

NIST SPECIAL PUBLICATION 1800-26

Data Integrity

Detecting and Responding to Ransomware and Other Destructive Events

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jennifer Cawthra
Michael Ekstrom
Lauren Lusty
Julian Sexton
John Sweetnam

DRAFT

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



NIST SPECIAL PUBLICATION 1800-26

Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jennifer Cawthra
National Cybersecurity Center of Excellence
NIST

Michael Ekstrom
Lauren Lusty
Julian Sexton
John Sweetnam
The MITRE Corporation
McLean, Virginia

DRAFT

January 2020



U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

NIST SPECIAL PUBLICATION 1800-26A

Data Integrity

Detecting and Responding to Ransomware and Other Destructive Events

Volume A: Executive Summary

Jennifer Cawthra

National Cybersecurity Center of Excellence
NIST

Michael Ekstrom

Lauren Lusty

Julian Sexton

John Sweetnam

Anne Townsend

The MITRE Corporation
McLean, Virginia

January 2020

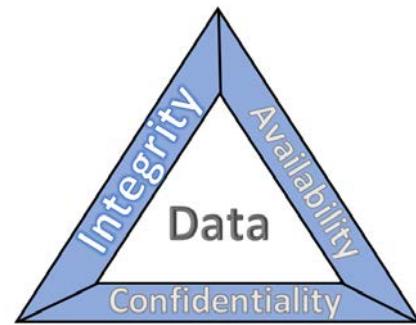
DRAFT

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

1 Executive Summary

2 The CIA triad represents the three pillars of information security: confidentiality, integrity, and
3 availability, as follows.

- 4 ▪ Confidentiality – preserving authorized restrictions on
5 information access and disclosure, including means for
6 protecting personal privacy and proprietary
7 information
- 8 ▪ Integrity – guarding against improper information
9 modification or destruction and ensuring information
10 non-repudiation and authenticity
- 11 ▪ Availability – ensuring timely and reliable access to and
12 use of information



13 This series of practice guides focuses on data integrity: the property that data has not been altered in an
14 unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
15 (Note: These definitions are from National Institute of Standards ([NIST Special Publication \(SP\) 800-12 Rev 1, An Introduction to Information Security](#).)

- 17 ▪ Destructive malware, ransomware, malicious insider activity, and even honest mistakes all set
18 the stage for why organizations need to quickly detect and respond to an event that impacts
19 data integrity. Businesses must be confident that these events are detected quickly and
20 responded to appropriately.
- 21 ▪ Attacks against an organization's data can compromise
22 emails, employee records, financial records, and customer
23 information—impacting business operations, revenue,
24 and reputation.
- 25 ▪ Examples of data integrity attacks include unauthorized
26 insertion, deletion, or modification of data to corporate
27 information such as emails, employee records, financial
28 records, and customer data.
- 29 ▪ The National Cybersecurity Center of Excellence (NCCoE)
30 at NIST built a laboratory environment to explore
31 methods to effectively detect and respond to a data
32 integrity event in various information technology (IT) enterprise environments, to immediately
33 react to the event in an effort to prevent a complete compromise.
- 34 ▪ This NIST Cybersecurity Practice Guide demonstrates how organizations can develop and
35 implement appropriate actions during a detected data integrity cybersecurity event.



36 CHALLENGE

37 Some organizations have experienced systemic attacks that force operations to cease. One variant of a
38 data integrity attack—ransomware—encrypts data, leaving it modified in an unusable state. Other data
39 integrity attacks may be more dynamic, targeting machines, spreading laterally across networks, and

40 continuing to cause damage throughout an organization. In either case, behaviors are exhibited—such
41 as files inexplicably becoming encrypted or network activity—that provide an ability to immediately
42 detect the occurrence and respond in a timely fashion to curtail the ramifications.

43 **SOLUTION**

44 NIST published version 1.1 of the Cybersecurity Framework in April 2018 to provide guidance on
45 protecting and developing resiliency for critical infrastructure and other sectors. The framework core
46 contains five functions, listed below.

- 47 ■ **Identify** – develop an organizational understanding
48 to manage cybersecurity risk to systems, people,
49 assets, data, and capabilities
- 50 ■ **Protect** – develop and implement appropriate
51 safeguards to ensure delivery of critical services
- 52 ■ **Detect** – develop and implement appropriate
53 activities to identify the occurrence of a
54 cybersecurity event
- 55 ■ **Respond** – develop and implement appropriate
56 activities to take action regarding a detected
57 cybersecurity incident
- 58 ■ **Recover** – develop and implement appropriate
59 activities to maintain plans for resilience and to restore any capabilities or services that were
60 impaired due to a cybersecurity incident



61 For more information, see the [Framework for Improving Critical Infrastructure Cybersecurity v1.1](#).

62 Applying the Cybersecurity Framework to data integrity, this practice guide informs organizations of
63 how to quickly **detect** and **respond** to data integrity attacks by implementing appropriate activities that
64 immediately inform about the data integrity events.

65 The NCCoE developed and implemented a solution that incorporates multiple systems working in
66 concert to **detect** an ongoing data integrity cybersecurity event. Additionally, the solution provides
67 guidance on how to **respond** to the detected event. Addressing these functions together enables
68 organizations to have the necessary tools to act during a data integrity attack.

69 The NCCoE sought existing technologies that provided the following capabilities:

- 70 ■ event detection
- 71 ■ forensics/analysis
- 72 ■ integrity monitoring
- 73 ■ logging
- 74 ■ mitigation and containment
- 75 ■ reporting

76 While the NCCoE used a suite of commercial products to address this challenge, this guide does not
77 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your
78 organization's information security experts should identify the products that will best integrate with
79 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that
80 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and
81 implementing parts of a solution.

82 **BENEFITS**

83 The NCCoE's practice guide to Data Integrity: Detecting and Responding to Ransomware and Other
84 Destructive Events can help your organization:

- 85 ▪ develop a strategy for detecting and responding to a data integrity cybersecurity event
- 86 ▪ facilitate effective detection and response to adverse events, maintain operations, and ensure
87 the integrity and availability of data critical to supporting business operations and revenue-
88 generating activities
- 89 ▪ manage enterprise risk (consistent with foundations of the NIST *Framework for Improving
90 Critical Infrastructure Cybersecurity*)

91 **SHARE YOUR FEEDBACK**

92 You can view or download the guide at [https://www.nccoe.nist.gov/projects/building-blocks/data-
93 integrity/detect-respond](https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/detect-respond). Help the NCCoE make this guide better by sharing your thoughts with us as
94 you read the guide. If you adopt this solution for your own organization, please share your experience
95 and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our
96 solution, so we encourage organizations to share lessons learned and best practices for transforming the
97 processes associated with implementing this guide.

98 To provide comments or to learn more by arranging a demonstration of this example implementation,
99 contact the NCCoE at ds-nccoe@nist.gov.

100 **TECHNOLOGY PARTNERS/COLLABORATORS**

101 Organizations participating in this project submitted their capabilities in response to an open call in the
102 Federal Register for all sources of relevant security capabilities from academia and industry (vendors
103 and integrators). The following respondents with relevant capabilities or product components (identified
104 as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development
105 Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.



106 Certain commercial entities, equipment, products, or materials may be identified by name or company
107 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an
108 experimental procedure or concept adequately. Such identification is not intended to imply special
109 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it

- 111 intended to imply that the entities, equipment, products, or materials are necessarily the best available
112 for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit <https://www.nccoe.nist.gov/nccoe@nist.gov>
301-975-0200

NIST SPECIAL PUBLICATION 1800-26B

Data Integrity

Detecting and Responding to Ransomware and Other Destructive Events

Volume B:
Approach, Architecture, and Security Characteristics

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 1800-26B, Natl. Inst. Stand. Technol.
9 Spec. Publ. 1800-26B, 53 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.

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

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 regulations
47 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 **Contents**

71	1 Summary.....	1
72	1.1 Challenge.....	2
73	1.2 Solution.....	2
74	1.3 Benefits.....	3
75	2 How to Use This Guide	4
76	2.1 Typographic Conventions.....	5
77	3 Approach	6
78	3.1 Audience.....	6
79	3.2 Scope	6
80	3.3 Assumptions	7
81	3.4 Risk Assessment	7
82	3.4.1 Risk.....	8
83	3.4.2 Security Control Map	9
84	3.5 Technologies.....	13
85	4 Architecture	16
86	4.1 Architecture Description	16
87	4.1.1 High-Level Architecture	16
88	4.1.2 Architecture Components.....	17
89	5 Security Characteristic Analysis.....	20
90	5.1 Assumptions and Limitations	20
91	5.2 Build Testing	20
92	5.3 Scenarios and Findings	20
93	5.3.1 Ransomware via Web Vector and Self-Propagation.....	21
94	5.3.2 Destructive Malware via USB Vector	22
95	5.3.3 Accidental VM Deletion via Maintenance Script	23
96	5.3.4 Backdoor Creation via E-mail Vector	24
97	5.3.5 Database Modification via Malicious Insider	25

98	5.3.6 File Modification via Malicious Insider	26
99	5.3.7 Backdoor Creation via Compromised Update Server	26
100	6 Future Build Considerations	27
101	Appendix A List of Acronyms.....	28
102	Appendix B Glossary	29
103	Appendix C References	33
104	Appendix D Functional Evaluation.....	35
105	D.1 Data Integrity Functional Test Plan	35
106	D.2 Data Integrity Use Case Requirements	36
107	D.3 Test Case: Data Integrity DR -1.....	43
108	D.4 Test Case: Data Integrity DR -2.....	45
109	D.5 Test Case: Data Integrity DR -3.....	46
110	D.6 Test Case: Data Integrity DR -4.....	47
111	D.7 Test Case: Data Integrity DR -5.....	49
112	D.8 Test Case: Data Integrity DR -6.....	50
113	D.9 Test Case: Data Integrity DR -7.....	51

114	List of Figures	
115	Figure 4-1 DI Detect & Respond High-Level Architecture	16
116	List of Tables	
117	Table 3--1 DI Reference Design Cybersecurity Framework Core Components Map	10
118	Table 3-2 Products and Technologies	13
119	Table 6-1 Test Case Fields.....	35
120	Table 6-2 Capability Requirements	36
121	Table 6-3 Test Case ID: Data Integrity DR -1	43
122	Table 6-4 Test Case ID: Data Integrity DR -2	45
123	Table 6-5 Test Case ID: Data Integrity DR -3	46
124	Table 6-6 Test Case ID: Data Integrity DR -4	47
125	Table 6-7 Test Case ID: Data Integrity DR -5	49
126	Table 6-8 Test Case ID: Data Integrity DR -6	50
127	Table 6-9 Test Case ID: Data Integrity DR -7	51

128 1 Summary

129 Businesses face a near-constant threat of destructive malware, ransomware, malicious insider activities,
130 and even honest mistakes that can alter or destroy critical data. These types of adverse events
131 ultimately impact data integrity (DI). It is imperative for organizations to be able to detect and respond
132 to DI attacks.

133 The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and
134 Technology (NIST) built a laboratory environment to explore methods to detect and respond to a data
135 corruption event in various information technology (IT) enterprise environments. The example solution
136 outlined in this guide describes the solution built in the NCCoE lab. It encourages detection and
137 mitigation of DI events while facilitating analysis of these events.

138 The goals of this NIST Cybersecurity Practice Guide are to help organizations confidently:

- 139 ▪ detect malicious and suspicious activity generated on the network, by users, or from
140 applications that could indicate a DI event
- 141 ▪ mitigate and contain the effects of events that can cause a loss of DI
- 142 ▪ monitor the integrity of the enterprise for detection of events and after-the-fact analysis
- 143 ▪ utilize logging and reporting features to speed response time to DI events
- 144 ▪ analyze DI events for the scope of their impact on the network, enterprise devices, and
145 enterprise data
- 146 ▪ analyze DI events to inform and improve the enterprise's defenses against future attacks

147 For ease of use, here is a short description of the different sections of this volume.

- 148 ▪ [Section 1](#): Summary presents the challenge addressed by the NCCoE project with an in-depth
149 look at our approach, the architecture, and the security characteristics we used; the solution
150 demonstrated to address the challenge; the benefits of the solution; and the technology
151 partners that participated in building, demonstrating, and documenting the solution. Summary
152 also explains how to provide feedback on this guide.
- 153 ▪ [Section 2](#): How to Use This Guide explains how readers—business decision-makers, program
154 managers, and IT professionals (e.g., systems administrators)—might use each volume of the
155 guide.
- 156 ▪ [Section 3](#): Approach offers a detailed treatment of the scope of the project and describes the
157 assumptions on which the security platform development was based, the risk assessment that
158 informed platform development, and the technologies and components that industry
159 collaborators gave us to enable platform development.

- 160 ▪ [Section 4](#): Architecture describes the usage scenarios supported by project security platforms,
161 including Cybersecurity Framework [1] functions supported by each component contributed by
162 our collaborators.
- 163 ▪ [Section 5](#): Security Characteristic Analysis provides details about the tools and techniques we
164 used to perform risk assessments.
- 165 ▪ [Section 6](#): Future Build Considerations is a brief treatment of other data security
166 implementations that NIST is considering consistent with Cybersecurity Framework Core
167 Functions: Identify, Protect, Detect, Respond, and Recover.

168 **1.1 Challenge**

169 Thorough collection of quantitative and qualitative data is important to organizations of all types and
170 sizes. It can impact all aspects of a business, including decision making, transactions, research,
171 performance, and profitability. When these data collections sustain a DI attack caused by unauthorized
172 insertion, deletion, or modification of information, such an attack can impact emails, employee records,
173 financial records, and customer data, rendering them unusable or unreliable. Some organizations have
174 experienced systemic attacks that caused a temporary cessation of operations. One variant of a DI
175 attack—ransomware—encrypts data and holds it hostage while the attacker demands payment for the
176 decryption keys.

177 When DI events occur, organizations should have the capabilities to detect and respond in real time.
178 Early detection and mitigation can reduce the potential impact of events, including damage to
179 enterprise files, infection of systems, and account compromise. Furthermore, organizations should be
180 able to learn from DI events to improve their defenses. Analysis of malicious behavior at the network
181 level, user level, and file level can reveal flaws in the security of the enterprise. Resolution of these
182 flaws, though out of scope of this guide, is often only possible once they have been exploited and with
183 the right solution in place.

184 **1.2 Solution**

185 The NCCoE implemented a solution that incorporates appropriate actions during and directly after a DI
186 event. The solution is composed of multiple systems working together to detect and respond to data
187 corruption events in standard enterprise components. These components include mail servers,
188 databases, end-user machines, virtual infrastructure, and file share servers. Furthermore, an important
189 function of the Respond Category of the Cybersecurity Framework is improvement of defenses—this
190 guide includes components that aid in analysis of DI events and for improving defenses against them.

191 The NCCoE sought existing technologies that provided the following capabilities:

- 192 • Event Detection
193 • Integrity Monitoring

- 194 • Logging
195 • Reporting
196 • Mitigation and Containment
197 • Forensics/Analytics

198 In developing our solution, we used standards and guidance from the following, which can also provide
199 your organization with relevant standards and best practices:

- 200 • NIST Framework for Improving Critical Infrastructure Cybersecurity (commonly known as the
201 NIST Cybersecurity Framework [\[1\]](#))
202 • NIST Interagency or Internal Report (NISTIR) 8050: *Executive Technical Workshop on Improving
203 Cybersecurity and Consumer Privacy* [\[2\]](#)
204 • NIST Special Publication (SP) 800-30 Rev. 1: *Guide for Conducting Risk Assessments* [\[3\]](#)
205 • NIST SP 800-37 Rev. 1: *Guide for Applying the Risk Management Framework to Federal
206 Information Systems: A Security Life Cycle Approach* [\[4\]](#)
207 • NIST SP 800-39: *Managing Information Security Risk* [\[5\]](#)
208 • NIST SP 800-40 Rev. 3: *Guide to Enterprise Patch Management Technologies* [\[6\]](#)
209 • NIST SP 800-53 Rev. 4: *Security and Privacy Controls for Federal Information Systems and
210 Organizations* [\[7\]](#)
211 • Federal Information Processing Standard 140-2: Security Requirements for Cryptographic
212 Modules [\[8\]](#)
213 • NIST SP 800-86: *Guide to Integrating Forensic Techniques into Incident Response* [\[9\]](#)
214 • NIST SP 800-92: *Guide to Computer Security Log Management* [\[10\]](#)
215 • NIST SP 800-100: *Information Security Handbook: A Guide for Managers* [\[11\]](#)
216 • NIST SP 800-34 Rev. 1: *Contingency Planning Guide for Federal Information Systems* [\[12\]](#)
217 • Office of Management and Budget, Circular Number A-130: Managing Information as a Strategic
218 Resource [\[13\]](#)
219 • NIST SP 800-61 Rev. 2: *Computer Security Incident Handling Guide* [\[14\]](#)
220 • NIST SP 800-83 Rev. 1: *Guide to Malware Incident Prevention and Handling for Desktops and
221 Laptops* [\[15\]](#)
222 • NIST SP 800-150: *Guide to Cyber Threat Information Sharing* [\[16\]](#)
223 • NIST SP 800-184: *Guide for Cybersecurity Event Recovery* [\[17\]](#)

224 **1.3 Benefits**

225 The NCCoE's practice guide can help your organization:

- 226 • develop an implementation plan for detecting and responding to cybersecurity events
227 • facilitate detection, response, and analysis of DI events to improve defenses and mitigate
228 impact

- 229 • maintain integrity and availability of data that is critical to supporting business operations
230 and revenue-generating activities
231 • manage enterprise risk (consistent with the foundations of the NIST Cybersecurity
232 Framework)

233 2 How to Use This Guide

234 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides
235 users with the information they need to replicate the DI detection and response solution. This reference
236 design is modular and can be deployed in whole or in part.

237 This guide contains three volumes:

- 238 ▪ NIST SP 1800-26A: *Executive Summary*
239 ▪ NIST SP 1800-26B: *Approach, Architecture, and Security Characteristics* – what we built and why
240 (**you are here**)
241 ▪ NIST SP 1800-26C: *How-To Guides* – instructions for building the example solution

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

243 **Business decision-makers, including chief security and technology officers**, will be interested in the
244 *Executive Summary*, NIST SP 1800-26A, which describes the following topics:

- 245 ▪ challenges that enterprises face in detecting and responding to data integrity events
246 ▪ example solution built at the NCCoE
247 ▪ benefits of adopting the example solution

248 **Technology or security program managers** who are concerned with how to identify, understand, assess,
249 and mitigate risk will be interested in this part of the guide, NIST SP 1800-26B, which describes what we
250 did and why. The following sections will be of particular interest:

- 251 ▪ [Section 3.4.1](#), Risk, provides a description of the risk analysis we performed.
252 ▪ [Section 3.4.2](#), Security Control Map, maps the security characteristics of this example solution to
253 cybersecurity standards and best practices.

254 You might share the *Executive Summary*, NIST SP 1800-26A, with your leadership team members to help
255 them understand the importance of adopting a standards-based solution to detect and respond to data
256 integrity events.

257 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.

258 You can use the how-to portion of the guide, NIST SP 1800-26C, to replicate all or parts of the build
259 created in our lab. The how-to portion of the guide provides specific product installation, configuration,
260 and integration instructions for implementing the example solution. We do not re-create the product

261 manufacturers' documentation, which is generally widely available. Rather, we show how we
 262 incorporated the products together in our environment to create an example solution.

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

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

276 2.1 Typographic Conventions

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

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

278 **3 Approach**

279 Based on key points expressed in NISTIR 8050: *Executive Technical Workshop on Improving Cybersecurity*
280 and *Consumer Privacy* (2015), the NCCoE is pursuing a series of DI projects to map the Core Functions of
281 the NIST Cybersecurity Framework. This project is centered on the Core Functions of Detect and
282 Respond, which consist of detecting and responding to DI attacks. Compromise can come from malicious
283 websites, targeted emails, insider threats, and honest mistakes. Monitoring solutions should be in place
284 to detect these events. Once detected, swift response to a threat is critical to mitigate the need for
285 recovery action after an event occurs. NCCoE engineers working with a Community of Interest (COI)
286 defined the requirements for this DI project.

287 Members of the COI, which include participating vendors referenced in this document, contributed to
288 development of the architecture and reference design, providing technologies that meet the project
289 requirements and assisting in installation and configuration of those technologies. The practice guide
290 highlights the approach used to develop the NCCoE reference solution. Elements include risk assessment
291 and analysis, logical design, build development, test and evaluation, and security control mapping. This
292 guide is intended to provide practical guidance to any organization interested in implementing a
293 solution for detecting and responding to a cybersecurity event.

294 **3.1 Audience**

295 This guide is intended for individuals responsible for implementing security solutions in organizations' IT
296 support activities. Current IT systems, particularly in the private sector, often lack the capability to
297 comprehensively detect, mitigate, and learn from cybersecurity events. The platforms demonstrated by
298 this project and the implementation information provided in this practice guide permit integration of
299 products to implement a data integrity detection and response system. The technical components will
300 appeal to system administrators, IT managers, IT security managers, and others directly involved in the
301 secure and safe operation of business IT networks.

302 **3.2 Scope**

303 The guide provides practical, real-world guidance on developing and implementing a DI solution
304 consistent with the principles in the NIST Framework for Improving Critical Infrastructure Cybersecurity
305 Volume 1, specifically the Core Functions of Detect and Respond. Detecting emphasizes developing and
306 implementing the appropriate activities to detect events in real time, compare the current system state
307 to a norm, and produce audit logs for use during and after the event. Responding emphasizes real-time
308 mitigation of events, forensic analysis during and after the event, and reporting. Examples of outcomes
309 within these functions are integrity monitoring, event detection, logging, reporting, forensics, and
310 mitigation.

311 **3.3 Assumptions**

312 This project is guided by the following assumptions:

- 313 ▪ The solution was developed in a lab environment. The environment is based on a basic
314 organization's IT enterprise. It does not reflect the complexity of a production environment: for
315 example, building across numerous physical locations, accommodating extreme working
316 conditions, or configuring systems to meet specific network/user needs. These demands can all
317 increase the level of complexity needed to implement a DI solution.
- 318 ▪ An organization has access to the skill sets and resources required to implement an event
319 detection and response system.
- 320 ▪ A DI event is taking place, and the organization is seeking to detect and mitigate the damage
321 that an event is causing.

322 **3.4 Risk Assessment**

323 [NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments](#), states that risk is “a measure of the
324 extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
325 (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of
326 occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and
327 prioritizing risks to organizational operations (including mission, functions, image, reputation),
328 organizational assets, individuals, other organizations, and the Nation, resulting from the operation of
329 an information system. Part of risk management incorporates threat and vulnerability analyses, and
330 considers mitigations provided by security controls planned or in place.”

331 The NCCoE recommends that any discussion of risk management, particularly at the enterprise level,
332 begins with a comprehensive review of [NIST SP 800-37 Revision 2, Risk Management Framework for](#)
333 [Information Systems and Organizations](#)—publicly available material. The [Risk Management Framework](#)
334 [\(RMF\)](#) guidance, as a whole, proved invaluable in giving us a baseline to assess risks, from which we
335 developed the project, the security characteristics of the build, and this guide.

336 We performed two types of risk assessment:

- 337 ▪ Initial analysis of the risk factors discussed with financial, retail, and hospitality institutions. This
338 analysis led to creation of the DI project and the desired security posture. See NISTIR 8050,
339 Executive Technical Workshop, for additional participant information.
- 340 ▪ Analysis of how to secure the components within the solution and minimize any vulnerabilities
341 they might introduce. See [Section 5](#), Security Characteristic Analysis.

342 **3.4.1 Risk**

343 Using the guidance in NIST's series of publications concerning risk, we worked with financial institutions
344 and the Financial Sector Information Sharing and Analysis Center to identify the most compelling risk
345 factors encountered by this business group. We participated in conferences and met with members of
346 the financial sector to define the main security risks to business operations. From these discussions
347 came identification of an area of concern—DI. Having produced *Data Integrity: Recovering from*
348 *Ransomware and Other Destructive Events*, which primarily focused on the recovery aspect of DI, we
349 identified a need for guidance in the areas of detecting and responding to cybersecurity events in real
350 time.

351 When considering risk from the perspective of detecting and responding to cybersecurity events during
352 their execution, we must consider not only the impact of an event on an organization's assets but also
353 the threats to those assets and the potential vulnerabilities these threats could exploit.

354 When discussing threats to an organization's assets from the perspective of DI, we consider these:

- 355 • malware
356 • insider threats
357 • accidents caused by human error
358 • compromise of trusted systems

359 The types of vulnerabilities we consider in relation to these threats include:

- 360 • zero-day vulnerabilities
361 • vulnerabilities due to outdated or unpatched systems
362 • custom software vulnerabilities/errors
363 • social engineering and user-driven events
364 • poor access control

365 Finally, the potential impact on an organization from a DI event:

- 366 • systems incapacitated
367 • modification/deletion of the organization's assets
368 • negative impact on the organization's reputation

369 Analysis of the threats, vulnerabilities, and potential impact to an organization has given us an
370 understanding of the risk for organizations with respect to DI. NIST SP 800-39, *Managing Information*
371 *Security Risk*, focuses on the business aspect of risk, namely at the enterprise level. This understanding is
372 essential for any further risk analysis, risk response/mitigation, and risk monitoring activities. The
373 following is a summary of the strategic risk areas we identified and their mitigations:

- 374 • Impact on system function—ensuring the availability of accurate data or sustaining an acceptable
375 level of DI reduces the risk of systems' availability being compromised.
376 • Cost of implementation—implementing event detection and response from DI events once and
377 using it across all systems may reduce system continuity costs.
378 • Compliance with existing industry standards—contributes to the industry requirement to
379 maintain a continuity of operations plan.
380 • Maintenance of reputation and public image—helps reduce the damage caused by active events
381 and facilitates the information needed to learn from the events.
382 • Increased focus on DI—includes not just loss of confidentiality but also harm from unauthorized
383 alteration of data (per NISTIR 8050).

384 We subsequently translated the risk factors identified to security Functions and Subcategories within
385 the NIST Cybersecurity Framework. In Table 3-1 we mapped the Categories to NIST SP 800-53 Rev. 4
386 controls.

387 [3.4.2 Security Control Map](#)

388 As explained in [Section 3.4.1](#), we identified the Cybersecurity Framework security Functions and
389 Subcategories that we wanted the reference design to support through a risk analysis process. This was
390 a critical first step in drafting the reference design and example implementation to mitigate the risk
391 factors. Table 3-1 lists the addressed Cybersecurity Framework Functions and Subcategories and maps
392 them to relevant NIST standards, industry standards, and controls and best practices. The references
393 provide solution validation points in that they list specific security capabilities that a solution addressing
394 the Cybersecurity Framework Subcategories would be expected to exhibit. Organizations can use Table
395 3-1 to identify the Cybersecurity Framework Subcategories and NIST SP 800-53 Rev. 4 controls that they
396 are interested in addressing.

397 When cross-referencing Functions of the Cybersecurity Framework with product capabilities used in this
398 practice guide, it is important to consider:

- 399 ▪ This practice guide, though primarily focused on Detect/Respond capabilities, also uses PR.DS-6,
400 a Protect Subcategory. This is primarily because creation of integrity baselines is used for
401 comparison when detecting attacks but is created prior to the start of an attack.
- 402 ▪ Not all the Cybersecurity Framework Subcategories guidance can be implemented using
403 technology. Any organization executing a DI solution would need to adopt processes and
404 organizational policies that support the reference design. For example, some of the
405 Subcategories within the Cybersecurity Framework Function called Respond are processes and
406 policies that should be developed prior to implementing recommendations.

407 **Table 3-1 DI Reference Design Cybersecurity Framework Core Components Map**

Cybersecurity Framework v1.1				Standards & Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
PROTECT (PR)	Data Security (PR.DS)	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	SC-16, SI-7	A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4	OM-DTA-001
DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	AC-4, CA-3, CM-2, SI-4	A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2	SP-ARC-001
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	AU-6, CA-7, IR-4, SI-4	A.12.4.1, A.16.1.1, A.16.1.4	PR-CDA-001
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	A.12.4.1, A.16.1.7	CO-OPS-001, PR-CIR-001
		DE.AE-4: Impact of events is determined.	CP-2, IR-4, RA-3, SI-4	A.16.1.4	PR-INF-001

Cybersecurity Framework v1.1				Standards & Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
RESPOND (RS)	Security Continuous Monitoring (DE.CM)	DE.AE-5: Incident alert thresholds are established.	IR-4, IR-5, IR-8	A.16.1.4	PR-CIR-001
		DE.CM-1: The network is monitored to detect potential cybersecurity events.	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4		OM-NET-001
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	A.12.4.1, A.12.4.3	AN-TWA-001
		DE.CM-4: Malicious code is detected.	SI-3, SI-8	A.12.2.1	SP-DEV-001
		DE.CM-5: Unauthorized mobile code is detected.	SC-18, SI-4, SC-44	A.12.5.1, A.12.6.2	SP-DEV-001
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	A.12.4.1, A.14.2.7, A.15.2.1	AN-TWA-001
	Detection Processes (DE.DP)	DE.DP-2: Detection activities comply with all applicable requirements.	AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	A.18.1.4, A.18.2.2, A.18.2.3	PR-CDA-001
RESPOND (RS)	Response Planning (RS.RP)	RS.RP-1: Response plan is executed during or after an incident.	CP-2, CP-10, IR-4, IR-8	A.16.1.5	PR-CIR-001

Cybersecurity Framework v1.1				Standards & Best Practices	
Function	Category	Subcategory	NIST SP 800-53 R4	ISO/IEC 27001:2013	NIST SP 800-181
	Communications (RS.CO)	RS.CO-2: Incidents are reported consistent with established criteria.	AU-6, IR-6, IR-8	A.6.1.3, A.16.1.2	IN-FOR-002
		RS.AN-1: Notifications from detection systems are investigated.	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	A.12.4.1, A.12.4.3, A.16.1.5	PR-CDA-001
	Analysis (RS.AN)	RS.AN-2: The impact of the incident is understood.	CP-2, IR-4	A.16.1.4, A.16.1.6	PR-CIR-001
		RS.AN-3: Forensics are performed.	AU-7, IR-4	A.16.1.7	IN-FOR-002
		RS.AN-4: Incidents are categorized consistent with response plans.	CP-2, IR-4, IR-5, IR-8	A.16.1.4	PR-CIR-001
	Mitigation (RS.MI)	RS.MI-1: Incidents are contained.	IR-4	A.12.2.1, A.16.1.5	PR-CIR-001
		RS.MI-2: Incidents are mitigated.	IR-4	A.12.2.1, A.16.1.5	PR-CIR-001

408 **3.5 Technologies**

409 Table 3-2 lists all of the technologies used in this project and provides a mapping among the generic application term, the specific product used,
 410 and the security control(s) the product provides. Refer to Table 3-1 for an explanation of the NIST Cybersecurity Framework Subcategory codes.

411 **Table 3-2 Products and Technologies**

Component	Product	Function	Cybersecurity Framework Subcategories
Integrity Monitoring	Tripwire Enterprise v8.7	<ul style="list-style-type: none"> • Provides file hashes and integrity checks for files and software, regardless of file type. • Provides integrity monitoring for data. • Provides integrity monitoring for Active Directory. 	PR.DS-6, DE.AE-1, DE.CM-3, DE.CM-7
	Semperis Directory Services Protector (DSP) v2.7		
Event Detection	Cisco Advanced Malware Protection (AMP) v5.4	<ul style="list-style-type: none"> • Provides the ability to receive information about new threats. • Provides the ability to statically detect malicious software. 	DE.AE-3, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-7
	Glasswall FileTrust ATP for Email v6.90.2.5		
	Cisco Stealthwatch v7.0.0		

Component	Product	Function	Cybersecurity Framework Subcategories
	Semperis DSP v2.7	<ul style="list-style-type: none"> Provides ability to dynamically detect malicious software. Provides ability to detect malicious email attachments. Provides ability to scan the network for anomalies. Provides the ability to monitor user behavior for anomalies. Provides ability to scan email attachments for deviations from file type specifications or organizational policy. 	
Logging	Micro Focus ArcSight Enterprise Security Manager (ESM) v7.0 Patch 2	<ul style="list-style-type: none"> Provides auditing and logging capabilities configurable to organizational policy. Correlates logs of cybersecurity events with user information. Provides automation for logging. 	DE.AE-1, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-3, DE.CM-7, RS.AN-2
	Tripwire Log Center v7.3.1		
Forensics/Analytics	Cisco AMP v5.4	<ul style="list-style-type: none"> Provides forensics to track effects of malware retrospectively. Provides network traffic analysis. Provides ability to analyze files sent over the network. Provides analysis capabilities for finding anomalies in enterprise activity. 	DE.AE-2, DE.AE-4, DE.CM-1, RS.RP-1, RS.AN-1, RS.AN-2, RS.AN-3
	Symantec Security Analytics v8.0.1		
	Micro Focus ArcSight ESM v7.0 Patch 2		
	Symantec Information Centric Analytics (ICA) v6.5.2		
	Cisco AMP v5.4		

Component	Product	Function	Cybersecurity Framework Subcategories
Mitigation and Containment	Cisco Identity Services Engine (ISE) v2.4	<ul style="list-style-type: none"> • Provides ability to sandbox files locally. • Provides ability to enforce policy across the enterprise. • Provides ability to quarantine devices across the enterprise. • Provides ability to sanitize files through file reconstruction. • Provides ability to revert changes to domain services. 	DE.CM-5, RS.RP-1, RS.MI-1, RS.MI-2
	Glasswall FileTrust ATP for Email v6.90.2.5		
	Semperis DSP v2.7		
Reporting	Micro Focus ArcSight ESM v7.0 Patch 2	<ul style="list-style-type: none"> • Provides ability to send security alerts based on organizational policy. • Provides ability to provide reports of enterprise health. • Provides ability to provide reports of malware detection across the enterprise. 	DE.AE-5, RS.RP-1, RS.CO-2

412 4 Architecture

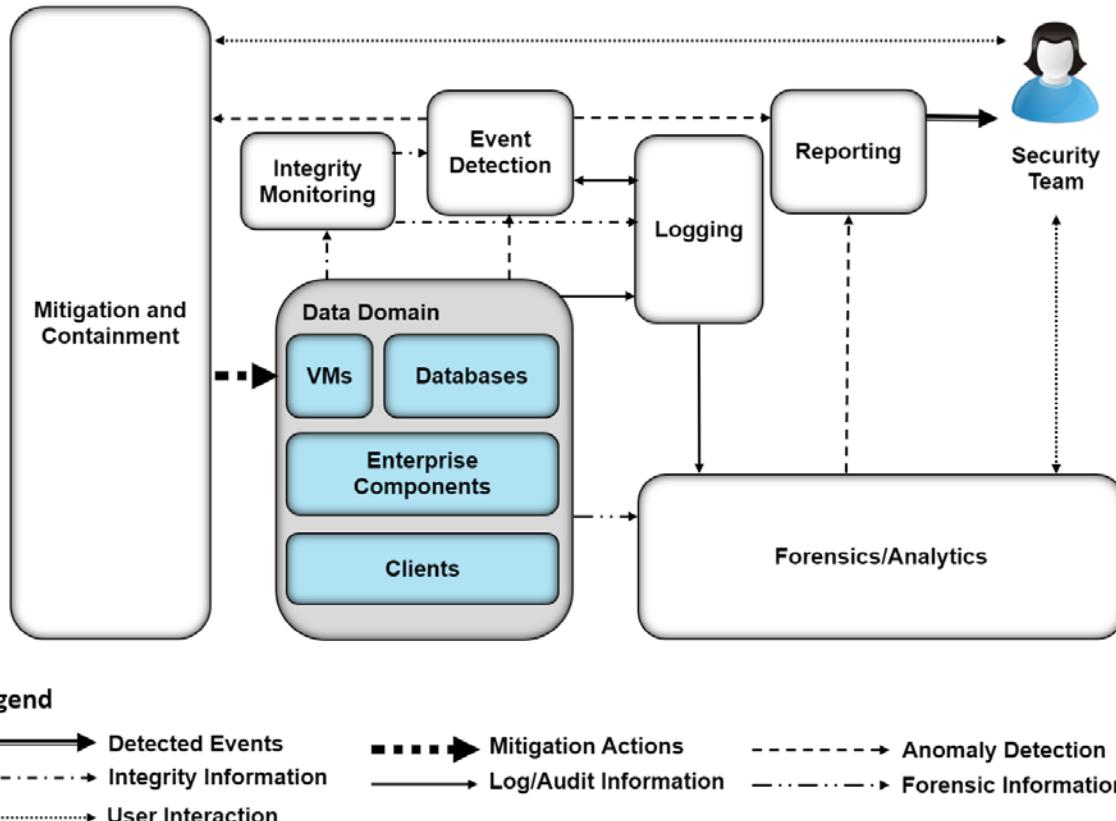
413 This section presents the high-level architecture used for implementation of a DI solution that detects
414 and responds to ransomware and other destructive events.

415 4.1 Architecture Description

416 4.1.1 High-Level Architecture

417 The DI solution is designed to address the security Functions and Subcategories described in Table 3-1
418 and is composed of the capabilities illustrated in Figure 4-1.

419 Figure 4-1 DI Detect & Respond High-Level Architecture



- 420 • Integrity Monitoring provides capabilities for comparing current system states against
421 established baselines.

- 422 • Event Detection provides capabilities for detecting ongoing events and can be composed of
423 intrusion detection, malware detection, user anomaly detection, and others, depending on the
424 established threat model of the organization.
425 • Logging records and stores all the log files produced by components within the enterprise.
426 • Forensics/Analytics provides the capability to probe/analyze logs and machines within the
427 enterprise to learn from DI events.
428 • Mitigation and Containment allows responding to DI events by containing and limiting the
429 threat's ability to affect the system.
430 • Reporting provides the capability to report on all activities within the enterprise and within the
431 reference architecture for analysis by a security team.

432 These capabilities work together to provide the Detect and Respond Functions for DI. The integrity
433 monitoring capability collects integrity information prior to attacks so that when an attack happens,
434 records of all file/system changes are preserved. In combination with event detection, these records not
435 only function as a tool to inform recovery but also as early indicators of compromise. Event detection
436 uses these records and its own mechanisms to actively detect events as they happen and to take
437 appropriate action through other components of the reference architecture. Logging collects
438 information from event detection and integrity monitoring for use in response functions. Mitigation and
439 Containment provides capabilities to stop ongoing attacks and limit their effect on the system.
440 Forensics/Analytics allow analysis of logs and threat behavior to aid the organization in learning from
441 the attack. Reporting provides capabilities for reporting information from analysis and logging to the
442 appropriate parties both during and after an attack. The information gained from these attacks can be
443 used to inform products that fall in the Identify Function of the Cybersecurity Framework to indicate
444 vulnerabilities in the enterprise that need to be remediated.

445 [**4.1.2 Architecture Components**](#)

446 [**4.1.2.1 Integrity Monitoring**](#)

447 The Integrity Monitoring component provides the ability to test, understand, and measure attacks that
448 occur on files and components within the enterprise. When considering DI from the perspective of
449 detecting and responding to an active attack, being able to track changes to files is critical. Asset
450 integrity changes can provide an early detection mechanism by tracking changes made at abnormal
451 times or by tracking users who typically do not make such changes. Furthermore, the changes tracked
452 during a DI event can be used to inform the recovery process; they provide information about what
453 changes happened, when changes began to take place, as well as what programs were involved in the
454 changes.

455 Integrity Monitoring typically requires an operation baseline to be taken prior to the start of a DI
456 event—this baseline is used for comparison against the system's state during an attack.

457 For the Integrity Monitoring capability, we use a combination of two tools: Tripwire Enterprise and
458 Semperis DSP. Once a baseline is taken prior to an attack, Tripwire Enterprise stores integrity
459 information for selected data across all systems. When a “check” is run, Tripwire collects all the changes
460 that occurred to monitored files on those systems. These changes are forwarded to the Logging
461 component, which can then report and alert on them, becoming an indicator of a DI event.
462 Furthermore, these collected changes can be used to help remediate the effects of malware on a
463 system.

464 Semperis DSP provides a similar function but with a focus on Active Directory. Changes to Active
465 Directory users, groups, and other services are collected and can be used to notify administrators of
466 potentially malicious activity. Given the sensitive nature of Active Directory, Semperis DSP does not rely
467 on a single source of information but instead monitors multiple aspects of Active Directory. This helps
468 ensure that any change to permissions or privileged credentials is captured, including changes that
469 attackers attempt to hide (for example, by circumventing security auditing).

4.1.2.2 Event Detection

471 The Event Detection component provides the ability to detect events as they happen. This can be
472 achieved through a combination of mechanisms, depending on the needs of the organization. Analysis
473 of integrity monitoring logs can indicate malicious activity. Malware detection, behavior-based anomaly
474 detection, and intrusion detection are all potential examples of event detection. The goal of this
475 component is to detect events as they happen, to trigger the appropriate responses, and to provide
476 information about the attack to the security team.

477 For the event detection capability, we use a combination of tools. Cisco AMP is used to detect malicious
478 files. Glasswall FileTrust ATP for Email is used to identify malicious email attachments that do not
479 conform to file standards and organizational policies. Cisco Stealthwatch is used to detect malicious
480 network activity. Finally, Semperis DSP is used to detect changes in Active Directory. Information from
481 these four can be correlated to identify malicious patterns of behavior from users.

4.1.2.3 Logging

483 Logging from each component serves several functions in an architecture that aims to detect and
484 respond to active DI events. Logs are produced through integrity monitoring and event detection, which
485 aid other components in responding to active events. Both Mitigation and Containment and
486 Forensics/Analytics use logs to inform their actions—logs tell them what systems are being affected and
487 what programs are causing the event. Further, these logs help decide what steps should be taken to
488 remediate the attack and protect against it going forward.

489 For the Logging capability, we use a combination of two tools: Micro Focus ArcSight and Tripwire Log
490 Center. While Tripwire Log Center’s purpose in this build is primarily to collect, transform, and forward
491 logs from Tripwire Enterprise to ArcSight, ArcSight performs a wider function. ArcSight collects logs from

492 various sources in the enterprise, such as Event Detection and Integrity Monitoring, as well as Windows
493 event logs and Ubuntu syslogs. The goal of this widespread collection is to provide a base for the
494 Forensics/Analytics component.

495 *4.1.2.4 Mitigation and Containment*

496 The Mitigation and Containment component provides the ability to limit a destructive event's effect on
497 the enterprise. This component may be able to interact with a security team for greater effectiveness
498 and may have the option to provide automated response to certain DI events. This response can involve
499 stopping execution of associated programs, disabling user accounts, disconnecting a system from the
500 network, and more, depending on the threat. Other actions may involve removing software from a
501 system, restarting services, or copying the threat to a safe environment for analysis.

502 For the Mitigation and Containment capability, we use a combination of tools. Cisco AMP provides the
503 ability to remove malicious files on sight—combined with its event detection capability, this can be
504 leveraged to quickly respond to malware on user systems. Cisco ISE provides quarantine functions that
505 can be used to respond to detected malware and poor machine posture as well as to network events in
506 Stealthwatch. Semperis DSP provides the ability to quickly and automatically revert detected changes in
507 Active Directory, mitigating the use of backdoors and other malicious domain changes. Semperis DSP
508 can also disable user accounts to prevent further changes from compromised or maliciously created
509 accounts. Glasswall provides the ability to sanitize malicious or noncompliant email attachments before
510 they ever reach the user's inbox, thereby eliminating malicious content in email attachments.

511 *4.1.2.5 Forensics/Analytics*

512 The Forensics/Analytics component uses the logs generated by event detection and the enterprise to
513 discover the source and effects of the DI event and learn about how to prevent similar events in the
514 future, if possible. This component will typically allow an organization to analyze malware or logs related
515 to the malware's execution and produce information such as: the servers that the malware
516 communicates with, or the executable's signature, to improve detection of the malware in the future.
517 Furthermore, the ability to examine machines affected by malware for lasting effects may be desirable.
518 The information gained from forensic analysis can also be used to enhance the organization's
519 protections against malware and potentially reform policy in the organization.

520 For the Forensics/Analytics capability, we use a combination of tools. Cisco AMP provides the ability to
521 review the history of malicious files to determine the source and movement across the enterprise.
522 Symantec Security Analytics provides the ability to analyze network traffic in a similar manner. ArcSight
523 ESM provides event correlation capabilities for logs collected from almost all the other capabilities,
524 allowing processing of events before they are reported to the security team. Symantec ICA provides
525 additional analysis capabilities for logs as well as aggregation and visualization of certain potentially
526 malicious movements within the enterprise. These products aid in the future prevention of such attacks
527 as well as determine the scope of the event's effect on the system.

528 **4.1.2.6 Reporting**

529 The Reporting component is primarily an interface between various components of the architecture and
530 the security team. It allows alerting based on events through email and dashboards, depending on the
531 organization's need. The reporting capabilities are best used throughout the entirety of an event—they
532 can be used to alert the security team when an event starts as well as to provide regular status updates
533 when events are not happening or have just finished.

534 For the Reporting capability, we use Micro Focus ArcSight. ArcSight can send email alerts and generate
535 reports based on the log correlation and analysis that it performs. By ensuring integration of as many
536 relevant logs as possible with ArcSight's logging capabilities, we can use various indicators to trigger
537 alerts when certain logs or sets of logs are received by ArcSight.

538 **5 Security Characteristic Analysis**

539 The purpose of the security characteristic analysis is to understand the extent to which the project
540 meets its objective of demonstrating a DI detect-and-respond solution. In addition, it seeks to
541 understand the security benefits and drawbacks of the example solution.

542 **5.1 Assumptions and Limitations**

543 The security characteristic analysis has the following limitations:

- 544 ▪ It is neither a comprehensive test of all security components nor a red-team exercise.
- 545 ▪ It cannot identify all weaknesses.
- 546 ▪ It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these
547 devices would reveal only weaknesses in implementation that would not be relevant to those
548 adopting this reference architecture.

549 **5.2 Build Testing**

550 The purpose of the security characteristic analysis is to understand the extent to which the building
551 block meets its objective of detecting and responding to DI events. Furthermore, the project aims to
552 facilitate analysis of these events during and after an attack. In addition, it seeks to understand the
553 security benefits and drawbacks of the reference design.

554 **5.3 Scenarios and Findings**

555 One aspect of our security evaluation involved assessing how well the reference design addresses the
556 security characteristics that it was intended to support. The Cybersecurity Framework Subcategories
557 were used to provide structure to the security assessment by consulting the specific sections of each
558 standard that are cited in reference to a Subcategory. The cited sections provide validation points that

559 the example solution would be expected to exhibit. Using the Cybersecurity Framework Subcategories
560 as a basis for organizing our analysis allowed us to systematically consider how well the reference design
561 supports the intended security characteristics.

562 Below are the scenarios created to test various aspects of this architecture. More detailed resolutions
563 and mappings of these scenarios' requirements to the Cybersecurity Framework can be found in
564 [Appendix D](#).

565 5.3.1 Ransomware via Web Vector and Self-Propagation

566 5.3.1.1 Scenario

567 The following scenario was simulated to test the architecture's defense against ransomware.
568 A user mistakenly downloads ransomware from an external web server. When the user executes this
569 malicious software, it generates a cryptographic key, which is sent back to the external web server. The
570 malware then utilizes a privilege escalation exploit to propagate across the network. The malicious
571 software encrypts files on the machines to which it propagated and demands payment in exchange for
572 decryption of these files.

573 5.3.1.2 Resolution

574 The build provides a significant defense in depth against this use case.

575 The **Event Detection** capability provides the ability to detect malicious software on the system and
576 generate logs and alerts based on this activity. It also allows for the detection of suspicious network
577 behavior, such as propagation.

578 The **Mitigation and Containment** capability provides the ability to halt execution of the ransomware and
579 remove it from the system. Furthermore, it allows quarantine of the affected machine(s) from the
580 network after detection of malicious activity.

581 The **Integrity Monitoring** capability provides the ability to collect changes to files, including changes
582 made by the ransomware as well as the ransomware's first creation or download onto the system.

583 When forwarded to the **Logging** capability, these logs in combination with others can be used to identify
584 the scope of the attack.

585 The **Reporting** capability uses logs from the above capabilities to report on malicious activity and to
586 increase response time.

587 The **Forensics/Analytics** capability analyzes logs related to the event to provide information that can be
588 used to strengthen defenses against the attack in the future. This includes the websites it communicated
589 with or was downloaded from, the signature of the executable, and the scope of the attack.

590 *5.3.1.3 Other Considerations*

591 Because malware comes in many forms, it is imperative to have multiple layers of defense against it
592 while also working to actively improve these defenses. An early defense against malware means
593 blacklisting known malicious sites. However, because this must be done entirely before the attack takes
594 place, it is out of scope of this build.

595 This build suggests a Forensics/Analytics capability specifically for informing and strengthening the
596 enterprise's defenses against future attacks. This is a function of the Respond Category—learning from
597 attacks can inform defense of such attacks in the future, both in the Protect and Detect phases of the
598 attack. Blacklisting is one such defense that can be informed by the Respond Category, and Event
599 Detection is another.

600 *5.3.2 Destructive Malware via USB Vector*601 *5.3.2.1 Scenario*

602 The following scenario was simulated to test the architecture's defense against destructive malware.

603 A user finds an unmarked Universal Serial Bus (USB) device and inserts it into his or her system. The USB
604 device contains malicious software that may run automatically or with user interaction. The malicious
605 software modifies and deletes the user's files, removing text from text files and entirely deleting any
606 media files it finds. The software does not offer a recovery mechanism as ransomware might, aiming
607 only to corrupt files.

608 *5.3.2.2 Resolution*

609 The build provides several mechanisms to detect and mitigate this use case.

610 The **Integrity Monitoring** capability provides the ability to detect changes to the file system, allowing the
611 changes and deletions to be detected and logged. Furthermore, information about what program (and
612 by extension, where the program was located—that is, on a USB drive) is included in the logs.

613 The **Logging** capability is used to collect logs from the integrity monitoring capability for posterity, as
614 well as from Windows event logs to monitor usage of external drives in comparison to normal usage.

615 The **Event Detection** capability provides the ability to detect malicious files on the USB inserted into the
616 system. It also can detect execution of these files.

617 The **Mitigation and Containment** capability provides the ability to stop malicious files from executing as
618 well as delete the files on the USB drive.

619 *5.3.2.3 Other Considerations*

620 USB attacks do not always come in the form of disguised file-based malware. As USB attacks allow direct
621 interfacing with the hardware of the system, they can aim to destroy the system via electrical attacks or
622 involve impersonation of a keyboard or other devices to avoid detection and gain privileges. These
623 attacks may be better mitigated through a thorough physical security policy and restrictions on the
624 types of allowed connected devices. Advanced attacks that involve manipulation of hardware can
625 become increasingly difficult to detect once plugged into the system. A prevention solution involving
626 backups, physical security, and employee education is often more effective.

627 *5.3.3 Accidental VM Deletion via Maintenance Script*628 *5.3.3.1 Scenario*

629 The following scenario was simulated to test the architecture's defense against data integrity events
630 that occur on virtual machines.

631 A routine maintenance script on the system causes an error. During a move operation in the Hyper-V
632 system, the script deletes an important virtual machine (VM). A maintenance script with an error of this
633 type could be a side effect of a normal system function or an error made by a member of the
634 organization. It is expected that the build will mitigate the damage caused to virtual machines in such an
635 incident.

636 *5.3.3.2 Resolution*

637 The build provides several methods for detecting and analyzing this use case. Errors in custom code are
638 often difficult to detect at run time and because they are usually run by privileged programs. Classifying
639 them as malware or even as "unintended" changes is often undesirable.

640 The **Integrity Monitoring** capability provides the ability to detect changes to VM configurations, allowing
641 the VM deletion to be detected and logged. Furthermore, information about what program (i.e., the
642 routine maintenance script) is included in the logs.

643 The **Logging** capability provides the ability to collect these events for posterity.

644 The **Forensics/Analytics** capability provides the ability to analyze the events after the fact to enable the
645 security team to understand the impact, resolve the error in the script, and inform the restoration
646 process.

647 *5.3.3.3 Other Considerations*

648 This solution will aid in identifying the script that causes a configuration change or deletion, but
649 ultimately some things cannot be automated by the solution. Understanding the impact of the event
650 requires a security team, and this build aims to provide the tools for a security team to do so.

651 Resolving an error in a maintenance script will also typically require effort on the part of the system
652 administrators. Judgment on whether a script should be deleted, disabled, or left running during the
653 remediation process is necessary and can depend on the size of the script, the affected assets, and the
654 availability of resources to put toward resolving the error. Because of these considerations, the
655 organization is left to decide whether a malfunctioning script should be treated like malware (see other
656 scenarios that deal with malware) or as a part of the enterprise as it is possible that the remediation
657 process is lengthy and exceeds the scope of the Detect/Respond Categories of the NIST Cybersecurity
658 Framework.

659 [5.3.4 Backdoor Creation via Email Vector](#)

660 [5.3.4.1 Scenario](#)

661 The following scenario was simulated to test the architecture’s defense against malicious email
662 attachments.

663 A user unknowingly opens a malicious attachment that was received in an email. When opened, the
664 attachment quietly fetches files from an external web server. It then creates several unapproved
665 backdoor accounts on the authentication server. It is expected that the build will mitigate the impacts of
666 such an incident.

