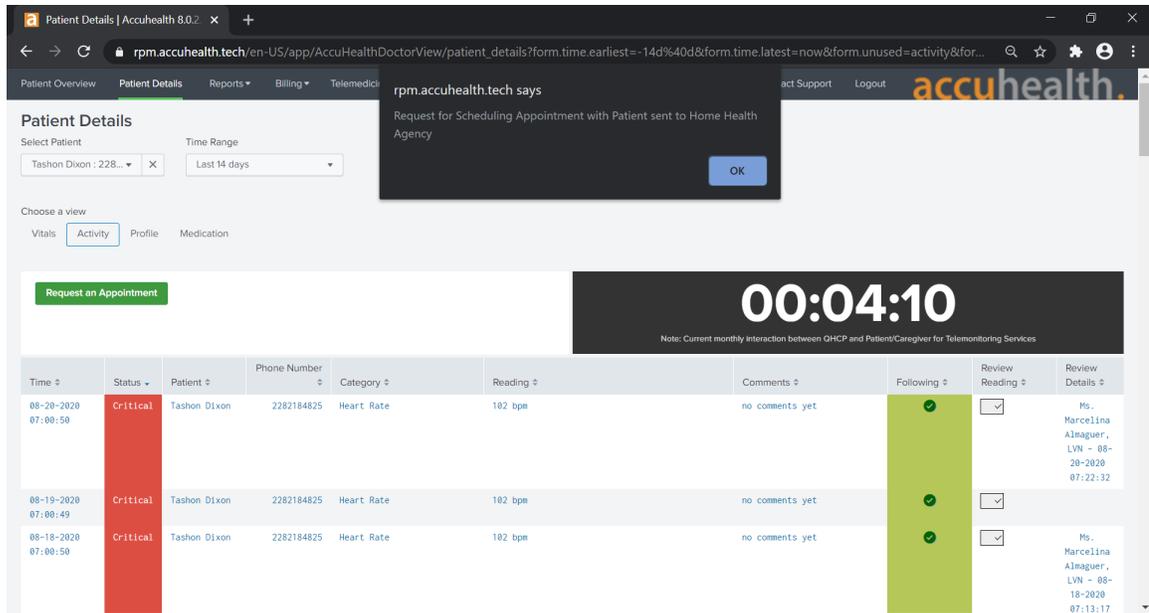
- 283 5. Click a **Patient** to display the **Patient Details** page, which displays all patient biomedical
 284 readings.



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



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



295 2.1.2 Vivify Health

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

303 2.1.2.1 Patient Home—Communication Path B

304 This practice guide assumes that the HDO enrolls the patient in an RPM program. Clinicians would
 305 determine when a patient may be enrolled in the program appropriately, and conversations then occur
 306 about understanding the roles and responsibilities associated with participating in the RPM program.
 307 When clinicians enroll patients in the RPM program, the HDO would collaborate with Vivify. Vivify
 308 received patient contact information and configured biometric devices and an interface device (i.e.,

309 tablet) appropriate for the RPM program in which the patient was enrolled. These devices were
310 configured to transmit data via cellular through the interface device, which is depicted as
311 communication path B in [Figure 2-1](#). Vivify assured device configuration and asset management.

312 *2.1.2.2 Patient Home—Communication Paths C and D*

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

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

331 *2.1.2.3 Telehealth Platform—Communication Paths C and D*

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

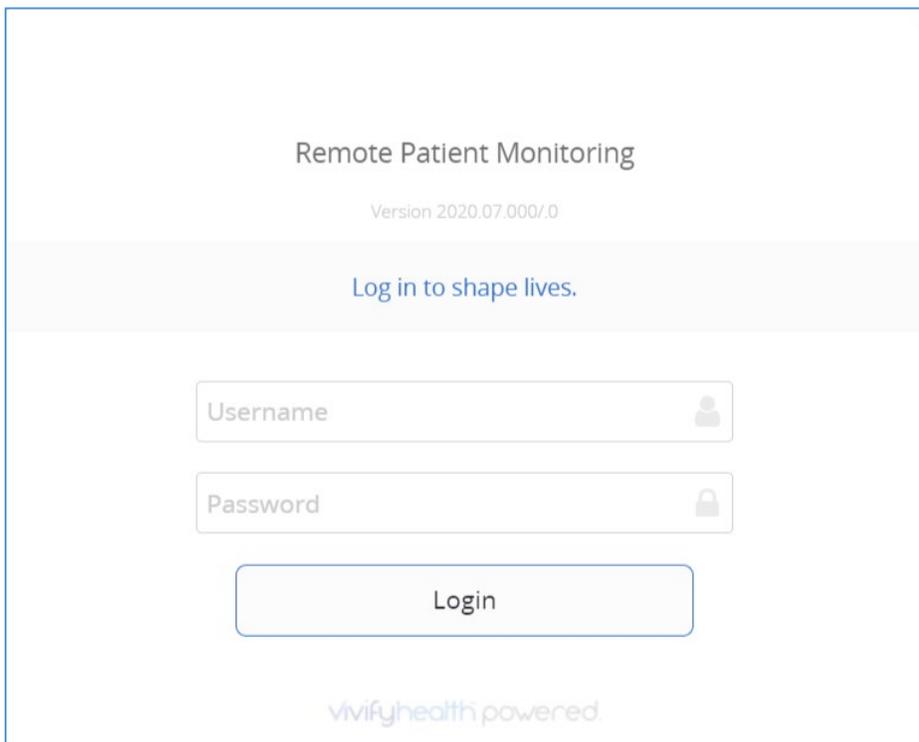
340 Communication path D required more add-on security controls to be configured in the virtual cloud
341 environment. For this communication pathway, the representative Vivify Pathways Care Team Portal
342 was connected to an Onclave Telehealth Gateway. This gateway accepted data transmissions from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

344 **2.1.2.4 HDO**

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

349 This section discusses the HDO application installation and configuration procedures.

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



- 354
- 355 4. Navigate to the **Care Team** menu item on the left-hand side of the screen.
356 Click **+ New User**.
- 357 5. In the **New User** screen, provide the following information:
358 a. **First Name:** Test

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

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

386 2.2 Security Capabilities

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

390 2.2.1 Risk Assessment Controls

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

395 2.2.1.1 Tenable.sc

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

402 System Requirements

403 **Central Processing Unit (CPU):** 4

404 **Memory:** 8 gigabytes (GB)

405 **Storage:** 250 GB

406 **Operating System:** CentOS 7

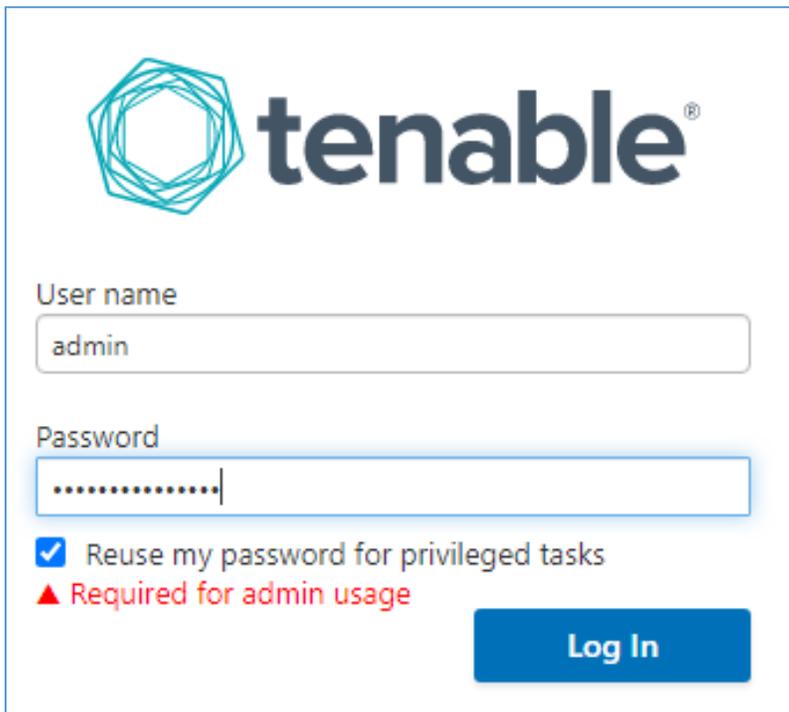
407 **Network Adapter:** virtual local area network (VLAN) 1348

408 Tenable.sc Installation

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

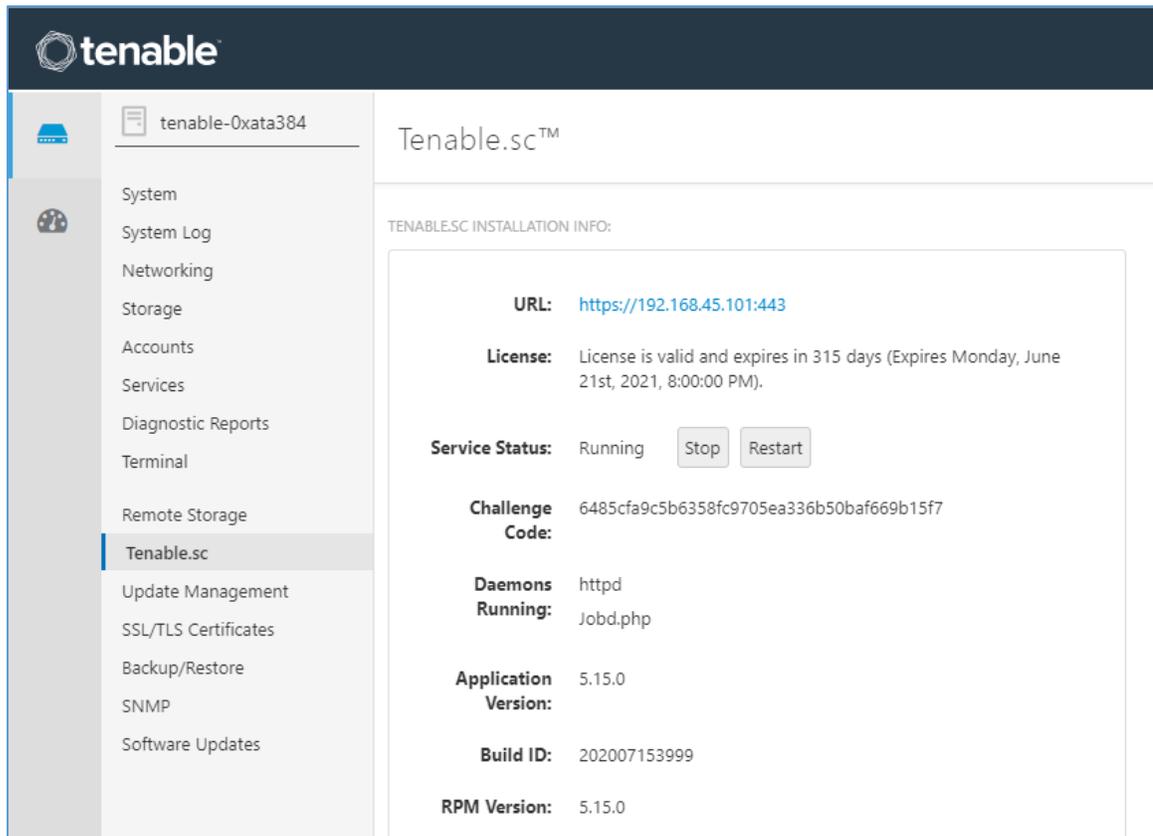
- 410 1. Import the Tenable.sc **open virtual appliance or appliance (OVA) file** to the virtual environment.
- 411 2. Assign the virtual machine (VM) to **VLAN 1348**.
- 412 3. Start the VM, and document the associated **internet protocol (IP) address**.
- 413 4. Open a web browser that can talk to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

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



The screenshot shows the Tenable login interface. At the top left is the Tenable logo, which consists of a teal geometric shape followed by the word 'tenable' in a dark blue sans-serif font. Below the logo are two input fields: 'User name' with the text 'admin' and 'Password' with masked characters represented by dots. Under the password field is a checkbox that is checked, with the text 'Reuse my password for privileged tasks'. Below this checkbox is a red warning triangle icon followed by the text 'Required for admin usage'. At the bottom right of the form is a blue button with the text 'Log In' in white.

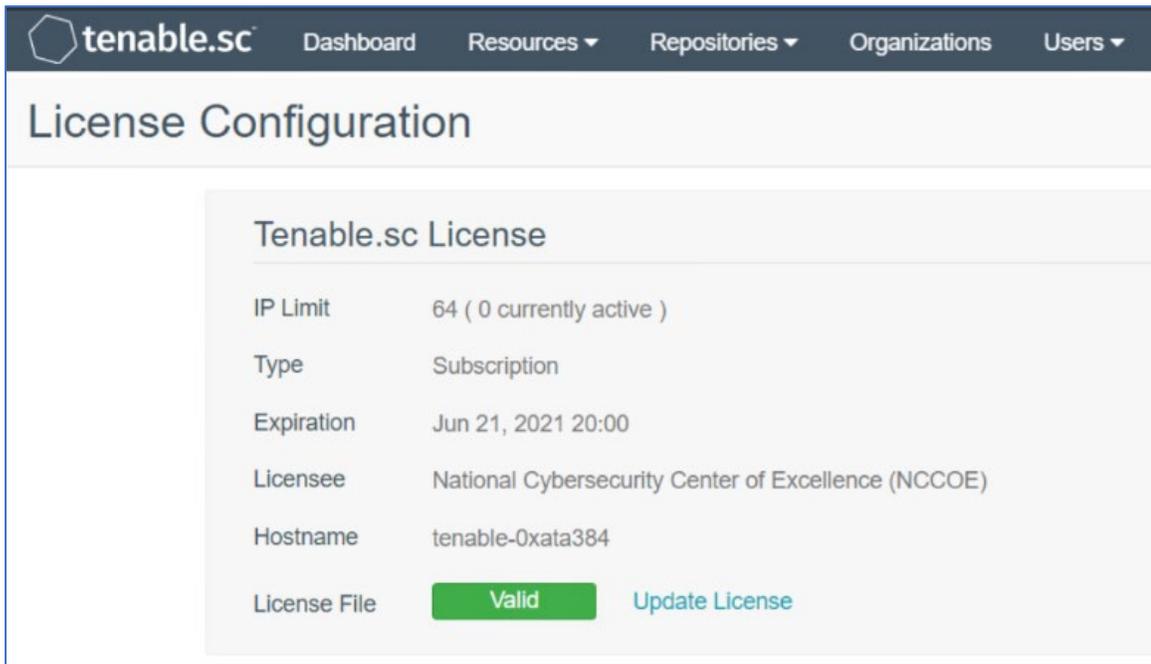
- 420 8. After logging in, the Tenable Management Console page displays.
- 421 9. Click the **Tenable.sc** menu option on the left side of the screen.
- 422 10. To access Tenable.sc, click the **IP address** next to the uniform resource locator (URL) field.



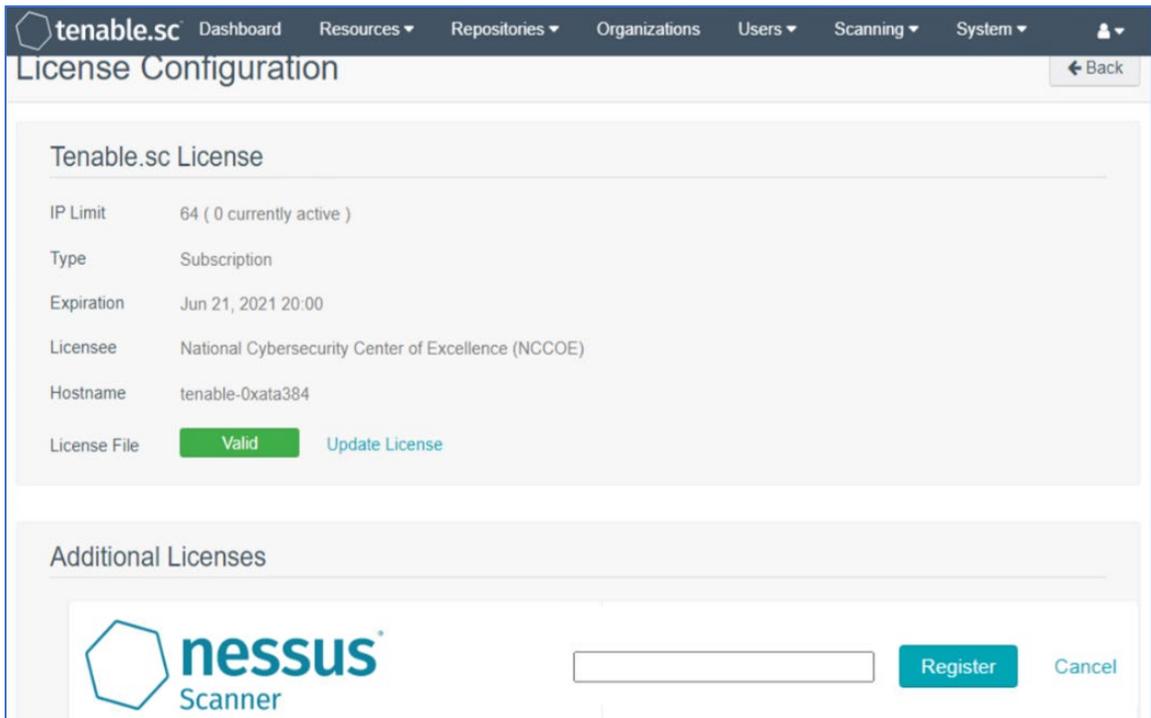
- 423 11. Log in to Tenable.sc by using the credentials created in previous steps, and click **Sign In**.
- 424 a. **Username:** admin
- 425 b. **Password:** *****



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



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

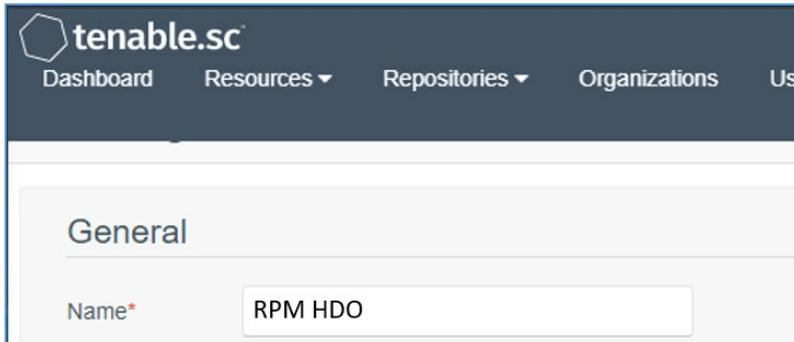


438 **Tenable.sc Configuration**

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

442 **Add an Organization**

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



447 Add a Repository

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

The screenshot shows the 'Add IPv4 Repository' page in the Tenable.sc interface. The navigation bar at the top includes 'tenable.sc', 'Dashboard', 'Resources', 'Repositories', and 'Organizations'. The main heading is 'Add IPv4 Repository'. The form is organized into three sections:

- General:** Contains a 'Name*' field with the value 'HDO Repository' and a 'Description' text area.
- Data:** Contains an 'IP Ranges*' field with the value '0.0.0.0/24'.
- Access:** Contains an 'Organizations' search field. A dropdown menu is open, showing a search bar and a single result: 'RPM HDO' with a checked checkbox.

456 Add a User

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

- 462 c. **First Name:** Test
 - 463 d. **Last Name:** User
 - 464 e. **Username:** TestSecManager
 - 465 f. **Password:** *****
 - 466 g. **Confirm Password:** *****
 - 467 h. Enable **User Must Change Password.**
 - 468 i. **Time Zone:** America/New York
- 469 4. Click **Submit.**

The screenshot shows the 'Add User' form in the Tenable.sc interface. The form is divided into two main sections: 'Membership' and a user information section. The 'Membership' section includes a 'Role' dropdown menu set to 'Security Manager' and an 'Organization*' dropdown menu set to 'RPM HDO'. The user information section includes the following fields and controls:

- First Name:** Text input field containing 'Test'.
- Last Name:** Text input field containing 'User'.
- Username*:** Text input field containing 'TestSecManager'.
- Password*:** Password input field with masked characters (dots).
- Confirm Password*:** Password input field with masked characters (dots).
- User Must Change Password:** A toggle switch that is currently turned on (blue).
- Time Zone*:** Dropdown menu set to 'America/New_York'.

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

472 Add a Scanner

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

tenable.sc Dashboard Resources Repositories Organizations Users

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*

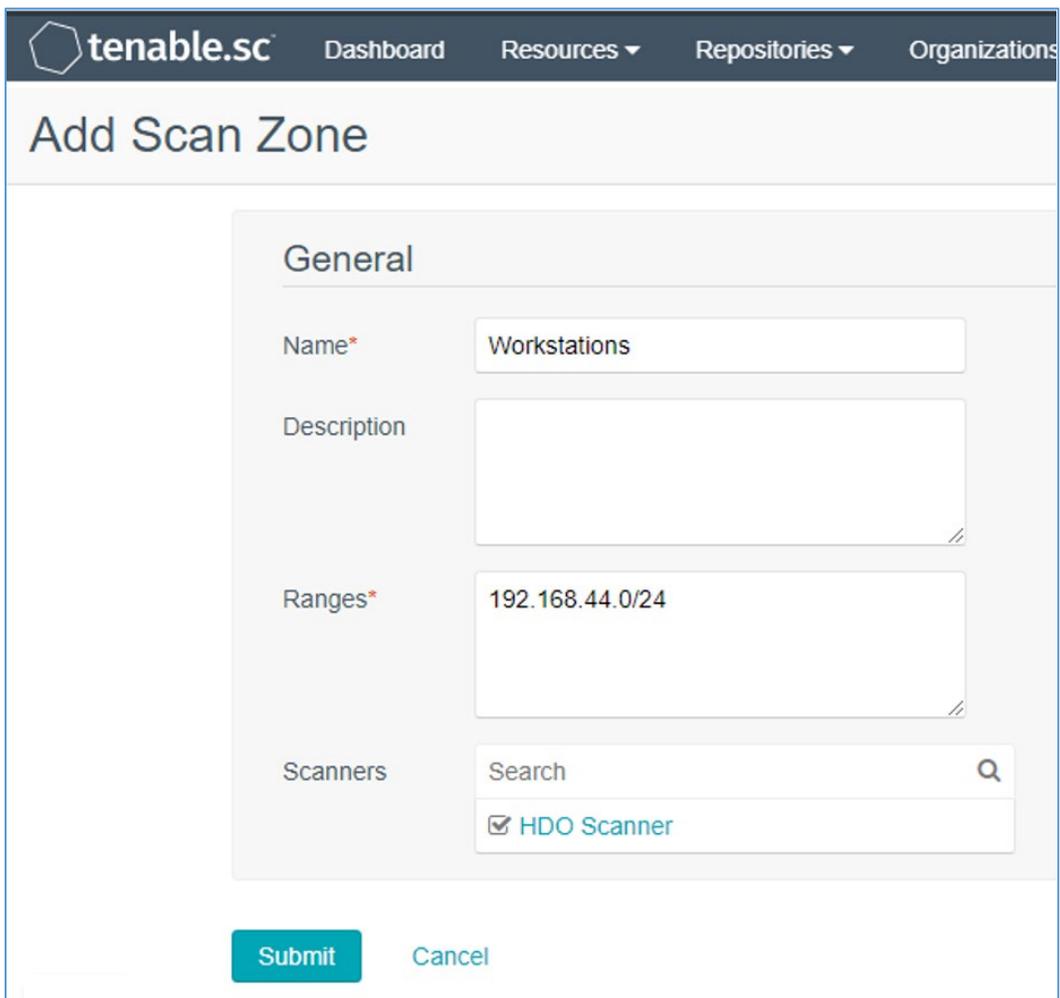
486 The engineers created a scan zone for each subnet established on the HDO network. The process to
487 create a scan zone is the same for each subnet aside from the IP address range.

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

489 Add a Scan Zone

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

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



The screenshot shows the Tenable.sc interface for adding a scan zone. The navigation bar at the top includes the Tenable.sc logo and links for Dashboard, Resources, Repositories, and Organizations. The main heading is 'Add Scan Zone'. Below this is a form with a 'General' section. The form contains the following fields:

- Name***: A text input field containing 'Workstations'.
- Description**: A large text area that is currently empty.
- Ranges***: A text input field containing '192.168.44.0/24'.
- Scanners**: A search input field with a magnifying glass icon. Below the search bar, a dropdown menu shows 'HDO Scanner' with a checked checkbox.

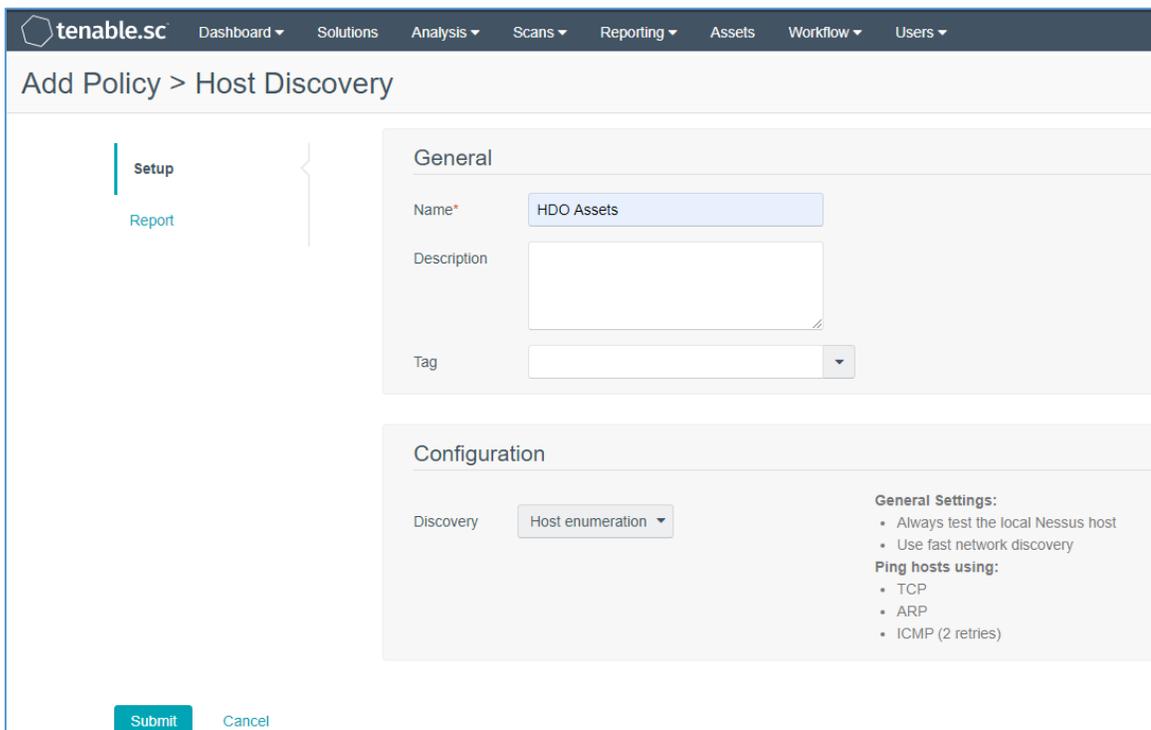
At the bottom of the form, there are two buttons: a teal 'Submit' button and a grey 'Cancel' button.

- 497 Repeat steps in Add a Scan Zone section for each VLAN.
- 498 To fulfil the identified NIST Cybersecurity Framework Subcategory requirements, the engineers utilized
- 499 Tenable's host discovery and vulnerability scanning capabilities. The first goal was to identify the hosts

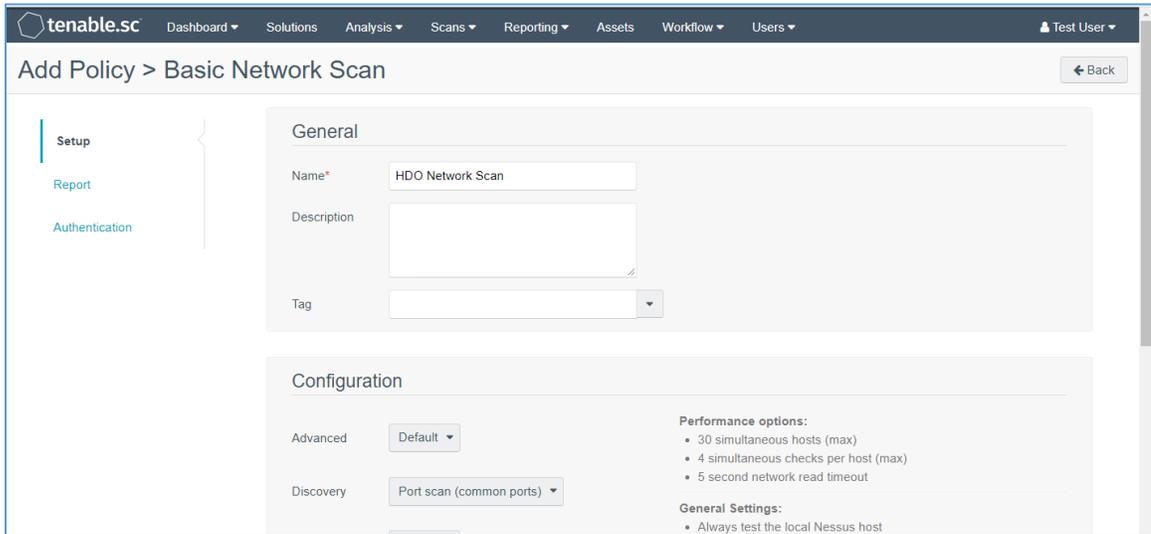
500 on each of the HDO VLANs. Once Tenable identifies the assets, Tenable.sc executes a basic network scan
 501 to identify any vulnerabilities on these assets.

502 Create Scan Policies

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



- 514 7. Click **+Add** in the top right corner.
- 515 8. Click **Basic Network Scan** in the **Add Policy** page. An **Add Policy > Basic Network Scan** page displays.
- 516
- 517 9. Name the scan **HDO Network Scan** and leave the remaining options to their default settings.
- 518 10. Click **Submit**.



519 Create Active Scans

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

524 **General**

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

528 **Targets**

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

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

- 535 a. Name the scan **HDO Network Scan**.
- 536 b. Set Policy to **HDO Network Scan**.

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

539 Execute Active Scans

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

547 View Active Scan Results in the Dashboard

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

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

553 2.2.1.2 *Nessus*

554 Nessus is a vulnerability scanning engine that evaluates a host’s operating system and configuration to

555 determine the presence of exploitable vulnerabilities. This project uses one Nessus scanner to scan each

556 VLAN created in the HDO environment to identify hosts on each VLAN and the vulnerabilities associated

557 with those hosts. Nessus sends the results back to Tenable.sc, which graphically represents the results in

558 dashboards.

559 System Requirements

560 **CPU:** 4

561 **Memory:** 8 GB

562 **Storage:** 82 GB

563 **Operating System:** CentOS 7

564 **Network Adapter:** VLAN 1348

565 Nessus Installation

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

tenable®

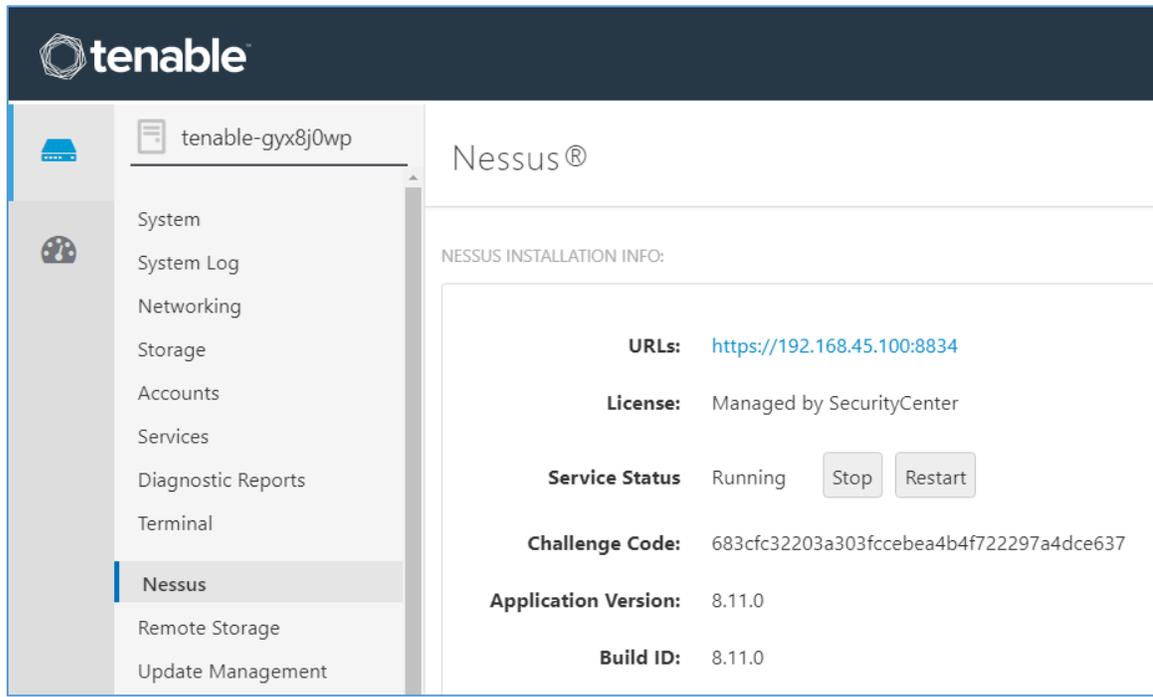
User name
admin

Password
.....

Reuse my password for privileged tasks
▲ Required for admin usage

Log In

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



578 **Nessus Configuration**

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

581 **2.2.2 Identity Management, Authentication, and Access Control**

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

589 **2.2.2.1 Domain Controller**

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

593 **Domain Controller Appliance Information**

594 **CPU:** 4

595 **Random Access Memory (RAM):** 8 GB

596 **Storage:** 120 GB (Thin Provision)

597 **Network Adapter 1:** VLAN 1327

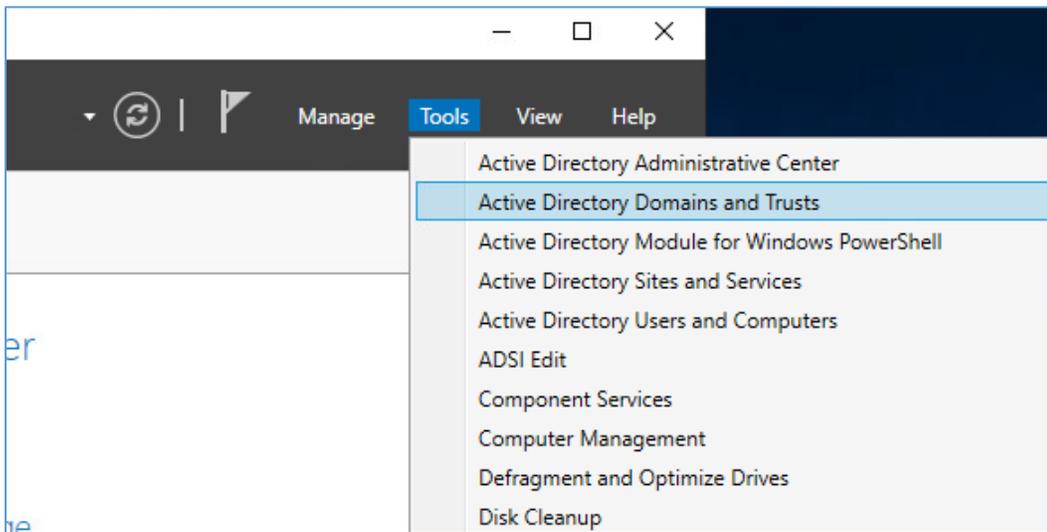
598 **Operating System:** Microsoft Windows Server 2019 Datacenter

599 **Domain Controller Appliance Installation Guide**

600 Install the appliance according to the instructions detailed in Microsoft’s Install Active Directory Domain
601 Services (Level 100) documentation [\[4\]](#).

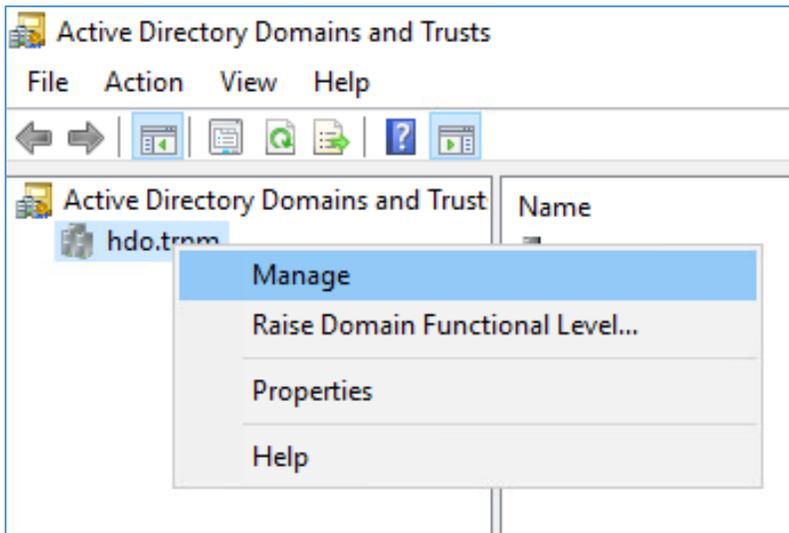
602 **Verify Domain Controller Installation**

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



605 3. Right-click **hdo.trpm**.

