

# Data Integrity

## Identifying and Protecting Assets Against Ransomware and Other Destructive Events

---

**Volume C:**  
**How-To Guides**

**Jennifer Cawthra**

National Cybersecurity Center of Excellence  
NIST

**Michael Ekstrom**

**Lauren Lusty**

**Julian Sexton**

**John Sweetnam**

The MITRE Corporation  
McLean, Virginia

January 2020

DRAFT

This publication is available free of charge from <https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/identify-protect>.

## 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 sta-  
5 tus or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it in-  
6 tended 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 1800-25C, Natl. Inst. Stand. Technol.  
9 Spec. Publ. 1800-25C, 487 pages, (January 2020), 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: [ds-nccoe@nist.gov](mailto:ds-nccoe@nist.gov).

14 Public comment period: January 27, 2020 through February 25, 2020

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

16 National Cybersecurity Center of Excellence  
17 National Institute of Standards and Technology  
18 100 Bureau Drive  
19 Mailstop 2002  
20 Gaithersburg, MD 20899  
21 Email: [nccoe@nist.gov](mailto:nccoe@nist.gov)

## 22 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## 38 NIST CYBERSECURITY PRACTICE GUIDES

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

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

## 48 ABSTRACT

49 Ransomware, destructive malware, insider threats, and even honest user mistakes present ongoing  
50 threats to organizations. Organizations' data, such as database records, system files, configurations,  
51 user files, applications, and customer data, are all potential targets of data corruption, modification, and  
52 destruction. Formulating a defense against these threats requires two things: a thorough knowledge of  
53 the assets within the enterprise, and the protection of these assets against the threat of data corruption  
54 and destruction. The NCCoE, in collaboration with members of the business community and vendors of  
55 cybersecurity solutions, has built an example solution to address these data integrity challenges.

56 Multiple systems need to work together to identify and protect an organization’s assets against the  
 57 threat of corruption, modification, and destruction. This project explores methods to effectively identify  
 58 assets (devices, data, and applications) that may become targets of data integrity attacks, as well as the  
 59 vulnerabilities in the organization’s system that facilitate these attacks. It also explores methods to  
 60 protect these assets against data integrity attacks using backups, secure storage, integrity checking  
 61 mechanisms, audit logs, vulnerability management, maintenance, and other potential solutions

## 62 **KEYWORDS**

63 *attack vector; asset awareness; data integrity; data protection; malicious actor; malware; ransomware.*

## 64 **ACKNOWLEDGMENTS**

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

Name	Organization
Kyle Black	Bay Dynamics
Sunjeet Randhawa	Broadcom Inc.
Peter Romness	Cisco Systems
Matthew Hyatt	Cisco Systems
Hans Ismirnioglou	Cryptonite
Sapna George	Cryptonite
Justin Yackoski	Cryptonite
Steve Petruzzo	GreenTec USA
Steve Roberts	Micro Focus
Timothy McBride	NIST

Name	Organization
Christopher Lowde	Semperis
Thomas Leduc	Semperis
Darren Mar-Elia	Semperis
Kirk Lashbrook	Semperis
Mickey Bresman	Semperis
Jim Wachhaus	Tripwire
Humphrey Christian	Symantec Corporation
Jon Christmas	Symantec Corporation
Kenneth Durbin	Symantec Corporation
Matthew Giblin	Symantec Corporation
Nancy Correll	The MITRE Corporation
Chelsea Deane	The MITRE Corporation
Sallie Edwards	The MITRE Corporation
Milissa McGinnis	The MITRE Corporation
Karri Meldorf	The MITRE Corporation
Denise Schiavone	The MITRE Corporation

Name	Organization
Anne Townsend	The MITRE Corporation

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

Technology Partner/Collaborator	Build Involvement
Symantec Corporation	Symantec Data Loss Prevention v15.1
Cisco Systems	Cisco ISE v2.4, Cisco Web Security Appliance v10.1
GreenTec USA	GreenTec WORMdisk v151228
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7, Tripwire IP360 v9.0.1
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Cryptonite	CryptoniteNXT v2.9.1
Semperis	Semperis Active Directory Forest Recovery v2.5, Semperis Directory Services Protector v2.7

## 70 Contents

71	<b>1 Introduction .....</b>	<b>1</b>
72	1.1 How to Use this Guide.....	1
73	1.2 Build Overview .....	2
74	Typographic Conventions.....	3
75	<b>2 Product Installation Guides .....</b>	<b>3</b>
76	2.1 Active Directory and Domain Name System (DNS Server) .....	4
77	2.1.1 Installing Features.....	4
78	2.1.2 Creating a Certificate Authority.....	19
79	2.1.3 Configure Account to Add Computers to Domain.....	34
80	2.1.4 Adding Machines to the Domain .....	41
81	2.1.5 Configure Active Directory to Audit Account Activity .....	46
82	2.1.6 Configure Reverse Lookup Zones .....	48
83	2.2 Microsoft Exchange Server.....	54
84	2.2.1 Install Microsoft Exchange.....	54
85	2.3 Windows Server Hyper-V Role .....	65
86	2.3.1 Production Installation .....	65
87	2.4 MS SQL Server .....	73
88	2.4.1 Install and Configure MS SQL.....	73
89	2.4.2 Open Port on Firewall.....	83
90	2.4.3 Add a New Login to the Database .....	88
91	2.5 Microsoft IIS Server .....	90
92	2.5.1 Install IIS.....	90
93	2.5.2 IIS Configuration .....	98
94	2.6 GreenTec WORMdisks.....	102
95	2.6.1 Format GreenTec WORMdisks .....	103
96	2.6.2 Obtain Status Information About GreenTec WORMdisks .....	103
97	2.6.3 Map GreenTec WORMdisks to Drive Letters.....	104
98	2.6.4 Activate Write Protection in GreenTec WORMdisks .....	105

99	<b>2.7</b>	<b>CryptoniteNXT</b> .....	<b>109</b>
100	2.7.1	Configure Cryptonite NXT .....	109
101	2.7.1.1	Verify a New Device.....	109
102	2.7.1.2	Create a New User .....	112
103	2.7.1.3	Create a New Policy.....	115
104	2.7.2	Integrate CryptoniteNXT with Active Directory.....	122
105	2.7.2.1	Generate a Keytab File .....	122
106	2.7.2.2	Import Keytab File to ACC .....	129
107	<b>2.8</b>	<b>Backups</b> .....	<b>136</b>
108	2.8.1	FileZilla FTPS Server Setup .....	136
109	2.8.2	FileZilla Configuration .....	139
110	2.8.3	Add a User to FileZilla .....	144
111	2.8.4	Duplicati Client Installation (Windows) .....	146
112	2.8.5	Duplicati Client Installation (Ubuntu) .....	149
113	2.8.6	Configure Duplicati .....	150
114	<b>2.9</b>	<b>Semperis Active Directory Forest Recovery</b> .....	<b>155</b>
115	2.9.1	Install Semperis ADFR .....	155
116	2.9.2	Create a Backup Schedule for the Domain Controller.....	164
117	2.9.3	Recover the Active Directory Forest from a Backup.....	167
118	<b>2.10</b>	<b>Semperis Directory Services Protector</b> .....	<b>170</b>
119	2.10.1	Configure Active Directory for Semperis DSP .....	170
120	2.10.2	Install Semperis DSP .....	183
121	<b>2.11</b>	<b>Micro Focus ArcSight Enterprise Security Manager (ESM)</b> .....	<b>195</b>
122	2.11.1	Install the ArcSight Console .....	196
123	2.11.2	Install Individual ArcSight Windows Connectors .....	209
124	2.11.3	Install Individual ArcSight Ubuntu Connectors.....	227
125	2.11.4	Install a Connector Server for ESM on Windows 2012 R2.....	240
126	2.11.5	Install Preconfigured Filters for ArcSight.....	253

127	2.11.5.1	Install Activate Base.....	253
128	2.11.5.2	Install Packages.....	255
129	2.11.6	Apply Filters to a Channel.....	256
130	2.12	Tripwire Enterprise.....	257
131	2.12.1	Install Tripwire Enterprise.....	257
132	2.12.2	Install the Axon Bridge.....	270
133	2.12.3	Install the Axon Agent (Windows).....	270
134	2.12.4	Install the Axon Agent (Linux).....	271
135	2.12.5	Configure Tripwire Enterprise.....	272
136	2.12.5.1	Terminology.....	272
137	2.12.5.2	Tags.....	273
138	2.12.5.3	Rules.....	275
139	2.12.5.4	Tasks.....	279
140	2.13	Tripwire Log Center.....	283
141	2.13.1	Install Tripwire Log Center Manager.....	283
142	2.13.2	Configure Tripwire Log Center Manager.....	283
143	2.13.3	Install Tripwire Log Center Console.....	289
144	2.14	Cisco Web Security Appliance (WSA).....	289
145	2.14.1	Network Configuration.....	289
146	2.14.2	System Setup.....	290
147	2.14.3	Using WSA to Proxy Traffic.....	298
148	2.14.3.1	Creating a PAC File.....	299
149	2.14.3.2	Setting Up WPAD (Web Proxy Auto Discovery).....	301
150	2.14.3.3	Configure Group Policy to Use Explicit Proxy.....	304
151	2.14.4	Blacklisting.....	309
152	2.15	Symantec Data Loss Prevention.....	316
153	2.15.1	Install Oracle 12c Enterprise.....	316
154	2.15.2	Create an Oracle Database for Symantec DLP.....	323
155	2.15.3	Configuring the Oracle Listener.....	324

156	2.15.4	Install Symantec DLP.....	336
157	2.15.5	Configure Symantec DLP.....	346
158	2.16	Cisco Identity Services Engine (ISE).....	347
159	2.16.1	Initial Setup.....	347
160	2.16.2	Inventory: Configure SNMP on Routers/Network Devices.....	347
161	2.16.3	Inventory: Configure Device Detection .....	347
162	2.16.4	Policy Enforcement: Configure Active Directory Integration .....	351
163	2.16.5	Policy Enforcement: Enable Passive Identity with AD .....	354
164	2.16.6	Policy Enforcement: Developing Policy Conditions .....	359
165	2.16.7	Policy Enforcement: Developing Policy Results.....	361
166	2.16.8	Policy Enforcement: Enforcing a Requirement in Policy .....	362
167	2.16.9	Policy Enforcement: Configuring a Web Portal .....	363
168	2.16.10	Configuring RADIUS with Your Network Device .....	364
169	2.16.11	Configuring an Authentication Policy .....	365
170	2.16.12	Configuring an Authorization Policy .....	367
171	2.17	Tripwire IP360 .....	368
172	2.17.1	Installation .....	368
173	2.17.2	Web Portal .....	373
174	2.17.3	Scanning.....	374
175	2.18	Integration: Tripwire Log Center and Tripwire Enterprise.....	377
176	2.19	Integration: Tripwire Log Center (TLC) and Tripwire IP360 .....	384
177	2.19.1	Configure IP360 and Log Center .....	384
178	2.19.2	Collect Tripwire IP360 Operational Logs .....	387
179	2.19.3	Configure Tripwire IP360 Scan Results Forwarding.....	399
180	2.20	Integration: Tripwire Enterprise and Backups .....	412
181	2.20.1	Export Configuration from Tripwire Enterprise.....	413
182	2.20.2	Back Up the Tripwire Enterprise Configuration.....	413
183	2.21	Integration: Cisco ISE and CryptoniteNXT .....	413
184	2.21.1	Requirements for Integrating Cisco ISE and CryptoniteNXT.....	413
185	2.21.2	Configuring CryptoniteNXT for RADIUS .....	414
186	2.22	Integration: Backups and GreenTec.....	415

187	2.22.1	Locate Backups with FileZilla and Duplicati .....	415
188	2.22.2	Back Up to a GreenTec Disk .....	417
189	2.22.3	Configure Network-Accessible GreenTec Disk.....	418
190	2.22.4	Secure Storage for Semperis ADFR.....	420
191	2.23	Integration: Micro Focus ArcSight and FileZilla.....	421
192	2.23.1	Enable Logs in FileZilla .....	421
193	2.23.2	Install Micro Focus ArcSight.....	423
194	2.24	Integration: Micro Focus ArcSight and Tripwire .....	438
195	2.24.1	Install Micro Focus ArcSight.....	438
196	2.25	Integration: Micro Focus ArcSight and Cisco WSA.....	451
197	2.25.1	Configure Cisco WSA to Forward Logs.....	451
198	2.26	Integration: Micro Focus ArcSight and Cisco ISE.....	454
199	2.26.1	Configure Cisco ISE to Forward Logs.....	454
200	2.26.2	Select Logs for Forwarding .....	457
201	2.27	Integration: Micro Focus ArcSight and Symantec DLP.....	458
202	2.27.1	Install Micro Focus ArcSight.....	458
203	2.27.2	Configure Symantec DLP to Forward Logs.....	468
204	2.28	Integration: Micro Focus ArcSight and CryptoniteNXT .....	472
205	2.28.1	Configure CryptoniteNXT to Forward Logs to ArcSight .....	472
206	2.29	Integration: Micro Focus ArcSight and Semperis DSP .....	473
207	2.29.1	Configure Semperis DSP to Forward Logs .....	473
208	2.30	Integrations: CryptoniteNXT .....	474
209	2.30.1	Active Directory and DNS.....	475
210	2.30.2	Microsoft Exchange .....	476
211	2.30.3	FileZilla .....	477
212	2.30.4	GreenTec.....	477
213	2.30.5	Tripwire Enterprise .....	478
214	2.30.6	ArcSight ESM.....	478
215	2.30.7	Cisco ISE .....	479
216	2.30.8	Semperis DSP .....	480

217	2.30.9 Symantec DLP .....	480
218	2.30.10 Cisco WSA .....	481
219	2.30.11 Tripwire IP360.....	482
220	2.30.12 Tripwire Log Center, Tripwire IP360, Tripwire Enterprise, and ArcSight ESM.....	483
221	2.30.13 FileZilla and ArcSight.....	484
222	2.30.14 Cisco ISE and ArcSight.....	484
223	2.30.15 Cisco WSA and ArcSight .....	485
224	2.30.16 Semperis DSP and ArcSight.....	485
225	2.30.17 Symantec DLP and ArcSight .....	486

## 226 1 Introduction

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

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

### 234 1.1 How to Use this Guide

235 This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a  
236 standards-based reference design and provides users with the information they need to replicate the  
237 data integrity identify-and protect-solution. This reference design is modular and can be deployed in  
238 whole or in part.

239 This guide contains three volumes:

- 240     ▪ NIST SP 1800-25A: *Executive Summary*
- 241     ▪ NIST SP 1800-25B: *Approach, Architecture, and Security Characteristics* – what we built and why
- 242     ▪ NIST SP 1800-25C: *How-To Guides* – instructions for building the example solution (**you are**  
243         **here**)

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

245 **Business decision makers, including chief security and technology officers,** will be interested in the  
246 *Executive Summary* (NIST SP 1800-25A), which describes the following topics:

- 247     ▪ challenges that enterprises face in identifying assets and protecting them from data integrity  
248         events
- 249     ▪ example solution built at the NCCoE
- 250     ▪ benefits of adopting the example solution

251 **Technology or security program managers** who are concerned with how to identify, understand, assess,  
252 and mitigate risk will be interested in NIST SP 1800-25B, which describes what we did and why. The  
253 following sections will be of particular interest:

- 254       ▪ Section 3.4.1, *Assessing Risk Posture*, provides a description of the risk analysis we performed.
- 255       ▪ Section 3.4.2, *Security Control Map*, maps the security characteristics of this example solution
- 256           to cybersecurity standards and best practices.

257 You might share the *Executive Summary*, NIST SP 1800-25A, with your leadership team members to help  
258 them understand the importance of adopting standards-based data integrity solutions.

259 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.  
260 You can use this How-To portion of the guide, NIST SP 1800-25C, to replicate all or parts of the build  
261 created in our lab. This How-To portion of the guide provides specific product installation, configuration,  
262 and integration instructions for implementing the example solution. We do not recreate the product  
263 manufacturers’ documentation, which is generally widely available. Rather, we show how we  
264 incorporated the products together in our environment to create an example solution.

265 This guide assumes that IT professionals have experience implementing security products within the  
266 enterprise. While we have used a suite of commercial products to address this challenge, this guide  
267 does not endorse these particular products. Your organization can adopt this solution or one that  
268 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and  
269 implementing parts of a data integrity identify-and-protect solution. Your organization’s security experts  
270 should identify the products that will best integrate with your existing tools and IT system  
271 infrastructure. We hope that you will seek products that are congruent with applicable standards and  
272 best practices. Section 3.5 of Volume B, *Technologies*, lists the products we used and maps them to the  
273 cybersecurity controls provided by this reference solution.

274 A NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. This is a  
275 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and  
276 success stories will improve subsequent versions of this guide. Please contribute your thoughts to [ds-](mailto:ds-nccoe@nist.gov)  
277 [nccoe@nist.gov](mailto:ds-nccoe@nist.gov).

## 278 **1.2 Build Overview**

279 The National Cybersecurity Center of Excellence (NCCoE) built a hybrid virtual-physical laboratory  
280 environment to explore methods to effectively identify assets and protect them against a data  
281 corruption event in various IT enterprise environments. The NCCoE also explored identifying  
282 vulnerabilities in advance of an incident. The servers in the virtual environment were built to the  
283 hardware specifications of their specific software components.

284 The NCCoE worked with members of the Data Integrity Community of Interest to develop a diverse but  
 285 noncomprehensive set of use case scenarios against which to test the reference implementation. These  
 286 are detailed in Volume B, Section 5.2. For a detailed description of our architecture, see Volume B,  
 287 Section 4.

## 288 **Typographic Conventions**

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

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

## 290 **2 Product Installation Guides**

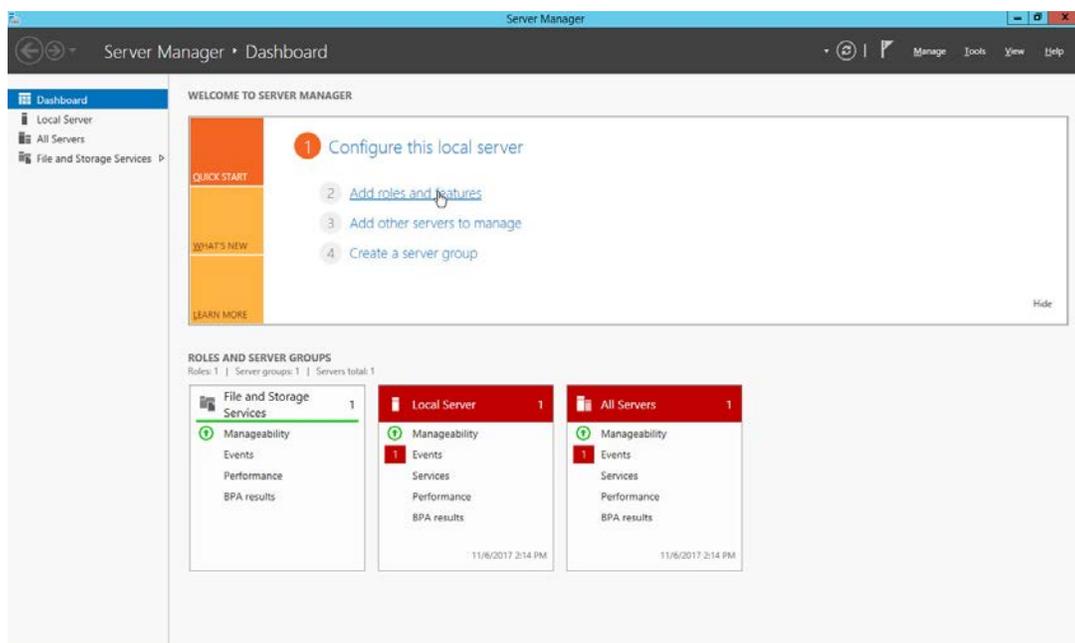
291 This section of the practice guide contains detailed instructions for installing and configuring all of the  
 292 products used to build an instance of the example solution.

## 293 2.1 Active Directory and Domain Name System (DNS Server)

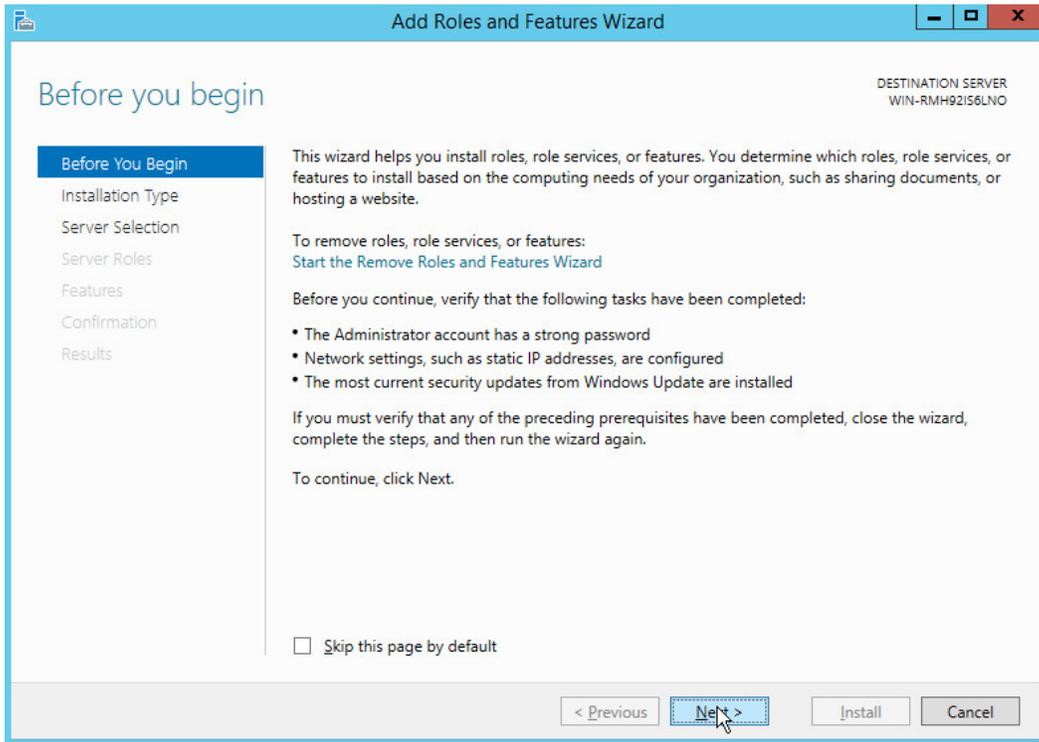
294 As part of our enterprise emulation, we included an Active Directory server that doubles as a DNS  
295 server. This section covers the installation and configuration process used to set up Active Directory and  
296 DNS on a Windows Server 2012 R2 machine.

### 297 2.1.1 Installing Features

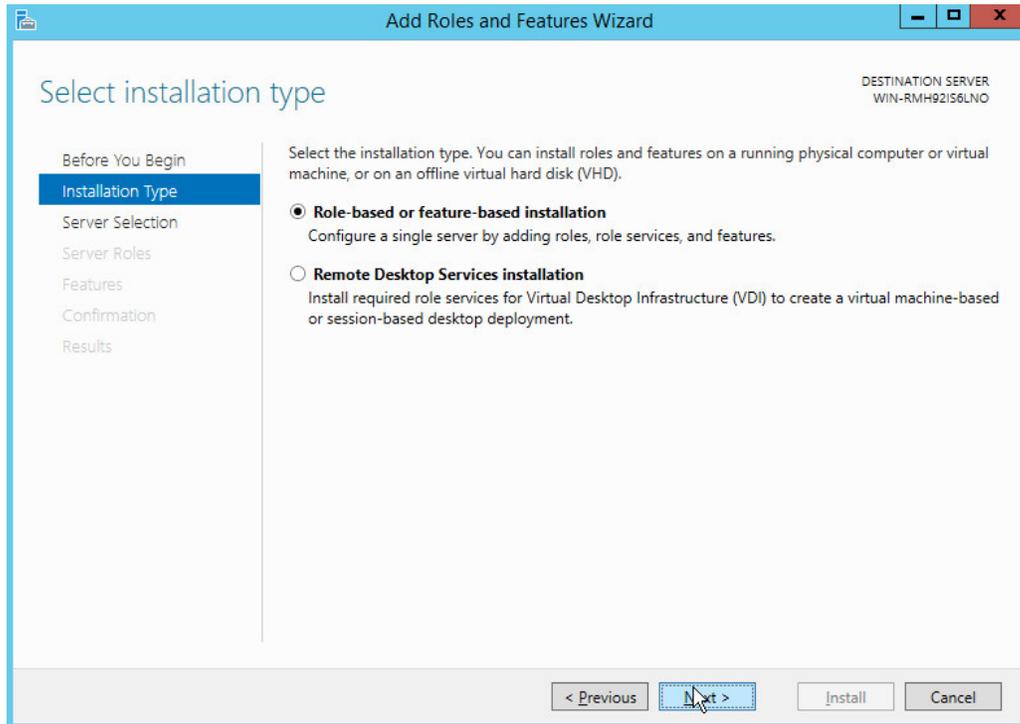
298 1. Open **Server Manager**.



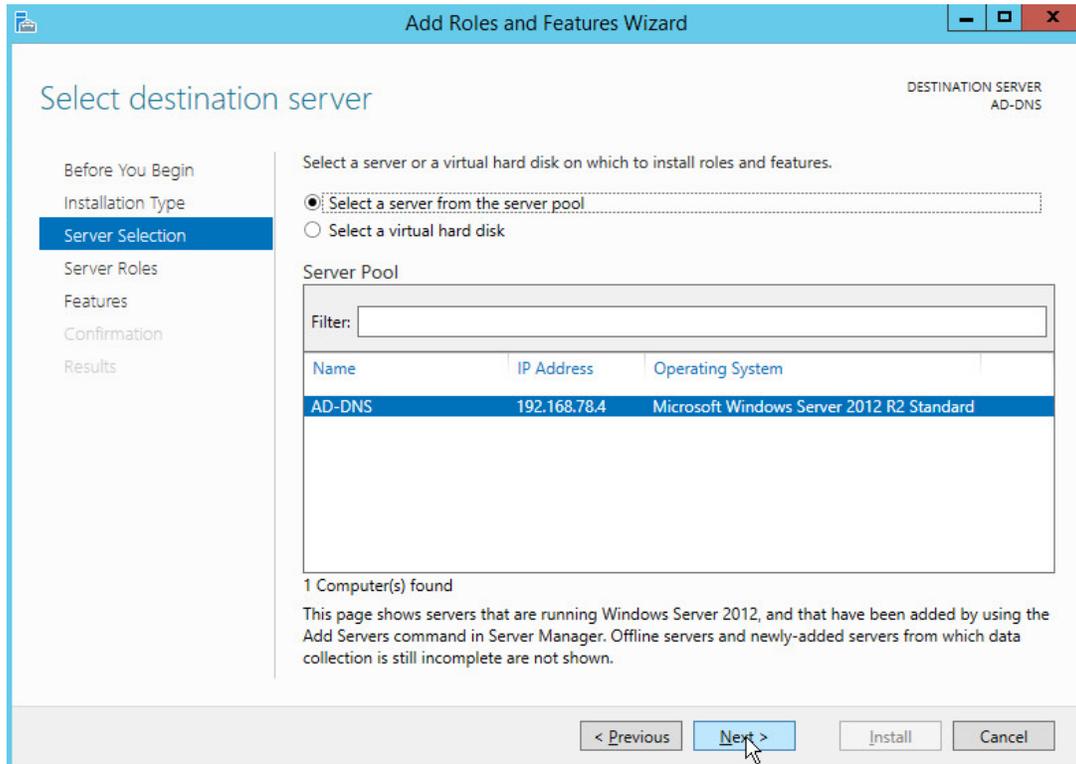
299 2. Click the link **Add roles and features**.



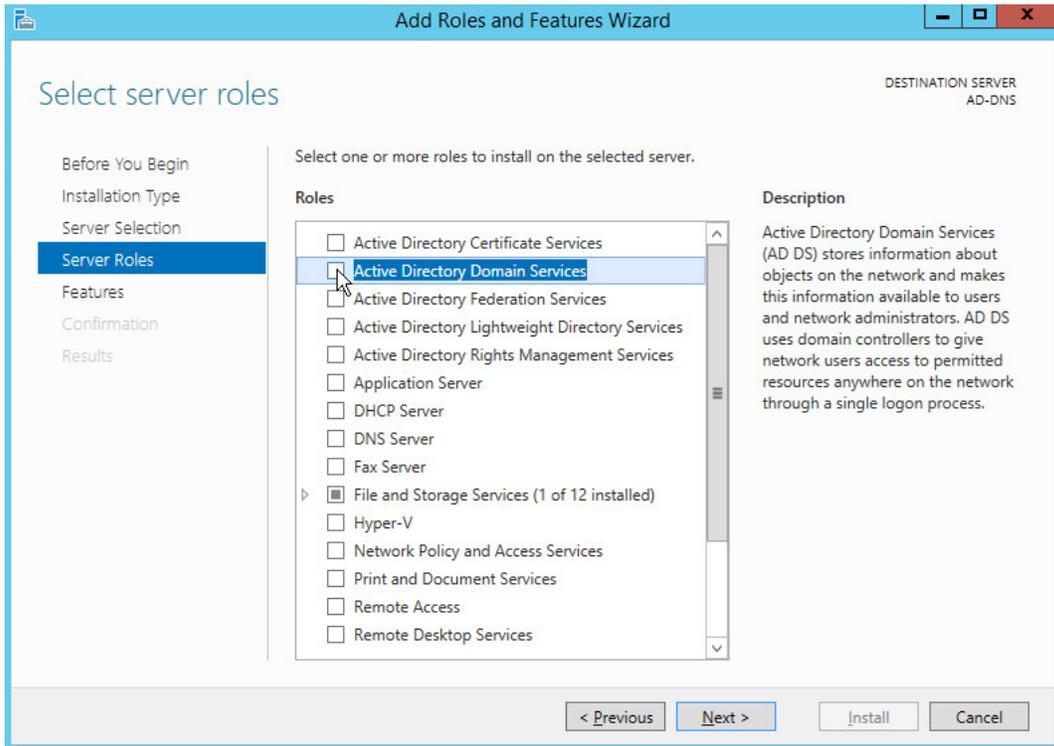
- 300 3. Click **Next**.
- 301 4. Select **Role-based or feature-based installation**.



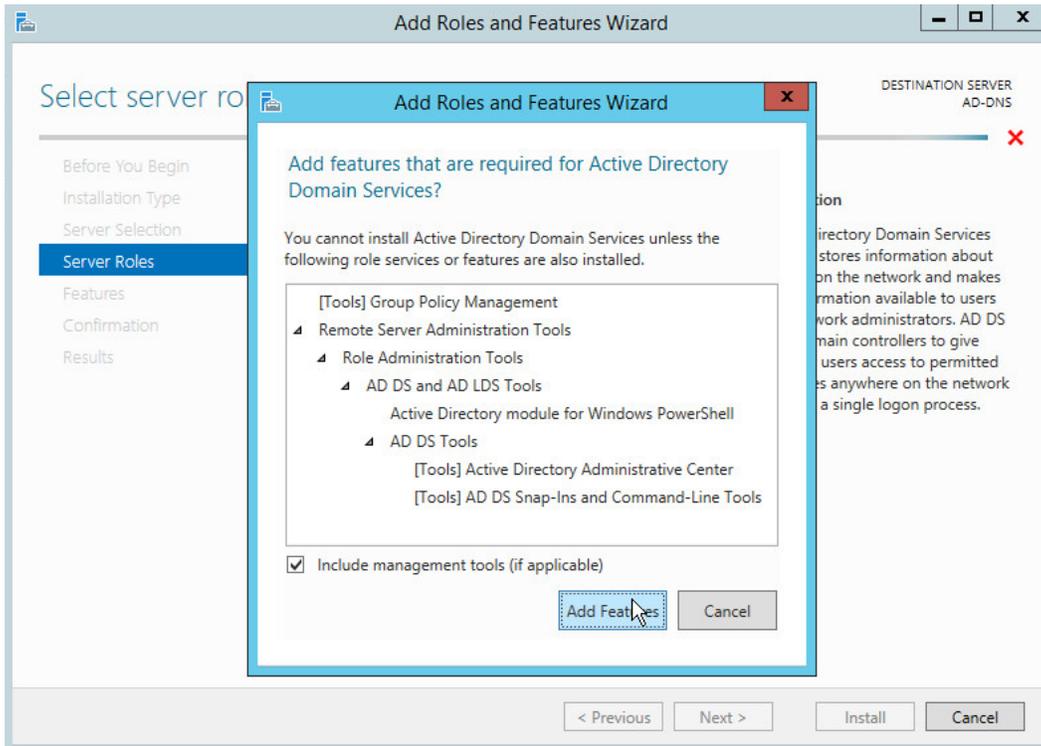
- 302 5. Click **Next**.
- 303 6. Select **Select a server from the server pool**.
- 304 7. Select the intended Active Directory server.



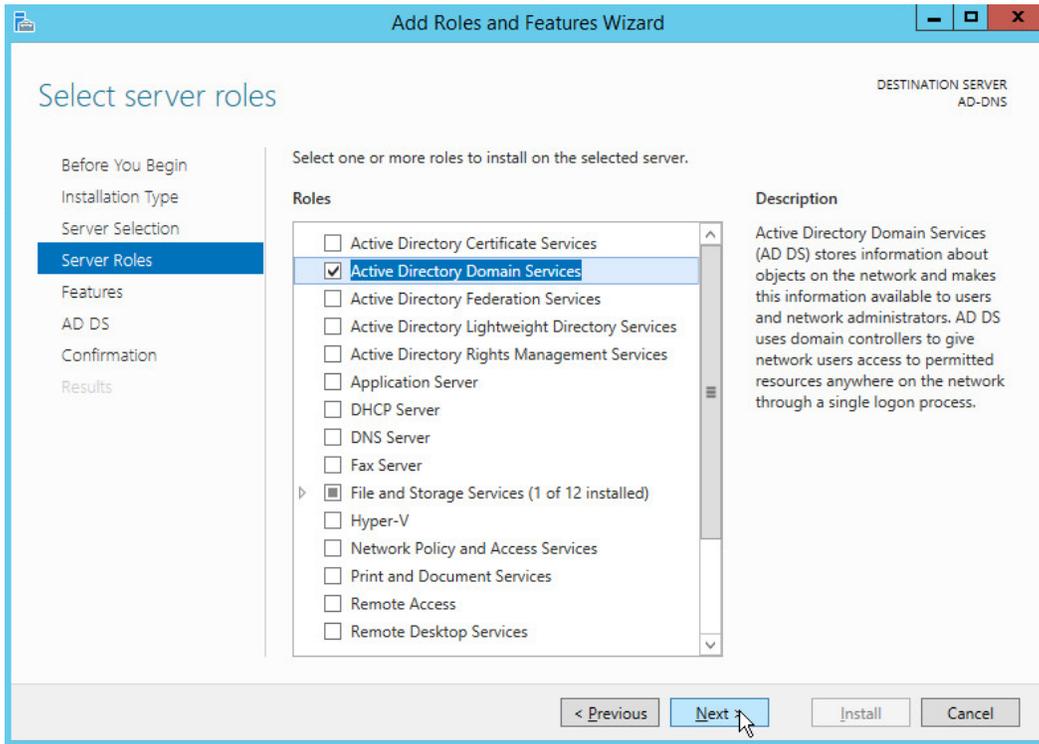
305 8. Click **Next**.



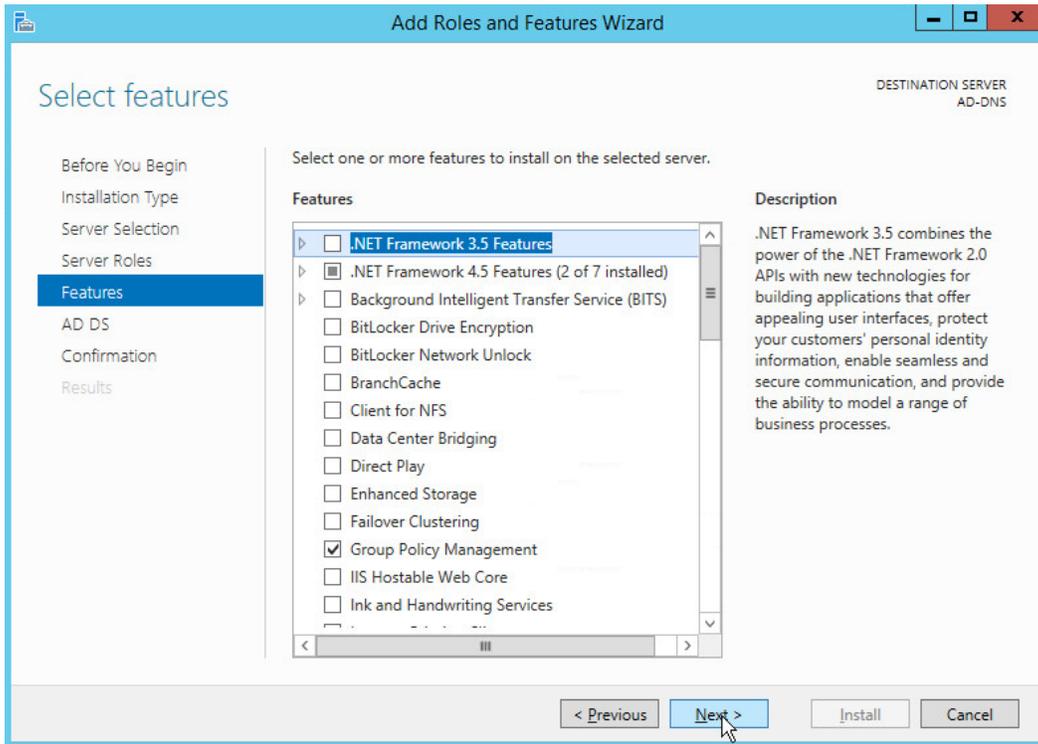
306 9. Check the box next to **Active Directory Domain Services**.



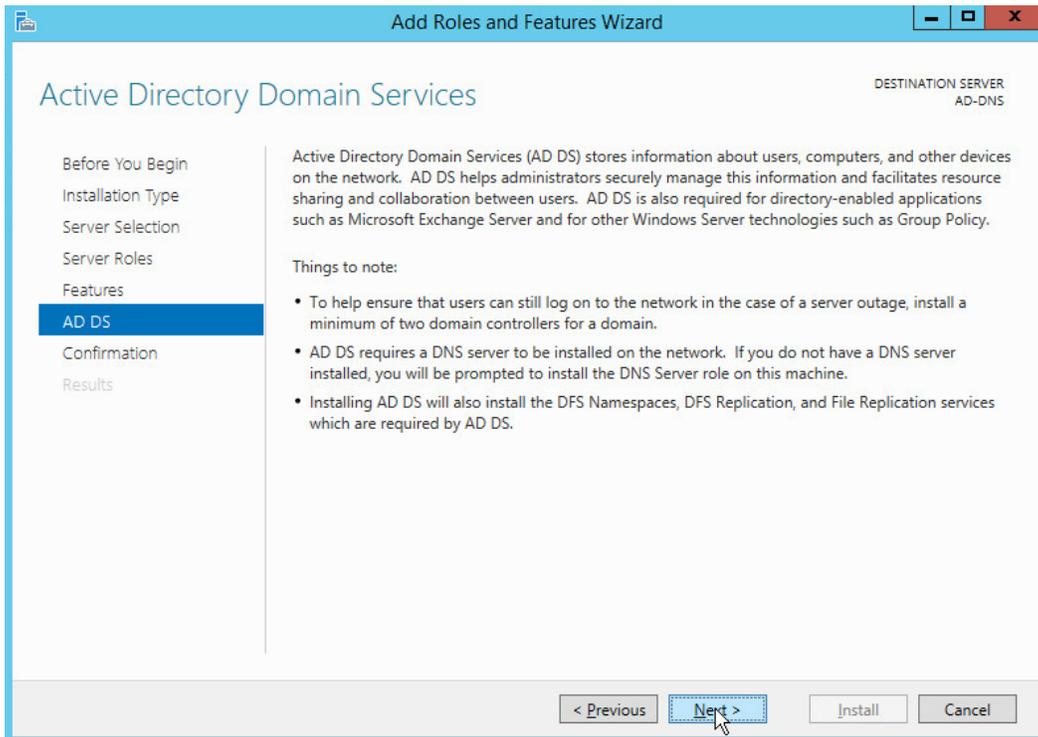
307 10. Click **Add Features**.



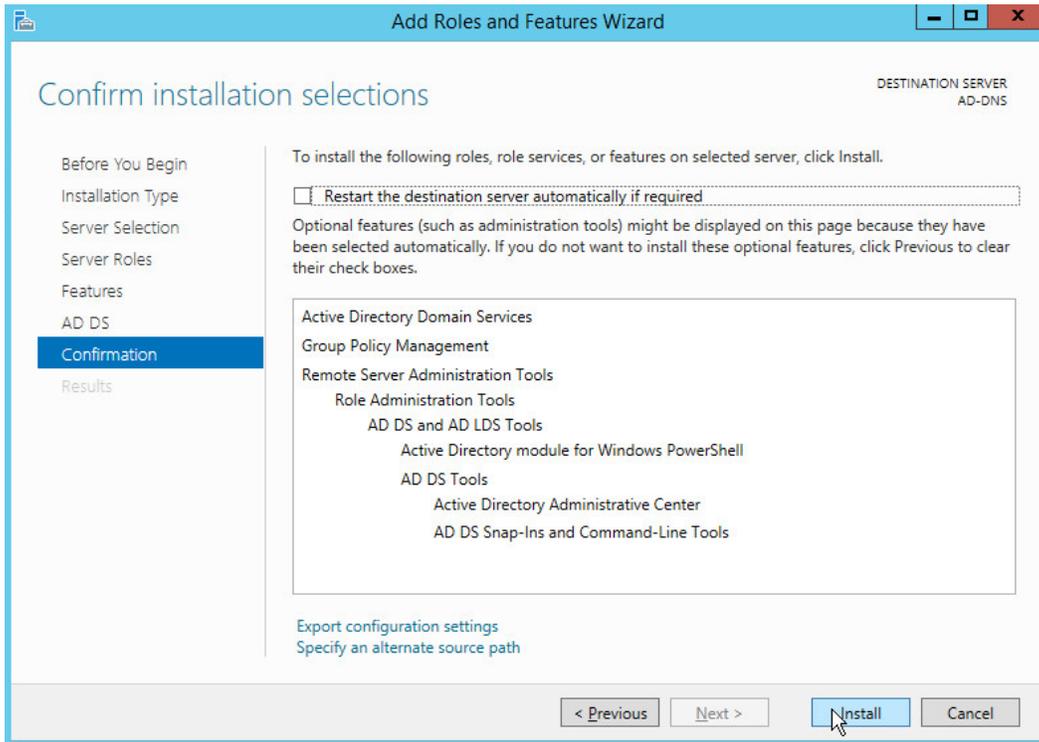
308 11. Click **Next**.



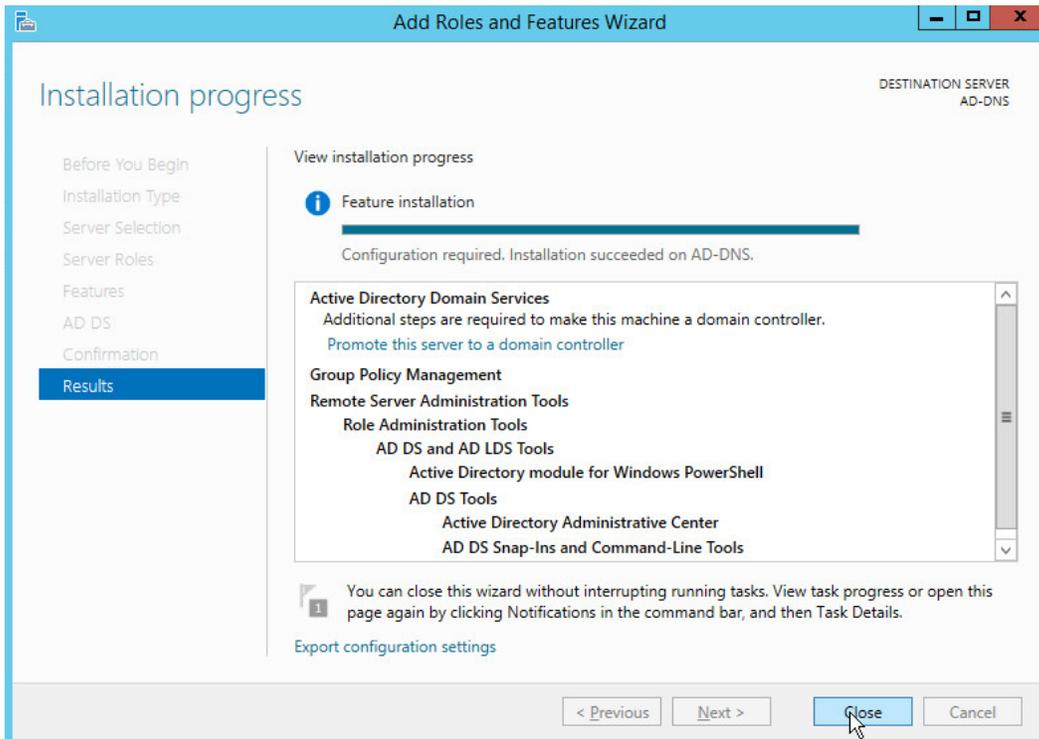
309 12. Click **Next**.



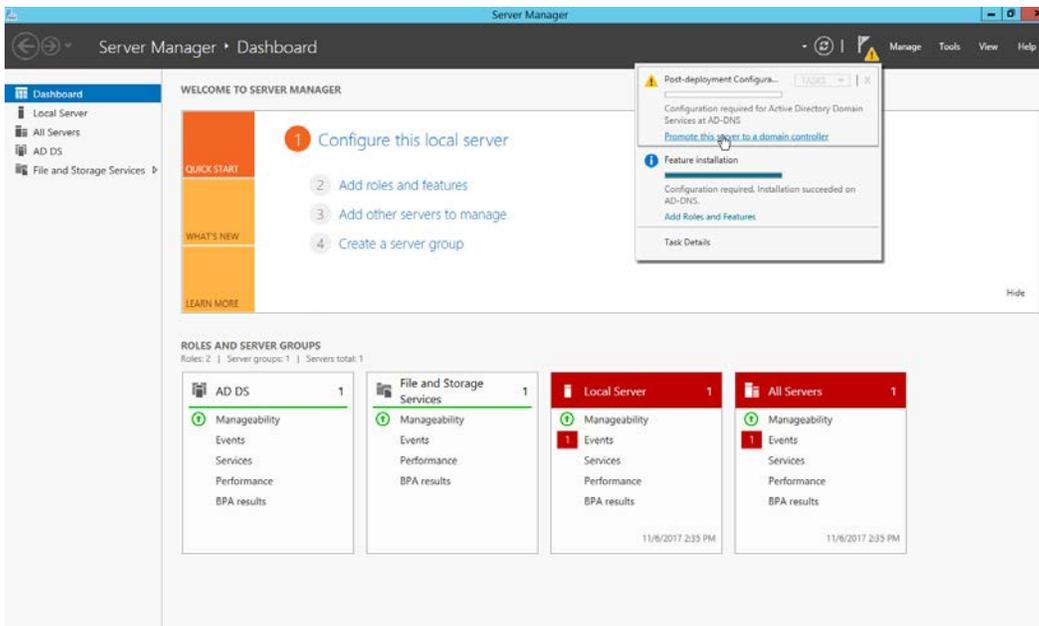
310 13. Click **Next**.



- 311 14. Click **Install**.
- 312 15. Wait for the installation to complete.



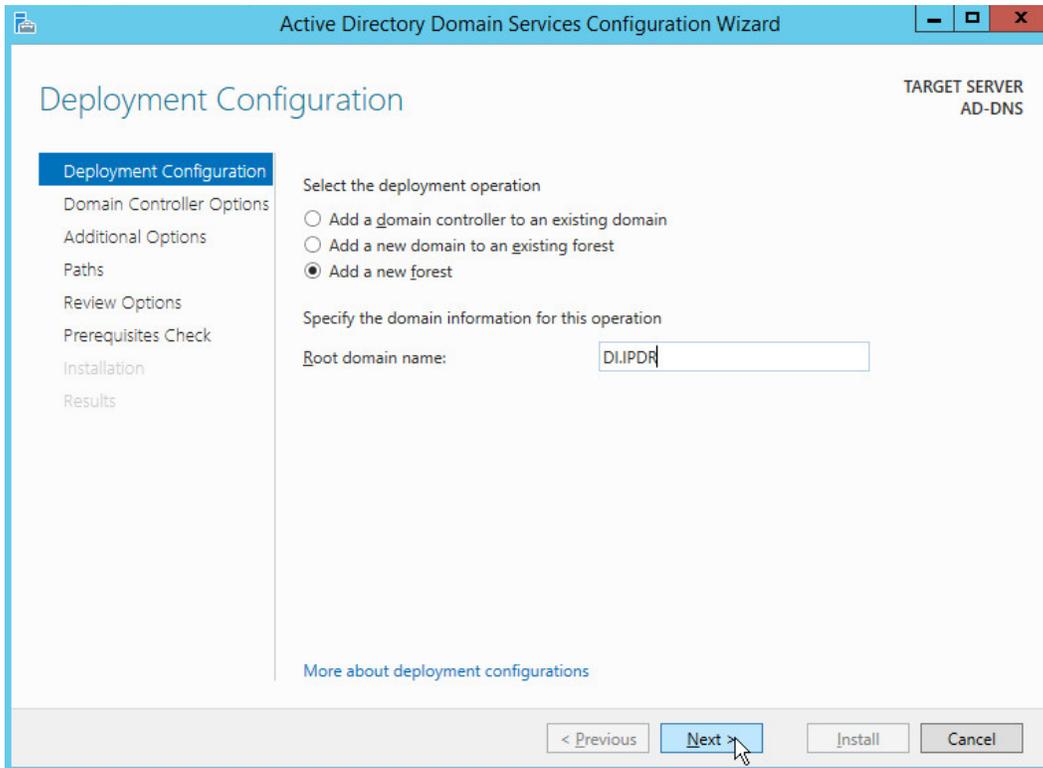
313 16. Click **Close**.



314 17. Click **Promote this server to a domain controller**.

315 18. Select **Add a new forest**.

316 19. Enter a **Root domain name**.

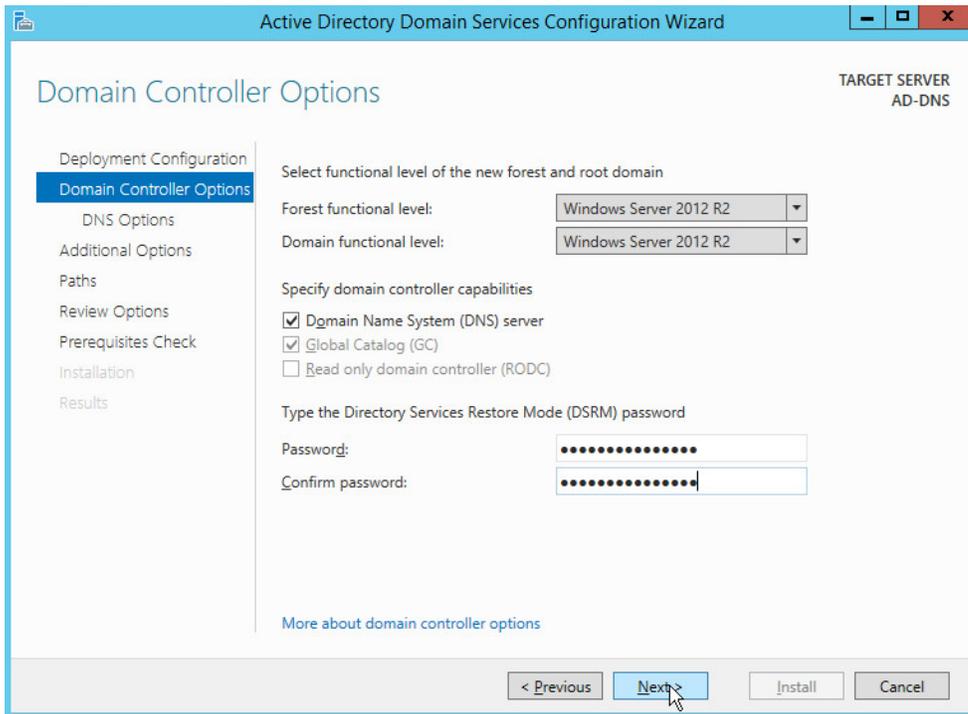


317 20. Click **Next**.

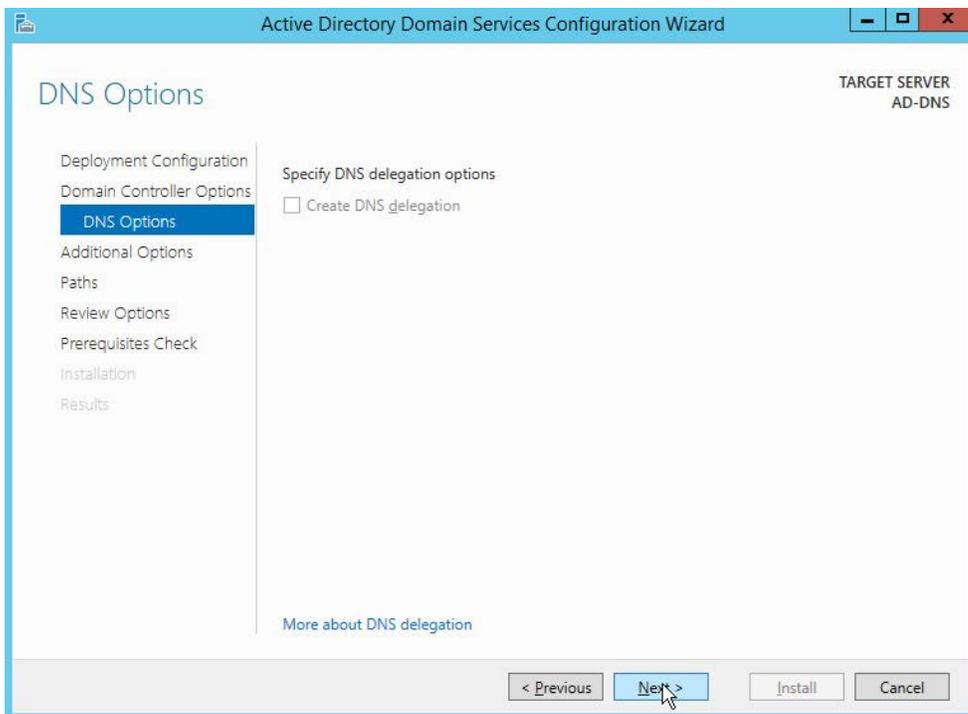
318 21. Select **Windows Server 2012 R2** for **Forest functional level** and **Domain functional level**.

319 22. Check the box next to **Domain Name System (DNS) server**.

320 23. Enter a **password**.



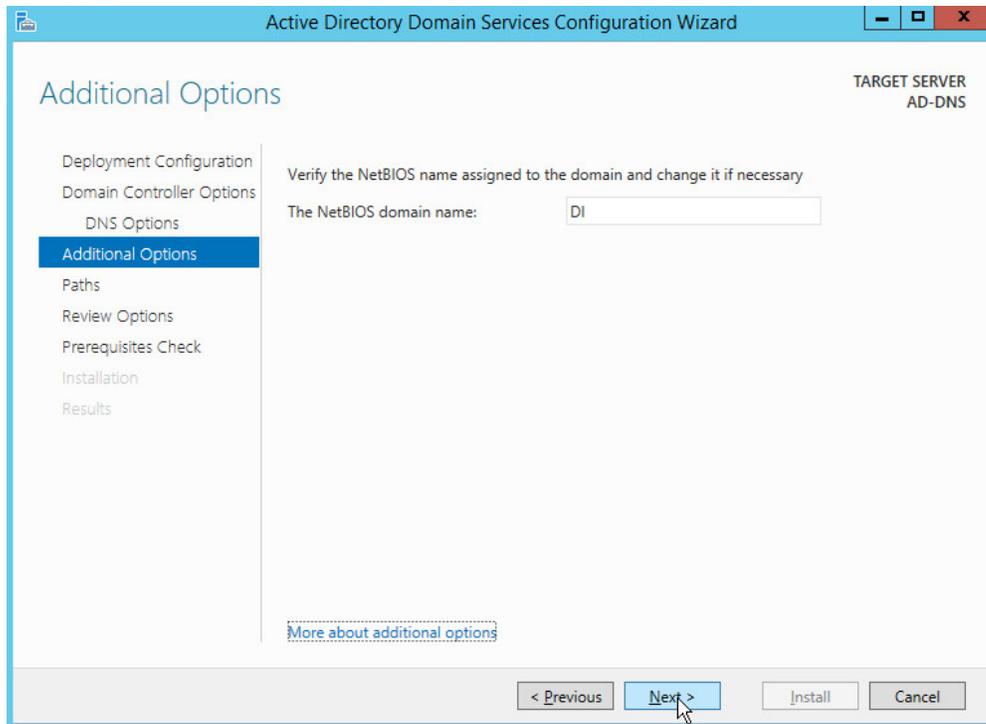
321 24. Click **Next**.



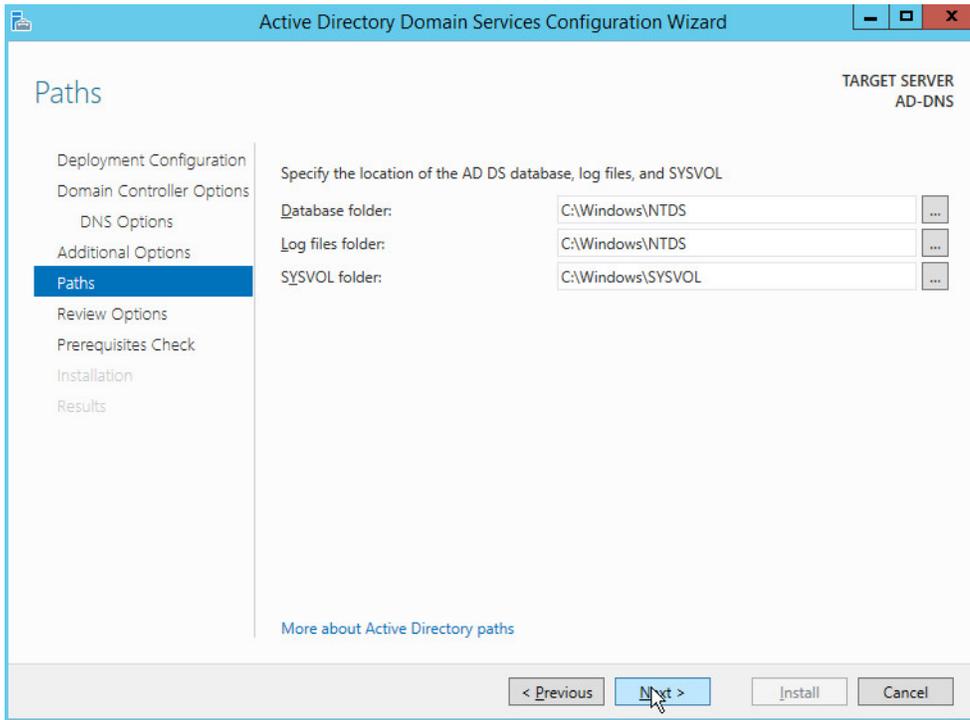
DRAFT

322 25. Click **Next**.

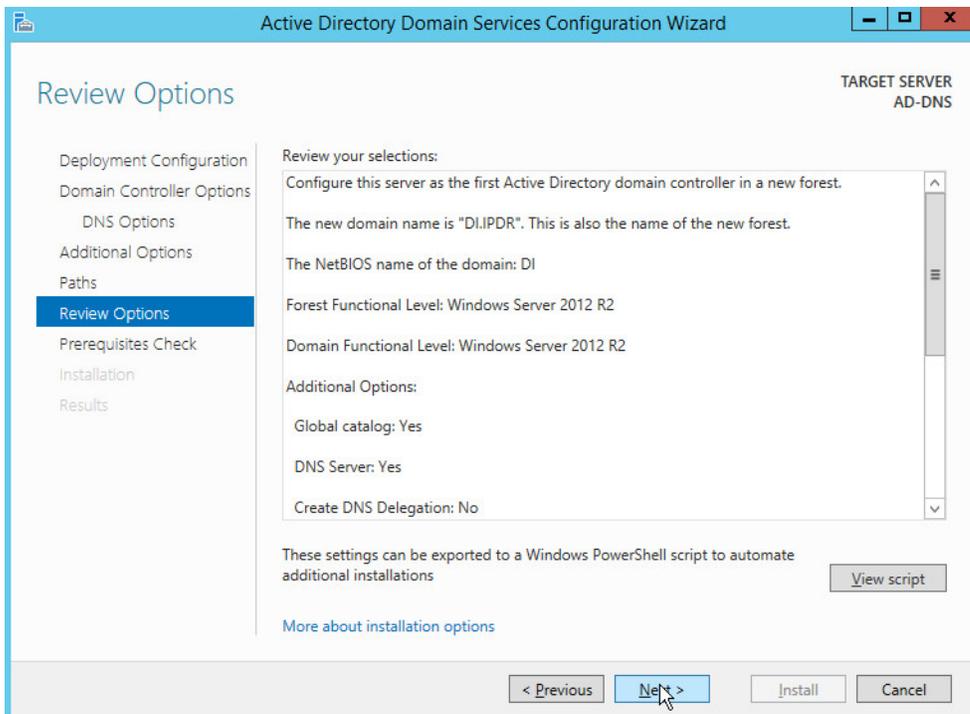
323 26. Verify the domain name.



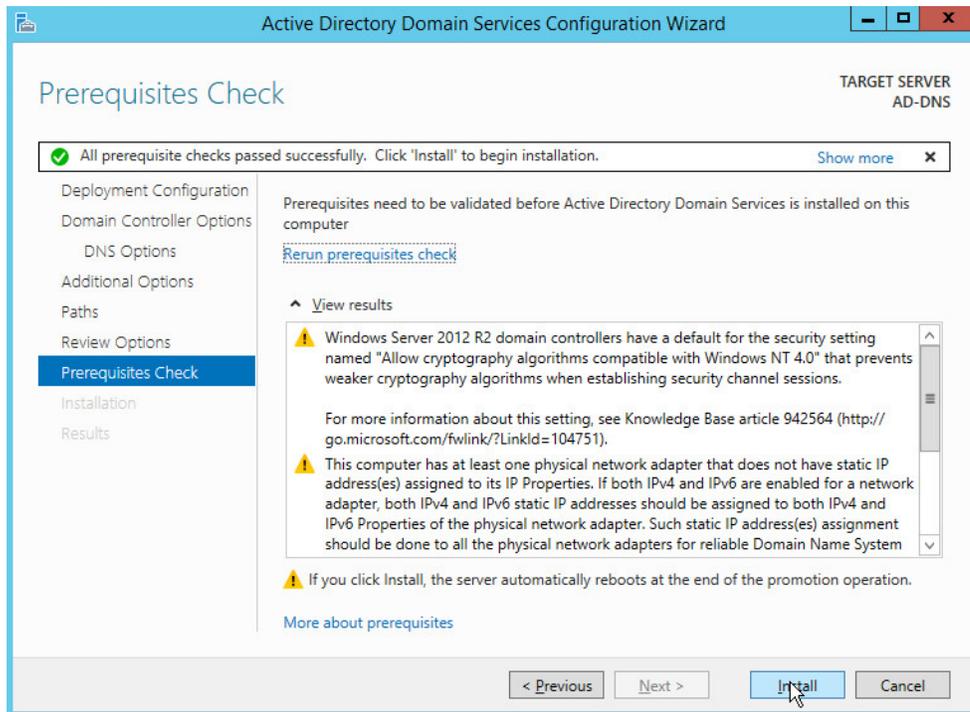
324 27. Click **Next**.



325 28. Click **Next**.



326 29. Click **Next**.



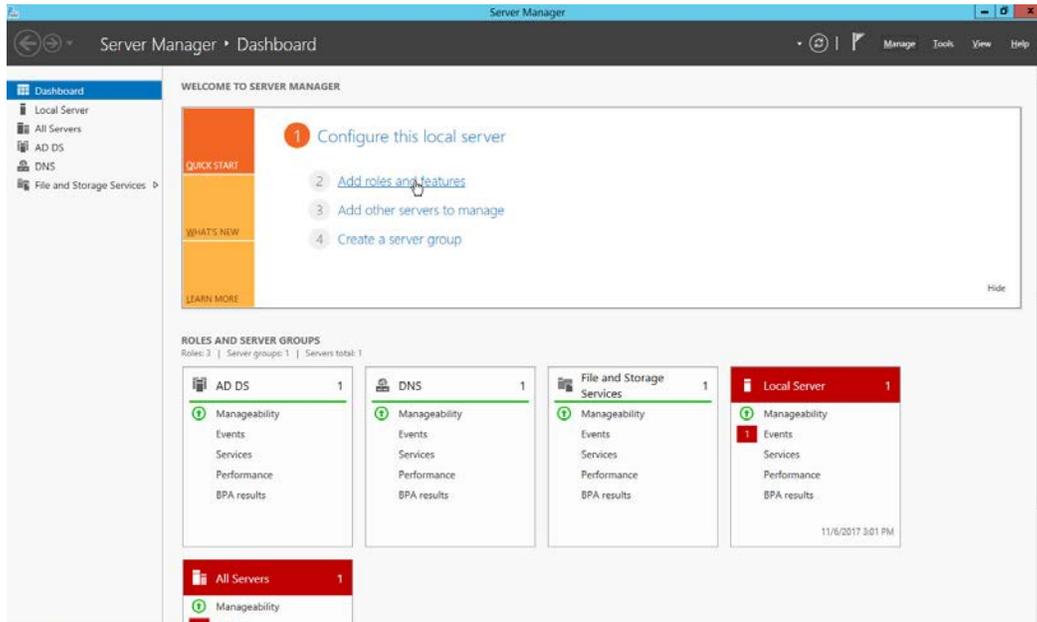
327 30. Click **Install**.

328 31. Wait for the installation to complete.

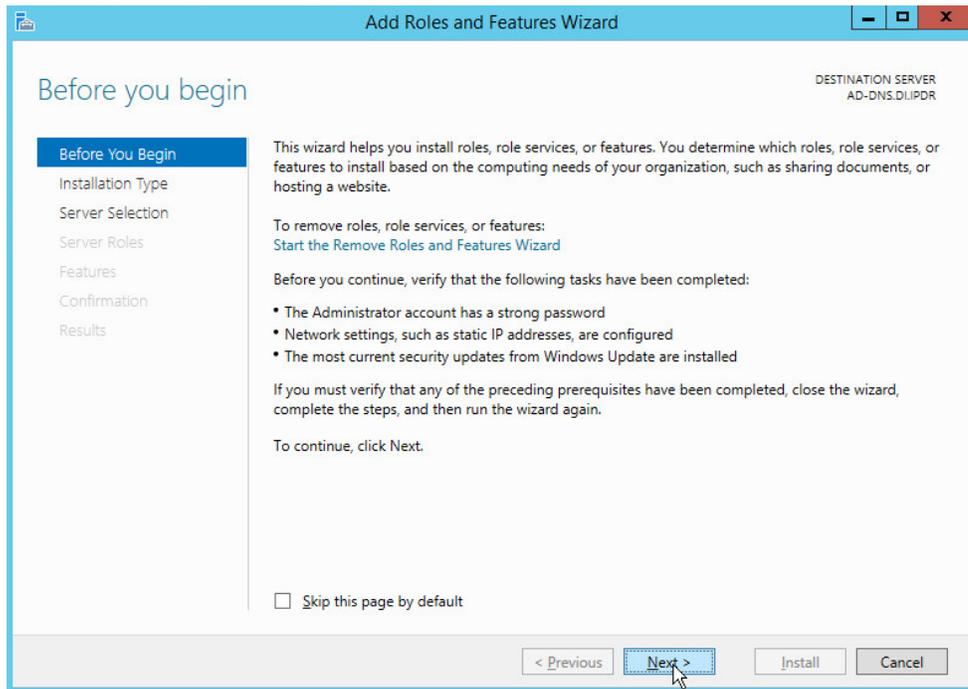
329 32. The server automatically reboots.

## 330 2.1.2 Creating a Certificate Authority

331 1. Open **Server Manager**.

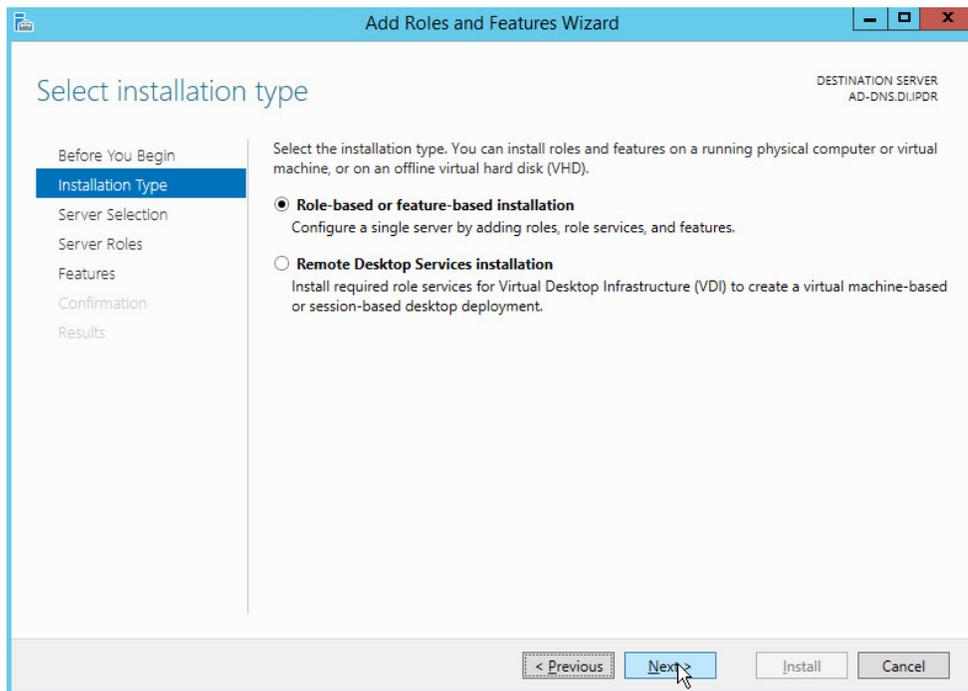


332 2. Click **Add roles and features**.

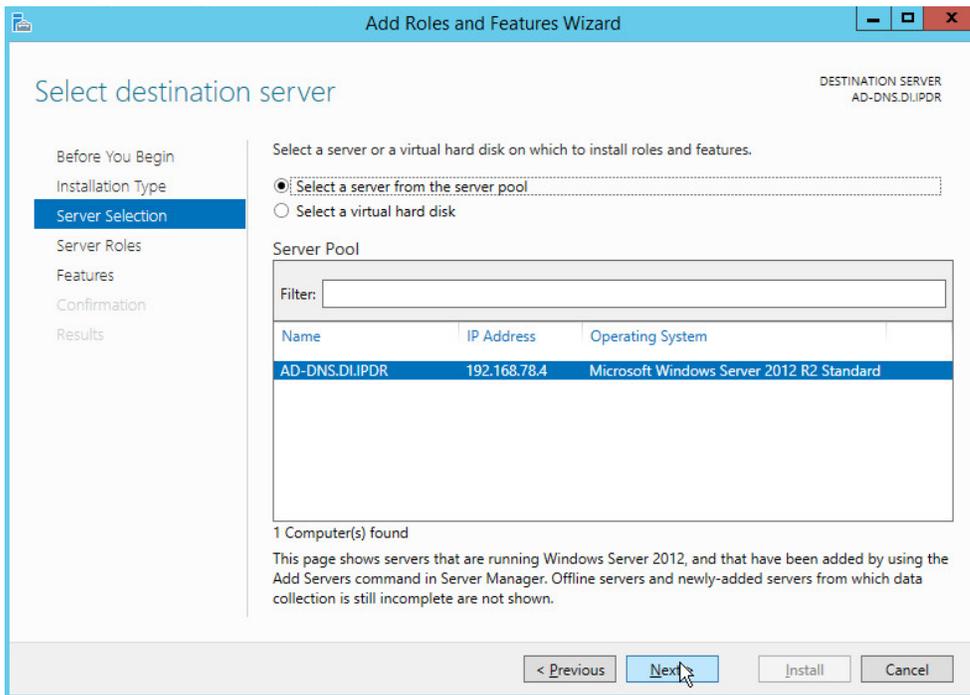


333 3. Click **Next**.

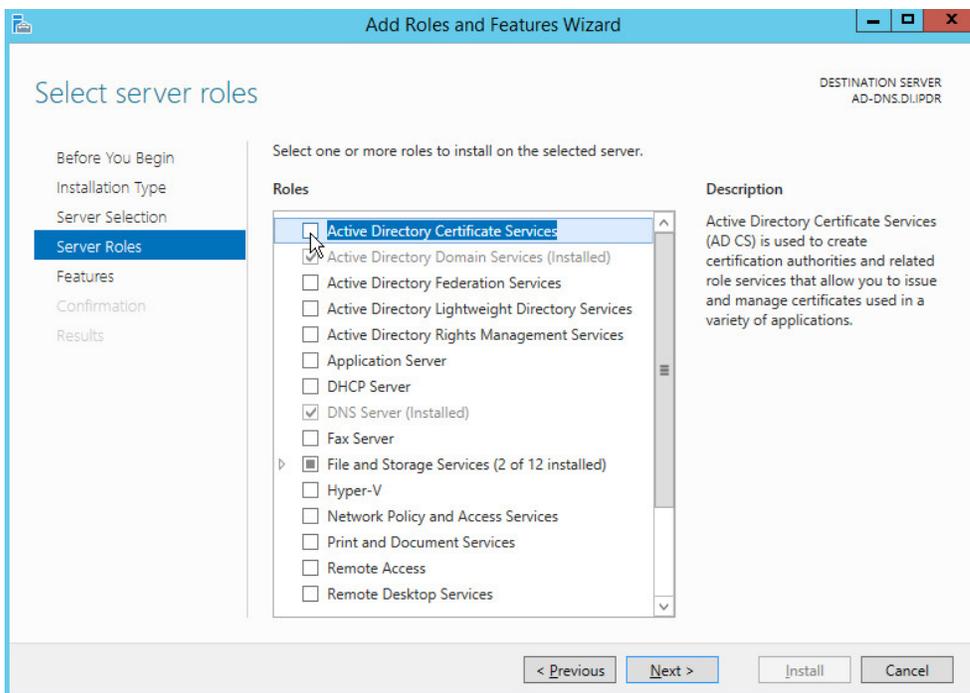
334 4. Select **Role-based or feature-based installation**.



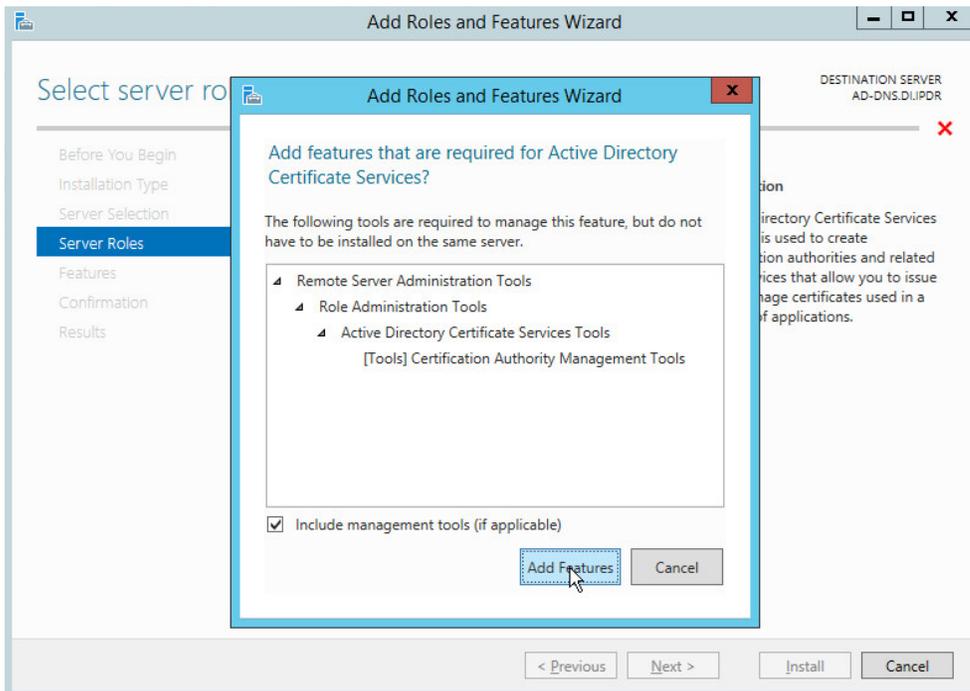
- 335 5. Click **Next**.
- 336 6. Select **Select a server from the server pool**.
- 337 7. Select the intended Active Directory server.



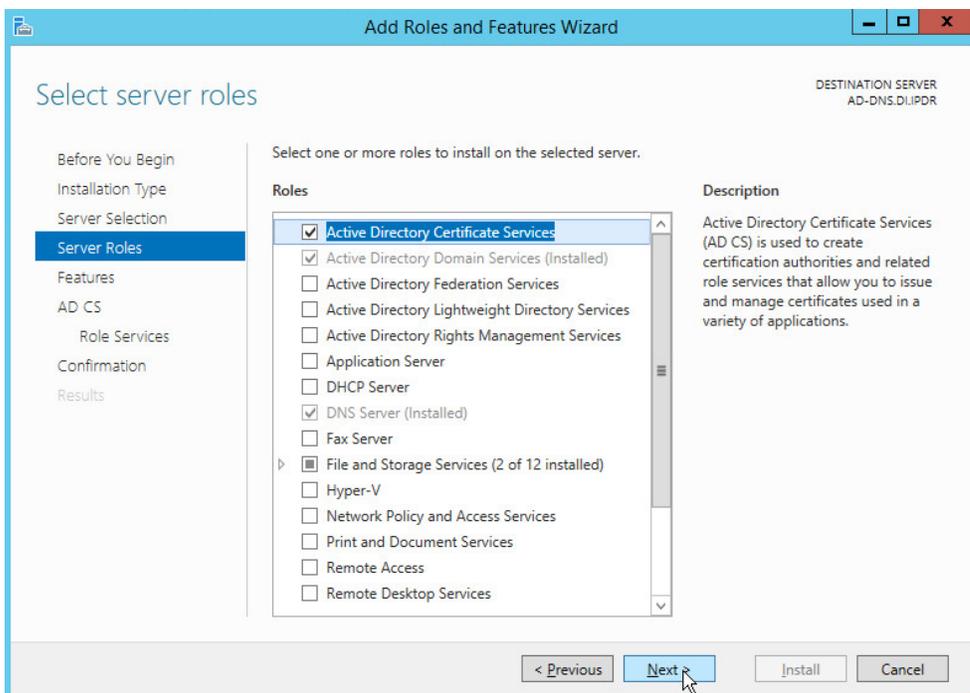
338 8. Click **Next**.



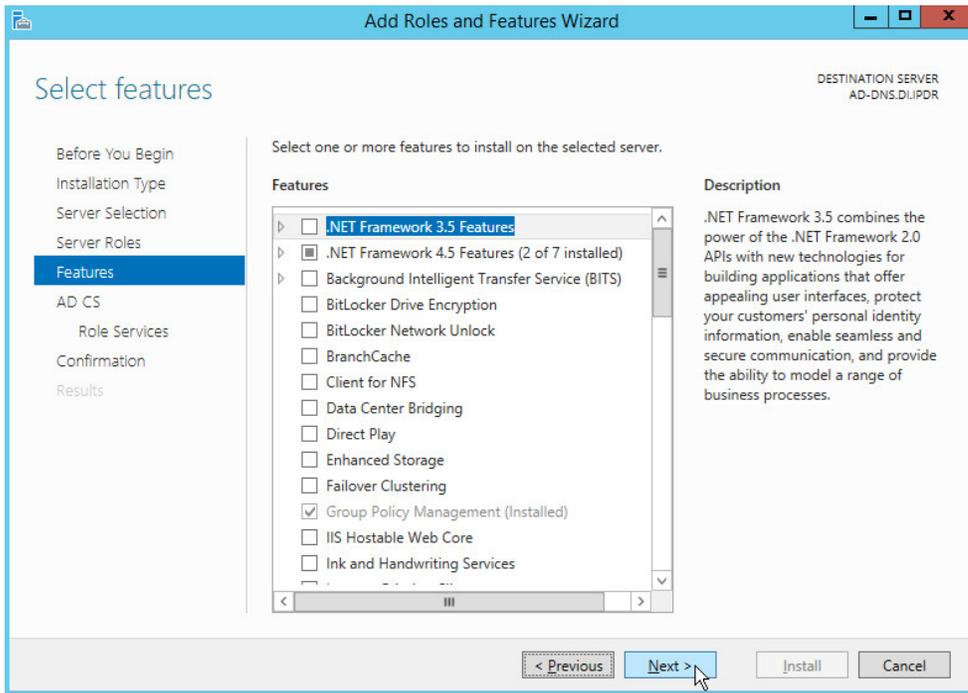
339 9. Check the box next to **Active Directory Certificate Services**.



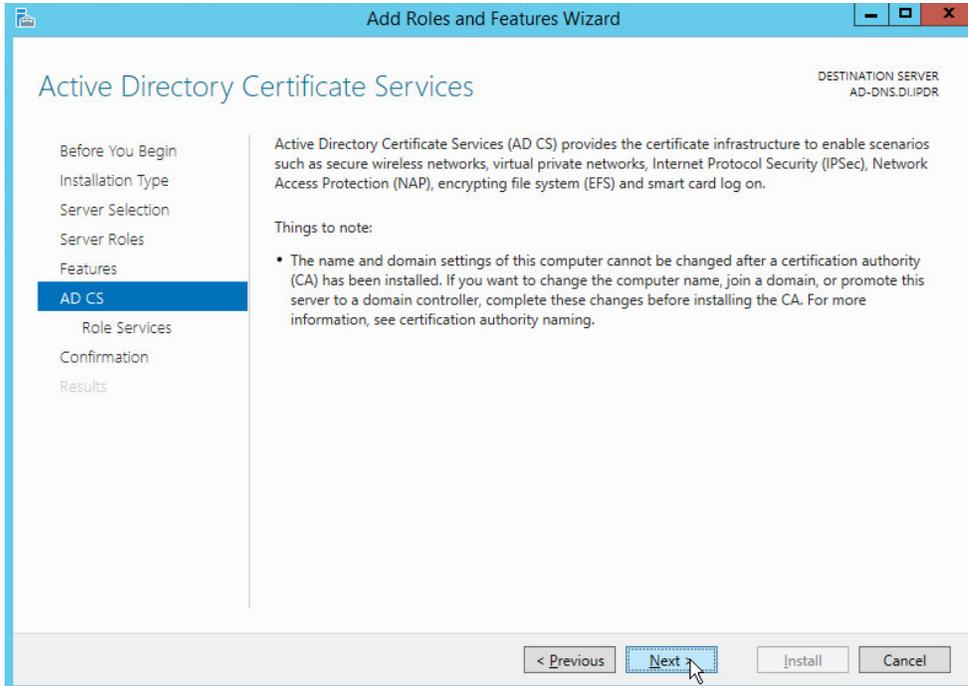
340 10. Click **Add Features**.



341 11. Click **Next**.

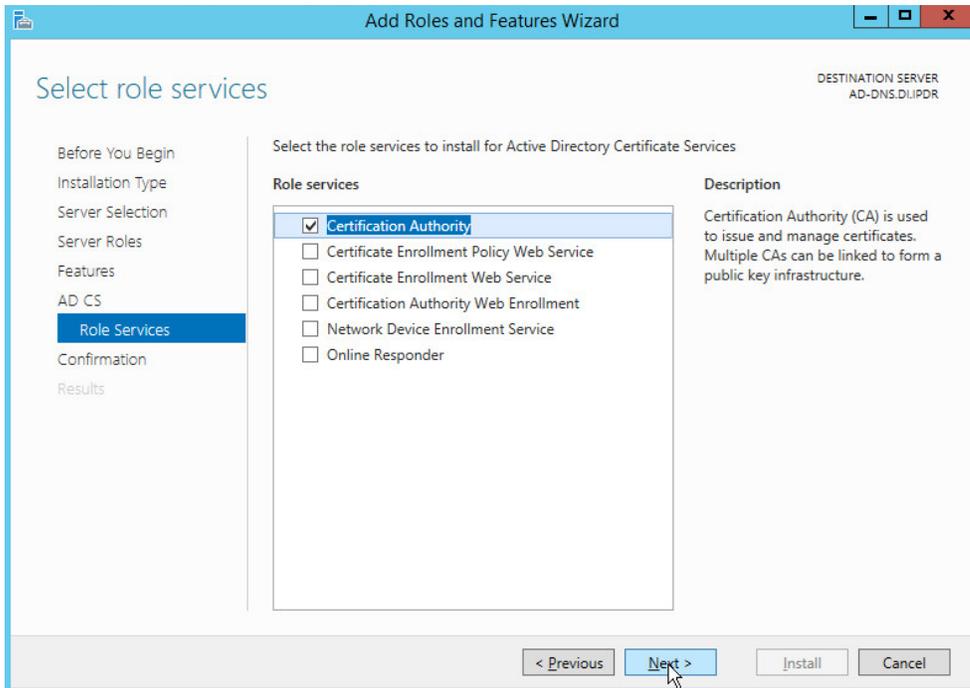


342 12. Click **Next**.

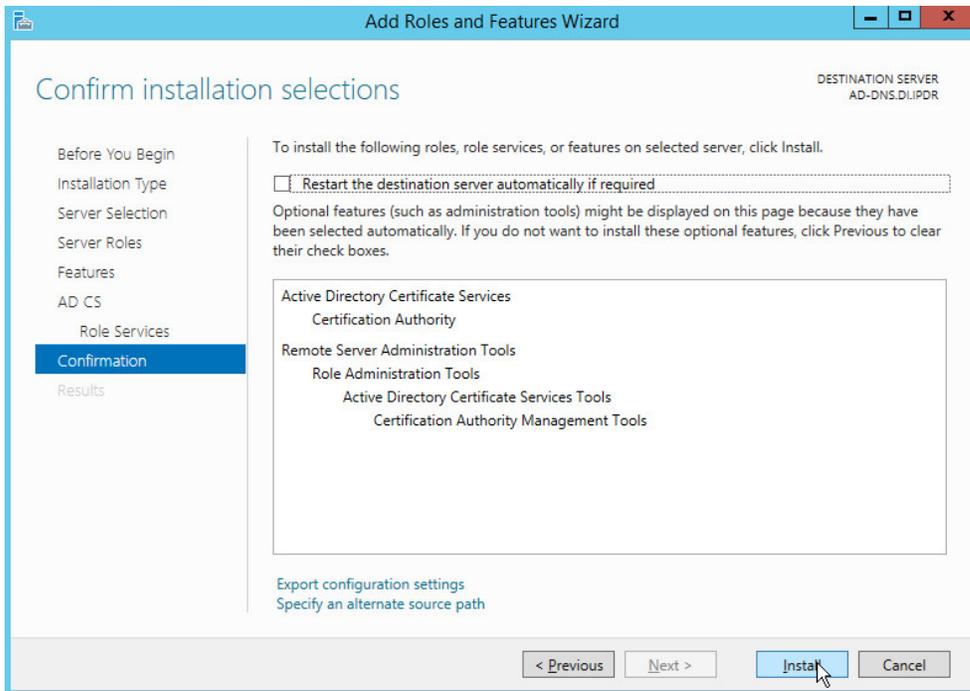


343 13. Click **Next**.

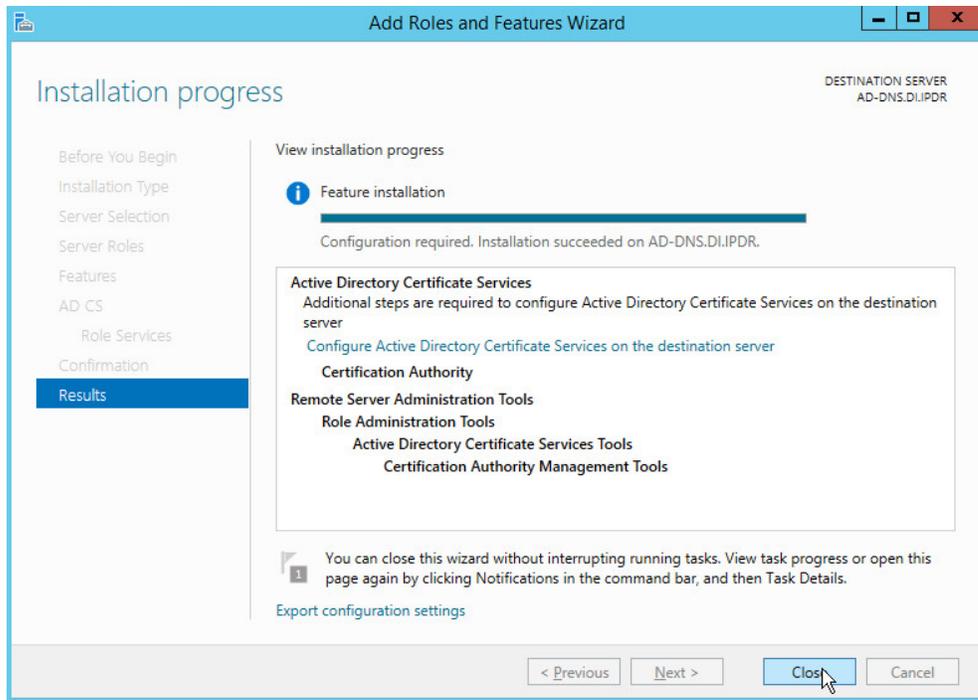
344 14. Check the box next to **Certification Authority**.



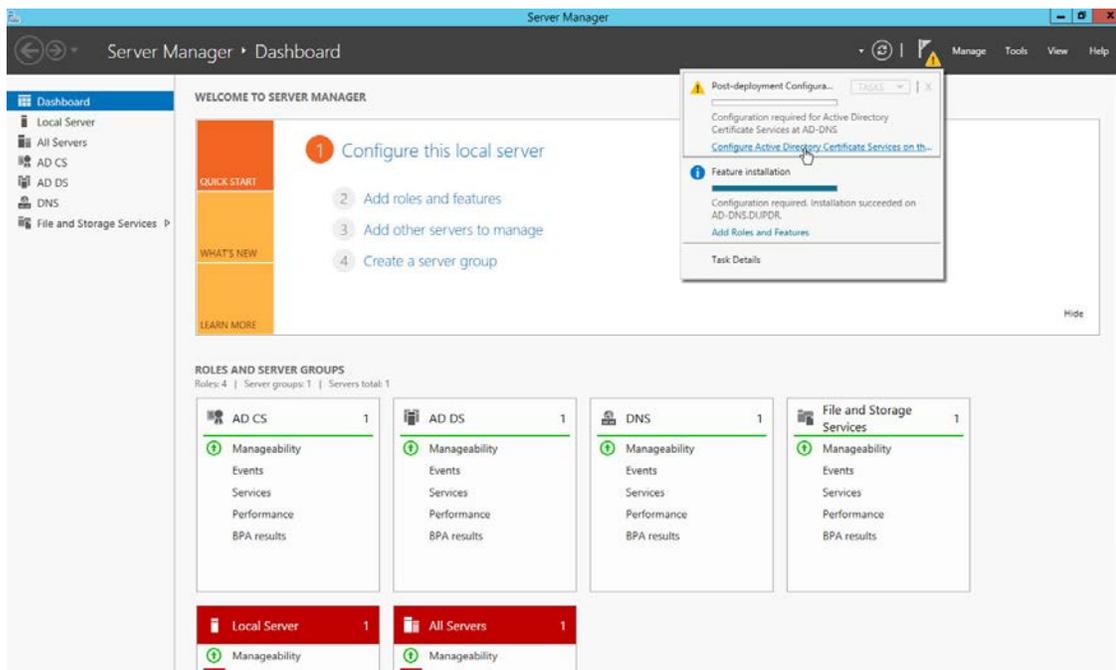
345 15. Click **Next**.



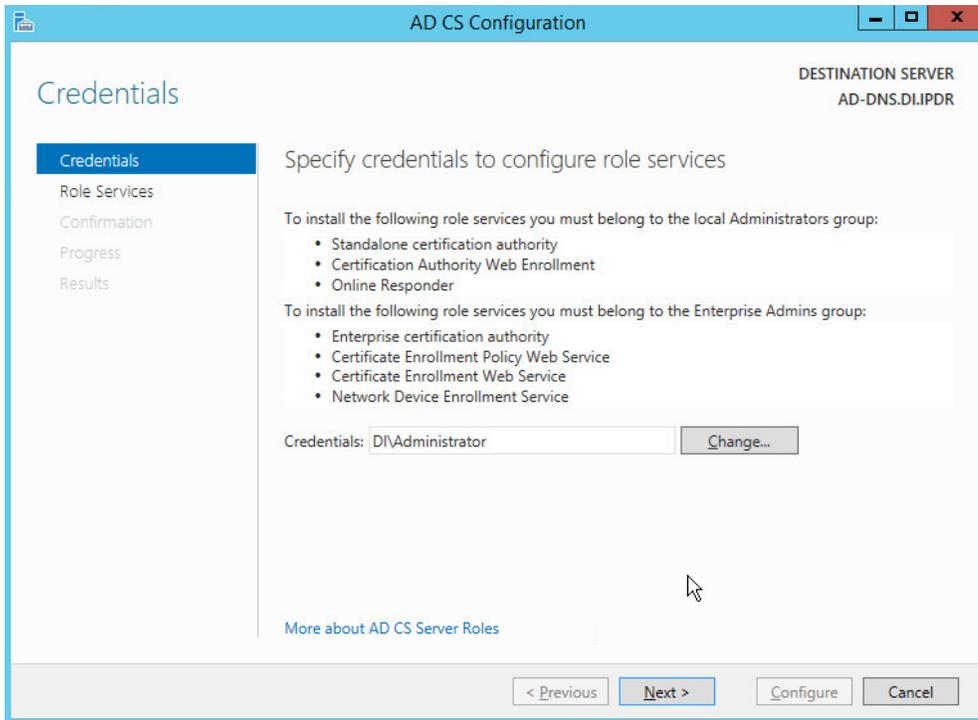
- 346 16. Click **Install**.
- 347 17. Wait for the installation to complete.



- 348 18. Click **Close**.

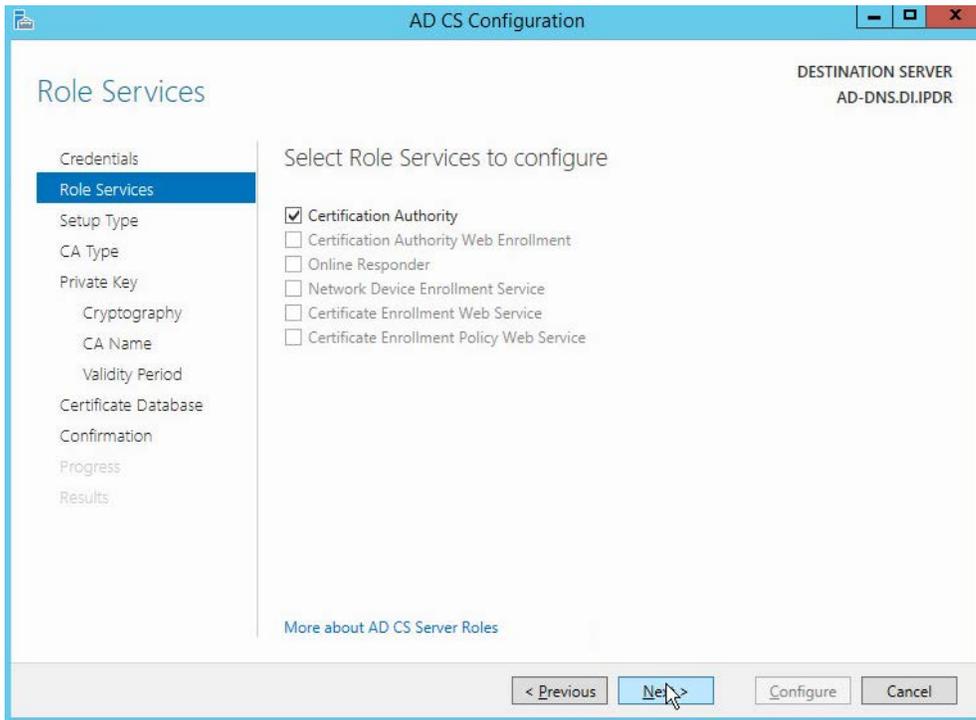


349 19. Click **Configure Active Directory Certificate Services on the destination server.**

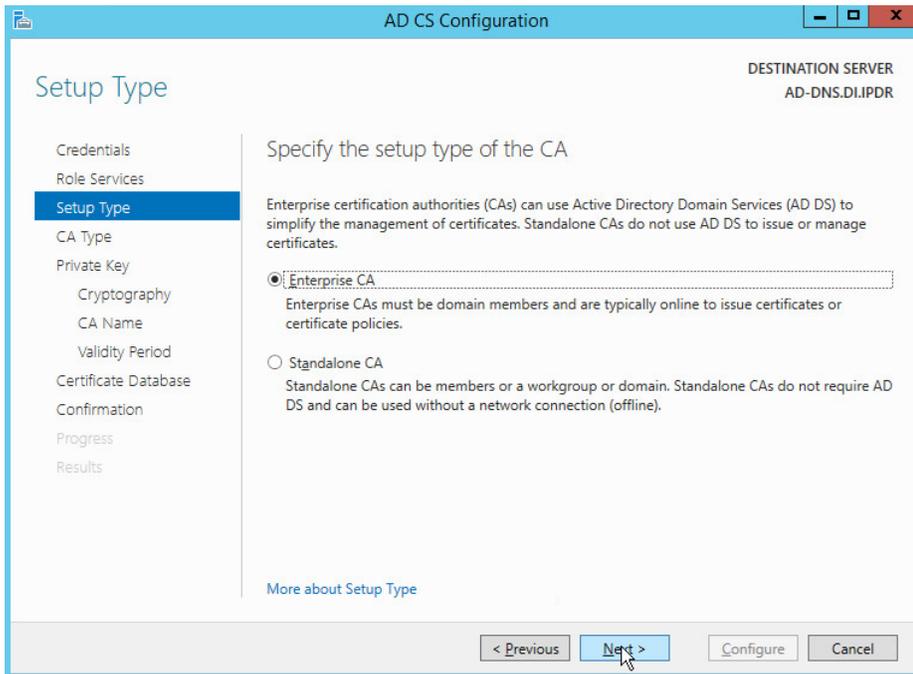


350 20. Click **Next.**

351 21. Check the box next to **Certification Authority.**

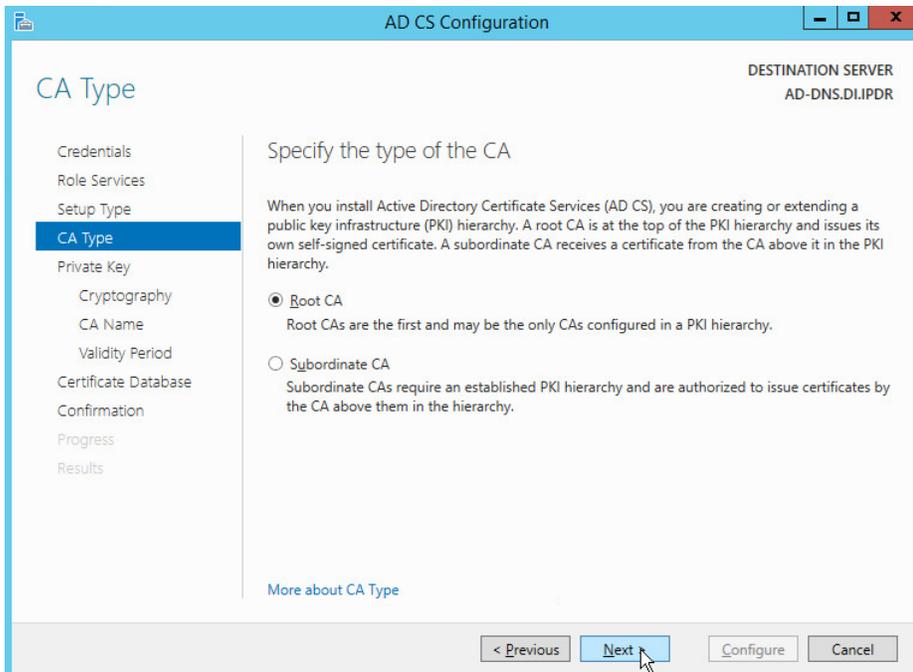


- 352 22. Click **Next**.
- 353 23. Select **Enterprise CA**.



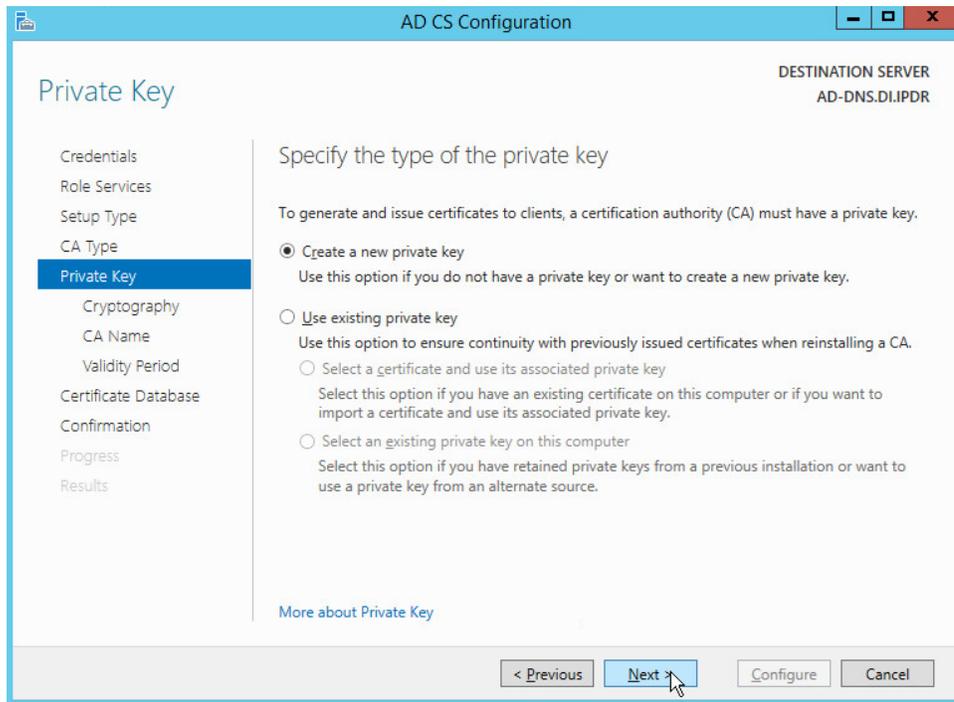
354 24. Click **Next**.

355 25. Select **Root CA**.



356 26. Click **Next**.

357 27. Select **Create a new private key**.

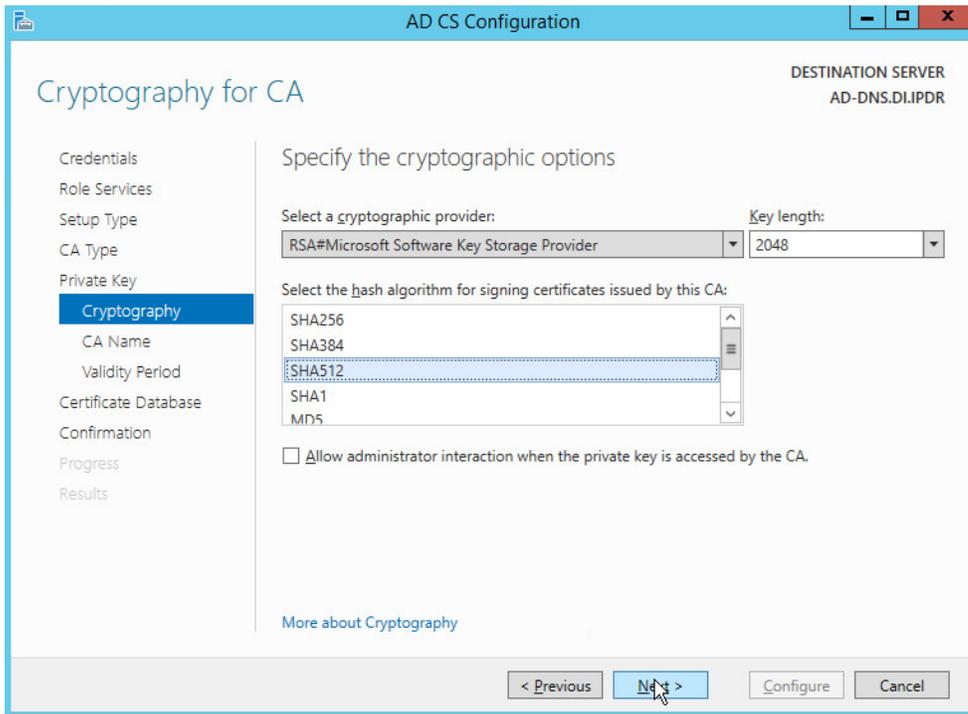


358 28. Click **Next**.

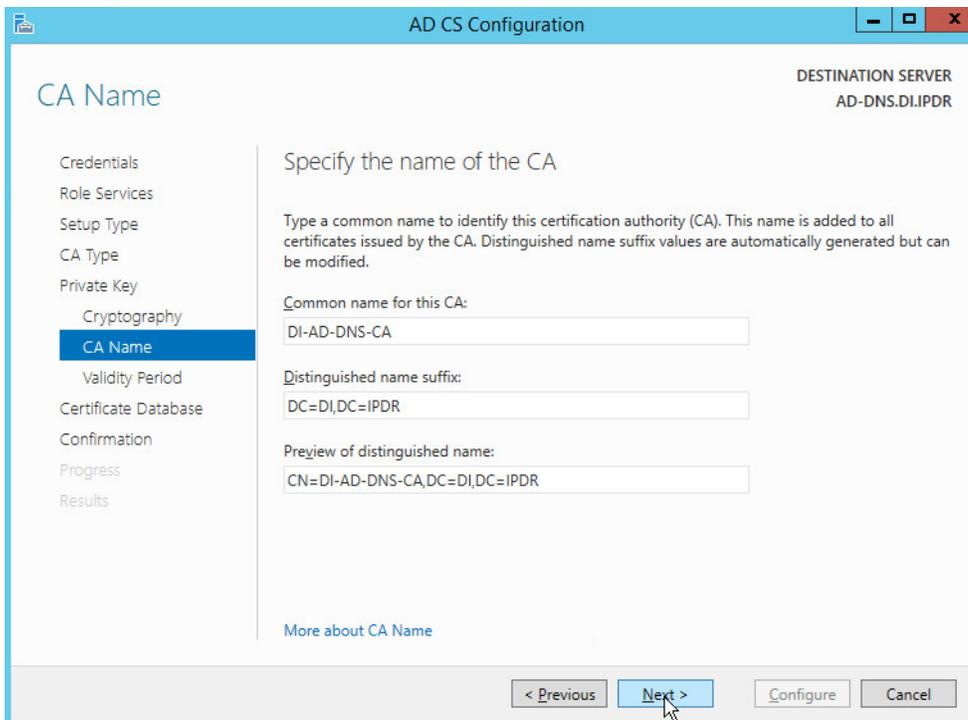
359 29. Select **RSA#Microsoft Software Key Storage Provider**.

360 30. Set the **Key length** to **2048**.

361 31. Select **SHA512** from the list.

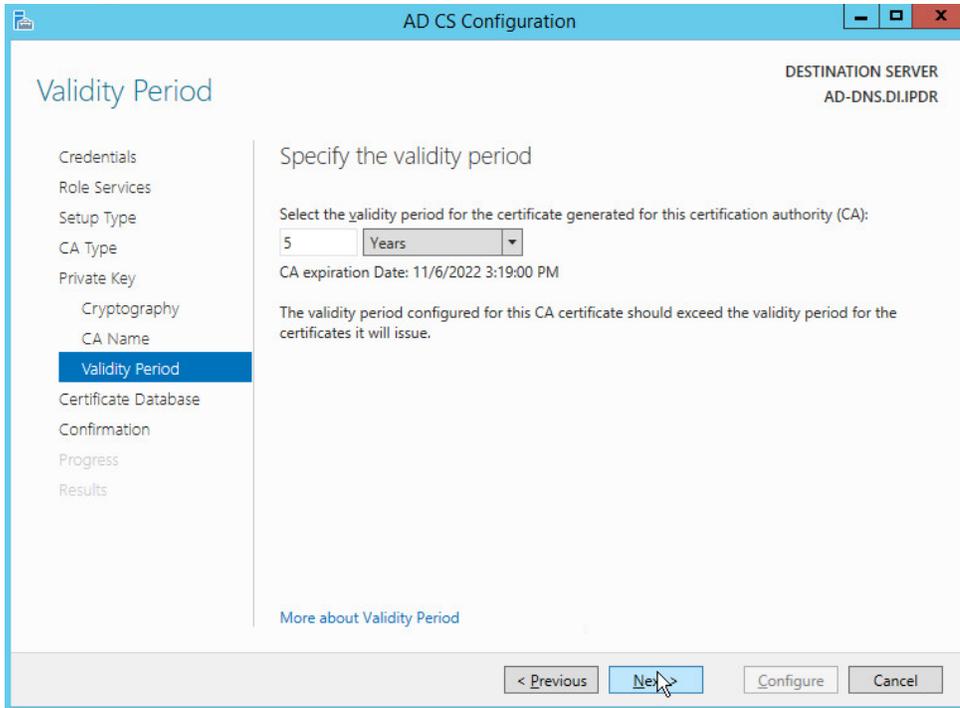


362 32. Click **Next**.

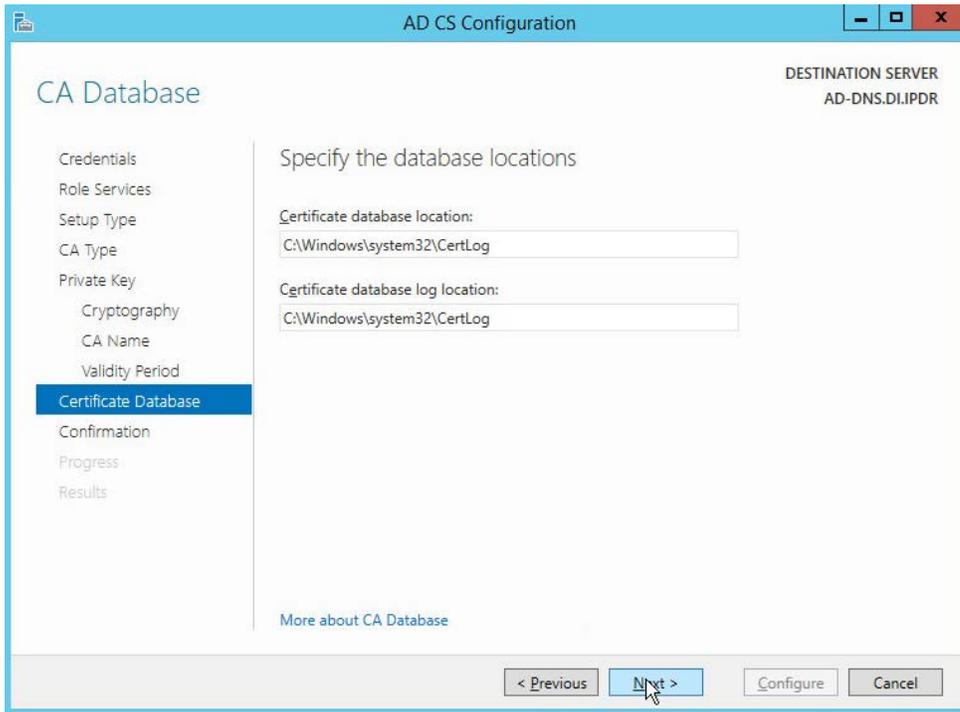


363 33. Click **Next**.

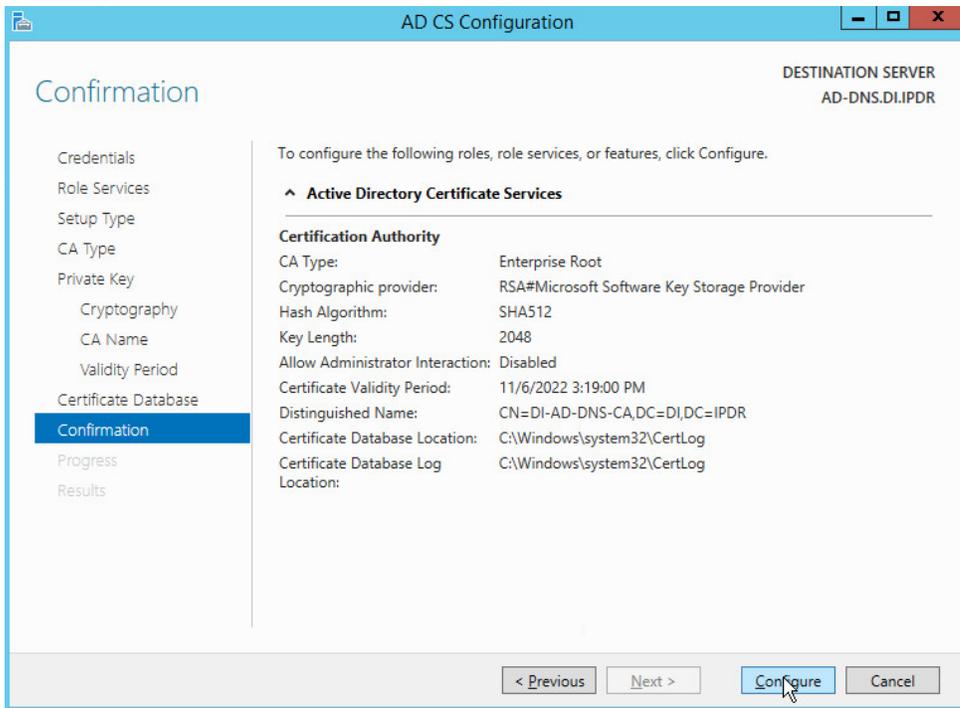
364 34. Set the time to 5 years.



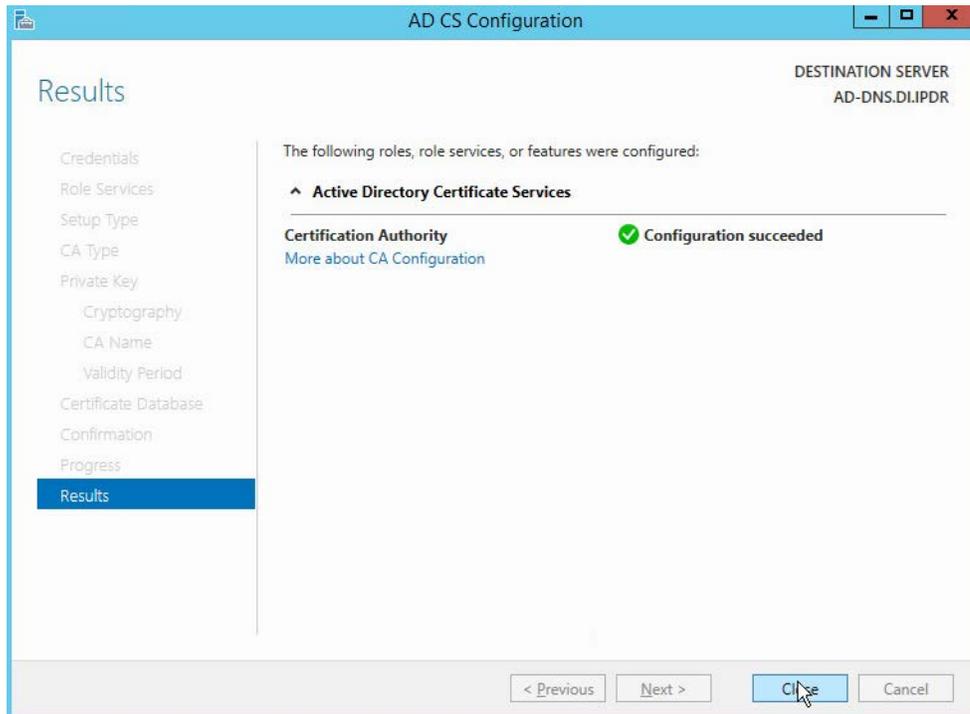
365 35. Click **Next**.



366 36. Click **Next**.



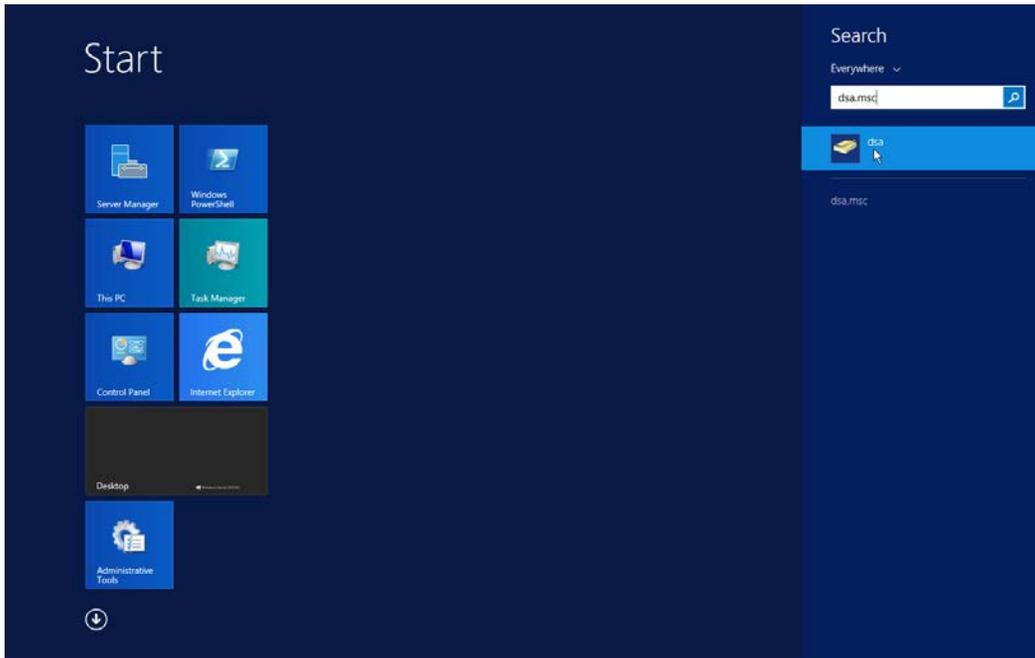
367 37. Click **Configure**.



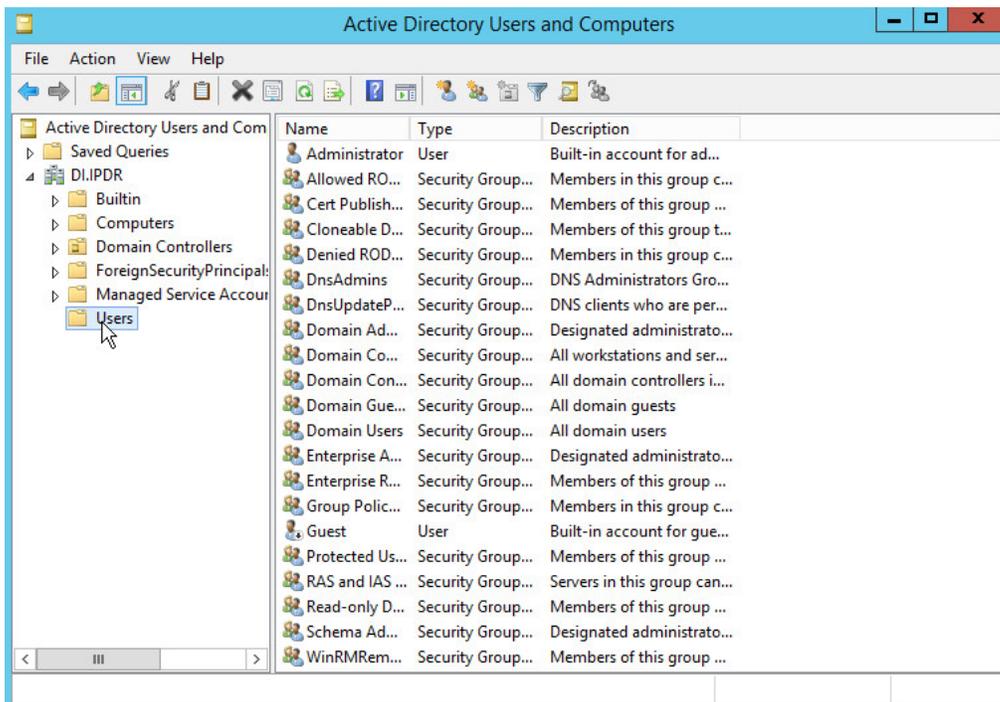
368 38. Click **Close**.

### 369 2.1.3 Configure Account to Add Computers to Domain

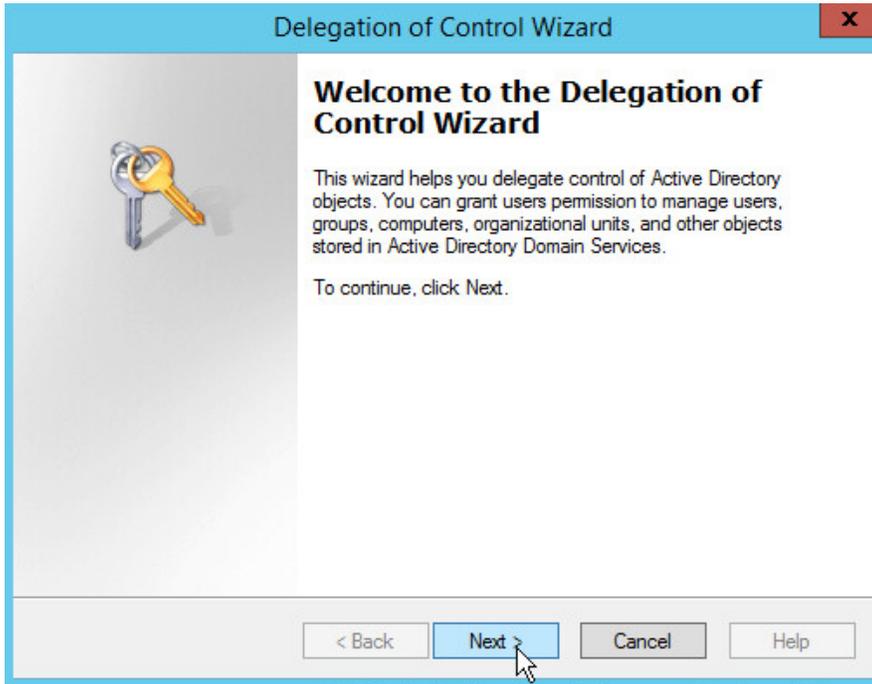
- 370 1. Open the Start menu.
- 371 2. Enter **dsa.msc** and run the program.



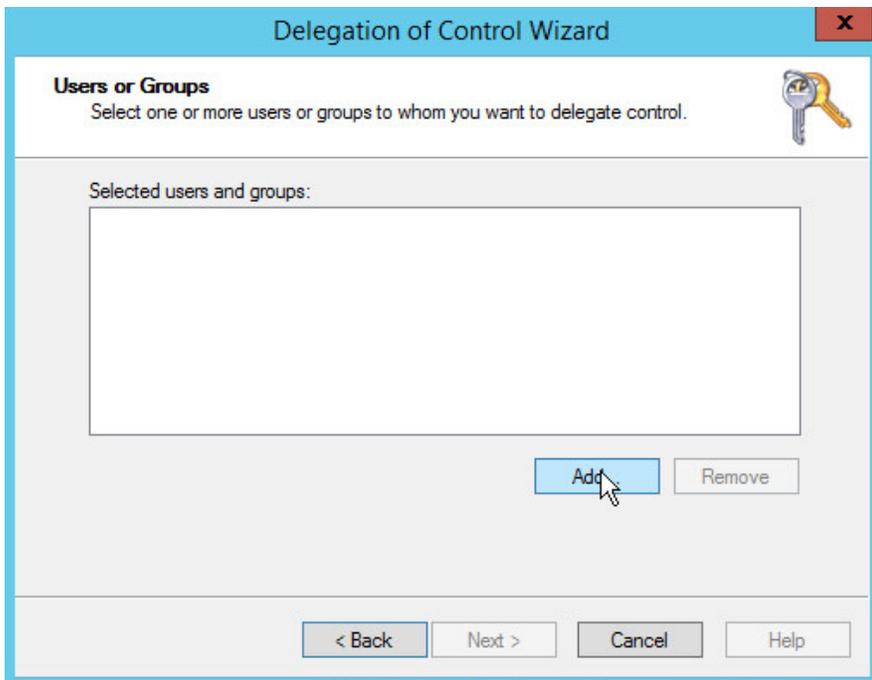
372 3. Right-click on **Users** in the left panel.



373 4. Click **Delegate Control**.

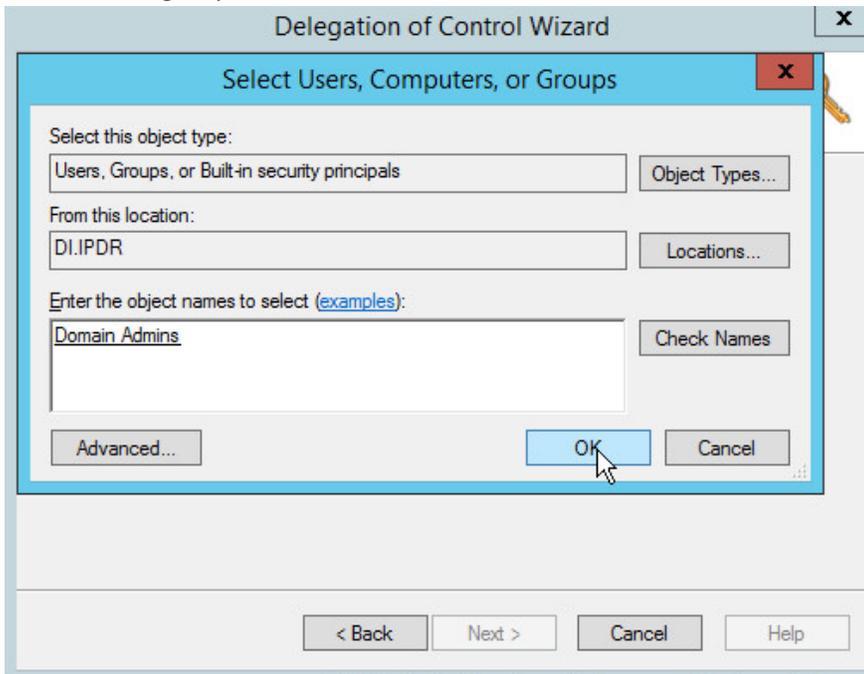


374 5. Click **Next**.

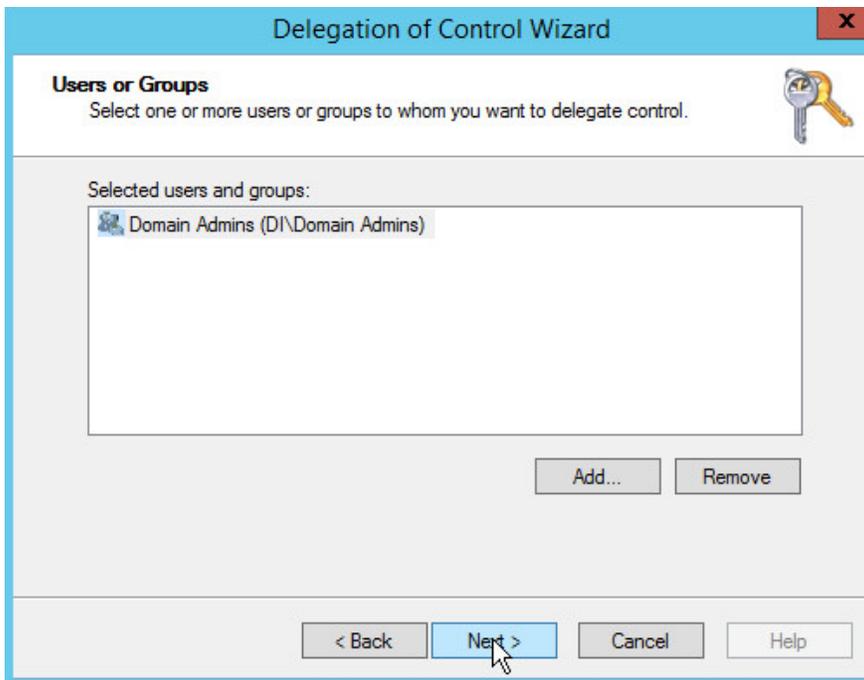


375 6. Click **Add** to select users or groups.

376 7. Add users or groups.

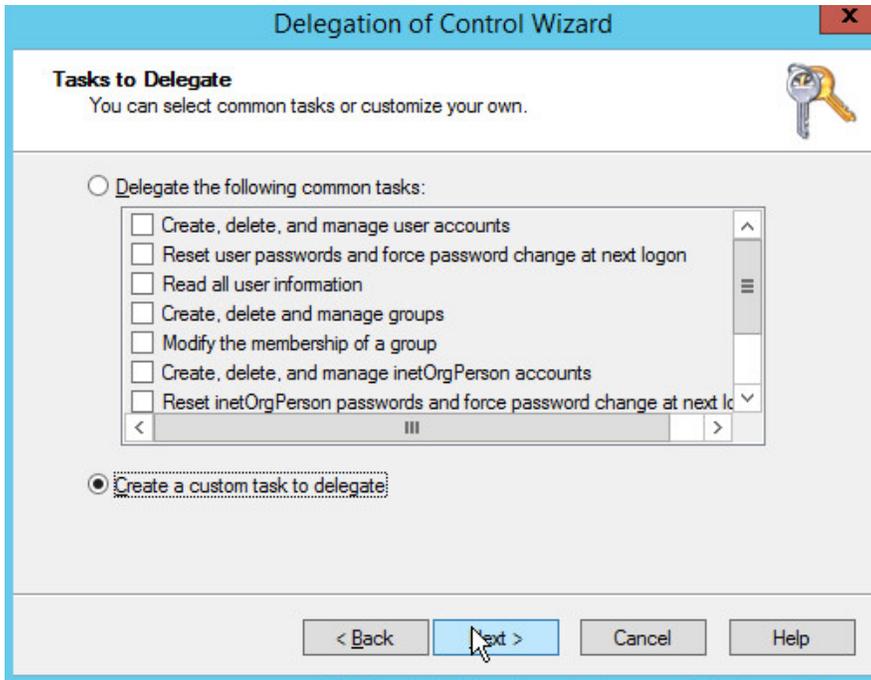


377 8. Click **OK**.



378 9. Click **Next**.

379 10. Choose **Create a custom task to delegate**.



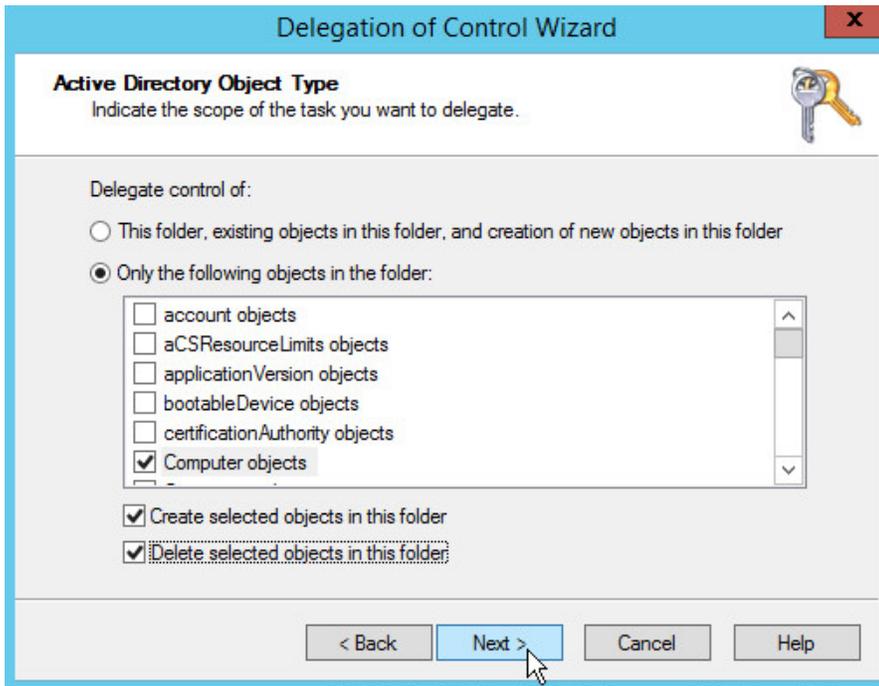
380 11. Click **Next**.

381 12. Choose **Only the following objects in the folder**.

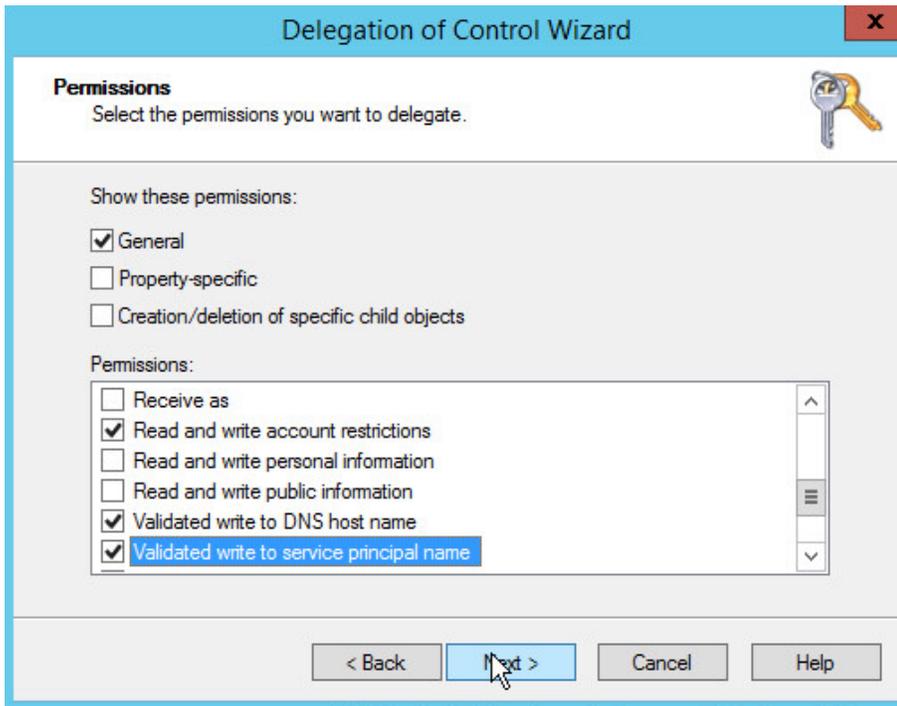
382 13. Check the box next to **Computer objects**.

383 14. Check the box next to **Create selected objects in this folder**.

384 15. Check the box next to **Delete selected objects in this folder**.



- 385 16. Click **Next**.
- 386 17. Check the boxes next to **Reset password, Read and write account restrictions, Validated write**
- 387 **to DNS host name, and Validated write to service principal name.**



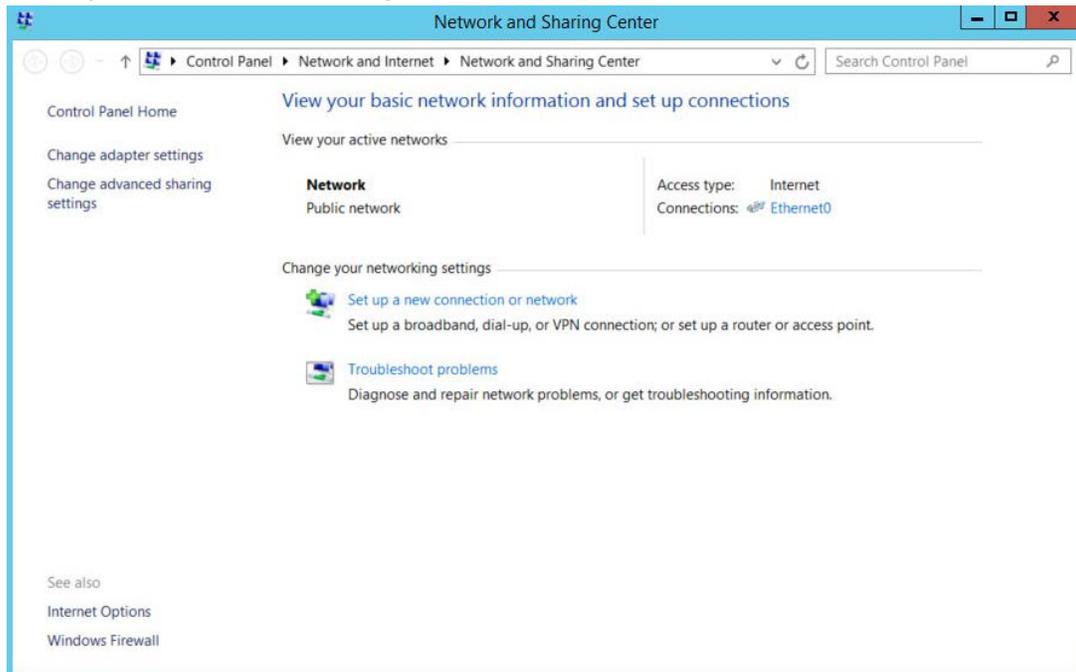
388 18. Click **Next**.



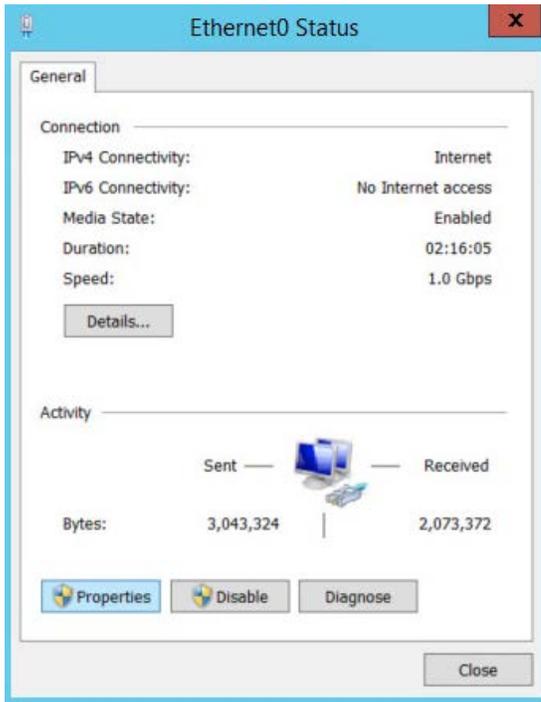
389 19. Click **Finish**.

390 **2.1.4 Adding Machines to the Domain**

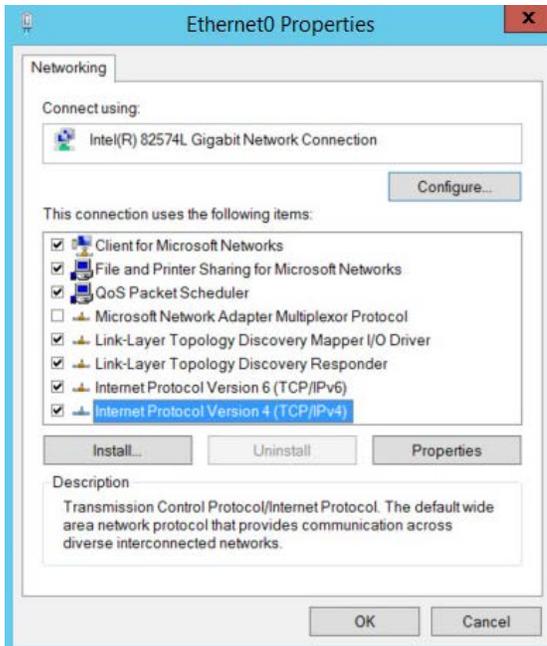
- 391 1. Right-click the network icon in the task bar on a computer that you wish to add to the domain.  
392 2. Click **Open Network and Sharing Center**.



- 393 3. Click the name of the internet adapter.



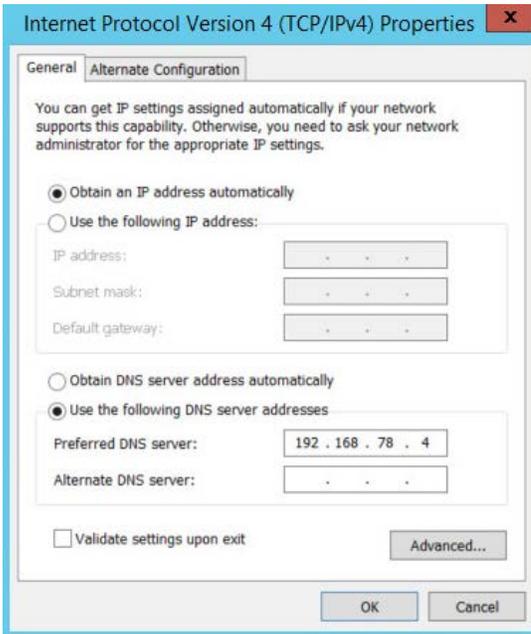
394 4. Click **Properties**.



395 5. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.

396 6. Select **Use the following DNS server addresses**.

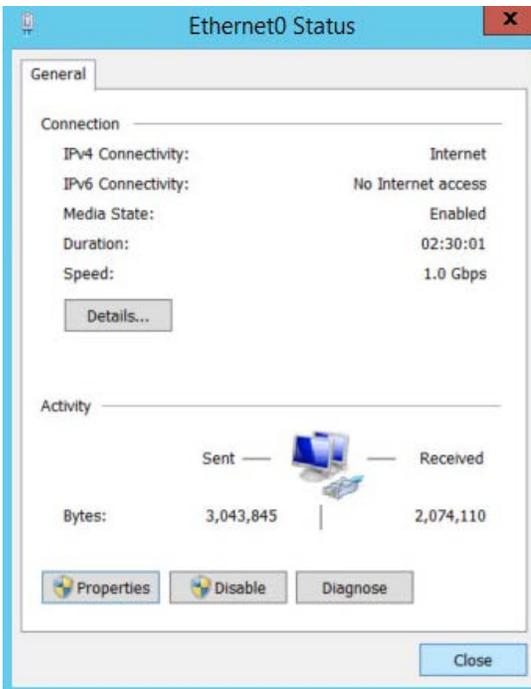
397 7. Enter the **IP address** of the DNS server.



398 8. Click **OK**.

399 9. Click **OK**.

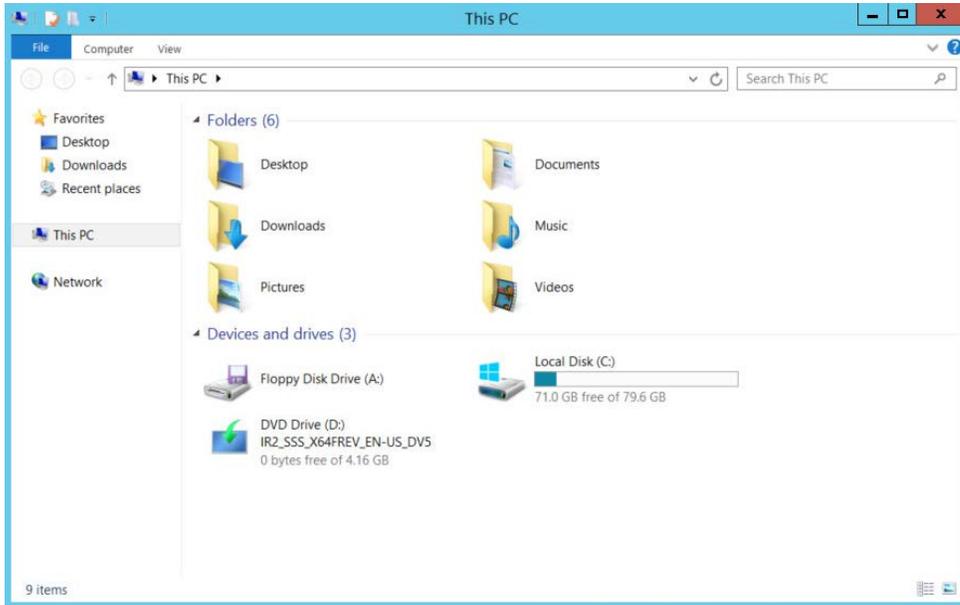
400



401 10. Click **Close**.

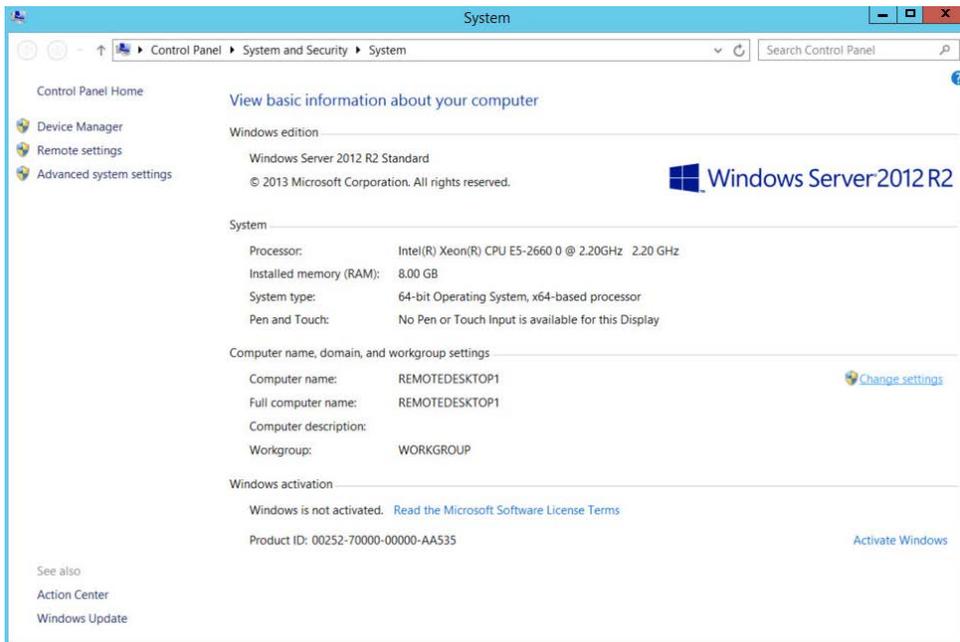
402

403 11. Navigate to **This PC**.



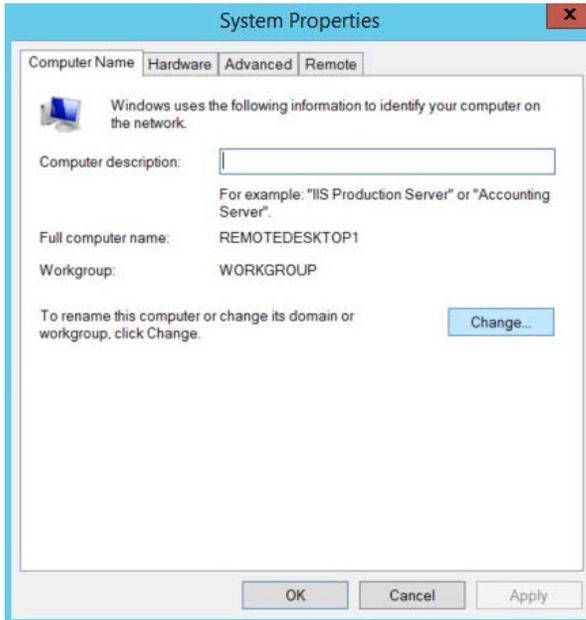
404

405 12. Right-click in the window and click **Properties**.



406

407 13. Click **Change Settings**.



408

409

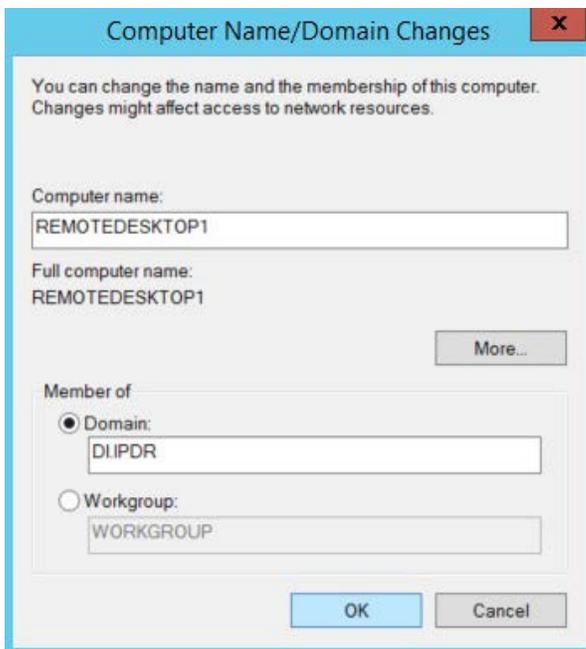
410

411

14. Click **Change**.

15. Select **Domain**.

16. Enter the domain.

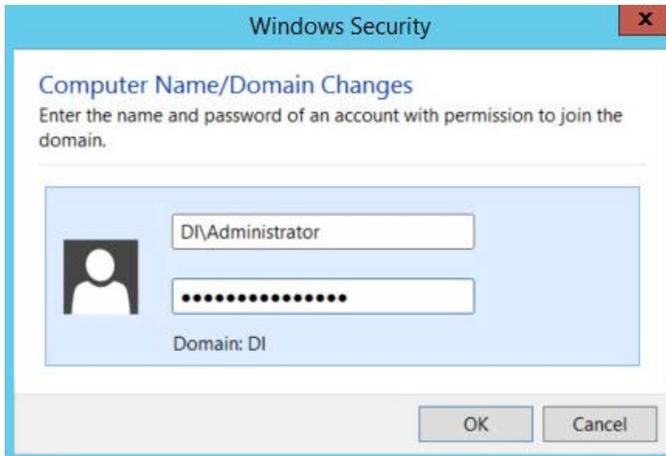


412

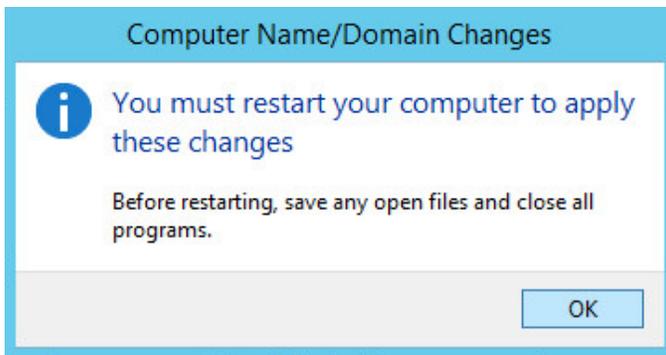
413

17. Click **OK**.

- 414 18. Enter the **username** and **password** of an account with privileges to add computers to the  
415 domain.



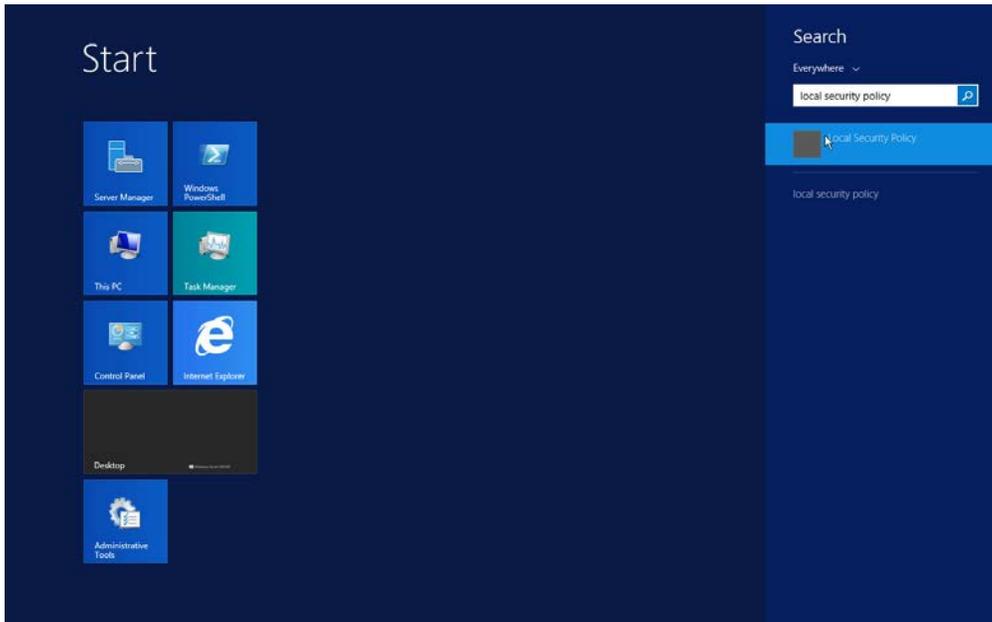
- 416  
417 19. Click **OK**.



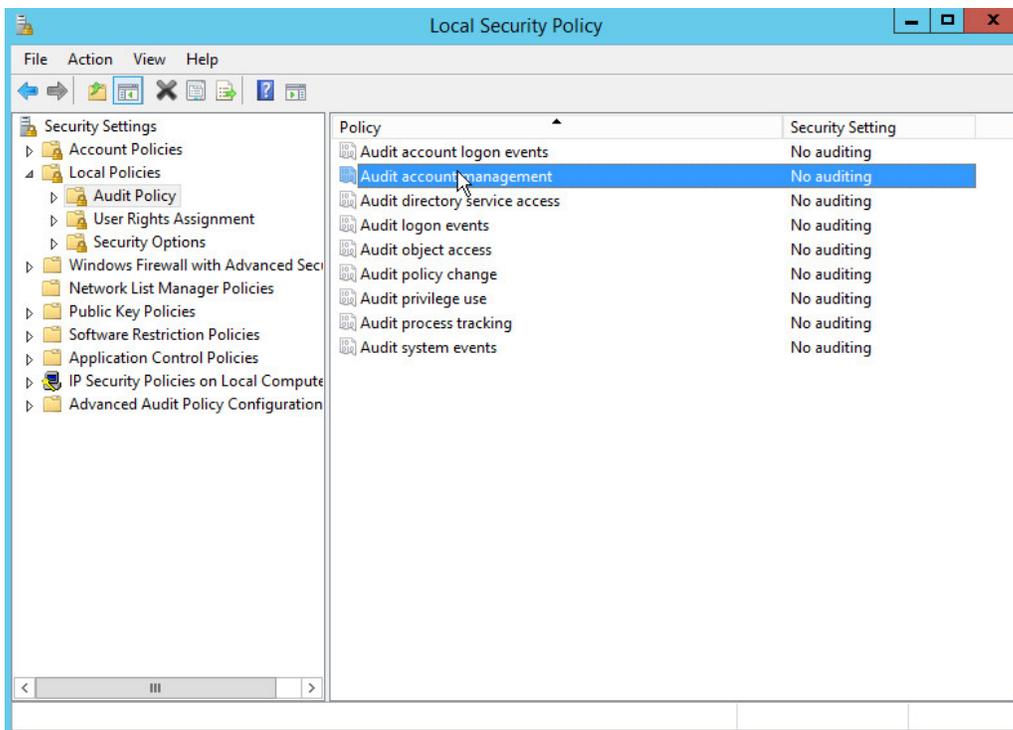
- 418  
419 20. Click **OK** when prompted to restart the computer.

## 420 2.1.5 Configure Active Directory to Audit Account Activity

- 421 1. Open the Start menu.

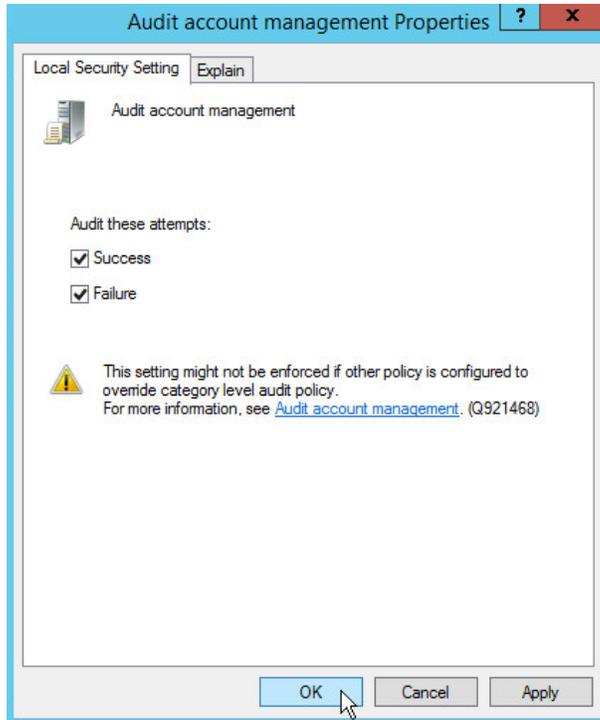


- 422
- 423 2. Enter "Local Security Policy" in the search bar and open the program.
- 424 3. Navigate to **Local Policies > Audit Policy**.
- 425 4. Right-click **Audit account management**.



426

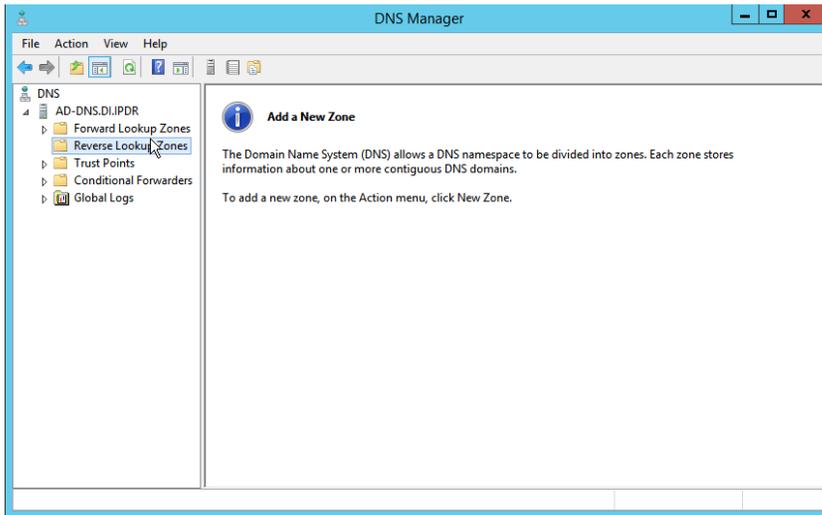
- 427 5. Click **Properties**.
- 428 6. Check the boxes next to **Success** and **Failure**.



- 429
- 430 7. Click **OK**.

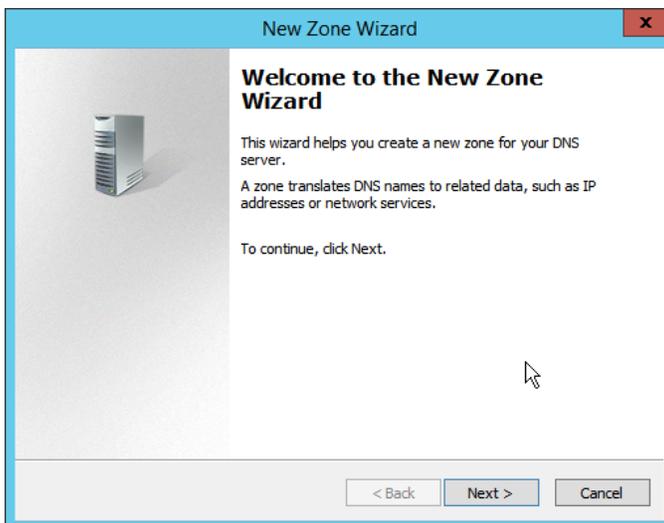
### 431 2.1.6 Configure Reverse Lookup Zones

- 432 1. Open **DNS Manager** by right-clicking the DNS server in **Server Manager**.
- 433 2. Click **Reverse Lookup Zones**.



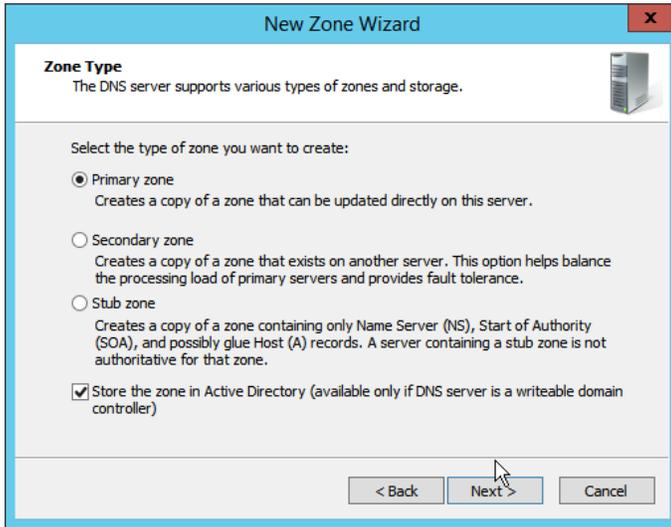
434  
435

3. Click **Action > New Zone**.



436  
437

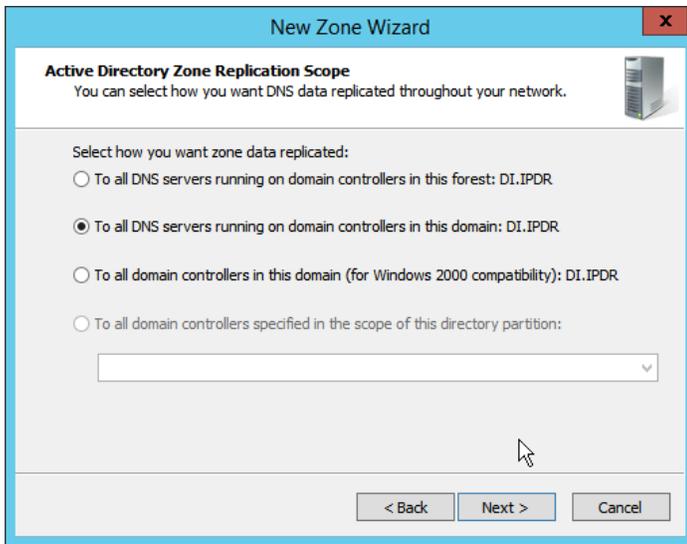
4. Click **Next**.



438

439

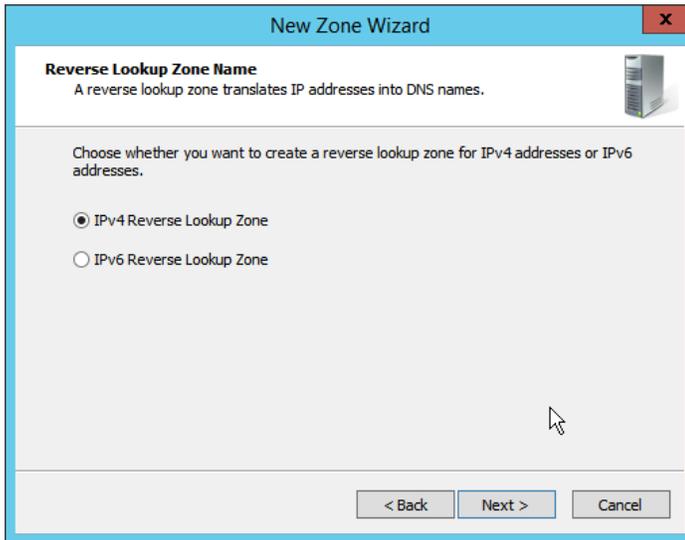
5. Click **Next**.



440

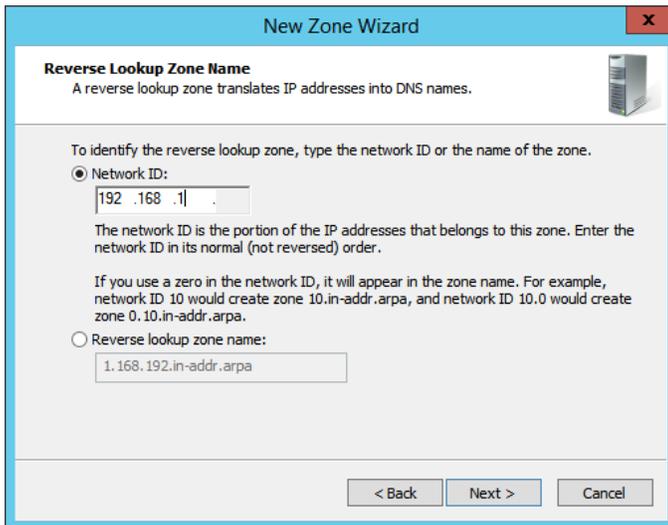
441

6. Click **Next**.



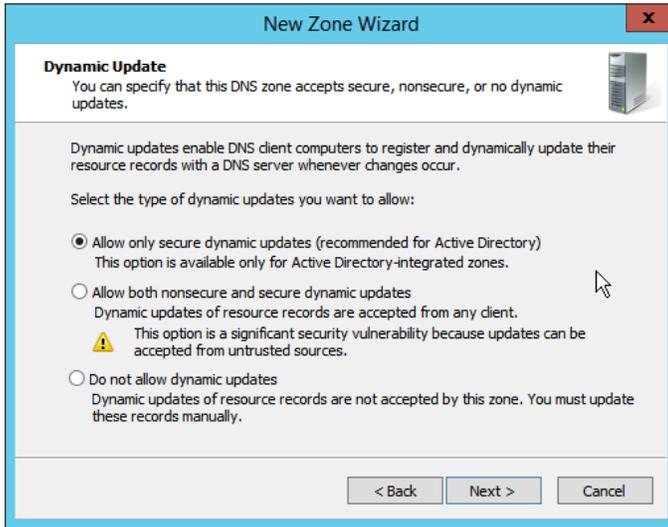
442  
443  
444  
445

7. Click **Next**.
8. Enter the first three parts of the IP address of the Active Directory (AD)/DNS server (for example, 192.168.1).



446  
447

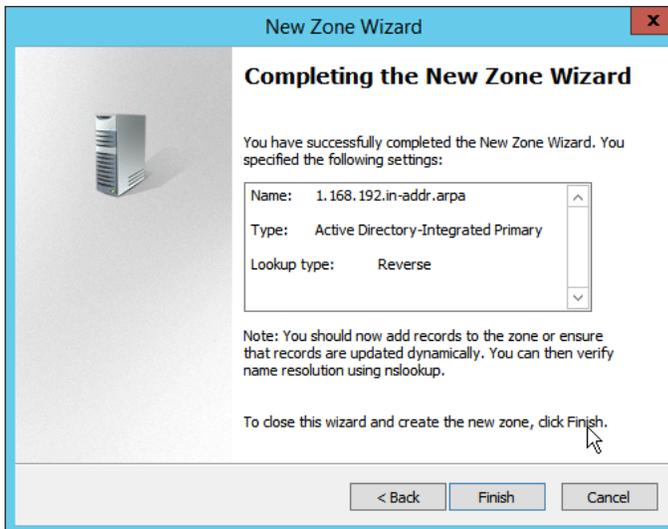
9. Click **Next**.



448

449

10. Click **Next**.



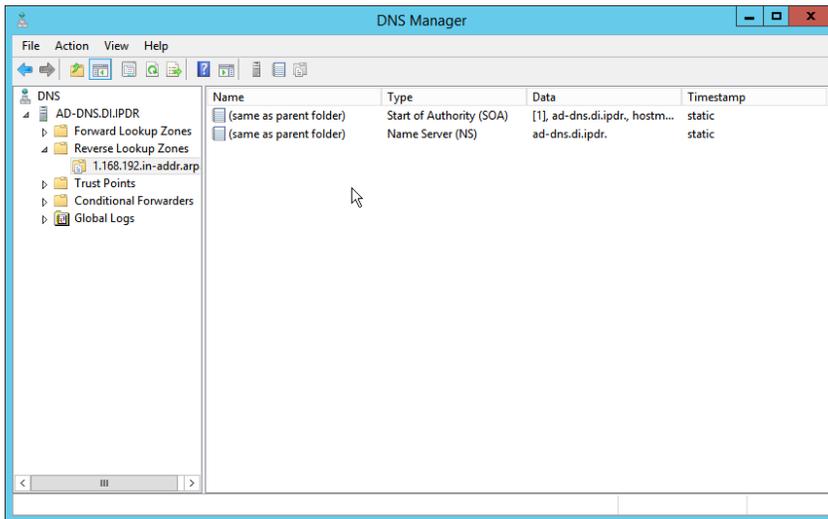
450

451

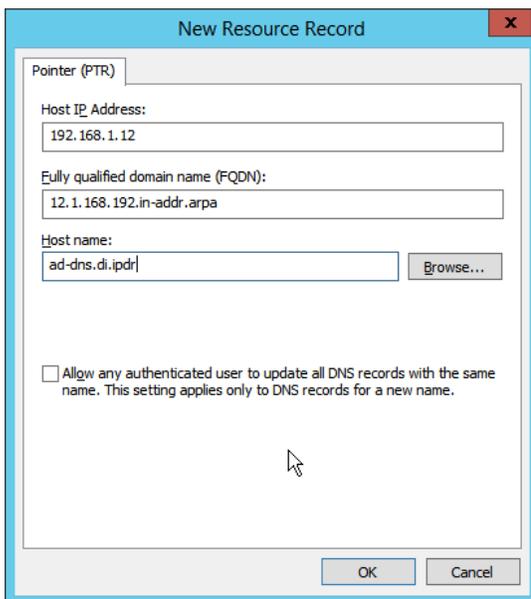
452

11. Click **Finish**.

12. Click on the newly created reverse lookup zone.

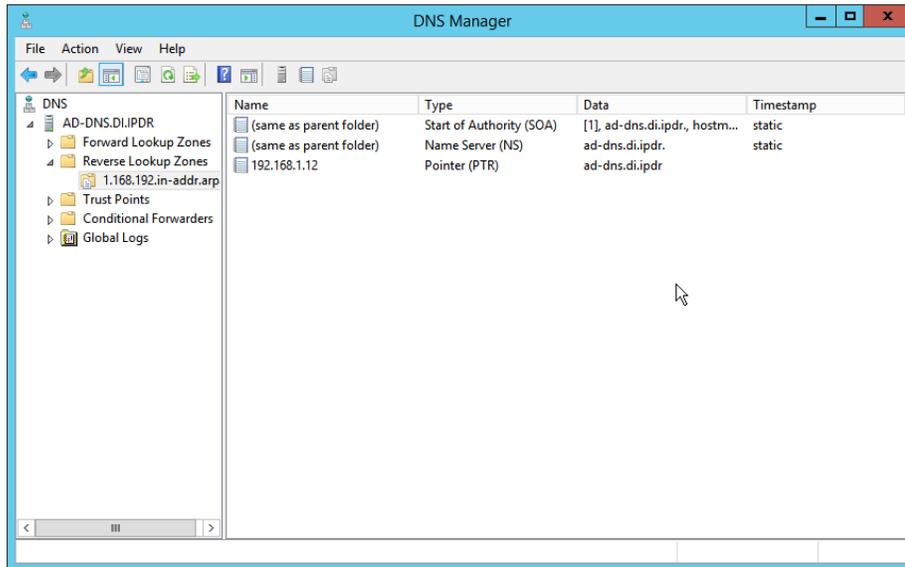


453

454 13. Right-click in the window and select **New Pointer (PTR)....**455 14. Enter the **IP address** of the AD/DNS server.456 15. Enter the **hostname** of the AD/DNS server.

457

458 16. Click **OK**.



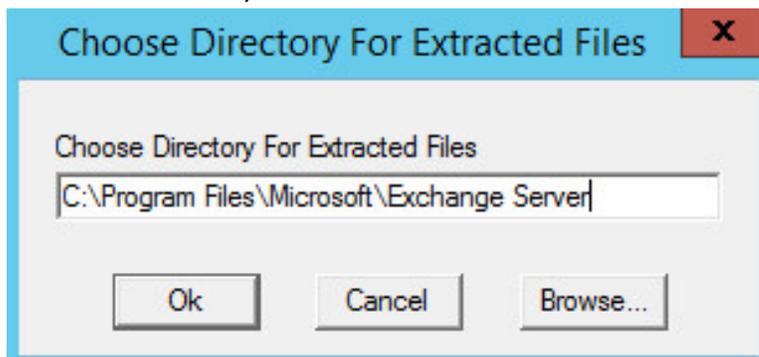
459

## 460 2.2 Microsoft Exchange Server

461 As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the  
 462 installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2  
 463 machine.

### 464 2.2.1 Install Microsoft Exchange

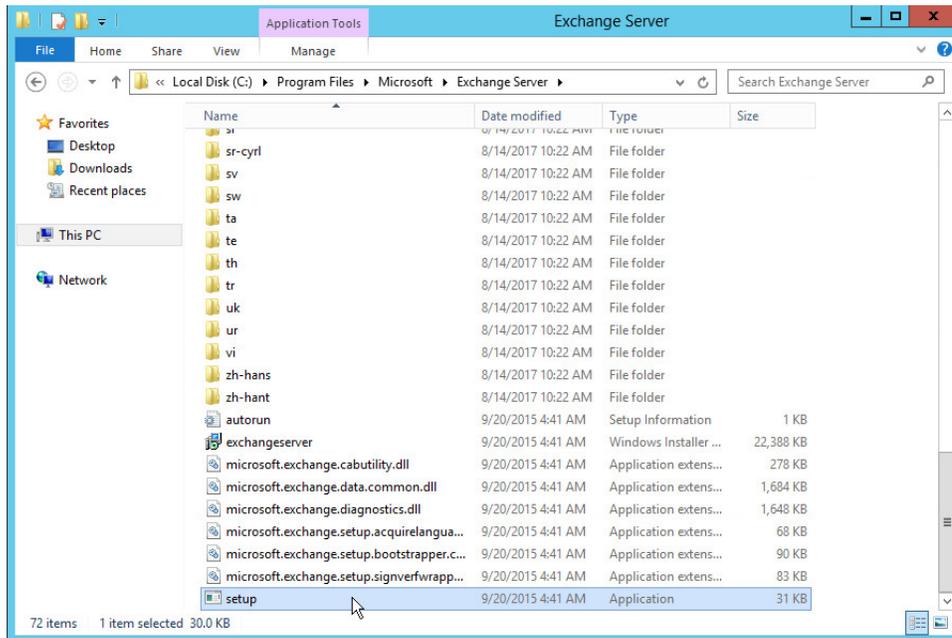
- 465 1. Run **Exchange2016-x64.exe**.
- 466 2. Choose the directory for the extracted files.