667 [5.3.4.2 Resolution](#)

668 The build provides several layers of defense against this use case. The **Integrity Monitoring** capability
669 forwards logs of file changes and Active Directory changes to the Logging capability, allowing recording
670 and detection of both the malicious attachment’s download and the changes it makes to the system
671 account structure.

672 The **Logging** and **Reporting** capabilities provide the ability to generate alerts based on events for the
673 security team to quickly take action to resolve them.

674 The **Event Detection** capability provides detection at two points in time—both before the attachment
675 reaches the user’s inbox and, should this fail, after the attachment downloads to the system.

676 The **Mitigation and Containment** capability provides mitigation before the attachment reaches the
677 user’s inbox, as well as when it is on the user’s system.

678 The **Forensics/Analytics** capability provides the ability to view the network traffic generated by the
679 spreadsheet when fetching its malicious files from the web server. This can inform defense of the
680 enterprise in the Protect Category of the Cybersecurity Framework before any similar events happen in
681 the future.

682 *5.3.4.3 Other Considerations*

683 Another defense that can partially prevent this use case is detection of the email as spam. However, as
684 this is often a function of the email provider and not a separate security solution, it is out of scope for
685 this build.

686 This build suggests a Forensics/Analytics capability specifically for informing and strengthening the
687 defenses of the enterprise against future attacks. This is a function of the Respond Category—learning
688 from attacks can inform the defense of such attacks in the future, both in the Protect and Detect phases
689 of the attack.

690 *5.3.5 Database Modification via Malicious Insider*691 *5.3.5.1 Scenario*

692 The following scenario was simulated to test the architecture’s defense against unwanted database
693 modification.

694 A malicious insider has access to an enterprise database through a web page. The insider leverages a
695 vulnerability in the web page to delete a large portion of the database. Though this scenario deals with a
696 web vulnerability, other vulnerabilities could be used to modify the database undesirably. It is expected
697 that the build will mitigate the impact that a user can have on the database.

698 *5.3.5.2 Resolution*

699 The build provides several layers of defense against this use case. The **Integrity Monitoring** capability is
700 used to detect changes to the database.

701 These changes are forwarded to the **Logging** capability, which also collects information about web
702 requests.

703 The **Reporting** capability provides the ability to generate alerts and quickly inform the security team of
704 an anomaly, based on the logs.

705 The **Forensics/Analytics** capability is used to investigate the malicious access as well as identify the page
706 with the vulnerability. Because this vulnerability is a vulnerability in custom code, it is important for
707 information-gathering mechanisms to be in place to provide ample information for the resolution of this
708 vulnerability.

709 *5.3.5.3 Other Considerations*

710 This use case highlights the need for a response-oriented build to collaborate with an identify-oriented
711 build. Identification and resolution of vulnerabilities in custom code are sometimes feasible only through
712 gathering information after the vulnerability has been exploited. This build provides the mechanisms to

713 gather such information, but it is ultimately up to the security team to resolve the vulnerability and learn
714 from the attack.

715 [5.3.6 File Modification via Malicious Insider](#)

716 [5.3.6.1 Scenario](#)

717 The following scenario was simulated to test the architecture's defense against malicious file and backup
718 modification.

719 A malicious insider is assumed to have stolen administrator-level credentials through non-technical
720 means. The insider, using these credentials, uses remote Windows PowerShell sessions to uniformly
721 modify employee stock information to their benefit across several machines. This attack will also target
722 the enterprise's backup system to modify all records of the previous stock information. It is expected
723 that the aspects of the build described above will mitigate the ability of the user to target and modify
724 enterprise data and backups. The method of securing administrator credentials will be considered out of
725 scope for this solution.

726 [5.3.6.2 Resolution](#)

727 The build has several layers of defense against this use case. The **Integrity Monitoring** capability detects
728 changes to files and backups caused by a malicious insider.

729 When forwarded to the **Logging and Reporting** capabilities, the build can report on these changes.
730 Irregularities or differences from the normal backup schedule are important indicators of a compromise.

731 When the security team is alerted to a malicious insider, they can use the **Mitigation and Containment**
732 capability to disable the insider's access.

733 [5.3.6.3 Other Considerations](#)

734 Malicious insiders are powerful adversaries, because they already have some level of access to the
735 system. The existence of malicious insiders widens the threat surface of an enterprise to needing
736 defense against internal machines as well as external machines. For this reason, this build includes
737 mitigations against threats already present inside the enterprise and not just threats that originate
738 externally. This includes the ability to disable user accounts, quarantine machines, and monitor network
739 traffic originating from within the enterprise.

740 [5.3.7 Backdoor Creation via Compromised Update Server](#)

741 [5.3.7.1 Scenario](#)

742 The following scenario was simulated to test the architecture's defense against compromised update
743 servers.

744 An update server that services an enterprise machine is compromised and provides an update to the
745 enterprise machine that contains a backdoor. The update contains a vulnerable version of vsftpd,
746 allowing an attacker root access into the machine updated by the compromised server. It is expected
747 that the build will mitigate the impact of a compromised update server.

748 *5.3.7.2 Resolution*

749 The build has several layers of defense against this use case. **Integrity Monitoring** detects changes to
750 programs, providing information about how and when the program was changed. It also detects
751 changes to any files made by an intruder.

752 The **Event Detection** capability is used to detect the malicious update through signature detection.
753 Furthermore, it detects the connection to the open port by an attacker.

754 The **Mitigation and Containment** capability is used to delete/quarantine the malicious update, stopping
755 the port from being accessible. It can also be used to quarantine the machine from the network, to
756 prevent the spread of the intrusion and remove the attacker's access.

757 *5.3.7.3 Other Considerations*

758 The use of the Event Detection capability to detect largely assumes that the update has been reported
759 as vulnerable, either through a well-known history of being vulnerable or through intelligence-sharing
760 channels. As such, an event detection capability would, in some cases of new custom attacks, be unable
761 to detect this at first sight. However, the build provides other tools, such as monitoring network activity,
762 that can alert security staff to such attacks.

763 Using a data integrity identify-and-protect build to incorporate Blacklisting and Network Protection as
764 part of the defense is beneficial, as a use case that involves connecting to an unused port would be
765 entirely defeated by a network protection white list of allowed ports.

766 **6 Future Build Considerations**

767 The NCCoE is creating an overarching guide to combining the architectures of the various DI projects:
768 Identify and Protect, Detect and Respond, and Recover. These architectures share some commonalities,
769 such as integrity monitoring, as well as some potential integrations and cycles that could not be
770 expressed in just one of the practice guides. The different Functions of the Cybersecurity Framework are
771 intended to prepare and inform one another, and the overarching guide addresses those issues.

772 The NCCoE is also considering additional data security projects that map to the Cybersecurity
773 Framework Core Functions of Identify, Protect, Detect, Respond, and Recover. These projects will focus
774 on data confidentiality—the defense of enterprise systems from attacks that would compromise the
775 secrecy of data.

776 **Appendix A List of Acronyms**

AMP	Advanced Malware Protection
COI	Community of Interest
DE	Detect
DI	Data Integrity
DSP	Directory Services Protector
ESM	Enterprise Security Manager
ICA	Information Centric Analytics
ISE	Identity Services Engine
IT	Information Technology
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
PR	Protect
RMF	Risk Management Framework
RS	Respond
SP	Special Publication
USB	Universal Serial Bus
VM	Virtual Machine
vsftpd	Very Secure File Transfer Protocol Daemon

777 **Glossary**

Access Control The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances)

SOURCE: Federal Information Processing Standard (FIPS) 201; CNSSI-4009

Architecture A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution, while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability).

SOURCE: FIPS 201-2

Audit Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.

SOURCE: CNSSI 4009-2015

Backdoor An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.

SOURCE: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 2

Backup A copy of files and programs made to facilitate recovery if necessary.

SOURCE: NIST SP 800-34 Rev. 1

Compromise Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

SOURCE: NIST SP 800-32

Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions.
	SOURCE: NIST SP 800-137
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
	SOURCE: CNSSI 4009-2015 (NSPD-54/HSPD-23)
Data	A subset of information in an electronic format that allows it to be retrieved or transmitted.
	SOURCE: CNSSI-4009
Data Integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
	SOURCE: CNSSI-4009
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
	SOURCE: FIPS 199 (44 U.S.C., Sec. 3542)
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
	SOURCE: CNSSI 4009-2015 (NIST SP 800-30 Rev. 1)
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
	SOURCE: FIPS 200 (44 U.S.C., Sec. 3502)
Insider	An entity inside the security perimeter that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

SOURCE: NIST SP 800-82 Rev. 2 (RFC 4949)

Kerberos An authentication system developed at the Massachusetts Institute of Technology (MIT). Kerberos is designed to enable two parties to exchange private information across a public network.

SOURCE: NIST SP 800-47

Log A record of the events occurring within an organization's systems and networks.

SOURCE: NIST SP 800-92

Malware A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

SOURCE: NIST SP 800-111

Privacy Assurance that the confidentiality of, and access to, certain information about an entity is protected.

SOURCE: NIST SP 800-130

Risk The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals, resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

SOURCE: FIPS 200

Risk Assessment The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis.

SOURCE: NIST SP 800-63-2

Risk Management Framework The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

SOURCE: NIST SP 800-82 Rev. 2 (NIST SP 800-37)

Security Control	A protection measure for a system. SOURCE: NIST SP 800-123
Virtual Machine	Software that allows a single host to run one or more guest operating systems. SOURCE: NIST SP 800-115
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: FIPS 200 (adapted from CNSSI 4009)

Appendix B References

- 778 [1] A. Sedgewick, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1,
779 National Institute of Standards and Technology, Gaithersburg, Maryland, Apr. 2018, 55 pp.
780 Available: <https://www.nist.gov/cyberframework/framework>.
- 781 [2] L. Kauffman, N. Lesser and B. Abe, *Executive Technical Workshop on Improving Cybersecurity
782 and Consumer Privacy*, NISTIR 8050, National Institute of Standards and Technology,
783 Gaithersburg, Maryland, April 2015, 155pp. Available:
784 <https://nccoe.nist.gov/sites/default/files/library/nistir-8050-draft.pdf>
- 785 [3] G. Stoneburner, *et al.*, *Guide for Conducting Risk Assessments*, NIST Special Publication (SP), 800-
786 30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland,
787 September 2012, 95 pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-30r1>.
- 788 [4] R. Ross, *et al.*, *Guide for Applying the Risk Management Framework to Federal Information
789 Systems*, NIST Special Publication (SP) 800-37, National Institute of Standards and Technology,
790 Gaithersburg, Maryland, February 2010, 101pp. Available:
791 <http://dx.doi.org/10.6028/NIST.SP.800-37r1>.
- 792 [5] R. Ross *et al.*, *Managing Information Security Risk*, NIST Special Publication (SP) 800-39, National
793 Institute of Standards and Technology, Gaithersburg, Maryland, March 2011, 87pp. Available:
794 <http://dx.doi.org/10.6028/NIST.SP.800-39>.
- 795 [6] M. Souppaya *et al.*, *Guide to Enterprise Patch Management Technologies*, NIST Special
796 Publication (SP) 800-40 Revision 3, National Institute of Standards and Technology,
797 Gaithersburg, Maryland, July 2013, 25pp. Available: [http://dx.doi.org/10.6028/NIST.SP.800-40r3](http://dx.doi.org/10.6028/NIST.SP.800-
798 40r3).
- 799 [7] R. Ross *et al.*, *Security and Privacy Controls for Federal Information Systems and Organizations*,
800 NIST Special Publication (SP) 800-53 Revision 4, National Institute of Standards and Technology,
801 Gaithersburg, Maryland, April 2013, 461pp. Available: [https://doi.org/10.6028/NIST.SP.800-53r4](https://doi.org/10.6028/NIST.SP.800-
802 53r4).
- 803 [8] U.S. Department of Commerce. *Security Requirements for Cryptographic Modules*, Federal
804 Information Processing Standards (FIPS) Publication 140-3, Mar. 2019, 65pp. Available:
805 <https://csrc.nist.gov/publications/detail/fips/140/3/final>.
- 806 [9] K. Kent *et al.*, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special
807 Publication (SP) 800-86, National Institute of Standards and Technology, Gaithersburg,
808 Maryland, August 2006, 121pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-86>.

- 809 [10] K. Kent and M. Souppaya, *Guide to Computer Security Log Management*, NIST Special
810 Publication (SP) 800-92, National Institute of Standards and Technology, Gaithersburg,
811 Maryland, September 2006, 72pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-92>.
- 812 [11] P. Bowen *et al.*, *Information Security Handbook: A Guide for Managers*, NIST Special Publication
813 (SP) 800-100, National Institute of Standards and Technology, Gaithersburg, Maryland, October
814 2006, 178pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-100>.
- 815 [12] M. Swanson *et al.*, *Contingency Planning Guide for Federal Information Systems*, NIST Special
816 Publication (SP) 800-34 Revision 1, National Institute of Standards and Technology,
817 Gaithersburg, Maryland, May 2010, 148pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-34r1>.
- 819 [13] Office of Management and Budget (OMB), *Management of Federal Information Resources*, OMB
820 Circular No. A-130, November 2000. Available:
https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a13_revised.pdf.
- 823 [14] P. Cichonski *et al.*, *Computer Security Incident Handling Guide*, NIST Special Publication (SP) 800-
824 61 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, August
825 2012, 79pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-61r2>.
- 826 [15] M. Souppaya and K. Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops
827 and Laptops*, NIST Special Publication (SP) 800-83 Revision 1, National Institute of Standards and
828 Technology, Gaithersburg, Maryland, July 2013, 46pp. Available:
<http://dx.doi.org/10.6028/NIST.SP.800-83r1>.
- 830 [16] C. Johnson *et al.*, *Guide to Cyber Threat Information Sharing*, NIST Special Publication (SP) 800-
831 150, National Institute of Standards and Technology, Gaithersburg, Maryland, October 2016,
832 42pp. Available: <http://dx.doi.org/10.6028/NIST.SP.800-150>.
- 833 [17] M. Bartock *et al.*, *Guide for Cybersecurity Event Recovery*, NIST Special Publication (SP) 800-184,
834 National Institute of Standards and Technology, Gaithersburg, Maryland, December 2016, 52pp.
<http://dx.doi.org/10.6028/NIST.SP.800-184>.

836 **Appendix C Functional Evaluation**

837 A functional evaluation of the data integrity (DI) example implementation, as constructed in our
838 laboratory, was conducted to verify that it meets its objective of detecting and responding to DI events.
839 Furthermore, this project aims to analyze the events to aid recovery and protection of the enterprise
840 against future attacks. The evaluation verified that the example implementation could perform the
841 following functions:

- 842 • Detect malicious network activity, malicious mobile code, malicious code execution, and
843 unauthorized user behavior.
844 • Contain and analyze these types of incidents.
845 • Mitigate the impact of these incidents as they occur.
846 • Report relevant details for use in mitigation and protection against future events.

847 [Section D.1](#) describes the format and components of the functional test cases. Each functional test case
848 is designed to assess the capability of the example implementation to perform the functions listed
849 above and detailed in [Section D.1](#).

850 **C.1 Data Integrity Functional Test Plan**

851 One aspect of our security evaluation involved assessing how well the reference design addresses the
852 security characteristics that it was intended to support. The Cybersecurity Framework Subcategories
853 were used to provide structure to the security assessment by consulting the specific sections of each
854 standard that are cited in reference to that Subcategory. The cited sections provide validation points
855 that the example solution is expected to exhibit. Using the Cybersecurity Framework Subcategories as a
856 basis for organizing our analysis allowed us to systematically consider how well the reference design
857 supports the intended security characteristics.

858 This plan includes the test cases necessary to conduct the functional evaluation of the DI example
859 implementation, which is currently deployed in a lab at the National Cybersecurity Center of Excellence.
860 The implementation tested is described in [Section 4](#).

861 Each test case consists of multiple fields that collectively identify the goal of the test, the specifics
862 required to implement the test, and how to assess the results of the test. Table 6-1 describes each field
863 in the test case.

864 **Table 6-1 Test Case Fields**

Test Case Field	Description
Parent requirement	Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement.

Test Case Field	Description
Testable requirement	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.
Description	Describes the objective of the test case.
Associated Cybersecurity Framework Subcategories	Lists the National Institute of Standards and Technology Special Publication 800-53 rev 4 controls addressed by the test case.
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
Expected results	The expected results for each variation in the test procedure.
Actual results	The observed results.
Overall result	The overall result of the test as pass/fail. In some test-case instances, the determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.

865 **C.2 Data Integrity Use Case Requirements**

866 Table 6-2 identifies the DI functional requirements addressed in the test plan and associated test cases.

867 **Table 6-2 Capability Requirements**

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 1	The DI example implementation shall detect and respond to malware that encrypts files and displays notice demanding payment.		Data Integrity DR-1

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 1.a		File integrity changes are collected and logged.	Data Integrity DR-1
CR 1.b		Access is halted.	Data Integrity DR-1
CR 1.c		Executable is identified as malicious, using a blacklist.	Data Integrity DR-1
CR 1.d		Executable is identified as malicious through analysis, and blacklist is updated.	Data Integrity DR-1
CR 1.e		Execution is halted.	Data Integrity DR-1
CR 1.f		Downloads are identified as malicious, using a blacklist.	Data Integrity DR-1
CR 1.g		Downloads are identified as malicious through analysis, and blacklist is updated.	Data Integrity DR-1
CR 1.h		Downloads are prevented.	Data Integrity DR-1
CR 1.i		Attempts to propagate are detected.	Data Integrity DR-1
CR 1.j		Machines attempting to propagate are prevented from propagating.	Data Integrity DR-1
CR 1.k		Suspicious network traffic is detected, and blacklist is updated.	Data Integrity DR-1

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 2	The DI example implementation shall detect and respond to malware inserted via Universal Serial Bus (USB) that modifies and deletes user data.		Data Integrity DR-2
CR 2.a		File integrity changes are collected and logged.	Data Integrity DR-2
CR 2.b		The insertion of a USB device is detected and logged.	Data Integrity DR-2
CR 2.c		The executable is identified as malicious, using a blacklist.	Data Integrity DR-2
CR 2.d		The executable is identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-2
CR 2.e		Malicious executable is halted or deleted.	Data Integrity DR-2
CR 3	The DI example implementation shall detect and respond to virtual machine deletion.		Data Integrity DR-3
CR 3.a		Virtual machine integrity changes are collected and logged.	Data Integrity DR-3

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 3.b		The event causing deletion of the virtual machine is analyzed.	Data Integrity DR-3
CR 4	The DI example implementation shall detect and respond to malware received via phishing email.		Data Integrity DR-4
CR 4.a		Configuration integrity changes are collected and logged.	Data Integrity DR-4
CR 4.b		Email is identified as malicious, using a blacklist.	Data Integrity DR-4
CR 4.c		Email is identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-4
CR 4.d		Email is deleted or sorted into spam.	Data Integrity DR-4
CR 4.e		The attachment is identified as malicious, using a blacklist.	Data Integrity DR-4
CR 4.f		The attachment is identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-4
CR 4.g		Execution of the spreadsheet is stopped, and the blacklist is updated if necessary.	Data Integrity DR-4

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 4.h		The downloads are identified as malicious, using a blacklist.	Data Integrity DR-4
CR 4.i		The downloads are identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-4
CR 4.j		The malicious executable is halted or deleted.	Data Integrity DR-4
CR 4.k		Suspicious network traffic is detected, and blacklist is updated.	Data Integrity DR-4
CR 5	The DI example implementation shall detect and respond to changes to the database made through a web server vulnerability in custom code.		Data Integrity DR-5
CR 5.a		Database integrity changes are collected and logged.	Data Integrity DR-5
CR 5.b		Information about the client interacting with the web service is collected and logged.	Data Integrity DR-5
CR 5.c		Information from the attack is reported for use in protection against future events.	Data Integrity DR-5

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 6	The DI example implementation shall detect and respond to targeted modification by malicious insiders with elevated privileges.		Data Integrity DR-6
CR 6.a		File integrity changes are collected and logged.	Data Integrity DR-6
CR 6.b		Backup integrity changes are collected and logged.	Data Integrity DR-6
CR 6.c		Detected changes are reported.	Data Integrity DR-6
CR 6.d		Associated user accounts are contained.	Data Integrity DR-6
CR 7	The DI example implementation shall detect and respond to an intrusion via compromised update server.		Data Integrity DR-7
CR 7.a		Program integrity changes are collected and logged.	Data Integrity DR-7
CR 7.b		The downloaded service is identified as malicious, using a blacklist.	Data Integrity DR-7
CR 7.c		The downloaded service is identified as malicious through analysis, and the blacklist is updated.	Data Integrity DR-7

Capability Requirement (CR) ID	Parent Requirement	Subrequirement 1	Test Case
CR 7.d		The service is halted and reverted or deleted.	Data Integrity DR-7
CR 7.e		The download site is temporarily added to the blacklist.	Data Integrity DR-7
CR 7.f		The port opened by the service is detected.	Data Integrity DR-7
CR 7.g		The opened port is closed.	Data Integrity DR-7
CR 7.h		The intrusion into the infected machine is detected.	Data Integrity DR-7
CR 7.i		The intrusion into the infected machine is contained.	Data Integrity DR-7

868 **C.3 Test Case: Data Integrity DR-1**869 **Table 6-3 Test Case ID: Data Integrity DR-1**

Parent requirement	(CR 1) The DI example implementation shall detect and respond to malware that encrypts files and displays notice demanding payment.
Testable requirement	(CR 1.a) Integrity Monitoring, Logging, Reporting, (CR 1.c, CR 1.d, CR 1.f, CR 1.g, CR 1.i) Event Detection, (CR 1.b, CR 1.e, CR 1.j) Mitigation and Containment, (CR 1.h, CR 1.k) Forensics and Analytics
Description	Show that the DI solution has capabilities to detect behaviors typical of ransomware, and mitigate these behaviors appropriately.
Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2, DE.CM-4, DE.CM-7, DE.DP-2, DE.AE-1, DE.CM-1
Preconditions	User navigates to a malicious website and clicks on an ad for a virus cleaner. The virus cleaner is ransomware, which propagates across the domain and encrypts user files.
Procedure	<p>The Integrity Monitoring capability is used to monitor and log changes to the integrity of files.</p> <p>The Logging capability and the Reporting capability are used to notify the security team of changes to the integrity of files and of potentially malicious events.</p> <p>The Event Detection capability is used to detect the ransomware in real time before or during its execution. It is also used to detect propagation of the ransomware.</p> <p>The Mitigation and Containment capability is used to halt the ransomware's execution and delete it from the system. It is also used to quarantine affected machines once a breach is discovered.</p> <p>The Forensics/Analytics capability is used to discover malicious hosts and websites accessed by the ransomware.</p>
Expected Results (pass)	<p>The build can monitor and report changes to the integrity of files (CR 1.a).</p> <p>The machine is quarantined when malware is detected (CR 1.b).</p>

	<p>Malicious executables are identified through signature detection or analysis (CR 1.c, CR 1.d).</p> <p>Malicious executables are prevented from executing (CR 1.e).</p> <p>Malicious downloads are identified through signature detection or analysis (CR 1.f, CR 1.g).</p> <p>Malicious downloads are prevented (CR 1.h).</p> <p>Propagation of malicious executables is detected (CR 1.i).</p> <p>Propagation of malicious executables is prevented (CR 1.j).</p> <p>Network traffic is captured and analyzed for suspicious activity (CR 1.k).</p>
Actual Results	<p>Tripwire Enterprise (Integrity Monitoring) is used to successfully detect changes to files on the affected systems.</p> <p>ArcSight ESM (Logging) is used to successfully log events from Event Detection and Integrity Monitoring for use in Reporting and Forensics/Analytics.</p> <p>ArcSight ESM (Reporting) is used to successfully report on malicious activity detected in logs.</p> <p>Cisco AMP (Event Detection) is used to successfully detect the malicious executable.</p> <p>Cisco AMP (Mitigation and Containment) is used to successfully remove malicious executables from the affected systems.</p> <p>Cisco Stealthwatch (Event Detection) is used to successfully capture malicious or suspicious network traffic from the executable.</p> <p>Cisco ISE (Mitigation and Containment) is used to successfully quarantine affected machines.</p> <p>Symantec Security Analytics (Forensics/Analytics) is used to successfully review network traffic generated by the ransomware for potentially malicious hosts and websites.</p>

	Symantec ICA (Forensics/Analytics) successfully displays relevant events from ArcSight for analysis to aid in identifying the malicious files for use in future Event Detection as well as for removal by the security team.
Overall Result	Pass. All requirements for this use case are met.

870 **C.4 Test Case: Data Integrity DR-2**

871 Table 6-4 Test Case ID: Data Integrity DR-2

Parent requirement	(CR 2) The DI example implementation shall detect and respond to malware inserted via USB that modifies and deletes user data.
Testable requirement	(CR 2.a) Integrity Monitoring, (CR 2.b, CR 2.c) Event Detection, (CR 2.d) Forensics and Analytics, (CR 2.e) Mitigation and Containment
Description	Show that the DI solution can detect behaviors of destructive malware and can mitigate these behaviors appropriately.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-4, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	A user inserts an unidentified USB drive into their computer. They click on a file on the drive, which immediately destroys any files on their machine.
Procedure	<p>The Integrity Monitoring capability is used to monitor integrity changes to the system.</p> <p>The Logging capability is used to collect logs from the integrity monitoring capability.</p> <p>The Event Detection capability is used to detect malicious files on the USB inserted into the system.</p> <p>The Mitigation and Containment capability is used to prevent malicious files from executing.</p>
Expected Results (pass)	<p>The build can monitor and report changes to the integrity of files (CR 2.a).</p> <p>The build can detect insertion of a USB (CR 2.b).</p> <p>Malicious executables are identified through signature detection or analysis (CR 2.c, CR 2.d).</p>

	<p>Malicious executables are prevented from executing (CR 2.e).</p> <p>Tripwire Enterprise (Integrity Monitoring) successfully detects changes made by an executable running from a USB.</p> <p>ArcSight ESM (Logging) successfully collects logs from the integrity monitoring capability. Furthermore, USB insertions can be collected by using Windows group policy.</p> <p>Cisco AMP (Event Detection) successfully detects malicious files on the USB drive.</p> <p>Cisco AMP (Mitigation and Containment) immediately deletes these malicious files on the system if they are copied. It also prevents execution if the file is run from the USB drive.</p>
Overall Result	Pass (partial). Cisco AMP does not immediately delete the file from the USB drive when it is plugged in if the user does not make any action (copy or execution). However, because both these actions trigger deletion, this is not a significant shortcoming as the file is otherwise harmless.

872 C.5 Test Case: Data Integrity DR-3

873 Table 6-5 Test Case ID: Data Integrity DR-3

Parent requirement	(CR 3) The DI example implementation shall detect and respond to virtual machine deletion.
Testable requirement	(CR 3.a) Integrity Monitoring, (CR 3.b) Forensics and Analytics
Description	Show that the DI solution can detect and analyze DI events that involve virtual machines.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	A routine maintenance script contains an error that accidentally deletes a virtual machine.
Procedure	<p>The Integrity Monitoring capability is used to monitor integrity changes to the system.</p> <p>The Logging capability is used to collect logs from the integrity monitoring capability.</p>

	The Forensics/Analytics capability is used to analyze logs and determine the cause of integrity events.
Expected Results (pass)	The build can monitor and report changes to the integrity of virtual machines (CR 3.a). The build can analyze the impact of DI events (CR 3.b).
Actual Results	Tripwire Enterprise (Integrity Monitoring) successfully monitors and logs changes to configurations of virtual machines. ArcSight ESM (Logging) successfully collects logs and reports on the events generated by the Integrity Monitoring capability, enabling faster response time. Symantec ICA (Forensics/Analytics) successfully displays relevant events from ArcSight for analysis to aid in identifying the file that causes the deletion.
Overall Result	Pass. All requirements for this use case are met.

874 **C.6 Test Case: Data Integrity DR-4**

875 Table 6-6 Test Case ID: Data Integrity DR-4

Parent requirement	(CR 4) The DI example implementation shall detect and respond to malware received via phishing email.
Testable requirement	(CR 4.a) Integrity Monitoring and Logging, (CR 4.b, CR4.e, CR 4.h, CR 4.k) Event Detection, (CR 4.c, CR 4.f, CR 4.i) Forensics and Analytics, (CR 4.d, CR 4.g, CR 4.j) Mitigation and Containment
Description	Show that the DI solution can detect malicious attachments and respond to malicious configuration changes.
Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	The user receives a phishing email with a malicious spreadsheet attached. The spreadsheet is downloaded and opened, causing account changes in Active Directory.
Procedure	The Integrity Monitoring capability is used to detect and log the account creation.

	<p>This information is forwarded to the Logging capability, along with other available Active Directory information.</p> <p>The email attachment is detected as malicious by the Event Detection capability and mitigated by the Mitigation and Containment capability, both when the file is in the inbox and when it is on the user's system.</p> <p>The solution can review the network traffic generated by the file when it calls out to the malicious web server to download files through Forensics/Analytics.</p>
Expected Results (pass)	<p>The build can monitor and report changes to the integrity of configurations (CR 4.a).</p> <p>Malicious emails are identified through signature detection or analysis (CR 4.b, CR 4.c).</p> <p>Emails identified as malicious are sorted into spam or deleted (CR 4.d).</p> <p>Malicious attachments are identified through signature detection or analysis (CR 4.e, CR 4.f).</p> <p>Malicious attachments are prevented from executing (CR 4.g).</p> <p>Malicious downloads are identified through signature detection or analysis (CR 4.h, CR 4.i).</p> <p>Malicious executables are prevented from executing (CR 4.j).</p> <p>Network traffic is captured and analyzed for suspicious activity (CR 4.k).</p>
Actual Results	<p>Semperis DSP (Integrity Monitoring) successfully monitors and logs changes to Active Directory.</p> <p>ArcSight ESM (Logging) successfully collects logs and reports on the events generated by the Integrity Monitoring capability, enabling faster response time.</p> <p>Glasswall FileTrust (Event Detection) successfully identifies the malicious attachment before it reaches the user's inbox.</p>

	<p>Glasswall FileTrust (Mitigation and Containment) successfully mitigates the malicious attachment before it reaches the user's inbox.</p> <p>The malicious file is successfully uploaded to Cisco AMP (Event Detection) for signature detection.</p> <p>Cisco AMP (Event Detection) successfully mitigates the file when found on user workstations.</p> <p>Symantec Security Analytics (Forensics/Analytics) is used to successfully detect network traffic involving download of files from the malicious server.</p>
Overall Result	<p>Pass (partial). Emails are not sorted into spam (CR 4.b-d); rather, the attachment is mitigated before reaching the user's inbox.</p> <p>Sorting emails into spam is often a function of the email infrastructure.</p>

876 **C.7 Test Case: Data Integrity DR-5**

877 Table 6-7 Test Case ID: Data Integrity DR-5

Parent requirement	(CR 5) The DI example implementation shall detect and respond to changes to the database made through a web server vulnerability in custom code.
Testable requirement	(CR 5.a) Integrity Monitoring, (CR 5.b) Logging, (CR 5.c) Reporting
Description	Show that the DI solution can detect and respond to an exploitation a vulnerability in custom code that leads to an attack on the database.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2
Preconditions	A vulnerability in the source code of an intranet web page is discovered by a malicious insider. The insider exploits this vulnerability to delete significant portions of the database.
Procedure	<p>The Integrity Monitoring capability is used to detect changes to the database.</p> <p>The Logging capability is used to monitor changes to the database and to log web requests.</p>

	<p>The Reporting capability is used to alert the security team of significant changes to the database.</p> <p>The Forensics/Analytics capability is used to investigate the malicious access as well as identify the page with the vulnerability.</p>
Expected Results (pass)	<p>The build can monitor and report changes to the integrity of the database (CR 5.a).</p> <p>Malicious interaction with the web server is detected (CR 5.b).</p> <p>Information about the attack is reported for use in maintaining the enterprise systems (CR 5.c).</p>
Actual Results	<p>Tripwire Enterprise (Integrity Monitoring) successfully monitors changes to the database configuration.</p> <p>ArcSight ESM (Logging) successfully logs changes to the database and web requests.</p> <p>ArcSight ESM (Reporting) successfully alerts the security team of changes to the database.</p> <p>Symantec Security Analytics (Forensics/Analytics) allows identification of web requests that could have caused the deletion, helping identify the web server's vulnerability in custom code.</p>
Overall Result	Pass. All requirements for this use case are met.

878 C.8 Test Case: Data Integrity DR-6

879 Table 6-8 Test Case ID: Data Integrity DR-6

Parent requirement	(CR 6) The DI example implementation shall detect and respond to targeted modification by malicious insiders with elevated privileges.
Testable requirement	(CR 6.a, 6.b) Integrity monitoring, (CR 6.c) Reporting, (CR 6.d) Mitigation and Containment
Description	Show that the DI solution can detect and respond to targeted modification of assets and backups by malicious insiders.
Associated Cybersecurity Framework Subcategories	DE.AE-5, DE.CM-3, DE.CM-7, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2

Preconditions	A malicious insider attempts to modify targeted information in both the enterprise systems and the backup systems by using elevated credentials obtained extraneously.
Procedure	<p>The Integrity Monitoring capability is used to detect changes to the file system.</p> <p>The Reporting capability is used to notify the security team of changes to critical data assets.</p> <p>The Mitigation and Containment capability is used to prevent the malicious user from making further modifications.</p>
Expected Results (pass)	<p>The build can monitor and report changes to the integrity of files and backups (CR 6.a, CR 6.b).</p> <p>Information about the attack is reported for use in responding to the threat (CR 6.c).</p> <p>User accounts associated with the attack are contained (CR 6.d).</p>
Actual Results	<p>Tripwire Enterprise (Integrity Monitoring) successfully detects changes to files and backups caused by a malicious insider.</p> <p>ArcSight ESM (Reporting) successfully reports and alerts administrators via email on changes made to files by a malicious insider.</p> <p>Semperis DSP (Mitigation and Containment) successfully disables the user accounts associated with malicious insider activity.</p>
Overall Result	Pass. All requirements for this use case are met.

880 C.9 Test Case: Data Integrity DR-7

881 Table 6-9 Test Case ID: Data Integrity DR-7

Parent requirement	(CR 7) The DI example implementation shall detect and respond to an intrusion via compromised update server.
Testable requirement	(CR 7.a) Integrity Monitoring, (CR 7.b) Event Detection, (CR 7.c) Forensics and Analytics, (CR 7.d, CR 7.e) Mitigation and Containment
Description	Show that the DI solution can detect a malicious update from a compromised update server as well as detect and respond to a resulting intrusion.

Associated Cybersecurity Framework Subcategories	PR.DS-6, DE.AE-5, DE.CM-5, DE.DP-2, RS.CO-2, DE.AE-2, DE.AE-3, DE.AE-4, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.RP-1, RS.MI-1, RS.MI-2, DE.CM-4, DE.CM-7, DE.AE-1, DE.CM-1,
Preconditions	An external update server has been compromised, and a user workstation attempts to update from this server.
Procedure	<p>The Integrity Monitoring capability is used to detect changes to the integrity of programs and files.</p> <p>The Event Detection capability is used to detect the malicious update. It is also used to detect the connection to the machine.</p> <p>The Mitigation and Containment capability is used to halt execution of the update and delete it. It is also used to contain the intrusion.</p>
Expected Results (pass)	<p>The build can monitor and report changes to the integrity of programs (CR 7.a).</p> <p>The malicious update is identified through signature detection or analysis (CR 7.b, CR 7.c).</p> <p>The malicious service is halted and reverted or deleted (CR 7.d).</p> <p>Other users are temporarily prevented from accessing this update server (CR 7.e).</p> <p>The port opened by the service is detected (CR 7.f).</p> <p>The port opened by the service is closed (CR 7.g).</p> <p>The intrusion is detected (CR 7.h).</p> <p>The intrusion is contained (CR 7.i).</p>
Actual Results	<p>Tripwire Enterprise (Integrity Monitoring) is used to identify changes in programs on the system as well as any changes made by the attacker.</p> <p>Cisco AMP (Event Detection) is used to detect the malicious update.</p> <p>Cisco Stealthwatch (Event Detection) is used to detect a connection to the machine via an unusual port.</p>

	<p>Cisco AMP (Mitigation and Containment) is used to halt the execution of the file and delete it, thereby closing the vulnerable port.</p> <p>Cisco ISE (Mitigation and Containment) is used to disconnect the affected machines from the network to prevent the spread of the intrusion.</p>
Overall Result	Pass (partial). Cisco AMP does not seem to support network blocking for Unix machines at the time this practice guide was written—it supports only detection (it does support network blocking for Windows use cases, though, so a similar use case on Windows machines would potentially work). Instead, we rely on network protection, a DI Protect capability, to prevent further access to the update server; and on Cisco AMP's mitigation capabilities to remedy any known malicious files downloaded from the server.

NIST SPECIAL PUBLICATION 1800-26C

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.

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

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	Contents	
71	1 Introduction	1
72	1.1 Practice Guide Structure	1
73	1.2 Build Overview	2
74	1.3 Typographical Conventions.....	3
75	2 Product Installation Guides	3
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	2.7.1.1	Install the IIS web server	120
103	2.7.1.2	Install Microsoft SQL 2014 Enterprise	122
104	2.7.1.3	Install Microsoft Visual C++ 2015	122
105	2.7.2	Install the Glasswall FileTrust Server Component	124
106	2.7.2.1	Install Glasswall Hub	124
107	2.7.2.2	Install Glasswall Integration Service	128
108	2.7.2.3	Install Glasswall Administrator Console	131
109	2.7.2.4	Add the Server's Certificate.....	133
110	2.7.2.5	Install the Smtp Analysis Agent	147
111	2.7.2.6	Distribute the Glasswall License File	149
112	2.7.3	Configure Glasswall FileTrust.....	151
113	2.7.3.1	Create a New Administrator Account.....	152
114	2.7.3.2	Configure Notifications and Policies	157
115	2.7.3.3	Configure Inbound SMTP Policy	158
116	2.7.3.4	Create a Receiver Group	159
117	2.7.3.5	Create a ThreatCensor Policy Set	161
118	2.7.3.6	Create a Processing Rule	162
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	2.8.5.1	Install Activate Base	221
127	2.8.5.2	Install Packages	223
128	2.8.6	Apply Filters to a Channel.....	224
129	2.8.7	Configure Email Alerts in ArcSight	225
130	2.8.7.1	Configure a New Destination	225
131	2.8.7.2	Configure a New Rule.....	226
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	2.9.5.1	Terminology	244
139	2.9.5.2	Tags.....	245
140	2.9.5.3	Rules	247
141	2.9.5.4	Tasks	251
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	2.12 Cisco Advanced Malware Protection	280
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	2.13 Cisco Stealthwatch	286
166	2.13.1 Configure Stealthwatch Flow Collector, Stealthwatch Management Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor	286
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
172	2.14 Symantec Analytics.....	301
173	2.14.1 Initial Setup.....	301
174	2.14.2 Capturing Data	307
175	2.15 Symantec Information Centric Analytics.....	308
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	2.15.4.1	Installing Integration Packs	331
181	2.15.4.2	Create a View.....	332
182	2.15.4.3	Open an Existing View	333
183	2.15.4.4	Viewing Detailed Analyzer Data	335
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	Appendix A List of Acronyms	440

1 Introduction

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

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

1.1 Practice Guide Structure

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

This guide contains three volumes:

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

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

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

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

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

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

You might share the *Executive Summary*, *NIST SP 1800-26a*, with your leadership team members to help 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-nccoe@nist.gov.
261

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> .
Bold	names of menus, options, command buttons and fields	Choose File > Edit .
Monospace	command-line input, on- screen computer output, sample code examples, sta- tus codes	<code>mkdir</code>
Monospace Bold	command-line user input contrasted with computer output	service sshd start
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov

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**

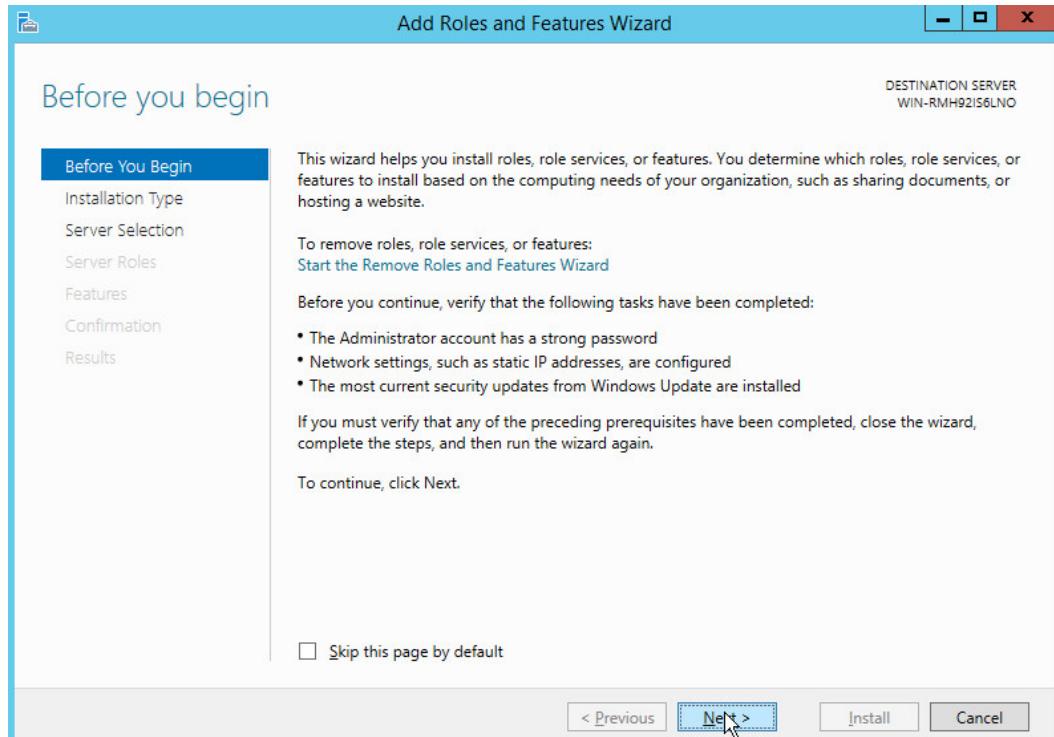
278 As part of our enterprise emulation, we included an Active Directory server that doubles as a Domain
279 Name System (DNS) server. This section covers the installation and configuration process used to set up
280 Active Directory and DNS on a Windows Server 2012 R2 machine.

281 **2.1.1 Install Features**

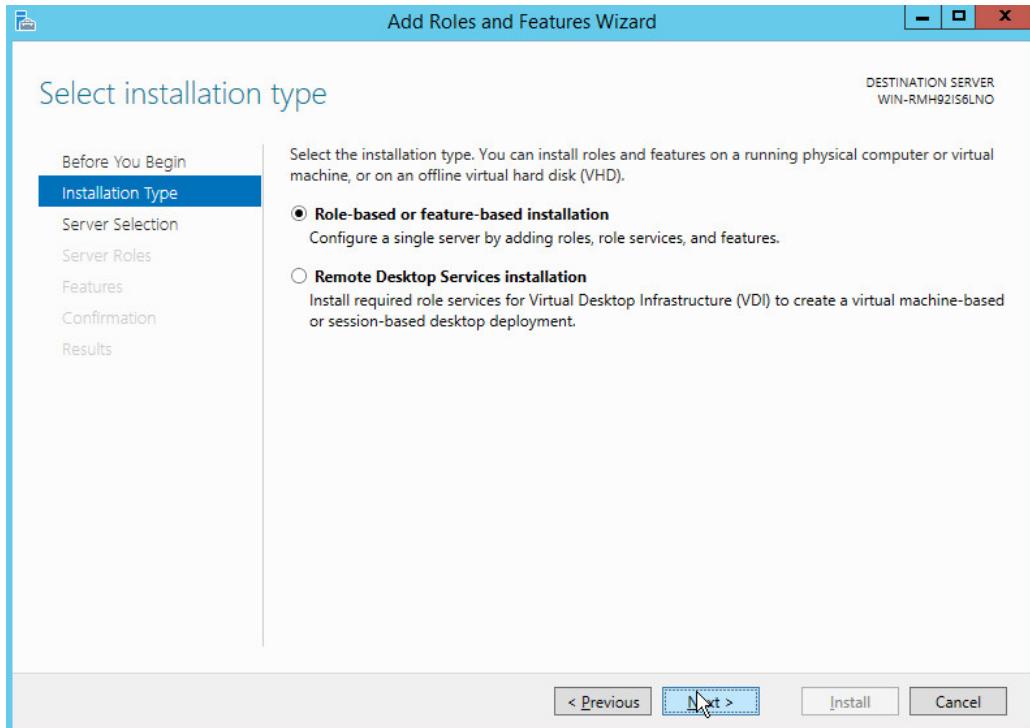
282 1. Open **Server Manager**.

283
284

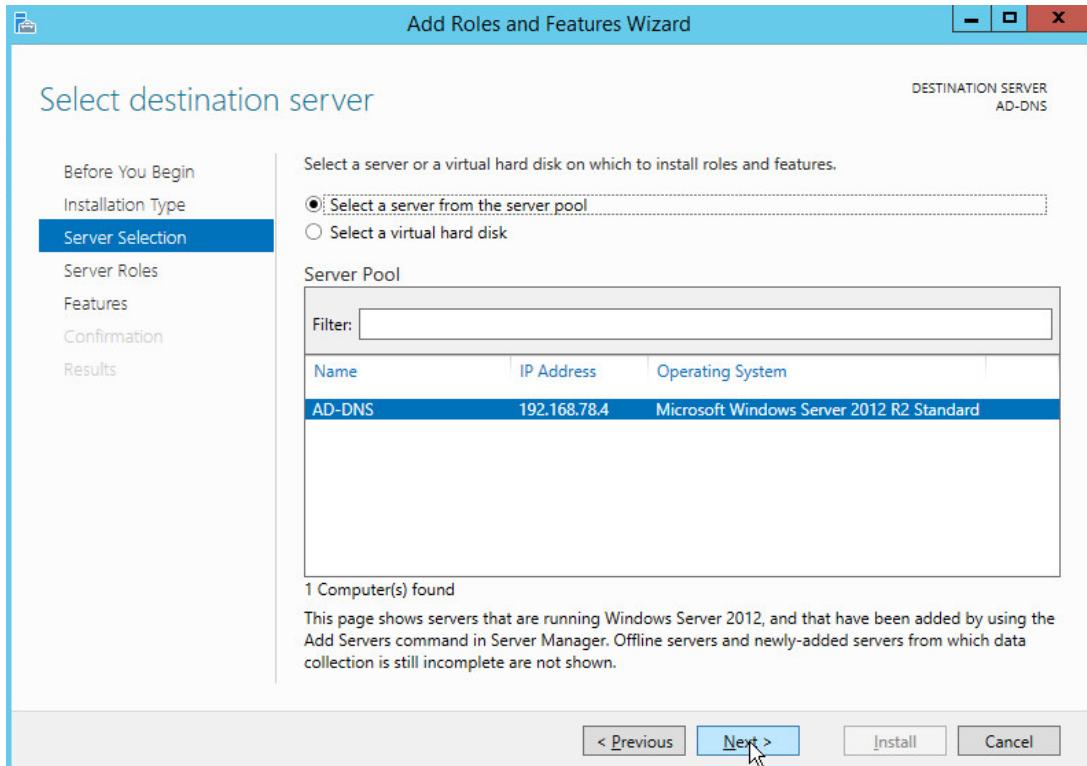
2. Click the link **Add roles and features**.

285
286
287

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

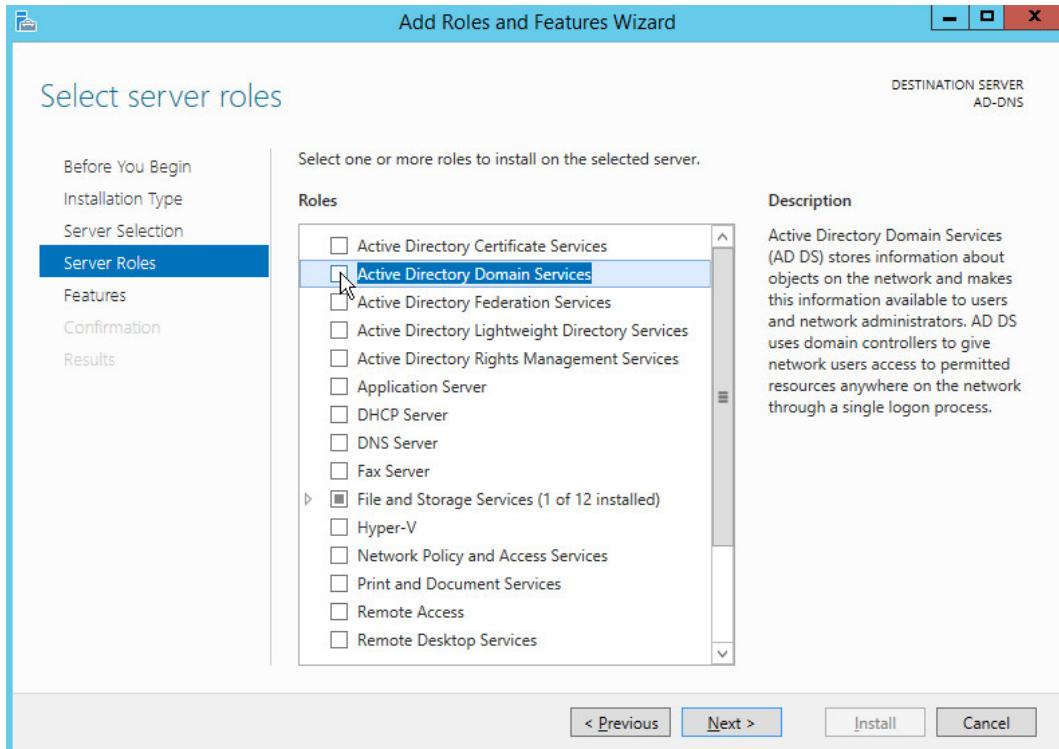


- 288
289 5. Click **Next**.
290 6. Select **Select a server from the server pool**.
291 7. Select the intended active directory server.



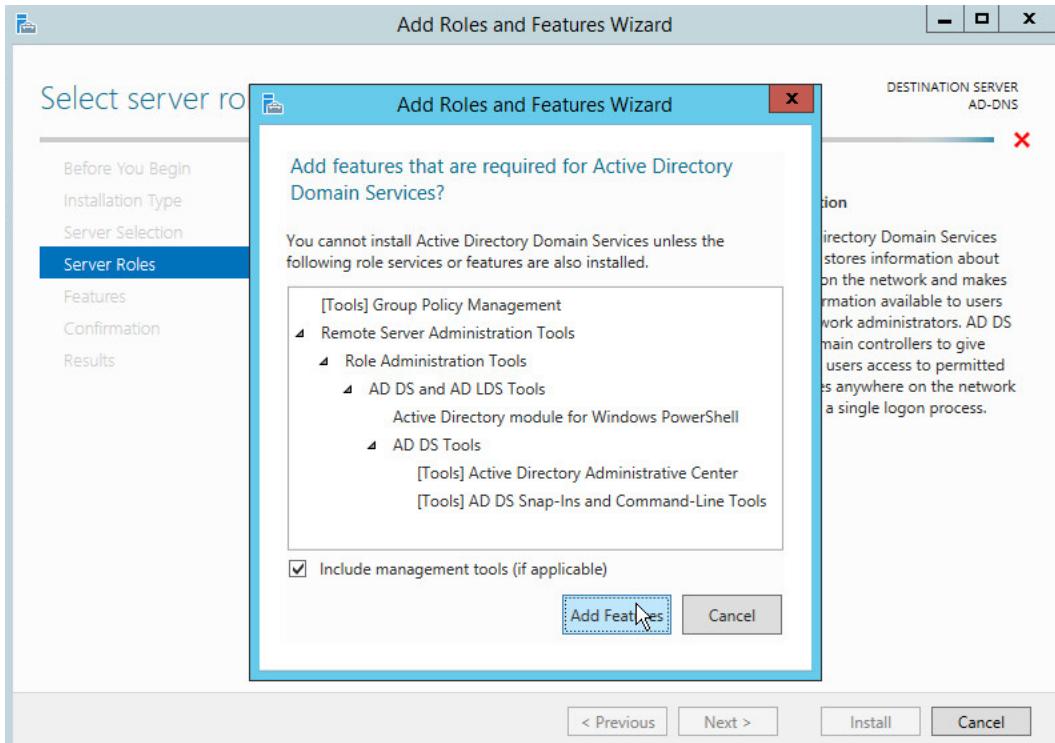
292
293

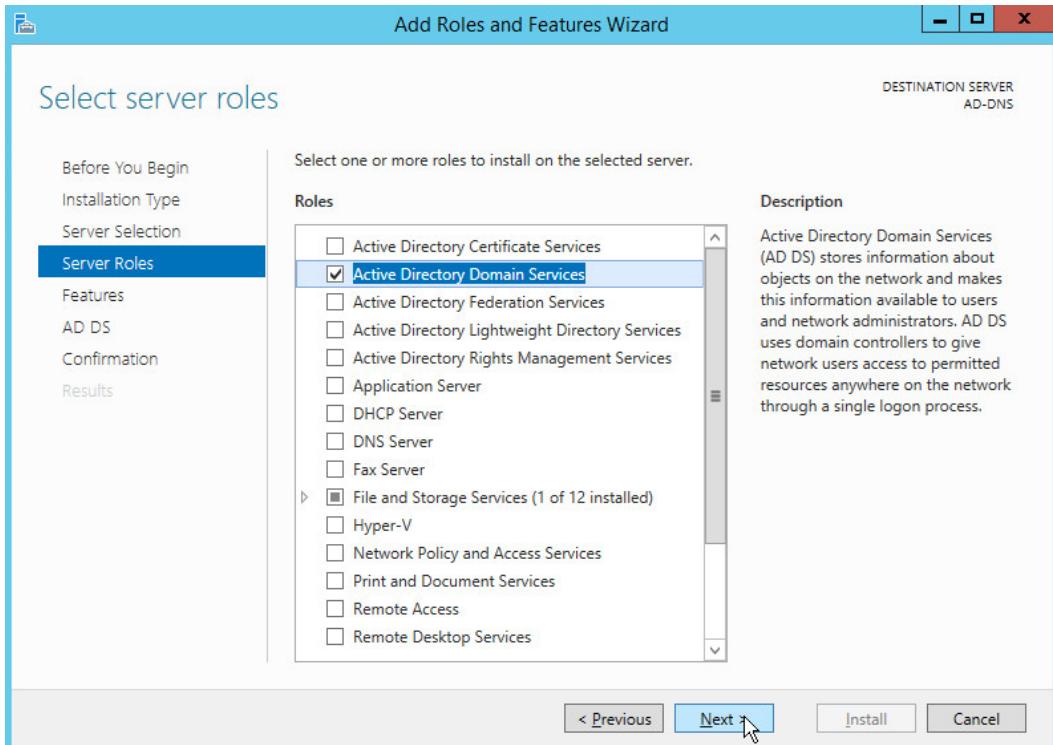
8. Click **Next**.



