

# Data Integrity

## Detecting and Responding to 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/detect-respond>.

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 1800-26C, Natl. Inst. Stand. Technol.  
9 Spec. Publ. 1800-26C, 440 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 mistakes present an ongoing threat  
50 to organizations that manage data in various forms. Database records and structure, system files,  
51 configurations, user files, application code, and customer data are all potential targets of data  
52 corruption and destruction.

53 A quick, accurate, and thorough detection and response to a loss of data integrity can save an  
54 organization time, money, and headaches. While human knowledge and expertise is an essential  
55 component of these tasks, the right tools and preparation are essential to minimizing downtime and

56 losses due to data integrity events. The NCCoE, in collaboration with members of the business  
 57 community and vendors of cybersecurity solutions, has built an example solution to address these data  
 58 integrity challenges. This project details methods and potential tool sets that can detect, mitigate, and  
 59 contain data integrity events in the components of an enterprise network. It also identifies tools and  
 60 strategies to aid in a security team’s response to such an event.

## 61 **KEYWORDS**

62 *attack vector; data integrity; malicious actor; malware; malware detection; malware response;*  
 63 *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
Matthew Shabat	Glasswall Government Solutions
Justin Rowland	Glasswall Government Solutions
Greg Rhein	Glasswall Government Solutions
Steve Roberts	Micro Focus
Timothy McBride	NIST
Christopher Lowde	Semperis

Thomas Leduc	Semperis
Darren Mar-Elia	Semperis
Kirk Lashbrook	Semperis
Mickey Bresman	Semperis
Humphrey Christian	Symantec Corporation
Jon Christmas	Symantec Corporation
Kenneth Durbin	Symantec Corporation
Matthew Giblin	Symantec Corporation
Jim Wachhaus	Tripwire
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
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 Information Centric Analytics v6.5.2 Symantec Security Analytics v8.0.1
Cisco Systems	Cisco Identity Services Engine v2.4, Cisco Advanced Malware Protection v5.4, Cisco Stealthwatch v7.0.0
Glasswall Government Solutions	Glasswall FileTrust ATP for Email v6.90.2.5
Tripwire	Tripwire Log Center v7.3.1, Tripwire Enterprise v8.7
Micro Focus	Micro Focus ArcSight Enterprise Security Manager v7.0 Patch 2
Semperis	Semperis Directory Services Protector v2.7

70	<b>Contents</b>	
71	<b>1 Introduction .....</b>	<b>1</b>
72	1.1 Practice Guide Structure .....	1
73	1.2 Build Overview .....	2
74	1.3 Typographical Conventions.....	3
75	<b>2 Product Installation Guides .....</b>	<b>3</b>
76	2.1 Active Directory and Domain Name System Server.....	3
77	2.1.1 Install Features.....	3
78	2.1.2 Create a Certificate Authority.....	17
79	2.1.3 Configure Account to Add Computers to Domain.....	30
80	2.1.4 Add Machines to the Domain .....	36
81	2.1.5 Configure Active Directory to Audit Account Activity .....	41
82	2.1.6 Configure Reverse Lookup Zones .....	43
83	2.2 Microsoft Exchange Server.....	48
84	2.2.1 Install Microsoft Exchange.....	49
85	2.3 Windows Server Hyper-V Role .....	59
86	2.3.1 Production Installation .....	59
87	2.4 MS SQL Server .....	65
88	2.4.1 Install and Configure MS SQL.....	65
89	2.4.2 Open Port on Firewall.....	73
90	2.4.3 Add a New Login to the Database .....	78
91	2.5 Microsoft IIS Server .....	80
92	2.5.1 Install IIS.....	80
93	2.5.2 IIS Configuration .....	87
94	2.6 Semperis Directory Services Protector .....	91
95	2.6.1 Configure Active Directory for Semperis DSP .....	91
96	2.6.2 Install Semperis DSP .....	103
97	2.6.3 Roll Back Changes with Semperis DSP .....	116
98	2.6.4 Configure Reporting with Semperis DSP .....	117

99	2.6.5	Configure Email Alerts with Semperis DSP .....	118
100	2.7	Glasswall FileTrust™ for Email .....	120
101	2.7.1	Install Prerequisites .....	120
102	<b>2.7.1.1</b>	<b>Install the IIS web server .....</b>	<b>120</b>
103	<b>2.7.1.2</b>	<b>Install Microsoft SQL 2014 Enterprise .....</b>	<b>122</b>
104	<b>2.7.1.3</b>	<b>Install Microsoft Visual C++ 2015 .....</b>	<b>122</b>
105	2.7.2	Install the Glasswall FileTrust Server Component .....	124
106	<b>2.7.2.1</b>	<b>Install Glasswall Hub .....</b>	<b>124</b>
107	<b>2.7.2.2</b>	<b>Install Glasswall Integration Service .....</b>	<b>128</b>
108	<b>2.7.2.3</b>	<b>Install Glasswall Administrator Console .....</b>	<b>131</b>
109	<b>2.7.2.4</b>	<b>Add the Server’s Certificate.....</b>	<b>133</b>
110	<b>2.7.2.5</b>	<b>Install the Smtip Analysis Agent .....</b>	<b>147</b>
111	<b>2.7.2.6</b>	<b>Distribute the Glasswall License File .....</b>	<b>149</b>
112	2.7.3	Configure Glasswall FileTrust.....	151
113	<b>2.7.3.1</b>	<b>Create a New Administrator Account.....</b>	<b>152</b>
114	<b>2.7.3.2</b>	<b>Configure Notifications and Policies.....</b>	<b>157</b>
115	<b>2.7.3.3</b>	<b>Configure Inbound SMTP Policy .....</b>	<b>158</b>
116	<b>2.7.3.4</b>	<b>Create a Receiver Group .....</b>	<b>159</b>
117	<b>2.7.3.5</b>	<b>Create a ThreatCensor Policy Set .....</b>	<b>161</b>
118	<b>2.7.3.6</b>	<b>Create a Processing Rule .....</b>	<b>162</b>
119	2.7.4	Configure Intelligence Sharing.....	163
120	2.8	Micro Focus ArcSight Enterprise Security Manager.....	165
121	2.8.1	Install the ArcSight Console .....	165
122	2.8.2	Install Individual ArcSight Windows Connectors.....	179
123	2.8.3	Install Individual ArcSight Ubuntu Connectors.....	197
124	2.8.4	Install a Connector Server for ESM on Windows 2012 R2.....	210

125	2.8.5	Install Pre-Configured Filters for ArcSight .....	221
126	<b>2.8.5.1</b>	<b>Install Activate Base .....</b>	<b>221</b>
127	<b>2.8.5.2</b>	<b>Install Packages.....</b>	<b>223</b>
128	2.8.6	Apply Filters to a Channel.....	224
129	2.8.7	Configure Email Alerts in ArcSight .....	225
130	<b>2.8.7.1</b>	<b>Configure a New Destination .....</b>	<b>225</b>
131	<b>2.8.7.2</b>	<b>Configure a New Rule.....</b>	<b>226</b>
132	2.9	Tripwire Enterprise.....	229
133	2.9.1	Install Tripwire Enterprise.....	230
134	2.9.2	Install the Axon Bridge.....	242
135	2.9.3	Install the Axon Agent (Windows) .....	242
136	2.9.4	Install the Axon Agent (Linux).....	243
137	2.9.5	Configure Tripwire Enterprise.....	244
138	<b>2.9.5.1</b>	<b>Terminology.....</b>	<b>244</b>
139	<b>2.9.5.2</b>	<b>Tags.....</b>	<b>245</b>
140	<b>2.9.5.3</b>	<b>Rules .....</b>	<b>247</b>
141	<b>2.9.5.4</b>	<b>Tasks .....</b>	<b>251</b>
142	2.10	Tripwire Log Center .....	254
143	2.10.1	Install Tripwire Log Center Manager .....	254
144	2.10.2	Configure Tripwire Log Center Manager .....	255
145	2.10.3	Install Tripwire Log Center Console .....	260
146	2.11	Cisco Identity Services Engine .....	261
147	2.11.1	Initial Setup .....	261
148	2.11.2	Inventory: Configure SNMP on Routers/Network Devices.....	261
149	2.11.3	Inventory: Configure Device Detection .....	261
150	2.11.4	Policy Enforcement: Configure Active Directory Integration .....	265
151	2.11.5	Policy Enforcement: Enable Passive Identity with AD .....	268
152	2.11.6	Policy Enforcement: Developing Policy Conditions .....	273

153	2.11.7 Policy Enforcement: Developing Policy Results.....	274
154	2.11.8 Policy Enforcement: Enforcing a Requirement in Policy .....	275
155	2.11.9 Policy Enforcement: Configuring a Web Portal .....	276
156	2.11.10 Configuring RADIUS with your Network Device .....	277
157	2.11.11 Configuring an Authentication Policy .....	278
158	2.11.12 Configuring an Authorization Policy .....	279
159	<b>2.12 Cisco Advanced Malware Protection .....</b>	<b>280</b>
160	2.12.1 Dashboard Configuration.....	280
161	2.12.2 Installing the Connector on a Windows Server .....	281
162	2.12.3 Installing the Connector on a Windows 10 Machine.....	282
163	2.12.4 Scanning using AMP.....	283
164	2.12.5 Configure AMP Policy .....	284
165	<b>2.13 Cisco Stealthwatch .....</b>	<b>286</b>
166	2.13.1 Configure Stealthwatch Flow Collector, Stealthwatch Management Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor .....	286
167		
168	2.13.2 Change Default Stealthwatch Console Passwords .....	291
169	2.13.3 Configure the Stealthwatch Management Console Web Interface .....	295
170	2.13.4 Configure the Stealthwatch UDP Director, Stealthwatch Flow Collector and Stealthwatch Flow Sensor Web Interfaces .....	298
171		
172	<b>2.14 Symantec Analytics.....</b>	<b>301</b>
173	2.14.1 Initial Setup.....	301
174	2.14.2 Capturing Data .....	307
175	<b>2.15 Symantec Information Centric Analytics.....</b>	<b>308</b>
176	2.15.1 Installing MS SQL 2017 .....	308
177	2.15.2 Install Windows Services .....	316
178	2.15.3 Installing Symantec ICA.....	324
179	2.15.4 Configuring Symantec ICA for Analysis.....	331

180	<b>2.15.4.1</b>	<b>Installing Integration Packs .....</b>	<b>331</b>
181	<b>2.15.4.2</b>	<b>Create a View .....</b>	<b>332</b>
182	<b>2.15.4.3</b>	<b>Open an Existing View.....</b>	<b>333</b>
183	<b>2.15.4.4</b>	<b>Viewing Detailed Analyzer Data .....</b>	<b>335</b>
184	2.16	Integration: Cisco Identity Services Engine and Cisco Stealthwatch .....	335
185	2.16.1	Configuring Certificates for pxGrid .....	335
186	2.16.2	Configuring Stealthwatch to Quarantine through ISE .....	347
187	2.17	Integration: Tripwire Log Center and Tripwire Enterprise.....	352
188	2.18	Integration: Symantec ICA and ArcSight ESM .....	359
189	2.18.1	Export the CSV File from ArcSight Console.....	359
190	2.18.2	Import the CSV File to Symantec ICA.....	361
191	2.18.3	Create a Mapping between ArcSight events and Symantec ICA .....	365
192	2.18.4	View ArcSight Events in the Analyzer .....	370
193	2.19	Integration: Micro Focus ArcSight and Tripwire .....	371
194	2.19.1	Install Micro Focus ArcSight.....	371
195	2.20	Integration: Micro Focus ArcSight and Cisco AMP.....	383
196	2.20.1	Create API Credentials for ArcSight to access AMP .....	383
197	2.20.2	Install Micro Focus ArcSight.....	384
198	2.20.3	Create a Parser for Cisco AMP REST events.....	392
199	2.21	Integration: Micro Focus ArcSight and Cisco ISE.....	393
200	2.21.1	Configure Cisco ISE to Forward Logs.....	394
201	2.21.2	Select Logs for Forwarding .....	395
202	2.22	Integration: Micro Focus ArcSight and Semperis DSP .....	397
203	2.22.1	Configure Semperis DSP to Forward Logs .....	397
204	2.23	Integration: Micro Focus ArcSight and Symantec Analytics .....	398
205	2.23.1	Configure Symantec Analytics to Forward Logs .....	398
206	2.23.2	Install Symantec Analytics Package for ArcSight .....	400
207	2.24	Integration: Micro Focus ArcSight and Glasswall FileTrust.....	408
208	2.24.1	Install Micro Focus ArcSight.....	408

209	2.25 Integration: Micro Focus ArcSight and Cisco Stealthwatch .....	423
210	2.25.1 Install Micro Focus ArcSight.....	423
211	2.25.2 Configure Cisco Stealthwatch .....	432
212	<b>Appendix A List of Acronyms .....</b>	<b>440</b>

## 213 1 Introduction

214 The following guides show IT professionals and security engineers how we implemented this example  
215 solution. We cover all of the products employed in this reference design. We do not recreate the  
216 product manufacturers' documentation, which is presumed to be widely available. Rather, these guides  
217 show how we incorporated the products together in our environment.

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

### 220 1.1 Practice Guide Structure

221 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides  
222 users with the information they need to replicate the data integrity detection and response solution.  
223 This reference design is modular and can be deployed in whole or in parts.

224 This guide contains three volumes:

- 225     ▪ NIST SP 1800-26a: *Executive Summary*
- 226     ▪ NIST SP 1800-26b: *Approach, Architecture, and Security Characteristics* – what we built and why
- 227     ▪ NIST SP 1800-26c: *How-To Guides* – instructions for building the example solution (**you are**  
228         **here**)

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

230 **Business decision makers, including chief security and technology** officers will be interested in the  
231 *Executive Summary (NIST SP 1800-26a)*, which describes the:

- 232     ▪ challenges enterprises face in detecting and responding to data integrity events
- 233     ▪ example solution built at the NCCoE
- 234     ▪ benefits of adopting the example solution

235 **Technology or security program managers** who are concerned with how to identify, understand,  
236 assess, and mitigate risk will be interested in *NIST SP 1800-26b*, which describes what we did and why.  
237 The following sections will be of particular interest:

- 238     ▪ Section 3.4.1, Risk, provides a description of the risk analysis we performed.
- 239     ▪ Section 3.4.2, Security Control Map, maps the security characteristics of this example solution  
240         to cybersecurity standards and best practices.

241 You might share the *Executive Summary, NIST SP 1800-26a*, with your leadership team members to help  
242 them understand the importance of adopting standards-based data integrity solutions.

243 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.  
244 You can use the How-To portion of the guide, *NIST SP 1800-26c*, to replicate all or parts of the build  
245 created in our lab. The How-To guide provides specific product installation, configuration, and  
246 integration instructions for implementing the example solution. We do not recreate the product  
247 manufacturers' documentation, which is generally widely available. Rather, we show how we  
248 incorporated the products together in our environment to create an example solution.

249 This guide assumes that IT professionals have experience implementing security products within the  
250 enterprise. While we have used a suite of commercial products to address this challenge, this guide  
251 does not endorse these particular products. Your organization can adopt this solution or one that  
252 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and  
253 implementing parts of a data integrity detection and response solution. Your organization's security  
254 experts should identify the products that will best integrate with your existing tools and IT system  
255 infrastructure. We hope you will seek products that are congruent with applicable standards and best  
256 practices. Volume B, Section 3.5, Technologies, lists the products we used and maps them to the  
257 cybersecurity controls provided by this reference solution.

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

## 262 **1.2 Build Overview**

263 The NCCoE built a hybrid virtual-physical laboratory environment to explore methods to effectively  
264 detect and respond to a data corruption event in various Information Technology (IT) enterprise  
265 environments. NCCoE also explored the issues of analysis and reporting to support incident response.  
266 The servers in the virtual environment were built to the hardware specifications of their specific  
267 software components.

268 The NCCoE worked with members of the Data Integrity Community of Interest to develop a diverse (but  
269 non-comprehensive) set of use case scenarios against which to test the reference implementation.  
270 These are detailed in Volume B, Section 5.2. For a detailed description of our architecture, see Volume  
271 B, Section 4.

## 272 1.3 Typographical Conventions

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

Typeface/ Symbol	Meaning	Example
<i>Italics</i>	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</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, sta- tus 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 National Cybersecurity Center of Excellence are available at <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a>

## 274 2 Product Installation Guides

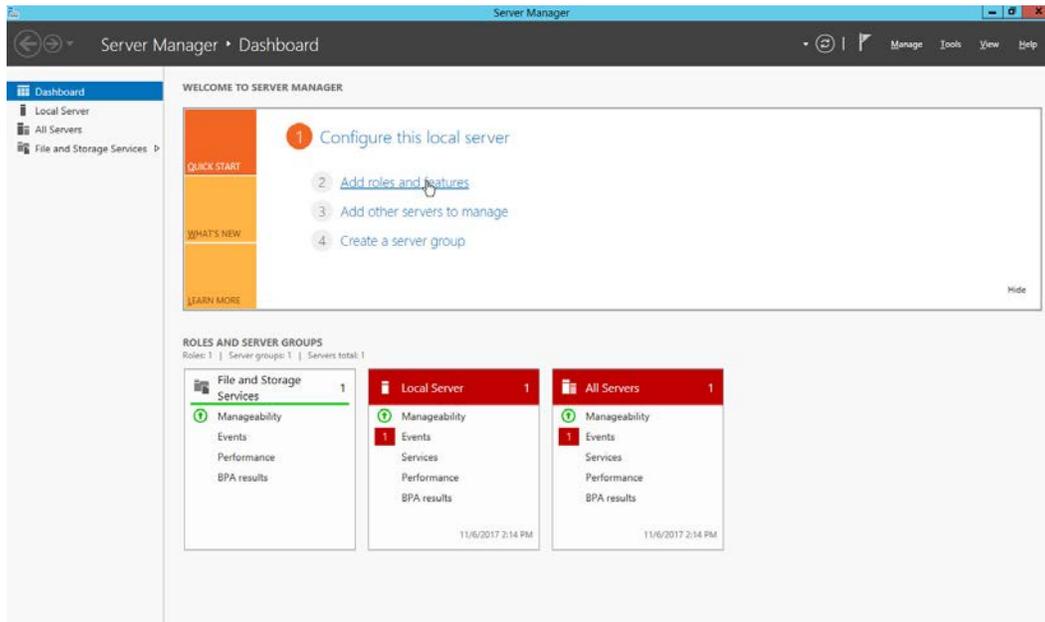
275 This section of the practice guide contains detailed instructions for installing and configuring all of the  
276 products used to build an instance of the example solution.

### 277 2.1 Active Directory and Domain Name System Server

278 As part of our enterprise emulation, we included an Active Directory server that doubles as a Domain  
279 Name System (DNS) server. This section covers the installation and configuration process used to set up  
280 Active Directory and DNS on a Windows Server 2012 R2 machine.

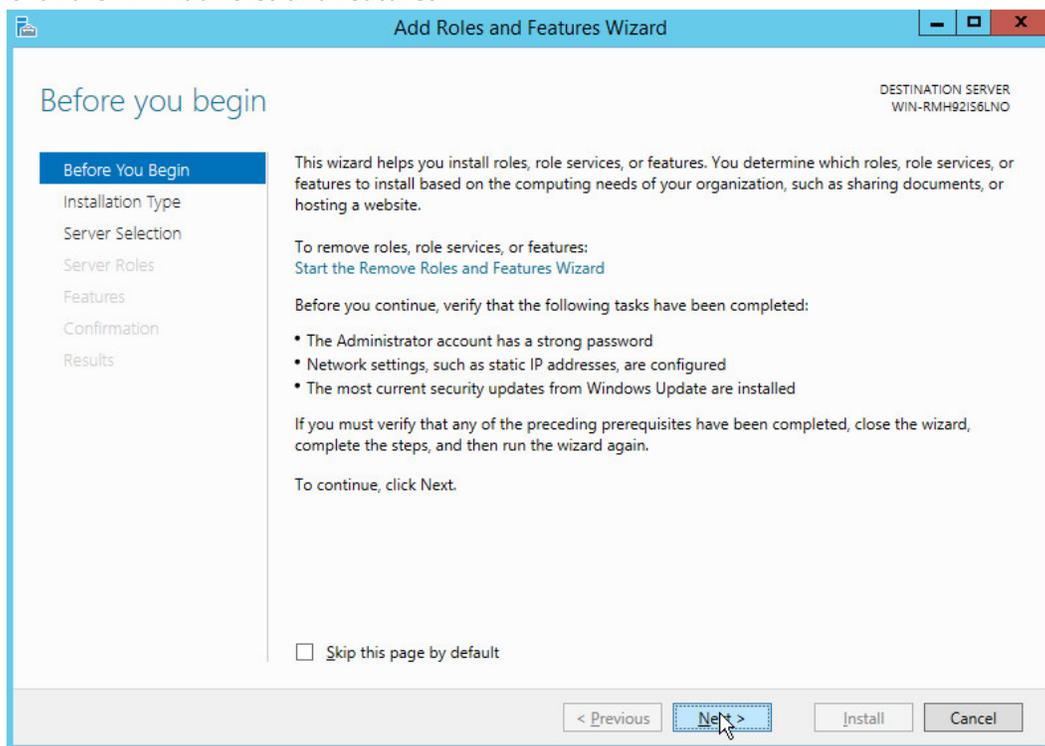
#### 281 2.1.1 Install Features

282 1. Open **Server Manager**.



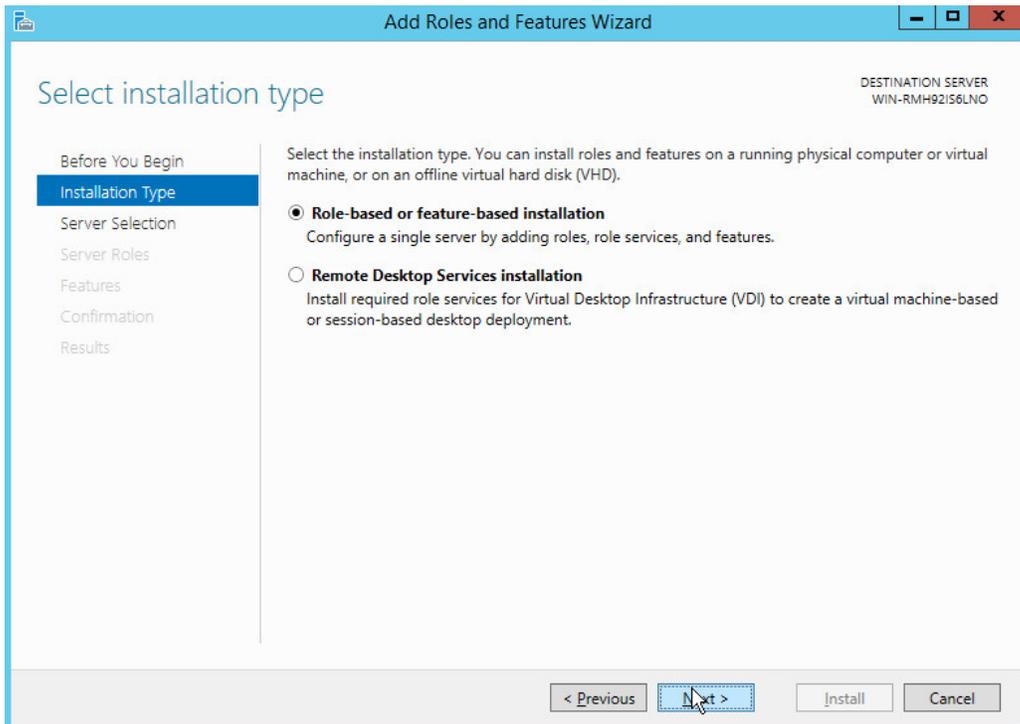
283  
284

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



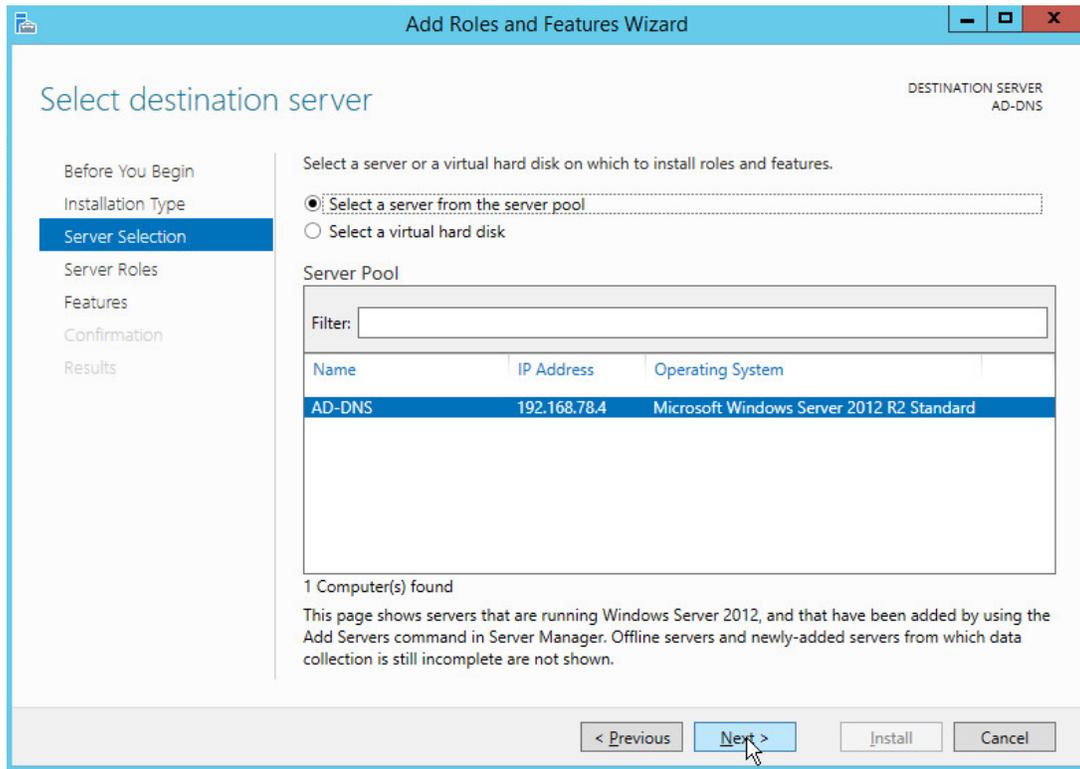
285  
286  
287

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



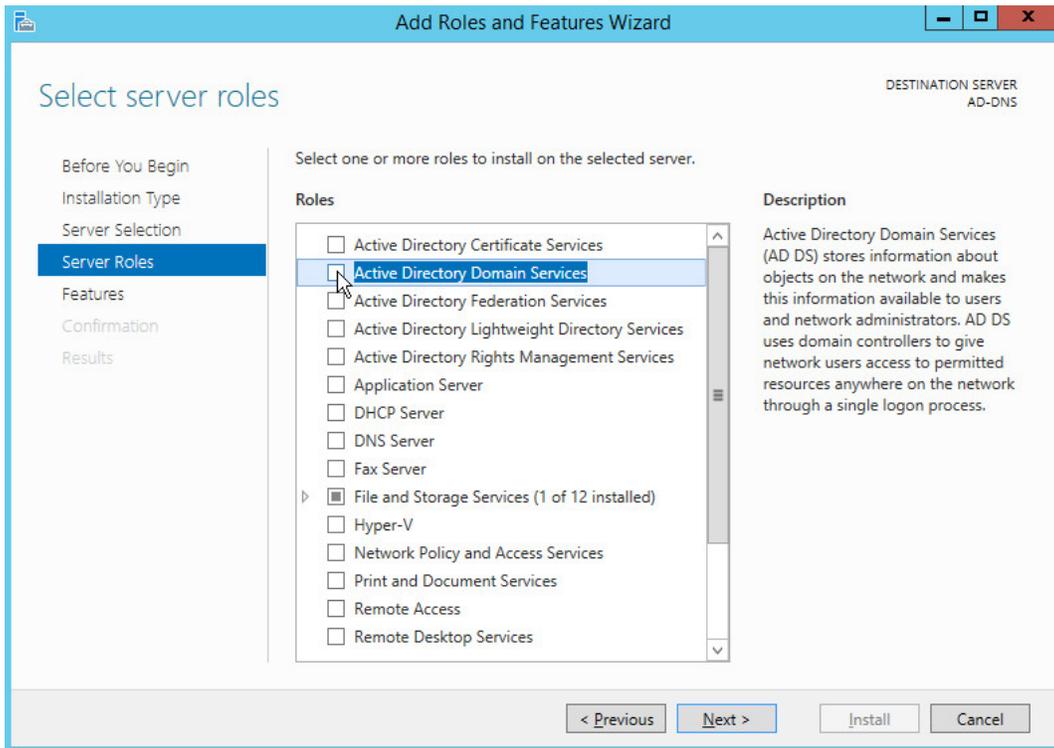
288  
289  
290  
291

5. Click **Next**.
6. Select **Select a server from the server pool**.
7. Select the intended active directory server.



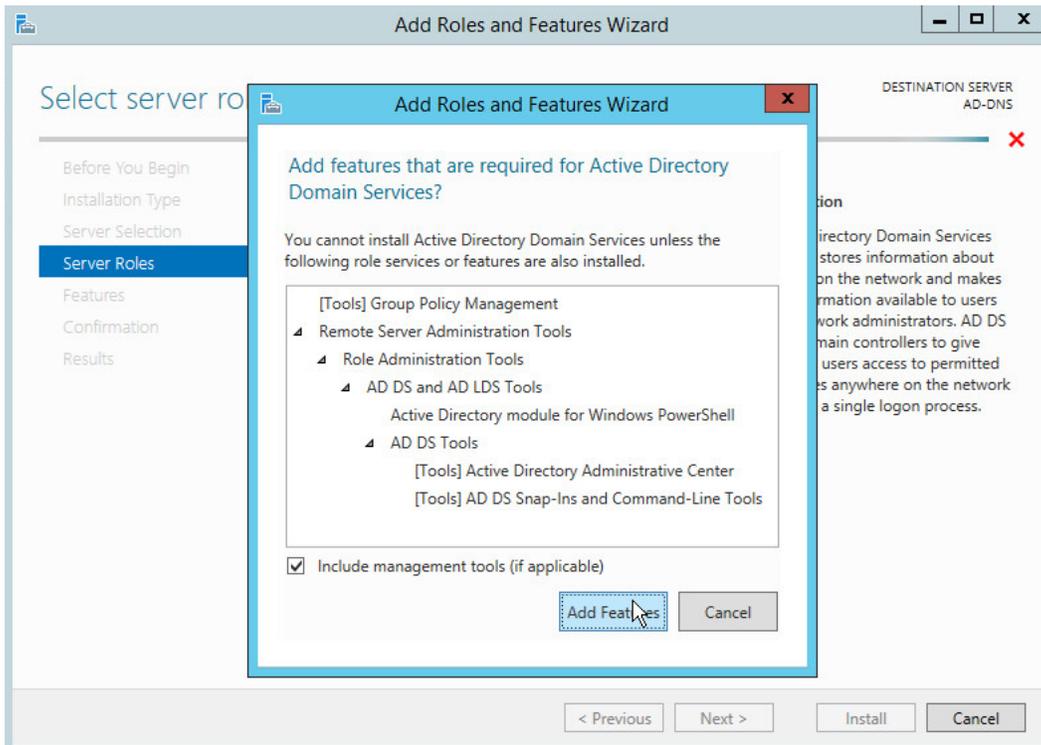
292  
293

8. Click **Next**.



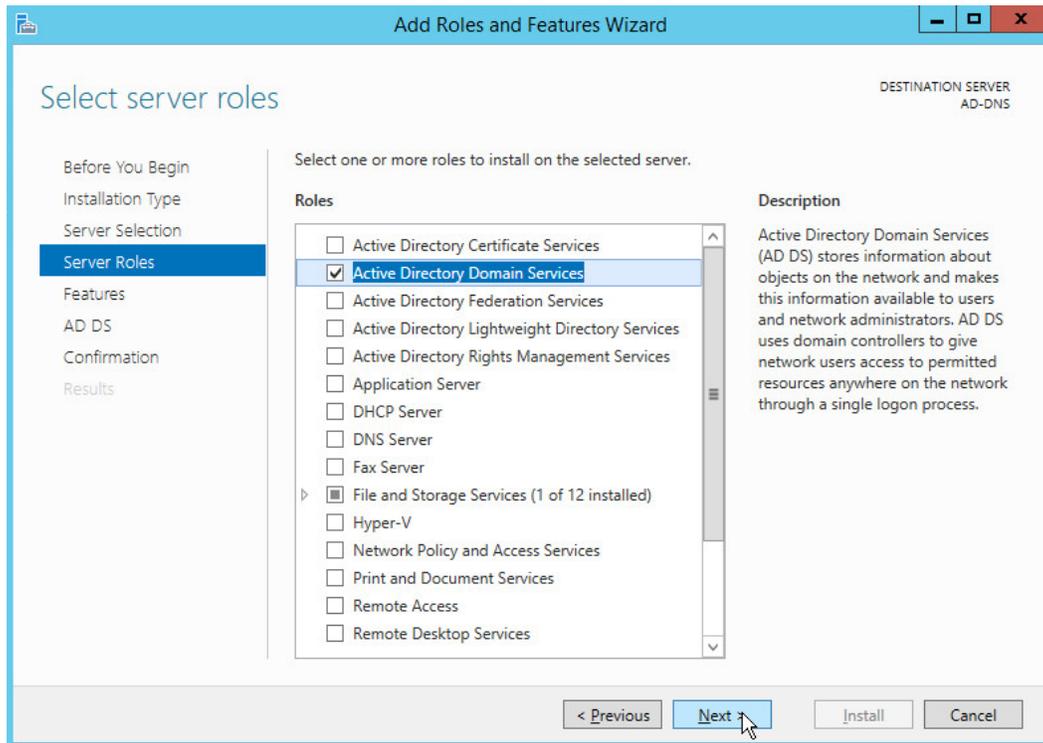
294  
295

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



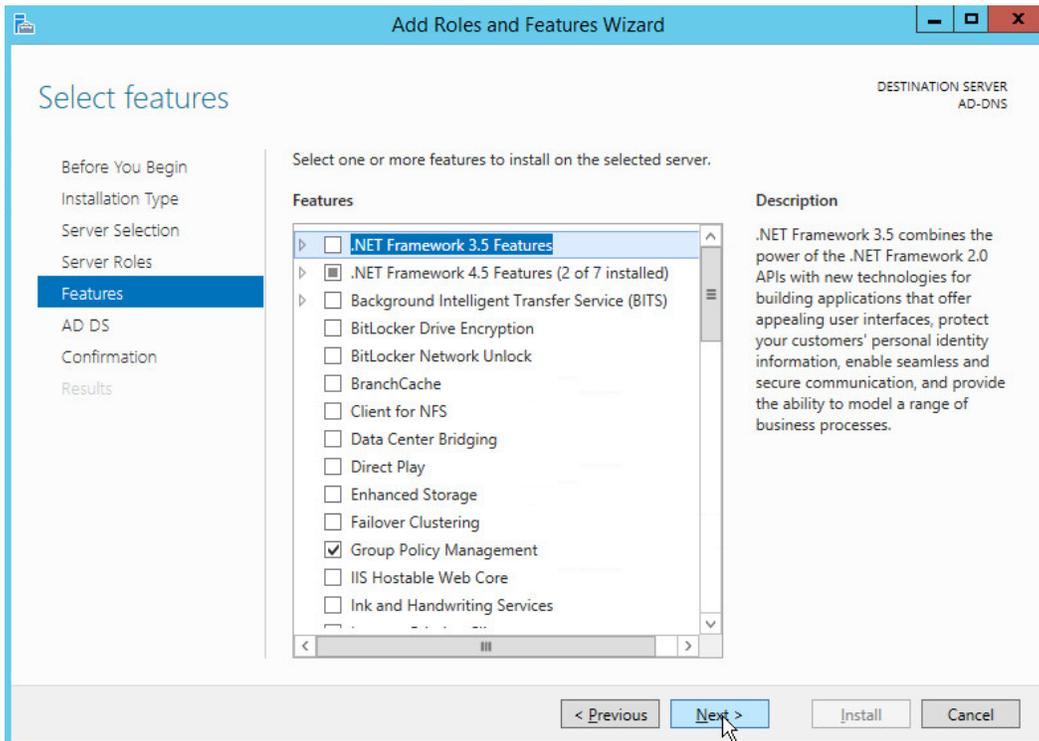
296  
297

10. Click **Add Features**.



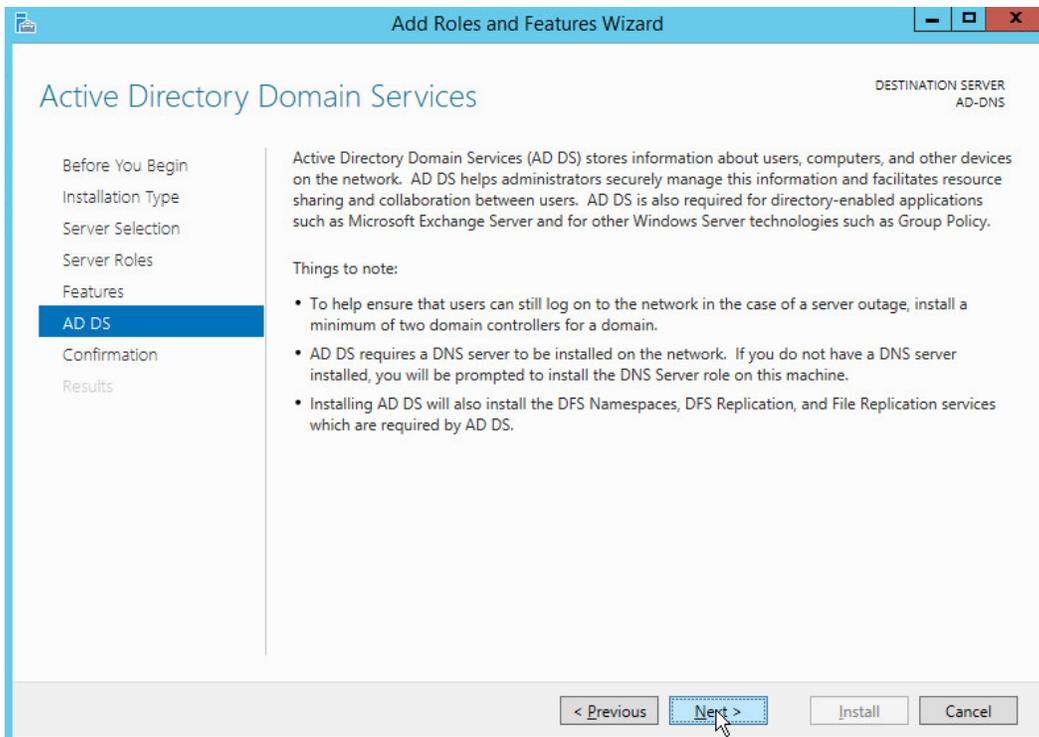
298  
299

11. Click **Next**.



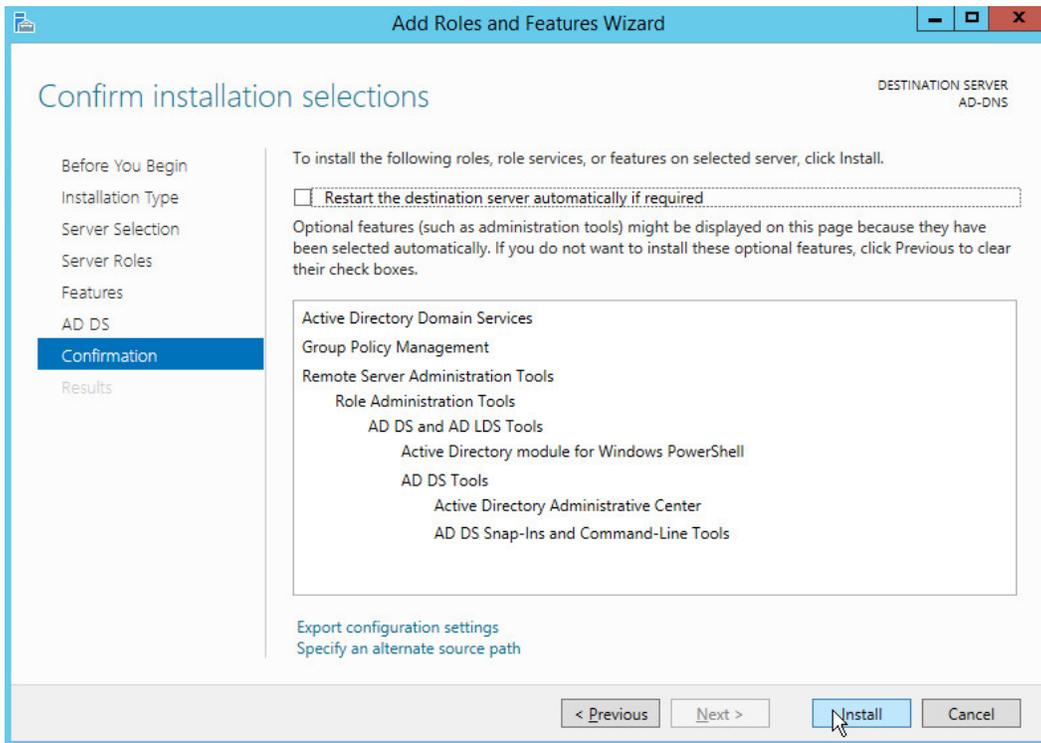
300  
301

12. Click **Next**.



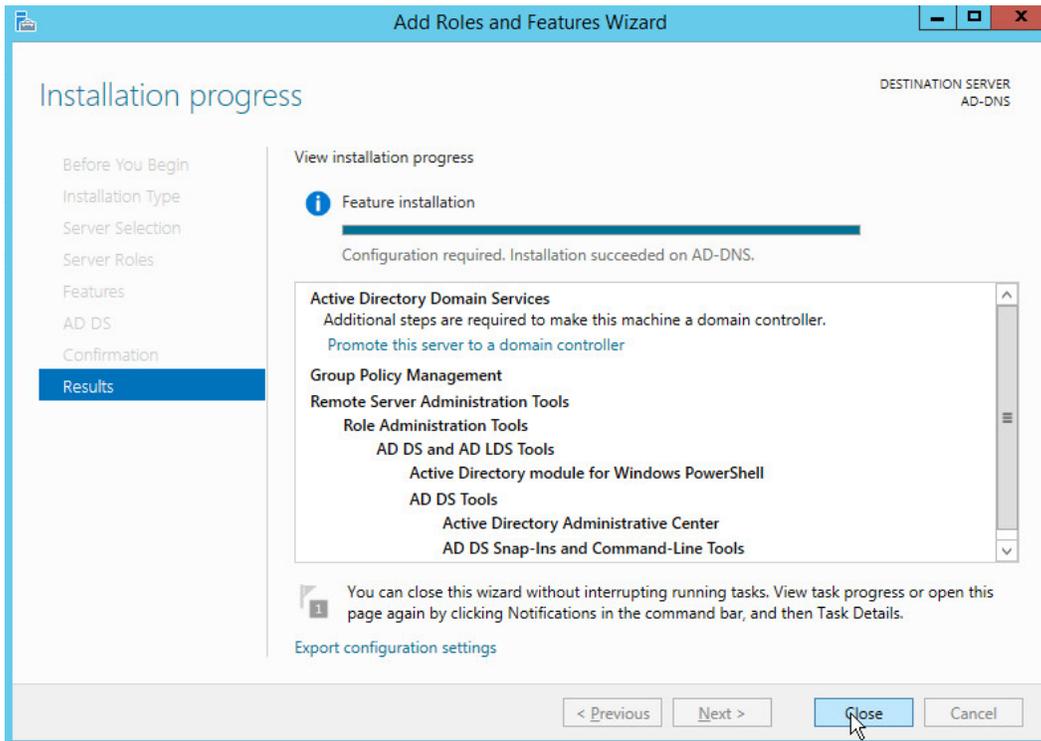
302

303 13. Click **Next**.



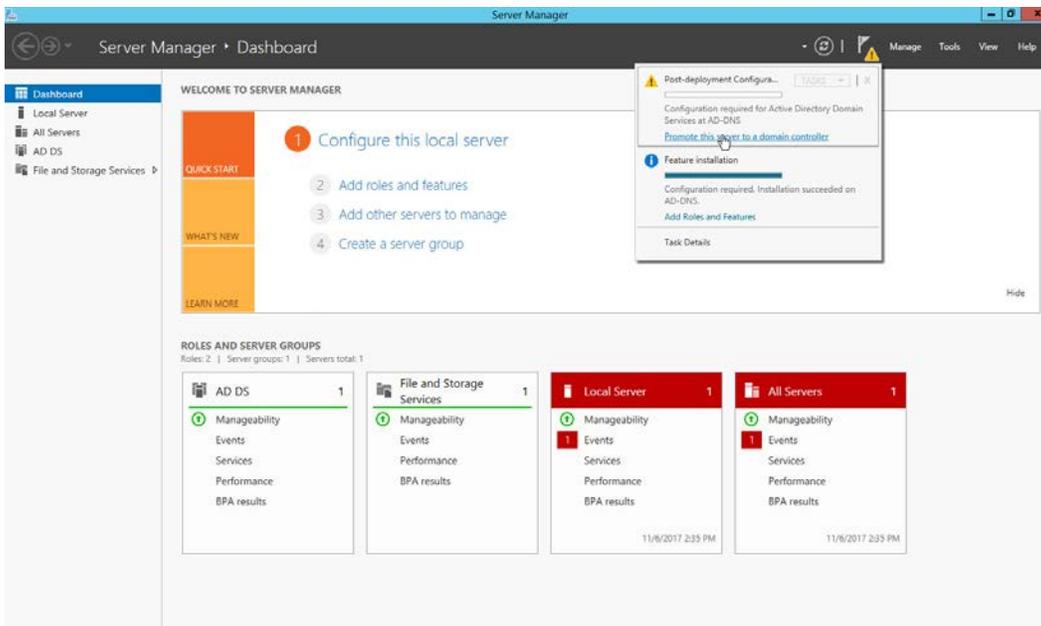
304 14. Click **Install**.

305 15. Wait for the installation to complete.



307  
308

16. Click **Close**.

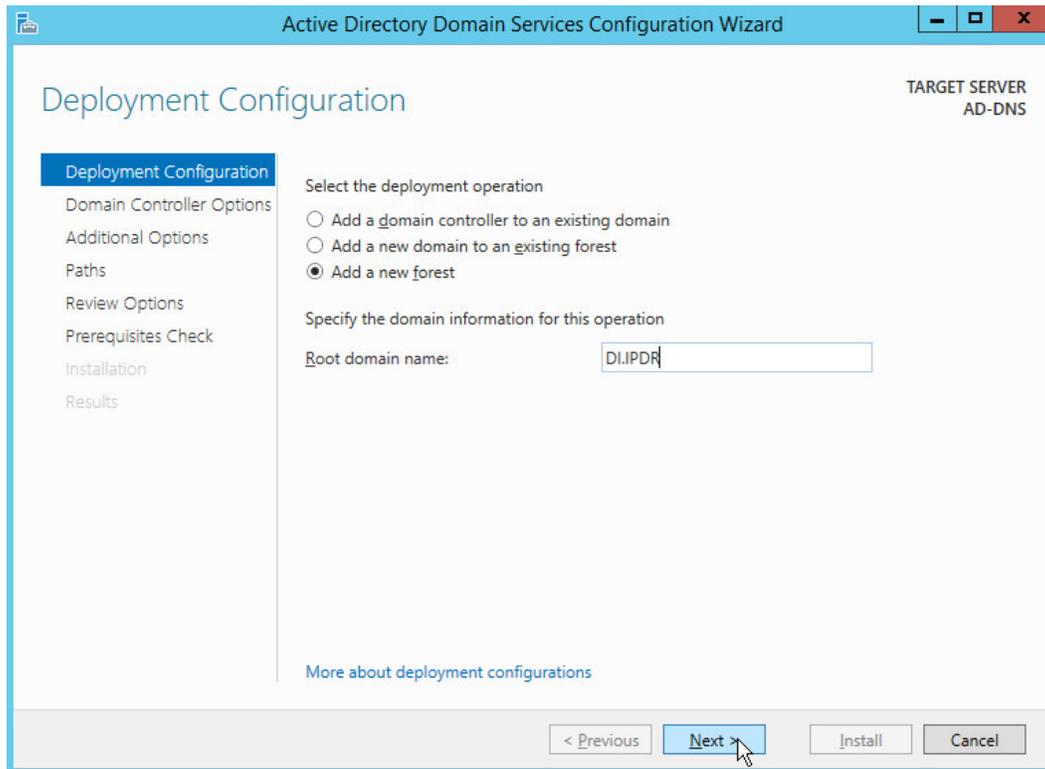


309  
310  
311  
312

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

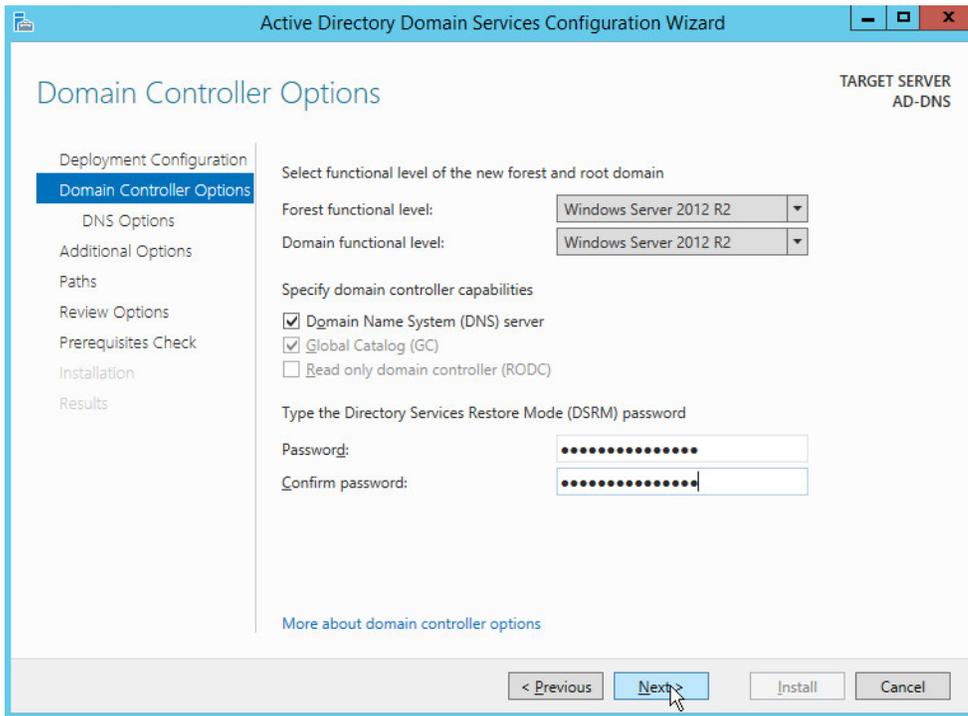
18. Select **Add a new forest**.

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



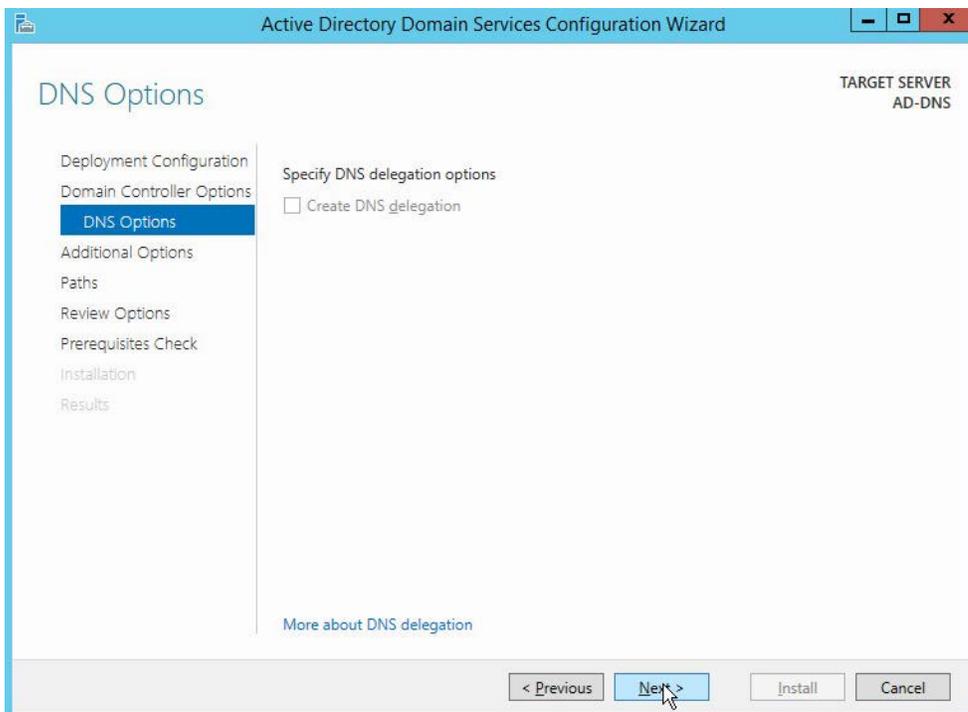
313  
314  
315  
316  
317

20. Click **Next**.
21. Select **Windows Server 2012 R2** for **Forest functional level** and **Domain functional level**.
22. Check the box next to **Domain Name System (DNS) server**.
23. Enter a password.



318  
319

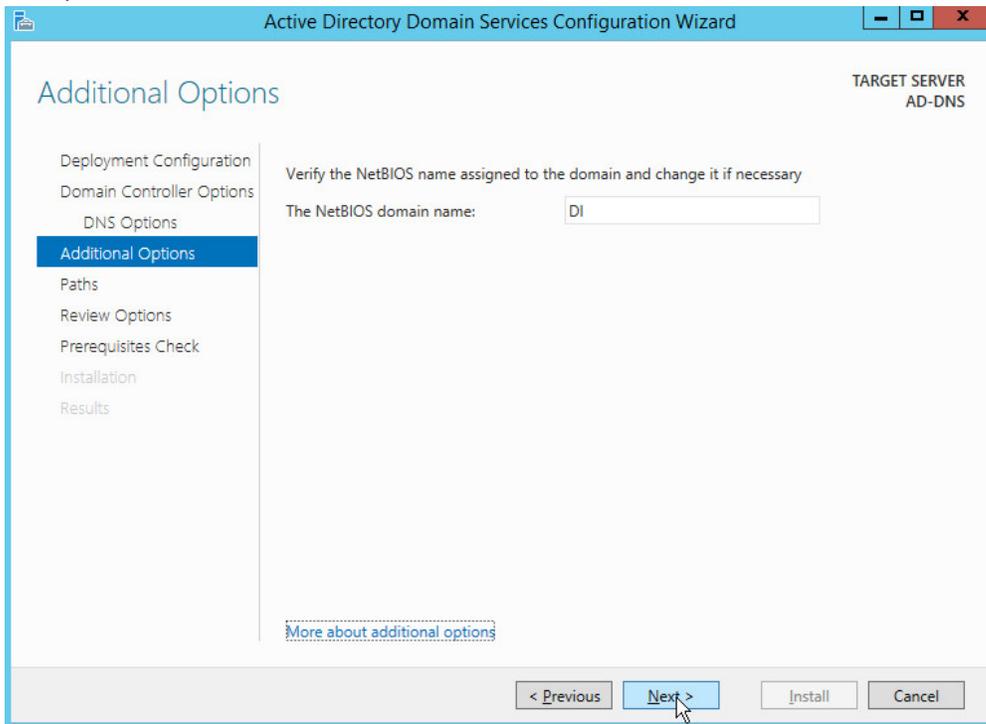
24. Click **Next**.



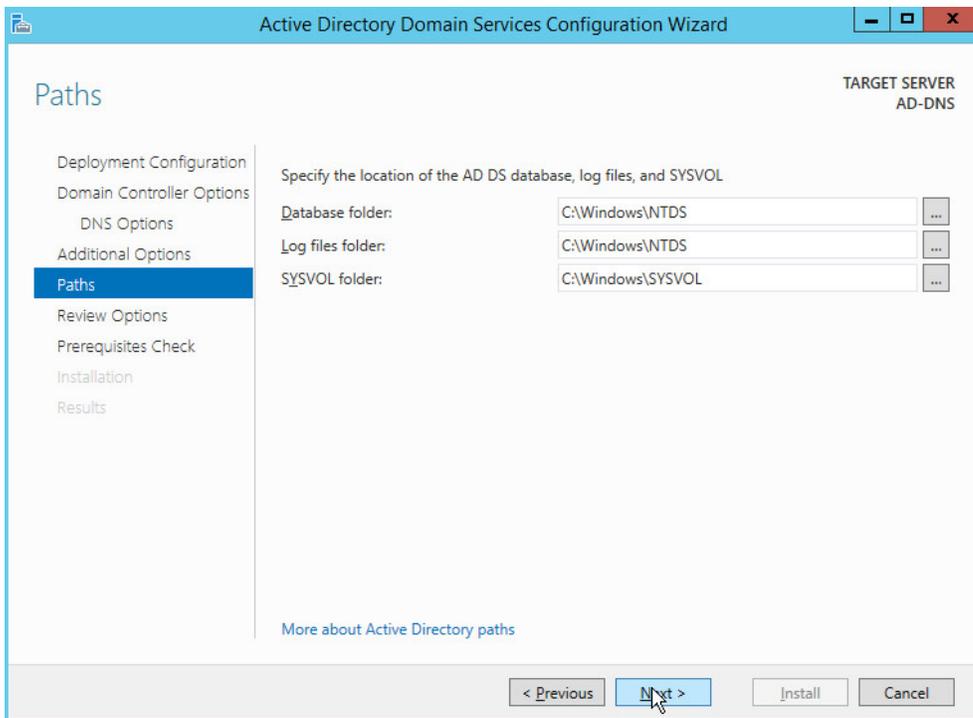
320  
321

25. Click **Next**.

322 26. Verify the domain name.

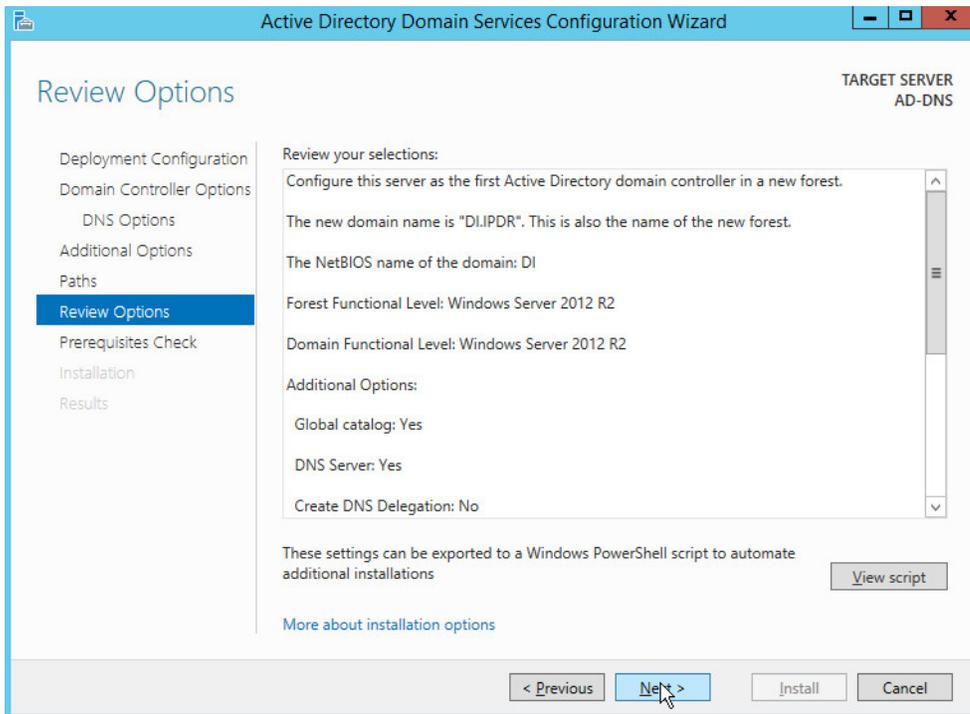


323 324 27. Click Next.

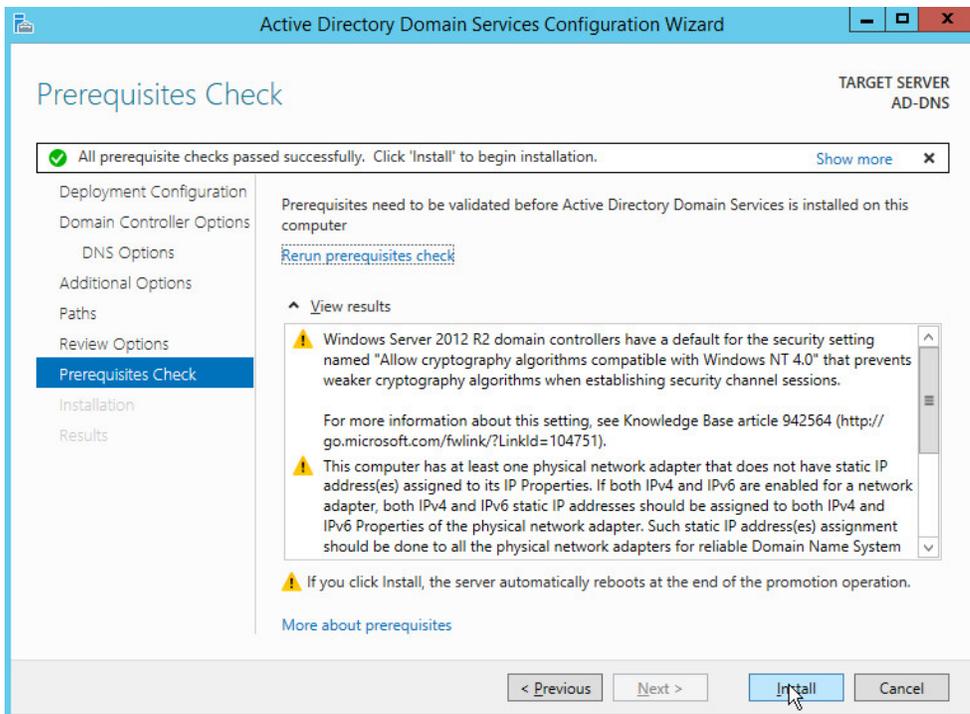


325

326 28. Click **Next**.



327 328 29. Click **Next**.

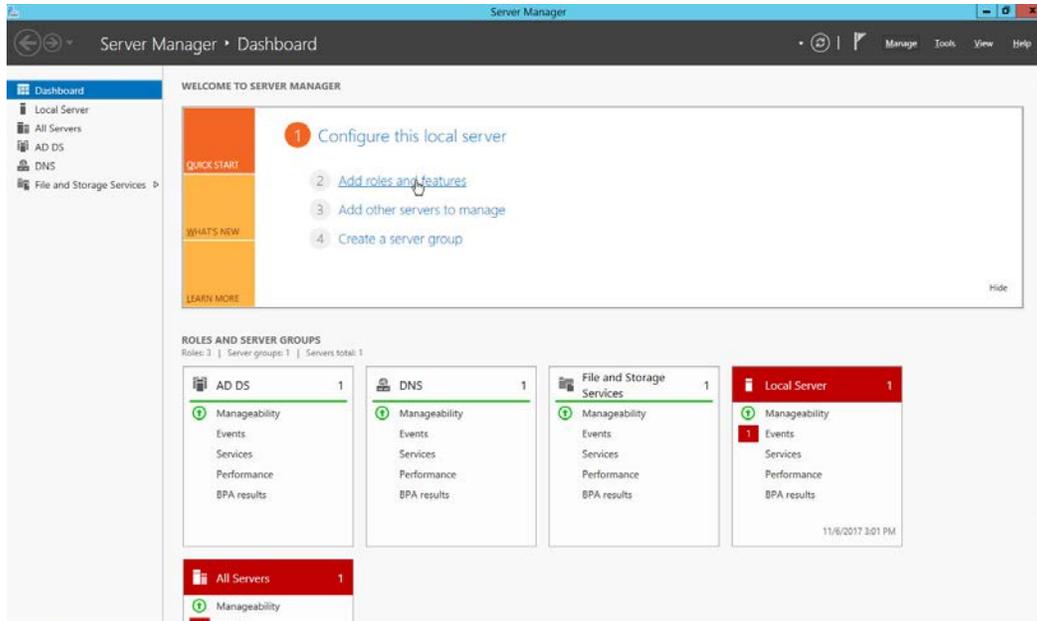


329

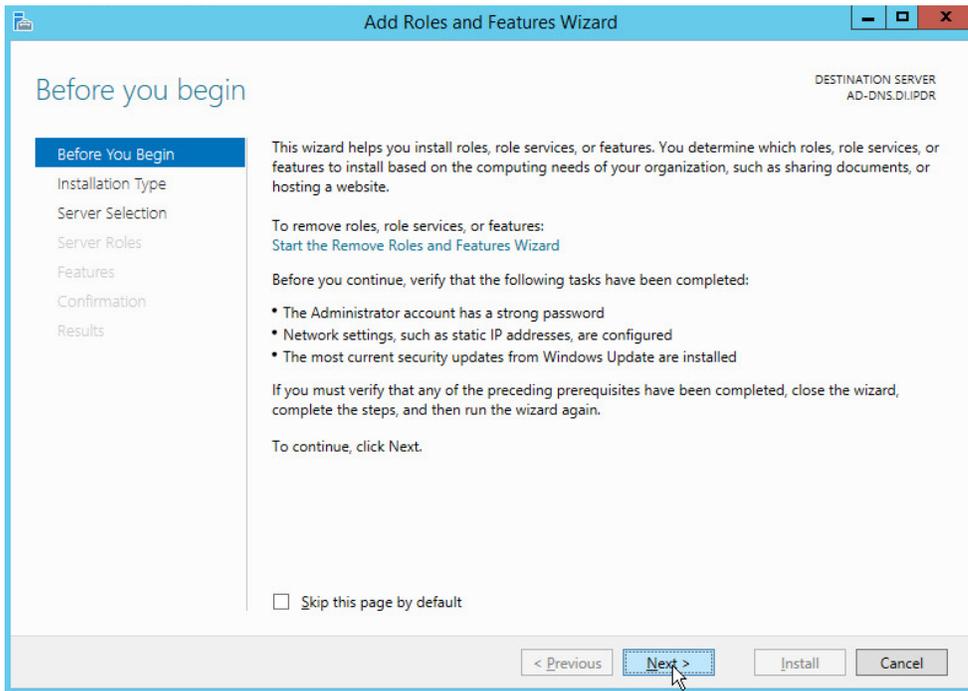
- 330 30. Click **Install**.
- 331 31. Wait for the installation to complete.
- 332 32. The server automatically reboots.

### 333 2.1.2 Create a Certificate Authority

- 334 1. Open **Server Manager**.

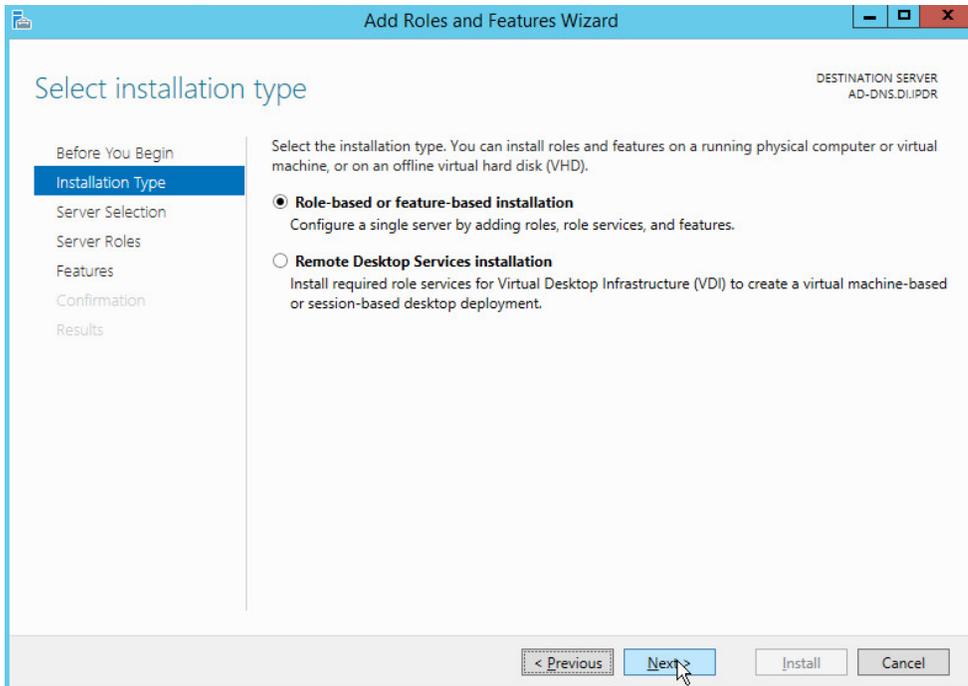


- 335
- 336 2. Click **Add roles and features**.



337  
338  
339

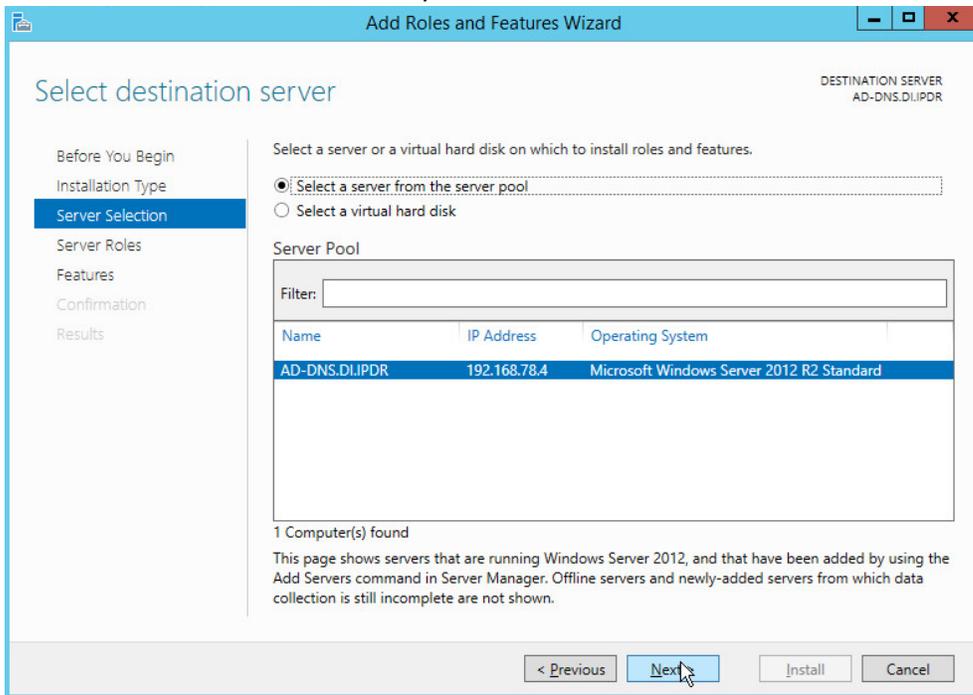
3. Click **Next**.
4. Select **Role-based or feature-based installation**.



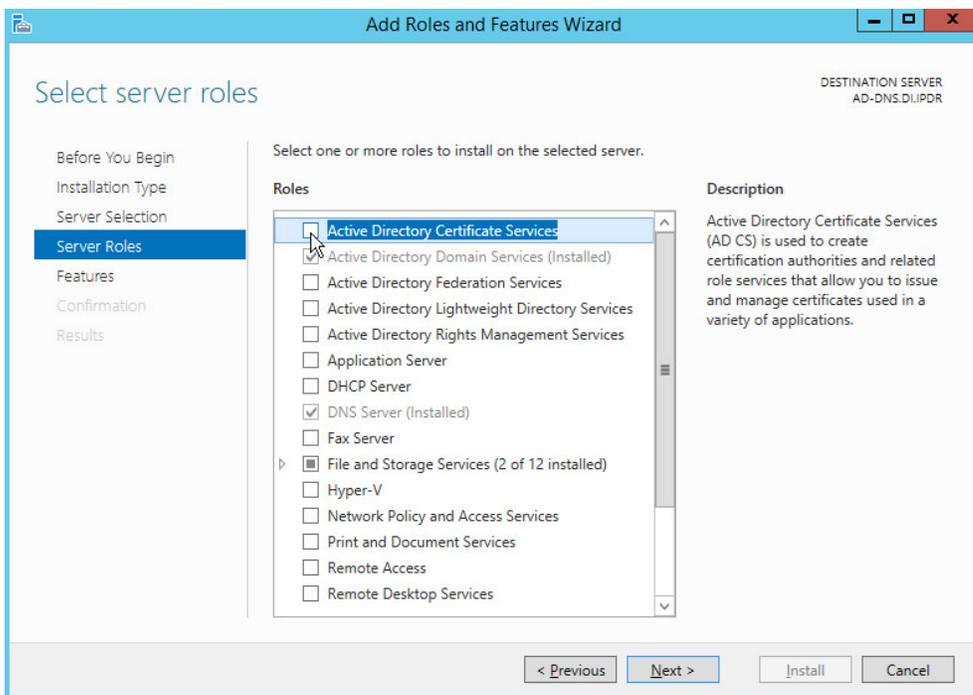
340  
341

5. Click **Next**.

- 342 6. Select **Select a server from the server pool**.
- 343 7. Select the intended Active Directory server.

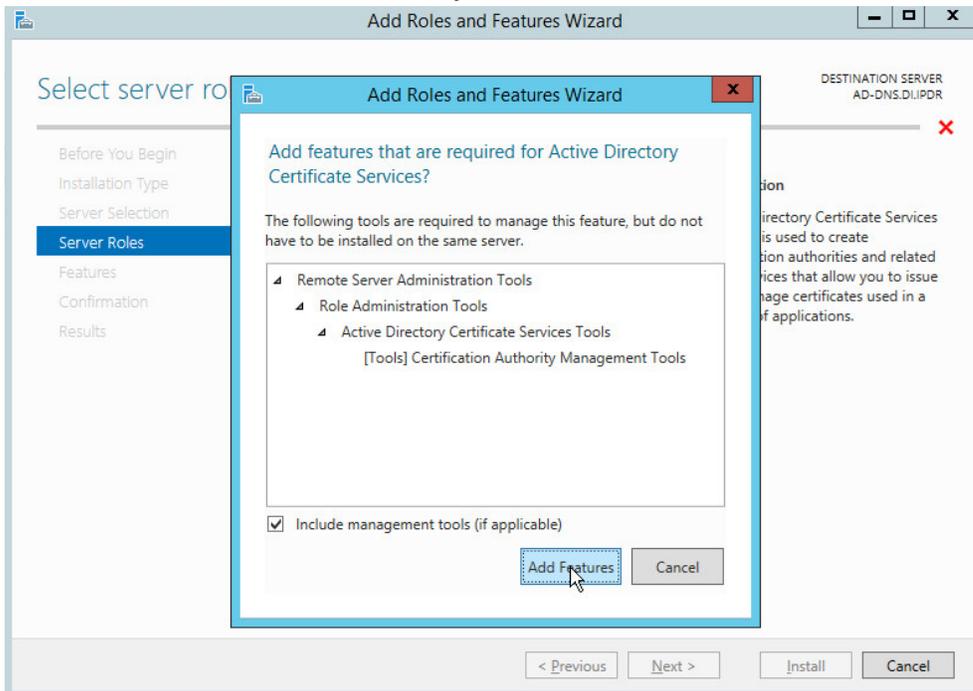


- 344 8. Click **Next**.
- 345

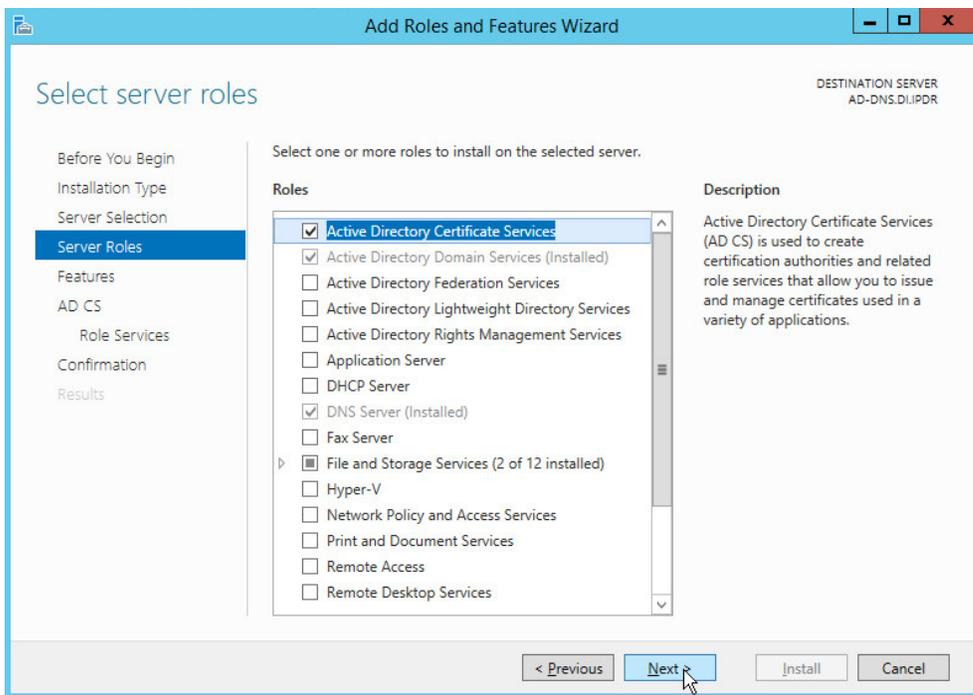


346

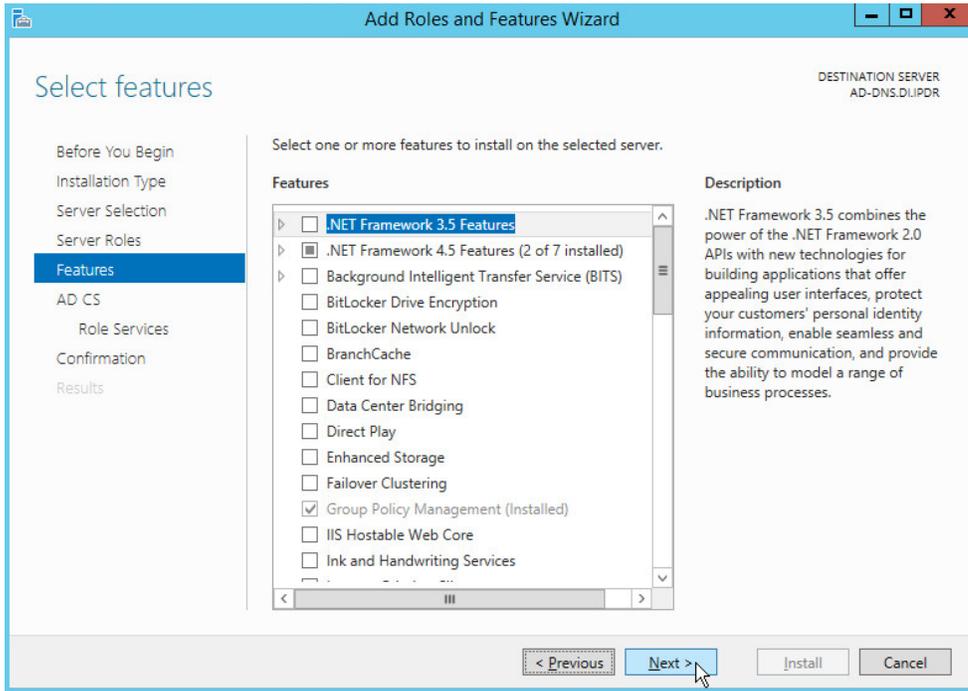
347 9. Check the box next to **Active Directory Certificate Services**.



348 10. Click **Add Features**.

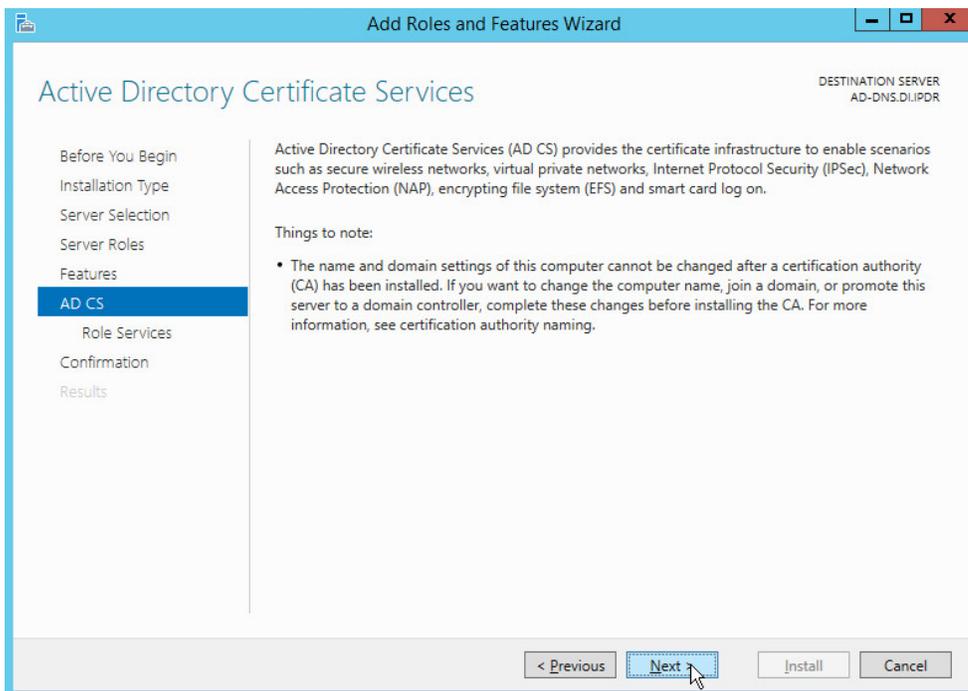


350 11. Click **Next**.



352  
353

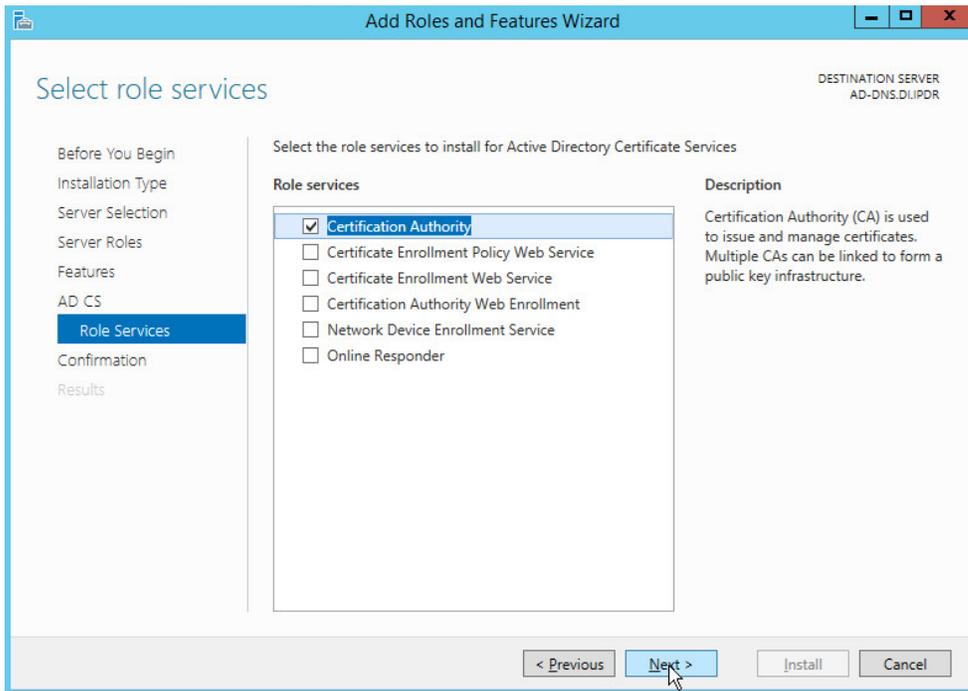
12. Click **Next**.



354  
355  
356

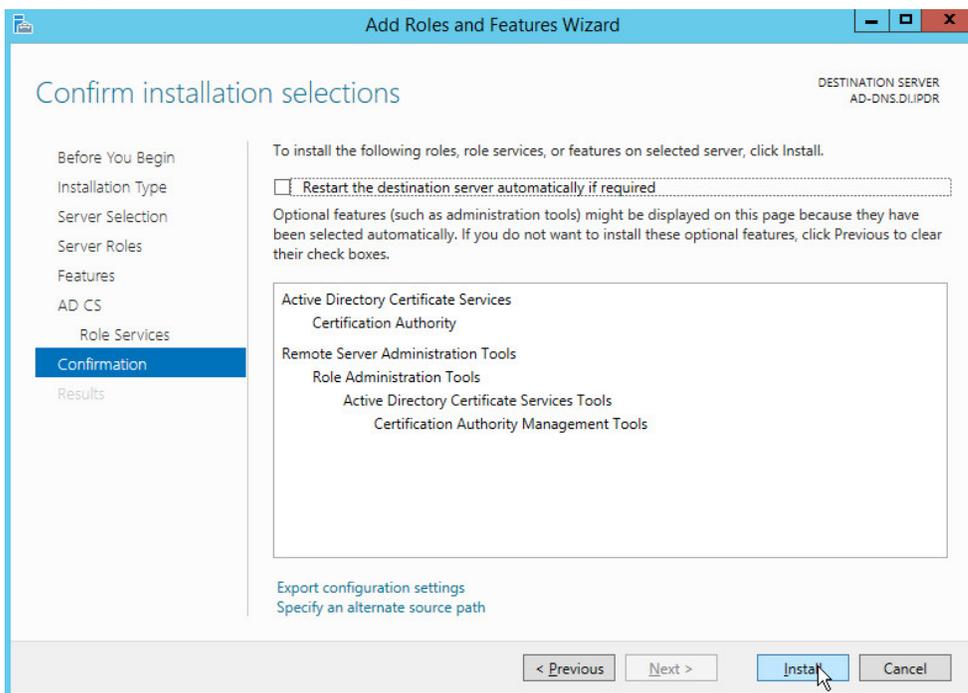
13. Click **Next**.

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



357  
358

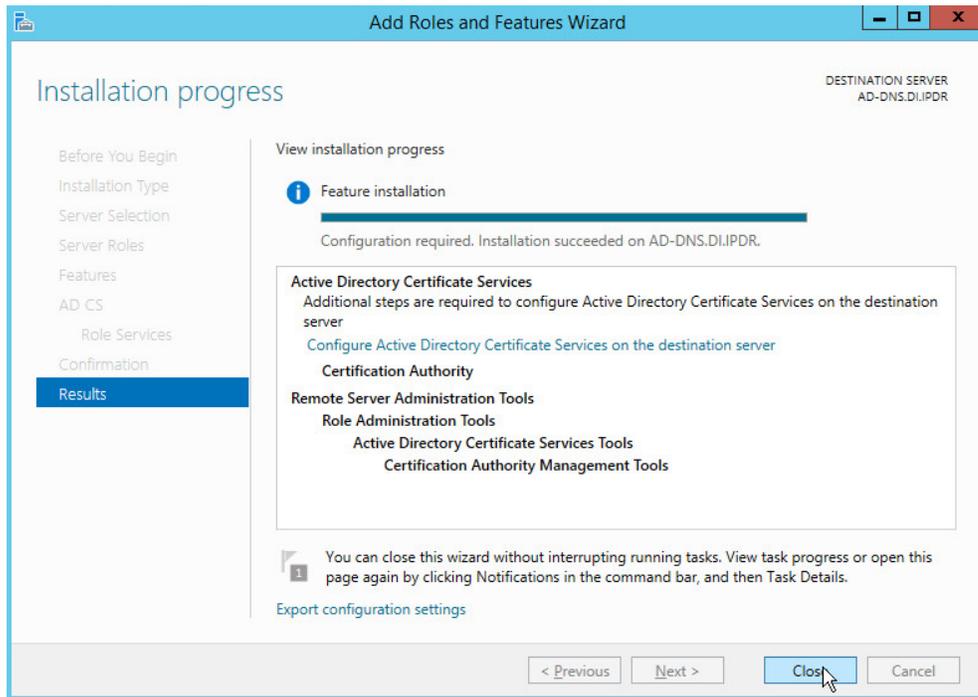
15. Click **Next**.



359  
360  
361

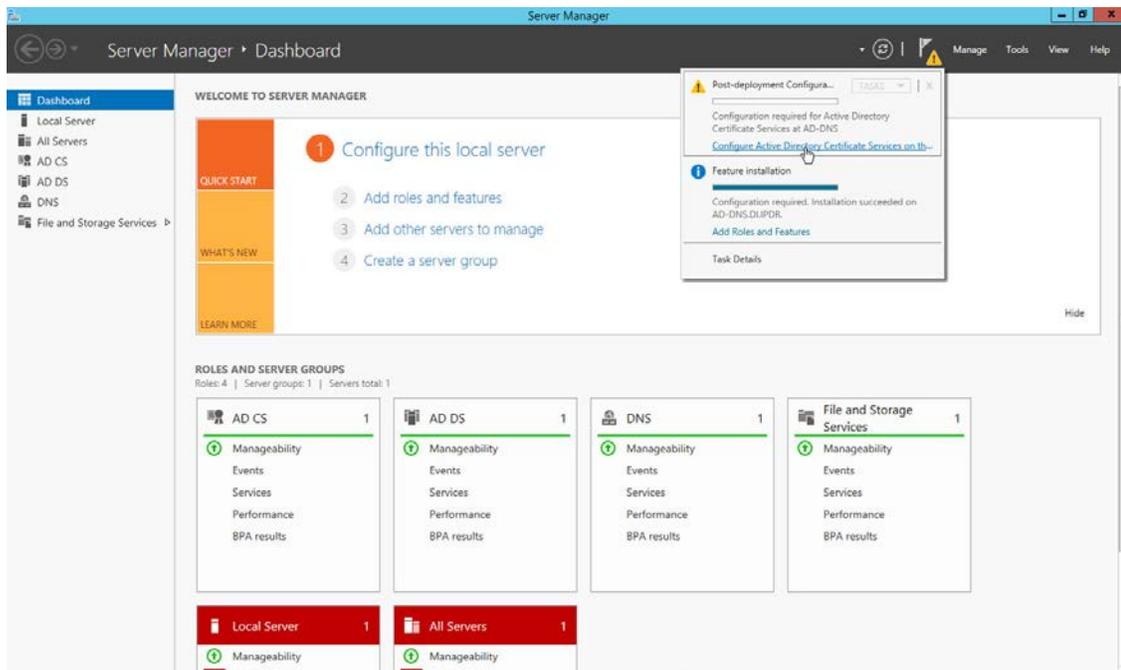
16. Click **Install**.

17. Wait for the installation to complete.



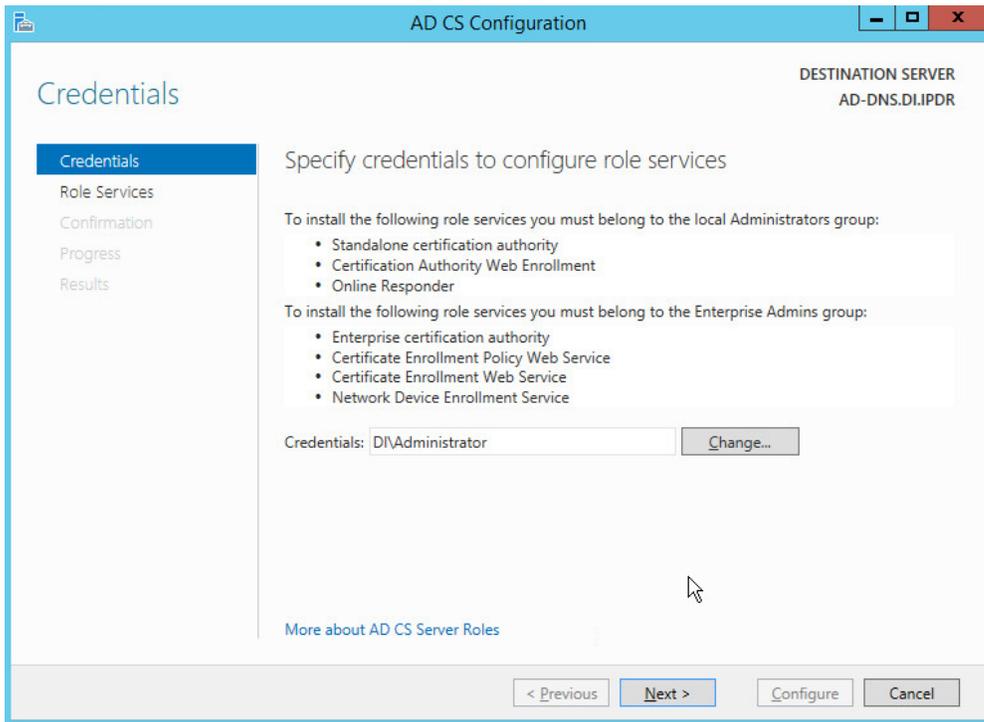
362  
363

18. Click **Close**.



364  
365

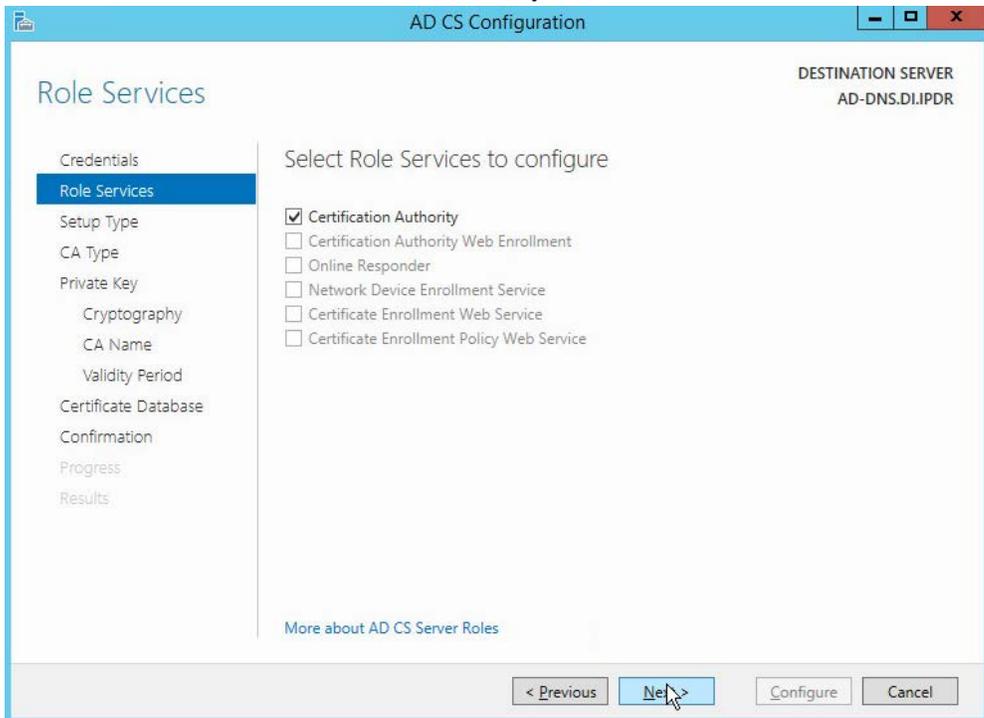
19. Click **Configure Active Directory Certificate Services on the destination server**.



366  
367  
368

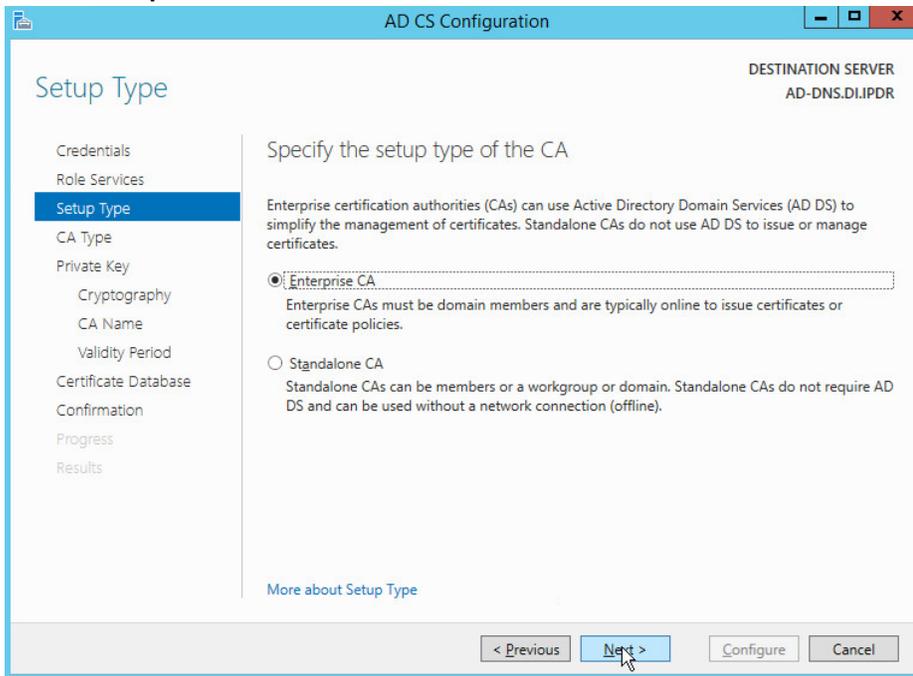
20. Click **Next**.

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

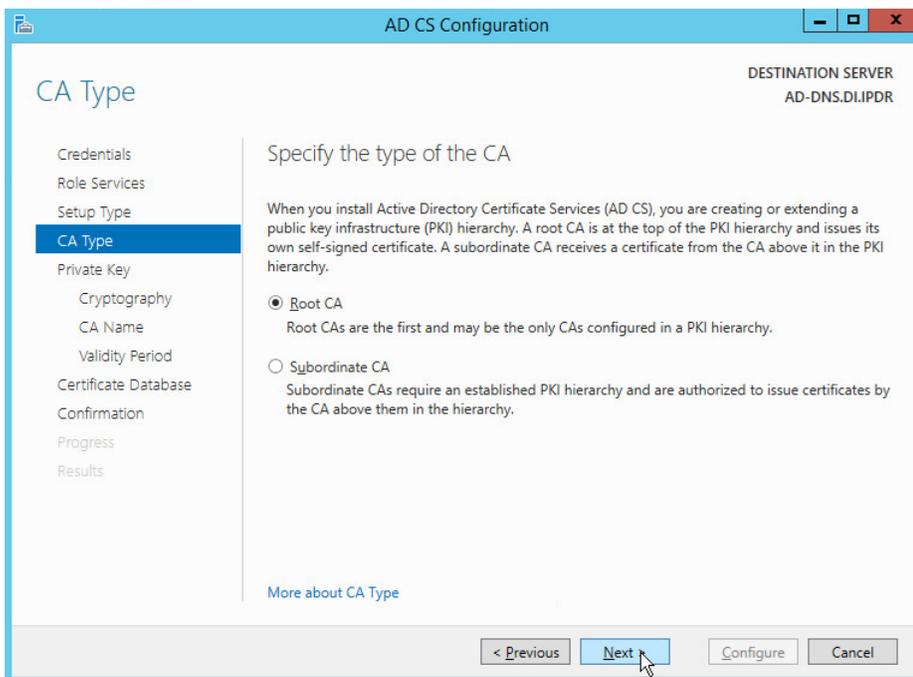


369

- 370 22. Click **Next**.
- 371 23. Select **Enterprise CA**.

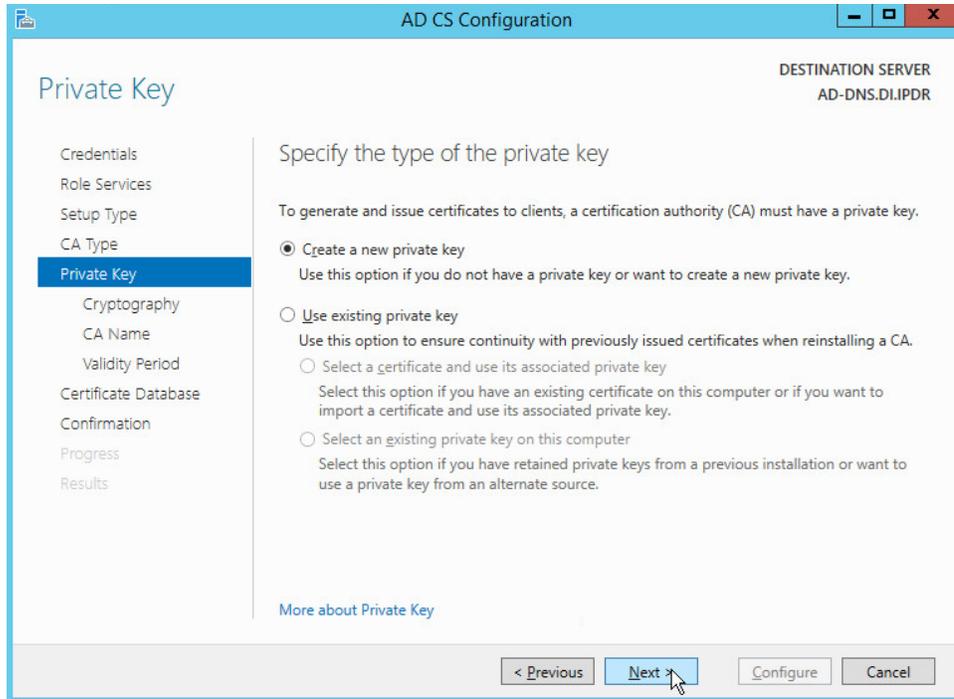


- 372 24. Click **Next**.
- 373 25. Select **Root CA**.
- 374

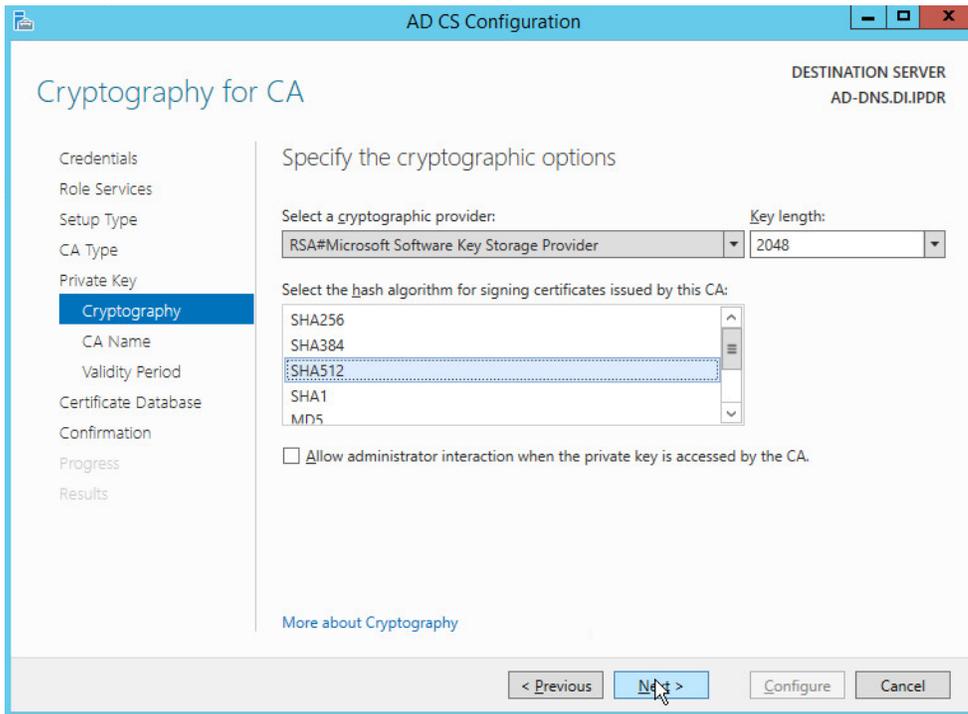


375

- 376 26. Click **Next**.
- 377 27. Select **Create a new private key**.

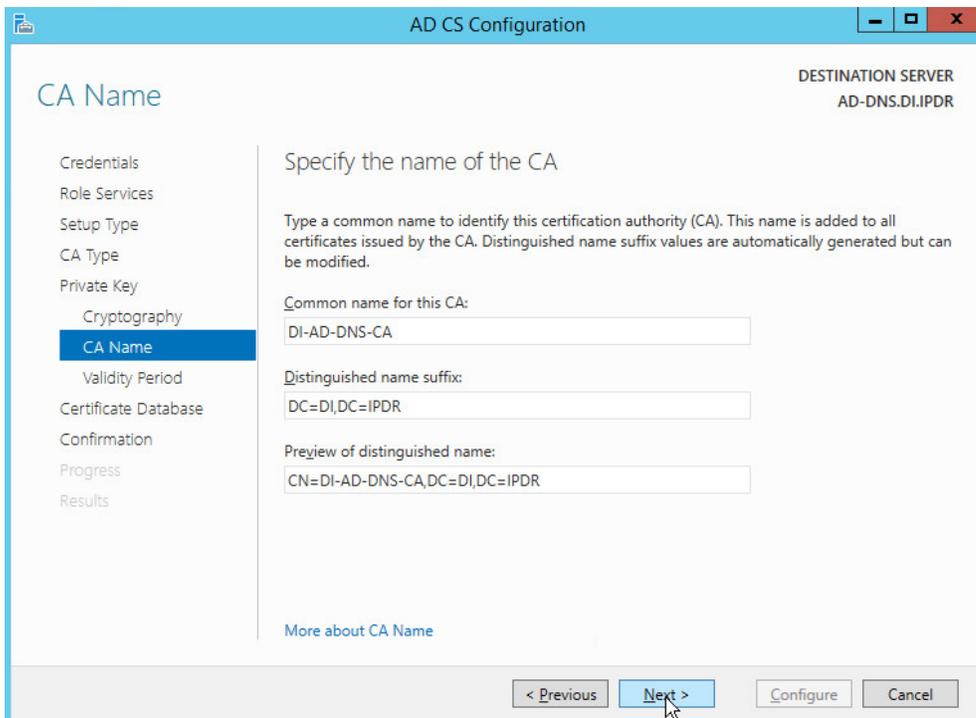


- 378 28. Click **Next**.
- 379 29. Select **RSA#Microsoft Software Key Storage Provider**.
- 380 30. Set the **Key length** to **2048**.
- 381 31. Select **SHA512** from the list.
- 382



383  
384

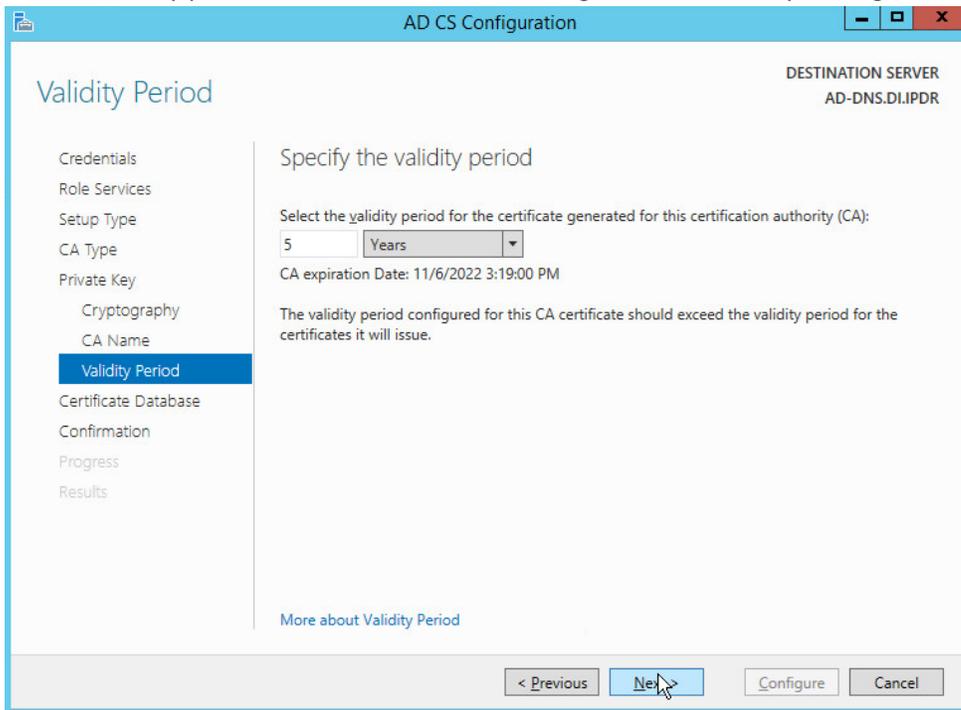
32. Click **Next**.



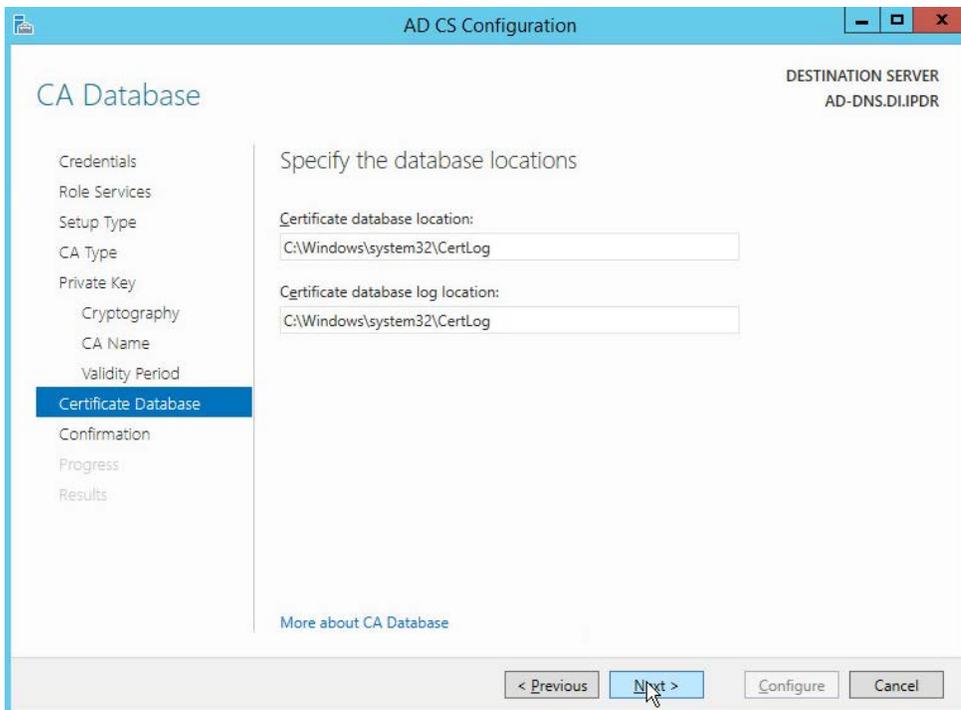
385  
386

33. Click **Next**.

387 34. Set the validity period of the certificate according to the needs of your organization.

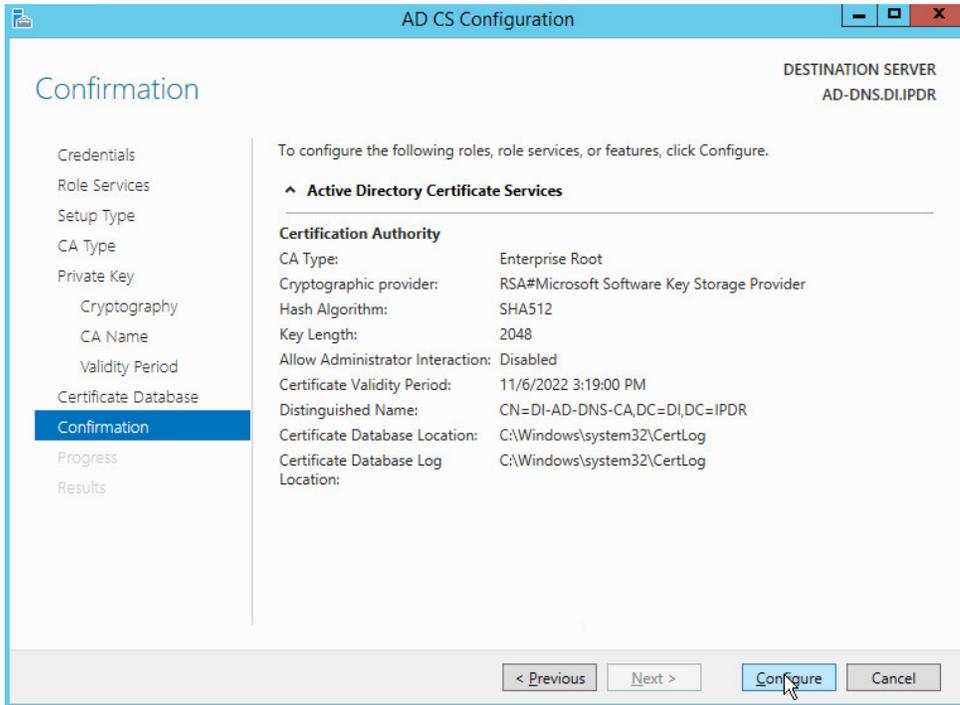


388 35. Click Next.

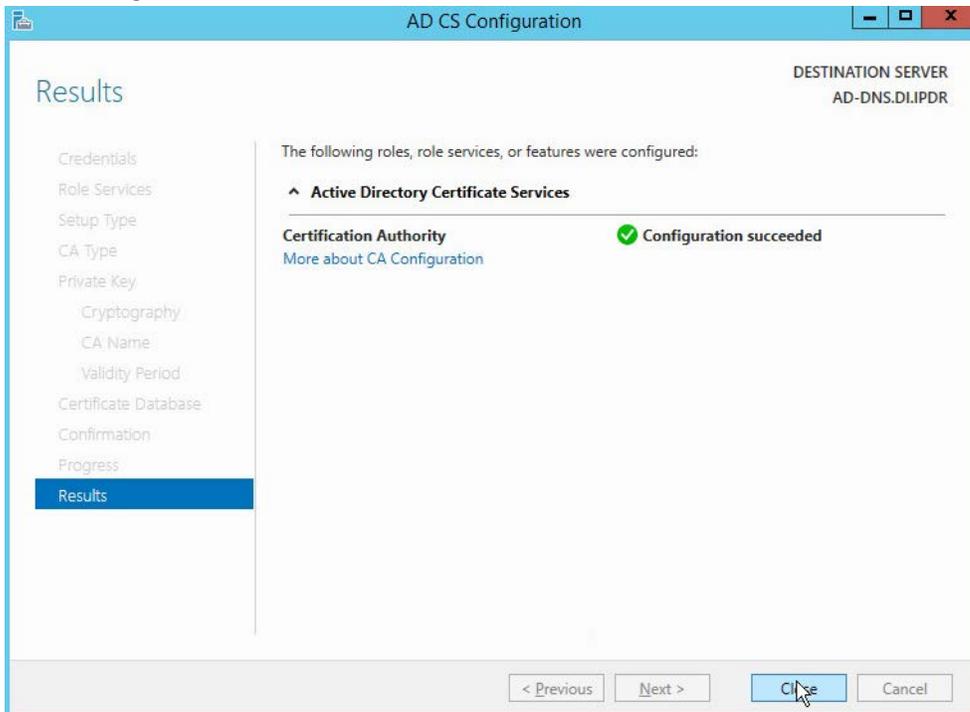


390

391 36. Click **Next**.



392 37. Click **Configure**.



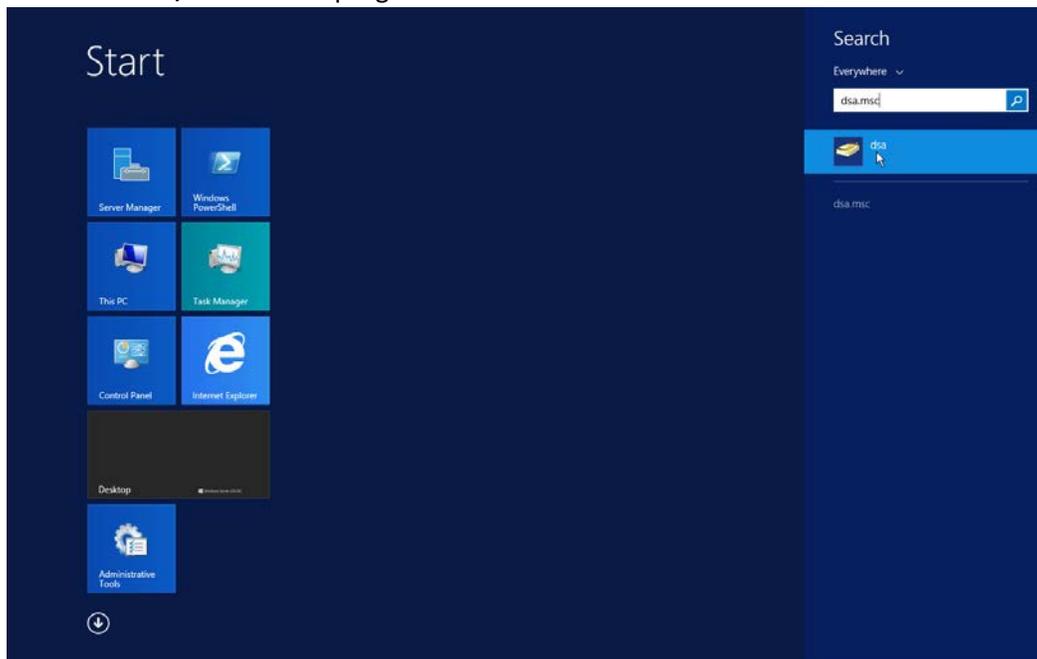
394

395 38. Click **Close**.

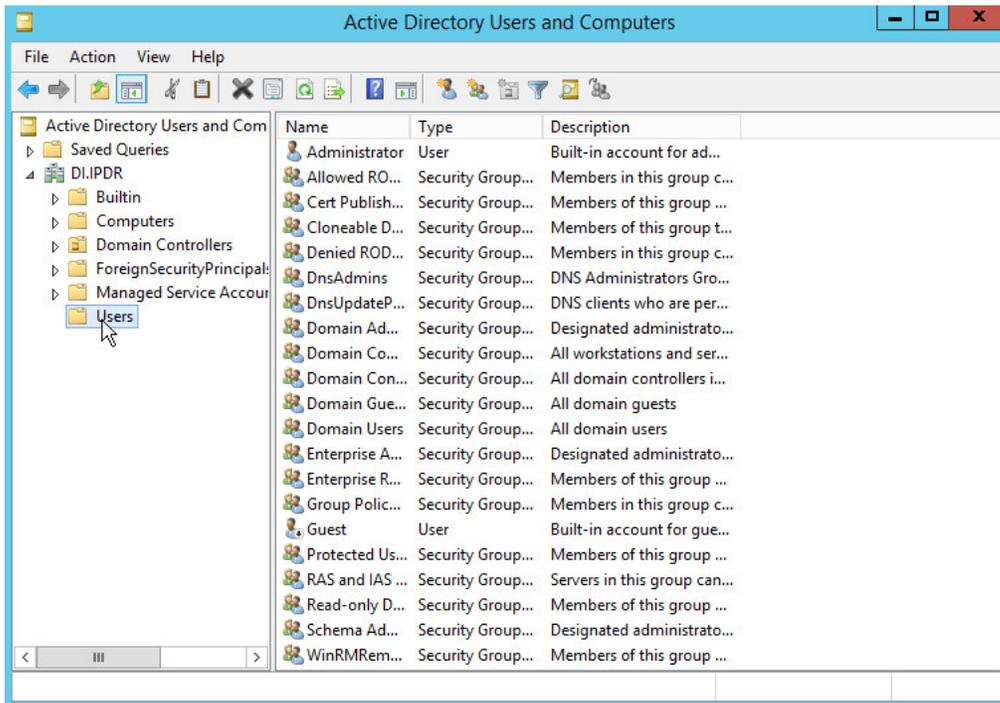
### 396 2.1.3 Configure Account to Add Computers to Domain

397 1. Open the **Start** menu.

398 2. Enter **dca.msc**, and run the program.

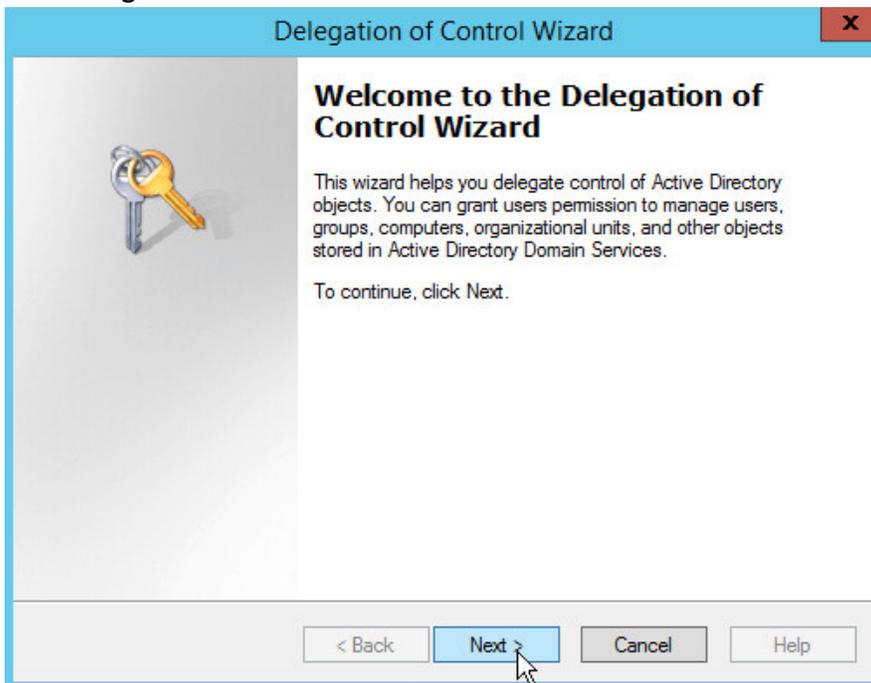


399 3. Right-click on **Users** in the left panel.  
400



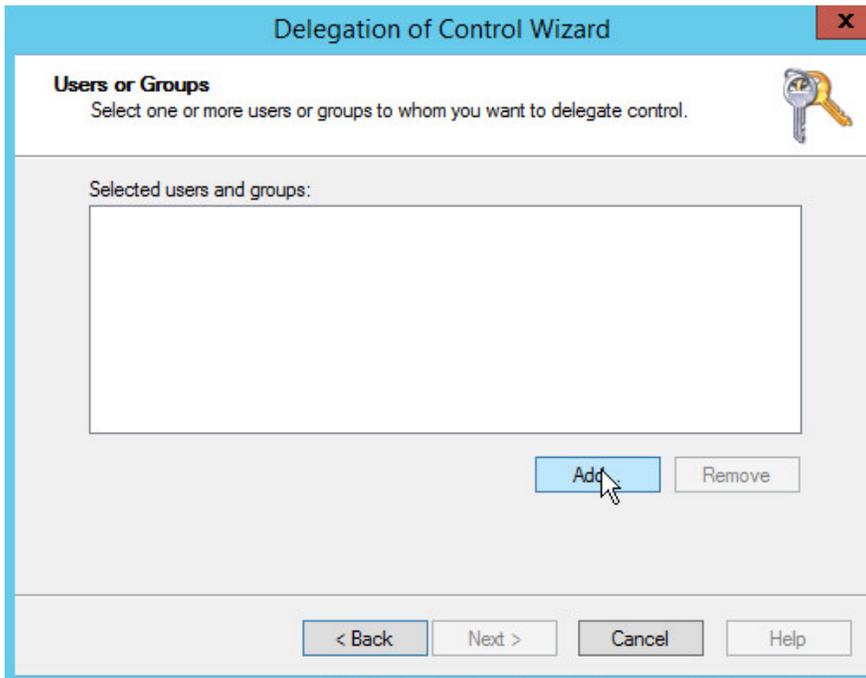
401  
402

4. Click **Delegate Control**.



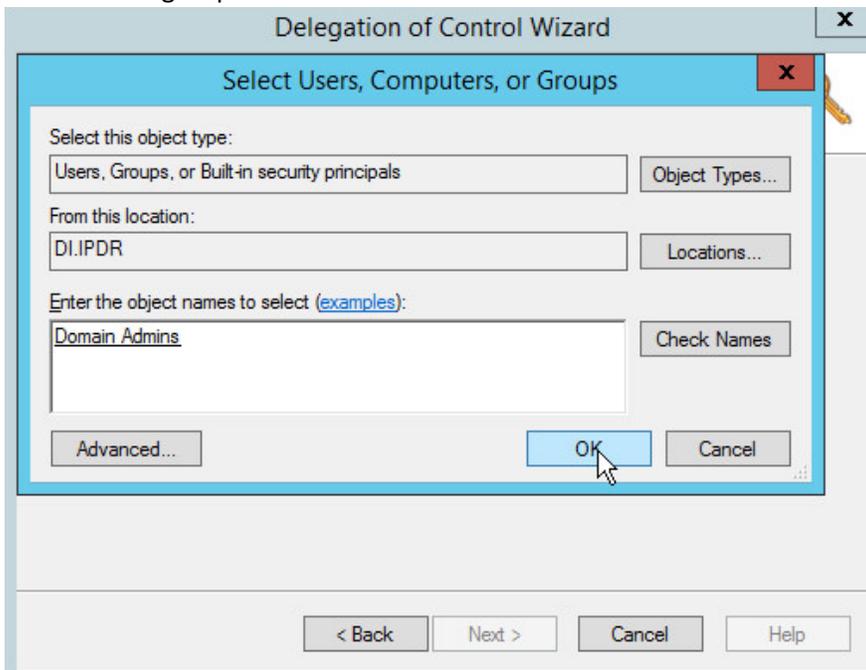
403  
404

5. Click **Next**.



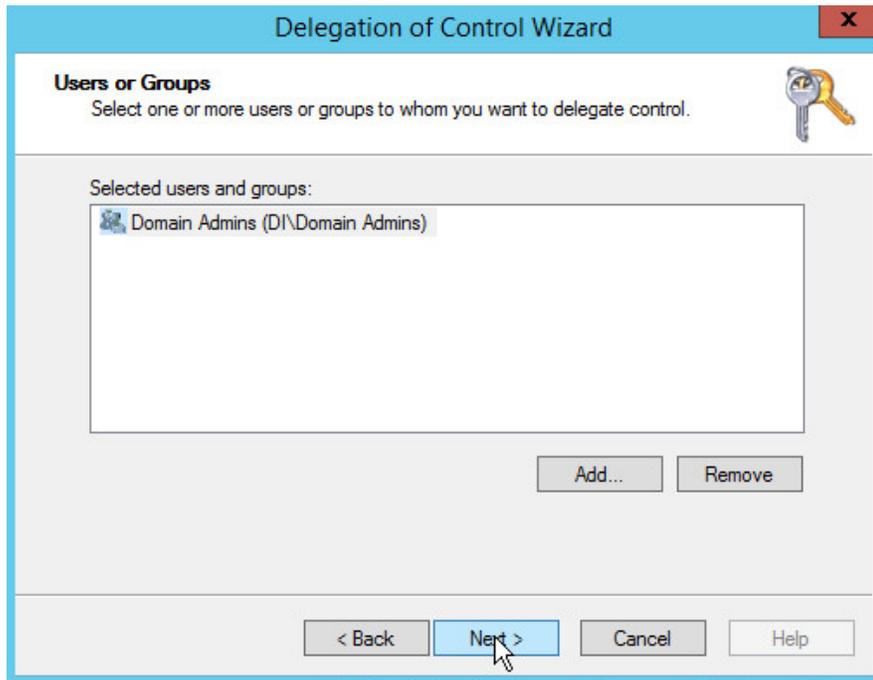
405  
406  
407

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



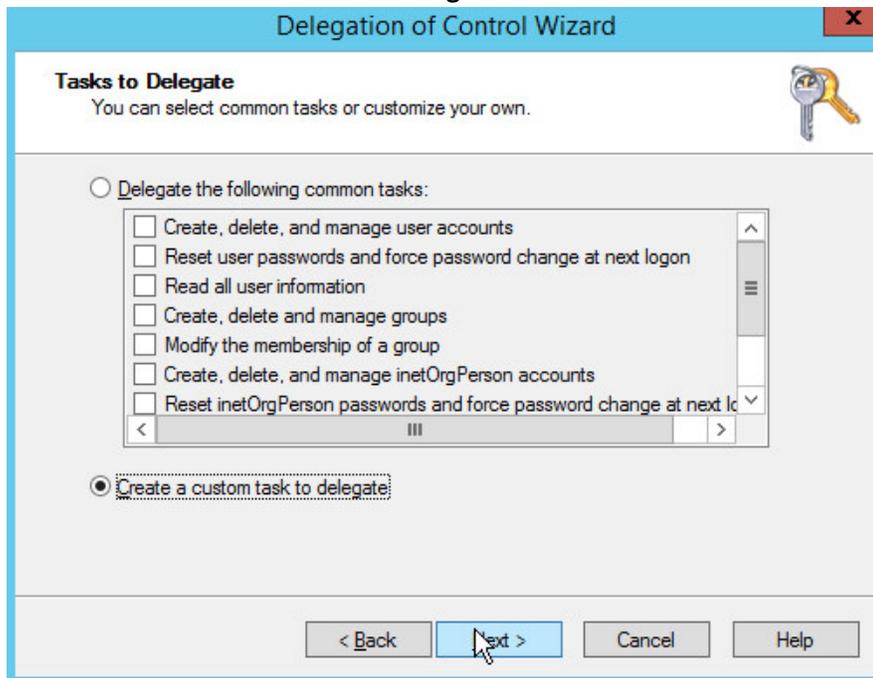
408  
409

8. Click **OK**.



410  
411  
412

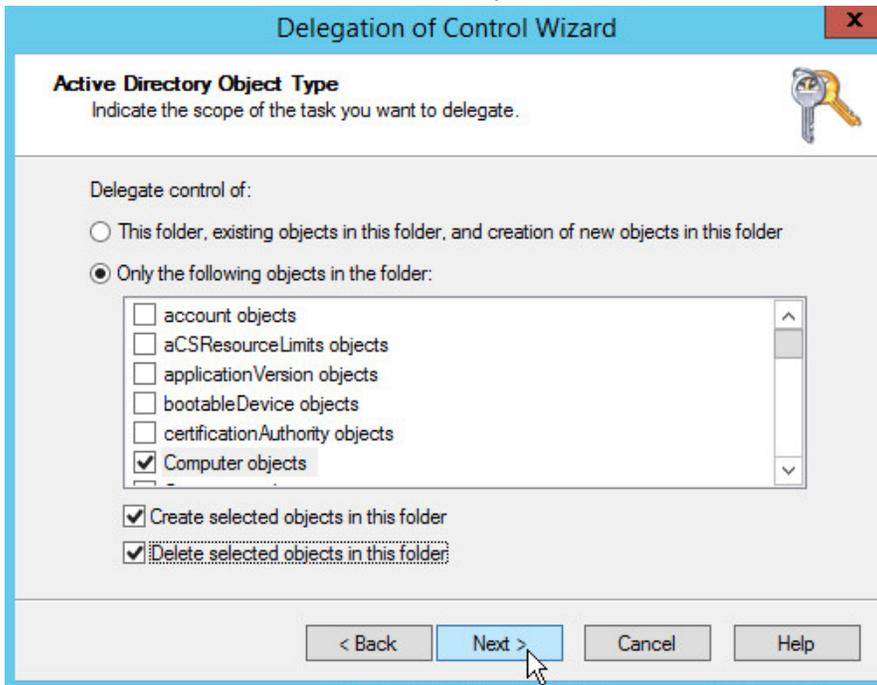
9. Click **Next**.
10. Choose **Create a custom task to delegate**.



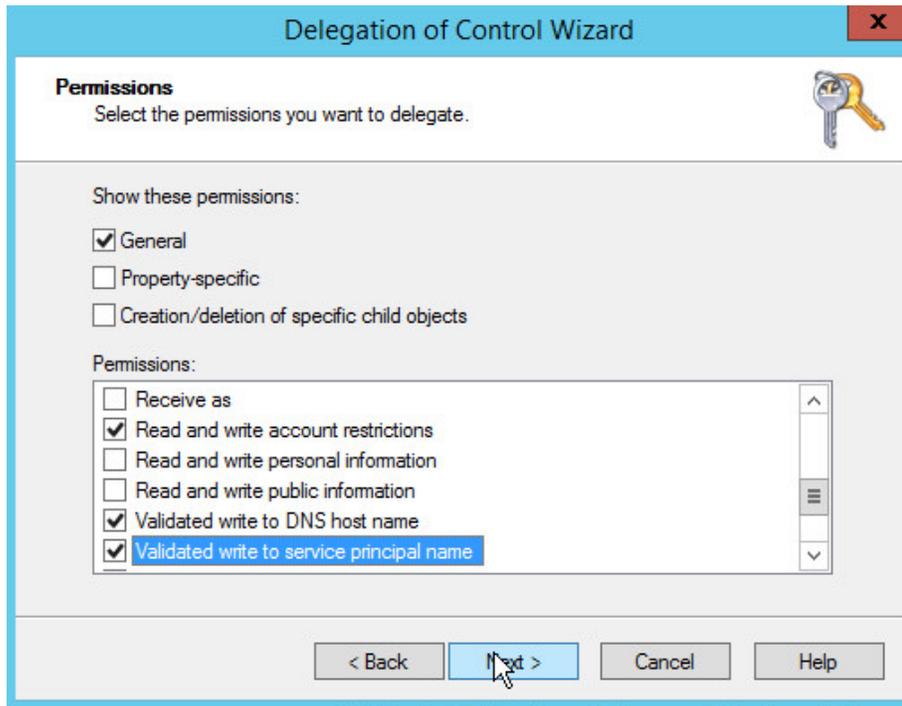
413  
414  
415

11. Click **Next**.
12. Choose **Only the following objects in the folder**.

- 416 13. Check the box next to **Computer objects**.
- 417 14. Check the box next to **Create selected objects in this folder**.
- 418 15. Check the box next to **Delete selected objects in this folder**.



- 419 16. Click **Next**.
- 420
- 421 17. Check the boxes next to **Reset password**, **Read and write account restrictions**, **Validated write**
- 422 **to DNS host name**, and **Validated write to service principal name**.



423  
424

18. Click **Next**.

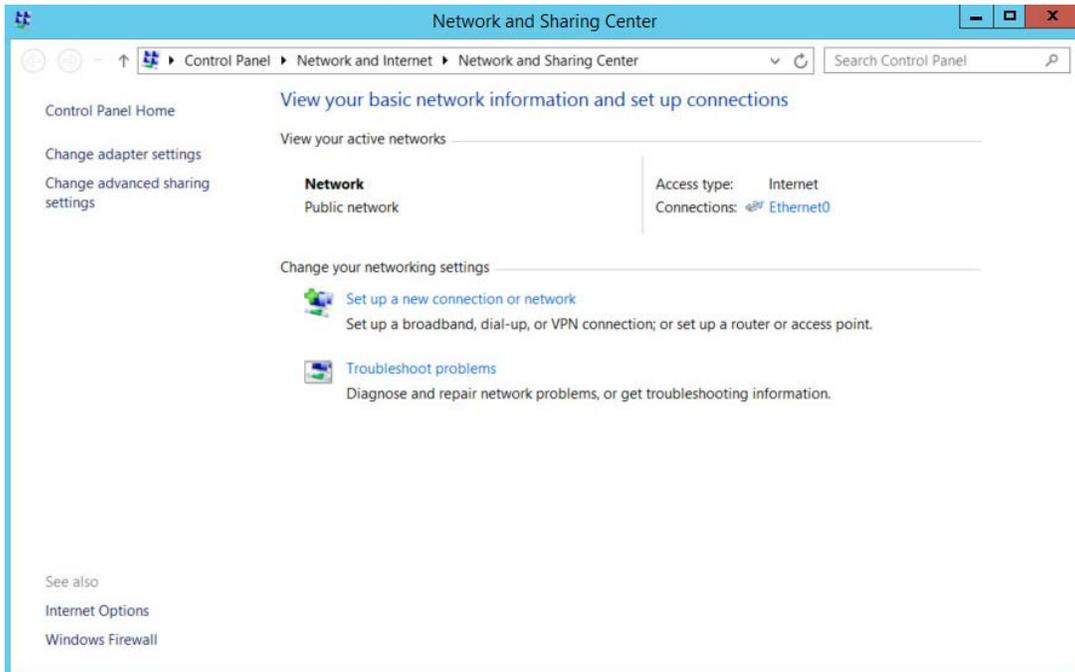


425  
426

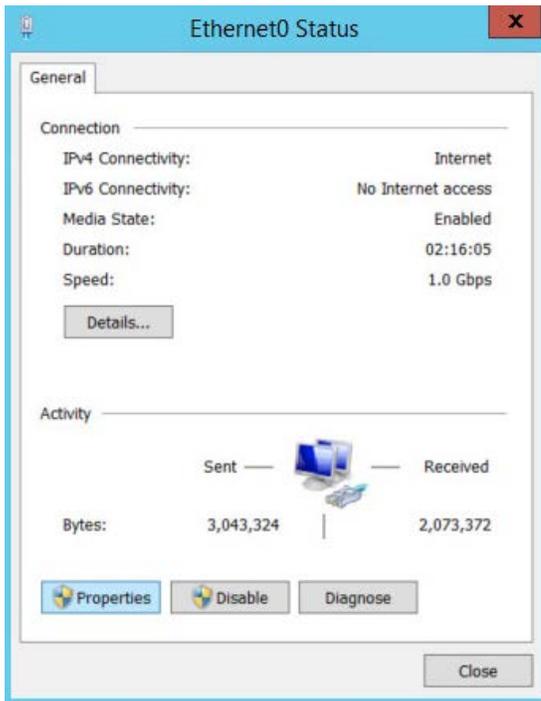
19. Click **Finish**.

427 **2.1.4 Add Machines to the Domain**

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

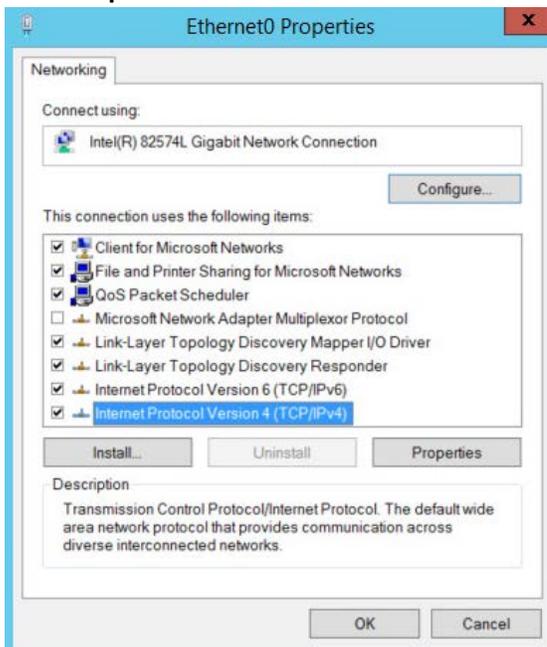


- 430 3. Click the name of the internet adapter.  
431



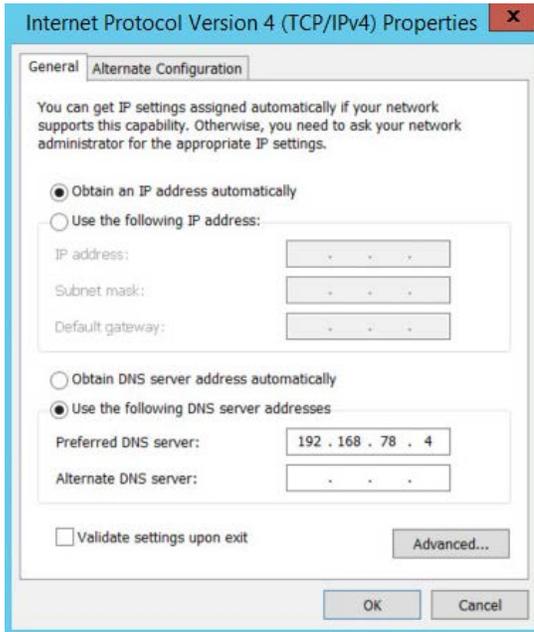
432  
433

4. Click **Properties**.

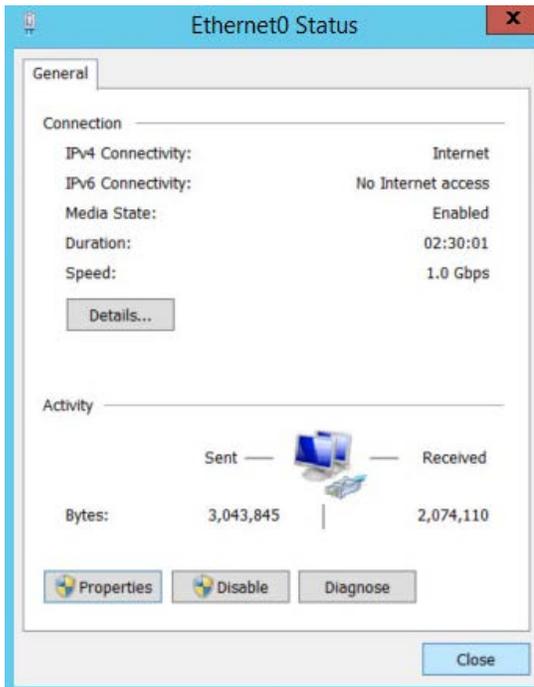


434  
435  
436  
437

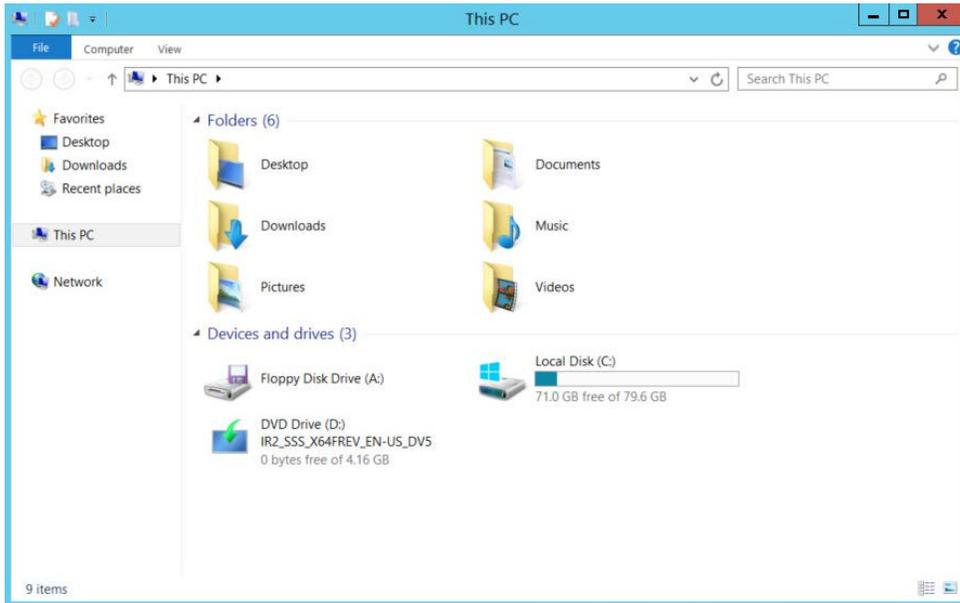
5. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
6. Select **Use the following DNS server addresses**.
7. Enter the **IP address** of the DNS server.



- 438
  - 439
  - 440
8. Click **OK**.
  9. Click **OK**.

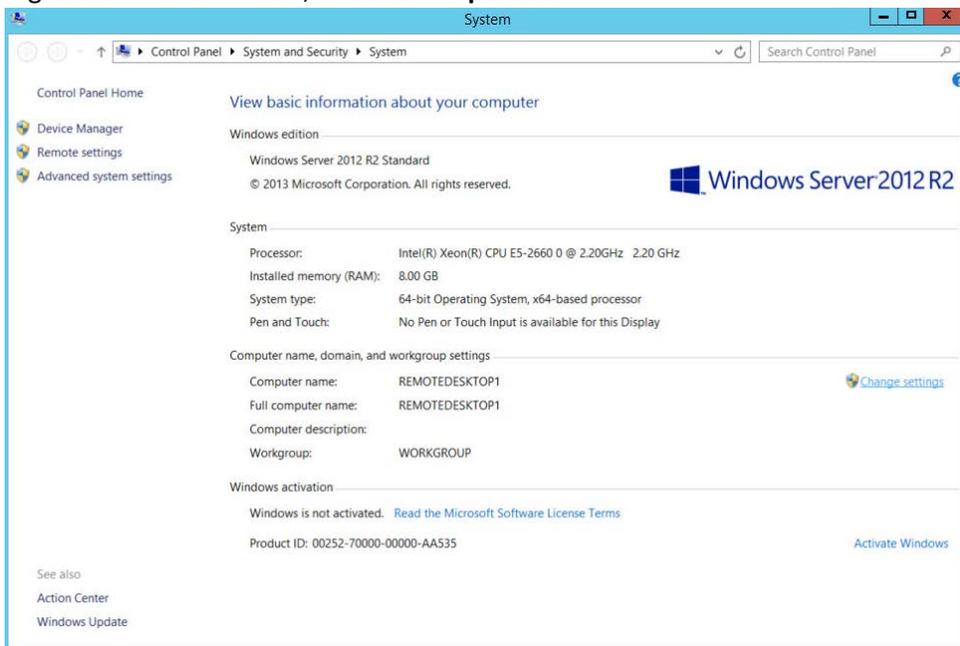


- 441
  - 442
  - 443
10. Click **Close**.
  11. Navigate to **This PC**.



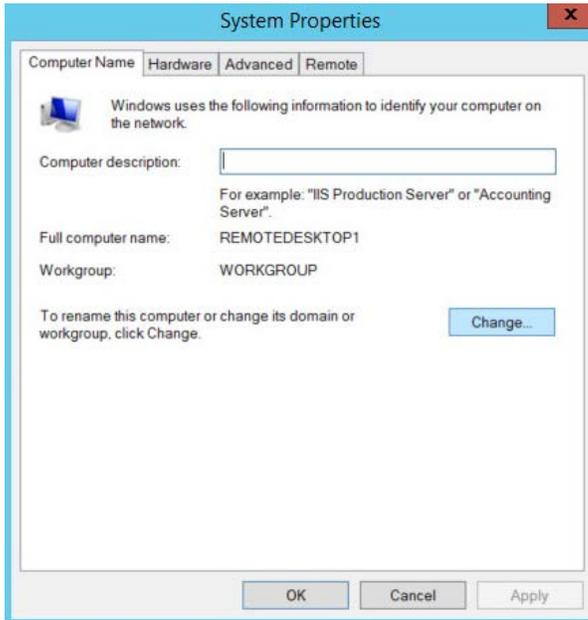
444  
445

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



446  
447

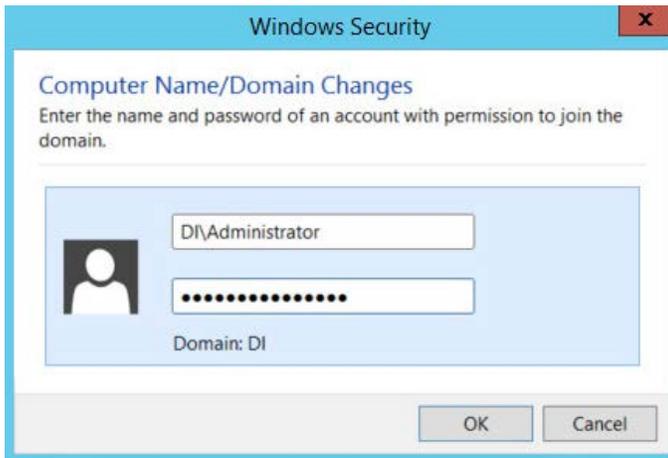
13. Click **Change Settings**.



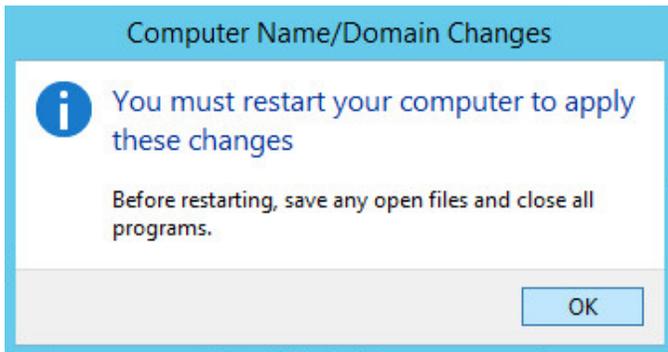
- 448
  - 449
  - 450
  - 451
14. Click **Change**.
  15. Select **Domain**.
  16. Enter the domain.



- 452
  - 453
  - 454
17. Click **OK**.
  18. Enter the name and password of an account with privileges to add computers to the domain.



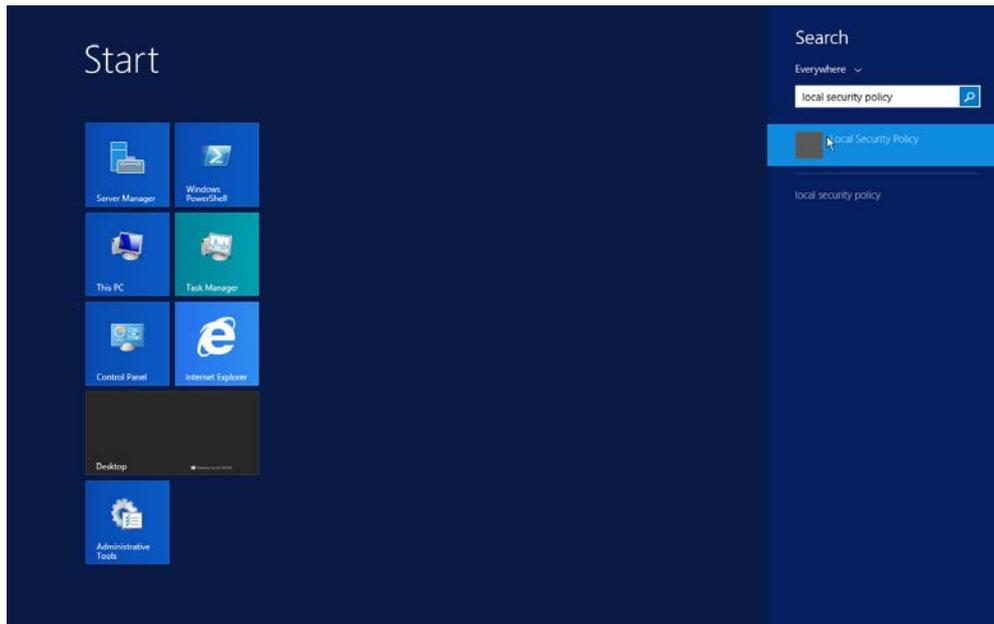
- 455
  - 456
19. Click **OK**.



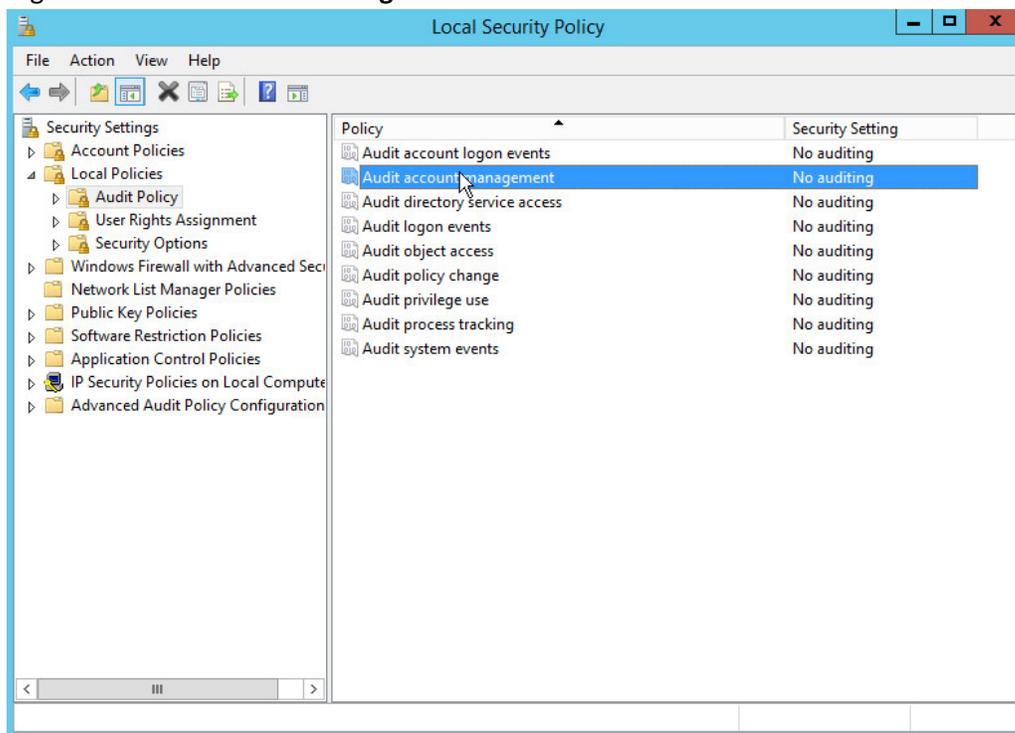
- 457
  - 458
20. Click **OK** when prompted to restart the computer.

## 459 2.1.5 Configure Active Directory to Audit Account Activity

- 460 1. Open the **Start** Menu.

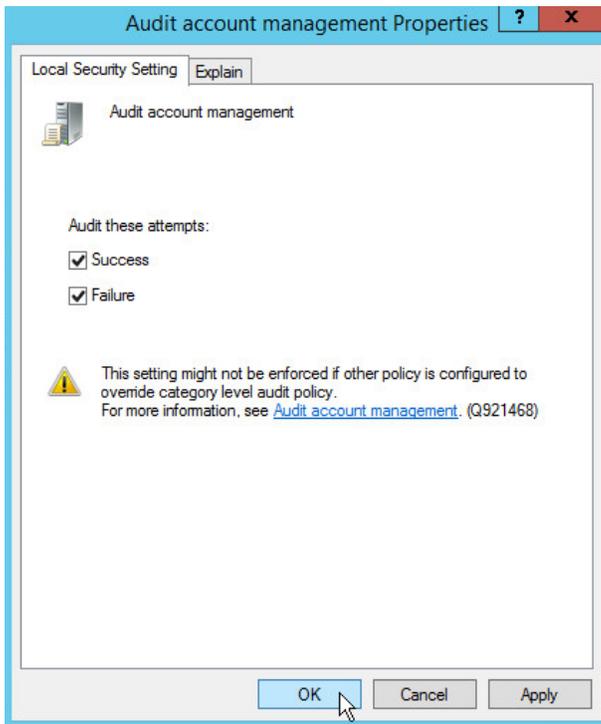


- 461
- 462 2. Enter Local Security Policy in the search bar, and open the program.
- 463 3. Navigate to **Local Policies > Audit Policy**.
- 464 4. Right-click **Audit account management**.



- 465
- 466 5. Click **Properties**.

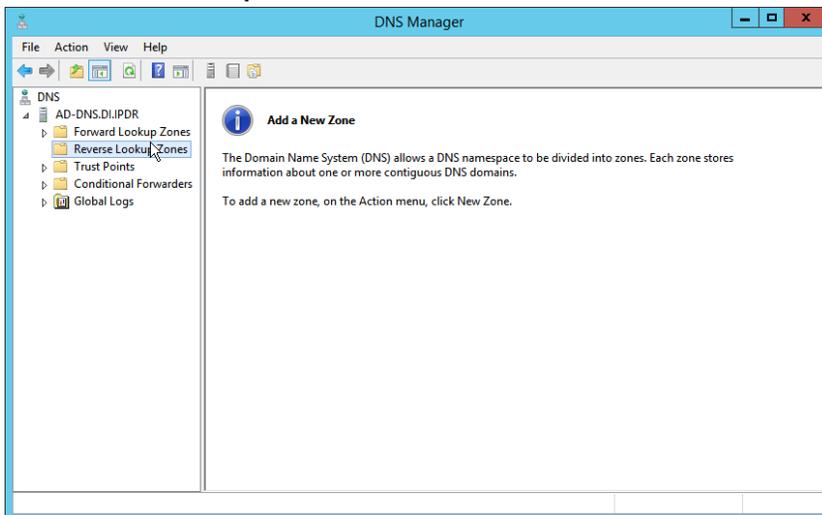
- 467 6. Check the boxes next to **Success** and **Failure**.



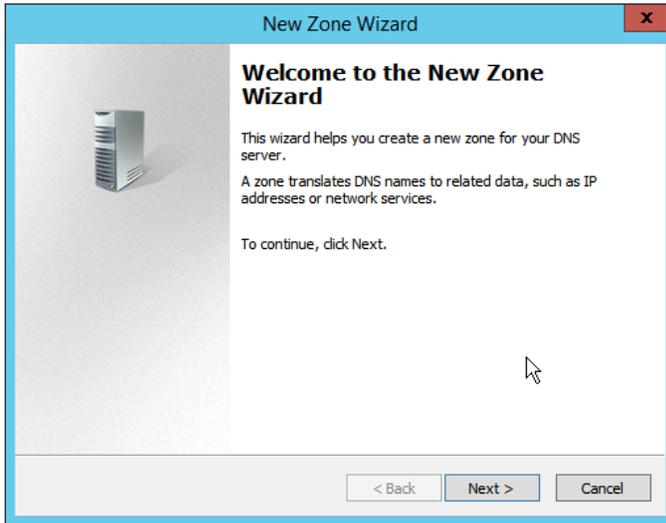
- 468  
469 7. Click **OK**.

## 470 2.1.6 Configure Reverse Lookup Zones

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

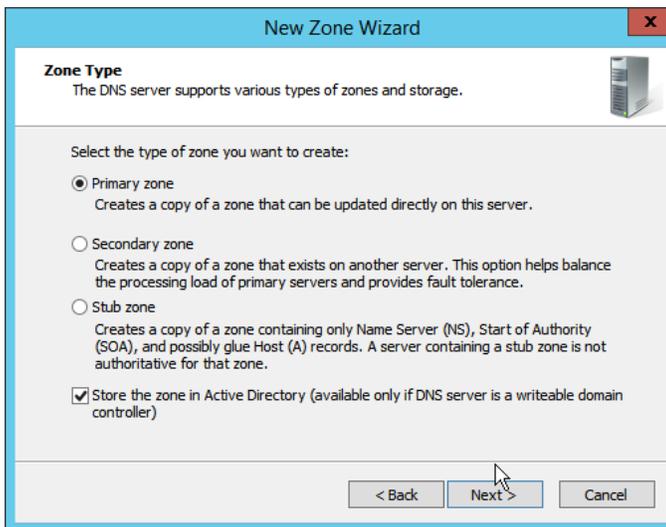


- 473  
474 3. Click **Action > New Zone**.



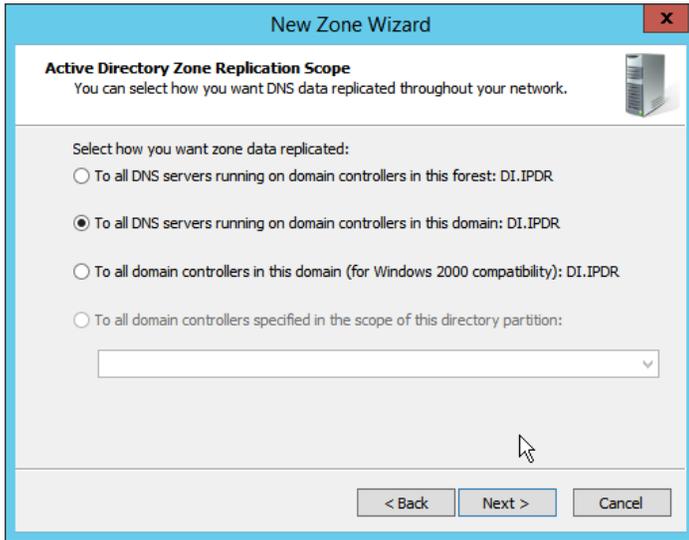
475  
476

4. Click **Next**.



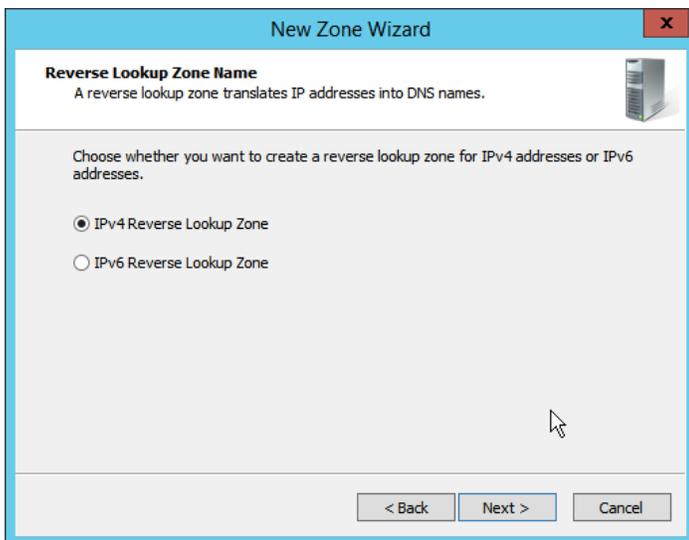
477  
478

5. Click **Next**.



479  
480

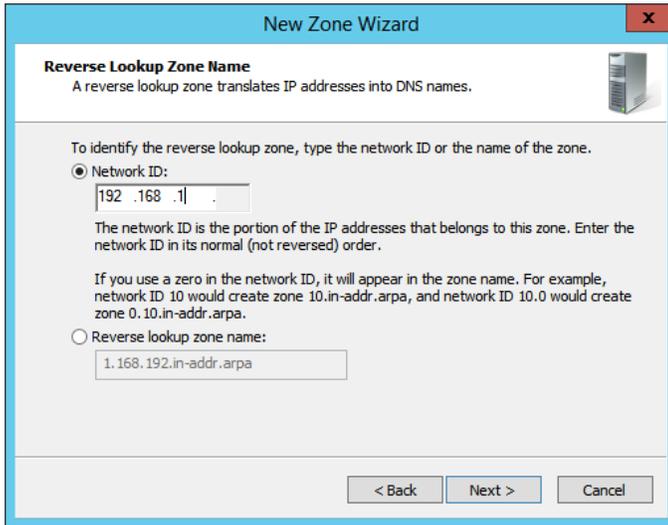
6. Click **Next**.



481  
482  
483

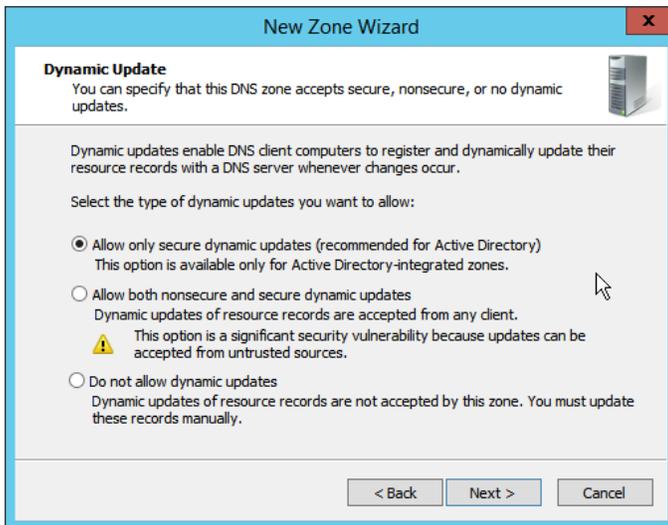
7. Click **Next**.

8. Enter the first three parts of the IP address of the AD/DNS server (for example, 192.168.1).



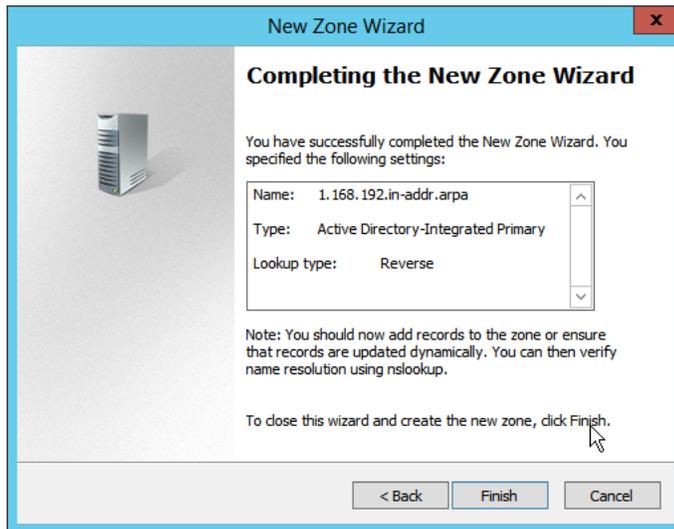
484  
485

9. Click **Next**.



486  
487

10. Click **Next**.



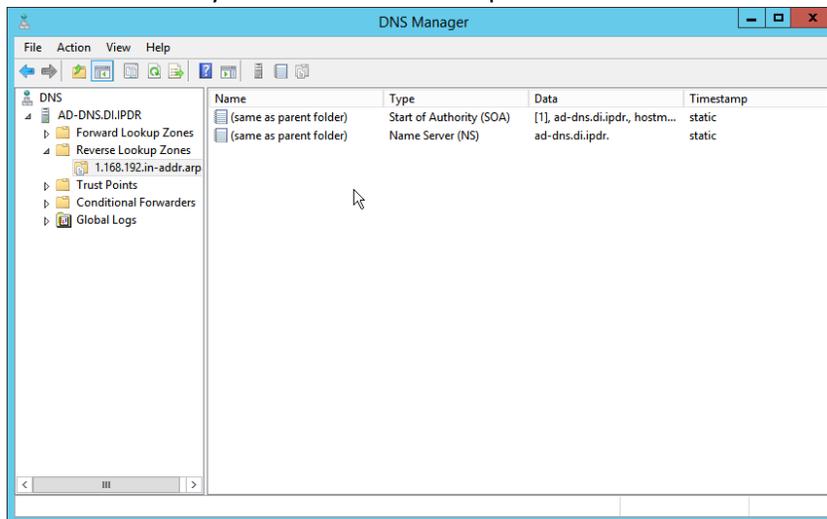
488

489

490

11. Click **Finish**.

12. Click on the newly created reverse lookup zone.



491

492

493

494

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

**New Resource Record**

Pointer (PTR)

Host IP Address:  
192.168.1.12

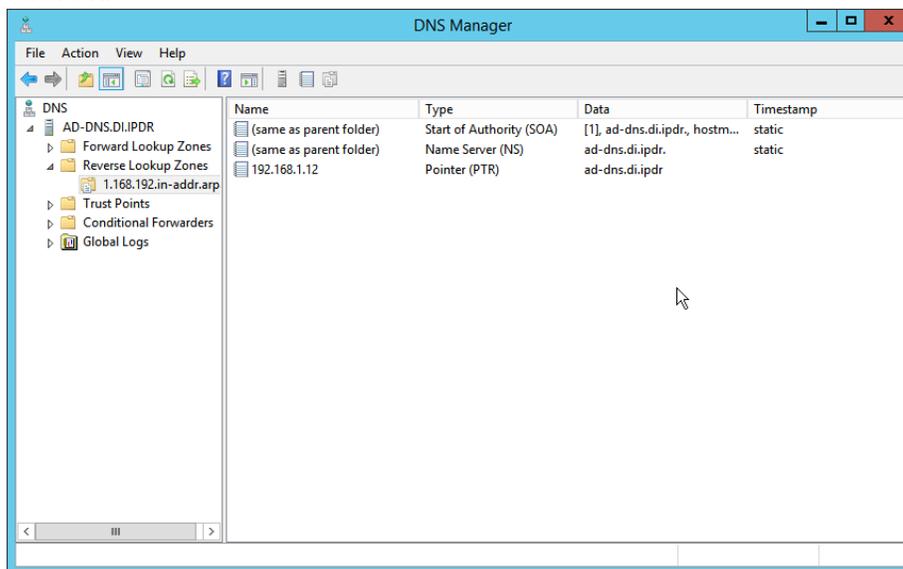
Fully qualified domain name (FQDN):  
12.1.168.192.in-addr.arpa

Host name:  
ad-dns.di.ipdr

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

495  
496

16. Click **OK**.



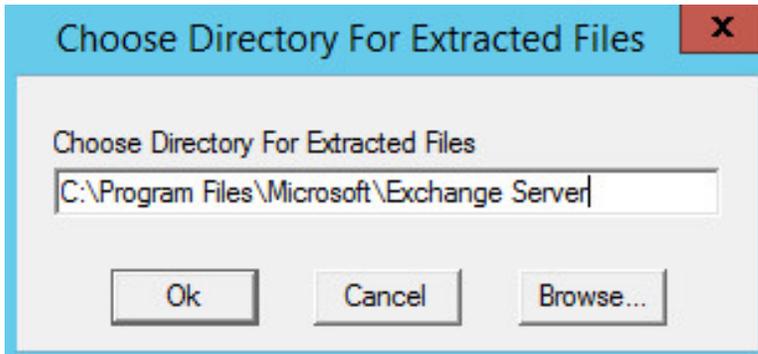
497

## 498 2.2 Microsoft Exchange Server

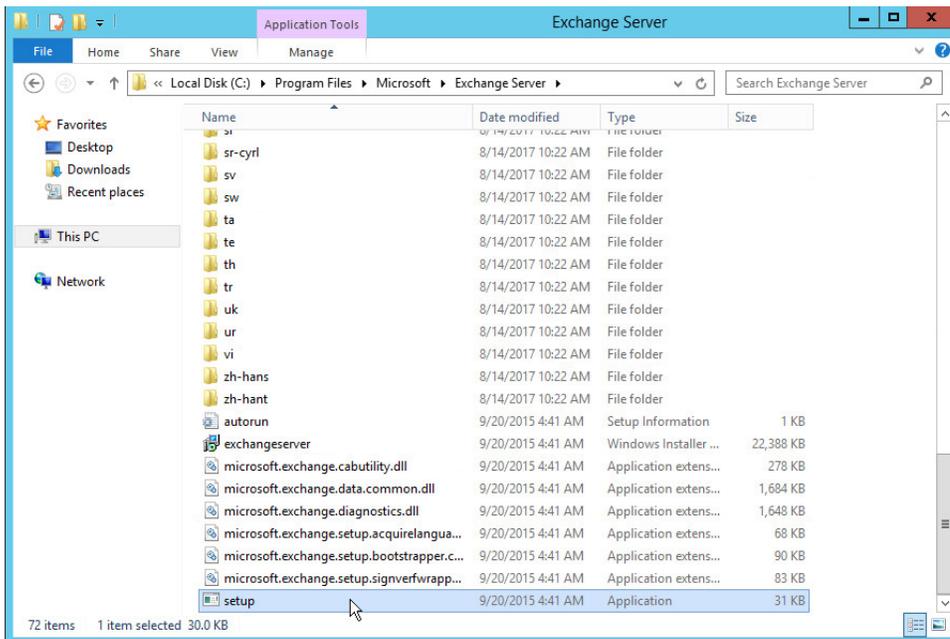
499 As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the  
500 installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2  
501 machine.

## 502 2.2.1 Install Microsoft Exchange

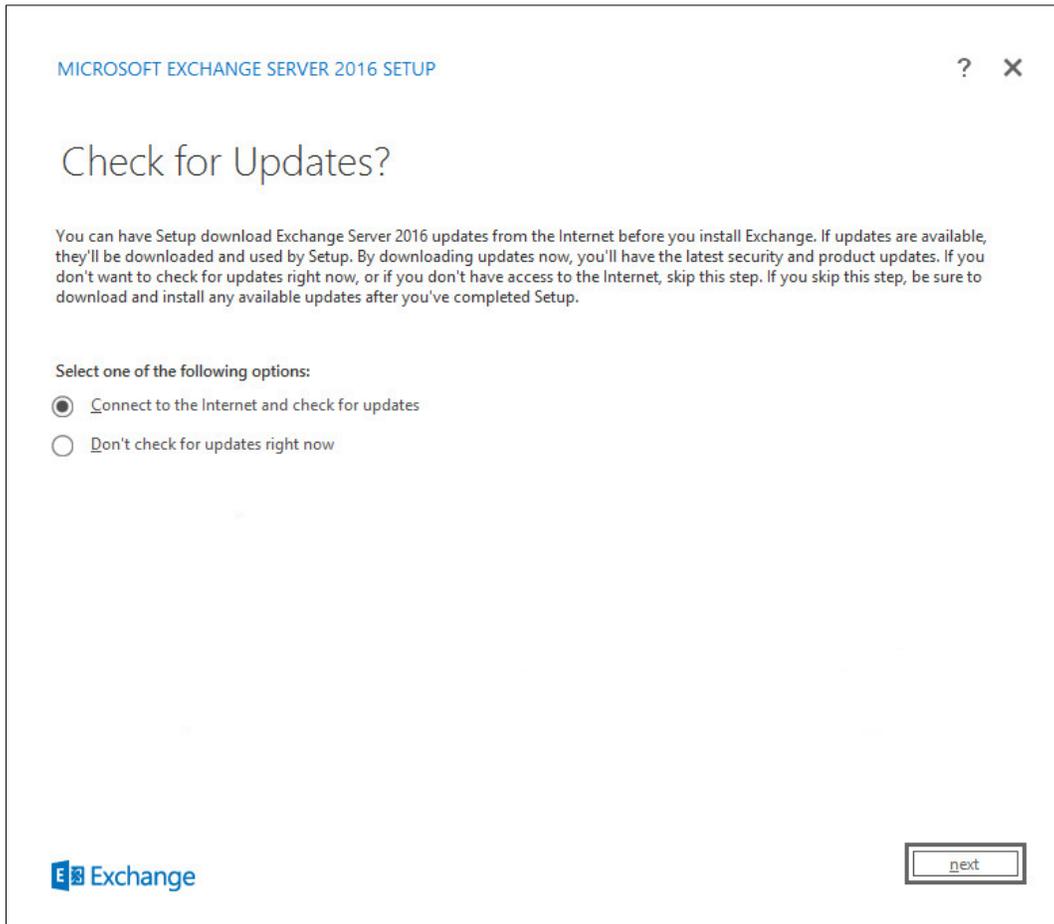
- 503 1. Run **Exchange2016-x64.exe**.  
 504 2. Choose the directory for the extracted files.