467

468

3. Click **OK**.

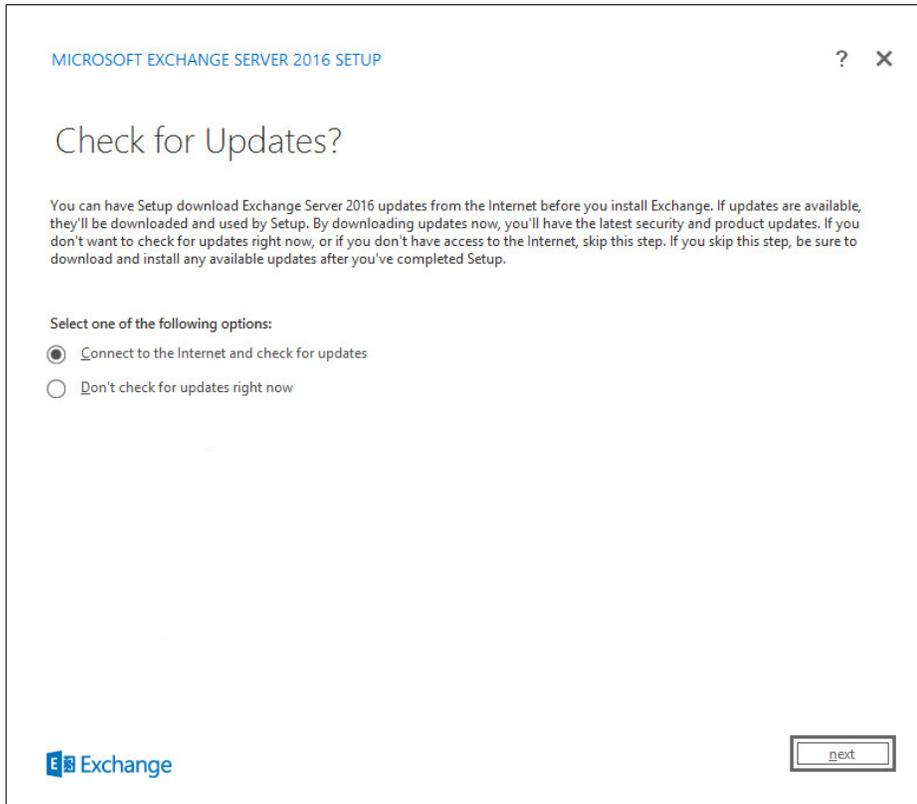


469

470

471

4. Enter the directory and run **setup.exe**.
5. Select **Connect to the Internet and check for updates**.

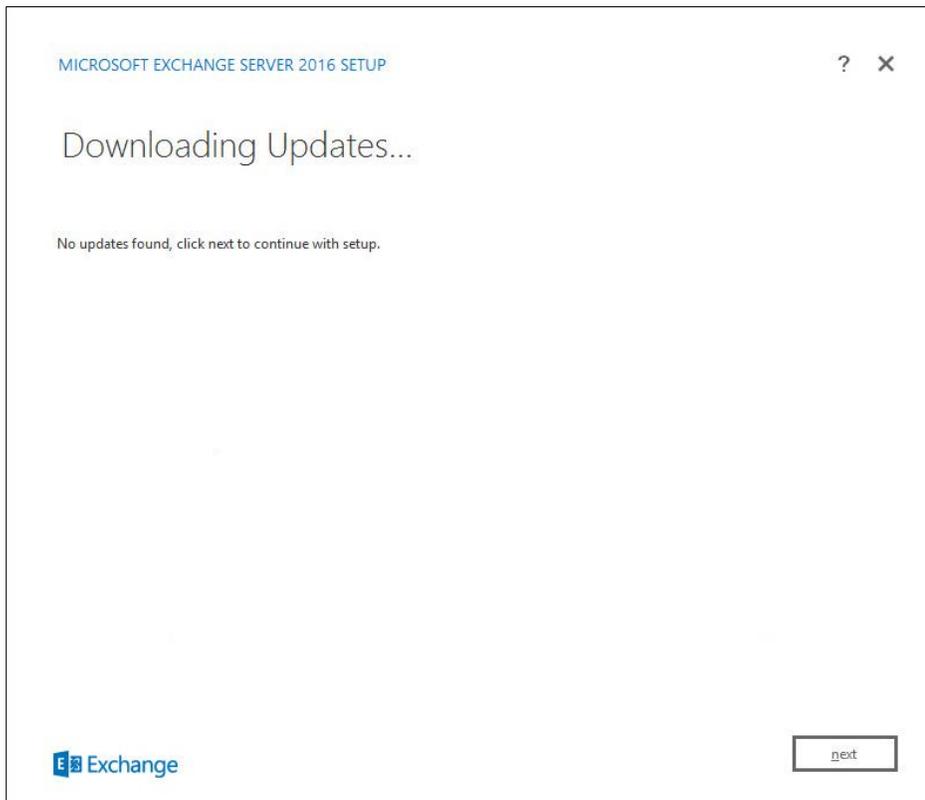


472

473

474

6. Click **Next**.
7. Wait for the check to finish.

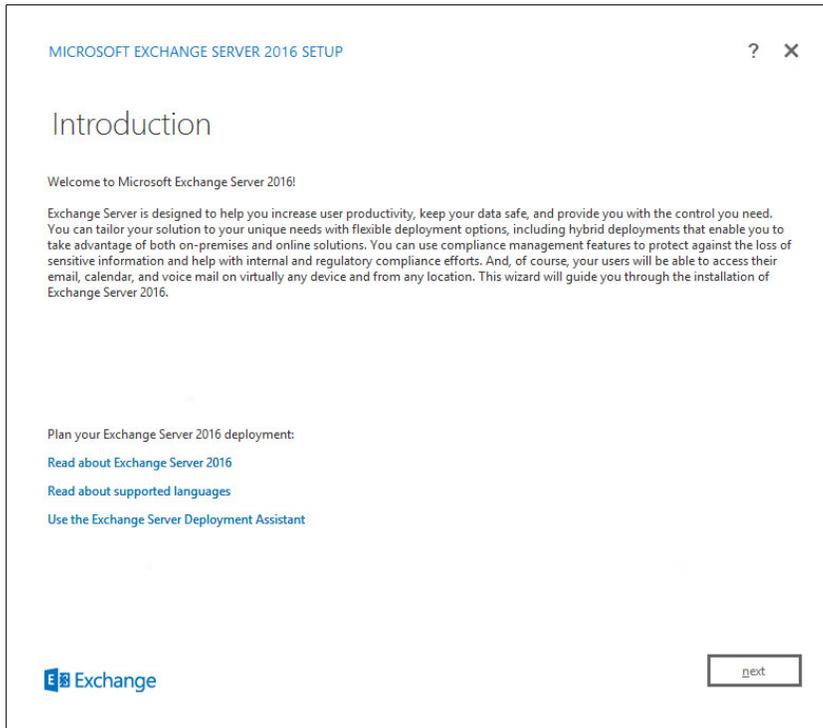


475

476

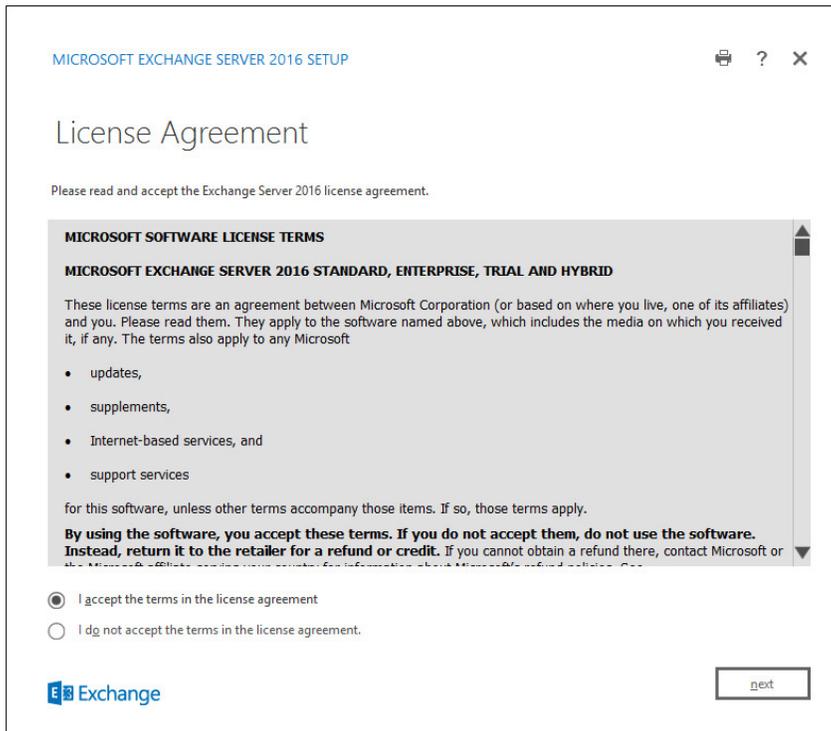
477

8. Click **Next**.
9. Wait for the copying to finish.



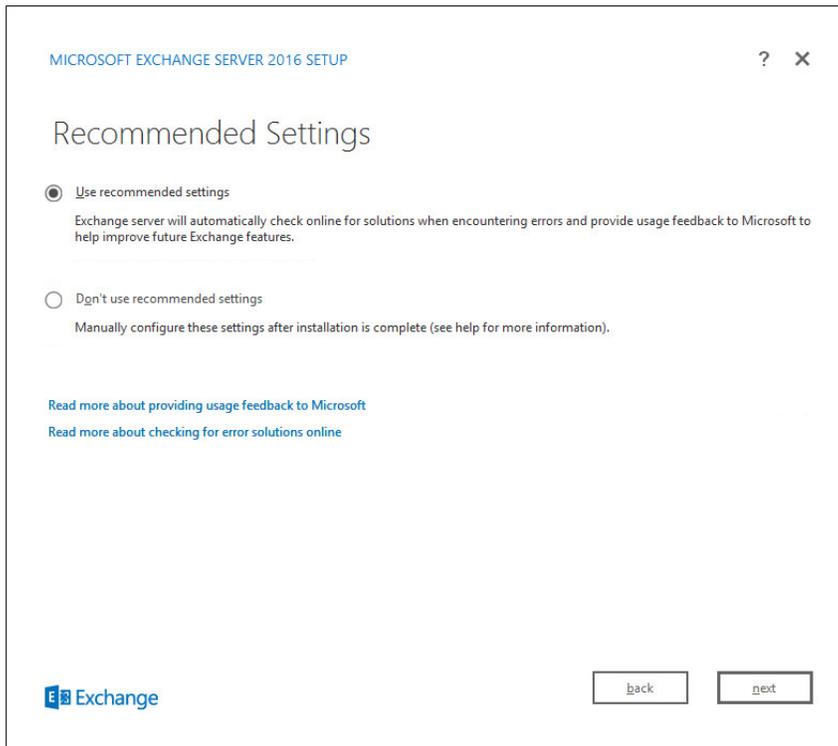
478  
479  
480

10. Click **Next**.
11. Click **I accept the terms in the license agreement**.



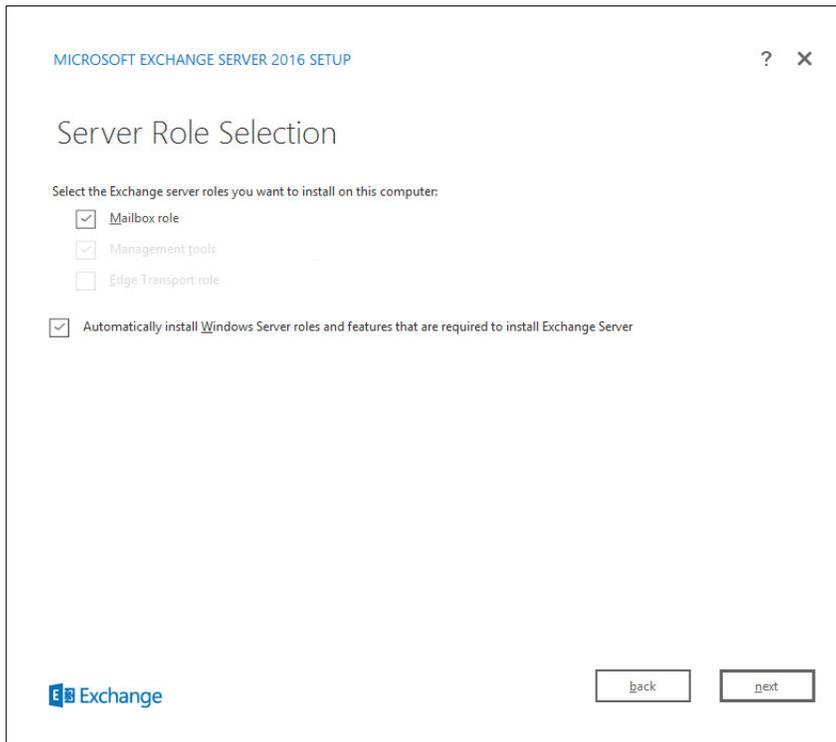
481  
482  
483

- 12. Click **Next**.
- 13. Click **Use Recommended Settings**.



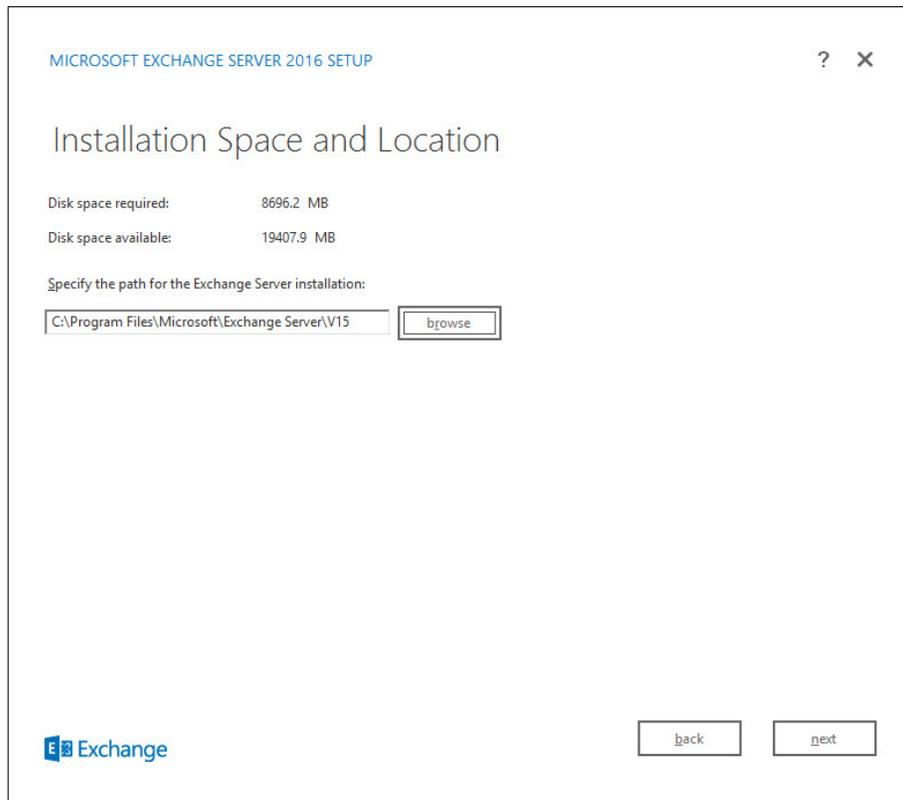
484  
485  
486  
487  
488

14. Click **Next**.
15. Check **Mailbox role**.
16. Check **Automatically install Windows Server roles and features that are required to install Exchange Server**.



489  
490  
491

- 17. Click **Next**.
- 18. Specify the installation path for MS Exchange.



492

493

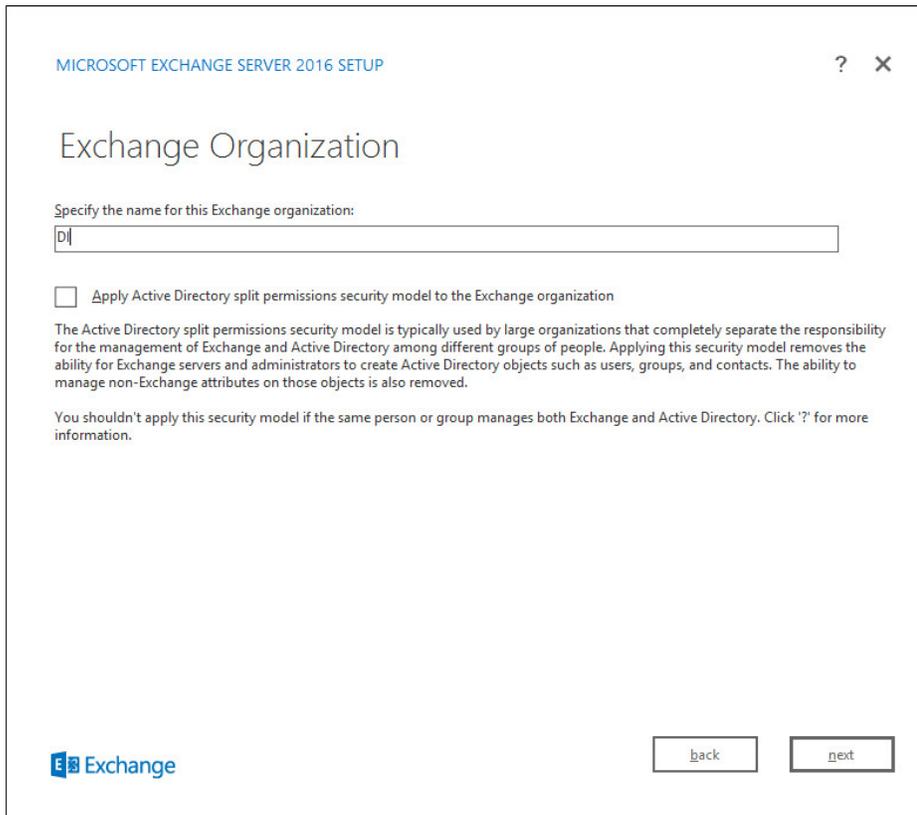
494

495

19. Click **Next**.

20. Specify the name for the Exchange organization, e.g., DI.

21. Decide whether to apply split permissions based on the needs of the enterprise.



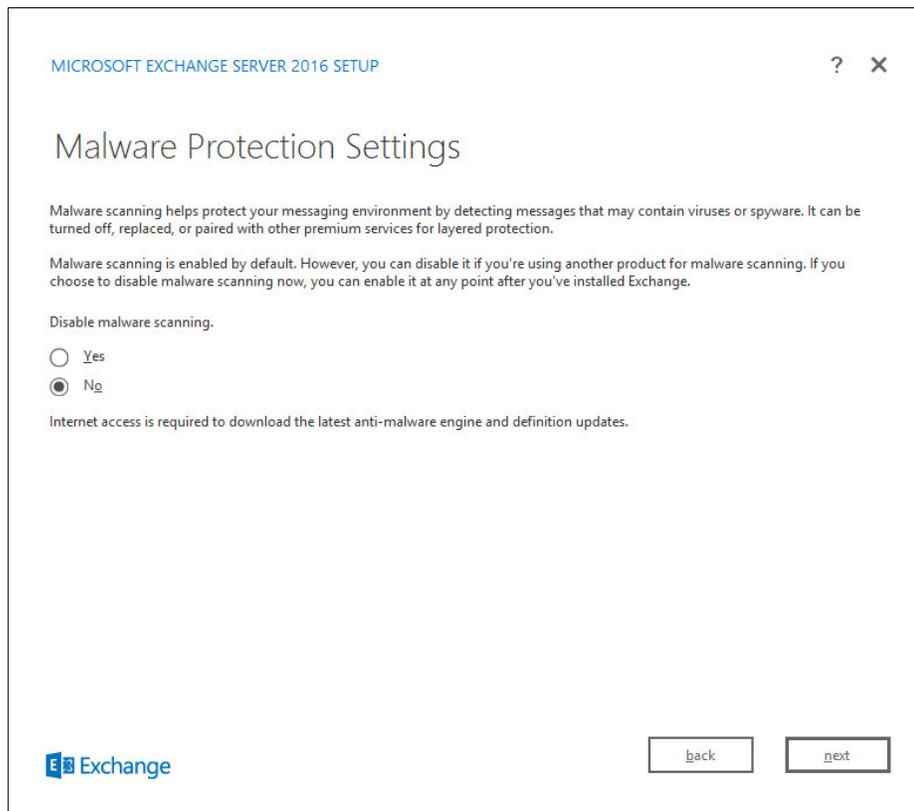
496

497

498

22. Click **Next**.

23. Select **No**.



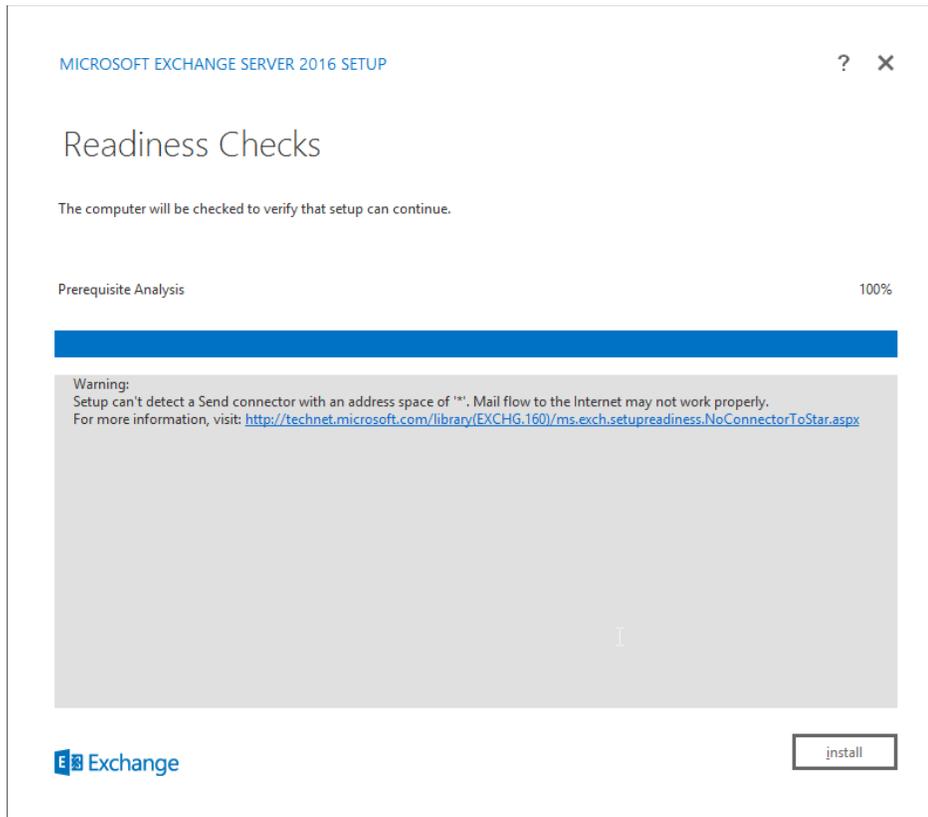
499

500

501

502

24. Click **Next**.25. Install any **prerequisites** listed.26. If necessary, restart the server and rerun **setup.exe**, following through steps 3–22 again.



503

504 27. Click **Install**.

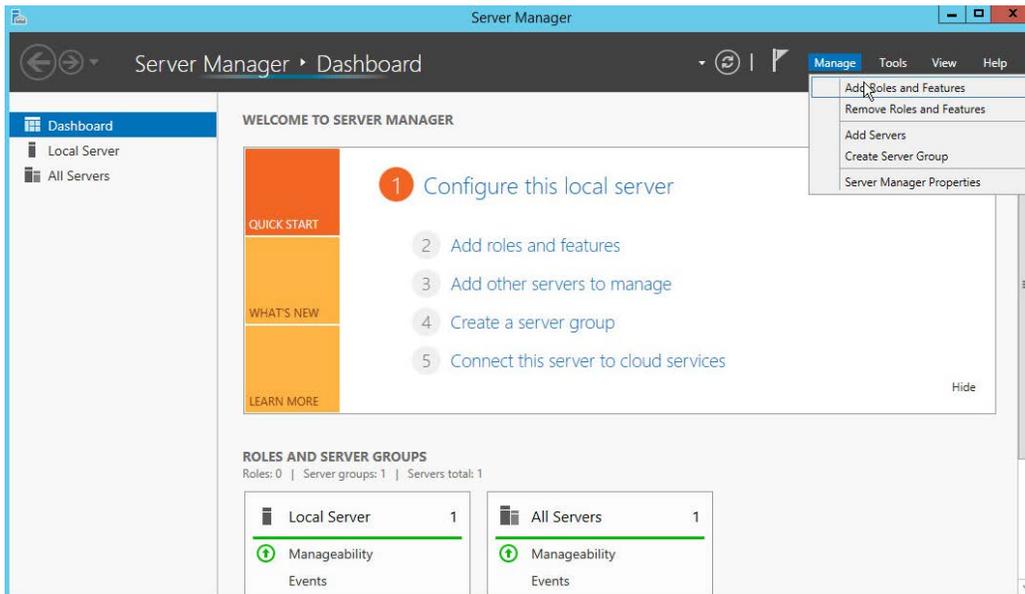
## 505 2.3 Windows Server Hyper-V Role

506 As part of our simulated enterprise, we include a Windows Hyper-V server. This section covers the  
507 instructions for installing the Windows Server Hyper-V Role on a Windows Server 2012 R2 machine.

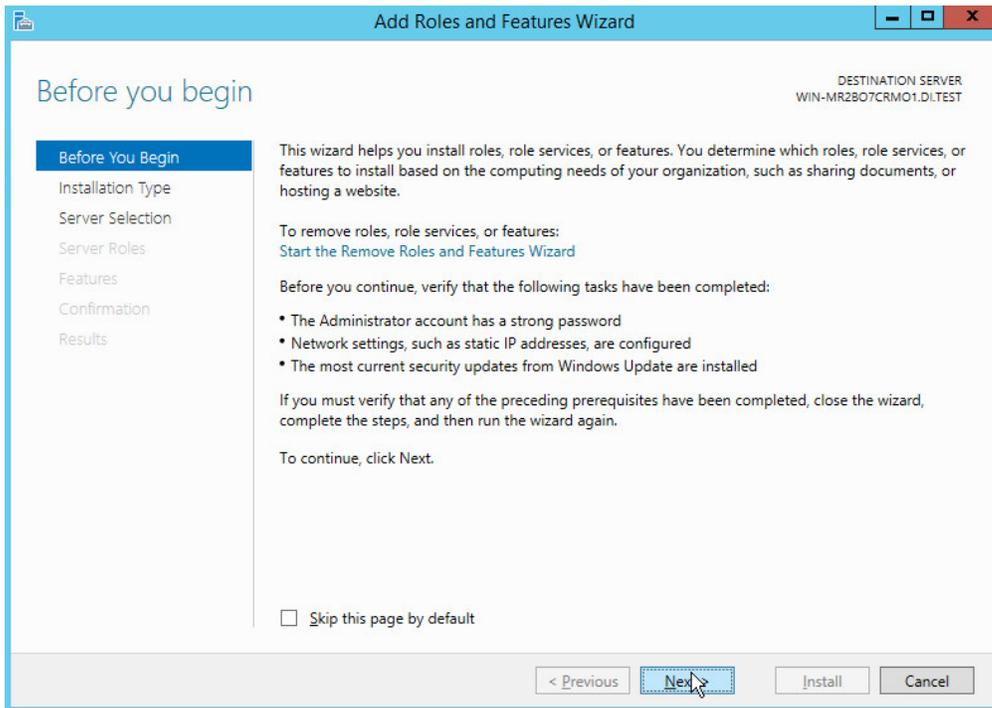
508 The instructions for enabling the Windows Server Hyper-V Role are retrieved from  
509 [https://technet.microsoft.com/en-us/library/hh846766\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh846766(v=ws.11).aspx) and are replicated below for  
510 preservation and ease of use.

### 511 2.3.1 Production Installation

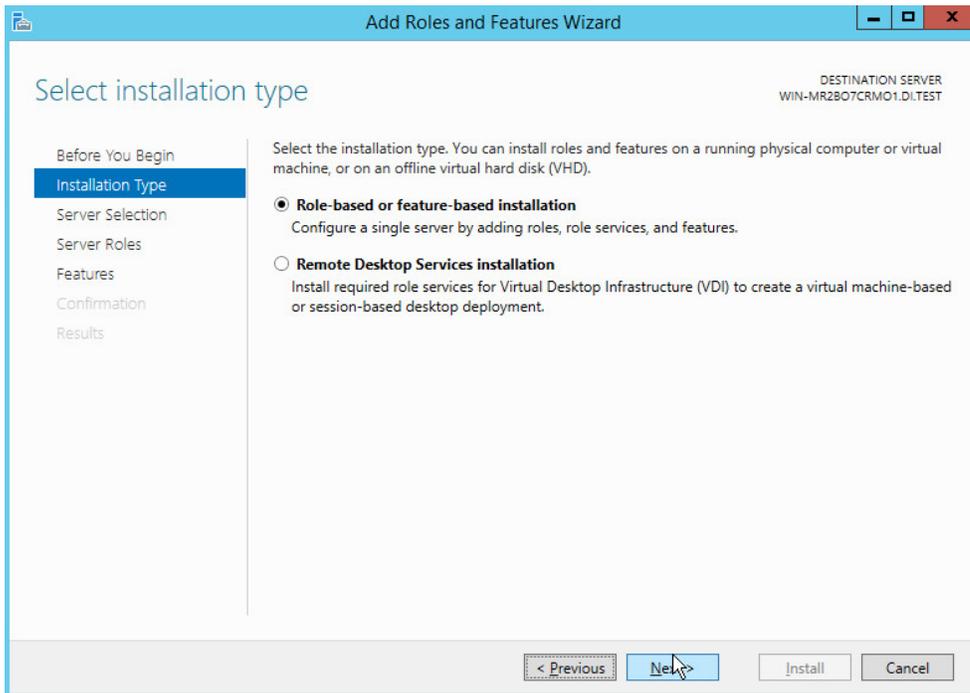
512 1. In **Server Manager** on the **Manage** menu, click **Add Roles and Features**.



- 513  
514  
515
2. On the **Before you begin** page, verify that your destination server and network environment are prepared for the role and feature you want to install.

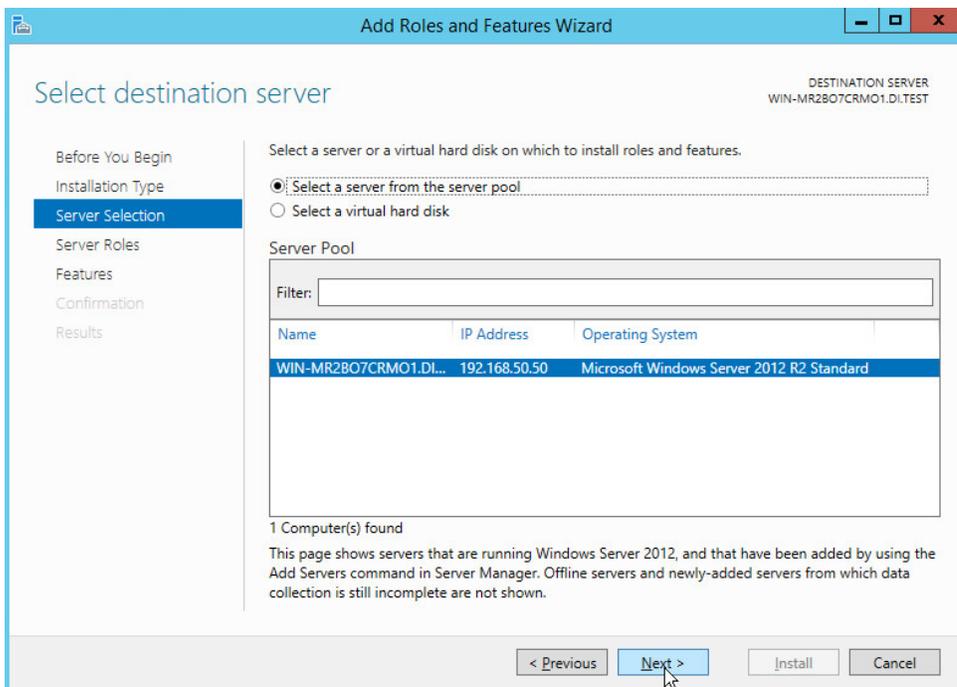


- 516  
517  
518
3. Click **Next**.
  4. On the **Select installation type** page, select **Role-based or feature-based installation**.



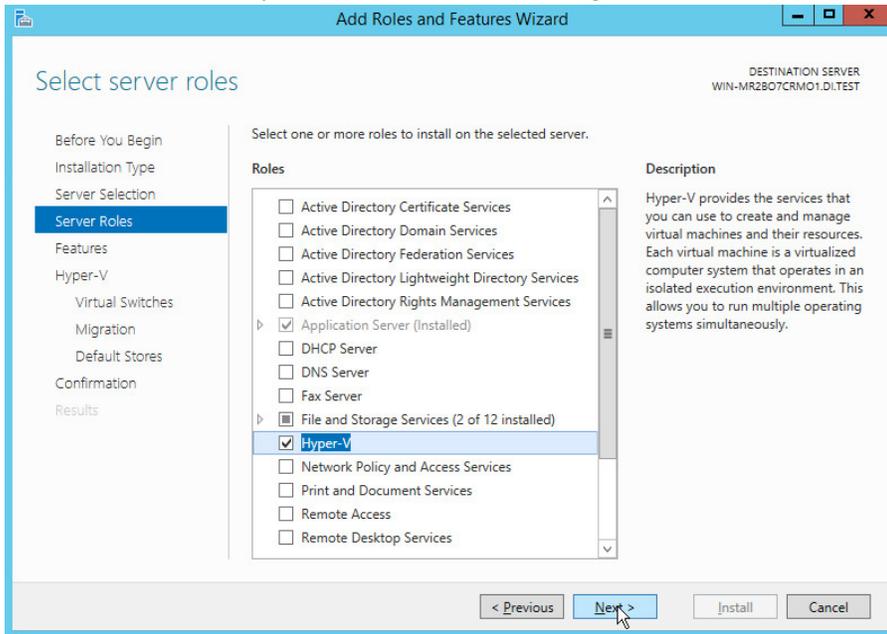
519  
520  
521

5. Click **Next**.
6. On the **Select destination server** page, select a server from the server pool.

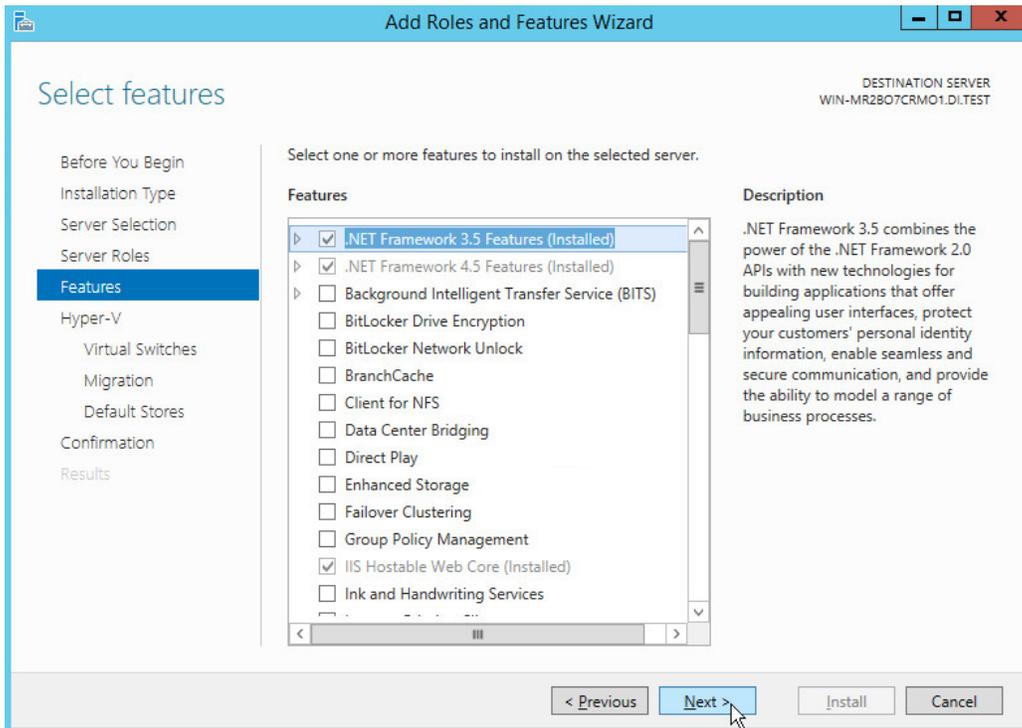


522

- 523 7. Click **Next**.
- 524 8. On the **Select server roles** page, select **Hyper-V**.
- 525 9. To add the tools that you use to create and manage virtual machines, click **Add Features**.



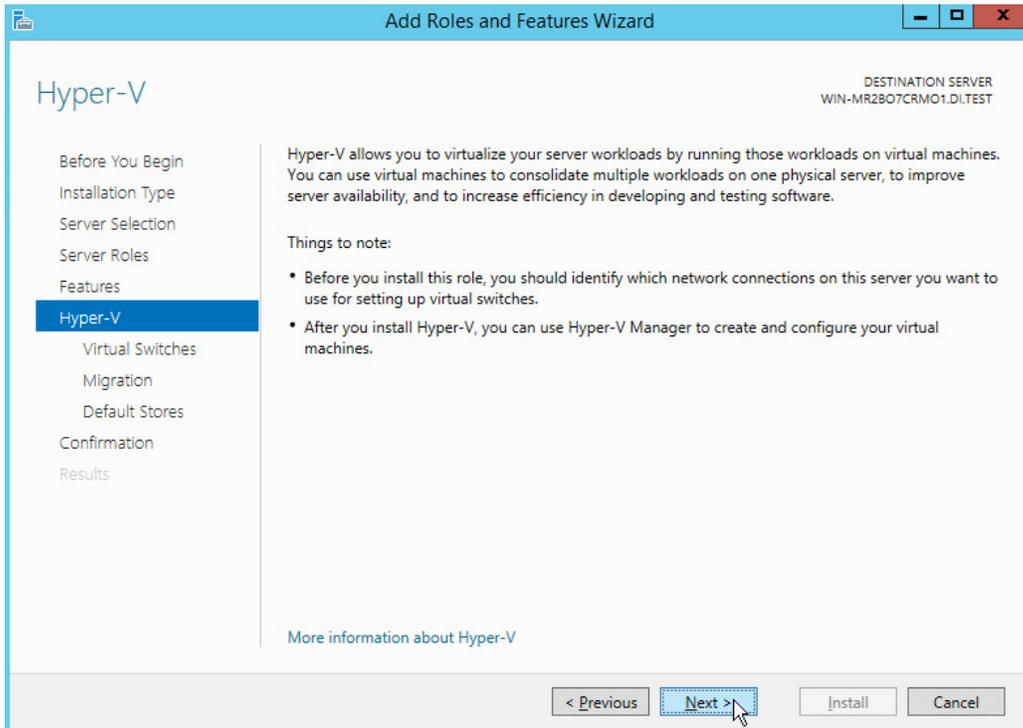
- 526 10. Click **Next**.
- 527



528

529

11. Click **Next**.



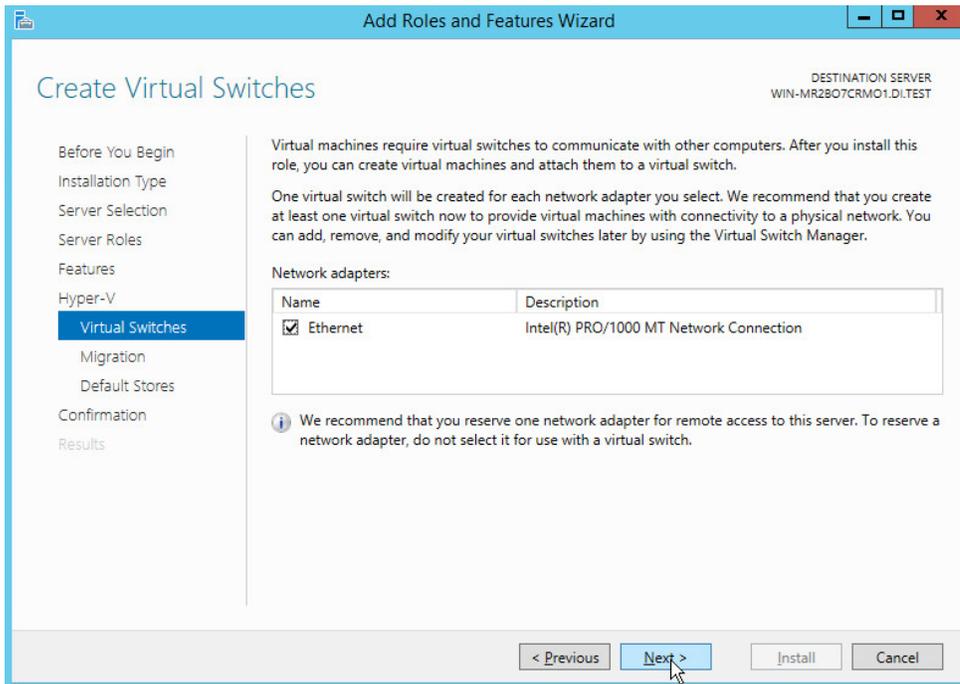
530

531

532

12. Click **Next**.

13. On the **Create Virtual Switches** page, select the appropriate options.



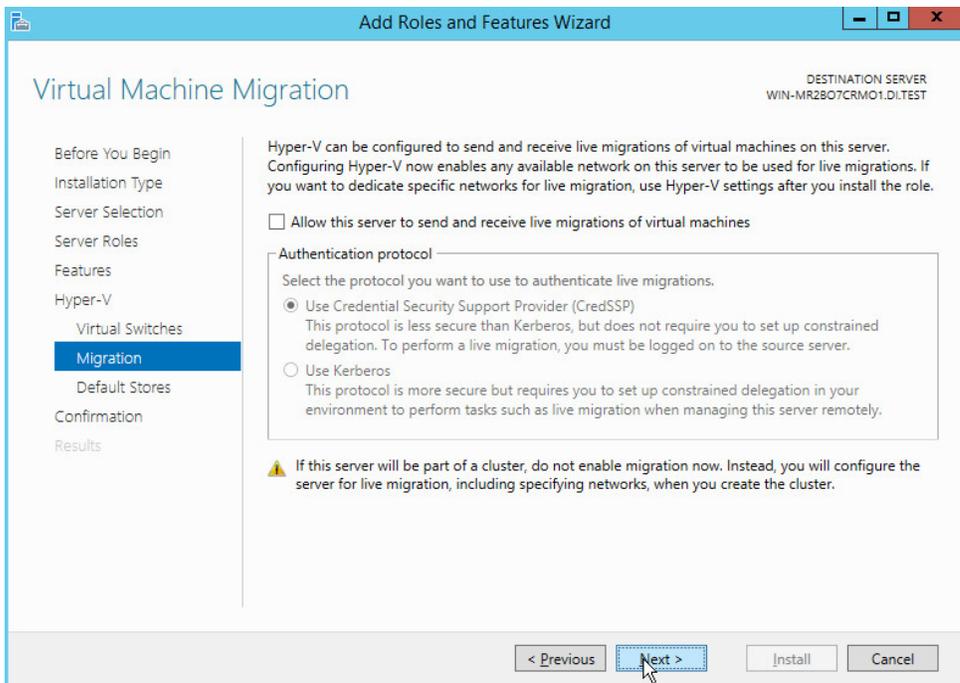
533

14. Click **Next**.

534

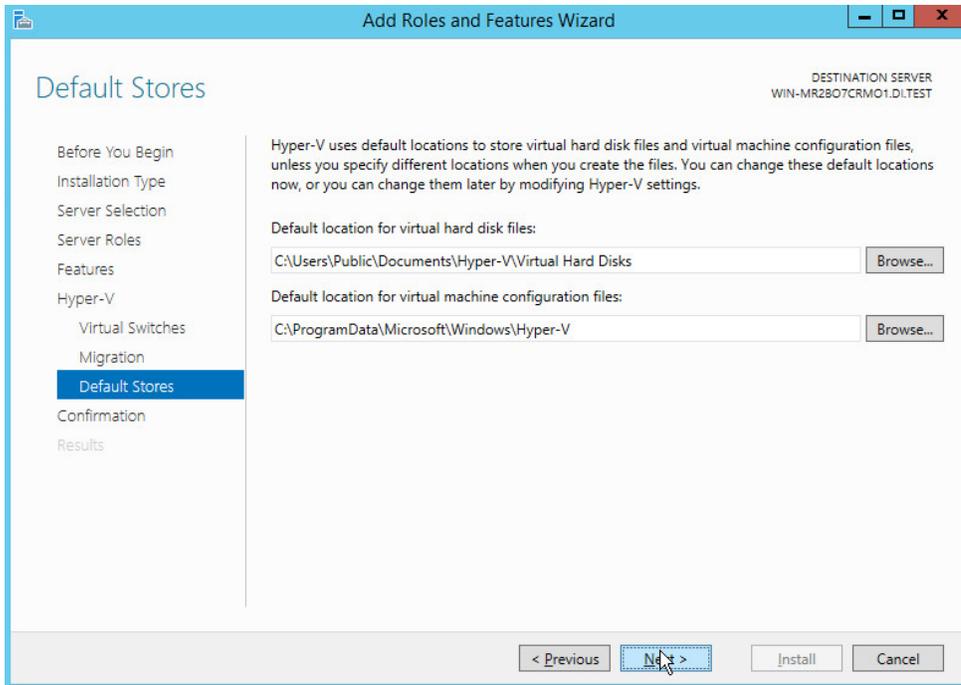
15. On the **Virtual Machine Migration** page, select the appropriate options.

535

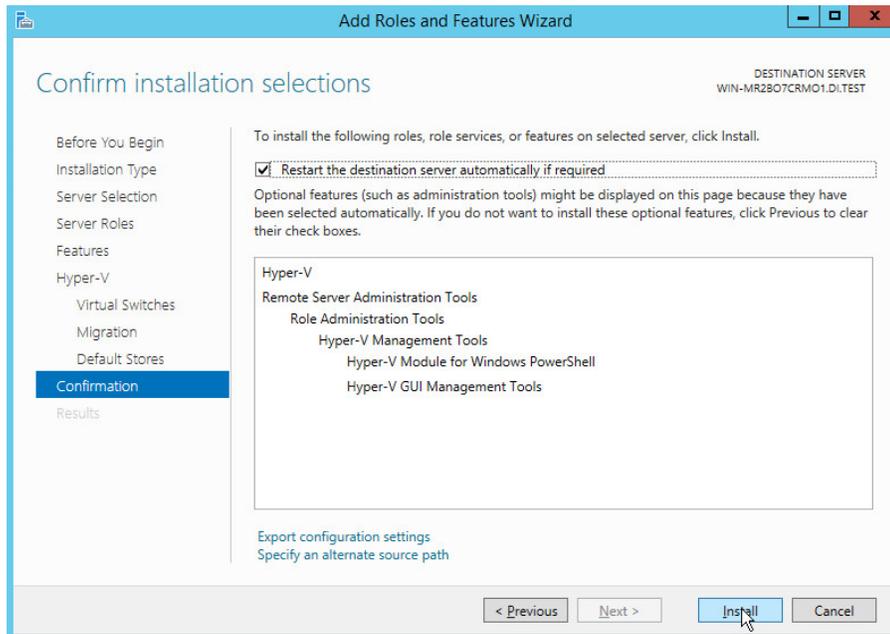


536

- 537 16. Click **Next**.
- 538 17. On the **Default Stores** page, select the appropriate options.



- 539
- 540 18. Click **Next**.
- 541 19. On the **Confirm installation selections** page, select **Restart the destination server automatically if required**.
- 542



543

544 20. Click **Install**.

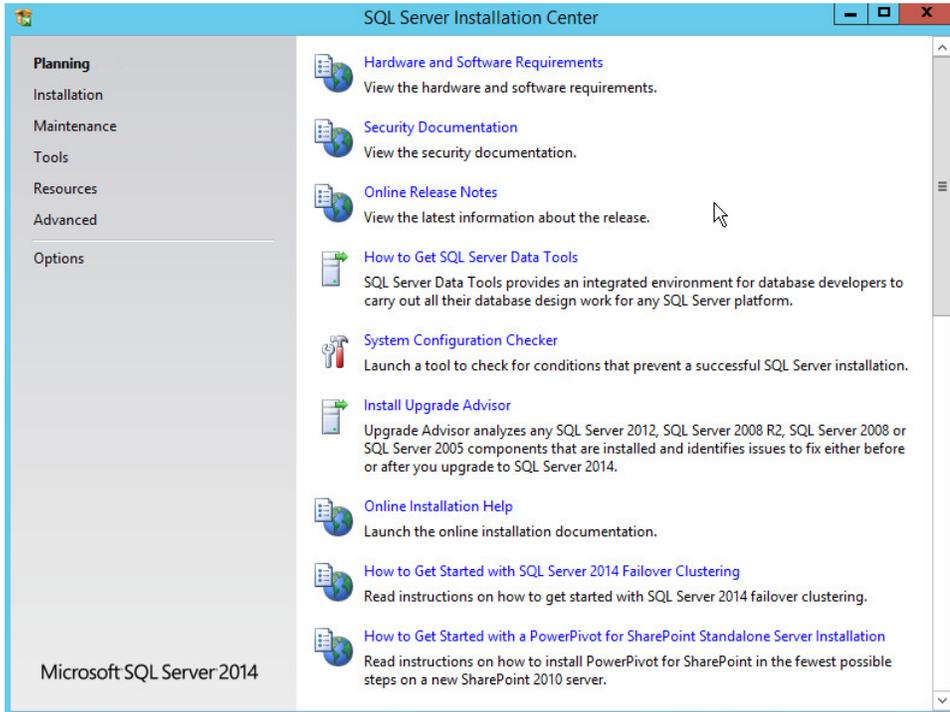
545 21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page  
 546 in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and**  
 547 **Features** tile on the page for the selected server.

## 548 2.4 MS SQL Server

549 As part of both our enterprise emulation and data integrity solution, we include a Microsoft SQL Server.  
 550 This section covers the installation and configuration process used to set up Microsoft SQL Server on a  
 551 Windows Server 2012 R2 machine.

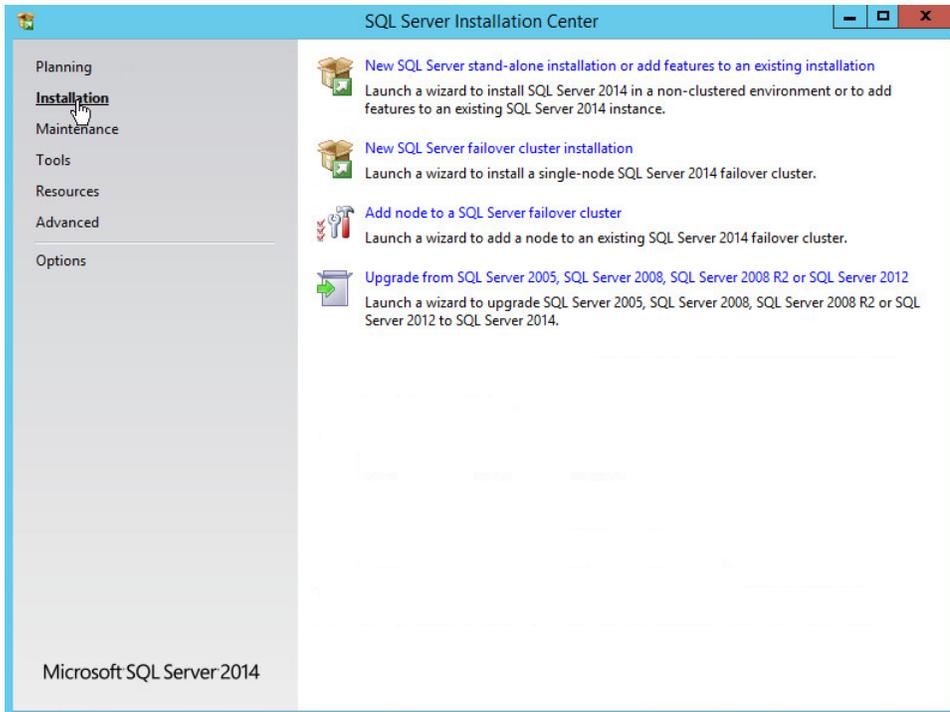
### 552 2.4.1 Install and Configure MS SQL

- 553 1. Acquire **SQL Server 2014 installation media**.
- 554 2. Locate the installation media in the machine and click on **SQL2014\_x64\_ENU** to launch **SQL**  
 555 **Server Installation Center**.



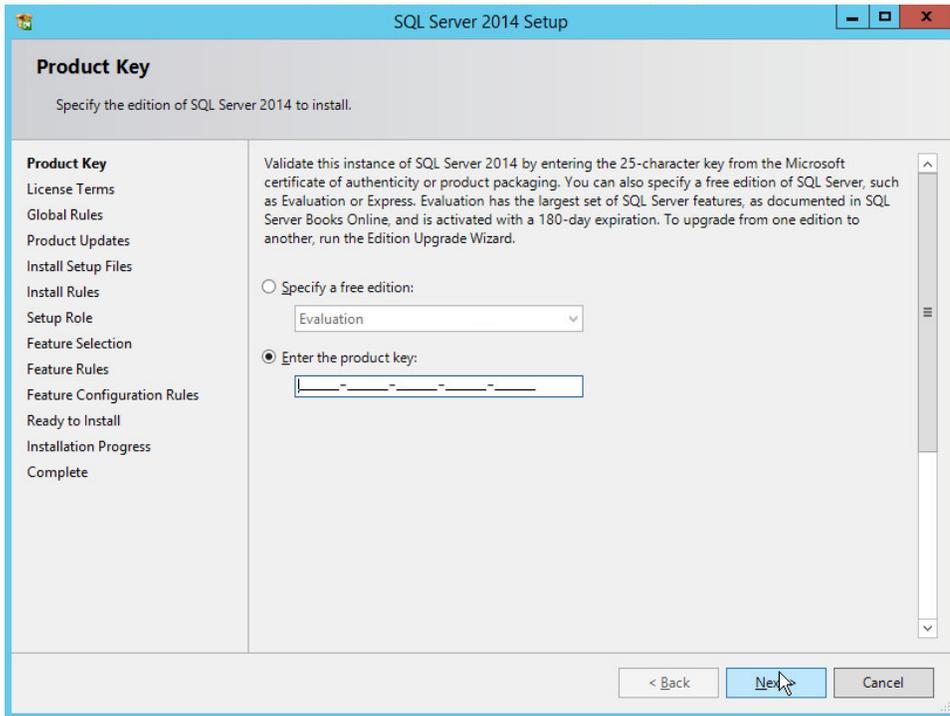
556

557 3. On the left menu, select **Installation**.

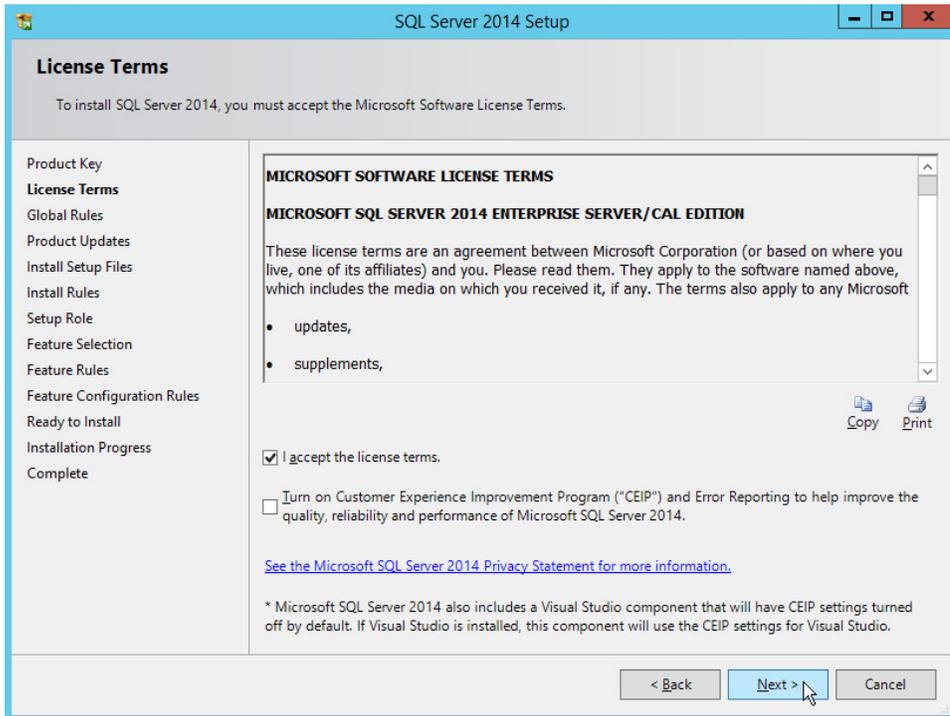


558

- 559 4. Select **New SQL Server stand-alone installation or add features to an existing installation**. This  
560 will launch the SQL Server 2014 setup.  
561 5. In the **Product Key** section, enter your product key.



- 562  
563 6. Click **Next**.  
564 7. In the **License Terms** section, read and click **I accept the license terms**.

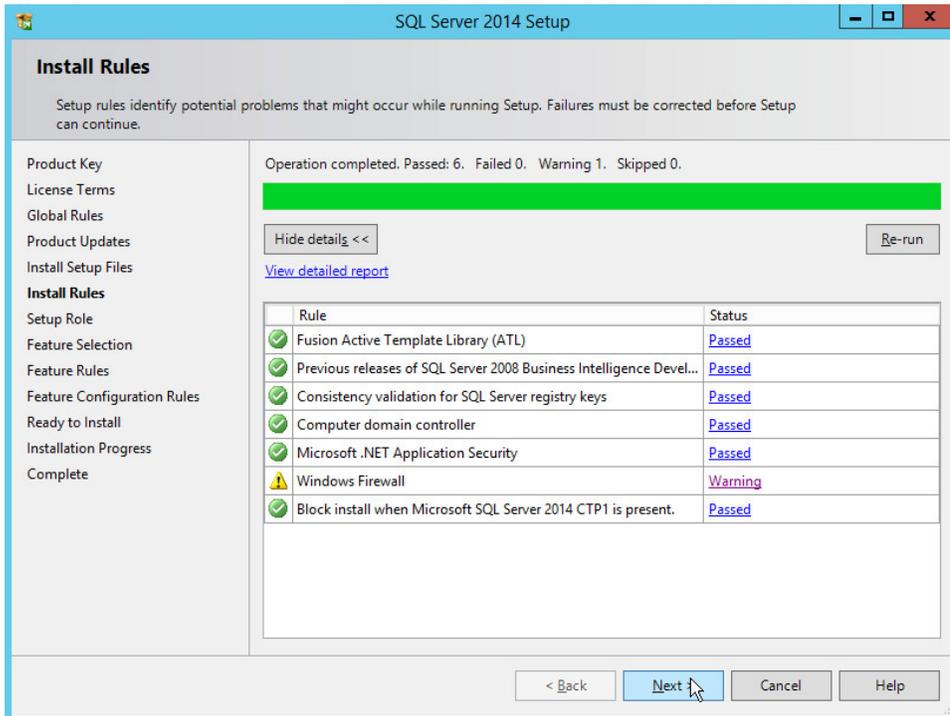


565

566

567

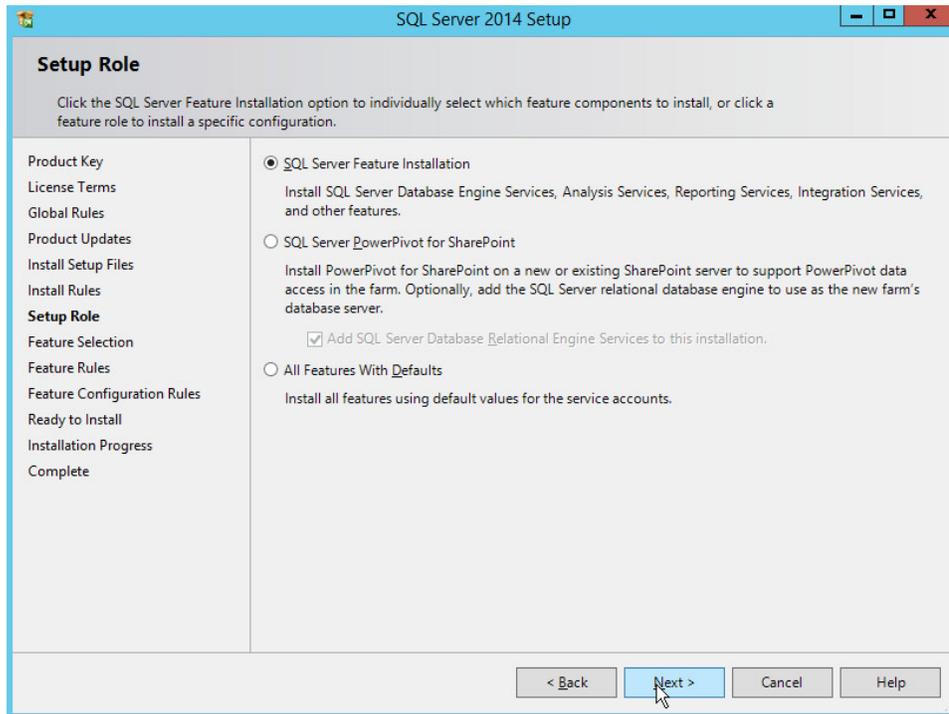
8. Click **Next**.
9. In the **Install Rules** section, note and resolve any further conflicts.



568

569 10. Click **Next**.

570 11. In the **Setup Role** section, select **SQL Server Feature Installation**.



571

572

12. Click **Next**.

573

13. In the **Feature Selection** section, select the following options:

574

a. **Database Engine Services**

575

b. **Client Tools Connectivity**

576

c. **Client Tools Backwards Compatibility**

577

d. **Client Tools SDK**

578

e. **Management Tools – Basic**

579

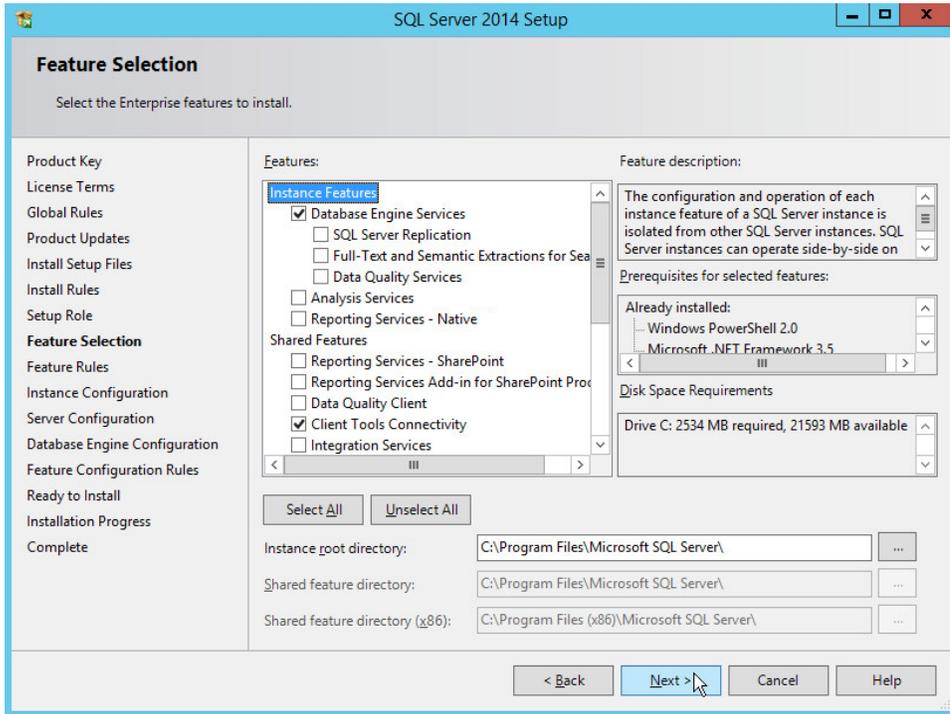
f. **Management Tools – Complete**

580

g. **SQL Client Connectivity SDK**

581

h. **Any other desired features**



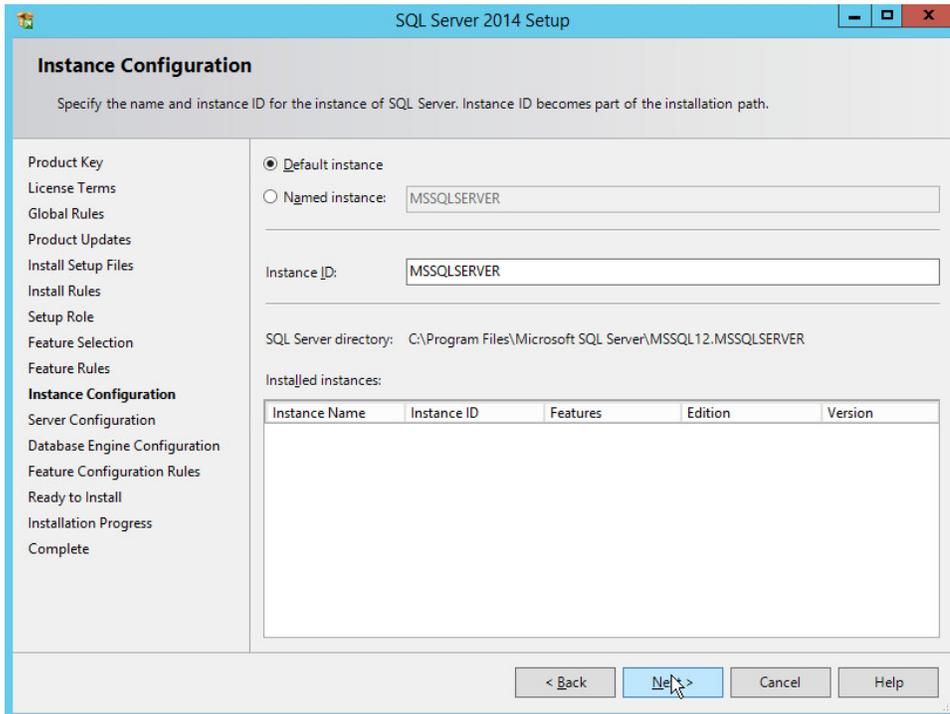
582

583

584

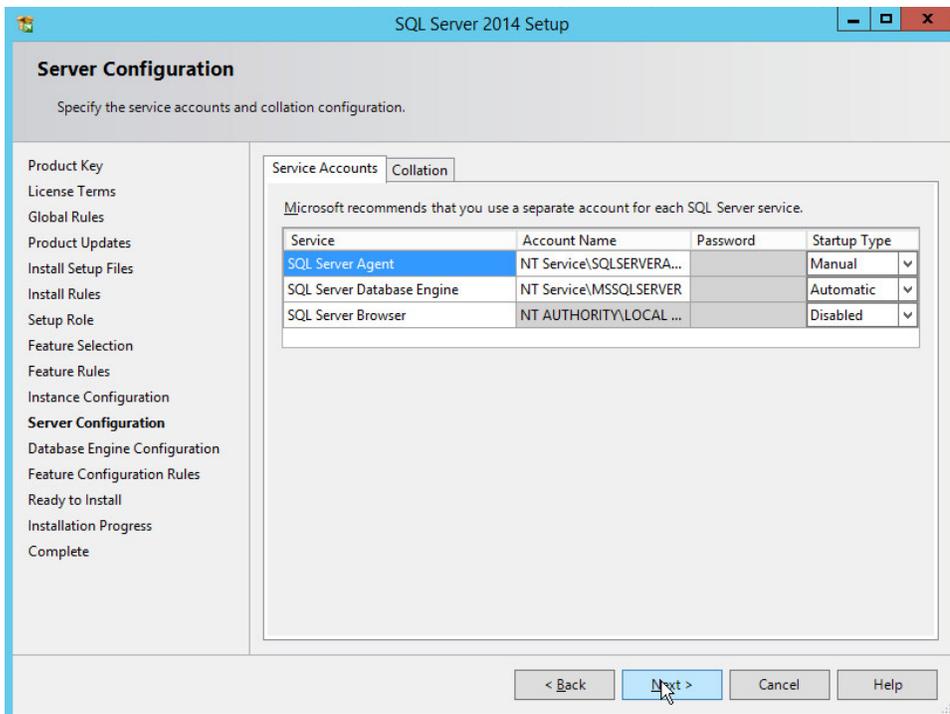
14. Click **Next**.

15. In the **Instance Configuration** section, select **Default instance**.



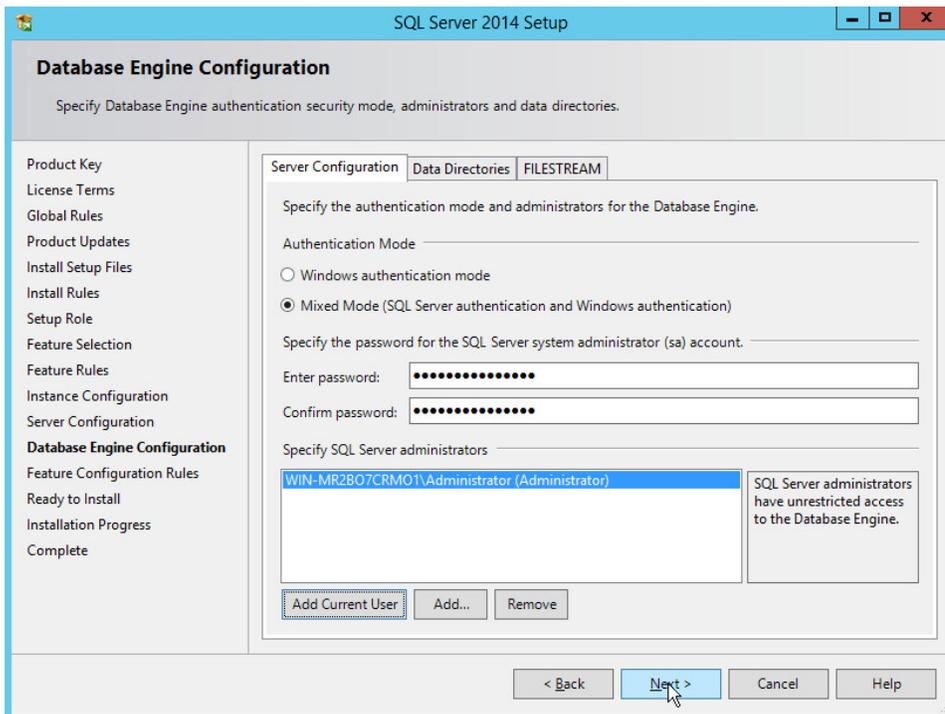
585

586 16. Click **Next**.



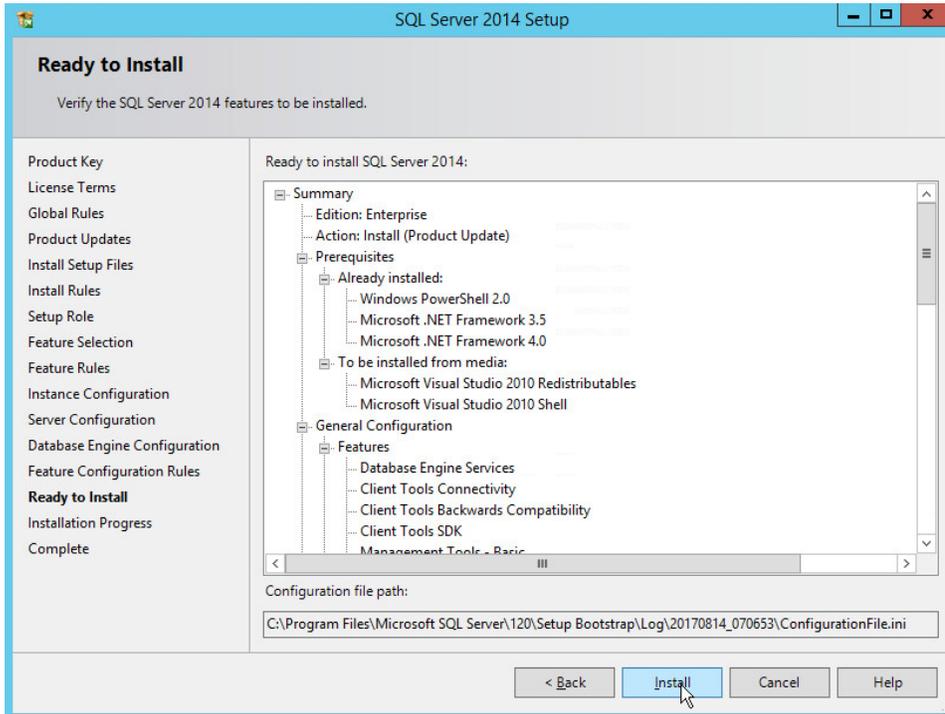
587

- 588 17. In the **Server Configuration** section, click **Next**.
- 589 18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.
- 590 19. Add all desired users as Administrators under **Specify SQL Server Administrators** by pressing
- 591 **Add Current User**.
- 592 a. For Domain accounts, simply type in **\$DOMAINNAME\USERNAME** into **Enter the**
- 593 **object names to select** text box.
- 594 b. Click **OK**.
- 595 c. For local computer accounts, click on **locations** and select the computer's name.
- 596 d. Click **OK**.
- 597 e. Type the username into the **Enter the object names to select** text box.
- 598 f. Once you are finished adding users, click **Next**.



599

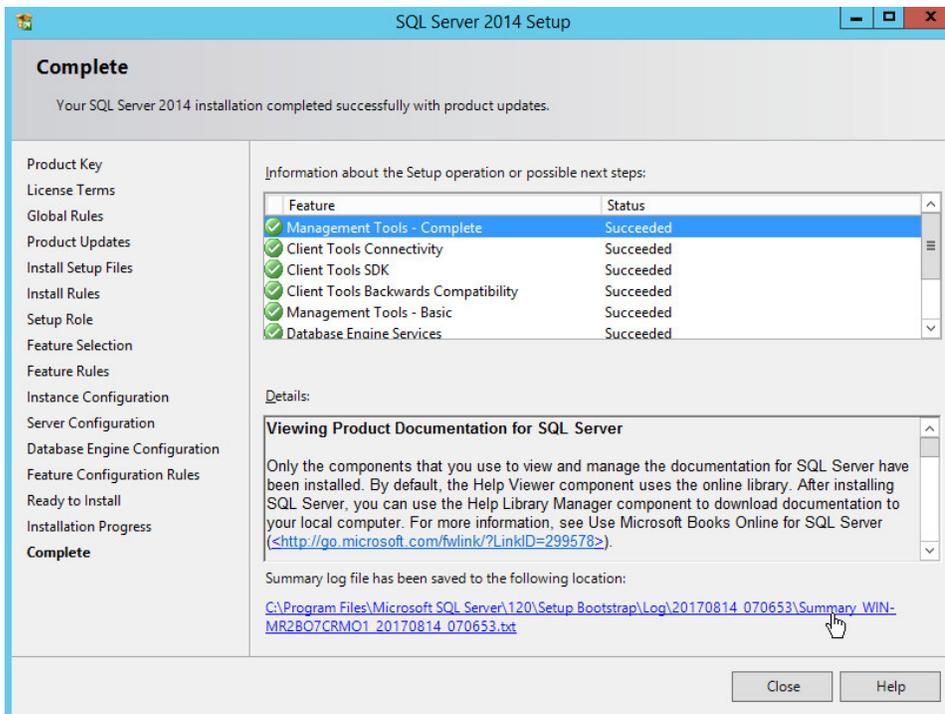
- 600 20. In the **Ready to install** section, verify the installation and click **Install**.



601

21. Wait for the installation to finish.

602



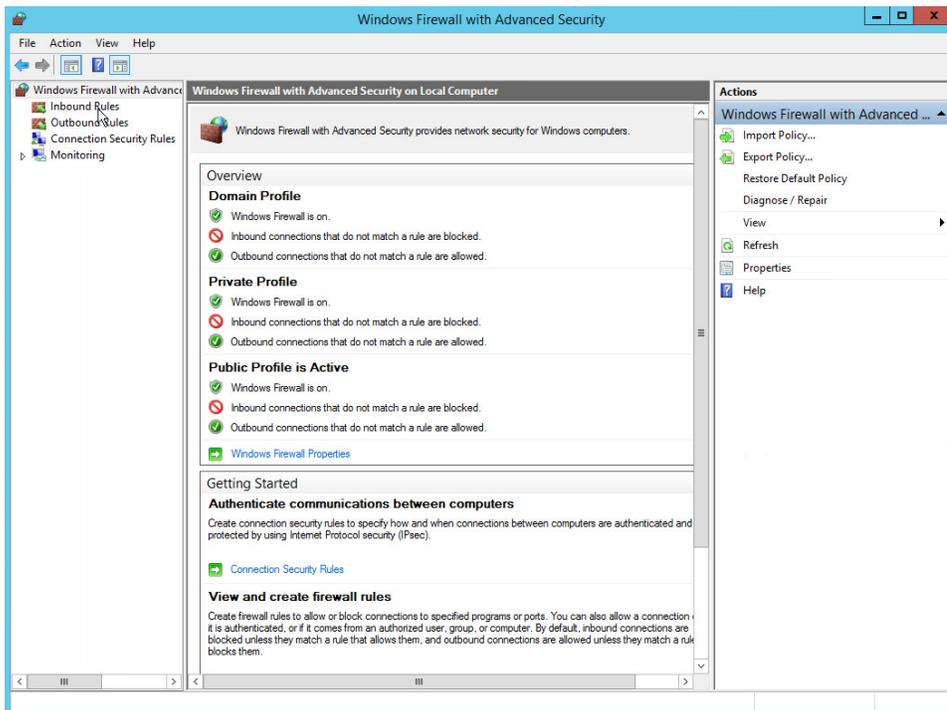
603

DRAFT

604 22. Click **Close**.

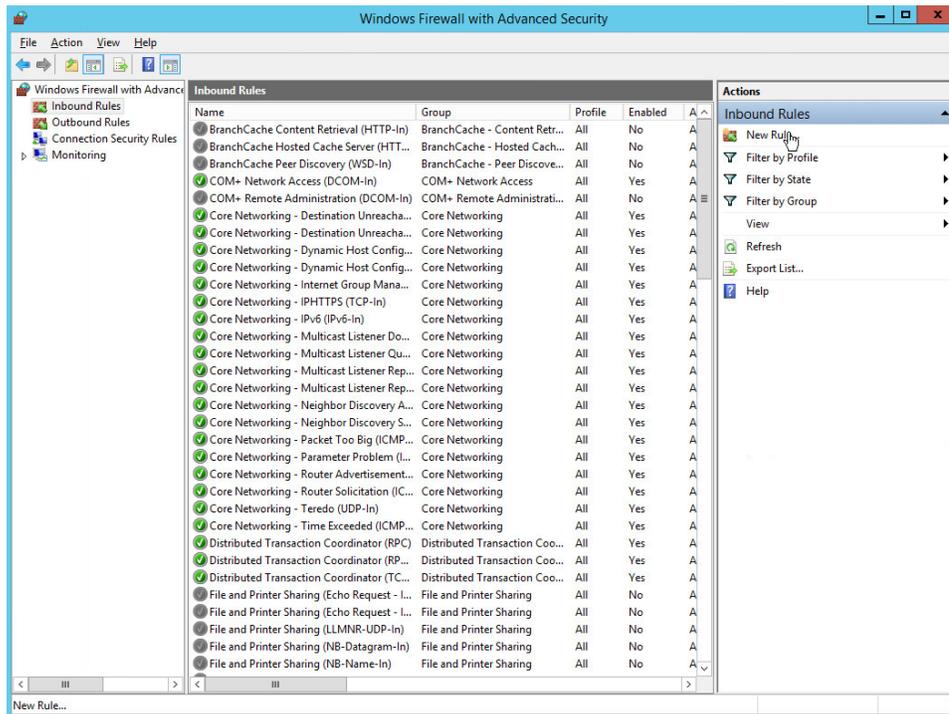
## 605 2.4.2 Open Port on Firewall

606 1. Open **Windows Firewall with Advanced Security**.



607  
608

2. Click **Inbound Rules**.



609

610

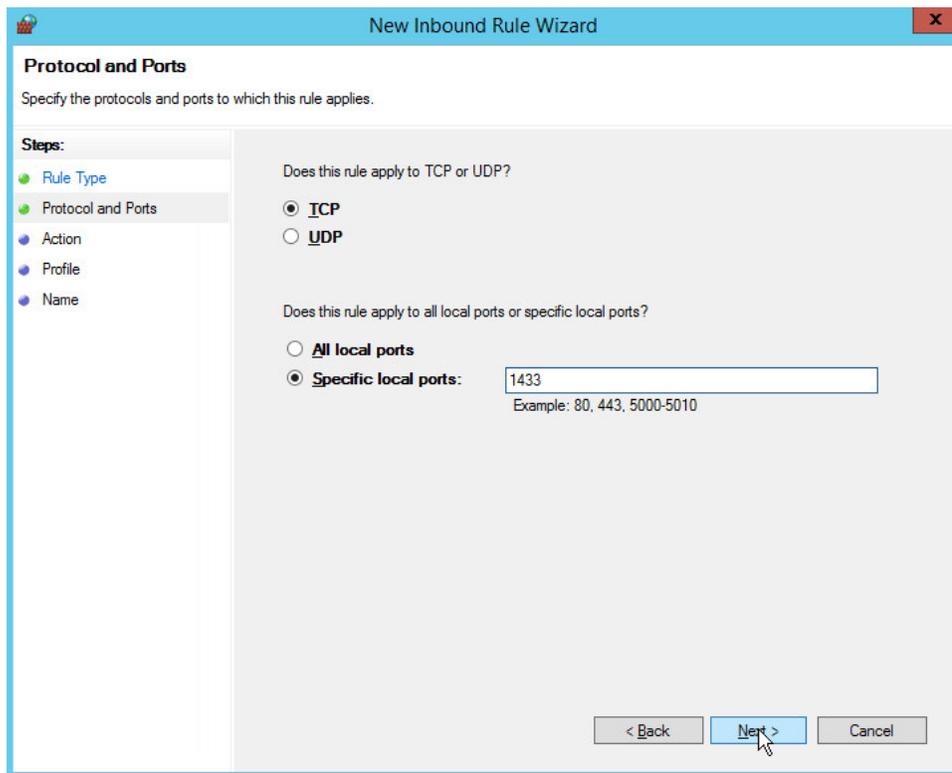
611

612

613

614

3. Click **New Rule**.
4. Select **Port**.
5. Click **Next**.
6. Select **TCP** and **Specific local ports**.
7. Type **1433** into the text field.

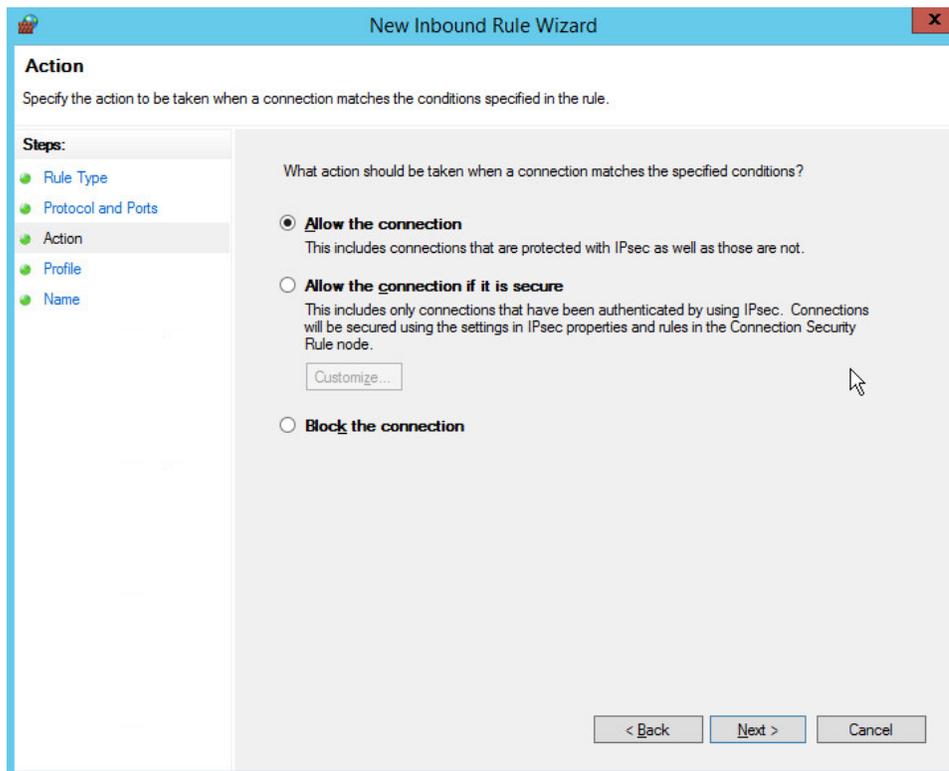


615

616

617

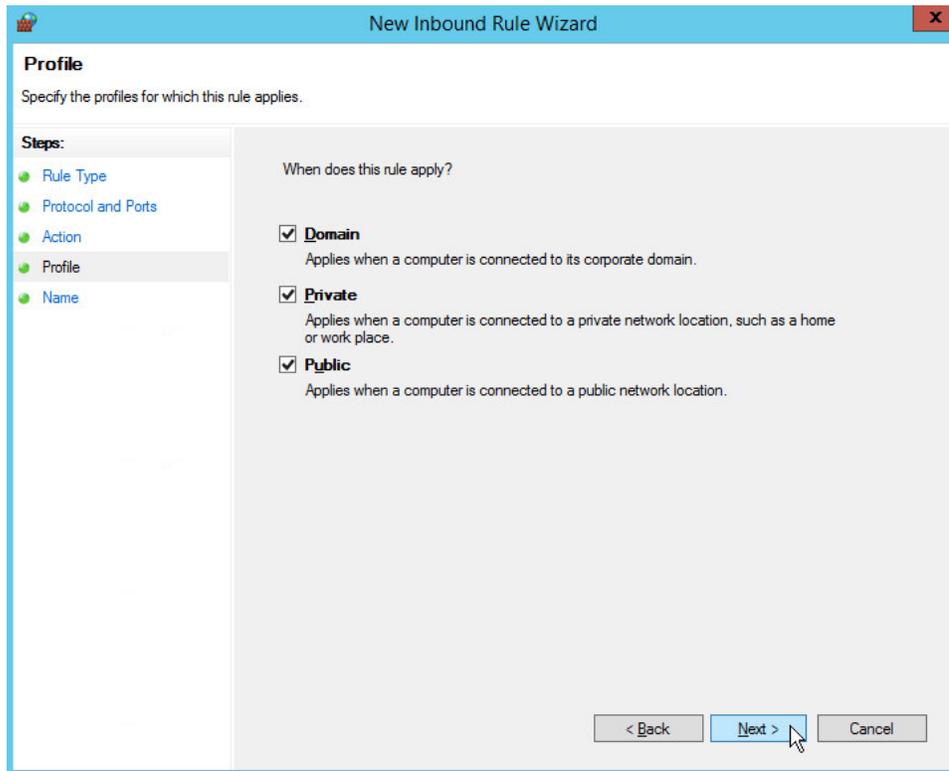
8. Click **Next**.
9. Select **Allow the connection**.



618

619 10. Click **Next**.

620 11. Select all applicable locations.



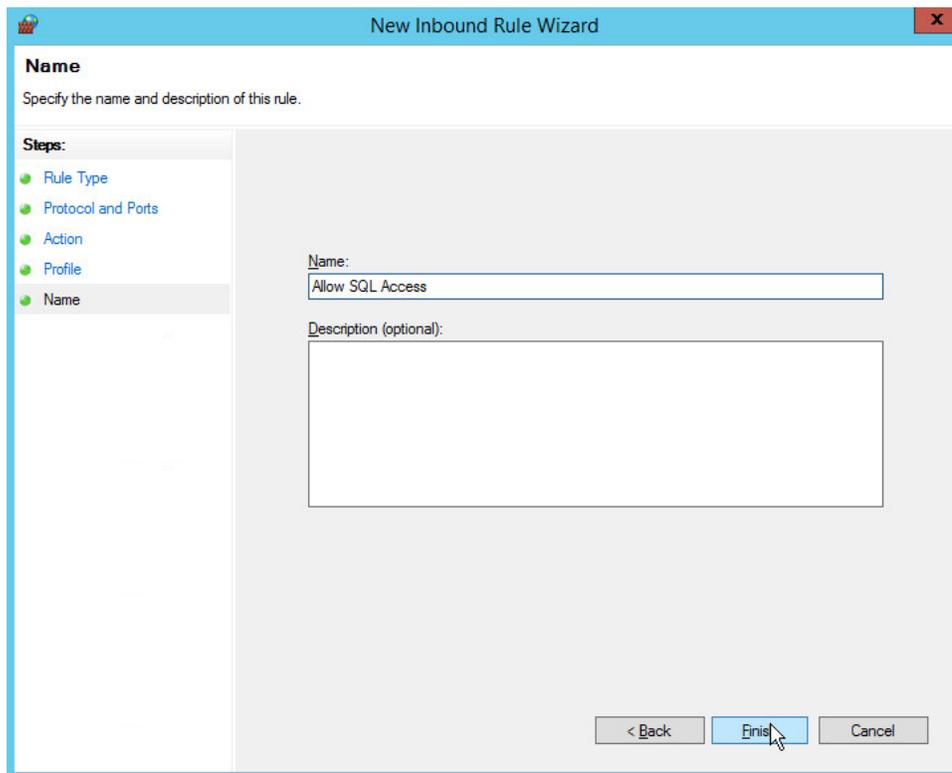
621

622

623

12. Click **Next**.

13. Name the rule **Allow SQL Access**.

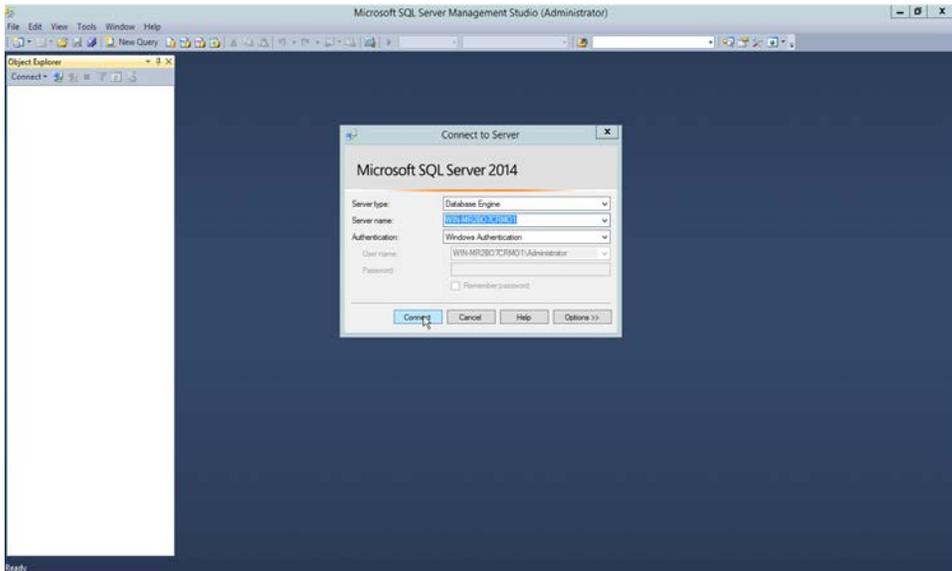


624

625 14. Click **Finish**.

### 626 2.4.3 Add a New Login to the Database

627 1. Open **SQL Server Management Studio**.

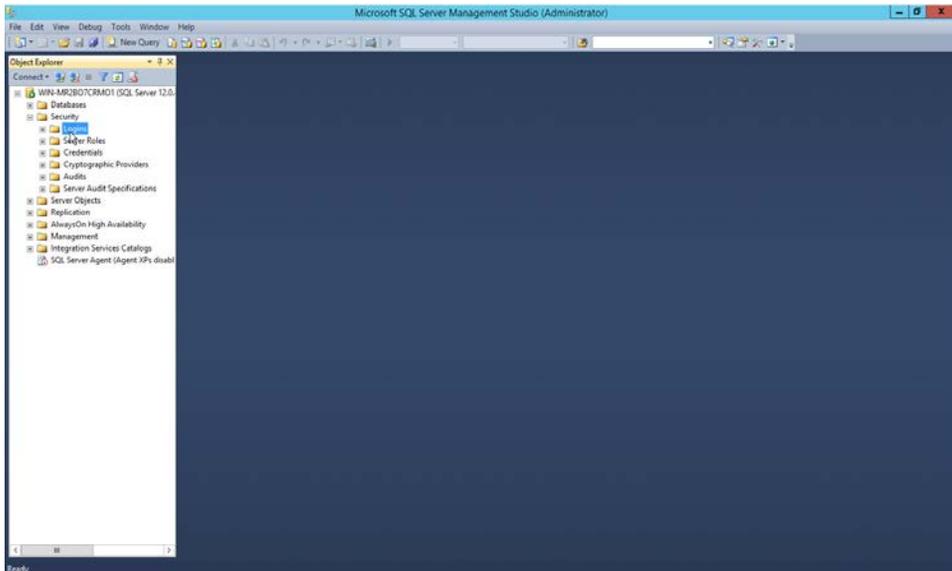


628

629

630

2. Click **Connect** to connect to the database.
3. In the **Object Explorer** window, expand the **Security** folder.

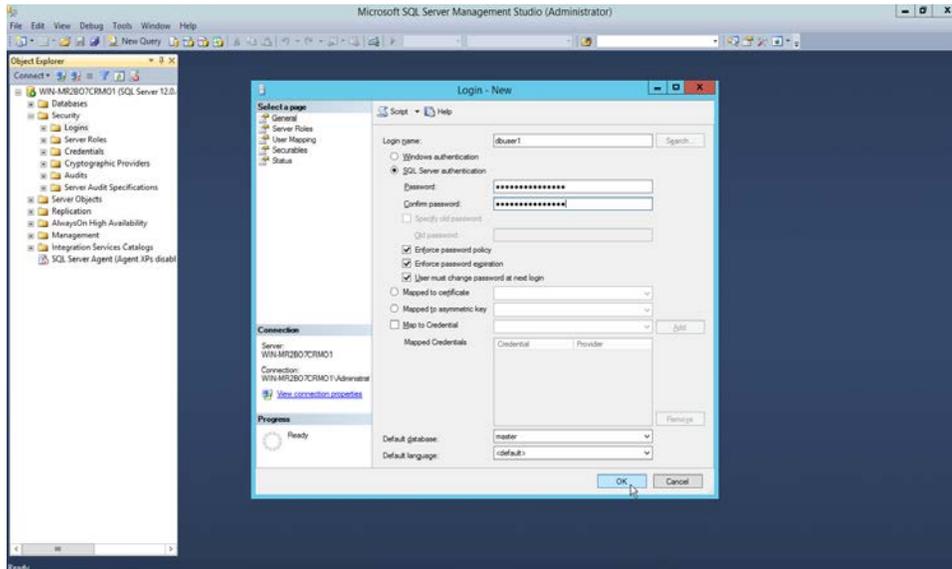


631

632

633

4. Right-click on the **Logins** folder and click **New Login....**
5. Input the desired user.



634

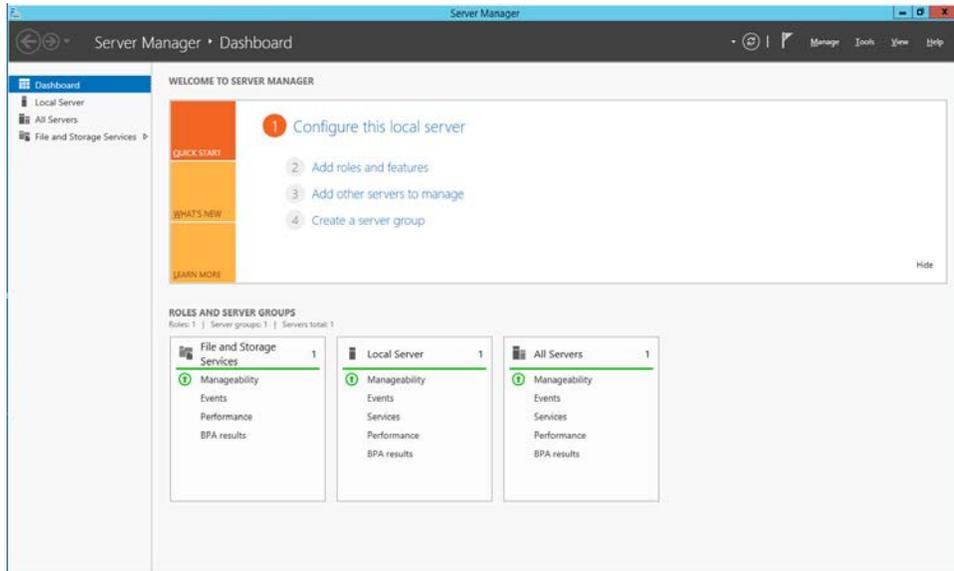
635 6. Click **OK**.

## 636 2.5 Microsoft IIS Server

637 As part of our enterprise emulation, we include a Microsoft IIS server. This section covers the  
 638 installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2  
 639 machine. This was conducted on the same machine as in Section 2.4.

### 640 2.5.1 Install IIS

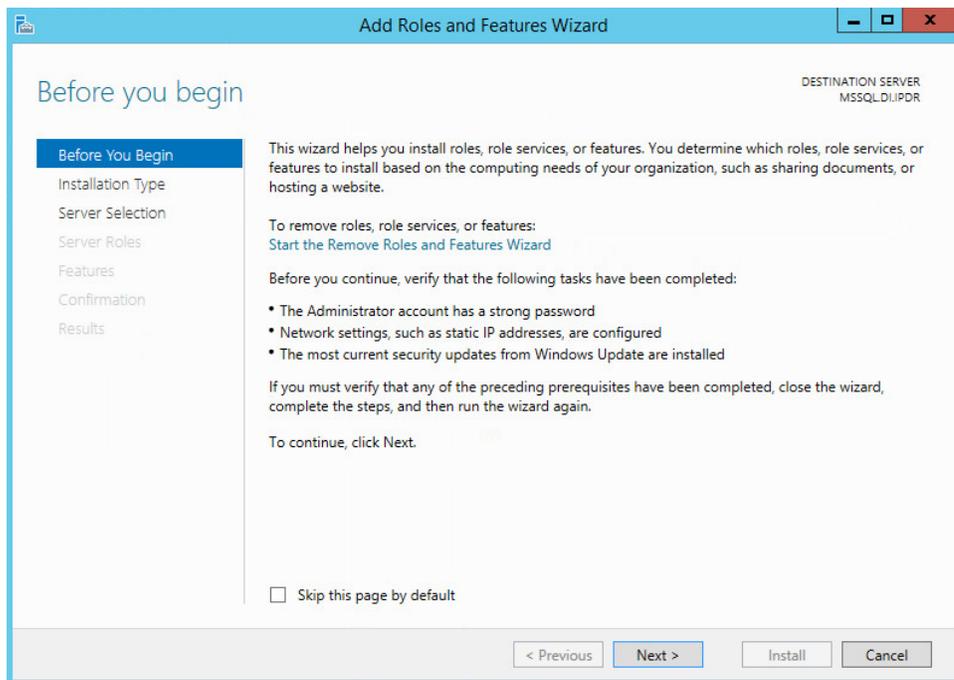
641 1. Open **Server Manager**.



642

643

2. Click **Add Roles and Features**.

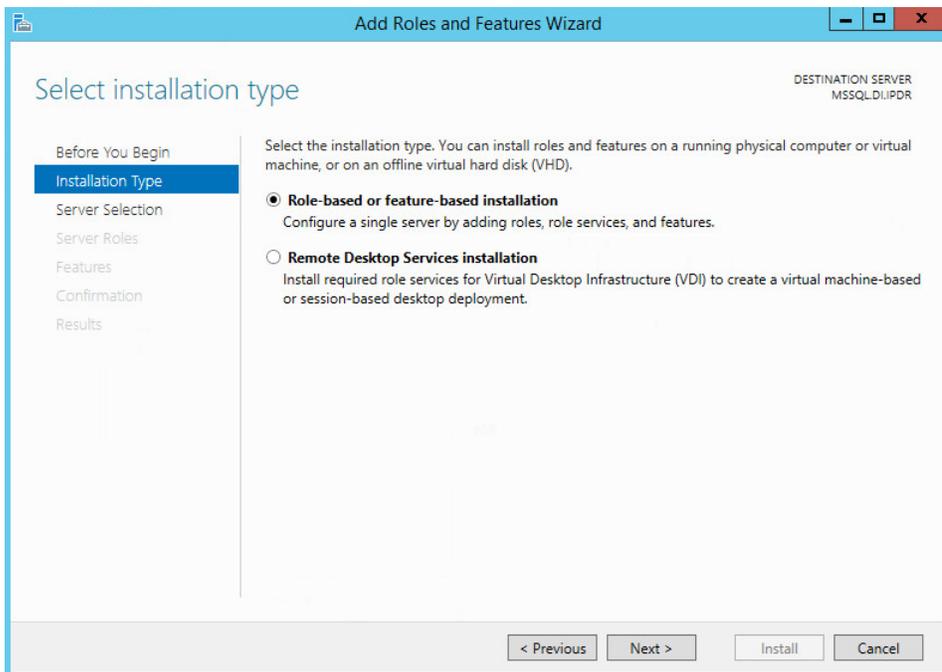


644

645

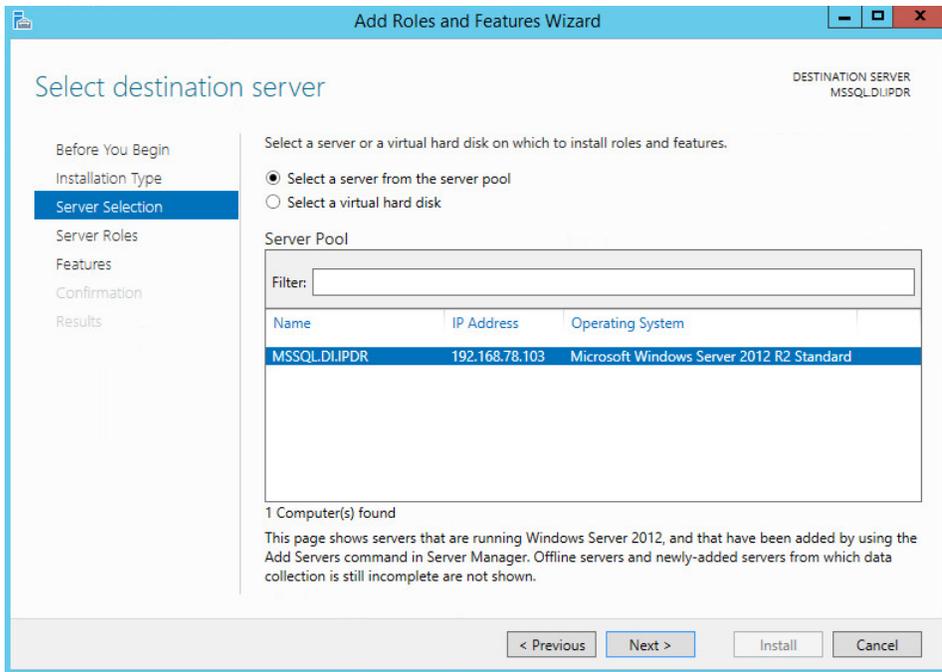
3. Click **Next**.

- 646 4. Select **Role-based or feature-based installation**.

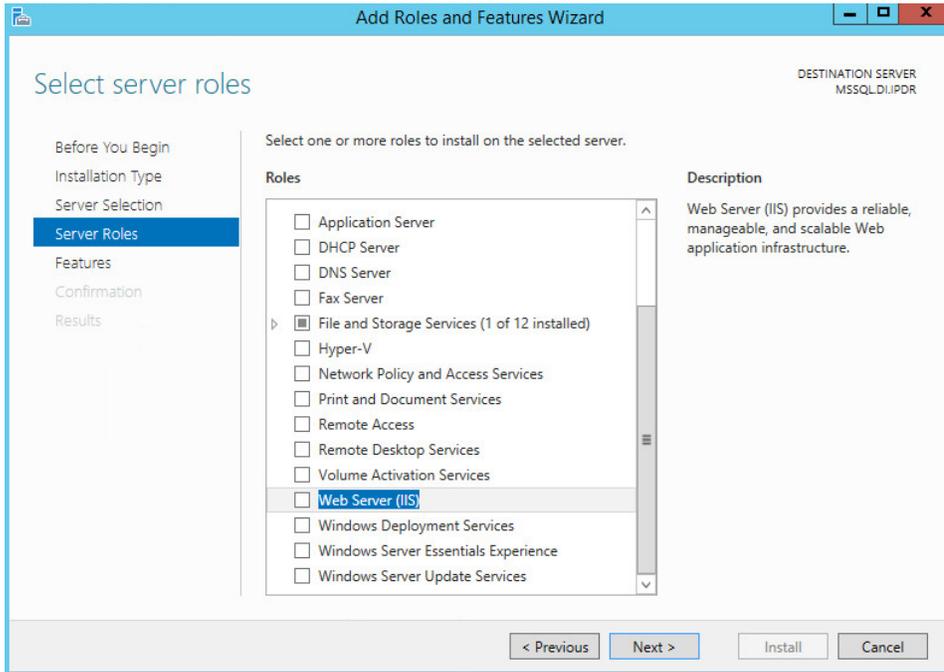


- 647 5. Click **Next**.

- 649 6. Select **MSSQL** (or the correct Windows Server name) from the list.

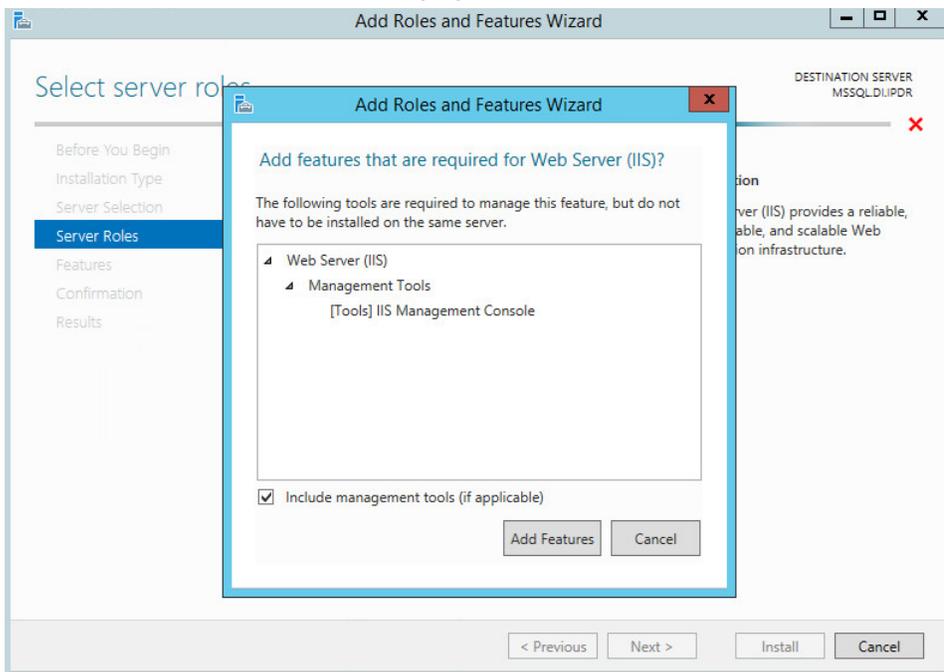


- 650 7. Click **Next**.



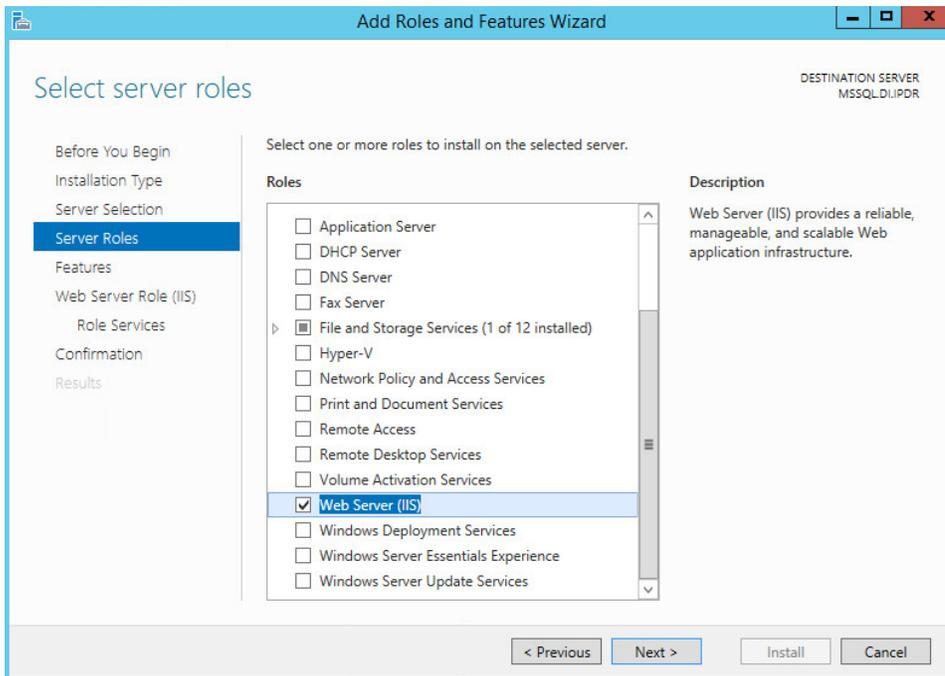
652

653 8. Check the box next to **Web Server (IIS)**.



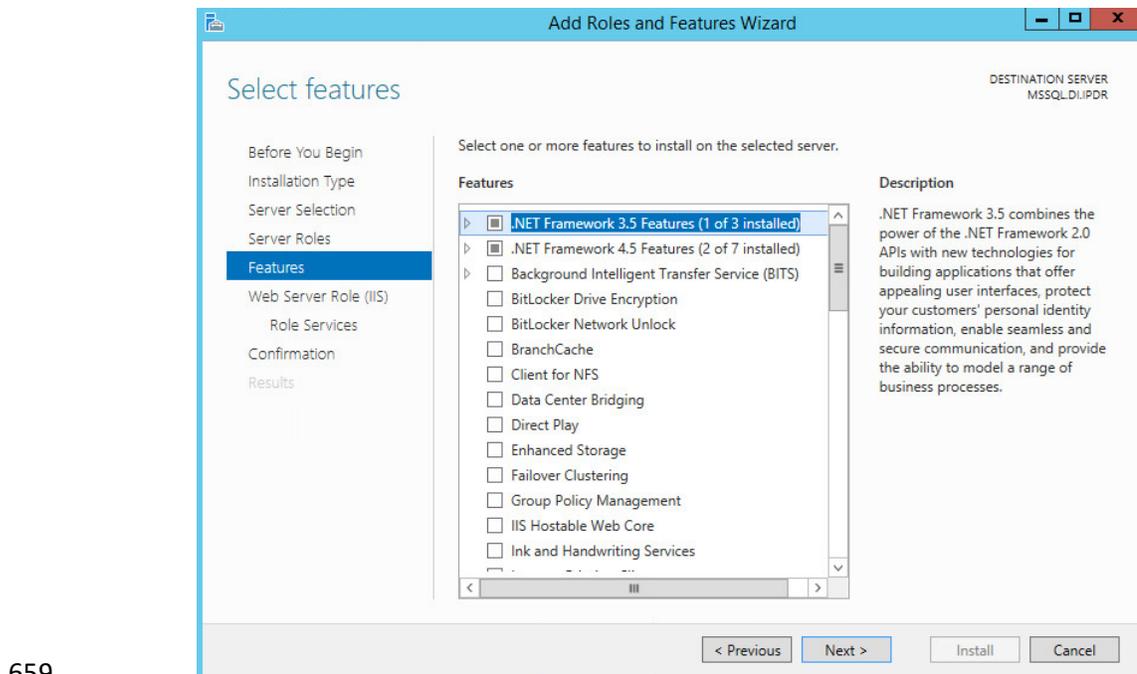
654

655 9. Click **Add Features**.



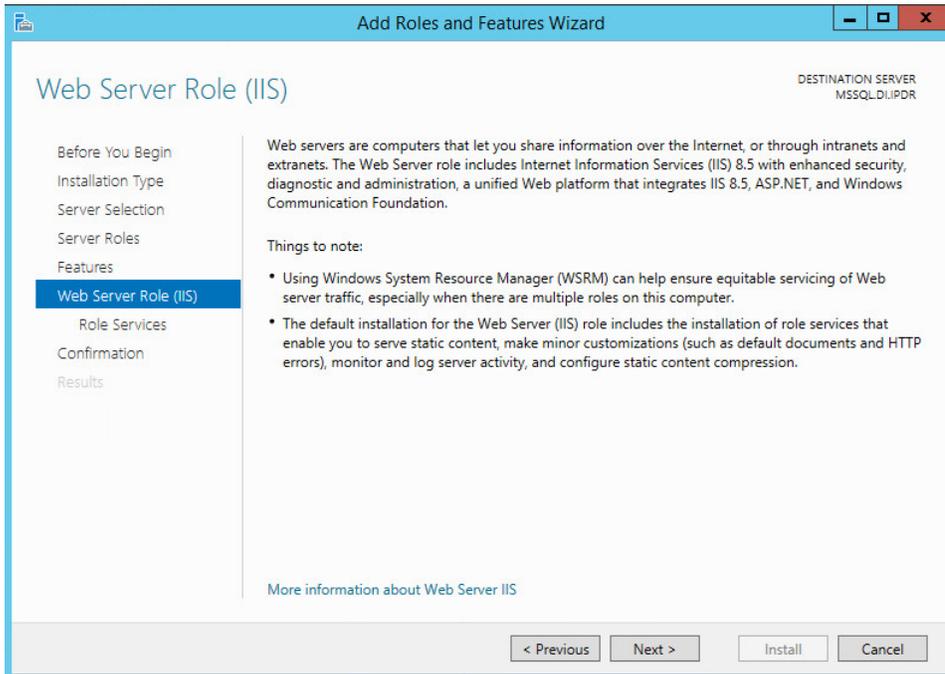
656 10. Click **Next**.

657 11. Ensure that all desired features are selected.



659 12. Click **Next**.

660



661

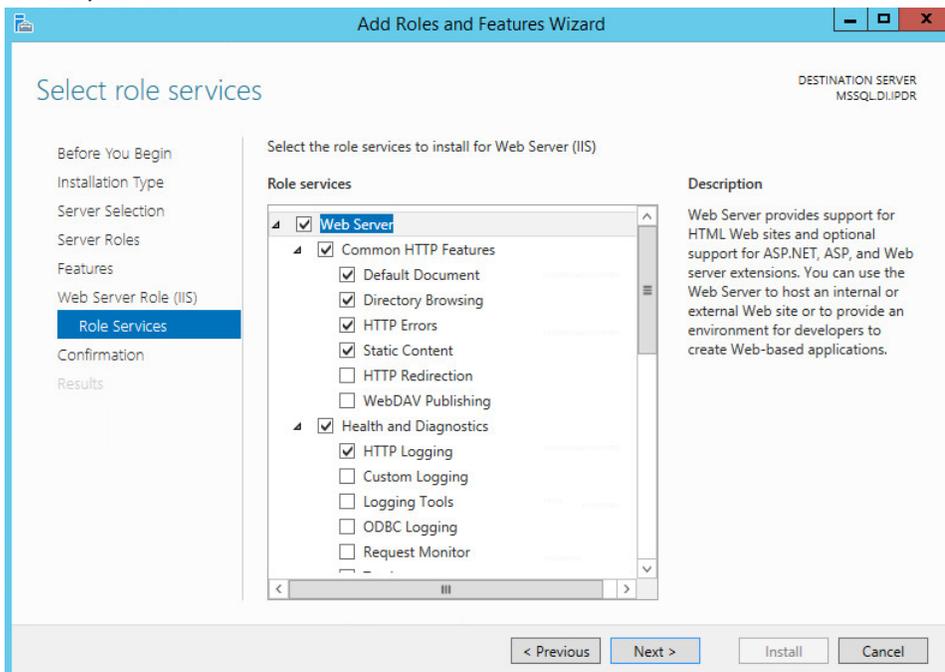
13. Click **Next**.

662

14. Ensure that **Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Logging,** and any other desired Role services are selected.

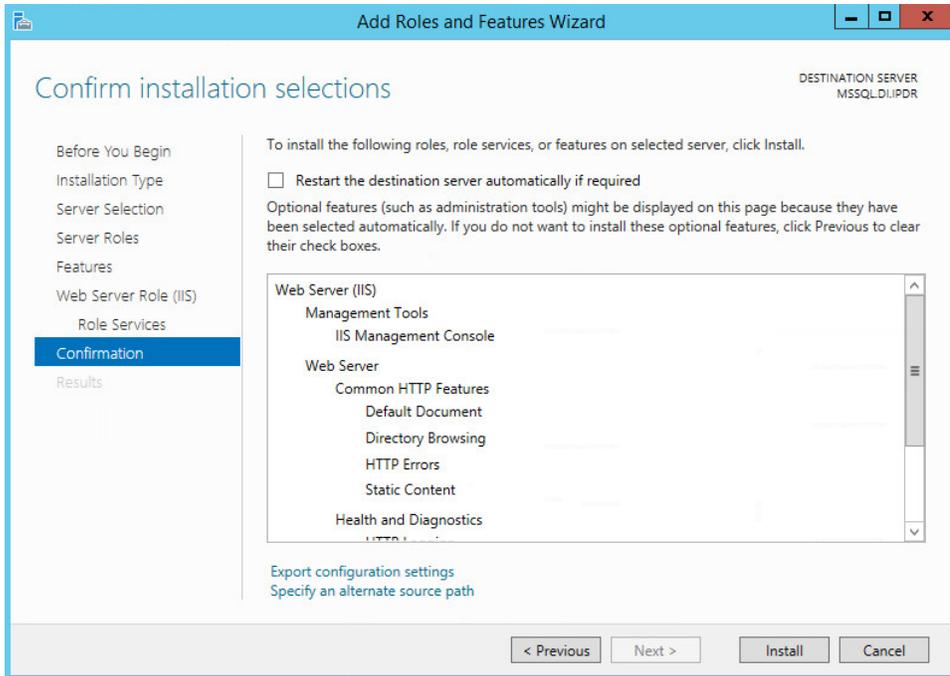
663

664



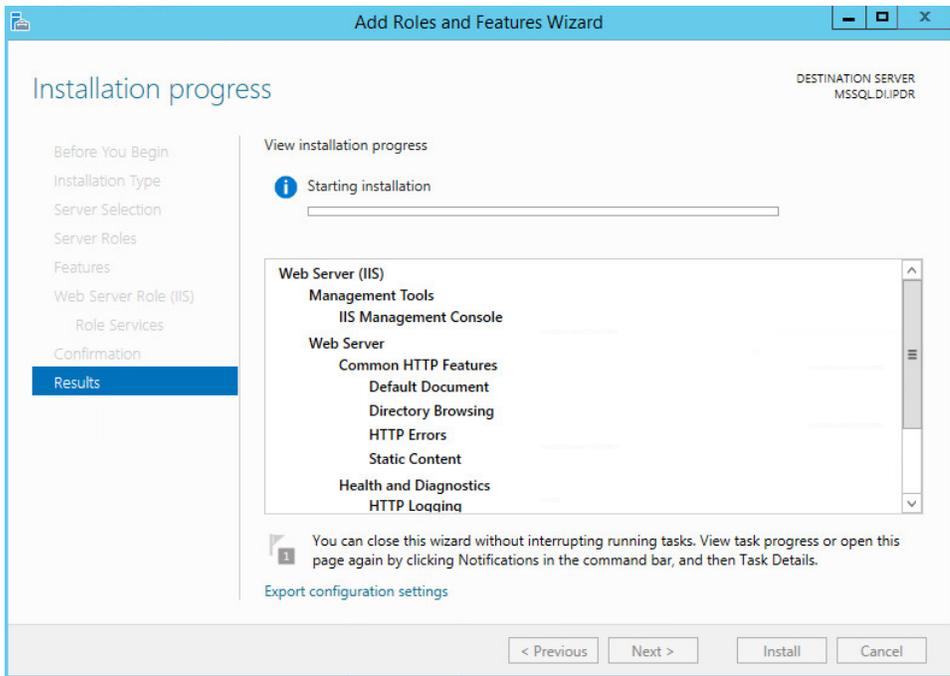
665

666 15. Click **Next**.



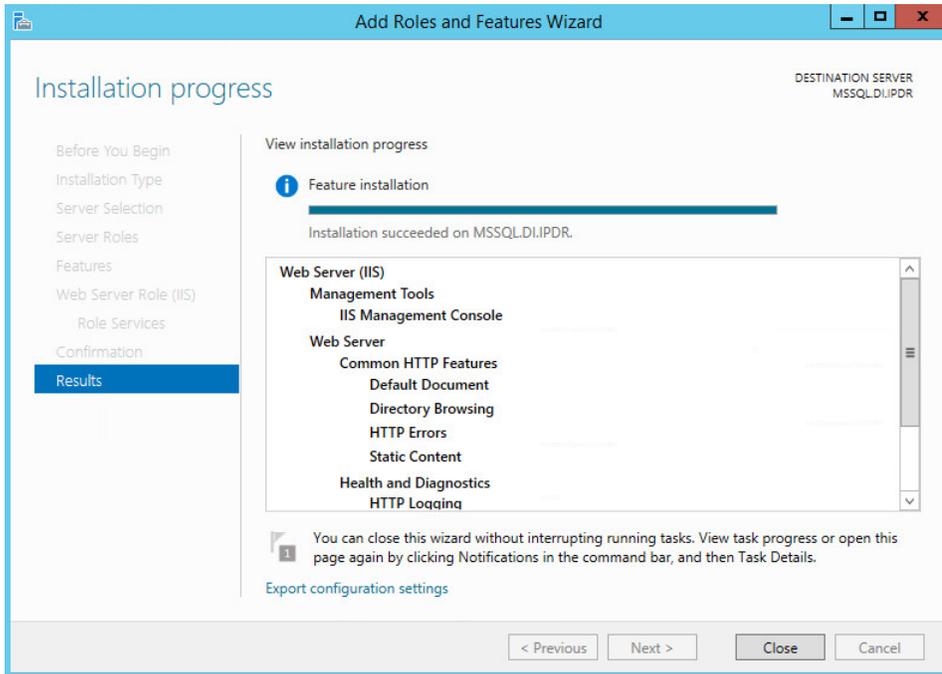
667

668 16. Click **Install**.



669

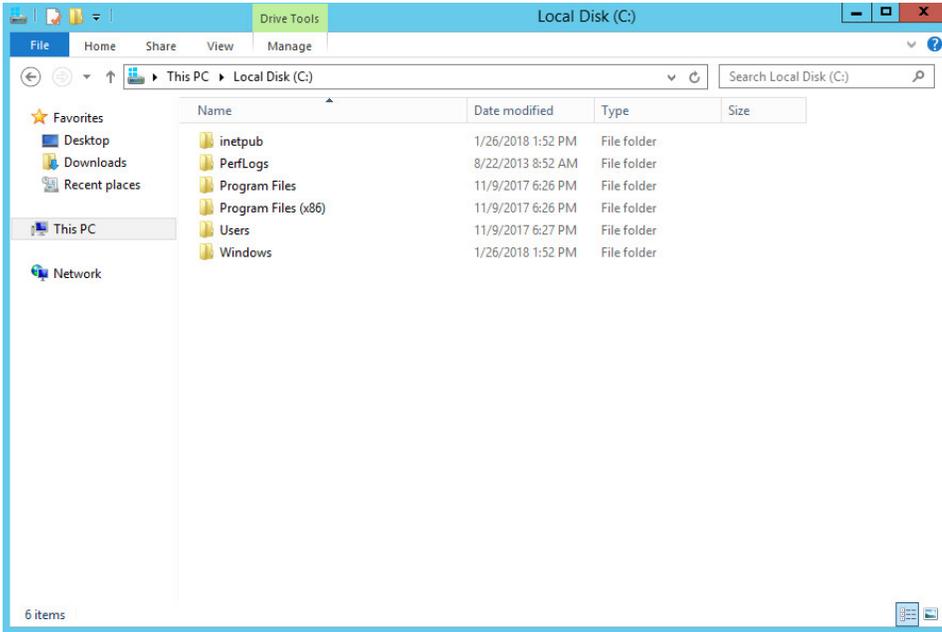
670 17. Wait for the installation to complete.



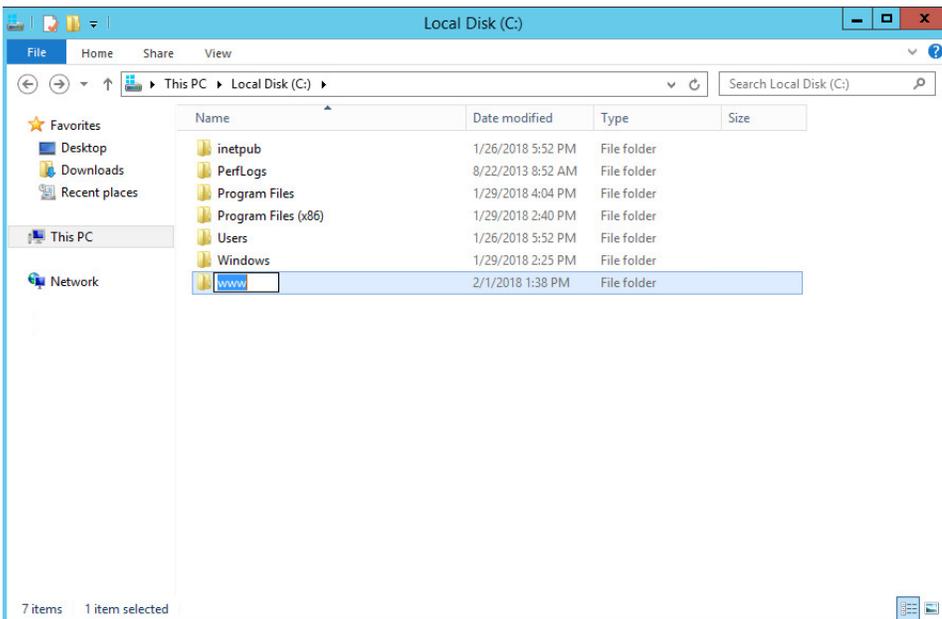
671 18. Click **Close**.  
672

673 2.5.2 IIS Configuration

- 674 1. Open Windows Explorer and click **This PC**.

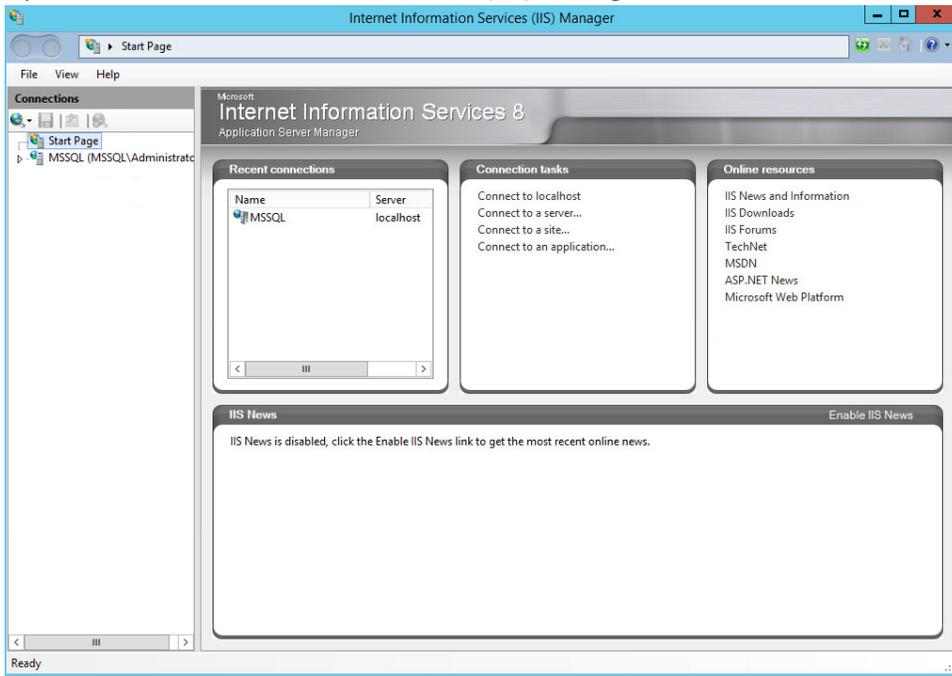


- 675 2. Right-click and select **Create Folder**.
- 676 3. Name the folder **www**.
- 677

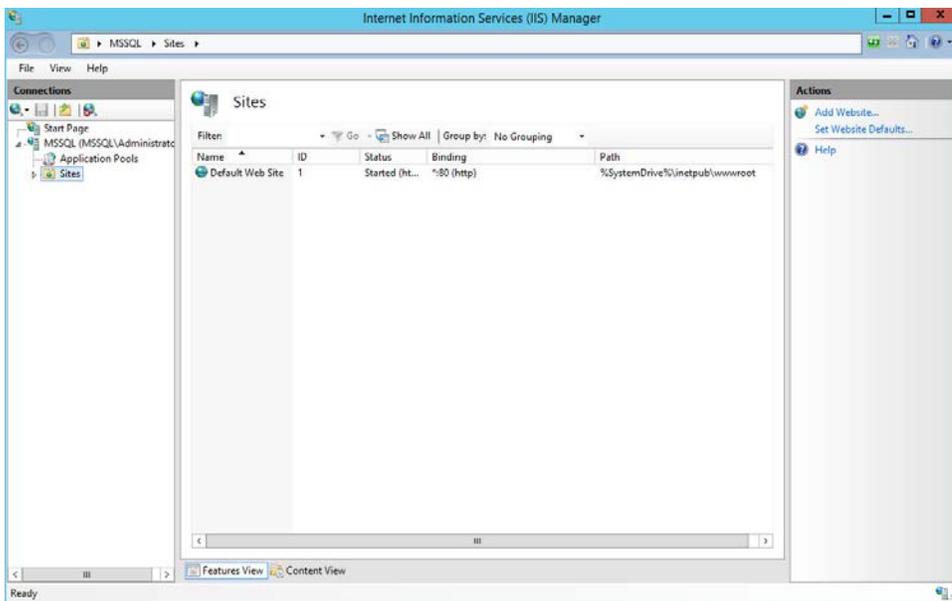


678

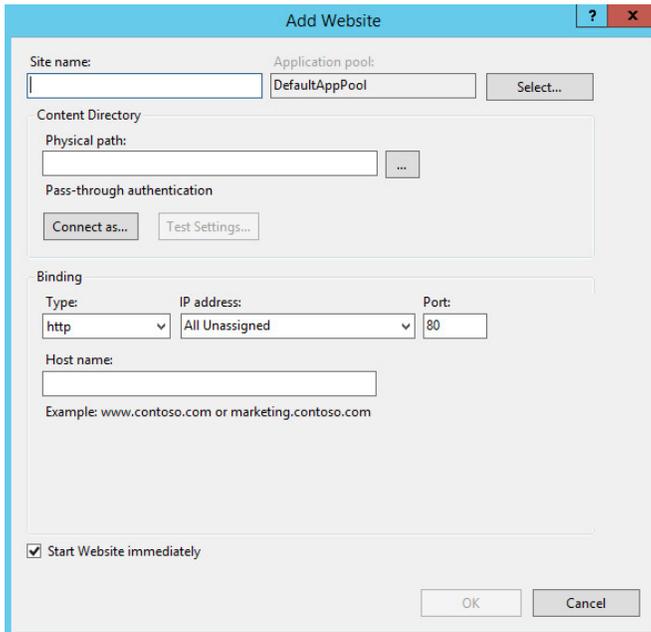
- 679 4. Open the **Internet Information Services (IIS) Manager**.



- 680  
681 5. Click the arrow next to **MSSQL** (or the chosen name of the server).  
682 6. Click **Sites**.

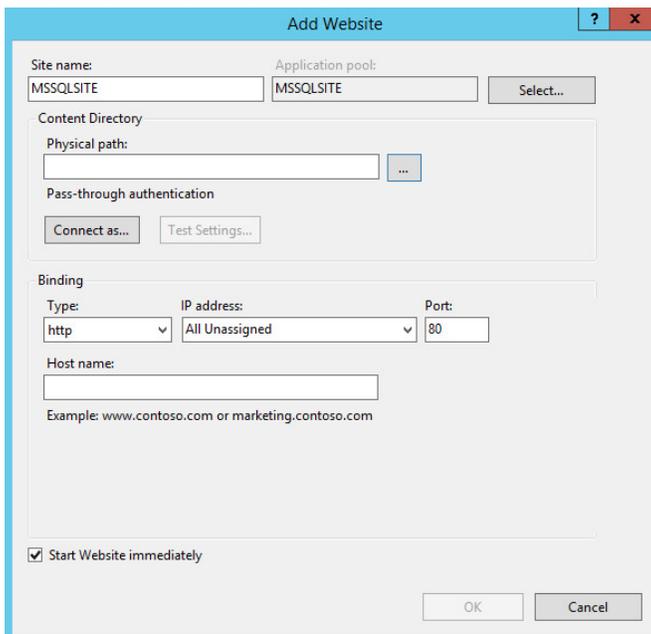


- 683  
684 7. Click **Add Website....**



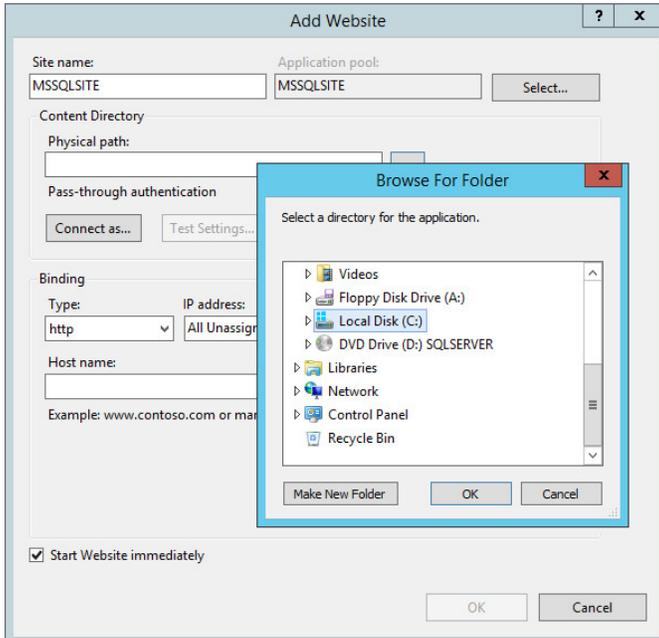
685  
686

8. Enter the desired site name.



687  
688

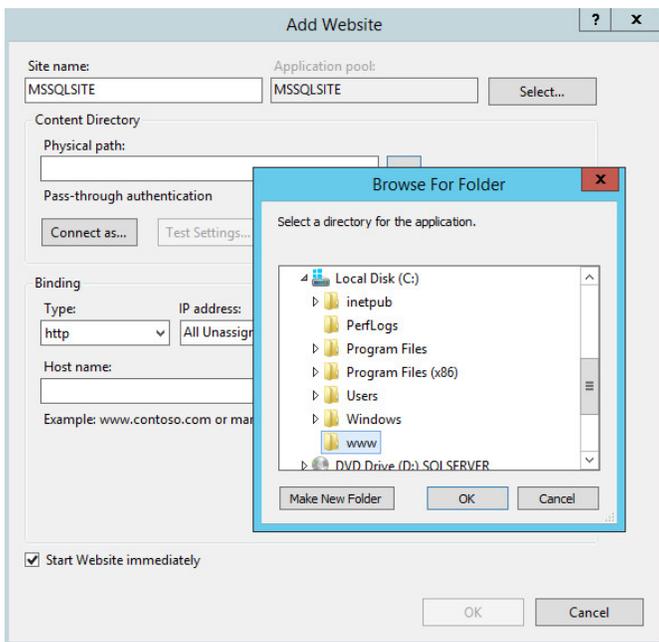
9. Click ... under **Physical path**.



689

690

10. Locate and select the folder created in step 3.



691

692

693

11. Click **OK**.

12. Set **Type** to **http** and **Port** to **80**.

- 694 13. Ensure that the **IP address** and **Host name** fields are filled in with the correct information for  
695 the machine.  
696 14. Ensure that **Start Website immediately** is selected.

The screenshot shows the 'Add Website' dialog box. The 'Site name' field is 'MSSQLSITE'. The 'Application pool' is 'MSSQLSITE'. The 'Physical path' is 'C:\www'. The 'IP address' is '192.168.81.107'. The 'Port' is '80'. The 'Host name' is 'MSSQL.di.ipdr'. The 'Start Website immediately' checkbox is checked.

- 697  
698 15. Click **OK**.  
699

## 700 2.6 GreenTec WORMdisks

701 See the *Installation of GreenTec Command Line Utilities* document, which should accompany the  
702 installation disk, for a detailed guide on how to install the GreenTec command line utilities.  
703 Furthermore, refer to the *GT\_WinStatus User Guide*, which should also accompany the installation disk,  
704 for instructions on how to effectively use GreenTec WORMdisks to preserve data. Read these  
705 instructions *carefully*, as locking GreenTec WORMdisks can result in making some or all of the disk or  
706 the entire disk unusable. Having portions of the disk or the entire disk permanently locked is sometimes  
707 desirable, but it is dependent on the needs of your organization, e.g., if you want to store backup  
708 information or logs securely.

709 The *GT\_WinStatus User Guide* provides instructions for locking and temporarily locking disk sectors. In  
710 this practice guide, we will not include instructions on when to lock GreenTec WORMdisks. However, we  
711 will provide instructions detailing how to save data to these disks and various commands used in

712 manipulating the disks. Below, find descriptions of some commands useful for automation of GreenTec  
713 WORMdisks. Actual automation of these disks will vary per organization.

### 714 2.6.1 Format GreenTec WORMdisks

715 To format GreenTec WORMdisks for use, the following command can be used.

716 > **gt\_format.exe <disk number> /parts:<number of parts> /label:<id>**

717 This command can be used to split a disk into a specified number of partitions, with each partition being  
718 labeled according to the label id specified.

719 For example, this command will split drive 1 into four parts, labeled DI001, DI002, DI003, and DI004:

720 > **gt\_format.exe 1 /parts:4 /label:DI**

721 Formatting drive 1 partition 1 file system NTFS label "DI001"

722 Format successful

723 Formatting drive 1 partition 2 file system NTFS label "DI002"

724 Format successful

725 Formatting drive 1 partition 3 file system NTFS label "DI003"

726 Format successful

727 Formatting drive 1 partition 4 file system NTFS label "DI004"

728 Format successful

### 729 2.6.2 Obtain Status Information About GreenTec WORMdisks

730 To verify information about GreenTec WORMdisks, use the following command.

731 > **wvlist.exe <drive number>**

732 This command can be used to display basic information about a drive, such as the amount of space of  
733 each partition, whether it is a WORMdisk, whether they have been locked, and what drive letter to  
734 which they are mapped.

735 For example, this command will list the characteristics of drive 1.

```

736 > wvlist.exe 1
737 WVLIST: List WORM Volume (WDV) Status on Physical WORMdisks(tm).
738 Copyright (C) 2015 GreenTec-USA, Inc. All rights reserved.
739 Drive#=1 Type=ATA F/W=GT5G Size=500{GB}
740 > IS WORM > IS *NOT* Finalized
741 **** WORMdisk Volume (WDV) Info ****
742 WDV # TB ENFORCED GREENTEC TLOCKED
743 <----> <----> <-----> <-----> <----->
744 001 0.125 NO YES NO G:\
745 002 0.125 NO YES NO H:\
746 003 0.125 NO YES NO I:\
747 004 0.125 NO YES NO J:\

```

### 748 2.6.3 Map GreenTec WORMdisks to Drive Letters

- 749 1. To unmap a partition from a drive letter, use the following command:
 

```
750 > wvmap.exe <drive letter>:
```

751 For example,

```
752 > wvmap.exe H:
```

753 will unmap *H:*, making it available for mapping to another partition.
- 754 2. To map a partition to a drive letter, use the following command:
 

```
755 > wvmap.exe <drive letter>: <drive number>.<partition number>
```

756 For example,

```
757 > wvmap.exe H: 1.2
```

758 will map the second partition of drive 1 to *H:*, making files available through accessing that drive  
759 letter.
- 760 3. To map the next partition to a drive letter, use the following command:
 

```
761 > wvnext.exe <drive letter>:
```

762 For example, if *H:* is mapped to partition 2 of drive 1 (1.2)

763 > `wvnext.exe H:`

764 will attempt to map *H:* to partition 3 of drive 1 (1.3).

## 765 2.6.4 Activate Write Protection in GreenTec WORMdisks

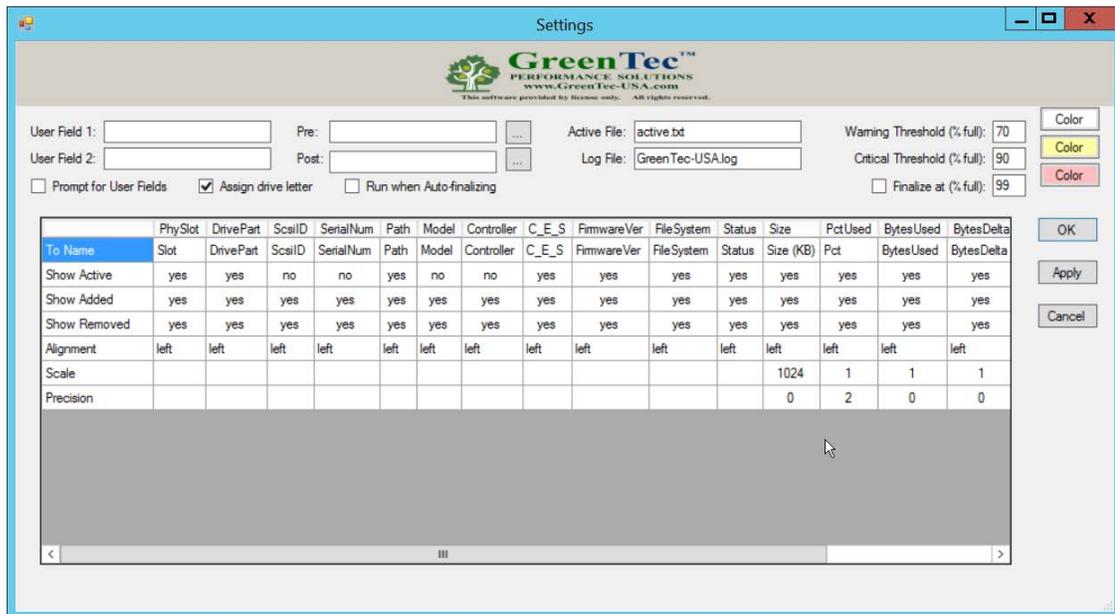
- 766 1. Running `GT_WinStatus.exe` will open the Graphical User Interface (GUI), which displays various  
767 information such as drive mappings, partitions, total space, and space used, as well as a range  
768 of other options.

The screenshot shows the GT\_WinStatus application window. At the top, there is a logo for 'WORM v151228' and a 'Period' dropdown menu set to '5'. There are 'Apply' and 'Refresh' buttons. The top right corner displays the date and time '6/28/2018 7:10:35 PM' and the status '7 Active, 0 Added, 0 Removed'. Below this is a tabbed interface with 'Active', 'Added', and 'Removed' tabs. The 'Active' tab is selected, showing a table with the following columns: Slot, DrivePart, Path, C\_E\_S, FirmwareVer, FileSystem, Status, Size (KB), Pct, BytesUsed, and BytesDelta. The table contains 10 rows of data.

Slot	DrivePart	Path	C_E_S	FirmwareVer	FileSystem	Status	Size (KB)	Pct	BytesUsed	BytesDelta
0/1	E:\	?		GT5G w2	NTFS	WORM (RW)	255,999,996	0.05	130,437,120	0
0/2		?		GT5G w2	NTFS	WORM (RO)	102,399,996	0.09	93,130,752	0
0/3	F:\	?		GT5G w2	NTFS	WORM (RW)	129,853,436	0.09	117,055,488	0
0	1/1	G:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0
0	1/2	H:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0
0	1/3	I:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0
0	1/4	J:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,065,736	0.09	116,776,960	0

769

- 770 2. More columns can be added by right-clicking anywhere in the **Active** window, opening the  
771 **Settings** window.



772

773

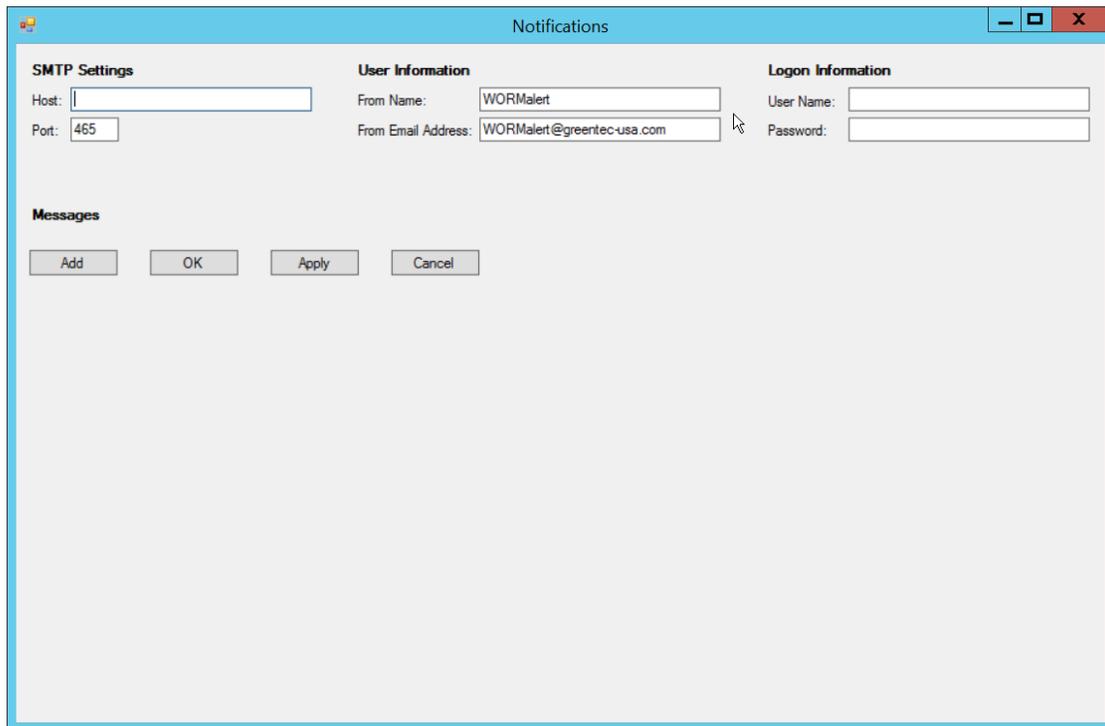
774

775

776

777

3. In the Settings window, **User Field 1** and **User Field 2** are for any metadata to be stored for a drive. **Pre:** runs a script prior to finalizing a drive, and **Post:** runs a script after finalizing a drive.
4. Also, from the **Settings** window, right-clicking on **Critical Threshold** or **Warning Threshold** will allow the user to set up alert preferences for drives that are nearly full (at a configurable percent value).



778

779 5. To display the GUI with options to lock and enforce locks on drives, the following command  
780 must be used to start the GUI:

781 > **GT\_WinStatus.exe /tlock /enf**

- 782 6. This will add columns called **TLock** and **Enforce** (as well as the ability to use the **Finalize**  
783 column).

The screenshot shows the GT\_WinStatus application window. The title bar reads "GT\_WinStatus". The interface includes a logo for "WORM v151228", a "Period" dropdown set to "3", and "Apply" and "Refresh" buttons. The top right corner displays the date and time "6/28/2018 7:30:18 PM" and the status "7 Active, 0 Added, 0 Removed". Below the header, there are tabs for "Active", "Added", and "Removed". The main content is a table with the following data:

Slot	DrivePart	Path	C_E_S	FirmwareVer	FileSystem	Status	Size (KB)	Pct	BytesUsed	BytesDelta	TLock	Enforce	Finalize
0/1	E:\	?		GT5G w2	NTFS	WORM (RW)	255,999,996	0.05	130,437,120	0	TLOCK	ENFORCE	FINALIZE
0/2		?		GT5G w2	NTFS	WORM (RO)	102,399,996	0.09	93,130,752	0	UNTLOCK	ENFORCE	FINALIZE
0/3	F:\	?		GT5G w2	NTFS	WORM (RW)	129,853,436	0.09	117,055,488	0	TLOCK	ENFORCE	FINALIZE
0	1/1	G:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0	TLOCK	ENFORCE	FINALIZE
0	1/2	H:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0	TLOCK	ENFORCE	FINALIZE
0	1/3	I:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,063,240	0.09	116,776,960	0	TLOCK	ENFORCE	FINALIZE
0	1/4	J:\	0/1/1	GT5G w2	NTFS	WORM (RW)	122,065,736	0.09	116,776,960	0	TLOCK	ENFORCE	FINALIZE

- 784  
785 7. The **TLock** column temporarily locks/unlocks a partition of the drive. This is useful to prevent  
786 modification during times when modification should be disallowed.

**Important: The following functions in steps 8 and 9 will permanently lock portions of the drive, making them read-only.**

**The Enforce function permanently locks all volumes up to the enforced volume.**

**The Finalize function permanently locks the entire drive.**

- 787  
788 8. The **Enforce** column is a *permanent incremental lock*. This means that it permanently prevents  
789 modification for the selected volume of a drive as well as all volumes that come before that  
790 volume on the drive. Once these sections are enforced, they cannot be written to ever again.  
791 This functionality is particularly useful in protecting data or backups that must never be  
792 modified, but as the enforce function is permanent, it must be used carefully.  
793 9. The **Finalize** column permanently locks the entire drive. This is useful when a drive is full and no  
794 longer needs to be written to. Data can still be read and copied from this drive to other places,  
795 but no write actions will be possible after this is used, so it also must be used carefully.

## 796 2.7 CryptoniteNXT

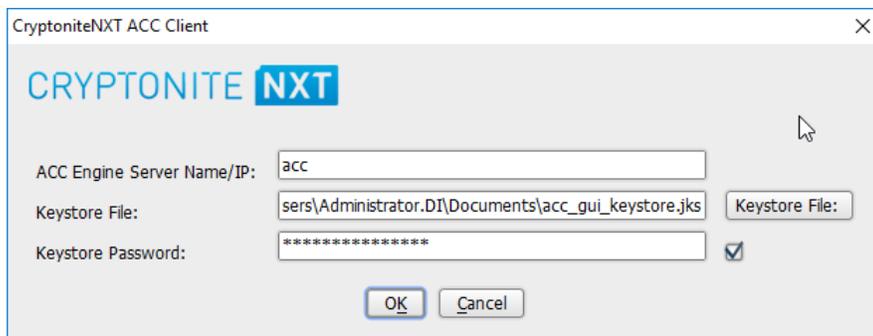
797 See the *CryptoniteNXT 2.6.2 Unified Installation Guide*, which should accompany the device for a  
798 detailed guide on how to install **CryptoniteNXT** on the provided device.

799 The *CryptoniteNXT 2.6.2 Unified Installation Guide* provides a full installation on both the  
800 **CryptoniteNXT** device and the management workstation. When finished, it should be possible to log in  
801 on the management workstation and interact with the **CryptoniteNXT ACC GUI**. Instructions are  
802 provided below for performing various useful functions, including adding new devices/users, as well as  
803 creating policy, but specific recommendations for policy are not provided, as those will be specific to the  
804 organization. Some integrations with other security products used in this guide will be provided, as  
805 exceptions for those products in CryptoniteNXT are often necessary for their functionality.

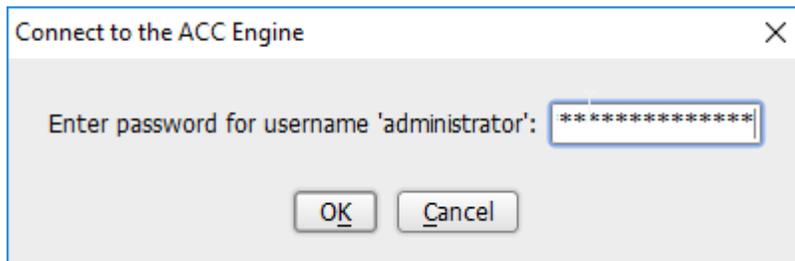
### 806 2.7.1 Configure Cryptonite NXT

#### 807 2.7.1.1 Verify a New Device

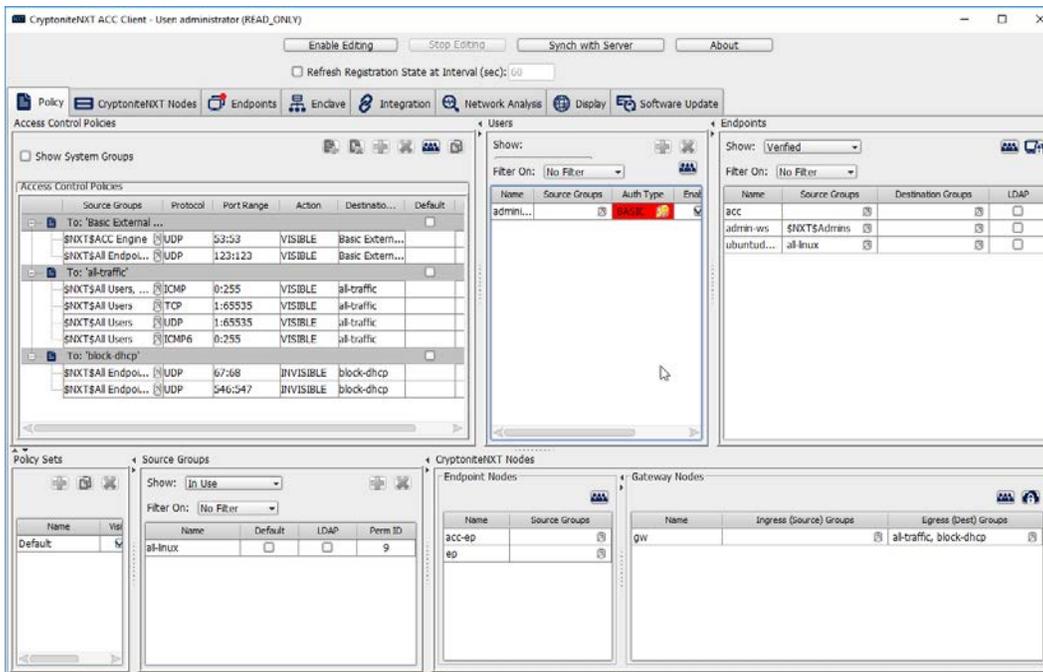
- 808 1. Open the **CryptoniteNXT ACC GUI** application.



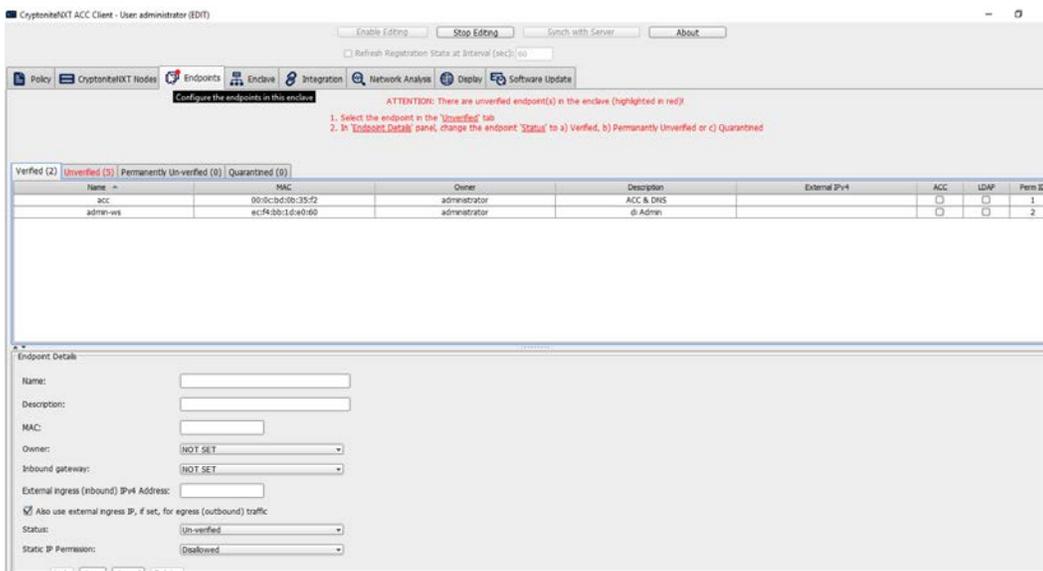
- 809 2. Click **OK**.
- 810 3. Enter the **password** for the account created during the installation.



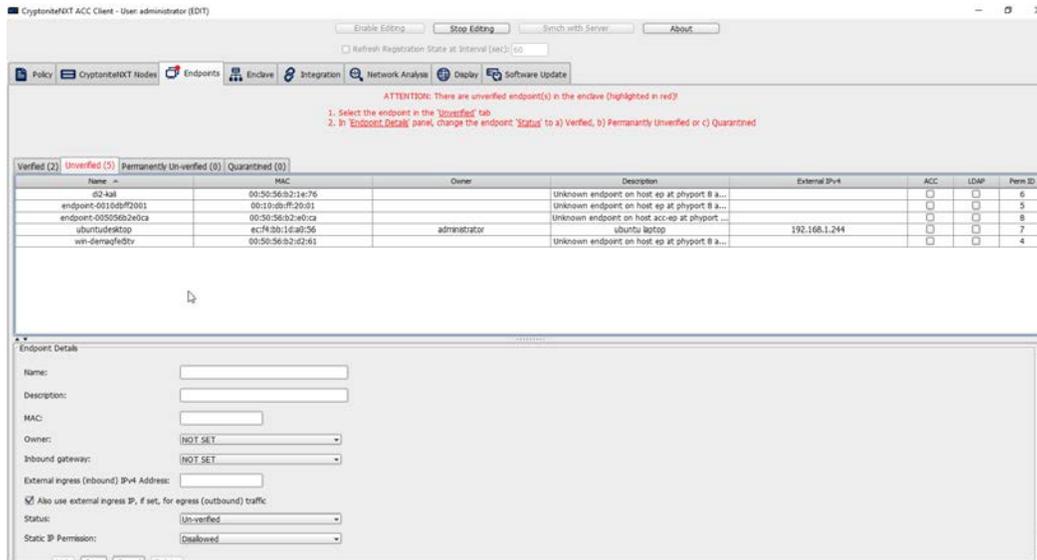
811 4. Click **OK**.



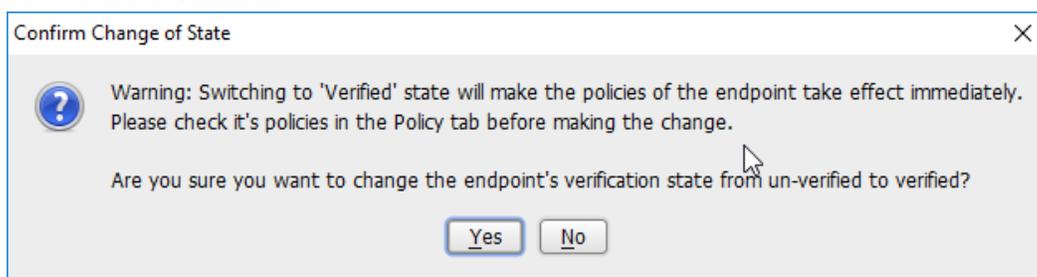
812 5. Click **Enable Editing** at the top of the application.  
 813 6. Click the **Endpoints** tab.  
 814



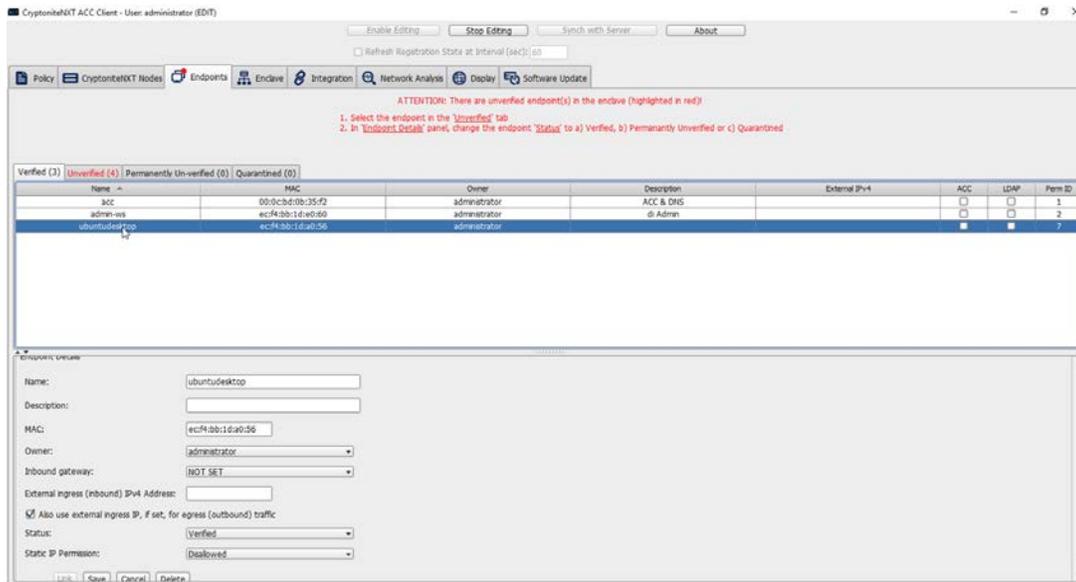
815 7. Click the **Unverified** tab. Any new devices connected to the network should appear here, if  
 816 configured to use Dynamic Host Configuration Protocol (DHCP).  
 817



- 818
- 819
- 820
- 821
- 822
- 823
- 824
- 825
- 826
- 827
- 828
8. Click the machine to verify.
  9. Enter a **name**.
  10. Enter a **description** of the machine.
  11. Select an **owner** if desired. If not selected, the owner will be the first user to log in to CryptoniteNXT on the machine.
  12. Leave **Inbound gateway**: as **NOT SET** to have it choose a default gateway.
  13. Leave **External ingress (inbound) IPv4 Address**: blank.
  14. Ensure the box next to **Also use external ingress IP, if set, for egress (outbound) traffic** is checked.
  15. Set **Status**: to **Verified**.

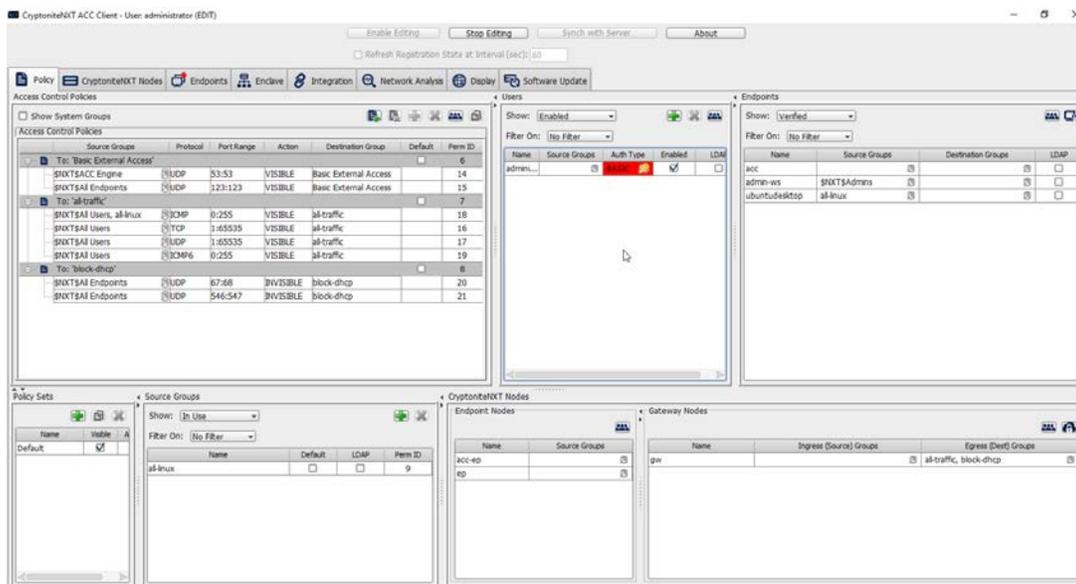


- 829
- 830
- 831
- 832
16. Click **Yes**.
  17. Click **Save**.
  18. The machine should now appear in the **Verified** tab.



833 [2.7.1.2 Create a New User](#)

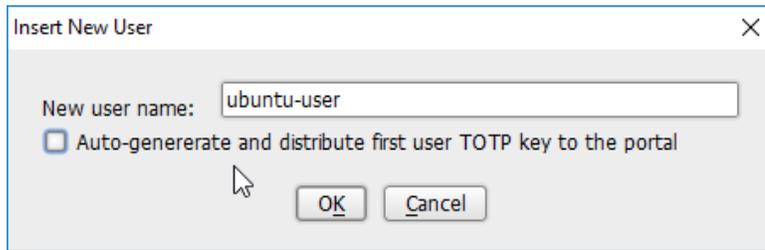
834 1. Go to the **Policy** tab.



- 835
- 836 2. Right-click in the **Users** window and select **New User**.
- 837 3. Enter the username, and uncheck the box next to **Auto-generate and distribute first user TOTP**
- 838 **key to the portal.**

839

840



4. Click **OK**.

841

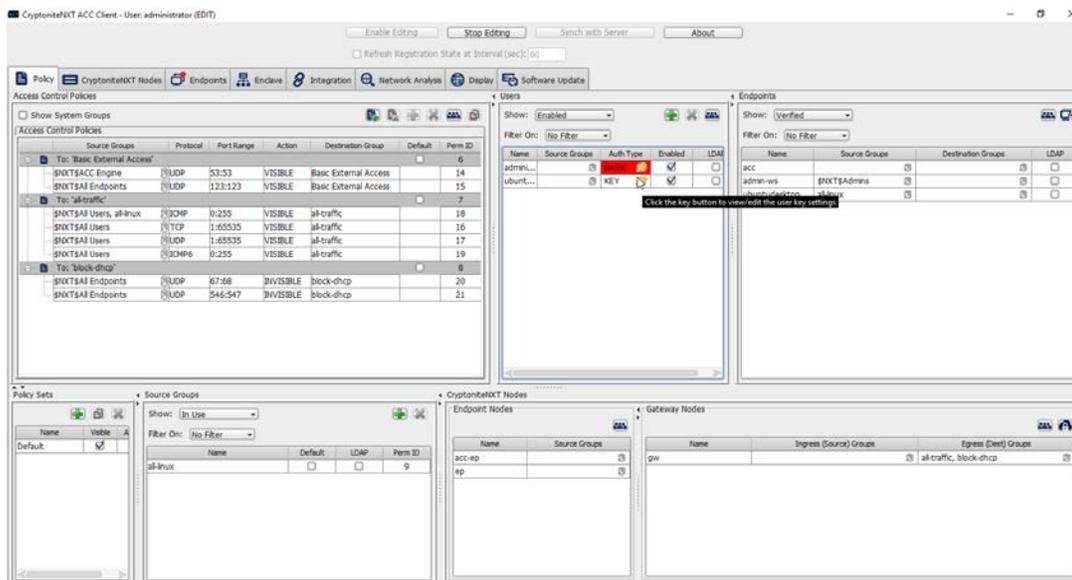
842

843

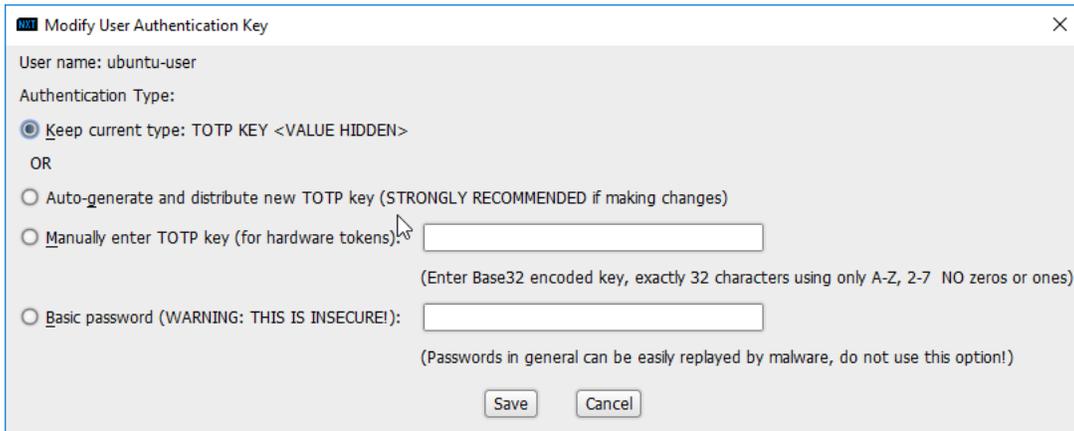
844

845

846

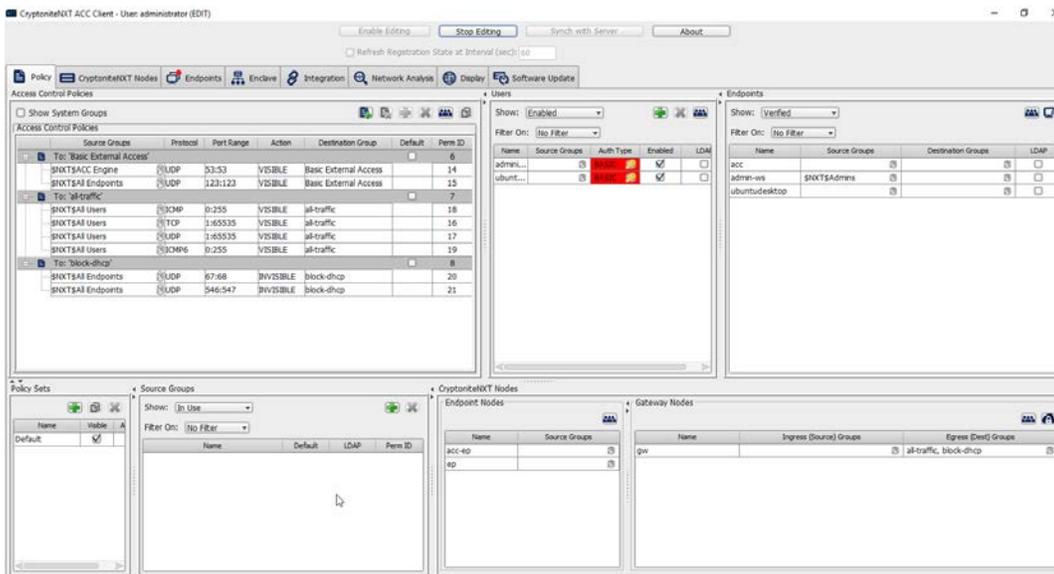


5. The new user should show up in the **Users** window. Click the key icon for the newly created user under **Auth Type**.
6. Decide on an authentication method for the user. (Note: It is not recommended to use passwords, but as this authentication decision depends on the needs of the organization, passwords are used for the purposes of this practice guide.)



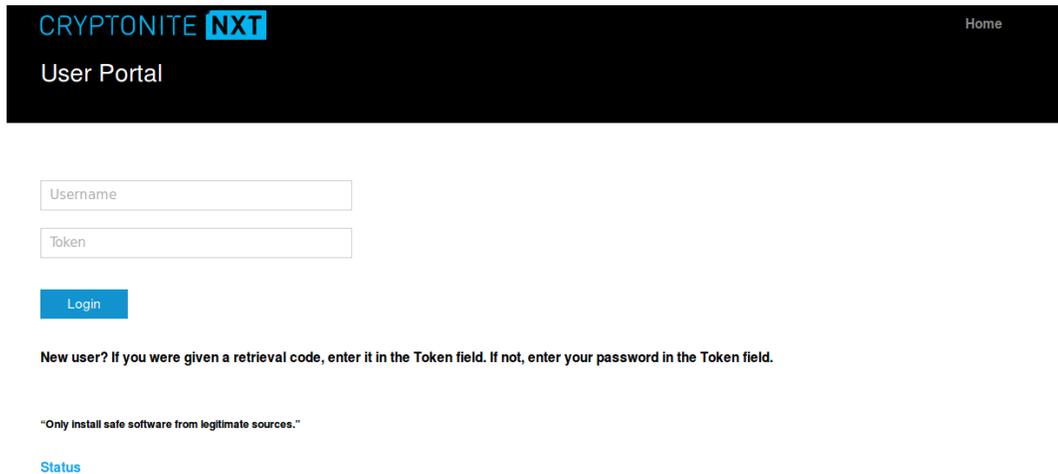
847  
848

7. Click **Save**.



849  
850  
851

8. On the client machine, the user should be required to sign in on the CryptoniteNXT portal to access the internet. Authenticate using the newly created user.

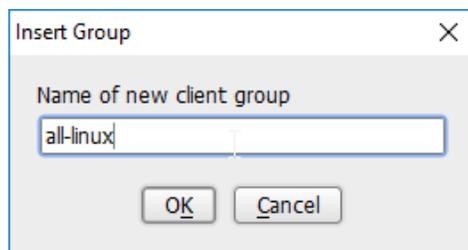


The screenshot shows the 'User Portal' for 'CRYPTONITE NXT'. It features a dark header with the logo and a 'Home' link. Below the header are two input fields: 'Username' and 'Token'. A blue 'Login' button is positioned below the 'Token' field. A note states: 'New user? If you were given a retrieval code, enter it in the Token field. If not, enter your password in the Token field.' A security warning reads: '\*Only install safe software from legitimate sources.\*' and a 'Status' link is at the bottom.

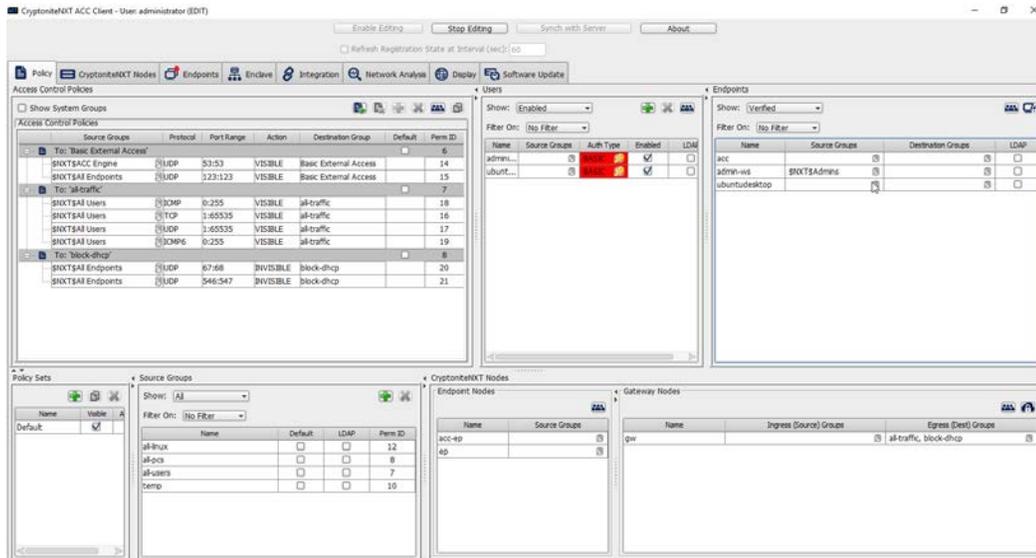
### 852 *2.7.1.3 Create a New Policy*

853 Creating policy in CryptoniteNXT essentially requires specifying allowed types of traffic. To do this,  
854 source groups and destination groups are created.