294
295

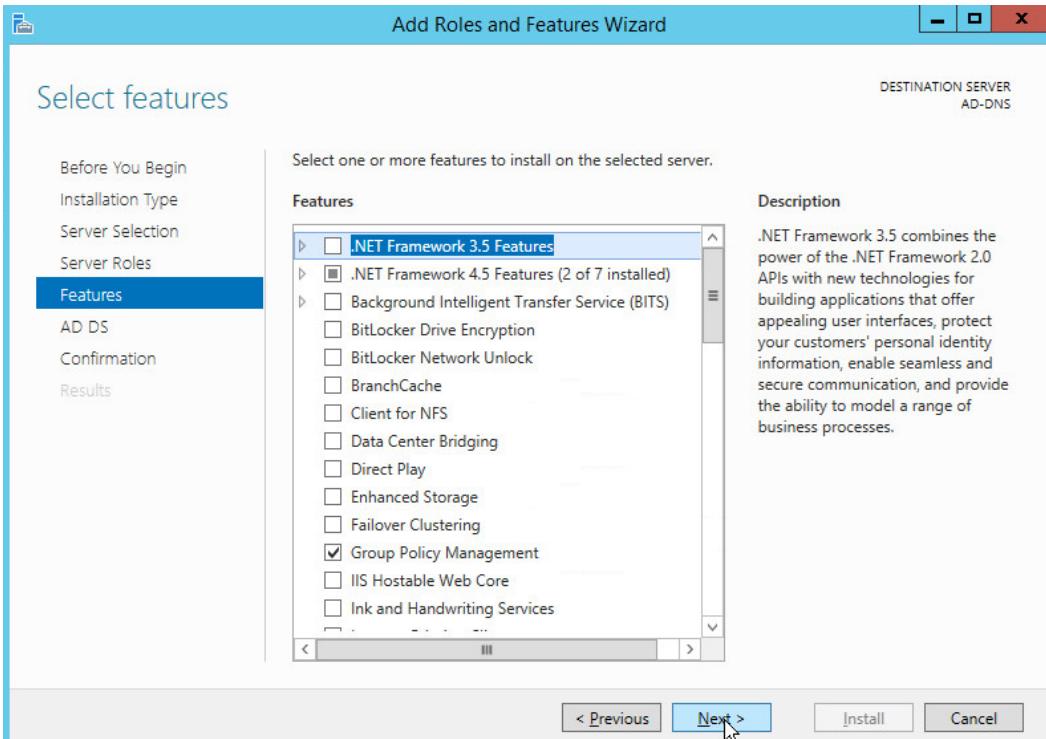
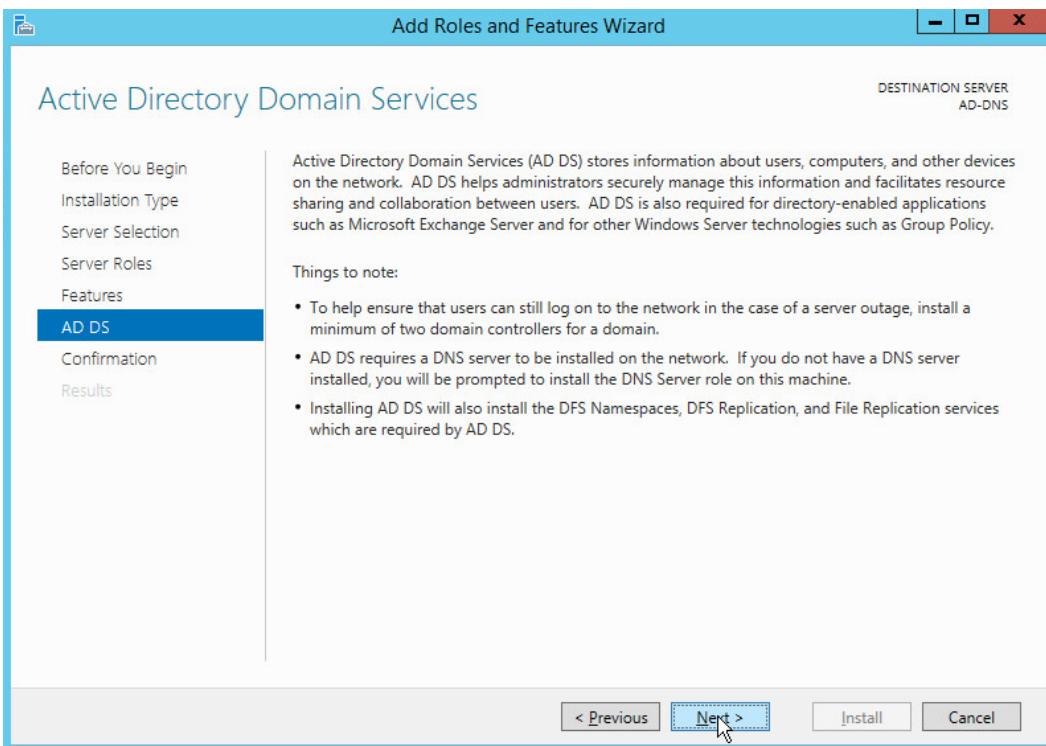
9. Check the box next to **Active Directory Domain Services**.

296
297**10. Click Add Features.**



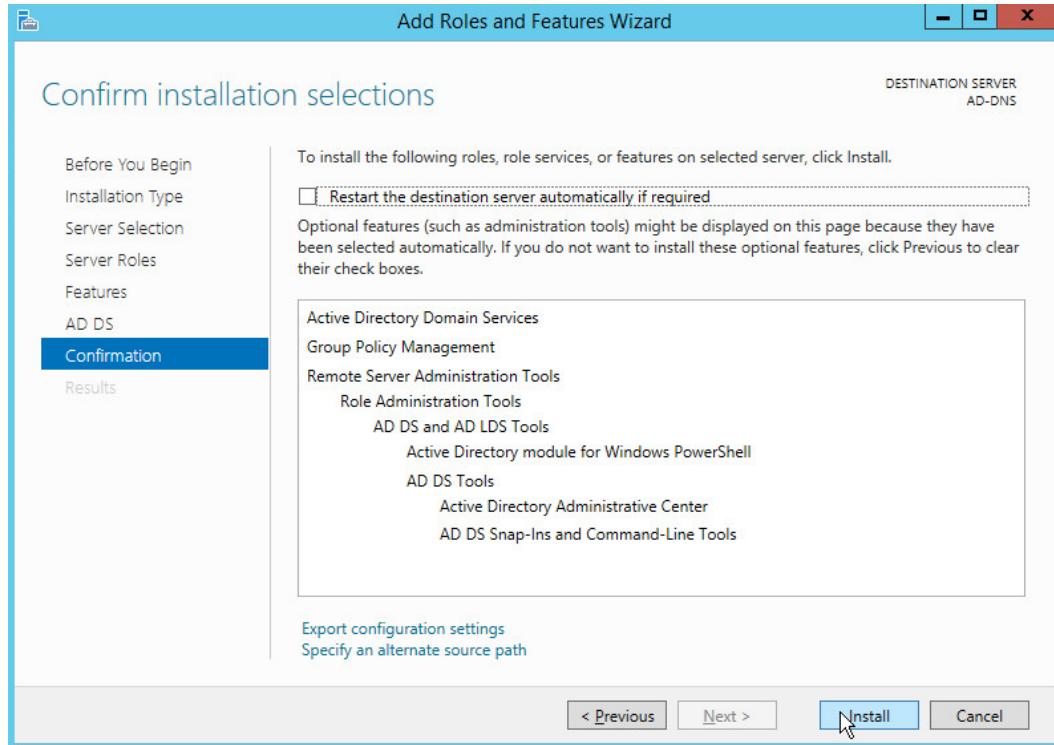
298
299

11. Click **Next**.

300
30112. Click **Next**.

302

303

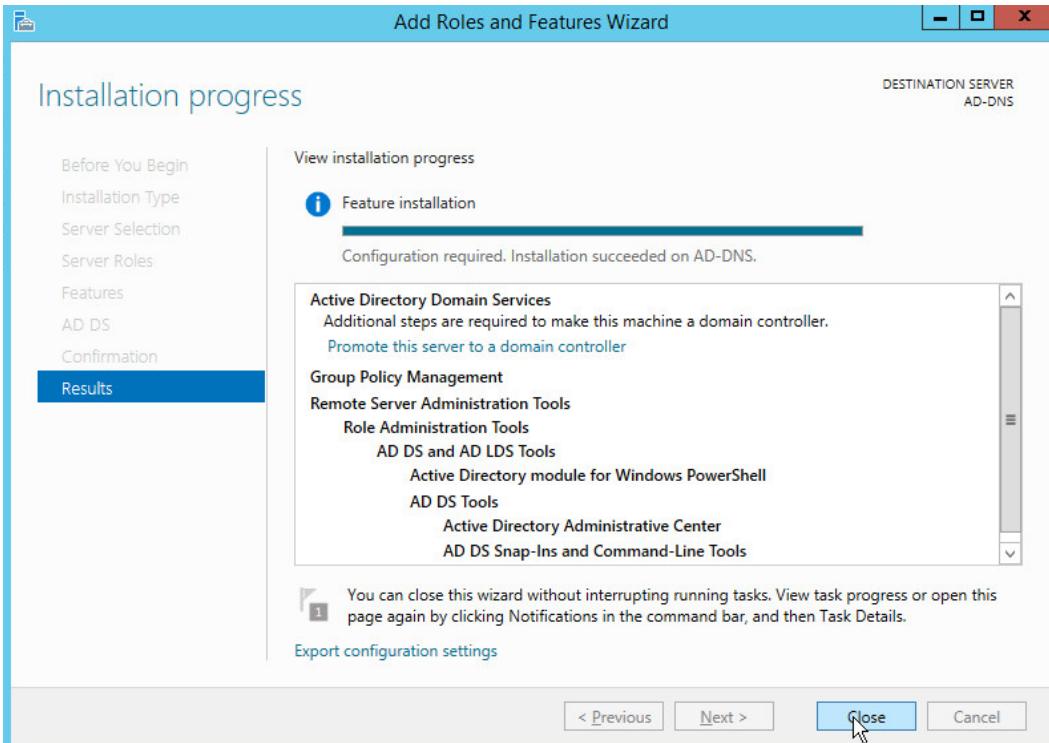
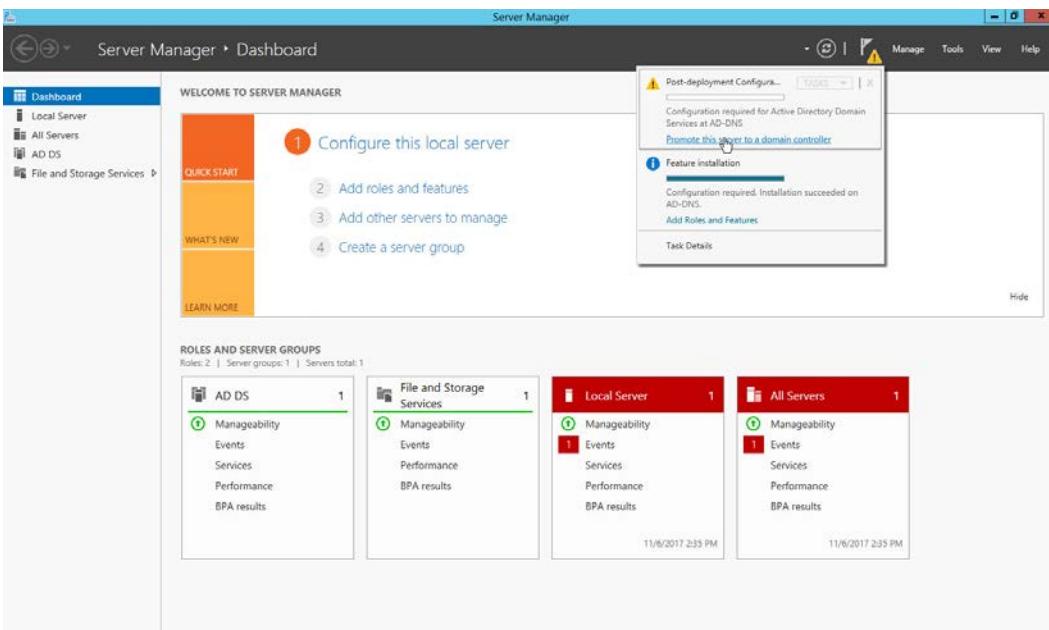
13. Click Next.

304

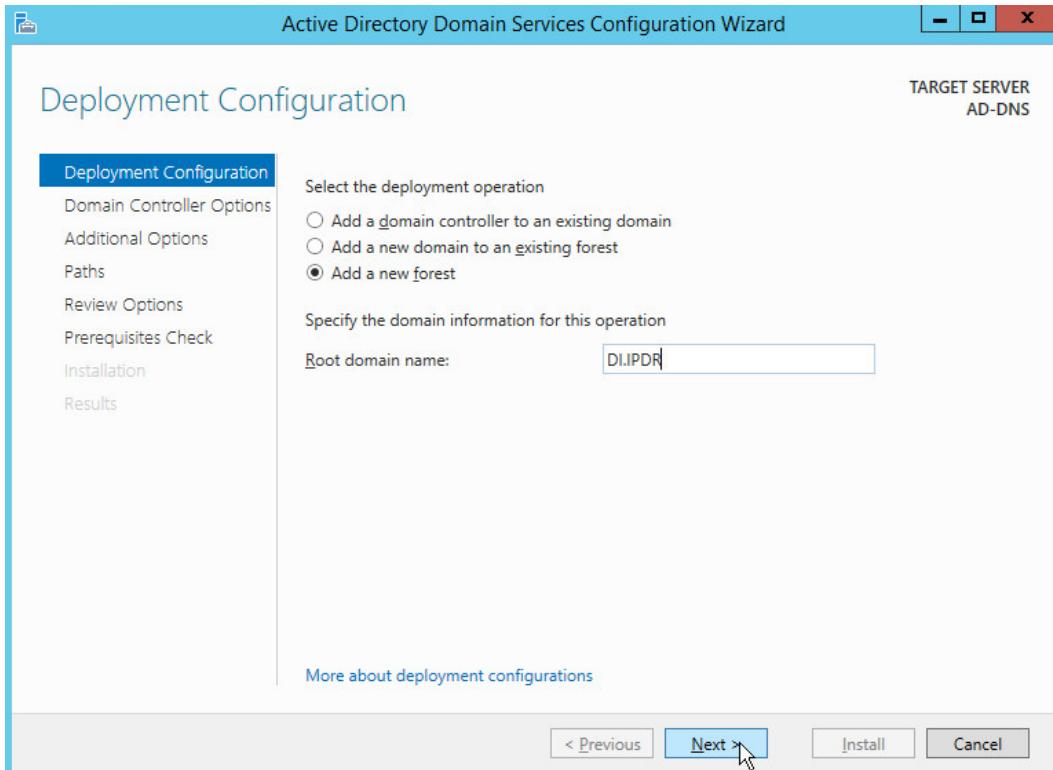
305

306

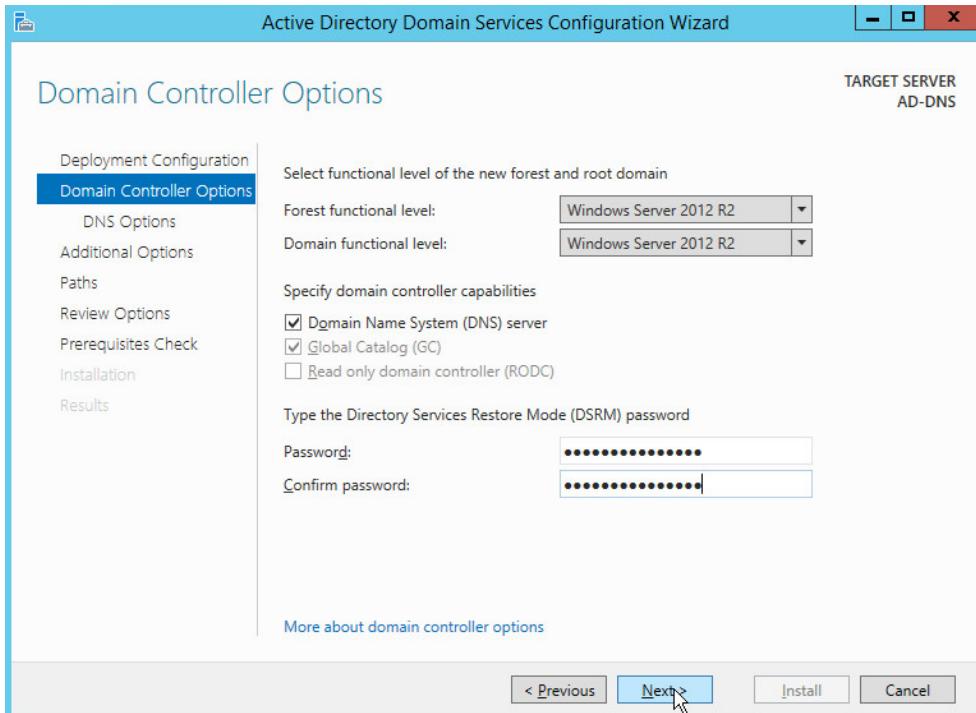
14. Click Install.**15. Wait for the installation to complete.**

307
30816. 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**.



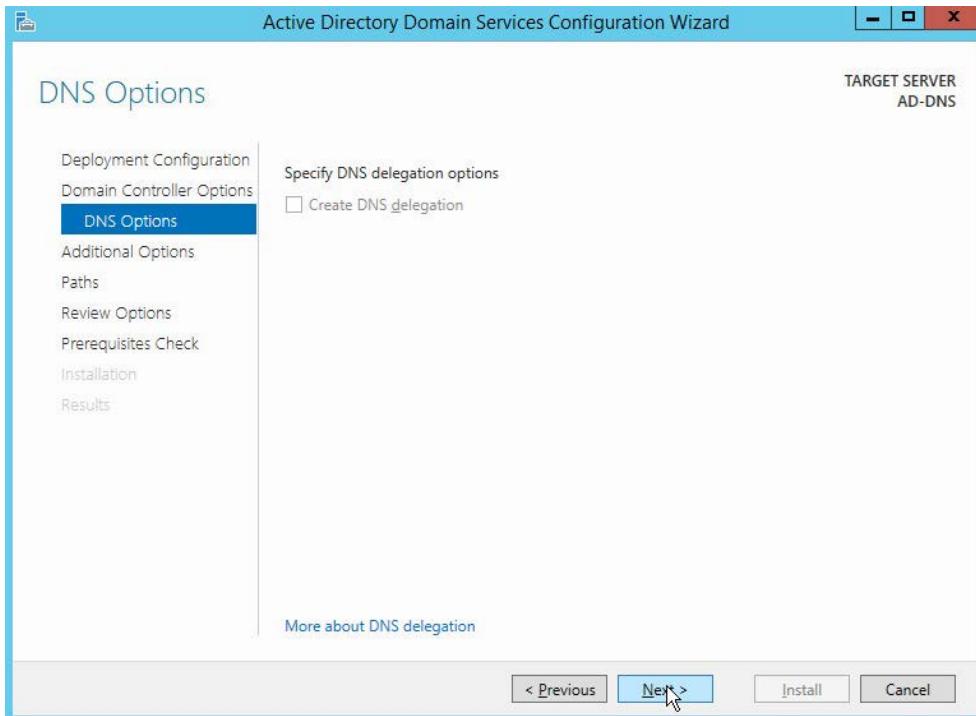
- 313
314 20. Click **Next**.
315 21. Select **Windows Server 2012 R2** for **Forest functional level** and **Domain functional level**.
316 22. Check the box next to **Domain Name System (DNS) server**.
317 23. Enter a password.



318

319

24. Click Next.



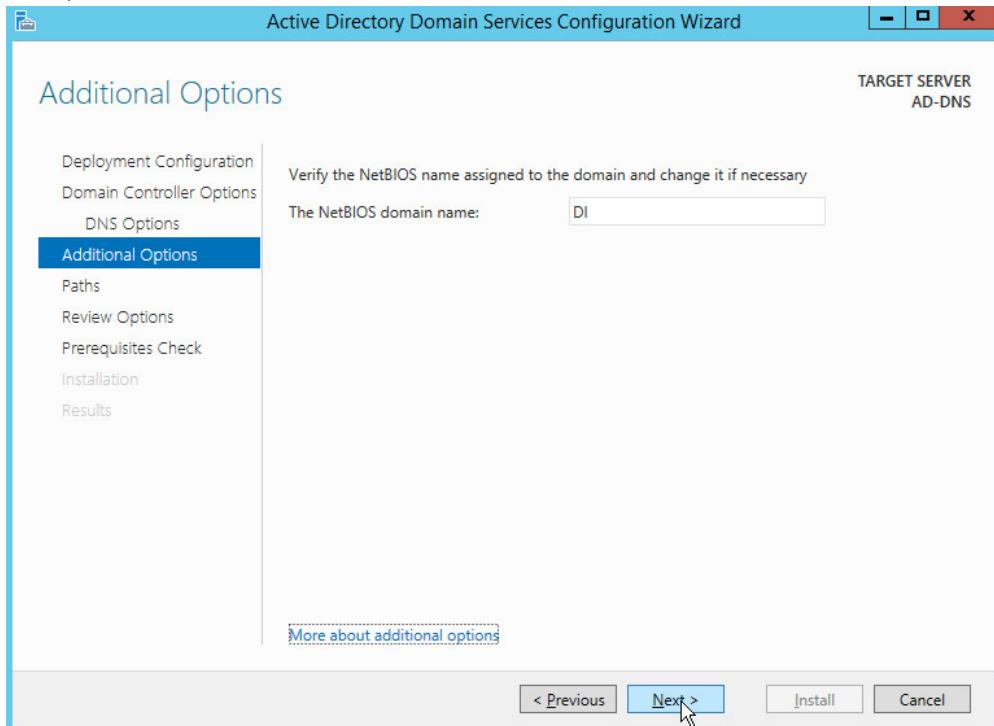
320

321

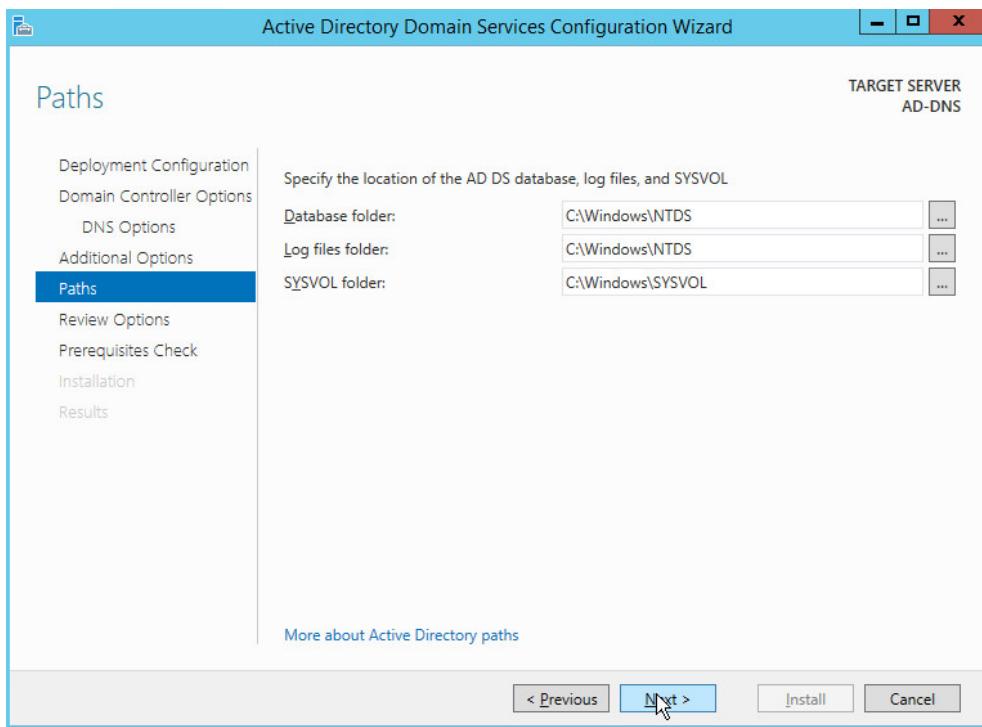
25. Click Next.

322

26. Verify the domain name.

323
324

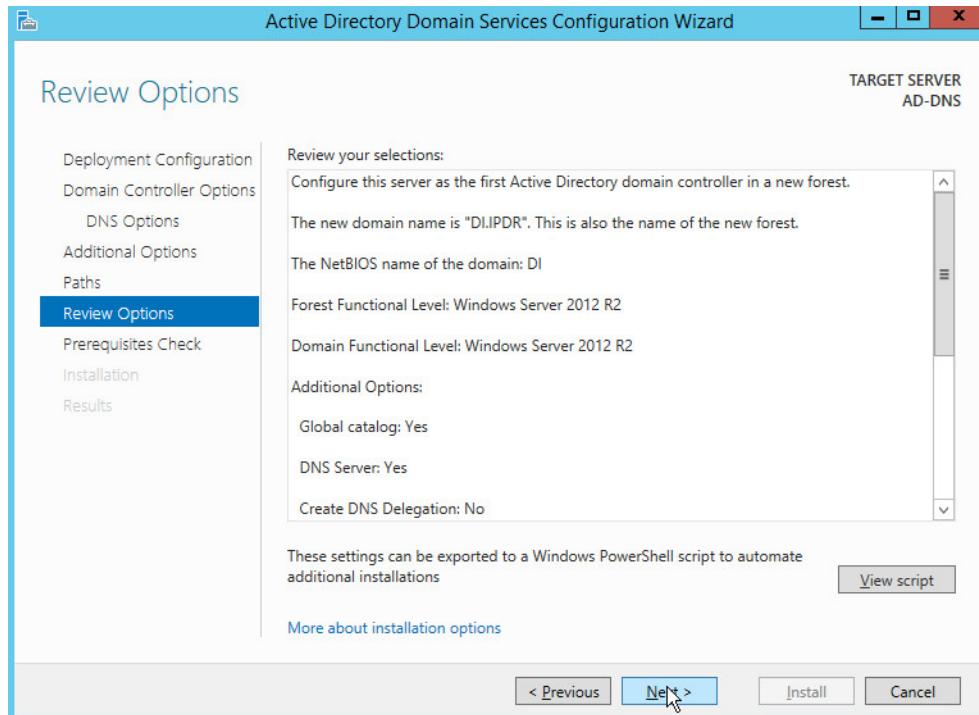
27. Click Next.



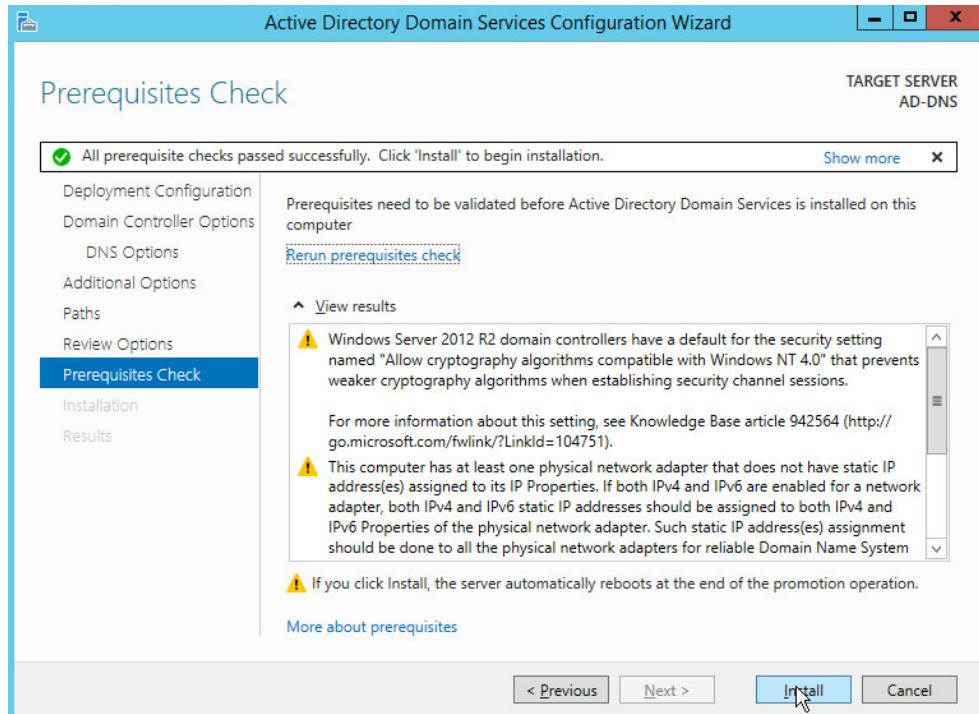
325

326

28. Click Next.

327
328

29. Click Next.

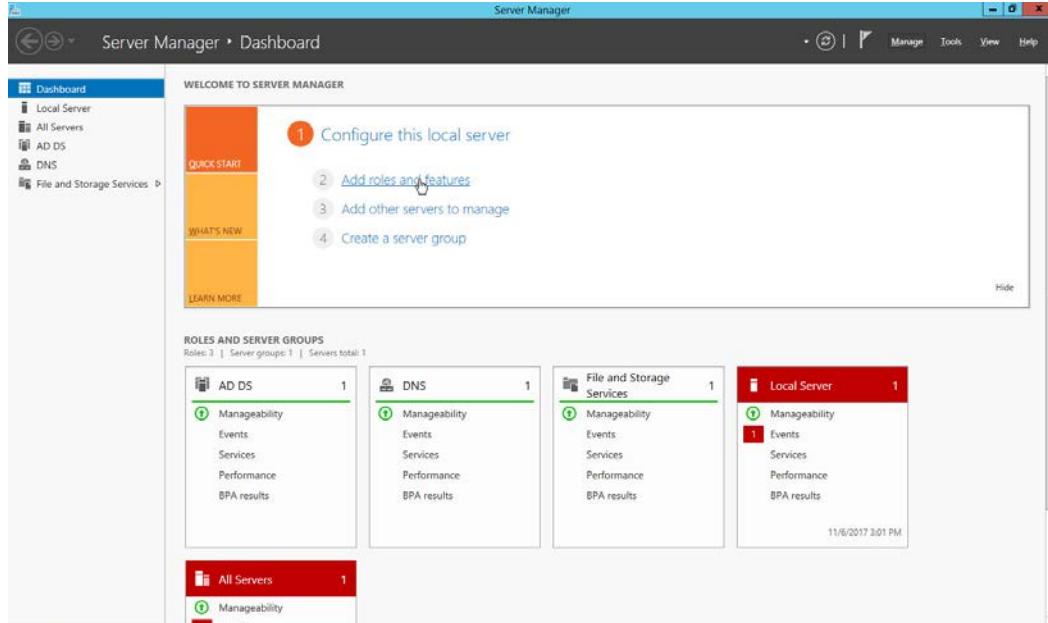


329

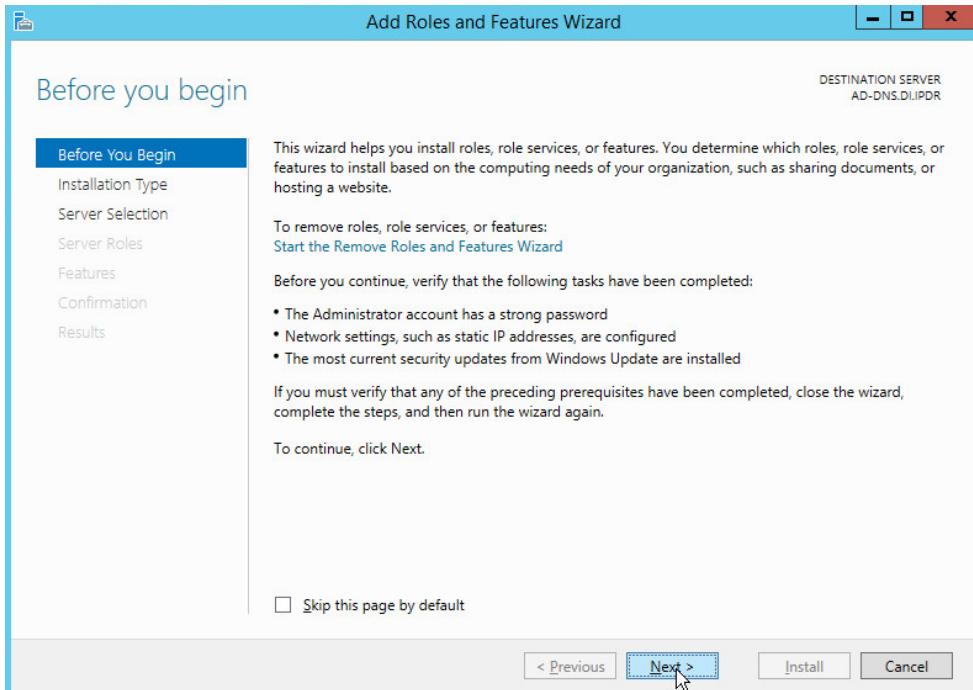
- 330 30. Click **Install**.
331 31. Wait for the installation to complete.
332 32. The server automatically reboots.

333 2.1.2 Create a Certificate Authority

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



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

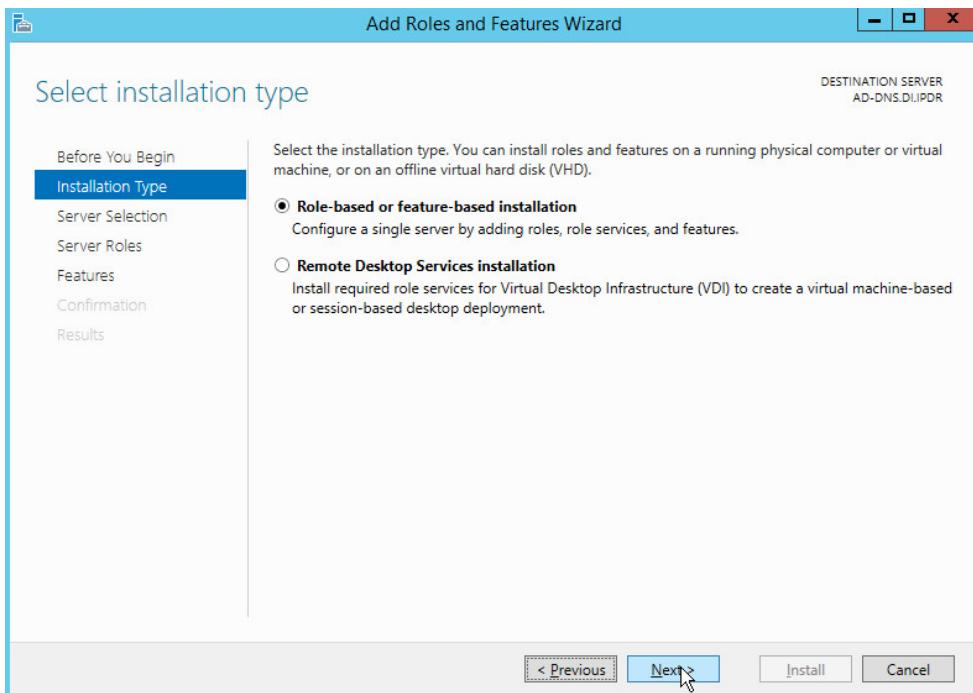


337

338

339

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

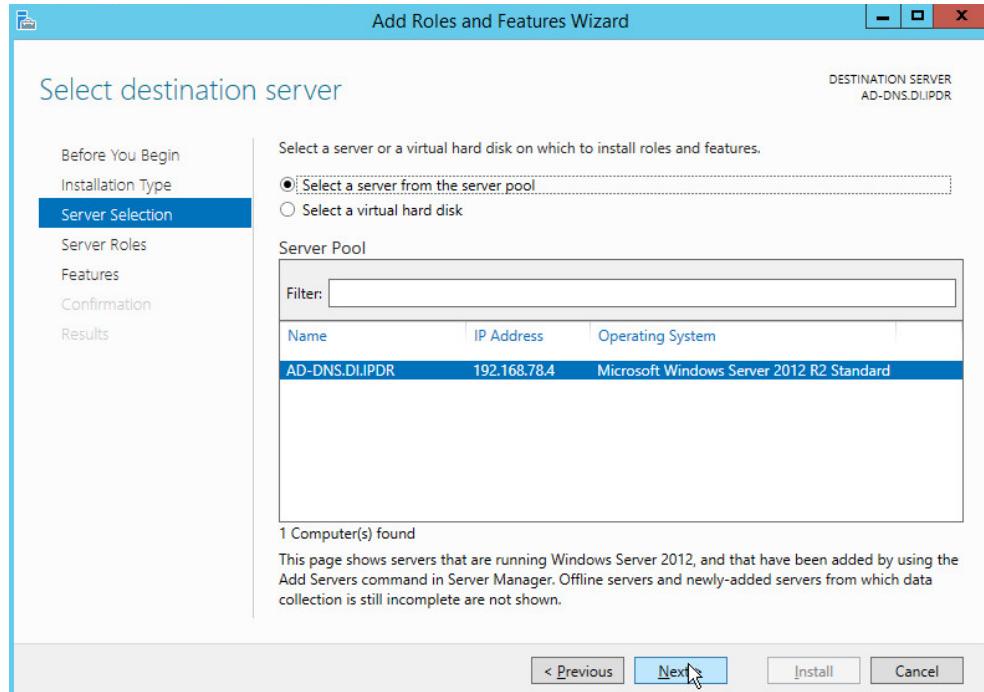


340

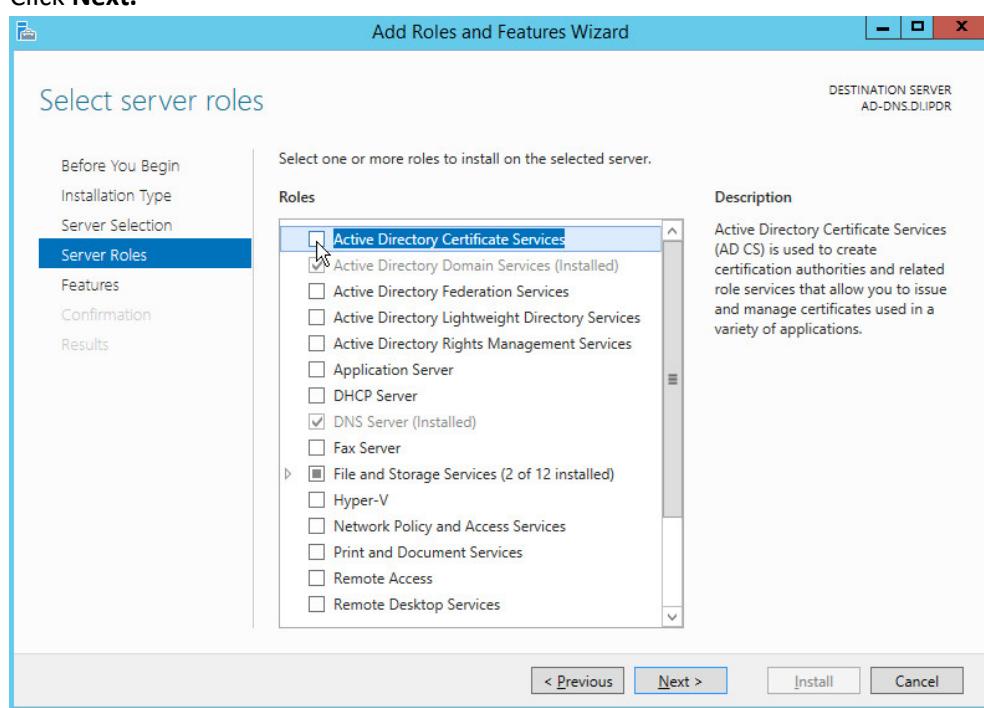
341

5. Click **Next**.

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



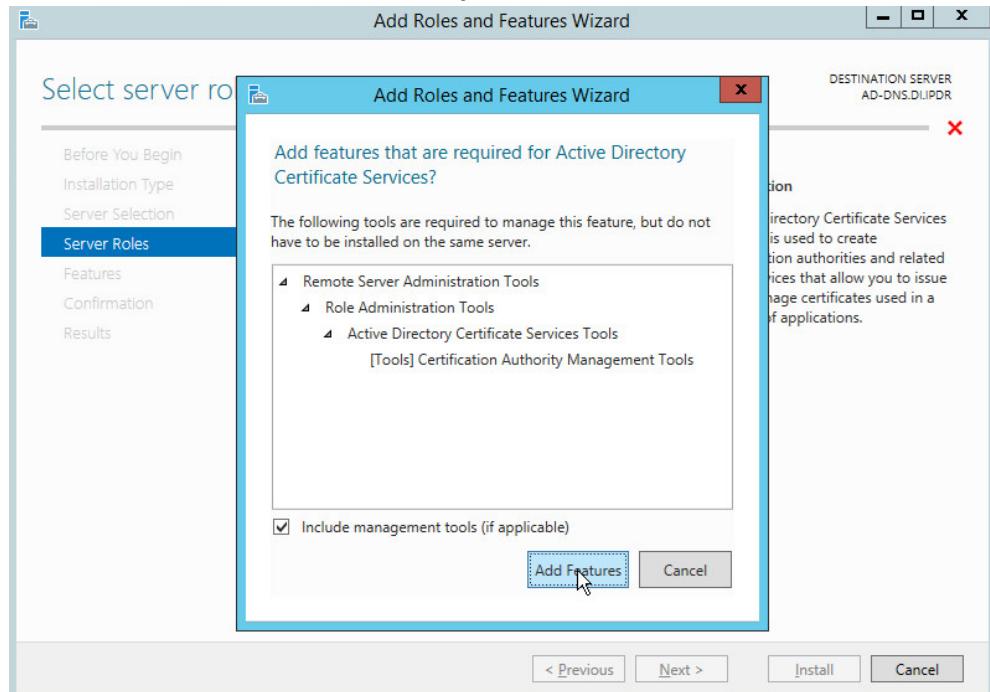
- 344
 345 8. Click **Next**.



346

347

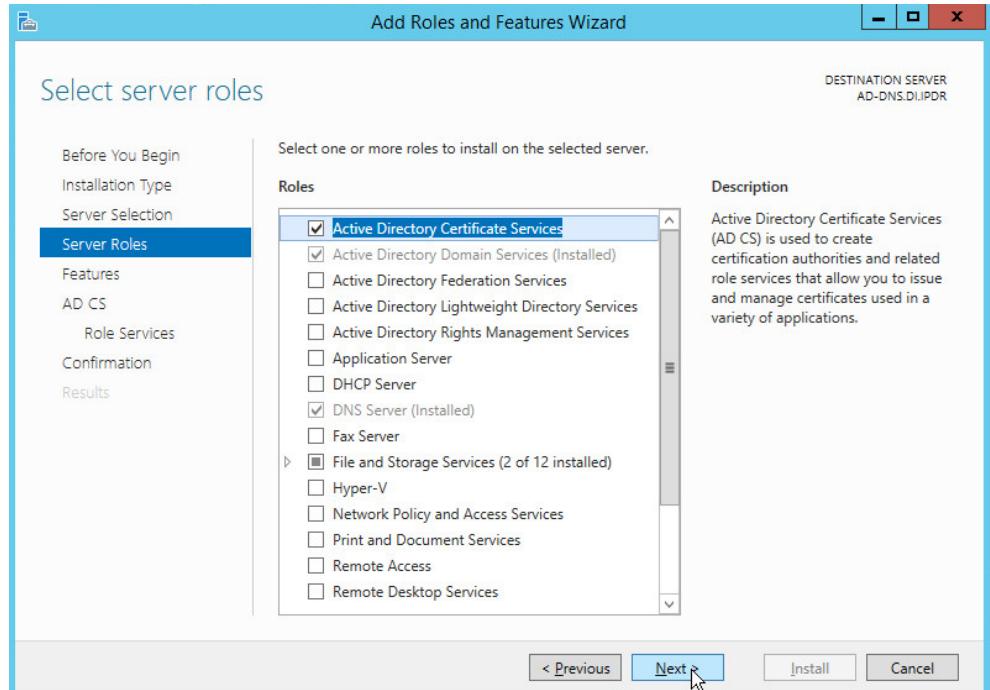
9. Check the box next to **Active Directory Certificate Services**.



348

349

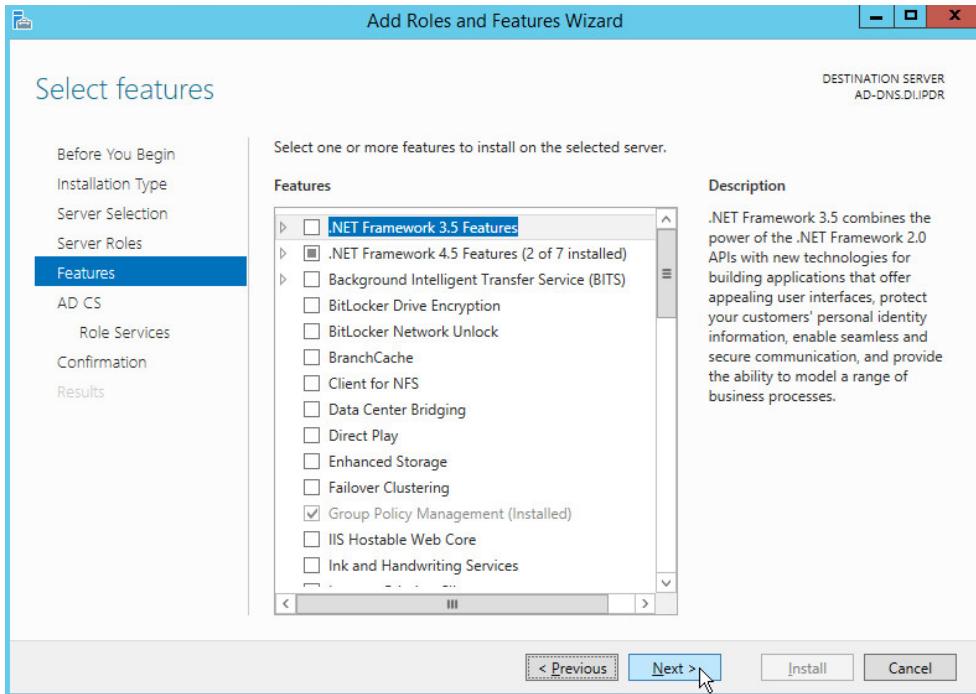
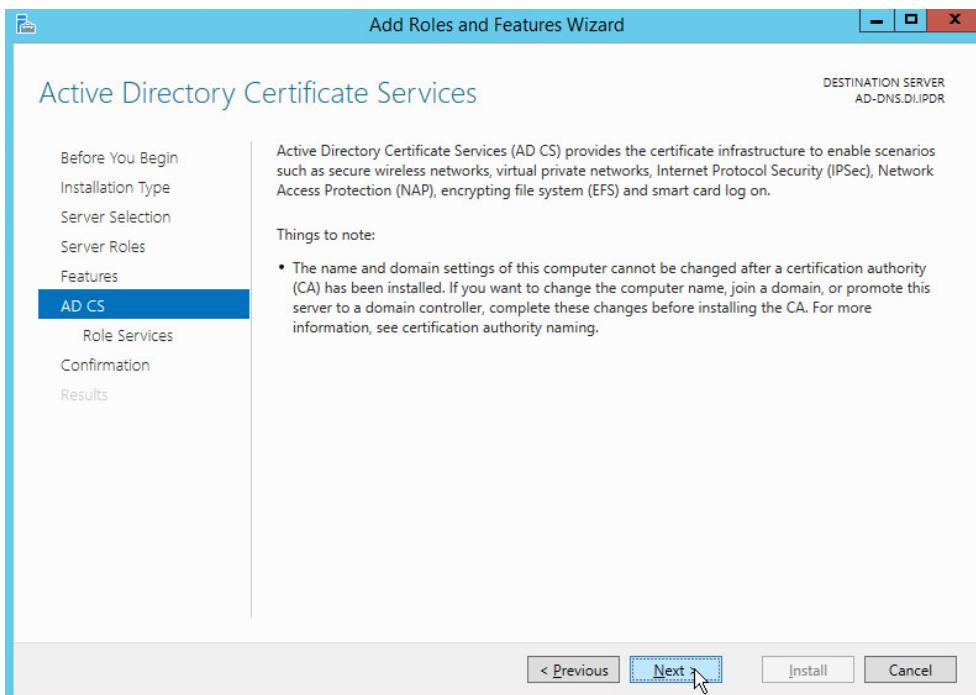
10. Click **Add Features**.