- 505 3. Click **OK**.  
 506



- 507 4. Enter the directory and run **setup.exe**.  
 508 5. Select **Connect to the Internet and check for updates**.  
 509

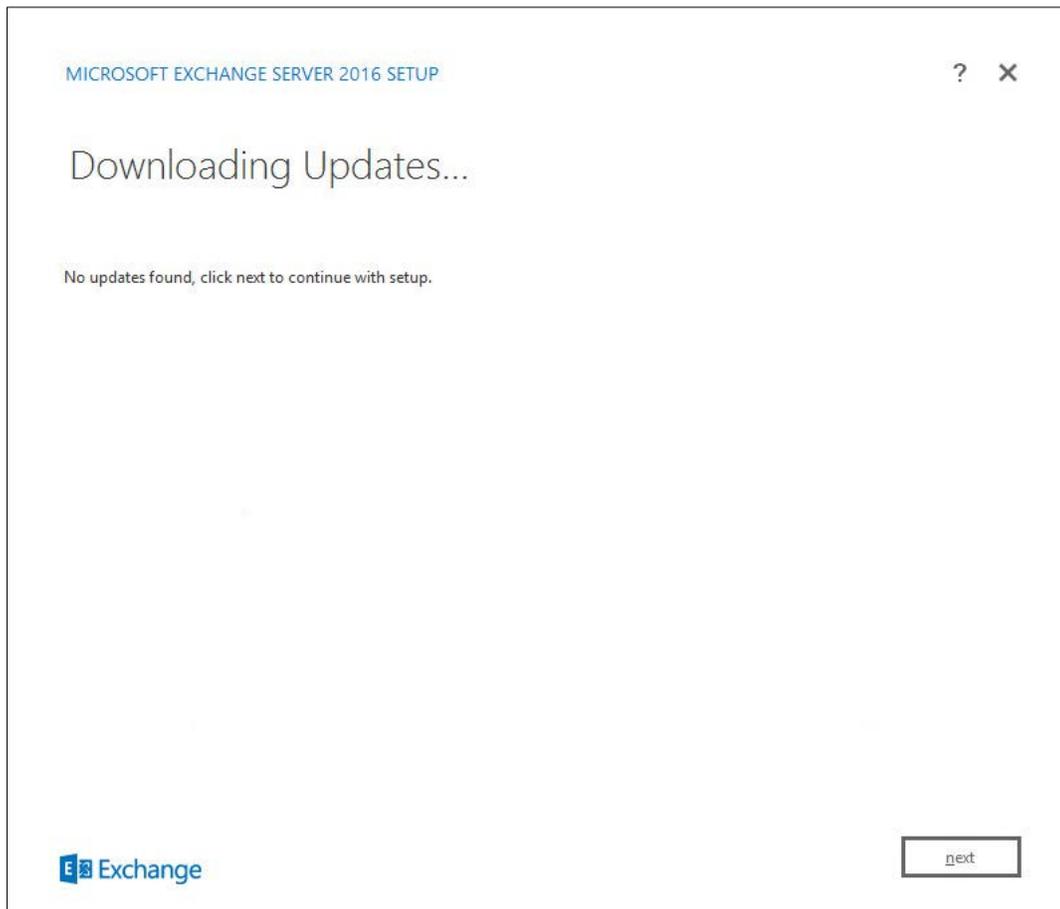


510

511

512

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



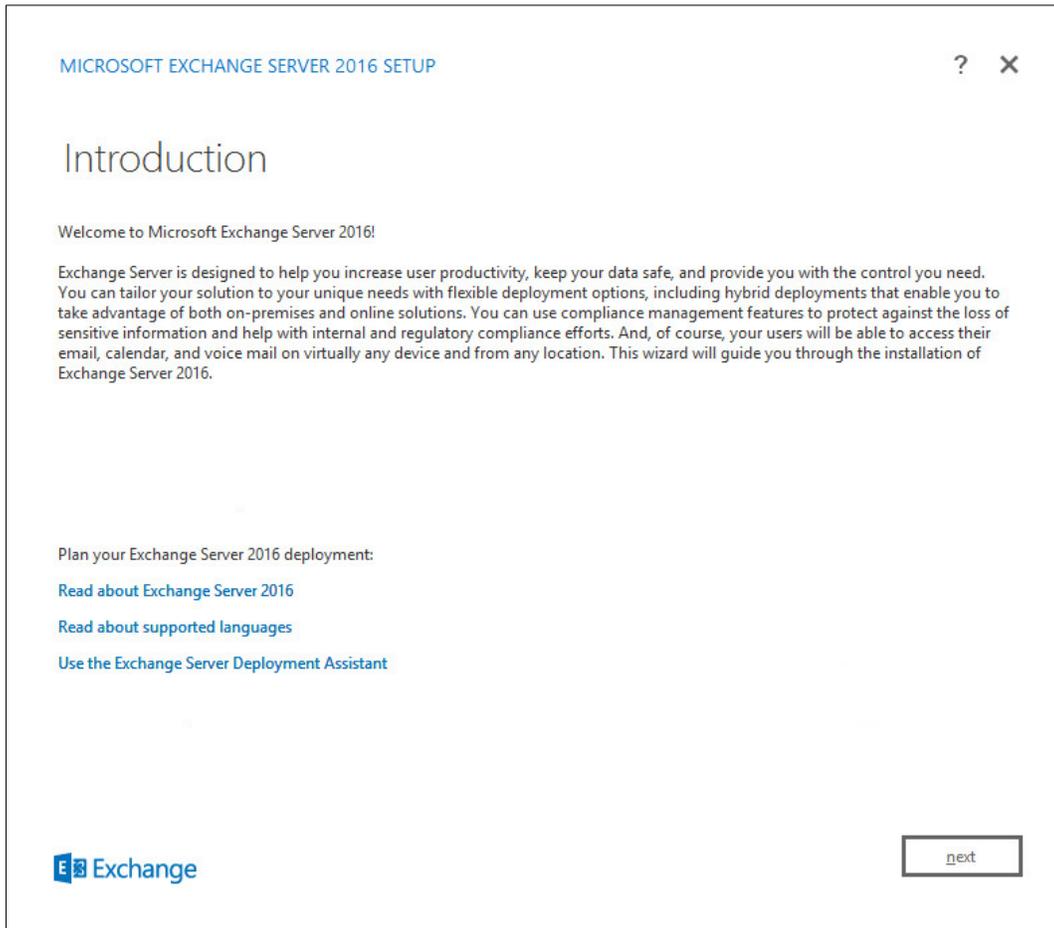
513

514

515

8. Click **Next**.

9. Wait for the copying to finish.



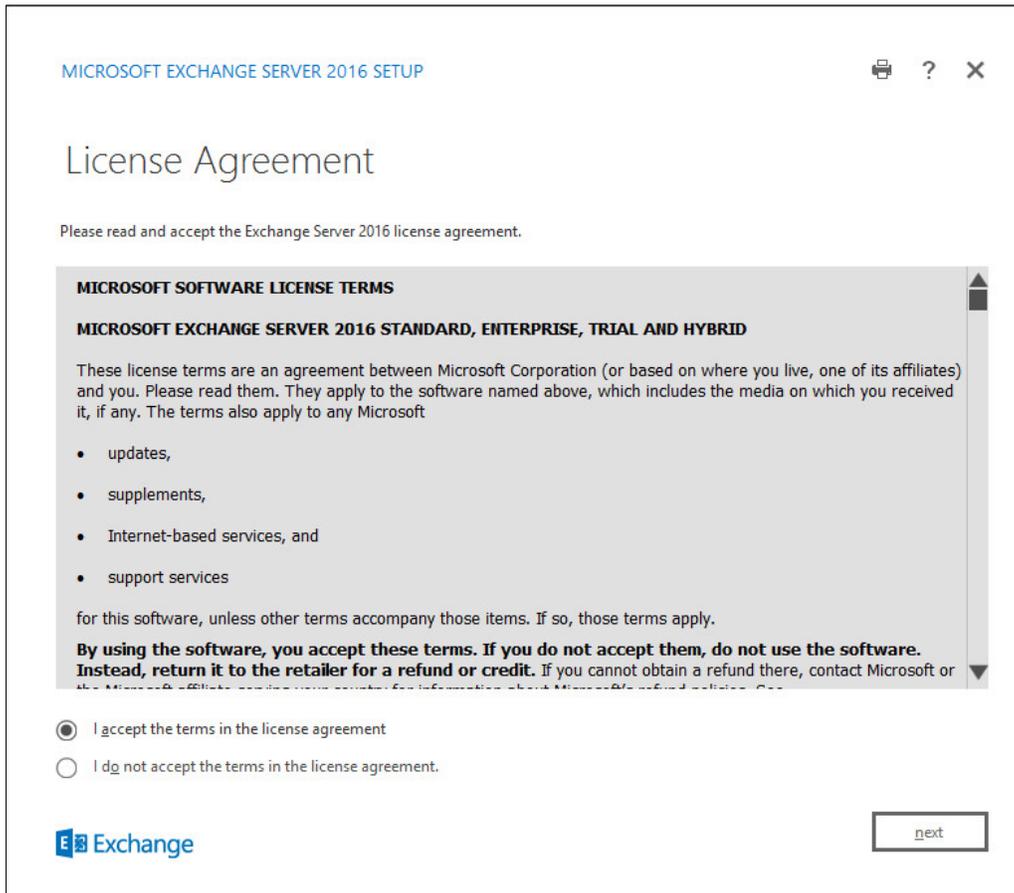
516

517

518

10. Click **Next**.

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



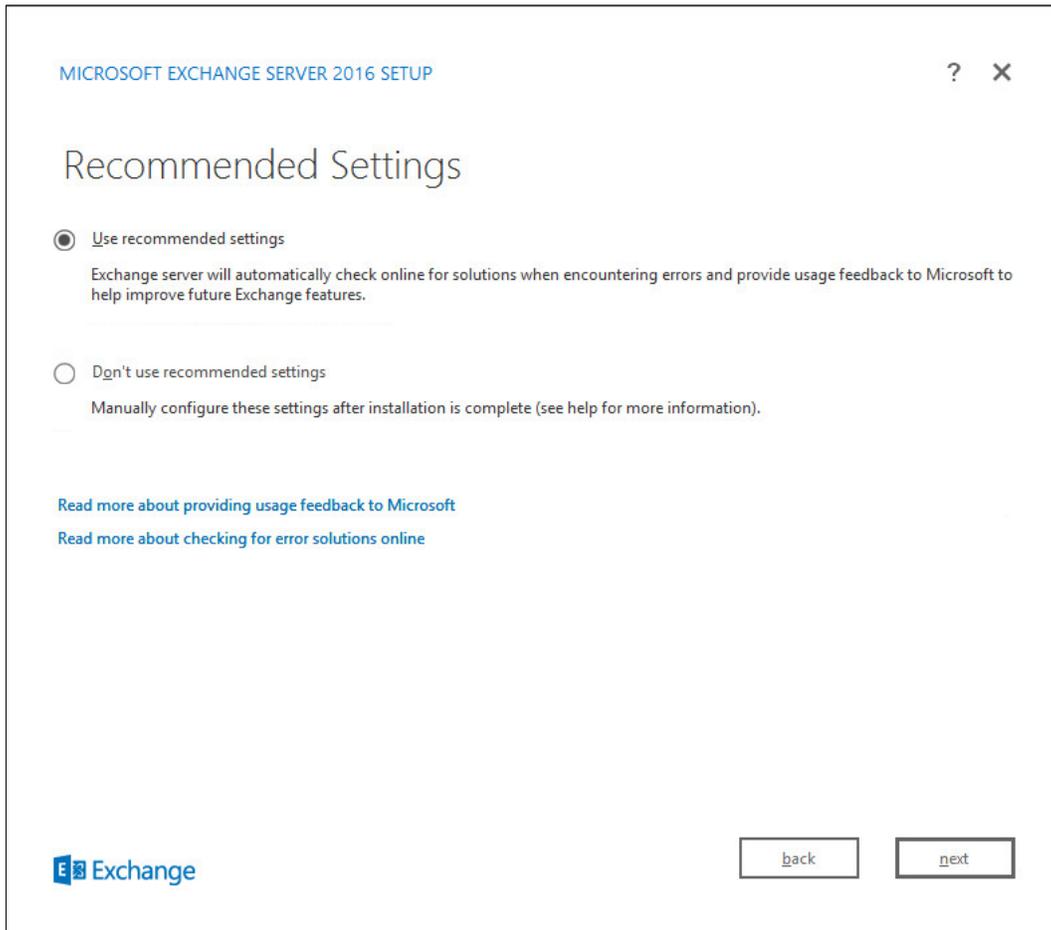
519

520

521

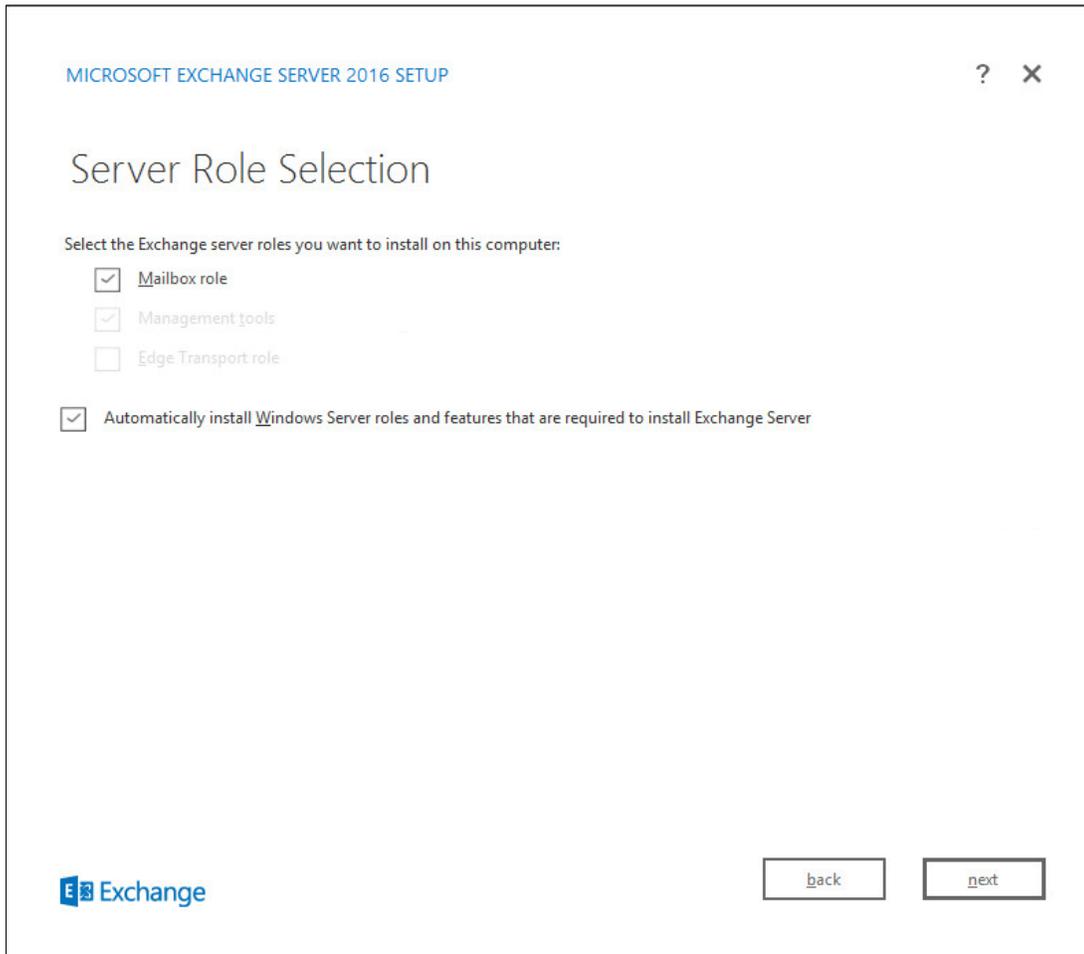
12. Click **Next**.

13. Click **Use Recommended Settings**.



522  
523  
524  
525  
526

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



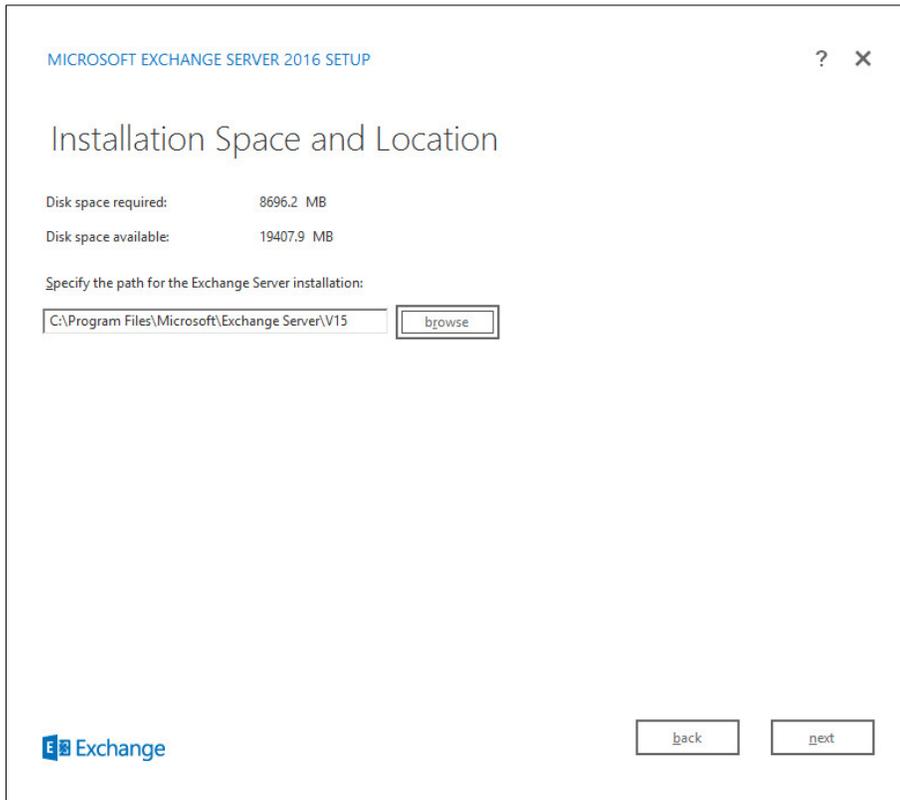
527

528

529

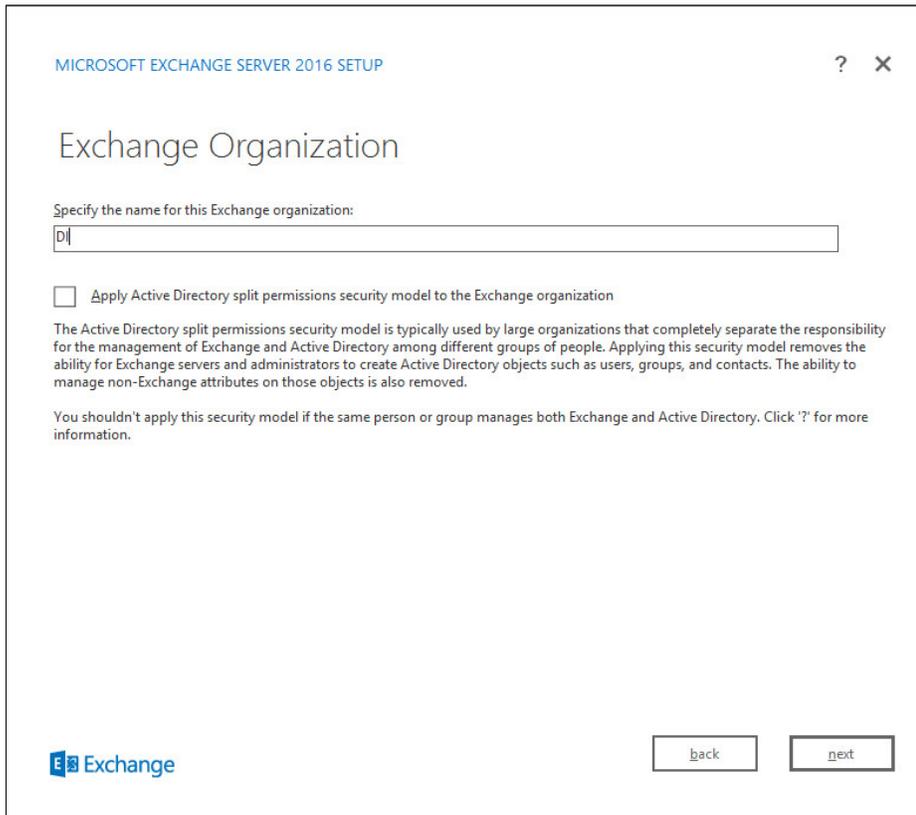
17. Click **Next**.

18. Specify the installation path for MS Exchange.



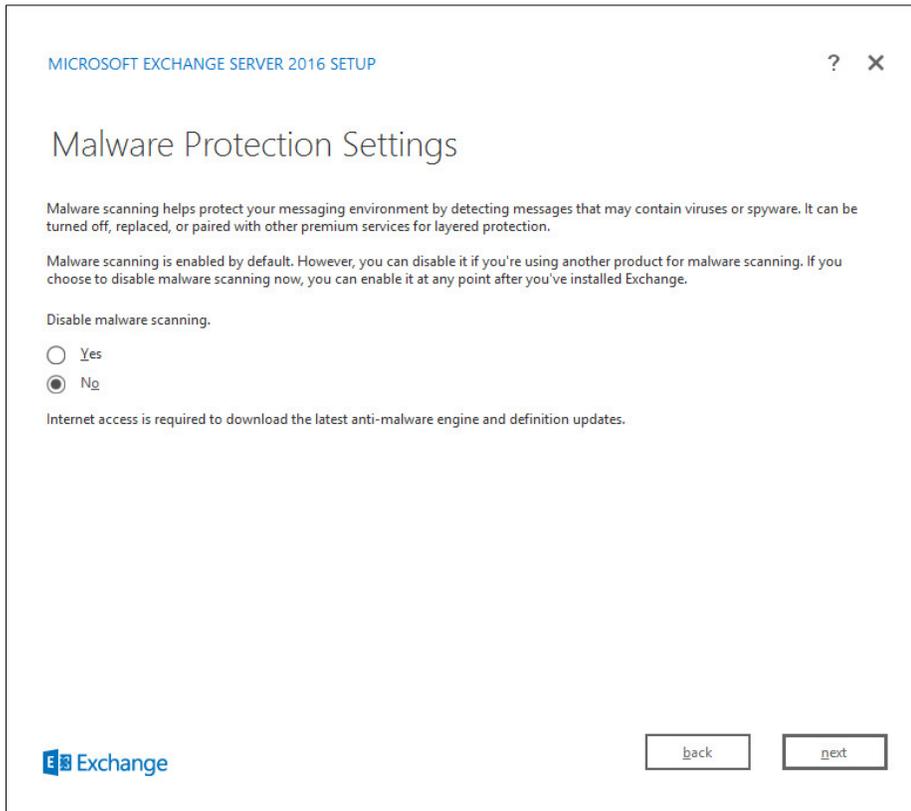
530  
531  
532  
533

19. Click **Next**.
20. Specify the name for the Exchange organization, for example, DI.
21. Decide whether to apply split permissions, based on the needs of the enterprise.



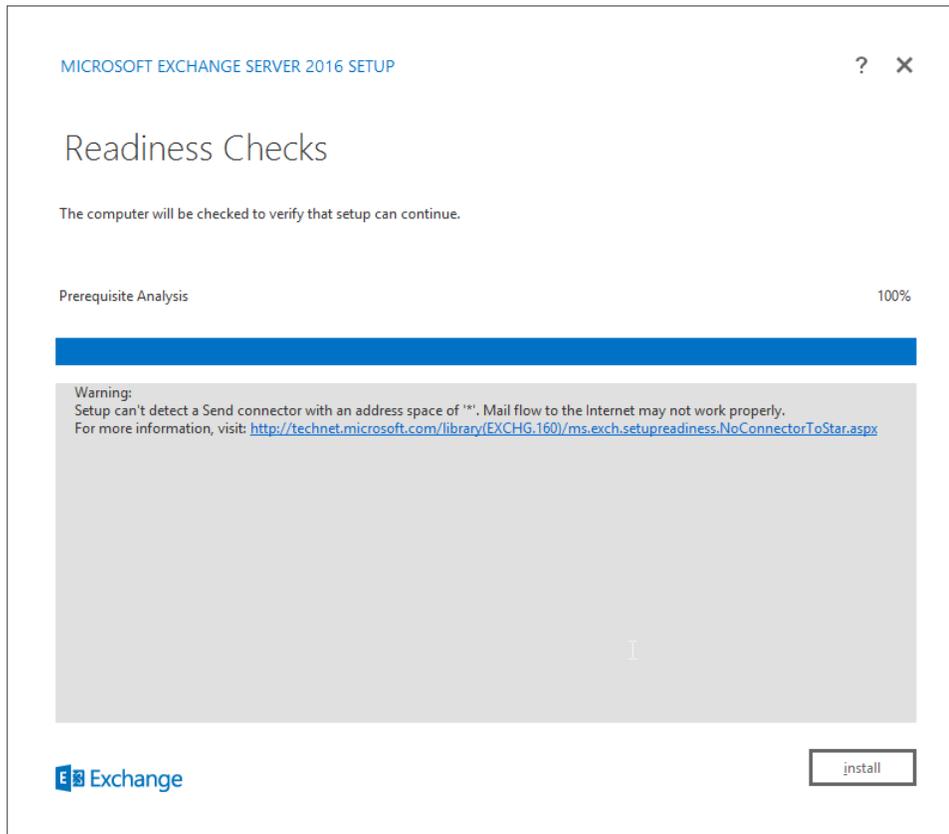
534  
535  
536

- 22. Click **Next**.
- 23. Select **No**.



537  
538  
539  
540

- 24. Click **Next**.
- 25. Install any **prerequisites** listed.
- 26. If necessary, restart the server and re-run **setup.exe**, completing steps 3-22 again.



541

542

27. Click **Install**.

543

## 2.3 Windows Server Hyper-V Role

544

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

545

546

The instructions for enabling the Windows Server Hyper-V Role are retrieved from

547

[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

548

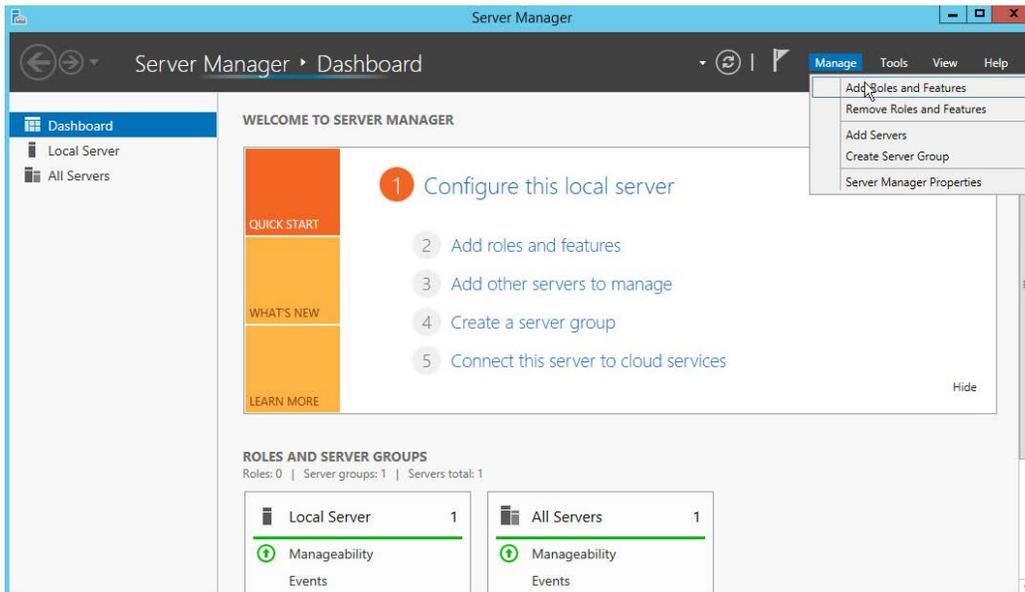
preservation and ease of use.

549

### 2.3.1 Production Installation

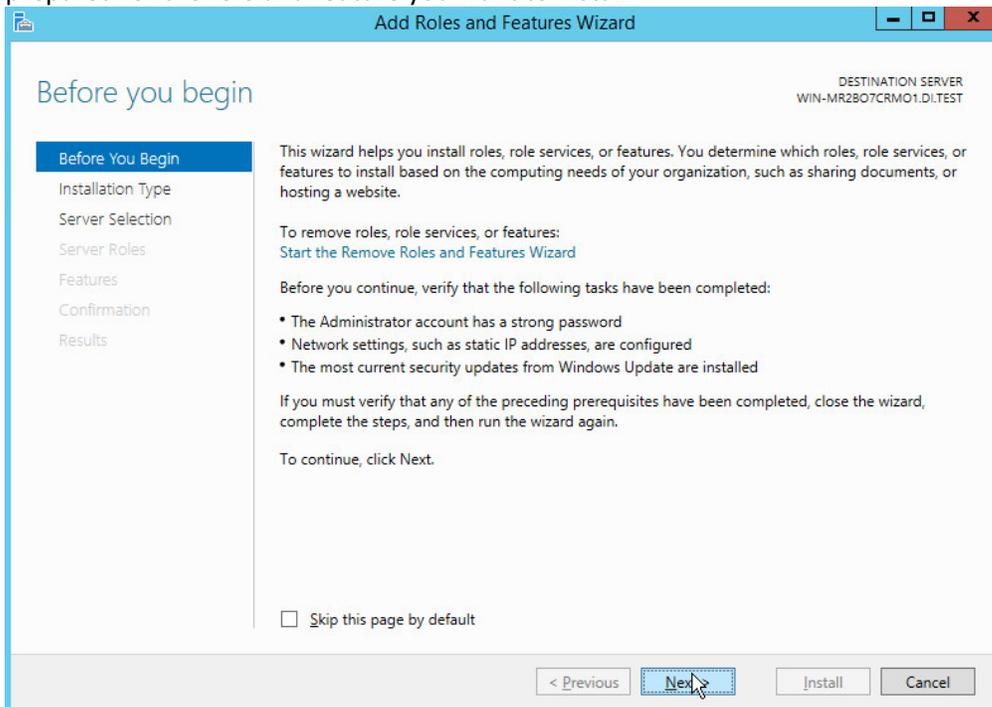
550

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



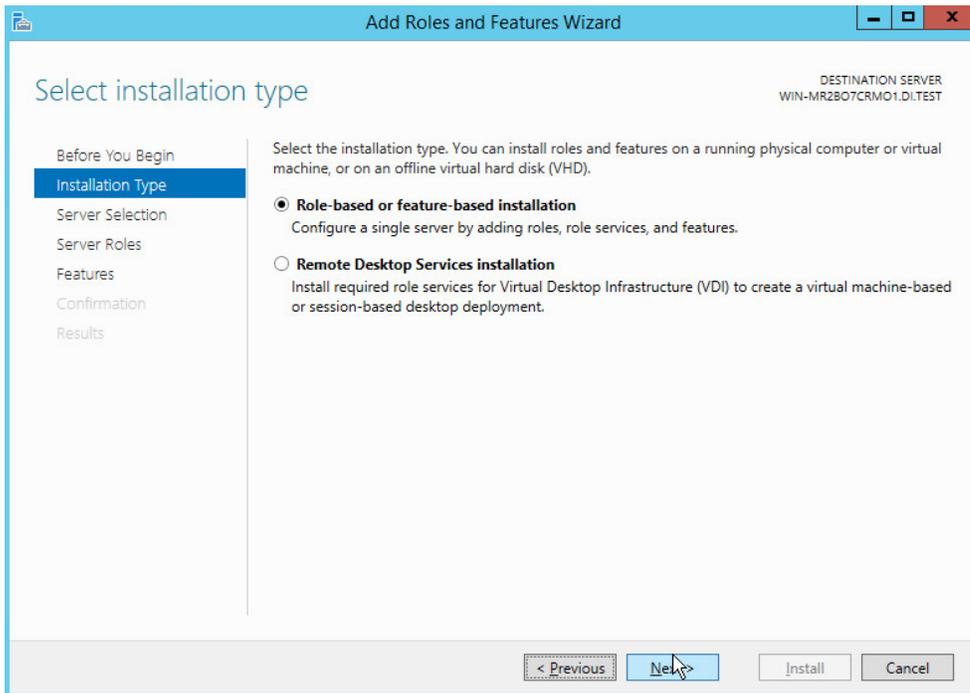
551  
552  
553

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.



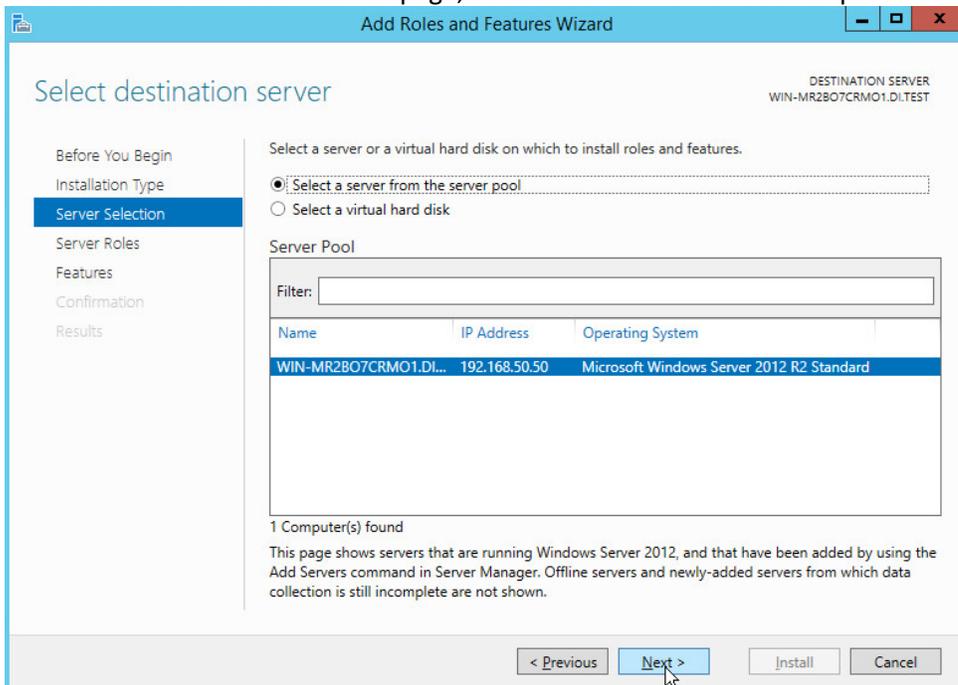
554  
555  
556

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



557  
558  
559

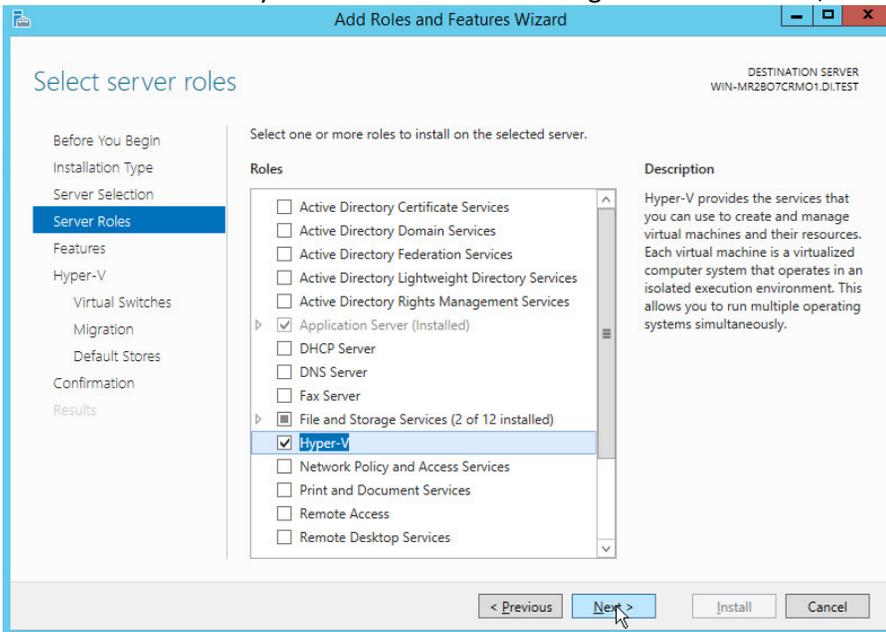
5. Click **Next**.
6. On the **Select destination server** page, select a server from the server pool.



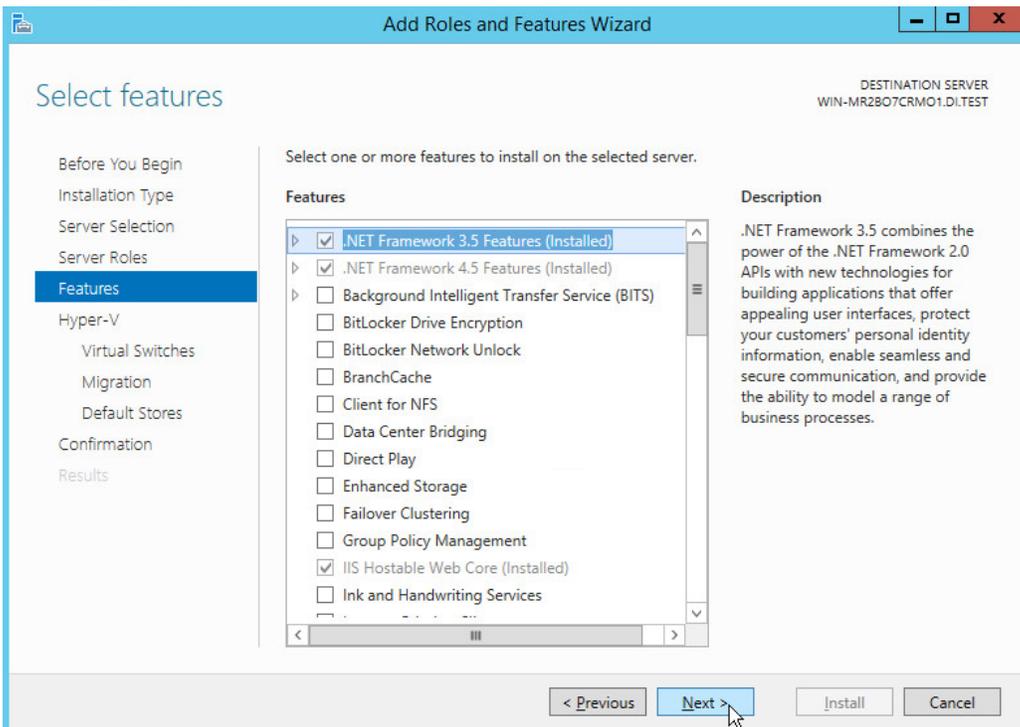
560  
561  
562

7. Click **Next**.
8. On the **Select server roles** page, select **Hyper-V**.

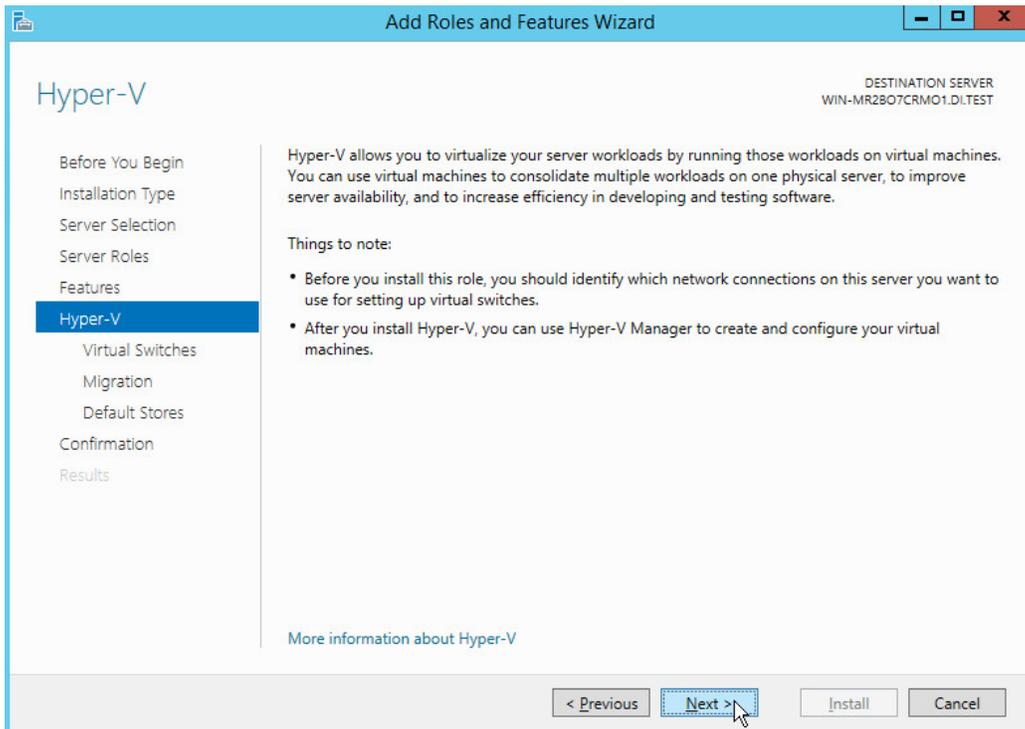
563 9. To add the tools that you use to create and manage virtual machines, click **Add Features**.



564 565 10. Click **Next**.

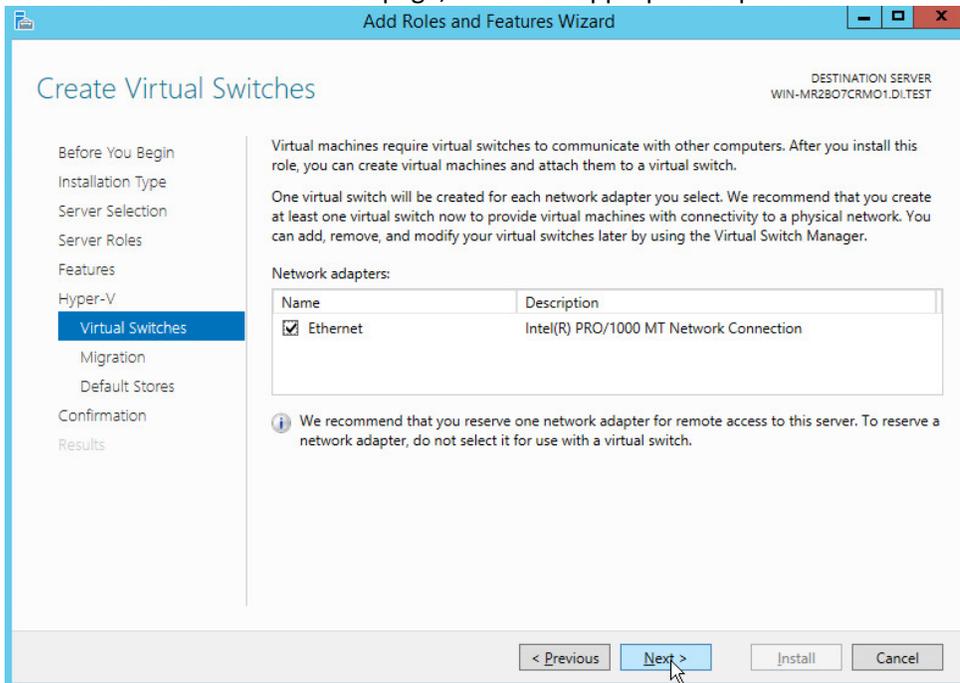


566 567 11. Click **Next**.



568  
569  
570

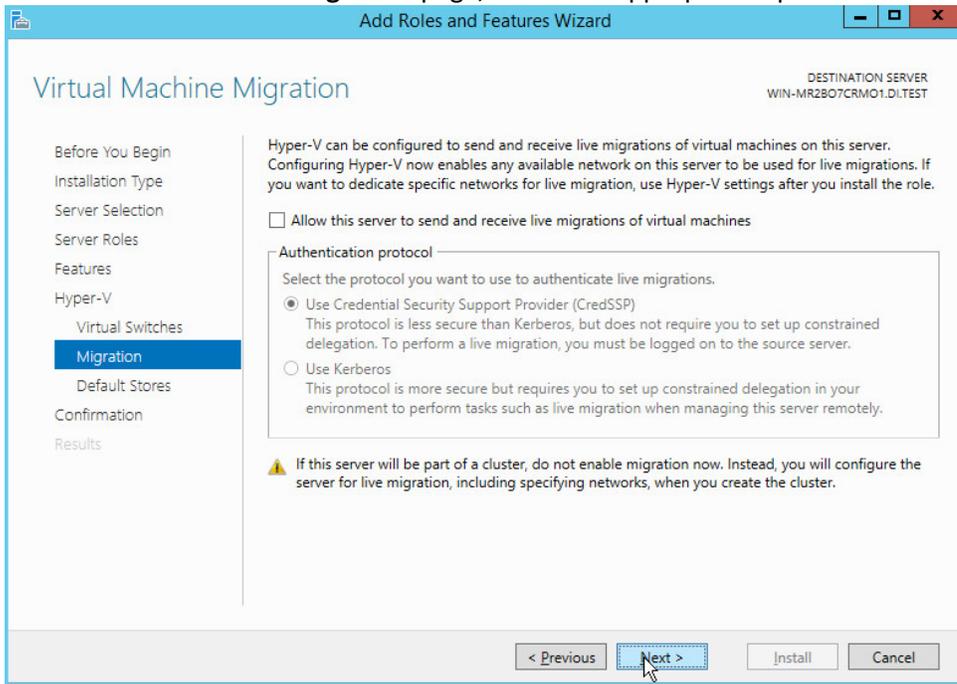
- 12. Click **Next**.
- 13. On the **Create Virtual Switches** page, select the appropriate options.



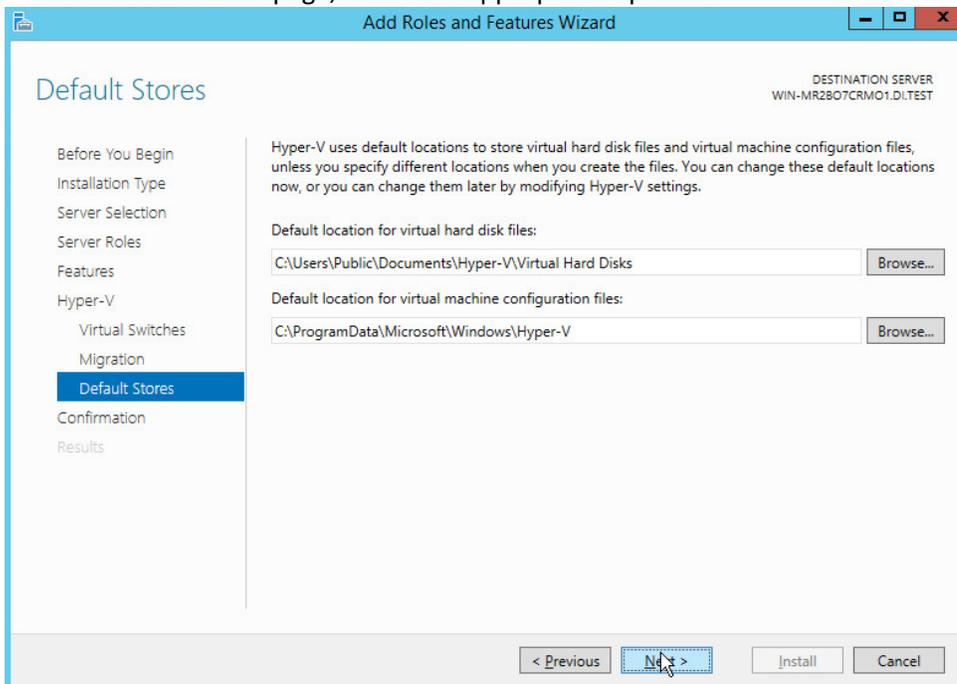
571  
572

- 14. Click **Next**.

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

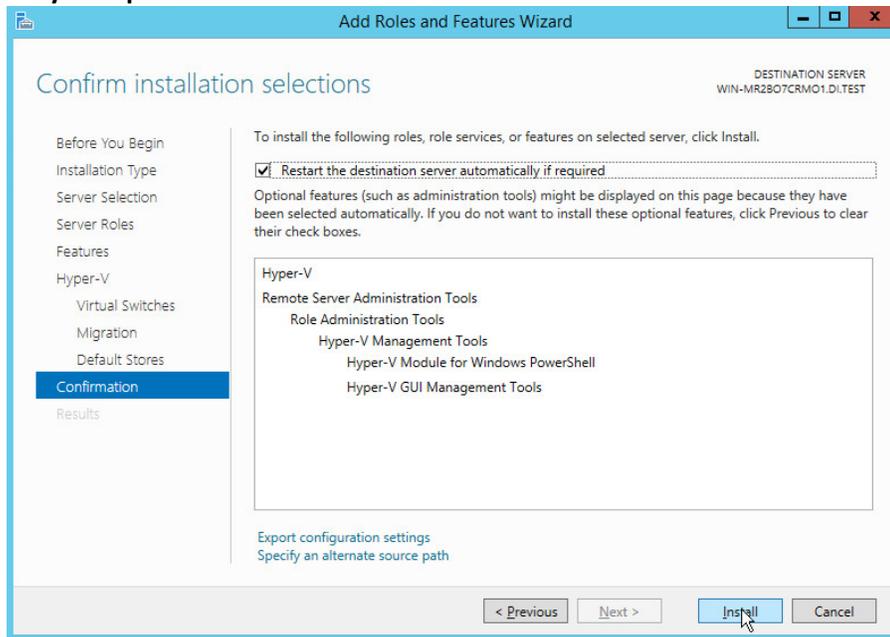


- 574 16. Click **Next**.  
 575  
 576 17. On the **Default Stores** page, select the appropriate options.



- 577 18. Click **Next**.  
 578

- 579 19. On the **Confirm installation selections** page, select **Restart the destination server automati-**  
 580 **cally if required.**



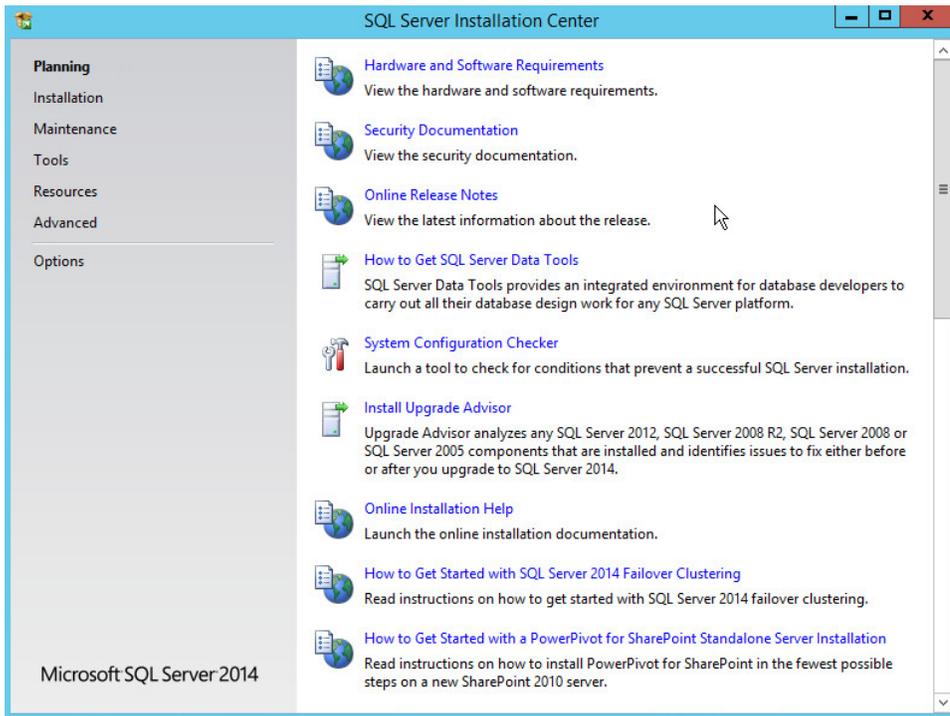
- 581 20. Click **Install**.  
 582  
 583 21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page  
 584 in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and**  
 585 **Features** tile on the page for the selected server.

## 586 2.4 MS SQL Server

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

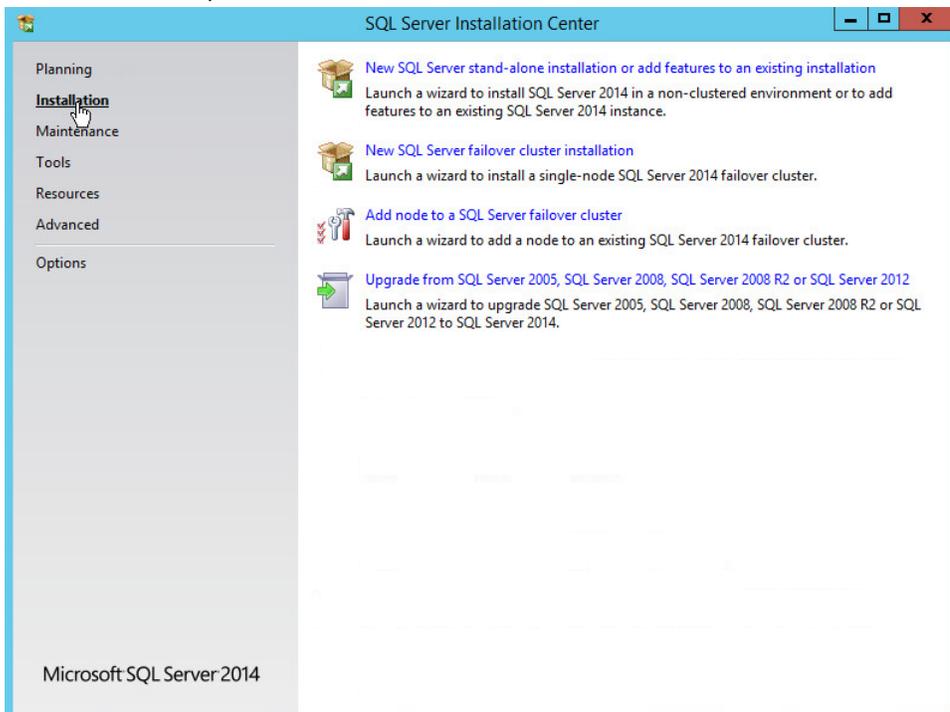
### 590 2.4.1 Install and Configure MS SQL

- 591 1. Acquire **SQL Server 2014 Installation Media**.  
 592 2. Locate the installation media in the machine and click on **SQL2014\_x64\_ENU** to launch **SQL**  
 593 **Server Installation Center**.



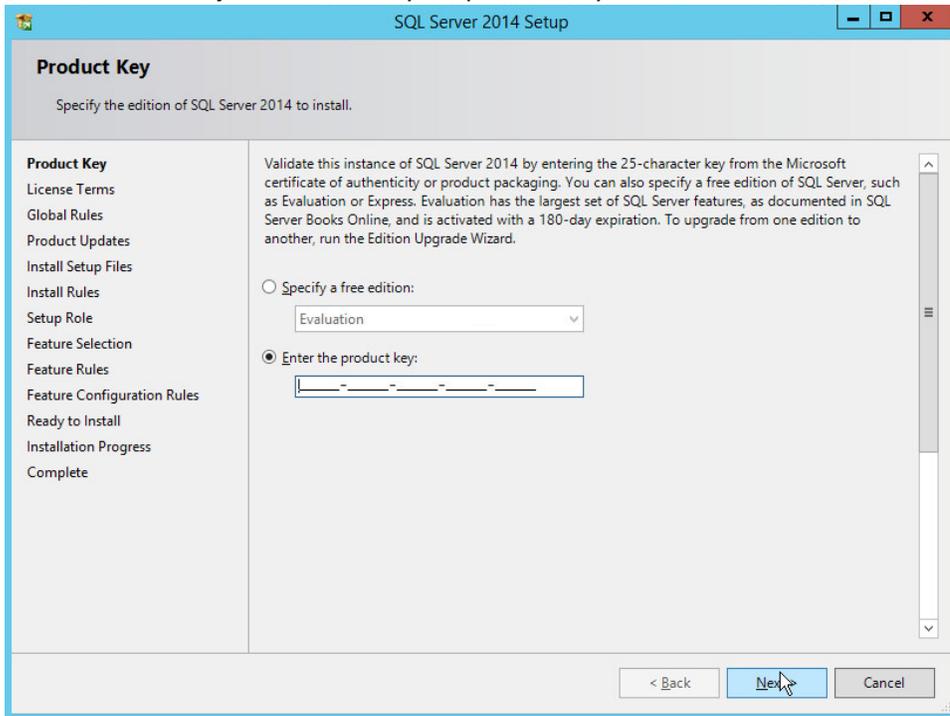
594  
595

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

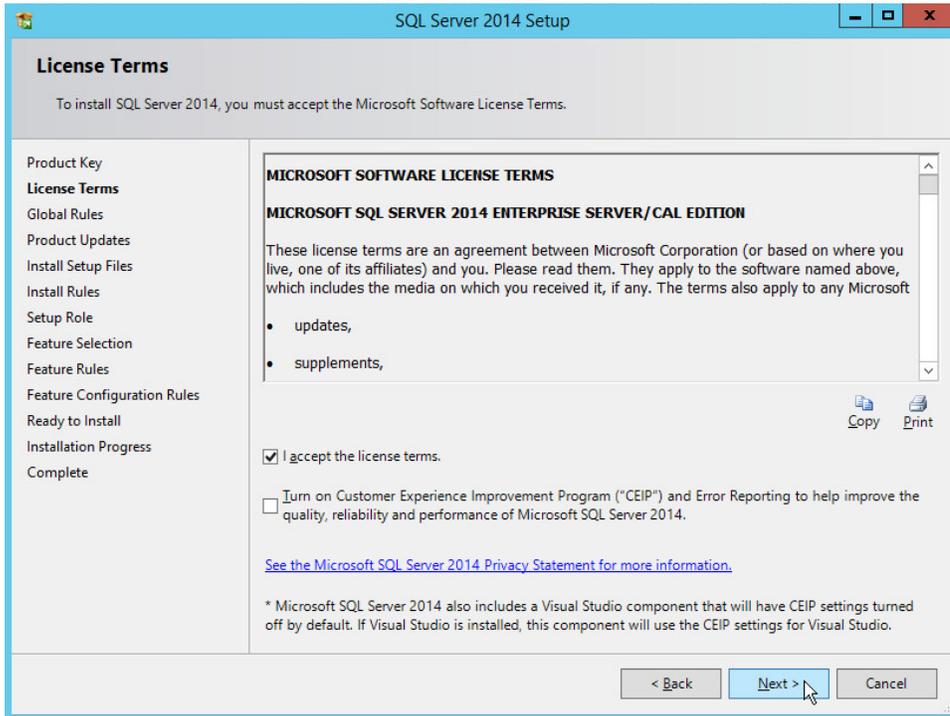


596

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

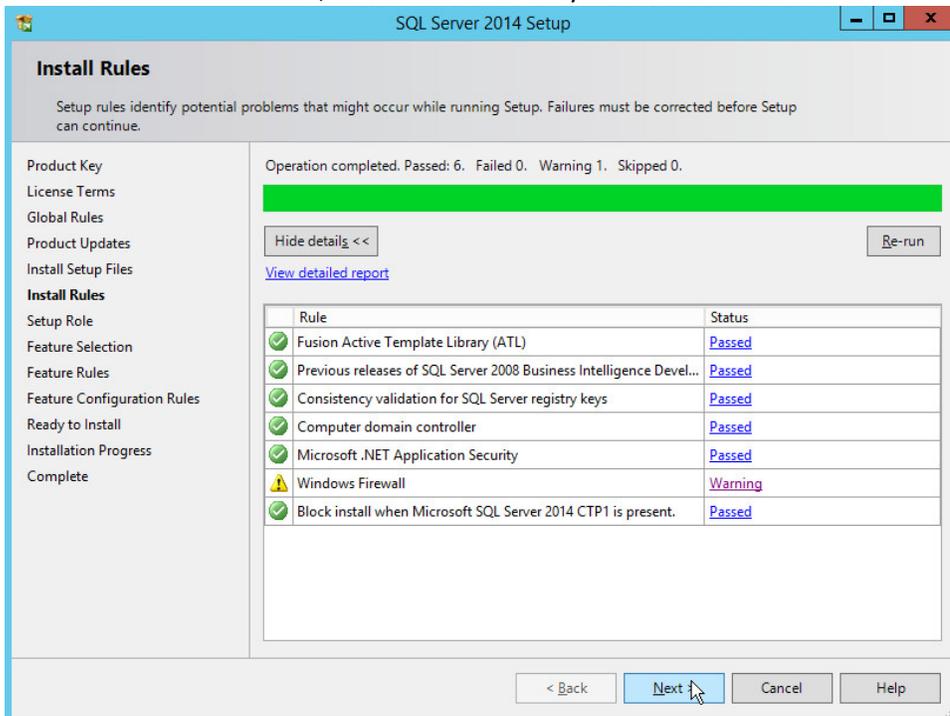


- 600 6. Click **Next**.
- 601 7. In the **License Terms** section, read and click **I accept the license terms**.
- 602



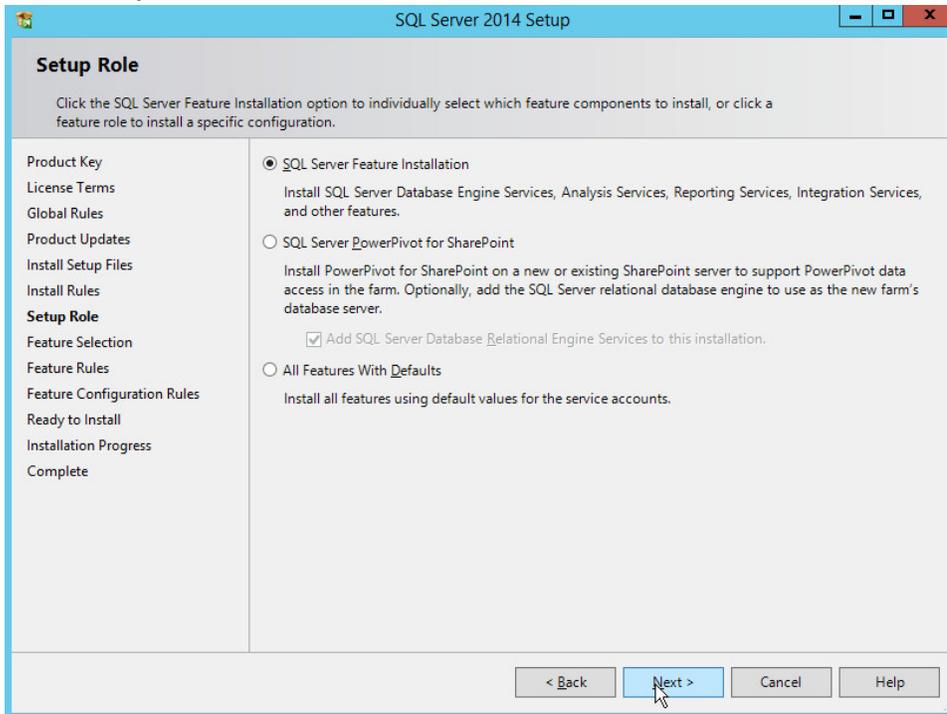
603  
604  
605

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

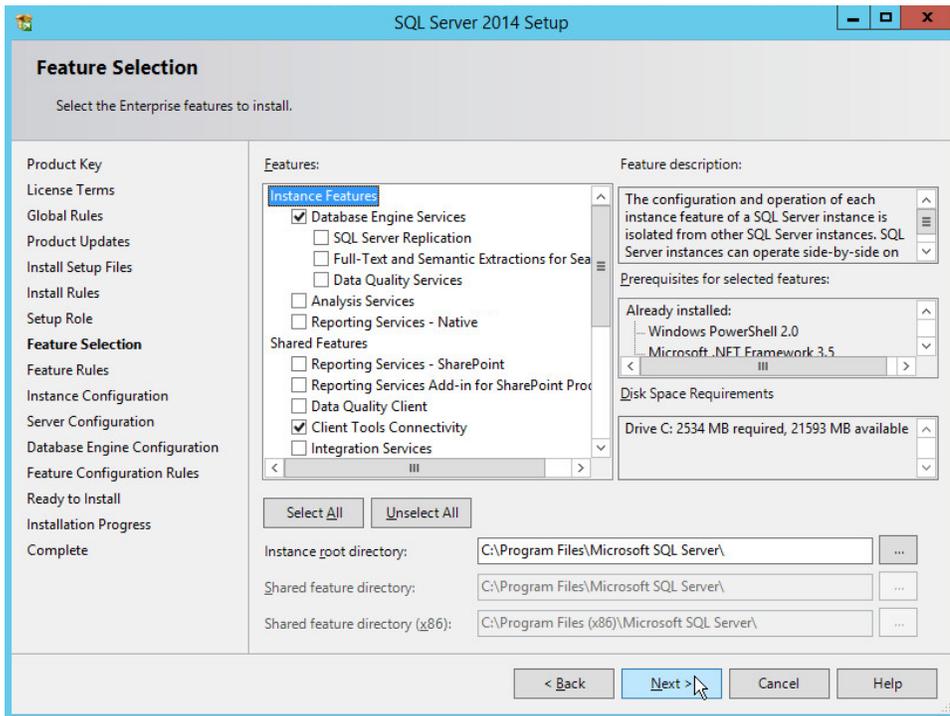


606

- 607 10. Click **Next**.  
608 11. In the **Setup Role** section, select **SQL Server Feature Installation**.

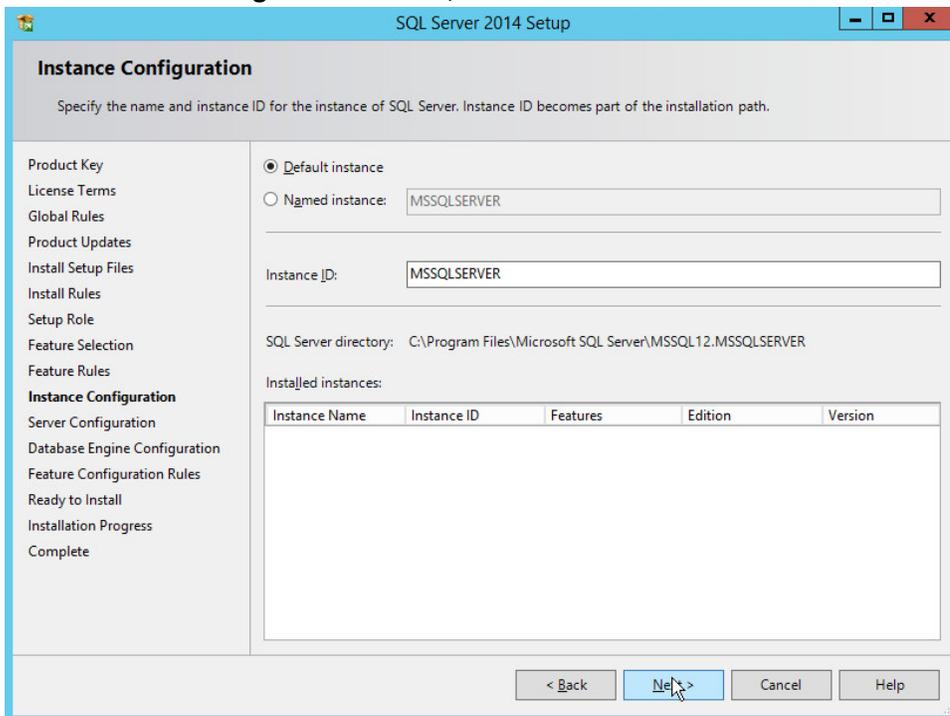


- 609 12. Click **Next**.  
610 13. In the **Feature Selection** section, select the following:  
611     a. **Database Engine Services**  
612     b. **Client Tools Connectivity**  
613     c. **Client Tools Backwards Compatibility**  
614     d. **Client Tools SDK**  
615     e. **Management Tools – Basic**  
616     f. **Management Tools – Complete**  
617     g. **SQL Client Connectivity SDK**  
618     h. **Any other desired features**  
619



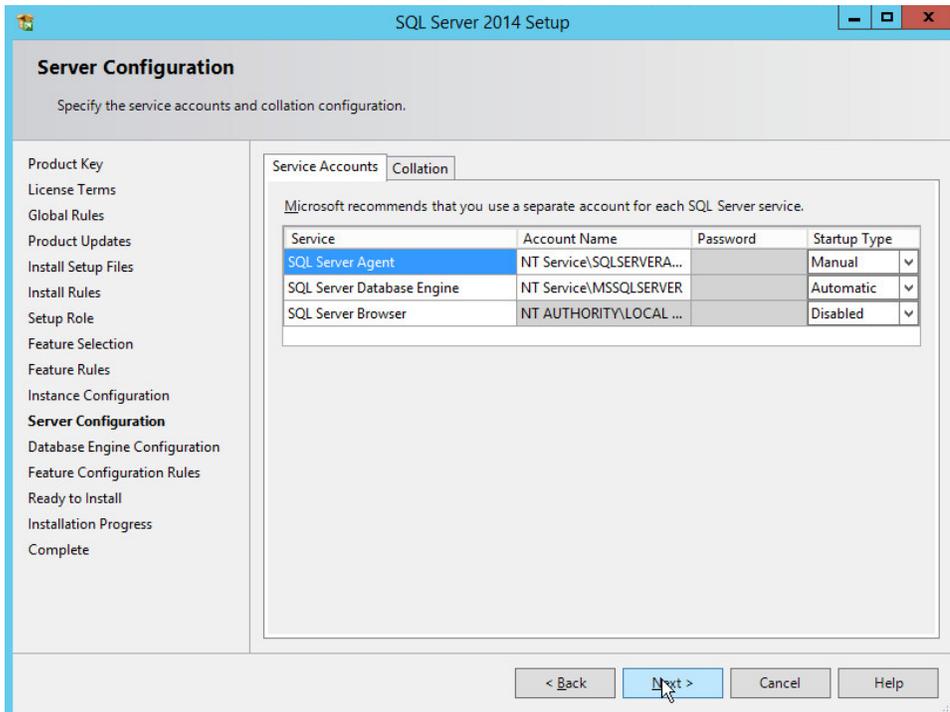
620  
621  
622

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



623

624 16. Click **Next**.



625 17. In the **Server Configuration** section, click **Next**.

626 18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.

627 19. Add all desired users as Administrators under **Specify SQL Server Administrators** by pressing **Add Current User**.

628 a. For Domain accounts, simply type in **\$DOMAINNAME\USERNAME** into **Enter the object names to select** textbox.

629 b. Click **OK**.

630 c. For local computer accounts, click on **locations** and select the computer's name.

631 d. Click **OK**.

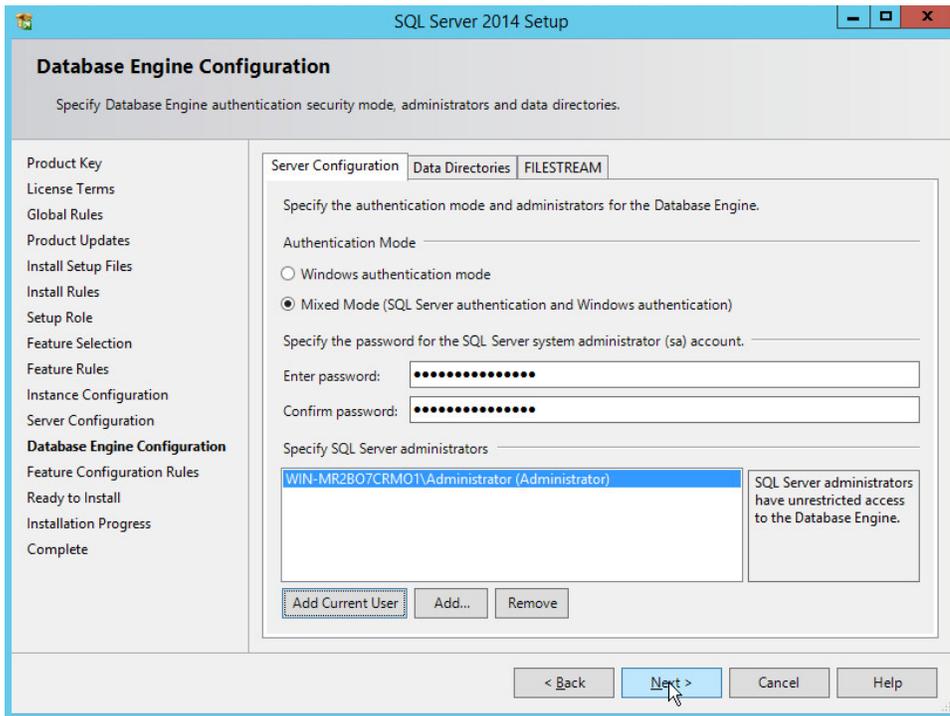
632 e. Type the username into the **Enter the object names to select** textbox.

633 f. Once you are finished adding users, click **Next**.

634

635

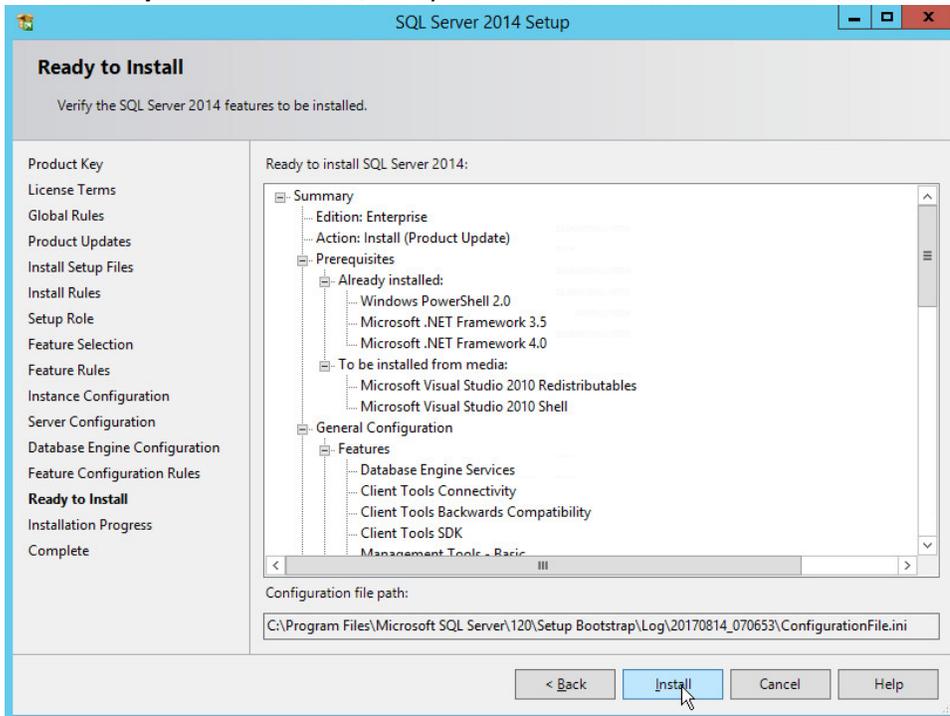
636



637

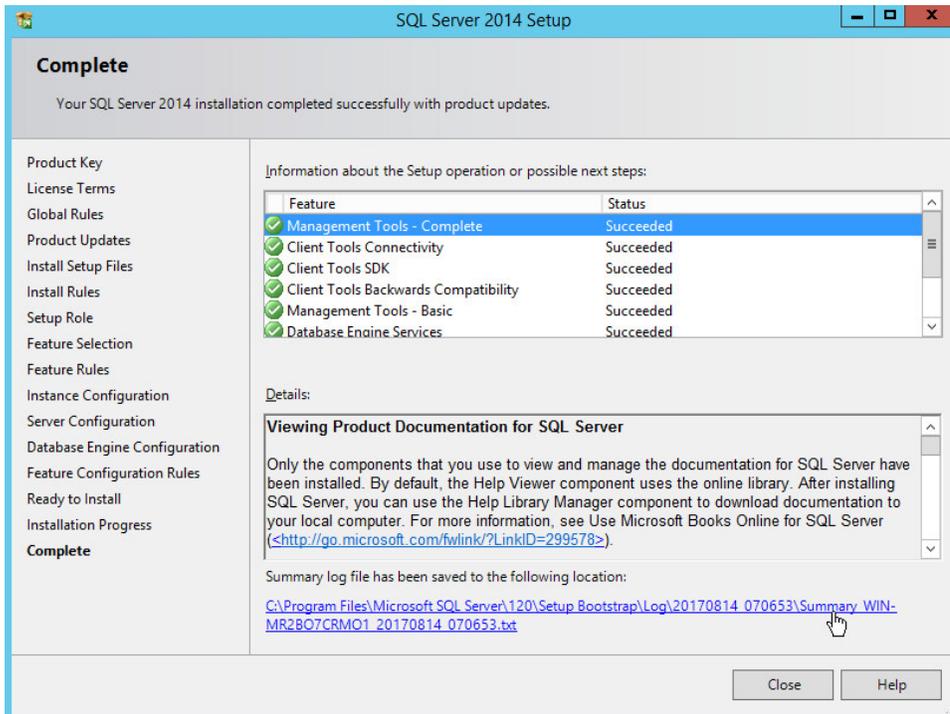
638

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



639

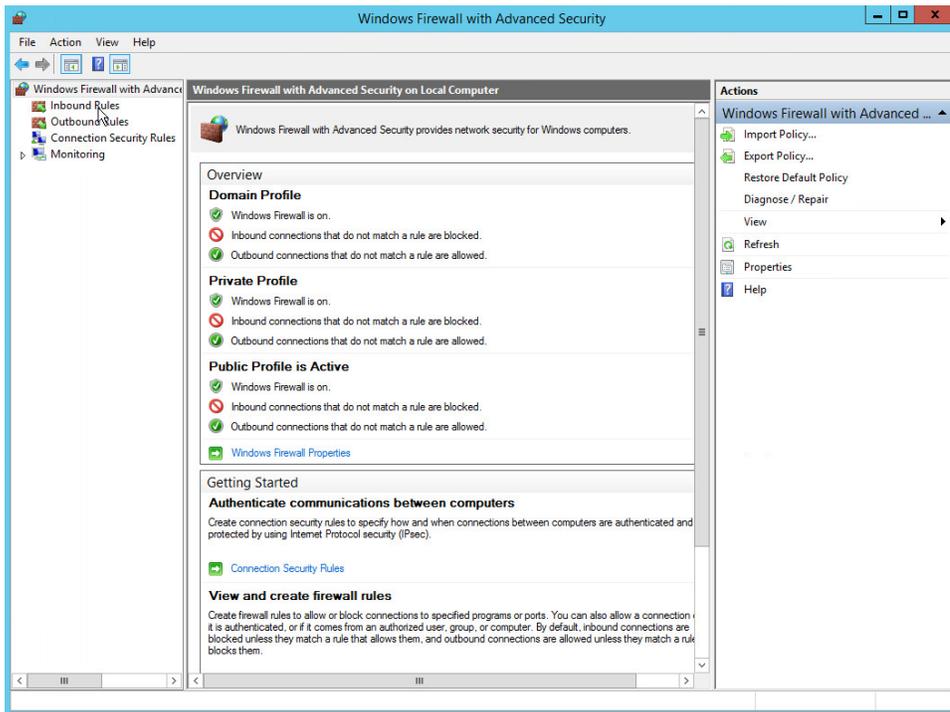
640 21. Wait for the install to finish.



641  
642 22. Click **Close**.

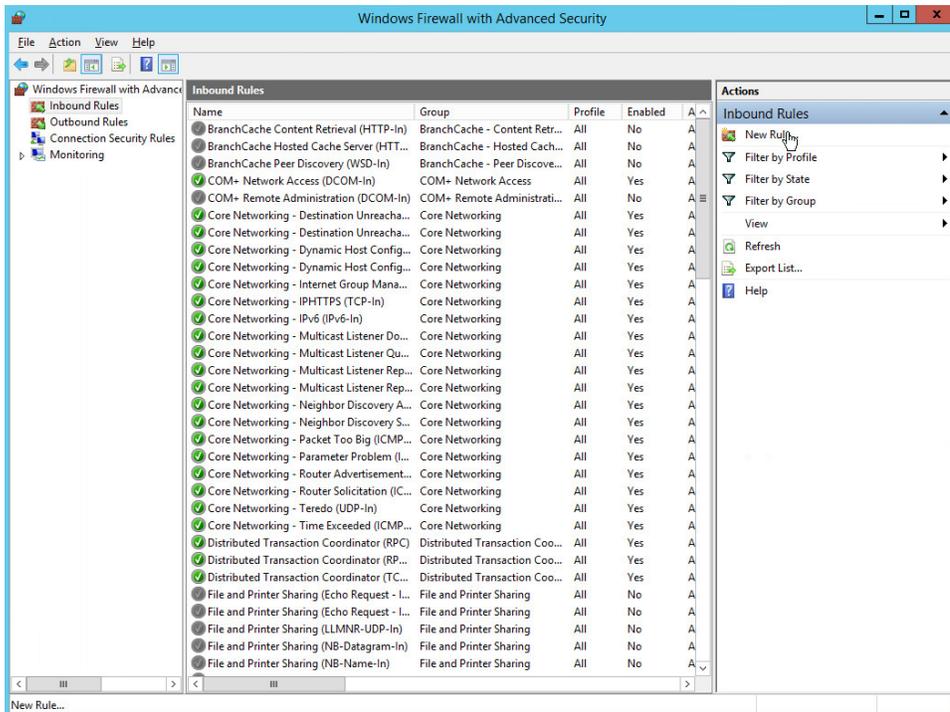
## 643 2.4.2 Open Port on Firewall

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



645  
646

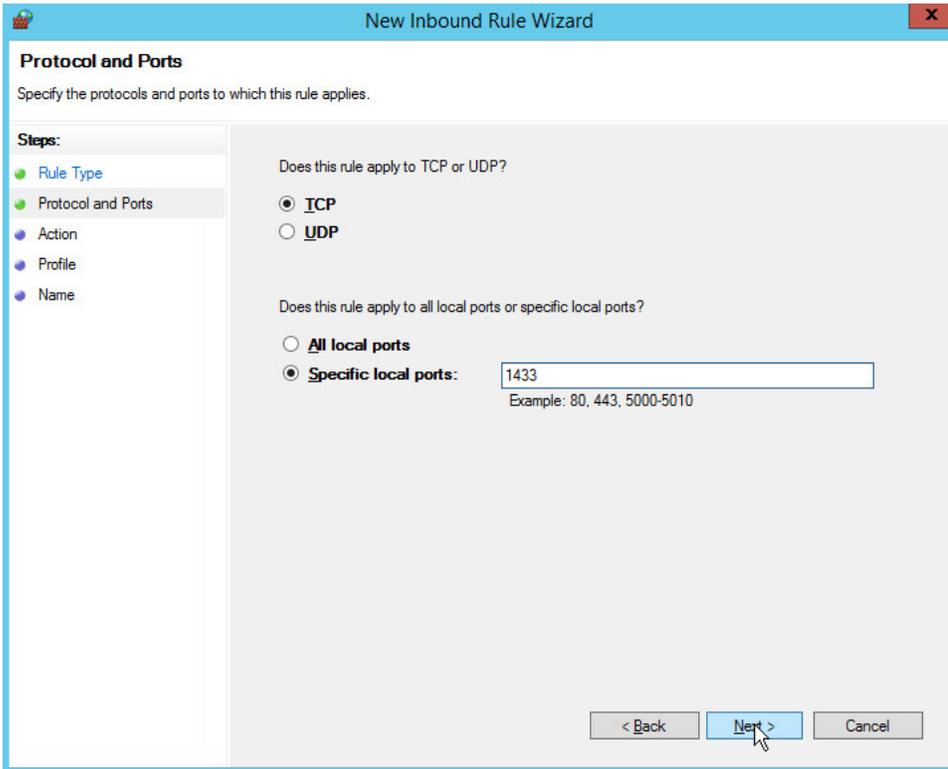
2. Click **Inbound Rules**.



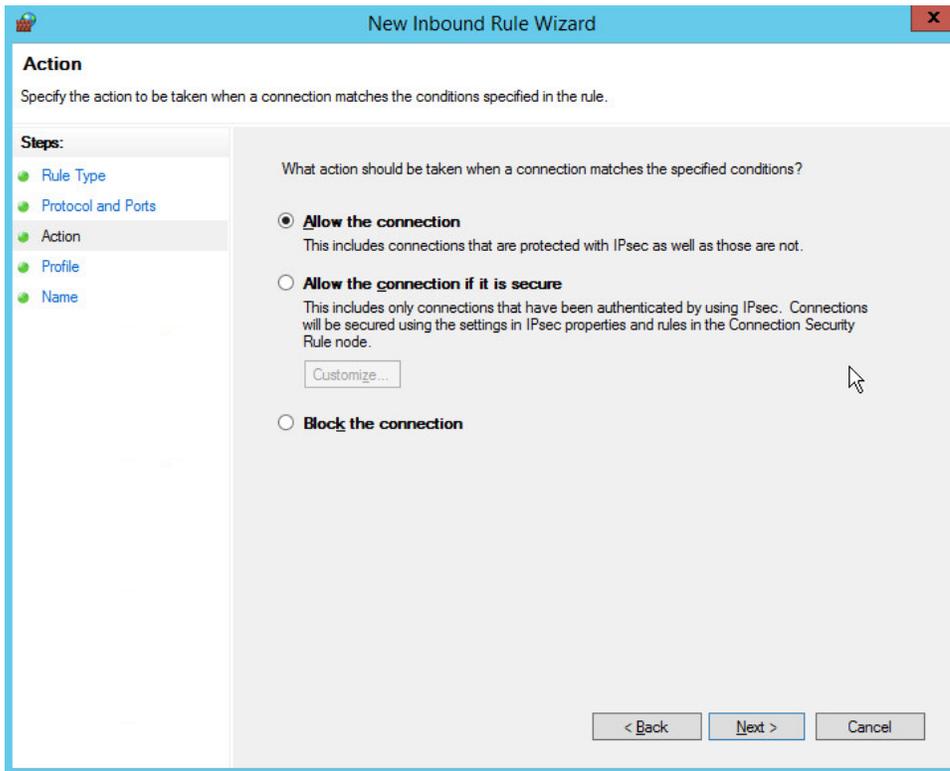
647  
648

3. Click **New Rule**.

- 649 4. Select **Port**.
- 650 5. Click **Next**.
- 651 6. Select **TCP** and **Specific local ports**.
- 652 7. Type **1433** into the text field.

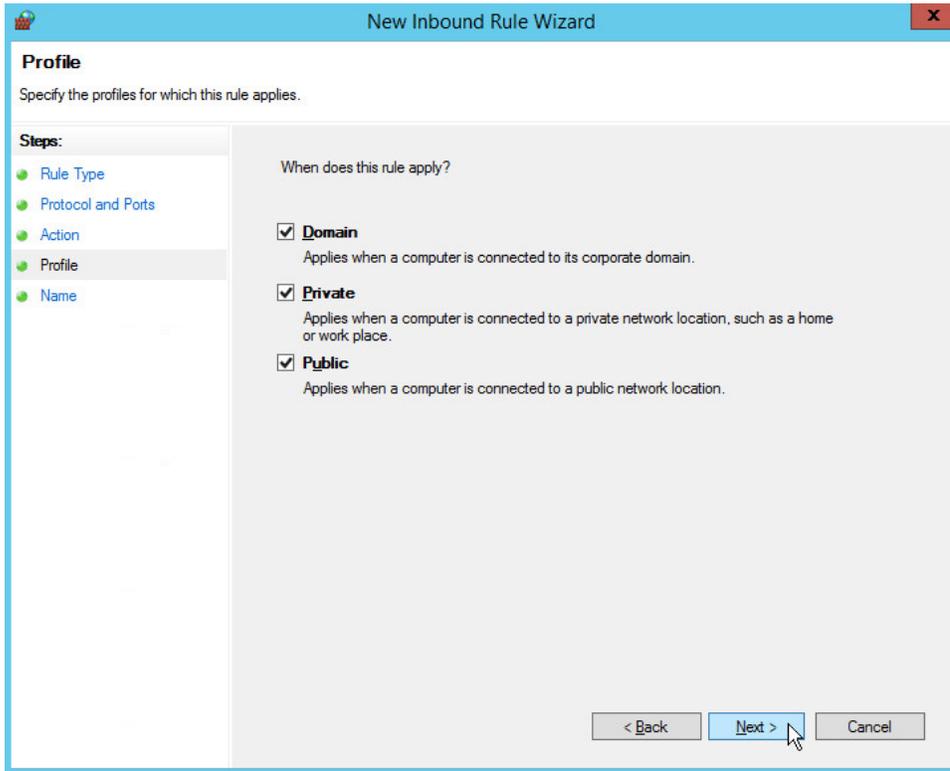


- 653 8. Click **Next**.
- 654 9. Select **Allow the connection**.
- 655



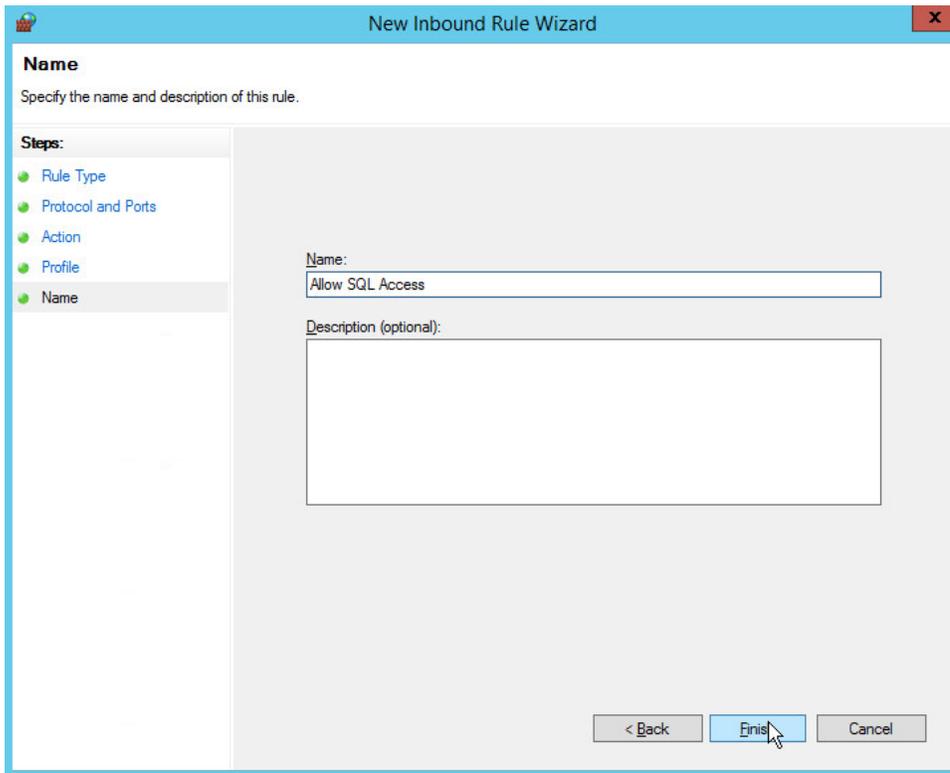
656  
657  
658

- 10. Click **Next**.
- 11. Select all applicable locations.



659  
660  
661

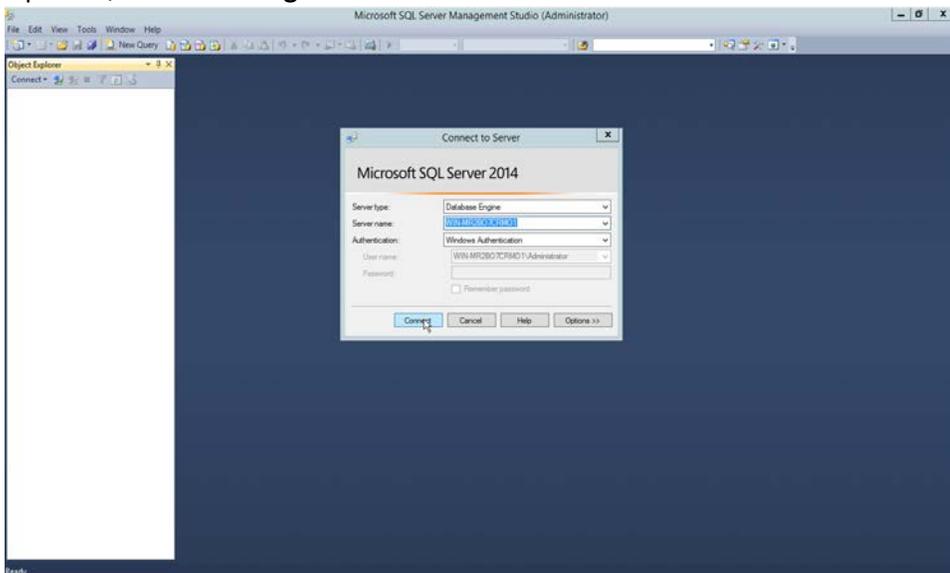
12. Click **Next**.
13. Name the rule **Allow SQL Access**.



662  
663 14. Click **Finish**.

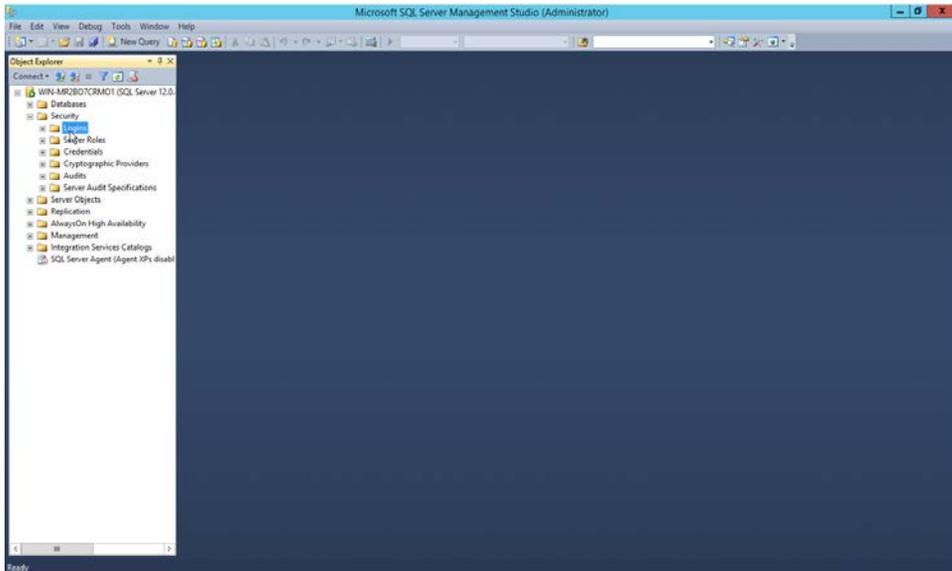
### 664 2.4.3 Add a New Login to the Database

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

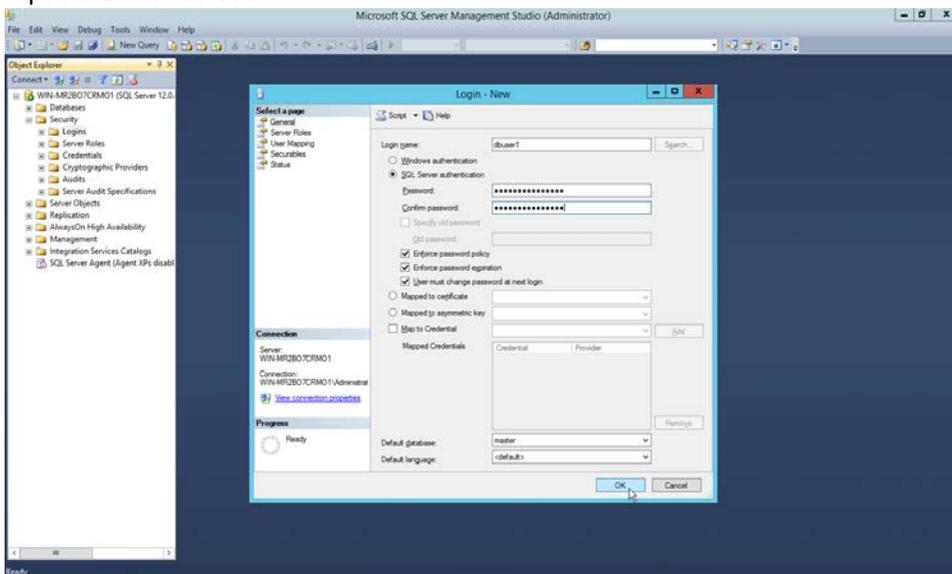


666

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



- 669 4. Right-click on the **Logins** folder and click **New Login....**
- 670 5. Input the desired user.
- 671



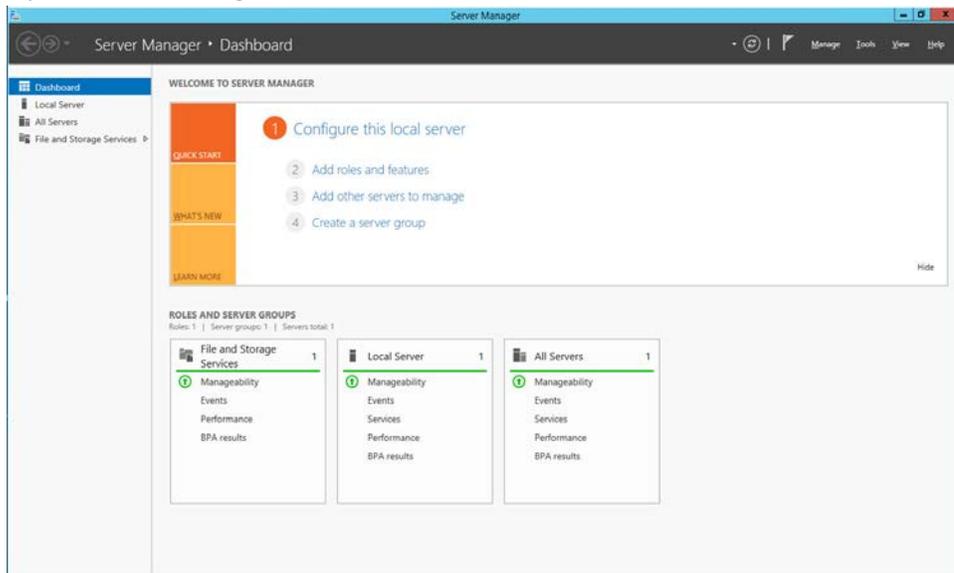
- 672 6. Click **OK**.
- 673

674 **2.5 Microsoft IIS Server**

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

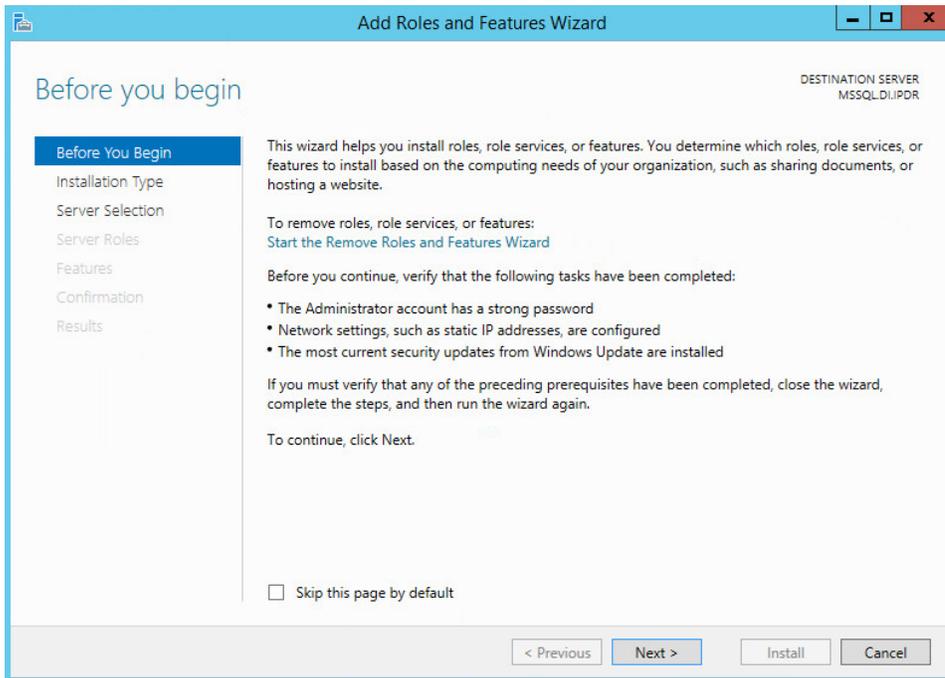
678 **2.5.1 Install IIS**

- 679 1. **Open Server Manager.**

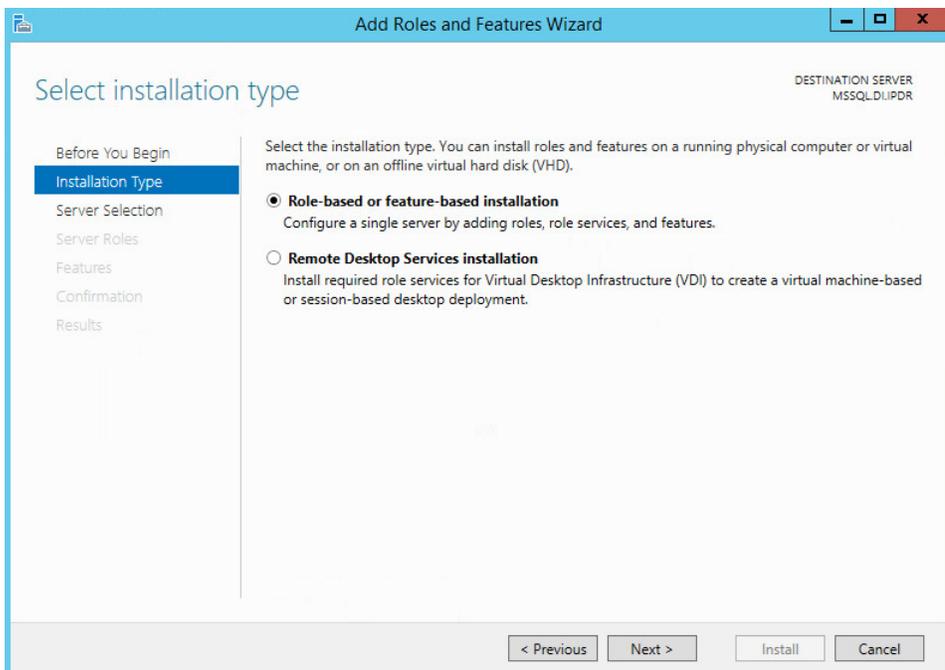


680

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

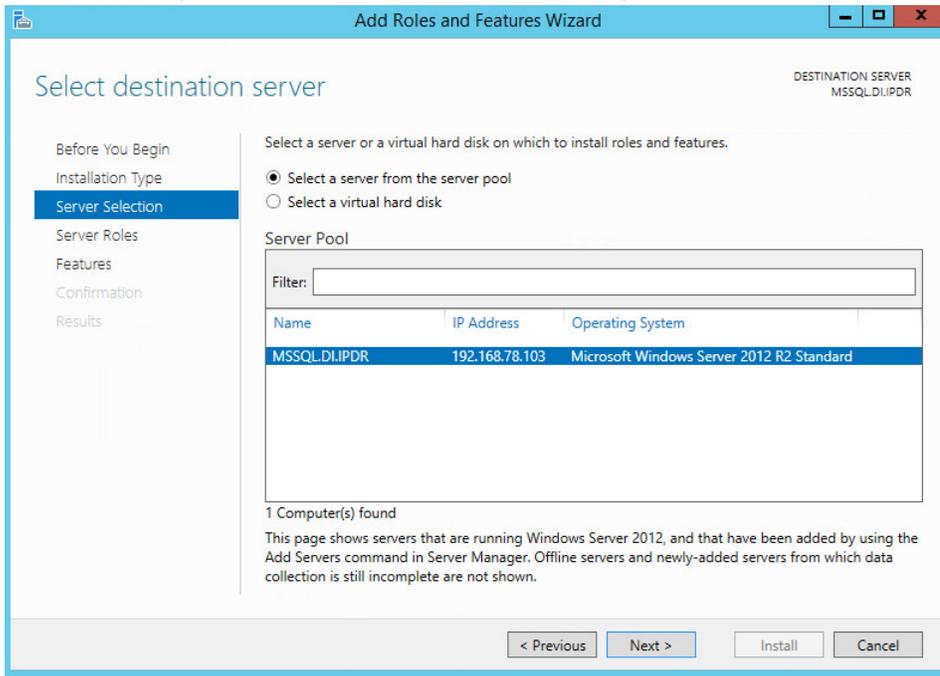


- 682 3. Click **Next**.
- 683
- 684 4. Select **Role-based or feature-based installation**.

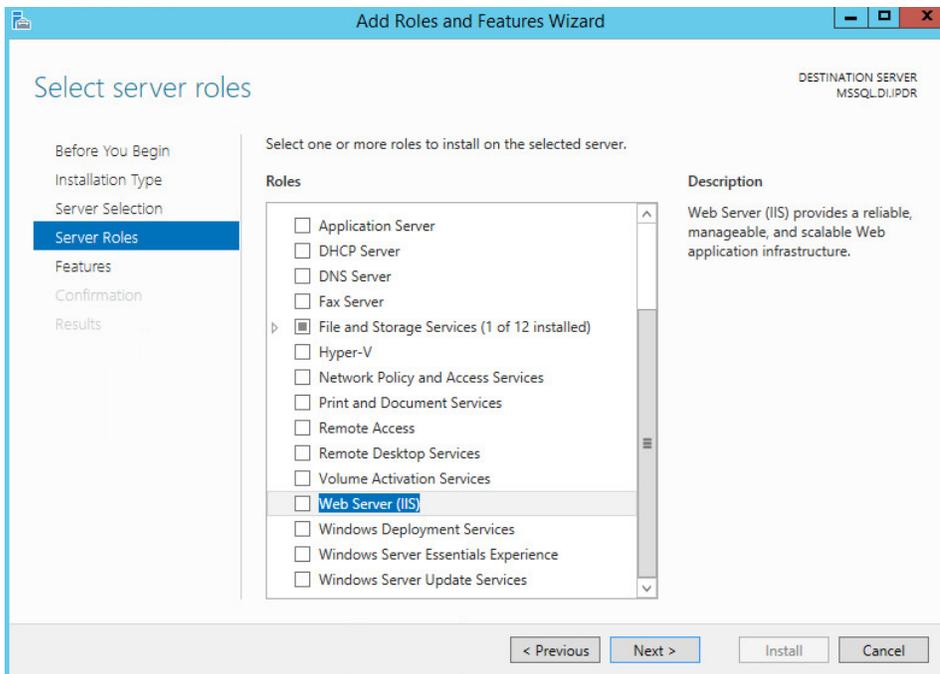


- 685 5. Click **Next**.
- 686

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

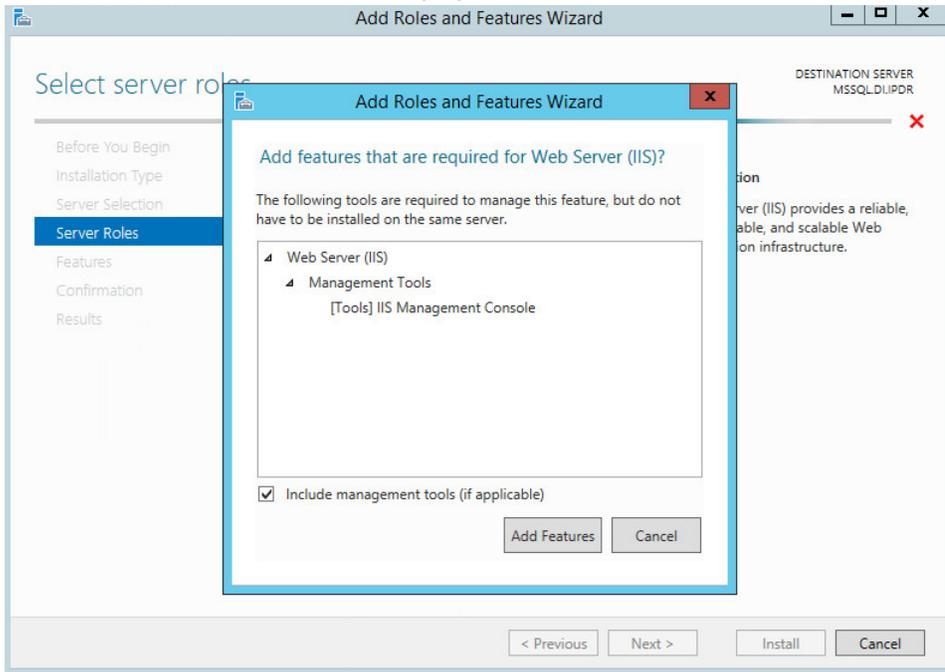


- 688  
689 7. Click **Next**.

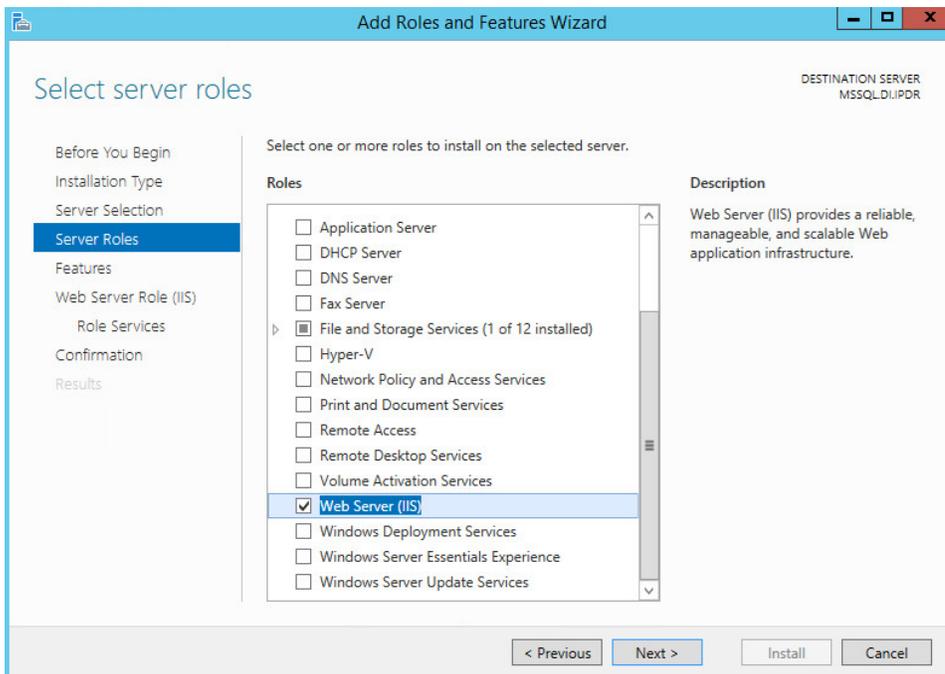


690

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

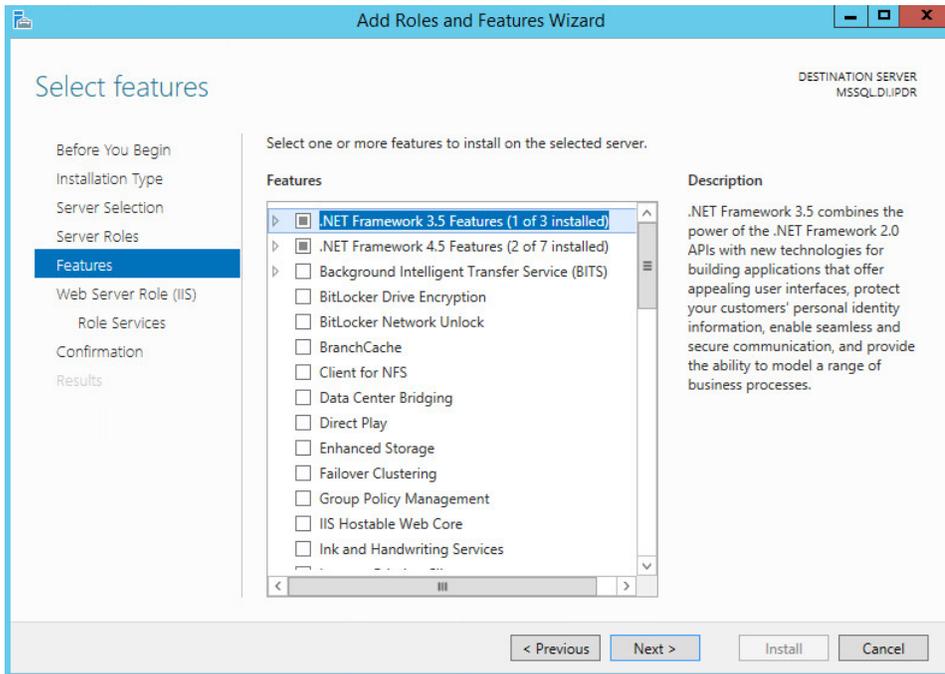


692 9. Click **Add Features**.

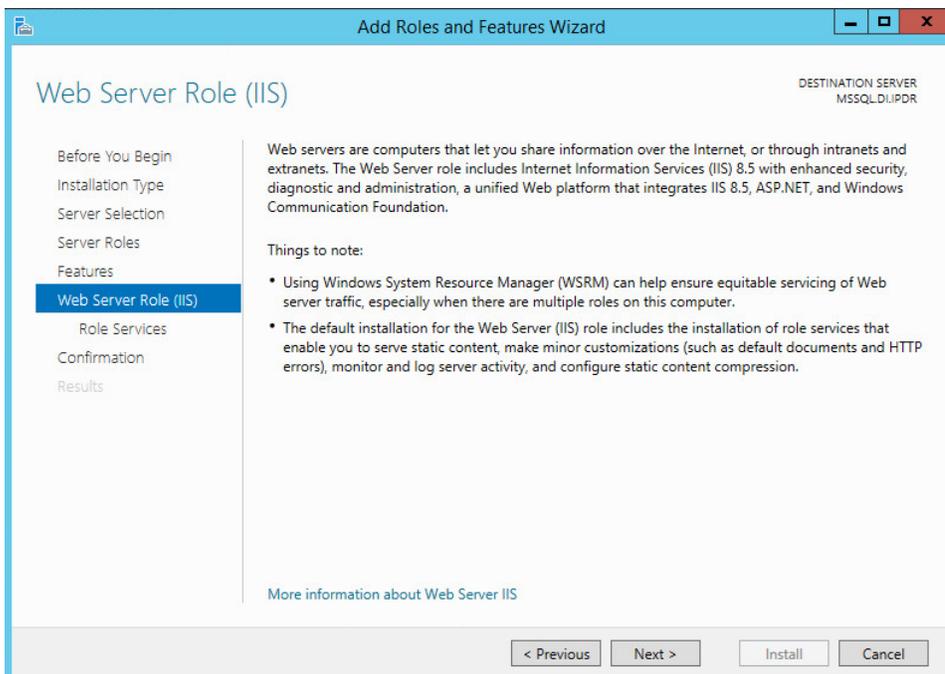


694 10. Click **Next**.

696 11. Ensure that all desired features are selected.

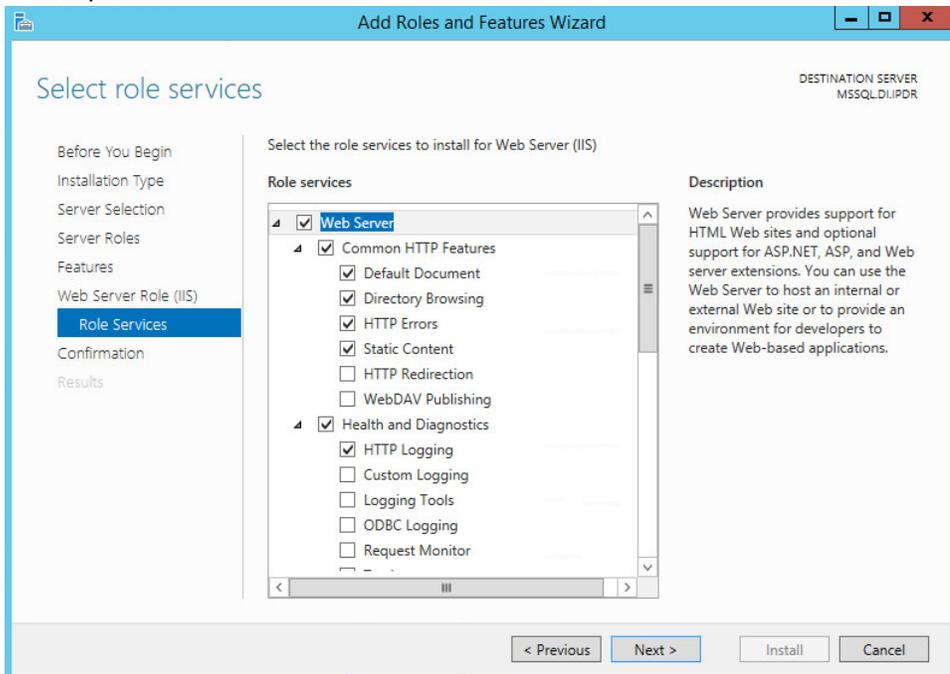


697  
698 12. Click **Next**.

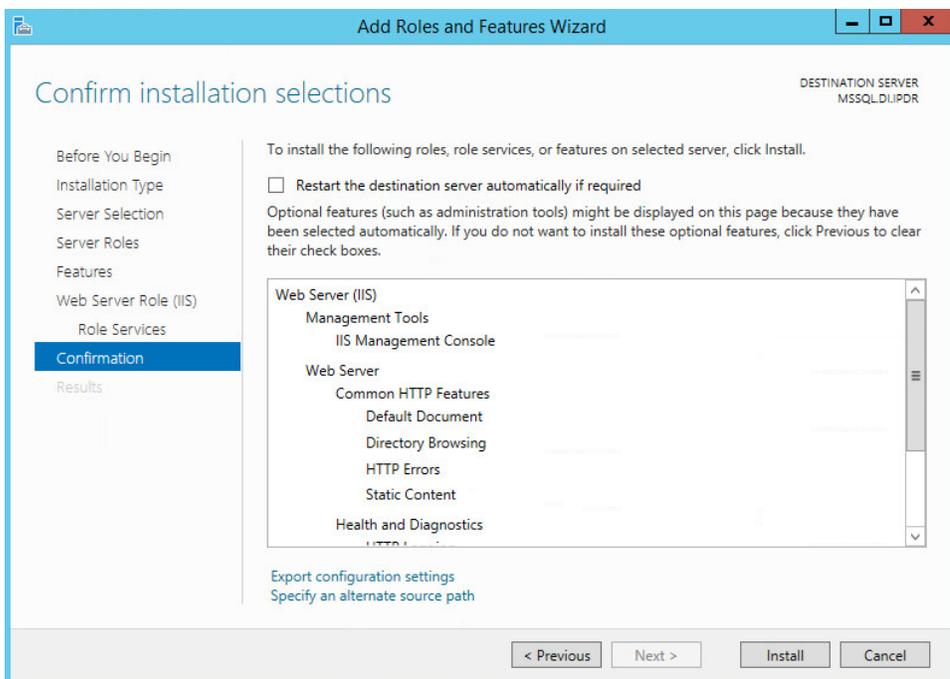


699  
700 13. Click **Next**.

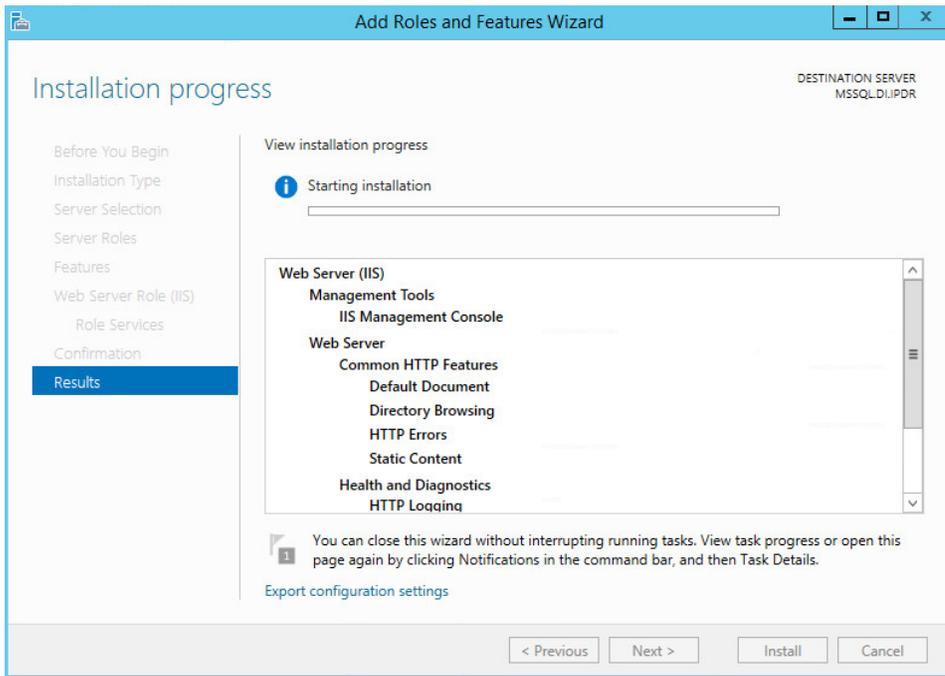
- 701 14. Ensure that **Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Logging,**  
702 and any other desired Role services are selected.



- 703 15. Click **Next.**  
704

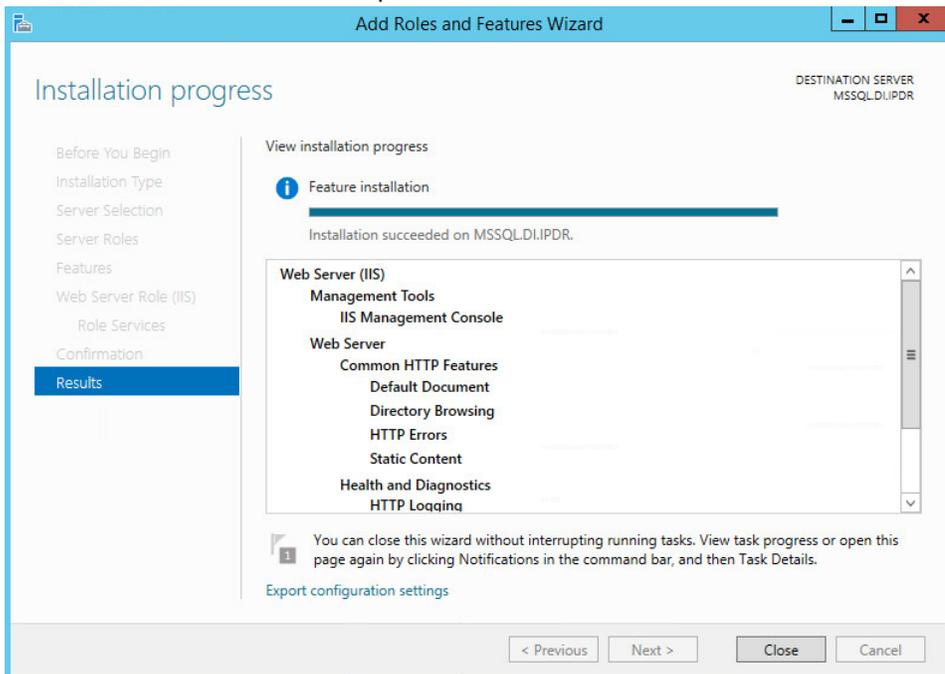


- 705 16. Click **Install.**  
706



707  
708

17. Wait for the installation to complete.

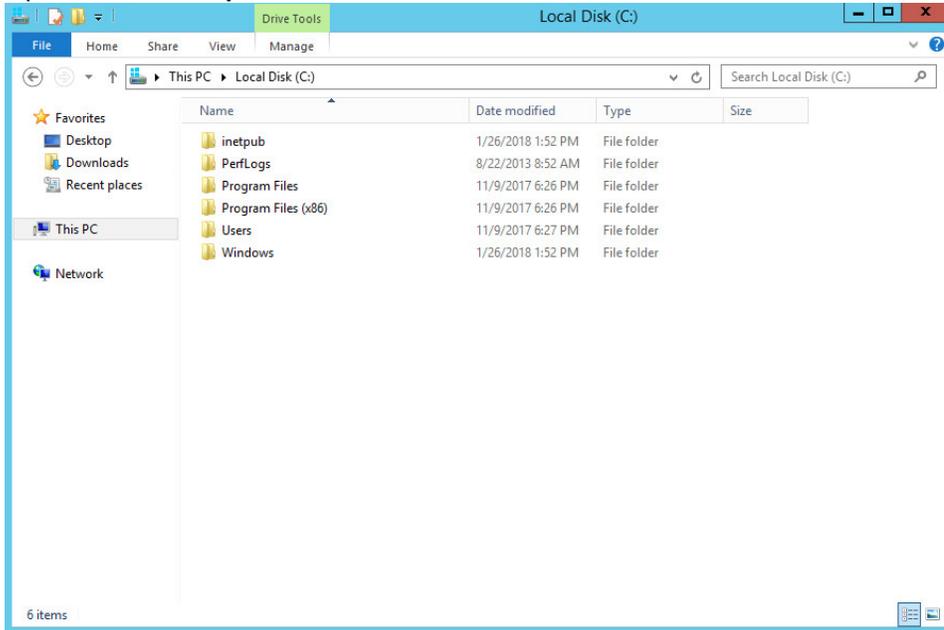


709  
710

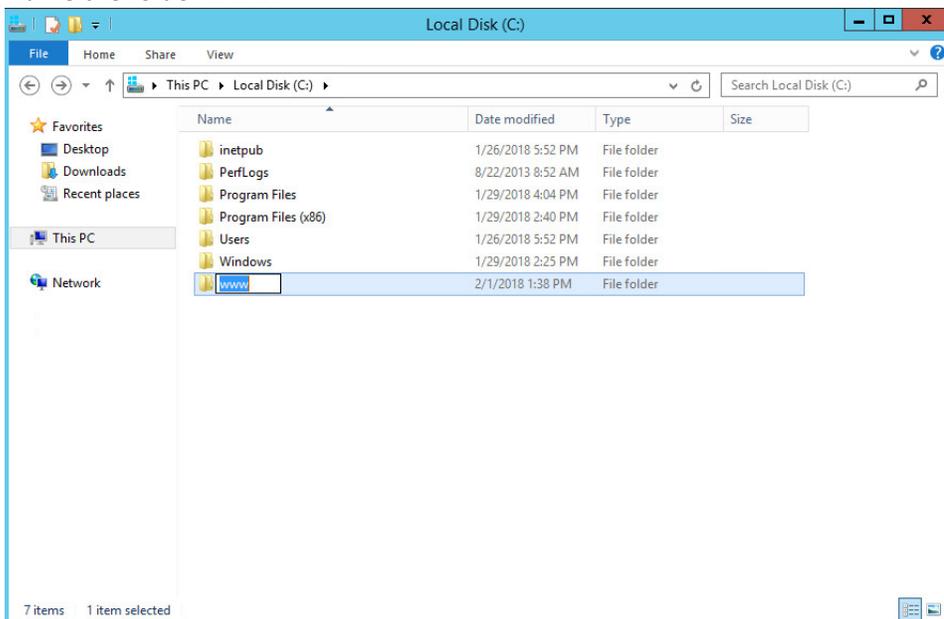
18. Click **Close**.

711 2.5.2 IIS Configuration

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

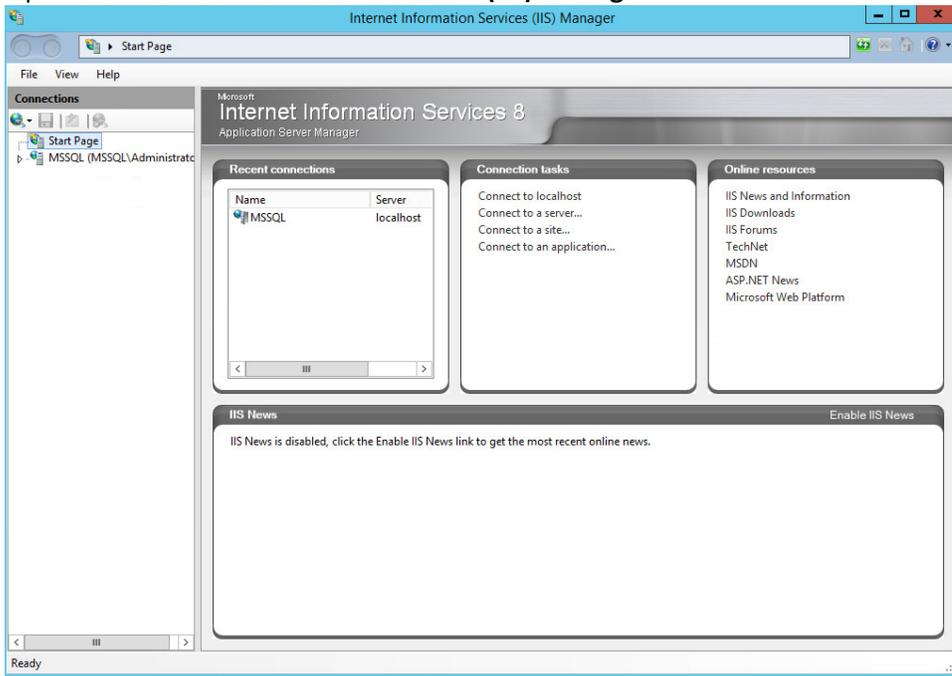


- 713 2. Right-click, and select **Create Folder**.  
714  
715 3. Name the folder **www**.

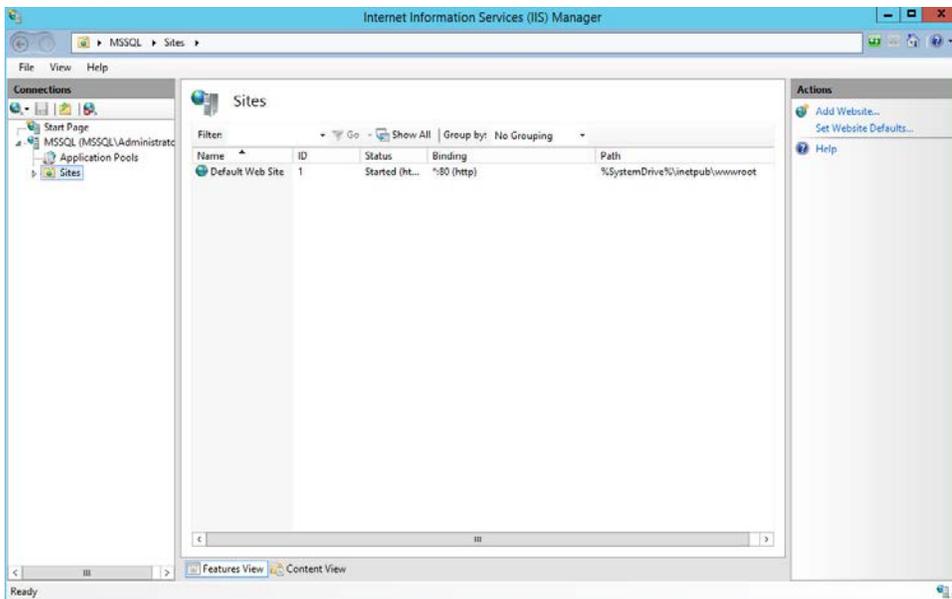


716

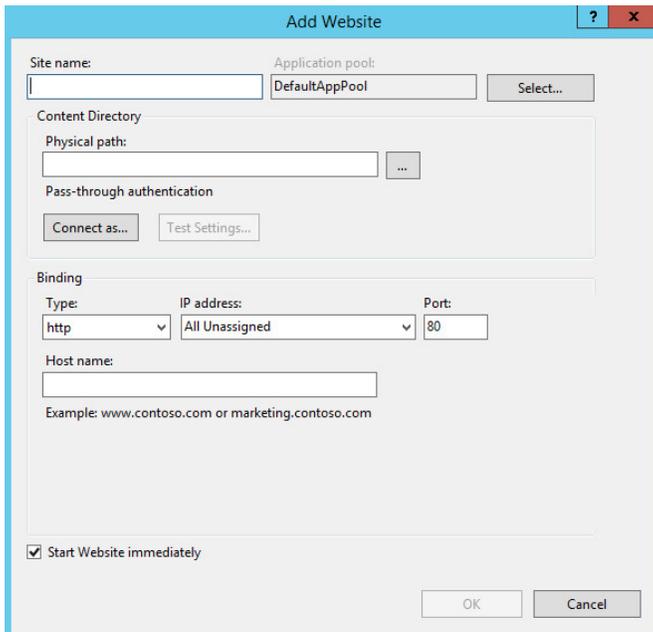
- 717 4. Open the **Internet Information Services (IIS) Manager**.



- 718  
719 5. Click the arrow next to **MSSQL** (or the chosen name of the server).  
720 6. Click **Sites**.

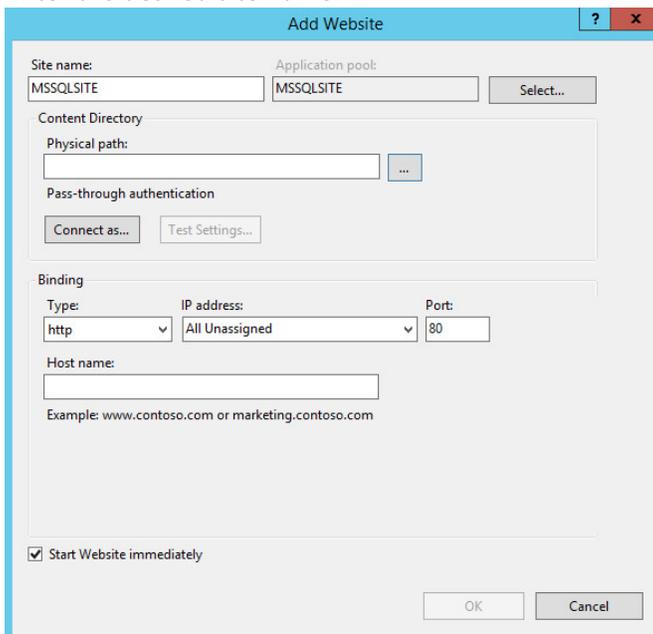


- 721  
722 7. Click **Add Website....**



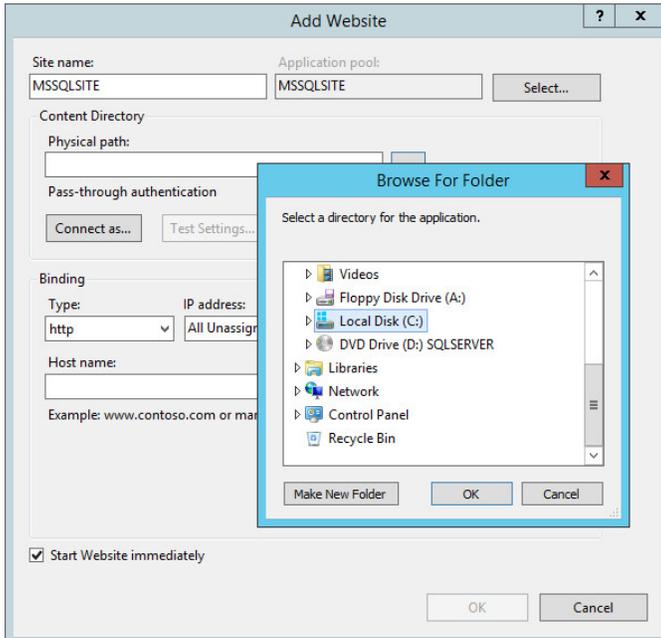
723  
724

8. Enter the desired site name.



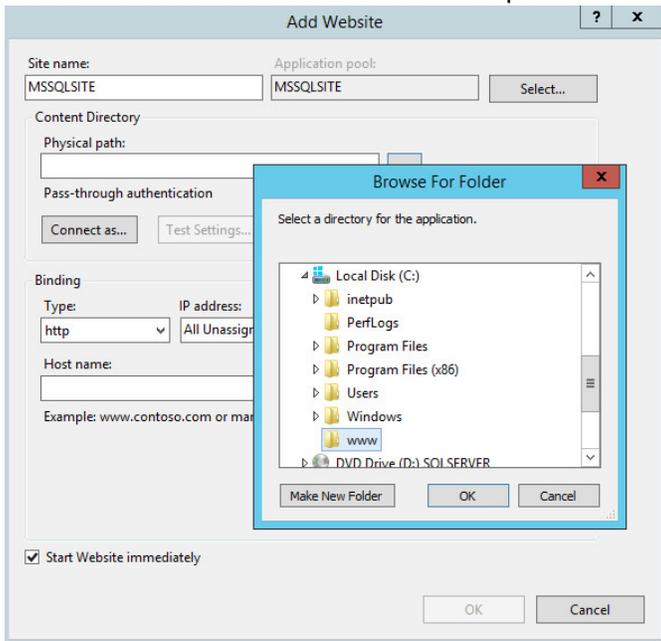
725  
726

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



727  
728

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



729  
730  
731  
732  
733

11. Click **OK**.

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

13. Ensure the **IP address** and **Host name** fields are filled in with the correct information for the machine.

734 14. Ensure that **Start Website immediately** is selected.

735  
736 15. Click **OK**.

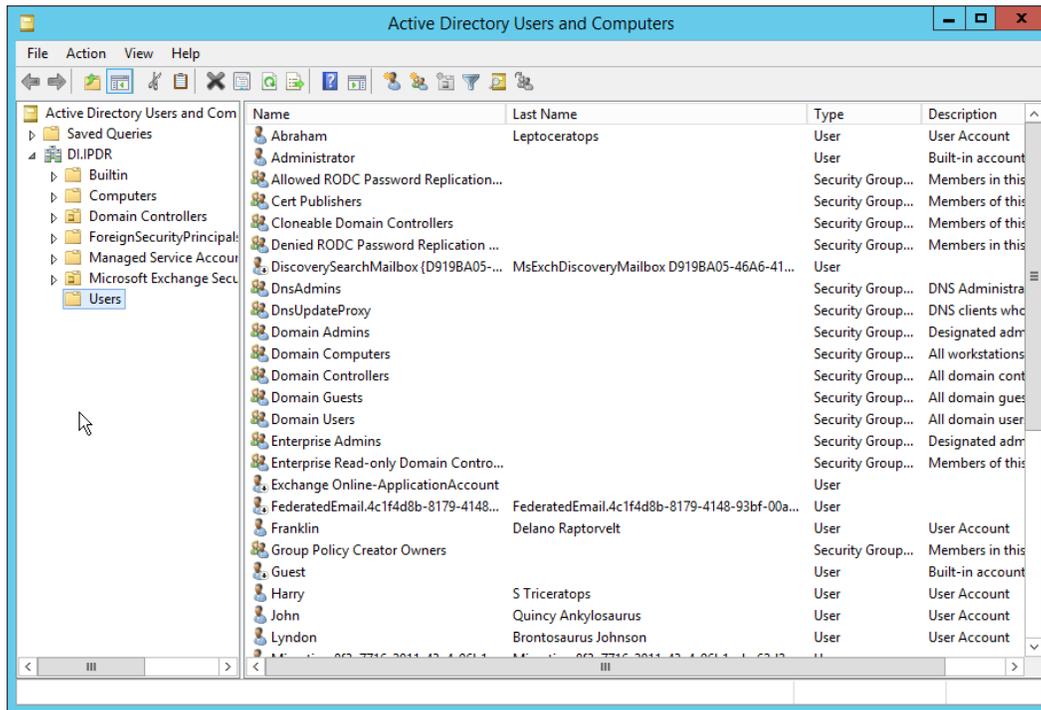
## 737 2.6 Semperis Directory Services Protector

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

- 743 • .NET Framework Version 3.5 SP1
- 744 • .NET Framework Version 4.5.2 or later
- 745 • Joined to the Active Directory Domain it is protecting
- 746 • Either the installer for SQL Express Advanced or connection information and credentials for a  
747 full version of Microsoft SQL (MSSQL)

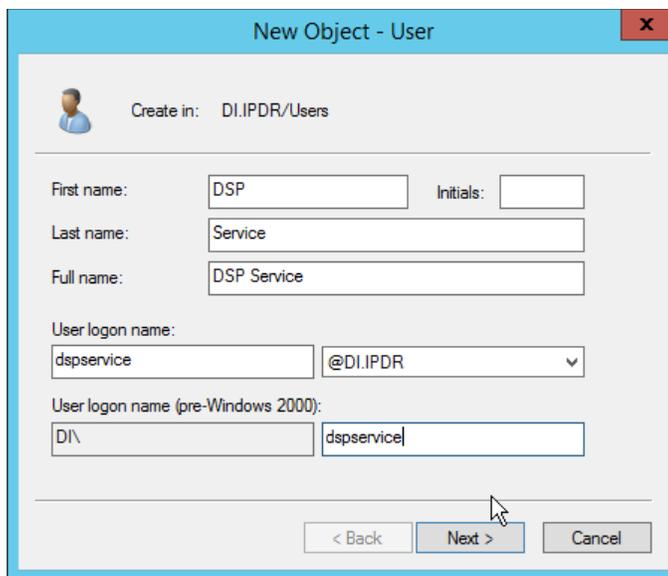
### 748 2.6.1 Configure Active Directory for Semperis DSP

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



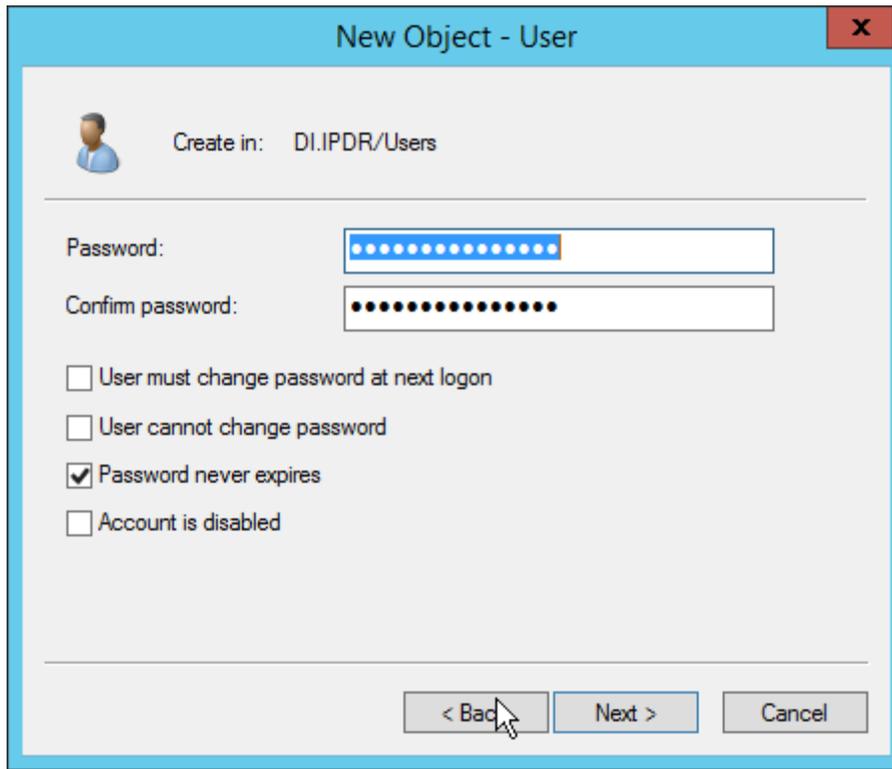
750  
751  
752

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



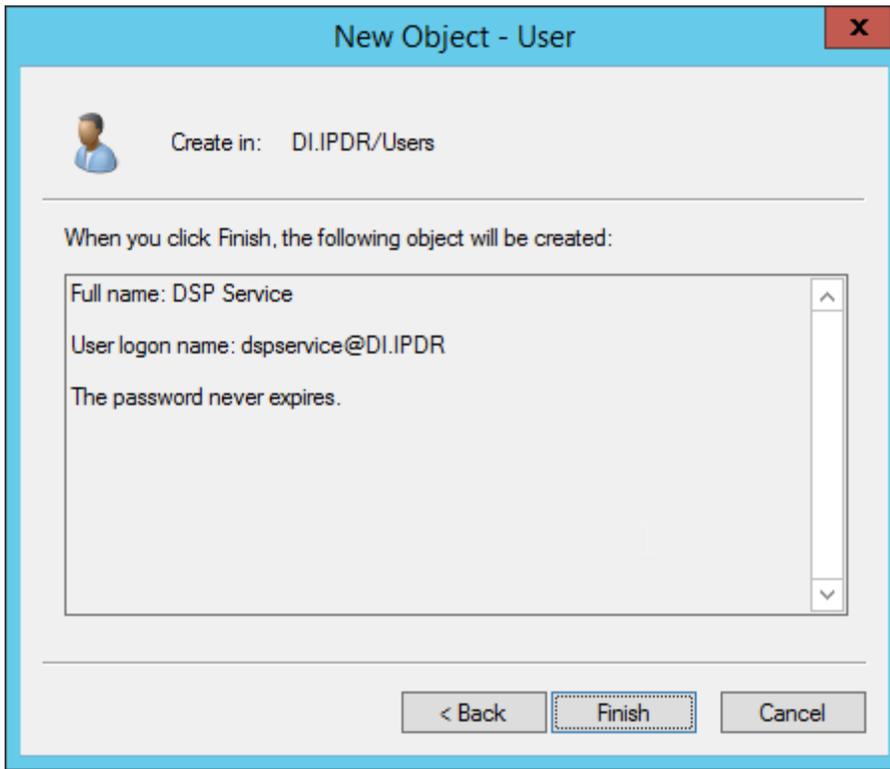
753  
754  
755  
756

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



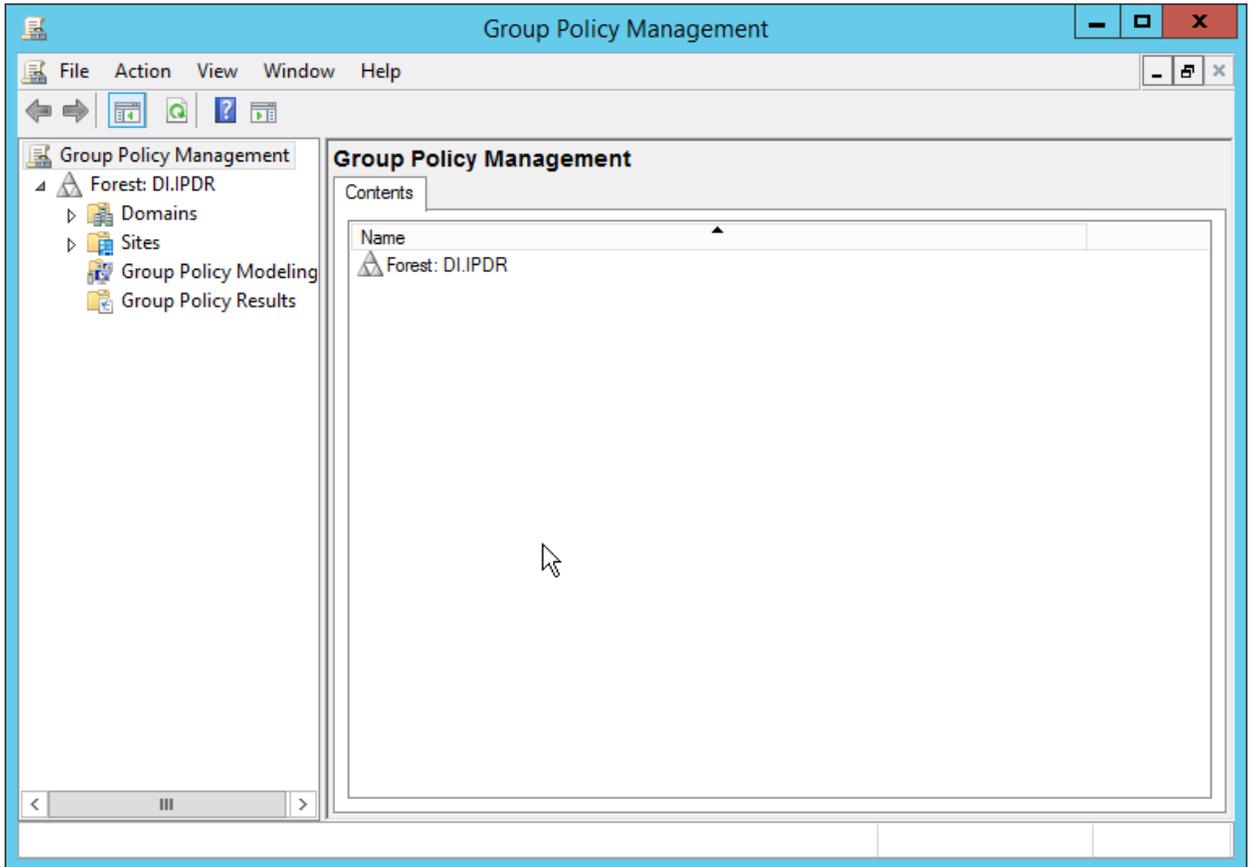
757  
758

7. Click **Next**.



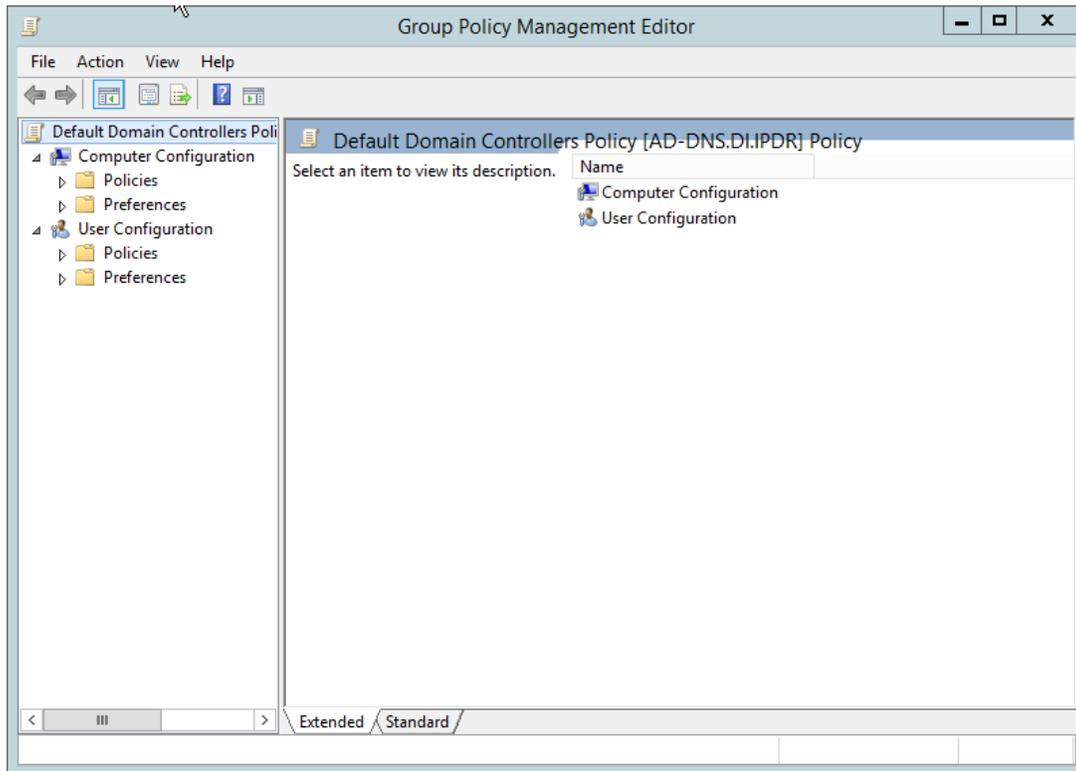
759  
760  
761

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



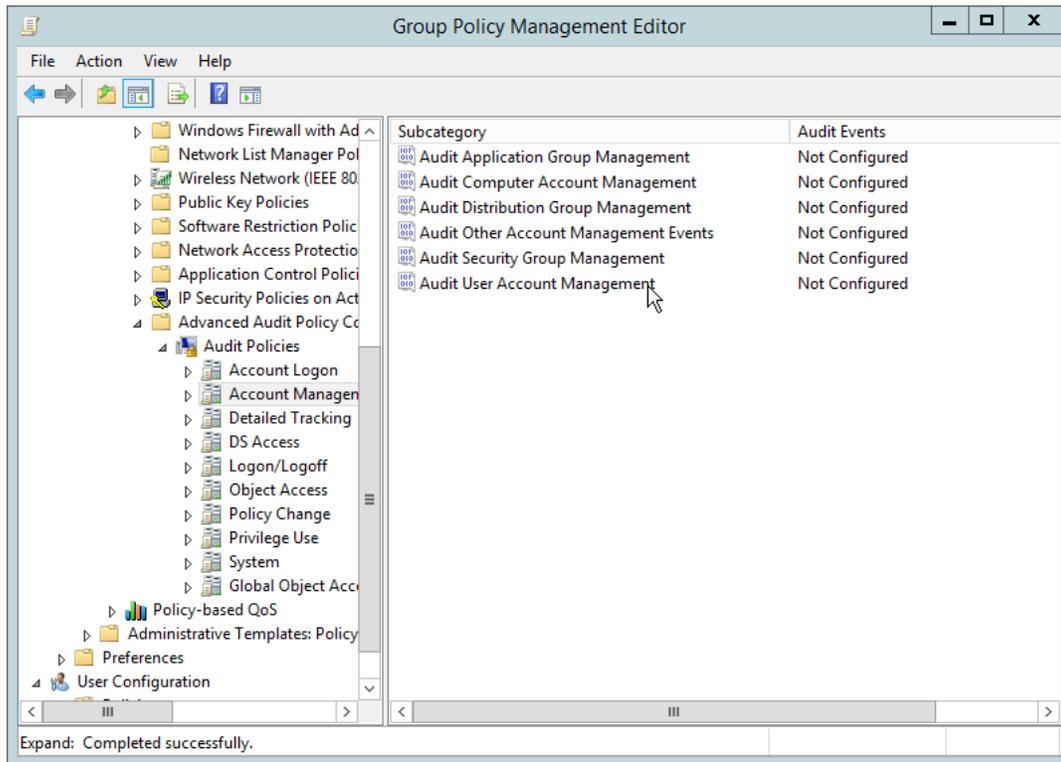
762  
763  
764

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



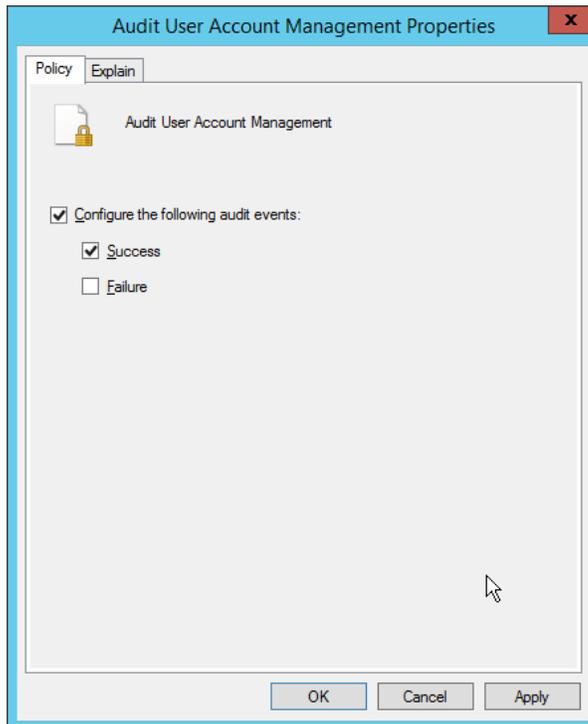
765  
766  
767

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



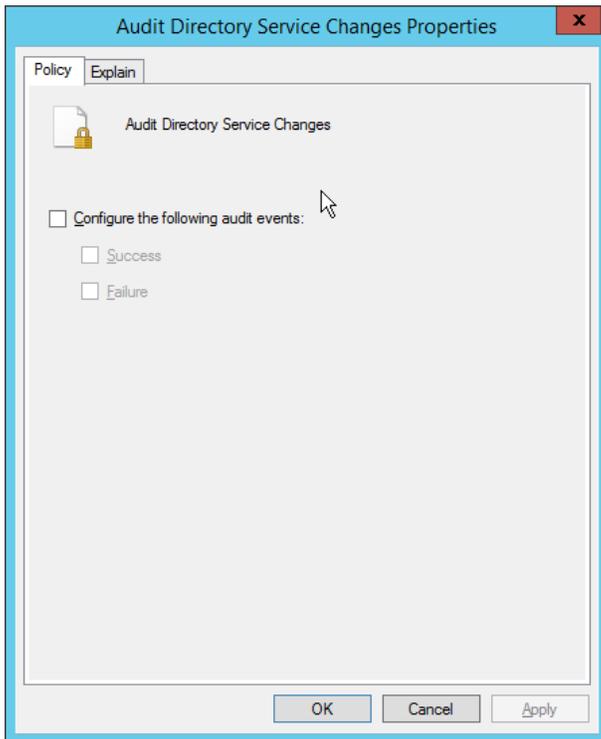
768  
769  
770  
771

12. Edit the **Audit User Account Management** field by double-clicking it.
13. Check the box next to **Configure the following audit events**.
14. Check the box next to **Success**.



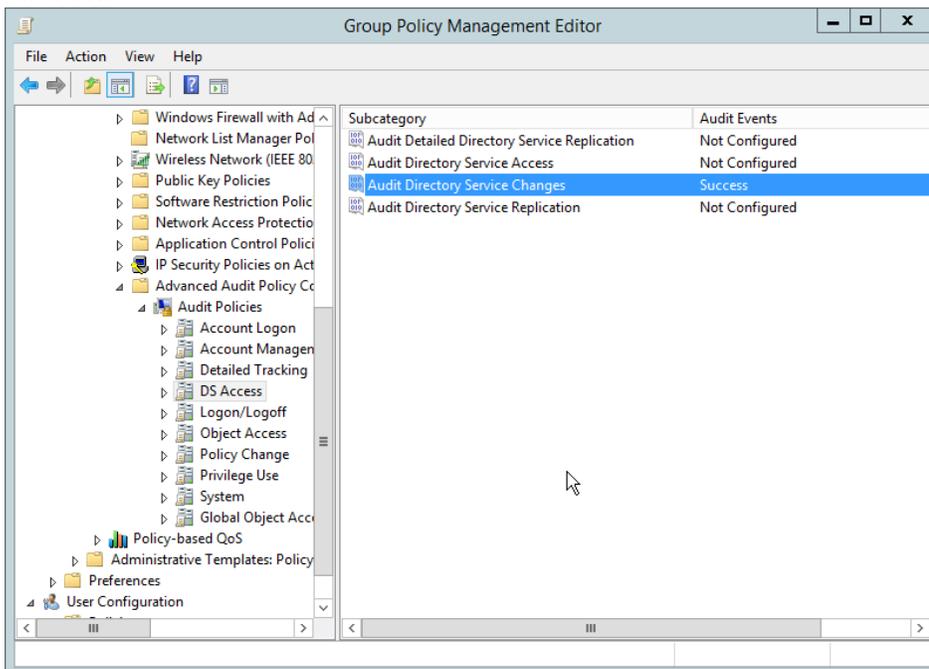
772  
773  
774  
775

15. Click **OK**.
16. Go to **Audit Policies > DS Access**.
17. Double-click **Audit Directory Services Changes**.



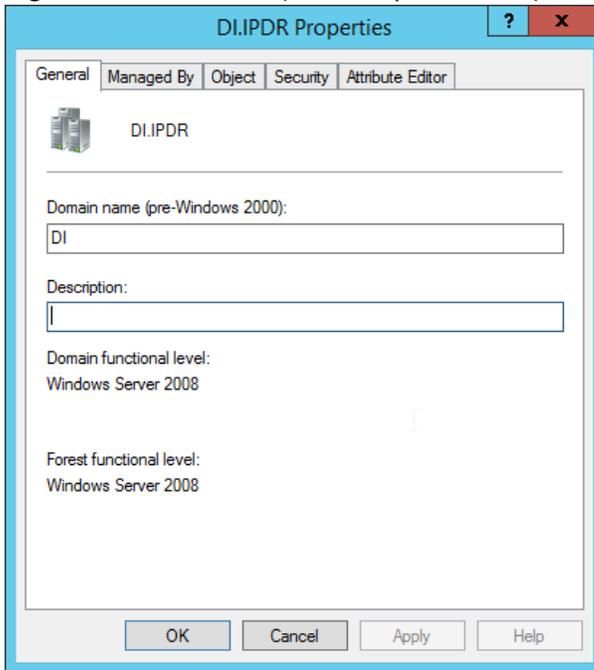
776  
777  
778  
779

18. Check the box next to **Configure the following audit events.**
19. Check the box next to **Success.**
20. Click **OK.**

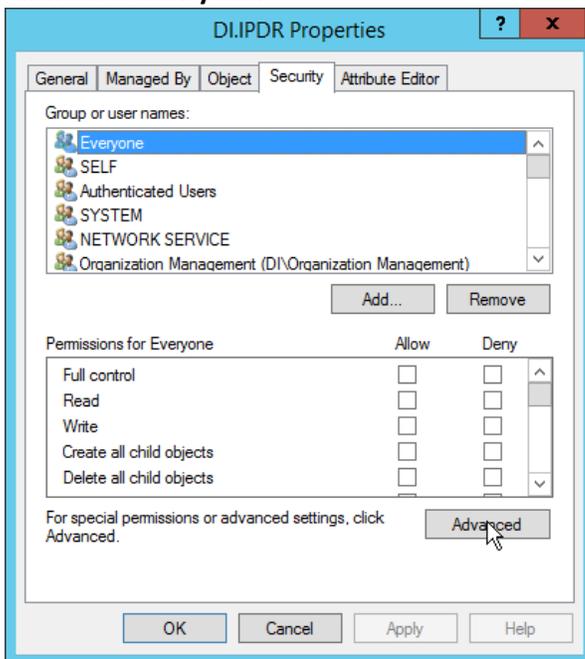


780

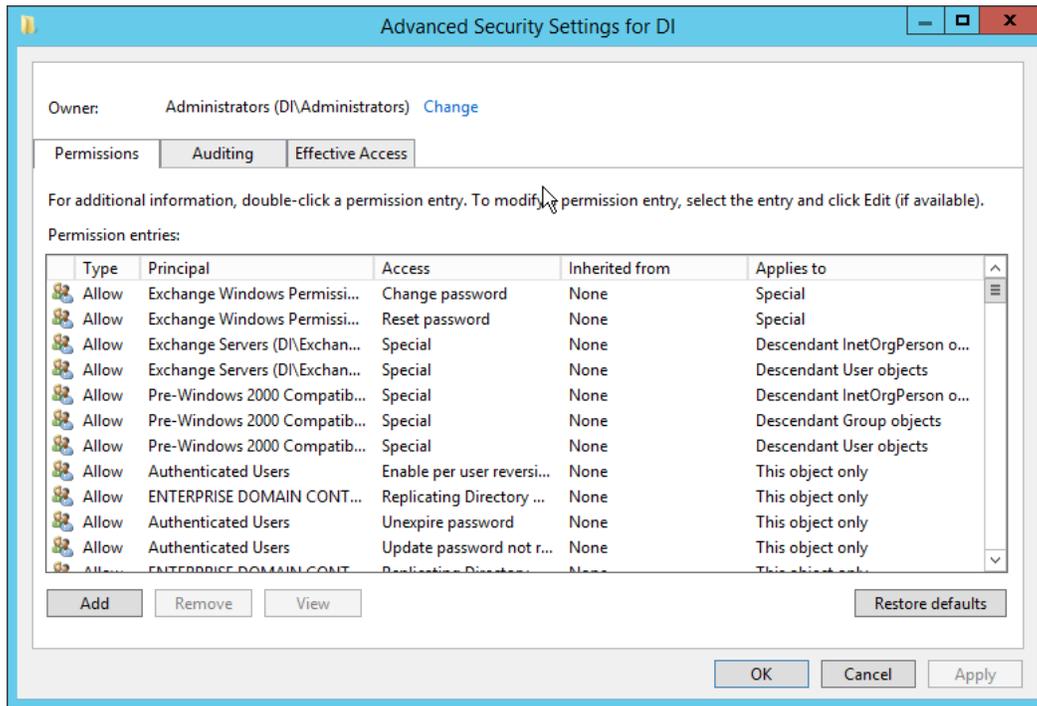
- 781 21. Open **Active Directory Users and Computers**.
- 782 22. Ensure **View > Advanced Features** is enabled.
- 783 23. Right-click the **domain** (for example, DI.IPDR) created earlier, and click **Properties**.



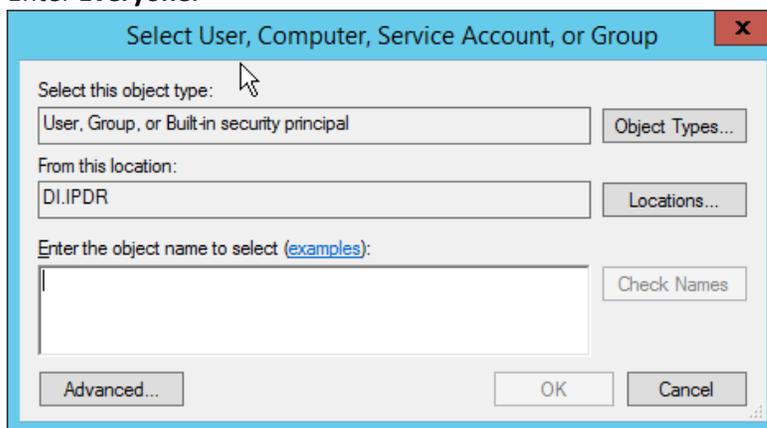
- 784 24. Click the **Security** tab.
- 785



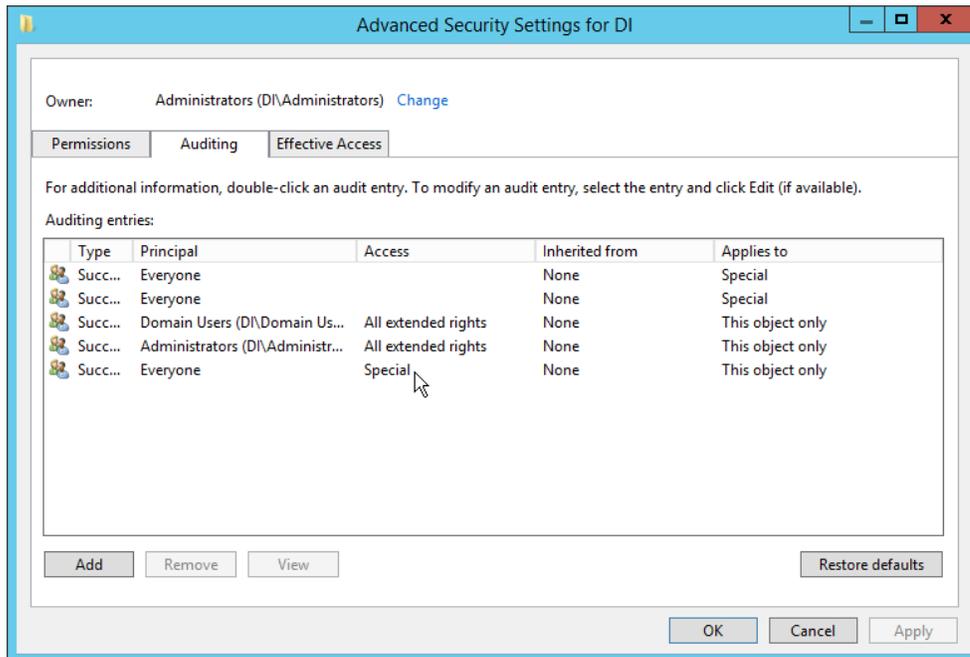
- 786 25. Click **Advanced**.
- 787



- 788
- 789 26. Click the **Auditing** tab.
- 790 27. Click **Add**.
- 791 28. Enter **Everyone**.

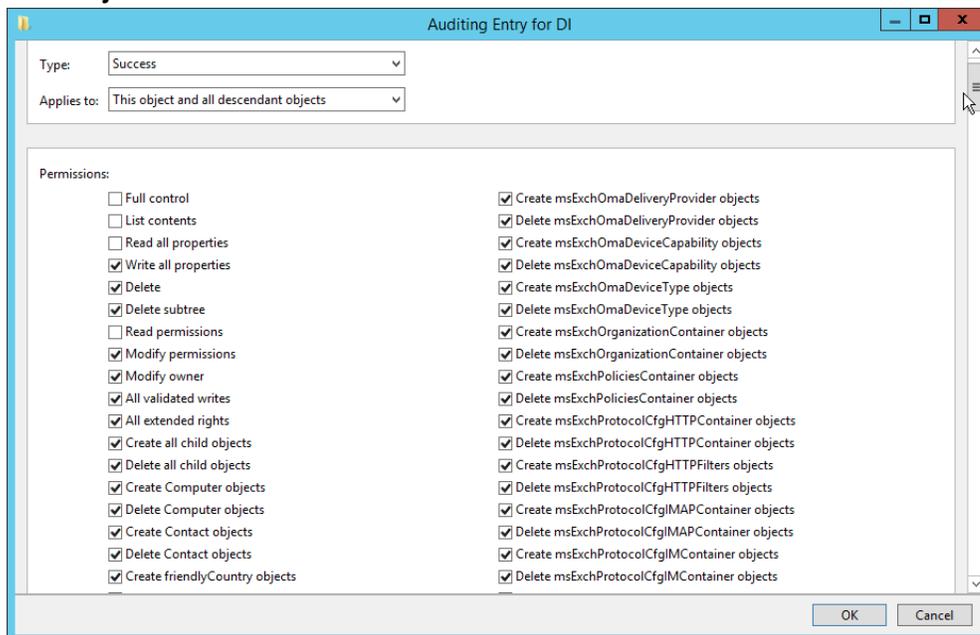


- 792
- 793 29. Click **OK**.