606 4. Click **Manage**.



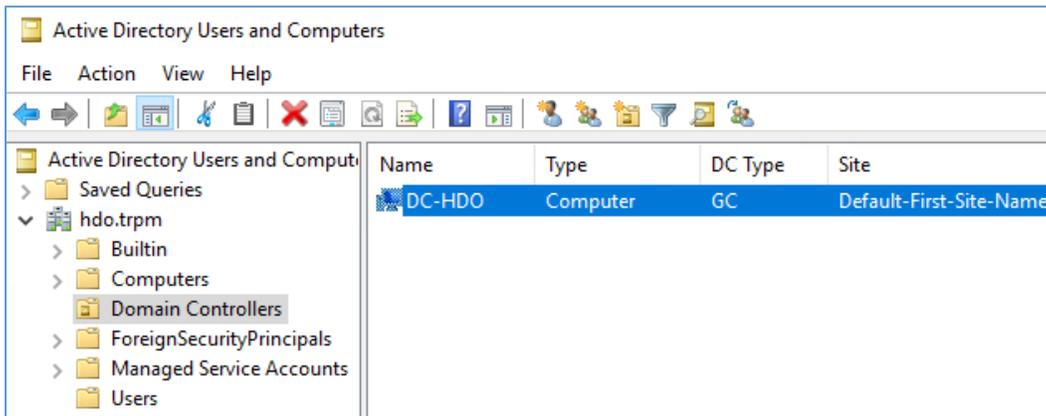
607

608

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

609

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



610

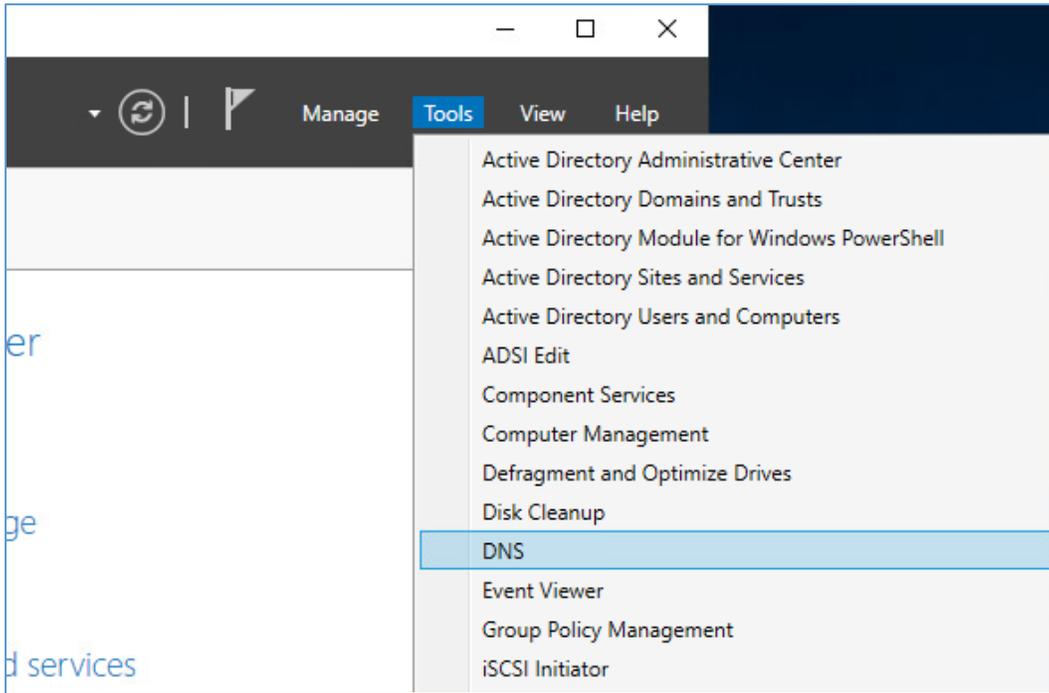
611 **Configure Local DNS**

612

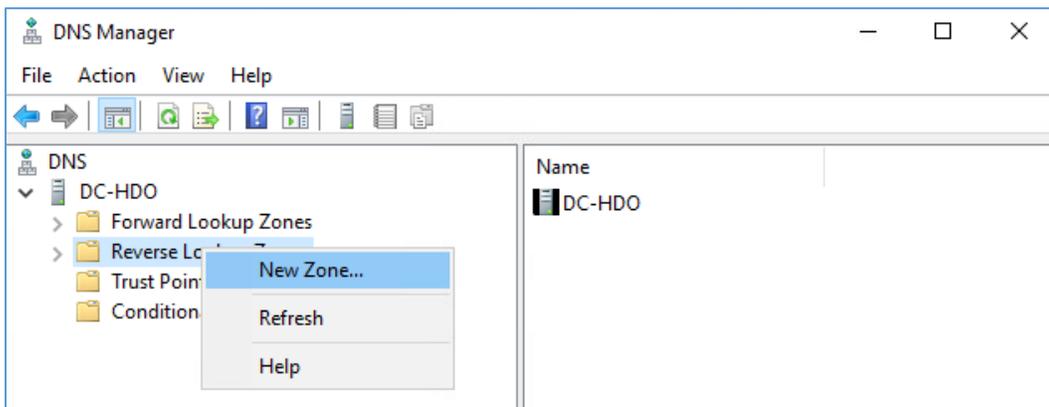
1. Launch **Server Manager**.

613

2. Click **Tools > DNS**.



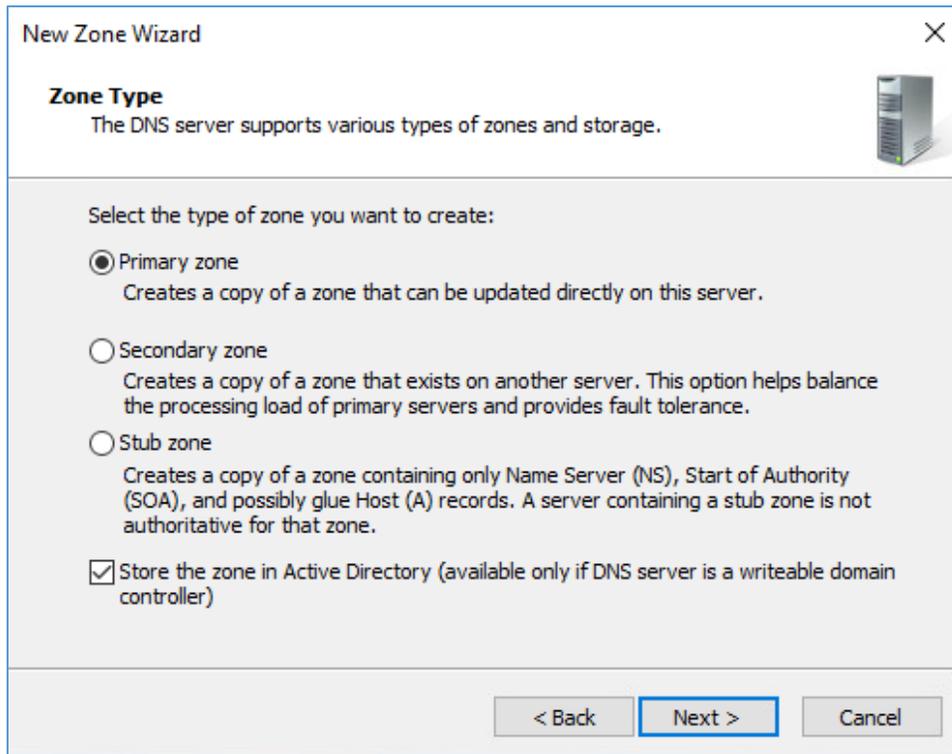
- 614 3. Click the **arrow symbol** for DC-HDO.
- 615 4. Right-click **Reverse Lookup Zones**.
- 616 5. Click **New Zone....** The New Zone Wizard displays.



- 617 6. Click **Next >**.

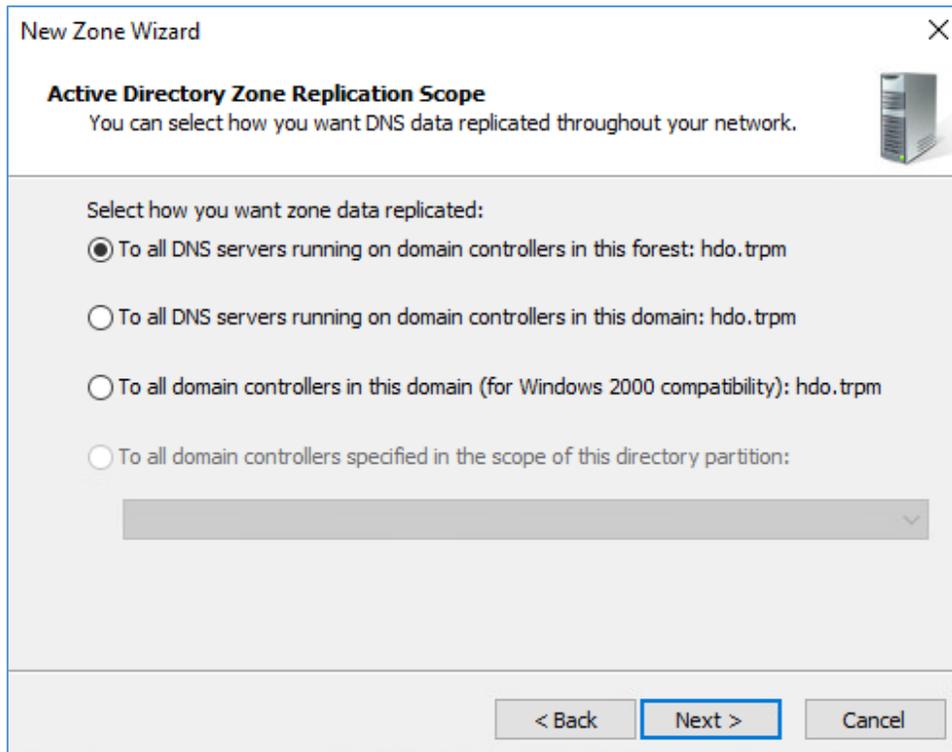


- 618 7. Click **Primary zone**.
- 619 8. Check **Store the zone in Active Directory**.
- 620 9. Click **Next >**.



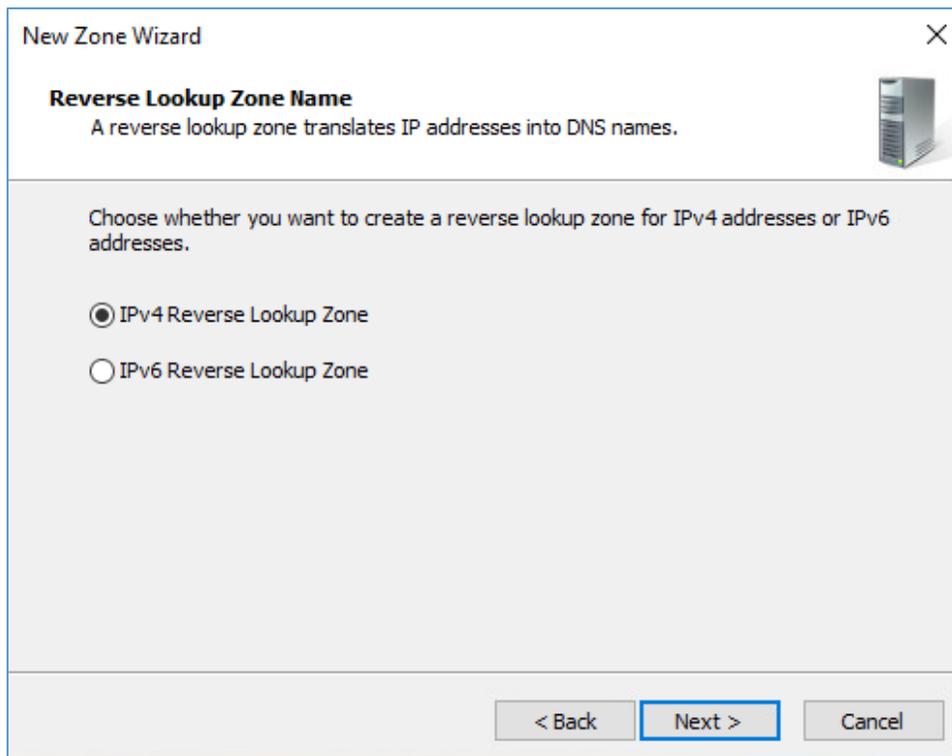
621 10. Check **To all DNS servers running on domain controllers in this forest: hdo.trpm.**

622 11. Click **Next >**.

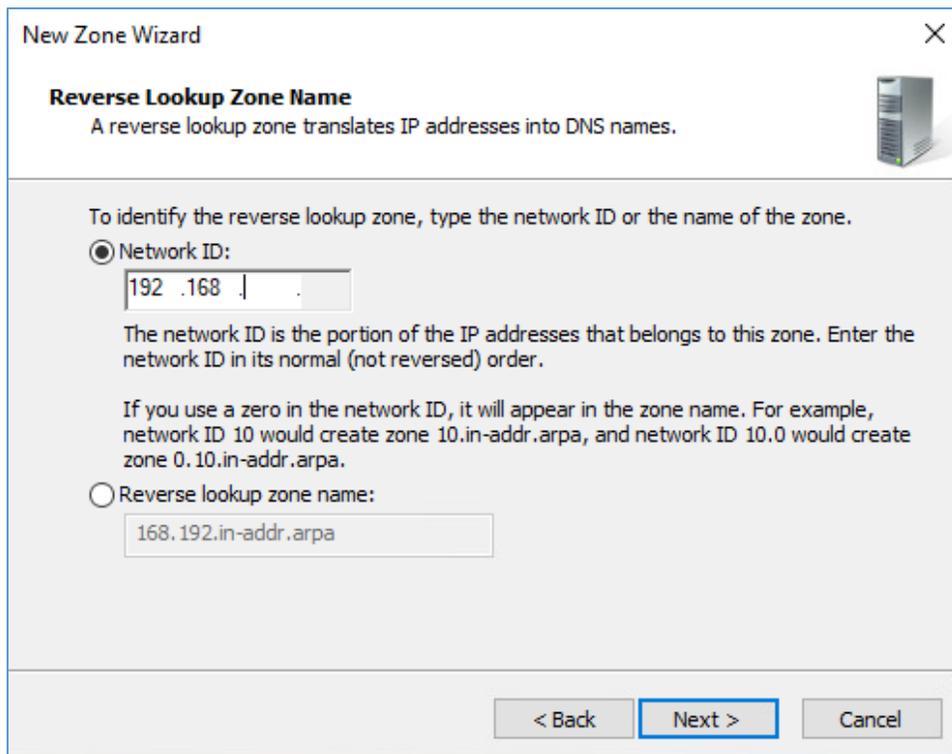


623 12. Check **IPv4 Reverse Lookup Zone**.

624 13. Click **Next >**.



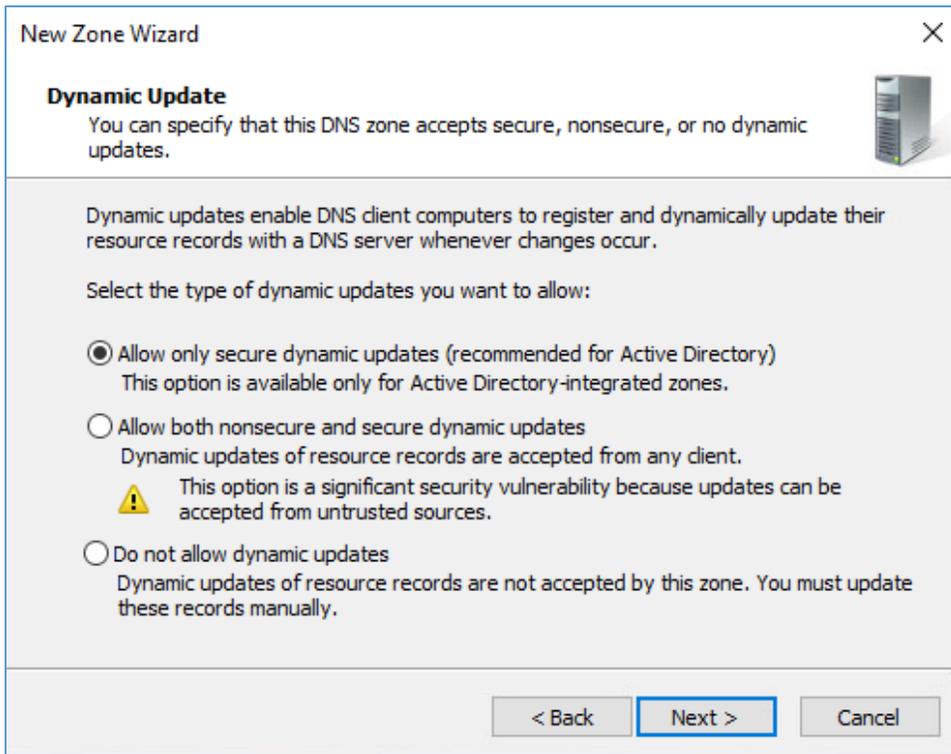
- 625 14. Check **Network ID**.
- 626 15. Under **Network ID**, type **192.168**.
- 627 16. Click **Next >**.



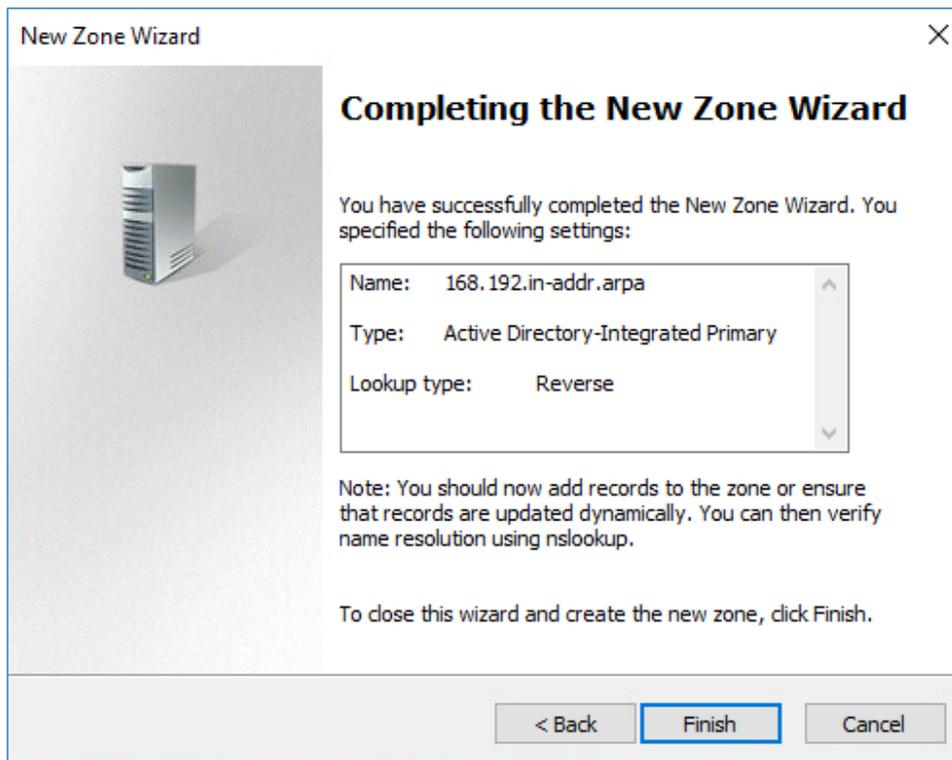
The screenshot shows a 'New Zone Wizard' dialog box with a close button (X) in the top right corner. The title bar reads 'New Zone Wizard'. The main heading is 'Reverse Lookup Zone Name', followed by the text 'A reverse lookup zone translates IP addresses into DNS names.' and a server icon. Below this, a paragraph states: 'To identify the reverse lookup zone, type the network ID or the name of the zone.' There are two radio button options. The first is 'Network ID:', which is selected. Its text box contains '192 .168 .'. Below this text box is explanatory text: '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.' and '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.' The second radio button option is 'Reverse lookup zone name:', with its text box containing '168.192.in-addr.arpa'. At the bottom of the dialog are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

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

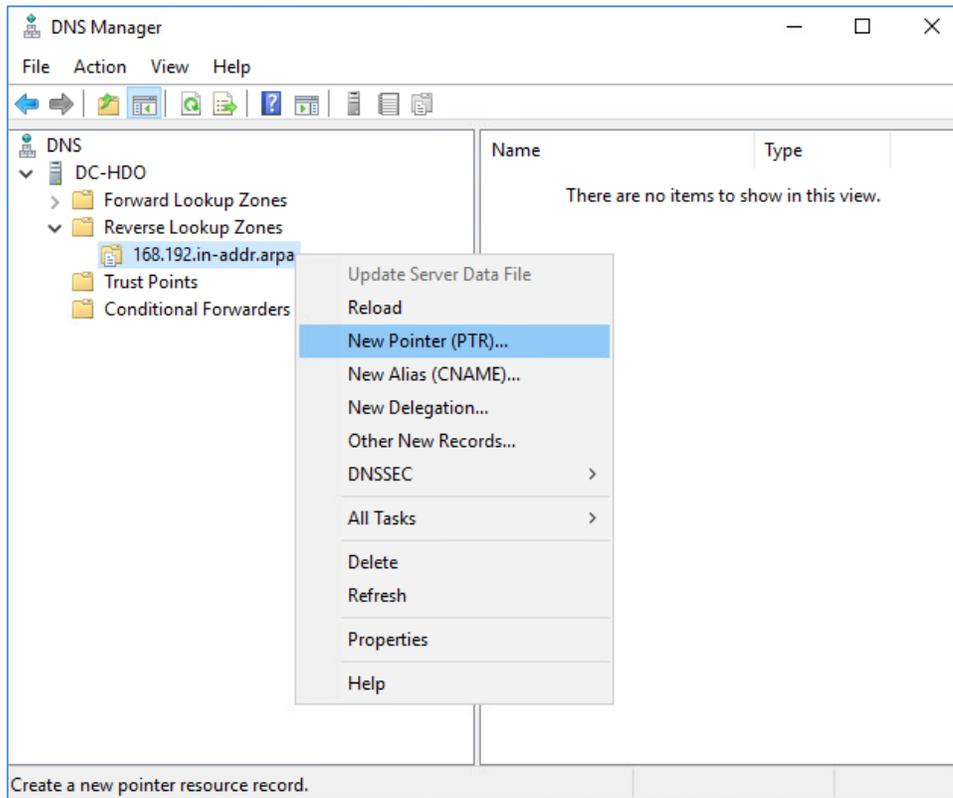
629 18. Click **Next >**.



630 19. Click **Finish**.



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



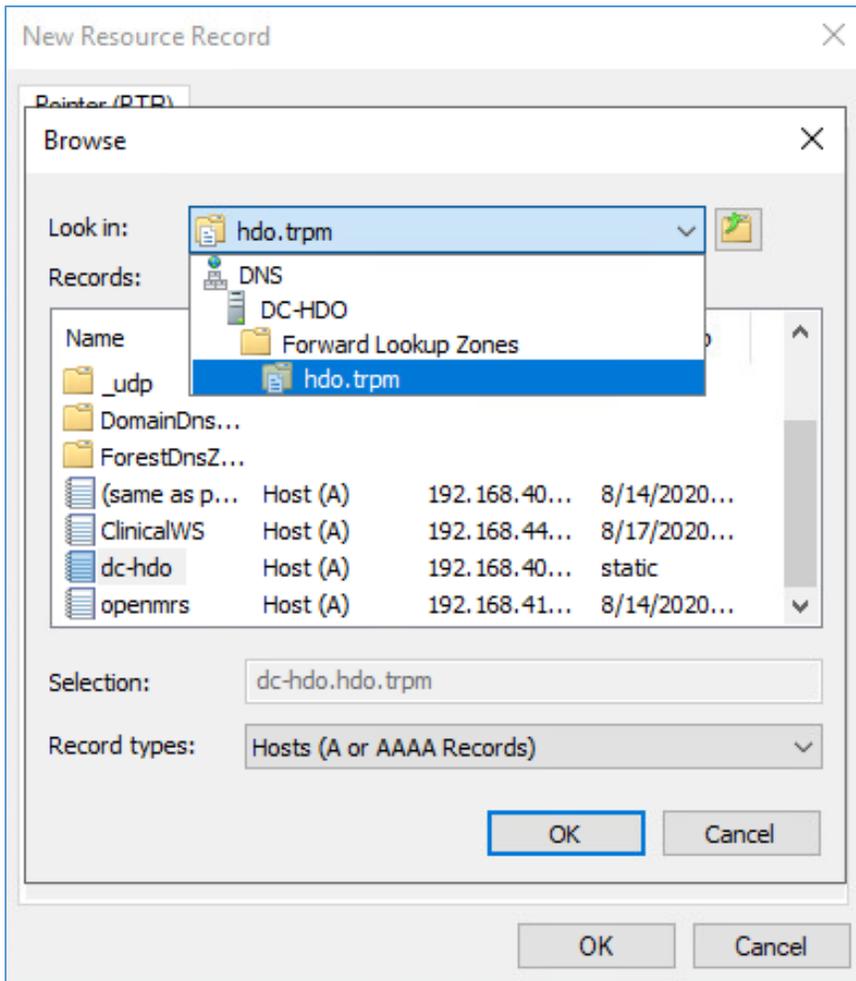
634 23. Under **Host name**, click **Browse....**

The image shows a 'New Resource Record' dialog box with a close button (X) in the top right corner. The dialog has a tab labeled 'Pointer (PTR)'. It contains three text input fields: 'Host IP Address' with the value '192.168.', 'Fully qualified domain name (FQDN)' with the value '168.192.in-addr.arpa', and 'Host name' which is empty. To the right of the 'Host name' field is a 'Browse...' button. Below these fields is a checkbox that is currently unchecked, with the text 'Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.' At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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

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

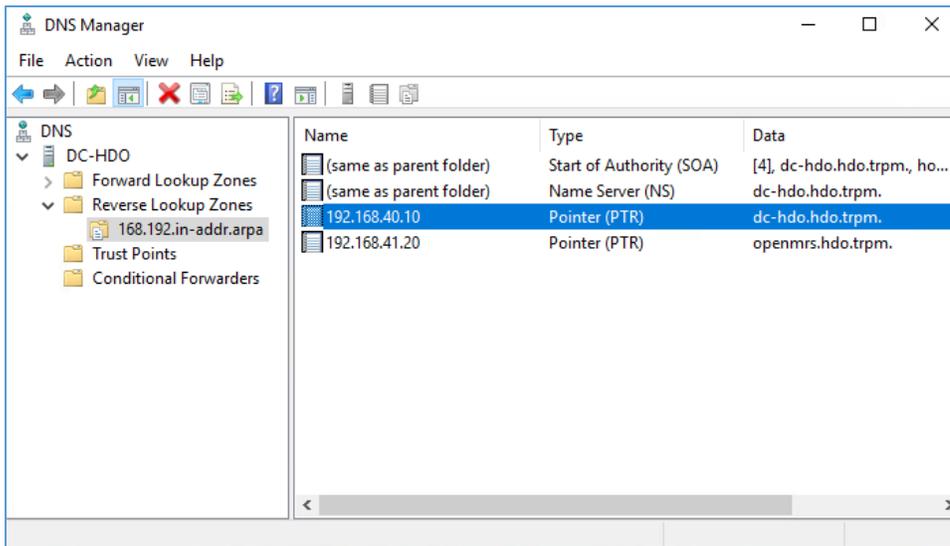
637 26. Click **OK**.



638 27. Click **OK**.

The image shows a 'New Resource Record' dialog box with a close button (X) in the top right corner. The dialog is titled 'New Resource Record' and has a tab labeled 'Pointer (PTR)'. It contains the following fields and controls:

- Host IP Address:** A text box containing '192.168.40.10'.
- Fully qualified domain name (FQDN):** A text box containing '10.40.168.192.in-addr.arpa'.
- Host name:** A text box containing 'dc-hdo.hdo.tpm' and a 'Browse...' button to its right.
- Permissions:** A checkbox labeled 'Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.' which is currently unchecked.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.



639 2.2.2.2 Cisco Firepower

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

646 Cisco Firepower Management Center (FMC) Appliance Information

647 **CPU:** 4

648 **RAM:** 8 GB

649 **Storage:** 250 GB (Thick Provision)

650 **Network Adapter 1:** VLAN 1327

651 **Operating System:** Cisco Fire Linux 6.4.0

652 Cisco Firepower Management Center Installation Guide

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

655 Cisco FTD Appliance Information

656 **CPU:** 8

657 **RAM:** 16 GB

658 **Storage:** 48.5 GB (Thick Provision)

659 **Network Adapter 1:** VLAN 1327

660 **Network Adapter 2:** VLAN 1327

661 **Network Adapter 3:** VLAN 1316

662 **Network Adapter 4:** VLAN 1327

663 **Network Adapter 5:** VLAN 1328

664 **Network Adapter 6:** VLAN 1329

665 **Network Adapter 7:** VLAN 1330

666 **Network Adapter 8:** VLAN 1347

667 **Network Adapter 9:** VLAN 1348

668 **Operating System:** Cisco Fire Linux 6.4.0

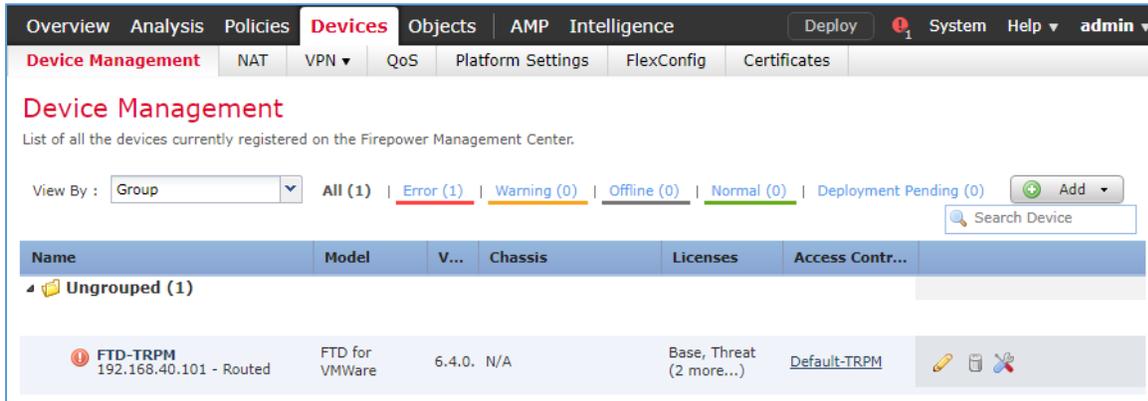
669 **Cisco FTD Installation Guide**

670 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 [\[6\]](#).

672 **Configure FMC Management of FTD**

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

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



678 From the Device Management section, the default routes, interfaces, and DHCP settings can be
679 configured. To view general information for the FTD appliance, navigate to **Devices > Device**
680 **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:	[Redacted]
Time:	2020-08-20 11:58:41
Time Zone:	UTC (UTC+0:00)
Version:	6.4.0.8

Health

Status:	[Warning Icon]
Policy:	Initial Health Policy 2020-02-26 20:00:53
Blacklist:	None

Management

Host:	192.168.40.101
Status:	[Checkmark Icon]

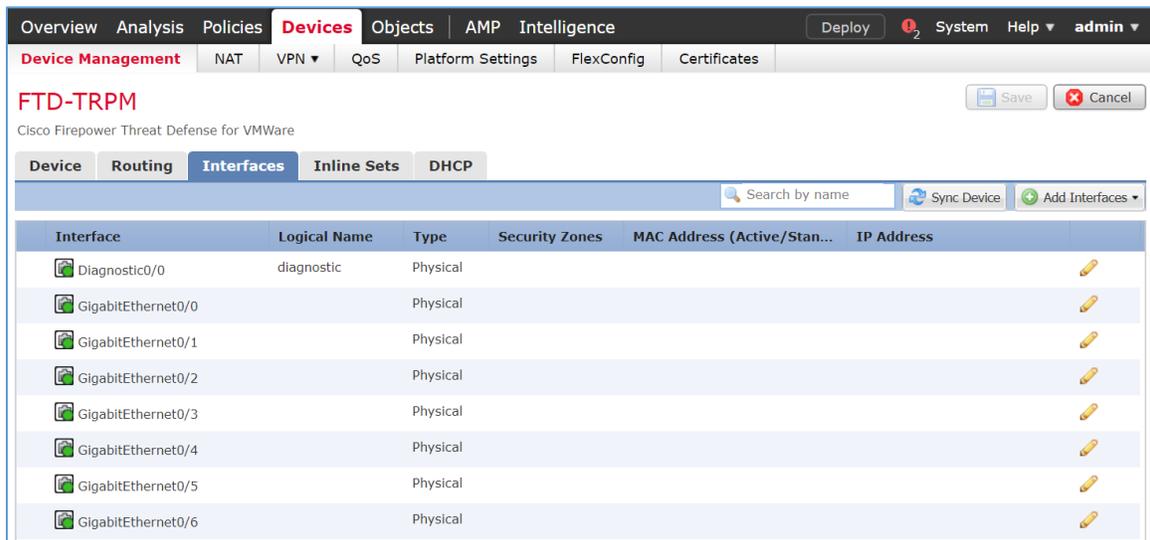
Advanced

Application Bypass:	No
Bypass Threshold:	3000 ms

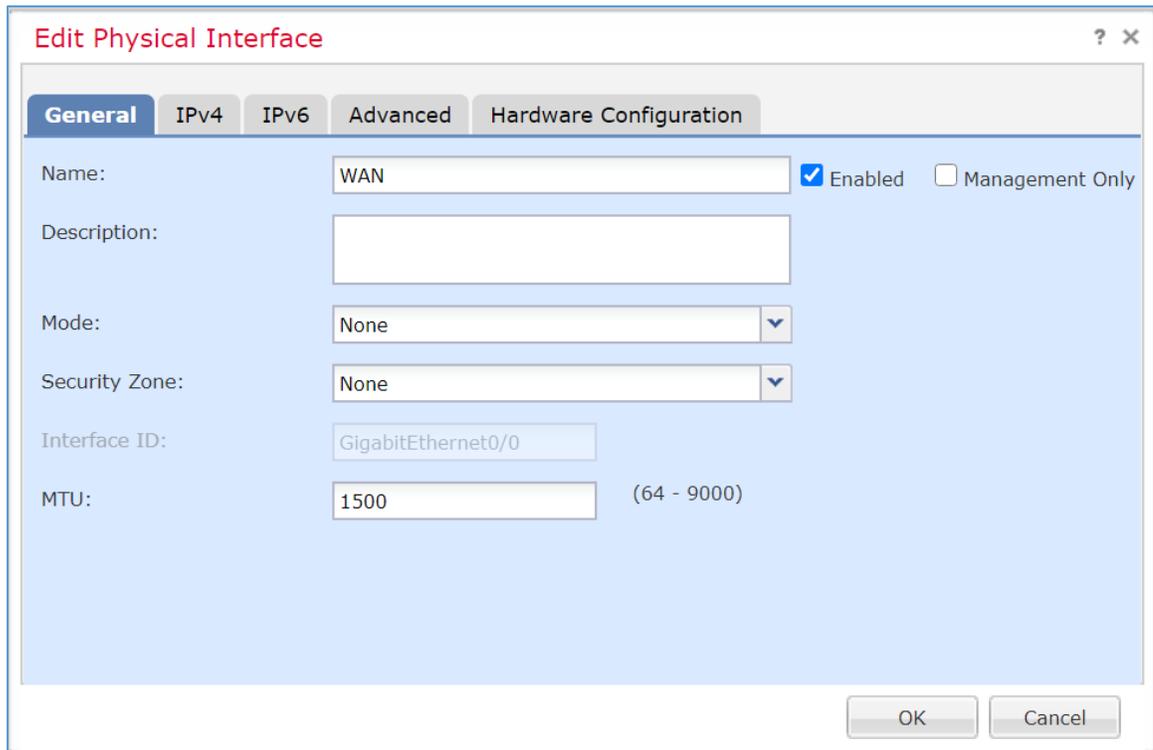
681 **Configure Cisco FTD Interfaces for the RPM Architecture**

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

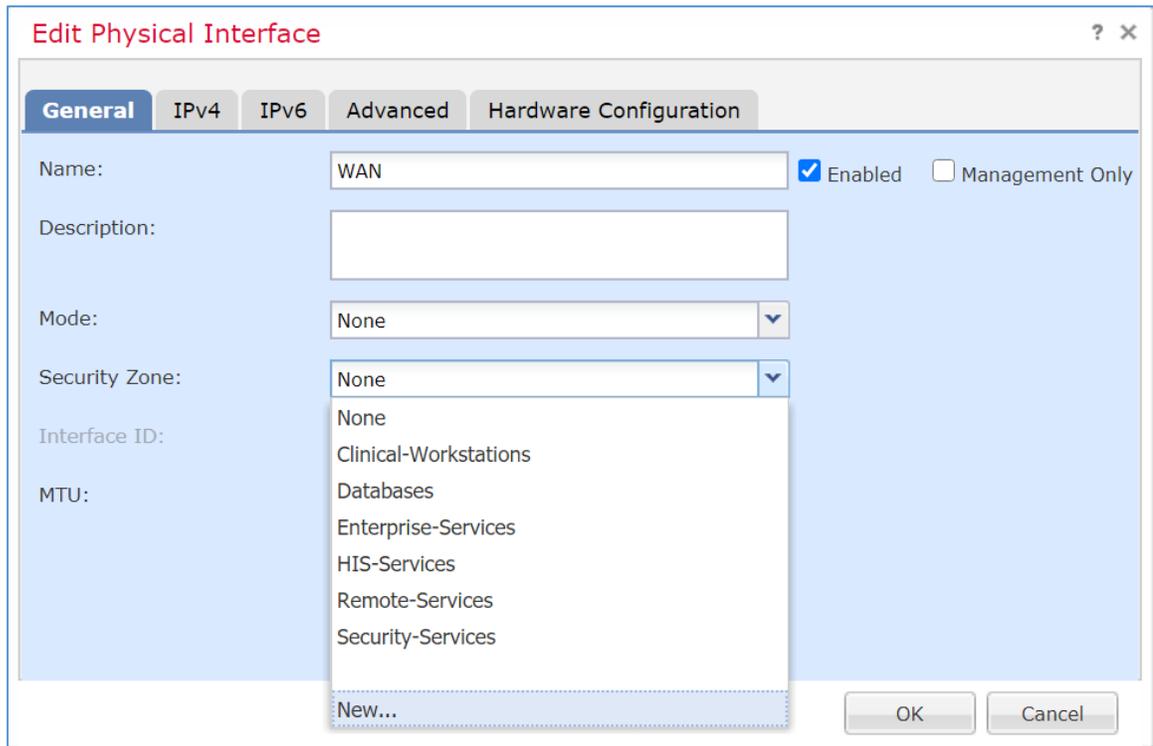
- 683 1. From **Devices > Device Management > FTD-TRPM > Device**, click **Interfaces**.
- 684 2. On the Cisco FTD Interfaces window, an Edit icon appears on the far right. The first
- 685 GigabitEthernet interface configured is GigabitEthernet0/0. Click the Edit icon to configure the
- 686 GigabitEthernet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



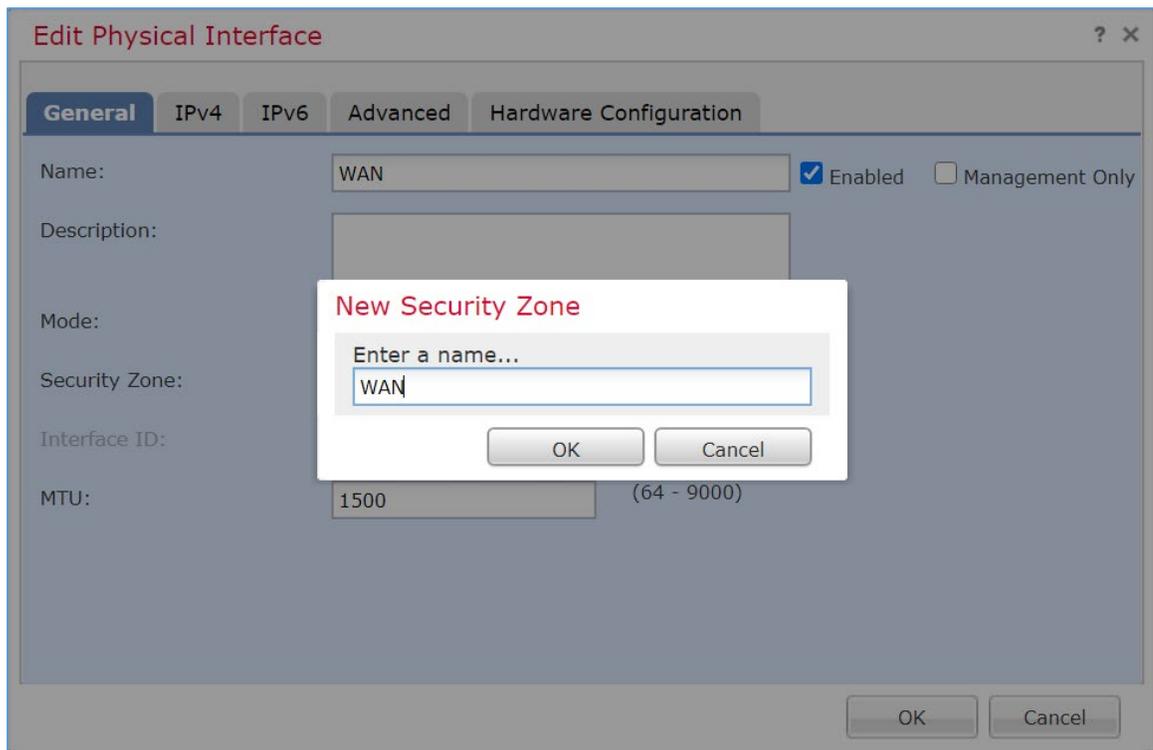
- 687 3. The Edit Physical Interface group box displays. Under the General tab, enter **WAN** in the **Name**
- 688 field.