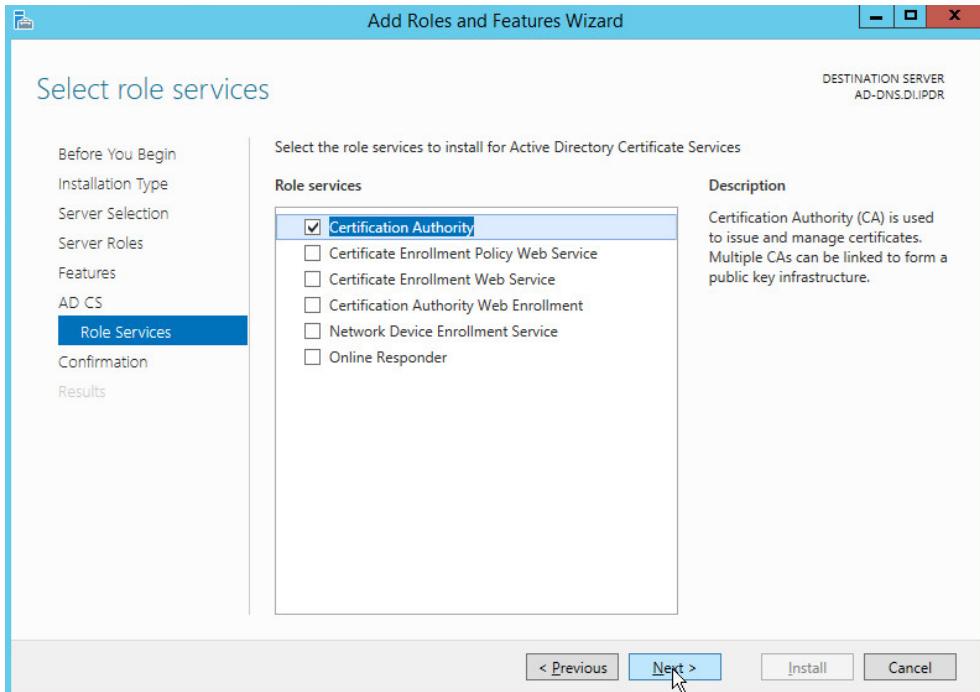
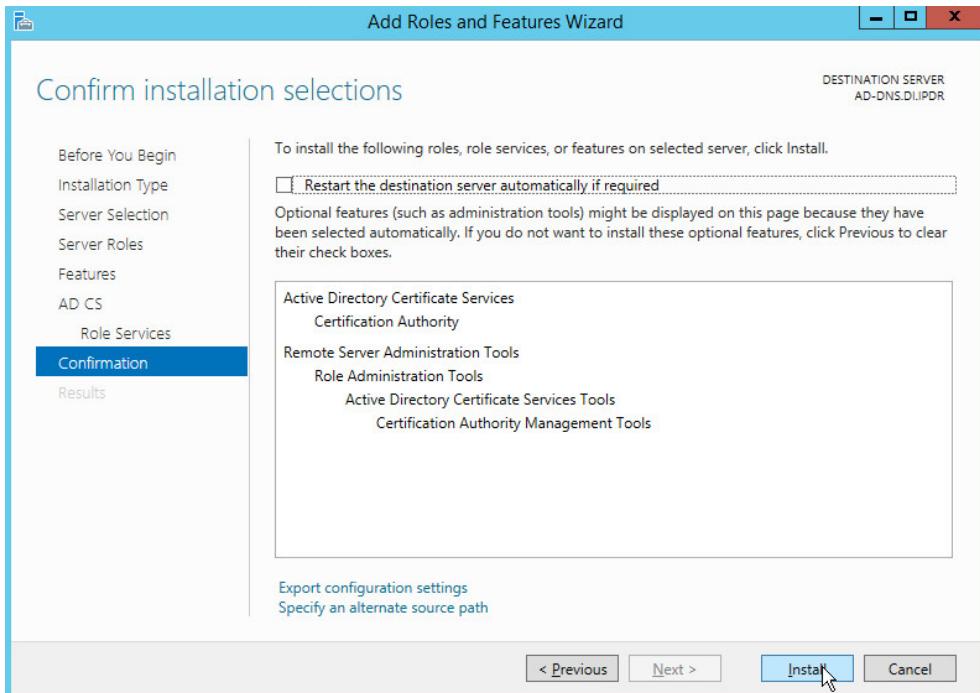


350

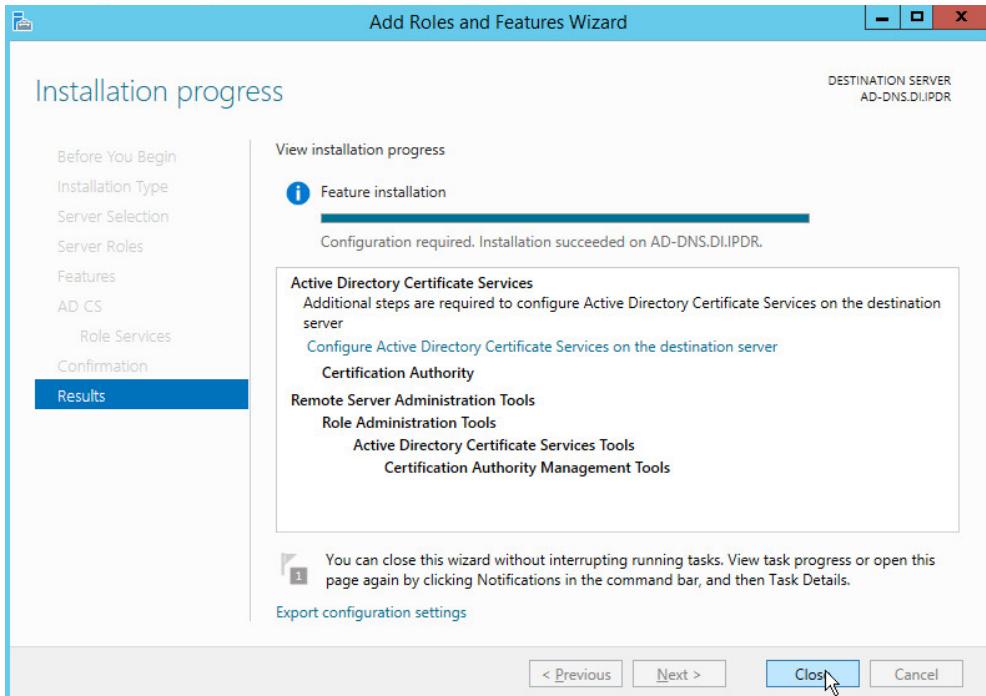
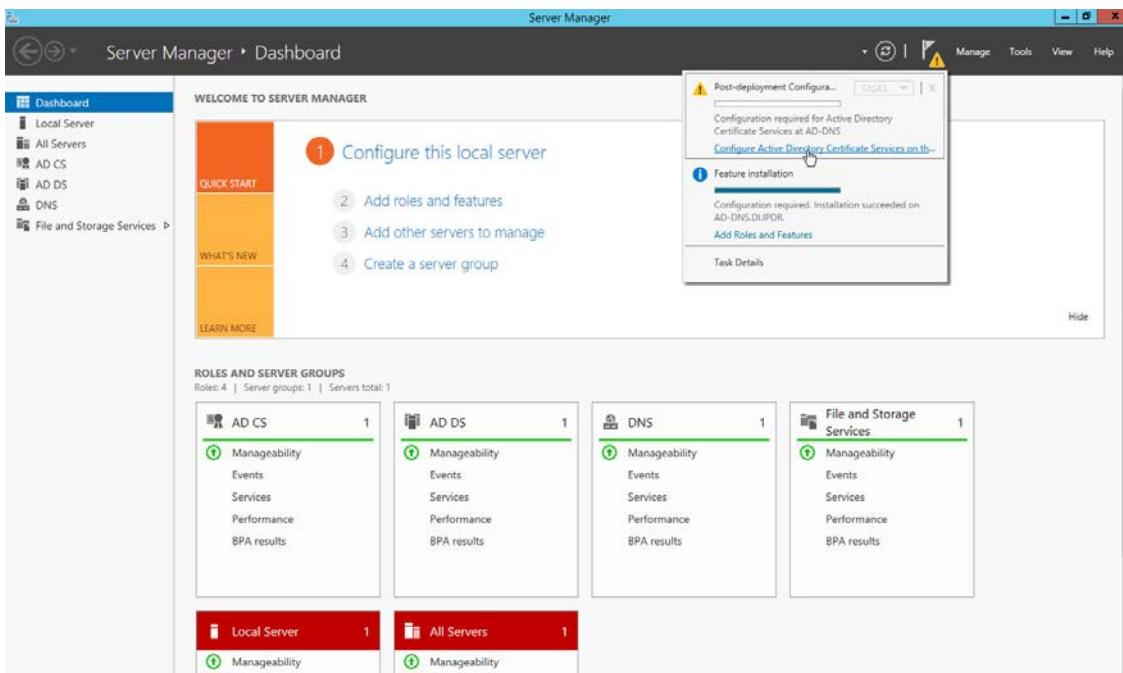
351

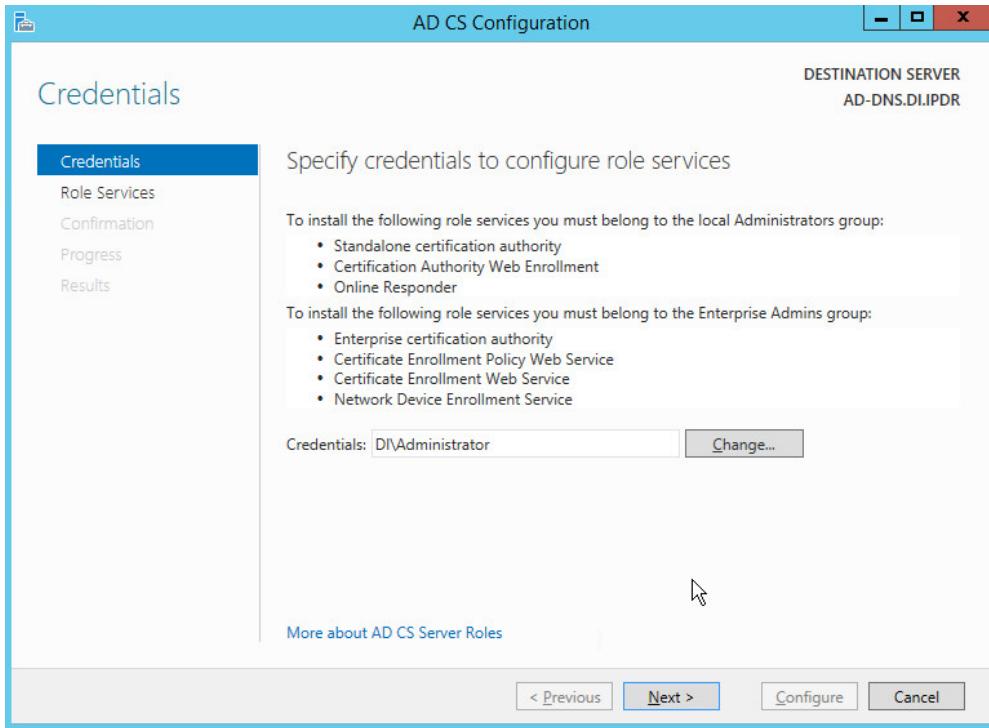
11. Click **Next**.

352
35312. Click **Next**.354
355
35613. Click **Next**.14. Check the box next to **Certification Authority**.

357
35815. Click **Next**.359
360
36116. Click **Install**.

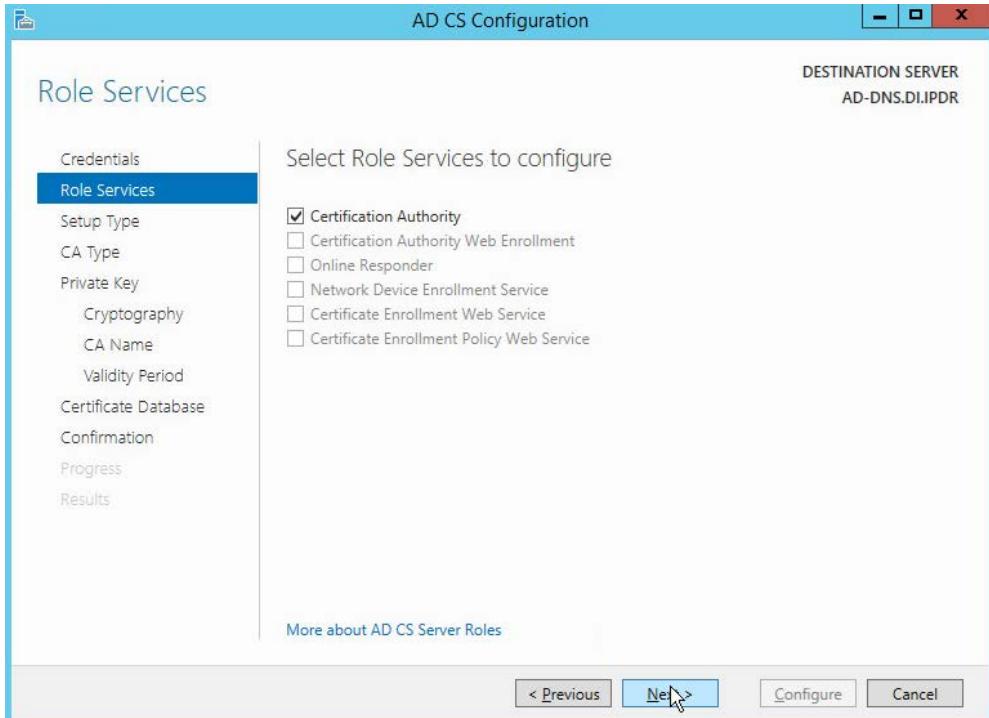
17. Wait for the installation to complete.

362
36318. Click **Close**.364
36519. Click **Configure Active Directory Certificate Serves on the destination server**.

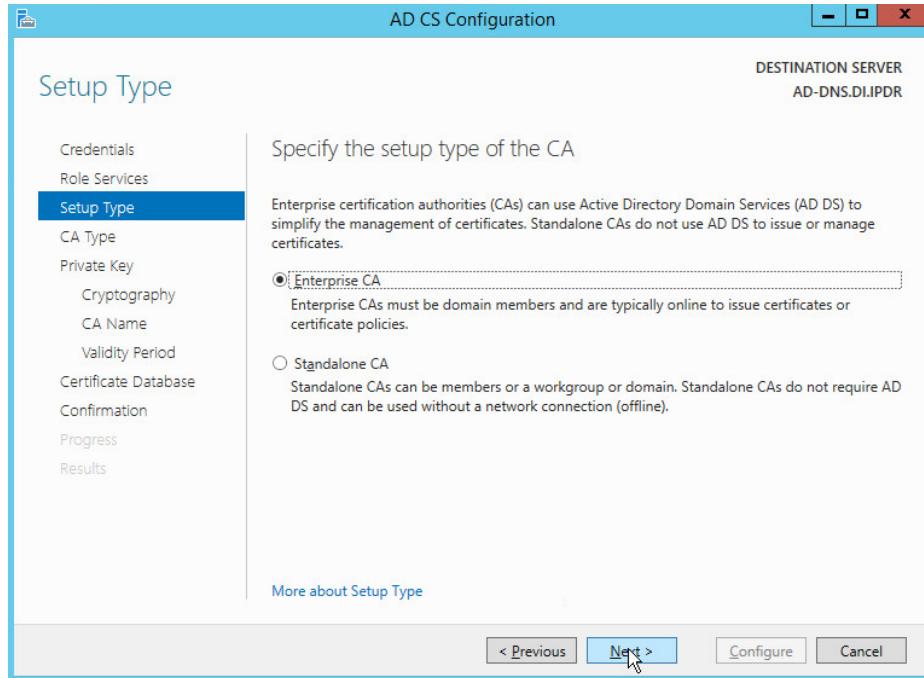
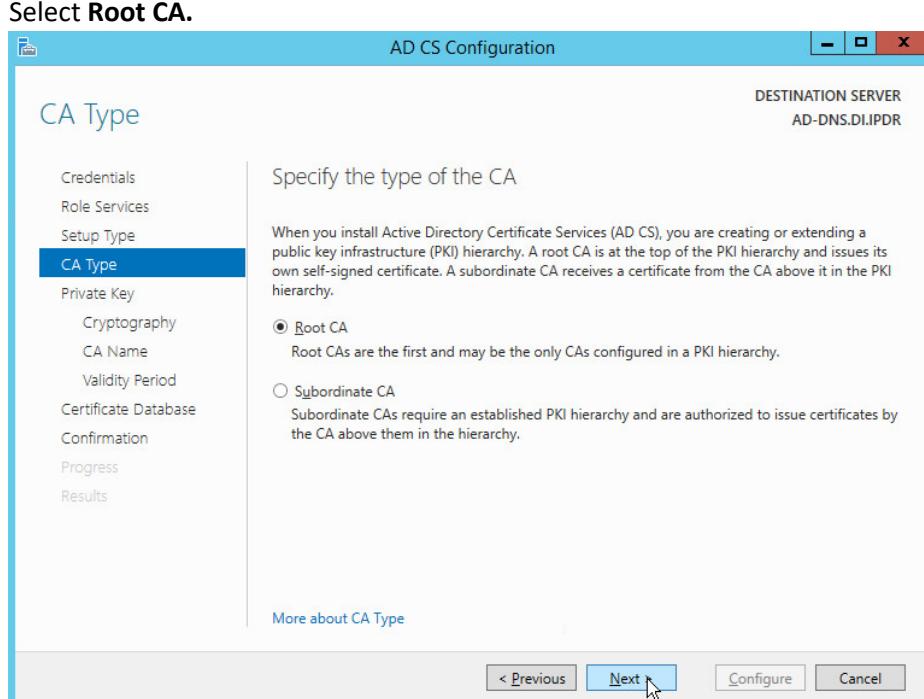


366
367
368

20. Click **Next**.
21. Check the box next to **Certification Authority**.



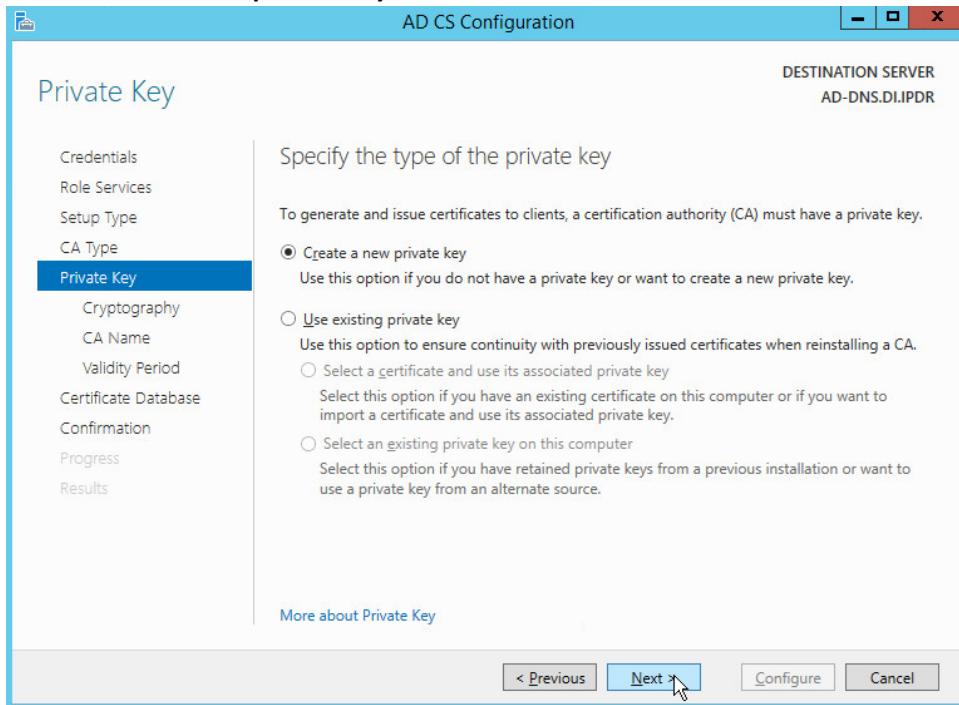
369

370 22. Click **Next**.371 23. Select **Enterprise CA**.372 24. Click **Next**.373 25. Select **Root CA**.

375

376 26. Click **Next**.

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



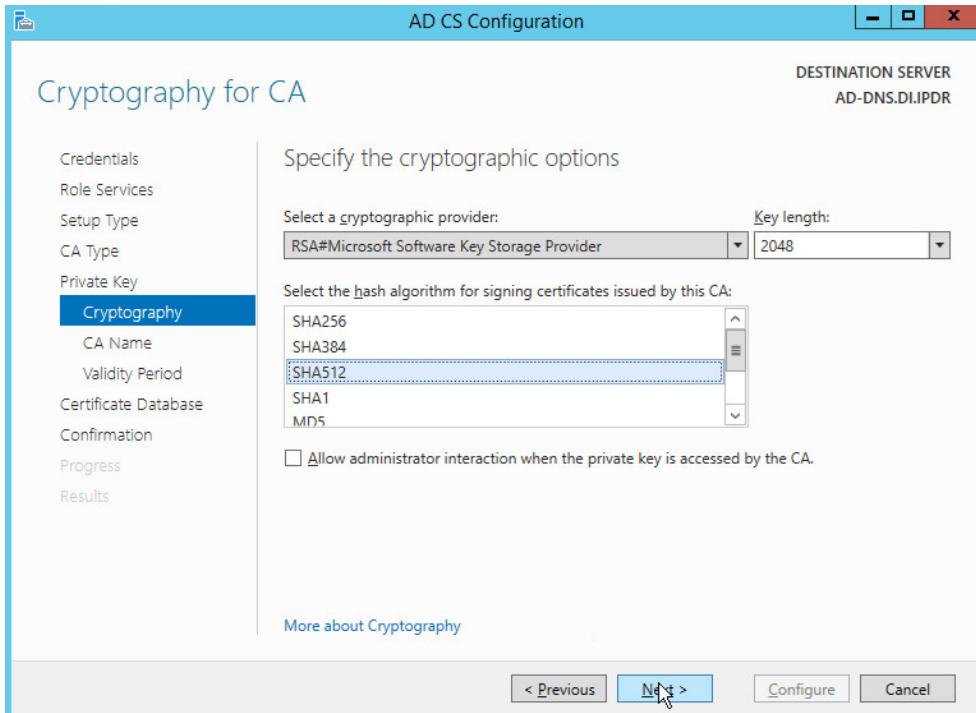
378 28. Click **Next**.

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

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

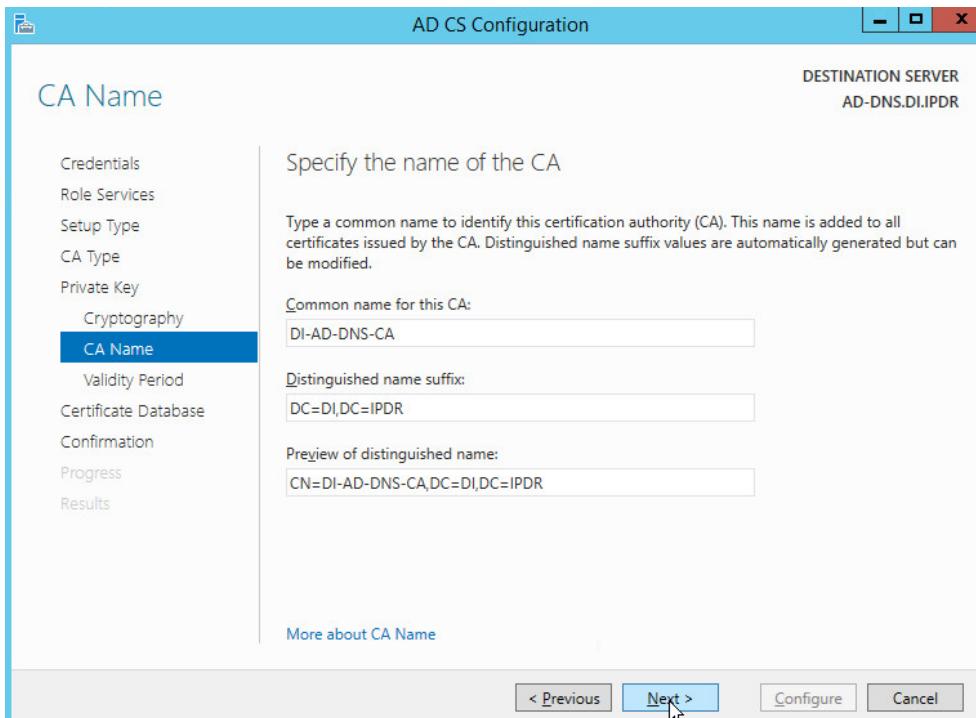
381 31. Select **SHA512** from the list.

382



383

384

32. Click **Next**.

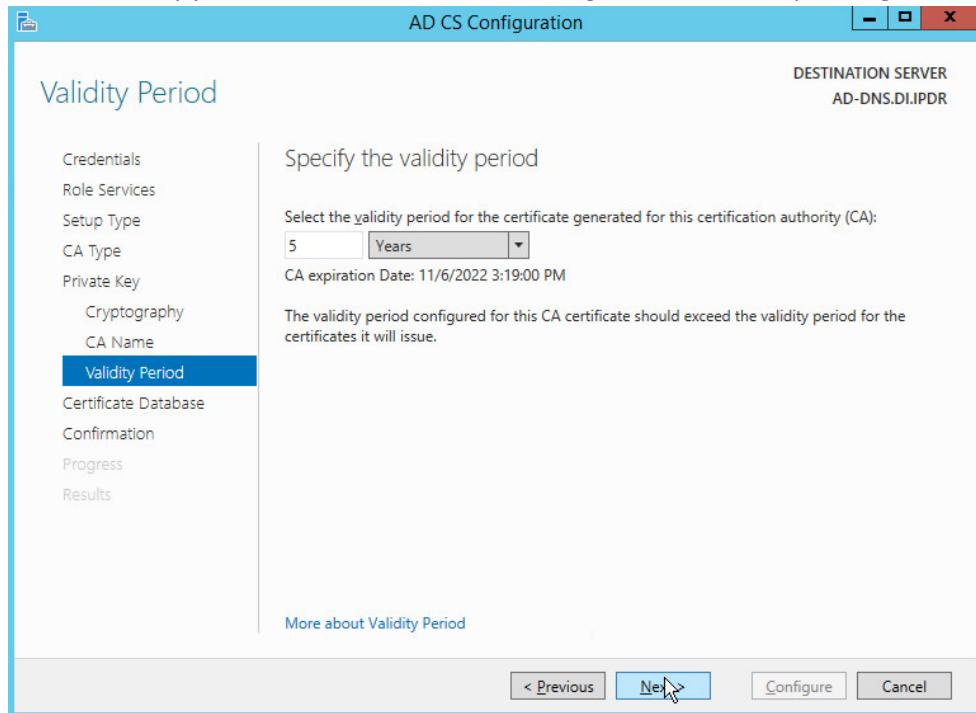
385

386

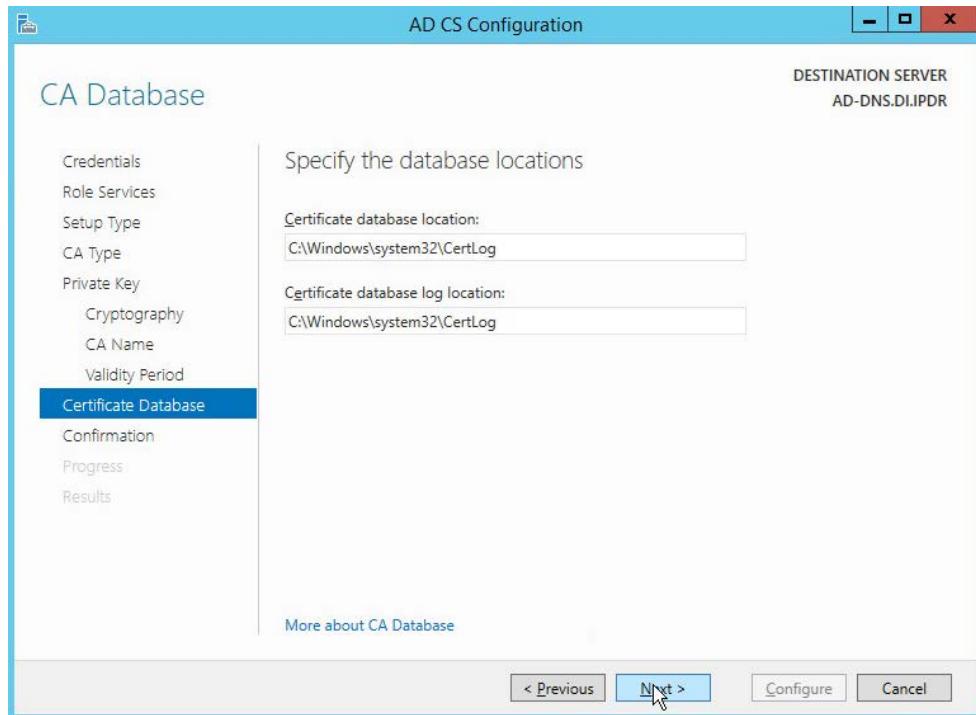
33. Click **Next**.

387

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

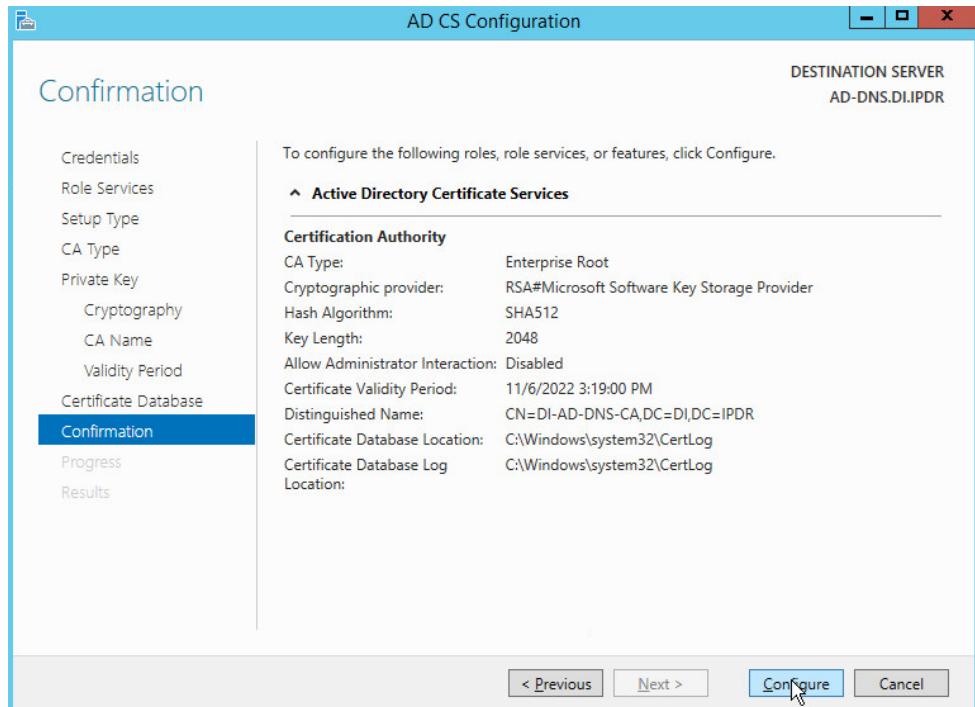
388
389

35. Click Next.



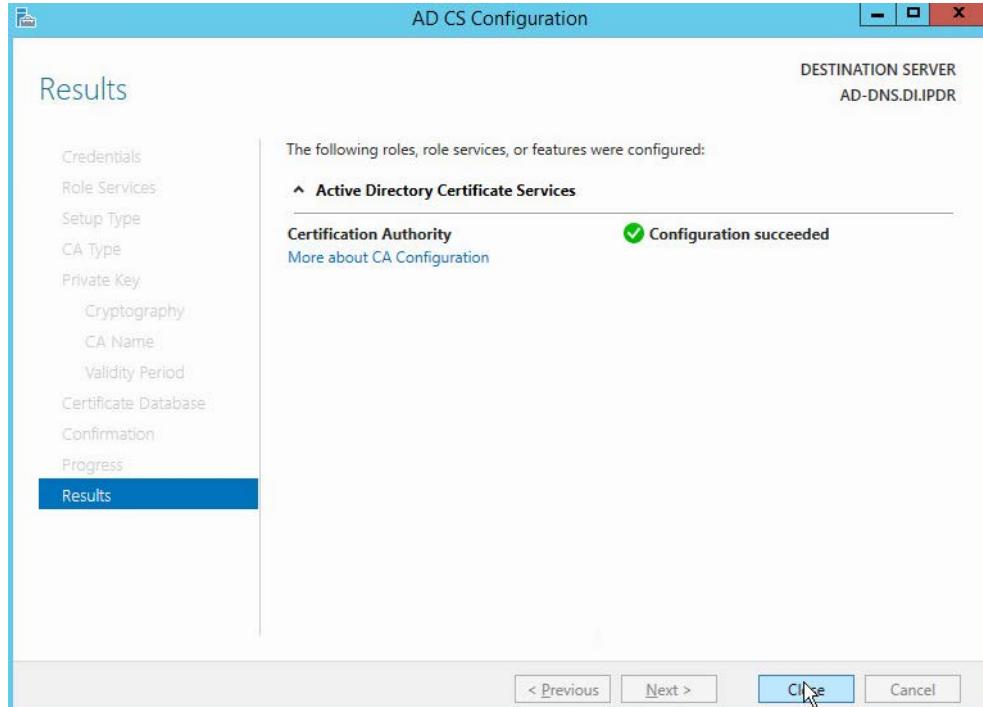
390

391

36. Click **Next**.

392

393

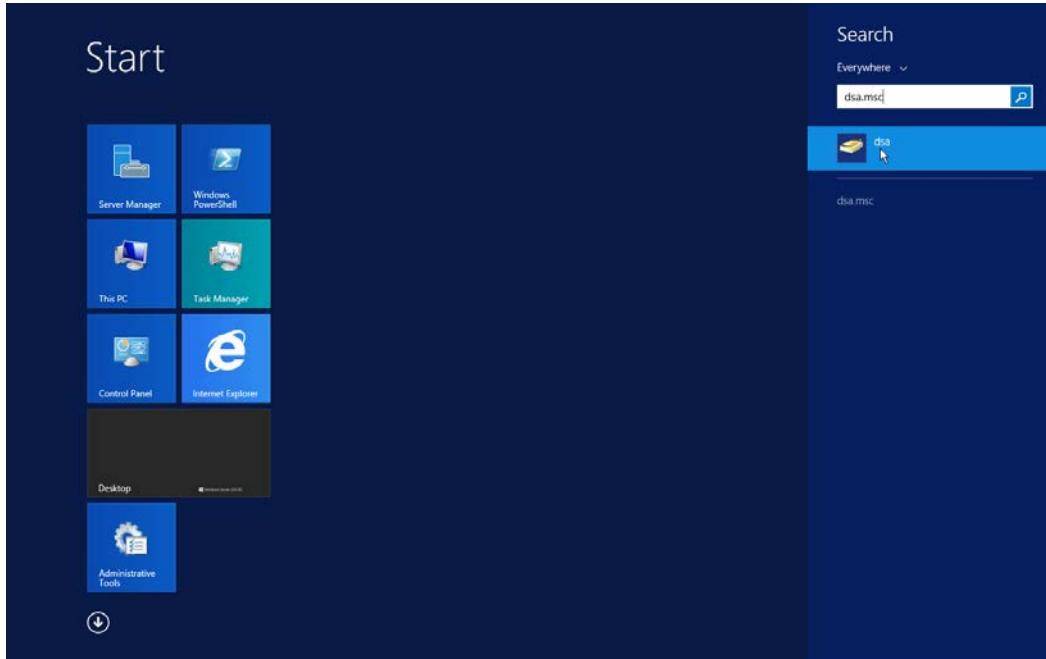
37. Click **Configure**.

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 **dsa.msc**, and run the program.



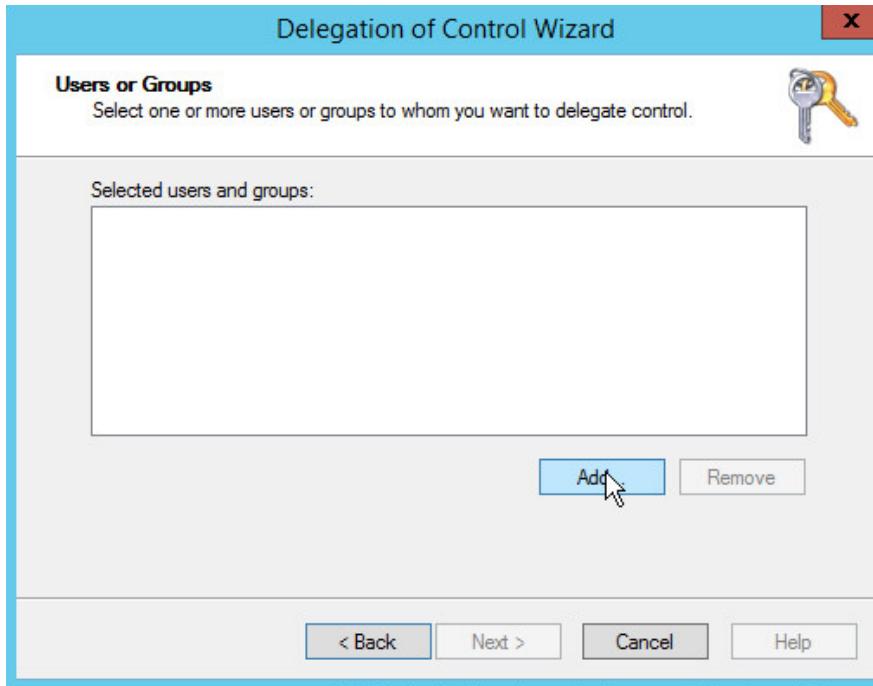
- 399
400 3. Right-click on **Users** in the left panel.

401
402

4. Click **Delegate Control**.

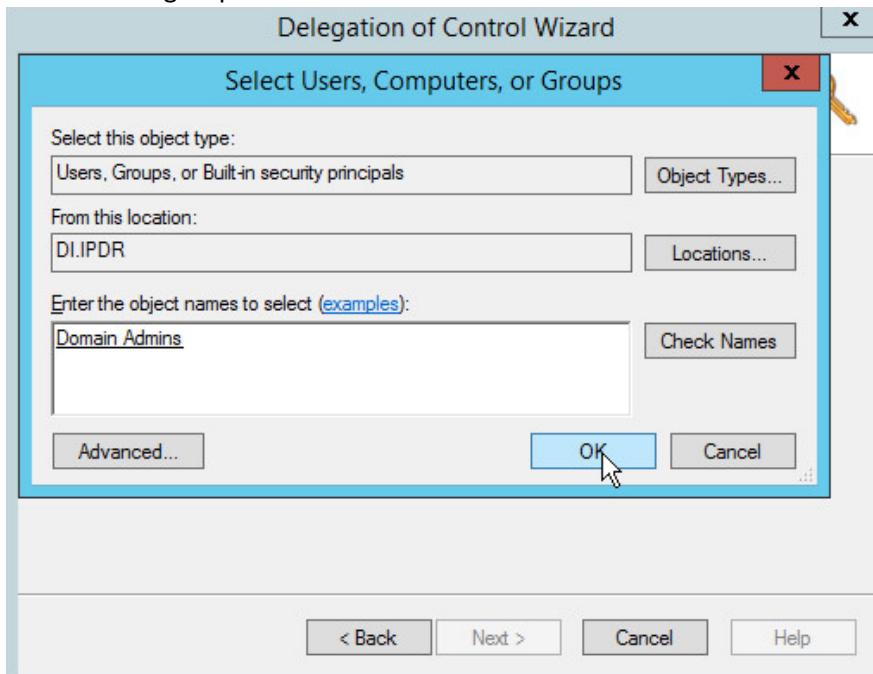
403
404

5. Click **Next**.



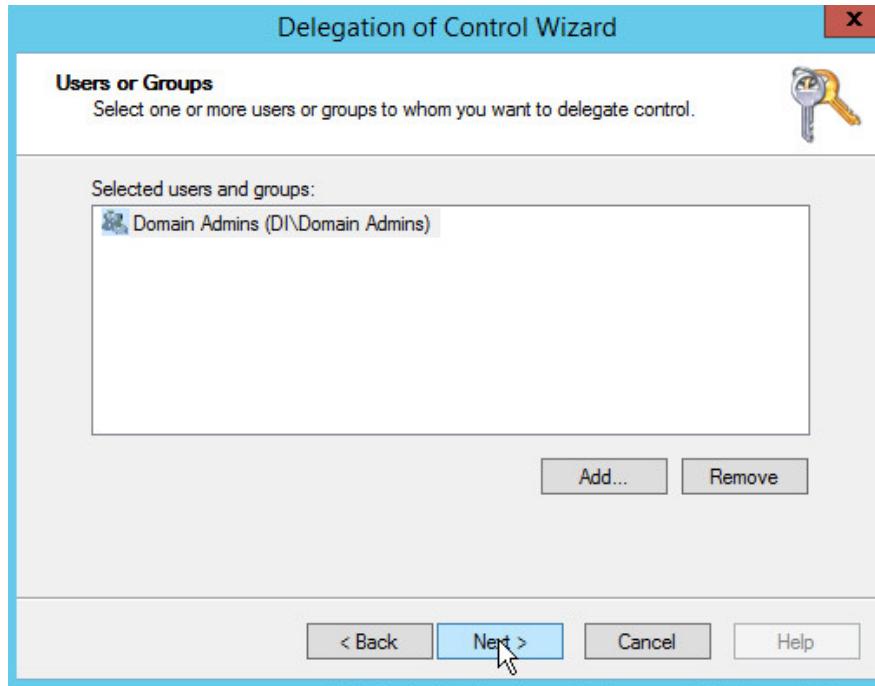
405
406
407

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



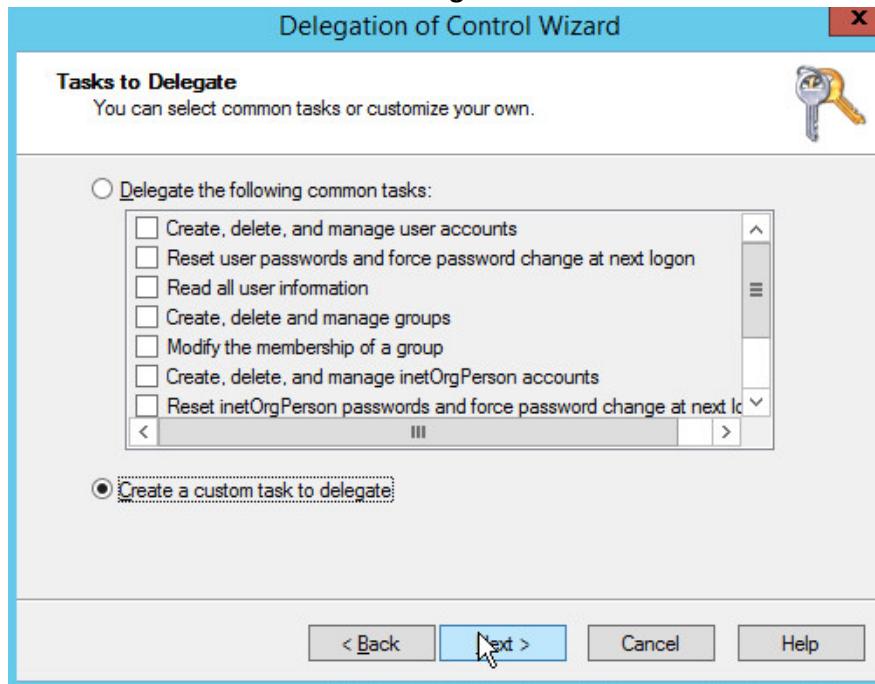
408
409

8. Click **OK**.



410
411
412

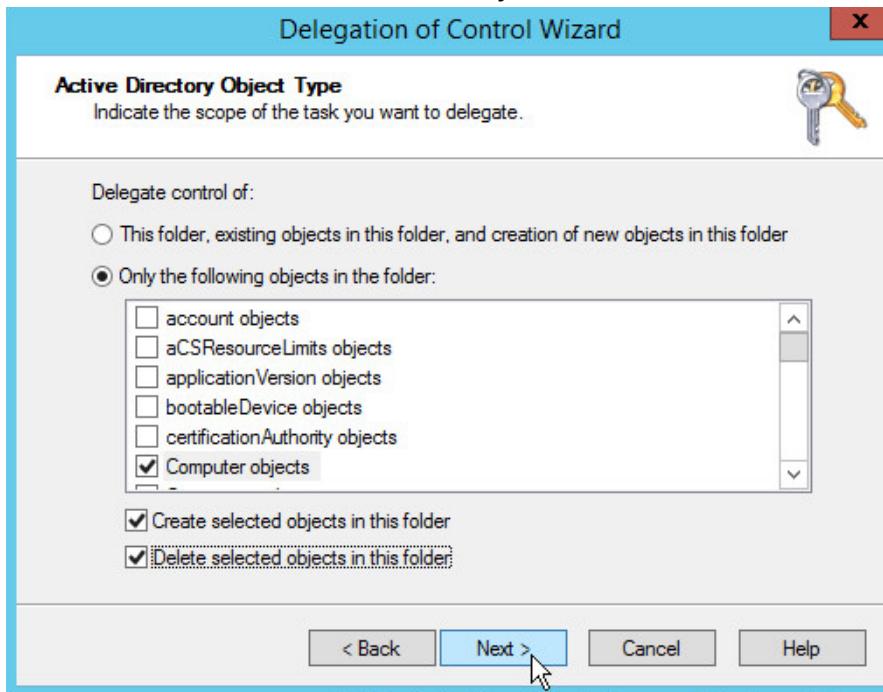
9. Click **Next**.
10. Choose **Create a custom task to delegate**.



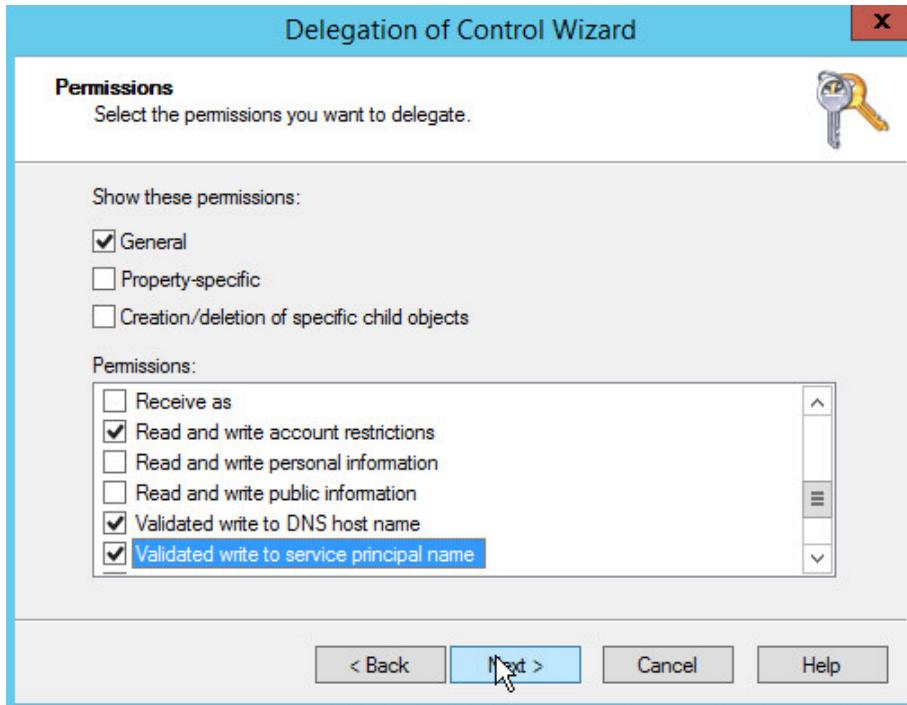
413
414
415

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**.

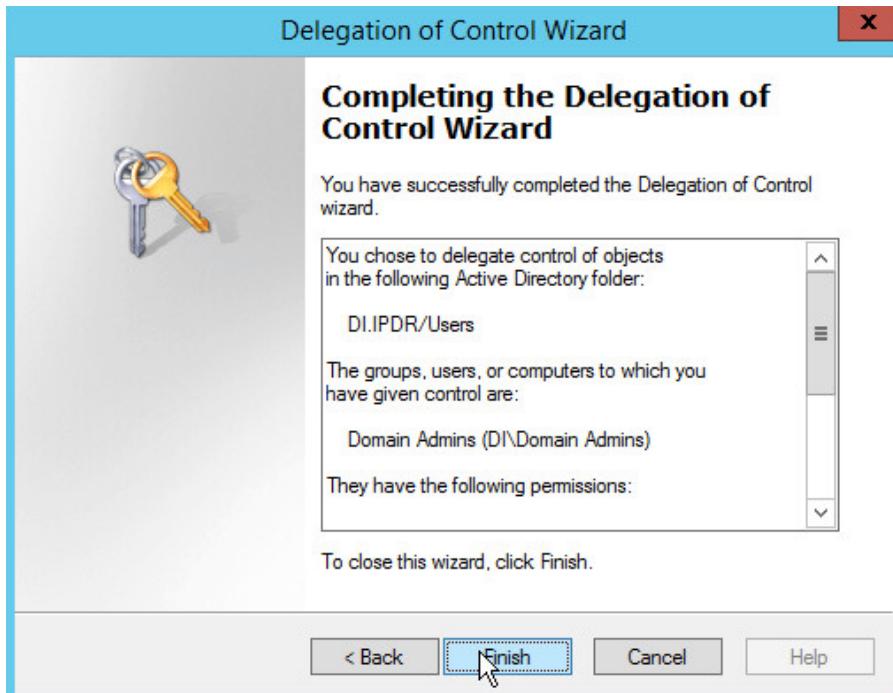


- 419
420 16. Click **Next**.
421 17. Check the boxes next to **Reset password**, **Read and write account restrictions**, **Validated write to DNS host name**, and **Validated write to service principal name**.



423
424

18. Click Next.

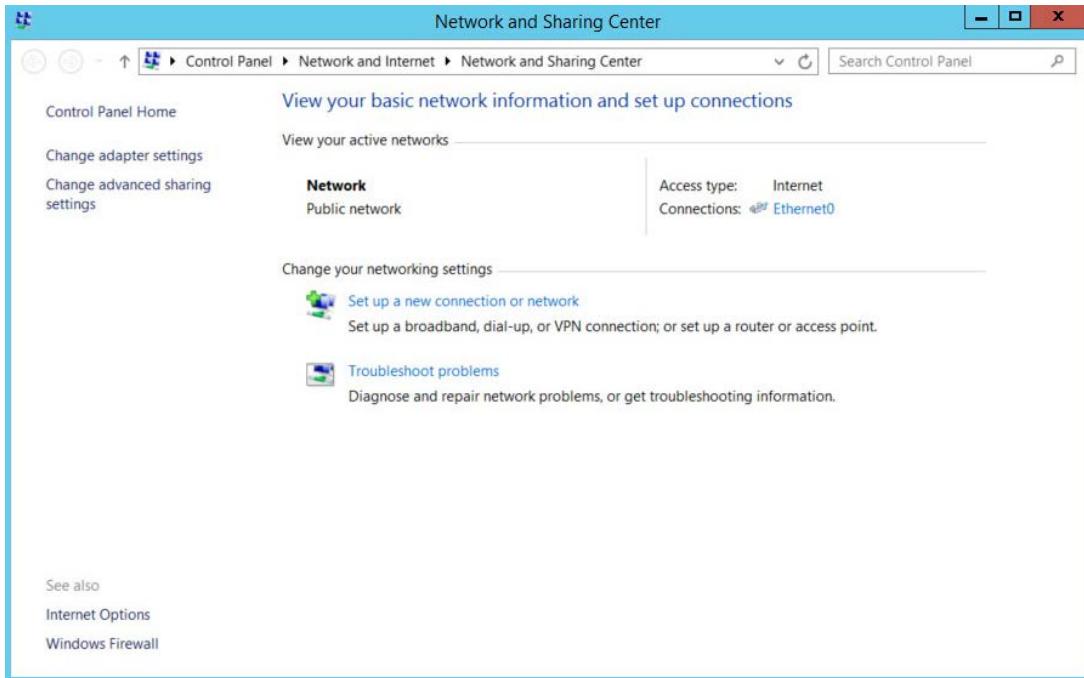


425
426

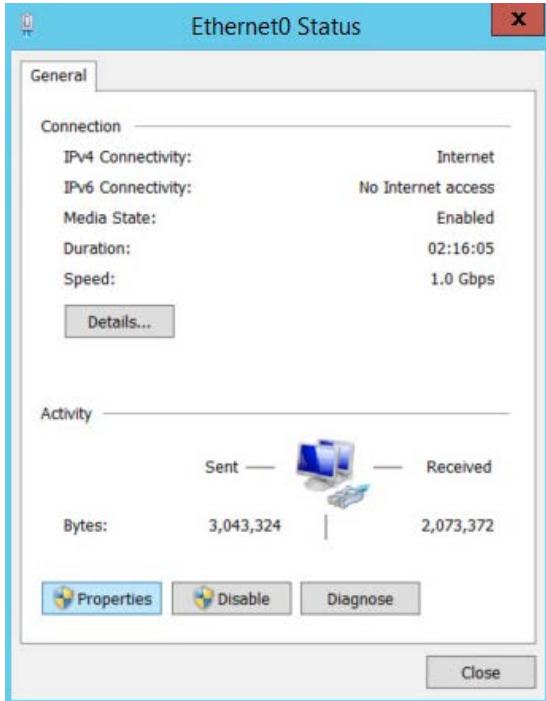
19. Click Finish.

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**.

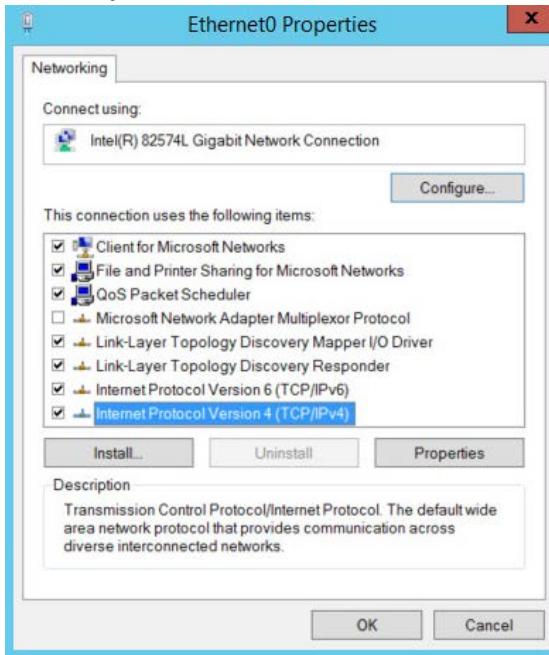


- 430
- 431 3. Click the name of the internet adapter.