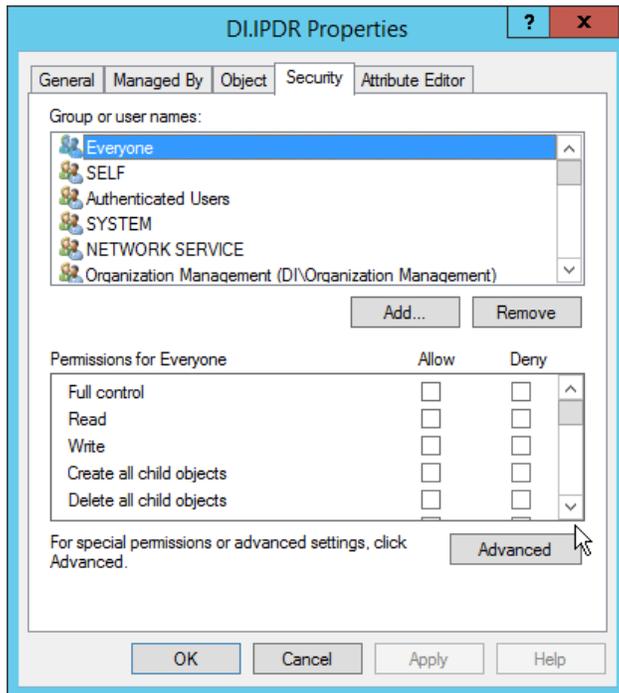
794  
795  
796  
797  
798

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



799  
800

32. Click **OK**.

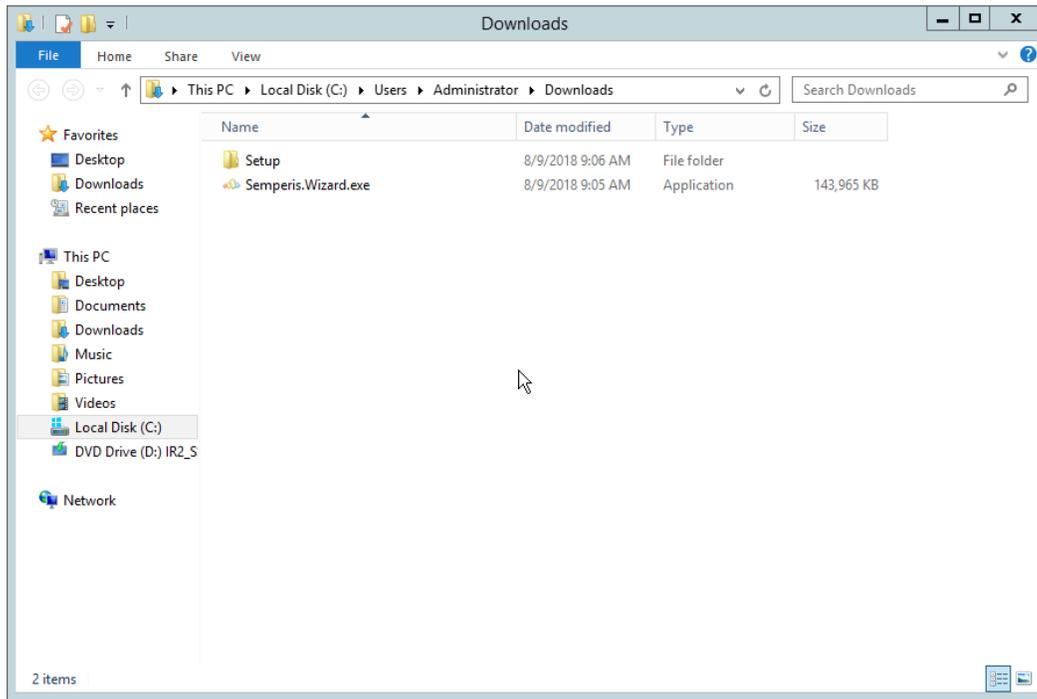


801  
802

33. Click **OK**.

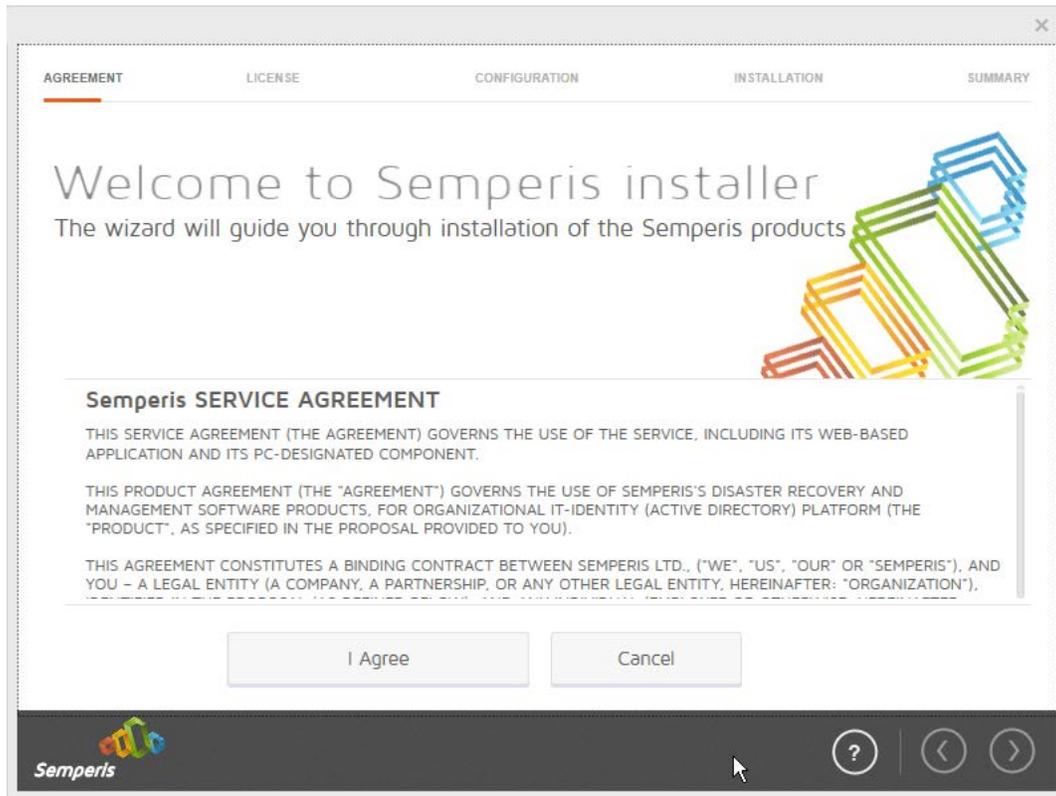
## 803 2.6.2 Install Semperis DSP

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



808  
809

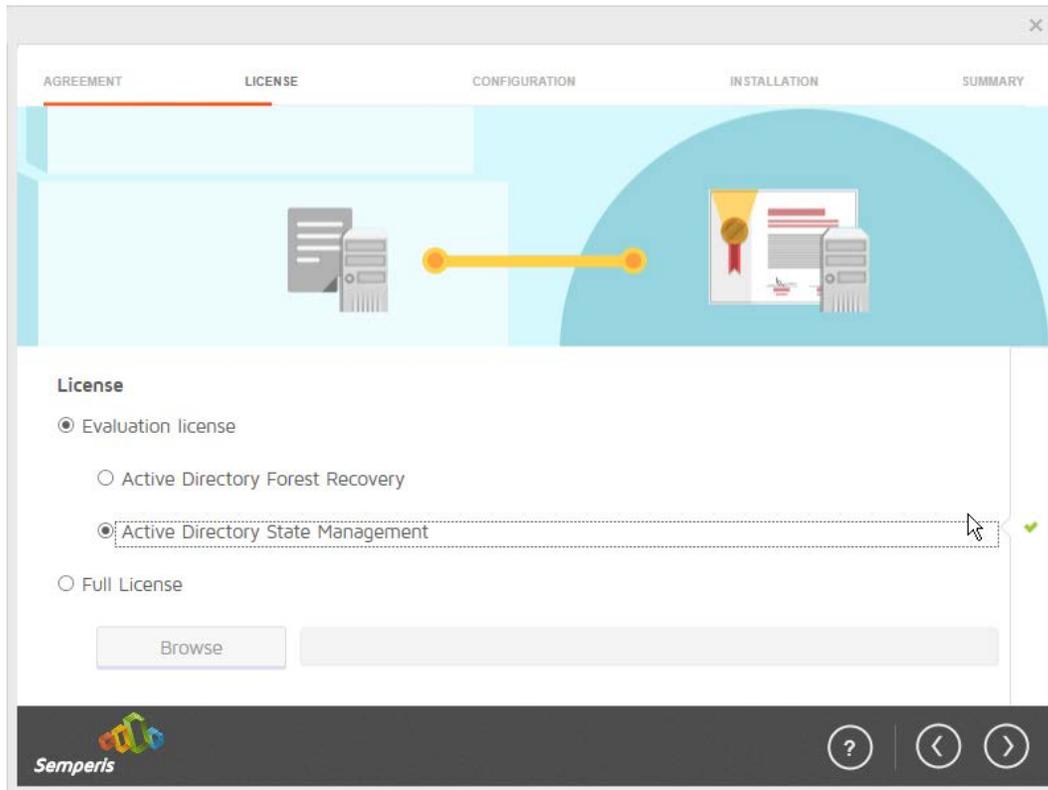
2. If prompted to restart the computer, do so.



810  
811  
812  
813

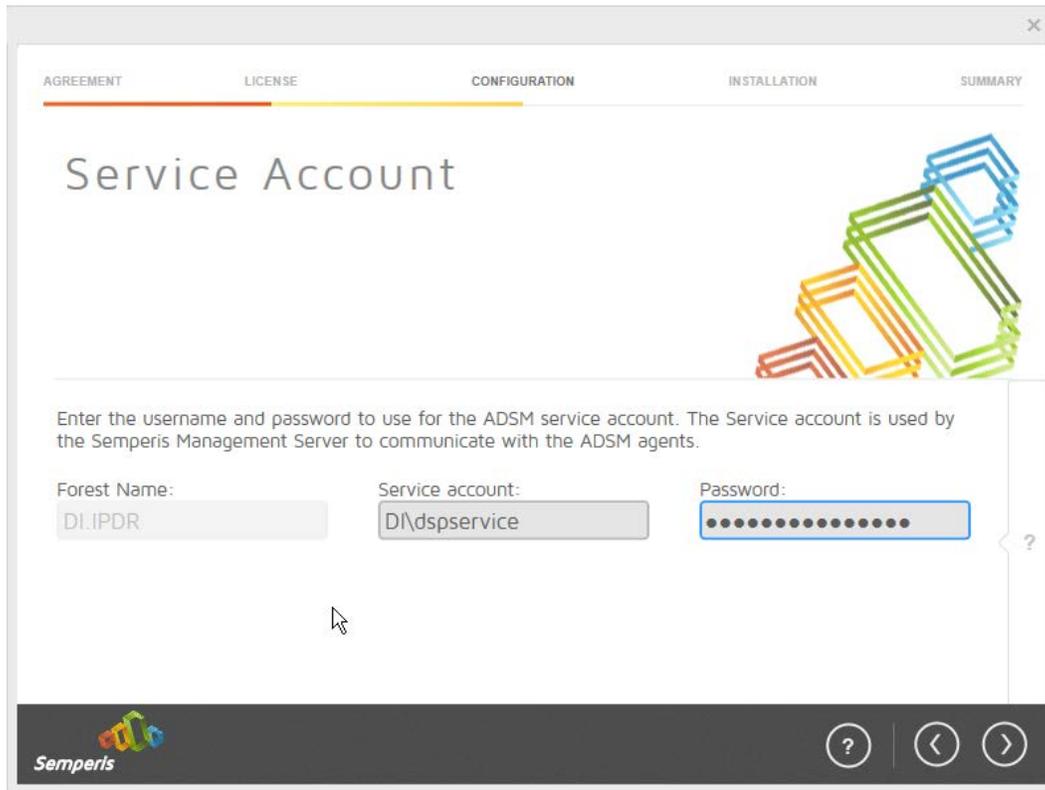
3. Click **I Agree**.
4. Select **Evaluation License**.
5. Select **Active Directory State Management**.

DRAFT



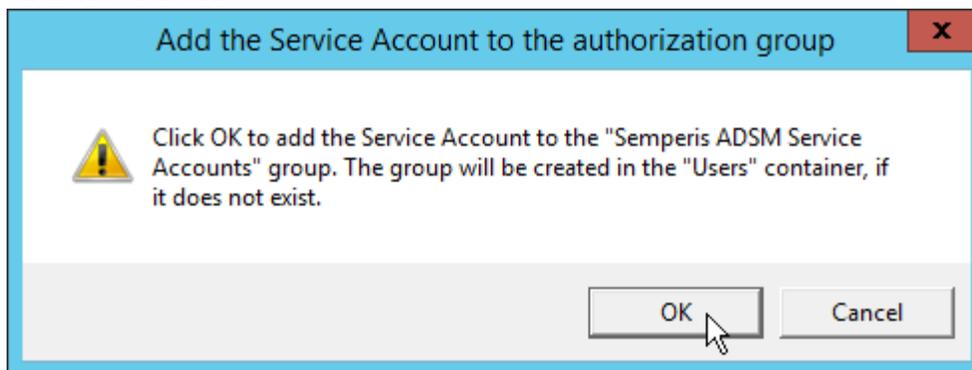
814  
815  
816

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



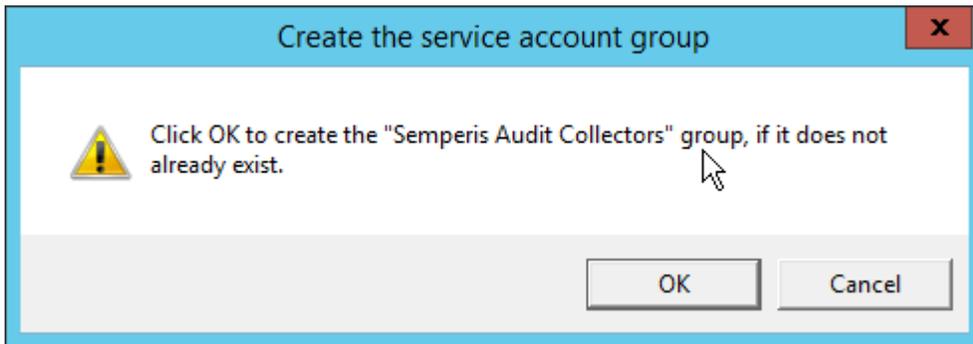
817  
818

8. Click the > button.



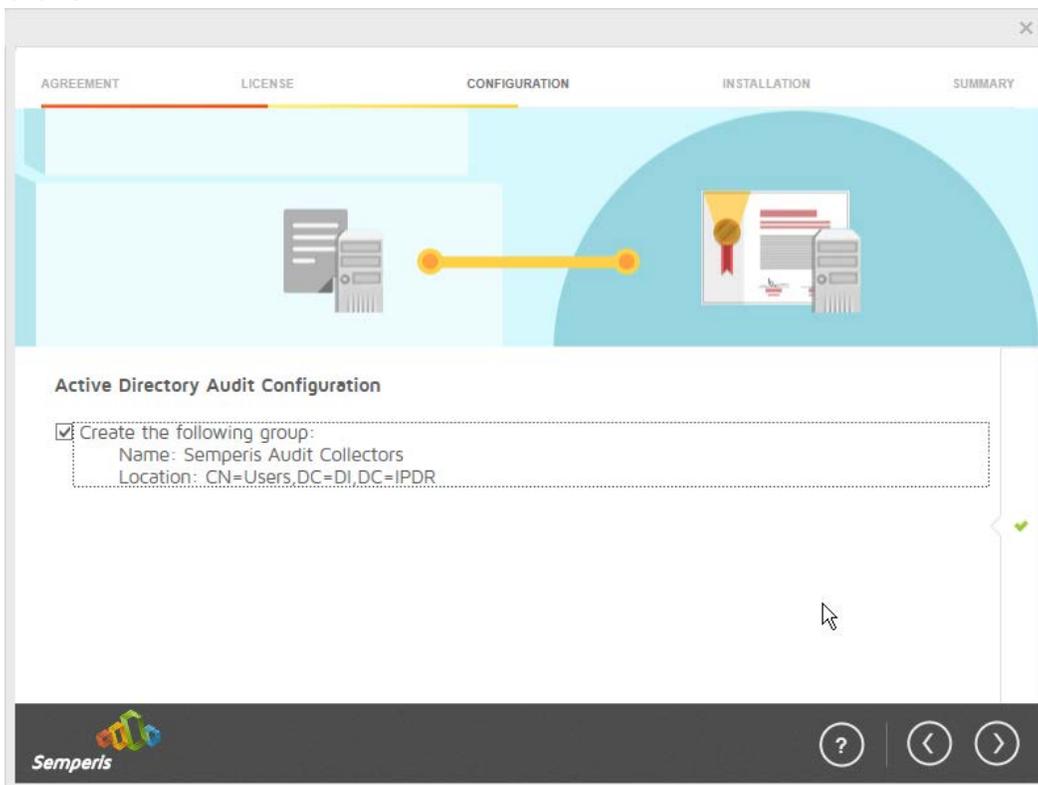
819  
820  
821

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



822  
823

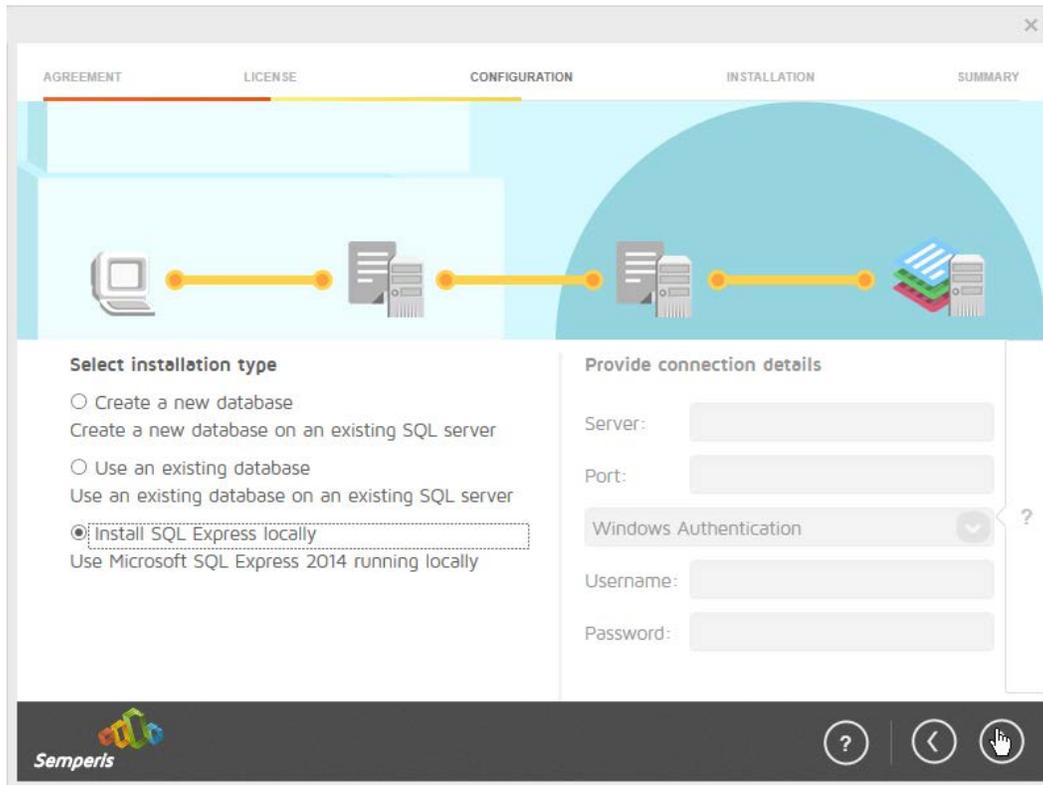
11. Click **OK**.



824  
825  
826

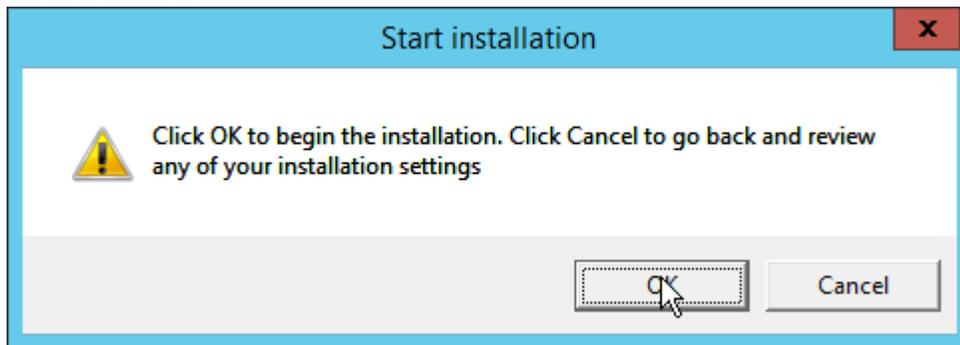
12. Click the > button.

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



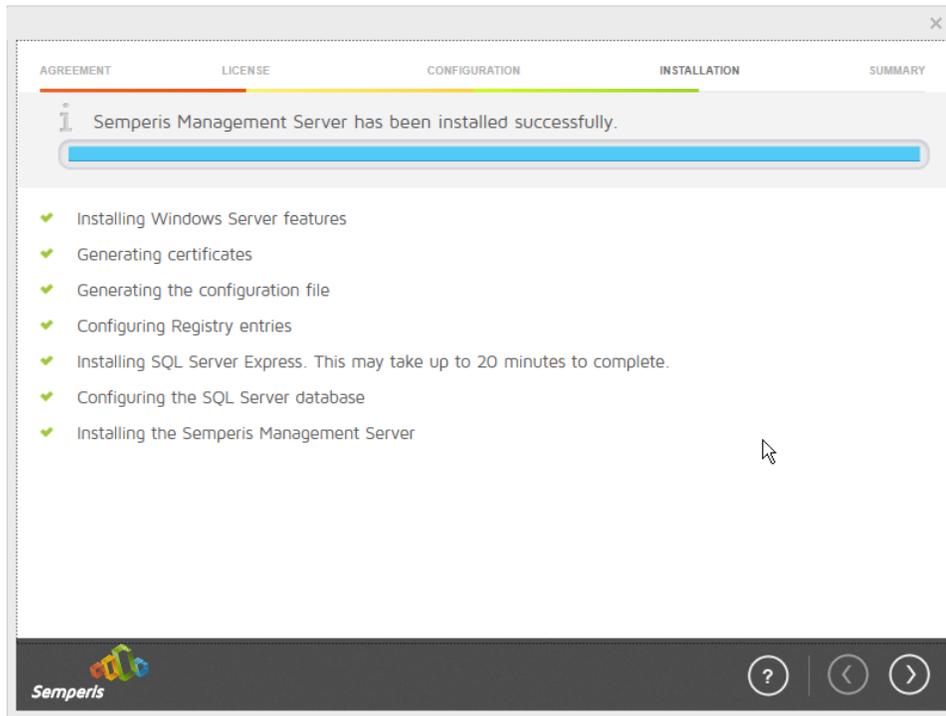
827  
828

14. Click the > button.



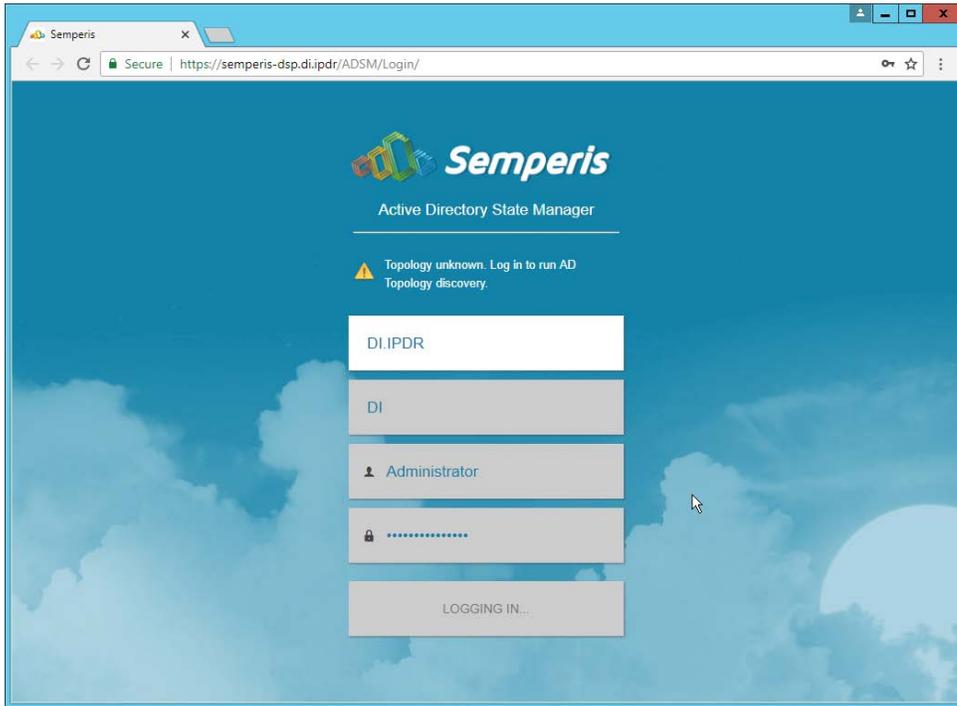
829  
830

15. Click **OK**.



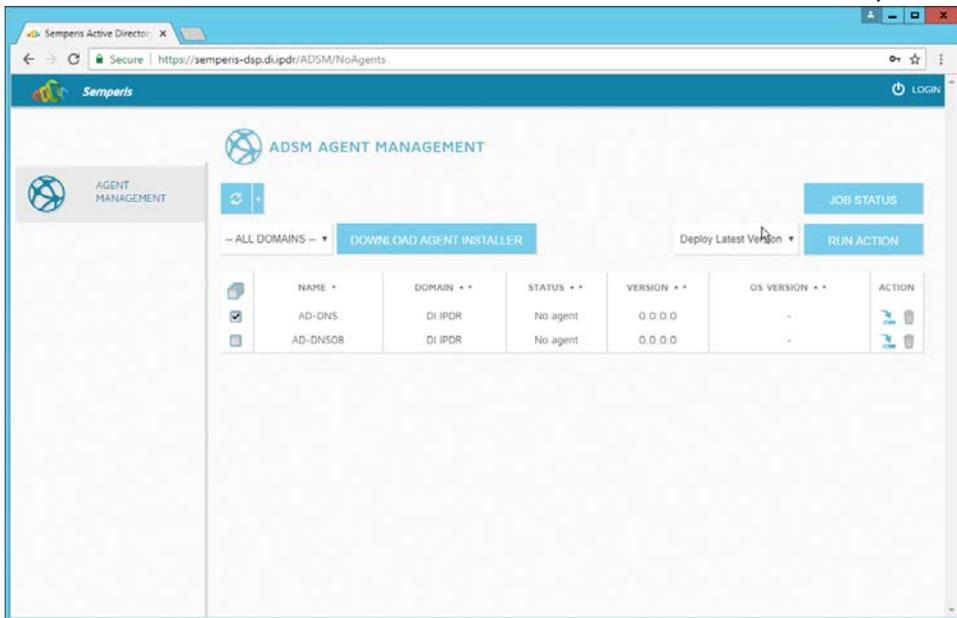
831  
832  
833  
834  
835  
836

16. Click the > button after the installation completes.
17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS Protector**.
18. On the login page, enter the full domain as well as the NetBIOS name.
19. Enter the **username** and **password** of an administrator on the domain.



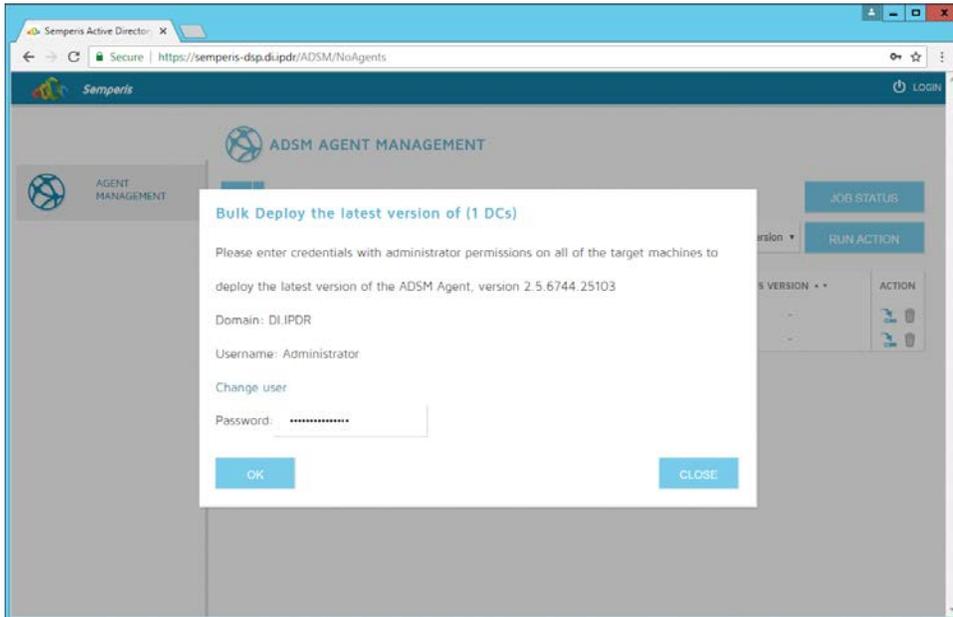
837  
838  
839

- 20. Click **Login**.
- 21. Check the box next to the domain controllers that should be monitored by DSP.



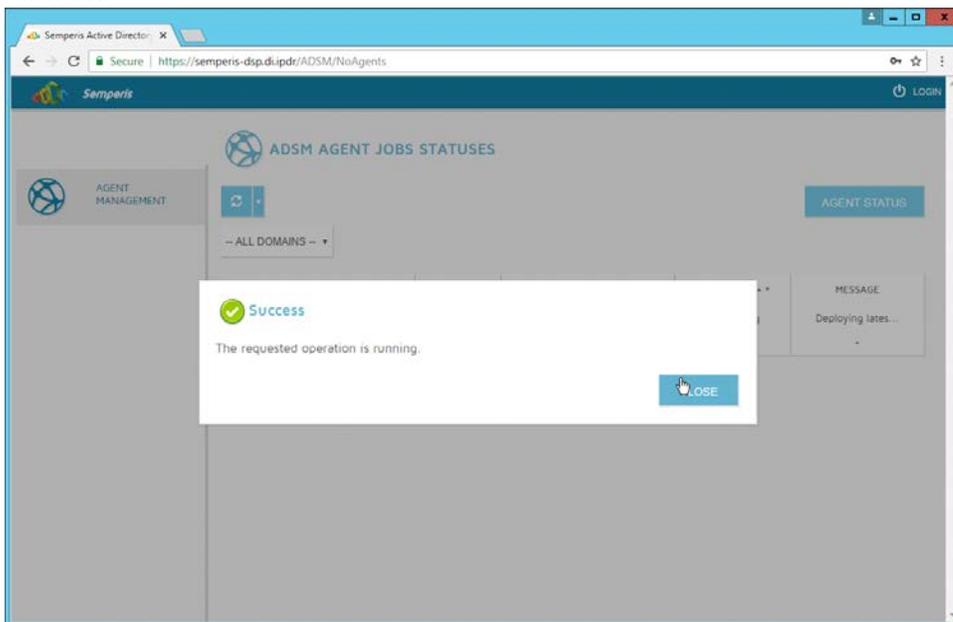
840  
841  
842

- 22. Click **Run Action**.
- 23. Enter the **password** for the account.



843  
844

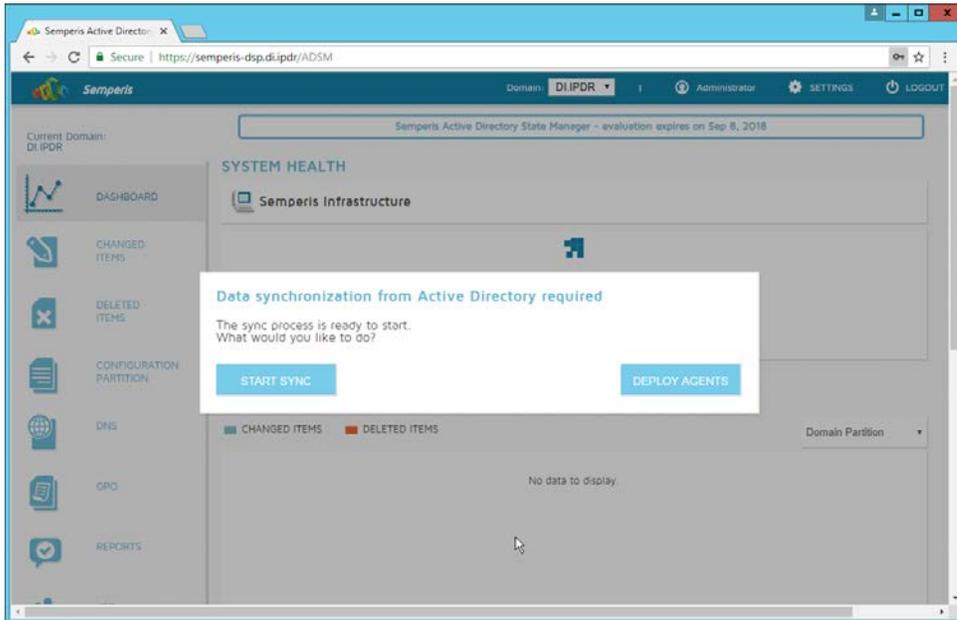
24. Click **OK**.



845  
846  
847

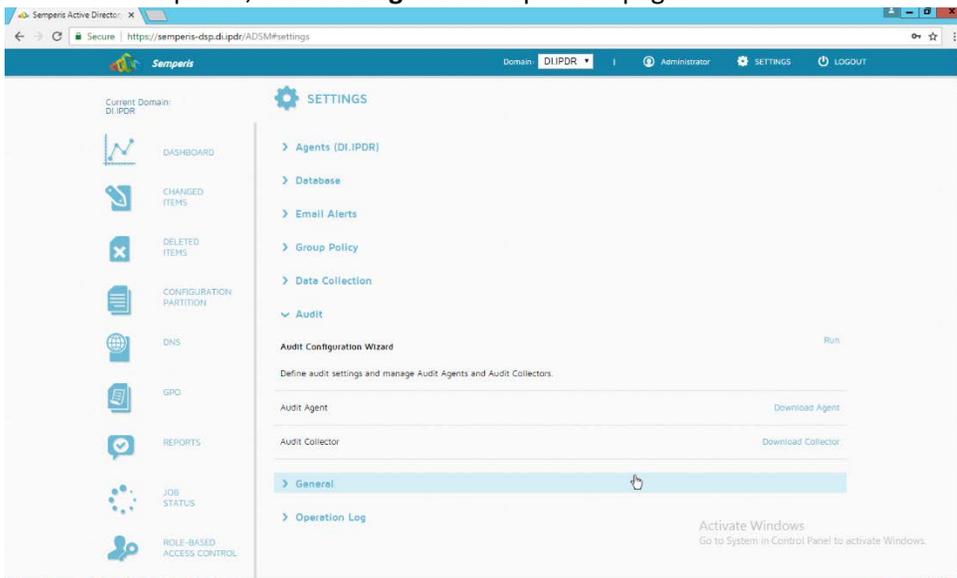
25. Click **Close**.

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



848  
849  
850

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

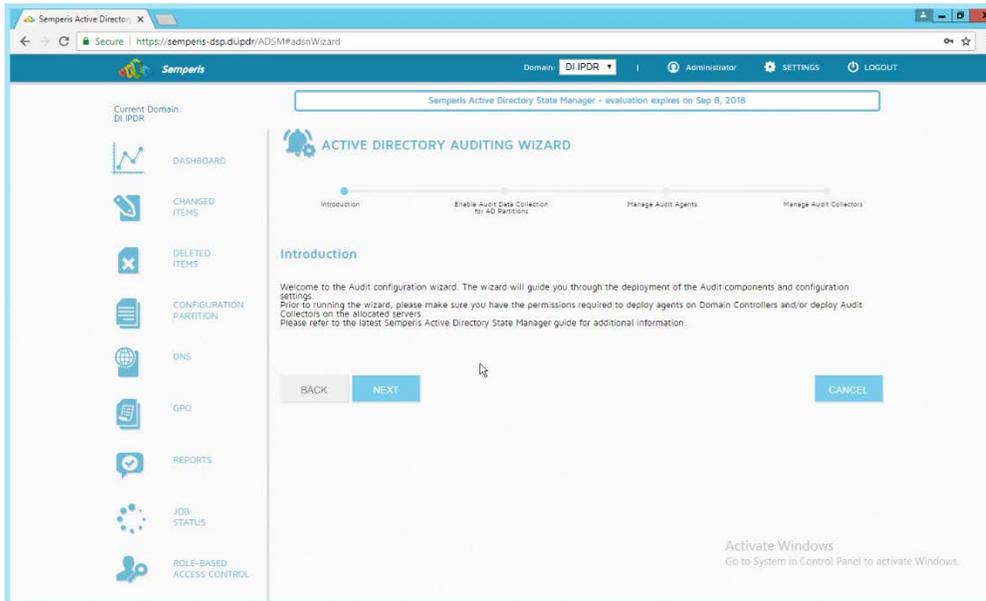


851  
852  
853

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

854  
855

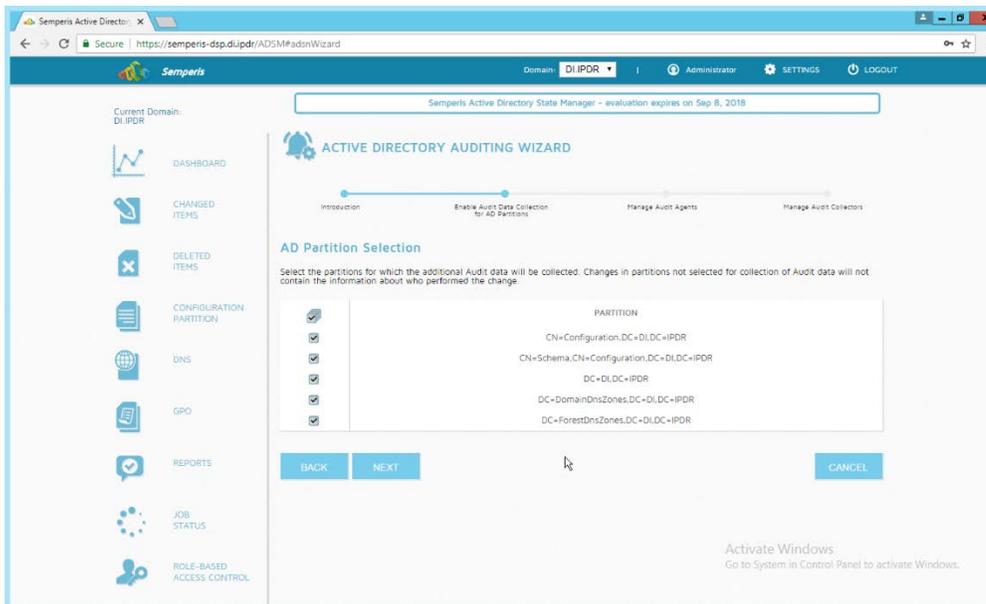
31. Click **Next**.



856  
857  
858

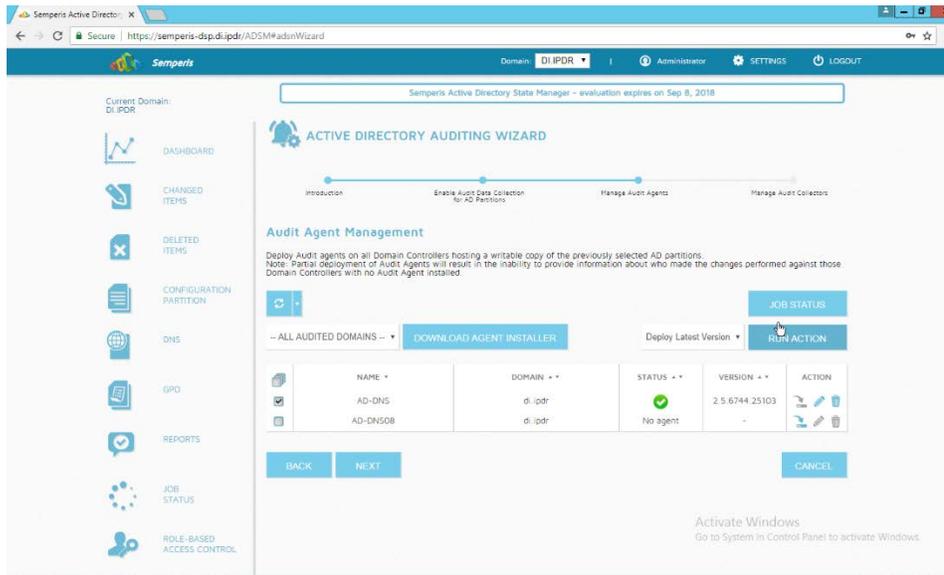
32. Click **Next**.

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



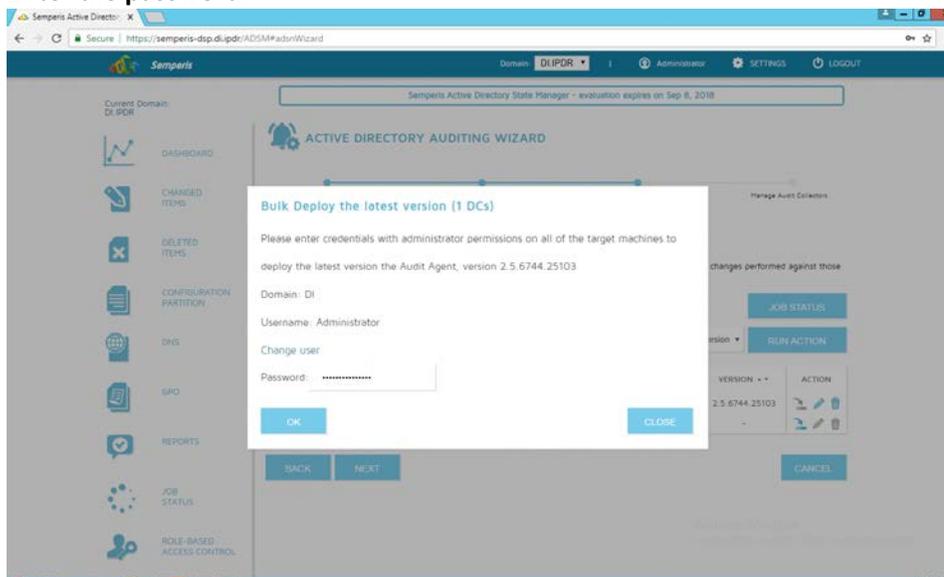
859  
860  
861

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



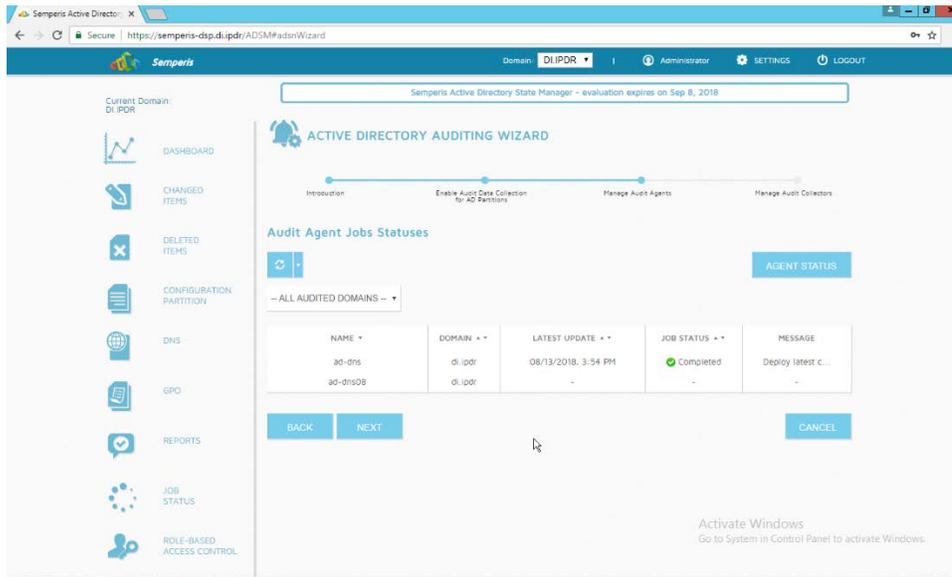
862  
863  
864

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



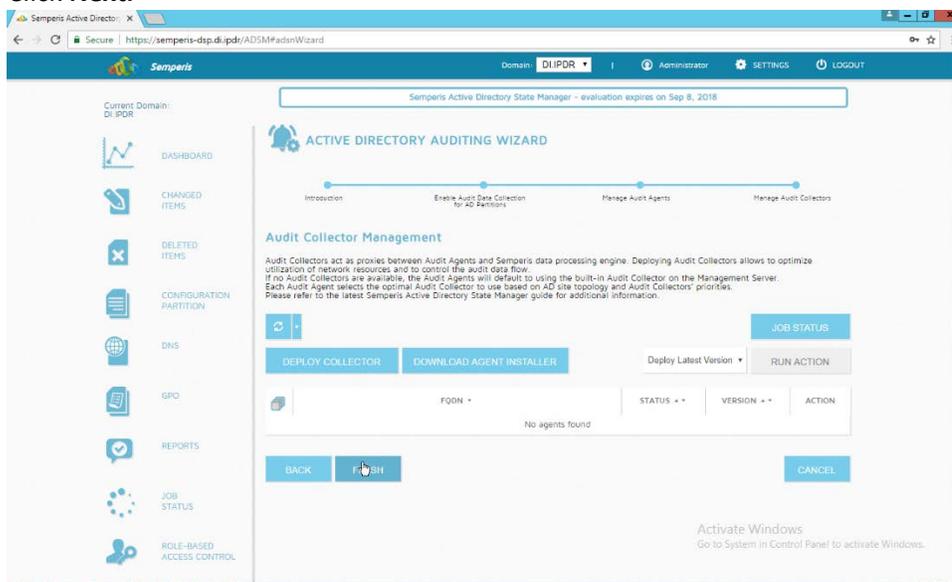
865  
866

38. Click **Next**.



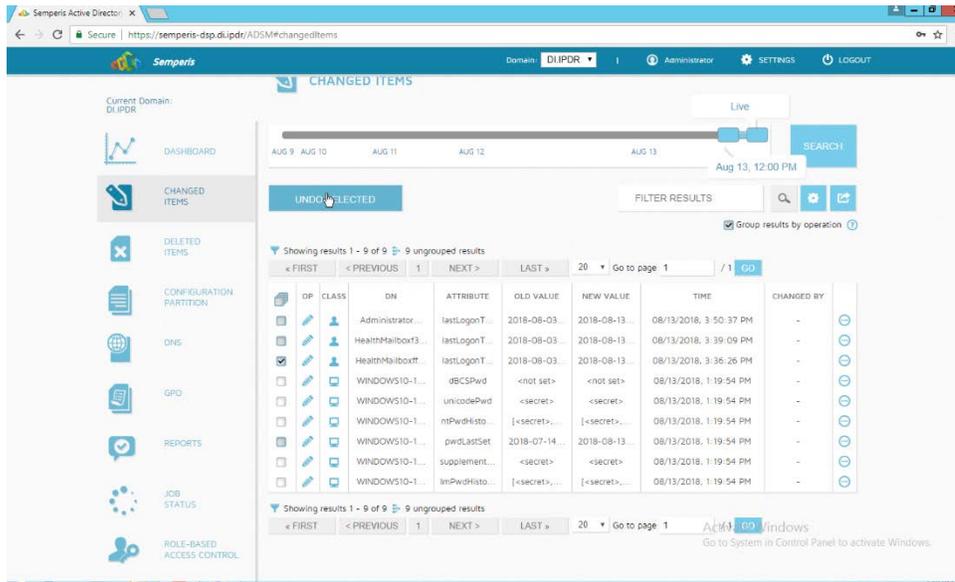
867  
868

39. Click **Finish**.



### 869 2.6.3 Roll Back Changes with Semperis DSP

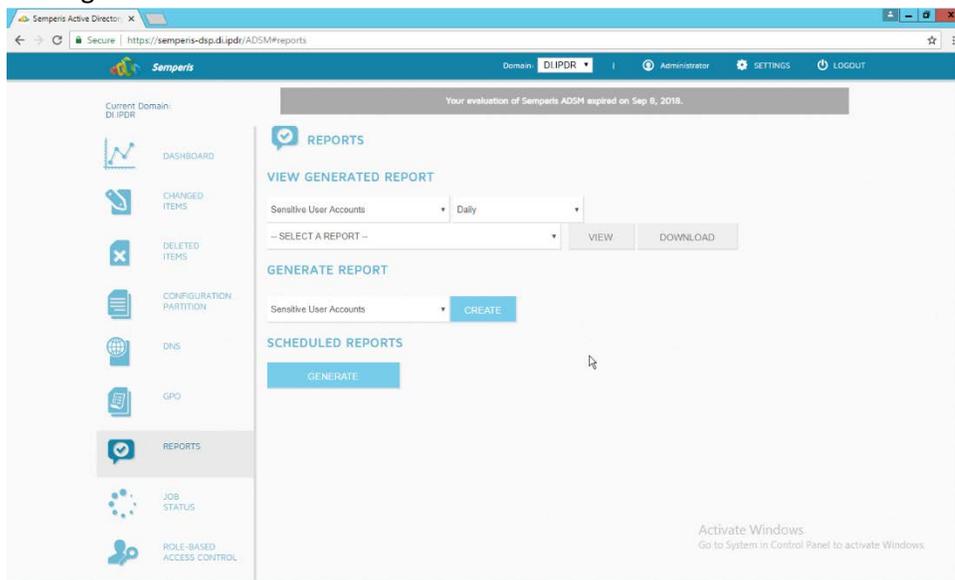
- 870 1. Go to **Changed Items** on the left navigation bar.
- 871 2. Check the box next to any undesired Active Directory changes.
- 872 3. Click the ... button to view more details about the change.



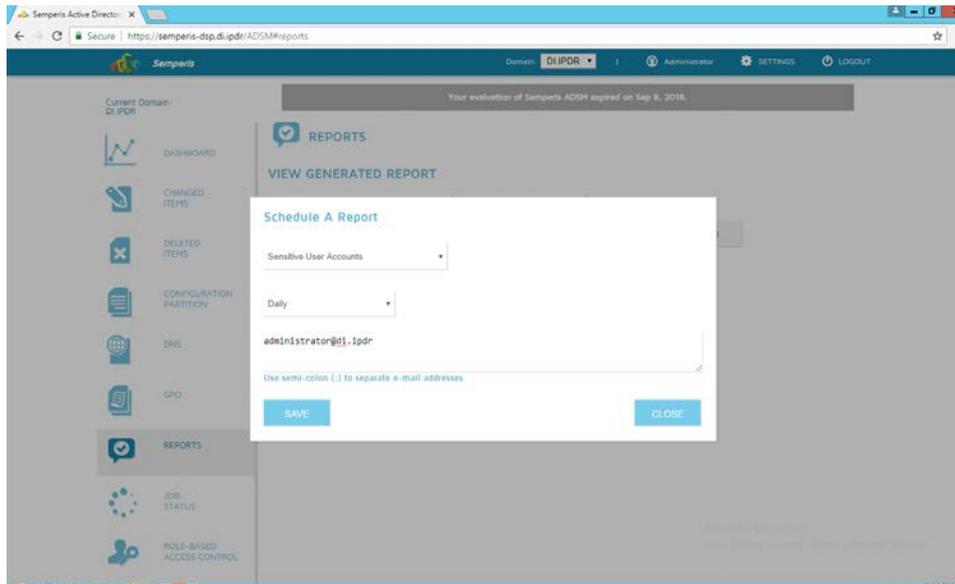
- 873  
874
4. Click **Undo Selected** to roll back these changes.

### 875 2.6.4 Configure Reporting with Semperis DSP

- 876  
877  
878
1. Click **Reports** on the left sidebar in the **Semperis DSP** web console.
  2. Under **Generate Report**, reports can be viewed instantly, by selecting a type of report and clicking **Create**.



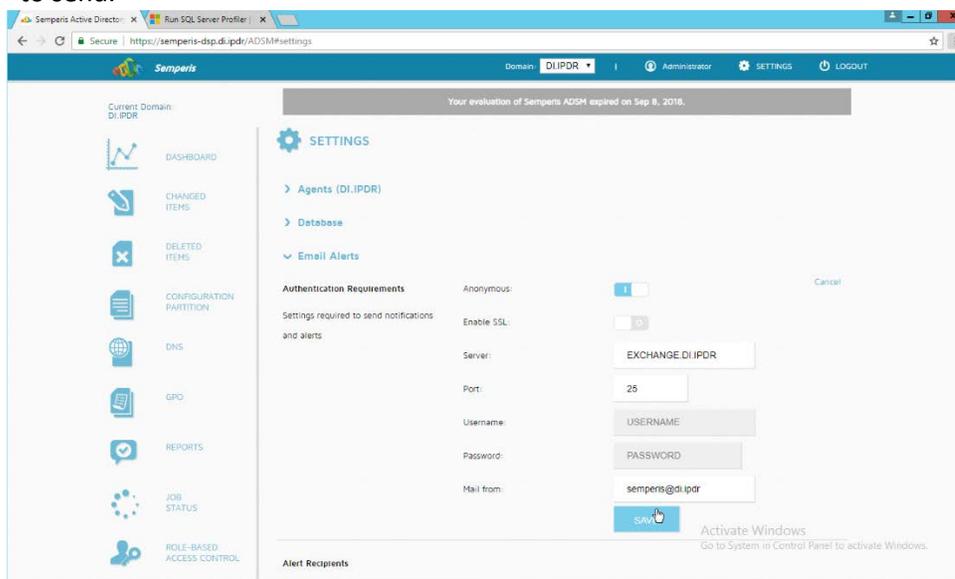
- 879  
880  
881  
882
3. Under **Scheduled Reports**, click **Generate** to automatically email specific reports.
  4. Select a report type and a schedule.
  5. Enter the email addresses of anyone who should receive this report.



- 883  
884
6. Click **Save**.

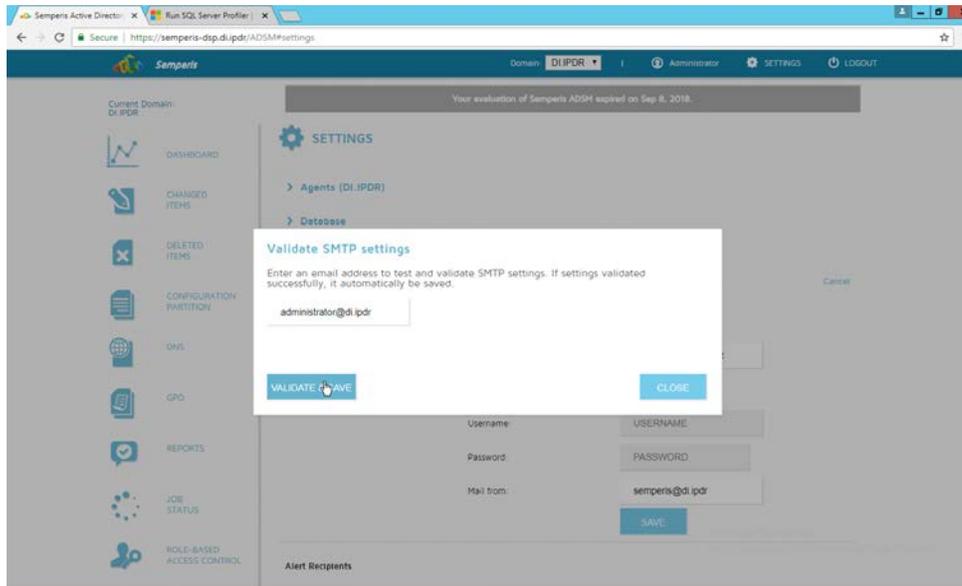
## 885 2.6.5 Configure Email Alerts with Semperis DSP

- 886  
887  
888  
889  
890
1. Click **Settings** on the **Semperis DSP** web console.
  2. Expand the **Email Alerts** section.
  3. Click **Edit**.
  4. Enter the information of the organization’s email server as well as an email address from which to send.

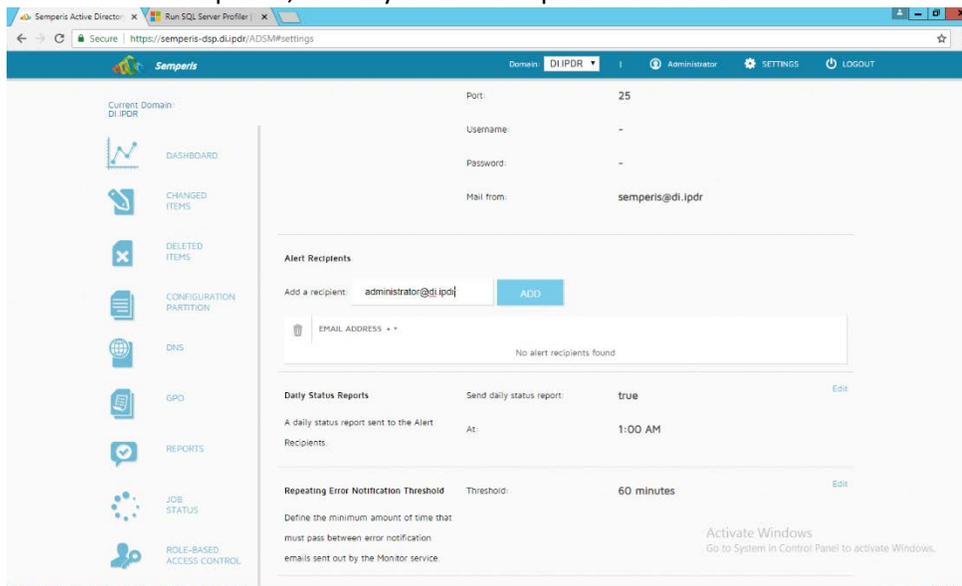


- 891  
892
5. Click **Save**.

- 893 6. Enter an email address to which to send a test email.



- 894 7. Click **Validate & Save**.  
 895 8. Under Alert Recipients, add any desired recipients of alerts.  
 896



- 897 9. Click **Add**.  
 898 10. Configure any schedule settings according to your organization's needs.  
 899

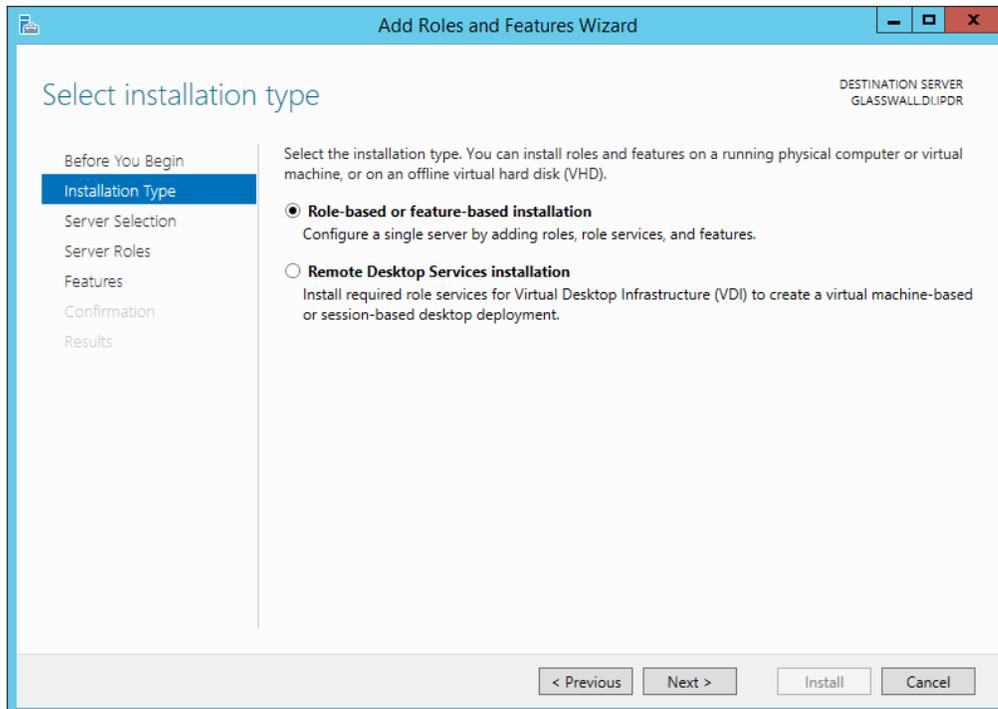
## 900 2.7 Glasswall FileTrust™ for Email

901 The following sections will detail the installation of **Glasswall FileTrust™ for Email**, an email security  
902 product, on a new Windows 2012 R2 machine. For the purposes of this guide, we use Microsoft  
903 Exchange as the email service provider.

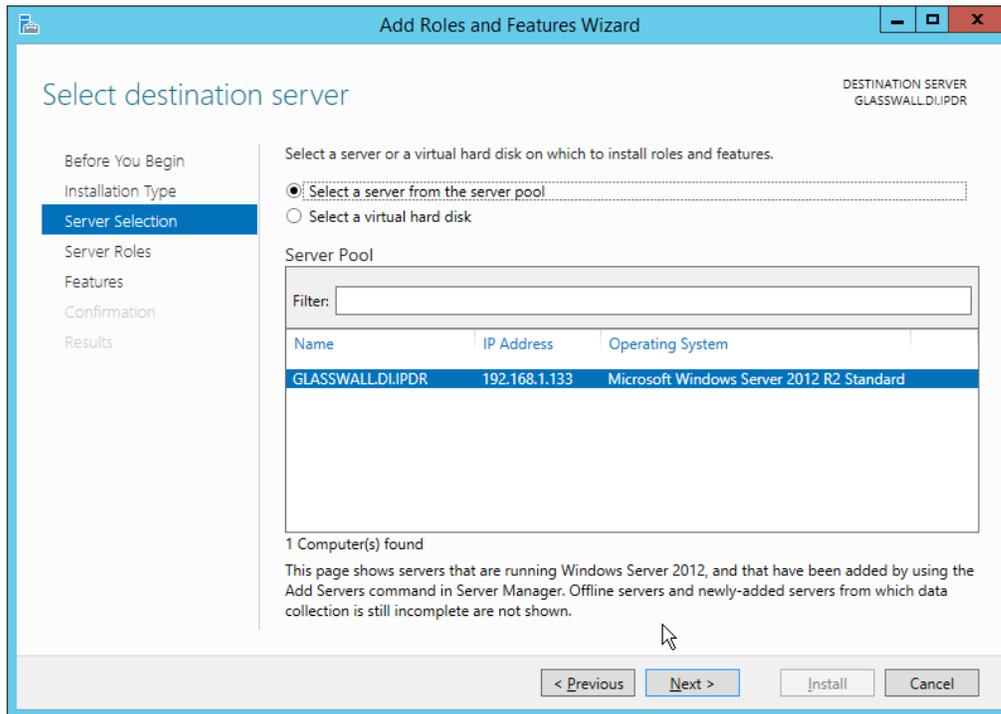
### 904 2.7.1 Install Prerequisites

#### 905 2.7.1.1 *Install the IIS web server*

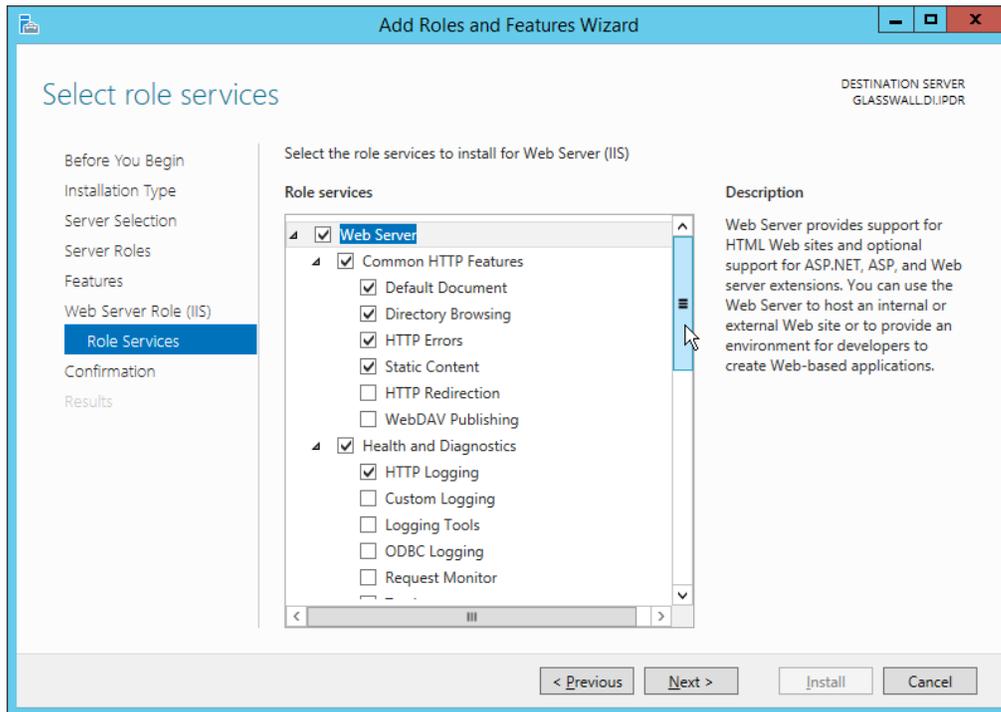
- 906 1. In **Server Manager**, click **Add Roles and Features**.
- 907 2. Click **Next**.
- 908 3. Select **Role-based or feature-based installation**.



- 909 4. Click **Next**.
- 910 5. Select the current server.
- 911



- 912
- 913 6. Click **Next**.
- 914 7. Select **Web Server (IIS)**.
- 915 8. Click **Next**.
- 916 9. Select **.NET Framework 4.5 Features**.
- 917 10. Click **Next**.
- 918 11. Select the following Role Services: **Web Server, Common HTTP Features, Default Document,**
- 919 **Directory Browsing, HTTP Errors, Static Content, Health and Diagnostics, HTTP Logging,**
- 920 **Performance, Static Content Compression, Security, Request Filtering, Client Certificate**
- 921 **Mapping Authentication, Application Development, .NET Extensibility 4.5, ASP.NET 4.5, ISAPI**
- 922 **Extensions, ISAPI Filters, Management Tools, and IIS Management Console.**



923

924 12. Click **Next**.925 13. Check the box next to **Restart the destination server automatically if required**.926 14. Click **Install**.927 

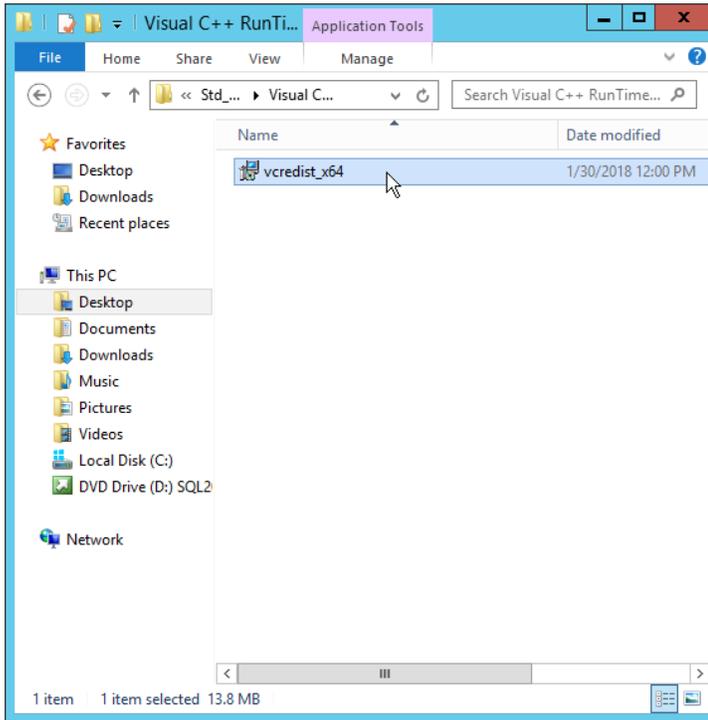
### 2.7.1.2 *Install Microsoft SQL 2014 Enterprise*

928 Please see Section 2.4 for an installation guide for MS SQL 2014; for simplicity it should be installed on  
 929 the same server as Glasswall FileTrust. Ensure that Mixed Mode authentication is selected when  
 930 installing.

931 

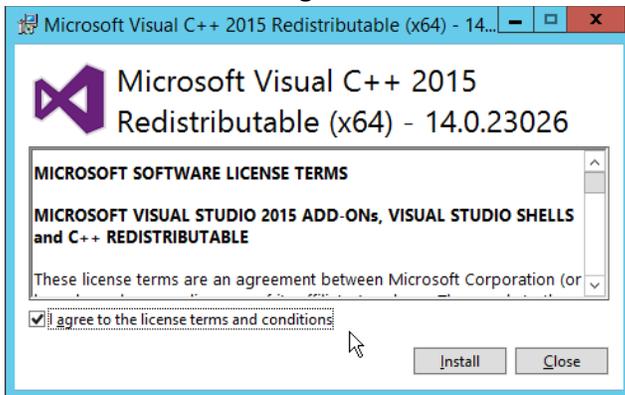
### 2.7.1.3 *Install Microsoft Visual C++ 2015*

932 1. Run the **vcredist\_x64** installer.



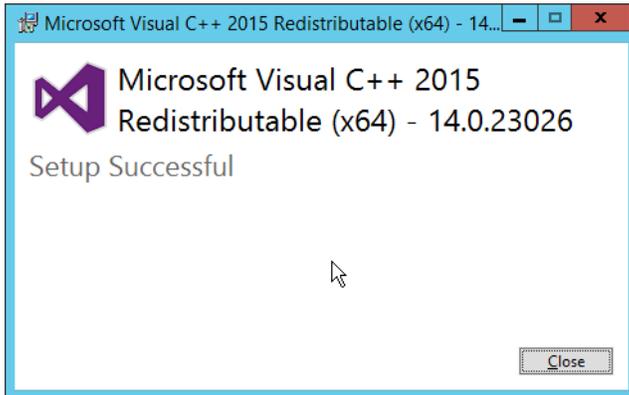
933  
934

2. Check the box next to **I agree to the license terms and conditions.**



935  
936  
937

3. Click **Install.**
4. After the installation is complete, click **Close.**

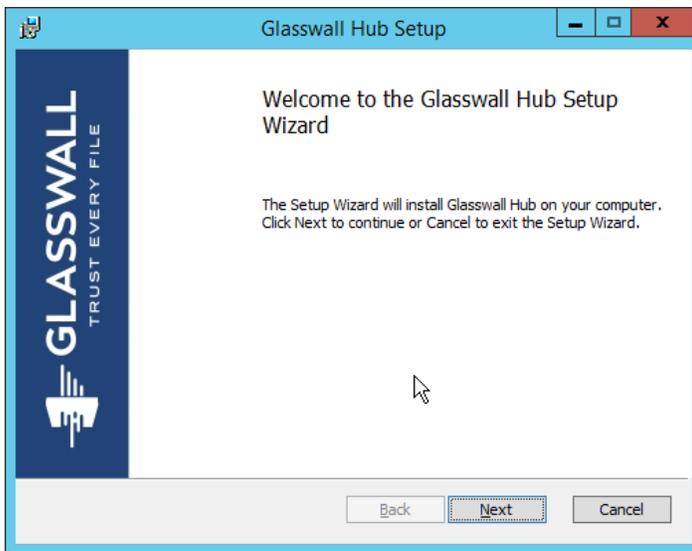


938

939 **2.7.2 Install the Glasswall FileTrust Server Component**

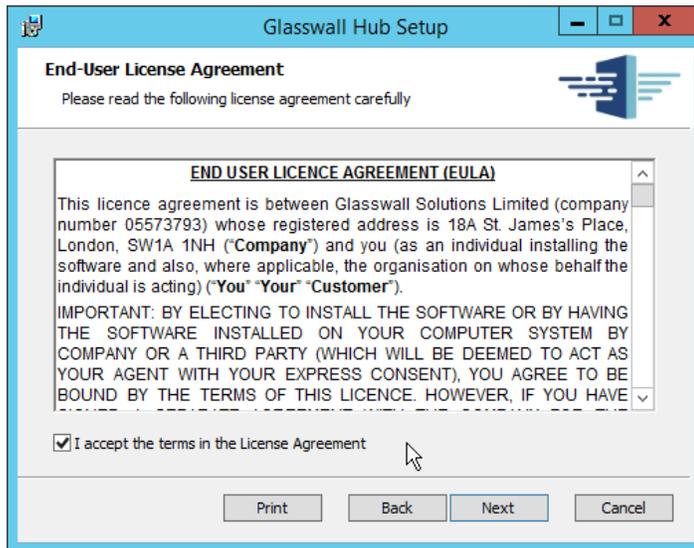
940 **2.7.2.1 Install Glasswall Hub**

- 941 1. Run **HubInstaller.msi**.



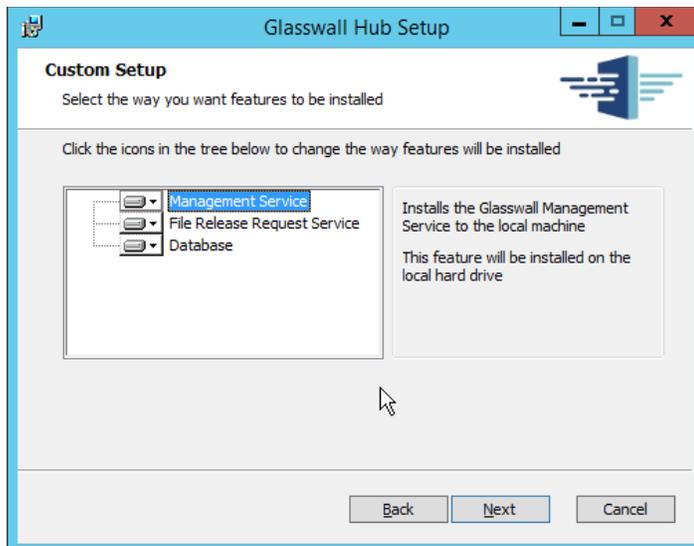
942

- 943 2. Click **Next**.



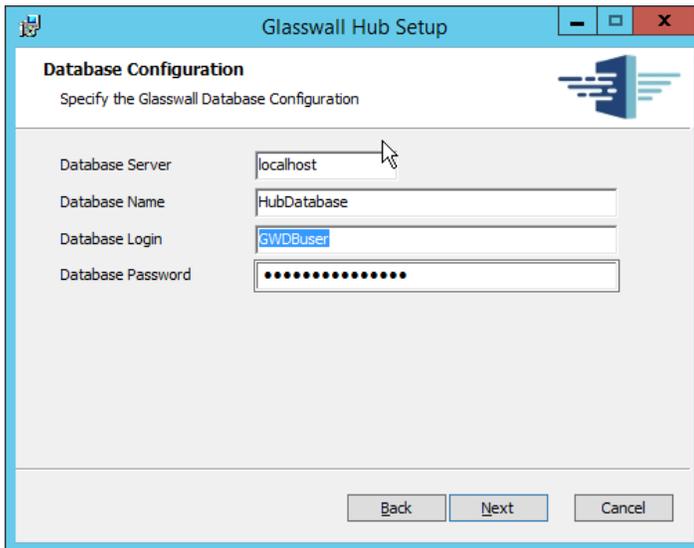
944  
945  
946

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



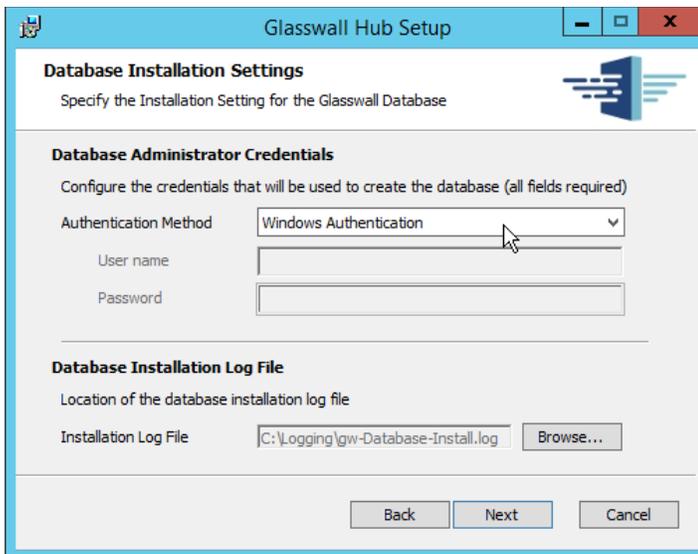
947  
948  
949  
950  
951

5. Click **Next.**
6. Enter **localhost** for the **Database Server.**
7. Enter **HubDatabase** for the **Database Name.**
8. Enter a **username** and **password** (and take note of these for later).



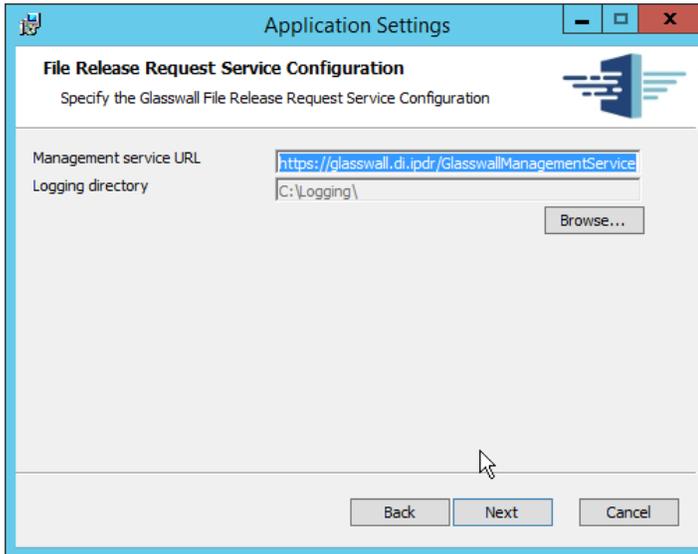
952  
953  
954

- 9. Click **Next**.
- 10. Select **Windows Authentication**.



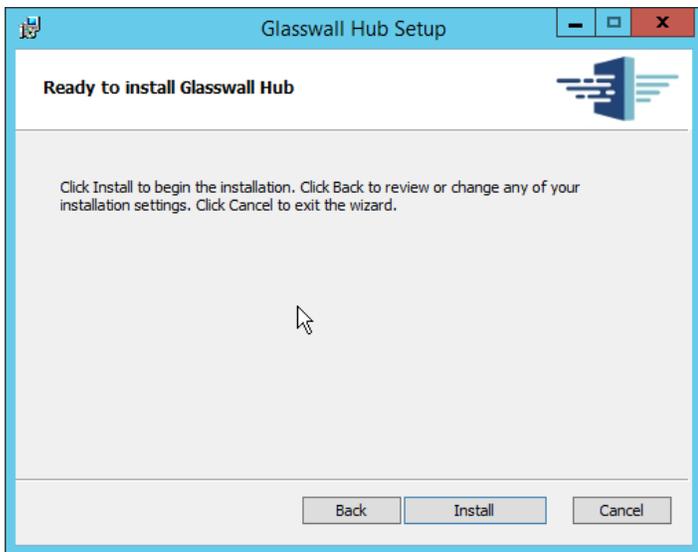
955  
956  
957  
958

- 11. Click **Next**.
- 12. Replace the domain of the **management service URL** with the address of the current machine, such as **glasswall.di.ipdr**.



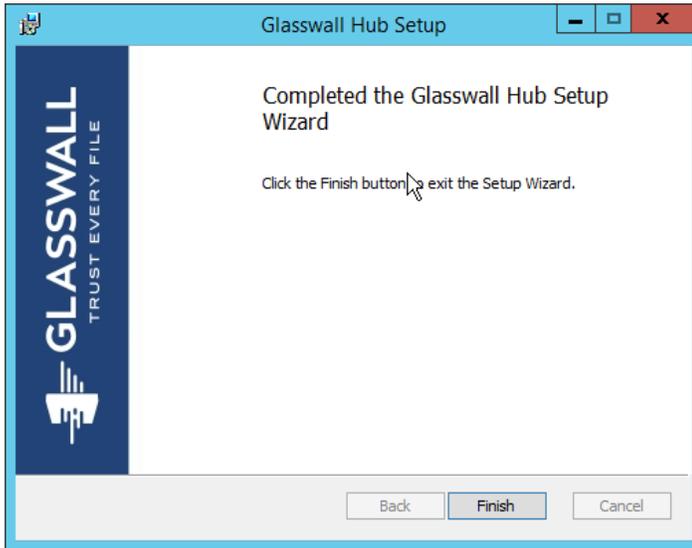
959  
960

13. Click **Next**.



961  
962

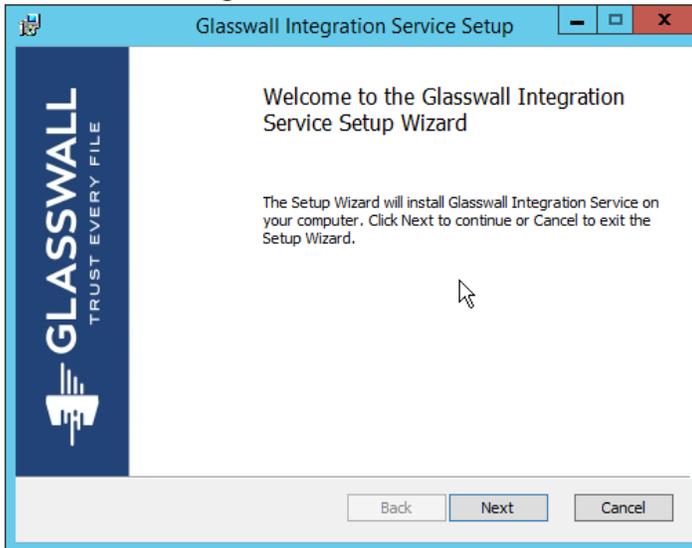
14. Click **Install**.



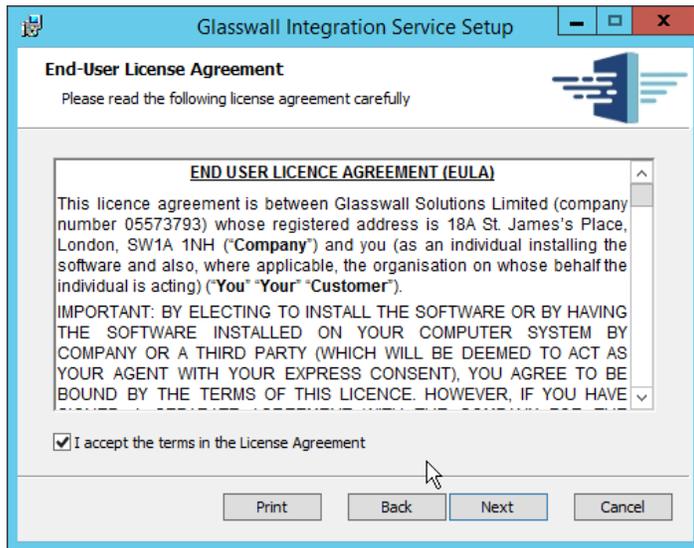
- 963
- 964 15. Click **Finish**.

### 965 2.7.2.2 *Install Glasswall Integration Service*

- 966 1. Run **GlasswallIntegrationService.msi**.

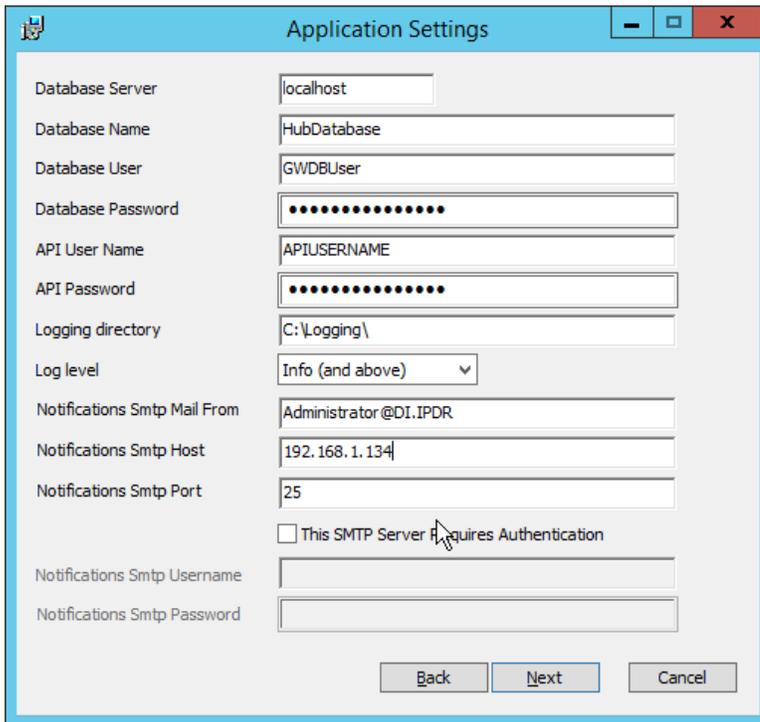


- 967
- 968 2. Click **Next**.
- 969 3. Check the box next to **I accept the terms in the License Agreement**.



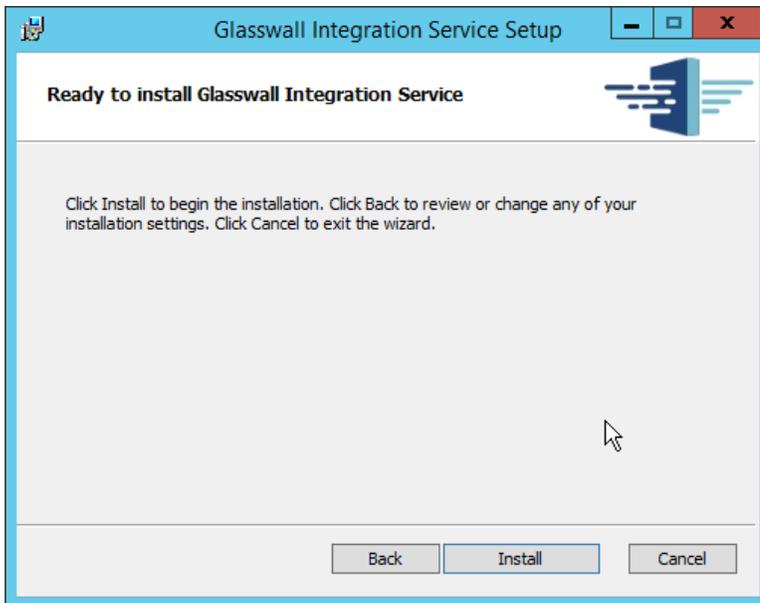
970  
971  
972  
973  
974  
975  
976  
977

4. Click **Next**.
5. For **Database Server, Database Name, Database User, and Database Password**, enter the information entered in the **Glasswall Hub Installer**.
6. Create a **username** and **password** for **API User Name** and **API Password**.
7. Enter an email address to be used for notifications in **Notifications Smtip Mail From**.
8. Enter the **address** for the mail server for **Notifications Smtip Host**.
9. Enter a **port (25 is used here)** for **Notifications Smtip Port**.



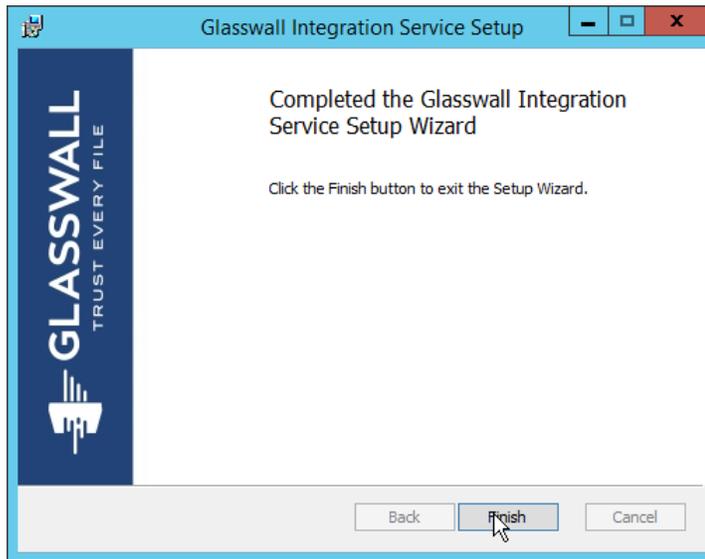
978  
979

10. Click **Next**.



980  
981

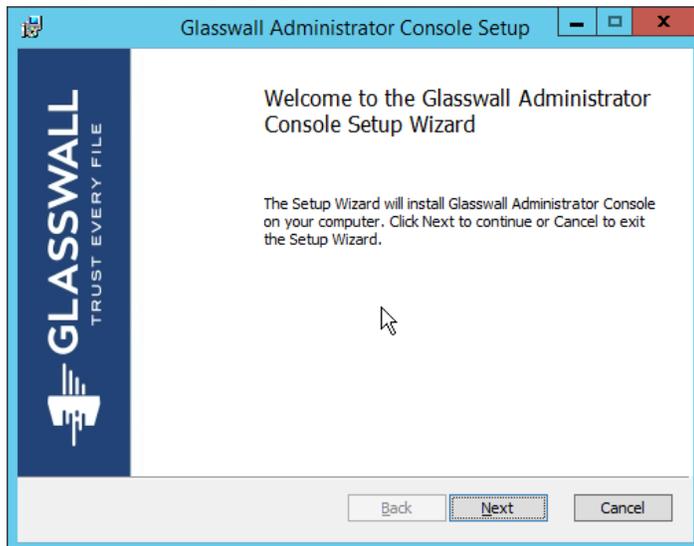
11. Click **Install**.



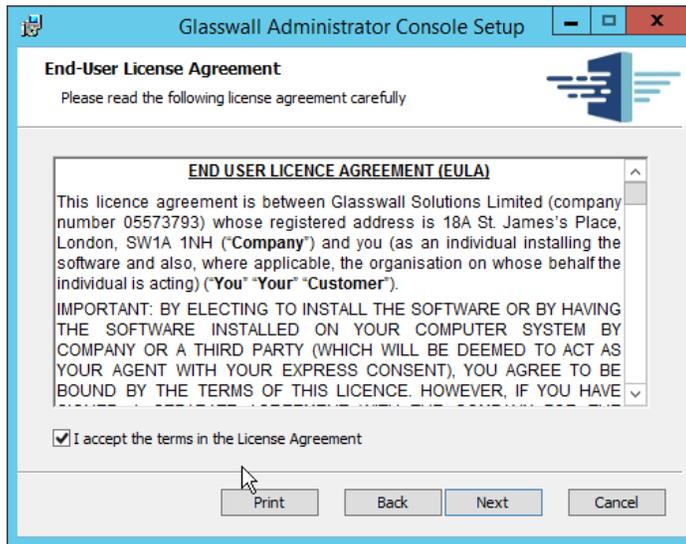
- 982  
983
12. Click **Finish**.

984 **2.7.2.3** *Install Glasswall Administrator Console*

- 985
1. Run **AdministratorConsoleInstaller.msi**.

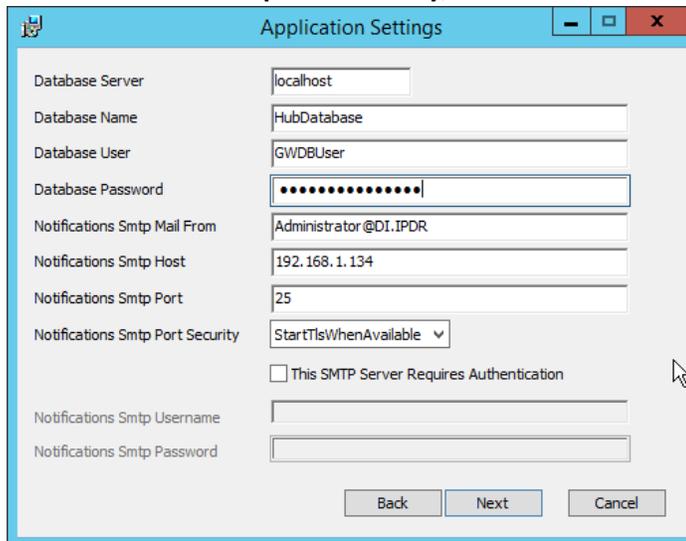


- 986  
987  
988
2. Click **Next**.
  3. Check the box next to **I accept the terms in the License Agreement**.



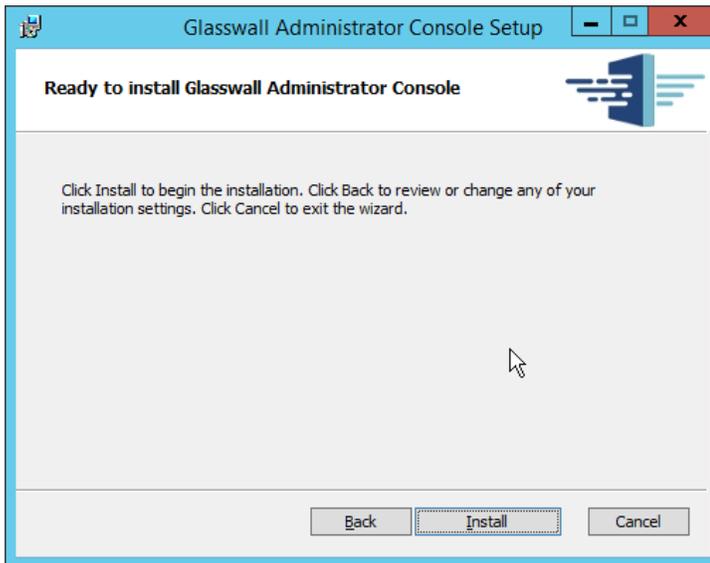
989  
990  
991  
992  
993  
994  
995

4. Click **Next**.
5. For **Database Server**, **Database Name**, **Database User**, and **Database Password**, enter the information entered in the **Glasswall Hub Installer**.
6. For **Notifications Smtplib Mail From**, **Notifications Smtplib Host**, **Notifications Smtplib Port**, enter the information entered in the **Glasswall Integration Service Installer**.
7. For **Notifications Smtplib Port Security**, select **StartTlsWhenAvailable**.



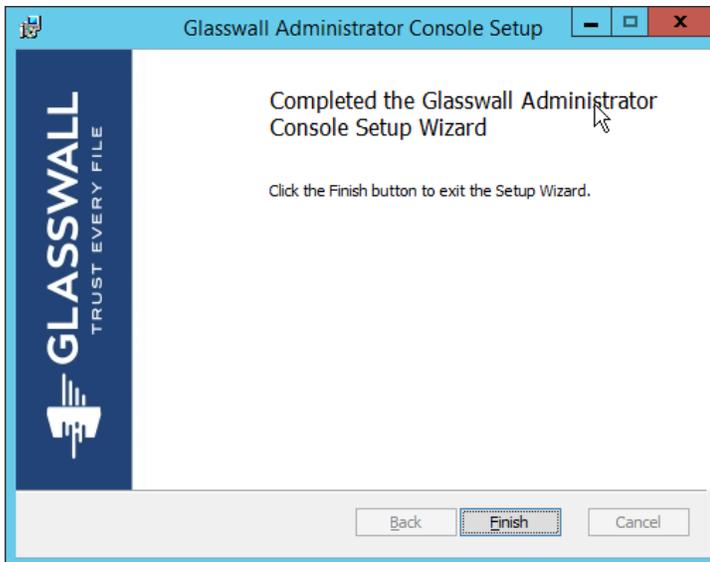
996  
997

8. Click **Next**.



998  
999

9. Click **Install**.



1000  
1001

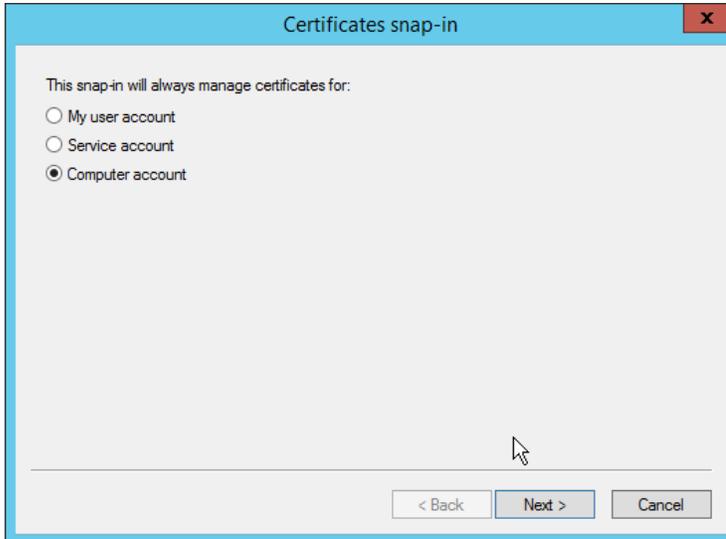
10. Click **Finish**.

1002 **2.7.2.4 Add the Server's Certificate**

- 1003 1. For the purposes of this build, a self-signed certificate is used, but this is dependent on the  
1004 needs of the organization. Ensure that the certificate used is issued to the domain, such as  
1005 **\*.di.ipdr**.  
1006 2. Open **mmc**.  
1007 3. Click **File > Add/Remove Snap-In....**  
1008 4. Select **Certificates** from the left pane, and click **Add**.

1009 5. Select **Computer Account**.

1010



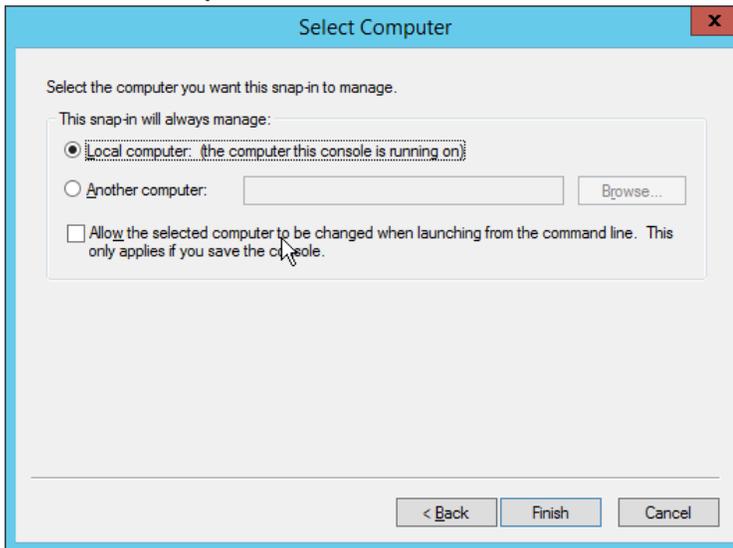
1011

6. Click **Next**.

1012

1013

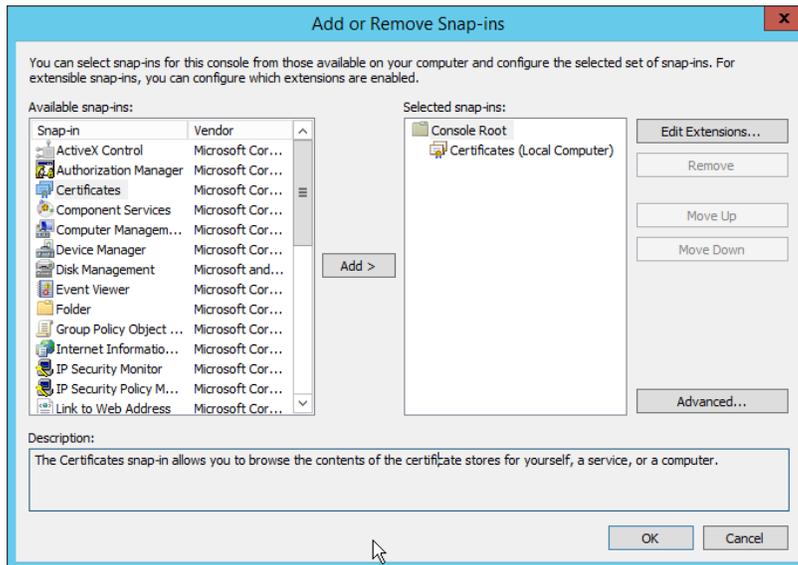
7. Select **Local computer**.



1014

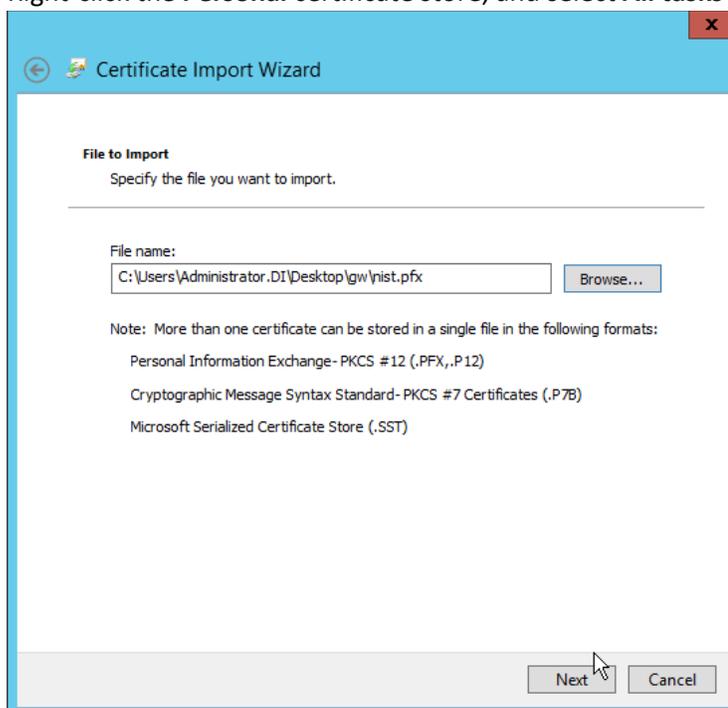
1015

8. Click **Finish**.



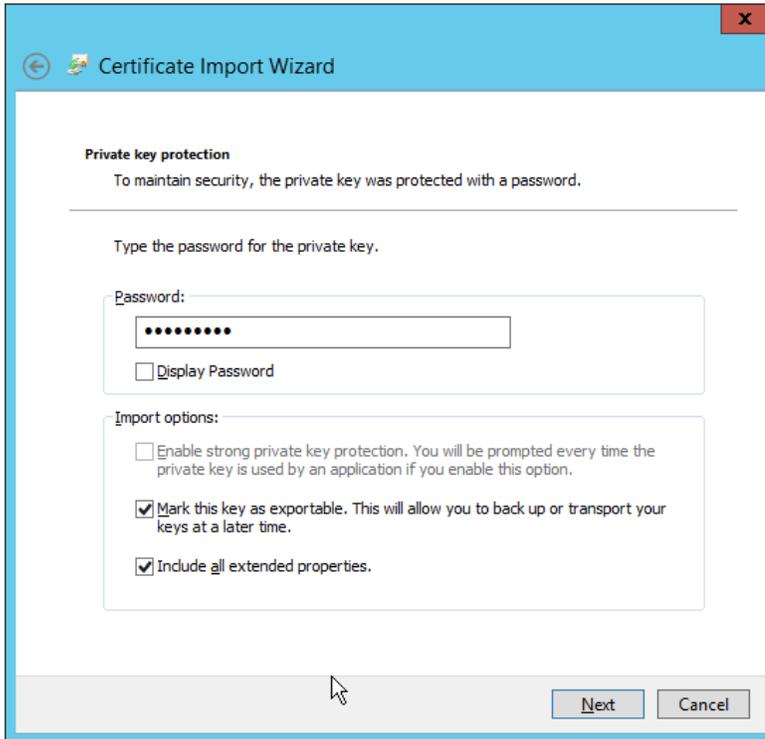
1016  
1017  
1018

9. Click **OK**.
10. Right-click the **Personal** certificate store, and select **All tasks > Import....**



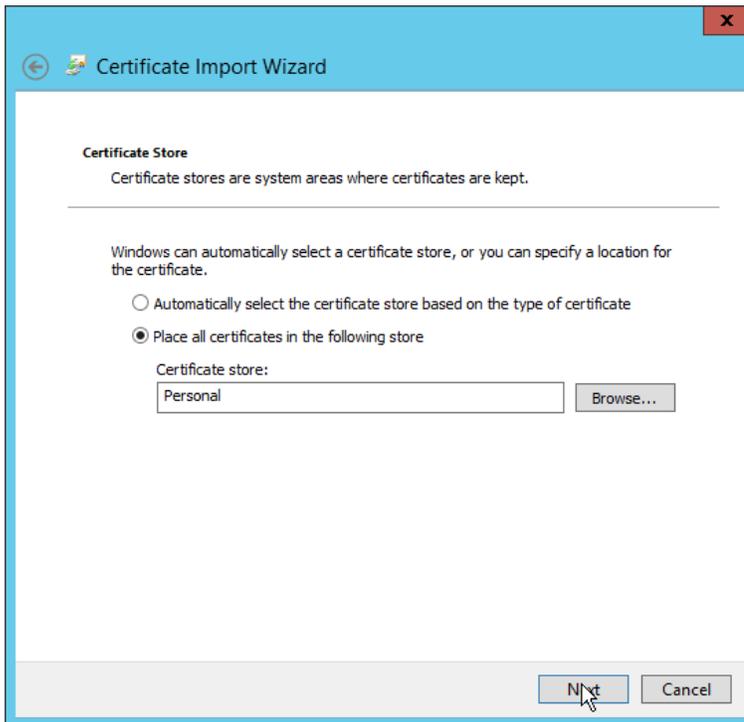
1019  
1020  
1021  
1022  
1023

11. Enter the **file name** of the certificate.
12. Click **Next**.
13. Enter the **password** for the certificate.
14. Check the box next to **Mark this key as exportable**.



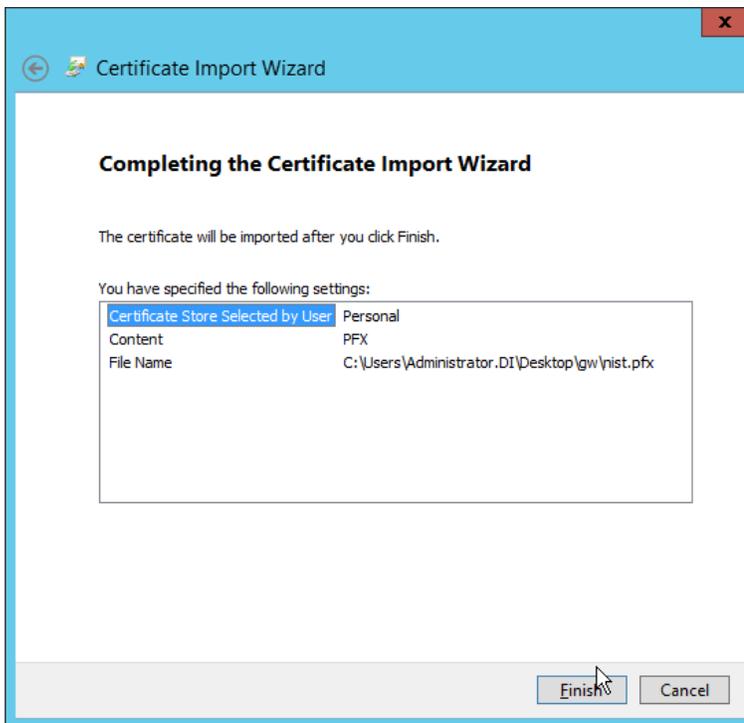
1024  
1025  
1026

15. Click **Next**.
16. Ensure that the **Certificate store** says **Personal**.



1027  
1028

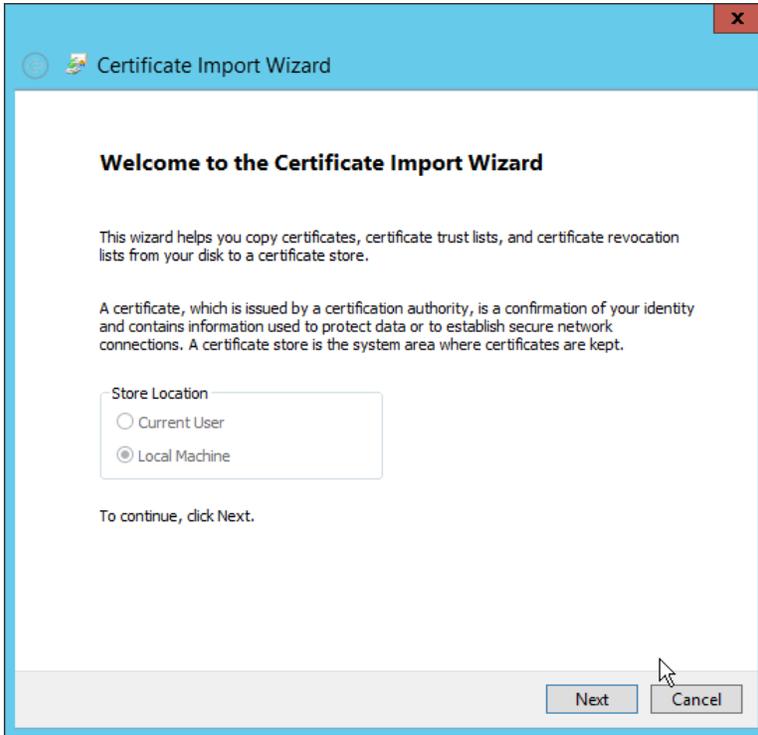
17. Click **Next**.



1029  
1030

18. Click **Finish**.

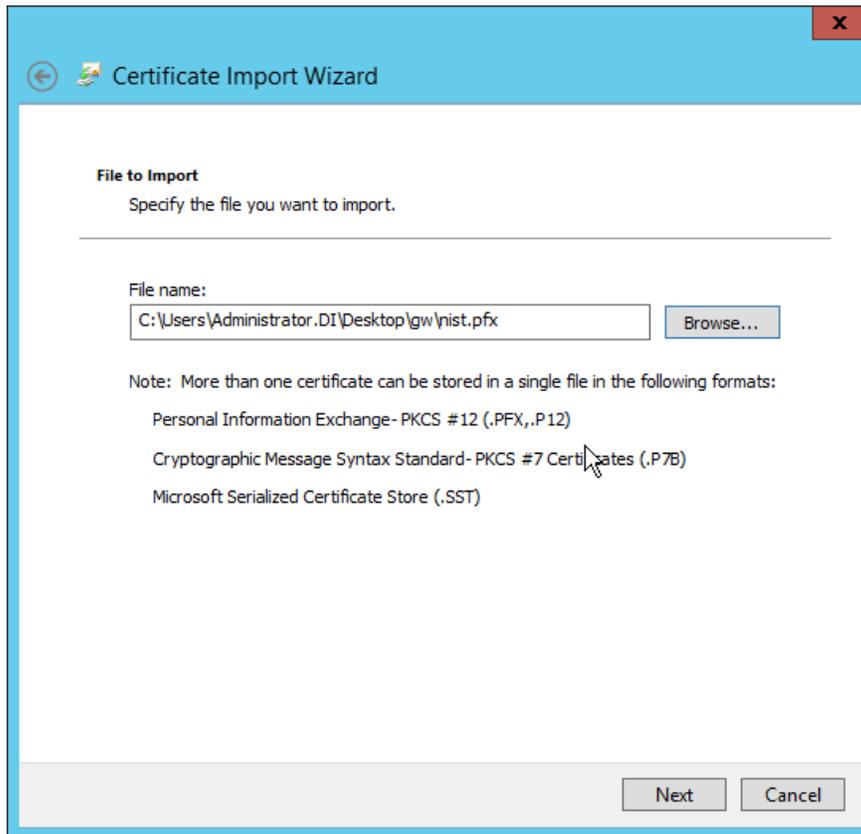
1031 19. Re-open the certificate import wizard but this time for **Trusted Root Certification Authorities**.



1032

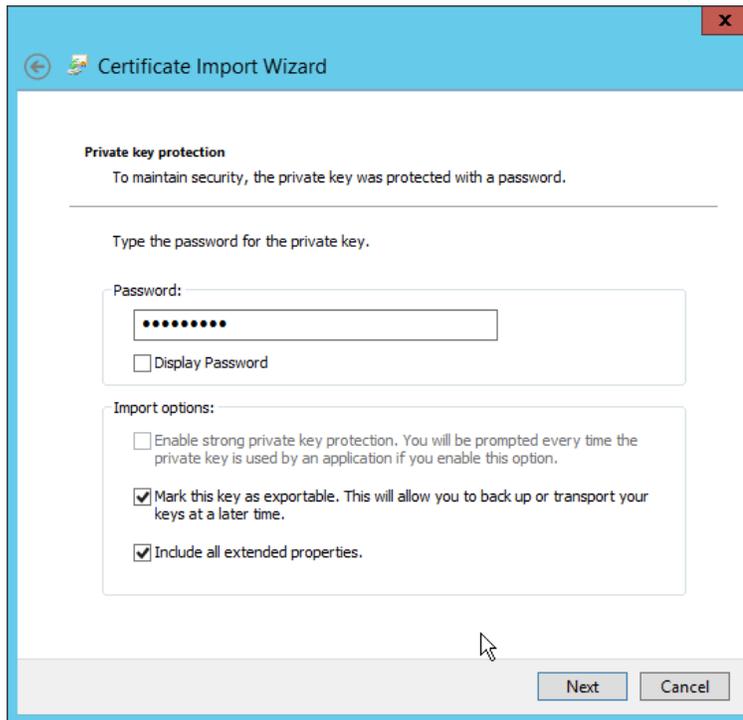
1033 20. Click **Next**.

1034 21. Select the same certificate.



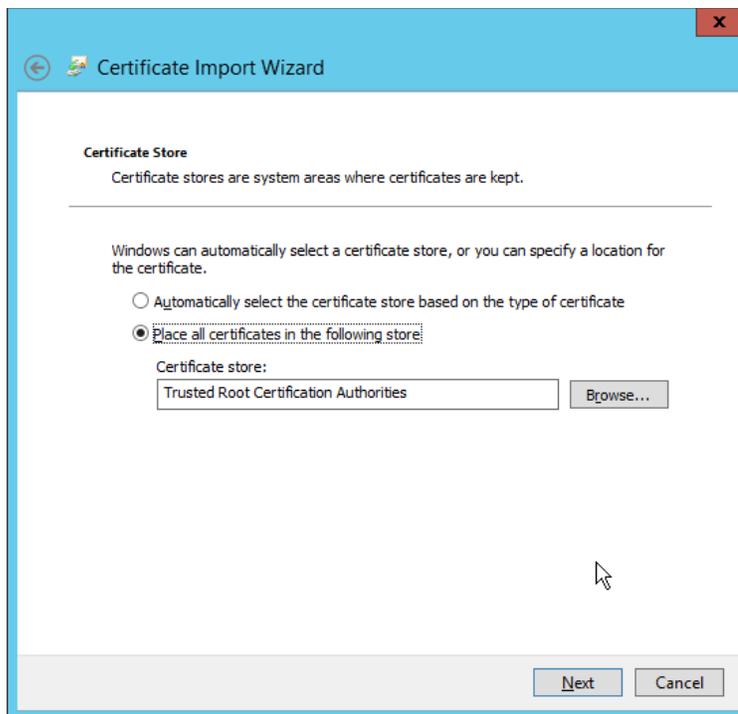
1035  
1036  
1037  
1038

22. Click **Next**.
23. Enter the certificate's **password**.
24. Check the box next to **Mark this key as exportable**.



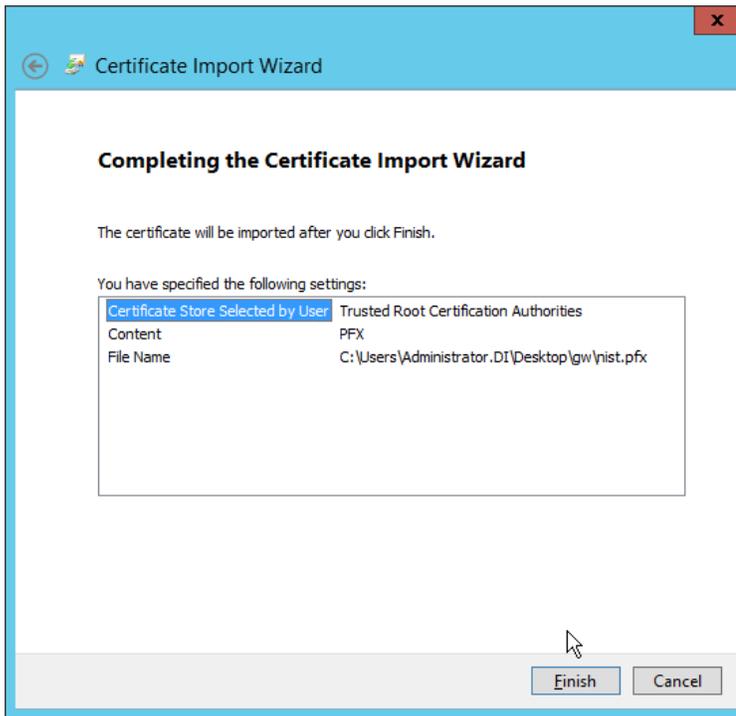
1039  
1040

25. Click **Next**.



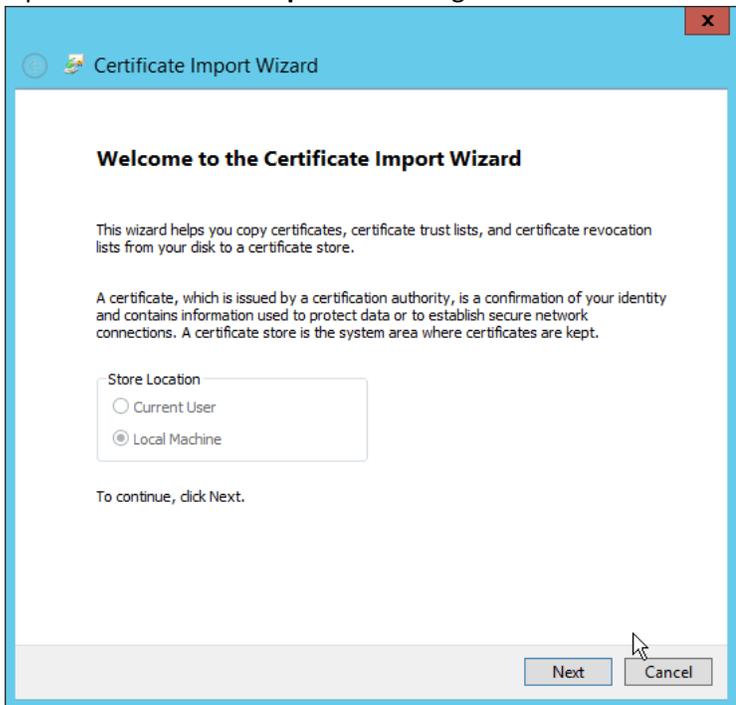
1041  
1042

26. Click **Next**.



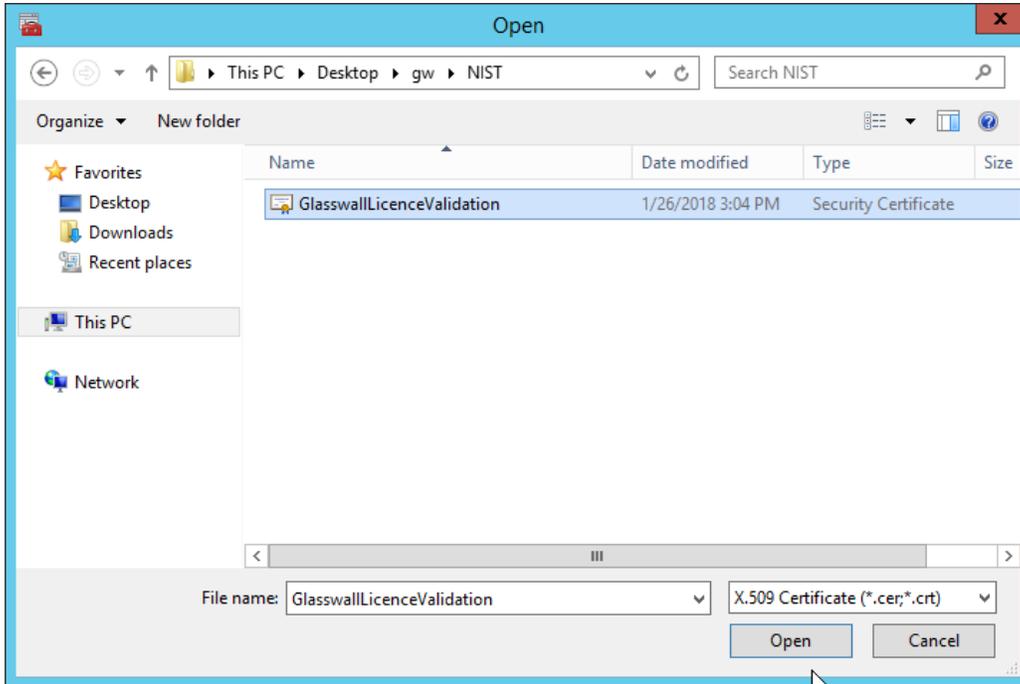
1043  
1044  
1045

- 27. Click **Finish**.
- 28. Open the **Certificate Import Wizard** again for the **Personal** store.

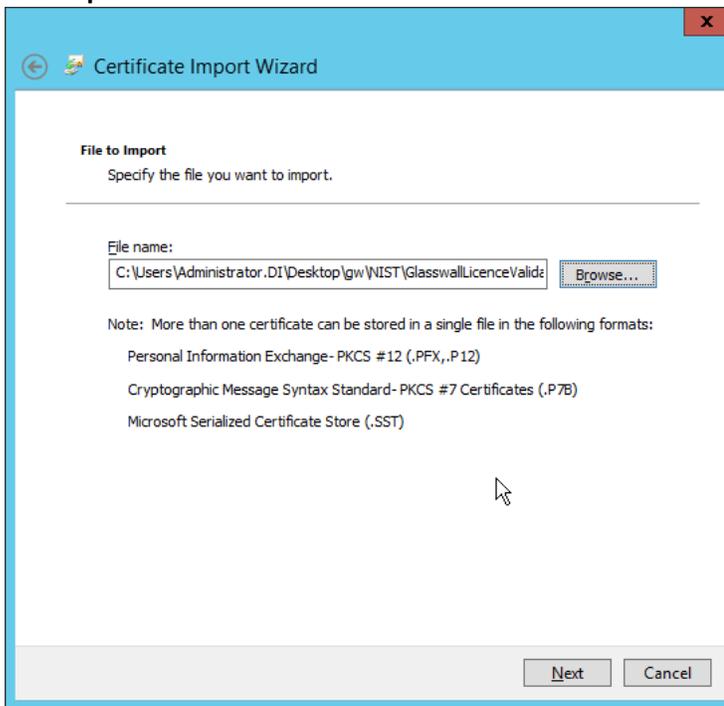


1046

- 1047 29. Click **Next**.
- 1048 30. Browse to the **GlasswallLicenceValidation** certificate.

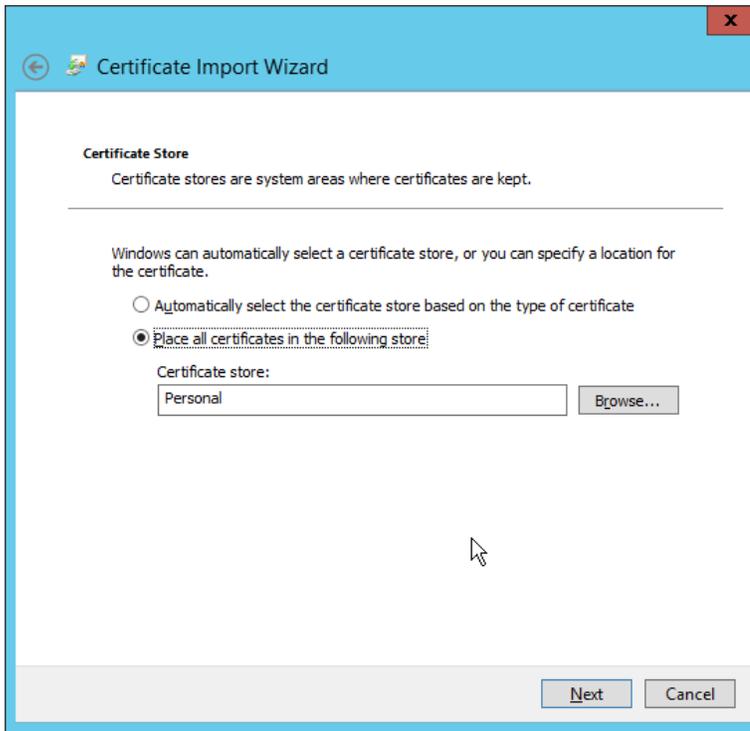


- 1049 31. Click **Open**.
- 1050

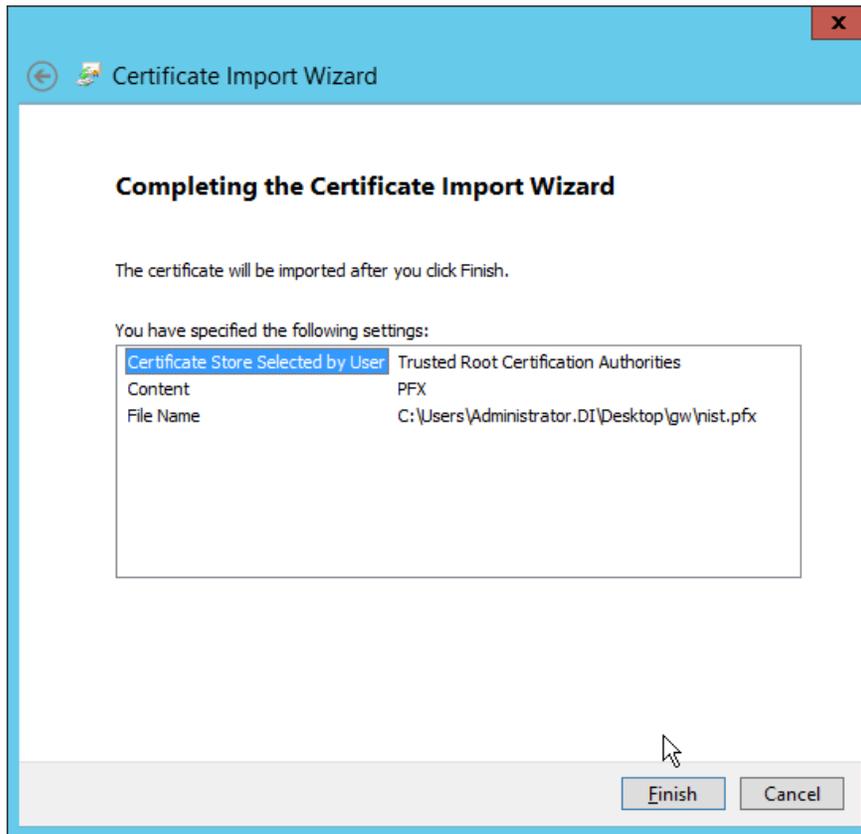


1051

1052 32. Click **Next**.

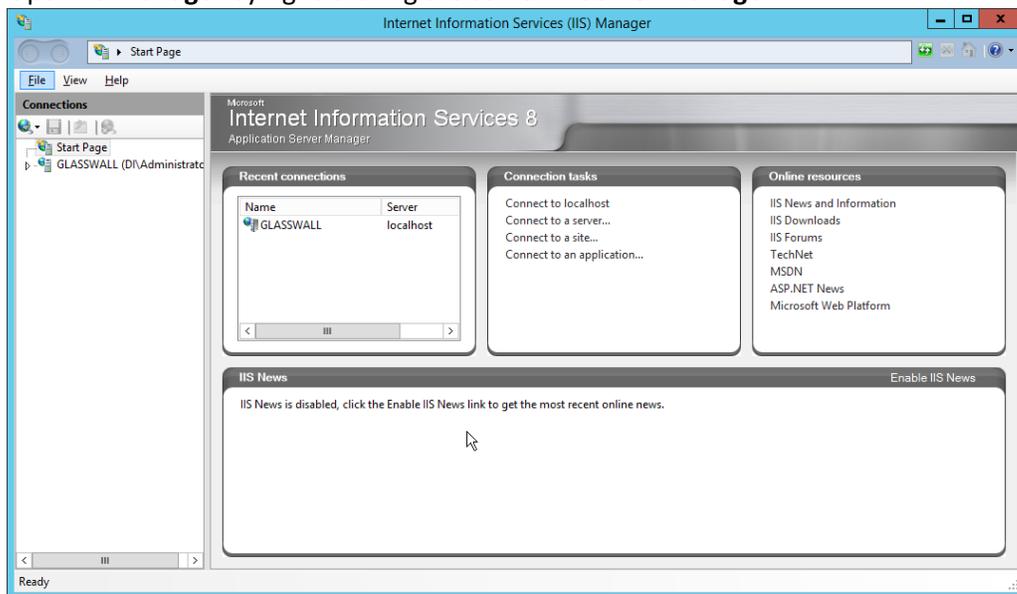


1053 33. Click **Next**.  
1054



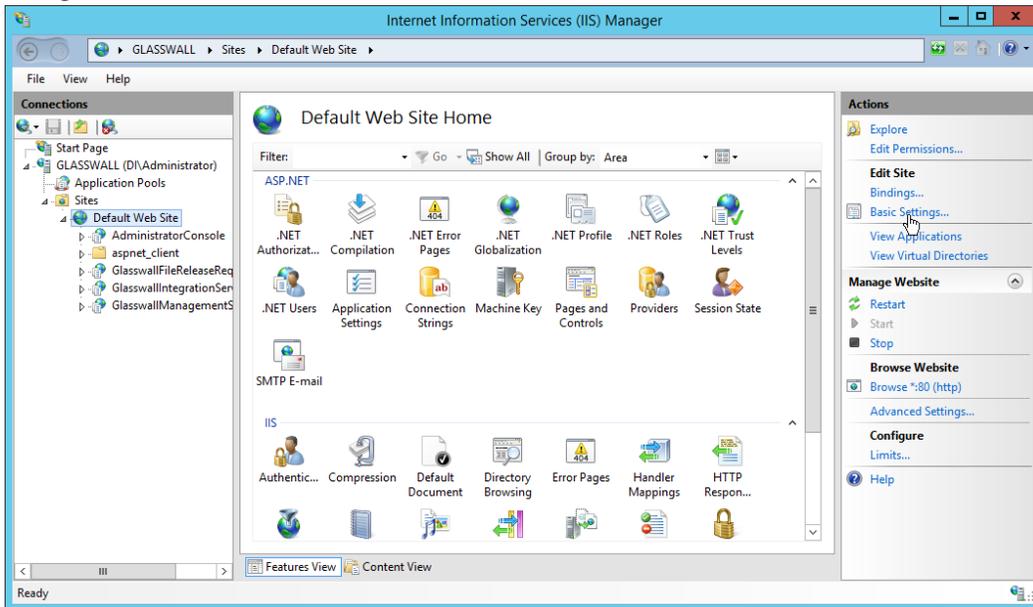
1055  
1056  
1057

- 34. Click **Finish**.
- 35. Open **IIS Manager** by right-clicking the server in **Server Manager**.

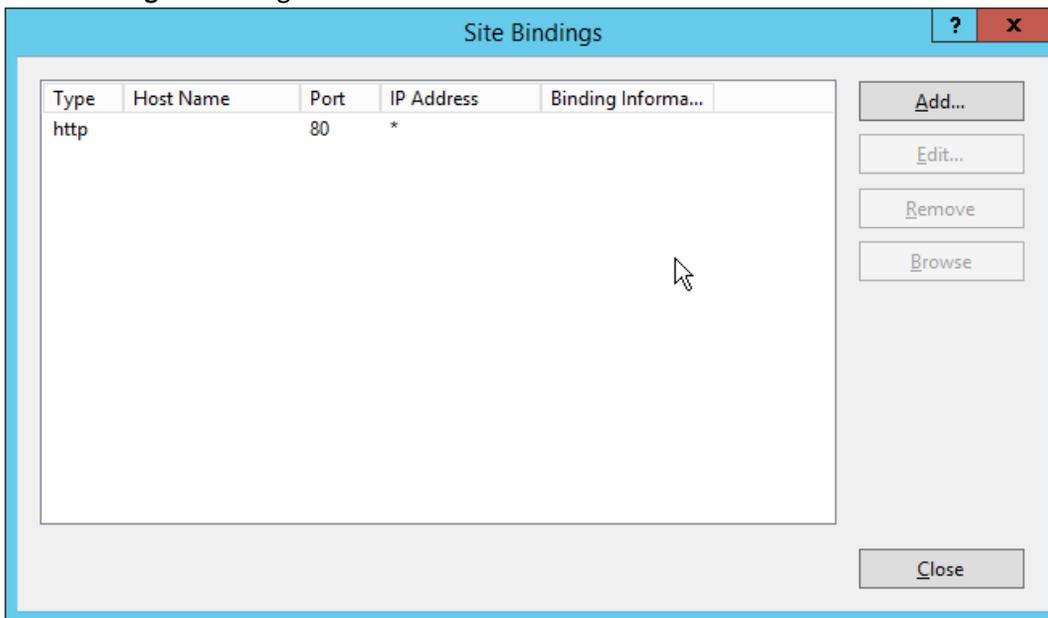


1058

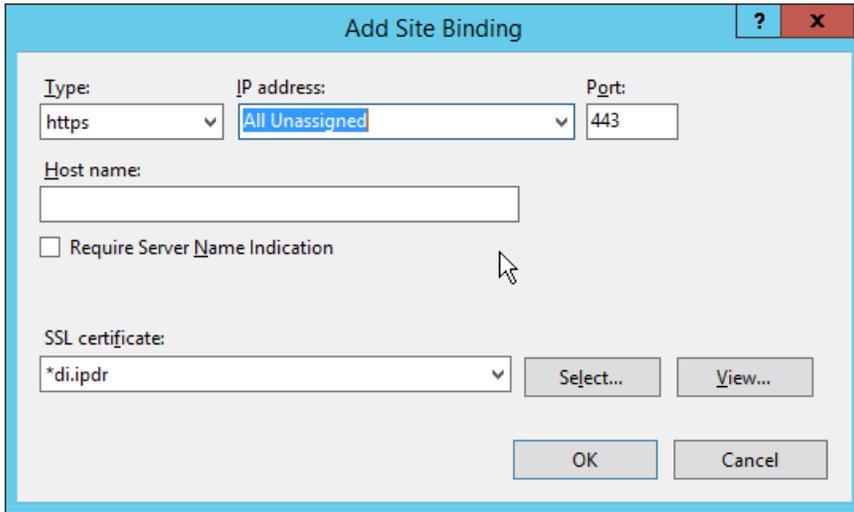
1059 36. Navigate to the **Default Website** in the tree.



1060  
1061 37. Click **Bindings** on the right sidebar.

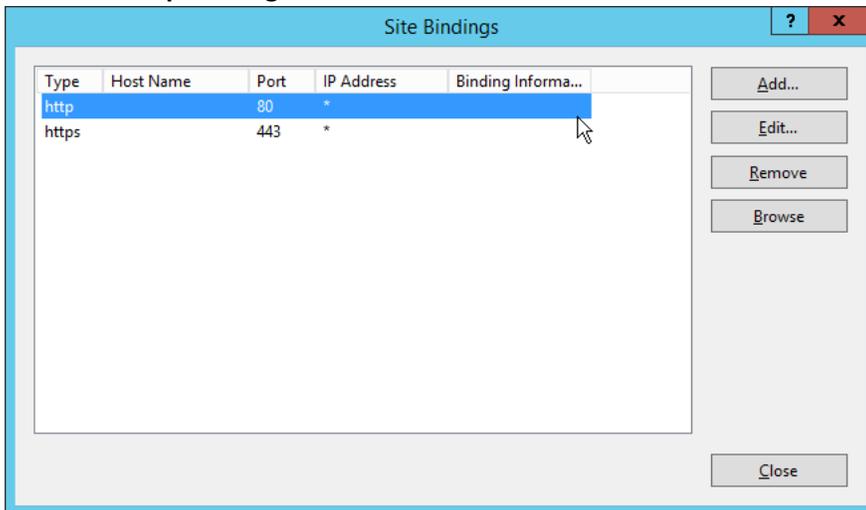


1062  
1063 38. Click **Add**.  
1064 39. Select **https** for the **Type**.  
1065 40. Select **All Unassigned** for **IP address**.  
1066 41. Select the **domain certificate** for **SSL certificate**.



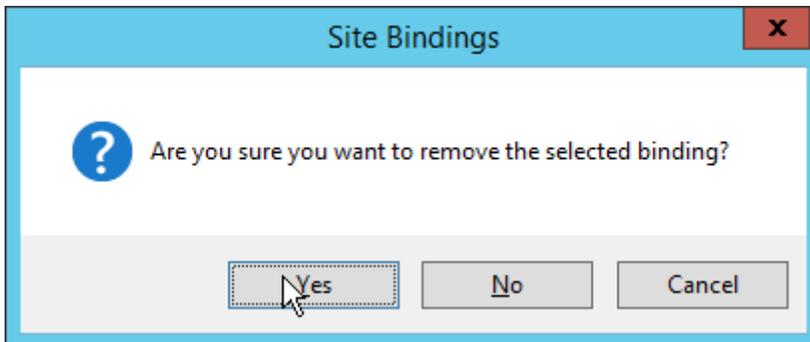
1067  
1068  
1069

- 42. Click **OK**.
- 43. Select the **http binding**.



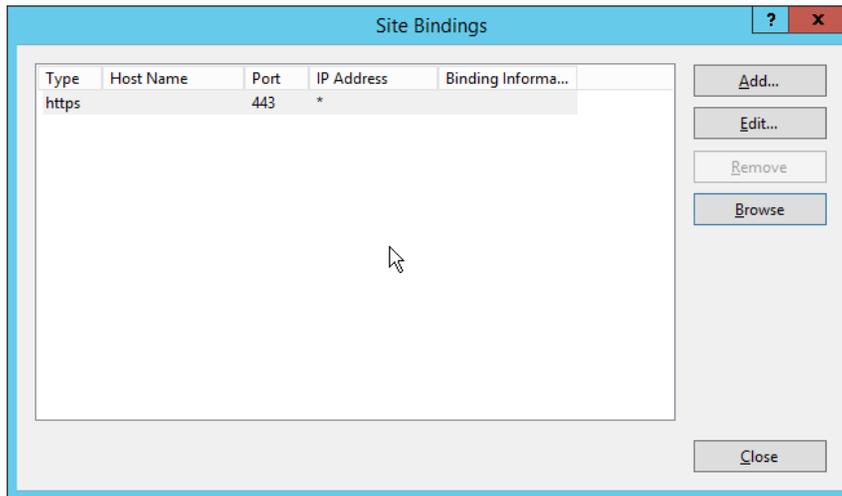
1070  
1071

- 44. Click **Remove**.



1072  
1073

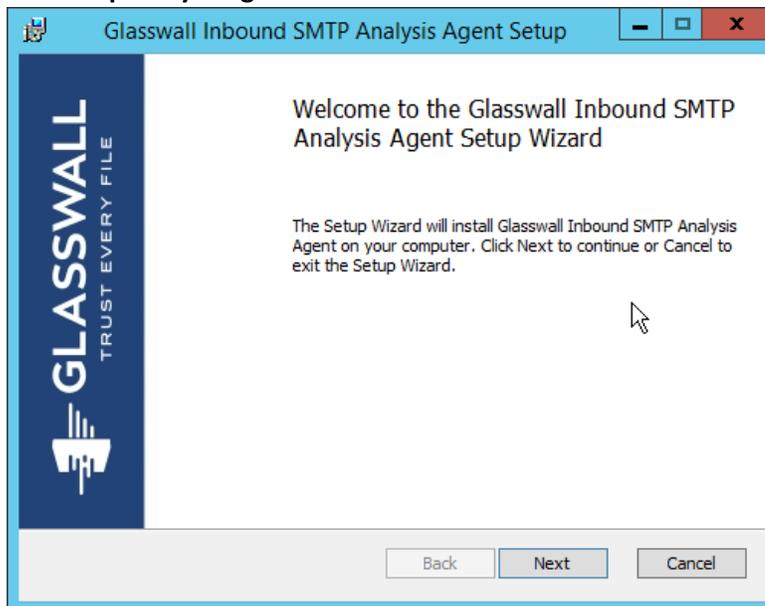
- 45. Click **Yes**.



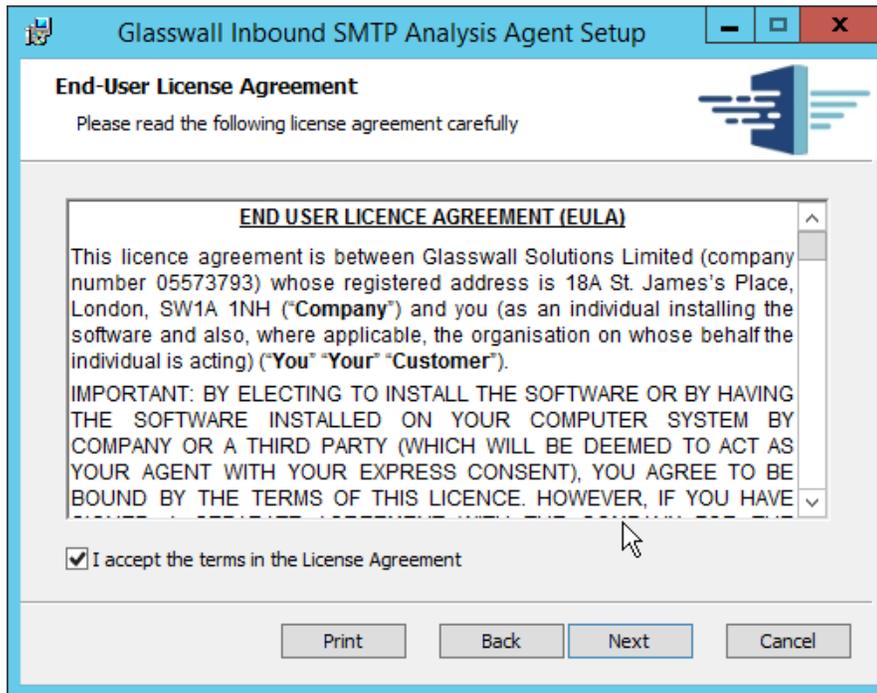
- 1074
- 1075 46. Click **Close**.
- 1076 47. Restart the IIS server. The Glasswall FileTrust console should now be accessible through a
- 1077 browser. (For example, <https://glasswall.di.ipdr/AdministratorConsole>). Ensure that there are
- 1078 no certificate errors.

1079 **2.7.2.5** *Install the Smtplib Analysis Agent*

- 1080 1. Run **SmtplibAnalysisAgentInstaller.msi**.

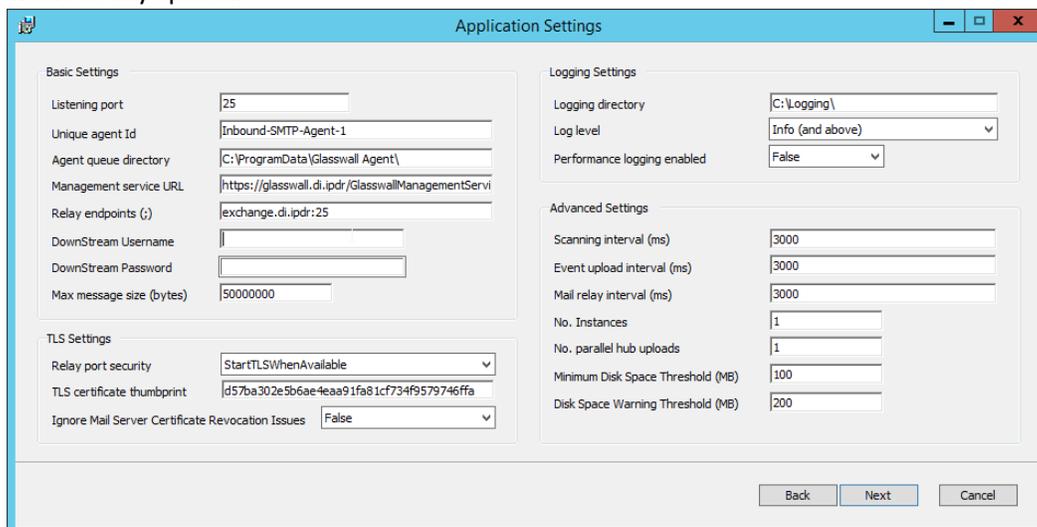


- 1081
- 1082 2. Click **Next**.
- 1083 3. Check the box next to **I accept the terms in the License Agreement**.



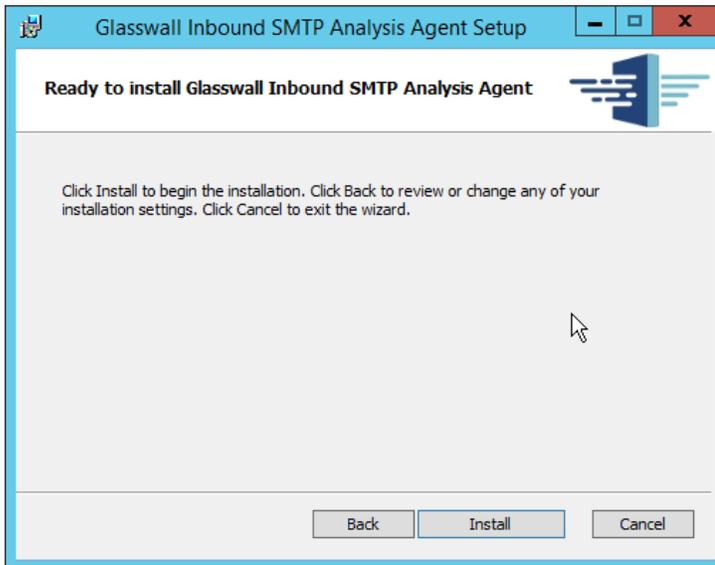
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092

4. Click **Next**.
5. For **Listening** port, enter **25**.
6. For **Management service URL**, correct the domain to be the web domain of the IIS server (for example, glasswall.di.ipdr).
7. For the **Relay endpoints**, enter the address of the Exchange server, followed by the port (for example, exchange.di.ipdr:25).
8. For the **TLS certificate thumbprint**, enter the value from the **thumbprint** field on the certificate, without any spaces.

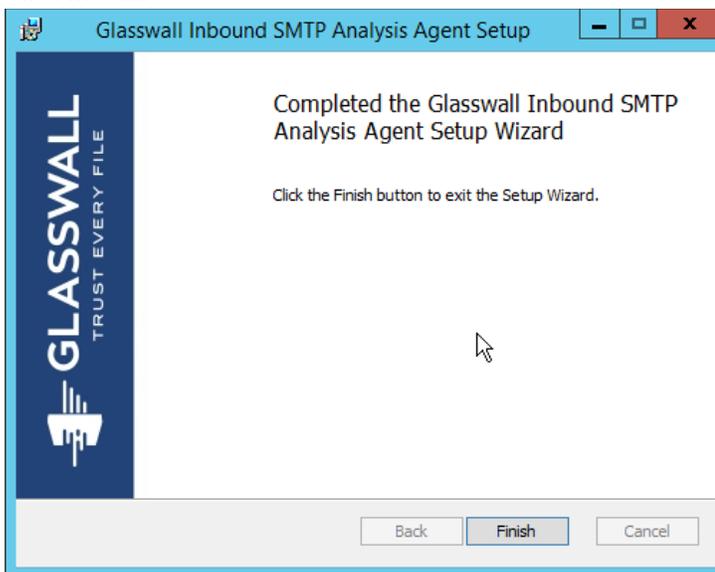


1093

1094 9. Click **Next**.



1095  
1096 10. Click **Install**.

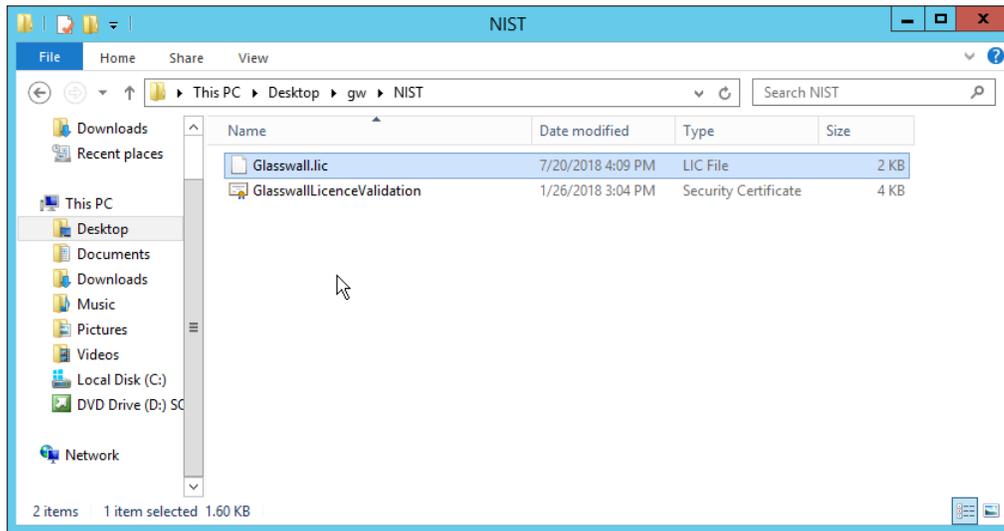


1097  
1098 11. Click **Finish**.

### 1099 2.7.2.6 *Distribute the Glasswall License File*

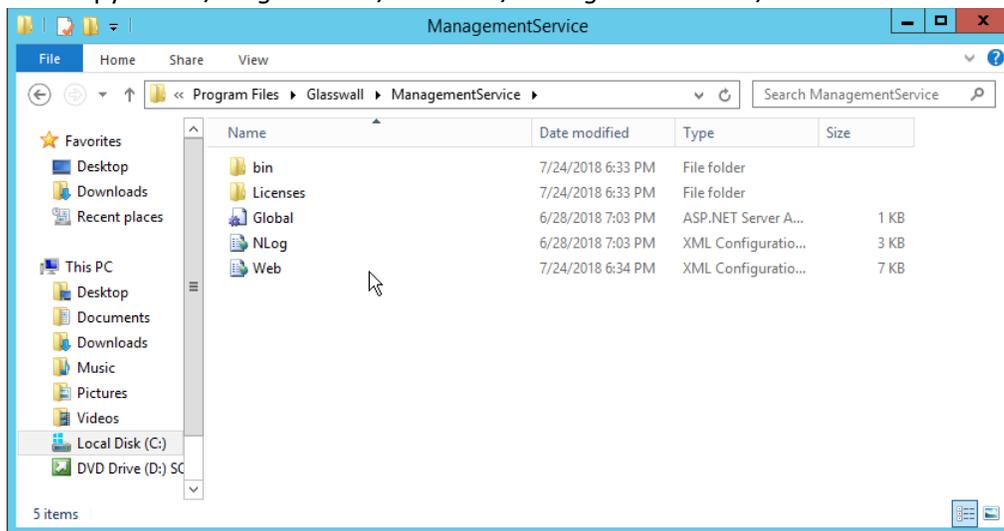
- 1100 1. Copy the **Glasswall License** file to the following locations, assuming **Glasswall** was installed to  
1101 *C:/Program Files/Glasswall*.

1102  
1103

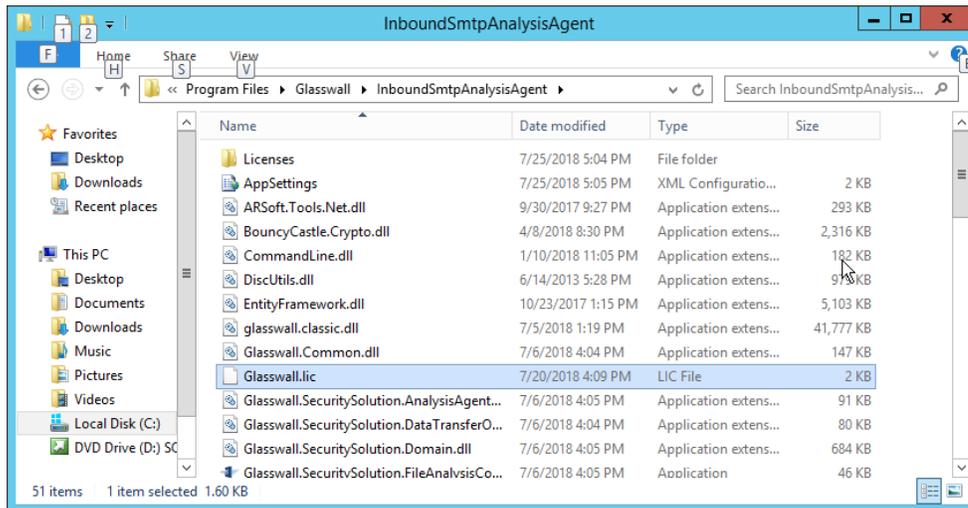


2. First copy it to *C:/Program Files/Glasswall/ManagementService/bin*.

1104  
1105

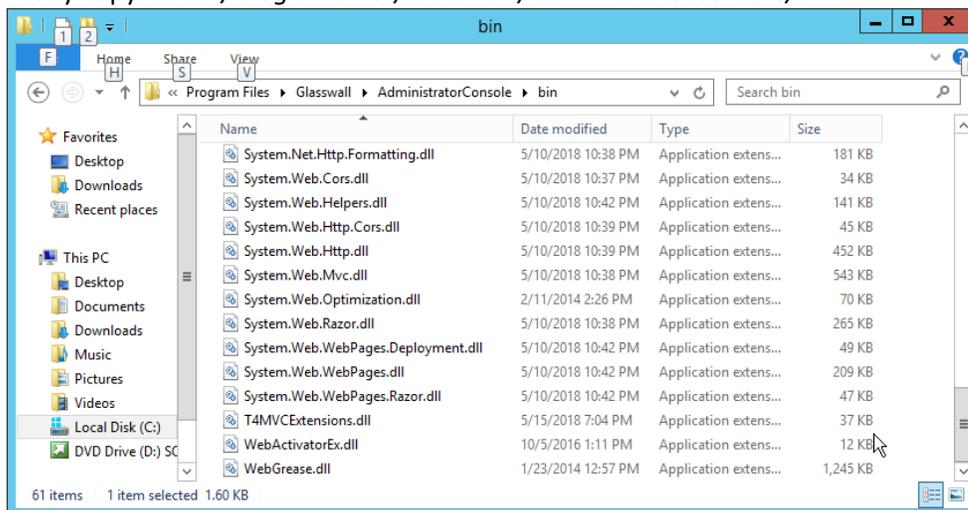


3. Then copy it to *C:/Program Files/Glasswall/InboundSntpAnalysisAgent*.



1106  
1107

4. Lastly copy it to `C:/Program Files/Glasswall/AdministratorConsole/bin`.



1108

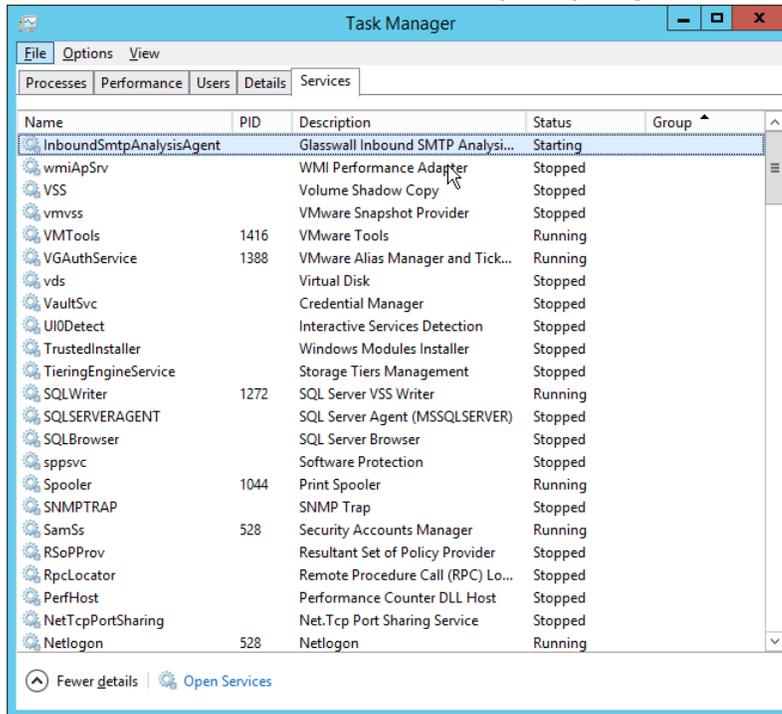
### 1109 2.7.3 Configure Glasswall FileTrust

1110 Please see <https://docs.glasswallsolutions.com/#Configuring/Office%20365%20Integration.htm> for an  
1111 example configuration that routes email with attachments from Office365 to Glasswall FileTrust.  
1112 Glasswall then forwards email back to Office365, after processing. Note that this linked configuration  
1113 does not work with on-premise Exchange setups.

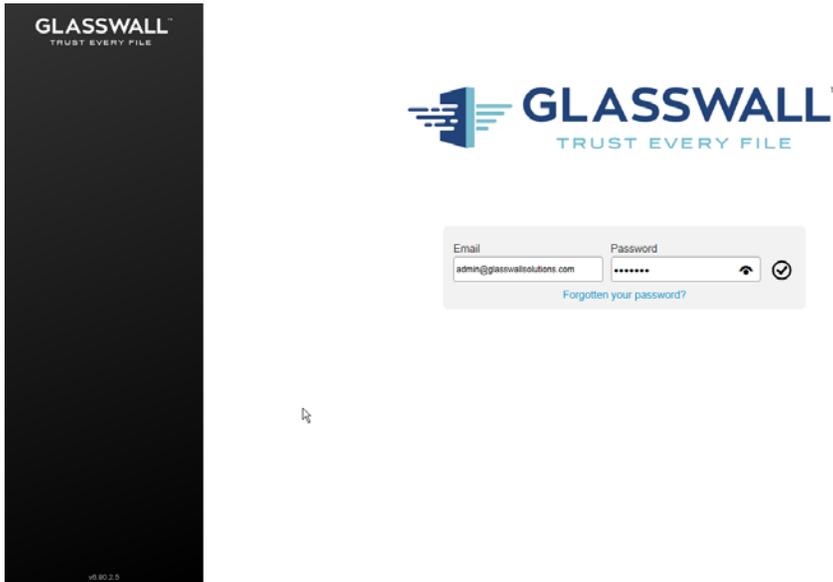
1114 Instead, to achieve the goal of routing email through Glasswall, we redirect local MX records to  
1115 Glasswall FileTrust. We implemented it this way because of limitations of the lab environment, but  
1116 organizations should consult with the vendor for the best solution to route email through the email  
1117 sanitization component, as other options may be available depending on the enterprise.

1118 2.7.3.1 *Create a New Administrator Account*

- 1119 1. Open **Task Manager**.
- 1120 2. In the **Services** tab, start the **InboundSmtpAnalysisAgent** service.

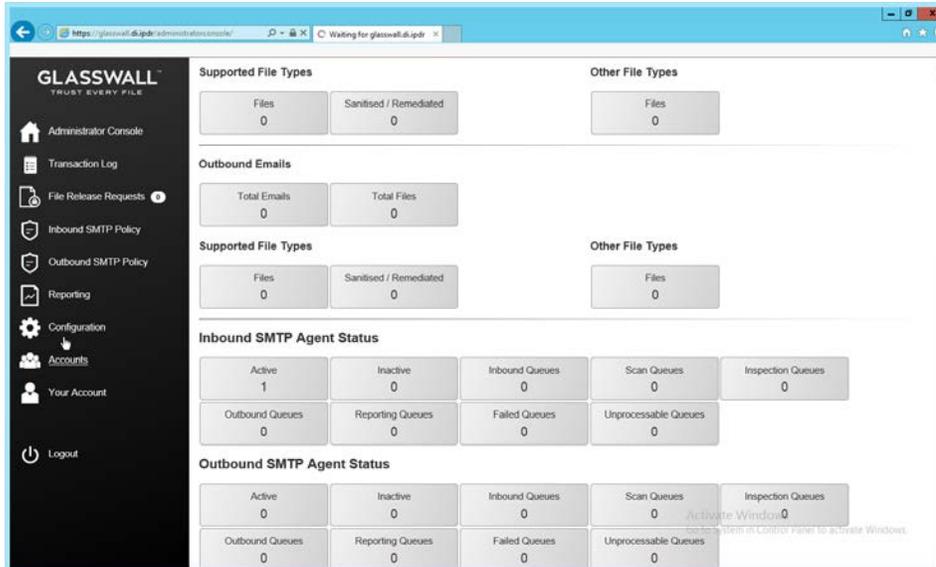


- 1121 3. Close **Task Manager**.
- 1122 4. Open a browser and navigate to the **Glasswall Administration Console** (for example,
- 1123 <http://glasswall.di.ipdr/AdministratorConsole>).
- 1124
- 1125 5. If this is the first time logging in, the default account will be **admin@glasswallsolutions.com**,
- 1126 and the password is **Welcome1?** .



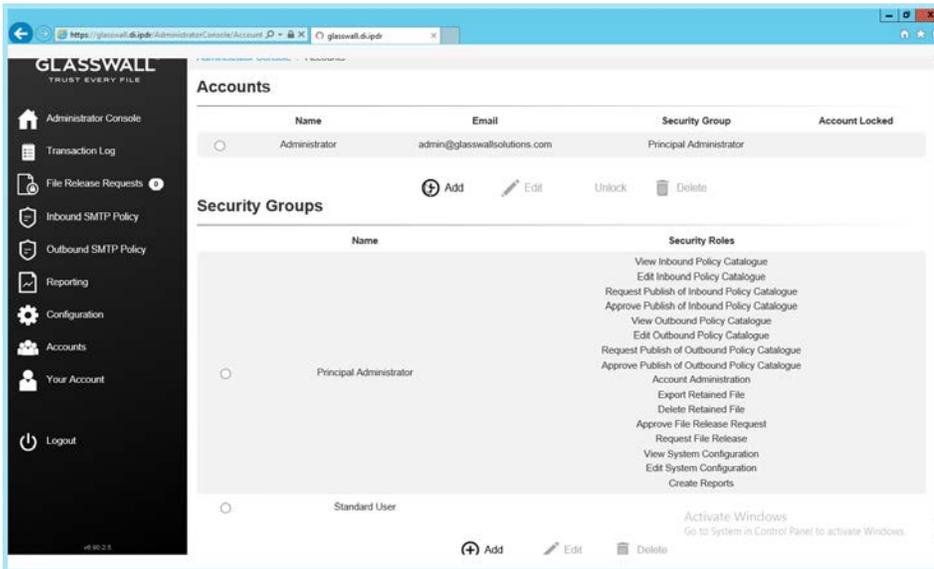
1127  
1128

6. Log in using these credentials.



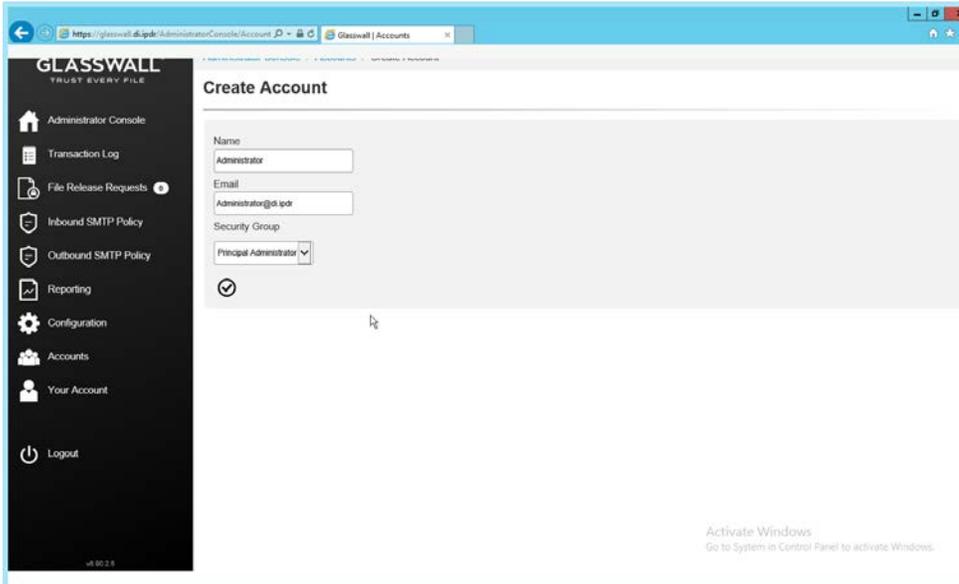
1129  
1130

7. On the left sidebar, click **Accounts**.



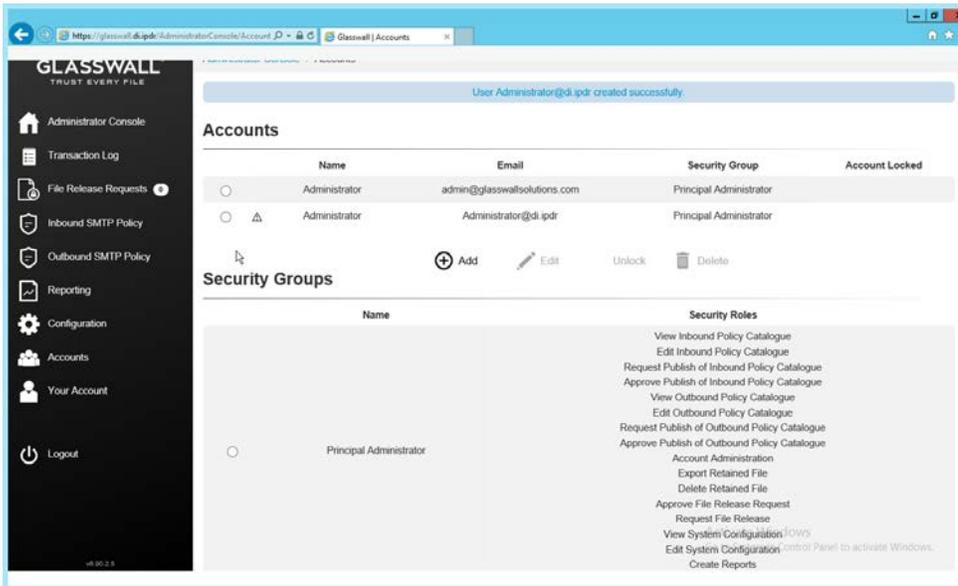
1131  
1132  
1133  
1134

8. Under **Accounts**, click **Add**.
9. Enter the **name** and **email address** of an administrator account from the email server.
10. Select **Principal Administrator** for **Security Group**.



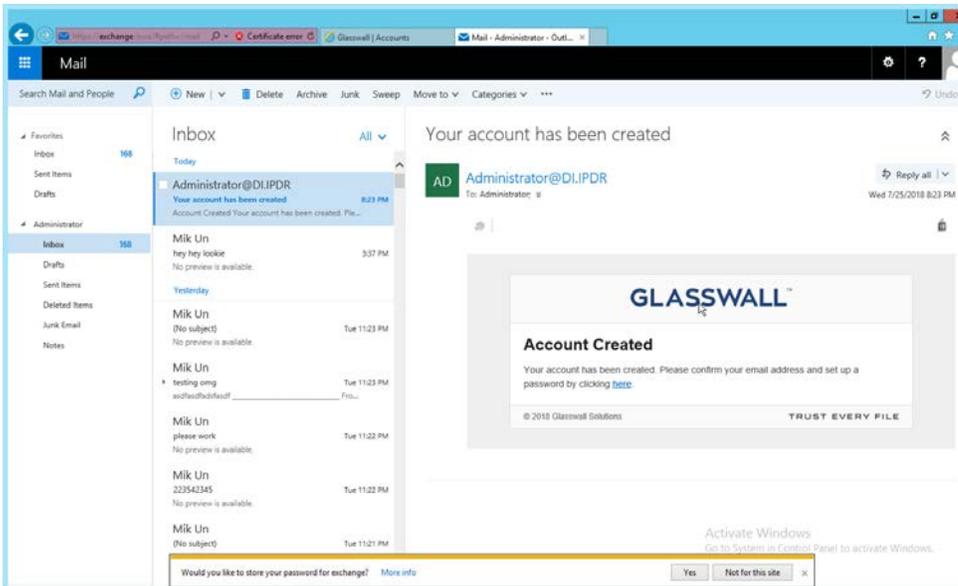
1135  
1136

11. Click the **checkmark** button when finished.



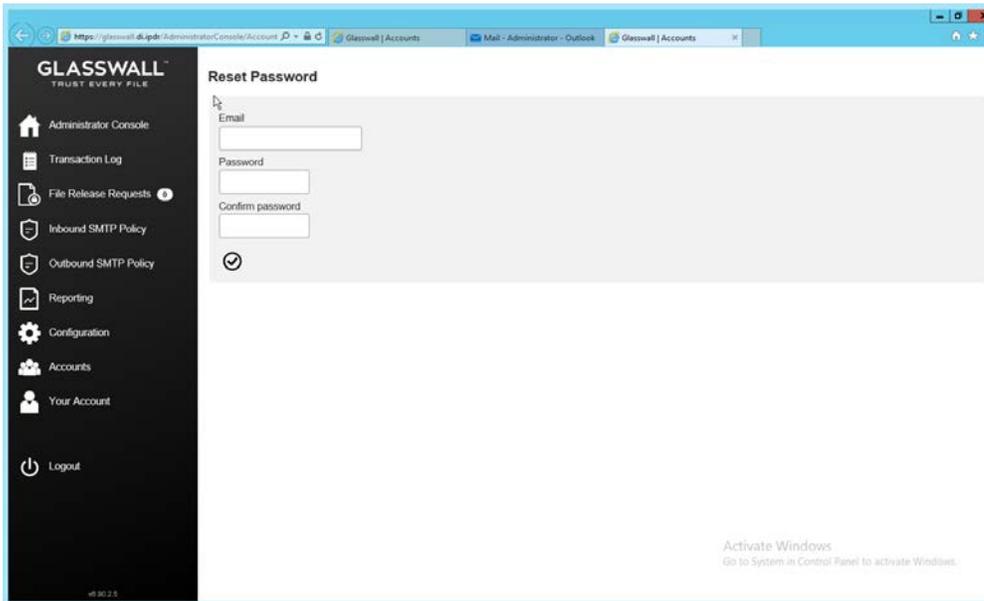
1137  
1138

12. The new administrator account should be created.



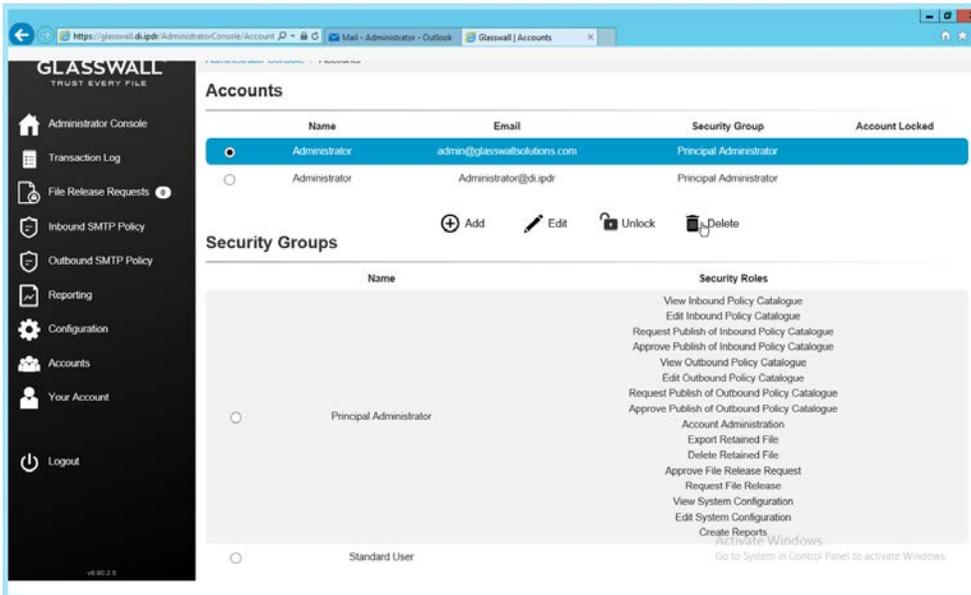
1139  
1140  
1141

13. Check the email inbox of the specified email address for a confirmation email, and click the link in the email.



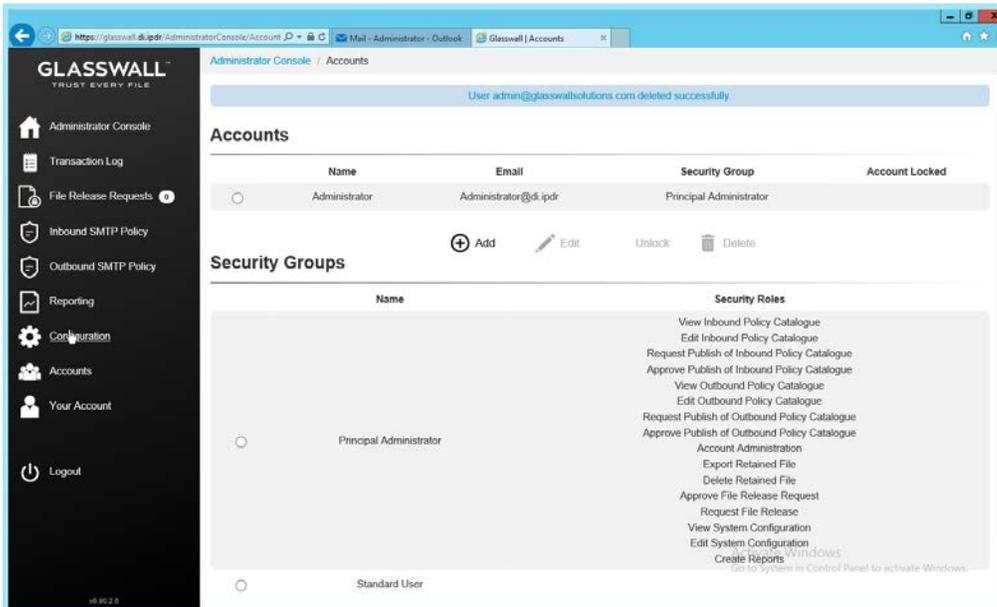
1142  
1143  
1144  
1145

14. Enter the email address as well as a password for this account.
15. Log in as this user, and then go to **Accounts**.
16. Select the old (default) Administrator account.



1146  
1147

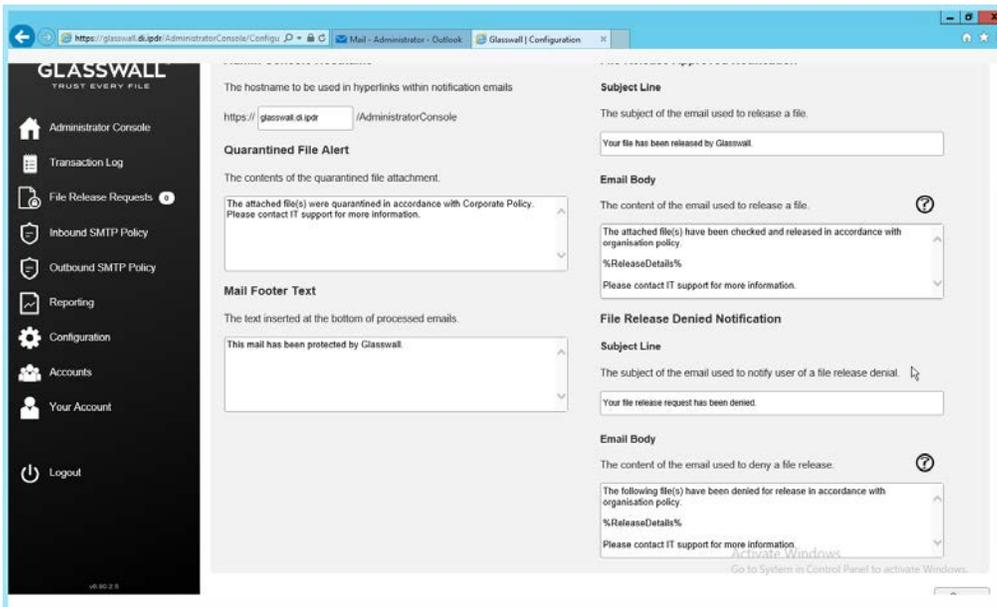
17. Click **Delete**.



- 1148  
 1149 18. This should remove the old administrator account (note: failure to remove this can result in a  
 1150 significant vulnerability for this server).

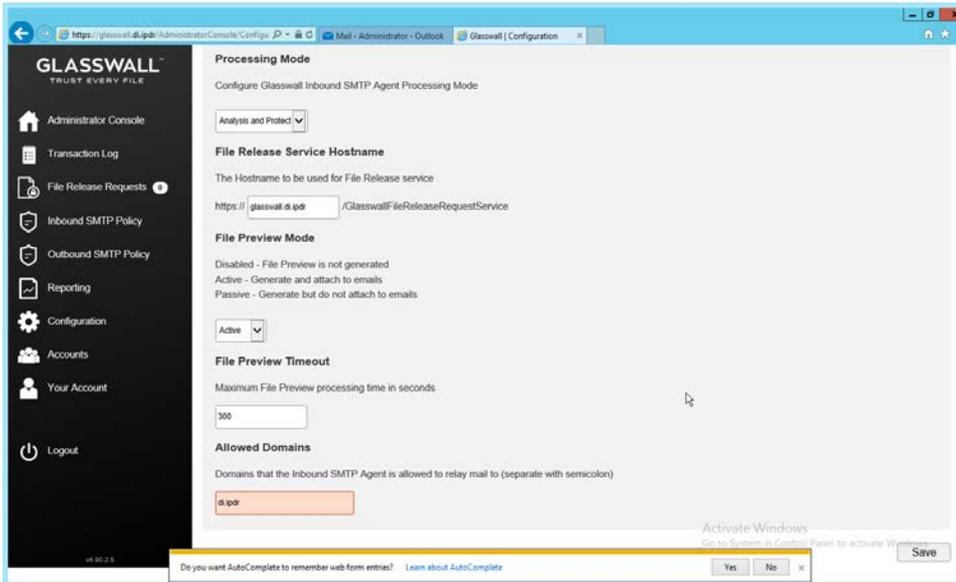
1151 **2.7.3.2 Configure Notifications and Policies**

- 1152 1. Click **Configuration** on the left sidebar.  
 1153 2. Click the **Notifications** tab.



- 1154  
 1155 3. On this page, enter the web domain in the first input box (for example, glasswall.di.ipdr).