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



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



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

The screenshot shows a configuration window titled "Edit Physical Interface". It has five tabs: "General", "IPv4", "IPv6", "Advanced", and "Hardware Configuration". The "General" tab is selected. The configuration fields are as follows:

- Name: WAN
- Description: (empty text box)
- Mode: None
- Security Zone: WAN
- Interface ID: GigabitEthernet0/0
- MTU: 1500 (with a range of 64 - 9000)

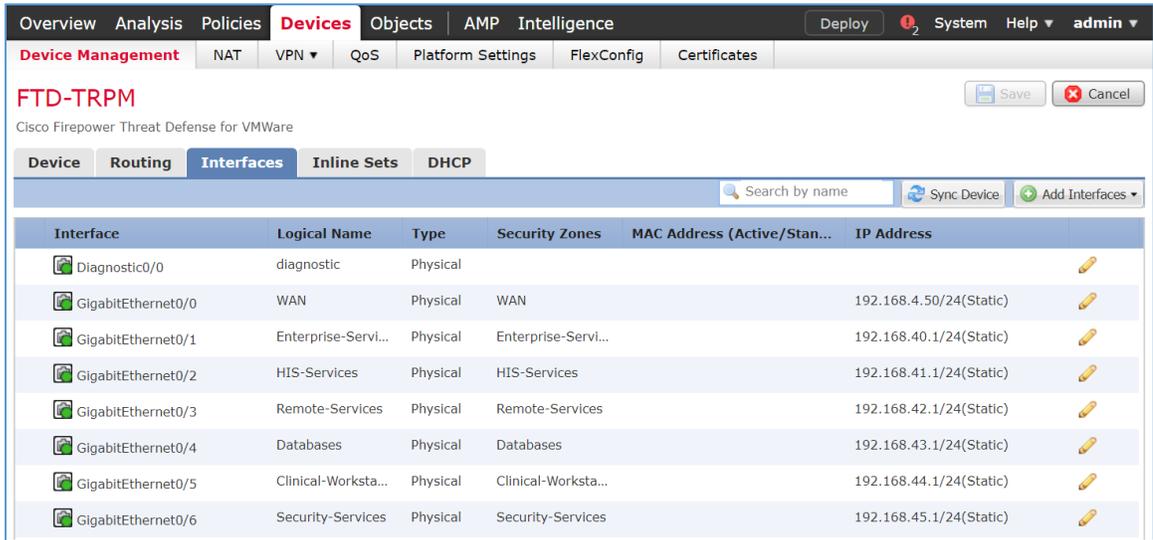
There are two checkboxes: "Enabled" (checked) and "Management Only" (unchecked). At the bottom right, there are "OK" and "Cancel" buttons.

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

The screenshot shows a configuration window titled "Edit Physical Interface" with a tabbed interface. The "IPv4" tab is selected. Under "IP Type", a dropdown menu is set to "Use Static IP". The "IP Address" field contains "192.168.4.50/24". To the right of this field, there is a note: "eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25". At the bottom right of the window are "OK" and "Cancel" buttons.

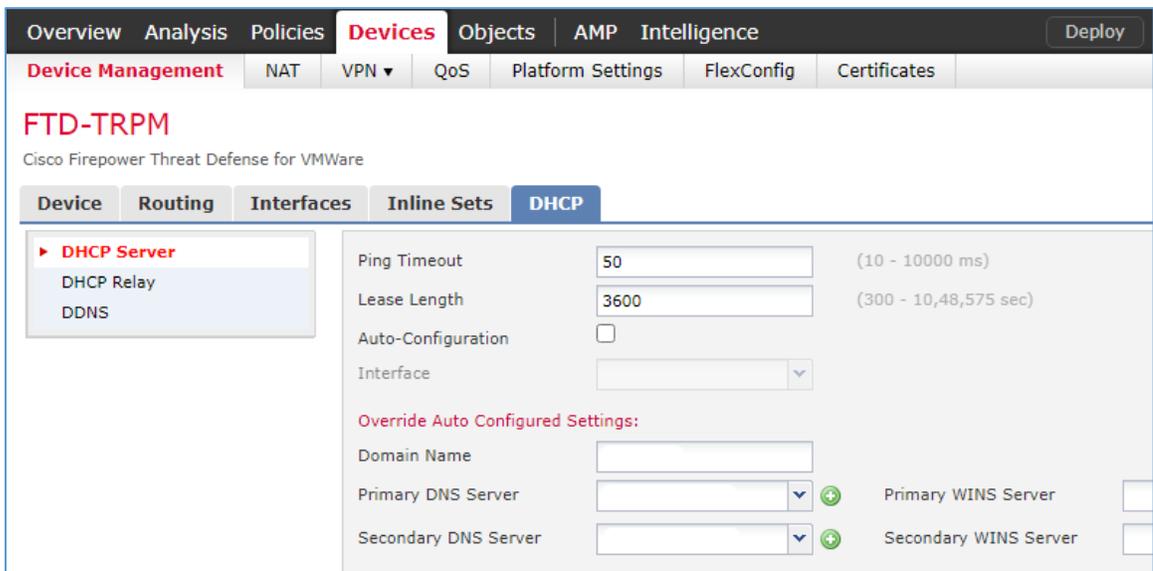
- 697 9. Configure each of the other GigabitEthernet interfaces following the same pattern described
698 above, populating the respective IP addresses that correspond to the appropriate VLAN. Values
699 for each VLAN are described below:
- 700 a. GigabitEthernet0/0 (VLAN 1316)
- 701 i. **Name:** WAN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

- 710 ii. **Security Zone:** HIS-Services
- 711 iii. **IP Address:** 192.168.41.1/24
- 712 d. GigabitEthernet0/3 (VLAN 1329)
 - 713 i. **Name:** Remote-Services
 - 714 ii. **Security Zone:** Remote-Services
 - 715 iii. **IP Address:** 192.168.42.1/24
- 716 e. GigabitEthernet0/4 (VLAN 1330)
 - 717 i. **Name:** Databases
 - 718 ii. **Security Zone:** Databases
 - 719 iii. **IP Address:** 192.168.43.1/24
- 720 f. GigabitEthernet0/5 (VLAN 1347)
 - 721 i. **Name:** Clinical-Workstations
 - 722 ii. **Security Zone:** Clinical-Workstations
 - 723 iii. **IP Address:** 192.168.44.1/24
- 724 g. GigabitEthernet0/6 (VLAN 1348)
 - 725 i. **Name:** Security-Services
 - 726 ii. **Security Zone:** Security-Services
 - 727 iii. **IP Address:** 192.168.45.1/24
- 728 10. Click **Save**.
- 729 11. Click **Deploy**. Verify that the interfaces have been configured properly. Selecting the Devices tab,
730 the Device Management screen displays the individual interfaces, assigned logical names, type
731 of interface, security zone labeling, and assigned IP address network that corresponds to the
732 VLANs that are assigned per security zone.



733 **Configure Cisco FTD DHCP**

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



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

739 4. Click **Save**.

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

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

- 742 a. **Name:** Umbrella-DNS-2
- 743 b. **Network (Host):** 192.168.40.31

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

745 8. Click **Add Server**.

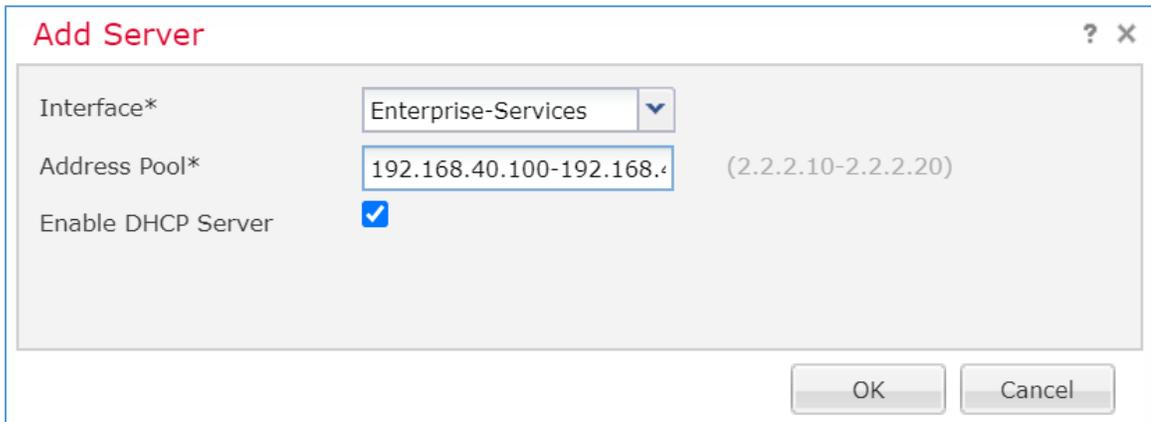
746 9. The Add Server pop-up window appears. Fill out the following information:

- 747 a. **Interface:** Enterprise-Services

748 b. **Address Pool:** 192.168.40.100-192.168.40.254

749 c. **Enable DHCP Server:** checked

750 10. Click **OK**.



751 11. Add additional servers by following the same pattern described above, populating the
 752 respective Interface and Address Pool, and check the **Enable DHCP Server** that corresponds to
 753 the appropriate server. Values for each server are described below:

754 a. **Interface:** Enterprise-Services

755 i. **Address Pool:** 192.168.40.100-192.168.40.254

756 ii. **Enable DHCP Server:** checked

757 b. **Interface:** HIS-Services

758 i. **Address Pool:** 192.168.41.100-192.168.41.254

759 ii. **Enable DHCP Server:** checked

760 c. **Interface:** Remote-Services

761 i. **Address Pool:** 192.168.42.100-192.168.42.254

762 ii. **Enable DHCP Server:** checked

763 d. **Interface:** Databases

764 i. **Address Pool:** 192.168.43.100-192.168.43.254

765 ii. **Enable DHCP Server:** checked

766 e. **Interface:** Clinical-Workstations

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

768 ii. **Enable DHCP Server:** checked

769 f. **Interface:** Security-Services

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

771 ii. **Enable DHCP Server:** checked

772 12. Click **Save**.

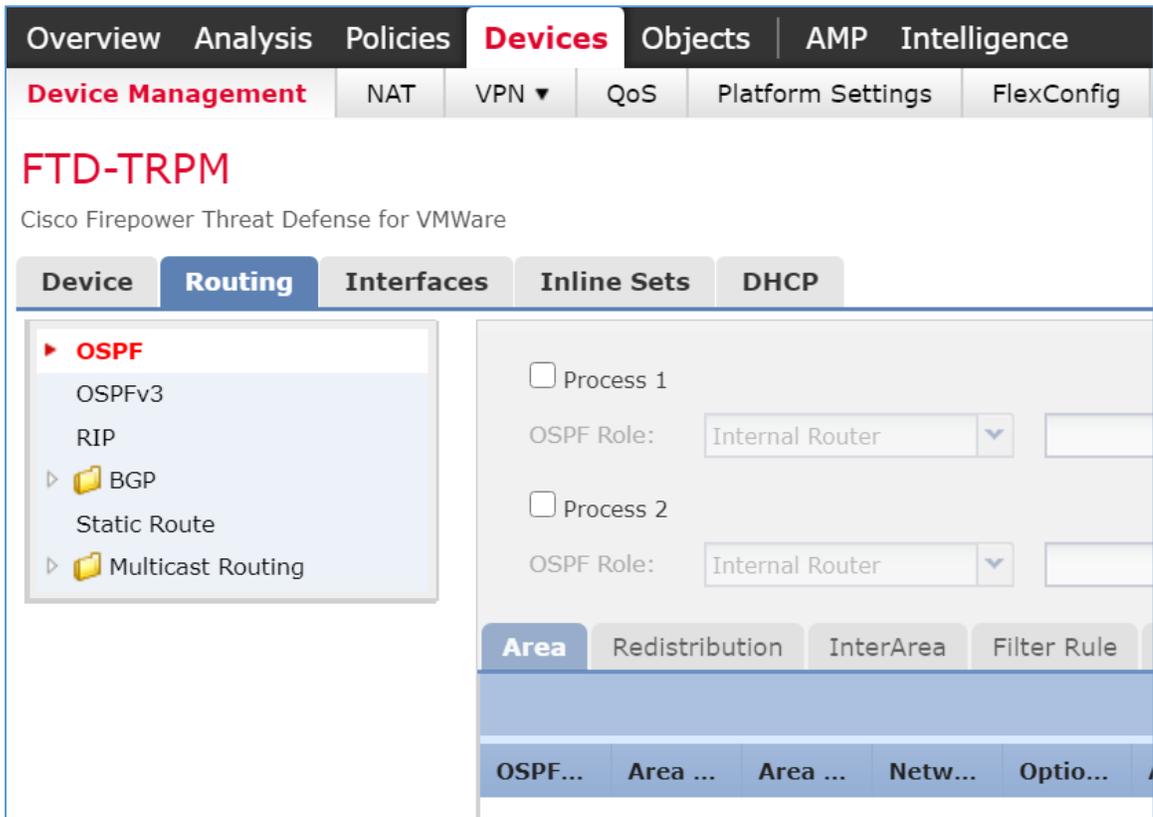
773 13. Click **Deploy**. Verify that the DHCP servers have been configured properly. Select the **Devices**
774 tab, and review the DHCP server configuration settings. Values for **Ping Timeout** and **Lease**
775 **Length** correspond to default values that were not altered. The **Domain Name** is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

The screenshot displays the Cisco FTD configuration page for FTD-TRPM, specifically the DHCP settings. The navigation bar includes Overview, Analysis, Policies, Devices (selected), Objects, AMP, and Intelligence. Below this, there are tabs for Device Management, NAT, VPN, QoS, Platform Settings, FlexConfig, and Certificates. The main heading is FTD-TRPM, with a sub-heading Cisco Firepower Threat Defense for VMWare. The configuration is organized into tabs: Device, Routing, Interfaces, Inline Sets, and DHCP (selected). On the left, a sidebar shows 'DHCP Server' (selected), DHCP Relay, and DDNS. The main configuration area includes fields for Ping Timeout (50), Lease Length (3600), Auto-Configuration (unchecked), and Interface. Under 'Override Auto Configured Settings', there are fields for Domain Name (hdo.trpm), Primary DNS Server (Umbrella-DNS-1), and Secondary DNS Server (Umbrella-DNS-2). Below these are checkboxes for Primary and Secondary WINS Servers. At the bottom, there are tabs for Server and Advanced. A table lists the following data:

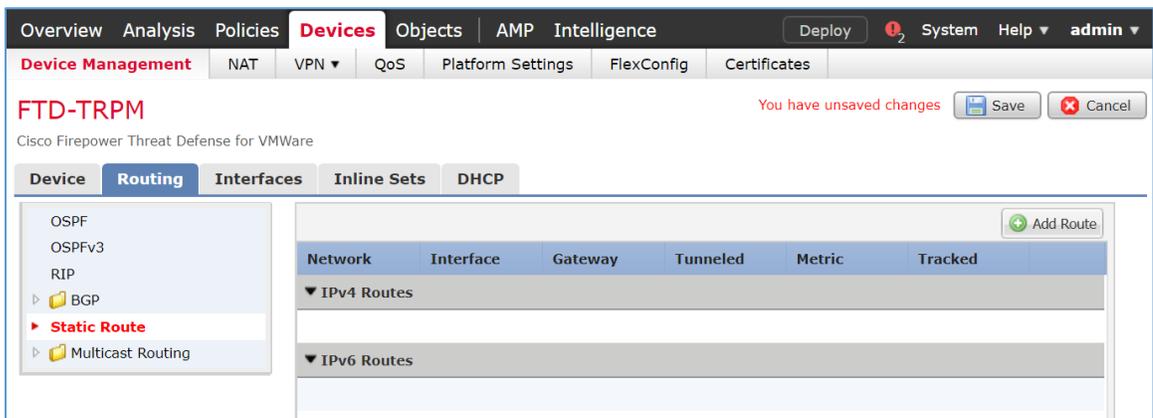
Interface	Address Pool	Enable DHCP Server
Enterprise-Services	192.168.40.100-192.168.40.254	✓
HIS-Services	192.168.41.100-192.168.41.254	✓
Remote-Services	192.168.42.100-192.168.42.254	✓
Databases	192.168.43.100-192.168.43.254	✓
Clinical-Workstations	192.168.44.100-192.168.44.254	✓

780 **Configure Cisco FTD Static Route**

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

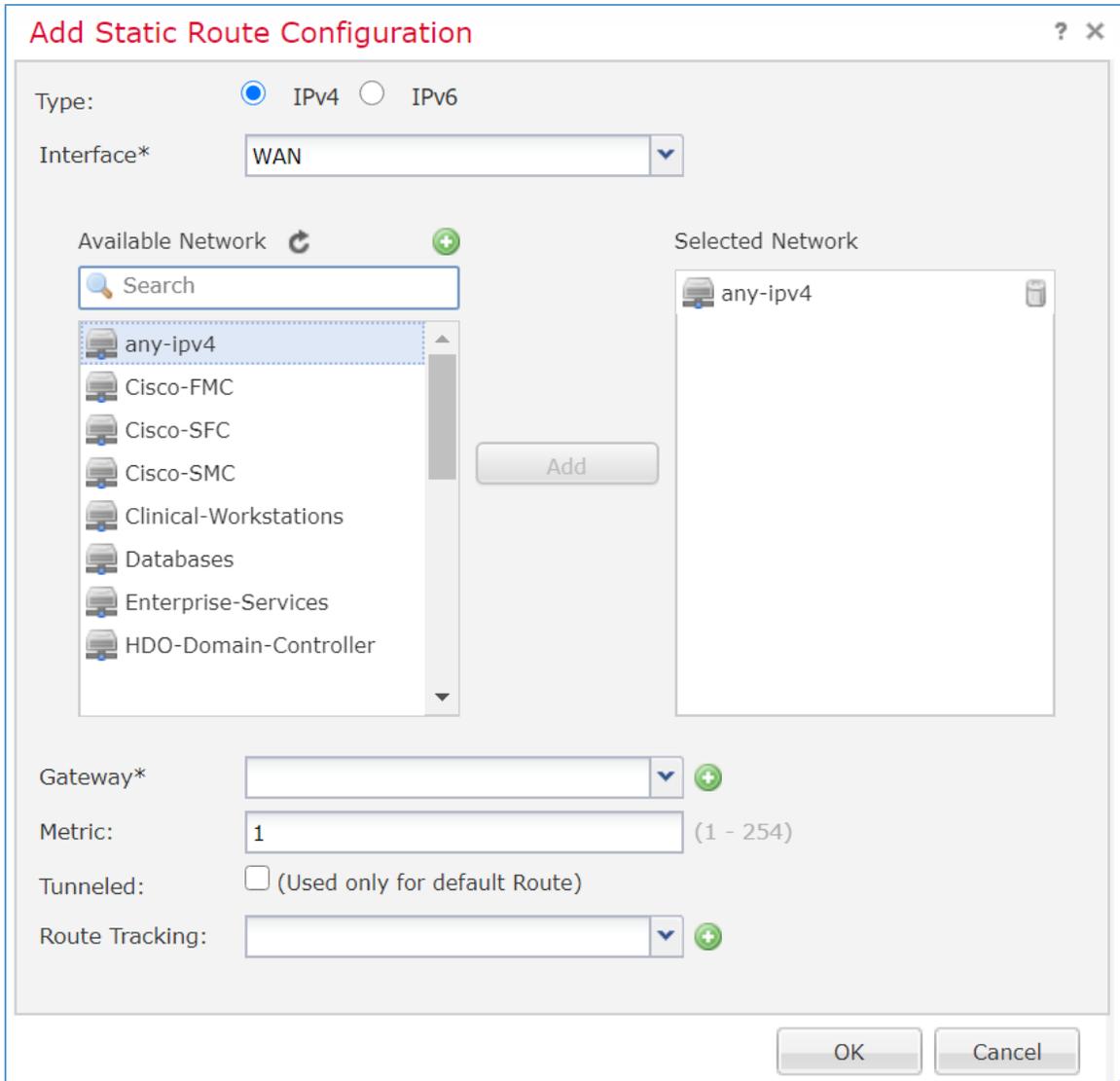


783 3. Click **Add Route**.



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

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



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

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

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

- 791 7. Click **Save**.

New Network Object ? x

Name: HDO-Upstream-Gateway

Description:

Network: Host Range Network FQDN

192.168.4.1

Allow Overrides:

Save Cancel

792 8. Click **OK**.

Add Static Route Configuration

Type: IPv4 IPv6

Interface*

Available Network

- any-ipv4
- Cisco-FMC
- Cisco-SFC
- Cisco-SMC
- Clinical-Workstations
- Databases
- Enterprise-Services
- HDO-Domain-Controller
- HDO-Upstream-Gateway

Selected Network

- any-ipv4

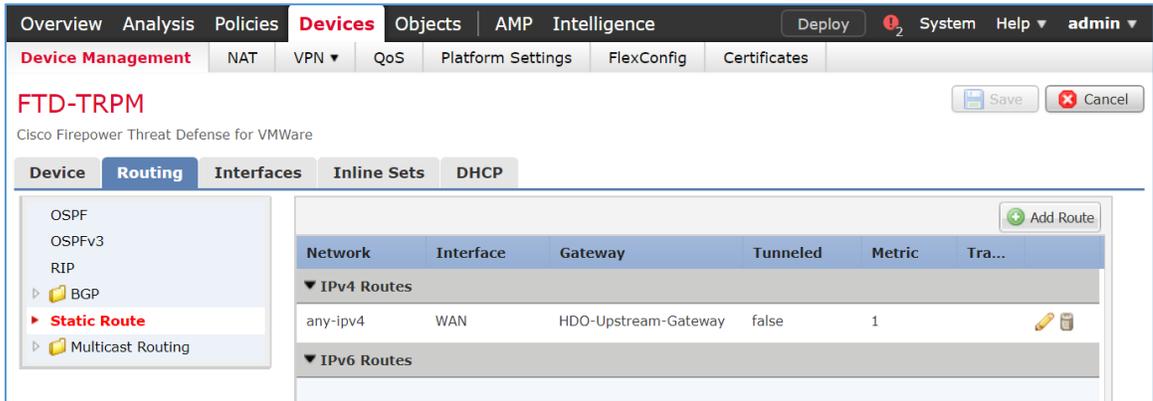
Gateway*

Metric: (1 - 254)

Tunneled: (Used only for default Route)

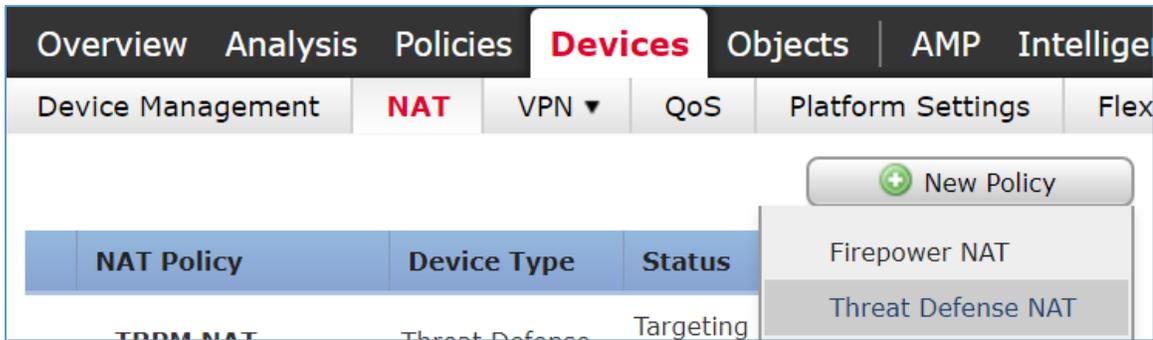
Route Tracking:

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

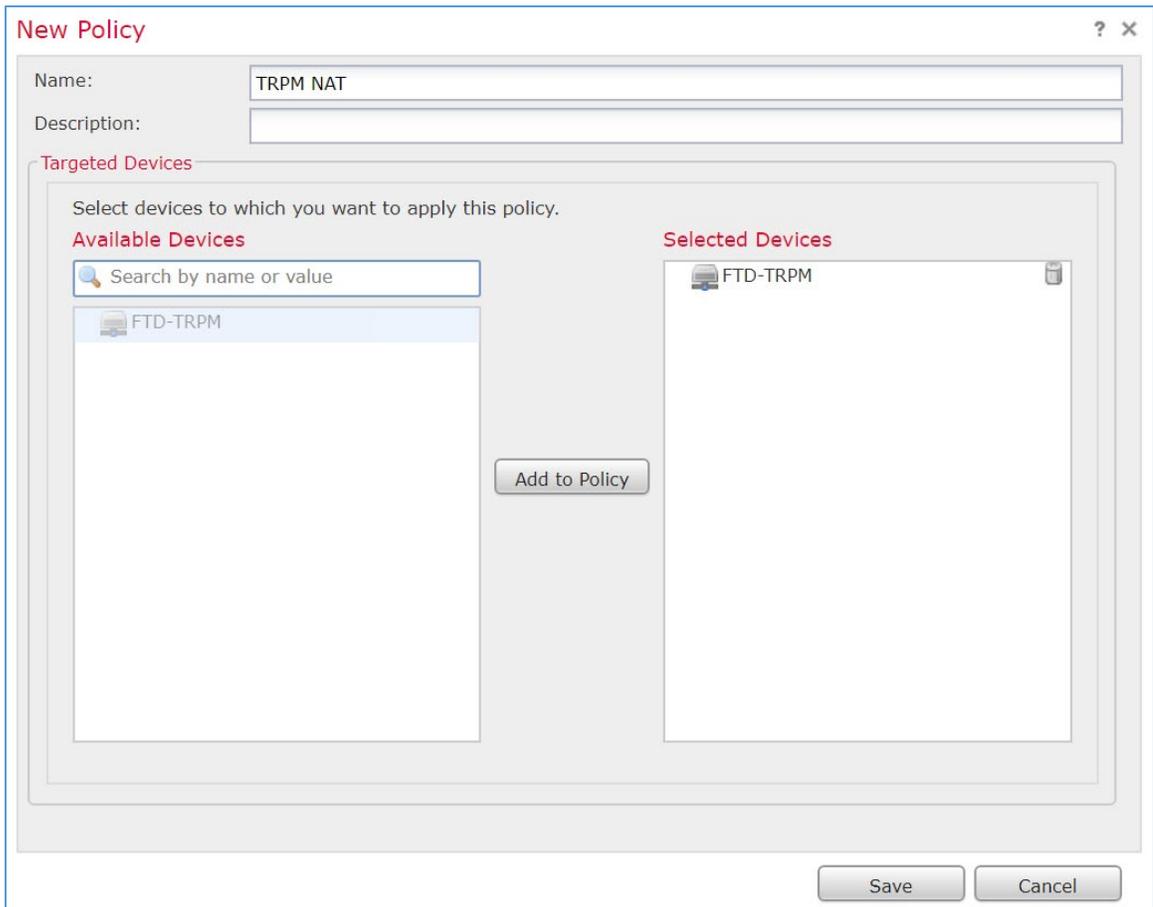


800 **Configure Cisco FTD Network Address Translation (NAT)**

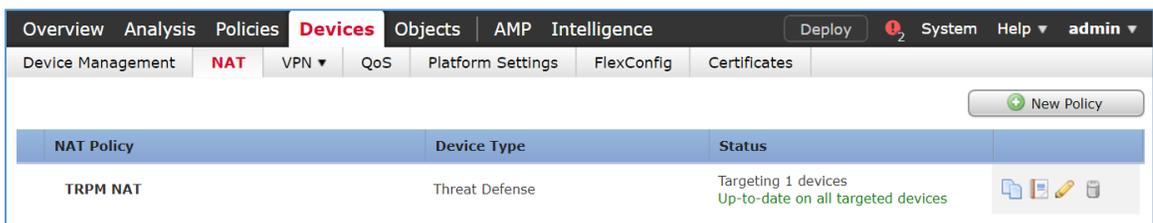
- 801 1. Click **Devices > NAT**.
- 802 2. Click **New Policy > Threat Defense NAT**.



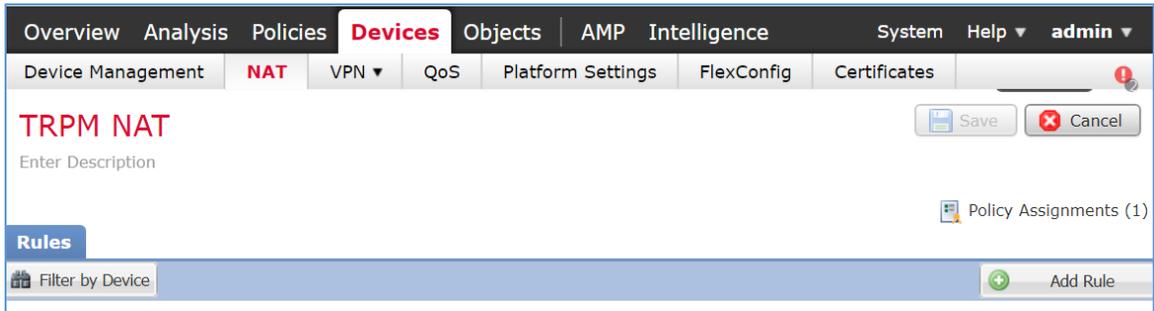
- 803 3. The New Policy pop-up window appears. Fill out the following information:
 - 804 a. **Name:** TRPM NAT
 - 805 b. **Selected Devices:** FTD-TRPM
- 806 4. Click **Save**.



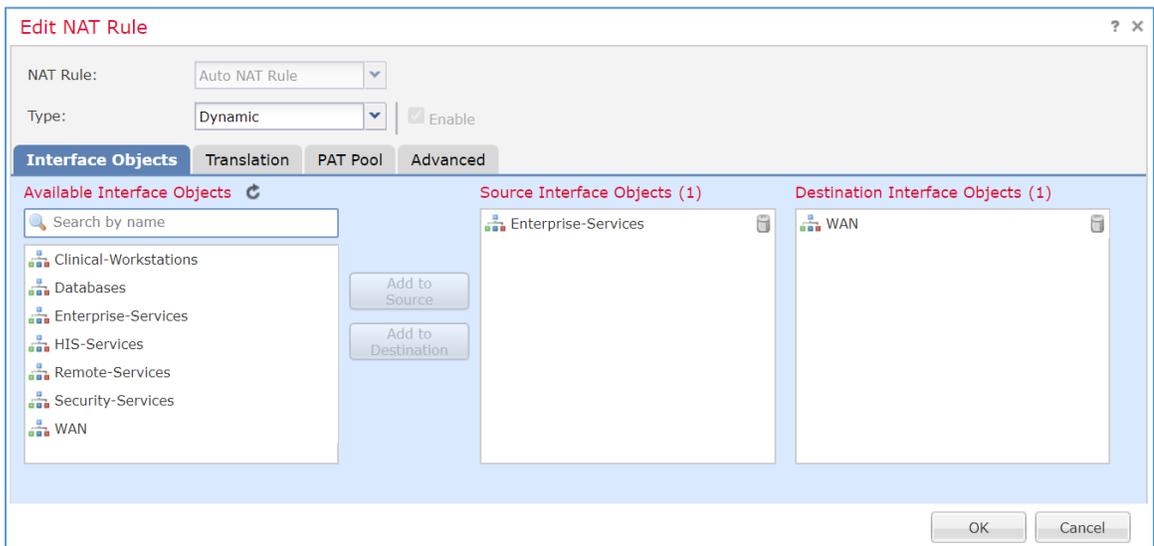
807 5. Click the **edit symbol** for **TRPM NAT**.



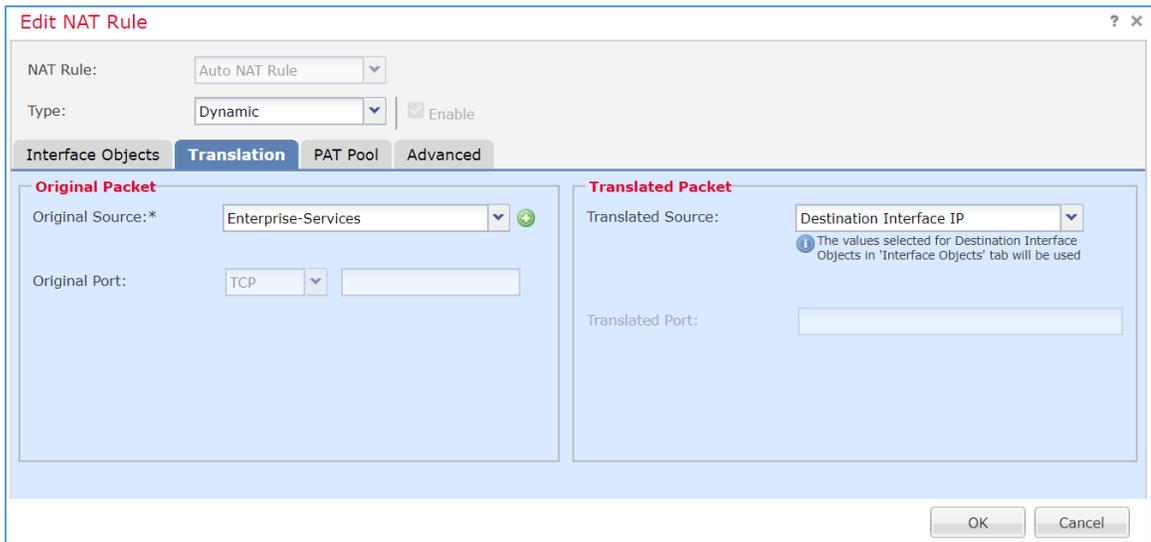
808 6. Click **Add Rule**.