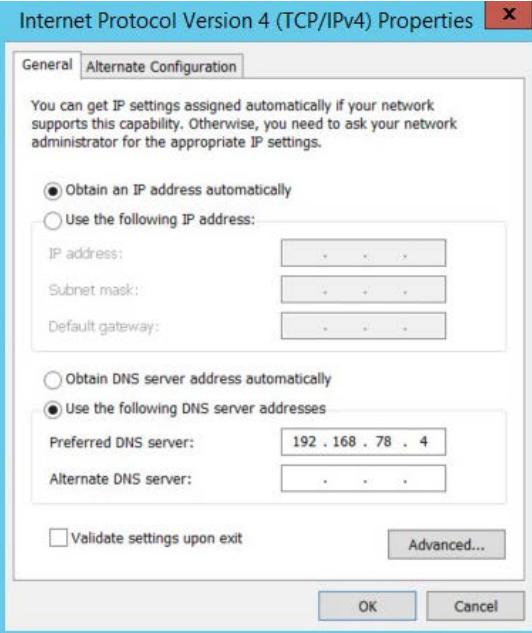
432
433

4. Click **Properties**.



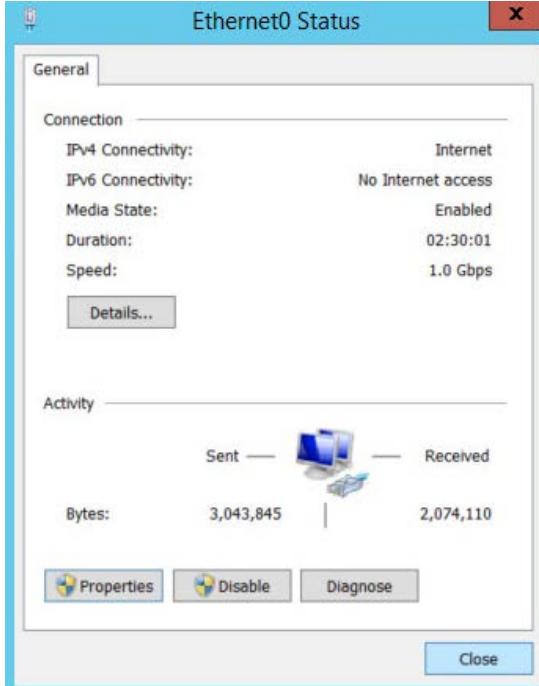
434
435
436
437

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**.

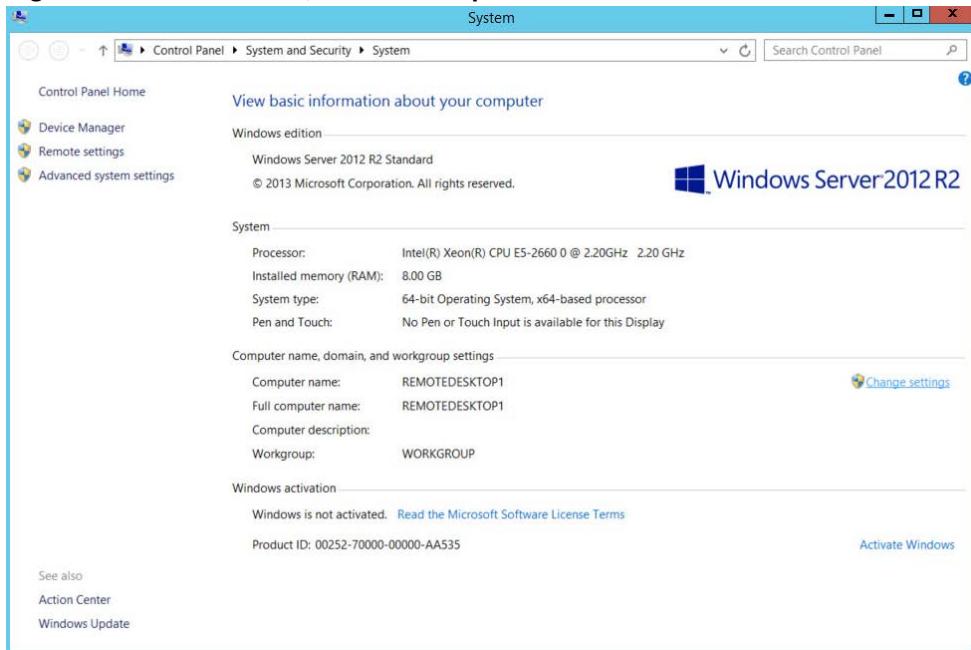


441
442
443

10. Click **Close**.
11. Navigate to **This PC**.

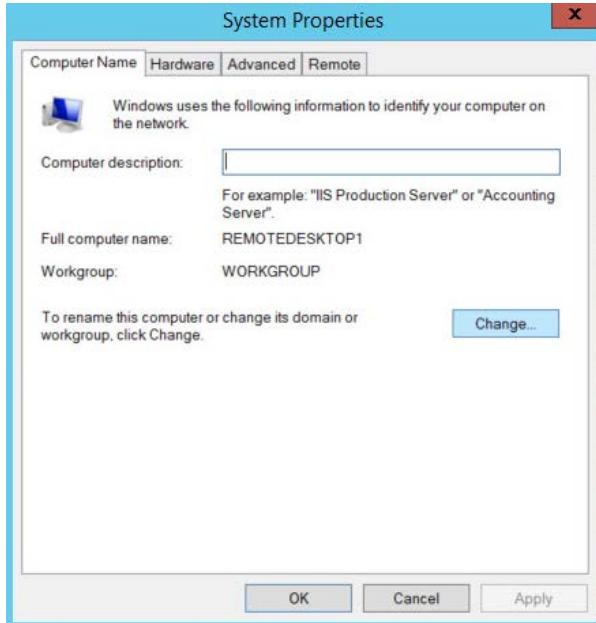
444
445

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



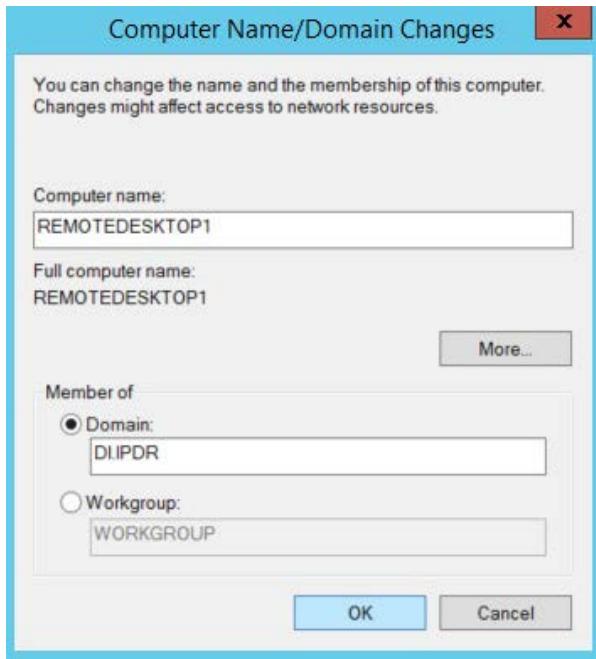
446
447

13. Click **Change Settings**.



448
449
450
451

14. Click **Change**.
15. Select **Domain**.
16. Enter the domain.



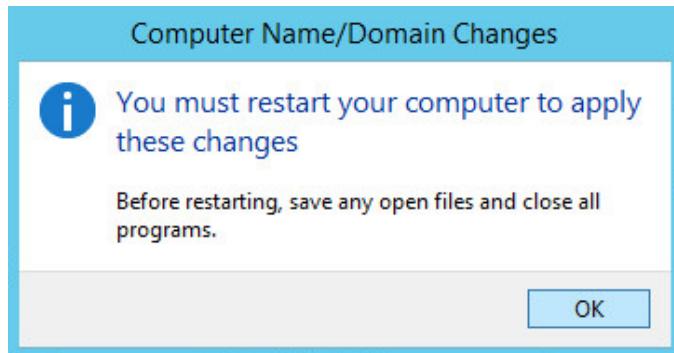
452
453
454

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



455
456

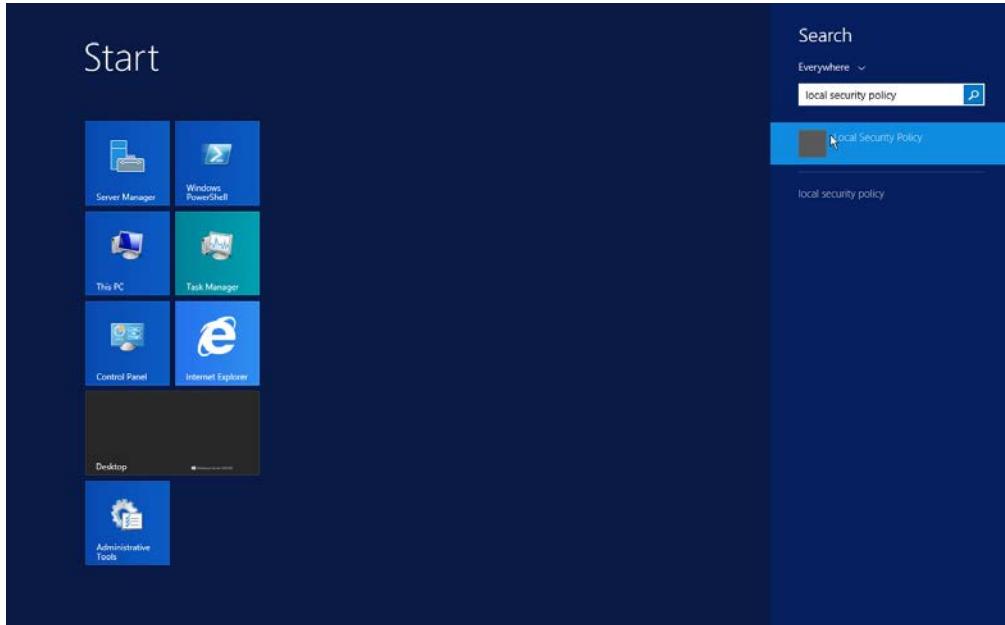
19. Click **OK**.



457
458

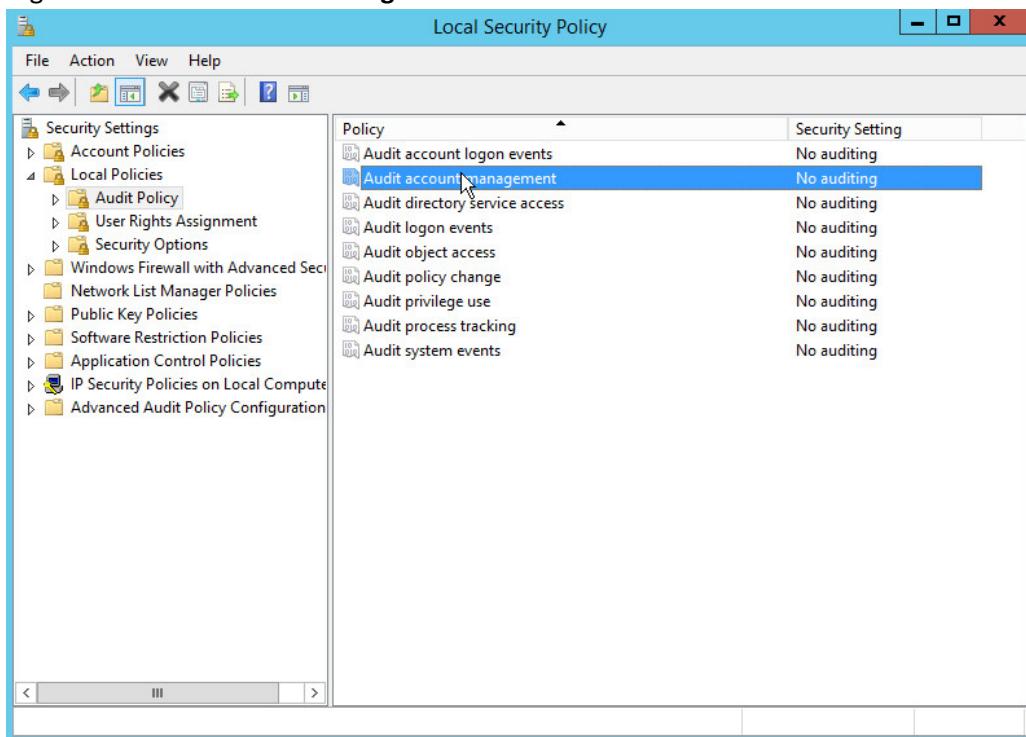
20. Click **OK** when prompted to restart the computer.

459 2.1.5 Configure Active Directory to Audit Account Activity
460 1. Open the **Start** Menu.



461
462
463
464

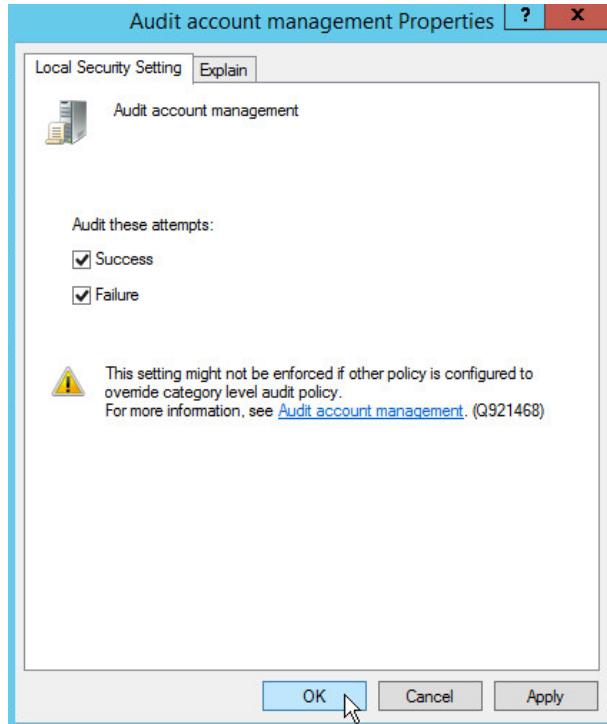
2. Enter Local Security Policy in the search bar, and open the program.
3. Navigate to **Local Policies > Audit Policy**.
4. Right-click **Audit account management**.



465
466

5. Click **Properties**.

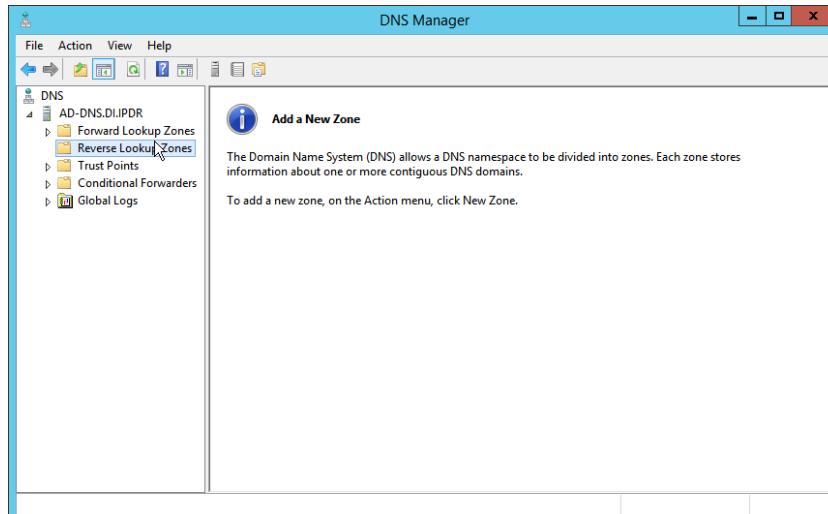
- 467 6. Check the boxes next to **Success** and **Failure**.



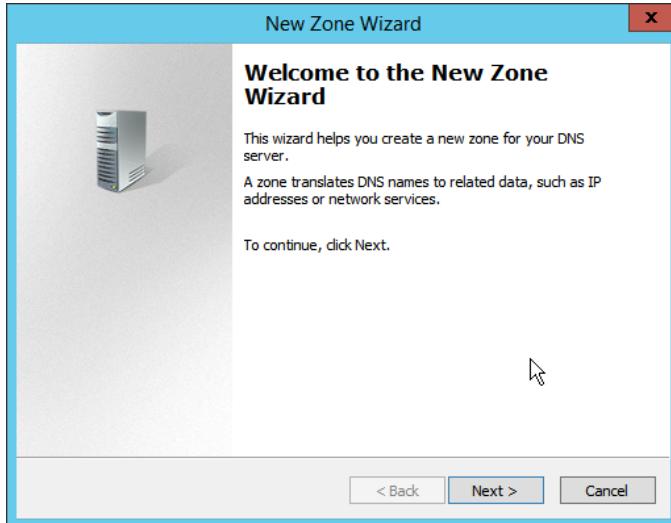
- 468
469 7. Click **OK**.

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**.



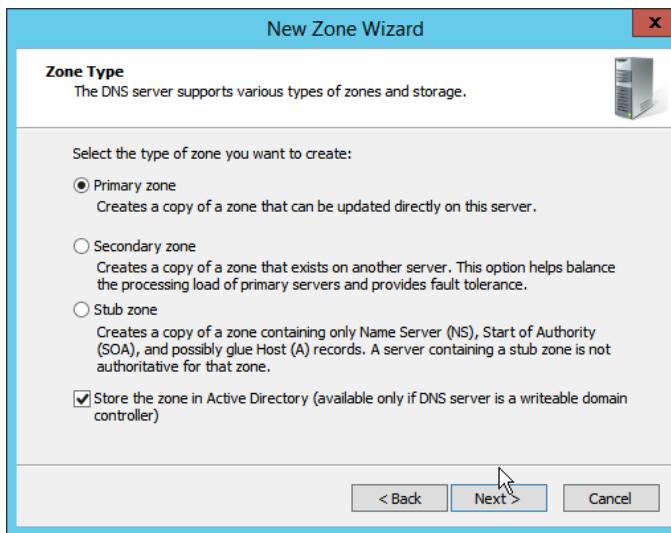
- 473
474 3. Click **Action > New Zone**.



475

476

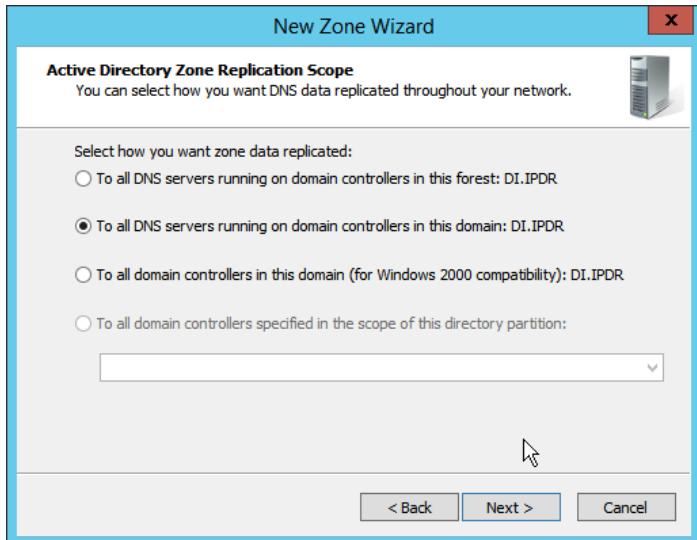
4. Click **Next**.



477

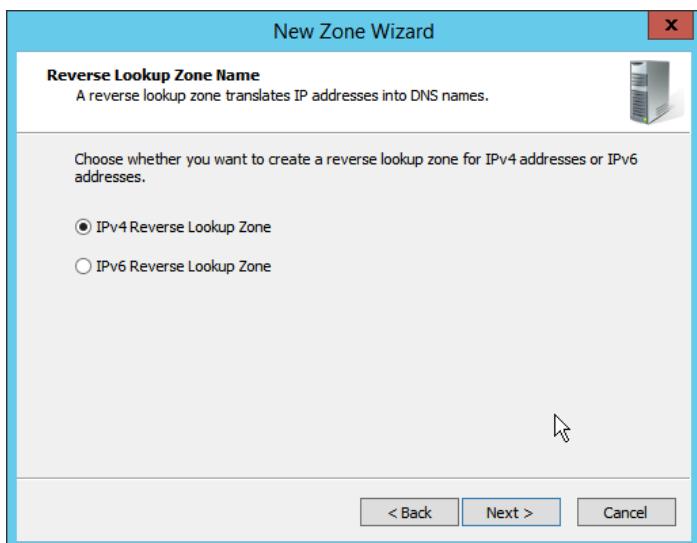
478

5. Click **Next**.



479
480

6. Click **Next**.

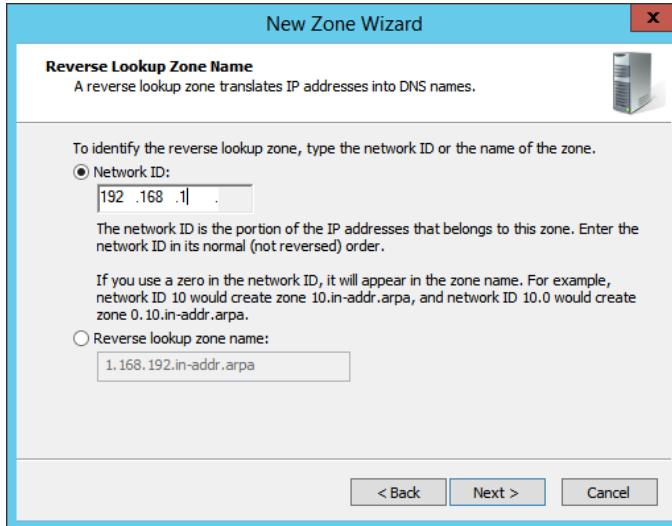


481
482
483

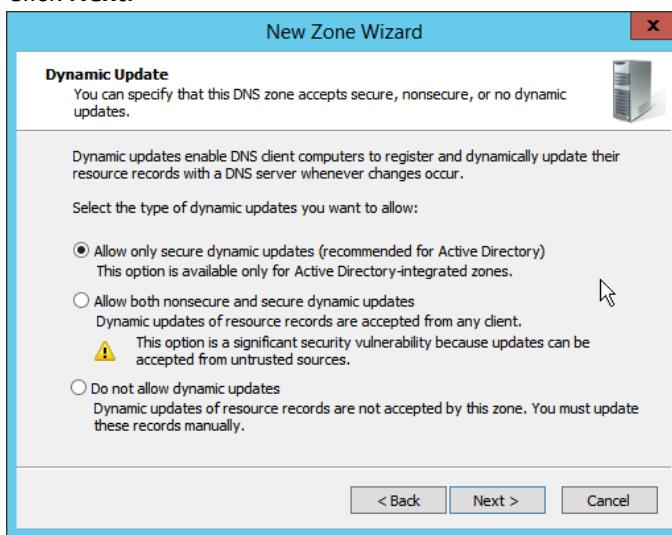
7. Click **Next**.
8. Enter the first three parts of the IP address of the AD/DNS server (for example, 192.168.1).

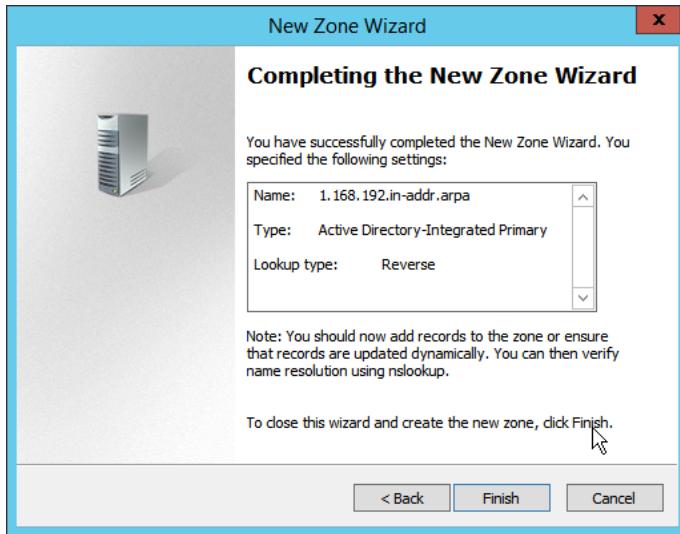
484
485

9. Click **Next**.

486
487

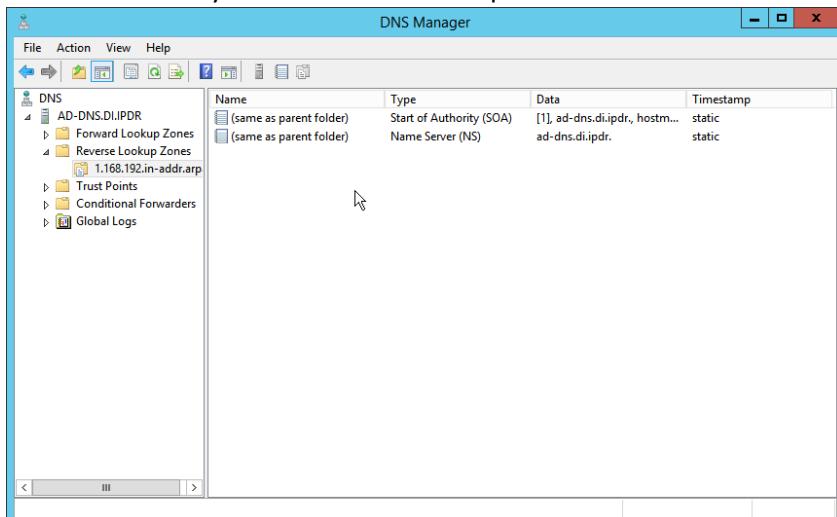
10. Click **Next**.





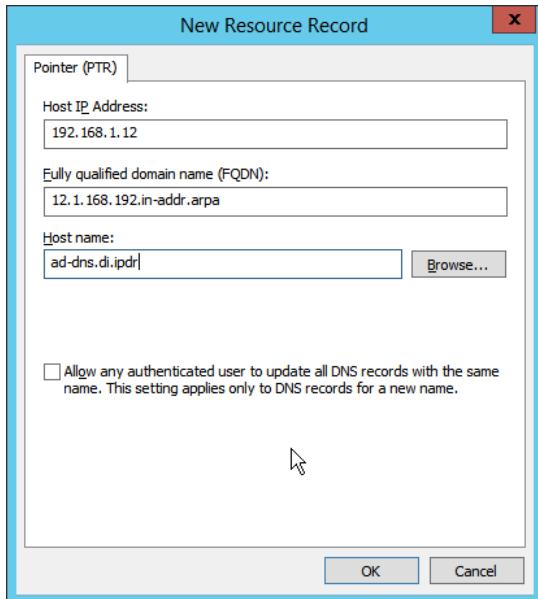
488
489
490

11. Click **Finish**.
12. Click on the newly created reverse lookup zone.

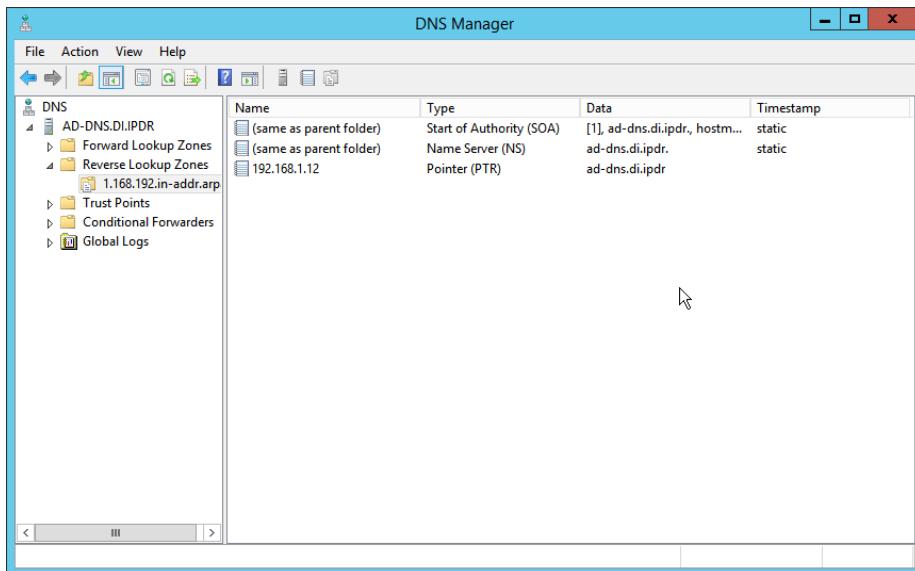


491
492
493
494

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.

495
496

16. Click OK.



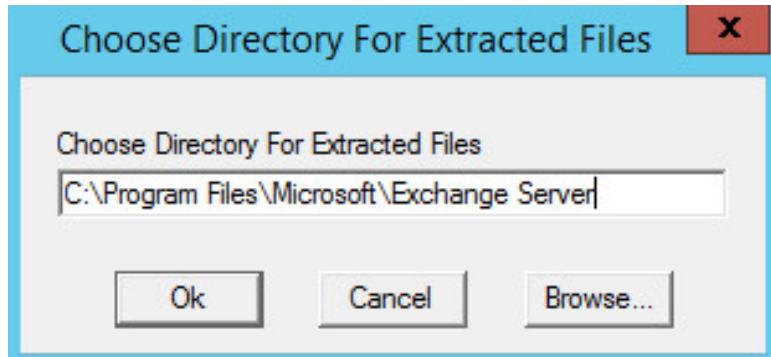
497

2.2 Microsoft Exchange Server

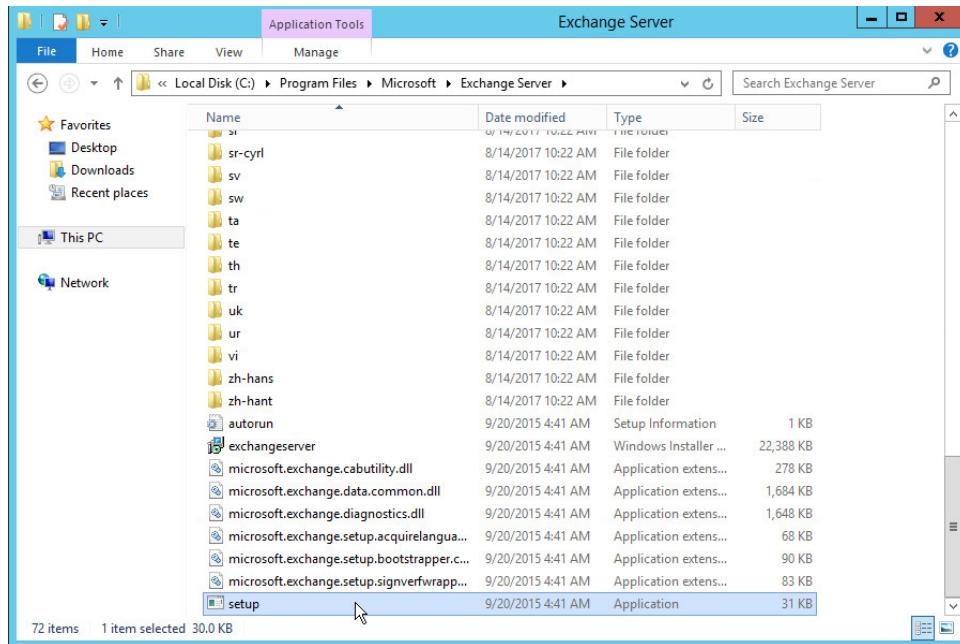
As part of our enterprise emulation, we include a Microsoft Exchange server. This section covers the installation and configuration process used to set up Microsoft Exchange on a Windows Server 2012 R2 machine.

502 **2.2.1 Install Microsoft Exchange**

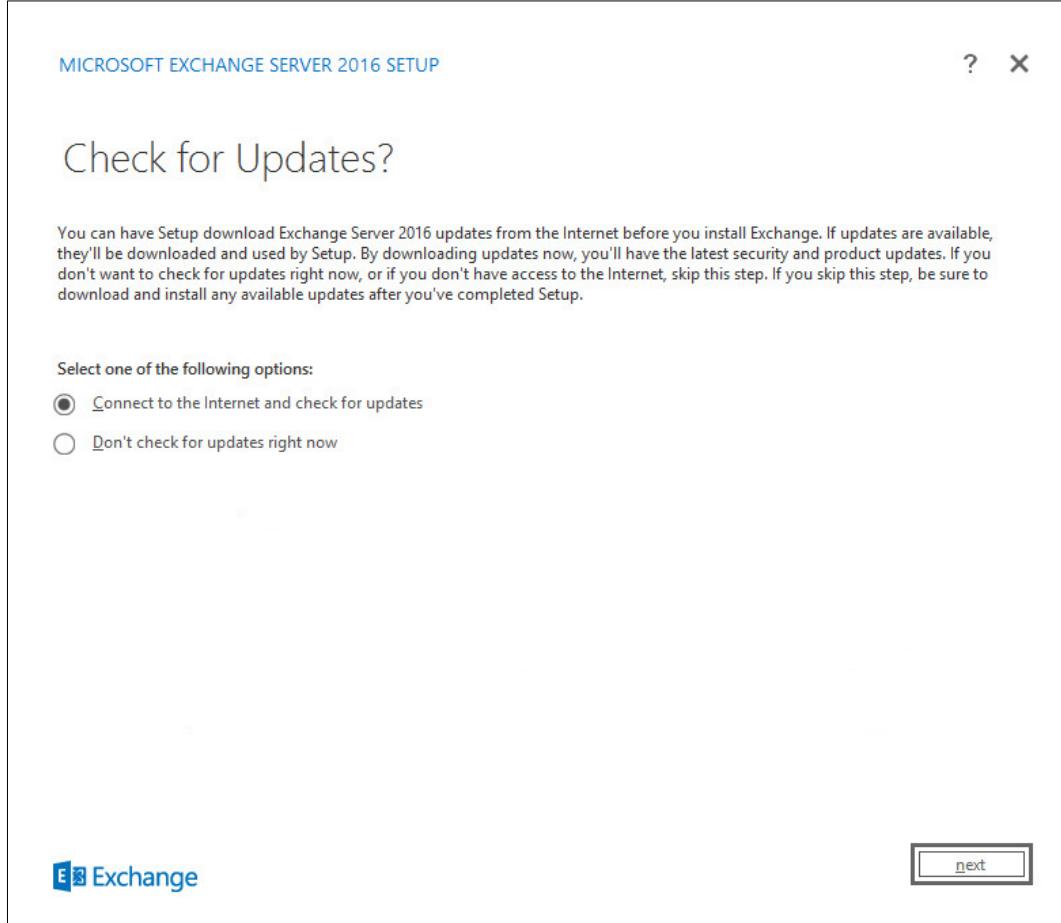
- 503 1. Run **Exchange2016-x64.exe**.
504 2. Choose the directory for the extracted files.



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

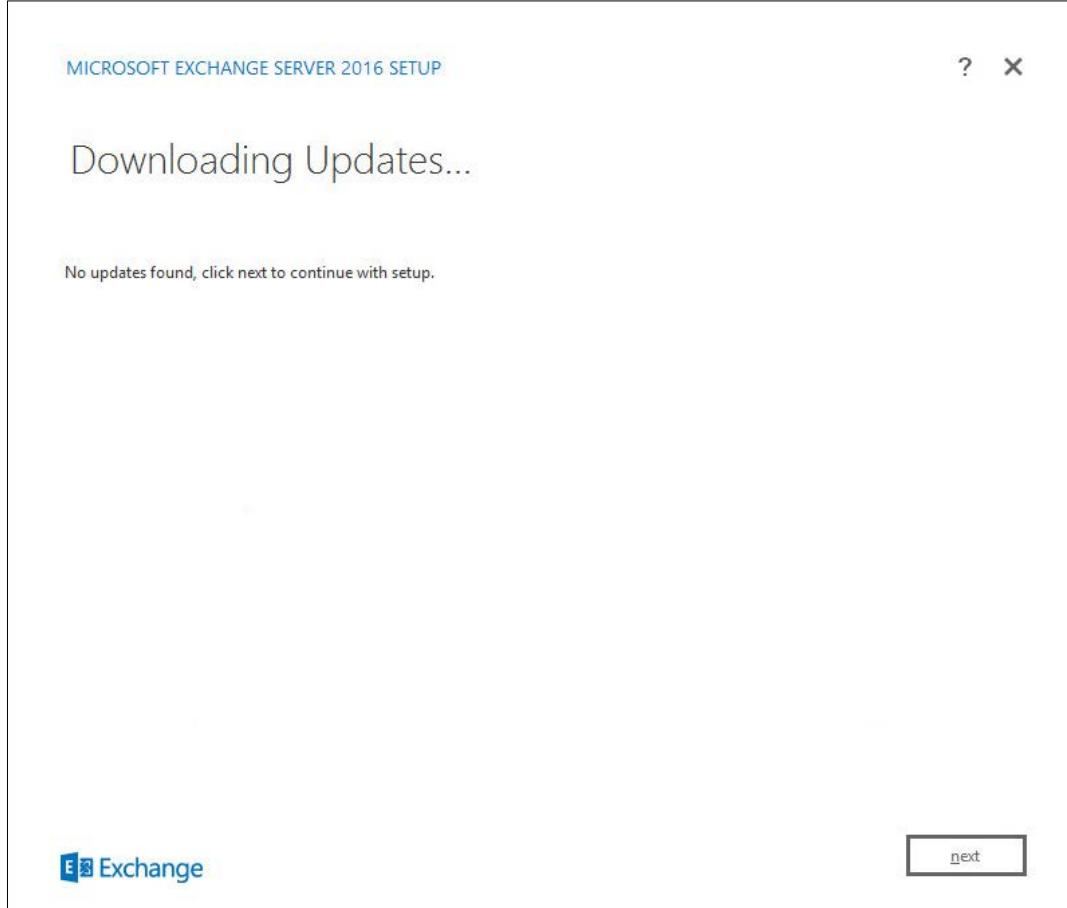


- 507
508 4. Enter the directory and run **setup.exe**.
509 5. Select **Connect to the Internet and check for updates**.

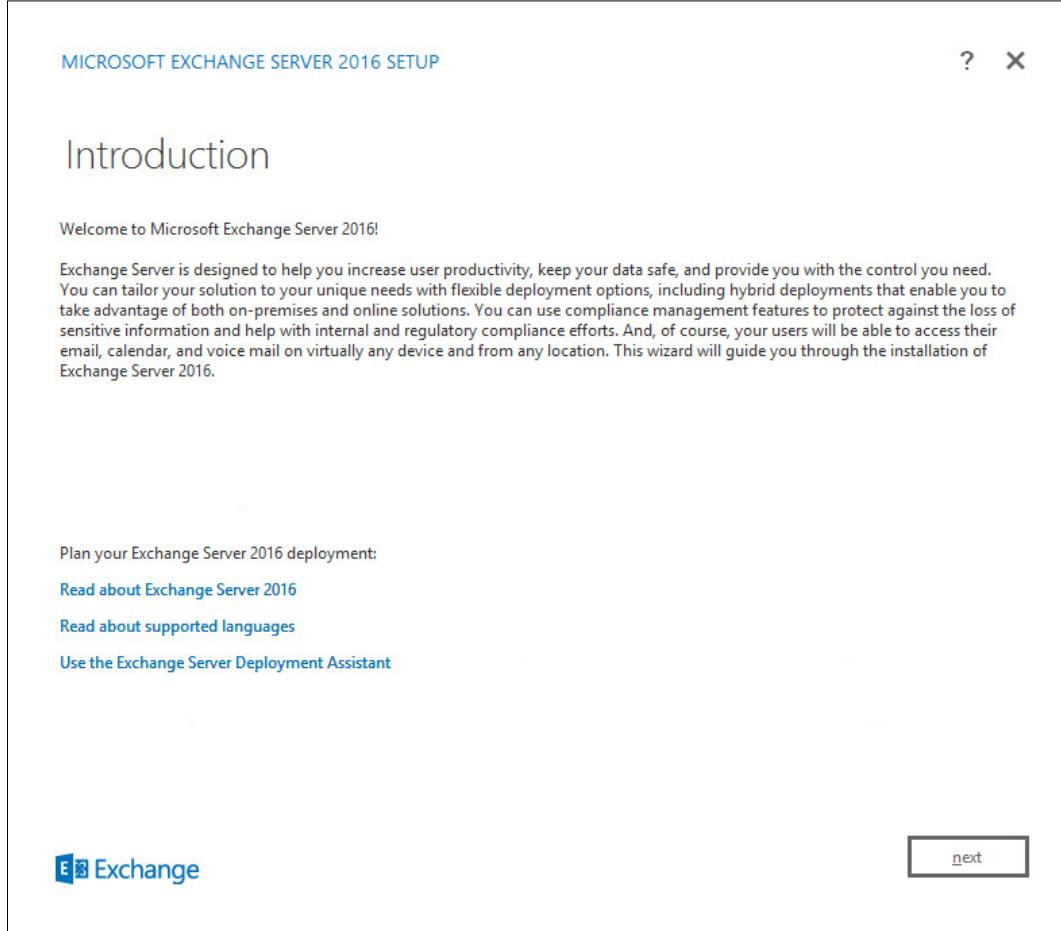


510
511
512

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

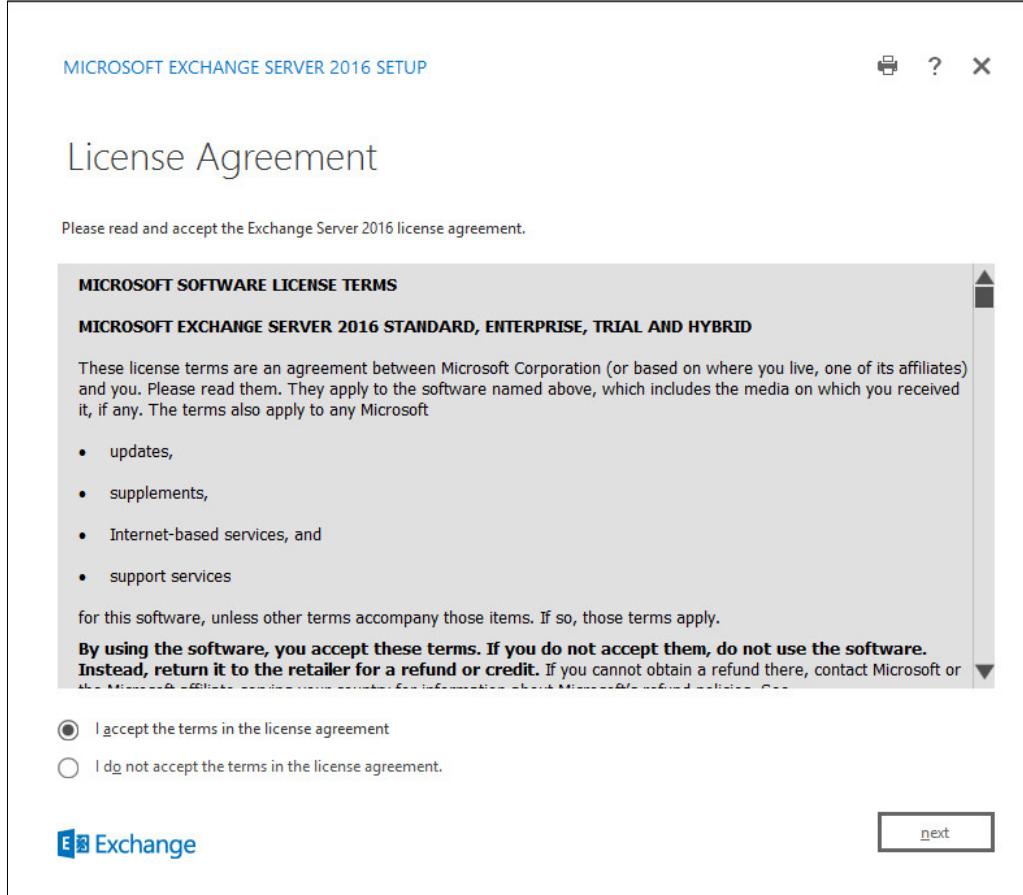


- 513
514 8. Click **Next**.
515 9. Wait for the copying to finish.



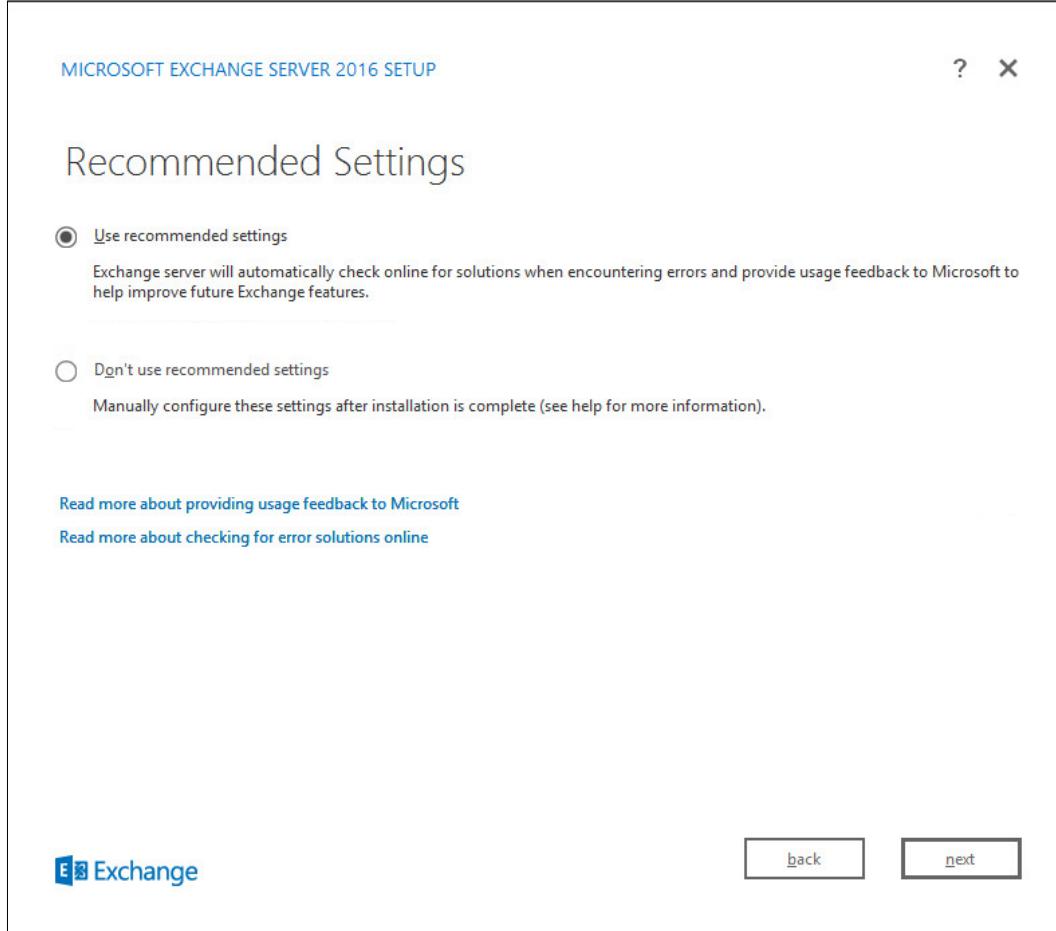
516
517
518

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

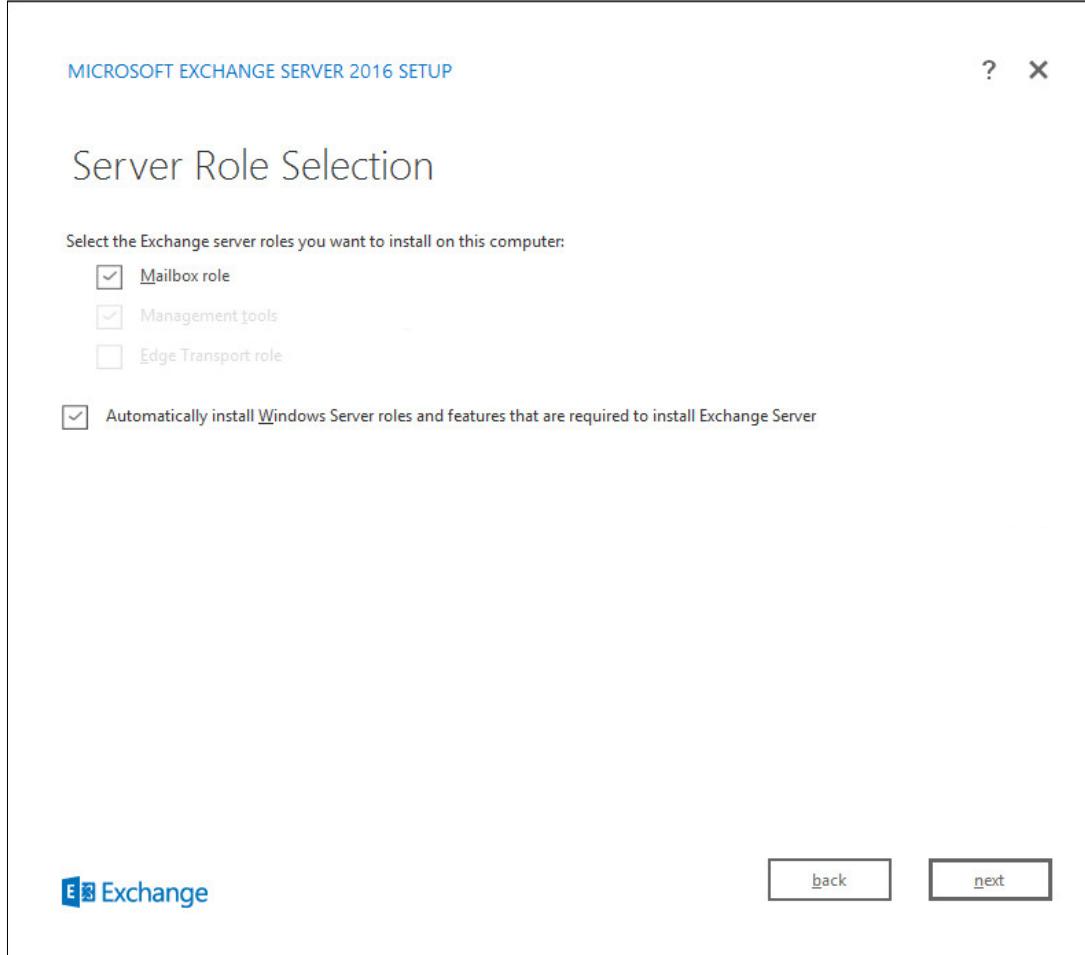


519
520
521

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

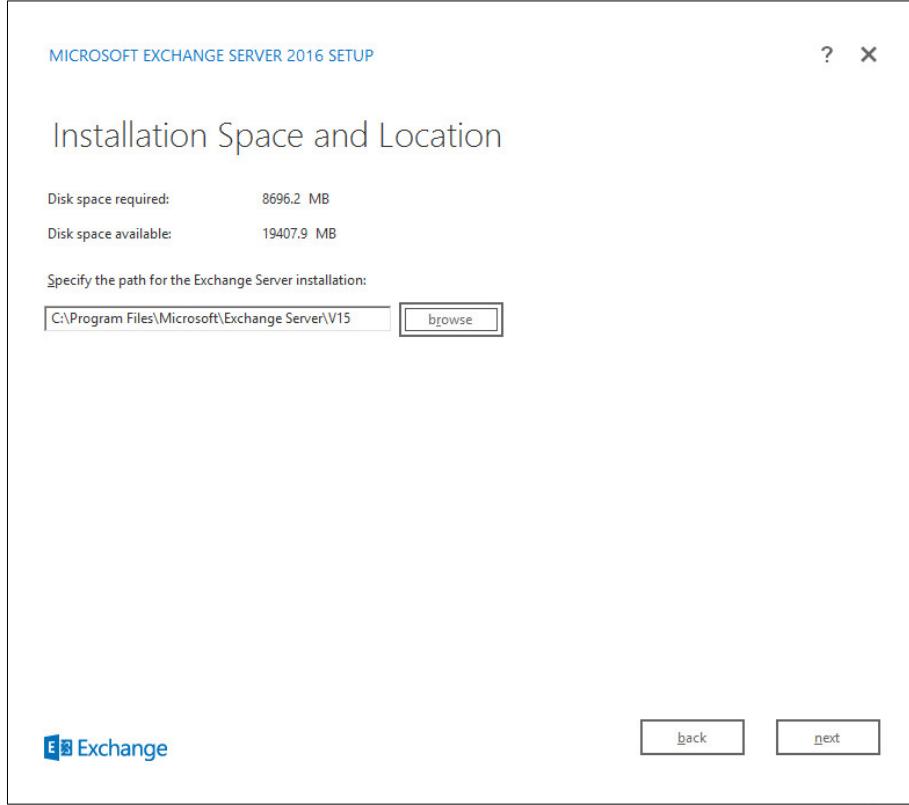


- 522
523 14. Click **Next**.
524 15. Check **Mailbox role**.
525 16. Check **Automatically install Windows Server roles and features that are required to install Exchange Server**.