- 1156 4. The various input boxes on this page allow you to specify the messages sent when files are  
 1157 quarantined, released, or prevented from being released.  
 1158 5. Click the **Inbound Agents** tab.  
 1159 6. Select **Analysis and Protect** for **Processing Mode**. (This analyzes and quarantines/reconstructs  
 1160 files based on policy.)  
 1161 7. Select **Active** for **File Preview Mode**. (This provides clients with a preview of their received files  
 1162 if they were quarantined, so they can determine whether they should request the file be  
 1163 released.)  
 1164 8. Enter the **domain** for **Allowed Domains** (for example, di.ipdr).



- 1165 9. Click **Save**.  
 1166

### 1167 2.7.3.3 *Configure Inbound SMTP Policy*

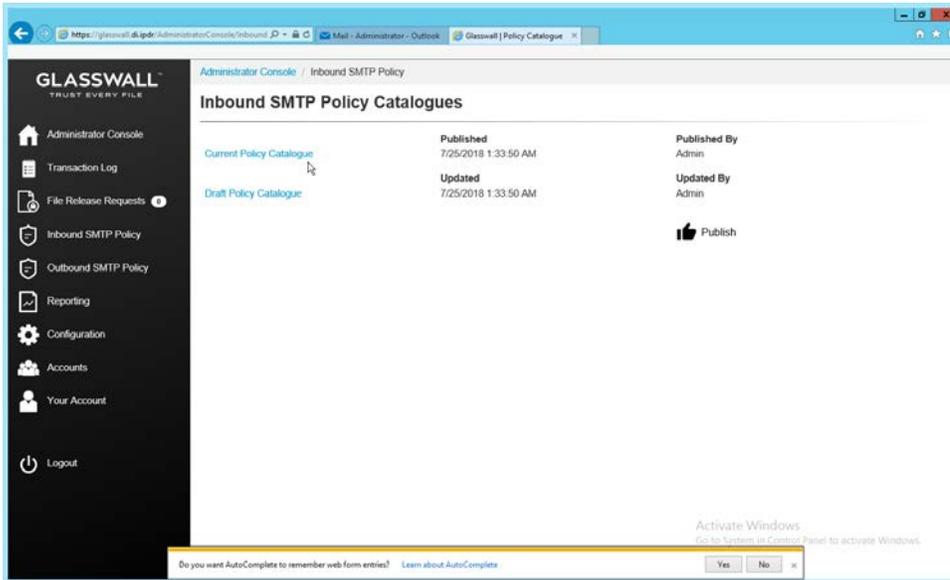
1168 This section discusses SMTP policy under Glasswall FileTrust. There are several layers of granularity for  
 1169 configuring Email policy. Because policy is dependent on the organization's needs, we will not prescribe  
 1170 a policy but will showcase how a policy is formed.

1171 Policy in Glasswall FileTrust consists of **Sender Groups**, **Receiver Groups**, **Content Management**  
 1172 **Policies**, and **ThreatCensor Policy Sets**. **Receiver groups** allow for the specification of users who receive  
 1173 email. **Sender groups** allow for the specification of emails received from specific senders. **Content**  
 1174 **Management Policies** refer to the default policy on various filetypes. Lastly, **ThreatCensor Policy Sets**  
 1175 allow for the specification of policy on specific error codes; through this it is possible to place policies on  
 1176 encrypted email, for example, depending on the organization's needs.

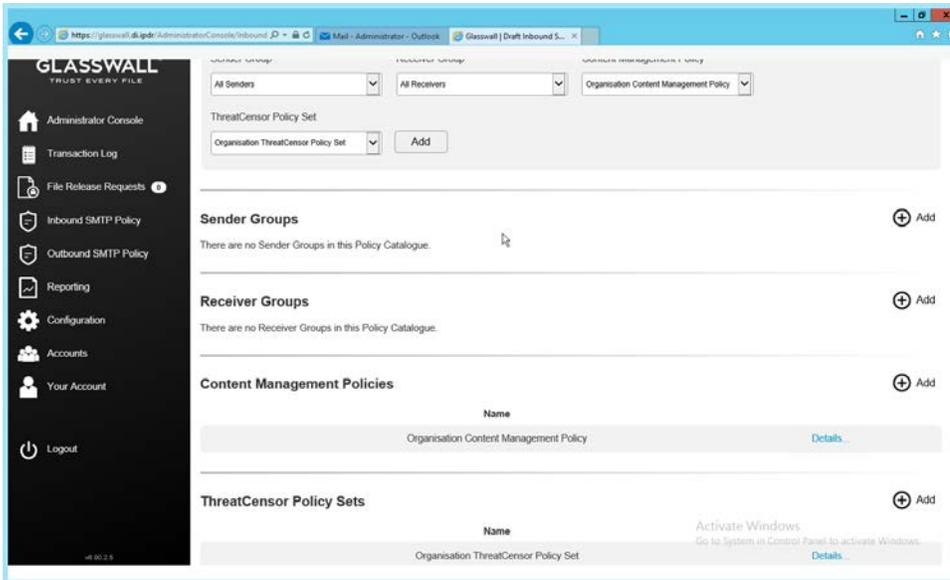
1177 2.7.3.4 *Create a Receiver Group*

1178 1. On the left sidebar, click **Inbound SMTP Policy**.

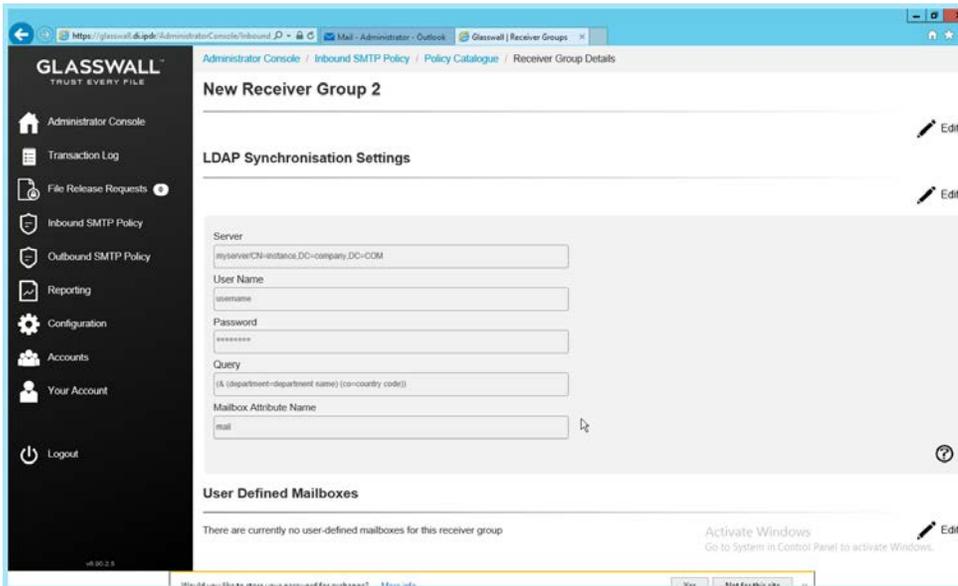
1179 2. Click **Draft Policy Catalogue**.



1180 3. Under **Receiver Groups**, click **Add**.

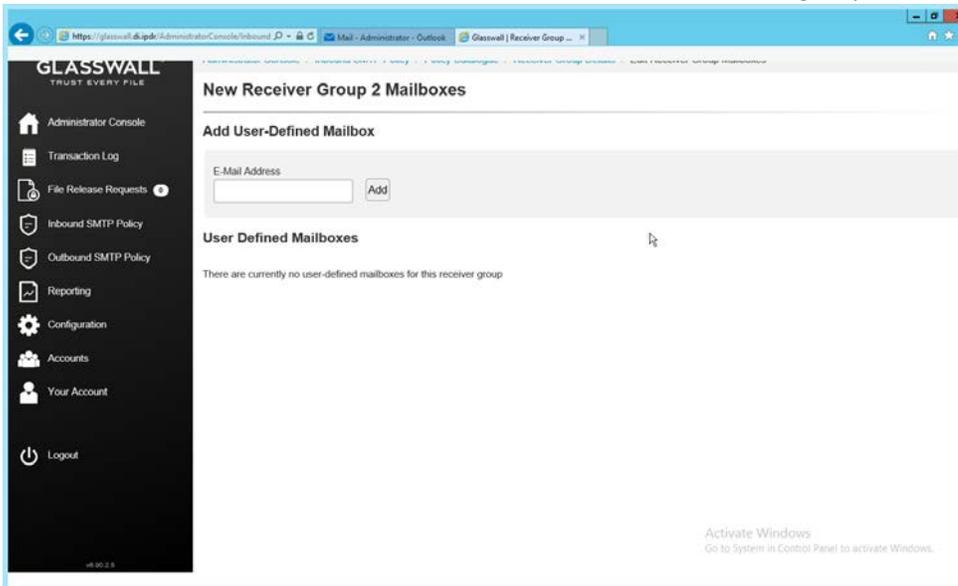


1182 4. Under **User Defined Mailboxes**, click **Edit**.



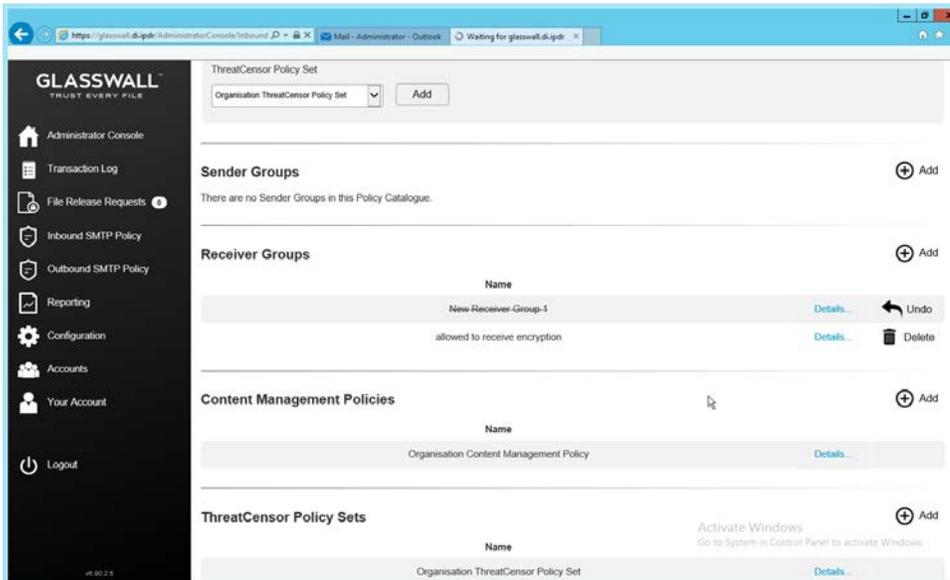
1184  
1185

5. Enter the email address(es) of users who should be in this receiver group.



1186  
1187  
1188

6. Click **Add**.
7. When finished, return to the **Policy Catalogue** page.



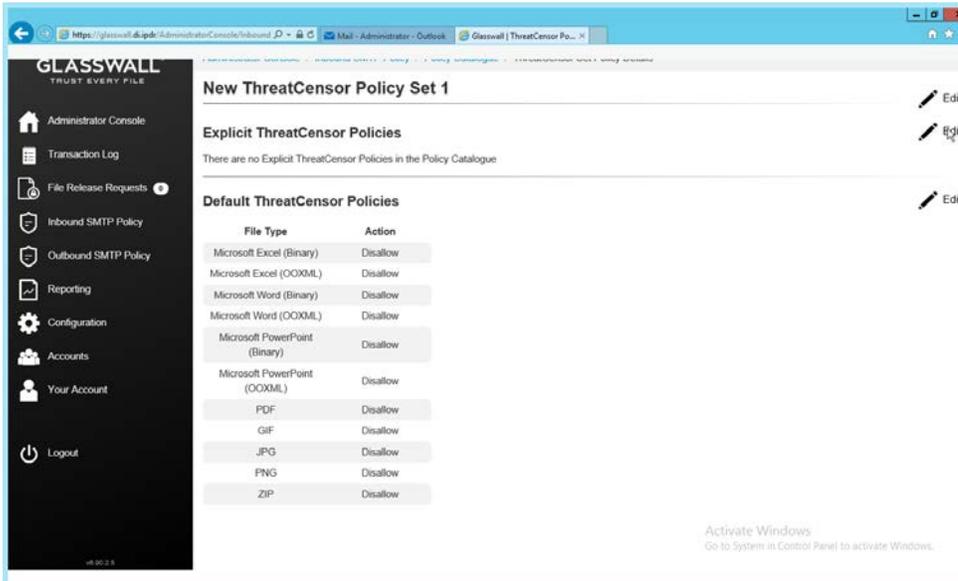
1189

2.7.3.5 *Create a ThreatCensor Policy Set*

1190

1191

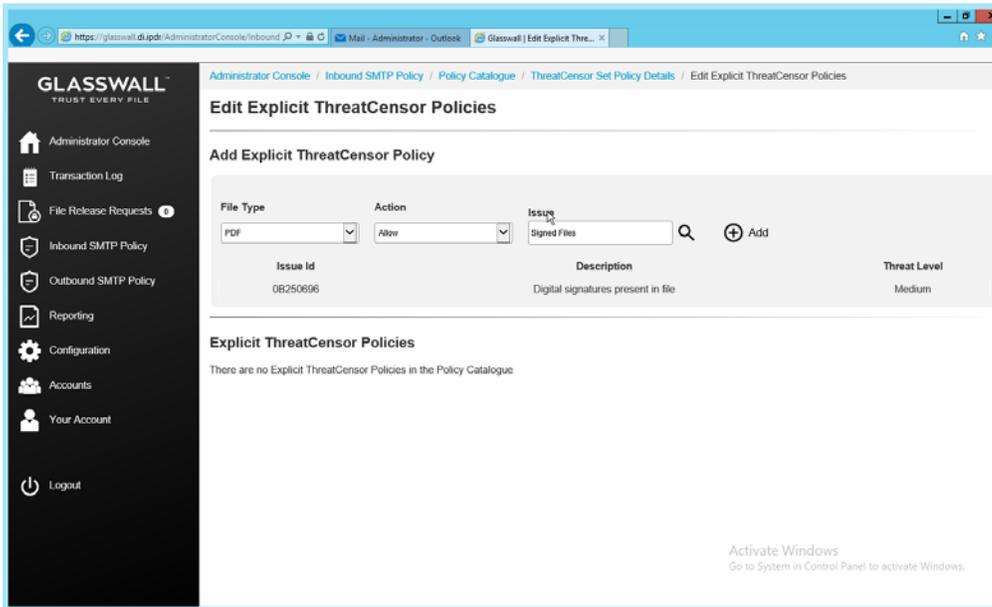
1. Under **ThreatCensor Policy Sets**, click **Add**.



1192

1193

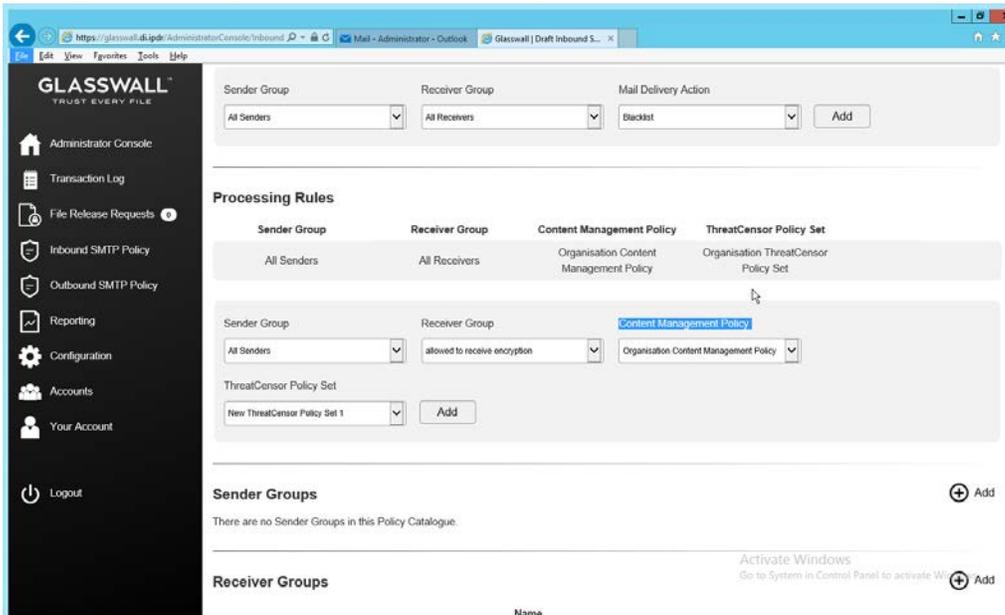
2. Under **Explicit ThreatCensor Policies**, click **Edit**.



- 1194
  - 1195
  - 1196
  - 1197
3. Select the **File Type** and **Action** for the rule.
  4. Under **Issue**, click the magnifying glass to search for an error code.
  5. Return to the **Policy Catalogue** page when finished.

1198 **2.7.3.6 Create a Processing Rule**

- 1199
  - 1200
1. Under Processing Rules, select the appropriate **Sender Group**, **Receiver Group**, **Content Management Policy**, and **ThreatCensor Policy Set**.

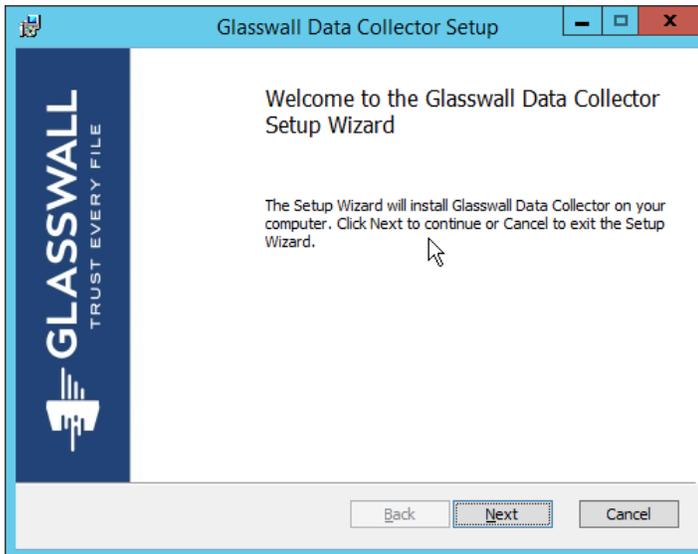


1201

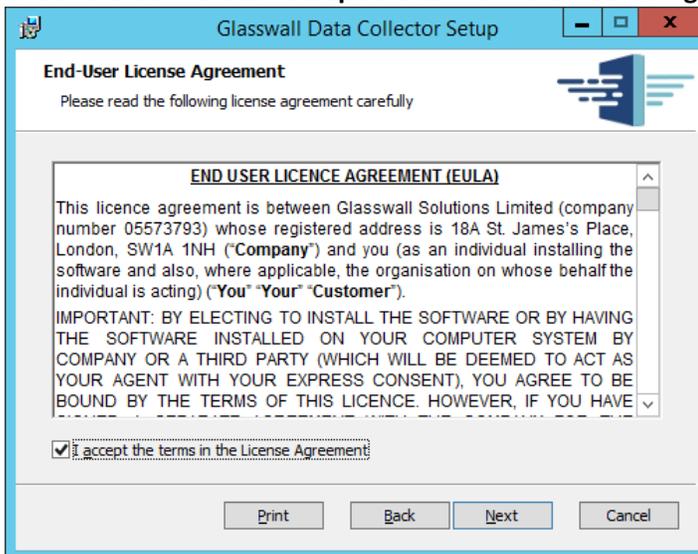
- 1202 2. Click **Add**.
- 1203 3. This allows for granular policy for email inspection, quarantine, and reconstruction.

## 1204 2.7.4 Configure Intelligence Sharing

- 1205 1. Run **DataCollectorInstaller.msi**.

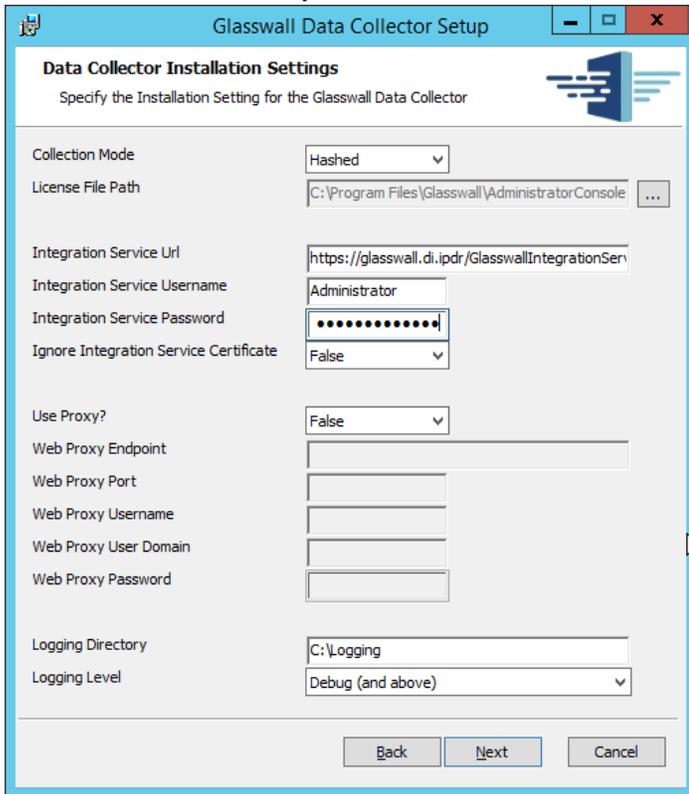


- 1206 2. Click **Next**.
- 1207 3. Check the box next to **I accept the terms in the License Agreement**.
- 1208

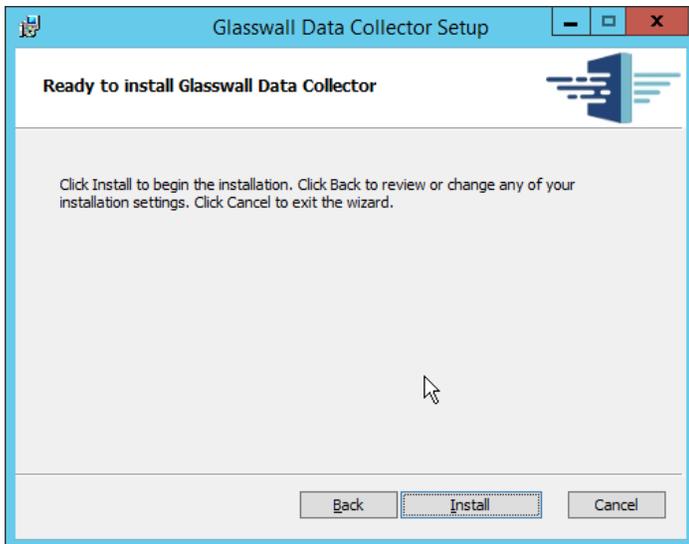


- 1209 4. Click **Next**.
- 1210 5. Select **Hashed** for **Collection Mode** (especially if your data is sensitive; this will prevent the
- 1211 release of any identifying information).
- 1212

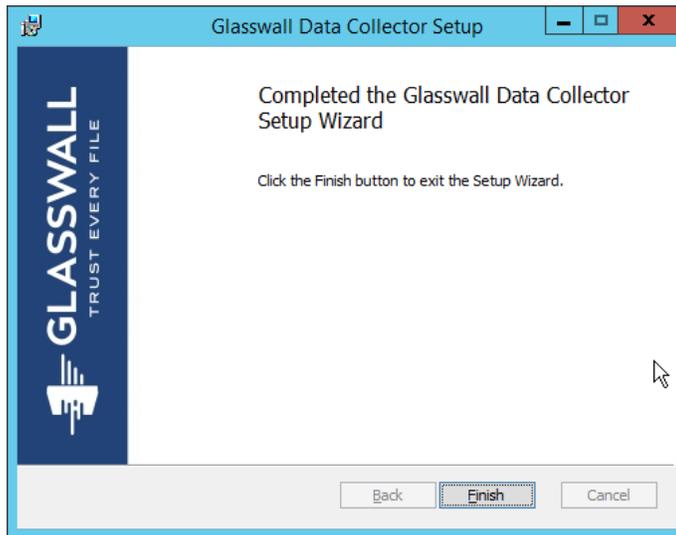
- 1213 6. For **Integration Service Url** replace **localhost** with the name of the computer running the
- 1214 **Integration Service**.
- 1215 7. Enter the **username** and **password**.



- 1216 8. Click **Next**.
- 1217



- 1218 9. Click **Install**.
- 1219



1220

1221

10. Click **Finish**.

1222

## 2.8 Micro Focus ArcSight Enterprise Security Manager

1223

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

1224

1225

1226

This installation guide assumes a pre-configured CentOS 7 machine with ESM already installed and licensed. This section covers the installation and configuration process used to set up ArcSight agents on various machines, as well as some analysis and reporting capabilities.

1227

1228

1229

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

1230

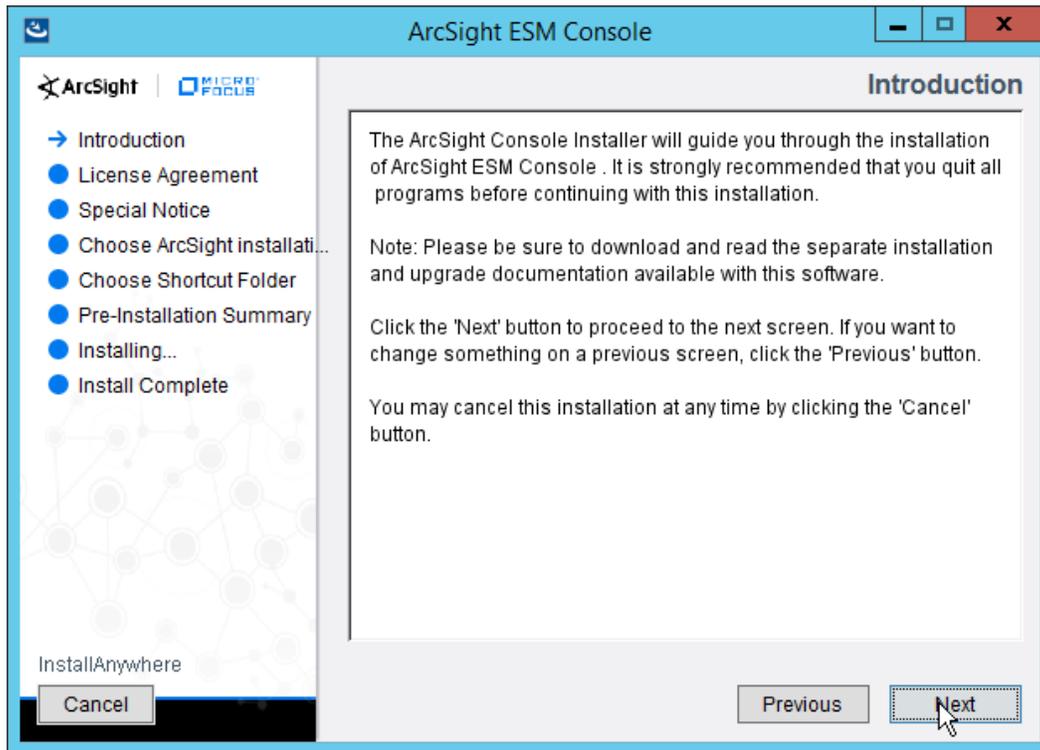
1231

1232

### 2.8.1 Install the ArcSight Console

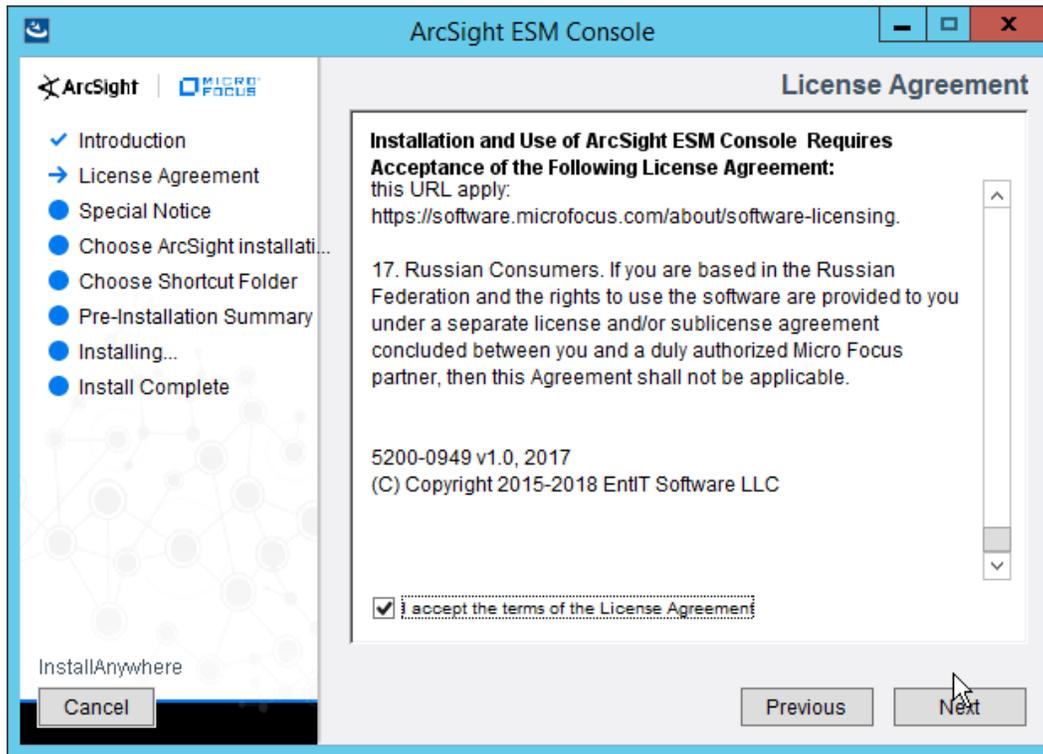
1233

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



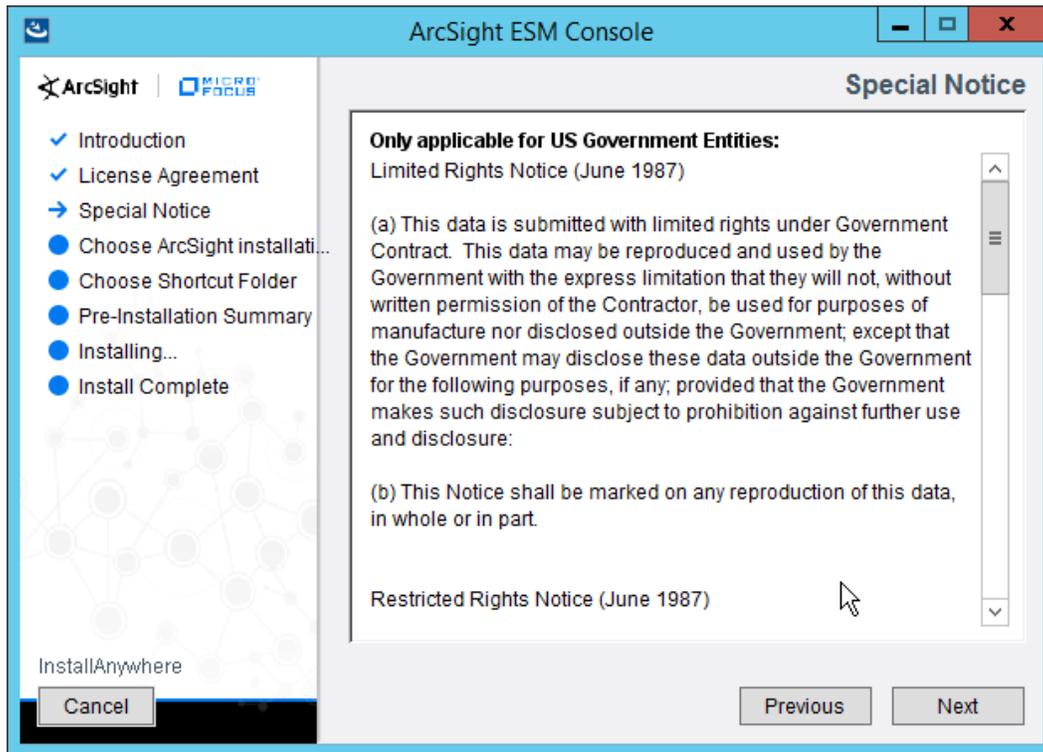
1234  
1235  
1236

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



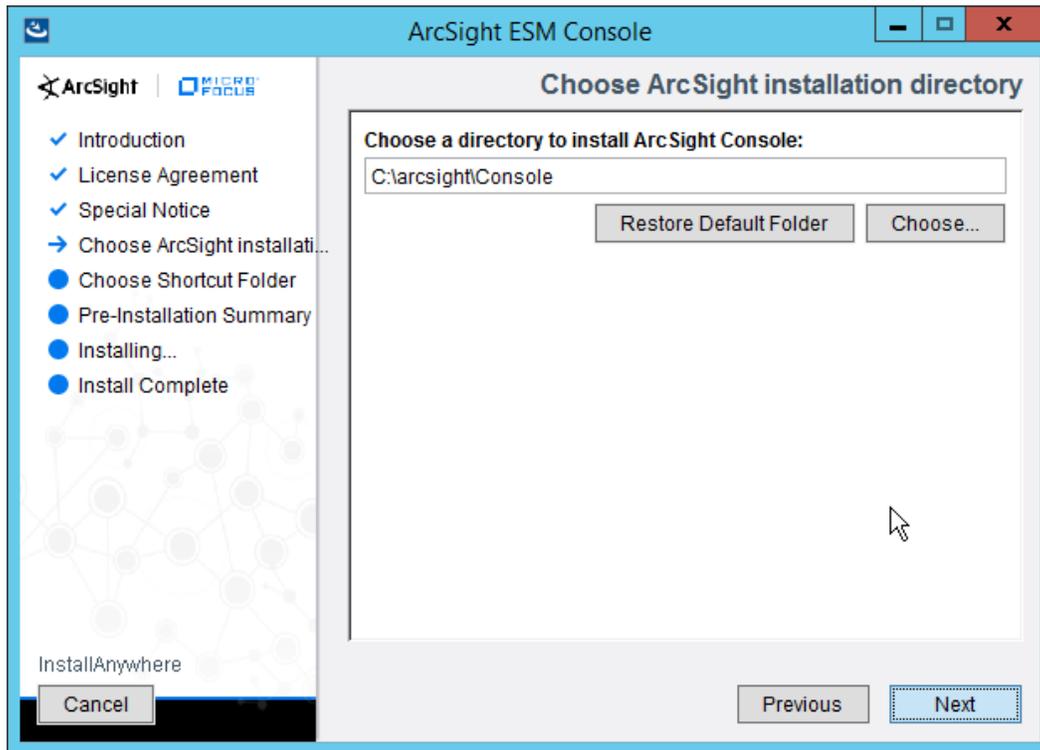
1237  
1238

4. Click **Next**.



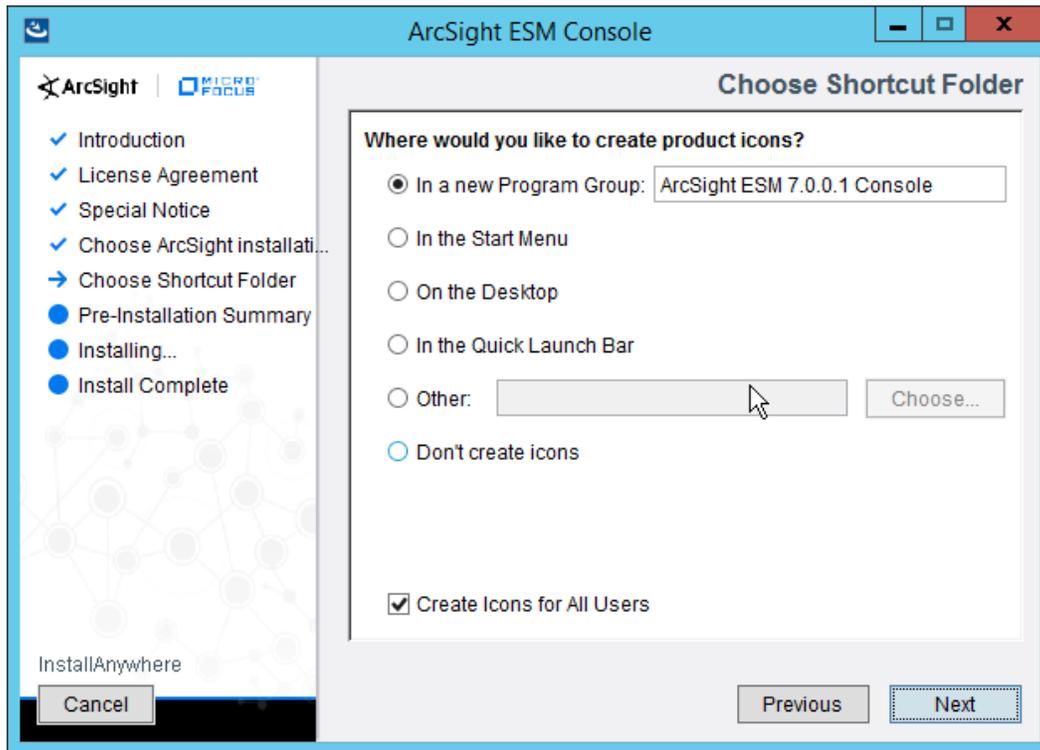
1239  
1240

5. Click **Next**.



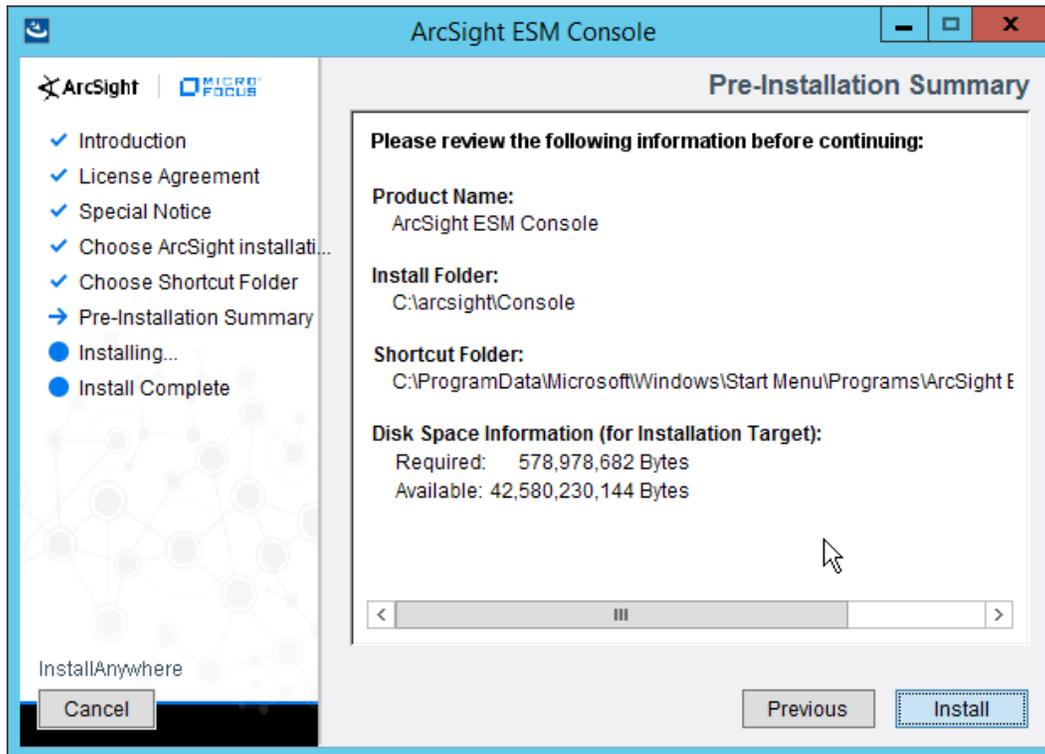
1241  
1242

6. Click **Next**.



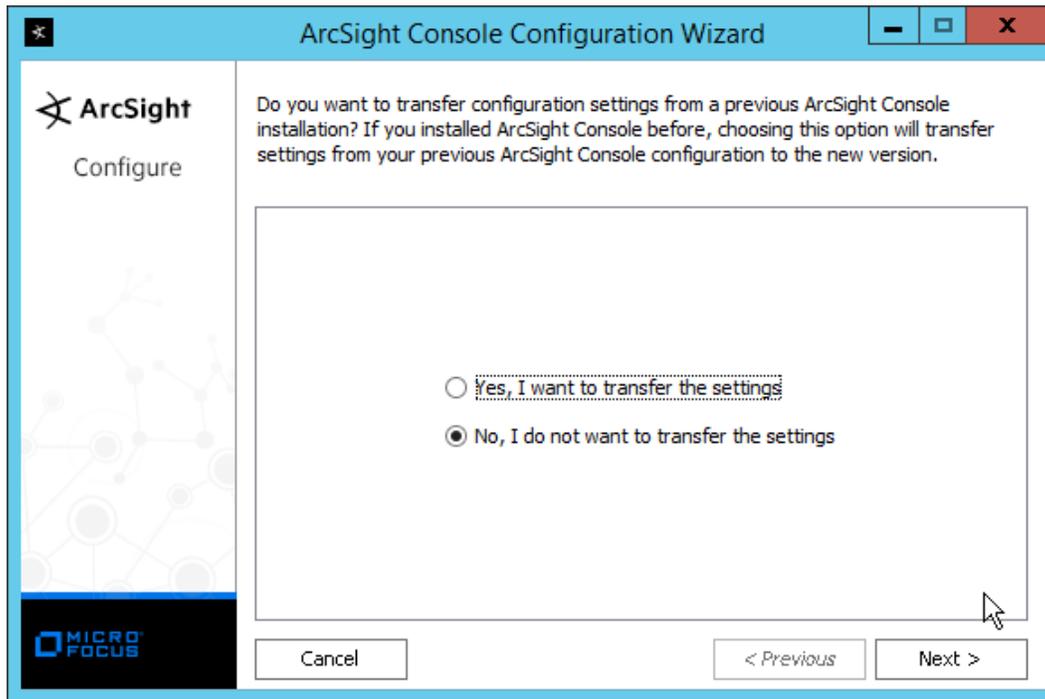
1243  
1244

7. Click **Next**.



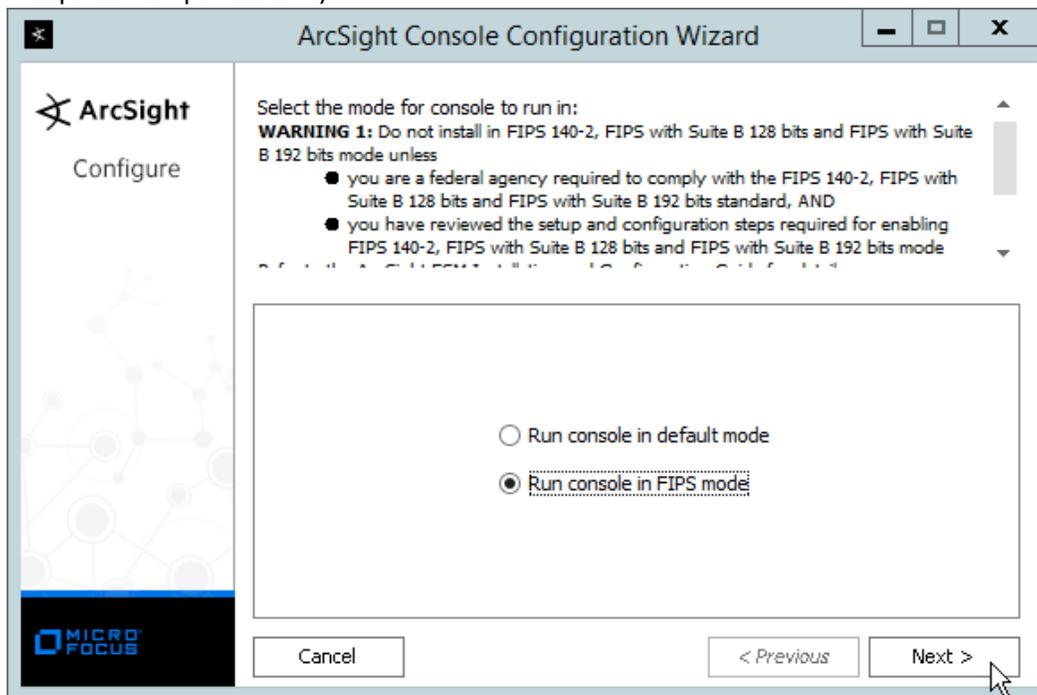
1245  
1246  
1247

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



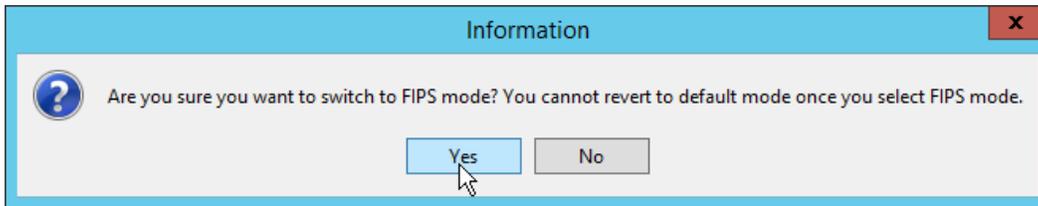
1248  
1249  
1250  
1251

10. Click **Next**.
11. Select **Run console in default mode**. (This can be changed later according to your organization’s compliance requirements.)



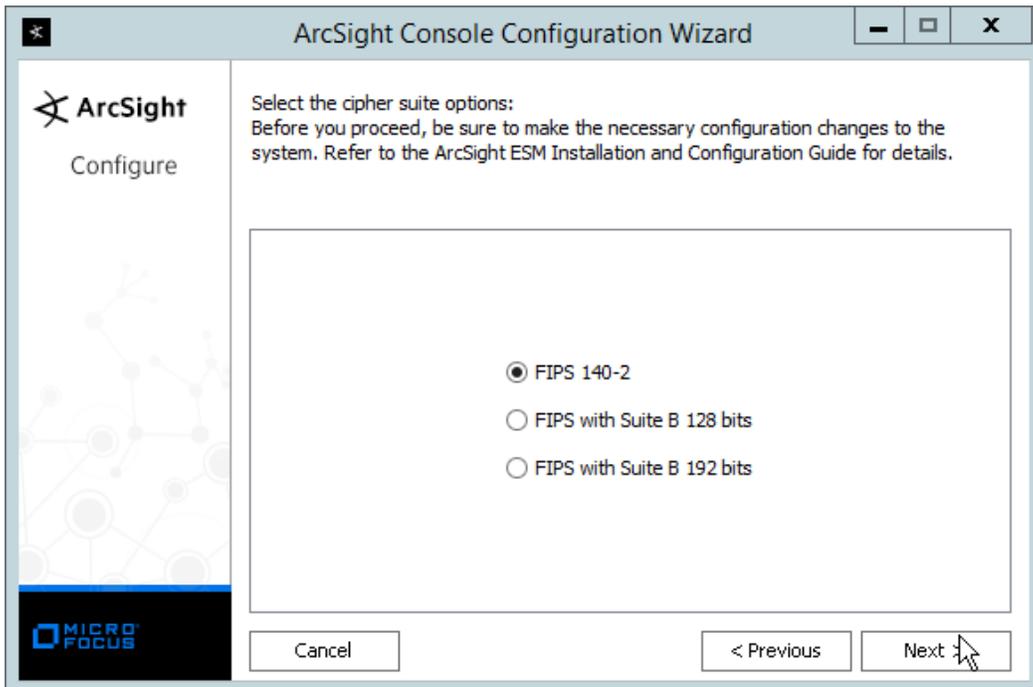
1252

1253 12. Click **Next**.



1254 13. Click **Yes**.

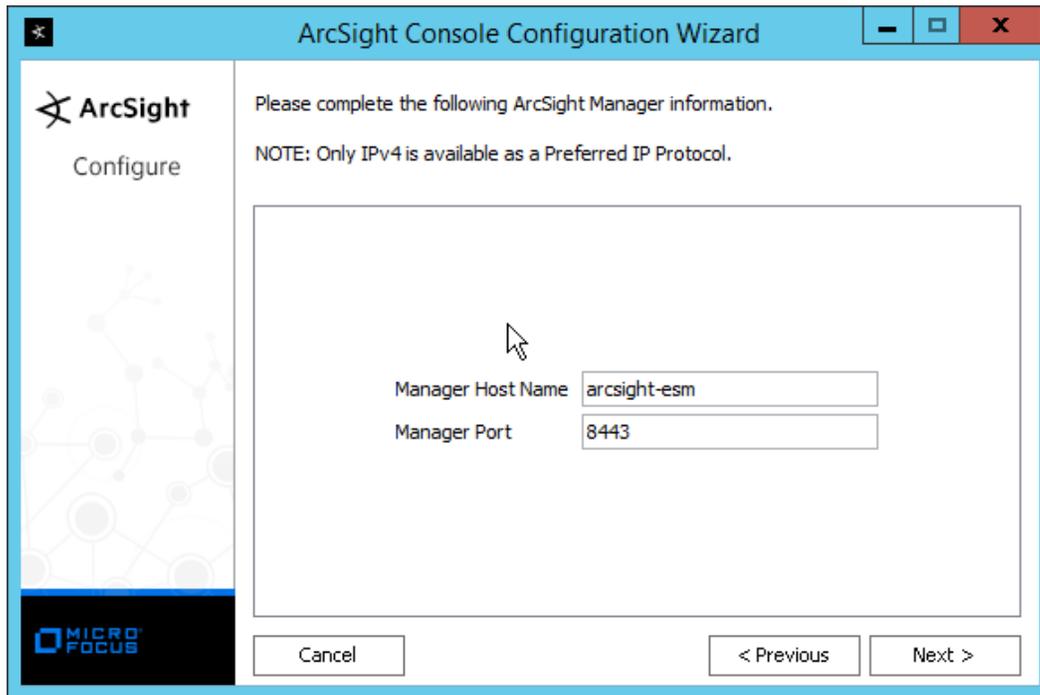
1255 14. Select **FIPS 140-2**.



1257 15. Click **Next**.

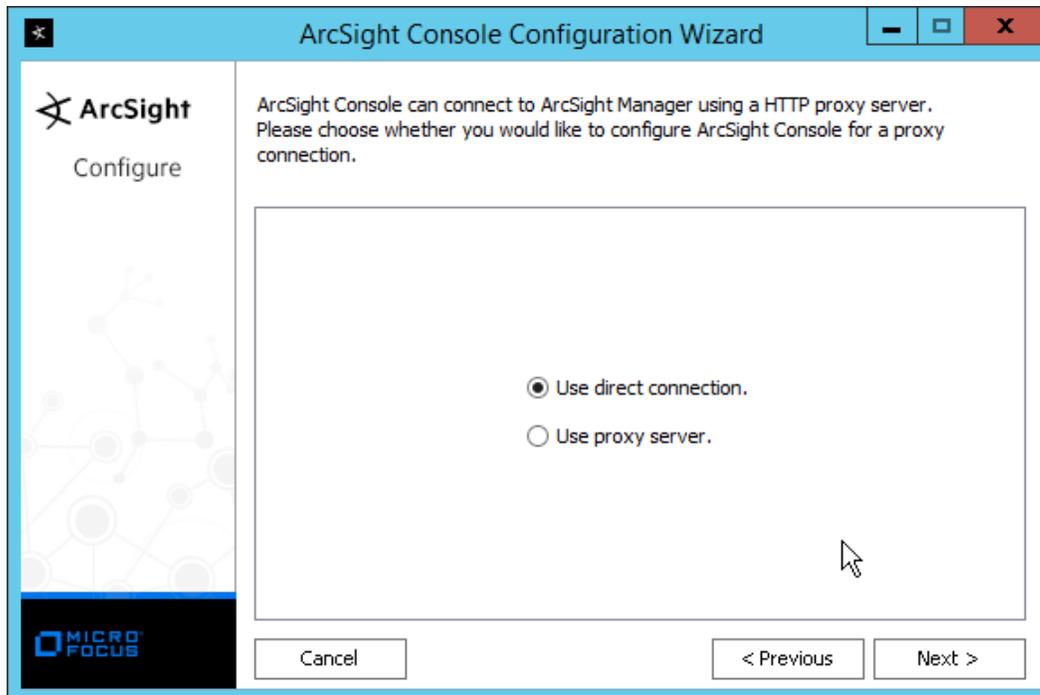
1258 16. Enter the **hostname** of the ESM server for **Manager Host Name**.

1259 17. Enter the **port** that ESM is running on for **Manager Port** (default: **8443**).



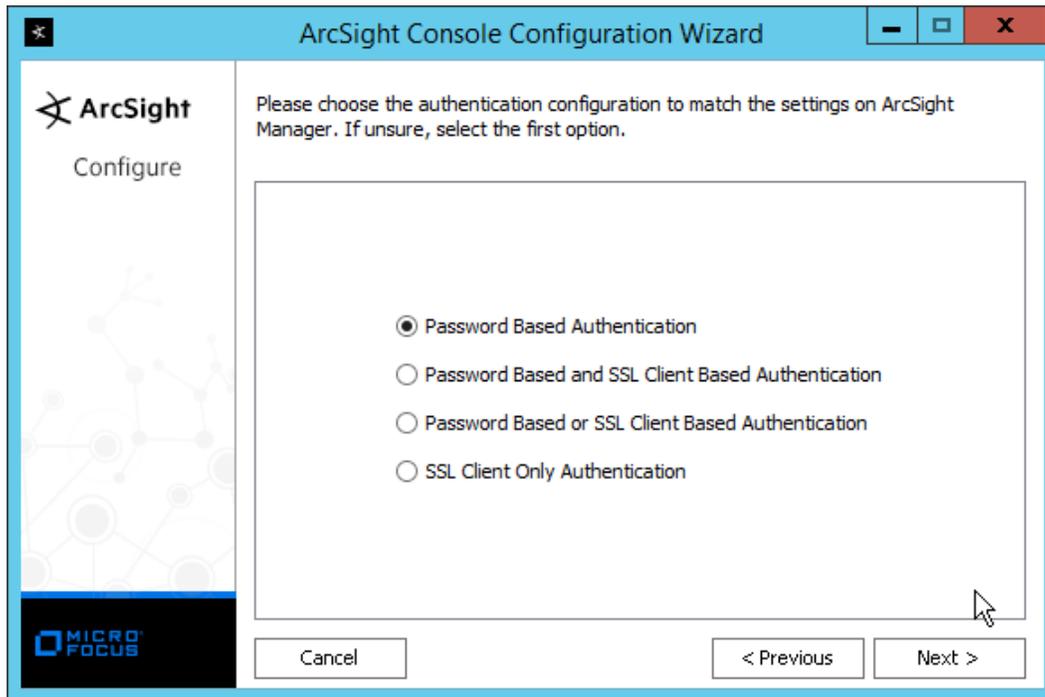
1261  
1262  
1263

- 18. Click **Next**.
- 19. Select **Use direct connection**.



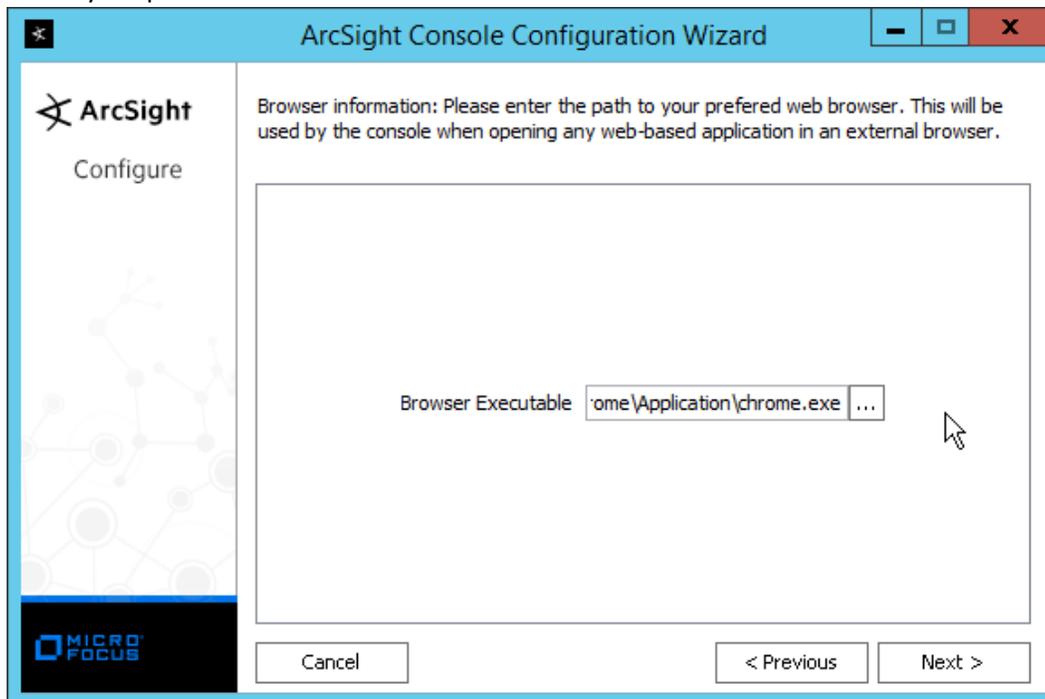
1264  
1265

- 20. Click **Next**.



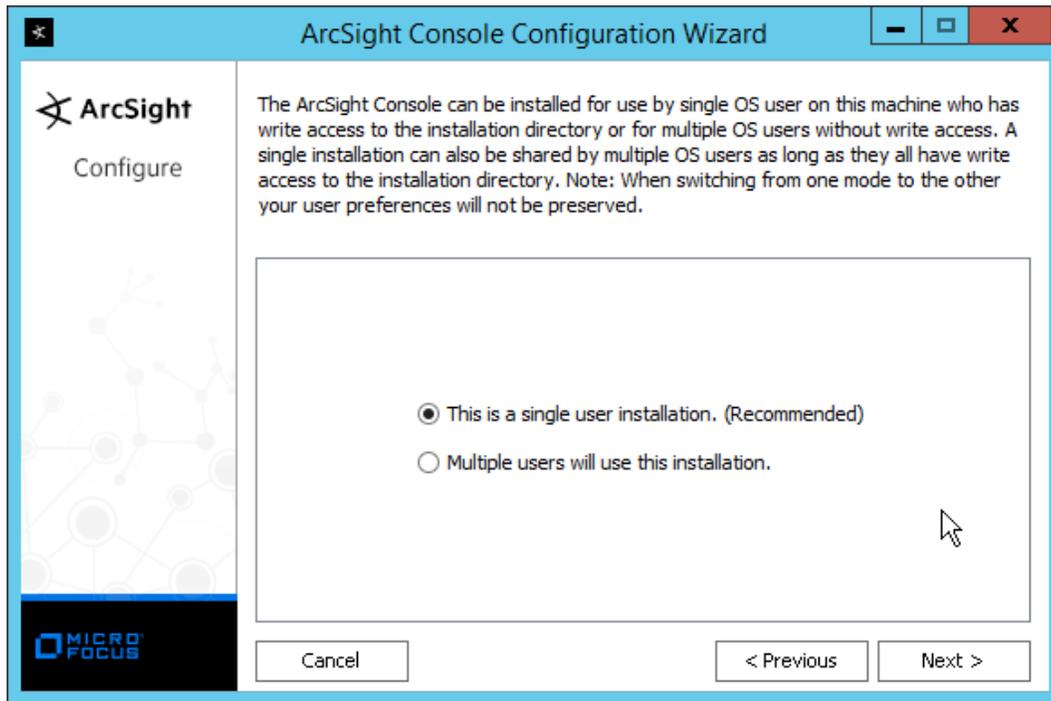
1266  
1267  
1268

- 21. Click **Next**.
- 22. Select your preferred browser.



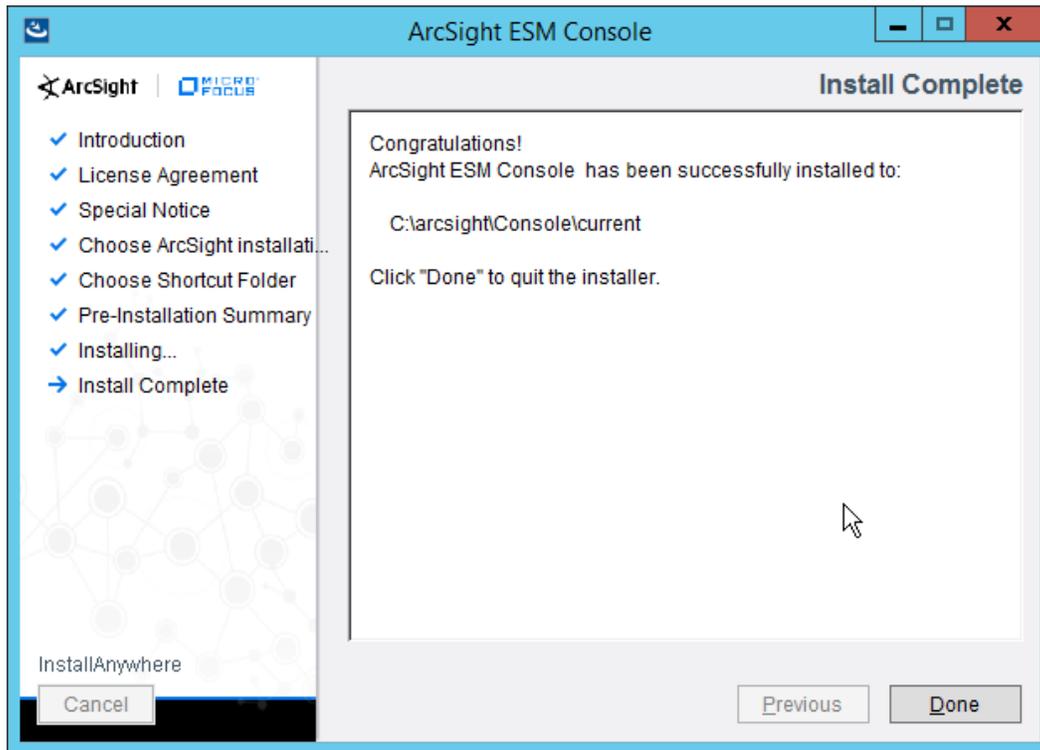
1269  
1270

- 23. Click **Next**.



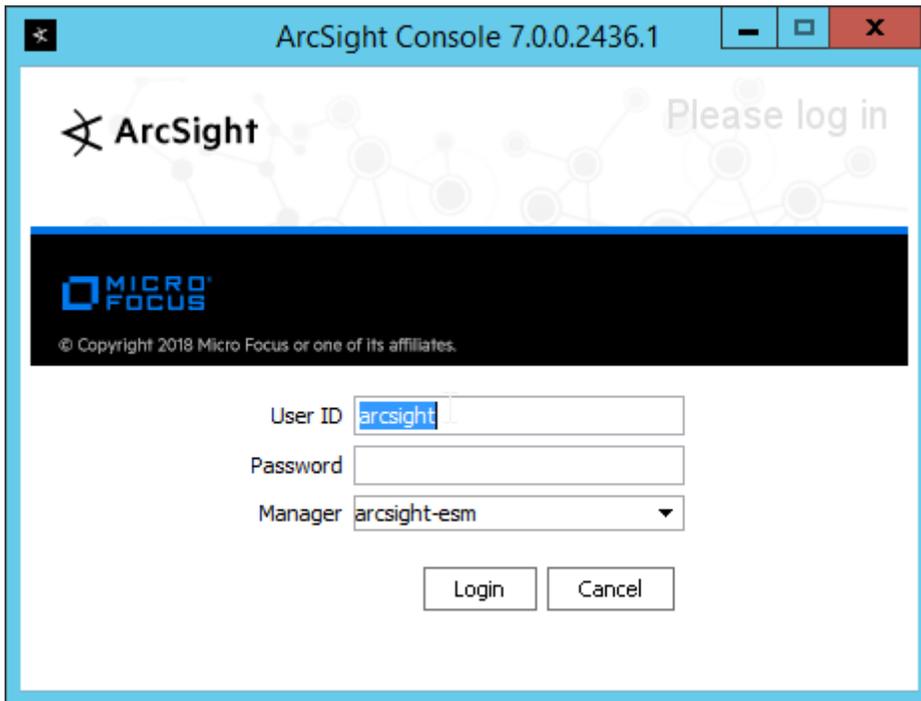
1271  
1272  
1273

- 24. Click **Next**.
- 25. Click **Finish**.



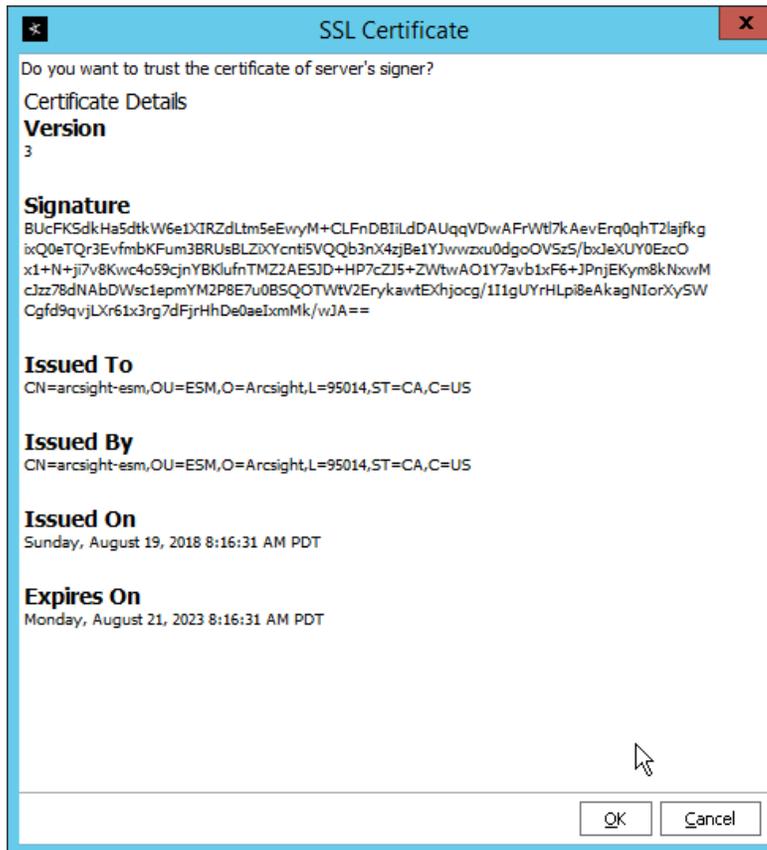
1274  
1275  
1276  
1277

26. Click **Done**.
27. Run **ArcSight Console** from the start menu.
28. Enter the **username** and **password**.



1278  
1279  
1280

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

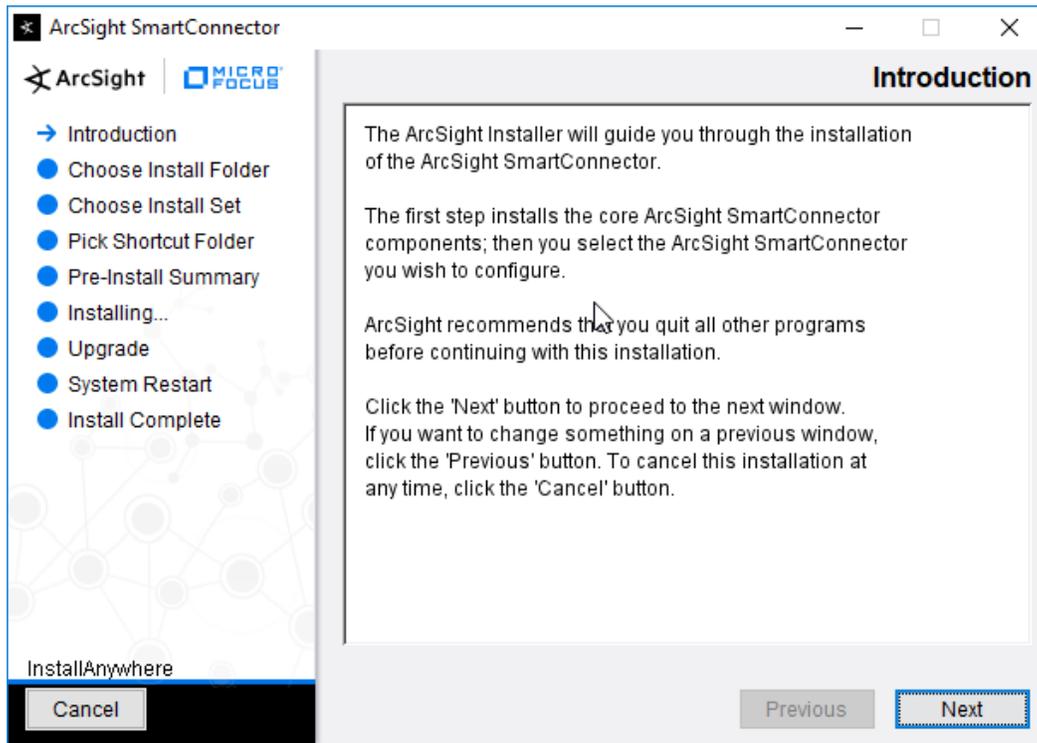


1281  
1282

30. Click **OK**.

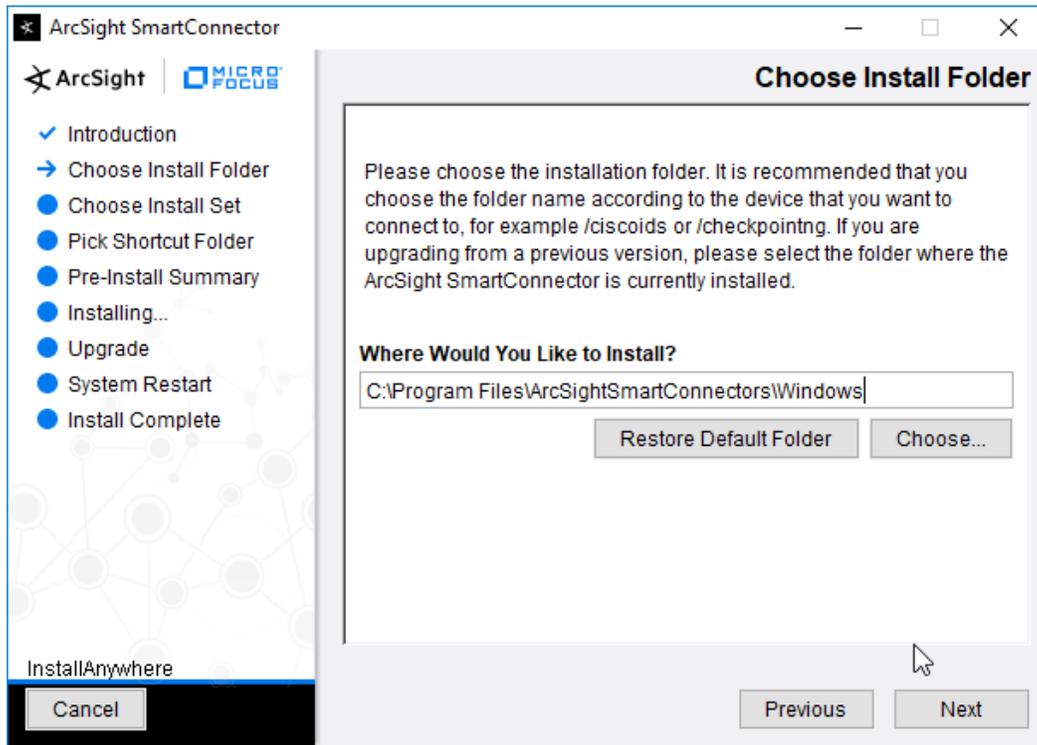
## 1283 2.8.2 Install Individual ArcSight Windows Connectors

- 1284 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



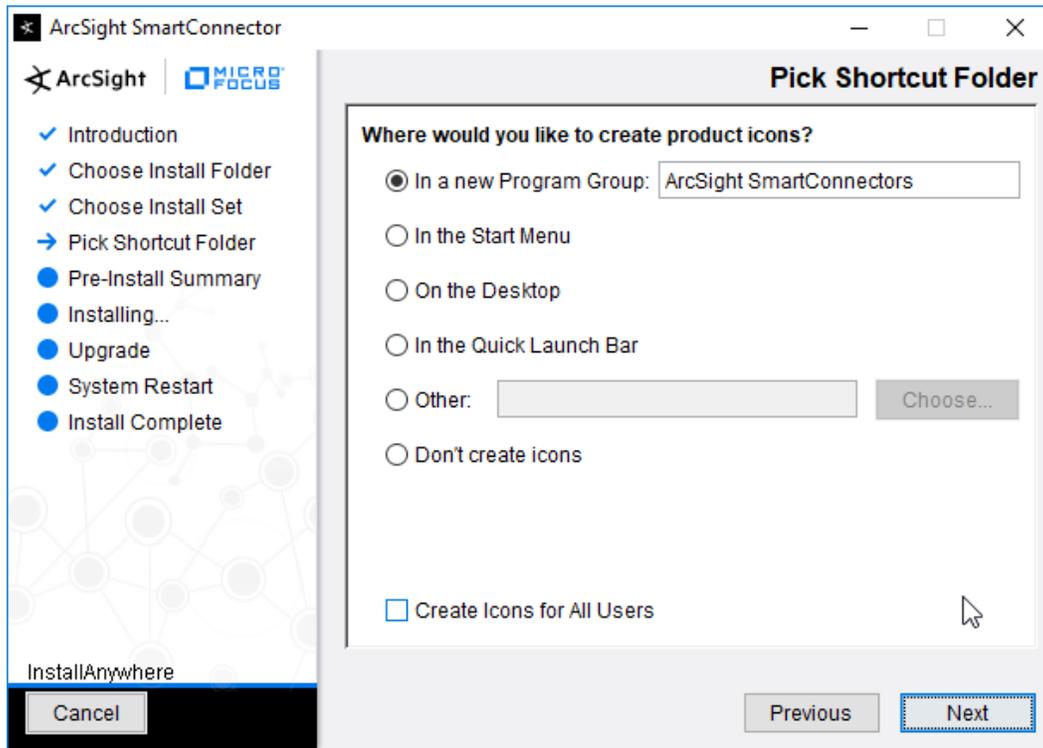
1285  
1286  
1287

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



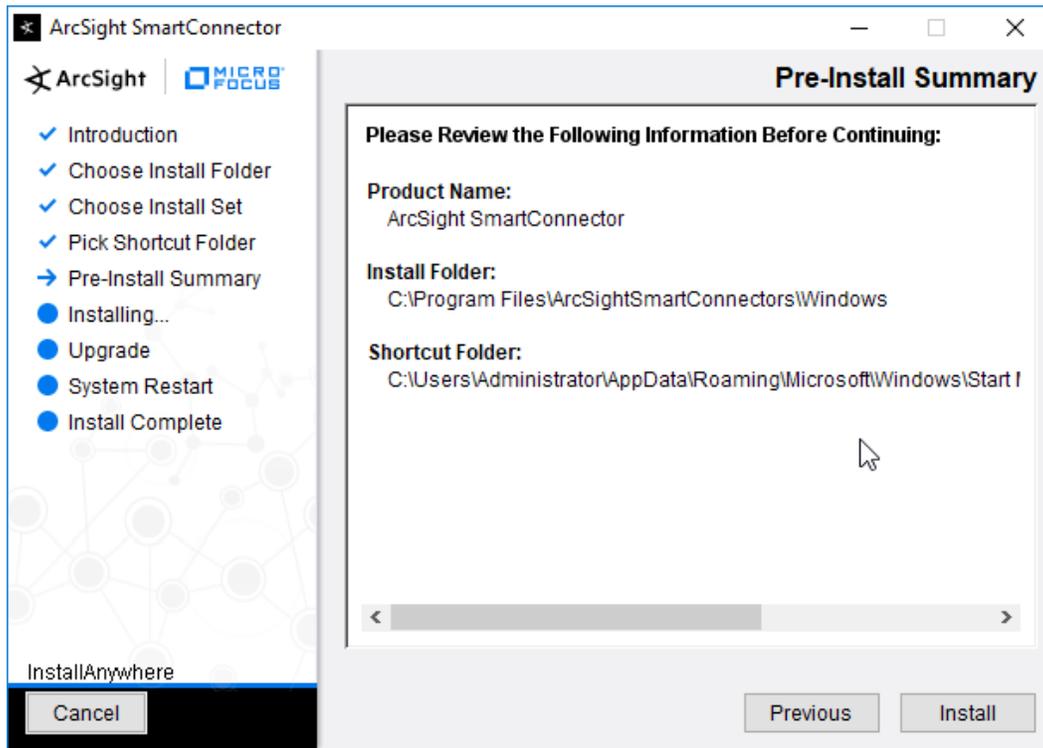
1288  
1289

4. Click **Next**.



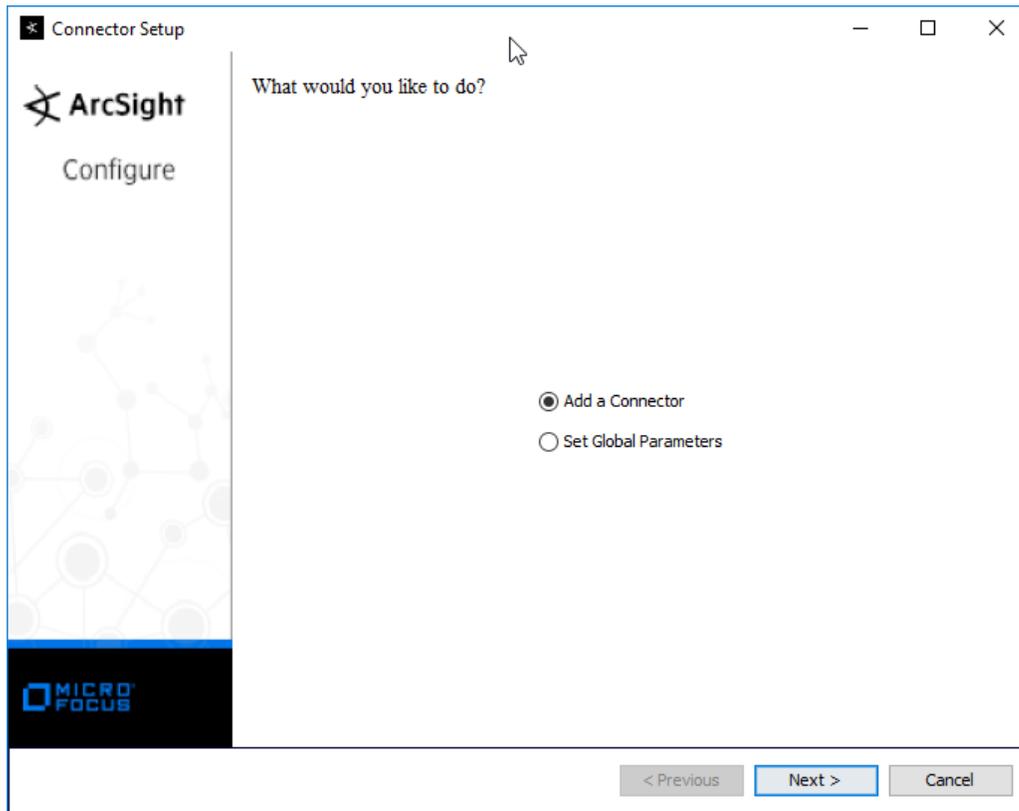
1290  
1291

5. Click **Next**.



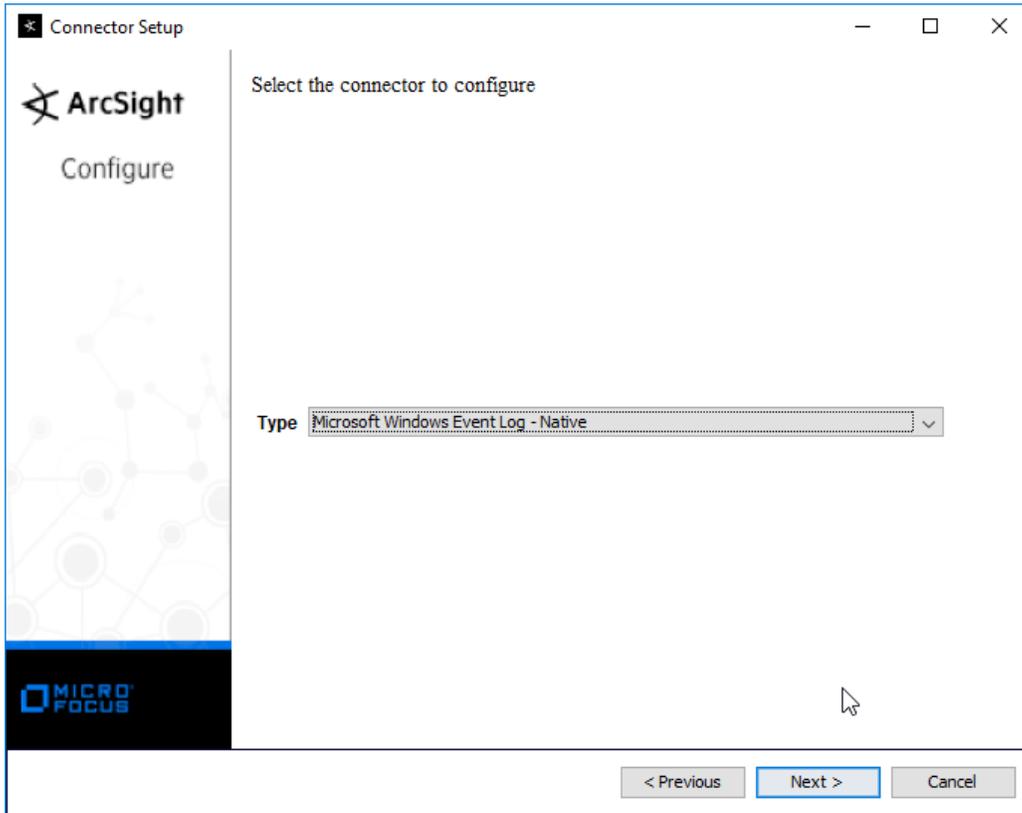
1292  
1293  
1294

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



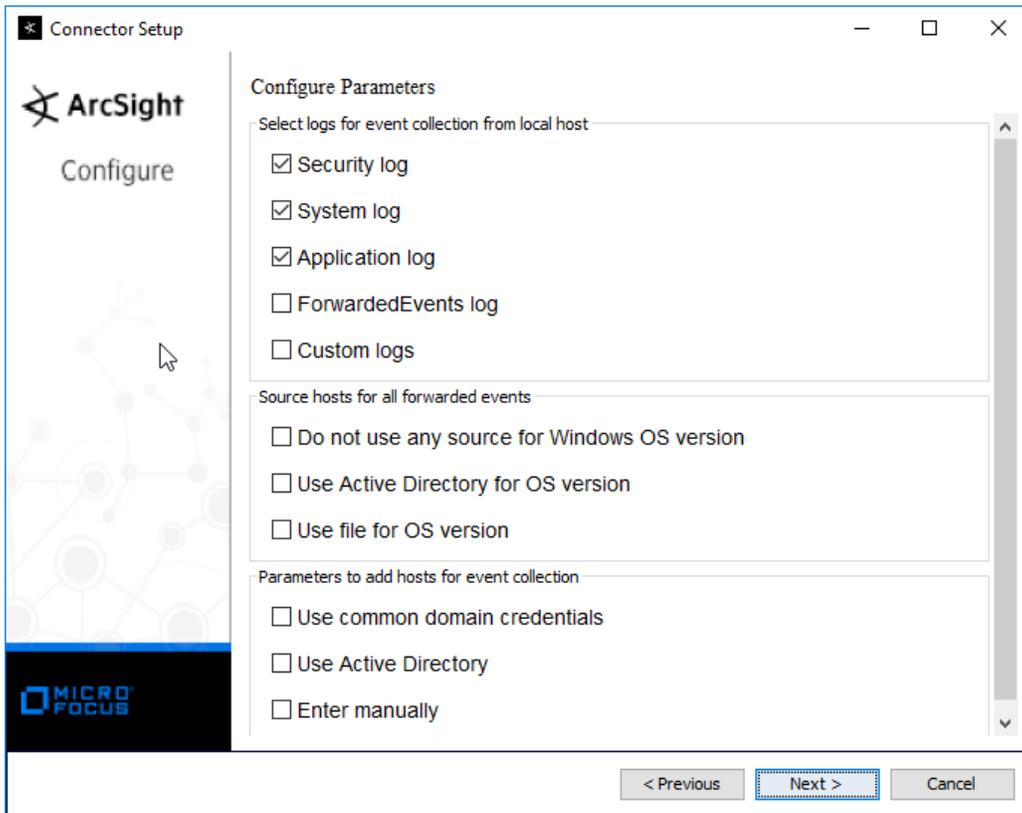
1295  
1296  
1297

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



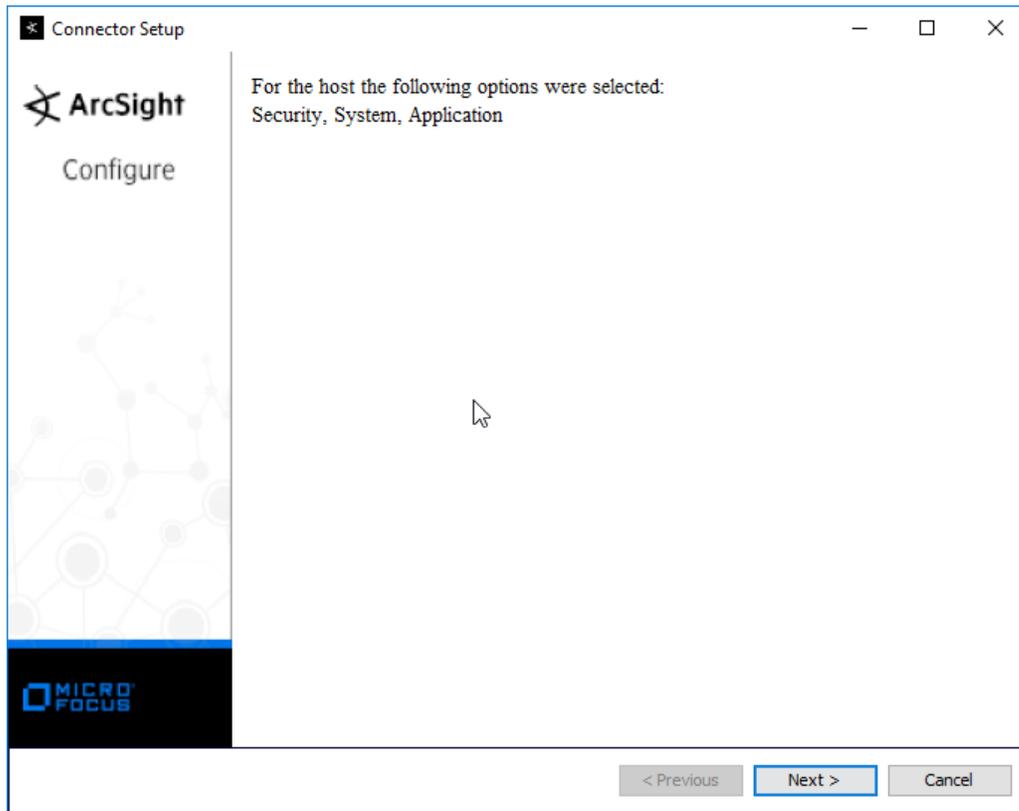
1298  
1299

10. Click **Next**.



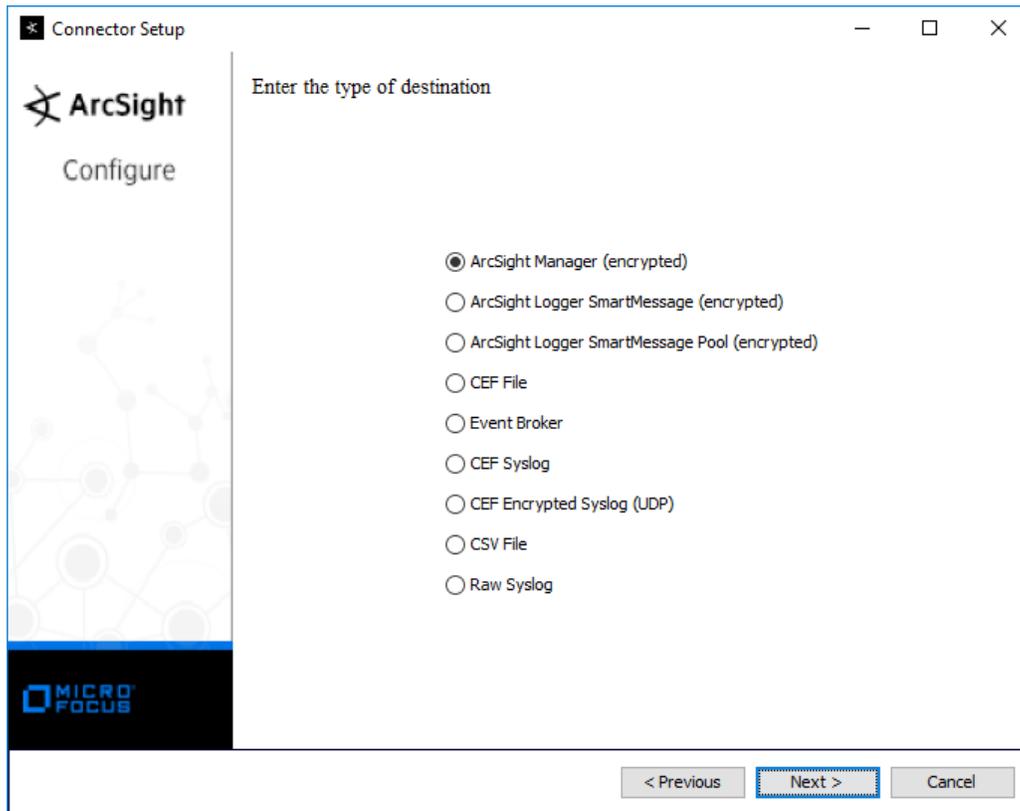
1300  
1301

11. Click **Next**.



1302  
1303  
1304

12. Click **Next**.
13. Select **ArcSight Manager (encrypted)**.



1305  
1306  
1307

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

Connector Setup

ArcSight  
Configure

Enter the destination parameters

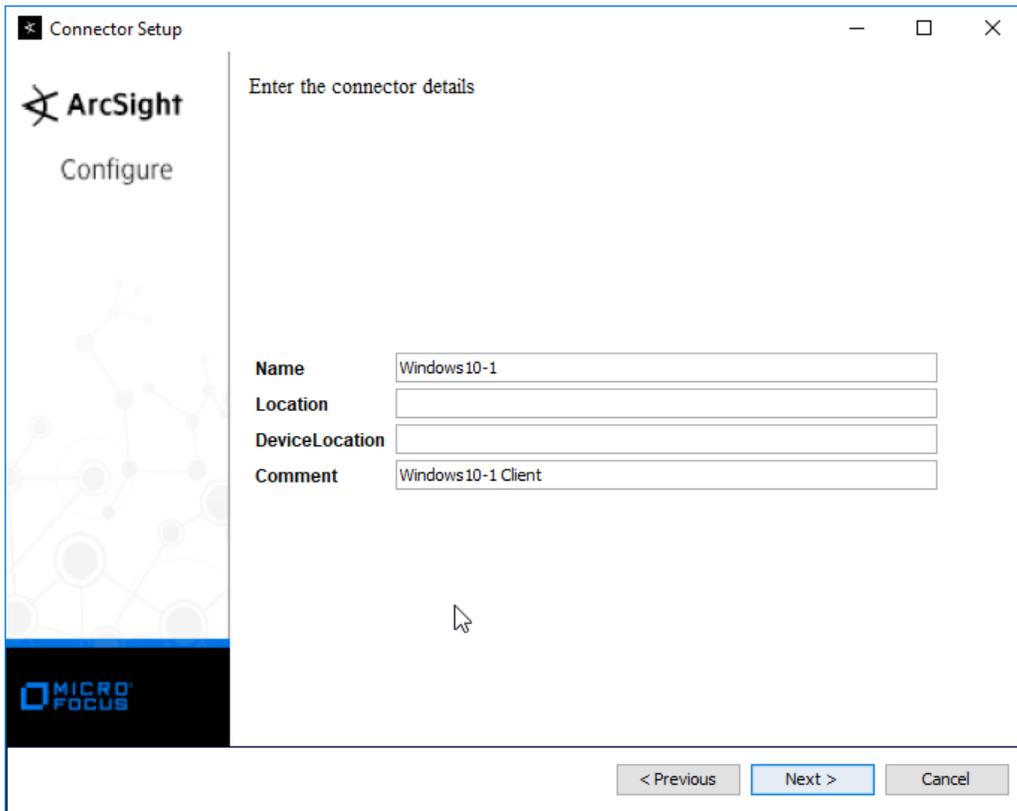
Manager Hostname: arcsight-esm  
Manager Port: 8443  
User: administrator  
Password: ●●●●●●

AUP Master Destination: false  
Filter Out All Events: false  
Enable Demo CA: false

< Previous   Next >   Cancel

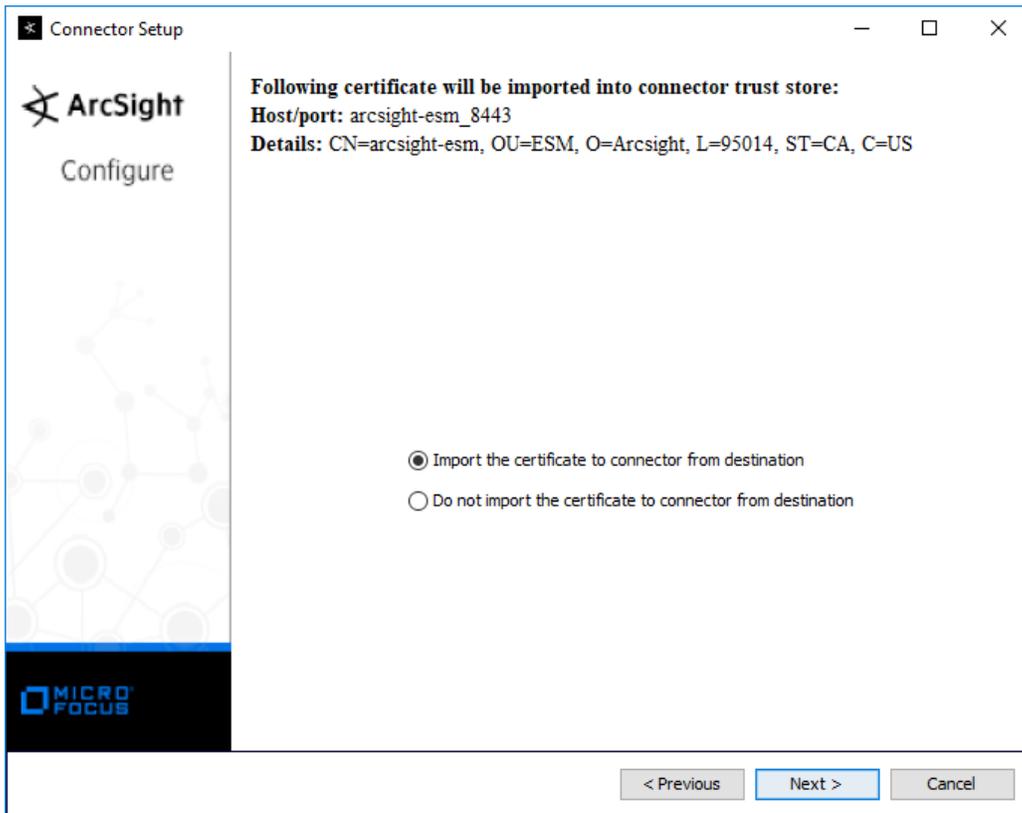
1308  
1309  
1310

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



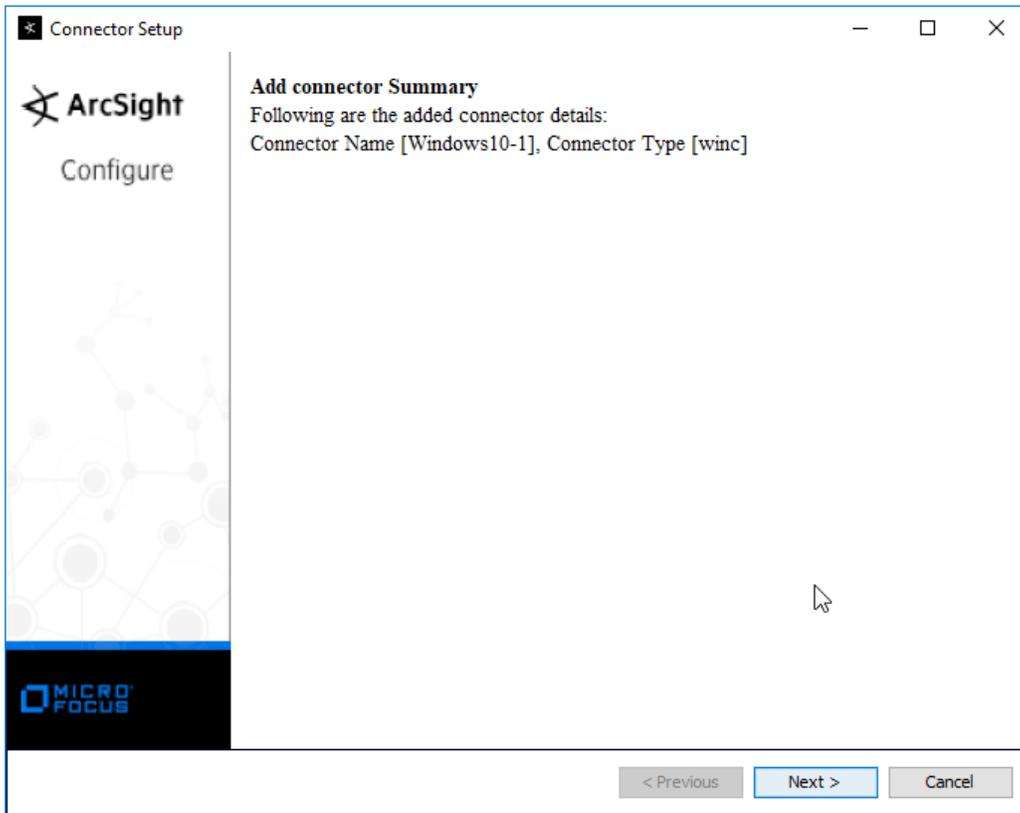
1311  
1312  
1313

- 18. Click **Next**.
- 19. Select **Import the certificate to connector from destination**.



1314  
1315

20. Click **Next**.



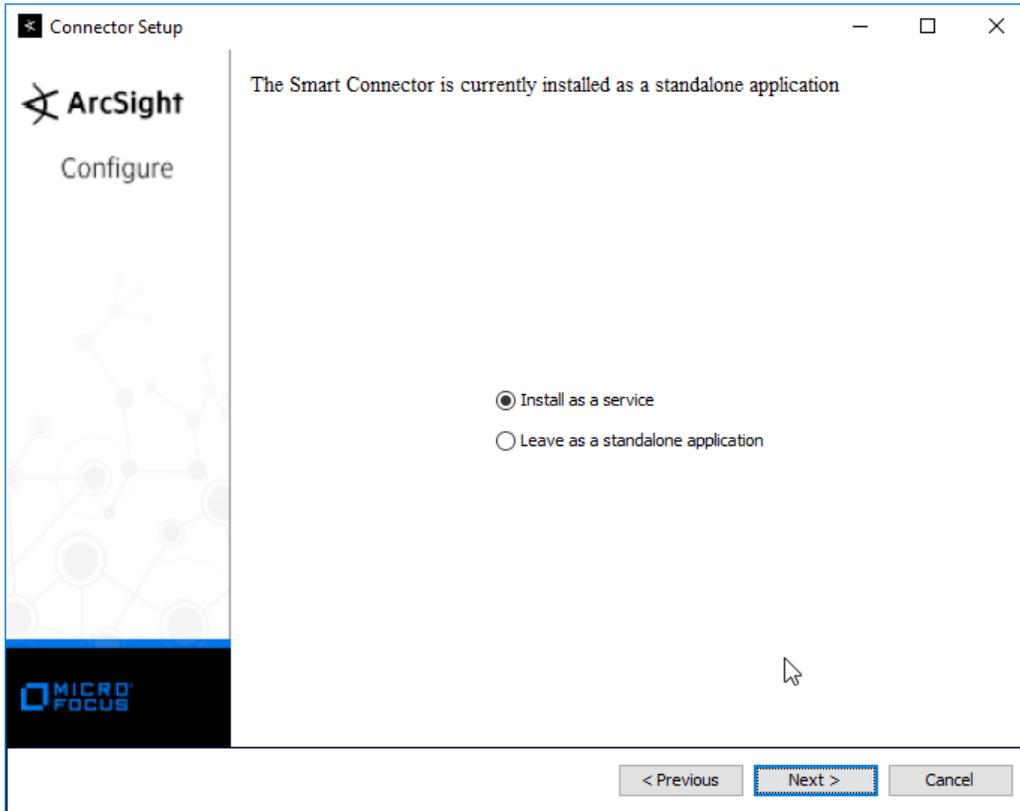
1316

1317

1318

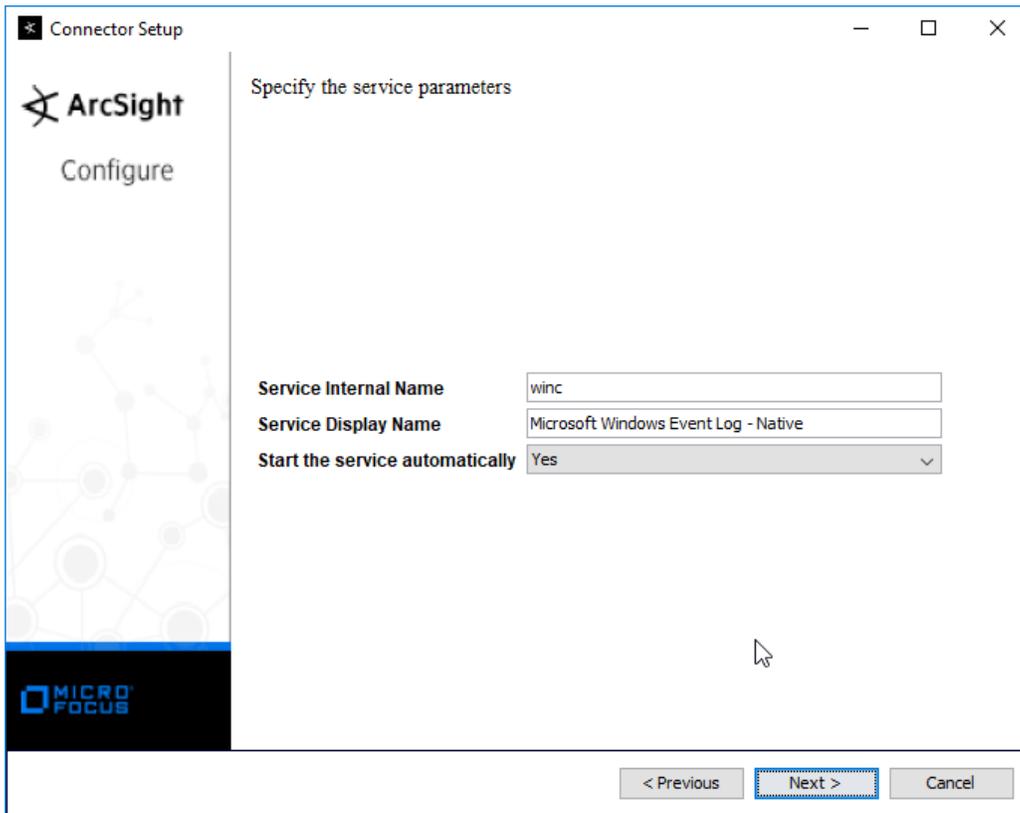
21. Click **Next**.

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



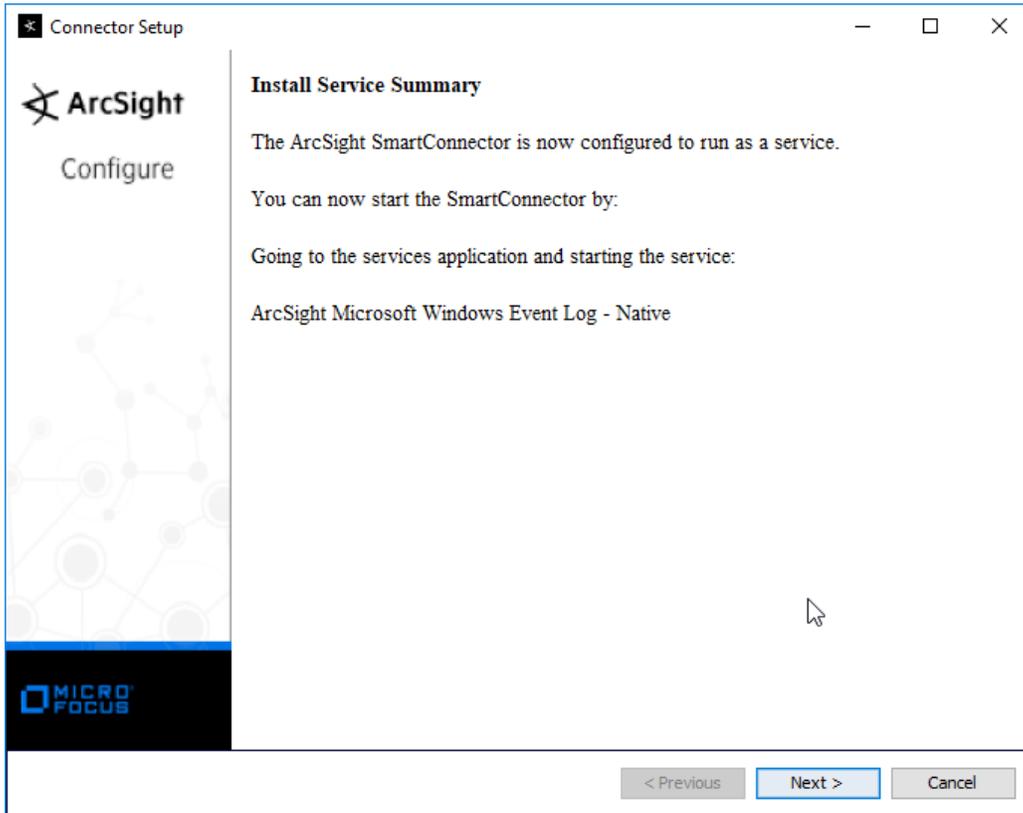
1319  
1320

23. Click **Next**.



1321  
1322

24. Click **Next**.



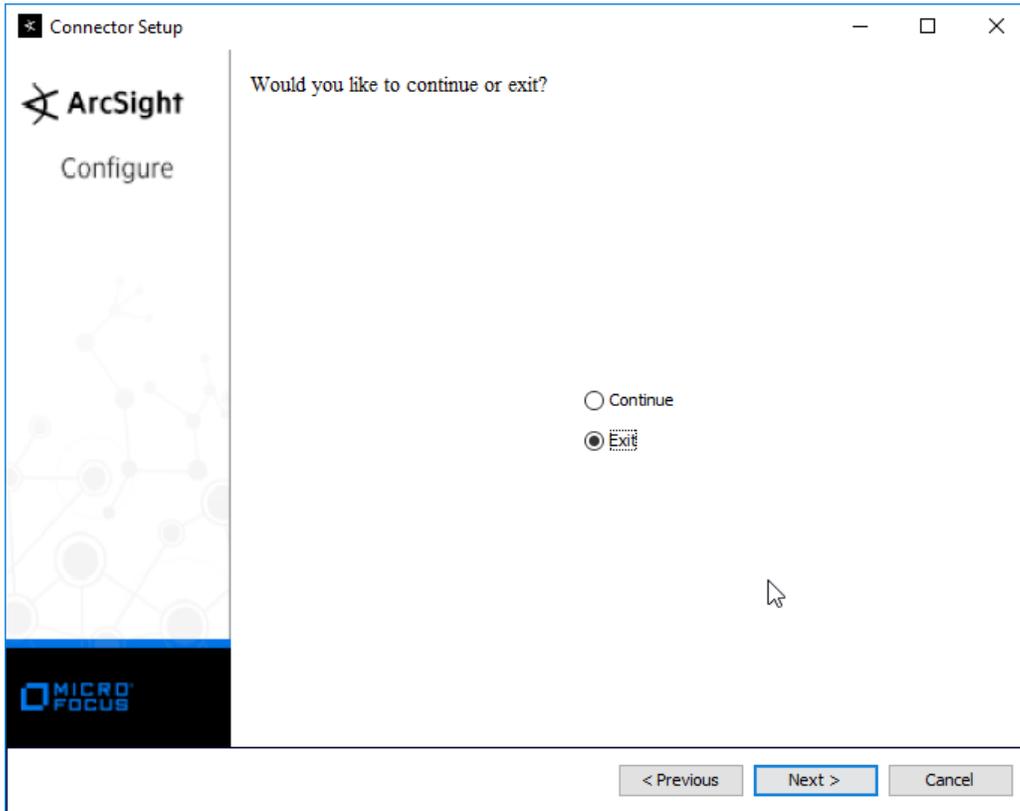
1323

1324

1325

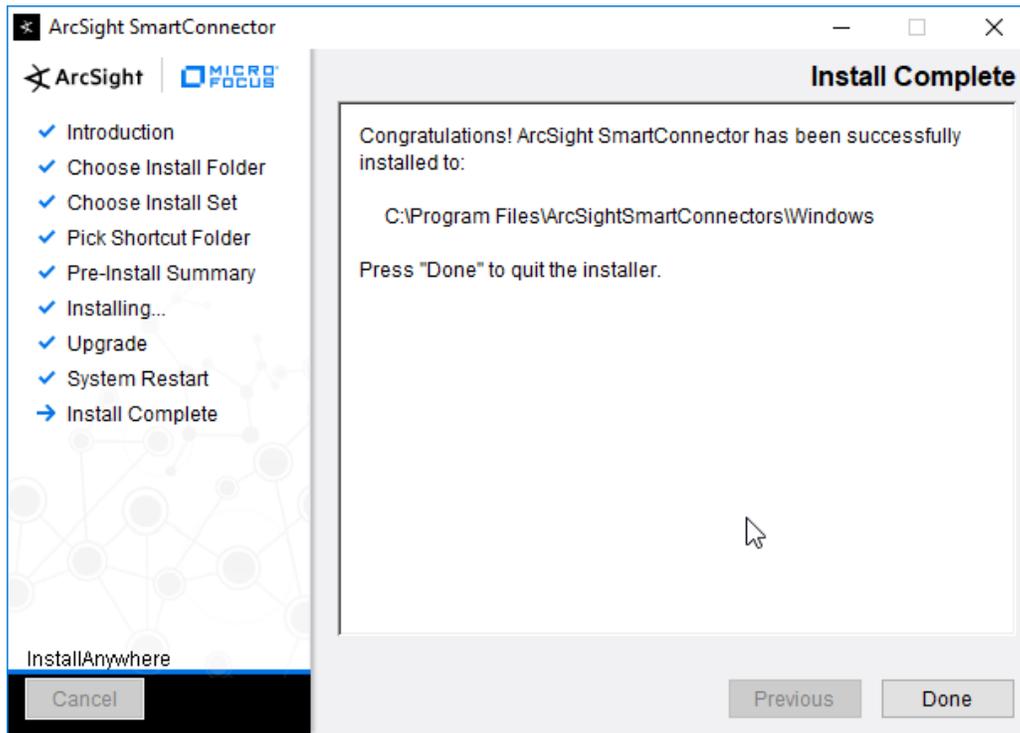
25. Click **Next**.

26. Select **Exit**.



1326  
1327

27. Click **Next**.

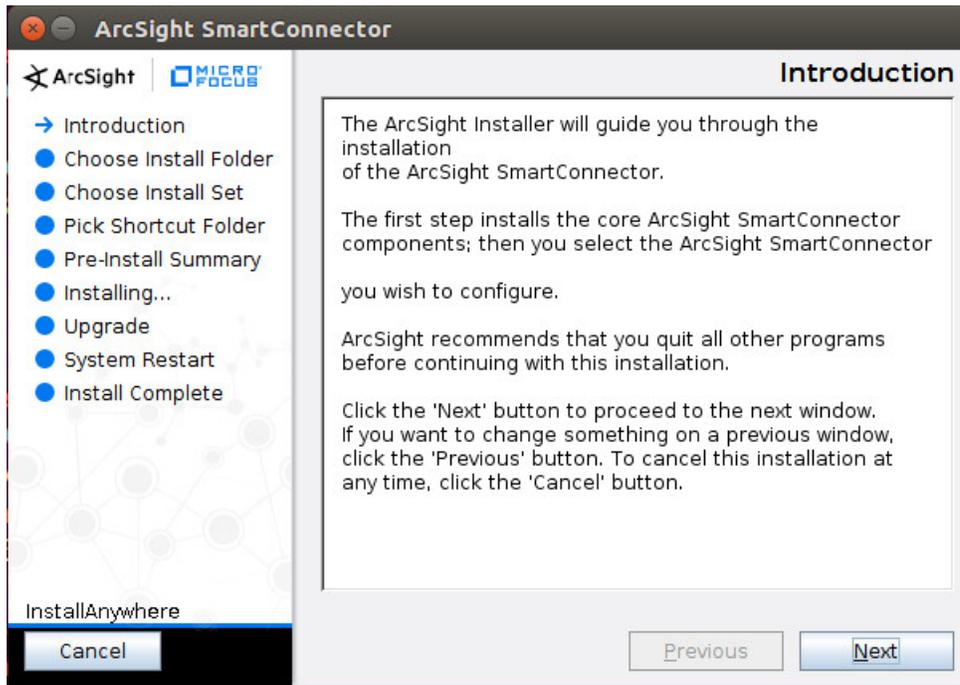


1328  
1329

28. Click **Done**.

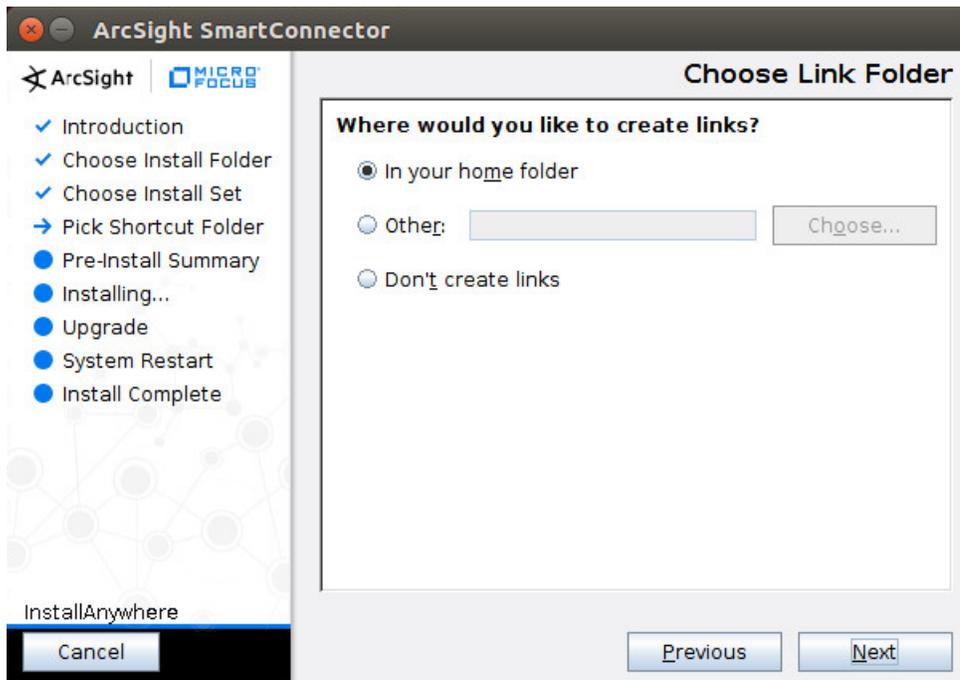
### 1330 2.8.3 Install Individual ArcSight Ubuntu Connectors

- 1331 1. From the command line, run:  
1332 > `sudo ./ArcSight-7.9.0.8084.0-Connector-Linux64.bin`
- 1333 2. Enter the **password** if prompted.



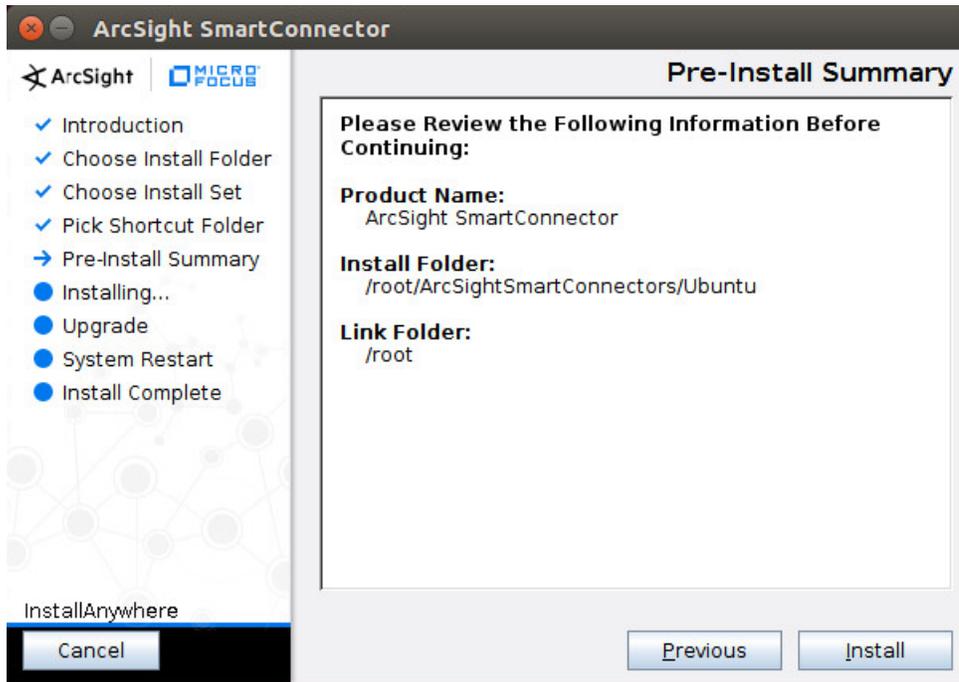
1334  
1335  
1336  
1337  
1338

3. Click **Next**.
4. Enter `/root/ArcSightSmartConnectors/Ubuntu`.
5. Click **Next**.



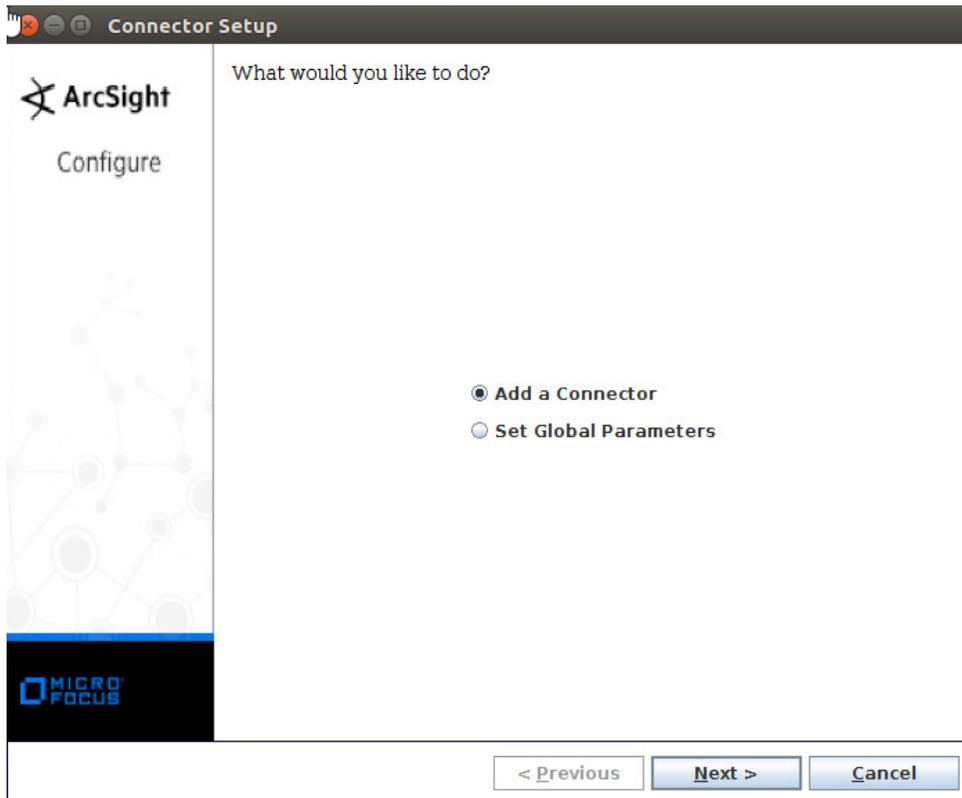
1339

1340 6. Click **Next**.



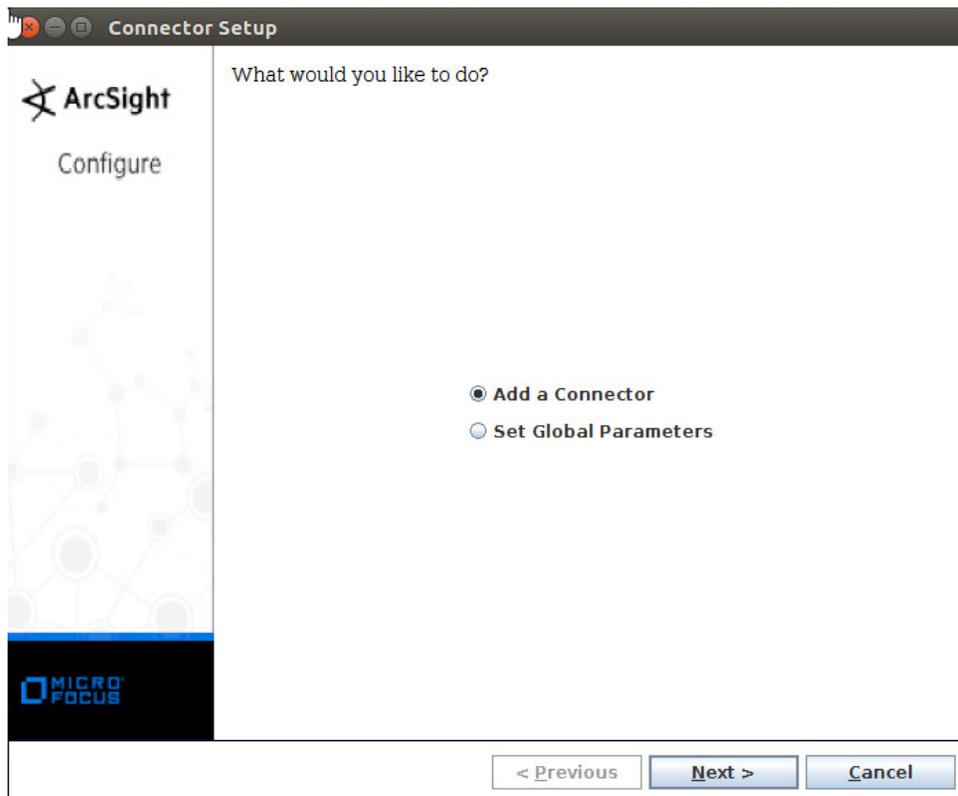
1341 7. Click **Install**.

1342 8. Select **Add a Connector**.



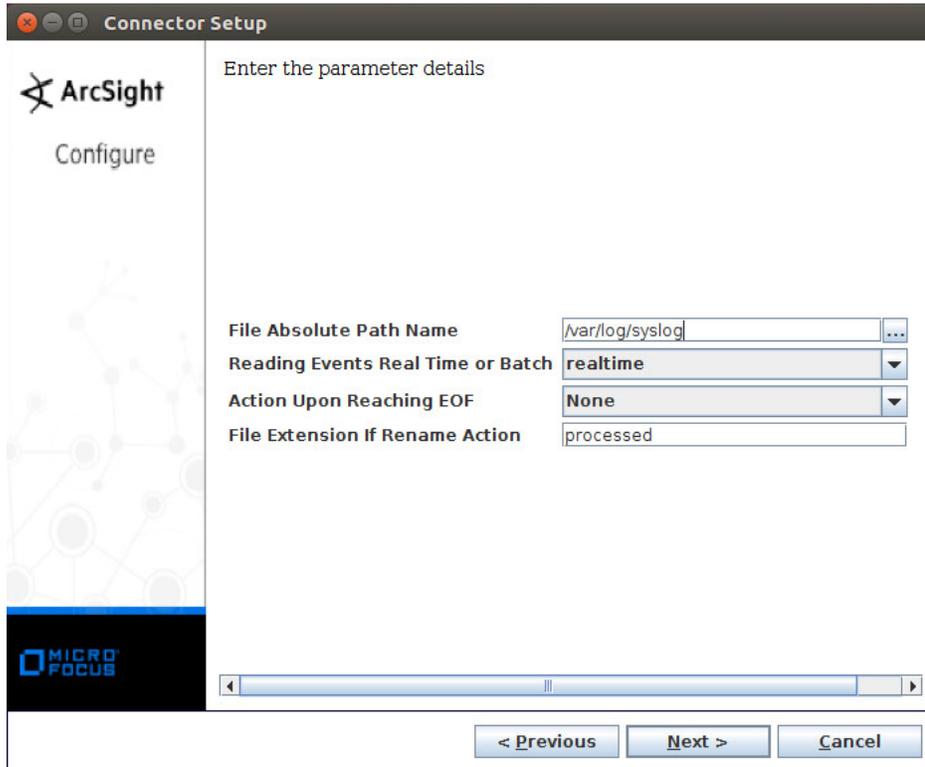
1344  
1345  
1346

9. Click **Next**.
10. Select **Syslog File**.



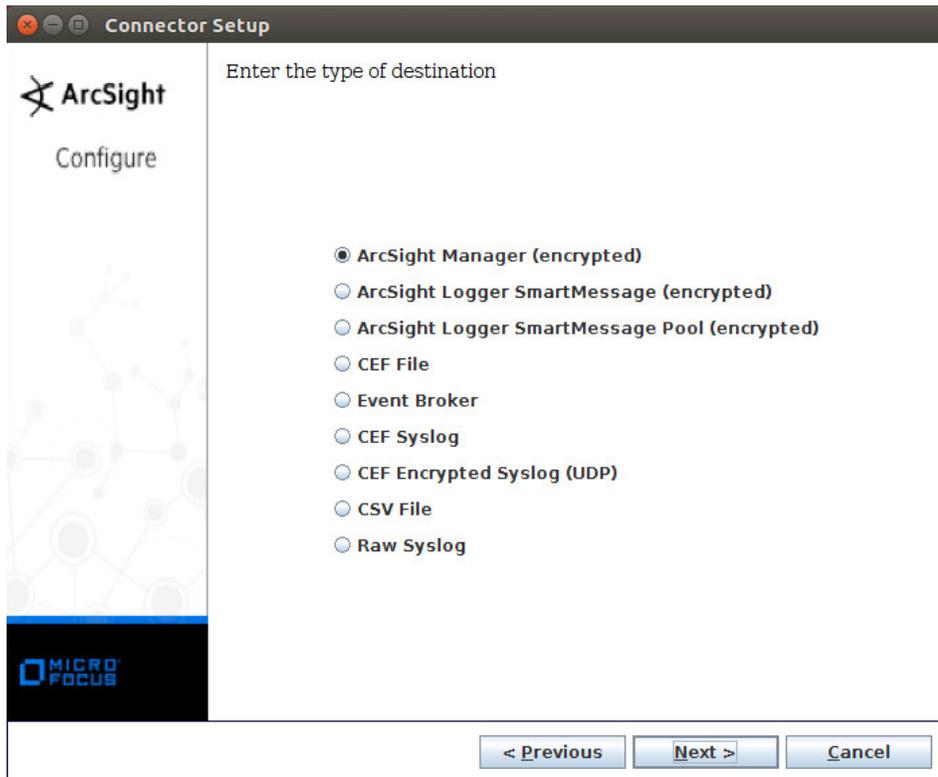
1347  
1348  
1349

11. Click **Next**.
12. Enter `/var/log/syslog` for the File Absolute Path Name.



1350  
1351  
1352

- 13. Click **Next**.
- 14. Select **ArcSight Manager (encrypted)**.



1353  
1354  
1355

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

Connector Setup

ArcSight  
Configure

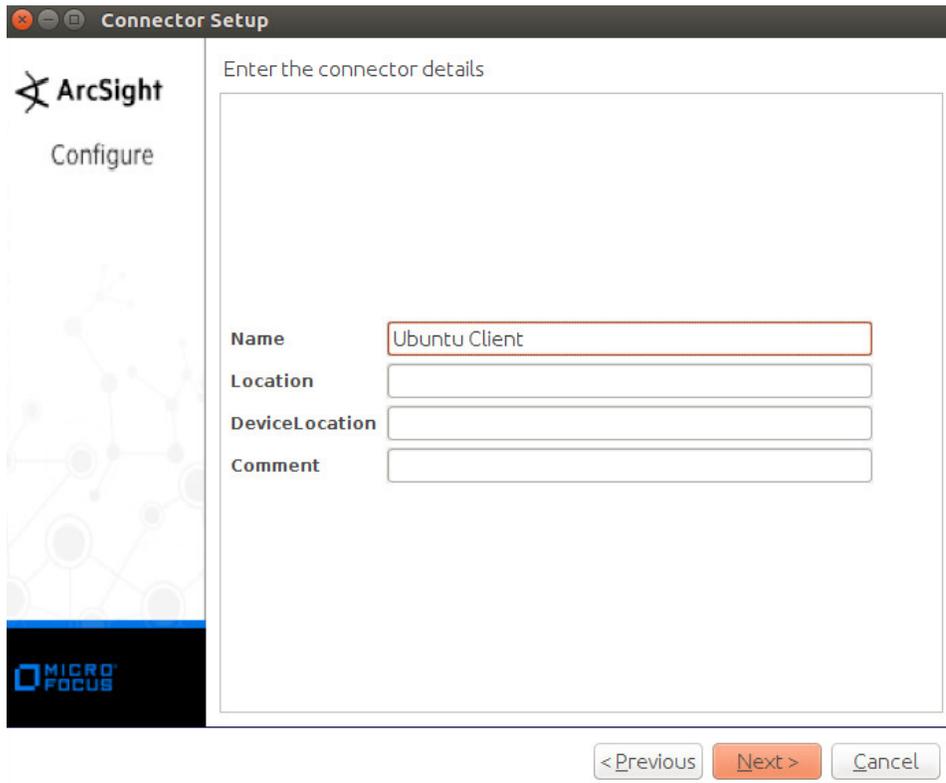
Enter the destination parameters

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

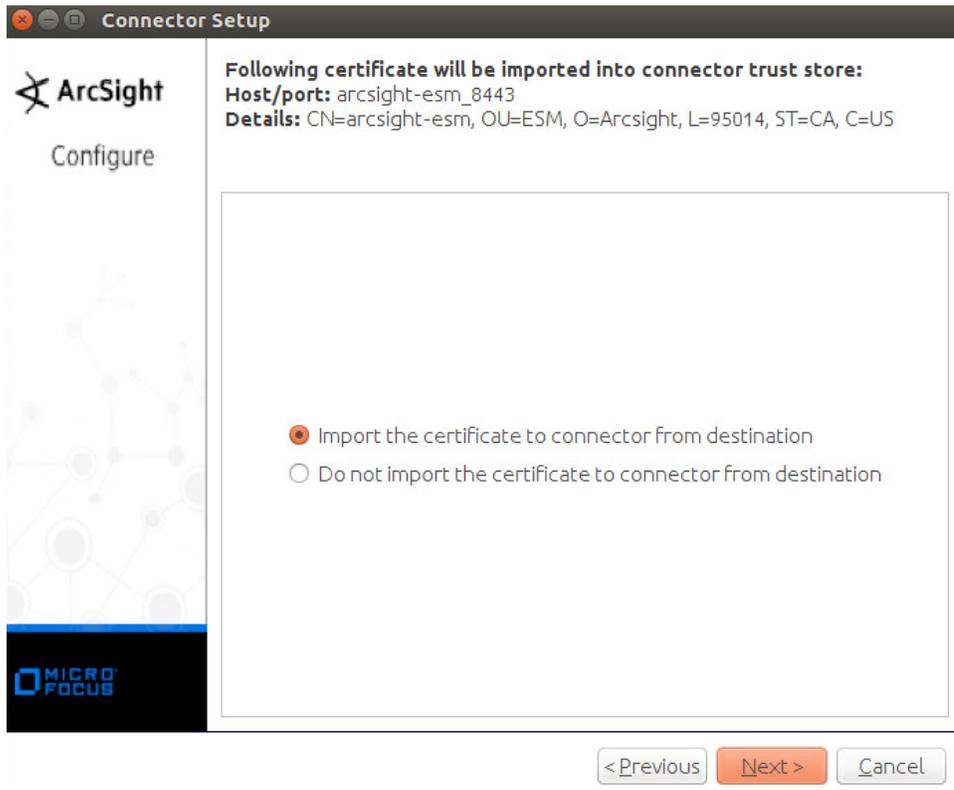
1356  
1357  
1358

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



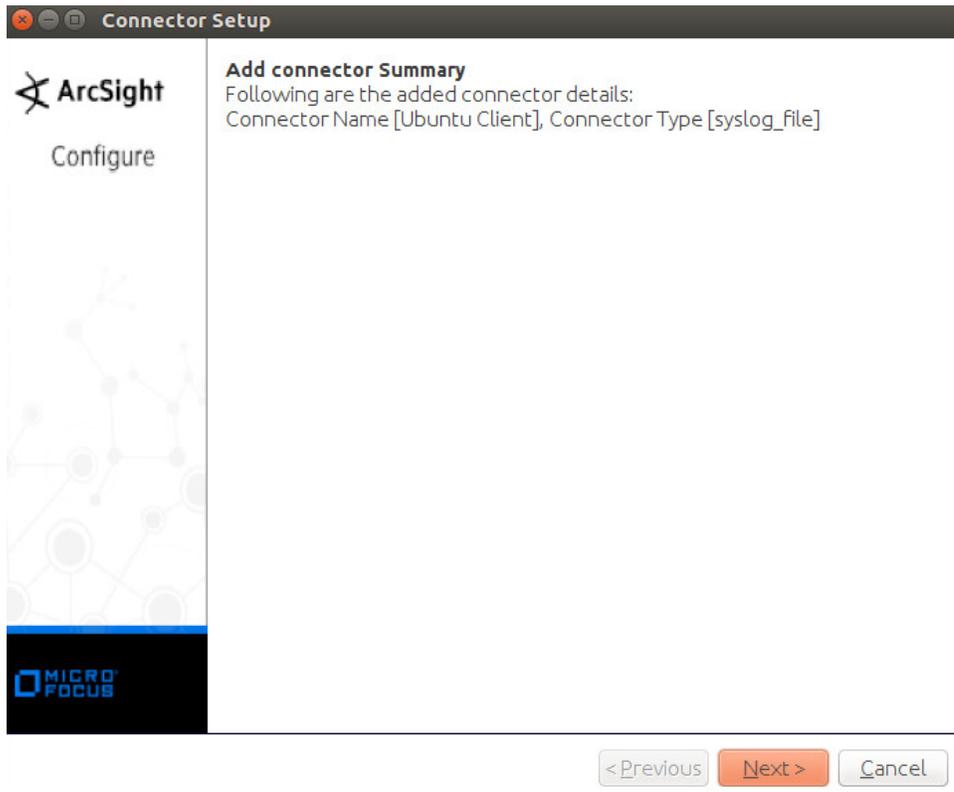
1359  
1360  
1361

19. Click **Next**.
20. Select **Import the certificate to connector from destination**.



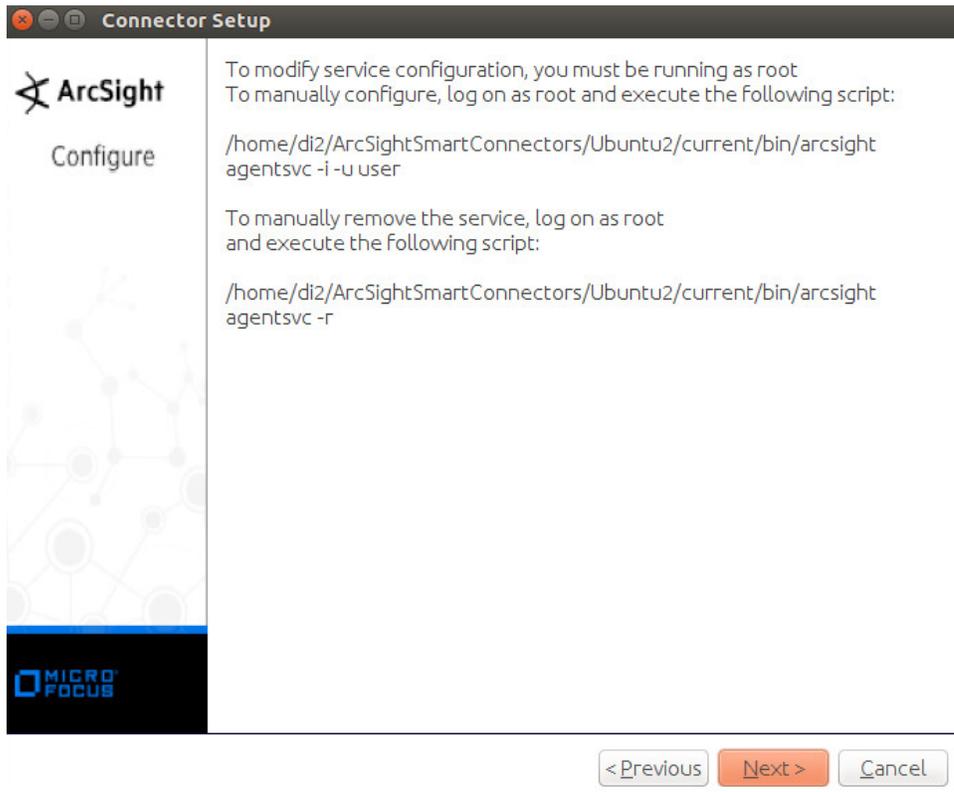
1362  
1363

21. Click **Next**.



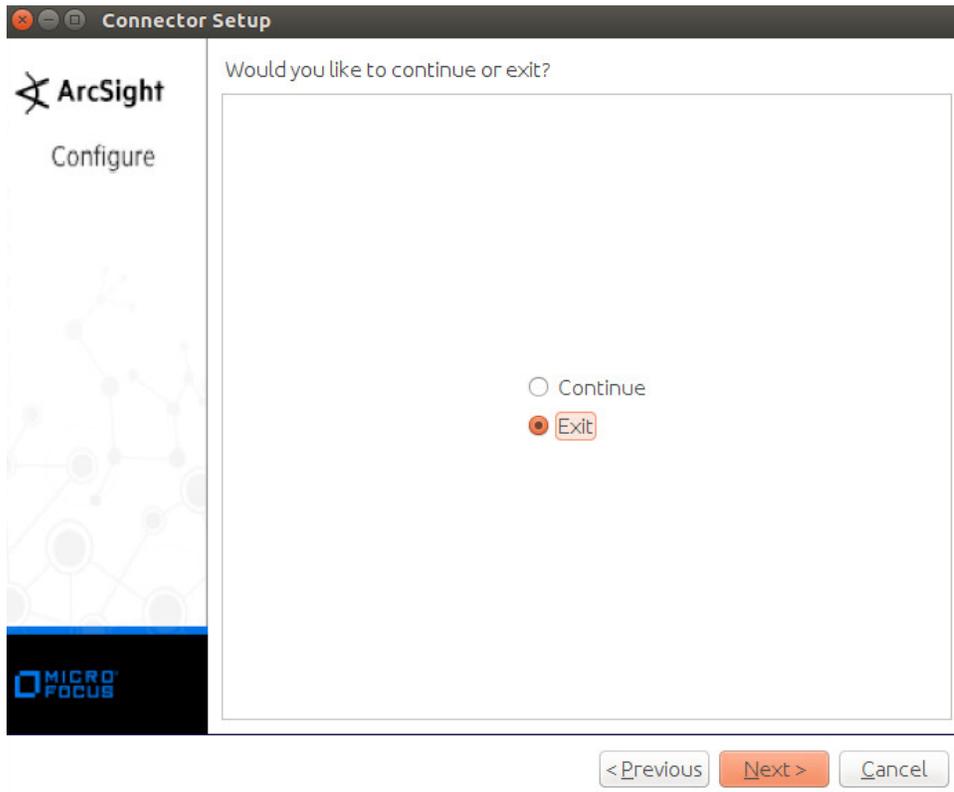
1364  
1365

22. Click **Next**.



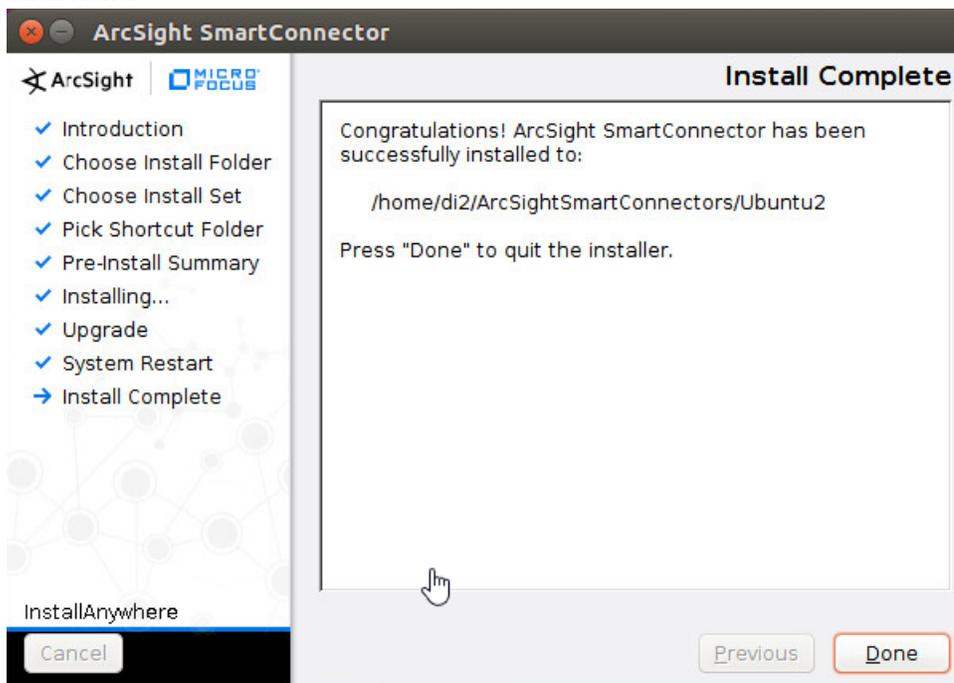
1366  
1367  
1368

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



1369  
1370

25. Click **Next**.

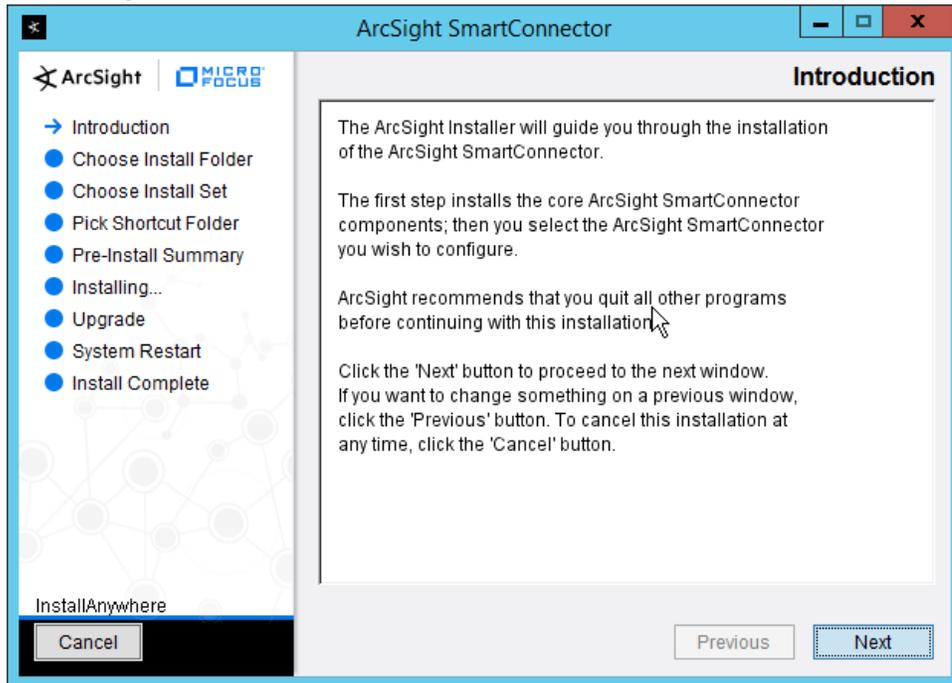


1371

1372 26. Click **Done**.

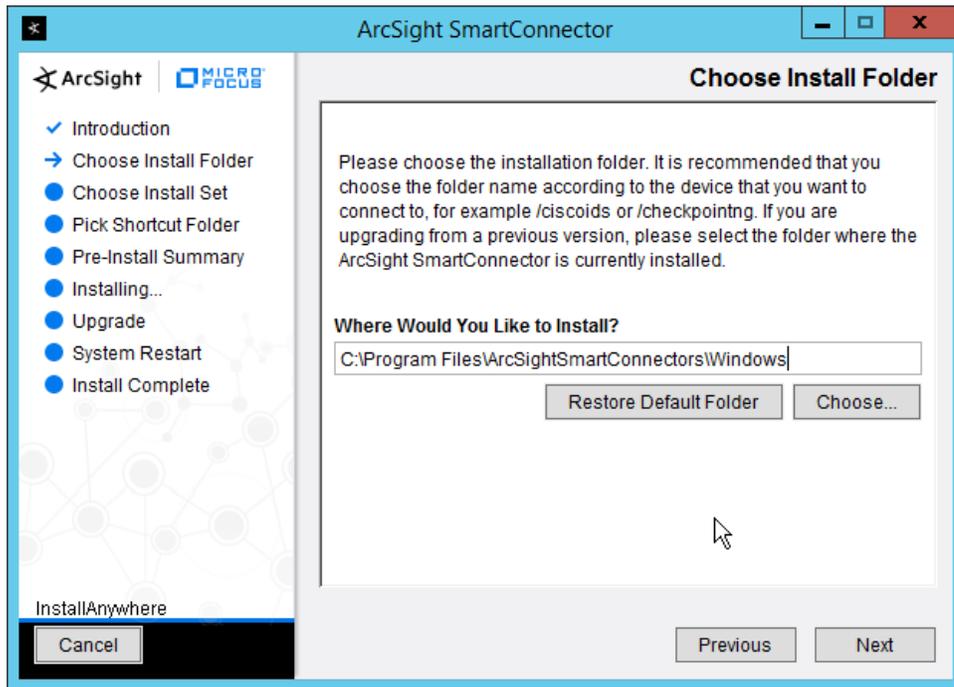
## 1373 2.8.4 Install a Connector Server for ESM on Windows 2012 R2

1374 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.



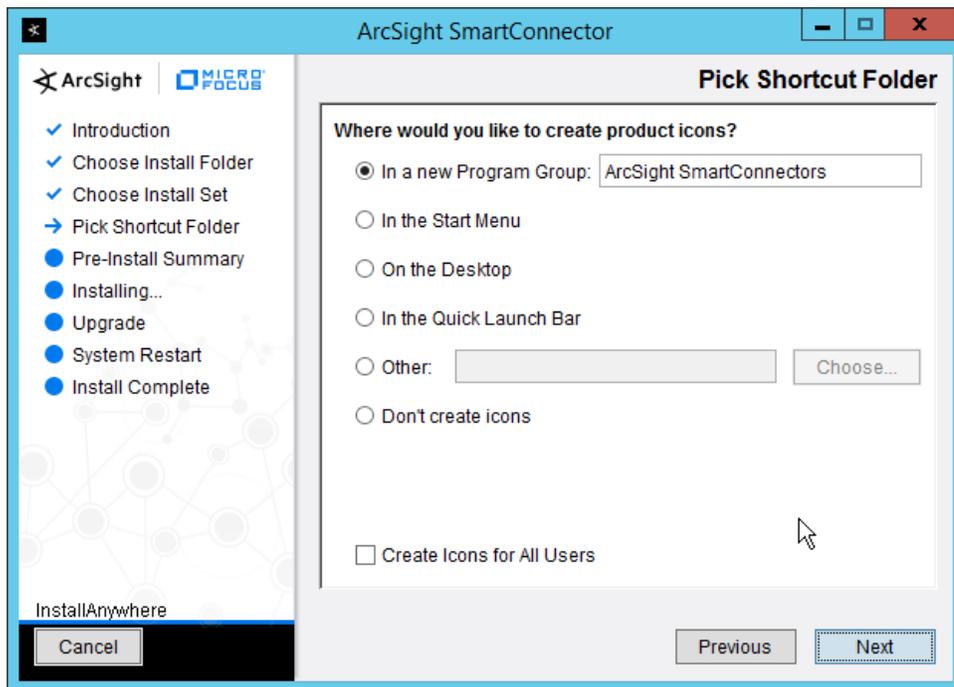
1375 2. Click **Next**.

1376 3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows*.



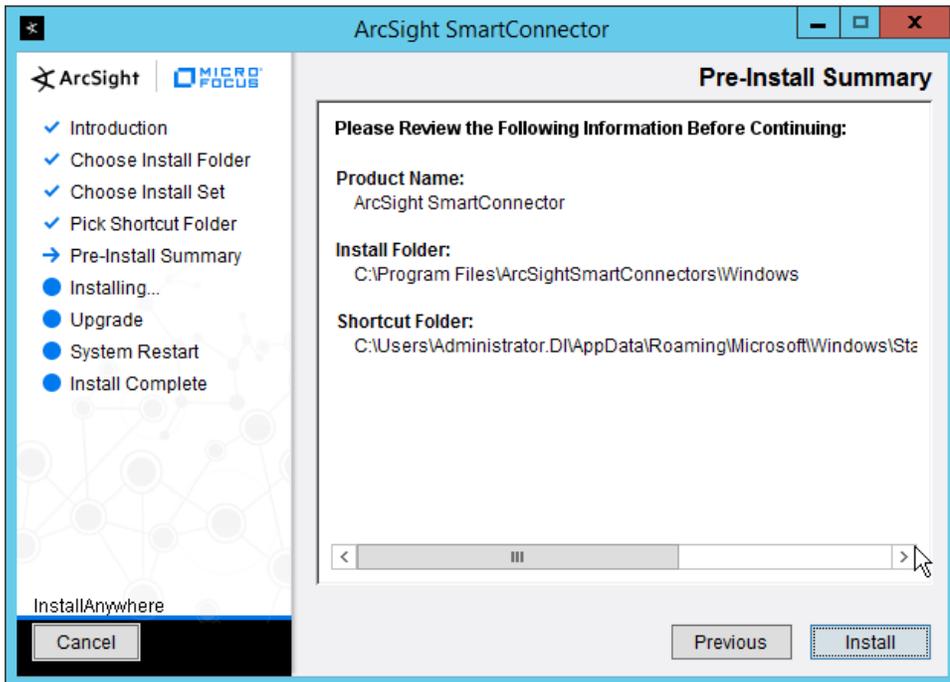
1378  
1379

4. Click **Next**.



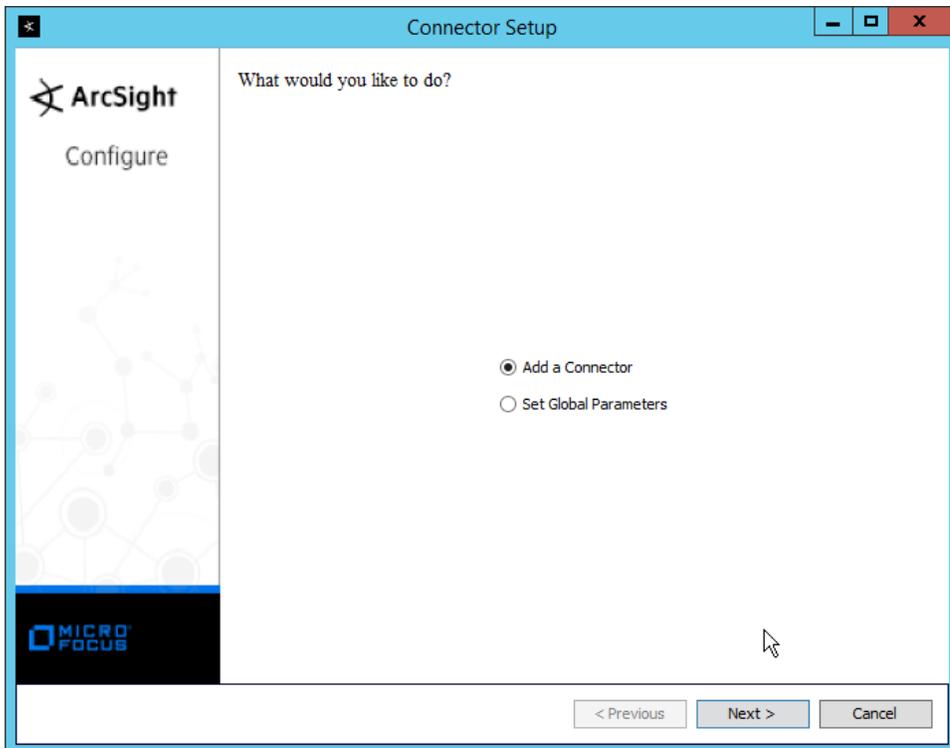
1380  
1381

5. Click **Next**.



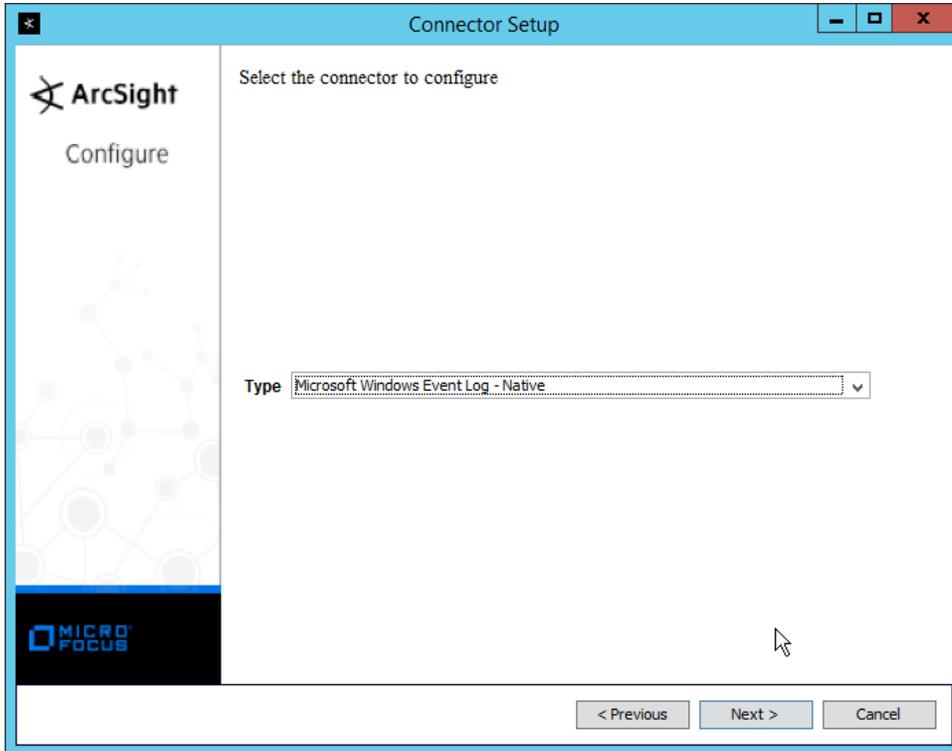
1382  
1383  
1384

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

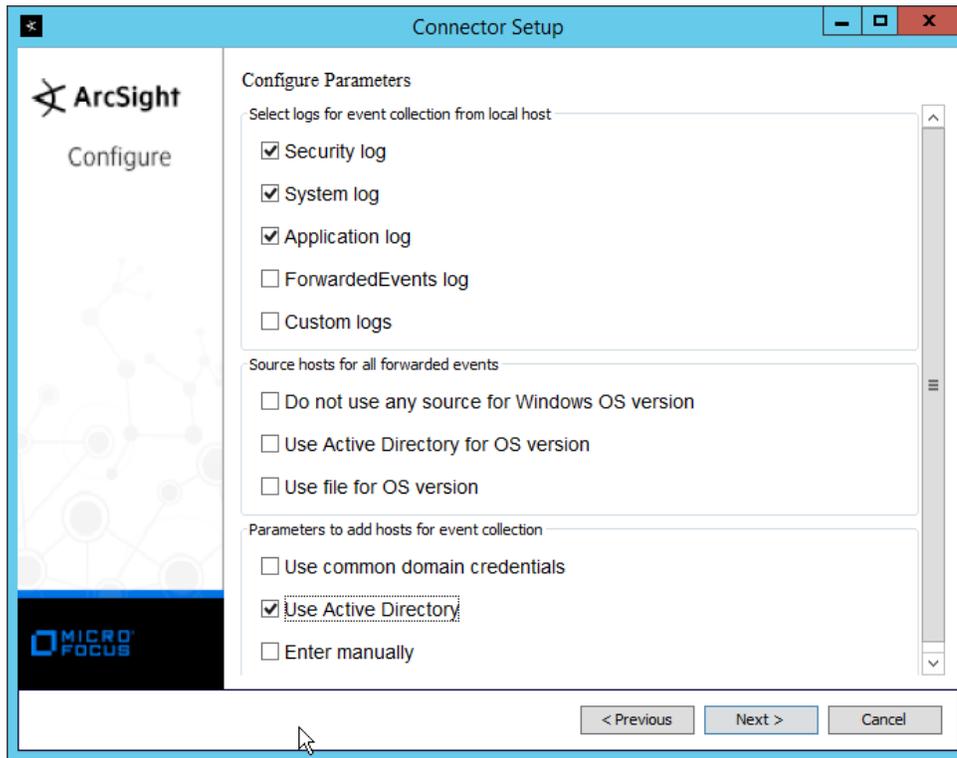


1385

- 1386 8. Click **Next**.
- 1387 9. Select **Microsoft Windows Event Log – Native**.

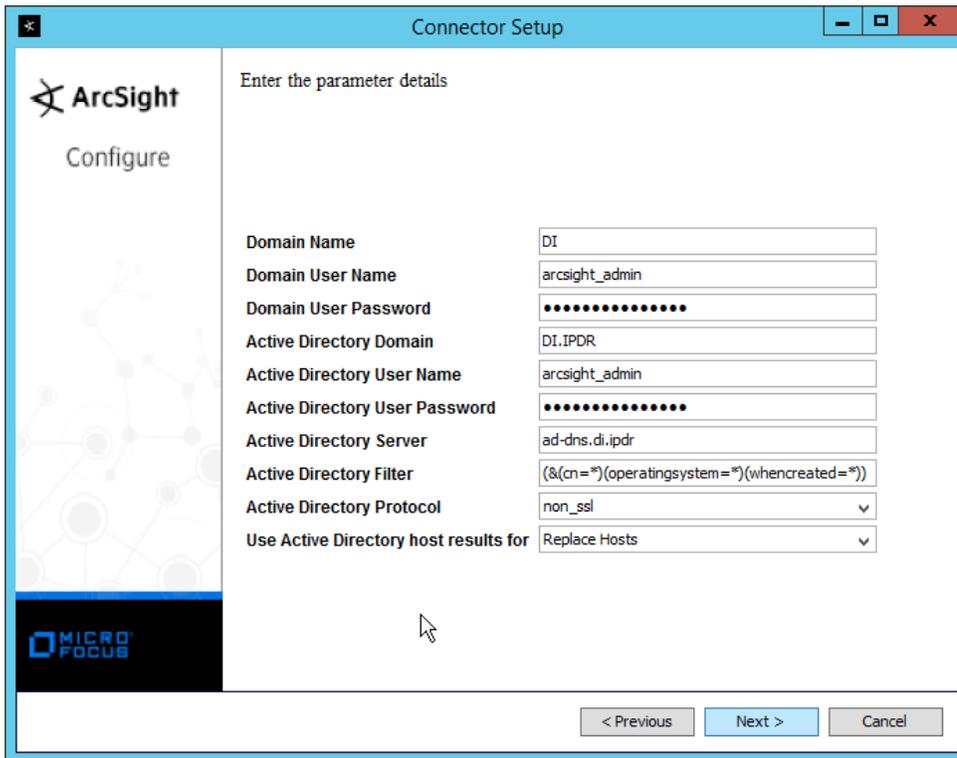


- 1388 10. Click **Next**.
- 1389 11. Check the box next to **Use Active Directory**.
- 1390



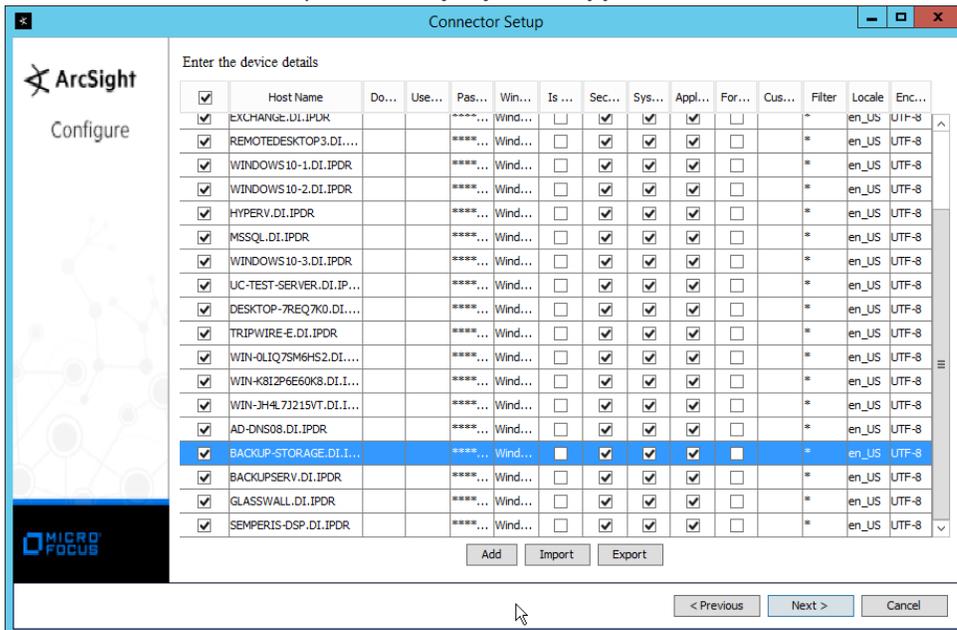
1391  
1392  
1393  
1394  
1395

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**.



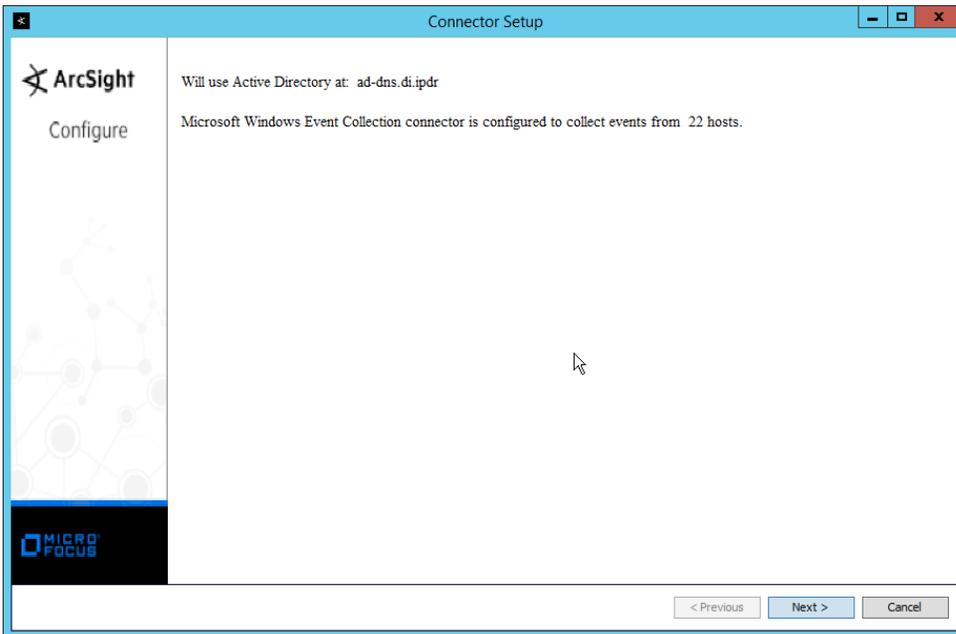
1396  
1397  
1398  
1399

15. Click **Next**.
16. Check the boxes under any event types that should be forwarded to this connector, for each individual host. For example: **Security, System, Application**.



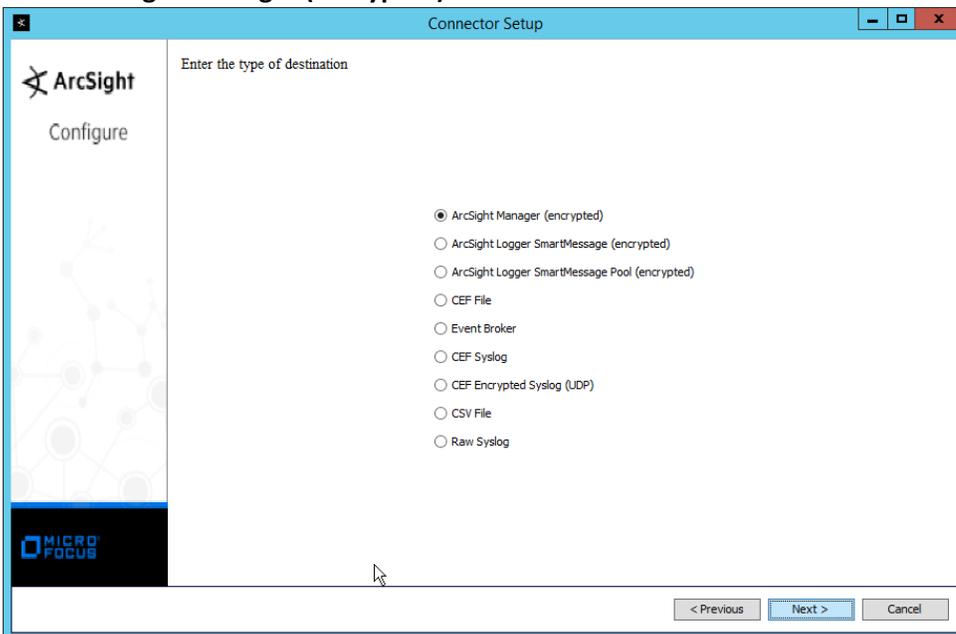
1400

1401 17. Click **Next**.



1402 18. Click **Next**.

1403 19. Select **ArcSight Manager (encrypted)**.



1405 20. Click **Next**.

1406 21. Enter the **hostname, port, username, and password** for the ArcSight ESM server.

The screenshot shows the 'Connector Setup' window with the title bar 'Connector Setup'. On the left is the ArcSight logo and 'Configure' text. The main area is titled 'Enter the destination parameters'. It contains the following fields:

- Manager Hostname:
- Manager Port:
- User:
- Password:
- AUP Master Destination:
- Filter Out All Events:
- Enable Demo CA:

At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'. The Micro Focus logo is in the bottom left corner.

1408  
1409  
1410

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

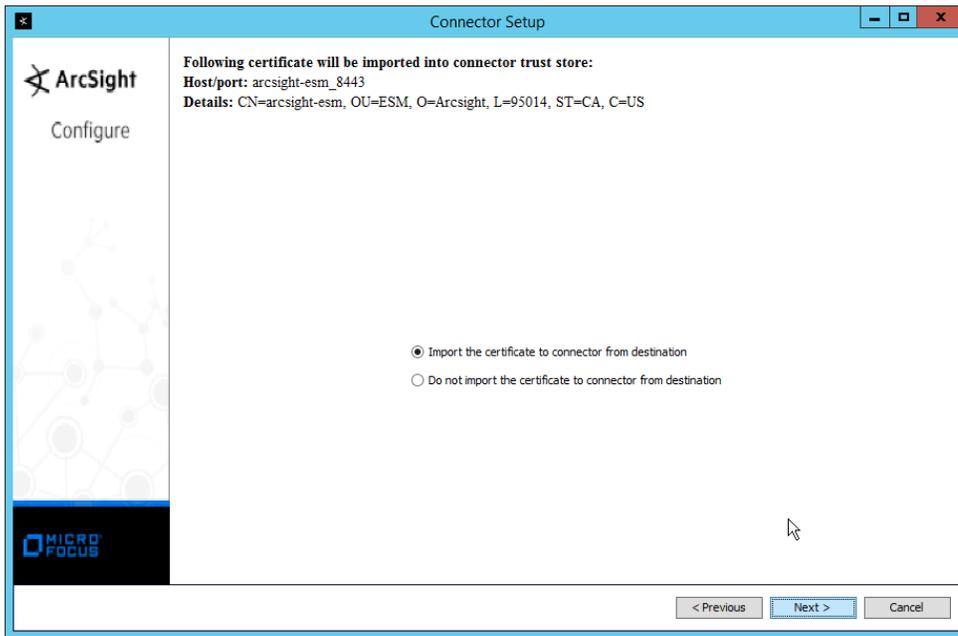
The screenshot shows the 'Connector Setup' window with the title bar 'Connector Setup'. On the left is the ArcSight logo and 'Configure' text. The main area is titled 'Enter the connector details'. It contains the following fields:

- Name:
- Location:
- DeviceLocation:
- Comment:

At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'. The Micro Focus logo is in the bottom left corner.

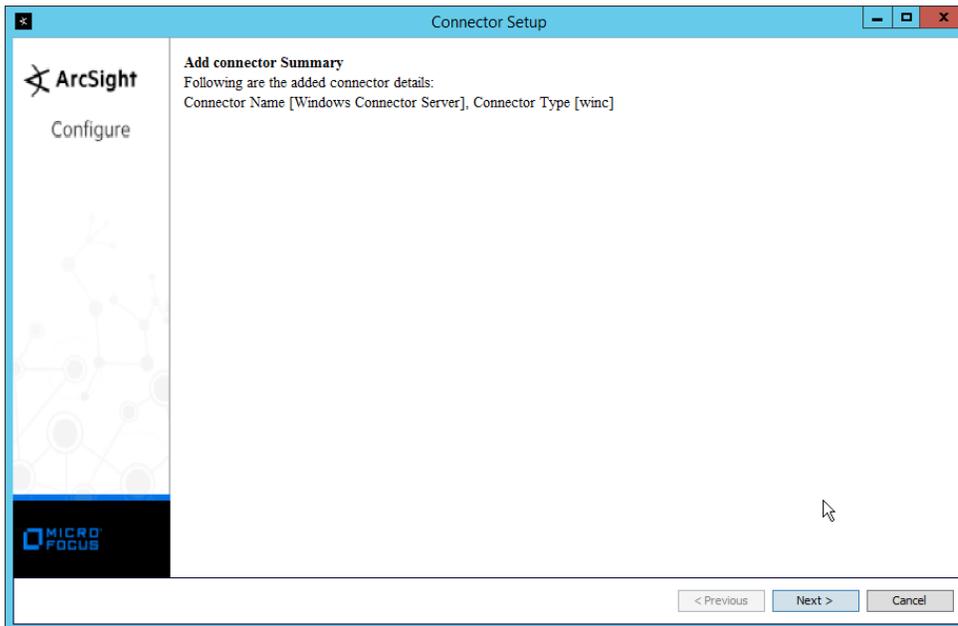
1411  
1412  
1413

- 24. Click **Next**.
- 25. Select **Import the certificate to connector from destination**.



1414  
1415

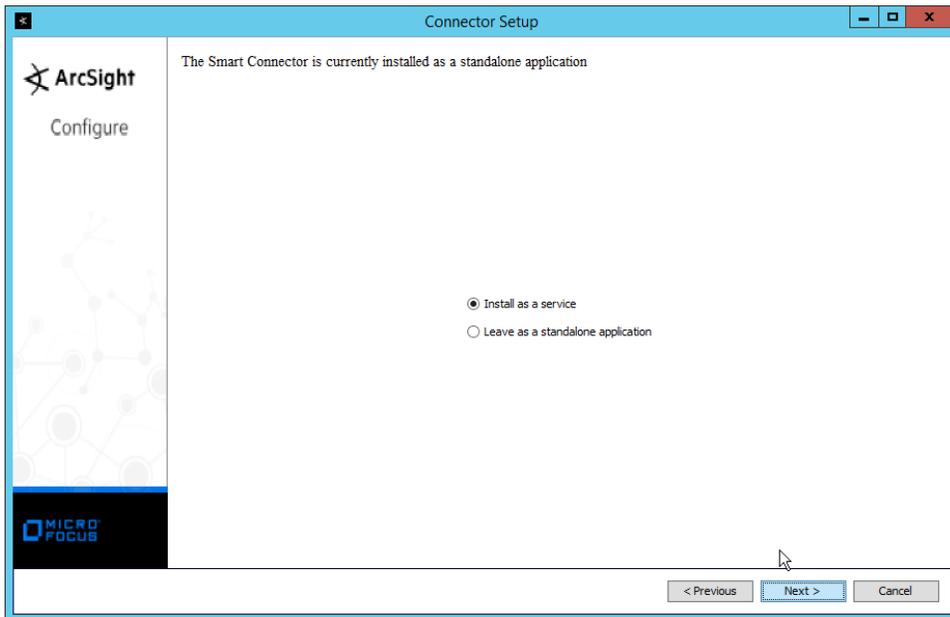
26. Click **Next**.