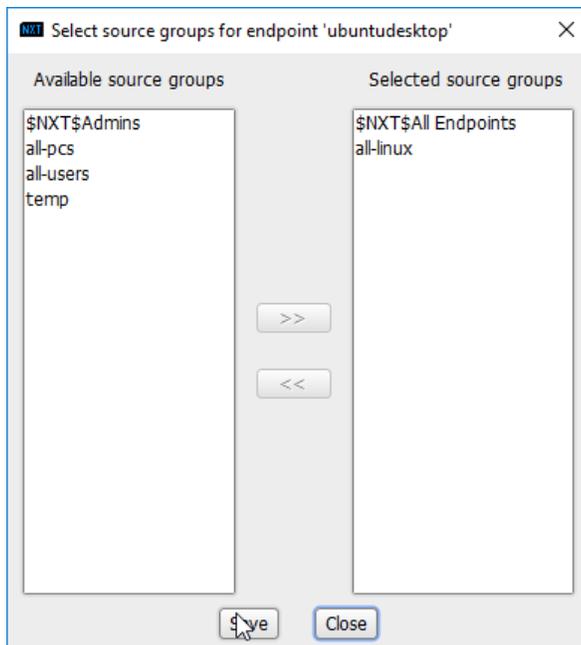
- 855 1. To create a source group, right-click in the **Source Groups** window and select **New Source**
- 856 **Group.**
- 857 2. Enter the name of the group.



- 858
- 859 3. Click **OK.**
- 860 4. The newly created group should appear in the **Source Groups** window.

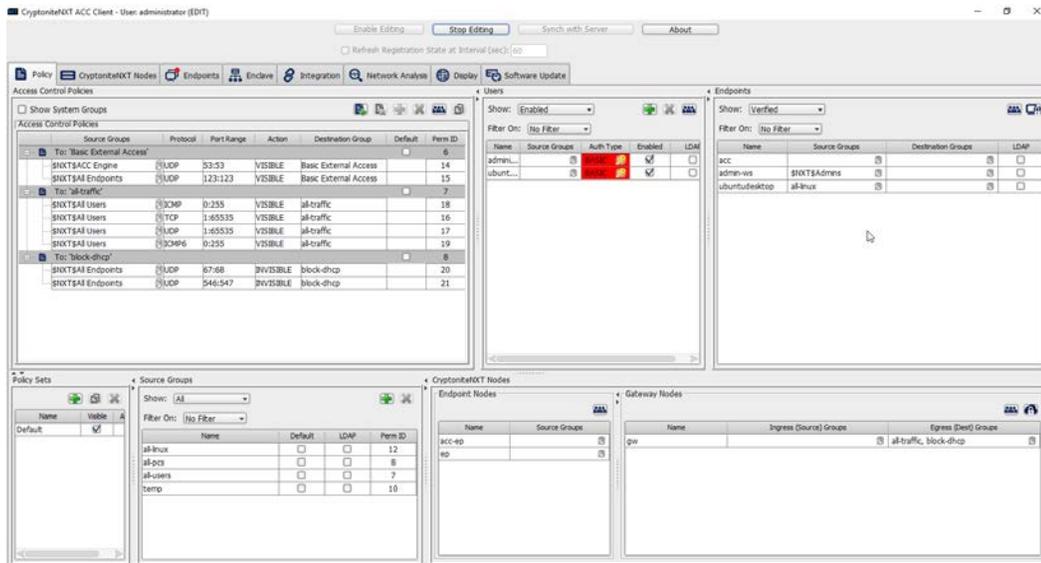


- 861 5. In the **Endpoints** window, click the arrow button under the **Source Groups** column for any  
 862 machines to be added to this **Source Group**.  
 863 6. Select the newly created group (or groups).  
 864 7. Click the >> button to add the endpoint to this group.



- 865  
 866 8. Click **Save**.  
 867 9. The group should show under the **Source Groups** column for those endpoints.

868

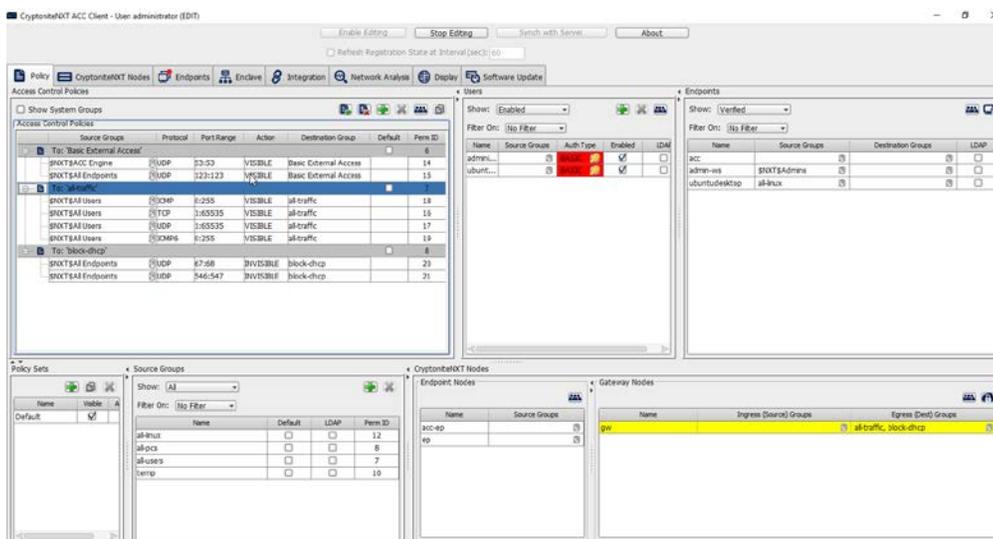


869 Destination groups are used to govern the allowed destinations of endpoints within certain source  
 870 groups. While destination groups can be created according to organizational property, this example  
 871 uses an existing group, **all-traffic**.

872 1. To allow or prevent the use of ping, we add it to the **all-traffic** group. In the **Access Control**  
 873 **Policies** window, right-click on the row labeled **To: 'all-traffic'** and select **New Access**  
 874 **Control Policy Entry**.

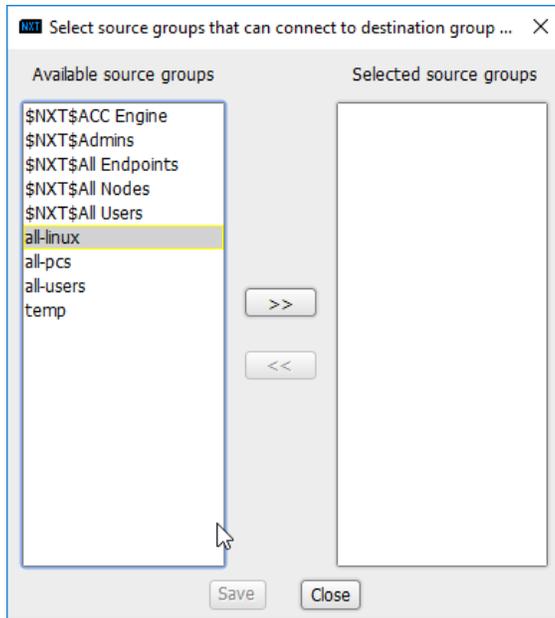
875

876

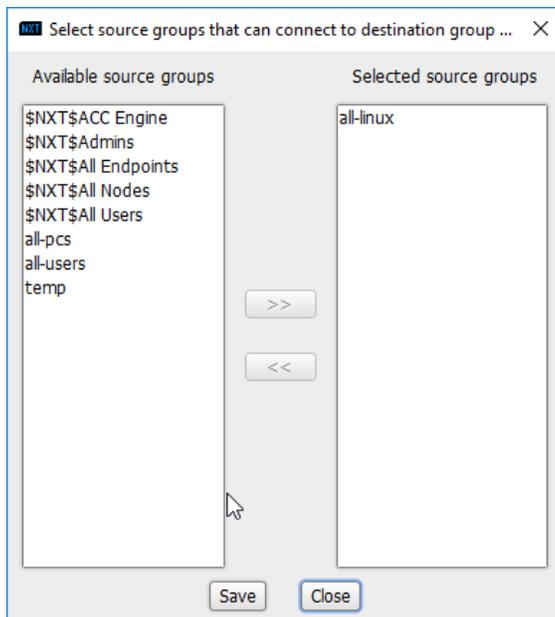


2. Click the arrow button under the **Source Groups** column.

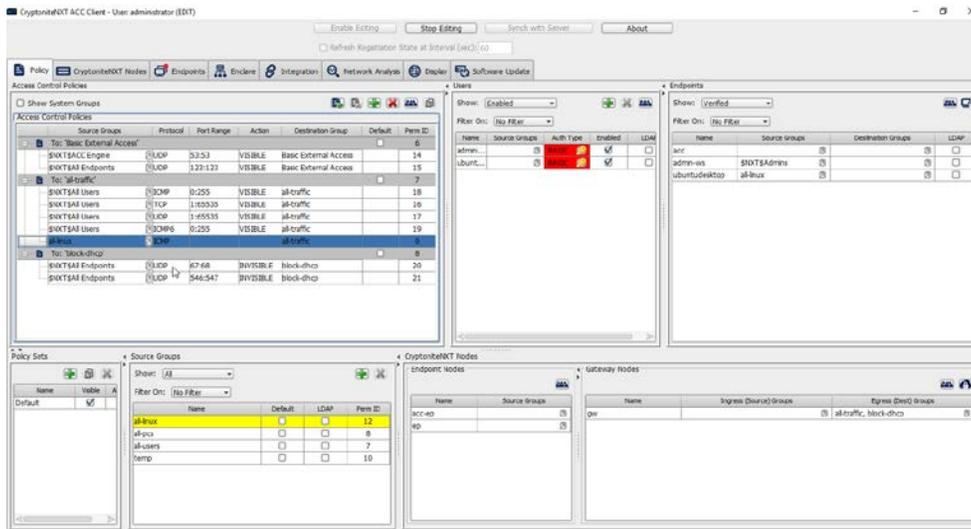
- 877 3. Select the newly created source group.  
878



- 879  
880 4. Click the >> button.

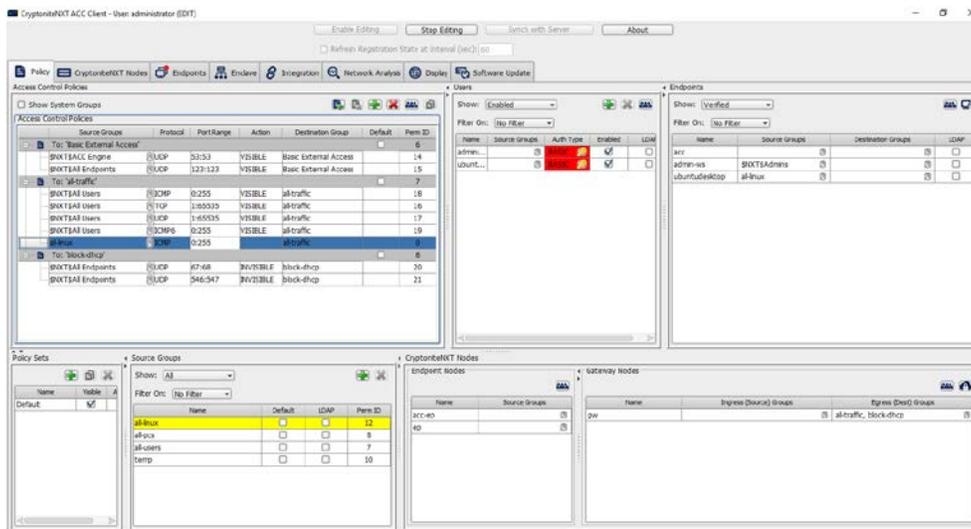


- 881  
882 5. Click **Save**.  
883 6. Select the **Protocol**. In this case, to prevent the machine from using ping, we choose **ICMP**.



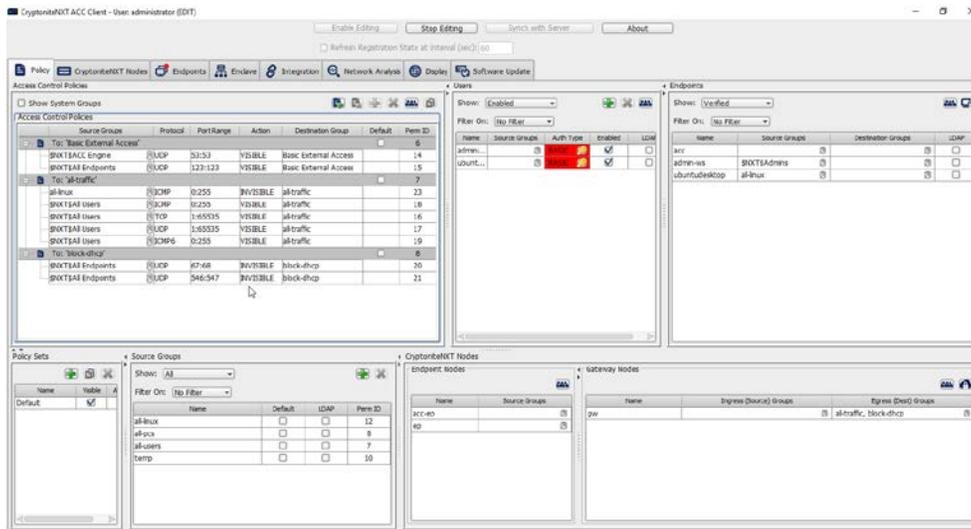
884  
885

7. Enter the port range that this traffic can operate on.



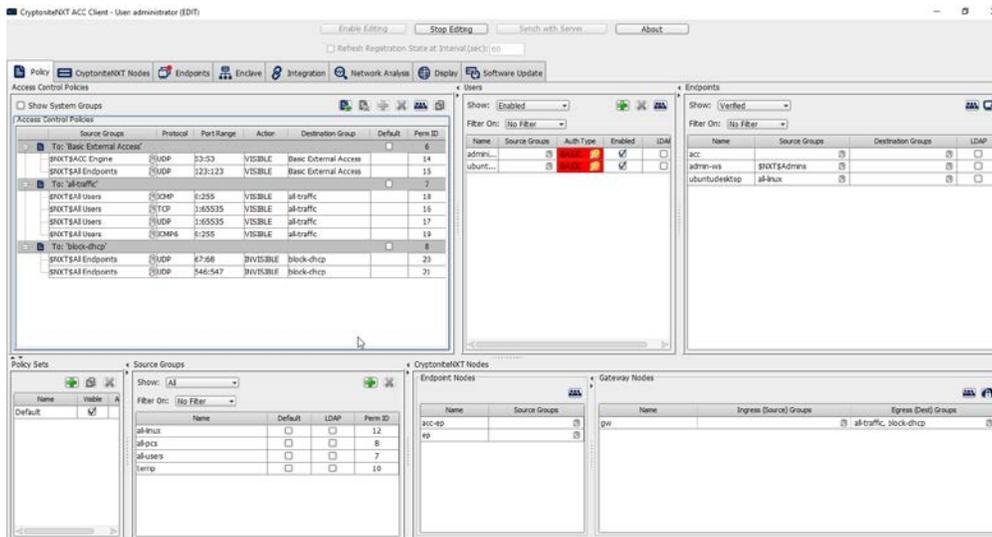
886  
887

8. Select **INVISIBLE** for the **Action** column.



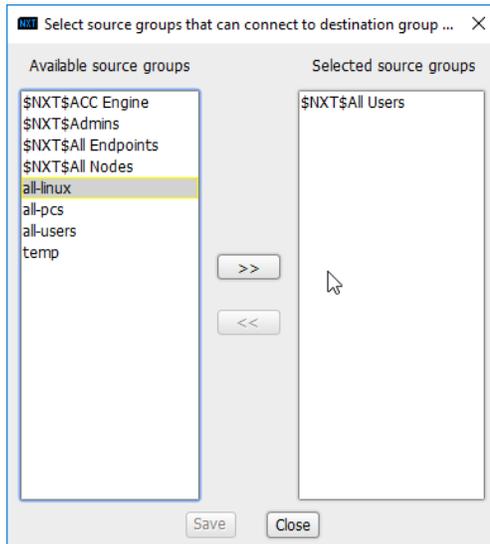
888  
889  
890  
891

9. This will prevent the members of this group from using ping.
10. To allow the members of this group to use ping, delete this rule. Right-click the entry and select **Delete Access Control Policy Entries**.



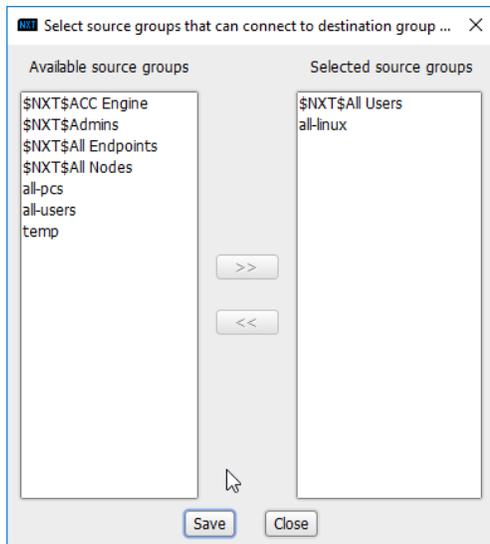
892  
893  
894  
895

11. Add the newly created group to the existing policy entry by clicking the arrow for that entry under **Source Groups**.
12. Select the newly created group.



896  
897

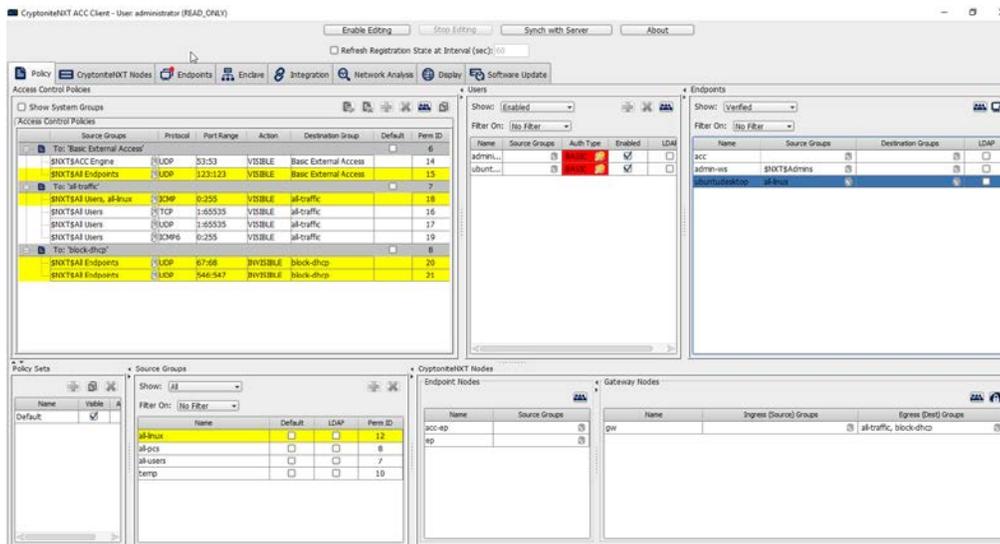
13. Click the >> button.



898  
899  
900

14. Click **Save**.

15. Click **Stop Editing** when finished.



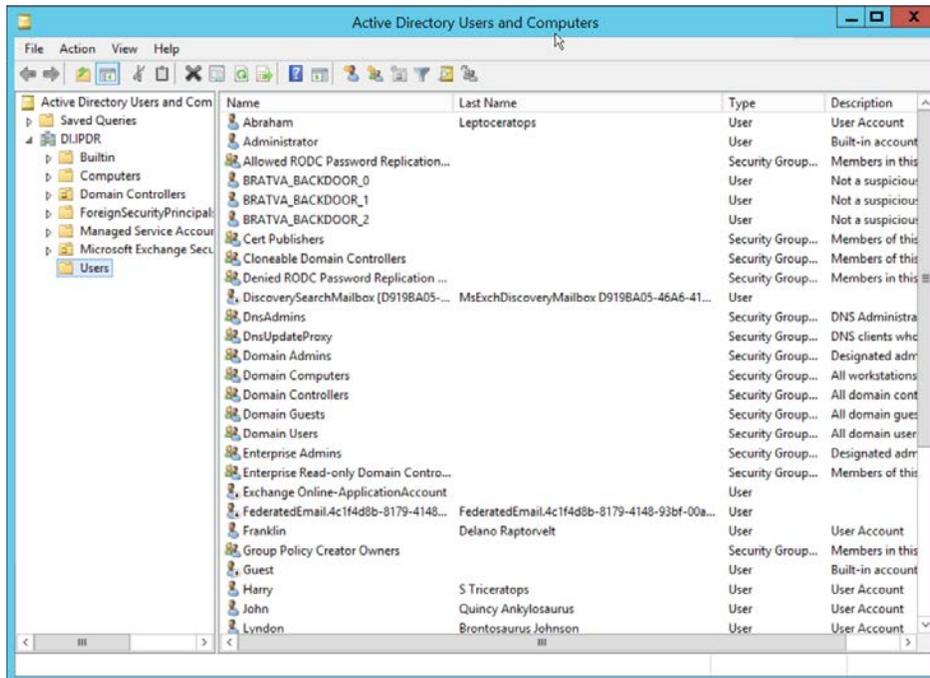
901  
 902 16. Now, the new machine should be allowed to use ping. With these policies it is possible to  
 903 manage all traffic through the specification of groups, ports, and protocols.

## 904 2.7.2 Integrate CryptoniteNXT with Active Directory

905 In this section, devices listed in Active Directory will be imported into CryptoniteNXT. For this to be  
 906 successful, the DNS server must have reverse lookup zones configured for the AD server. Please see  
 907 Section 2.1.6 for setting up reverse lookup zones on the AD/DNS server.

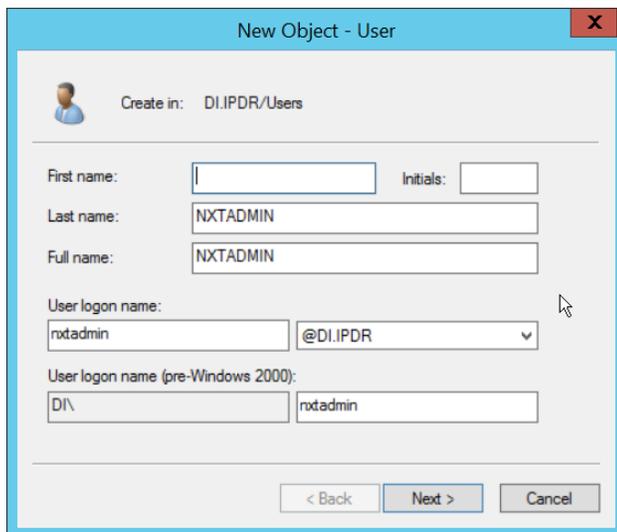
### 908 2.7.2.1 Generate a Keytab File

909 1. Open **Active Directory Users and Computers**.



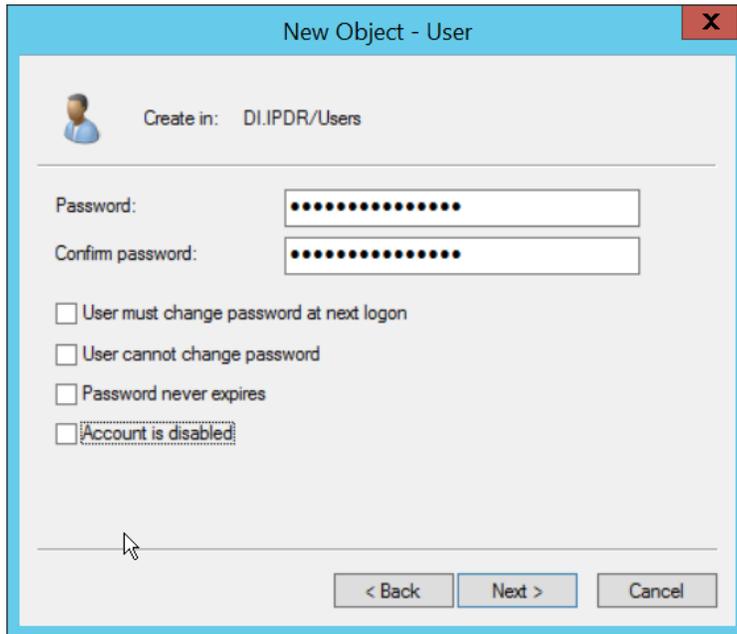
910  
911  
912

2. Right-click the **Users** folder in the left pane and select **New > User**.
3. Enter a **name** for this user, such as nxtadmin.



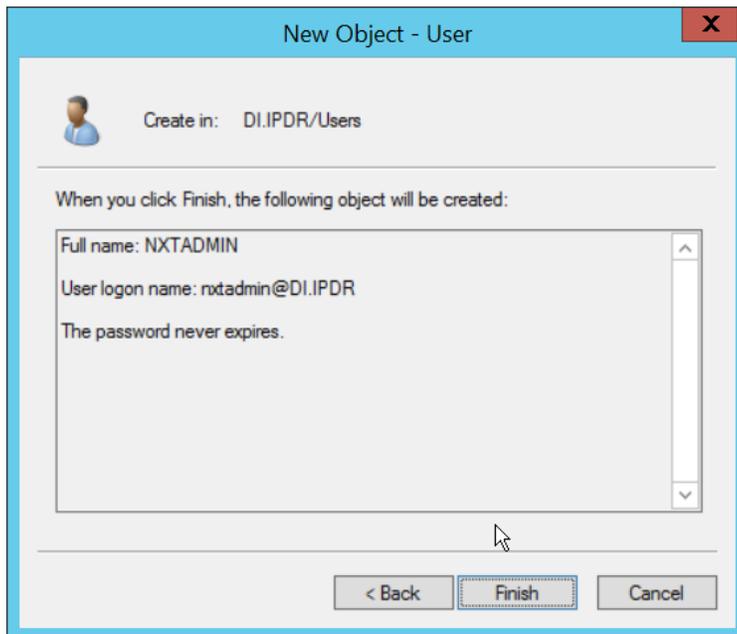
913  
914  
915

4. Click **Next**.
5. Enter a **password** for this user, and set the password policy.



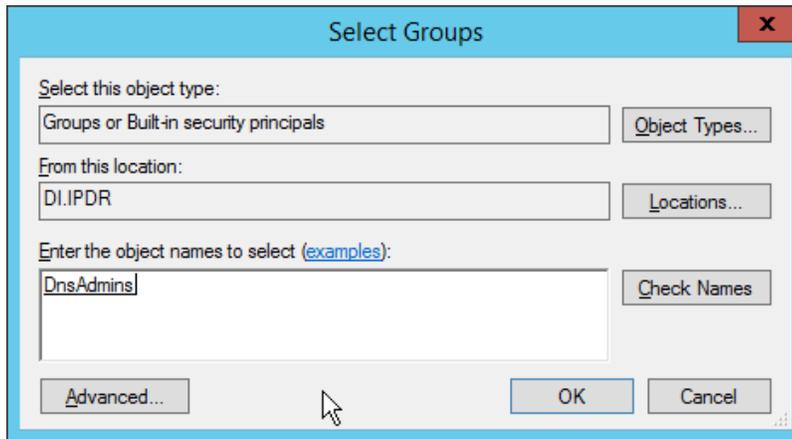
916  
917

6. Click **Next**.



918  
919  
920  
921

7. Click **Finish**.
8. Right-click the newly created user and select **Add to a group....**
9. Enter **DnsAdmins**.



922

923

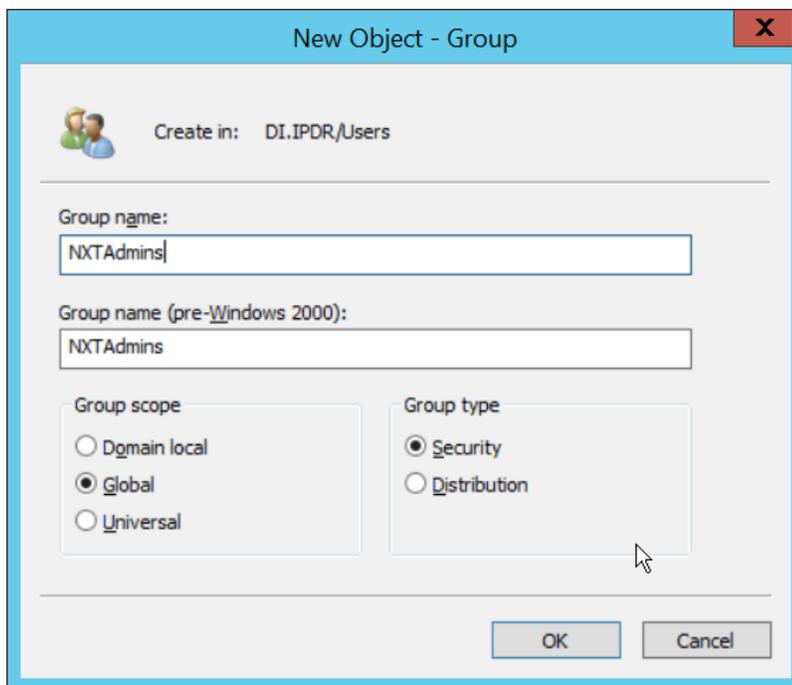
924

925

10. Click **OK**.

11. Right-click the **Users** folder in the left pane and select **New > Group**.

12. Enter **NXTAdmins** as the group name.



926

927

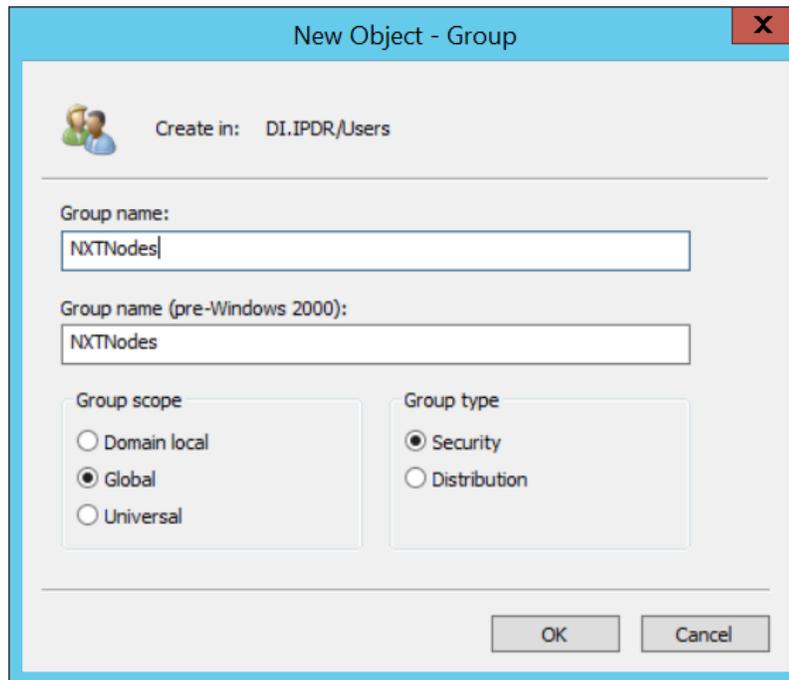
928

929

13. Click **OK**.

14. Right-click the **Users** folder in the left pane and select **New > Group**.

15. Enter **NXTNodes** as the group name.



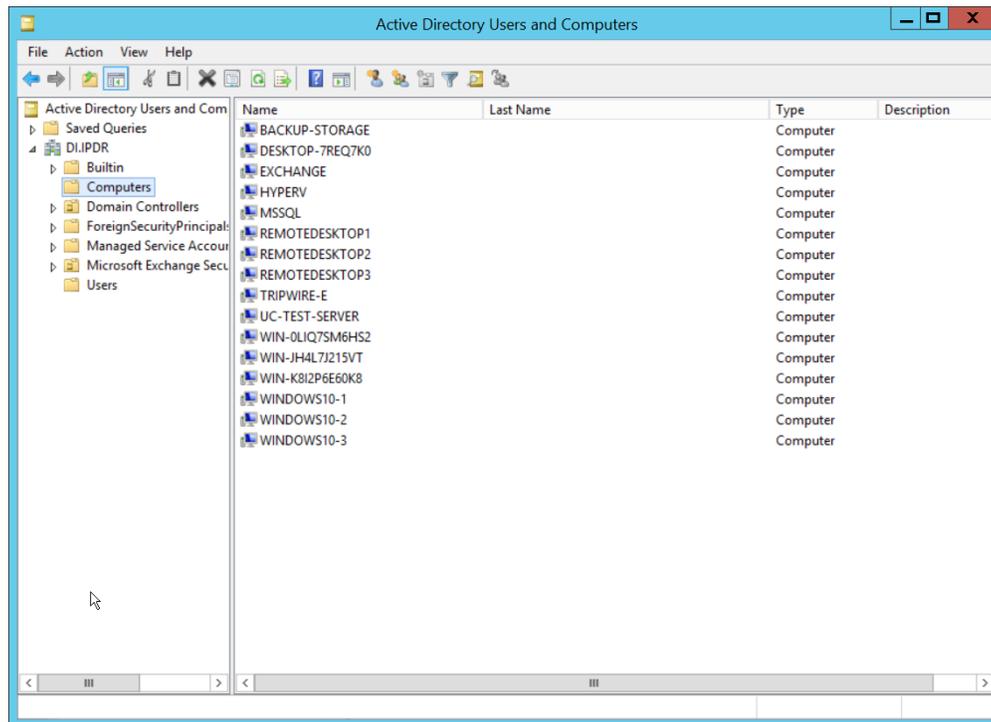
930

931

932

16. Click **OK**.

17. Click **Computers** in the left pane.



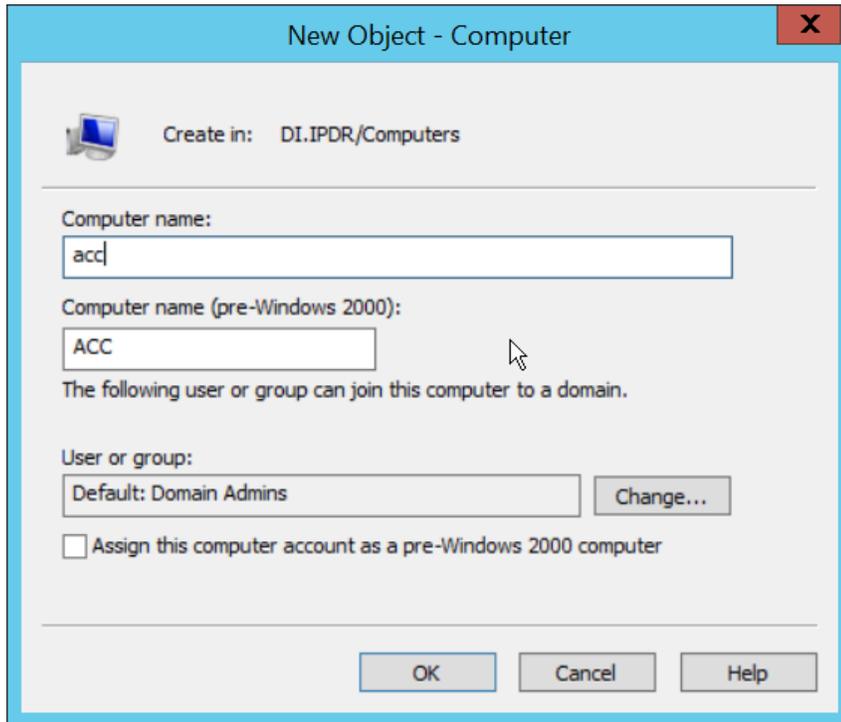
933

934

935

18. Right-click **Computers** in the left pane and select **New > Computer**.

19. Enter the name of the acc server for **CryptoniteNXT** (Node A).



936

20. Click **OK**.

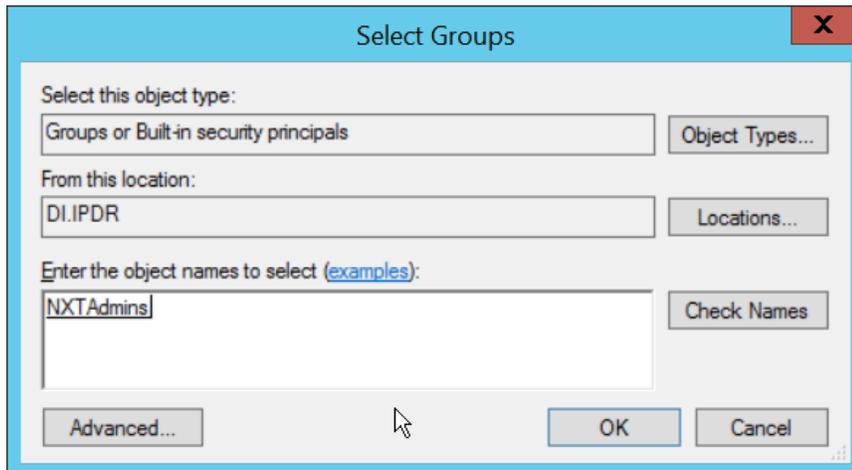
937

938

21. Right-click the newly created computer and select **Add to a group...**

939

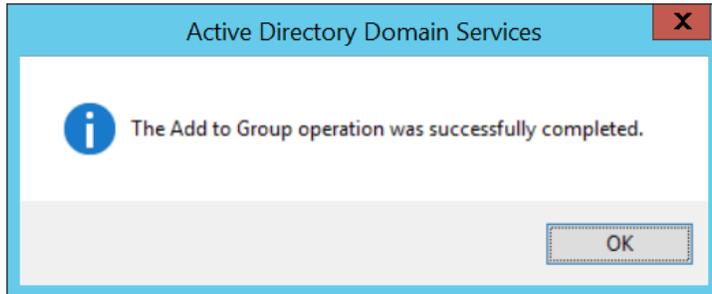
22. Enter **NXTAdmins** in the box labeled **Enter the object names to select (examples):**.



940

23. Click **OK**.

941



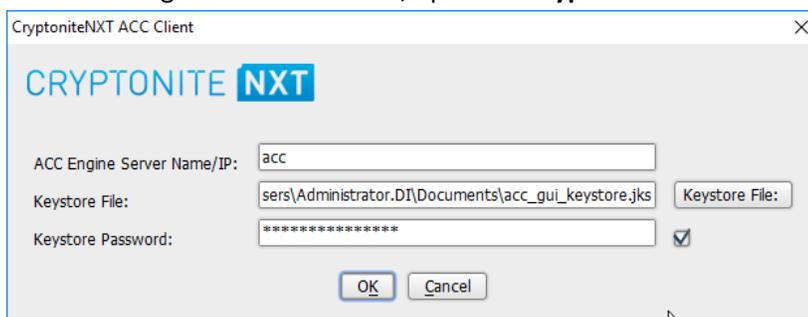
- 942
- 943 24. Click **OK**.
- 944 25. Open a new Administrator **PowerShell** window.
- 945 26. Enter the following command, using the newly created user in the **DnsAdmins** group:
- 946 `> ktpass -princ DNS/<user>.<domain>@<DOMAIN> -mapuser`
- 947 `<user>@<domain> -pass <user password> -out .\<keytab filename>`
- 948 `-ptype krb5_nt_principal -crypto all`

- 949
- 950 For example:
- 951 `> ktpass -princ DNS/nxtadmin.di.ipdr@DI.IPDR -mapuser`
- 952 `nxtadmin@di.idpr -pass password123 -out .\keytab.out -ptype`
- 953 `krb5_nt_principal -crypto all`

- 954
- 955 27. This will produce a keytab file. Copy this file to the CryptoniteNXT Management
- 956 workstation.

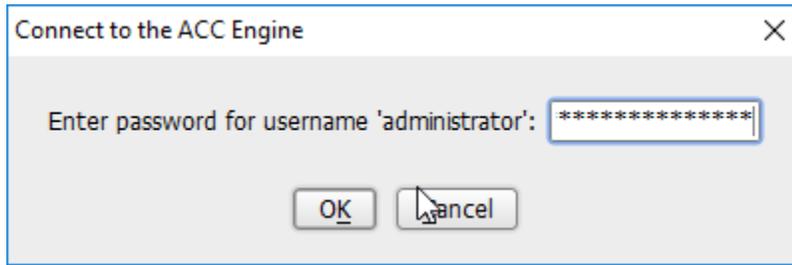
### 957 *2.7.2.2 Import Keytab File to ACC*

- 958 1. On the management workstation, open the **CryptoniteNXT ACC GUI**.

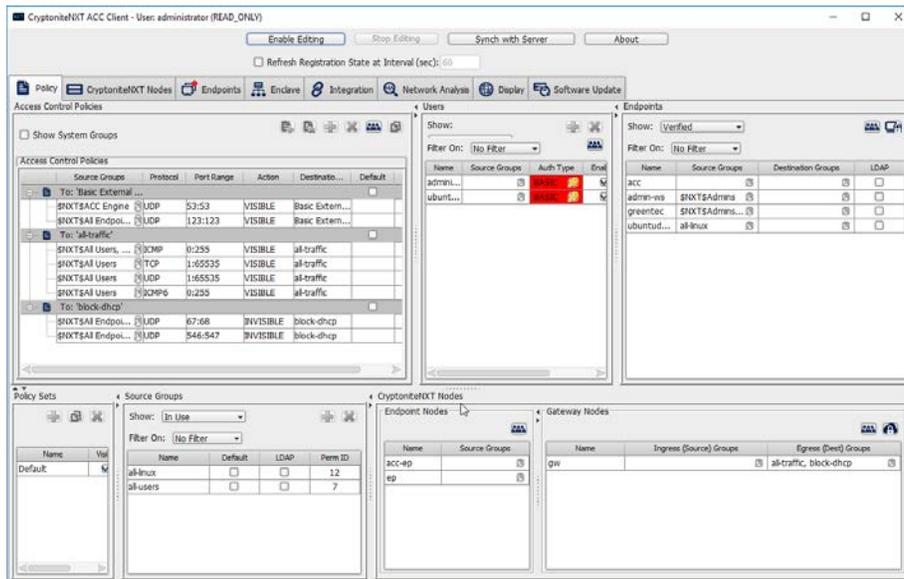


- 959
- 960 2. Click **OK**.
- 961 3. Enter the **password** configured during installation.

962  
963

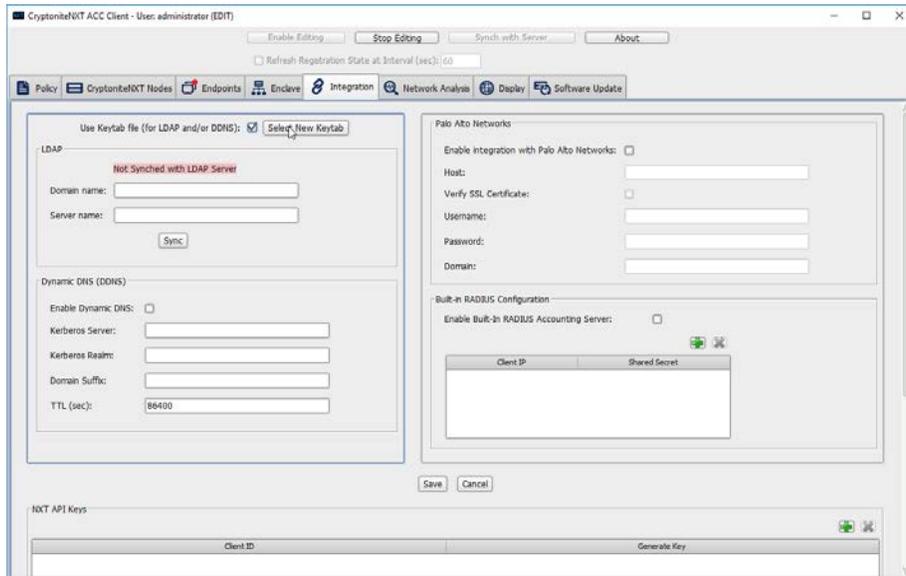


4. Click **OK**.



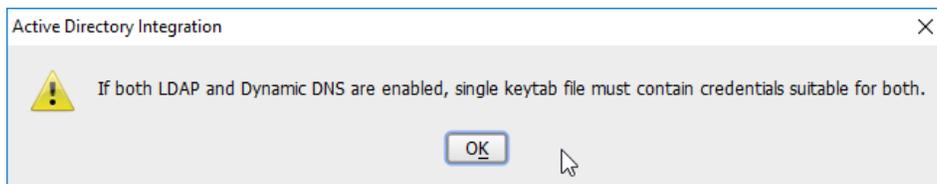
964  
965  
966  
967

5. Click **Enable Editing**.
6. Click the **Integration** tab.
7. Check the box next to **Use Keytab file (for LDAP and/or DDNS):**.



968  
969

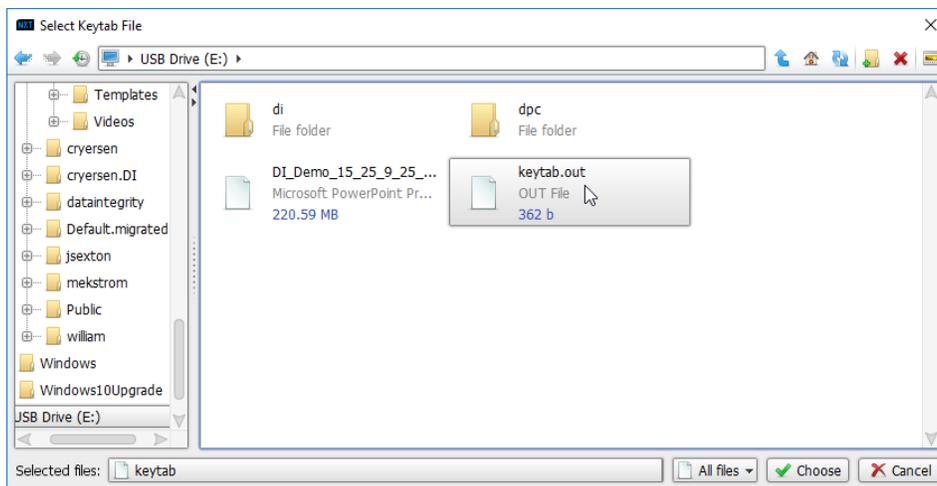
8. Click **Select New Keytab**.



970  
971  
972

9. Click **OK**.

10. Navigate to the keytab file.

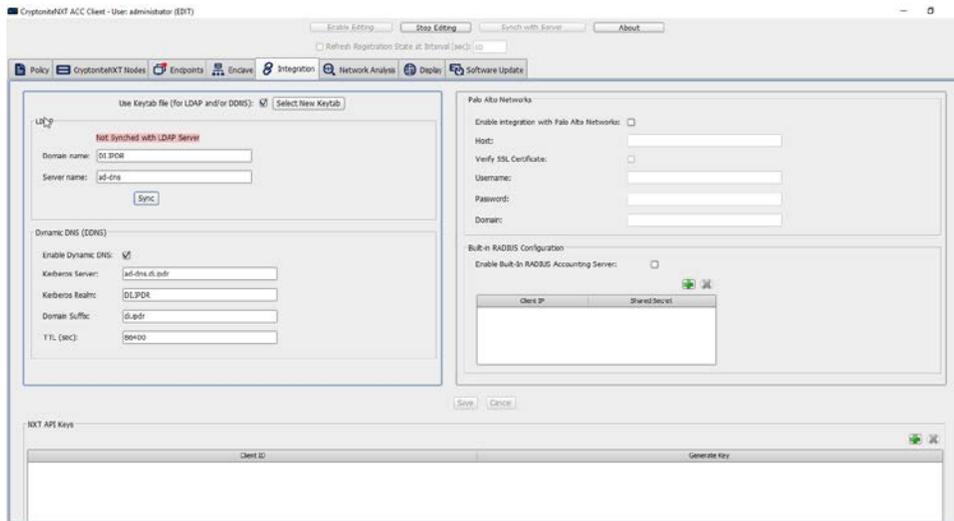


973  
974  
975

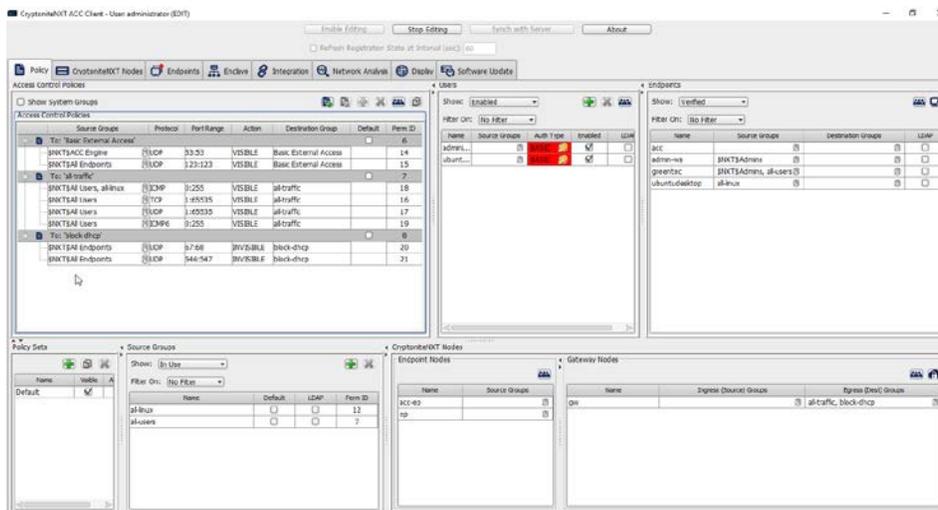
11. Click **Choose**.

12. Click **Save**.

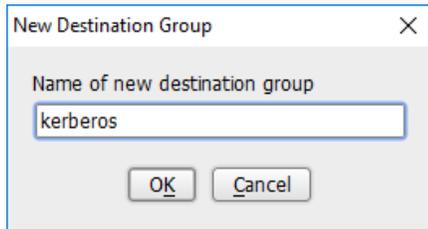
- 976 13. Under **LDAP**, enter the **Domain name** (such as DI.IPDR) and the **Server name** (such as ad-  
 977 dns).
- 978 14. Check the box next to **Enable Dynamic DNS:**
- 979 15. Enter the **fully qualified domain name** of the DNS server (such as ad-dns.di.ipdr).
- 980 16. Enter the **Kerberos realm** (such as DI.IPDR).
- 981 17. Enter the **domain suffix** (such as di.ipdr).



- 982
- 983 18. Click **Save**.
- 984 19. Click the **Policies** tab.

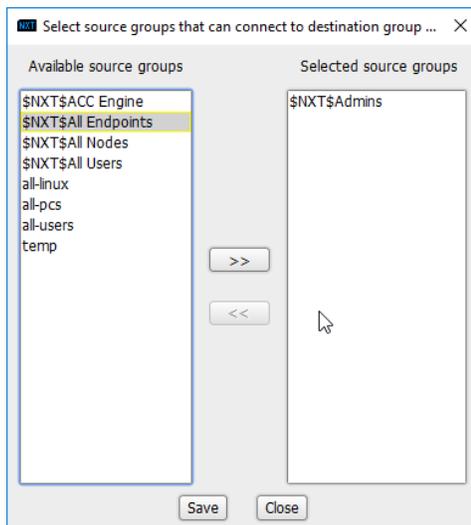


- 985
- 986 20. Right-click in the **Access Control Policies Window** and select **New Destination Group**.
- 987 21. Enter **kerberos**.



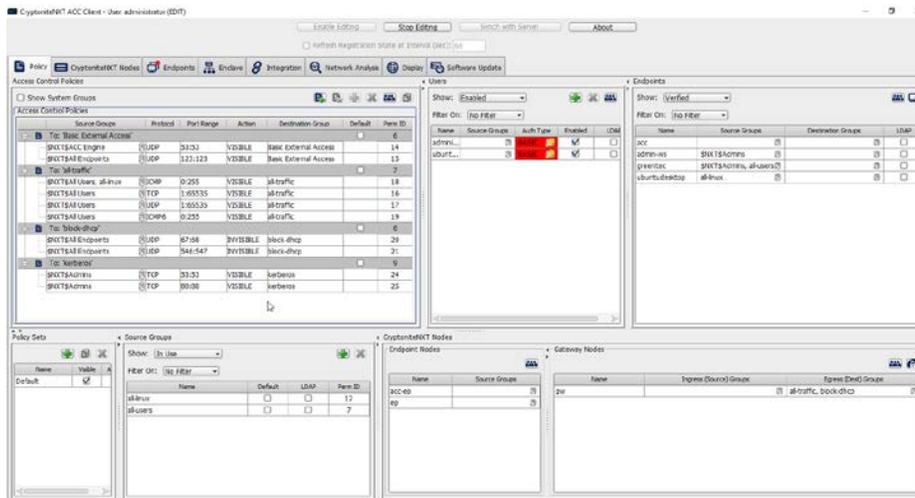
988  
989  
990  
991  
992  
993  
994  
995

- 22. Click **OK**.
- 23. Select **TCP** under **Action**.
- 24. Enter 53:53 under **Port Range**.
- 25. Select **VISIBLE** under **Action**.
- 26. Click the arrow under **Source Groups**.
- 27. Select **\$NXT\$Admins**.
- 28. Click the >> button.



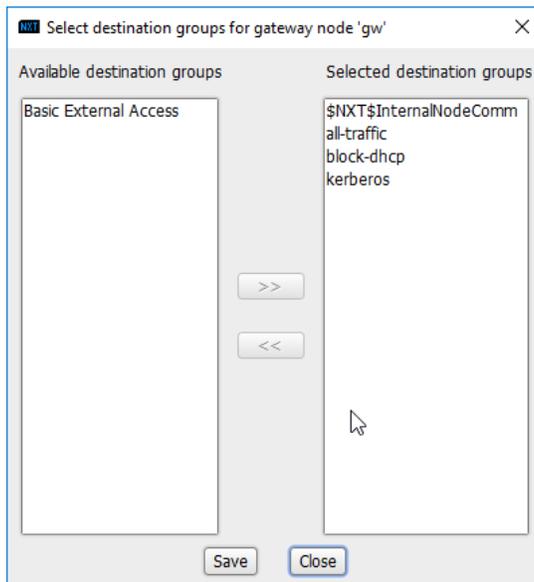
996  
997  
998  
999

- 29. Click **Save**.
- 30. Right-click the **To: 'kerberos'** destination group, and select **New Access Control Policy Entry**.



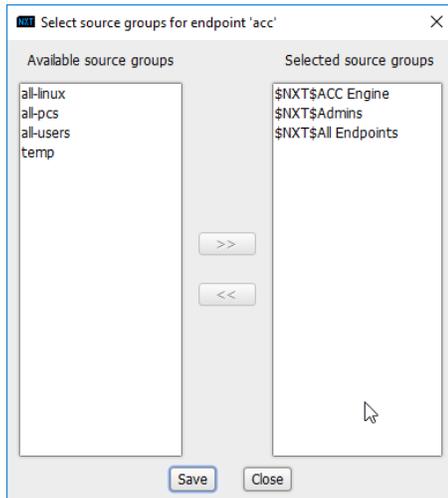
1000  
1001  
1002  
1003  
1004

31. Repeat steps 21–29, but replace 53:53 with 88:88.
32. In the **Gateway Nodes** window, click the arrow under **Egress (Dest) Groups**.
33. Select “kerberos”.
34. Click the >> button.



1005  
1006  
1007  
1008  
1009  
1010

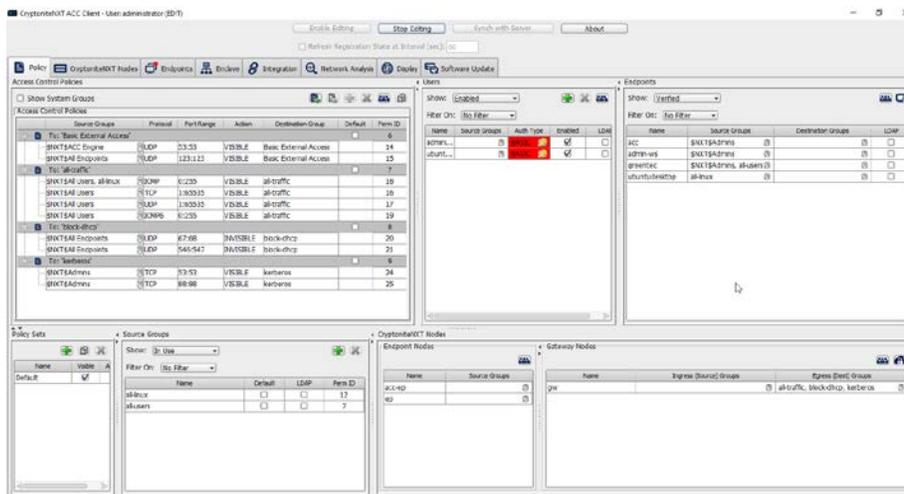
35. Click **Save**.
36. In the **Endpoints** window, click the arrow under **Source Groups** associated with the Administration Control Center (ACC).
37. Select **\$NXT\$Admins**.
38. Click the >> button.



1011

1012

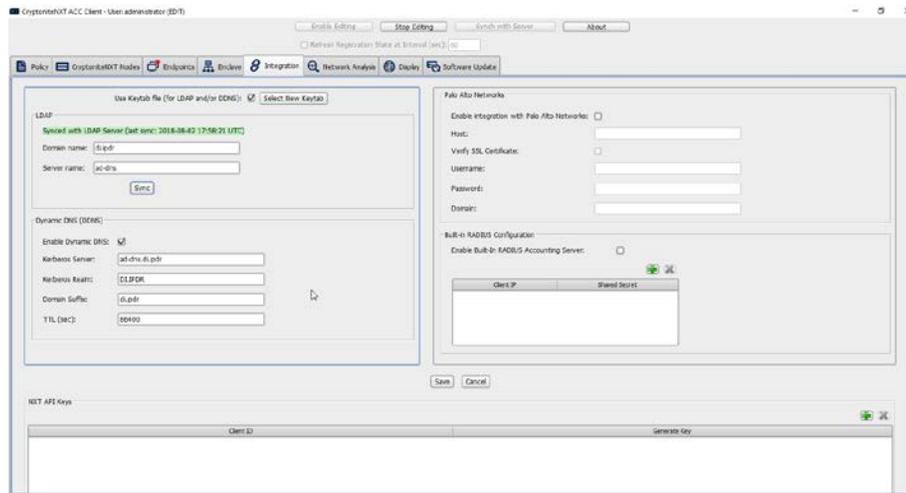
39. Click **Save**.



1013

1014

40. Return to the **Integration** tab.



1015

1016

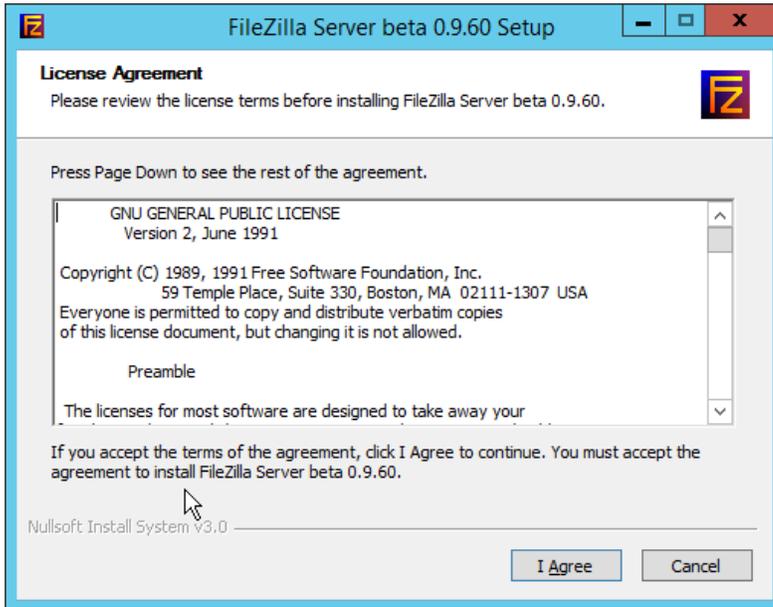
41. Click **Sync**.

## 1017 2.8 Backups

1018 For this capability we use an integration of two open-source tools: **Duplicati** and **FileZilla**. **FileZilla** acts  
 1019 as a File Transfer Protocol (FTP) (over TLS) server component, while **Duplicati** acts as an encrypted  
 1020 backup client. This section details the installation and integration of both tools, as well as the process  
 1021 for creating a backup schedule, but does not provide specific recommendations on backup frequency or  
 1022 backup targets as those are specific to the organization.

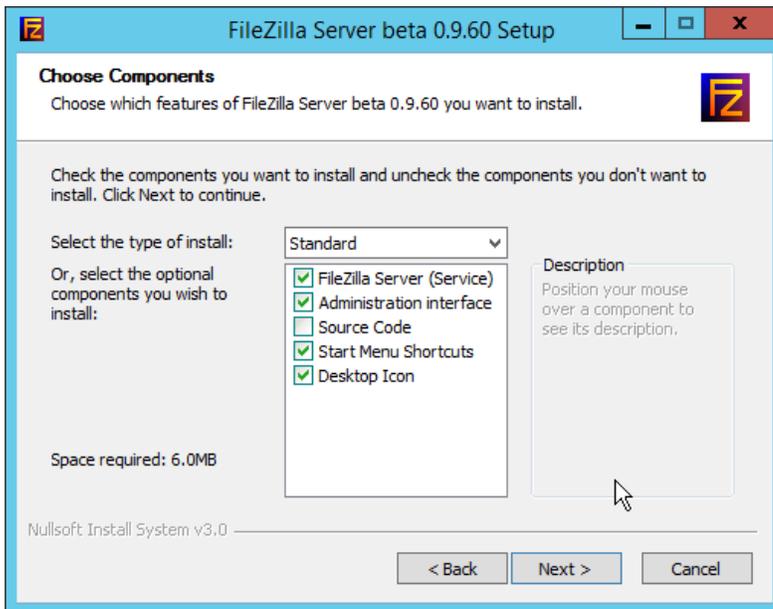
### 1023 2.8.1 FileZilla FTPS Server Setup

1024 1. Run **FileZilla\_Server-0\_9\_60\_2.exe**.



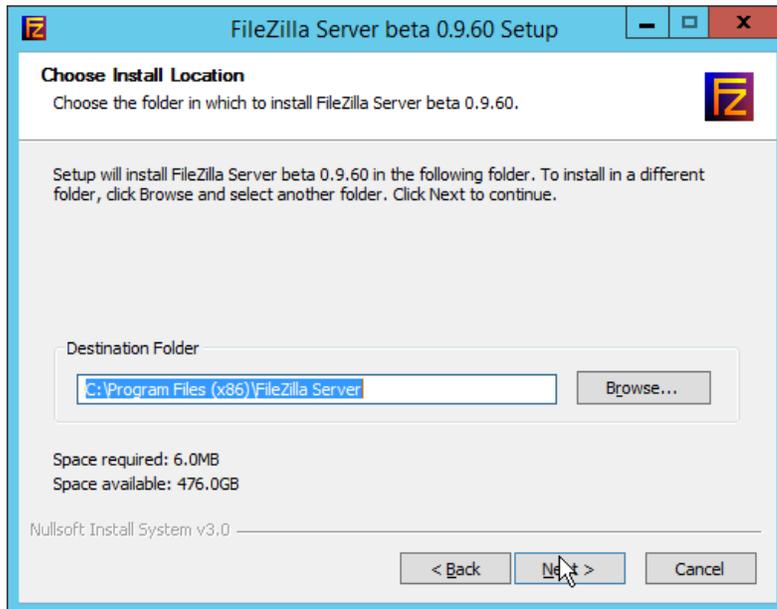
1025  
1026  
1027

2. Click **I Agree**.
3. Select **Standard** from the drop-down menu.



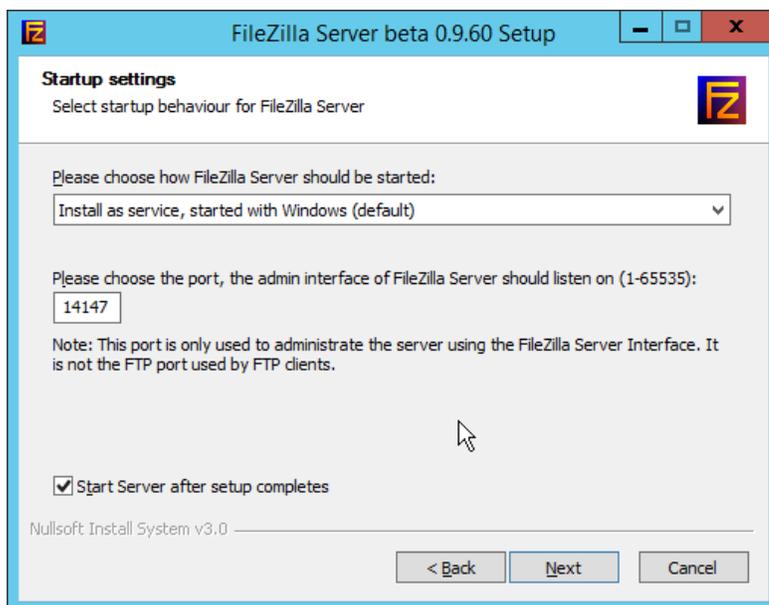
1028  
1029

4. Click **Next**.



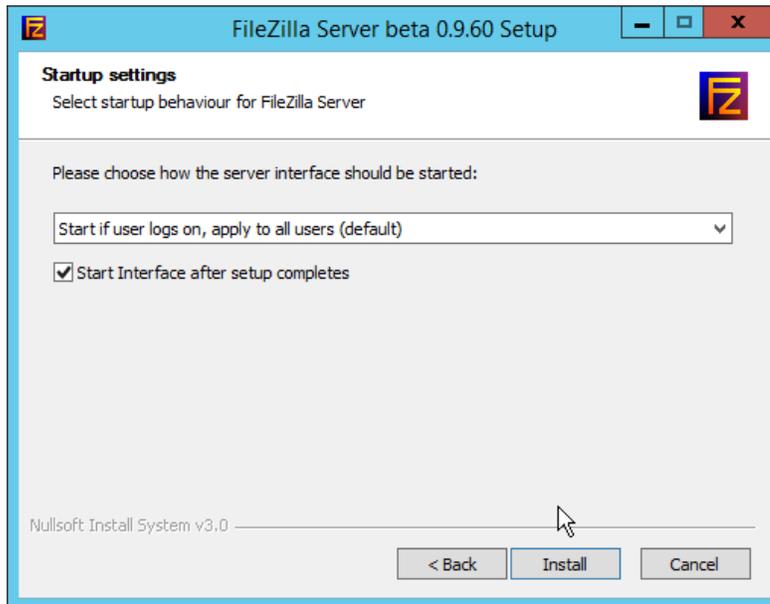
1030  
1031  
1032  
1033  
1034

5. Click **Next**.
6. Select **Install as service, started with Windows (default)** from the drop-down.
7. Specify a port (for the administrator interface to run on) if desired (the default is 14147).
8. Ensure the box next to **Start Server after setup completes** is checked.



1035  
1036

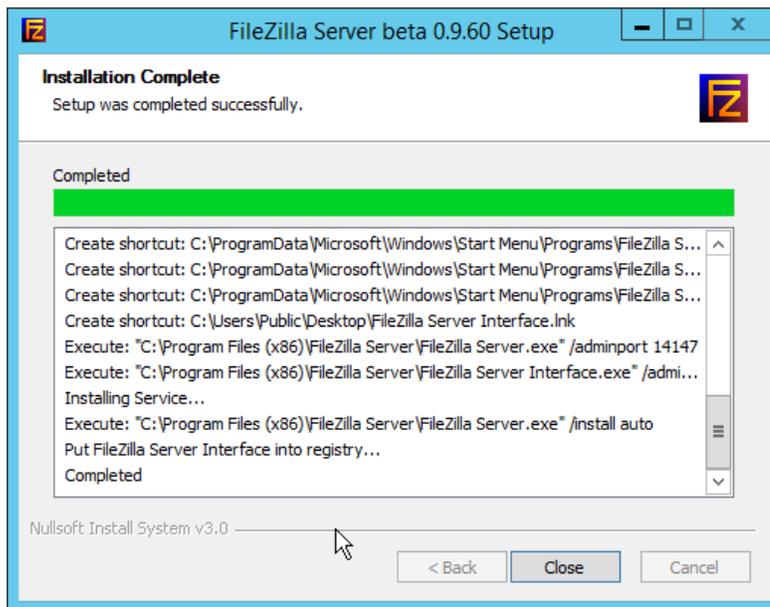
9. Click **Next**.



1037

1038

10. Click **Install**.



1039

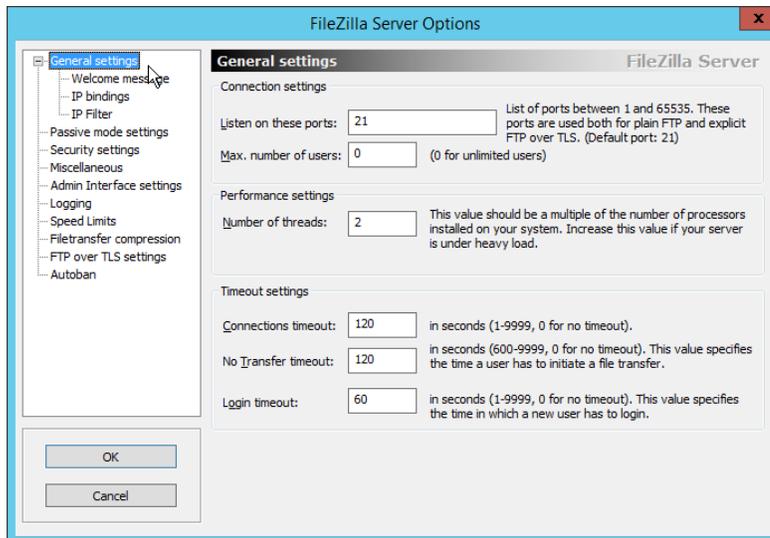
1040

11. Click **Close**.

## 1041 2.8.2 FileZilla Configuration

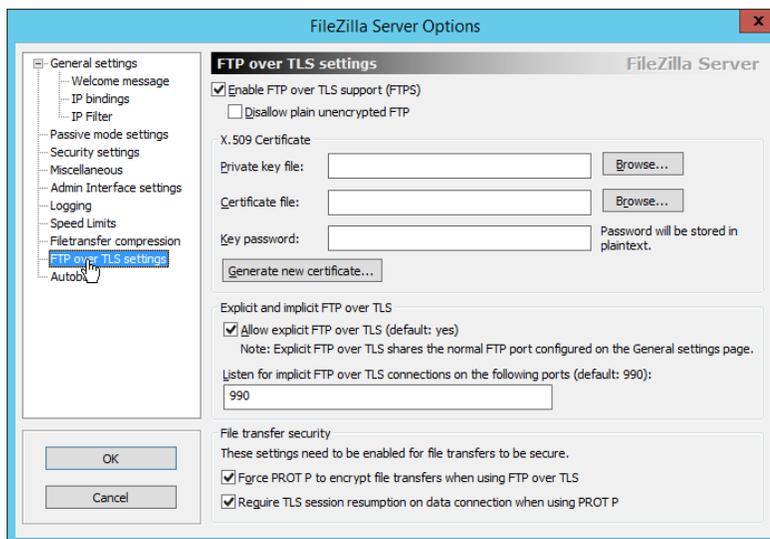
1042 1. When the administrator interface comes up, ensure that the port is correct and click **Connect**.

- 1043 2. Click **Edit > Settings**.



1044

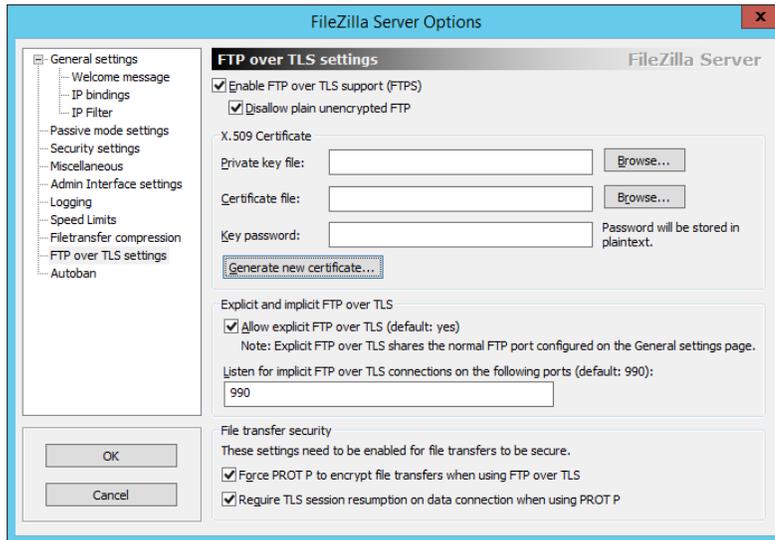
- 1045 3. Click **FTP over TLS settings**.



1046

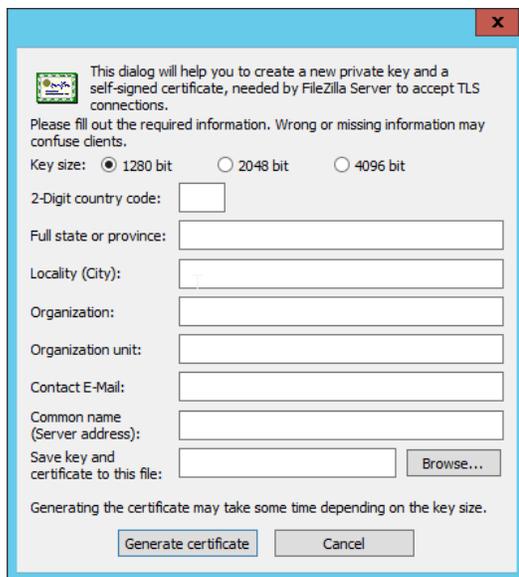
- 1047 4. Check the box next to **Enable FTP over TLS support (FTPS)**.

- 1048 5. Check the box next to **Disallow plain unencrypted FTP**.



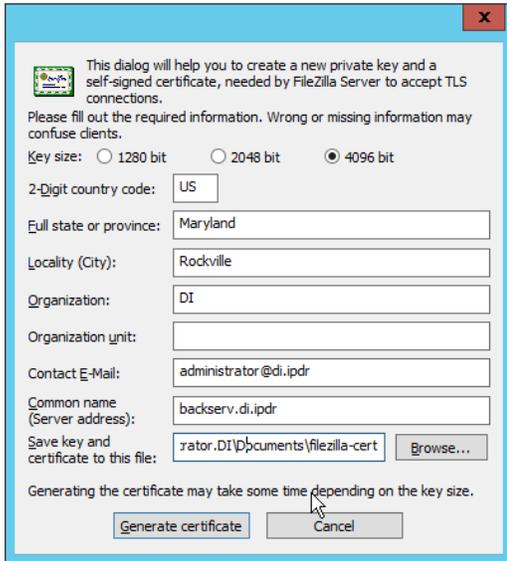
1049  
1050

6. Click **Generate new certificate**.



1051  
1052  
1053  
1054  
1055

7. Select **4096 bit** for **Key Size**.
8. Enter the information for the certificate specific to your organization.
9. For the **common name**, enter the address of the server on which this is installed.
10. Click **Browse** and specify a file location for the certificate.



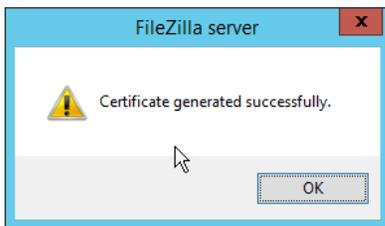
1056

1057

1058

1059

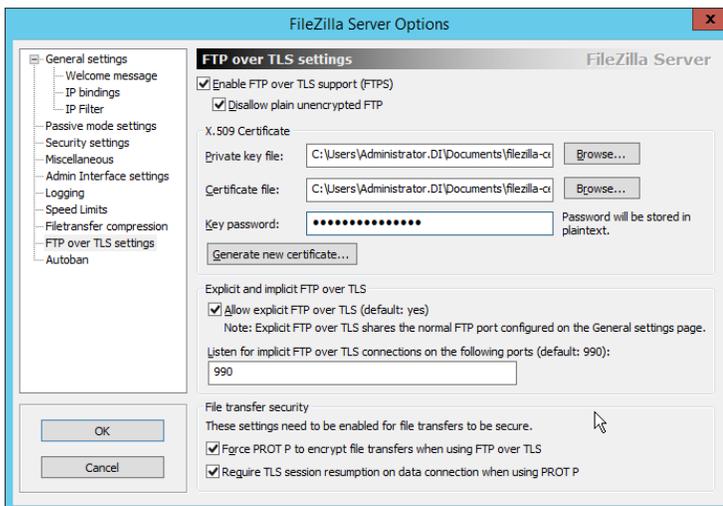
11. Click **Generate certificate**. (The file now contains both the private key and the certificate. These can be separated, for ease of use, as long as the correct file locations are specified in the settings.)



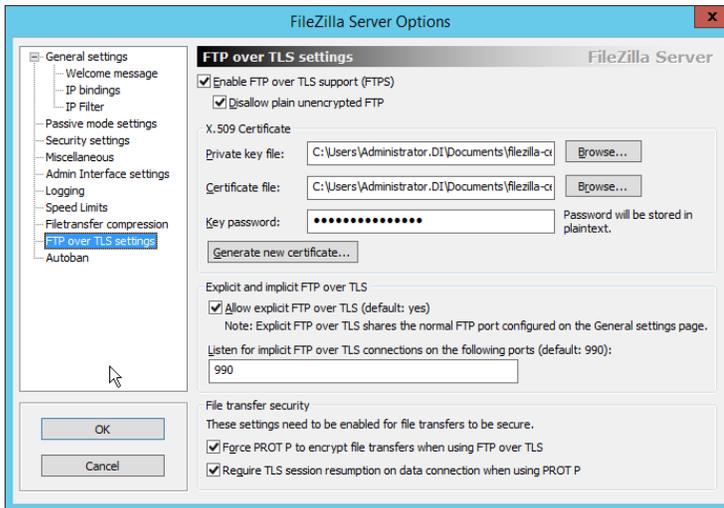
1060

1061

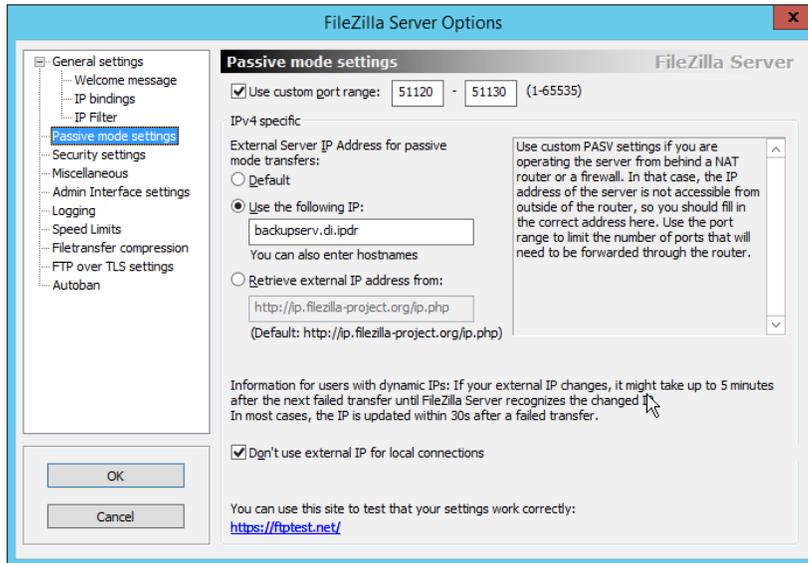
12. Click **OK**.



- 1062 13. Enter a **password** for the key.
- 1063 14. Ensure the box next to **Force PROT P to encrypt file transfers when using FTP over TLS** is
- 1064 checked.
- 1065 15. Ensure the box next to **Require TLS session resumption on data connection when using PROT P**
- 1066 is checked.



- 1067 16. Click **Passive mode settings**. Check the box next to **Use custom port range**. (This is necessary in
- 1068 cases of a local server behind Network Address Translation (NAT) or a firewall.)
- 1069 17. Enter a range of ports for passive mode to use. Ensure that these ports are allowed through the
- 1070 firewall.
- 1071 18. Select **Use the following IP**.
- 1072 19. Enter the server address.
- 1073

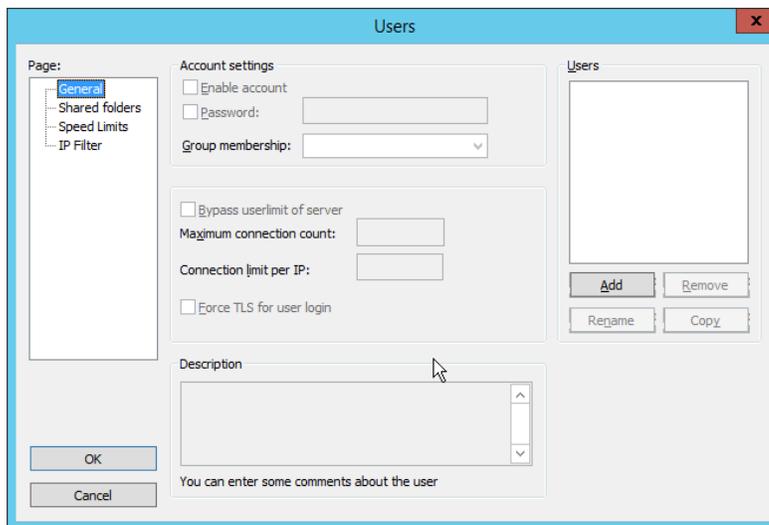


1074

1075 20. Click **OK**.

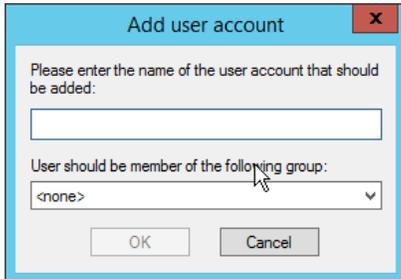
### 1076 2.8.3 Add a User to FileZilla

1077 1. In the FileZilla administrator interface, click **Edit > Users**.



1078

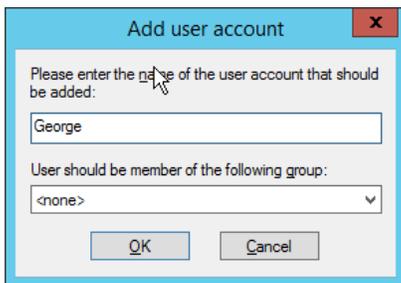
1079 2. Click **Add**.



1080

1081

3. Enter a **name** for the user.



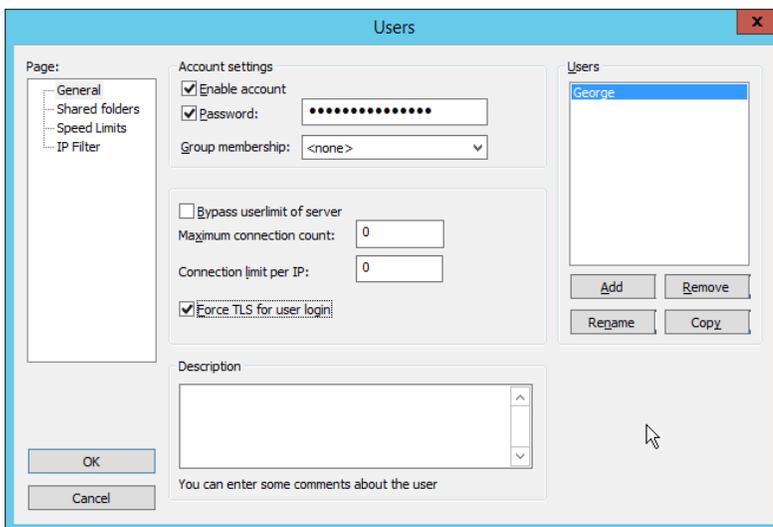
1082

1083

1084

1085

4. Click **OK**.
5. Check the box next to **Password**.
6. Enter a **password** for the user.



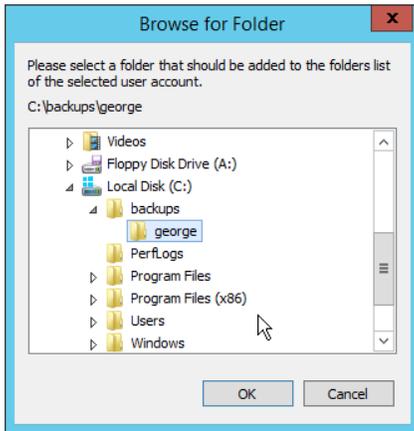
1086

1087

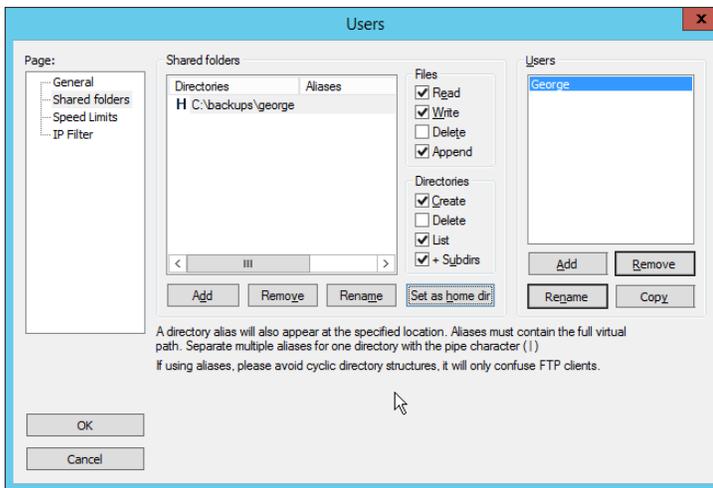
1088

1089

7. Check the box next to **Force TLS for user login**.
8. Click **Shared Folders**.
9. Click **Add**, under **Shared Folders**.



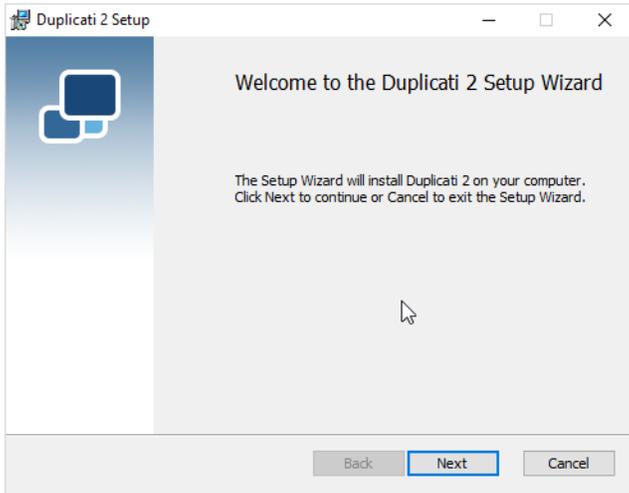
- 1090
- 1091 10. Select a place for backups *for this user* to be stored.
- 1092 11. Check the boxes next to **Write** and **Append**, under **Files**.
- 1093 12. Check the box next to **Create**, under **Directories**.
- 1094 13. Select this entry and click **Set as home dir**.



- 1095
- 1096 14. Click **OK**.

## 1097 2.8.4 Duplicati Client Installation (Windows)

- 1098 1. On the client machine, run **duplicati-2.0.3.3\_beta\_2018-04-02-x64.msi**.

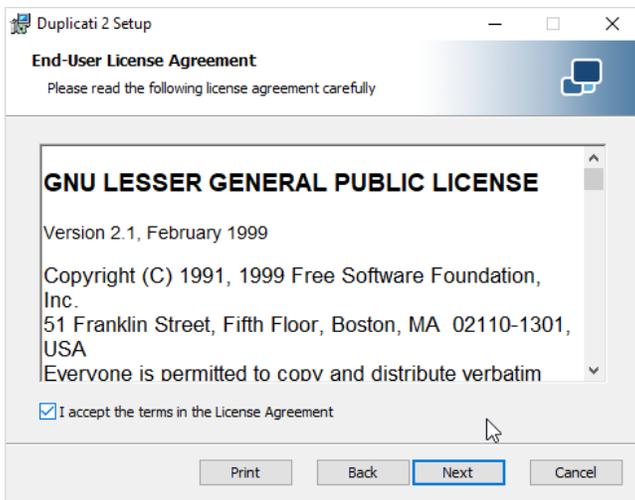


1099

1100

1101

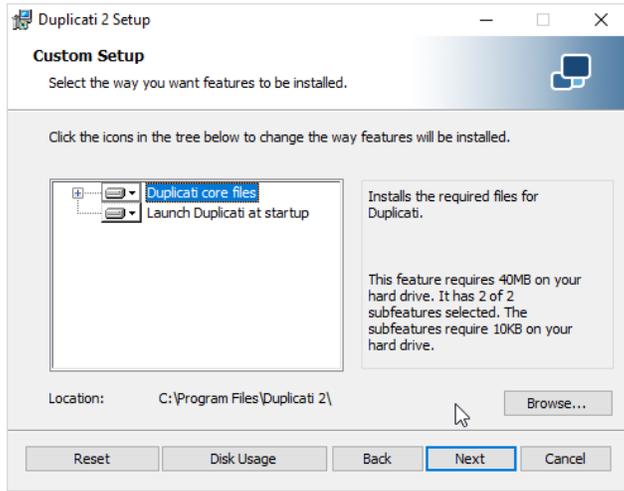
2. Click **Next**.
3. Check the box next to **I accept the terms in the License Agreement**.



1102

1103

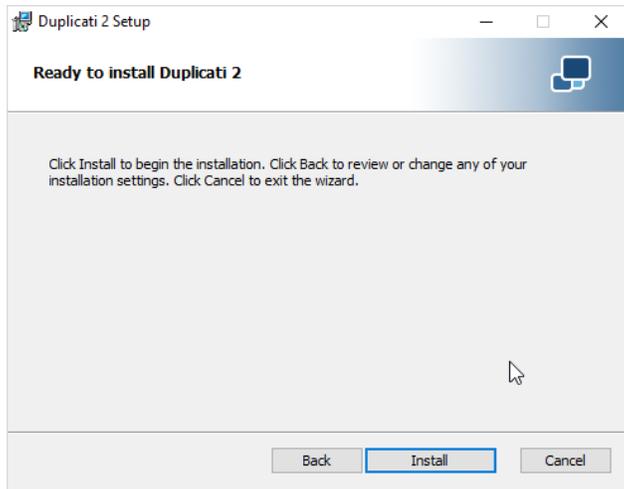
4. Click **Next**.



1104

1105

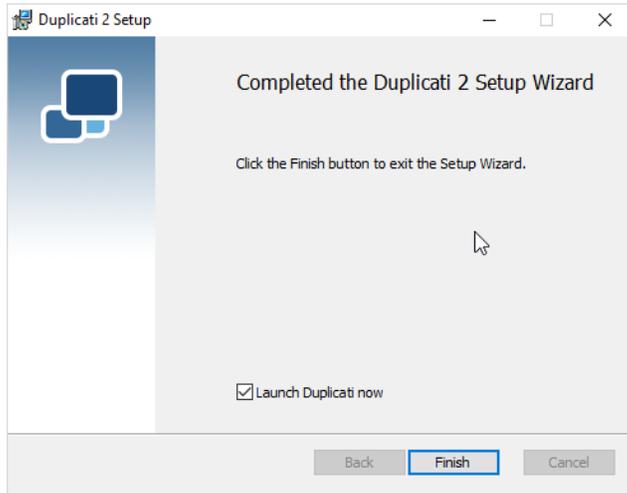
5. Click **Next**.



1106

1107

6. Click **Install**.



1108

1109

7. Click **Finish**.

1110

8. Start **Duplicati** by going to **localhost:8200**.

### 1111 2.8.5 Duplicati Client Installation (Ubuntu)

1112

1. Install mono by using the following command:

1113

1114

```
> sudo apt install mono-runtime
```

1115

1116

2. Download the Duplicati package by running the following command:

1117

1118

```
> wget
```

1119

```
https://github.com/duplicati/duplicati/releases/download/v2.0.3.9  
-2.0.3.9_canary_2018-06-30/duplicati_2.0.3.9-1_all.deb
```

1121

1122

3. Install Duplicati by using the following command:

1123

1124

```
> sudo dpkg -i duplicati_2.0.3.9-1_all.deb
```

1125

1126

4. Run Duplicati as a service by running the following command:

1127

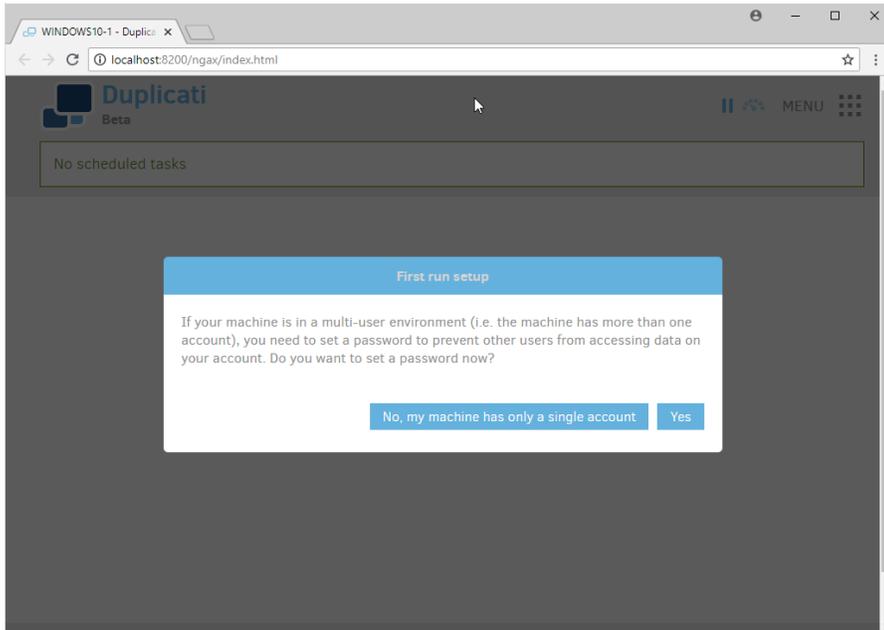
1128

```
> sudo systemctl enable duplicati
```

1129

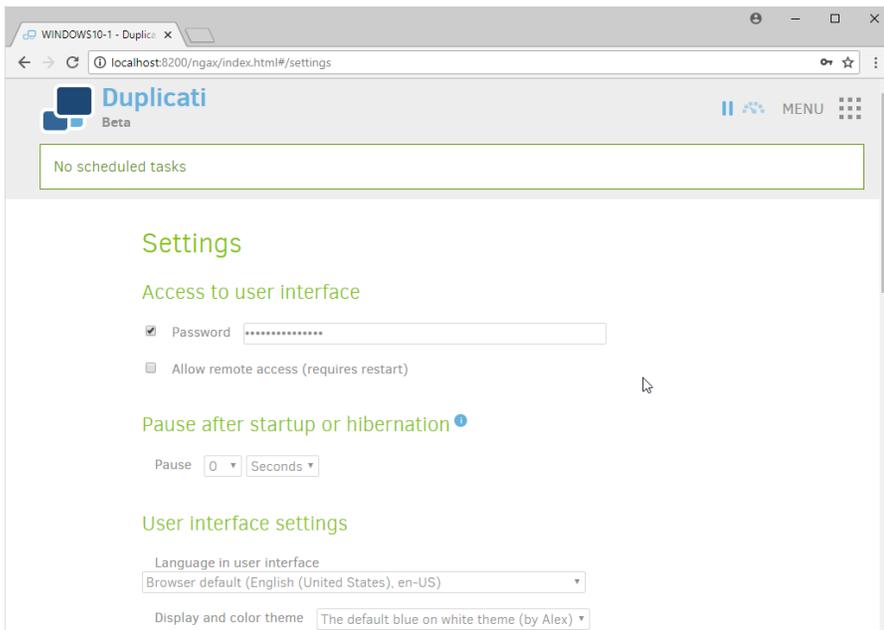
## 1130 2.8.6 Configure Duplicati

1131 1. When it first starts, **Duplicati** will have a **First run setup**.

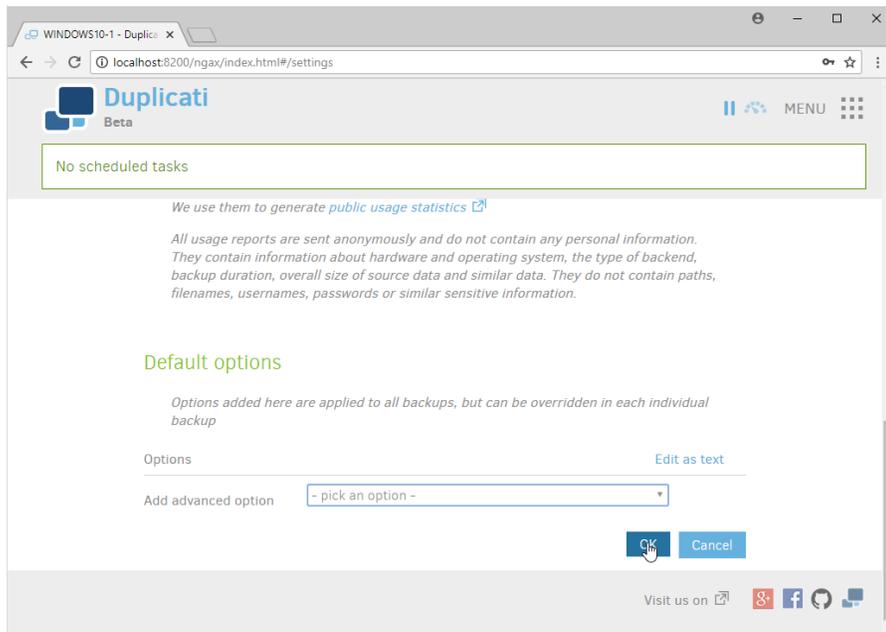


1132 2. Click **Yes**.

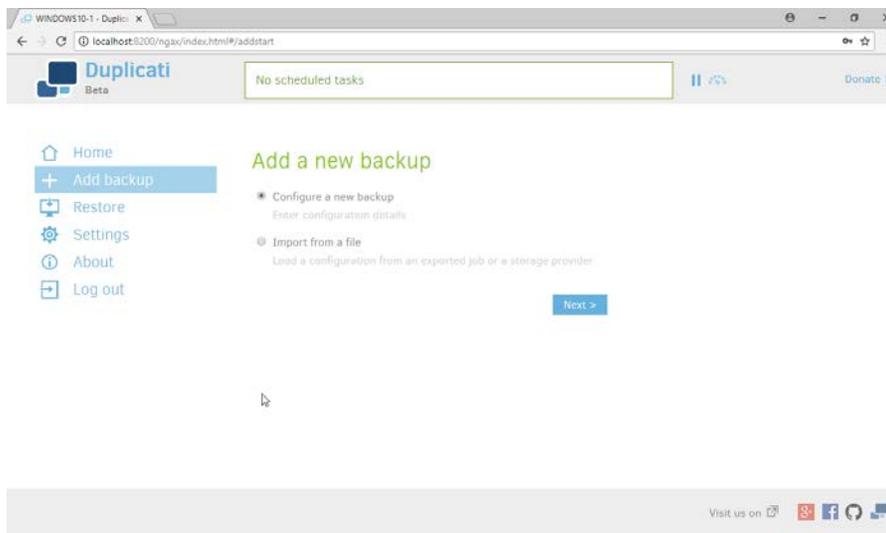
1133 3. Check the box next to **Password**.



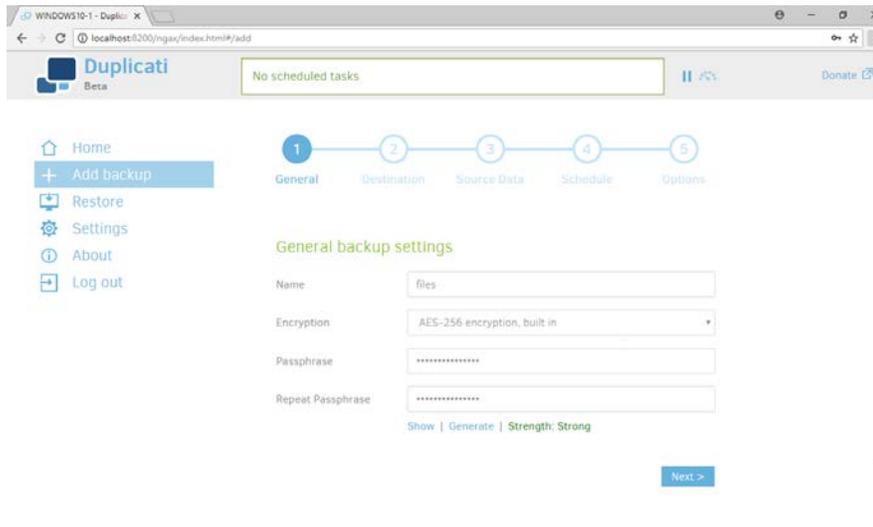
1135 4. Enter a **password**.



- 1137  
1138  
1139  
1140
5. Click **OK**.
  6. On the home page, click **Add backup**.
  7. Select **Configure a new backup**.

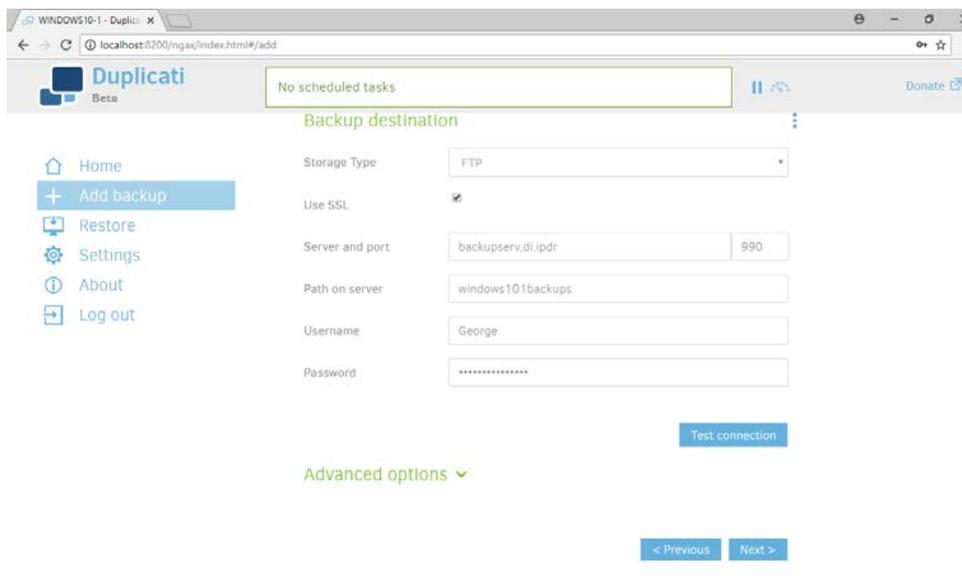


- 1141  
1142  
1143  
1144  
1145
8. Click **Next**.
  9. Enter a **name** for the backup.
  10. Select **AES-256 encryption, built in** from the drop-down menu.
  11. Enter a **password**.



1146  
1147  
1148  
1149  
1150  
1151  
1152

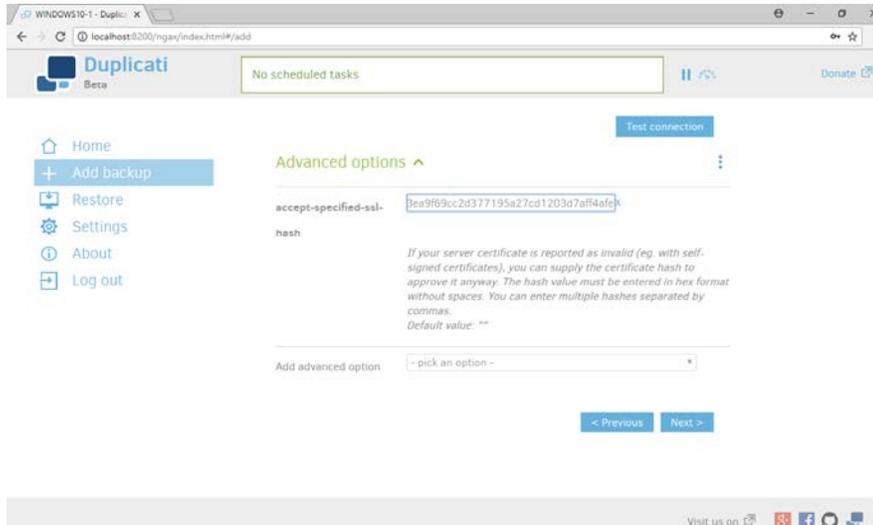
12. Click **Next**.
13. Select **FTP** for **Storage Type**.
14. Check the box next to **Use SSL**.
15. Enter the **server name** and **port** (default: 21) of the server running **FileZilla**.
16. Enter a **path** for the backup to be stored in (within the specified shared directory of the user).
17. Enter the **username** and **password** created for **FileZilla**.



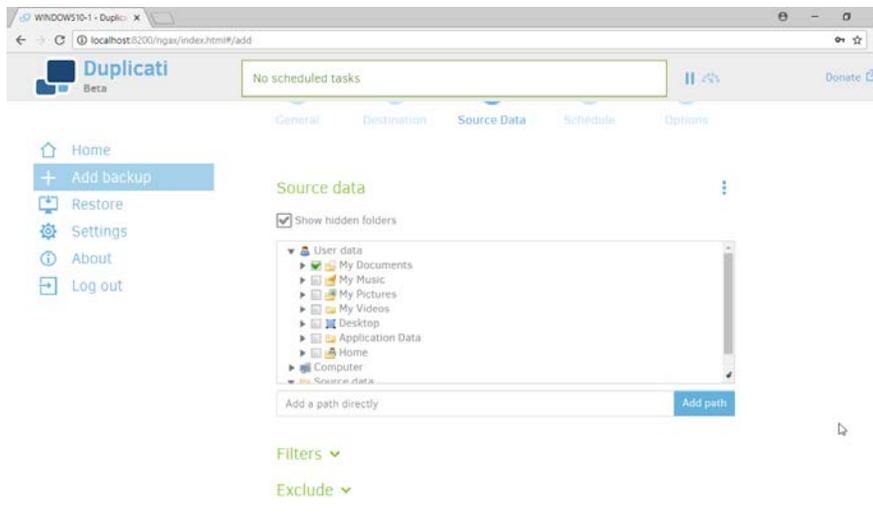
1153  
1154  
1155

18. Click **Test Connection** (if the connection fails, ensure that the port is allowed in your server's firewall).

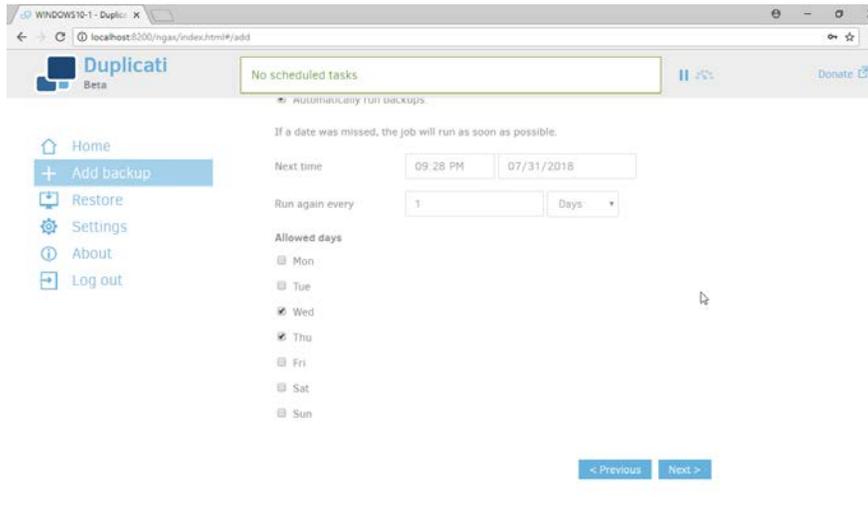
- 1156 19. If you receive an error about a certificate, you can go to **Advanced Options**, select **accept-**  
 1157 **specified-ssl-hash**, and enter the **thumbprint** from the server's certificate.



- 1158  
 1159 20. Click **Next**.  
 1160 21. Select the folders on the local machine to be backed up to the server according to your  
 1161 organization's needs.



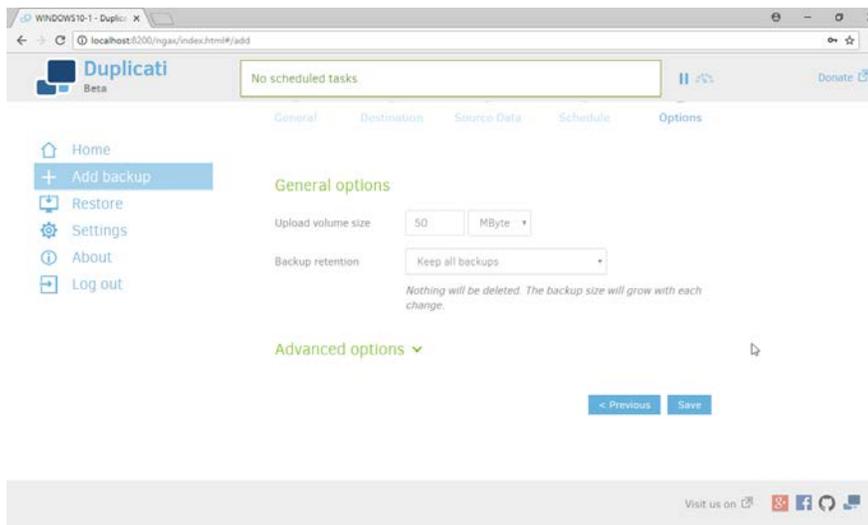
- 1162  
 1163 22. Click **Next**.  
 1164 23. Select a backup schedule according to your organization's needs.



1165

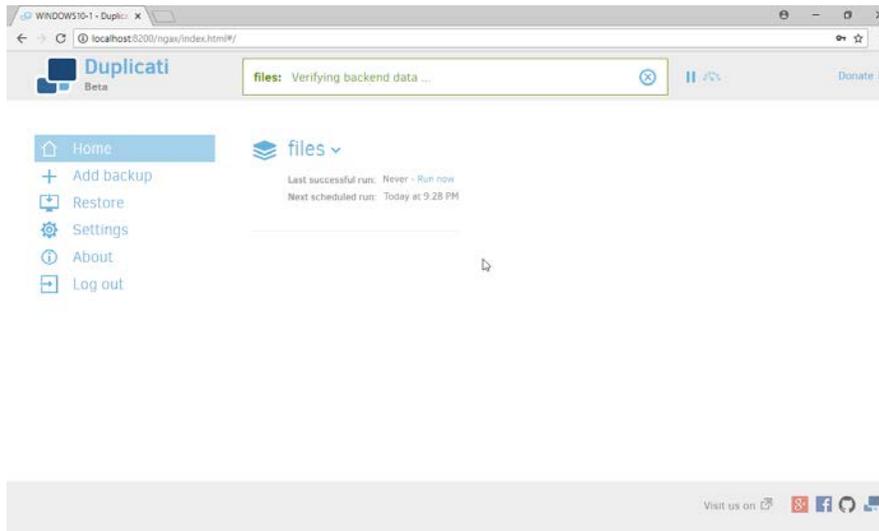
1166 24. Click **Next**.

1167 25. Select any other options according to your organization's needs.



1168

1169 26. Click **Save**.



1170

1171

27. When finished, you can choose to **Run now** to start a backup immediately.

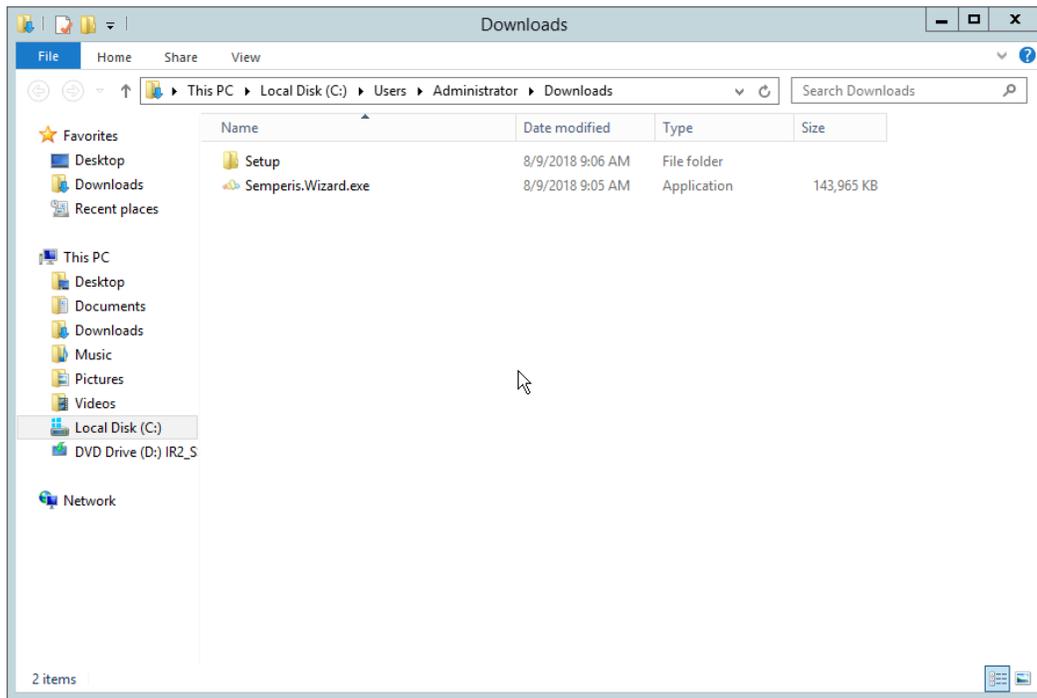
## 1172 2.9 Semperis Active Directory Forest Recovery

1173 This section details the installation of **Semperis Active Directory Forest Recovery (ADFR)**, a tool used  
 1174 for backing up and restoring Active Directory forests. This installation requires both a copy of SQL Server  
 1175 Express as well as the **Semperis Wizard**. See the **Semperis ADFR v2.5 Technical Requirements**  
 1176 document for specifics on the requirements. For a Windows Server 2012 R2 installation, simply meet  
 1177 the following requirements:

- 1178 • .NET Framework Version 3.5 SP1
- 1179 • .NET Framework Version 4.5.2 or later
- 1180 • not joined to the Active Directory domain it is protecting
- 1181 • SQL Express is not installed on the machine, but the installer SQLEXP\_x64\_ENU.exe is  
 1182 downloaded.

### 1183 2.9.1 Install Semperis ADFR

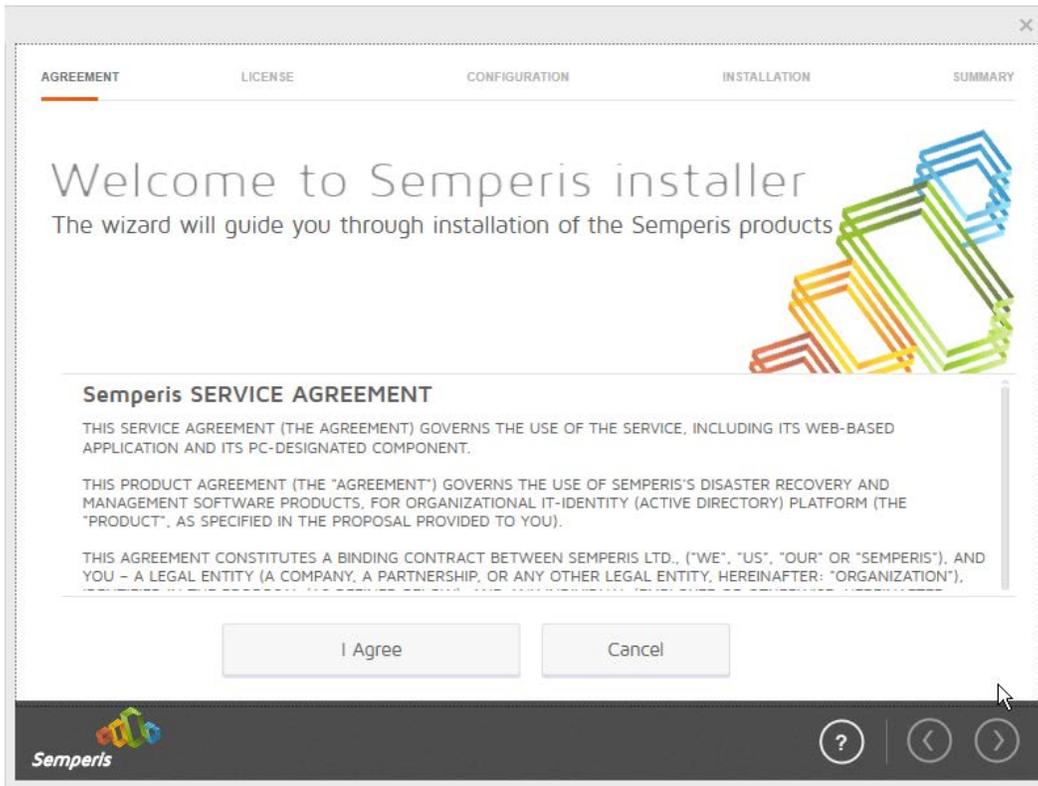
- 1184 1. Place the **SQLEXP\_x64\_ENU.exe** installer in a directory called Setup, and ensure that the  
 1185 **Semperis Wizard** is adjacent to the **Setup** folder (not inside it).



1186

1187

2. If prompted to restart the computer, do so.



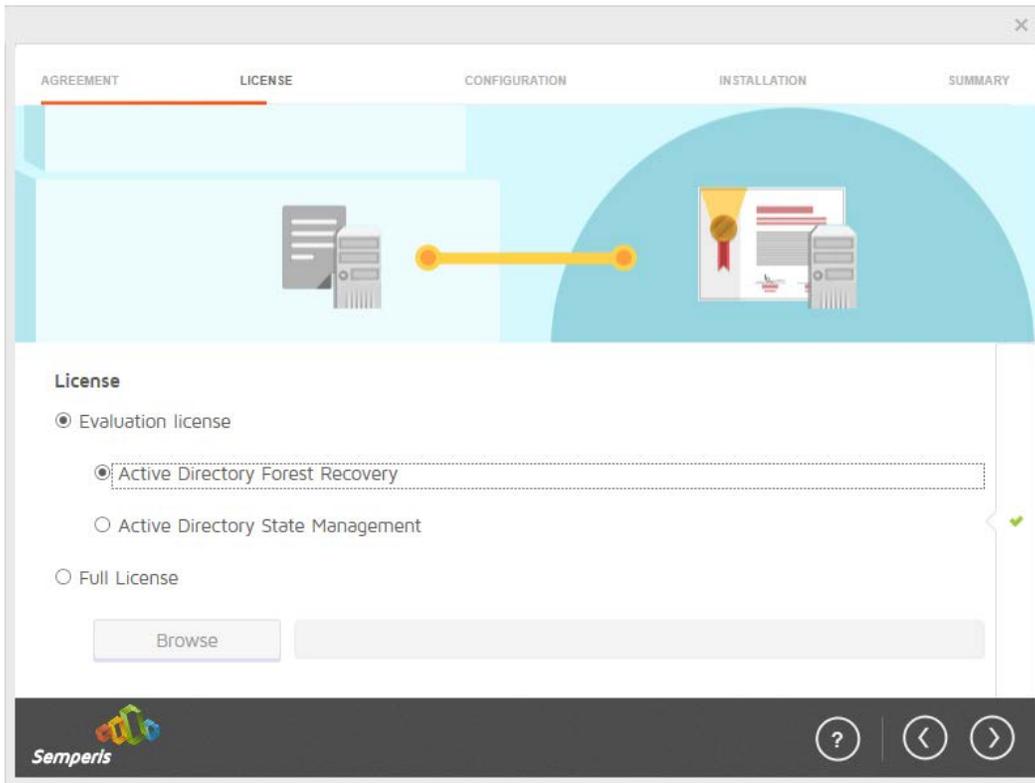
1188

1189

1190

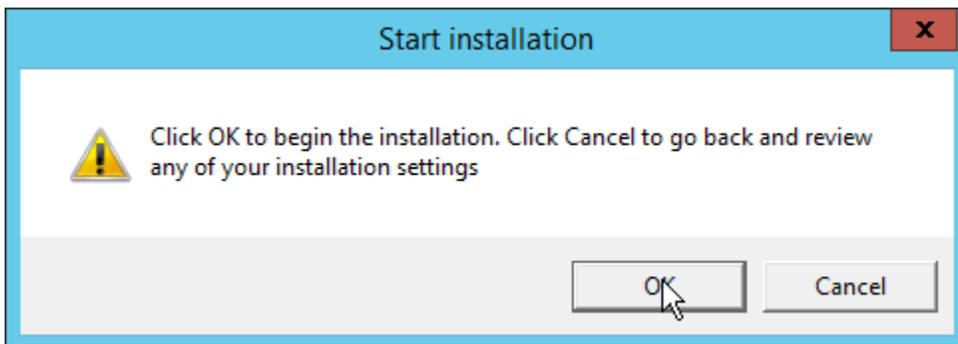
1191

3. Click **I Agree**.
4. Select **Evaluation License**.
5. Select **Active Directory Forest Recovery**.



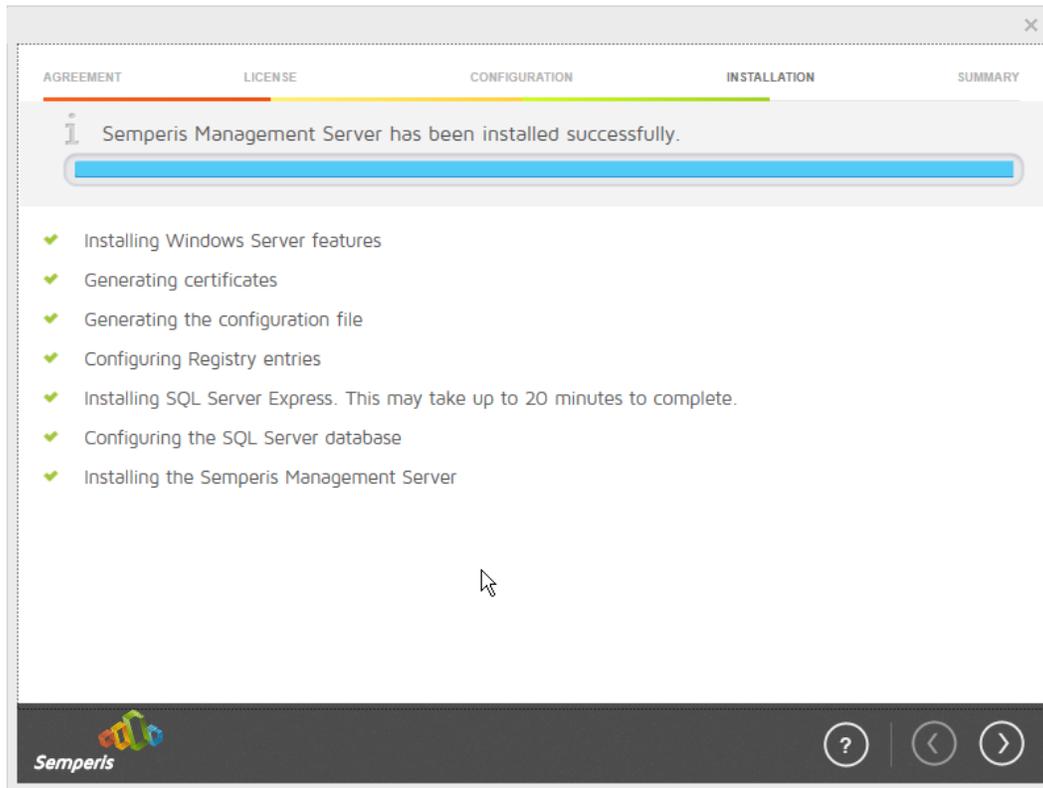
1192  
1193

6. Click the > button.



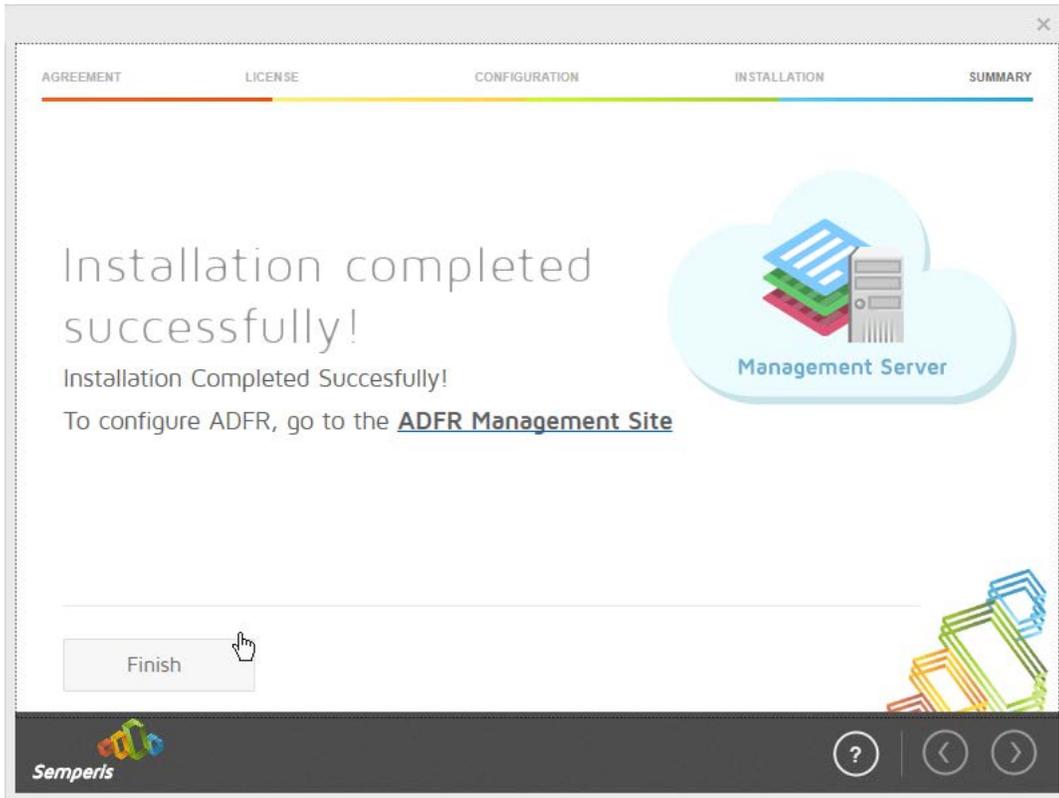
1194  
1195  
1196

7. Click **OK**.
8. Wait for the installation to complete.



1197  
1198

9. Click the > button.



1199

1200

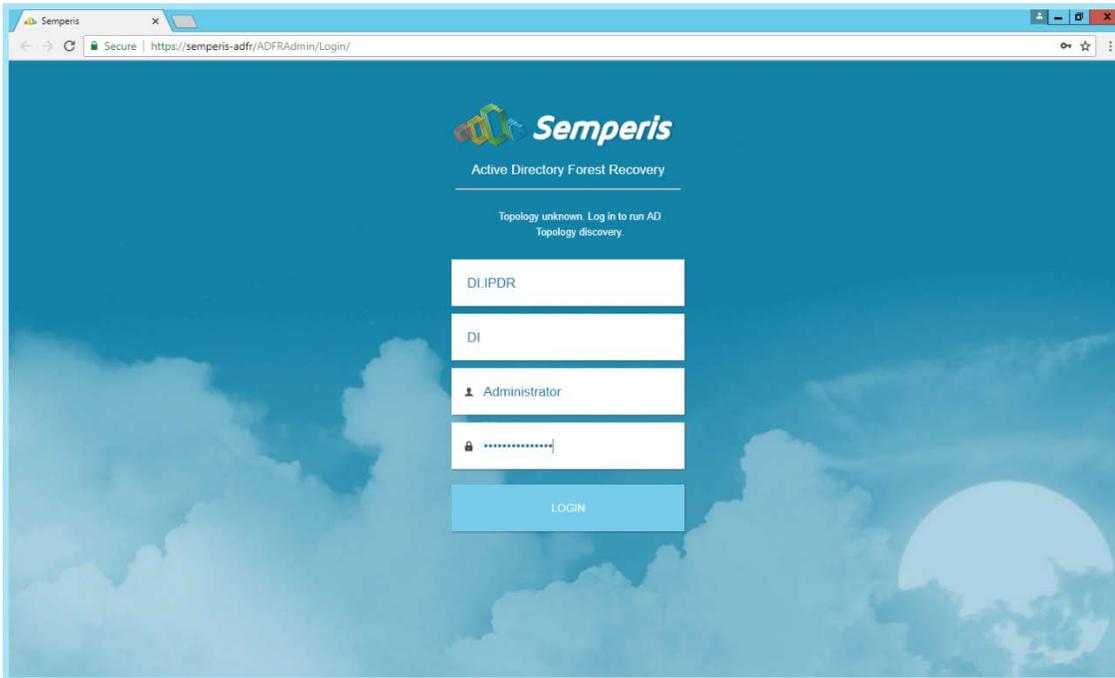
1201

1202

1203

10. Click **Finish**.
11. There should now be a shortcut on the desktop linking to the web console for **Semperis ADFR**.
12. On the login page, enter the full domain as well as the NetBIOS name.
13. Enter the **username** and **password** of an administrator on the domain.

DRAFT



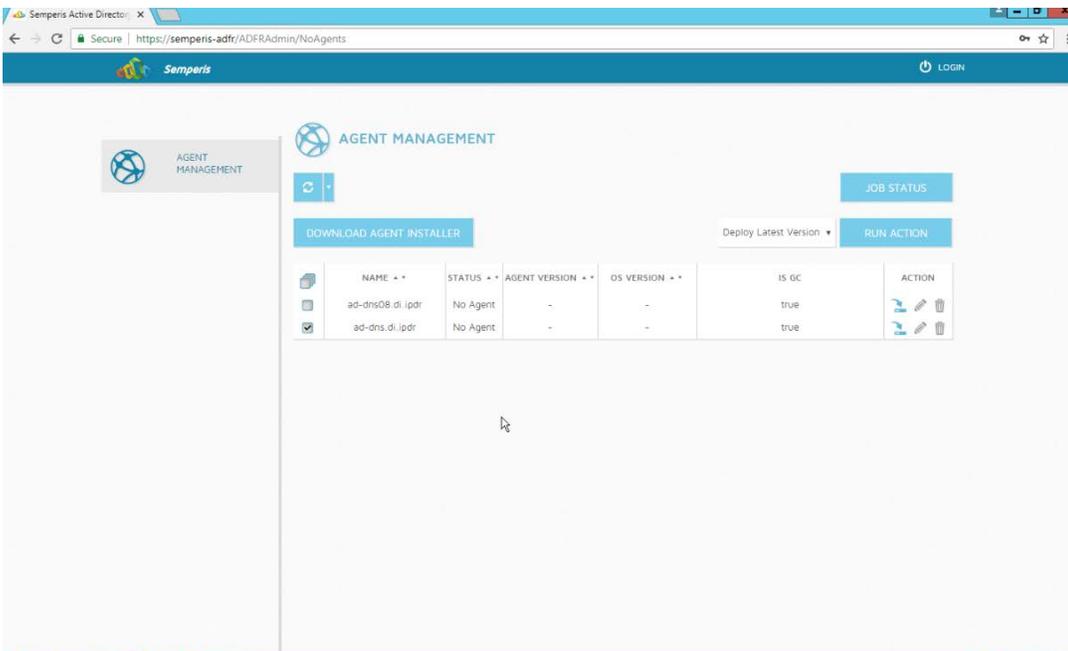
1204

1205

1206

14. Click **Login**.

15. Check the box next to any domain controllers that should be backed up.

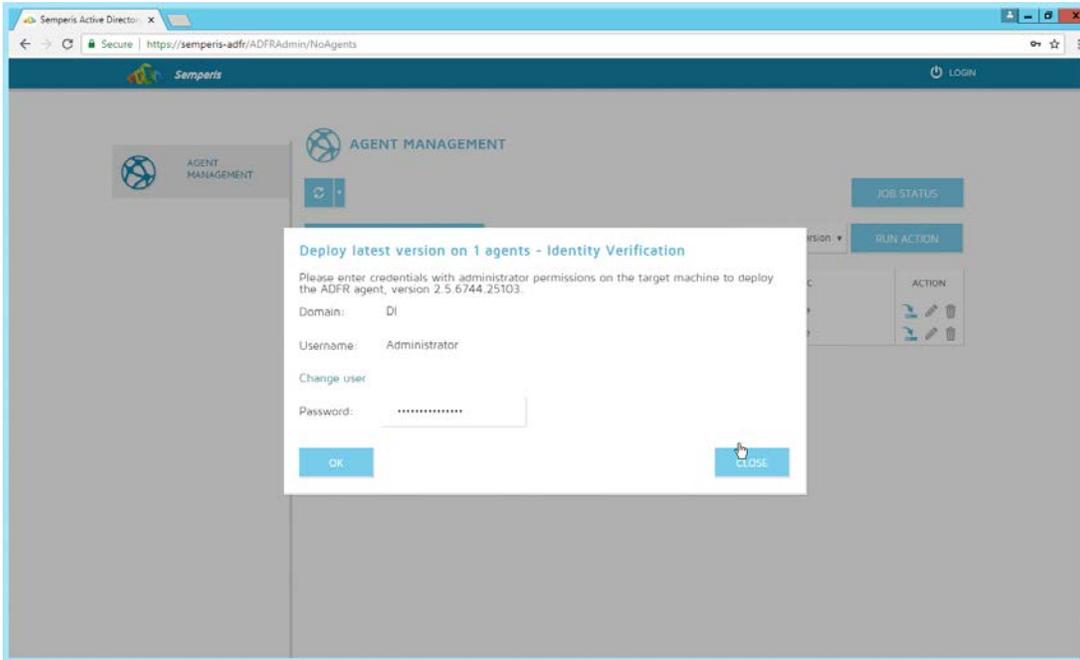


1207

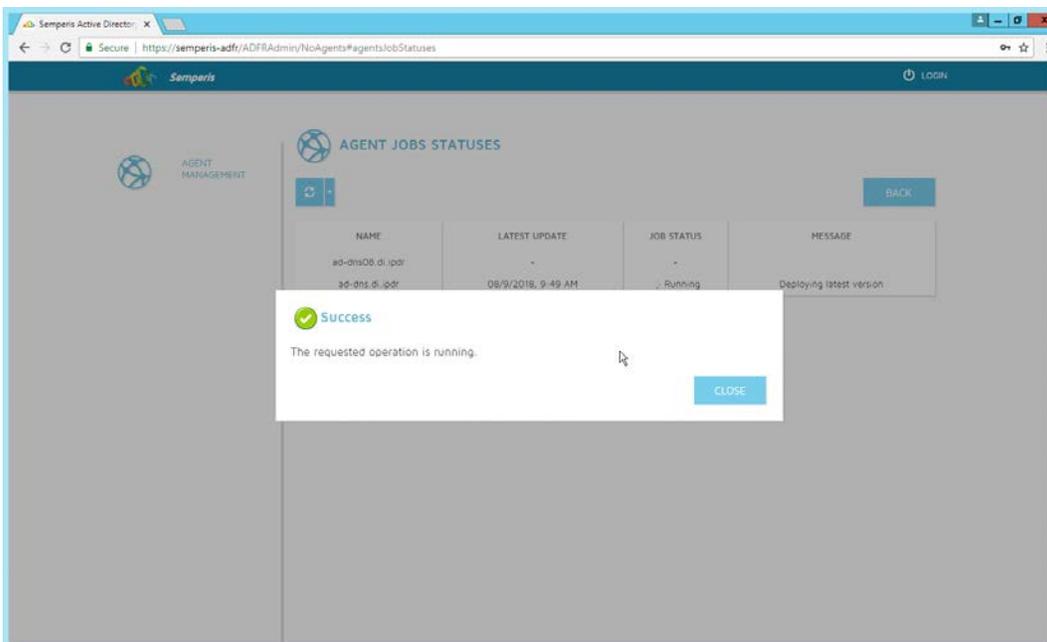
1208

16. Click **Run Action**.

1209 17. Enter the **password** in the prompt.

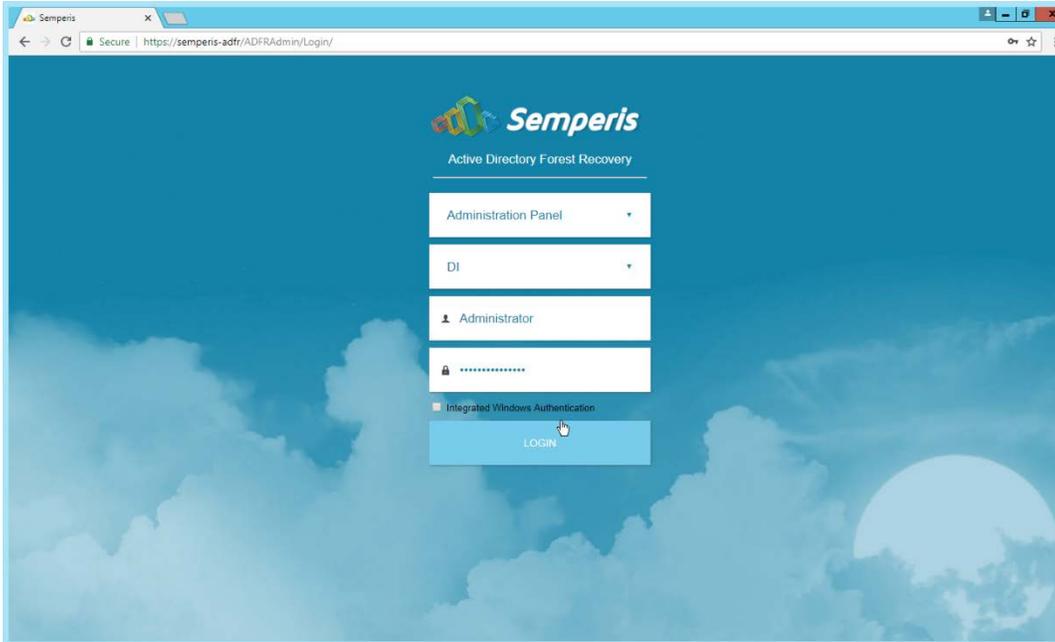


1210  
1211 18. Click **OK**.

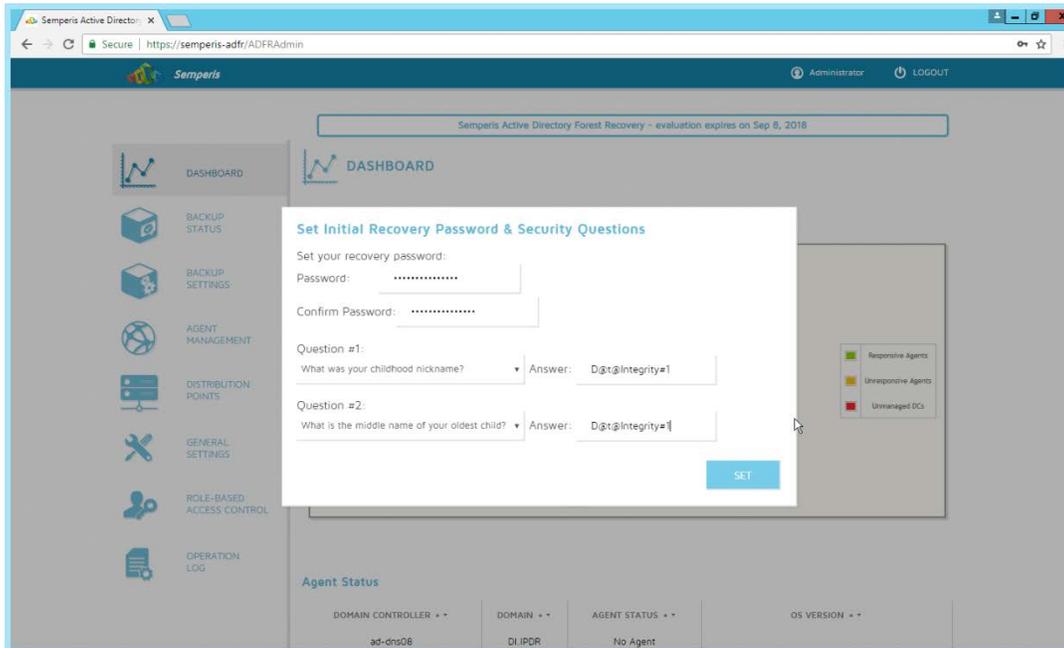


1212  
1213 19. Click **Close**.  
1214 20. After the installation finishes, click **Login** at the top of the page.

1215 21. Enter the login credentials for the domain.



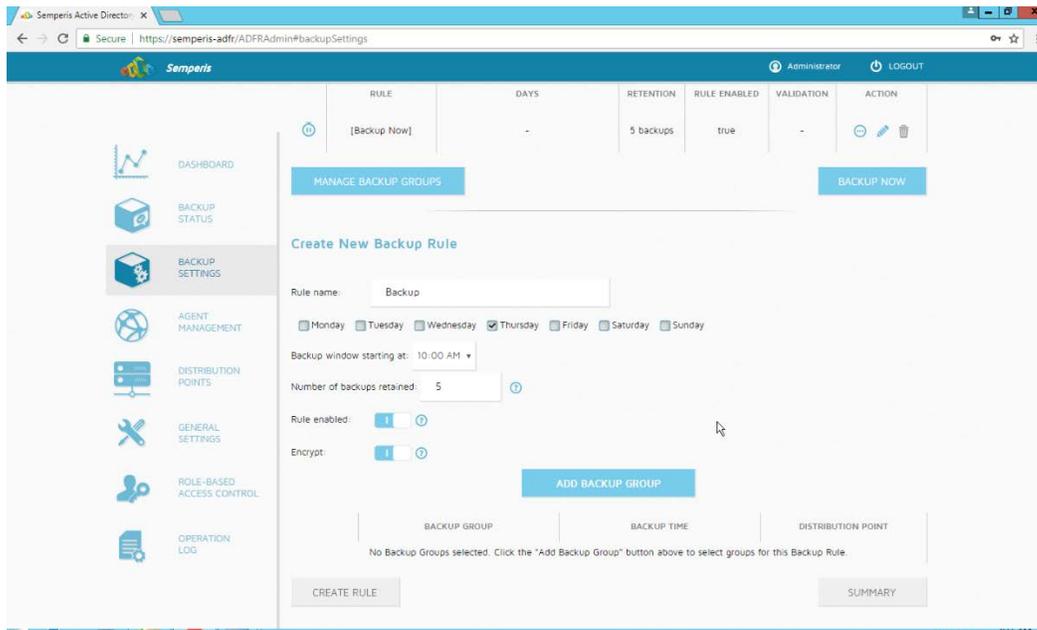
- 1216
- 1217 22. Click **Login**.
- 1218 23. Create a recovery **password**. (Note: In the event of a restoration, Active Directory will
- 1219 potentially be unavailable, so a separate password that is not domain-associated is needed here
- 1220 for restorations.)



- 1221
- 1222 24. Set recovery questions for the password.
- 1223 25. Click **Set**.

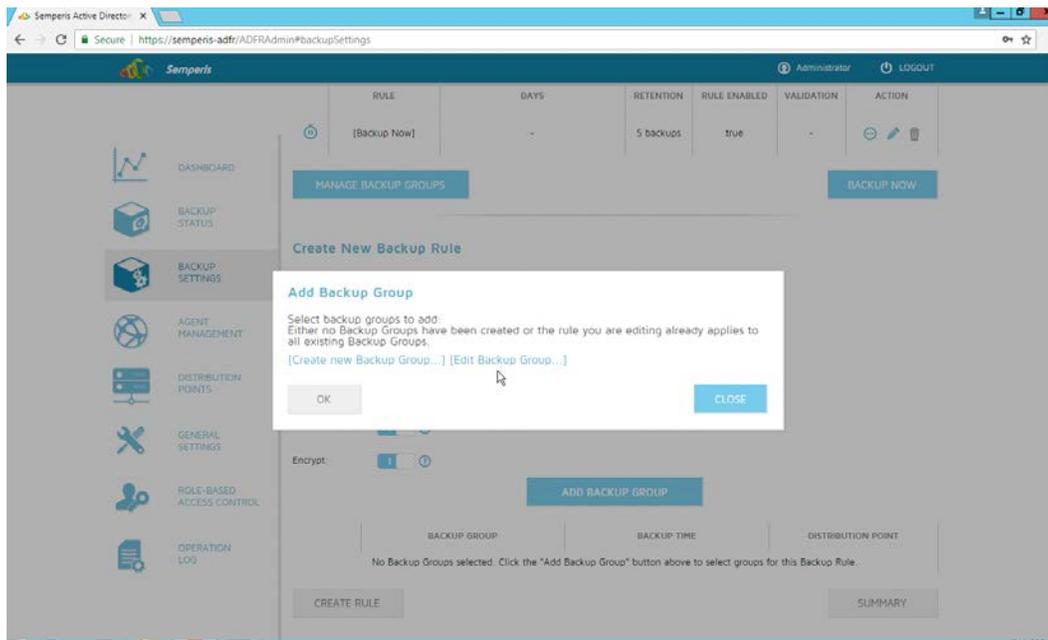
## 1224 2.9.2 Create a Backup Schedule for the Domain Controller

- 1225 1. Click the **Backup Settings** tab.
- 1226 2. Enter a **name** for the rule.
- 1227 3. Select the days and times that the domain controller should be backed up.
- 1228 4. Enter the maximum number of backups that should be kept. (Note: The oldest backup will be
- 1229 deleted upon creation of a new backup, which would exceed this maximum.)
- 1230 5. Ensure that **Encrypt** and **Rule enabled** are both turned on.



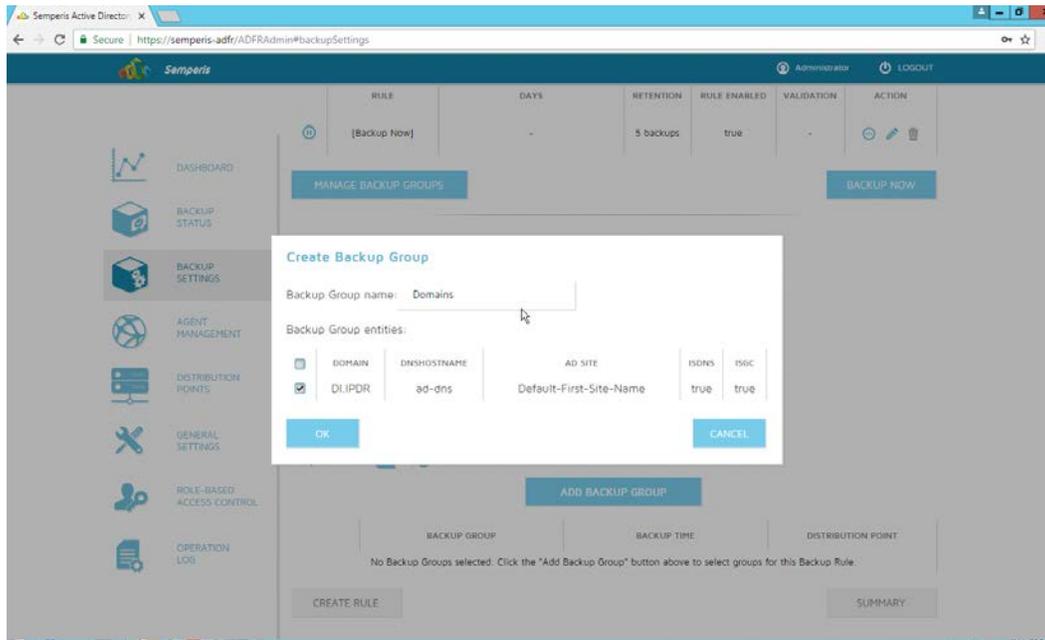
1231  
1232

6. Click **Add Backup Group**.



1233  
1234  
1235  
1236

7. Click **Create new Backup Group**.
8. Enter a **name** for the backup group.
9. Select the domain controllers to be part of the backup group.



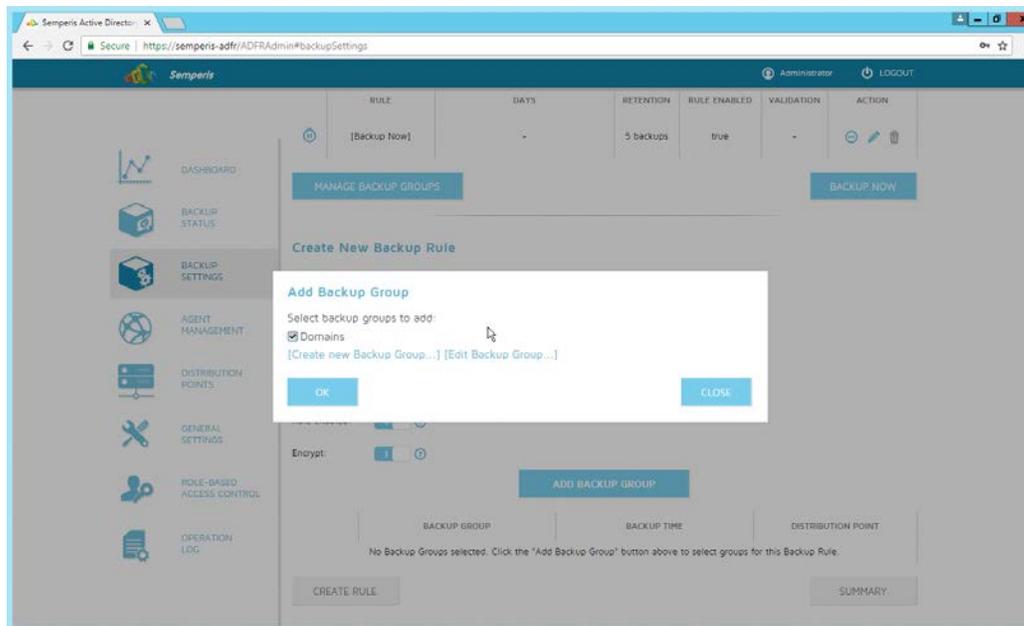
1237

1238

1239

10. Click **OK**.

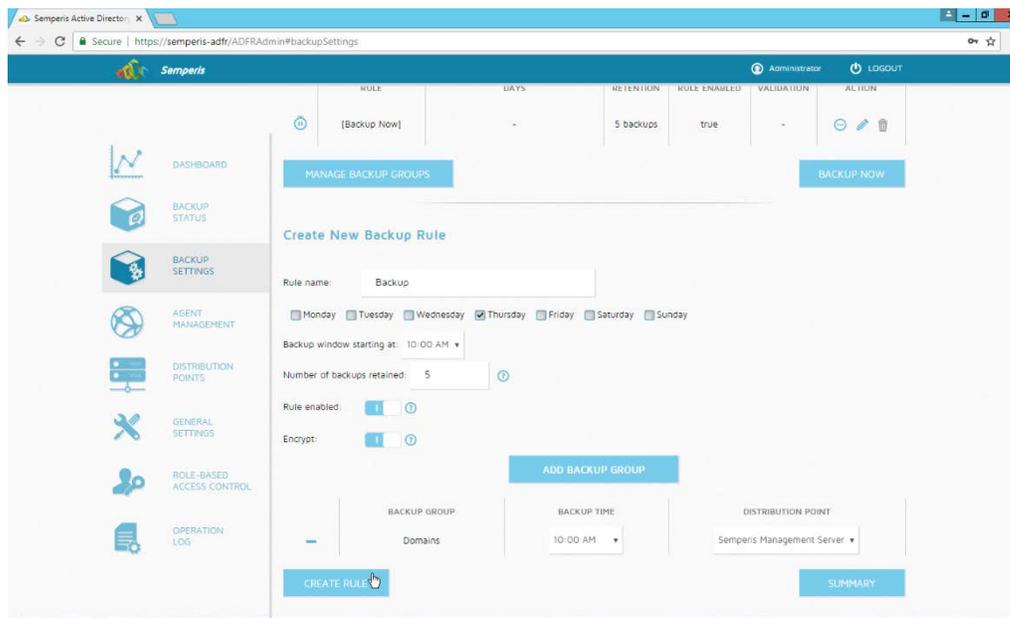
11. Select the newly created backup group.



1240

1241

12. Click **OK**.



1242

1243

13. Click **Create Rule**.

### 1244 2.9.3 Recover the Active Directory Forest from a Backup

1245

1. Open the **Semperis ADFR** web console.

1246

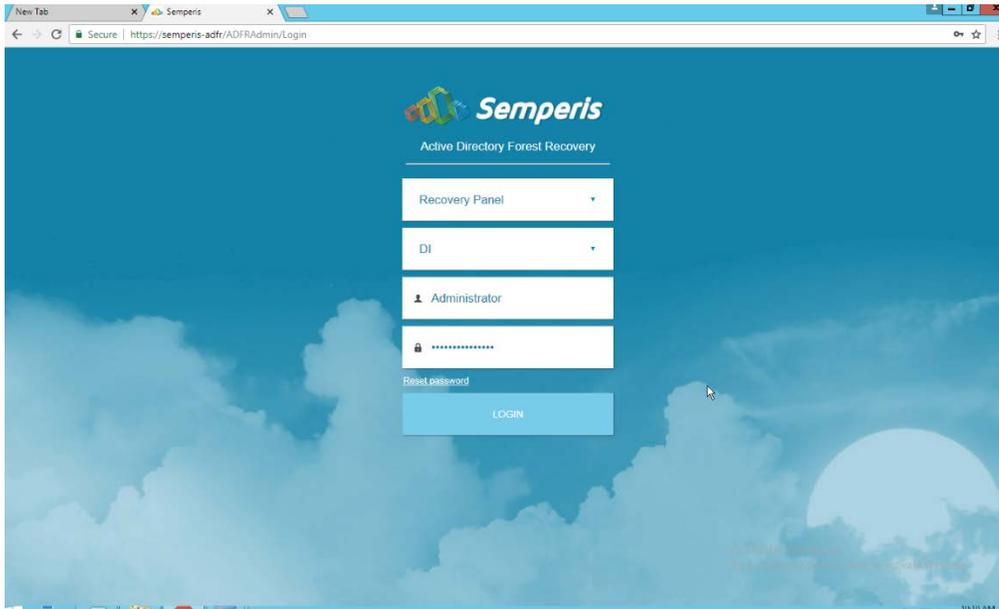
2. Select **Recovery Panel** from the drop-down.

1247

3. Select the **Domain** that you wish to recover.

1248

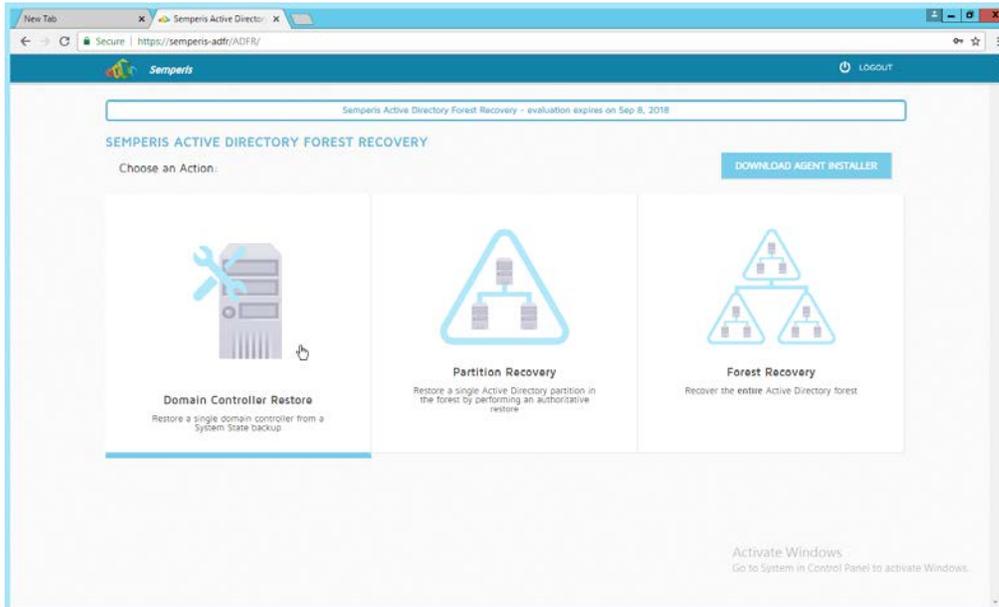
4. Enter the **username** and **password**.



1249

1250

5. Click **Login**.



1251

1252

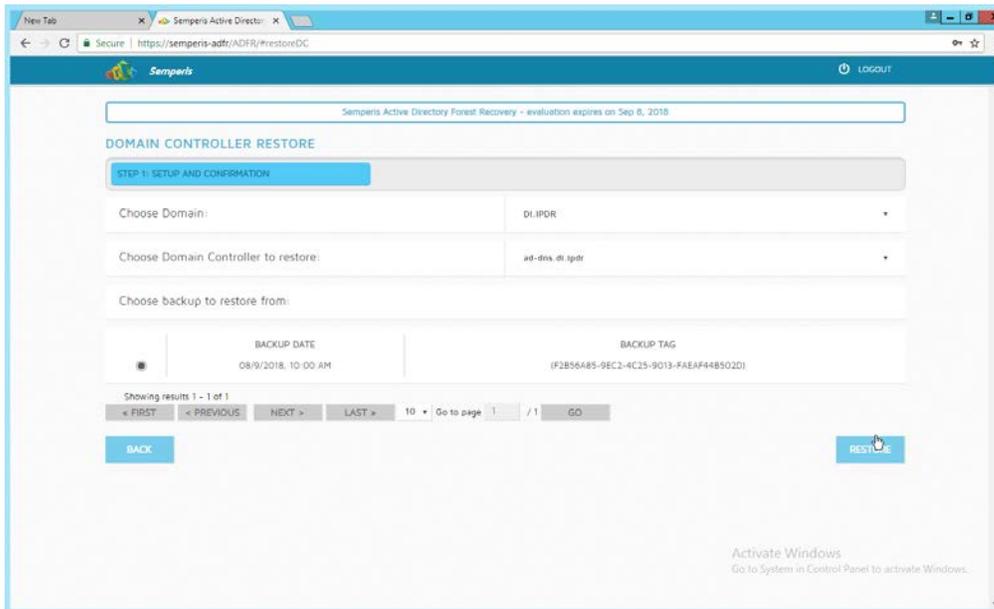
1253

1254

1255

1256

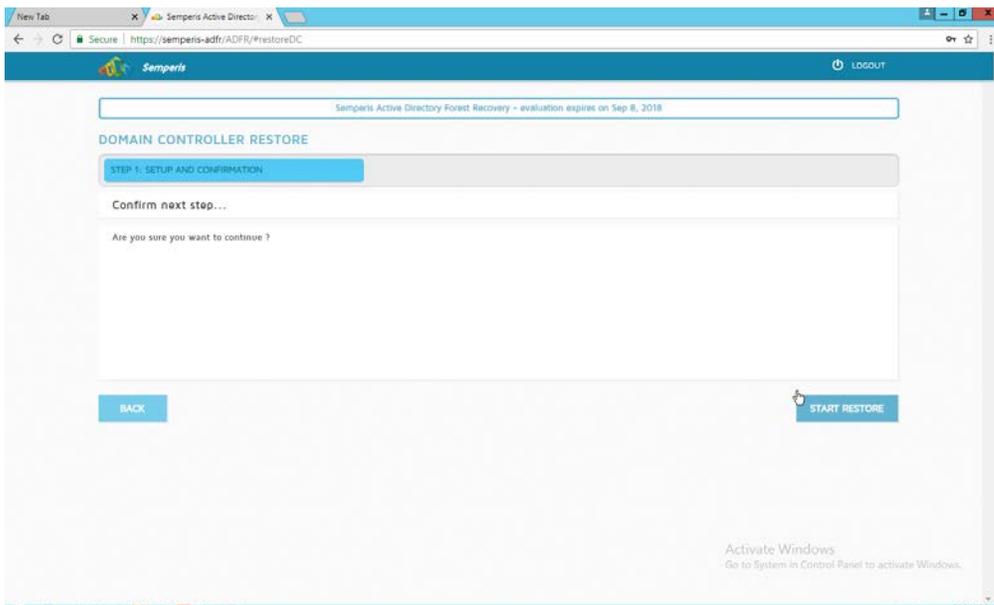
6. Select an action based on the recovery needs of the organization. In this example we select **Domain Controller Restore**.
7. Provide the information for the restoration, namely the **domain**, the **domain controller**, and which backup to use.



1257

1258

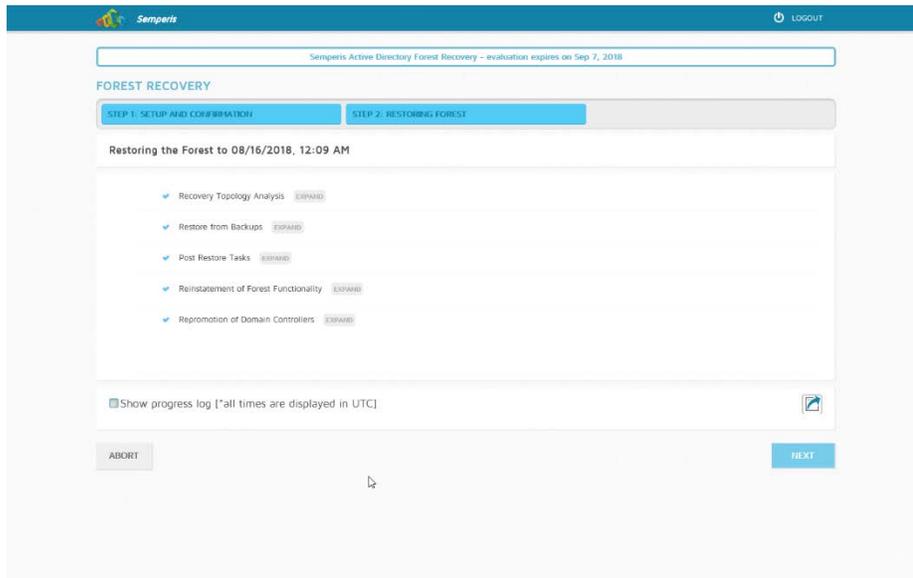
8. Click **Restore**.



1259

1260

9. Click **Start Restore** to begin the restoration process.



1261

1262 10. Click **Next** when the restoration finishes.1263 

## 2.10 Semperis Directory Services Protector

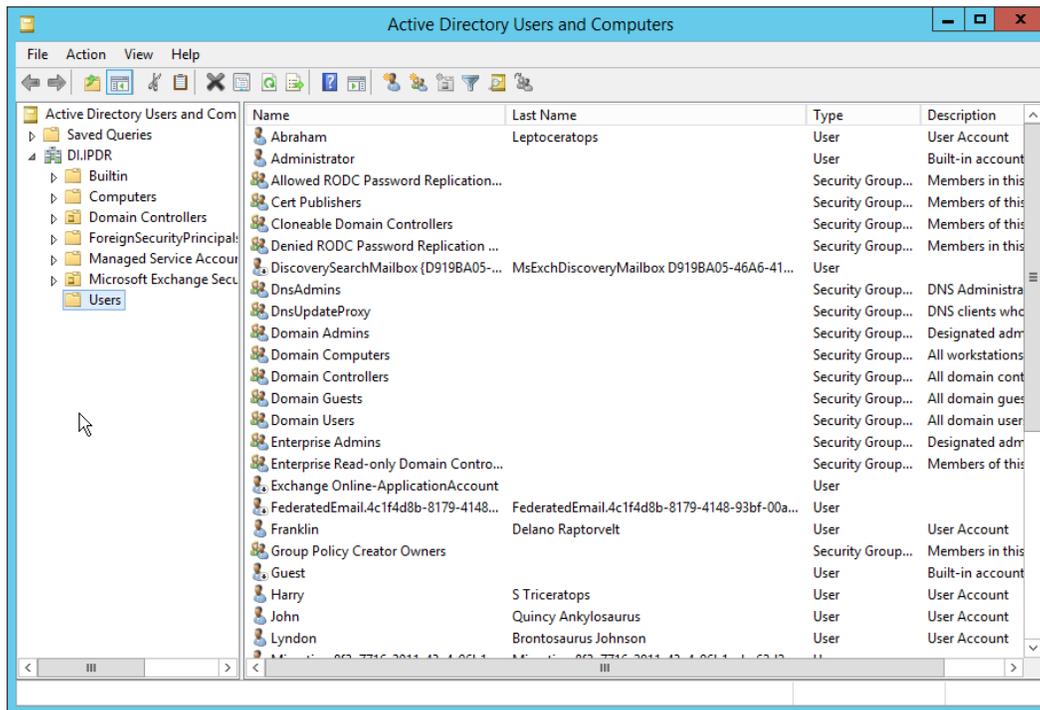
1264 This section details the installation of **Semperis Directory Services Protector (DSP)**, a tool used for  
 1265 monitoring Active Directory environments. This installation requires both a copy of SQL Server Express  
 1266 as well as the **Semperis Wizard**. See the **Semperis DS Protector v2.5 Technical Requirements** document  
 1267 for specifics on the requirements. For a Windows Server 2012 R2 installation, simply meet the following  
 1268 requirements:

- 1269 • .NET Framework Version 3.5 SP1
- 1270 • .NET Framework Version 4.5.2 or later
- 1271 • joined to the Active Directory domain it is protecting
- 1272 • either the installer for SQL Express Advanced or connection information and credentials for a  
 1273 full version of Microsoft SQL (MSSQL)

1274 

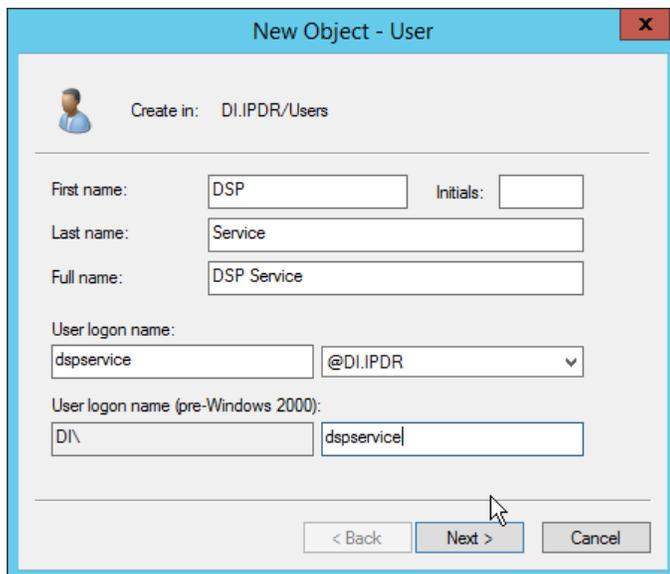
### 2.10.1 Configure Active Directory for Semperis DSP

- 1275 1. Open **Active Directory Users and Computers**.



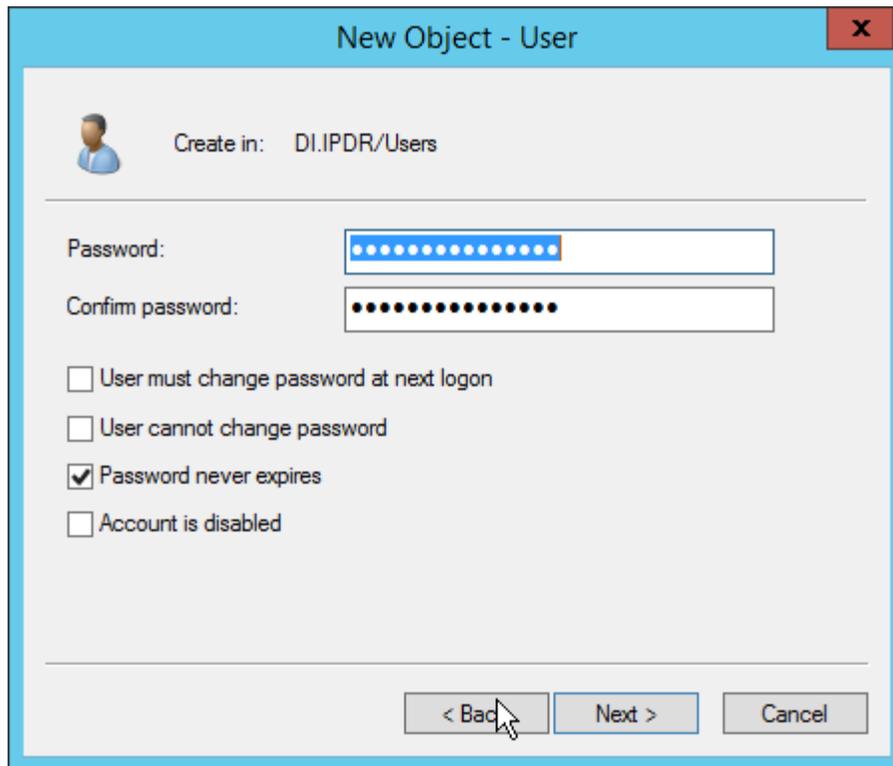
1276  
1277  
1278

2. Right-click **Users** in the left pane and select **New > User**.
3. Enter the information for a new user for the DSP service.



1279  
1280  
1281  
1282

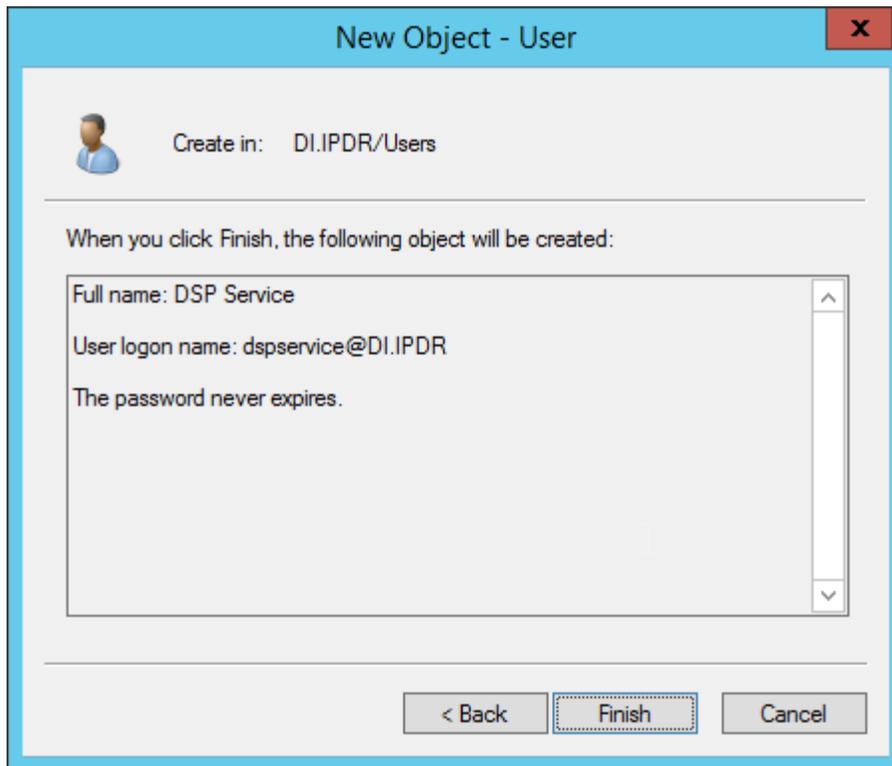
4. Click **Next**.
5. Enter a **password** twice for this user.
6. Set the password policy.