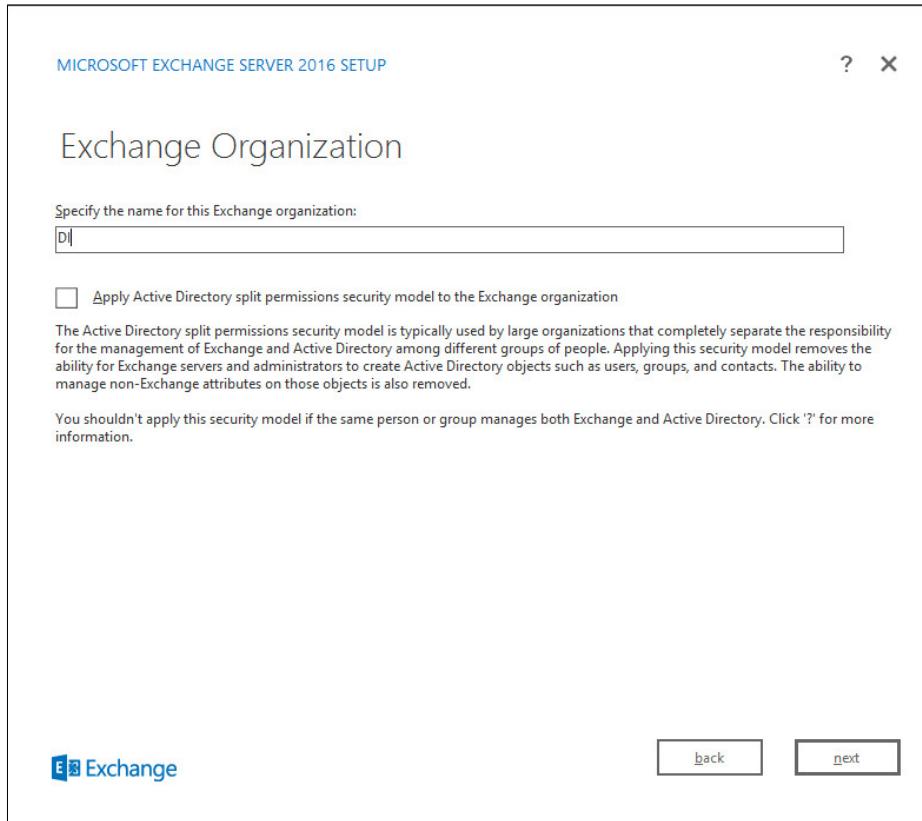


527
528
529

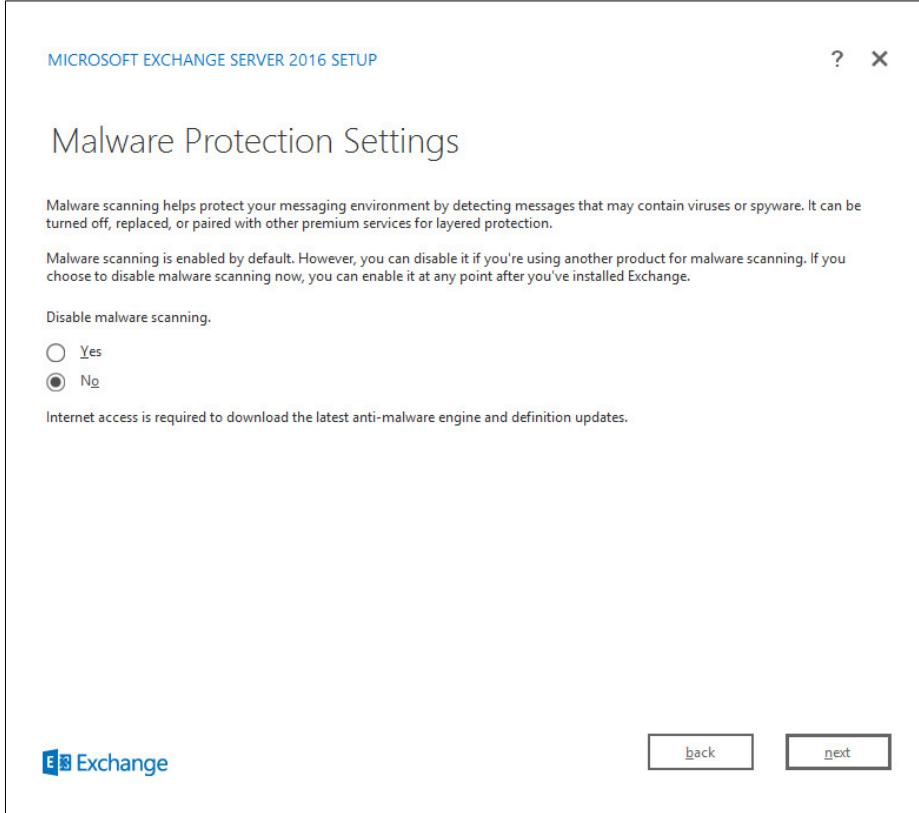
17. Click **Next**.
18. Specify the installation path for MS Exchange.



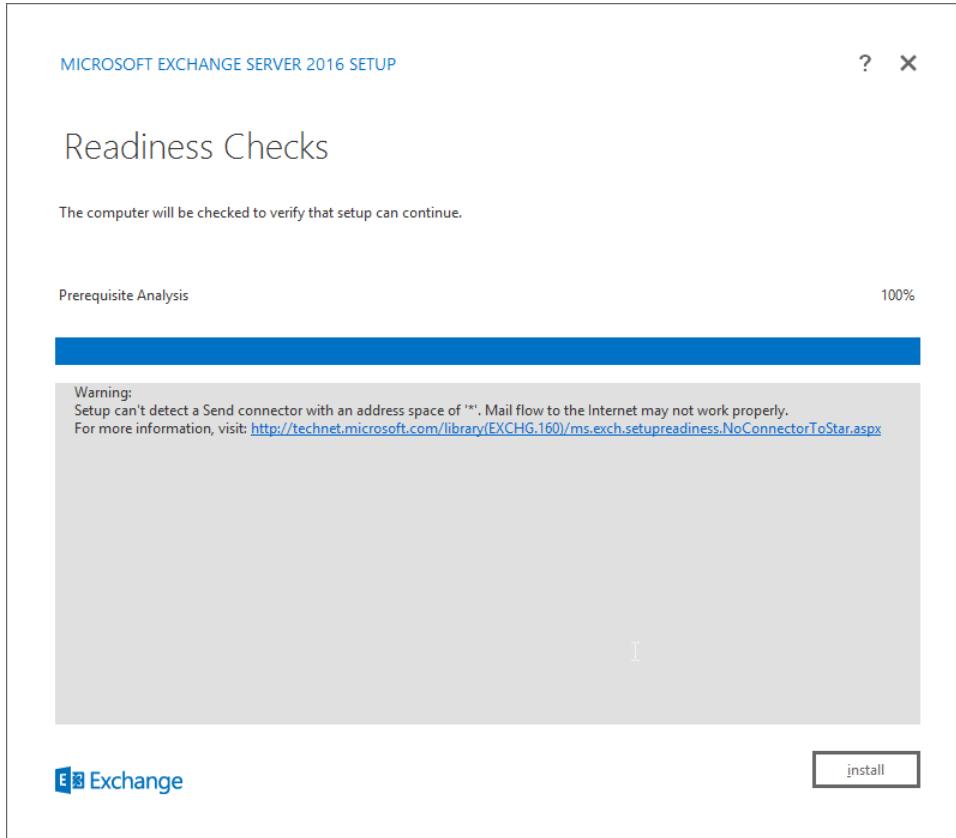
- 530
531 19. Click **Next**.
532 20. Specify the name for the Exchange organization, for example, DI.
533 21. Decide whether to apply split permissions, based on the needs of the enterprise.



534
535 22. Click **Next**.
536 23. Select **No**.



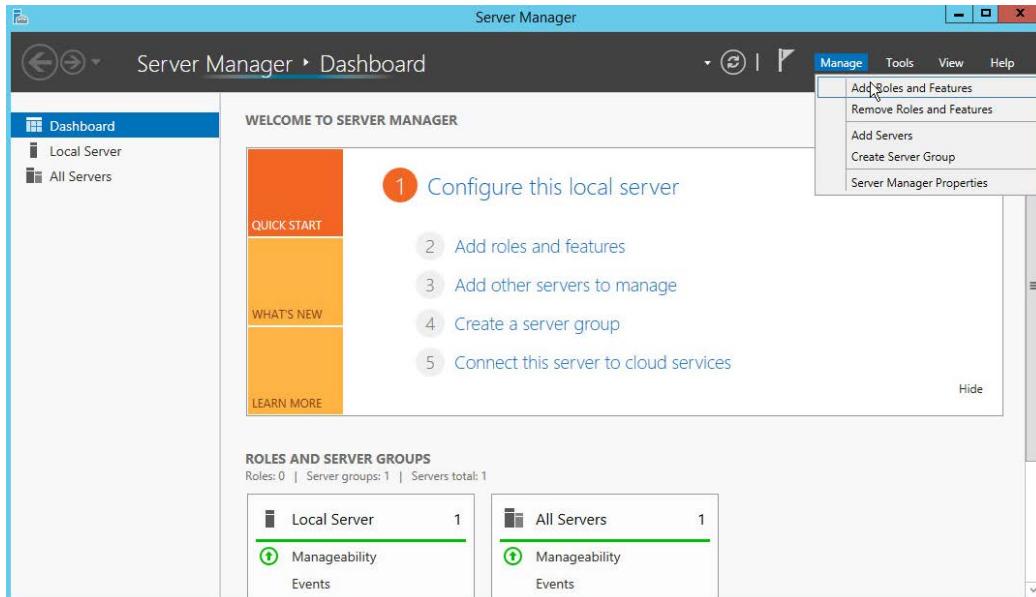
- 537
538 24. Click **Next**.
539 25. Install any **prerequisites** listed.
540 26. If necessary, restart the server and re-run **setup.exe**, completing steps 3-22 again.



541
542

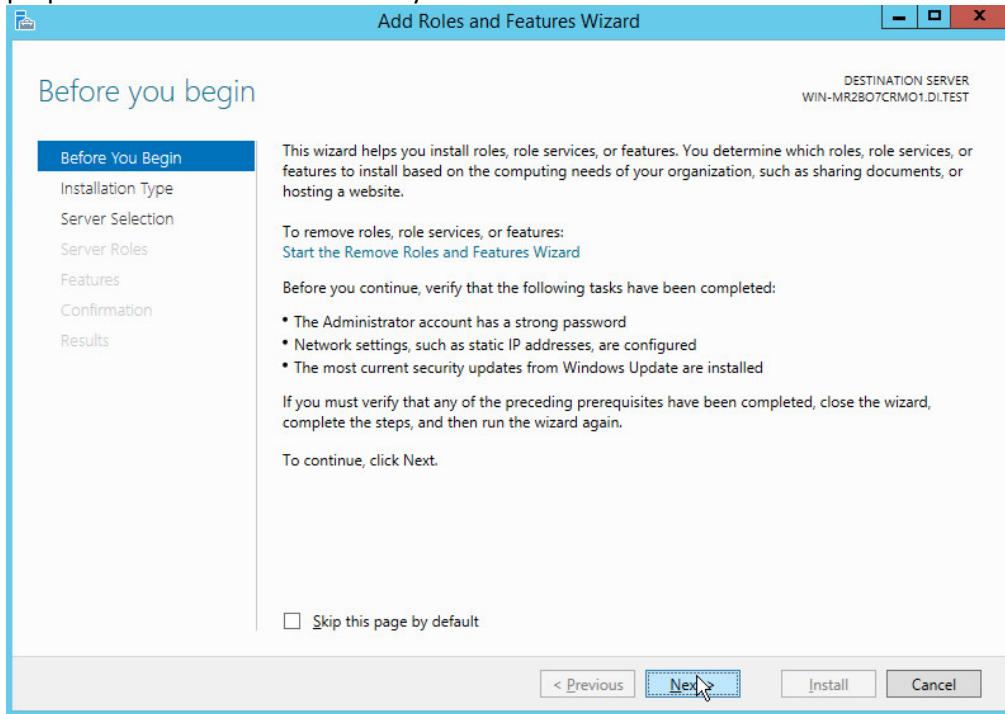
27. Click **Install**.

- 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
545 instructions for installing Windows Server Hyper-V on a Windows Server 2012 R2 machine.
- 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**.



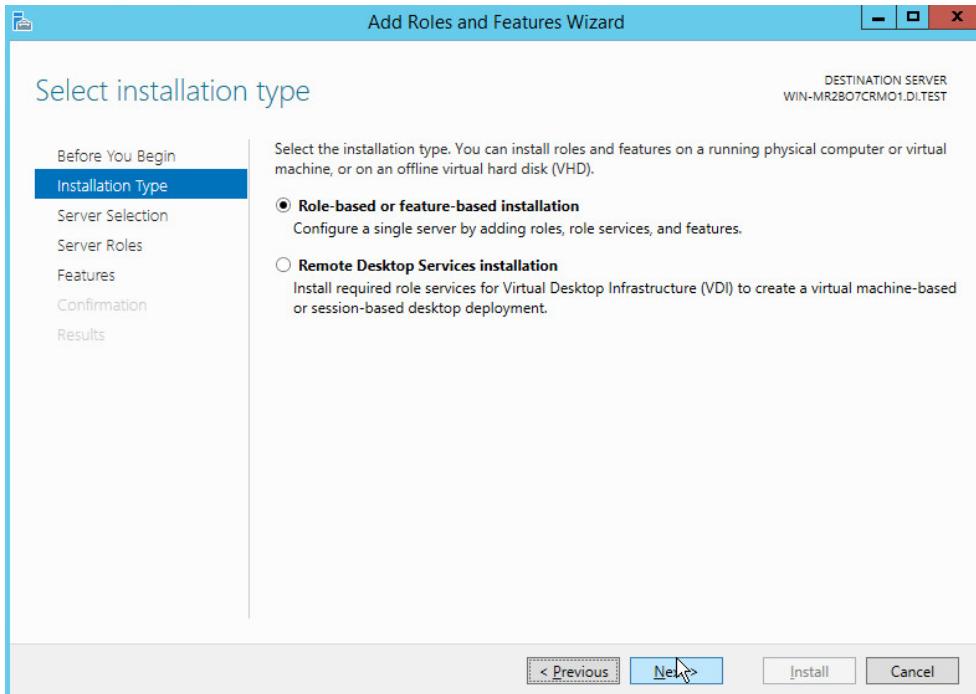
551
552
553

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**.

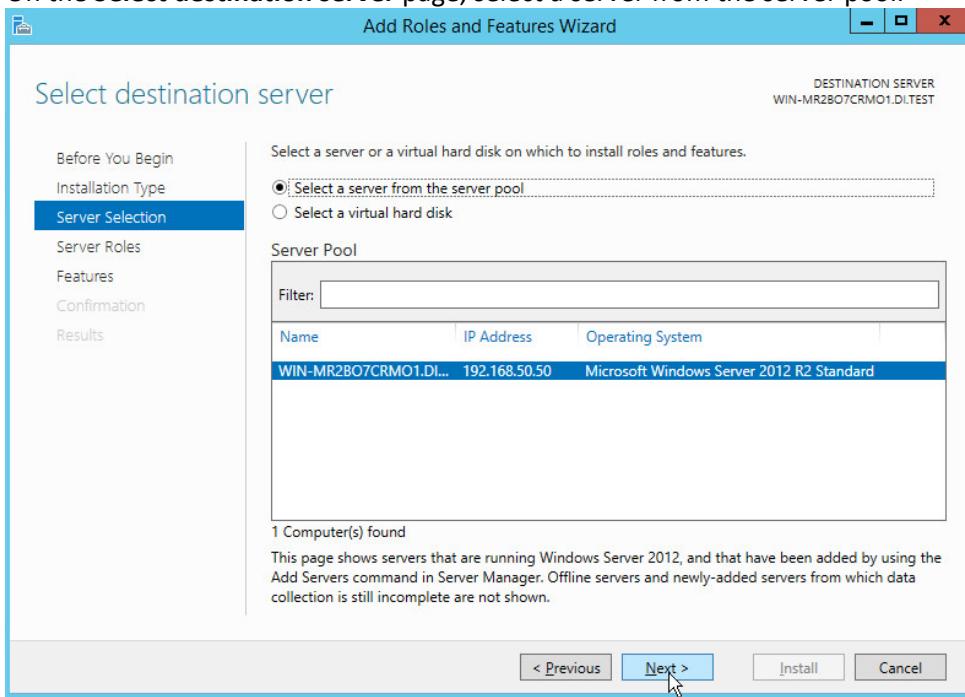


557

558

559

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



560

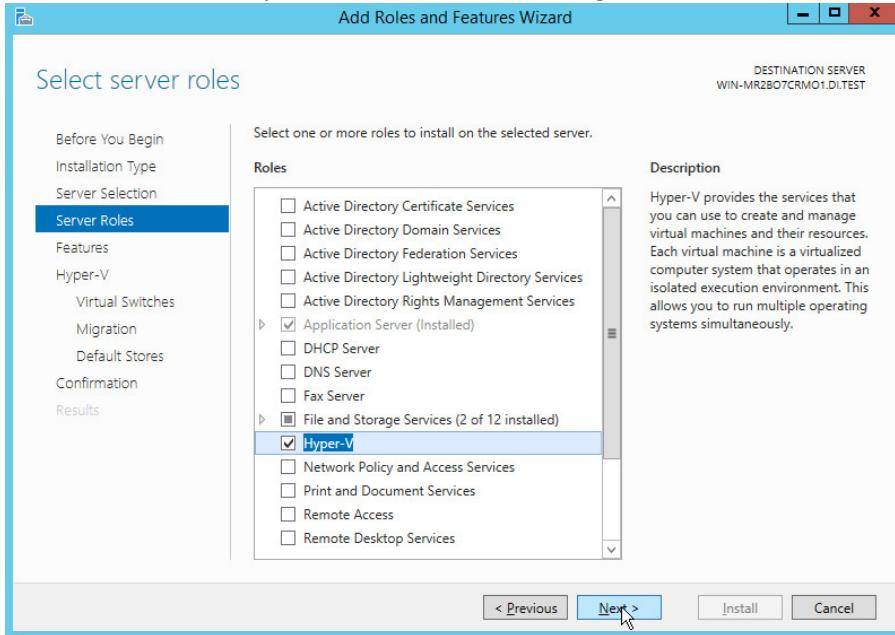
561

562

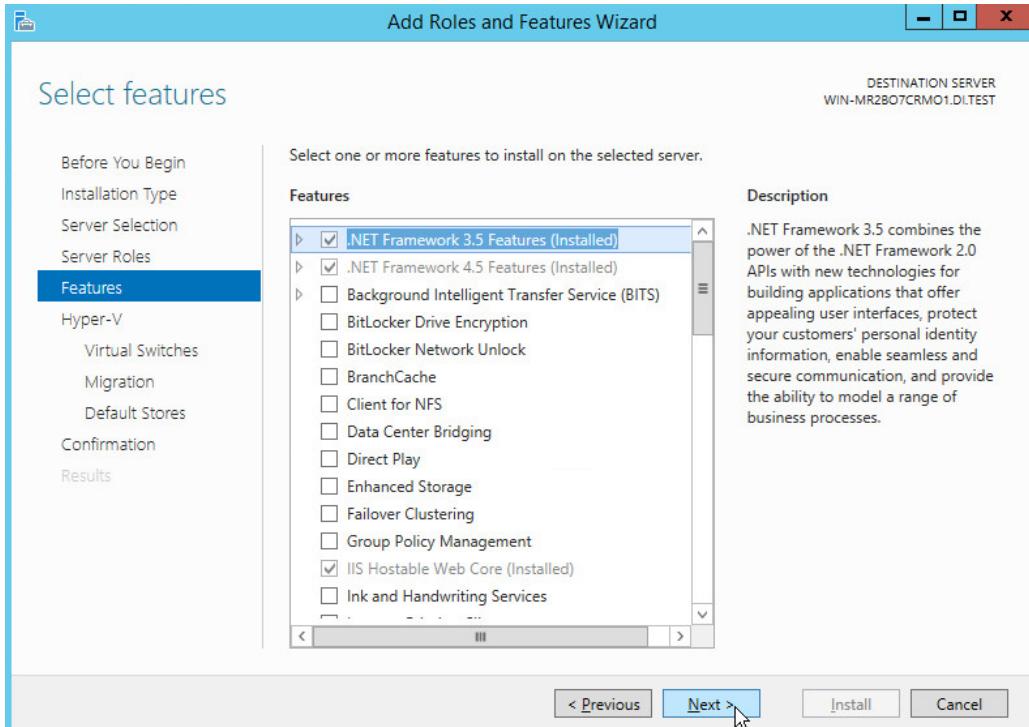
7. Click **Next**.
8. On the **Select server roles** page, select **Hyper-V**.

563

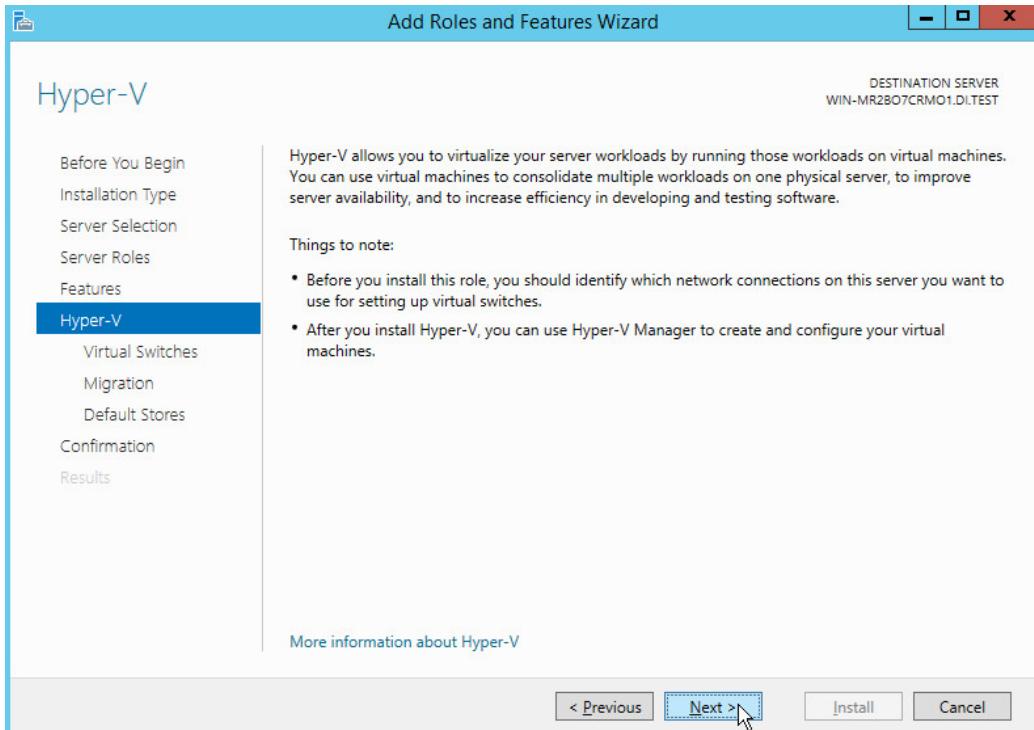
9. To add the tools that you use to create and manage virtual machines, click **Add Features**.

564
565

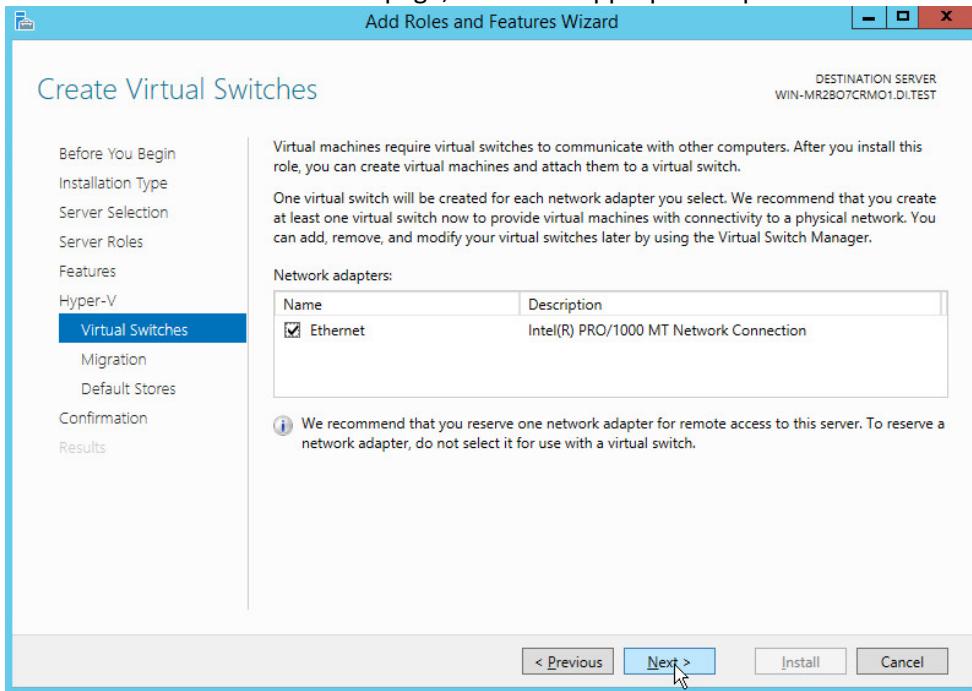
10. Click **Next**.

566
567

11. Click **Next**.

568
569
570

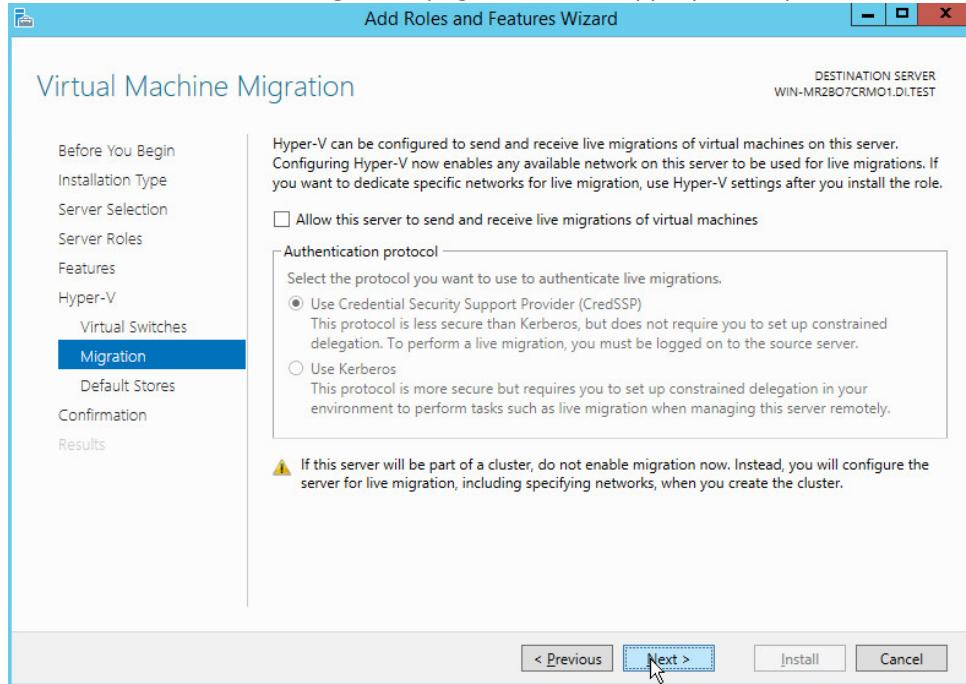
12. Click **Next**.
13. On the **Create Virtual Switches** page, select the appropriate options.

571
572

14. Click **Next**.

573

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

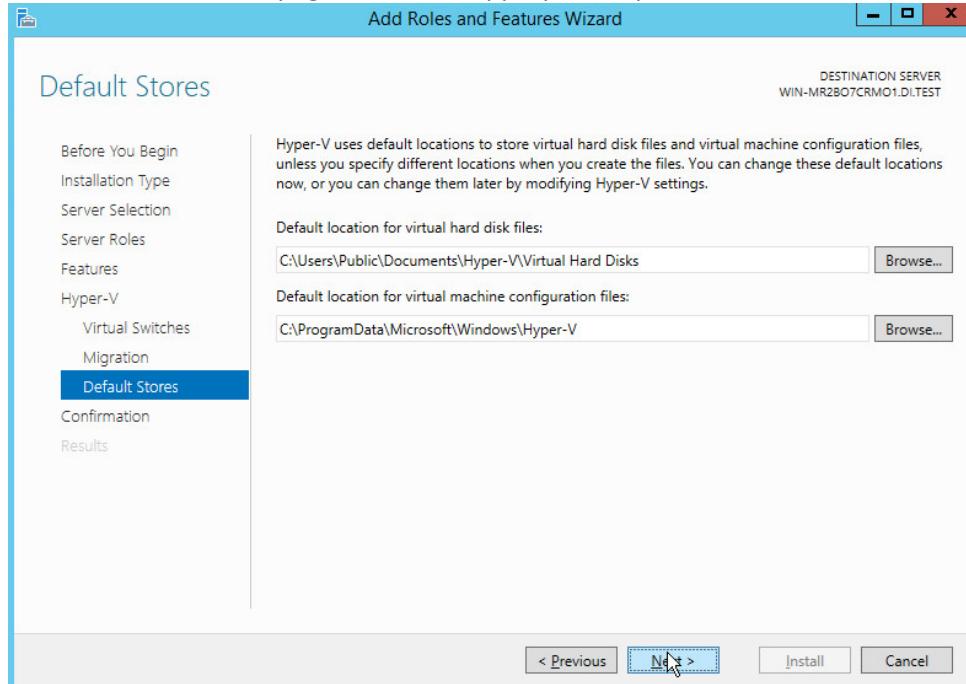


574

16. Click **Next**.

575

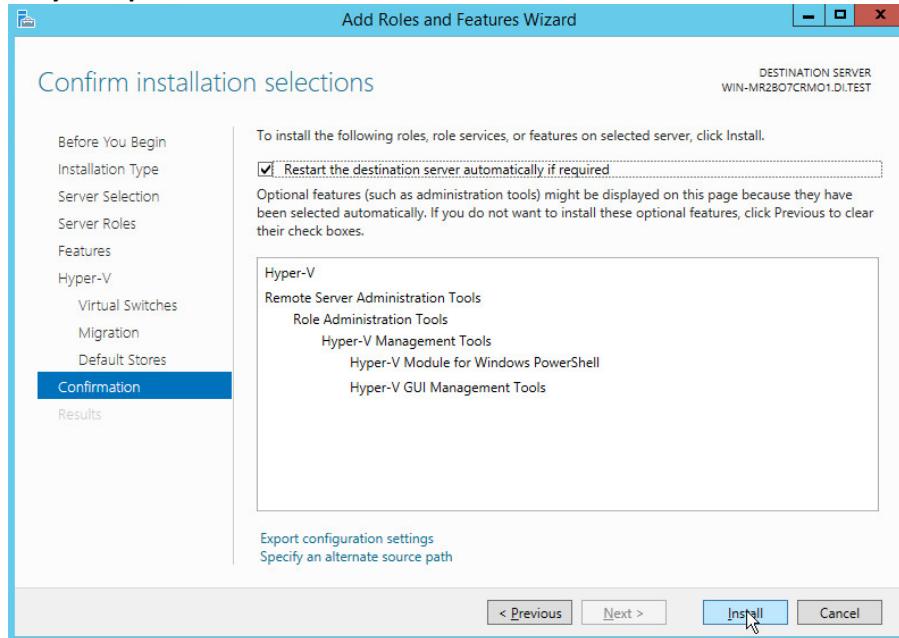
17. On the **Default Stores** page, select the appropriate options.



577

18. Click **Next**.

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



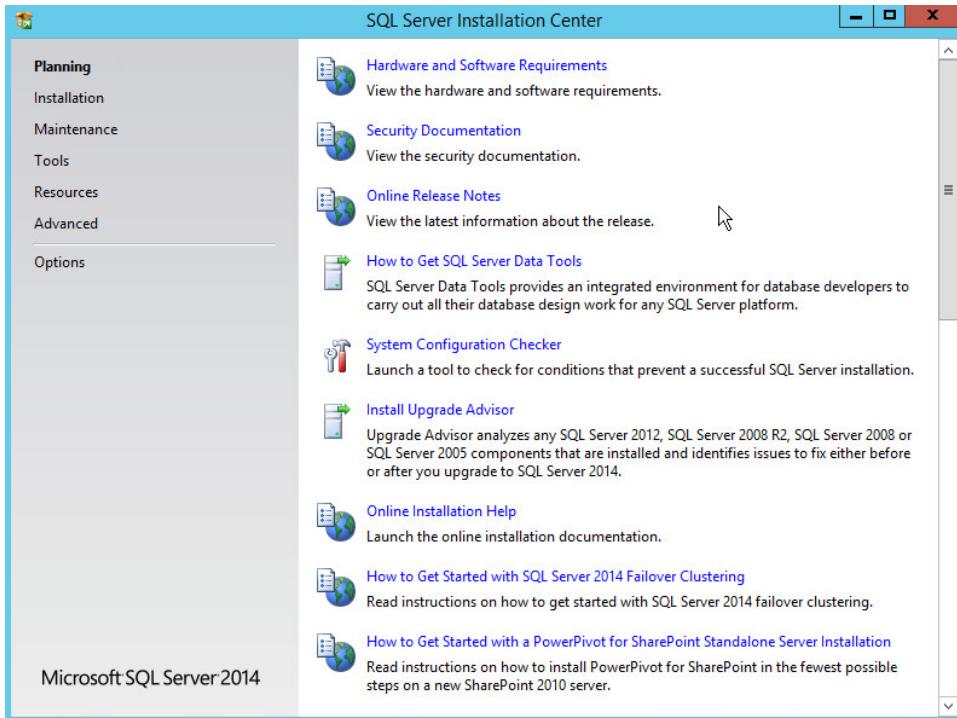
- 581 20. Click **Install**.
- 582 21. When installation is finished, verify that Hyper-V installed correctly. Open the **All Servers** page in Server Manager, and select a server on which you installed Hyper-V. Check the **Roles and Features** tile on the page for the selected server.

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

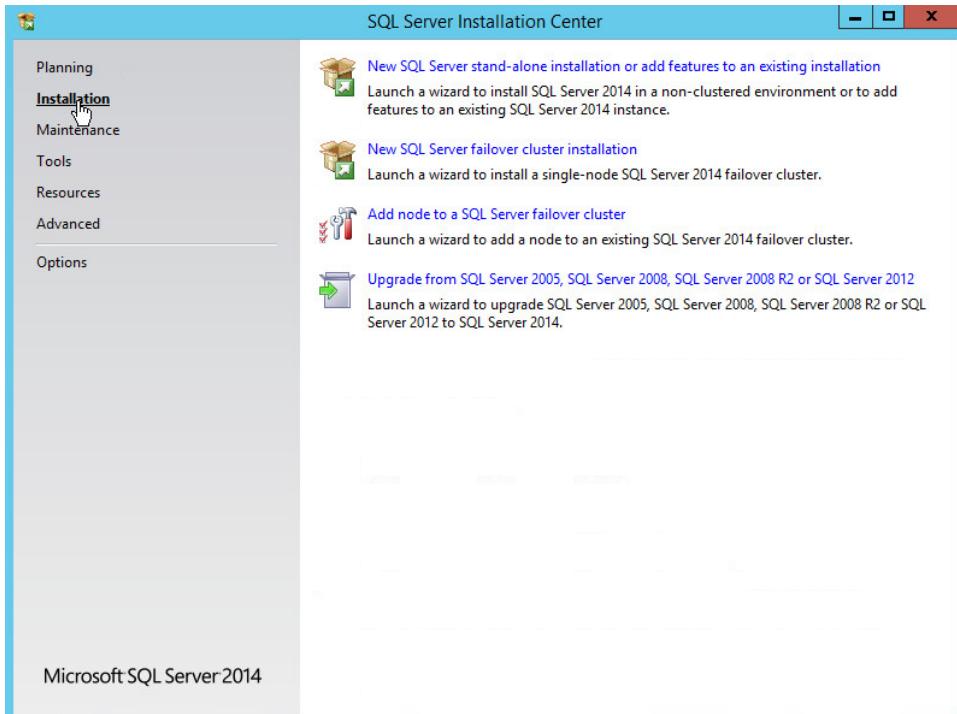
- 591 1. Acquire **SQL Server 2014 Installation Media**.
- 592 2. Locate the installation media in the machine and click on **SQL2014_x64_ENU** to launch **SQL Server Installation Center**.



594

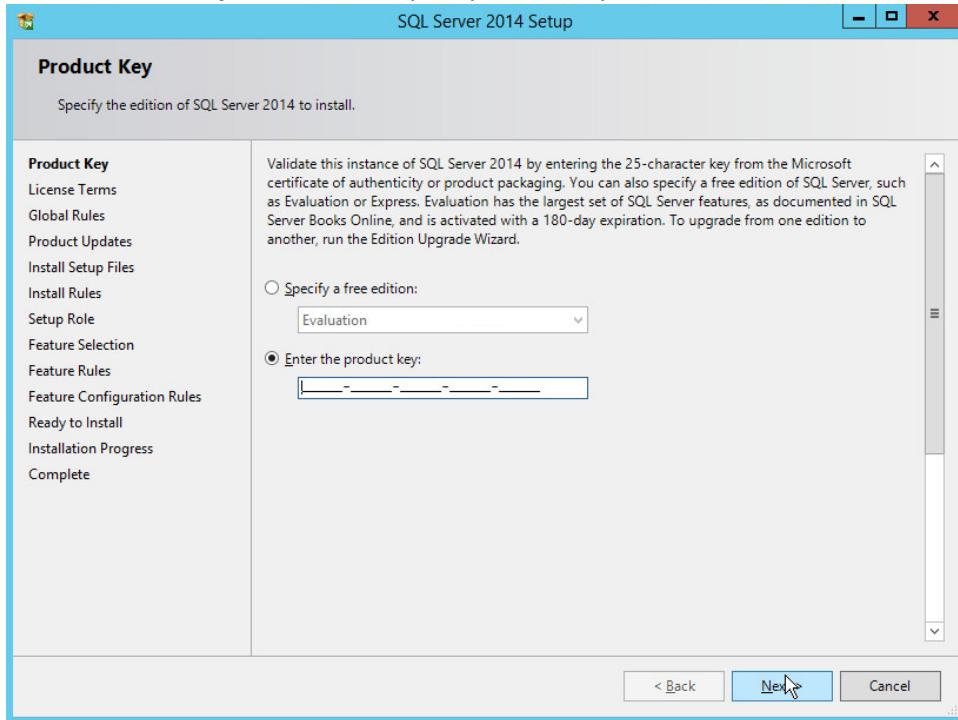
595

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

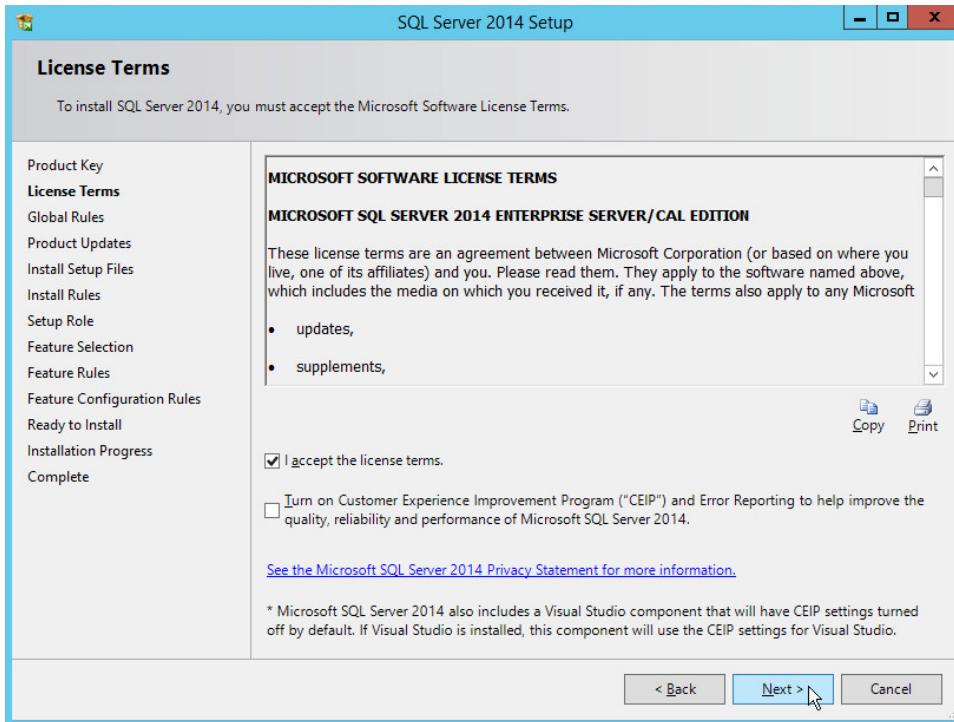


596

- 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.

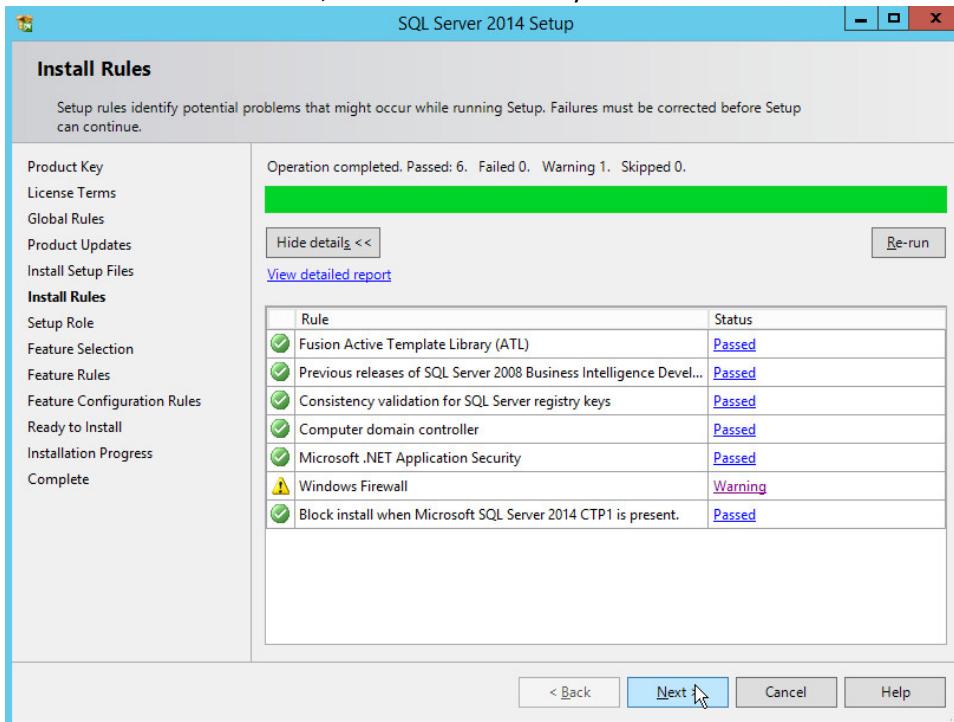


- 600 6. Click **Next**.
601 7. In the **License Terms** section, read and click **I accept the license terms**.



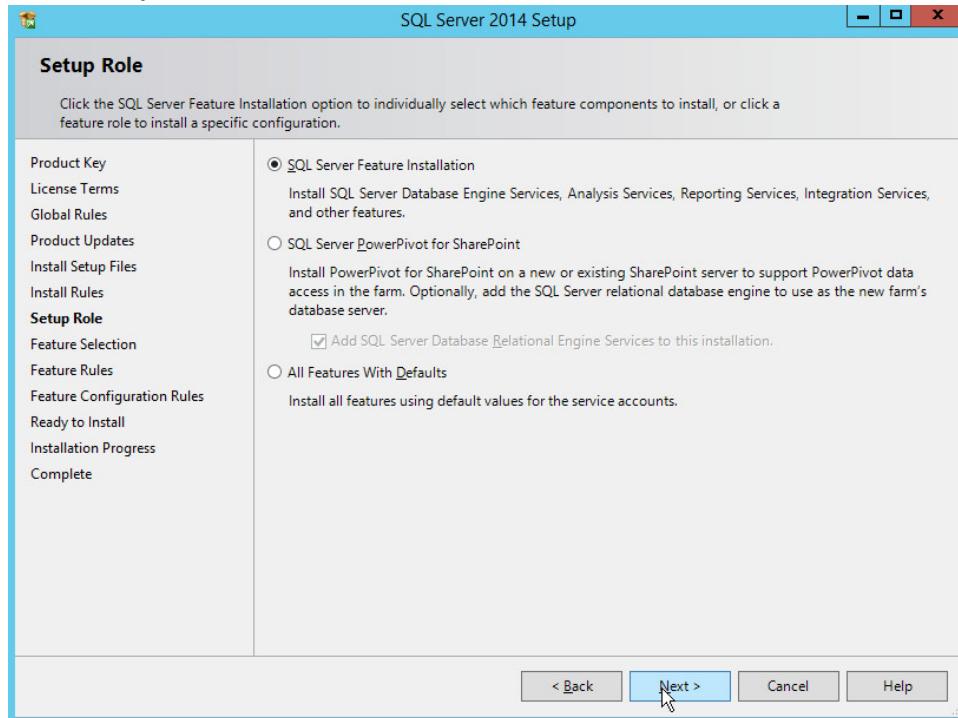
603
604
605

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

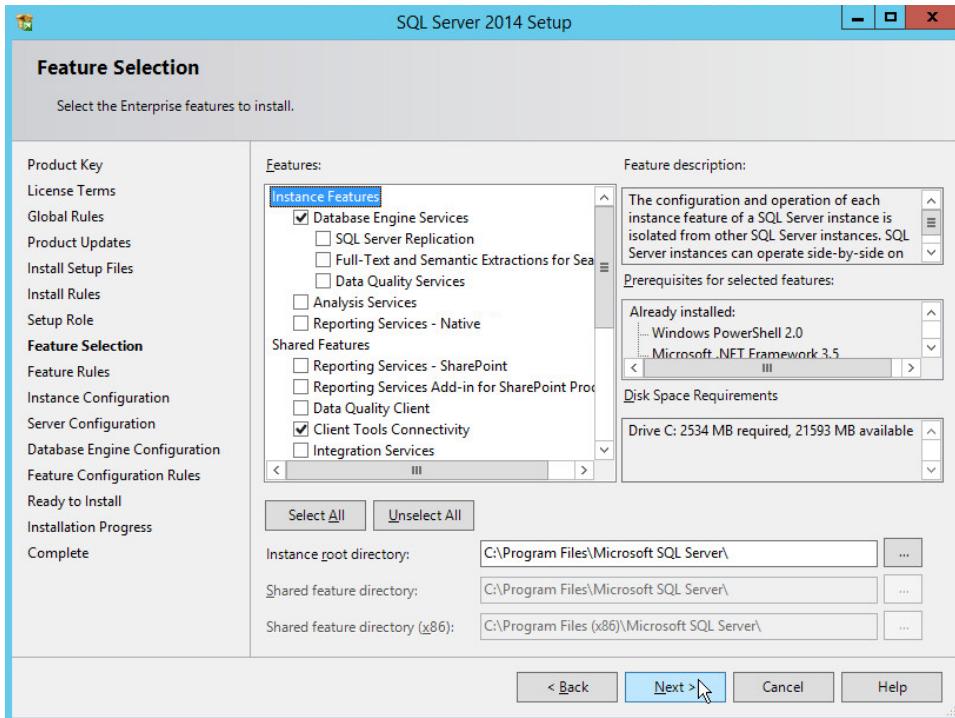


606

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



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



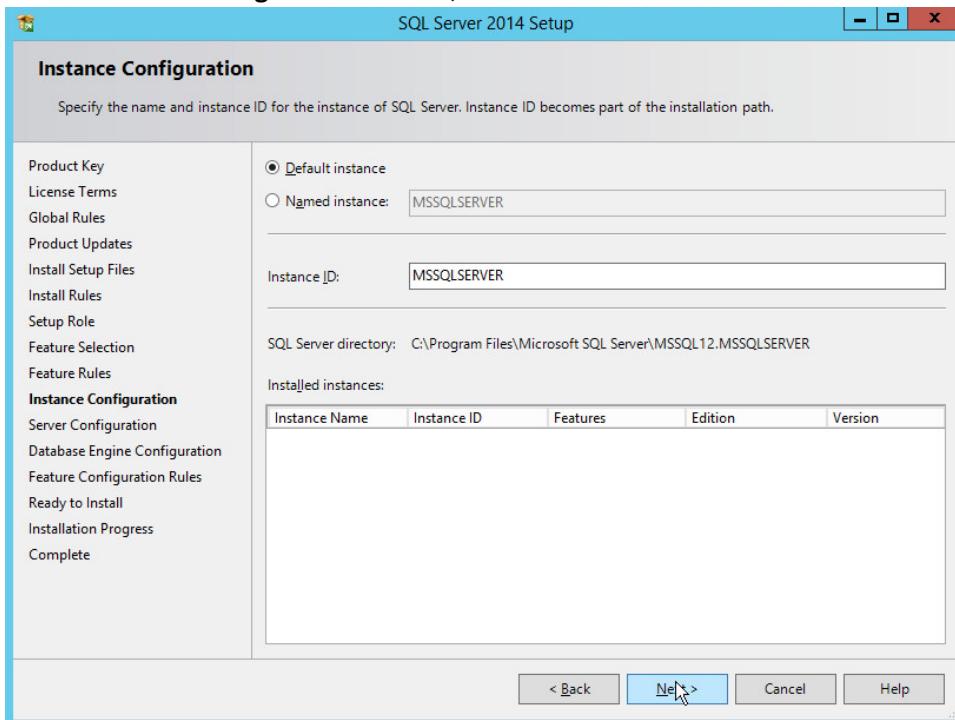
620

621

622

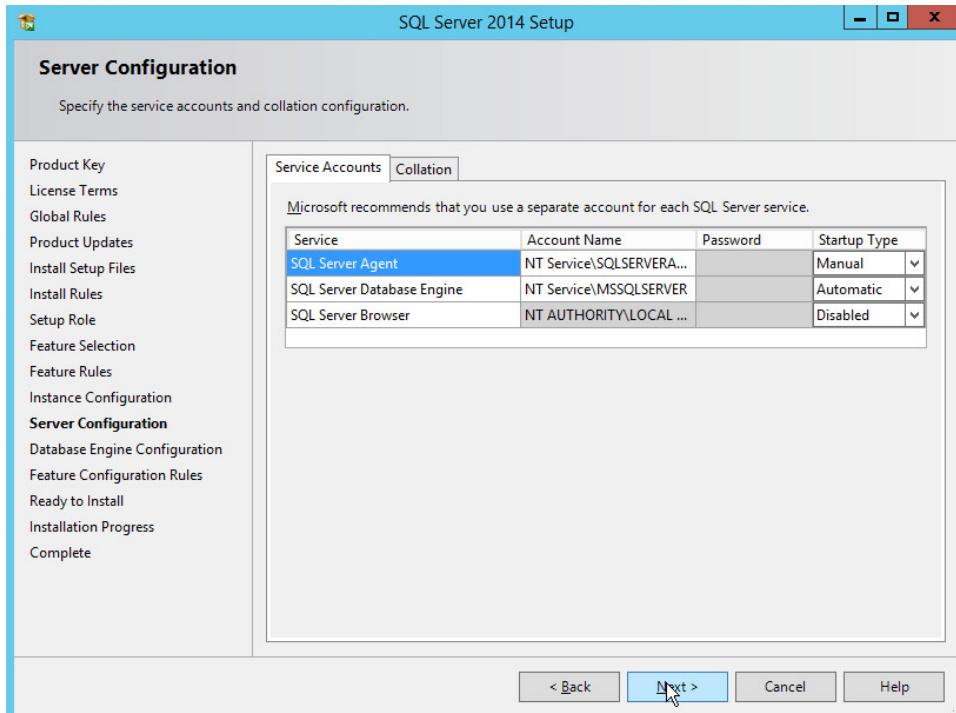
14. Click Next.

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



623

624

16. Click **Next**.

625

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

626

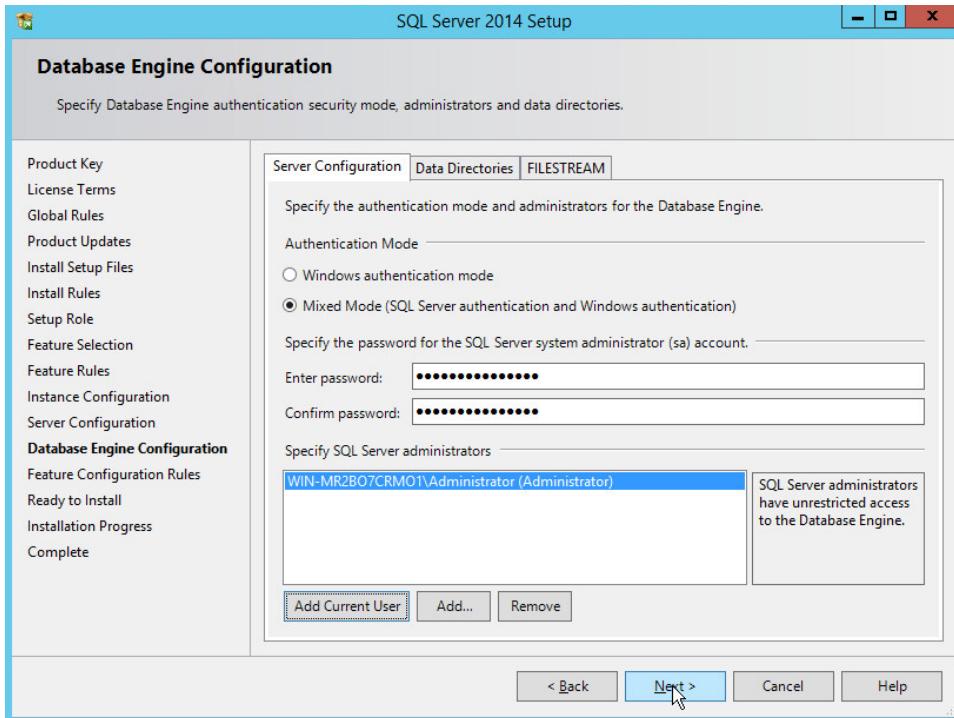
18. In the **Database Engine Configuration** section, make sure **Mixed Mode** is selected.