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



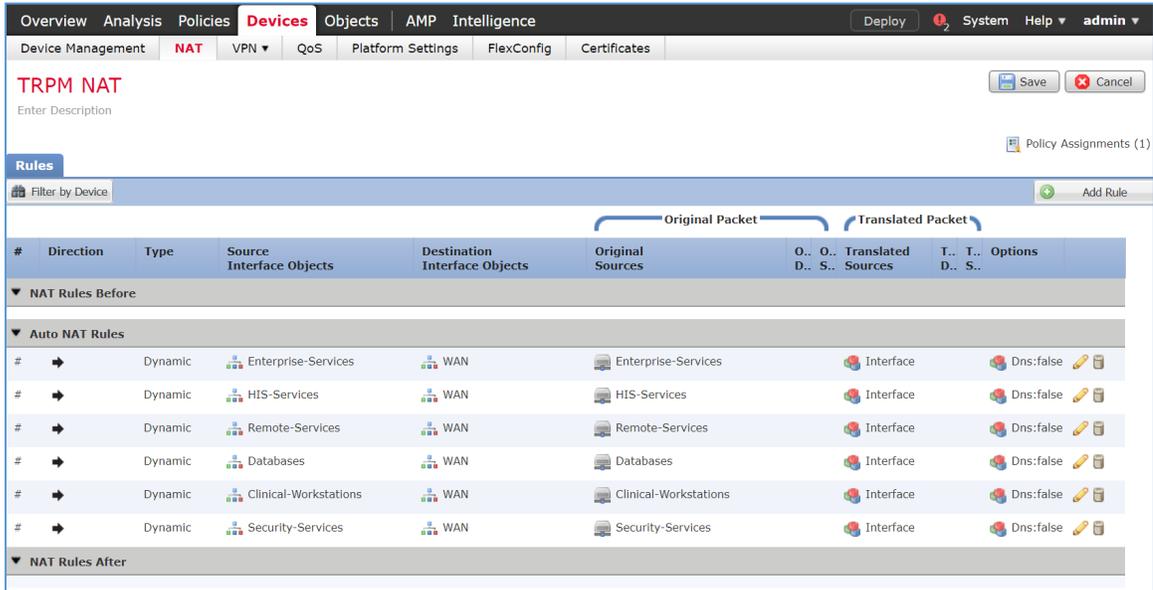
- 816 9. Under **Translation**, fill out the following information:
- 817 a. **Original Source:** Enterprise-Services
- 818 b. **Translated Source:** Destination Interface IP
- 819 10. Click **OK**.



- 820 11. Create additional rules following the same pattern described above, populating the respective
 821 information for each rule. Values for each rule are described below:
- 822 a. HIS-Services
 - 823 i. **NAT Rule:** Auto NAT Rule
 - 824 ii. **Type:** Dynamic
 - 825 iii. **Source Interface Objects:** HIS-Services
 - 826 iv. **Destination Interface Objects:** WAN
 - 827 v. **Original Source:** HIS-Services
 - 828 vi. **Translated Source:** Destination Interface IP
 - 829 b. Remote-Services
 - 830 i. **NAT Rule:** Auto NAT Rule
 - 831 ii. **Type:** Dynamic
 - 832 iii. **Source Interface Objects:** Remote-Services
 - 833 iv. **Destination Interface Objects:** WAN
 - 834 v. **Original Source:** Remote-Services
 - 835 vi. **Translated Source:** Destination Interface IP

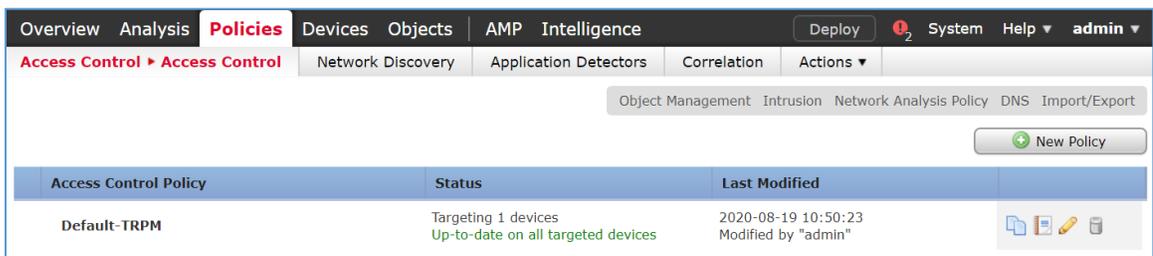
- 836 c. Databases
- 837 i. **NAT Rule:** Auto NAT Rule
- 838 ii. **Type:** Dynamic
- 839 iii. **Source Interface Objects:** Databases
- 840 iv. **Destination Interface Objects:** WAN
- 841 v. **Original Source:** Databases
- 842 vi. **Translated Source:** Destination Interface IP
- 843 d. Clinical-Workstations
- 844 i. **NAT Rule:** Auto NAT Rule
- 845 ii. **Type:** Dynamic
- 846 iii. **Source Interface Objects:** Clinical-Workstations
- 847 iv. **Destination Interface Objects:** WAN
- 848 v. **Original Source:** Clinical-Workstations
- 849 vi. **Translated Source:** Destination Interface IP
- 850 e. Security-Services
- 851 i. **NAT Rule:** Auto NAT Rule
- 852 ii. **Type:** Dynamic
- 853 iii. **Source Interface Objects:** Security-Services
- 854 iv. **Destination Interface Objects:** WAN
- 855 v. **Original Source:** Security-Services
- 856 vi. **Translated Source:** Destination Interface IP
- 857 12. Click **Save**.
- 858 13. Click **Deploy**. Verify the NAT settings through the **Devices** screen. The **NAT** rules are displayed in
- 859 a table format. The table includes values for **Direction** of the NAT displayed as a directional
- 860 arrow, the **NAT Type**, the **Source Interface Objects** (i.e., the security zone IP networks), the
- 861 **Destination Interface Objects**, the **Original Sources** (i.e., these addresses correspond to the IP
- 862 network from where the network traffic originates), the **Translated Sources**, and **Options**. The

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

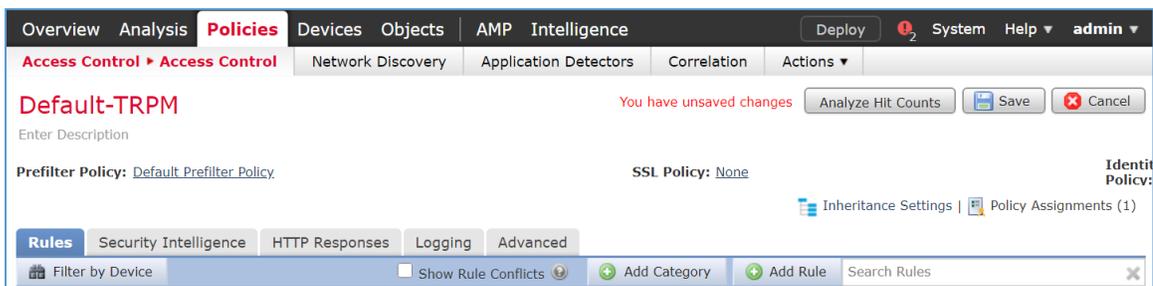


865 **Configure Cisco FTD Access Control Policy**

- 866 1. Click **Policies > Access Control > Access Control**.
- 867 2. Click the **edit** symbol for **Default-TRPM**.



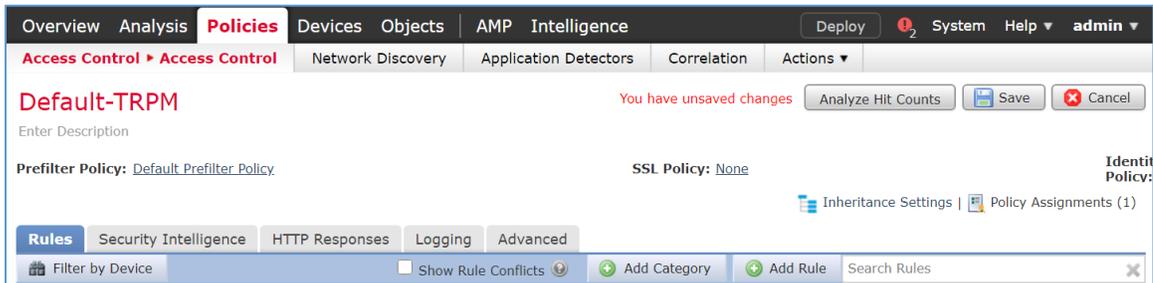
- 868 3. Click **Add Category**.



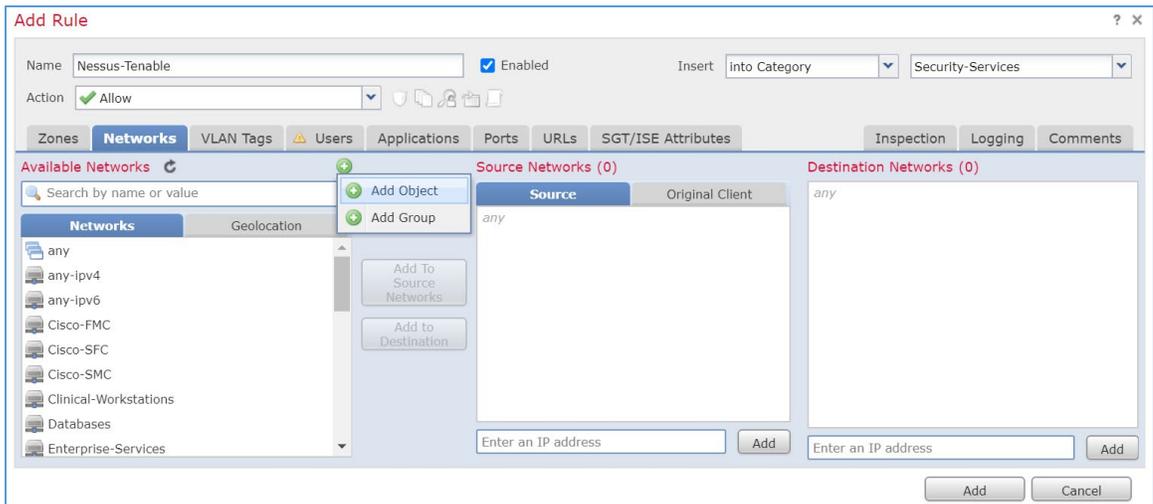
- 869 4. Fill out the following information:
- 870 a. **Name:** Security Services
- 871 b. **Insert:** into Mandatory
- 872 5. Click **OK**.

The screenshot shows a dialog box titled "Add Category" with a close button (X) in the top right corner. Inside the dialog, there are two input fields: "Name:" with the text "Security-Services" and "Insert:" with a dropdown menu showing "into Mandatory". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

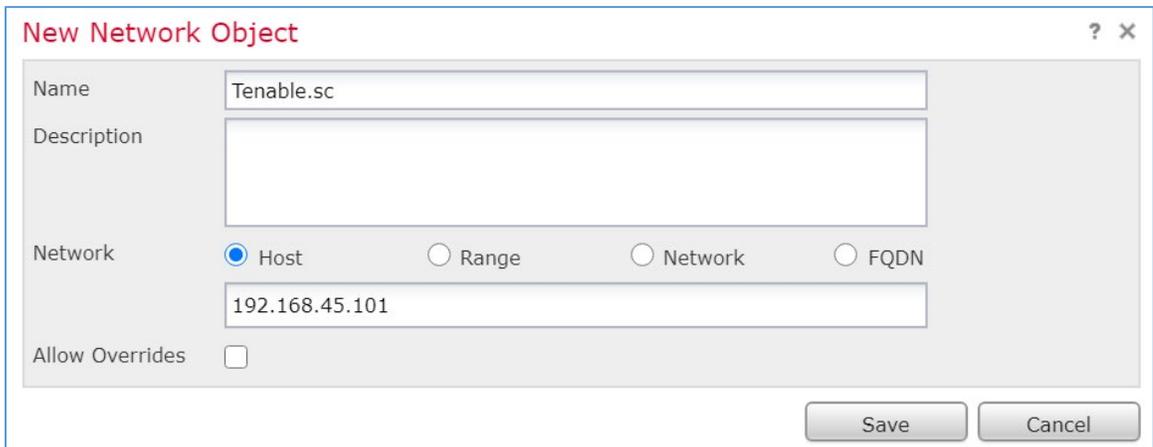
- 873 6. Repeat the previous steps of **Add Category** section for each network segment in the
- 874 architecture.
- 875 7. Click **Add Rule**.



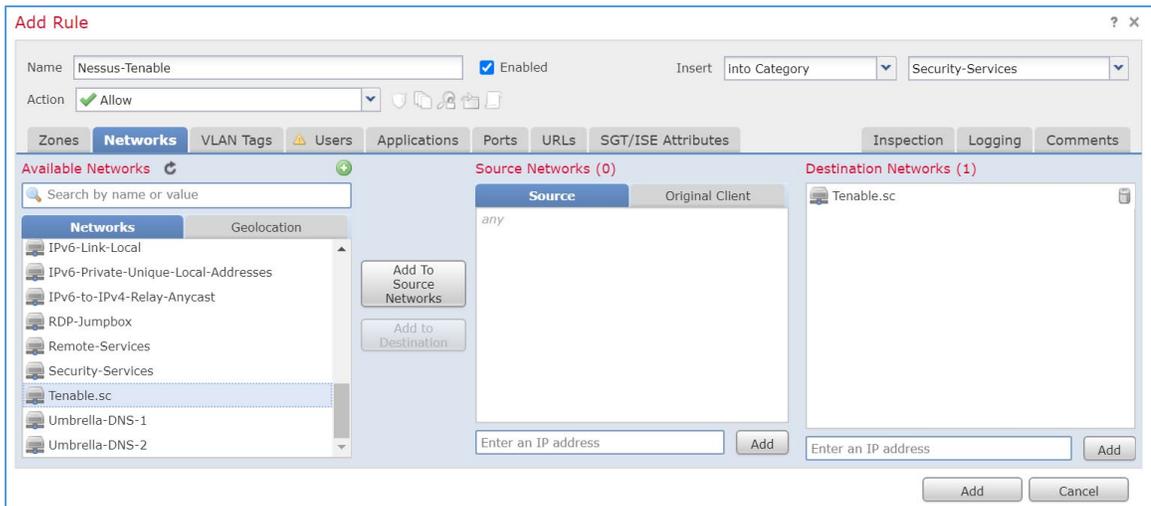
- 876 8. When the Add Rule screen appears, fill out the following information:
- 877 a. **Name:** Nessus-Tenable
- 878 b. **Action:** Allow
- 879 c. **Insert:** into Category, Security Services
- 880 d. Under **Networks**, click the **plus symbol** next to **Available Networks**, and select **Add**
-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



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

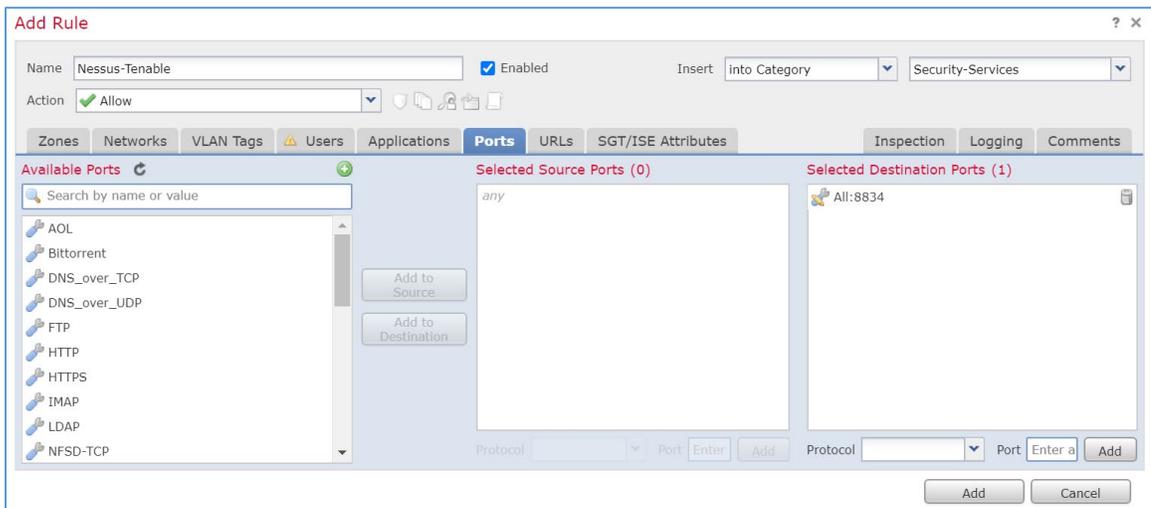


- 886 11. In the Add Rule screen, under the **Networks** tab, set **Destination Networks** to **Tenable.sc**.
- 887 12. Click **Ports**.



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

889 14. Click **Add**.



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

891 16. Click **Save**.

892 17. Click **Deploy**.

893 2.2.3 Security Continuous Monitoring

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

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

898 *2.2.3.1 Cisco Stealthwatch*

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

902 **Cisco Stealthwatch Management Center (SMC) Appliance Information**

903 **CPU:** 4

904 **RAM:** 16 GB

905 **Storage:** 200 GB (Thick Provision)

906 **Network Adapter 1:** VLAN 1348

907 **Operating System:** Linux

908 **Cisco SMC Appliance Installation Guide**

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

911 **Cisco SFC Appliance Information**

912 **CPU:** 4

913 **RAM:** 16 GB

914 **Storage:** 300 GB (Thick Provision)

915 **Network Adapter 1:** VLAN 1348

916 **Operating System:** Linux

917 **Cisco SFC Appliance Installation Guide**

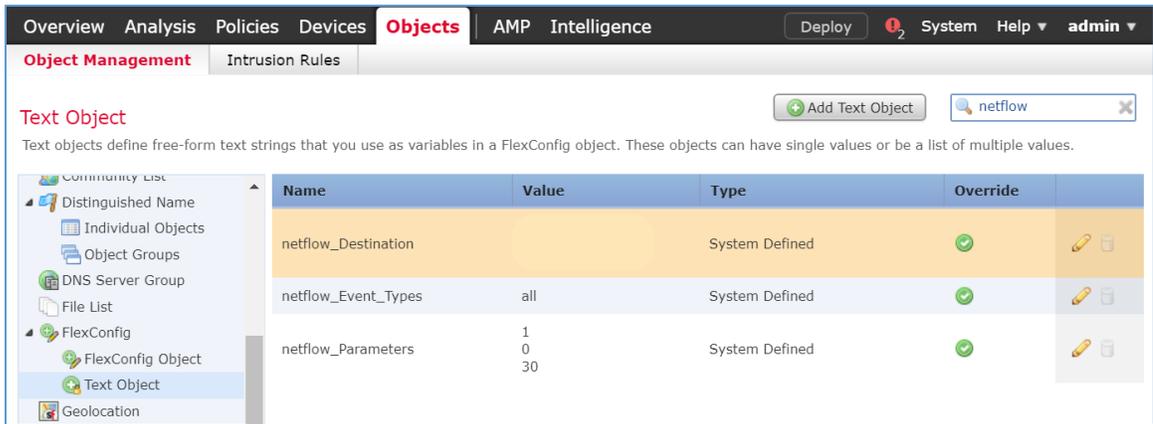
918 Install the appliance according to the instructions detailed in the *Cisco Stealthwatch Installation and*
919 *Configuration Guide 7.1* [8].

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

921 **Configure Cisco FTD NetFlow for Cisco SFC**

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

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



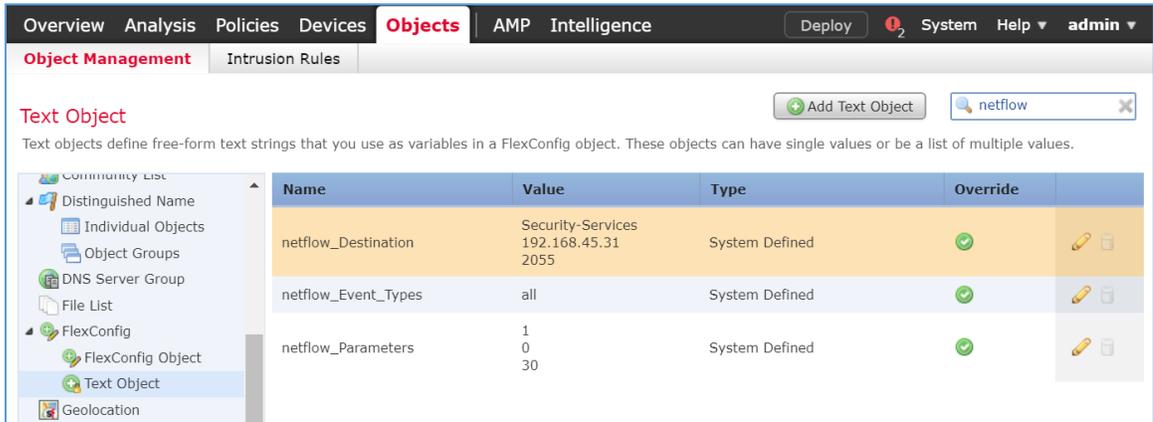
- 925 4. When the Edit Text Object pop-up window appears, fill out the following information:
 - 926 a. **Count: 3**
 - 927 b. **1: Security Services**
 - 928 c. **2: 192.168.45.31**
 - 929 d. **3: 2055**
 - 930 e. **Allow Overrides: checked**
- 931 5. Click **Save**.

The screenshot shows a dialog box titled "Edit Text Object" with a red title bar. It contains the following fields and controls:

- Name:** A text input field containing "netflow_Destination".
- Description:** A text area containing the text: "This variable defines a single NetFlow export destination. 1. interface 2. destination 3. port <1-65535> UDP port number".
- Variable Type:** A dropdown menu set to "Multiple".
- Count:** A numeric spinner box set to "3".
- Table:** A table with 3 rows and 2 columns. The first row is highlighted in blue. The data is as follows:

1	Security-Services
2	192.168.45.31
3	2055
- Allow Overrides:** A checkbox that is checked.
- Override (0):** A dropdown menu showing "Override (0)".
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

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



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

Edit Text Object ? X

Name:

Description:

Variable Type: Count:

1	all
---	-----

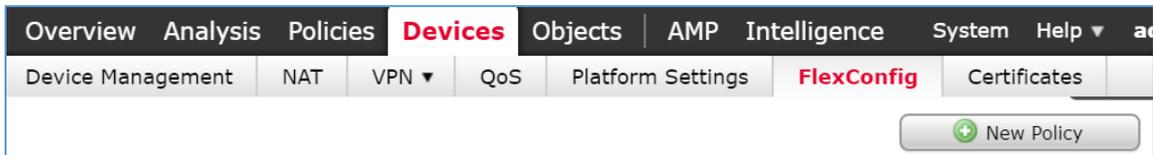
Allow Overrides:

Override (0)

Save Cancel

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

939 10. Click **New Policy**.

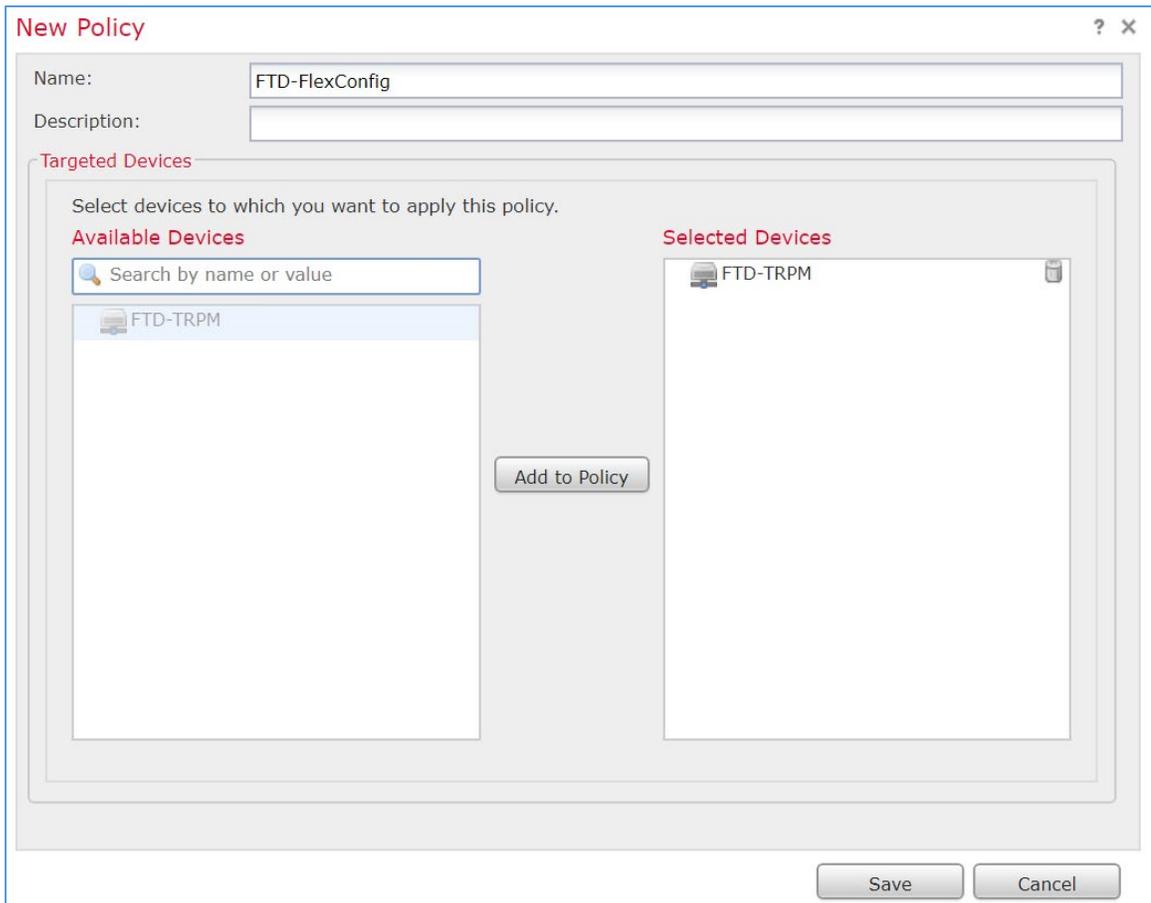


940 11. When the New Policy screen appears, fill out the following information:

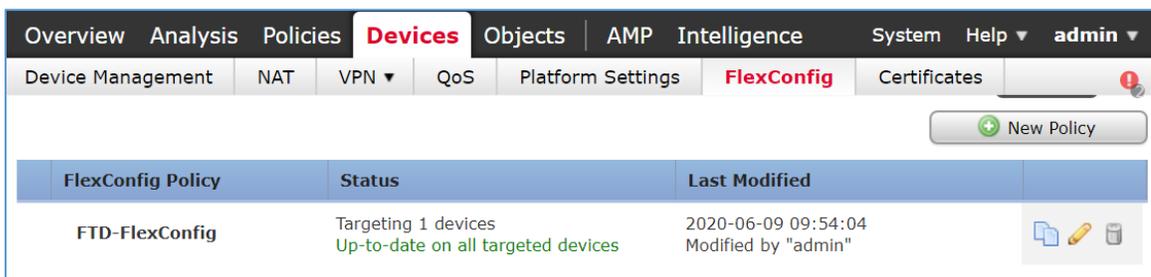
941 a. **Name:** FTD-FlexConfig

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

943 12. Click **Save**.

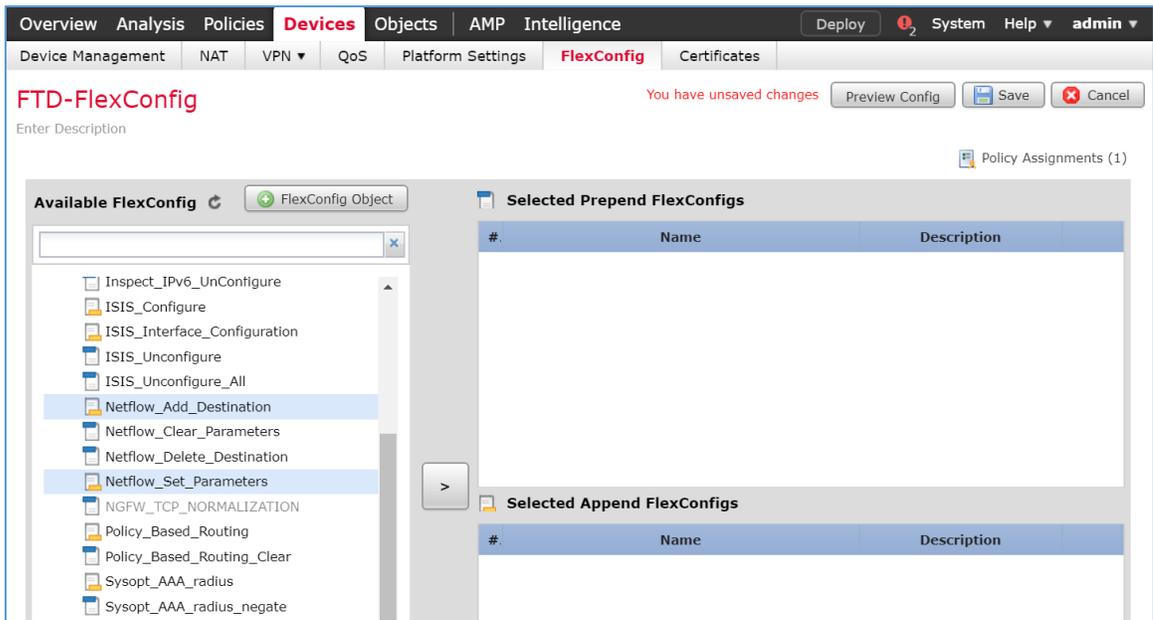


944 13. Click the **edit symbol** for **FTD-FlexConfig**.

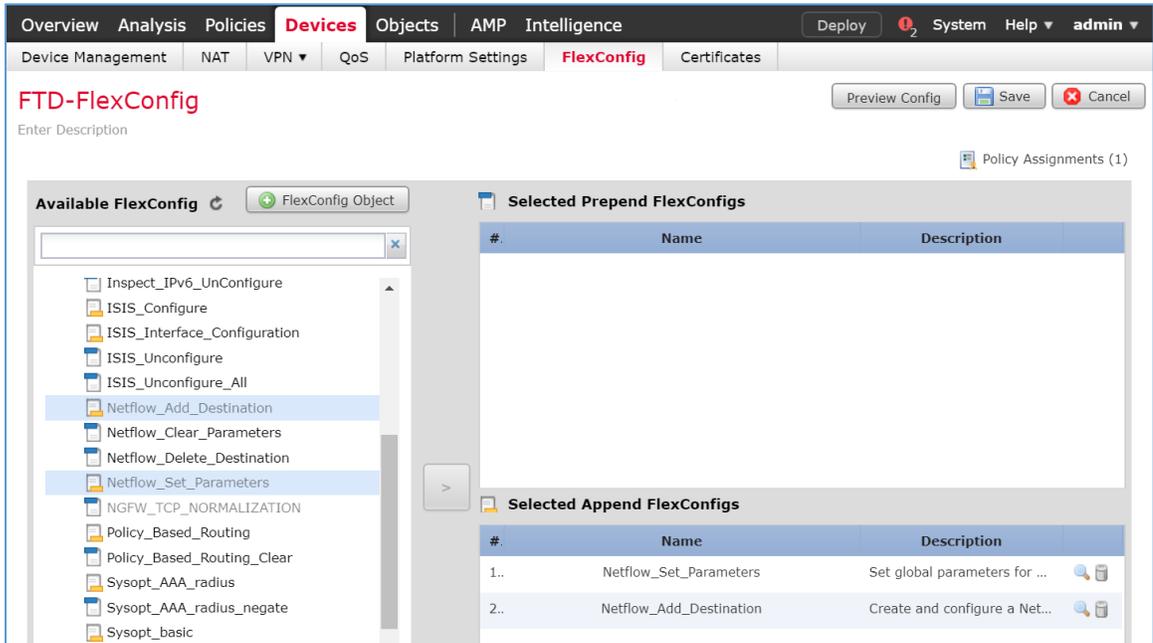


945 14. Under the **Devices** tab, select **Netflow_Add_Destination** and **Netflow_Set_Parameters**.

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

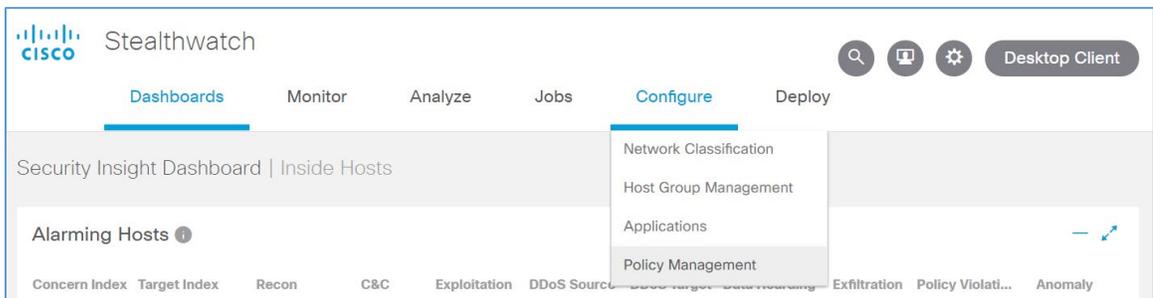


- 948 16. Click **Save**.
- 949 17. Click **Deploy**. From the **Devices** screen, verify the **FlexConfig** settings. Select the **FlexConfig** tab.
- 950 The **NetFlow** configurations appear in the lower right of the screen as a table. Under **Selected**
- 951 **Append FlexConfigs**, the table includes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

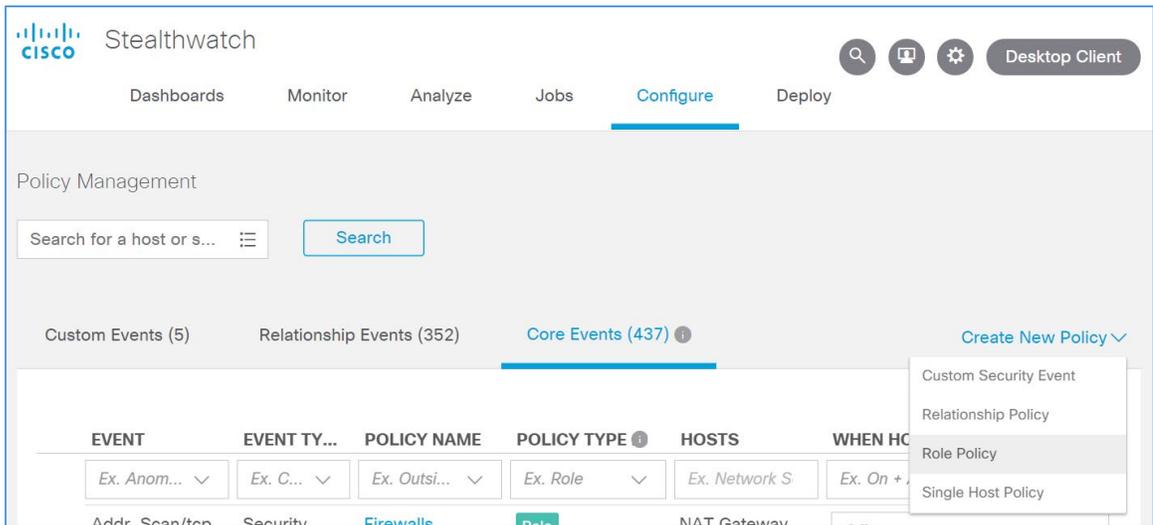


953 **Create a Custom Policy Management Rule**

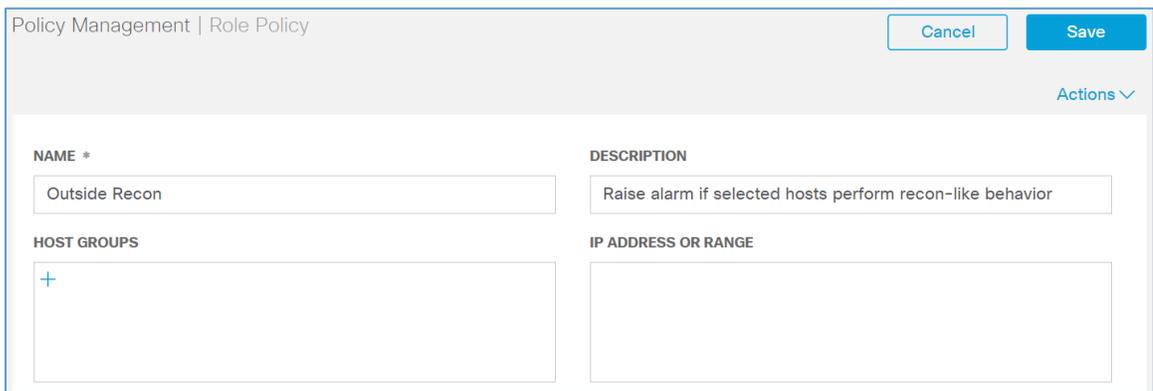
- 954 1. Click **Configure > Policy Management**.