1283

1284

7. Click **Next**.

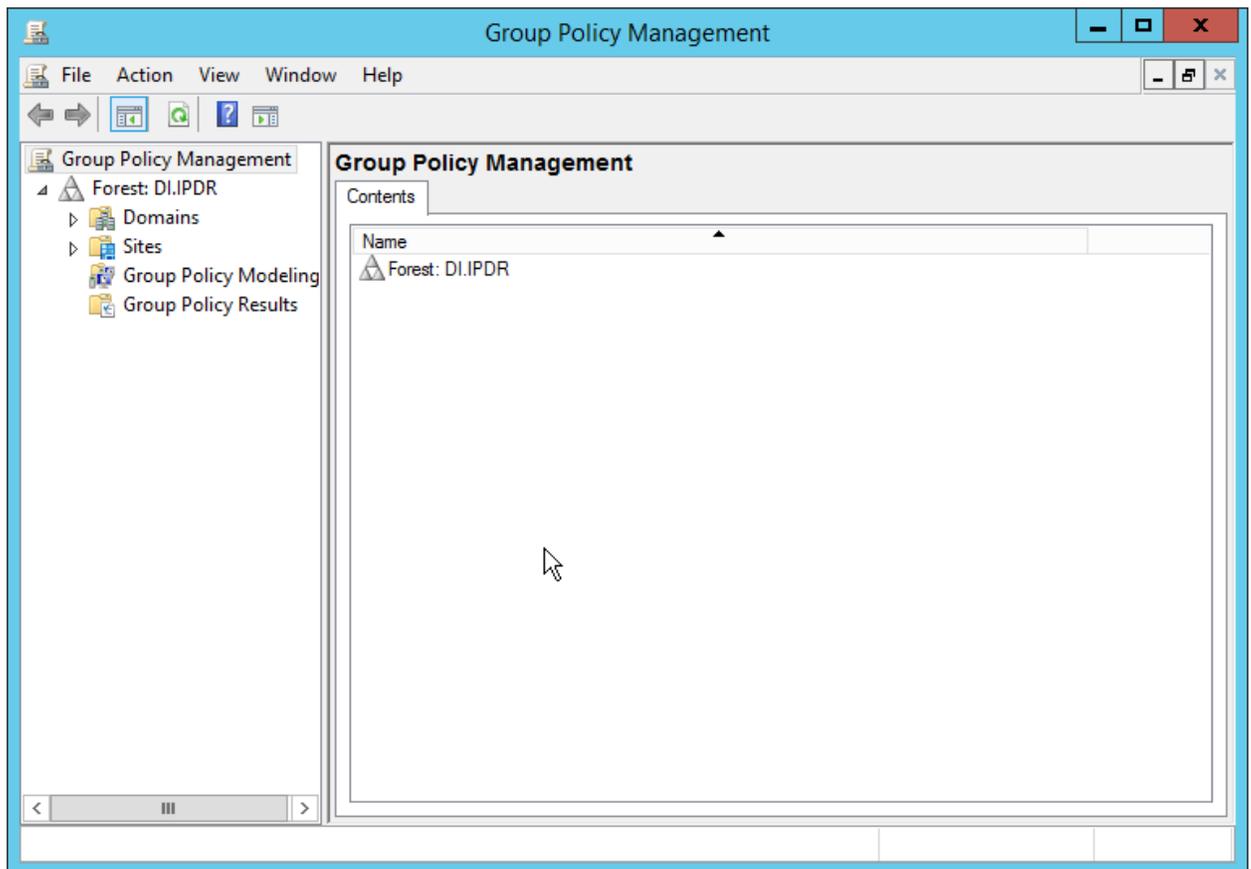


1285

1286

1287

8. Click **Finish**.
9. Open **Group Policy Management**.

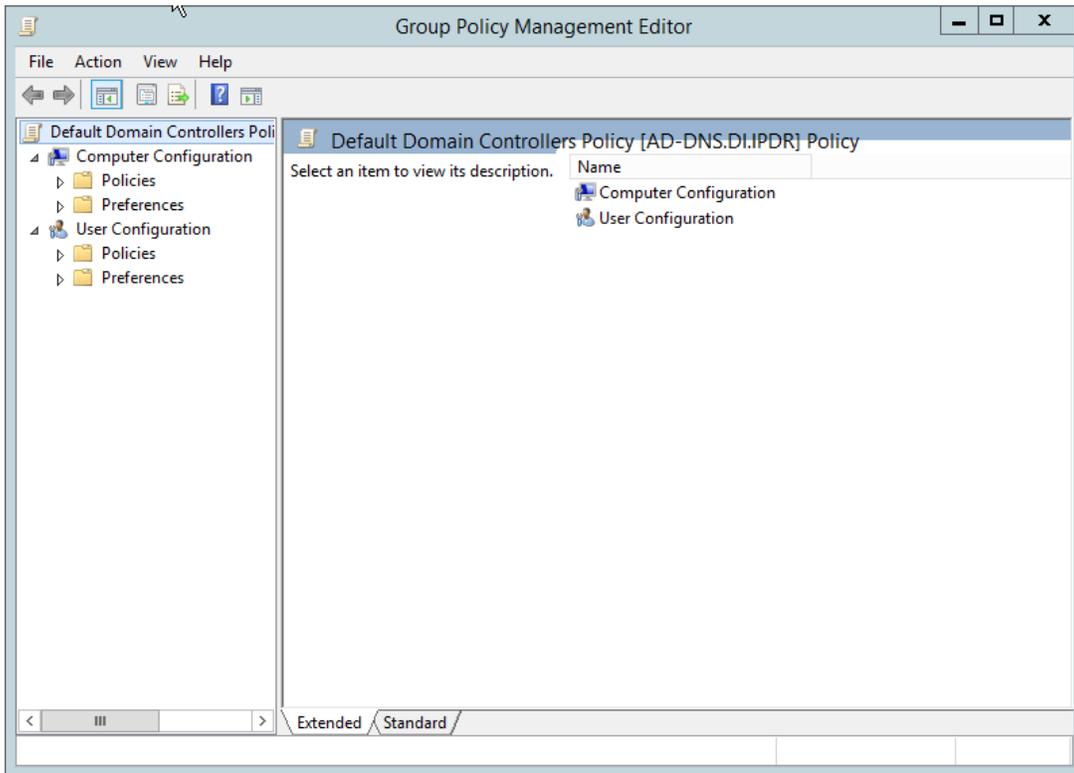


1288

1289

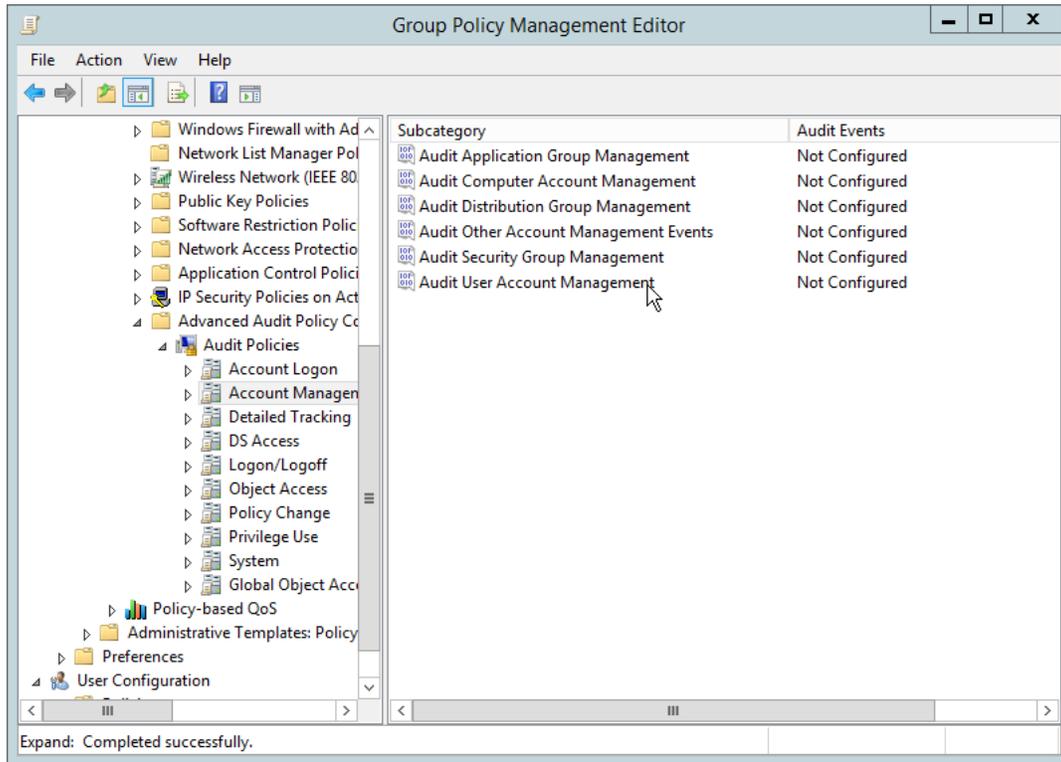
1290

10. Right-click **Domains > DI.IPDR > Domain Controllers > Default Domain Controllers Policy** and click **Edit**.



1291  
1292  
1293

11. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management.**



1294

1295

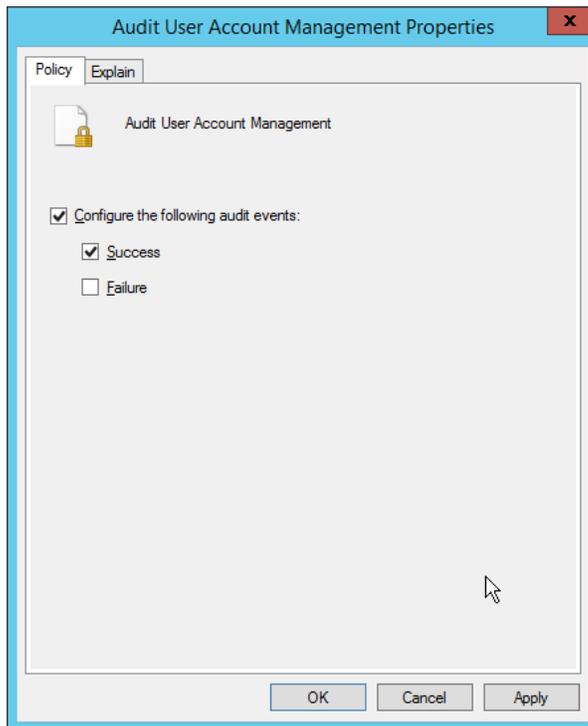
12. Edit the **Audit User Account Management** field by double-clicking it.

1296

13. Check the box next to **Configure the following audit events**.

1297

14. Check the box next to **Success**.



1298

1299

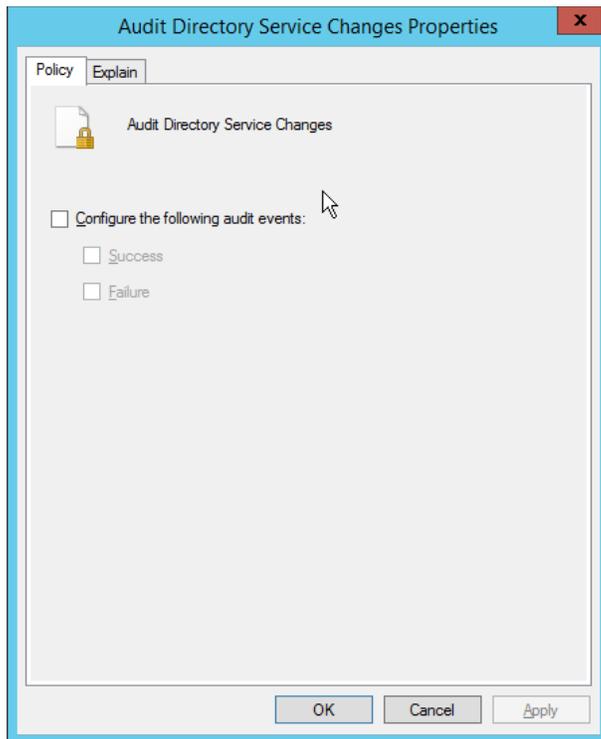
1300

1301

15. Click **OK**.

16. Go to **Audit Policies > DS Access**.

17. Double-click **Audit Directory Service Changes**.



1302

1303

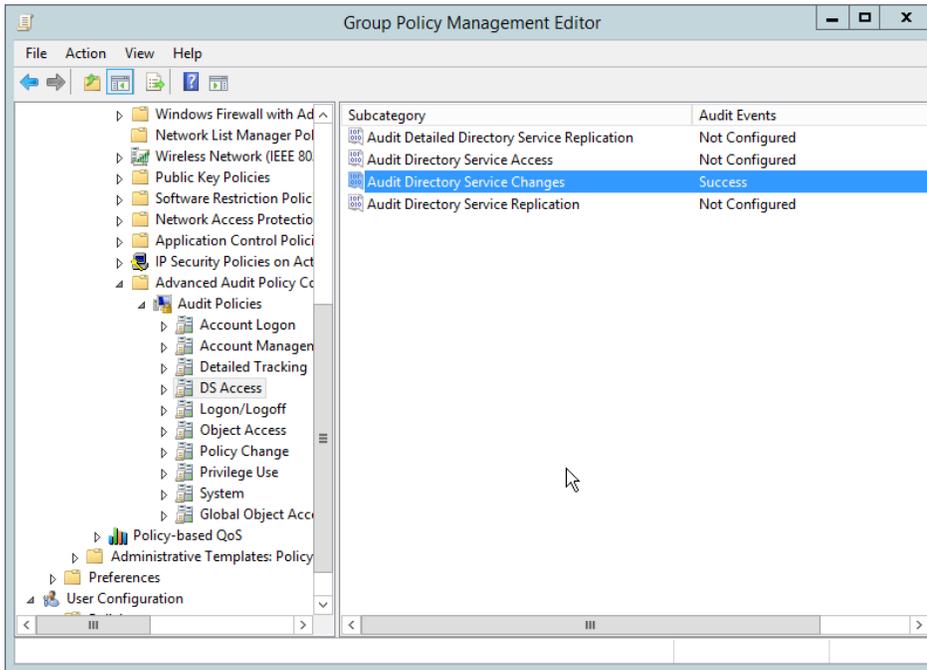
1304

1305

18. Check the box next to **Configure the following audit events.**

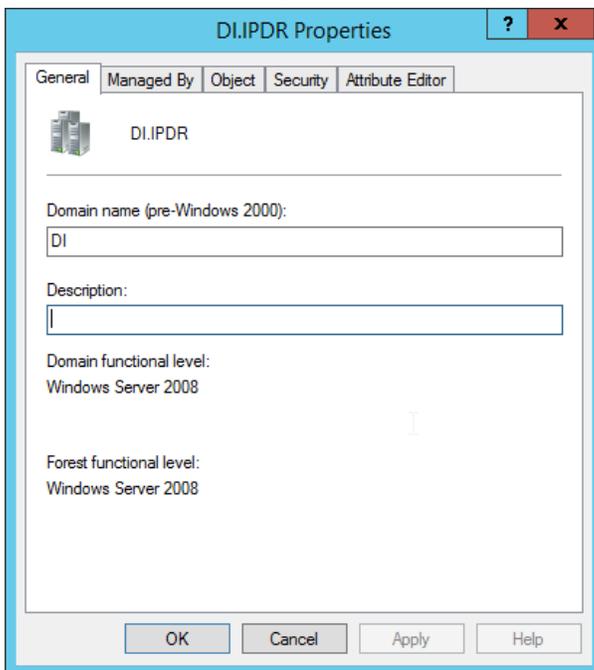
19. Check the box next to **Success.**

20. Click **OK.**



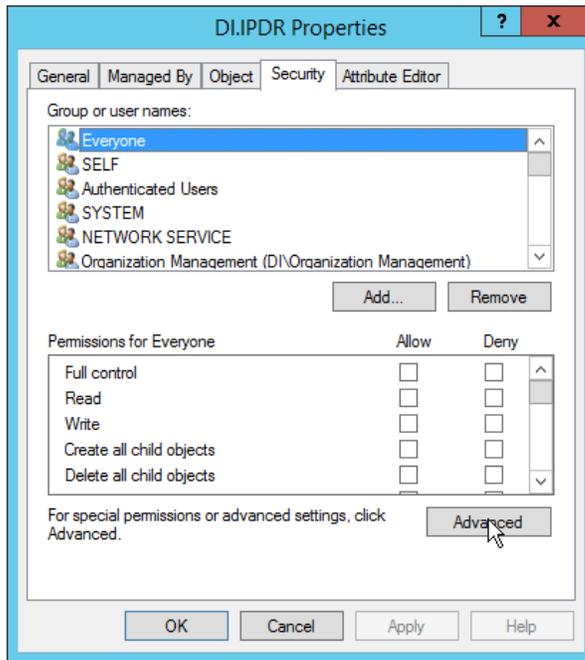
1306  
1307  
1308  
1309

21. Open **Active Directory Users and Computers**.
22. Ensure that **View > Advanced Features** is enabled.
23. Right-click the **domain** (for example, DI.IPDR) created earlier and click **Properties**.



1310  
1311

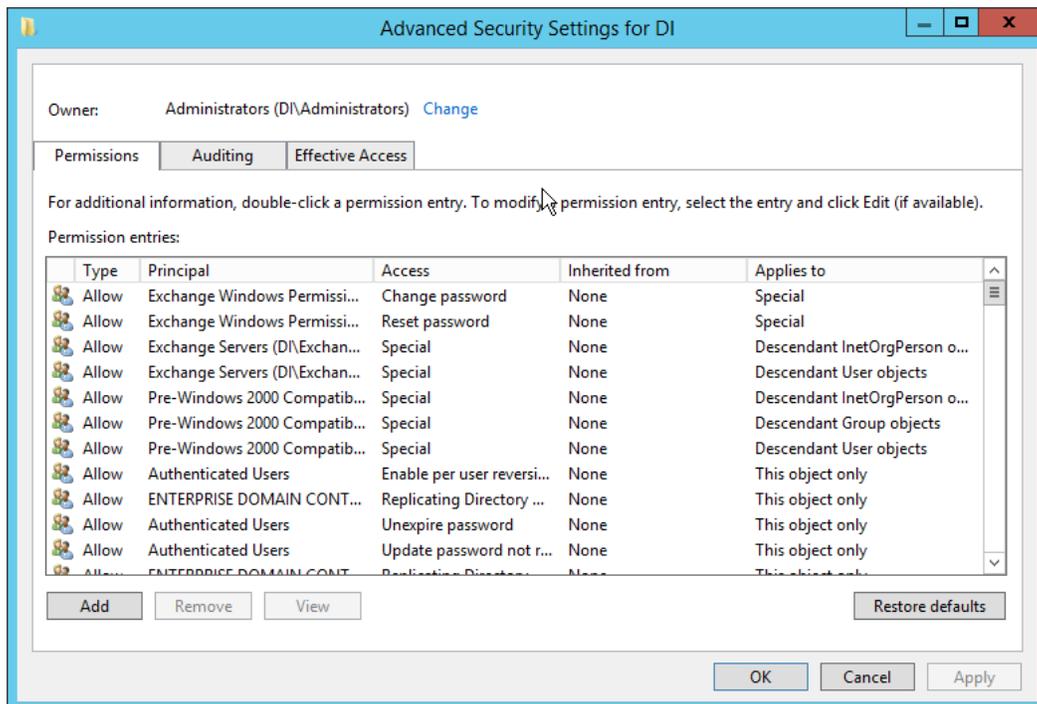
24. Click the **Security** tab.



1312

1313

25. Click **Advanced**.



1314

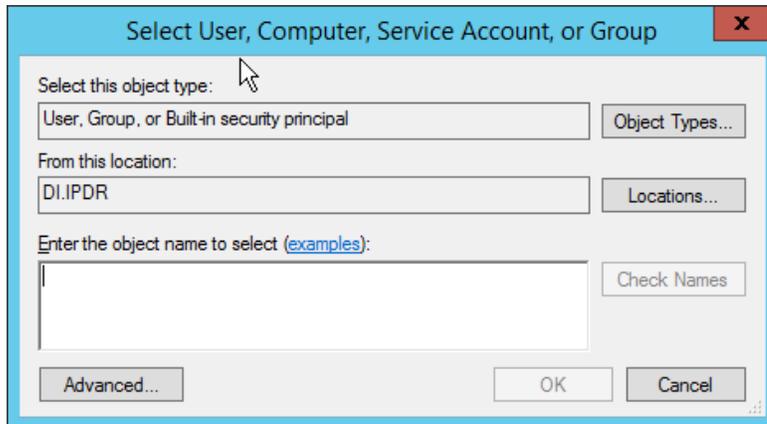
1315

1316

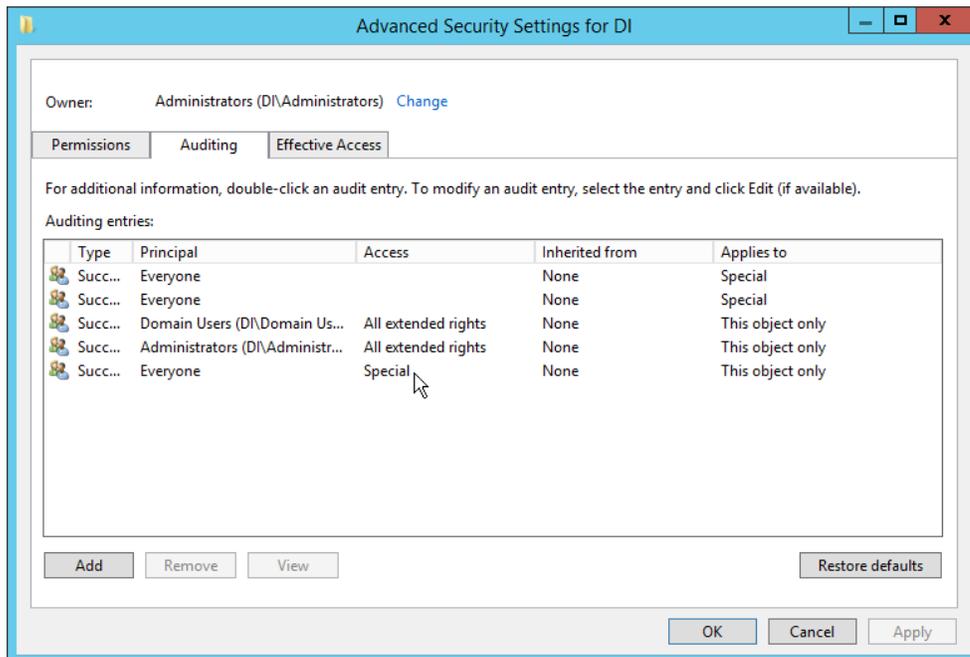
26. Click the **Auditing** tab.

27. Click **Add**.

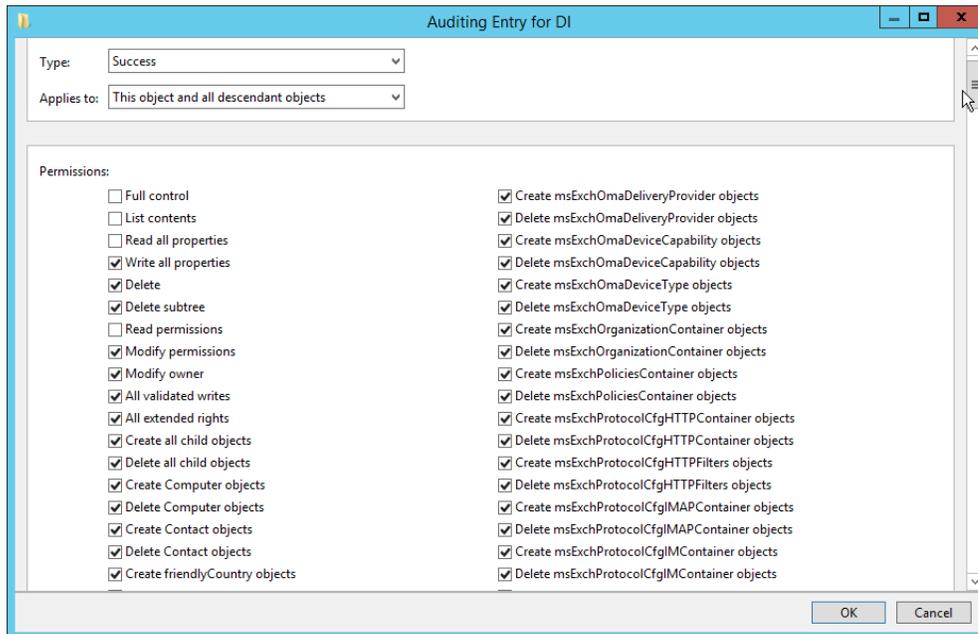
1317 28. Enter **Everyone**.



1318  
1319 29. Click **OK**.



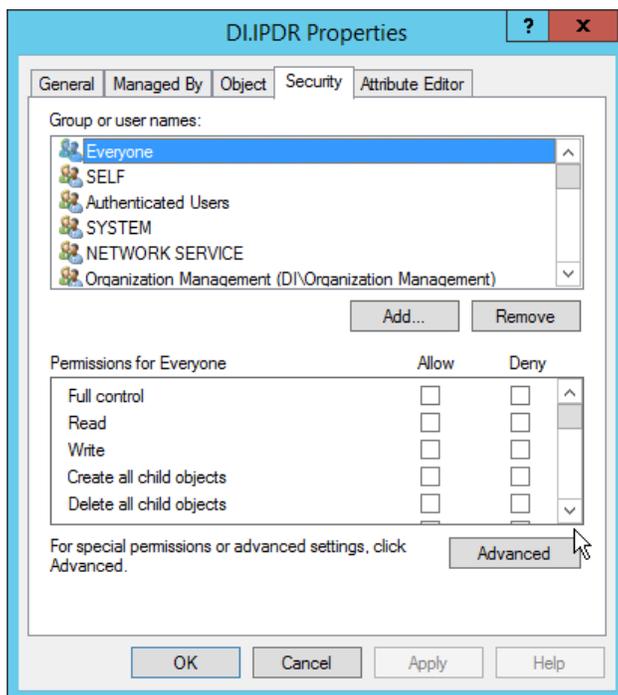
1320  
1321 30. Double-click **Everyone**.  
1322 31. Check the boxes next to **Write all properties, Delete, Delete subtree, Modify permissions,**  
1323 **Modify owner, All validated writes, All extended rights, Create all child objects, Delete all**  
1324 **child objects.**



1325

1326

32. Click **OK**.



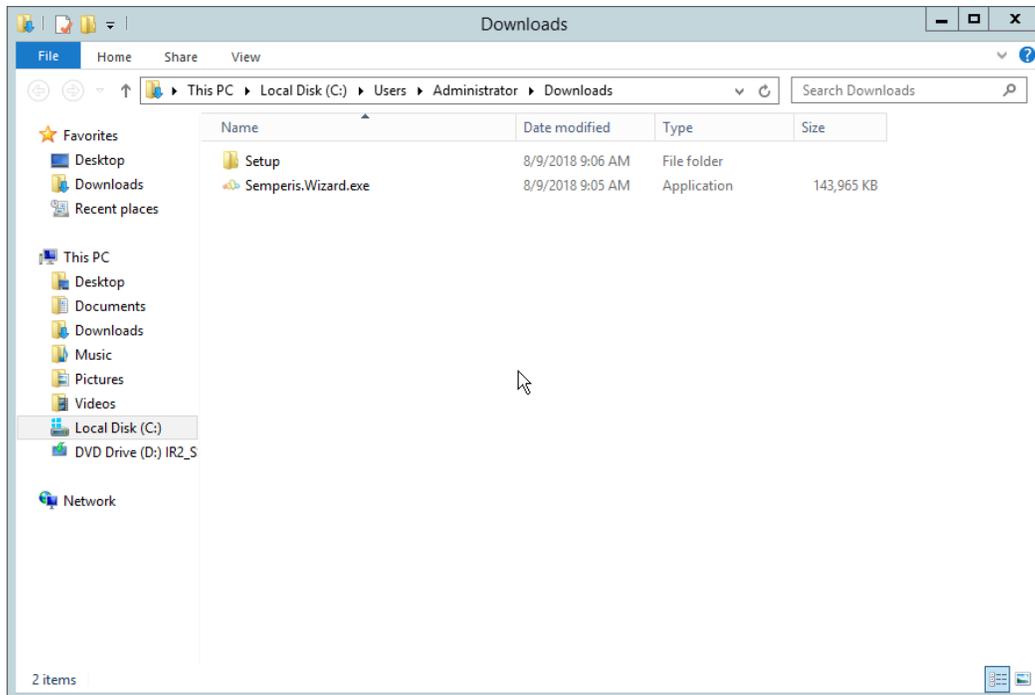
1327

1328

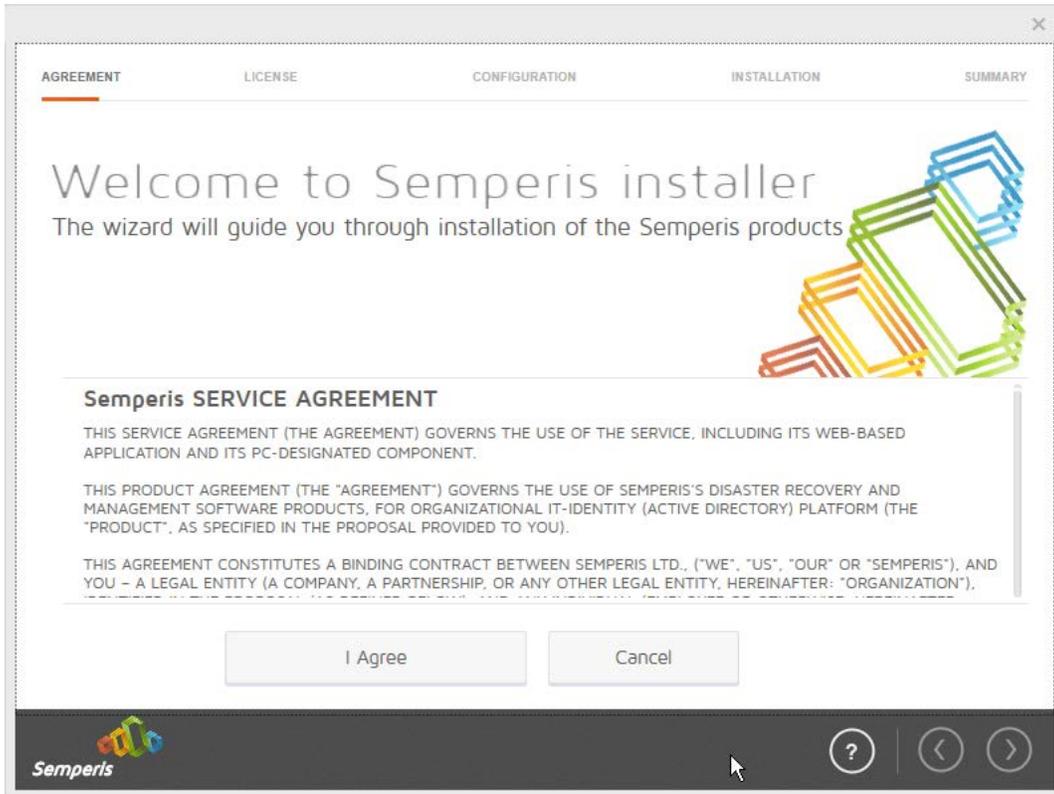
33. Click **OK**.

1329 **2.10.2 Install Semperis DSP**

- 1330 1. If you are using a local SQL Express Advanced server, place the **SQLEXPADV\_x64\_ENU.exe**  
1331 installer in a directory called Setup, and ensure that the **Semperis Wizard** is adjacent to the  
1332 **Setup** folder (not inside it). If an SQL Express Advanced server is not being used, no **Setup** folder  
1333 is required.



- 1334  
1335 2. If prompted to restart the computer, do so.



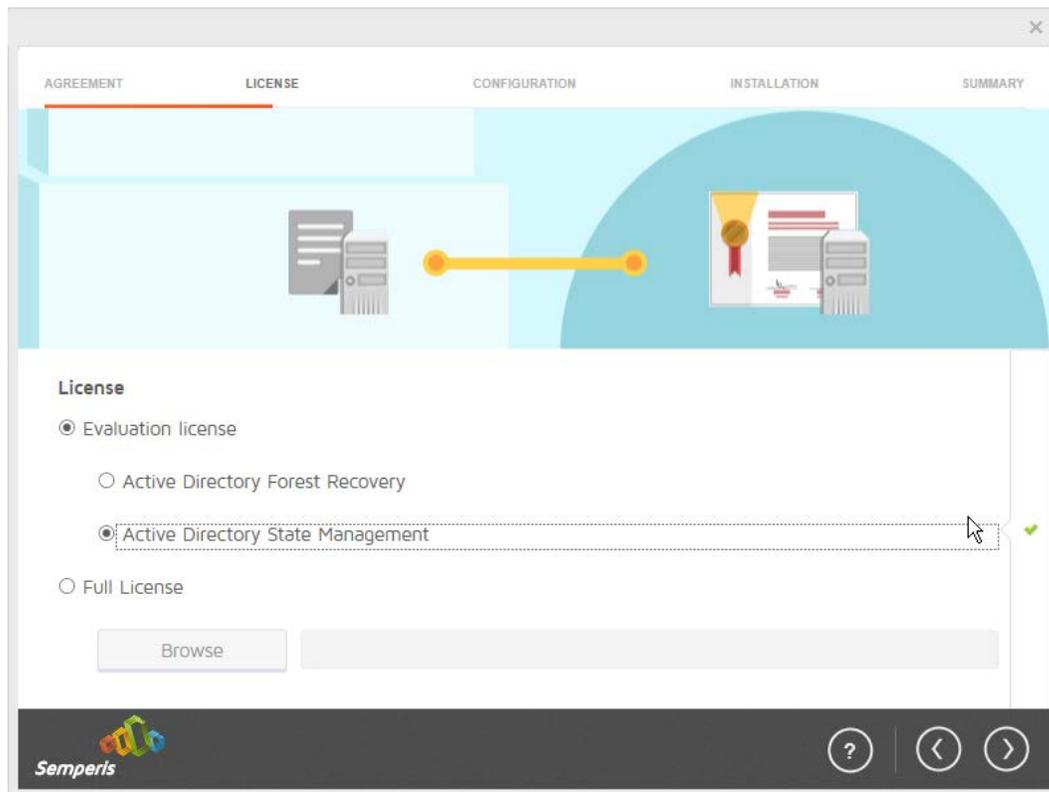
1336

1337

1338

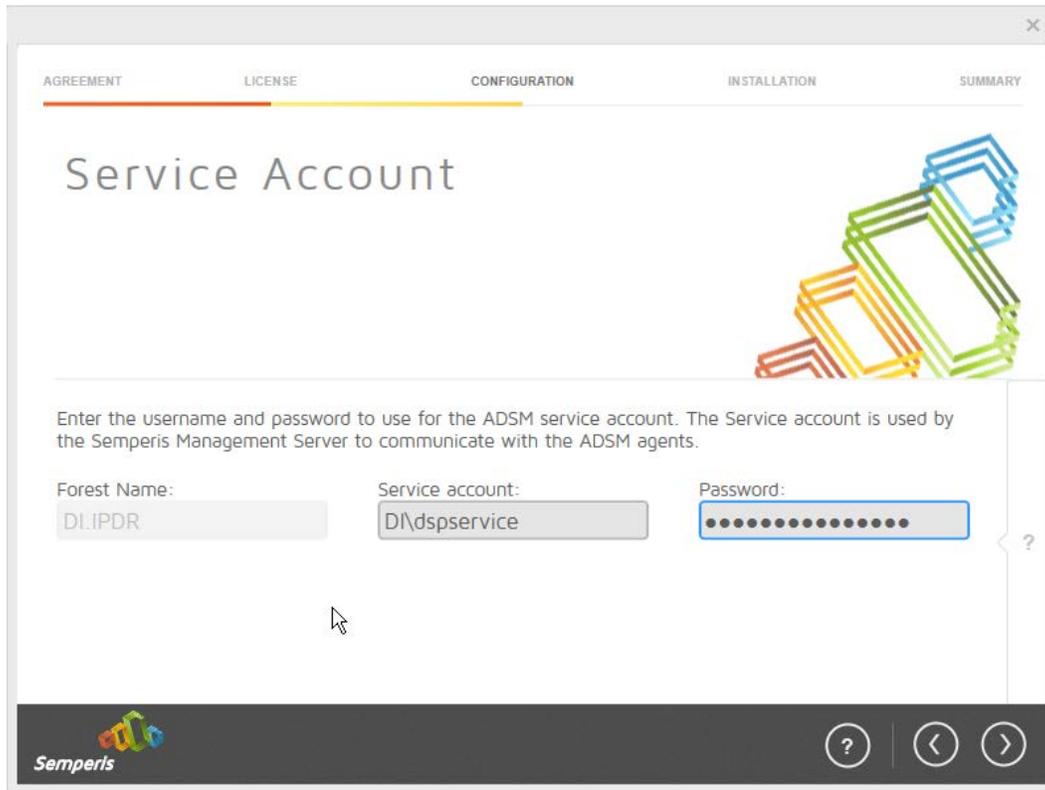
1339

3. Click **I Agree**.
4. Select **Evaluation License**.
5. Select **Active Directory State Management**.



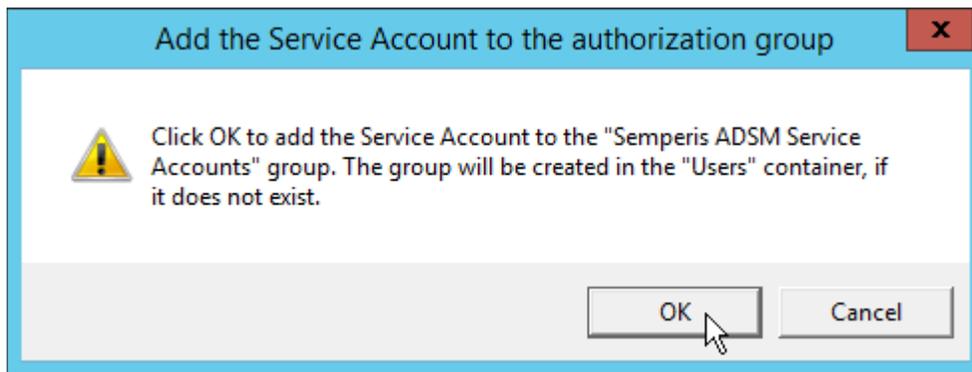
1340  
1341  
1342

6. Click the > button.
7. Enter the **username** and **password** of the account created earlier.



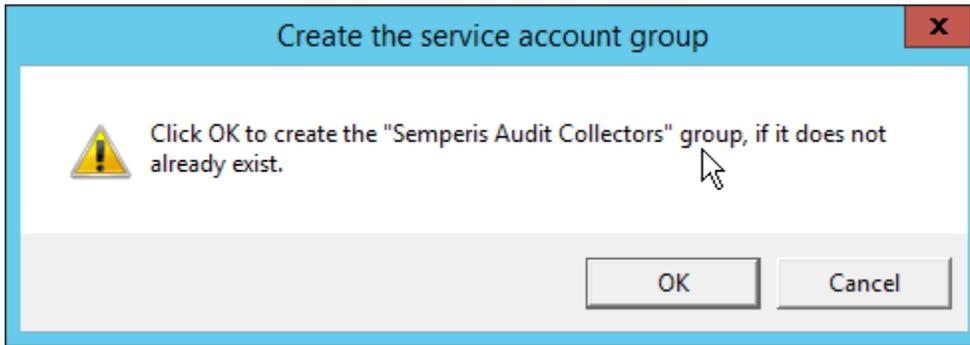
1343  
1344

8. Click the > button.



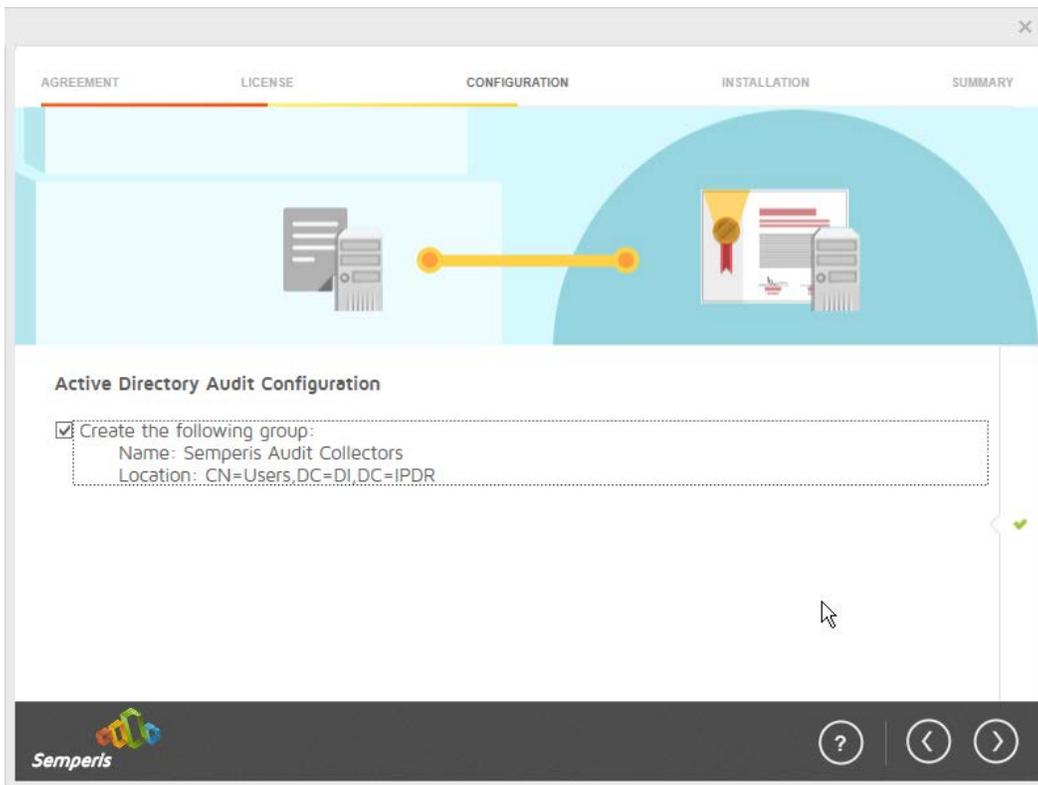
1345  
1346  
1347

9. Click **OK**.
10. Check the box next to **Create the following group**.



1348  
1349

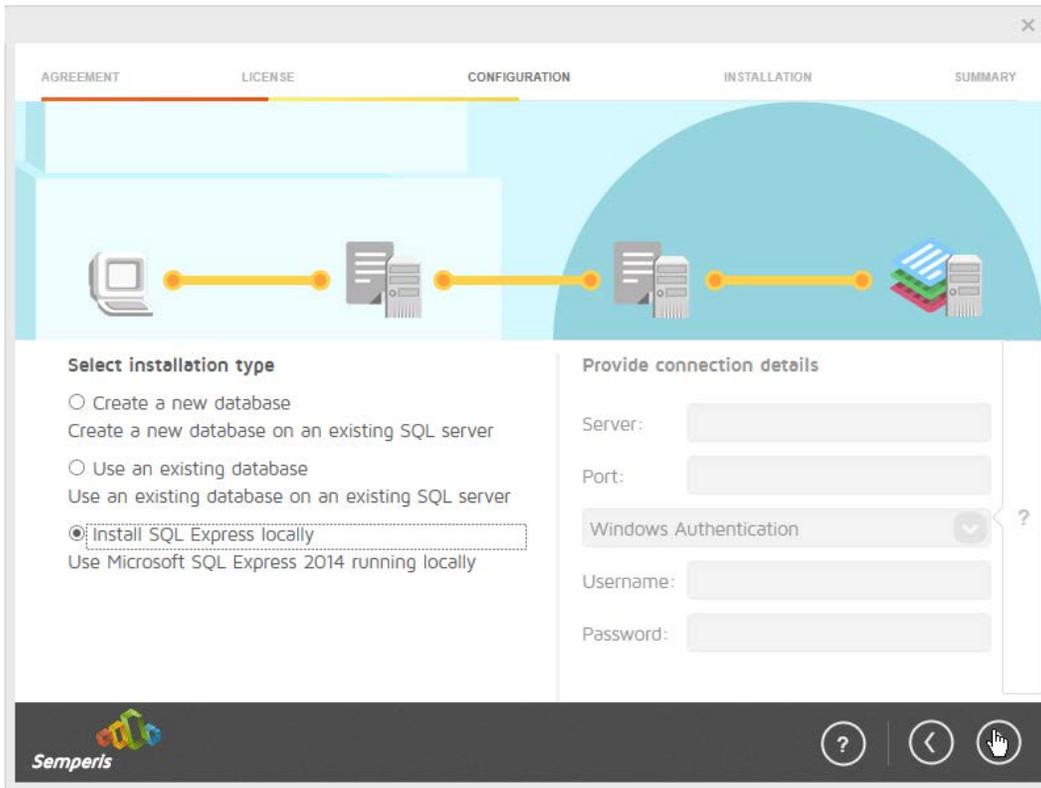
11. Click **OK**.



1350  
1351  
1352

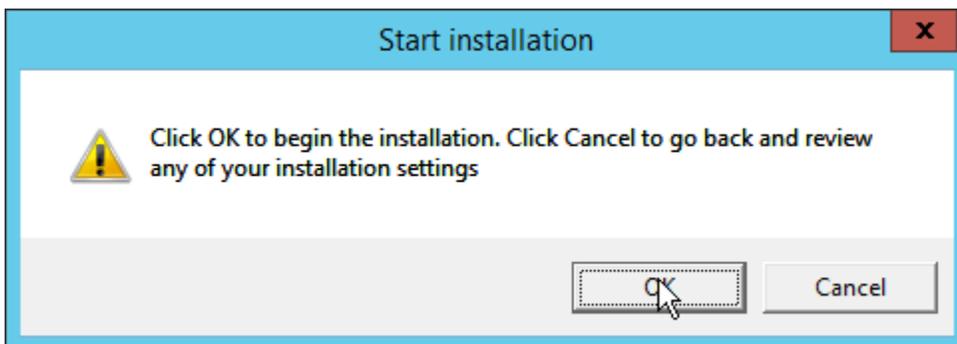
12. Click the > button.

13. Select the appropriate database option, and enter any required information.



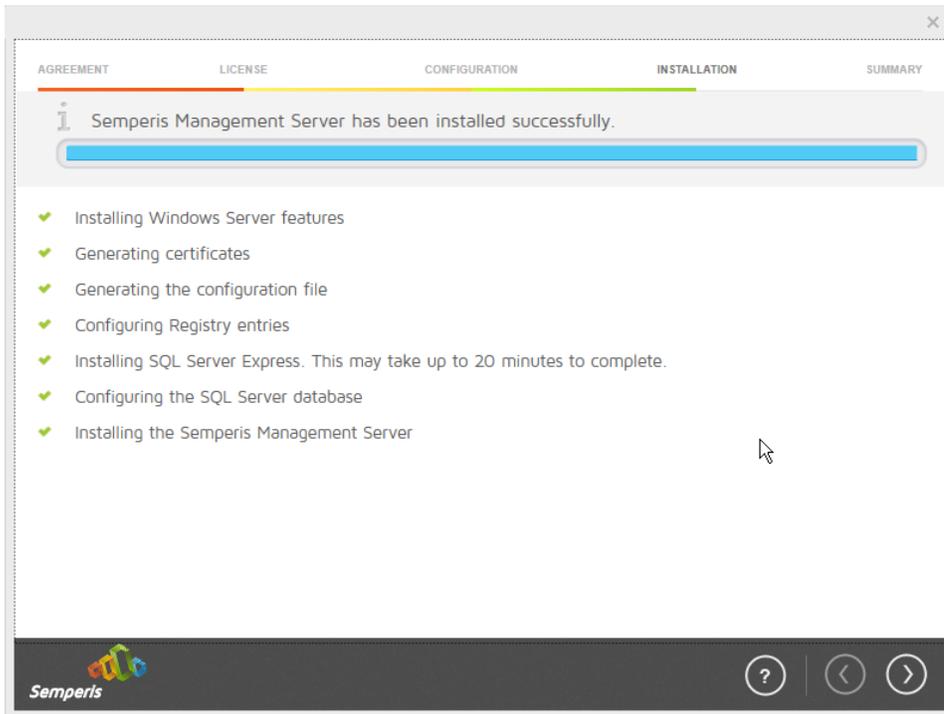
1353  
1354

14. Click the > button.



1355  
1356

15. Click **OK**.



1357

1358

16. Click the > button after the installation completes.

1359

17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS Protector**.

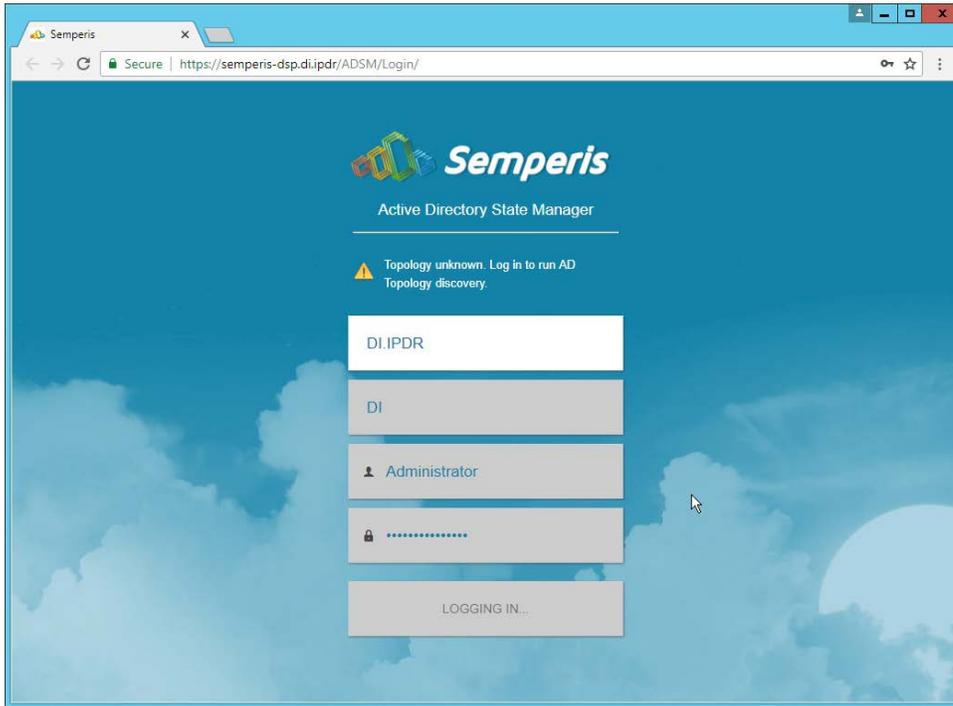
1360

1361

18. On the login page, enter the full domain as well as the NetBIOS name.

1362

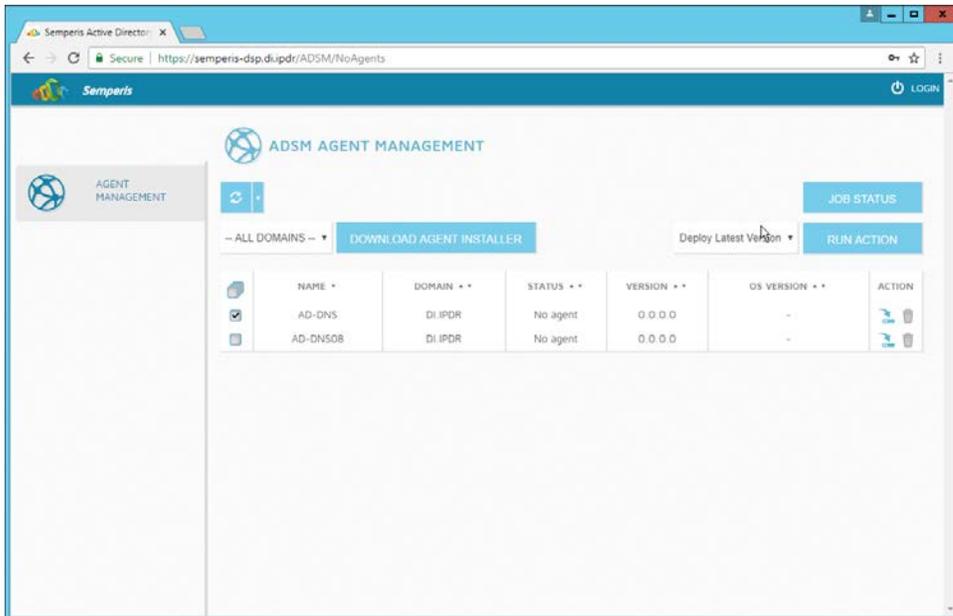
19. Enter the **username** and **password** of an administrator on the domain.



1363  
1364  
1365

20. Click **Login**.

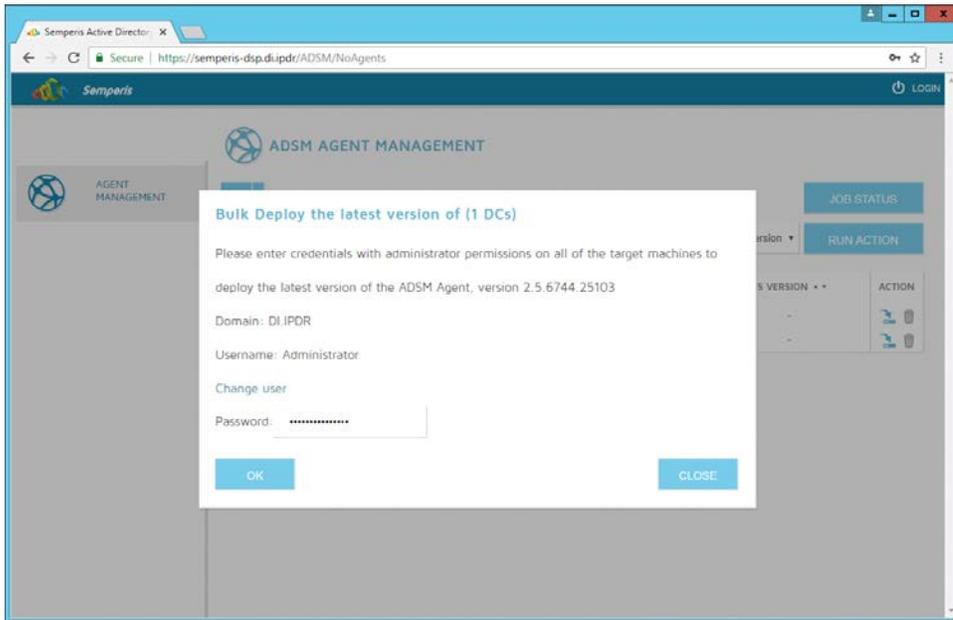
21. Check the box next to the domain controllers that should be monitored by DSP.



1366  
1367  
1368

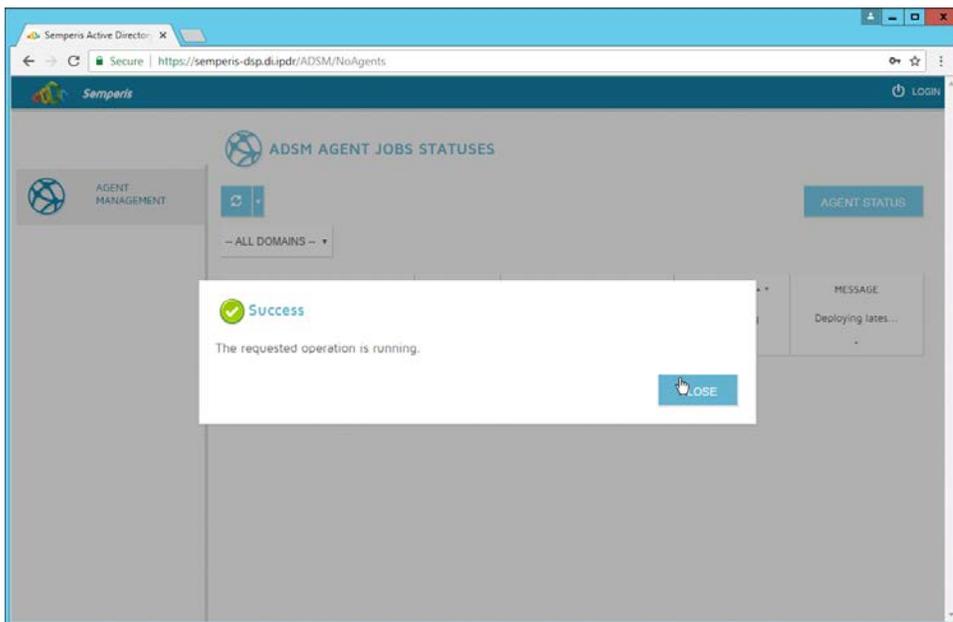
22. Click **Run Action**.

23. Enter the **password** for the account.



1369  
1370

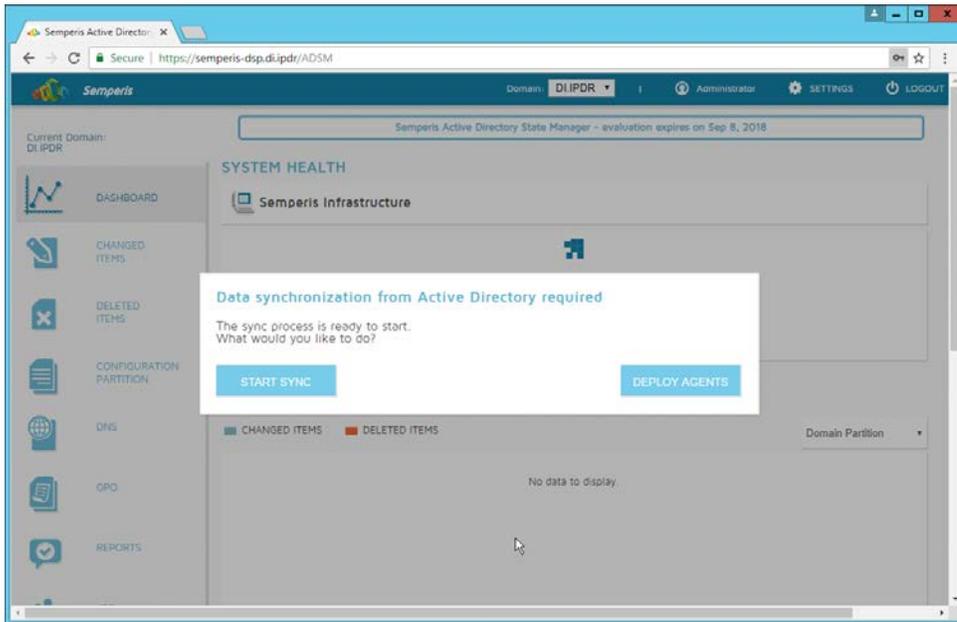
24. Click **OK**.



1371  
1372  
1373

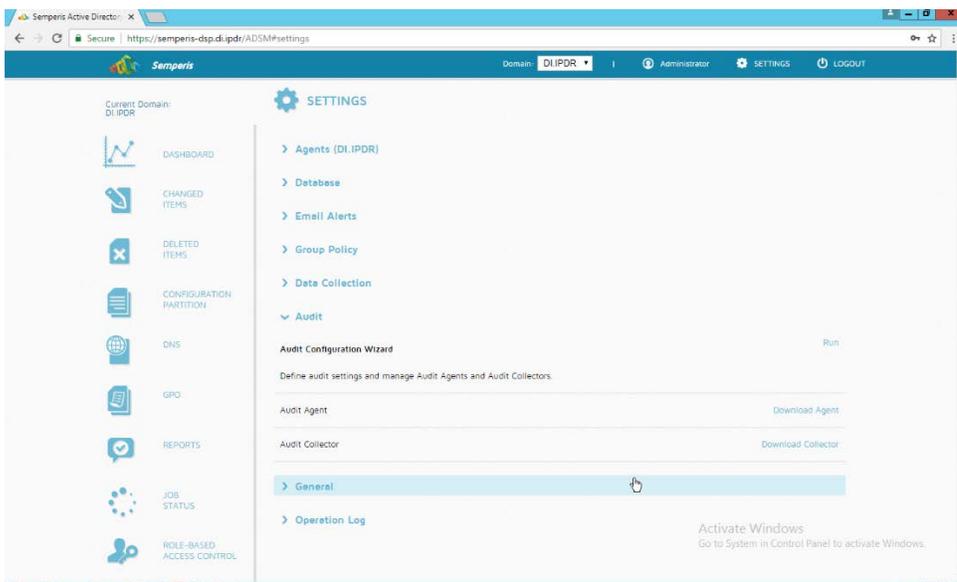
25. Click **Close**.

26. After the agent finishes deploying, click **Login** at the top of the page and log in.



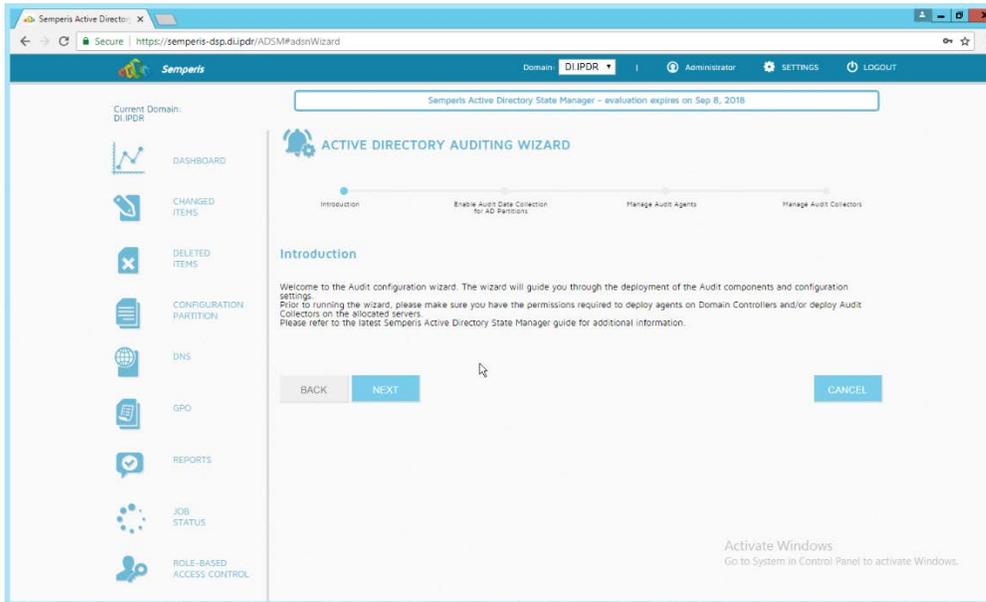
1374  
1375  
1376

- 27. Click **Start Sync**.
- 28. After this completes, click **Settings** at the top of the page.



1377  
1378  
1379

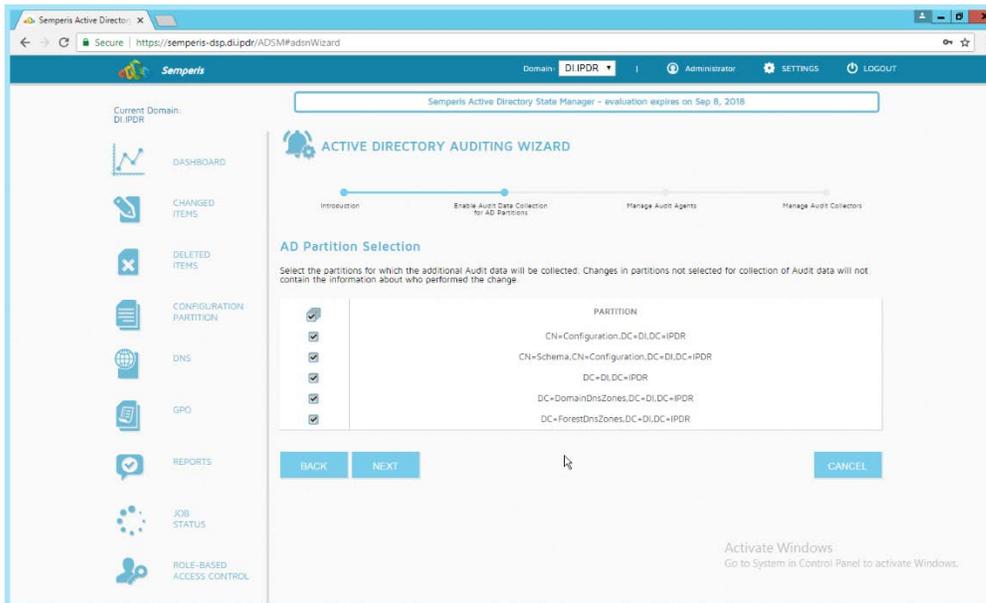
- 29. Click **Audit**.
- 30. Click **Run**.



1380

1381

31. Click **Next**.



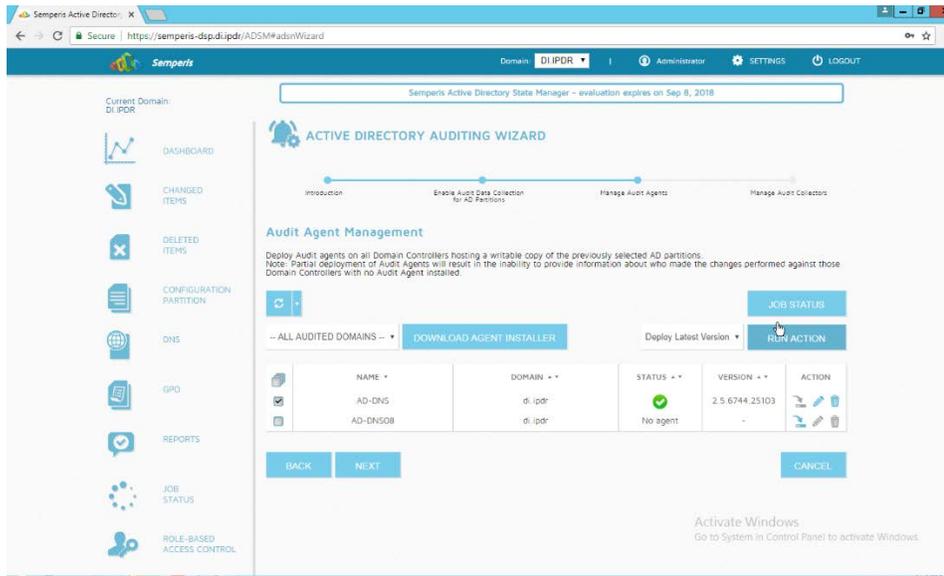
1382

1383

1384

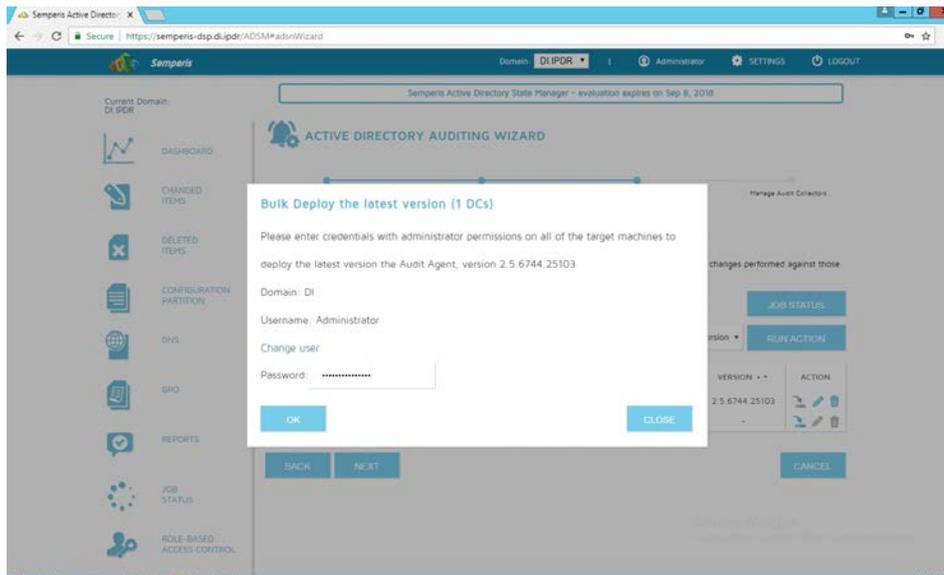
32. Click **Next**.

33. Check the boxes next to any Domain Controllers that should be monitored.



1385  
1386  
1387

- 34. Click **Run Action**.
- 35. Enter the **password**.

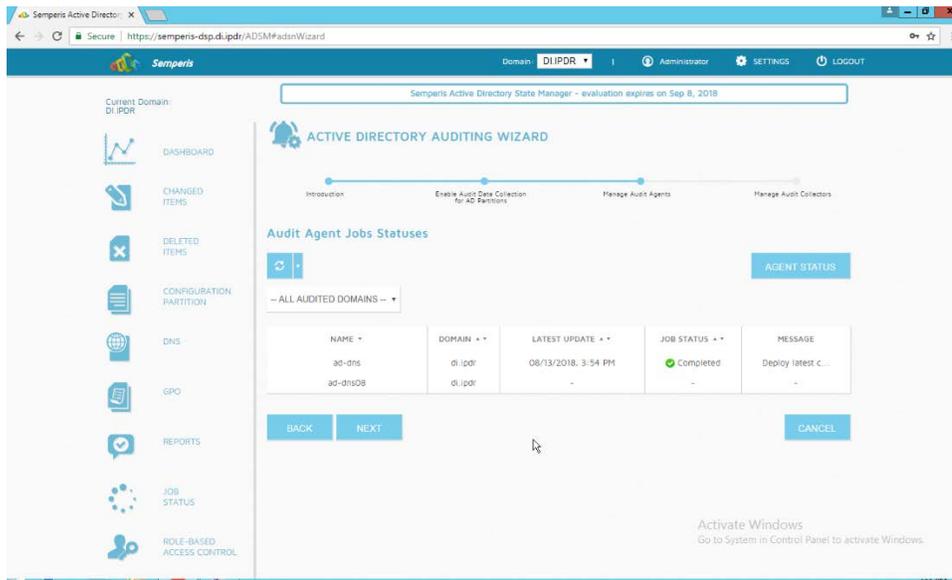


1388  
1389  
1390

- 36. Click **OK**.
- 37. Wait for the deployment to finish.

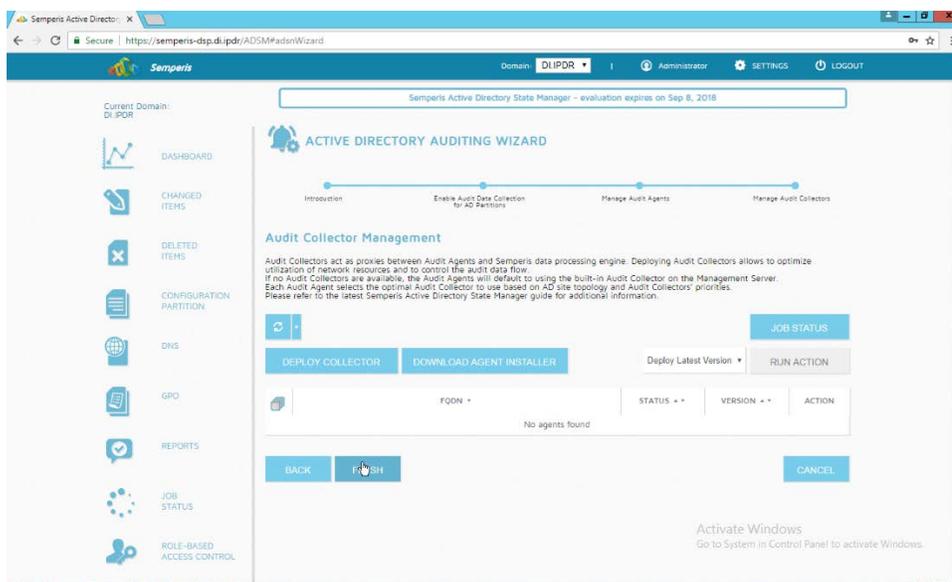
1391  
1392

38. Click **Next**.



1393  
1394

39. Click **Finish**.



## 1395 2.11 Micro Focus ArcSight Enterprise Security Manager

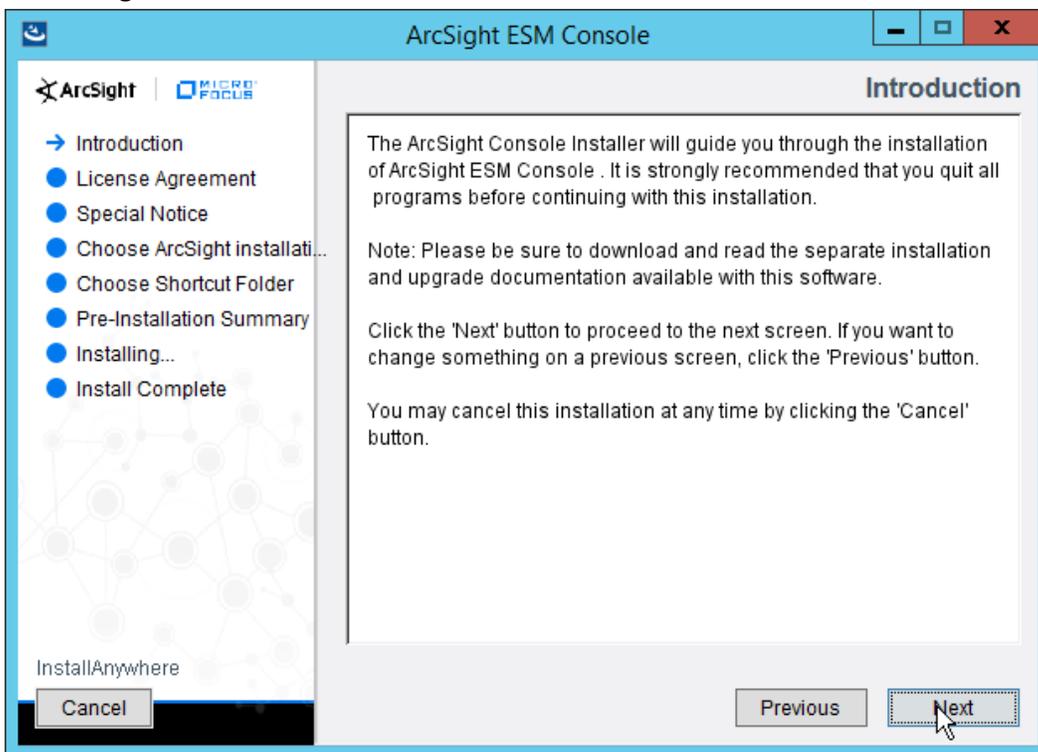
1396 Micro Focus ArcSight Enterprise Security Manager is primarily a log collection/analysis tool with  
1397 features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs  
1398 generated by various systems, applications, and security solutions.

1399 This installation guide assumes a preconfigured CentOS 7 machine with Enterprise Security Manager  
1400 (ESM) already installed and licensed. This section covers the installation and configuration process used  
1401 to set up ArcSight agents on various machines, as well as some analysis and reporting capabilities.

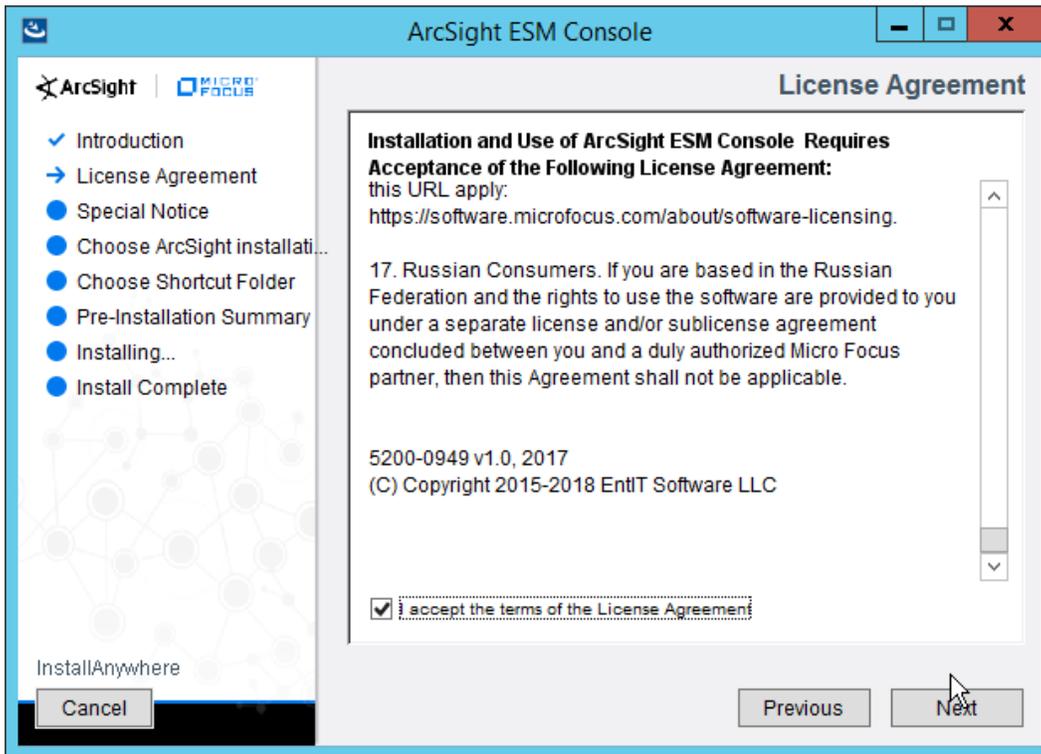
1402 Installation instructions are included for both Windows and UNIX machines, as well as for collecting  
1403 from multiple machines. Furthermore, integrations with other products in the build are included in later  
1404 sections.

### 1405 2.11.1 Install the ArcSight Console

- 1406 1. Run **ArcSight-7.0.0.2436.1-Console-Win.exe**.

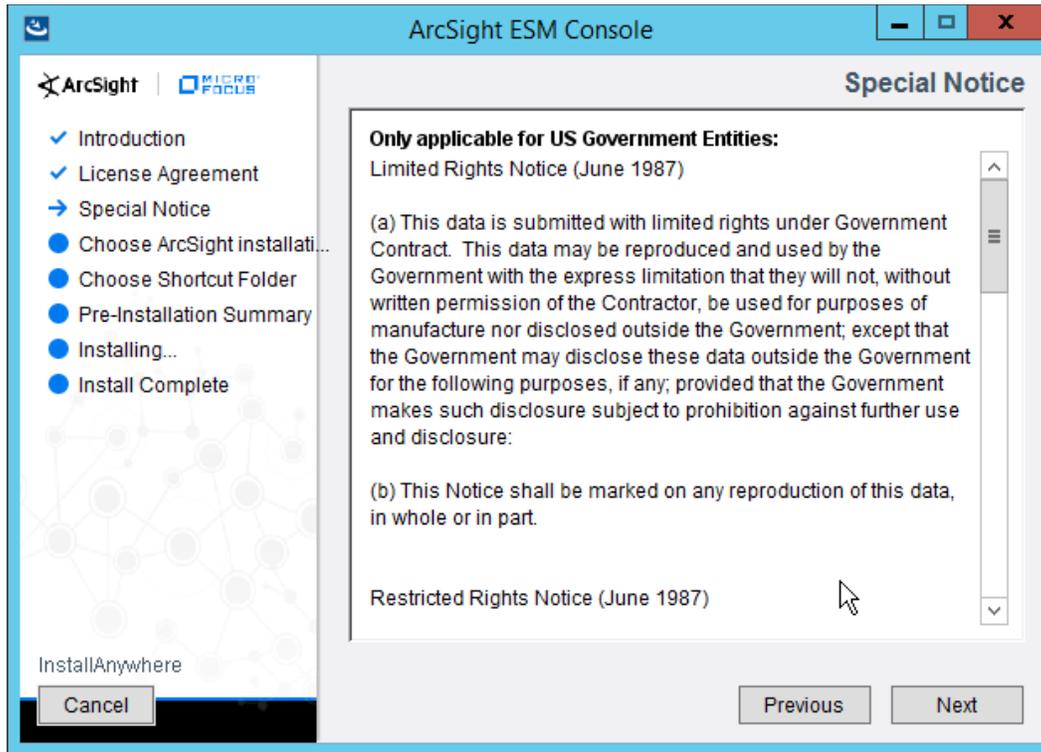


- 1407
- 1408 2. Click **Next**.
- 1409 3. Check the box next to **I accept the License Agreement**.



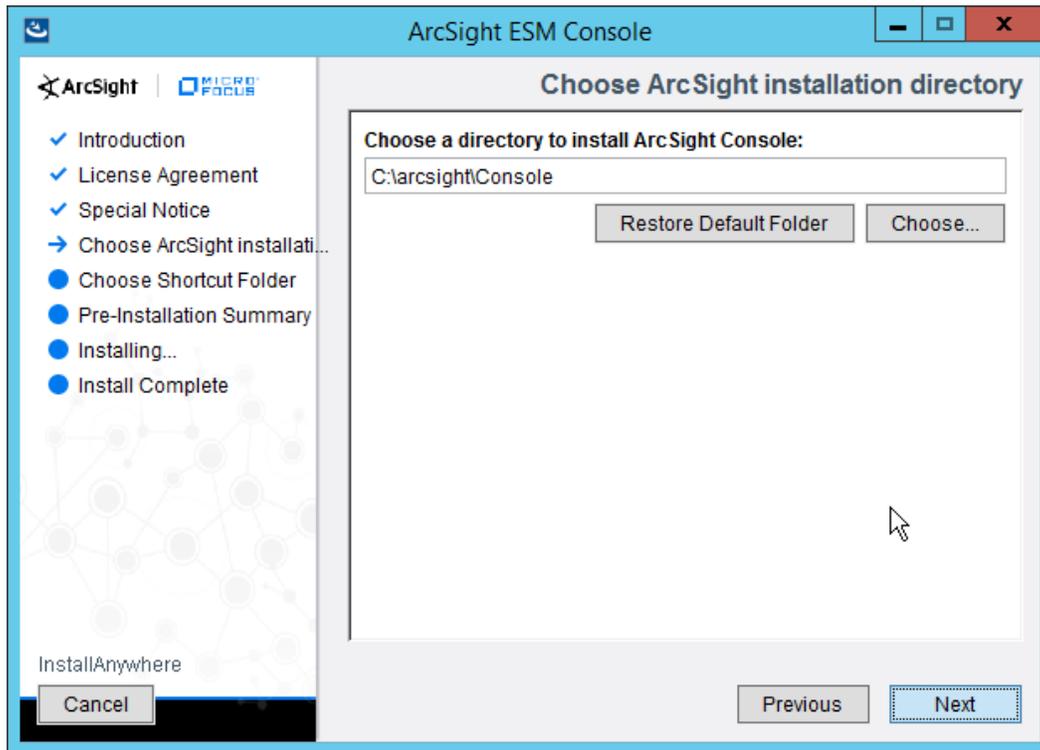
1410  
1411

4. Click **Next**.



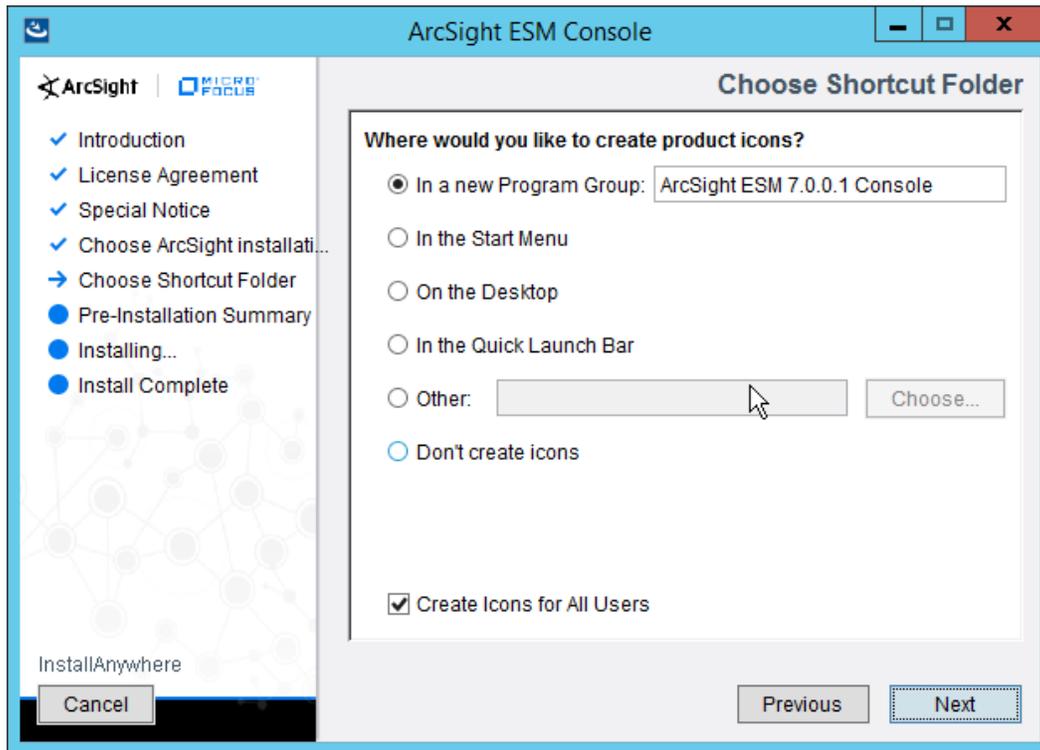
1412  
1413

5. Click **Next**.



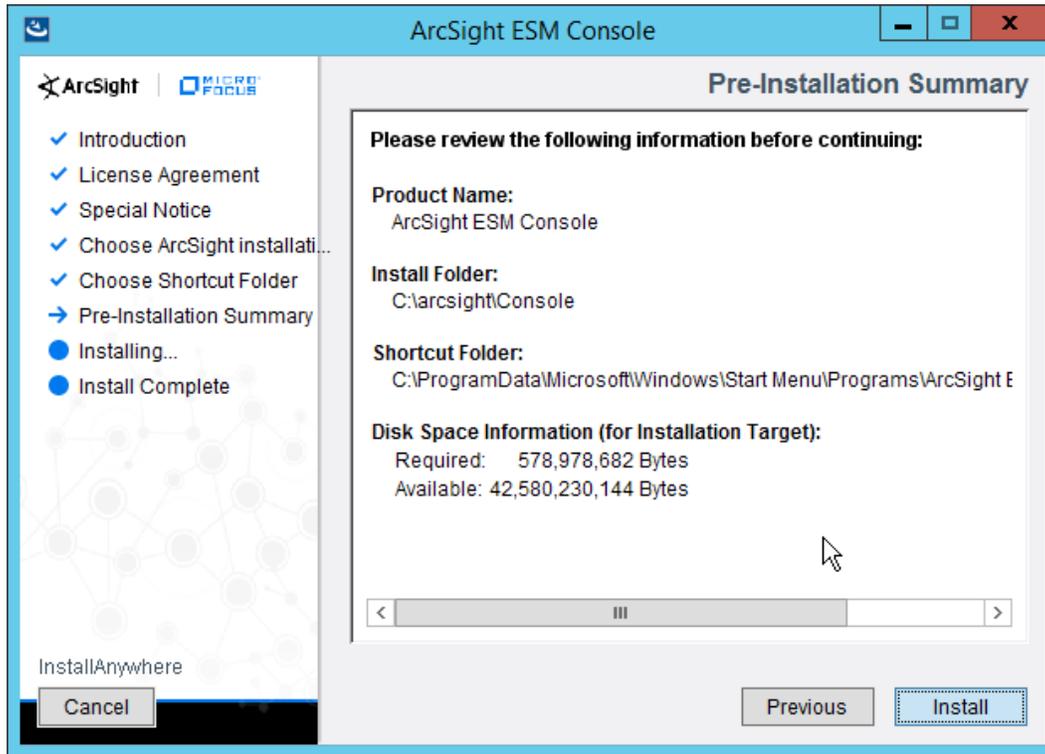
1414  
1415

6. Click **Next**.



1416  
1417

7. Click **Next**.

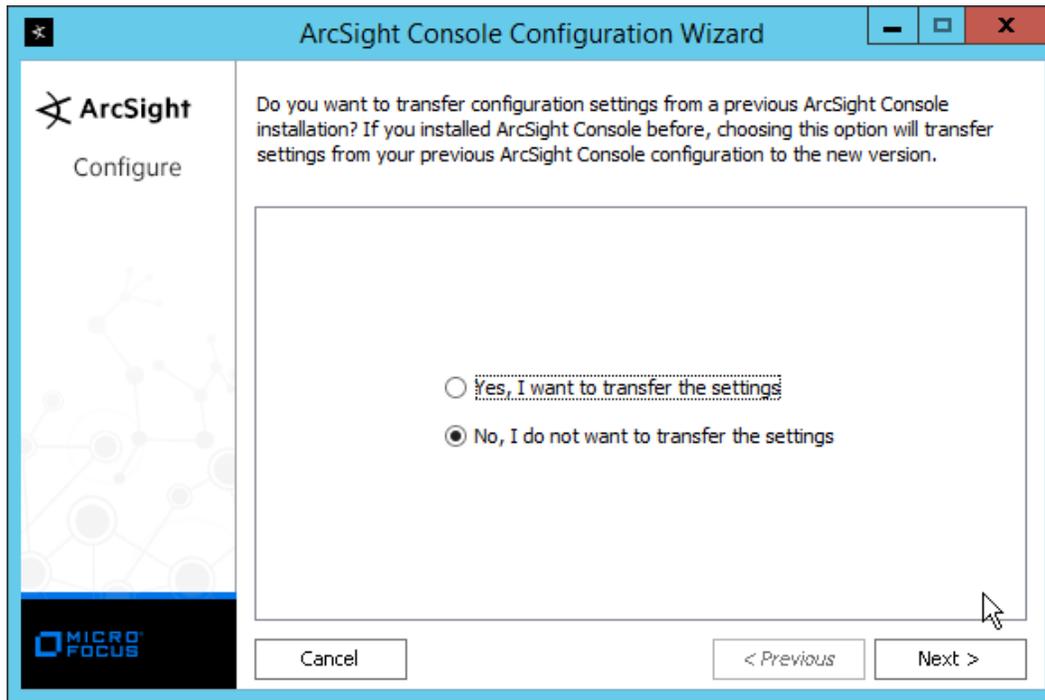


1418

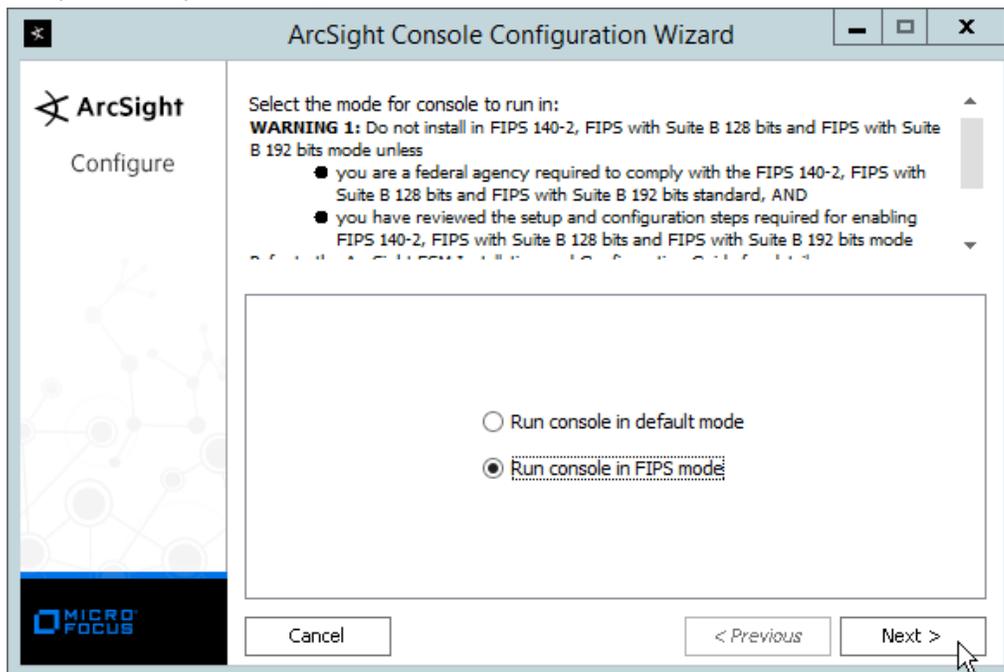
1419

1420

8. Click **Install**.
9. Select **No, I do not want to transfer the settings**.

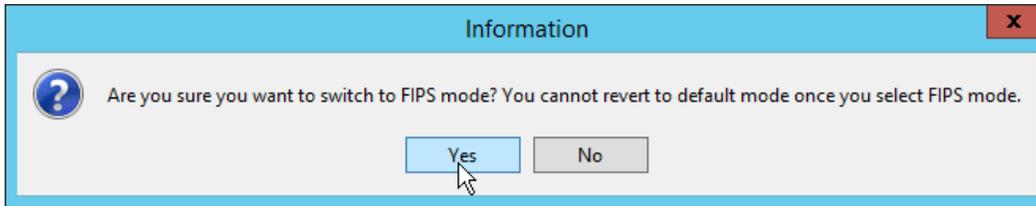


- 1421
- 1422 10. Click **Next**.
- 1423 11. Select **Run console in default mode**. (This can be changed later according to your organization's
- 1424 compliance requirements.)



1425

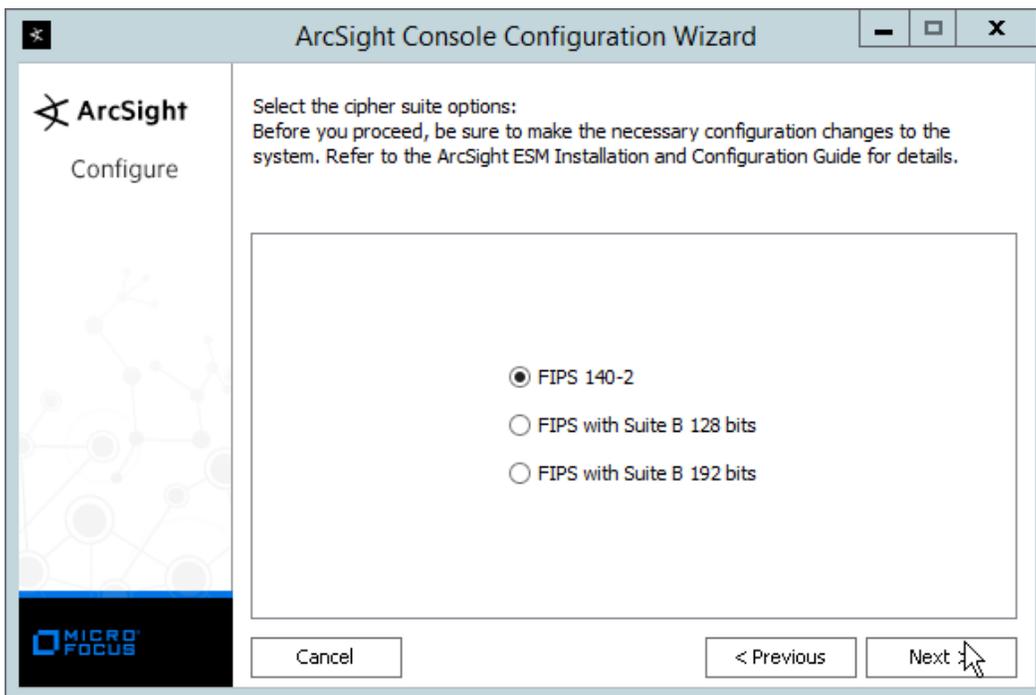
1426 12. Click **Next**.



1427

1428 13. Click **Yes**.

1429 14. Select **FIPS 140-2**.

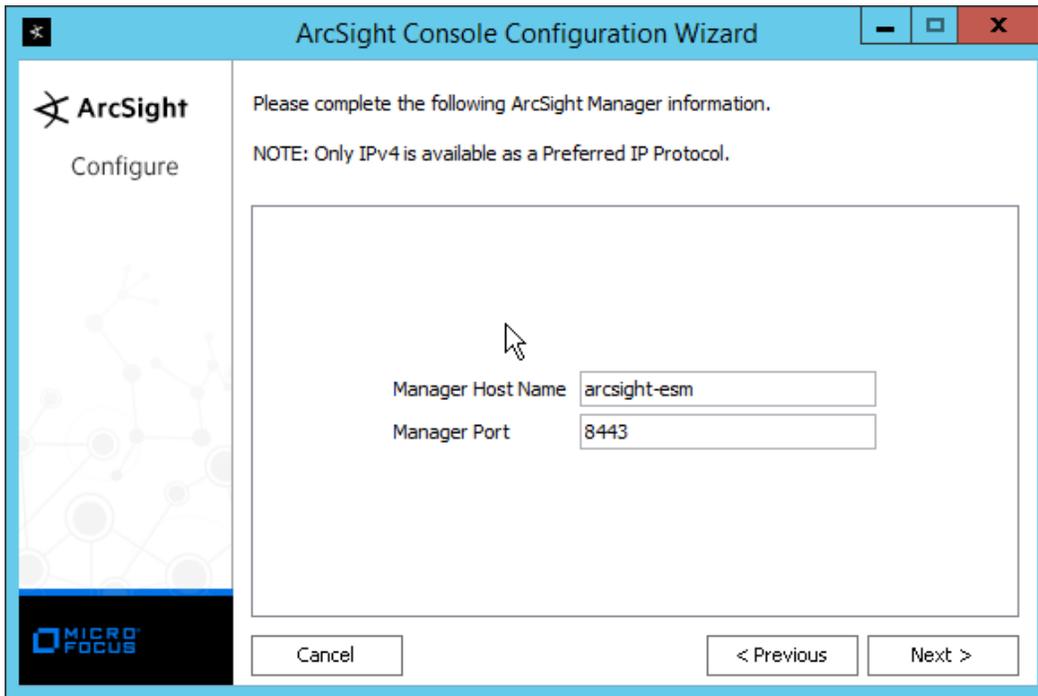


1430

1431 15. Click **Next**.

1432 16. Enter the **hostname** of the ESM server for **Manager Host Name**.

1433 17. Enter the **port** that ESM is running on for **Manager Port** (default: 8443).



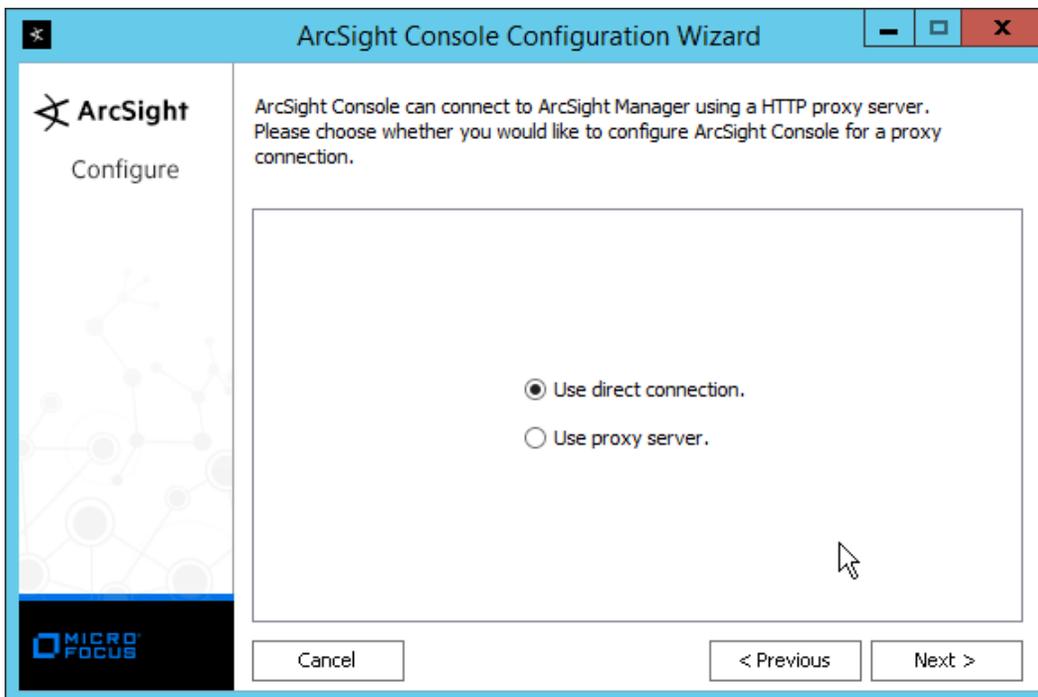
1434

1435

1436

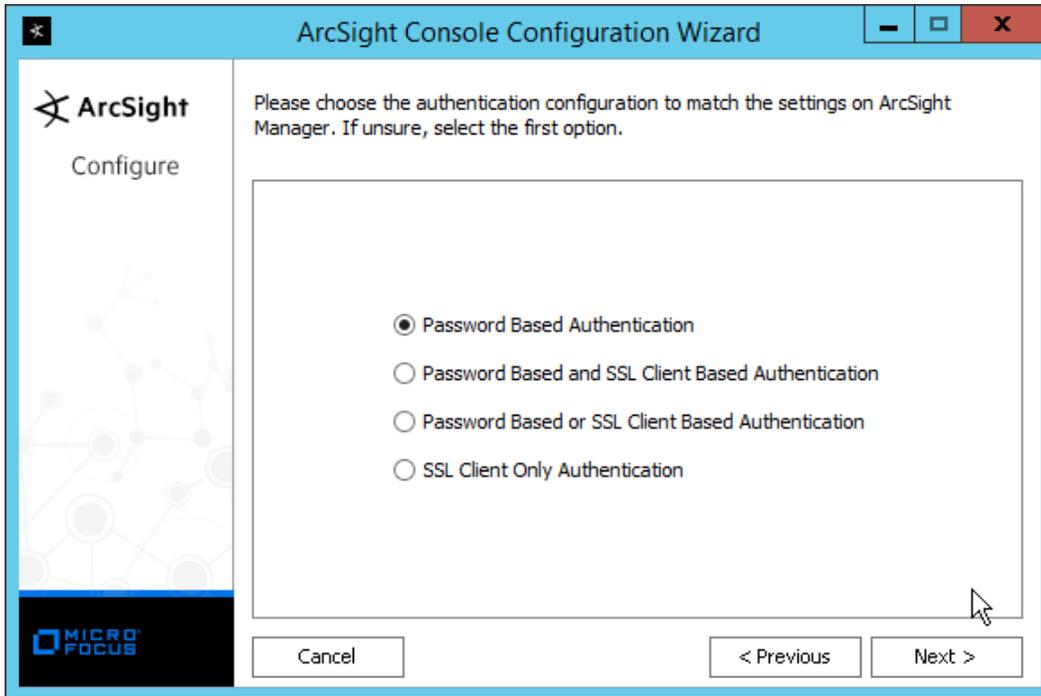
18. Click **Next**.

19. Select **Use direct connection**.



1437

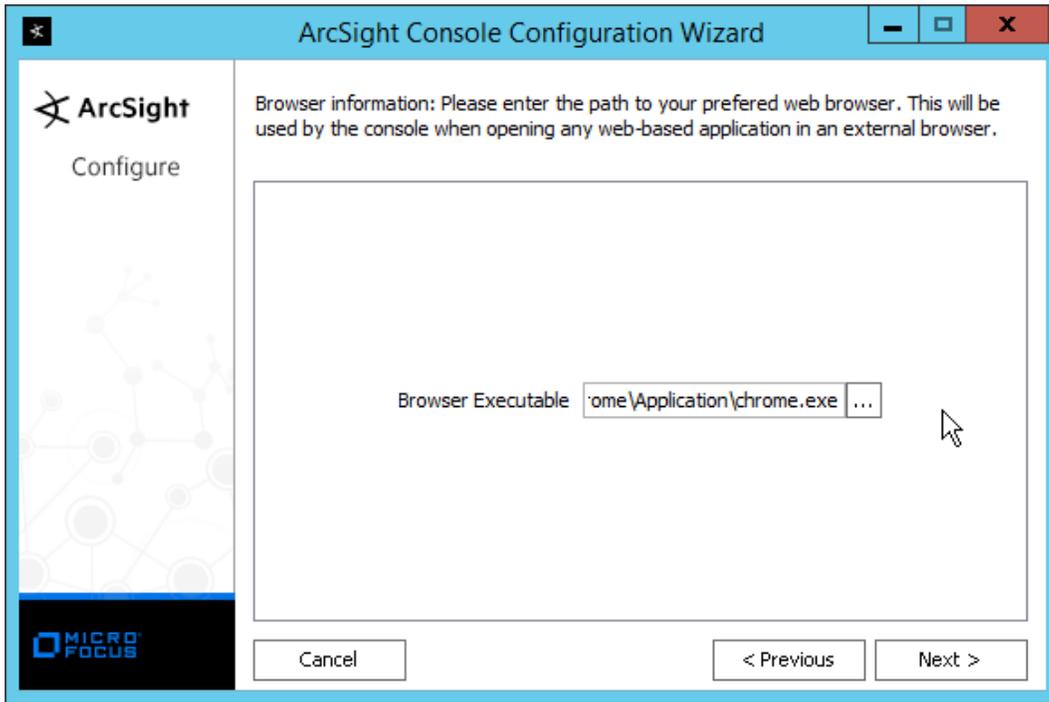
1438 20. Click **Next**.



1439

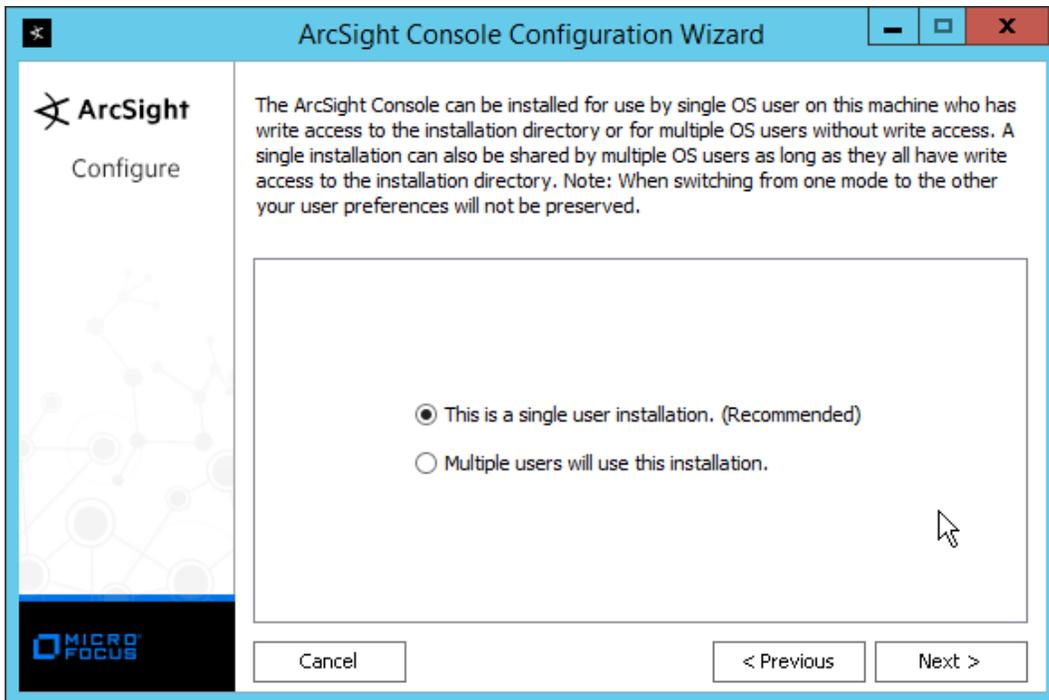
1440 21. Click **Next**.

1441 22. Select your preferred browser.



1442  
1443

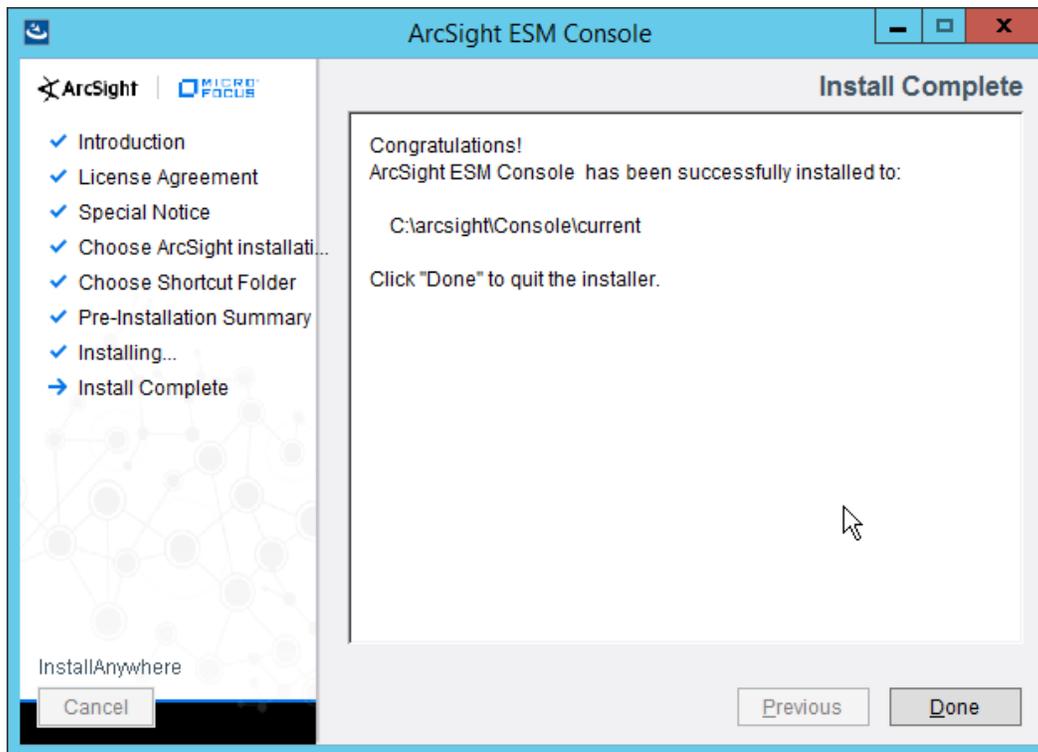
23. Click **Next**.



1444  
1445

24. Click **Next**.

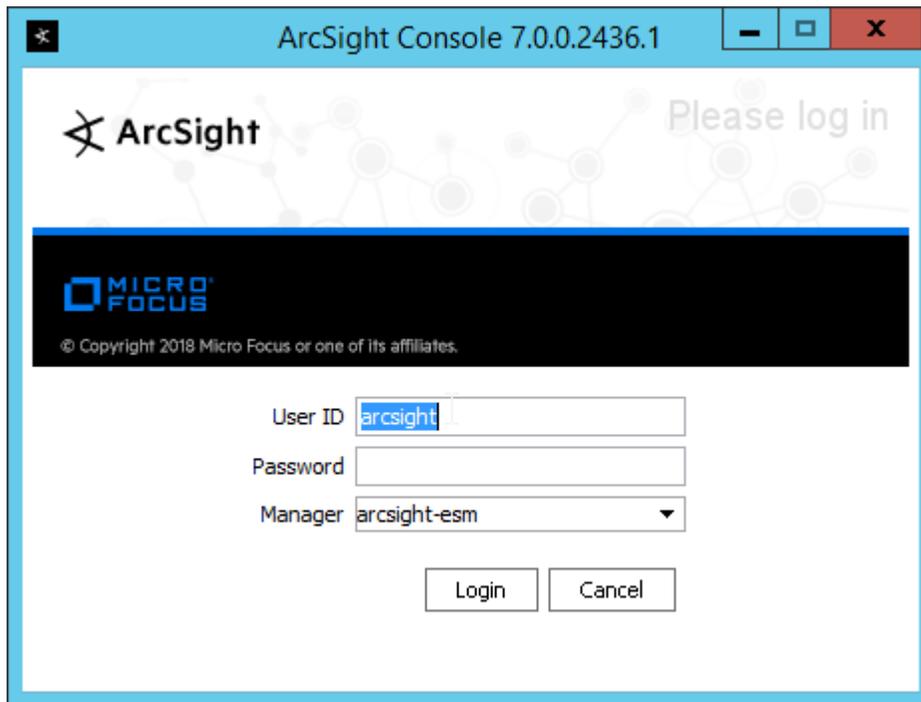
1446 25. Click **Finish**.



1447  
1448 26. Click **Done**.

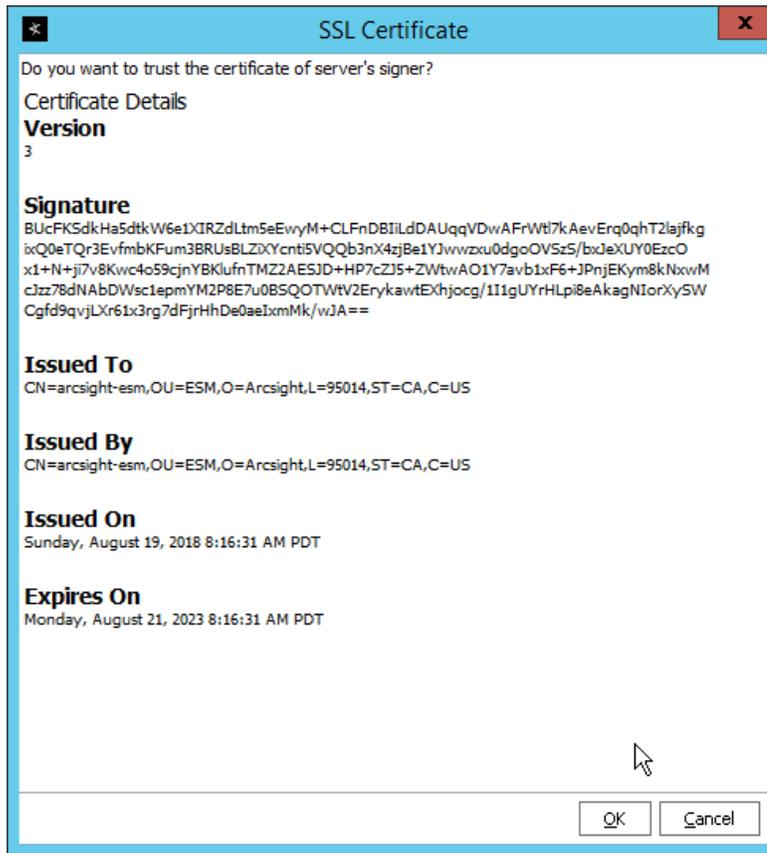
1449 27. Run **ArcSight Console** from the Start menu.

1450 28. Enter the **username** and **password**.



1451  
1452  
1453

29. Click **Login**. (If you are unable to connect, ensure that the hostname of the ESM server is present in your DNS server.)

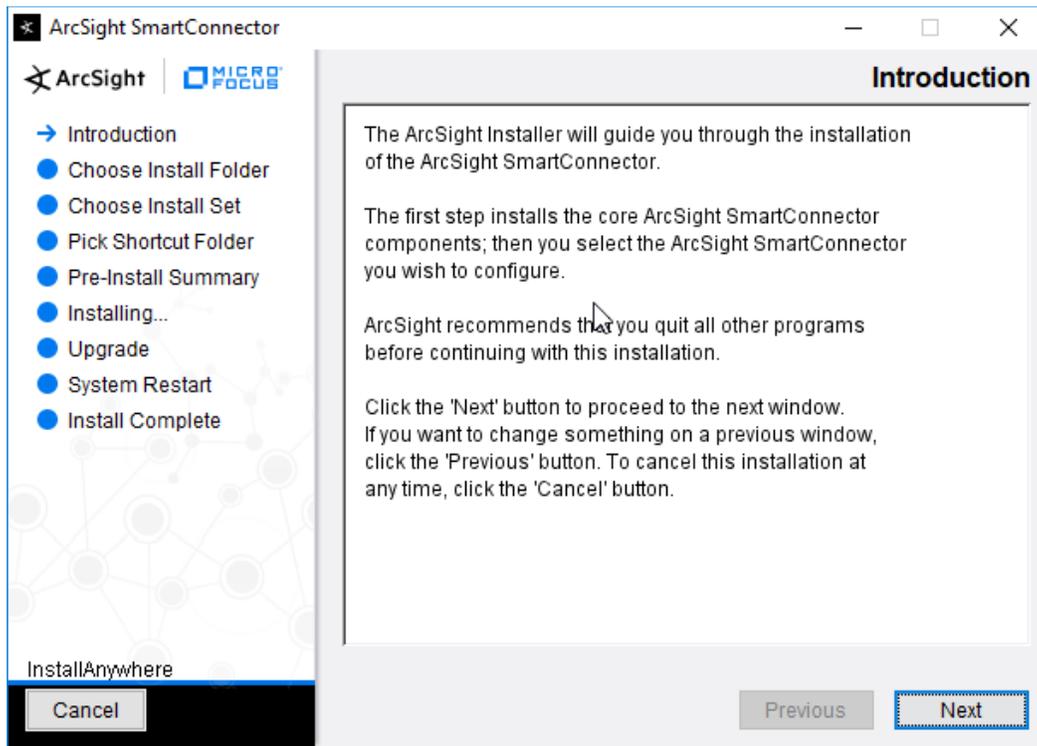


1454

1455 30. Click **OK**.

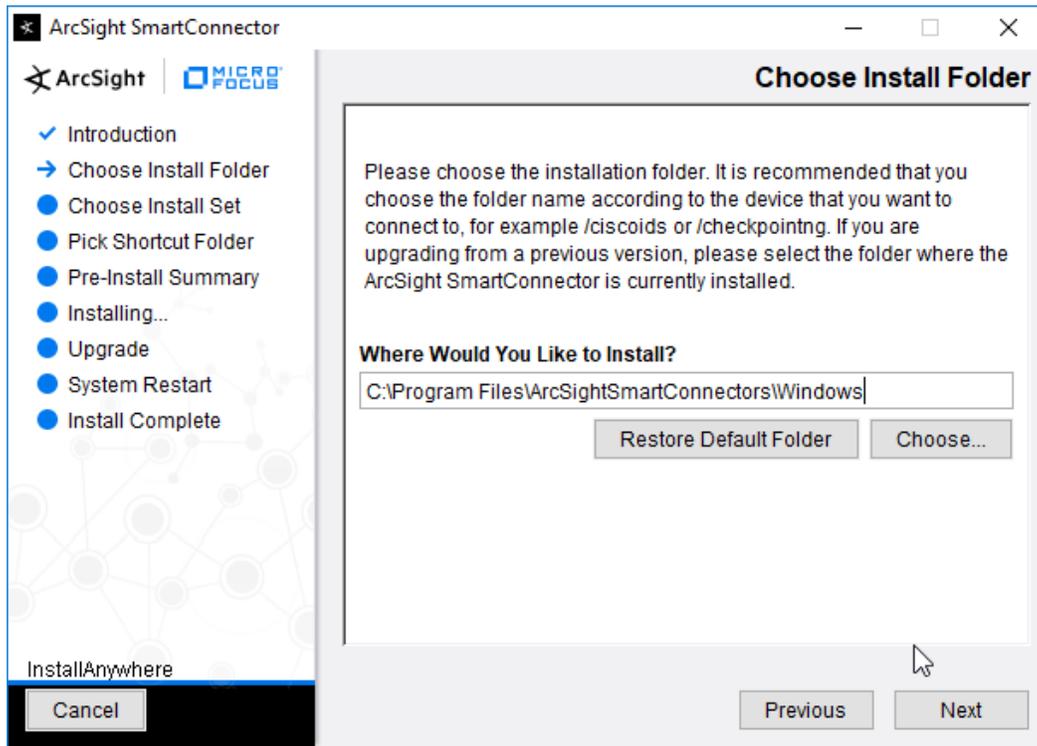
## 1456 2.11.2 Install Individual ArcSight Windows Connectors

1457 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



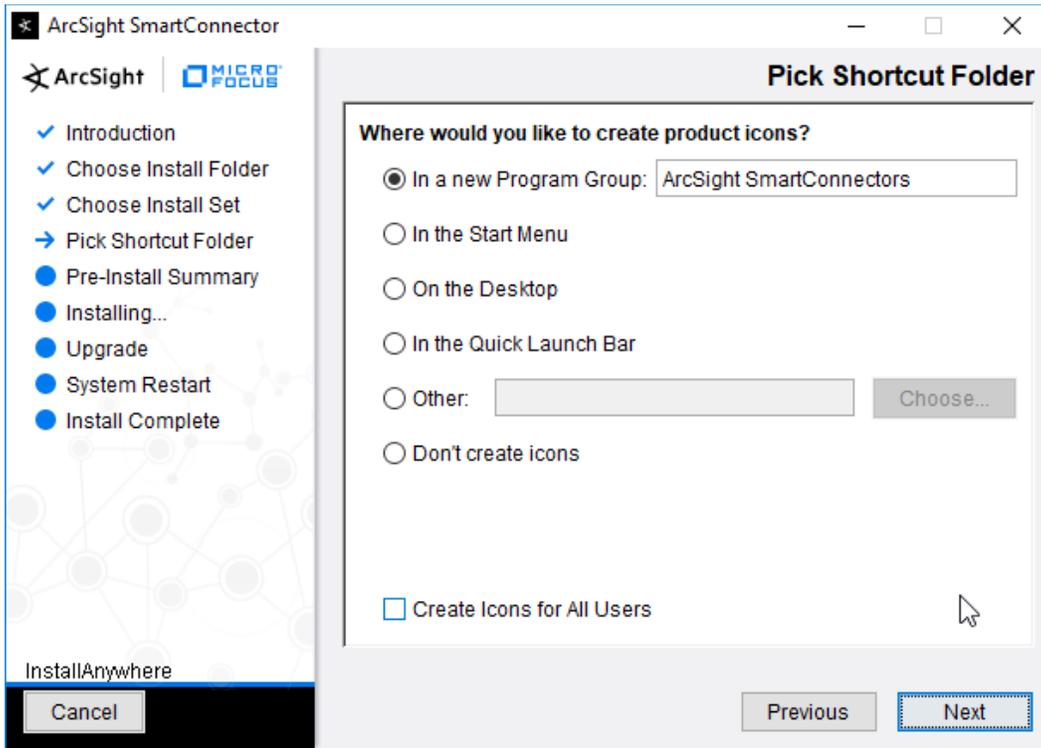
1458  
1459  
1460

2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



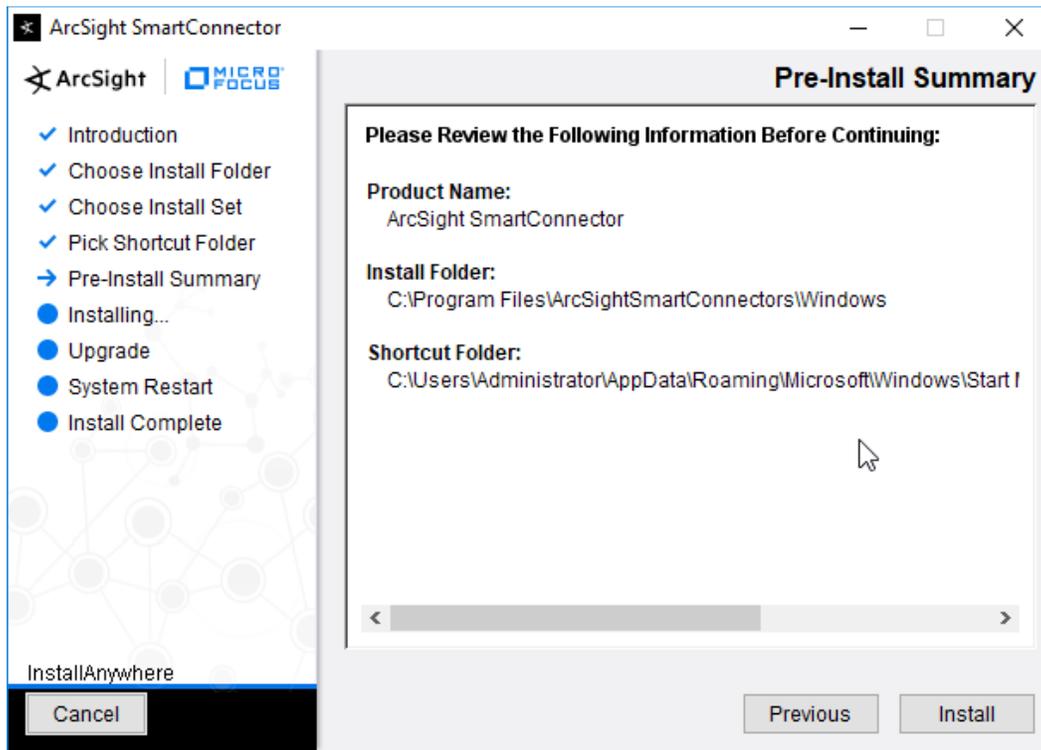
1461  
1462

4. Click **Next**.



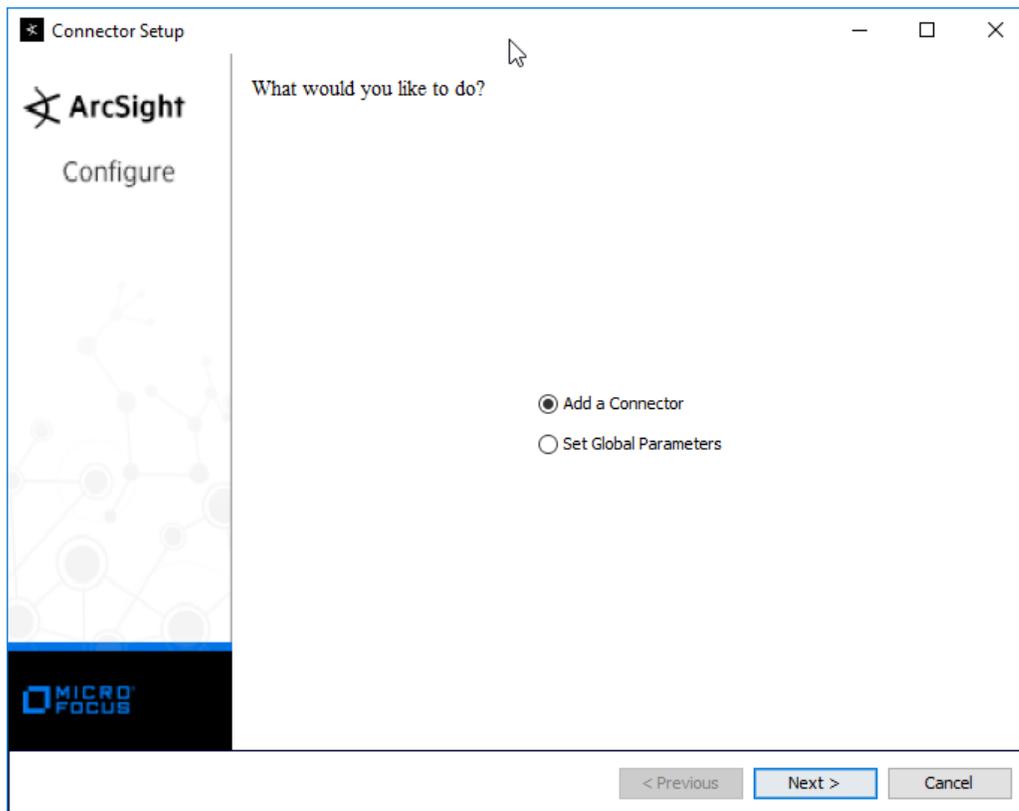
1463  
1464

5. Click **Next**.



1465  
1466  
1467

6. Click **Install**.
7. Select **Add a Connector**.

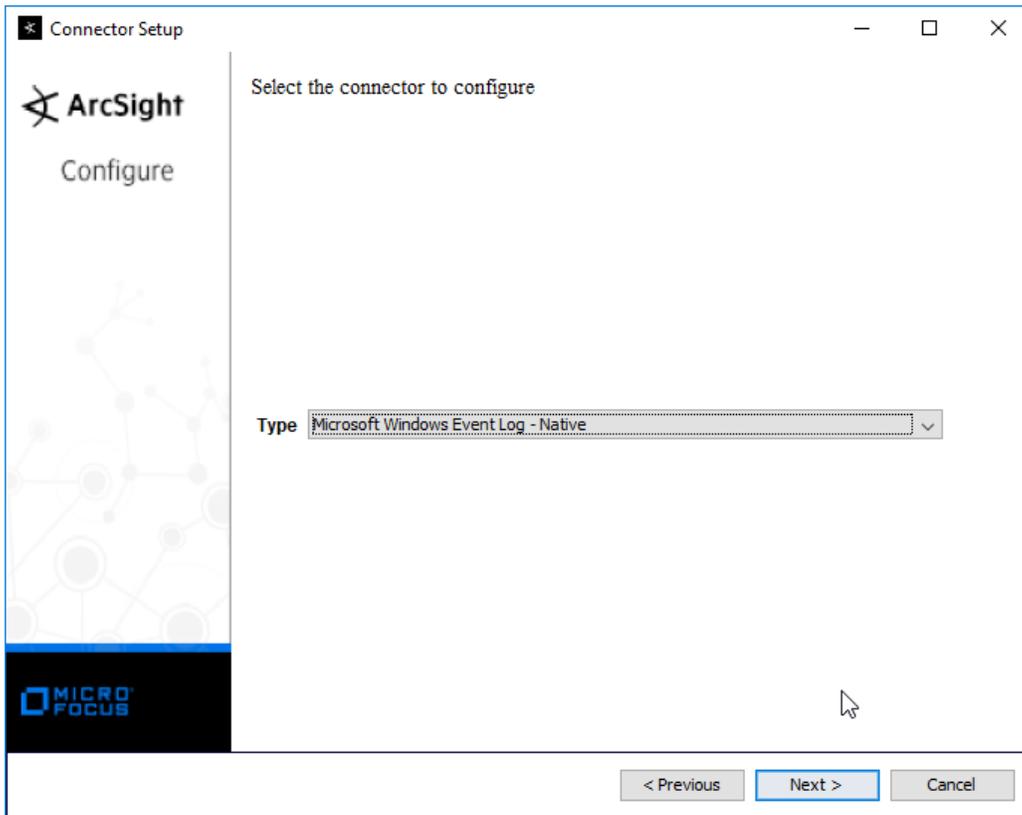


1468

1469

1470

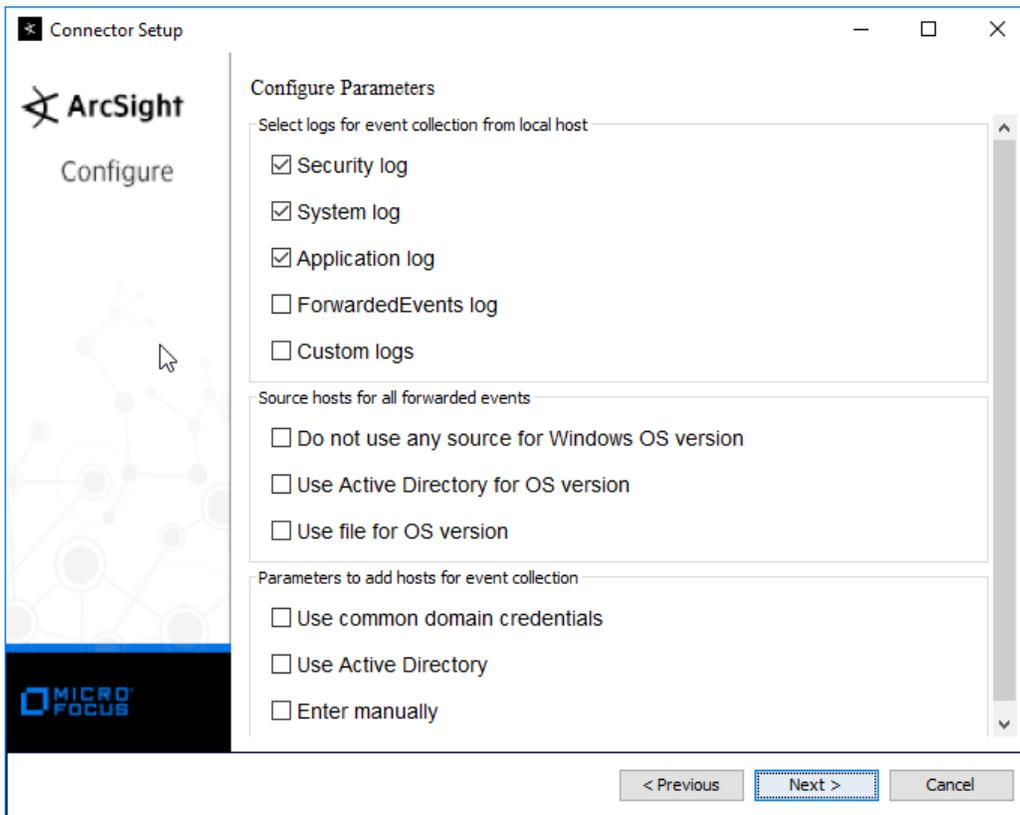
8. Click **Next**.
9. Select **Microsoft Windows Event Log–Native**.



1471

1472

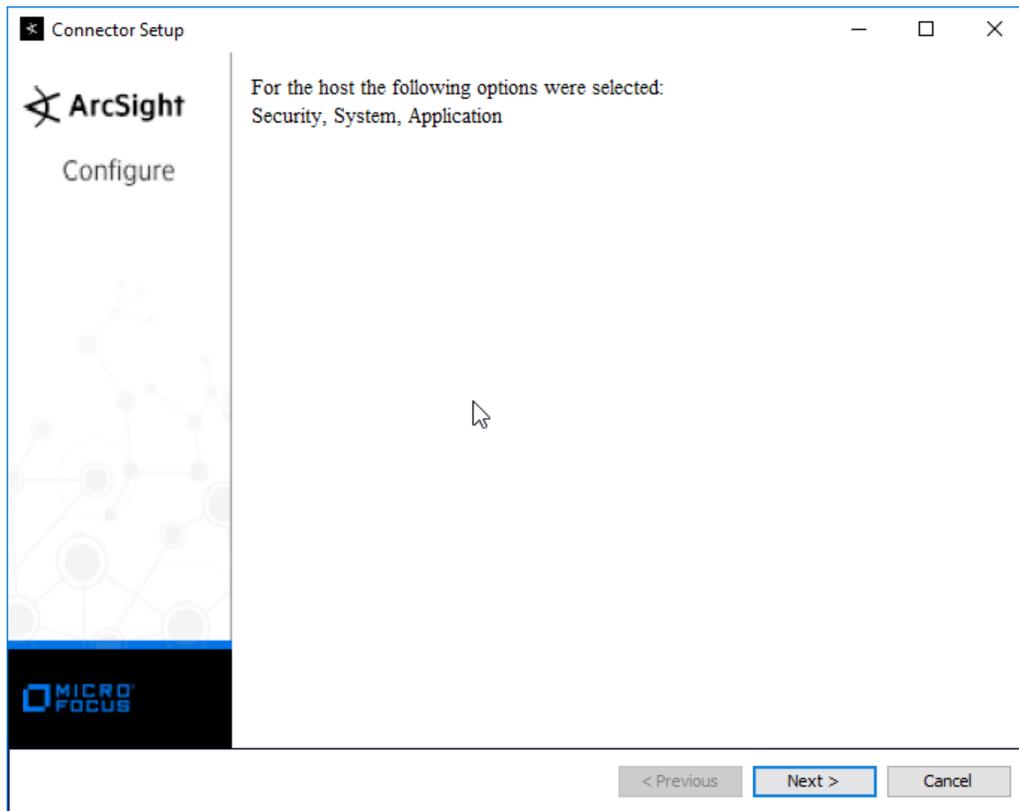
10. Click **Next**.



1473

1474

11. Click **Next**.



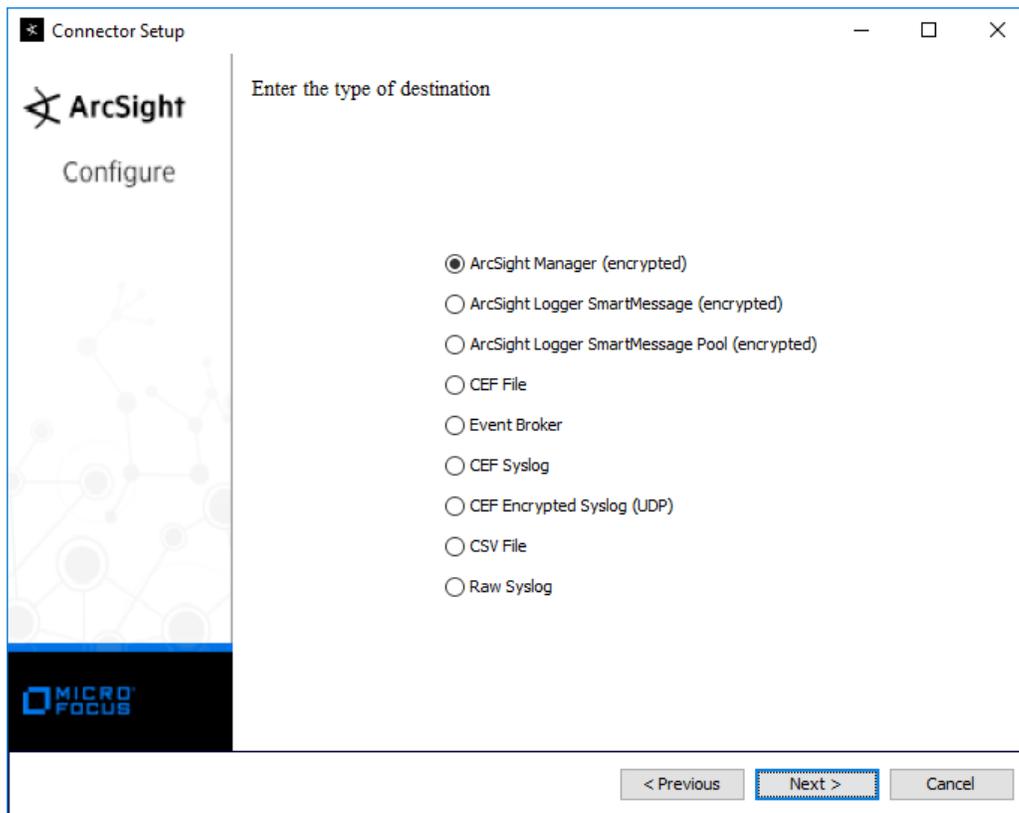
1475

1476

1477

12. Click **Next**.

13. Select **ArcSight Manager (encrypted)**.



1478

1479

1480

14. Click **Next**.

15. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.

Connector Setup

ArcSight  
Configure

Enter the destination parameters

Manager Hostname	arcsight-esm
Manager Port	8443
User	administrator
Password	••••••••
AUP Master Destination	false
Filter Out All Events	false
Enable Demo CA	false

< Previous   Next >   Cancel

1481

1482

1483

16. Click **Next**.17. Enter identifying details about the system (only **Name** is required).

Connector Setup

ArcSight  
Configure

Enter the connector details

Name: Windows10-1

Location:

DeviceLocation:

Comment: Windows10-1 Client

< Previous   Next >   Cancel

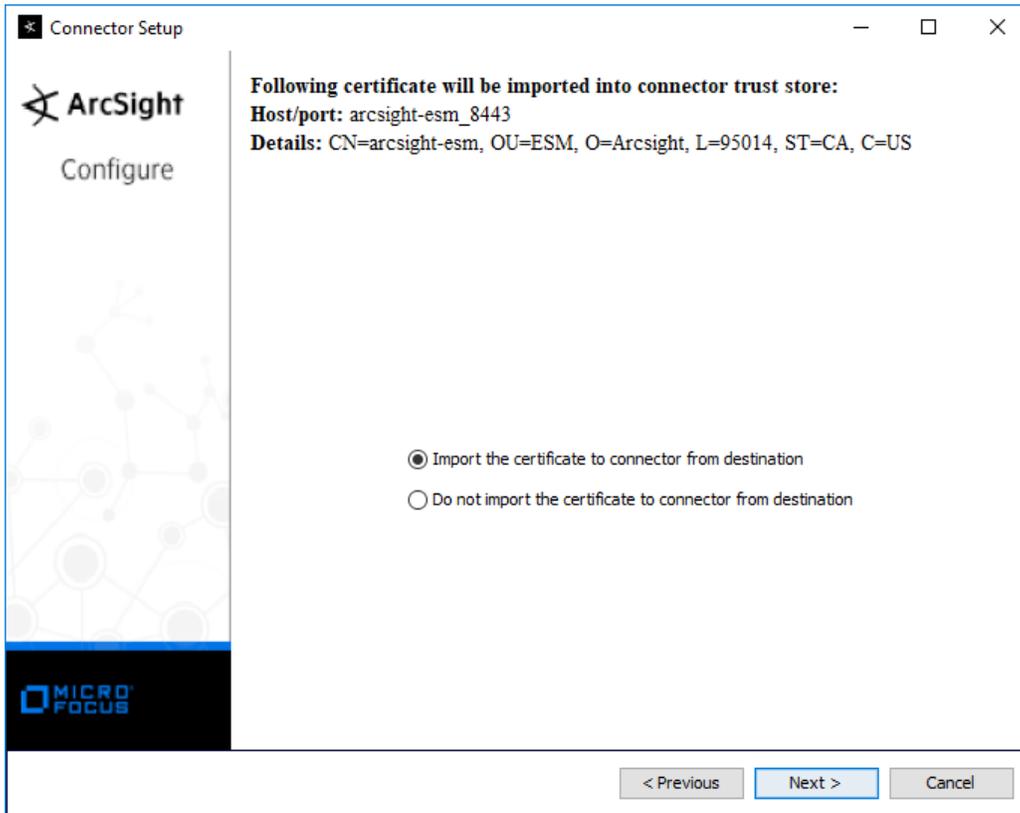
1484

1485

1486

18. Click **Next**.

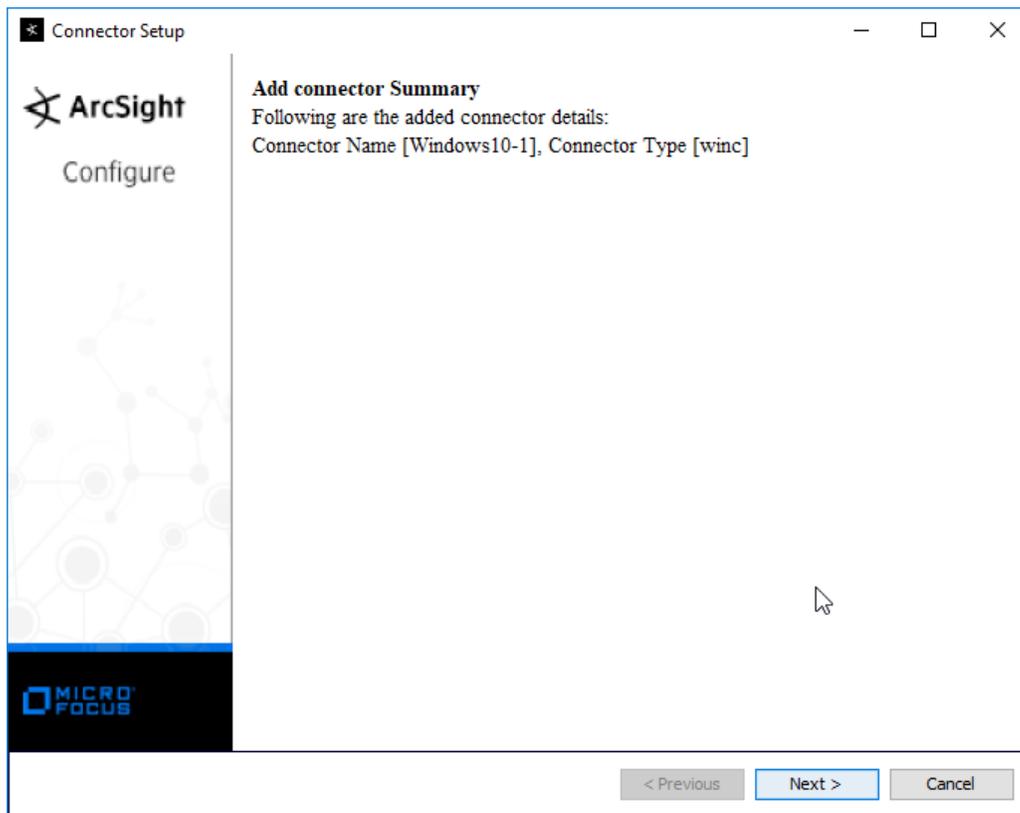
19. Select **Import the certificate to connector from destination**.



1487

1488

20. Click **Next**.



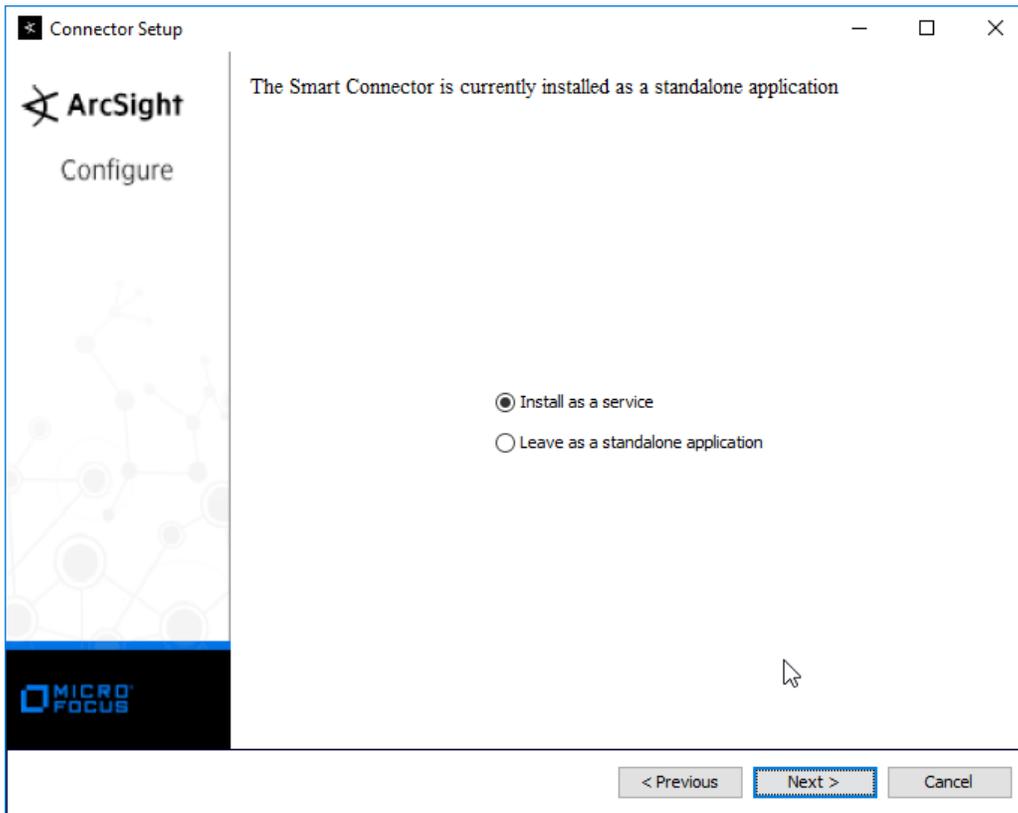
1489

1490

1491

21. Click **Next**.

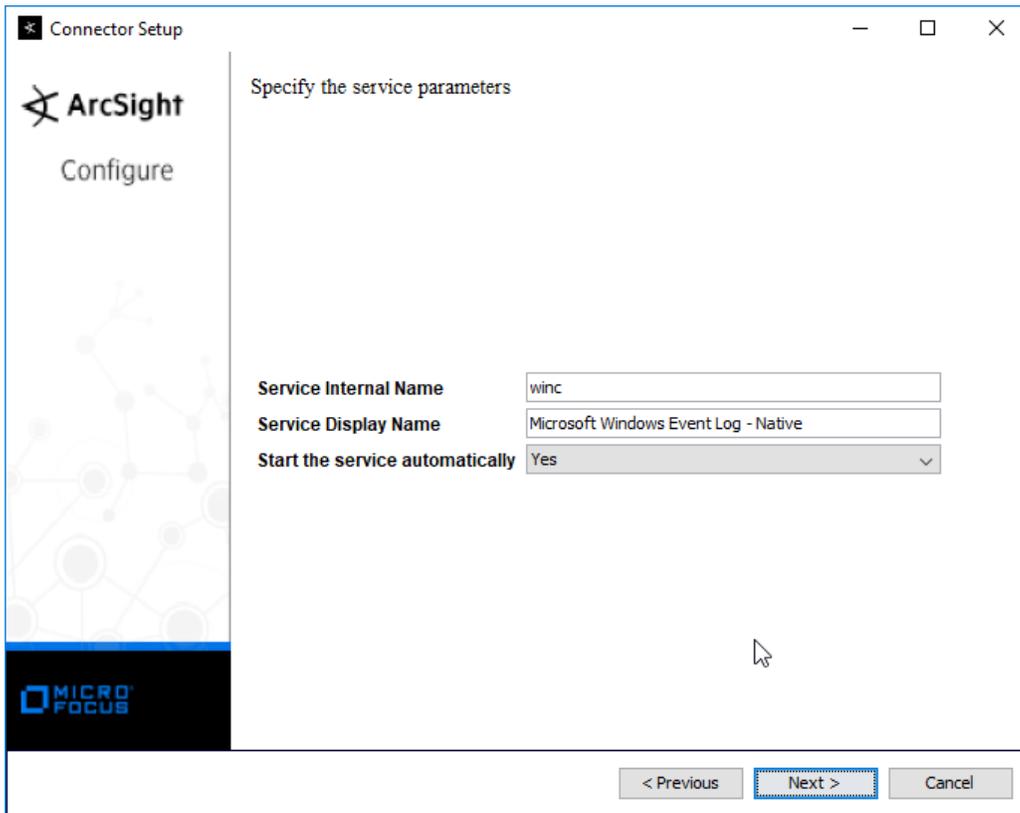
22. Select **Install as a service**.



1492

1493

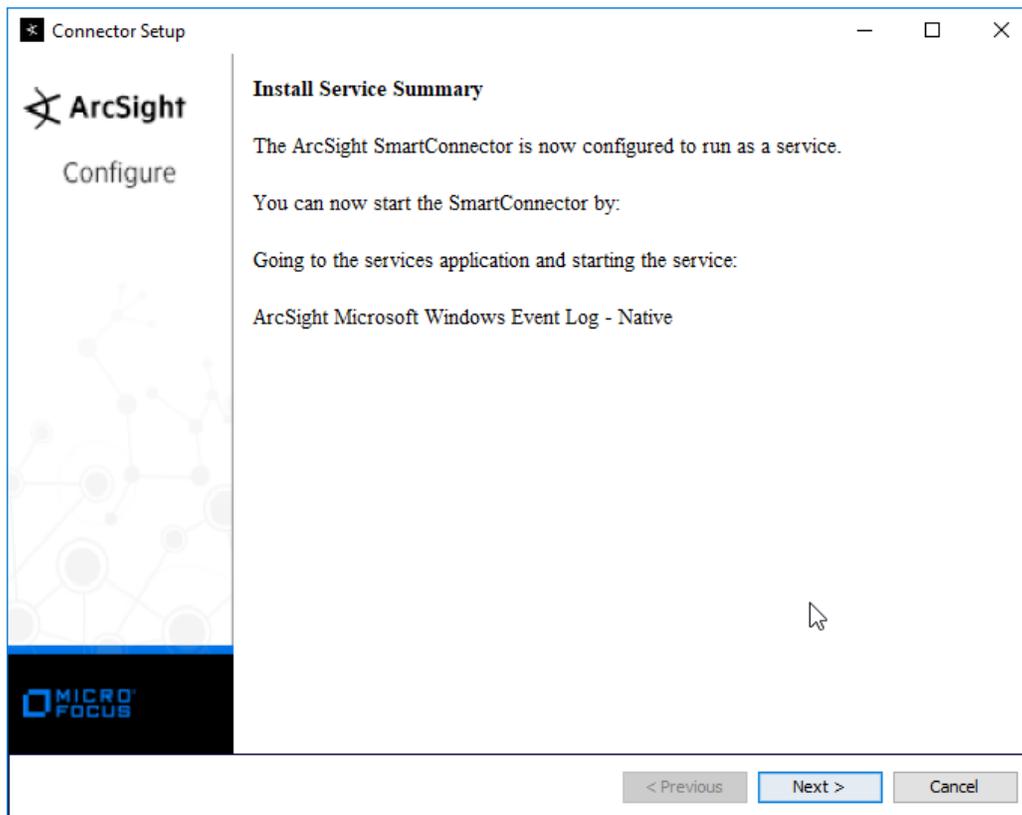
23. Click **Next**.



1494

1495

24. Click **Next**.



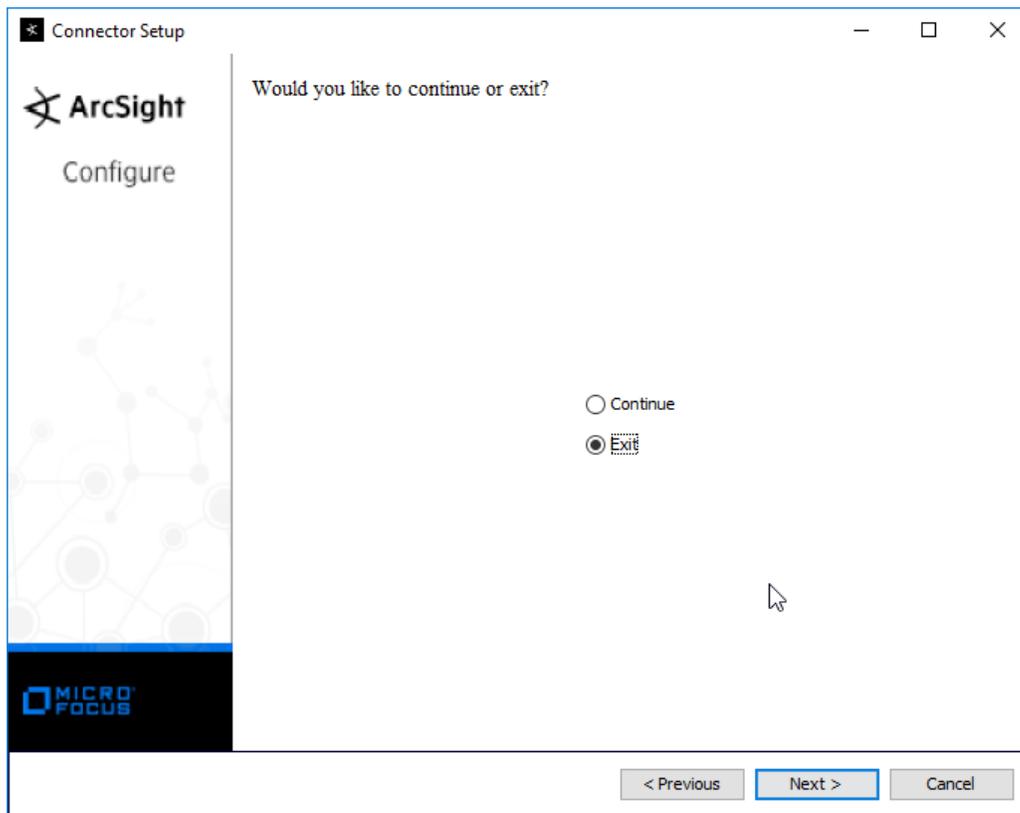
1496

1497

1498

25. Click **Next**.

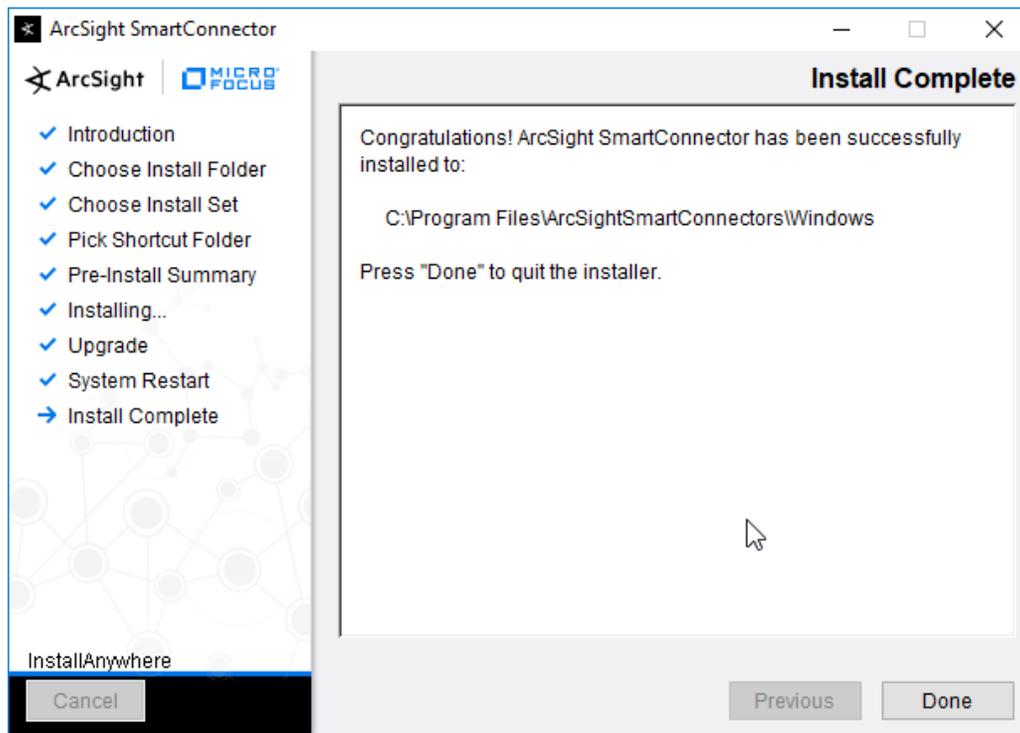
26. Select **Exit**.



1499

1500

27. Click **Next**.



1501

1502

28. Click **Done**.1503 

### 2.11.3 Install Individual ArcSight Ubuntu Connectors

1504

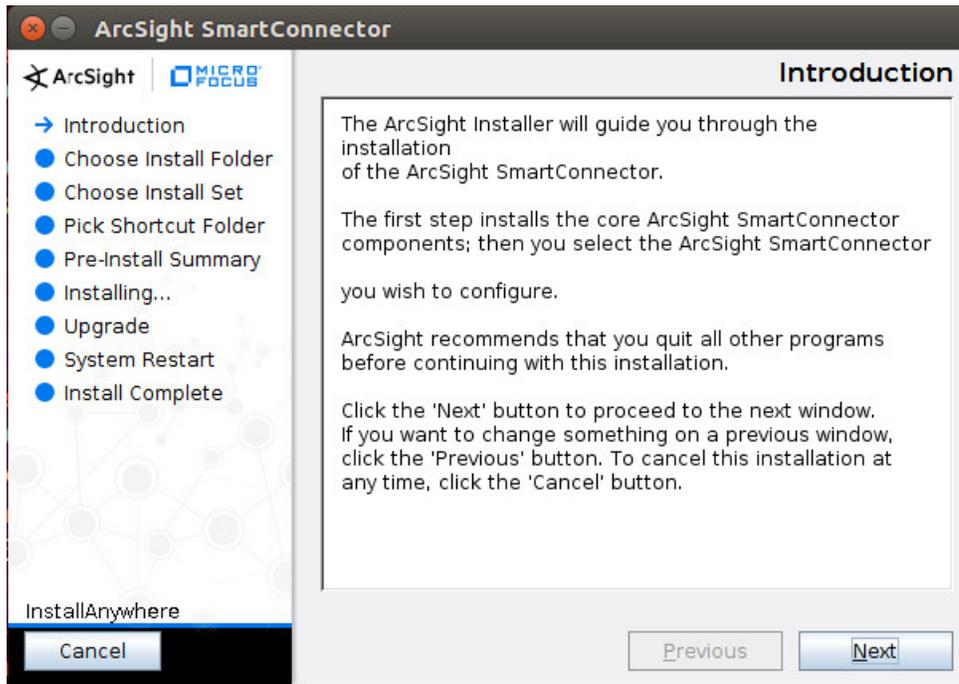
1. From the command line, run:

1505

&gt; sudo ./ArcSight-7.9.0.8084.0-Connector-Linux64.bin

1506

2. Enter the password if prompted.



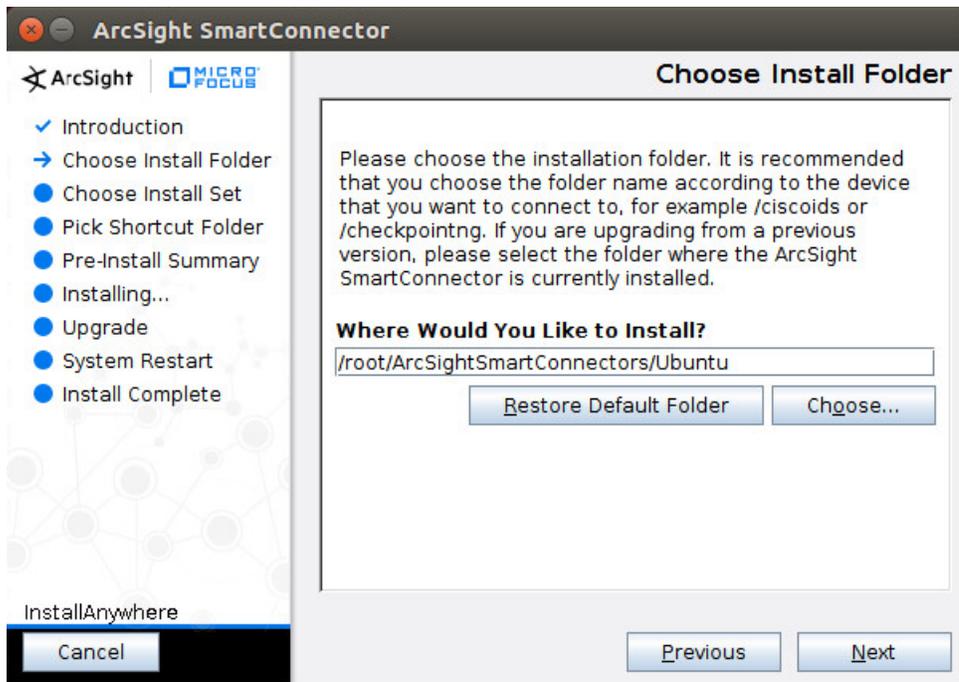
1507

1508

3. Click **Next**.

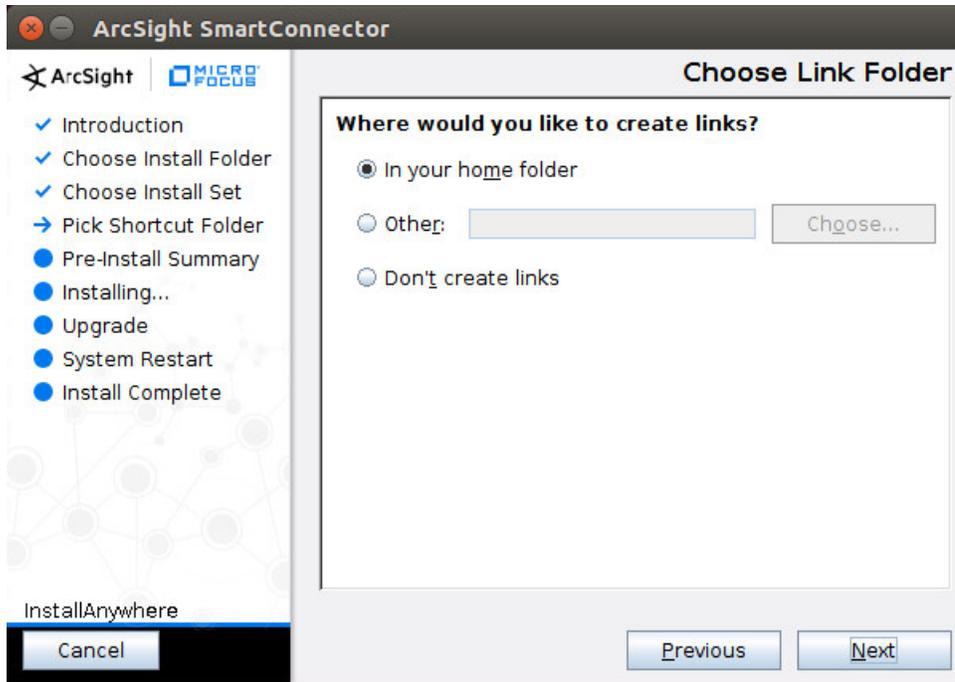
1509

4. Enter `/root/ArcSightSmartConnectors/Ubuntu`.



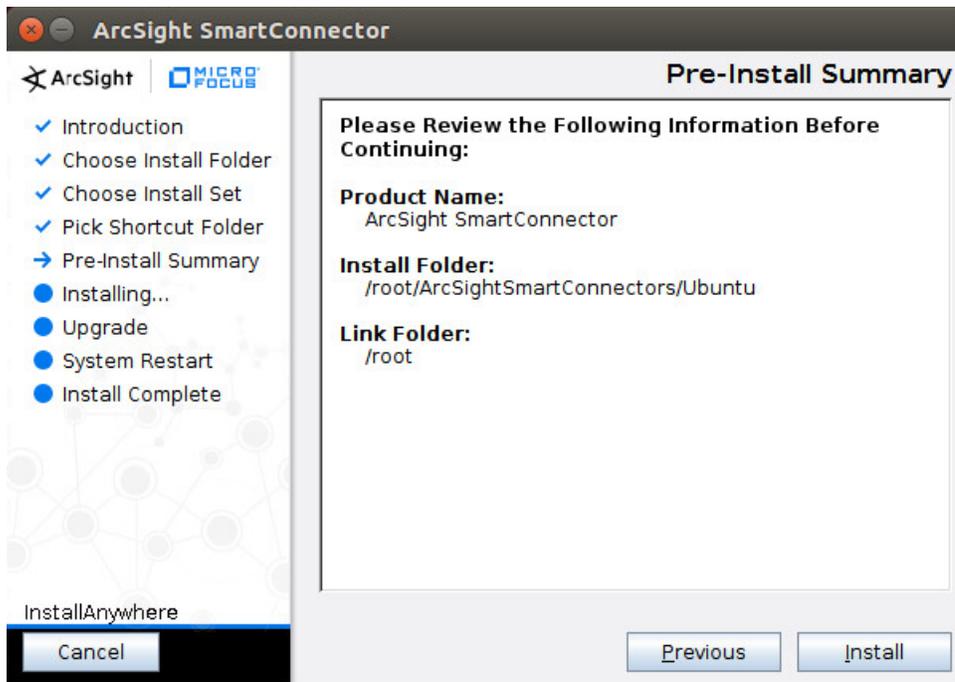
1510

1511 5. Click **Next**.



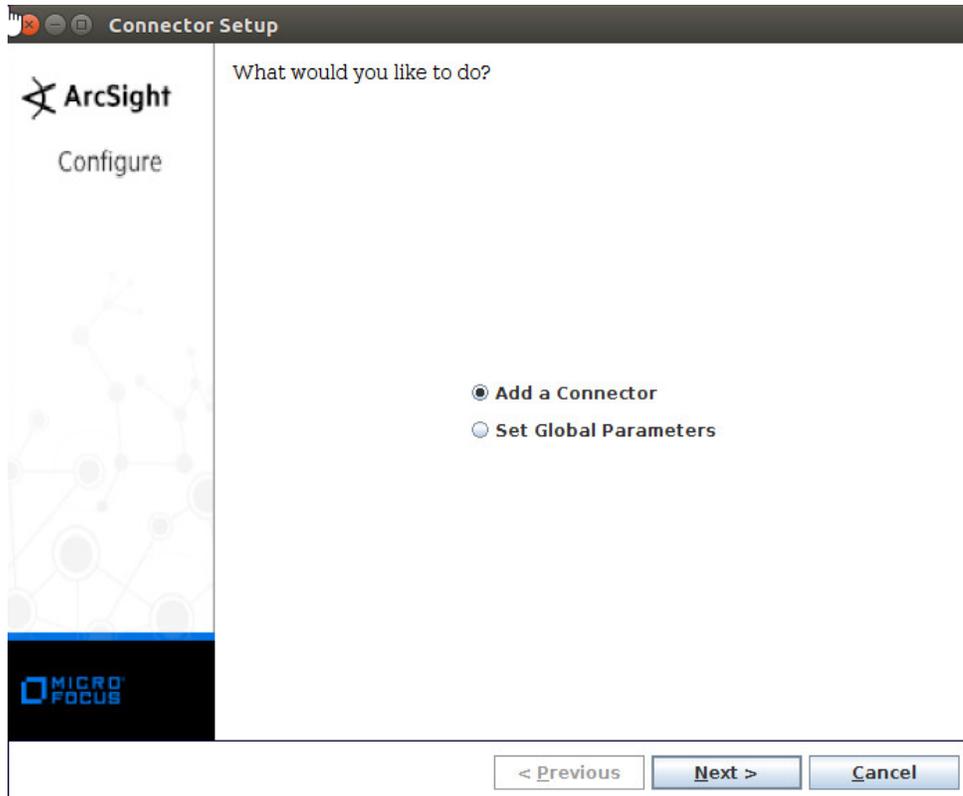
1512

1513 6. Click **Next**.

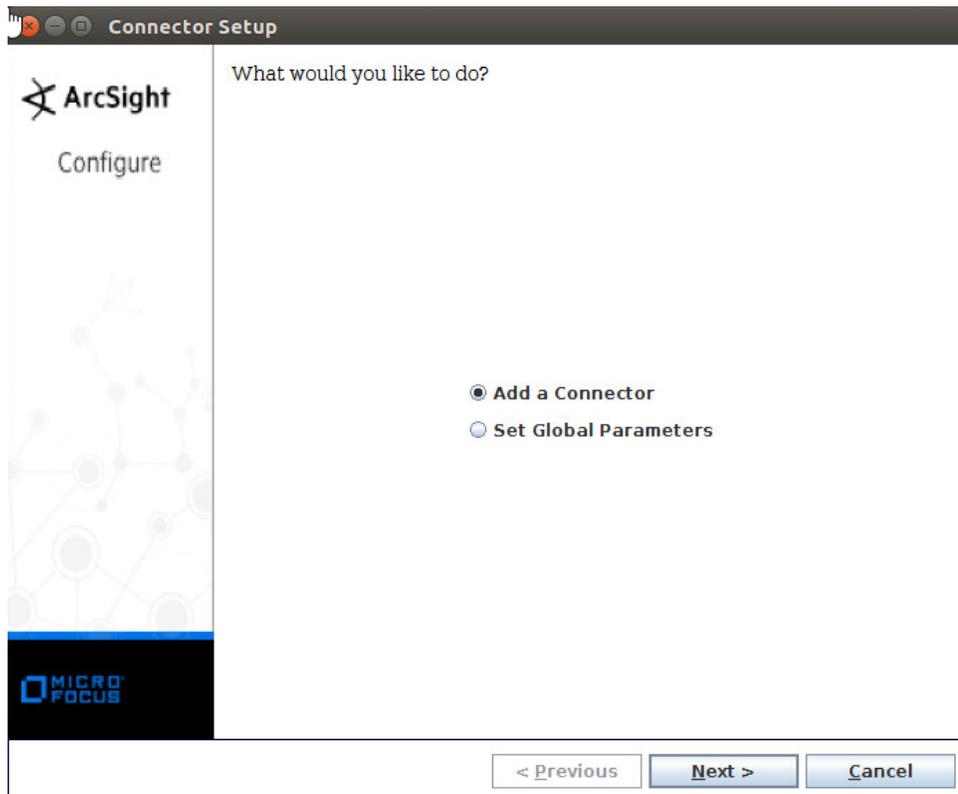


1514

- 1515 7. Click **Install**.
- 1516 8. Select **Add a Connector**.



- 1517
- 1518 9. Click **Next**.
- 1519 10. Select **Syslog File**.



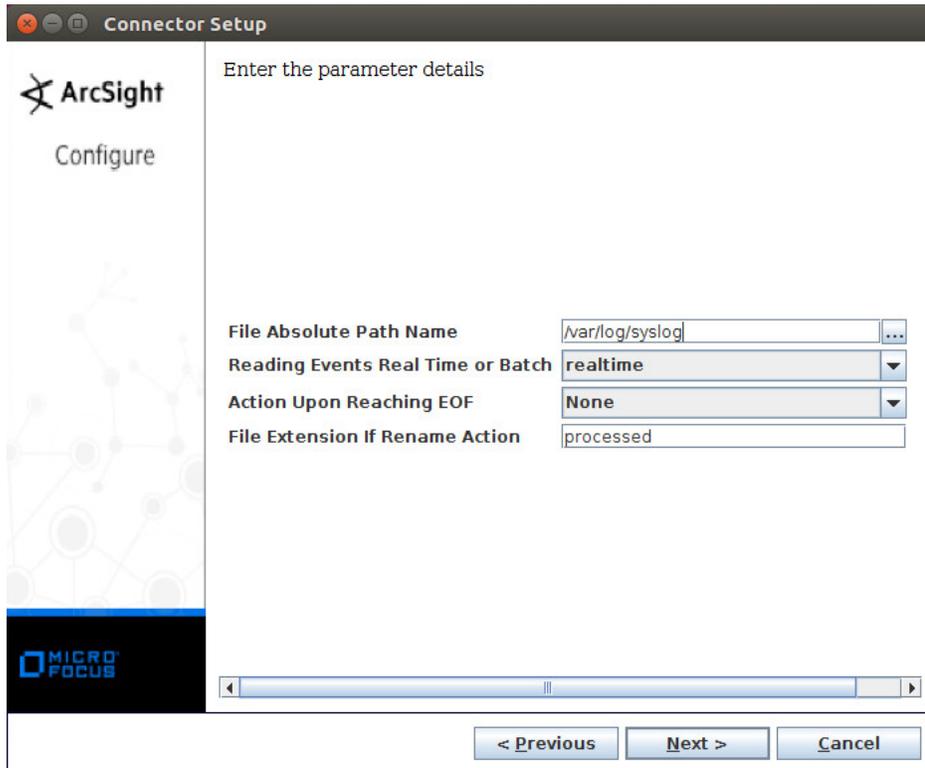
1520

1521

1522

11. Click **Next**.

12. Enter `/var/log/syslog` for the File Absolute Path Name.



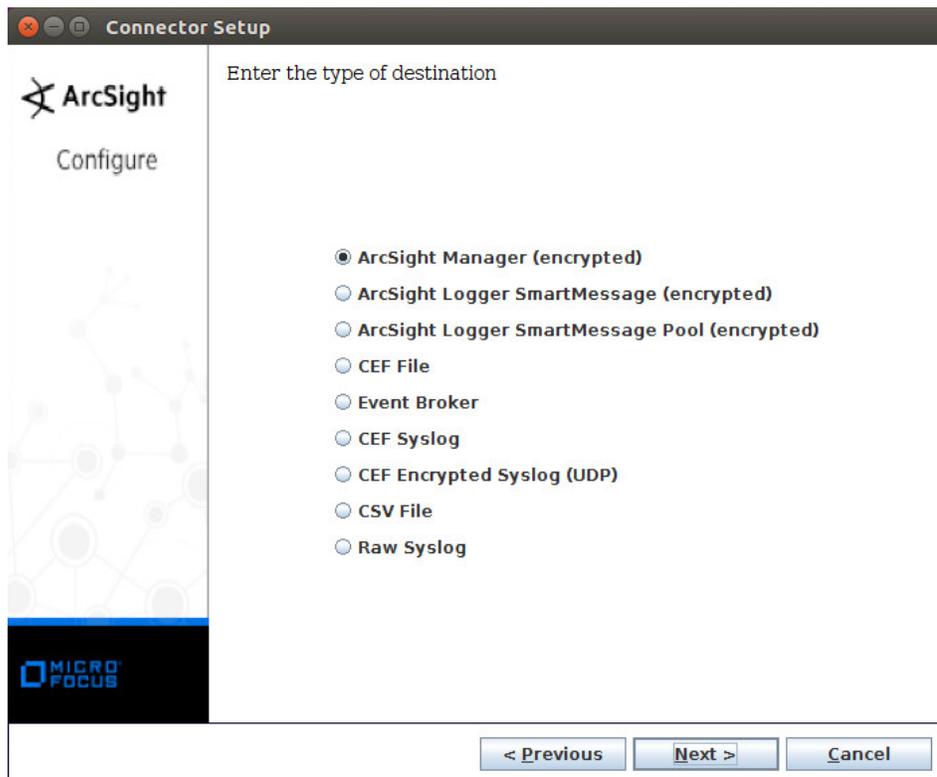
1523

1524

1525

13. Click **Next**.

14. Select **ArcSight Manager (encrypted)**.



1526

1527

1528

15. Click **Next**.

16. Enter the **hostname**, **port**, **username**, and **password** for ArcSight ESM.

Connector Setup

ArcSight  
Configure

Enter the destination parameters

Manager Hostname: arcsight-esm  
Manager Port: 8443  
User: administrator  
Password: .....  
AUP Master Destination: false  
Filter Out All Events: false  
Enable Demo CA: false

< Previous   Next >   Cancel

1529

1530

1531

17. Click **Next**.

18. Enter identifying details about the system (only **Name** is required).

Connector Setup

ArcSight  
Configure

Enter the connector details

Name

Location

DeviceLocation

Comment

< Previous   Next >   Cancel

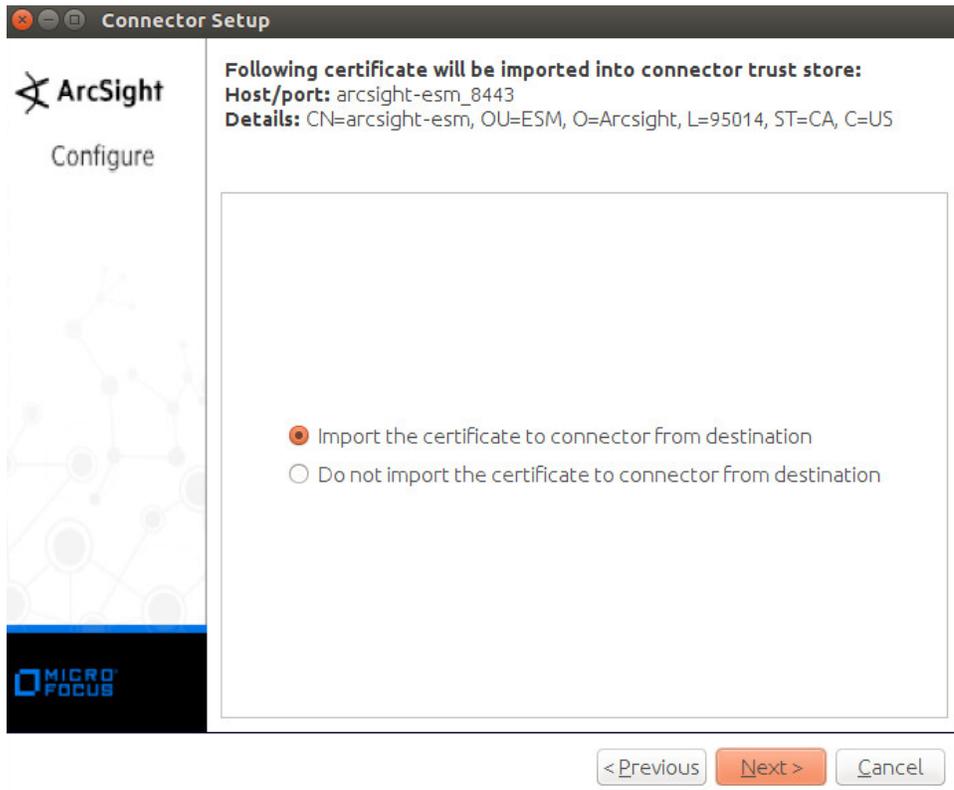
1532

1533

1534

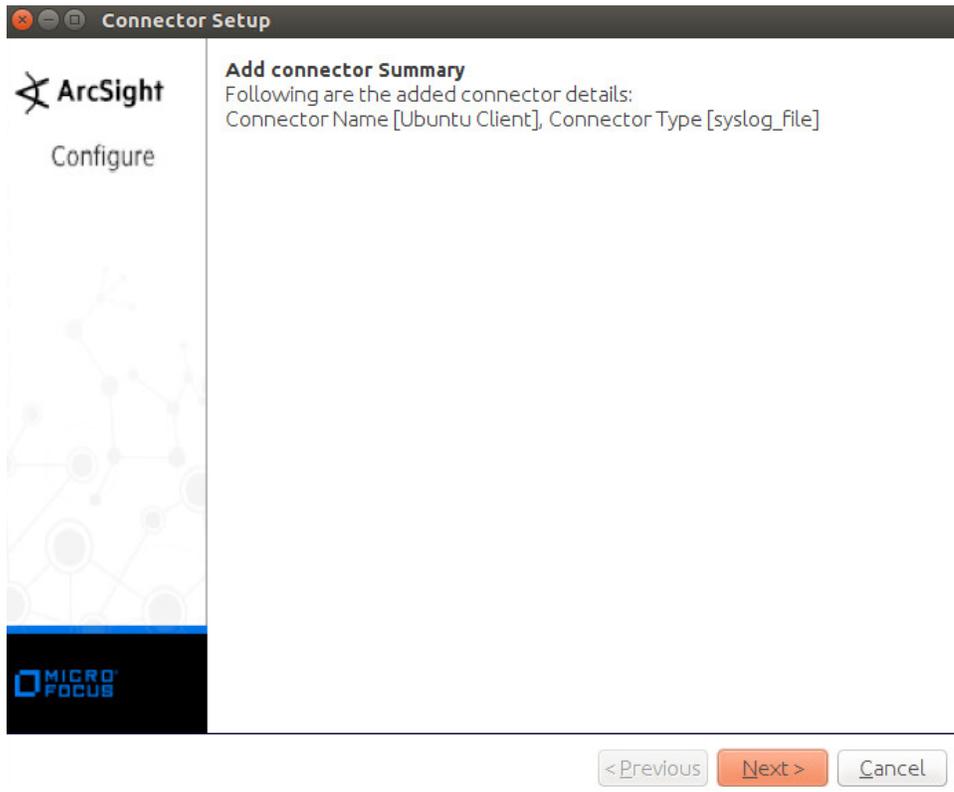
19. Click **Next**.