627

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

628

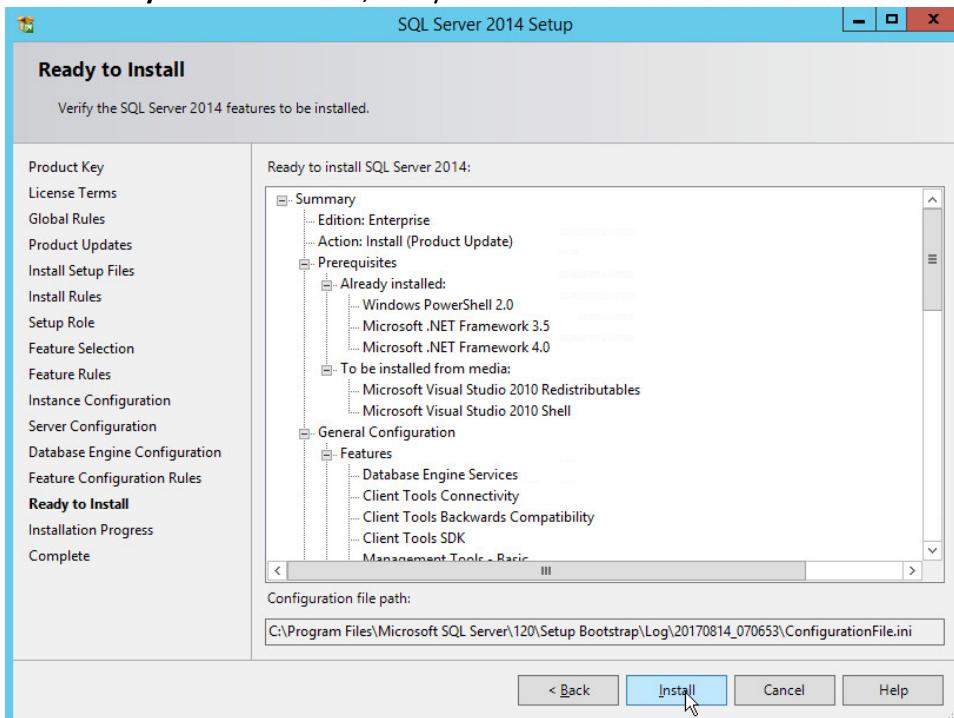
- For Domain accounts, simply type in **\$DOMAINNAME\\$USERNAME** into **Enter the object names to select** textbox.
- Click **OK**.
- For local computer accounts, click on **locations** and select the computer's name.
- Click **OK**.
- Type the username into the **Enter the object names to select** textbox.
- Once you are finished adding users, click **Next**.



637

638

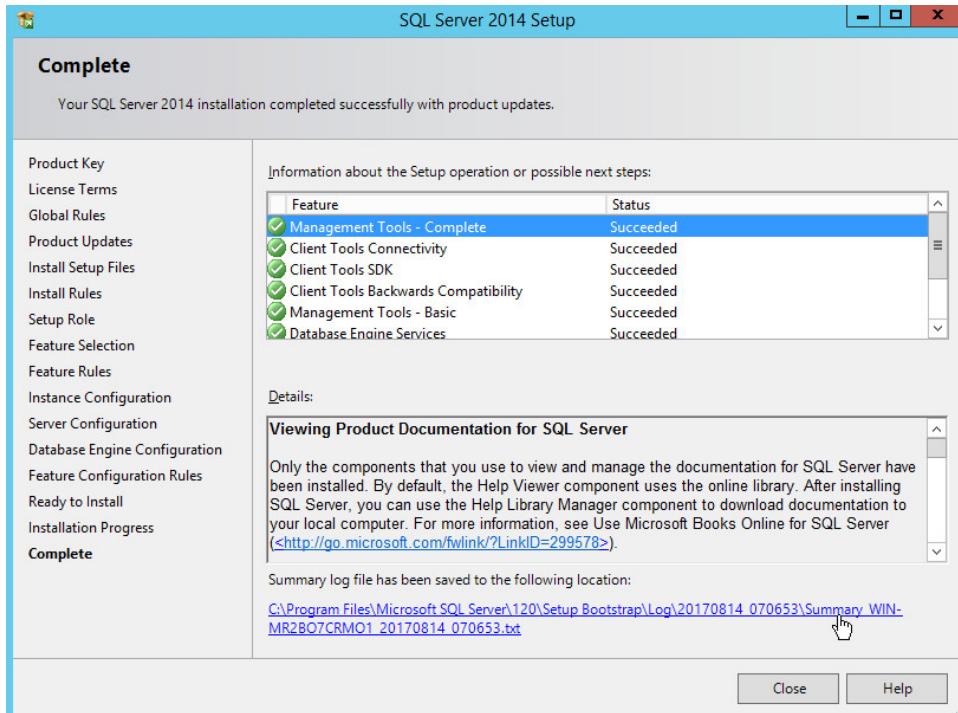
20. In the Ready to install section, verify the installation and click Install.



639

640

21. Wait for the install to finish.



641

642

22. Click **Close**.

643

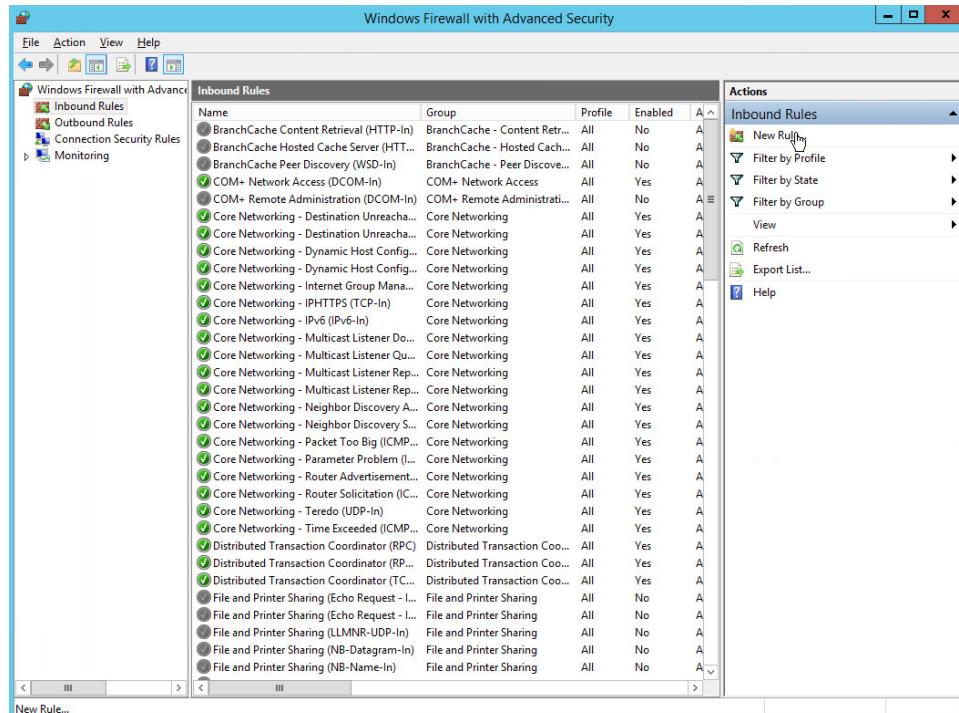
2.4.2 Open Port on Firewall

644

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

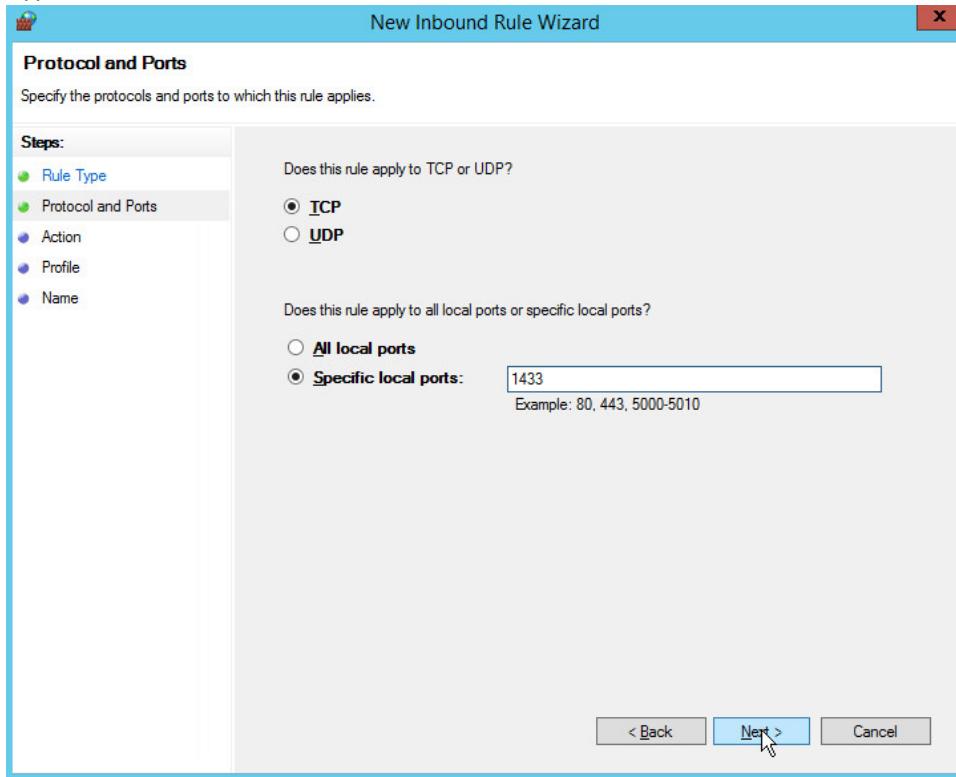
645
646

2. Click Inbound Rules.

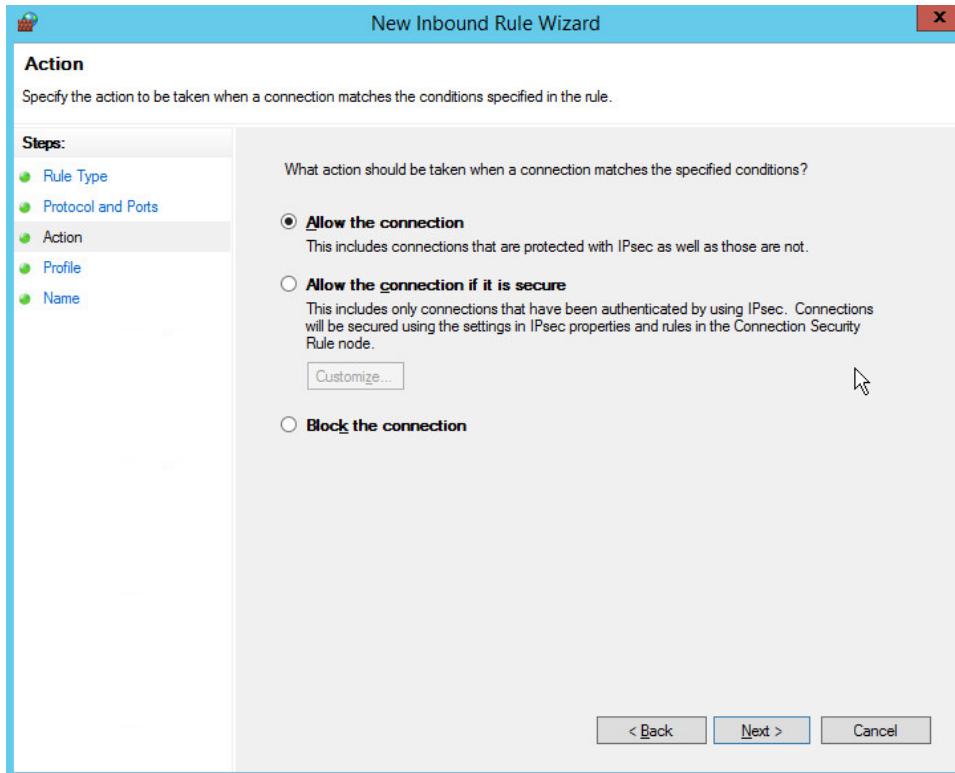
647
648

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.

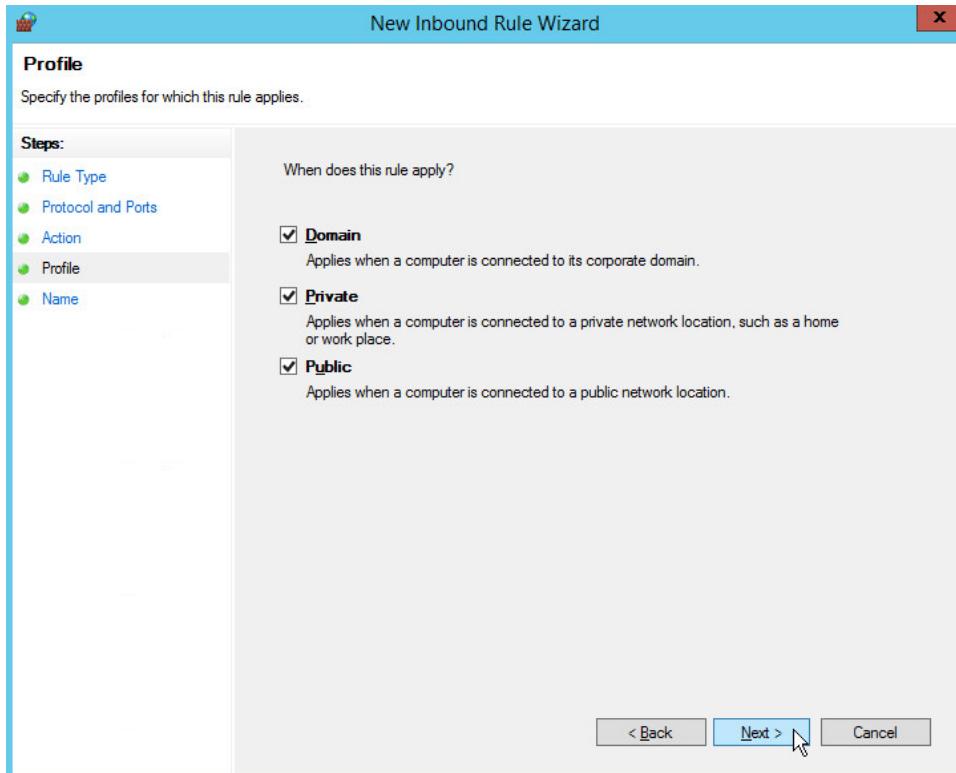


- 653
654 8. Click **Next**.
655 9. Select **Allow the connection**.



656
657
658

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



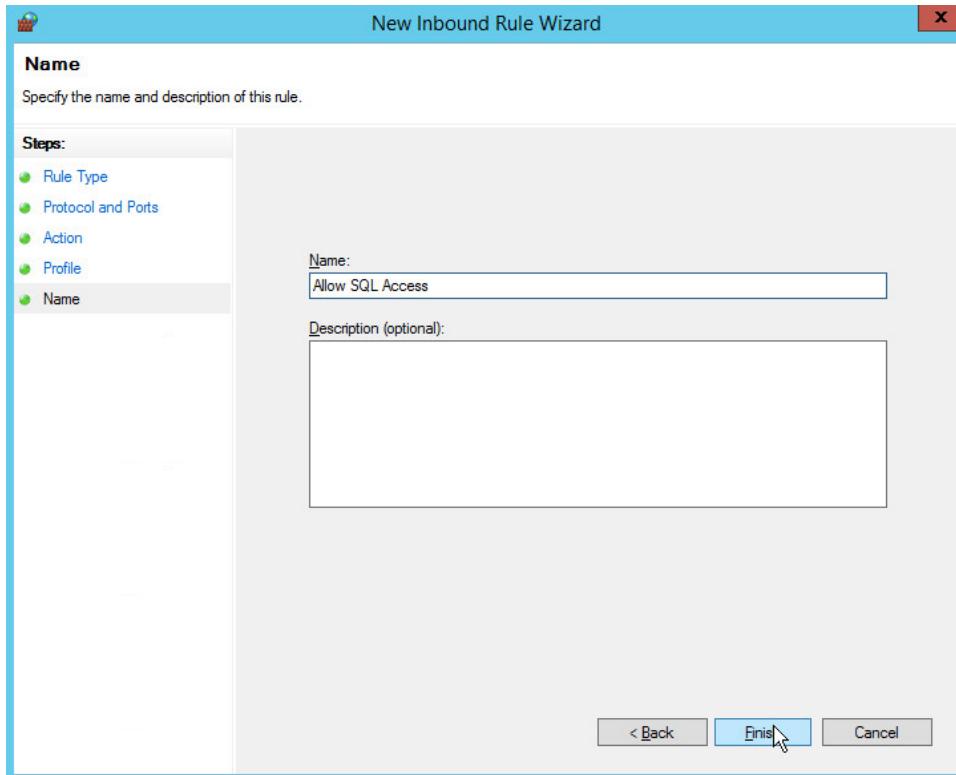
659

660

661

12. Click **Next**.

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

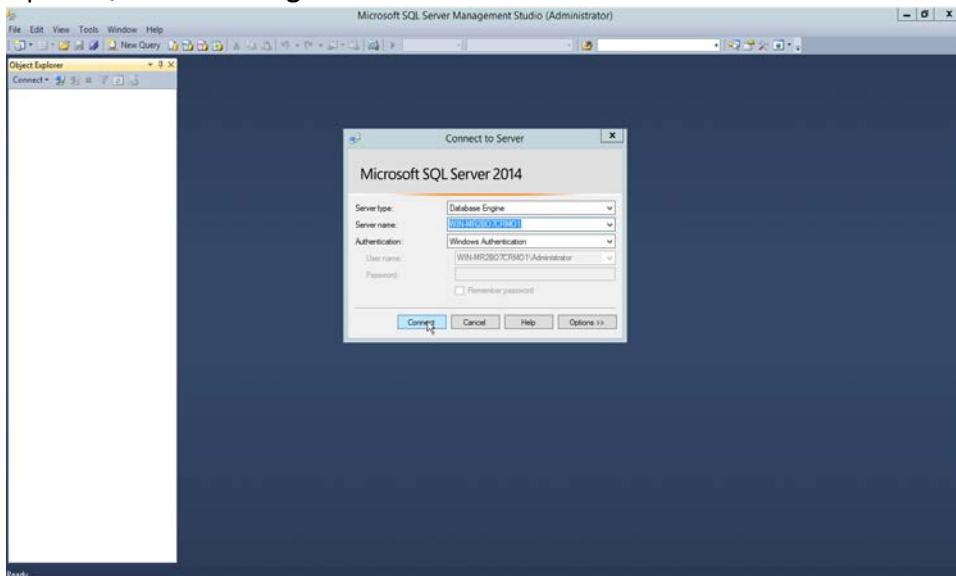


662
663

14. Click **Finish**.

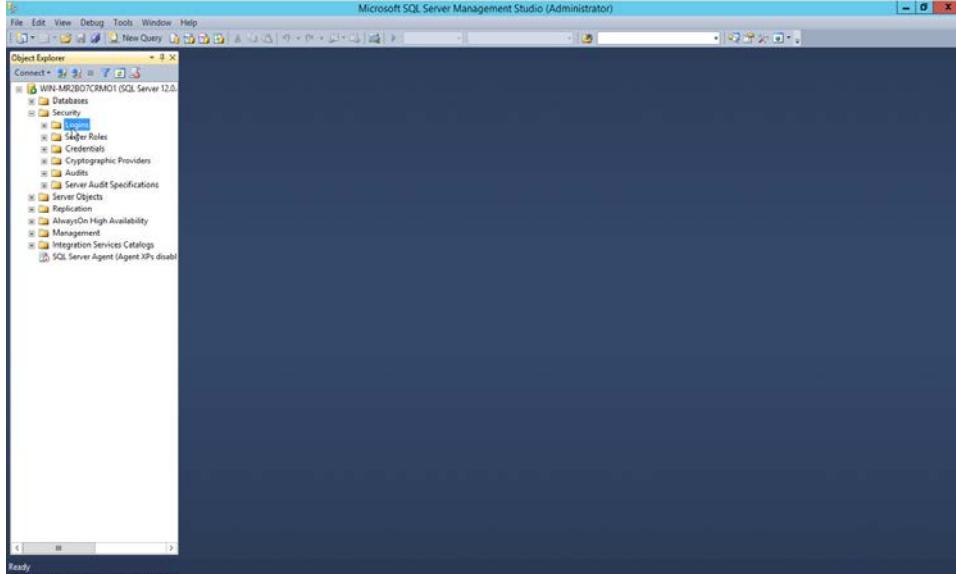
2.4.3 Add a New Login to the Database

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

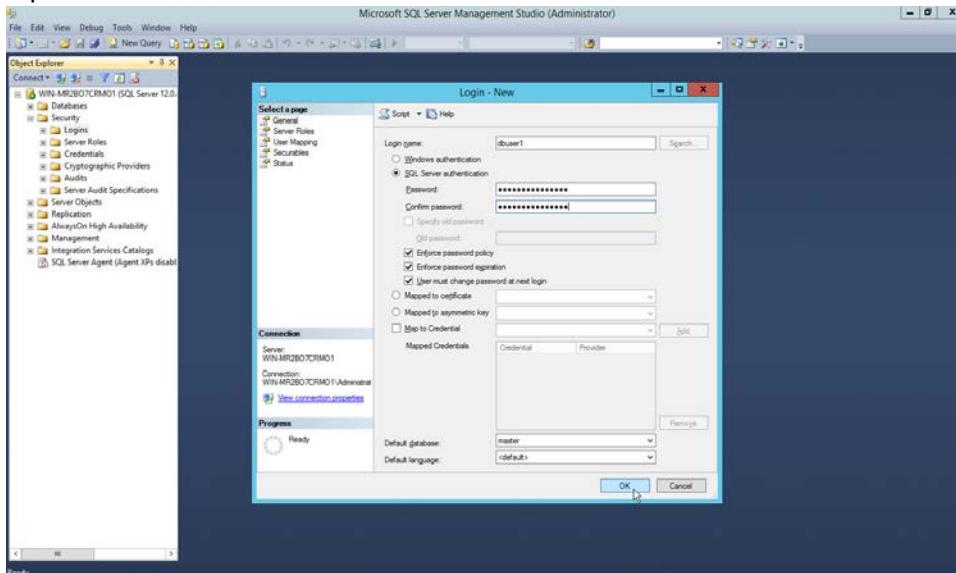


666

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



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



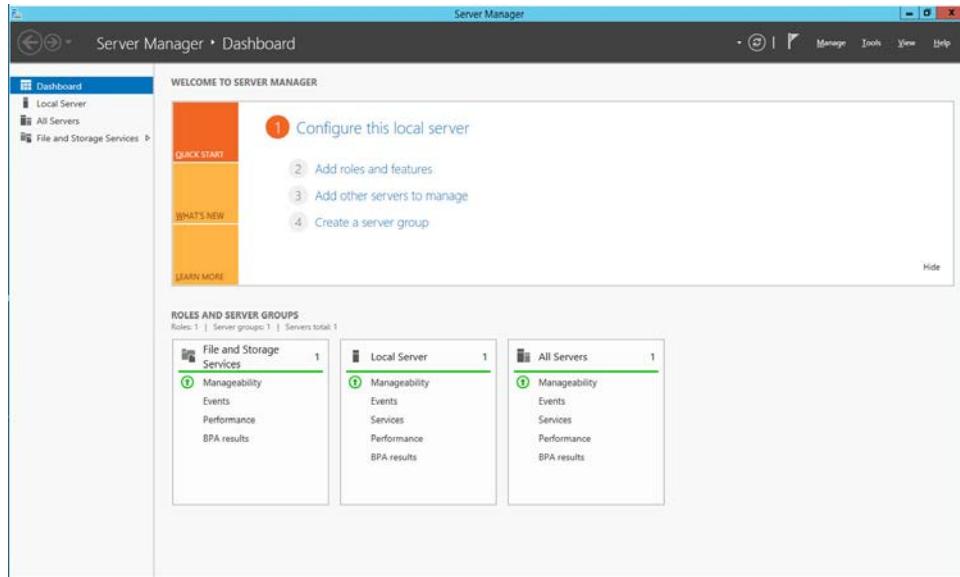
- 672
673 6. Click **OK**.

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.

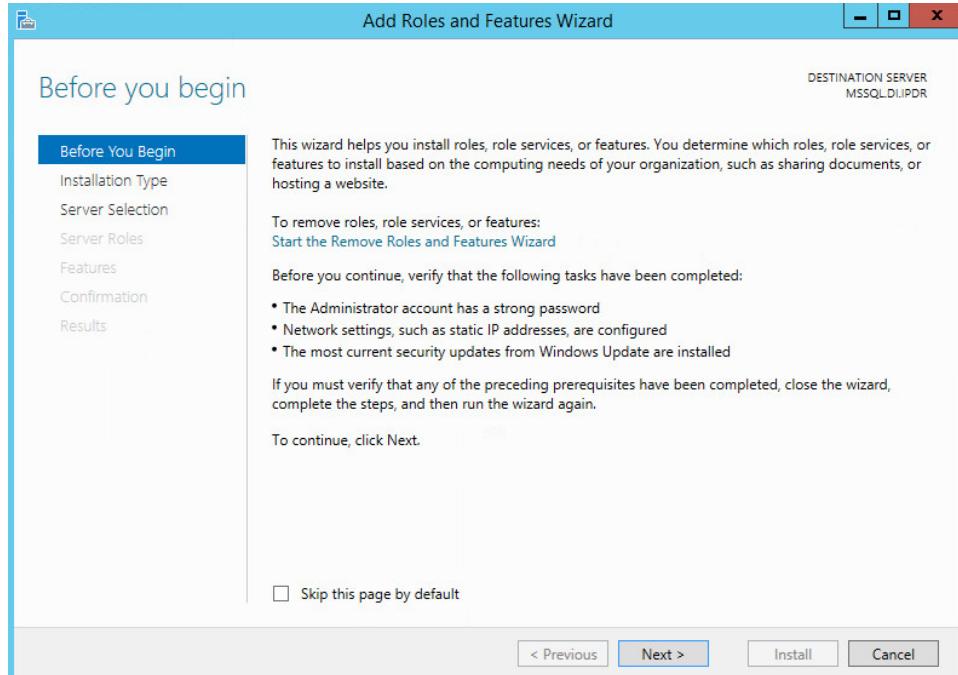
678 **2.5.1 Install IIS**

679 1. Open Server Manager.



680

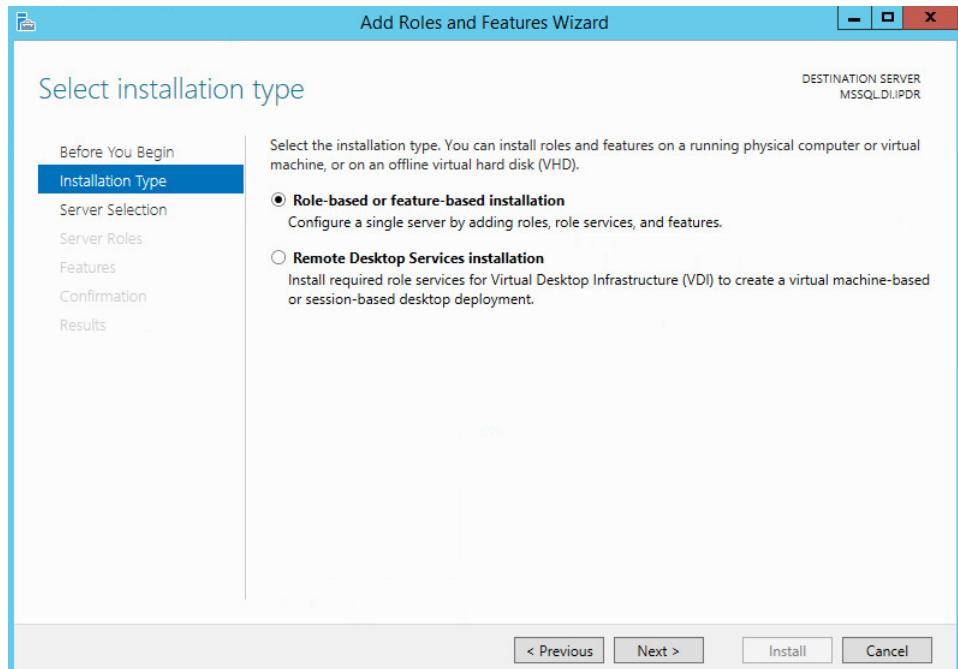
681

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

682

3. Click **Next**.

683

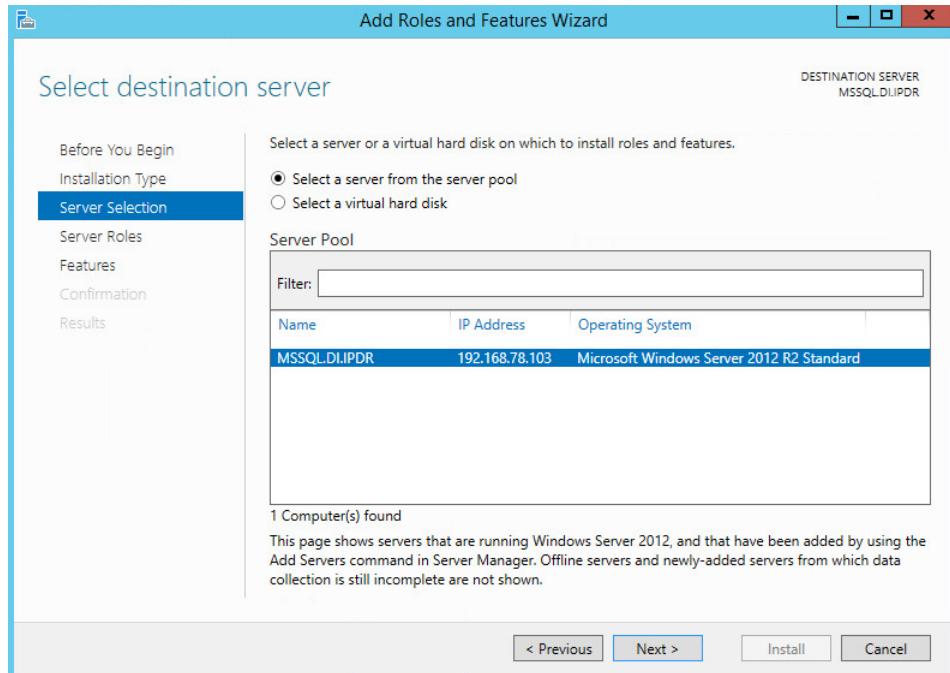
4. Select **Role-based or feature-based installation**.

685

5. Click **Next**.

687

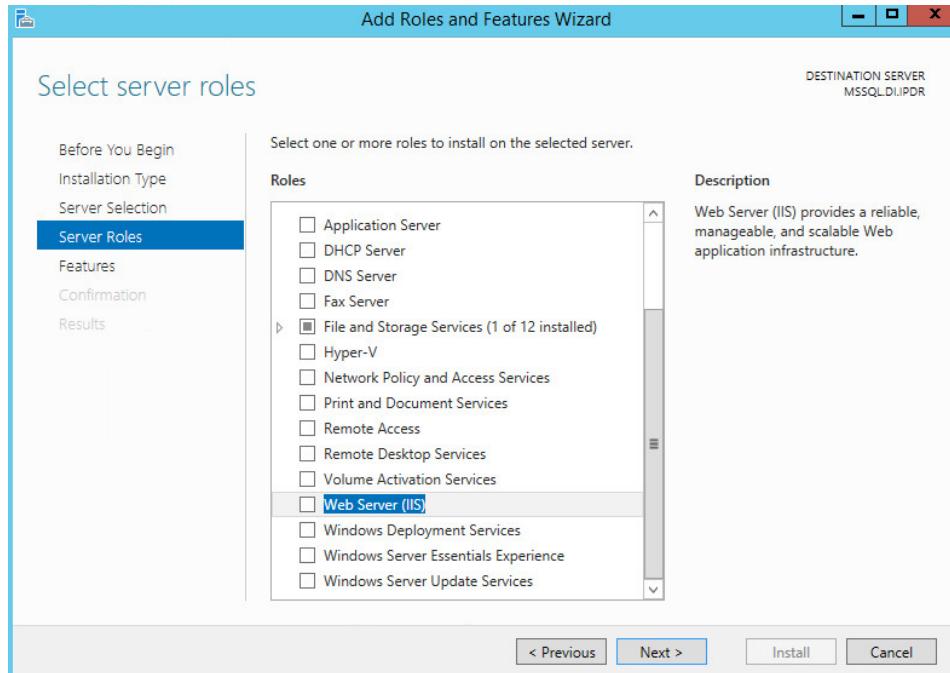
6. Select **MSSQL** (or the correct Windows Server name) from the list.



688

689

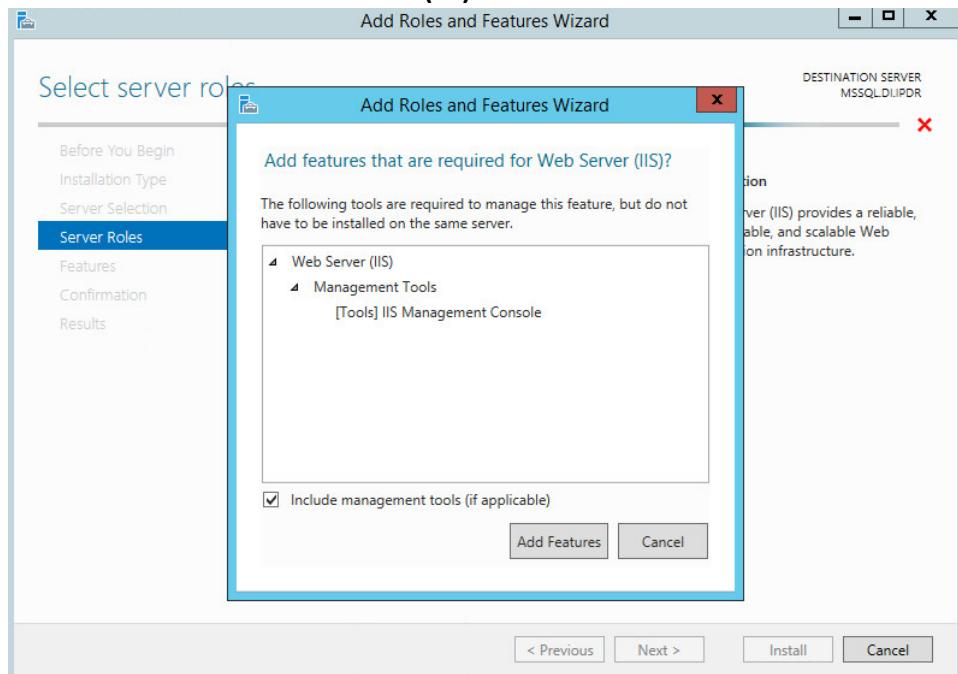
7. Click **Next**.



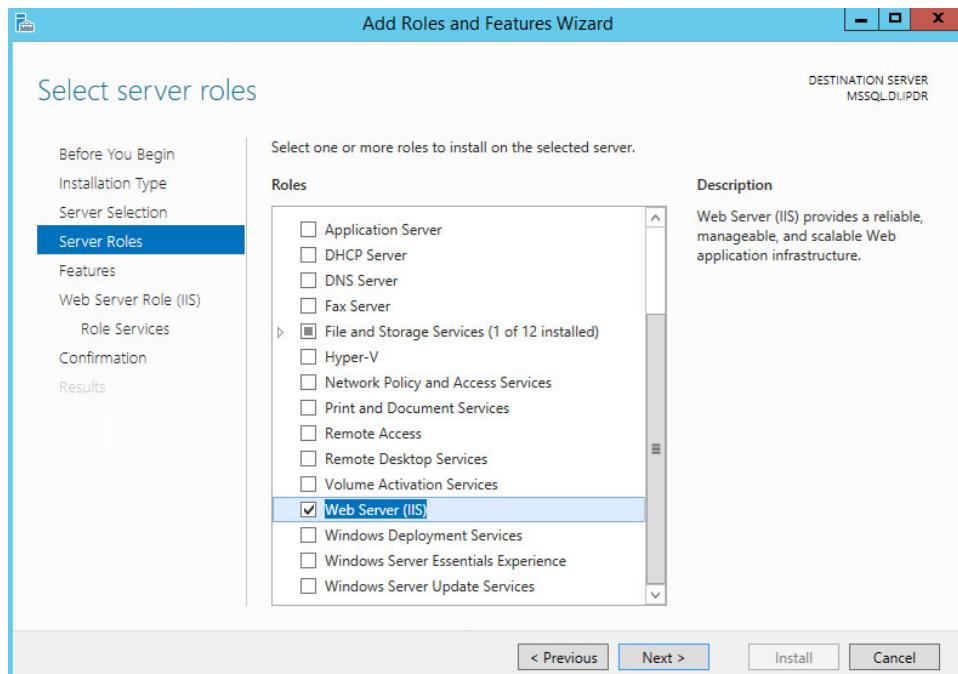
690

691

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

692
693

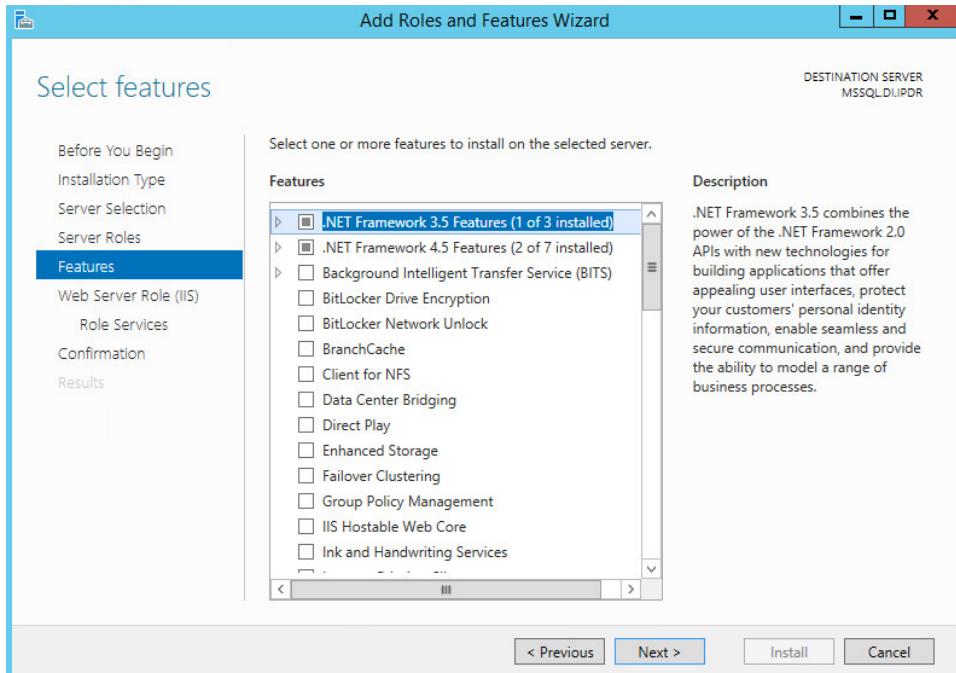
9. Click **Add Features**.

694
695

10. Click **Next**.

696

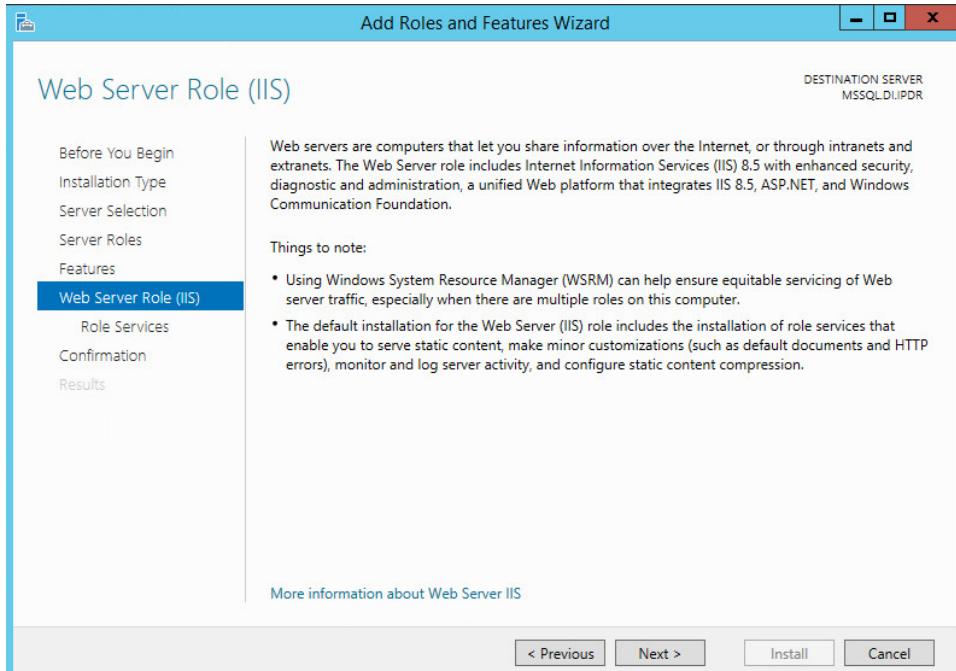
11. Ensure that all desired features are selected.



697

698

12. Click Next.

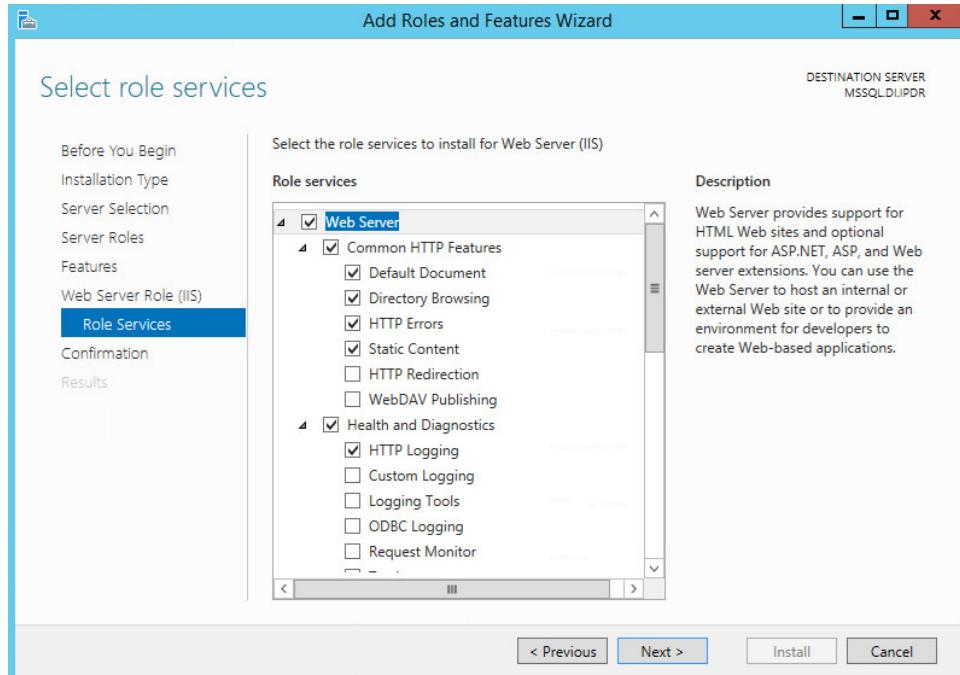


699

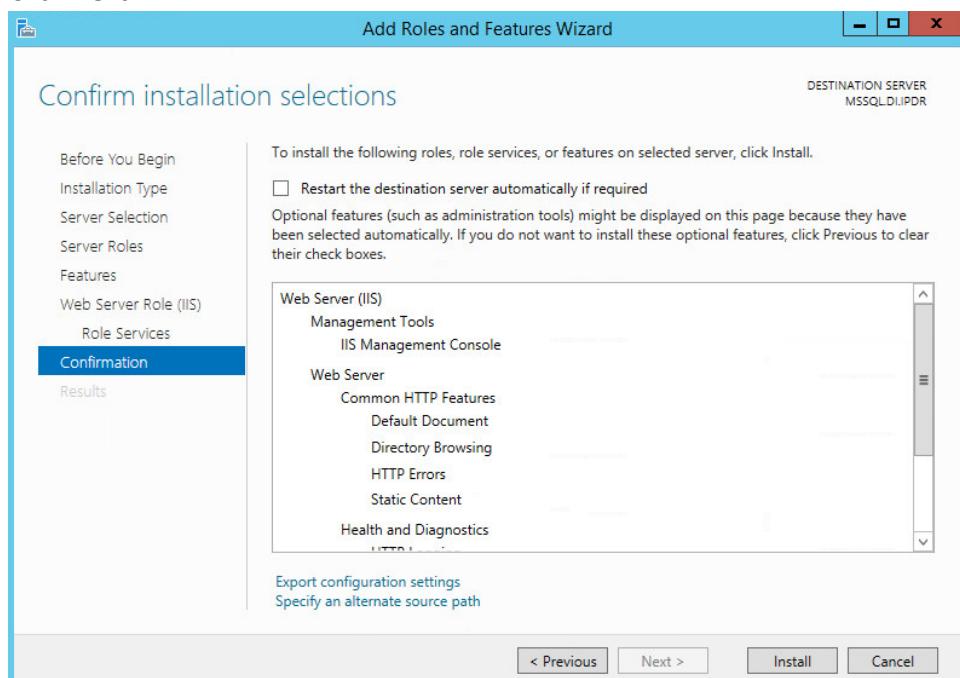
700

13. Click Next.

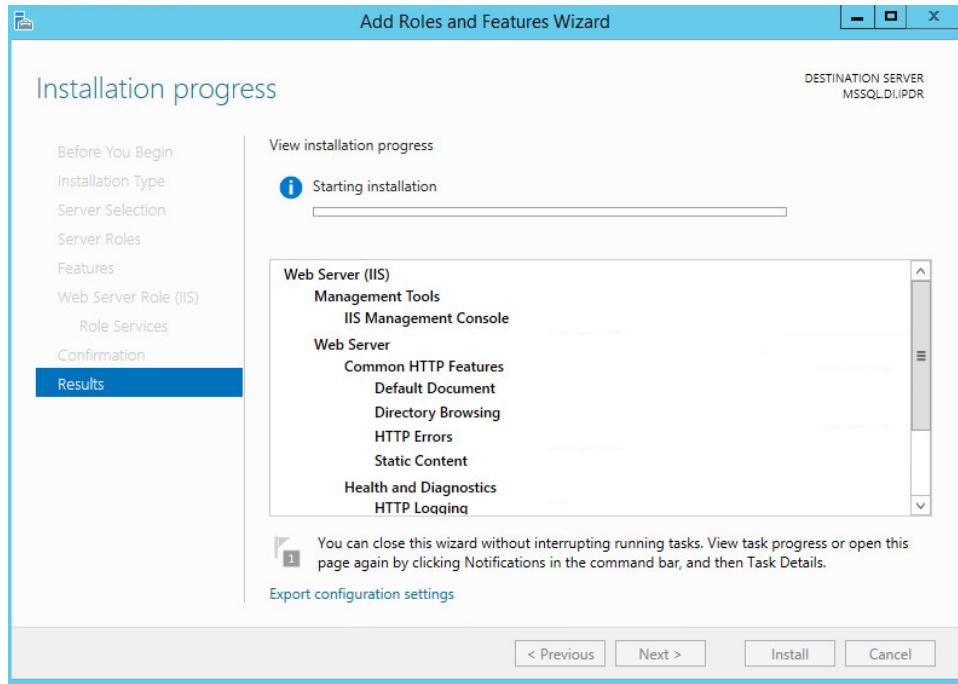
- 701 14. Ensure that **Default Document**, **Directory Browsing**, **HTTP Errors**, **Static Content**, **HTTP Logging**,
 702 and any other desired Role services are selected.



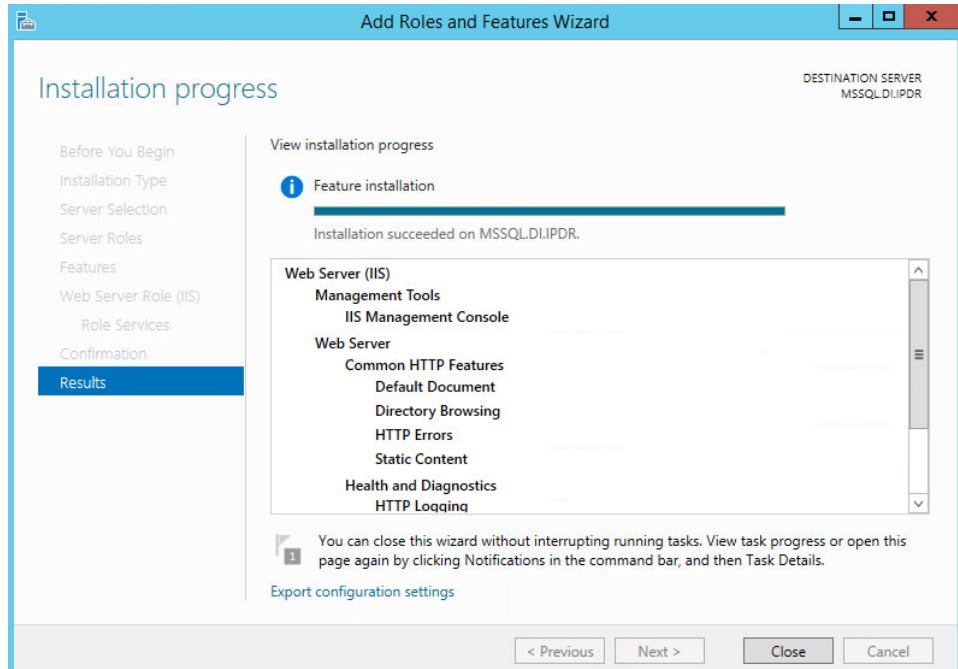
- 703
 704 15. Click **Next**.



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

707
708

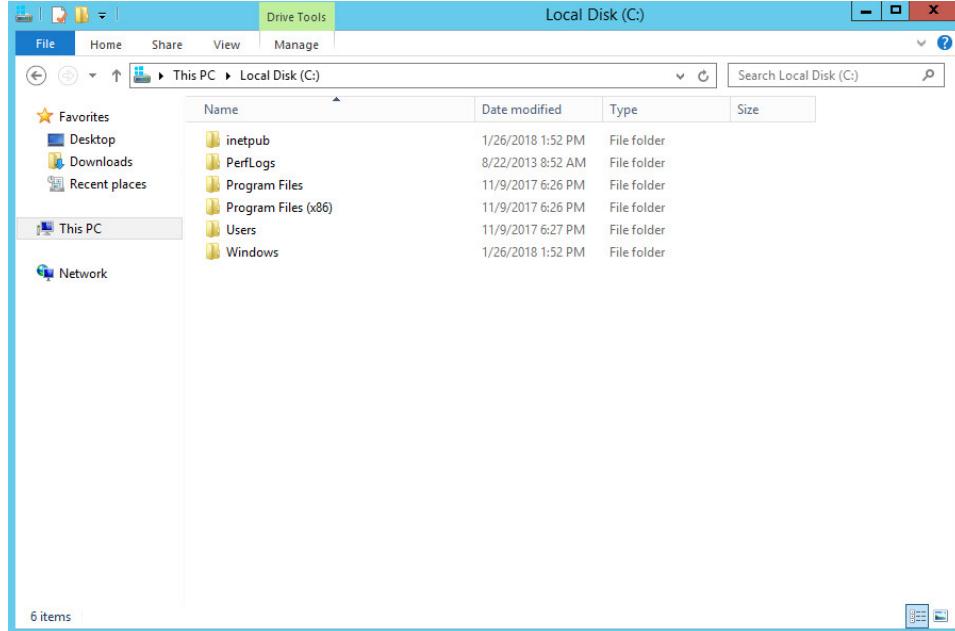
17. Wait for the installation to complete.