1416  
1417  
1418

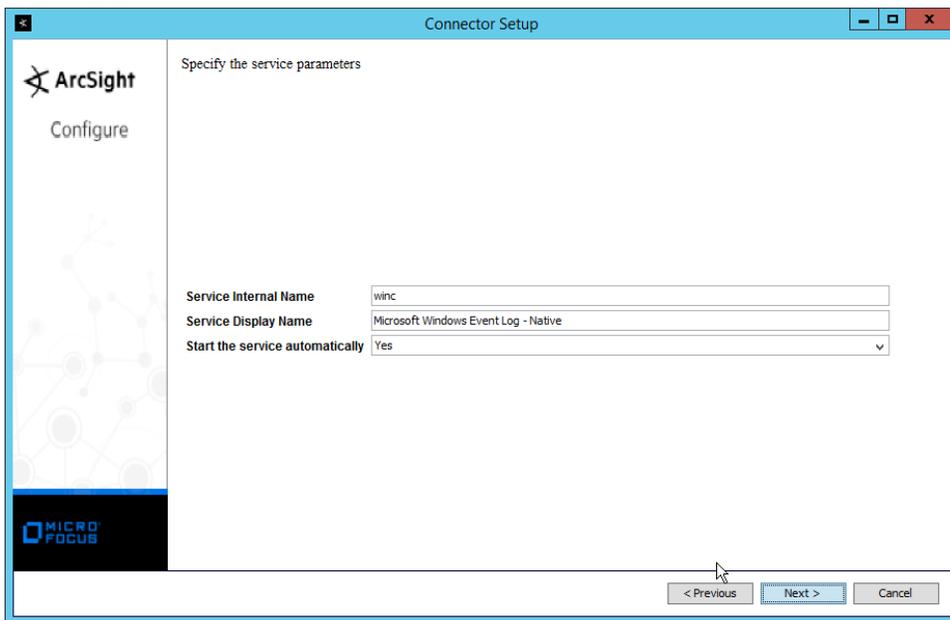
27. Click **Next**.

28. Select **Install as a service**.



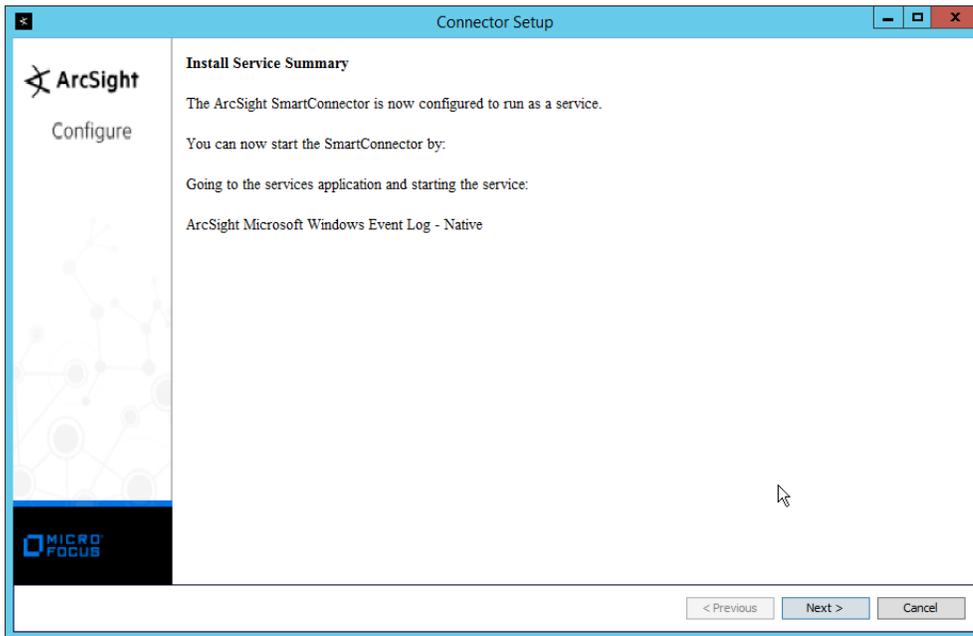
1419  
1420

29. Click **Next**.



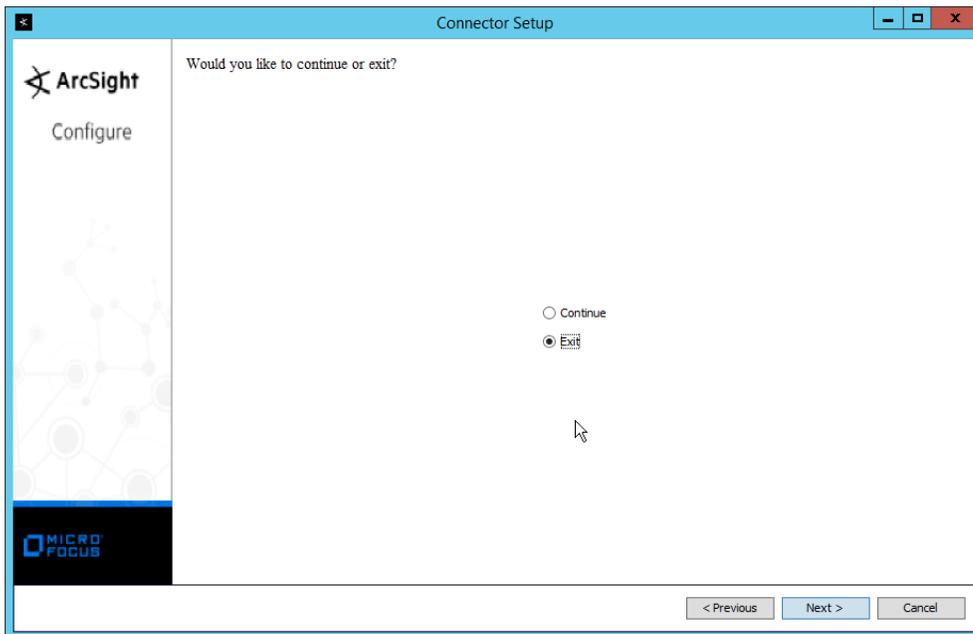
1421  
1422

30. Click **Next**.



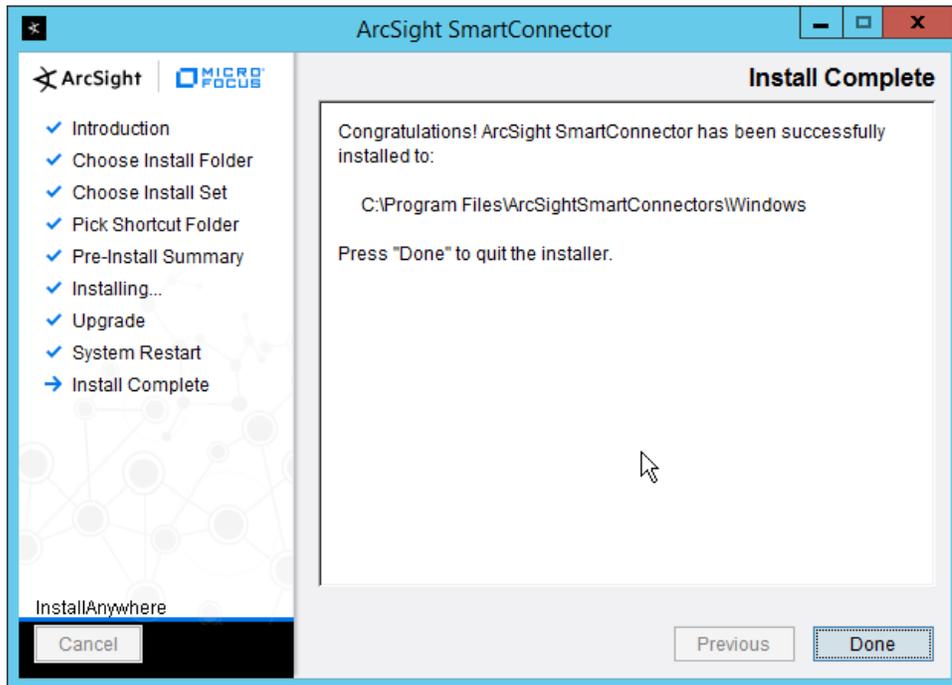
1423  
1424  
1425

- 31. Click **Next**.
- 32. Select **Exit**.



1426  
1427

- 33. Click **Next**.



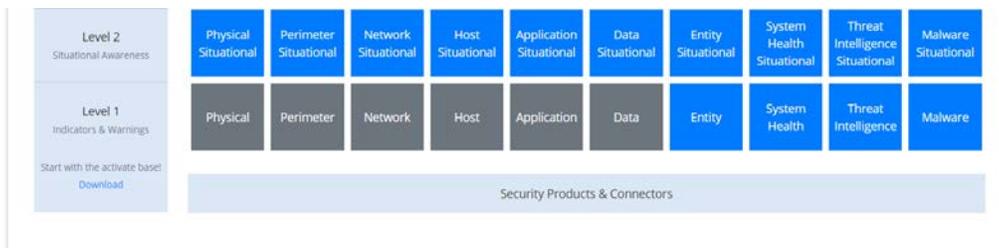
1428  
1429  
1430  
1431

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

## 1432 2.8.5 Install Pre-Configured Filters for ArcSight

### 1433 2.8.5.1 *Install Activate Base*

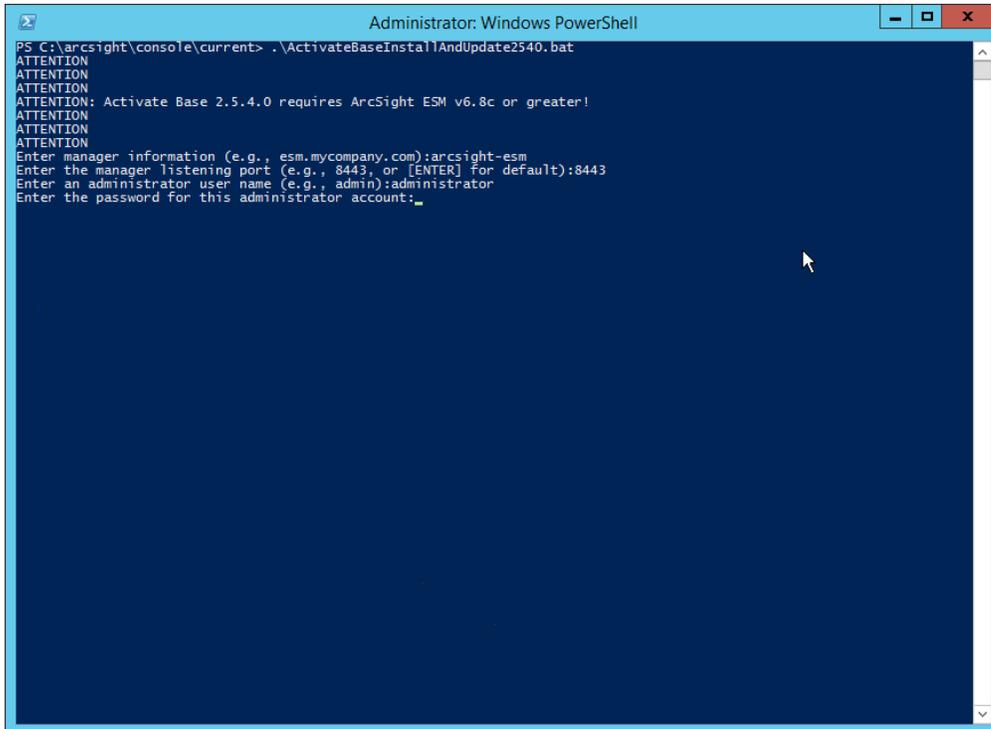
1. Go to the ArcSight Content Brain web app (<https://arcsightcontentbrain.com/app/>) and log in. This page allows you to keep track of packages to be installed—which packages should be installed is dependent on the needs of the organization, but the “activate base” is required for all products.



1438  
1439  
1440  
1441  
1442

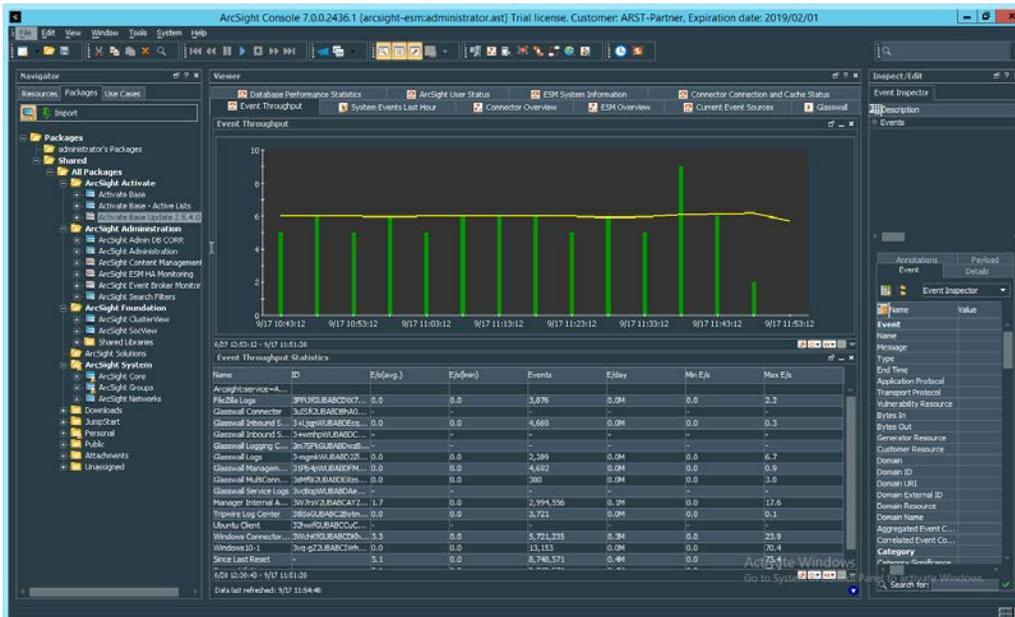
2. Click the **Download** link for the activate base. (Note: This package should be installed on the Arcsight Console, not on the ESM.)
3. Copy the contents of the zip file to `ARCSIGHT_HOME`. The default for this is `C:\arcsight\Console\current`, assuming a Windows Server.

- 1443 4. In PowerShell, navigate to the *ARCSIGHT\_HOME* directory (*C:\arcsight\Console\current*), and  
1444 run:  
1445 > `.\ActivateBaseInstallAndUpdate2540.bat`



```
Administrator: Windows PowerShell
PS C:\arcsight\console\current> .\ActivateBaseInstallAndUpdate2540.bat
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: _
```

- 1446 5. Enter the **hostname** of the ArcSight machine, the **port** (default: **8443**), and the **username** and  
1447 **password** used to connect to the **ESM**.  
1448  
1449 6. Delete **Activate\_Base\_Updated\_2.5.4.0.arb** from the *ARCSIGHT\_HOME* directory.  
1450 7. Log in to **ArcSight Console**.



- 1451  
1452 8. Under **Packages > Shared > All Packages > ArcSight Activate**, right-click **Activate Base Update**  
1453 **2.5.4.0**, and select **Delete Package**.

1454 **2.8.5.2 Install Packages**

1455 Once the Activate Base is installed, packages can be installed to monitor for specific types of events. As  
1456 an example, find below instructions for the Malware Monitoring package.

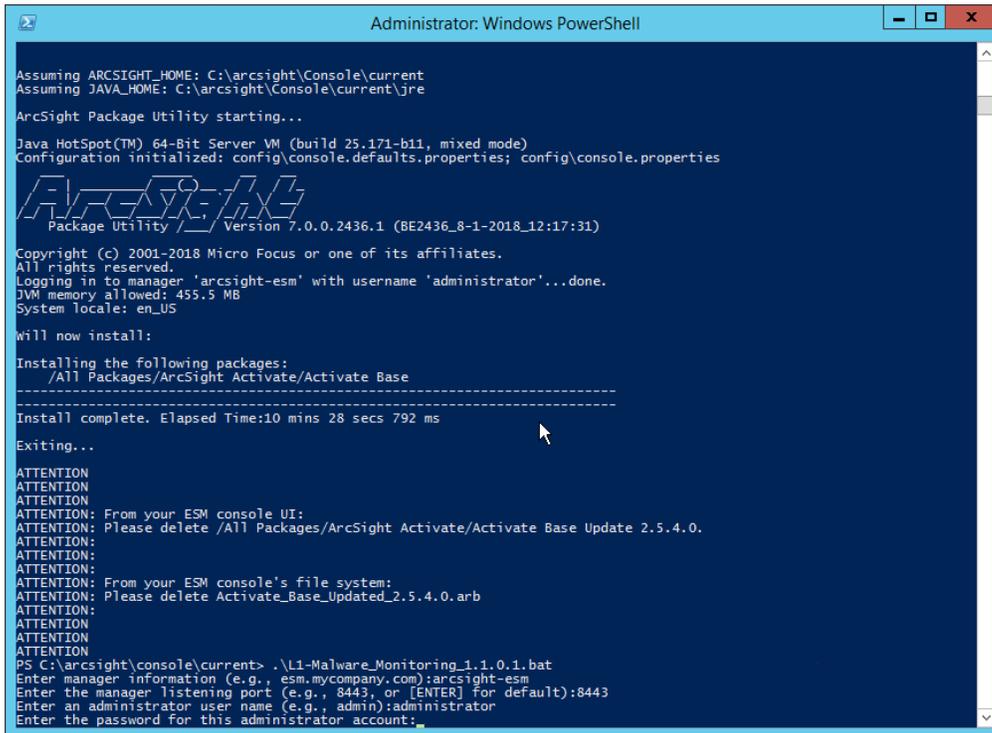
- 1457 1. Navigate to the **ArcSight Content Brain** web app.  
1458 2. Select the **Level 1** box labeled **Malware**.



- 1459  
1460 3. In the **Track Execution** section, under **Associated Packages**, you can see the list of packages  
1461 used to address the challenge of “Malware Monitoring.” In this case, there is just one package,  
1462 “L1 – Malware Monitoring – Indicators and Warnings.” Click the link to be taken to a download  
1463 page for the package, and download it. (Note: This package should be installed on the Arcsight  
1464 Console, not on the ESM.)



- 1465 4. Copy the contents of the zip file to *ARCSIGHT\_HOME*. The default for this is *C:\arcsight\Console*  
 1466 *\current*, assuming a Windows Server.  
 1467 5. In PowerShell, navigate to the *ARCSIGHT\_HOME* directory (*C:\arcsight\Console\current*), and  
 1468 run:  
 1469 `> .\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 (BE2436_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...

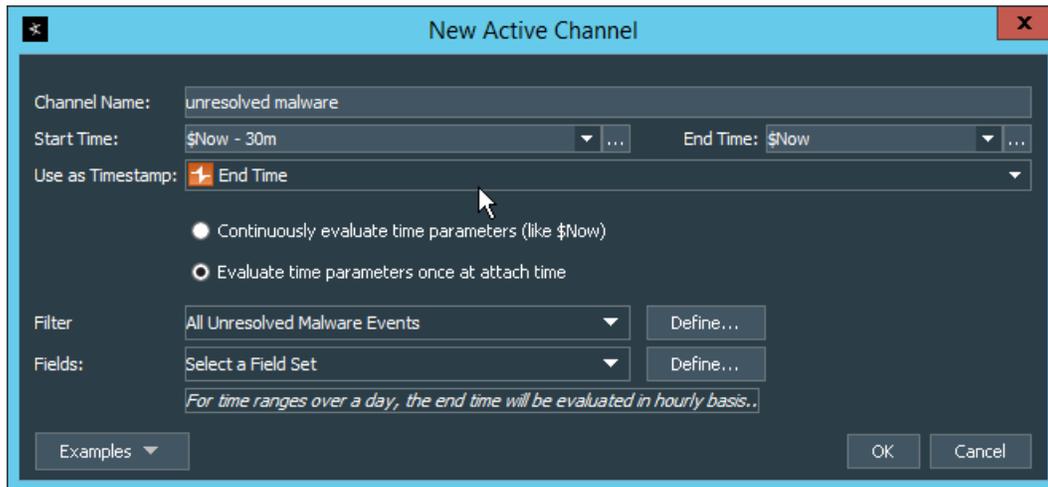
ATTENTION
ATTENTION
ATTENTION
ATTENTION: From your ESM console UI:
ATTENTION: Please delete /All Packages/ArcSight Activate/Activate Base Update 2.5.4.0.
ATTENTION:
ATTENTION:
ATTENTION: From your ESM console's file system:
ATTENTION: Please delete Activate_Base_Updated_2.5.4.0.arb
ATTENTION:
ATTENTION
ATTENTION
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:

```

- 1470  
 1471 6. Enter the **hostname** of the ArcSight machine, the **port** (default: **8443**), and the **username** and  
 1472 **password** used to connect to the **ESM**.

## 1473 2.8.6 Apply Filters to a Channel

- 1474 1. In the **ArcSight Console**, click **File > New > Active Channel**.  
 1475 2. Enter a **name** for the channel.  
 1476 3. Select a time frame.  
 1477 4. For **Filter**, select one the filters that was imported from the packages you installed.



1478  
1479  
1480  
1481

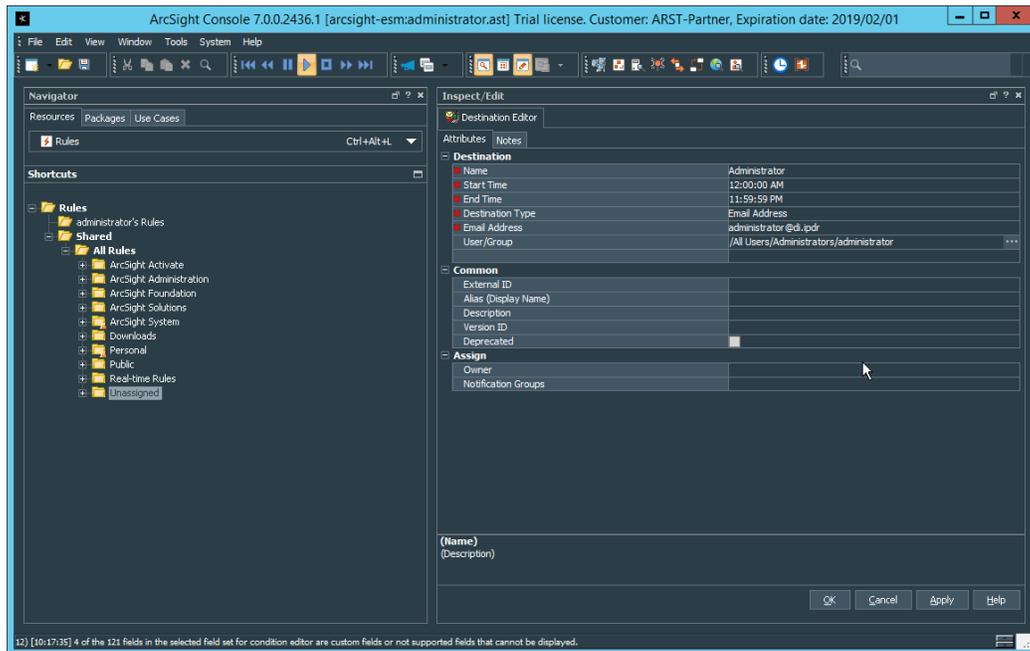
5. Click **OK**. All events that match the filter can be displayed in the newly created channel. Filters from imported packages can be found under **Filters > Shared > All Filters > ArcSight Activate > Solutions**.

## 1482 2.8.7 Configure Email Alerts in ArcSight

### 1483 2.8.7.1 Configure a New Destination

1. In **ArcSight Console**, click **File > New > Destination**.
2. Enter a name for the **Destination**.
3. For **Destination Type**, select **Email Address**.
4. For **Email Address**, enter the email that should be associated with this destination.

1487



1488

1489

1490

1491

5. Click **OK**.
6. Select a place to save the new **Destination**.
7. Click **OK**.

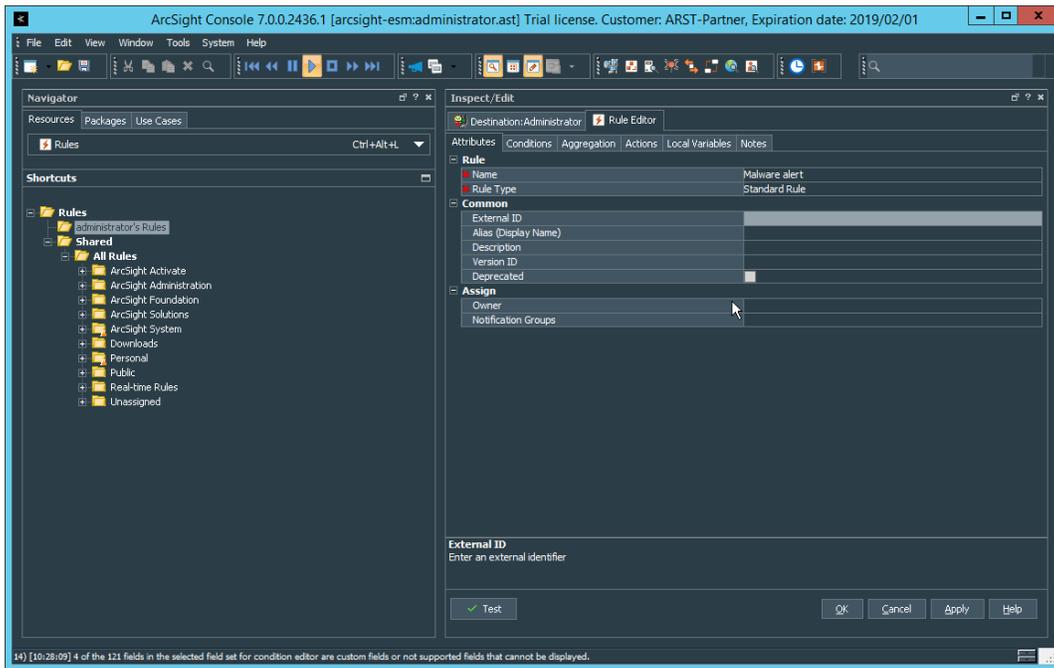
1492

### 2.8.7.2 *Configure a New Rule*

1493

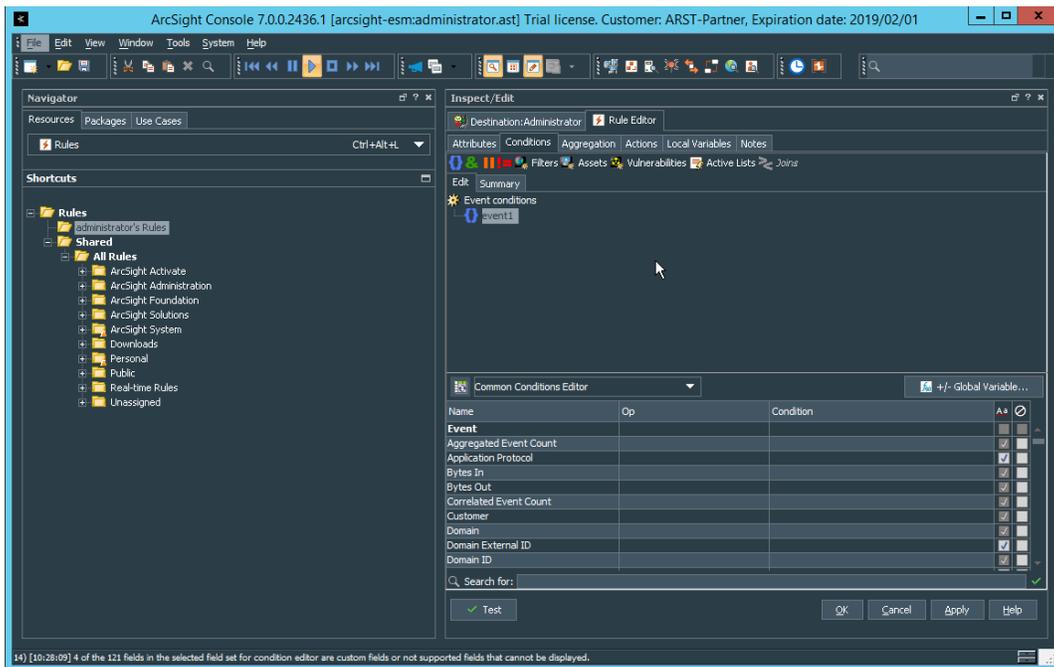
1494

1. Click **File > New > Rule > Standard Rule**.
2. Enter a name for the rule.



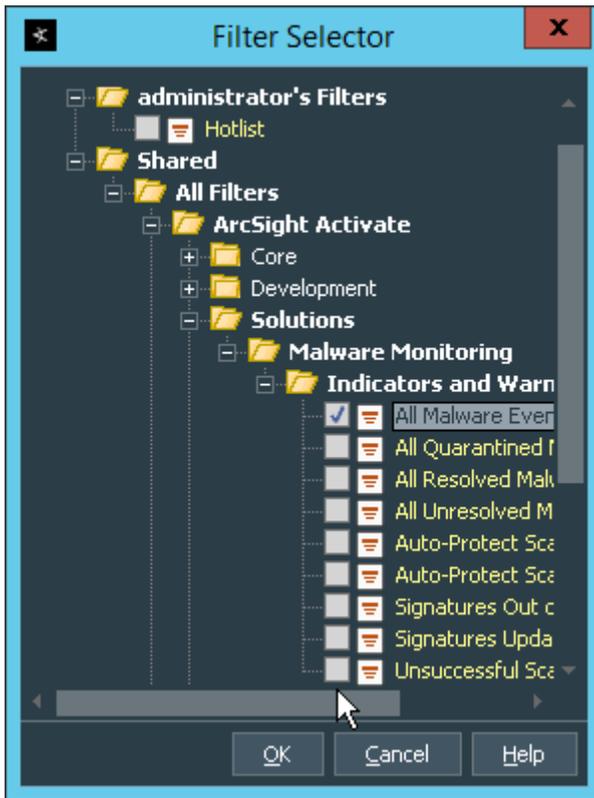
1495  
1496

3. Click the **Conditions** tab.



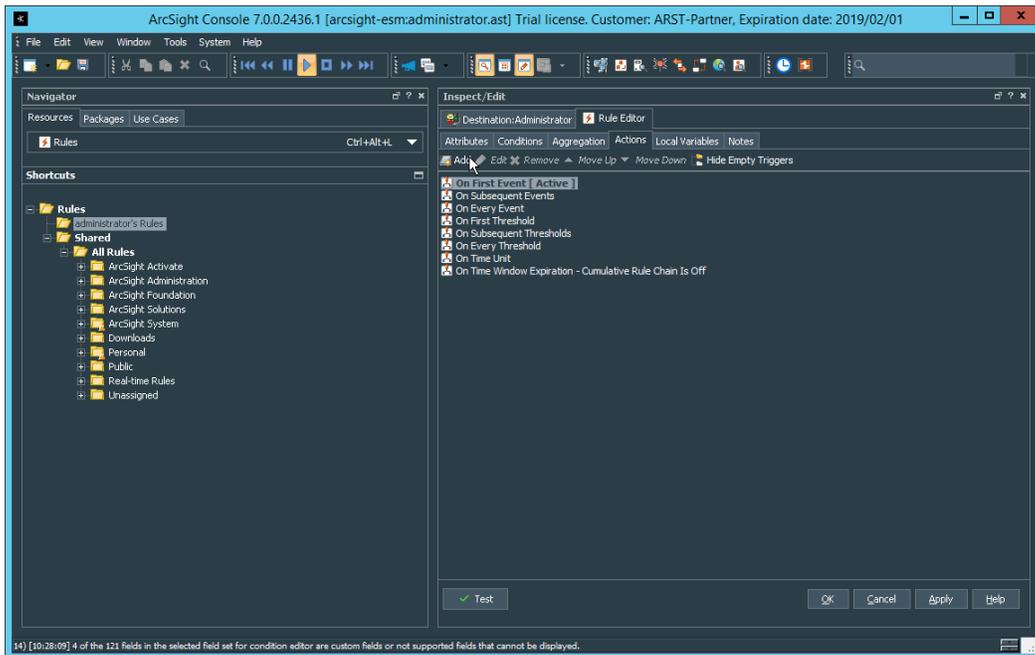
1497  
1498  
1499  
1500

4. Either create a custom condition for the rule or click the **Filters** button to select a pre-configured Filter. (Ensure you check the box next to desired filters if you choose to select a pre-configured filter.)



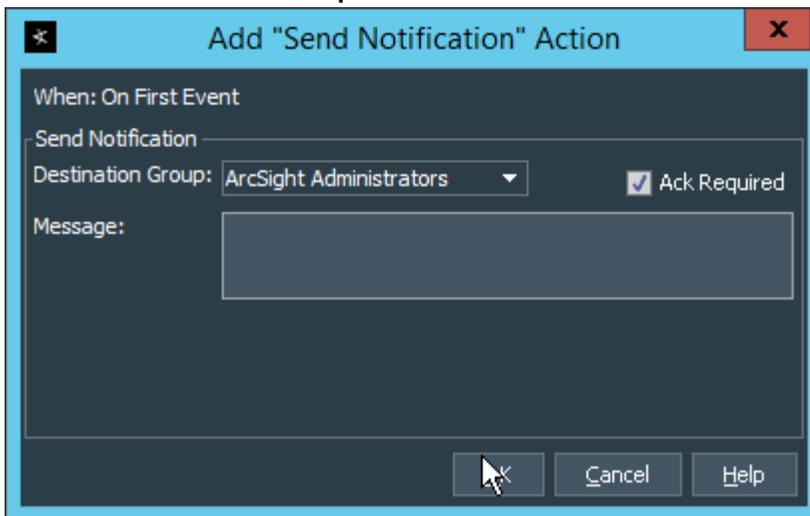
1501  
1502  
1503

5. If you selected a filter, click **OK**.
6. Click the **Actions** tab.



1504  
1505  
1506

7. Select the trigger for the notification, and click **Add > Send Notification**.
8. Select the **Destination Group** in which the desired destinations reside.



1507  
1508

9. Click **OK**.

## 1509 2.9 Tripwire Enterprise

1510 Notes:

1511 This installation requires MSSQL to be installed on a remote server and configured according to the  
1512 instructions in the *Tripwire Enterprise 8.6.2 Installation and Maintenance Guide*.

## 1513 2.9.1 Install Tripwire Enterprise

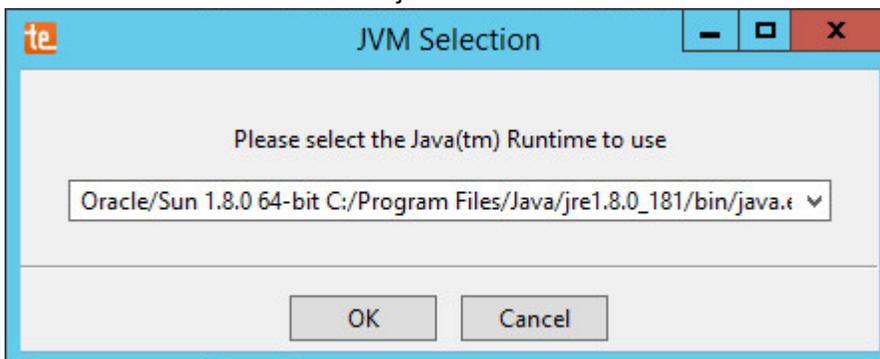
- 1514 1. Ensure that you have a current version of Oracle Java. You must install both the Java Runtime  
 1515 Environment (JRE) and the Java Cryptography Extension (JCE).  
 1516 2. Download and run the **JRE installer**.



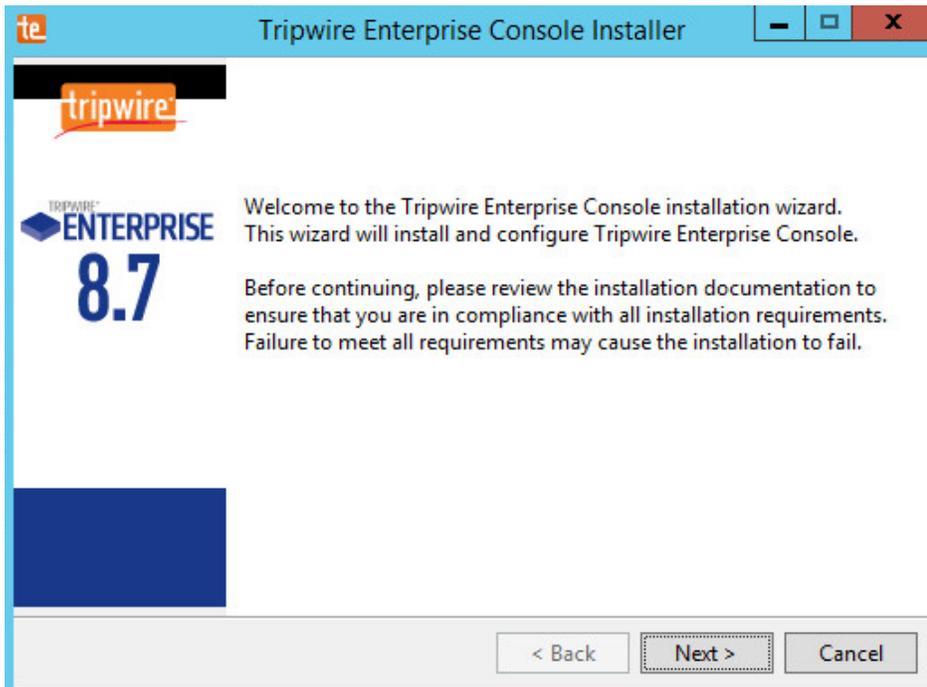
- 1517 3. Click **Install**.  
 1518 4. Download the JCE, and extract the files.  
 1519

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

- 1520 5. Copy the **local\_policy.jar** and **US\_export\_policy.jar** files to */lib/security/Unlimited/* and  
 1521 */lib/security/Limited* in the Java installation directory.  
 1522 6. Run **install-server-windows-amd64**.  
 1523 7. Select the Java runtime that was just installed.  
 1524

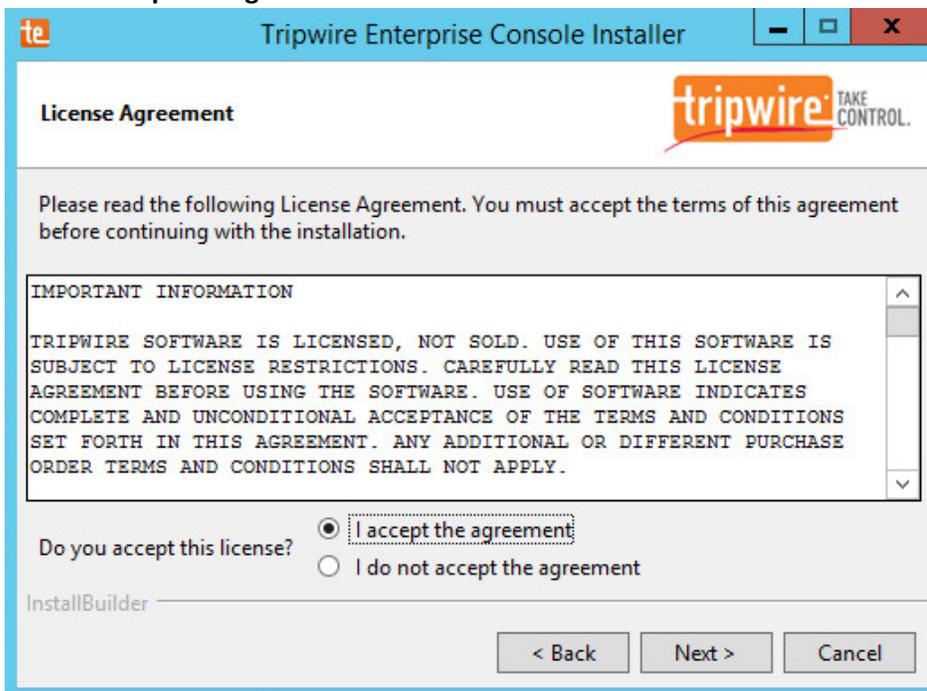


- 1525 8. Click **OK**.  
 1526



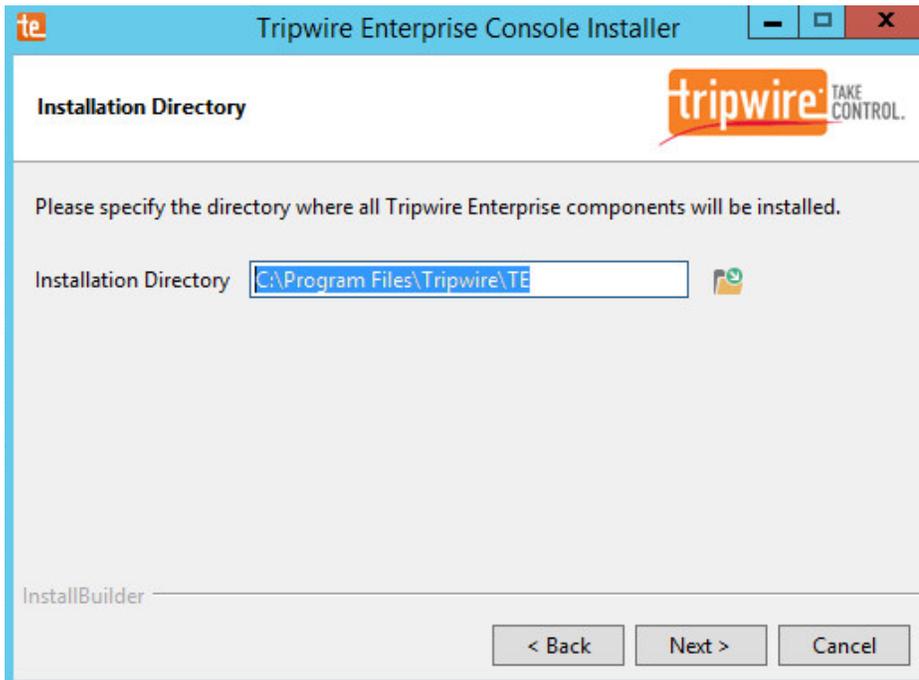
1527  
1528  
1529

- 9. Click **Next**.
- 10. Select **I accept the agreement**.



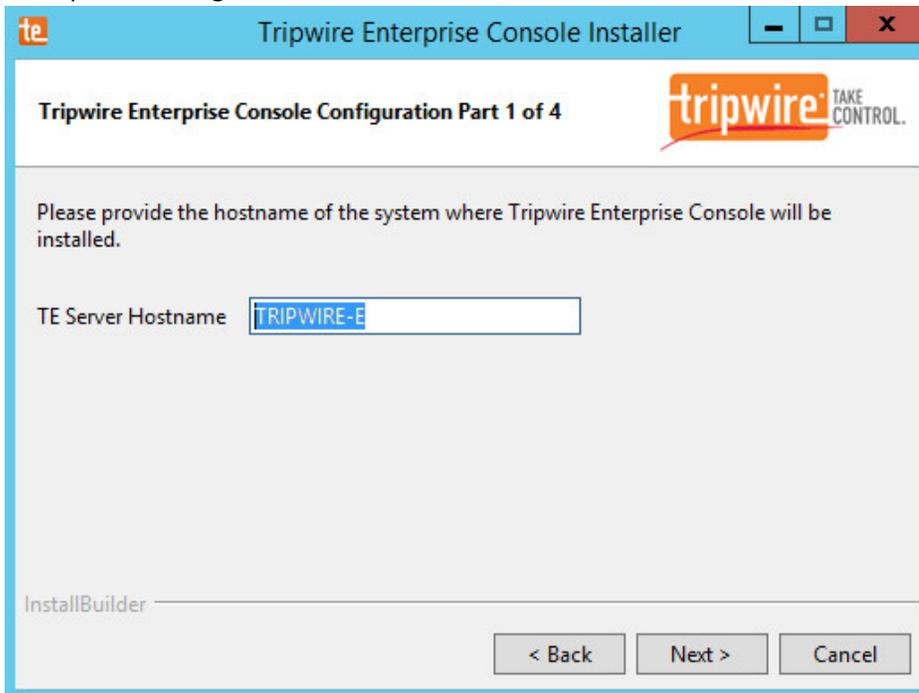
1530  
1531

- 11. Click **Next**.



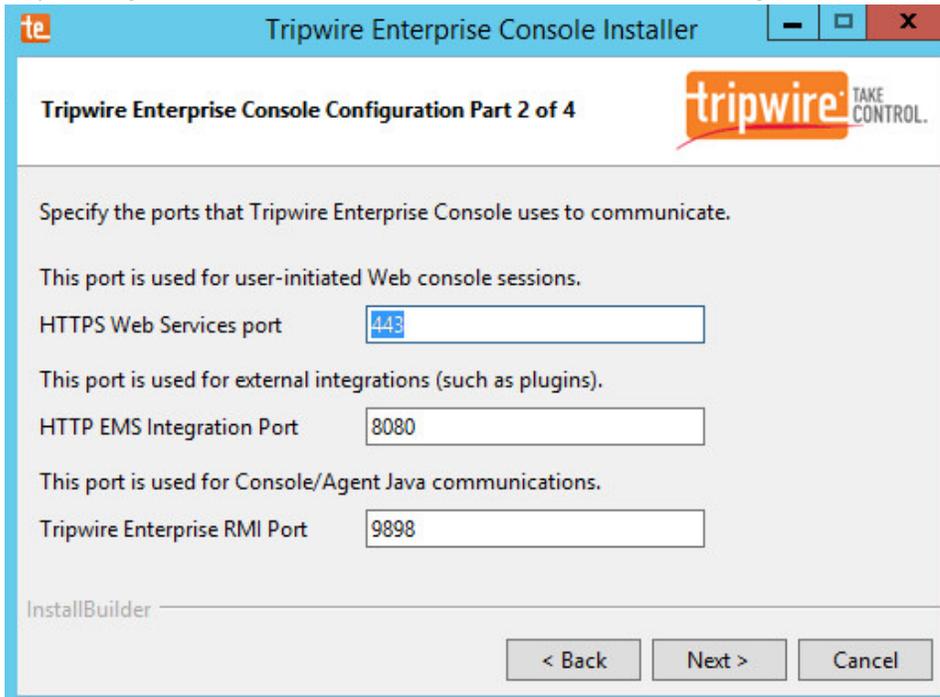
1532  
1533  
1534  
1535

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

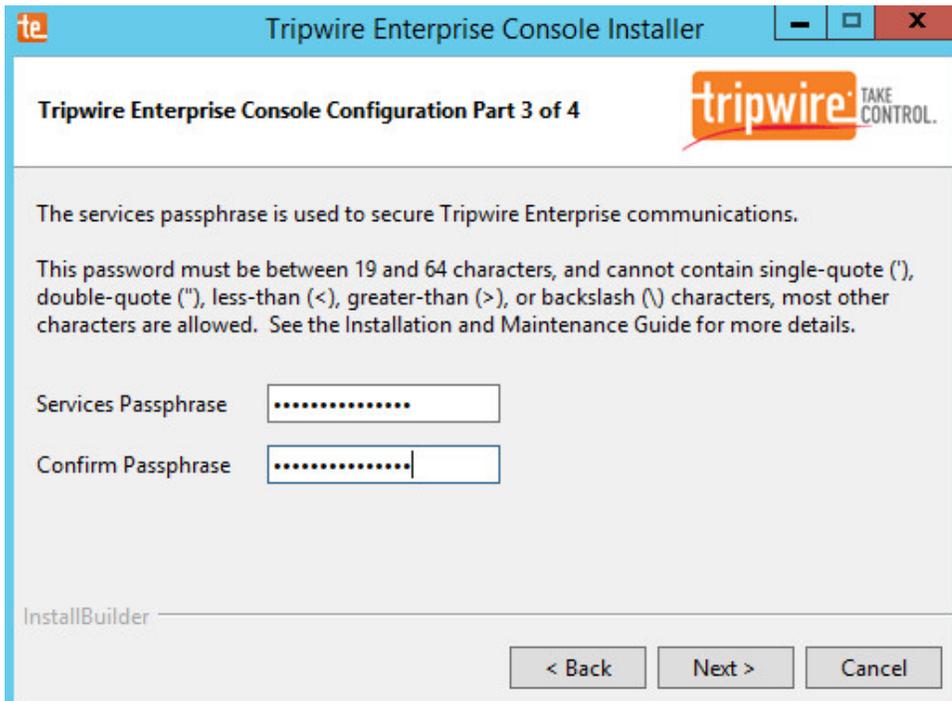


1536

- 1537 14. Click **Next**.
- 1538 15. Enter the port numbers to use for each of the **HTTPS Web Services port**, **HTTP EMS Integration**
- 1539 **Port**, and **Tripwire Enterprise RMI port**. The RMI port is used for inbound communication from
- 1540 Tripwire agents to the server, so ensure that it is allowed through the firewall.

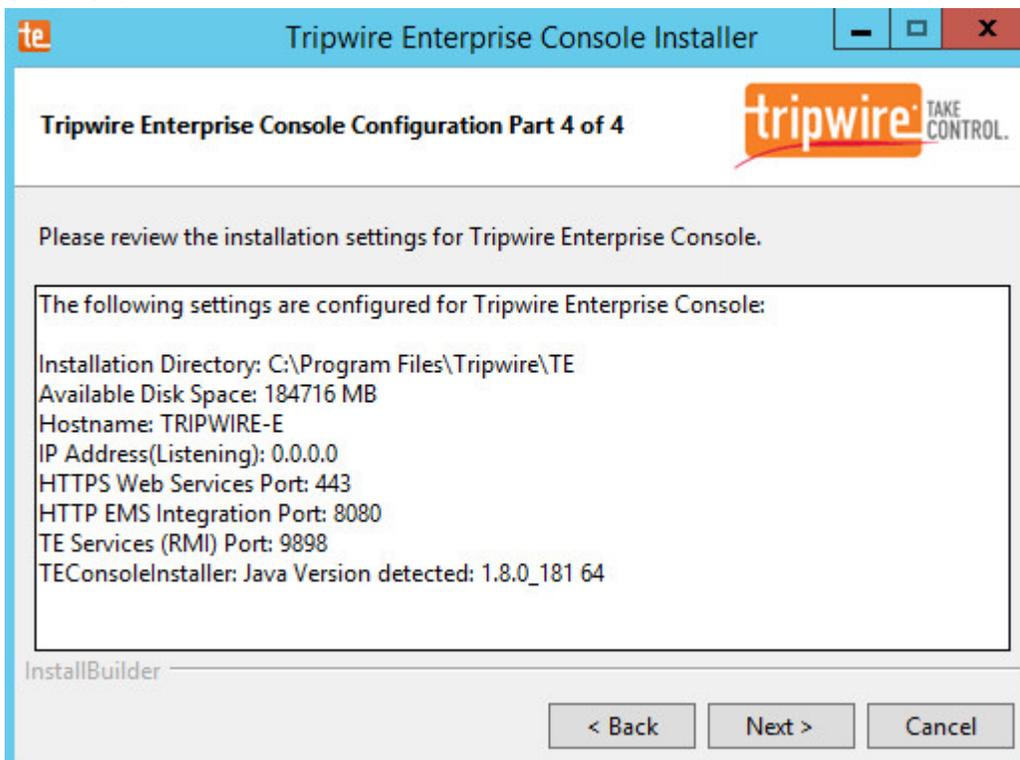


- 1541 16. Click **Next**.
- 1542 17. Enter a passphrase to use.
- 1543



1544  
1545

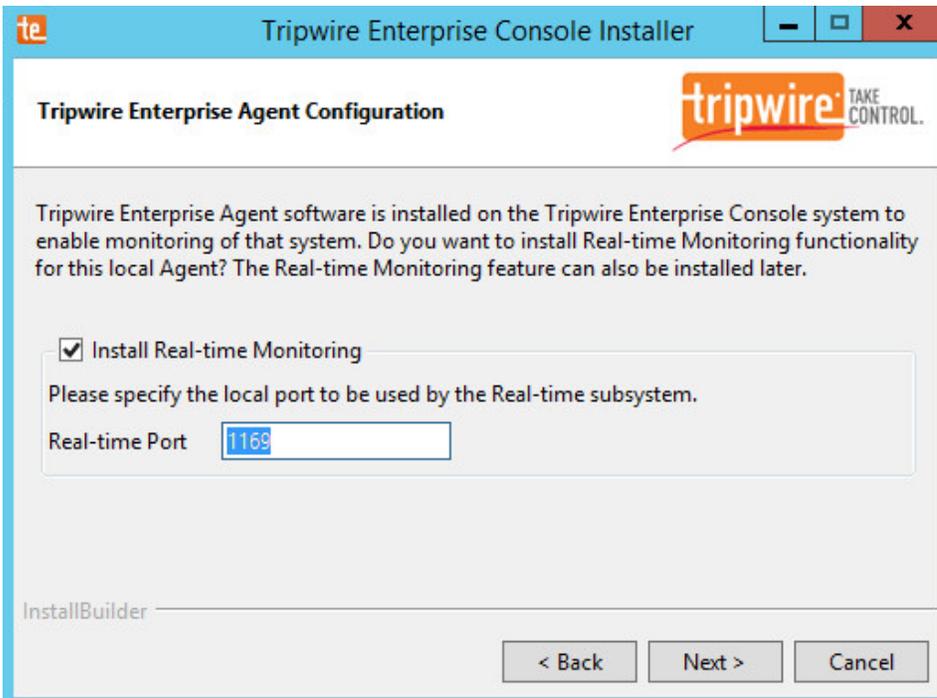
18. Click **Next**.



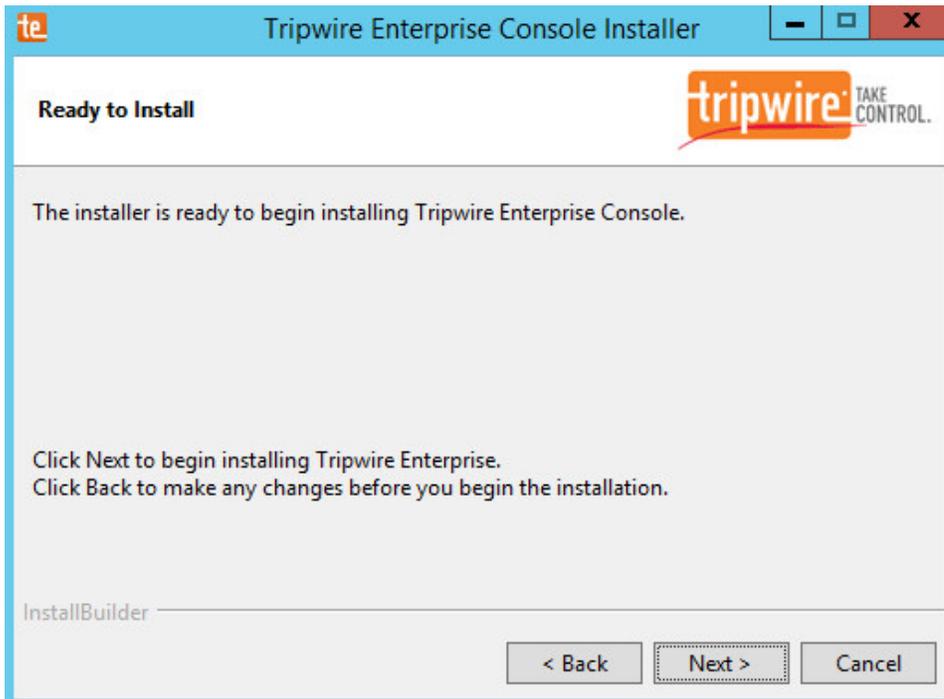
1546

DRAFT

- 1547 19. Click **Next**.
- 1548 20. Check the box next to **Install Real-time Monitoring**.
- 1549 21. Enter **1169** for **Real-time Port**.

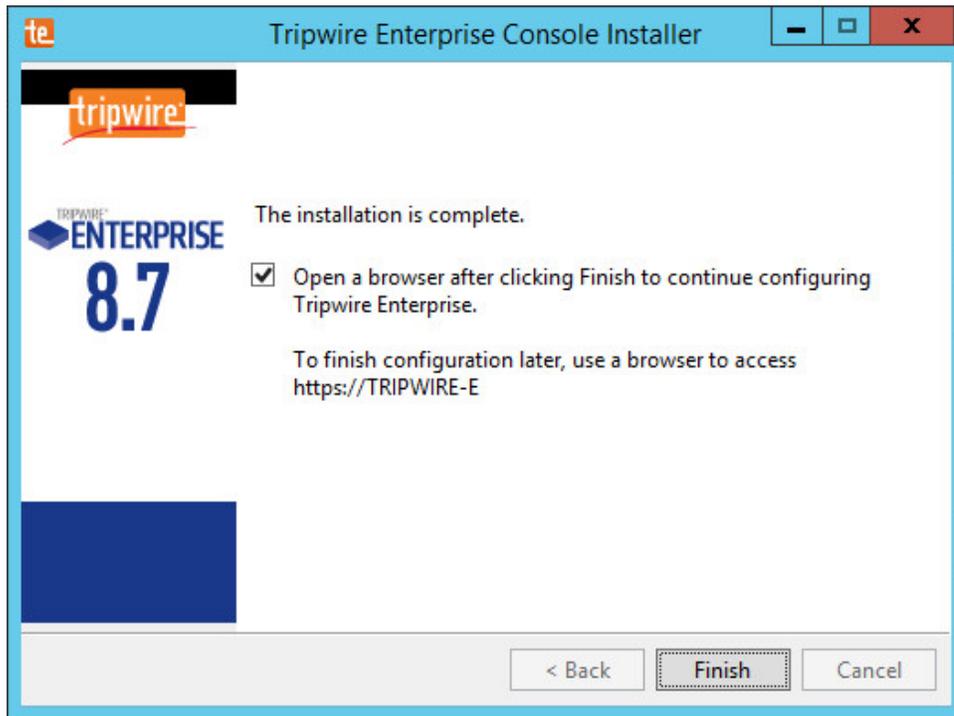


- 1550 22. Click **Next**.
- 1551



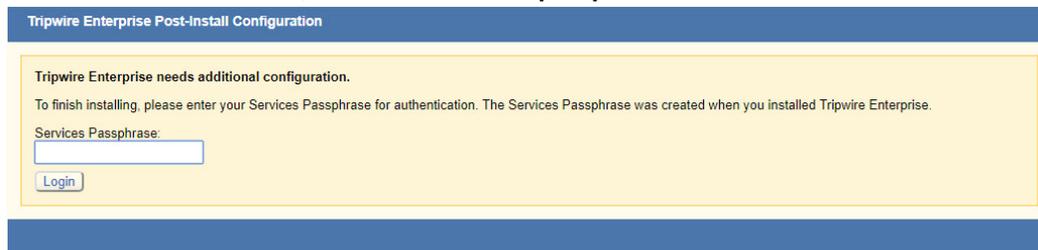
1552  
1553  
1554  
1555

23. Click **Next**.
24. Check the box next to **Open a browser after clicking Finish to continue configuring Tripwire Enterprise**.



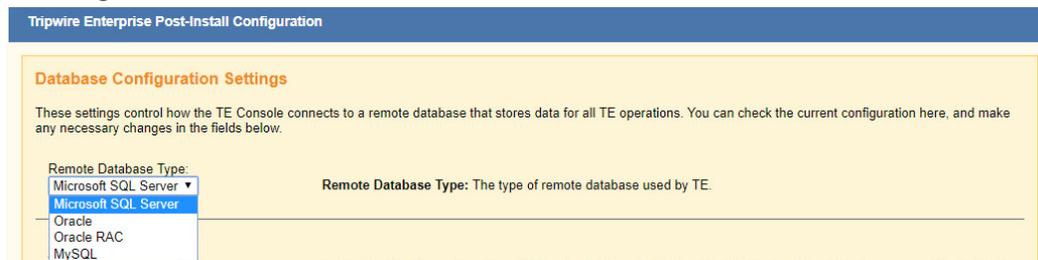
1556  
1557  
1558

25. Click **Finish**.
26. Once at the web address, enter the **Services passphrase** chosen earlier.



1559  
1560

27. Click **Login**.



1561  
1562  
1563  
1564  
1565

28. Select **Microsoft SQL Server** for **Remote Database Type**.
29. Select **SQL Server** for **Authentication Type**.
30. Enter login details for the account created during the MSSQL setup.
31. Enter the **hostname** or **IP** of the database server.

- 1566 32. Enter the **port** on which the database is operating.
- 1567 33. Enter the **name** of the database to be used for Tripwire Enterprise.
- 1568 34. Select the appropriate setting for **SSL** according to your organization’s needs.

The screenshot shows a configuration window with the following fields and descriptions:

- Authentication Type:** A dropdown menu set to "SQL Server". Description: 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:** A text box containing "twadmin". Description: The login name that TE will use to authenticate with the database.
- Password:** A text box with masked characters. Description: The password that TE will use to authenticate with the database.
- Database Host:** A text box containing "192.168.78.125". Description: The fully qualified domain name, hostname or IP address of the system where the database is installed.
- Port (default 1433):** A text box containing "1433". Description: 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:** A text box containing "TE\_DB". Description: 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):** An empty text box. Description: The location/name of the database instance on the server. Ask your DBA if a non-default instance should be used for TE.
- SSL:** A dropdown menu set to "Off". Description: 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.

At the bottom of the form is a "Test Database Login" button with a green checkmark icon.

- 1569 35. Click **Test Database Login** to ensure the connection is functional.
- 1570

The screenshot shows the "Test Results" section of the configuration window. It contains a text box with the message "Connection Succeeded." Below this, there is a footer bar with the text "Tripwire Enterprise 8.7.0.b8.7.0.r20180606173604-e215728.b40" on the left and "Save Configuration and Restart Console" and "Logout" buttons on the right.

- 1571 36. Click **Save Configuration and Restart Console**.
- 1572
- 1573 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

1574  
1575

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.

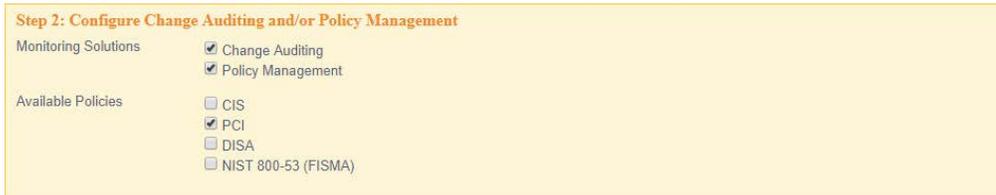
Note: After Fast Track configures Tripwire Enterprise, you can always make changes to your configuration later from the Tripwire Enterprise user interface.

1576  
1577

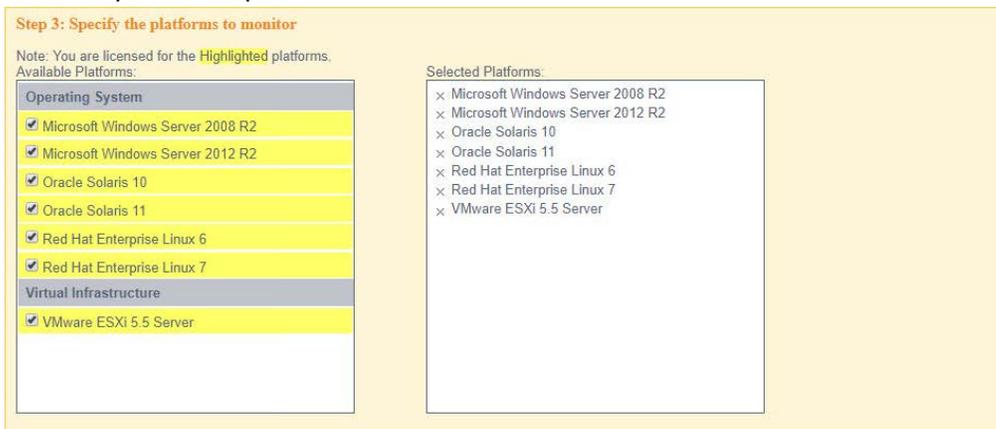
39. Click **Configure Tripwire Enterprise**.



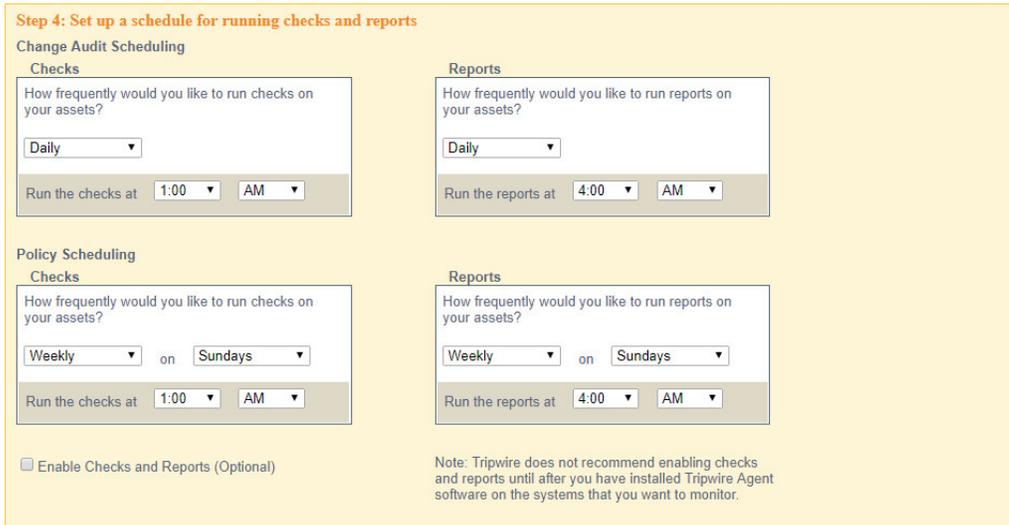
- 1578
- 1579
- 1580
- 40. Click **Choose File**, and select the Tripwire Enterprise license file, which should be a *.cert* file.
- 41. Check the box next to **Change Auditing and Policy Management**.



- 1581
- 1582
- 42. Select any available policies desired.



- 1583
- 1584
- 43. Select all the operating systems that you wish to monitor with Tripwire Enterprise (TE).



- 1585
- 1586
- 1587
- 44. Set up a schedule for running checks and reports according to your organization's needs. Leave the box next to **Enable Checks and Reports** unchecked for now.

1588  
1589



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

1590  
1591



46. Enter a username and password for a new administrator account for TE Console.

1592  
1593

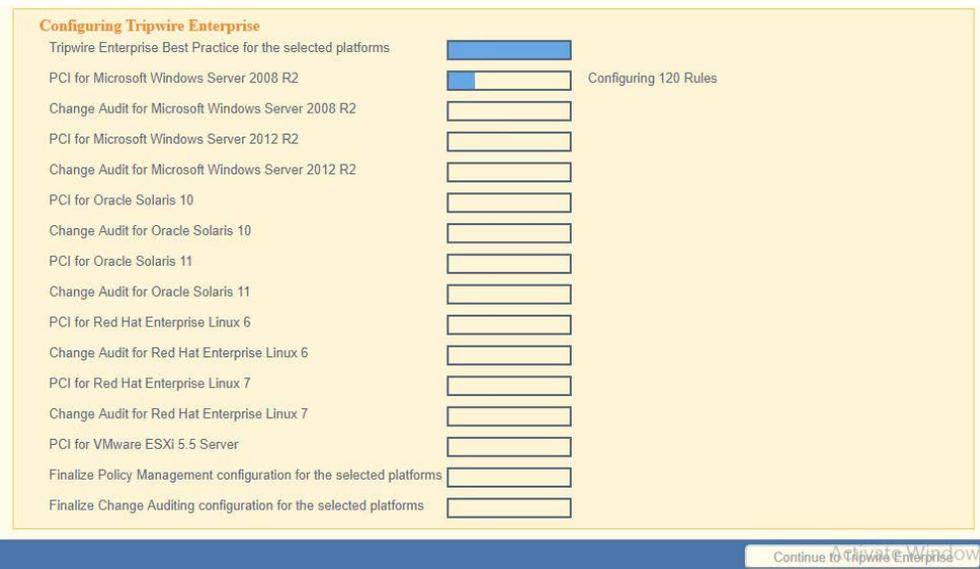


47. Click **Preview Configuration**.

1594  
1595



48. Click **Apply Configuration**.



1596

1597

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

1598

## 2.9.2 Install the Axon Bridge

1599

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

1600

2. Navigate to the TE Console installation directory, to the `/server/data/config` folder. Copy `bridge_sample.properties` to `bridge.properties`.

1601

1602

3. In the `bridge.properties` file, find the line that says:

1603

```
#tw.cap.bridge.registrationPreSharedKey=
```

1604

Remove the `#` character. After the `=` character, enter a password. The password has some restrictions, so ensure that it meets the requirements if the connection fails later.

1605

1606

4. Restart the TE console by running the following command from an administrator command prompt, where `<te_root>` is the TE installation directory:

1607

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

1608

1609

## 2.9.3 Install the Axon Agent (Windows)

1610

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

1611

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

1612

2. Unzip the file.

1613

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

1614

1615

4. After the Axon Agent is installed, navigate to `C:\ProgramData\Tripwire\agent\config`, and copy `twagent_sample.conf` to `twagent.conf`.

1616

```
#
# 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
#
```

- 1617
- 1618
- 1619
- 1620
- 1621
- 1622
- 1623
- 1624
- 1625
5. Open *twagent.conf*, and find the line that says `bridge.host`. Remove the `#` character, and enter the hostname or IP address of the Axon Bridge server.
  6. In a file called *registration\_pre\_shared\_key*, enter the value of the pre-shared key that was set in the Axon Bridge.
  7. Restart the Axon Agent Service by opening a command prompt and running the following commands:

```
> net stop TripwireAxonAgent
> 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>
```

- 1626
- 1627
- 1628
- 1629
- 1630
- 1631
- 1632
- 1633
- 1634
- 1635
- ### 2.9.4 Install the Axon Agent (Linux)
1. Download the Axon Agent *.tgz* file from the Tripwire customer website (<https://tripwireinc.force.com/customers>), under the **Product Downloads** tab.
  2. To install the software, run the following commands:  
 RHEL or CentOS: `> rpm -ivh <installer_file>`  
 Debian or Ubuntu: `> dpkg -i <installer_file>`
  3. Navigate to `/etc/tripwire/` and copy *twagent\_sample.conf* to *twagent.conf*.
  4. Open *twagent.conf*, and find the line that says `bridge.host`. Remove the `#` character, and enter the hostname or IP address of the Axon Bridge server.

- 1636 5. In a file called *registration\_pre\_shared\_key.txt*, enter the value of the pre-shared key that was  
1637 set in the Axon Bridge.
- 1638 6. Restart the Axon Agent Service by opening a command prompt and running the following  
1639 commands:
- 1640 RHEL or CentOS:
- 1641 > /sbin/service tripwire-axon-agent stop  
1642 > /sbin/service tripwire-axon-agent start  
1643
- 1644 Debian or Ubuntu:
- 1645 > /usr/sbin/service tripwire-axon-agent stop  
1646 > /usr/sbin/service tripwire-axon-agent start

## 1647 2.9.5 Configure Tripwire Enterprise

### 1648 2.9.5.1 Terminology

1649 **Node:** A monitored system, such as a file system, directory, network device, database, or virtual  
1650 infrastructure component.

1651 **Element:** A monitored object, which is a component or property of a node being audited by TE.

1652 **Element Version:** A record of an element's state at specific points in time. Multiple element versions  
1653 create a historical archive of changes made to the element.

1654 **Rule:** A rule identifies one or more elements to the TE Console.

1655 **Action:** An object that initiates a response to either changes detected by TE or by failures generated  
1656 from policy tests.

1657 **Task:** A TE operation that runs on a scheduled or manual basis.

1658 **TE Policy:** A measurement of the degree to which elements comply with a policy.

1659 **Policy Test:** A determination of whether elements comply with the requirements of a policy.

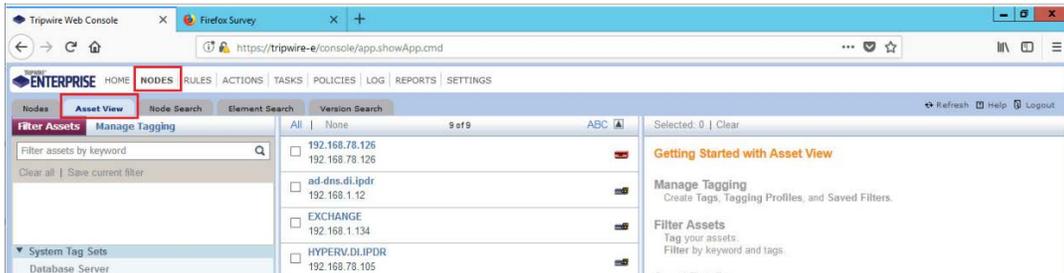
1660 **Baseline:** The act of creating an element that reflects the current state of a monitored object (also  
1661 called the **current baseline**. When a node's baseline is promoted, TE saves the former baseline as a  
1662 **historic baseline**.

1663 **Version Check:** A check on monitored objects/elements. It is a comparison of the current state of the  
1664 element against its already recorded baseline for changes.

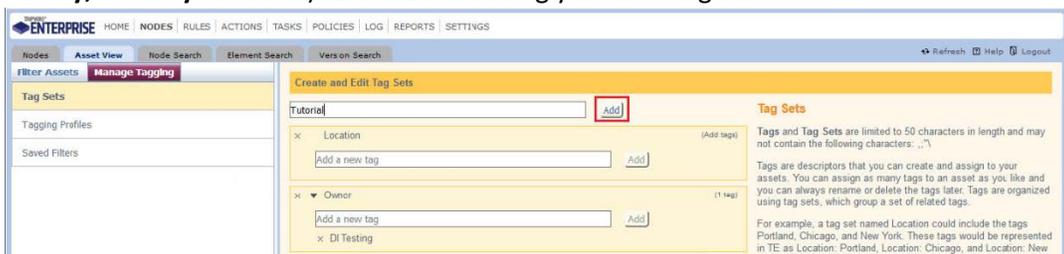
1665 2.9.5.2 *Tags*

1666 In TE, tags can be used to label and target specific nodes. Tags are not required but allow for targeting  
 1667 nodes more granularly than by the operating system. This section will describe how to create and assign  
 1668 tags.

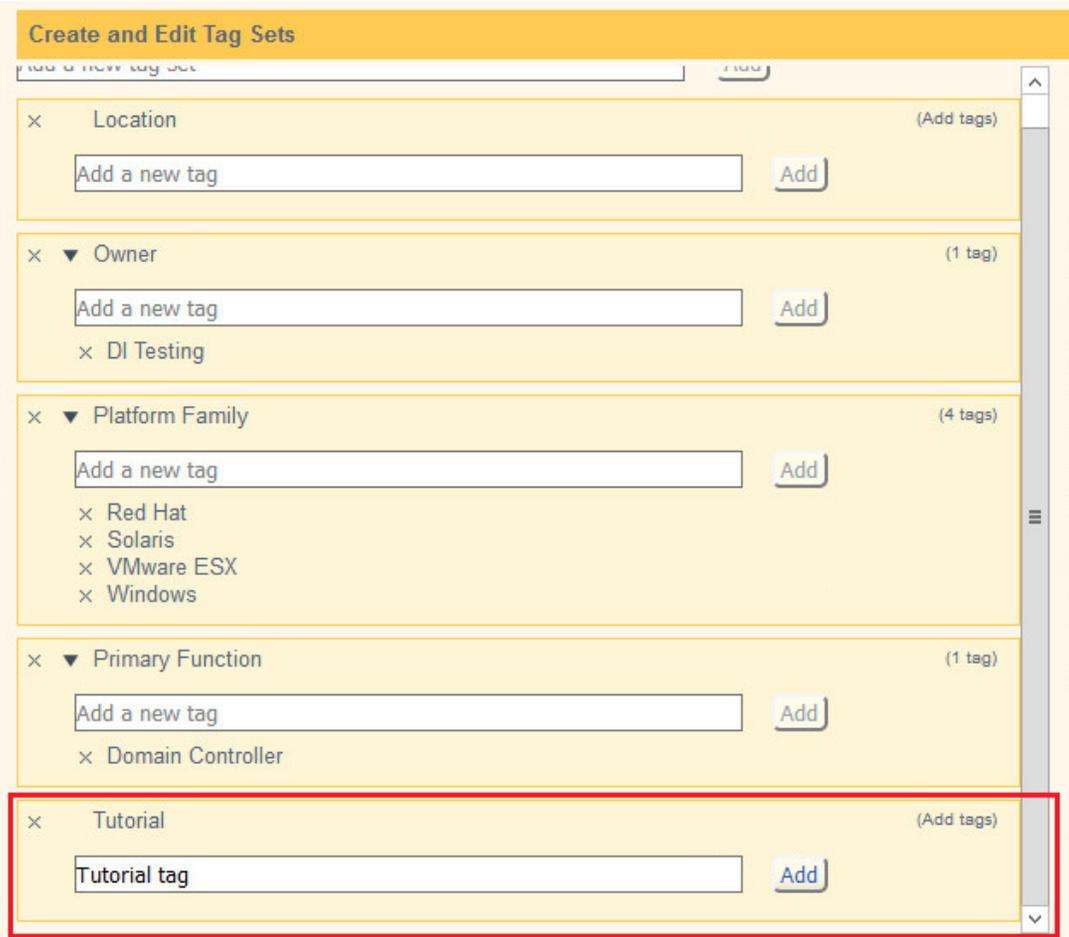
- 1669 1. Navigate to the TE Console in your browser.  
 1670 2. Click **Asset View**.



- 1671 3. Click the **Manage Tagging** tab.  
 1672 4. Enter the name of a tag set or use one of the four existing ones (**Location, Owner, Platform**  
 1673 **Family, Primary Function**). Click **Add** if adding your own tag set.  
 1674

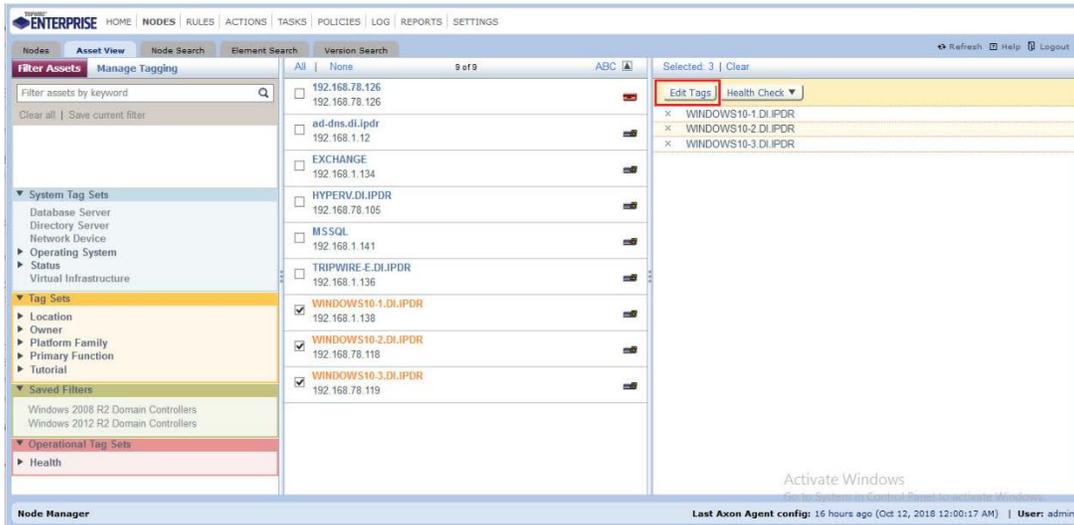


- 1675 5. Under the tag set you wish to add a tag to, enter the name of the tag.  
 1676



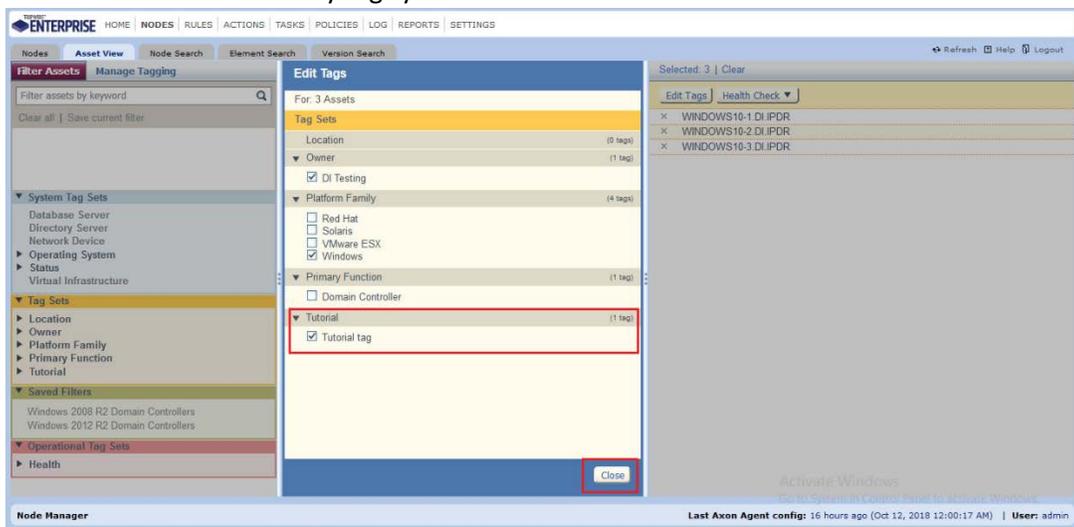
1677  
1678  
1679  
1680

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.



1681  
1682  
1683

9. Click **Edit Tags**.
10. Check the boxes next to any tags you wish to add to these nodes.



1684  
1685

11. Click **Close**.

### 1686 2.9.5.3 Rules

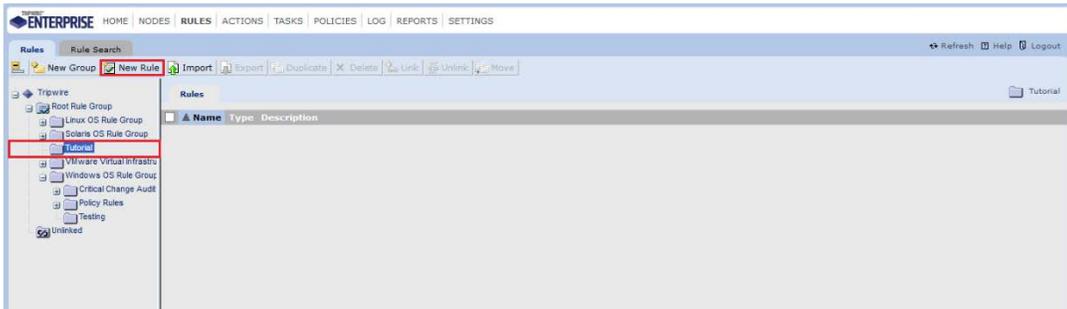
1687 This section will describe how to create a rule.

- 1688 1. Click **Rules**.



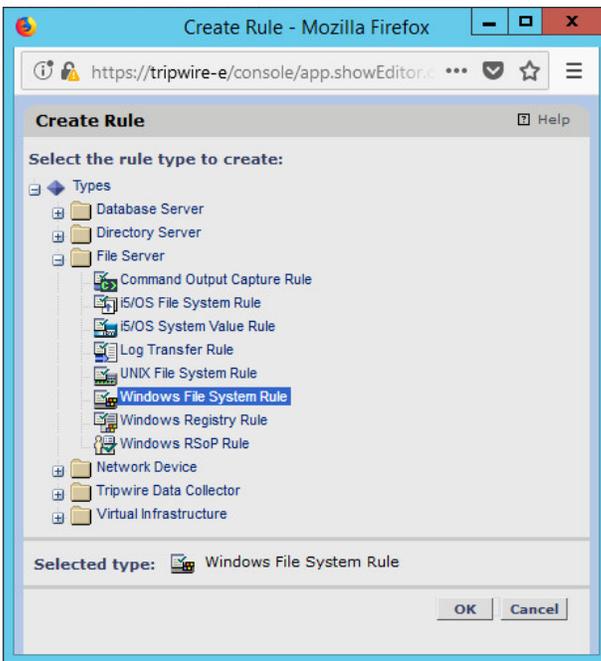
1689  
1690

2. Select or create a rule group in which to put the new rule.



1691  
1692  
1693  
1694  
1695

3. Click **New Rule**.
4. Select the type of rule. For monitoring Windows filesystems, we choose **Windows File System Rule**.



1696  
1697  
1698

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

New Windows File System Rule Wizard - Mozilla Firefox

https://tripwire-e/console/app.showWizard.cmd?wizardName=si.web.specifierRuleV

**New Windows File System Rule Wizard** Help

Enter a name and description for the rule.

Name: tutorial rule

Description: a rule specifically for tutorial documentation

Enable Tracking Identifier

< Back Next > Finish Cancel

1699  
1700

7. Click **Next**.

New Windows File System Rule Wizard - Mozilla Firefox

https://tripwire-e/console/app.showWizard.cmd?wizardName=si.web.specifierRuleV

**New Windows File System Rule Wizard** Help

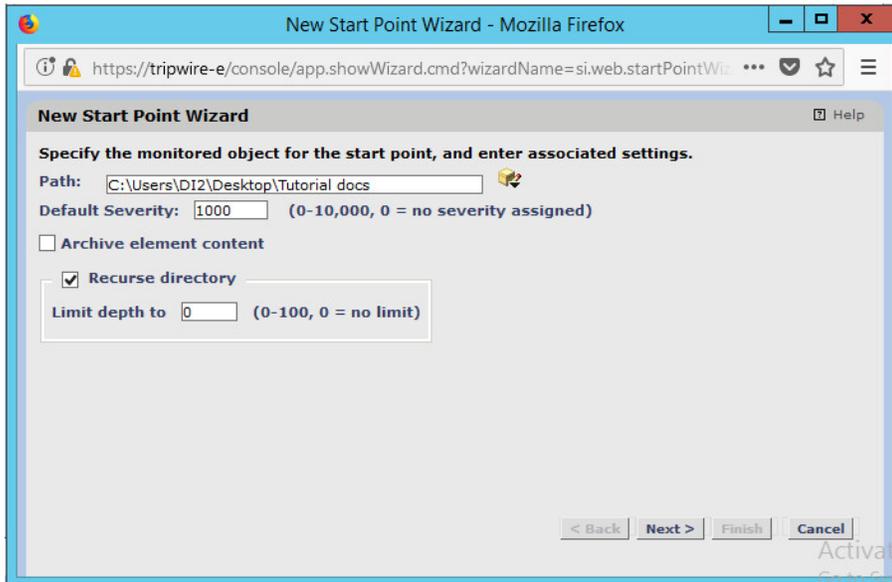
New Start Point New Stop Point Browse Delete

<input type="checkbox"/>	Path	Type	Default Severity	Criteria Set	Recurse Level	Archive Content

< Back Next > Finish Cancel

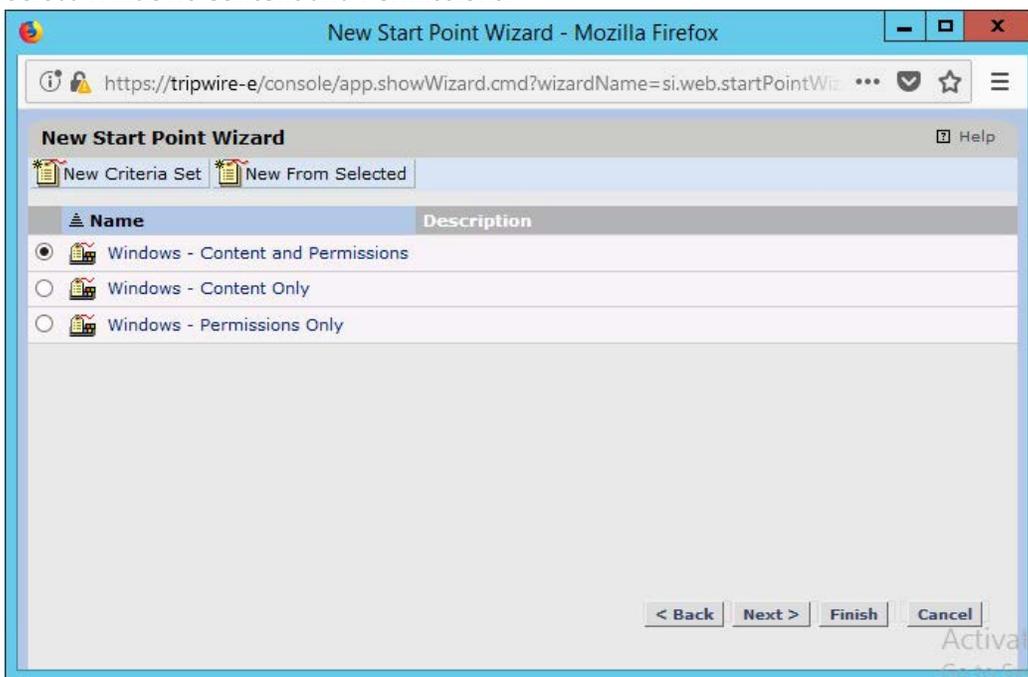
1701  
1702  
1703  
1704  
1705  
1706

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.



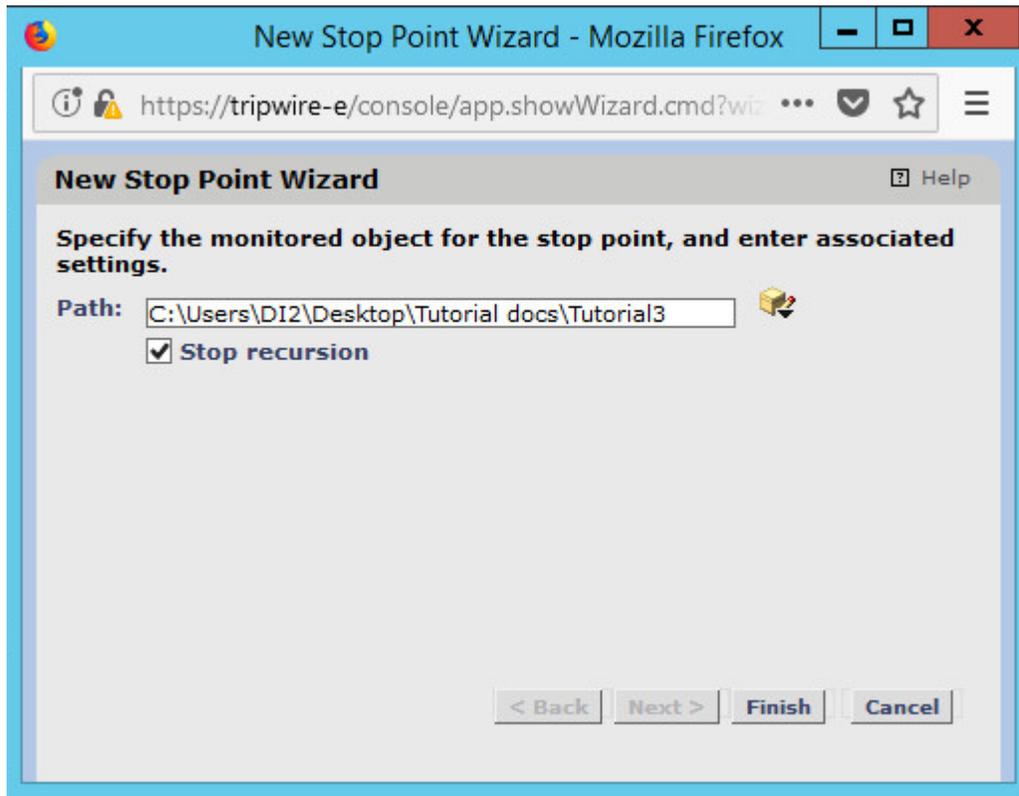
1707  
1708  
1709

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



1710  
1711  
1712  
1713  
1714

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.



- 1715
- 1716 16. Click **Finish**.
- 1717 17. Click **Next**.
- 1718 18. Click **Next**.
- 1719 19. Click **Finish**.

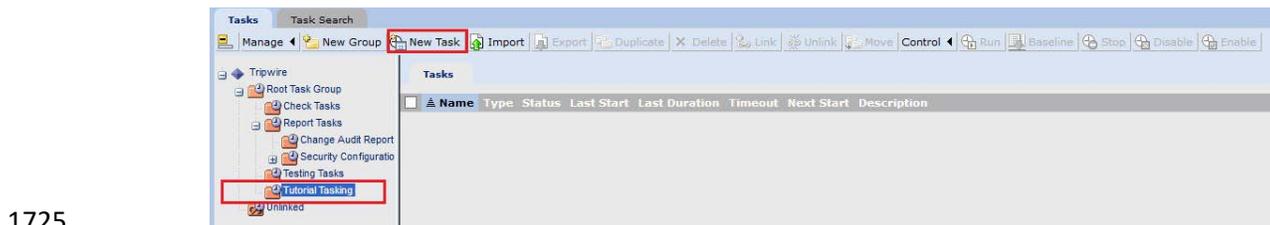
#### 1720 2.9.5.4 *Tasks*

1721 This section will describe how to create a task.

- 1722 1. Click **Tasks**.

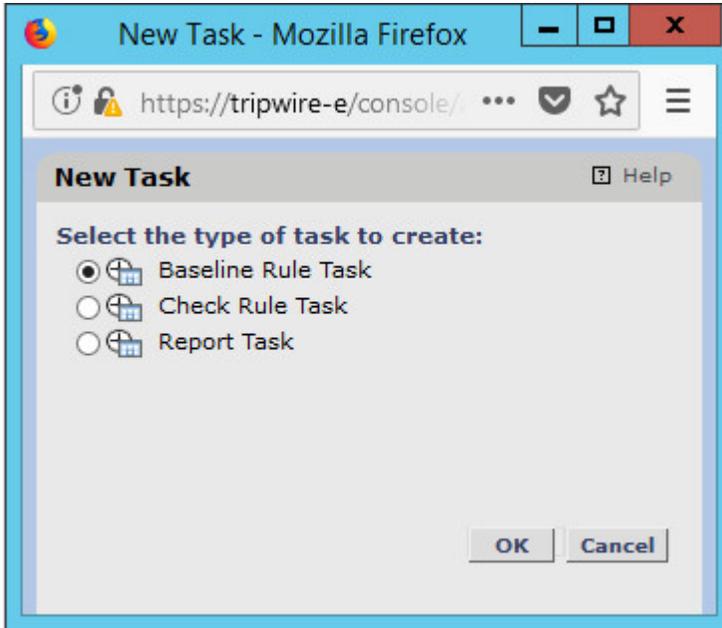


- 1723 2. Select a folder for a new task or create one.

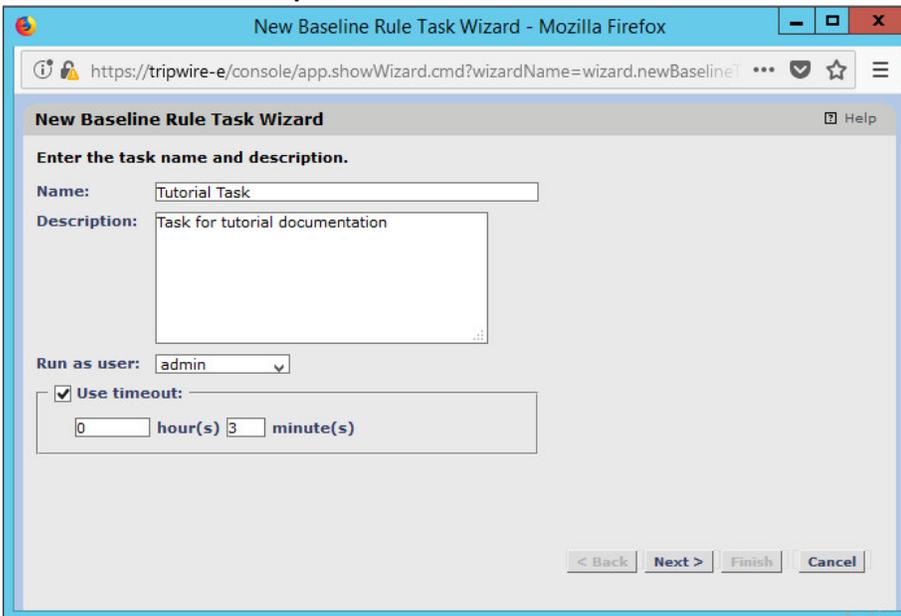


- 1725 3. Click **New Task**.
- 1726

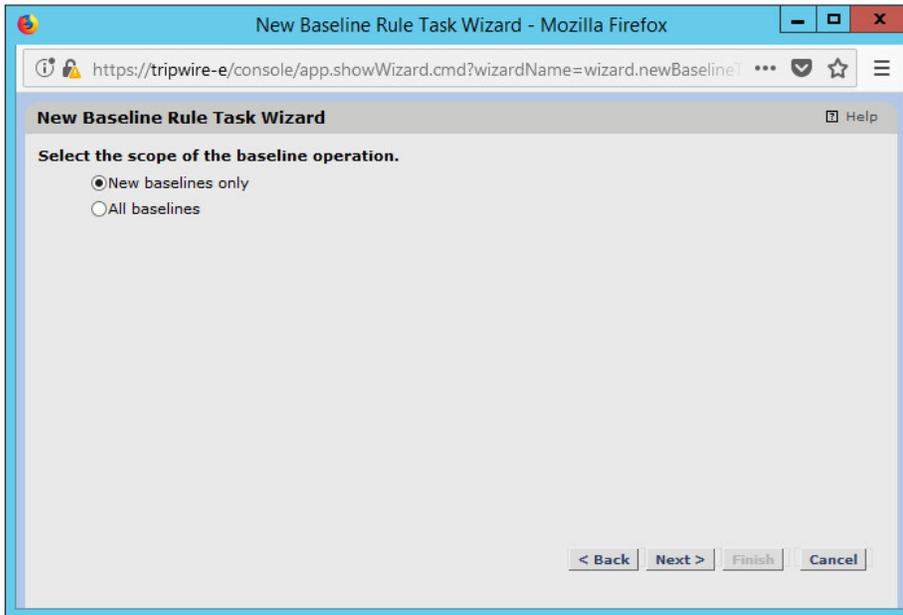
- 1727 4. Select **Baseline Rule Task** or **Check Rule Task** (Note: Both are needed: baseline creates the  
1728 initial state of the monitored object, and check updates the state and reports any changes).



- 1729 5. Click **OK**.  
1730  
1731 6. Enter a **name** and **description** for the task.

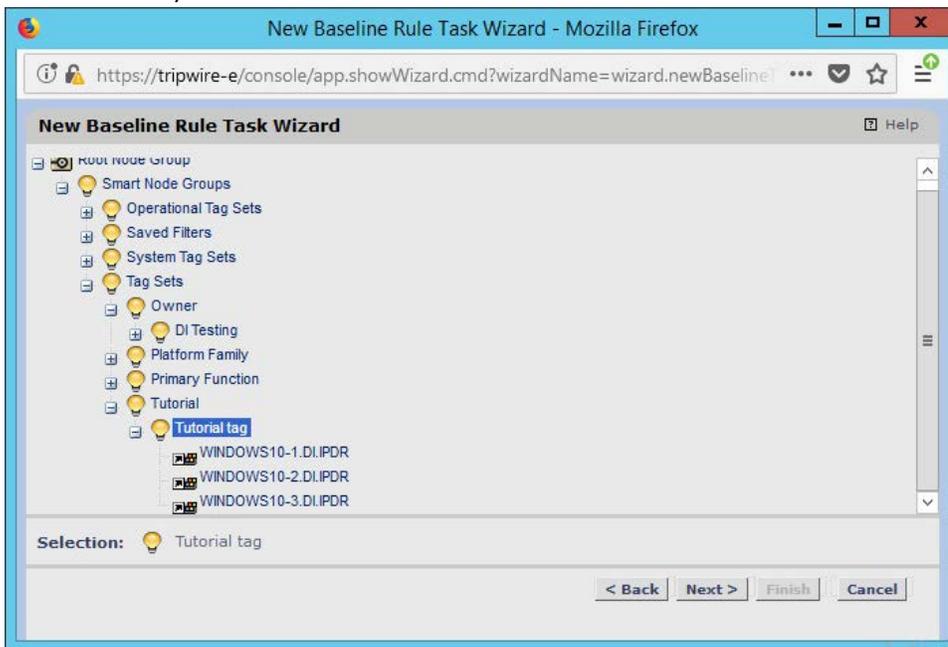


- 1732 7. Click **Next**.  
1733  
1734 8. Select whether you want all baselines to be updated or to only create new baselines.



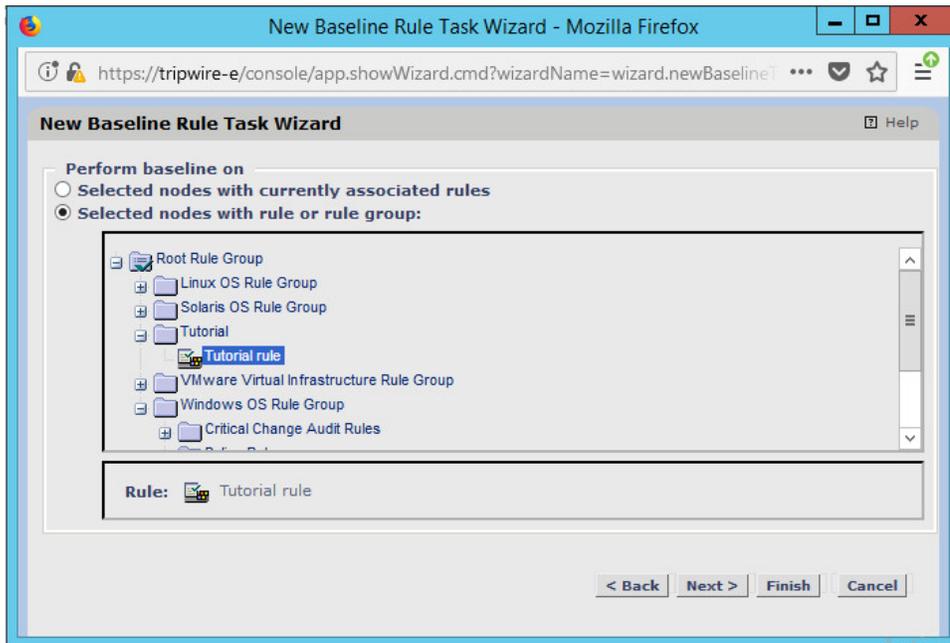
1735  
1736  
1737  
1738

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).



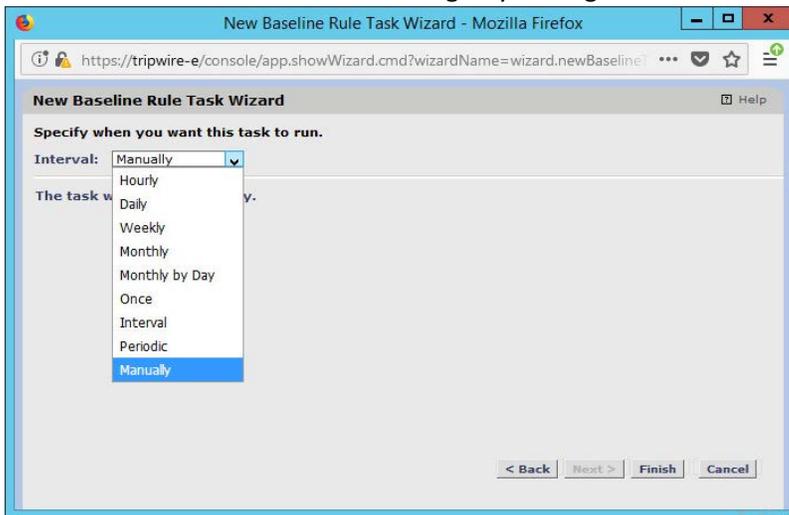
1739  
1740  
1741

11. Click **Next**.
12. Select the rule created earlier.



1742  
1743  
1744

13. Click **Next**.
14. Set the schedule of this task according to your organization's needs.



1745  
1746

15. Click **Finish**.

## 1747 2.10 Tripwire Log Center

### 1748 2.10.1 Install Tripwire Log Center Manager

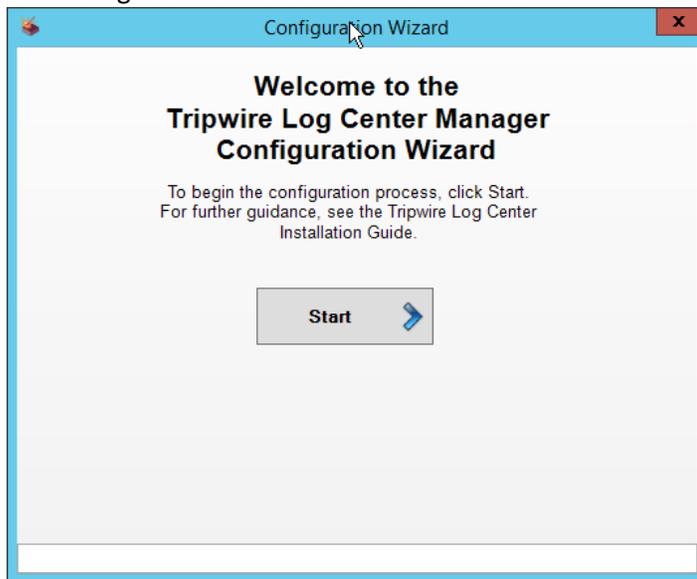
1749 See the *Tripwire Log Center 7.3.1 Installation Guide* that should accompany the installation media for  
1750 instructions on how to install **Tripwire Log Center**. Use the **Tripwire Log Center Manager** installer.

1751 Notes:

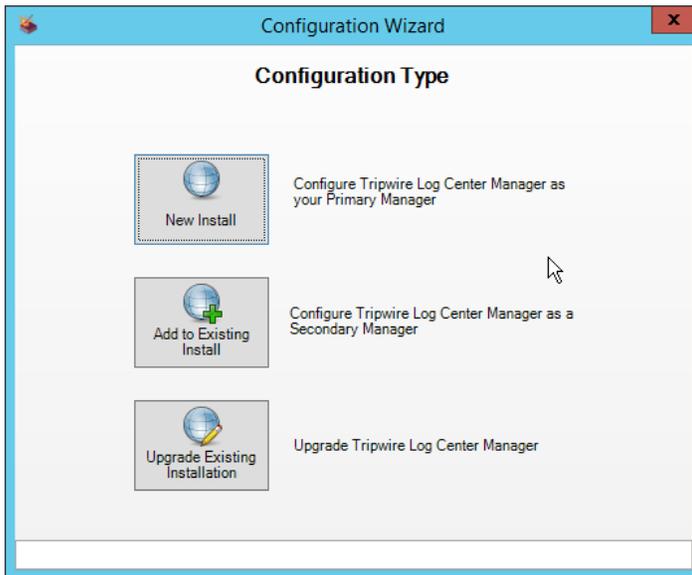
- 1752 a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire**
- 1753 **Enterprise**.
- 1754 b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log*
- 1755 *Center 7.3.1 Installation Guide*.
- 1756 c. .NET Framework 3.5 is required for this installation; install this from the Server Manager.
- 1757 d. You may need to unblock port **9898** on your firewall for the TE agents.
- 1758 e. Do not install PostgreSQL if you wish to use a database on another system; this guide will use a
- 1759 local PostgreSQL database, however.
- 1760 f. When it finishes installing, there should be a configuration wizard (see below for configuration
- 1761 steps).

## 1762 2.10.2 Configure Tripwire Log Center Manager

- 1763 1. The configuration wizard should start after the installation is complete.

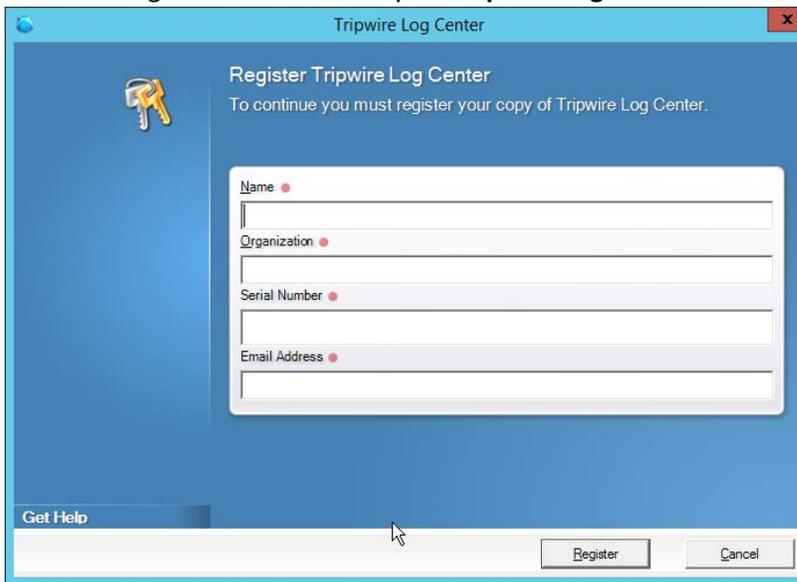


- 1764 2. Click **Start**.
- 1765



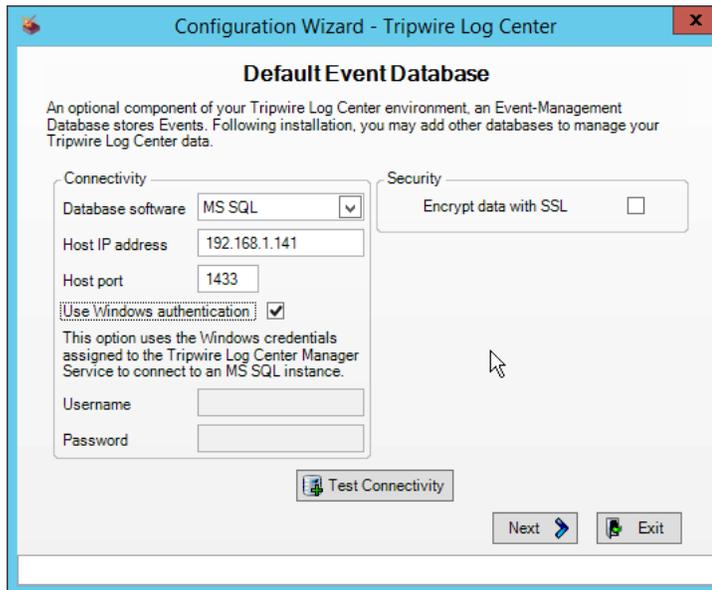
1766  
1767  
1768

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



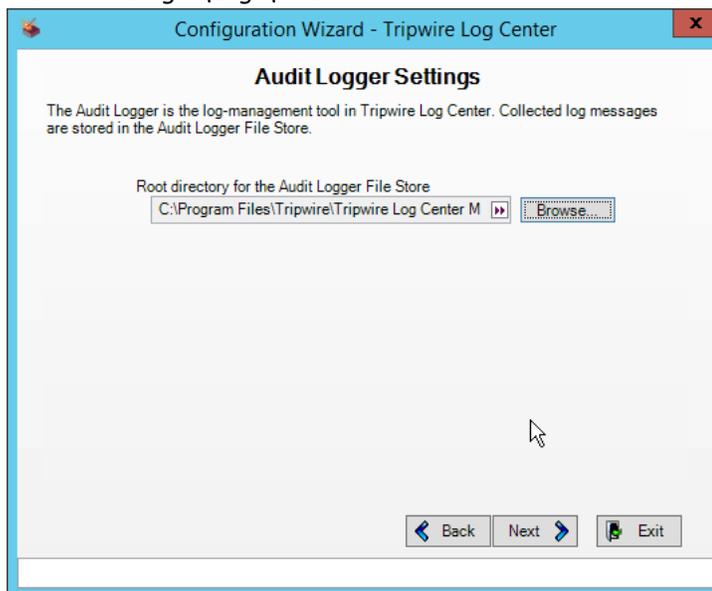
1769  
1770  
1771

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



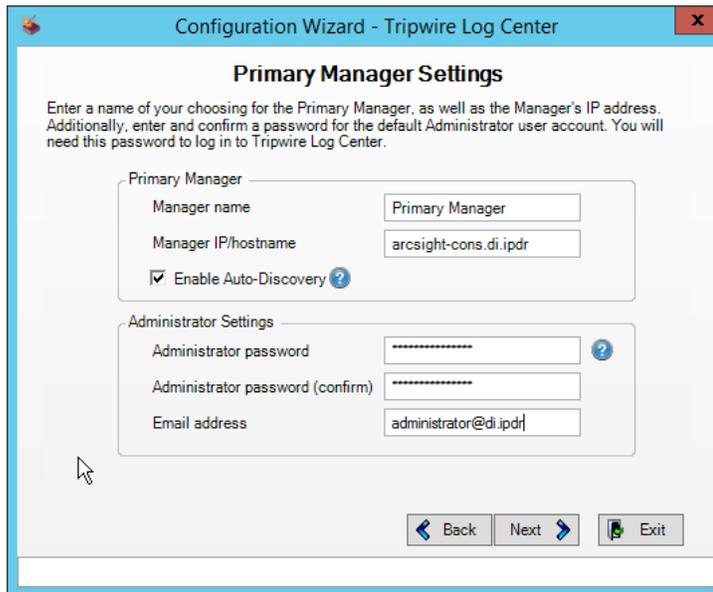
1772  
1773  
1774  
1775

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



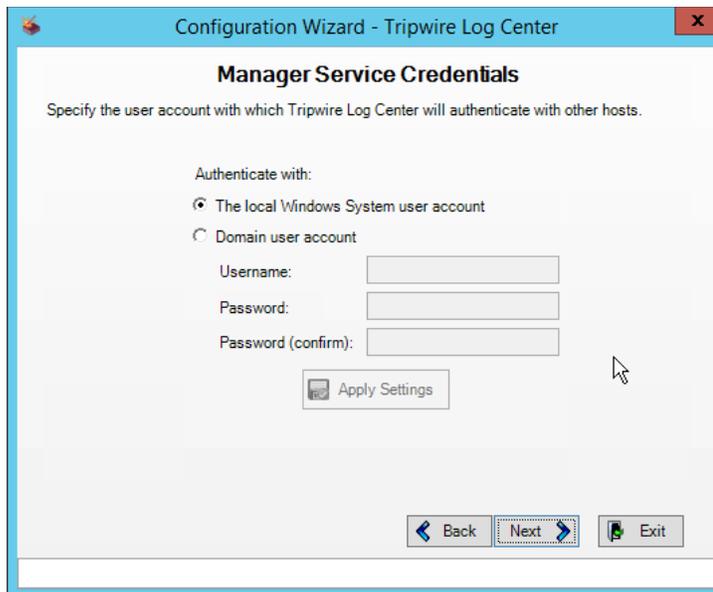
1776  
1777  
1778  
1779

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



1780  
1781

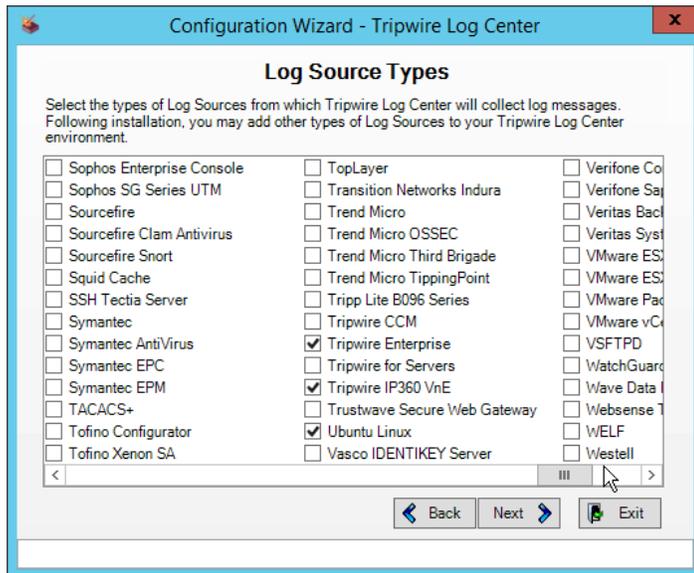
12. Click **Next**.



1782  
1783  
1784  
1785  
1786

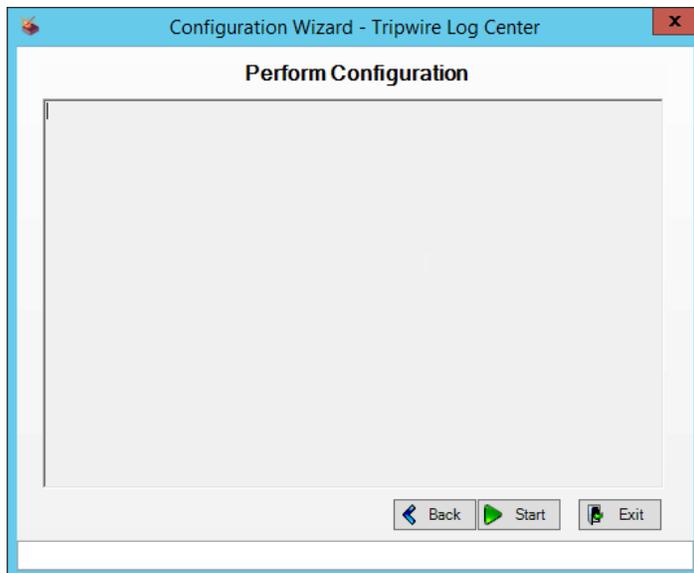
13. Click **Next**.

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.**



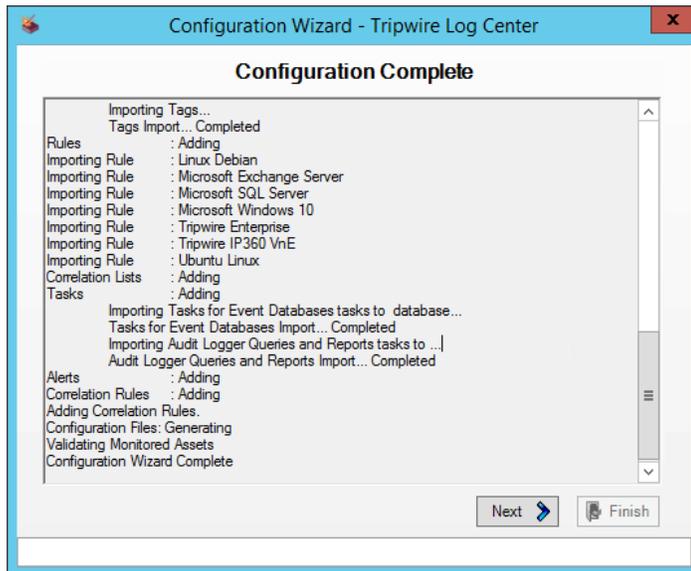
1787  
1788

15. Click **Next**.



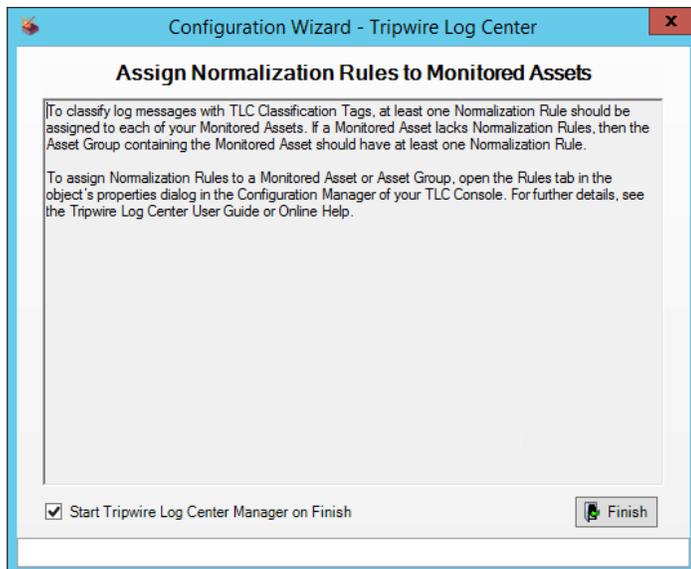
1789  
1790

16. Click **Start**.



1791  
1792

17. Click **Next**.



1793  
1794

18. Click **Finish**.

### 1795 2.10.3 Install Tripwire Log Center Console

1796 Chapter 4 of the *Tripwire Log Center 7.3.1 Installation Guide* details the installation of the **Tripwire Log**  
1797 **Center Console**. Use the **Tripwire Log Center Console** installer.

1798 You can install this on the same machine as the **Tripwire Log Center Manager**, if desired.

## 1799 2.11 Cisco Identity Services Engine

1800 This section will detail the installation and some configurations for the Cisco Identity Services Engine  
1801 (ISE). It assumes the use of the ISE virtual machine.

### 1802 2.11.1 Initial Setup

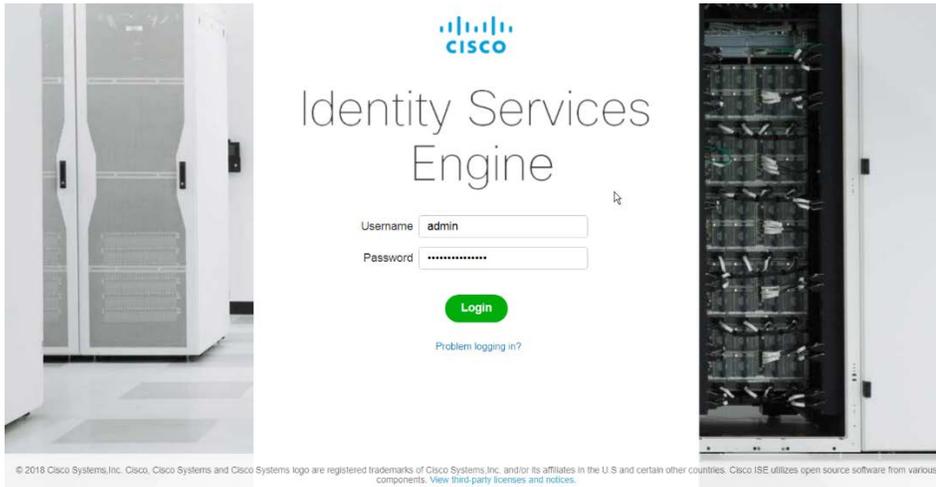
- 1803 1. When prompted to log in for the first time, enter **setup**. (You can use the command `reset-`  
1804 `config` to change these values later.)
- 1805 2. Enter the desired **hostname** for the machine.
- 1806 3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname is associated  
1807 with this IP address in your DNS.)
- 1808 4. Enter the **netmask** for the machine.
- 1809 5. Enter the **default gateway**.
- 1810 6. Enter the **default DNS domain** (the name of your domain).
- 1811 7. Enter the **primary nameserver** (the IP address of your DNS).
- 1812 8. Enter a second nameserver if desired.
- 1813 9. Enter an **NTP time server**.
- 1814 10. Enter the **timezone**.
- 1815 11. Enter **Y** for **SSH service**.
- 1816 12. Enter an administrator **username** for the machine.
- 1817 13. Enter a **password** twice.

### 1818 2.11.2 Inventory: Configure SNMP on Routers/Network Devices

1819 See the corresponding vendor documentation for the correct way to enable SNMP on your network  
1820 device. Ensure that the community string you choose is considered sensitive, like a password.

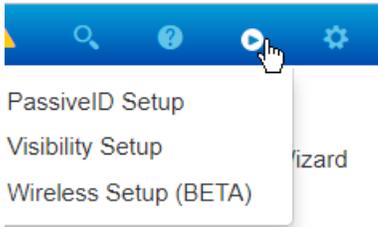
### 1821 2.11.3 Inventory: Configure Device Detection

- 1822 1. Log in to the web client by visiting <https://hostname/admin>, but replace **hostname** with the  
1823 hostname of the ISE machine.



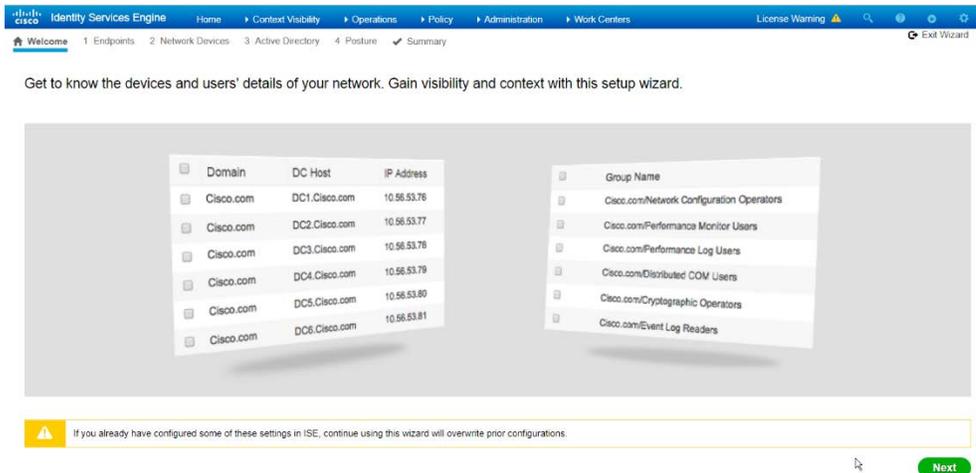
1824  
1825

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



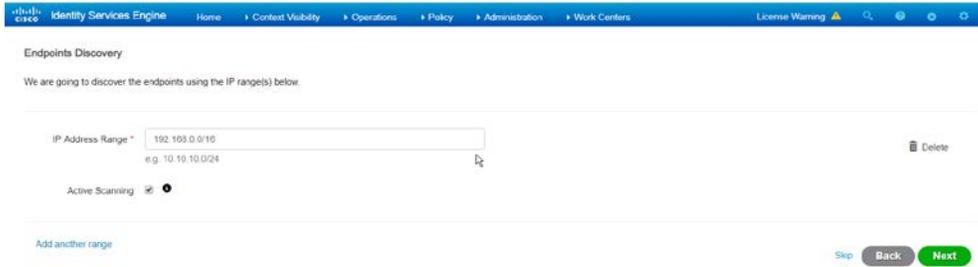
1826  
1827

3. Click **Next**.

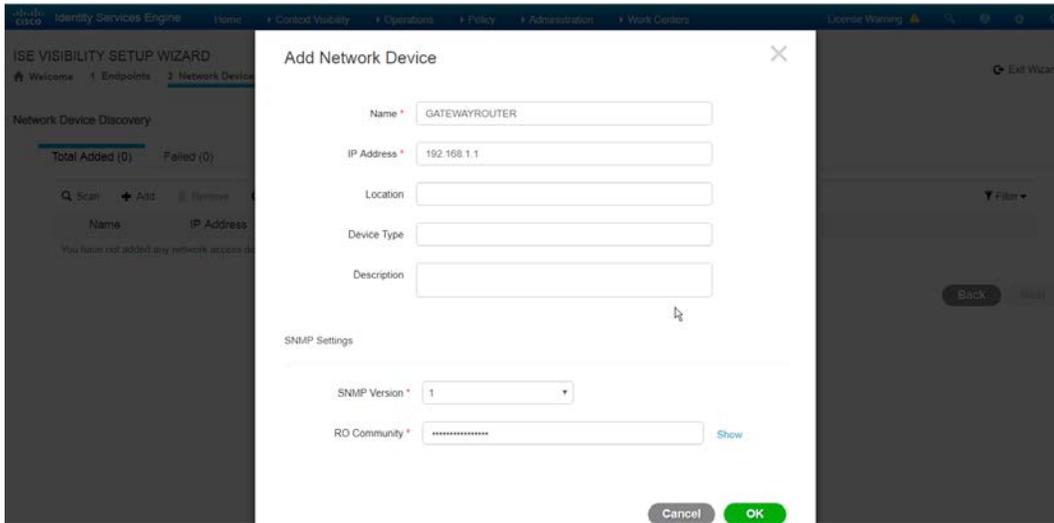


1828  
1829  
1830

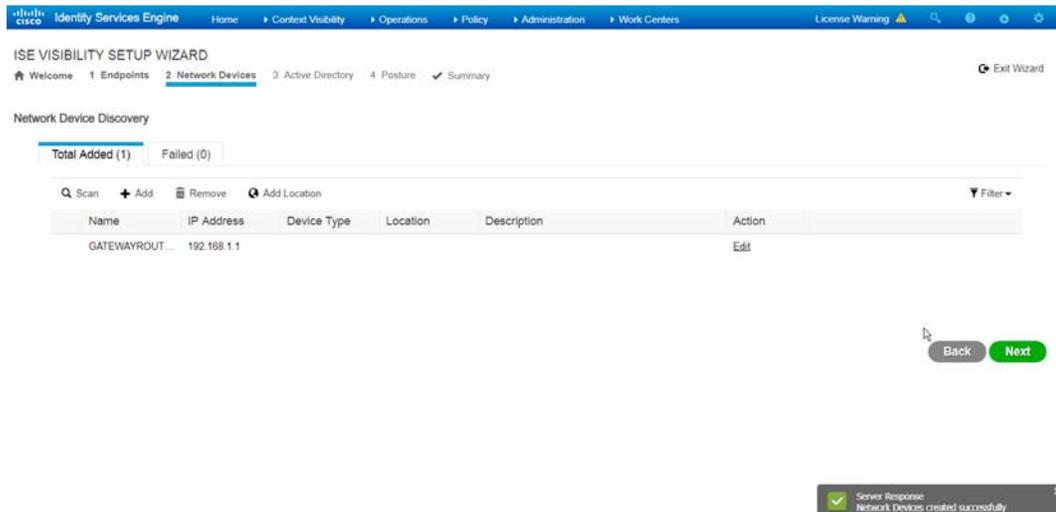
4. Enter the range of IP addresses to add to ISE's inventory.
5. Ensure that **Active Scanning** is checked.



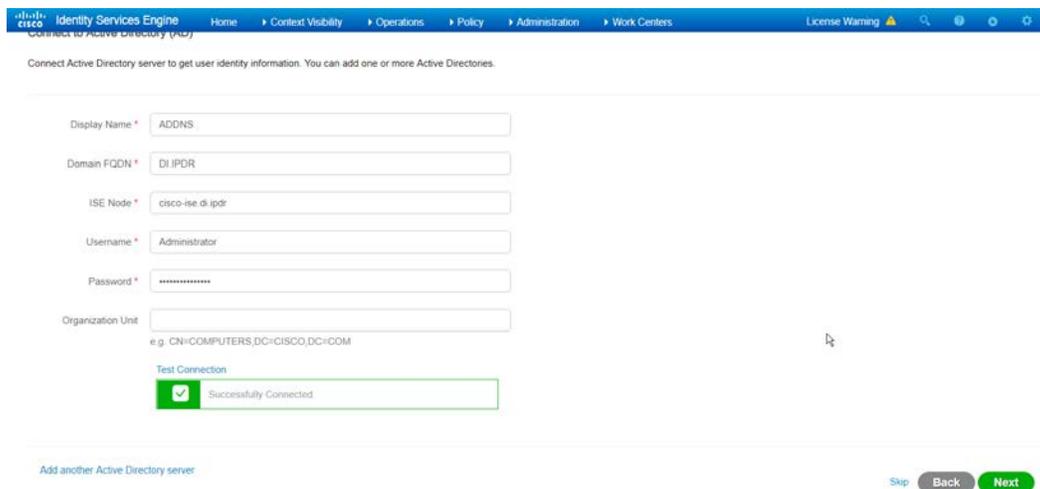
- 1831
  - 1832
  - 1833
  - 1834
  - 1835
  - 1836
  - 1837
6. Click **Next**.
  7. Click the **Add Device Manually** link.
  8. Enter a **name**.
  9. Enter the **IP address** of the network device you configured for SNMP.
  10. Select **1** for **SNMP version**.
  11. Enter the **community string** you created.



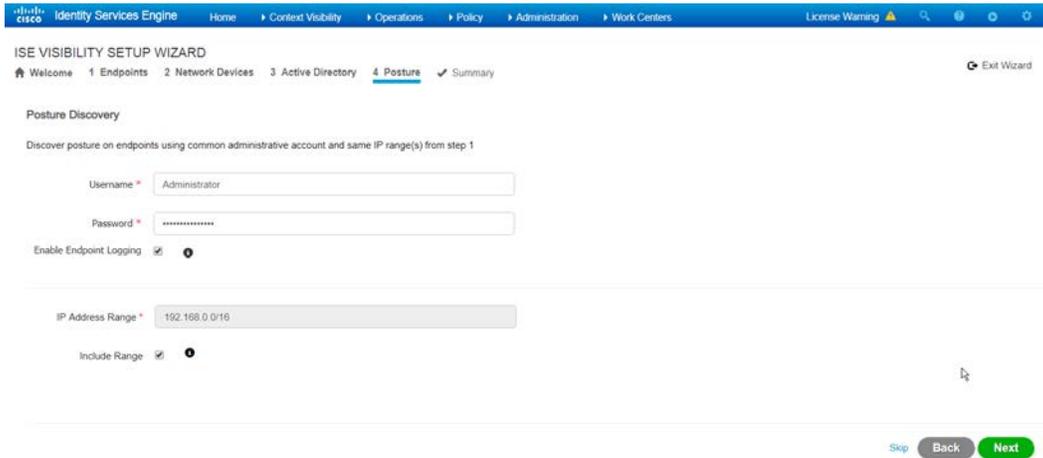
- 1838
  - 1839
12. Click **OK**.



- 1840
- 1841 13. Click **Next**.
- 1842 14. Enter a **display name**.
- 1843 15. Enter the **domain name**.
- 1844 16. Enter the **hostname** of Cisco ISE.
- 1845 17. Enter a **username** and **password**.
- 1846 18. Click **Test Connection** to ensure that this works.

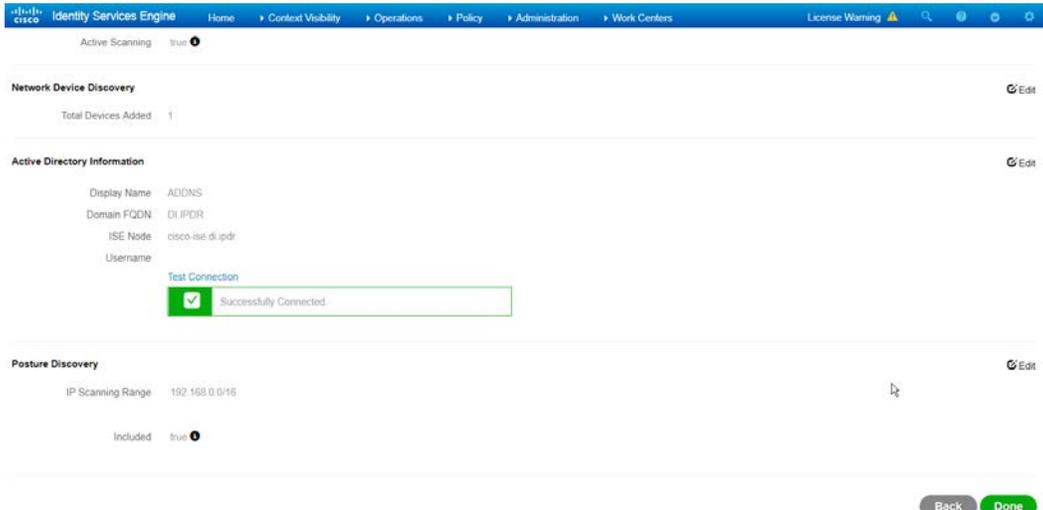


- 1847
- 1848 19. Click **Next**.
- 1849 20. Enter a **username** and **password**.
- 1850 21. Check the box next to **Enable Endpoint Logging**.
- 1851 22. Check the box next to **Include Range**.



1852  
1853

23. Click **Next**.

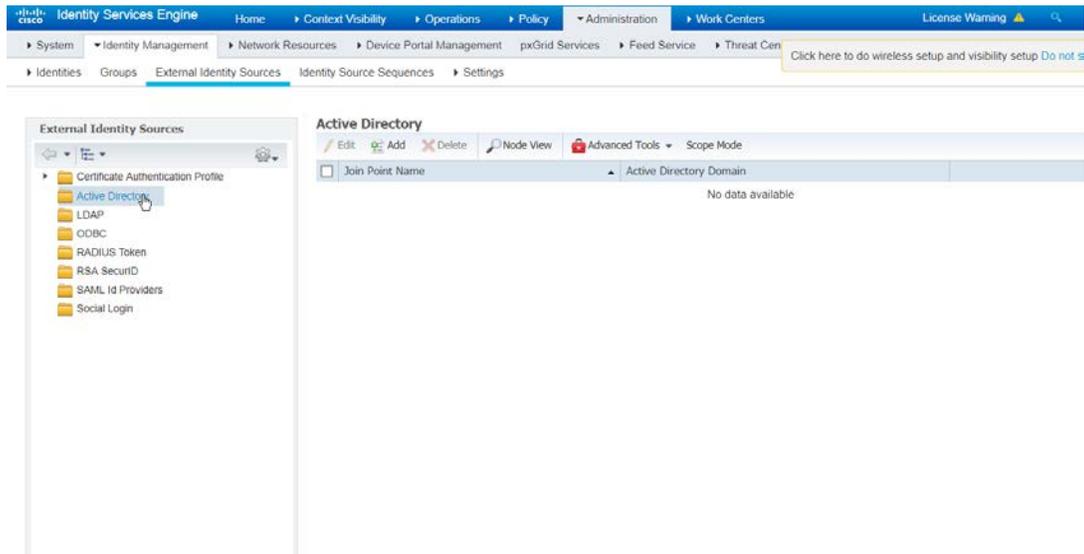


1854  
1855  
1856

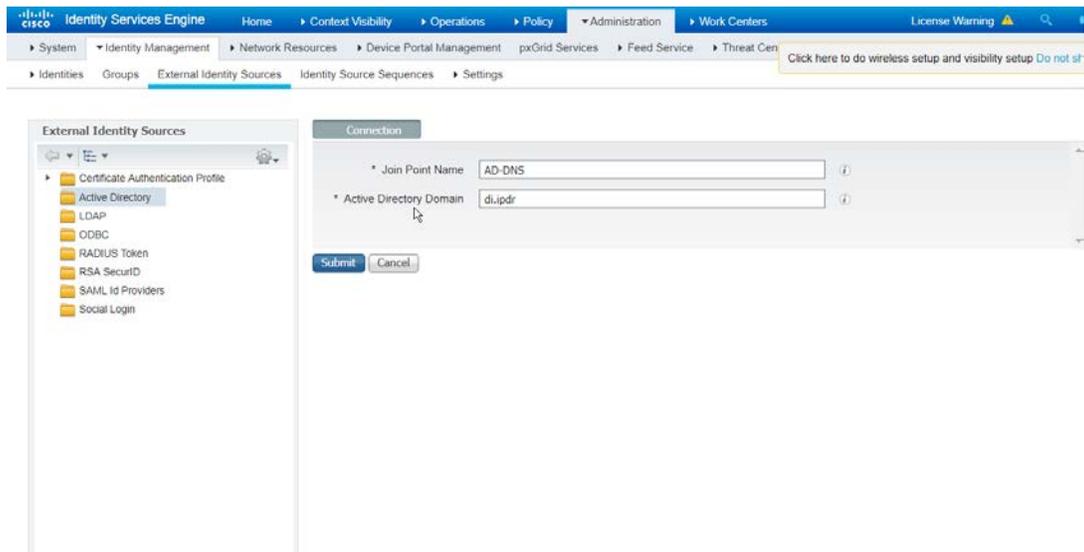
24. Verify the settings, and click **Done**. (This should begin importing endpoints connected to the network device, and they will be visible on the ISE dashboard.)

1857 **2.11.4 Policy Enforcement: Configure Active Directory Integration**

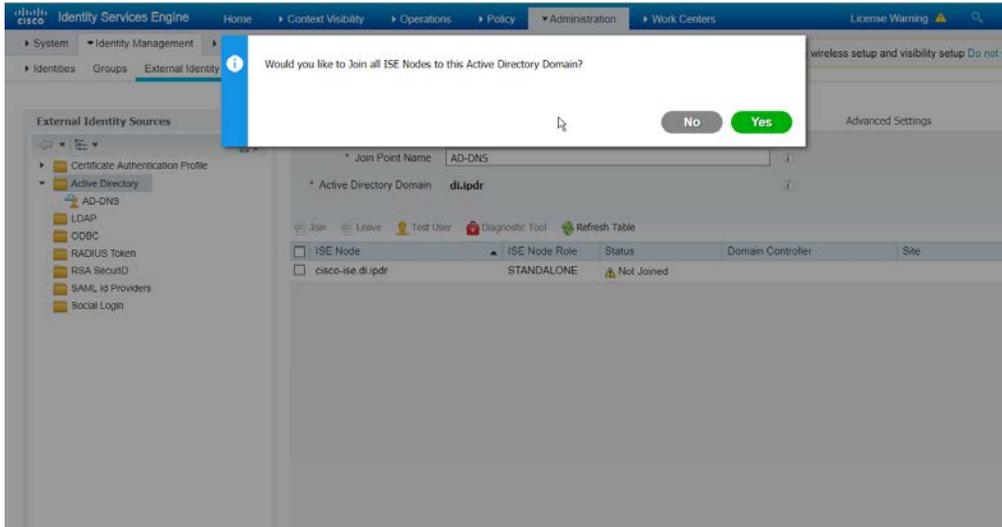
- 1858 1. Navigate to *Administration > Identity Management > External Identity Sources > Active*  
1859 *Directory*.



- 1860
  - 1861
  - 1862
  - 1863
2. Click **Add**.
  3. Enter a **name**.
  4. Enter the **domain**.

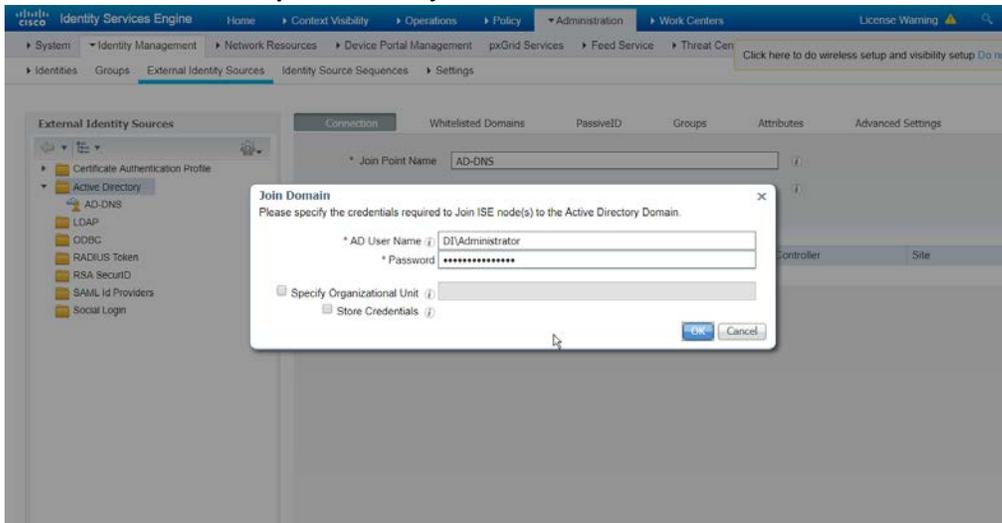


- 1864
  - 1865
5. Click **Submit**.



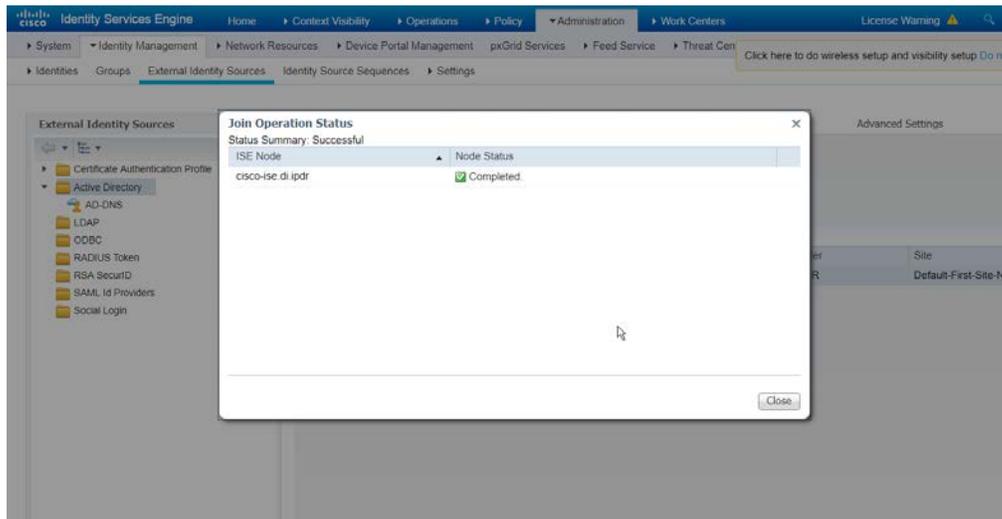
1866  
1867  
1868

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



1869  
1870

8. Click **OK**.

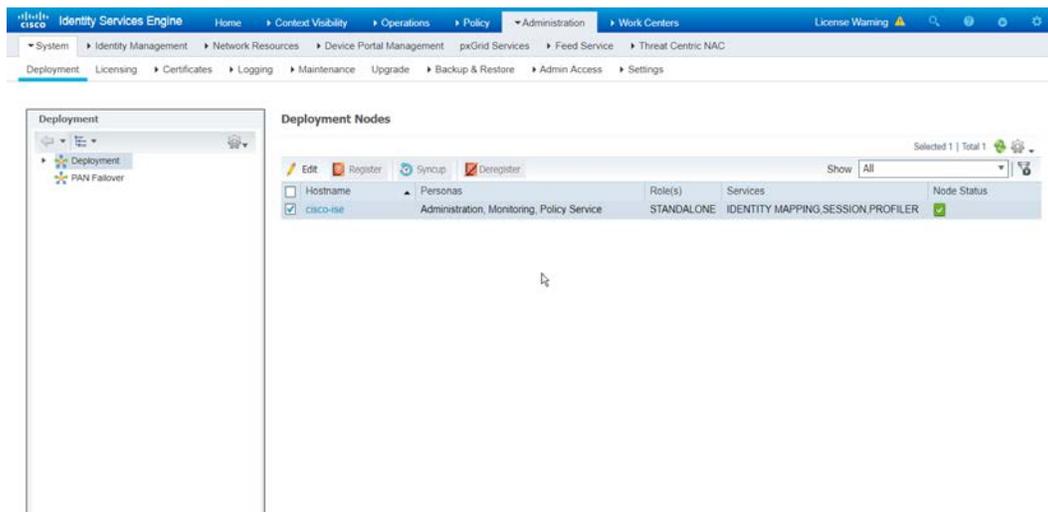


- 1871  
1872
9. Click **Close** when the join is finished.

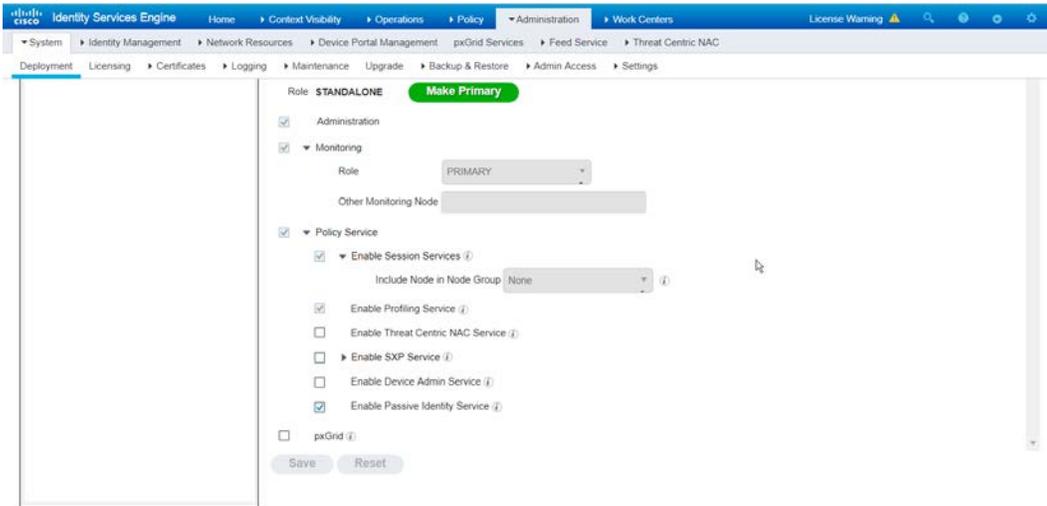
### 1873 2.11.5 Policy Enforcement: Enable Passive Identity with AD

1874 This configuration allows users to use Active Directory usernames/passwords as authentication for the  
1875 portal. The web portal will allow clients to download profiling software to ensure that clients have up to  
1876 date software and can be trusted on the network.

- 1877
1. Navigate to **Administration > System > Deployment**.
  2. Check the box next to **ISE**.
- 1878

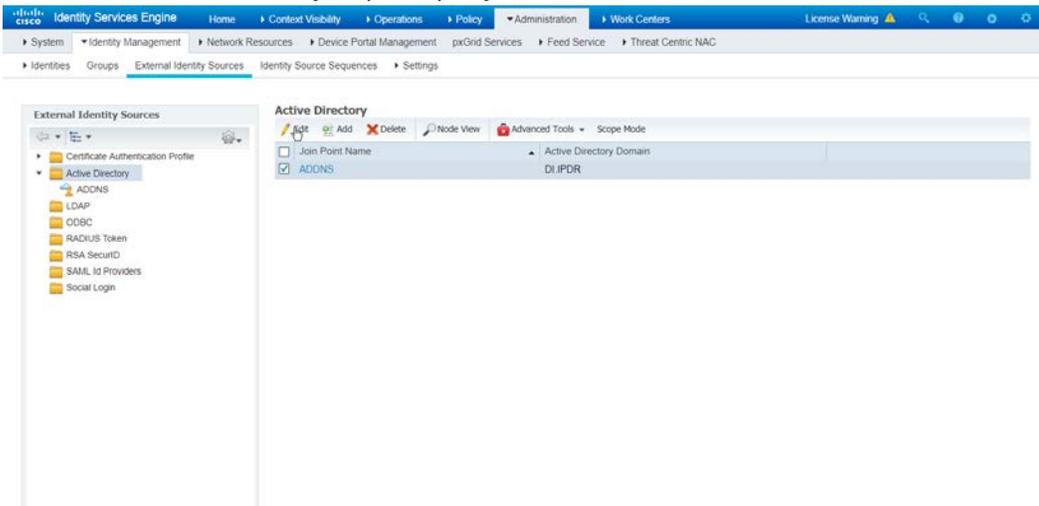


- 1879
3. Click **Edit**.
  4. Check the box next to **Enable Passive Identity Service**.
- 1880  
1881



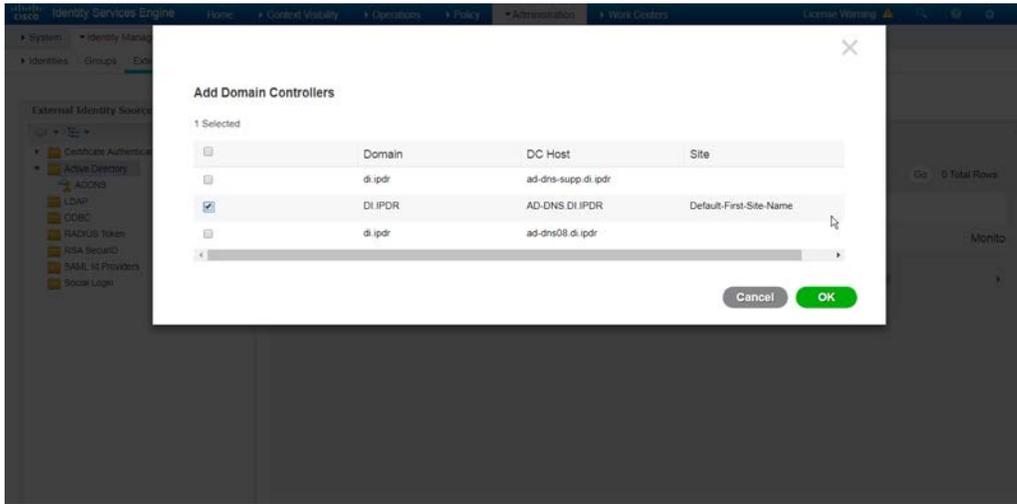
1882  
1883  
1884  
1885  
1886  
1887

5. Click **Save**.
6. Navigate to *Administration > Identity Management > External Identity Sources > Active Directory*.
7. Click the name of the Active Directory machine.
8. Check the box next to the join point you just created.

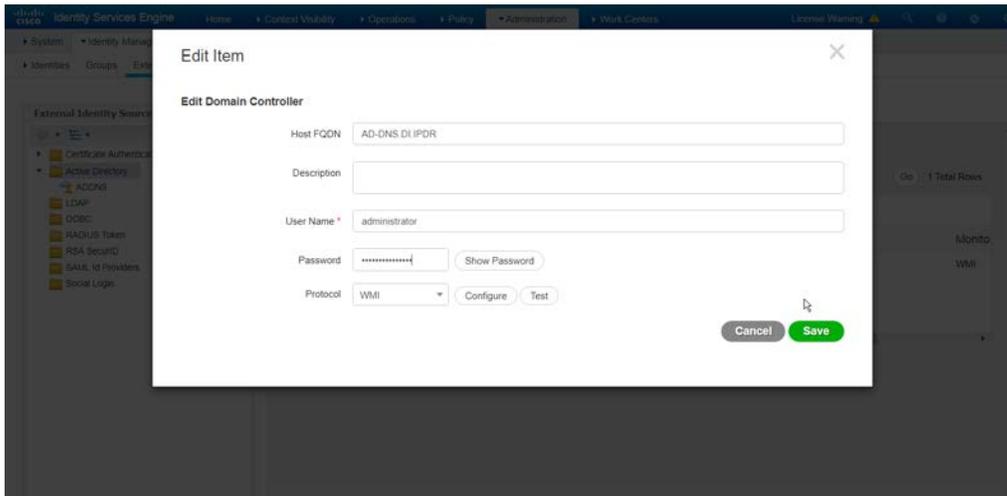


1888  
1889  
1890  
1891

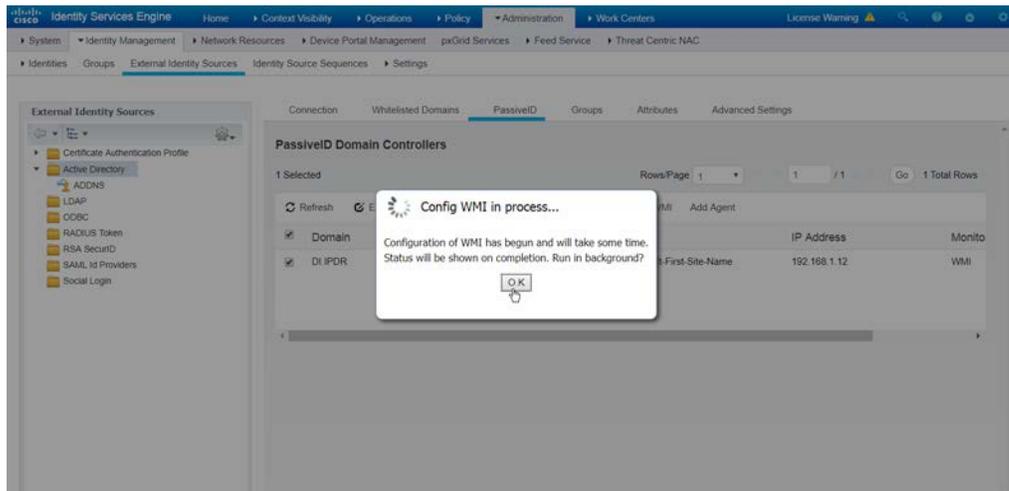
9. Click **Edit**.
10. Click the **PassiveID** tab.
11. Click **Add DCs** if there are no domain controllers listed.



- 1892
  - 1893
  - 1894
  - 1895
  - 1896
  - 1897
12. Select the Active Directory domain controller.
  13. Click **OK**.
  14. Check the box next to the selected domain controller.
  15. Click **Edit**.
  16. Enter credentials for an administrator account.

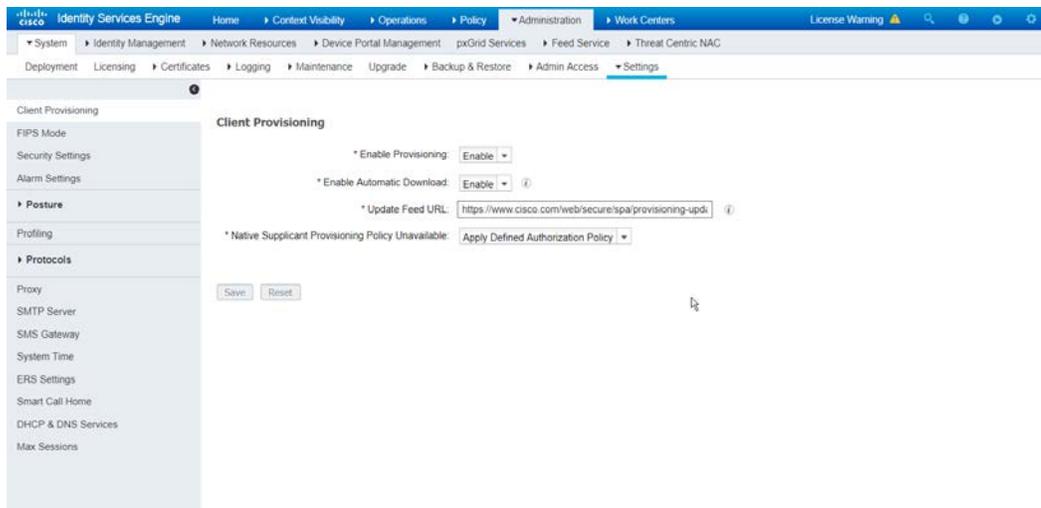


- 1898
  - 1899
  - 1900
  - 1901
17. Click **Save**.
  18. Click **Config WMI**.
  19. Click **OK**.



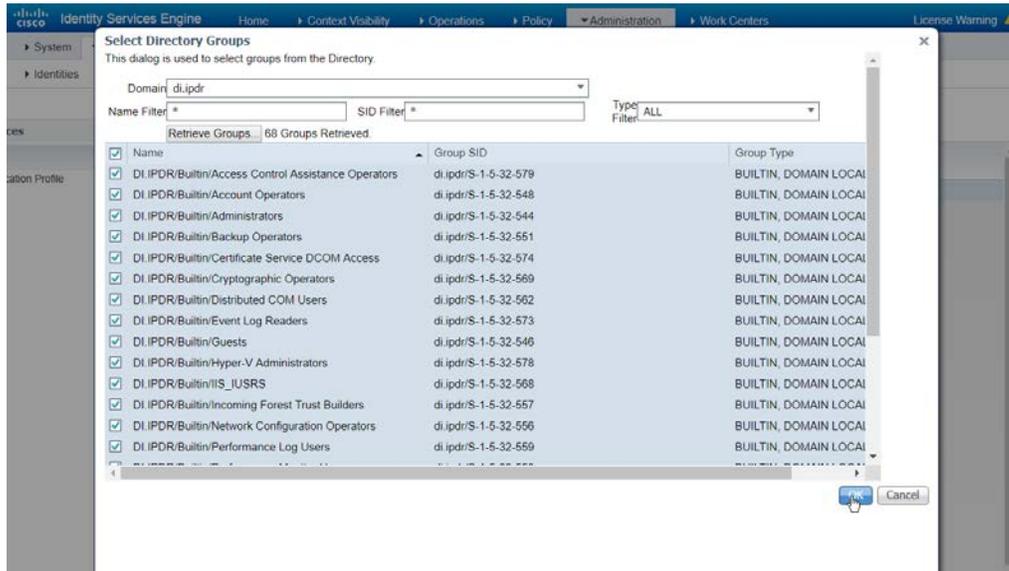
1902  
1903  
1904  
1905

20. Click **OK** when this configuration finishes.
21. Navigate to *Administration > System > Settings > Client Provisioning*.
22. Set Enable **Automatic Download** to **Enable**.

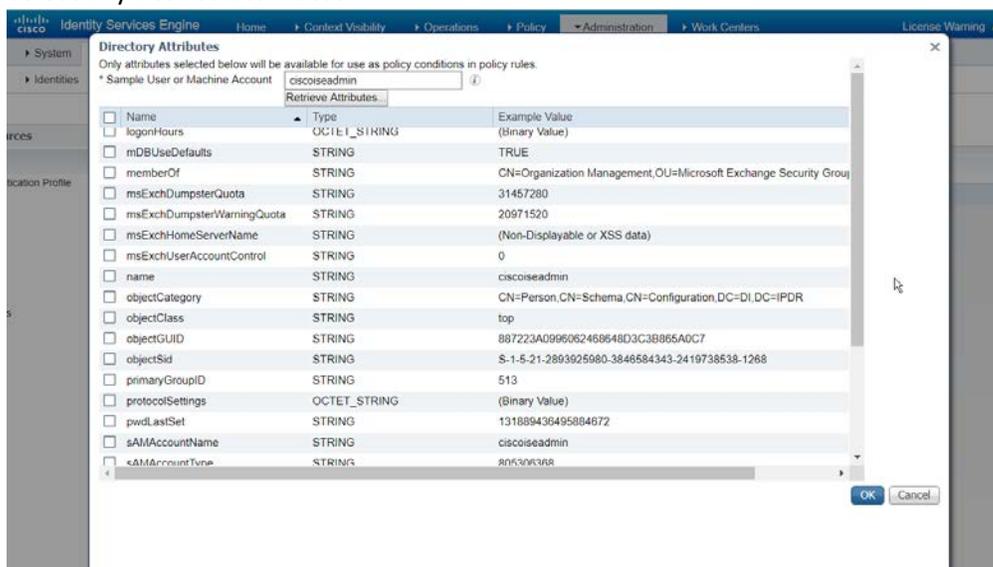


1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914

23. Click **Save**.
24. Navigate to *Administration > Identity Management > External Identity Sources > Active Directory*.
25. Click the **Groups** tab.
26. Click **Add > Select Groups from Directory**.
27. Click **Retrieve Groups**. (This should populate the window with the groups from Active Directory.)
28. Select them all.



- 1915
- 1916 29. Click **OK**. (If you add more groups to Active Directory, they can be imported in the same way in
- 1917 the future.)
- 1918 30. Click the **Attributes** tab.
- 1919 31. Click **Add > Select Attributes from Directory**.
- 1920 32. Enter a **username**.
- 1921 33. Click **Retrieve Attributes**. (This will populate the window with Active Directory's available
- 1922 attributes, so they can be used for policy in Cisco ISE.)
- 1923 34. Click **OK**.
- 1924 35. Select any desired attributes.

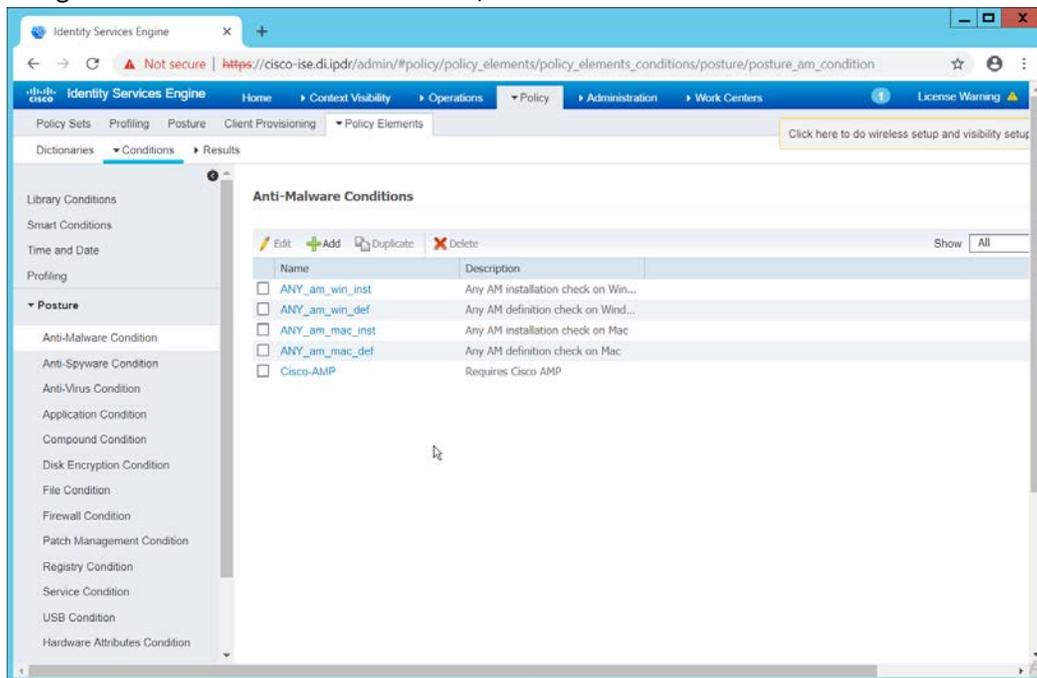


- 1925
- 1926 36. Click **OK**.

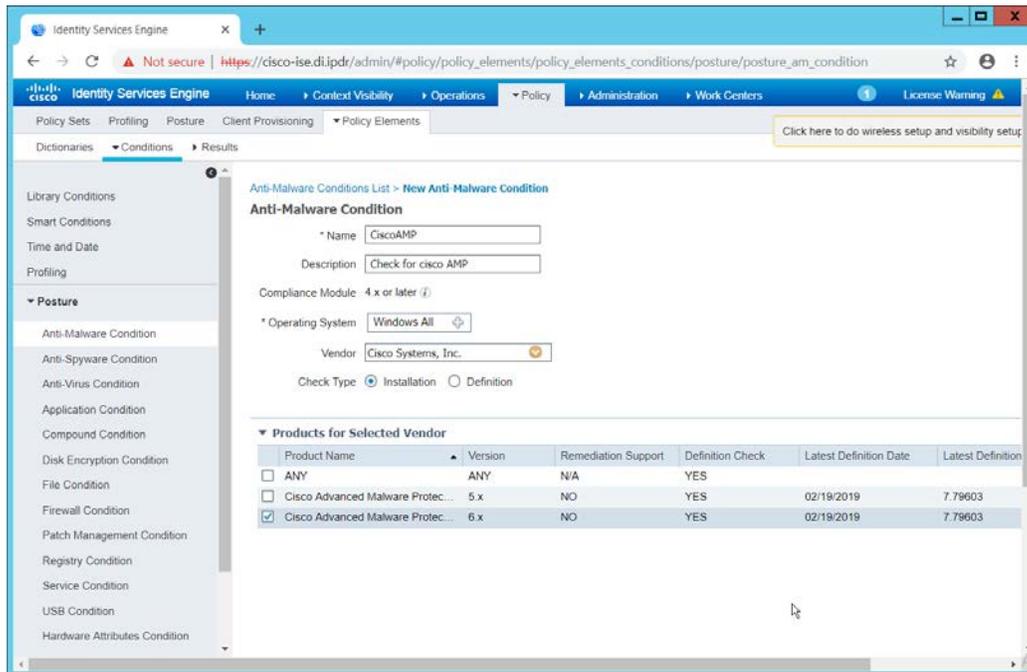
1927 37. Click **Save**.

## 1928 2.11.6 Policy Enforcement: Developing Policy Conditions

- 1929 1. Navigate to **Policy > Policy Elements > Conditions > Posture**.
- 1930 2. Expand the **Posture** section. This will reveal a list of categories for conditions. (Note: these
- 1931 conditions allow you to select or define requirements that endpoints should meet. In typical
- 1932 enterprises these conditions can be used as requirements to gain network access; however, this
- 1933 strongly depends on the capabilities of your network device. Furthermore, the network device
- 1934 3. As an example, we will require that Cisco AMP be installed on all Windows devices. If you are
- 1935 using a different anti-malware software, locate that instead. Click **Anti-Malware Condition**.



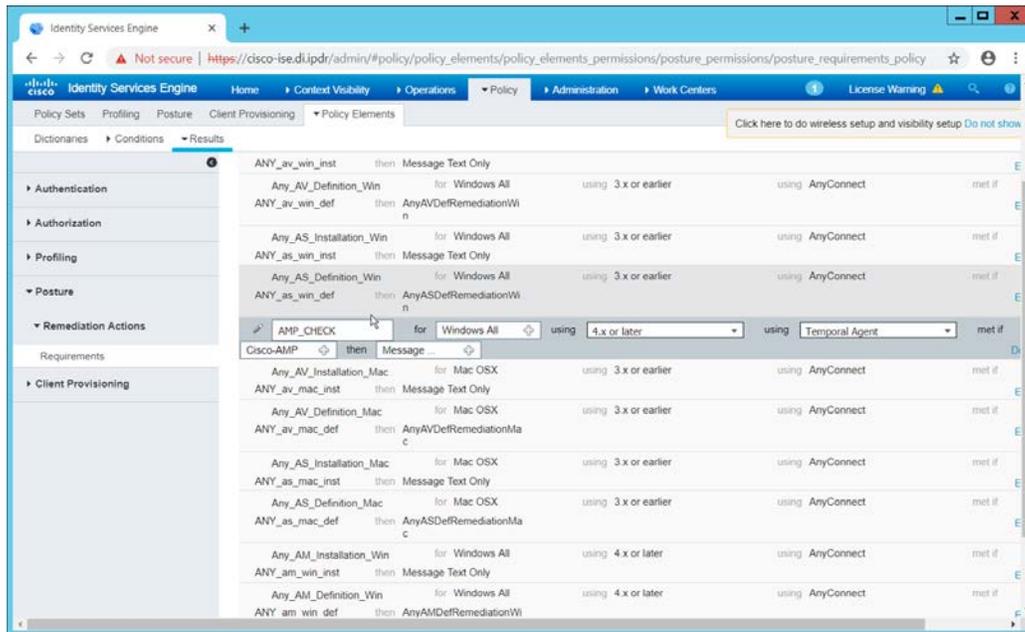
- 1936 4. Click **Add**.
- 1937 5. Enter a **name**.
- 1938 6. Enter a **description** if desired.
- 1939 7. Select **Windows All** for **Operating System**.
- 1940 8. Select **Cisco Systems, Inc.** for **Vendor**.
- 1941 9. Under **Products for Selected Vendor**, check the box next to **Cisco Advanced Malware**
- 1942 **Protection**, with the version number you have installed.
- 1943



1944  
1945 10. Click **Submit**.

## 1946 2.11.7 Policy Enforcement: Developing Policy Results

- 1947 1. Navigate to **Policy > Policy Elements > Results > Posture > Requirements**.
- 1948 2. Click one of the black arrows next to the **Edit** link, and select **Insert New Requirement**.
- 1949 3. Enter a **name**.
- 1950 4. Select **Windows All** for **Operating Systems**.
- 1951 5. Select **4.x or later** for **Compliance Module**.
- 1952 6. Select **Temporal Agent** for **Posture**.
- 1953 7. Select **User Defined Conditions > Anti-Malware Condition > Cisco AMP** (substitute "Cisco AMP" with the name of the condition you just created).
- 1954
- 1955 8. Select **Message Text Only** for the **Remediation Action**. (Other remediation actions can be
- 1956 defined by going to **Policy > Policy Elements > Results > Posture > Remediation Actions**, but
- 1957 there is no option for Cisco AMP to be installed, so we leave the default for now.)
- 1958 9. Enter a **Message** to show to the user to inform them that they must install Cisco AMP.



1959  
1960

10. Click **Save**.

1961

## 2.11.8 Policy Enforcement: Enforcing a Requirement in Policy

1962

1. Navigate to **Policy > Posture**.

1963

2. Click one of the black arrows next to the **Edit** link and select **Insert New Policy**.

1964

3. Enter a **name**.

1965

4. Select **Windows All** for **Operating Systems**.

1966

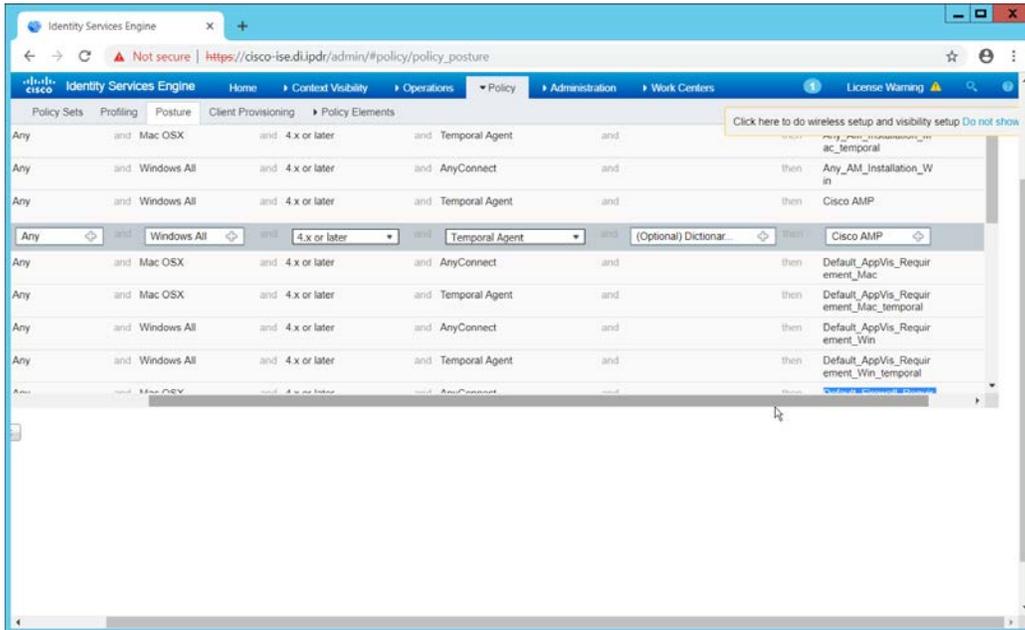
5. Select **4.x or later** for **Compliance Module**.

1967

6. Select **Temporal Agent** for **Posture Type**.

1968

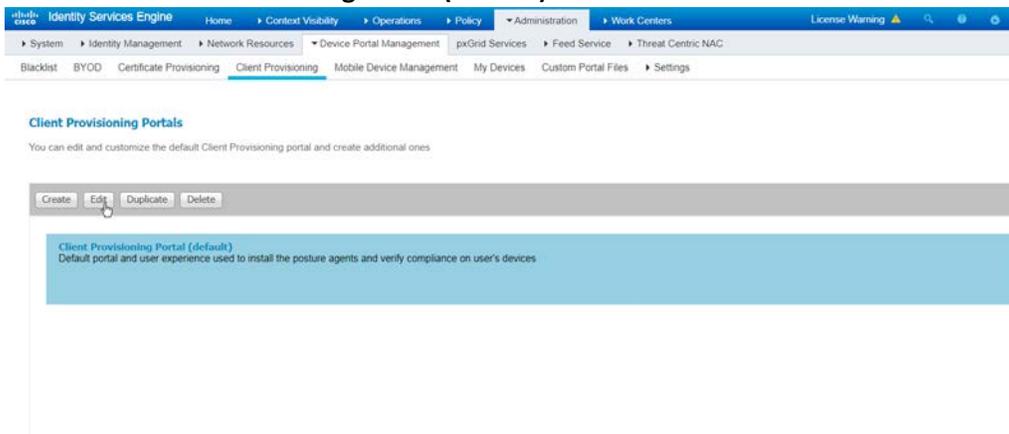
7. Select **Cisco AMP** (substitute "Cisco AMP" with the name of the requirement you just created).



- 1969
  - 1970
  - 1971
  - 1972
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.

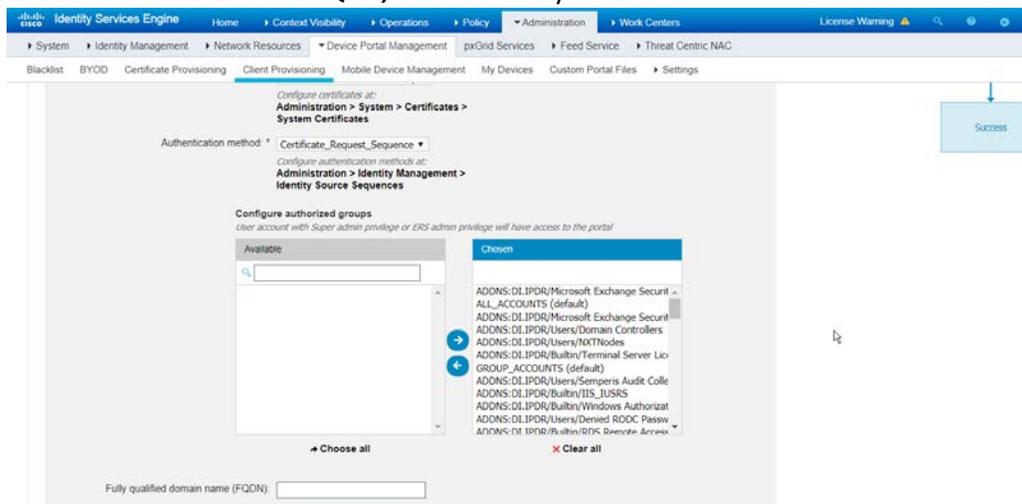
### 1973 2.11.9 Policy Enforcement: Configuring a Web Portal

- 1974
  - 1975
1. Navigate to **Administration > Device Portal Management > Client Provisioning**.
  2. Select the **Client Provisioning Portal (default)**.



- 1976
  - 1977
3. Click **Edit**.

- 1978 4. Under **Portal Settings**, go to **Configure authorized groups**, and select the groups that should  
 1979 require a Cisco ISE client.  
 1980 5. Enter a domain name for **FQDN**, and add it to your DNS.



- 1981 6. Click **Save**.  
 1982

### 1983 2.11.10 Configuring RADIUS with your Network Device

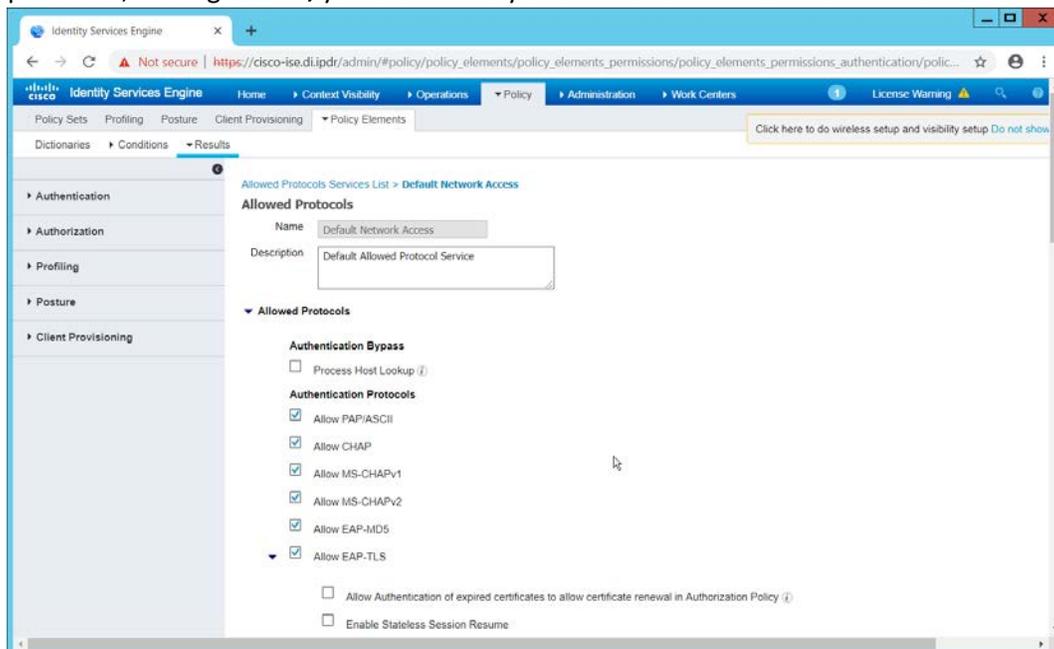
1984 Cisco ISE requires a RADIUS session for posture to function. Posture refers to ISE's ability to check that a  
 1985 machine complies with a specified policy, which may be based on the OS and may contain requirements  
 1986 such as the installation of certain security applications or the presence of configuration files. Machines  
 1987 that are not in compliance can be kept separated from the network. The process for setting this up  
 1988 varies widely between machines, but the overall requirements have commonalities between systems.

- 1989 1. The **Network Device** (i.e. the router or switch) must support RADIUS functions, specifically  
 1990 **Authentication, Authorization, and Accounting**. Furthermore, it must also support **CoA**, which  
 1991 is **Change of Authorization**.  
 1992 a. To configure this, you must configure your network device to use Cisco ISE as a Radius  
 1993 Server. What this means is that your network device will forward authentication  
 1994 requests to Cisco ISE, and Cisco ISE will respond with an "accept" or "reject."  
 1995 2. The **Network Device** must support some form of **802.1x**. Note that this is not supported on  
 1996 certain routers, even if RADIUS is supported. **802.1x** is a mechanism for authenticating the end  
 1997 workstation to the network device, potentially over wireless or through ethernet.  
 1998 a. This can take various forms, such as a captive web portal, MAC address authentication,  
 1999 or user authentication. A captive web portal, if the device supports it, may be ideal for  
 2000 configuration without the correct hardware.  
 2001 b. There are also many switches that provide direct 802.1x username/password  
 2002 authentication. Note that if you choose to use this mechanism, a client is still required,

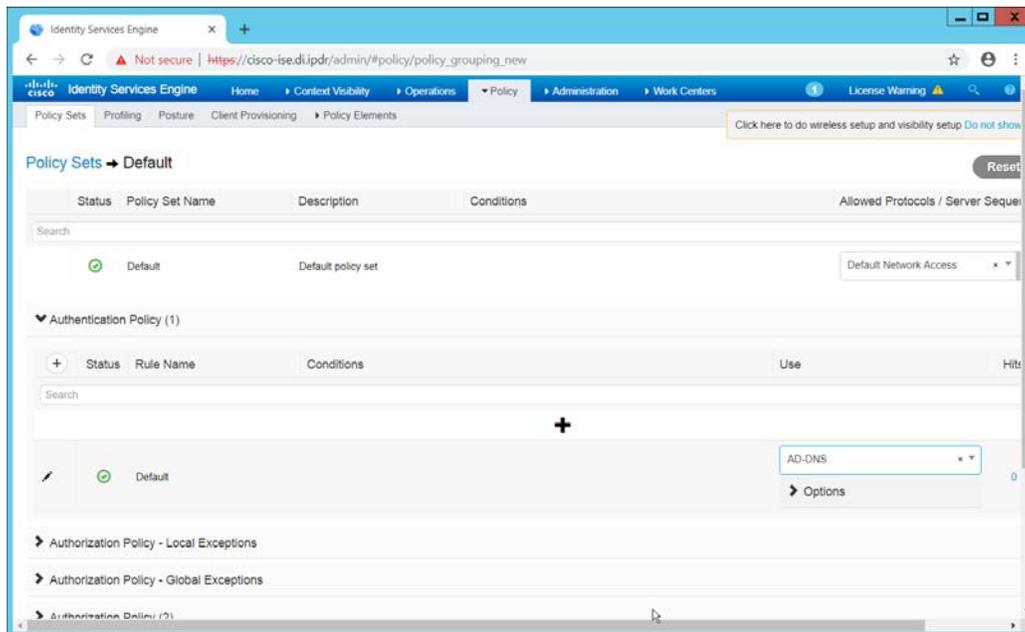
- 2003 and it will not be in the web browser. Windows has a built-in **802.1x** client that can be  
 2004 configured on Network adapters under the **Authentication** tab. To enable it, you must  
 2005 first start the service **Wired AutoConfig**, and then the **Authentication** tab will become  
 2006 available for configuration.
- 2007 c. Whichever form of **802.1x** is chosen, the request for authentication must be forwarded  
 2008 to Cisco ISE. Cisco ISE will process the request for authentication.
- 2009 3. The two steps above detail the **authentication** phase. Once authenticated, the network device  
 2010 must redirect the user to the client provisioning portal (or to a guest portal), depending on the  
 2011 setup. The URL for this can be acquired from the active **Authorization Profile** in ISE.
- 2012 4. The user will then authenticate to the **Guest Portal** or **Client Provisioning Portal** (depending on  
 2013 your setup). The portal will prompt the user to download an executable, which will run posture.
- 2014 5. The executable will *first* check for the existence of a RADIUS session in Cisco ISE for the user  
 2015 who downloaded the executable. It will primarily check the MAC address that visited the ISE  
 2016 web portal against the MAC addresses of existing sessions. *If and only if a session exists*, it will  
 2017 run posture based on the policy you set up. You can verify that a session exists by navigating to  
 2018 **Operations > RADIUS > Live Sessions**.

### 2019 2.11.11 Configuring an Authentication Policy

- 2020 1. Navigate to **Policy > Policy Elements > Results > Authentication > Allowed Protocols**.
- 2021 2. Select the **Default Network Access** protocol, or create your own.
- 2022 3. Ensure any protocols that need to be supported for your network setup are allowed. In  
 2023 particular, if using **802.1x**, you should likely check the box next to **Allow MS-CHAPv2**.



- 2025 4. Click **Save**.
- 2026 5. Navigate to **Policy > Policy Sets**.
- 2027 6. Select the default policy.
- 2028 7. Ensure that the **Allowed Protocol** selection matches the allowed protocol you just
- 2029 created/edited.
- 2030 8. Expand the **Authentication Policy** section, and select the ID stores from which to authenticate
- 2031 users. For example, if you set up an Active Directory integration, it may be desirable to
- 2032 authenticate users from there.

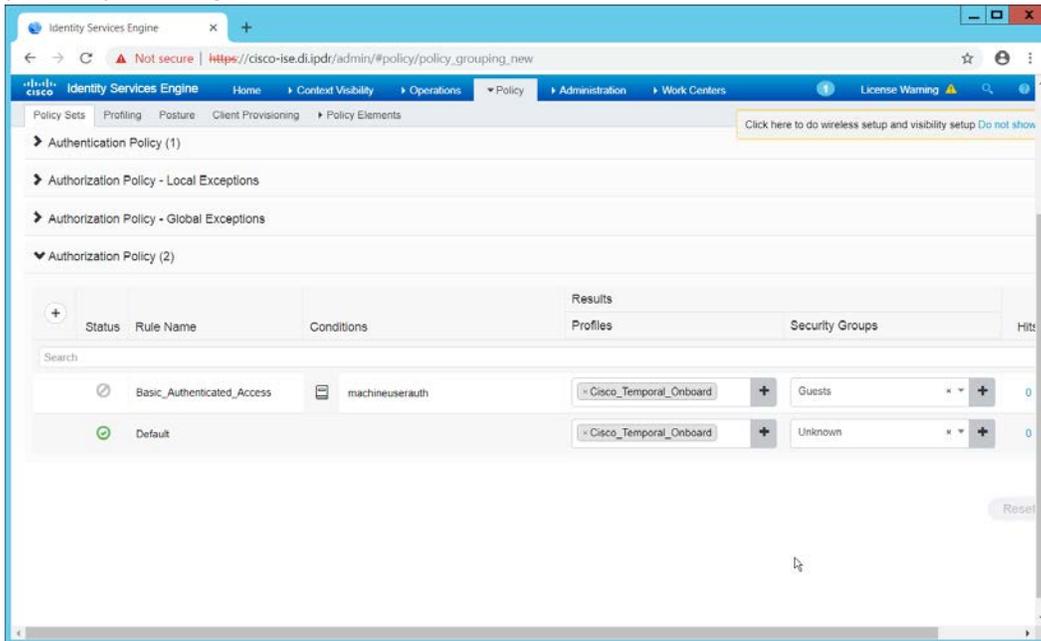


- 2033 9. Click **Save**.
- 2034

### 2035 2.11.12 Configuring an Authorization Policy

- 2036 1. The Authorization Profile is likely dependent on your network device, but it is possible that the
- 2037 **Cisco\_Temporal\_Onboard** profile will work even for non-Cisco devices. You can edit the
- 2038 authorization policy by navigating to **Policy > Policy Elements > Results > Authorization >**
- 2039 **Authorization Profiles**.
- 2040 2. The temporal onboard profile will attempt to redirect the user to a client provisioning portal–
- 2041 this redirection will most likely only happen automatically on compatible Cisco network devices.
- 2042 If another device is used, the device may need to manually redirect the user to the client
- 2043 provisioning portal after authentication. (We accomplished this in PFSense for our build using a
- 2044 “Post-authentication redirection” feature in the Captive Portal.)
- 2045 3. Once you are finished configuring the **Authorization Profile**, navigate to **Policy > Policy Sets**.
- 2046 4. Select the default policy.
- 2047 5. Expand the **Authorization Policy** section.

- 2048 6. Note that you can configure this for as many groups and conditions as desired, potentially  
 2049 specifying different authorization profiles for various user groups or levels of authentication,  
 2050 including unauthenticated access. Under **Results > Profiles**, you can select the authorization  
 2051 profiles you configured.



- 2052 7. Click **Save**.  
 2053

## 2054 2.12 Cisco Advanced Malware Protection

2055 This section assumes the use of the Cisco Advanced Malware Protection (AMP) Console, a cloud-based  
 2056 server that connects to clients on individual machines. There is some configuration to be done on this  
 2057 cloud-based server, which may impact the installation. Cisco provides best practices guides online for  
 2058 AMP configuration. Here is a link to one such guide:

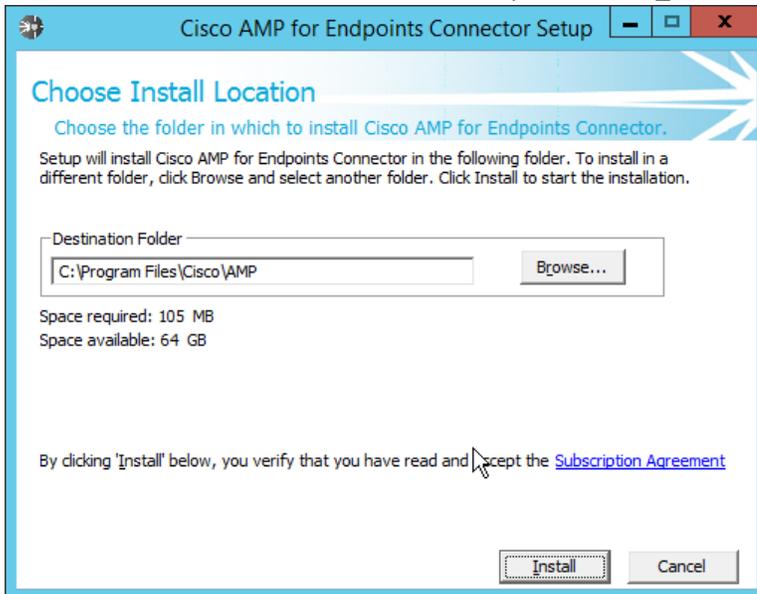
2059 <https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/213681-best-practices-for-amp-for-endpoint-excl.html>.  
 2060

### 2061 2.12.1 Dashboard Configuration

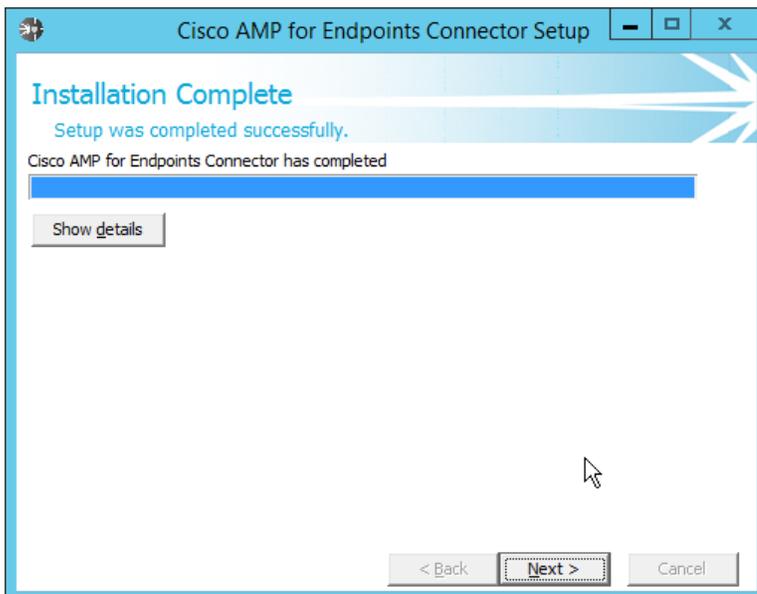
- 2062 1. From the Cisco AMP dashboard, located at <https://console.amp.cisco.com/dashboard>, click **Set**  
 2063 **Up Windows Connector**.  
 2064 2. The configuration of this will be different for each enterprise, so consult your Cisco  
 2065 representative for the proper way to set this up. For the purposes of this build, we accepted the  
 2066 default values.

2067 **2.12.2 Installing the Connector on a Windows Server**

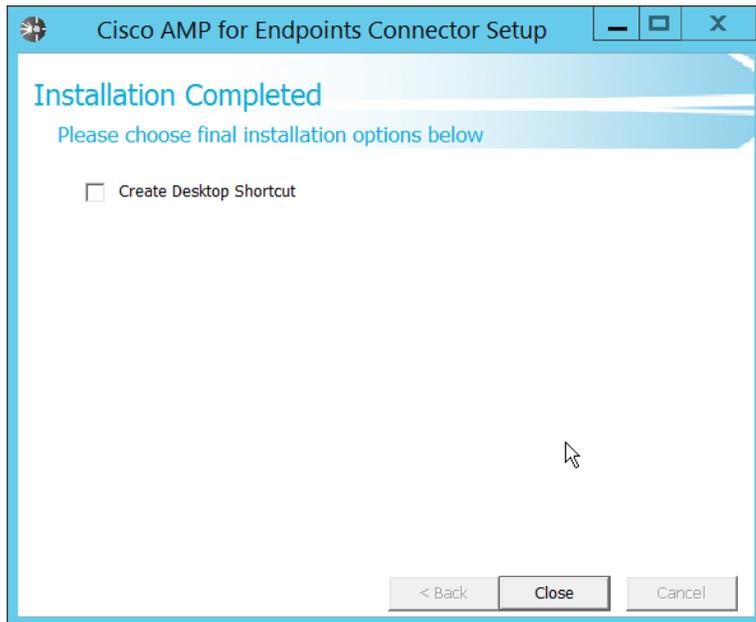
- 2068 1. On the Cisco AMP dashboard, navigate to **Management > Download Connector**.
- 2069 2. Select the AMP group in which to put the machine. For example, when installing on an Active
- 2070 Directory machine, we chose **Domain Controller**.
- 2071 3. Find the correct OS version of the installer, and click **Download**.
- 2072 4. Run the downloaded executable (for example, **Domain\_Controller\_FireAMPSetup.exe**).



- 2073 5. Click **Install**.
- 2074



- 2075 6. Click **Next**.
- 2076

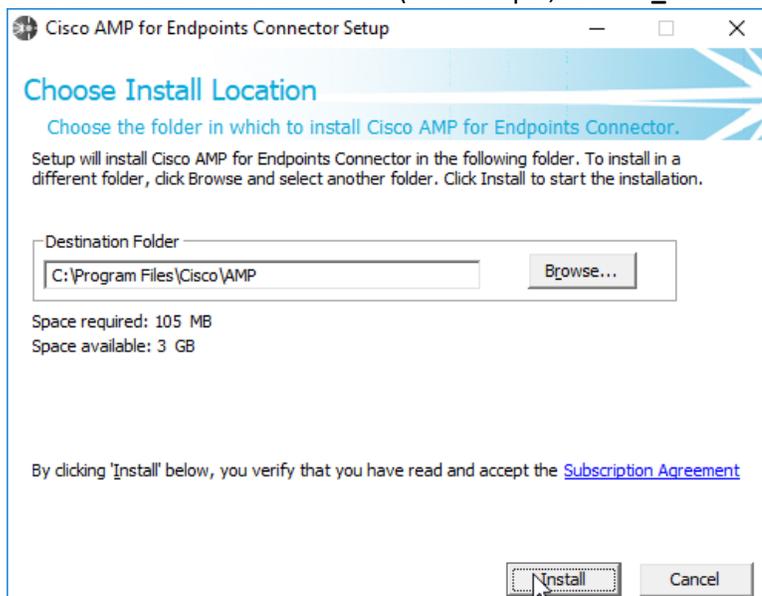


2077  
2078

7. Click **Close**.

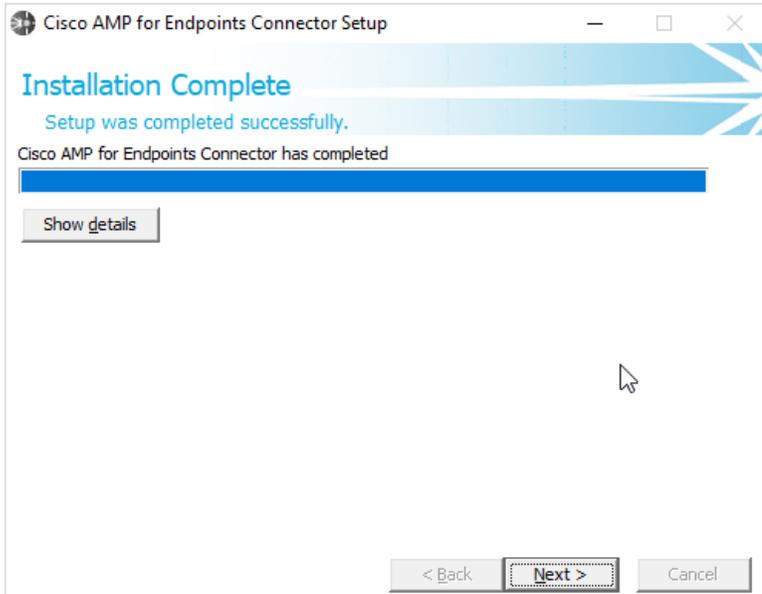
### 2079 2.12.3 Installing the Connector on a Windows 10 Machine

- 2080 1. On the Cisco AMP dashboard, navigate to **Management > Download Connector**.
- 2081 2. Select the AMP group in which to put the machine. For this installation we chose **Protect**.
- 2082 3. Find the correct OS version of the installer, and click **Download**.
- 2083 4. Run the downloaded executable (for example, **Protect\_FireAMPSetup.exe**).

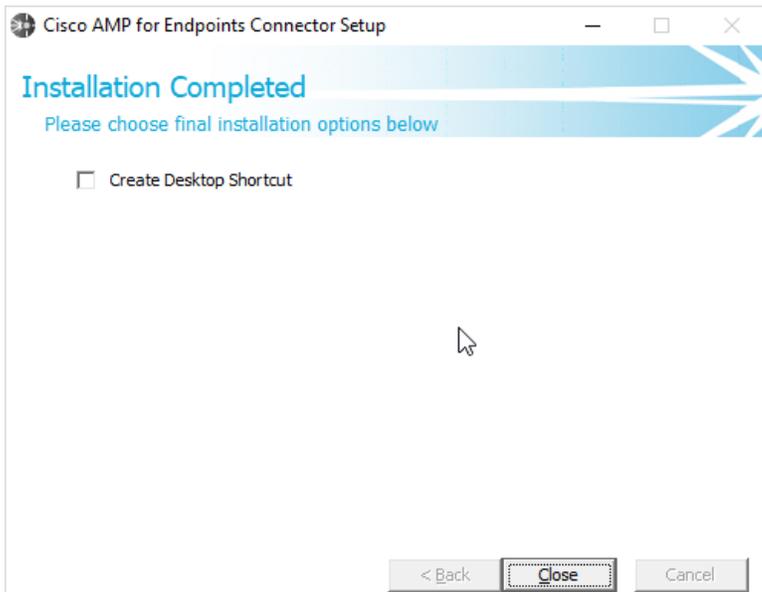


2084

2085 5. Click **Install**.



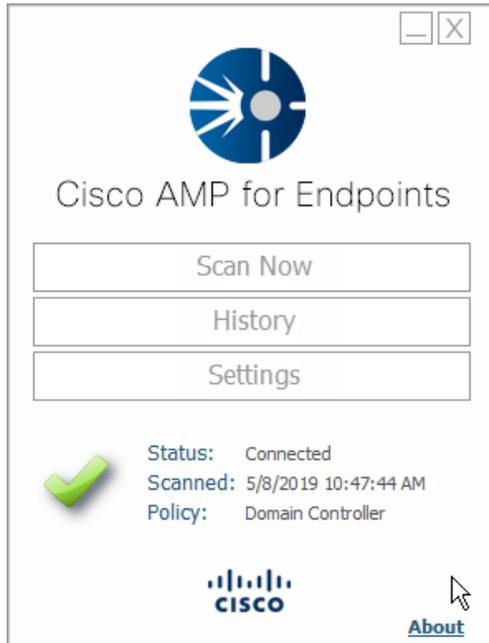
2086 6. Click **Next**.  
2087



2088 7. Click **Close**.  
2089

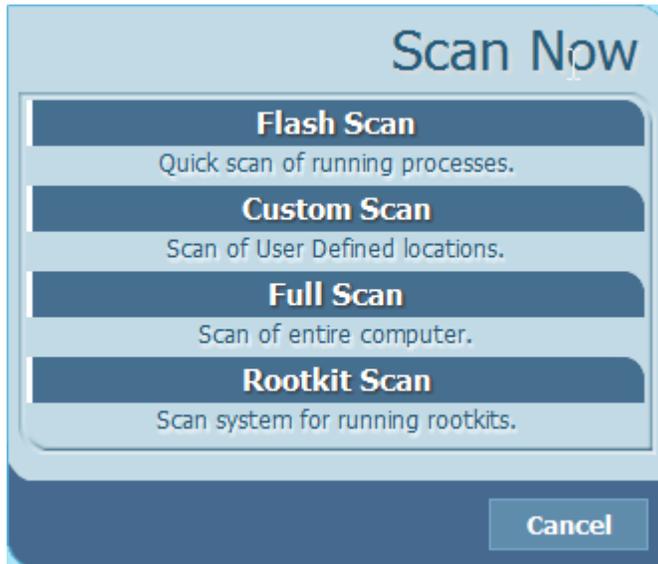
## 2090 2.12.4 Scanning using AMP

2091 1. If the AMP software does not run automatically, open it from the **start** menu.



2092  
2093

2. Click **Scan Now**.



2094  
2095  
2096

3. Click **Full Scan**.
4. A scan should begin.

## 2097 2.12.5 Configure AMP Policy

- 2098 1. On the web console, navigate to **Management > Policies**.

- 2099 2. Select a policy to edit; for this example, we choose **Domain Controllers**. (To edit which policies  
2100 map to which groups, select **Management > Groups**, and click **Edit** on the group for which you  
2101 wish to select a policy. You can select a policy for each Operating System (OS) in that group.)

**Policies** [View All Changes](#)

Search

All Products Windows Android Mac Linux iOS + New Policy...

Audit This policy puts the AMP for Endpoints Connector in a mode that will only detect malicious files but not quarantine them. ... 1 0

Audit Mode Policy-This is for monitoring and visibility only. NO BLOCKING This policy puts the AMP for Endpoints Connector in ... 1 0

Blocking Policy. All detections are set to BLOCK. This is the standard policy for the AMP for Endpoints Connector that will quara... 1 0

Domain Controller This is a lightweight policy for use on Active Directory Domain Controllers. 1 2

Modes and Engines		Exclusions	Proxy	Groups
Files	Audit	Altiris by Symantec	Not Configured	Domain Controller 2
Network	Disabled	AVAST		
Malicious Activity Prote...	Disabled	Avira		
System Process Protection Protect		Diebold Warsaw		

**Outbreak Control**

Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
File Blacklist	Not Configured	Execution Blacklist File Whitelist	Blocked Allowed

[View Changes](#) Modified 2019-05-20 14:56:48 UTC Serial Number 54 [Download XML](#) [Duplicate](#) [Edit](#) [Delete](#)

Protect This is the standard policy for the AMP for Endpoints Connector that will quarantine malicious files and block malicious ... 1 0

Server This is a lightweight policy for high availability computers and servers that require maximum performance and uptime. 1 0

1 - 8 of 8 total records 25 / page 1 of 1

- 2102 3. Click **Edit**.
- 2103 4. In the **Modes and Engines** tab, “Conviction Modes” refers to the *response* taken to various  
2104 detected suspicious activity or files.  
2105
- 2106 • **Audit** is a detection/logging approach that does not take any action other than logging  
2107 the activity.
  - 2108 • **Quarantine** involves the move of the offending file to its own folder, where it is  
2109 monitored and deleted after a certain amount of time. Quarantining can also be applied  
2110 to processes, in which the process is monitored and prevented from affecting system  
2111 operations.
  - 2112 • **Block** involves the deletion of the file or the stopping of the process or network traffic.
- 2113 5. “Detection Engines” refer to the actual detection of the suspicious activity.
- 2114 • **TETRA** is intended to be an anti-malware engine and recommends that it not be used  
2115 when other antimalware software is in use.
  - 2116 • **Exploit Prevention** refers to an engine that defends endpoints against memory injection  
2117 attacks.

Name: Domain Controller

Description: This is a lightweight policy for use on Active Directory Domain Controllers.

**Modes and Engines**

**Exclusions**  
20 exclusion sets

**Proxy**

**Outbreak Control**

**Product Updates**

**Advanced Settings**

**Conviction Modes**

These settings control how AMP for Endpoints responds to suspicious files and network activity.

Files

Quarantine Audit

Network

Block Audit Disabled

Malicious Activity Protection

Quarantine Block Audit Disabled

System Process Protection

Protect Audit Disabled

**Detection Engines**

TETRA ⓘ

Exploit Prevention ⓘ

**Recommended Settings**

**Workstation**

Files: Quarantine

Network: Block

Malicious Activity Protection: Quarantine

System Process Protection: Protect

**Server**

Files: Quarantine

Network: Disabled

Malicious Activity Protection: Disabled

System Process Protection: Disabled

Cancel Save

2118  
2119

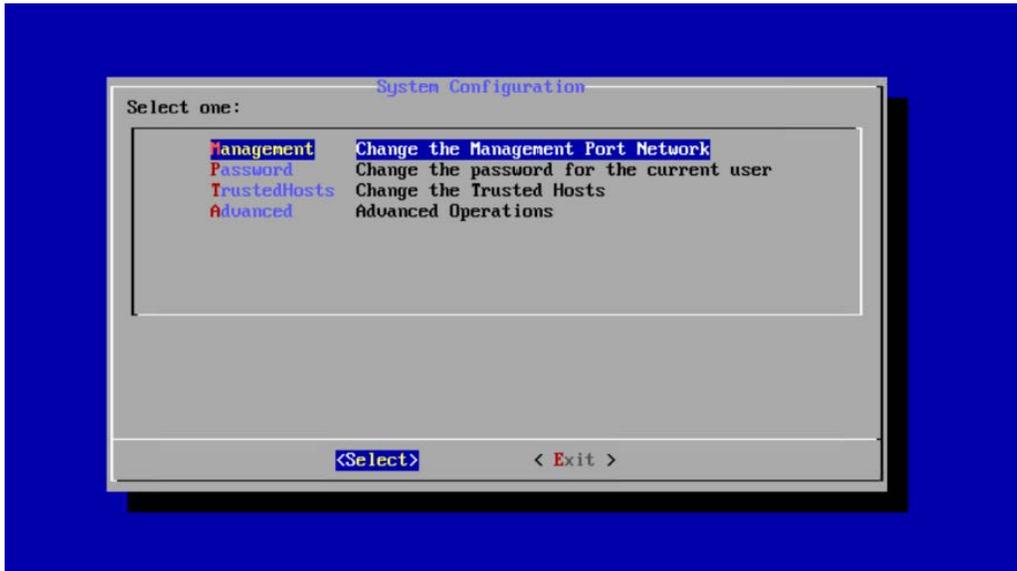
6. Click **Save**.

## 2120 2.13 Cisco Stealthwatch

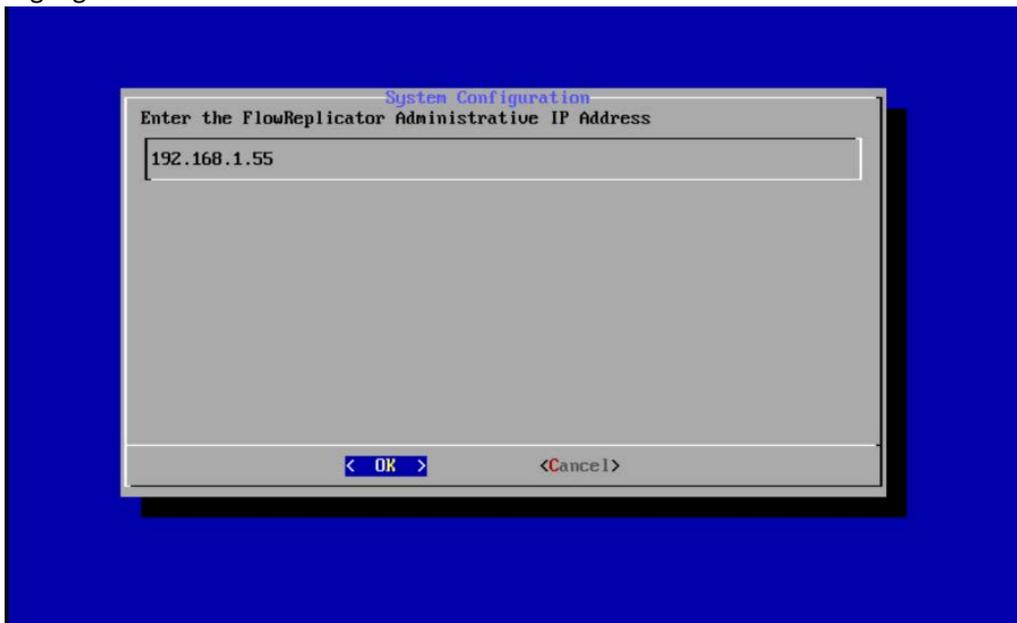
2121 This section will describe the setup and configuration of Cisco Stealthwatch, a network monitoring  
2122 solution. This guide assumes the use of the Stealthwatch virtual machines.

### 2123 2.13.1 Configure Stealthwatch Flow Collector, Stealthwatch Management 2124 Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor

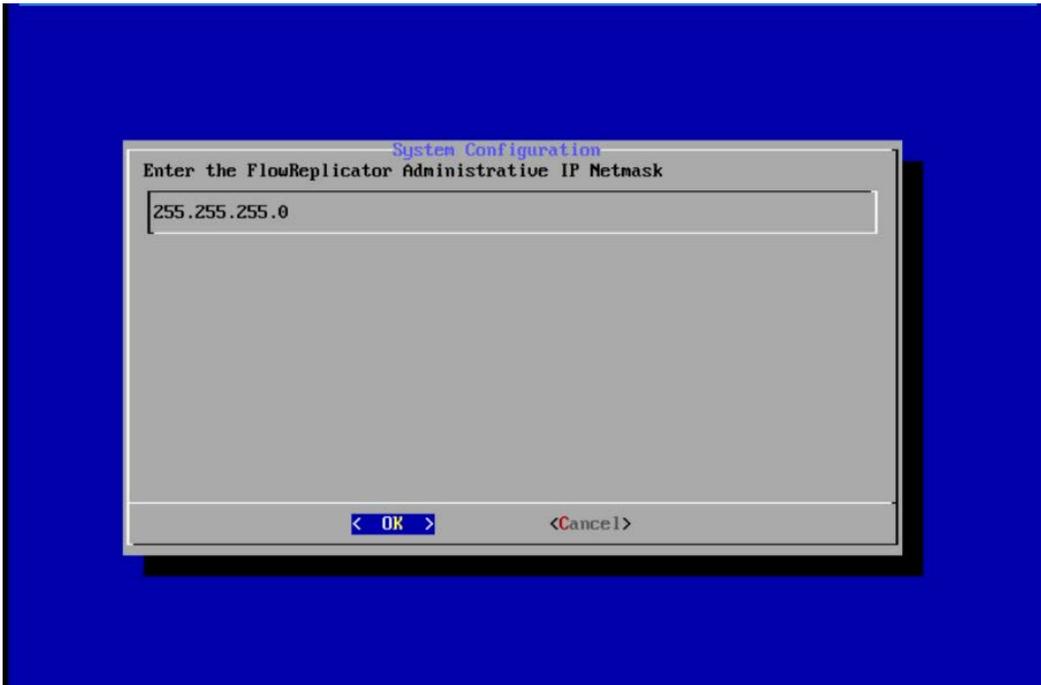
- 2125 1. Log in to the console of **Stealthwatch Flow UDP Director**.
- 2126 2. Navigate the menu to highlight **Management** and **Select**.



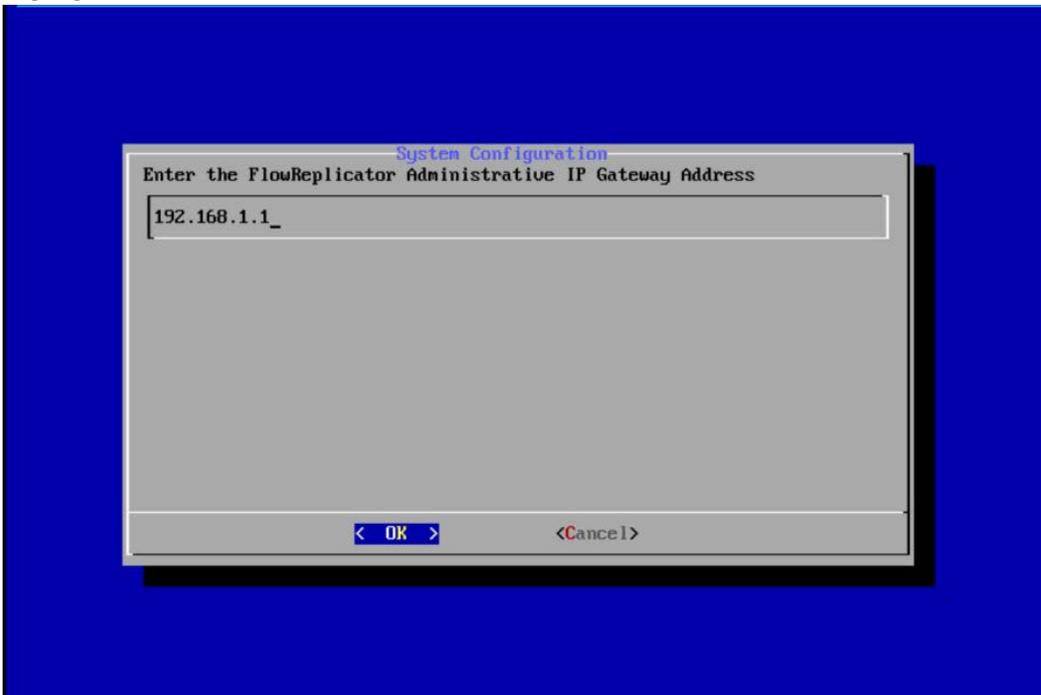
- 2127
  - 2128
  - 2129
  - 2130
3. Press **Enter**.
  4. Enter an **IP Address** for this machine.
  5. Highlight **OK**.



- 2131
  - 2132
  - 2133
  - 2134
6. Press **Enter**.
  7. Enter a **network mask** for the IP Address.
  8. Highlight **OK**.

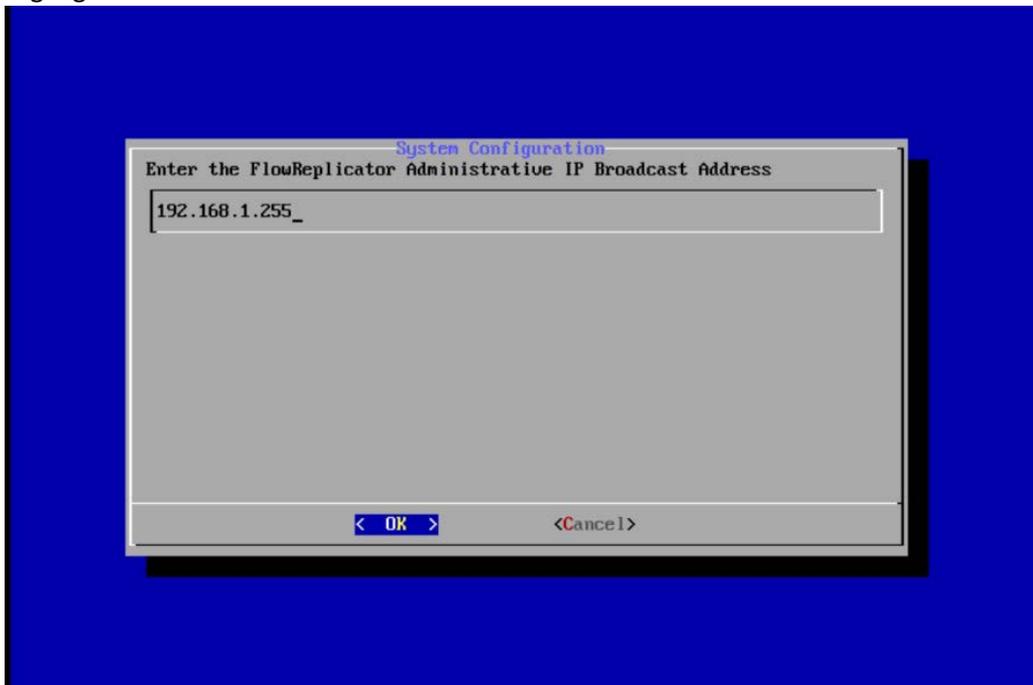


- 2135
- 2136 9. Press **Enter**.
- 2137 10. Enter the network **gateway**.
- 2138 11. Highlight **OK**.

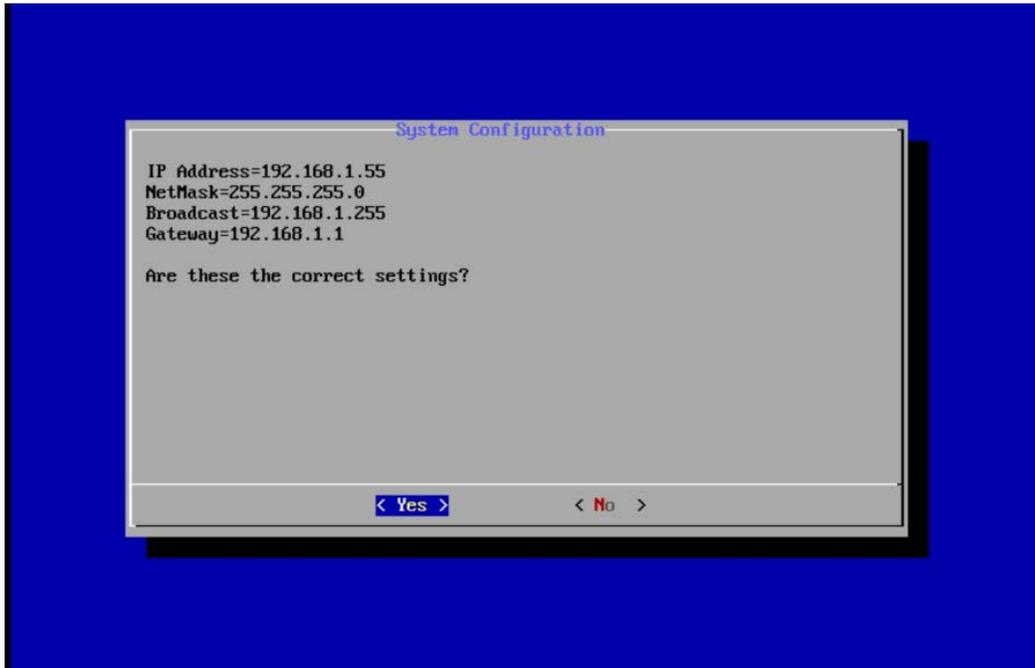


2139

- 2140 12. Press **Enter**.
- 2141 13. Enter the network **broadcast address**.
- 2142 14. Highlight **OK**.



- 2143 15. Press **Enter**.
- 2144 16. Highlight **Yes**.
- 2145



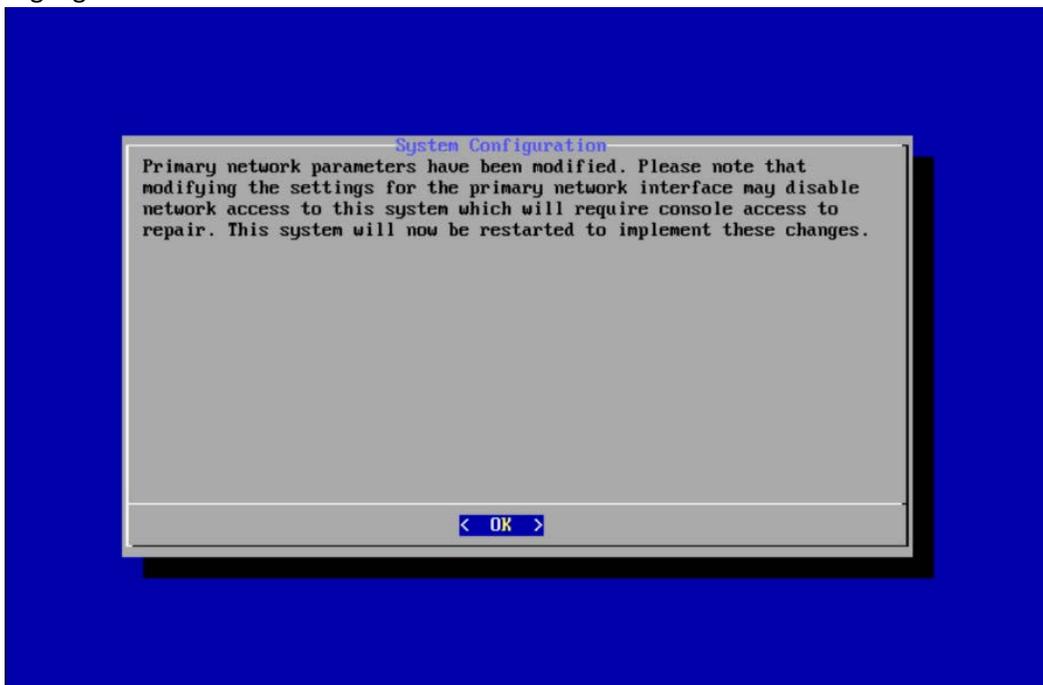
2146

2147

2148

17. Press **Enter**.

18. Highlight **OK**.



2149

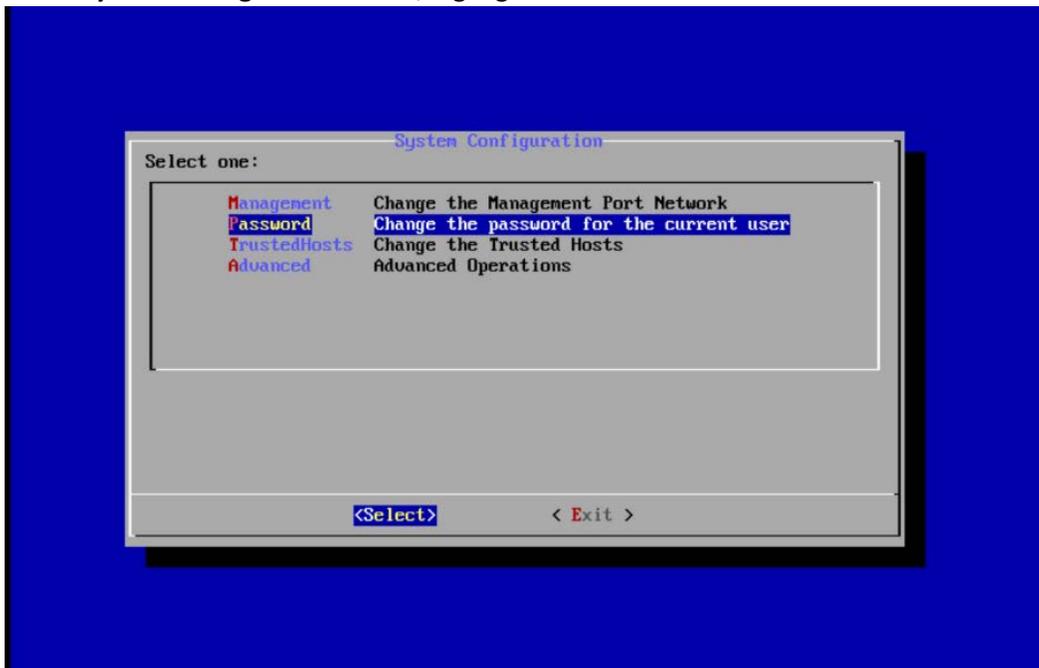
2150

19. Press **Enter**.

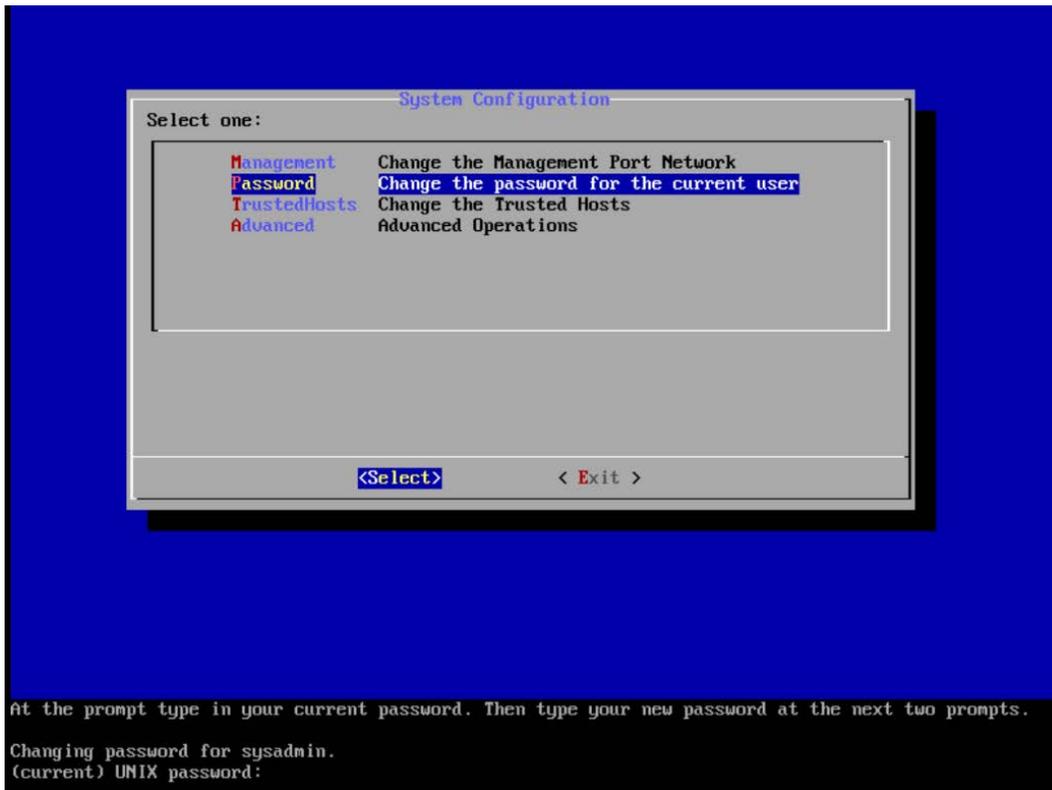
- 2151       **20.** Repeat steps 1-19 for each of the **Stealthwatch Management Console, Stealthwatch UDP**  
2152               **Director, Stealthwatch Flow Sensor, and Stealthwatch Flow Collector.**

2153    **2.13.2**    Change Default Stealthwatch Console Passwords

- 2154        1. In the **System Configuration** menu, highlight **Password** and **Select**.

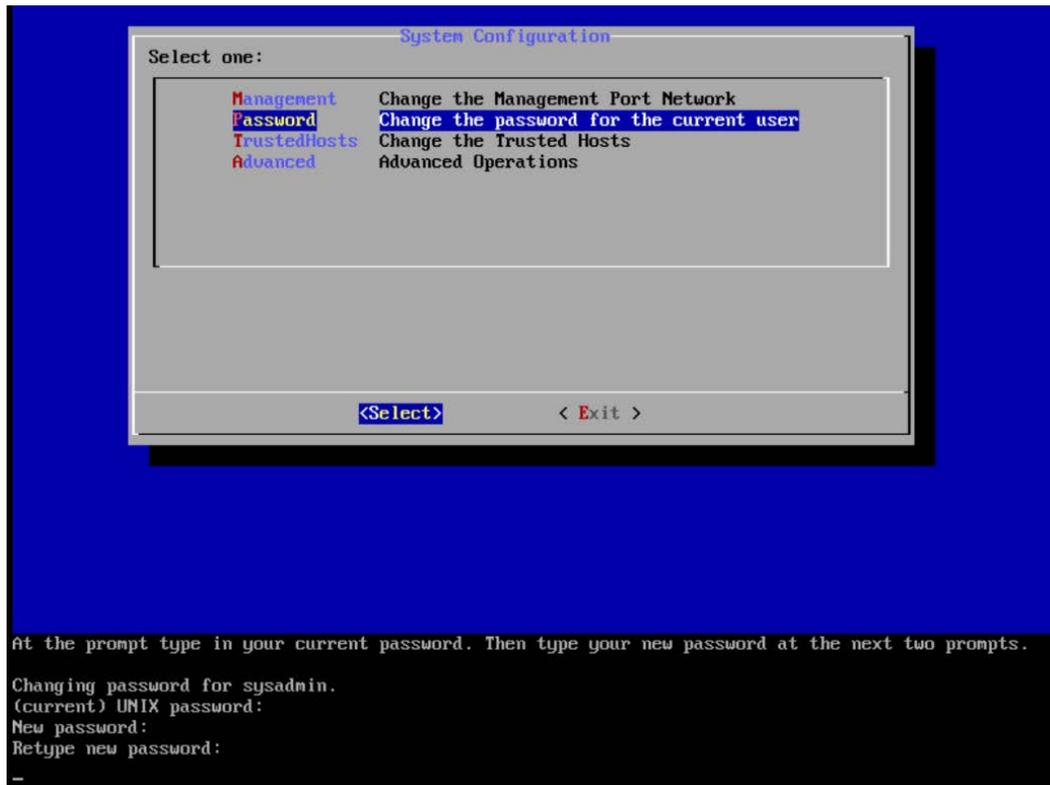


- 2155        2. Press **Enter**.  
2156        3. Enter the original password.  
2157

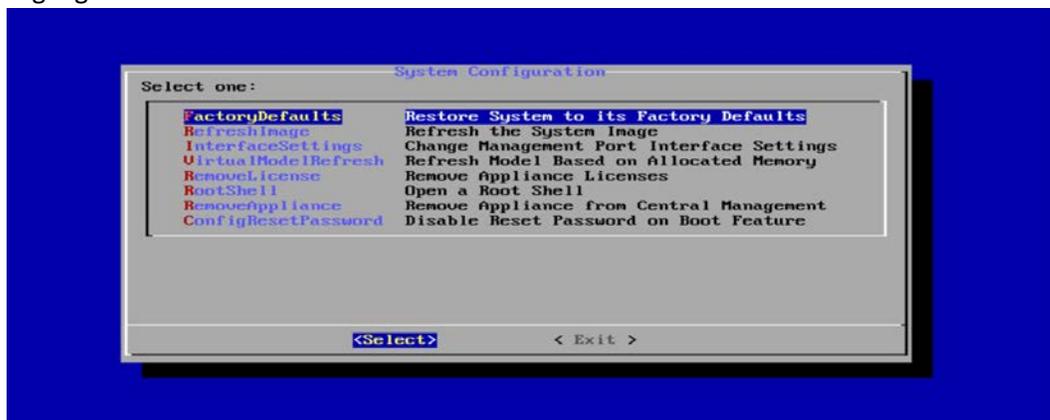


2158  
2159  
2160

4. Press **Enter**.
5. Enter the new password, and confirm it.



- 2161  
2162  
2163  
2164  
2165
6. Press **Enter**.
  7. In the **System Configuration** menu, highlight **Advanced** and **Select**.
  8. Press **Enter**.
  9. Highlight **RootShell** and **Select**.



- 2166  
2167  
2168
10. Press **Enter**.
  11. Log in using the original root shell password.