20. Select **Import the certificate to connector from destination**.



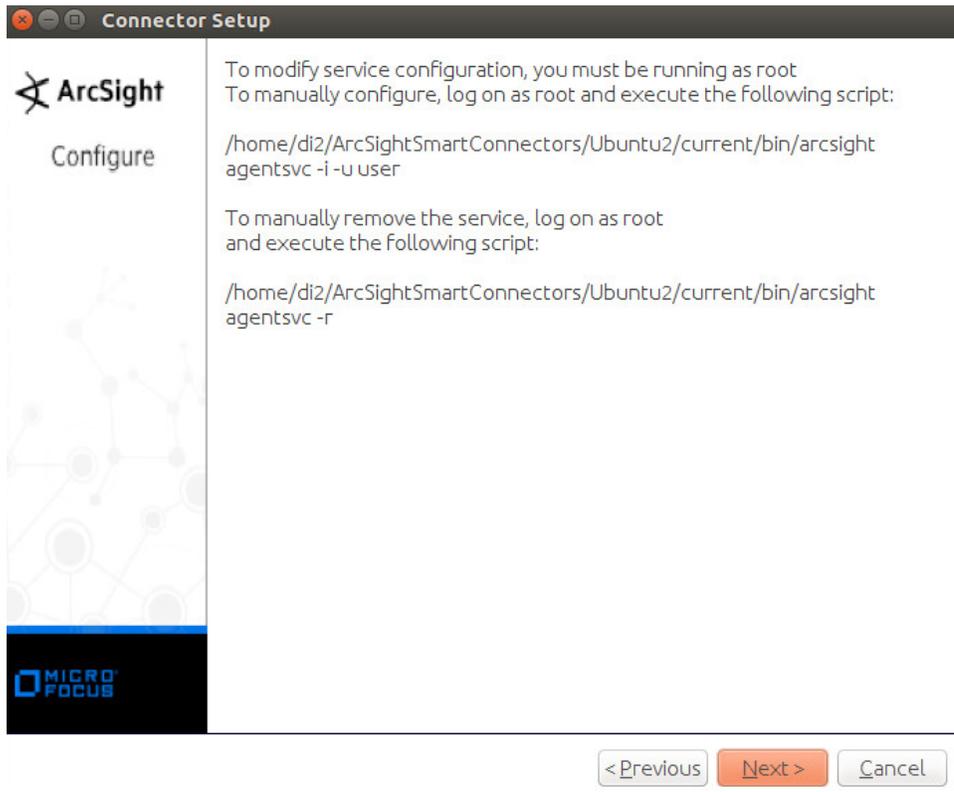
1535  
1536

21. Click **Next**.



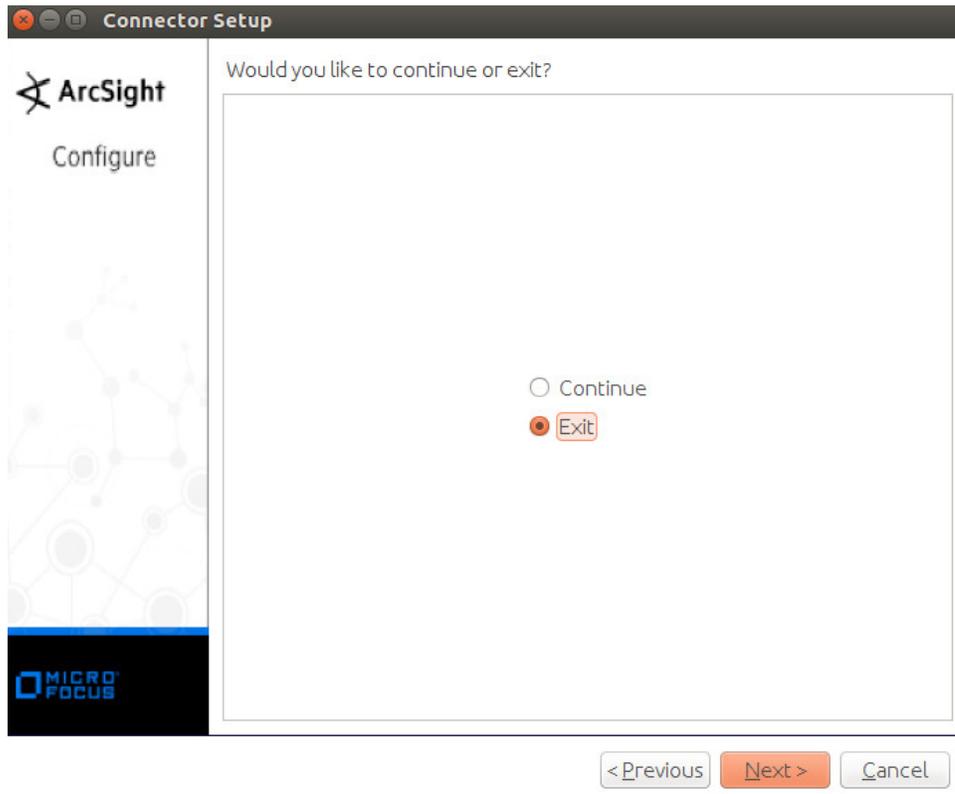
1537  
1538

22. Click **Next**.



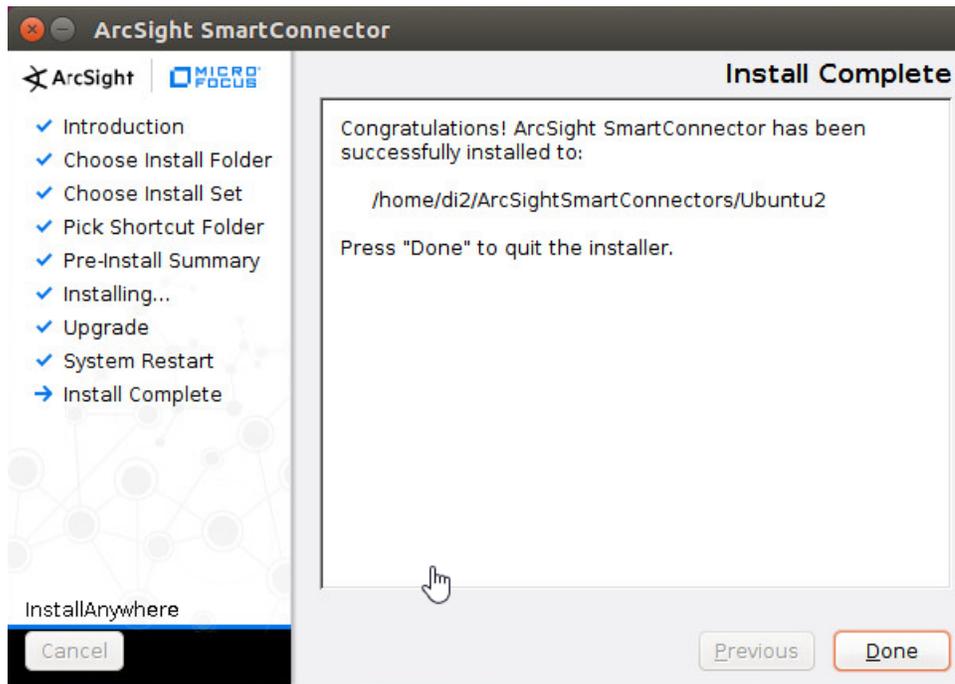
1539  
1540  
1541

- 23. Click **Next**.
- 24. Select **Exit**.



1542  
1543

25. Click **Next**.

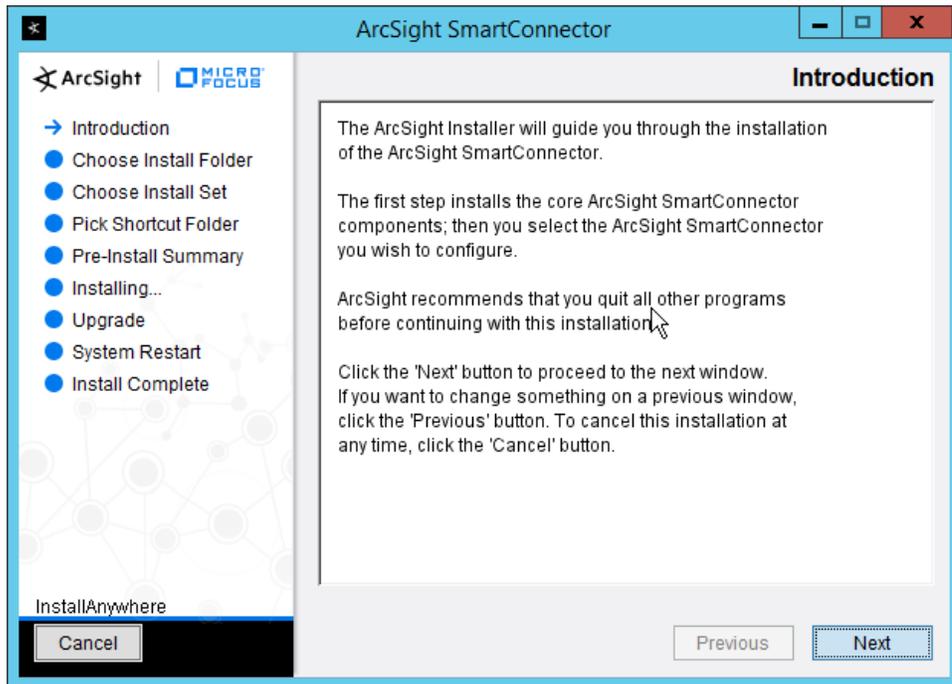


1544

1545 26. Click **Done**.

#### 1546 2.11.4 Install a Connector Server for ESM on Windows 2012 R2

1547 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.

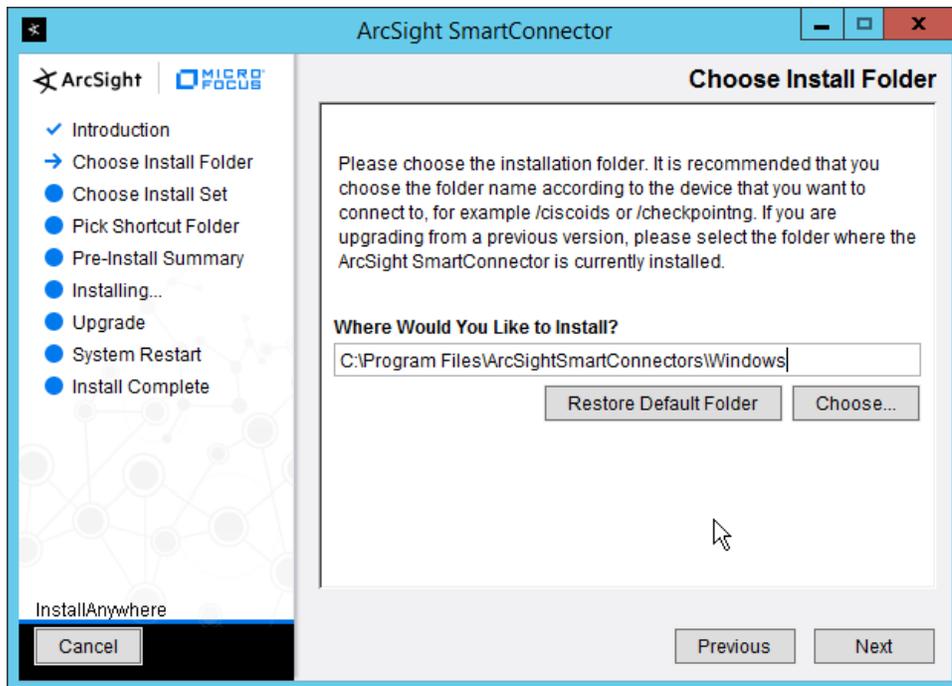


1548

1549

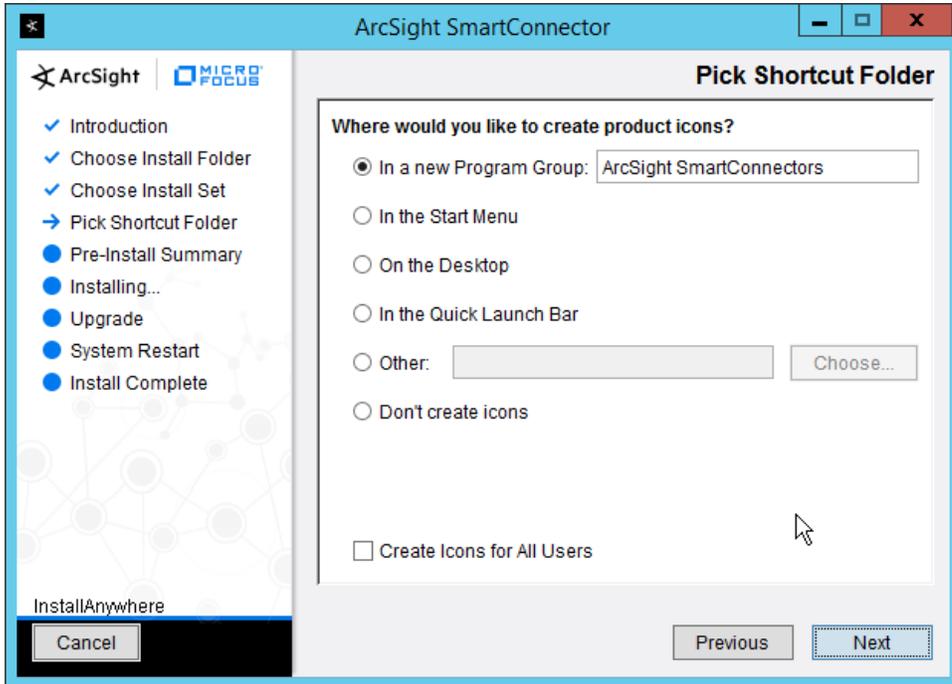
1550

2. Click **Next**.
3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



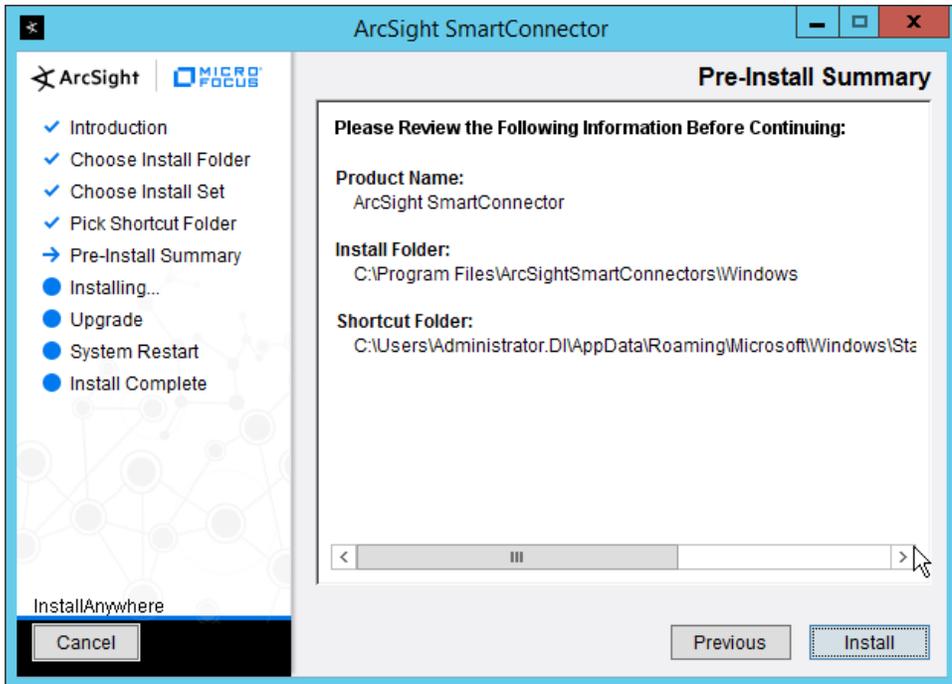
1551

1552 4. Click **Next**.



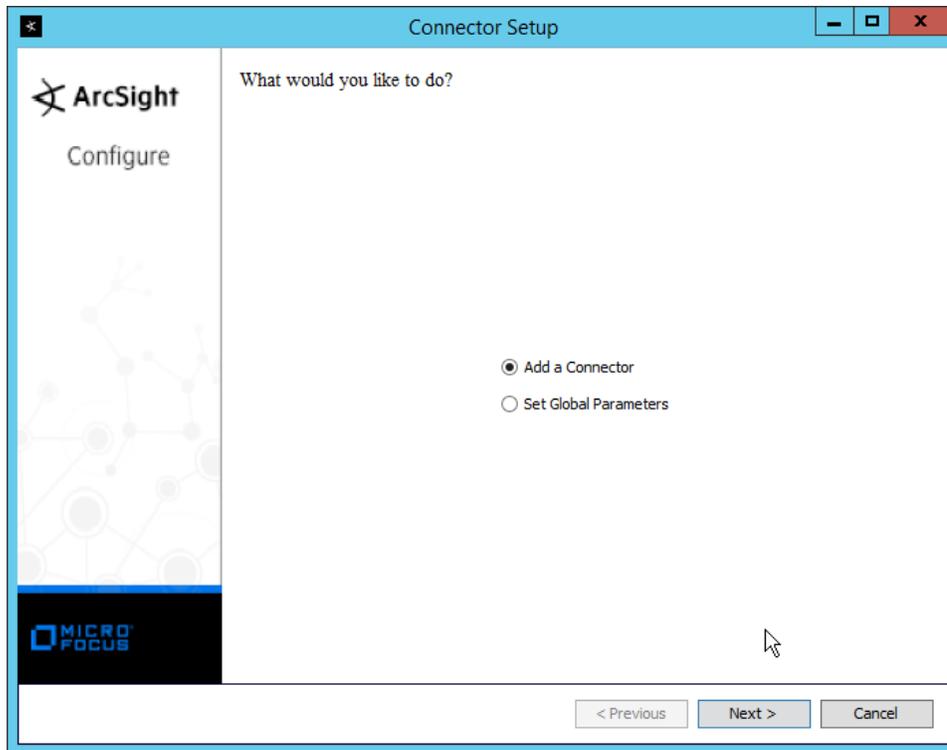
1553

1554 5. Click **Next**.

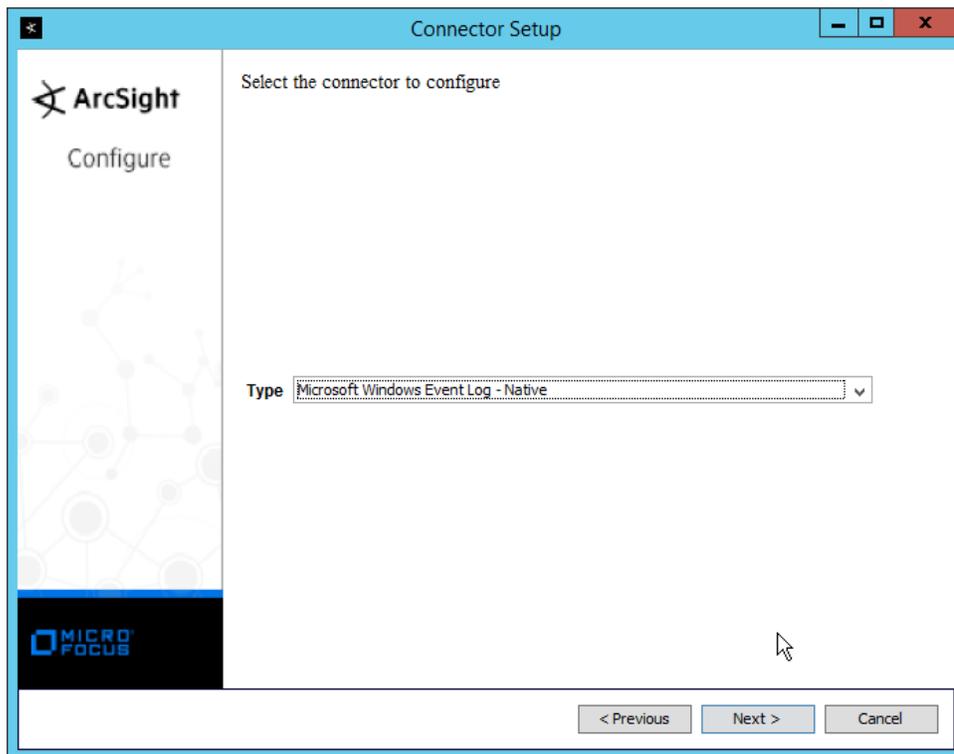


1555

- 1556 6. Click **Install**.
- 1557 7. Select **Add a Connector**.

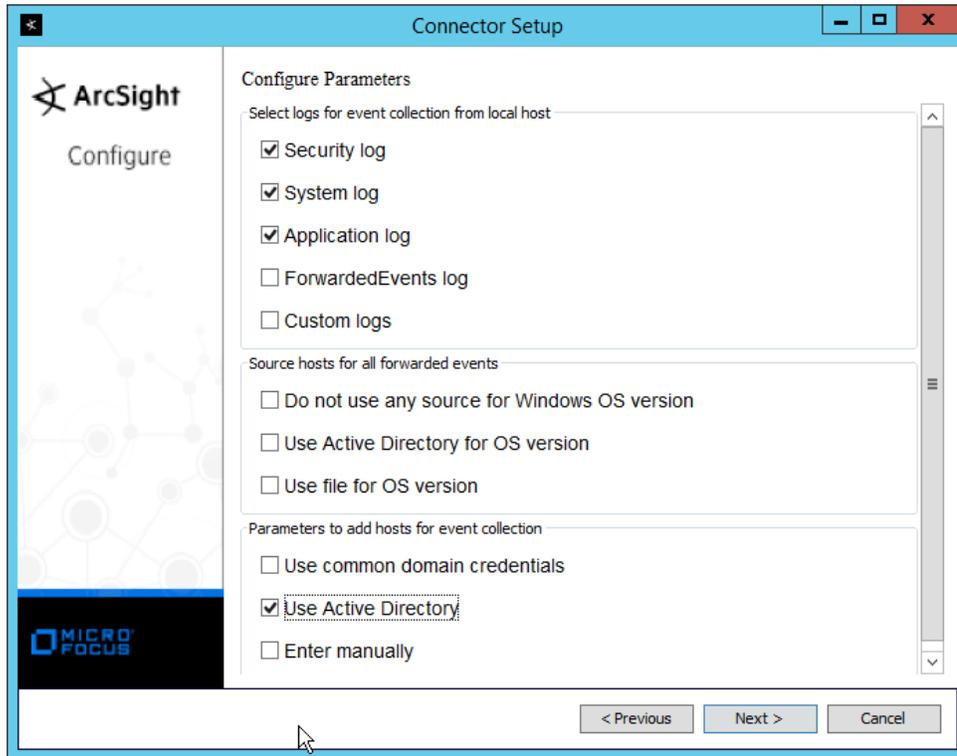


- 1558 8. Click **Next**.
- 1559 9. Select **Microsoft Windows Event Log–Native**.
- 1560



1561  
1562  
1563

10. Click **Next**.
11. Check the box next to **Use Active Directory**.



1564

1565

1566

1567

1568

12. Click **Next**.
13. Enter information about your Active Directory server. (It is recommended to create a new administrator account for ArcSight to use.)
14. Set **Use Active Directory host results for** to **Replace Hosts**.

Connector Setup

ArcSight  
Configure

Enter the parameter details

Domain Name: DI

Domain User Name: arcsight\_admin

Domain User Password: .....

Active Directory Domain: DI.IPDR

Active Directory User Name: arcsight\_admin

Active Directory User Password: .....

Active Directory Server: ad-dns.di.ipdr

Active Directory Filter: (&(cn=\*)(operatingsystem=\*)(whenevercreated=\*))

Active Directory Protocol: non\_ssl

Use Active Directory host results for: Replace Hosts

< Previous   Next >   Cancel

1569

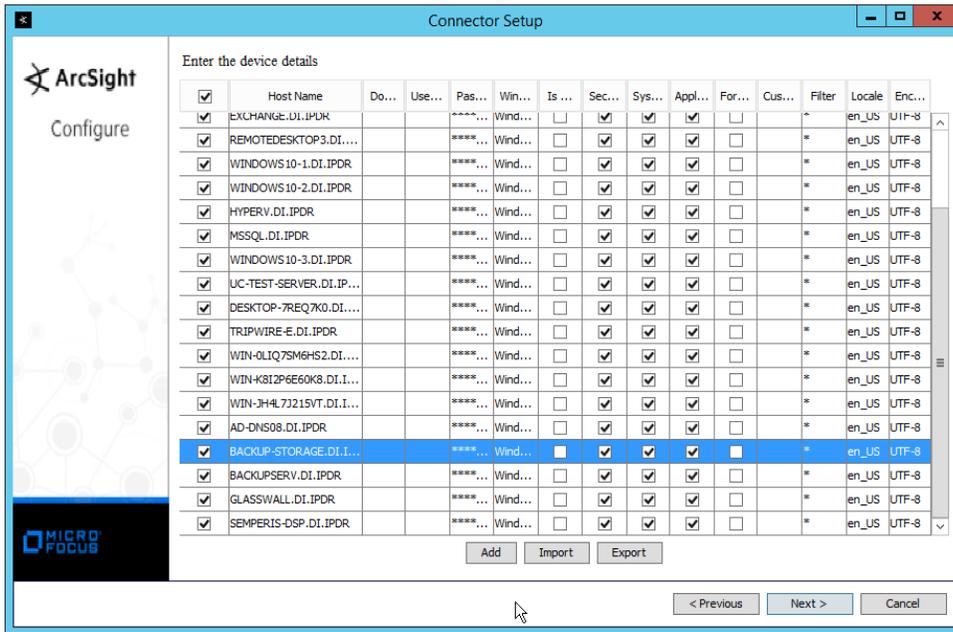
1570

15. Click **Next**.

1571

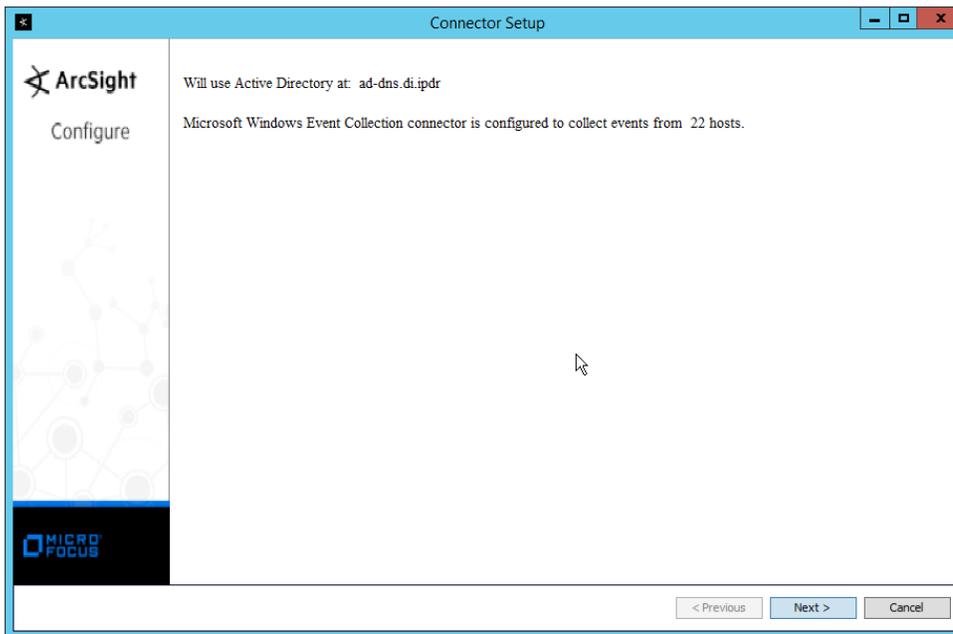
16. Check the boxes under any event types that should be forwarded to this connector, for each individual host, e.g., **Security, System, Application**.

1572



1573  
1574

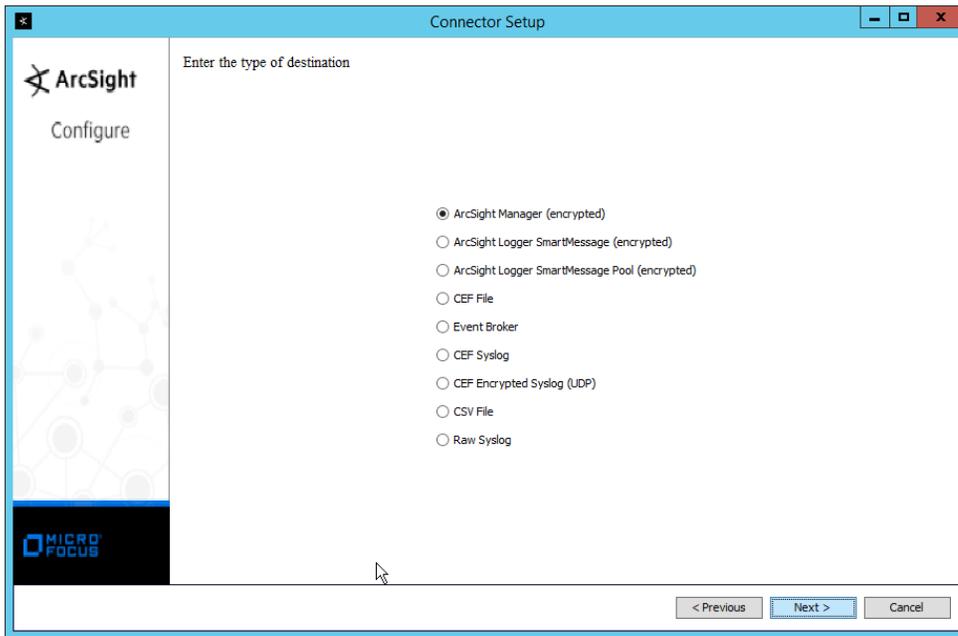
17. Click **Next**.



1575  
1576  
1577

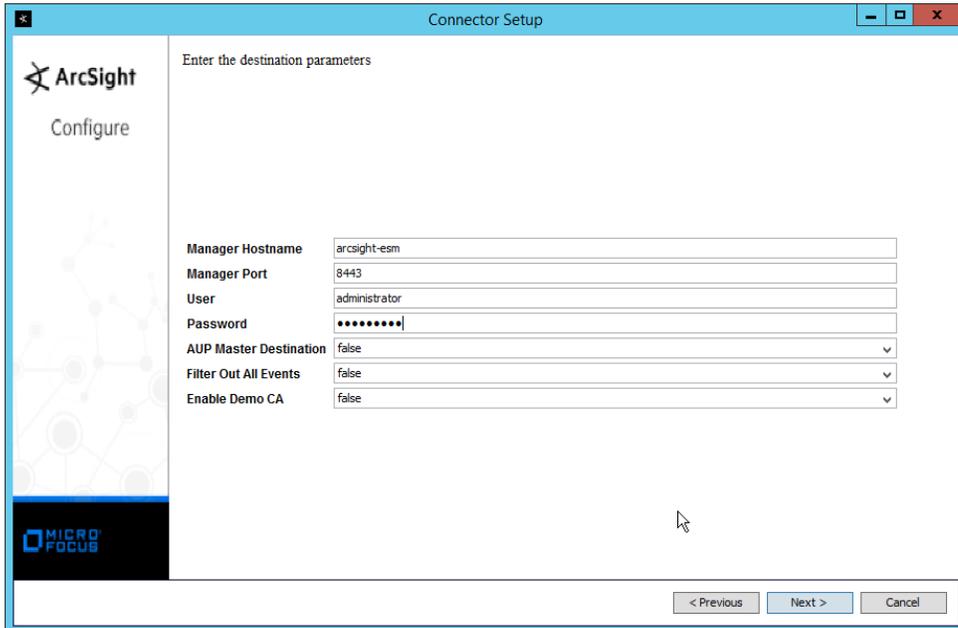
18. Click **Next**.

19. Select **ArcSight Manager (encrypted)**.



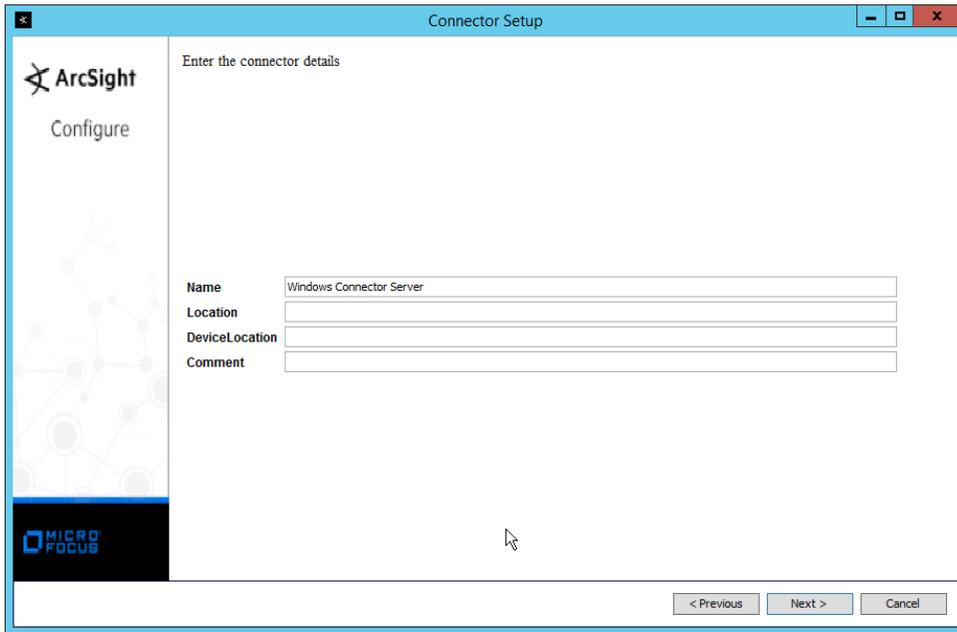
1578  
1579  
1580

- 20. Click **Next**.
- 21. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.



1581  
1582  
1583

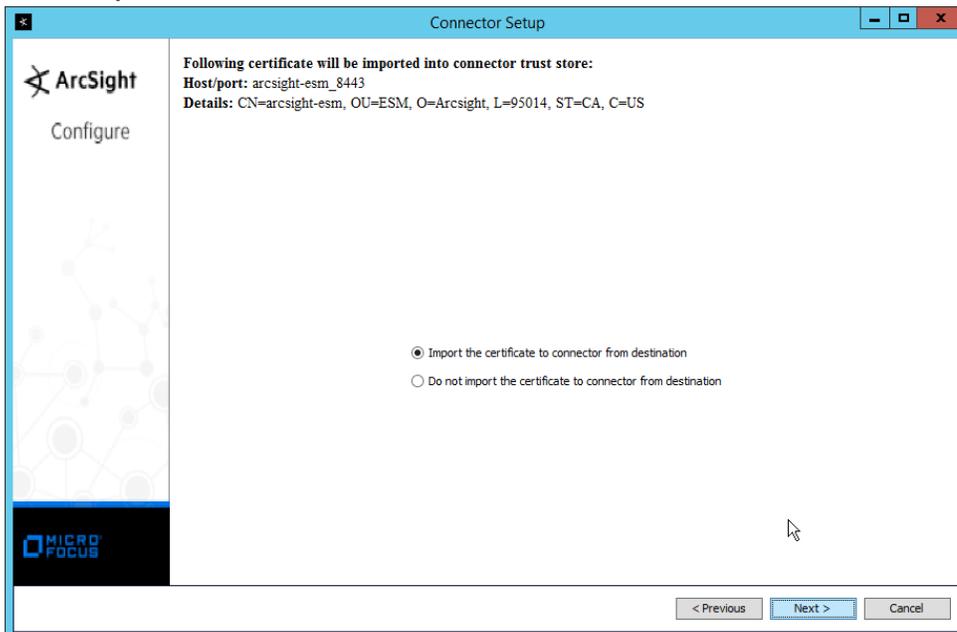
- 22. Click **Next**.
- 23. Enter identifying details about the system (only **Name** is required).



1584  
1585  
1586

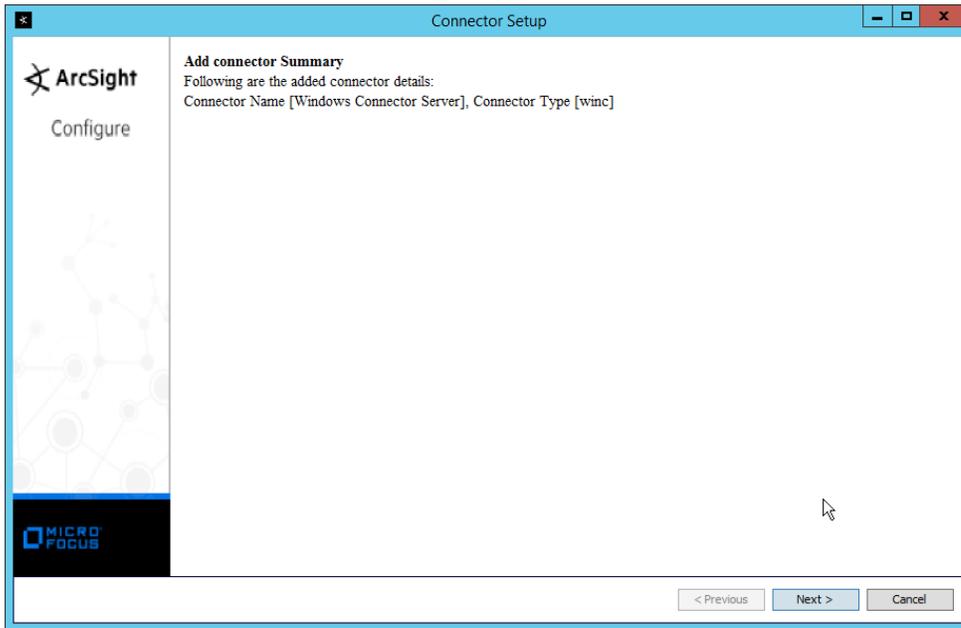
24. Click **Next**.

25. Select **Import the certificate to connector from destination**.



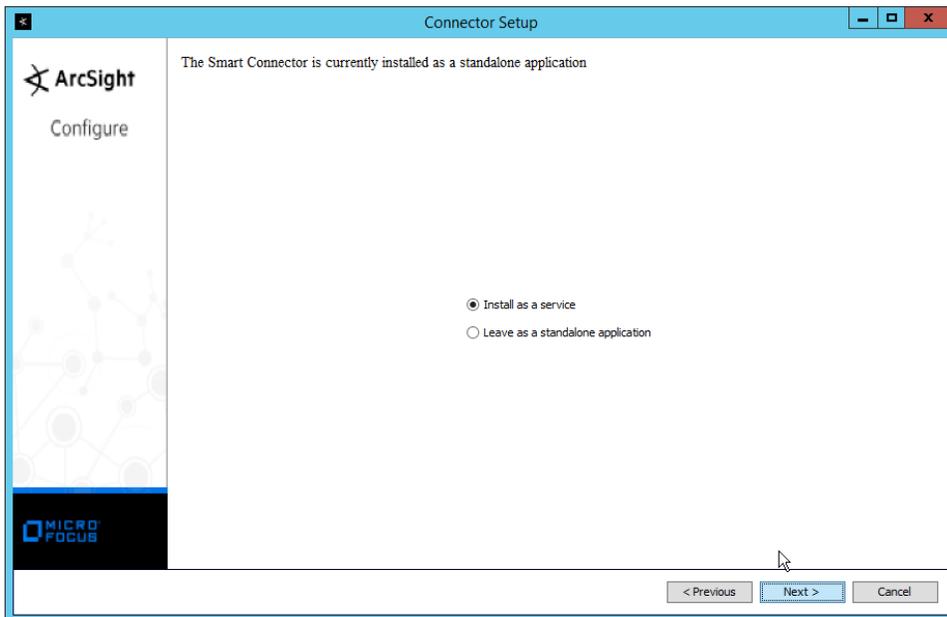
1587  
1588

26. Click **Next**.



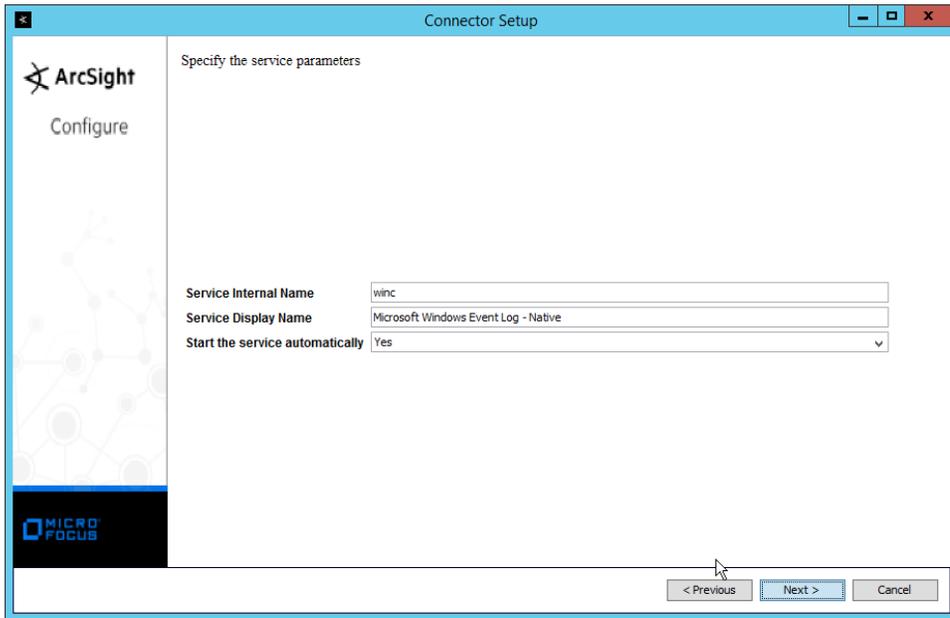
1589  
1590  
1591

- 27. Click **Next**.
- 28. Select **Install as a service**.



1592  
1593

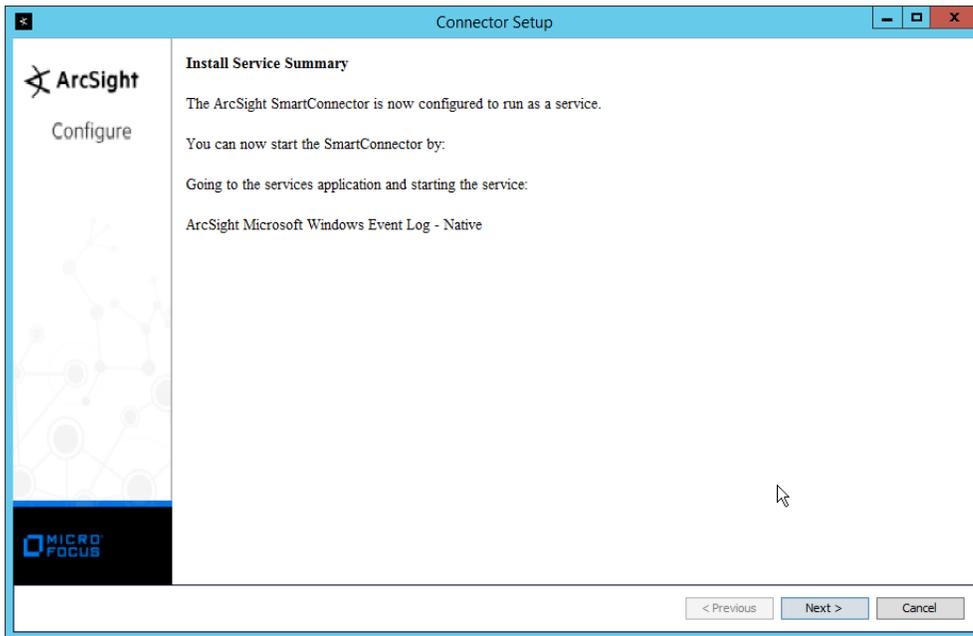
- 29. Click **Next**.



1594

1595

30. Click **Next**.



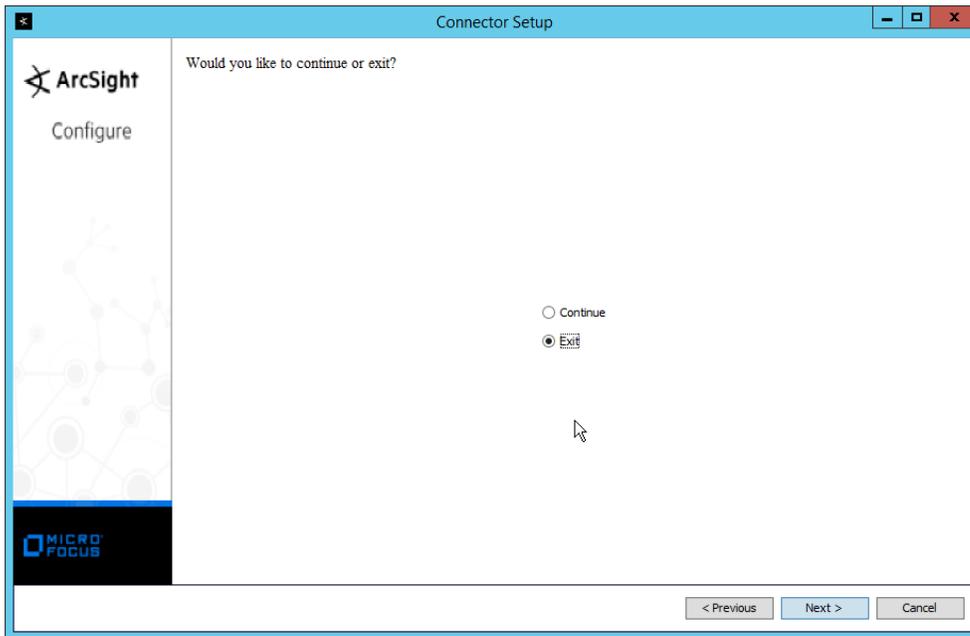
1596

1597

1598

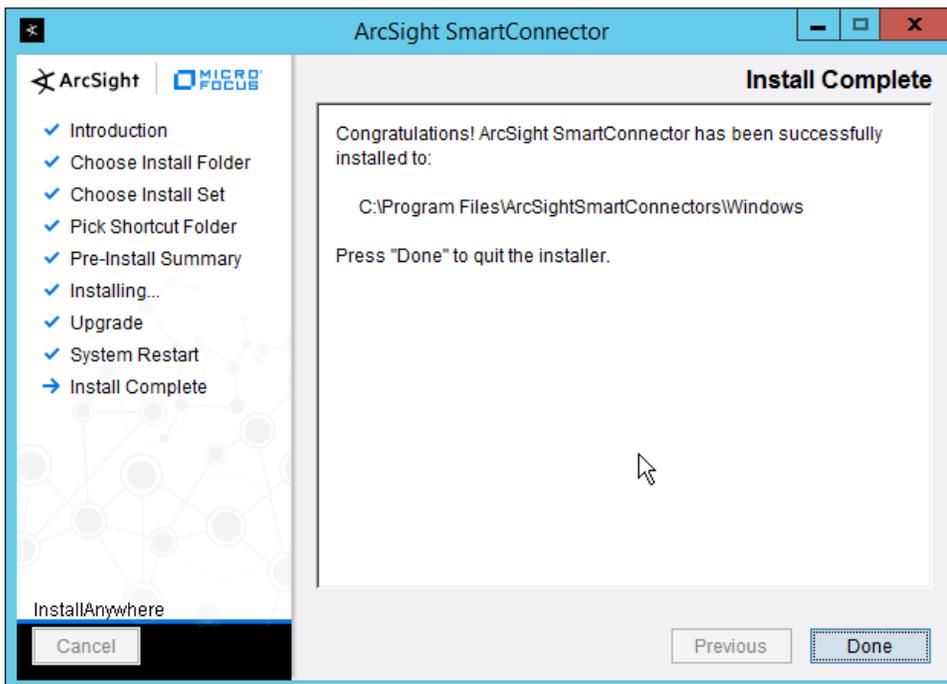
31. Click **Next**.

32. Select **Exit**.



1599  
1600

33. Click **Next**.



1601  
1602  
1603  
1604

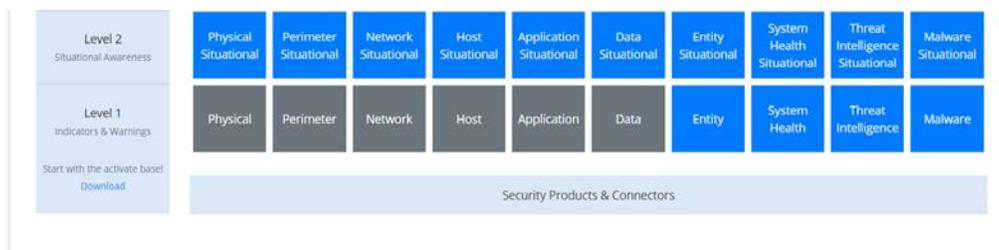
34. Click **Done**.

35. Note: Ensure that all machines selected do not block traffic from this device through their firewalls.

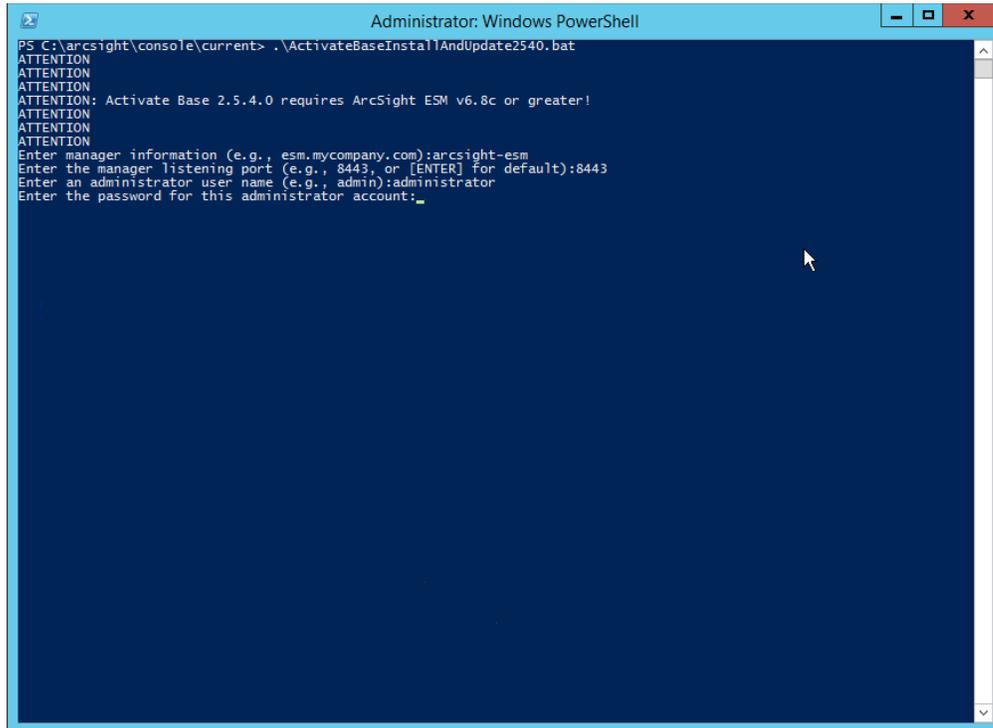
## 1605 2.11.5 Install Preconfigured Filters for ArcSight

### 1606 2.11.5.1 Install Activate Base

- 1607 1. Go to the ArcSight Content Brain web application (<https://arcsightcontentbrain.com/app/>) and  
 1608 log in. This page allows you to keep track of packages to be installed—what packages should be  
 1609 installed depends on the needs of the organization, but the “Activate Base” is required for all  
 1610 products.



- 1611
- 1612 2. Click the **Download** link for the Activate Base. (Note: This package should be installed on the  
 1613 ArcSight Console, not on the ESM.)
- 1614 3. Copy the contents of the zip file to ARCSIGHT\_HOME. The default for this is C:\arcsight\Con-  
 1615 sole\current, assuming a Windows Server.
- 1616 4. In PowerShell, navigate to the ARCSIGHT\_HOME directory (C:\arcsight\Console\current) and  
 1617 run:  
 1618 > .\ActivateBaseInstallAndUpdate2540.bat



```
Administrator: Windows PowerShell
PS C:\arcsight\console\current> .\ActivateBaseInstallAndUpdate2540.bat
ATTENTION
ATTENTION
ATTENTION
ATTENTION: Activate Base 2.5.4.0 requires ArcSight ESM v6.8c or greater!
ATTENTION
ATTENTION
ATTENTION
Enter manager information (e.g., esm.mycompany.com):arcsight-esm
Enter the manager listening port (e.g., 8443, or [ENTER] for default):8443
Enter an administrator user name (e.g., admin):administrator
Enter the password for this administrator account: _
```

1619

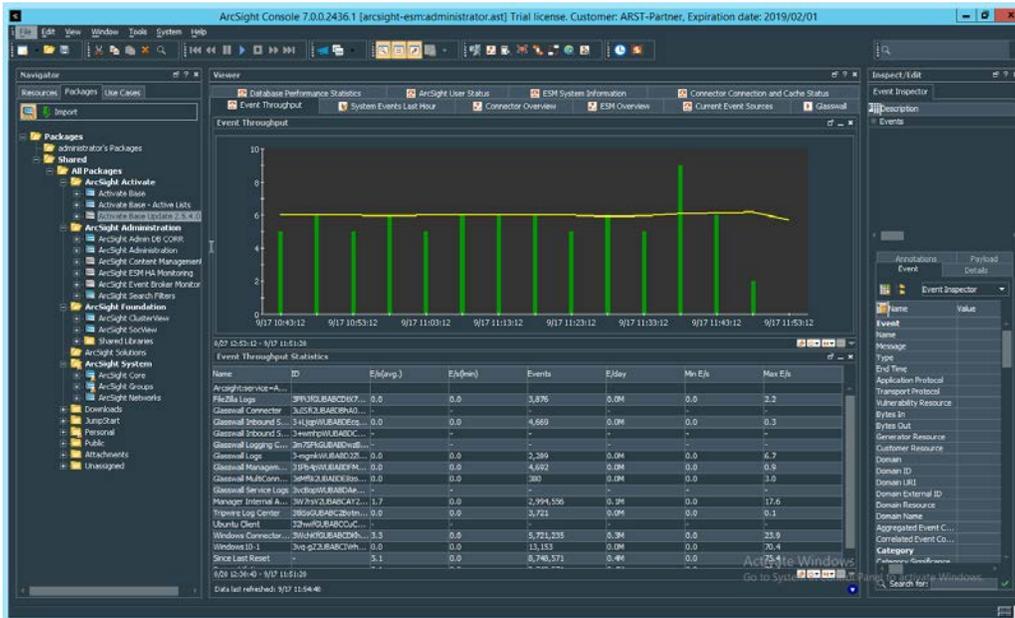
1620

1621

1622

1623

5. Enter the **hostname** of the ArcSight machine, the **port** (default: 8443), and the **username** and **password** used to connect to the **ESM**.
6. Delete **Activate\_Base\_Updated\_2.5.4.0.arb** from the ARCSIGHT\_HOME directory.
7. Log in to **ArcSight Console**.



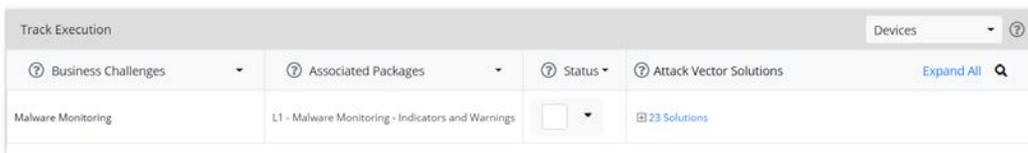
- 1624
- 1625
- 1626
8. Under **Packages > Shared > All Packages > ArcSight Activate**, right-click **Activate Base Update 2.5.4.0**, and select **Delete Package**.

1627 *2.11.5.2 Install Packages*

1628 Once the Activate Base is installed, packages can be installed to monitor for specific types of events. As

1629 an example, find below instructions for the Malware Monitoring package.

- 1630
- 1631
1. Navigate to the **ArcSight Content Brain** web application.
  2. Select the **Level 1** box labeled **Malware**.



- 1632
- 1633
- 1634
3. In the Track Execution section, under Associated Packages, you can see the list of packages used to address the challenge of Malware Monitoring. In this case, there is just one package, L1–

- 1635 Malware Monitoring—Indicators and Warnings. Click the link to be taken to a download page for  
 1636 the package, and download it. (Note: This package should be installed on the ArcSight Console,  
 1637 not on the ESM.)
- 1638 4. Copy the contents of the zip file to ARCSIGHT\_HOME. The default for this is C:\arcsight\Console  
 1639 console\current, assuming a Windows Server.
- 1640 5. In PowerShell, navigate to the ARCSIGHT\_HOME directory (C:\arcsight\Console\current) and  
 1641 run:  
 1642 > .\L1-Malware\_Monitoring\_1.1.0.1.bat

```

Administrator: Windows PowerShell
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
ArcSight Package Utility starting...
Java HotSpot(TM) 64-Bit Server VM (build 25.171-b11, mixed mode)
Configuration initialized: config\console.defaults.properties; config\console.properties
ArcSight
Package Utility Version 7.0.0.2436.1 (8E2436_8-1-2018_12:17:31)
Copyright (c) 2001-2018 Micro Focus or one of its affiliates.
All rights reserved.
Logging in to manager 'arcsight-esm' with username 'administrator'...done.
JVM memory allowed: 455.5 MB
System locale: en_US
will now install:
Installing the following packages:
  /All Packages/ArcSight Activate/Activate Base
-----
Install complete. Elapsed Time:10 mins 28 secs 792 ms
Exiting...
ATTENTION
ATTENTION
ATTENTION: From your ESM console UI:
ATTENTION: Please delete /All Packages/ArcSight Activate/Activate Base Update 2.5.4.0.
ATTENTION:
ATTENTION:
ATTENTION: From your ESM console's file system:
ATTENTION: Please delete Activate_Base_Updated_2.5.4.0.arb
ATTENTION:
ATTENTION:
ATTENTION: Please delete Activate_Base_Updated_2.5.4.0.arb
ATTENTION
ATTENTION
PS C:\arcsight\console\current> .\L1-Malware_Monitoring_1.1.0.1.bat
Enter manager information (e.g., esm.mycompany.com):arcsight-esm
Enter the manager listening port (e.g., 8443, or [ENTER] for default):8443
Enter an administrator user name (e.g., admin):administrator
Enter the password for this administrator account:

```

- 1643
- 1644 6. Enter the **hostname** of the ArcSight machine, the **port** (default: 8443), and the **username** and  
 1645 **password** used to connect to the **ESM**.

## 1646 2.11.6 Apply Filters to a Channel

- 1647 1. In the **ArcSight Console**, click **File > New > Active Channel**.
- 1648 2. Enter a **name** for the channel.
- 1649 3. Select a time frame.
- 1650 4. For **Filter**, select one the filters that was imported from the packages you installed.

- 1651
- 1652 5. Click **OK**. All events that match the filter can be displayed in the newly created channel. Filters
- 1653 from imported packages can be found under **Filters > Shared > All Filters > ArcSight Activate >**
- 1654 **Solutions**.

## 1655 2.12 Tripwire Enterprise

1656 Notes:

1657 This installation requires MSSQL to be installed on a remote server and configured according to the

1658 instructions in the ***Tripwire Enterprise 8.6.2 Installation and Maintenance Guide***.

### 1659 2.12.1 Install Tripwire Enterprise

- 1660 1. Ensure that you have an up-to-date version of Oracle Java. You must install both the Java
- 1661 Runtime Environment (JRE) and the Java Cryptography Extension (JCE).
- 1662 2. Download and run the **JRE installer**.



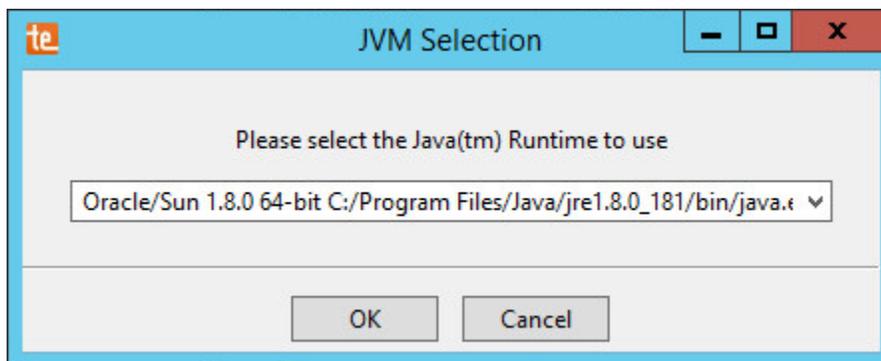
1663  
1664  
1665

3. Click **Install**.
4. Download the JCE and extract the files.

Name	Date modified	Type	Size
local_policy	12/20/2013 1:54 PM	JAR File	3 KB
README	12/20/2013 1:54 PM	Text Document	8 KB
US_export_policy	12/20/2013 1:54 PM	JAR File	3 KB

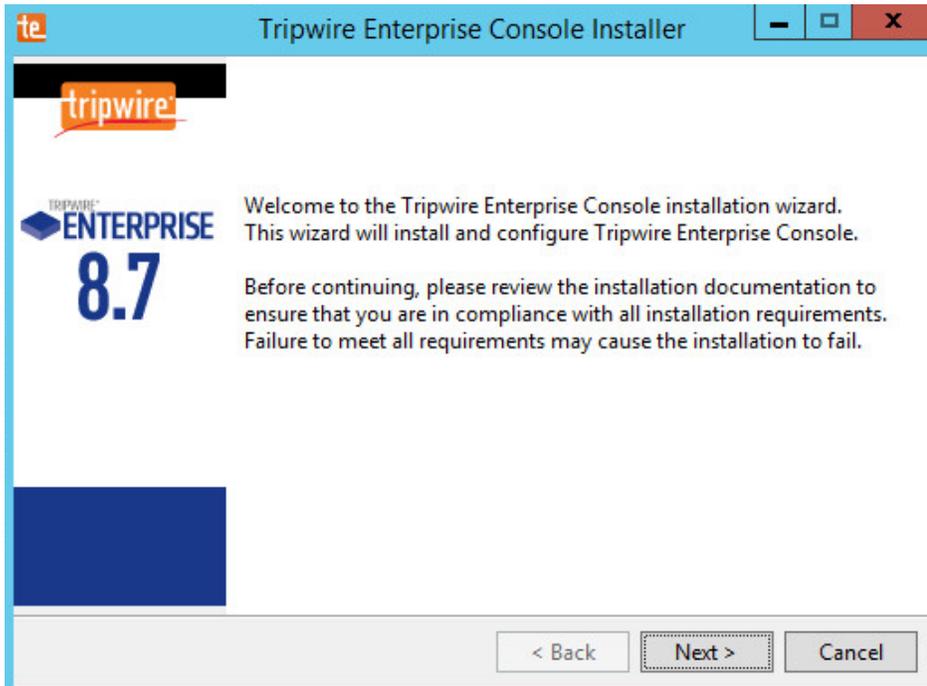
1666  
1667  
1668  
1669  
1670

5. Copy the *local\_policy.jar* and *US\_export\_policy.jar* files to `/lib/security/Unlimited/` and `/lib/security/Limited` in the Java installation directory.
6. Run **install-server-windows-amd64**.
7. Select the Java runtime that was just installed.



1671  
1672

8. Click **OK**.



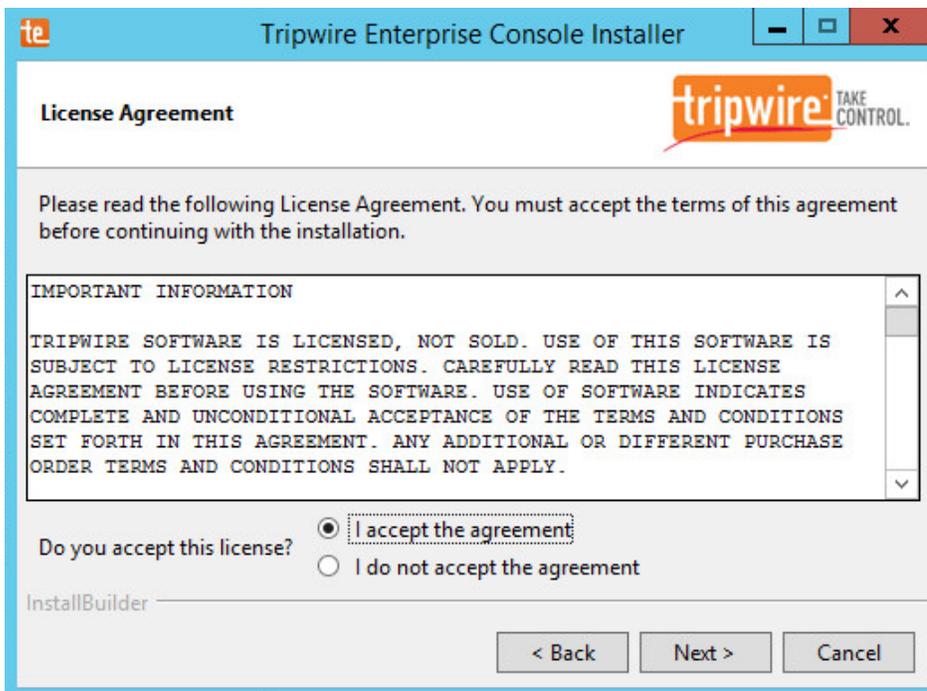
1673

1674

1675

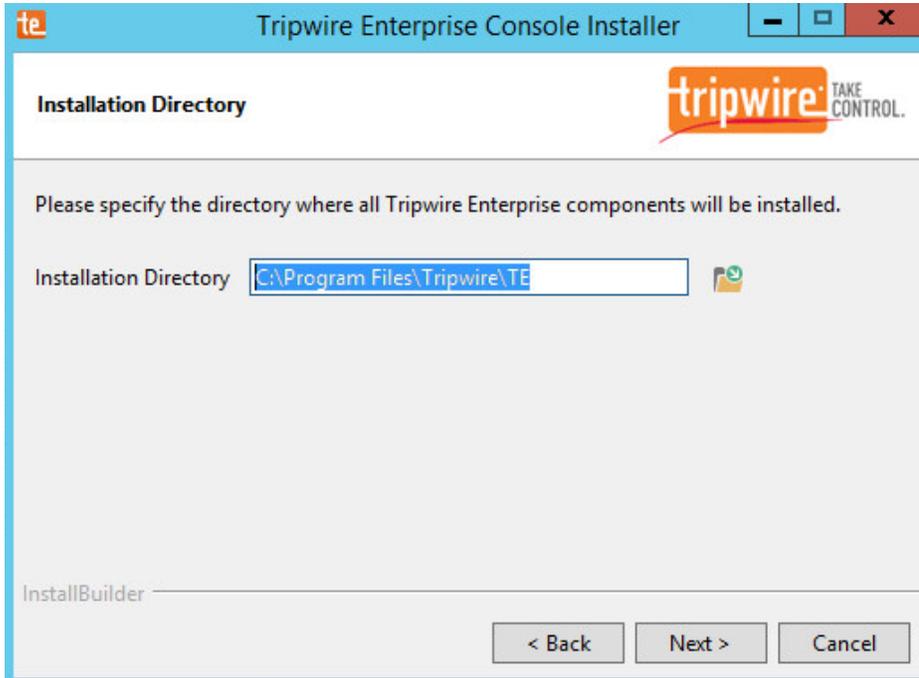
9. Click **Next**.

10. Select **I accept the agreement**.



1676

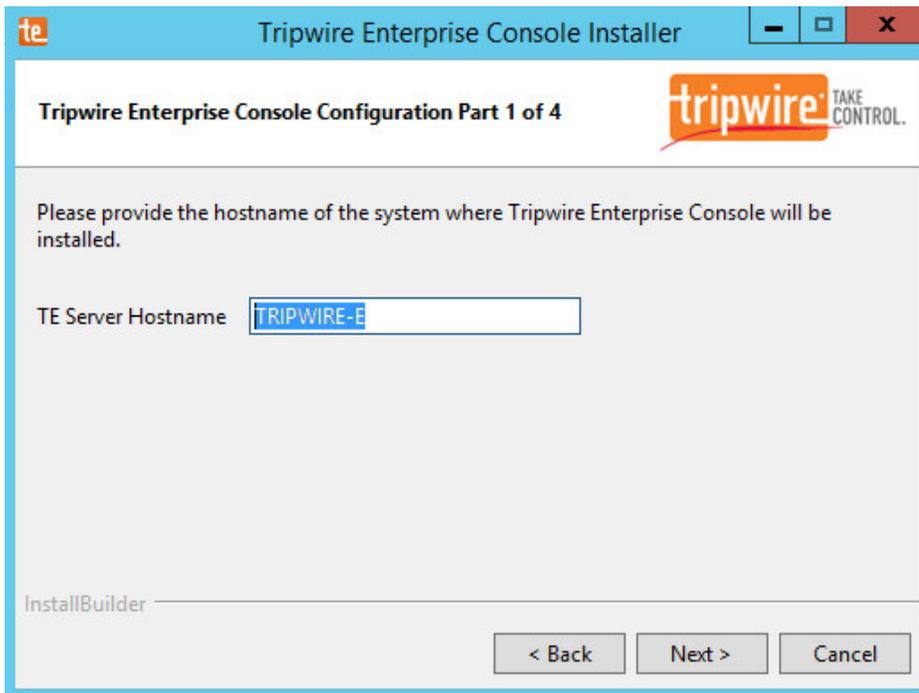
1677 11. Click **Next**.



1678

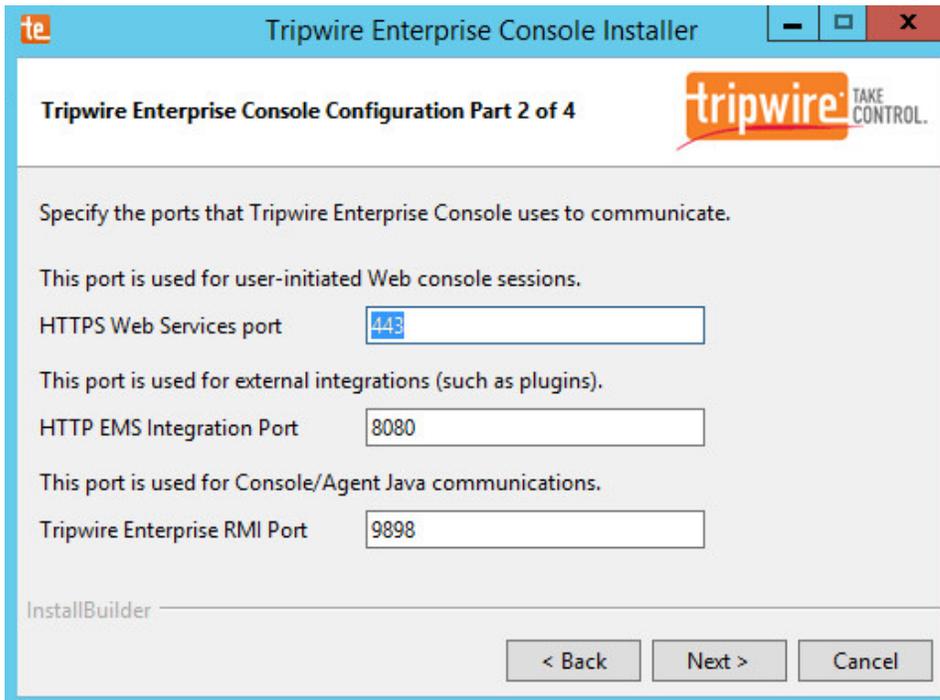
1679 12. Click **Next**.

1680 13. The installer should automatically detect the hostname of the system on which Tripwire  
1681 Enterprise is being installed. If it does not, enter the hostname here.



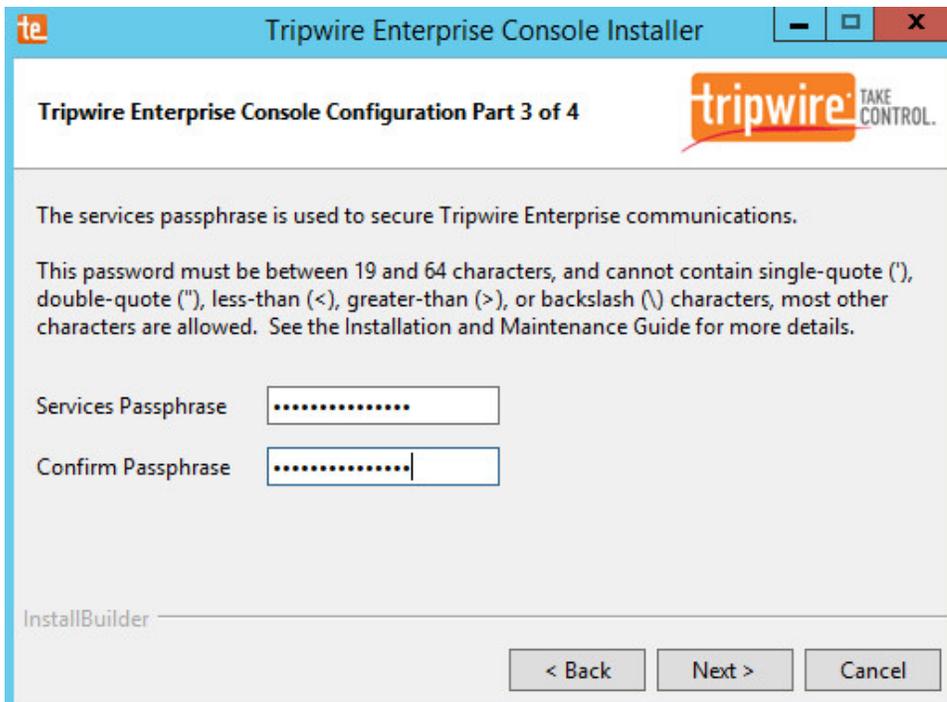
1682  
1683  
1684  
1685  
1686

14. Click **Next**.
15. Enter each port number to use for the HTTPS Web Services port, HTTP EMS Integration Port, and Tripwire Enterprise RMI port. The RMI port is used for inbound communication from Tripwire agents to the server, so ensure that it is allowed through the firewall.



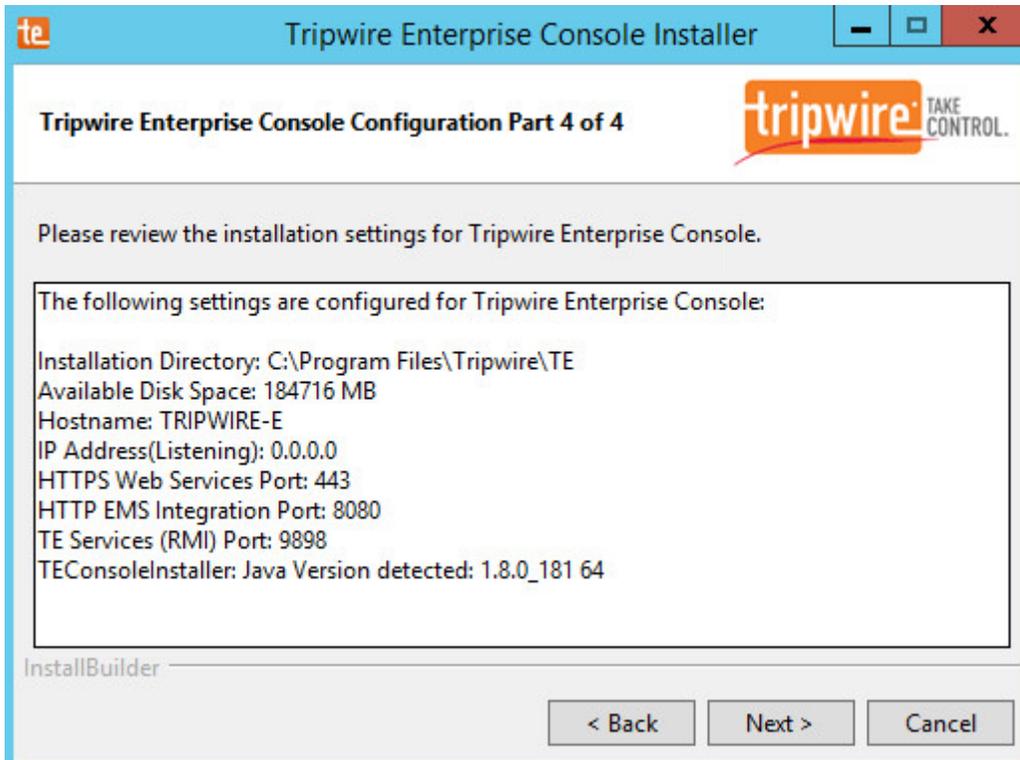
1687  
1688  
1689

- 16. Click **Next**.
- 17. Enter a passphrase to use.



1690

1691 18. Click **Next**.

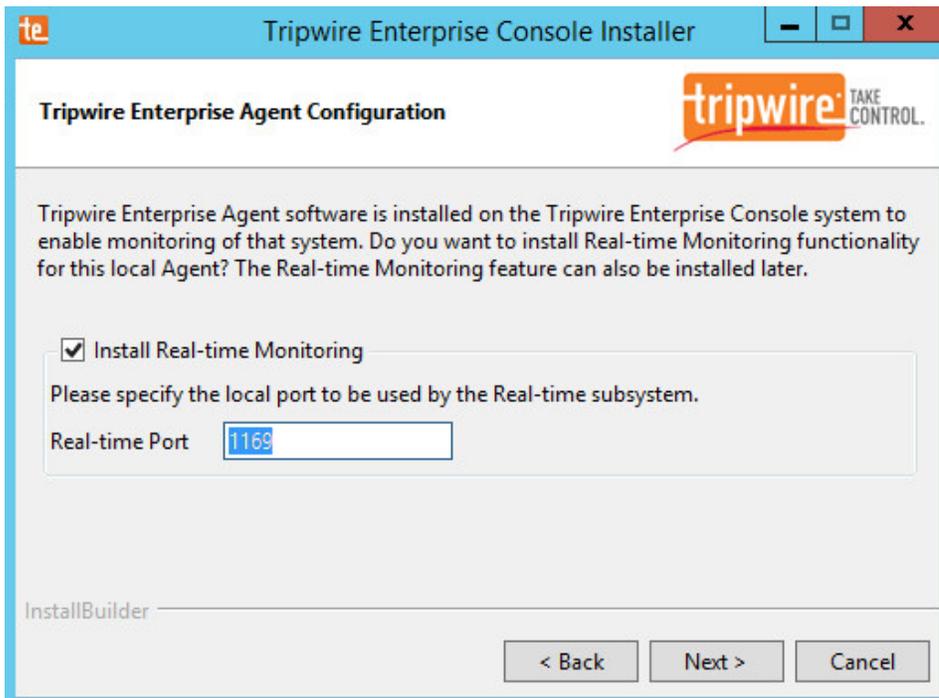


1692

1693 19. Click **Next**.

1694 20. Check the box next to **Install Real-time Monitoring**.

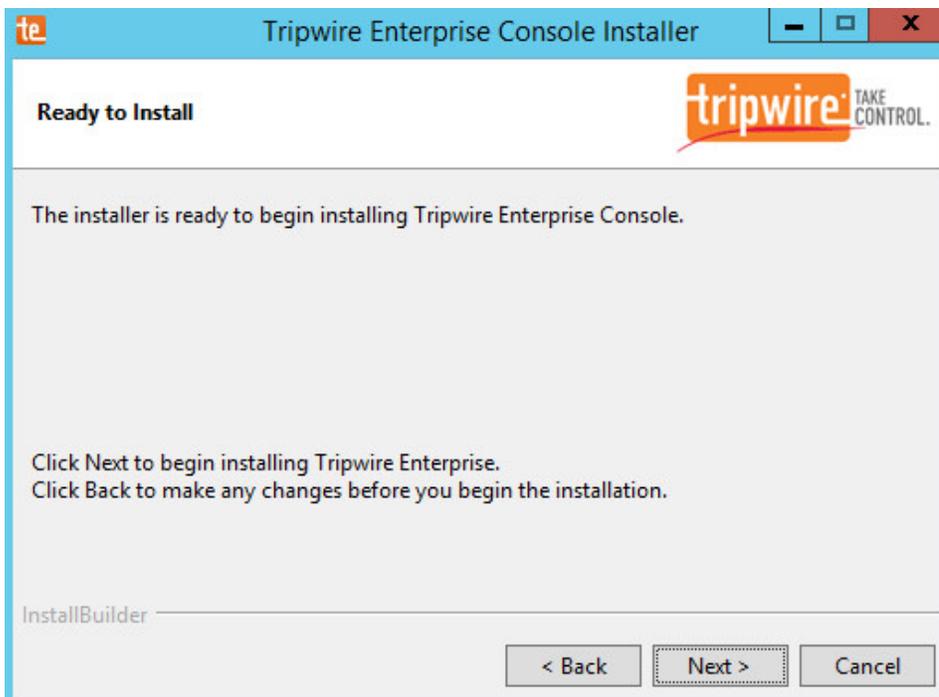
1695 21. Enter **1169** for **Real-time Port**.



1696

1697

22. Click **Next**.

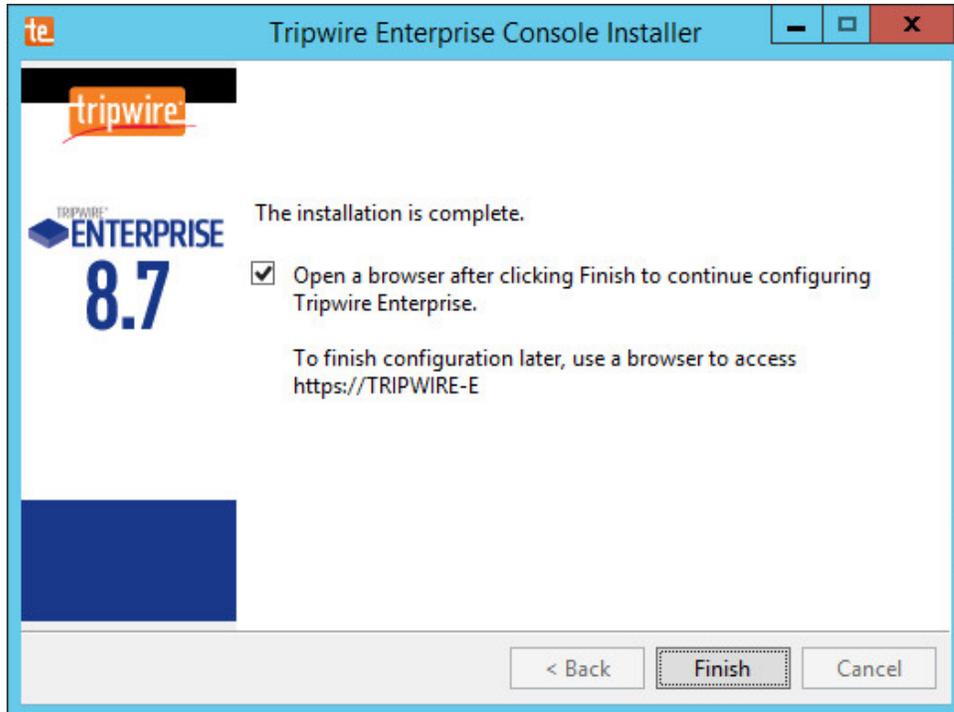


1698

1699

23. Click **Next**.

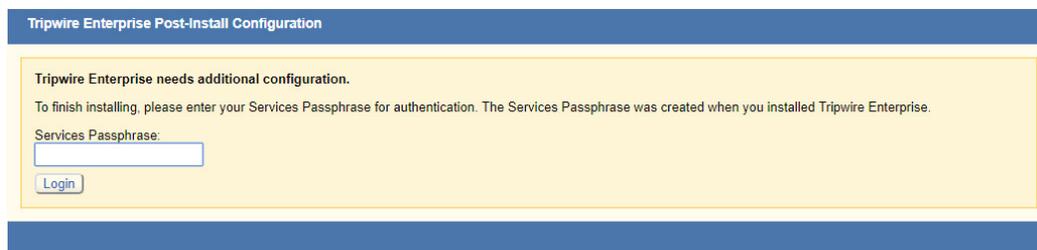
- 1700 24. Check the box next to **Open a browser after clicking Finish to continue configuring Tripwire Enterprise**.  
1701



1702

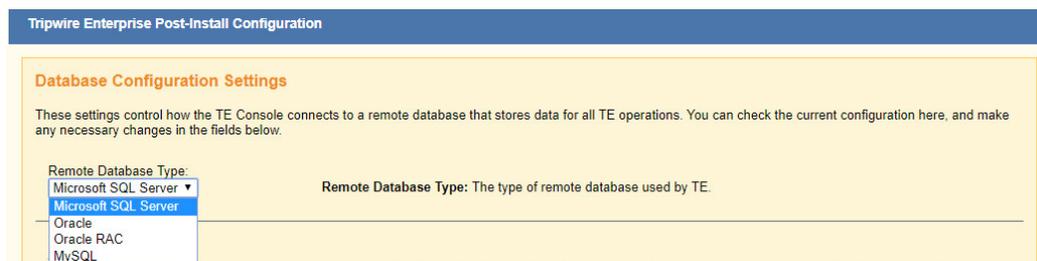
- 1703 25. Click **Finish**.

- 1704 26. Once at the web address, enter the **Services passphrase** chosen earlier.



1705

- 1706 27. Click **Login**.



1707

- 1708 28. Select **Microsoft SQL Server** for **Remote Database Type**.
- 1709 29. Select **SQL Server** for **Authentication Type**.
- 1710 30. Enter login details for the account created during the MSSQL setup.
- 1711 31. Enter the **hostname** or **IP** of the database server.
- 1712 32. Enter the **port** on which the database is operating.
- 1713 33. Enter the **name** of the database to be used for Tripwire Enterprise.
- 1714 34. Select the appropriate setting for **SSL** according to your organization’s needs.

Authentication Type:

Authentication Type: Specifies whether the database login should authenticate using a Windows account (typically of the format domain\user), or an SQL Server account (an account defined only in SQL Server). With the Windows authentication type, NTLMv2 should be used, as it is cryptographically superior to the first version of NTLM. However, as NTLMv2 is configured in the operating system, not in the database or application, TE can be used with NTLM to ensure compatibility.

Login Name:

Login Name: The login name that TE will use to authenticate with the database.

Password:

Password: The password that TE will use to authenticate with the database.

Database Host:

Database Host: The fully qualified domain name, hostname or IP address of the system where the database is installed.

Port (default 1433):

Port: The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.

Database Name:

Database Name: The name of the database that TE should use when connecting to the remote database. Note that the login name in SQL Server should have this database set as the default, and the login name should be mapped to this database.

Instance Name (Optional):

Instance Name (Optional): The location/name of the database instance on the server. Ask your DBA if a non-default instance should be used for TE.

SSL:

SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL.

- Request - SSL will be used if available.
- Require - SSL will always be used, and an error will occur if SSL is not available for the database.
- Authenticate - SSL will always be used, and an error will occur if SSL is not available for the database. In addition, the certificate chain of the database server's public key will be authenticated using TE's trust store. If the certificate chain does not originate from a trusted source, an error will occur.
- Off - SSL will never be used. This setting is not recommended.

✓

- 1715
- 1716 35. Click **Test Database Login** to ensure the connection is functional.

✓

Test Results:

Connection Succeeded.

Tripwire Enterprise 8.7.0.b8.7.0.r20180606173604-e215728.b40

- 1717
- 1718 36. Click **Save Configuration and Restart Console**.
- 1719 37. After the reboot, enter a new administrator **password**.

**Tripwire Enterprise Post-Install Configuration**

**Configuration Steps Needed:**

Tripwire administrator account password needs to be changed from the default.

**Create Administrator Password**

Passwords must:  
Be between 8 and 128 characters in length  
Contain at least 1 numeric character  
Contain at least 1 uppercase character  
Contain at least 1 non-alphanumeric character  
Supported characters: ~!@#\$%^&\*()\_-=+{}|\;:'" < > / ?

Password:

Confirm Password:

**Support Information**

Still having problems with your installation?  
Contact Tripwire Support: <https://secure.tripwire.com/customers/contact-support.cfm>  
Or open a Support ticket: <https://secure.tripwire.com/customers/>

For faster assistance from Support, please generate a support bundle to collect information about your system and this installation. Attach the support bundle file to your web ticket or email. [What is a Support Bundle?](#)

Tripwire Enterprise 8.7.0.b8.7.0.r20180606173604-e215728.b40

1720

1721

38. Click **Confirm and Continue**.

**Tripwire Enterprise Fast Track**

Welcome to Tripwire Enterprise Fast Track!



Fast Track will help you to configure Tripwire Enterprise for Change Auditing, Policy Management, or an integrated Security Configuration Management (SCM) solution. It only takes a few minutes to complete the setup questionnaire. After you do, Fast Track will use your answers to install the components that you need.

Step 1: Add your license file and describe your environment. This includes the platforms you want Tripwire Enterprise to monitor, the policies you want to enforce, and the schedule that Tripwire Enterprise should use.

Step 2: Review the items that will be configured and save the manifest for your records.

Step 3: Apply the configuration and let Fast Track do the rest.

Note: After Fast Track configures Tripwire Enterprise, you can always make changes to your configuration later from the Tripwire Enterprise user interface.

1722

1723

39. Click **Configure Tripwire Enterprise**.

1724



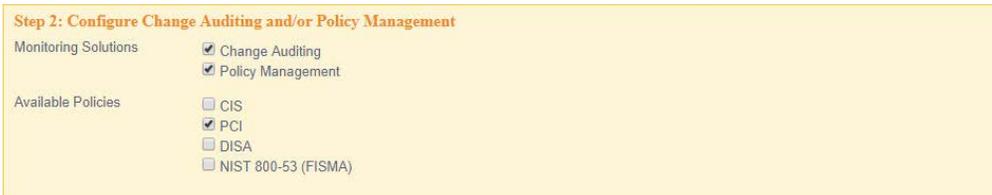
1725

40. Click **Choose File** and select the Tripwire Enterprise license file, which should be a **.cert** file.

1726

41. Check the boxes next to **Change Auditing** and **Policy Management**.

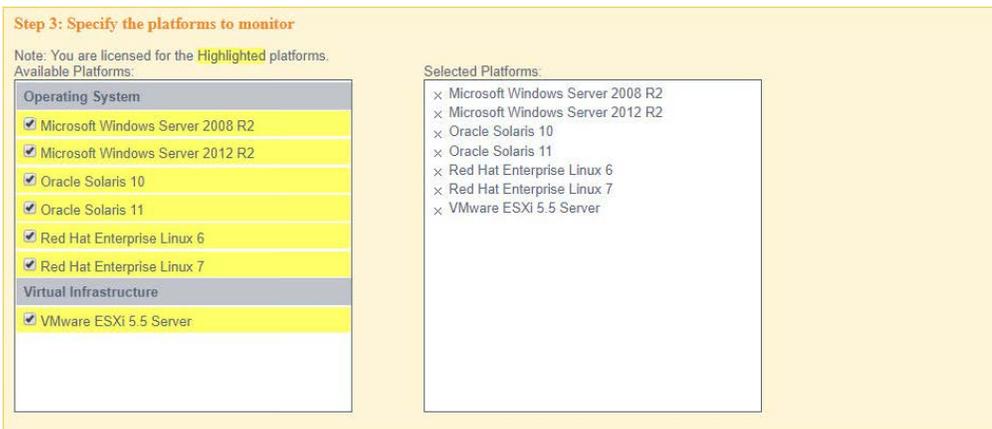
1727



1728

42. Select any available policies desired.

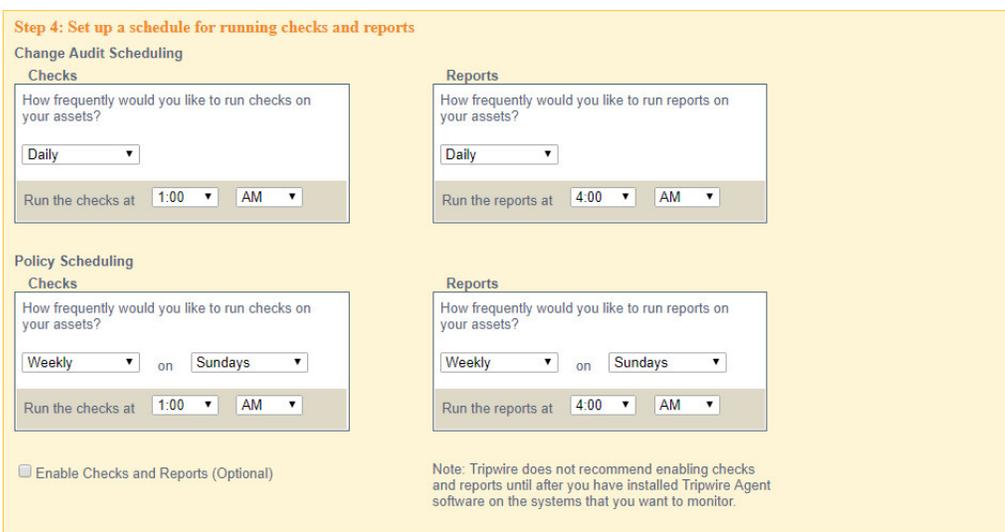
1729



1730

43. Select all the operating systems that you wish to monitor with Tripwire Enterprise.

1731



- 1732 44. Set up a schedule for running checks and reports according to your organization’s needs. Leave  
1733 the box next to **Enable Checks and Reports** unchecked for now.



- 1734  
1735 45. Select **Set up the email server at another time**.



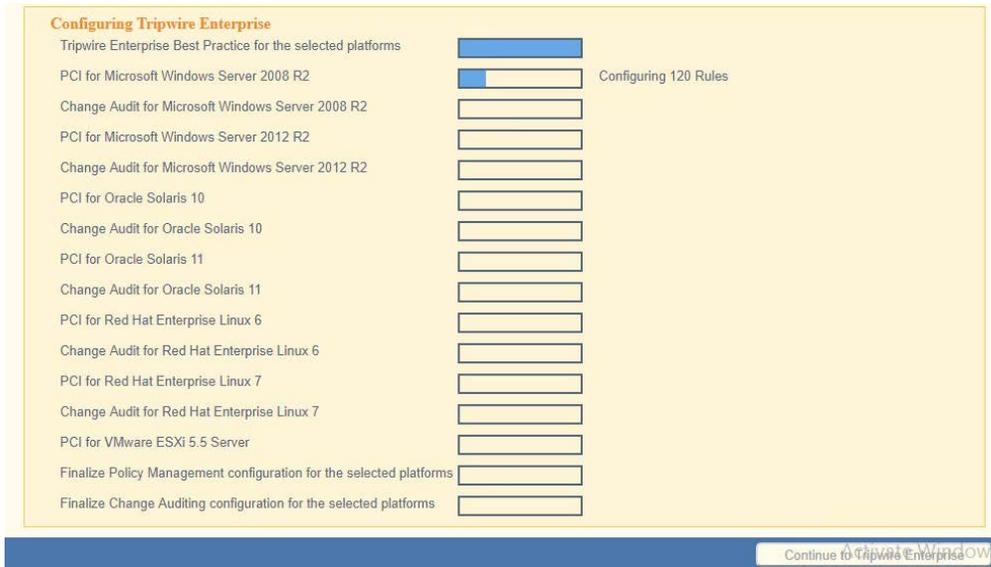
- 1736  
1737 46. Enter a **username** and **password** for a new administrator account for Tripwire Enterprise  
1738 Console.



- 1739  
1740 47. Click **Preview Configuration**.



- 1741  
1742 48. Click **Apply Configuration**.



1743

1744 49. Click **Continue to Tripwire Enterprise** when the installation finishes.1745 

## 2.12.2 Install the Axon Bridge

1746 1. Ensure that TCP traffic on port 5670 is allowed through the firewall.

1747 2. Navigate to the Tripwire Enterprise Console installation directory to the `/server/data/config`  
1748 folder. Copy `bridge_sample.properties` to `bridge.properties`.1749 3. In the `bridge.properties` file, find the line that says:1750 `#tw.cap.bridge.registrationPreSharedKey=`1751 Remove the “#” character. After the “=” character, enter a **password**. The password has some  
1752 restrictions, so ensure that it meets the requirements in case the connection fails later.1753 4. Restart the TE console by running the following command from an administrative command  
1754 prompt, where `<te_root>` is the TE installation directory:1755 

```
> <te_root>/server/bin/twserver restart
```

1756 

## 2.12.3 Install the Axon Agent (Windows)

1757 1. Download the Axon Agent zip file from the Tripwire customer website

1758 (<https://tripwireinc.force.com/customers>), under the Product Downloads tab.

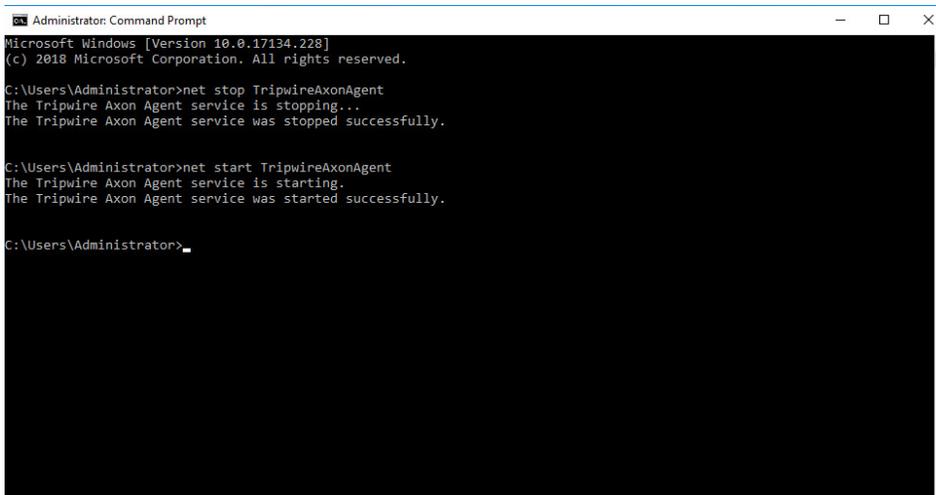
1759 2. Unzip the file.

1760 3. To begin the installation, double-click the `.msi` file in the extracted folder. Note: No installation  
1761 wizard will appear; the installation happens automatically.

- 1762 4. After the Axon Agent is installed, navigate to C:\ProgramData\Tripwire\agent\config, and copy  
1763 *twagent\_sample.conf* to *twagent.conf*.

```
#
# HOST based agent configuration:
#   Instead of using a DNS SRV record, the agent may be configured
#   to talk to a specific host, or list of hosts. Lists use a comma separator and
#   can optionally specify a port. The default of port 5670 will be used if a port
#   is not specified.
#
#   Example: host1, host2:5900, 10.123.0.15, [feac:ba80:6fff:93fe]:7582
#
#   The agent may be configured to connect to hosts in a randomized or textual order
#   (default: true)
#
bridge.host=192.168.1.136
#bridge.port=5670
#bridge.randomize.hosts=true
#
```

- 1764
- 1765 5. Open **twagent.conf** and find the line that says `bridge.host`. Remove the “#” character, and  
1766 enter the hostname or IP address of the Axon Bridge server.
- 1767 6. In a file called **registration\_pre\_shared\_key**, enter the value of the preshared key that was set  
1768 in the Axon Bridge.
- 1769 7. Restart the Axon Agent Service by opening a command prompt and running the following  
1770 commands:  
1771 > net stop TripwireAxonAgent  
1772 > net start TripwireAxonAgent



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net stop TripwireAxonAgent
The Tripwire Axon Agent service is stopping...
The Tripwire Axon Agent service was stopped successfully.

C:\Users\Administrator>net start TripwireAxonAgent
The Tripwire Axon Agent service is starting.
The Tripwire Axon Agent service was started successfully.

C:\Users\Administrator>
```

1773

#### 1774 2.12.4 Install the Axon Agent (Linux)

- 1775 1. Download the Axon Agent *.tgz* file from the Tripwire customer website  
1776 (<https://tripwireinc.force.com/customers>), under the Product Downloads tab.  
1777 2. To install the software, run the following commands:

1778 RHEL or CentOS: > rpm -ivh <installer\_file>  
1779 Debian or Ubuntu: > dpkg -i <installer\_file>  
1780 3. Navigate to /etc/tripwire/ and copy **twagent\_sample.conf** to **twagent.conf**.  
1781 4. Open **twagent.conf** and find the line that says `bridge.host`. Remove the “#” character and  
1782 enter the hostname or IP address of the Axon Bridge server.  
1783 5. In a file called **registration\_pre\_shared\_key.txt**, enter the value of the preshared key that was  
1784 set in the Axon Bridge.  
1785 6. Restart the Axon Agent Service by opening a command prompt and running the following  
1786 commands:  
1787 RHEL or CentOS:  
1788 > /sbin/service tripwire-axon-agent stop  
1789 > /sbin/service tripwire-axon-agent start  
1790  
1791 Debian or Ubuntu:  
1792 > /usr/sbin/service tripwire-axon-agent stop  
1793 > /usr/sbin/service tripwire-axon-agent start

## 1794 2.12.5 Configure Tripwire Enterprise

### 1795 2.12.5.1 Terminology

1796 **Node:** a monitored system, such as a file system, directory, network device, database, or virtual  
1797 infrastructure component

1798 **Element:** a monitored object, which is a component or property of a node being audited by TE

1799 **Element Version:** a record of an element’s state at specific points in time. Multiple element versions  
1800 create a historical archive of changes made to the element.

1801 **Rule:** A rule identifies one or more elements to the TE Console.

1802 **Action:** an object that initiates a response to either changes detected by TE or by failures generated  
1803 from policy tests

1804 **Task:** a TE operation that runs on a scheduled or manual basis

1805 **TE Policy:** a measurement of the degree to which elements comply with a policy

1806 **Policy Test:** a determination of whether elements comply with the requirements of a policy

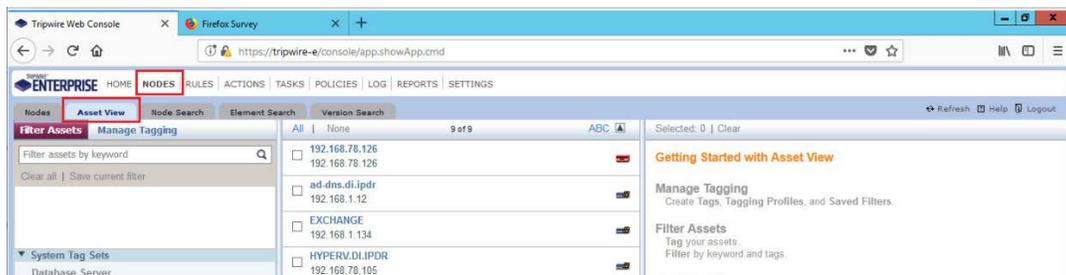
1807 **Baseline:** the act of creating an element that reflects the current state of a monitored object (also called  
1808 the **current baseline**). When a node's baseline is promoted, TE saves the former baseline as a **historic**  
1809 **baseline**.

1810 **Version Check:** a check on monitored objects/elements. It is a comparison of the current state of the  
1811 element against its already recorded baseline for changes.

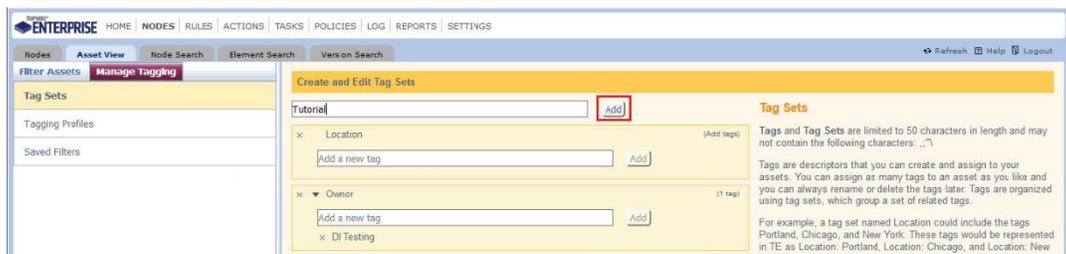
### 1812 [2.12.5.2 Tags](#)

1813 In Tripwire Enterprise, tags can be used to label and target specific nodes. Tags are not required but  
1814 allow for targeting nodes more granularly than by the operating system. This section describes how to  
1815 create and assign tags.

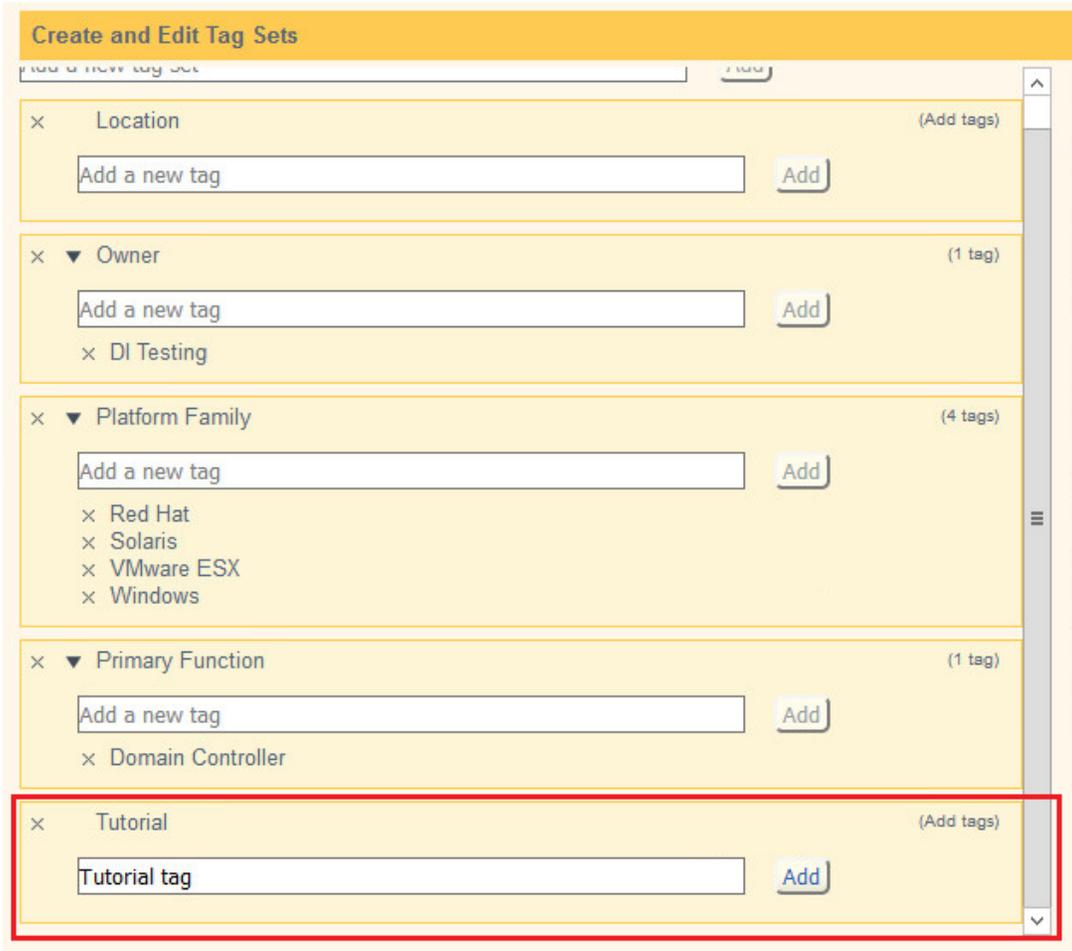
- 1816 1. Navigate to the TE Console in your browser.
- 1817 2. Click **Asset View**.



- 1818 3. Click the **Manage Tagging** tab.
- 1819 4. Enter the name of a tag set, or use one of the four existing ones (Location, Owner, Platform  
1820 Family, Primary Function). Click **Add** if adding your own tag set.



- 1822 5. Under the tag set to which you wish to add a tag, enter the name of the tag.
- 1823



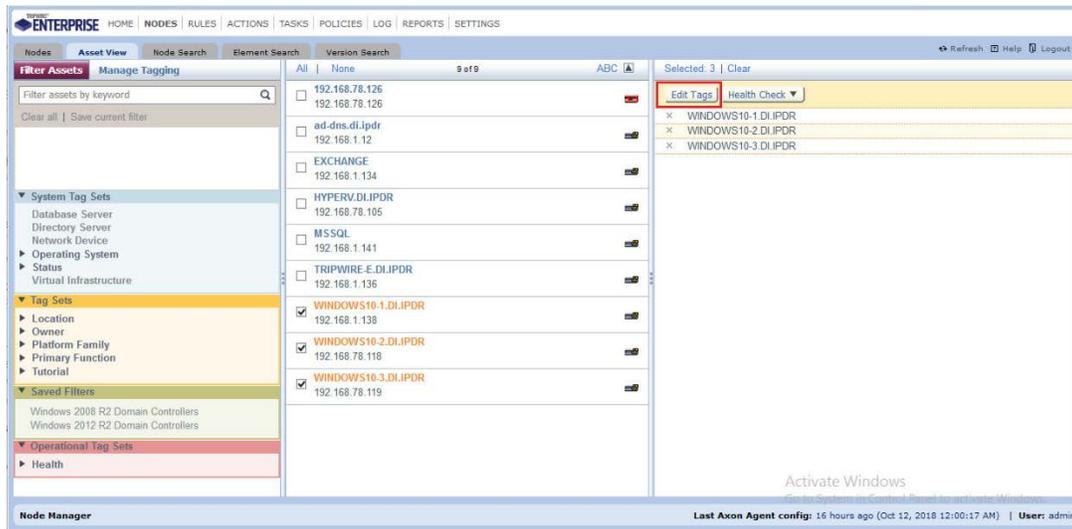
1824

1825

1826

1827

6. Click **Add**.
7. Navigate to **Nodes > Asset View > Filter Assets**.
8. Check the boxes next to the nodes to which you wish to add this tag.



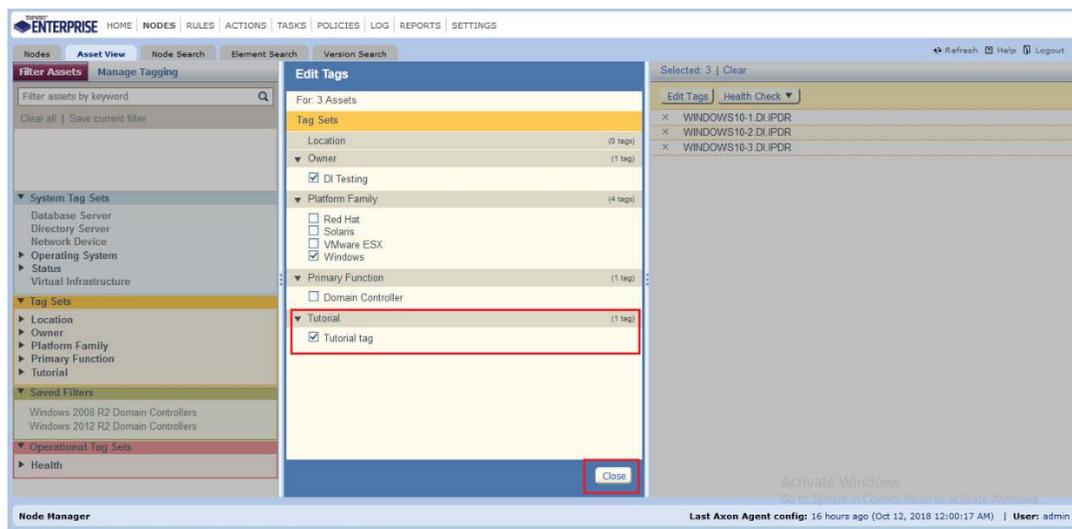
1828

1829

1830

9. Click **Edit Tags**.

10. Check the boxes next to any tags you wish to add to these nodes.



1831

1832

11. Click **Close**.

### 1833 [2.12.5.3 Rules](#)

1834 This section describes how to create a rule.

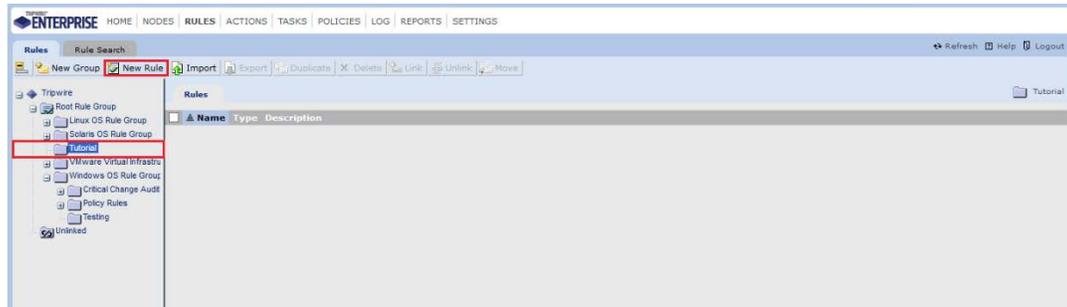
1835 1. Click **Rules**.

1836



1837

2. Select or create a rule group into which the new rule should be put.



1838

3. Click **New Rule**.

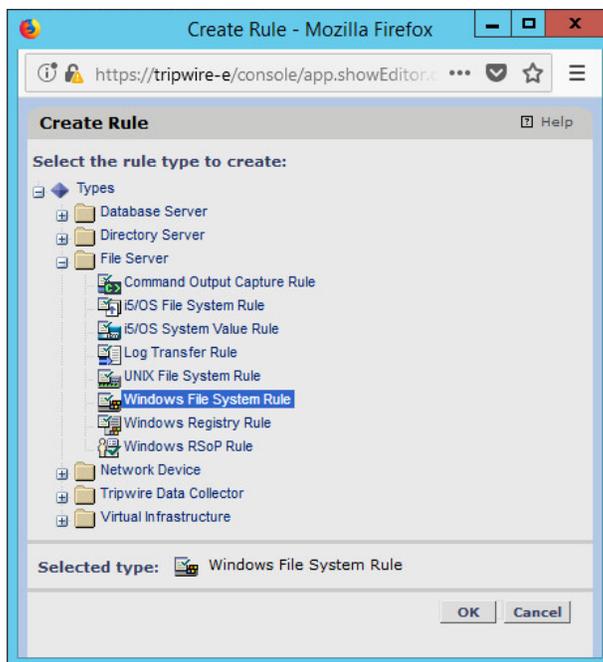
1839

1840

4. Select the type of rule. For monitoring Windows file systems, we choose **Windows File System Rule**.

1841

1842



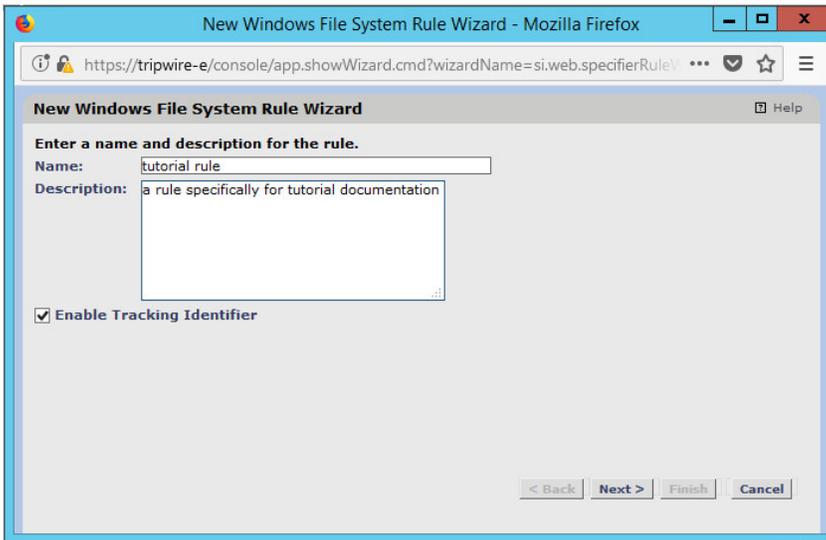
1843

5. Click **OK**.

1844

1845

6. Enter a **name** and **description** for the rule.



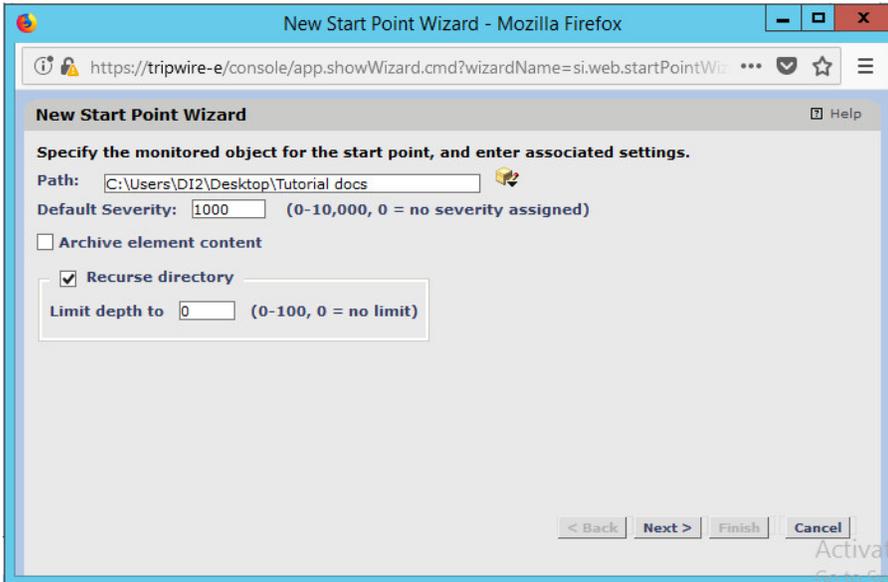
1846  
1847

7. Click **Next**.



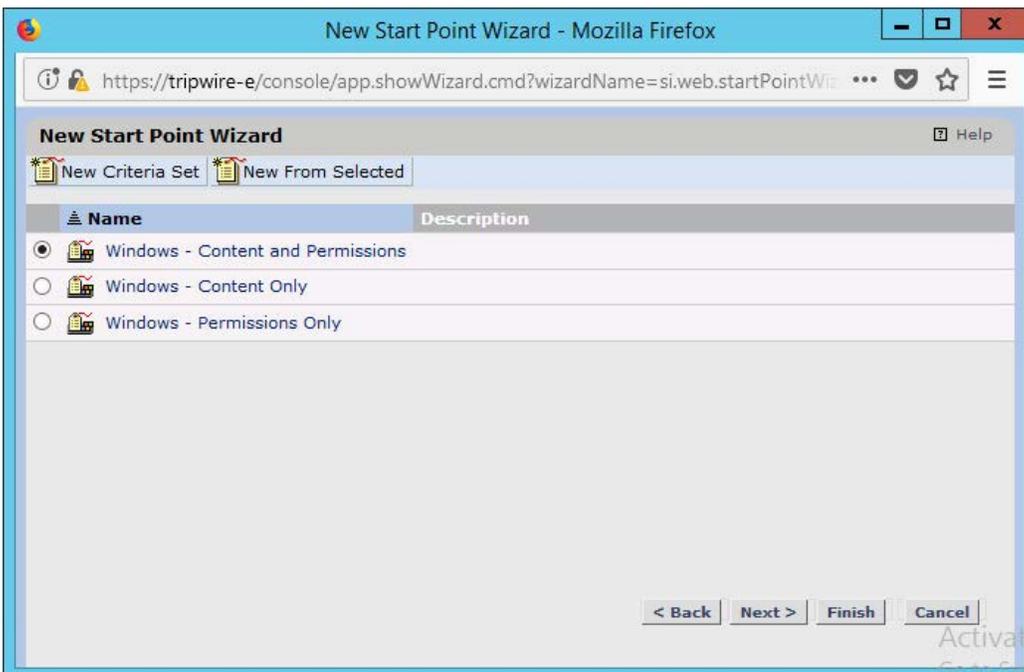
1848  
1849  
1850  
1851  
1852  
1853

8. Click **New Start Point**.
9. For **Path**, enter a directory that represents the scope of the scan. It can be limited to the documents folder or be wide enough to encompass all the files on a system. Note that the latter will take much longer to scan.
10. Check the box next to **Recurse directory** if you also wish to scan all subfolders.



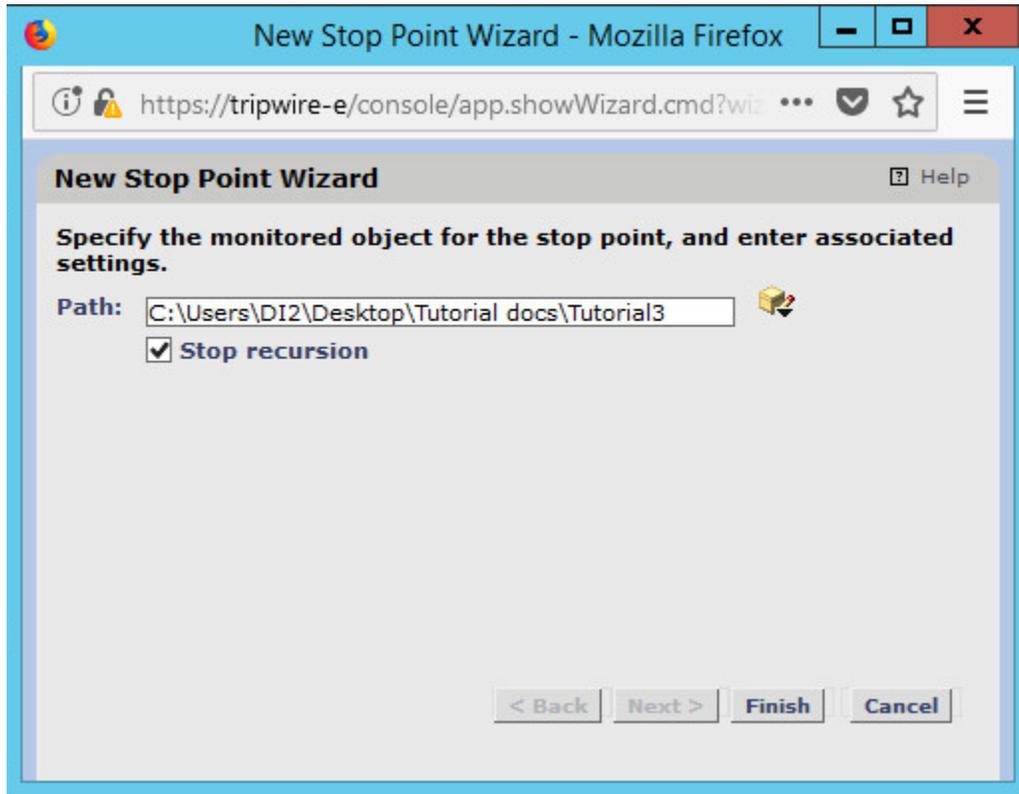
1854  
1855  
1856

11. Click **Next**.
12. Select **Windows Content and Permissions**.



1857  
1858  
1859  
1860  
1861

13. Click **Finish**.
14. Click **New Stop Point**.
15. Enter the path of any folders or files that should not be included in the scan, and indicate whether they should end the recursion.



1862

1863 16. Click **Finish**.

1864 17. Click **Next**.

1865 18. Click **Next**.

1866 19. Click **Finish**.

#### 1867 [2.12.5.4 Tasks](#)

1868 This section describes how to create a task on a schedule. These tasks can also be run manually if  
1869 necessary.

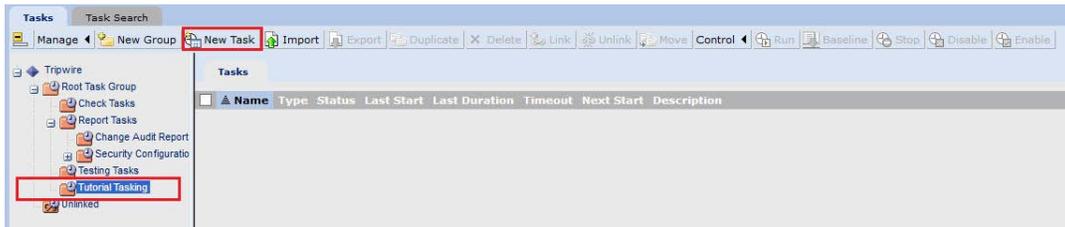
1870 1. Click **Tasks**.



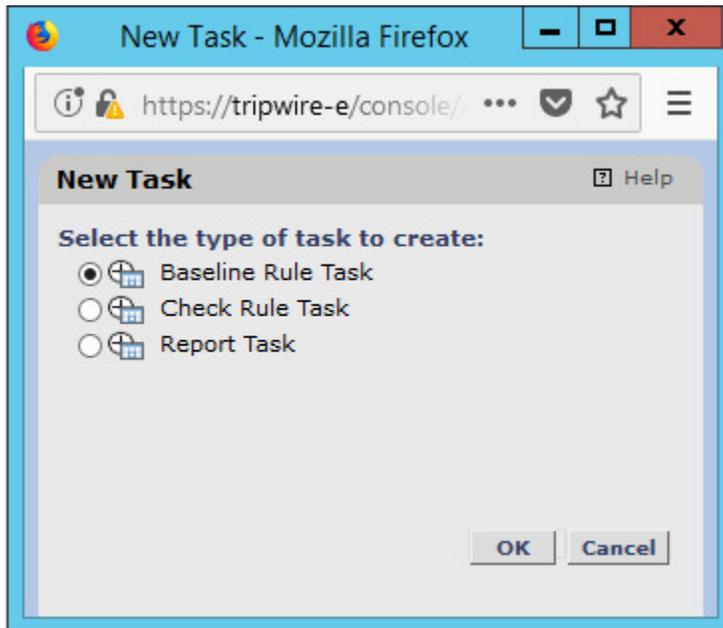
1871

1872 2. Select a folder for a new task, or create one.

1873  
1874  
1875  
1876

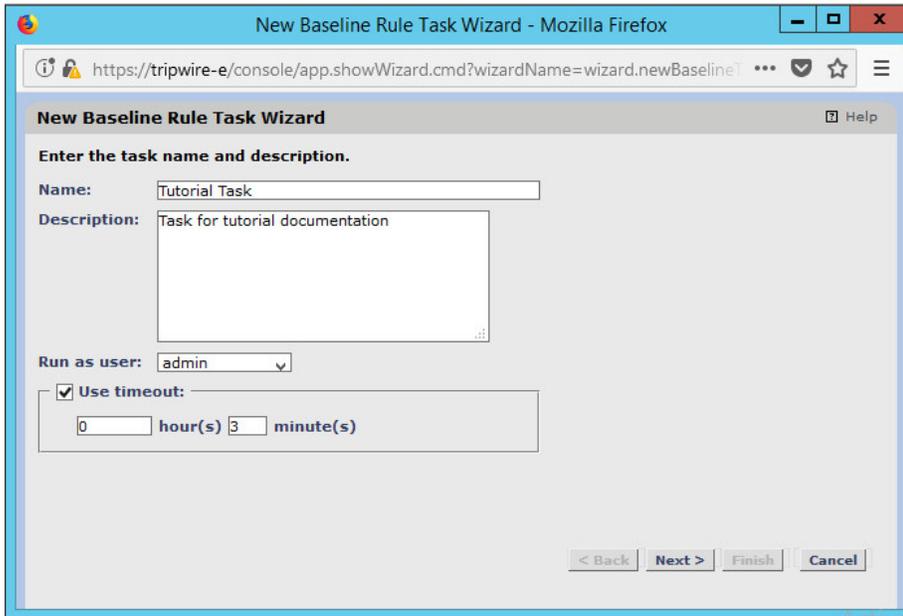


3. Click **New Task**.
4. Select **Baseline Rule Task** or **Check Rule Task**. (Note: Both are needed—baseline creates the initial state of the monitored object, and check updates the state and reports any changes.)



1877  
1878  
1879

5. Click **OK**.
6. Enter a **name** and **description** for the task.

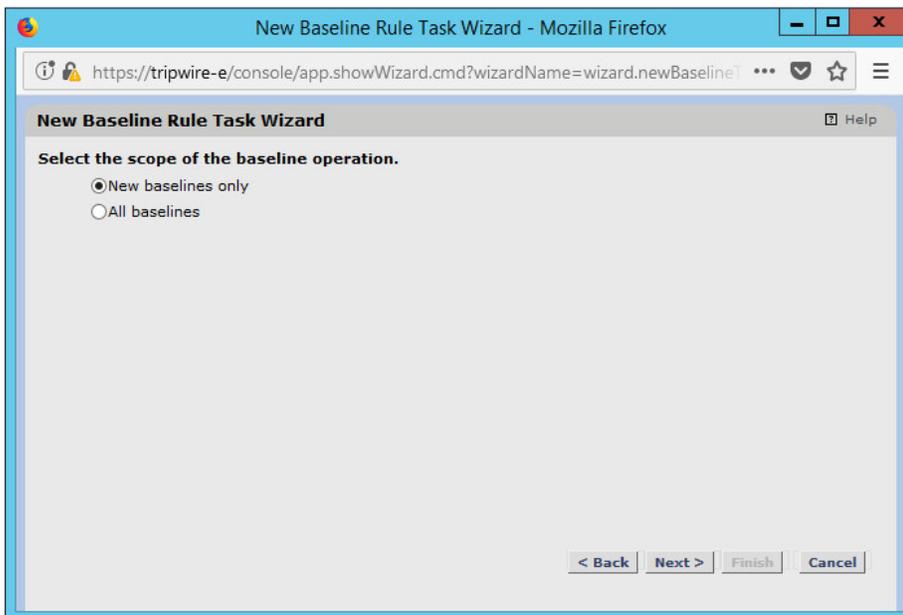


1880

1881

1882

7. Click **Next**.
8. Select whether you want all baselines to be updated or to only create new baselines.



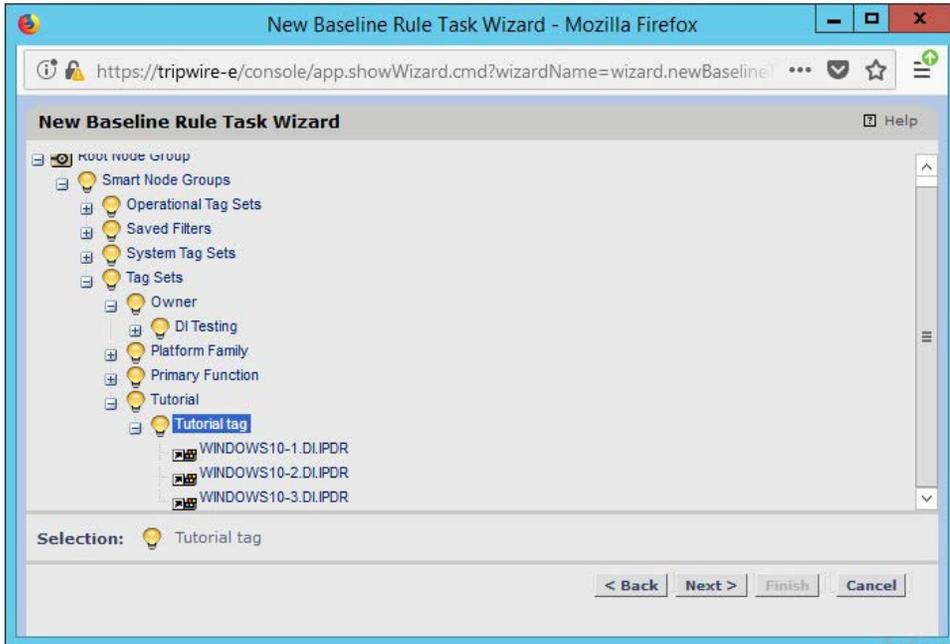
1883

1884

1885

1886

9. Click **Next**.
10. Select the systems to be included in the task. You can use tags or select by operating system (or other defaults).



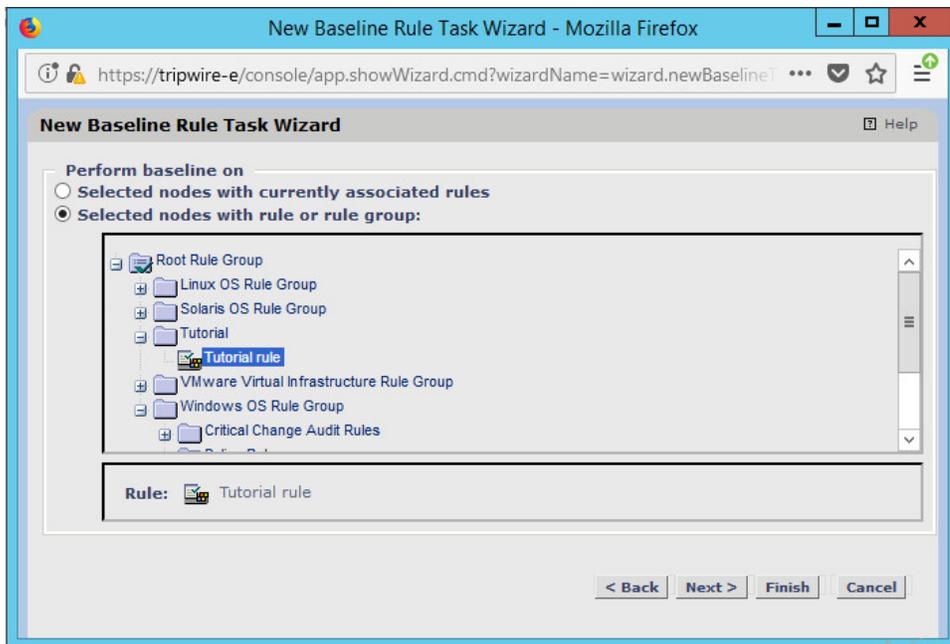
1887

1888

1889

11. Click **Next**.

12. Select the rule created earlier.



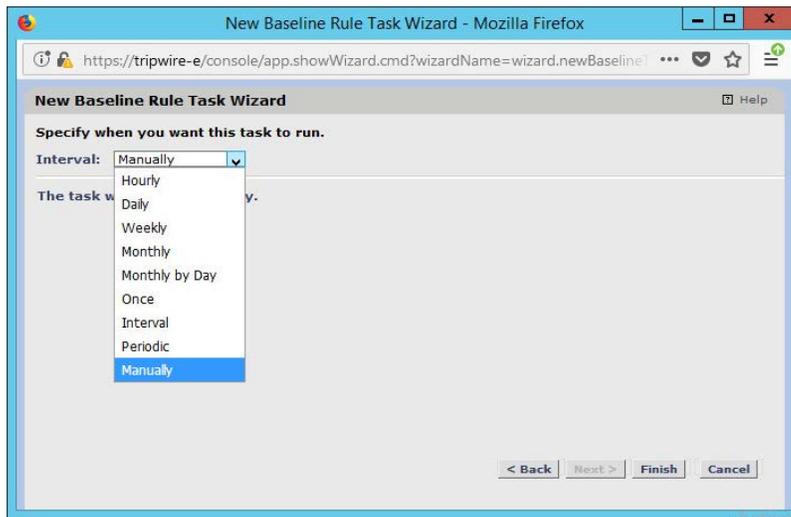
1890

1891

1892

13. Click **Next**.

14. Set the schedule of this task according to your organization's needs.



1893

1894

15. Click **Finish**.

## 1895 2.13 Tripwire Log Center

### 1896 2.13.1 Install Tripwire Log Center Manager

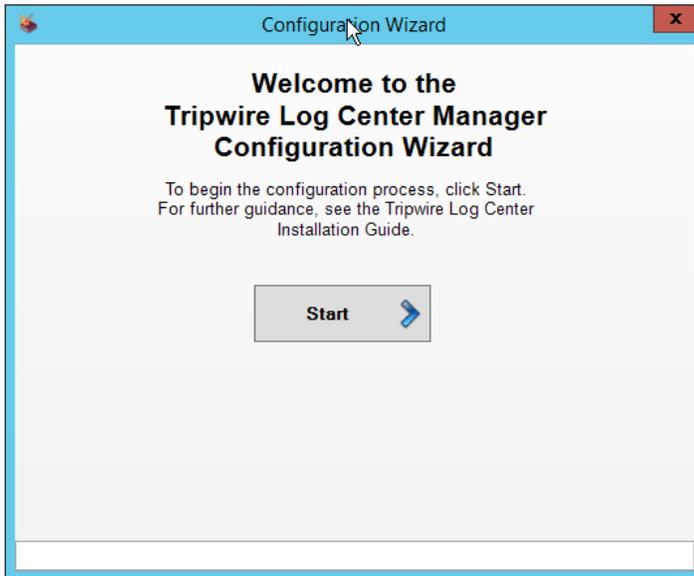
1897 See the *Tripwire Log Center 7.3.1 Installation Guide*, which should accompany the installation media, for  
 1898 instructions on how to install **Tripwire Log Center**. Use the **Tripwire Log Center Manager** installer.

1899 Notes:

- 1900 a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire**  
 1901 **Enterprise**.
- 1902 b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log*  
 1903 *Center 7.3.1 Installation Guide*.
- 1904 c. .NET Framework 3.5 is required for this installation—install this from the Server Manager.
- 1905 d. You may need to unblock port 9898 on your firewall for the Tripwire Enterprise agents.
- 1906 e. Do not install PostgreSQL if you wish to use a database on another system—this guide will use a  
 1907 local PostgreSQL database, however.
- 1908 f. When it finishes installing, there should be a configuration wizard (see below for configuration  
 1909 steps).

### 1910 2.13.2 Configure Tripwire Log Center Manager

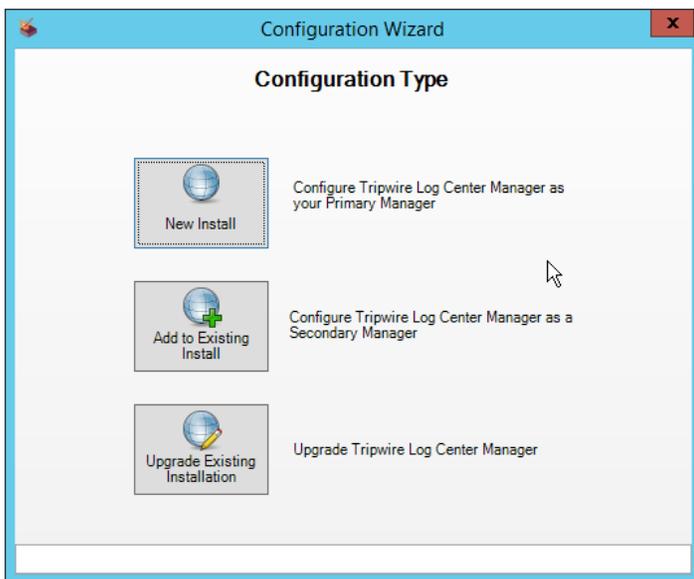
- 1911 1. The configuration wizard should start after the installation is complete.



1912

1913

2. Click **Start**.

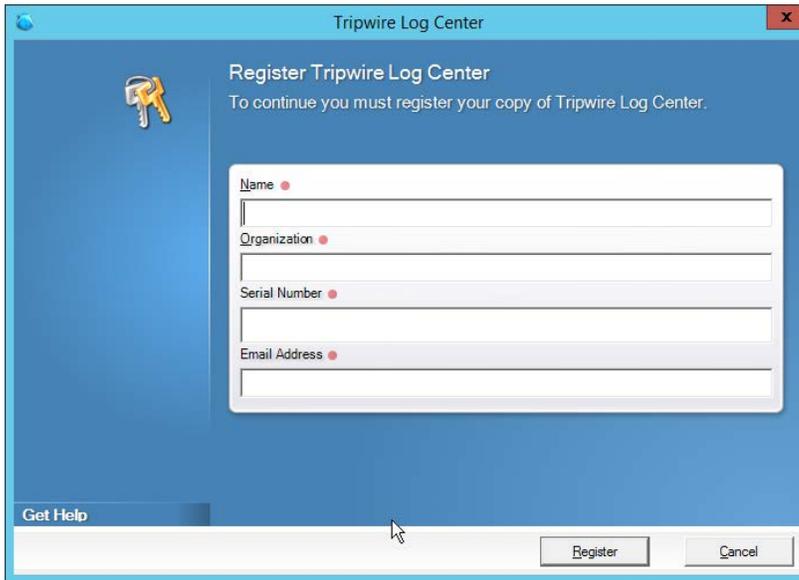


1914

1915

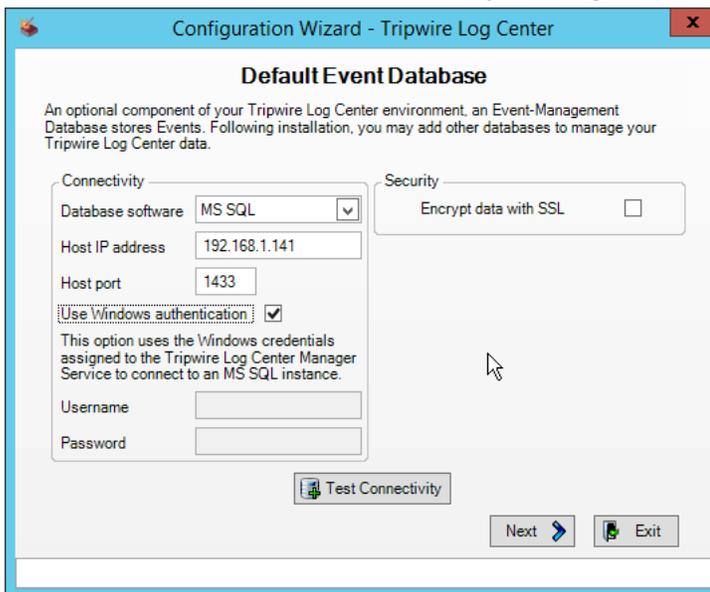
1916

3. Click **New Install**.
4. Enter the registration details for your **Tripwire Log Center** license.



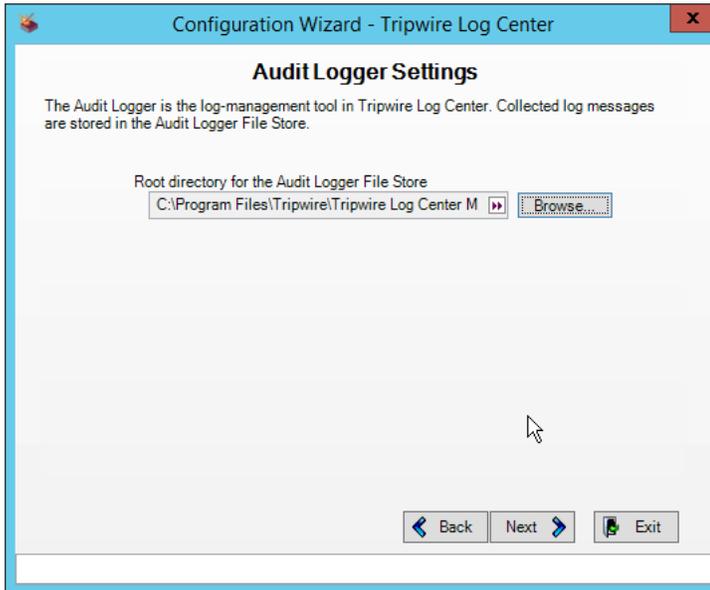
1917  
1918  
1919

5. Click **Register**.
6. Enter details about the database that **Tripwire Log Center** should use.



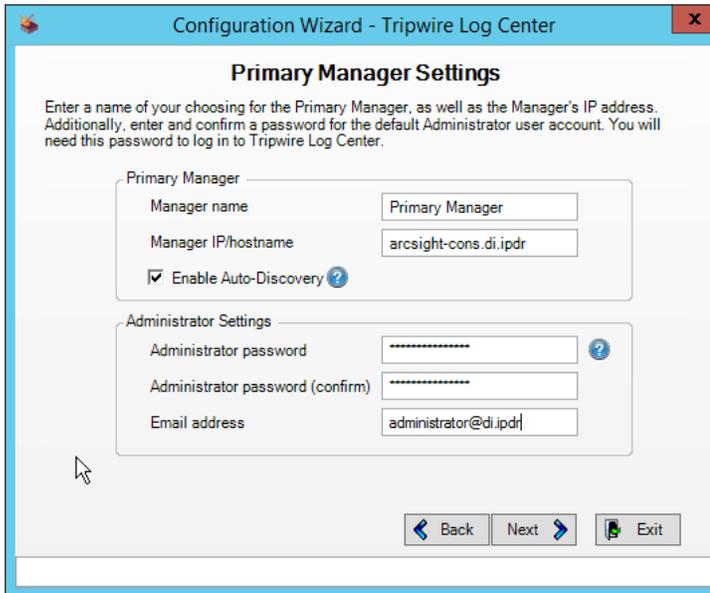
1920  
1921  
1922  
1923

7. Click **Next**.
8. Select a directory in which to store log messages, such as C:\Program Files\Tripwire\Tripwire Log Center Manager\Logs\AUDIT.



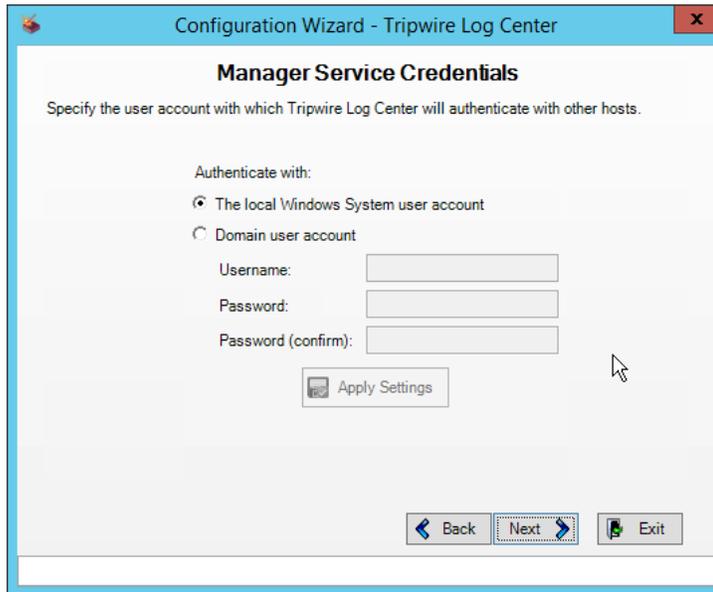
1924  
1925  
1926  
1927

9. Click **Next**.
10. Enter a **password** and an **email**.
11. Change the IP to a hostname if preferred.



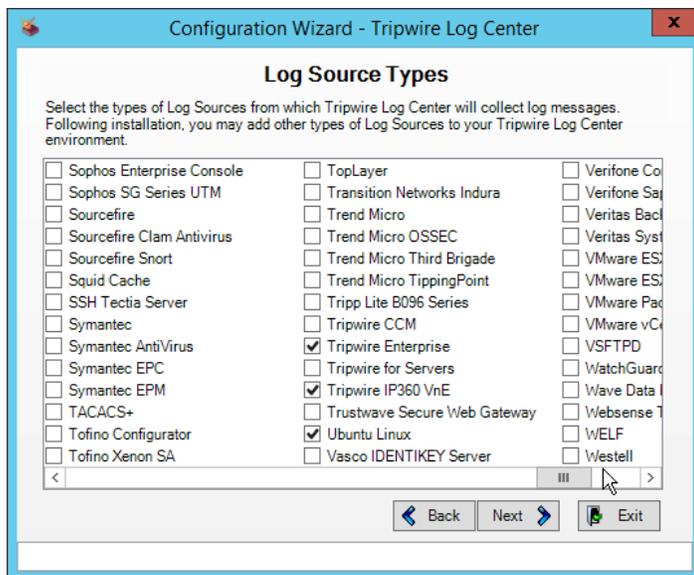
1928  
1929

12. Click **Next**.



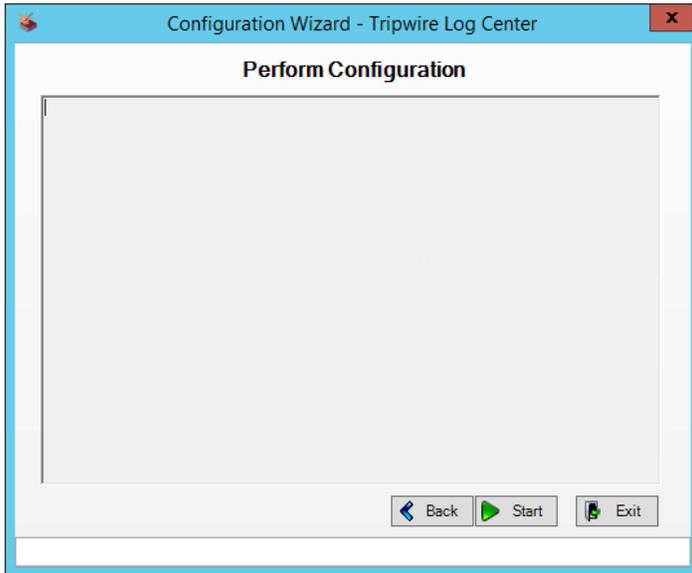
1930  
1931  
1932  
1933  
1934

13. Click **Next**.
14. Select any log sources that you expect to collect with **Tripwire Log Center**. Examples: Tripwire Enterprise, Microsoft Windows 10, Tripwire IP360 VnE, Linux Debian, Ubuntu Linux, Microsoft Exchange, Microsoft SQL Server.



1935  
1936

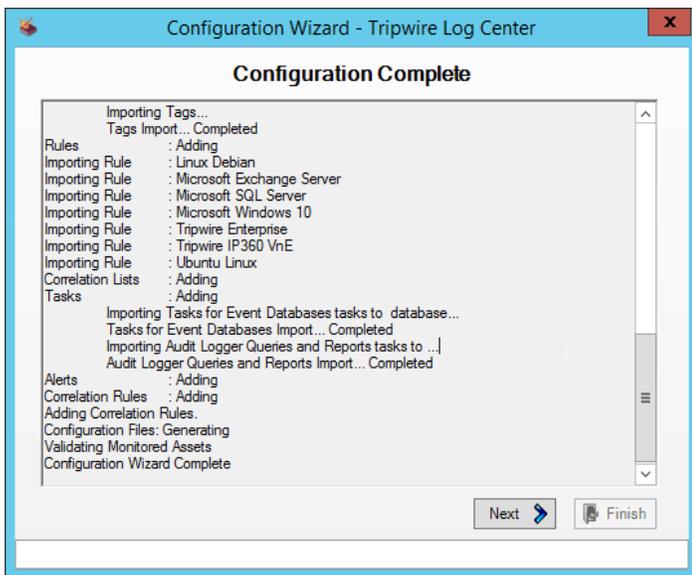
15. Click **Next**.



1937

1938

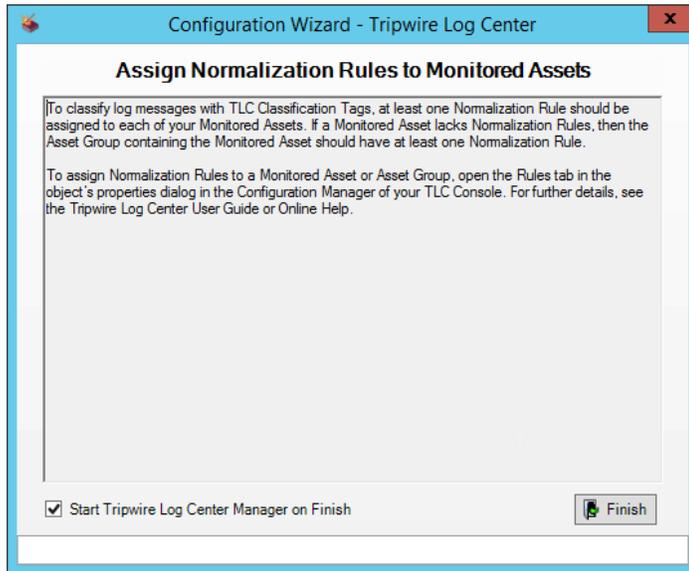
16. Click **Start**.



1939

1940

17. Click **Next**.



1941

1942 18. Click **Finish**.

### 1943 2.13.3 Install Tripwire Log Center Console

1944 Chapter 4 of the *Tripwire Log Center 7.3.1 Installation Guide* details installation of the **Tripwire Log**  
 1945 **Center Console**. Use the **Tripwire Log Center Console** installer.

1946 You can install this on the same machine as the Tripwire Log Center Manager, if desired.

## 1947 2.14 Cisco Web Security Appliance

1948 This section details installation and some configurations for the Cisco Web Security Appliance (WSA). It  
 1949 assumes the use of the WSA virtual machine.

### 1950 2.14.1 Network Configuration

- 1951 1. Log in to WSA by using the default **username** and **password** (admin/ironport).
- 1952 2. Use the command `sethostname` to set the hostname of the machine.
- 1953 3. Use the command `dnsconfig` to set the DNS server. Enter **SETUP** when prompted, and then  
 1954 enter DNS information specific to your organization's needs.
- 1955 4. Use the command `interfaceconfig` to set the IP of the machine. Enter **EDIT** when  
 1956 prompted, and then enter IP information specific to your organization's needs.
- 1957 5. Use the command `passwd` to change the default password of the machine.

- 1958 6. Use the command `commit` to commit all of these changes.
- 1959 7. Use the command `reboot` to reboot the machine.
- 1960 8. Use the command `loadlicense` to either paste the license file contents or select a license
- 1961 file uploaded via FTP. You can enable FTP in the `interfaceconfig` command.
- 1962 9. You should be prompted at the console to visit a web page in the browser, usually
- 1963 `http://<ip_address>:8080`. The setup wizard will be here.

## 1964 2.14.2 System Setup

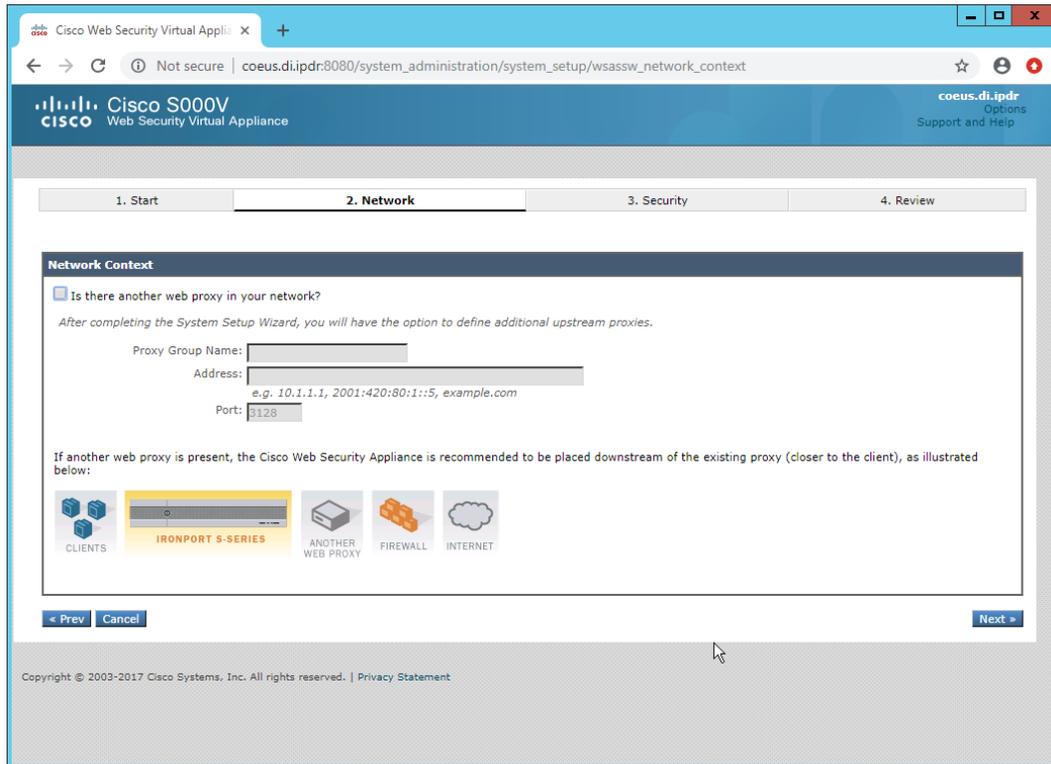
- 1965 1. In the web console, click **System Administration > System Setup Wizard**.
- 1966 2. Verify that the hostname matches the desired hostname.
- 1967 3. Enter the desired **DNS servers**.
- 1968 4. Enter a **time server** if desired.
- 1969 5. Select the time zone.
- 1970 6. Select **Standard** for an on-premise setup.

The screenshot shows the Cisco S000V Web Security Virtual Appliance System Setup Wizard. The wizard is in the '2. Network' step. The 'System Settings' section includes: Default System Hostname: coeus.di.ipdr; DNS Server(s): Use these DNS Servers (192.168.1.12); NTP Server: time.dmz.nccoe.nist.gov; Time Zone: Region: America, Country: United States, Time Zone / GMT Offset: Eastern Time (New\_York). The 'Appliance Mode' section has 'Standard' selected. Navigation buttons: < Prev, Cancel, Next >.

1971

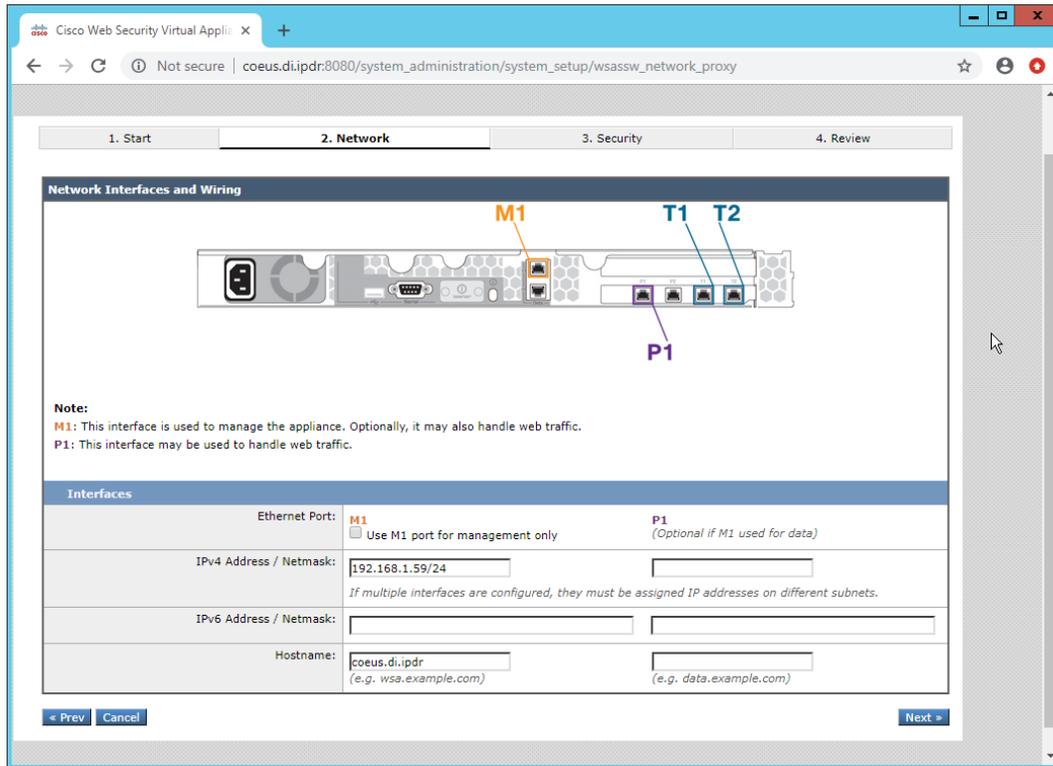
1972

7. Click **Next**.



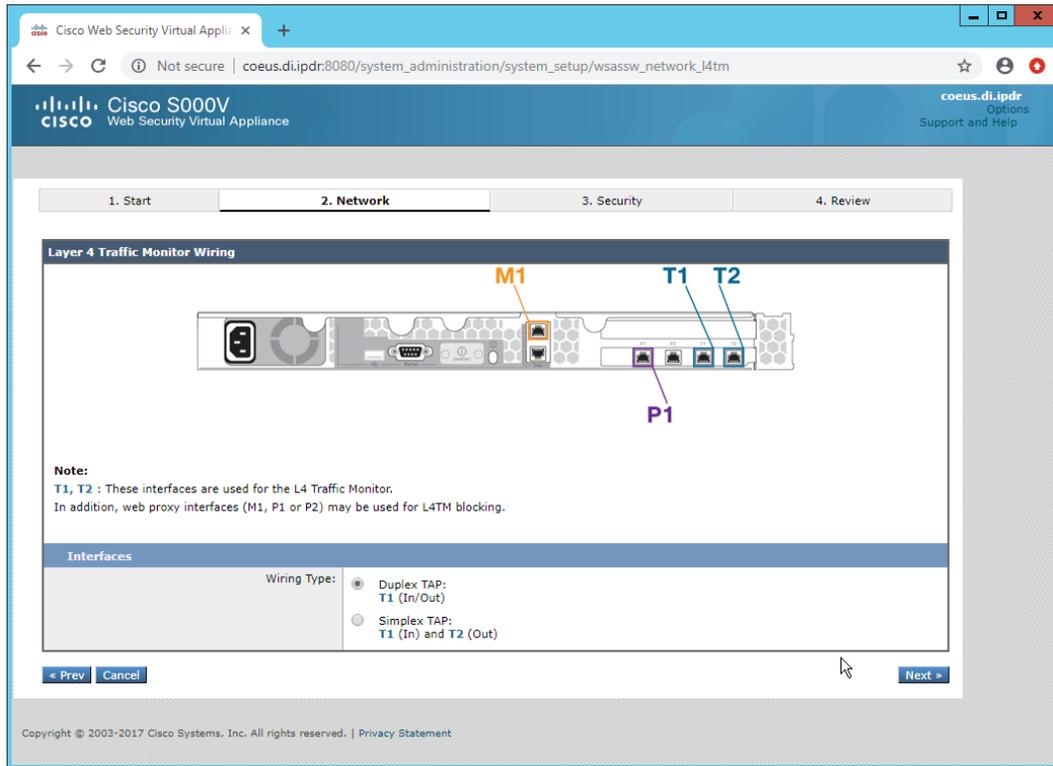
1973  
1974  
1975

8. Click **Next**.
9. Verify that the interface is correctly configured.



1976  
1977

10. Click **Next**.



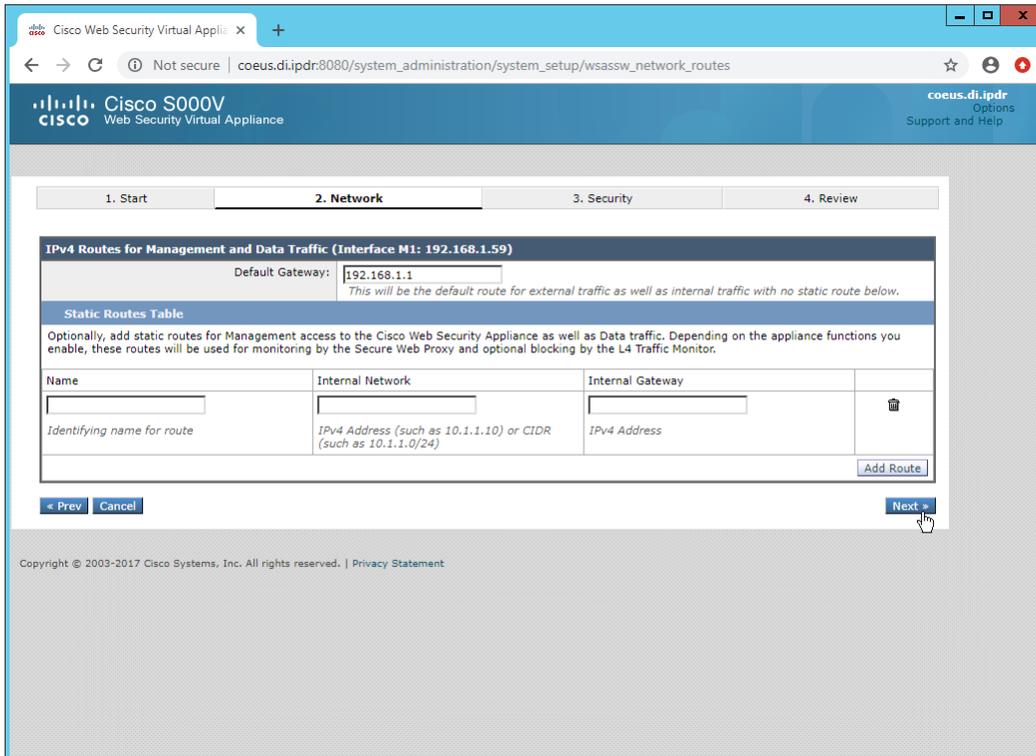
1978

1979

1980

11. Click **Next**.

12. Enter the **default gateway** and any additional gateways to use for routing.



1981

1982

13. Click **Next**.

1. Start    **2. Network**    3. Security    4. Review

**Transparent Connection Settings**

For the Cisco Web Security Appliance to accept transparent connections, it must be connected via a Layer 4 switch or WCCP router.

Transparent Redirection Device:

- Layer 4 Switch or No Device  
*If no transparent redirection device is connected, only explicit forward requests can be proxied.*
- WCCP v2 Router
  - Enable standard service ID: 0 web\_cache (port 80)
  - Router Addresses:   
*Separate multiple addresses with commas or whitespace.*
  - Enable router security for this service
    - Passphrase:
    - Confirm Passphrase:   
*Must be 7 or less characters.*

*Additional WCCP services and advanced options can be configured after completing the System Setup Wizard.*

< Prev    Cancel    Next >

Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

1983

1984

14. Click **Next**.

1985

15. Set a **passphrase** for the administrator.

1986

16. Enter an **email address** to which alerts should be sent.

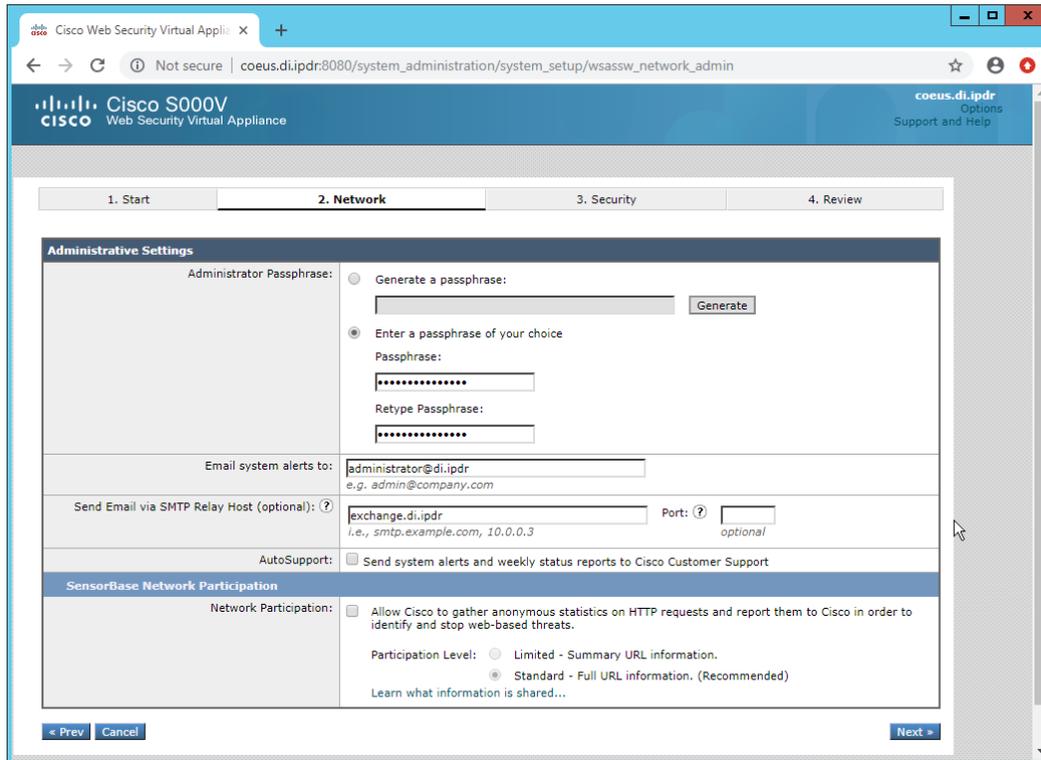
1987

17. Enter the **hostname** of the email server.

1988

18. Decide whether to forward alerts and reports to Cisco Customer Support, as well as whether to share anonymous statistics based on the needs of your organization.

1989



1990

1991

1992

1993

1994

1995

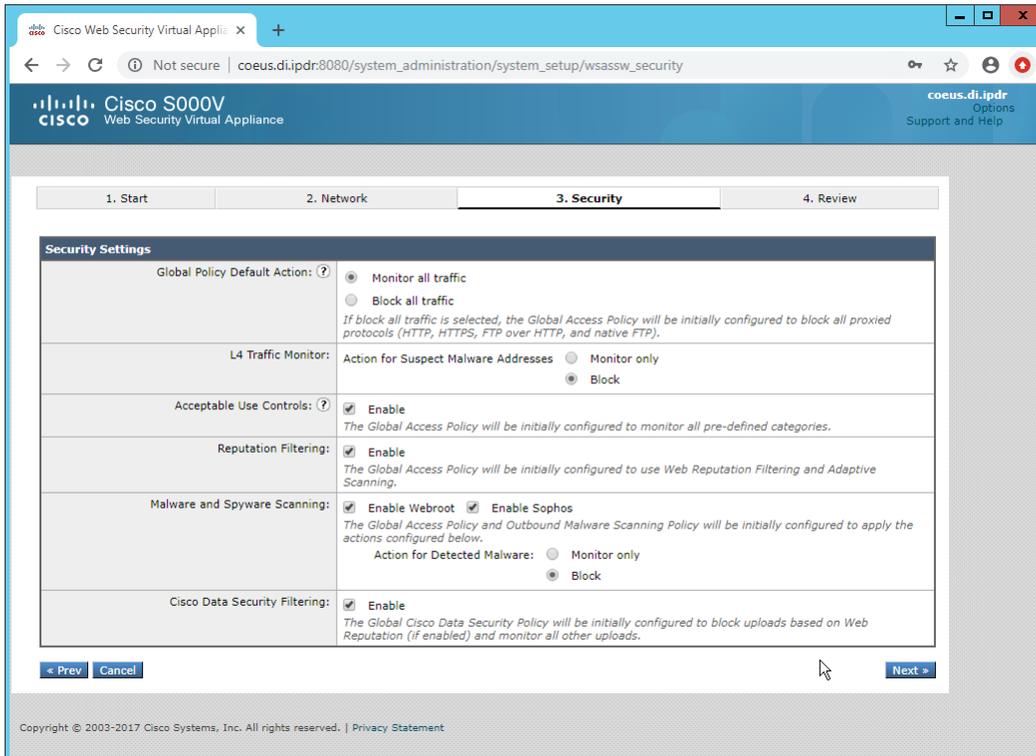
19. Click **Next**.

20. Select **Monitor All Traffic**.

21. Select **Block** for **Action for Suspect Malware Addresses**.

22. Select **Block** for **Action for Detected Malware**.

23. Configure the rest of the malware policy according to your organization's needs.



1996

1997

24. Click **Next**.

Management (M1)	
IPv4 Address:	192.168.1.59/24
Hostname:	coeus.di.ipdr
Use M1 port for management only:	No
L4 Traffic Monitor:	
Wiring Type:	Duplex TAP: T1 (In/Out)
Routes	
Default IPv4 Gateway:	192.168.1.1
Static IPv4 Routes:	No static routes have been defined.
Transparent Connection Settings	
Transparent Redirection Device Type:	Layer 4 Switch or No Device
Administrative Settings	
Administrator Passphrase:	(hidden)
Email System Alerts To:	administrator@di.ipdr
Internal SMTP Relay Hosts:	exchange.di.ipdr:25
AutoSupport:	No
SensorBase Network Participation:	No
Security Settings	
Global Policy Default Action:	Monitor
L4 Traffic Monitor:	Monitor and Block
Acceptable Use Controls:	Enabled
Reputation Filtering:	Enabled
Cisco DVS Engine:	Webroot: Enabled McAfee: Disabled Sophos: Enabled
Cisco Data Security Filtering:	Disabled

1998

1999 25. Click **Install This Configuration**.2000 

### 2.14.3 Using WSA to Proxy Traffic

2001 Cisco WSA is intended to act as a proxy between clients and the internet, to prevent malicious traffic  
 2002 and software from reaching the client systems before they can do any damage. The appliance must  
 2003 have a way of intercepting traffic from the clients to the internet.

2004 To achieve this, we used a Proxy Auto Config (PAC) file on our DNS server (Windows 2012 DNS), and this  
 2005 section details how to set up a simple PAC file to forward all traffic to WSA. This may not be an ideal  
 2006 setup for every environment, particularly in environments that use an external DNS server.

2007 **2.14.3.1 Creating a PAC File**

- 2008 1. Create a new file named **wpad.dat** and enter the following JavaScript function:

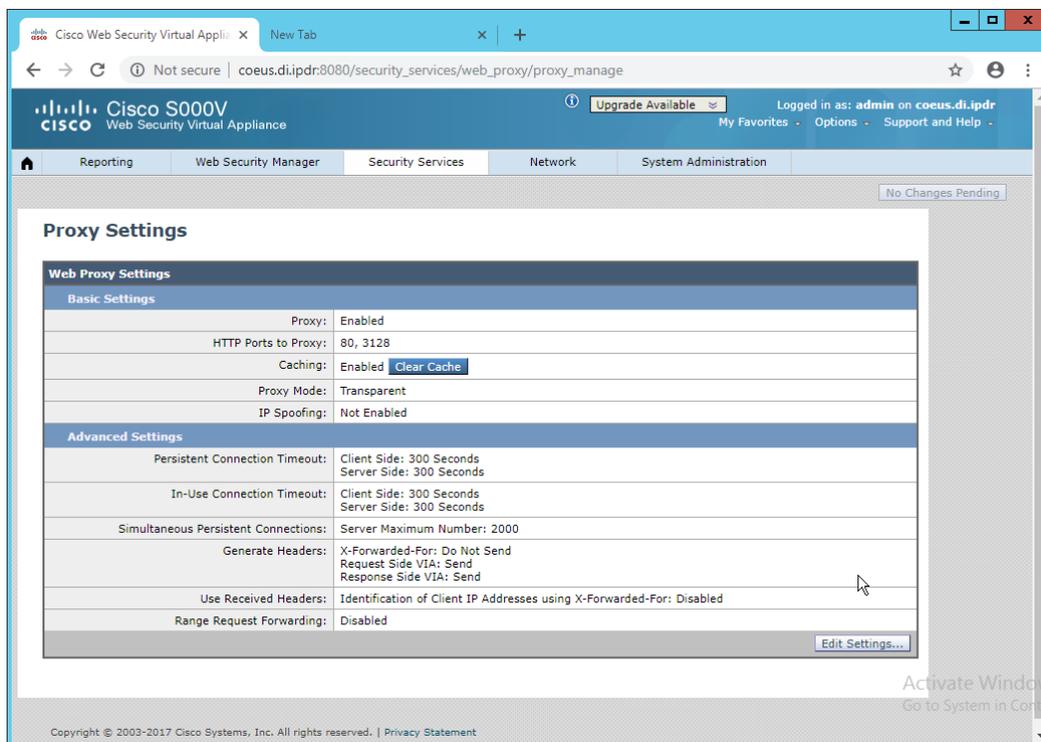
```
function FindProxyForURL(url, host) {
    return "PROXY coeus.di.ipdr:3128";
}
```

2009

2010 This is the most basic template for a proxy that directs all traffic to the host coeus.di.ipdr. The  
 2011 return value of this function can take the form "PROXY <hostname1>; PROXY  
 2012 <hostname2>" if you wish to have fail-over proxies, or "DIRECT" to not use any proxy. You can  
 2013 also add rules to allow certain types of traffic through the proxy or direct them to other proxies. For  
 2014 more information, see <https://findproxyforurl.com>.

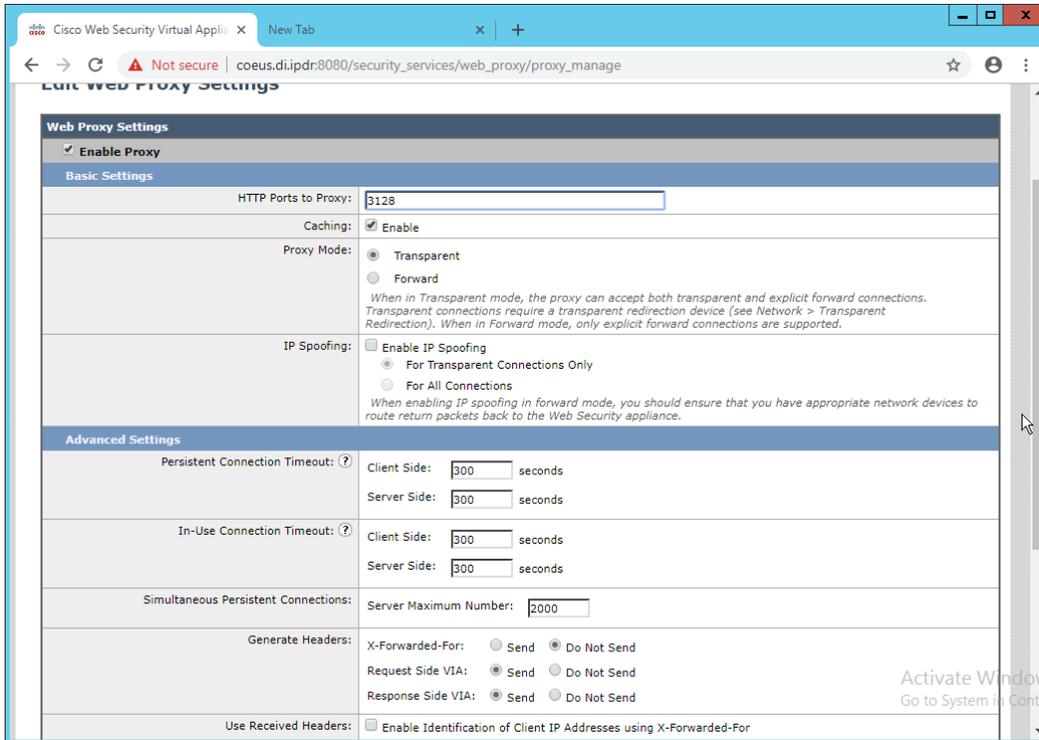
2015 For the purposes of our setup, we will simply direct all traffic to Cisco WSA, but be aware that PAC  
 2016 files can be more complex and designed according to the needs of the organization.

- 2017 2. In the web console, navigate to **Security Services > Web Proxy**.



2018

- 2019 3. Click **Edit Settings**.
- 2020 4. Remove port 80 from **HTTP Ports to Proxy** (ensure that **3128** is in this field).



- 2021 5. Click **Submit**.
- 2022 6. Navigate to **Security Services > PAC File Hosting**.
- 2023 7. Click **Enable and Edit Settings**.
- 2024 8. Under **PAC Files**, click **Choose File**.
- 2025 9. Select the **wpad.dat** file created earlier.
- 2026 10. Click **Open**.
- 2027 11. Click **Upload**.
- 2028 12. Enter **80** for **PAC Server Ports**.
- 2029

The screenshot shows the 'Edit Proxy Auto-Configuration File Hosting Settings' page in a web browser. The page is titled 'Edit Proxy Auto-Configuration File Hosting Settings' and has a 'Commit Changes' button in the top right corner. The main content is organized into several sections:

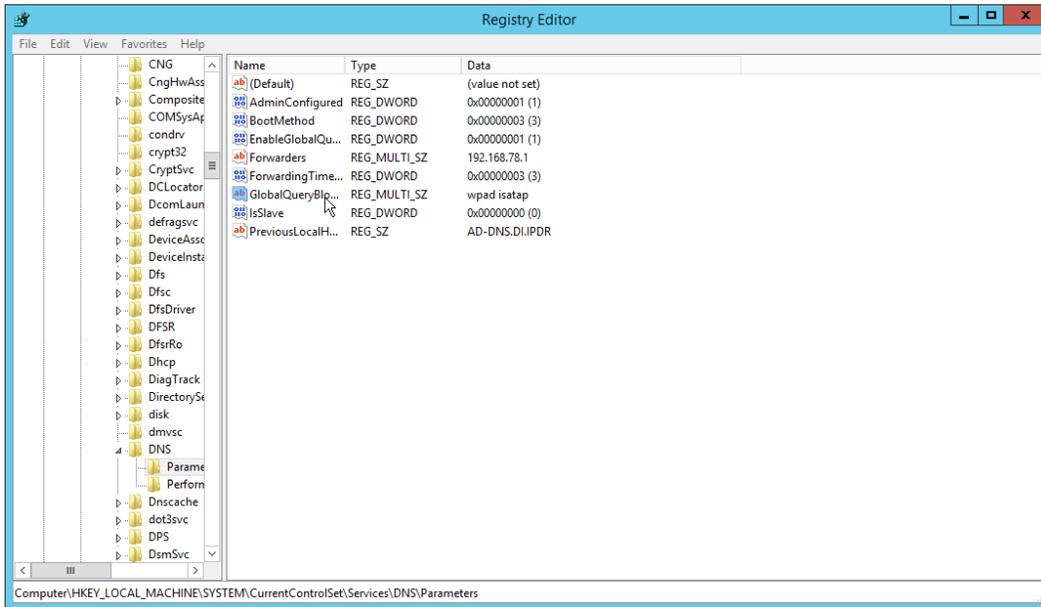
- Proxy Auto-Configuration File Hosting:** A section with a checked checkbox for 'Enable Proxy Auto-Config File Hosting'.
- Basic Settings:** Contains two main settings:
  - PAC Server Ports:** A text input field containing '80' with a note: 'Enter multiple ports separated with a comma'.
  - PAC File Expiration:** A checkbox for 'Allow PAC file to expire in browser's cache'. Below it, a note states: 'PAC file will expire after [0] minutes. If this option is enabled, some supported browsers will automatically download a new copy of the PAC file if it is available after the defined expiration schedule.'
- PAC Files:** A section with an 'Uploaded Files' table. The table has one row with 'wpad.dat' and a 'Download PAC File...' link. Below the table is a 'Choose File' button and an 'Upload' button.
- Hostnames for Serving PAC Files Directly:** A section with a table for adding hostnames. The table has two columns: 'Hostname' and 'Default PAC File for "Get/" Request through Proxy Port'. The second column has a dropdown menu currently set to 'wpad.dat' and an 'Add Row' button.

At the bottom of the page, there is a 'Cancel' button on the left and a 'Submit' button on the right. The footer contains the text: 'Copyright © 2003-2017 Cisco Systems, Inc. All rights reserved. | Privacy Statement'.

- 2030
- 2031 13. Click **Submit**.
- 2032 14. Click **Commit Changes**.
- 2033 15. Enter a comment if desired.
- 2034 16. Click **Commit Changes**.

2035 *2.14.3.2 Setting Up Web Proxy Auto Discovery (WPAD)*

- 2036 1. On the DNS server, open **regedit.exe**.
- 2037 2. Navigate to **HKEY\_LOCAL\_MACHINE > SYSTEM > CurrentControlSet > Services > DNS >**
- 2038 **Parameters**.

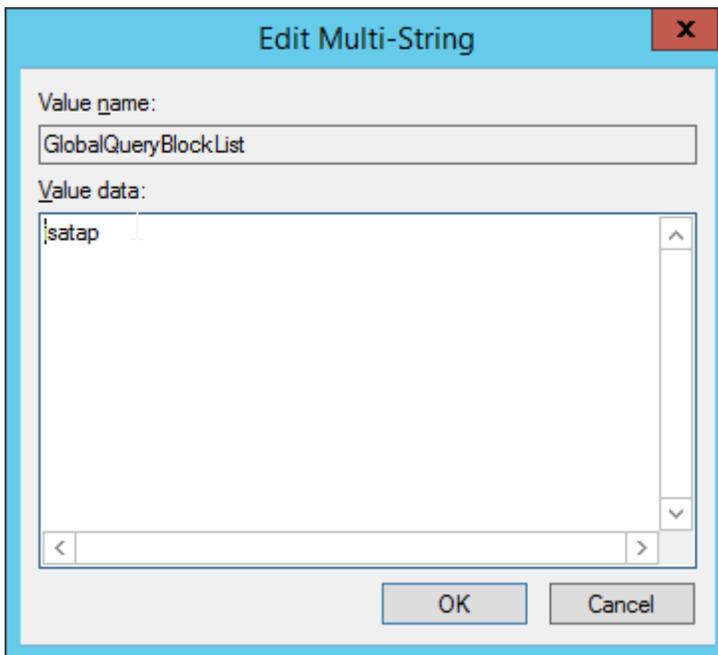


2039

2040

2041

3. Double-click **GlobalQueryBlockList**.
4. Remove wpad from the list but leave isatap on the list.



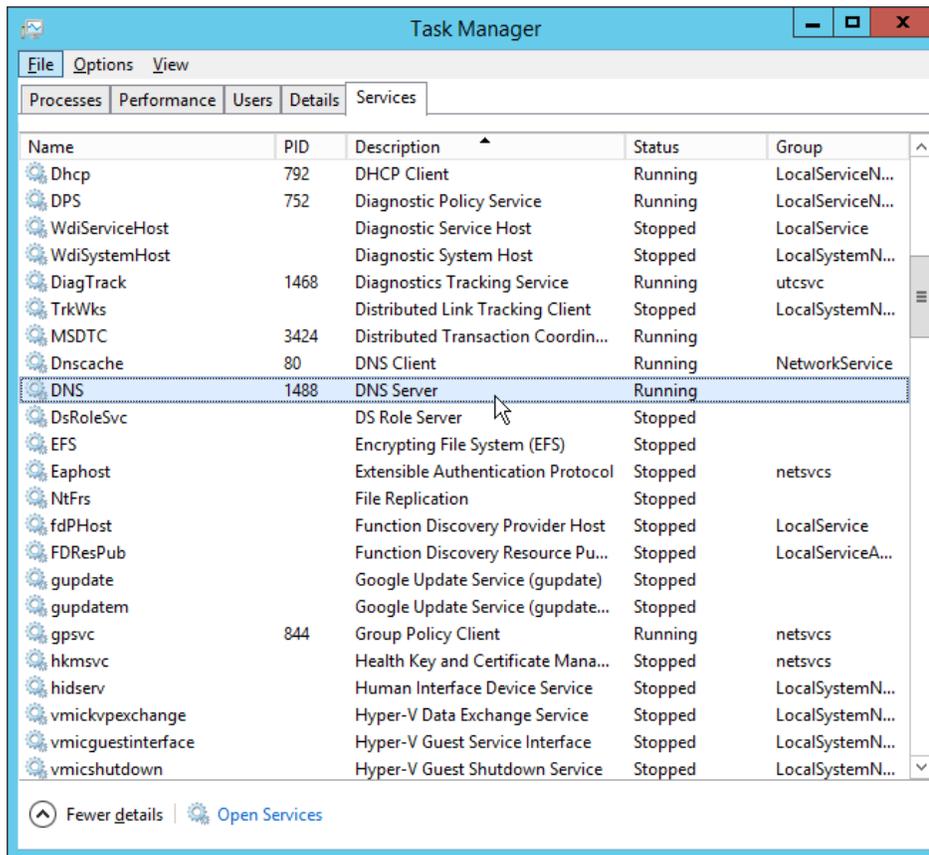
2042

2043

2044

2045

5. Click **OK**.
6. Open **Task Manager**.
7. Click **Services**.



2046

2047

8. Restart the **DNS Server** service.

2048

9. Open **DNS Manager**.

2049

10. Right-click on your enterprise's domain, and click **New Host (A or AAAA)**.

2050

11. Enter **wpad** for **Name**.

2051

12. Enter the **IP address** of WSA.

2052

2053 13. Click **Add Host**.

2054 This will set up the WPAD proxy file as the default proxy—so browsers that are using “Automatically  
 2055 detect settings” for their proxy setting will find this file. Be aware that this is not sufficient for a  
 2056 secure setup but will allow you to quickly test the proxy’s functionality.

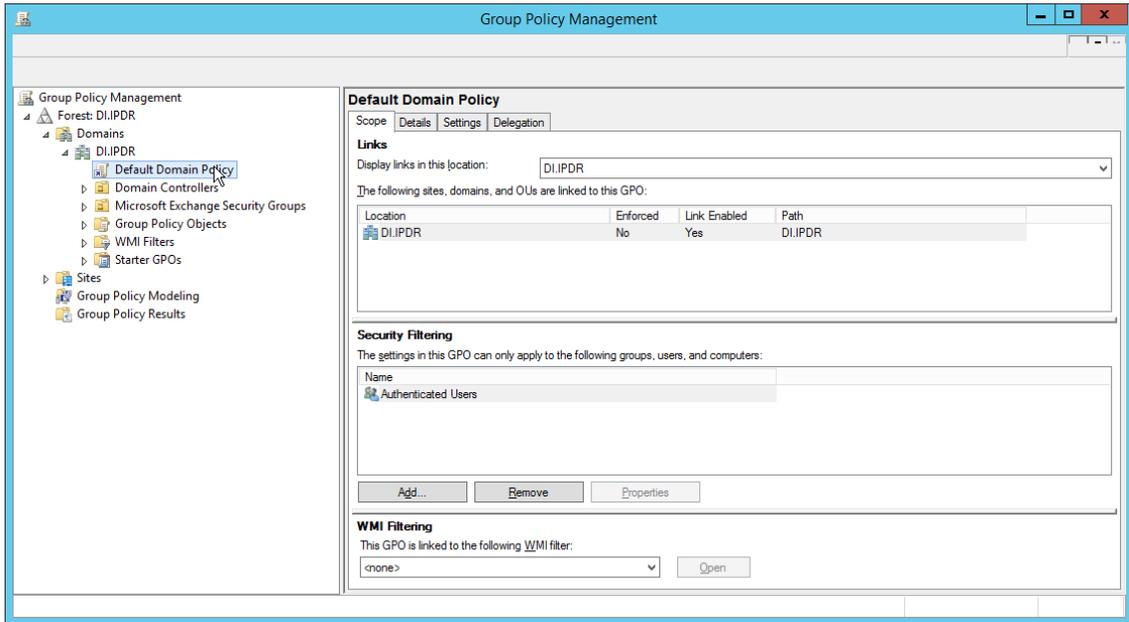
### 2057 *2.14.3.3 Configure Group Policy to Use Explicit Proxy*

2058 Note that, at this point, WPAD is vulnerable to an attack where the server hosting WPAD is brought  
 2059 down and the browser automatically attempts to find the next WPAD proxy, which may be  
 2060 controlled by an attacker.

2061 To mitigate this vulnerability, we explicitly point to this proxy file with any browsers used by clients.  
 2062 For Internet Explorer and Google Chrome, it is sufficient to change group policy in Active Directory  
 2063 to direct the change across all systems.

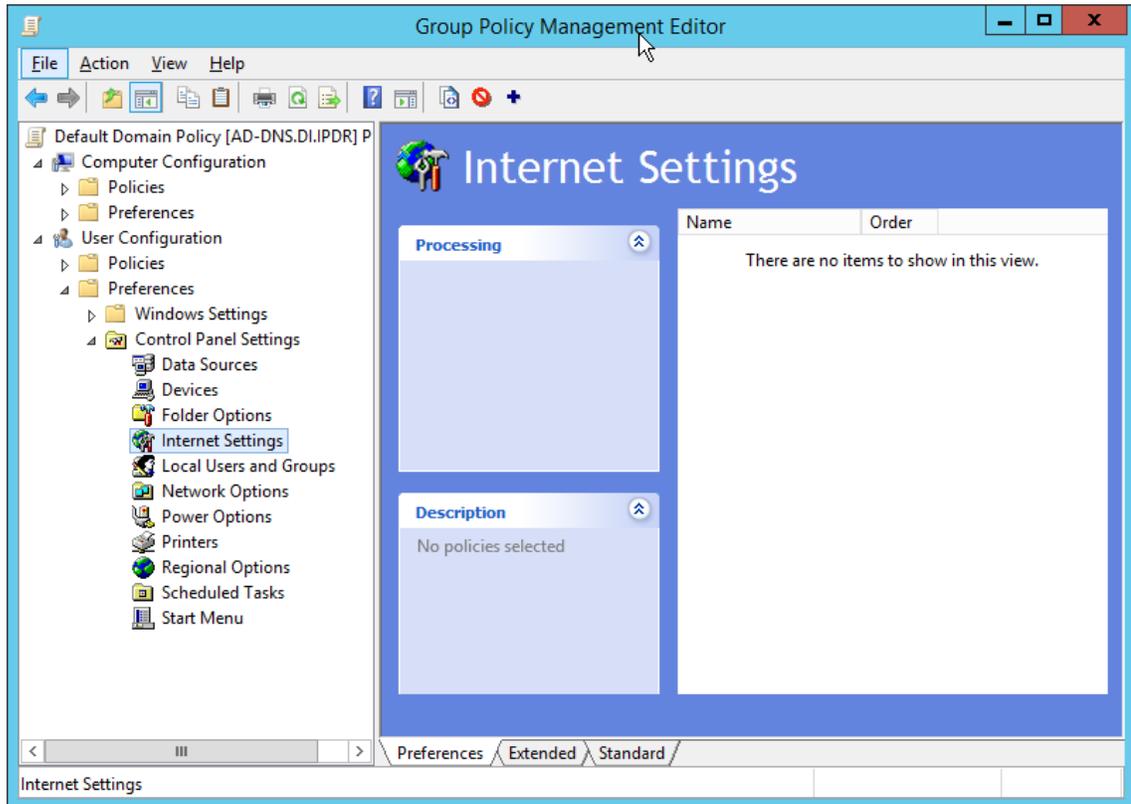
2064 For Mozilla Firefox, see this link (<https://support.mozilla.org/en-US/kb/connection-settings-firefox>)  
 2065 for configuration, including how to set it to “Use system proxy settings.”

2066 1. In **Group Policy Management**, right-click the **Default Domain Policy** and click **Edit**.



2067  
2068  
2069

2. In Group Policy Management Editor, navigate to **User Configuration > Preferences > Control Panel Settings > Internet Settings**.

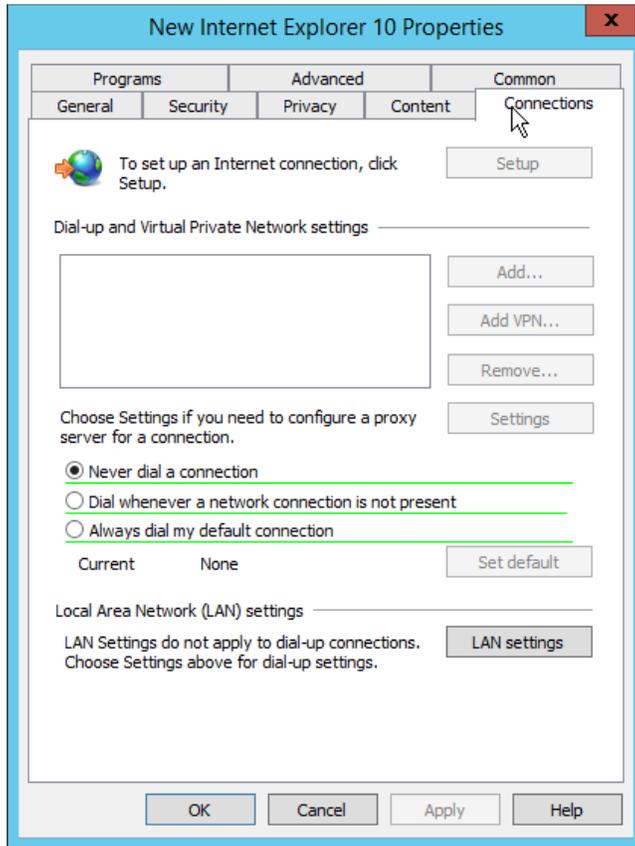


2070

2071

2072

3. Right-click **Internet Settings** and select **New > Internet Explorer 10**.
4. Click the **Connections** tab.



2073

2074

2075

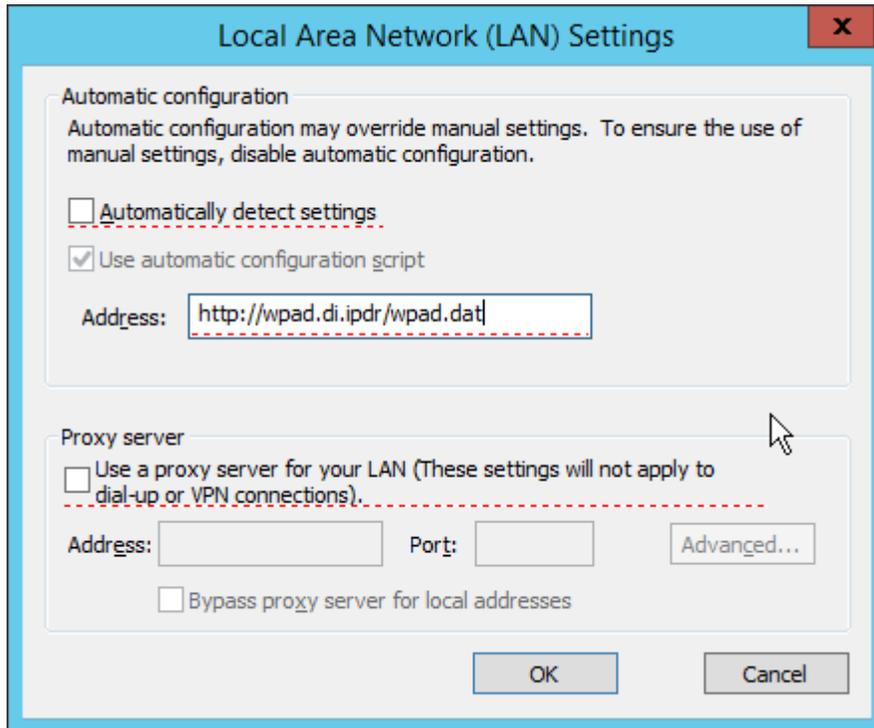
2076

2077

2078

2079

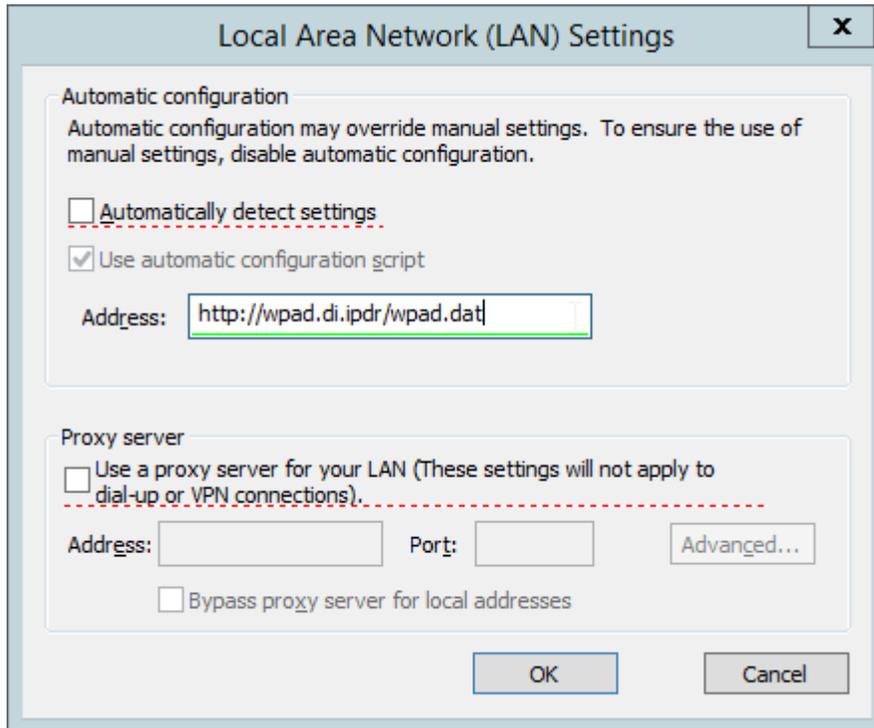
5. Click **LAN Settings**.
6. Enter the **address** of the WPAD file for address. This will likely take the form <http://wpad.my.domain/wpad.dat> if you followed these instructions for configuring the proxy file.
7. Press the **F8** key to disable all settings in this dialogue box. (Note: This should underline everything in the box in red.)



2080

2081

8. Select the **Address** you just entered.



2082

2083 9. Press **F6** to enable this setting. (Note: The explicit WPAD address should now be underlined in  
2084 green.)

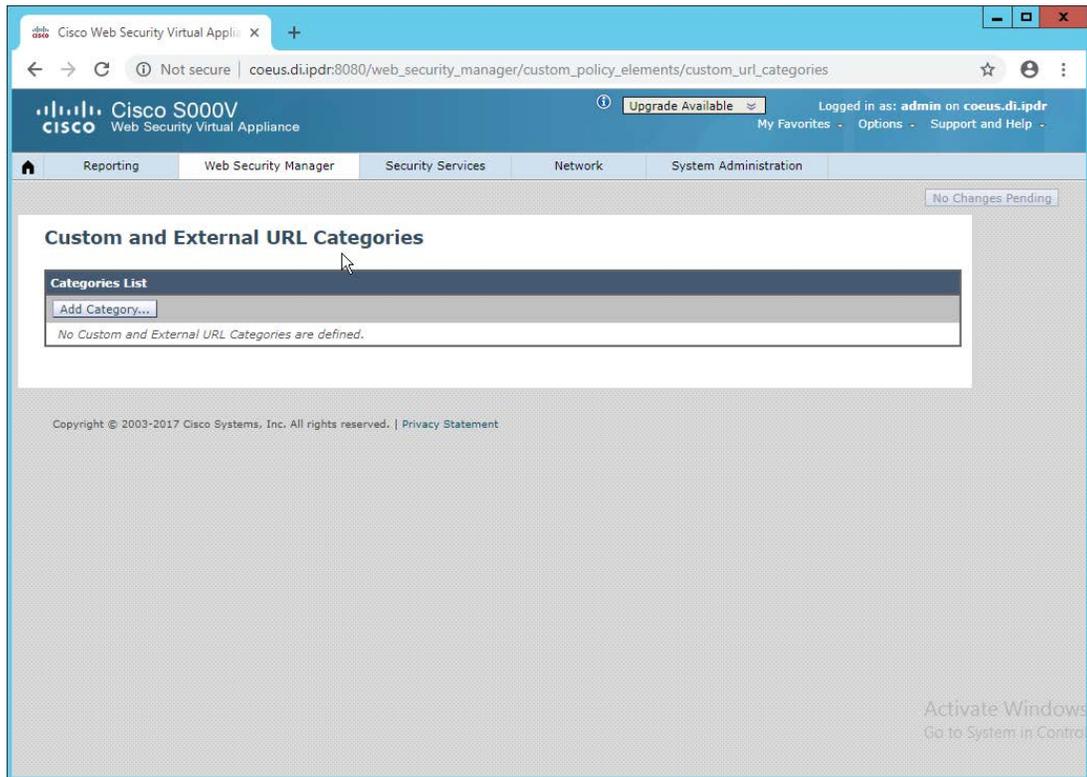
2085 10. Click **OK**.

2086 11. Click **OK**.

2087 This Group Policy Object will update across all Windows systems whenever gpupdate.exe runs. An  
2088 insider or technically capable user could manually disable this to avoid using the proxy, but benign  
2089 clients who do not attempt to circumvent it will be protected from external (internet-based) threats  
2090 by Cisco WSA. Protection from insiders and local threats on the network is provided by other  
2091 products in the architecture, such as the network protection component (CryptoniteNXT).

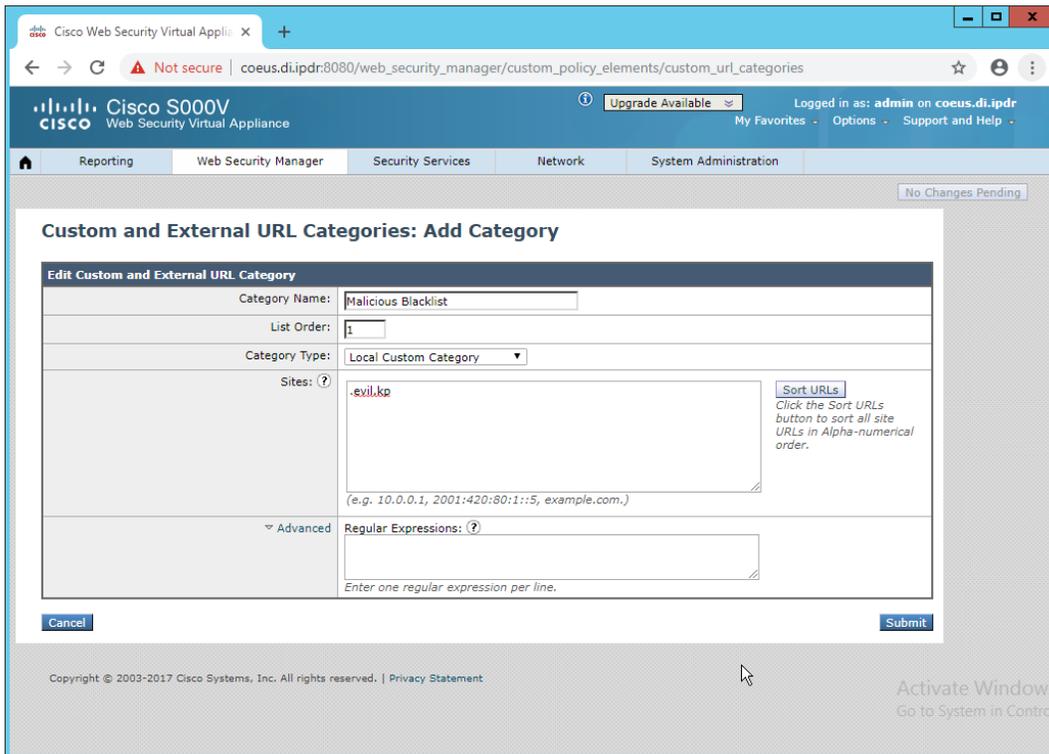
#### 2092 2.14.4 Blacklisting

2093 1. Navigate to **Web Security Manager > Custom and External URL Categories**.



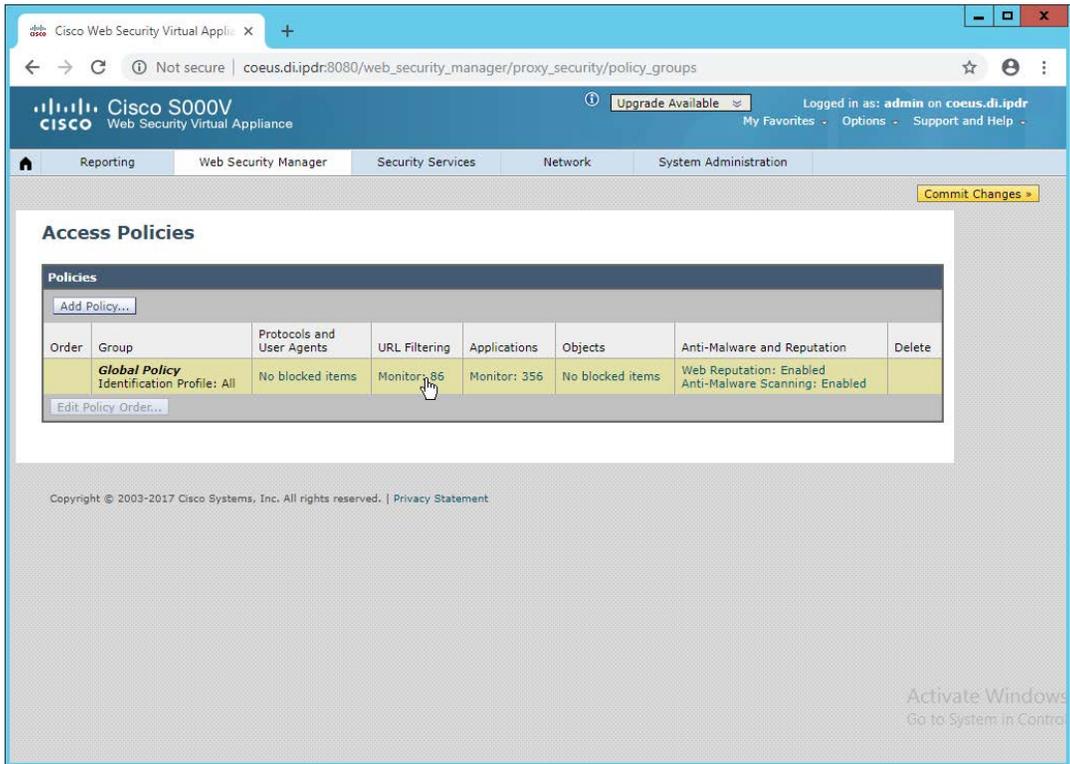
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102

2. Click **Add Category**.
3. Enter a **name** for **Category Name**.
4. Select **Local Custom Category**. (The other option, **External Live Feed Category**, allows WSA to use a list of websites hosted somewhere else, potentially externally. For this demonstration we will simply enter websites in the **Sites** field, but note that this other option is available for convenience.)
5. For **Sites**, enter any sites to blacklist. (Note: Entering **.mysite.abc** will include any subdomains of **mysite.abc**.)



2103  
2104  
2105

6. Click **Submit**.
7. Navigate to **Web Security Manager > Access Policies**.



2106

2107

8. Click the link under **URL Filtering**.

Access Policies: URL Filtering: Global Policy

**Custom and External URL Category Filtering**

No Custom Categories are included for this Policy.

Select Custom Categories...

**Predefined URL Category Filtering**

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

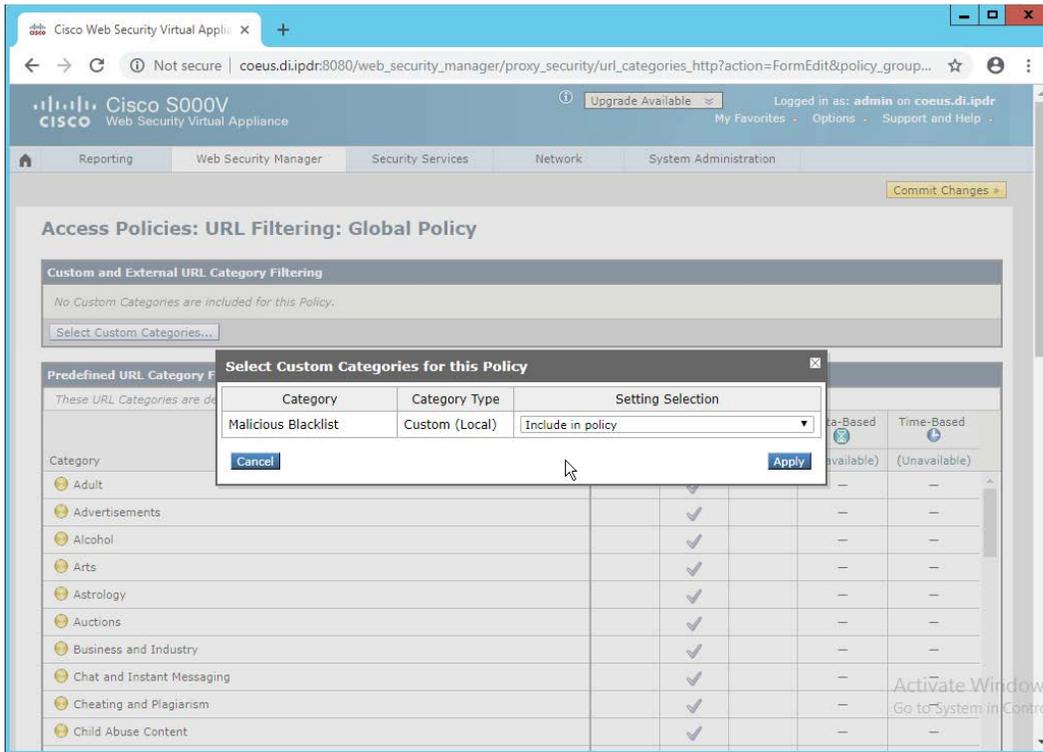
Category	Block	Monitor	Warn (?)	Quota-Based	Time-Based
	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Adult		✓		—	—
Advertisements		✓		—	—
Alcohol		✓		—	—
Arts		✓		—	—
Astrology		✓		—	—
Auctions		✓		—	—
Business and Industry		✓		—	—
Chat and Instant Messaging		✓		—	—
Cheating and Plagiarism		✓		—	—
Child Abuse Content		✓		—	—

2108

2109

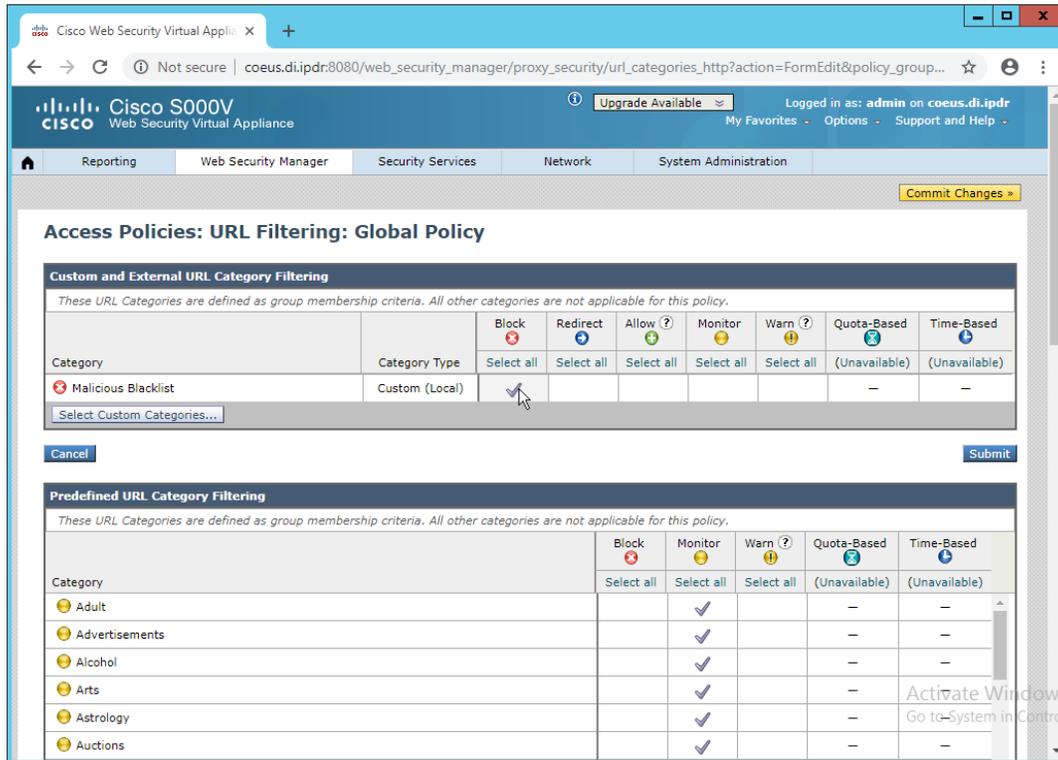
2110

9. Click **Select Custom Categories**.10. For the category just created, select **Include in policy** under **Setting Selection**.

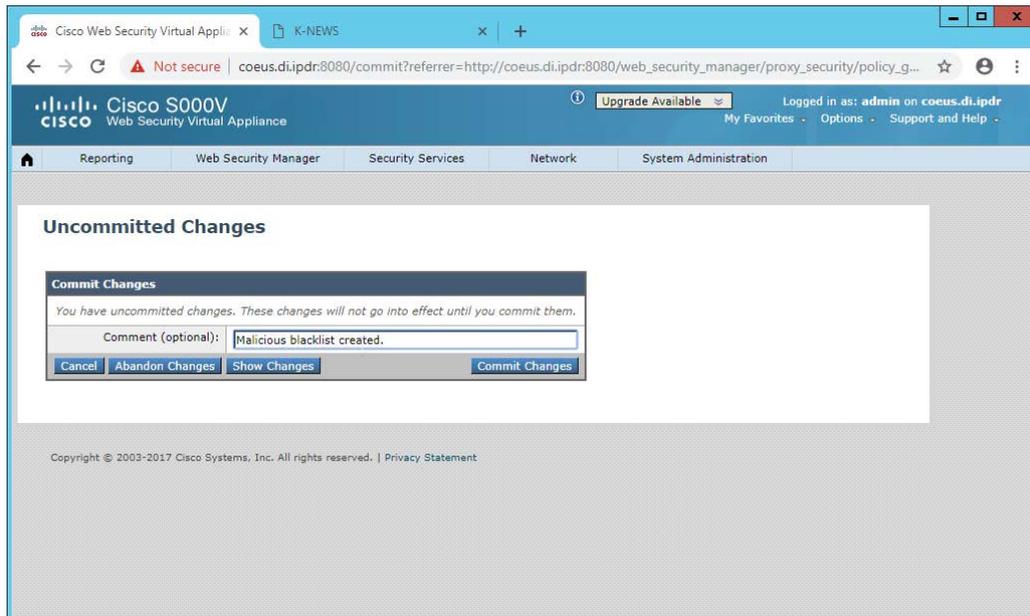


2111  
2112

11. Click **Apply**.



- 2113
- 2114 12. The category should now show under **Custom and External URL Category Filtering**. Put a
- 2115 checkmark in the **Block** box. (Selecting **Allow** lets you white-list domains that are being
- 2116 incorrectly classified as malicious.)
- 2117 13. Click **Submit**.
- 2118 14. Click **Commit Changes**.
- 2119 15. Enter a comment if desired.



2120

2121 16. Click **Commit Changes**.

2122

2123 

## 2.15 Symantec Data Loss Prevention

2124 

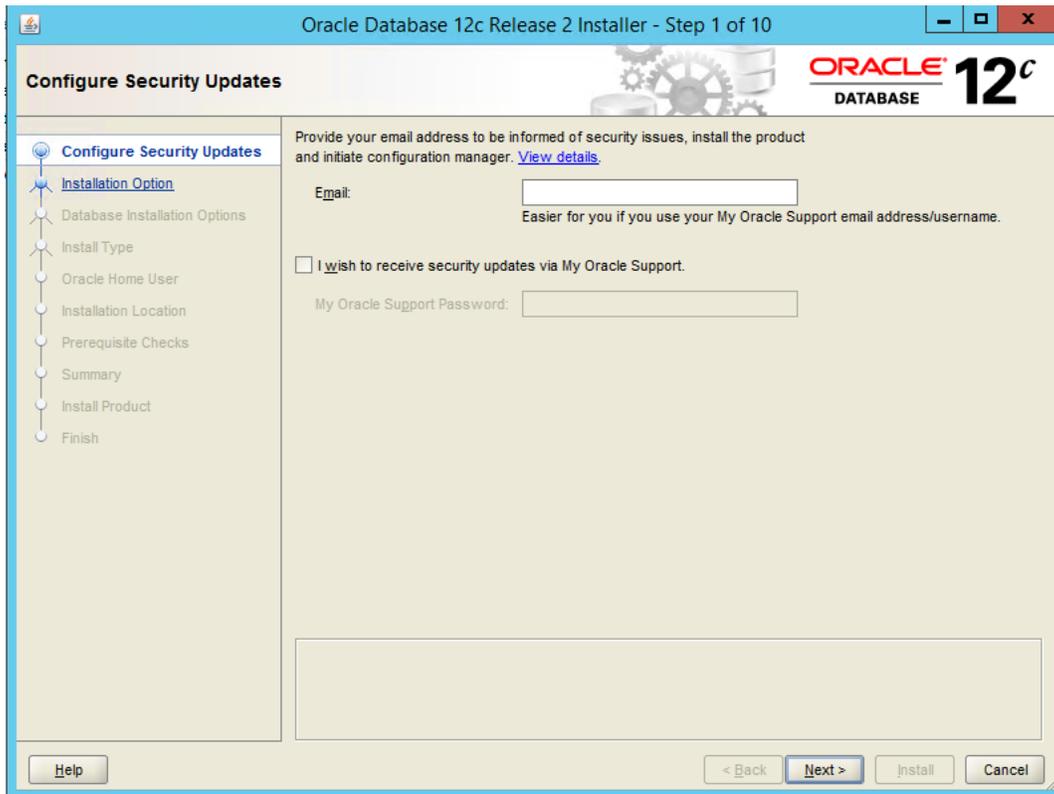
### 2.15.1 Install Oracle 12c Enterprise

- 2125 1. Unzip the Symantec DLP installation files.
- 2126 2. Download the Oracle 12c installation files from <https://www.oracle.com> if they are not included
- 2127 with the Symantec DLP installation files.
- 2128 3. Move both sets of installation files to a temporary directory, such as **C:\temp**.
- 2129 4. Copy the Symantec **12.2.0.1\_64\_bit\_Installation\_Tools** folder to **C:\temp\Oracle\tools**.
- 2130 5. From a command prompt, navigate to **C:\temp\Oracle\database**, assuming the Oracle
- 2131 installation files were unzipped to **C:\temp\Oracle**.
- 2132 6. Run the following command:
- 2133 