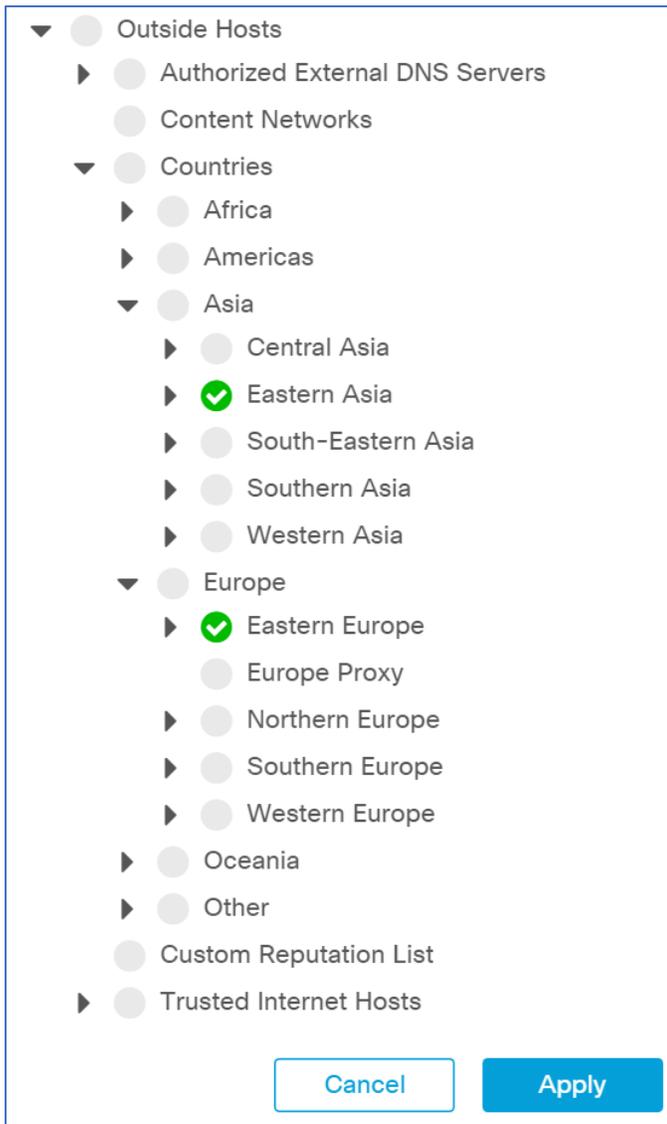
- 955 2. Click **Create New Policy > Role Policy**.



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



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



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

Policy Management | Role Policy Cancel Save Actions

NAME * Outside Recon	DESCRIPTION Raise alarm if selected hosts perform recon-like behavior
HOST GROUPS + Eastern Asia × Eastern Europe ×	IP ADDRESS OR RANGE

Core Events (0) Select Events

You must select at least one event before saving this policy. [Click here to select events.](#)

- 961 8. Select **Recon.**
- 962 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

Cancel
Apply

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

Core Events (1)
Select Events

EVENT	EVENT TYPE	WHEN HOST IS SOURCE	WHEN HOST IS TARGET	ACTIONS
<i>Ex. Anomaly</i> ▼	<i>Ex. Category</i> ▼	<i>Ex. On + Alarm</i> ▼	<i>Ex. On + Alarm</i> ▼	
▶ Recon	Category	<div style="border: 1px solid #0070C0; padding: 2px;"> Off ▼ Off On On + Alarm </div>	NA	Delete

50 ▼ items per page
1 / 1

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

Core Events (1) Select Events

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 / 100

Never trigger alarm when less than: points in 24 hours

Always trigger alarm when greater than: points in 24 hours

966 13. Click **Save**.

Policy Management | Role Policy Cancel Save

Actions ▼

NAME *	DESCRIPTION
Outside Recon	Raise alarm if selected hosts perform recon-like behavior
HOST GROUPS	IP ADDRESS OR RANGE
+ Eastern Europe × Eastern Asia ×	

Core Events (1) Select Events

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

967 [2.2.3.2 Cisco Umbrella](#)

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

971 **Cisco Umbrella Forwarder Appliance Information**972 **CPU:** 1973 **RAM:** 0.5 GB974 **Storage:** 6.5 GB (Thick Provision)975 **Network Adapter 1:** VLAN 1327976 **Operating System:** Linux977 **Cisco Umbrella Forwarder Appliance Installation Guide**978 Install the appliance according to the instructions detailed in Cisco's Deploy VAs in VMware guidance [\[9\]](#).979 **Create an Umbrella Site**

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

Deployments / Configuration
 Sites and Active Directory

Settings Add DC Download

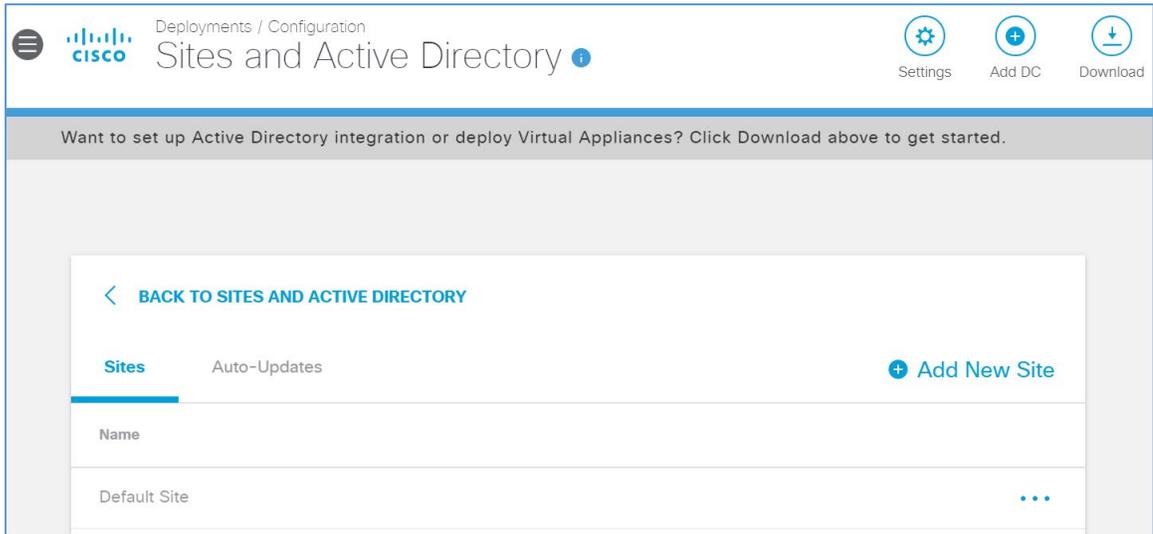
Want to set up Active Directory integration or deploy Virtual Appliances? Click Download above to get started.

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

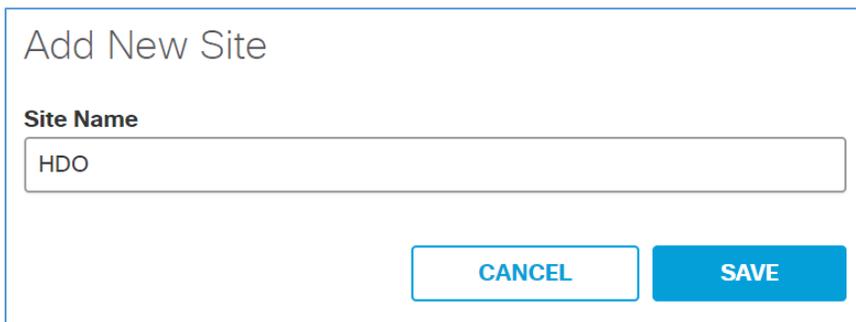
Page: 1 Results Per Page: 10 1-2 of 2 < >

- 982 3. Click
- Add New Site**
- .



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

984 5. Click **Save**.

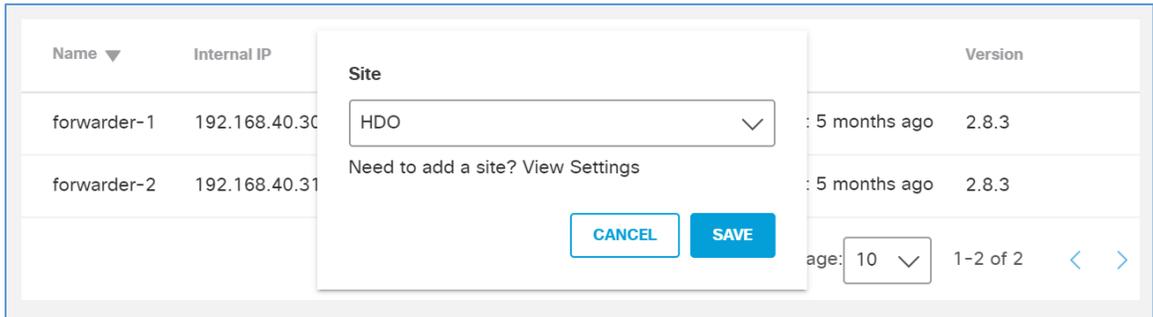


985 6. Click **Deployments > Configuration > Sites and Active Directory**.

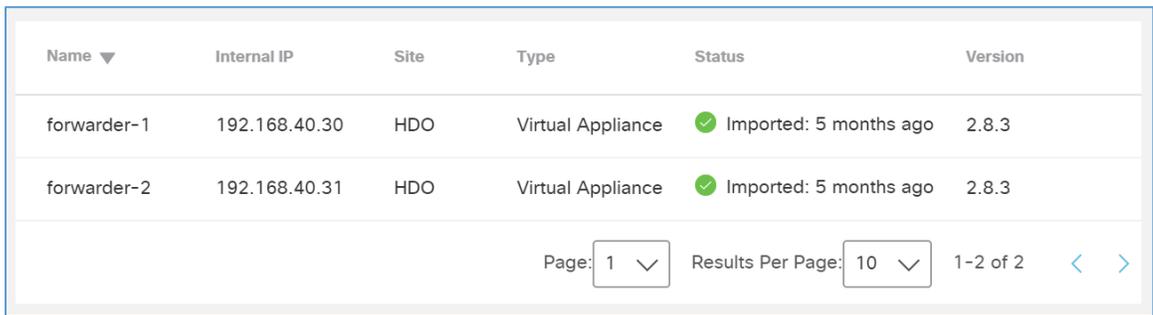
986 7. Click the **edit symbol** for the Site of **forwarder-1**.

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

988 9. Click **Save**.

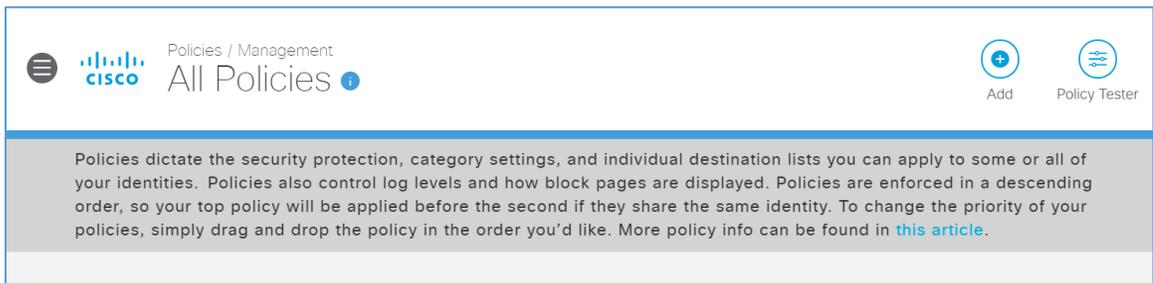


989 10. Repeat the previous steps for **forwarder-2**.



990 **Configure an Umbrella Policy**

- 991 1. Click **Policies > Management > All Policies**.
- 992 2. Click **Add**.



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

What would you like to protect?

Select Identities

All Identities

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

0 Selected

CANCEL NEXT

994 4. Select **HDO**.

995 5. Click **Next**.

What would you like to protect?

Select Identities

All Identities / Sites

<input checked="" type="checkbox"/>	HDO	0 >
<input type="checkbox"/>	Default Site	0 >

1 Selected REMOVE ALL

HDO 0

CANCEL NEXT

996 6. Click **Next**.

What should this policy do?

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

- Enforce Security at the DNS Layer**
Ensure domains are blocked when they host malware, command and control, phishing, and more.
- Inspect Files**
Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.
- Limit Content Access**
Block or allow sites based on their content, such as file sharing, gambling, or blogging.
- Control Applications**
Block or allow applications and application groups for identities using this policy.
- Apply Destination Lists**
Lists of destinations that can be explicitly blocked or allowed for any identities using this policy.

▶ [Advanced Settings](#)

CANCEL PREVIOUS NEXT

997 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 ▾

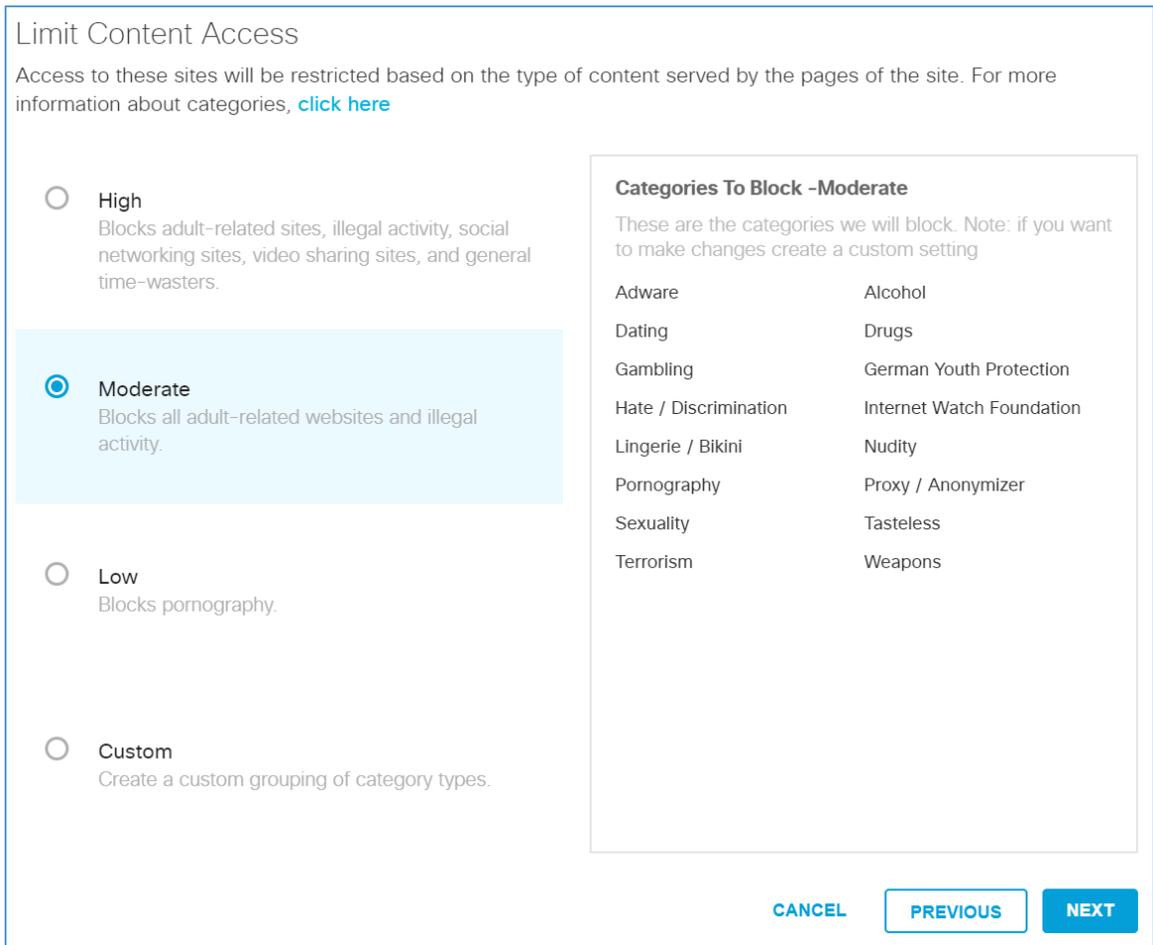
Categories To Block EDIT

- **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.

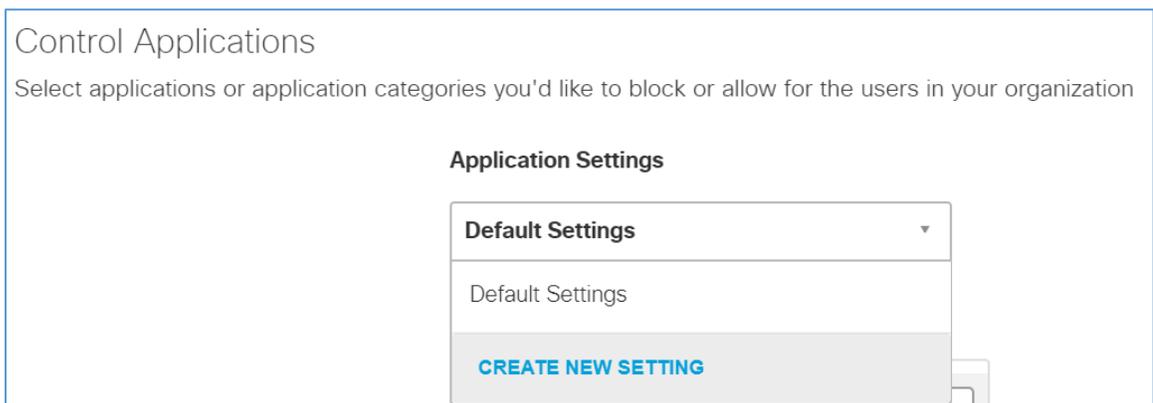
CANCEL
PREVIOUS
NEXT

998 8. Select **Moderate**.

999 9. Click **Next**.



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



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

- 1002 a. **Name:** HDO Application Control
- 1003 b. **Applications to Control:** Cloud Storage
- 1004 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

Applications To Control

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

CANCEL **SAVE**

- 1005 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

CANCEL PREVIOUS NEXT

1006 14. Click **Next**.

Apply Destination Lists [ADD NEW LIST](#)

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

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Global Allow List	0 >
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Global Block List	0 >

1 Allow Lists Applied

<input checked="" type="checkbox"/>	Global Allow List	0
-------------------------------------	-------------------	---

1 Block Lists Applied

<input checked="" type="checkbox"/>	Global Block List	0
-------------------------------------	-------------------	---

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

1007 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).

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

1008 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

▸ [BYPASS USERS](#) _____

▸ [BYPASS CODES](#) _____

[CANCEL](#) [PREVIOUS](#) [NEXT](#)

1009 17. In the Policy Summary screen, set the **Name** to **HDO Site Policy**.

1010 18. Click **Save**.

Policy Summary

Policy Name

HDO Site Policy

 **1 Identity Affected**
1 Site
[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](#)

 **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](#)

 **2 Destination Lists Enforced**
1 Block List
1 Allow List
[Edit](#)

 **File Analysis Enabled**
File Inspection Enabled
[Edit](#)

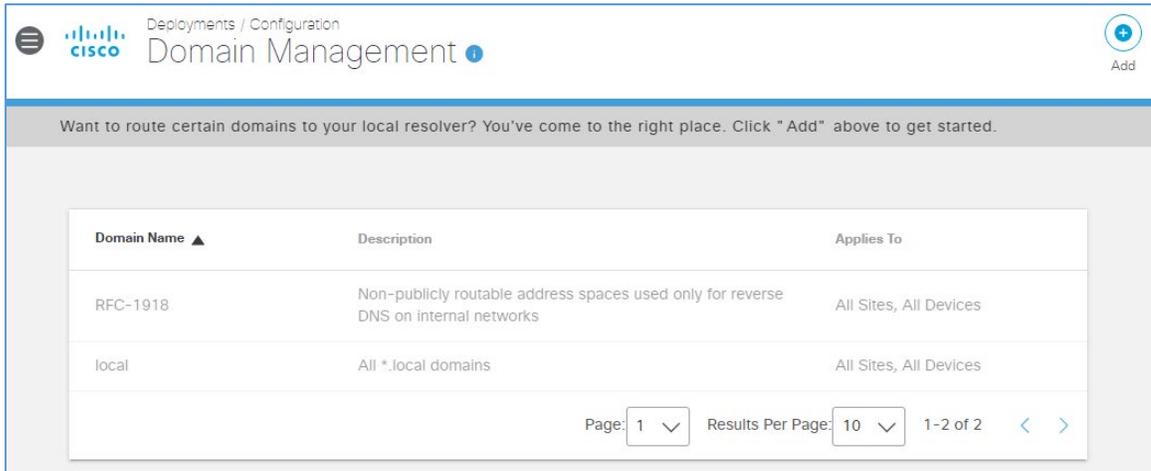
 **Umbrella Default Block Page Applied**
[Edit](#) [Preview Block Page](#)

► [Advanced Settings](#)

[CANCEL](#) [PREVIOUS](#) [SAVE](#)

1011 **Configure Windows Domain Controller as the Local DNS Provider**

- 1012 1. Click **Deployments > Configuration > Domain Management**.
- 1013 2. Click **Add**.



- 1014 3. In the **Add New Bypass Domain or Server** popup window, fill out the following information:
- 1015 a. **Domain:** hdo.trpm
- 1016 b. **Applies To:** All Sites, All Devices
- 1017 4. Click **Save**. Verify that 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 x All Devices x

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 < >

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

1019 LogRhythm XDR is a SIEM system that receives log and machine data from multiple end points and
 1020 evaluates the data to determine when cybersecurity events occur. The project utilizes LogRhythm XDR in

1021 the HDO environment to enable a continuous view of business operations and detect cyber threats on
1022 assets.

1023 **System Requirements**

1024 **CPU:** 20 virtual central processing units (vCPUs)

1025 **Memory:** 96 GB RAM

1026 **Storage:**

- 1027 ▪ **hard drive C:** 220 GB
- 1028 ▪ **hard drive D:** 1 terabyte (TB)
- 1029 ▪ **hard drive L:** 150 GB

1030 **Operating System:** Microsoft Windows Server 2016 X64 Standard Edition

1031 **Network Adapter:** VLAN 1348

1032 **LogRhythm XDR Installation**

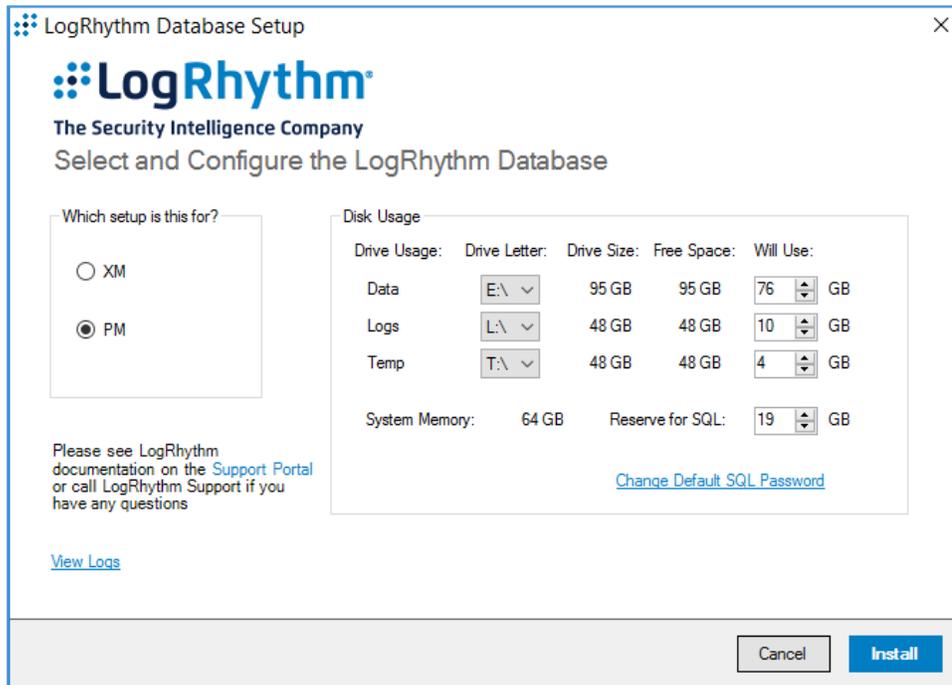
1033 This section describes LogRhythm installation processes.

1034 **Download Installation Packages**

- 1035 1. Acquire the installation packages from LogRhythm, Inc.
- 1036 2. Prepare a virtual Windows Server per the system requirements.
- 1037 3. Create three new drives.
- 1038 4. Create a new folder from C:\ on the Platform Manager server, and name the folder **LogRhythm**.
- 1039 5. Extract the provided Database Installer tool and LogRhythm XDR Wizard from the installation
1040 package in C:\LogRhythm.

1041 **Install Database**

- 1042 1. Open *LogRhythmDatabaseInstallTool* folder.
- 1043 2. Double-click **LogRhythmDatabaseInstallTool** application file.
- 1044 3. Click **Run**.
- 1045 4. A **LogRhythm Database Setup** window will appear. Set the **Which setup is this for?** to **PM** and
1046 use the default values for **Disk Usage**.



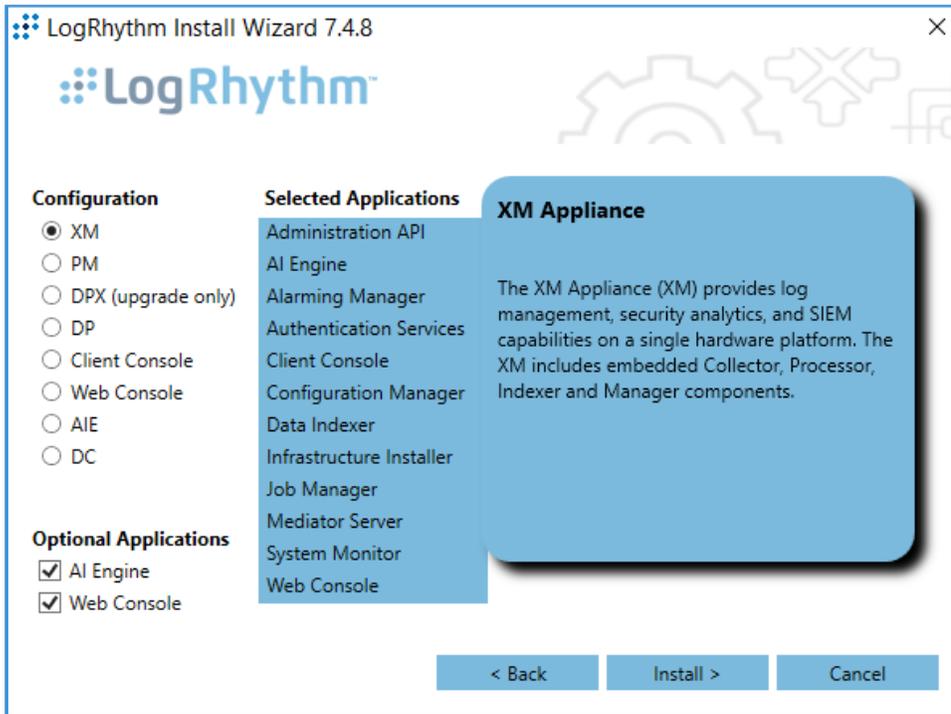
- 1047 5. The remaining fields will automatically populate with the appropriate values. Click **Install**.
- 1048 6. Click **Done** to close the **LogRhythm Database Setup** window.

1049 Install LogRhythm XDR

- 1050 1. Navigate to **C:** and open **LogRhythm XDR Wizard** folder.
- 1051 2. Double-click the **LogRhythmInstallerWizard** application file.
- 1052 3. The LogRhythm Install Wizard 7.4.8 window will appear.
- 1053 4. Click **Next**.
- 1054 5. A **LogRhythm Install Wizard Confirmation** window will appear.
- 1055 6. Click **Yes** to continue.
- 1056 7. Check the box beside **I accept the terms in the license agreement** to accept the License
- 1057 Agreement.
- 1058 8. Click **Next**.
- 1059 9. In the **Selected Applications** window, select the following attributes:
- 1060 a. **Configuration:** Select the XM radio button.

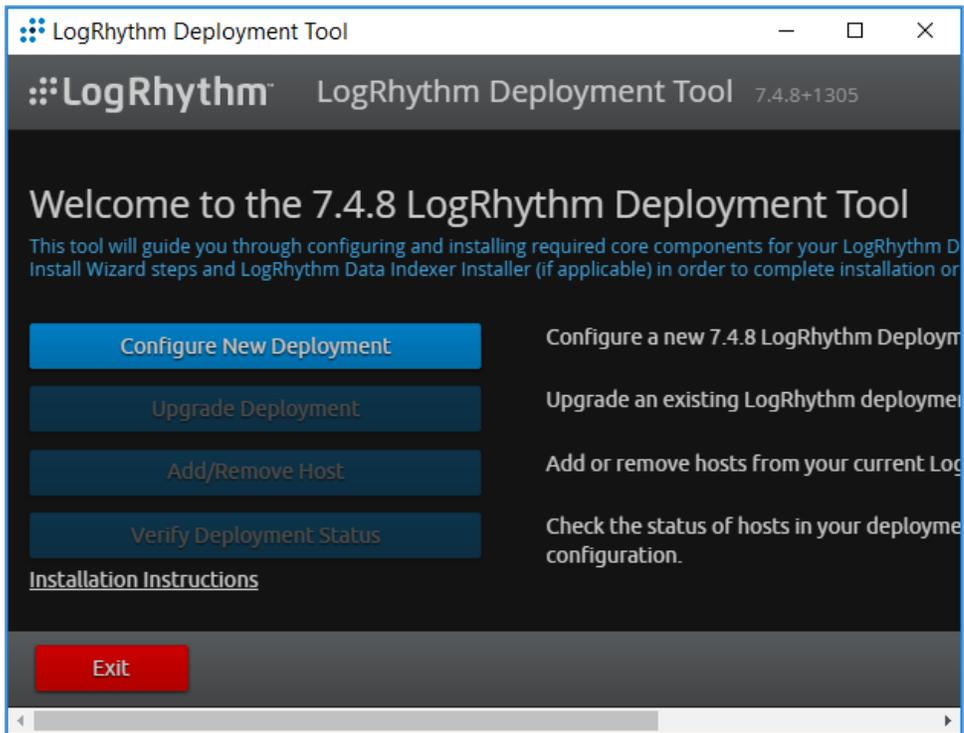
1061 b. **Optional Applications:** Check both **AI Engine** and **Web Console** boxes.

1062 10. Click **Install**.

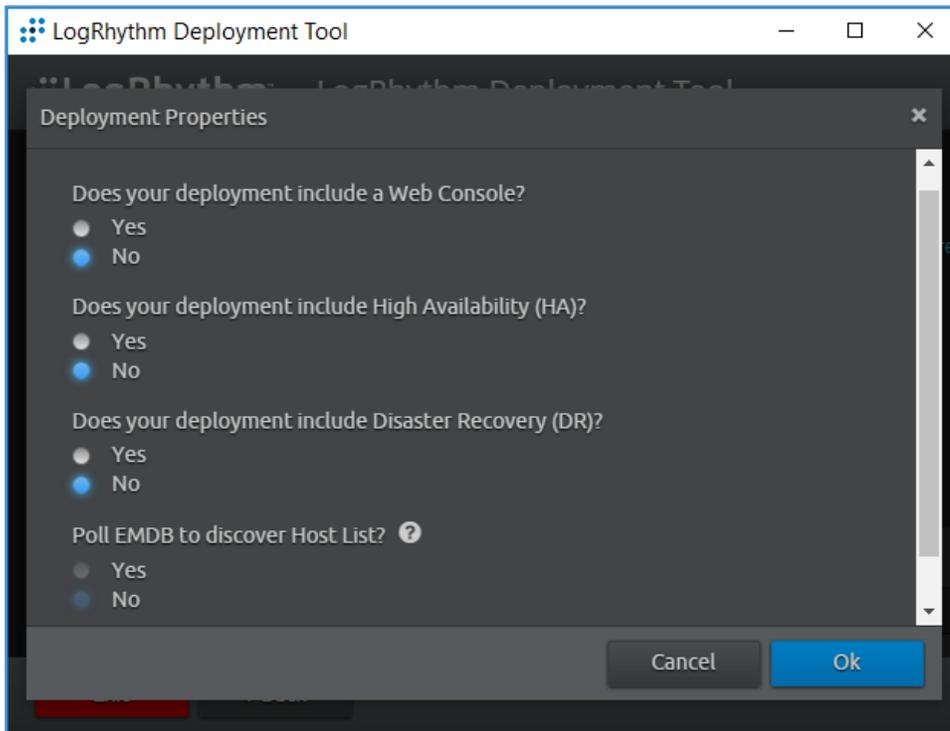


1063 11. A **LogRhythm Deployment Tool** window displays.

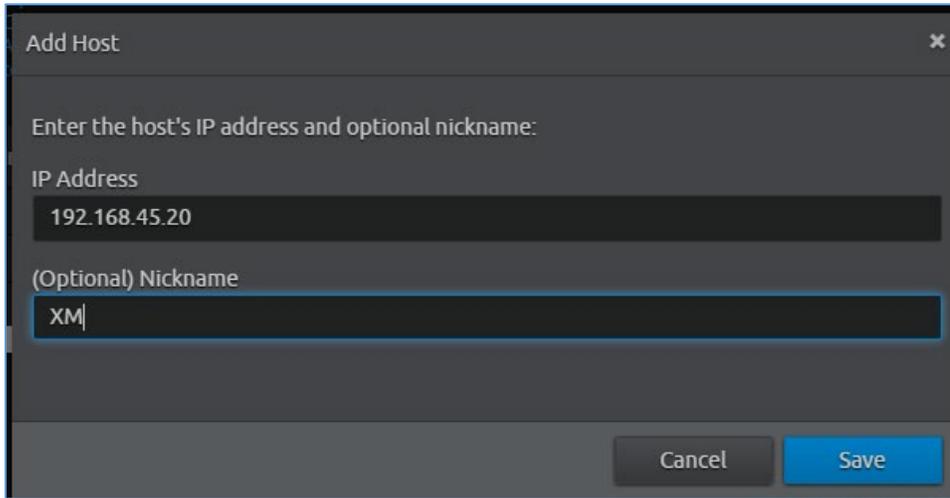
1064 12. Click **Configure New Deployment**.



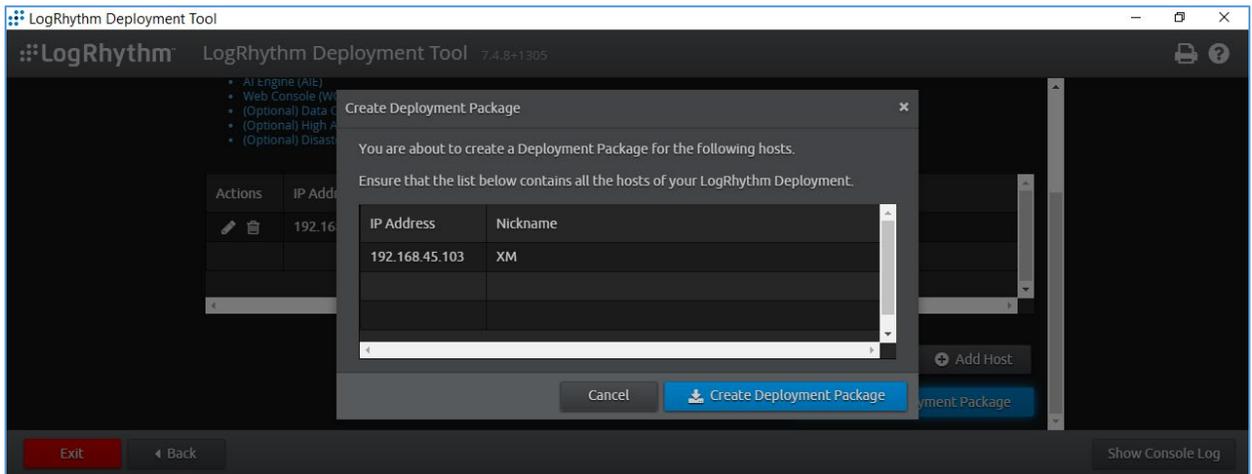
1065 13. In the **Deployment Properties window**, keep the default configurations and click **Ok**.