```
                Type the root password at the prompt to open a root shell.  
Password:  
snc-01:~#
```

2169  
2170  
2171

12. Enter the command `root`.
13. Type the new password, and confirm it.

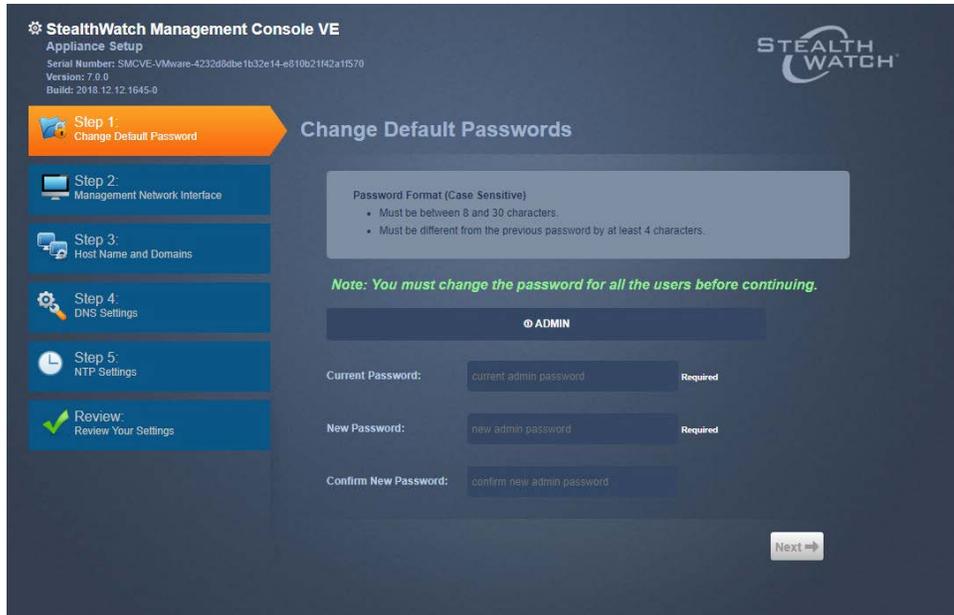
```
                Type the root password at the prompt to open a root shell.  
Password:  
snc-01:~# passud root  
New password:  
Retype new password:  
passud: password updated successfully  
snc-01:~#
```

2172  
2173

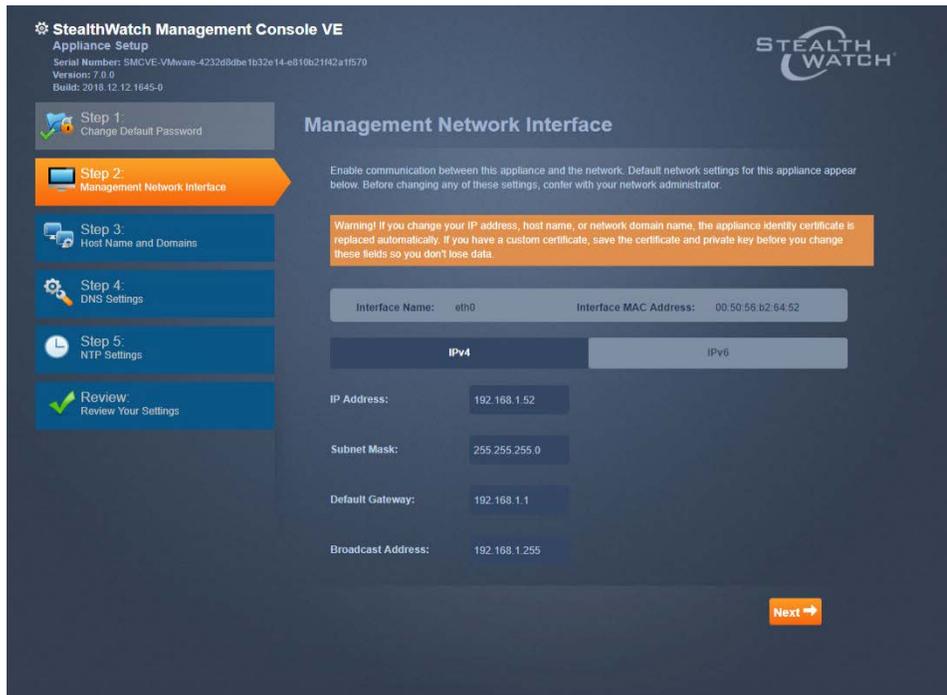
- 2174
- 2175 14. Press **Enter**.
- 2176 15. Repeat steps 1-14 for each console.

### 2177 2.13.3 Configure the Stealthwatch Management Console Web Interface

- 2178 1. Change the default password by filling in the fields for **Current Password**, **New Password**, and
- 2179 **Confirm New Password**.

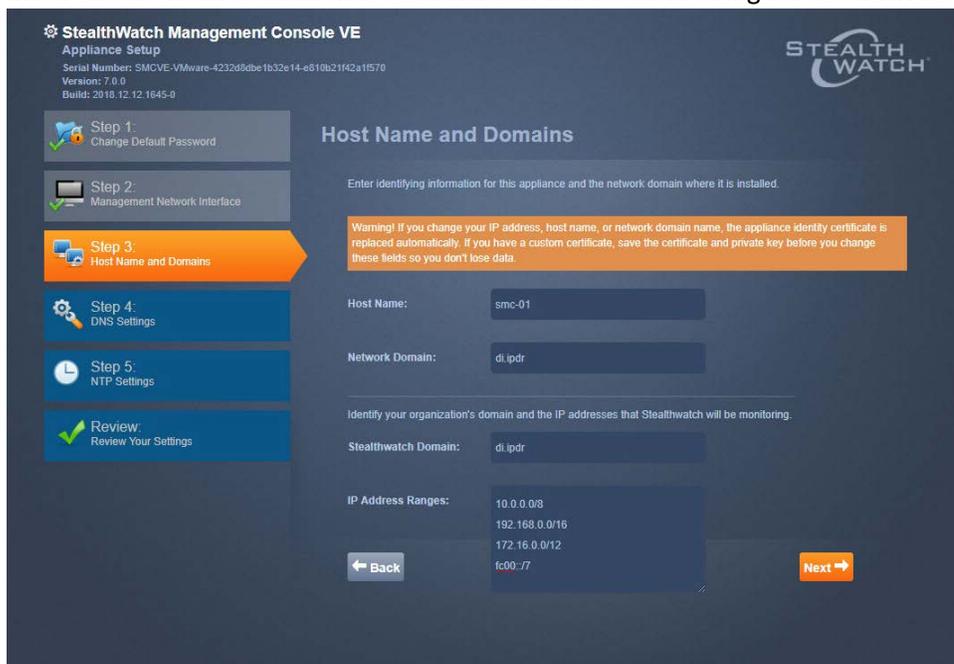


- 2180
- 2181 2. Click **Next**.
- 2182 3. Fill in the fields for **IP Address**, **Subnet Mask**, **Default Gateway** and **Broadcast Address**
- 2183 according to your network topology.



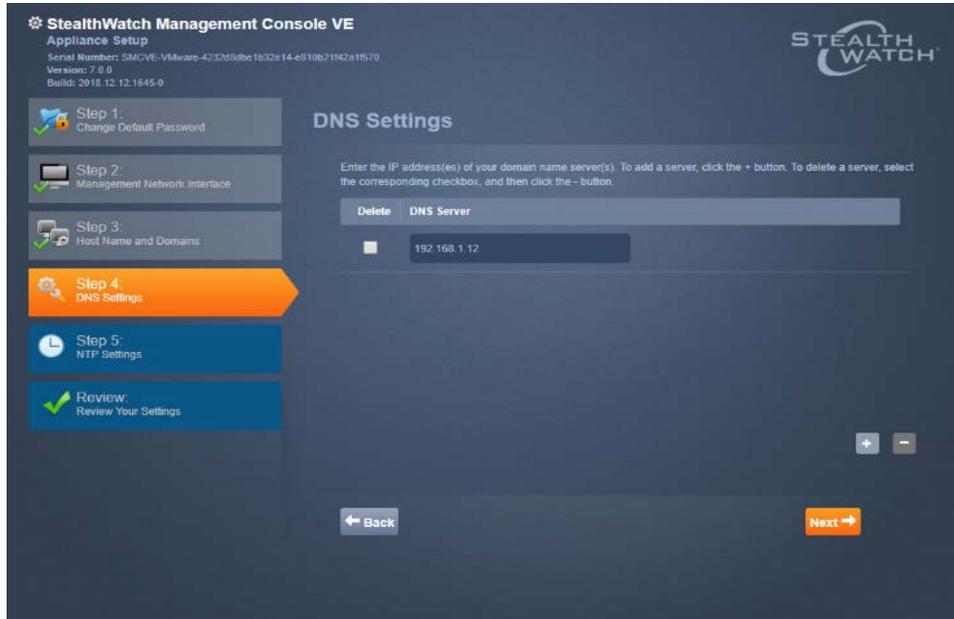
2184  
2185  
2186  
2187  
2188

4. Click **Next**.
5. Enter a **host name**.
6. Enter the network domain that Stealthwatch is in for **Network Domain**.
7. Enter the network domain that Stealthwatch will be monitoring for **Stealthwatch Domain**.

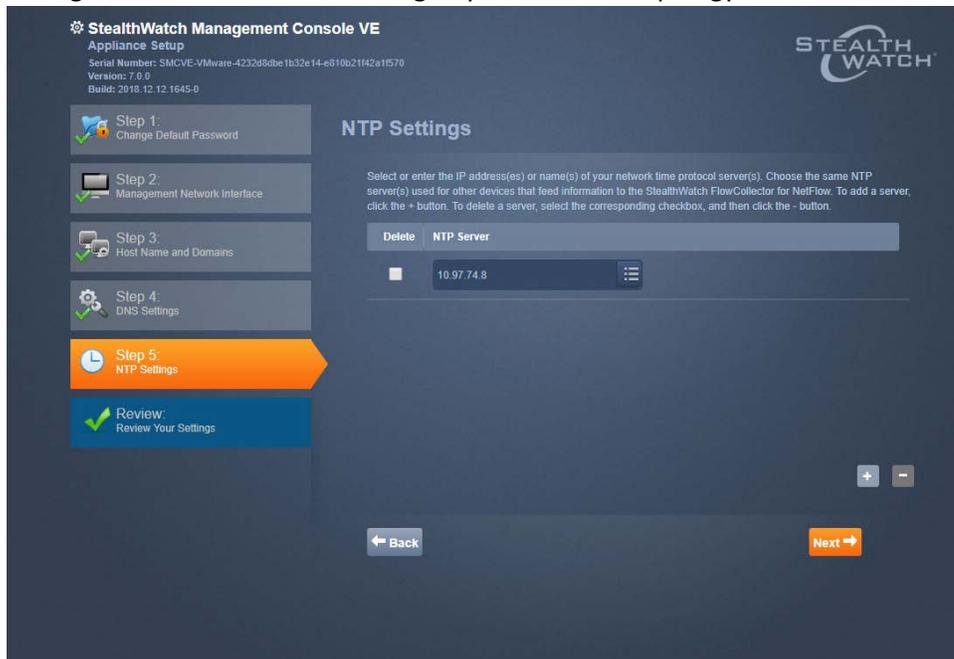


2189

- 2190 8. Click **Next**.
- 2191 9. Enter a **DNS Server**.



- 2192 10. Click **Next**.
- 2193 11. Configure the NTP server according to your network topology.
- 2194



- 2195 12. Click **Next**.
- 2196 13. Select **Restart**.
- 2197



2198  
2199

14. Click **Apply**.

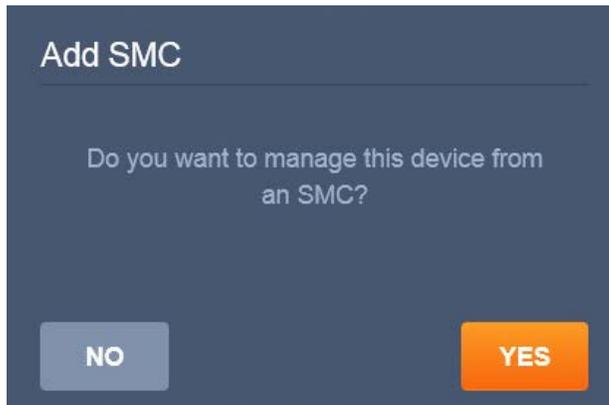


2200  
2201

15. After the restart, click **Next**.

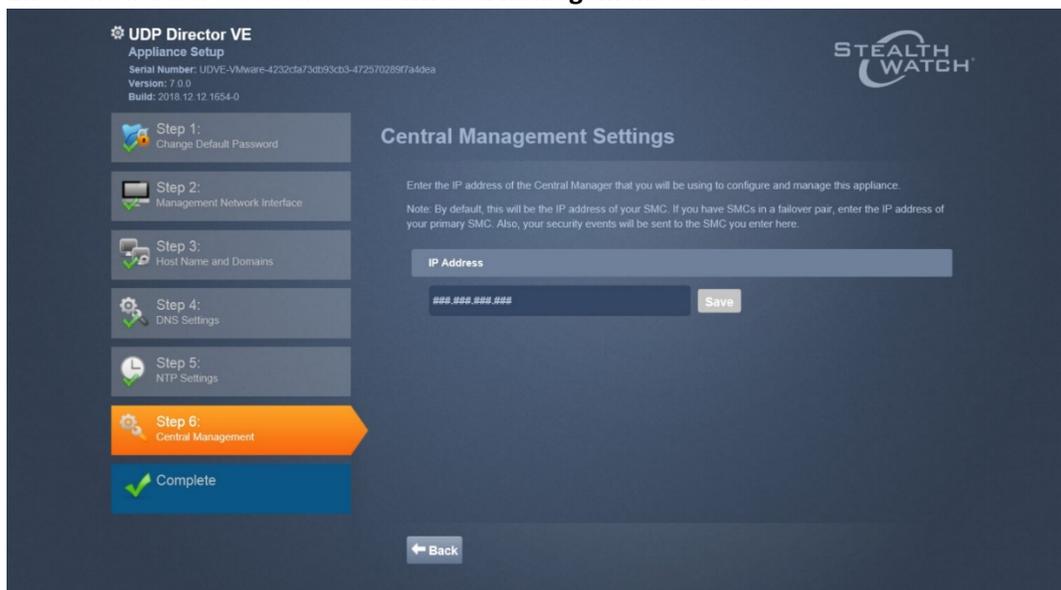
## 2.13.4 Configure the Stealthwatch UDP Director, Stealthwatch Flow Collector and Stealthwatch Flow Sensor Web Interfaces

1. Repeat steps 1-12 from *Configure the Stealthwatch Management Console Web Interface*.



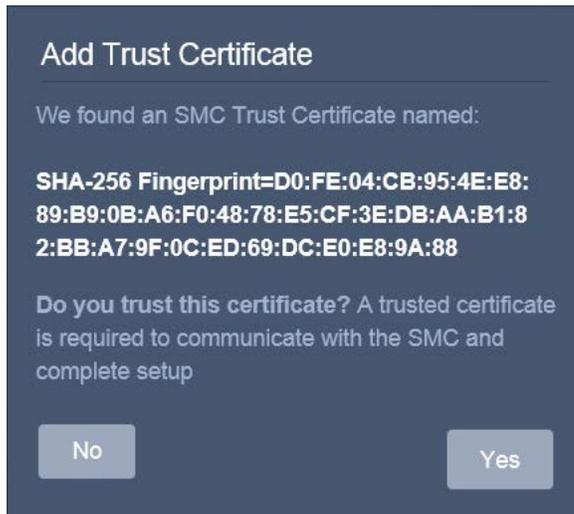
2205  
2206  
2207

2. When prompted to manage this device from an SMC, click **Yes**.
3. Enter the IP Address of the **Stealthwatch Management Console**.



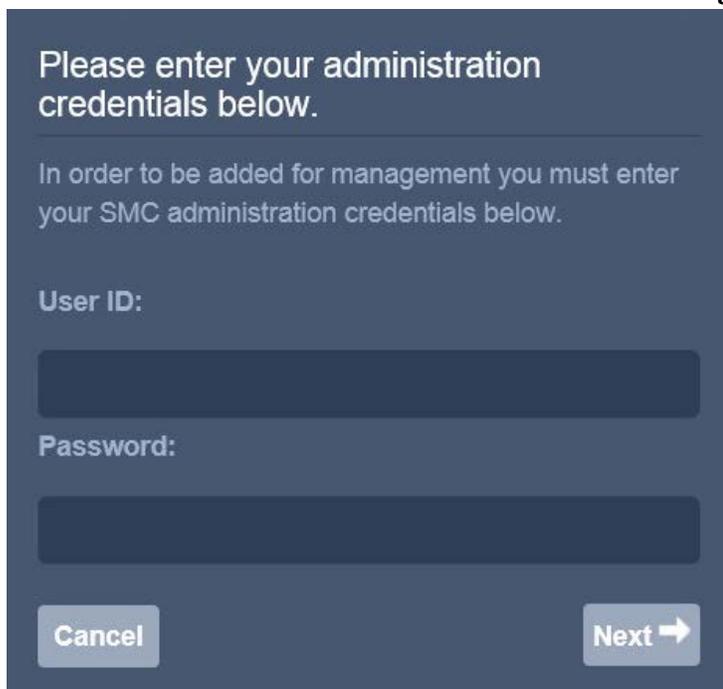
2208  
2209  
2210

4. Click **Save**.
5. Verify the certificate.



2211  
2212  
2213

6. Click **Yes**.
7. Enter the **User ID** and **Password** for the **Stealthwatch Management Console**.



2214  
2215  
2216  
2217  
2218

8. Click **Next**.
9. Repeat steps 1-8 for the Flow Collector *first* and *then* for the Flow Sensor. The Flow Sensor cannot be added to the Management Console until after the Flow Collector is successfully added.

## 2219 2.14 Symantec Analytics

2220 This section details the installation and configuration of Symantec Analytics, a network analysis tool.

2221 This guide assumes that Symantec Analytics is connected via serial to a terminal.

### 2222 2.14.1 Initial Setup

- 2223 1. Log in to the Symantec Analytics command line.
- 2224 2. Enter the following command to configure the IP for the interface:

2225 `sudo cfg_bond_interface.py -i eth0 -n 192.168.1.42/255.255.255.0 -g 192.168.1.1`

```

COM2 - PuTTY
ether 00:e0:ed:7a:82:1d txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xfbe00000-fbe1ffff

eth2: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 00:e0:ed:7a:82:1c txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xfbe20000-fbe3ffff

eth3: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 00:e0:ed:7a:82:1b txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xfbe40000-fbe5ffff

eth4: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 00:e0:ed:7a:82:1a txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xfbe60000-fbe7ffff