```
> C:\temp\Oracle\database\setup.exe -noconfig -responsefile
```
- 2134 

```
C:\temp\Oracle\tools\responsefiles\Oracle_12.2.0.1_Enterprise_Edi
```
- 2135 

```
tion_Installation_WIN.rsp
```
- 2136 7. Once the wizard opens, you will be asked to configure security updates. If you do not possess a
- 2137 My Oracle Support account, leave the box unchecked and provide an **email**.

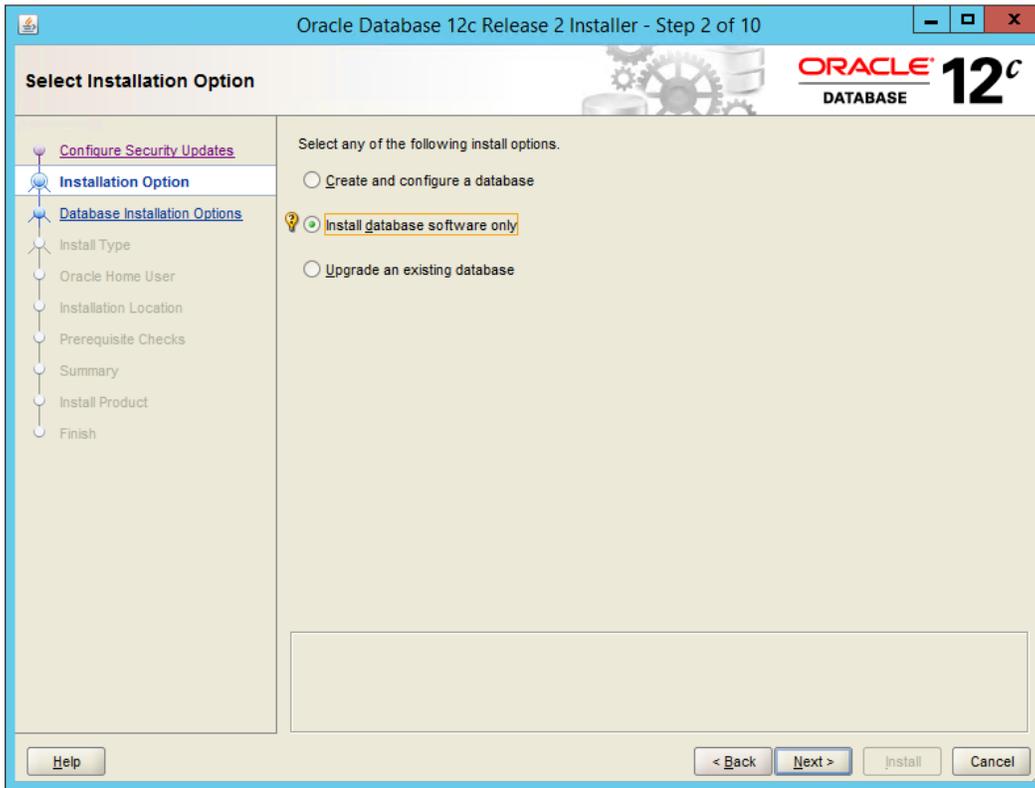


2138

2139

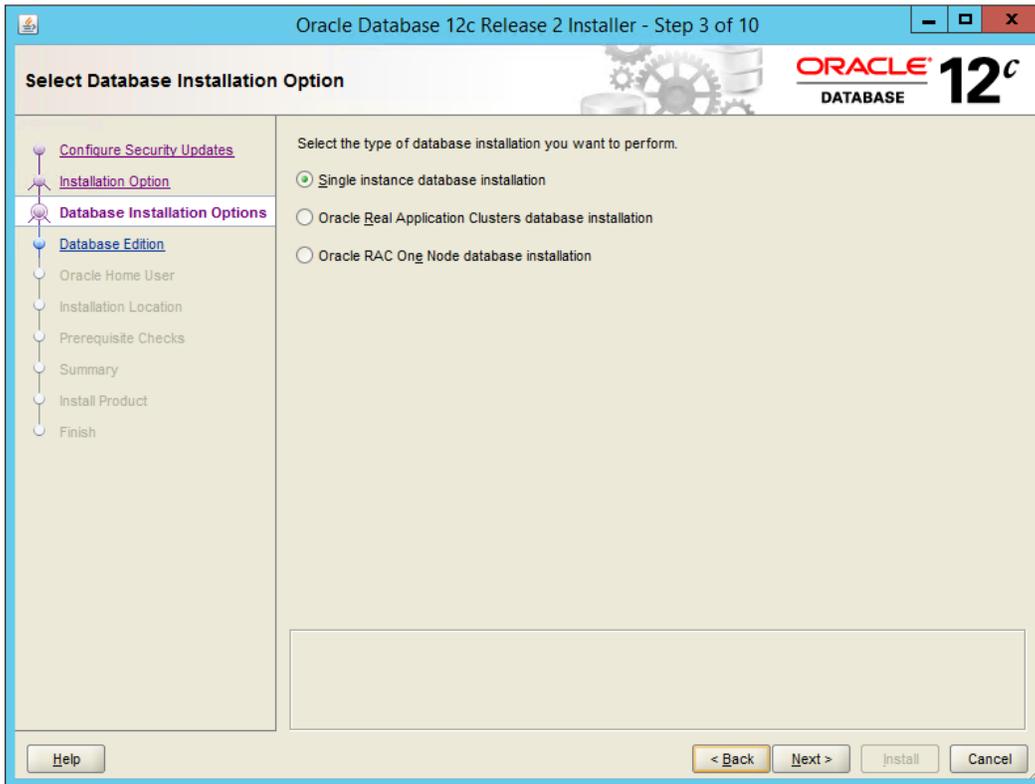
2140

8. Click **Next**.
9. Select **Install database software only**.



2141  
2142  
2143

10. Click **Next**.
11. Select **Single instance database installation**.



2144

2145

12. Click **Next**.

2146

13. Select **Standard Edition**.

2147

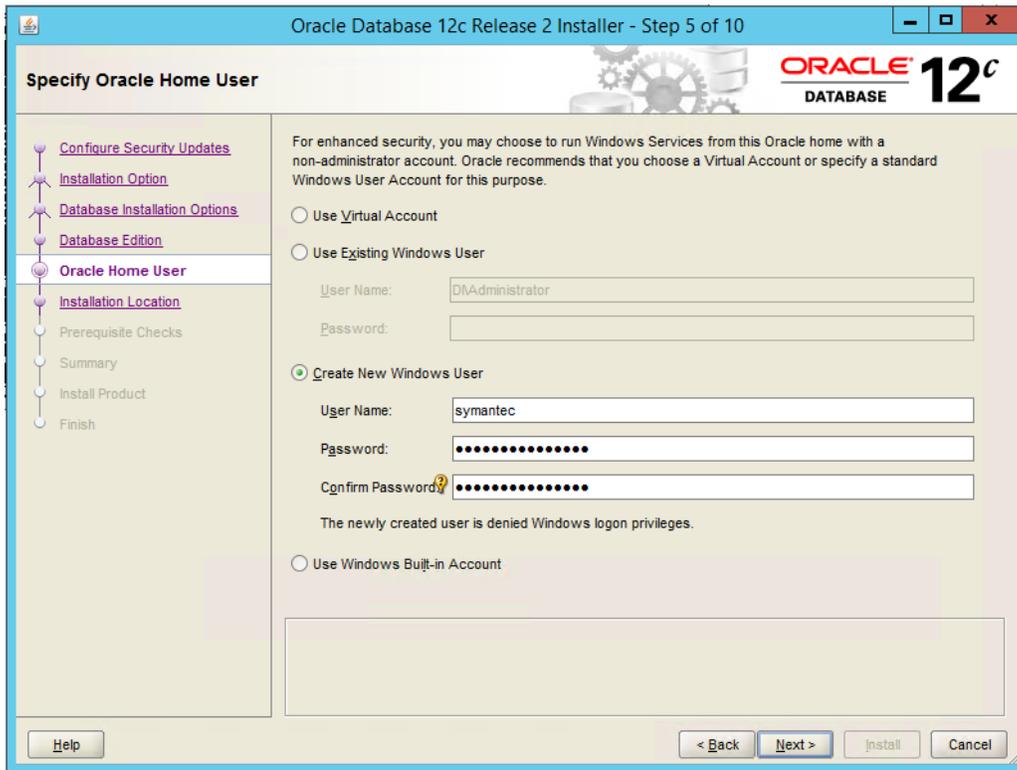
14. Click **Next**.

2148

15. Select **Create New Windows User**.

2149

16. Enter the **username** and **password** of a new user for Active Directory.



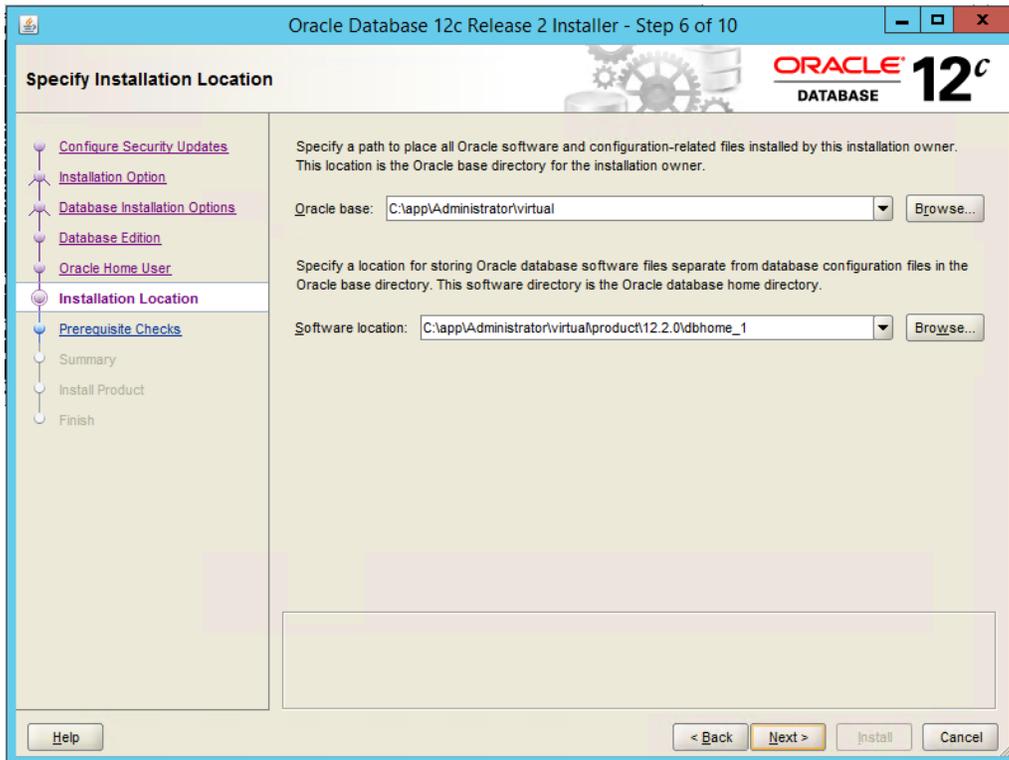
2150

2151

2152

17. Click **Next**.

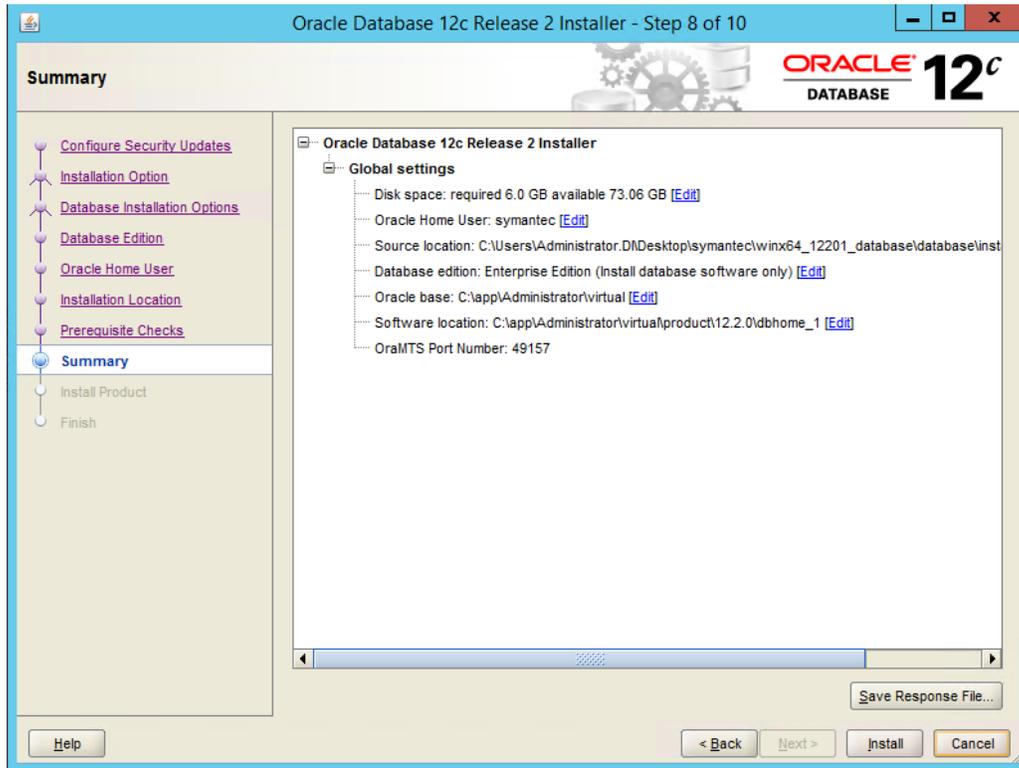
18. Select a location to install the software, if desired.



2153

2154

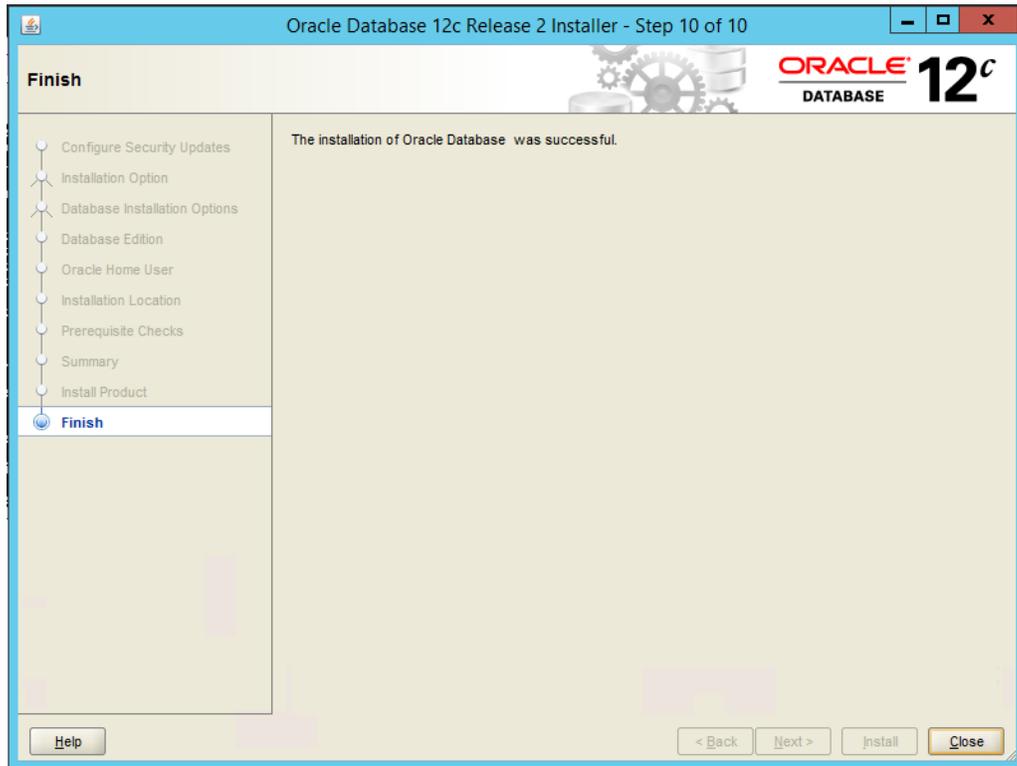
19. Click **Next**.



2155

2156

20. Verify the information and click **Install**. The installation may take a long time.



2157

2158 21. Click **Close** when the installation is complete.2159 **2.15.2 Create an Oracle Database for Symantec DLP**2160 1. Set the ORACLE\_HOME environment variable by running the following command. Adjust the  
2161 path accordingly if using a version other than 12.2.0.

2162 &gt; set

2163 ORACLE\_HOME=C:\app\Administrator\virtual\product\12.2.0\dbhome\_1

2164 2. Copy the Oracle database template named **Oracle\_12.2.0.1\_Template\_for\_64\_bit\_WIN.dbt**  
2165 from the Symantec DLP zip file into2166 **C:\app\Administrator\virtual\product\12.2.0\dbhome\_1\assistants\dbca\templates.**2167 3. Ensure that the response file **Oracle\_12.2.0.1\_DBCA\_WIN.rsp** is located in the folder  
2168 **C:\temp\Oracle\database\tools\responsefiles.**

2169 4. Run the following command.

2170 > %ORACLE\_HOME%\bin\dbca -createDatabase -progressOnly -  
2171 responseFile

2172 C:\temp\Oracle\database\tools\responsefiles\Oracle\_12.2.0.1\_DBCA\_  
 2173 WIN.rsp

- 2174 5. Enter a **password** for the **SYS** user. (Only the special characters **\_**, **#**, or **\$** are allowed.)
- 2175 6. Enter a **password** for the **SYSTEM** user. (Only the special characters **\_**, **#**, or **\$** are allowed.)
- 2176 7. Enter a **password** for the **Oracle Home User**.

### 2177 2.15.3 Configuring the Oracle Listener

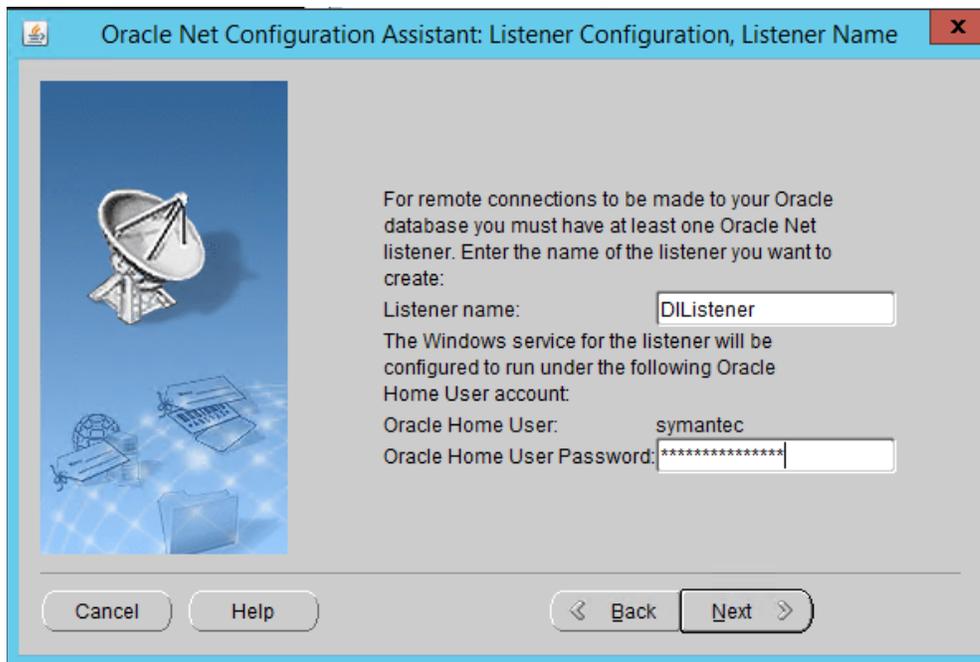
- 2178 1. Ensure that the database services OracleServicePROTECT and  
 2179 DistributedTransactionCoordinator are running.
- 2180 2. In the file **%ORACLE\_HOME%\network\admin\sqlnet.ora**, change the line  
 2181 SQLNET.AUTHENTICATION\_SERVICES=(NTS) to SQLNET.AUTHENTICATION\_SERVICES=(none).
- 2182 3. Navigate to **Start > All Programs > Oracle 12.2.0 > Configuration and Migration Tools > Net  
 2183 Configuration Assistant** and run the program.
- 2184 4. Select **Listener configuration**.



- 2185
- 2186 5. Click **Next**.
- 2187 6. Select **Add**.



- 2188
  - 2189
  - 2190
  - 2191
7. Click **Next**.
  8. Enter a **name** for the listener.
  9. Enter a **password**.



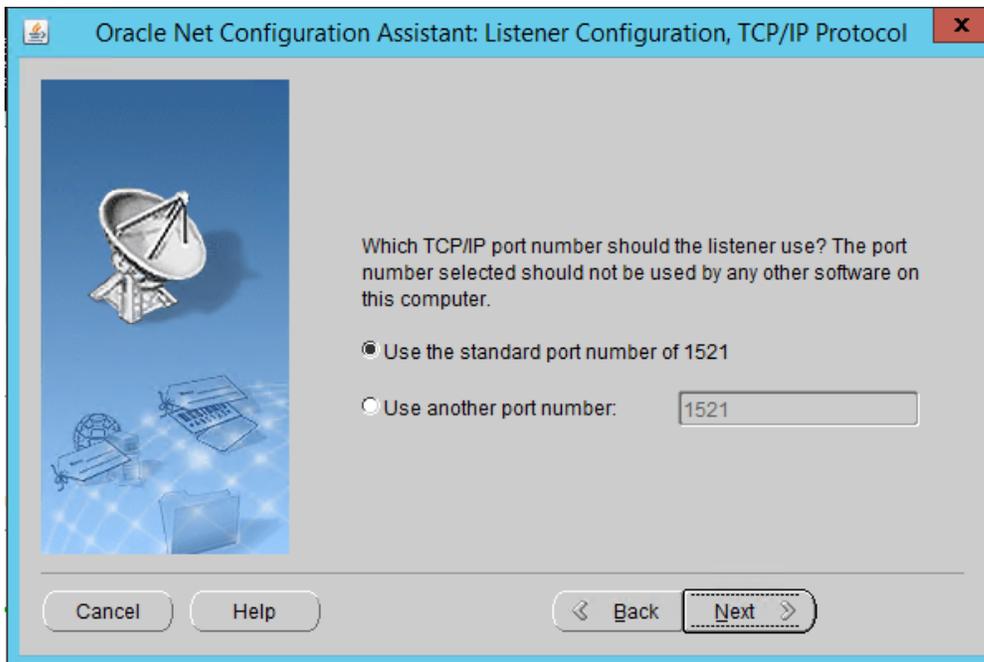
- 2192
  - 2193
10. Click **Next**.

2194 11. Move the **TCP** protocol to the **Selected Protocols** column.



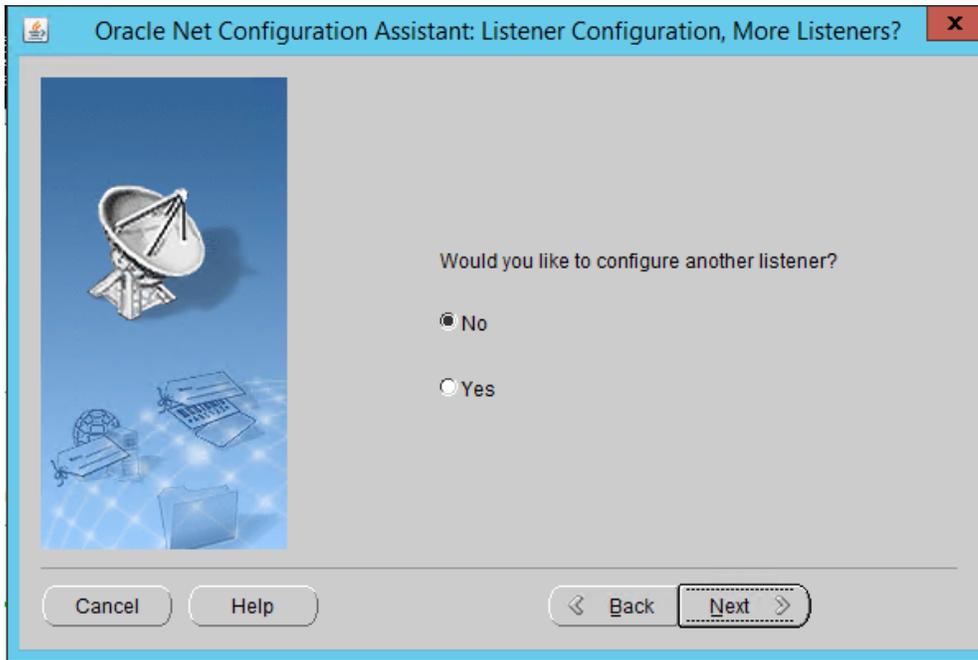
2195  
2196 12. Click **Next**.

2197 13. Select **Use the standard port number of 1521**.



2198  
2199 14. Click **Next**.

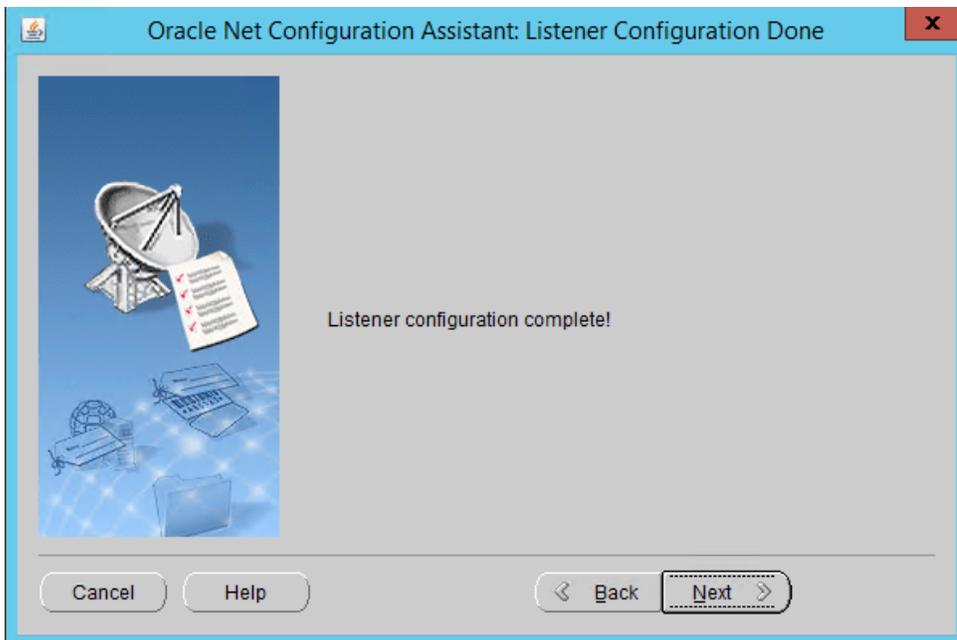
2200 15. Select **No**.



2201

2202

16. Click **Next**.



2203

2204

2205

17. Click **Next**.

18. Select **Local Net Service Name configuration**.



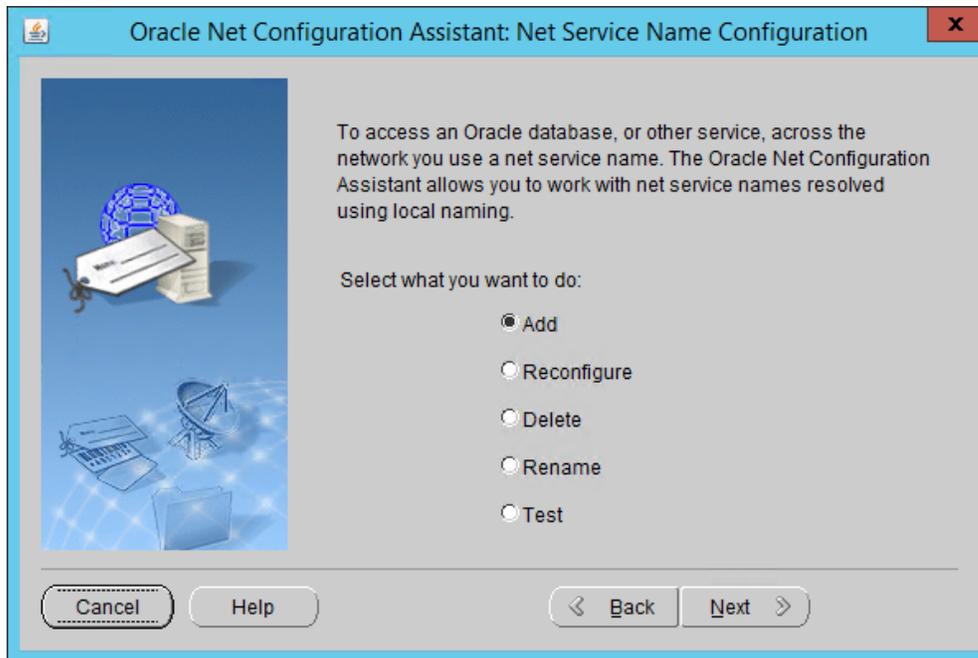
2206

2207

2208

19. Click **Next**.

20. Select **Add**.



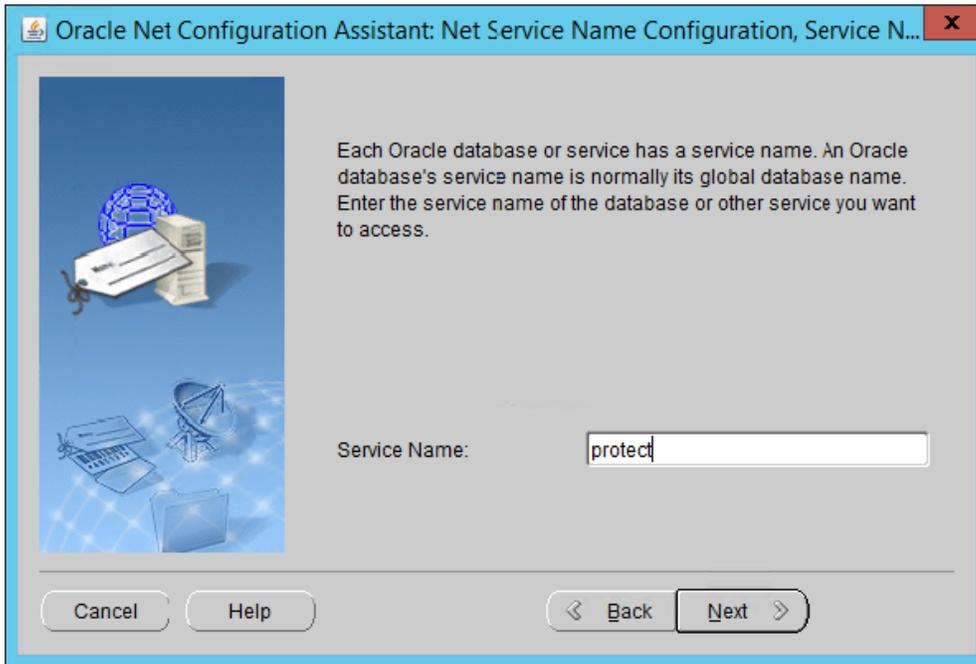
2209

2210

2211

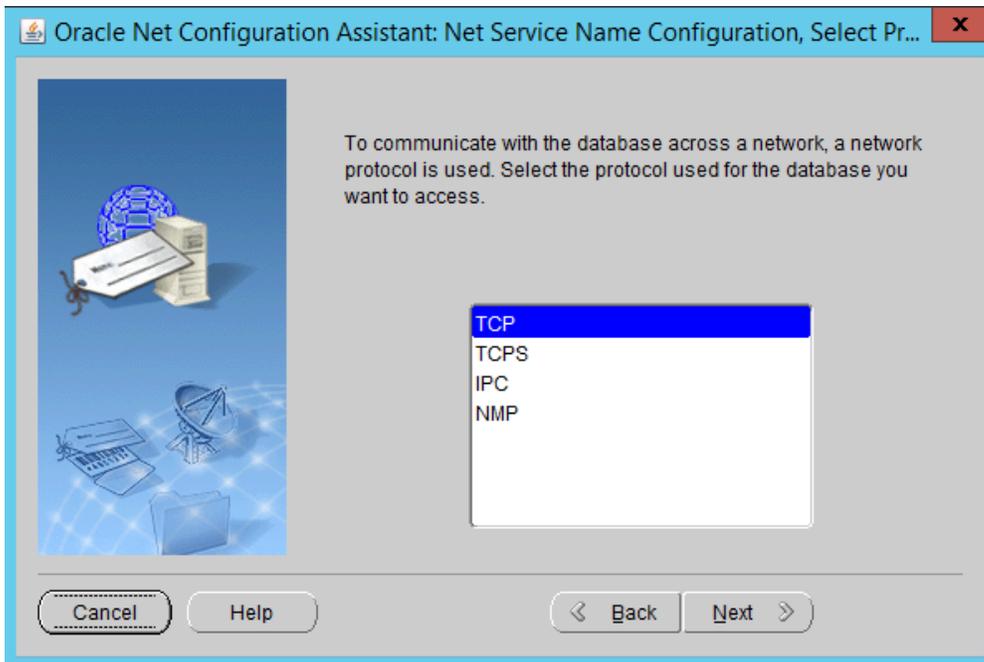
21. Click **Next**.

22. Enter the word "protect" for the **name**.



2212  
2213  
2214

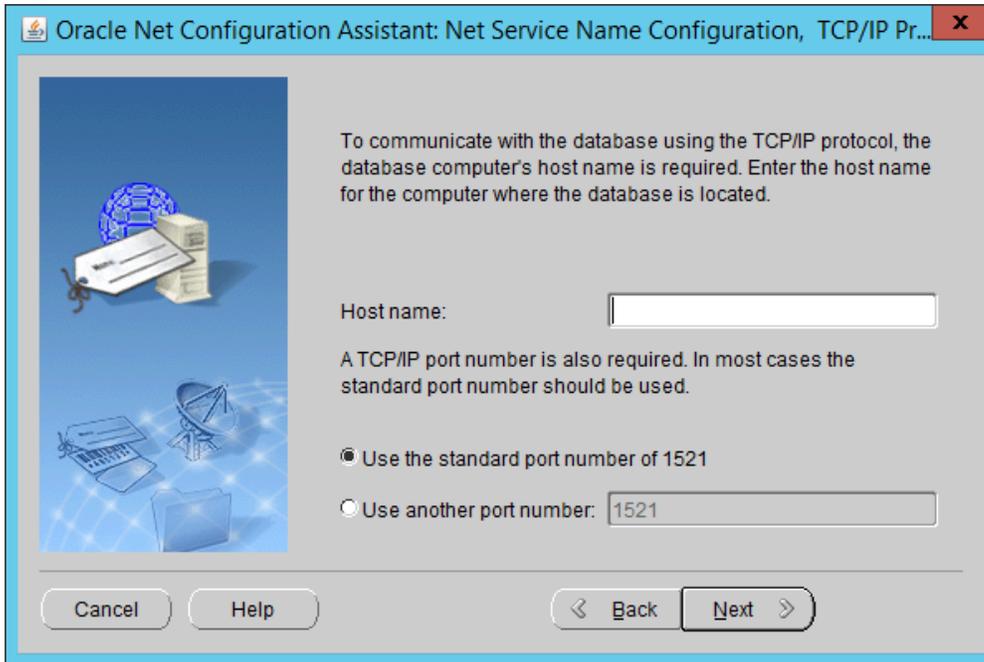
- 23. Click **Next**.
- 24. Select **TCP**.



2215  
2216  
2217

- 25. Click **Next**.
- 26. Enter the **IP address** of the system hosting the Oracle Database.

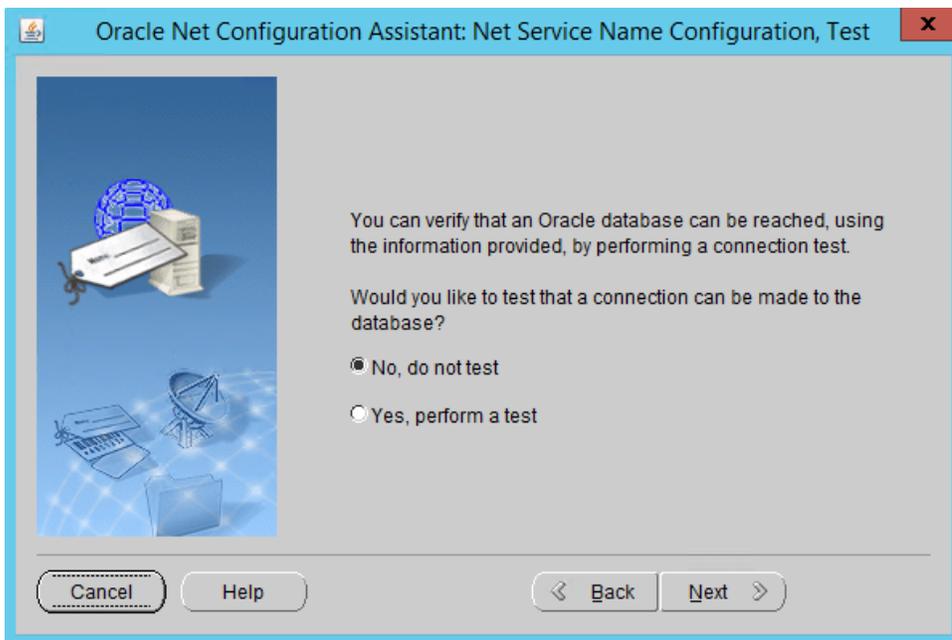
2218 27. Select **Use the standard port number of 1521**.



2219

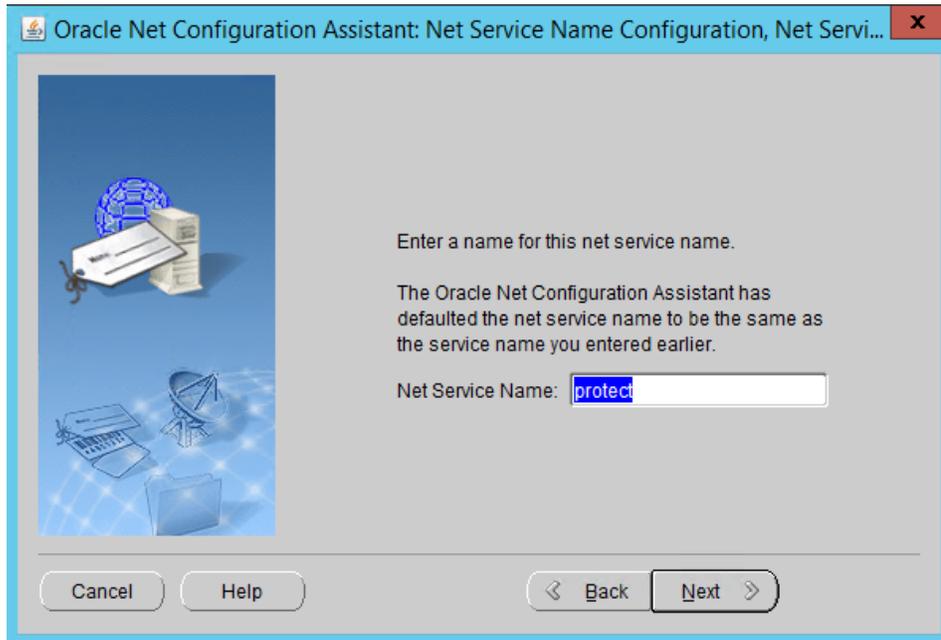
2220 28. Click **Next**.

2221 29. Select **No, do not test**.



2222

2223 30. Click **Next**.



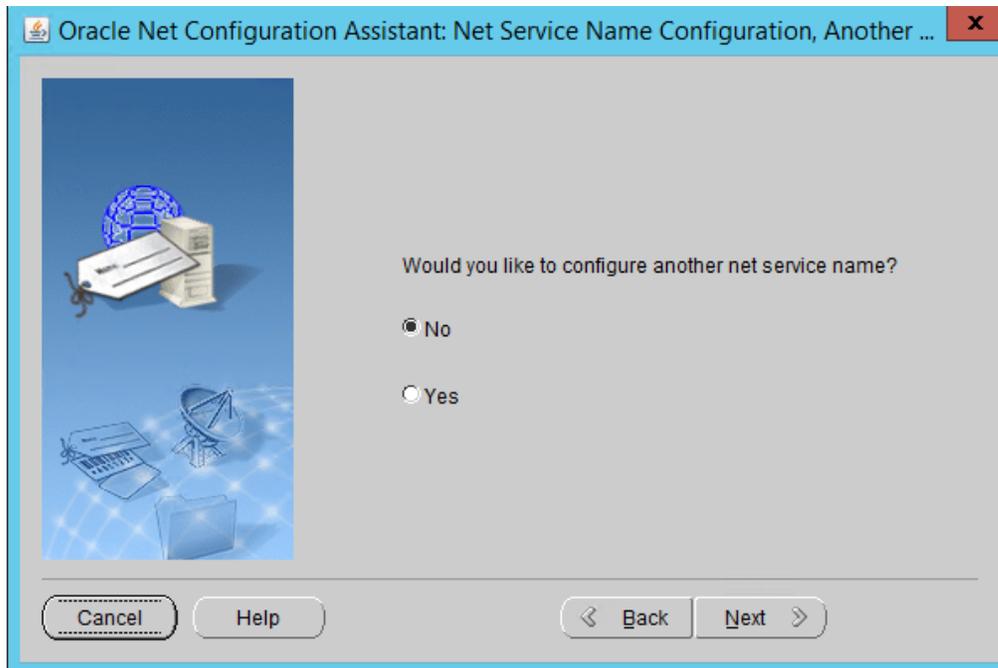
2224

2225

2226

31. Click **Next**.

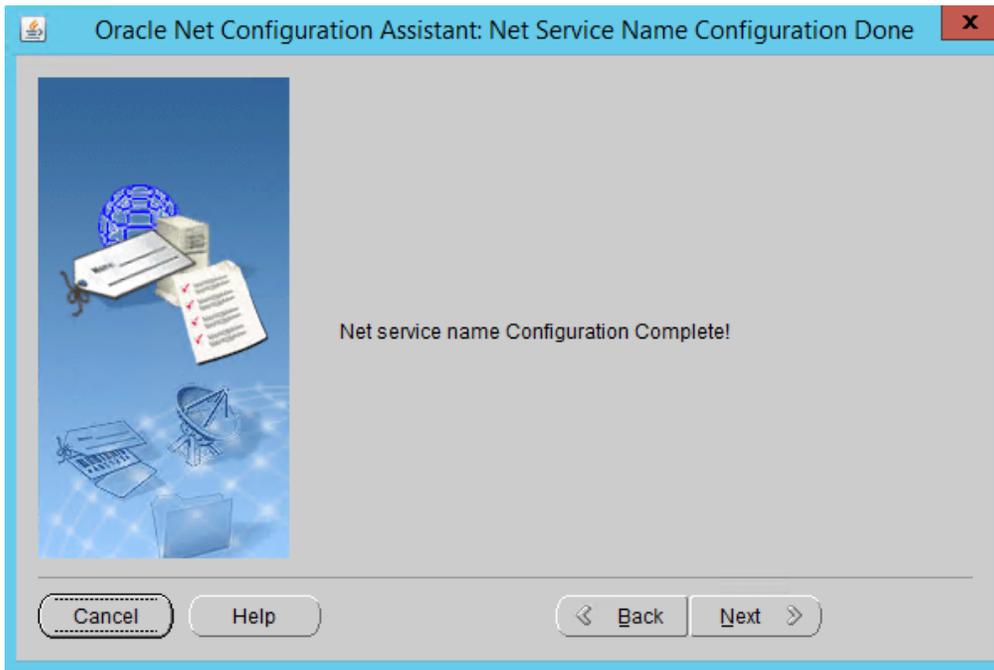
32. Select **No**.



2227

2228

33. Click **Next**.



2229  
2230

34. Click **Next**.



2231  
2232  
2233

35. Click **Finish**.

36. In an administrative command prompt, run the following command to stop the listener.

2234 > lsnrctl stop

2235 37. Open the file **%ORACLE\_HOME%\network\admin\listener.ora**.

2236 38. Change (ADDRESS = (PROTOCOL = IPC)(KEY = <key\_value>)) to (ADDRESS = (PROTOCOL =  
2237 IPC)(KEY = PROTECT)).

2238 39. Add the line **SECURE\_REGISTER\_LISTENER=(IPC)** to the end of the file.

```
listener - Notepad
# listener.ora Network Configuration File: C:\app\Administrator\virtual\product\12.2.0\dbhome_1\network\admin\listener.ora
# Generated by Oracle configuration tools.

SID_LIST_DILISTENER =
(SID_LIST =
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\app\Administrator\virtual\product\12.2.0\dbhome_1)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\app\Administrator\virtual\product\12.2.0\dbhome_1\bin\oraclr12.dll")
)
(SID_DESC =
(SID_NAME = CLRExtProc)
(ORACLE_HOME = C:\app\Administrator\virtual\product\12.2.0\dbhome_1)
(PROGRAM = extproc)
(ENVS = "EXTPROC_DLLS=ONLY:C:\app\Administrator\virtual\product\12.2.0\dbhome_1\bin\oraclr12.dll")
)
)
DILISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = SYMANTEC-DLP.DE.IPDR)(PORT = 1521))
(ADDRESS = (PROTOCOL = IPC)(KEY = PROTECT))
)
)
SECURE_REGISTER_LISTENER = (IPC) |
```

2239

2240 40. Save the file and exit the editor.

2241 41. Ensure that OracleServicePROTECT and OracleVssWriterPROTECT services are running in Task  
2242 Manager.

2243 42. In an administrative command prompt, run the following command to start the listener. Re-  
2244 place dilistener with the name given to your listener.

2245 > lsnrctl start dilistener

2246 43. Run the following commands to connect the listener to the database using SQL Plus. Replace  
2247 password with the password used for the SYS user.

2248 > sqlplus /nolog

2249 > conn sys/password as sysdba

2250 44. Run the following commands in the SQL prompt. (Note: If errors occur relating to the SPFILE, try  
2251 replacing ORACLE\_HOME or ORACLE\_base values in %ORACLE\_HOME%\dbs\init.ora with the

2252 absolute path. Then run CREATE SPFILE FROM PFILE='%ORACLE\_HOME%\dbs\init.ora' and CRE-  
 2253 ATE PFILE FROM SPFILE='%ORACLE\_HOME%\dbs\init.ora'. Restart the database after doing  
 2254 this.)

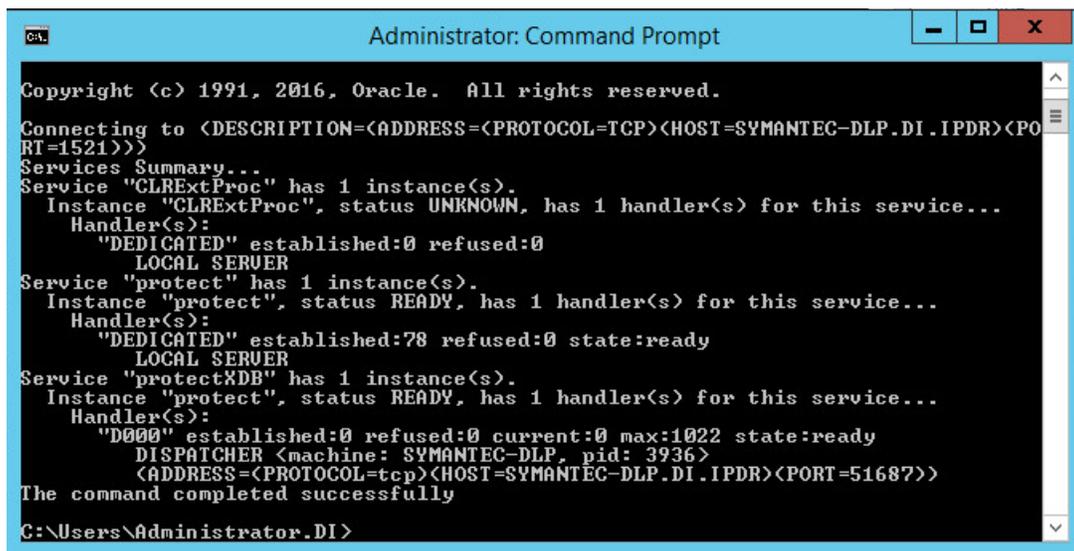
2255 > ALTER SYSTEM SET local\_listener = '(DESCRIPTION=(ADDRESS=(PRO-  
 2256 TOCOL=ipc)(KEY=PROTECT)))' SCOPE=both;

2257 > ALTER SYSTEM REGISTER;

2258 > exit

2259 45. Run the following command to verify the status of the listeners:

2260 > lsnrctl services



```

Administrator: Command Prompt
Copyright (c) 1991, 2016, Oracle. All rights reserved.
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=SYMANTEC-DLP.DI.IPDR)(PORT=1521)))
Services Summary...
Service "CLRExtProc" has 1 instance(s).
  Instance "CLRExtProc", status UNKNOWN, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:0 refused:0
      LOCAL SERVER
Service "protect" has 1 instance(s).
  Instance "protect", status READY, has 1 handler(s) for this service...
    Handler(s):
      "DEDICATED" established:78 refused:0 state:ready
      LOCAL SERVER
Service "protectXDB" has 1 instance(s).
  Instance "protect", status READY, has 1 handler(s) for this service...
    Handler(s):
      "D000" established:0 refused:0 current:0 max:1022 state:ready
      DISPATCHER <machine: SYMANTEC-DLP, pid: 3936>
      (ADDRESS=(PROTOCOL=tcp)(HOST=SYMANTEC-DLP.DI.IPDR)(PORT=51687))
The command completed successfully
C:\Users\Administrator.DI>
  
```

2261

2262 46. Open a new administrative command window.

2263 47. Navigate to C:\Temp\Oracle\database\tools.

2264 48. Run the following command:

2265 > sqlplus /nolog

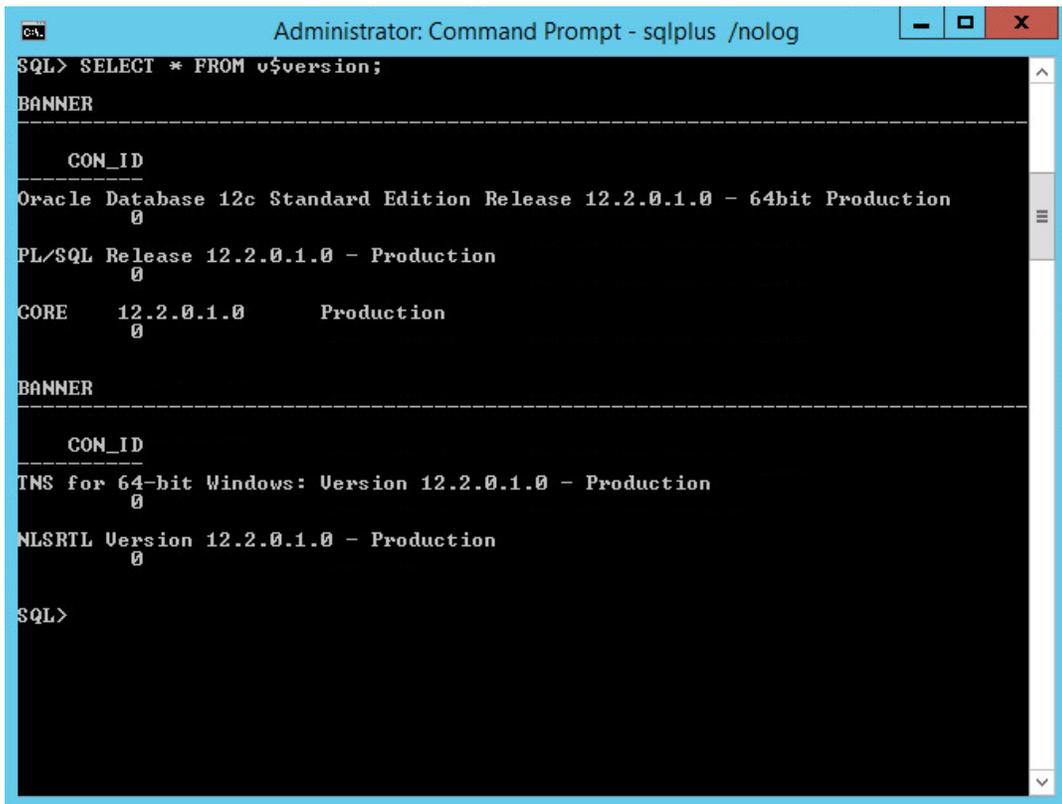
2266 > @oracle\_create\_user.sql

2267 49. Enter the **password** for the **SYS** user.

2268 50. For **sid**, enter "protect".

2269 51. For a **username**, enter "protect".

- 2270 52. Enter a **password** for the “protect” user. (The special characters &, \$, and # are not allowed.)
- 2271 53. When this process is finished, open a new administrative command window and run the follow-
- 2272 ing command.
- 2273 > sqlplus /nolog
- 2274 54. Log in as the **SYS** user with the following command (replace “password” with the password for
- 2275 the **SYS** user).
- 2276 > connect sys/password@protect as sysda
- 2277 55. Verify the version information with the following command.
- 2278 > SELECT \* FROM v\$version;

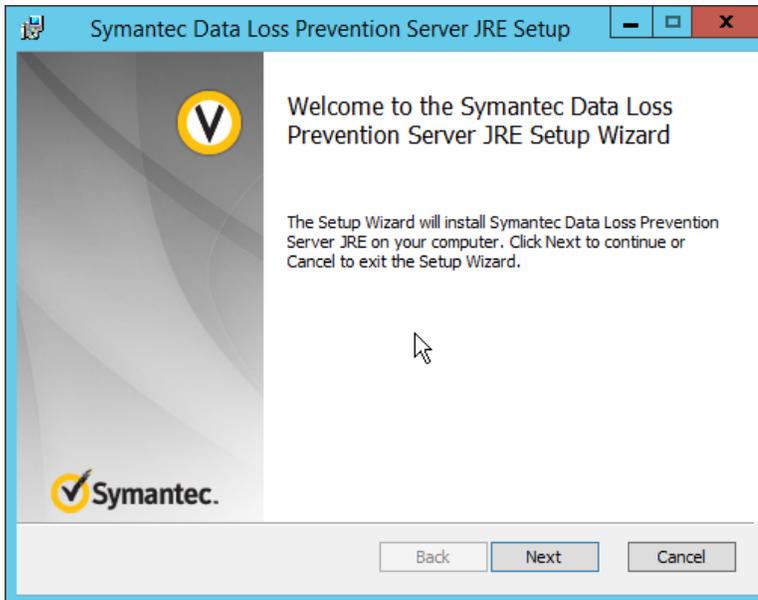


```
Administrator: Command Prompt - sqlplus /nolog
SQL> SELECT * FROM v$version;
BANNER
-----
      CON_ID
Oracle Database 12c Standard Edition Release 12.2.0.1.0 - 64bit Production
      0
PL/SQL Release 12.2.0.1.0 - Production
      0
CORE      12.2.0.1.0      Production
      0
BANNER
-----
      CON_ID
TNS for 64-bit Windows: Version 12.2.0.1.0 - Production
      0
NLSRTL Version 12.2.0.1.0 - Production
      0
SQL>
```

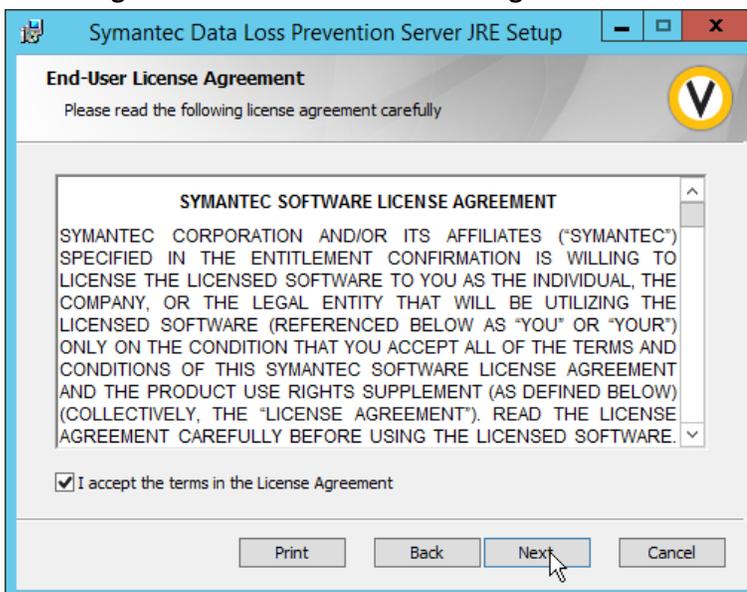
2279

2280 **2.15.4 Install Symantec DLP**

- 2281 1. In the folder **DLP Installs\DLP 15.1\Symantec\_DLP\_15.1\_Platform\_Win-**  
2282 **IN\_15.1.0.25021\DLP\15.1\New\_Installs\x64\Release**, located in the download folder for the  
2283 DLP files, run **ServerJRE.msi**.

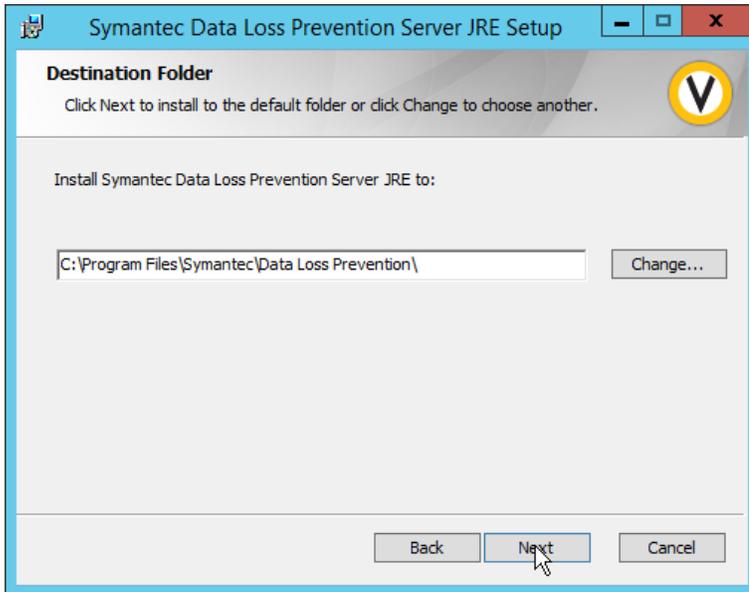


- 2284  
2285 2. Click **Next**.  
2286 3. Select **I agree to the terms in the license agreement**.

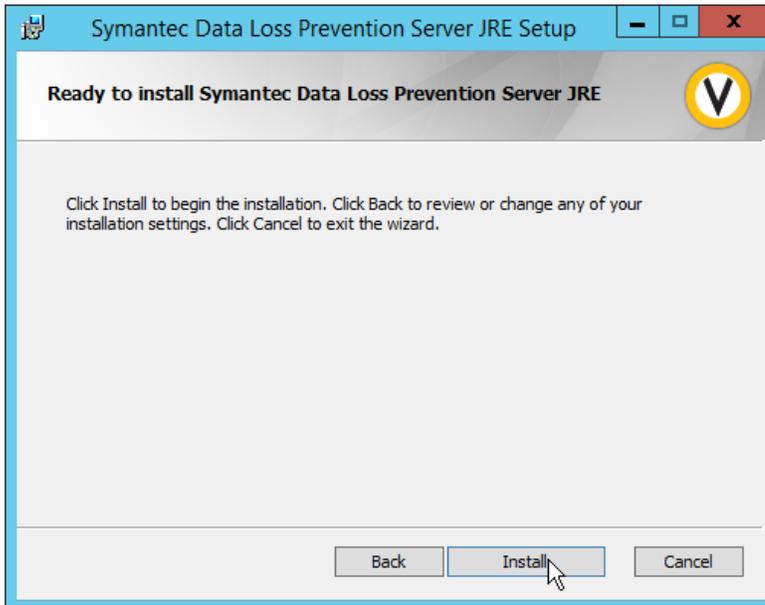


2287

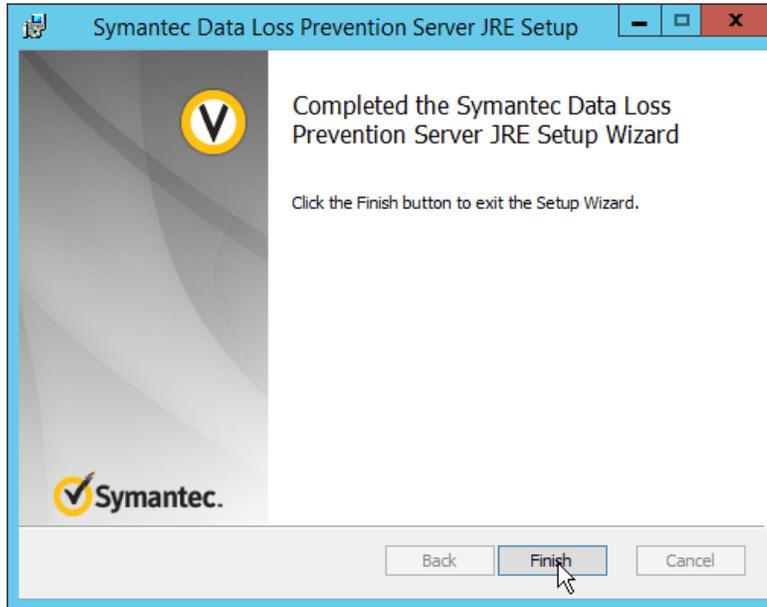
- 2288 4. Click **Next**.



- 2289 5. Click **Next**.



- 2291 6. Click **Install**.

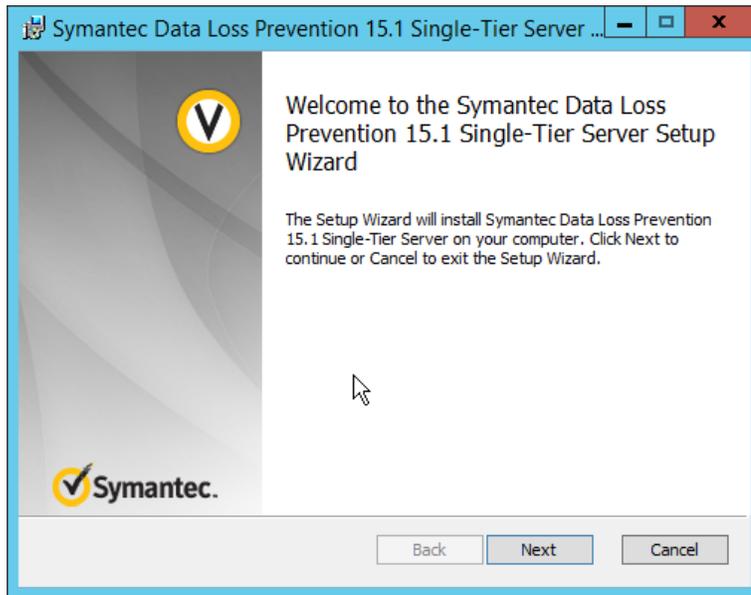


2293

2294

2295

7. Click **Finish**.
8. Run **SingleTierServer.msi** (located in the same folder as **ServerJRE.msi**).

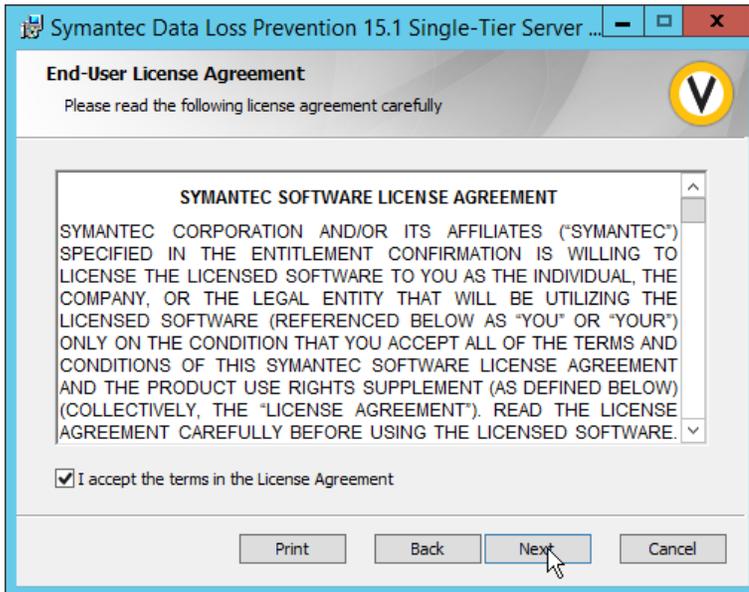


2296

2297

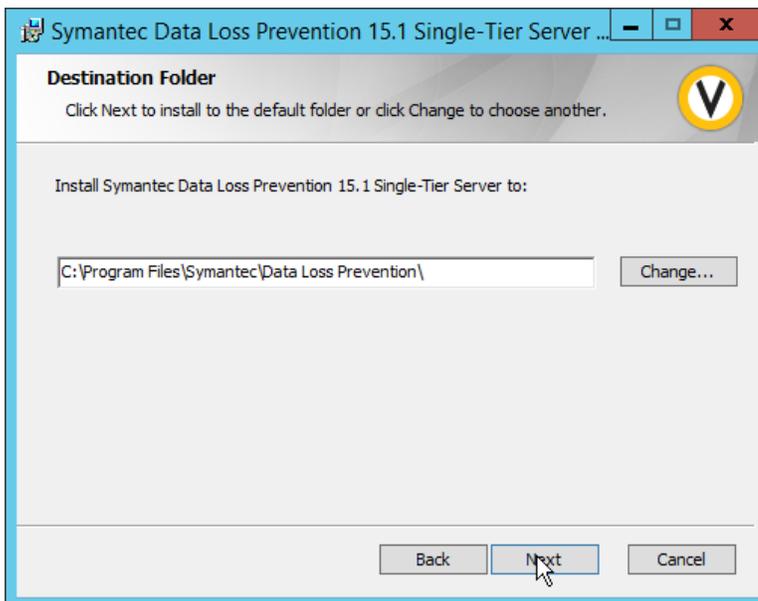
2298

9. Click **Next**.
10. Check the box to accept the license agreement.



2299  
2300

11. Click **Next**.



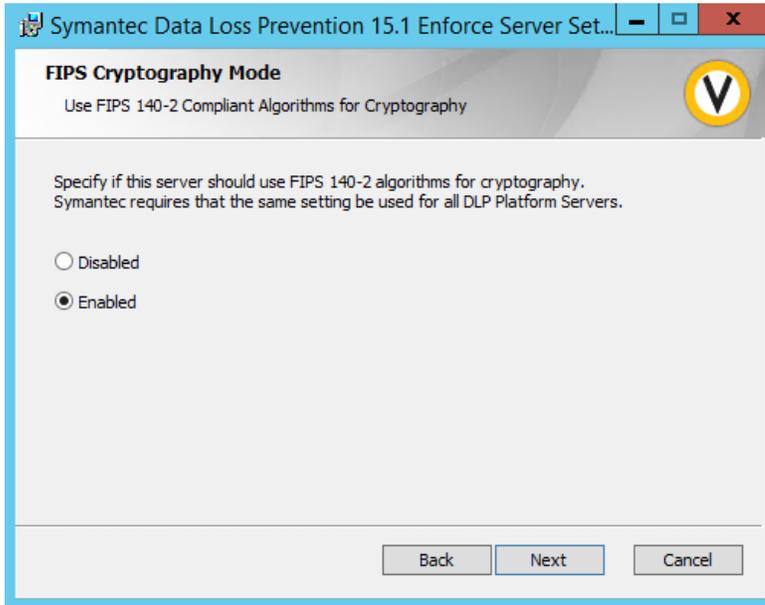
2301

2302

2303

12. Click **Next**.

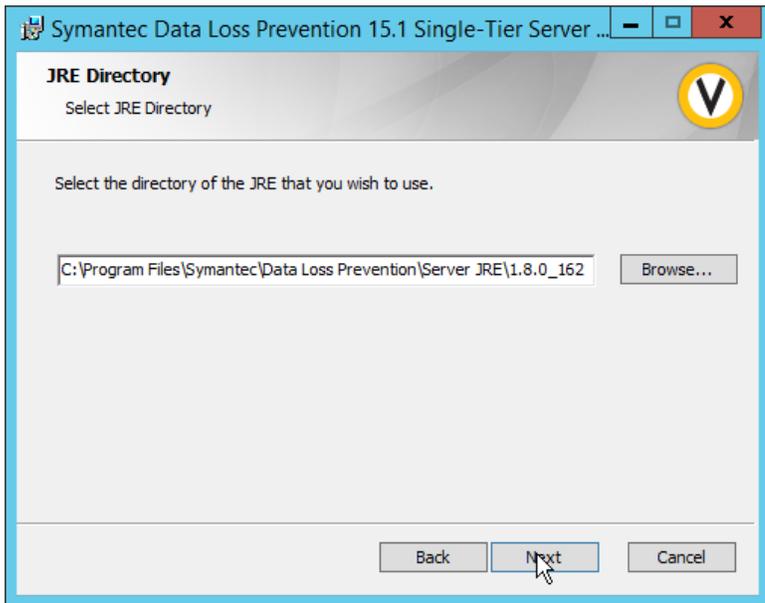
13. Select **Enabled** for **FIPS 140-2 Compliant Algorithms**.



2304

2305

14. Click **Next**.



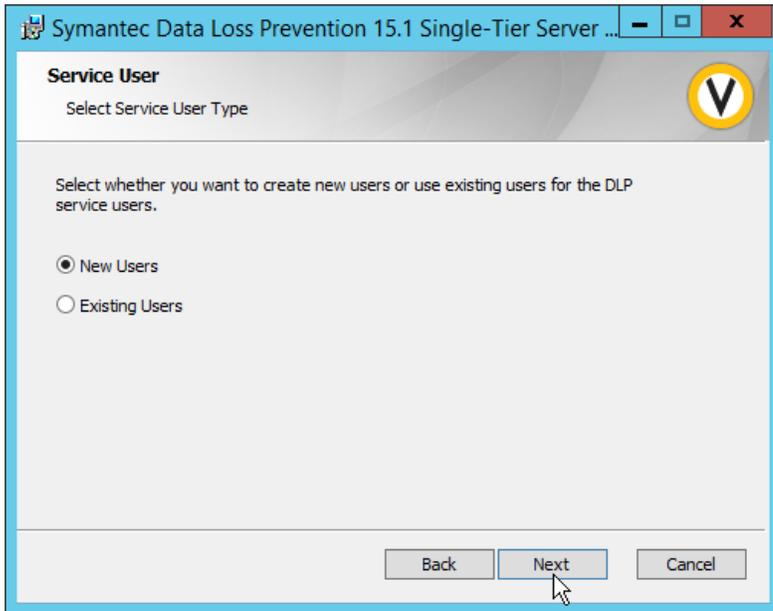
2306

2307

2308

15. Click **Next**.

16. Click on **New Users**.



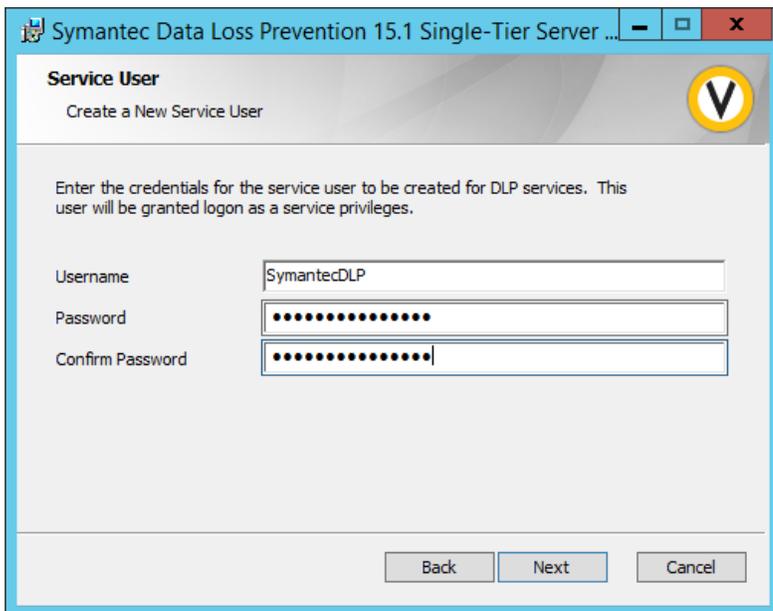
2309

2310

2311

17. Click **Next**.

18. Enter a **password** and optionally a **username**.



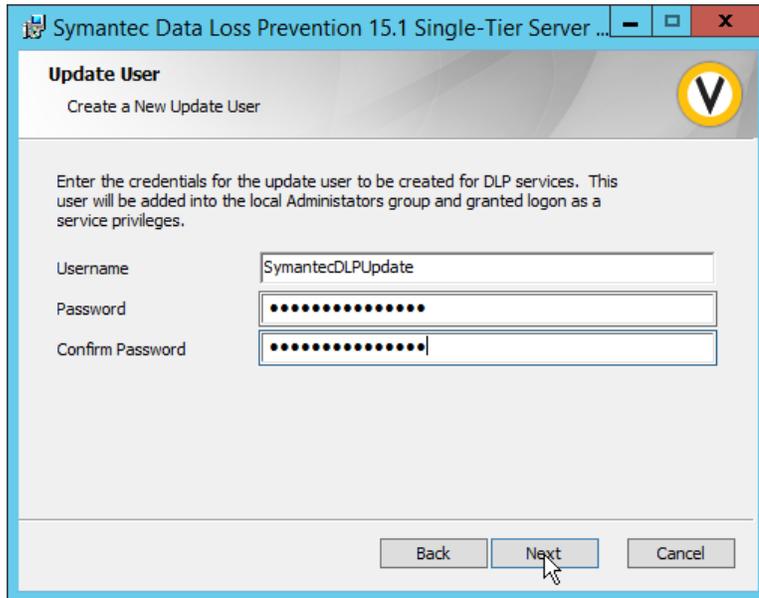
2312

2313

2314

19. Click **Next**.

20. Enter a **password** and optionally a **username**.



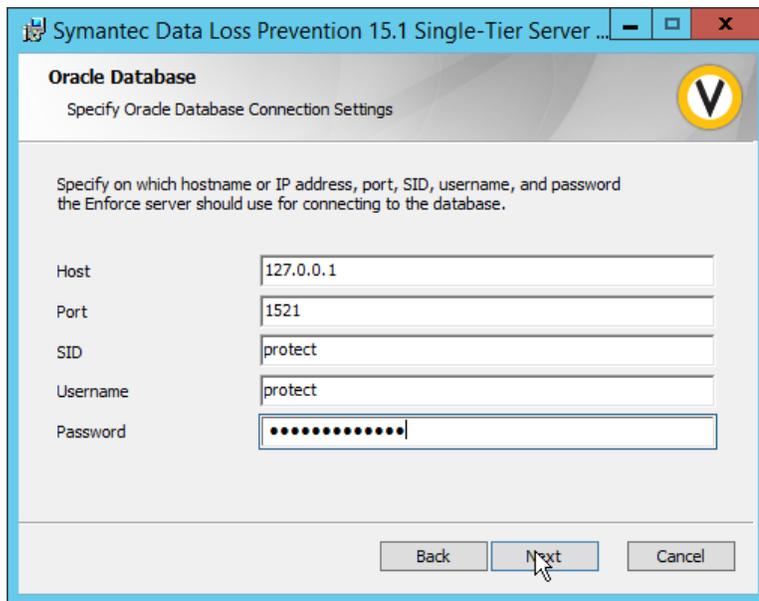
2315

2316

2317

21. Click **Next**.

22. Enter the **password** used for the “protect” user.



2318

2319

2320

2321

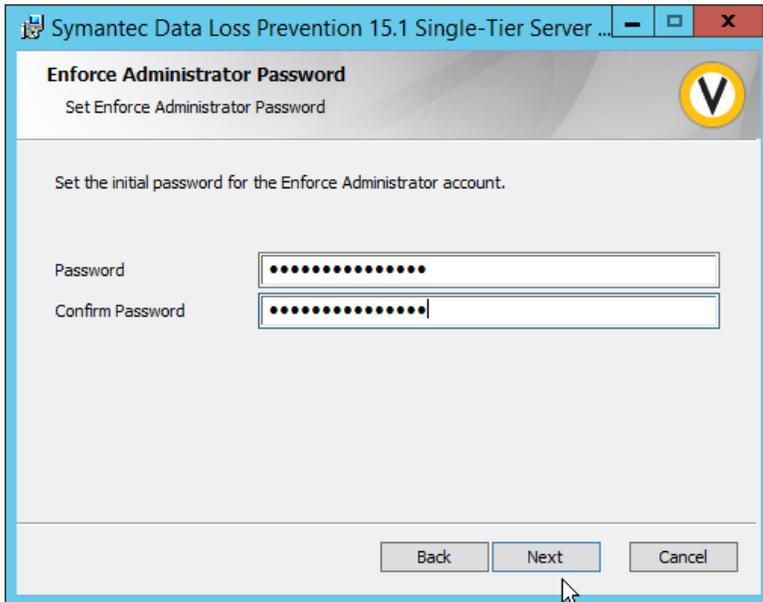
2322

23. Click **Next**.

24. Select **Initialize Database**.

25. Click **Next**.

26. Set the initial **password** for logging into the Enforce Administrator account.



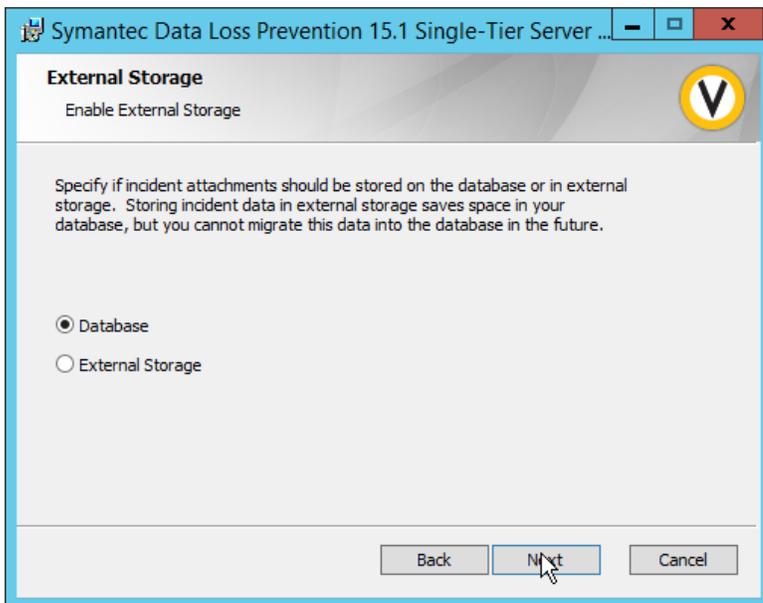
2323

2324

2325

27. Click **Next**.

28. Select **Database**.



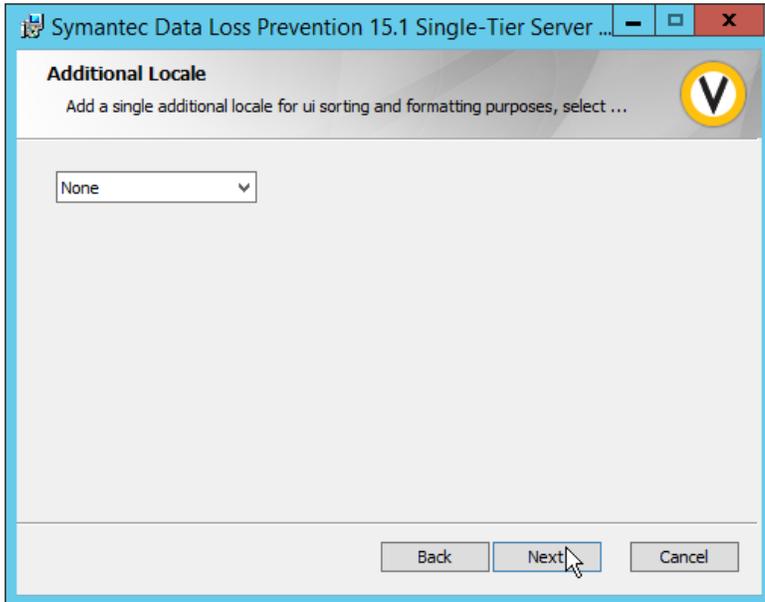
2326

2327

2328

29. Click **Next**.

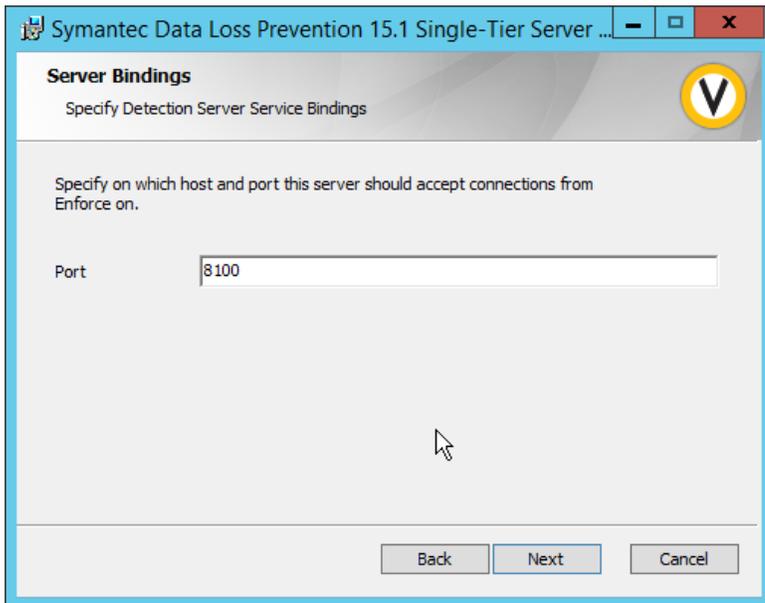
30. Select **None**.



2329

2330

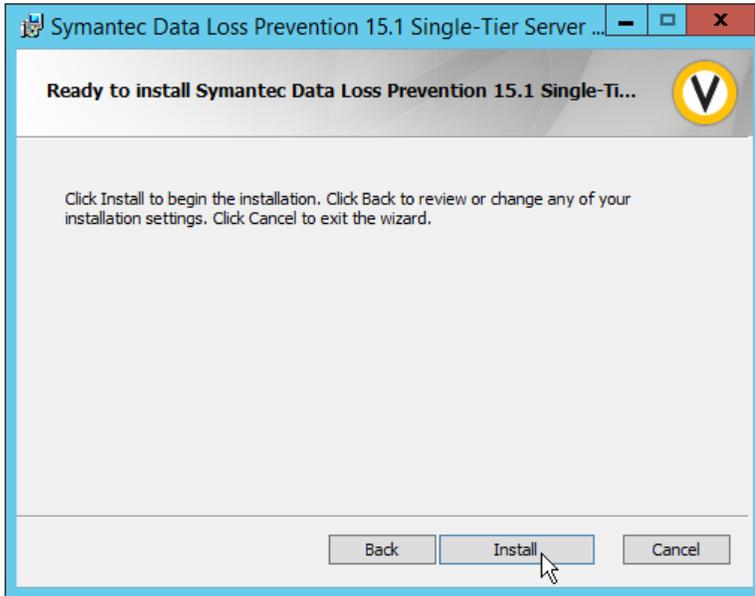
31. Click **Next**.



2331

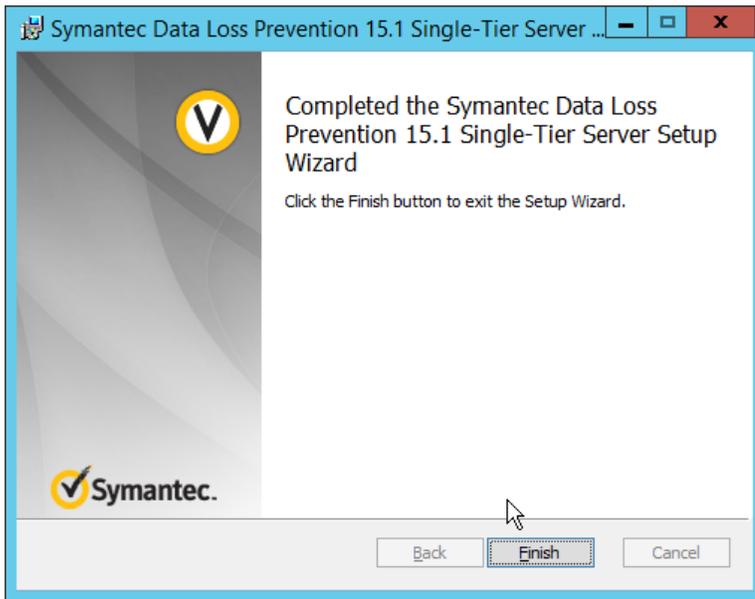
2332

32. Click **Next**.



2333

2334 33. Click **Install**.



2335

2336 34. Click **Finish**.

2337 35. Ensure that the services are running in Task Manager:

- 2338 a. SymantecDLPManager
- 2339 b. SymantecDLPIncidentPersister
- 2340 c. SymantecDLPNotifier

2341 d. SymantecDLPDetectionServer

## 2342 2.15.5 Configure Symantec DLP

- 2343 1. Navigate to `https://127.0.0.1` in the browser to get to the Symantec DLP web console.
- 2344 2. Navigate to **System > Settings > General** and click **Configure**.
- 2345 3. In the **Edit General Settings** screen, upload your license file provided by Symantec.
- 2346 4. Click **Save**.
- 2347 5. In Task Manager, stop the **SymantecDLPManager** service.
- 2348 6. Copy the `classpath.txt` file located in `<DLP Download Home>\DLP\15.1\Solution_Packs\` and
- 2349 overwrite the `classpath.txt` located at `C:\Program Files\Symantec\Data Loss`
- 2350 **Prevention\Enforce Server\15.1\Protect\Config\SolutionPackInstaller**.
- 2351 7. In an administrative command window, use the following commands to import the chosen
- 2352 solution pack. For example, to import the financial solution pack, use:
- 2353 

```
> cd "C:\Program Files\Symantec\Data Loss Prevention\Enforce
```
- 2354 

```
Server\15.1\protect\bin"
```
- 2355 

```
> .\SolutionPackInstaller.exe import "C:\Program
```
- 2356 

```
Files\Symantec\Data Loss Prevention\Financial_v15.1.vsp"
```
- 2357 8. After this is installed, restart the **SymantecDLPManager** service.
- 2358 9. Log on to the Enforce Web Console as Administrator.
- 2359 10. Navigate to **System > Servers > Overview**.
- 2360 11. Click **Add Server**.
- 2361 12. Select the type of Detection Server to add.
- 2362 13. Click **Next**.
- 2363 14. Enter a **name**.
- 2364 15. Enter the **hostname** of the DLP server.
- 2365 16. Enter **8100** for the **port**.
- 2366 17. Navigate to **System > Settings > General**.

### Process Control

Advanced Process Control



2367

- 2368 18. Check the box next to **Advanced Process Control**.
- 2369 19. Specify any configuration options according to the needs of your organization.
- 2370 20. Click **Save**.

## 2371 2.16 Cisco Identity Services Engine

2372 This section details the installation and some configurations for the Cisco Identity Services Engine (ISE).  
2373 It assumes the use of the ISE virtual machine.

### 2374 2.16.1 Initial Setup

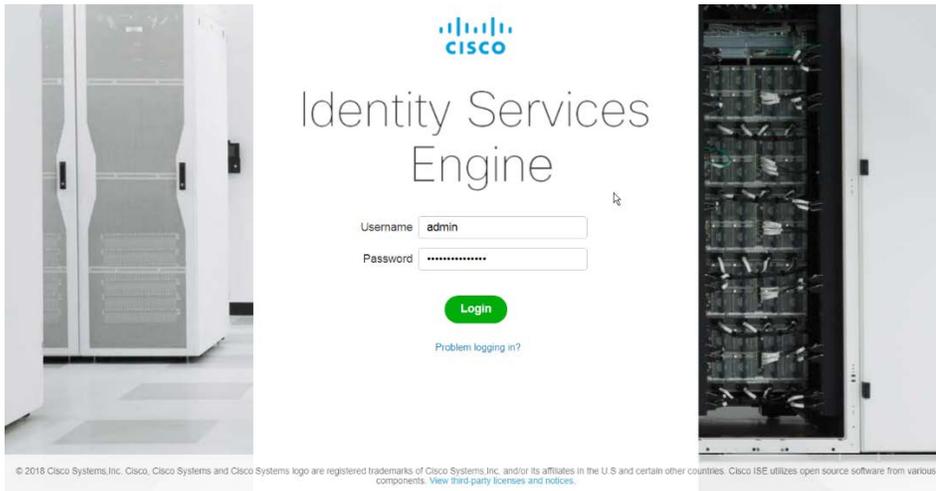
- 2375 1. When prompted to log in for the first time, enter `setup`. (You can use the command `reset-`  
2376 `config` to change these values later.)
- 2377 2. Enter the desired **hostname** for the machine.
- 2378 3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname is associated  
2379 with this IP address in your DNS.)
- 2380 4. Enter the **netmask** for the machine.
- 2381 5. Enter the **default gateway**.
- 2382 6. Enter the **default DNS domain** (the name of your domain).
- 2383 7. Enter the **primary nameserver** (the IP address of your DNS).
- 2384 8. Enter a second nameserver if desired.
- 2385 9. Enter a **Network Time Protocol (NTP) time server**.
- 2386 10. Enter the **timezone**.
- 2387 11. Enter **Y** for **SSH service**.
- 2388 12. Enter an administrator **username** for the machine.
- 2389 13. Enter a **password** twice.

### 2390 2.16.2 Inventory: Configure SNMP on Routers/Network Devices

2391 See the corresponding vendor documentation for the correct way to enable Simple Network  
2392 Management Protocol (SNMP) on your network device. Ensure that the community string you choose is  
2393 considered sensitive, like a password.

### 2394 2.16.3 Inventory: Configure Device Detection

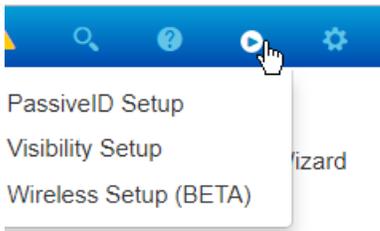
- 2395 1. Log in to the web client by visiting `https://hostname/admin` but replace **hostname** with the  
2396 hostname of the ISE machine.



2397

2398

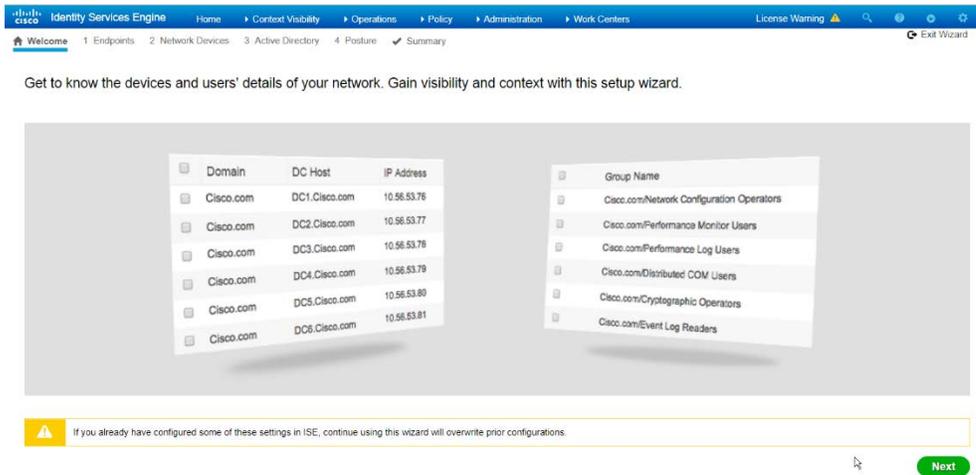
2. On the top right, use the small Play button to select **Visibility Setup**.



2399

2400

3. Click **Next**.

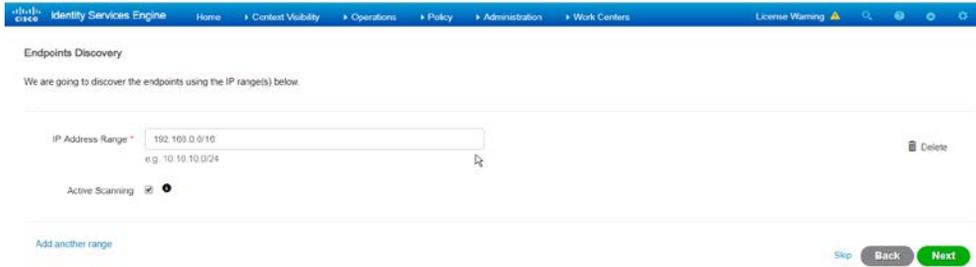


2401

2402

2403

4. Enter the range of IP addresses to add to ISE's inventory.
5. Ensure that **Active Scanning** is checked.



2404

2405

6. Click **Next**.

2406

7. Click the **Add Device Manually** link.

2407

8. Enter a **name**.

2408

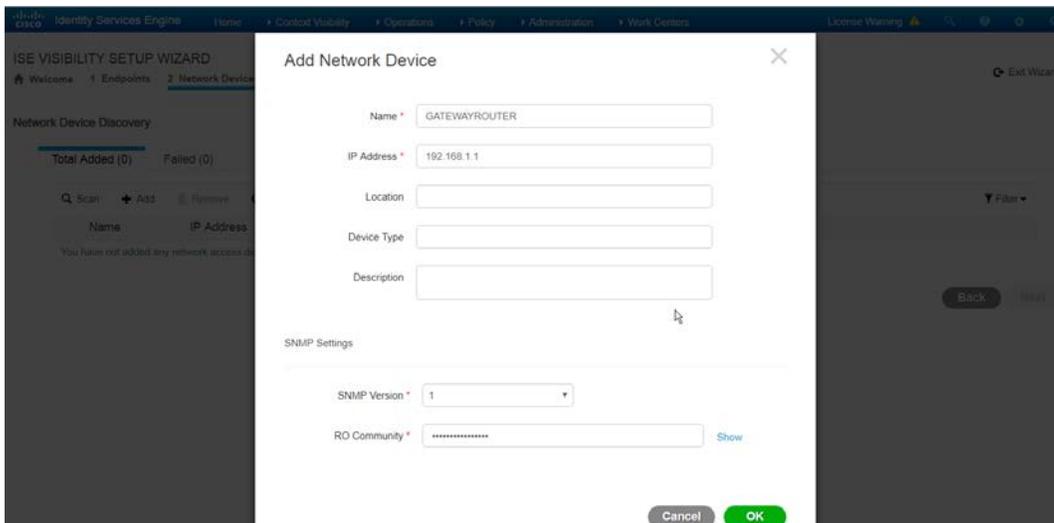
9. Enter the **IP address** of the network device you configured for SNMP.

2409

10. Select **1** for **SNMP version**.

2410

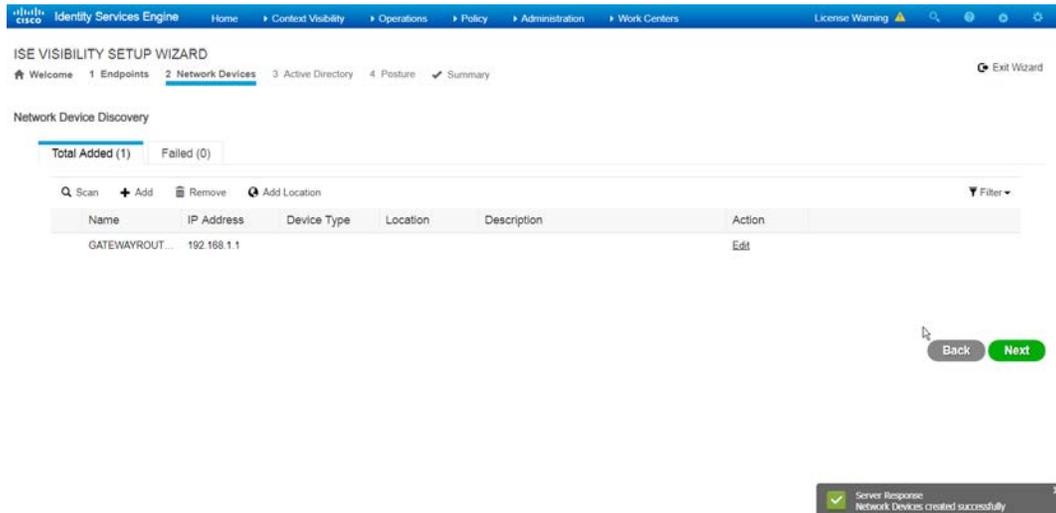
11. Enter the **community string** you created.



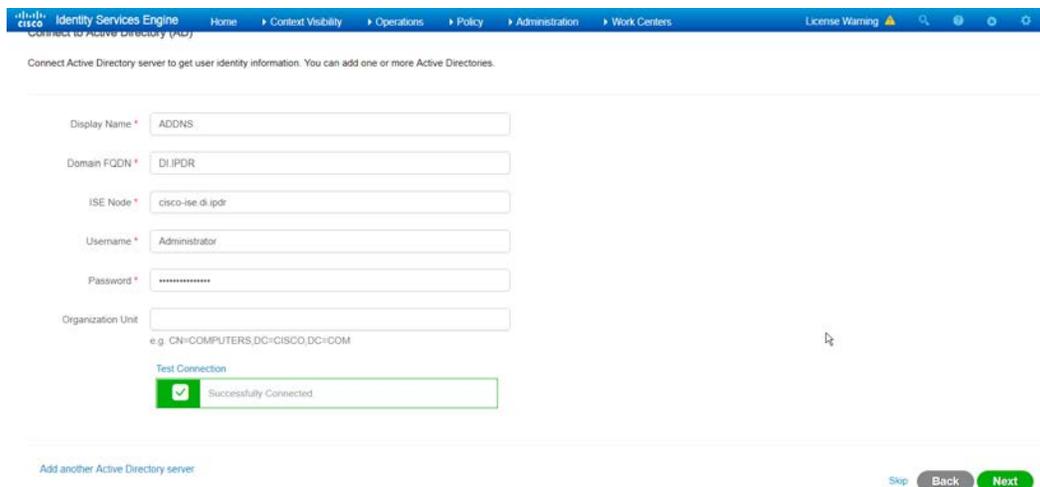
2411

2412

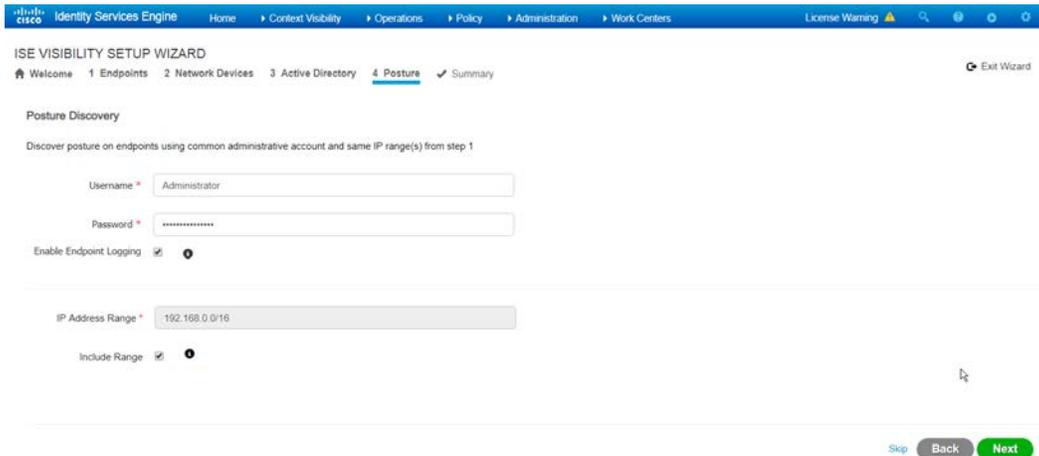
12. Click **OK**.



- 2413
- 2414 13. Click **Next**.
- 2415 14. Enter a **display name**.
- 2416 15. Enter the **domain name**.
- 2417 16. Enter the **hostname** of **Cisco ISE**.
- 2418 17. Enter a **username** and **password**.
- 2419 18. Click **Test Connection** to ensure that this works.



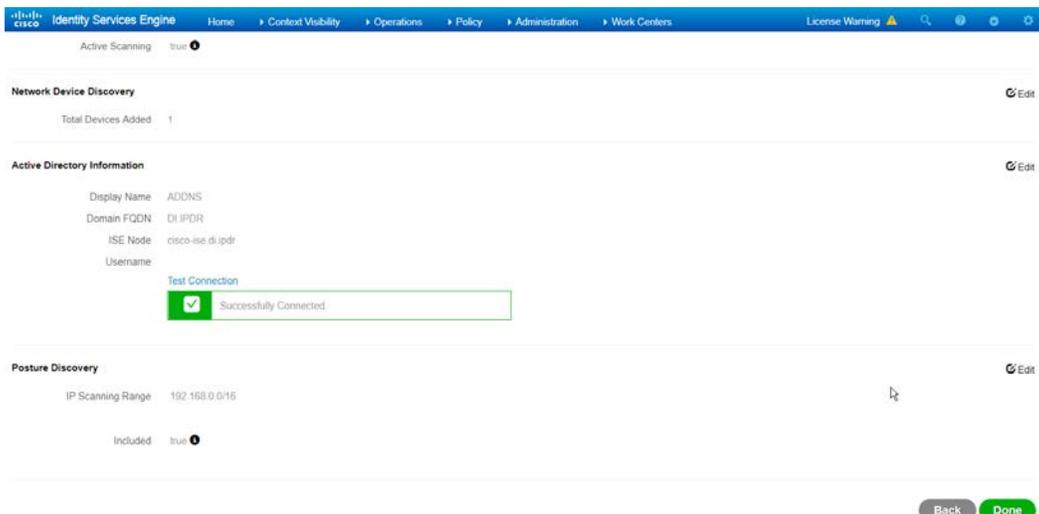
- 2420
- 2421 19. Click **Next**.
- 2422 20. Enter a **username** and **password**.
- 2423 21. Check the box next to **Enable Endpoint Logging**.
- 2424 22. Check the box next to **Include Range**.



2425

2426

23. Click **Next**.



2427

2428

2429

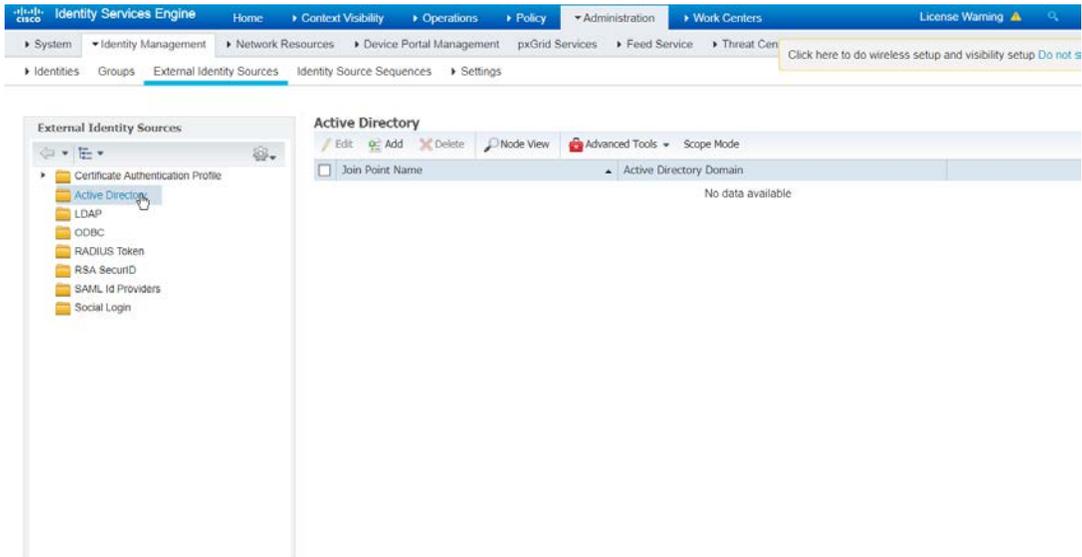
24. Verify the settings and click **Done**. (This should begin importing endpoints connected to the network device, and they will be visible on the ISE dashboard.)

## 2430 2.16.4 Policy Enforcement: Configure Active Directory Integration

2431

2432

1. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.



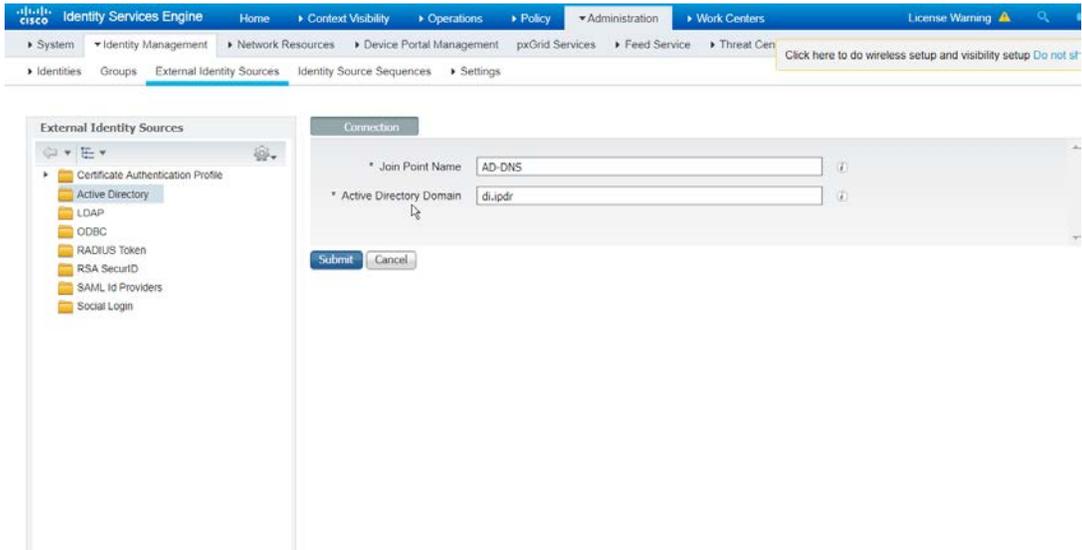
2433

2434

2435

2436

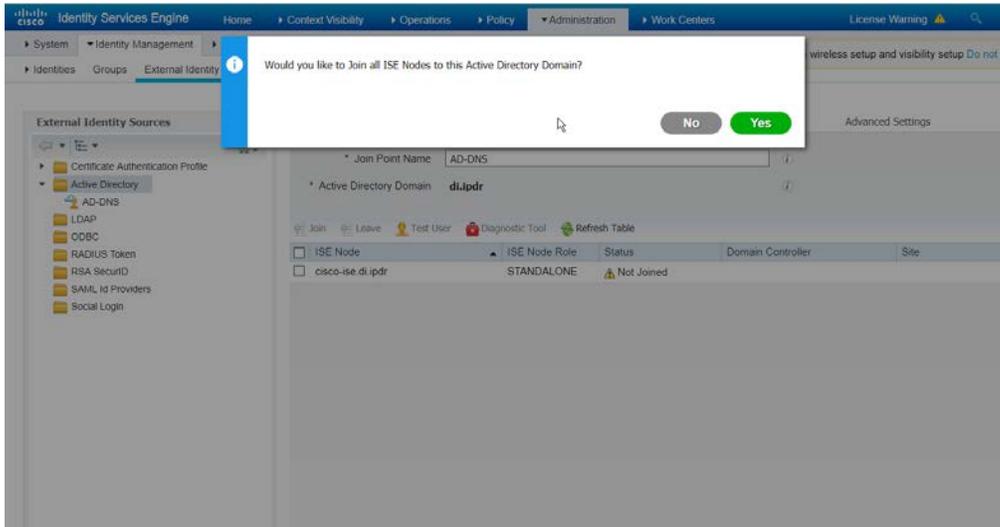
2. Click **Add**.
3. Enter a **name**.
4. Enter the **domain**.



2437

2438

5. Click **Submit**.

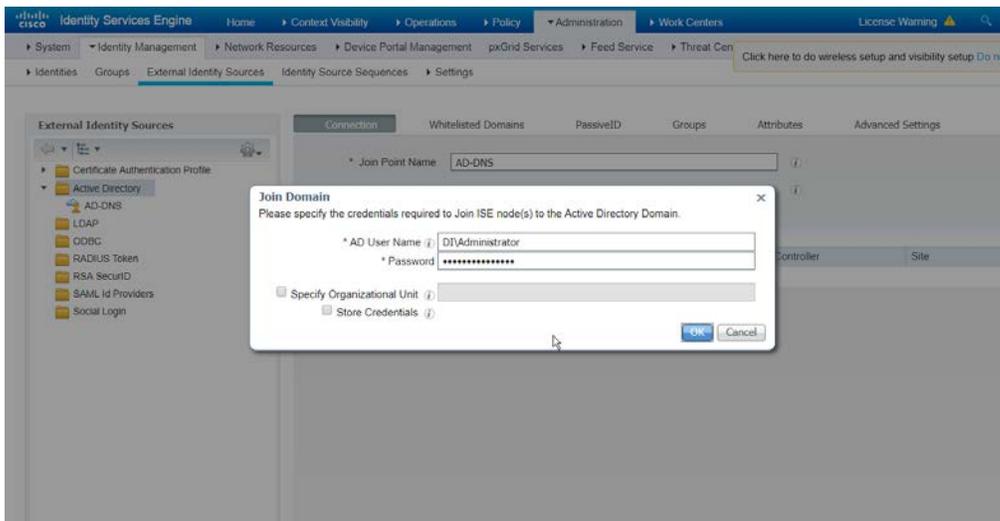


2439

2440

2441

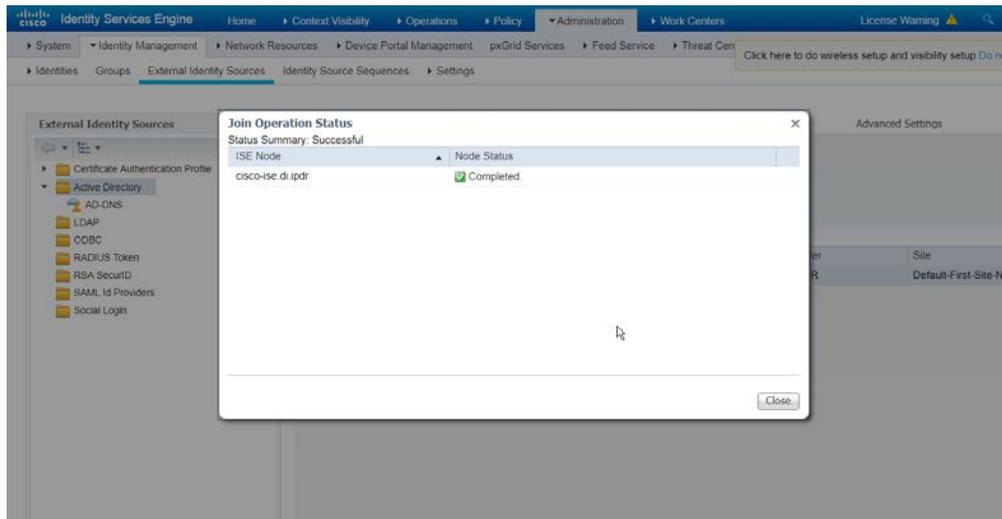
6. Click **Yes**.
7. Enter a **username** and **password** to join ISE to the domain.



2442

2443

8. Click **OK**.



2444

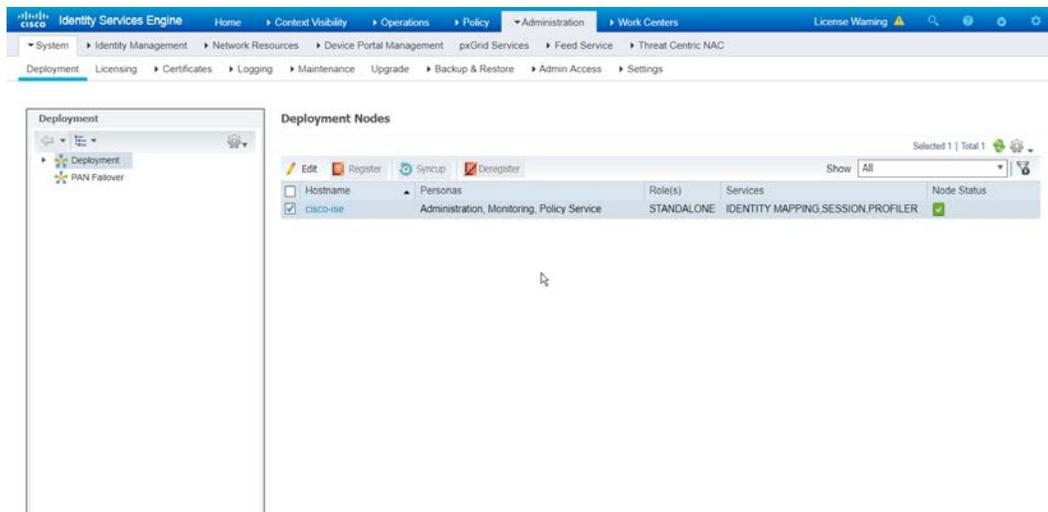
2445 9. Click **Close** when the join is finished.

### 2446 2.16.5 Policy Enforcement: Enable Passive Identity with AD

2447 This configuration allows users to use Active Directory usernames/passwords as authentication for the  
 2448 portal. The web portal will allow clients to download profiling software to ensure that clients have up to  
 2449 date software and can be trusted on the network.

2450 1. Navigate to **Administration > System > Deployment**.

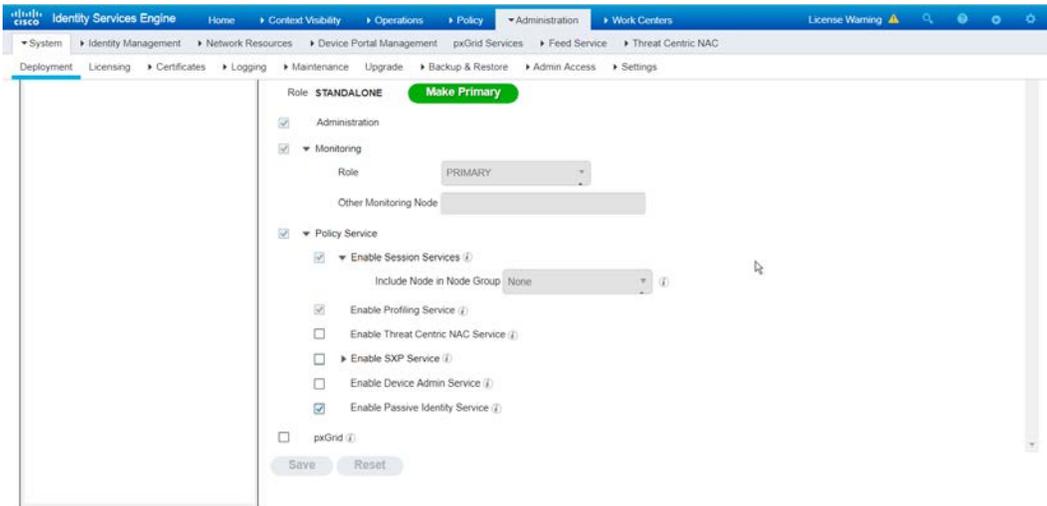
2451 2. Check the box next to ISE.



2452

2453 3. Click **Edit**.

2454 4. Check the box next to **Enable Passive Identity Service**.

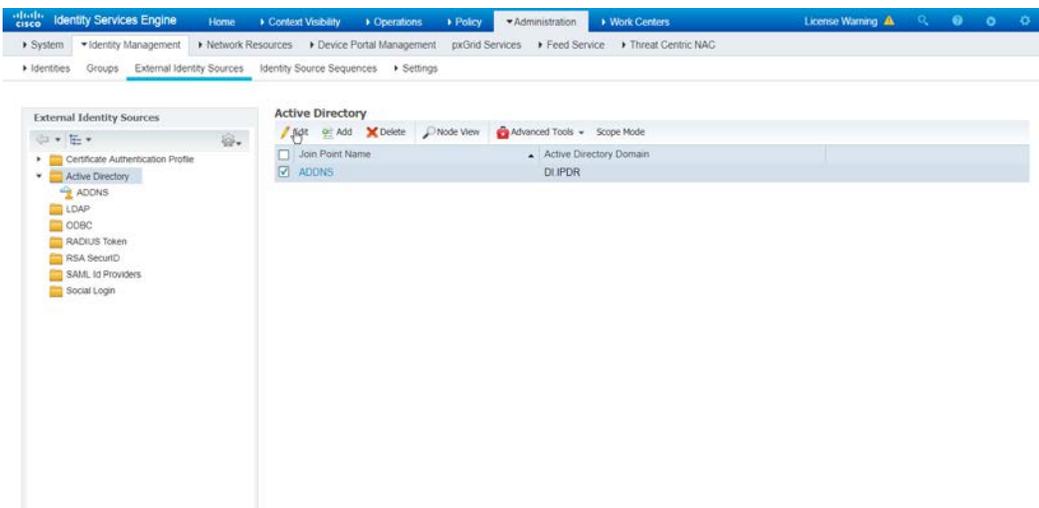


2455 5. Click **Save**.

2456 6. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.

2457 7. Click the name of the Active Directory machine.

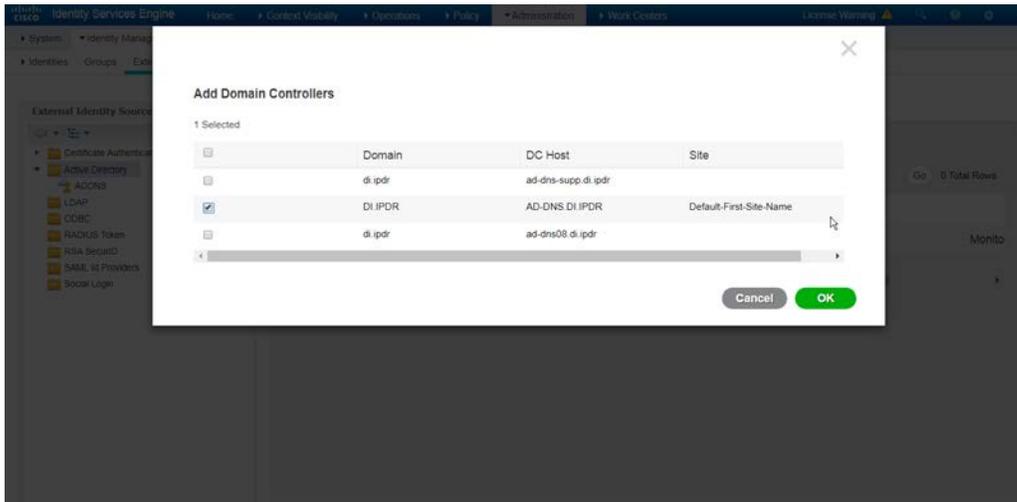
2458 8. Check the box next to the join point you just created.



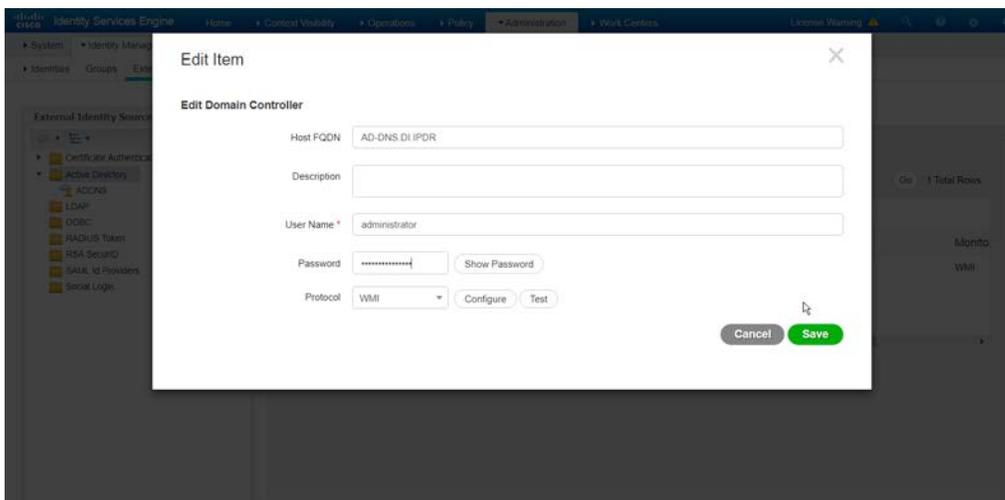
2461 9. Click **Edit**.

2462 10. Click the **PassiveID** tab.

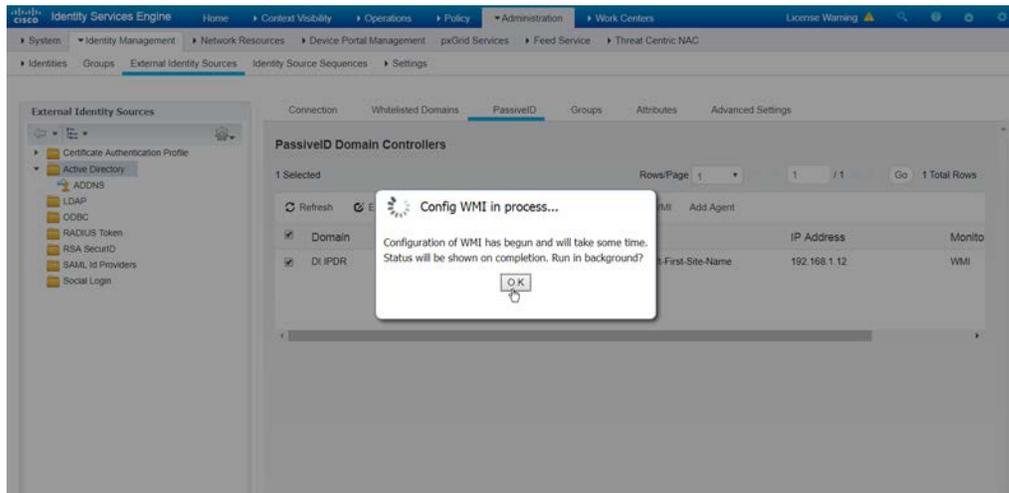
2463 11. Click **Add DCs** if there are no domain controllers listed.



- 2465
- 2466 12. Select the Active Directory domain controller.
- 2467 13. Click **OK**.
- 2468 14. Check the box next to the selected domain controller.
- 2469 15. Click **Edit**.
- 2470 16. Enter credentials for an administrator account.



- 2471
- 2472 17. Click **Save**.
- 2473 18. Click **Config WMI**.
- 2474 19. Click **OK**.



2475

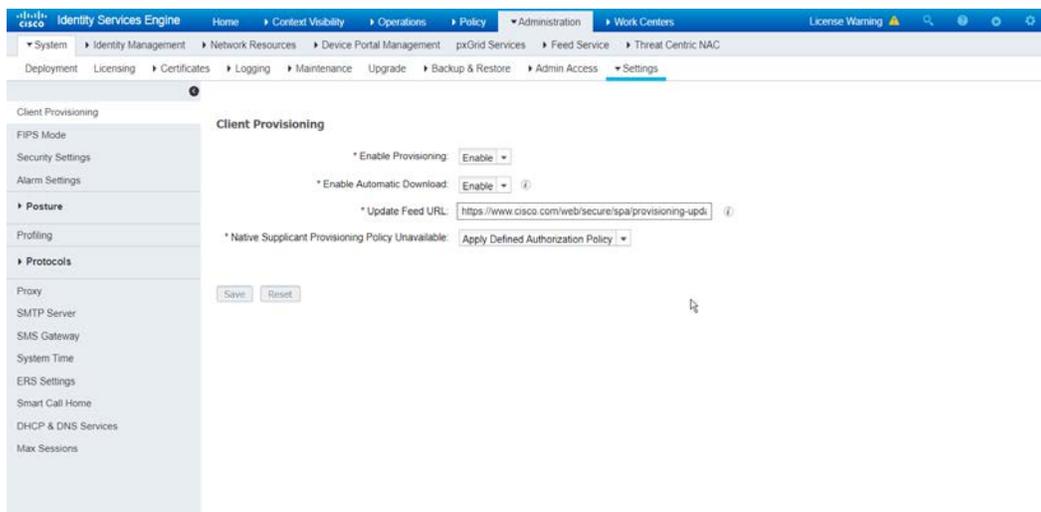
2476

20. Click **OK** when this configuration finishes.

2477

21. Navigate to **Administration > System > Settings > Client Provisioning**.

2478

22. Set **Enable Automatic Download** to **Enable**.

2479

23. Click **Save**.

2480

2481

24. Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.

2482

2483

25. Click the **Groups** tab.

2484

26. Click **Add > Select Groups from Directory**.

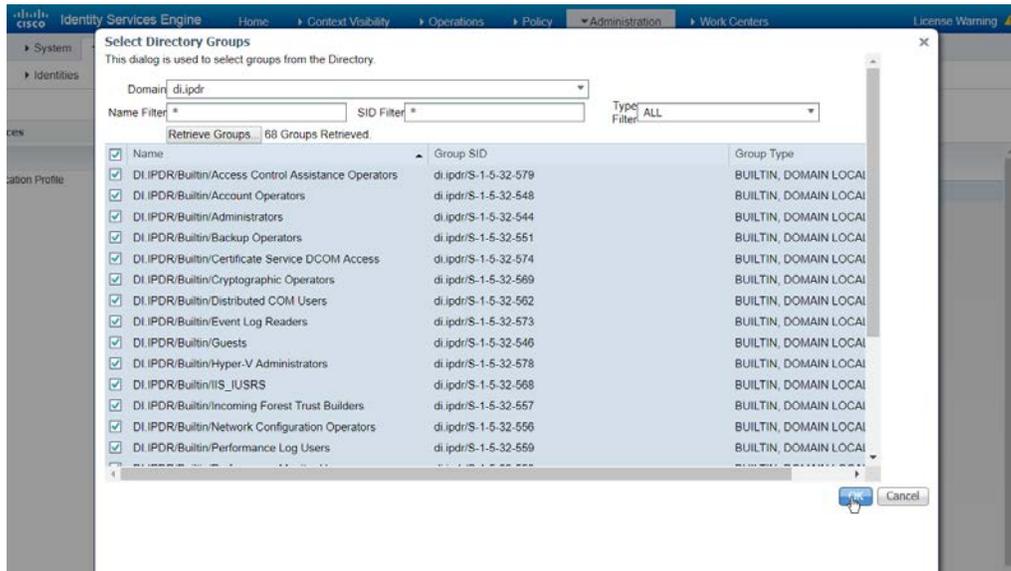
2485

27. Click **Retrieve Groups**. (This should populate the window with the groups from Active Directory.)

2486

2487

28. Select them all.



2488

2489 29. Click **OK**. (If you add more groups to Active Directory they can be imported in the same way in  
 2490 the future.)

2491 30. Click the **Attributes** tab.

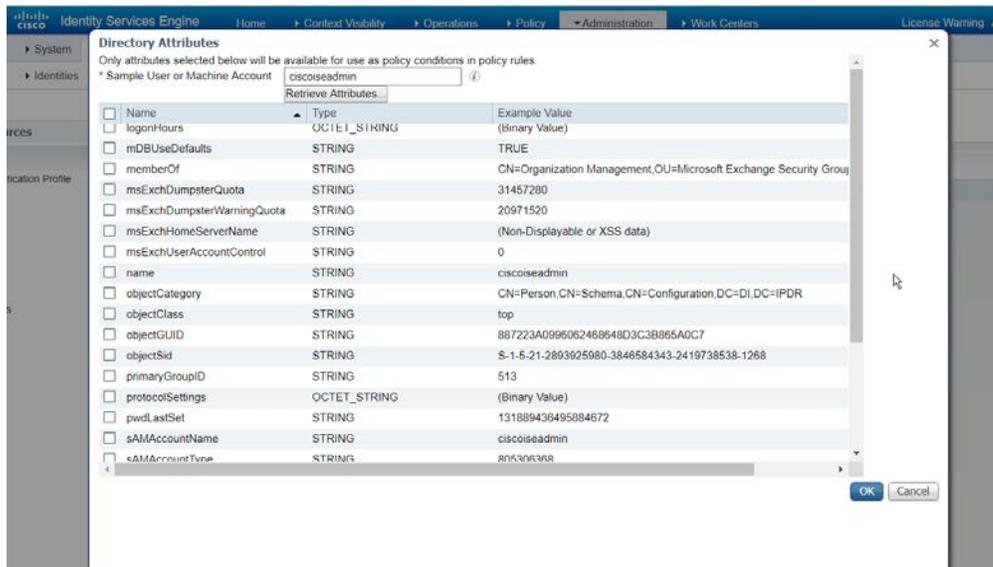
2492 31. Click **Add > Select Attributes from Directory**.

2493 32. Enter a **username**.

2494 33. Click **Retrieve Attributes**. (This will populate the window with Active Directory's available  
 2495 attributes, so they can be used for policy in Cisco ISE.)

2496 34. Click **OK**.

2497 35. Select any desired attributes.



2498

2499 36. Click **OK**.2500 37. Click **Save**.

## 2501 2.16.6 Policy Enforcement: Developing Policy Conditions

2502 1. Navigate to **Policy > Policy Elements > Conditions > Posture**.

2503 2. Expand the **Posture** section. This will reveal a list of categories for conditions. (Note: These

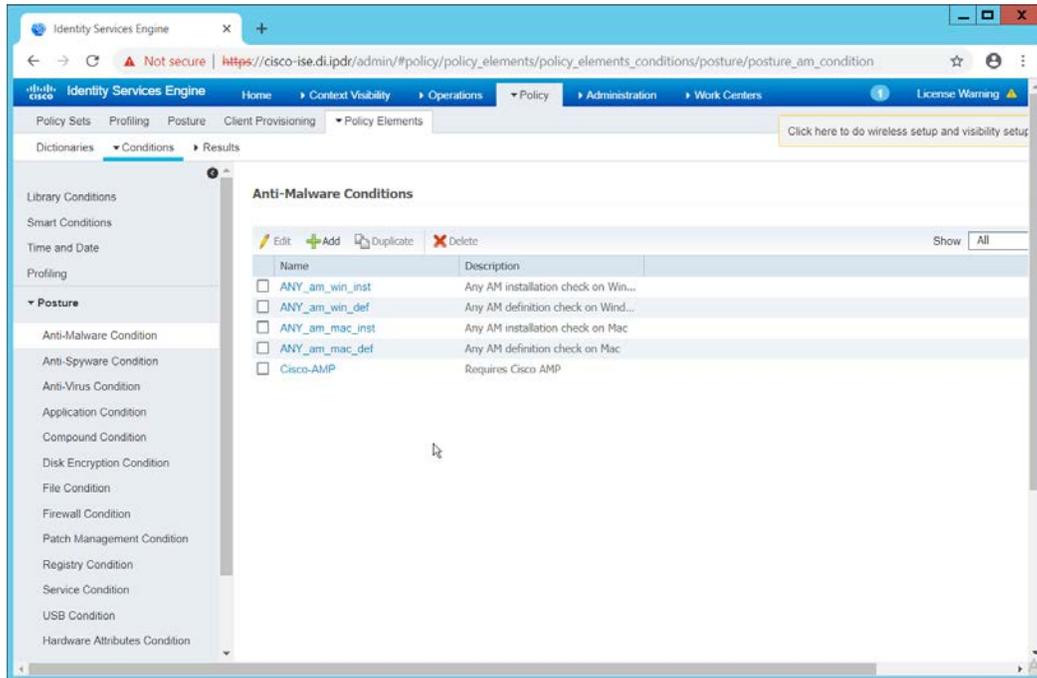
2504 conditions allow you to select or define requirements that endpoints should meet. In typical

2505 enterprises, these conditions can be used as requirements to gain network access—however,

2506 this strongly depends on the capabilities of your network device.)

2507 3. As an example, we will require that Cisco AMP be installed on all Windows devices. If you are

2508 using a different anti-malware software, locate that instead. Click **Anti-Malware Condition**.



2509

2510

2511

2512

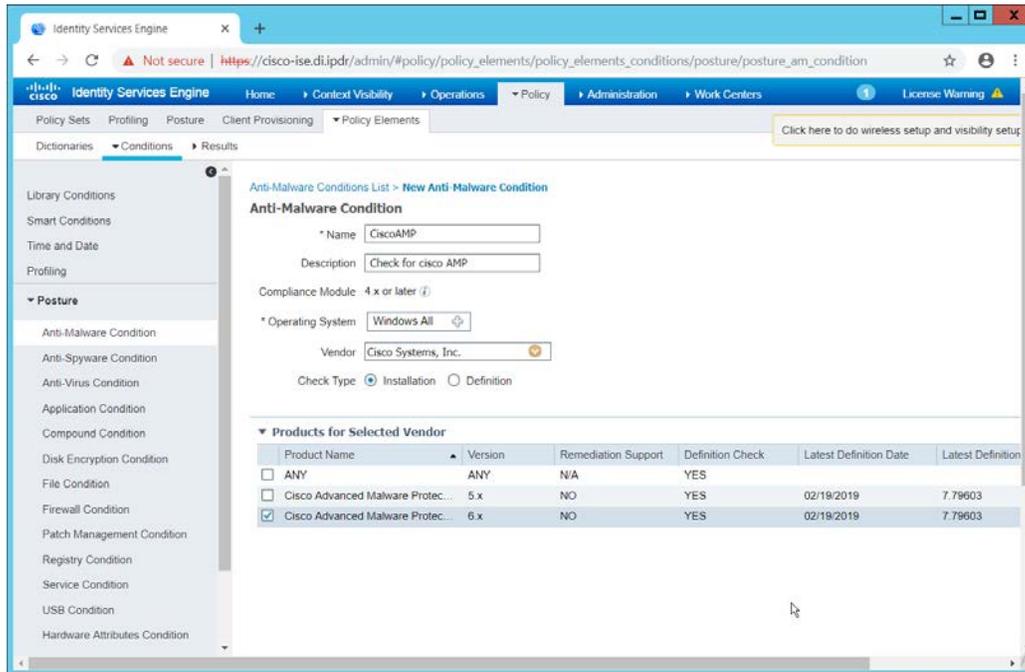
2513

2514

2515

2516

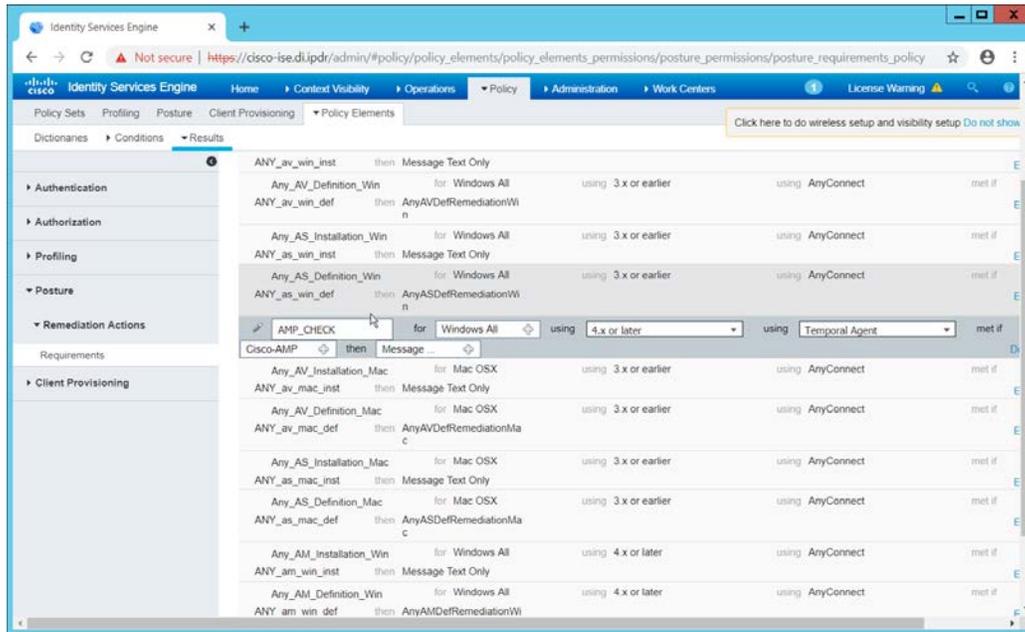
4. Click **Add**.
5. Enter a **name**.
6. Enter a **description** if desired.
7. Select **Windows All** for **Operating System**.
8. Select **Cisco Systems, Inc.** for **Vendor**.
9. Under **Products for Selected Vendor**, check the box next to **Cisco Advanced Malware Protection** with the version number you have installed.



2517  
2518 10. Click **Submit**.

## 2519 2.16.7 Policy Enforcement: Developing Policy Results

- 2520 1. Navigate to **Policy > Policy Elements > Results > Posture > Requirements**.
- 2521 2. Click one of the black arrows next to the **Edit** link, and select **Insert New Requirement**.
- 2522 3. Enter a **name**.
- 2523 4. Select **Windows All** for **Operating Systems**.
- 2524 5. Select **4.x or later** for **Compliance Module**.
- 2525 6. Select **Temporal Agent** for **Posture**.
- 2526 7. Select **User Defined Conditions > Anti-Malware Condition > Cisco AMP** (substitute Cisco AMP  
2527 with the name of the condition you just created).
- 2528 8. Select **Message Text Only** for the **Remediation Action**. (Other remediation actions can be  
2529 defined by going to **Policy > Policy Elements > Results > Posture > Remediation Actions**, but  
2530 there is not an option for Cisco AMP to be installed, so we leave the default for now.)
- 2531 9. Enter a **Message** to inform the user that they must install Cisco AMP.

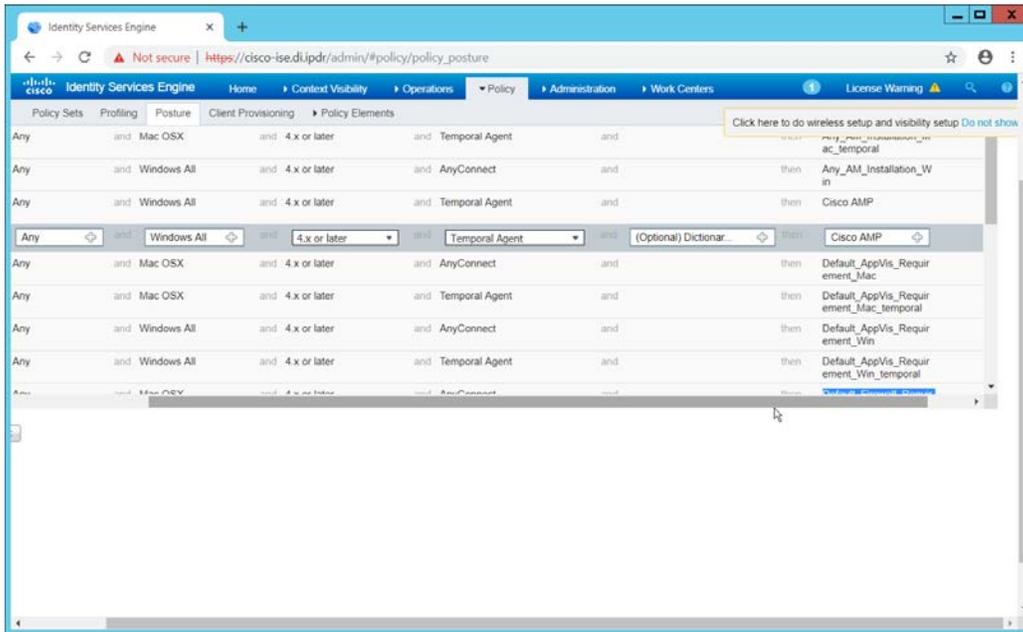


2532  
2533

10. Click **Save**.

## 2534 2.16.8 Policy Enforcement: Enforcing a Requirement in Policy

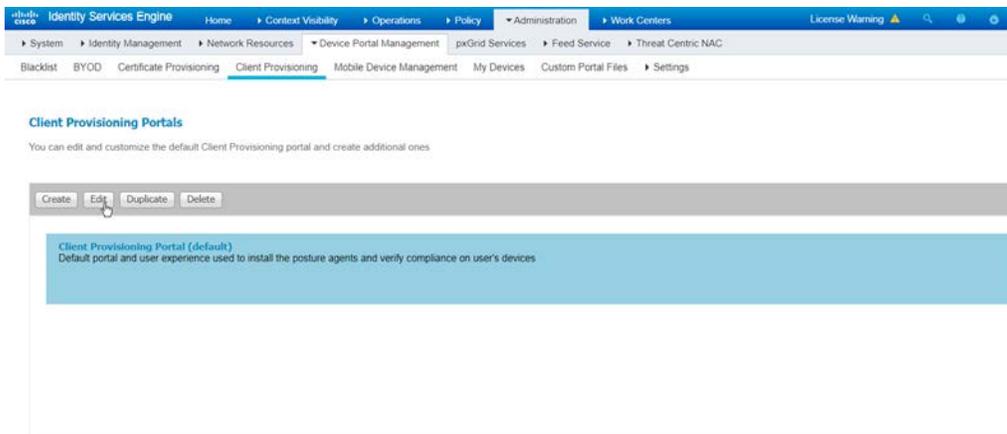
- 2535 1. Navigate to **Policy > Posture**.
- 2536 2. Click one of the black arrows next to the **Edit** link, and select **Insert New Policy**.
- 2537 3. Enter a **name**.
- 2538 4. Select **Windows All** for **Operating Systems**.
- 2539 5. Select **4.x or later** for **Compliance Module**.
- 2540 6. Select **Temporal Agent** for **Posture Type**.
- 2541 7. Select **Cisco AMP** (substitute Cisco AMP with the name of the requirement you just created).



- 2542
  - 2543
  - 2544
  - 2545
8. Click **Done**.
  9. Ensure that the green checkboxes next to the rules you wish to apply are the only checkboxes enabled, as anything enabled will be enforced.

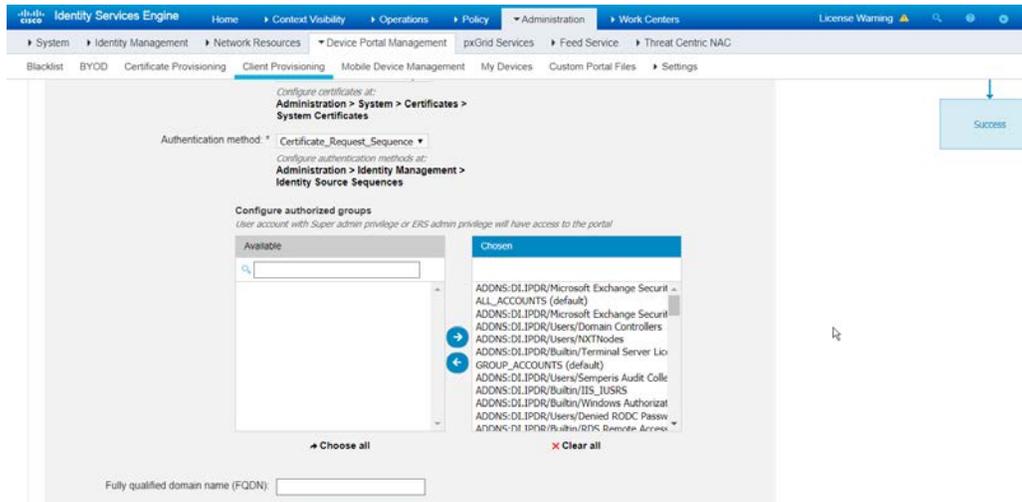
### 2546 2.16.9 Policy Enforcement: Configuring a Web Portal

- 2547 1. Navigate to **Administration > Device Portal Management > Client Provisioning**.
- 2548 2. Select the **Client Provisioning Portal (default)**.



- 2549
  - 2550
3. Click **Edit**.

- 2551 4. Under **Portal Settings**, go to **Configure authorized groups** and select the groups that should  
 2552 require a Cisco ISE client.  
 2553 5. Enter a domain name for **FQDN**, and add it to your DNS.



- 2554  
 2555 6. Click **Save**.

## 2556 2.16.10 Configuring RADIUS with Your Network Device

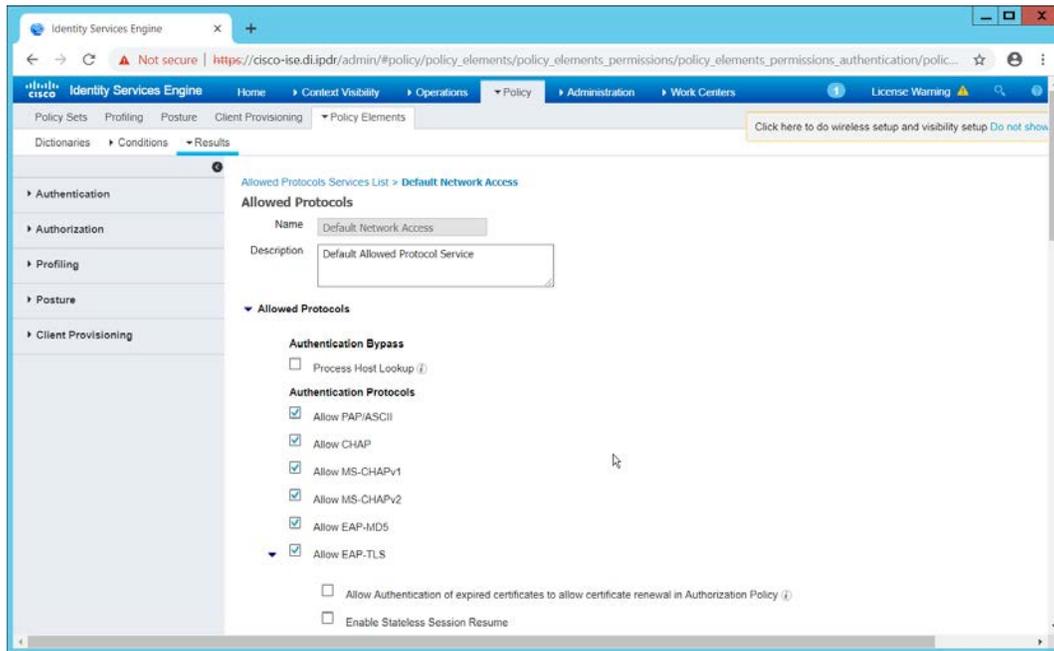
2557 Cisco ISE requires a Remote Authentication Dial-In User Service (RADIUS) session for posture to  
 2558 function. Posture refers to ISE's ability to check that a machine complies with a specified policy, which  
 2559 may be based on the operating system (OS) and may contain requirements such as installation of  
 2560 certain security applications or the presence of configuration files. Machines that are not in compliance  
 2561 can be kept separated from the network. The process for setting this up varies widely among machines,  
 2562 but the overall requirements have commonalities among systems.

- 2563 • The **Network Device** (i.e., the router or switch) must support RADIUS functions, specifically  
 2564 **Authentication, Authorization, and Accounting**. Furthermore, it must also support **CoA**, which  
 2565 is **Change of Authorization**. To configure this, you must configure your network device to use  
 2566 Cisco ISE as a RADIUS server. What this means is that your network device will forward  
 2567 authentication requests to Cisco ISE, and Cisco ISE will respond with an "accept" or "reject."
- 2568 • The **Network Device** must support some form of **802.1x**. Note that this is not supported on  
 2569 certain routers, even if RADIUS is supported. **802.1x** is a mechanism for authenticating the end  
 2570 workstation to the network device, potentially over wireless or through Ethernet.

- 2571 a. This can take various forms, such as a captive web portal, MAC address authentication,  
2572 or user authentication. A captive web portal, if the device supports it, may be ideal for  
2573 configuration without the correct hardware.
- 2574 b. There are also many switches that provide direct 802.1x username/password  
2575 authentication. Note that if you choose to use this mechanism, a client is still required,  
2576 and it will not be in the web browser. Windows has a built-in 802.1x client, which can be  
2577 configured on network adapters under the **Authentication** tab. To enable it, you must  
2578 first start the service **Wired AutoConfig**, and then the **Authentication** tab will become  
2579 available for configuration.
- 2580 c. Whatever form of 802.1x is chosen, the request for authentication must be forwarded  
2581 to Cisco ISE. Cisco ISE will process the request for authentication.
- 2582 • The two steps above detail the **authentication** phase. Once authenticated, the network device  
2583 must redirect the user to the client provisioning portal (or to a guest portal), depending on the  
2584 setup. The URL for this can be acquired from the active **Authorization Profile** in ISE.
  - 2585 • The user will then authenticate to the **Guest Portal** or **Client Provisioning Portal** (depending on  
2586 your setup). The portal will prompt the user to download an executable, which will run posture.
  - 2587 • The executable will *first* check for the existence of a RADIUS session in Cisco ISE for the user  
2588 who downloaded the executable. It will primarily check the MAC address that visited the ISE  
2589 web portal against the MAC addresses of existing sessions. *If and only if a session exists*, it will  
2590 run posture based on the policy you set up. You can verify that a session exists by navigating to  
2591 **Operations > RADIUS > Live Sessions**.

### 2592 2.16.11 Configuring an Authentication Policy

- 2593 1. Navigate to **Policy > Policy Elements > Results > Authentication > Allowed Protocols**.
- 2594 2. Select the **Default Network Access** protocol or create your own.
- 2595 3. Ensure that any protocols that need to be supported for your network setup are allowed. In  
2596 particular, if using 802.1x, it is likely that you should check the box next to **Allow MS-CHAPv2**.



2597

2598

2599

2600

2601

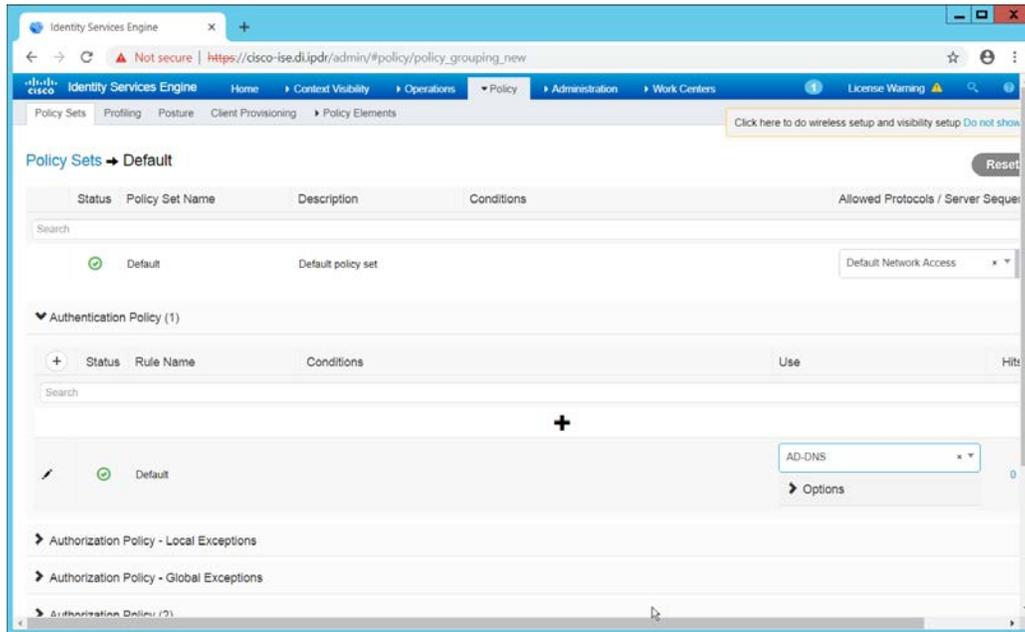
2602

2603

2604

2605

4. Click **Save**.
5. Navigate to **Policy > Policy Sets**.
6. Select the default policy.
7. Ensure that the **Allowed Protocol** selection matches the allowed protocol you just created/edited.
8. Expand the **Authentication Policy** section, and select the ID stores from which to authenticate users. For example, if you set up an Active Directory integration, it may be desirable to authenticate users from there.

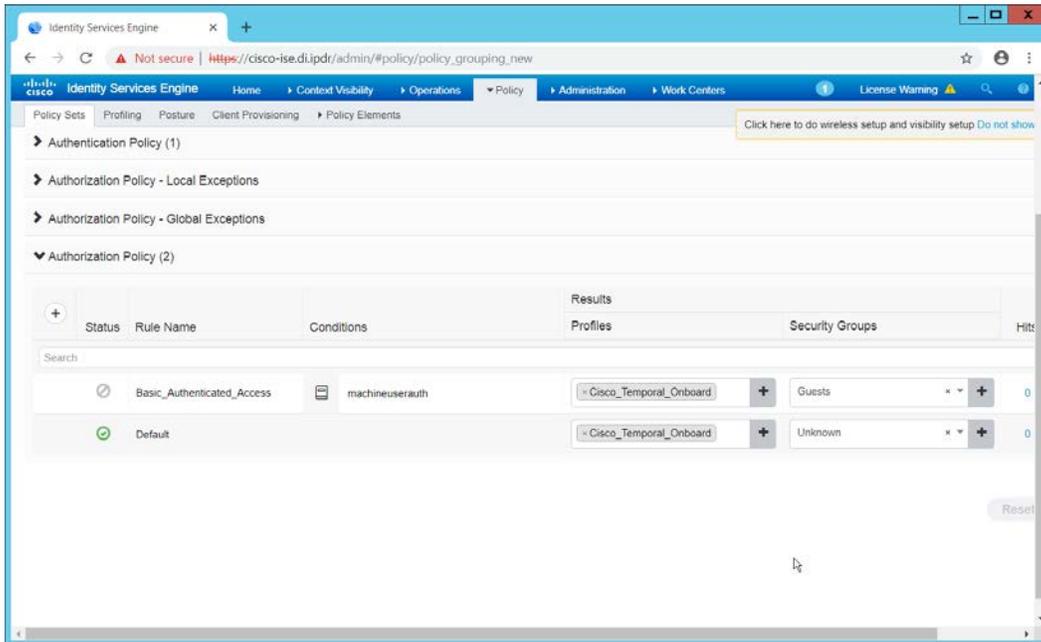


2606  
2607

9. Click **Save**.

## 2608 2.16.12 Configuring an Authorization Policy

- 2609 1. The Authorization Profile is likely dependent on your network device, but it is possible that the  
2610 **Cisco\_Temporal\_Onboard** profile will work even for non-Cisco devices. You can edit the  
2611 authorization policy by navigating to **Policy > Policy Elements > Results > Authorization >**  
2612 **Authorization Profiles**.
- 2613 2. The temporal onboard profile will attempt to redirect the user to a client-provisioning portal.  
2614 This redirection will most likely happen only automatically on compatible Cisco network devices.  
2615 If another device is used, the device may need to manually redirect the user to the client-  
2616 provisioning portal after authentication. (We accomplished this in pfSense for our build by using  
2617 a “post-authentication redirection” feature in the Captive Portal.)
- 2618 3. Once you are finished configuring the **Authorization Profile**, navigate to **Policy > Policy Sets**.
- 2619 4. Select the default policy.
- 2620 5. Expand the **Authorization Policy** section.
- 2621 6. Note that you can configure this for as many groups and conditions as desired, potentially  
2622 specifying different authorization profiles for various user groups or levels of authentication,  
2623 including unauthenticated access. Under **Results > Profiles**, you can select the authorization  
2624 profiles you configured.



2625

2626 7. Click **Save**.2627 

## 2.17 Tripwire IP360

2628 This section details installation and configuration for Tripwire IP360.

2629 

### 2.17.1 Installation

- 2630 1. Move or copy the Tripwire IP360 Virtual Machine into your virtual environment; start Virtual  
2631 Machine and observe its successful start-up.

## 2632 2. Log in using default admin credentials.