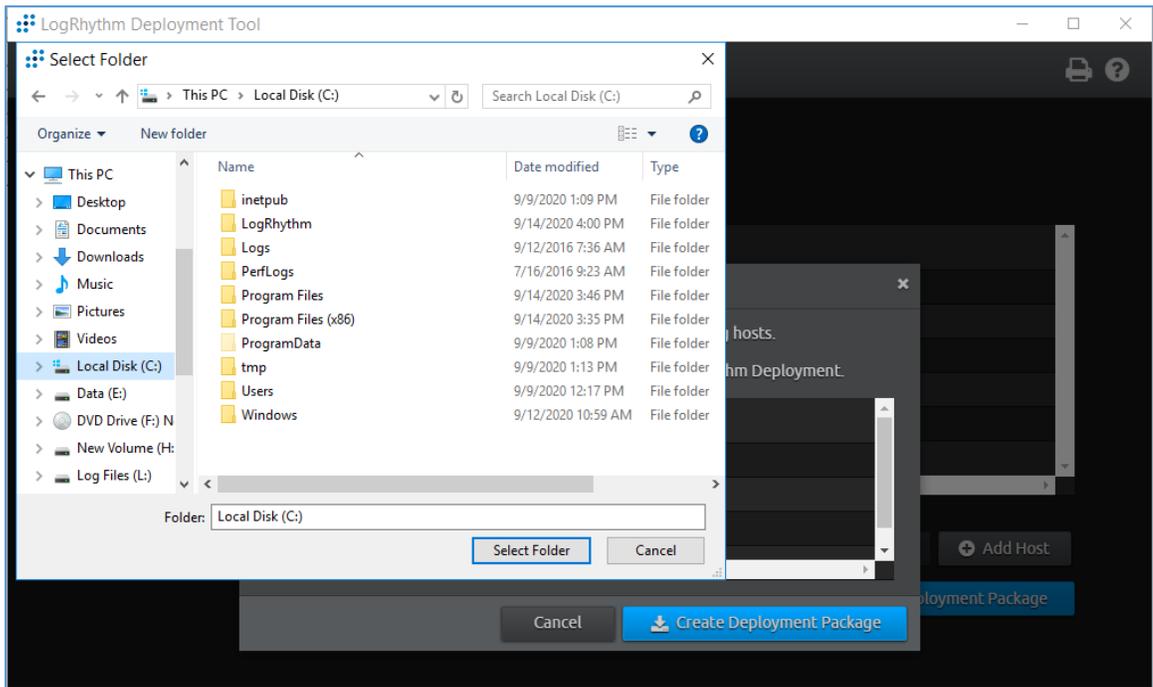
- 1066 14. Click **+Add Host IP** in the bottom right corner of the screen, and provide the following
1067 information:
- 1068 a. **IP Address:** 192.168.45.20
 - 1069 b. **Nickname:** XM
- 1070 15. Click **Save**.



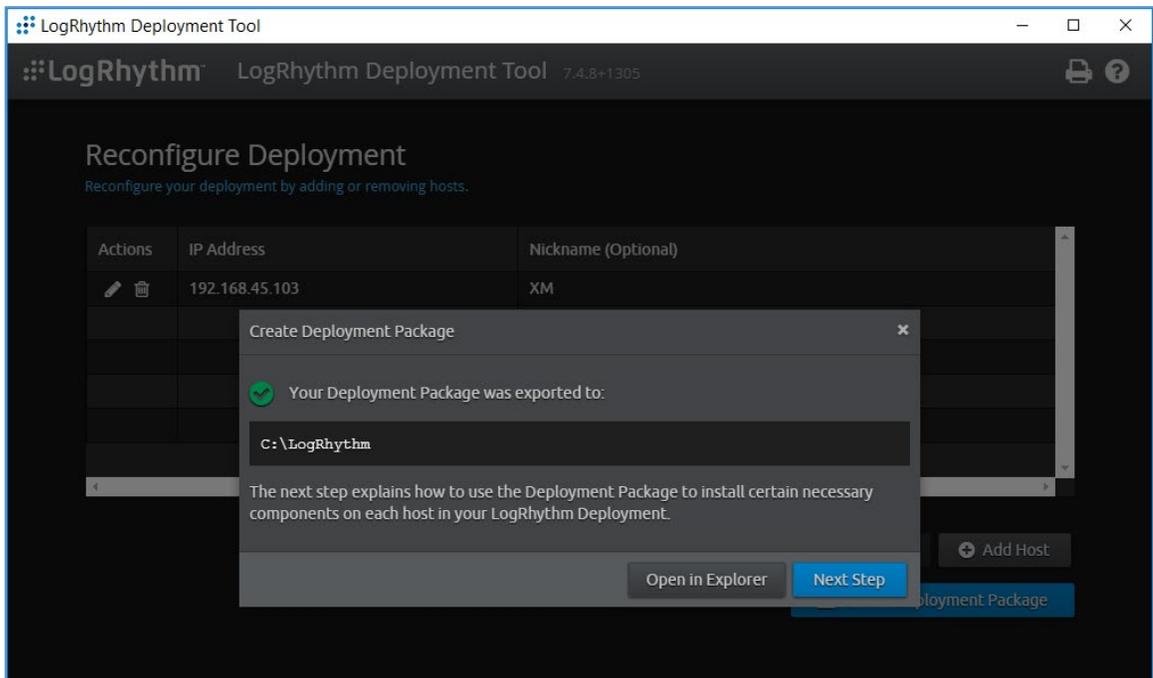
- 1071 16. Click **Create Deployment Package** in the bottom right corner of the screen.
- 1072 17. A **Create Deployment Package** window displays.
- 1073 18. Click **Create Deployment Package**.



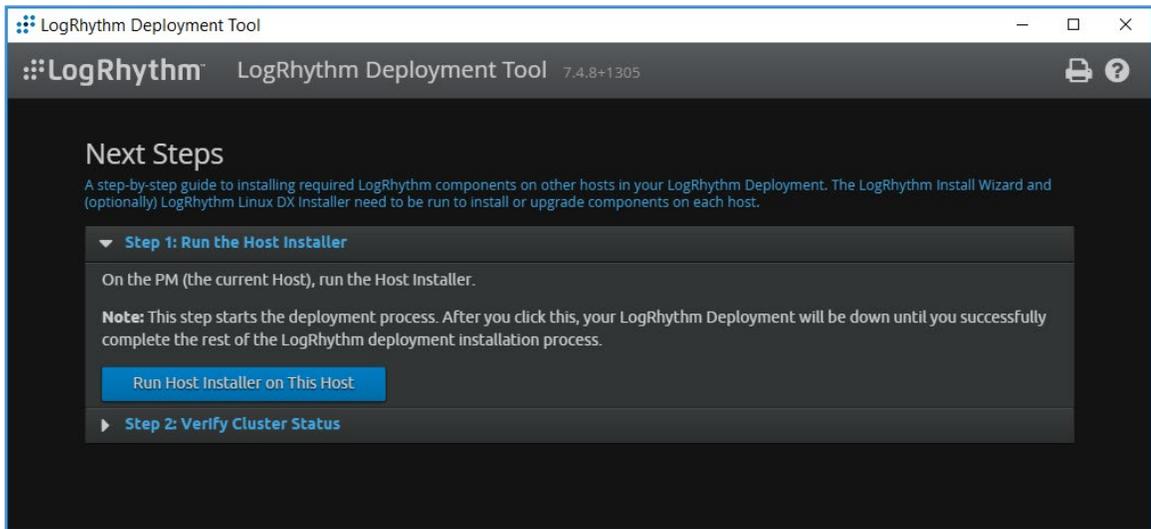
- 1074 19. A **Select Folder** window appears.
- 1075 20. Navigate to **C:\LogRhythm**.
- 1076 21. Click **Select Folder**.



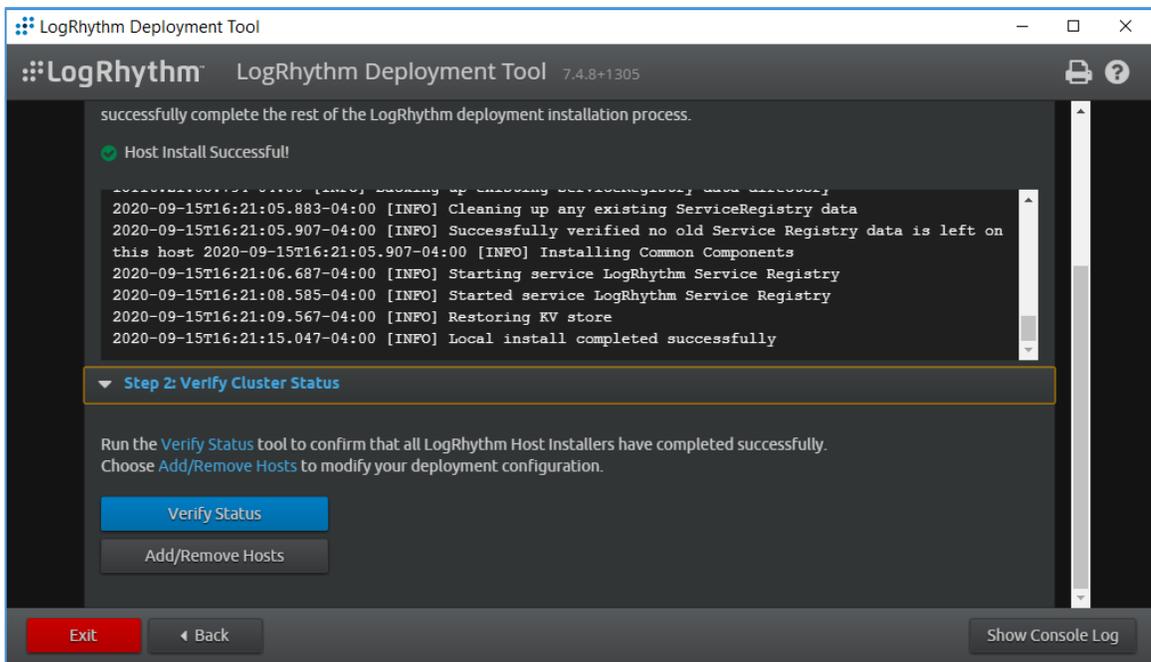
1077 22. Click **Next Step**.



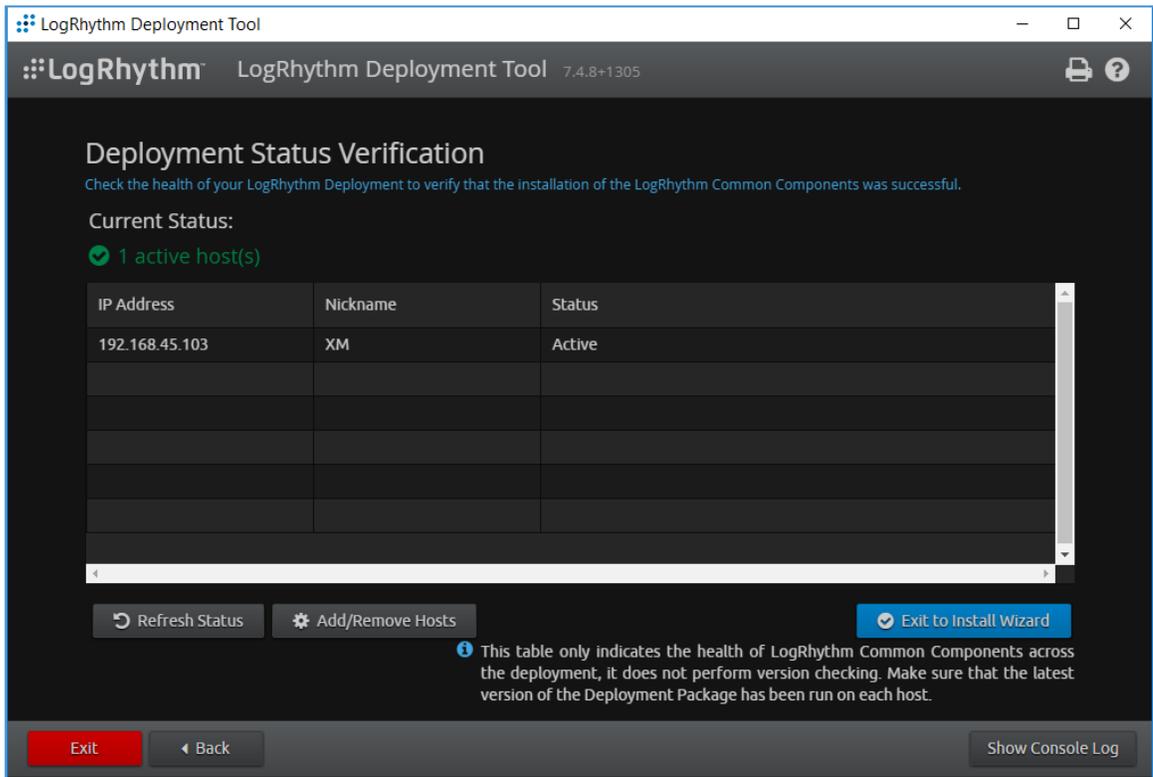
1078 23. Click **Run Host Installer on this Host**.



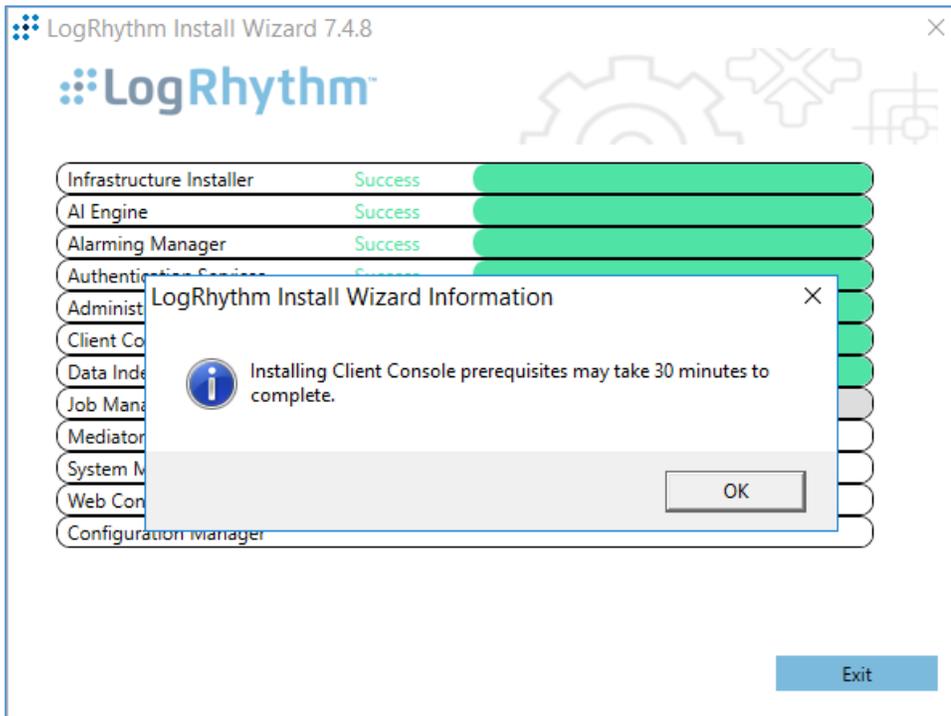
1079 24. After the Host Installer has finished, click **Verify Status**.



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

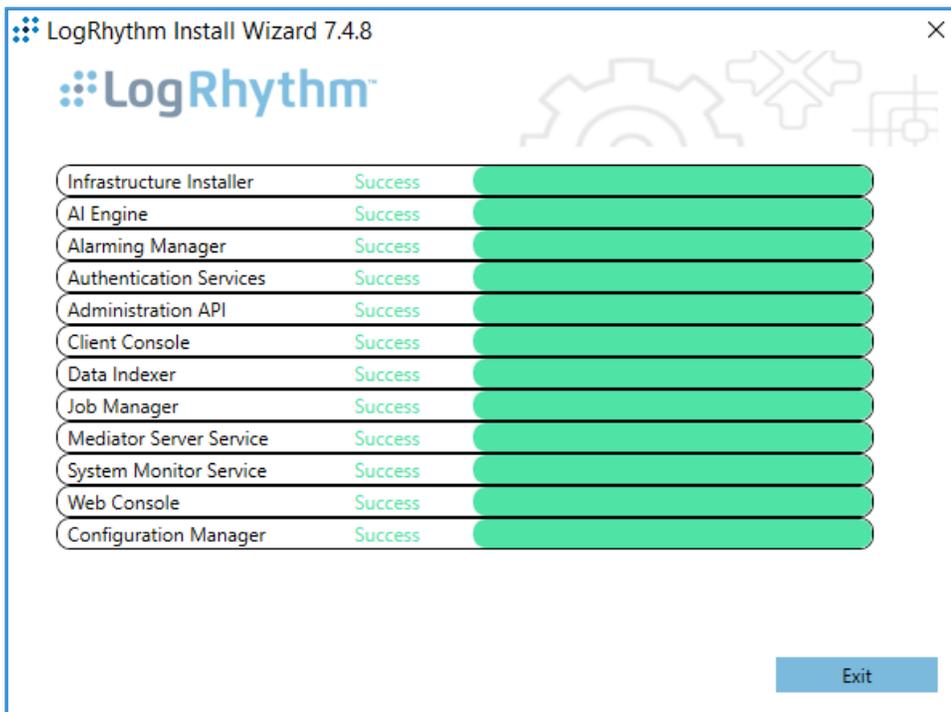


1081 26. A notification window displays stating the installation could take as long as 30 minutes. Click **OK**.



1082

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



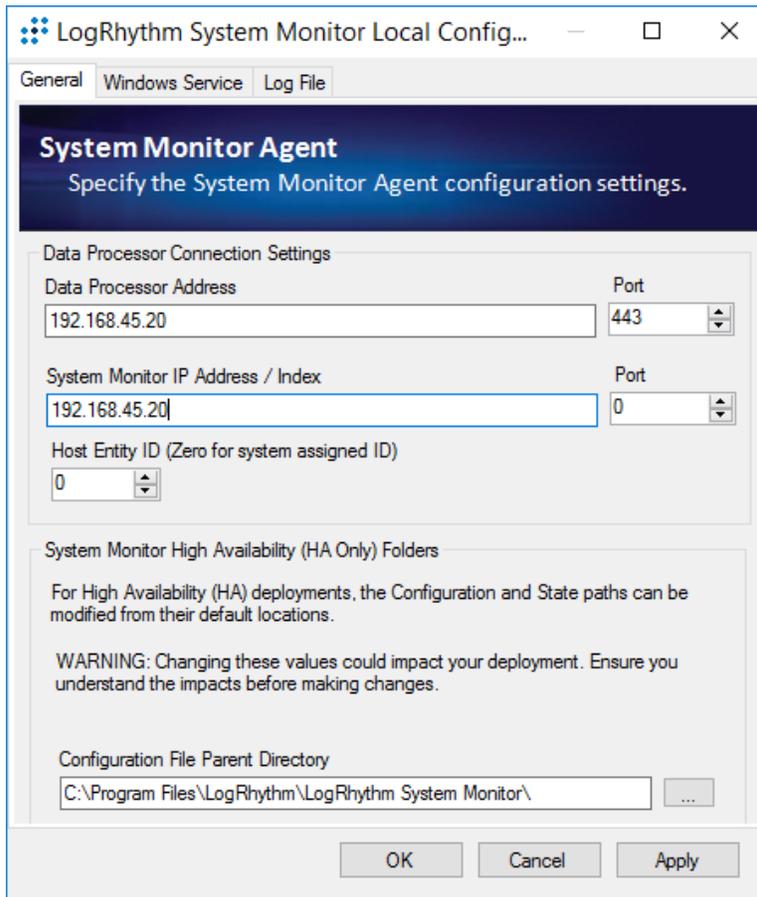
1083 **LogRhythm XDR Configuration**

1084 The LogRhythm XDR configuration includes multiple related components:

- 1085 ▪ System Monitor
- 1086 ▪ LogRhythm Artificial Intelligence (AI) Engine
- 1087 ▪ Mediator Server
- 1088 ▪ Job Manager
- 1089 ▪ LogRhythm Console

1090 **Configure System Monitor**

- 1091 1. Open **File Explorer**, and navigate to **C:\Program Files\LogRhythm**.
- 1092 2. Navigate to **LogRhythm System Monitor**.
- 1093 3. Double-click the **lrconfig** application file.
- 1094 4. In the **LogRhythm System Monitor Local Configuration Manager** window, provide the following
1095 information, and leave the remaining fields as their default values:
 - 1096 a. **Data Processor Address:** 192.168.45.20
 - 1097 b. **System Monitor IP Address/Index:** 192.168.45.20
- 1098 5. Click **Apply**, and then click **OK**.



1099 **Configure LogRhythm AI Engine**

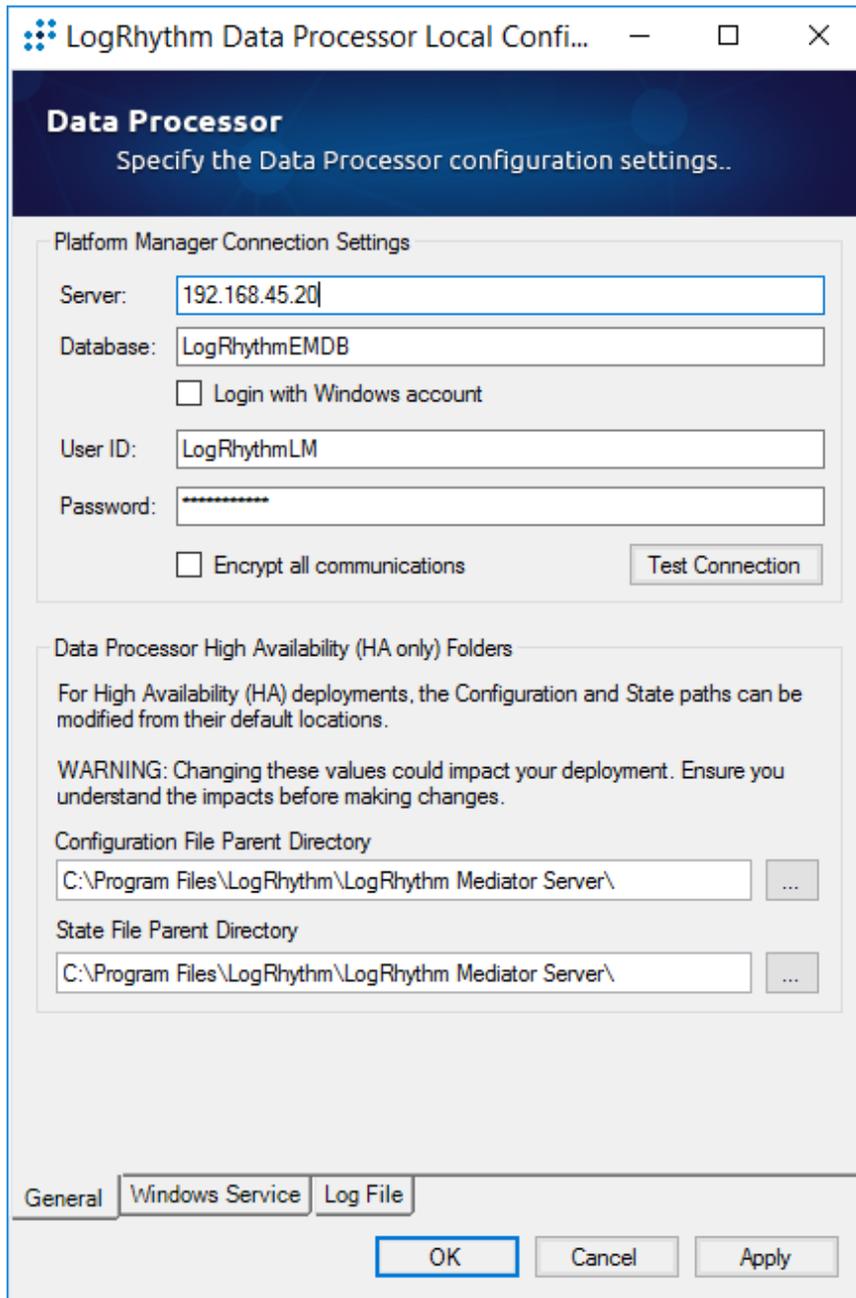
- 1100 1. Open **File Explorer**, and navigate to **C:\Program Files\LogRhythm**.
- 1101 2. Navigate to **LogRhythm AI Engine**.
- 1102 3. Double-click the **lrconfig** application file.
- 1103 4. In the **LogRhythm AI Engine Local Configuration Manager** window, provide the following
- 1104 information, and leave the remaining fields as their default values:
- 1105 a. **Server:** 192.168.45.20
- 1106 b. **Password:** *****
- 1107 5. Click **Test Connection**, then follow the instruction of the alert window to complete the test
- 1108 connection.
- 1109 6. Click **Apply**, and then click **OK**.

1110 **Configure Mediator Server**

- 1111 1. Open File Explorer, and navigate to **C:\Program Files\LogRhythm**.
- 1112 2. Navigate to **Mediator Server**.
- 1113 3. Double-click **Irconfig** application file.
- 1114 4. In the **LogRhythm Data Processor Local Configuration Manager** window, provide the following
- 1115 information, and leave the remaining fields as their default values:
- 1116 a. **Server:** 192.168.45.20
- 1117 b. **Password:** *****

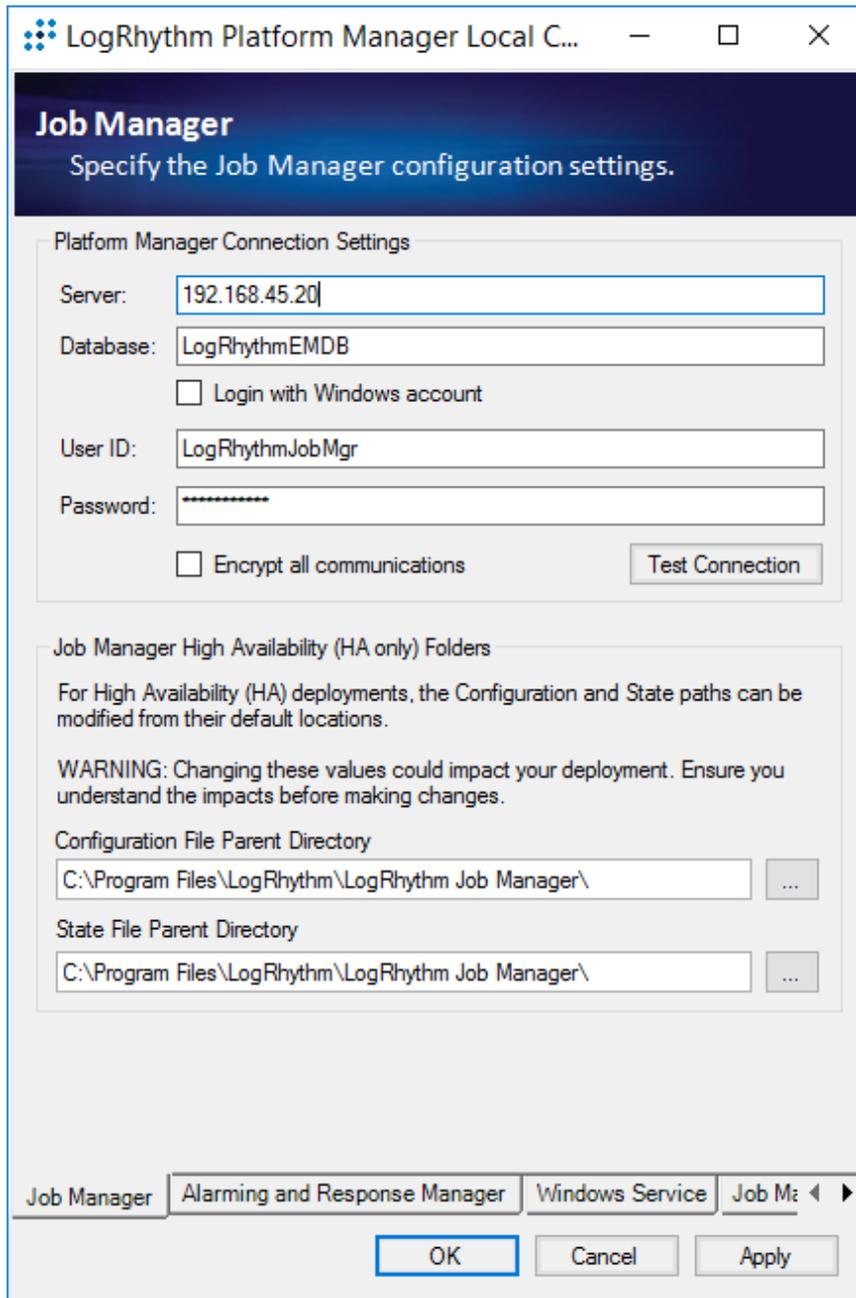
1118

- 1119 5. Click **Test Connection**, then follow the instruction of the alert window to complete the test
- 1120 connection.
- 1121 6. Click **Apply**, and then click **OK**.



1122 **Configure Job Manager**

- 1123 1. Open File Explorer and navigate to **C:\Program Files\LogRhythm**.
- 1124 2. Navigate to **Job Manager**.
- 1125 3. Double-click the **lrconfig** application file.
- 1126 4. In the **LogRhythm Platform Manager Local Configuration Manager** window, provide the
1127 following information, and leave the remaining fields as their default values:
 - 1128 a. **Server:** 192.168.45.20
 - 1129 b. **Password:** *****
- 1130 5. Click **Test Connection**, then follow the instruction of the alert window to complete the test
1131 connection.
- 1132 6. Click **Apply**, and then click **OK**.

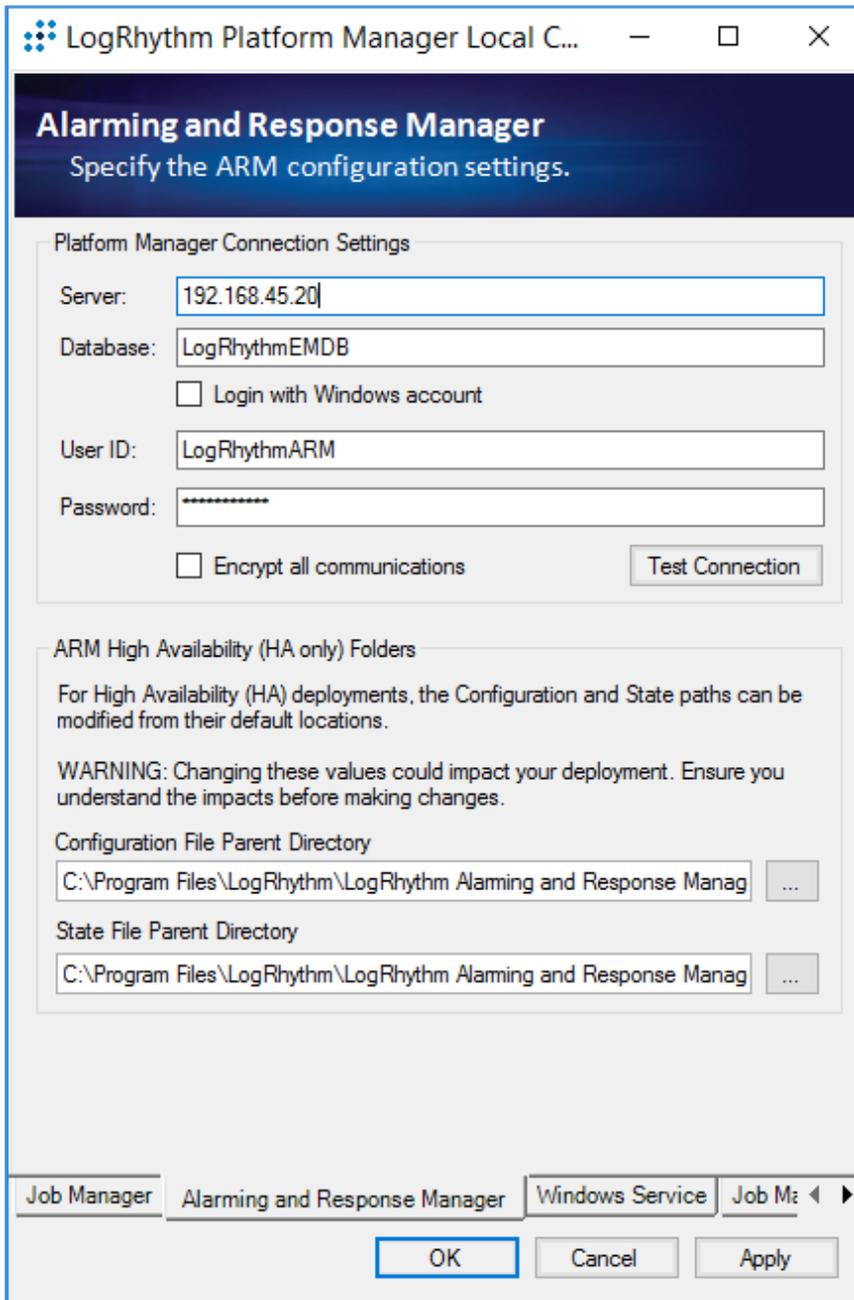


- 1133 7. Navigate to the **Alarming and Response Manager** tab in the bottom menu ribbon.
- 1134 8. In the **Alarming and Response Manager** window, provide the following information, and leave
- 1135 the remaining fields as their default values:
- 1136 a. **Server:** 192.168.45.20

1137 b. **Password:** *****

1138 9. Click **Test Connection**, then follow the instruction of the alert window to complete the test
1139 connection.

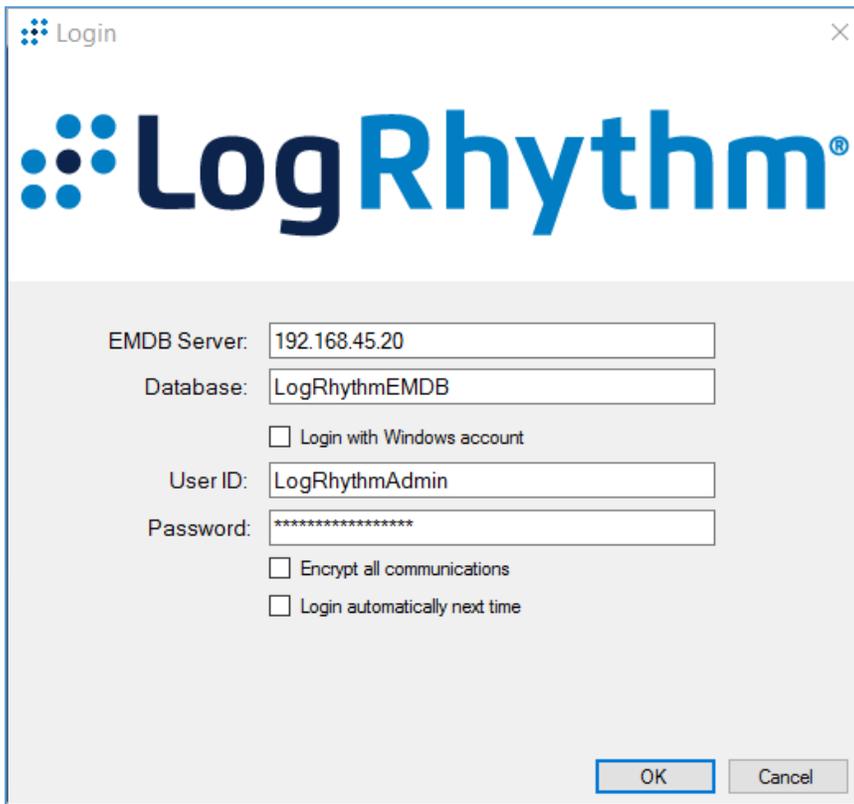
1140 10. Click **Apply**, and then click **OK**.



1141 **Configure LogRhythm Console**

- 1142 1. Open File Explorer and navigate to **C:\Program Files\LogRhythm.**
- 1143 2. Navigate to **LogRhythm Console.**

- 1144 3. Double-click *Irconfig* application file.
- 1145 4. In the LogRhythm Login window, provide the following information:
- 1146 a. **EMDB Server:** 192.168.45.20
- 1147 b. **UserID:** LogRhythmAdmin
- 1148 c. **Password:** *****
- 1149 5. Click **OK**.



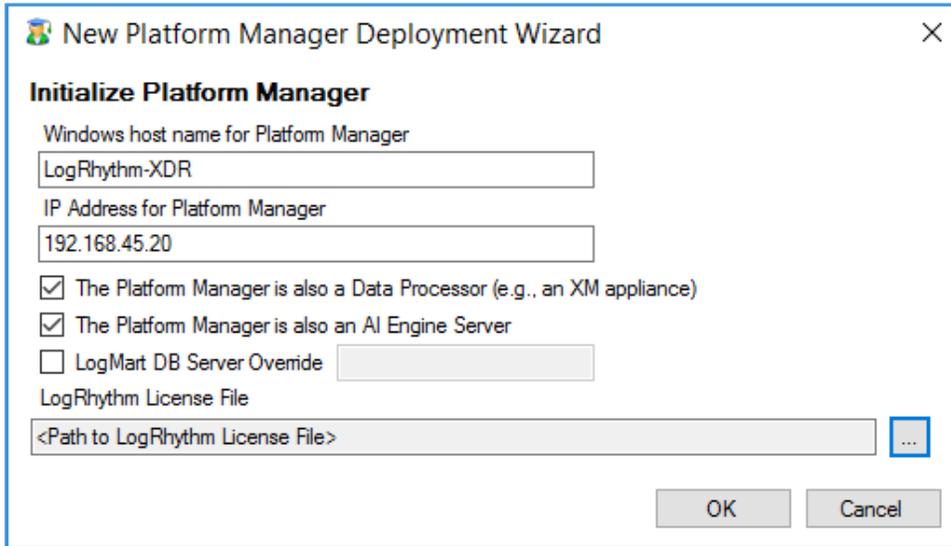
The screenshot shows a 'Login' dialog box for LogRhythm. The title bar says 'Login' with a close button. The LogRhythm logo is prominently displayed. Below the logo, the following fields and options are visible:

- EMDB Server: 192.168.45.20
- Database: LogRhythmEMDB
- Login with Windows account
- User ID: LogRhythmAdmin
- Password: *****
- Encrypt all communications
- Login automatically next time

At the bottom right, there are 'OK' and 'Cancel' buttons.