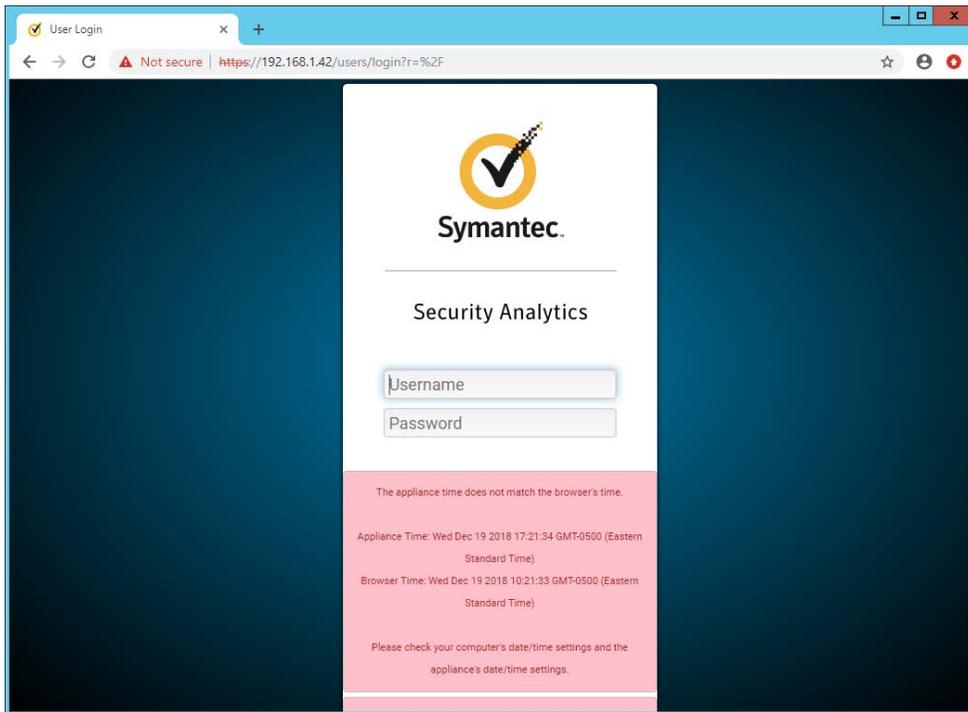
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1 (Local Loopback)
RX packets 1165 bytes 428654 (418.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1165 bytes 428654 (418.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@DS2B7A ~]# sudo cfg_bond_interface.py -i eth0 -n 192.168.1.42/255.255.255.0 -g 192.168.1.1

```

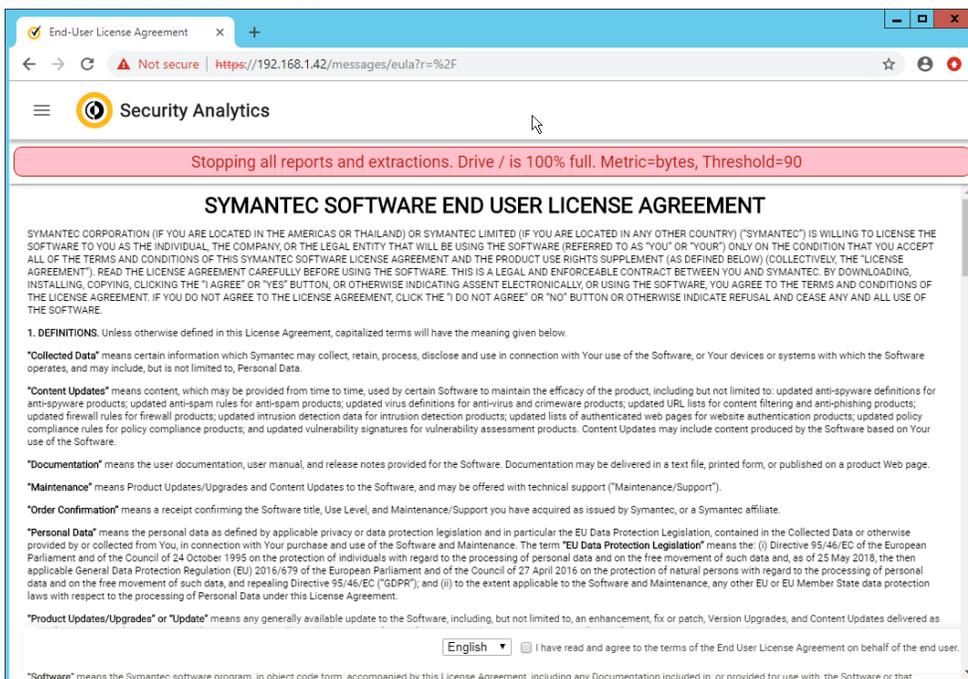
2226

- 2227 3. Navigate to the IP you assigned in a browser.



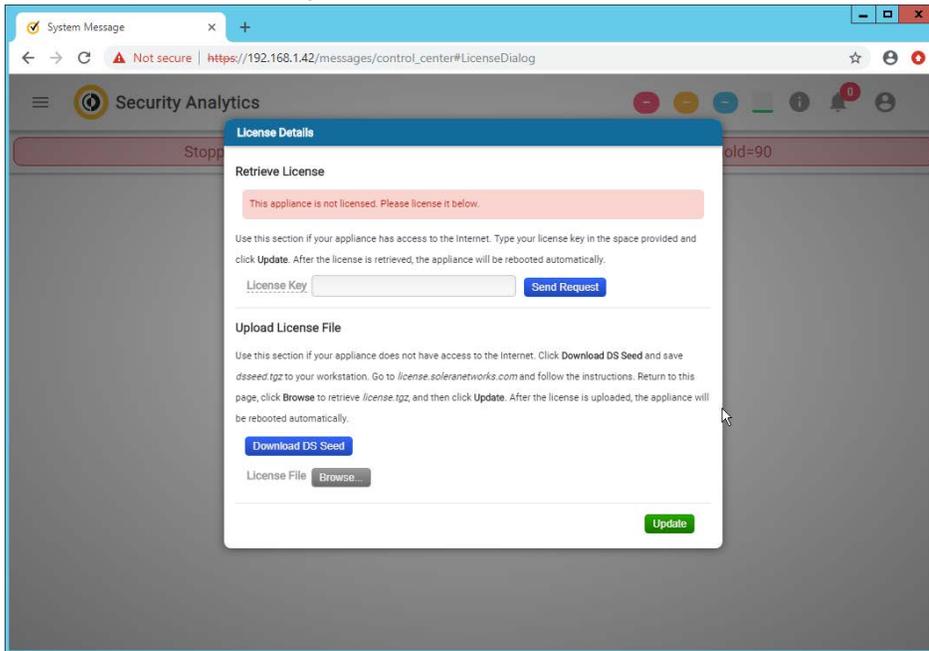
2228  
2229  
2230  
2231

4. Enter the username and password to log in. The default is **(Admin/Solera)**.
5. Check the box next to **I have read and agreed to the terms of the End User License Agreement on behalf of the end user.**



2232

- 2233 6. Click **Next**.
- 2234 7. Enter the license key.
- 2235 8. If you do not have internet connectivity, follow the instructions under **Upload License File**.
- 2236 Otherwise, click **Send Request**.

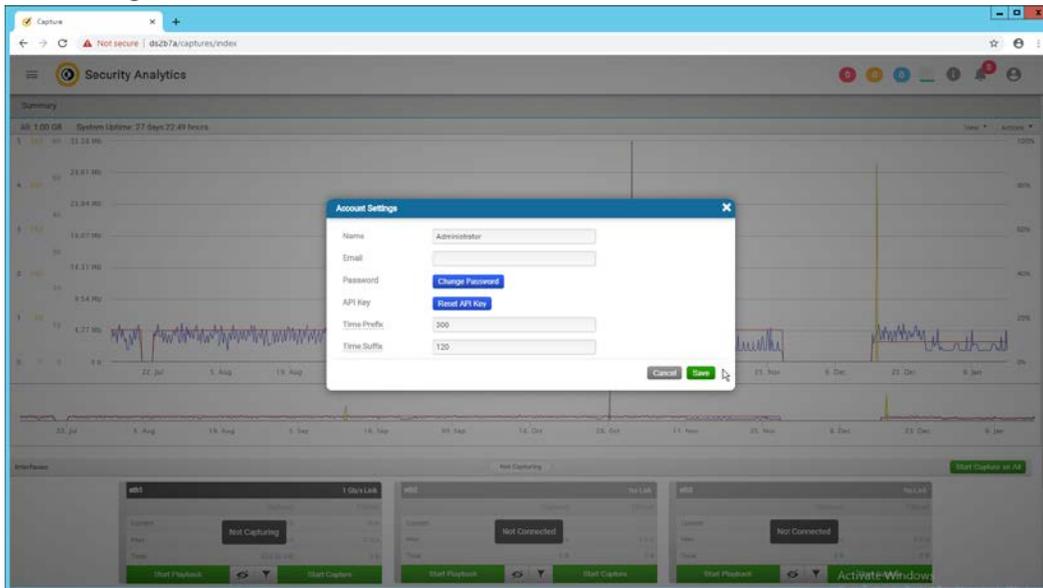


- 2237 9. Click **Update**. The device will reboot.
- 2238 10. Log in to the web page again.
- 2239 11. Click the silhouette in the top right corner and click **Account Settings**.
- 2240

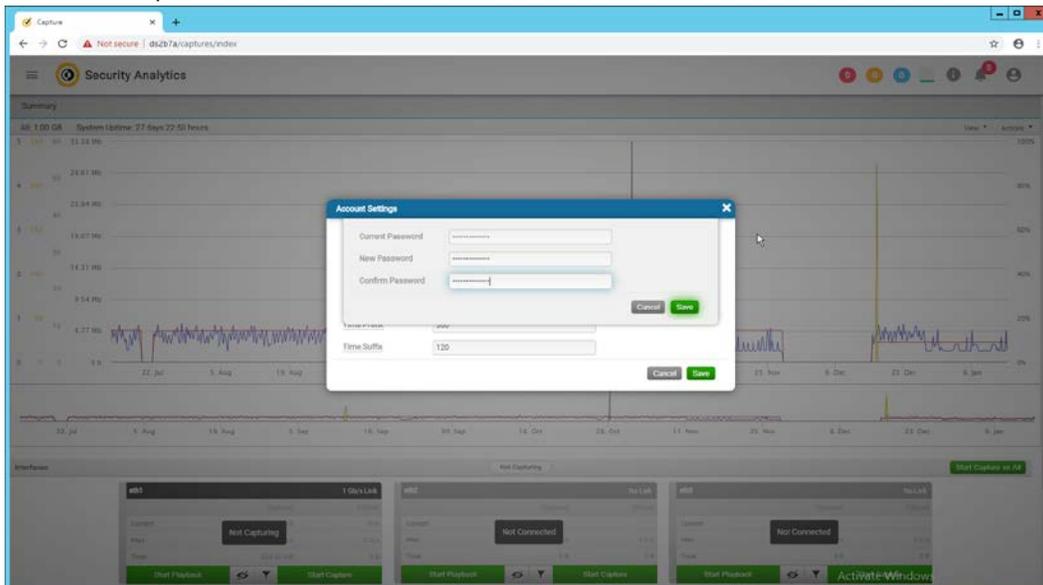


2241

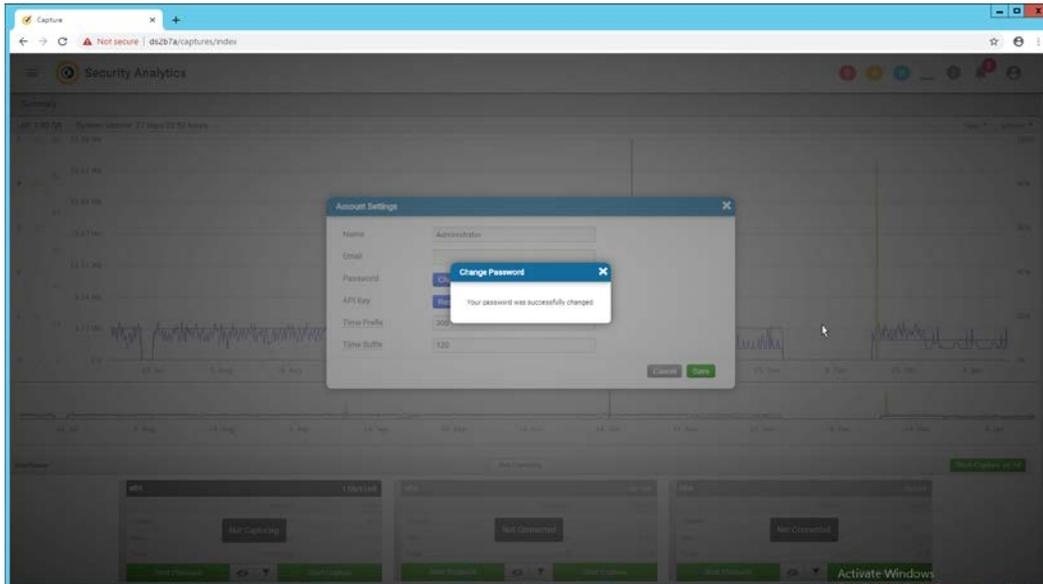
2242 12. Click **Change Password**.



2243 2244 13. Enter a new password. Click **Save**.

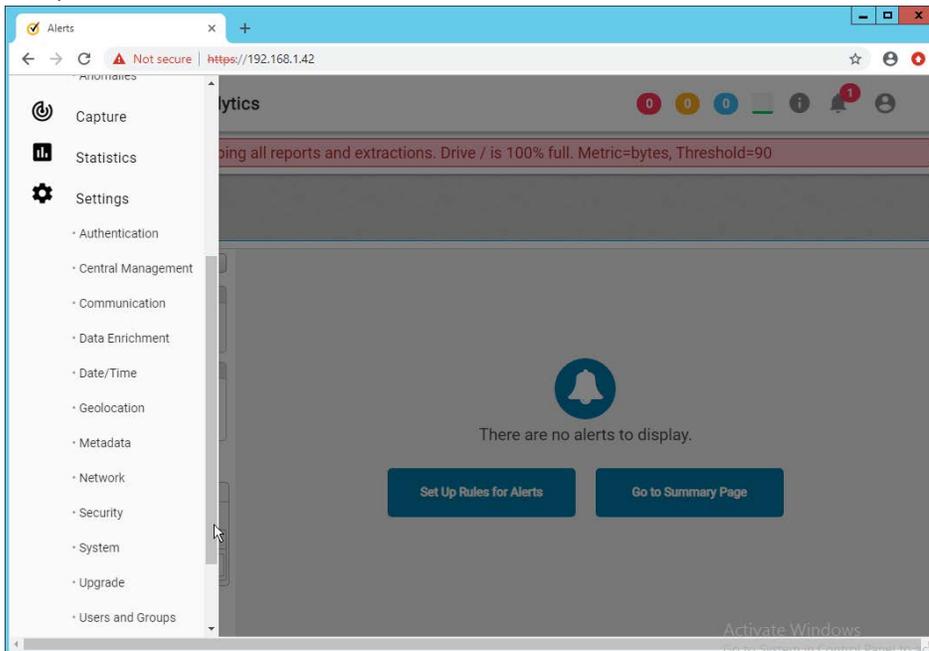


2245 2246 2247 14. The screen should reflect that the password has been changed. Close out of both windows and return to the main web console.



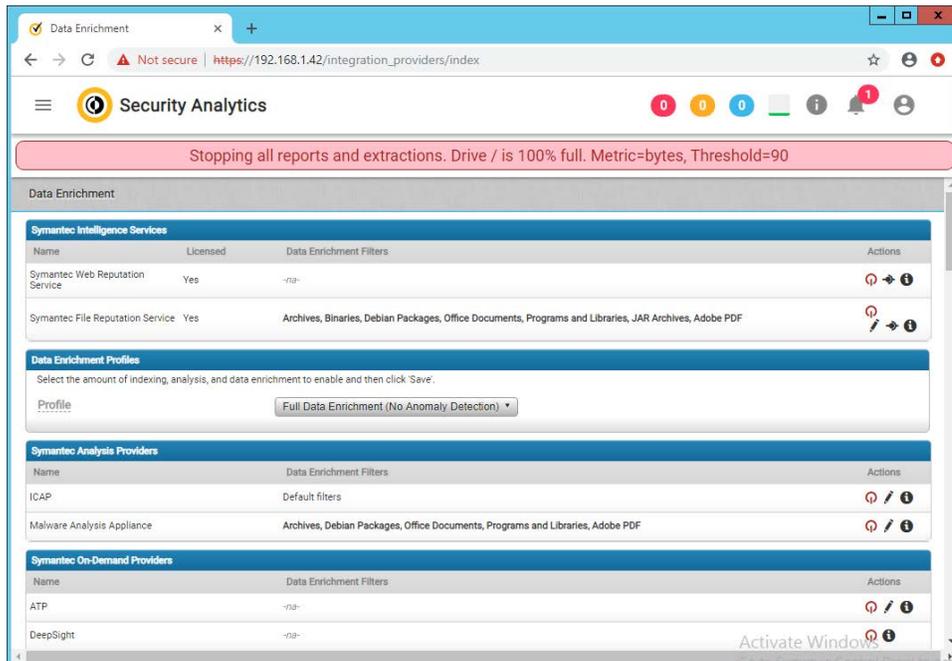
2248  
2249  
2250

15. In the top left corner of the web console, click the menu button. (It shows as three horizontal bars).



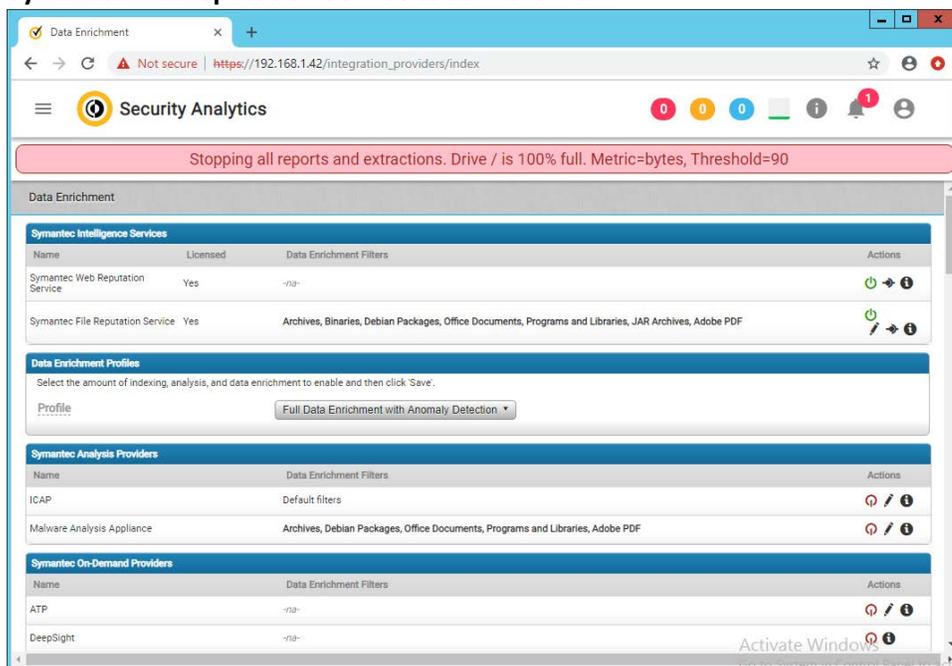
2251  
2252

16. Navigate to **Settings > Data Enrichment**.



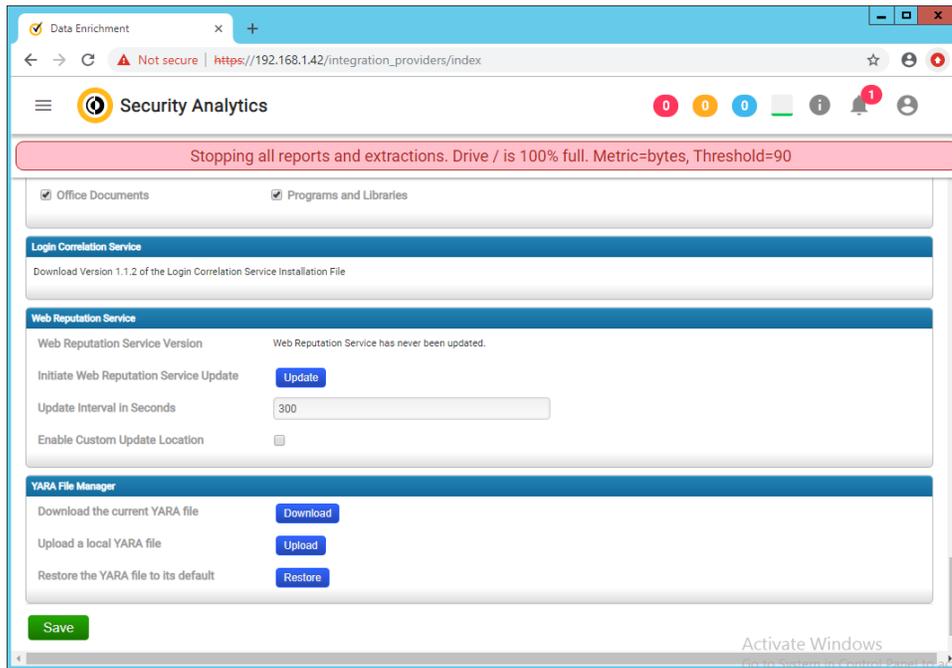
2253  
2254  
2255

17. Click the red upside-down power symbols next to **Symantec Web Reputation Service** and **Symantec File Reputation Service** to turn them on.



2256  
2257  
2258

18. Select **Full Data Enrichment (with Anomaly Protection)** for the profile under **Data Enrichment Profiles**.

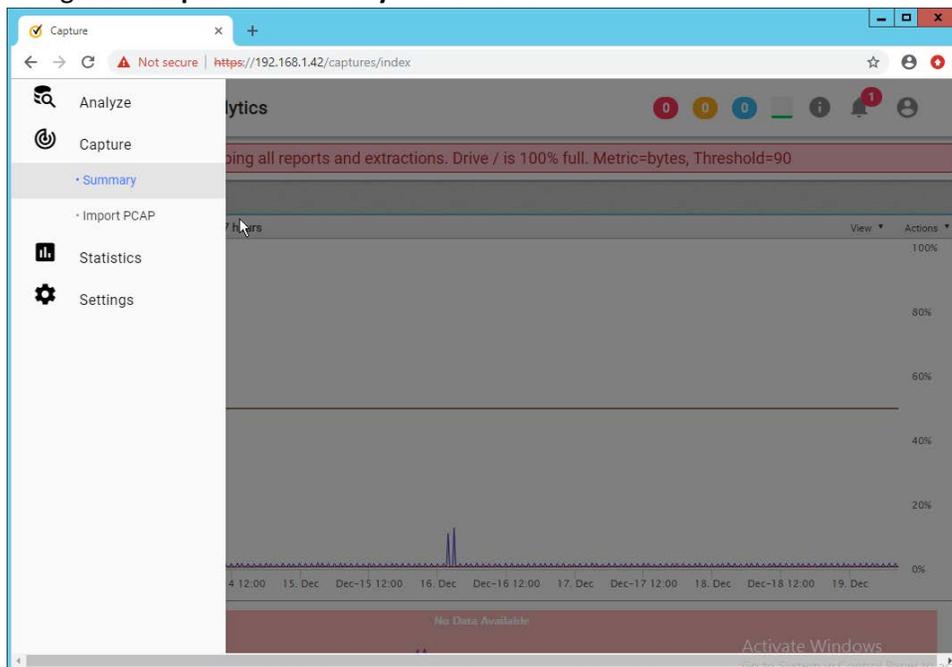


2259  
2260

19. Click **Save**.

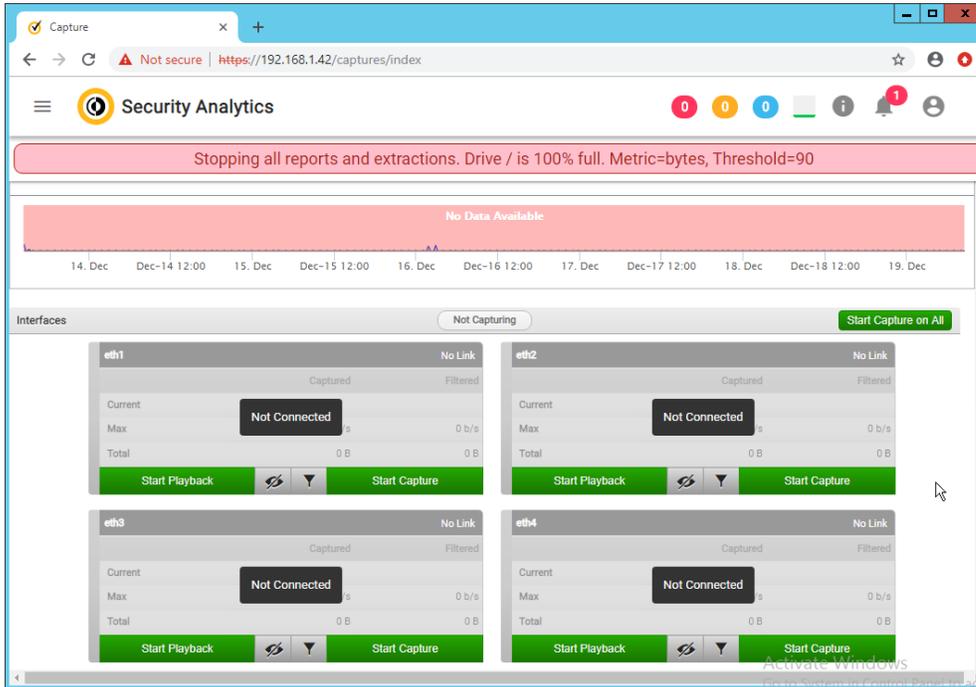
## 2261 2.14.2 Capturing Data

2262 1. Navigate to **Capture > Summary** in the menu.



2263

- 2264 2. Begin capturing data on any desired interfaces by clicking **Start Capture**.



2265

## 2266 2.15 Symantec Information Centric Analytics

2267 This section describes the installation and configuration of Symantec Information Centric Analytics  
2268 (ICA).

### 2269 2.15.1 Installing MS SQL 2017

- 2270 1. Launch the SQL Setup Wizard.



2271  
2272

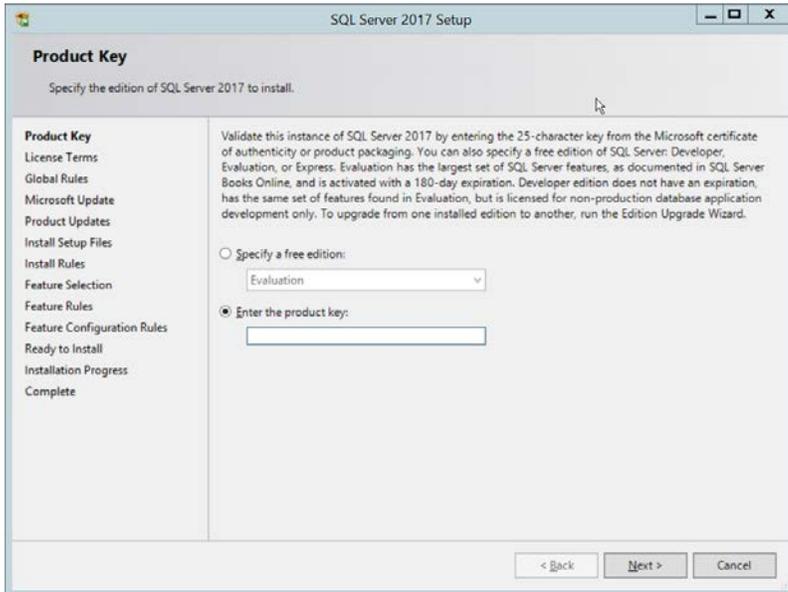
2. Click **Installation**.



2273  
2274  
2275

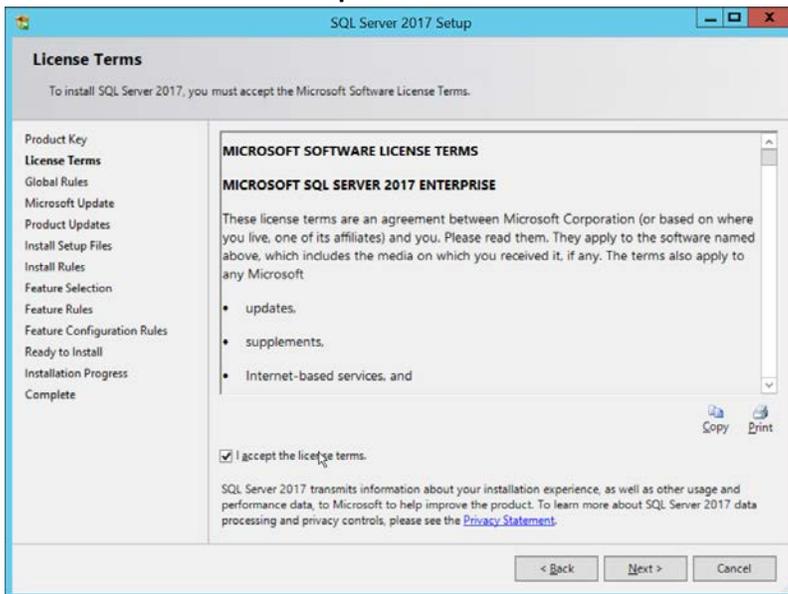
3. Click **New SQL Server stand-alone installation or add features to an existing installation**.

4. Enter a **product key**.



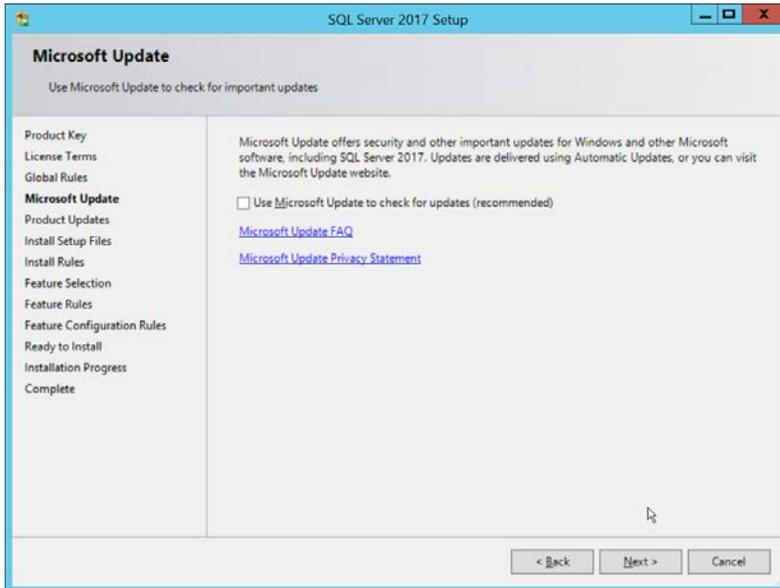
2276  
2277  
2278

5. Click **Next**.
6. Check the box next to **I accept the license terms**.



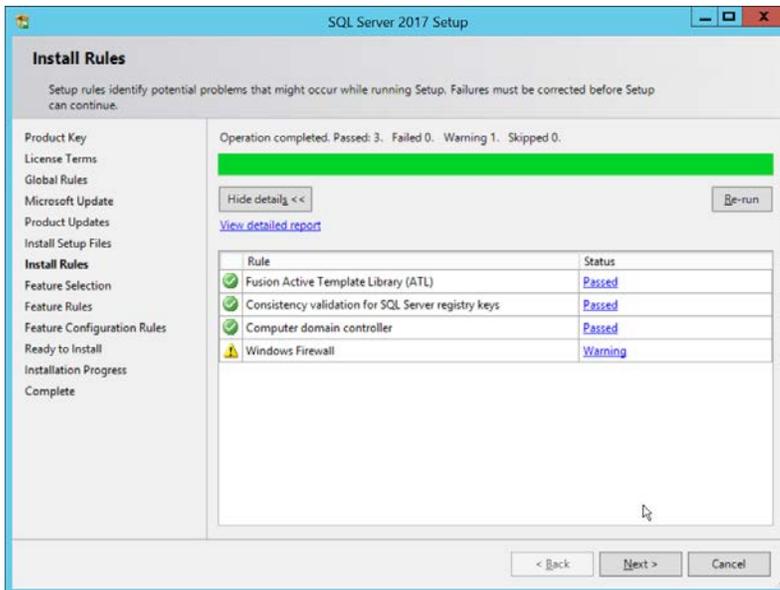
2279  
2280

7. Click **Next**.



2281  
2282

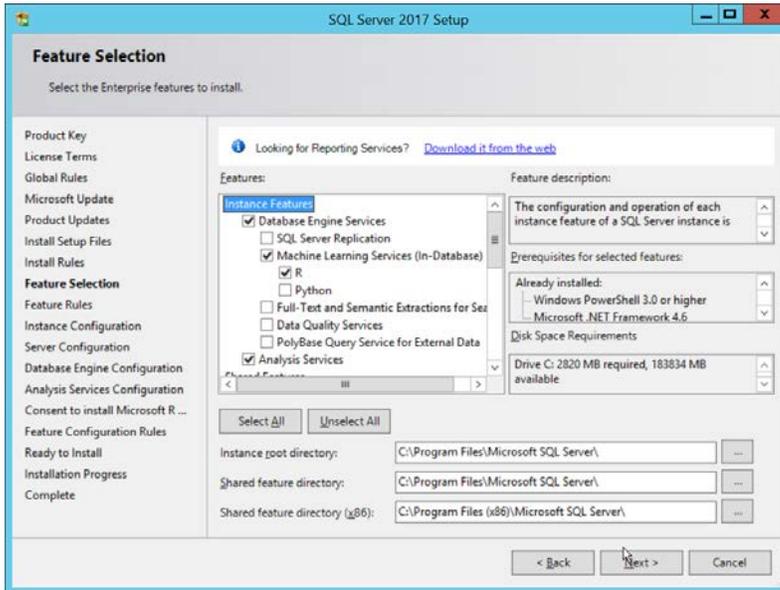
8. Click **Next**.



2283  
2284  
2285

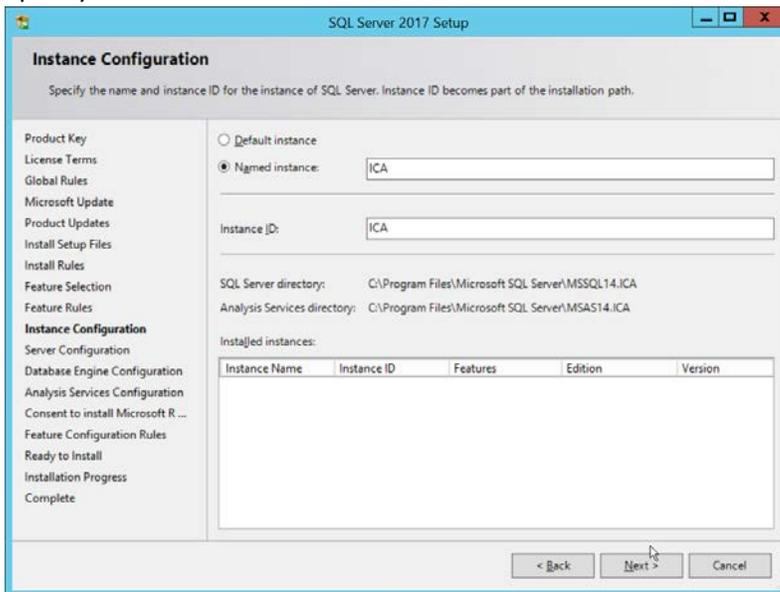
9. Click **Next**.

10. Ensure that box next to **R** and the box next to **Analysis Services** is checked.



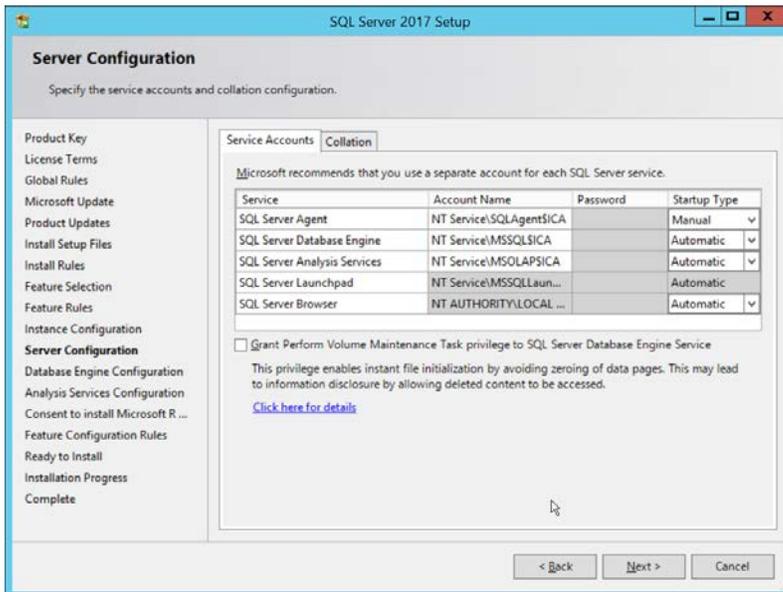
2286  
2287  
2288  
2289

11. Click **Next**.
12. Select **Named instance**.
13. Specify a name for the instance.



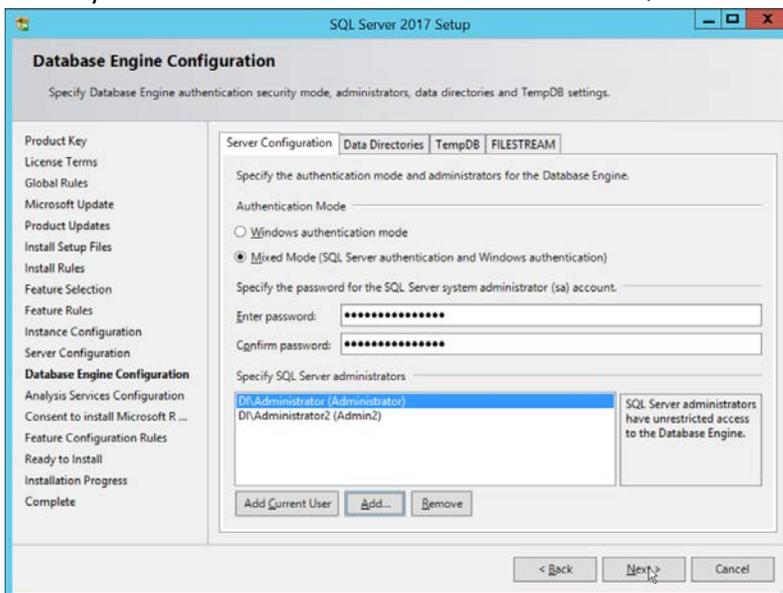
2290  
2291

14. Click **Next**.



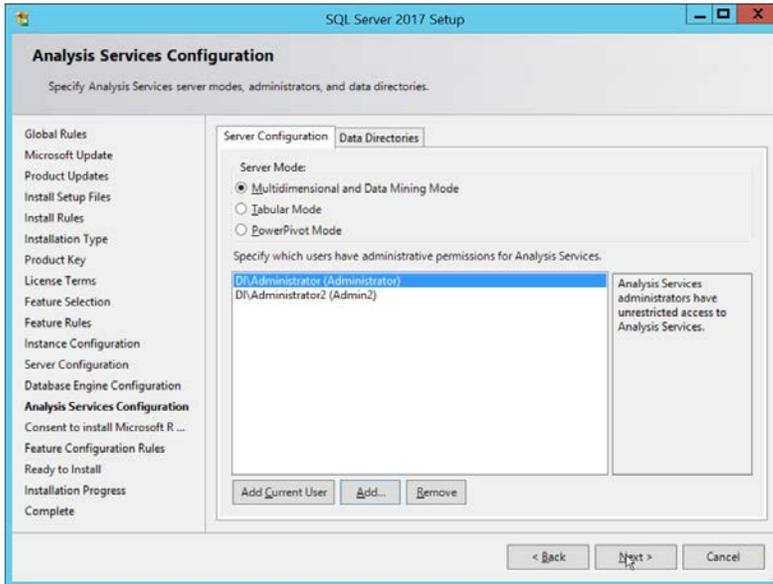
2292  
2293  
2294  
2295  
2296

15. Click **Next**.
16. Select **Mixed Mode (SQL Server authentication and Windows authentication)**.
17. Enter a **password**.
18. Add any users who should be administrators of the SQL database.



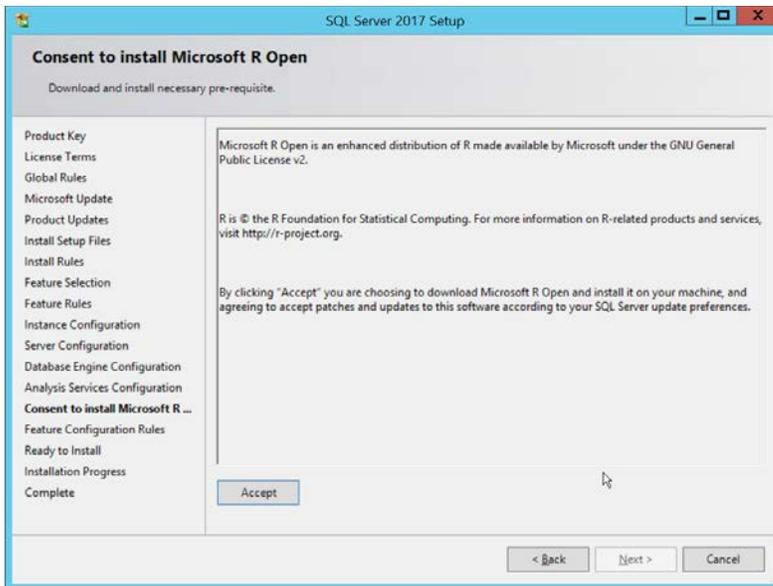
2297  
2298  
2299  
2300

19. Click **Next**.
20. Select **Multidimensional and Data Mining Mode**.
21. Add any users who should be administrators of the Analysis Services.



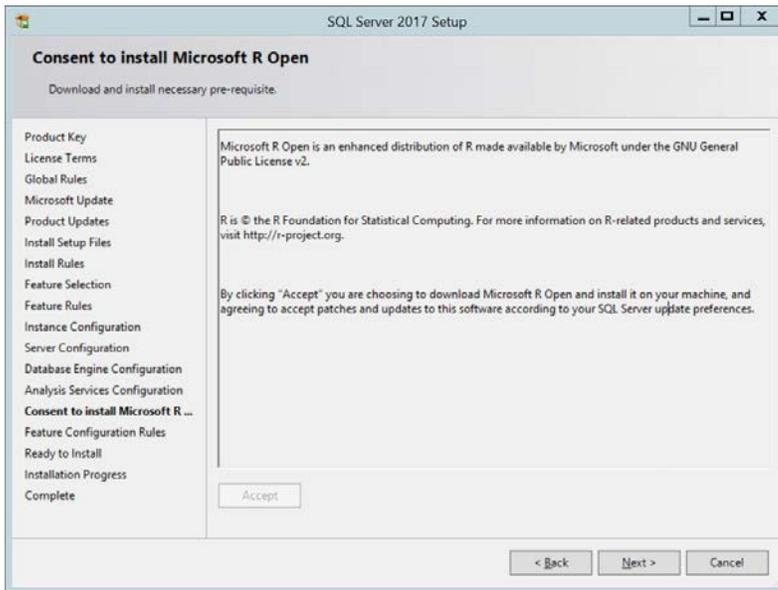
2301  
2302

22. Click **Next**.



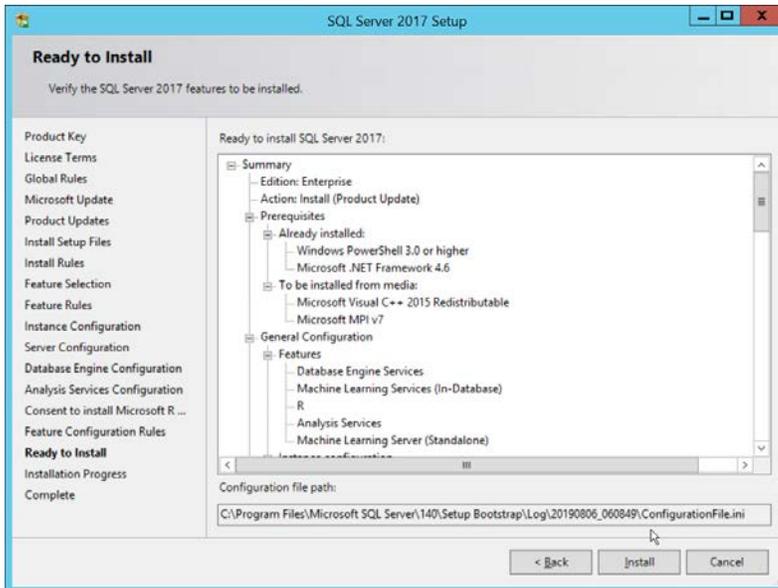
2303  
2304

23. Click **Accept**.



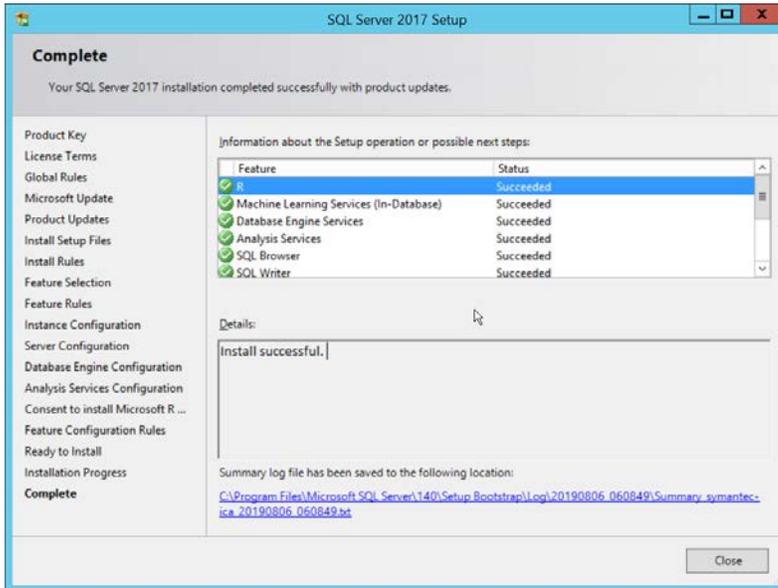
2305  
2306

24. Click **Next**.



2307  
2308

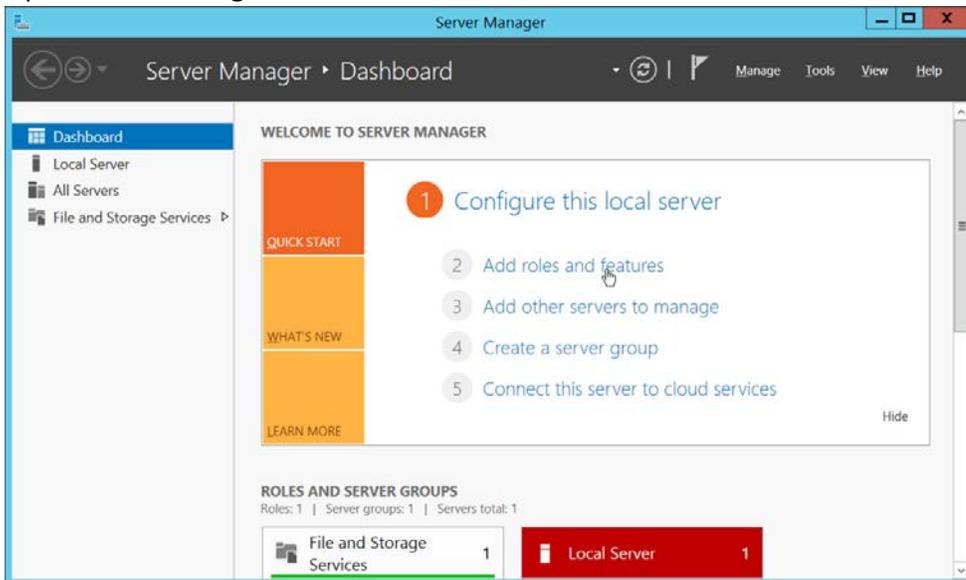
25. Click **Install**.



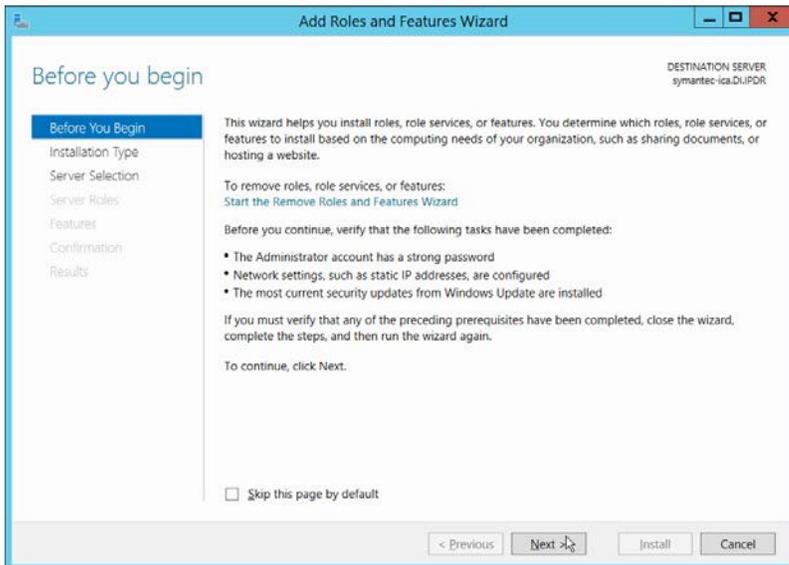
2309  
2310 26. Click **Close**.

## 2311 2.15.2 Install Windows Services

2312 1. Open **Server Manager**.

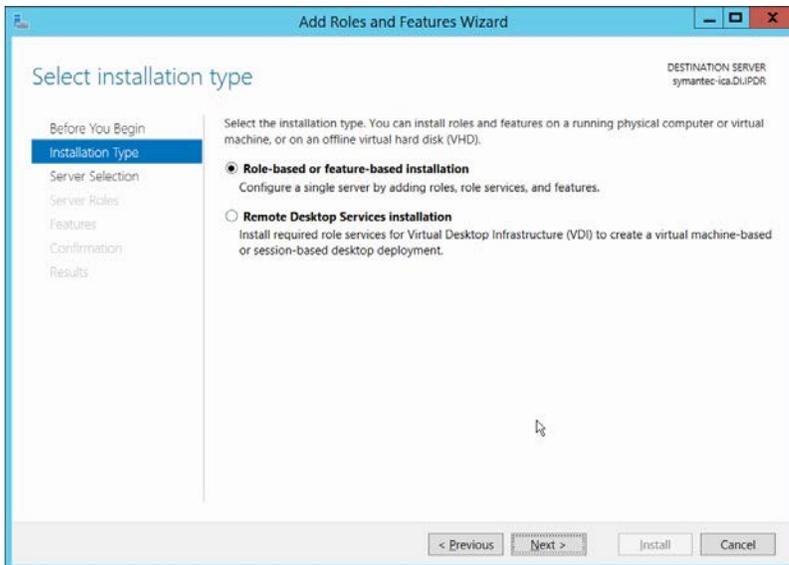


2313  
2314 2. Click **Add Roles and Features**.



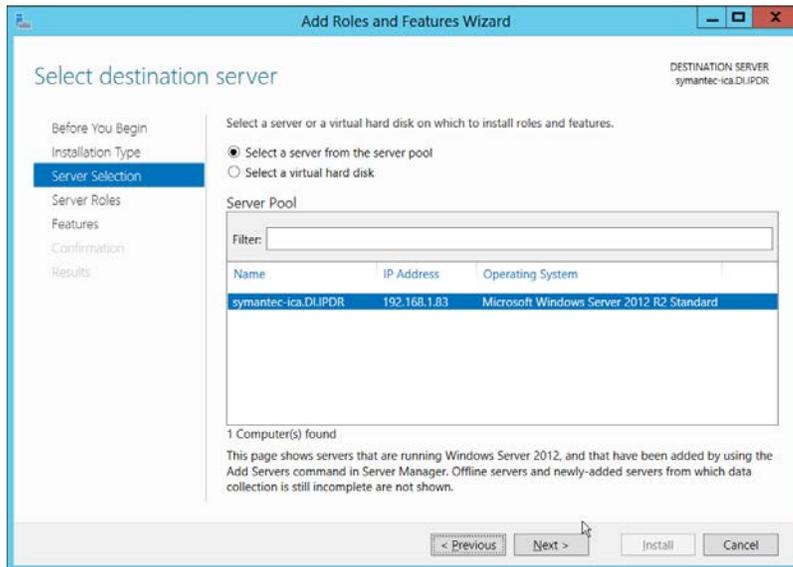
2315  
2316

3. Click **Next**.



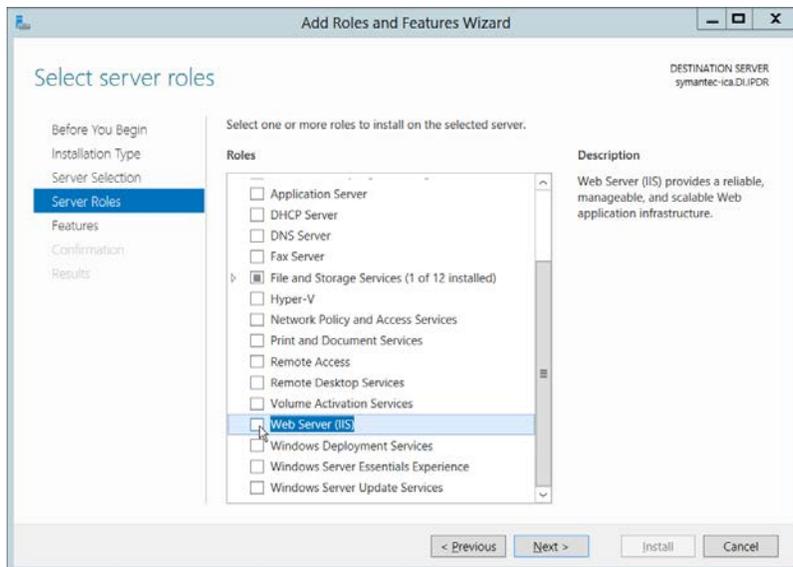
2317  
2318

4. Click **Next**.



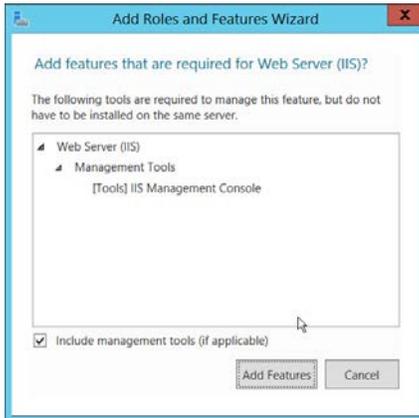
2319  
2320

5. Click **Next**.



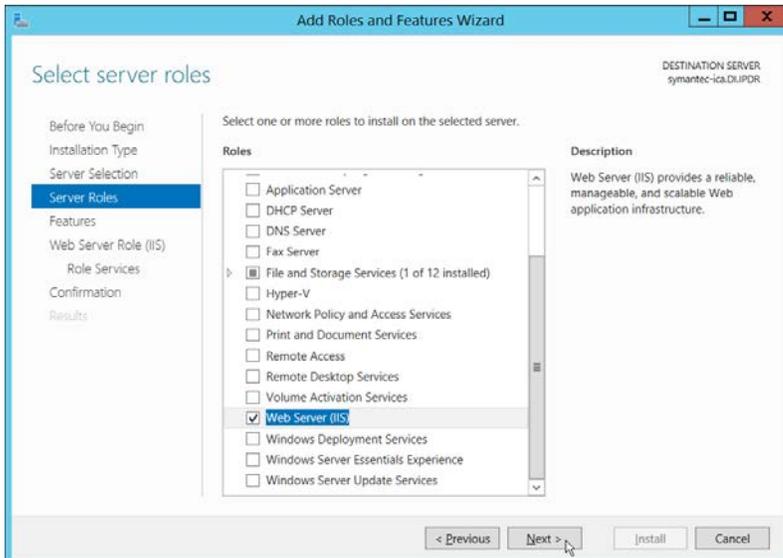
2321  
2322

6. Select **Web Server (IIS)**.



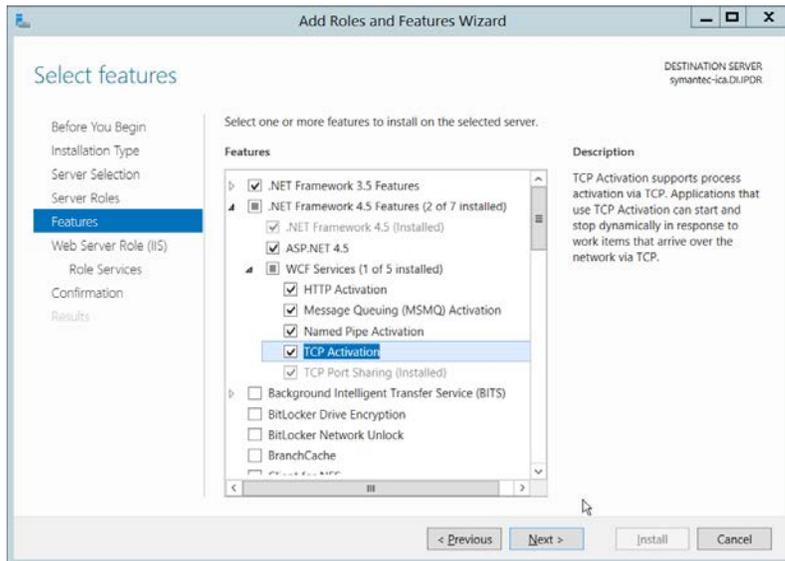
2323  
2324

7. Click **Add Features**.



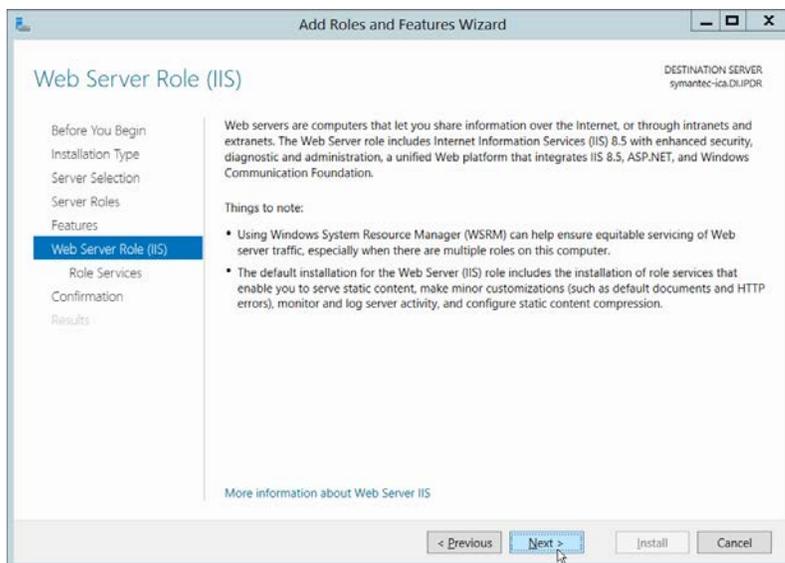
2325  
2326  
2327  
2328

- 8. Click **Next**.
- 9. Select all services under **.NET Framework 3.5 Features**.
- 10. Select all services under **.NET Framework 4.5 Features**.



2329  
2330

11. Click **Next**.



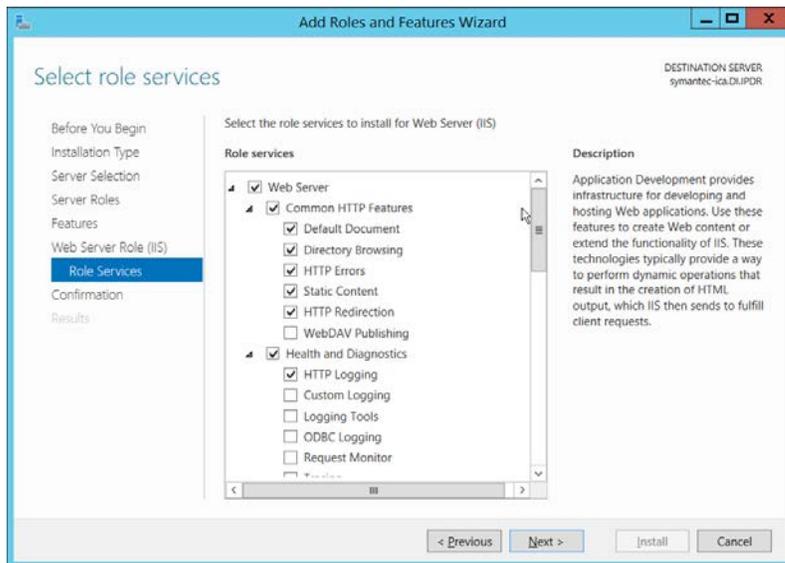
2331  
2332  
2333  
2334  
2335  
2336  
2337  
2338  
2339  
2340

12. Click **Next**.

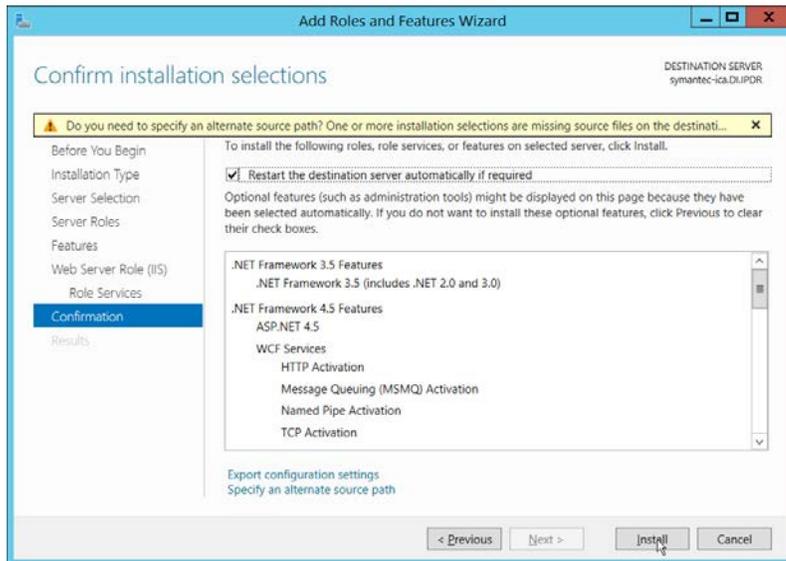
13. Ensure that the following **Role Services** are selected:

- a. **Common HTTP Features**
  - i. **Default Document**
  - ii. **Directory Browsing**
  - iii. **HTTP Redirection**
- b. **Health and Diagnostics**
  - i. **HTTP Logging**
- c. **Performance**

- 2341 i. Static Content Compression
- 2342 d. Security
- 2343 i. Windows Authentication
- 2344 e. Application Development
- 2345 i. .NET Extensibility 4.5
- 2346 ii. ASP.NET 4.5
- 2347 iii. ISAPI Extensions
- 2348 iv. ISAPI Filters

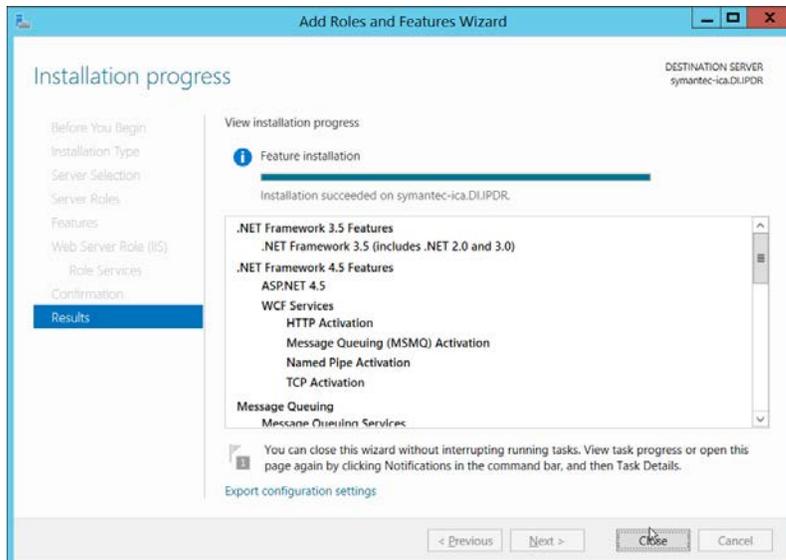


- 2349 14. Click **Next**.
- 2350 15. If necessary, specify a path to **/Sources/SxS**, which is found in the Windows Installation Media.
- 2351 16. Check the box next to **Restart the destination server automatically if required**.
- 2352



2353  
2354

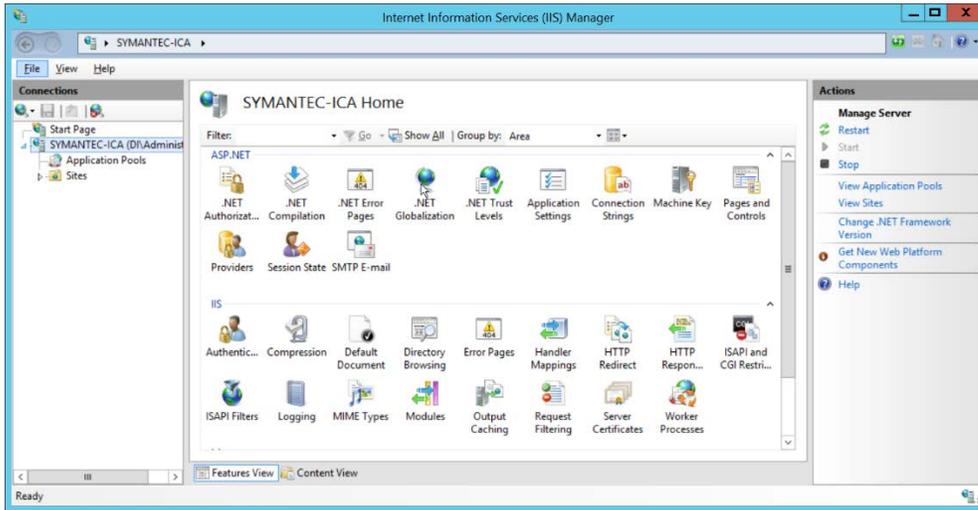
17. Click **Install**.



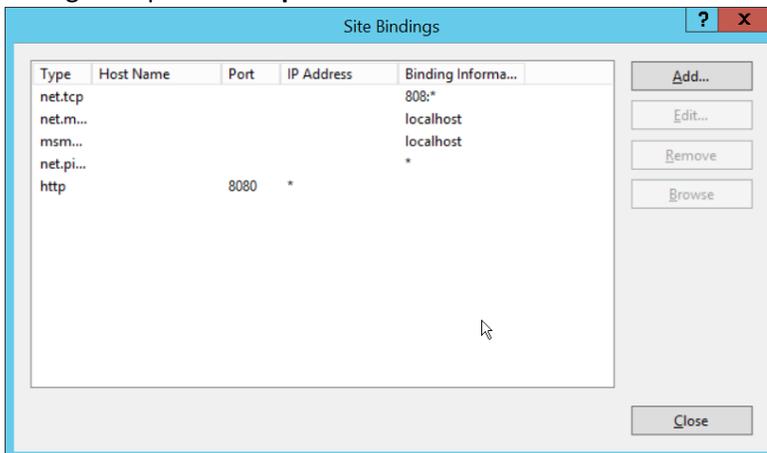
2355  
2356  
2357

18. Click **Close** when the installation finishes.

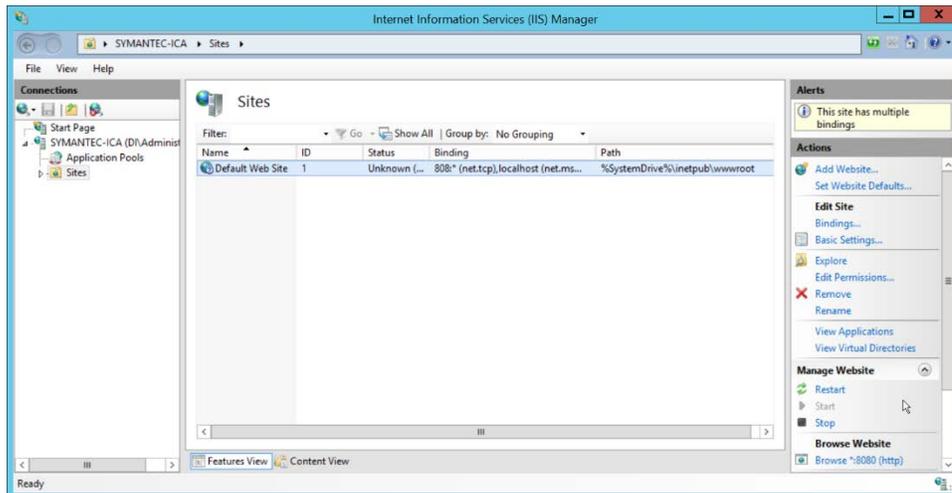
19. Open **Internet Information Services Manager**.



- 2358
  - 2359
  - 2360
  - 2361
20. Navigate to **SERVER-NAME > Sites**.
  21. Right-click the **Default Web Site**, and select **Bindings**.
  22. Change the port for **http** to **8080**.



- 2362
  - 2363
23. Click **Close**.

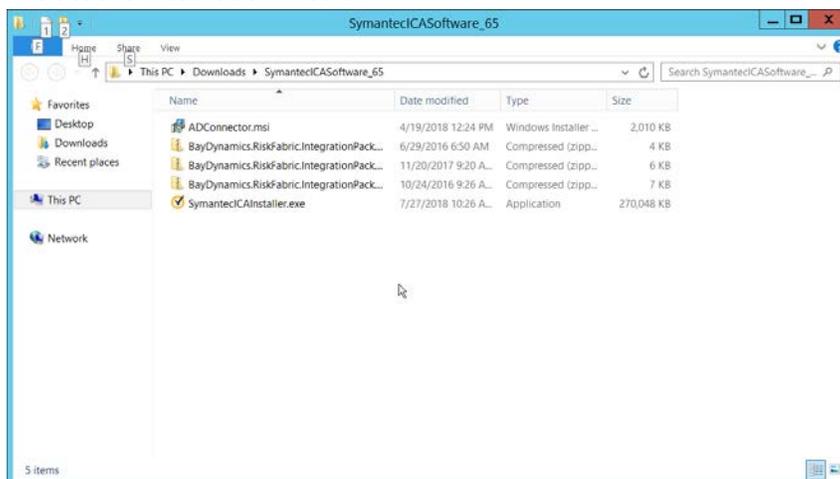


2364  
2365

24. Click **Restart** under **Manage Website**.

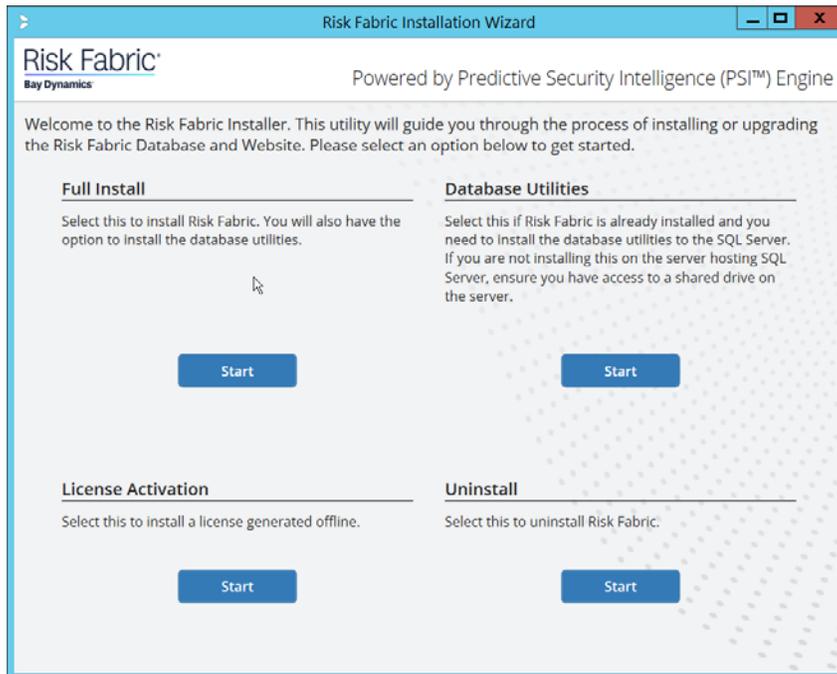
### 2366 2.15.3 Installing Symantec ICA

- 2367 1. In Task Manager, verify that the **SQL Server Agent** service is running.
- 2368 2. Copy the installation media **SymantecICASoftware\_65.zip** onto the server.
- 2369 3. Extract the installation media.



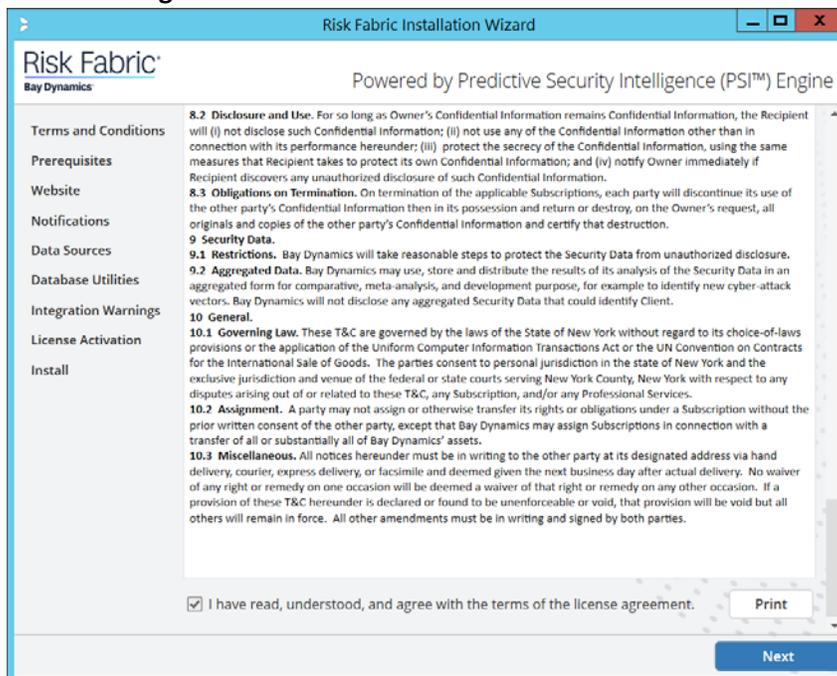
2370  
2371

4. Run **SymantecCAInstaller.exe**.



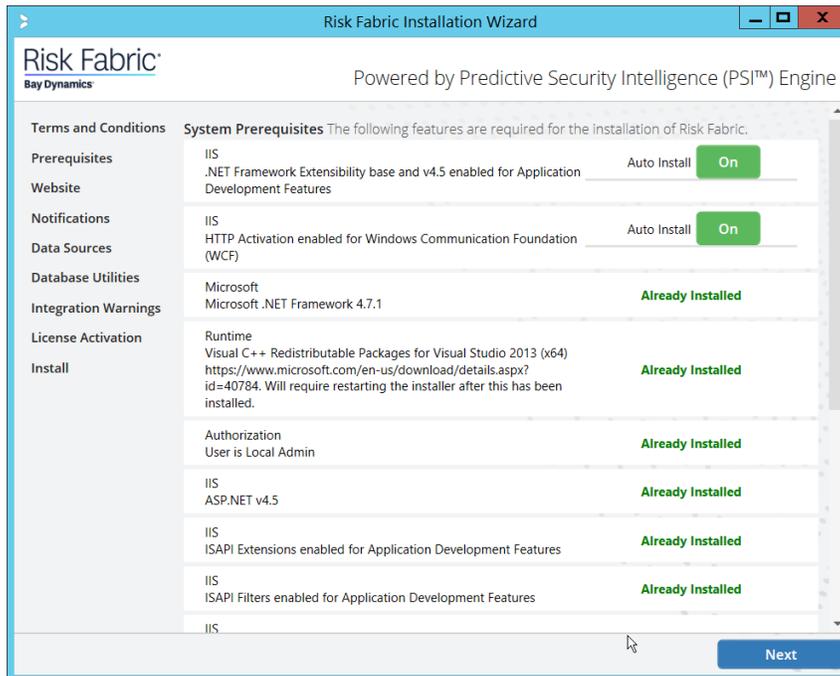
2372  
2373  
2374  
2375

5. Under **Full Install**, click **Start**.
6. Scroll down and check the box next to **I have read, understood, and agree with the terms of the license agreement**.



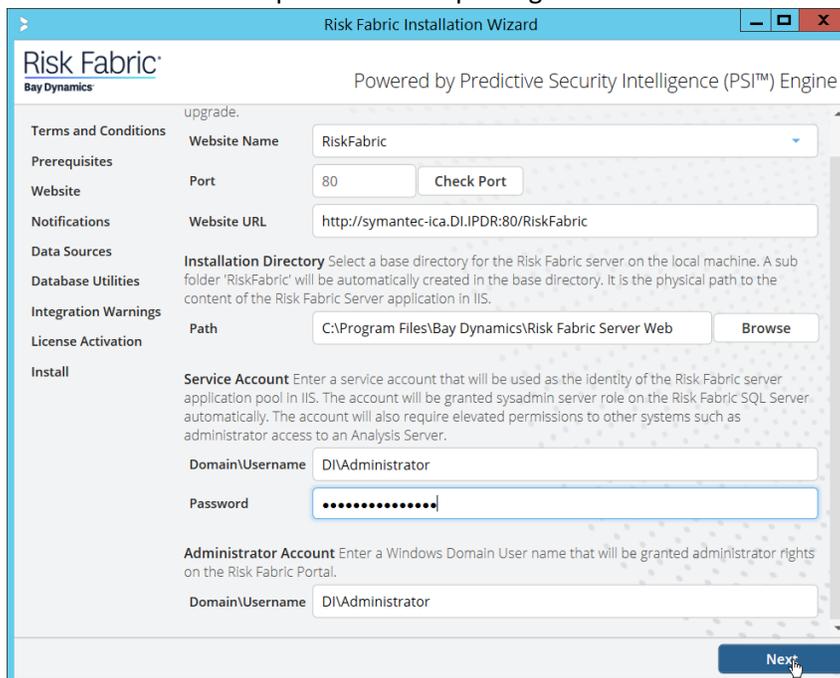
2376  
2377

7. Click **Next**.



2378  
2379  
2380

8. Click **Next**.
9. Enter a username and password with privileges on the domain.

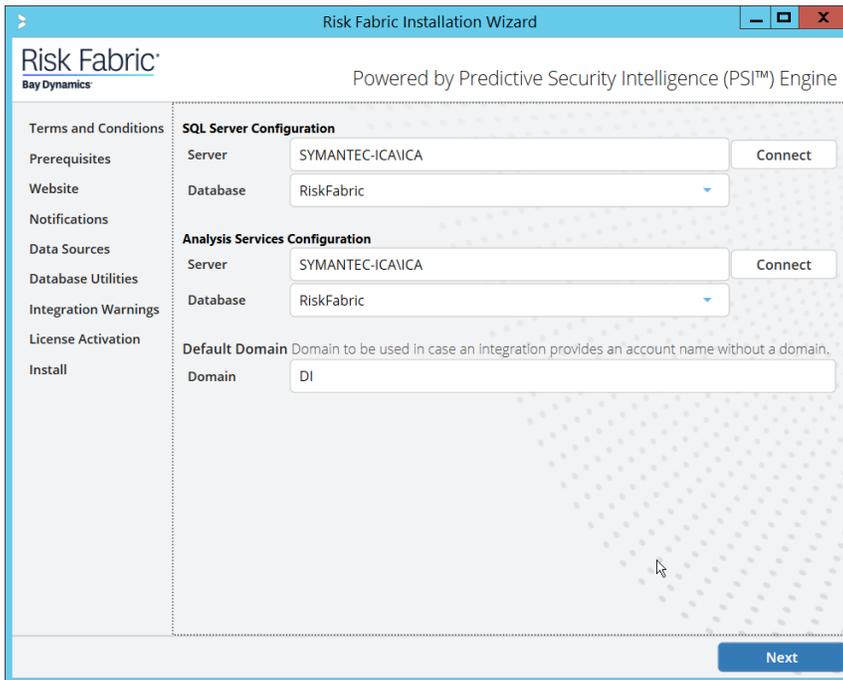


2381  
2382  
2383

10. Click **Next**.
11. Configure any alert settings desired; these can be changed later.

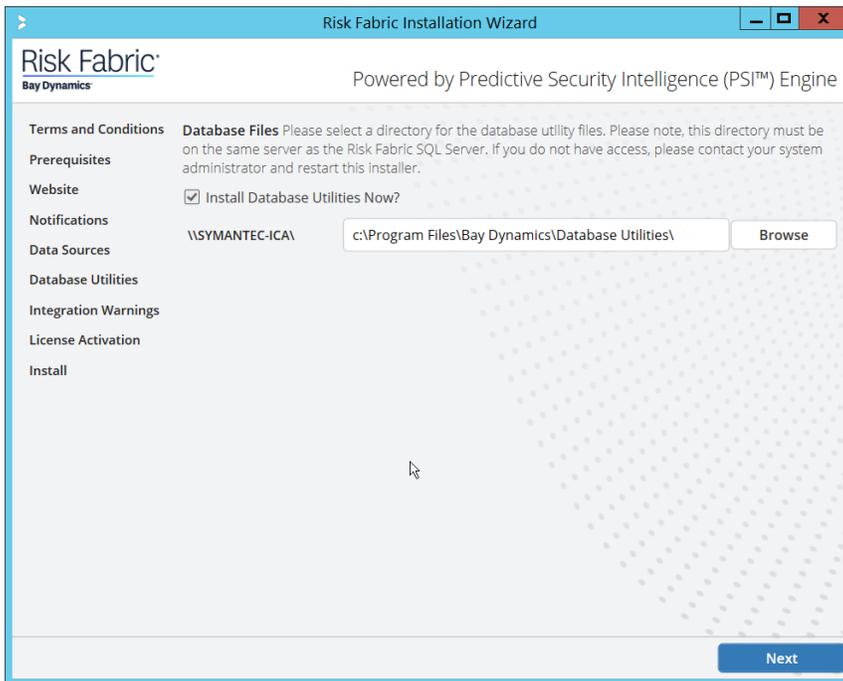
2384  
2385  
2386  
2387  
2388  
2389  
2390  
2391

12. Click **Next**.
13. Enter the name of the SQL Server you created in the format **<SERVER-DOMAIN-NAME>\<SQL-SERVER-NAME>**.
14. Click **Connect**, and verify that there are no connection issues.
15. Enter the name of the SQL Analysis Services server you created in the format **<SERVER-DOMAIN-NAME>\<SQL-SERVER-NAME>**. (It may be the same as the SQL Server).
16. Click **Connect**, and verify that there are no connection issues.



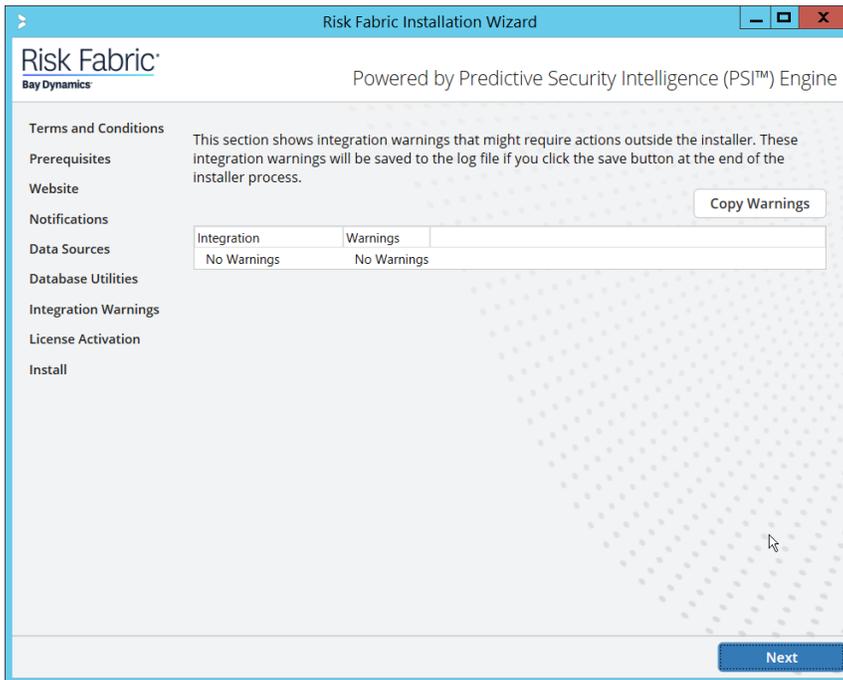
2392  
2393

17. Click **Next**.



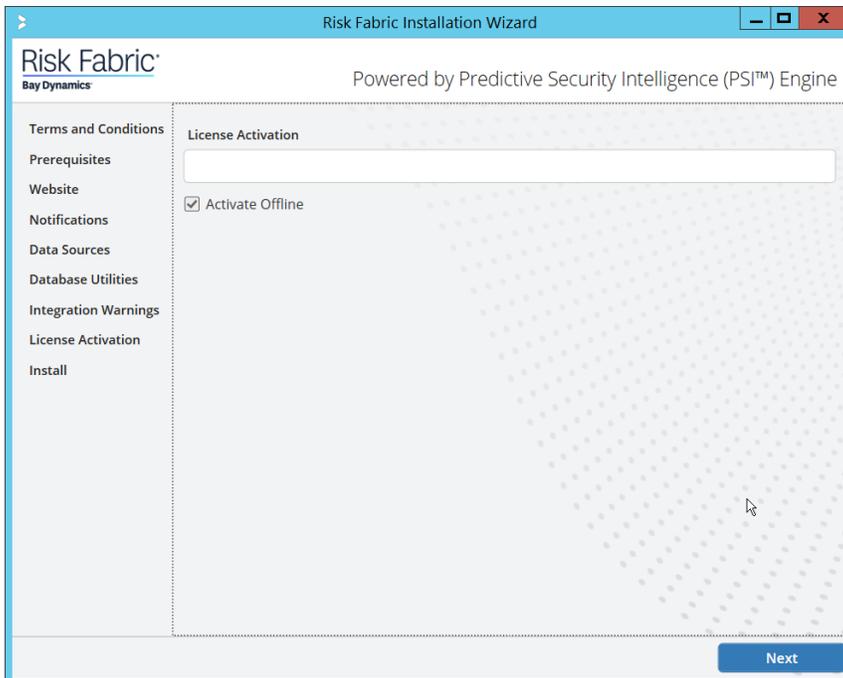
2394  
2395

18. Click **Next**.



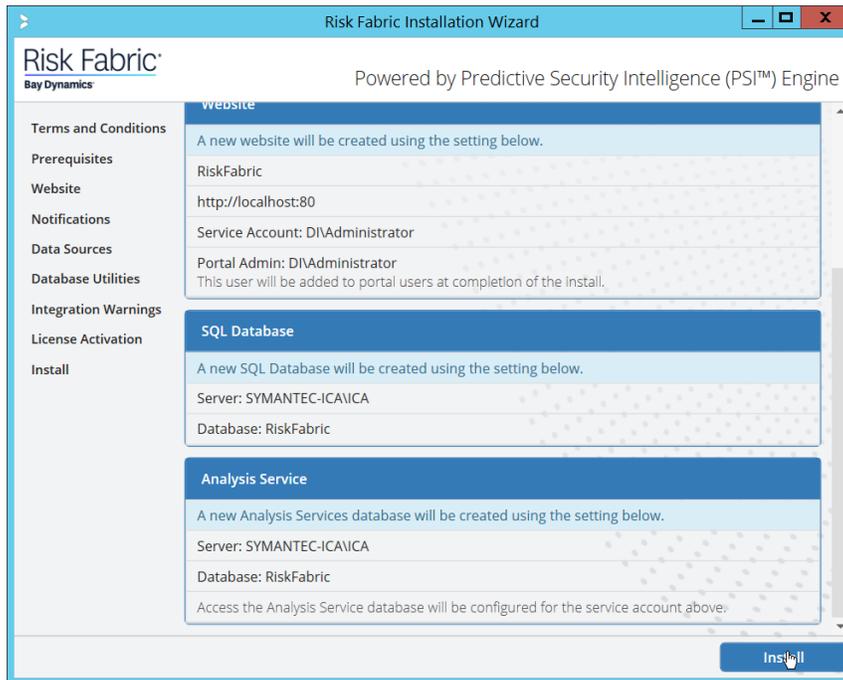
2396  
2397  
2398

- 19. Click **Next**.
- 20. Check the box next to **Activate Offline**.



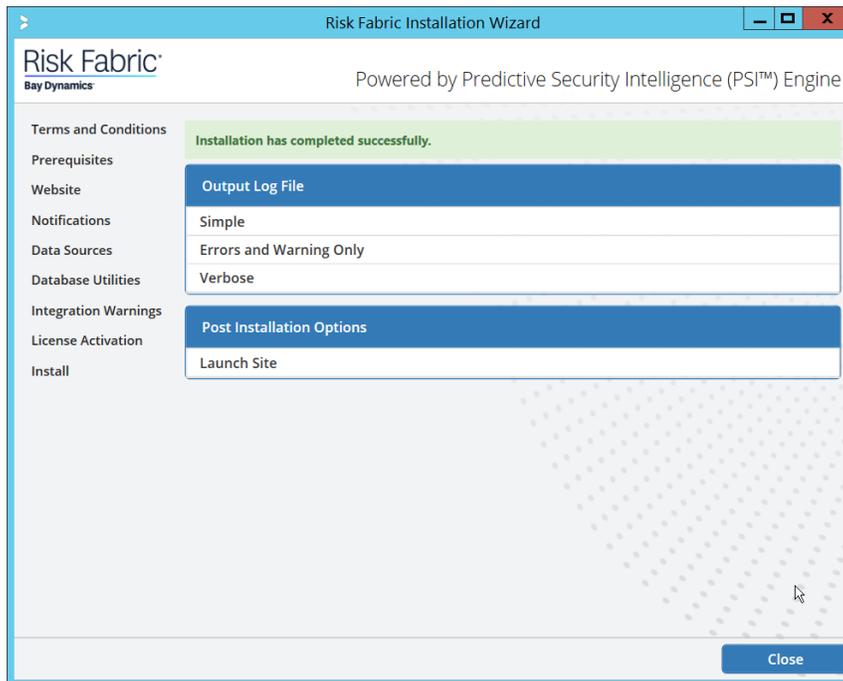
2399  
2400

- 21. Click **Next**.



2401  
2402

22. Click **Install**.



2403  
2404

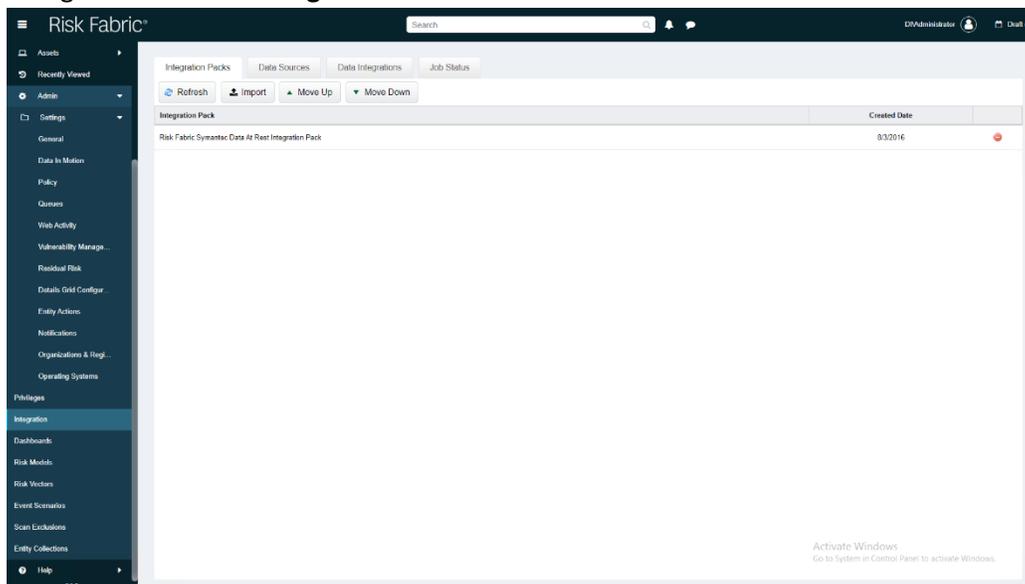
23. Click **Close**.

## 2405 2.15.4 Configuring Symantec ICA for Analysis

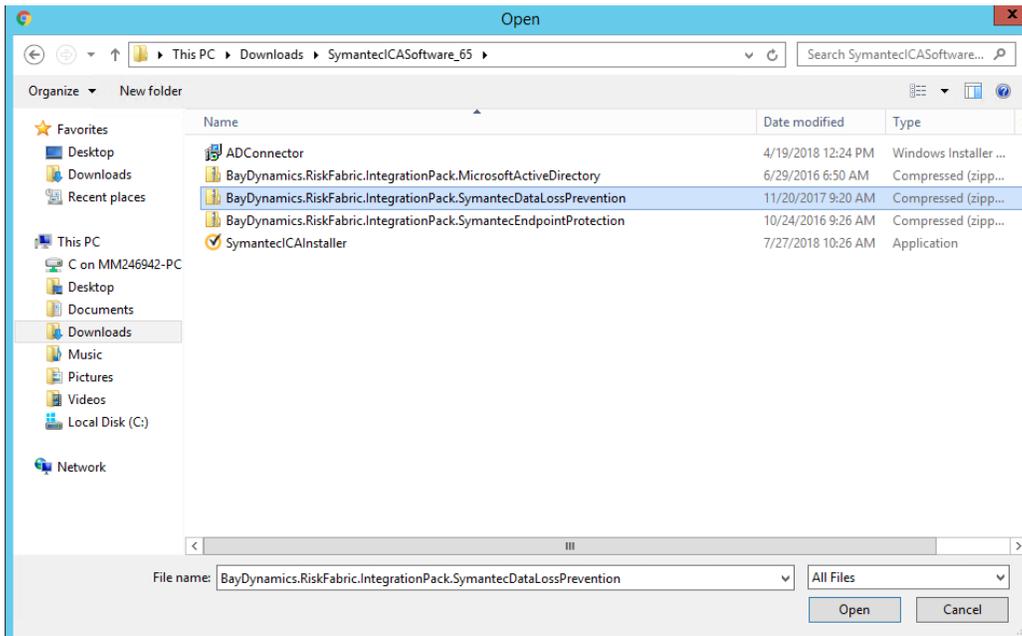
2406 This section will contain instructions for navigating some aspects of the ICA admin console and  
2407 dashboards, though this largely depends on the specific data your organization has identified and is  
2408 trying to analyze.

### 2409 2.15.4.1 Installing Integration Packs

- 2410 1. Download the relevant integration packs to someone on the local system. These are typically  
2411 provided by Symantec, in a zip file. The zip file should be titled in the format of  
2412 *BayDynamics.RiskFabric.IntegrationPack.<productName>*.
- 2413 2. Log in to the Risk Fabric web interface.
- 2414 3. Navigate to **Admin > Integration**.

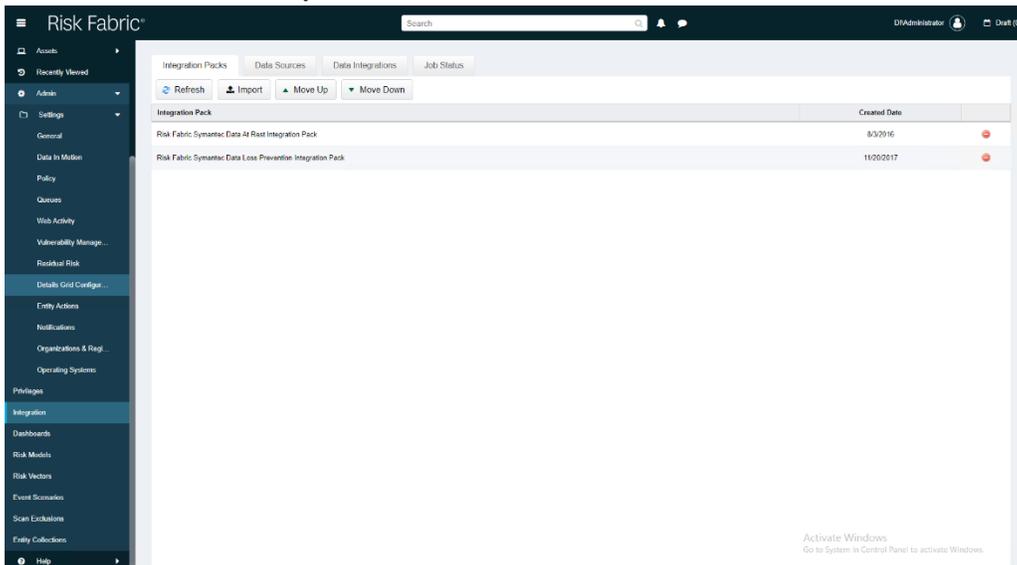


- 2415 4. Click **Import**.
- 2416 5. Find the zip file for the integration pack that you downloaded earlier.
- 2417



2418  
2419

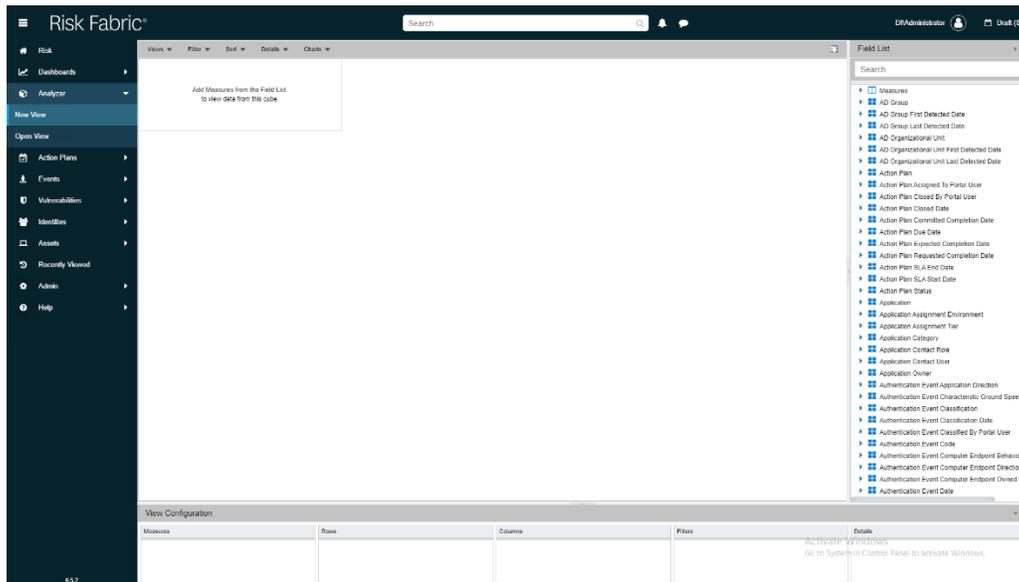
6. Select the file and click **Open**.



2420

2421 2.15.4.2 *Create a View*

2422 1. Navigate to **Analyzer > New View**.

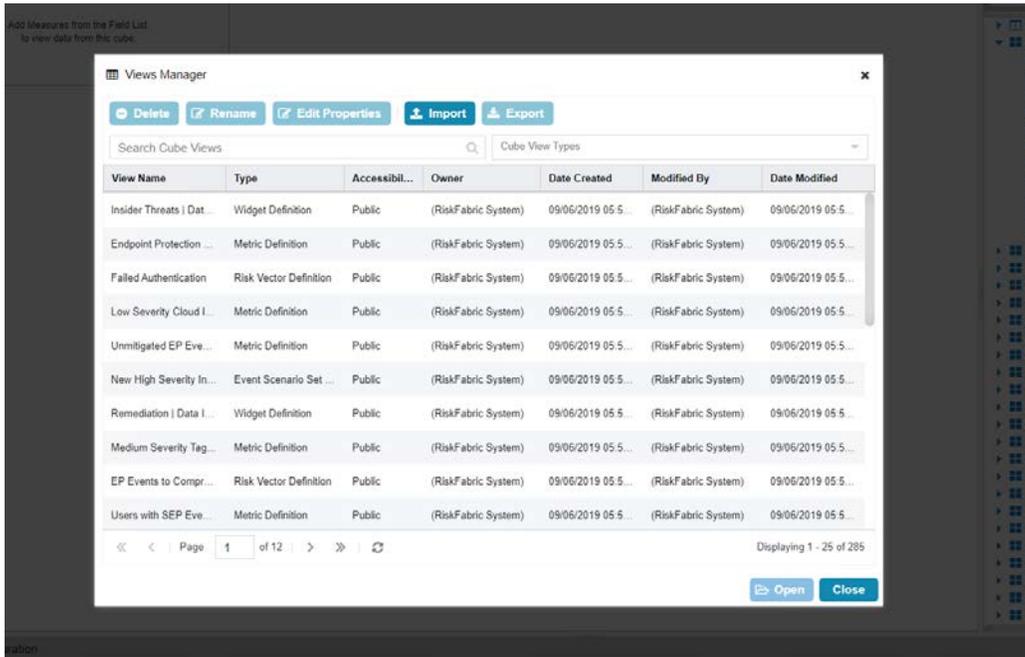


- 2423
- 2424
- 2425
- 2426
- 2427
- 2428
- 2429
- 2430
- 2431
- 2432
2. In the field list on the right, manually select or search for the data fields desired.
  3. The fields can be added either by dragging the field onto the screen or by right-clicking on the field and selecting where it should be added. Ultimately, which views to select depends on the needs and preferences of your organization.
  4. When finished, click **Save**.
  5. Enter a name for the **View Name**.
  6. Select the type of View for **Type**.
  7. Check the box next to **This view is accessible by all Users (Public)** only if you wish for this view to be visible by anyone logged in.

- 2433
- 2434
8. Click **Save**.

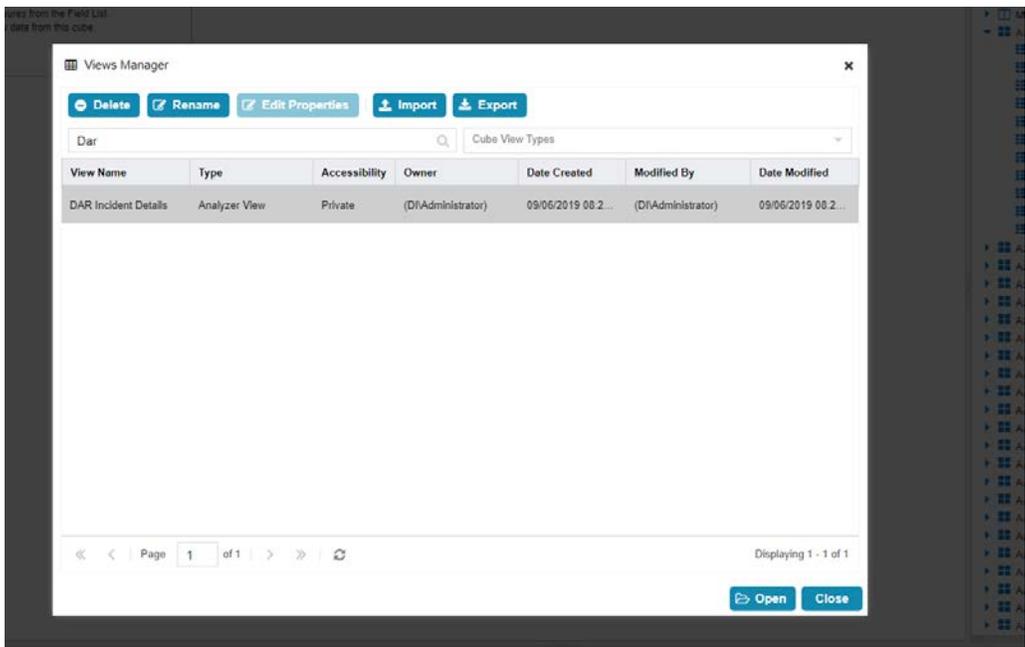
### 2435 2.15.4.3 *Open an Existing View*

- 2436
1. Navigate to **Analyzer > Open View**.



2437  
2438  
2439  
2440  
2441

2. Begin to search for the view you want by typing a search term into **Search Cube Views**. (Note: if you created a view, it will also be present in this list).
3. Click the **Search** icon.
4. Select a view.

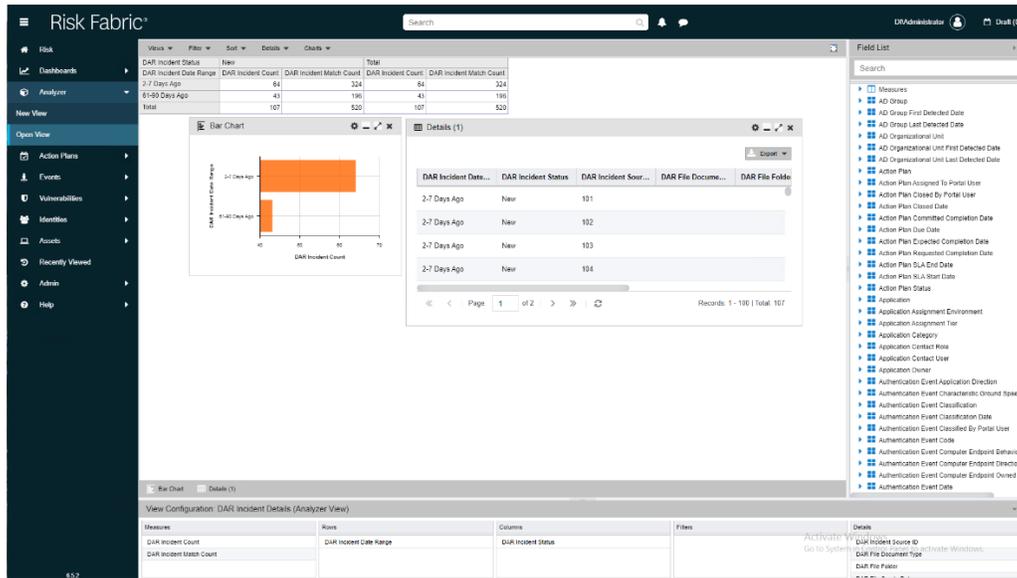


2442  
2443

5. Click **Open**.

2444 2.15.4.4 *Viewing Detailed Analyzer Data*

- 2445 1. The desired field data can be exported to either a *.csv* or *.excel* format, by clicking on the **Export**
- 2446 button in the details tab.



- 2447 2. Charts can be added or removed using the **Charts** dropdown menu near the top of the analyzer.
- 2448 3. Any data in the **Field List** on the right side can be added to or removed from the view and will
- 2449 be automatically incorporated into its relevant rows or columns.
- 2450 4. The entire view format can be exported as a *.json* file from the **Open View** option.
- 2451

2452 2.16 **Integration: Cisco Identity Services Engine and Cisco Stealthwatch**

2453 This section will detail an integration between Cisco Identity Services Engine (ISE) and Cisco

2454 Stealthwatch, allowing Stealthwatch to apply certain policies to hosts in ISE. Stealthwatch acts as a

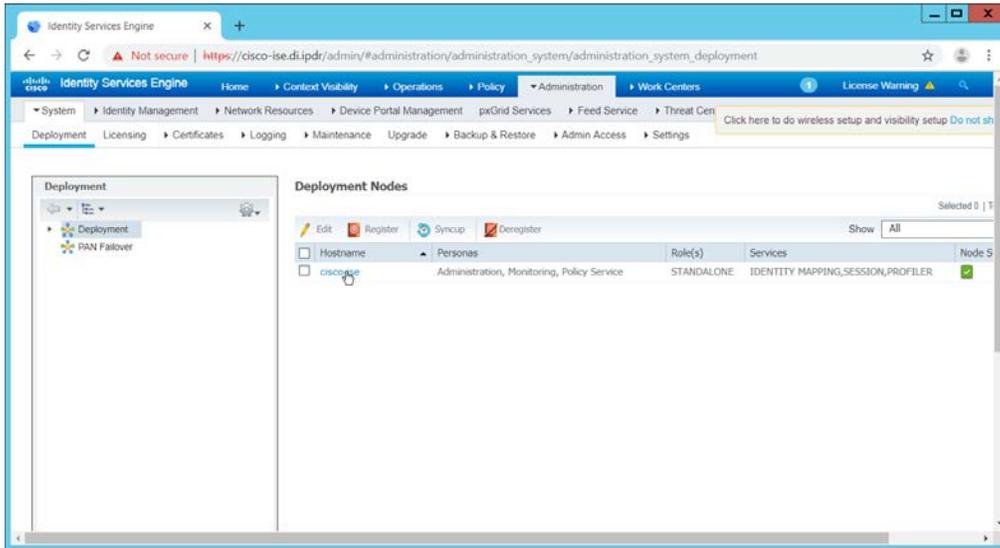
2455 network monitoring solution and can be integrated with ISE to enable mitigation capabilities in

2456 response to events. Please see *Deploying Cisco Stealthwatch 7.0 with Cisco ISE 2.4 using pxGrid* for

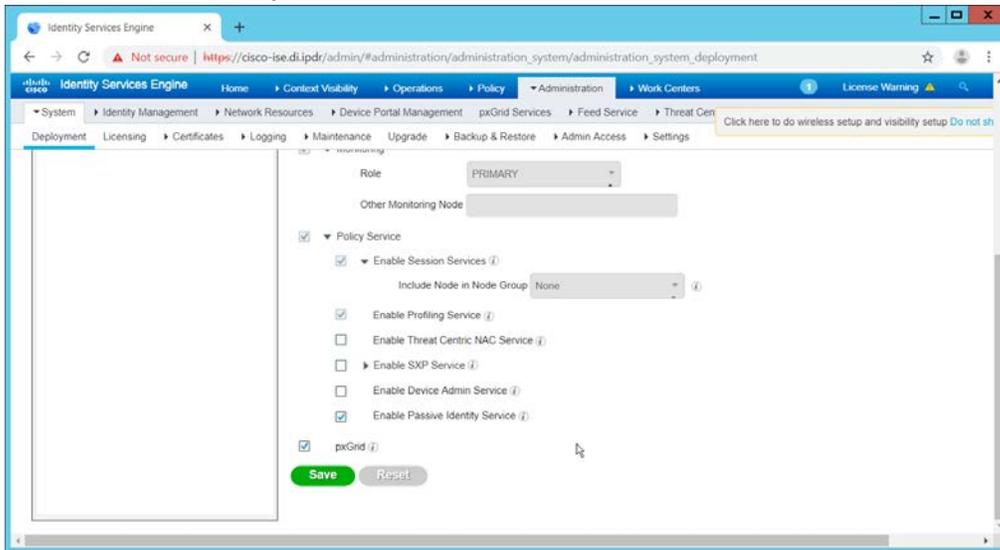
2457 details and other potential uses of the integration.

2458 2.16.1 **Configuring Certificates for pxGrid**

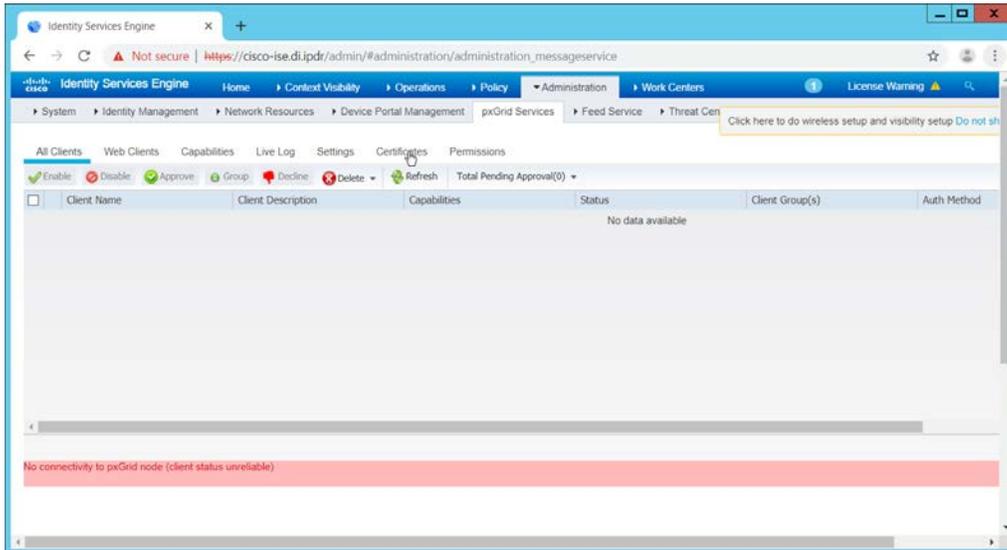
- 2459 1. Log in to the Cisco ISE web console in a browser.
- 2460 2. Navigate to **Administration > System > Deployment**.



- 2461
  - 2462
  - 2463
3. Click the hostname of the Cisco ISE machine.
  4. Check the box next to **pxGrid**.

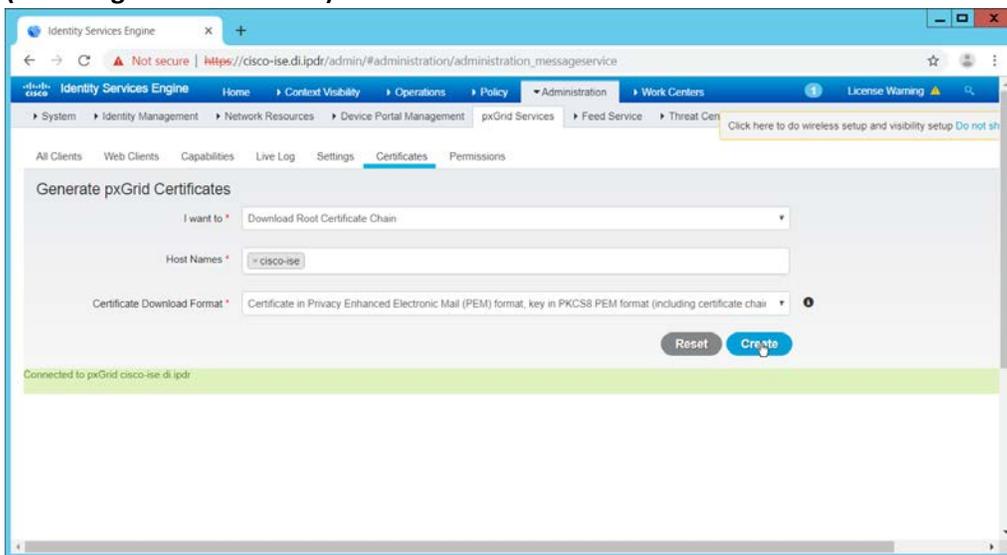


- 2464
  - 2465
  - 2466
5. Click **Save**.
  6. Navigate to **Administration > pxGrid Services**.



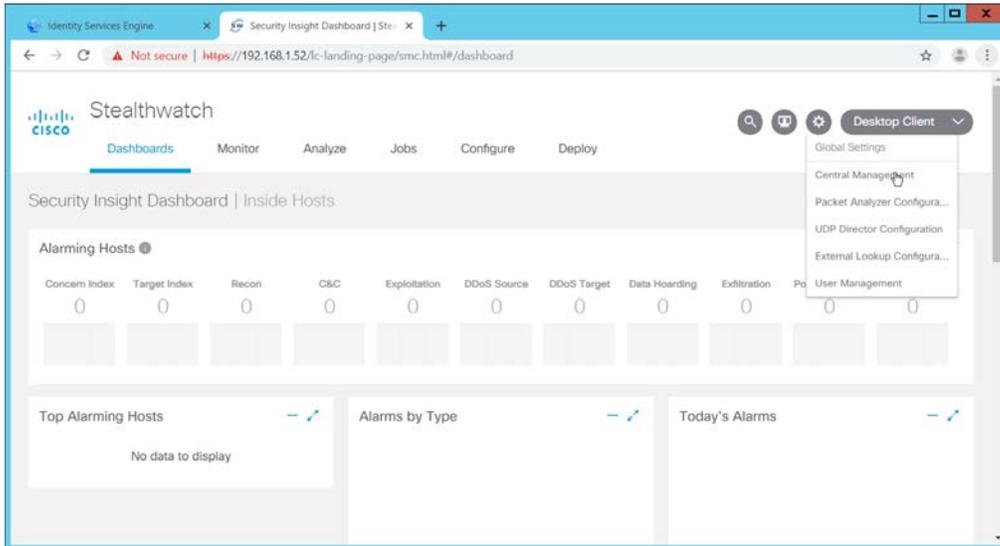
2467  
2468  
2469  
2470  
2471  
2472

7. Click **Certificates**.
8. Select **Download Root Certificate Chain** for **I want to**.
9. Select the hostname of the Cisco ISE server for **Host Names**.
10. Select **Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)** for **Certificate Download Format**.



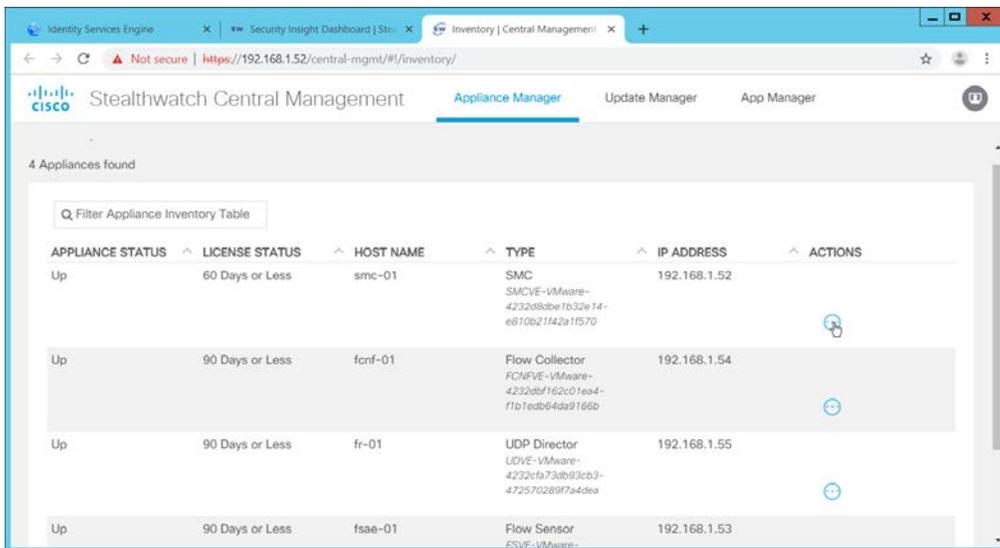
2473  
2474  
2475  
2476

11. Click **Create**. This will download a zip file containing the certificate.
12. Extract the zip file—it may contain several files—the one we are interested in is the Root CA.
13. Log in to the **Stealthwatch Management Console** through the browser.



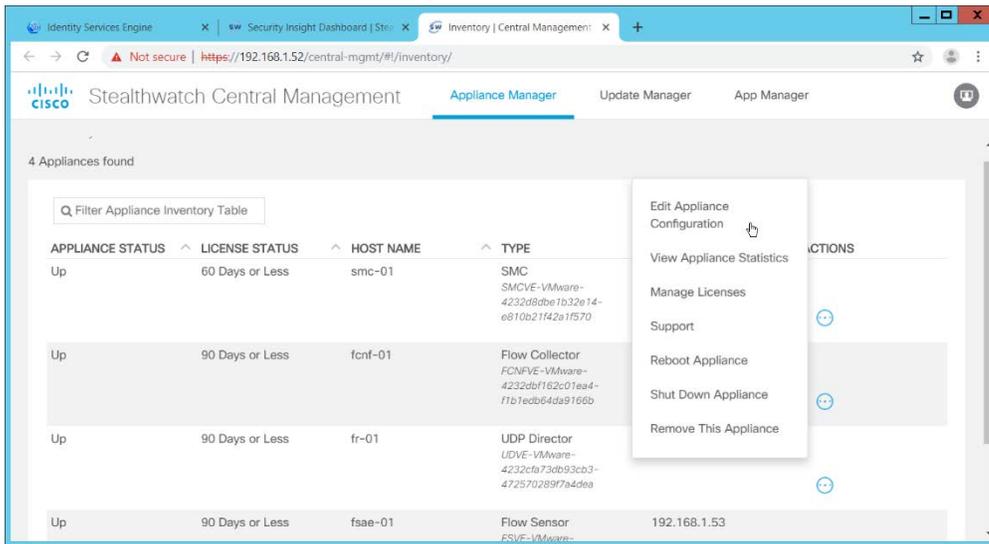
2477  
2478  
2479

- In the top right corner of the console, hover over the **gear icon** and select **Central Management** from the submenu.

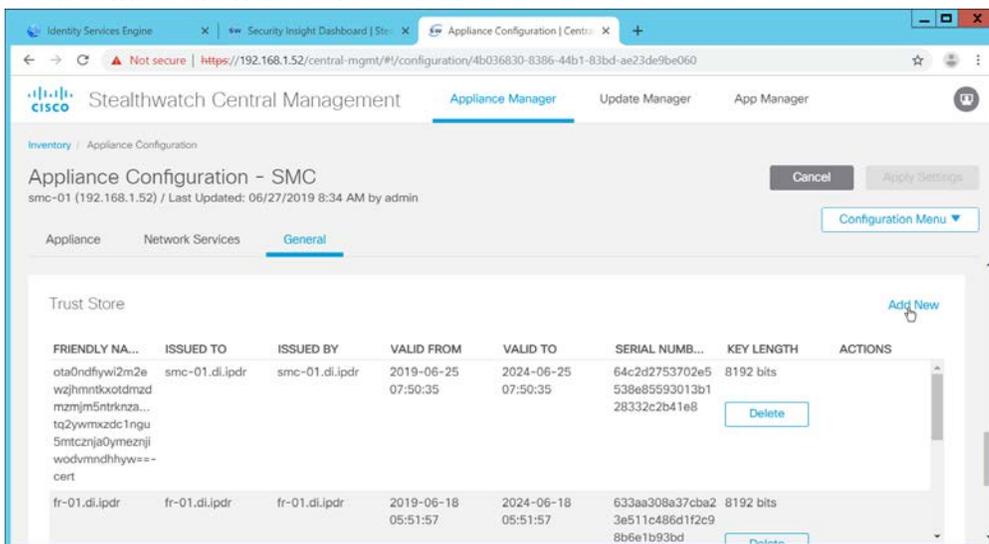


2480  
2481  
2482

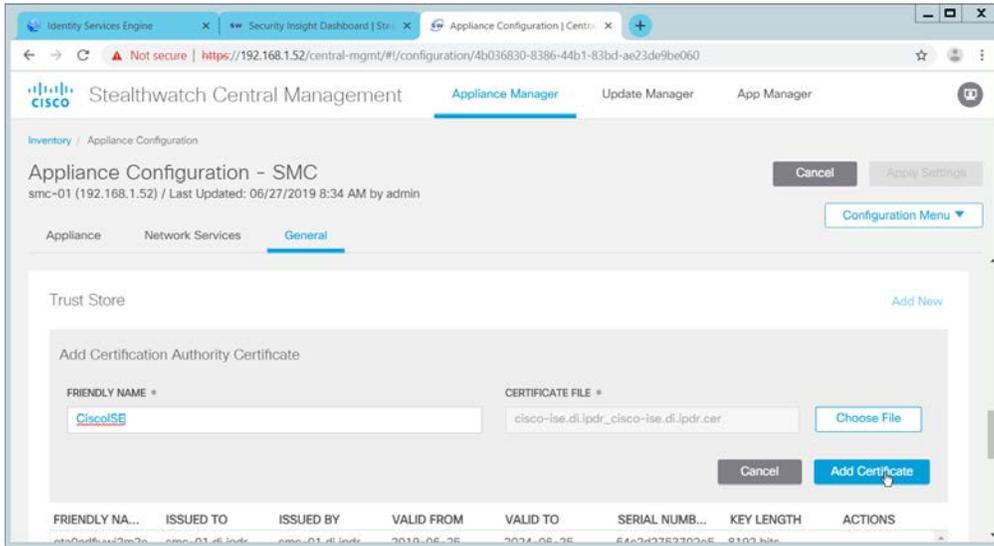
- In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC). Click the **ellipses button** in the **Actions** column.



- 2483
  - 2484
  - 2485
  - 2486
16. This will open a submenu. Select **Edit Appliance Configurations**.
  17. Click the **General** tab.
  18. Scroll down to the **Trust Store** section.

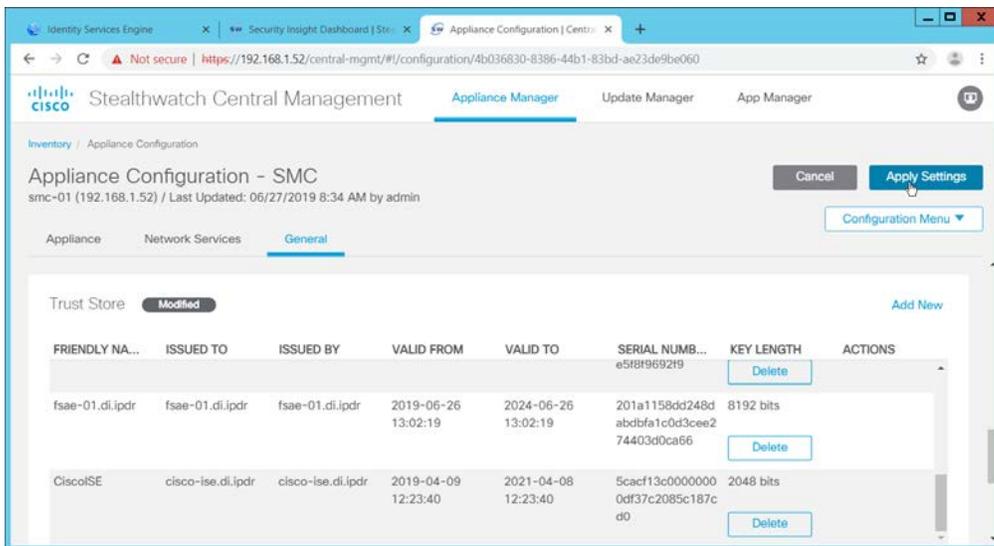


- 2487
  - 2488
  - 2489
  - 2490
  - 2491
19. Click **Add New**.
  20. Enter a **name**.
  21. Click **Choose File**.
  22. Select the Cisco ISE Root certificate from the files downloaded earlier.



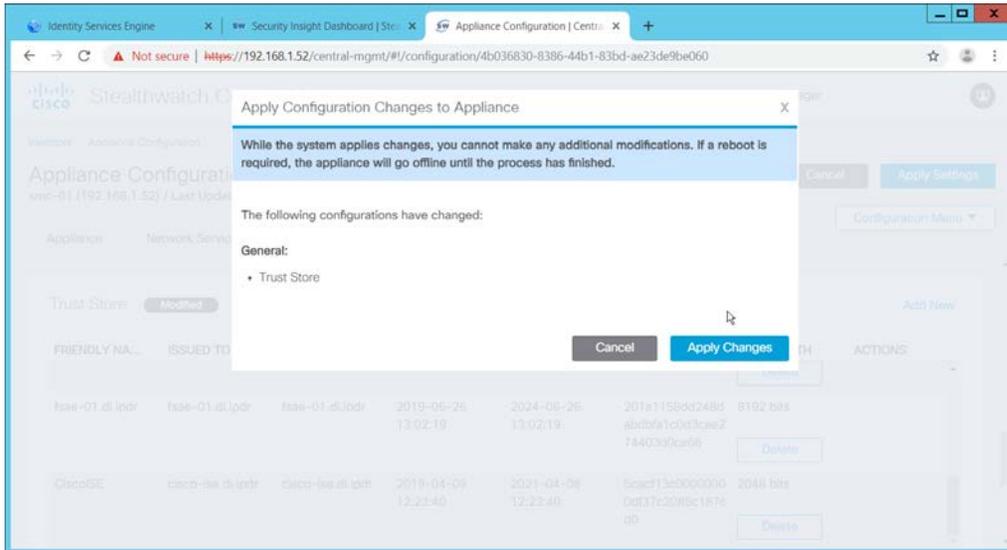
2492  
2493

23. Click **Add Certificate**.

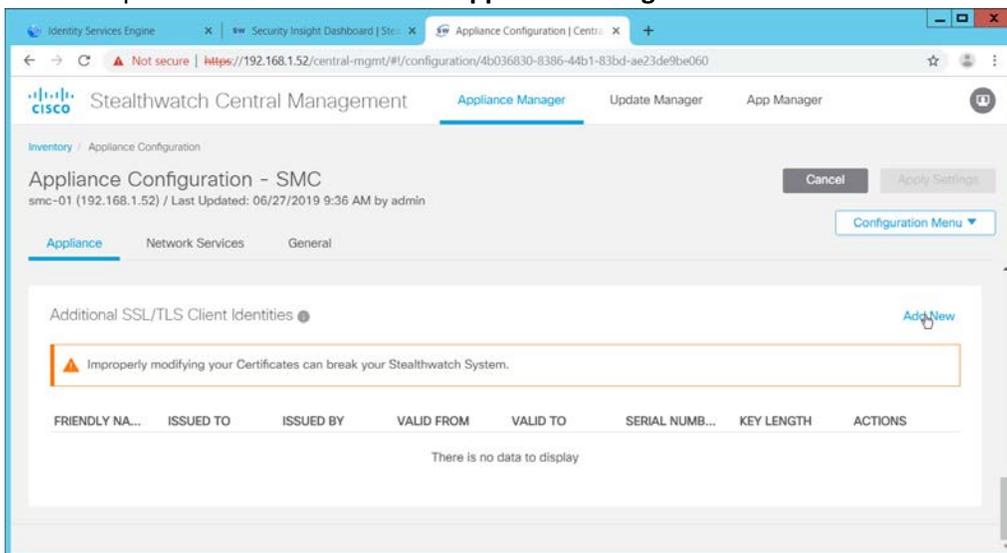


2494  
2495

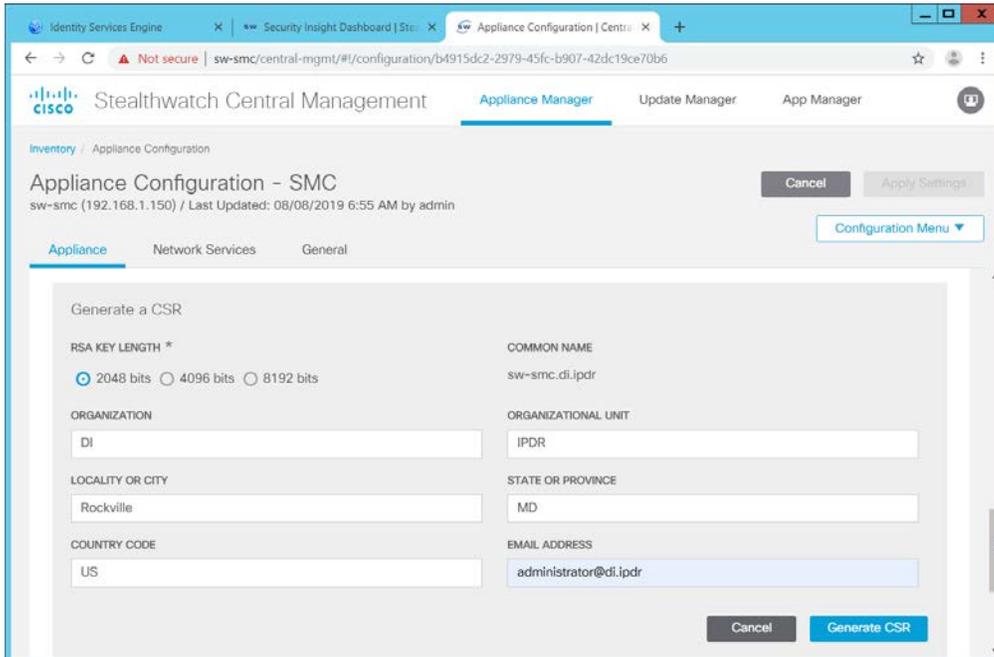
24. Click **Apply Settings**.



- 2496
  - 2497
  - 2498
  - 2499
  - 2500
  - 2501
25. Click **Apply Changes** if prompted to confirm the changes.
  26. When that finishes, navigate back to the **Appliance Configurations** section.
  27. In the table, find the row with the Stealthwatch Management Console (likely labeled as SMC). Click the **ellipses button** in the **Actions** column.
  28. This will open a submenu. Select **Edit Appliance Configurations**.

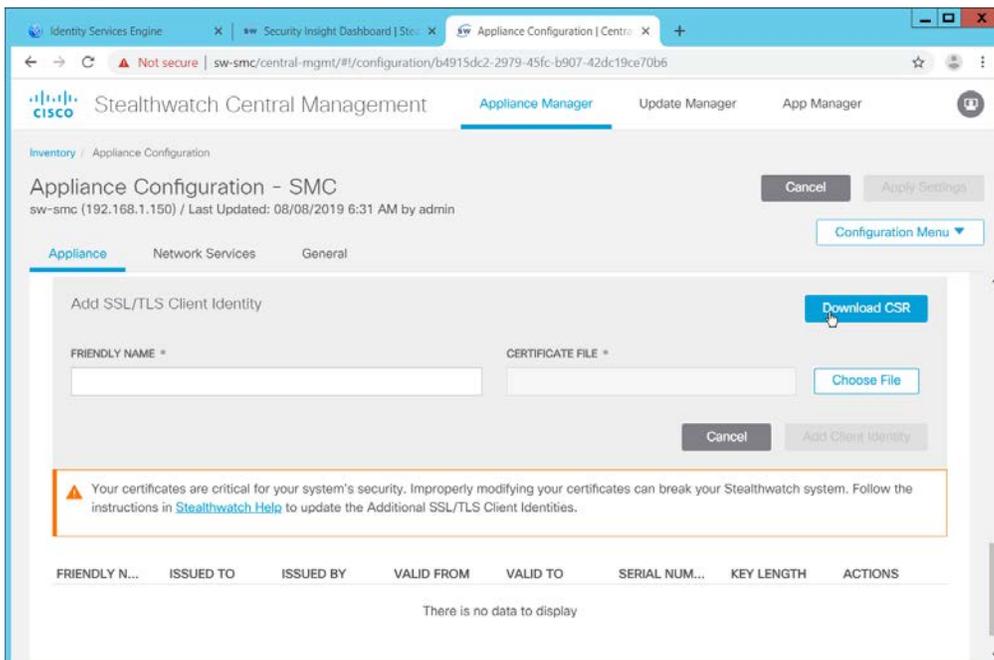


- 2502
  - 2503
  - 2504
  - 2505
29. Click **Add New** under **Additional SSL/TLS Client Identities**.
  30. Select **2048** for **RSA Key Length**.
  31. Enter your organization's information.



2506  
2507

32. Click **Generate CSR**.



2508  
2509  
2510  
2511  
2512

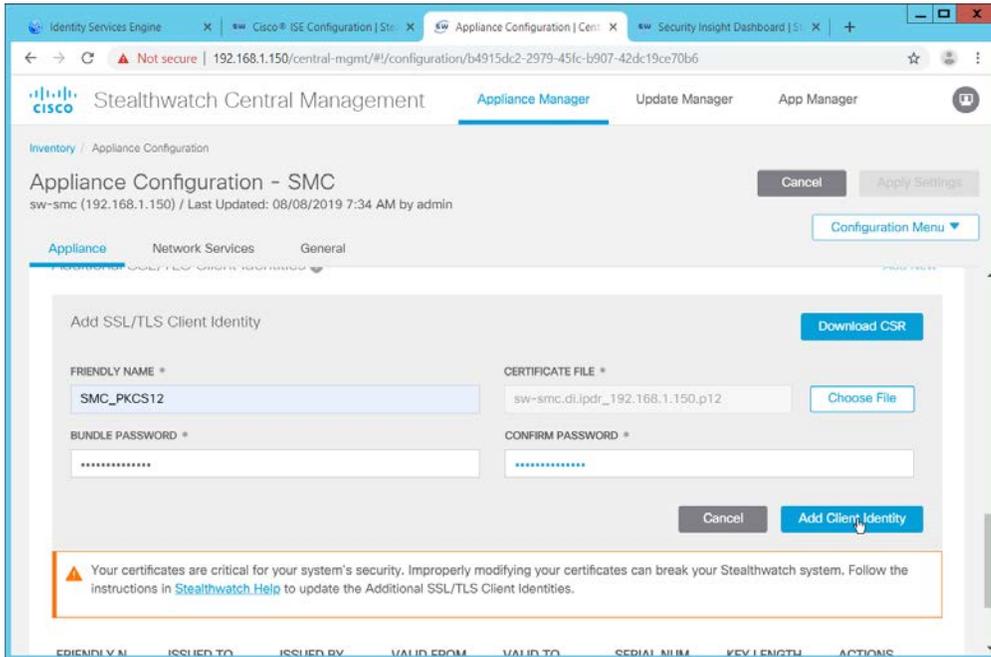
33. When this finishes, click **Download CSR**.

34. Open the CSR in a text file, and copy all the contents.

35. On the ISE web console, navigate to **Administration > pxGrid Services > Certificates > Generate pxGrid Certificates**.

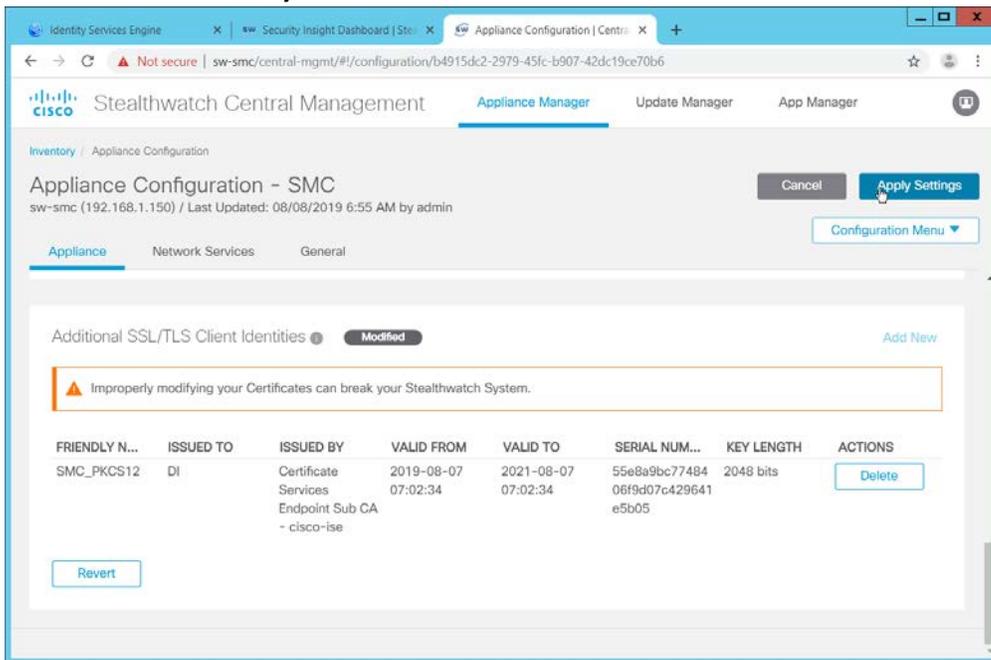
- 2513 36. Select **Generate a single certificate (with certificate signing request)** for I want to.
- 2514 37. Paste the copied text into the **Certificate Signing Request Details**.
- 2515 38. Enter a description such as **SMC** for the **Description**.
- 2516 39. Select **IP Address** for **Subject Alternative Name (SAN)**.
- 2517 40. Enter the **IP Address** of the Stealthwatch Management Console.
- 2518 41. Select **PKCS12 format (including certificate chain; one file for both the certificate chain and**
- 2519 **key)** for **Certificate Download Format**.
- 2520 42. Enter a password, and confirm the password.

- 2521 43. Click **Create**.
- 2522 44. This will download a zip file. Unzip the file.
- 2523 45. On the Stealthwatch Management Console (SMC) web console, under **Additional SSL/TLS Client**
- 2524 **Identities** (where you downloaded the CSR), click **Choose File**.
- 2525 46. Upload the certificate file from the zip file that has the hostname of the SMC in it; the file
- 2526 extension should be **.p12**.
- 2527 47. Enter a name for **Friendly Name**.
- 2528 48. Enter the password used in ISE when generating the certificate.
- 2529



2530  
2531

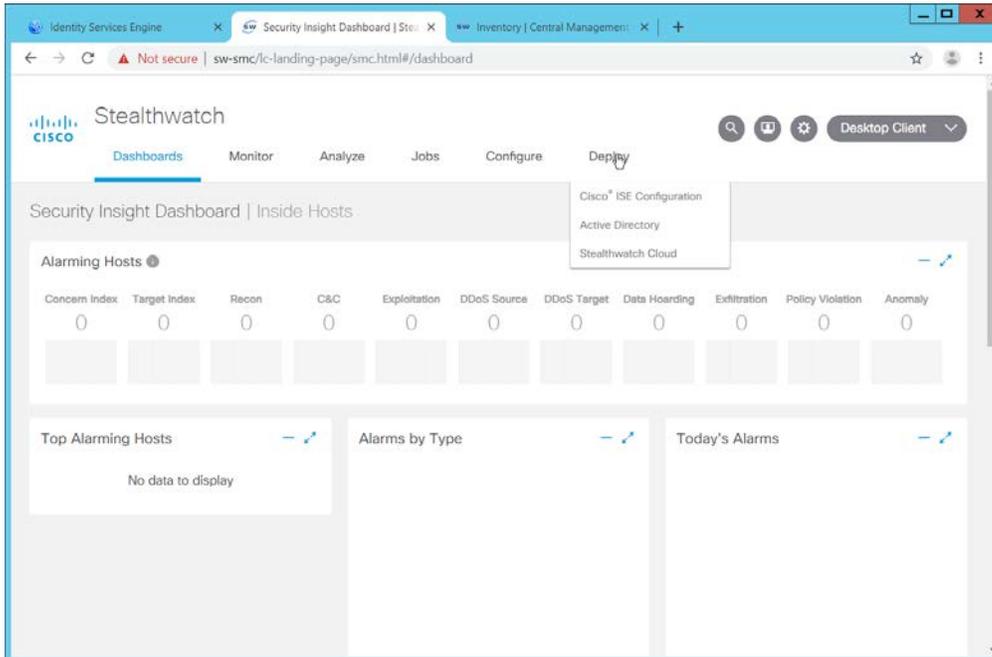
49. Click **Add Client Identity**.



2532  
2533  
2534

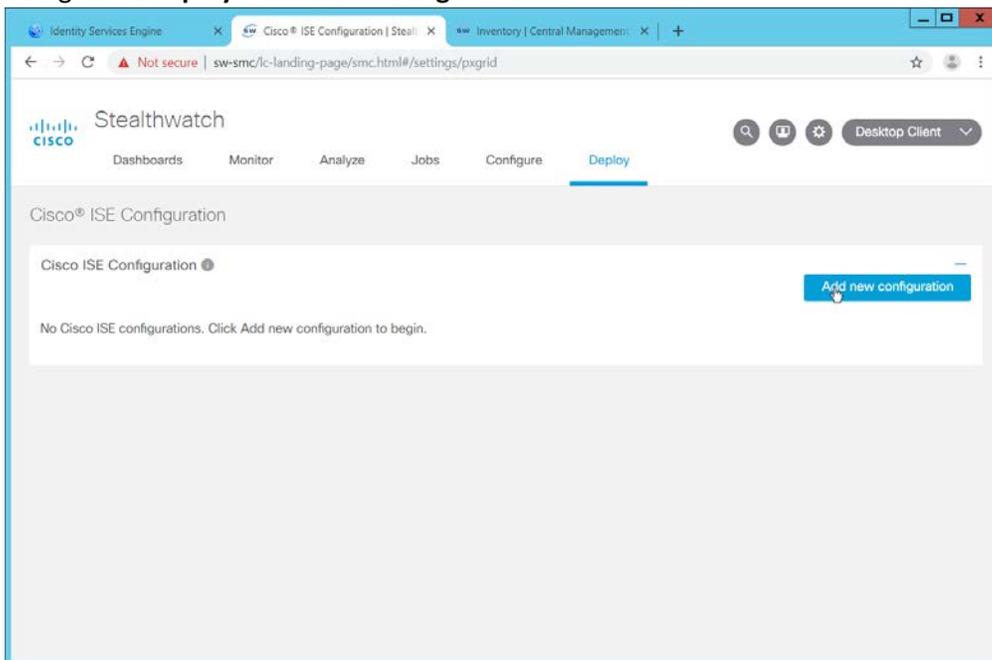
50. Click **Apply Settings**.

51. Navigate back to the SMC web console home screen.



2535  
2536

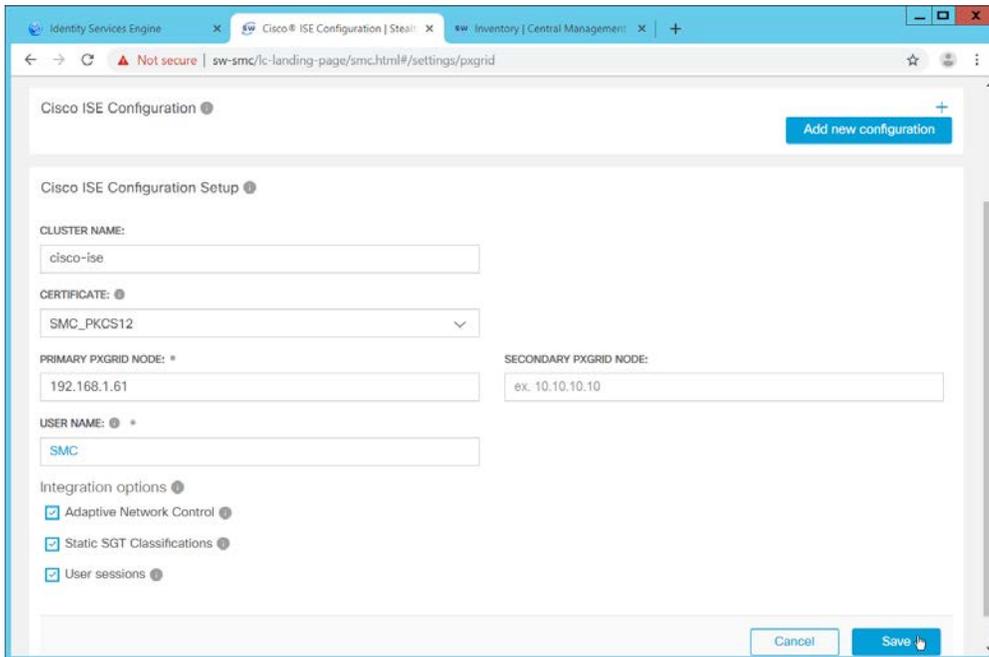
52. Navigate to **Deploy > Cisco ISE Configuration**.



2537  
2538  
2539  
2540  
2541

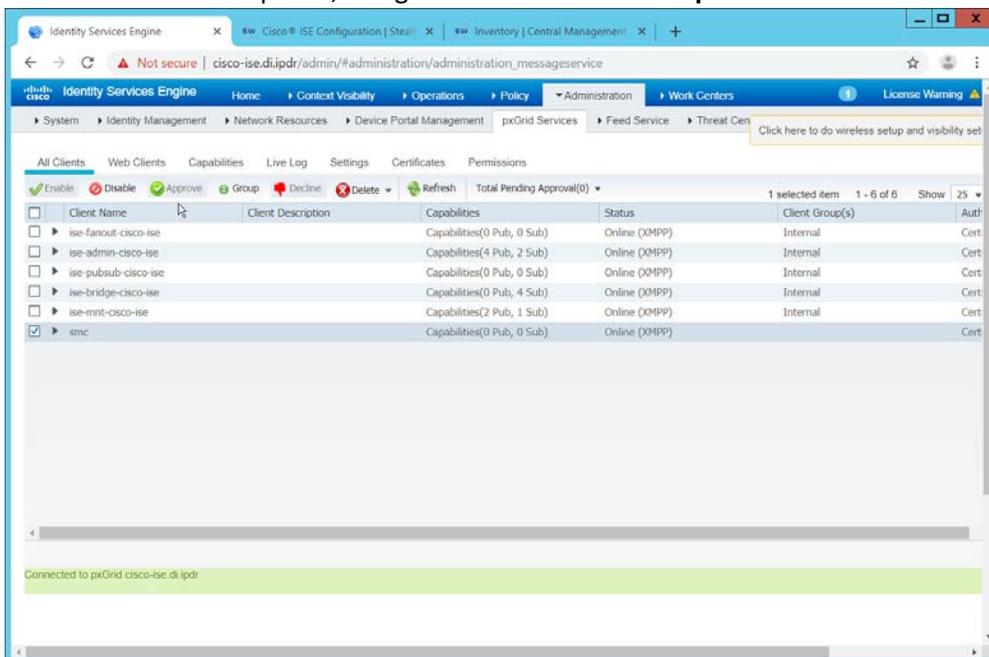
- 53. Click **Add New Configuration**.
- 54. Enter a Cisco ISE cluster name.
- 55. Select the certificate you just uploaded for **Certificate**.
- 56. Enter the **IP Address** of Cisco ISE for **Primary pxGrid Node**.

2542 57. Enter a **username** for the SMC to use.

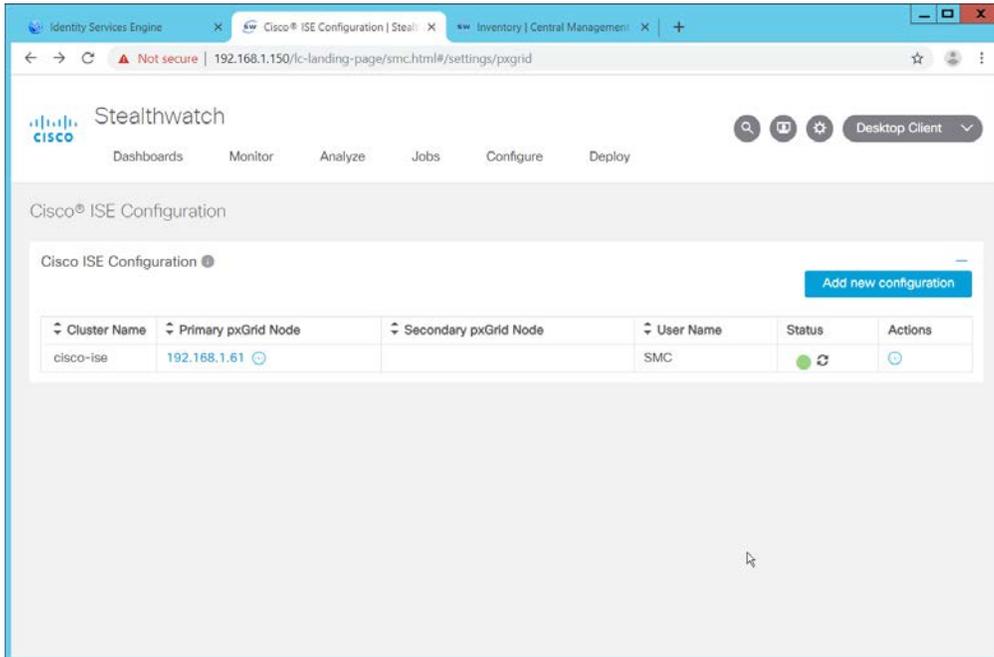


2543 58. Click **Save**.

2544 59. On the Cisco ISE web portal, navigate to **Administration > pxGrid Services > All Clients**.



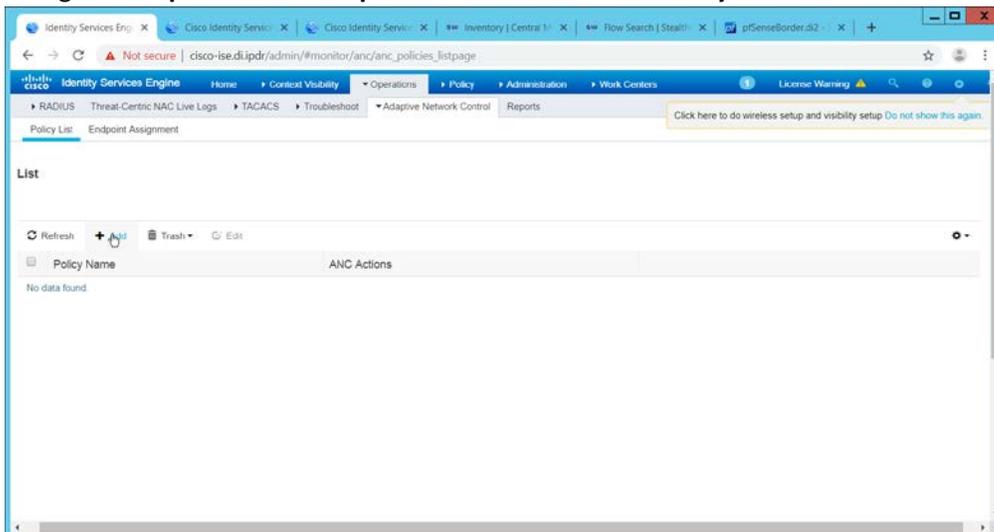
2546 60. If the SMC client you just created says **Pending**, check the box next to it and click **Approve**.



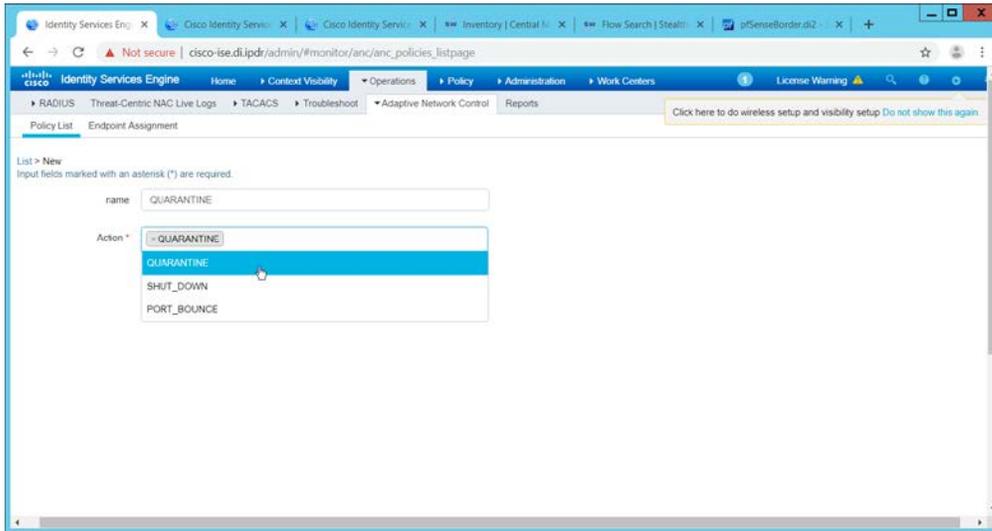
- 2548  
2549 61. The SMC Cisco ISE Configuration page will have a green status icon if it can successfully  
2550 authenticate to ISE.

## 2551 2.16.2 Configuring Stealthwatch to Quarantine through ISE

- 2552 1. Navigate to **Operations > Adaptive Network Control > Policy List**.

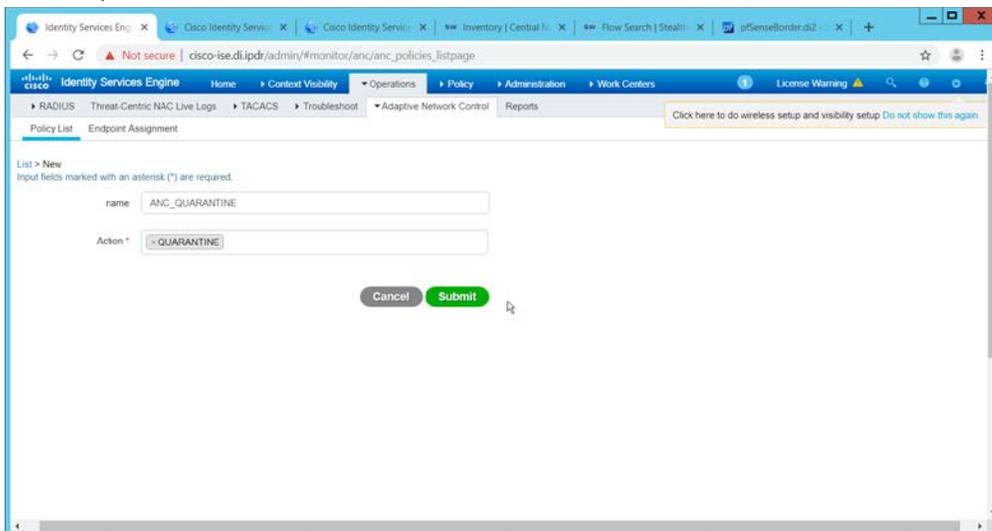


- 2553  
2554 2. Click **Add**.  
2555 3. Enter a name for a quarantine action.



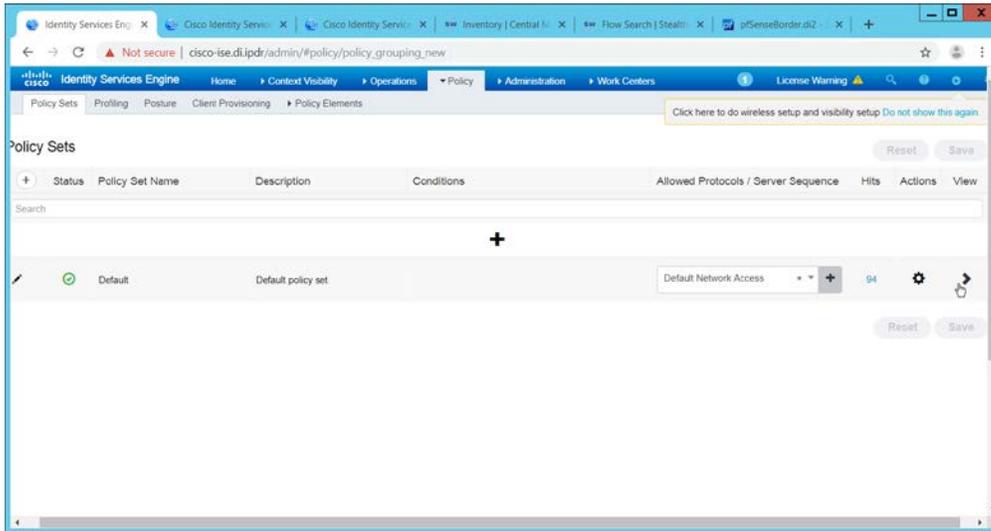
2556  
2557

4. Select **QUARANTINE** for the **Action**.

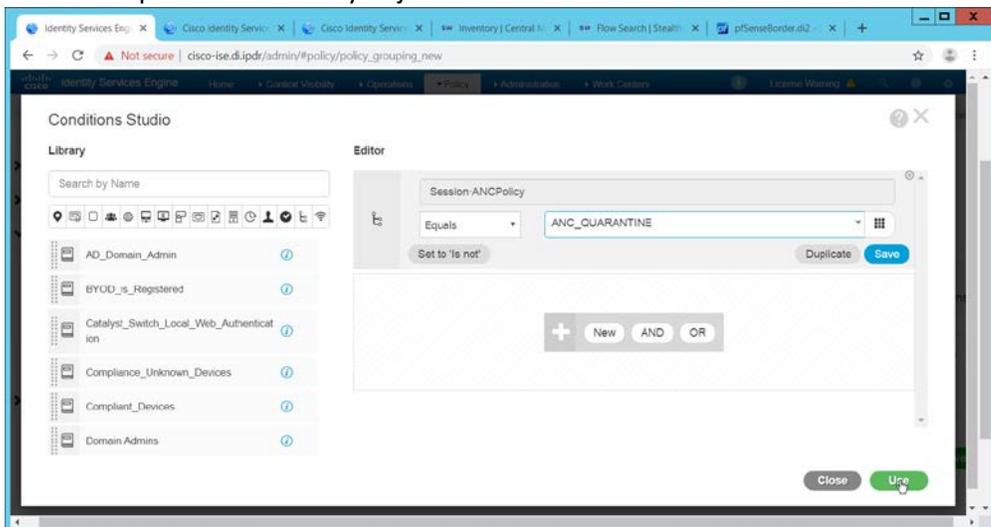


2558  
2559  
2560

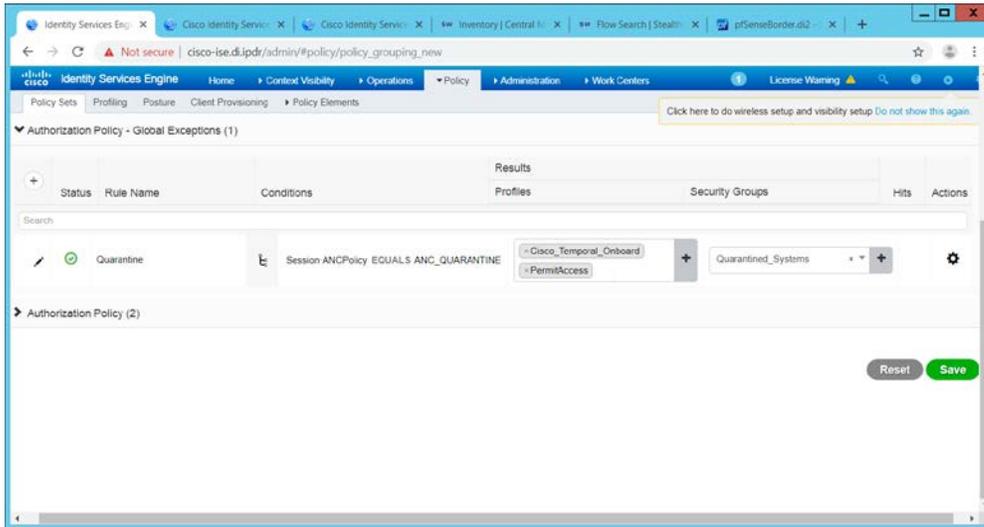
5. Click **Submit**.
6. Navigate to **Policy > Policy Sets**.



- 2561
  - 2562
  - 2563
  - 2564
  - 2565
  - 2566
  - 2567
7. Click the > arrow next to the default policy set.
  8. Expand the **Authorization Policy - Global Exceptions** section.
  9. Click the + plus sign to add a new policy.
  10. Click the + plus sign under **Conditions**.
  11. Select the field **Session – ANCPolicy**.
  12. Select the quarantine action you just created for the Attribute value.

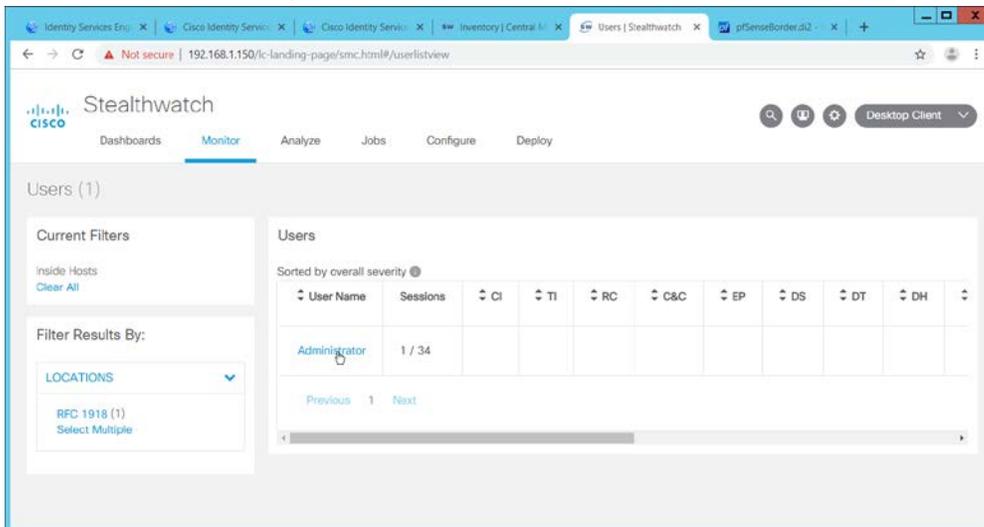


- 2568
  - 2569
  - 2570
  - 2571
  - 2572
13. Click **Use**.
  14. Select the **Deny Access** profile; the profile selected here will be applied to the machine when the machine is added to the quarantine group.
  15. Select **Quarantined\_Systems** for **Security Groups**.



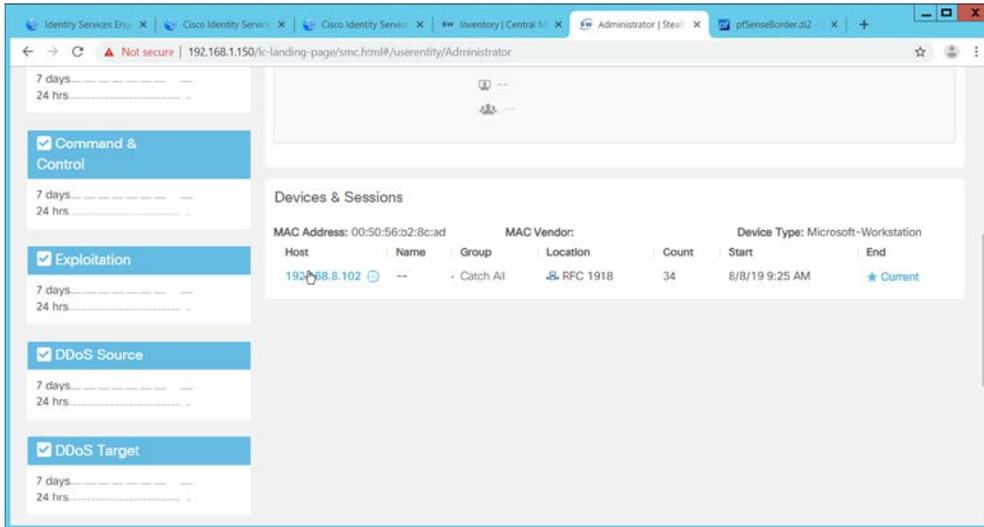
2573  
2574  
2575

- 16. Click **Save**.
- 17. In the SMC web console, click **Monitor > Users**.



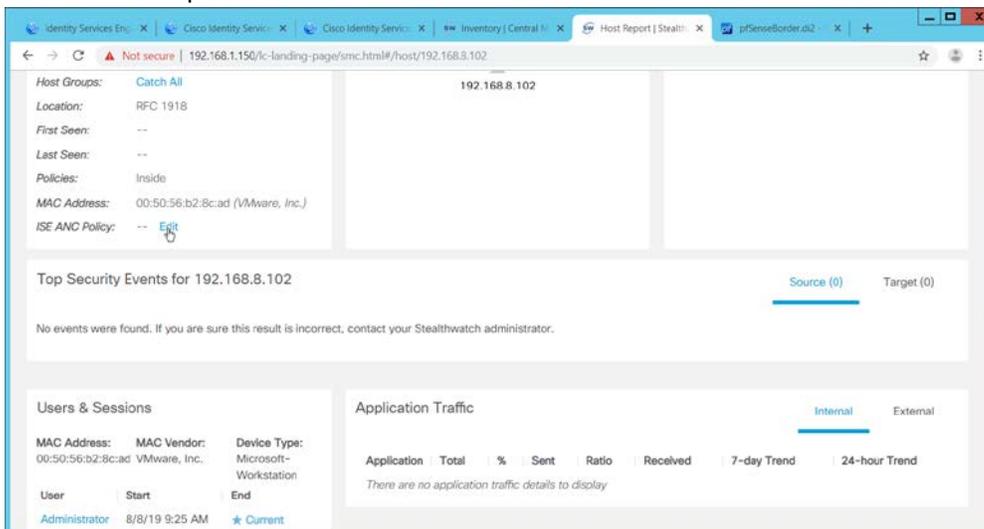
2576  
2577

- 18. Select a user to quarantine.



2578  
2579

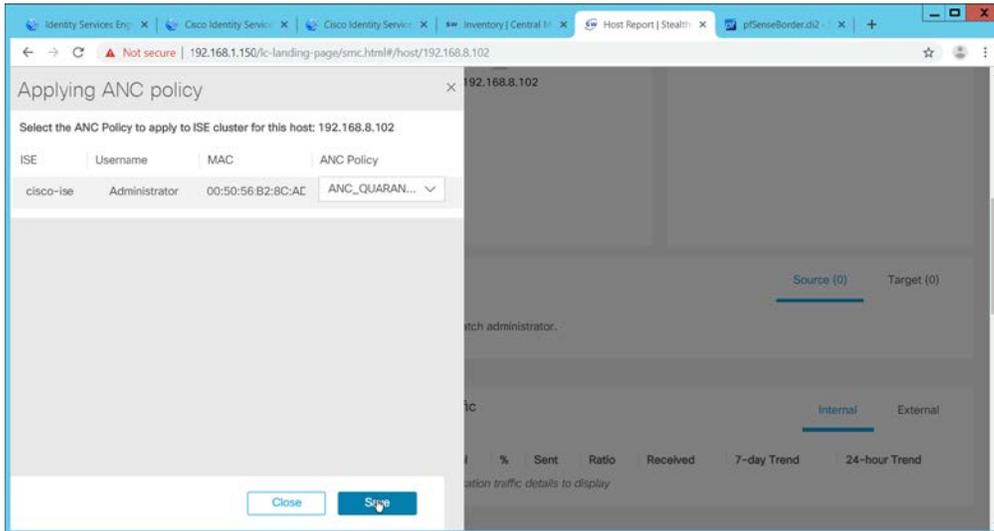
19. Click a host to quarantine.



2580  
2581  
2582

20. Click **Edit** next to **ISE ANC Policy**.

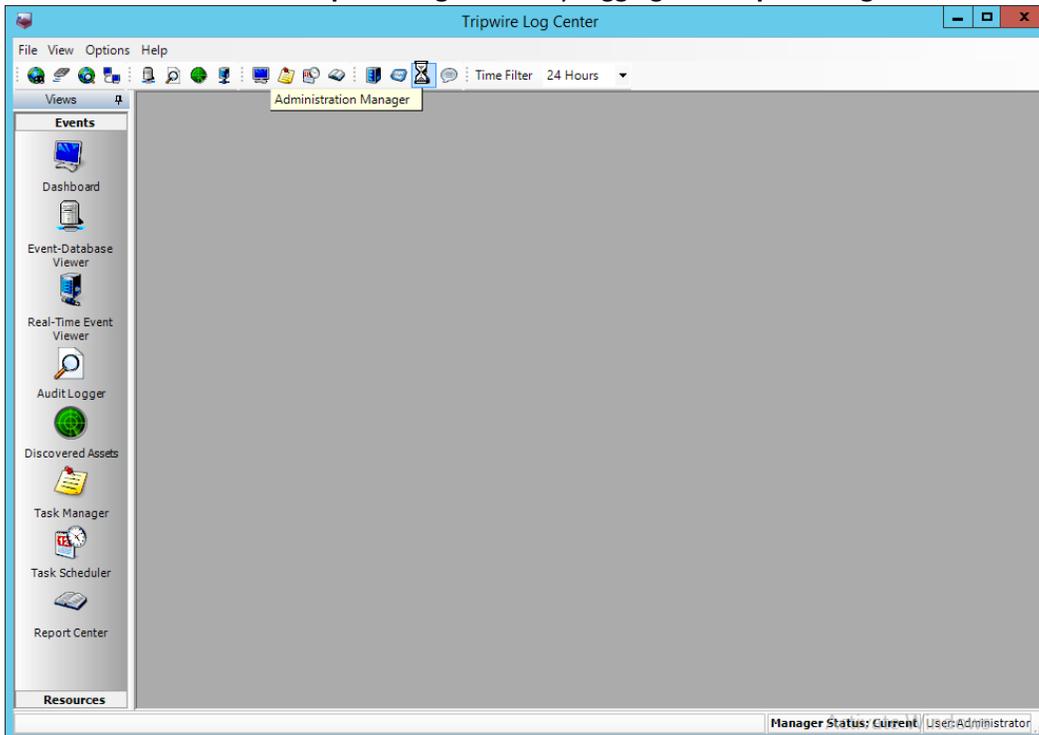
21. From the drop down, select the quarantine action you created earlier.



- 2583
  - 2584
  - 2585
22. Click **Save**.
  23. This will apply the quarantine action to the machine.

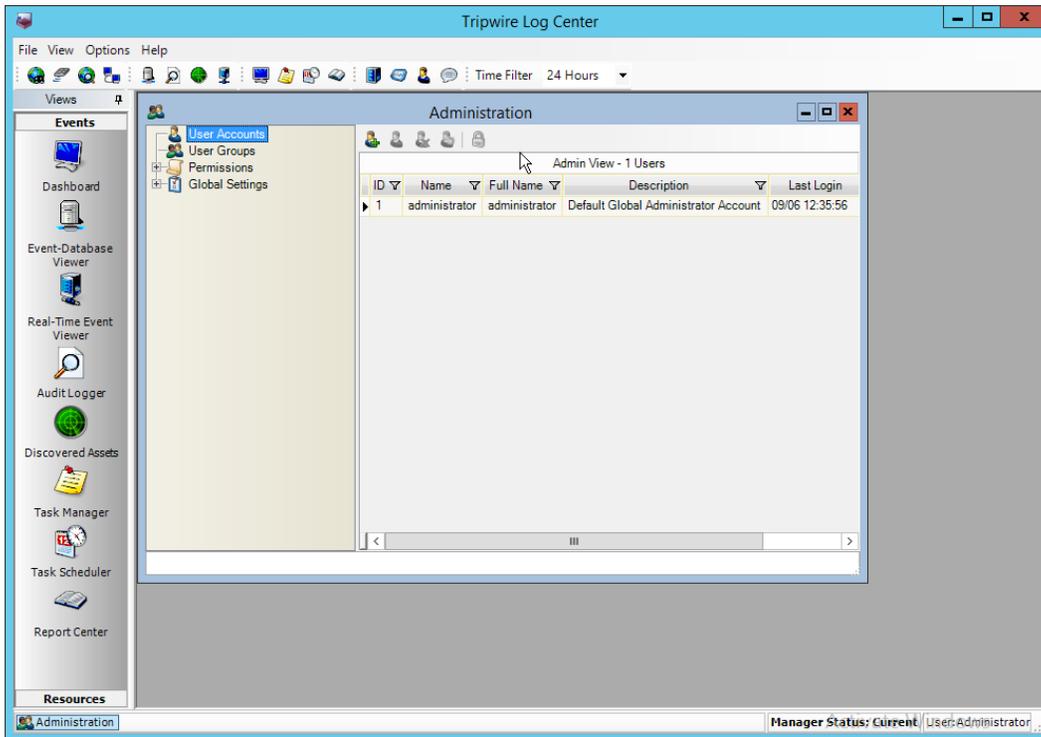
## 2.17 Integration: Tripwire Log Center and Tripwire Enterprise

- 2586
  - 2587
1. Create a user account in **Tripwire Log Center** by logging into **Tripwire Log Center Console**.



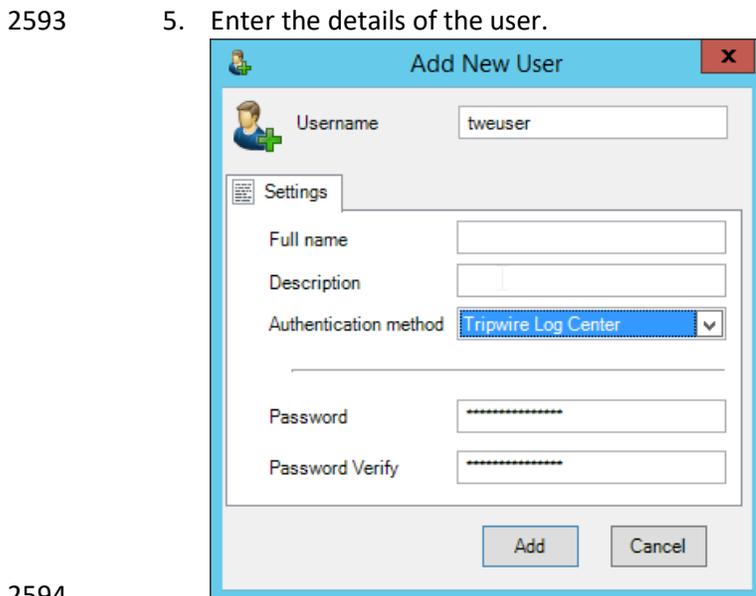
- 2588
  - 2589
2. Click the **Administration Manager** button.

2590 3. Click **User Accounts**.



2591 4. Click the **Add** button.

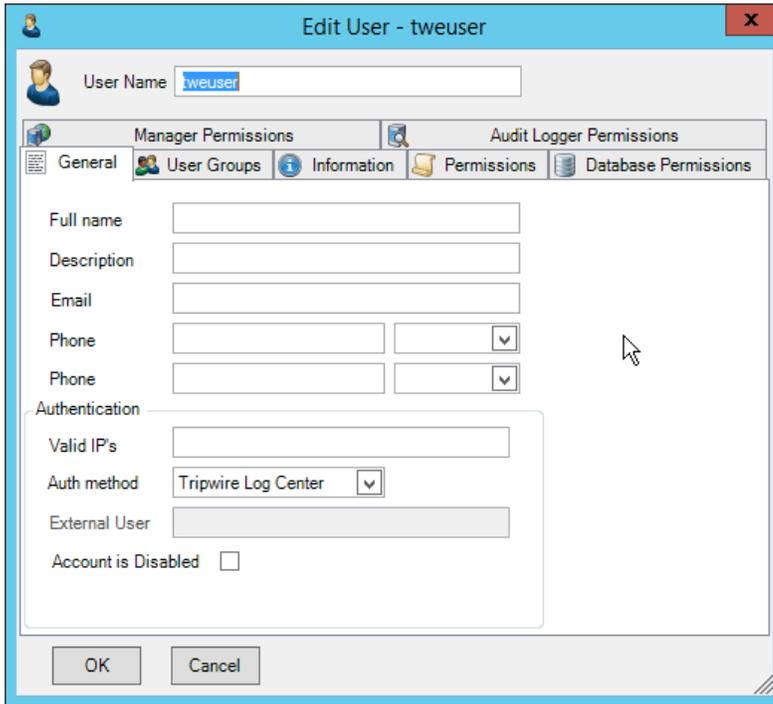
2592 5. Enter the details of the user.



2594 6. Click **Add**.

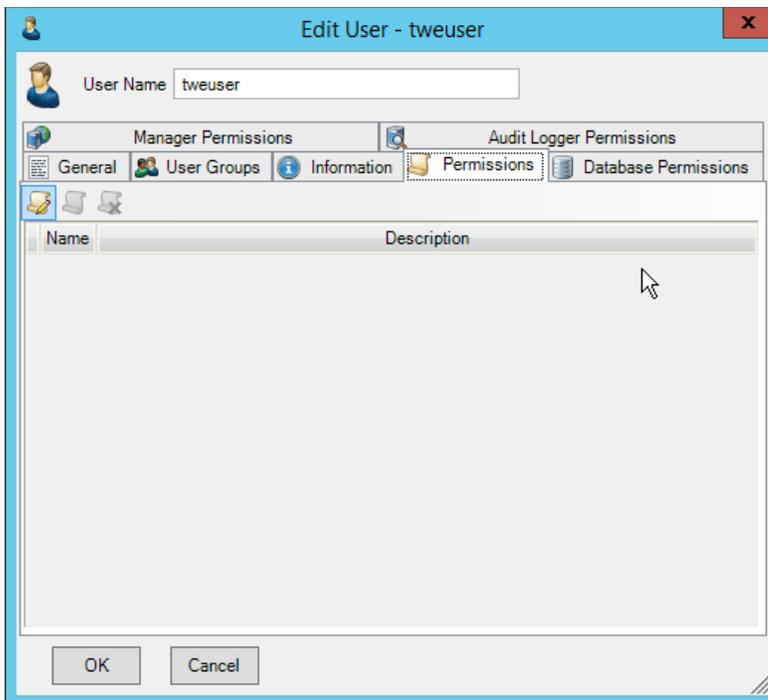
2595 7. Double-click the user account.

2596



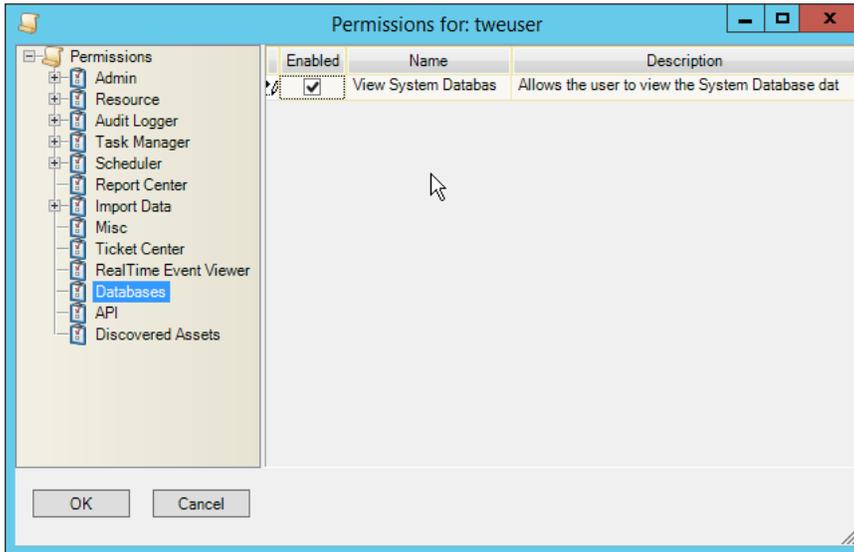
2597  
2598

8. Click the **Permissions** tab.



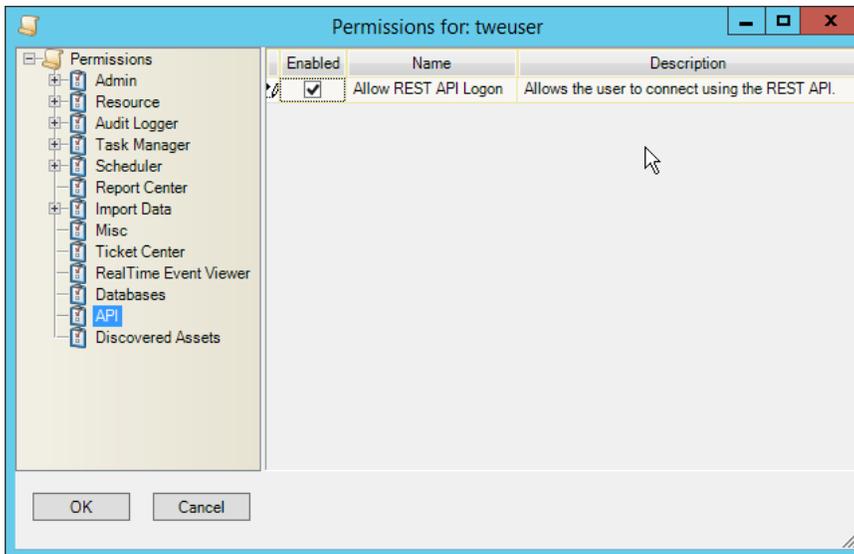
2599  
2600  
2601

9. Click **Edit list of permissions.**
10. Select **Databases.**



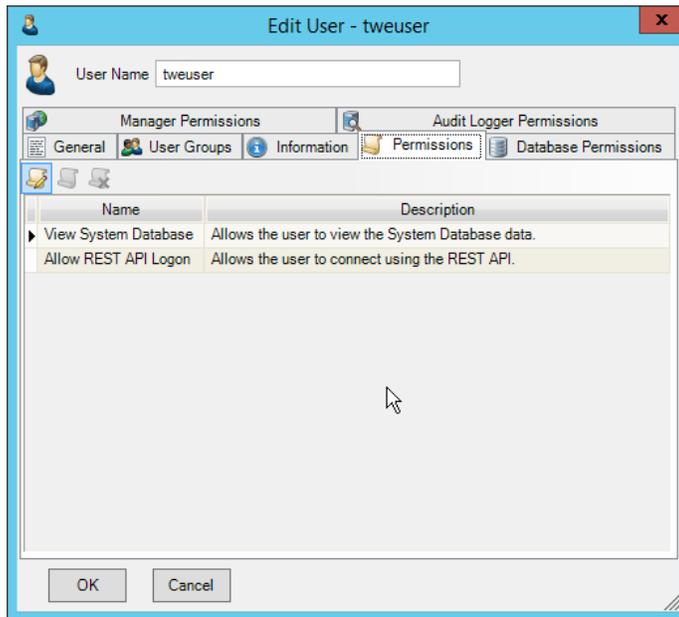
2602  
2603  
2604

- 11. Check the box next to **View System Database**.
- 12. Select **API**.

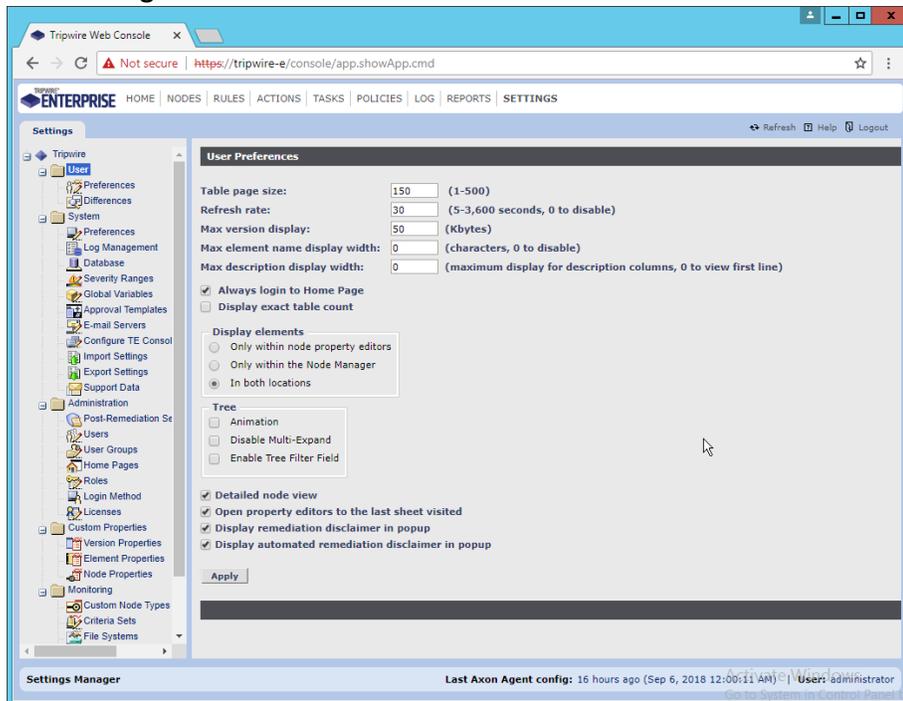


2605  
2606

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

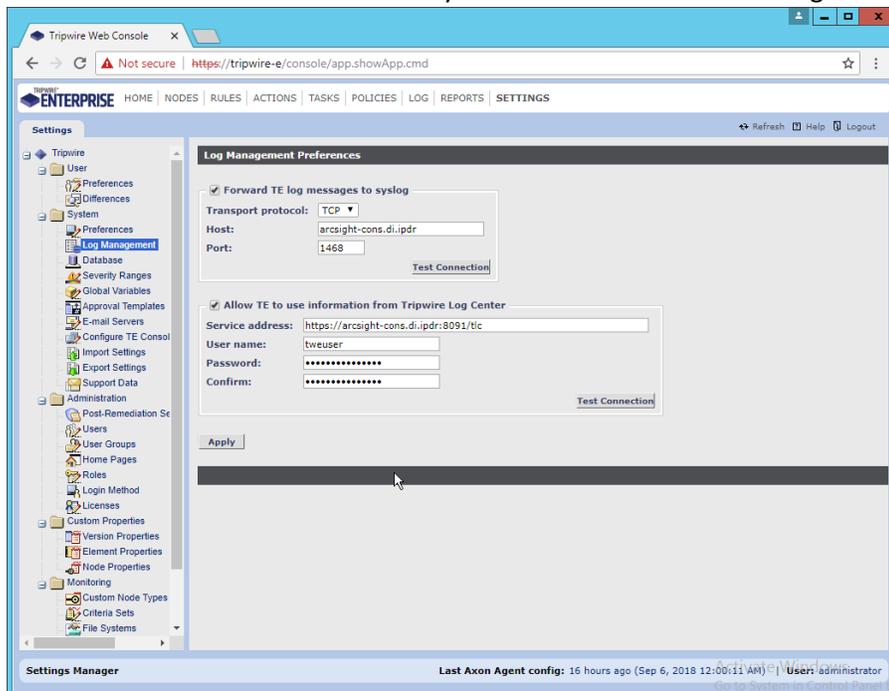


- 2607
  - 2608
  - 2609
  - 2610
  - 2611
14. Click **OK**.
  15. Click **OK**.
  16. Log in to the **Tripwire Enterprise** web console.
  17. Click **Settings**.

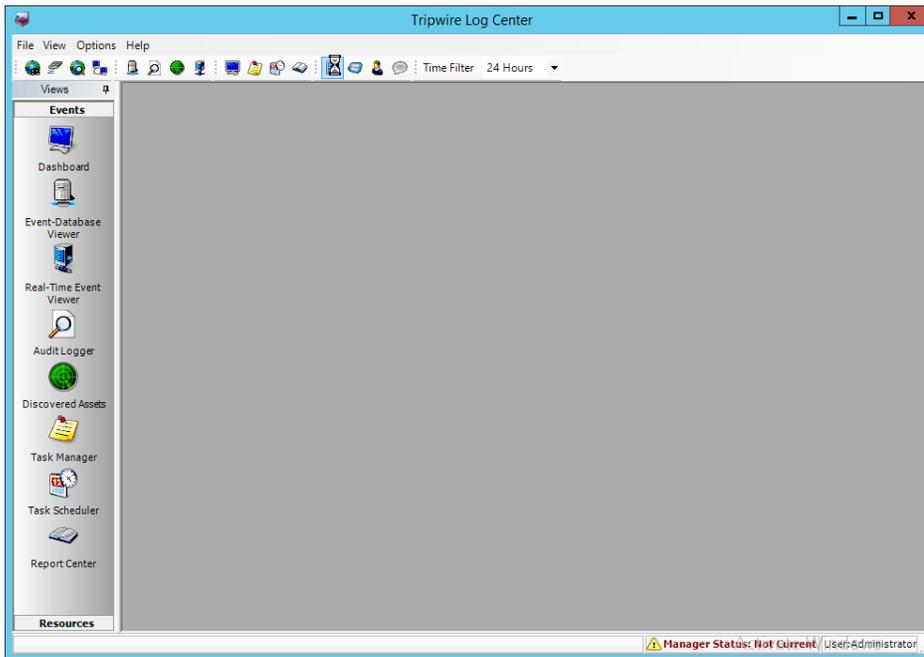


- 2612
  - 2613
18. Go to **System > Log Management**.

- 2614 19. Check the box next to **Forward TE log messages to syslog**.
- 2615 20. Enter the **hostname** and **port** of the **Tripwire Log Center** server. The default port is **1468**.
- 2616 21. Check the box next to **Allow TE to use information from Tripwire Log Center**.
- 2617 22. Enter the **service address** like this: <https://arcsight-cons.di.ipdr:8091/tlc>, replacing the
- 2618 **hostname** with the hostname of your **Tripwire Log Center** server.
- 2619 23. Enter the account information of the account just created for **Tripwire Log Center**.
- 2620 24. You can use **Test Connection** to verify that the connection is working.

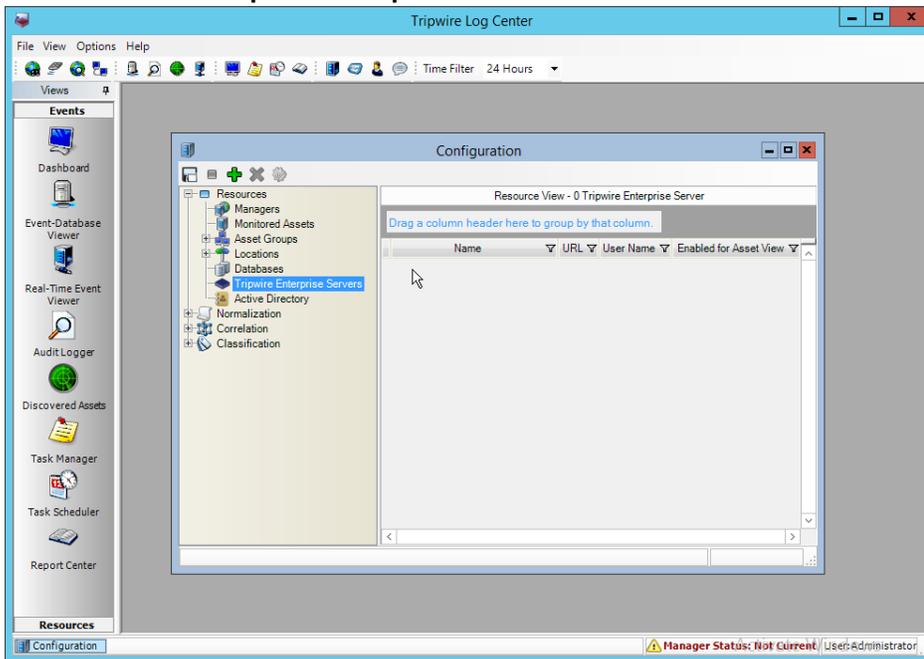


- 2621 25. Click **Apply** when finished.
- 2622 26. Go back to the **Tripwire Log Center Console**.
- 2623



2624  
2625  
2626

- 27. Click **Configuration Manager**.
- 28. Click **Resources > Tripwire Enterprise Servers**.



2627  
2628  
2629  
2630

- 29. Click **Add**.
- 30. Enter a **name** for the server.
- 31. Enter the **URL** of the TE server.

- 2631 32. Enter the **name** of a user account on the TE server. The account must have the following  
 2632 permissions: create, delete, link, load, update, view.

- 2633  
 2634 33. Click **Save**.

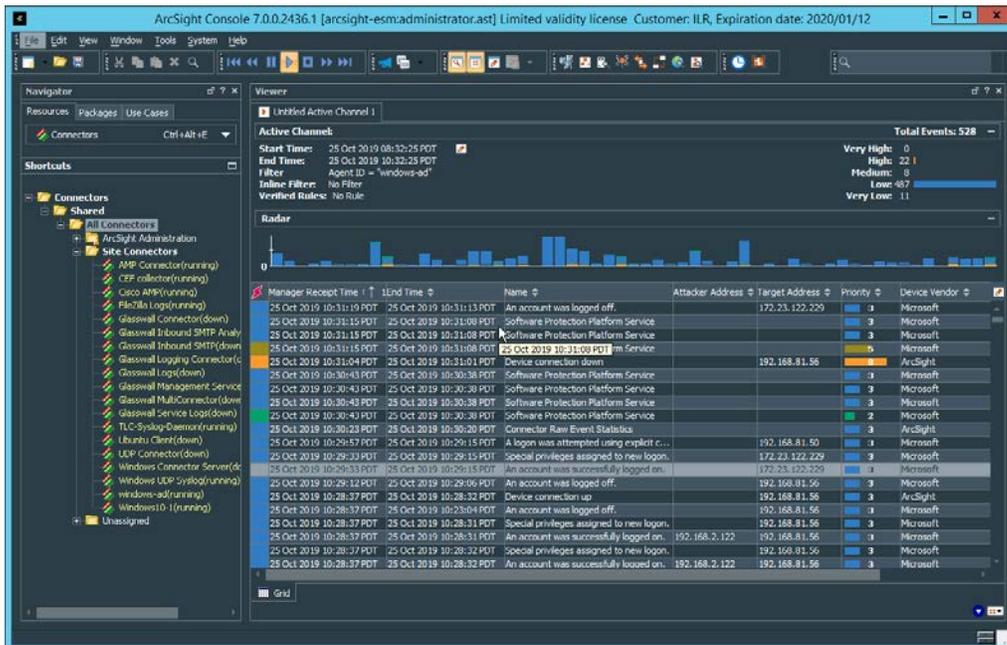
## 2635 2.18 Integration: Symantec ICA and ArcSight ESM

2636 This section describes the integration of Symantec ICA and ArcSight ESM, to import data from ArcSight  
 2637 into ICA for analysis. For the purposes of this build, we did not use ArcSight Logger, a tool which  
 2638 provides a web API for other applications. Because of this, the standard integration between ICA and  
 2639 ESM was unavailable. However, it is still possible to import CSV files exported from ArcSight into ICA,  
 2640 and we will detail the process below. There are a few things to note when doing this import:

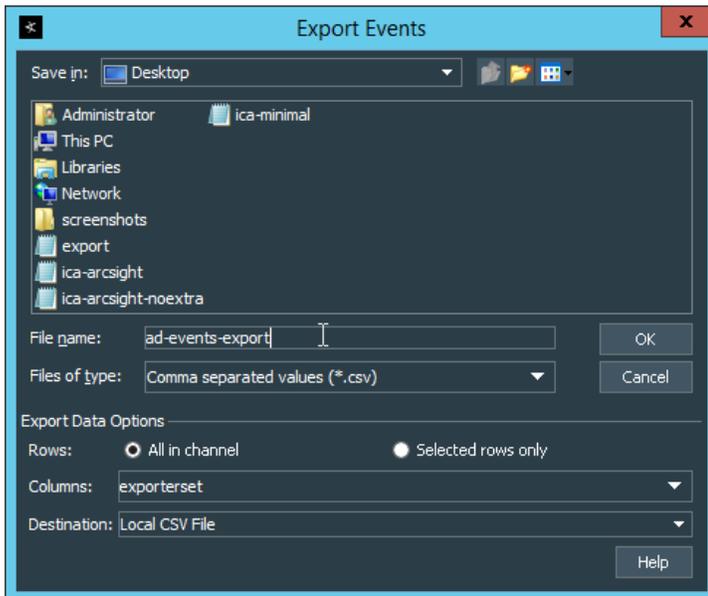
- 2641 • On the version of Symantec ICA we are using, it is required to replace empty fields in the CSV  
 2642 with NULL. This may be unnecessary in future updates.
- 2643 • The CSV file should be in a location accessible to the ICA server. You can replace this file with a  
 2644 new CSV file on a daily basis, and Symantec ICA has the capability to import the new data.
- 2645 • The following integration details how to do it for a subset of fields on Active Directory logging  
 2646 events, but the process can be expanded for your organization's needs.

### 2647 2.18.1 Export the CSV File from ArcSight Console

- 2648 1. In ArcSight Console, find a connector which you wish to import events from. Right-click it, and  
 2649 select **Create Channel with Filter**.
- 2650 2. In the channel, apply any filters desired.



- 2651
  - 2652
  - 2653
  - 2654
  - 2655
  - 2656
  - 2657
3. When finished, right-click any of the events in the channel, and select **Export > Events in Channel...**
  4. Enter a name for the CSV file for **File name:**.
  5. Select **All in Channel** for **Rows:**.
  6. For **Columns:** either select a custom field-set to determine the output columns or leave the default selected.

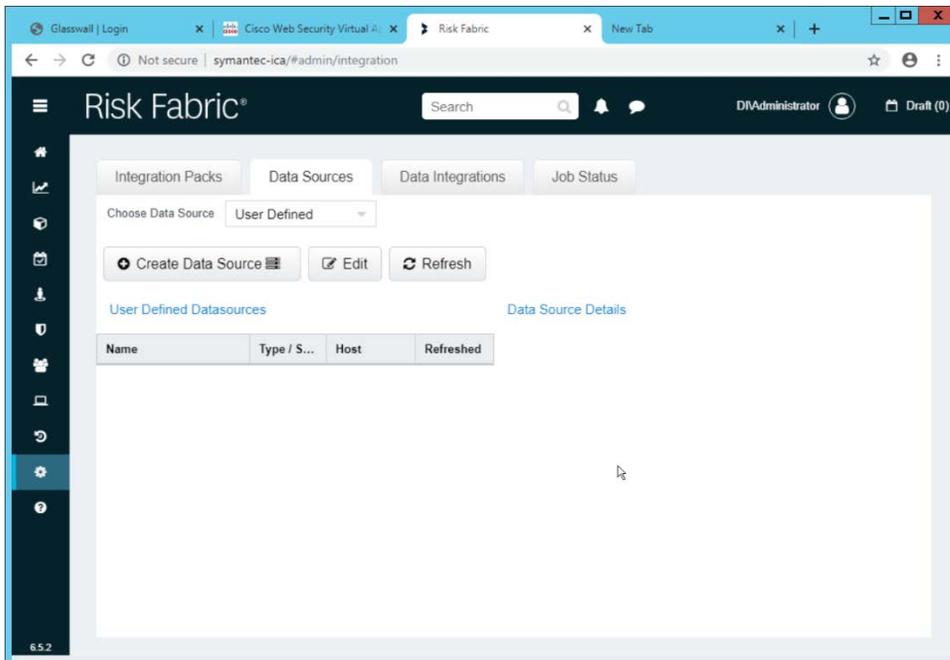


- 2658
  - 2659
7. Click **OK**.

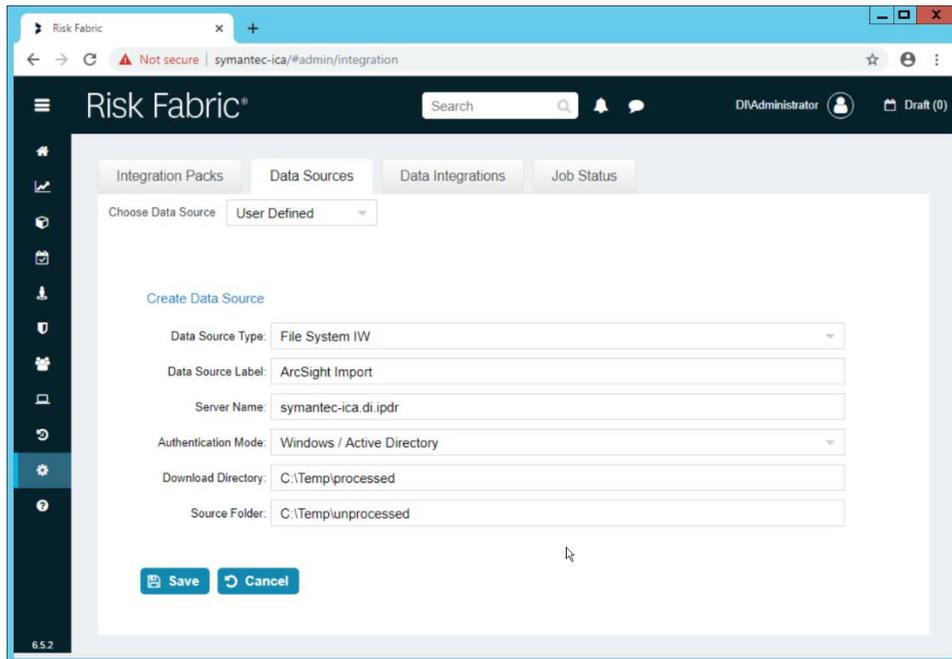
- 2660 8. Move the file to the desired location for ICA to collect. (Ensure that if required for your version  
 2661 of Symantec ICA, all empty fields are replaced with "NULL") For the purposes of this  
 2662 demonstration, we moved it to *C:\Temp\unprocessed* on the Symantec ICA server.

## 2663 2.18.2 Import the CSV File to Symantec ICA

- 2664 1. On the Symantec ICA web console, navigate to **Gear Icon > Integration**.  
 2665 2. Click the **Data Sources** tab.

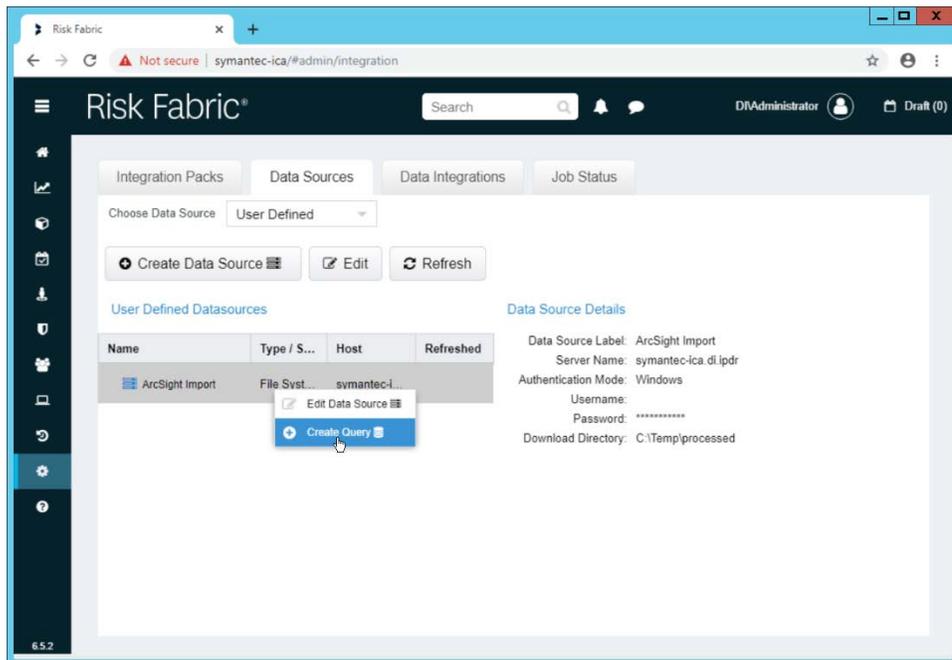


- 2666 3. Select **User Defined** for **Choose Data Source**.  
 2667 4. Click **Create Data Source**.  
 2668 5. Select **File System IW** for the **Data Source Type**.  
 2669 6. Enter a name for the data source for **Data Source Label**.  
 2670 7. Enter the hostname of the Symantec ICA server for **Server Name**.  
 2671 8. Select **Windows/Active Directory** for the **Authentication Mode**.  
 2672 9. Enter the location for the downloaded CSV file for **Download Directory** (relative to the  
 2673 Symantec ICA server).  
 2674 10. Enter the location for the CSV file to be downloaded from for **Source Folder** (relative to the  
 2675 Symantec ICA server).  
 2676



2677  
2678

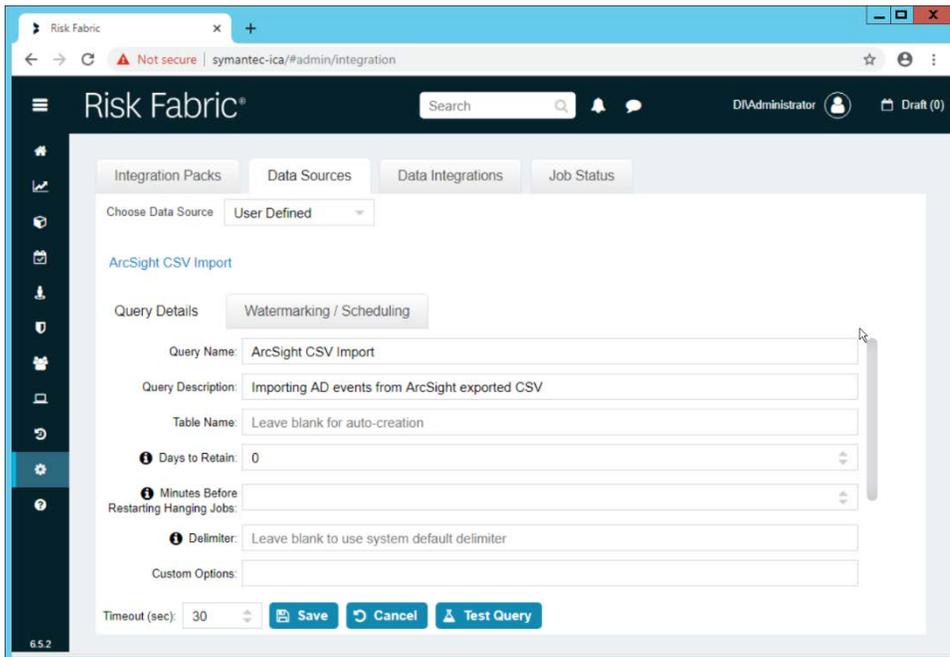
11. Click **Save**.



2679  
2680  
2681

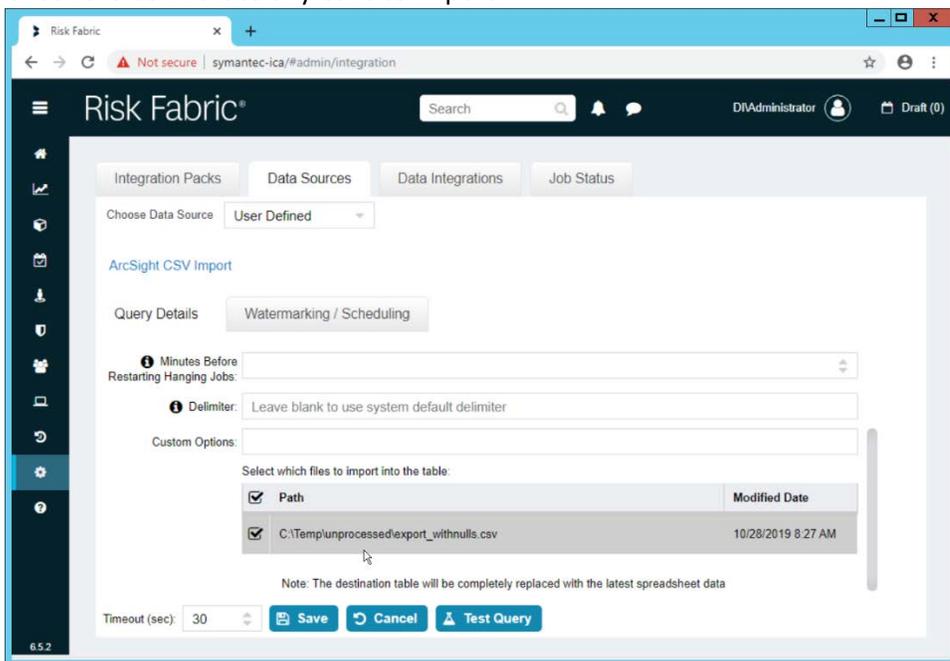
12. Right-click the newly created data source and select **Create Query**.

13. Enter a **Query Name** and **Query Description**.



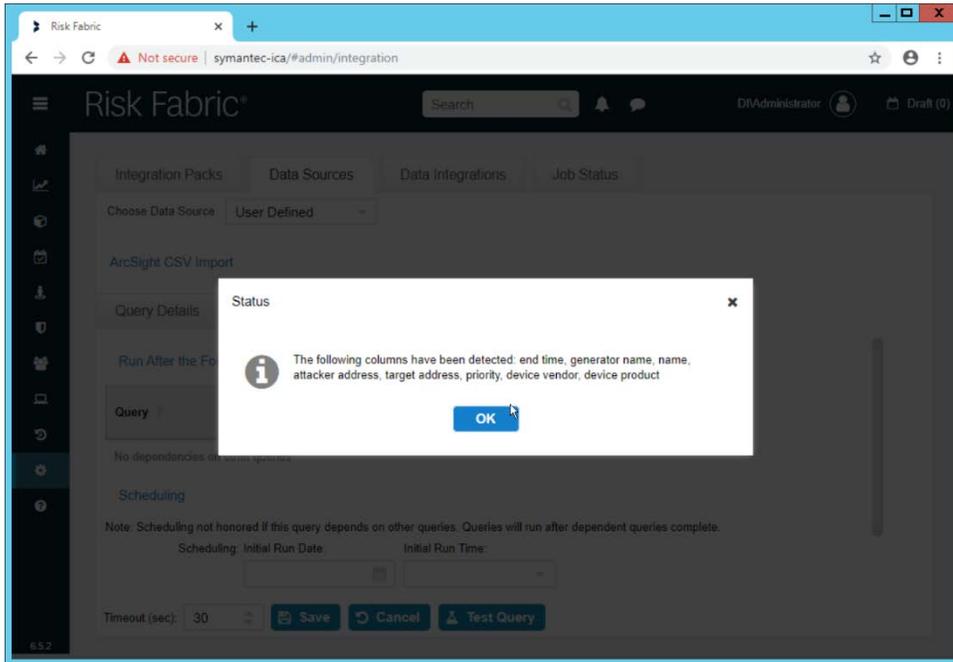
2682  
2683  
2684

- 14. If you specified the **Source Folder** correctly, you will see the CSV file listed.
- 15. Check the box next to any CSVs to import.



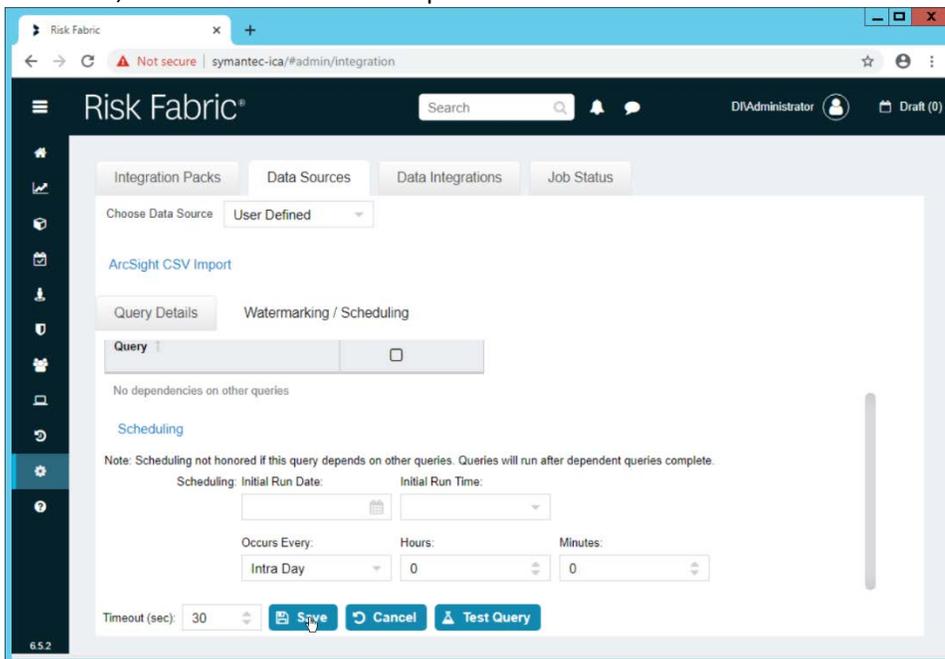
2685  
2686

- 16. Click **Save**.



2687  
2688  
2689

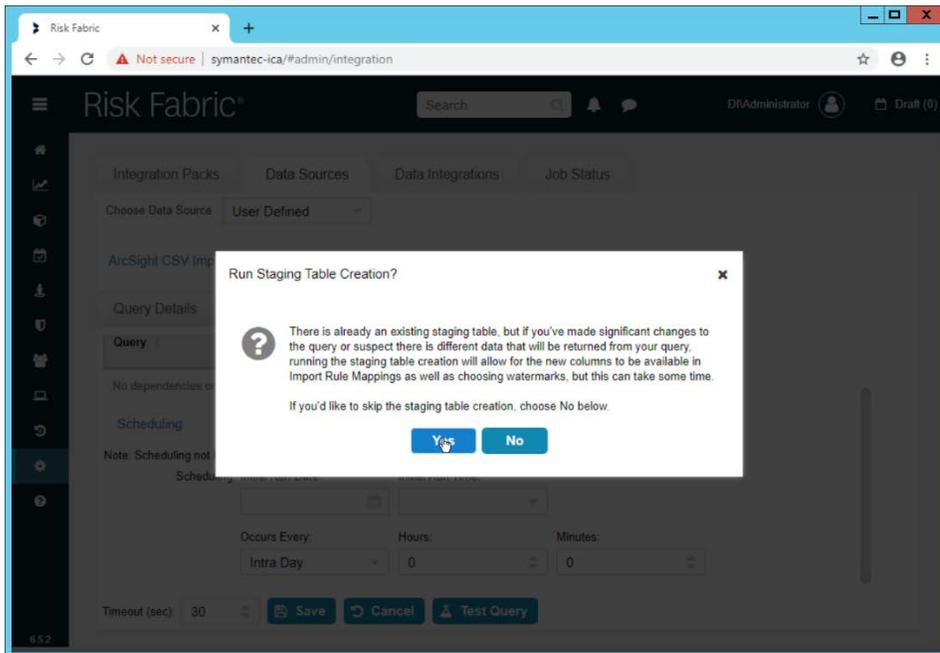
- 17. Click **OK**.
- 18. If desired, set a schedule for this import.



2690  
2691

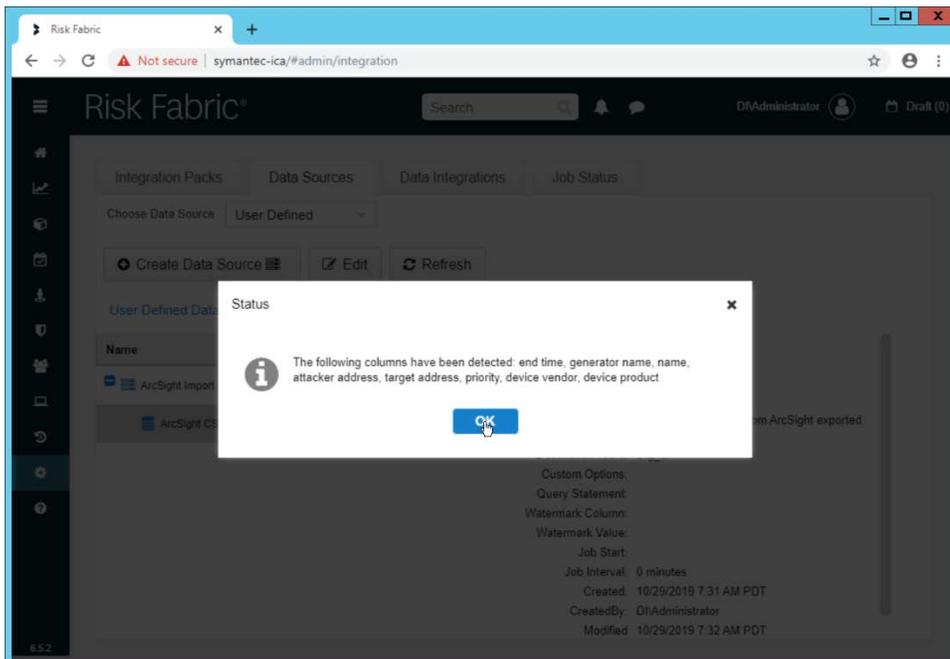
- 19. Click **Save**.

2692  
2693



20. Click **Yes**.

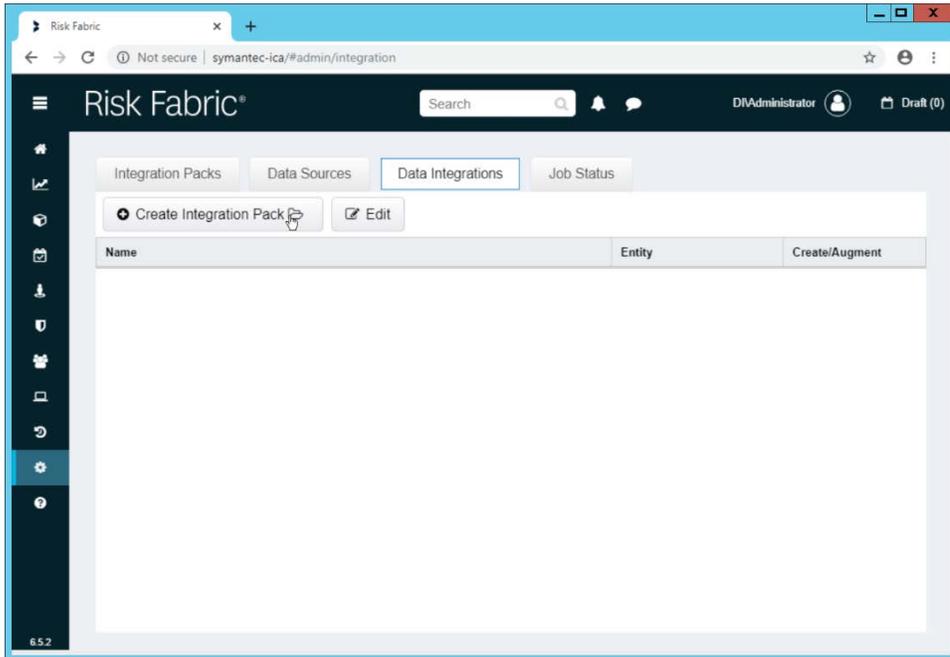
2694  
2695



21. Click **OK**.

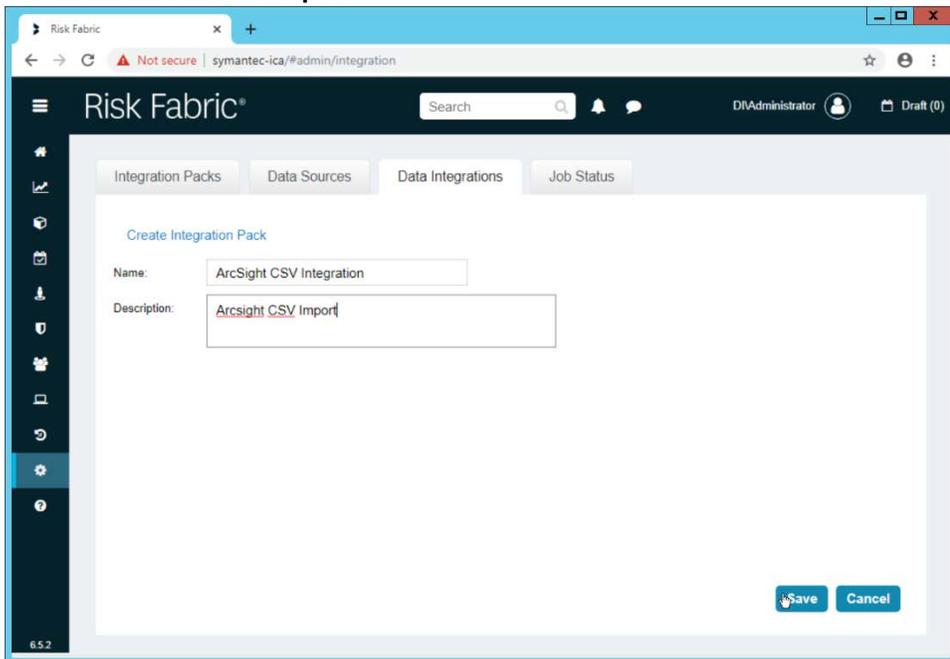
### 2696 2.18.3 Create a Mapping between ArcSight events and Symantec ICA

2697 1. Navigate to the **Data Integrations** tab.



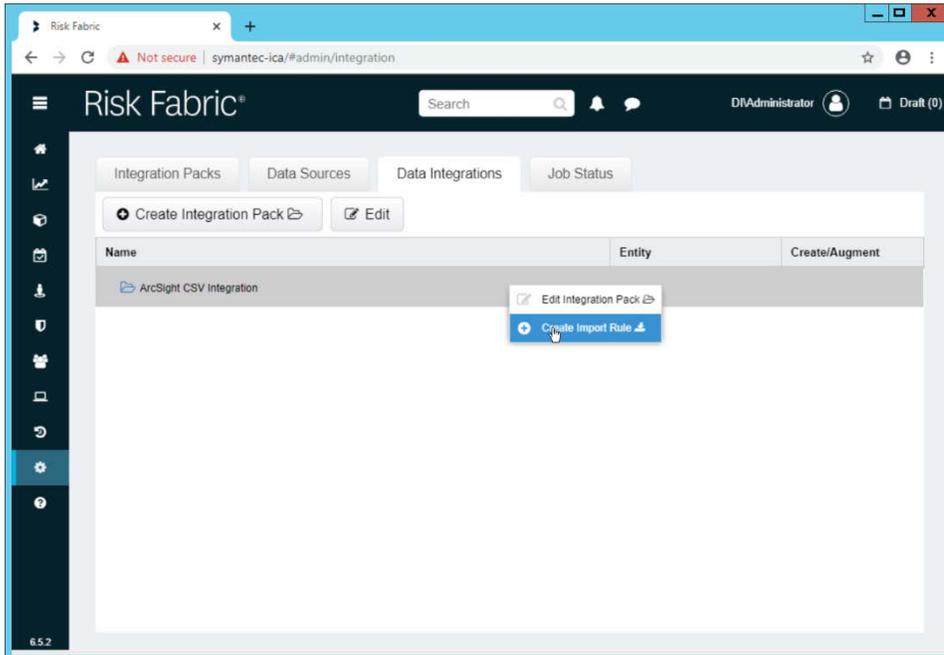
2698  
2699  
2700

2. Click **Create Integration Pack**.
3. Enter a **Name** and **Description**.



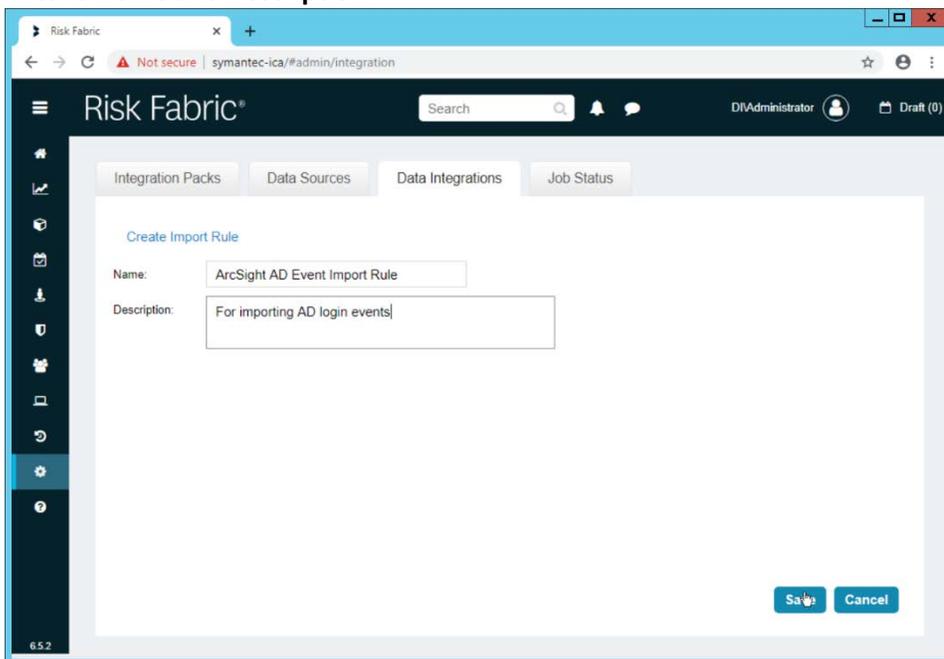
2701  
2702

4. Click **Save**.



2703  
2704  
2705

5. Right-click the newly created Integration Pack, and select **Create Import Rule**.
6. Enter a **Name** and **Description**.



2706  
2707  
2708  
2709

7. Click **Save**.
8. Right-click the newly created **Import Rule** and select **Create Import Rule Mapping**.
9. Enter a **Name** for the mapping.

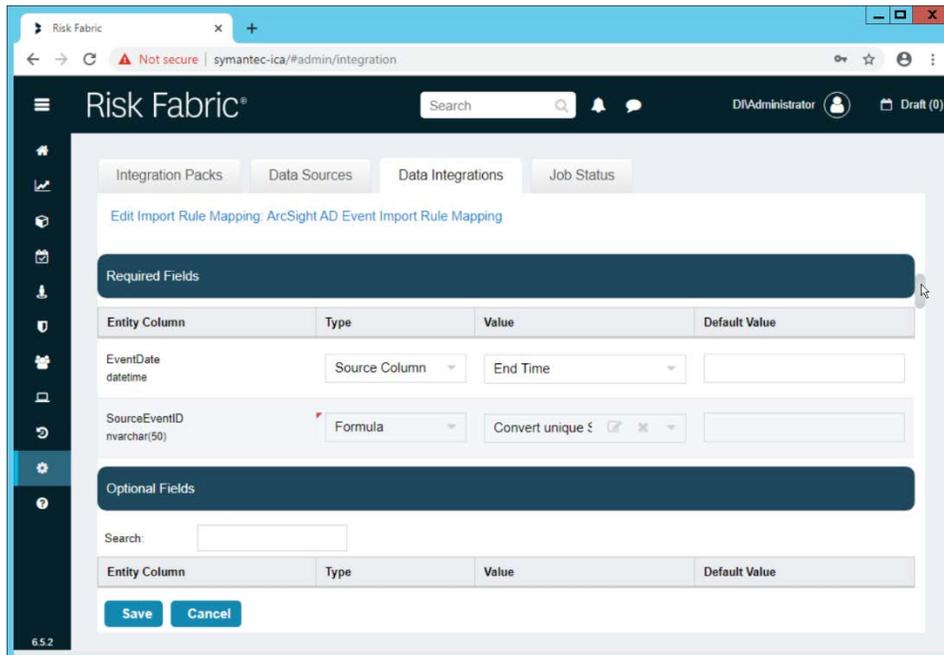
- 2710 10. Enter a **Description**.
- 2711 11. Select the **Data Source** created earlier.
- 2712 12. Select the **Query** created earlier.
- 2713 13. Select **EP Events** for the **Entity Type** (or explore other Entity Types that may better match the
- 2714 events you are importing).

The screenshot shows the Risk Fabric web interface. The browser address bar indicates the URL is symantec-ica/#admin/integration. The page title is 'Risk Fabric'. The user is logged in as 'DIAdministrator'. The main content area is titled 'Edit Import Rule Mapping: ArcSight AD Event Import Rule Mapping'. The form contains the following fields:

- Mapping Name: ArcSight AD Event Import Rule Mapping
- Description: AD events
- Data Source: ArcSight Import
- Query: ArcSight CSV Import
- Risk Fabric Processing Watermark: 528
- Run Intra-Day: No
- Run Order: 0
- Entity Type: EP Events
- Update Pre-Process Table: Yes
- Create Entities: Yes

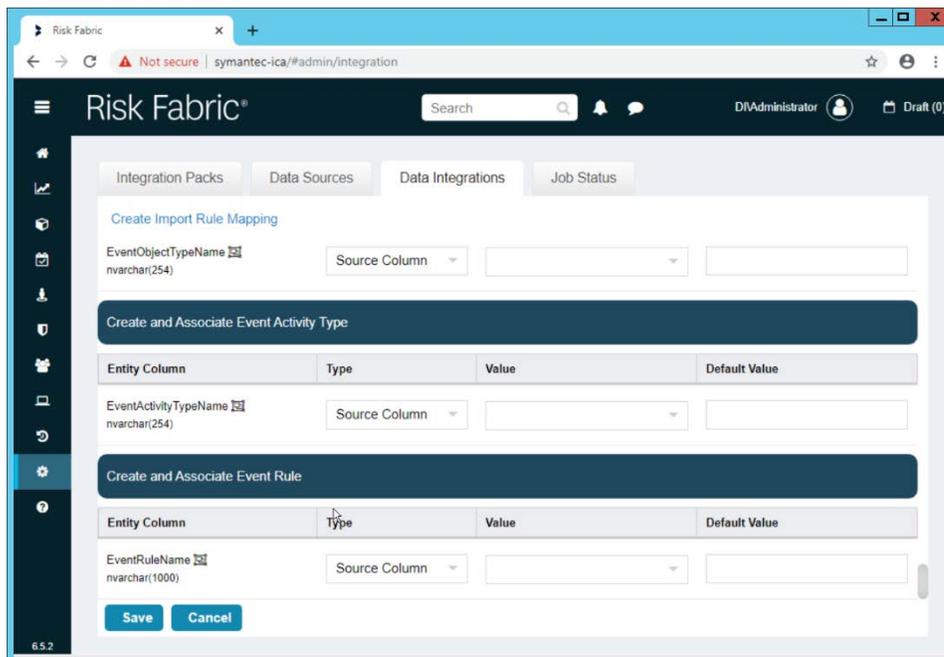
At the bottom of the form are 'Save' and 'Cancel' buttons. The version number '6.5.2' is visible in the bottom left corner of the interface.

- 2715 14. Below, the **Entity Column** refers to the target field in ICA to which a field is being mapped. Map
- 2716 event fields from the CSV to fields in the Entity Column.
- 2717
- 2718 15. For example, **EventDate** in ICA corresponds directly to the **End Time** in ArcSight, so we select
- 2719 that value directly as a **Source Column** for the mapping.



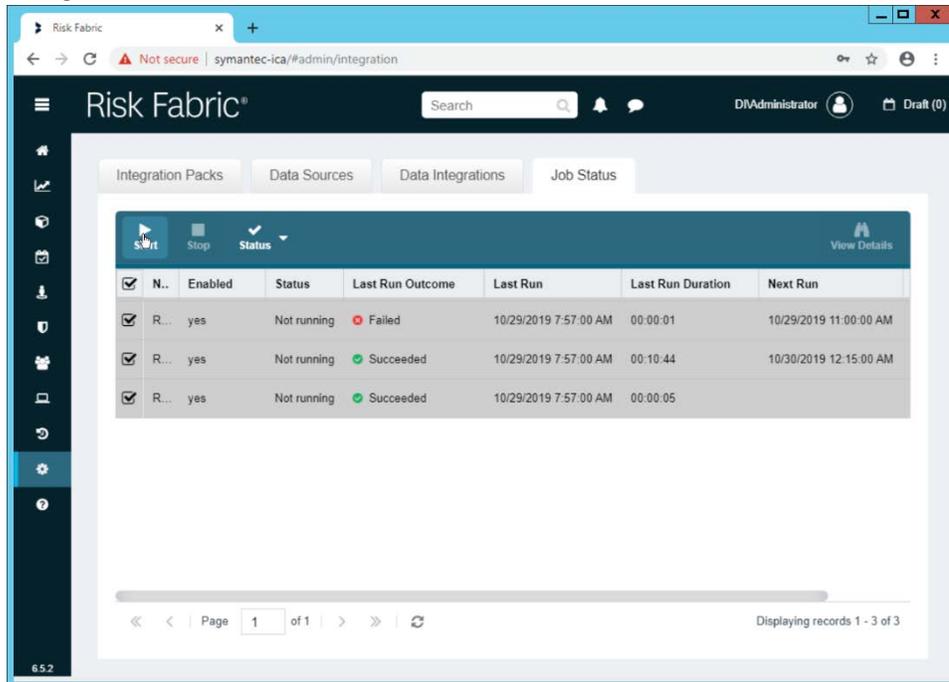
2720  
2721  
2722  
2723  
2724  
2725

16. **Formulas** can be used to transform columns in the CSV to something more specific in ICA. Because we did not export an event ID to our CSV file, we use a formula to create a hash of the **End Time** and use that as the ID.
17. All **Required Fields** must be mapped, and you will likely also want to map some optional fields to make useful data.



2726

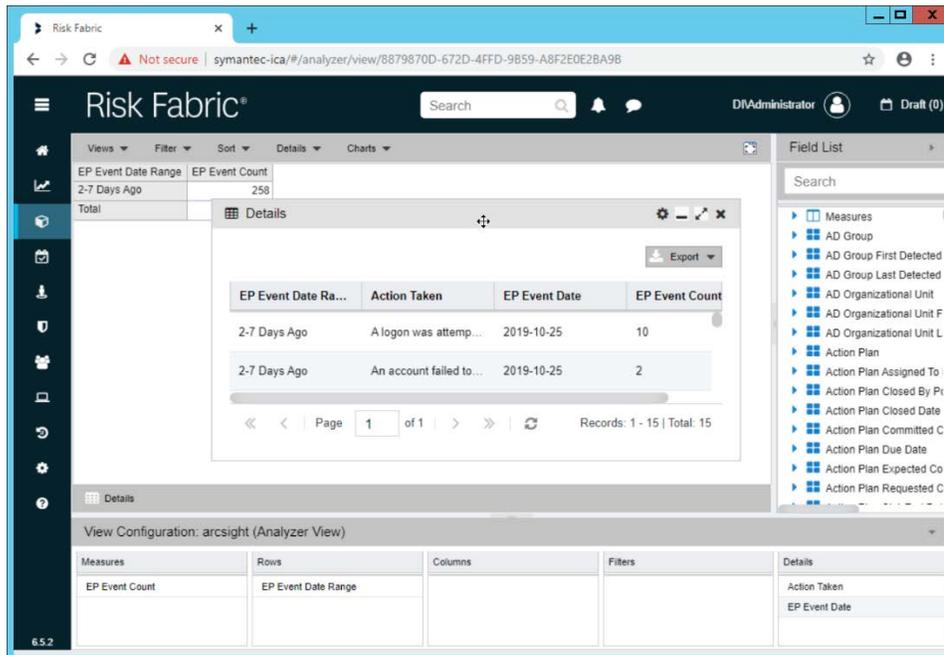
- 2727 18. Click **Save** when finished.  
 2728 19. Navigate to the **Job Status** tab.



- 2729 20. Select all the jobs and click **Start**. This is to force a refresh of the ICA processing, allowing the  
 2730 data from the CSV to be imported immediately.  
 2731

#### 2732 2.18.4 View ArcSight Events in the Analyzer

- 2733 1. Once the processing jobs are finished, navigate to the **Analyzer**.



2734  
2735  
2736

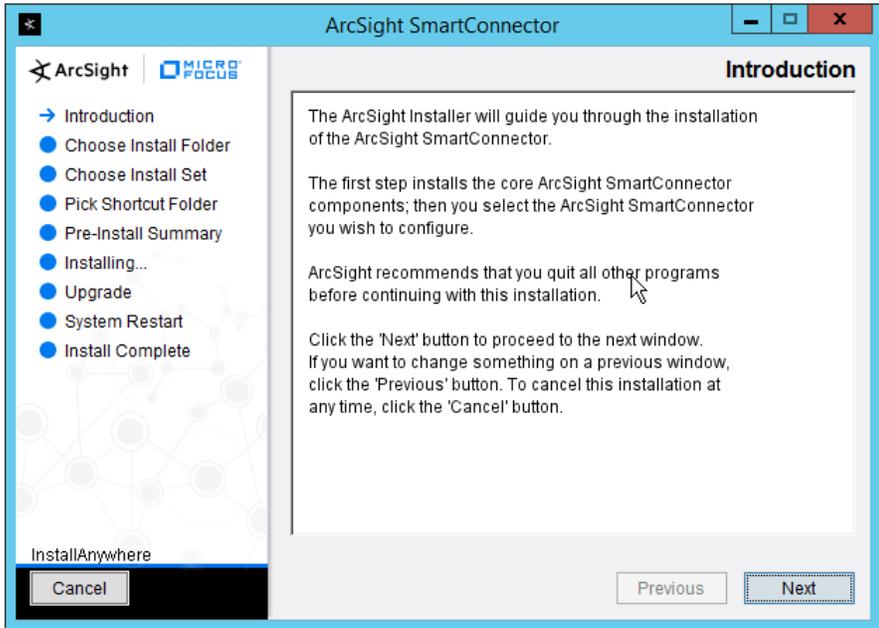
2. Drag mapped columns (from the import rule mapping you created) from the list on the right to view them in the analyzer.

## 2737 2.19 Integration: Micro Focus ArcSight and Tripwire

2738 This section will detail the forwarding of logs from **Tripwire Log Center** to **Micro Focus ArcSight**. This  
2739 will forward **Tripwire IP360** and **Tripwire Enterprise** logs to **ArcSight**, assuming those logs are being  
2740 collected by **Tripwire Log Center**.

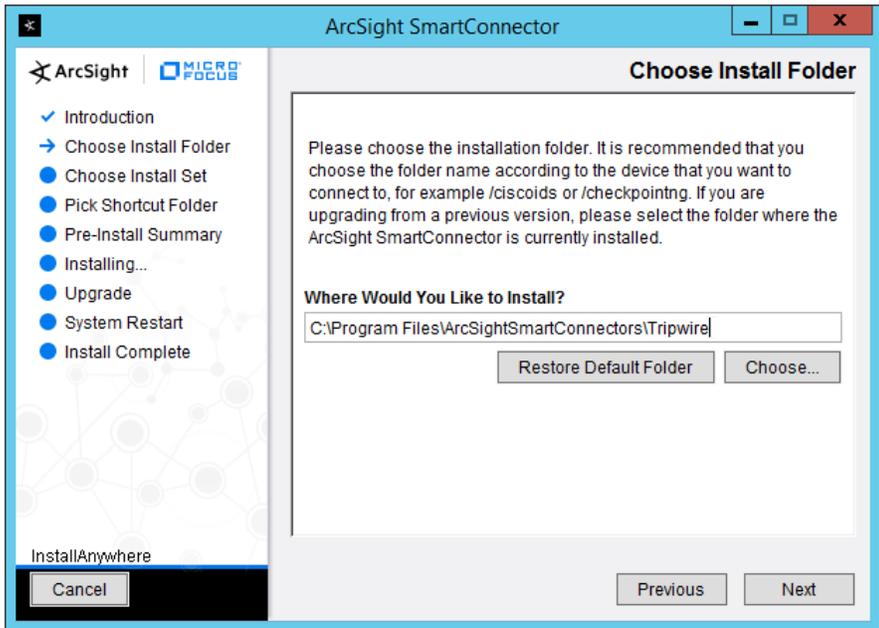
### 2741 2.19.1 Install Micro Focus ArcSight

- 2742 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running  
2743 **Tripwire Log Center**.



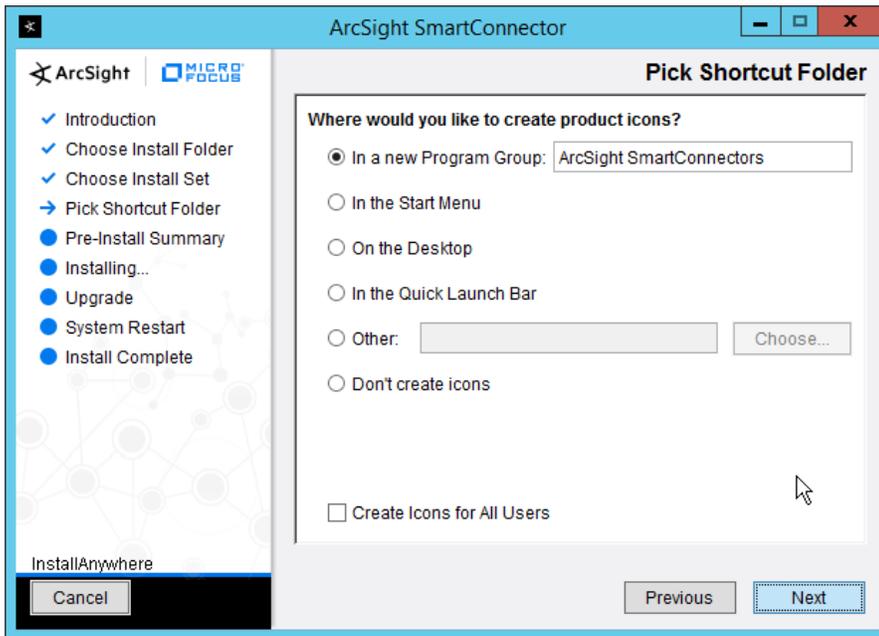
2744  
2745

2. Click **Next**.



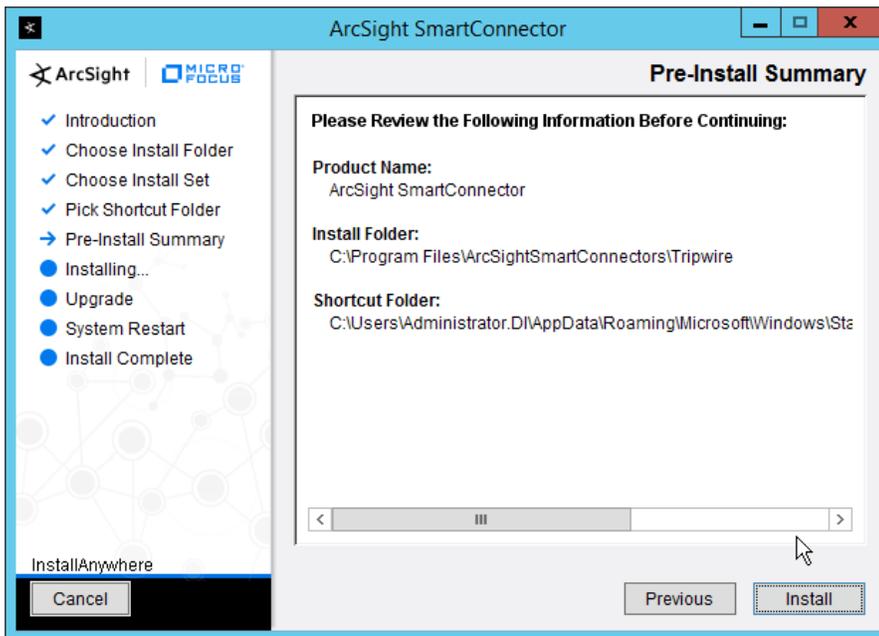
2746  
2747

3. Enter *C:\Program Files\ArcSightSmartConnectors\Tripwire*.



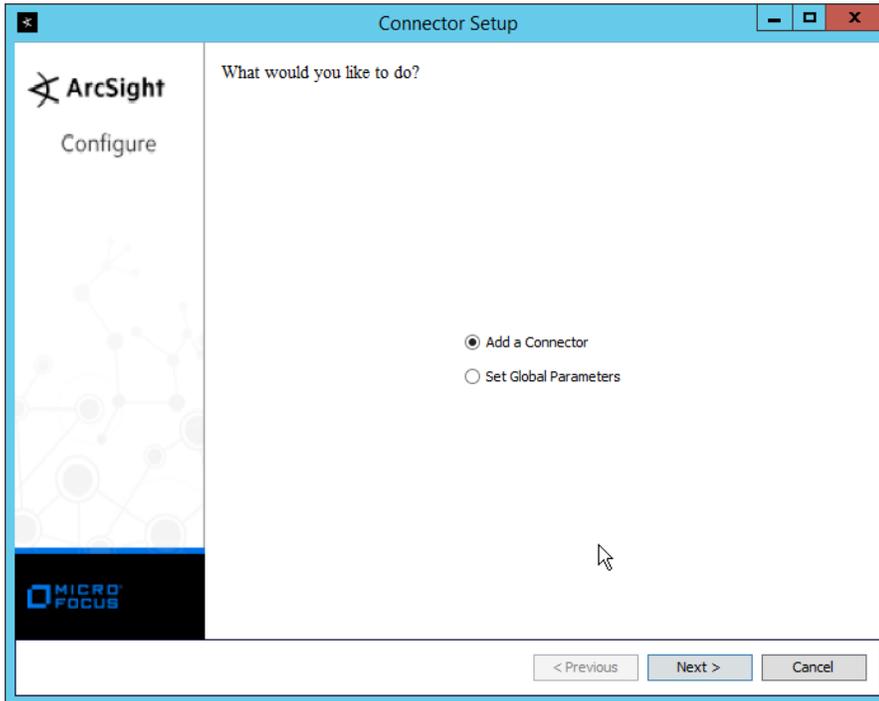
2748  
2749

4. Click **Next**.



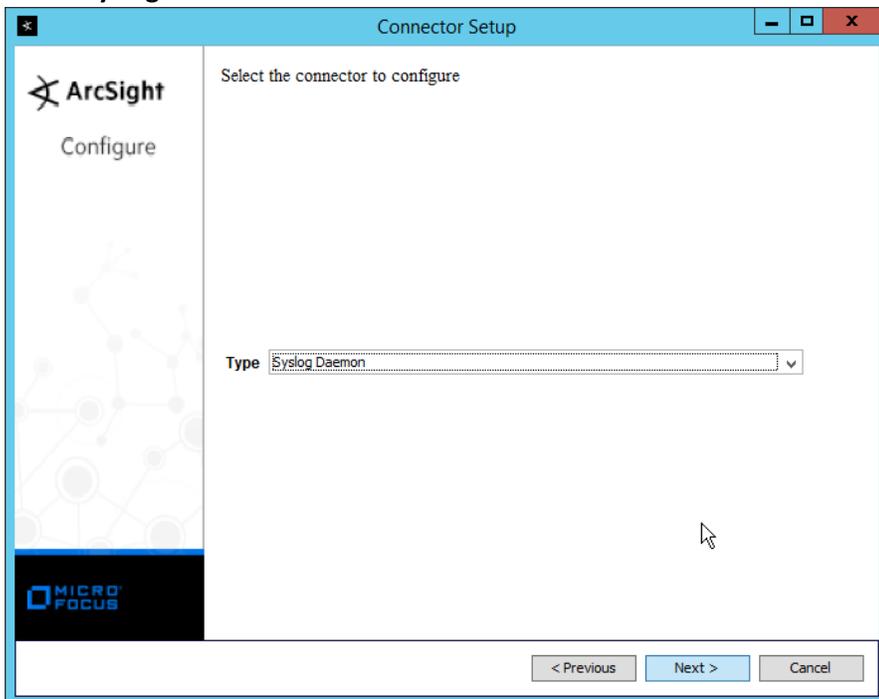
2750  
2751  
2752

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



2753  
2754  
2755

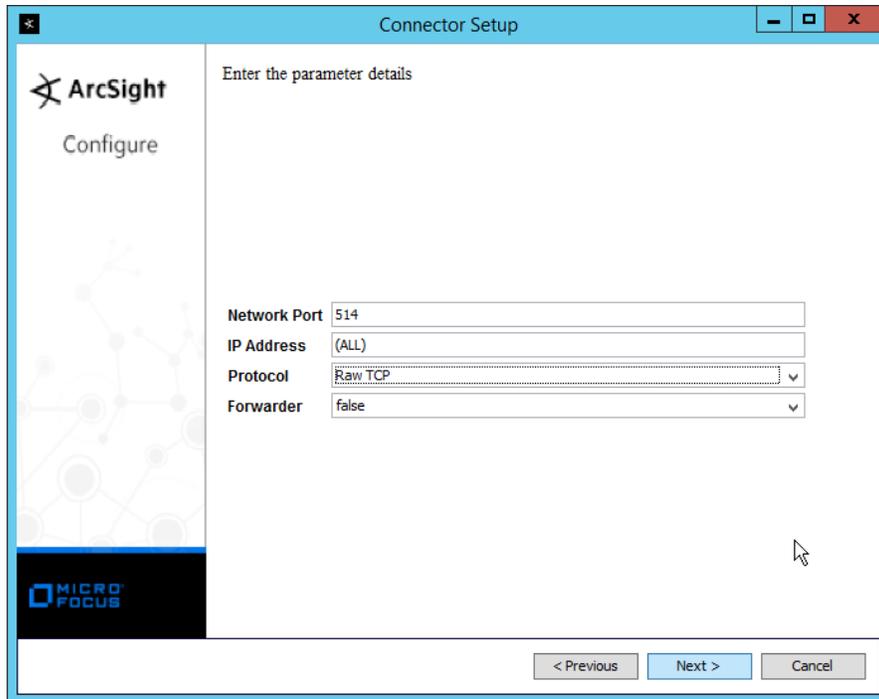
7. Click **Next**.
8. Select **Syslog Daemon**.



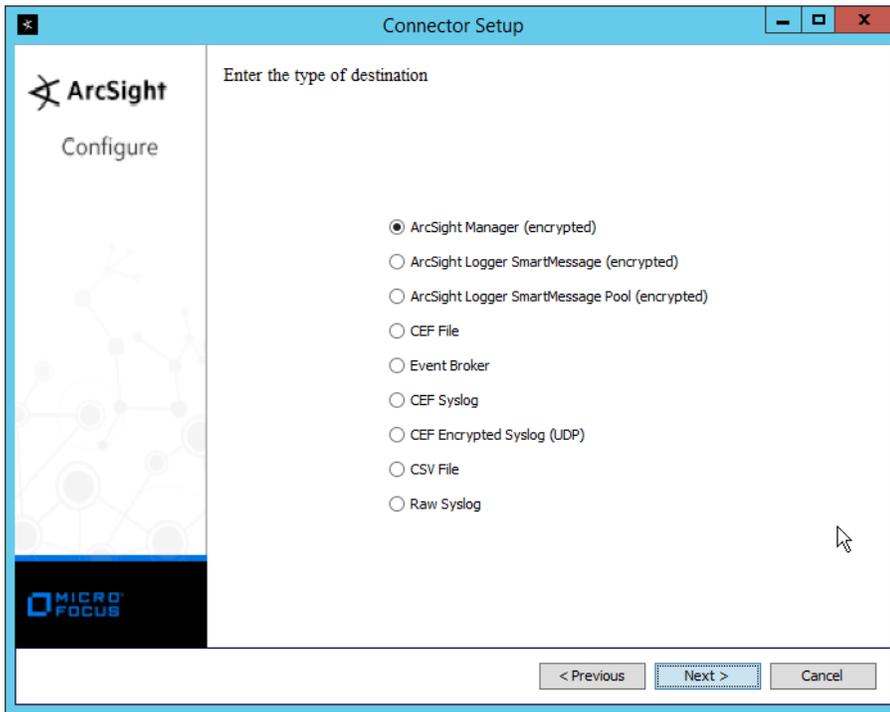
2756  
2757

9. Click **Next**.

- 2758 10. Enter a port for the daemon to run on.
- 2759 11. Select **Raw TCP** for **Protocol**.

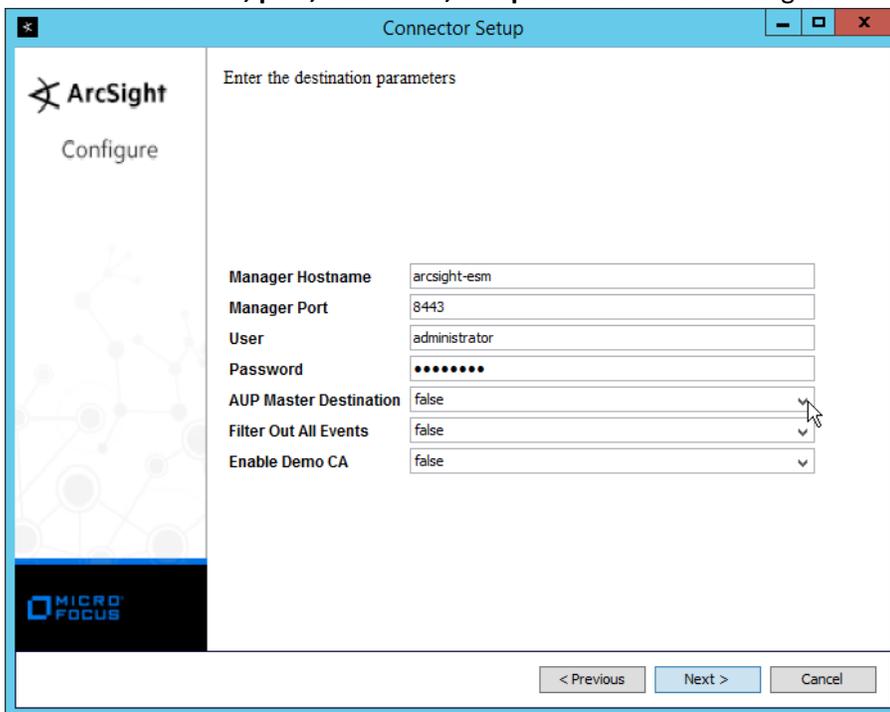


- 2760 12. Click **Next**.
- 2761
- 2762 13. Select **ArcSight Manager (encrypted)**.



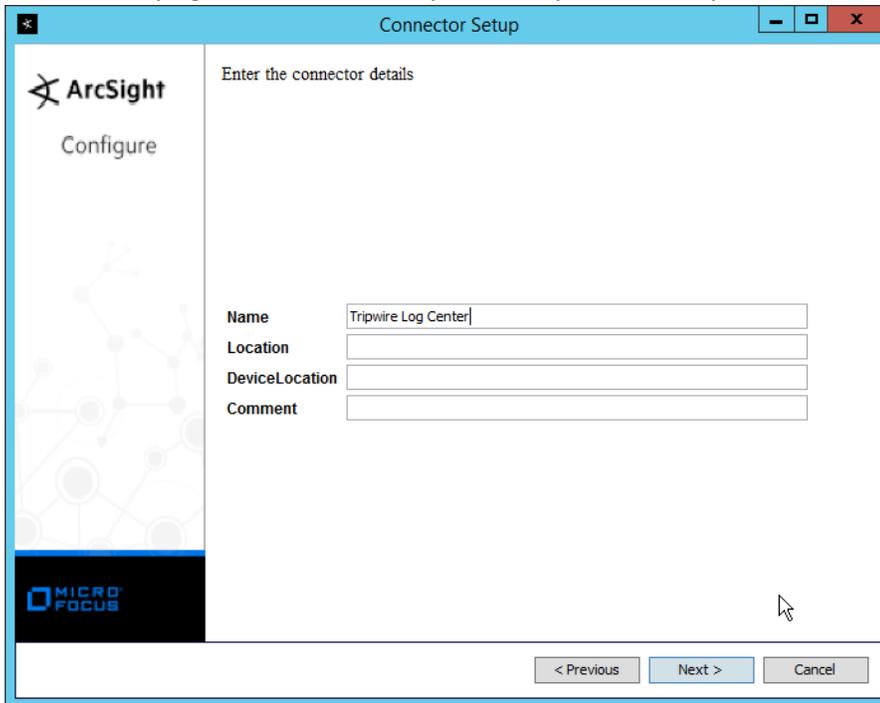
2763  
2764  
2765

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

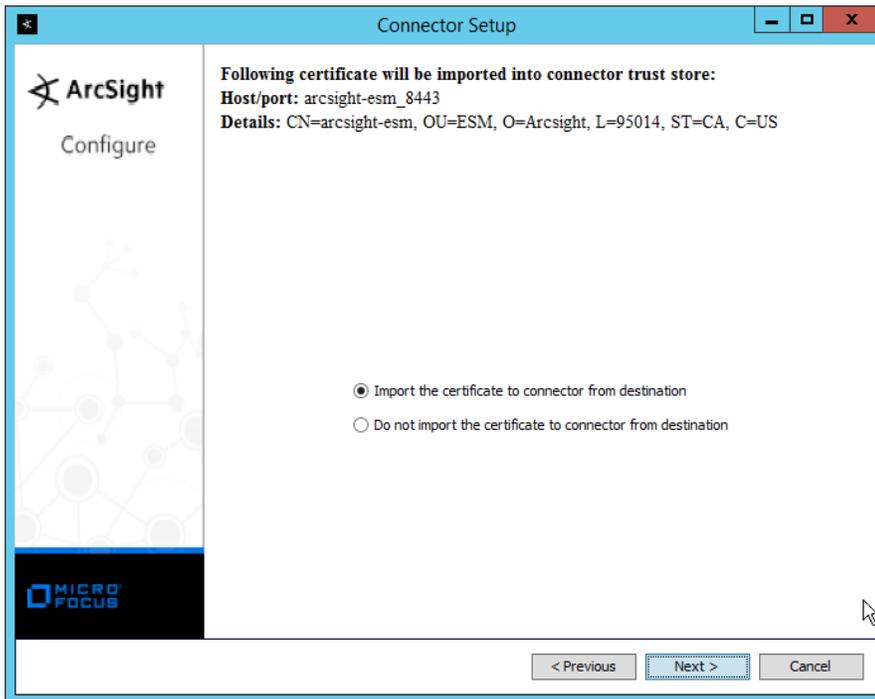


2766

- 2767 16. Click **Next**.
- 2768 17. Enter identifying details about the system (only **Name** is required).

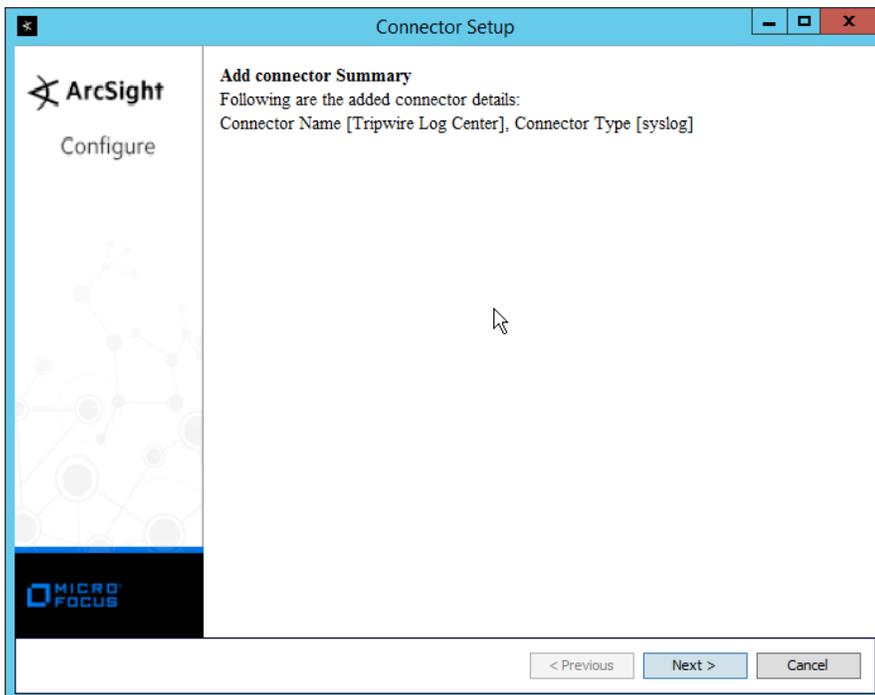


- 2769 18. Click **Next**.
- 2770 19. Select **Import the certificate to connector from destination**.
- 2771



2772  
2773

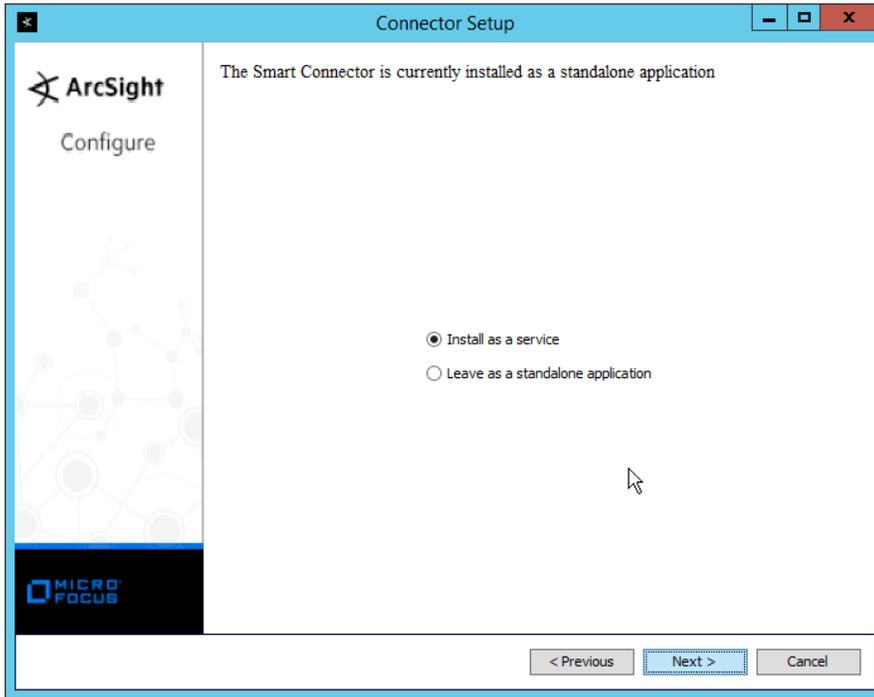
20. Click **Next**.



2774  
2775  
2776

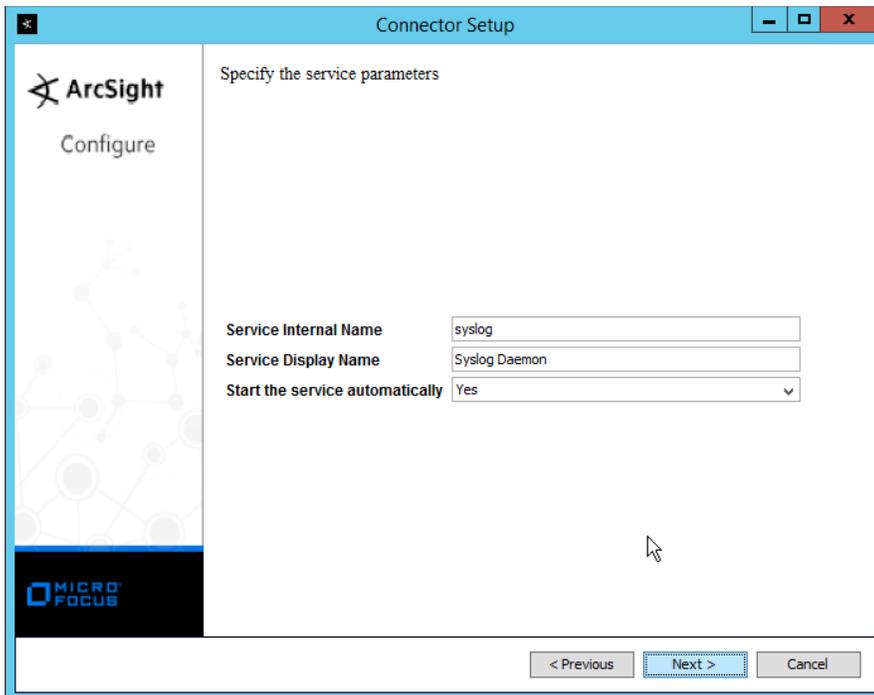
21. Click **Next**.

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



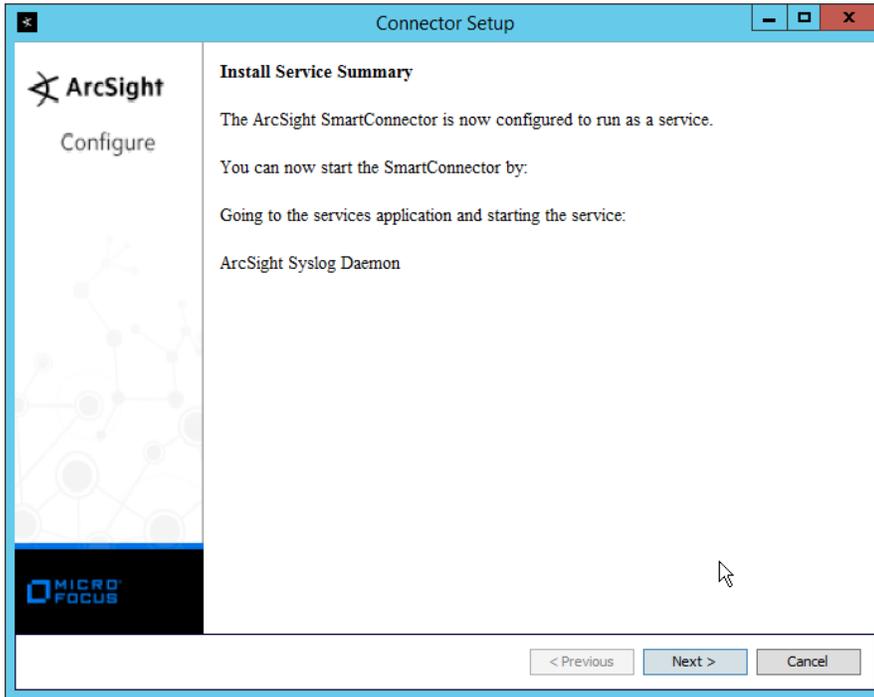
2777  
2778

23. Click **Next**.



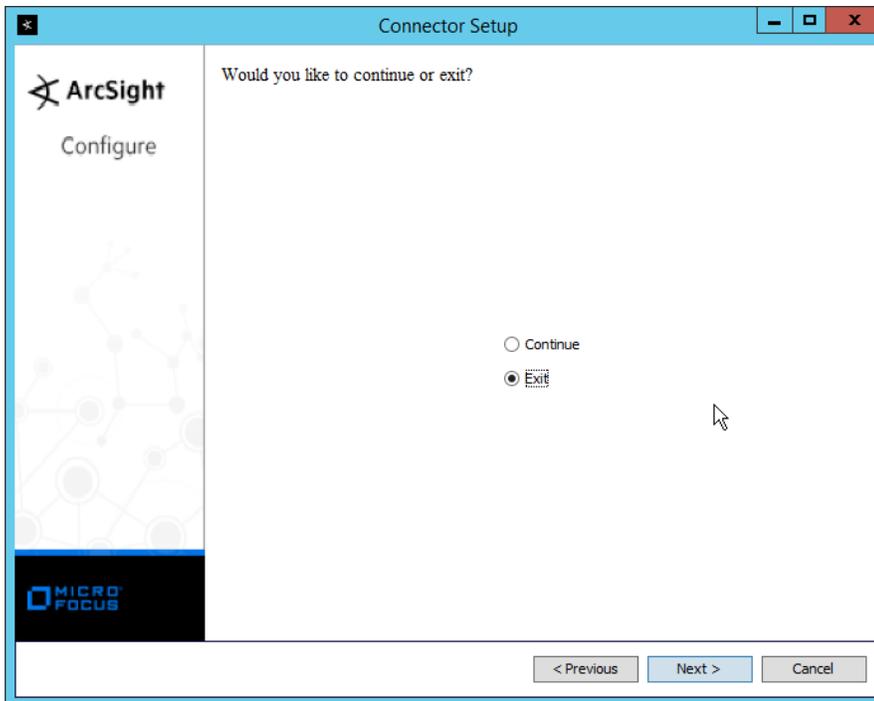
2779  
2780

24. Click **Next**.



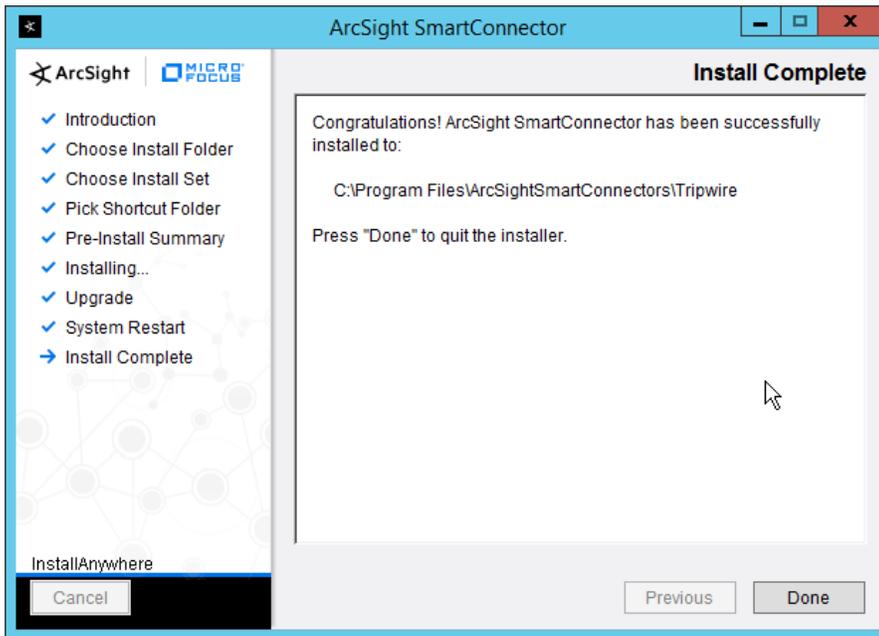
2781  
2782  
2783

- 25. Click **Next**.
- 26. Select **Exit**.



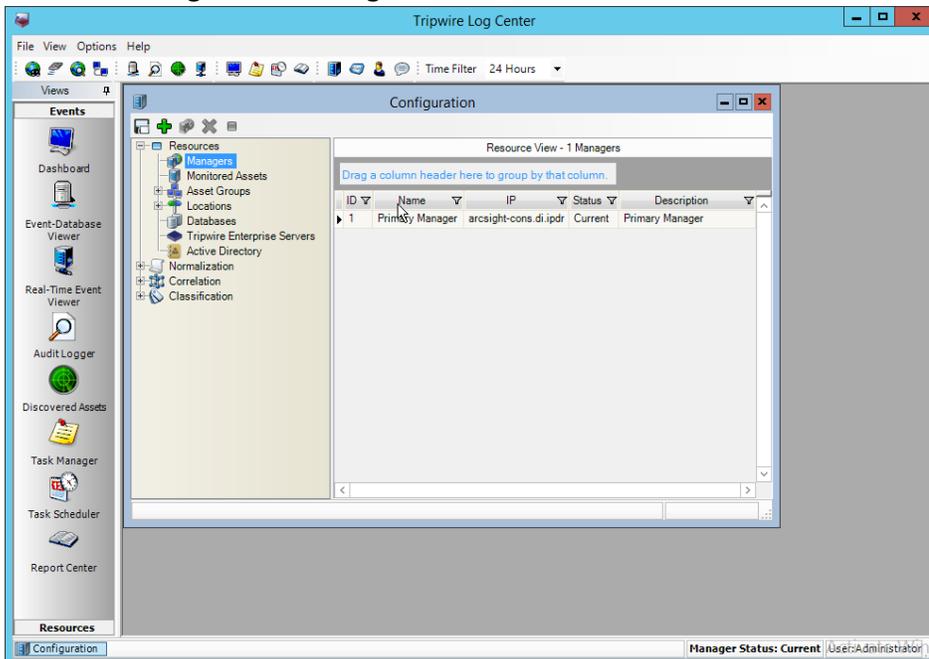
2784  
2785

- 27. Click **Next**.



2786  
2787  
2788  
2789

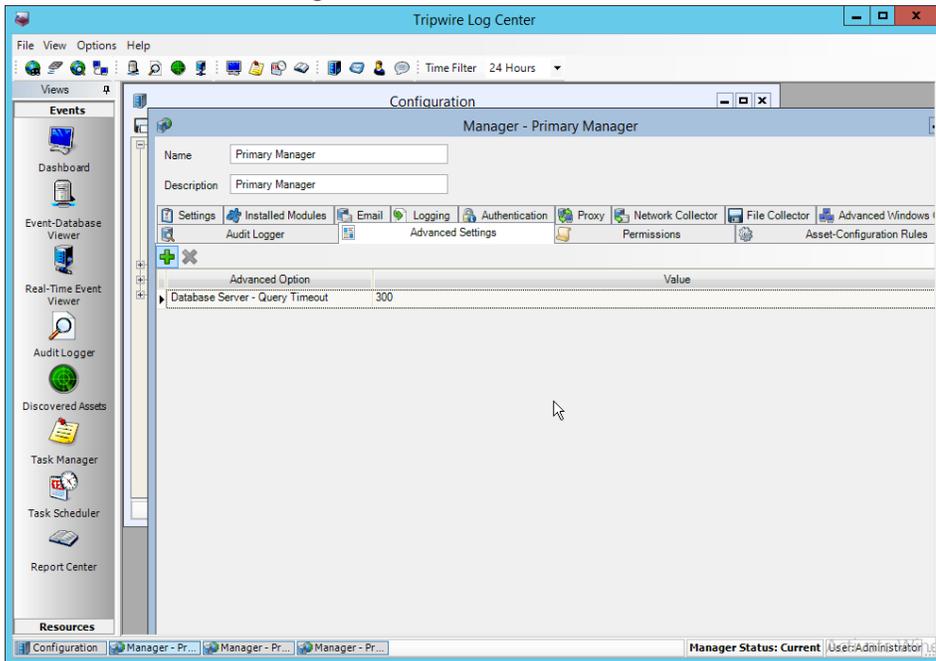
28. Click **Done**.
29. Open the **Tripwire Log Center Console**.
30. Go to the **Configuration Manager**.



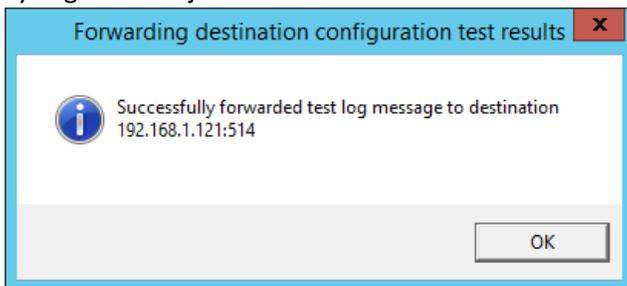
2790  
2791  
2792

31. Select **Resources > Managers**.
32. Double-click the **Primary Manager**.

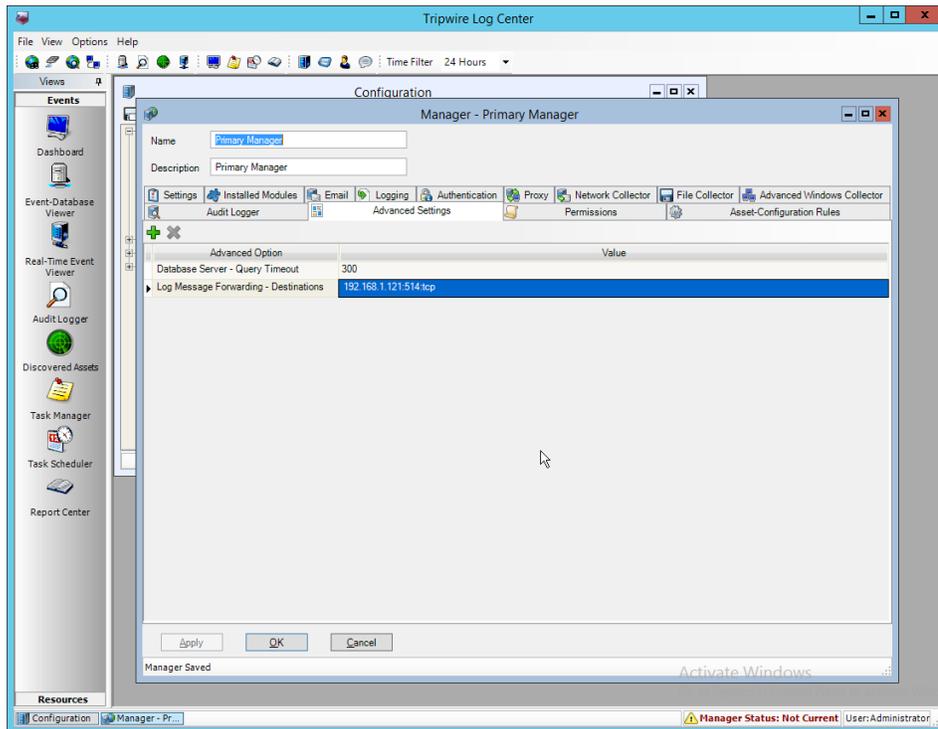
2793 33. Click the **Advanced Settings** tab.



2794  
 2795 34. Click the **Add** button.  
 2796 35. In the **Advanced Option** box select **Log Message Forwarding – Destinations**.  
 2797 36. In the **Value** box next to it, type `<ip_address>:<port>:tcp` with the **IP address** and **port** of the  
 2798 syslog daemon just created.



2799  
 2800 37. Click **OK**.



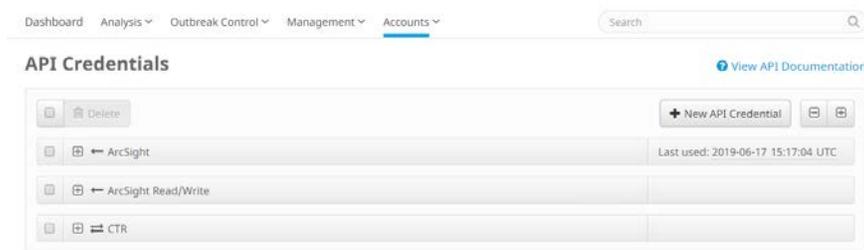
- 2801
  - 2802
  - 2803
38. Click **OK**.
  39. Restart the **Tripwire Log Center Manager**.

## 2804 2.20 Integration: Micro Focus ArcSight and Cisco AMP

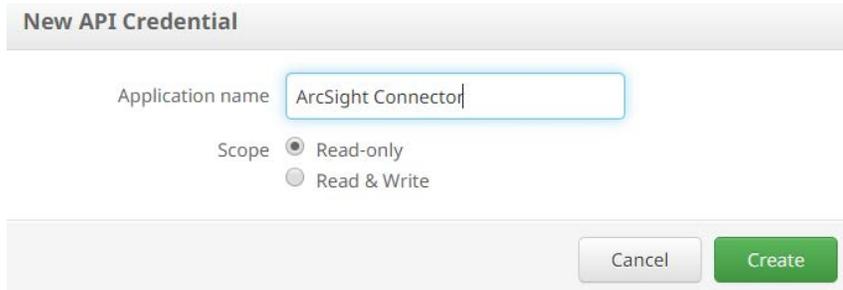
2805 This section will detail the collection of logs from **Cisco AMP's** REST APIs using **Micro Focus ArcSight**.

### 2806 2.20.1 Create API Credentials for ArcSight to access AMP

- 2807 1. On the Cisco AMP web console, log in and navigate to **Accounts > API Credentials**.



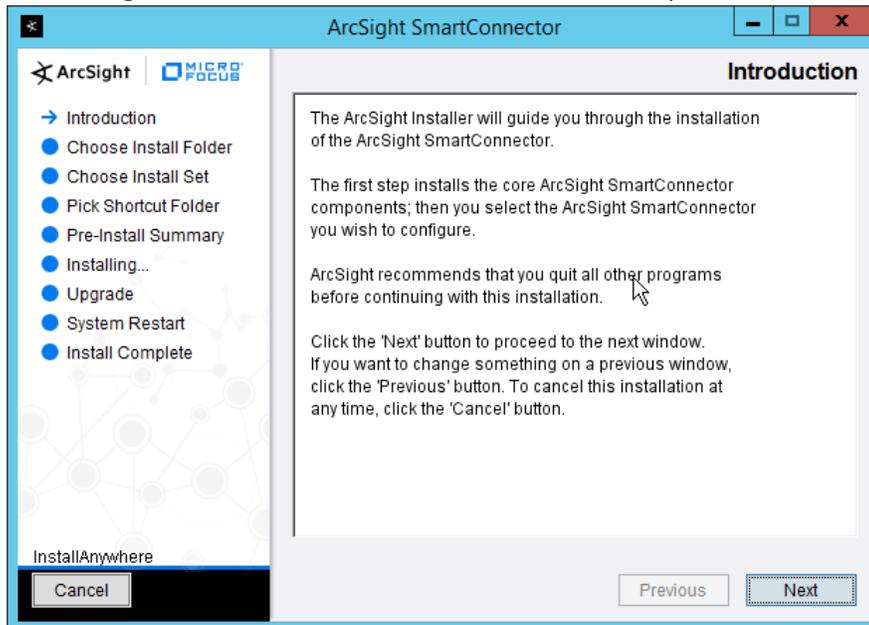
- 2808
  - 2809
  - 2810
  - 2811
2. Click **New API Credential**.
  3. Enter a name for the credential.
  4. Select **Read-only**.



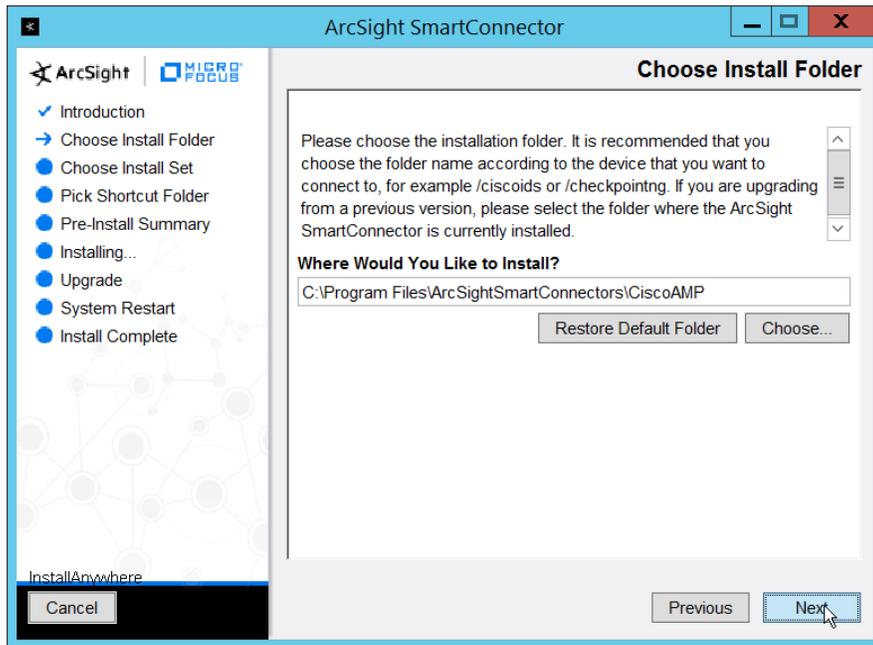
- 2812
  - 2813
  - 2814
  - 2815
5. Click **Create**.
  6. This will direct you to a page with an **ID** and **API Key**. Keep track of these, as you will need them in the setup for the ArcSight Connector, and Cisco AMP may not let you view them again.

## 2816 2.20.2 Install Micro Focus ArcSight

- 2817
1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server.

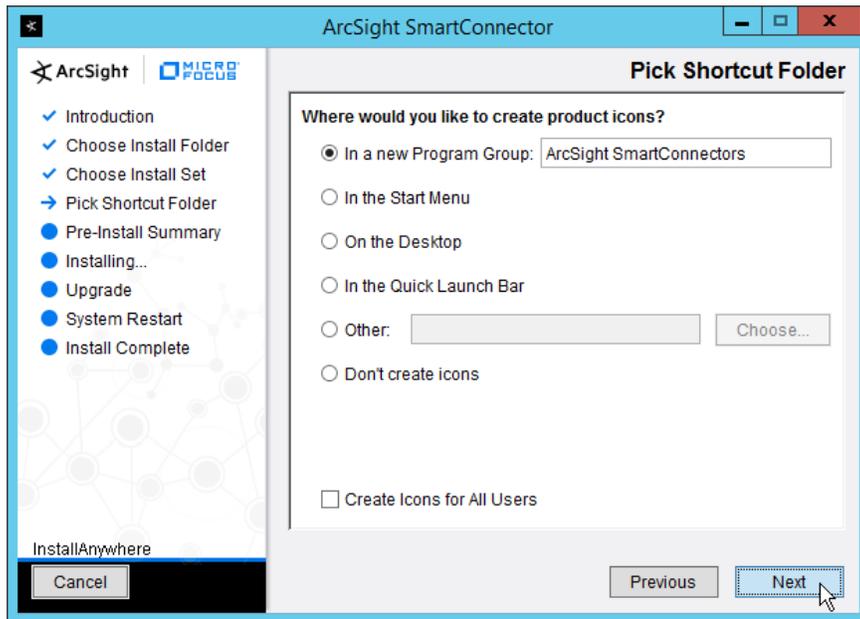


- 2818
  - 2819
  - 2820
2. Click **Next**.
  3. Enter *C:\Program Files\ArcSightSmartConnectors\CiscoAMP*.



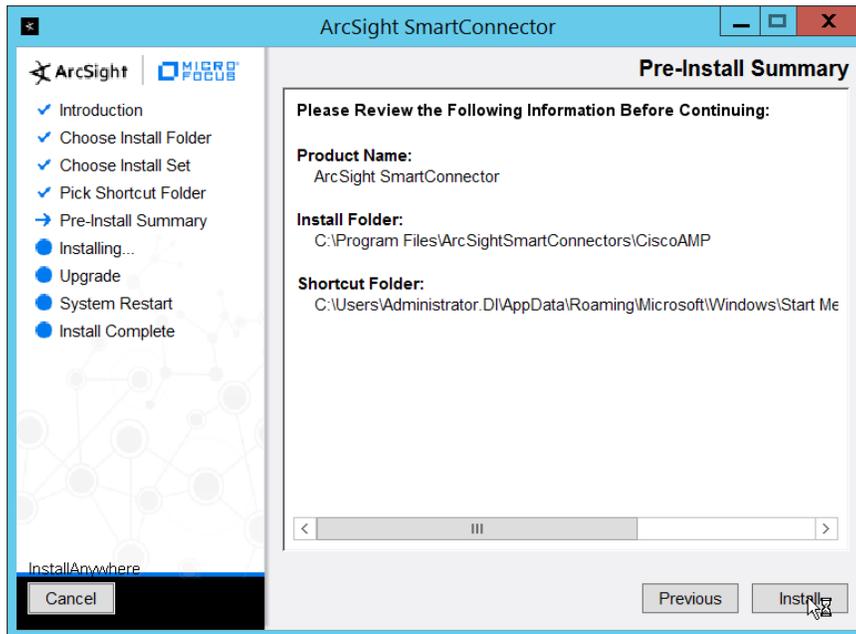
2821  
2822

4. Click **Next**.



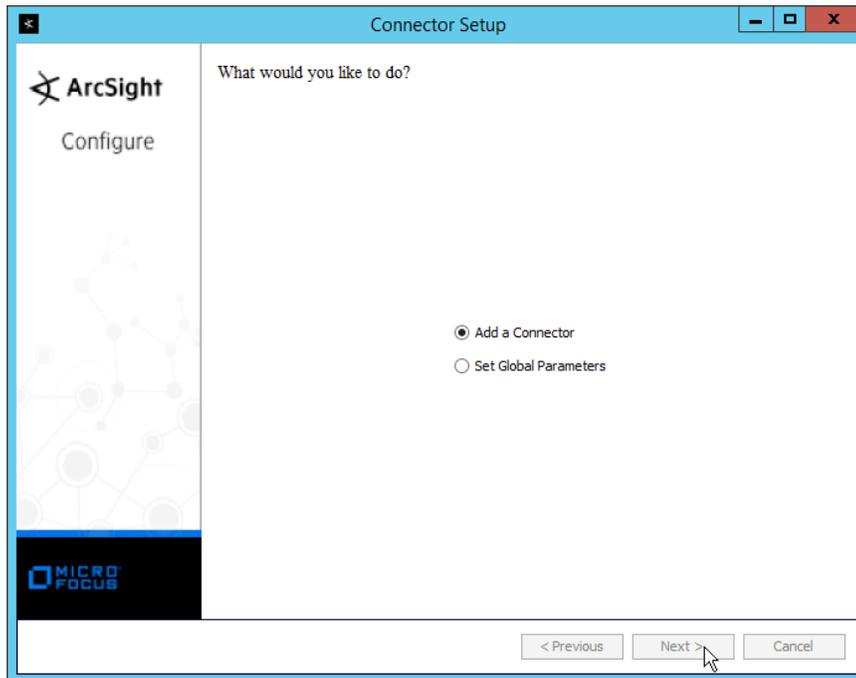
2823  
2824

5. Click **Next**.



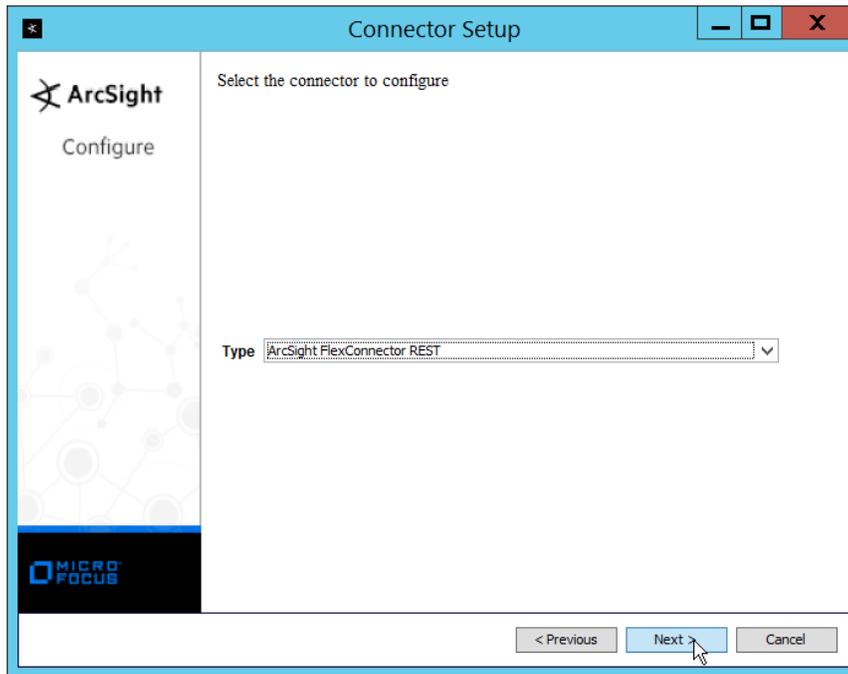
2825  
2826  
2827

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

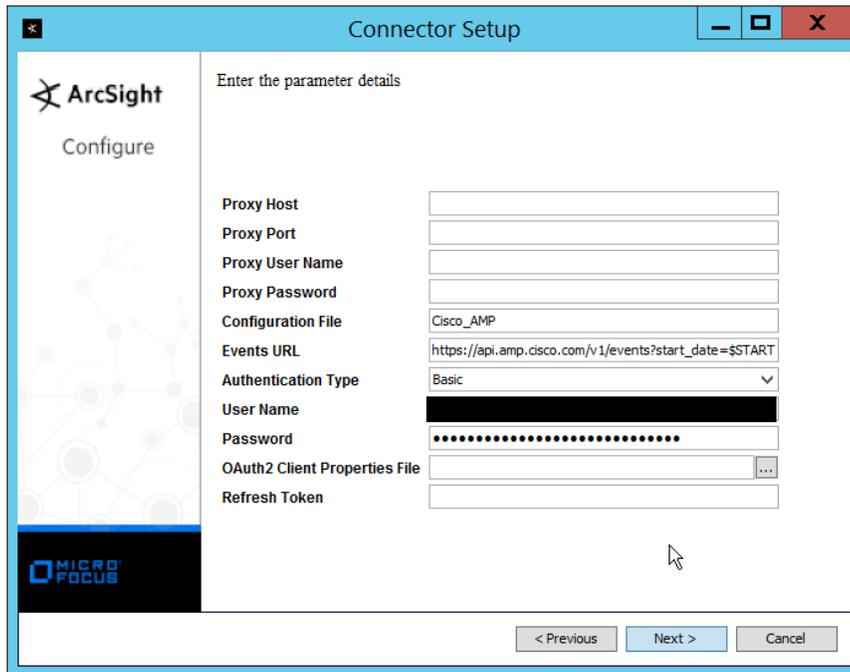


2828  
2829  
2830

8. Click **Next**.
9. Select **ArcSight FlexConnector REST**.

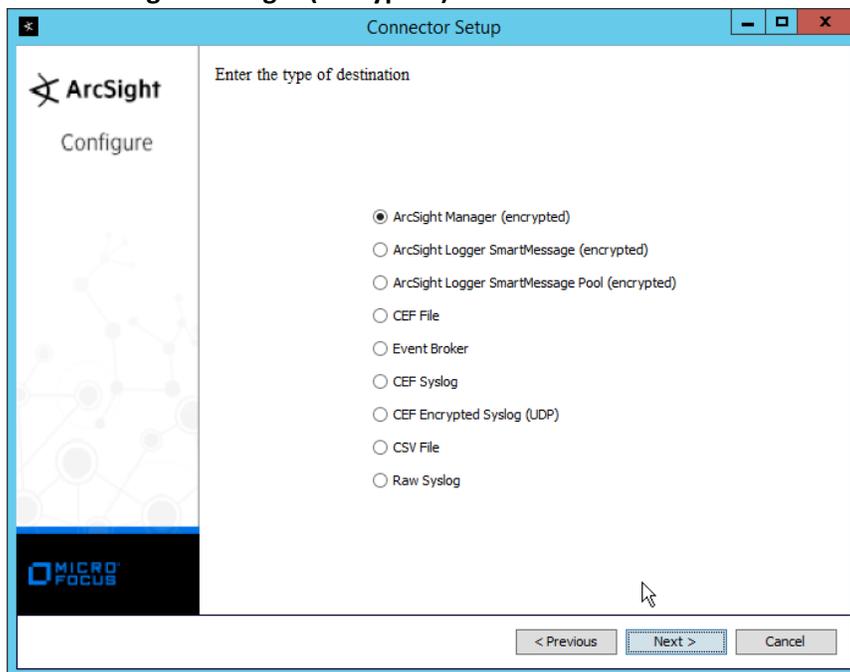


- 2831
- 2832
- 2833
- 2834
- 2835
- 2836
- 2837
- 2838
10. Click **Next**.
  11. Enter *Cisco\_AMP* for the **Configuration File**.
  12. Enter [https://api.amp.cisco.com/v1/events?start\\_date=\\$START\\_AT\\_TIME](https://api.amp.cisco.com/v1/events?start_date=$START_AT_TIME) for the **Events URL**.  
(Note: You can see the Cisco AMP REST API documentation for more information on how to formulate this URL for things other than events.)
  13. Enter the username and password from the credential generated on Cisco AMP in Section 2.20.1.



2839  
2840  
2841

- 14. Click **Next**.
- 15. Select **ArcSight Manager (encrypted)**.



2842  
2843  
2844

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

The screenshot shows the 'Connector Setup' window with the title bar containing a close button, a maximize button, and a window control button. The window is divided into two main sections. On the left is a sidebar with the ArcSight logo and the word 'Configure' below it. On the right, the heading 'Enter the destination parameters' is followed by a list of configuration fields: 'Manager Hostname' (text input with 'arcsight-esm'), 'Manager Port' (text input with '8443'), 'User' (text input with 'administrator'), 'Password' (password input with masked characters), 'AUP Master Destination' (dropdown menu with 'false'), 'Filter Out All Events' (dropdown menu with 'false'), and 'Enable Demo CA' (dropdown menu with 'false'). At the bottom of the window are three buttons: '< Previous', 'Next >', and 'Cancel'.

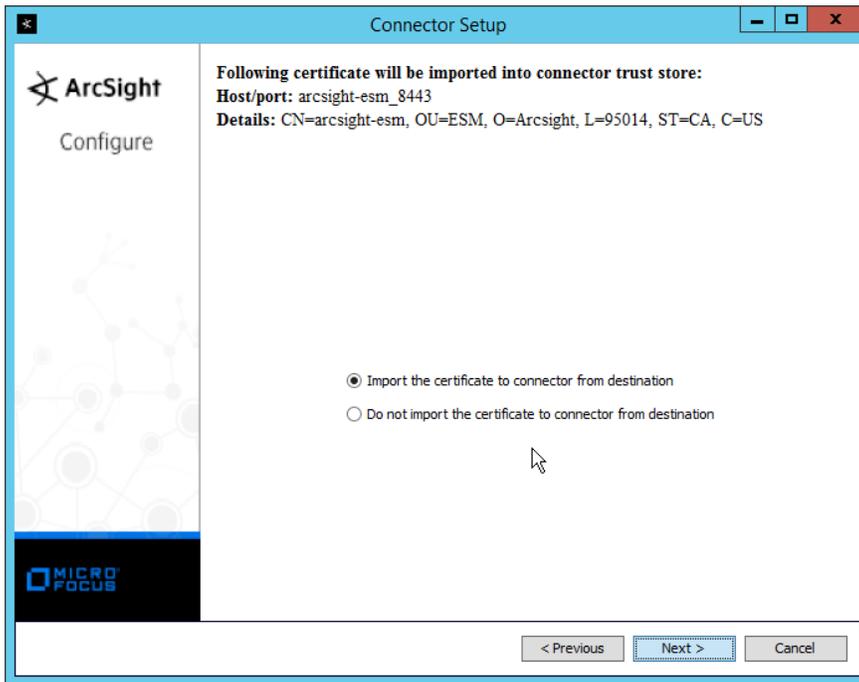
2845  
2846  
2847

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

The screenshot shows the 'Connector Setup' window with the title bar containing a close button, a maximize button, and a window control button. The window is divided into two main sections. On the left is a sidebar with the ArcSight logo and the word 'Configure' below it. On the right, the heading 'Enter the connector details' is followed by a list of configuration fields: 'Name' (text input with 'Cisco AMP'), 'Location' (text input), 'DeviceLocation' (text input), and 'Comment' (text input). At the bottom of the window are three buttons: '< Previous', 'Next >', and 'Cancel'.

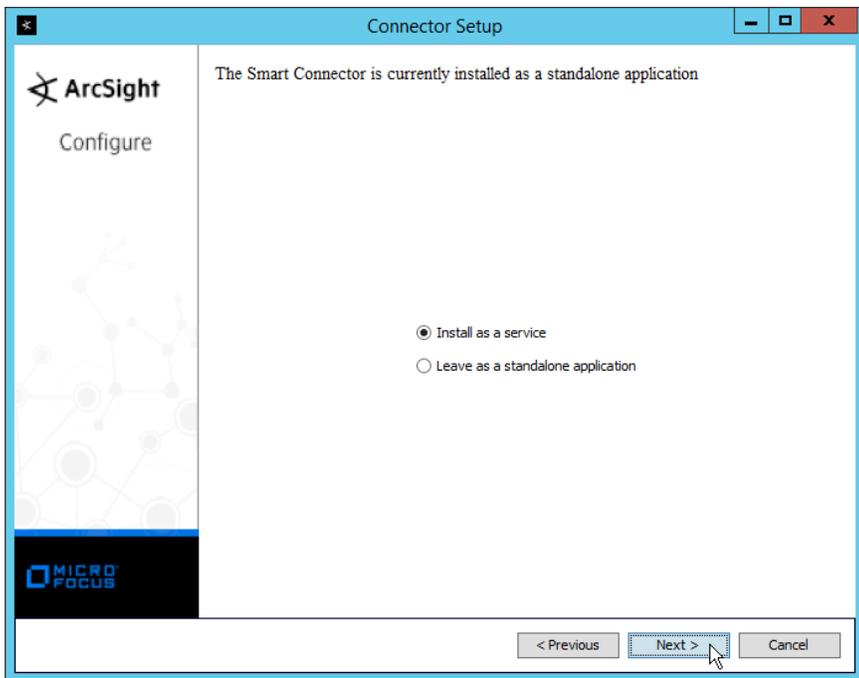
2848  
2849  
2850

- 20. Click **Next**.
- 21. Select **Import the certificate to connector from destination**.



2851  
2852  
2853  
2854

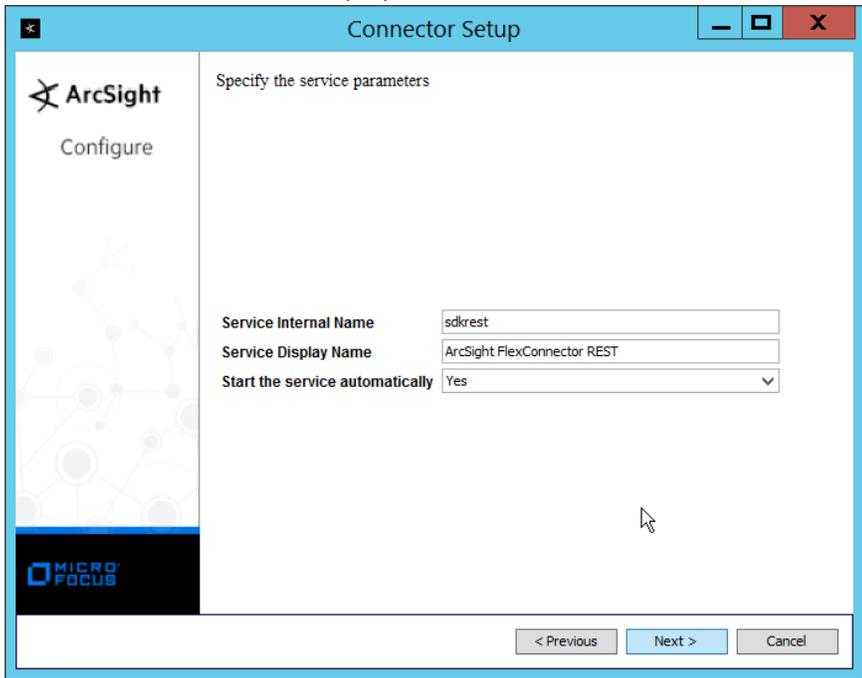
- 22. Click **Next**.
- 23. Click **Next**.
- 24. Select **Install as a service**.



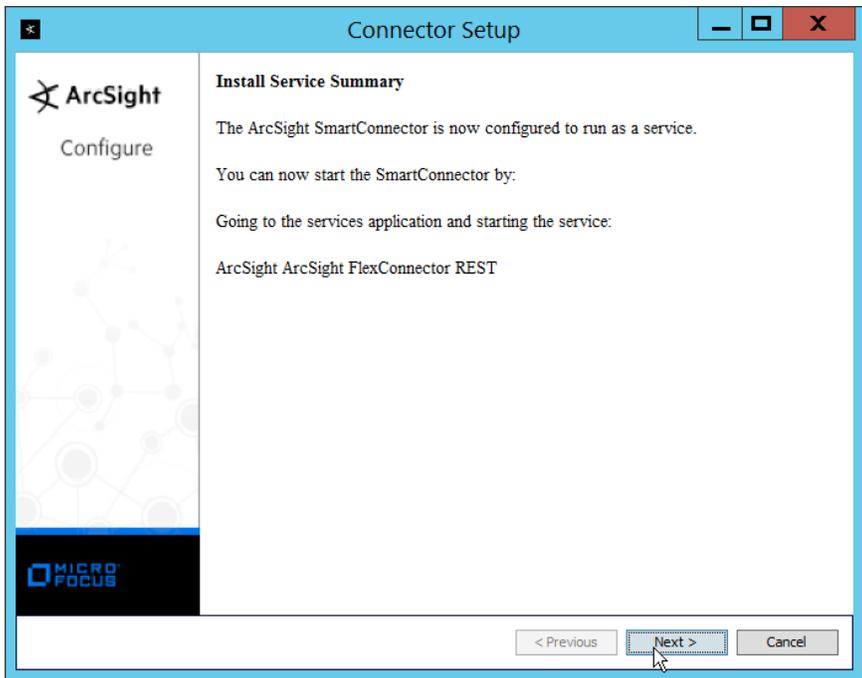
2855  
2856

- 25. Click **Next**.

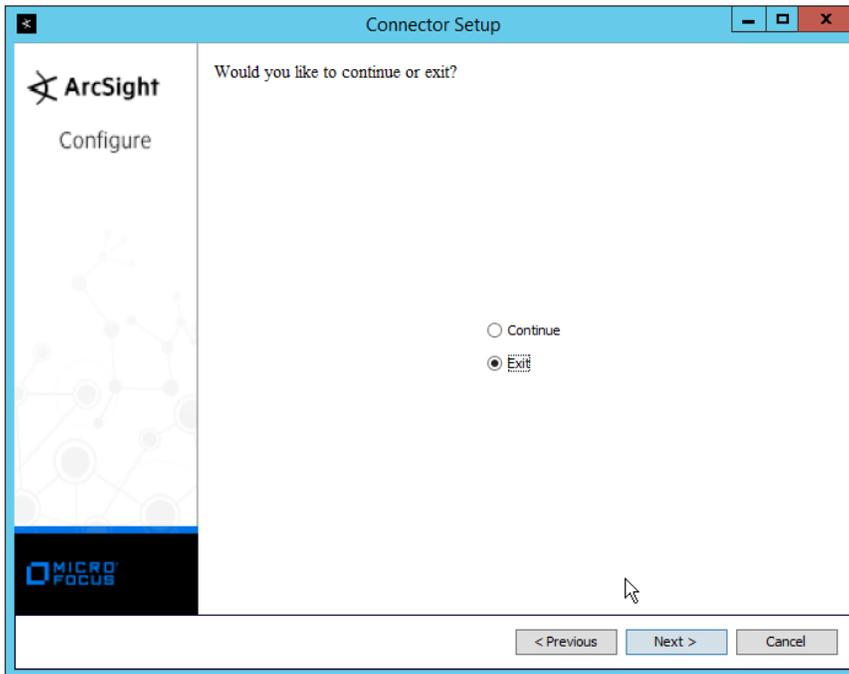
2857 26. Enter a service name and display name.



2858 27. Click **Next**.  
2859

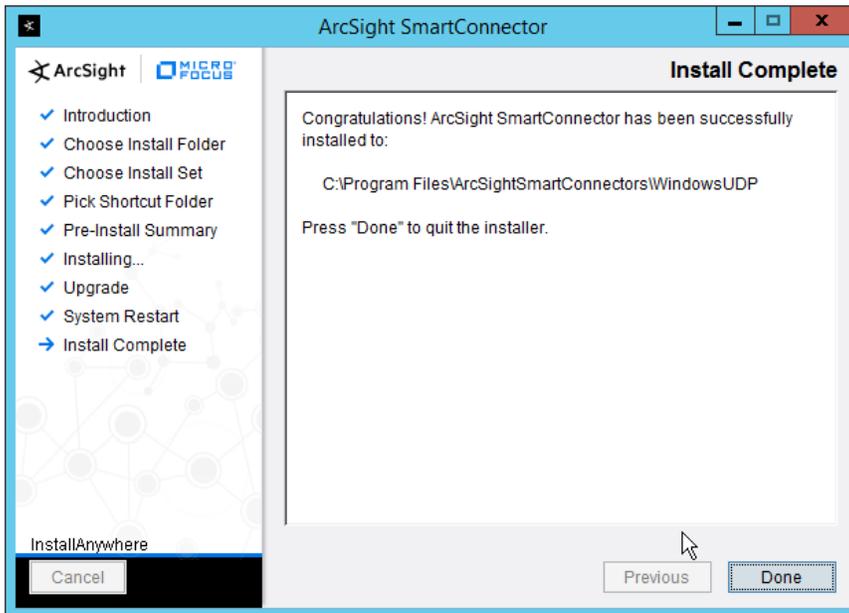


2860 28. Click **Next**.  
2861 29. Select **Exit**.  
2862



2863  
2864

30. Click **Next**.



2865  
2866

31. Click **Done**.

### 2867 2.20.3 Create a Parser for Cisco AMP REST events

- 2868 1. Ensure that the ArcSight connector service is not running.

- 2869       2. Create a text file located at  
 2870       <ARCSIGHT\_HOME>/current/user/agent/flexagent/Cisco\_AMP.jsonparser.properties. (Note:  
 2871       Replace *Cisco\_AMP* with the name used for “Configuration File” during setup.)  
 2872       3. Use the following text to parse some basic information such as the IP, the type of event, and  
 2873       links to Cisco AMP’s more detailed descriptions of the event.