```

Running airs-firstboot: [ OK ]
Starting postfix: [ OK ]
Running vnc-airs-firstboot: [ OK ]
Installing Ontology: [ 2789.687610] sched: RT throttling activated [ OK ]

Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Waiting for Tripwire Axon Access Point Gateway.....
running: PID:27875
Starting HAL daemon: [ OK ]
Starting ched: [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory
Starting dbd: [ OK ]
Starting hostd: [ OK ]
Starting objectapixx: [ OK ]
Starting reportd: [ OK ]
Starting vnc-php-fpm: [ OK ]
Starting vnc-airs: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nclib: U7.48 and libche: U4.6
Starting imageserver: [ OK ]
Starting httpd: [ OK ]
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cronld: [ OK ]
digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting loader: [ OK ]

Starting incronld: [ OK ]
Starting monit: Cannot translate 'vnc-934358a2' to FQDN name -- Name or service not known
Generated unique Monit id fdc3ed1c4764a7a1c25183899c9e128a and stored to '/var/monit/id'
Starting Monit 5.14 daemon with http interface at [localhost]:2812 [ OK ]

Starting ntlmops:

Tripwire Appliance
vnc-934358a2 login:

Tripwire Appliance
vnc-934358a2 login: admin
Password: _

```

2633

2634

## 3. When prompted after initial login, set a new password and record it in a safe location.

```

Installing Ontology: [ 2789.687610] sched: RT throttling activated [ OK ]

Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Waiting for Tripwire Axon Access Point Gateway.....
running: PID:27875
Starting HAL daemon: [ OK ]
Starting ched: [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory
Starting dbd: [ OK ]
Starting hostd: [ OK ]
Starting objectapixx: [ OK ]
Starting reportd: [ OK ]
Starting vnc-php-fpm: [ OK ]
Starting vnc-airs: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nclib: U7.48 and libche: U4.6
Starting imageserver: [ OK ]
Starting httpd: [ OK ]
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cronld: [ OK ]
digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting loader: [ OK ]

Starting incronld: [ OK ]
Starting monit: Cannot translate 'vnc-934358a2' to FQDN name -- Name or service not known
Generated unique Monit id fdc3ed1c4764a7a1c25183899c9e128a and stored to '/var/monit/id'
Starting Monit 5.14 daemon with http interface at [localhost]:2812 [ OK ]

Starting ntlmops:

Tripwire Appliance
vnc-934358a2 login:

Tripwire Appliance
vnc-934358a2 login: admin
Password:
You must change your password.
This will also change the password for ip360@tripwire.com.
New password:

```

2635

- 2636 4. Use the command **system hostname update <hostname>** to update the system's hostname in  
2637 accordance with your environment's naming scheme.

```
[ 1.647488] [drm] Max dedicated hypervisor surface memory is 0 kiB
[ 1.647586] [drm] Maximum display memory size is 20480 kiB
[ 1.647799] [drm] VRAM at 0xc0000000 size is 20480 kiB
[ 1.647995] [drm] GTT0 at 0xc0000000 size is 256 kiB
[ 1.648022] [drm] global init.
[ 1.648373] [TTM] Zone kernel: Available graphics memory: 8214352 kiB
[ 1.648544] [TTM] Zone dma32: Available graphics memory: 2897152 kiB
[ 1.648694] [TTM] Initializing pool allocator
[ 1.648837] [TTM] Initializing DMA pool allocator
[ 1.649381] [drm] Supports vblank timestamp caching Rev 2 (21.10.2013).
[ 1.649576] [drm] No driver support for vblank timestamp query.
[ 1.659538] [drm] Screen Target Display device initialized
[ 1.659551] [drm] width 1280
[ 1.659661] [drm] height 768
[ 1.659801] [drm] bpp 32
[ 1.651637] [drm] Fifo max 0x00040000 min 0x00001000 cap 0x000007ff
[ 1.652583] [drm] Using command buffers with DMA pool.
[ 1.652695] [drm] DX: no.
[ 1.656728] fbcon: sgdmafb (FBD) is primary device
[ 1.659833] Console: switching to colour frame buffer device 160x48
[ 1.672613] [drm] Initialized vmgfx 2.12.0 20170221 for 0000:00:0f:0 on minor 0
[ 1.716876] random: Fast init done
[ 1.728649] Floppy device(s): fdb is 1.44M
[ 1.733372] PDC 0 is a post-1991 82877.
[ 1.817166] EXT4-Fs (sda2): mounted filesystem with ordered data mode. Dpts: (null)
[ 1.822838] dracut: Mounted root filesystem /dev/sda2
[ 1.881843] dracut: Switching root
Welcome to Tripwire Appliance
Starting udev: [ 2.251929] udev: starting version 147
[ 2.353284] shpchp: Standard Hot Plug PCI Controller Driver version: 0.4
[ 2.562832] random: crng init done
[ 3.843626] p1xd_smbus 0000:00:07:3: SMBus Host Controller not enabled!
[ 3.851658] vma_vnc1 0000:00:07:7: Found VNC PCI device at 0x1000, irq 16
[ 3.851728] vma_vnc1 0000:00:07:7: Using capabilities 0xc
[ 3.851843] Guest personality initialized and is active
[ 3.851989] VNCI host device registered (name=vnc1, major=10, minor=57)
[ 3.852059] Initialized host personality.
[ 3.869249] input: PC Speaker as /devices/platform/pcspkr/input/input5
[ 3.118276] FUJITSU Extended Socket Network Device Driver - version 1.1 - Copyright (c) 2015 FUJITSU LIMITED
[ 3.195277] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[ 3.195365] e1000: Copyright (c) 1999-2006 Intel Corporation.
[ 3.538622] e1000 0000:02:00:0 eth0: (PCI:16MHz:32-bit) 00:50:56:12:3a:b1
[ 3.538615] e1000 0000:02:00:0 eth0: Intel(R) PRO/1000 Network Connection
[ 3.557272] ppdev: user-space parallel port driver
Setting hostname localhost.localdomain: [ OK ]
Checking filesystems: [ OK ]
```

- 2638 5. Use command **network interface update <interface> <IP>/<Broadcast IP>** to update network  
interface information in accordance with your environment's network.

```
Stopping esentd: [ OK ]
Stopping hostd: [ FAILED ]
Stopping reportd: [ OK ]
Stopping cheserver: [ OK ]
Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Triggerer failed udev events [ OK ]
digest_proxy does not need to start
Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Triggerer failed udev events [ OK ]
Starting cheserver: [ OK ]
Configuring PostgreSQL Memory [ OK ]
Starting hostd: [ OK ]
Starting reportd: [ OK ]
Starting esentd: [INFO] IP360 Event Daemon build # starting up
[INFO] nc1ib: U7.40 and libche: U4.6 [ OK ]
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cronid: [ OK ]
digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting monit: Cannot translate 'vnc-934358a2' to FQDN name -- Name or service not known
Starting Monit 5.14 daemon with http interface at [localhost]:2012 [ OK ]

Tripwire Appliance
vnc-934358a2 login: admin
Password:
Last login: Tue Sep 11 17:05:12 on tty1
vnc-934358a2: system hostname update tw360.d1.ipdr
Command succeeded.
vnc-934358a2: network interface update eth0 192.168.1.144/255.255.255.0
[552868.264771] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552868.264771] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552868.275441] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vnc-934358a2: _
```

6. Use command `network route_default create <gateway>` to update the system's default gateway information in accordance with your environment's network.

```

Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Retrigger failed udev events [ OK ]
Digest_proxy does not need to start
Calling the system activity data collector (sadc)...
Starting Tripwire Axon Access Point...
Tripwire Axon Access Point is already running.
Starting Tripwire Axon Access Point Gateway...
Tripwire Axon Access Point Gateway is already running.
Retrigger failed udev events [ OK ]
Starting cheserver? [ OK ]
Configuring PostgreSQL Memory
Starting hostd: [ OK ]
Starting reportd: [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nc11b: 07.40 and libche: 04.6
Starting axon-agent-supervisor: [ OK ]
Starting axon-data-loader: [ OK ]
Starting axon-data-transformer: [ OK ]
Starting axon-stream-listener: [ OK ]
Starting cron: [ OK ]
Digest_proxy does not need to start
Starting lifeguard: [ OK ]
Starting monit: Cannot translate 'vne-934358a2' to FQDN name -- Name or service not known
Starting Moinit 5.14 daemon with http interface at [localhost]:2012 [ OK ]

Tripwire Appliance
vne-934358a2 login: admin
Password:
Last login: Tue Sep 11 17:05:12 on tty1
vne-934358a2> system hostname update tw360.di.ipdr
Command succeeded.
vne-934358a2> network interface update eth0 192.168.1.144/255.255.255.0
[552869.264774] e1800: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552869.264774] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552869.275411] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2> network route_default create 192.168.1.1
[552116.598551] e1800: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552116.603950] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552116.608708] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2>

```

7. Use command **system nameserver create <nameserver IP>** to set up the DNS server.

```

Tripwire Axon Access Point Gateway is already running.
Retrigger failed udev events          [ OK ]
Starting cheserver:                   [ OK ]
Configuring PostgreSQL Memory
Starting hostd:                       [ OK ]
Starting reportd:                    [ OK ]
Starting eventd: [INFO] IP360 Event Daemon build # starting up
[INFO] nclib: U7.40 and libche: U4.6
Starting axon-agent-supervisor:       [ OK ]
Starting axon-data-loader:           [ OK ]
Starting axon-data-transformer:      [ OK ]
Starting axon-stream-listener:       [ OK ]
Starting cron:                       [ OK ]
Digest proxy does not need to start
Starting lifeguard:                  [ OK ]
Starting monit: Cannot translate 'vne-934358a2' to FQDN name -- Name or service not known
Starting Monit 5.14 daemon with http interface at [localhost]:2812
[ OK ]

Tripwire Appliance
vne-934358a2 login: admin
Password:
Last login: Tue Sep 11 17:05:12 on tty1
vne-934358a2> system hostname update tu360.di.ipdr
Command succeeded.
vne-934358a2> network interface update eth0 192.168.1.144/255.255.255.0
[552868.264771] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552868.264774] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552868.275441] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2> network route default create 192.168.1.1
[552116.598551] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[552116.603958] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[552116.608788] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Command succeeded.
vne-934358a2> system name server create 192.168.1.12
add nameserver.

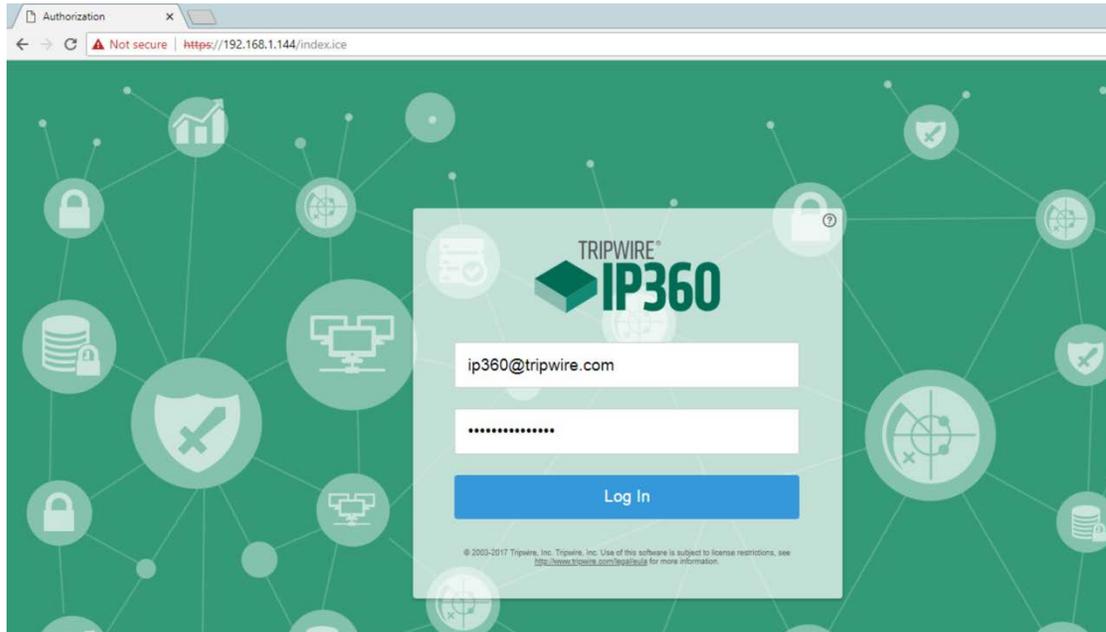
Usage:
system nameserver create <ip>

Example:
system nameserver create 192.168.1.2
tu360.di.ipdr> system nameserver create 192.168.1.12
Command succeeded.
tu360.di.ipdr> _

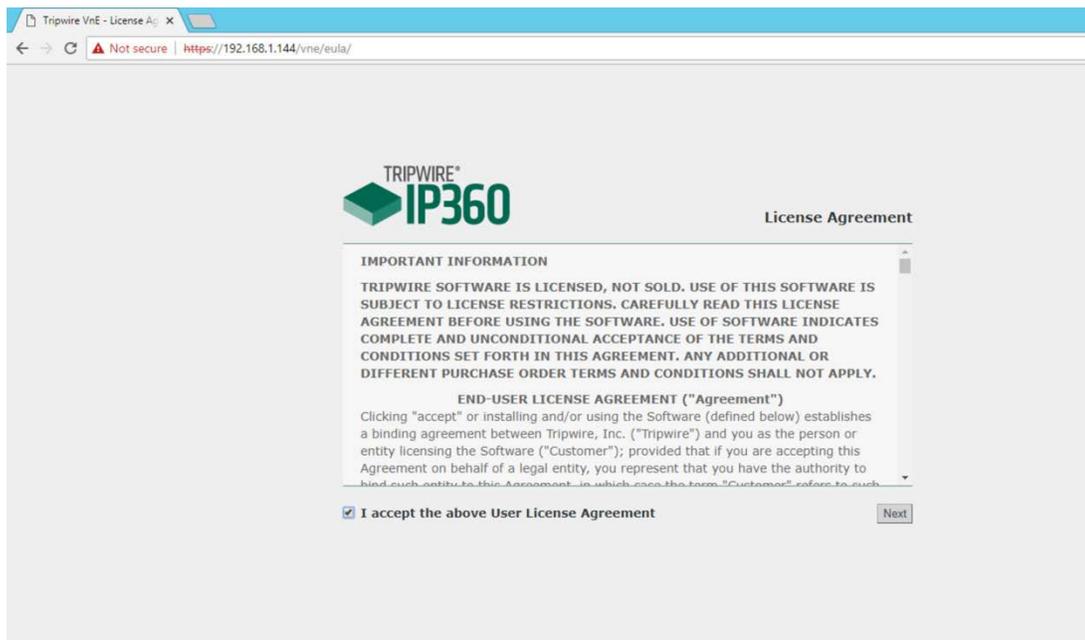
```

2639 2.17.2 Web Portal

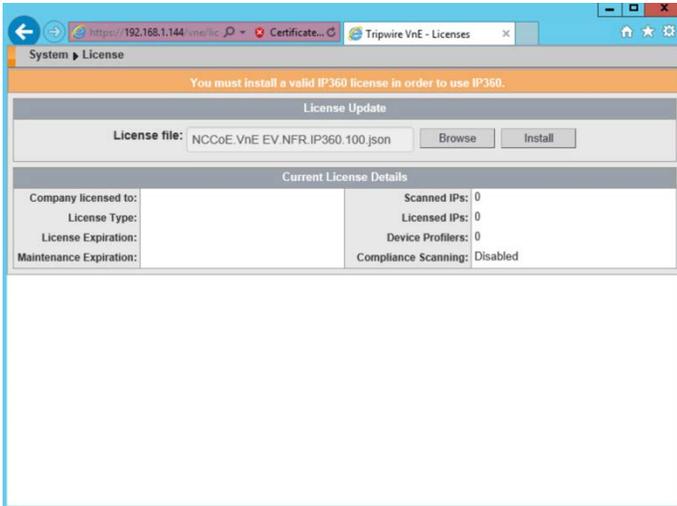
- 2640 1. From a web browser that can access the newly installed machine’s IP address, navigate to the IP  
2641 address and log in using the updated credentials from the setup process.



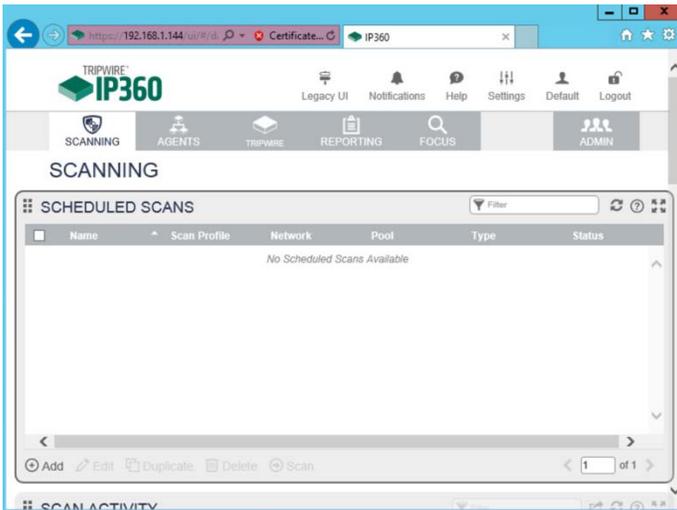
- 2642 2. Check the box next to **I accept the above User License Agreement.**  
2643



- 2644 3. Click **Next**.
- 2645 4. Browse to location of downloaded license file.



- 2646 5. Click **Install**.
- 2647
- 2648 6. Tripwire IP360 should now be installed and running.

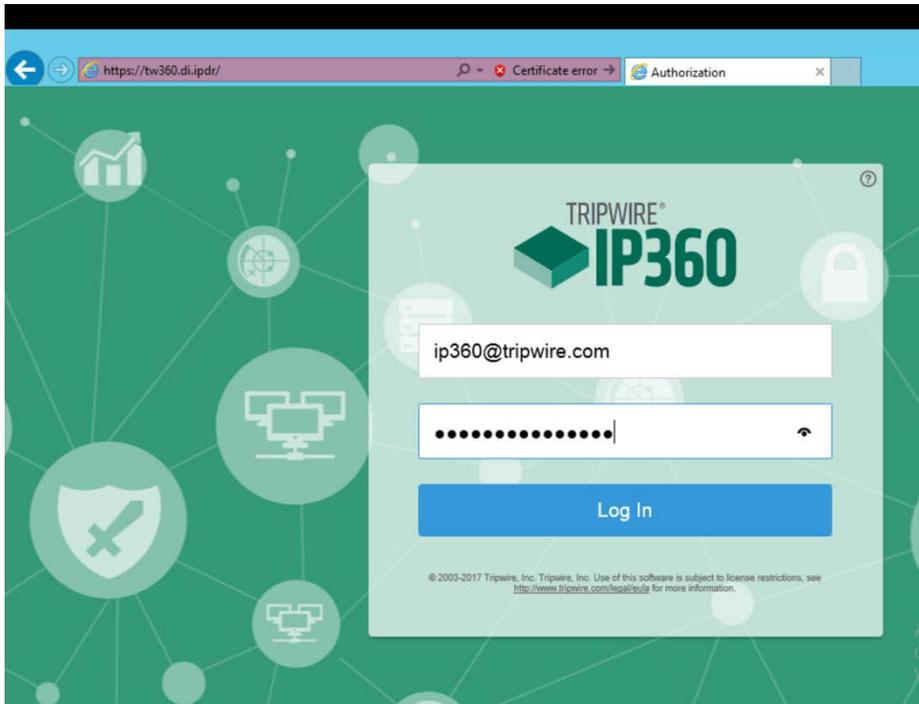


2649

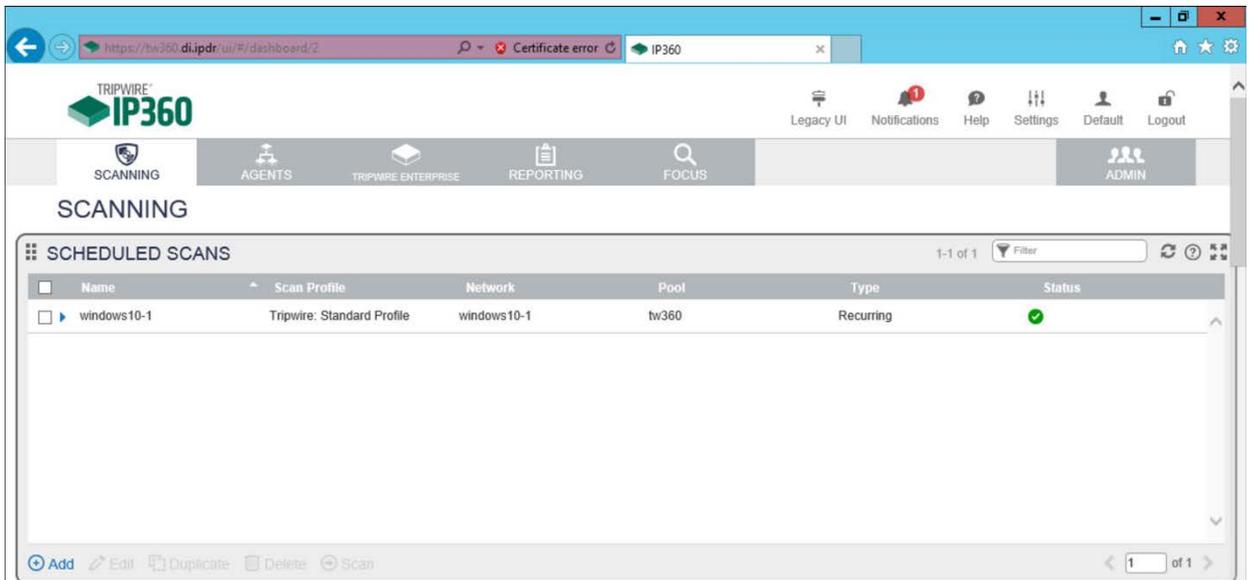
### 2650 2.17.3 Scanning

2651 This section details instructions for using Tripwire IP360 to run a scan on enterprise systems. The  
2652 specific details of the scan will vary based on each enterprise’s security needs.

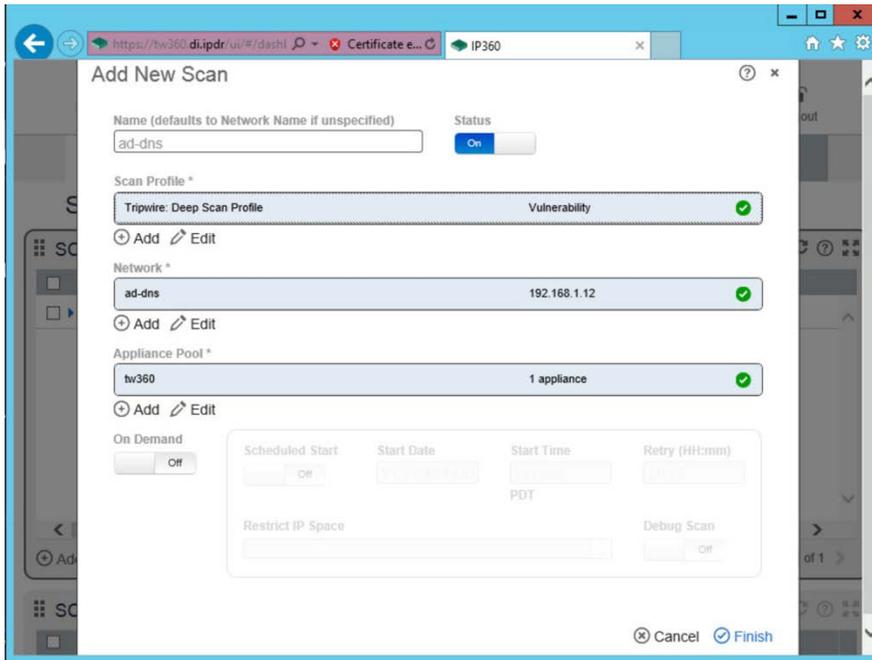
- 2653 1. Navigate to the web interface and log in.



- 2654 2. Navigate to the **Scanning** tab.

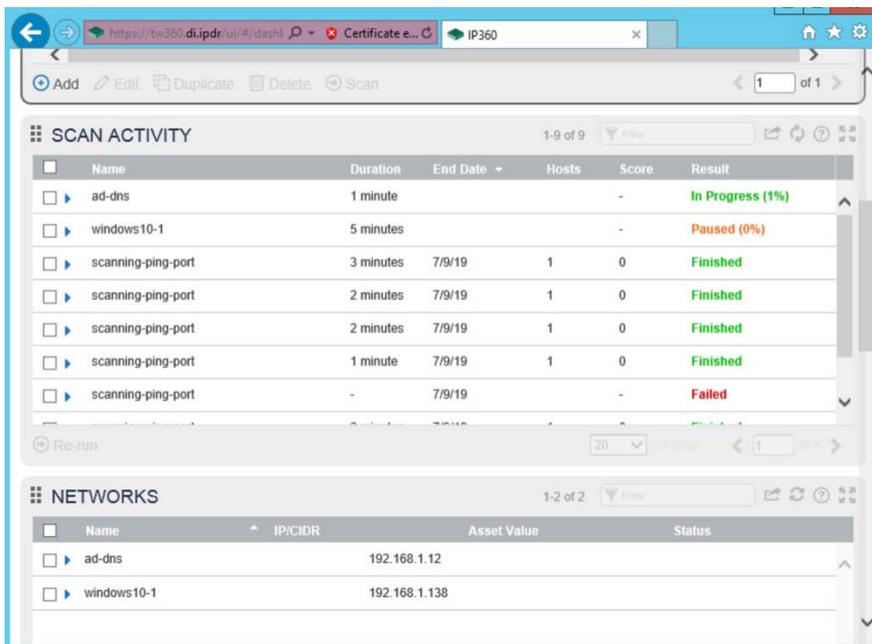


- 2656 3. Click **Add**.
- 2657
- 2658 4. Complete the information regarding the new scan according to the preferences of your
- 2659 organization.



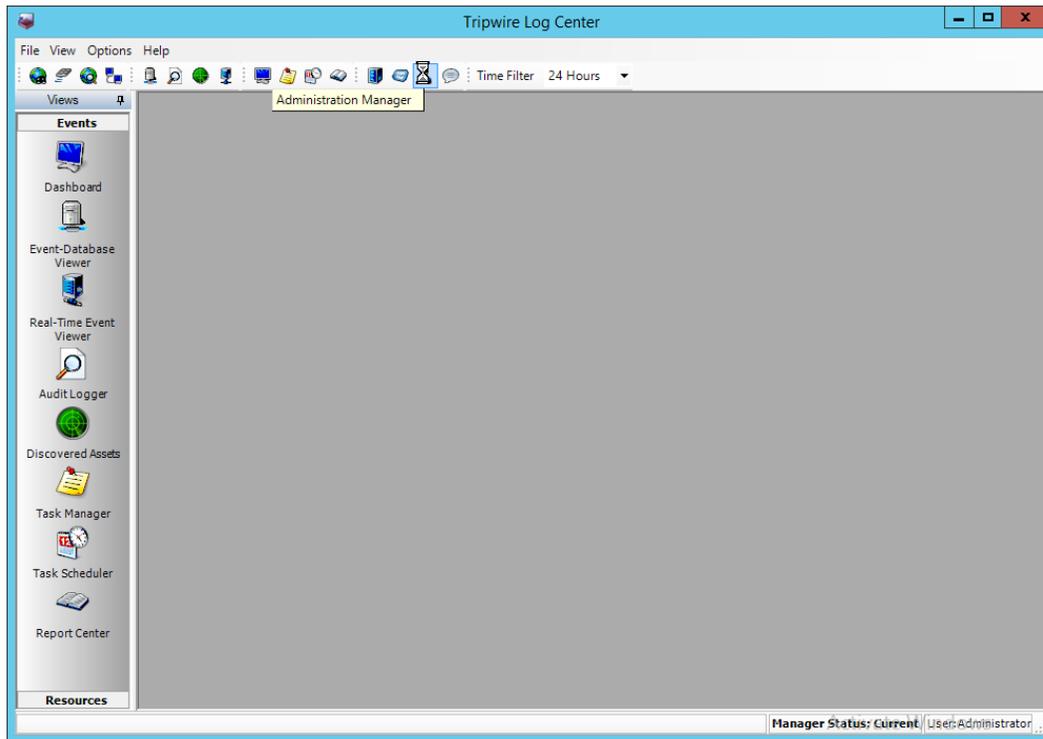
2660  
2661

5. Observe successful scan activity.

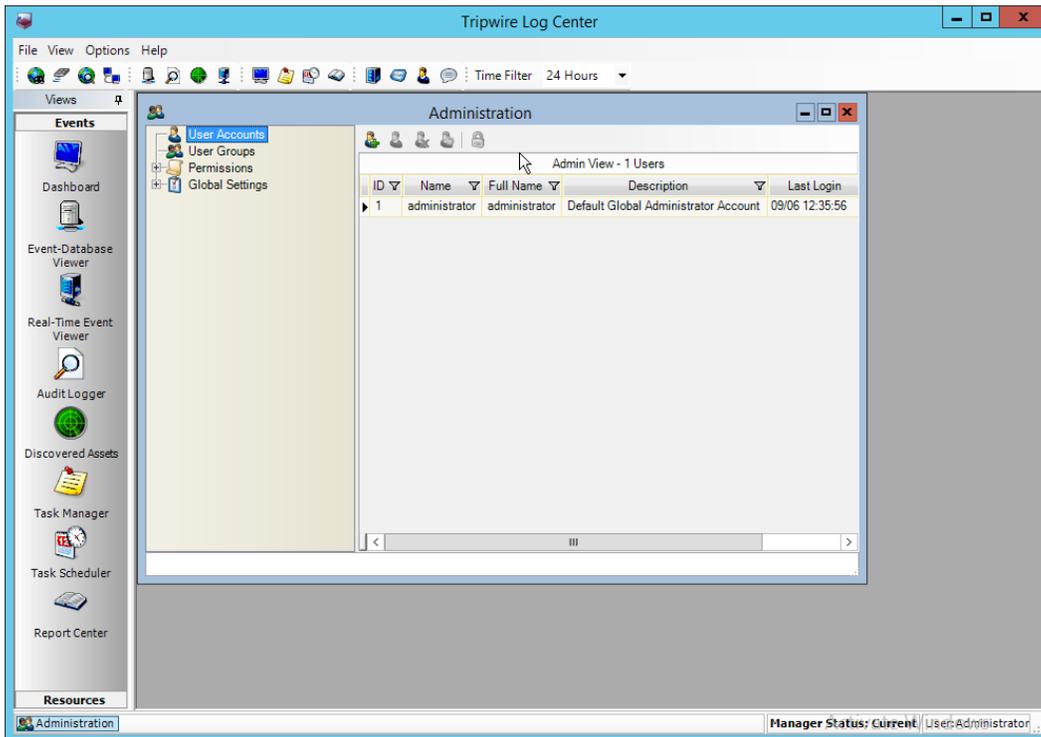


2662 **2.18 Integration: Tripwire Log Center and Tripwire Enterprise**

- 2663 1. Create a user account in **Tripwire Log Center** by logging into **Tripwire Log Center Console**.

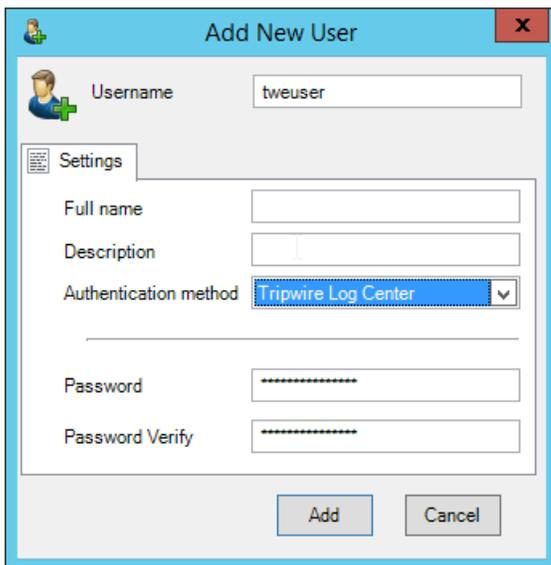


- 2664
- 2665 2. Click the **Administration Manager** button.
- 2666 3. Click **User Accounts**.



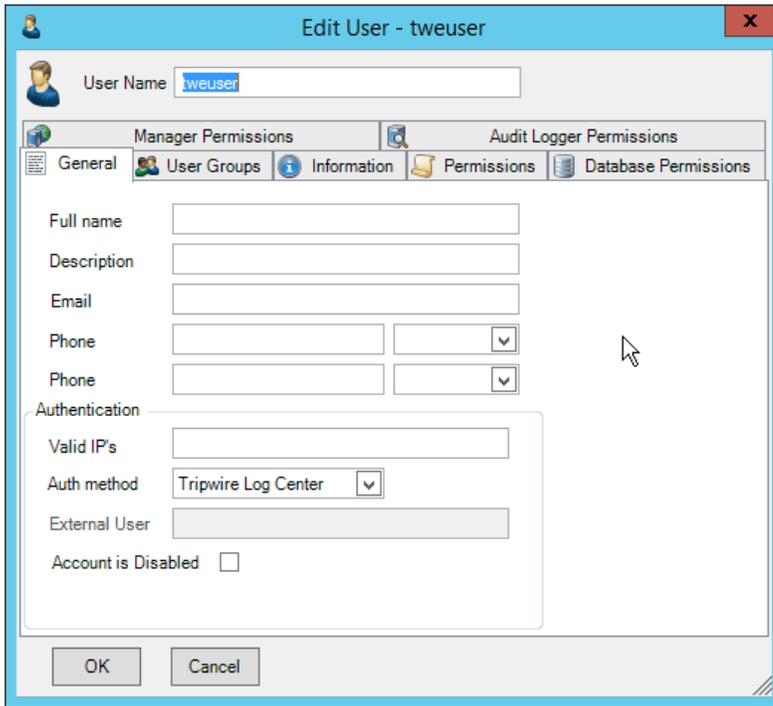
2667  
2668  
2669

4. Click the **Add** button.
5. Enter the details of the user.



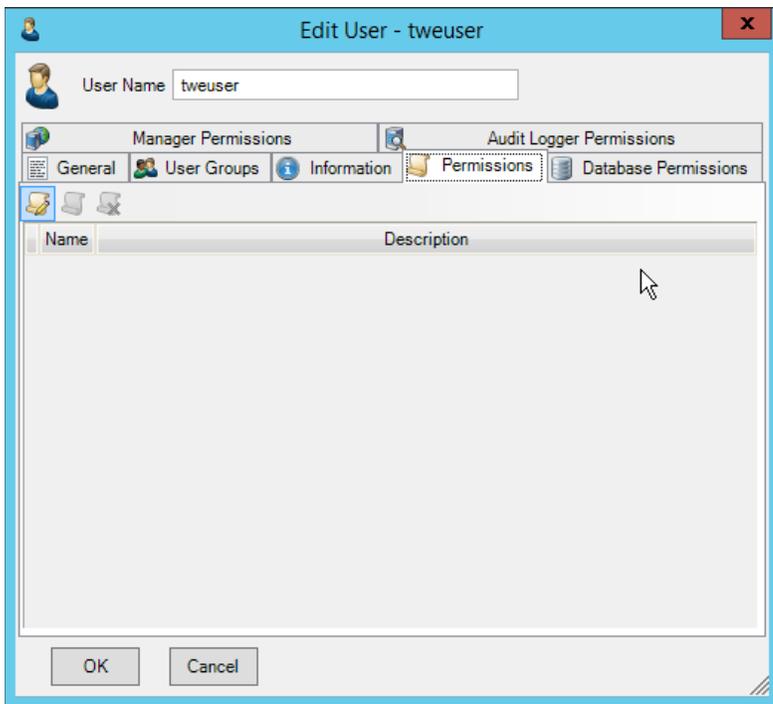
2670  
2671  
2672

6. Click **Add**.
7. Double-click the user account.



2673  
2674

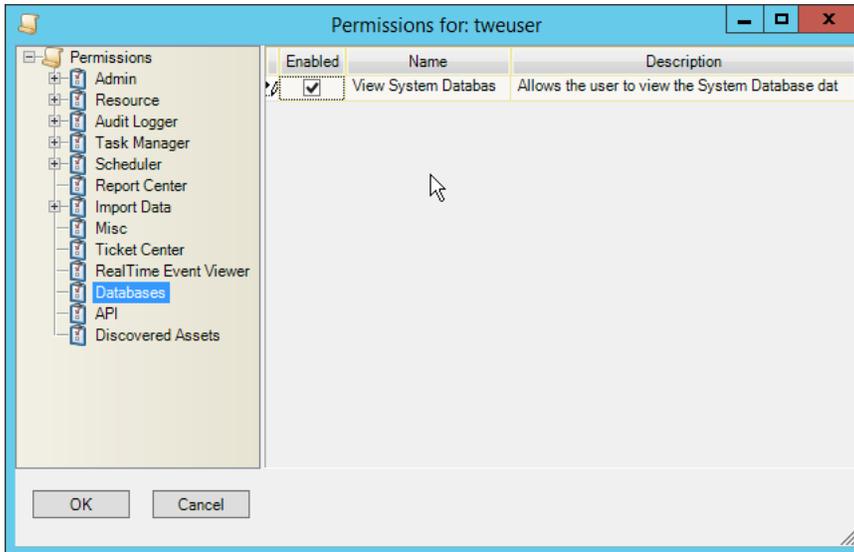
- 8. Click the **Permissions** tab.



2675  
2676

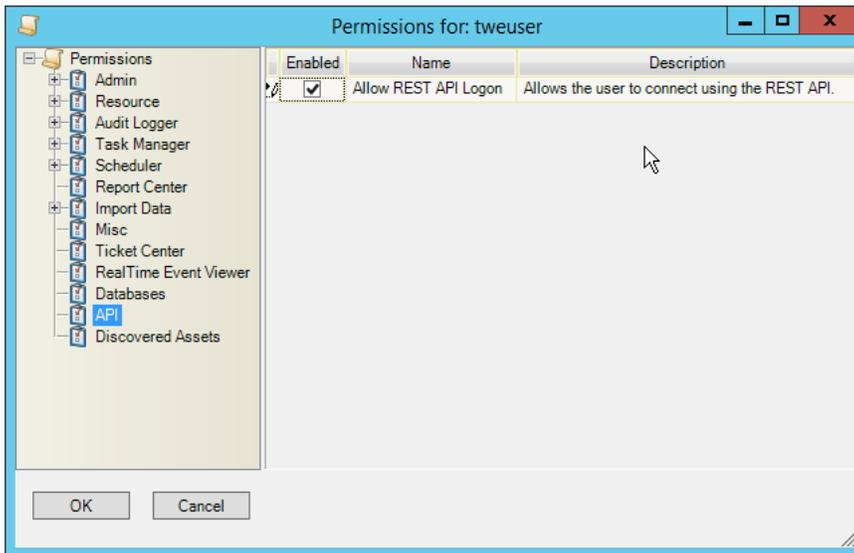
- 9. Click **Edit list of permissions**.

2677 10. Select **Databases**.



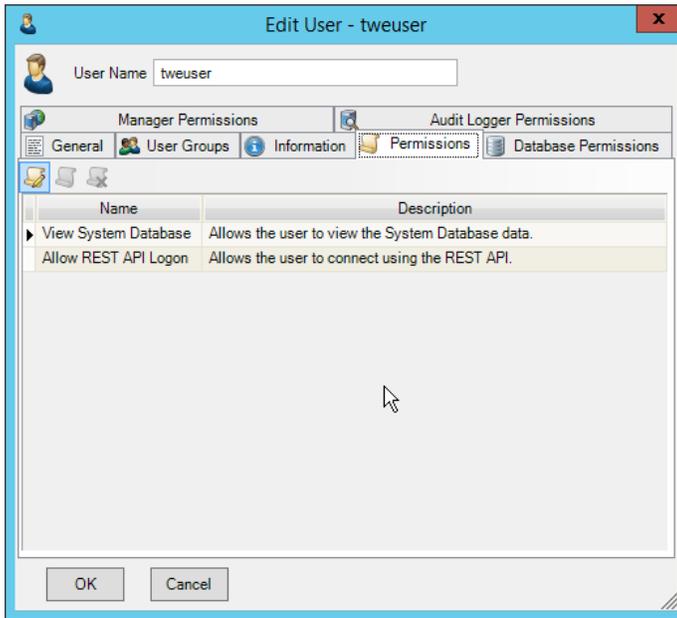
2678 11. Check the box next to **View System Database**.

2679 12. Select **API**.

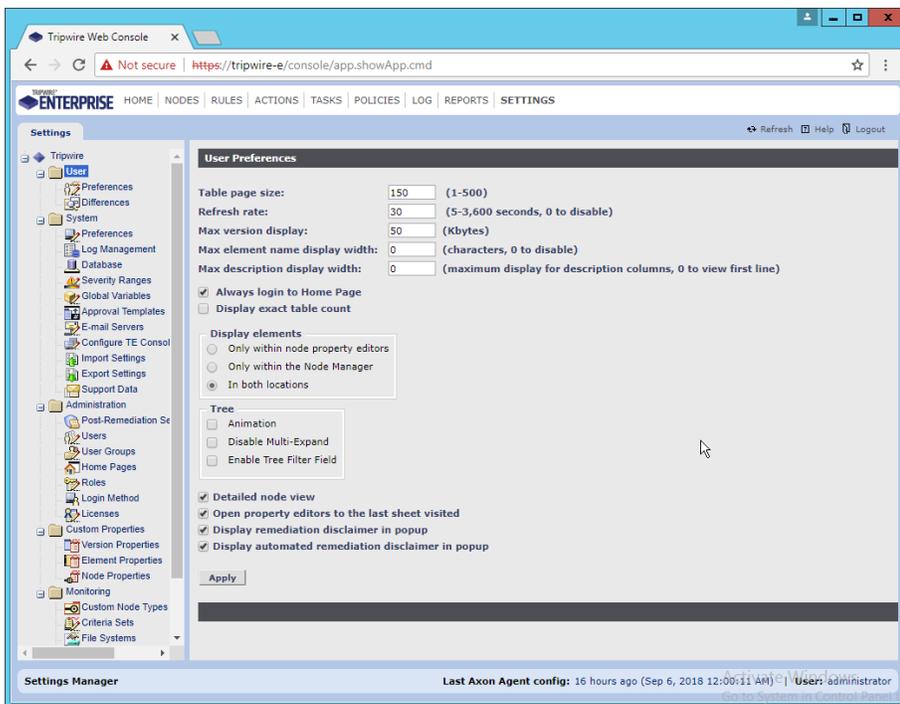


2681 13. Check the box next to **Allow REST API Logon**.

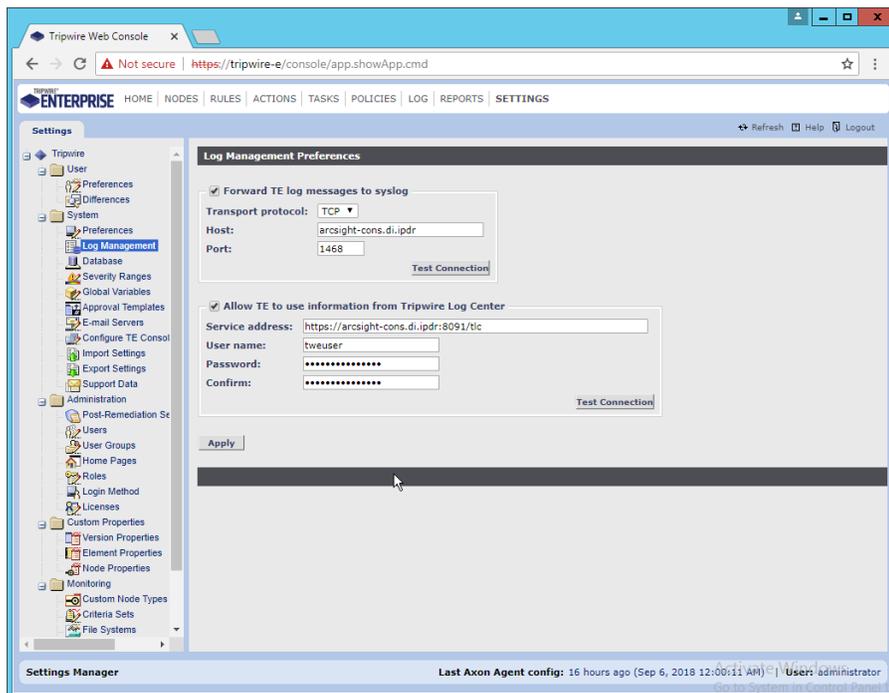
2682



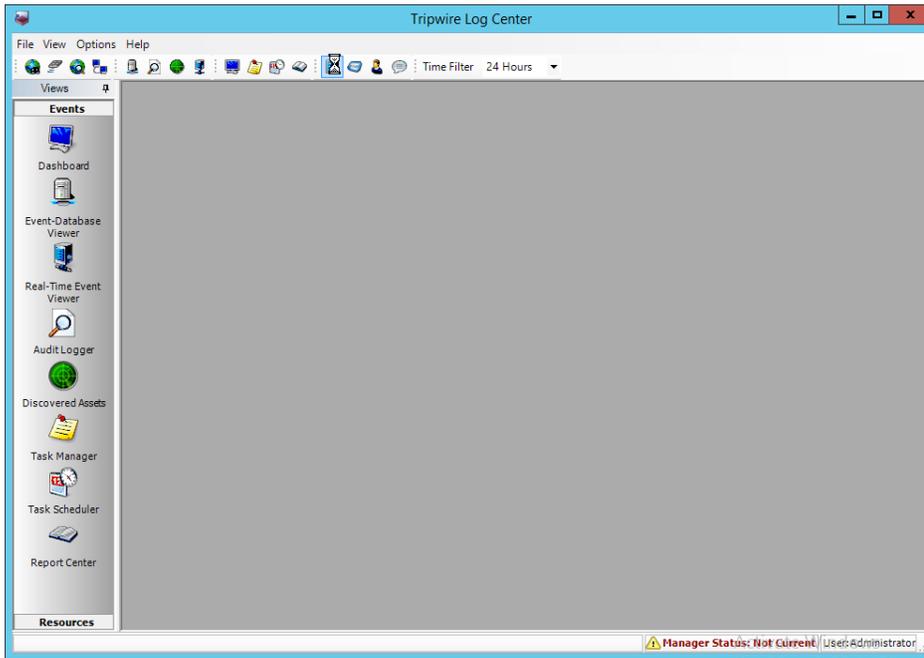
- 2683
- 2684 14. Click **OK**.
- 2685 15. Click **OK**.
- 2686 16. Log in to the **Tripwire Enterprise** web console.
- 2687 17. Click **Settings**.



- 2688 18. Go to **System > Log Management**.
- 2689 19. Check the box next to **Forward TE log messages to syslog**.
- 2690 20. Enter the **hostname** and **port** of the **Tripwire Log Center** server. The default port is 1468.
- 2691 21. Check the box next to **Allow TE to use information from Tripwire Log Center**.
- 2692 22. Enter the **service address** like this: <https://arcsight-cons.di.ipdr:8091/tlc>. Replace the **hostname**
- 2693 with the hostname of your **Tripwire Log Center** server.
- 2694 23. Enter the account information of the account just created for **Tripwire Log Center**.
- 2695 24. You can use **Test Connection** to verify that the connection is working.



- 2696
- 2697 25. Click **Apply** when finished.
- 2698 26. Go back to the **Tripwire Log Center Console**.



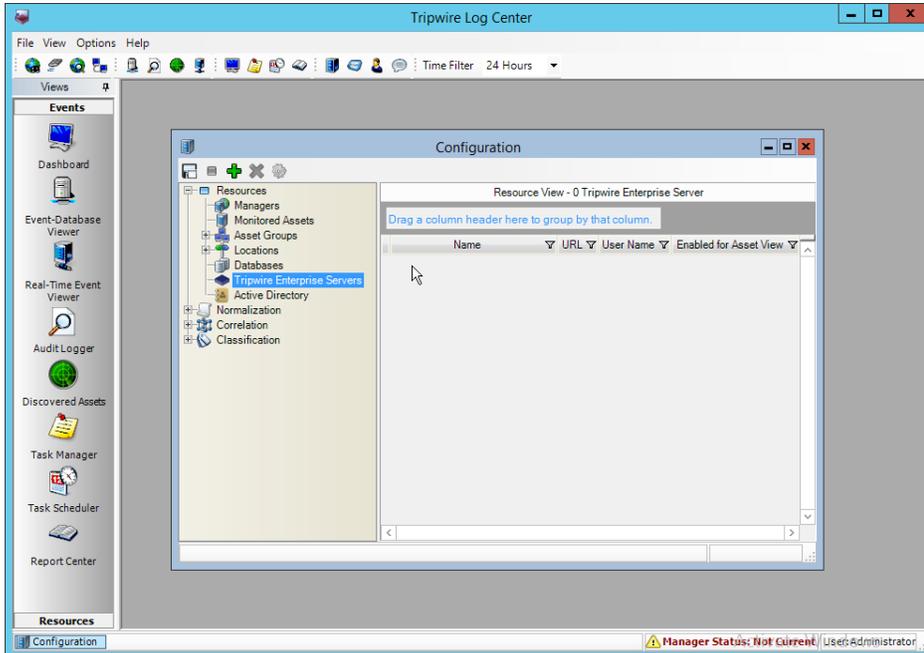
2699

2700

2701

27. Click **Configuration Manager**.

28. Click **Resources > Tripwire Enterprise Servers**.



2702

2703

2704

29. Click **Add**.

30. Enter a **name** for the server.

- 2705 31. Enter the **URL** of the Tripwire Enterprise server.
- 2706 32. Enter the **name** of a user account on the Tripwire Enterprise server. The account must have the
- 2707 following permissions: create, delete, link, load, update, view.

- 2708
- 2709 33. Click **Save**.

## 2710 2.19 Integration: Tripwire Log Center and Tripwire IP360

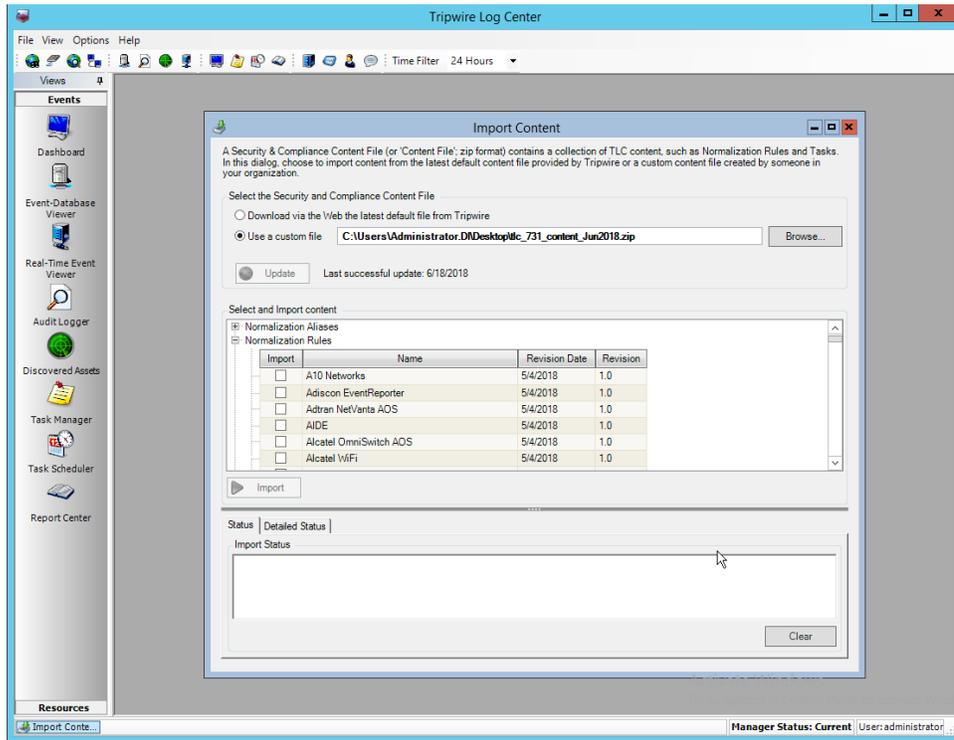
### 2711 2.19.1 Configure IP360 and Log Center

- 2712 1. On the **Tripwire Log Center Manager** machine, navigate to C:\Program Files\Tripwire\Tripwire
- 2713 Log Center Manager\Agent Services\config.
- 2714 2. Copy **bridge\_sample.properties** to **bridge.properties**.
- 2715 3. Modify the Pre-Shared Key to use a password by changing the following line (be sure to remove the “#”
- 2716 sign):
- 2717 `tw.cap.bridge.registrationPreSharedKey=newpasswordhere`
- 2718 4. Save the file.
- 2719 5. From the command line, run the following two commands:
- 2720 `> net stop TripwireBridge`
- 2721 `> net start TripwireBridge`
- 2722 6. On the Tripwire IP360 machine, from the command line, enter the following command to
- 2723 specify the hostname of the Tripwire Log Center (TLC) machine:
- 2724 `> tlc config bridge host update <hostname>`

- 2725 7. Enter the following command using the preshared key specified earlier:  
2726 > `tlc config bridge password update <password>`  
2727 8. Enter the following command to start the TLC service on the IP360 machine (this will use port  
2728 5670 on the TLC machine by default):  
2729 > `system service tlc enable`  
2730 9. Download the “Content update–June 2018” package from the **Tripwire Customer Center**.  
2731 10. Open the **Tripwire Log Center Console**.  
2732 11. Enter the **username** and **password**.

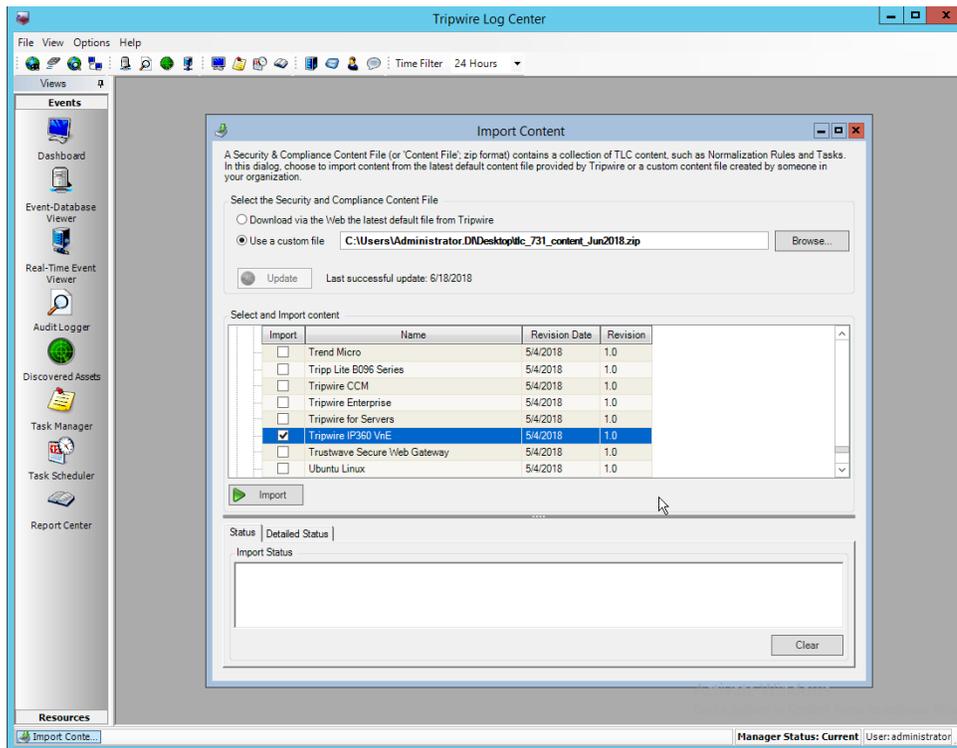


- 2733  
2734 12. Click **Login**.  
2735 13. Click **Options > Import TLC Content > Content**.  
2736 14. Select **Use a custom file**.  
2737 15. Click **Browse**, and locate the zip file downloaded from the **Tripwire Customer Center**.



2738  
2739  
2740

16. Expand the **Normalization Rules** section.
17. Check the box next to **Tripwire IP360 VnE**.



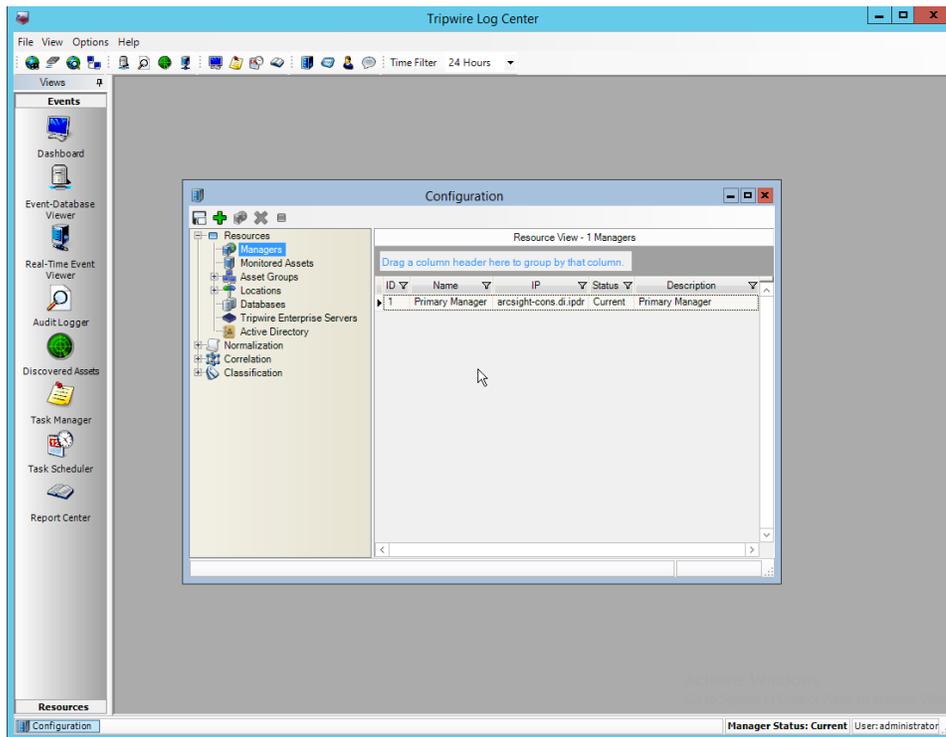
2741

2742

18. Click **Import**.2743 

## 2.19.2 Collect Tripwire IP360 Operational Logs

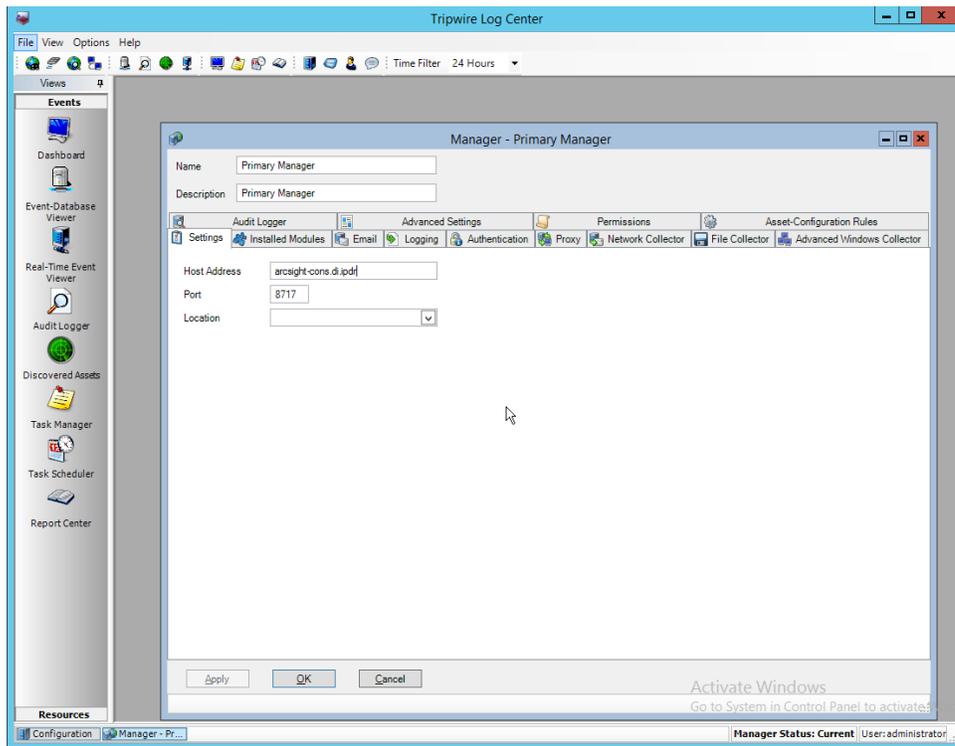
2744 1. Click **Configuration Manager**.2745 2. Click **Resources > Managers**.



2746

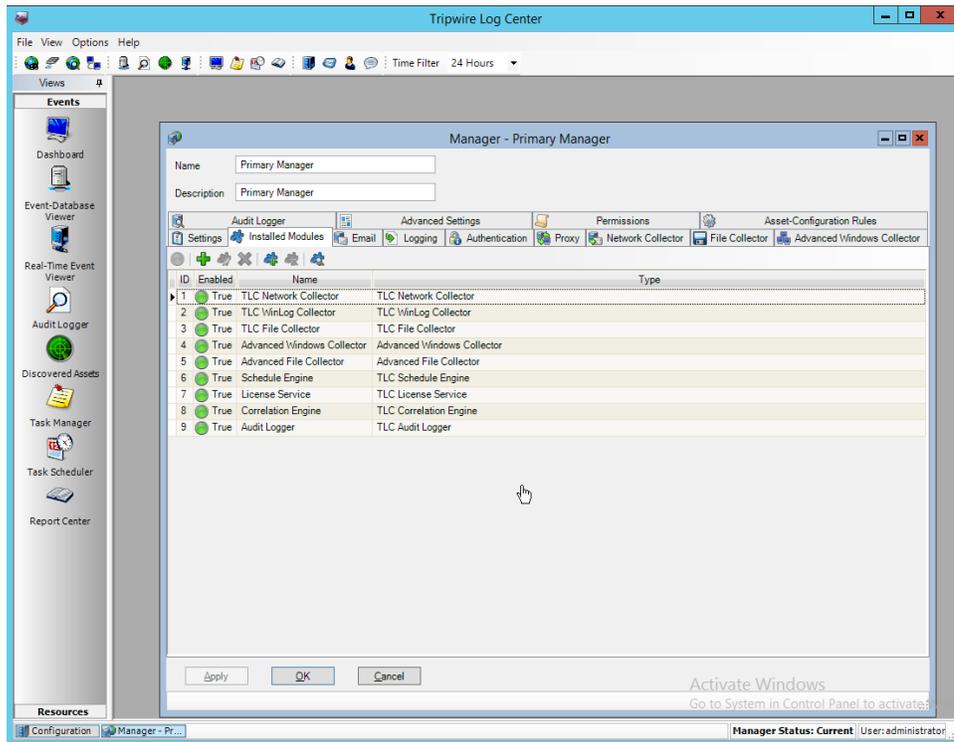
2747

3. Double-click the **Primary Manager**.



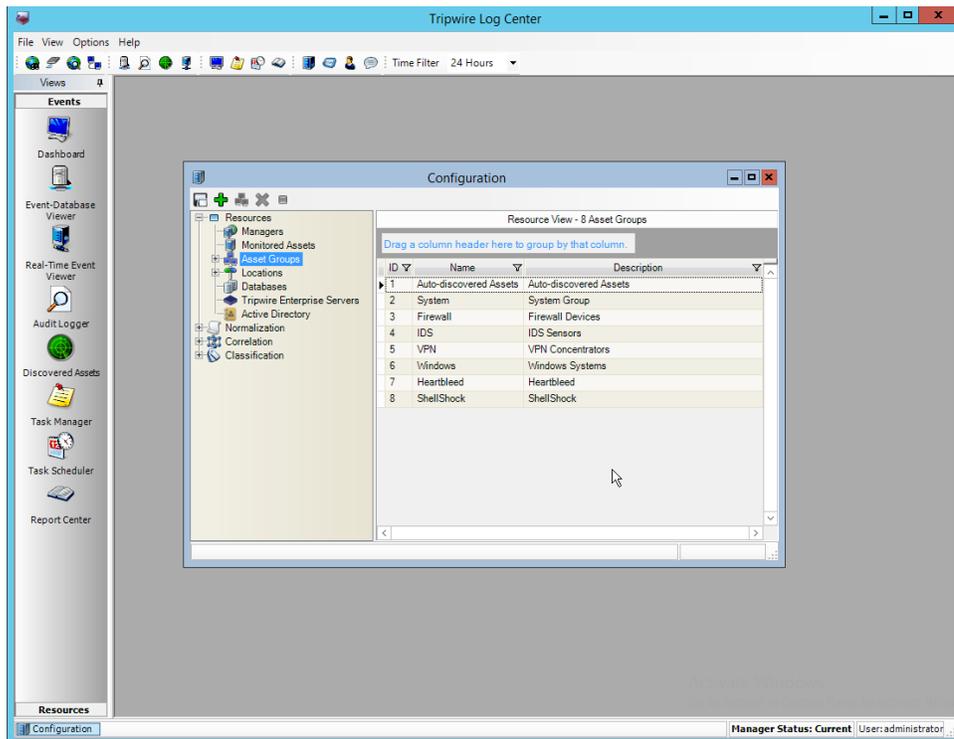
2748  
2749

4. Click the **Installed Modules** tab.



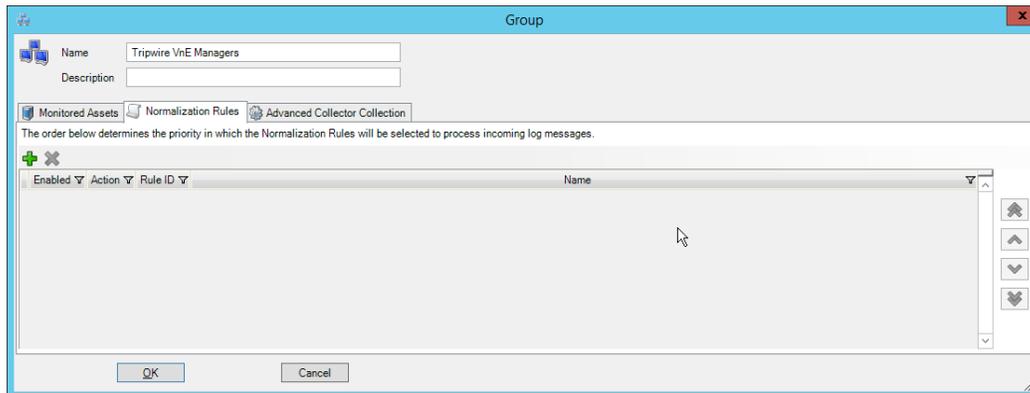
2750  
2751  
2752  
2753  
2754  
2755

5. Ensure that there is an **Advanced File Collector**. If not, click the **Create new module** button, and specify a **name**. Set the type to **Advanced File Collector**. If there is an **Advanced File Collector**, skip this step.
6. Click **OK**.
7. Click **Resources > Asset Groups**.



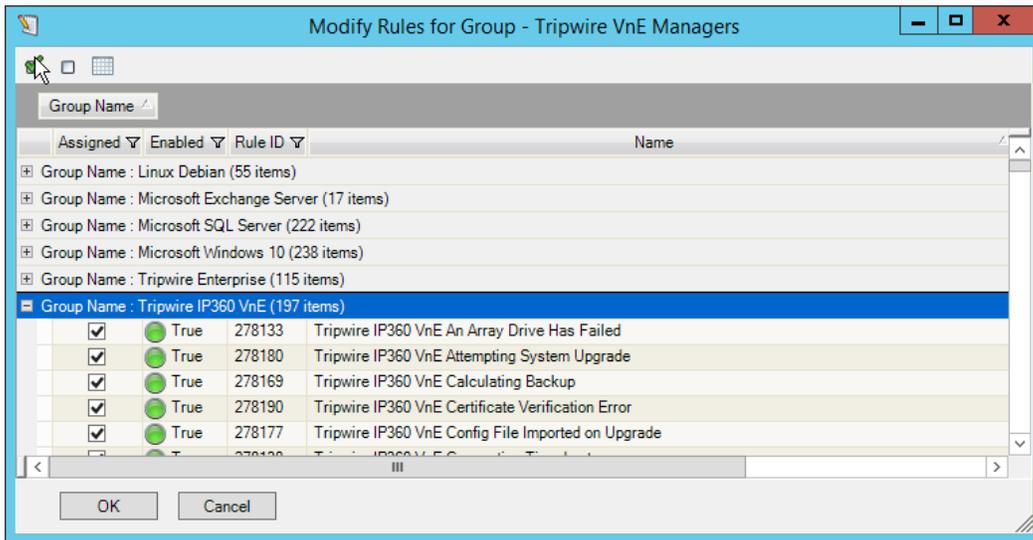
2756  
2757  
2758  
2759

8. Click **Add**.
9. Enter **Tripwire VnE Managers** in the **Name** field.
10. Click the **Normalization Rules** tab.



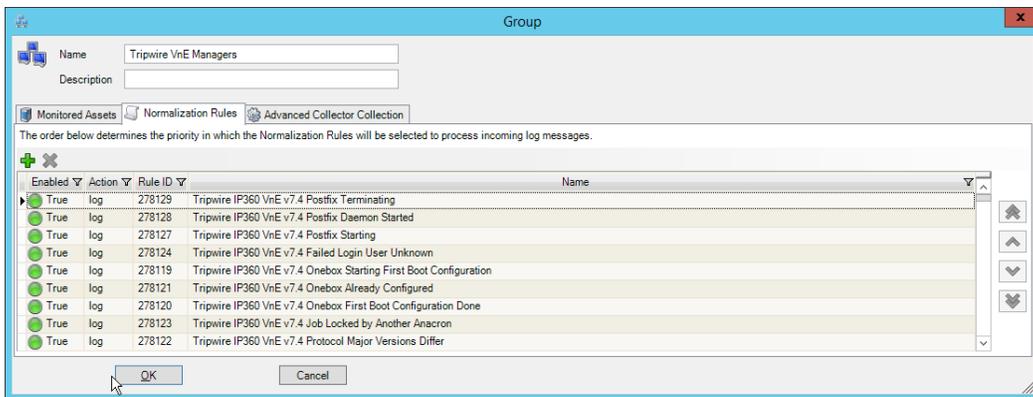
2760  
2761  
2762  
2763  
2764

11. Click **Add**.
12. Expand the **Tripwire IP360 VnE** group.
13. Click the **Check selected rows** button at the top to check the box next to everything in this section.



2765  
2766

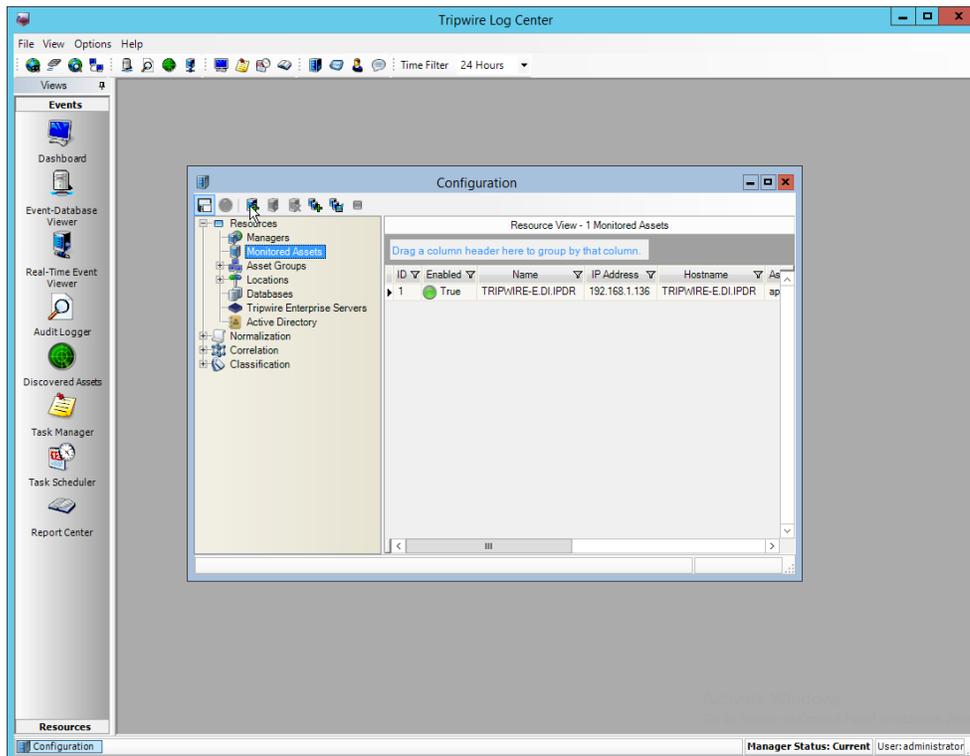
14. Click **OK**.



2767  
2768  
2769

15. Click **OK**.

16. Click **Resources > Monitored Assets**.



2770

2771

17. Click **Add Monitored Asset**.

2772

18. Enter a **name**.

2773

19. Select **Advanced File Collector** for **Collector**.

2774

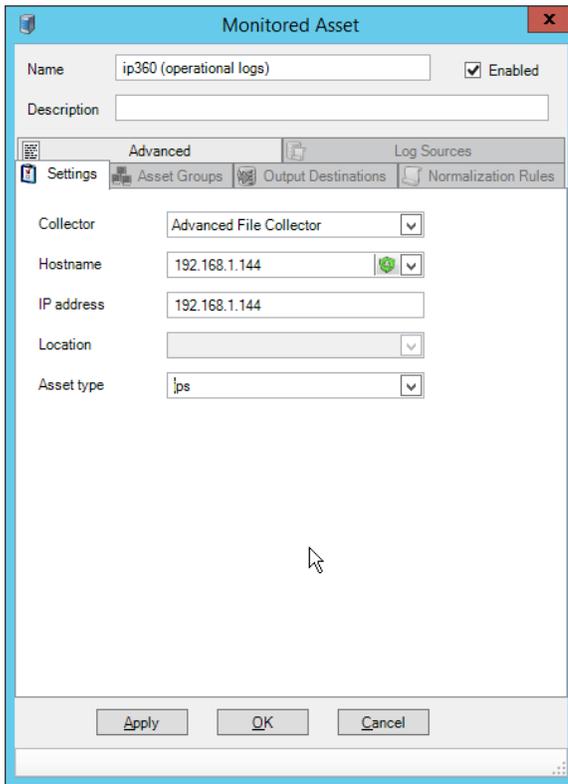
20. Select the IP360 server from the **Hostname** drop-down. It may appear as an IP address.

2775

21. Enter the **IP address** of the server.

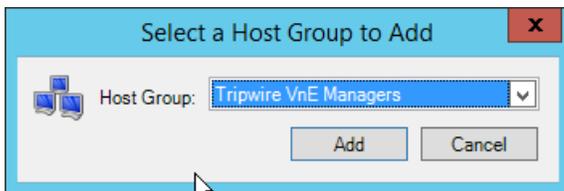
2776

22. Select **ips** for **Asset type**.



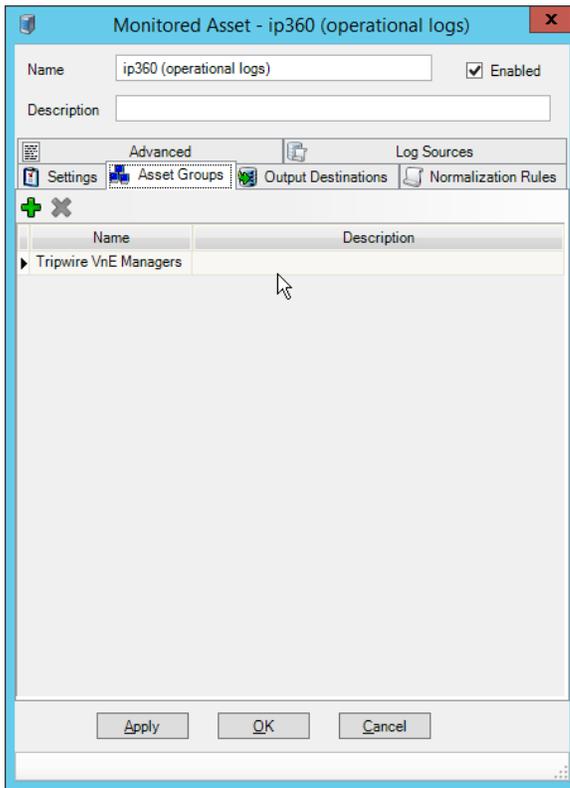
2777  
2778  
2779  
2780

- 23. Click the **Asset Groups** tab.
- 24. Click **Add**.
- 25. Select **Tripwire VnE Managers**.

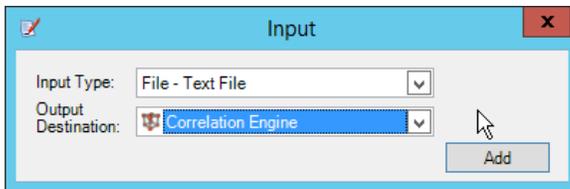


2781  
2782

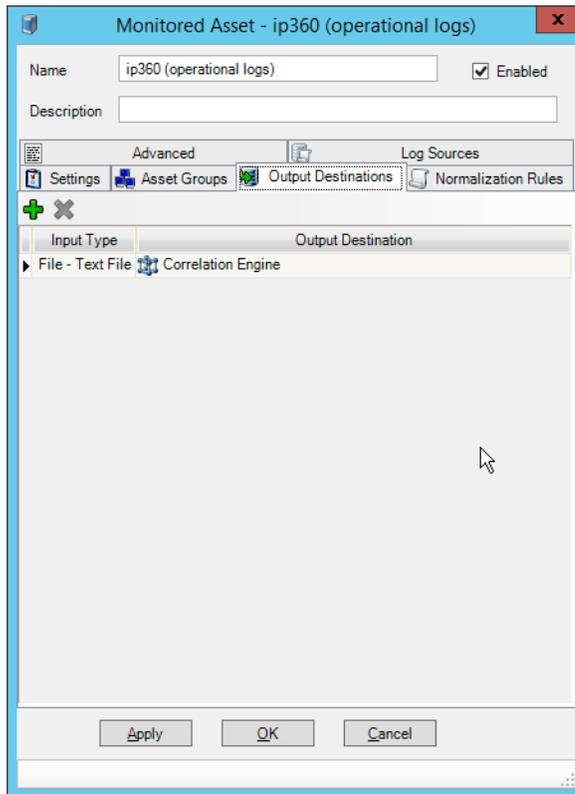
- 26. Click **Add**.



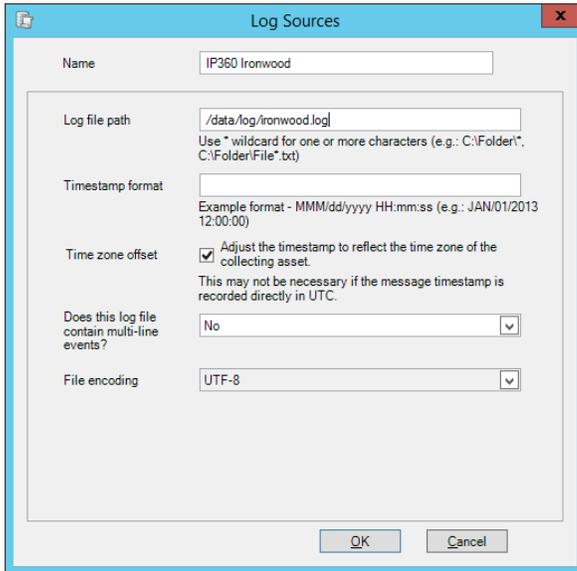
- 2783
- 2784 27. Click the **Output Destinations** tab.
- 2785 28. Click **Add**.
- 2786 29. Select **File–Text File** for **Input Type**.
- 2787 30. Select **Correlation Engine** for Output Destination.



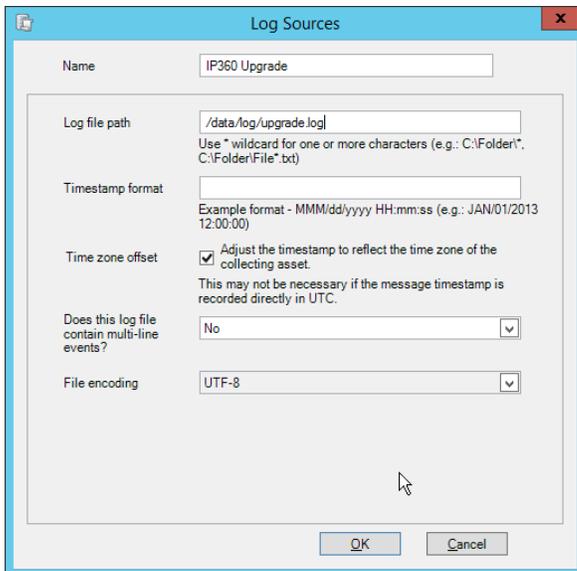
- 2788 31. Click **Add**.
- 2789



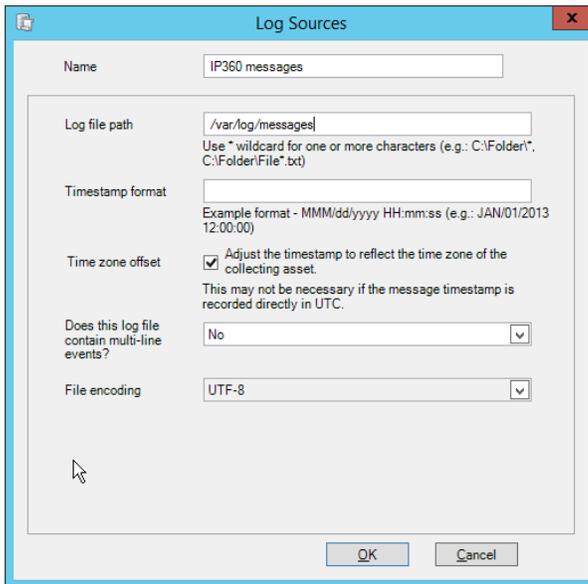
- 2790
- 2791 32. Click the **Log Sources** tab.
- 2792 33. Click **Add**.
- 2793 34. Enter a **name** for the log.
- 2794 35. Enter /data/log/ironwood.log for **Log file path**.



- 2795
- 2796 36. Click **OK**.
- 2797 37. Click **Add**.
- 2798 38. Enter a **name** for the log.
- 2799 39. Enter /data/log/upgrade.log for **Log file path**.

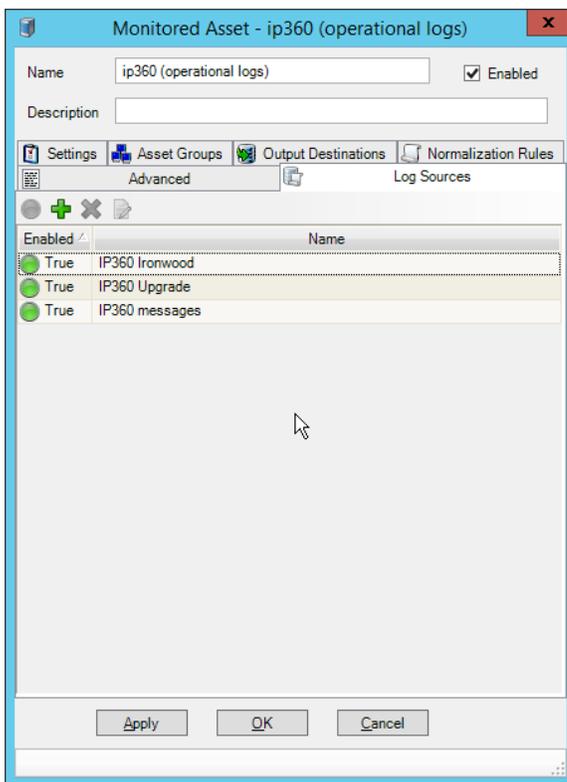


- 2800
- 2801 40. Click **OK**.
- 2802 41. Click **Add**.
- 2803 42. Enter a **name** for the log.
- 2804 43. Enter /var/log/messages for **Log file path**.



2805  
2806

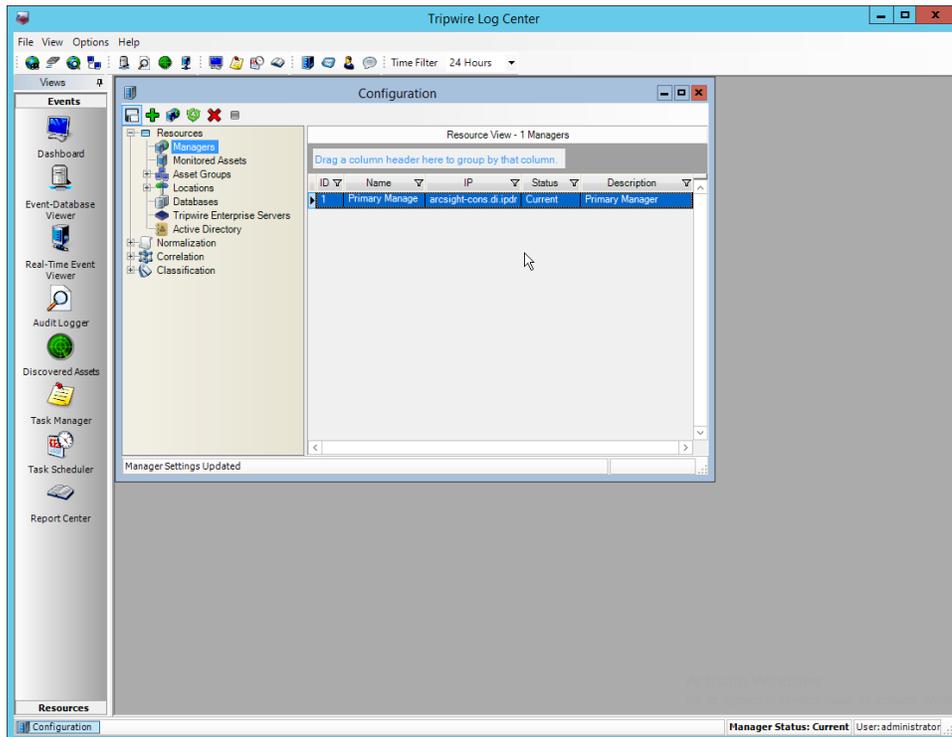
44. Click **OK**.



2807  
2808  
2809

45. Click **OK**.

46. Click **Resources > Managers**.



2810

2811

47. Select the **Primary Manager** and click **Push Updates to Manager**.

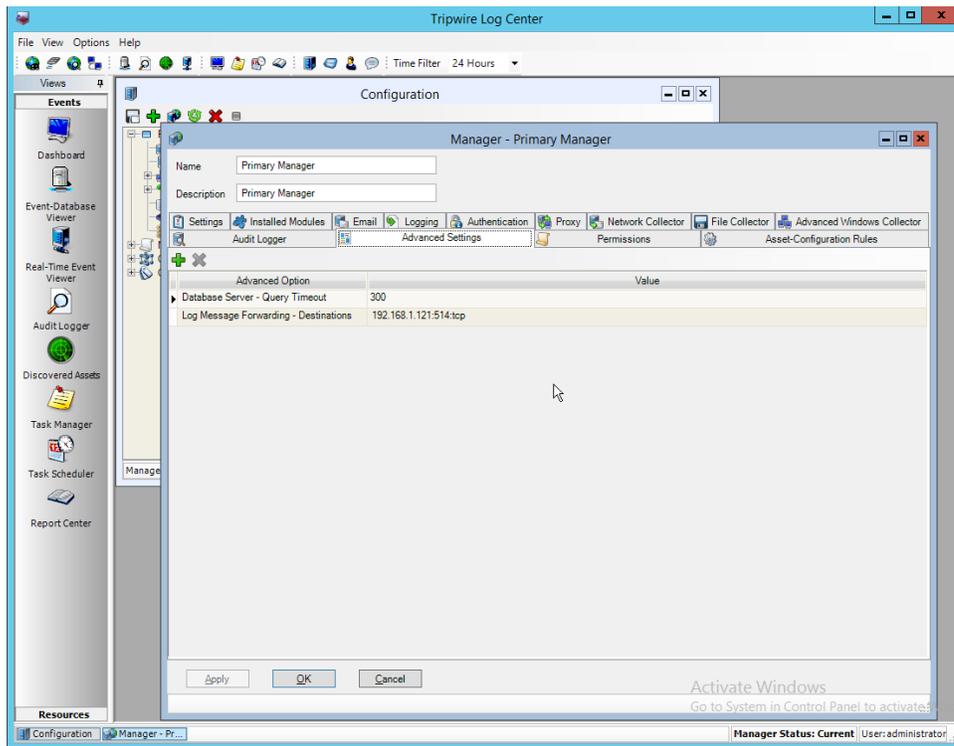
### 2812 2.19.3 Configure Tripwire IP360 Scan Results Forwarding

2813 1. Click **Configuration Manager**.

2814 2. Click **Resources > Manager**.

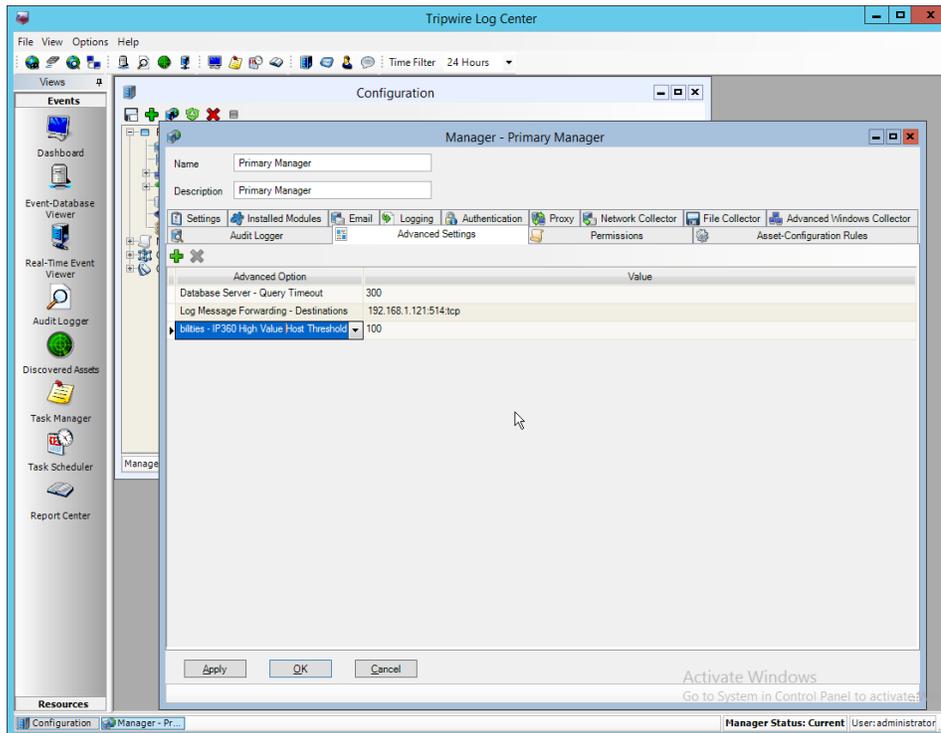
2815 3. Double-click the **Primary Manager**.

2816 4. Click the **Advanced Settings** tab.



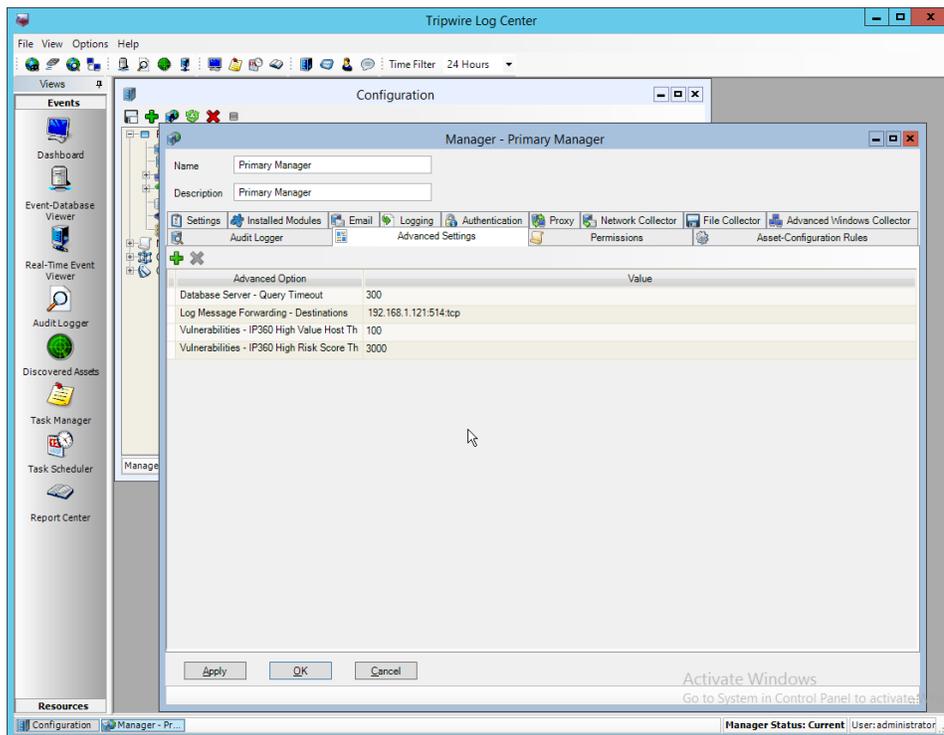
2817  
2818  
2819  
2820  
2821  
2822  
2823

5. Click **Add**.
6. Select **Vulnerabilities–IP360 High Value Host Threshold** for the **Advanced Option**.
7. Enter a number between 0 and 999,999,999 for the **Value**. This number corresponds to the priority level of the host system being scanned. The value entered will be the minimum value for a host machine to be considered high priority. Half of this value will be the minimum value for a host machine to be considered medium priority.



2824  
2825  
2826  
2827  
2828  
2829  
2830

8. Click **Add**.
9. Select **Vulnerabilities—IP360 High Risk Score Threshold** for the **Advanced Option**.
10. Enter a number between 0 and 999,999,999 for the **Value**. This number corresponds to the risk level of a vulnerability event. The value entered will be the minimum value for an event to be considered high risk. Half of this value will be the minimum value for an event to be considered medium risk.



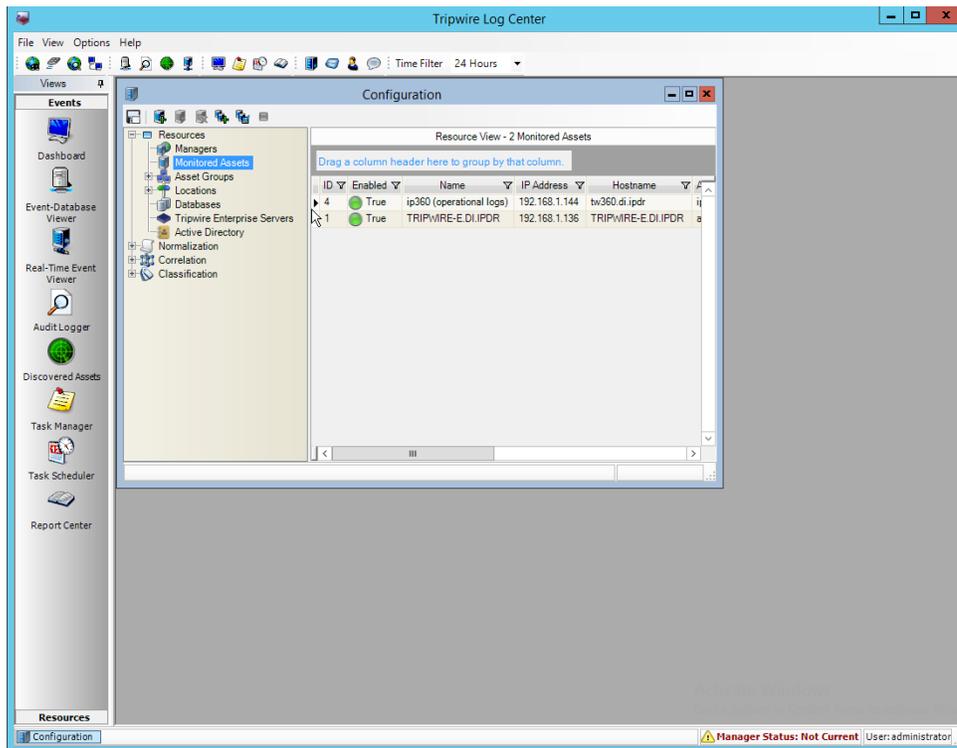
2831

2832

2833

2834

11. Click **Apply**.12. Click **OK**.13. Click **Resources > Monitored Assets**.



2835

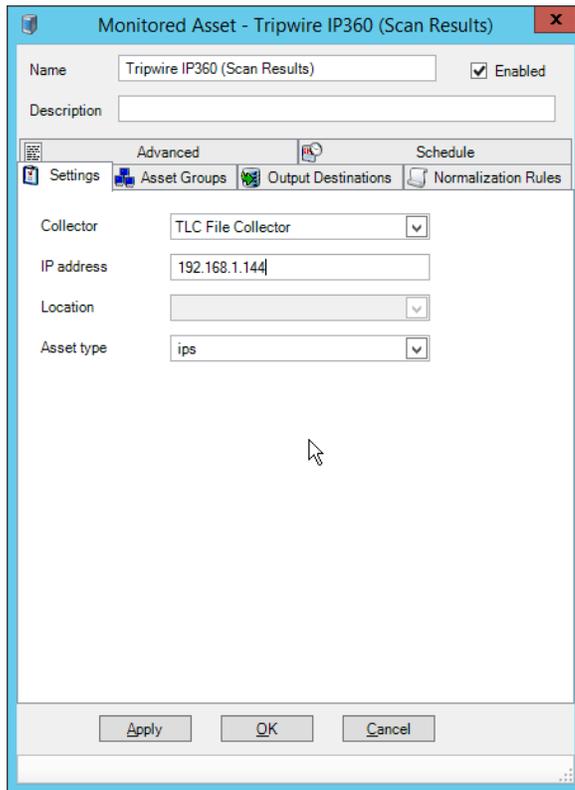
2836

2837

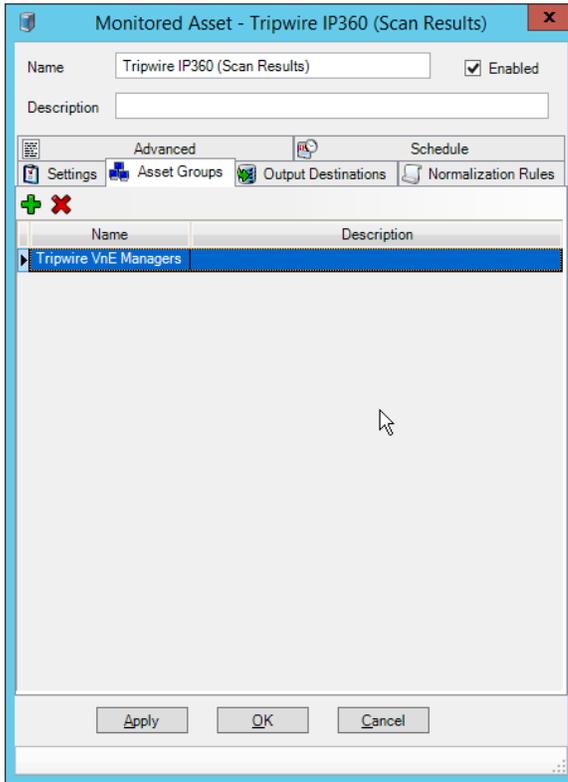
2838

2839

14. Click **Add Asset**.15. Select **TLC File Collector** for **Collector**.16. Enter the **IP address** of the **IP360** machine.17. Select **ips** for **Asset type**.

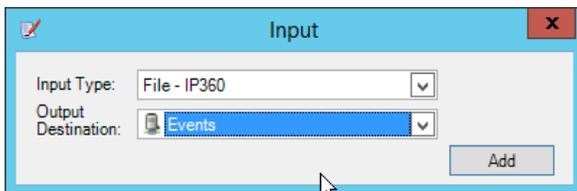


- 2840
- 2841 18. Click the **Asset Groups** tab.
- 2842 19. Click **Add**.
- 2843 20. Select **Tripwire VnE Managers** for **Host Group**.
- 2844 21. Click **Add**.



2845  
2846  
2847  
2848

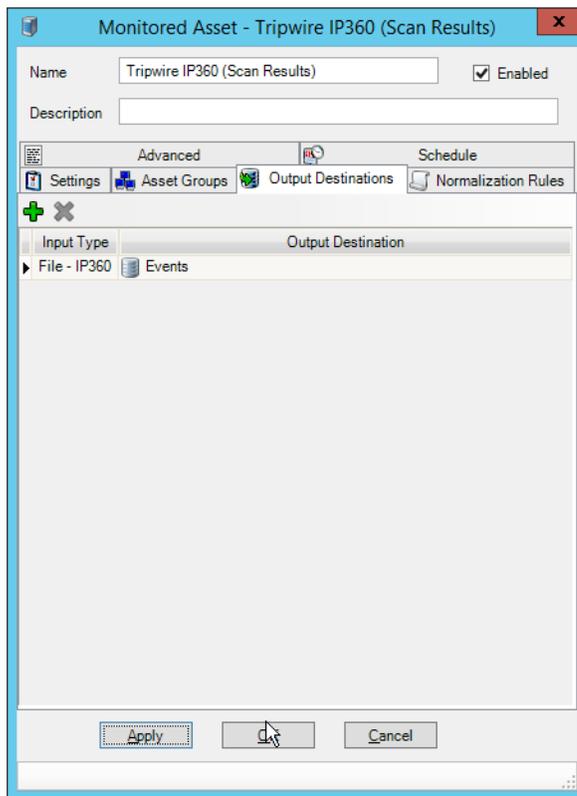
- 22. Click the **Output Destinations** tab.
- 23. Select **File-IP360** for **Input Type**.
- 24. Select **Events** for **Output Destination**.



2849  
2850

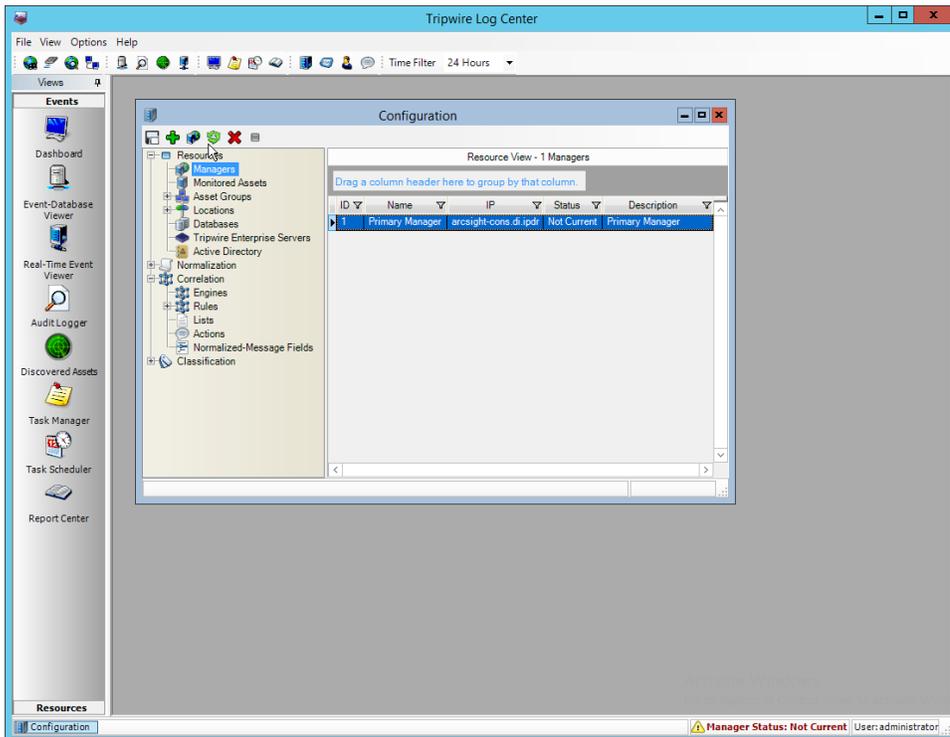
- 25. Click **Add**.

DRAFT



2851  
2852  
2853  
2854

26. Click **OK**.
27. Click **Resources > Managers**.
28. Select the **Primary Manager**.



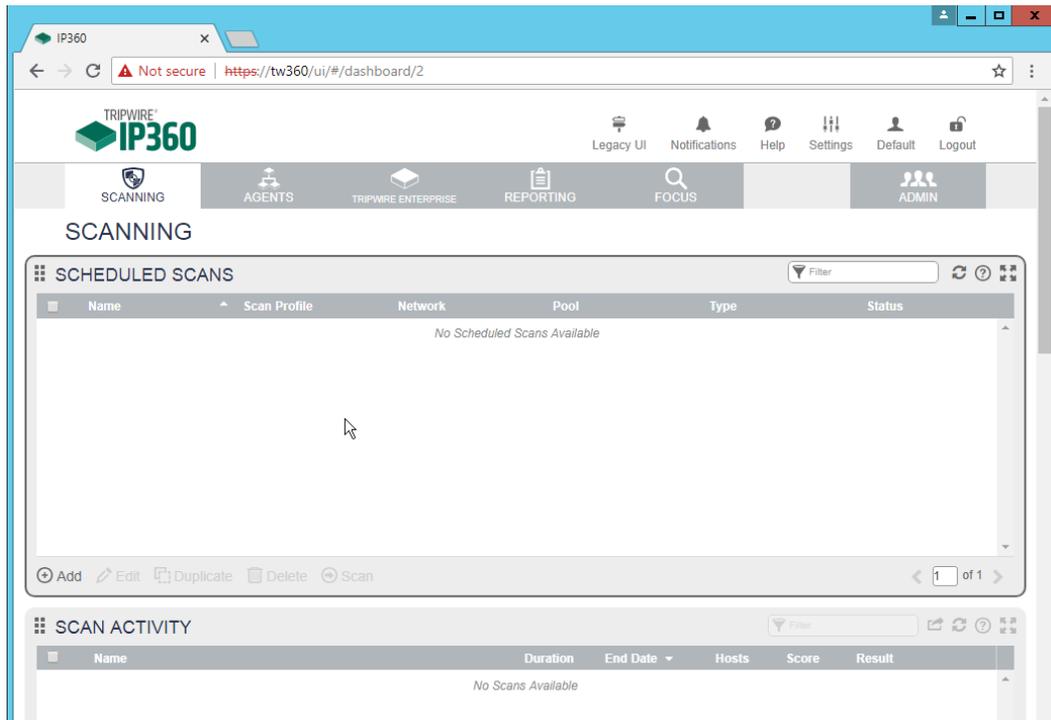
2855

2856

2857

29. Click **Push Update to Manager**.

30. Log in to the **Tripwire IP360 Web Console**.

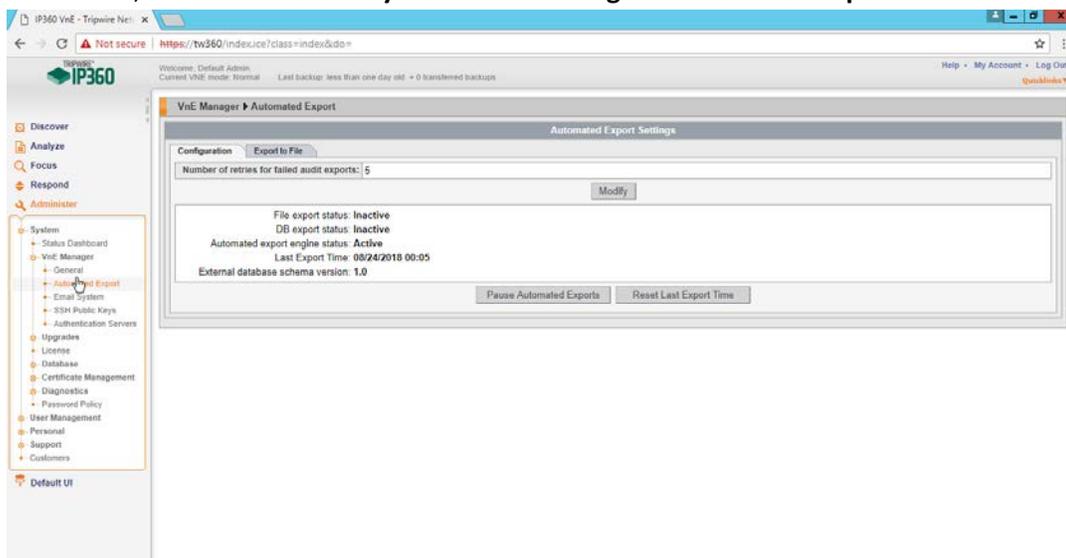


2858

2859

2860

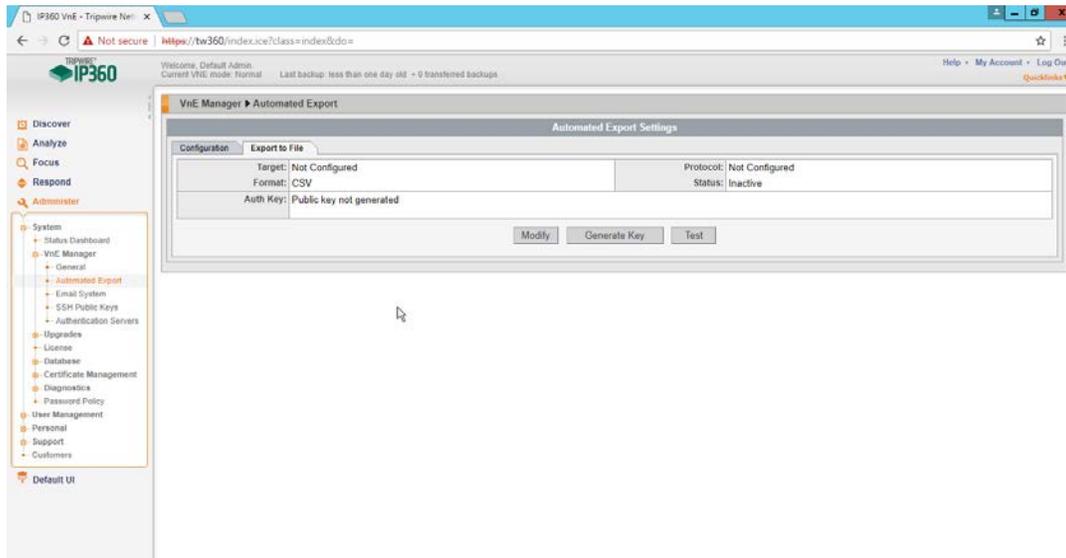
- 31. Click **Legacy UI** at the top.
- 32. On the left, click **Administer > System > VnE Manager > Automated Export**.



2861

2862

- 33. Click the **Export to File** tab.



2863

2864

34. Click **Modify**.

2865

35. Enter the **username** of a TLC user account for **User**.

2866

36. Enter the **IP address** of the TLC Manager for **Host**.

2867

37. Enter **"/"** for the **directory**.

2868

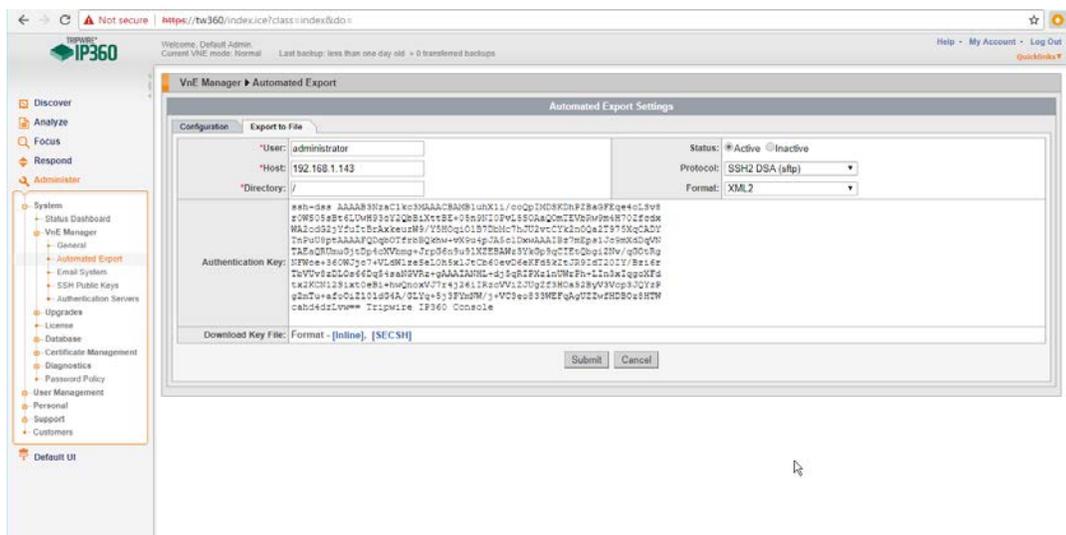
38. Select **Active**.

2869

39. Select **SSH2 DSA (sftp)** for **Protocol**.

2870

40. Select **XML2** for **Format**.



2871

41. Click **Submit**.

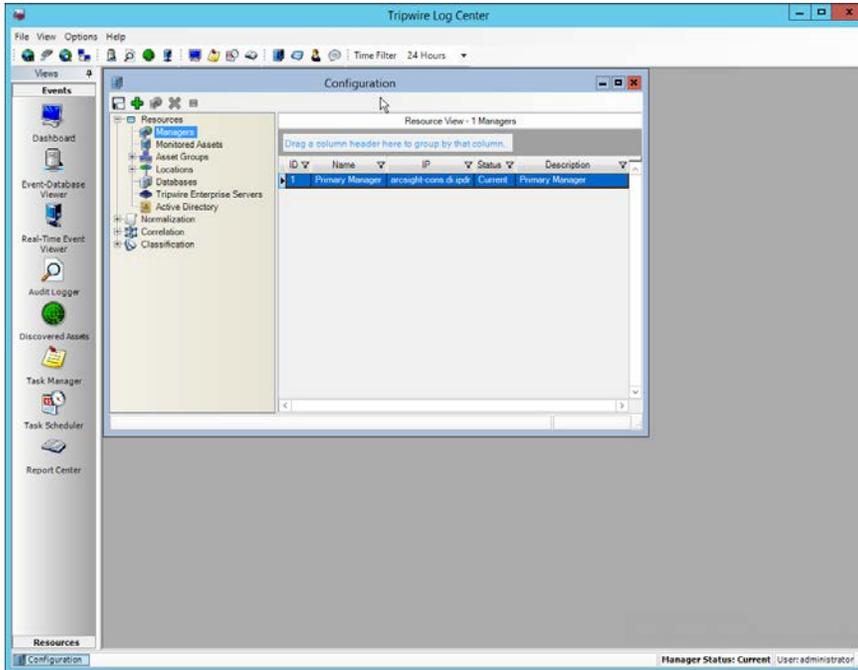
2872

42. Download the generated key by clicking **[Inline]**.

2873

2874 43. In **TLC Console**, click **Configuration Manager**.

2875 44. Click **Resources > Managers**.



2876 45. Double-click the **Primary Manager**.

2878 46. Click the **File Collector** tab.

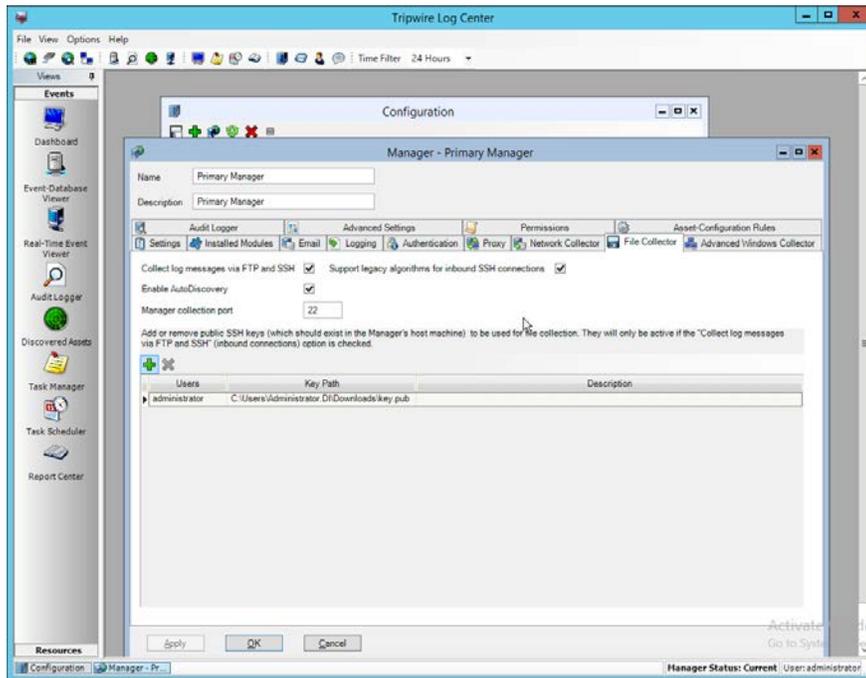
2879 47. Ensure that the **Collect log messages via FTP and SSH** option is enabled.

2880 48. Enter **22** for the **port**. (Note: The *IP360 Integration Guide* says to use a different port, but the  
2881 IP360 system appears to be unable to use a port other than 22.)

2882 49. Click **Add**.

2883 50. Under **Users**, select the user for whom the key was generated.

2884 51. Under **Key Path**, enter the path to the downloaded key.



2885

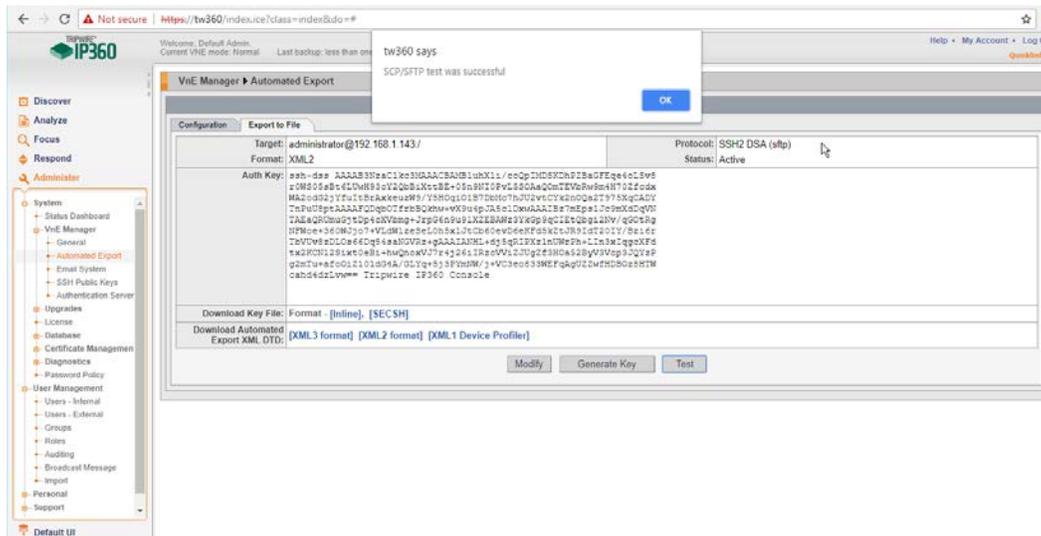
2886

2887

2888

2889

52. Click **OK**.
53. Select the **Primary Manager**.
54. Click **Push Updates to Manager**.
55. On the **IP360** web console, click **Test** to ensure that the connection is successful.

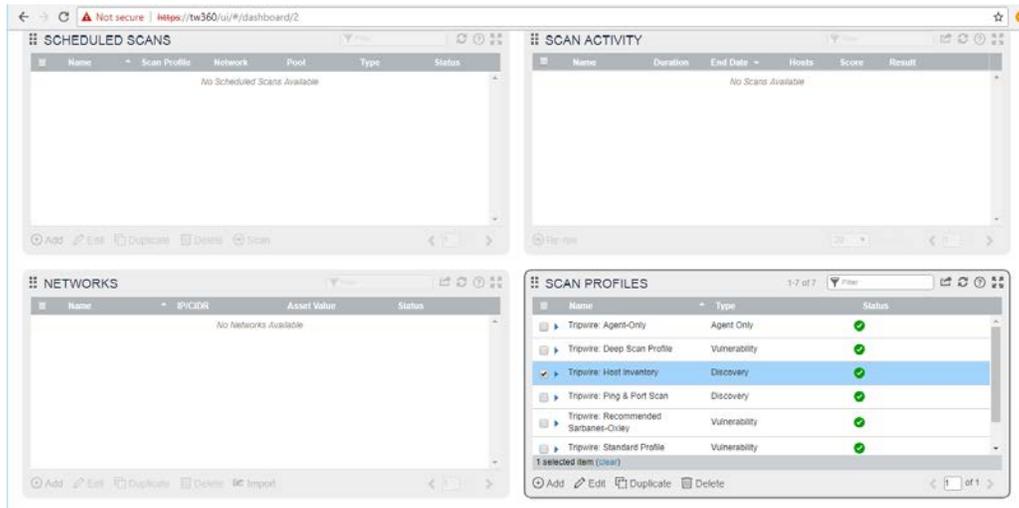


2890

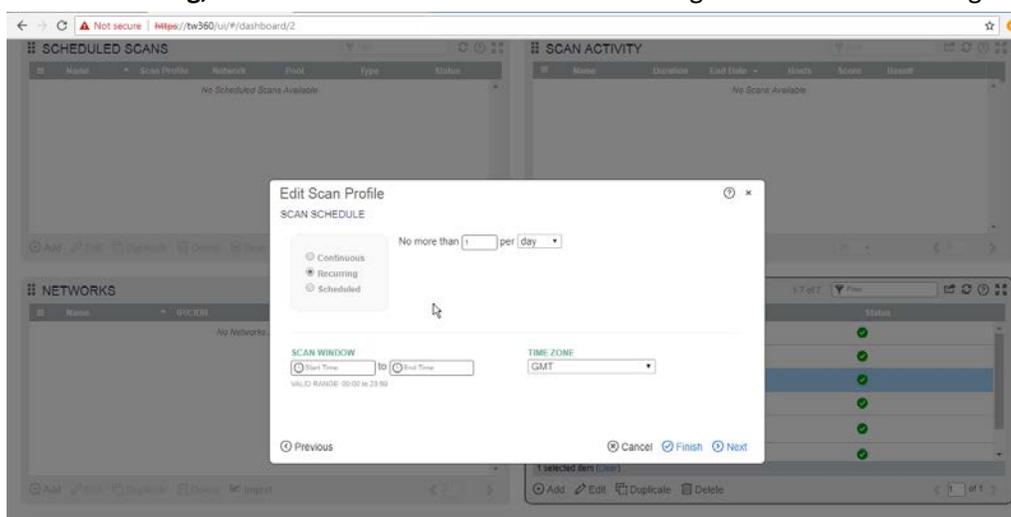
2891

2892

56. Any recurring scans will now forward the scan results to **Tripwire Log Center**. To ensure that a scan is recurring, select a scan in **Scan Profiles** on the main dashboard of the **IP360** web console.



- 2893
- 2894 57. Click **Edit**.
- 2895 58. Click **Next** until the **Scan Schedule** page.
- 2896 59. Select **Recurring**, and set a schedule for the scan according to the needs of the organization.



- 2897
- 2898 60. Click **Finish**.

## 2899 2.20 Integration: Tripwire Enterprise and Backups

- 2900 This section details how to back up **Tripwire Enterprise** configuration data.
- 2901 To back up **Tripwire Enterprise** integrity information, refer to the database vendor’s documentation for
- 2902 backing up data.

## 2903 2.20.1 Export Configuration from Tripwire Enterprise

- 2904 1. On the Tripwire Enterprise server, navigate to C:\Program Files\Tripwire\TE\Server\bin.
- 2905 2. Run the following command to stop **Tripwire Services**.  
2906 > twservices stop
- 2907 3. Run the following command to export the configuration files to a backup (replace config.bak  
2908 with the desired name of the backup).  
2909 > tefool backup config.bak
- 2910 4. Run the following command to restart **Tripwire Services**.  
2911 > twservices start

## 2912 2.20.2 Back Up the Tripwire Enterprise Configuration

2913 The configuration backup will be stored in the file specified in step 3 of the previous section. To back  
2914 this up to the enterprise backup server through a **Duplicati** client, see the documentation in Section  
2915 2.8.4 for how to set up a **Duplicati** instance on the **Tripwire Enterprise** server, and then simply select  
2916 the configuration file.

## 2917 2.21 Integration: Cisco ISE and CryptoniteNXT

2918 This section details an integration between **Cisco ISE** and **CryptoniteNXT**, allowing ISE to dictate the  
2919 Cryptonite registration process based on the posture of the client machine. Please see the  
2920 *CryptoniteNXT Generic RADIUS Integration Guide* for more details about the integration.

### 2921 2.21.1 Requirements for Integrating Cisco ISE and CryptoniteNXT

2922 As described in the ISE installation section, ISE requires RADIUS to be configured to perform posture. As  
2923 such, this guide assumes the use of some sort of switch to provide RADIUS functionality.

2924 CryptoniteNXT requires the switch to use L2 technologies for the RADIUS server, which means a captive  
2925 portal will not work for this scenario. The feasibility of this depends on your networking setup.

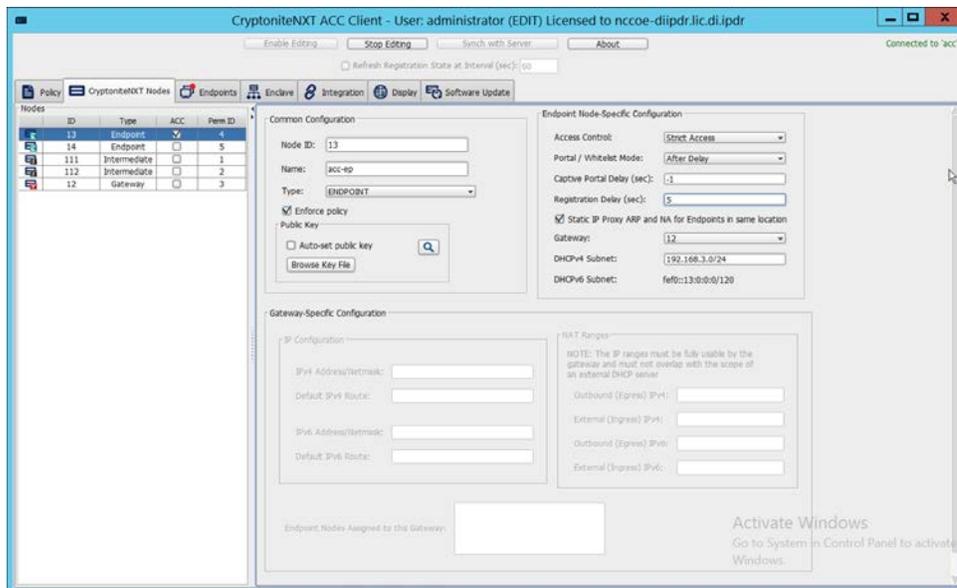
2926 This integration requires the following:

- 2927 1. The switch is bridged to CryptoniteNXT.
- 2928 2. Cryptonite is configured to accept RADIUS packets from the switch (detailed below).
- 2929 3. Clients on the switch's Local Area Network (LAN) authenticate to the switch via 802.1x (see your  
2930 switch's documentation).

- 2931 4. The switch is configured to accept CoA packets from ISE (see ISE installation).  
 2932 5. The switch sends RADIUS accounting and authentication packets to Cisco ISE (see ISE  
 2933 installation).  
 2934 6. ISE sends an authentication response to the switch and then later uses CoA to modify the  
 2935 authorization based on posture (see ISE installation).  
 2936 7. If the authorization is successful, the switch tells the client and forwards the accounting packets  
 2937 to the CryptoniteNXT ACC node (see your switch's documentation).

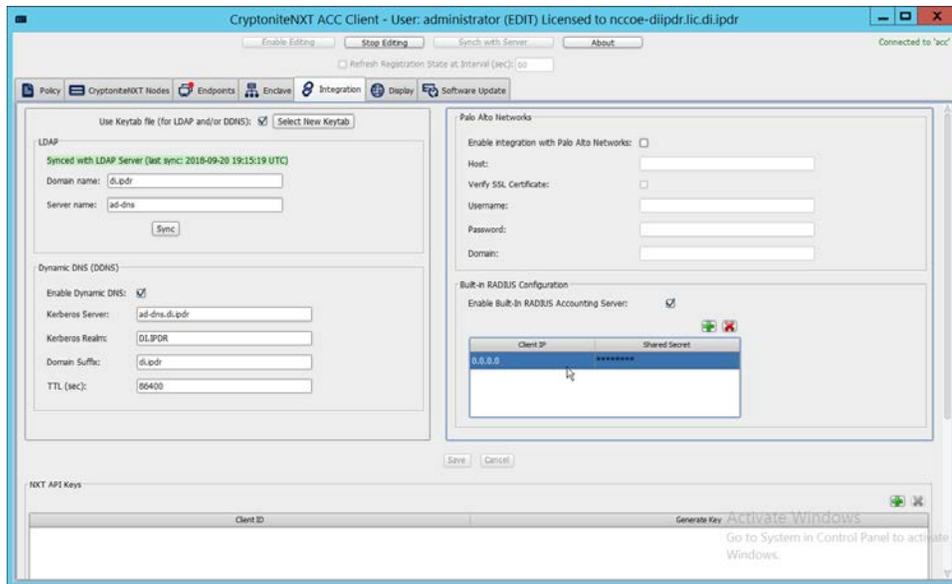
### 2938 2.21.2 Configuring CryptoniteNXT for RADIUS

- 2939 1. Open the CryptoniteNXT GUI and log in.  
 2940 2. Navigate to the **CryptoniteNXT Nodes** tab.  
 2941 3. Click **Enable Editing**.  
 2942 4. Select the **Endpoint** node, which will have your switch attached to it.  
 2943 5. Under **Endpoint Node-Specific Configuration**, select **Strict Access** for **Access Control**.  
 2944 6. Select **After Delay** for the **Portal/Whitelist Mode**.  
 2945 7. Enter -1 for **Captive Portal delay**.  
 2946 8. Enter 5 for the **Registration delay**.  
 2947 9. Select the **Gateway** node.



- 2948 10. Click **Save**.  
 2949 11. Navigate to the Integration tab.  
 2950

- 2951 12. Under **Built-In RADIUS Configuration**, check the box next to Enable Built-In RADIUS Accounting  
 2952 Server.



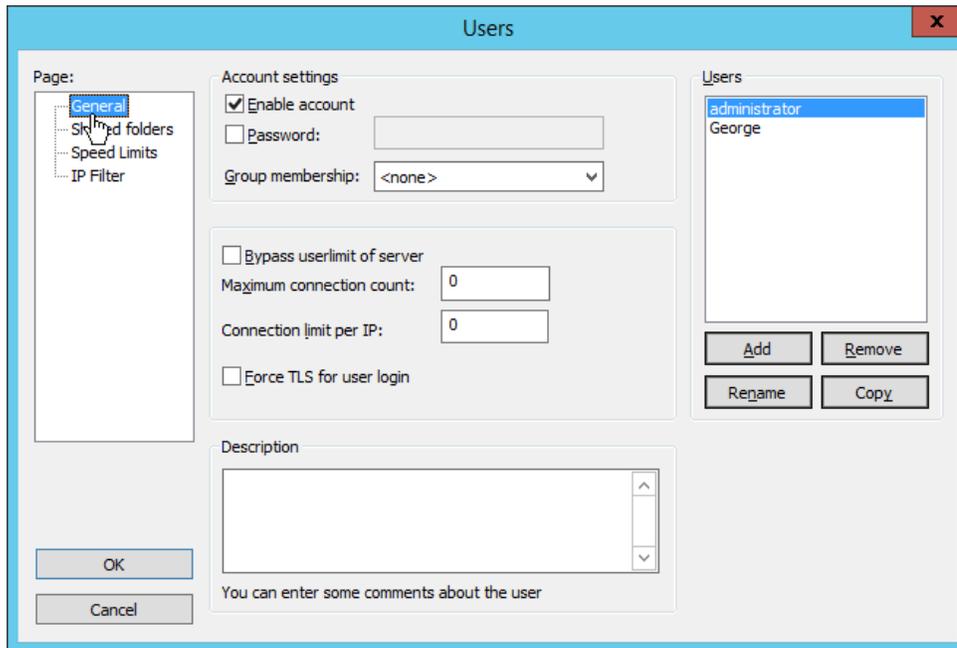
- 2953 13. Click the **plus button** to add the IP of the switch as well as a shared secret. You can use 0.0.0.0/  
 2954 as the IP to accept RADIUS Accounting packets from all IPs, however this is not recommended in  
 2955 production.

## 2956 2.22 Integration: Backups and GreenTec

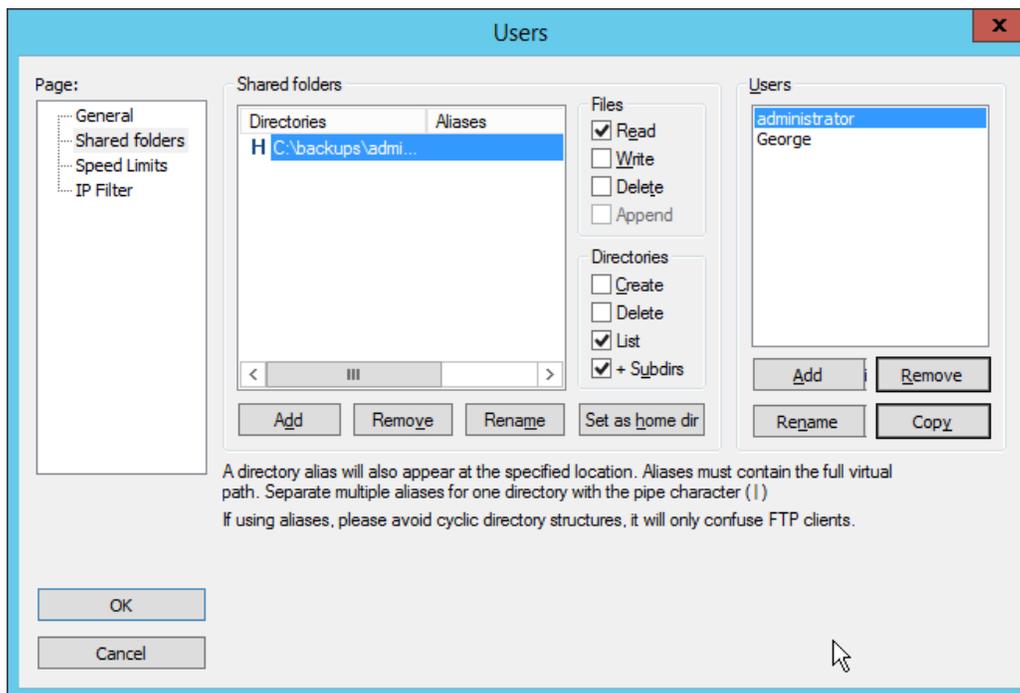
2957 This section details integration between the backup capability and **GreenTec WORMdisks**. Because  
 2958 **GreenTec WORMdisks** provide write protection for files on the disk, they are an ideal place to store  
 2959 important backups. There are a couple options for this integration, but before these backups can be  
 2960 replicated onto secure storage, it is important to be able to identify the location of backups to be  
 2961 replicated.

### 2962 2.22.1 Locate Backups with FileZilla and Duplicati

- 2963 1. To locate backups in **FileZilla**, open the **FileZilla Server** console.
- 2964 2. Click **Edit > Users**.

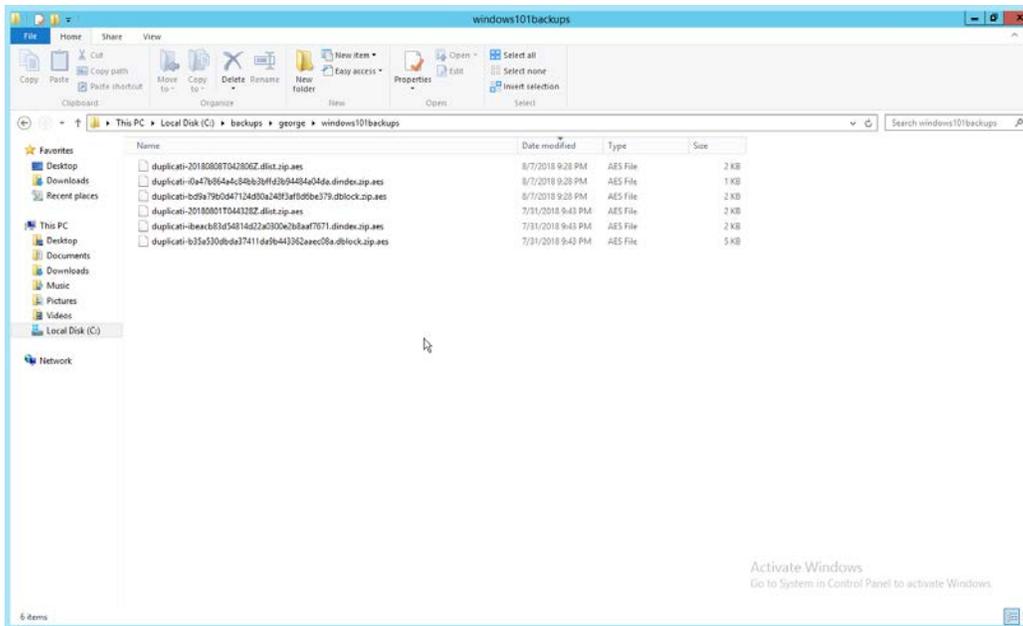


2965 3. Click **Shared folders** in the left pane.



2966 4. Under **Directories** is a list of directories in which the selected user can store backups. The one  
 2967 marked **H** is the default home directory.

- 2968 5. The path to the backups from the home directory is specified in the **Path on server** field in  
 2969 **Duplicati** (see Section 2.8.6).



- 2970 6. Each backup should have three associated files. An easy way to determine what files belong  
 2971 together is to check the **Date Modified** field. These files are encrypted.

## 2972 2.22.2 Back Up to a GreenTec Disk

2973 The first, most flexible option involves backing up the backup server to a separate server with **GreenTec**  
 2974 **WORMdisks**. Simply set up a **FileZilla** server on the **GreenTec** storage server and a **Duplicati** client on  
 2975 the backup server (see Section 2.8 for these installation processes). When choosing where to store files  
 2976 on FileZilla, indicate a folder on the **GreenTec WORMdisk**. Sectors of the disk can be locked using the  
 2977 mechanism in Section 2.6.4, providing firmware-level write security for any backups in the locked  
 2978 sectors.

2979 There are some considerations when doing this. First, if this is done on a schedule and permanent locks  
 2980 are used, space will be consumed quickly and the **WORMdisks** will need replacements as the space  
 2981 cannot be reused. The trade-off between space and backup frequency must be considered—a lower  
 2982 backup frequency inevitably means more data loss in the event of a restoration, while higher backup  
 2983 frequency increases the cost of maintaining secure storage.

2984 Alternatively, secure storage can be used for specific types of backups, such as “golden disks”—which  
 2985 would contain backups of the basic level of functionality required for the enterprise without necessarily

2986 utilizing a backup schedule. This would afford protection for some basic functionality but would forfeit  
2987 the secure storage capability for day-to-day data.

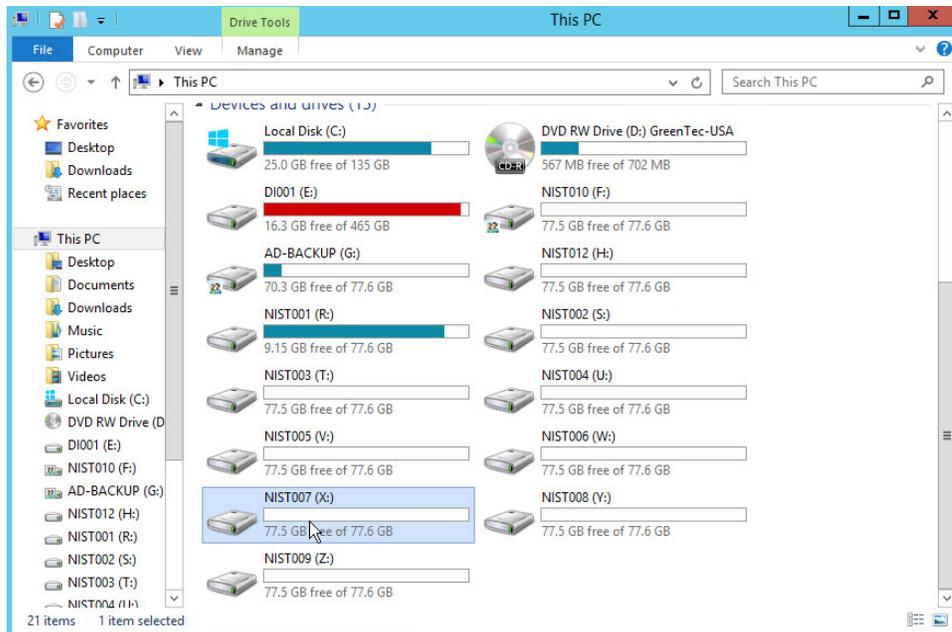
2988

2989 In addition to the options above, there are other ways to minimize wasted space on a GreenTec disk.  
2990 Temporary Locks, or TLocks, can be employed after the data is backed up to a GreenTec disk to protect  
2991 data integrity while making less space unavailable for future use. After the drive is full, a permanent lock  
2992 should still be executed. Wasted space can also be minimized with the use of dynamic partitions, or  
2993 with the Force-Field Write-Once File System, which can also reduce the overhead administration of the  
2994 GreenTec disk.

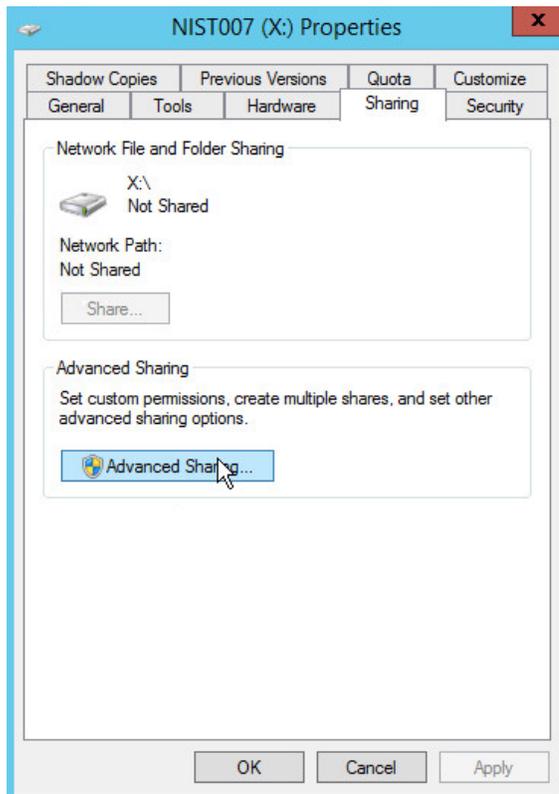
### 2995 2.22.3 Configure Network-Accessible GreenTec Disk

2996 Another option for GreenTec disks is to make them network accessible. This allows them to be used  
2997 specifically in situations where secure storage protection is desired, and it makes them options for  
2998 backup locations even on servers to which they are not necessarily physically connected.

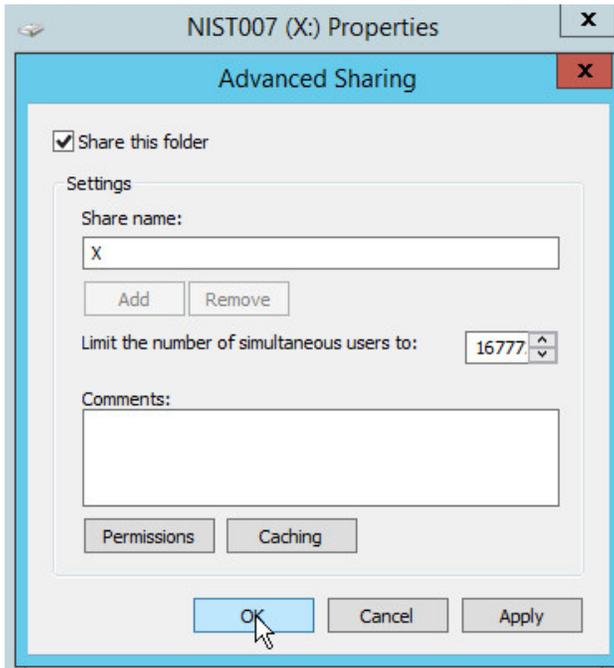
- 2999 1. To configure a GreenTec disk to be network accessible, right-click the disk on the GreenTec  
3000 server.



- 3001 2. Click **Share With > Advanced Sharing**.



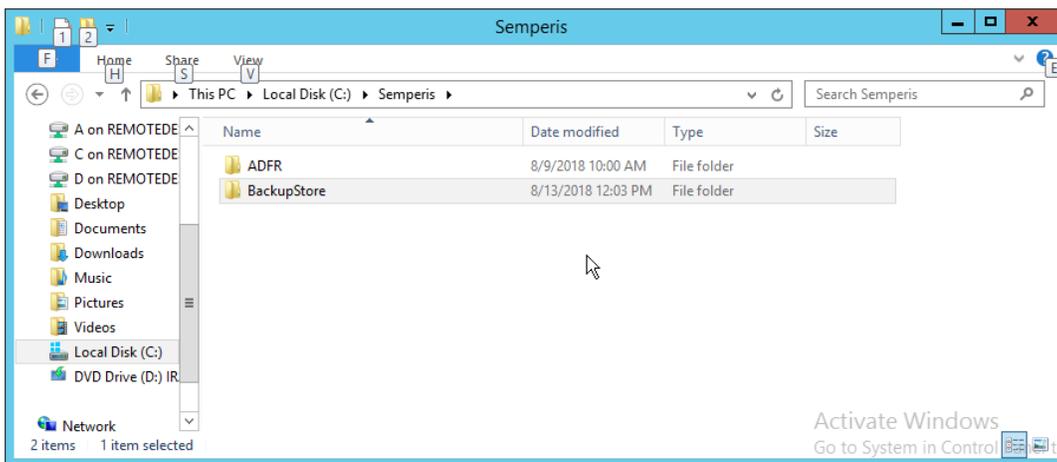
- 3002 3. Click **Advanced Sharing**.
- 3003 4. Check the box next to **Share this folder**.
- 3004 5. Enter a name for the drive if desired.



- 3005 6. Click **OK**.
- 3006 7. Click **Close**.
- 3007 8. The drive should now be accessible at **//SERVER-NAME/X**.

#### 3008 2.22.4 Secure Storage for Semperis ADFR

- 3009 1. On the Semperis ADFR server, the default backup location is C:\Semperis.
- 3010 2. In this folder there is metadata for the backups (C:\Semperis\ADFR) as well as the backups
- 3011 themselves (C:\Semperis\BackupStore).



3012 It is important to consider the limitations of the backup software when considering whether to replicate  
 3013 backups to secure storage. Ideally, the replication of backups ensures that they can be used on a  
 3014 separate server when the original server is affected by an incident. The replication of backups in this  
 3015 case can offer some write protection for these specific backup files, but if the entire server is lost, it is  
 3016 not guaranteed that the backups will be usable on a new instance of ADFR. This risk can be mitigated by  
 3017 exporting the configuration of the ADFR server for the purpose of building a failover ADFR server.

3018 Though these backups can be replicated to WORMdisks, this is currently not supported by Semperis  
 3019 ADFR. Instead, Semperis ADFR offers a different type of “secure storage” by not joining to the domain,  
 3020 allowing the machine to be taken offline and brought online only during creation/application of a  
 3021 backup.

## 3022 2.23 Integration: Micro Focus ArcSight and FileZilla

3023 In this section an integration between ArcSight and FileZilla is detailed so that logs from FileZilla are  
 3024 forwarded to ArcSight by using an ArcSight syslog file connector.

### 3025 2.23.1 Enable Logs in FileZilla

- 3026 1. On the server with **FileZilla** installed, open **FileZilla Server**.

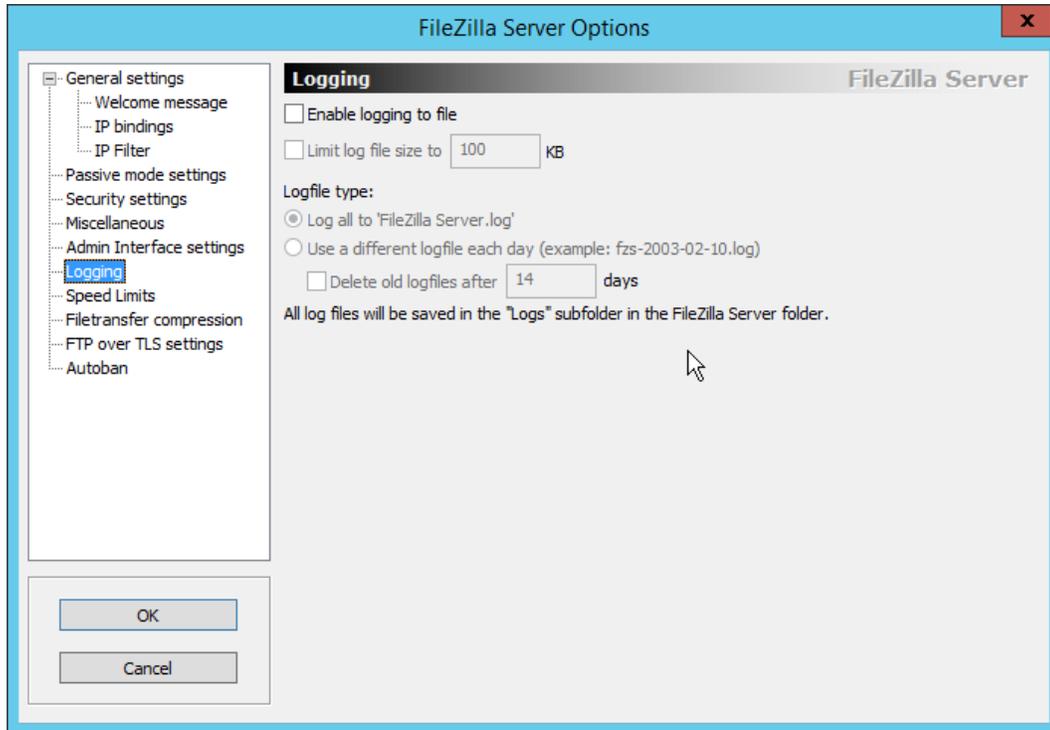
The screenshot shows the FileZilla Server application window. The title bar reads "FileZilla Server (127.0.0.1)". The main area is a terminal window displaying the following log output:

```
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> z20 filezilla server 0.0.0.0 user
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> Z20-written by Tim Kosse (tim.kosse@filezilla-project.org)
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> Z20 Please visit https://filezilla-project.org/
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> AUTH TLS
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> 234 Using authentication type TLS
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> TLS connection established
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> USER george
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> 331 Password required for george
(000086)8/22/2018 21:28:18 PM - (not logged in) (192.168.1.138)> PASS *****
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 230 Logged on
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> PBSZ 0
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 200 PBSZ=0
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> PROT P
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 200 Protection level set to P
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> OPTS utf8 on
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 202 UTF8 mode is always enabled. No need to send this command.
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> PWD
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 257 "/" is current directory.
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> TYPE I
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 200 Type set to I
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> PASV
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 227 Entering Passive Mode (192,168,1,121,199,178)
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> RETR windows10backups/duplicati-bd9a79b0d47124d80a248f3af8d6e379.dblock.zip.aes
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 150 Opening data channel for file download from server of "/windows10backups/duplicati-bd9a79b0d47124d80a248f3af8d6e379.dblock.zip.aes"
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> TLS connection for data connection established
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 226 Successfully transferred "/windows10backups/duplicati-bd9a79b0d47124d80a248f3af8d6e379.dblock.zip.aes"
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> QUIT
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> 221 Goodbye
(000086)8/22/2018 21:28:18 PM - george (192.168.1.138)> disconnected.
Retrieving settings, please wait...
Done retrieving settings
```

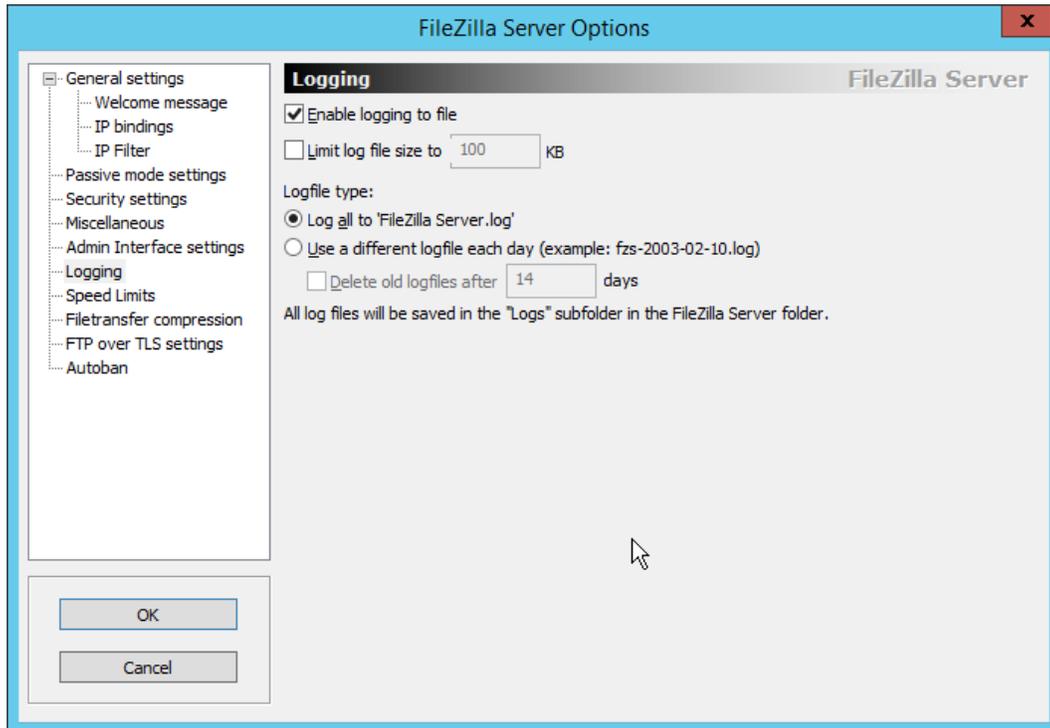
At the bottom of the window, a progress bar shows "7,712 bytes received 0 B/s" and "39,760 bytes sent 0 B/s".

- 3027 2. Click **Edit > Settings**.

- 3028 3. Click **Logging**.



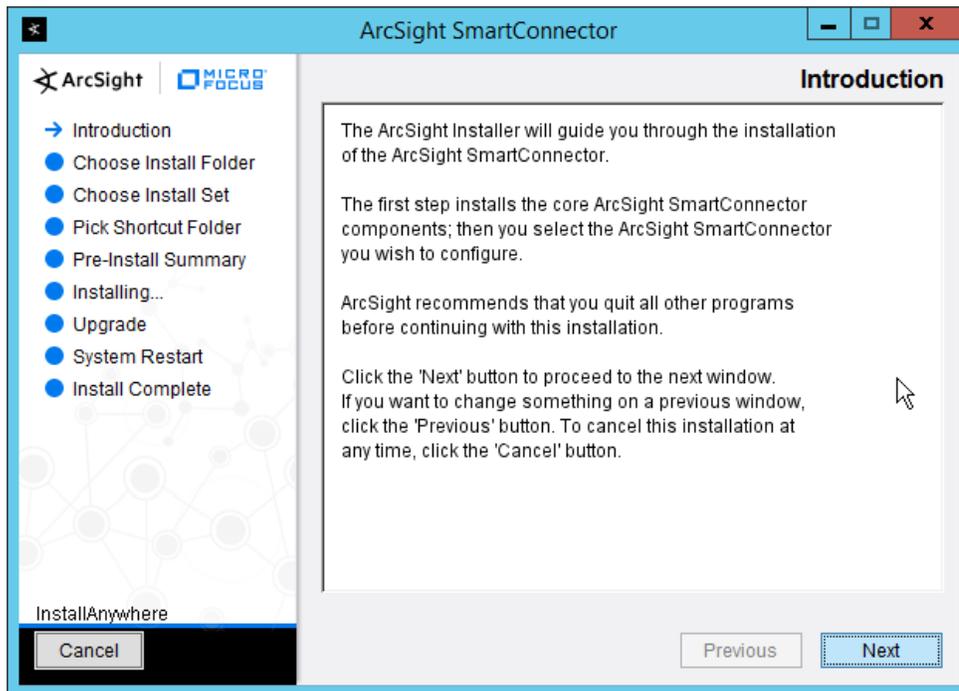
- 3029 4. Check the box next to **Enable logging to file**.



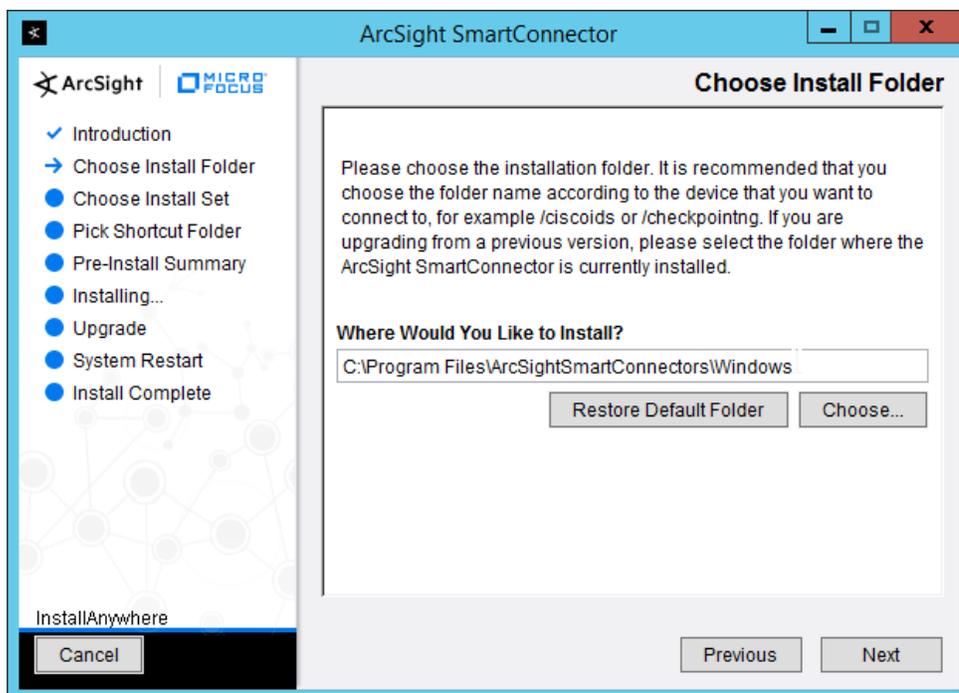
3030 5. Click **OK**.

### 3031 2.23.2 Install Micro Focus ArcSight

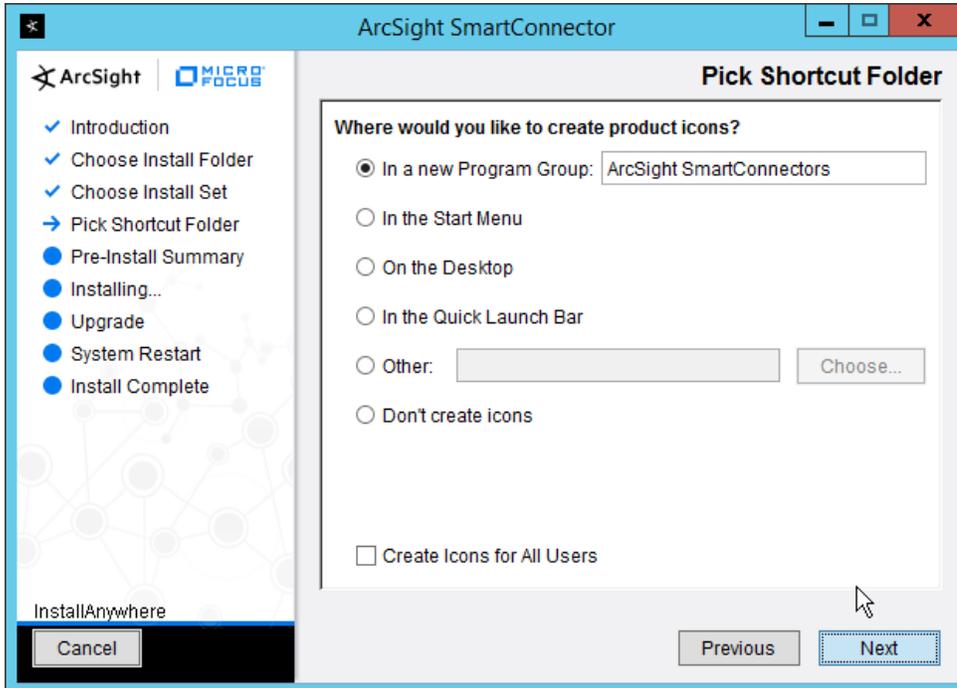
3032 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



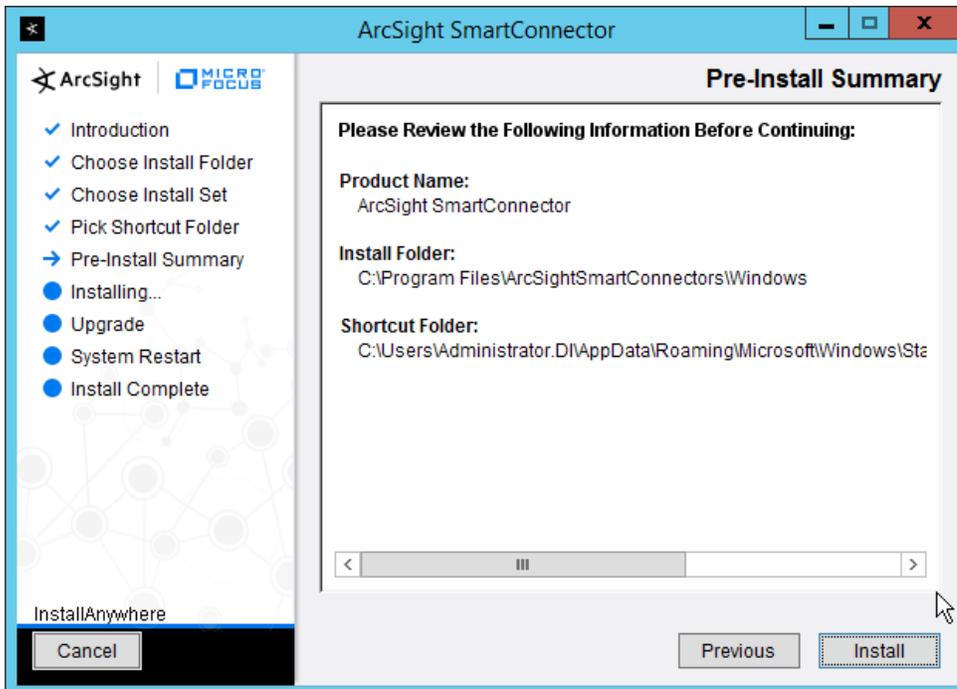
- 3033 2. Click **Next**.
- 3034 3. Enter C:\Program Files\ArcSightSmartConnectors\Windows.



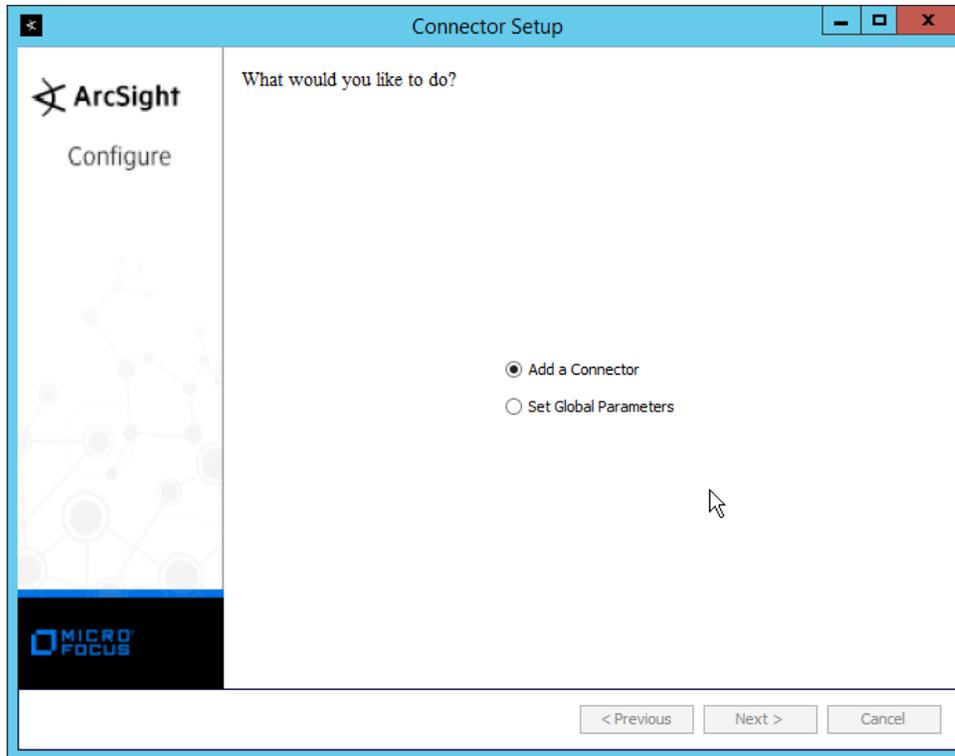
3035 4. Click **Next**.



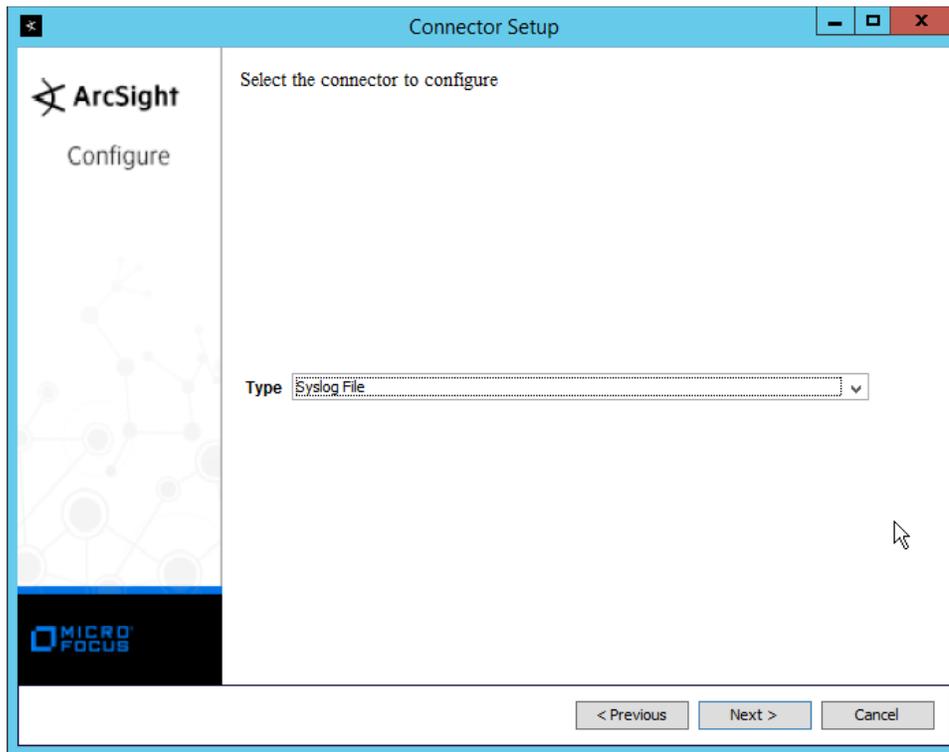
3036 5. Click **Next**.



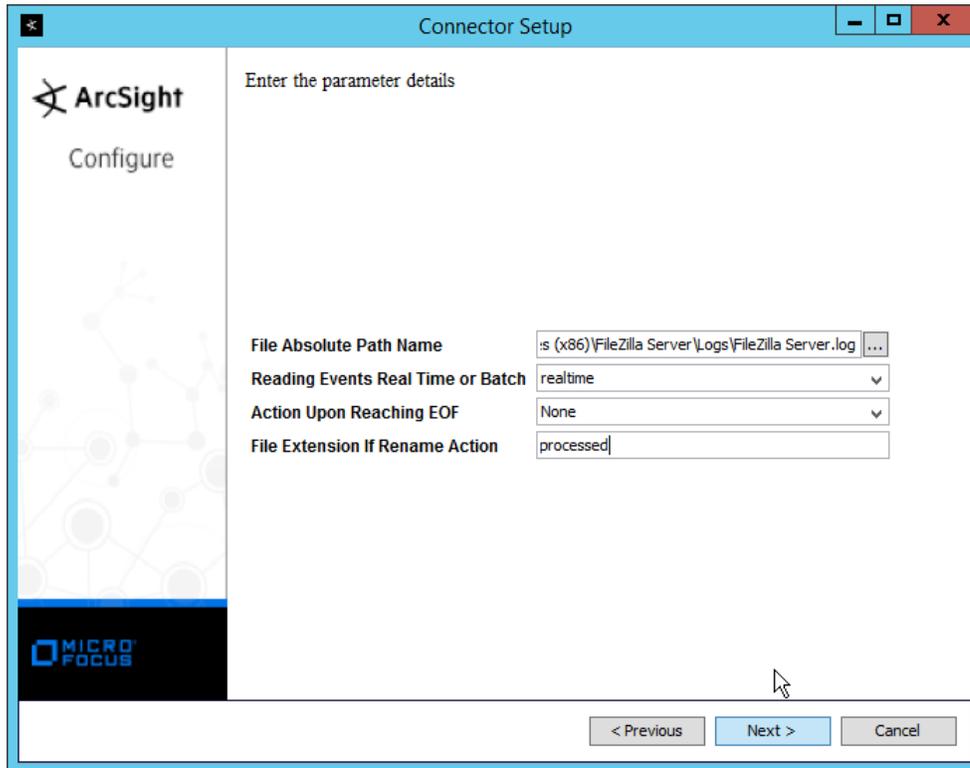
- 3037 6. Click **Install**.
- 3038 7. Select **Add a Connector**.



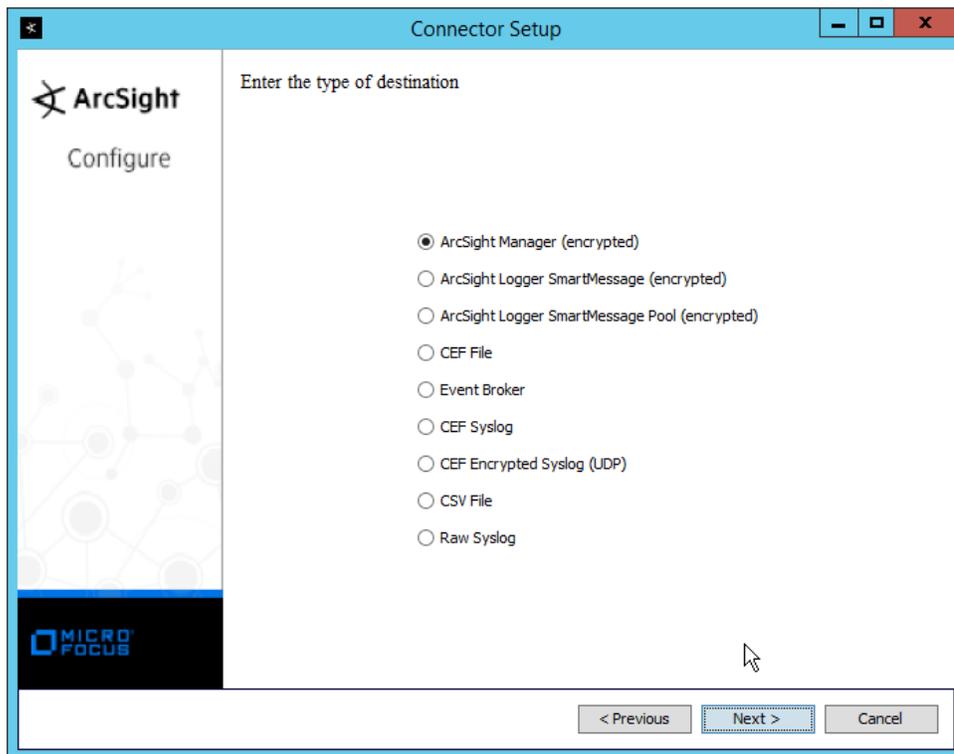
- 3039 8. Click **Next**.
- 3040 9. Select **Syslog File**.



- 3041 10. Click **Next**.
- 3042 11. Enter C:\Program Files (x86)\FileZilla Server\Logs\FileZilla Server.log for **File Absolute Path**
- 3043 **Name**.



- 3044 12. Click **Next**.
- 3045 13. Select **ArcSight Manager (encrypted)**.



3046

14. Click **Next**.

3047

15. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.

Connector Setup

ArcSight  
Configure

Enter the destination parameters

Manager Hostname: arcsight-esm

Manager Port: 8443

User: administrator

Password: ●●●●●●

AUP Master Destination: false

Filter Out All Events: false

Enable Demo CA: false

< Previous   Next >   Cancel

- 3048 16. Click **Next**.
- 3049 17. Enter identifying details about the system (only **Name** is required).

Connector Setup

ArcSight  
Configure

Enter the connector details

Name: FileZilla Logs

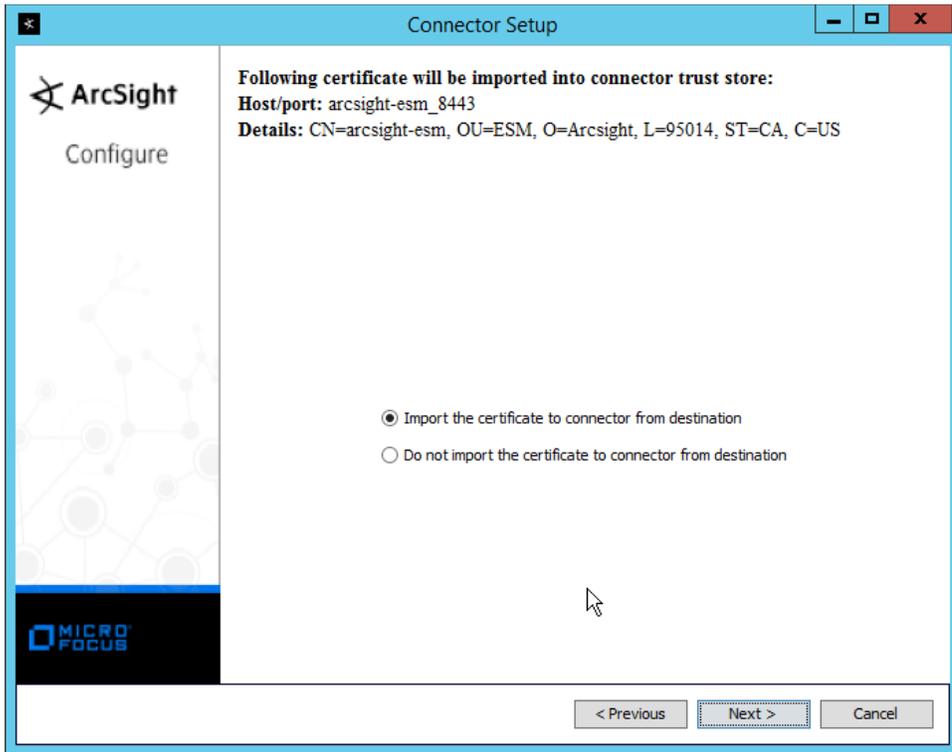
Location: [Empty]

DeviceLocation: [Empty]

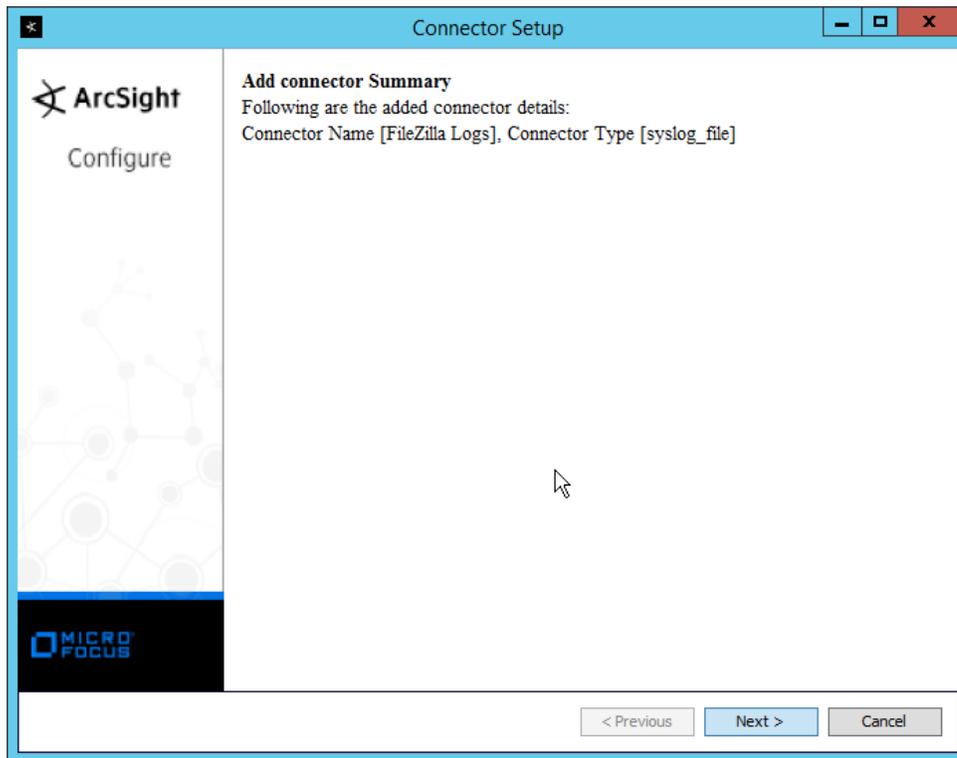
Comment: [Empty]

< Previous   Next >   Cancel

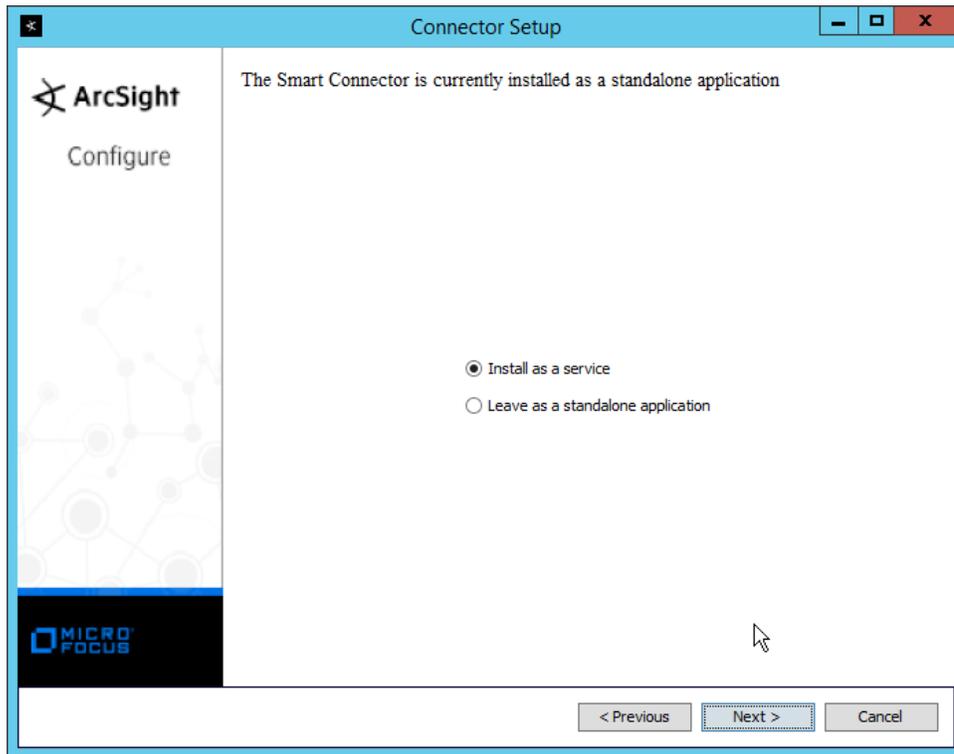
- 3050      18. Click **Next**.
- 3051      19. Select **Import the certificate to connector from destination**.



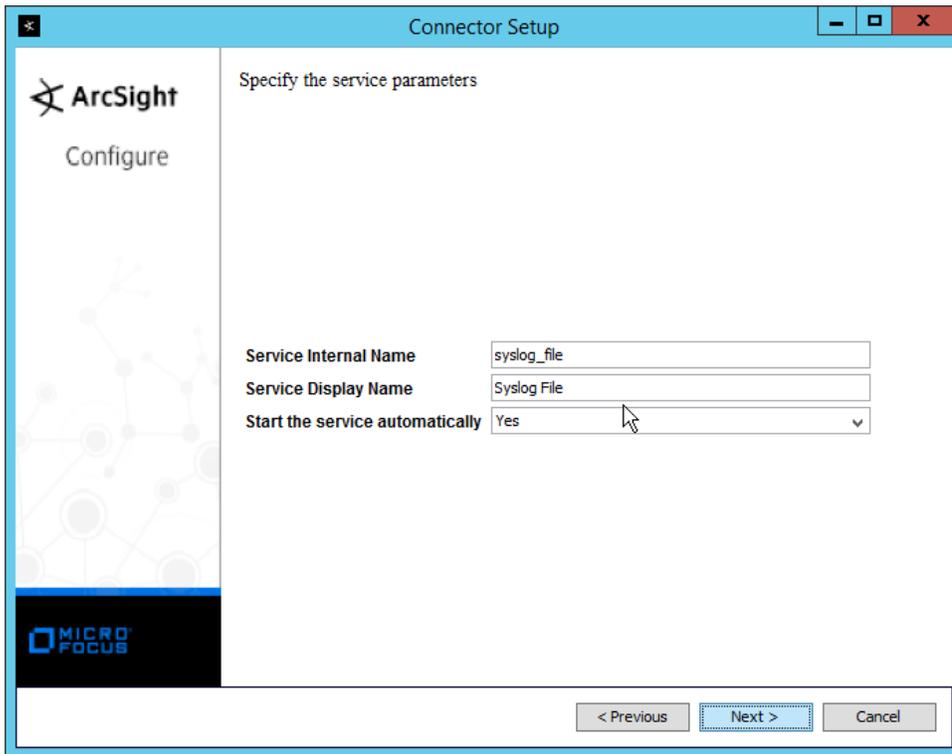
3052      20. Click **Next**.



- 3053 21. Click **Next**.
- 3054 22. Select **Install as a service**.

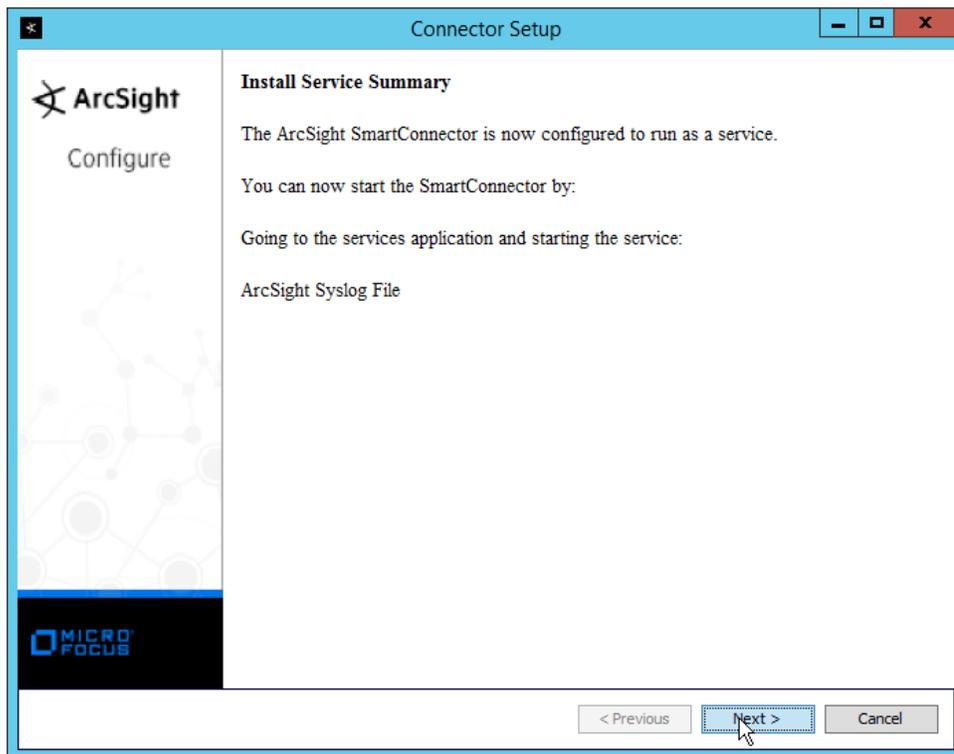


3055 23. Click **Next**.



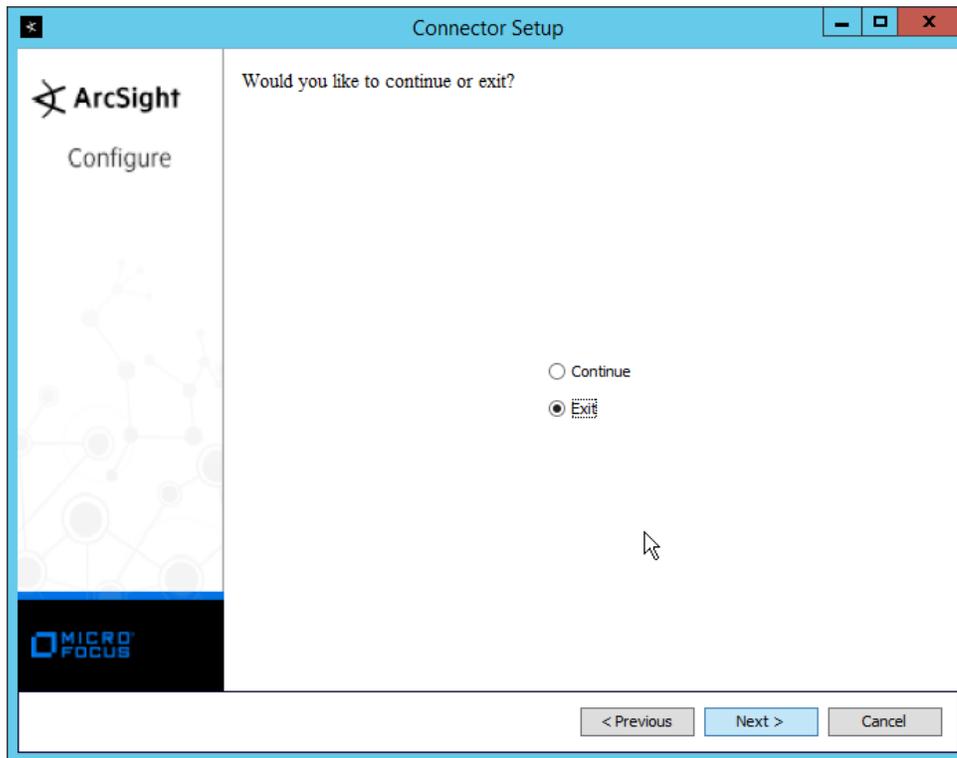
3056

24. Click **Next**.

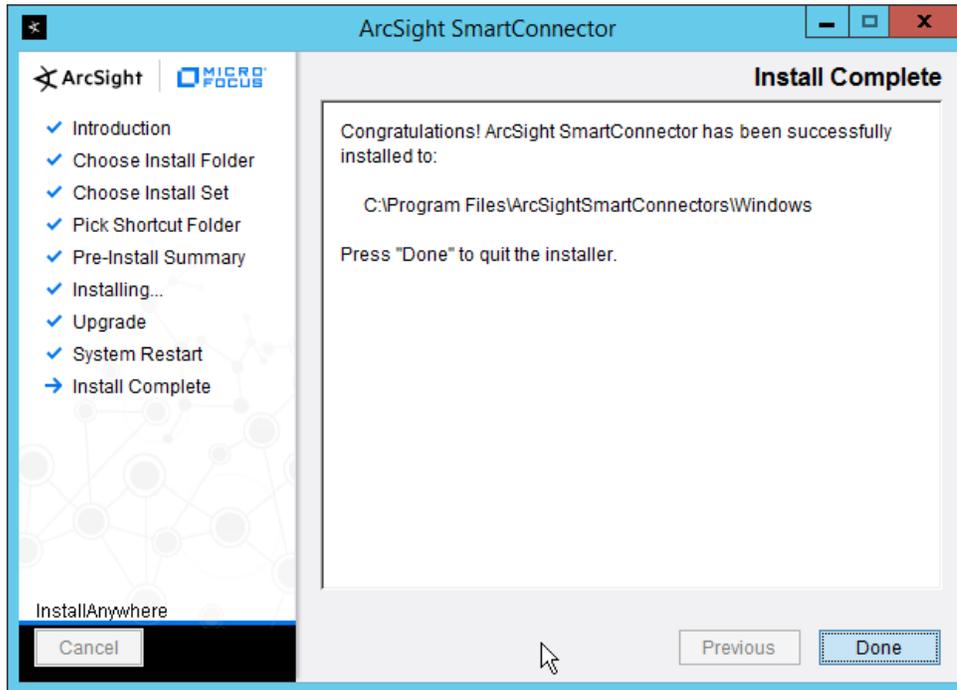


3057 25. Click **Next**.

3058 26. Select **Exit**.



3059 27. Click **Next**.



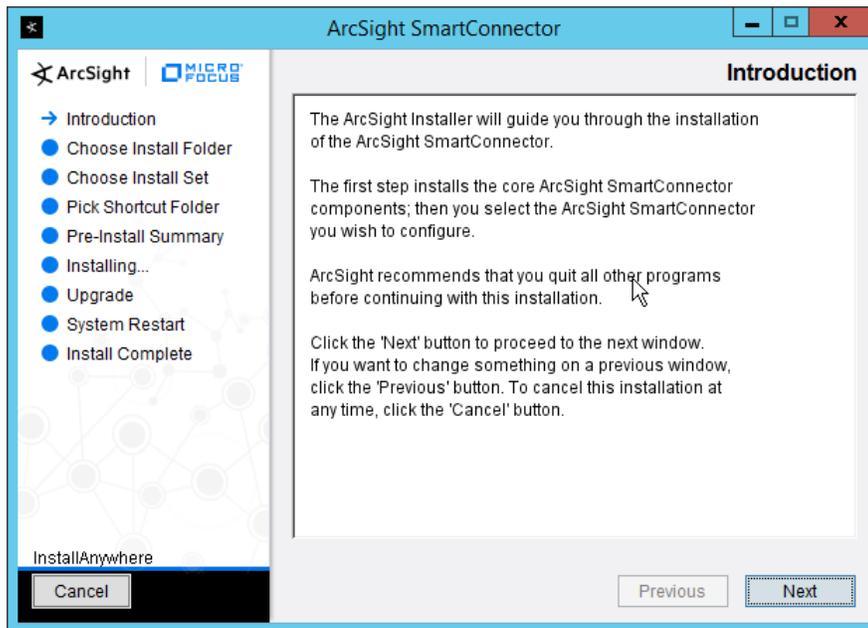
3060 28. Click **Done**.

## 3061 2.24 Integration: Micro Focus ArcSight and Tripwire

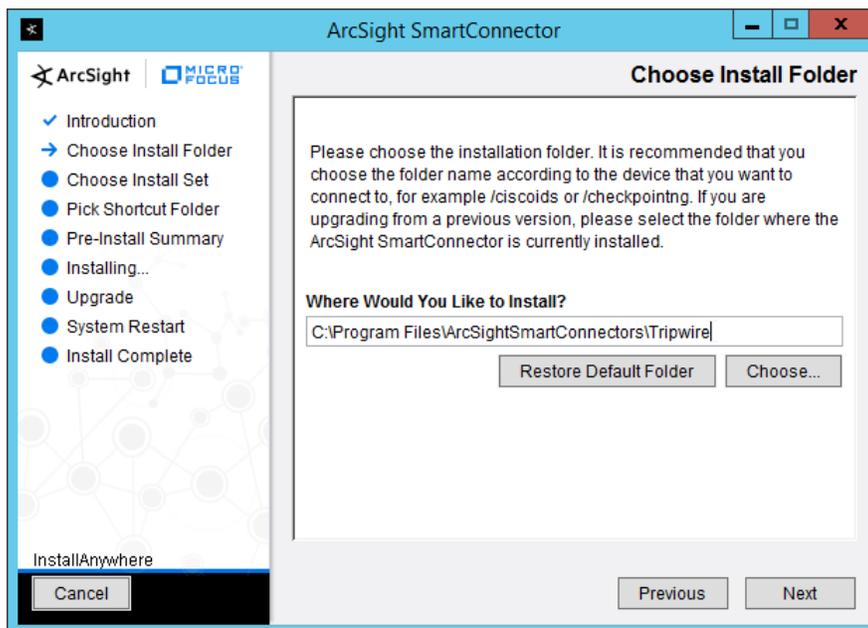
3062 This section details forwarding logs from **Tripwire Log Center** to **Micro Focus ArcSight**. This will forward  
3063 **Tripwire IP360** and **Tripwire Enterprise** logs to **ArcSight**, assuming those logs are being collected by  
3064 **Tripwire Log Center**.

### 3065 2.24.1 Install Micro Focus ArcSight

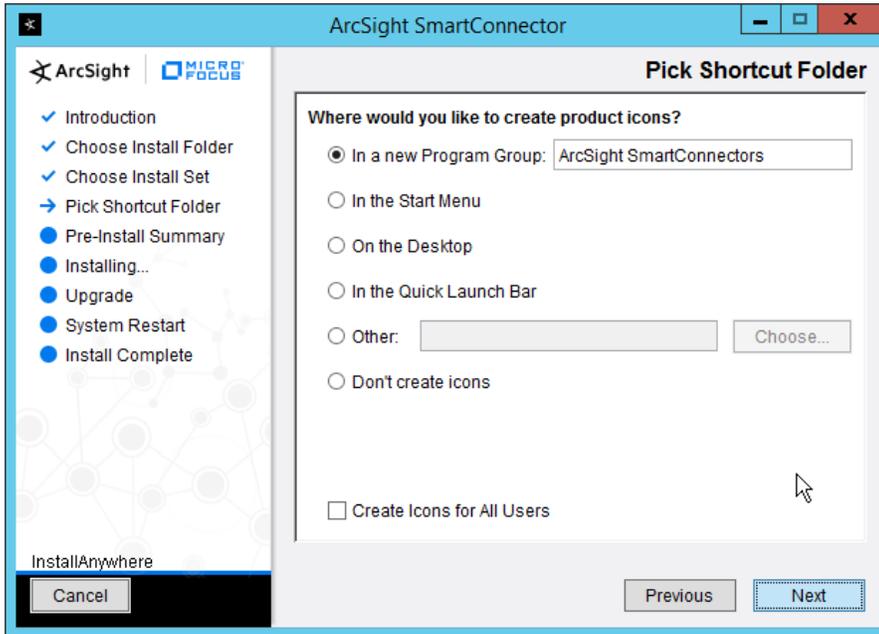
- 3066 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running Tripwire  
3067 Log Center.



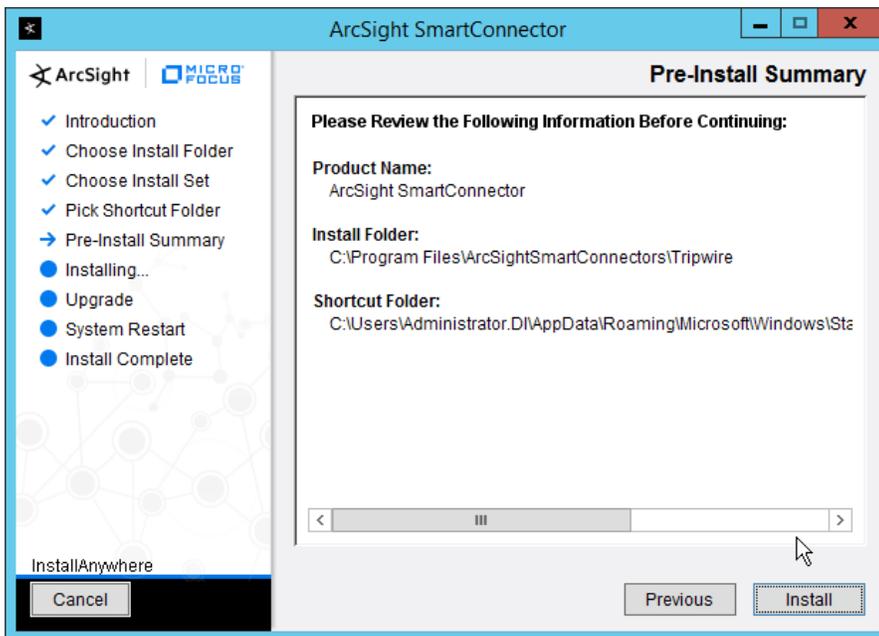
- 3068 2. Click **Next**.



- 3069 3. Enter C:\Program Files\ArcSightSmartConnectors\Tripwire.

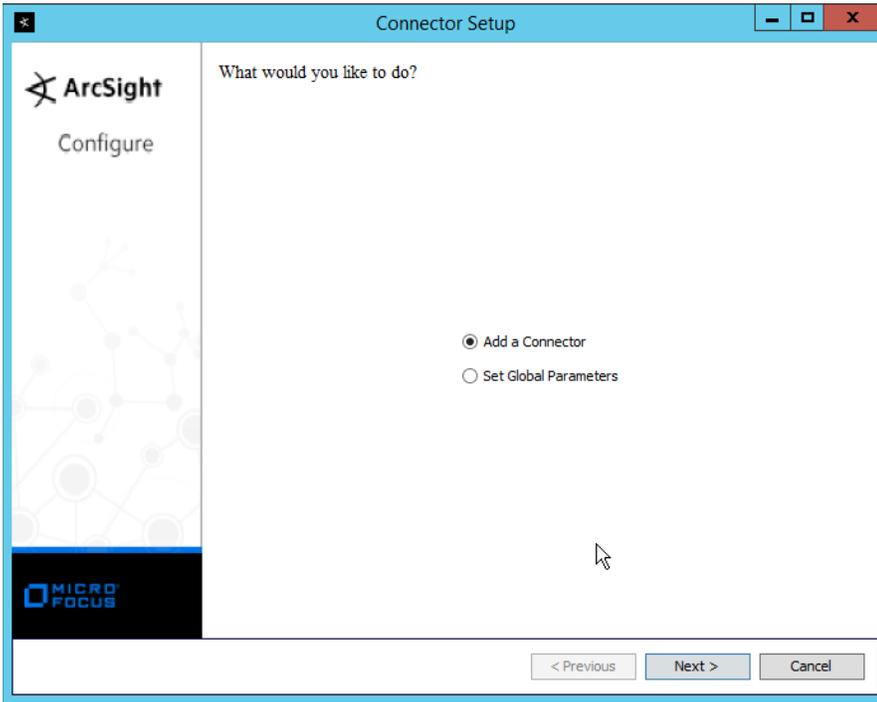


3070 4. Click **Next**.

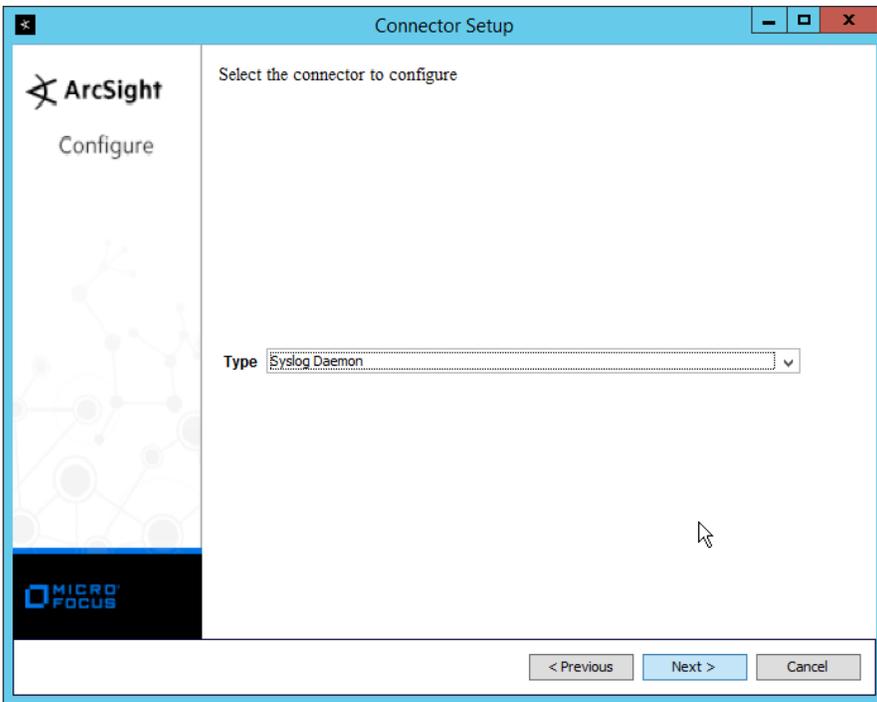


3071 5. Click **Install**.

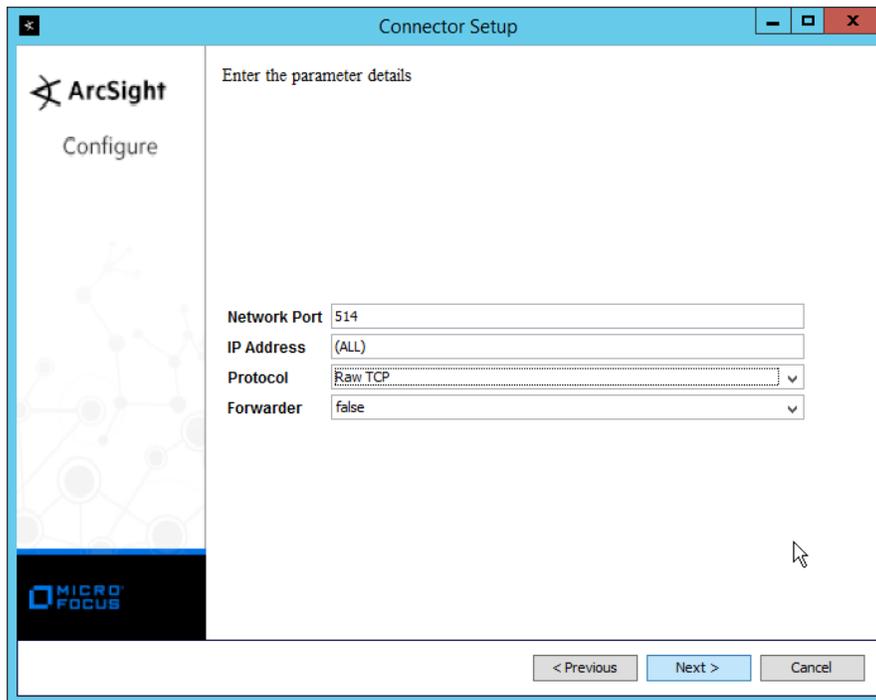
3072 6. Select **Add a Connector**.



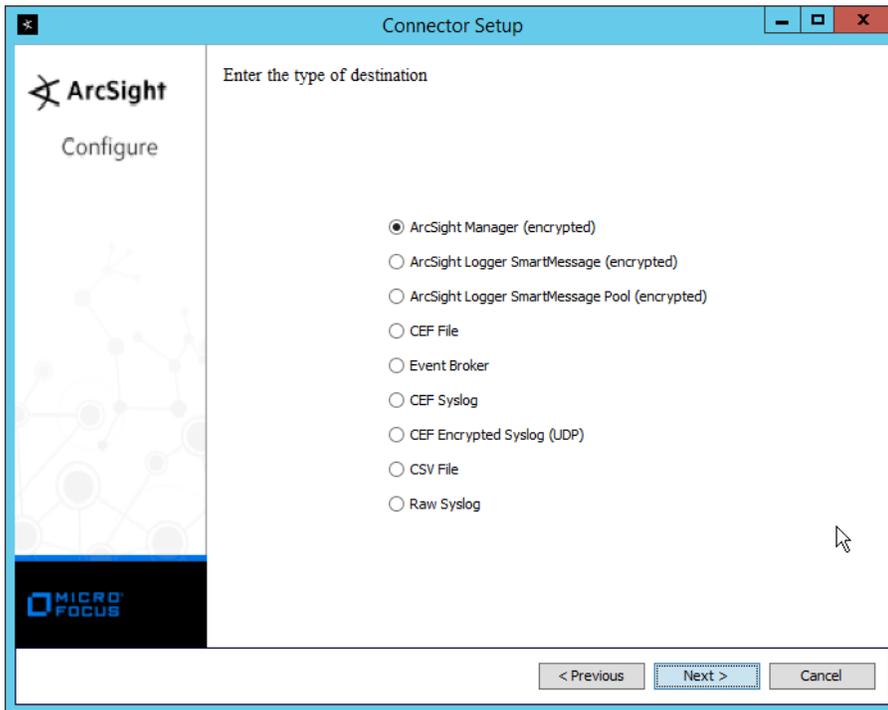
- 3073 7. Click **Next**.
- 3074 8. Select **Syslog Daemon**.



- 3075 9. Click **Next**.
- 3076 10. Enter a port for the daemon to run on.
- 3077 11. Select **Raw TCP** for **Protocol**.



- 3078 12. Click **Next**.
- 3079 13. Select **ArcSight Manager (encrypted)**.

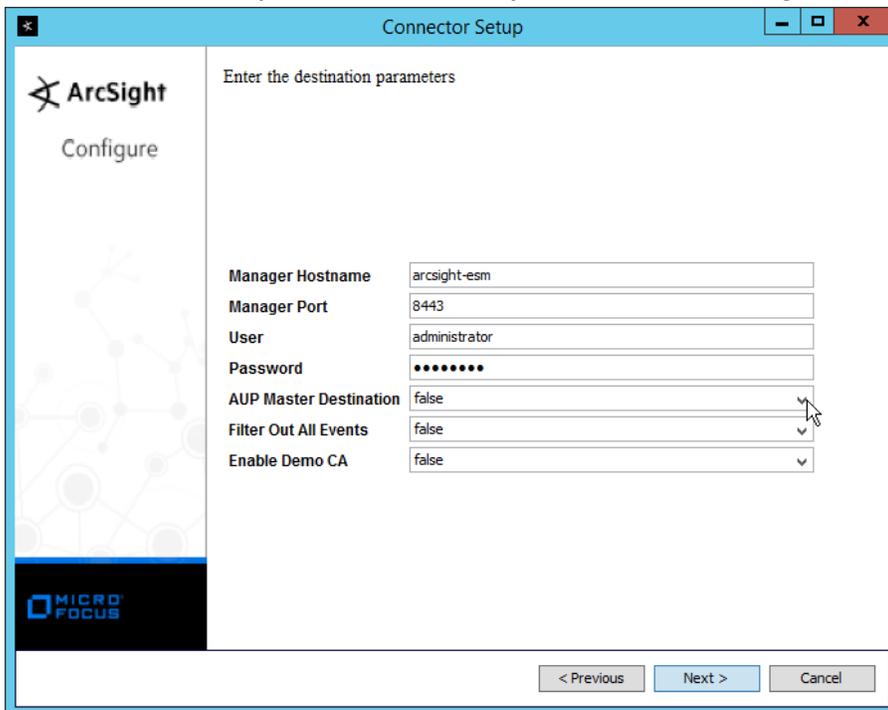


3080

14. Click **Next**.

3081

15. Enter the **hostname, port, username, and password** for the ArcSight ESM server.



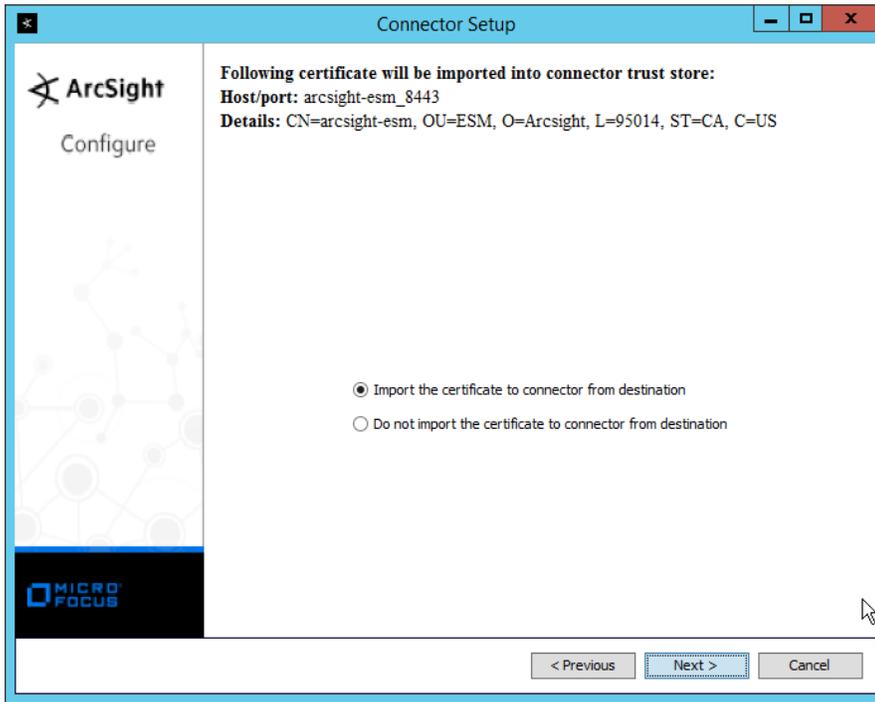
3082 16. Click **Next**.

3083 17. Enter identifying details about the system (only **Name** is required).

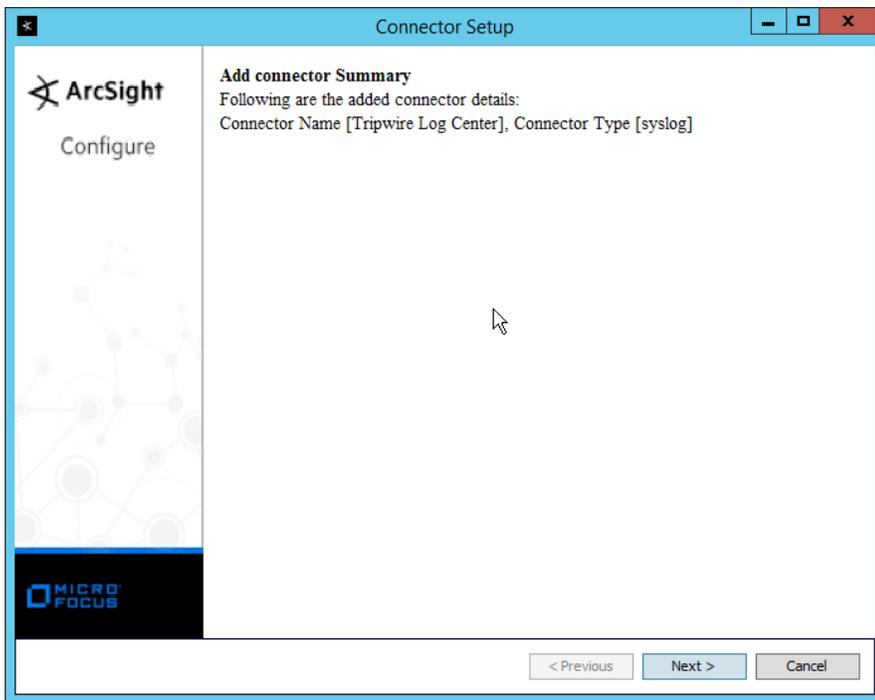
The screenshot shows a software window titled "Connector Setup". On the left side, there is a sidebar with the ArcSight logo and the word "Configure". The main content area is titled "Enter the connector details" and contains four text input fields: "Name" (with the text "Tripwire Log Center" entered), "Location", "DeviceLocation", and "Comment". At the bottom right of the window, there are three buttons: "< Previous", "Next >", and "Cancel".

3084 18. Click **Next**.

3085 19. Select **Import the certificate to connector from destination**.

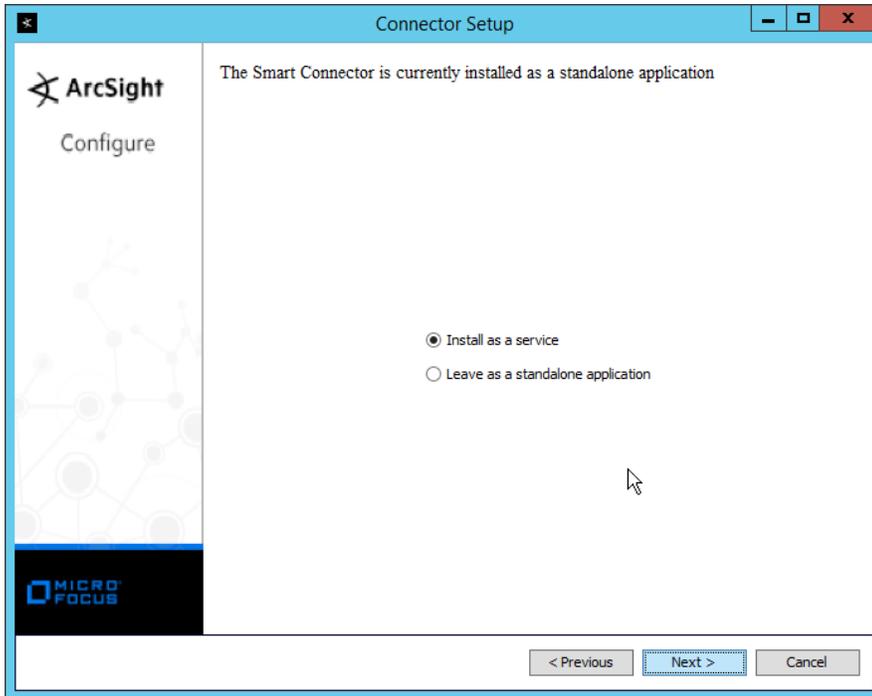


3086 20. Click **Next**.

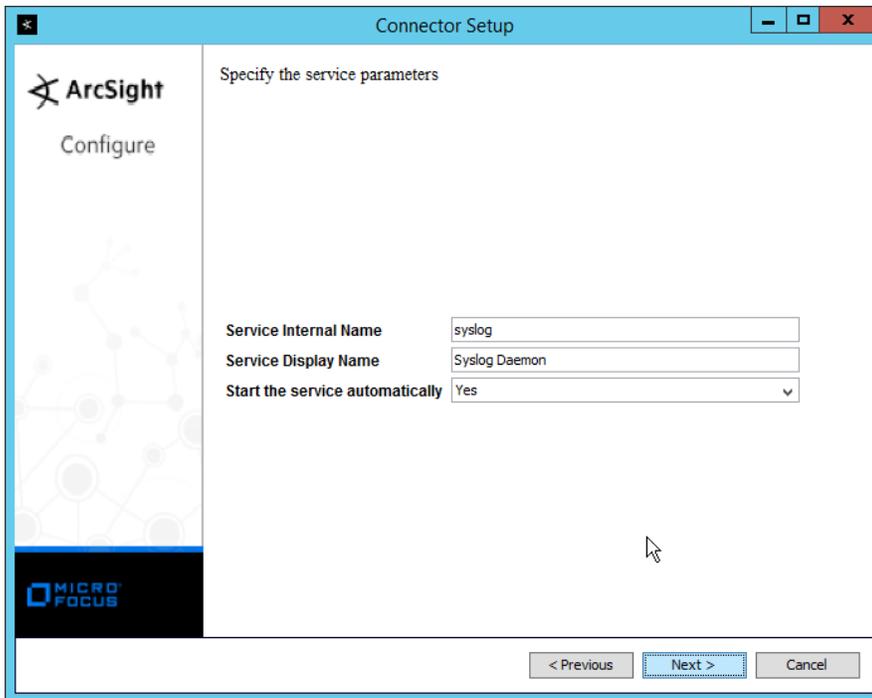


3087 21. Click **Next**.

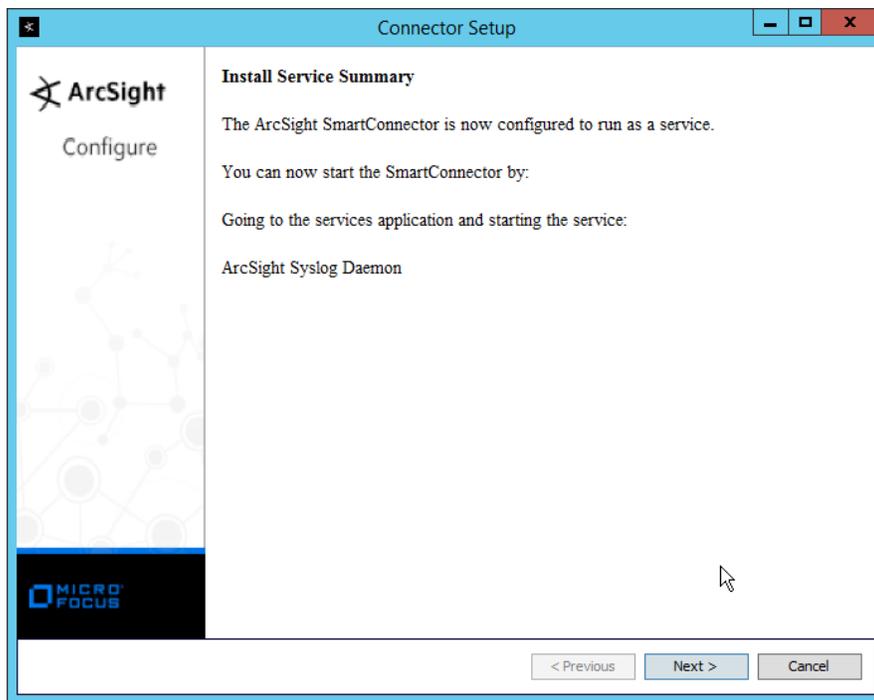
3088 22. Select **Install as a service**.



3089 23. Click **Next**.

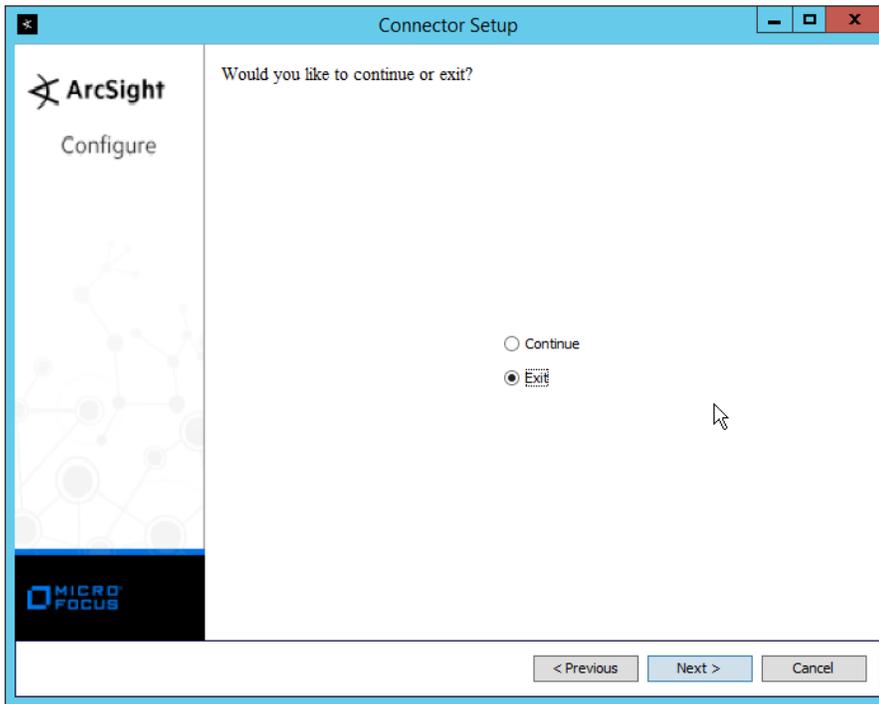


3090 24. Click **Next**.

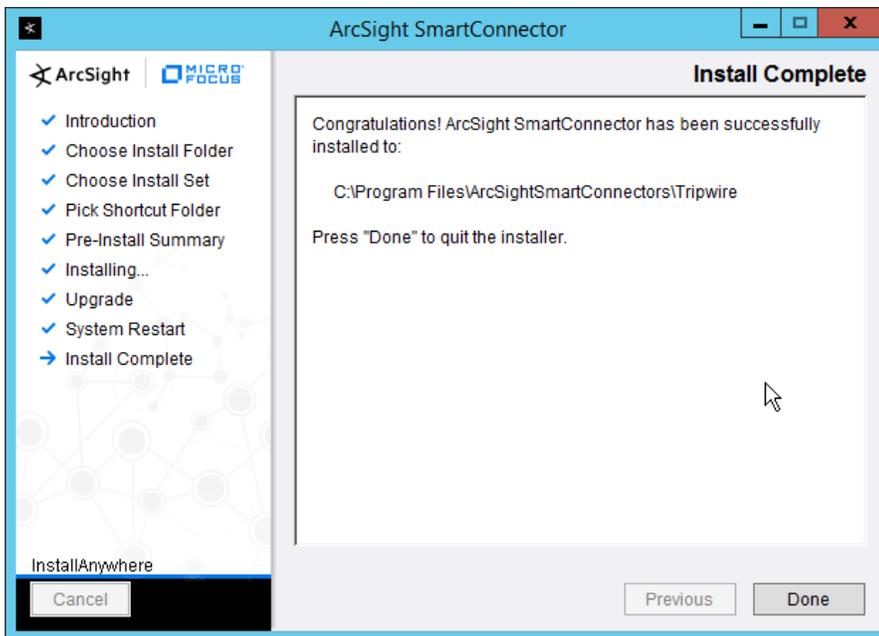


3091 25. Click **Next**.

3092 26. Select **Exit**.



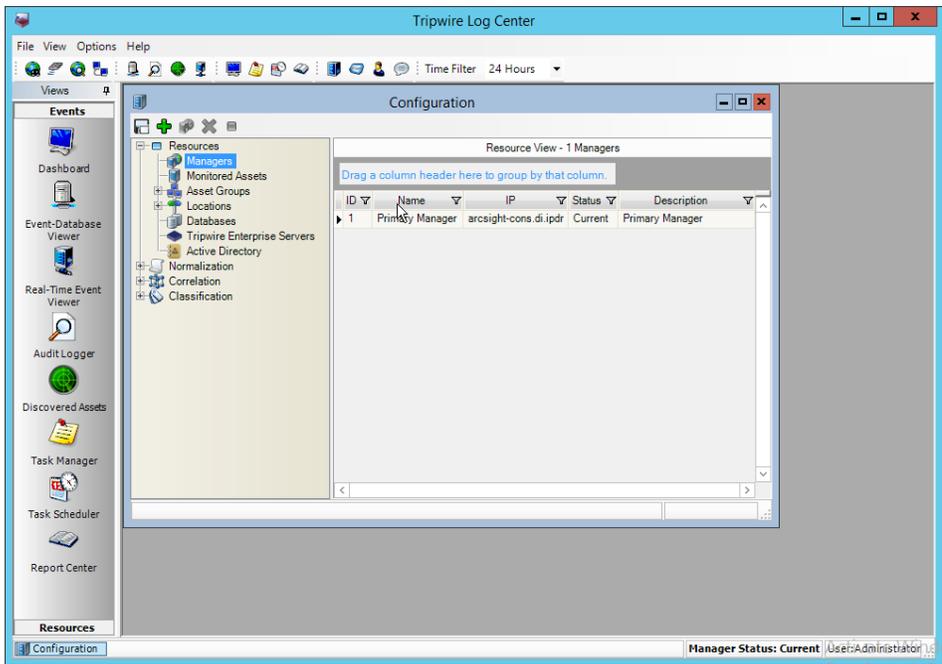
3093 27. Click **Next**.



3094 28. Click **Done**.

3095 29. Open the **Tripwire Log Center Console**.

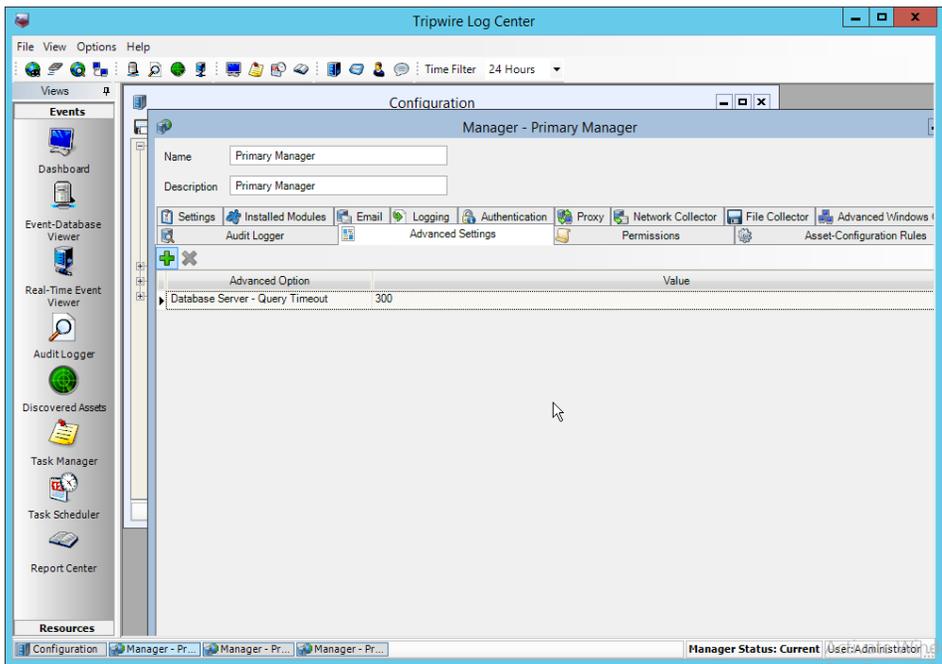
3096 30. Go to the **Configuration Manager**.



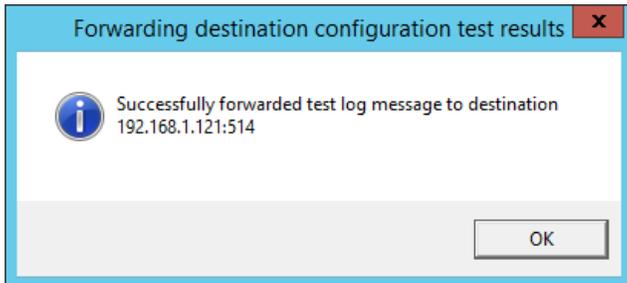
3097 31. Select **Resources > Managers**.

3098 32. Double-click the **Primary Manager**.

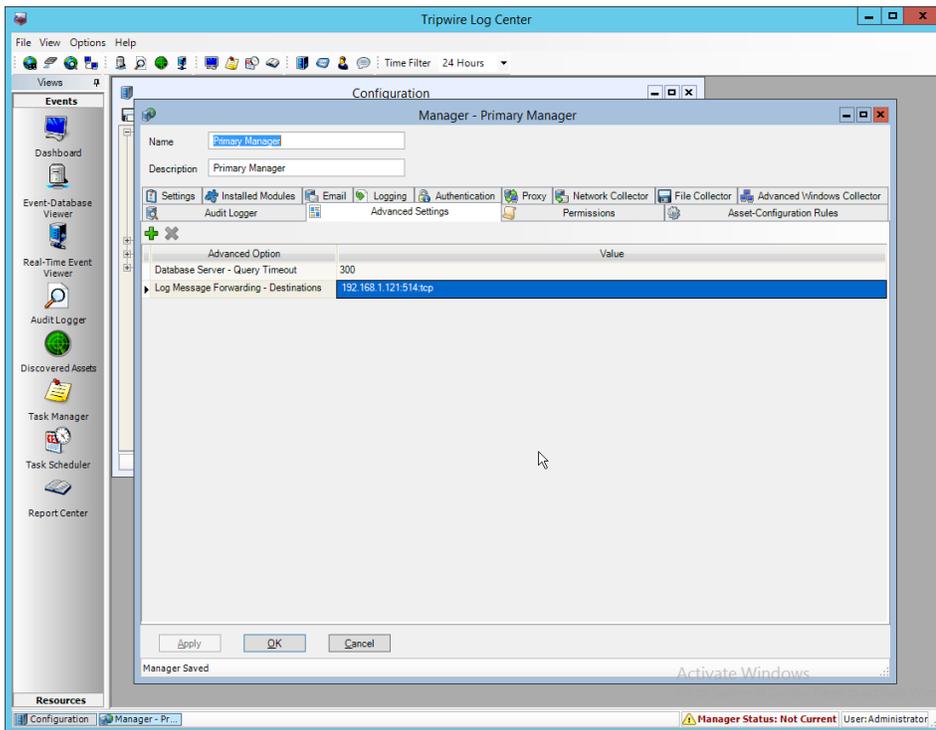
33. Click the **Advanced Settings** tab.



- 3099 34. Click the **Add** button.
- 3100 35. In the **Advanced Option** box select **Log Message Forwarding–Destinations**.
- 3101 36. In the Value box next to it, type **<ip\_address>:<port>:tcp** with the **IP address** and **port** of the
- 3102 syslog daemon just created.



- 3103 37. Click **OK**.



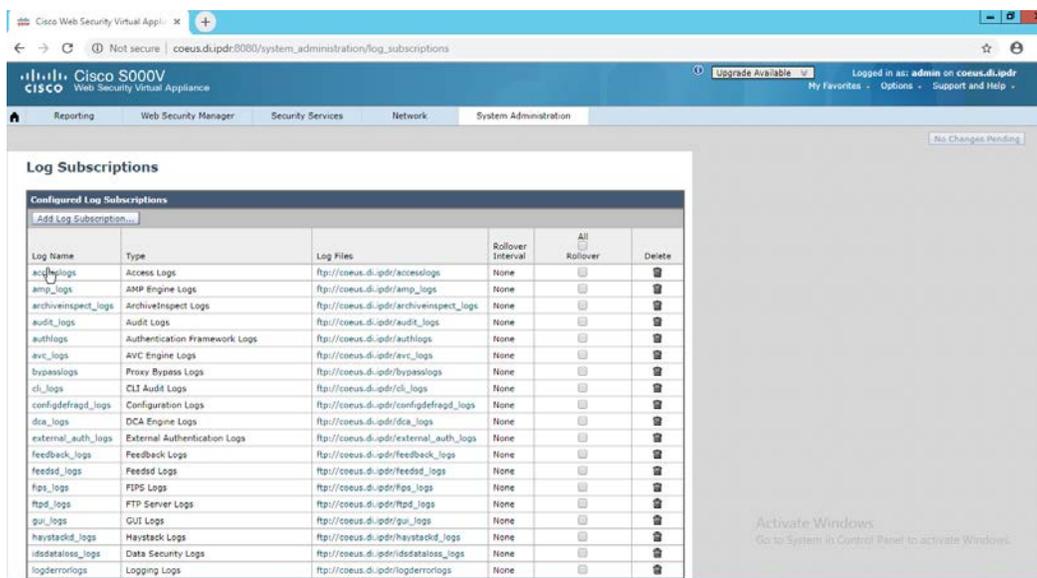
- 3104 38. Click **OK**.
- 3105 39. Restart the **Tripwire Log Center Manager**.

## 3106 2.25 Integration: Micro Focus ArcSight and Cisco WSA

3107 This integration briefly details how to send logs to an ArcSight syslog collector from Cisco WSA. Please  
 3108 see Section 2.24 for instructions for setting up an ArcSight syslog collector. If a server is already  
 3109 configured, you do not need to install a new one— simply forward logs to the address of that server.

### 3110 2.25.1 Configure Cisco WSA to Forward Logs

3111 1. In the Cisco WSA web client, navigate to **System Administration > Log Subscriptions**.



3112 2. Click **Add Log Subscription**.

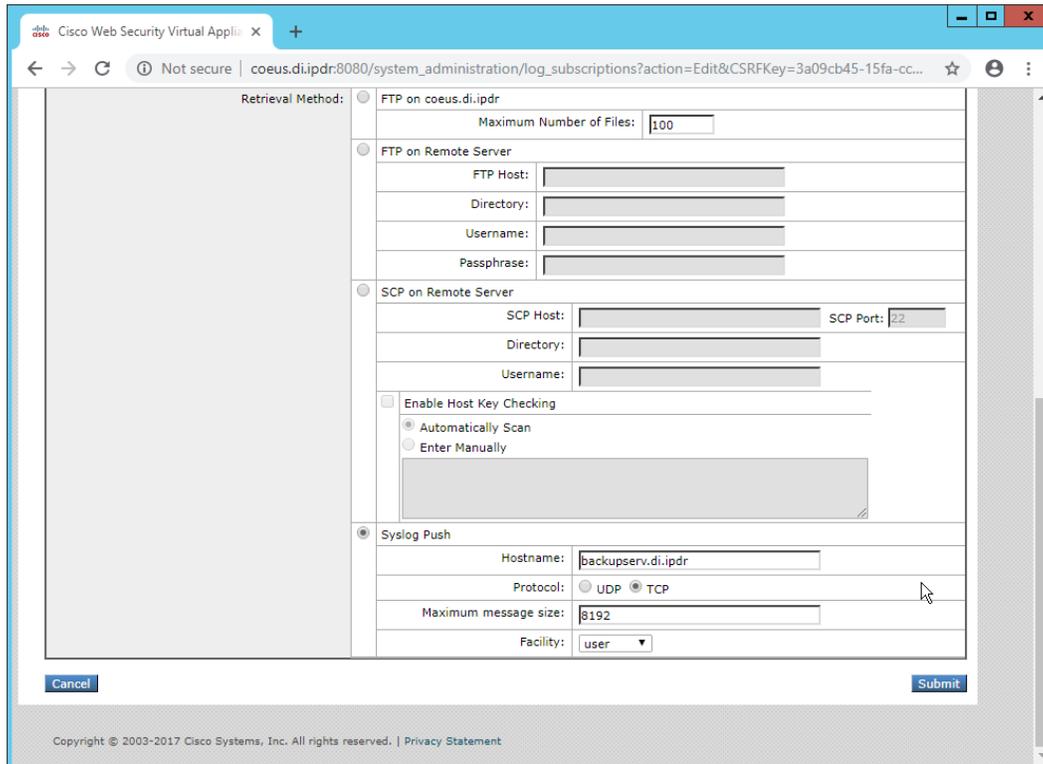
3113 3. Select **Access Logs for Log Type**. (These are the logs of client web requests that have gone  
 3114 through the proxy.)

3115 4. Enter a **name** for **Log Name**.

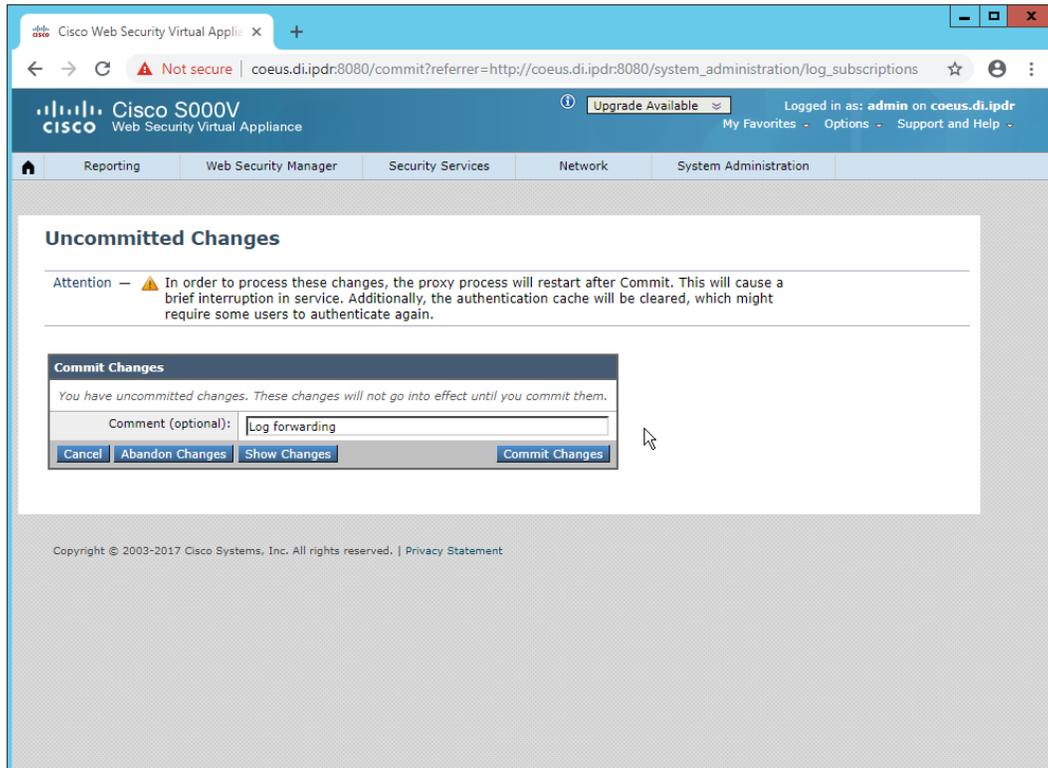
The screenshot shows the 'New Log Subscription' configuration page in the Cisco S000V Web Security Virtual Appliance. The page is titled 'New Log Subscription' and contains a form with the following fields and values:

- Log Type:** Access Logs
- Log Name:** Access Logs ArcSight Forwarding (will be used to name the log directory)
- Rollover by File Size:** 100M Maximum (Add a trailing K or M to indicate size units)
- Rollover by Time:** None
- Log Style:** Squid (selected), Apache, Squid Details
- Custom Fields (optional):** (empty field) Custom Fields Reference
- File Name:** aclog
- Log Compression:** Enable
- Log Exclusions (Optional):** (empty field) (Enter the HTTP status codes of transactions that should not be included in the Access Log)
- Retrieval Method:**
  - FTP on coeus.di.ipdr
    - Maximum Number of Files: 100
  - FTP on Remote Server
    - FTP Host: (empty field)

- 3116 5. Select **Syslog Push**.
- 3117 6. Enter the **hostname** of the ArcSight syslog collector server.
- 3118 7. Select **TCP**. (Ensure that your syslog collector server is configured to use TCP.)
- 3119 8. Enter **8192** or a custom message-size limit.



- 3120 9. Click **Submit**.
- 3121 10. Click **Commit Changes**.
- 3122 11. Enter a **comment** if desired.



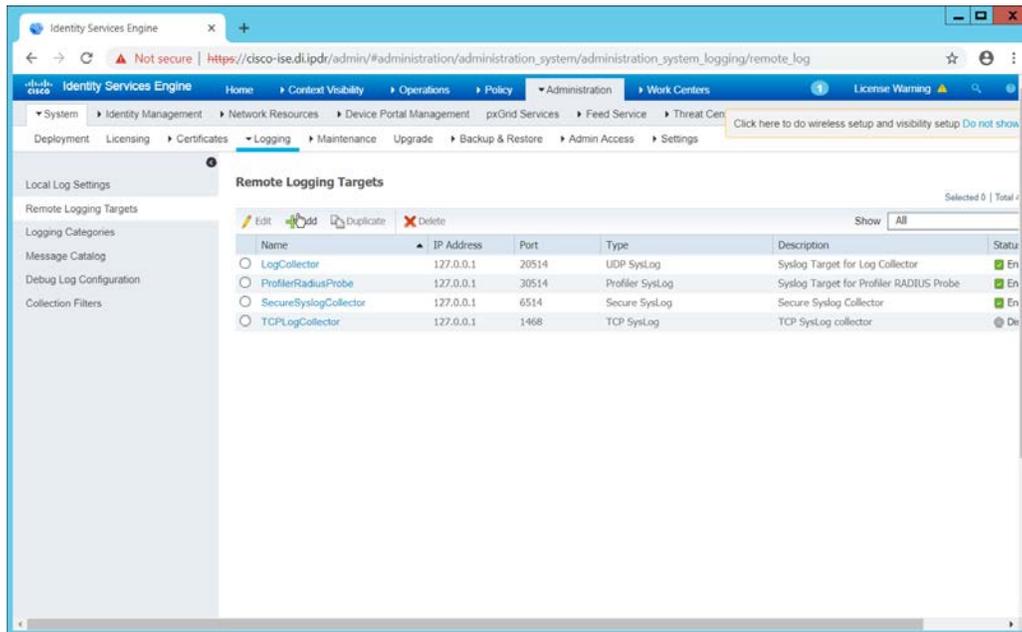
- 3123 12. Click **Commit Changes**. The server will restart, so the web page connection will be temporarily  
 3124 lost.

## 3125 2.26 Integration: Micro Focus ArcSight and Cisco ISE

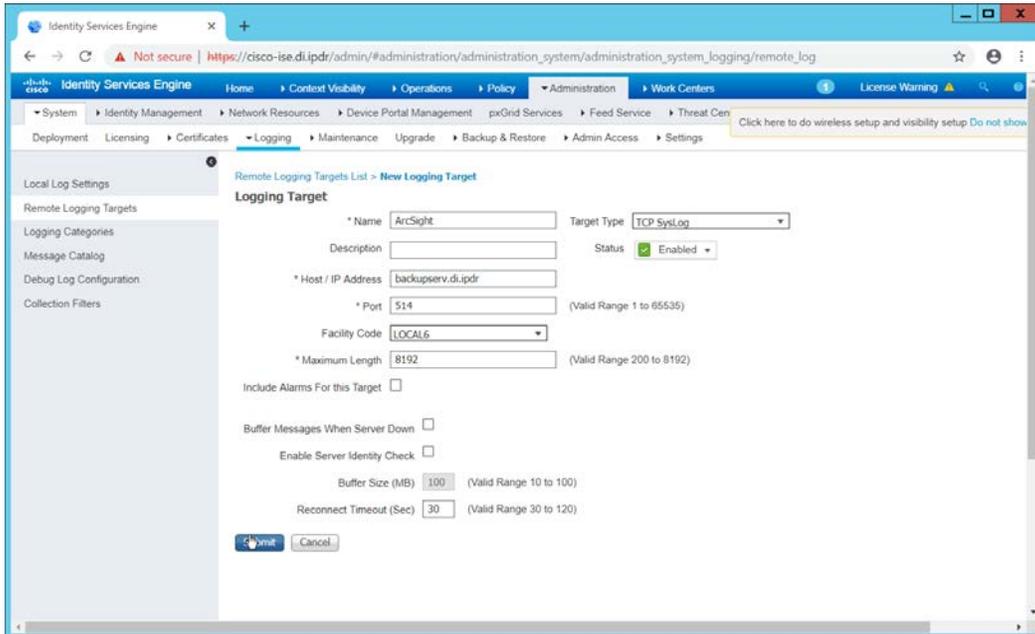
3126 This integration briefly details how to send logs to an ArcSight syslog collector from Cisco ISE. Please see  
 3127 Section 2.24 for instructions for setting up an ArcSight syslog collector. If a server is already configured,  
 3128 you do not need to install a new one—simply forward logs to the address of that server.

### 3129 2.26.1 Configure Cisco ISE to Forward Logs

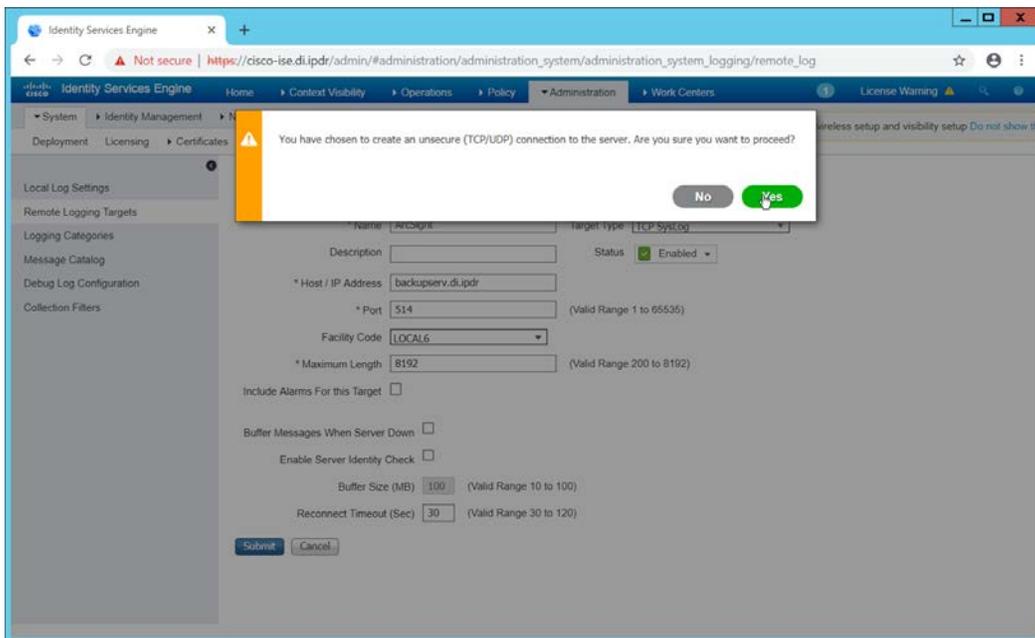
- 3130 1. In the Cisco ISE web client, navigate to **Administration > System > Logging > Remote Logging**  
 3131 **Targets**.



- 3132 2. Click **Add**.
- 3133 3. Enter a **Name**.
- 3134 4. Enter the **hostname** of the ArcSight syslog collector server for **Host/IP Address**.
- 3135 5. Select **TCP SysLog** for Target Type. (Ensure that your syslog collector server is configured to use
- 3136 TCP.)
- 3137 6. Enter **514** or the port used on the syslog server.
- 3138 7. Enter **8192** or a custom message-size limit for **Maximum Length**.
- 3139 8. Ensure that **Status** is set to **Enabled**.



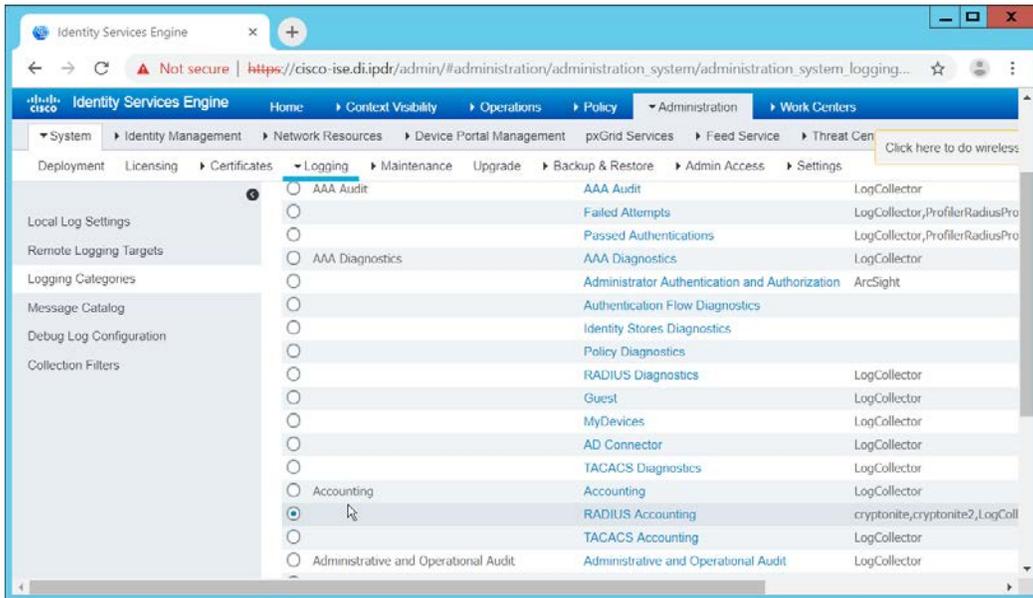
3140 9. Click **Submit**.



3141 10. Click **Yes**.

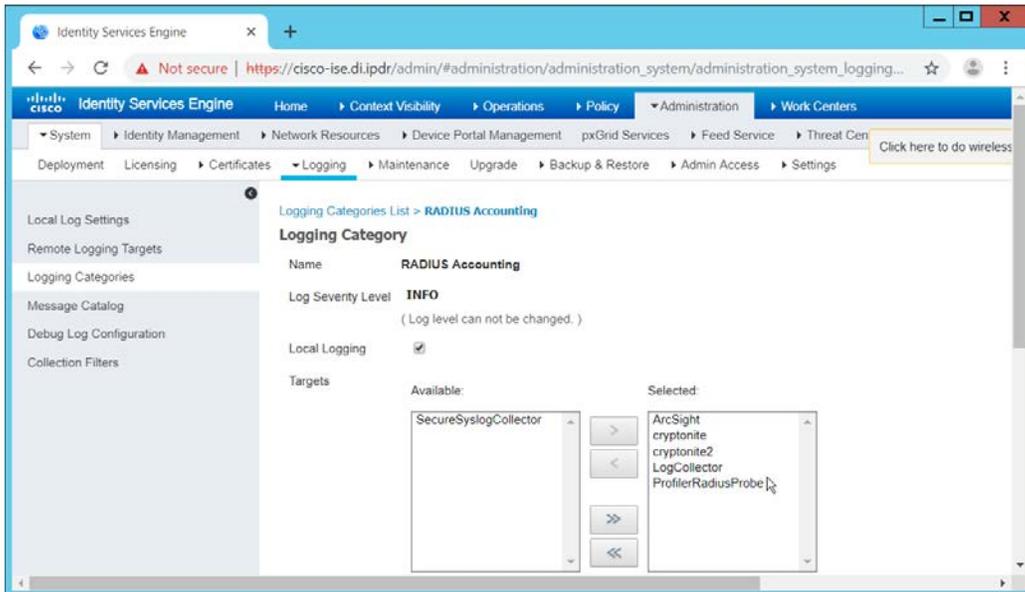
3142 2.26.2 Select Logs for Forwarding

- 3143 1. Navigate to **System > Logging > Logging Categories**.

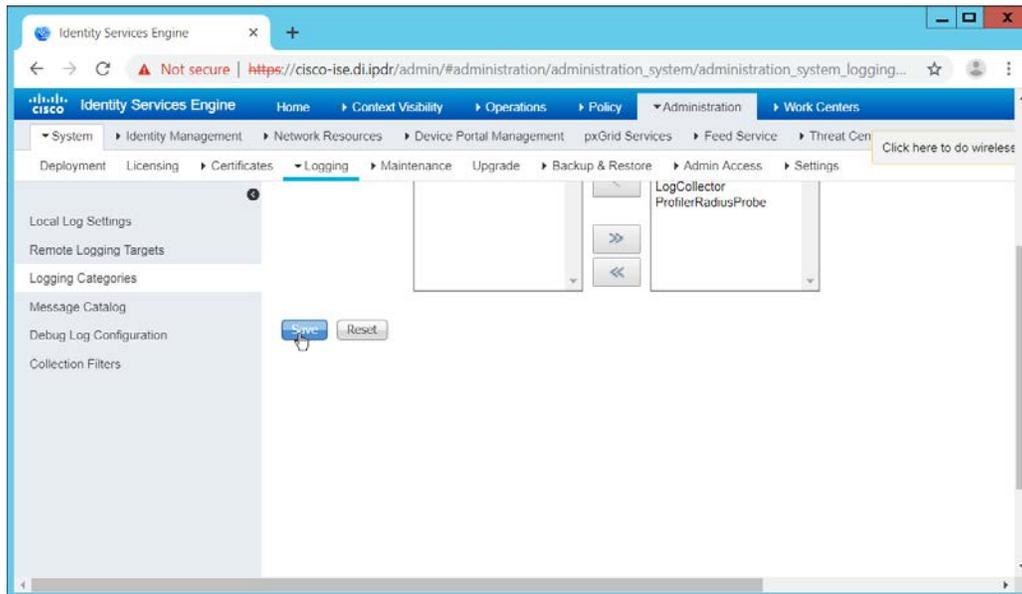


- 3144 2. Select a log file to forward to ArcSight.

- 3145 3. Click **Edit**.



- 3146 4. Move the ArcSight logging target you just created to the **Selected** box.



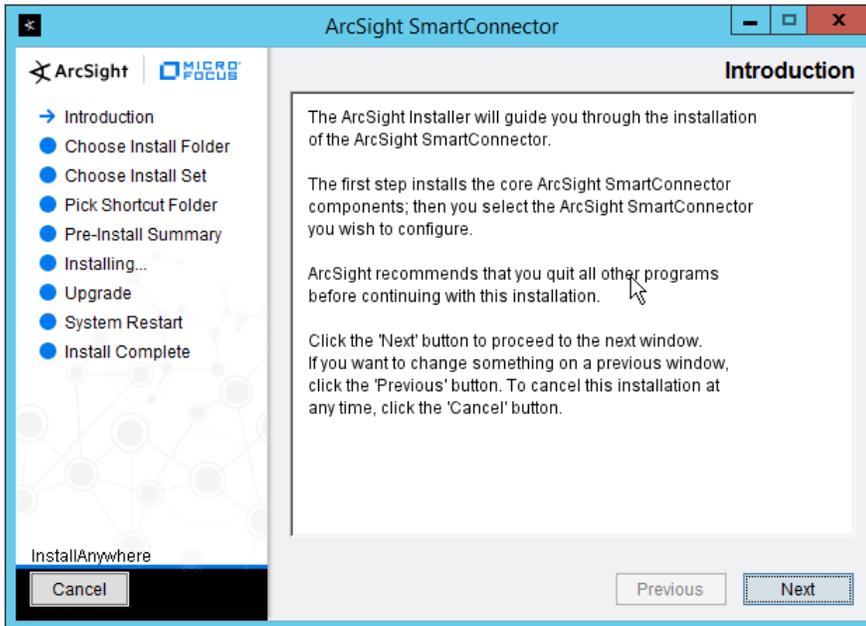
- 3147 5. Click **Save**.
- 3148 6. Repeat steps 1–5 for any log files you wish to forward to ArcSight.

## 3149 2.27 Integration: Micro Focus ArcSight and Symantec DLP

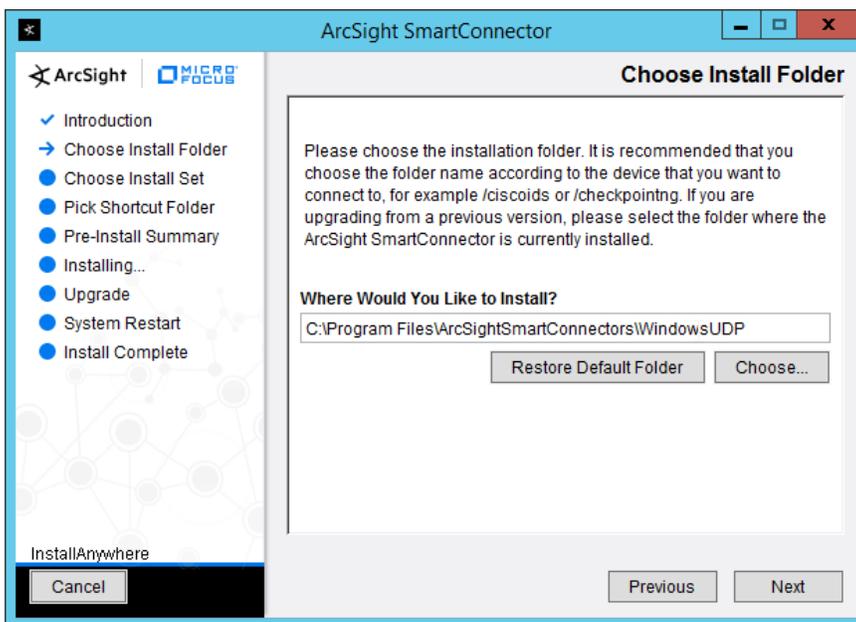
3150 This integration briefly details how to send logs to an ArcSight syslog collector from Symantec DLP. If a  
 3151 server is already configured, you do not need to install a new one—simply forward logs to the address of  
 3152 that server. It is important to note that DLP requires a UDP server, so a TCP syslog server will not work.

### 3153 2.27.1 Install Micro Focus ArcSight

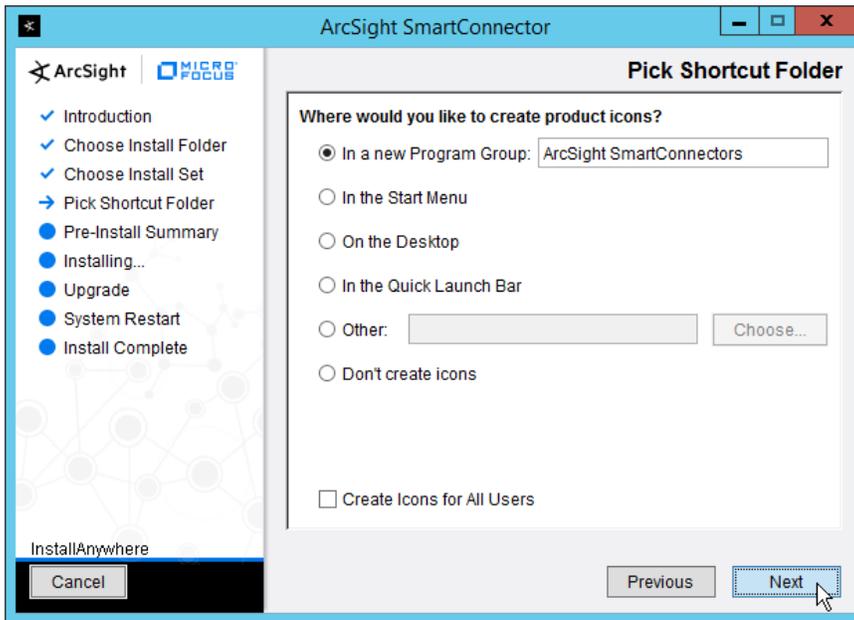
- 3154 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running Cisco  
 3155 Stealthwatch.



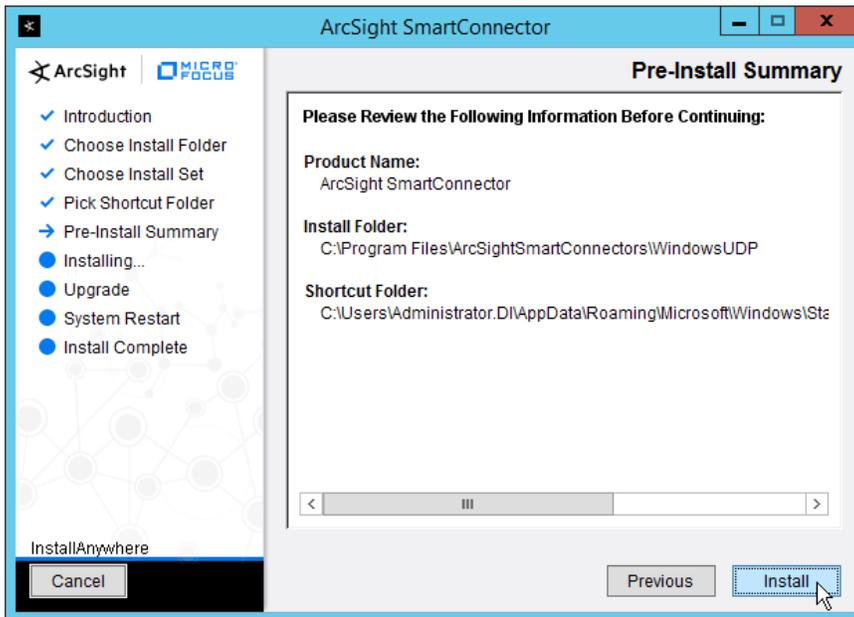
- 3156 2. Click **Next**.
- 3157 3. Enter C:\Program Files\ArcSightSmartConnectors\WindowsUDP.



- 3158 4. Click **Next**.

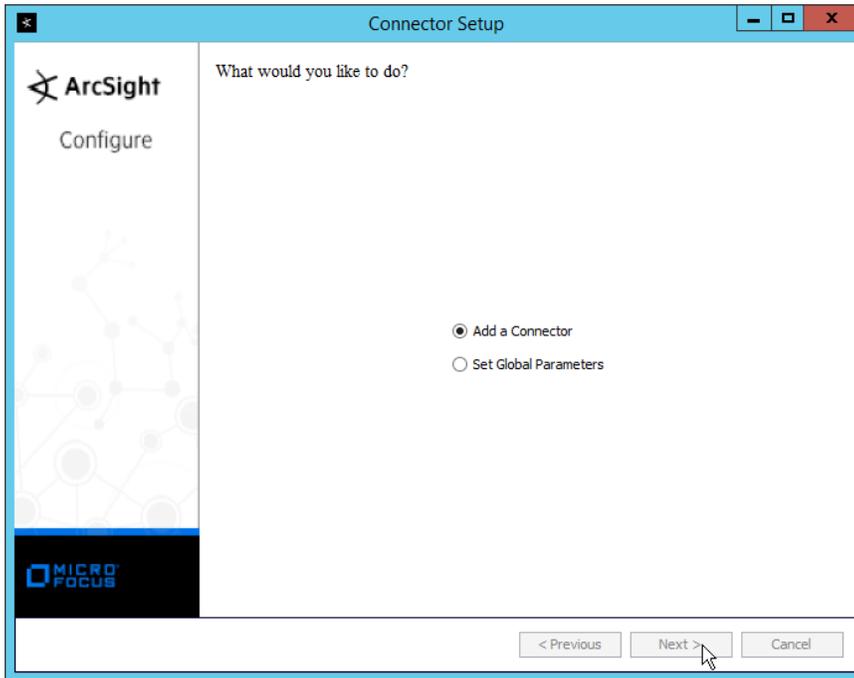


3159 5. Click **Next**.

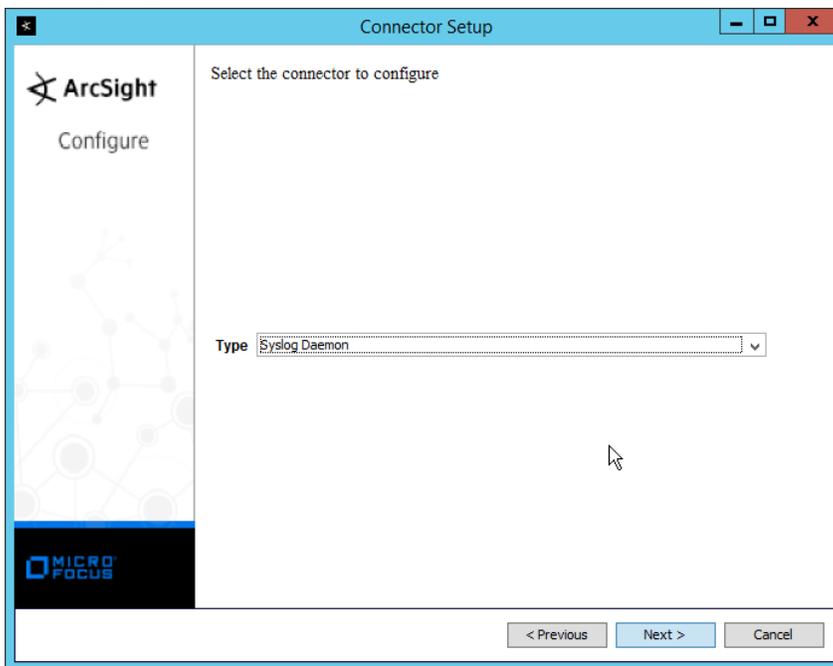


3160 6. Click **Install**.

3161 7. Select **Add a Connector**.

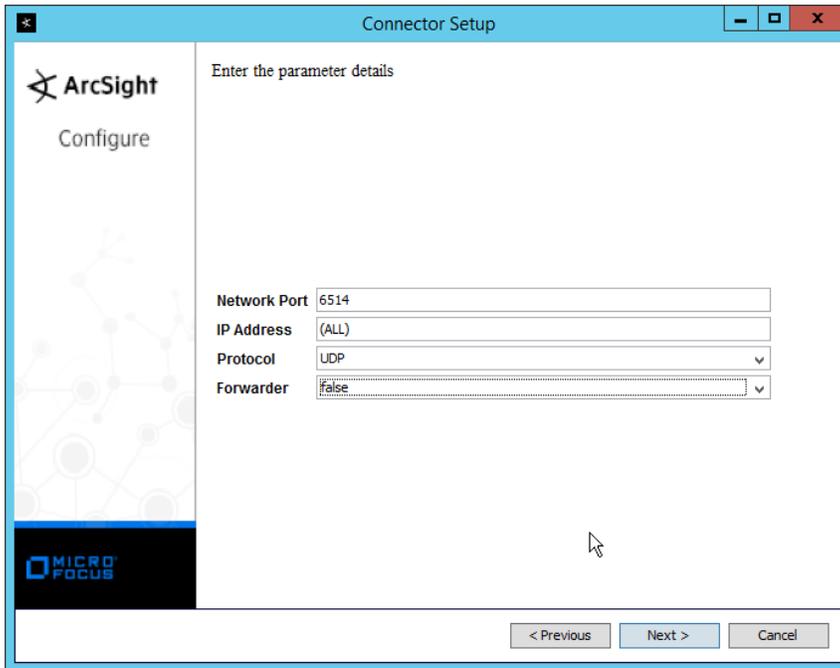


- 3162 8. Click **Next**.
- 3163 9. Select **Syslog Daemon**.

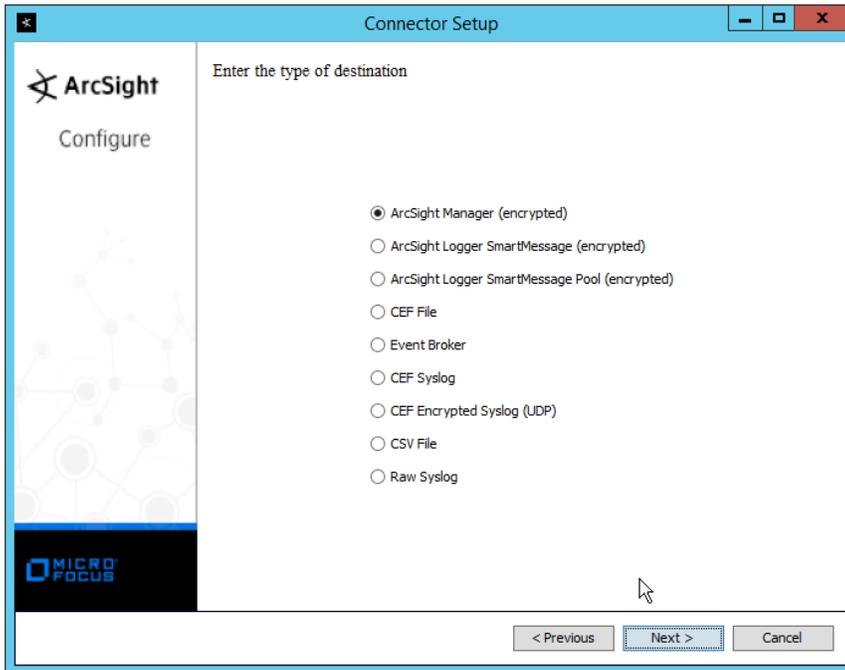


- 3164 10. Click **Next**.

- 3165 11. Enter an unused port on which the daemon can run. (Ensure that this port is allowed through
- 3166 the firewall.)
- 3167 12. Select **UDP** for Protocol.

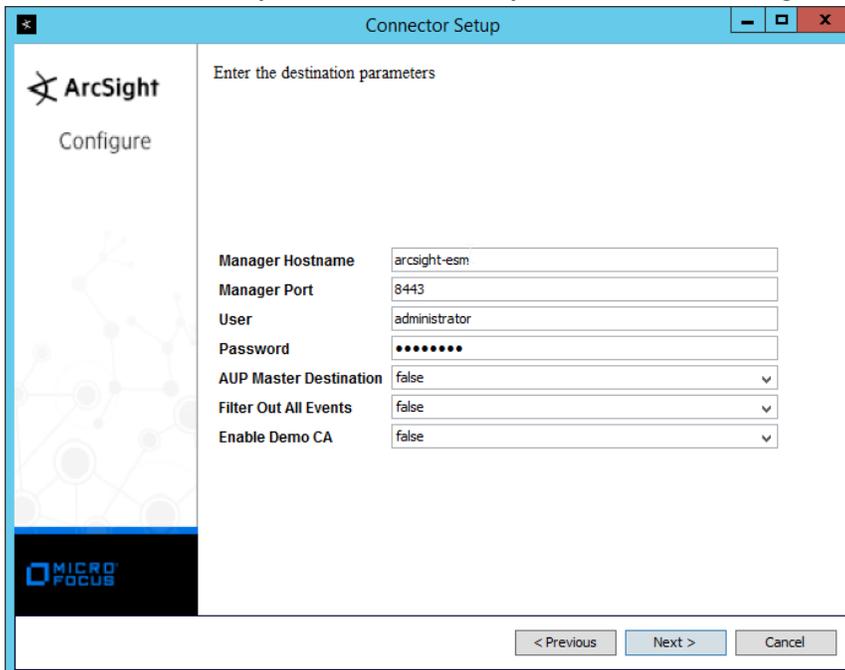


- 3168 13. Click **Next**.
- 3169 14. Select **ArcSight Manager (encrypted)**.



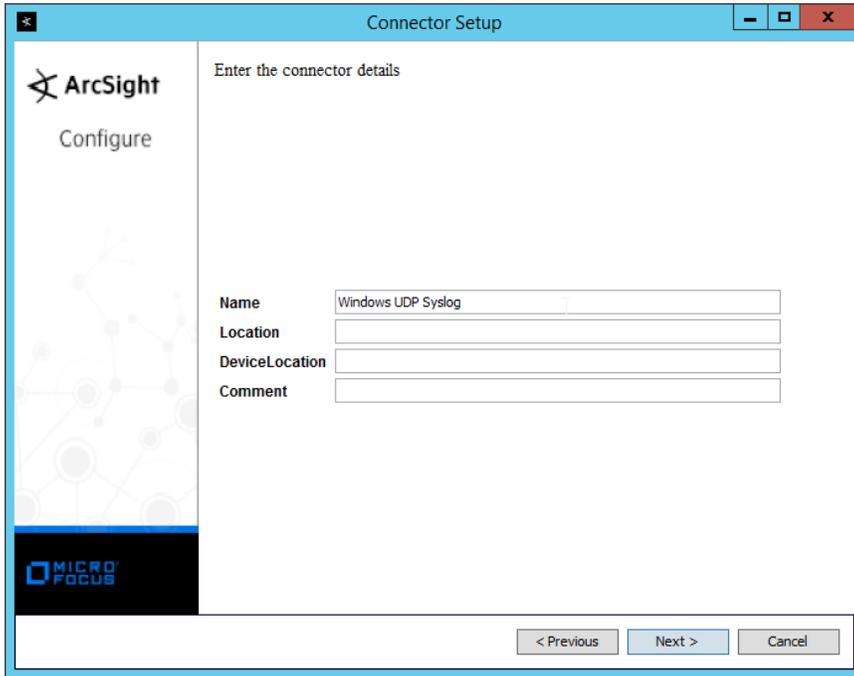
3170 15. Click **Next**.

3171 16. Enter the **hostname, port, username, and password** for the ArcSight ESM server.



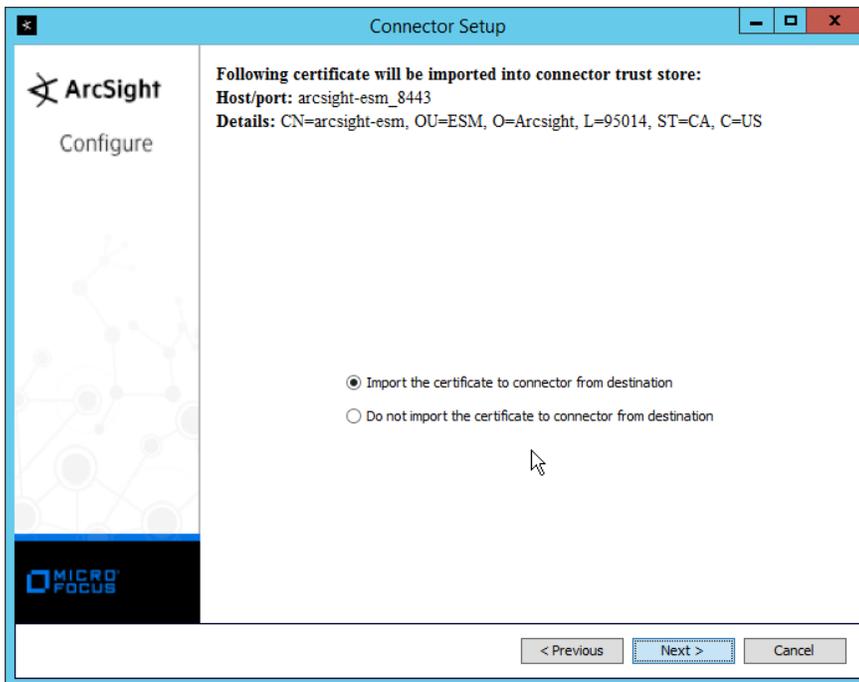
3172 17. Click **Next**.

3173 18. Enter identifying details about the system (only **Name** is required).

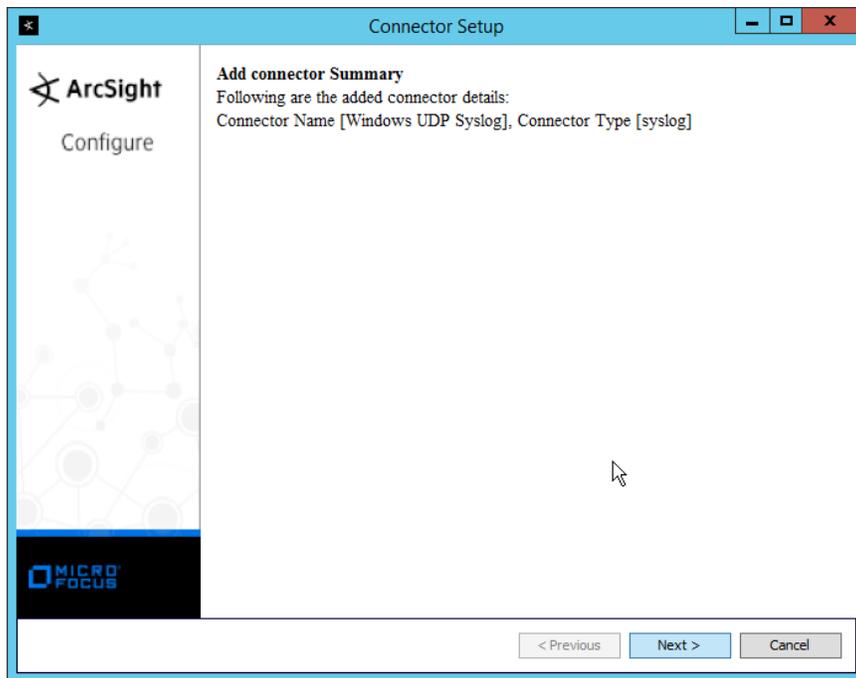


3174 19. Click **Next**.

3175 20. Select **Import the certificate to connector from destination**.

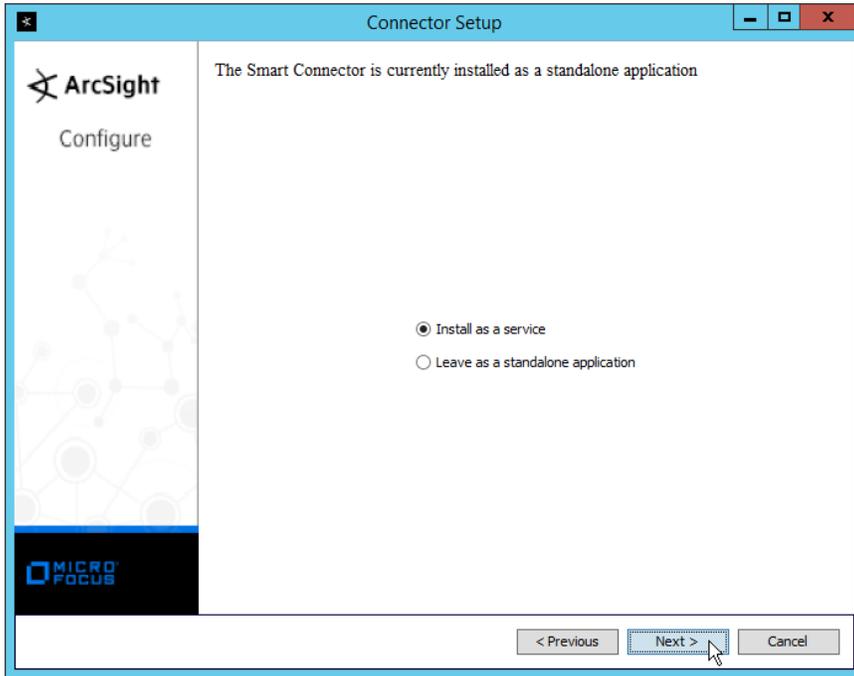


3176 21. Click **Next**.



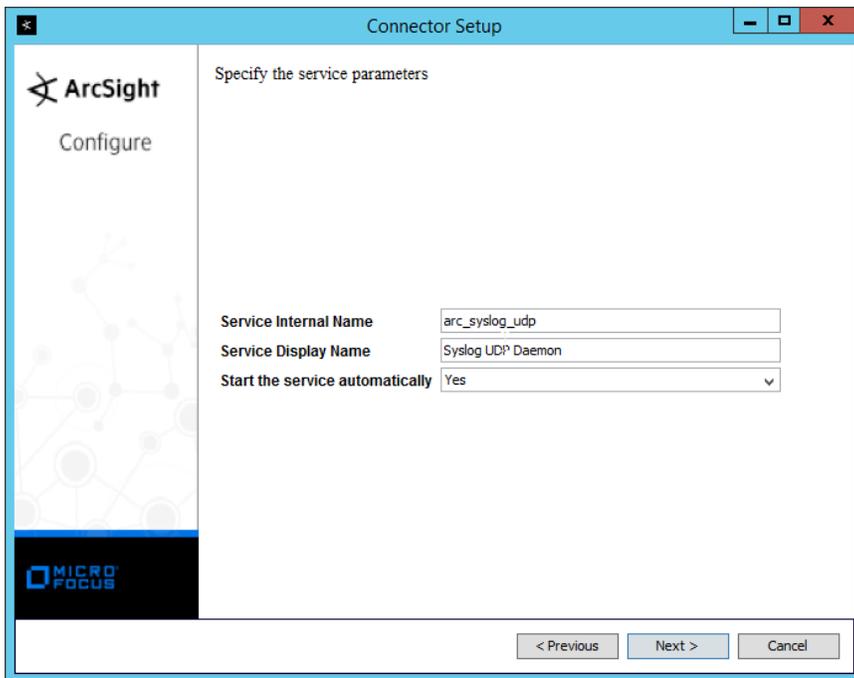
3177 22. Click **Next**.

3178 23. Select **Install as a service**.

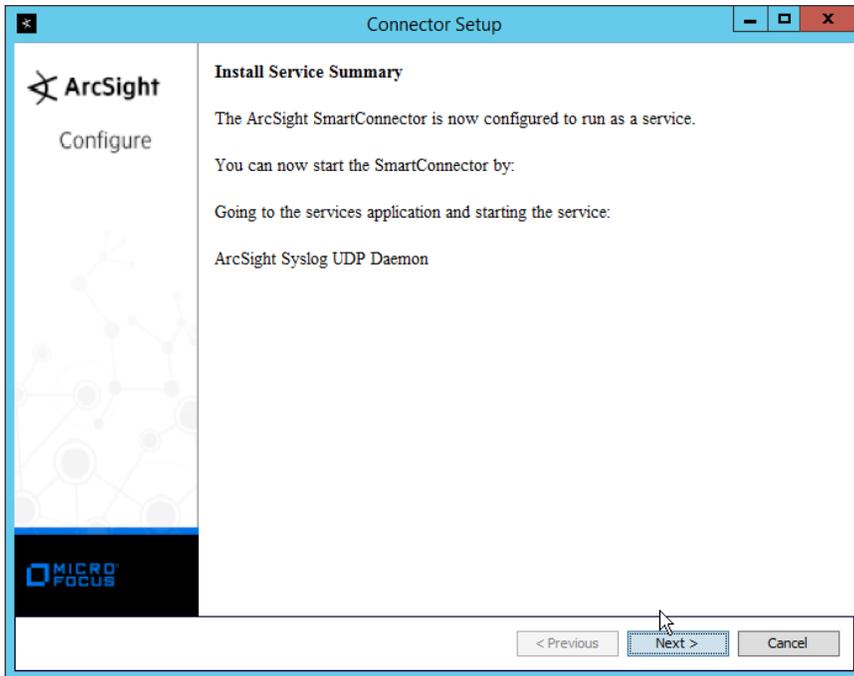


3179 24. Click **Next**.

3180 25. Enter a **service name** and **display name**.

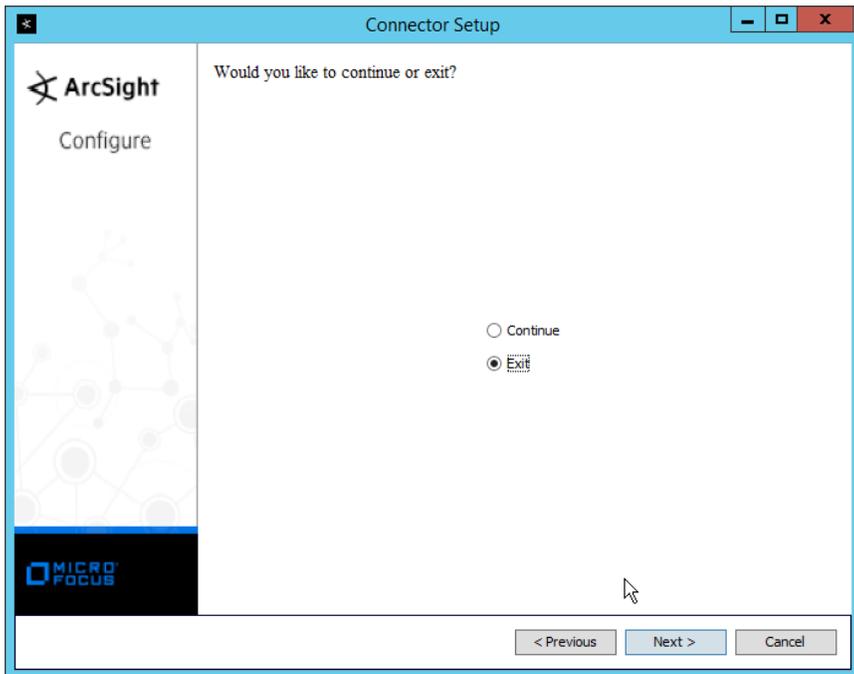


3181 26. Click **Next**.

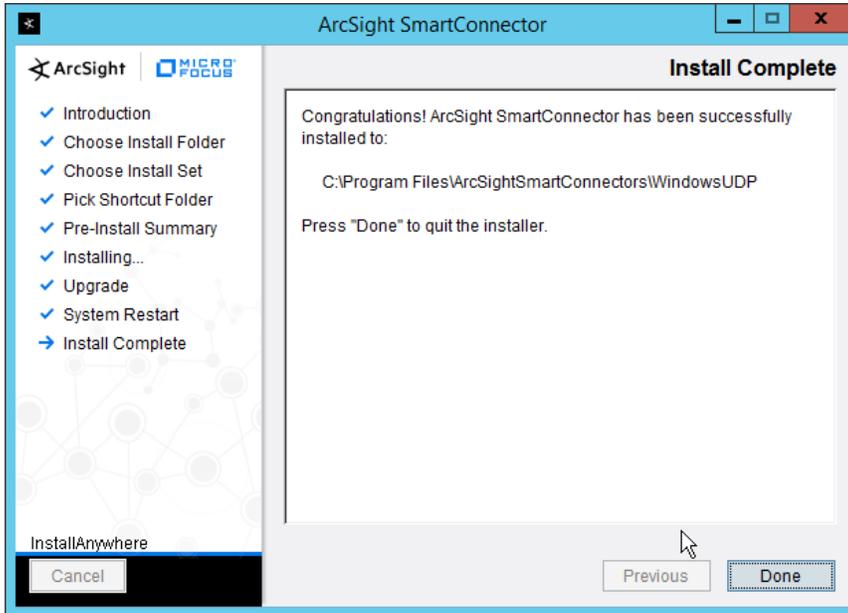


3182 27. Click **Next**.

3183 28. Select **Exit**.



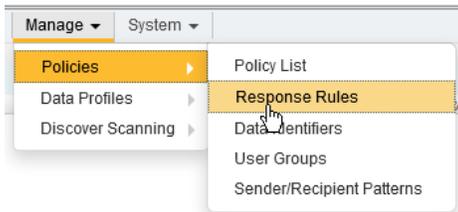
3184 29. Click **Next**.



3185 30. Click **Done**.

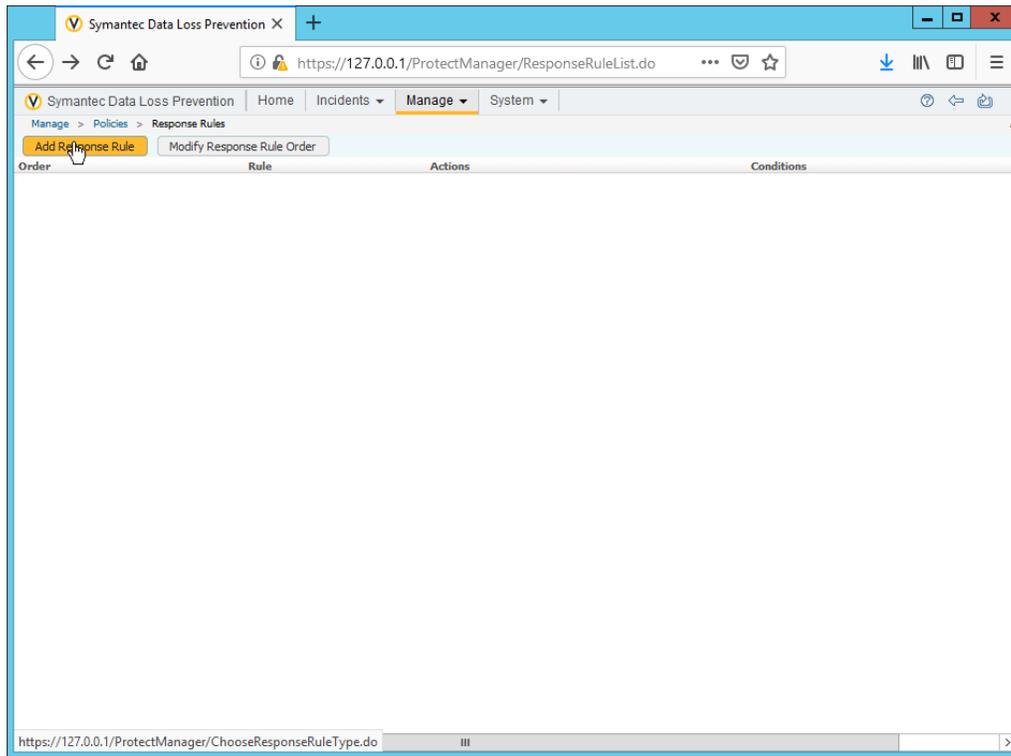
## 3186 2.27.2 Configure Symantec DLP to Forward Logs

3187 1. Log in to the Symantec DLP web console.

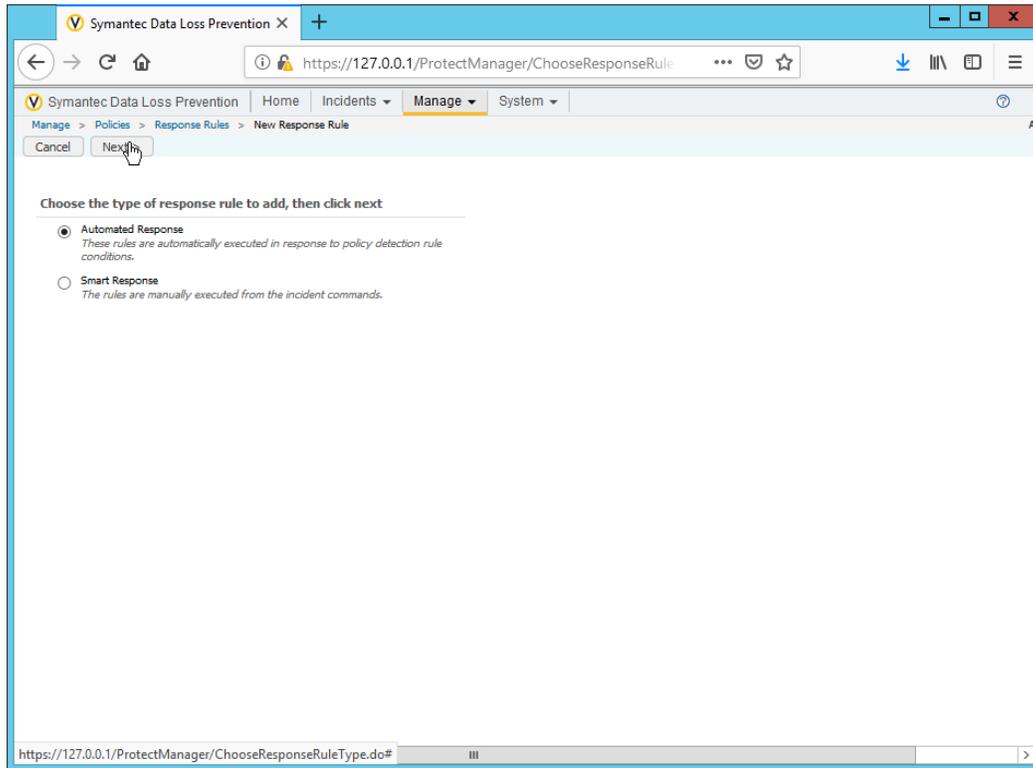


3188 2. Navigate to **Manage > Policies > Response Rules**.

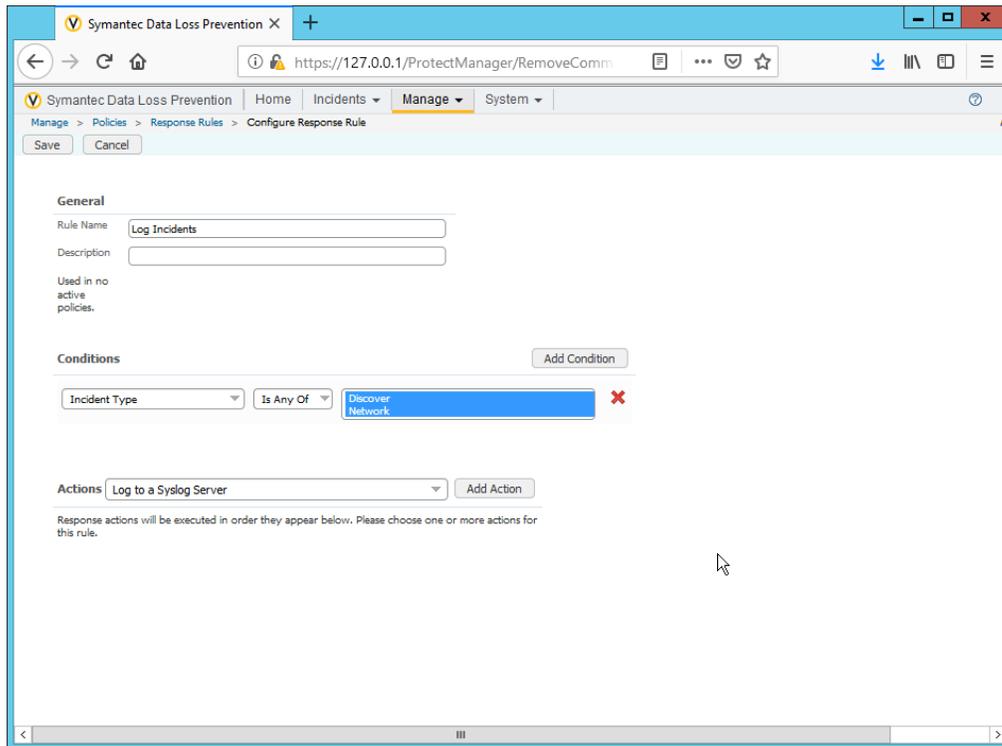
DRAFT



- 3189      3. Click **Add Response Rule**.



- 3190 4. Click **Next**.
- 3191 5. Enter a **name** for the rule.
- 3192 6. Set any conditions for sending syslog messages. If you do not add conditions, all incidents will
- 3193 be forwarded.
- 3194 7. Select **Log to a Syslog Server** for **Actions**.

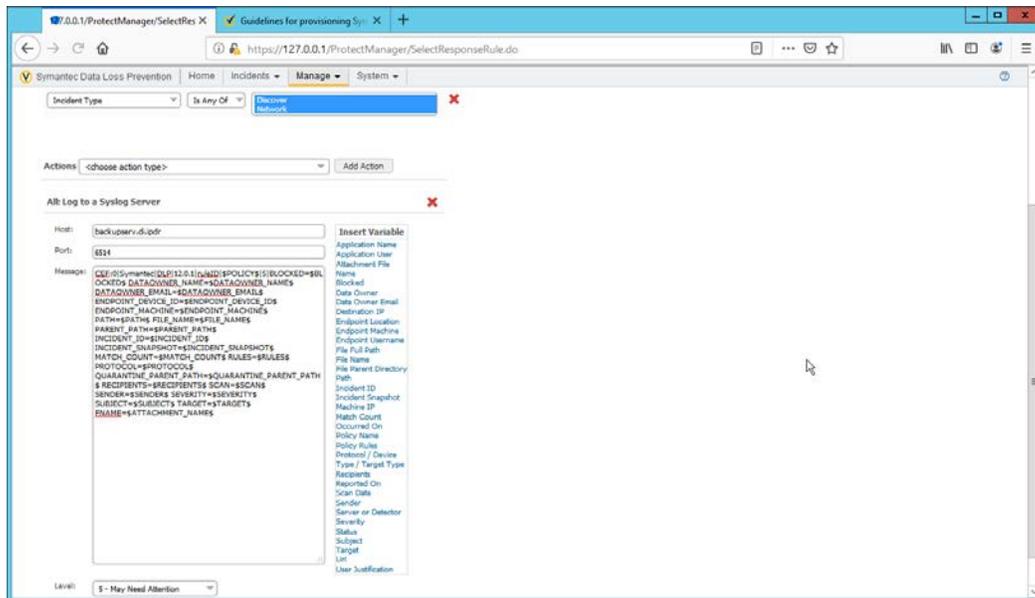


- 3195 8. Click **Add Action**.
- 3196 9. Enter the **IP address** of the ArcSight syslog server.
- 3197 10. Enter the **port** of the ArcSight syslog UDP server.
- 3198 11. Select variables and format a log message to include all the information desired to be sent to
- 3199 the ArcSight server. Below is a sample format for the syslog message, which can potentially be
- 3200 parsed according to the needs of your organization.

```

3201
3202 CEF:0|Symantec|DLP|12.0.1|ruleID|$POLICY$|5|BLOCKED=$BLOCKED$
3203 DATAOWNER_NAME=$DATAOWNER_NAME$ DATAOWNER_EMAIL=$DATAOWNER_EMAIL$
3204 ENDPOINT_DEVICE_ID=$ENDPOINT_DEVICE_ID$
3205 ENDPOINT_MACHINE=$ENDPOINT_MACHINE$ PATH=$PATH$
3206 FILE_NAME=$FILE_NAME$ PARENT_PATH=$PARENT_PATH$
3207 INCIDENT_ID=$INCIDENT_ID$ INCIDENT_SNAPSHOT=$INCIDENT_SNAPSHOT$
3208 MATCH_COUNT=$MATCH_COUNT$ RULES=$RULES$ PROTOCOL=$PROTOCOL$
3209 QUARANTINE_PARENT_PATH=$QUARANTINE_PARENT_PATH$
3210 RECIPIENTS=$RECIPIENTS$ SCAN=$SCAN$ SENDER=$SENDER$
3211 SEVERITY=$SEVERITY$ SUBJECT=$SUBJECT$ TARGET=$TARGET$
3212 FNAME=$ATTACHMENT_NAME$

```



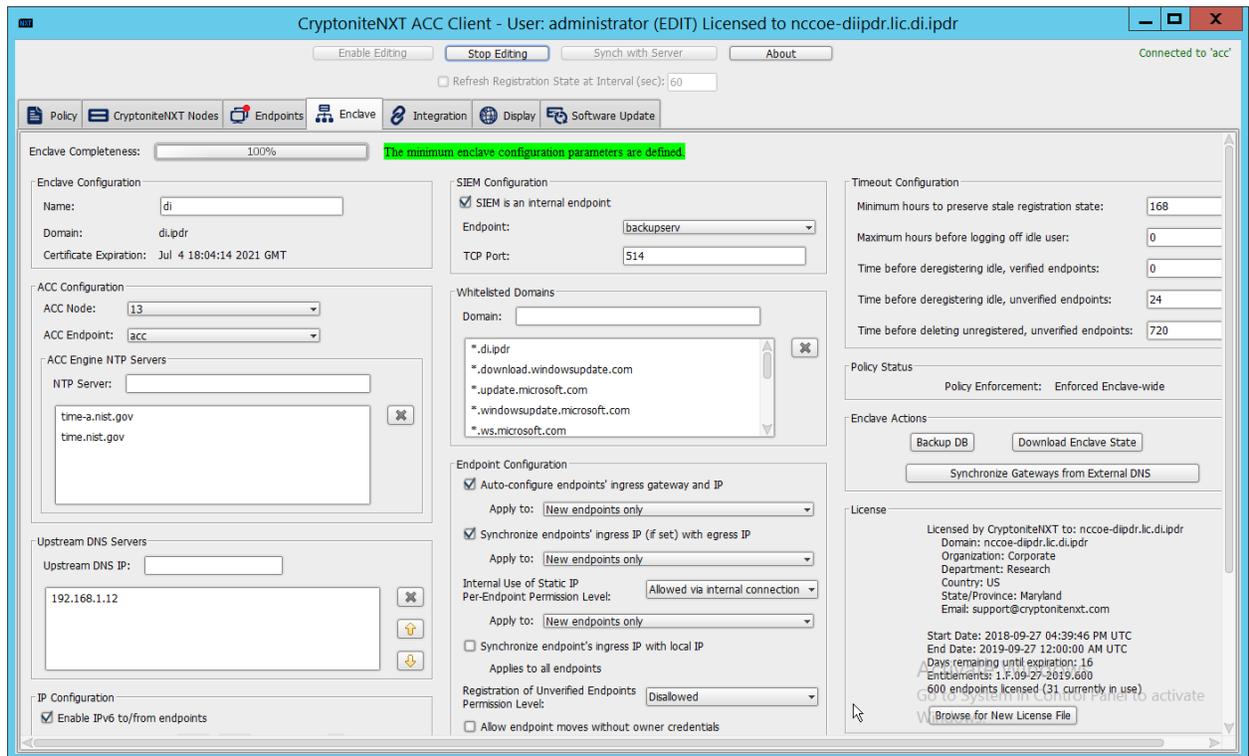
3213 12. Click **Save**.

## 3214 2.28 Integration: Micro Focus ArcSight and CryptoniteNXT

3215 This integration briefly details how to send logs to an ArcSight syslog collector from CryptoniteNXT.  
 3216 Please see Section 2.24 for instructions for setting up an ArcSight syslog collector. If a server is already  
 3217 configured, you do not need to install a new one— simply forward logs to the address of that server.  
 3218 Ensure that you are using a TCP syslog collector. This section assumes that the collector is already under  
 3219 CryptoniteNXT’s network protection.

### 3220 2.28.1 Configure CryptoniteNXT to Forward Logs to ArcSight

- 3221 1. Navigate to the **Enclave** tab in the **CryptoniteNXT ACC GUI**.
- 3222 2. Under **SIEM Configuration**, check the box next to **SIEM is an internal endpoint**.
- 3223 3. Select the endpoint running the TCP syslog collector.
- 3224 4. Enter the port used.



3225 5. Click **Save**.

## 3226 2.29 Integration: Micro Focus ArcSight and Semperis DSP

3227 This integration briefly details how to send logs to an ArcSight syslog collector from Semperis DSP.

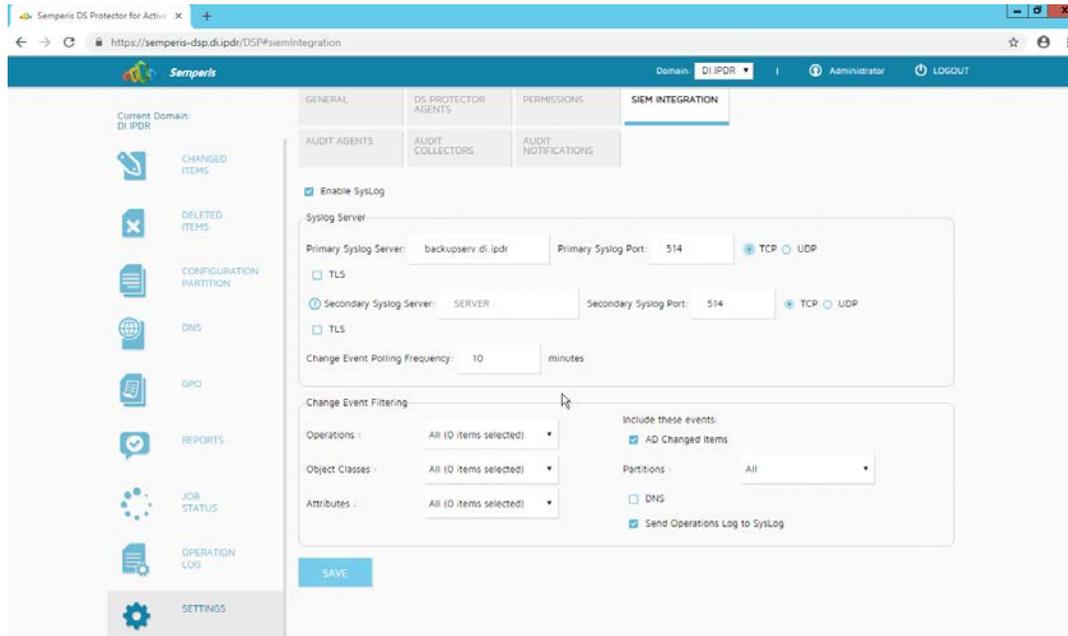
3228 Please see Section 2.24 for instructions for setting up an ArcSight syslog collector. If a server is already  
3229 configured, you do not need to install a new one—simply forward logs to the address of that server.

3230 Note: This integration requires Semperis DSP version 2.6.

### 3231 2.29.1 Configure Semperis DSP to Forward Logs

- 3232 1. In Semperis DSP, navigate to **Settings > SIEM Integration**.
- 3233 2. Check the box next to **Enable SysLog**.
- 3234 3. Under **Syslog Server**, enter the **hostname** for the ArcSight syslog collector, as well as the **port**.
- 3235 4. Select **TCP**.
- 3236 5. Enter a value for **Change Event Polling Frequency** based on the needs of your organization— this  
3237 is how often it will poll for new logs to forward.

- 3238 6. Under **Change Event Filtering**, select **AD Changed Items**, and **Send Operation Log to SysLog**.  
 3239 Ensure that **All** is selected for **Partitions**.  
 3240 7. You can also select any specific **operations**, **classes**, and **attributes** to be forwarded or simply  
 3241 leave as **All**.



- 3242 8. Click **Save**.



- 3243 9. Click **Close**.

### 3244 2.30 Integrations: CryptoniteNXT

3245 For the architecture, it is necessary to create the following source groups. If your organization’s desired  
 3246 architecture is different from the one described in this document, it is necessary to adapt the following  
 3247 instructions to avoid loss of network or security function. This section will describe the creation of  
 3248 source groups and destination groups used in this enterprise.

3249 Create the following destination groups and source groups and apply them to the correct endpoints to  
 3250 allow these products and integrations to communicate under CryptoniteNXT.

### 3251 2.30.1 Active Directory and DNS

3252 This guide assumes the use of Active Directory and DNS on the same Windows 2012 server. The  
 3253 following ports may vary for other products.

Destination Group Name	Source Group Name	Protocol	Port Range
ad-dns	ad-dns-clients	TCP	389
ad-dns	ad-dns-clients	UDP	389
ad-dns	ad-dns-clients	UDP	53
ad-dns	ad-dns-clients	TCP	88
ad-dns	ad-dns-clients	UDP	88
ad-dns	ad-dns-clients	TCP	25
ad-dns	ad-dns-clients	TCP	42
ad-dns	ad-dns-clients	TCP	137
ad-dns	ad-dns-clients	TCP	139
ad-dns	ad-dns-clients	TCP	53
ad-dns	ad-dns-clients	TCP	636
ad-dns	ad-dns-clients	TCP	3268:3269
ad-dns	ad-dns-clients	TCP	445
ad-dns	ad-dns-clients	UDP	445
ad-dns	ad-dns-clients	TCP	9389
ad-dns	ad-dns-clients	TCP	5722
ad-dns	ad-dns-clients	TCP	464
ad-dns	ad-dns-clients	UDP	464
ad-dns	ad-dns-clients	UDP	123
ad-dns	ad-dns-clients	UDP	137:138
ad-dns	ad-dns-clients	UDP	67
ad-dns	ad-dns-clients	UDP	2535
ad-dns	ad-dns-clients	UDP	49152:65535
ad-dns	ad-dns-clients	TCP	49152:65535

Endpoint	Source Groups	Destination Groups
(all endpoints that need access to AD/DNS)	ad-dns-clients	
AD/DNS server		ad-dns

### 3254 2.30.2 Microsoft Exchange

3255 This guide assumes the use of Microsoft Exchange. The following ports may vary for other products.

Destination Group Name	Source Group Name	Protocol	Port Range
exchange	exchange-clients	TCP	443
exchange	exchange-clients	TCP	80
exchange	exchange-clients	TCP	25
exchange	exchange-clients	TCP	379
exchange	exchange-clients	TCP	3268:3269
exchange	exchange-clients	TCP	636
exchange	exchange-clients	TCP	143
exchange	exchange-clients	TCP	993
exchange	exchange-clients	TCP	110
exchange	exchange-clients	TCP	995
exchange	exchange-clients	TCP	119
exchange	exchange-clients	TCP	563
exchange	exchange-clients	TCP	465
exchange	exchange-clients	TCP	443691
exchange	exchange-clients	TCP	102
exchange	exchange-clients	TCP	135
exchange	exchange-clients	TCP	389:390
exchange	exchange-clients	TCP	53
exchange	exchange-clients	UDP	53
exchange	exchange-clients	TCP	2525
exchange	exchange-clients	TCP	475

Endpoint	Source Groups	Destination Groups
MS Exchange	exchange-clients	exchange
(all email clients)	exchange-clients	
AD/DNS server	exchange-clients	

### 3256 2.30.3 FileZilla

3257 The default port for FileZilla is 21.

- 3258 1. To determine the ports being used for your instance, open the FileZilla console.
- 3259 2. Navigate to **Edit > Settings > General Settings > Listen on these ports**, and allow any ports listed
- 3260 here.
- 3261 3. If your server listens in passive mode, navigate to **Edit > Settings > Passive mode settings > Use**
- 3262 **custom port range**, and allow any ports listed here.

Destination Group Name	Source Group Name	Protocol	Port Range
FileZilla	BackupClients	TCP	21 (default—see instructions)
FileZilla	BackupClients	TCP	51120-511230 (passive mode—see instructions)

Endpoint	Source Groups	Destination Groups
(any endpoints that need to perform backups)	BackupClients	
FileZilla server		FileZilla

### 3263 2.30.4 GreenTec

3264 If GreenTec is configured to use a FileZilla server, refer to the above section. If GreenTec is configured to

3265 use Windows Network Share, see below for ports required.

Destination Group Name	Source Group Name	Protocol	Port Range
NetworkShare	GreenTecClients	TCP	80
NetworkShare	GreenTecClients	TCP	135-139
NetworkShare	GreenTecClients	TCP	445

Endpoint	Source Groups	Destination Groups
(any endpoints that need access to GreenTec disks)	GreenTecClients	
GreenTec server		NetworkShare

### 3266 2.30.5 Tripwire Enterprise

3267 In Tripwire, the Axon Bridge is used for Tripwire Enterprise to contact endpoints. Therefore, the port  
 3268 5670 must be allowed on endpoints to allow TE to initiate communications. Furthermore, TE requires  
 3269 MSSQL to function, so it must be granted access to that as well.

Destination Group Name	Source Group Name	Protocol	Port Range
TripwireEnterprise	TEClients	TCP	443
TripwireEnterprise	TEClients	TCP	8080
TripwireEnterprise	TEClients	TCP	9898
TripwireEnterprise	TEClients	TCP	1169
TEAxon	TripwireE	TCP	5670
MSSQL	MSSQLClients	TCP	1433

Endpoint	Source Groups	Destination Groups
(any endpoints that need to be monitored by Tripwire Enterprise)	TEClients	TEAxon
Tripwire Enterprise server	TripwireE, MSSQLClients	TripwireEnterprise
MSSQL server		MSSQL

### 3270 2.30.6 ArcSight ESM

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSight	ArcSightConnectors	TCP	8443

Endpoint	Source Groups	Destination Groups
(any endpoints with an ArcSight Connector installed)	ArcSightConnectors	
ArcSight ESM server		ArcSight

### 3271 2.30.7 Cisco ISE

3272 Please see the *CryptoniteNXT Generic RADIUS Integration Guide* for instructions on how ISE should be  
3273 integrated with CryptoniteNXT.

3274 To access the web console for ISE, allow port 443 for any machines that should be able to access the ISE  
3275 administrative console.

3276 To access the portal for ISE, allow port 8443 (default) for any machines that will need to access the  
3277 portal. You can find this value by looking at your portal configuration in ISE.

3278 Furthermore, if RADIUS is configured for the posture integration, you will need to add any ports used in  
3279 RADIUS for both ISE and the internal switch. The default for these is 1812 (Authentication), 1813  
3280 (Accounting), and 1700 (CoA). RADIUS can be TCP or UDP, so you can restrict this to your organization's  
3281 configuration.

Destination Group Name	Source Group Name	Protocol	Port Range
ISE	ISEConsole	TCP	443
ISE	ISEClients	TCP	8443
radius	ISESwitch, ISEServer	TCP	1812
radius	ISESwitch, ISEServer	UDP	1812
radius	ISESwitch, ISEServer	TCP	1813
radius	ISESwitch, ISEServer	UDP	1813
radius	ISESwitch, ISEServer	TCP	1700
radius	ISESwitch, ISEServer	UDP	1700

Endpoint	Source Groups	Destination Groups
(any endpoints that need to do posture under ISE)	ISEClients	

(any endpoints that need to access the ISE web console)	ISEConsole	
ISE server	ISEServer	ISE, radius
(internal switches or RADIUS servers used for ISE Posture)	ISESwitch, ISEClients	radius
Cryptonite ACC Node		radius

### 3282 2.30.8 Semperis DSP

3283 Semperis DSP recommends allowing full network access during the initial database sync. After that, the  
 3284 following ports should be left open for communication.

Destination Group Name	Source Group Name	Protocol	Port Range
dsp	dsp-admin	TCP	443
dsp	dsp-agents	TCP	8903
dsp	dsp-agents	TCP	135
dsp	dsp-agents	TCP	445
dsp	dsp-agents	TCP	1024:1034
ad-dsp	dsp-client	TCP	8772
ad-dsp	dsp-client	TCP	8750
ad-dsp	dsp-client	ICMP	0:255

Endpoint	Source Groups	Destination Groups
(any endpoints that need admin access to DSP)	dsp-admin	
Semperis DSP	ad-dns-clients, dsp-client, exchange-clients	dsp
Active Directory server	dsp-agents	ad-dsp

### 3285 2.30.9 Symantec DLP

3286 This largely depends on how distributed the setup of DLP is. See here for a list of ports required by  
 3287 Symantec DLP: <https://support.symantec.com/us/en/article.tech220846.html>.

3288 For this build, we used a single server that contained the database, so only the agents and  
 3289 administrative clients needed to be allowed to communicate through Cryptonite.

Destination Group Name	Source Group Name	Protocol	Port Range
dlp	dlp-admin	TCP	443
dlp	dlp-clients	TCP	10443

### 3290 2.30.10 Cisco WSA

3291 WSA uses a proprietary command line, which means it does not have a way of authenticating to the  
 3292 CryptoniteNXT portal. For devices such as this, there are two options.

- 3293 1. The device can be left outside CryptoniteNXT.
- 3294 2. The device can be placed under CryptoniteNXT on a CryptoniteNXT Endpoint Node with the  
 3295 portal disabled.

3296 To prevent MAC spoofing, by default Cryptonite pins MAC addresses to the port + VLAN (Virtual LAN) to  
 3297 which a device is connected, so a malicious device connecting to the end-point node with the same  
 3298 MAC as an already connected IP360 would still be required to authenticate. Physical security for the  
 3299 end-point node can further mitigate concerns about MAC spoofing.

3300 If you can find a way to authenticate WSA to CryptoniteNXT or decide to use the disabled portal option  
 3301 with strong physical security, we provide the ports below for integration.

3302 To access the web console for WSA, allow port 8080 for any machines that should be able to access the  
 3303 ISE administrative console.

3304 To access the proxy, allow port 80 and port 3128 for any machines that will need to go through the  
 3305 proxy, which will likely be most clients in the enterprise. Port 80 is for the *wpad.dat* file, and port 3128  
 3306 is for the proxy itself.

Destination Group Name	Source Group Name	Protocol	Port Range
wsa	wsa-clients	TCP	80
wsa	wsa-clients	TCP	3128
wsa	wsa-admin	TCP	8080

Endpoint	Source Groups	Destination Groups
(any endpoints that need to use the proxy to connect to the internet)	wsa-clients	
(any endpoints that need to access the WSA web console)	wsa-admin	
Cisco WSA		wsa

### 3307 2.30.11 Tripwire IP360

3308 IP360 uses a proprietary command line, which means it does not have a way of authenticating to the  
3309 CryptoniteNXT portal. For devices such as this, there are two options.

3310 3. The device can be left outside CryptoniteNXT.

3311 4. The device can be placed under CryptoniteNXT on a CryptoniteNXT Endpoint Node with the  
3312 portal disabled.

3313 To prevent MAC spoofing, by default Cryptonite pins MAC addresses to the port+VLAN to which a  
3314 device is connected, so a malicious device connecting to the end-point node with the same MAC as an  
3315 already connected IP360 would still be required to authenticate. Physical security for the end-point  
3316 node can further mitigate concerns about MAC spoofing.

3317 If you can find a way to authenticate IP360 to CryptoniteNXT or decide to use the disabled portal option  
3318 with strong physical security, we provide the ports below for integration.

3319 To access the web console for IP360, allow port 443 for any machines that should be able to access the  
3320 IP360 administrative console.

3321 IP360 should have access to all ports of the client machines it needs to scan. Another option is to simply  
3322 add IP360 to all the source groups present in your enterprise, and it will give an overview of the  
3323 vulnerabilities of clients on ports that CryptoniteNXT is not actively protecting. Alternatively, you can  
3324 disable policy enforcement temporarily on the CryptoniteNXT Endpoint Node to which IP360 is  
3325 connected, but you should do this only during scans.

Destination Group Name	Source Group Name	Protocol	Port Range
ip360	ip360admin	TCP	443
scantarget	ip360scanner	TCP	1:65535

scantarget	ip360scanner	UDP	1:65535
scantarget	ip360scsanner	ICMP	0:255

Endpoint	Source Groups	Destination Groups
(any endpoints need to access the IP360 web console)	ip360admin	
(any endpoints to be fully scanned by IP360)		scantarget
IP360	ip360scanner	ip360

### 3326 2.30.12 Tripwire Log Center, Tripwire IP360, Tripwire Enterprise, and ArcSight ESM

3327 The guide details an integration among Tripwire IP360, Tripwire Enterprise, Tripwire Log Center, and  
3328 ArcSight ESM. This section describes the ports needed to allow the integrations through Cryptonite.

3329 First, traffic must be allowed from Tripwire Log Center to the MSSQL server. To do this, ensure that  
3330 Tripwire Log Center can access 1433 on the MSSQL server. (Note: Tripwire Enterprise also has access to  
3331 this port, as described above in the Tripwire Enterprise section.)

3332 Then traffic from Tripwire Enterprise to Tripwire Log Center should be allowed on ports 8091 and 1468.

3333 Traffic from IP360 to Tripwire Log Center should be allowed on port 22 for the SFTP (Secure FTP)  
3334 transfer. Also, traffic from Tripwire Log Center to 5670 on Tripwire IP360 should be allowed. If you  
3335 chose to leave IP360 out of the Cryptonite NXT enclave, Tripwire Log Center will need to be able to  
3336 reach it externally.

3337 Traffic from Tripwire Log Center to the machine containing the ArcSight TCP syslog container should be  
3338 allowed on the port configured (in the guide, we use port 514). As a last note, the server running the  
3339 ArcSight syslog connector requires an IP and not a hostname for its integration with Tripwire Log  
3340 Center—you must set a static IP for the connector server in Cryptonite and enter this IP in the  
3341 appropriate place in Tripwire Log Center’s configuration.

Destination Group Name	Source Group Name	Protocol	Port Range
MSSQL	MSSQLClients	TCP	1443
TLC	TLClients	TCP	8091
TLC	TLClients	TCP	1468

TLC	TLCClients	TCP	22
ArcSightTCPSysConn	TCPSysClients	TCP	514
ip360	ip360admin	TCP	5670

Endpoint	Source Groups	Destination Groups
Tripwire Log Center	TCPSysClients, MSSQLClients, ip360admin	TLC
Tripwire Enterprise	TLCClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn
MSSQL		MSSQL
IP360	TLCClients	ip360

### 3342 2.30.13 FileZilla and ArcSight

3343 The guide details an integration between FileZilla and ArcSight ESM to forward logs from FileZilla to  
3344 ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

3345 Because this integration involves the use of an ArcSight Connector directly on the FileZilla server, only  
3346 one port is needed. The FileZilla server should be able to directly communicate with 8443 on the  
3347 ArcSight ESM server.

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSight	ArcSightConnectors	TCP	8443

Endpoint	Source Groups	Destination Groups
FileZilla	ArcSightConnectors	
ArcSight ESM		ArcSight

### 3348 2.30.14 Cisco ISE and ArcSight

3349 The guide details an integration between Cisco ISE and ArcSight ESM to forward logs from ISE to  
3350 ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

3351 Traffic from Cisco ISE to the machine containing the ArcSight TCP syslog container should be allowed on  
3352 the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

3353

Endpoint	Source Groups	Destination Groups
Cisco ISE	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

3354

### 3355 2.30.15 Cisco WSA and ArcSight

3356 The guide details an integration between Cisco WSA and ArcSight ESM to forward logs from WSA to  
3357 ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

3358 Traffic from Cisco WSA to the machine containing the ArcSight TCP syslog container should be allowed  
3359 on the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

3360

Endpoint	Source Groups	Destination Groups
Cisco WSA	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

3361

### 3362 2.30.16 Semperis DSP and ArcSight

3363 The guide details an integration between Semperis DSP and ArcSight ESM to forward logs from DSP to  
3364 ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

3365 Traffic from Semperis DSP to the machine containing the ArcSight TCP syslog container should be  
 3366 allowed on the port configured (in the guide, we use port 514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	TCP	514

3367

Endpoint	Source Groups	Destination Groups
Semperis DSP	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

3368

### 3369 [2.30.17 Symantec DLP and ArcSight](#)

3370 The guide details an integration between Symantec DLP and ArcSight ESM to forward logs from DLP to  
 3371 ArcSight. This section describes the ports needed to allow the integrations through Cryptonite.

3372 Traffic from Symantec DLP to the machine containing the ArcSight UDP syslog container should be  
 3373 allowed on the port configured (in the guide, we use UDP and port 6514).

Destination Group Name	Source Group Name	Protocol	Port Range
ArcSightTCPSysConn	TCPSysClients	UDP	6514

3374

Endpoint	Source Groups	Destination Groups
Symantec DLP	TCPSysClients	
(server running ArcSight TCP syslog connector)		ArcSightTCPSysConn

3375 **Appendix A—List of Acronyms**

<b>ACC</b>	Administration Control Center
<b>AD</b>	Active Directory
<b>ADFR</b>	Active Directory Forest Recovery
<b>CoA</b>	Change of Authorization
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DNS</b>	Domain Name System
<b>DSP</b>	Directory Services Protector
<b>ESM</b>	Enterprise Security Manager
<b>FTP</b>	File Transfer Protocol
<b>FTPS</b>	File Transfer Protocol over TLS
<b>GUI</b>	Graphical User Interface
<b>IIS</b>	Internet Information Services
<b>ISE</b>	Identity Services Engine
<b>IT</b>	Information Technology
<b>JCE</b>	Java Cryptography Extension
<b>JRE</b>	Java Runtime Environment
<b>LAN</b>	Local Area Network
<b>MSSQL</b>	Microsoft SQL
<b>NAT</b>	Network Address Translation
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NIST</b>	National Institute of Standards and Technology
<b>OS</b>	Operating System
<b>PAC</b>	Proxy Auto Config
<b>RADIUS</b>	Remote Authentication Dial-In User Service
<b>SFTP</b>	Secure FTP
<b>SNMP</b>	Simple Network Management Protocol
<b>TE</b>	Tripwire Enterprise
<b>TLC</b>	Tripwire Log Center
<b>VLAN</b>	Virtual LAN
<b>WDV</b>	WORM Disk Volume
<b>WORM</b>	Write Once Read Many
<b>WPAD</b>	Web Proxy Auto Discovery
<b>WSA</b>	Web Security Appliance