- 1150 6. A New Platform Manager Deployment Wizard window displays. Provide the following
- 1151 information:
- 1152 a. **Windows host name for Platform Manager:** LogRhythm-XDR
- 1153 b. **IP Address for Platform Manager:** 192.168.45.20
- 1154 c. Check the box next to **The Platform Manager is also a Data Processor (e.g., an XM**
- 1155 **appliance).**

- 1156 d. Check the box next to **The Platform Manager is also an AI Engine Server**.
- 1157 7. Click the **ellipsis button** next to **<Path to LogRhythm License File>**, and navigate to the location
- 1158 of the LogRhythm License File.



- 1159 8. The New Knowledge Base Deployment Wizard window displays and shows the import progress
- 1160 status. Once LogRhythm has successfully imported the file, a message window will appear
- 1161 stating more configurations need to be made for optimum performance. Click **OK** to open the
- 1162 **Platform Manager Properties** window.
- 1163 9. In the Platform Manager Properties window, provide the following information:
- 1164 a. **Email address:** no_reply@logrhythm.com
- 1165 b. **Address:** 192.168.45.20
- 1166 10. Click the button next to **Platform**, enable the **Custom Platform** radio button, and complete the
- 1167 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

Primary Secondary Tertiary

Advanced Defaults OK Cancel Apply

- 1168 11. After the Platform Manager Properties window closes, a message window displays for
1169 configuring the Data Processor. Click **OK** to open the **Data Processor Properties** window.
- 1170 12. Click the button next to **Platform**, and enable the **Custom Platform** radio button.
- 1171 13. Click **OK**.
- 1172 14. Leave the remaining fields in the Data Processor Properties window as their default values, and
1173 click **Apply**.
- 1174 15. Click **OK** to close the window.

Data Processor Properties

General | AI Engine | Automatic Log Source Configuration

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

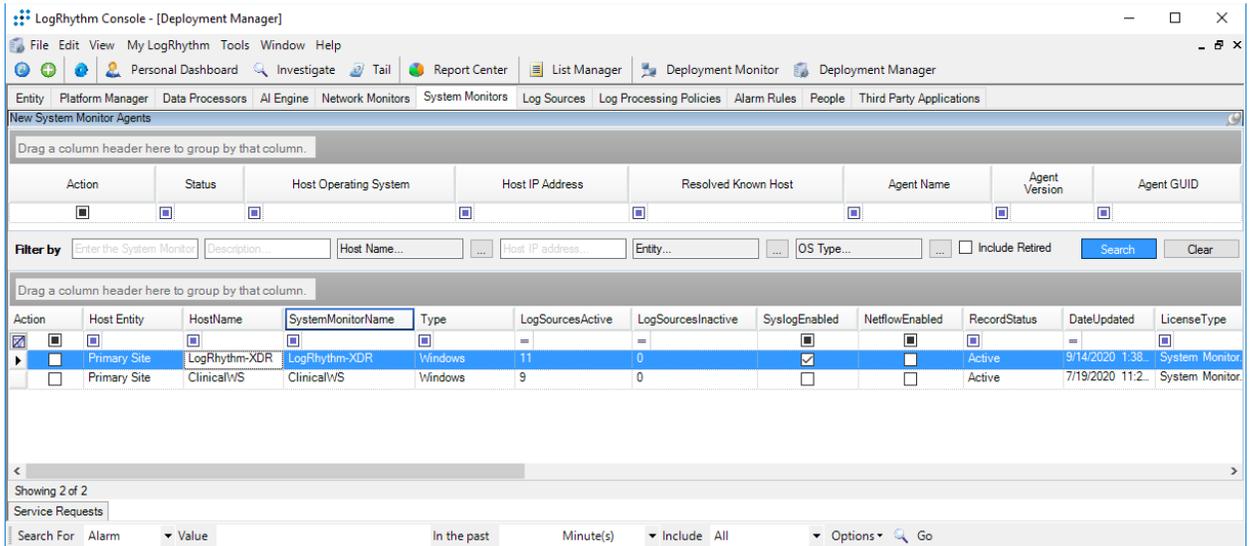
Disable MPE Event forwarding

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

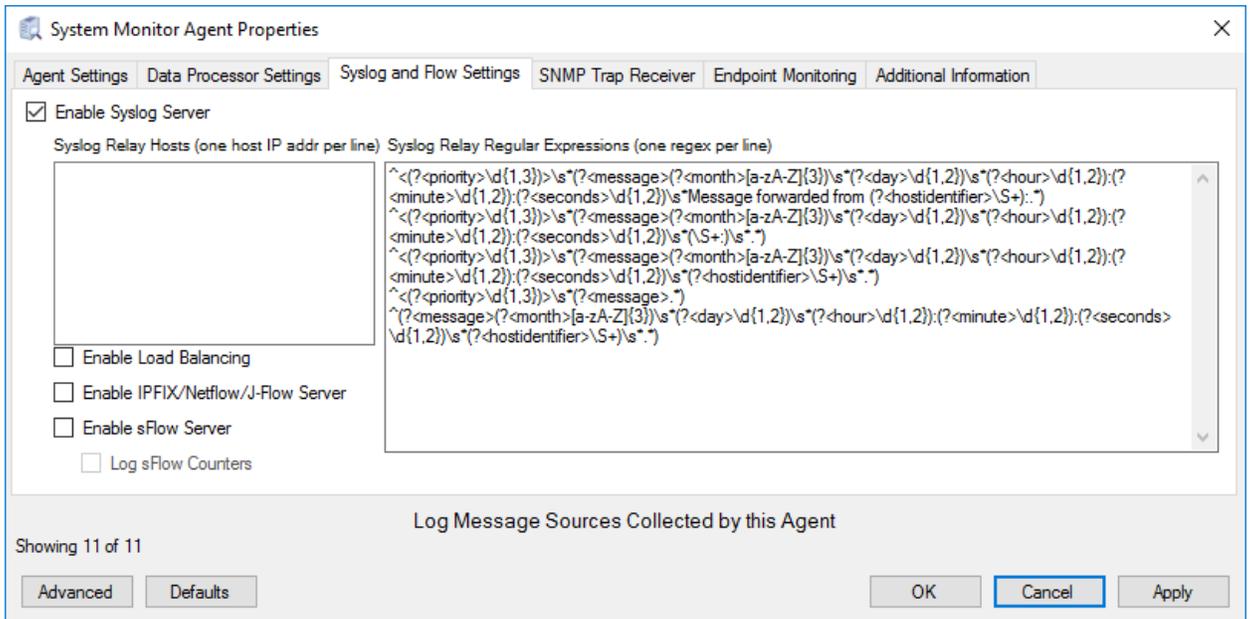
Advanced Defaults OK Cancel Apply

1175 **Set LogRhythm-XDR for System Monitor**

- 1176 1. Back in the LogRhythm console, navigate to the **Deployment Manager** tab in the menu ribbon.
- 1177 2. Navigate to **System Monitors** on the Deployment Manager menu ribbon.
- 1178 3. Double-click **LogRhythm-XDR**.



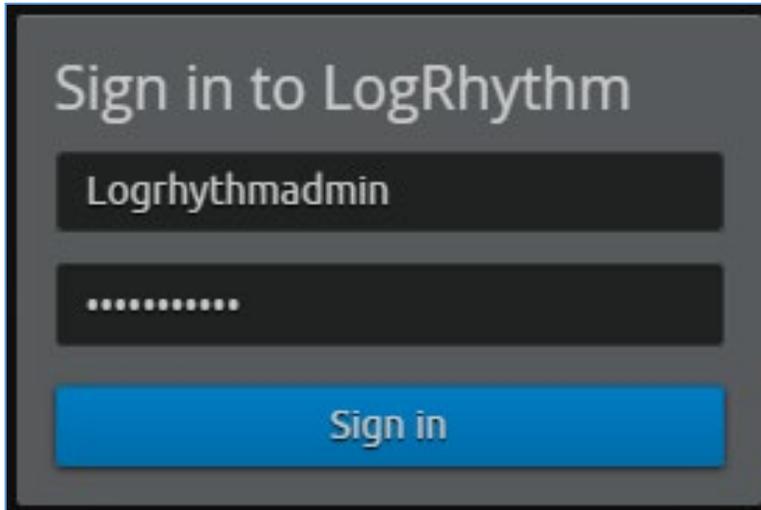
- 1179 4. In the **System Monitor Agent Properties** window, navigate to **Syslog and Flow Settings**.
- 1180 5. Click the checkbox beside **Enable Syslog Server**.
- 1181 6. Click **OK** to close the System Monitor Agent Properties window.



- 1182 **Use the LogRhythm Web Console**
- 1183 1. Open a web browser, and navigate to **https://localhost:8443**.

1184 2. Enter the **Username:** logrhythmadmin

1185 3. Enter the **Password:** *****



1186 *2.2.3.4 LogRhythm NetworkXDR*

1187 LogRhythm NetworkXDR paired with LogRhythm XDR enables an environment to monitor network
1188 traffic between end points and helps suggest remediation techniques for identified concerns. This
1189 project utilizes NetworkXDR for continuous visibility on network traffic between HDO VLANs and
1190 incoming traffic from the telehealth platform provider.

1191 **System Requirements**

1192 **CPU:** 24 vCPUs

1193 **Memory:** 64 GB RAM

1194 **Storage:**

- 1195 ■ Operating System Hard Drive: 220 GB
- 1196 ■ Data Hard Drive: 3 TB
- 1197 ■ Operating System: CentOS 7

1198

1199 **Network Adapter:** VLAN 1348

1200 **LogRhythm NetworkXDR Installation**

1201 LogRhythm provides an International Organization for Standardization (.iso) disk image to simplify
1202 installation of NetMon. The .iso is a bootable image that installs CentOS 7.7 Minimal and NetMon. Note:
1203 Because this is an installation on a Linux box, there is no need to capture the screenshots.

1204 **Download the Installation Software**

- 1205 1. Open a new tab in the web browser, and navigate to <https://community.logrhythm.com>.
- 1206 2. Log in using the appropriate credentials.
- 1207 3. Click **LogRhythm Community**.
- 1208 4. Navigate to **Documentation & Downloads**.
- 1209 5. Register a **Username**.
- 1210 6. Click **Accept**.
- 1211 7. Click **Submit**.
- 1212 8. Navigate to **NetMon**.
- 1213 9. Click **downloads: netmon4.0.2**.
- 1214 10. Select **NetMon ISO** under Installation Files.

1215 **Install LogRhythm NetworkXDR**

- 1216 1. In the host server, mount the *.iso* for the installation.
- 1217 2. Start the VM with the mounted *.iso*.
- 1218 3. When the welcome screen loads, select **Install LogRhythm Network Monitor**.
- 1219 4. The installer completes the installation, and the system reboots.
- 1220 5. When the system reboots, log in to the console by using **logrhythm** as the login and ********* as
1221 the password.
- 1222 6. Then change the password by typing the command **passwd**, type the default **password**, and
1223 then type and verify the **new password**.

1224 **LogRhythm NetworkXDR Configuration**

- 1225
- 1226 1. **Data Process Address:** 192.168.45.20
- 1227 2. Click **Apply**.

The screenshot shows the 'LogRhythm System Monitor Local Config...' dialog box with the 'Windows Service' tab selected. The dialog has three tabs: 'General', 'Windows Service', and 'Log File'. A dark blue header contains the text 'System Monitor Agent' and 'Specify the System Monitor Agent configuration settings.' Below this, there are two main sections: 'Data Processor Connection Settings' and 'System Monitor High Availability (HA Only) Folders'. The first section contains three fields: 'Data Processor Address' (192.168.45.20), 'Port' (443), 'System Monitor IP Address / Index' (192.168.45.20), and 'Port' (3333). The second section contains a warning message and two directory fields: 'Configuration File Parent Directory' and 'State File Parent Directory', both set to 'C:\Program Files\LogRhythm\LogRhythm System Monitor\'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

LogRhythm System Monitor Local Config... — □ ×

General Windows Service Log File

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.

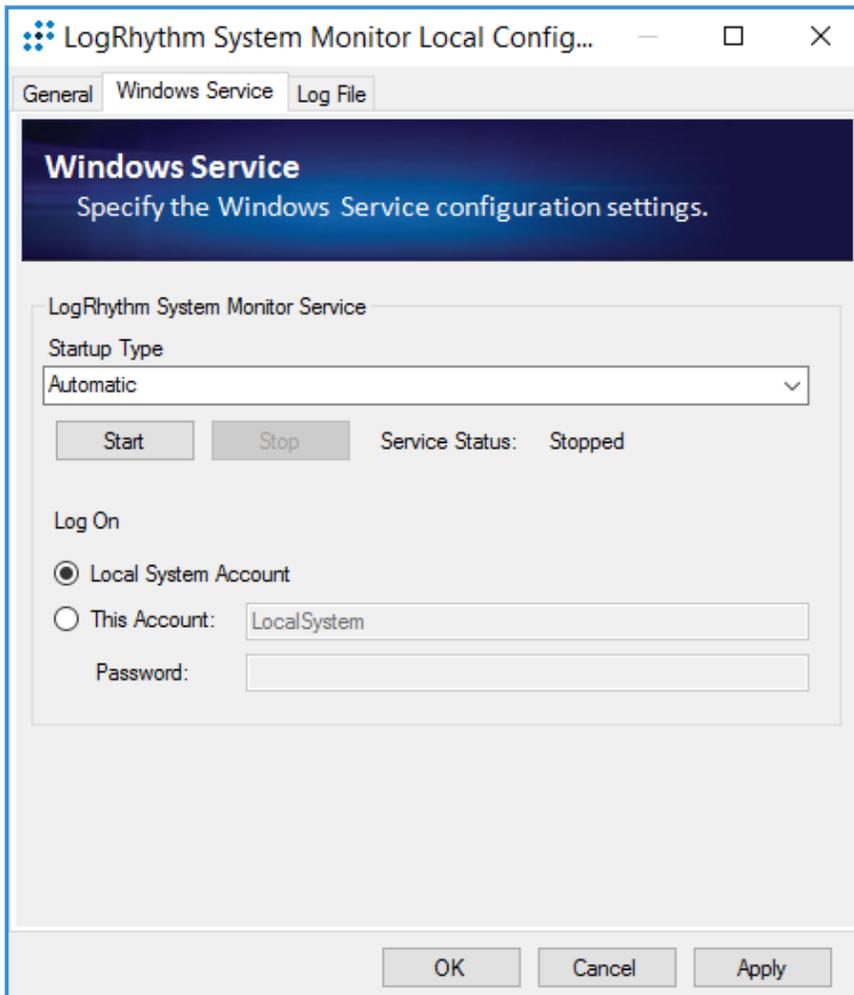
WARNING: Changing these values could impact your deployment. Ensure you understand the impacts before making changes.

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

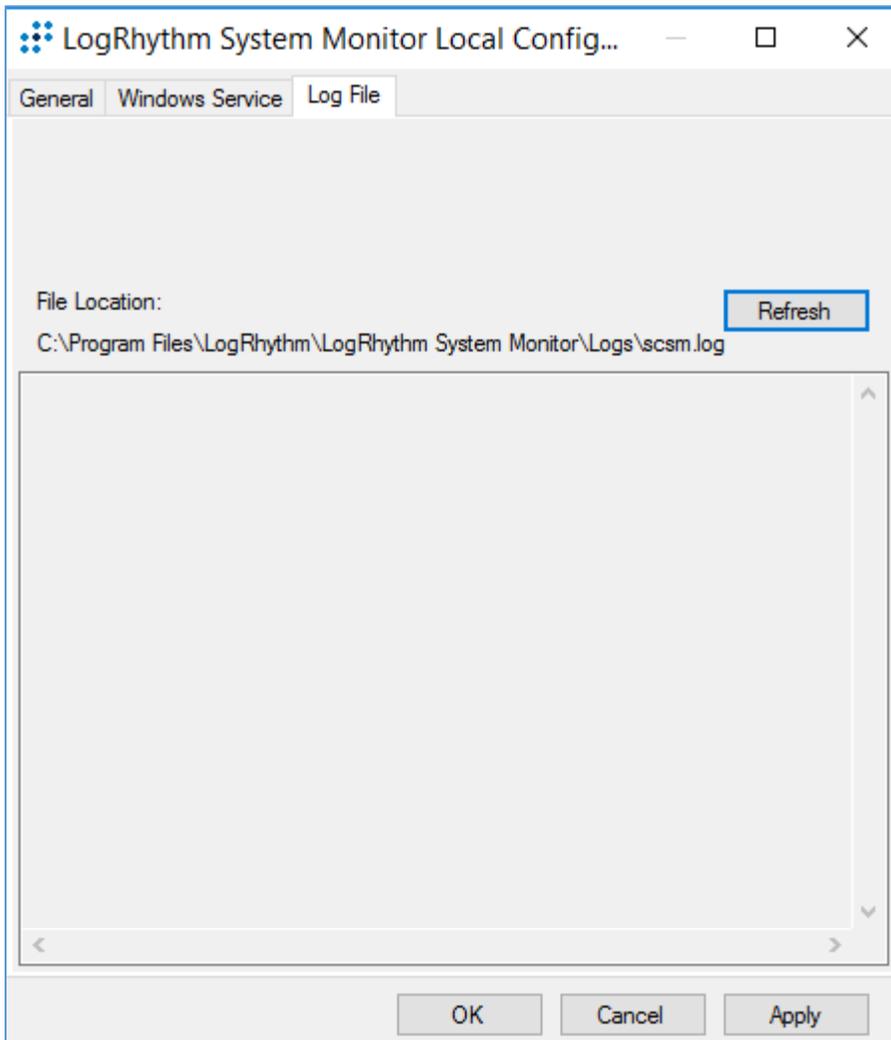
State File Parent Directory
C:\Program Files\LogRhythm\LogRhythm System Monitor\

OK Cancel Apply

- 1228 3. Click the **Windows Service** tab.
- 1229 4. Change the **Service Type** to **Automatic**.
- 1230 5. Click **Apply**.



- 1231 6. Click the **Log File** tab.
- 1232 7. Click **Refresh** to ensure NetworkXDR log collection.
- 1233 8. Click **OK** to exit the **Local Configuration Manager**.



1234 *2.2.3.5 LogRhythm System Monitor Agent*

1235 LogRhythm System Monitor Agent is a component of LogRhythm XDR that receives end-point log files
1236 and machine data in an IT infrastructure. The system monitor transmits ingested data to LogRhythm XDR
1237 where a web-based dashboard displays any identified cyber threats. This project deploys LogRhythm's
1238 System Monitor Agents on end points in each identified VLAN.

1239 Install the LogRhythm System Monitor Agent on one of the end points (e.g., Clinical Workstation) in the
1240 HDO environment so that the LogRhythm XDR can monitor the logs, such as syslog and eventlog, of this
1241 workstation.

1242 **System Monitor Agent Installation**

1243 This section describes installation of the system monitor agent.

1244 **Download Installation Packages**

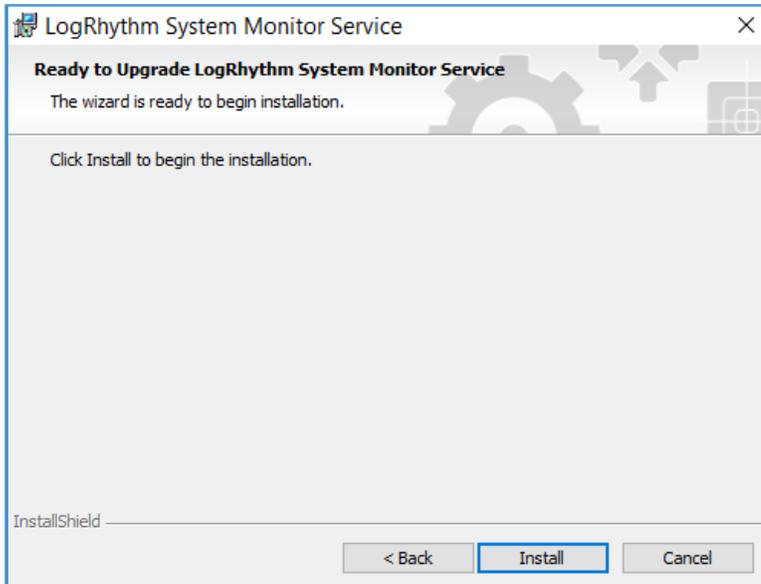
- 1245 1. Using a Clinical Workstation, open a web browser.
- 1246 2. Navigate to <https://community.logrhythm.com>.
- 1247 3. Log in using the credentials made when installing and configuring LogRhythm XDR.
- 1248 4. Navigate to **LogRhythm Community**.
- 1249 5. Click **Documents & Downloads**.
- 1250 6. Click **SysMon**.
- 1251 7. Click **SysMon – 7.4.10**.
- 1252 8. Click **Windows System Monitor Agents**, and save to the **Downloads** folder on the Workstation.

1253 **Install System Monitor Agent**

- 1254 1. On the Workstation, navigate to **Downloads** folder.
- 1255 2. Click **LRWindowsSystemMonitorAgents**.
- 1256 3. Click **LRSysmon_64_7**.
- 1257 4. On the Welcome page, follow the Wizard, and click **Next....**



- 1258 5. On the ready to begin installation page, click **Install**.



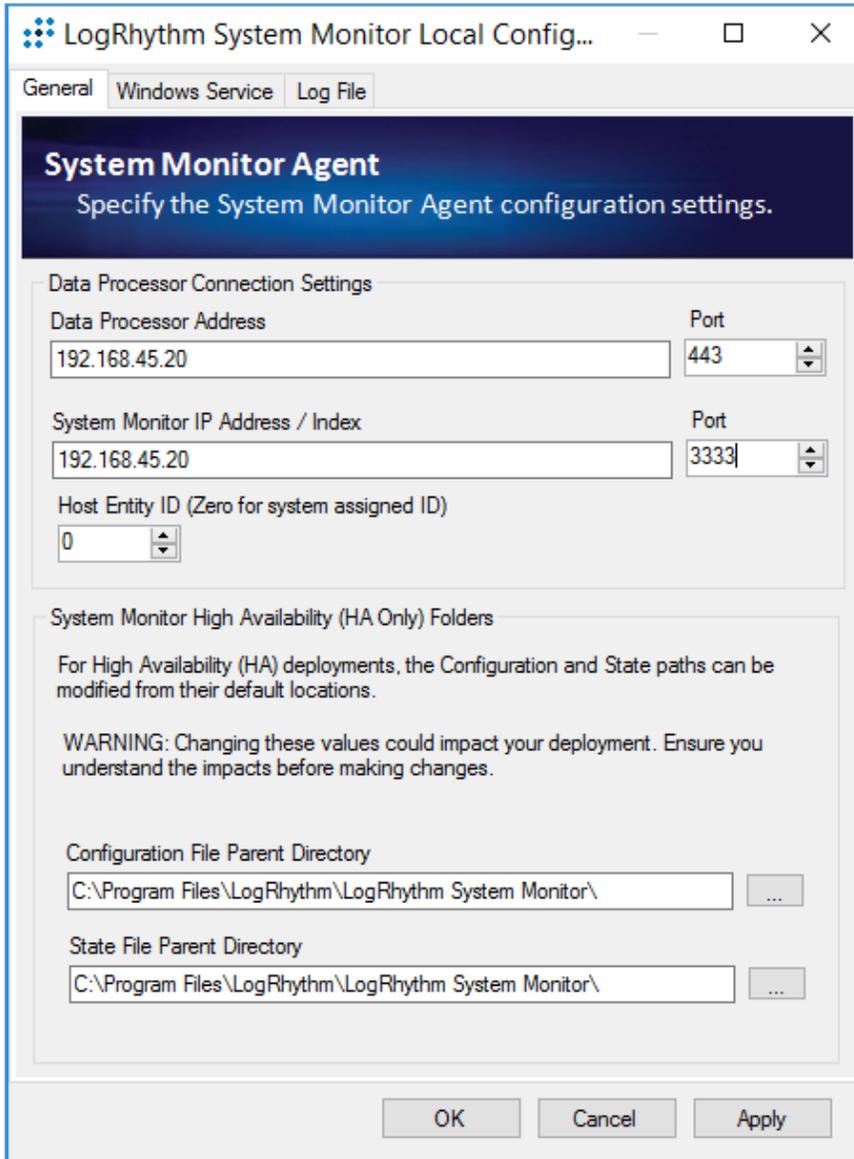
- 1259 6. Click **Finish**.



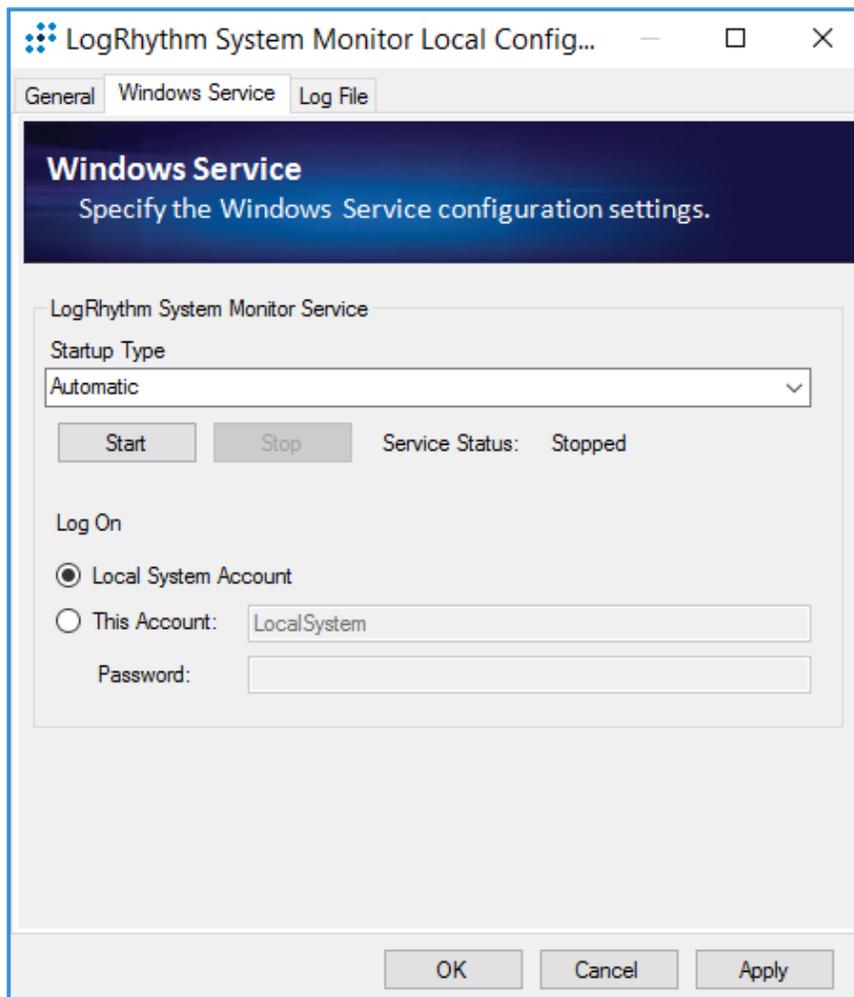
1260 **System Monitor Agent Configuration**

- 1261 1. After exiting the **LogRhythm System Monitor Service Install Wizard**, a LogRhythm System
1262 Monitor Local Configuration window displays. Under the **General** tab, provide the following
1263 information:

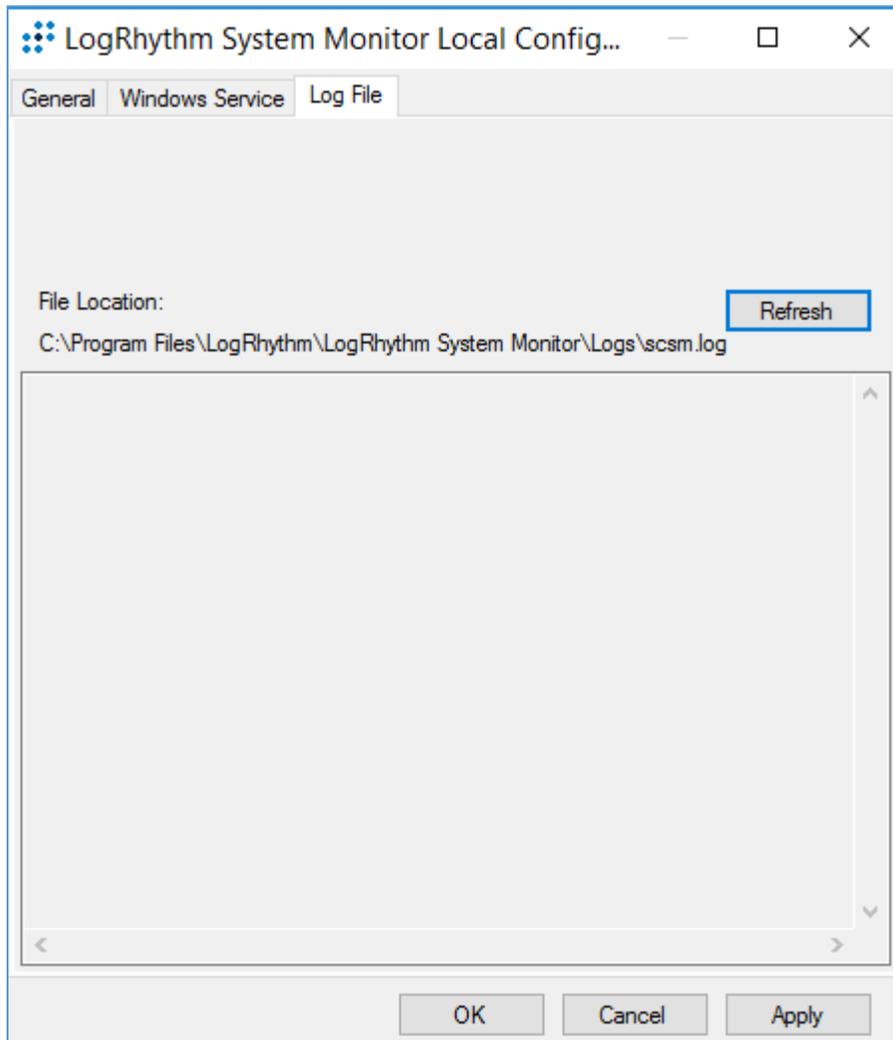
- 1264 a. **Data Process Address:** 192.168.45.20
- 1265 b. **System Monitor IP Address/Index:** 192.168.45.20
- 1266 2. Click **Apply**.



- 1267 3. Click the **Windows Service** tab.
- 1268 4. Change the **Service Type** to **Automatic**.
- 1269 5. Click **Apply**.



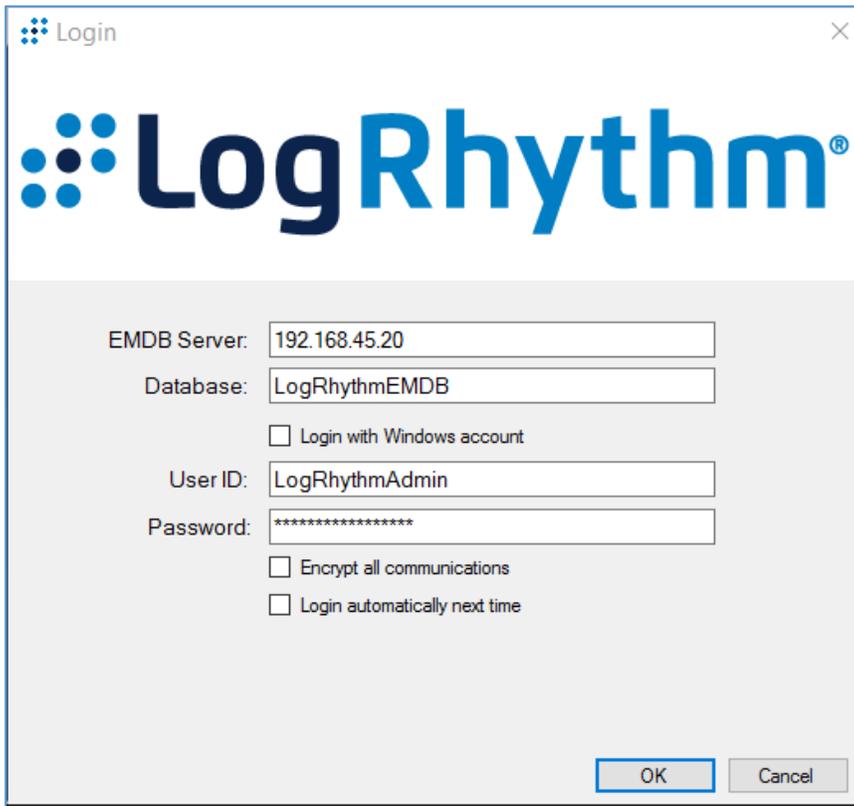
- 1270 6. Click the **Log File** tab.
- 1271 7. Click **Refresh** to ensure NetworkXDR log collection.
- 1272 8. Click **OK** to exit the **Local Configuration Manager**.



1273 **Add Workstation for System Monitor**

1274 Engineers added Clinical Workstation for System Monitor and Set Its Message Source Types in the
1275 LogRhythm Deployment Manager.

- 1276 1. Log in to the **LogRhythm Console**.
 - 1277 a. **User ID:** LogRhythmAdmin
 - 1278 b. **Password:** *****



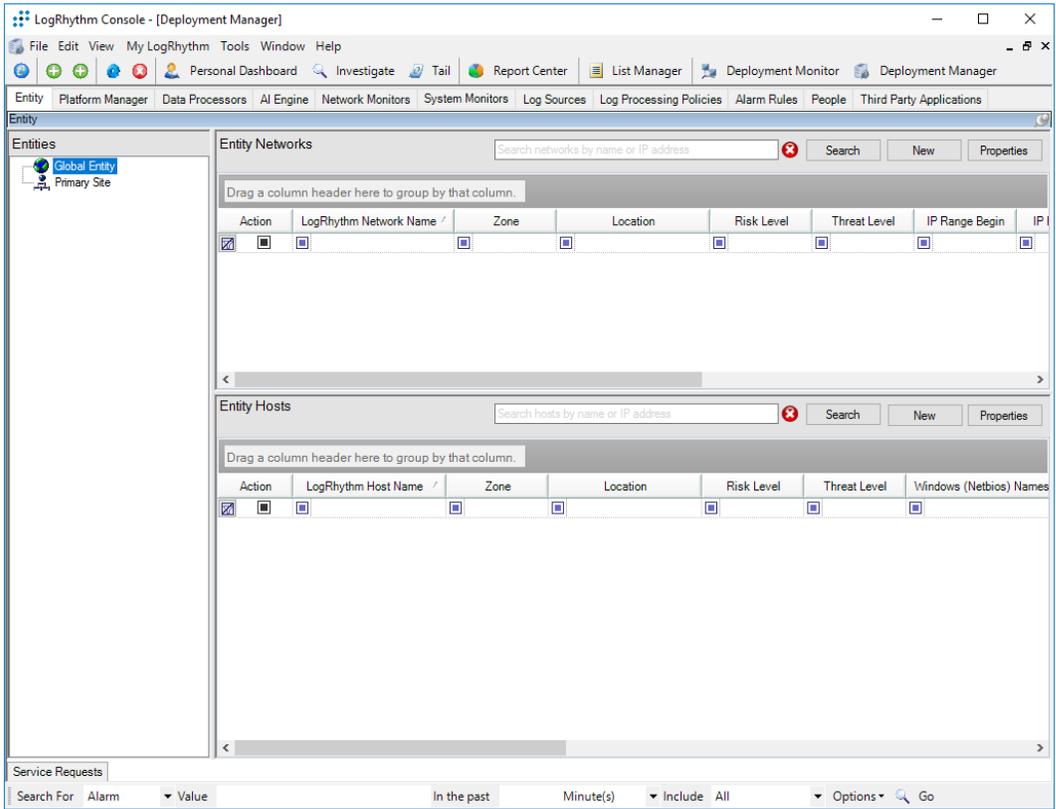
- 1279 2. Navigate to the **Deployment Manager** in the menu ribbon.