```

2874           trigger.node.location=/data
2875           token.count=6
2876
2877           token[0].name=id
2878           token[0].type=String
2879           token[0].location=id
2880
2881           token[1].name=timestamp
2882           token[1].type=String
2883           token[1].location=date
2884
2885           token[2].name=event_type
2886           token[2].type=String
2887           token[2].location=event_type
2888
2889           token[3].name=hostname
2890           token[3].type=String
2891           token[3].location=computer/hostname
2892
2893           token[4].name=external_ip
2894           token[4].type=IPAddress
2895           token[4].location=computer/external_ip
2896
2897           token[5].name=links
2898           token[5].type=String
2899           token[5].location=links
2900
2901           event.deviceReceiptTime=__createOptionalTimeStampFromString(timestamp,"y
2902           yyy-MM-dd'T'HH:mm:ssX")
2903           event.destinationAddress=external_ip
2904           event.destinationHostName=hostname
2905           event.name=event_type
2906           event.message=links
2907           event.deviceCustomString1=id
2908           event.deviceCustomString1Label=__stringConstant("AMP Event ID")
  
```

- 2910       4. This parser will allow for details of Cisco AMP events to be shown in ArcSight. Custom parsers  
 2911       are a functionality of ArcSight. For more information on the creation of custom parsers, please  
 2912       see the *ArcSight FlexConnector Developer’s Guide* as well as the *FlexConnector REST Developer’s*  
 2913       *Guide*. You can start the service for these changes to take effect.

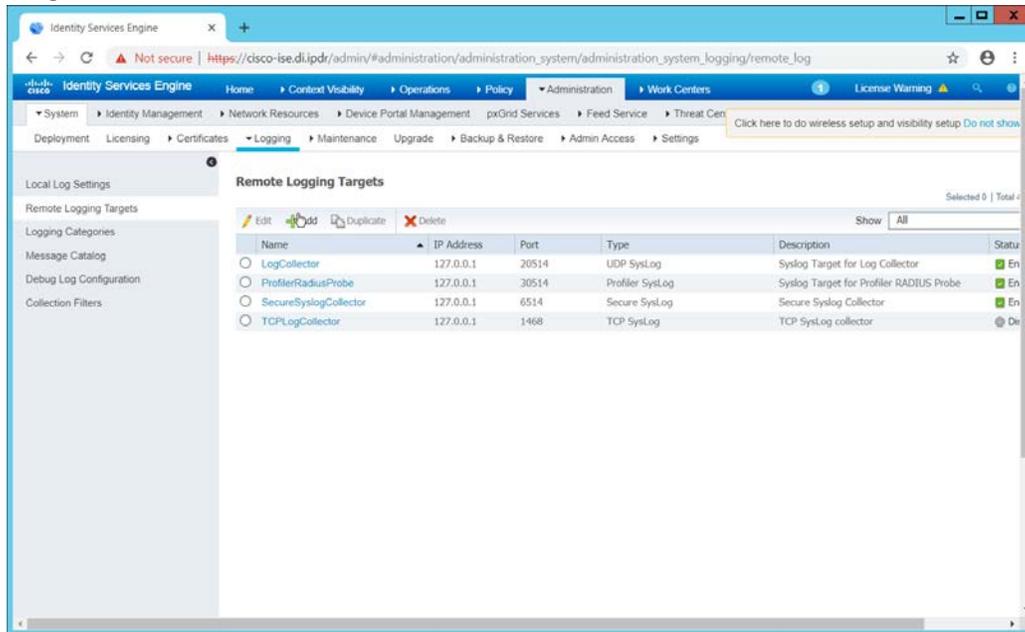
## 2914   2.21   Integration: Micro Focus ArcSight and Cisco ISE

2915   This integration will briefly detail how to send logs to an ArcSight syslog collector from Cisco ISE. Please  
 2916   see Section 2.18 (under integrating Tripwire & ArcSight) for instructions for setting up an ArcSight syslog

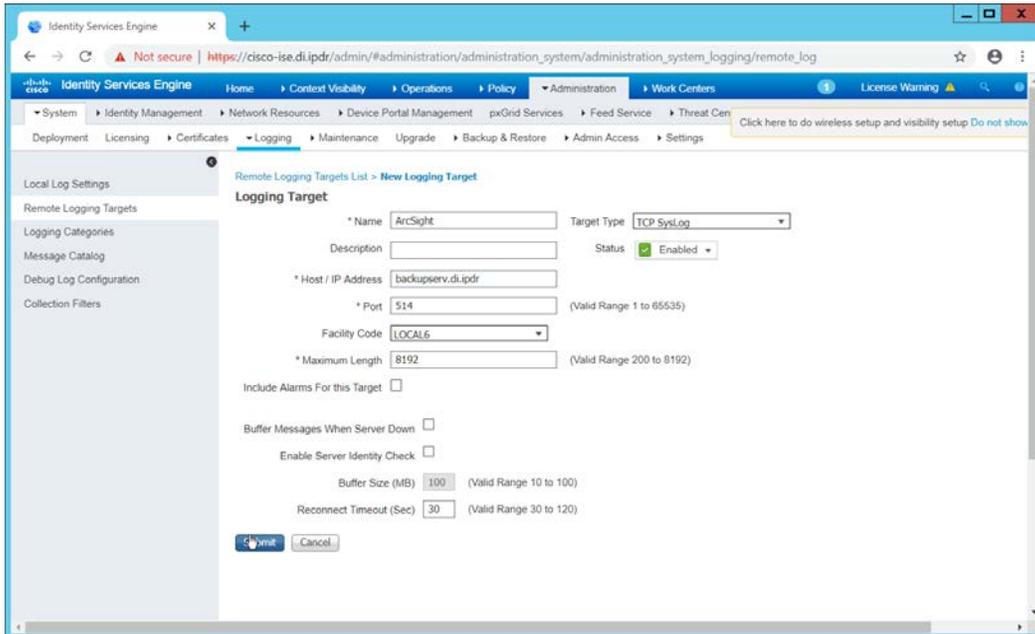
2917 collector. If a server is already configured, you do not need to install a new one—simply use the address  
2918 of that server to which to forward logs.

## 2919 2.21.1 Configure Cisco ISE to Forward Logs

2920 1. In the Cisco ISE web client, navigate to **Administration > System > Logging > Remote Logging**  
2921 **Targets.**

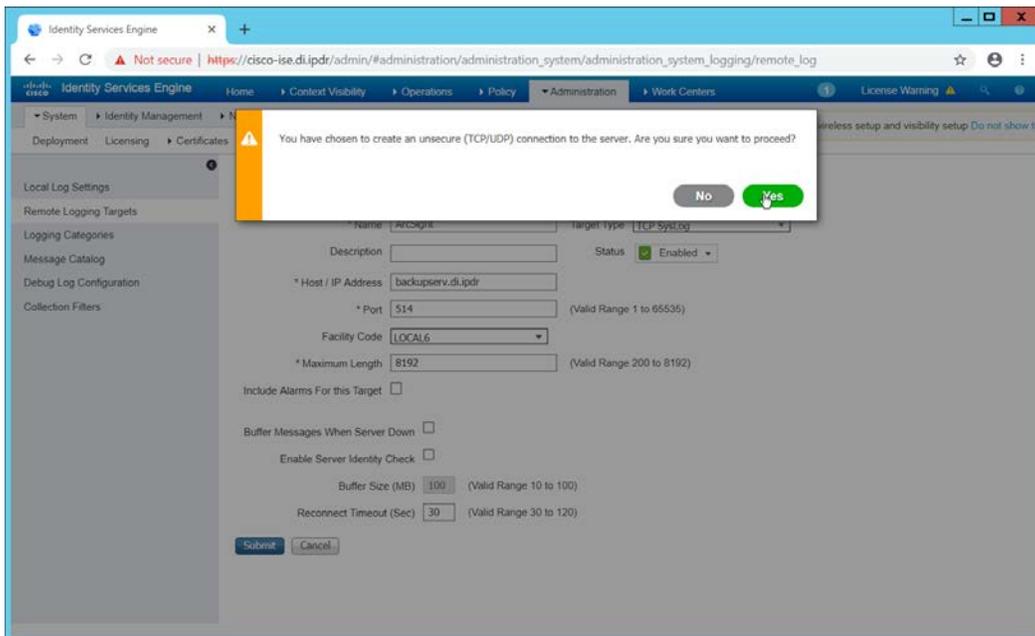


2922 2. Click **Add**.  
2923 3. Enter a name for **Name**.  
2924 4. Enter the **hostname** of the ArcSight syslog collector server for **Host/IP Address**.  
2925 5. Select **TCP SysLog** for Target Type. (Ensure that your syslog collector server is configured to use  
2926 TCP).  
2927 6. Enter **514** or the port used on the syslog server.  
2928 7. Enter **8192** or a custom message size limit for **Maximum Length**.  
2929 8. Ensure that **Status** is set to **Enabled**.  
2930



2931  
2932

9. Click **Submit**.

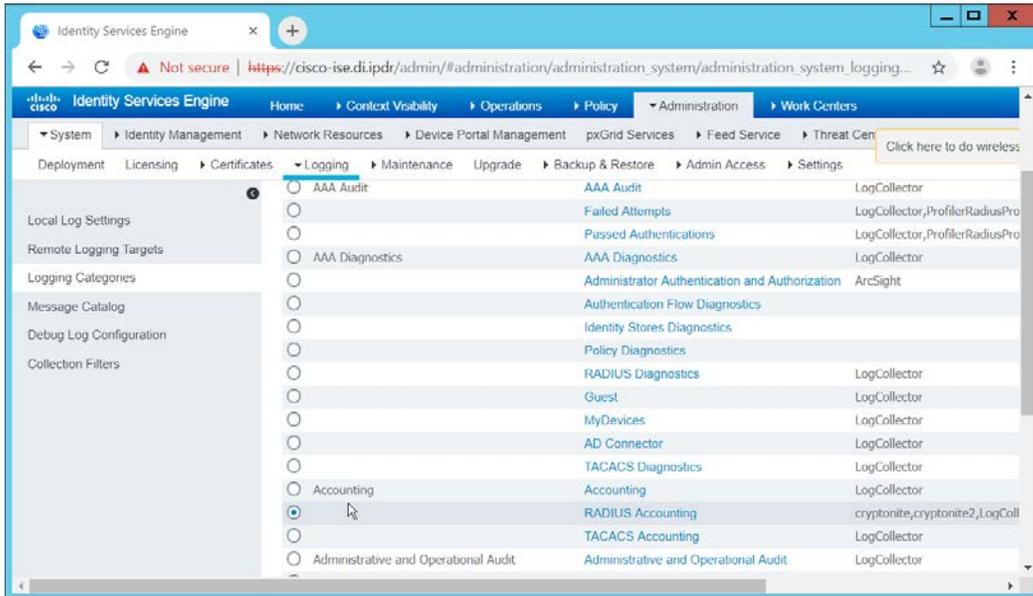


2933  
2934

10. Click **Yes**.

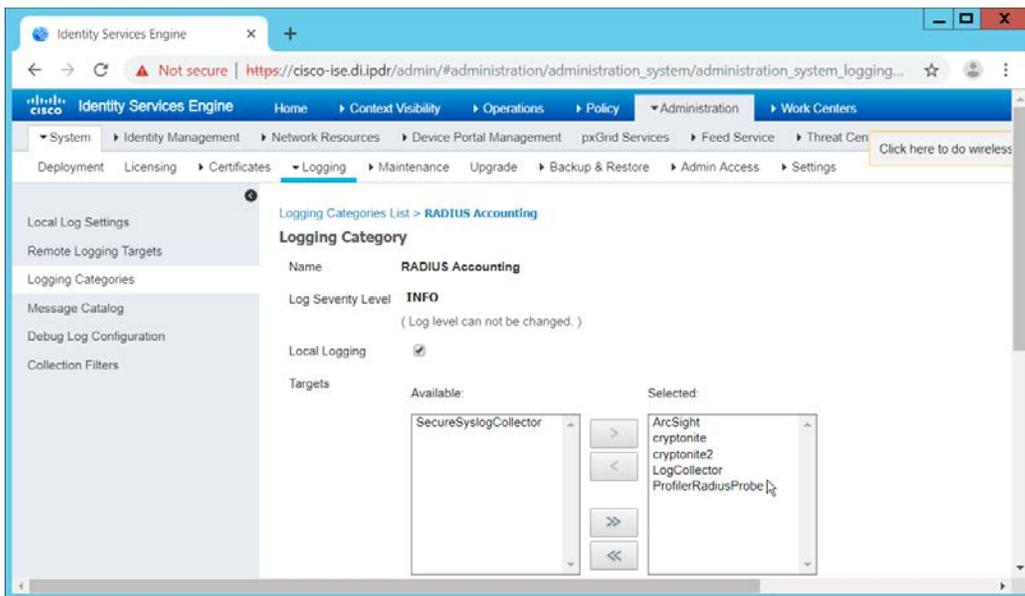
## 2935 2.21.2 Select Logs for Forwarding

2936 1. Navigate to **System > Logging > Logging Categories**.



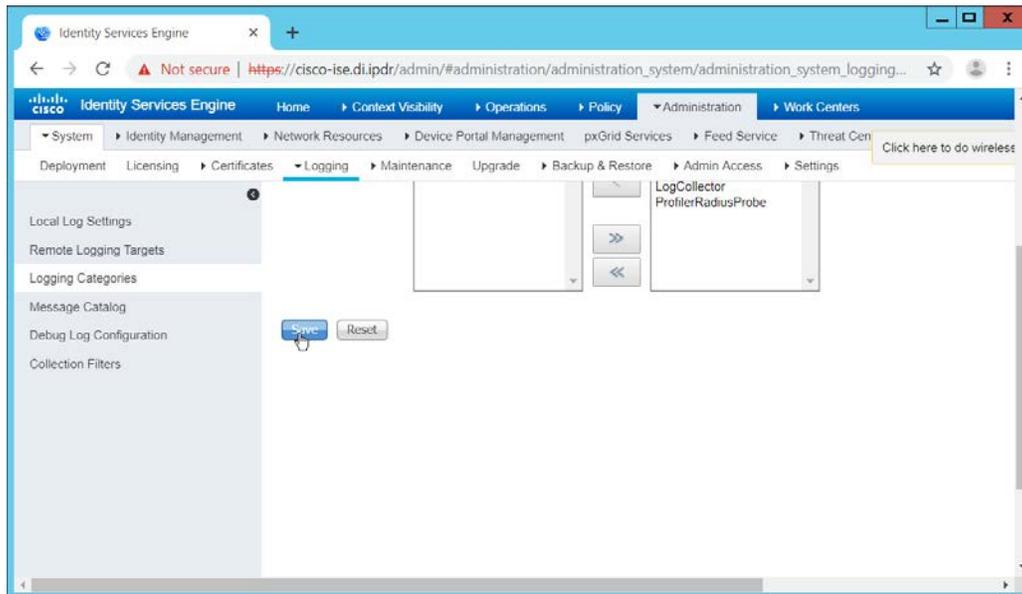
2937  
2938  
2939

2. Select a log file to forward to ArcSight.
3. Click **Edit**.



2940  
2941

4. Move the ArcSight logging target you just created to the **Selected** box.



- 2942
- 2943
- 2944
5. Click **Save**.
  6. Repeat steps 1-5 for any log files you wish to forward to ArcSight.

## 2945 2.22 Integration: Micro Focus ArcSight and Semperis DSP

2946 This integration will briefly detail how to send logs to an ArcSight syslog collector from Semperis DSP.

2947 Please see Section 2.18 (under integrating Tripwire & ArcSight) for instructions for setting up an

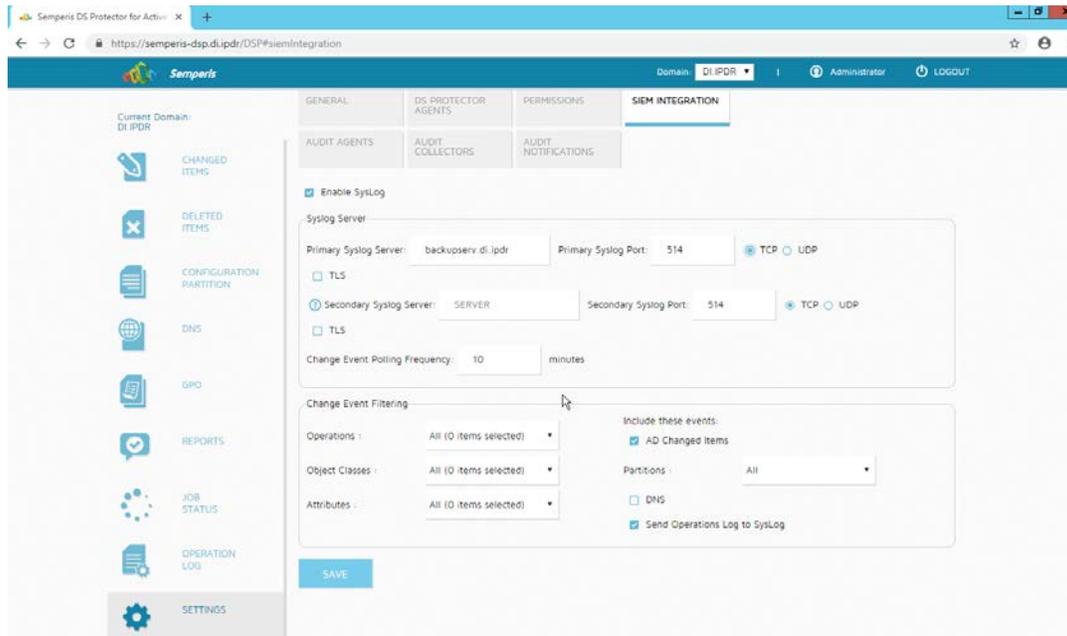
2948 ArcSight syslog collector. If a server is already configured, you do not need to install a new one—simply

2949 use the address of that server to which to forward logs.

2950 Note: This integration requires Semperis DSP version 2.6.

### 2951 2.22.1 Configure Semperis DSP to Forward Logs

- 2952
- 2953
- 2954
- 2955
- 2956
- 2957
- 2958
- 2959
- 2960
- 2961
1. In Semperis DSP, navigate to **Settings > SIEM Integration**.
  2. Check the box next to **Enable SysLog**.
  3. Under **Syslog Server**, enter the **hostname** for the ArcSight syslog collector, as well as the **port**.
  4. Select **TCP**.
  5. Enter a value for **Change Event Polling Frequency** based on the needs of your organization; this is how often it will poll for new logs to forward.
  6. Under **Change Event Filtering**, select **AD Changed Items**, and **Send Operation Log to SysLog**. Ensure that **All** is selected for **Partitions**.
  7. You can also select any specific **operations**, **classes**, and **attributes** to be forwarded or simply leave it as **All**.



2962  
2963

8. Click **Save**.



2964  
2965

9. Click **Close**.

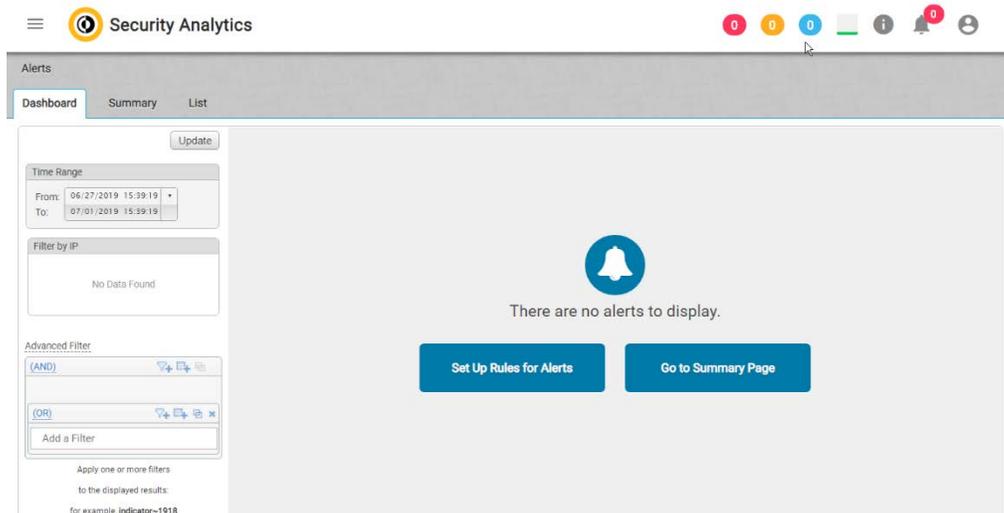
## 2966 2.23 Integration: Micro Focus ArcSight and Symantec Analytics

2967 This section will first detail the forwarding of logs from **Symantec Analytics** to **Micro Focus ArcSight**.  
2968 Please see section **2.18** (under integrating Tripwire & ArcSight) for instructions for setting up an  
2969 ArcSight syslog collector. If a server is already configured, you do not need to install a new one; simply  
2970 use the address of that server to which to forward logs.

2971 The second part of this section will detail a further integration for ArcSight that allows ArcSight to better  
2972 analyze network packets received from Symantec Analytics.

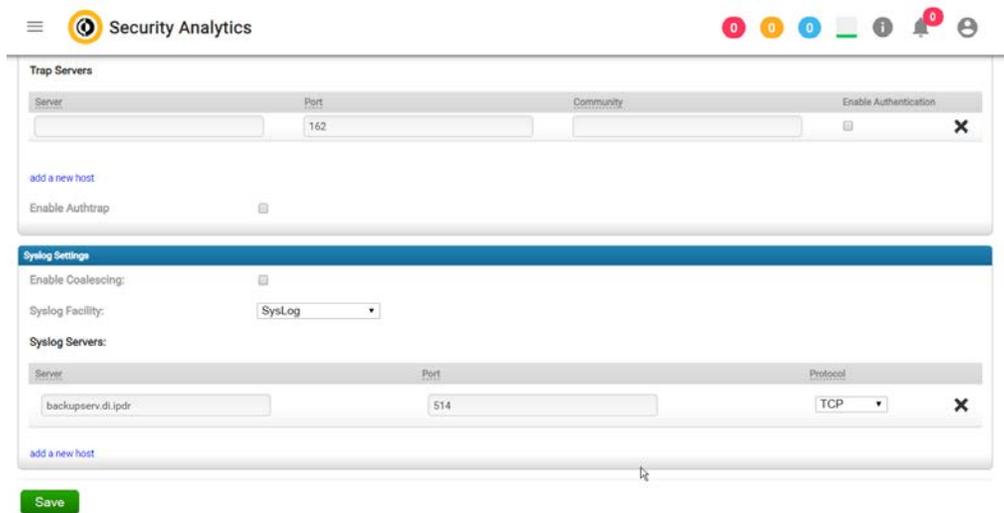
### 2973 2.23.1 Configure Symantec Analytics to Forward Logs

- 2974 1. Log in to the Symantec Analytics web console.



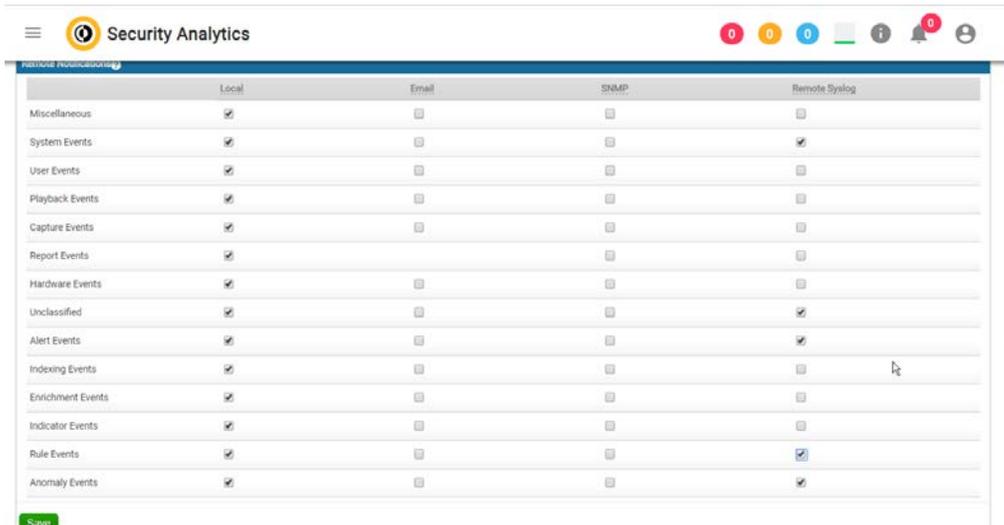
2975  
2976  
2977  
2978  
2979  
2980  
2981  
2982

2. Click the **menu** icon in the top left.
3. Navigate to **Settings > Communication**.
4. Scroll down to the **Syslog Settings** section.
5. Select **SysLog** for **Syslog Facility**.
6. Enter the hostname or IP of the ArcSight syslog collector server under **Server**.
7. Enter **514** for the port.
8. Select **TCP** for the protocol.



2983  
2984  
2985  
2986  
2987  
2988

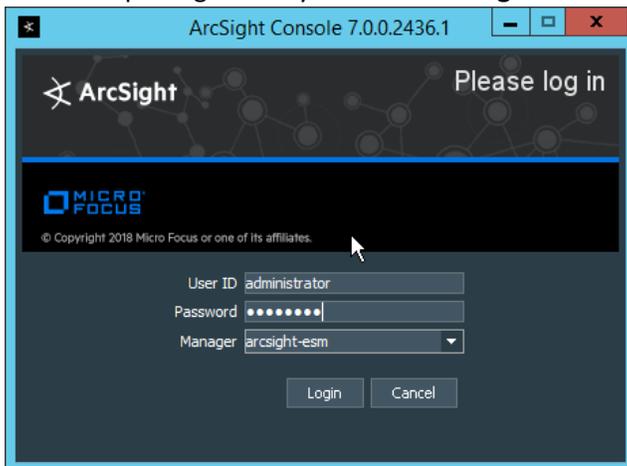
9. Click **Save**.
10. Click the **Advanced** tab.
11. Select the box under **Remote Syslog** column for any events that you wish to forward to ArcSight, for example, **System Events, Unclassified Events, Alert Events, Rule Events, Anomaly Events**.



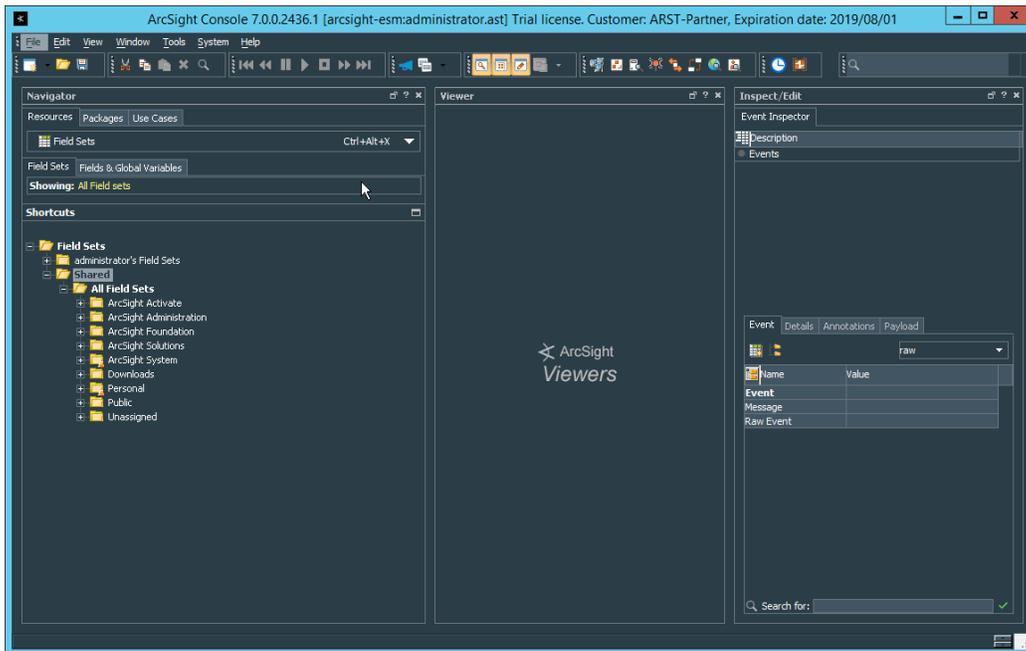
2989  
2990 12. Click **Save**.

2991 **2.23.2 Install Symantec Analytics Package for ArcSight**

- 2992 1. Navigate to the ArcSight marketplace. Look for the “Blue Coat Security Analytics” package for  
 2993 ArcSight. It may be available here: [https://marketplace.microfocus.com/arc-sight/content/blue-](https://marketplace.microfocus.com/arc-sight/content/blue-coat-security-analytics-platform)  
 2994 [coat-security-analytics-platform](https://marketplace.microfocus.com/arc-sight/content/blue-coat-security-analytics-platform) but not please contact your ArcSight representative to get the  
 2995 package. The package should be called **Blue\_Coat\_SA\_HP\_ArcSight-3.0.arb**.  
 2996 2. Place this package on a system with **ArcSight ESM Console** installed.

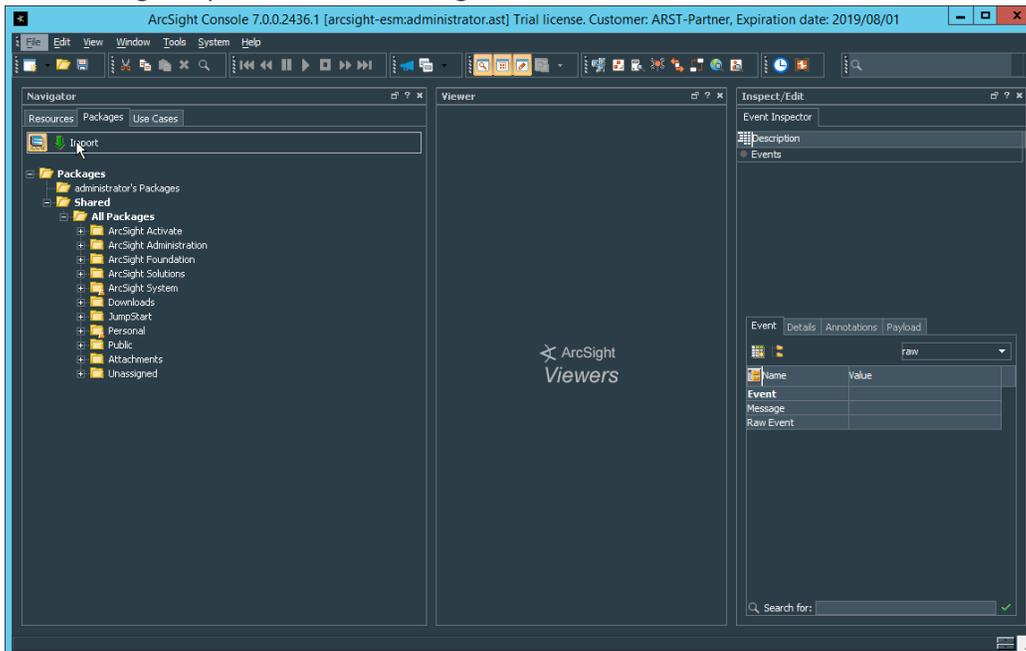


2997 3. Log in to the **ArcSight ESM Console** with a user that has the privileges to install packages.  
 2998



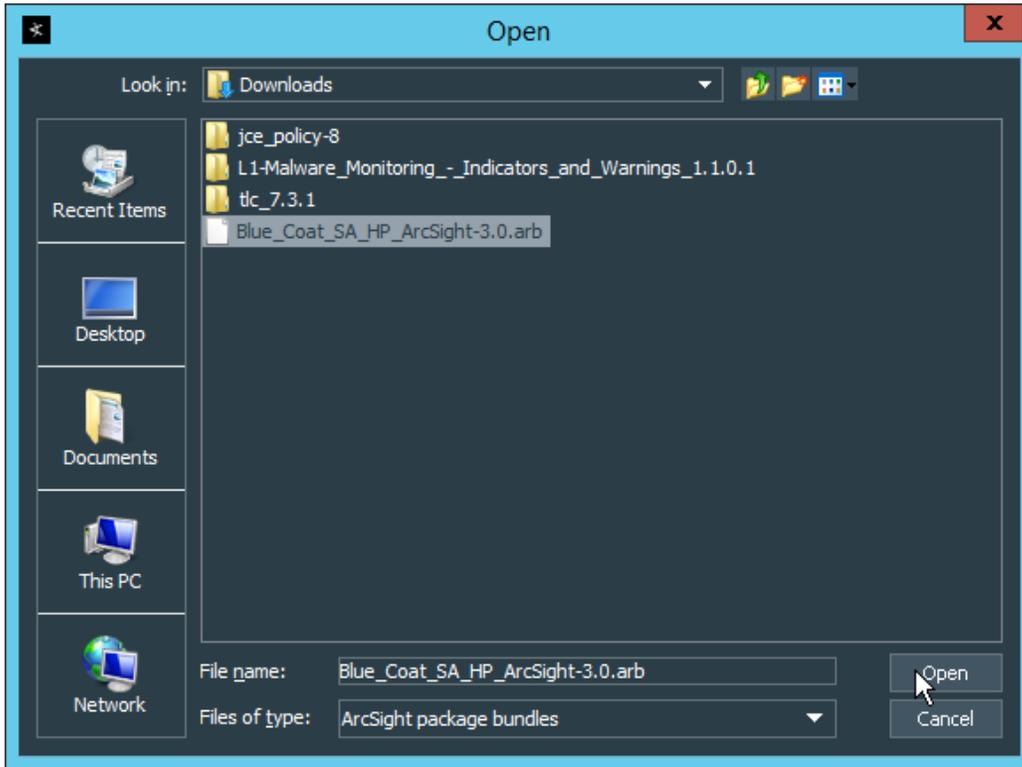
2999  
3000

4. In the **Navigator** pane, click the **Packages** tab.



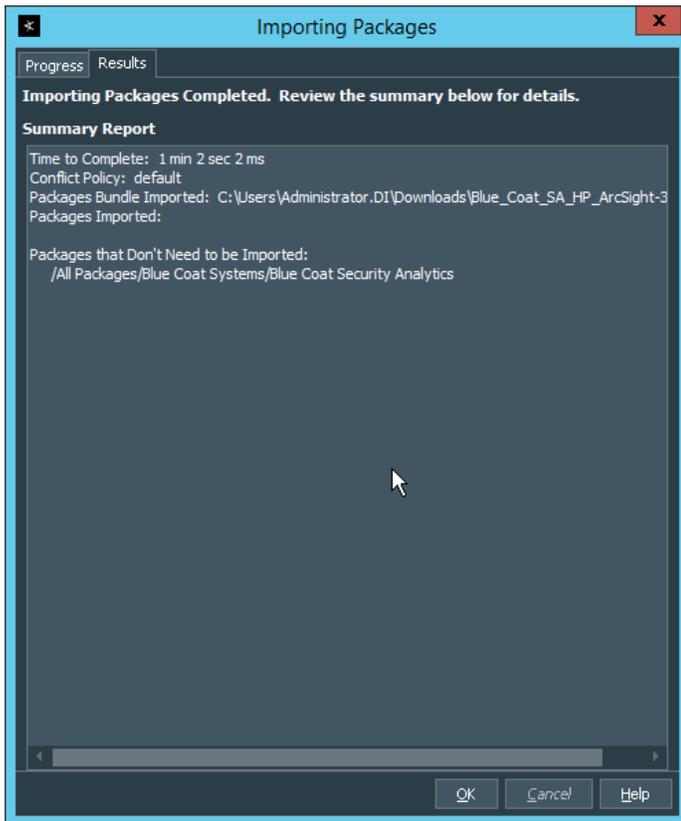
3001  
3002  
3003

5. Click **Import**.
6. In the window that it opens, find and select the package you downloaded.



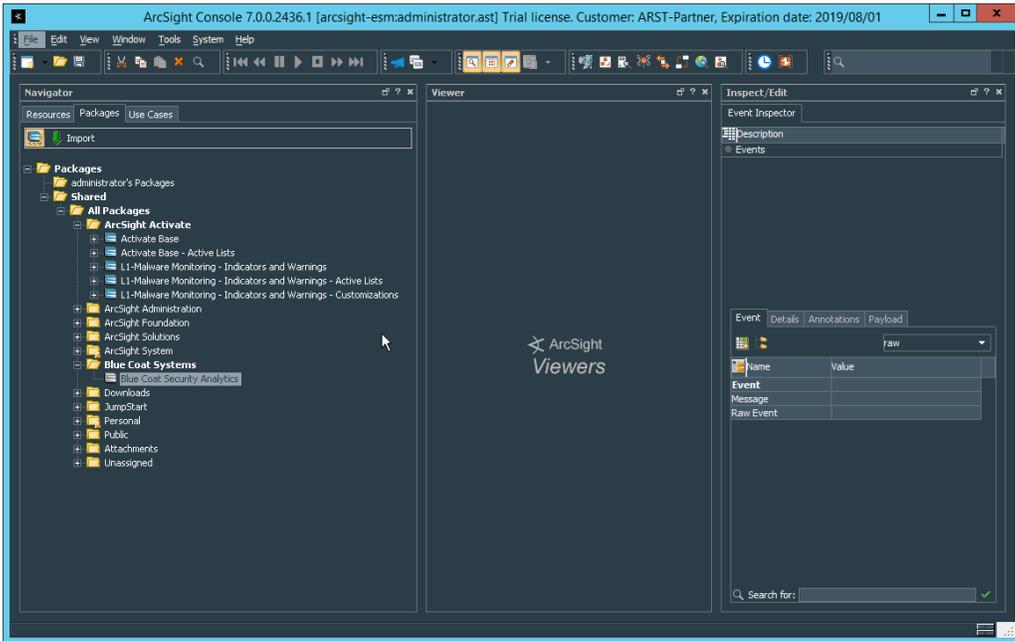
3004  
3005

7. Click **Open**.



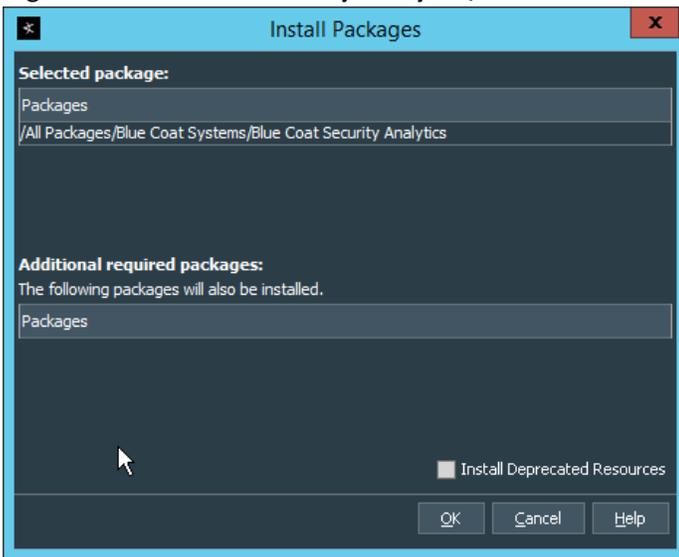
3006  
3007  
3008  
3009

8. Click **OK** when the import finishes.
9. Under the **Packages** tab in the **Navigator** pane, navigate to **Packages > Shared > All Packages > Blue Coat Systems > Blue Coat Security Analytics**.



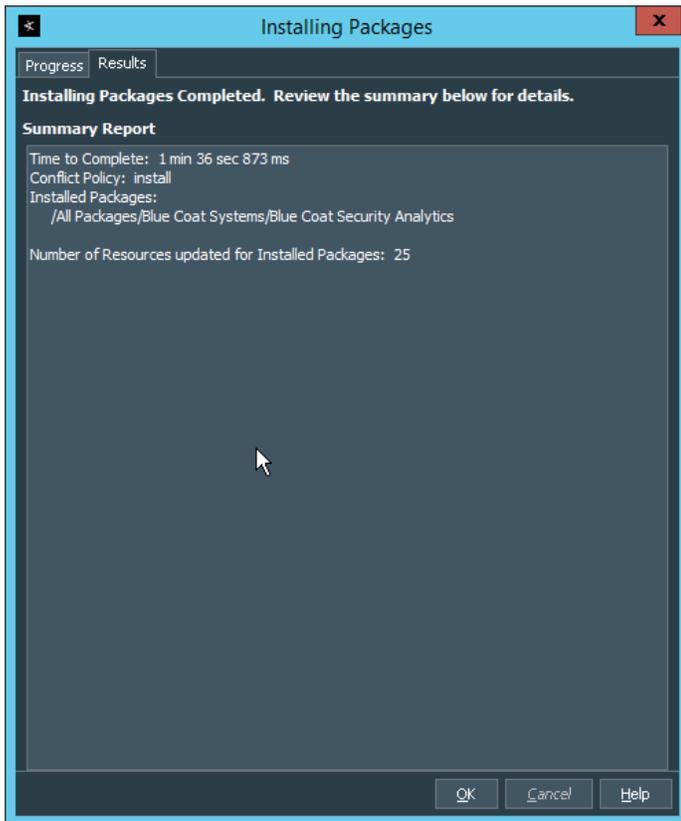
3010  
3011

10. Right-click **Blue Coat Security Analytics**, and select **Install Package**.



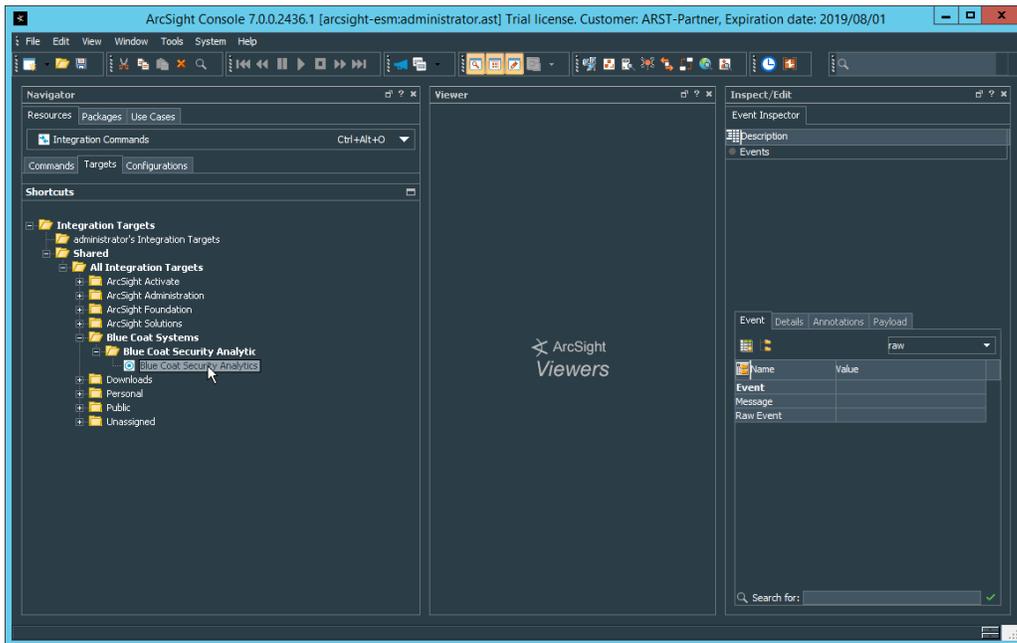
3012  
3013

11. Click **OK**.



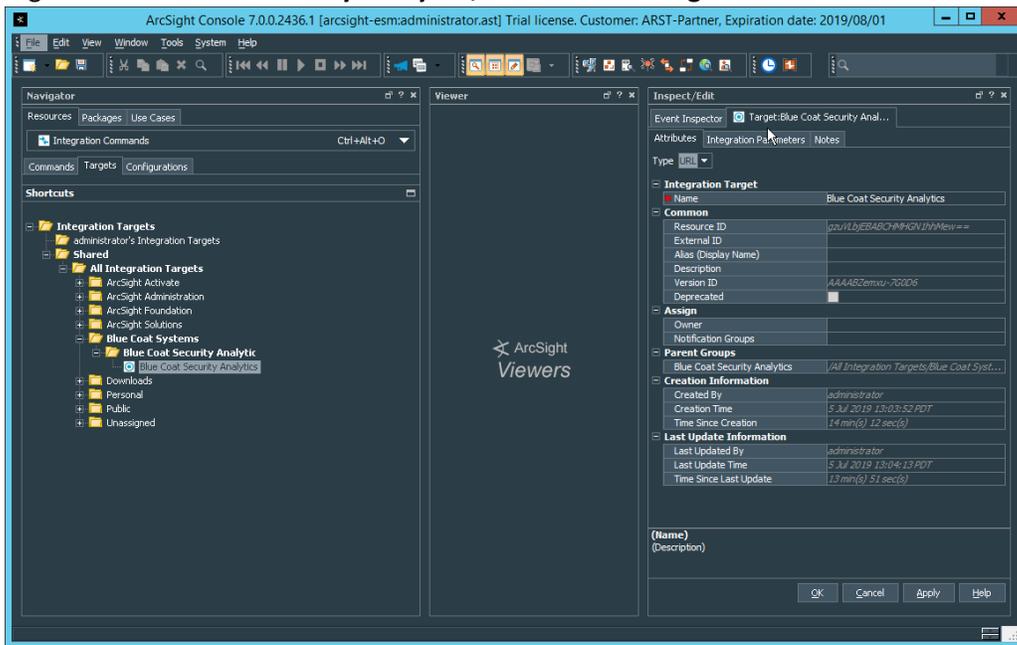
3014  
3015  
3016  
3017  
3018  
3019  
3020  
3021  
3022

12. Click **OK**.
13. When this completes, you can verify that the installation was successful by the existence of a **Blue Coat Systems** folder when you navigate to **Resources > Integration Commands > Commands > Shared > All Integration Commands**.
14. In the **Resources** tab of the **Navigation** pane, under **Integration Commands**, select the **Targets** tab.
15. Navigate to **Integration Targets > Shared > All Integration Targets > Blue Coat Systems > Blue Coat Security Analytic > Blue Coat Security Analytics**.



3023  
3024

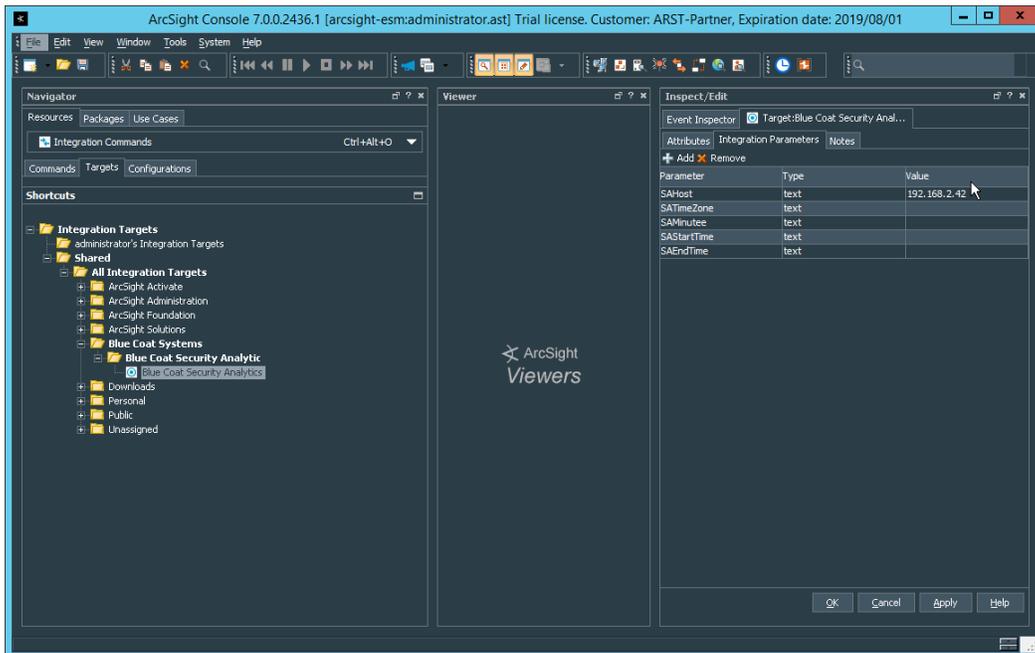
16. Right-click **Blue Coat Security Analytics**, and click **Edit Target**.



3025  
3026  
3027

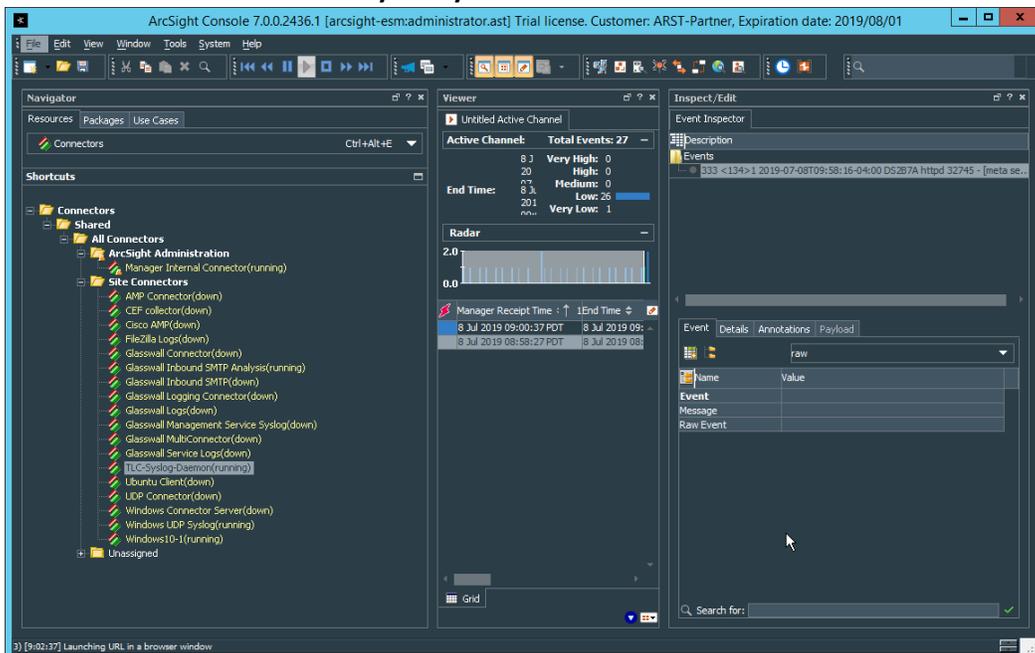
17. Click the **Integration Parameters** tab.

18. Replace the **SAHost** value with the IP address of Symantec Analytics.



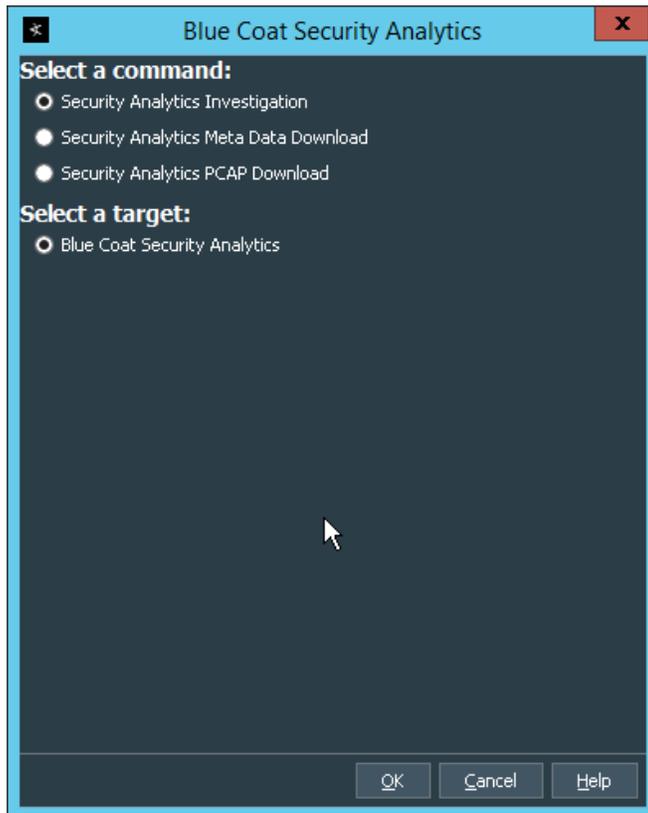
3028  
3029  
3030  
3031

19. Click **OK**.
20. To verify the functionality, right-click an event in any channel, and select **Integration Commands > Blue Coat Security Analytics**.



3032  
3033

21. Select **Security Analytics Investigation**.



3034  
3035  
3036

22. Click **OK**. This will open Security Analytics in the browser and perform a packet search based on the event parameters.

3037

## 2.24 Integration: Micro Focus ArcSight and Glasswall FileTrust

3038

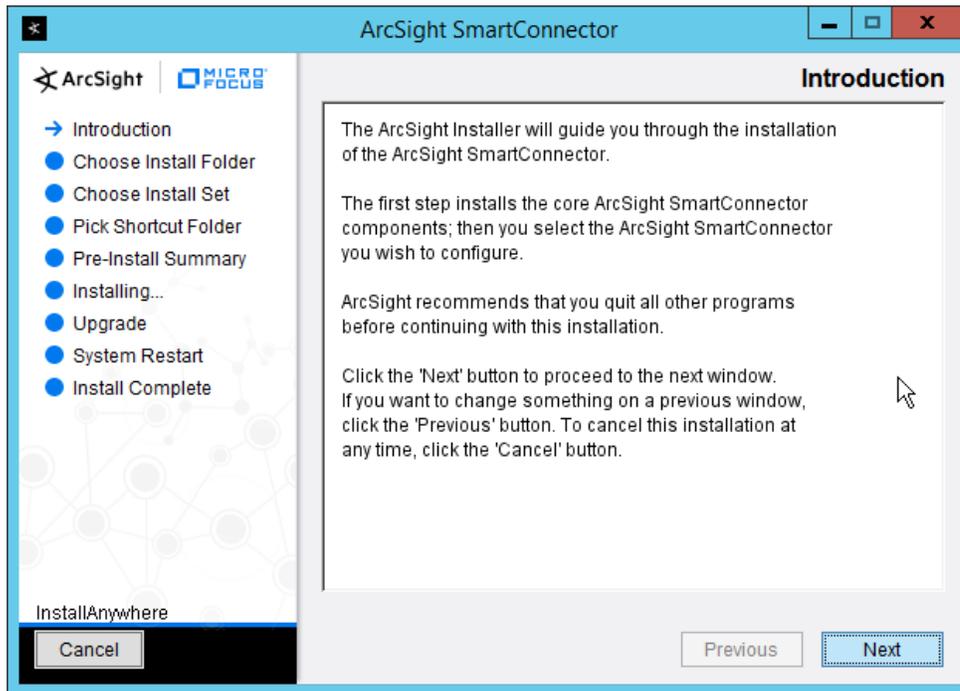
**Glasswall FileTrust for Email** stores its logs in *C:\Logging*, on the server running the **Glasswall** services.

3039

### 2.24.1 Install Micro Focus ArcSight

3040

1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on the same server as **Glasswall FileTrust**.

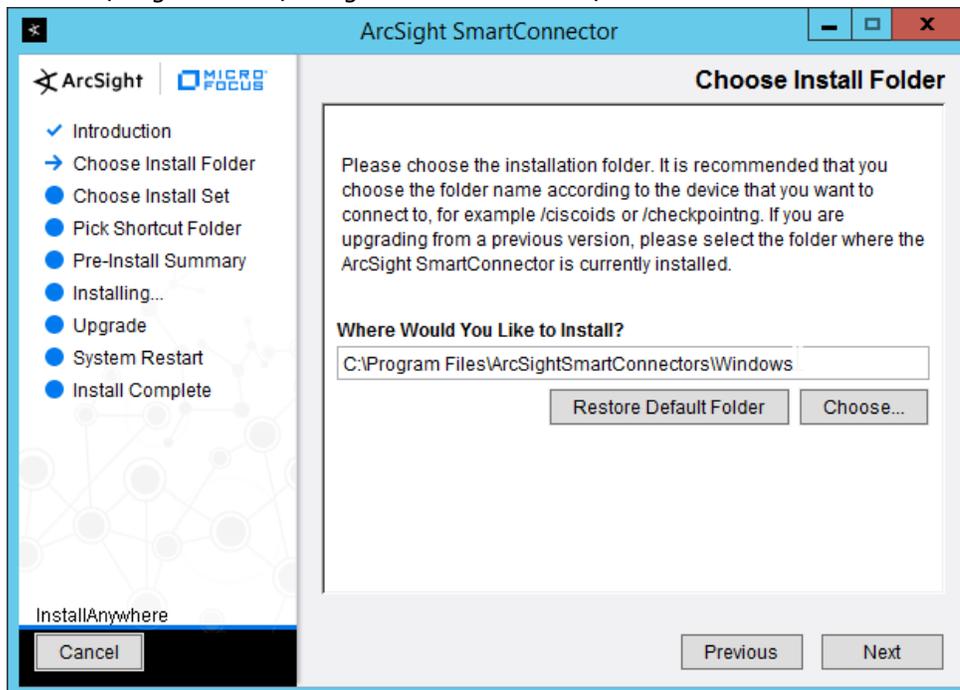


3041

3042

3043

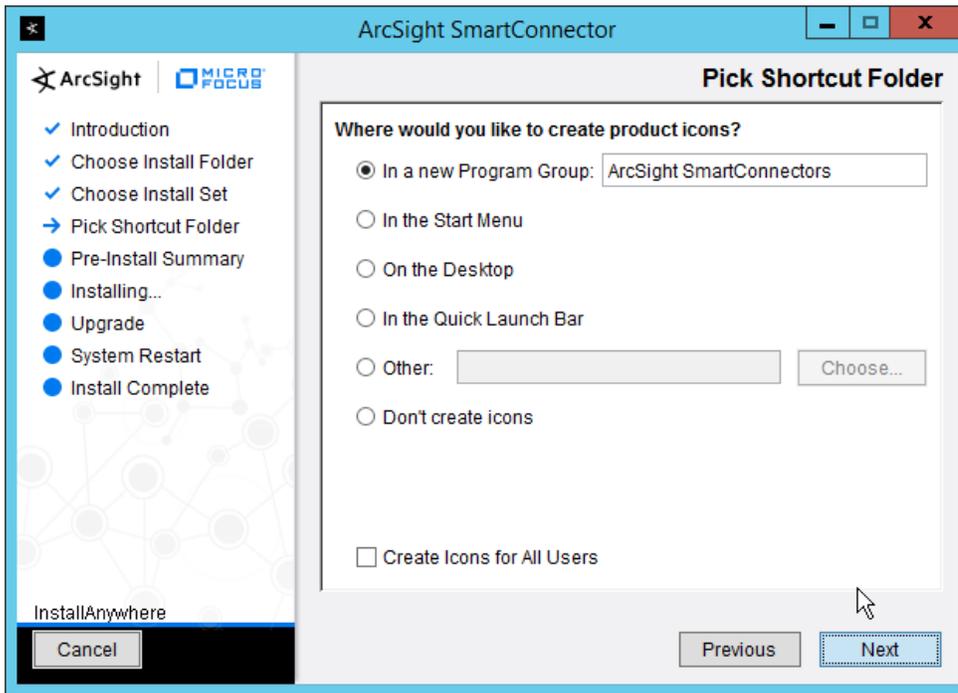
2. Click **Next**.
3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows*.



3044

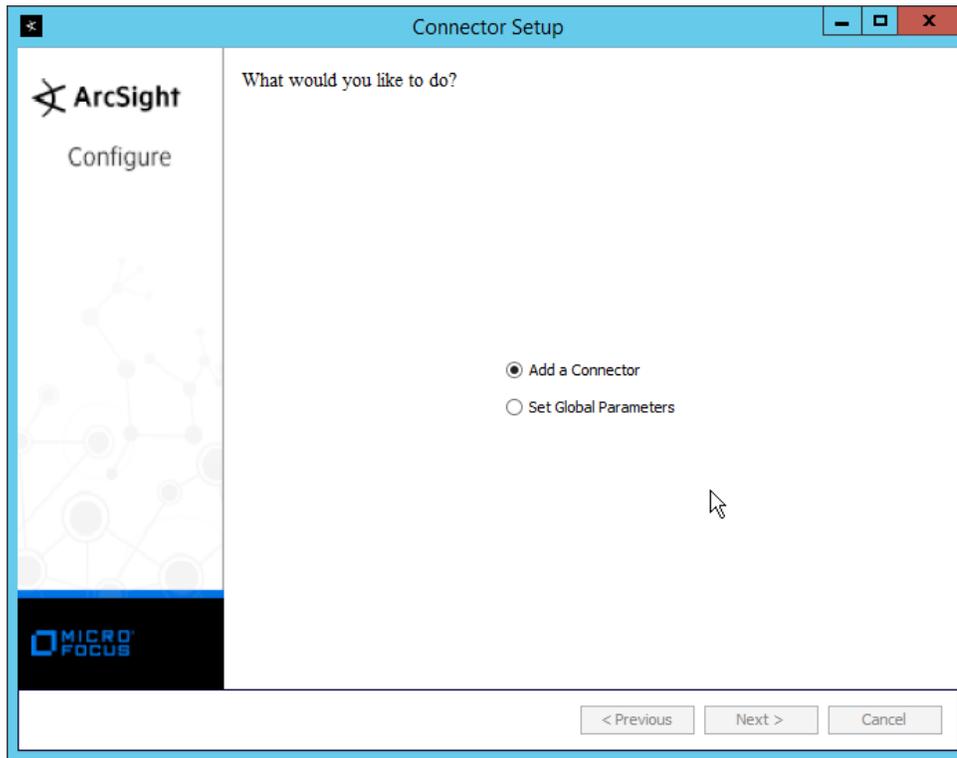
3045

4. Click **Next**.



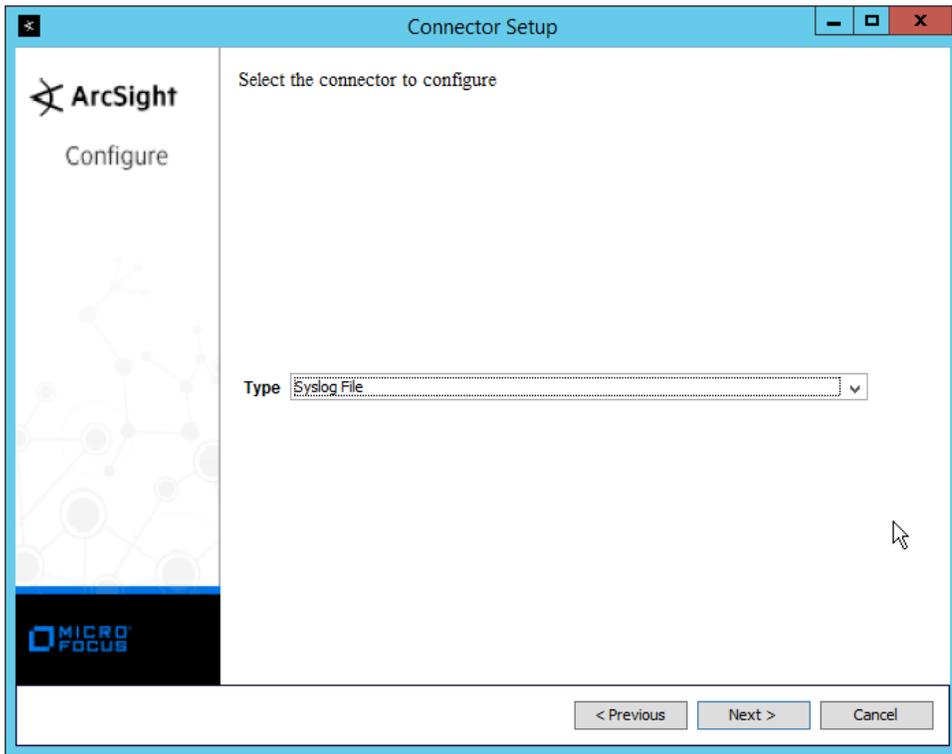
3046  
3047  
3048  
3049

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



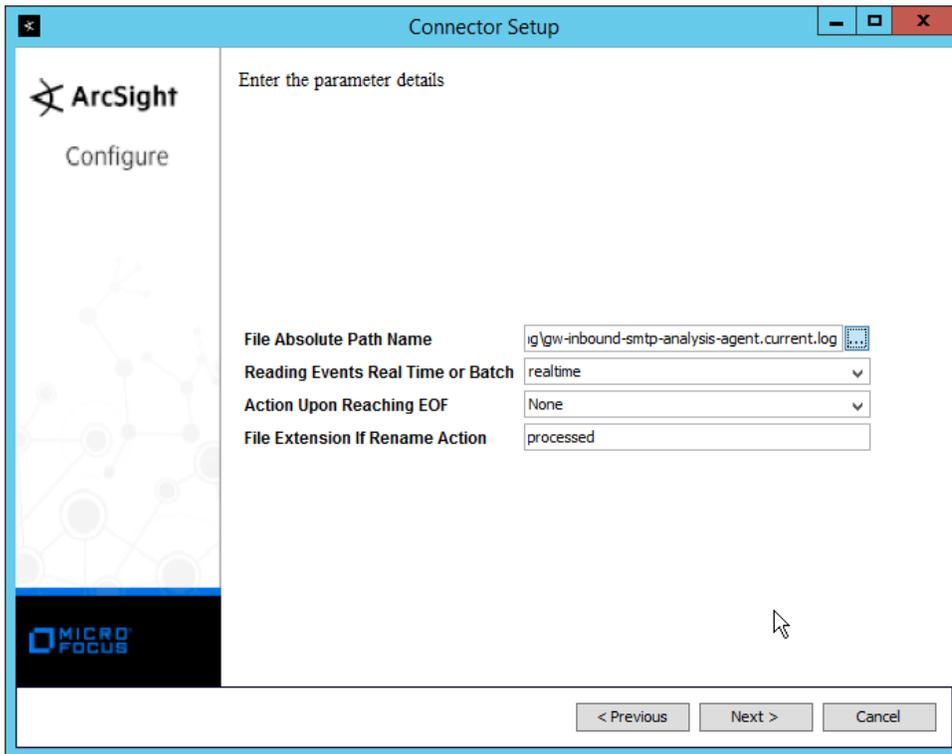
3050  
3051  
3052

8. Click **Next**.
9. Select **Syslog File**.



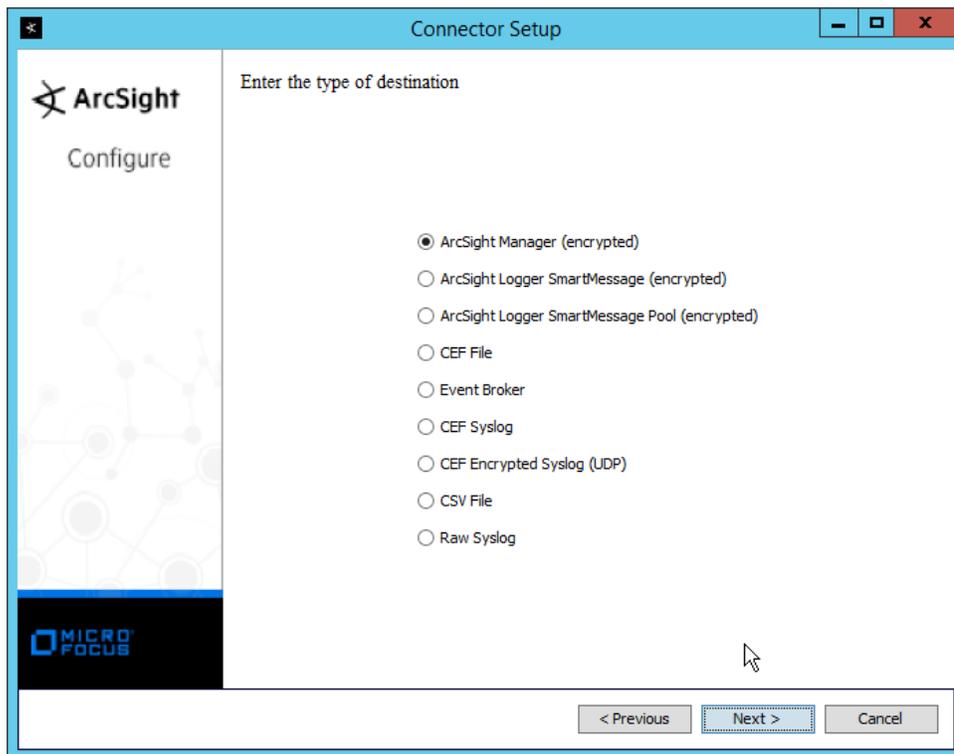
3053  
3054  
3055

10. Click **Next**.
11. Enter `C:\Logging\gw-inbound-smtp-analysis-agent.current.log` for **File Absolute Path Name**.



3056  
3057  
3058

12. Click **Next**.
13. Select **ArcSight Manager (encrypted)**.



3059  
3060  
3061

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

3062  
3063  
3064

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

Connector Setup

ArcSight  
Configure

Enter the connector details

Name: Glasswall Inbound SMTP Analysis

Location: [Empty]

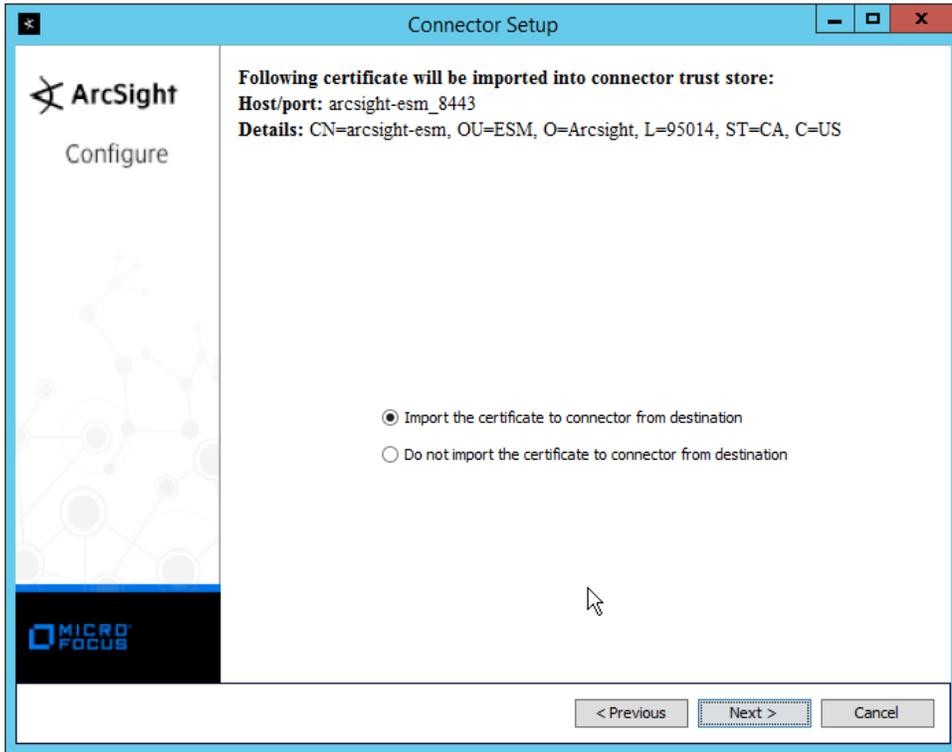
DeviceLocation: [Empty]

Comment: [Empty]

< Previous   Next >   Cancel

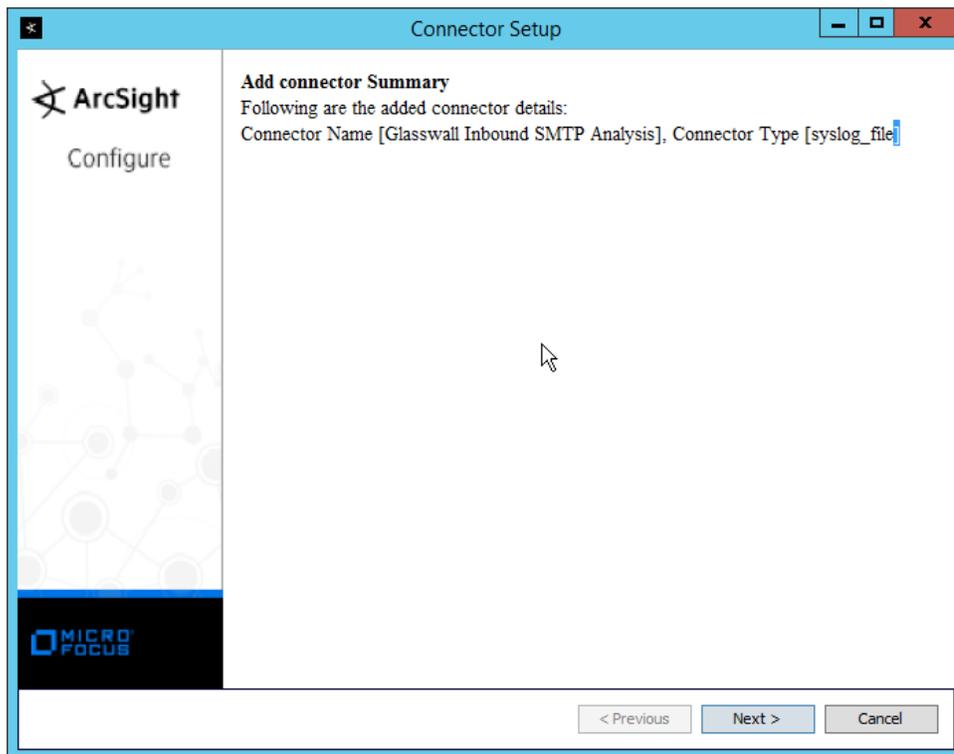
3065  
3066  
3067

- 18. Click **Next**.
- 19. Select **Import the certificate to connector from destination**.



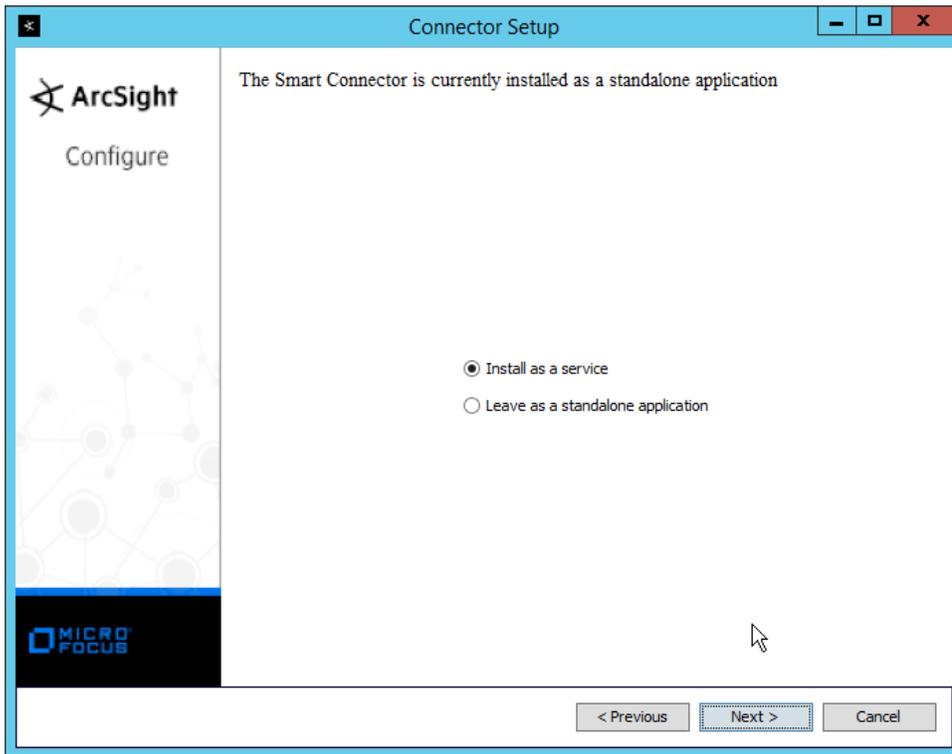
3068  
3069

20. Click **Next**.



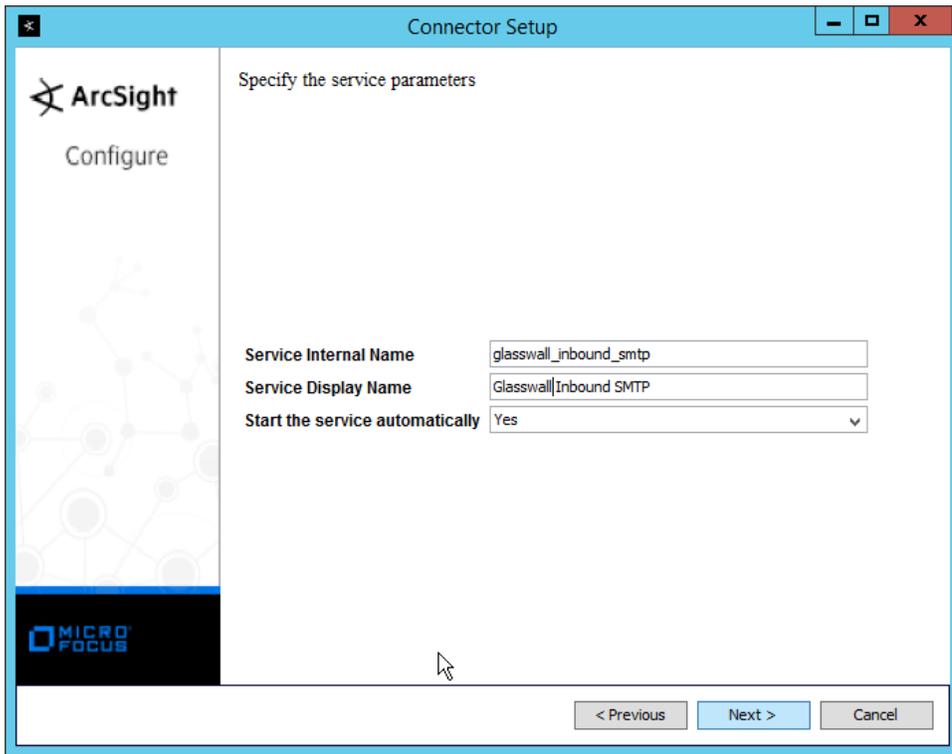
3070  
3071  
3072

21. Click **Next**.
22. Select **Install as a service**.



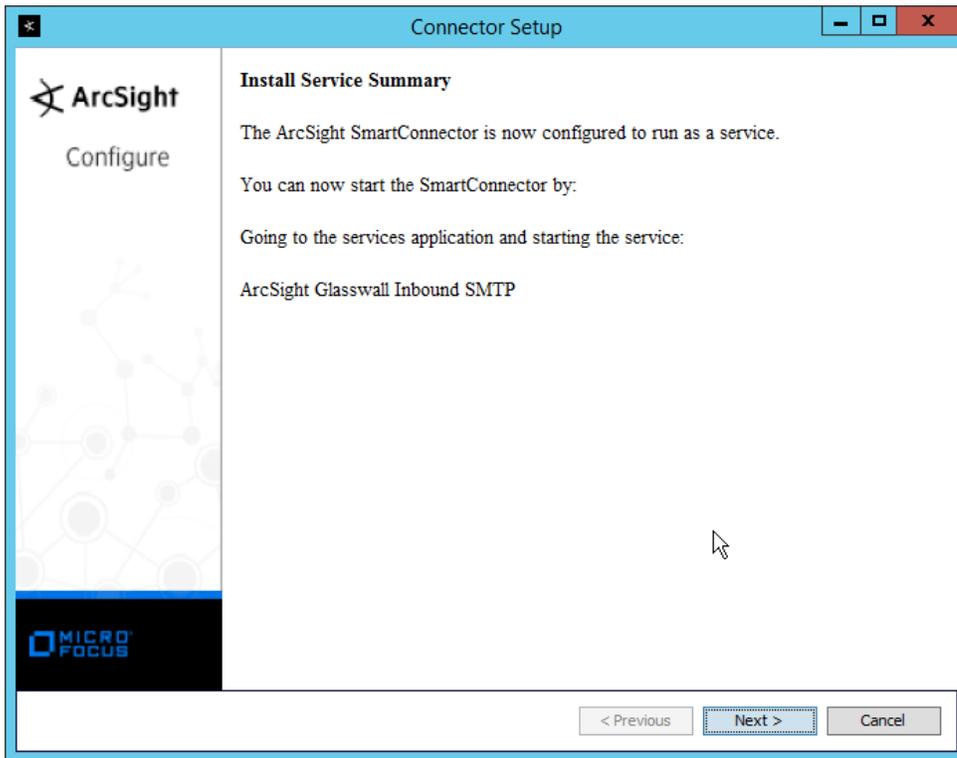
3073  
3074  
3075  
3076

23. Click **Next**.
24. Change the service parameters to more appropriate names, because multiple connectors need to be installed on this server.



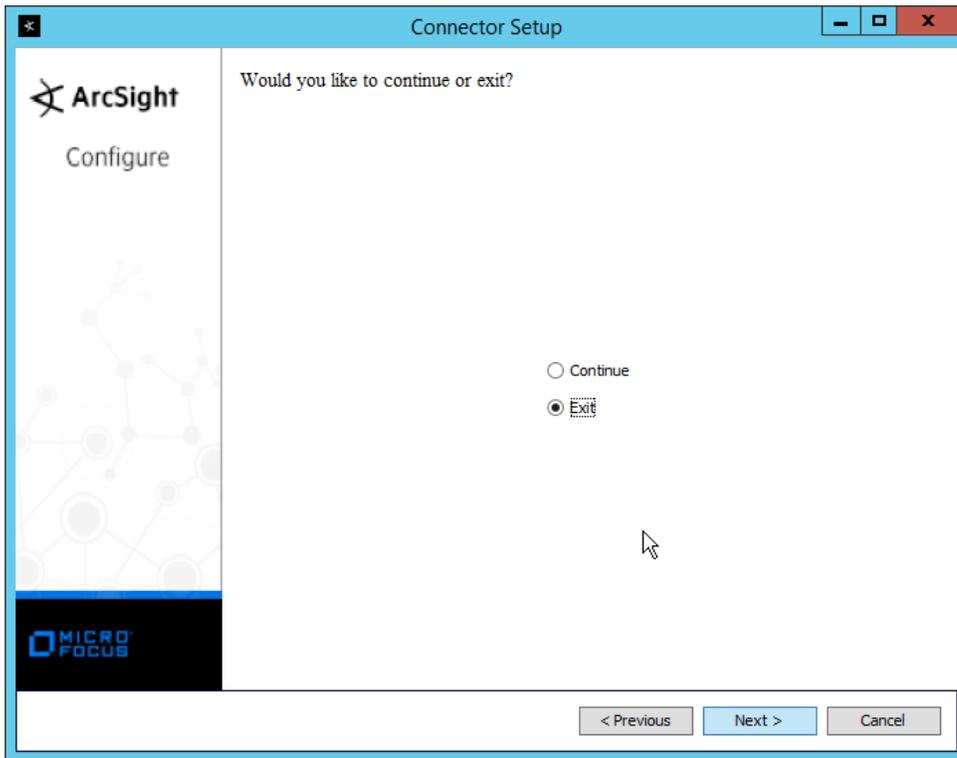
3077  
3078

25. Click **Next**.



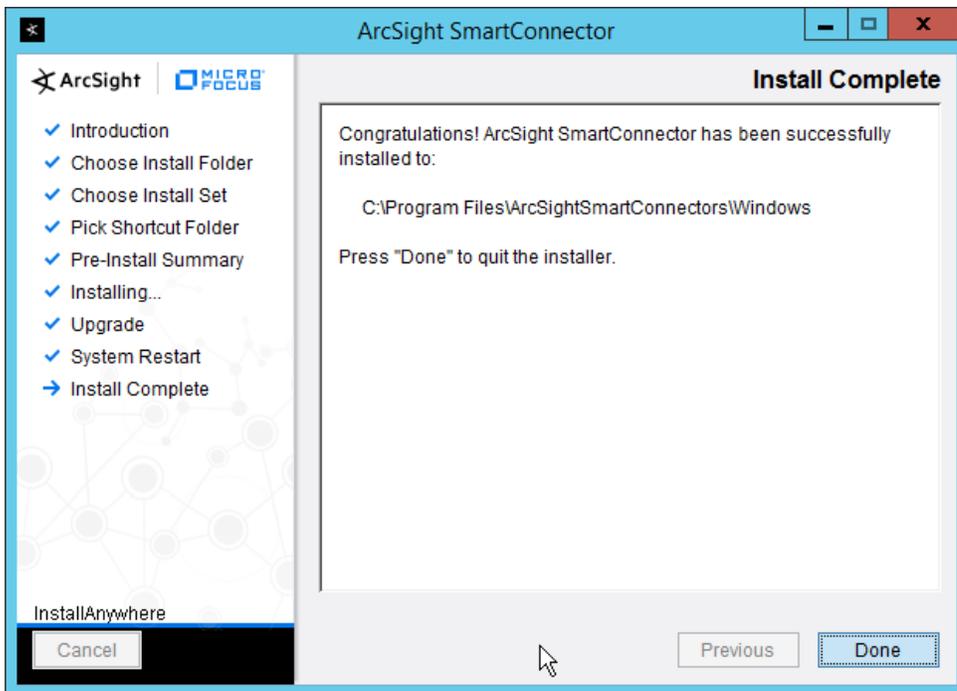
3079  
3080  
3081

- 26. Click **Next**.
- 27. Select **Exit**.



3082  
3083

28. Click **Next**.



3084  
3085

29. Click **Done**.

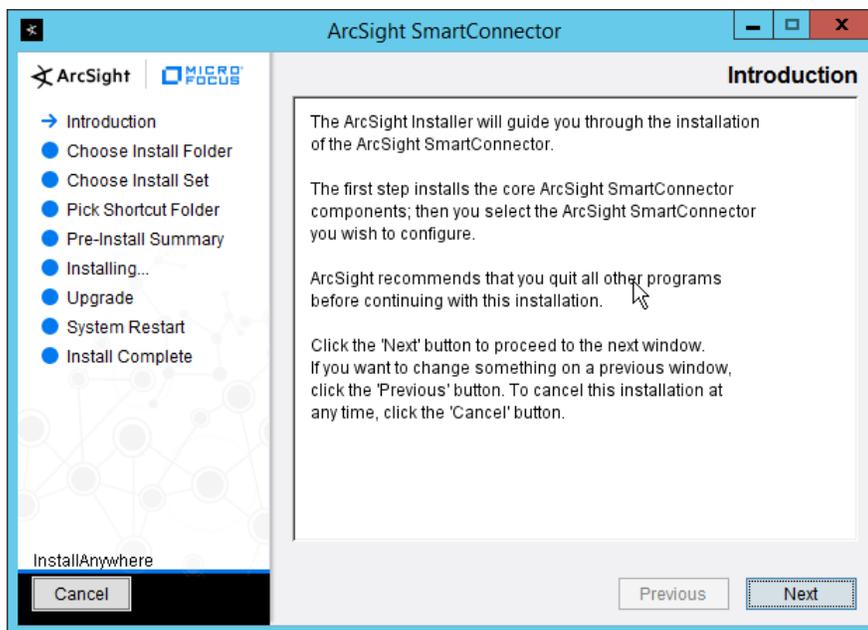
- 3086 30. Repeat steps 1-29 for the other three “current” log files in *C:\Logging*, with the following  
 3087 caveats:
- 3088 a. Replace *C:\Program Files\ArcSightSmartConnectors\Windows* with a different folder  
 3089 name for each connector.
  - 3090 b. Replace *C:\Logging\gw-inbound-smtp-analysis-agent.current.log* with the appropriate  
 3091 log file.
    - 3092 i. *C:\Logging\gw-management-service.current.log*
    - 3093 ii. *C:\Logging\gw-file-analysis-process-InboundSMTPAgent-0.current.log*
    - 3094 iii. *C:\Logging\gw-administration-console.current.log*
  - 3095 c. Replace the **Name** of the connector in its identifying details.
  - 3096 d. Replace the **service parameters** with different names so that the services do not  
 3097 conflict.

## 3098 2.25 Integration: Micro Focus ArcSight and Cisco Stealthwatch

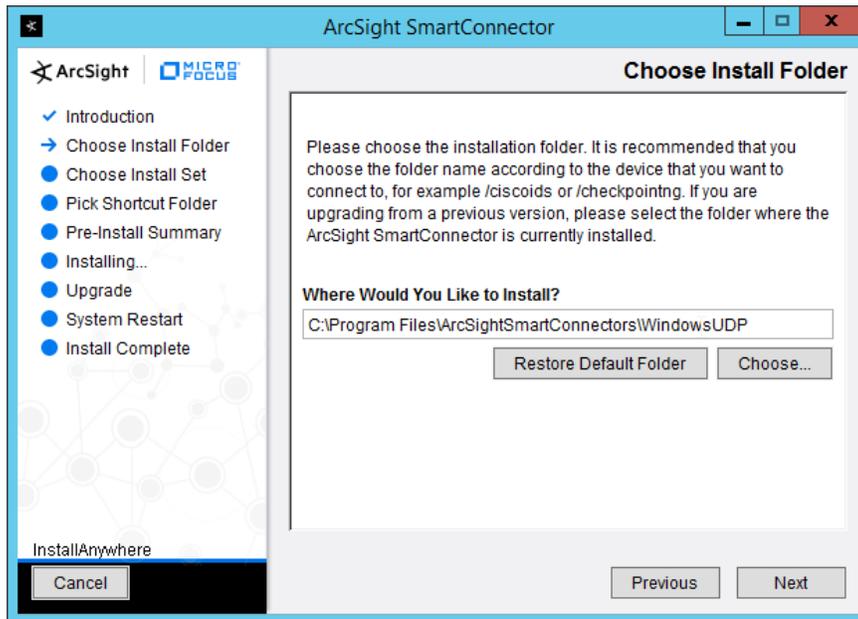
3099 This section will detail the forwarding of logs from **Cisco Stealthwatch** to **Micro Focus ArcSight**.

### 3100 2.25.1 Install Micro Focus ArcSight

- 3101 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running **Cisco**  
 3102 **Stealthwatch**.

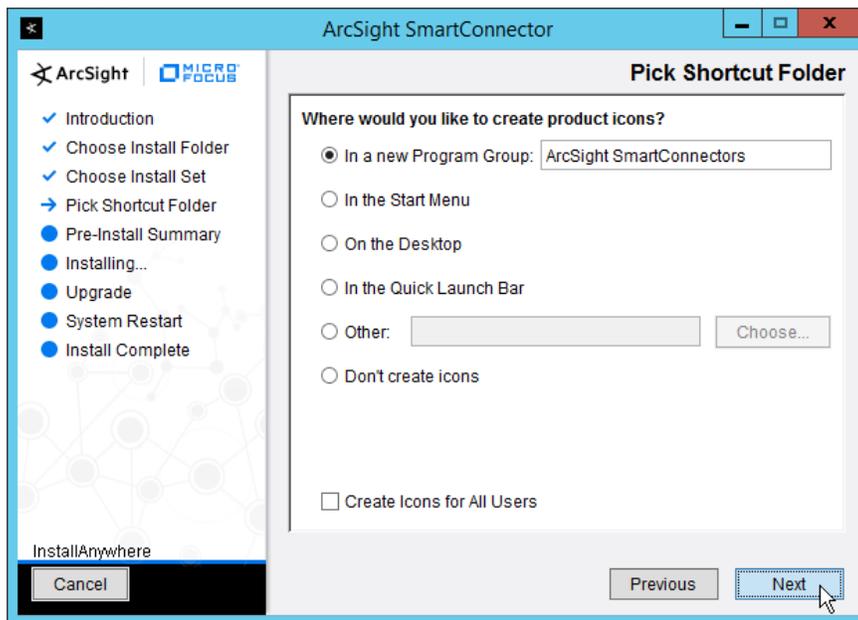


- 3103 2. Click **Next**.
- 3104 3. Enter *C:\Program Files\ArcSightSmartConnectors\WindowsUDP*.
- 3105



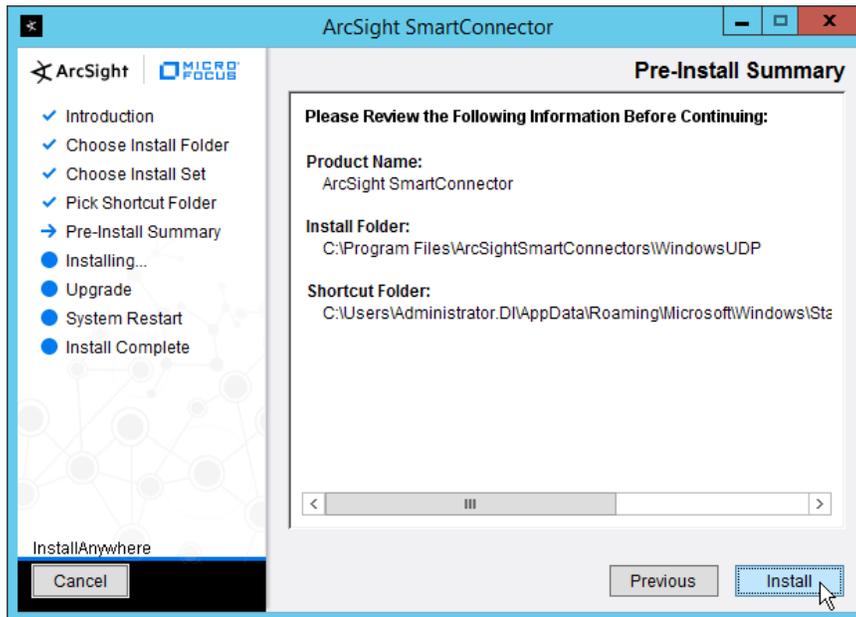
3106  
3107

4. Click **Next**.



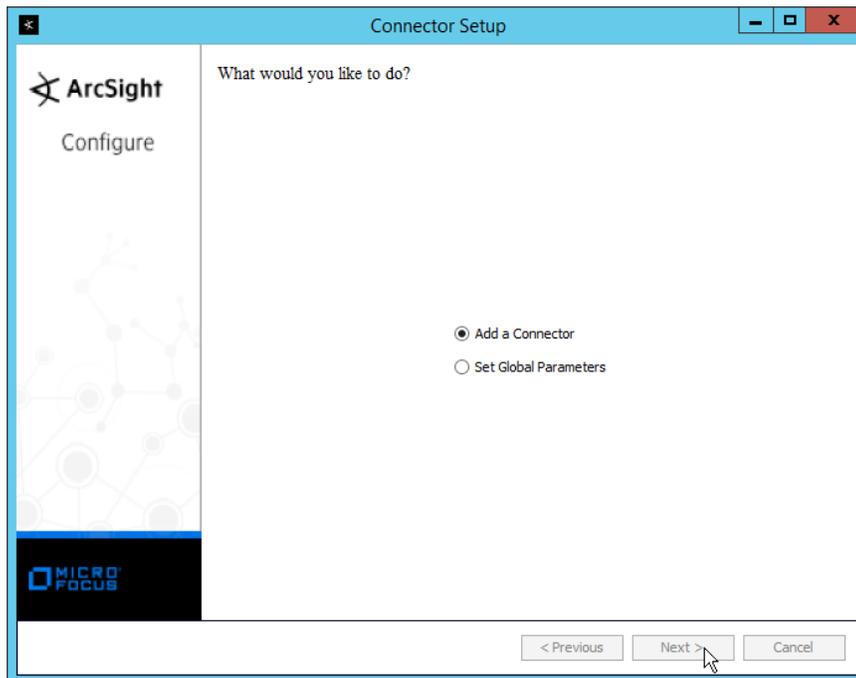
3108  
3109

5. Click **Next**.



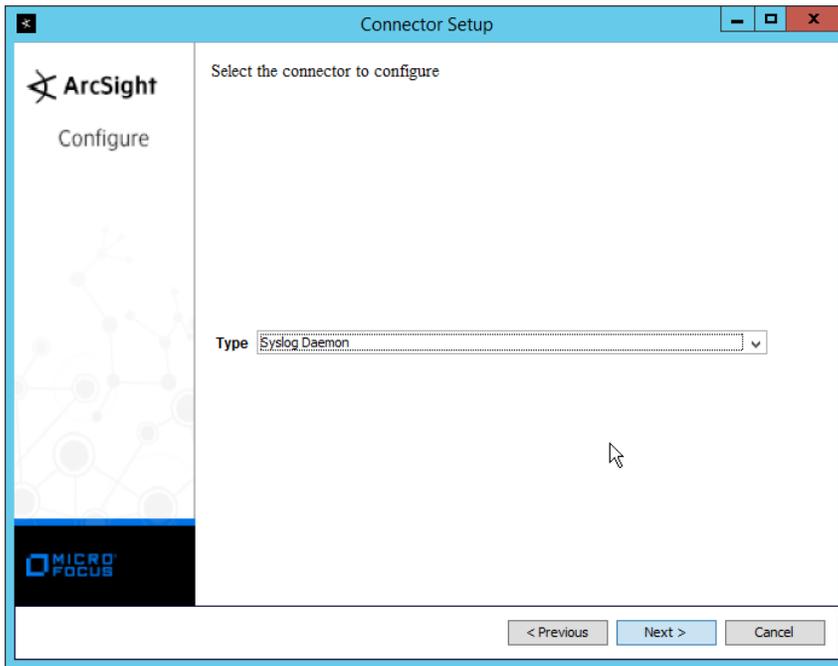
3110  
3111  
3112

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



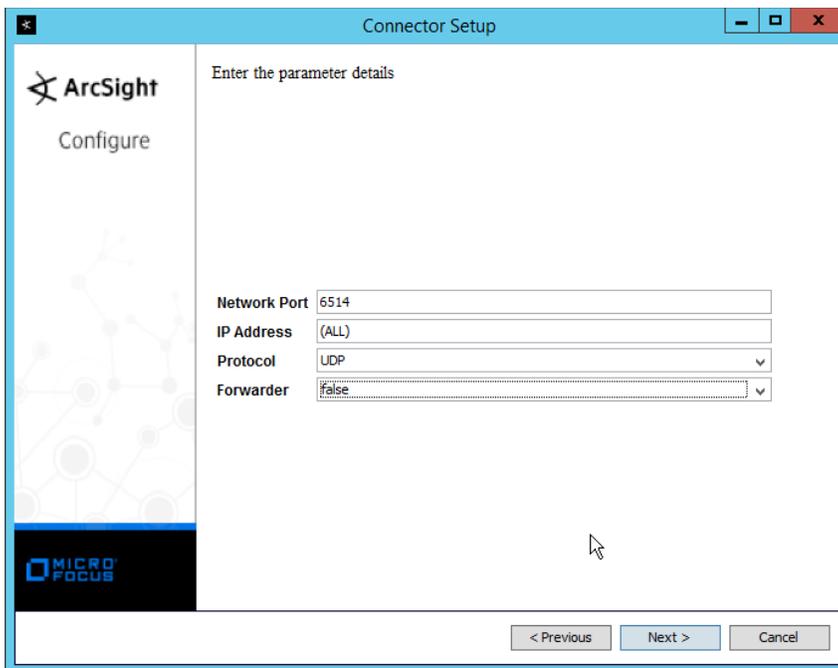
3113  
3114  
3115

8. Click **Next**.
9. Select **Syslog Daemon**.



3116  
3117  
3118  
3119  
3120

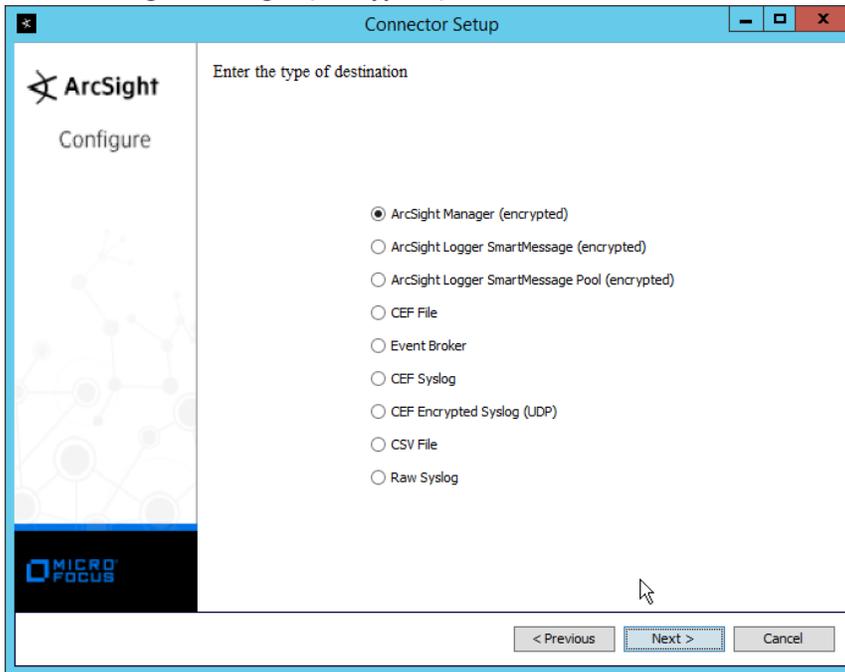
- 10. Click **Next**.
- 11. Enter an unused port for the daemon to run on. (Ensure that this port is allowed through the firewall.)
- 12. Select **UDP** for **Protocol**.



3121  
3122

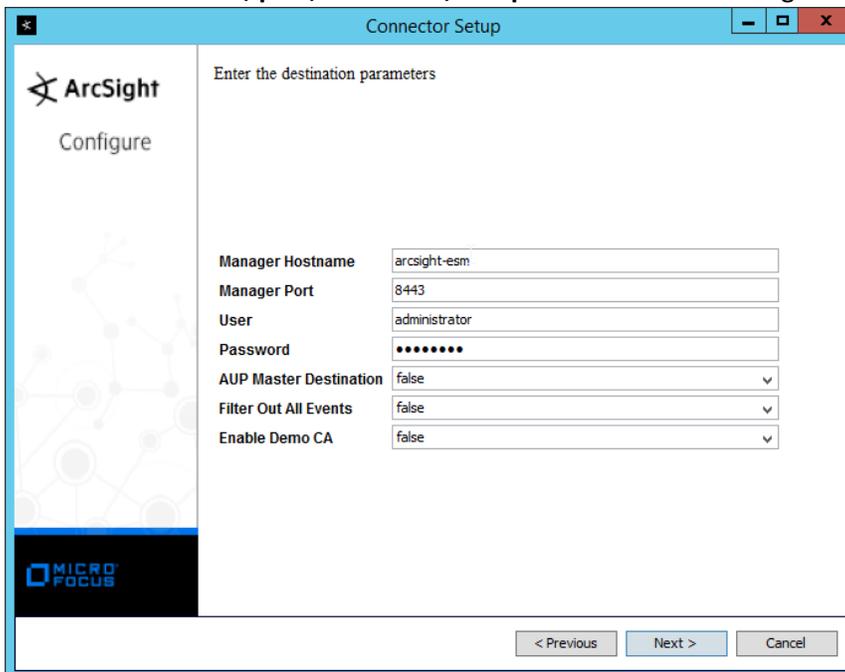
- 13. Click **Next**.

3123 14. Select **ArcSight Manager (encrypted)**.



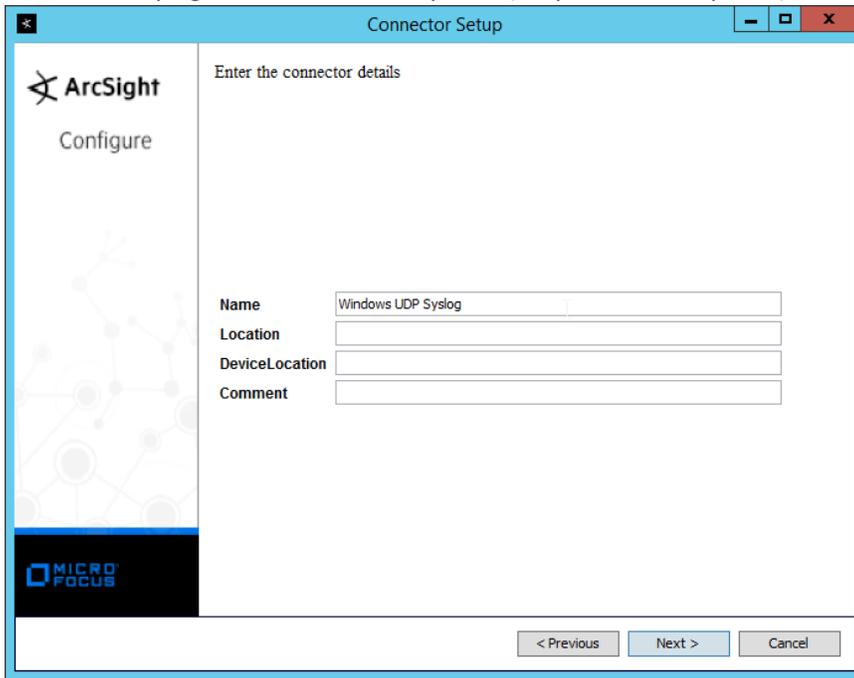
3124 15. Click **Next**.

3125 16. Enter the **hostname, port, username, and password** for the ArcSight ESM server.



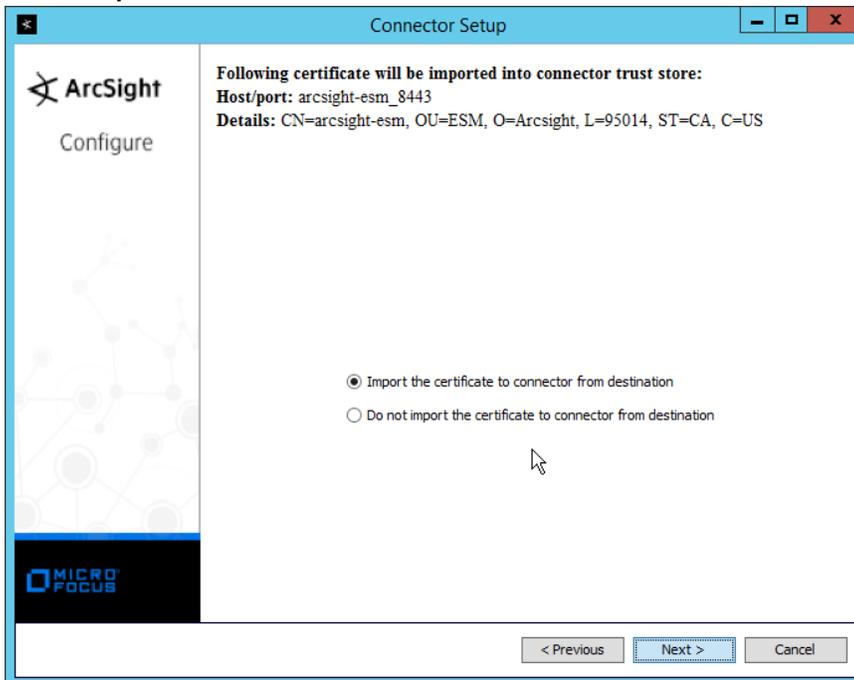
3127 17. Click **Next**.

3129 18. Enter identifying details about the system (only **Name** is required).

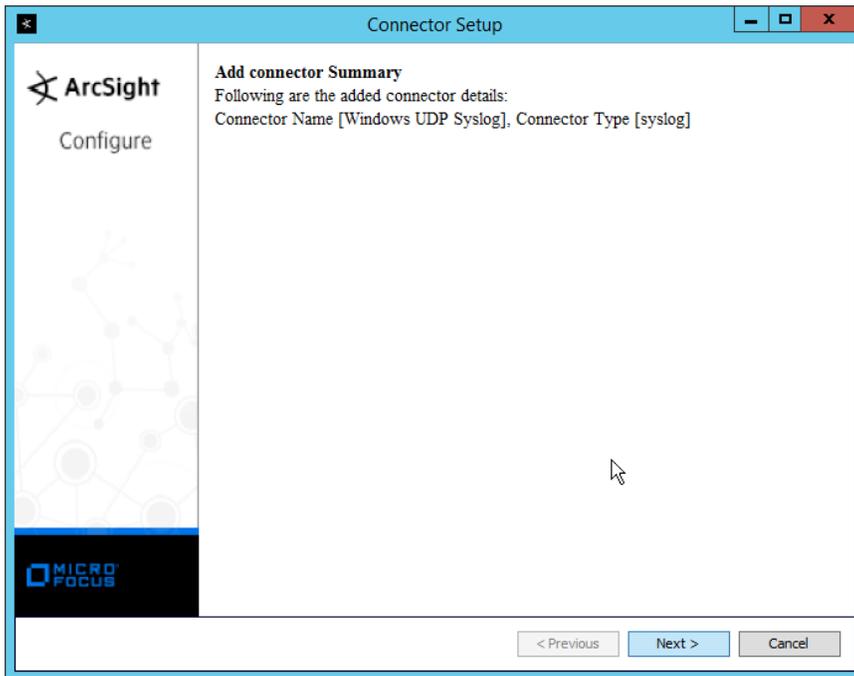


3130 19. Click **Next**.

3131 20. Select **Import the certificate to connector from destination**.

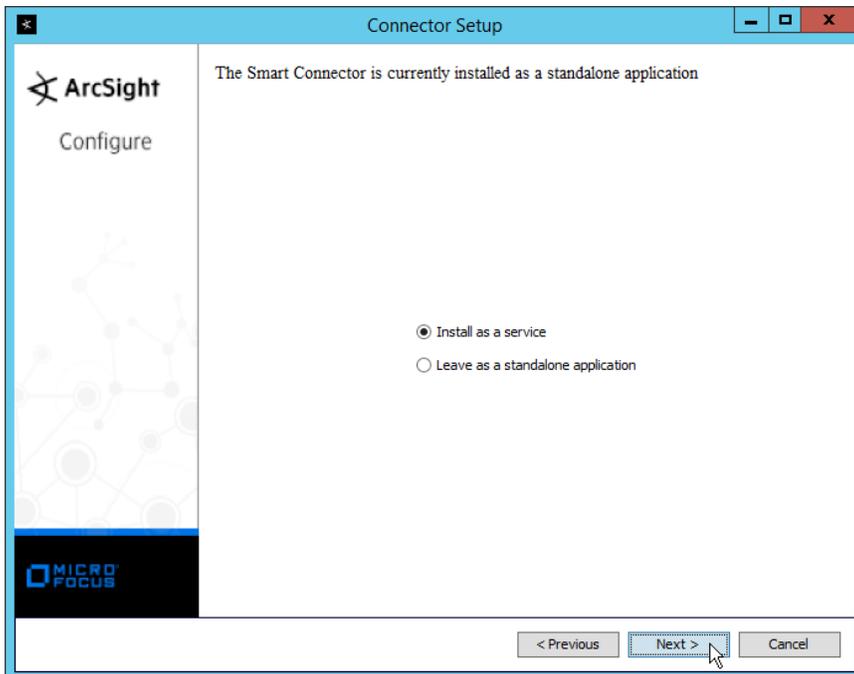


3133 21. Click **Next**.



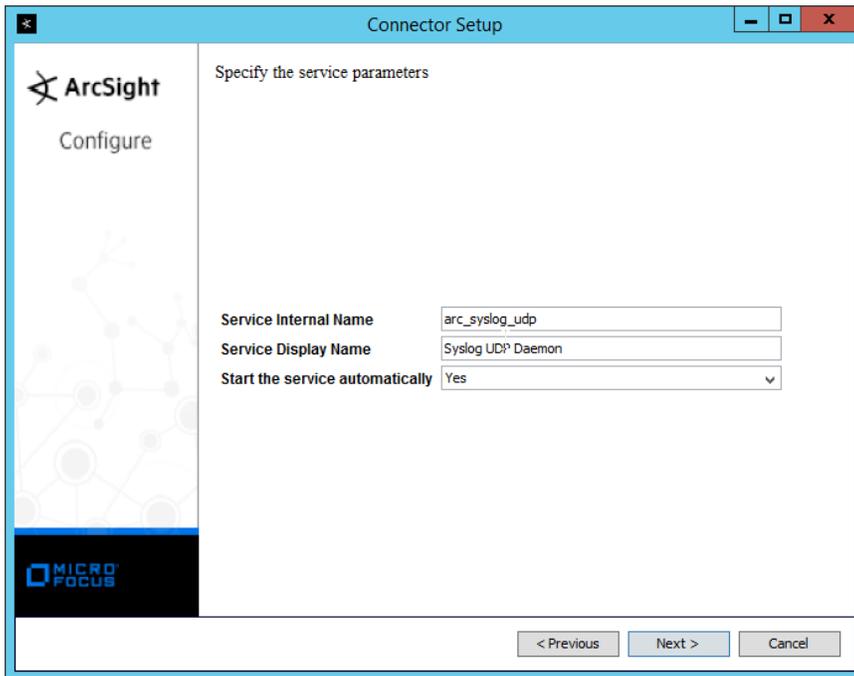
3135 22. Click **Next**.

3136 23. Select **Install as a service**.

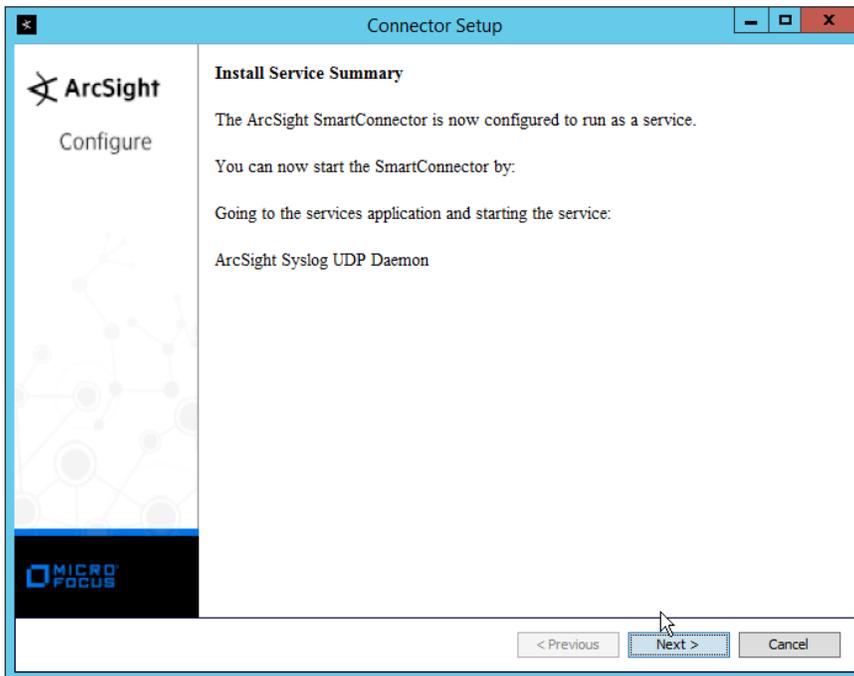


3137 24. Click **Next**.

3138 25. Enter a service name and display name.

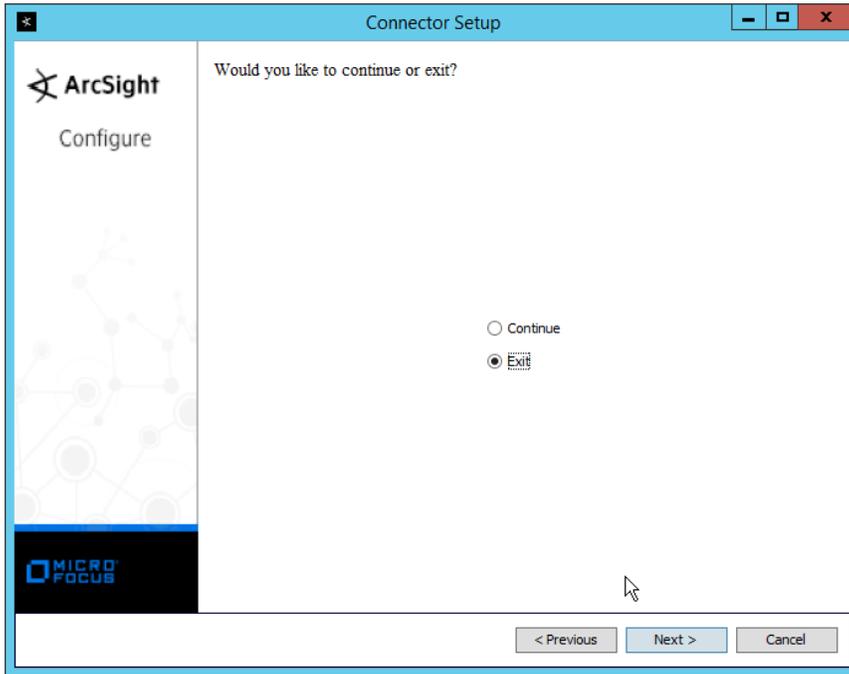


3139 26. Click **Next**.

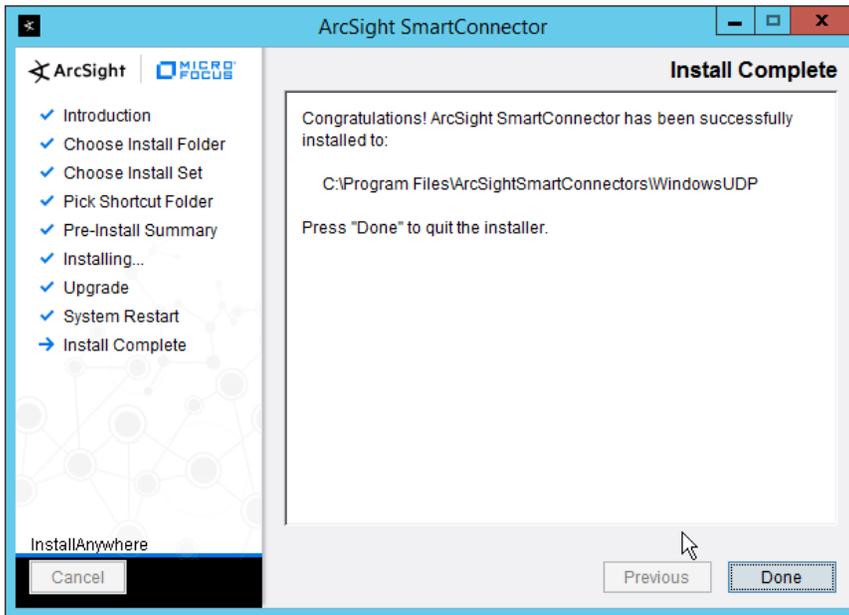


3140 27. Click **Next**.

3141 28. Select **Exit**.



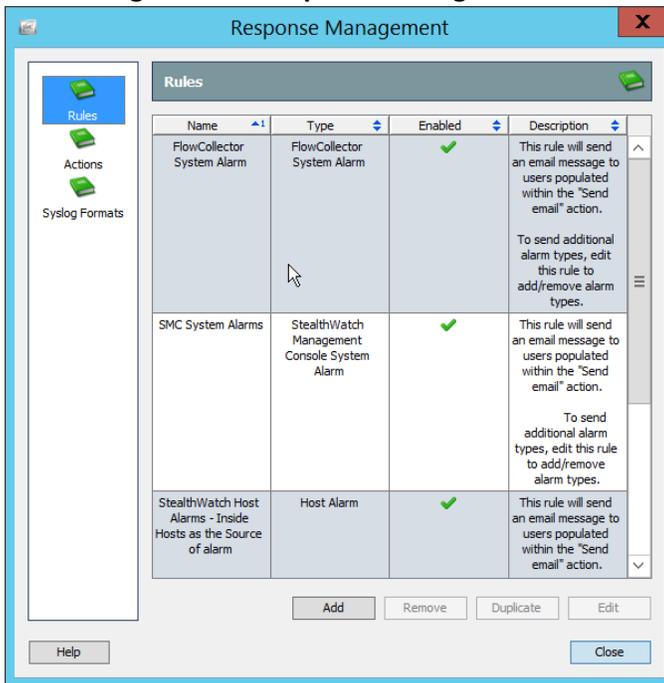
3142 29. Click **Next**.



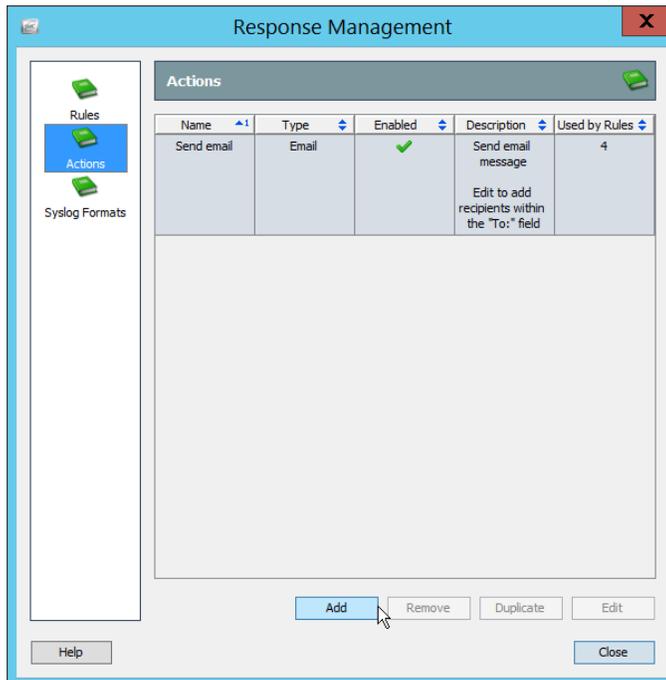
3143 30. Click **Done**.

## 3144 2.25.2 Configure Cisco Stealthwatch

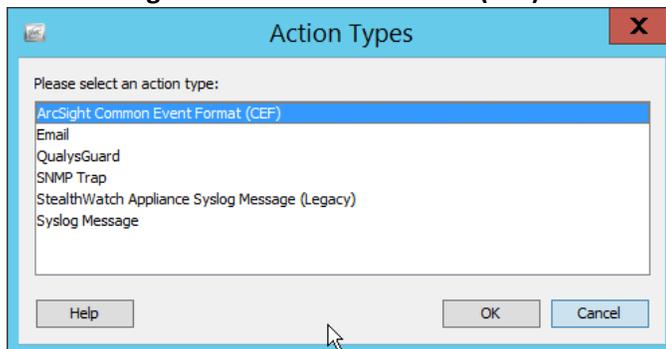
- 3145 1. Log in to the **Cisco Stealthwatch Management Console** desktop interface. (This can be  
3146 downloaded from the web interface and run using **javaws.exe**. You may need to add the site to  
3147 your Java exceptions in **Control Panel > Java**.)  
3148 2. Click **Configuration > Response Management**.



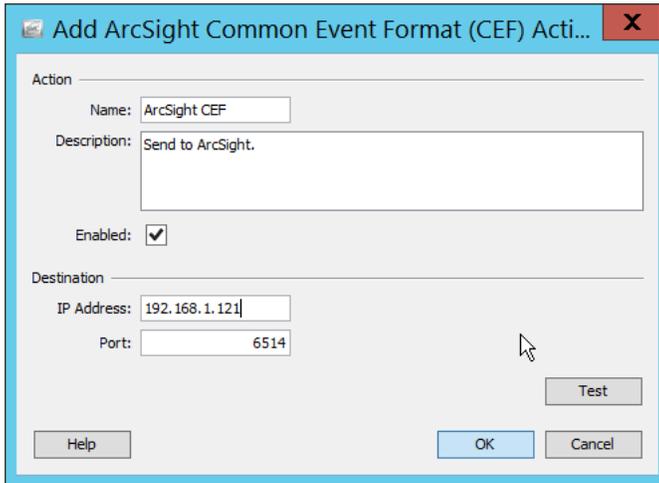
- 3149 3. Click **Actions**.



- 3150 4. Click **Add**.
- 3151 5. Select **ArcSight Common Event Format (CEF)**.

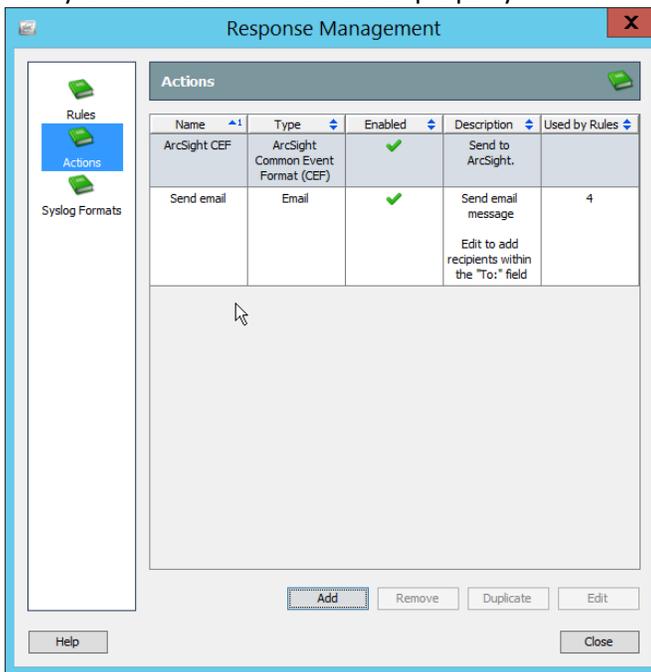


- 3152 6. Click **OK**.
- 3153 7. Enter a **name** for the **Action**.
- 3154 8. Enter a **description**.
- 3155 9. Enter the **IP address** of the server with the UDP ArcSight Connector that you just created.
- 3156 10. Enter the **port** used in the UDP ArcSight Connector that you just created.
- 3157 11. (Optional) Click **Test** to send a test message to ArcSight, and verify that ArcSight receives the
- 3158 message.

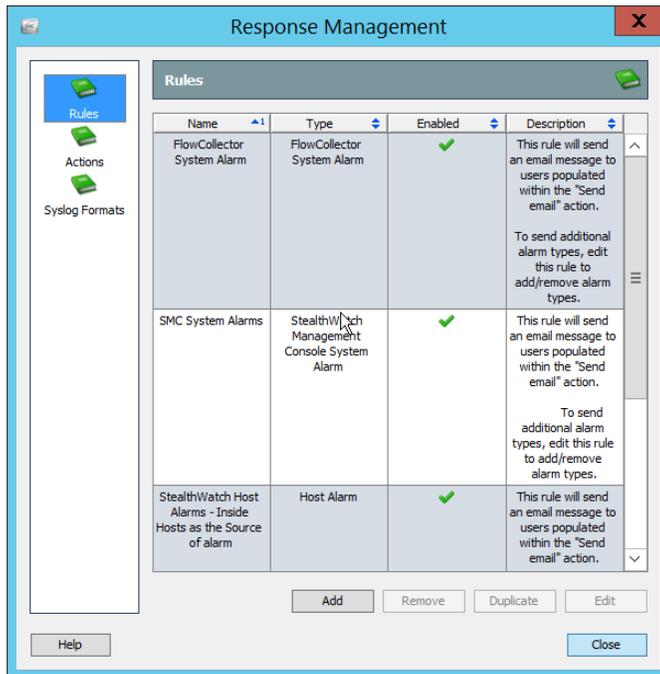


3159 12. Click **OK**.

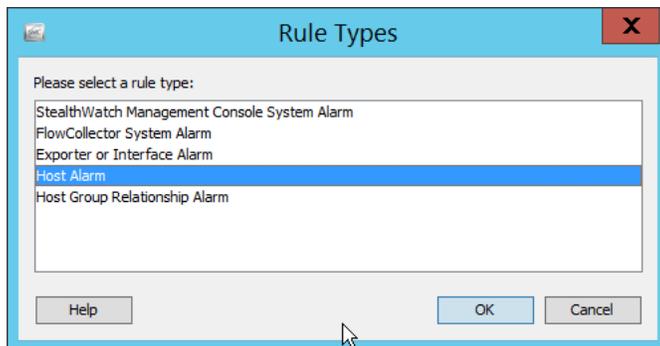
3160 13. Verify that the action was created properly.



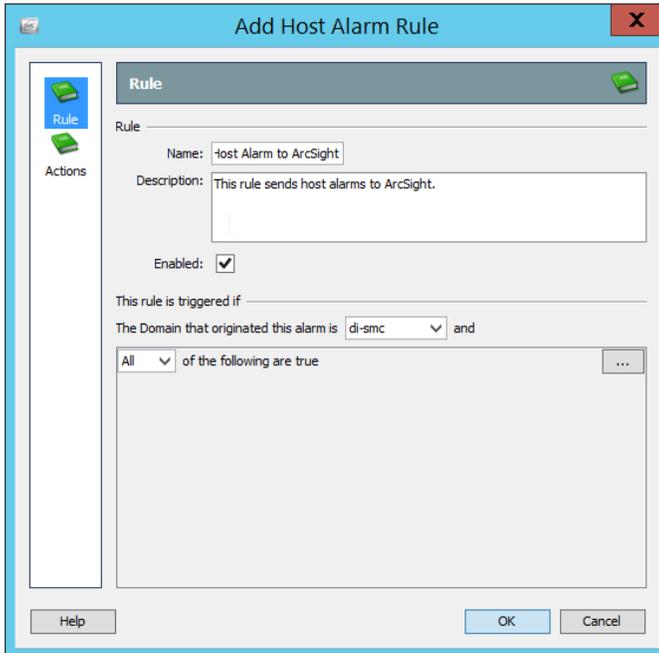
3161 14. Click **Rules**.



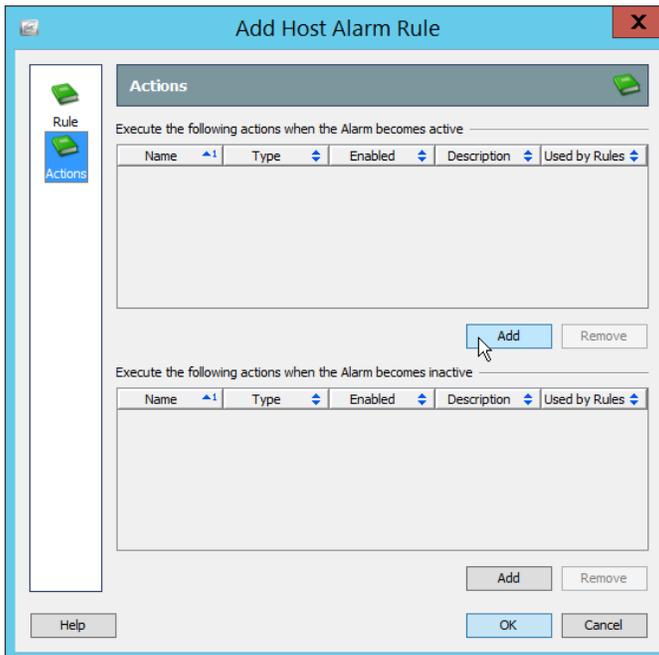
- 3162 15. Click **Add**.
- 3163 16. Select **Host Alarm**.



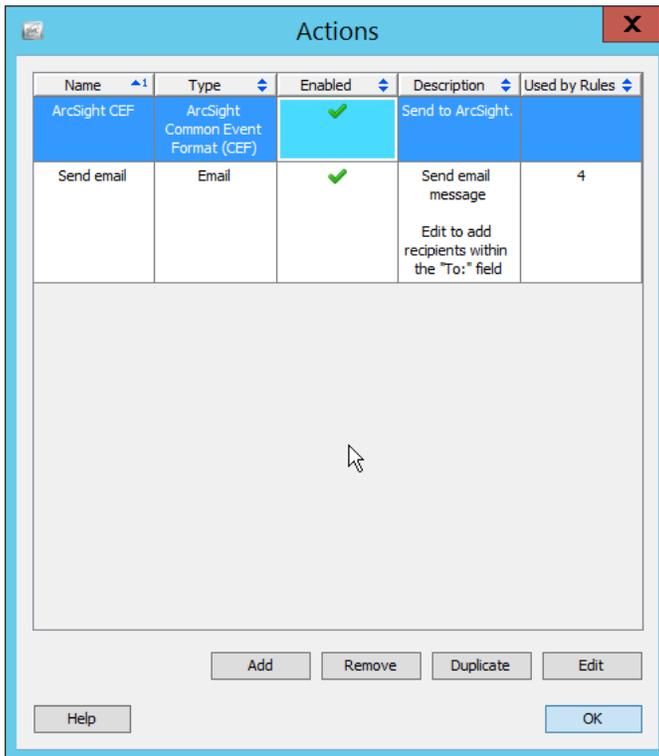
- 3164 17. Click **OK**.
- 3165 18. Enter a **name**.
- 3166 19. Enter a **description**.



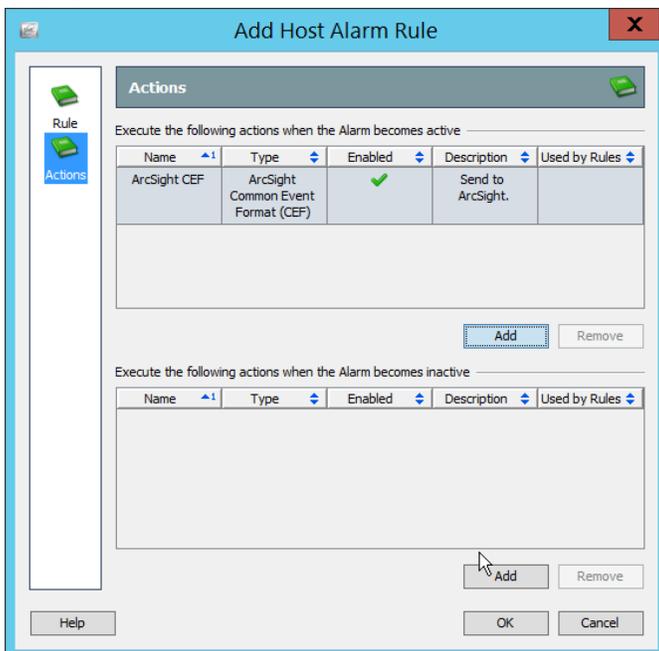
3167 20. Click **Actions**.



3168 21. Click the **Add** button for the top section; this adds an action when the alarm becomes active.  
 3169 22. Select the ArcSight CEF rule you just created.

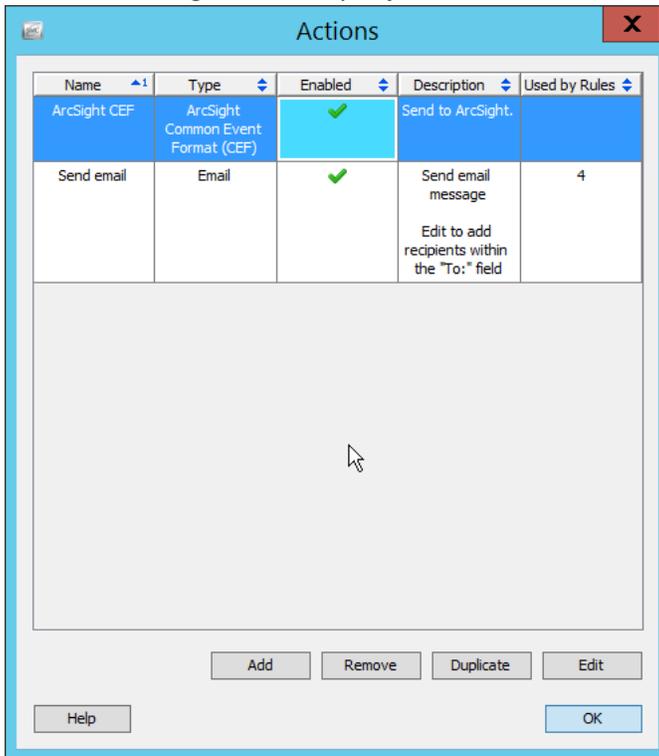


3170 23. Click **OK**.

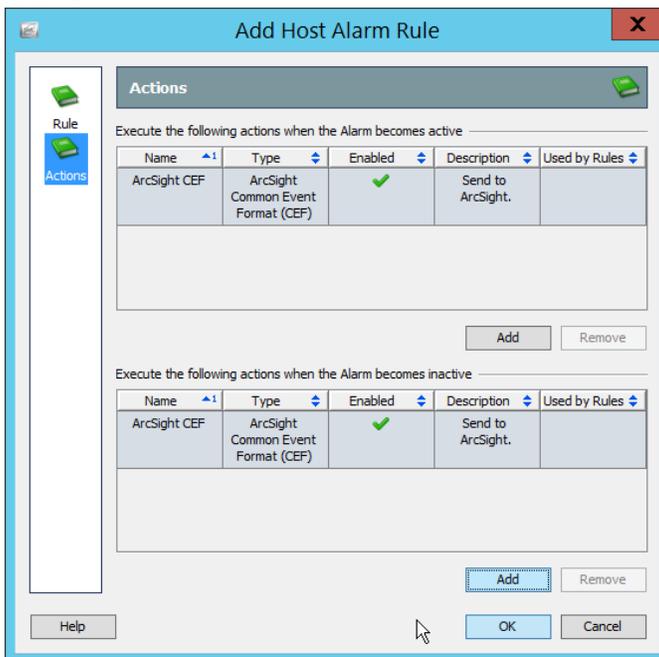


3171 24. Click the **Add** button for the bottom section; this adds an action when the alarm becomes  
3172 inactive.

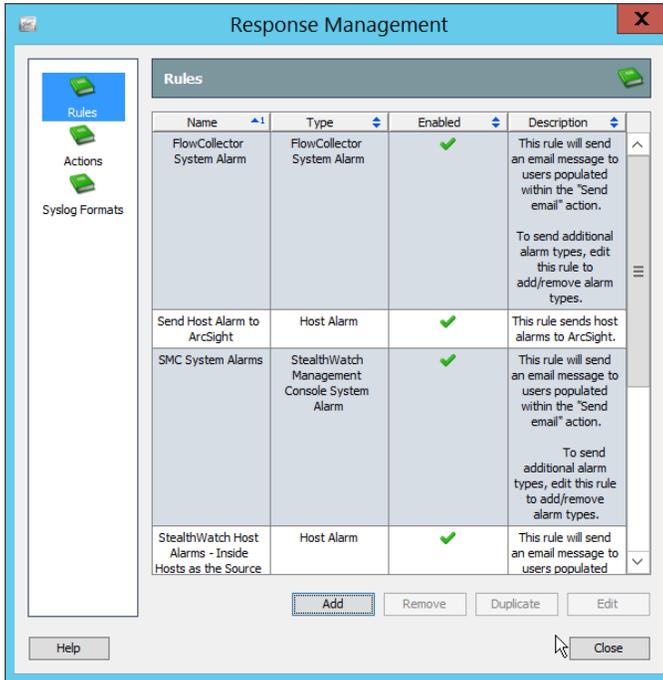
3173 25. Select the ArcSight CEF rule you just created.



3174 26. Click OK.



3175 27. Click **OK**.



3176 28. Click **Close**.

## 3177 **Appendix A** List of Acronyms

<b>AD</b>	Active Directory
<b>AMP</b>	Advanced Malware Protection
<b>CEF</b>	Common Event Format
<b>DNS</b>	Domain Name System
<b>DSP</b>	Directory Services Protector
<b>ESM</b>	Enterprise Security Manager
<b>ICA</b>	Information Centric Analytics
<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>MSSQL</b>	Microsoft SQL
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NIST</b>	National Institute of Standards and Technology
<b>OS</b>	Operating System
<b>PEM</b>	Privacy Enhanced Mail
<b>SAN</b>	Subject Alternative Name
<b>SMC</b>	Stealthwatch Management Console