1280

1281

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



1282

1283

1284

1285

1286

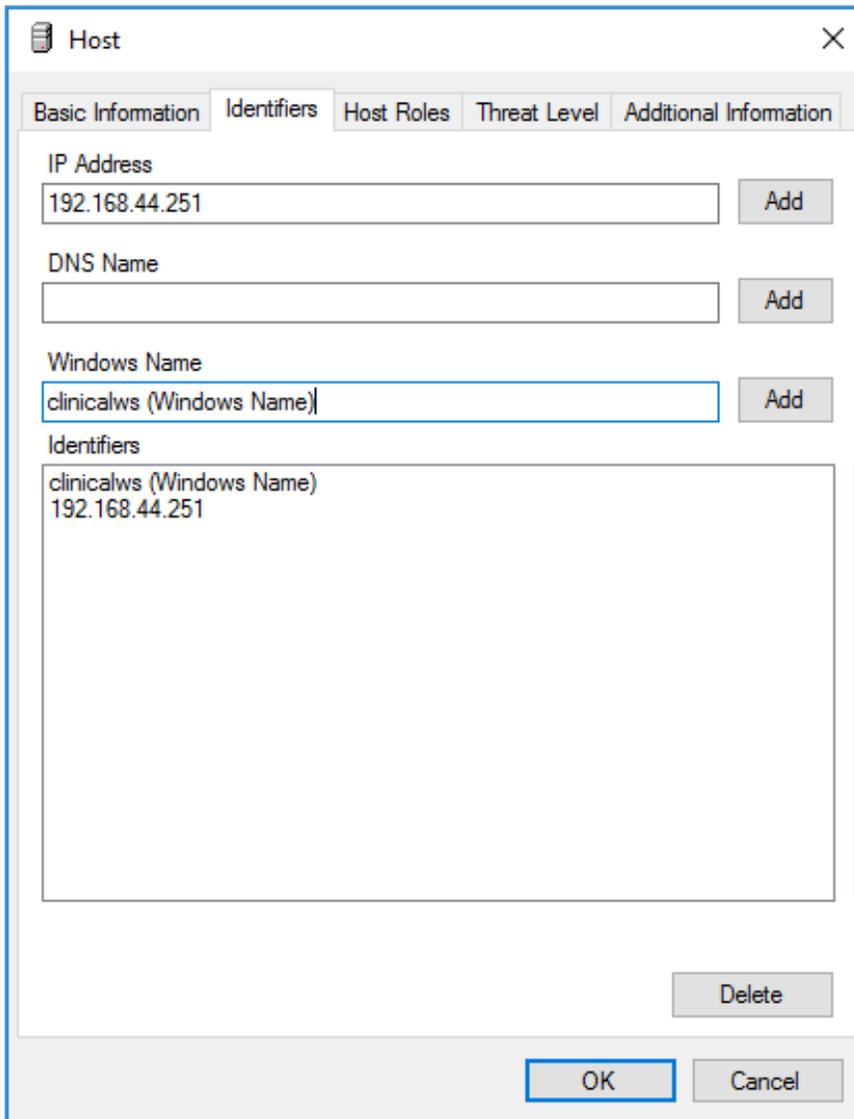
4. Click **New** to open the **Host** pop-up window, and enter the following under the **Basic Information** tab:
 - a. **Name:** ClinicalWS
 - b. **Host Zone:** Internal

The screenshot shows a 'Host' configuration window with the following fields and options:

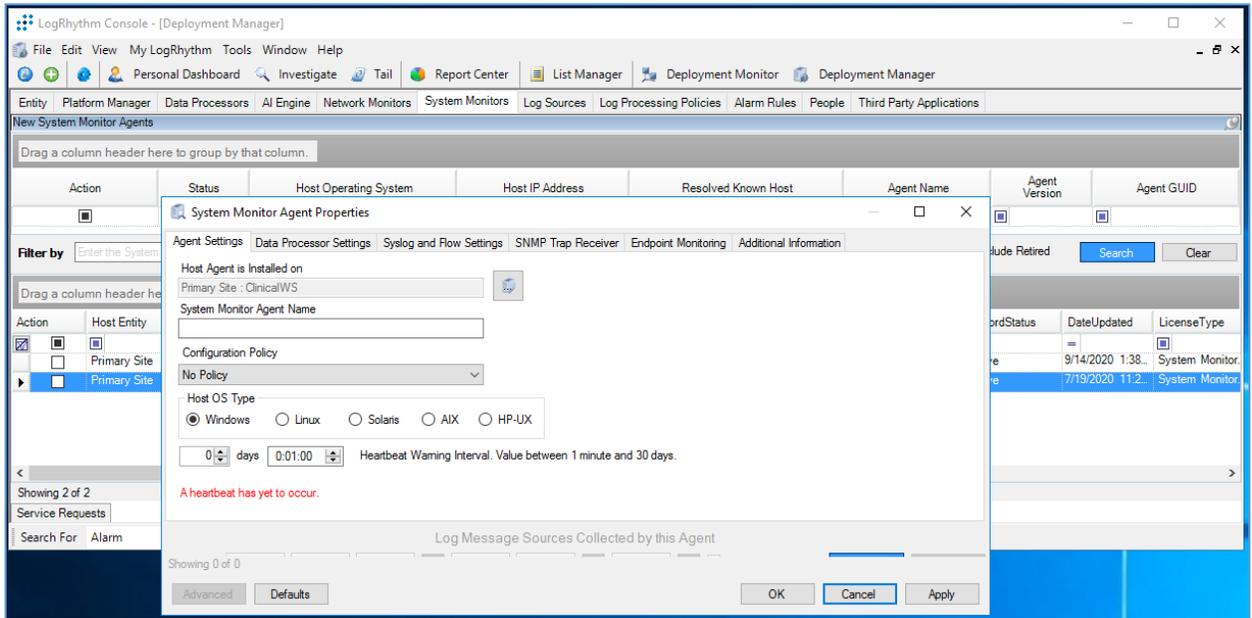
- Name:** ClinicalWS
- Host Zone:** Internal (selected), DMZ, External
- Operating System:** Windows
- Operating System Version:** Windows 10
- Host Location:** (Empty field)
- Brief Description:** (Empty text area)
- Host Risk Level:** 0 None (no risk)
- Windows Event Log Credentials:**
 - Use specified credentials
 - Password:** (Empty field)
 - Username (domain\username):** (Empty field)
 - Confirm Password:** (Empty field)

Buttons: OK, Cancel

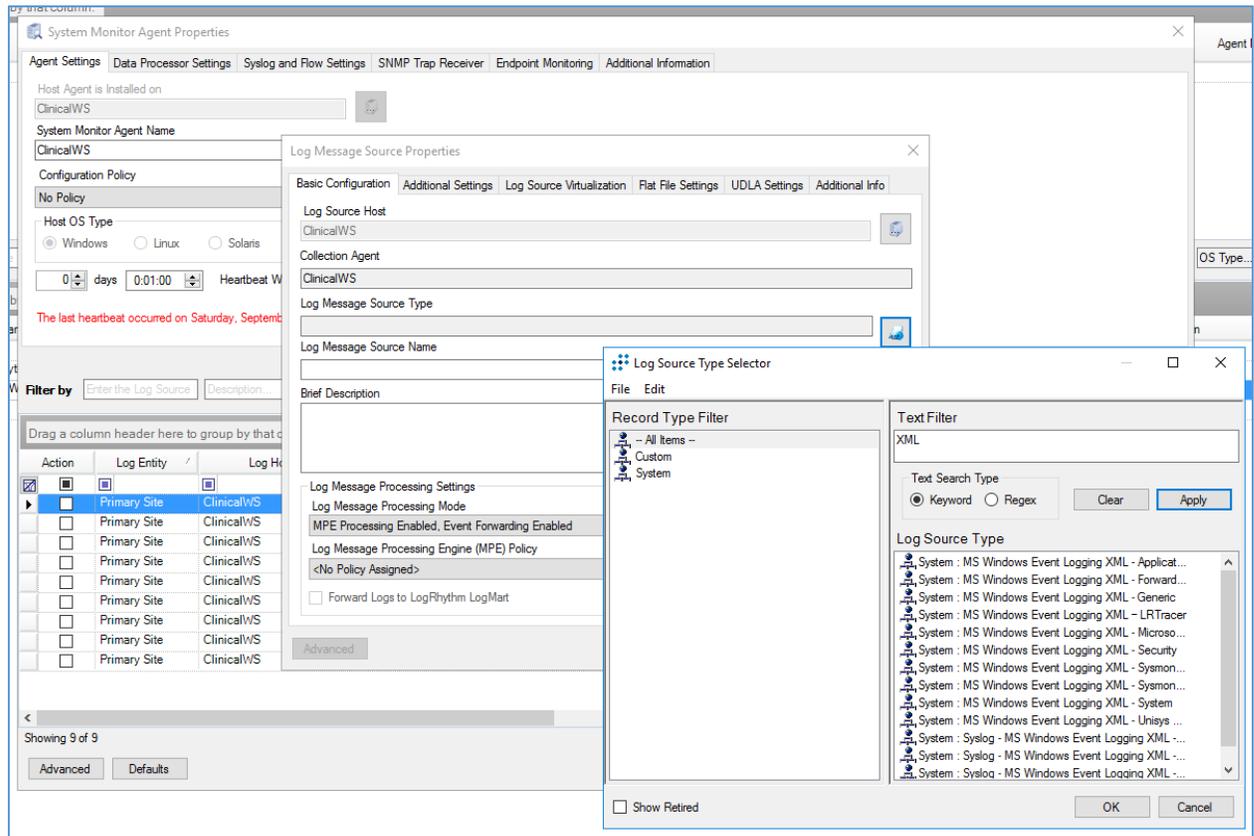
- 1287 5. Navigate to the **Identifiers** tab, provide the following information in the appropriate fields, and
1288 click **Add**.
- 1289 a. **IP Address:** 192.168.44.251
- 1290 b. **Windows Name:** clinicalws (Windows Name)



- 1291 6. Add the **ClinicalWS** as a new system monitor agent by navigating to the **System Monitors** tab,
1292 right-clicking in the empty space, and selecting **New**.
- 1293 7. In the System Monitor Agent Properties window, click the button next to **Host Agent is Installed**
1294 **on**, and select **Primary Site: ClinicalWS**.



- 1295 8. Go to **System Monitors**.
- 1296 9. Double-click **ClinicalWS**.
- 1297 10. Under **LogSource** of the **System Monitor Agent Property** window, right-click in the empty space,
1298 and select **New**. The **Log Message Source Property** window will open.
- 1299 11. Under the **Log Message Source Property** window, click the button associated with **Log Message**
1300 **Source Type**. It will open the **Log Source Selector** window.
- 1301 12. In the text box to the right of the **Log Source Selector** window, type **XML**, and click **Apply**.
- 1302 13. Select the **Log Source Type**, and click **OK**.



1303 2.2.4 Data Security

1304 Data security controls align with the NIST Cybersecurity Framework's PR.DS category. For this practice
 1305 guide, the Onclave Networks solution was implemented as a component in the simulated patient home
 1306 and simulated telehealth platform provider cloud environment. The Onclave Networks suite of tools
 1307 provides secure communication between the two simulated environments when using broadband
 1308 communications to exchange data.

1309 2.2.4.1 Onclave SecureIoT

1310 The Onclave SecureIoT deployment consists of six components: Onclave Blockchain, Onclave
 1311 Administrator Console, Onclave Orchestrator, Onclave Bridge, and two Onclave Gateways. These
 1312 components work together to provide secure network sessions between the deployed gateways.

1313 **Onclave SecureIoT Virtual Appliance Prerequisites**

1314 All Onclave devices require Debian 9.9/9.11/9.13. In addition, please prepare the following:

- 1315 1. GitHub account.

1316 2. Request an invitation to the Onclave Github account.

1317 Once the GitHub invitation has been accepted and a Debian VM has been installed in the virtual
1318 environment, download and run the installation script to prepare the VM for configuration.

1319 1. Run the command `sudo apt-get update`

1320 2. Run the command `apt install git -y`

1321 3. Run the command `sudo apt install openssh-server`

1322 4. Run the command `git clone`

1323 `https://readonly:Sh1bboleth45@gitlab.onclave.net/onclave/build/install.git`

1324 5. Navigate to the `/home/onclave/install` directory.

1325 6. Run the command `chmod +x *.sh`

1326 This process can be repeated for each virtual appliance that is deployed. The following guidance
1327 assumes the system user is named **onclave**.

1328 **Onclave SecureIoT Blockchain Appliance Information**

1329 **CPU:** 4

1330 **RAM:** 8 GB

1331 **Storage:** 120 GB (Thick Provision)

1332 **Network Adapter 1:** VLAN 1317

1333 **Operating System:** Debian Linux 9.11

1334 **Onclave SecureIoT Blockchain Appliance Configuration Guide**

1335 Before starting the installation script, prepare an answer for each question. The script will configure the
1336 server, assign a host name, create a self-signed certificate, and start the required services.

1337 1. Run the command `nano/etc/hosts`

1338 a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device,
1339 as well as Onclave's docker server. This will include:

1340 i. 192.168.5.11 tele-adco.trpm.hclab

1341 ii. 192.168.5.12 tele-orch.trpm.hclab

1342 iii. 192.168.5.13 tele-bg.trpm.hclab

- 1343 iv. 192.168.5.14 tele-gw1.trpm.hclab
- 1344 v. 192.168.21.10 tele-gw2.trpm.hclab
- 1345 vi. 38.142.224.131 docker.onclave.net
- 1346 2. Save the **file** and **exit**.
- 1347 3. Navigate to the **/home/onclave/install** directory.
- 1348 4. Run the command `./go.sh` and fill out the following information:
- 1349 a. **What type of device is being deployed?:** bci
- 1350 b. **Enter device hostname (NOT FQDN):** tele-bci
- 1351 c. **Enter device DNS domain name:** trpm.hclab
- 1352 d. **Enter the public NIC:** ens192
- 1353 e. **Enter the private NIC, if does not exist type in NULL:** NULL
- 1354 f. **Enter the IP Settings (DHCP or Static):** PUBLIC NIC (Static)
- 1355 i. address 192.168.5.10
- 1356 ii. netmask 255.255.255.0
- 1357 iii. gateway 192.168.5.1
- 1358 iv. dns-nameservers 192.168.1.10
- 1359 g. **What is the BCI FQDN for this environment?:** tele-bci.trpm.hclab
- 1360 h. **Enter the Docker Service Image Path:** NULL
- 1361 i. **Will system need TPM Emulator? (yes/no):** no
- 1362 j. **Keystore/Truststore password to be used?:** Onclave56
- 1363 k. **GitLab Username/Password (format username:password):** readonly:Sh1bboleth45
- 1364 5. Wait for the **Blockchain server** to reboot.
- 1365 6. Login to the appliance.
- 1366 7. Run the command `su root` and enter the password.
- 1367 8. Wait for the configuration process to finish.
- 1368 **Onclave SecureIoT Administrator Console Appliance Information**

1369 **CPU:** 4

1370 **RAM:** 8 GB

1371 **Storage:** 32 GB (Thick Provision)

1372 **Network Adapter 1:** VLAN 1317

1373 **Operating System:** Debian Linux 9.11

1374 **Onclave SecureIoT Administrator Console Appliance Configuration Guide**

1375 1. Run the command `scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-`
1376 `bci.trpm.hclab.crt /root/certs`

1377 2. Run the command `nano/etc/hosts`

1378 a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device,
1379 as well as Onclave's docker server. This will include:

1380 i. 192.168.5.10 tele-bci.trpm.hclab

1381 ii. 192.168.5.12 tele-orch.trpm.hclab

1382 iii. 192.168.5.13 tele-bg.trpm.hclab

1383 iv. 192.168.5.14 tele-gw1.trpm.hclab

1384 v. 192.168.21.10 tele-gw2.trpm.hclab

1385 vi. 38.142.224.131 docker.onclave.net

1386 b. Save the **file** and **exit**.

1387 3. Navigate to the **/home/onclave/install** directory.

1388 4. Run the command `chmod +x *.sh`

1389 5. Run the command `./go.sh` and fill out the following information:

1390 a. **What type of device is being deployed?:** adco

1391 b. **Enter device hostname (NOT FQDN):** tele-adco

1392 c. **Enter device DNS domain name:** trpm.hclab

1393 d. **Enter the public NIC:** ens192

1394 e. **Enter the private NIC, if does not exist type in NULL:** NULL

- 1395 f. **Enter the IP Settings (DHCP or Static): PUBLIC NIC (Static)**
- 1396 i. address 192.168.5.11
- 1397 ii. netmask 255.255.255.0
- 1398 iii. gateway 192.168.5.1
- 1399 iv. dns-nameservers 192.168.1.10
- 1400 g. **What is the BCI FQDN for this environment?:** tele-bci.trpm.hclab
- 1401 h. **Enter the Docker Service Image Path:** NULL
- 1402 i. **Will system need TPM Emulator? (yes/no):** yes
- 1403 j. **Keystore/Truststore password to be used?:** Onclave56
- 1404 k. **GitLab Username/Password (format username:password):** readonly:Sh1bboleth45
- 1405 6. Wait for the **Administrator Console server** to reboot.
- 1406 7. Login to the appliance.
- 1407 8. Run the command `su root` and enter the password.
- 1408 9. Wait for the configuration process to finish.
- 1409 10. Navigate to the **/home/onclave** directory.
- 1410 11. Run the command `docker pull docker.onclave.net/orchestrator-service:1.1.0`
- 1411 12. Run the command `docker pull docker.onclave.net/bridge-service:1.1.0`
- 1412 13. Run the command `docker pull docker.onclave.net/gateway-service:1.1.0`
- 1413 **Administrator Console Initialization and Bundle Creation**
- 1414 1. Using a web browser, navigate to **https://tele-adco.trpm.hclab**.
- 1415 2. Click **Verify**.
- 1416 3. Provide the following information:
- 1417 a. **Software ID** (provided by Onclave)
- 1418 b. **Password** (provided by Onclave)
- 1419 c. **PIN** (provided by Onclave)
- 1420 4. Provide the following information to create a superuser account:

- 1421 a. **First Name:** *****
- 1422 b. **Last Name:** *****
- 1423 c. **Username:** *****@email.com
- 1424 d. **Password:** *****
- 1425 e. **Organization Name:** NCCoEHC
- 1426 5. Click **Software Bundles**.
- 1427 6. Click the **plus symbol** (top right), and provide the following information:
 - 1428 a. **Bundle name:** nccoe-tele-orch
 - 1429 b. **Bundle type:** Orchestrator
 - 1430 c. **Owned by:** NCCoEHC
 - 1431 d. **Orchestrator owner name:** HCLab
 - 1432 e. **PIN:** ****
 - 1433 f. **Password:** *****
- 1434 7. Click **Create**.
- 1435 8. Click the **plus symbol** (top right), and provide the following information:
 - 1436 a. **Bundle name:** nccoe-tele-bg
 - 1437 b. **Bundle type:** Bridge
 - 1438 c. **Owned by:** NCCoEHC
- 1439 9. Click **Create**.
- 1440 10. Click the **plus symbol** (top right), and provide the following information:
 - 1441 a. **Bundle name:** nccoe-tele-gw
 - 1442 b. **Bundle type:** Gateway
 - 1443 c. **Owned by:** NCCoEHC
- 1444 11. Click **Create**.
- 1445 **Transfer Ownership of Onclave Devices to the Orchestrator**

1446 Once each Onclave device has been created and provisioned, it will show up in the Admin Console's web
1447 GUI. From here, the devices can be transferred to the Orchestrator with the following steps:

- 1448 1. Using a web browser, navigate to **https://tele-adco.trpm.hclab**.
- 1449 2. Click **Devices**.
- 1450 3. Select the **checkbox** next to **tele-bg**, **tele-gw1**, and **tele-gw2**.
- 1451 4. Click **Transfer ownership**.
- 1452 5. Under **Select a new owner**, select **HCLab**.
- 1453 6. Click **Transfer ownership**.

1454 Onclave SecureIoT Orchestrator Appliance Information

1455 **CPU:** 4

1456 **RAM:** 8 GB

1457 **Storage:** 32 GB (Thick Provision)

1458 **Network Adapter 1:** VLAN 1317

1459 **Operating System:** Debian Linux 9.11

1460 Onclave SecureIoT Orchestrator Appliance Configuration Guide

1461 1. Run the command `scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-`
1462 `bci.trpm.hclab.crt /root/certs`

1463 2. Run the command `nano/etc/hosts`

1464 a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device, as
1465 well as Onclave's docker server. This will include:

1466 i. 192.168.5.10 tele-bci.trpm.hclab

1467 ii. 192.168.5.11 tele-adco.trpm.hclab

1468 iii. 192.168.5.13 tele-bg.trpm.hclab

1469 iv. 192.168.5.14 tele-gw1.trpm.hclab

1470 v. 192.168.21.10 tele-gw2.trpm.hclab

1471 vi. 38.142.224.131 docker.onclave.net

1472 b. Save the **file** and **exit**.

- 1473 3. Run the command `nano /etc/network/interfaces`
- 1474 a. Edit the **Interfaces** file to include:
- 1475 i. `iface ens192 inet static`
- 1476 1. `address 192.68.5.12`
- 1477 2. `netmask 255.255.255.0`
- 1478 3. `gateway 192.168.5.1`
- 1479 4. `dns-nameservers 192.168.1.10`
- 1480 b. Save the **file** and **exit**.
- 1481 4. Run the command `git clone https://github.com/Onclave-Networks/orch.git`
- 1482 5. Navigate to the **/home/onclave/orch** directory.
- 1483 6. Run the command `chmod +x *.sh`
- 1484 7. Run the command `./go.sh` and fill out the following information:
- 1485 a. **What will be the hostname for your orchestrator?:** tele-orch
- 1486 b. **What will be the domain name for your orchestrator?:** trpm.hclab
- 1487 c. **Enter the device's public NIC:** ens192
- 1488 d. **What is the Blockchain environment?:** tele-bci
- 1489 e. **Will system need TPM Emulator? (yes/no):** yes
- 1490 f. **What is the docker image for the Orchestrator Service?:** docker.onclave.net/orchestrator-
1491 service:1.1.0- nccoe-tele-orch
- 1492 8. Reboot the **Orchestrator server**.
- 1493 9. Using a web browser, navigate to **https://tele-orch.trpm.hclab**.
- 1494 10. Click **Verify**.
- 1495 11. Provide the following information (created when making the bundle in the Admin Console):
- 1496 a. **Software ID**
- 1497 b. **Password**
- 1498 c. **PIN**

1499 12. Provide the following information to create a superuser account:

- 1500 a. **First Name:** *****
- 1501 b. **Last Name:** *****
- 1502 c. **Username:** *****@email.com
- 1503 d. **Password:** *****
- 1504 e. **Organization Name:** Telehealth Lab

1505 **Create a Customer in the Orchestrator**

- 1506 1. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
- 1507 2. Click **Customers.**
- 1508 3. Click the **plus symbol.**
- 1509 4. Under **Attributes > Customer Name**, enter **Telehealth Lab.**
- 1510 5. Click **Create.**

1511 **Create a Secure Enclave**

1512 Once each Onclave device has been transferred to the Orchestrator, it will show up in the Orchestrator's
1513 web GUI. From here, the secure enclave can be created with the following steps:

- 1514 1. Using a web browser, navigate to **https://tele-orch.trpm.hclab.**
- 1515 2. Click **Secure Enclaves.**
- 1516 3. Click the **plus symbol.**
- 1517 4. Under **General**, provide the following information:
 - 1518 a. **Secure Enclave name:** TeleHealth Secure Enclave
 - 1519 b. **Customer:** Telehealth Lab
 - 1520 c. **Sleeve ID:** 51
- 1521 5. Under **Subnets**, provide a **Network Address (CIDR notation)** of **192.168.50.0/24.**
- 1522 6. Under **Session Key**, provide a **Lifespan (minutes)** of **60.**
- 1523
- 1524 7. Click **Create.**

1525 **Prepare the Bridge for Inclusion in the Secure Enclave**

- 1526 1. Using a web browser, navigate to **<https://tele-orch.trpm.hclab>**.
- 1527 2. Click **Devices**.
- 1528 3. Select the **bridge**, and provide the following information:
 - 1529 a. **Device Name:** tele-bg
 - 1530 b. **Customer:** Telehealth Lab
 - 1531 c. **Secure Enclaves:** Not assigned to any Secure Enclave
 - 1532 d. **State:** Orchestrator Acquired
 - 1533 e. **Secure tunnel port number:** 820
 - 1534 f. **Private interface IP address undefined:** checked
- 1535 4. Click **Save**.

1536 **Prepare the Telehealth Gateway for Inclusion in the Secure Enclave**

- 1537 1. Using a web browser, navigate to **<https://tele-orch.trpm.hclab>**.
- 1538 2. Click **Devices**.
- 1539 3. Select the **bridge**, and provide the following information:
 - 1540 a. **Device Name:** tele-gw1
 - 1541 b. **Customer:** Telehealth Lab
 - 1542 c. **Secure Enclaves:** Not assigned to any Secure Enclave
 - 1543 d. **State:** Orchestrator Acquired
 - 1544 e. **Secure tunnel port number:** 820
 - 1545 f. **Private interface IP address undefined:** checked
- 1546 4. Click **Save**.

1547 **Prepare the Home Gateway for Inclusion in the Secure Enclave**

- 1548 1. Using a web browser, navigate to **<https://tele-orch.trpm.hclab>**.
- 1549 2. Click **Devices**.
- 1550 3. Select the **bridge**, and provide the following information:

- 1551 a. **Device Name:** tele-gw2
- 1552 b. **Customer:** Telehealth Lab
- 1553 c. **Secure Enclaves:** Not assigned to any Secure Enclave
- 1554 d. **State:** Orchestrator Acquired
- 1555 e. **Secure tunnel port number:** 820
- 1556 f. **Private interface IP address undefined:** checked

1557 4. Click **Save**.

1558 **Establish the Secure Enclave**

1559 Once the secure enclave has been created and each Onclave device has been configured with a name
1560 and customer, the secure enclave can be established with the following steps:

- 1561 1. Using a web browser, navigate to **<https://tele-orch.trpm.hclab>**.
- 1562 2. Click **Secure Enclaves**.
- 1563 3. Click the **edit symbol** for the previously created secure enclave.
- 1564 4. Under **Topology**, click **Add a Bridge**.
- 1565 5. Select **tele-bg**.
- 1566 6. Click **Add**.
- 1567 7. Click **Add a Gateway**.
- 1568 8. Select **tele-gw1**.
- 1569 9. Click **Add**.
- 1570 10. Click **Add a Gateway**.
- 1571 11. Select **tele-gw2**.
- 1572 12. Click **Add**.
- 1573 13. Under **Topology Controls**, toggle on **Approve topology**.
- 1574 14. Click **Save Changes**.
- 1575 15. Click **Devices**.
- 1576 16. Refresh the **Devices** page until each device is labeled as **Topology Approved**.

- 1577 17. Click **Secure Enclaves**.
- 1578 18. Click the **edit symbol** for the previously created secure enclave.
- 1579 19. Under **Topology**, toggle on **Trust All Devices**.
- 1580 20. Click **Save Changes**.
- 1581 21. Click **Devices**.
- 1582 22. Refresh the **Devices** page until each device is labeled as **Secured**.

1583 **Onclave SecureIoT Bridge Appliance Information**

1584 **CPU:** 4

1585 **RAM:** 8 GB

1586 **Storage:** 32 GB (Thick Provision)

1587 **Network Adapter 1:** VLAN 1317

1588 **Network Adapter 2:** VLAN 1319

1589 **Operating System:** Debian Linux 9.11

1590 **Onclave SecureIoT Bridge Appliance Configuration Guide**

- 1591 1. Run the command `scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-`
1592 `bci.trpm.hclab.crt /root/certs`
- 1593 2. Run the command `nano /etc/hosts`
- 1594 a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device,
1595 as well as Onclave's docker server. This will include:
- 1596 i. 192.168.5.10 tele-bci.trpm.hclab
- 1597 ii. 192.168.5.11 tele-adco.trpm.hclab
- 1598 iii. 192.168.5.12 tele-orch.trpm.hclab
- 1599 iv. 192.168.5.14 tele-gw1.trpm.hclab
- 1600 v. 192.168.21.10 tele-gw2.trpm.hclab
- 1601 vi. 38.142.224.131 docker.onclave.net
- 1602 3. Run the command `nano /etc/network/interfaces`

- 1603 a. Edit the **Interfaces** file to include:
- 1604 i. `iface ens192 inet static`
- 1605 1. `address 192.68.5.13`
- 1606 2. `netmask 255.255.255.0`
- 1607 3. `gateway 192.168.5.1`
- 1608 4. `dns-nameservers 192.168.1.10`
- 1609 ii. `iface ens224 inet static`
- 1610 b. Save the **file** and **exit**.
- 1611 4. Run the command `git clone https://github.com/Onclave-Networks/bridge.git`
- 1612 5. Navigate to the **/home/onclave/bridge** directory.
- 1613 6. Run the command `chmod +x *.sh`
- 1614 7. Run the command `./go.sh`
- 1615 a. **What will be the hostname for your bridge?:** tele-bg
- 1616 b. **What will be the domain name for your bridge?:** trpm.hclab
- 1617 c. **Enter the device's public NIC:** ens192
- 1618 d. **Enter the device's private NIC:** ens224
- 1619 e. **What is the Blockchain environment?:** tele-bci
- 1620 f. **Will system need TPM Emulator? (yes/no):** yes
- 1621 g. **What is the docker image for the Bridge Service?:** docker.onclave.net/bridge-
1622 service:1.1.0- nccoe-tele-bg
- 1623 8. Reboot the **Bridge server**.

1624 **Onclave SecureIoT Telehealth Gateway Appliance Information**

1625 **CPU:** 2

1626 **RAM:** 8 GB

1627 **Storage:** 16 GB

1628 **Network Adapter 1:** VLAN 1317

1629 **Network Adapter 2:** VLAN 1349

1630 **Operating System:** Debian Linux 9.11

1631 **Onclave SecureIoT Telehealth Gateway Appliance Configuration Guide**

1632 1. Run the command `scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-`
1633 `bci.trpm.hclab.crt /root/certs`

1634 2. Run the command `nano /etc/hosts`

1635 a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device,
1636 as well as Onclave's docker server. This will include:

1637 i. 192.168.5.10 tele-bci.trpm.hclab

1638 ii. 192.168.5.11 tele-adco.trpm.hclab

1639 iii. 192.168.5.12 tele-orch.trpm.hclab

1640 iv. 192.168.5.13 tele-bg.trpm.hclab

1641 v. 192.168.21.10 tele-gw2.trpm.hclab

1642 vi. 38.142.224.131 docker.onclave.net

1643 3. Run the command `nano /etc/network/interfaces`

1644 a. Edit the **Interfaces** file to include:

1645 i. `iface enp3s0 inet static`

1646 1. `address 192.168.5.14`

1647 2. `netmask 255.255.255.0`

1648 3. `gateway 192.168.5.1`

1649 4. `dns-nameservers 192.168.1.10`

1650 ii. `iface ens224 inet dhcp`

1651 b. Save the **file** and **exit**.

1652 4. Run the command `git clone https://github.com/Onclave-Networks/gateway.git`

1653 5. Navigate to the `/home/onclave/gateway` directory.

1654 6. Run the command `chmod +x *.sh`

- 1655 7. Run the command `./go.sh`
- 1656 a. **What will be the hostname for your gateway?:** tele-gw1
- 1657 b. **What will be the domain name for your gateway?:** trpm.hclab
- 1658 c. **Enter the device's public NIC:** enp3s0
- 1659 d. **Enter the device's private NIC:** enp2s0
- 1660 e. **What is the Blockchain environment?:** tele-bci
- 1661 f. **Will system need TPM Emulator? (yes/no):** no
- 1662 g. **What is the docker image for the Gateway Service?:** docker.onclave.net/gateway-
1663 service:1.1.0- nccoe-tele-gw
- 1664 8. Reboot the **Gateway server**.

1665 **Onclave SecureIoT Home Wi-Fi Gateway Appliance Information**

1666 **CPU:** 1

1667 **RAM:** 4 GB

1668 **Storage:** 16 GB

1669 **Network Adapter 1:** VLAN 1332

1670 **Network Adapter 2:** VLAN 1350 (Wi-Fi)

1671 **Operating System:** Debian Linux 9.11

1672 **Onclave SecureIoT Home Wi-Fi Gateway Appliance Configuration Guide**

1673 1. Run the command `scp onclave@192.168.5.10:/home/onclave/blockchain/certs/tele-`
1674 `bci.trpm.hclab.crt /root/certs`

1675 2. Run the command `nano /etc/hosts`

1676 a. Edit the **Hosts** file to include the **IP address** and **domain name** of each Onclave device,
1677 as well as Onclave's docker server. This will include:

1678 i. 192.168.5.10 tele-bci.trpm.hclab

1679 ii. 192.168.5.11 tele-adco.trpm.hclab

1680 iii. 192.168.5.12 tele-orch.trpm.hclab

1681 iv. 192.168.5.13 tele-bg.trpm.hclab

- 1682 v. 192.168.5.14 tele-gw1.trpm.hclab
- 1683 vi. 38.142.224.131 docker.onclave.net
- 1684 3. Run the command `nano /etc/network/interfaces`
- 1685 a. Edit the **Interfaces** file to include:
- 1686 i. `iface enp3s0 inet static`
- 1687 1. `address 192.168.21.10`
- 1688 2. `netmask 255.255.255.0`
- 1689 3. `gateway 192.168.21.1`
- 1690 4. `dns-nameservers 192.168.1.10`
- 1691 ii. `iface br0 inet static`
- 1692 1. `bridge_ports br51 wlp5s0`
- 1693 iii. `iface wlp5s0 inet manual`
- 1694 b. Save the **file** and **exit**.
- 1695 4. Run the command `git clone https://github.com/Onclave-Networks/hostapd-29.git`
- 1696 5. Navigate to the **/home/onclave/hostapd-29** directory.
- 1697 6. Run the command `chmod +x *.sh`
- 1698 7. Run the command `./hostapd-29.sh`
- 1699 8. Navigate to the **/home/onclave** directory.
- 1700 9. Run the command `git clone https://github.com/Onclave-Networks/hostapd-client.git`
- 1701 10. Navigate to the **/home/onclave/hostapd-client** directory.
- 1702 11. Run the command `chmod +x *.sh`
- 1703 12. Run the command `./hostapd-client.sh`
- 1704 13. Navigate to the **/home/onclave** directory.
- 1705 14. Run the command `git clone https://github.com/Onclave-Networks/gateway.git`
- 1706 15. Navigate to the **/home/onclave/gateway** directory.
- 1707 16. Run the command `chmod +x *.sh`

- 1708 17. Run the command `./go.sh`
- 1709 a. **What will be the hostname for your gateway?:** tele-gw2
- 1710 b. **What will be the domain name for your gateway?:** trpm.hclab
- 1711 c. **Enter the device's public NIC:** enp3s0
- 1712 d. **Enter the device's private NIC:** wlp5s0
- 1713 e. **What is the Blockchain environment?:** tele-bci
- 1714 f. **Will system need TPM Emulator? (yes/no):** no
- 1715 g. **What is the docker image for the Gateway Service?:** docker.onclave.net/ gateway-
- 1716 service:1.1.0- nccoe-tele-gw
- 1717 18. Reboot the **Gateway server**.

1718 **Appendix A List of Acronyms**

AD	Active Directory
CPU	Central Processing Unit
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
FMC	Firepower Management Center
FTD	Firepower Threat Defense
GB	Gigabyte
HDO	Healthcare Delivery Organization
HIS	Health Information System
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
NAT	Network Address Translation
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
OVA	Open Virtual Appliance or Application
PACS	Picture Archiving and Communication System
RAM	Random Access Memory
RPM	Remote Patient Monitoring
SFC	Stealthwatch Flow Collector
SIEM	Security Incident Event Management
SMC	Stealthwatch Management Center
SP	Special Publication
TB	Terabyte
URL	Uniform Resource Locator
vCPU	Virtual Central Processing Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
XDR	Extended Detection and Response

1719 **Appendix B** **References**

- 1720 [1] J. Cawthra et al., *Securing Picture Archiving and Communication System (PACS)*, National
1721 Institute of Standards and Technology (NIST) Special Publication 1800-24, NIST, Gaithersburg,
1722 Md., Sep. 2019. Available: [https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-pacs-nist-sp1800-24-draft.pdf)
1723 [pacs-nist-sp1800-24-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-pacs-nist-sp1800-24-draft.pdf).
- 1724 [2] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, Gaithersburg,
1725 Md., Apr. 16, 2018. Available:
1726 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- 1727 [3] Tenable. Managed by Tenable.sc. [Online]. Available:
1728 https://docs.tenable.com/nessus/8_10/Content/ManagedbyTenablesc.htm.
- 1729 [4] Microsoft. Install Active Directory Domain Services (Level 100). [Online]. Available:
1730 [https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-](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)
1731 [directory-domain-services--level-100-#to-install-ad-ds-by-using-server-manager](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).
- 1732 [5] Cisco. *Cisco Firepower Management Center Virtual Getting Started Guide*. [Online]. Available:
1733 [https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmfv/fpmc-](https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmfv/fpmc-virtual/fpmc-virtual-vmware.html)
1734 [virtual/fpmc-virtual-vmware.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmfv/fpmc-virtual/fpmc-virtual-vmware.html).
- 1735 [6] Cisco. *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide: Deploy the*
1736 *Firepower Threat Defense Virtual*. [Online]. Available:
1737 [https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-](https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg/ftdv-vmware-deploy.html)
1738 [vmware-gsg/ftdv-vmware-deploy.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg/ftdv-vmware-deploy.html).
- 1739 [7] Cisco. *Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide: Managing the*
1740 *Firepower Threat Defense Virtual with the Firepower Management Center*. [Online]. Available:
1741 [https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-](https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg/ftdv-vmware-fmc.html)
1742 [vmware-gsg/ftdv-vmware-fmc.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-gsg/ftdv-vmware-fmc.html).
- 1743 [8] Cisco. *Cisco Stealthwatch Installation and Configuration Guide 7.1*. [Online]. Available:
1744 [https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/system_installation config-](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)
1745 [uration/SW_7_1_Installation_and_Configuration_Guide_DV_1_0.pdf](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).
- 1746 [9] Cisco. Deploy VAs in VMware. [Online]. Available: [https://docs.umbrella.com/deployment-](https://docs.umbrella.com/deployment-umbrella/docs/deploy-vas-in-vmware)
1747 [umbrella/docs/deploy-vas-in-vmware](https://docs.umbrella.com/deployment-umbrella/docs/deploy-vas-in-vmware).