709
710

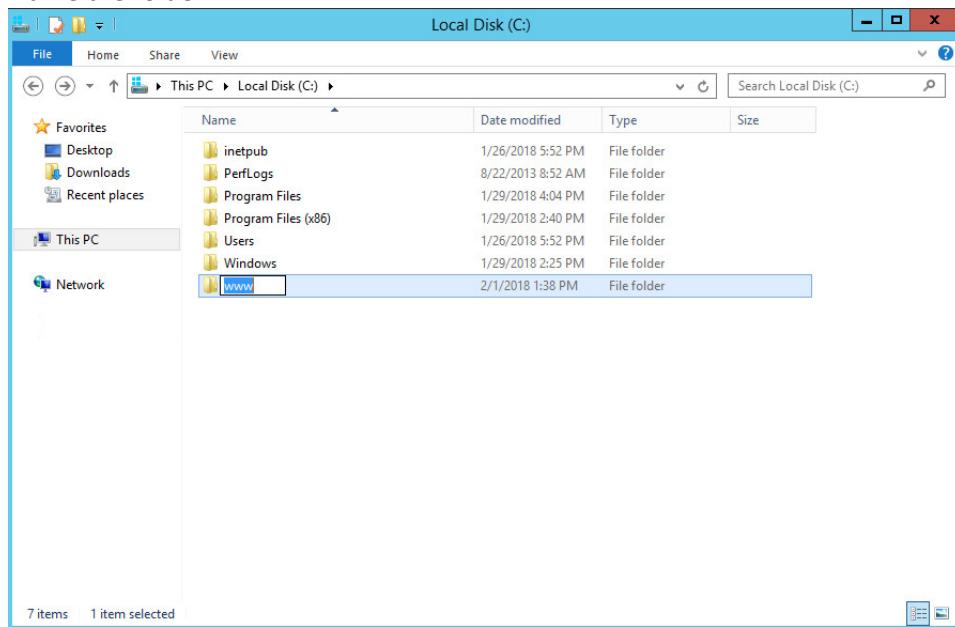
18. Click **Close**.

711 2.5.2 IIS Configuration

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

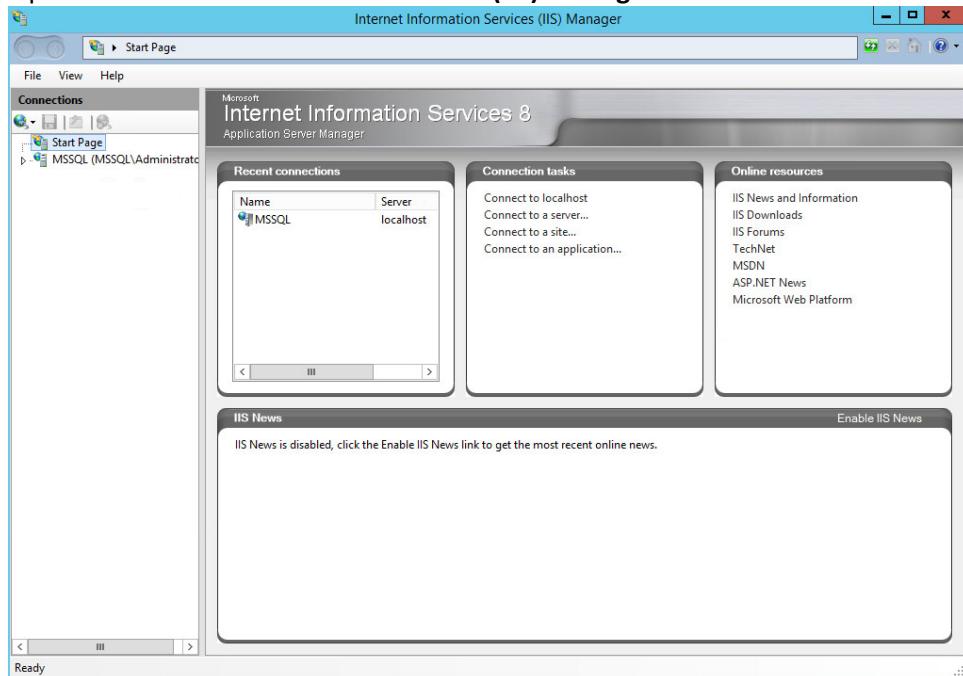


- 713
714 2. Right-click, and select Create Folder.
715 3. Name the folder www.



717

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

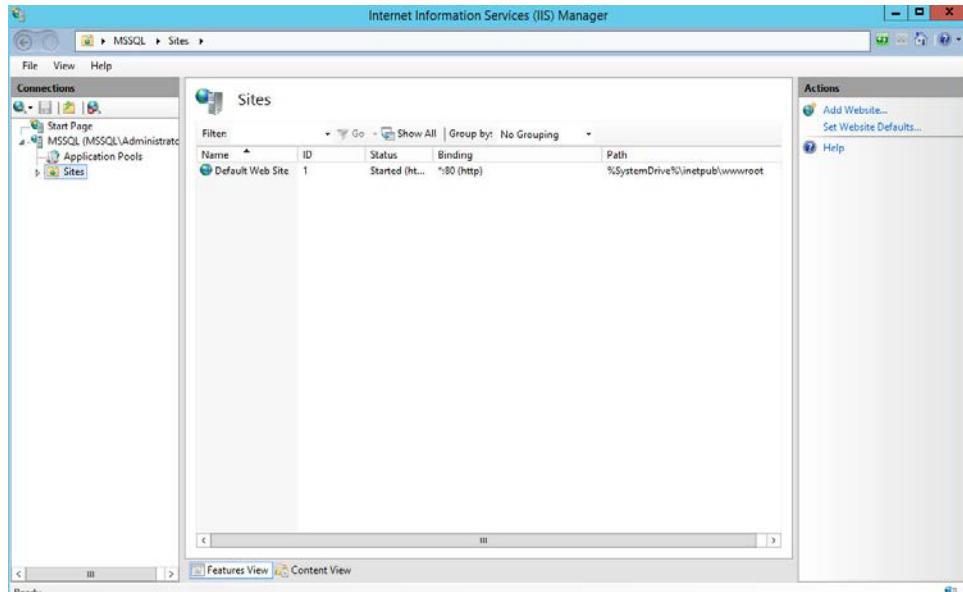


718

5. Click the arrow next to **MSSQL** (or the chosen name of the server).

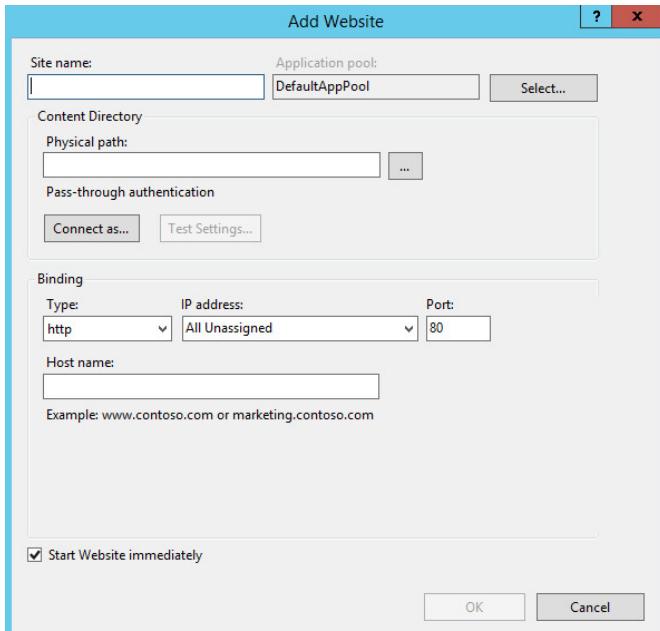
719

6. Click **Sites**.

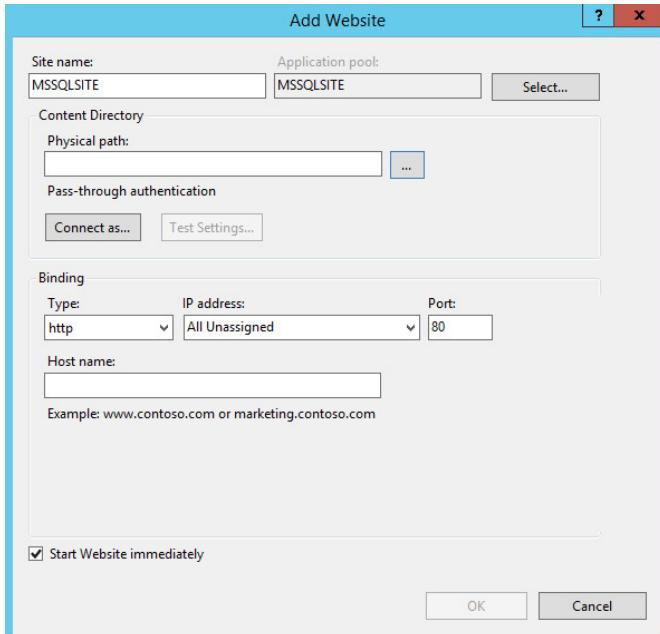


720

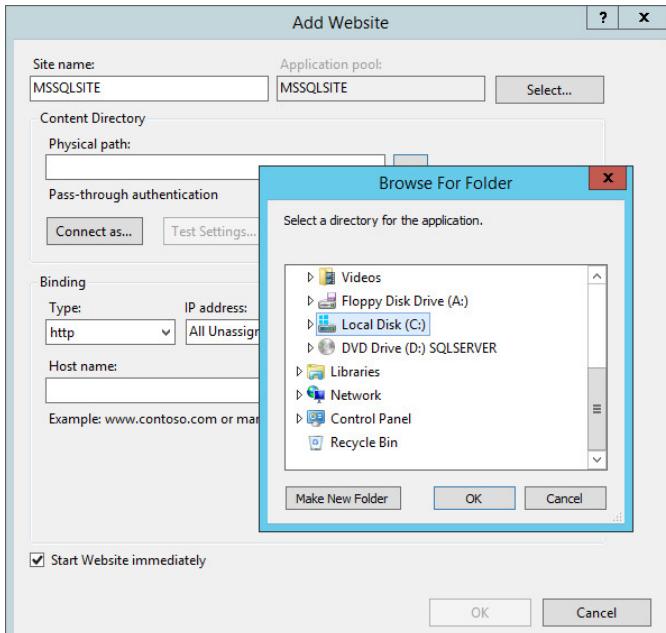
7. Click **Add Website....**

723
724

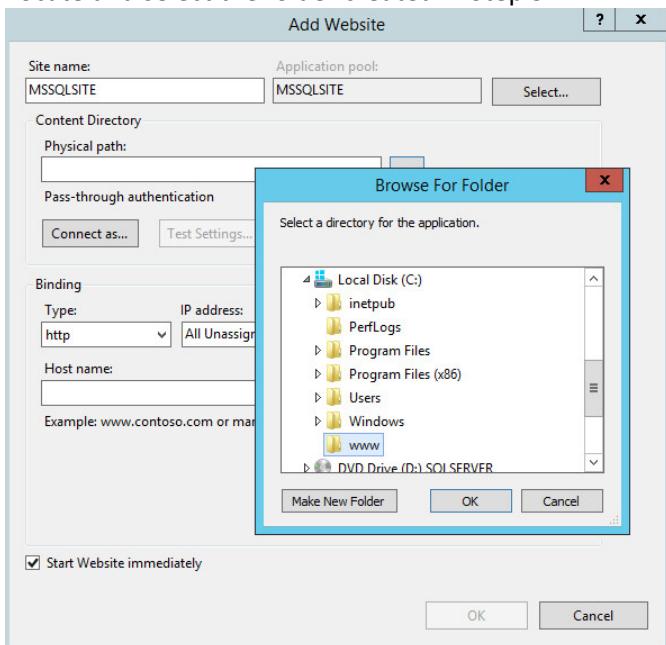
8. Enter the desired site name.

725
726

9. Click ... under Physical path:.

727
728

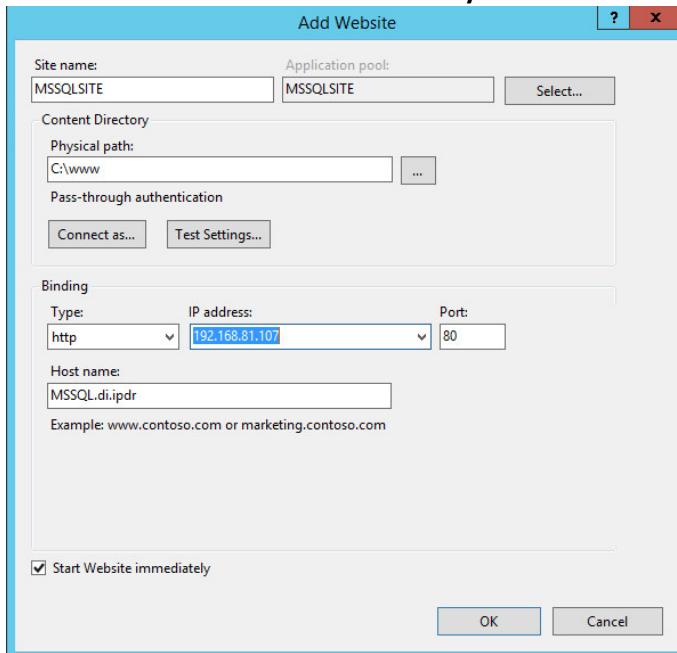
10. Locate and select the folder created in Step 3.

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

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 monitoring Active Directory environments. This installation requires both a copy of SQL Server Express as well as the **Semperis Wizard**. See the **Semperis DS Protector v2.5 Technical Requirements** document for specifics on the requirements. For a Windows Server 2012 R2 installation, simply meet the following requirements:

743

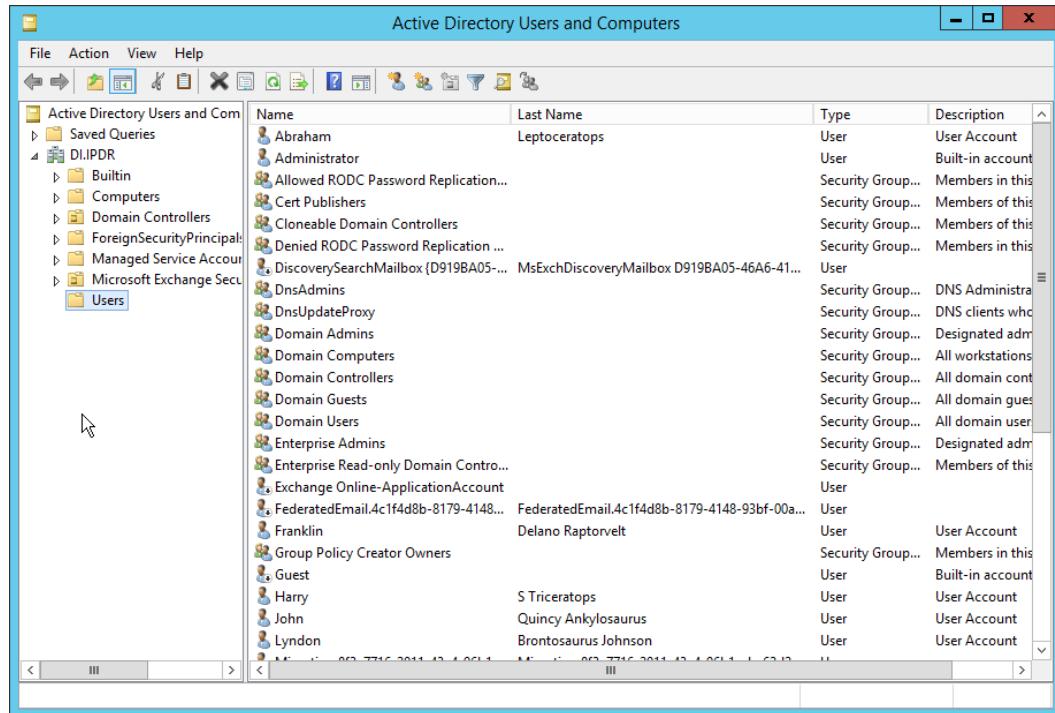
- .NET Framework Version 3.5 SP1
- .NET Framework Version 4.5.2 or later
- Joined to the Active Directory Domain it is protecting
- Either the installer for SQL Express Advanced or connection information and credentials for a full version of Microsoft SQL (MSSQL)

748

2.6.1 Configure Active Directory for Semperis DSP

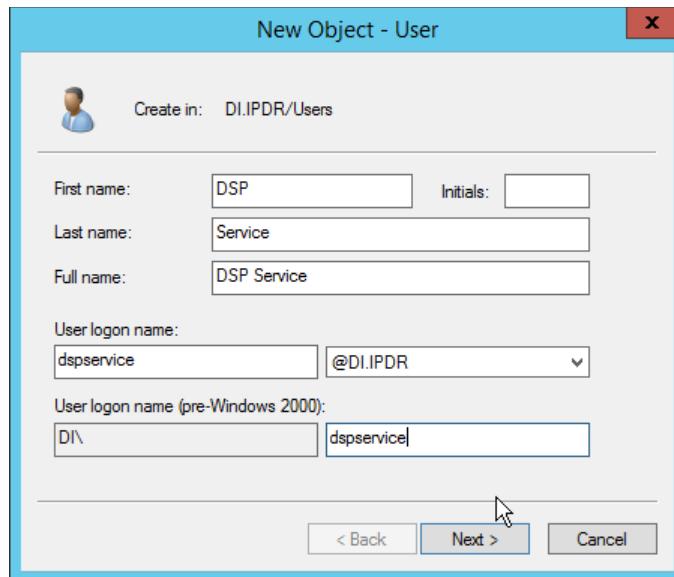
749

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



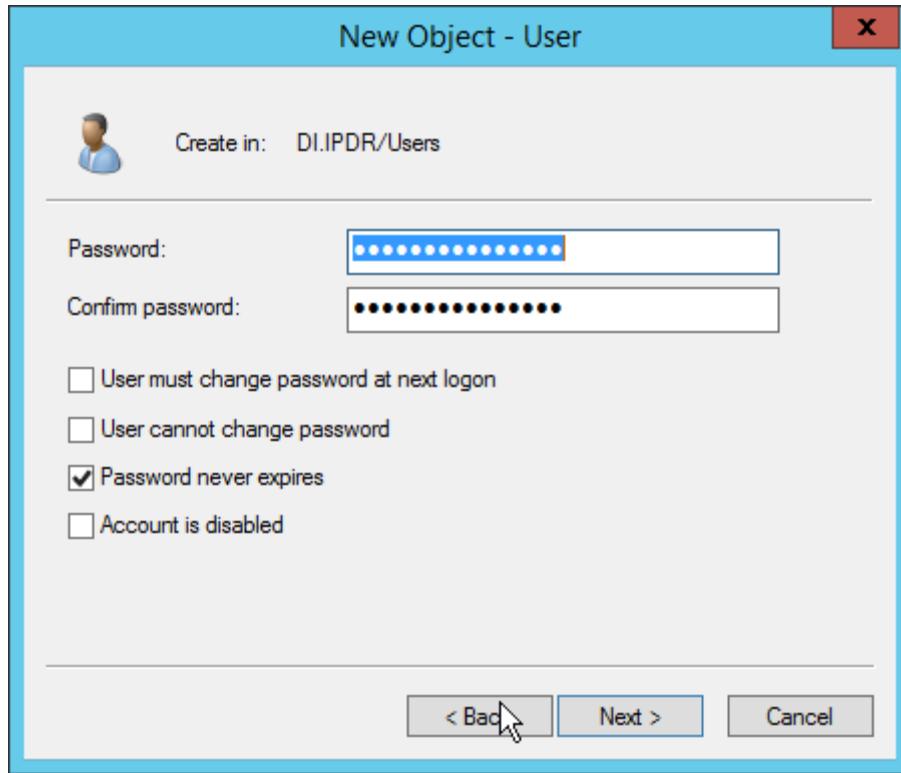
750
751
752

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



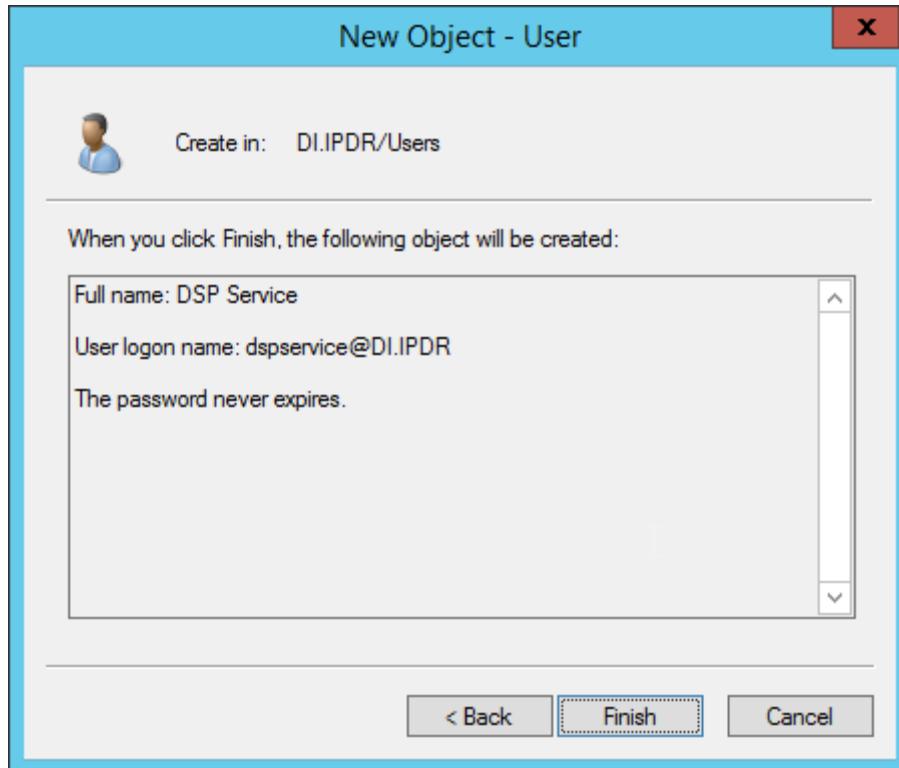
753
754
755
756

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



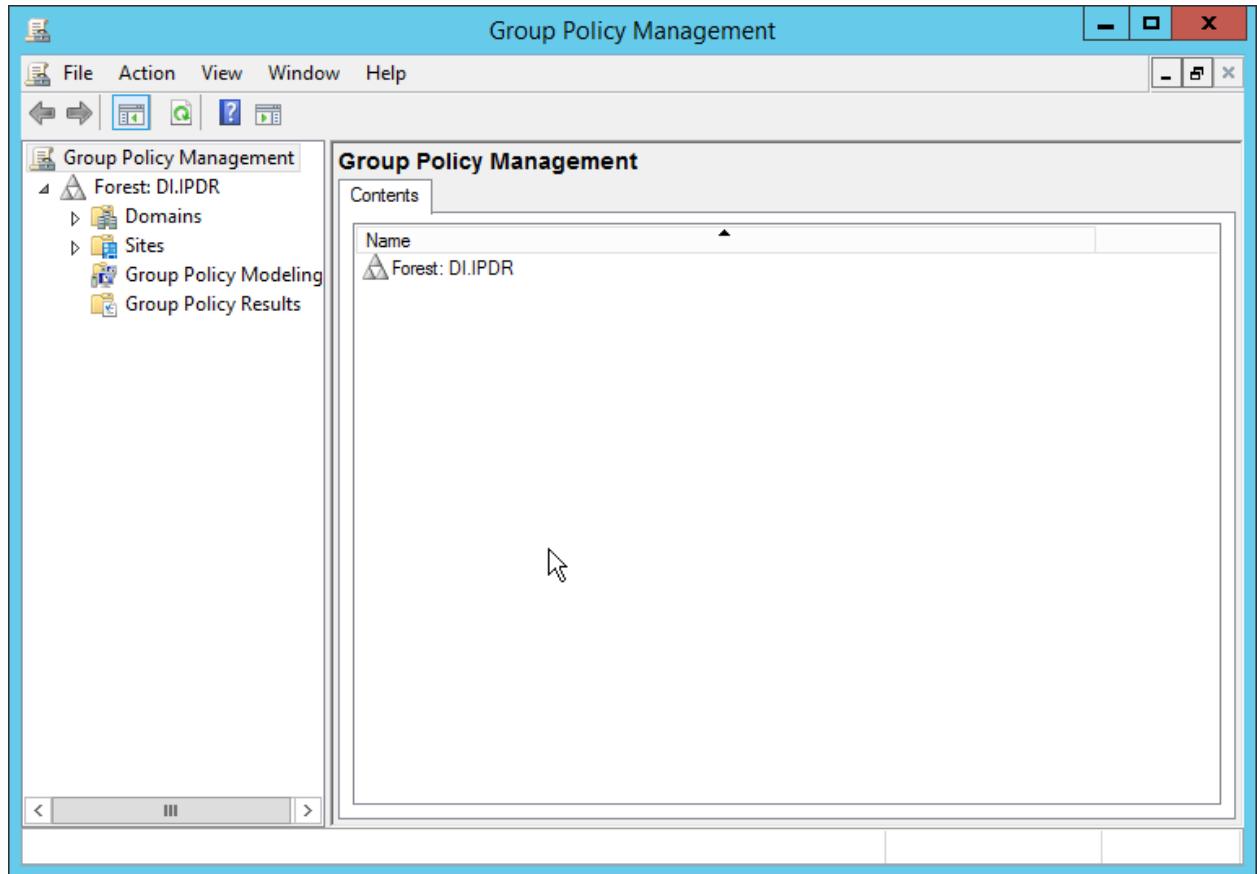
757
758

7. Click **Next**.



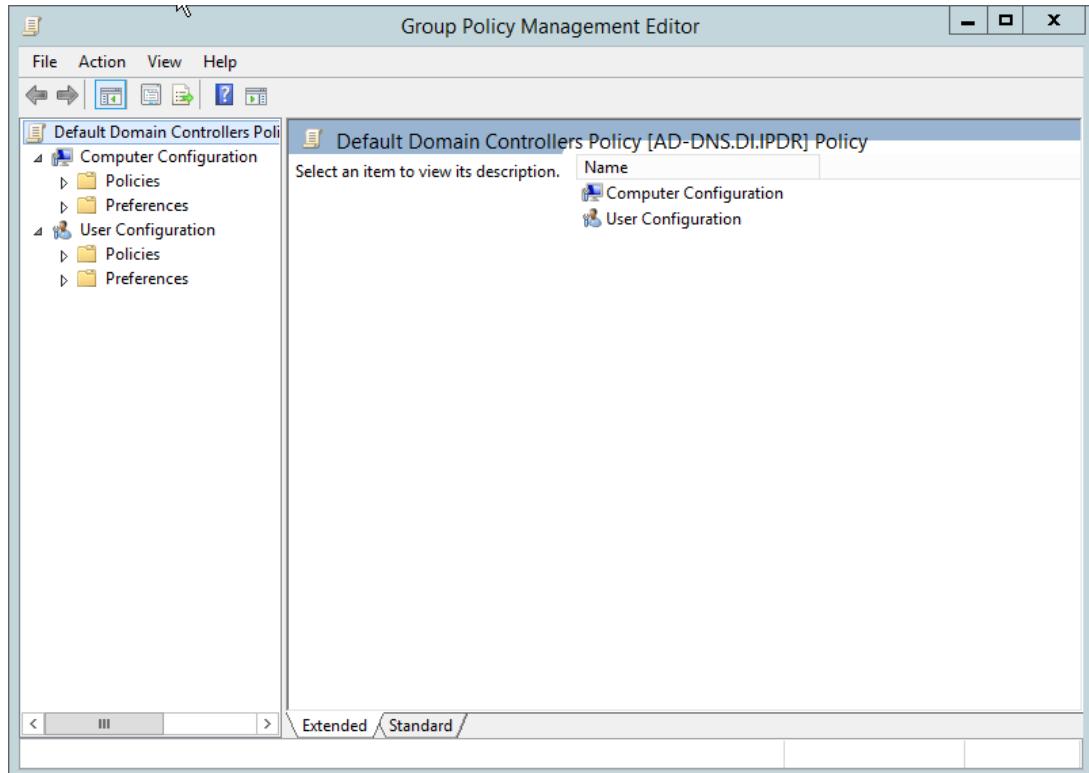
759
760
761

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



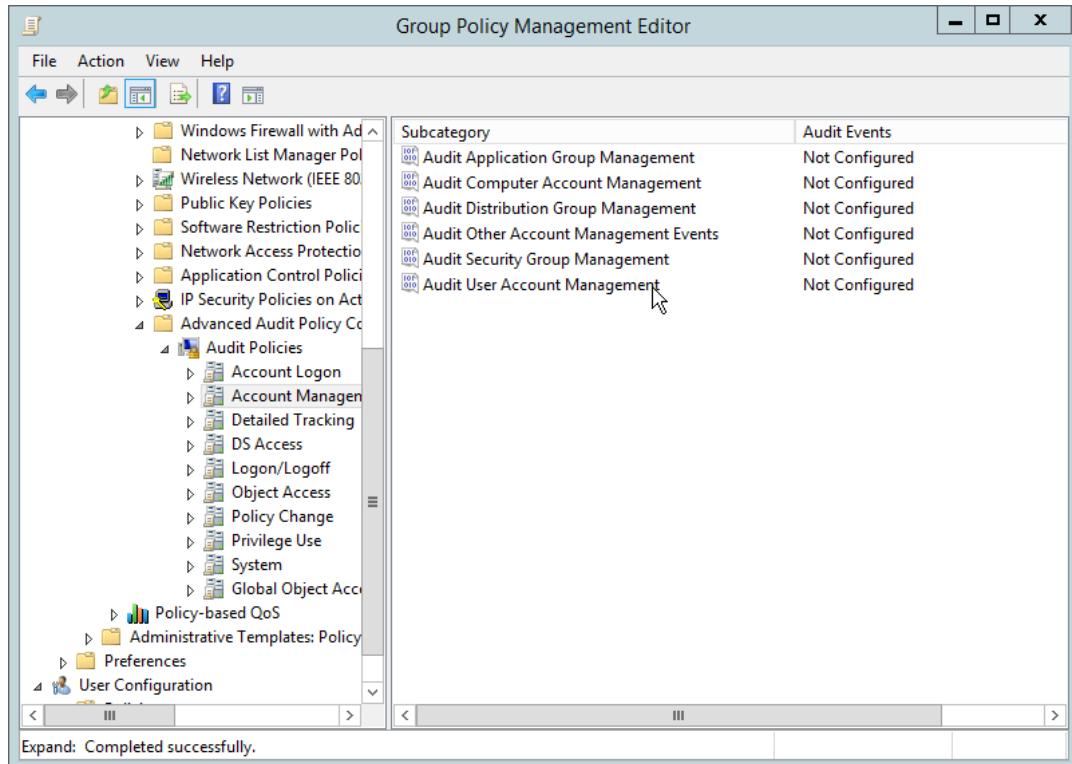
762
763
764

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



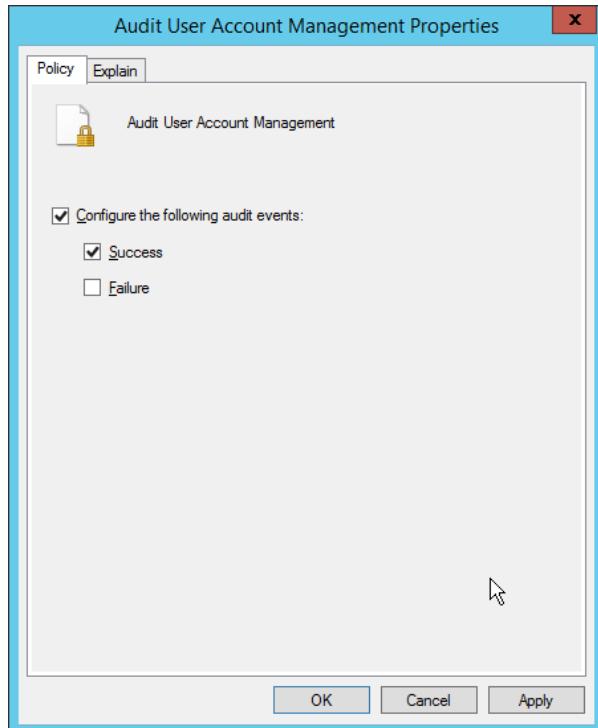
765
766
767

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

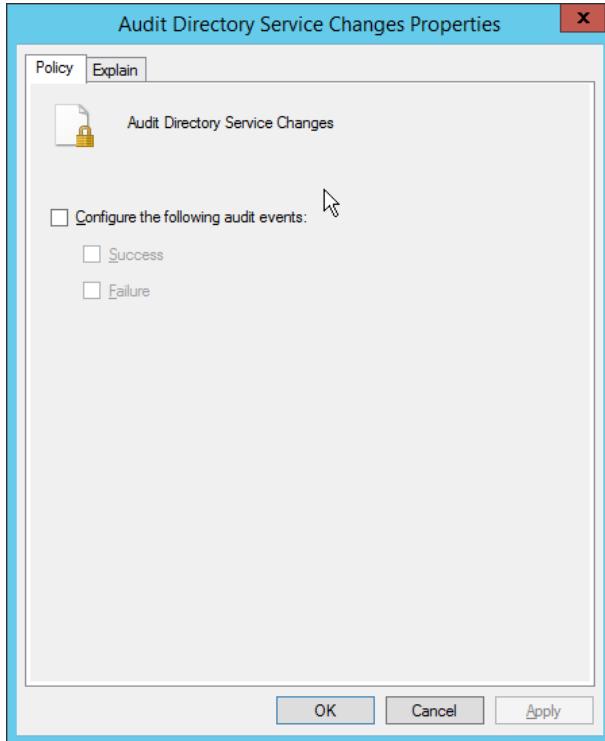


768
769
770
771

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**.

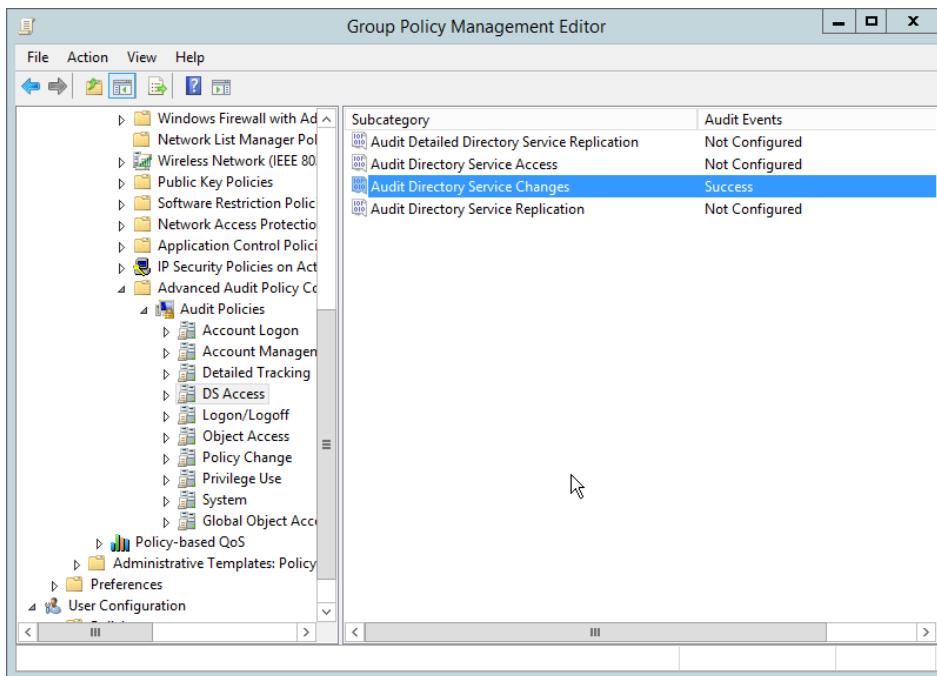


- 772
773 15. Click **OK**.
774 16. Go to **Audit Policies > DS Access**.
775 17. Double-click **Audit Directory Services Changes**.



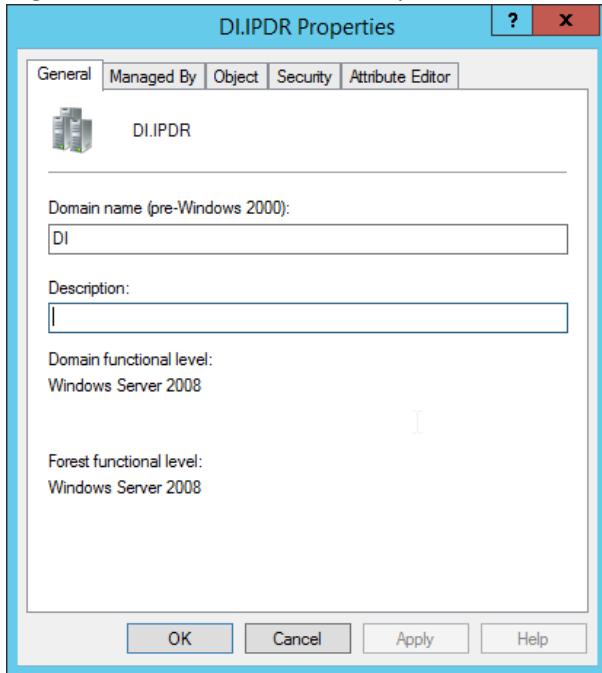
776
777
778
779

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

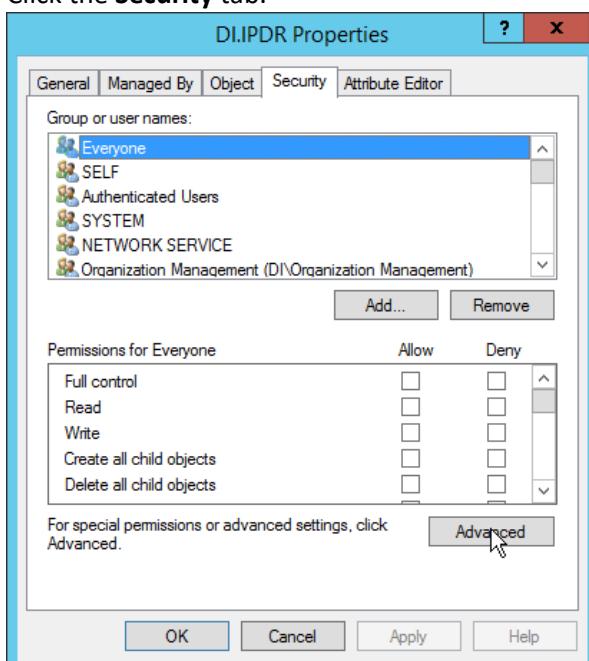


780

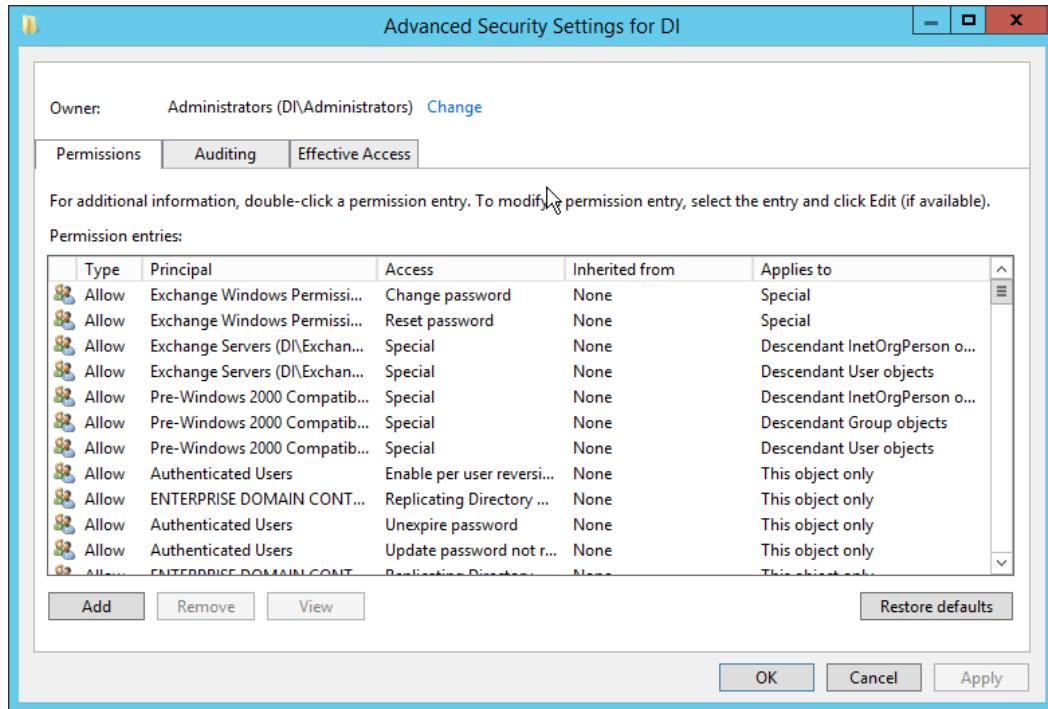
- 781 21. Open **Active Directory Users and Computers**.
782 22. Ensure **View > Advanced Features** is enabled.
783 23. Right-click the **domain** (for example, DI.IPDR) created earlier, and click **Properties**.



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



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



788

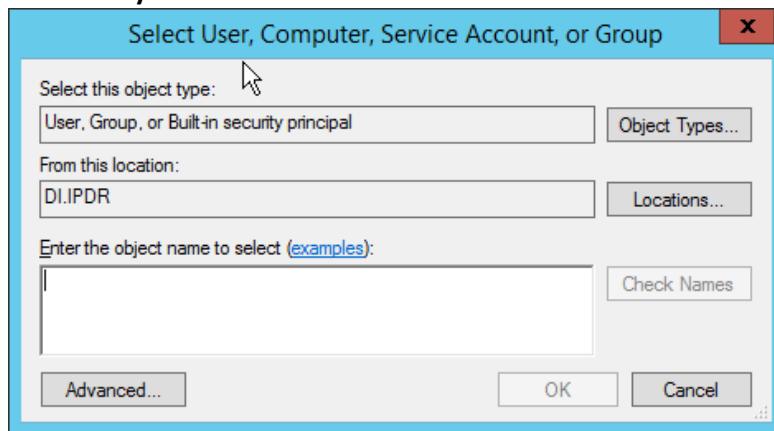
789

26. Click the **Auditing** tab.

790

27. Click **Add**.

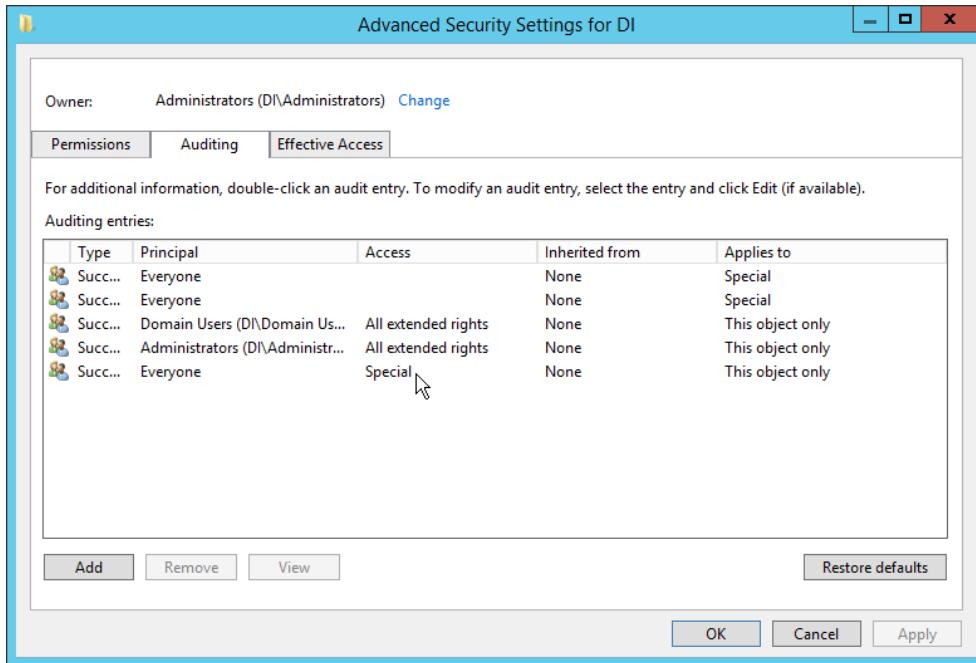
791

28. Enter **Everyone**.

792

793

29. Click **OK**.



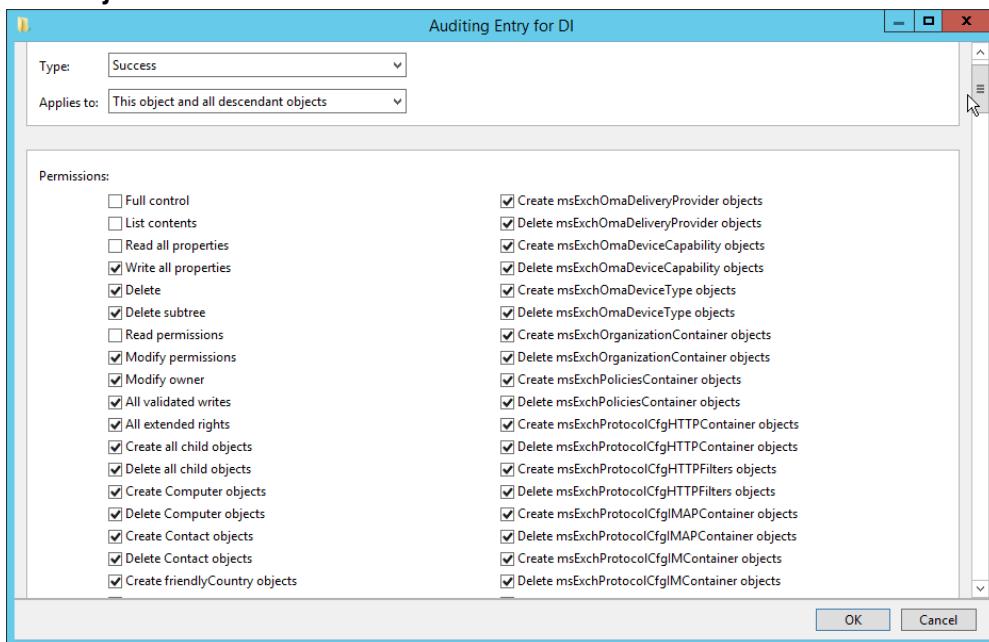
794

795

30. Double-click **Everyone.**

796

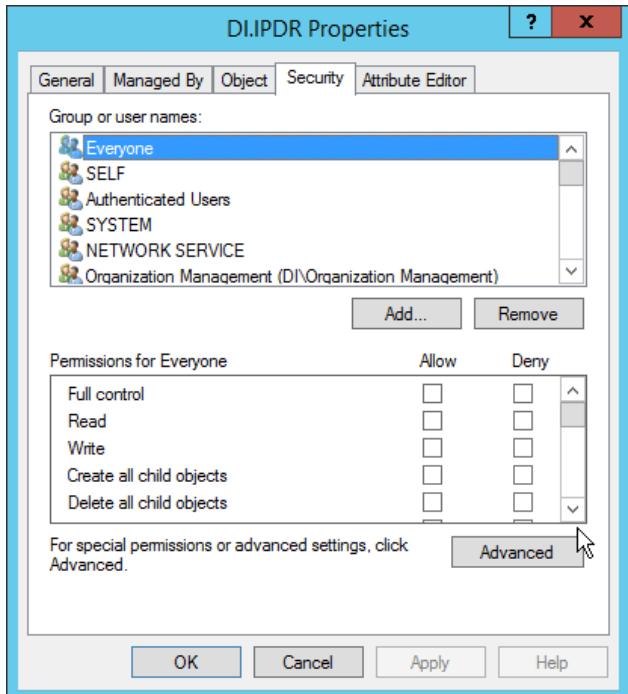
31. Check the boxes next to **Write all properties, Delete, Delete subtree, Modify permissions, Modify owner, All validated writes, All extended rights, Create all child objects, Delete all child objects.**



799

800

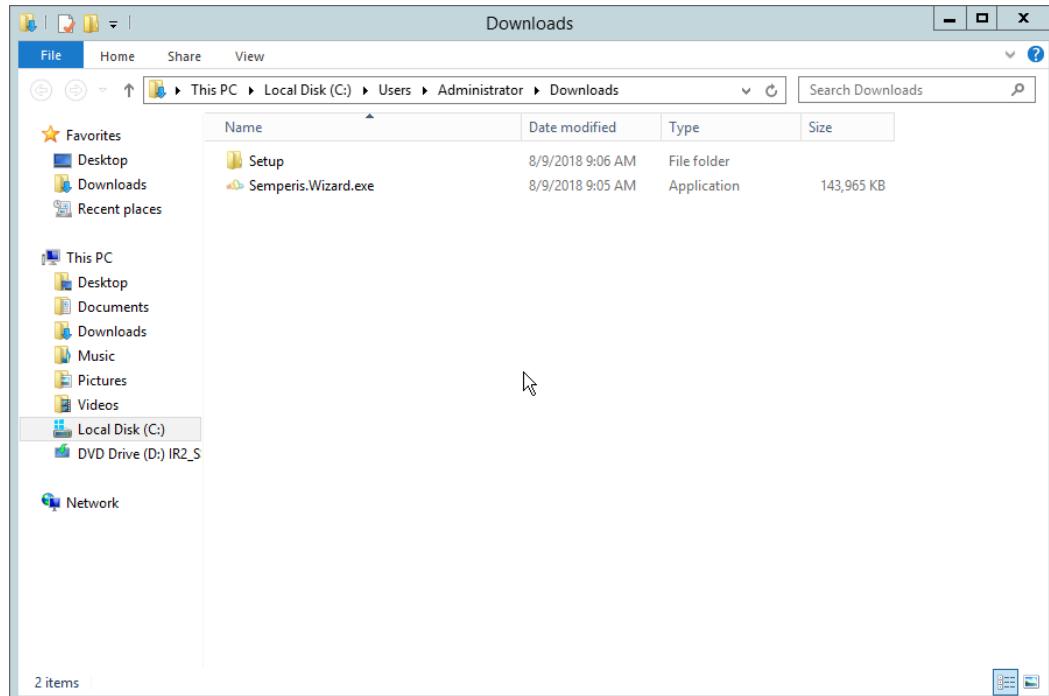
32. Click **OK.**



801
802

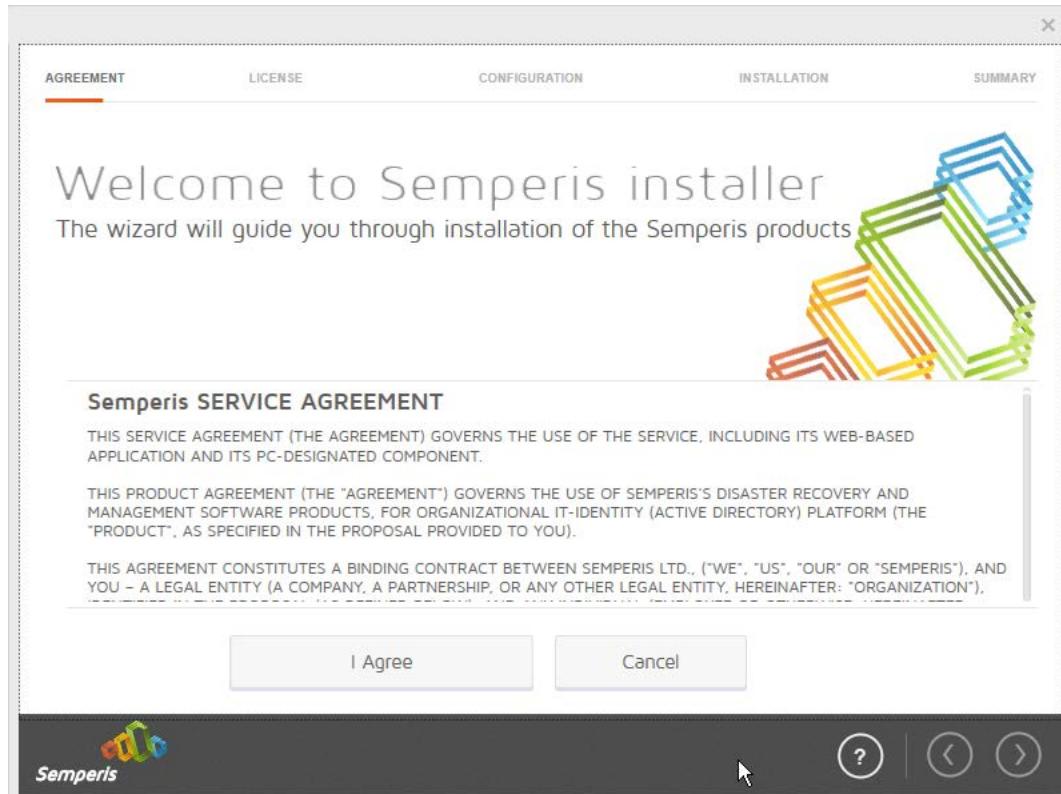
33. Click OK.

- 803 **2.6.2 Install Semperis DSP**
- 804 1. If you are using a local SQL Express Advanced server, place the **SQLEXPRAADV_x64_ENU.exe** installer in a directory called *Setup*, and ensure that the **Semperis Wizard** is adjacent to the **Setup** folder (not inside it). If a SQL Express Advanced server is not being used, no **Setup** folder is required.

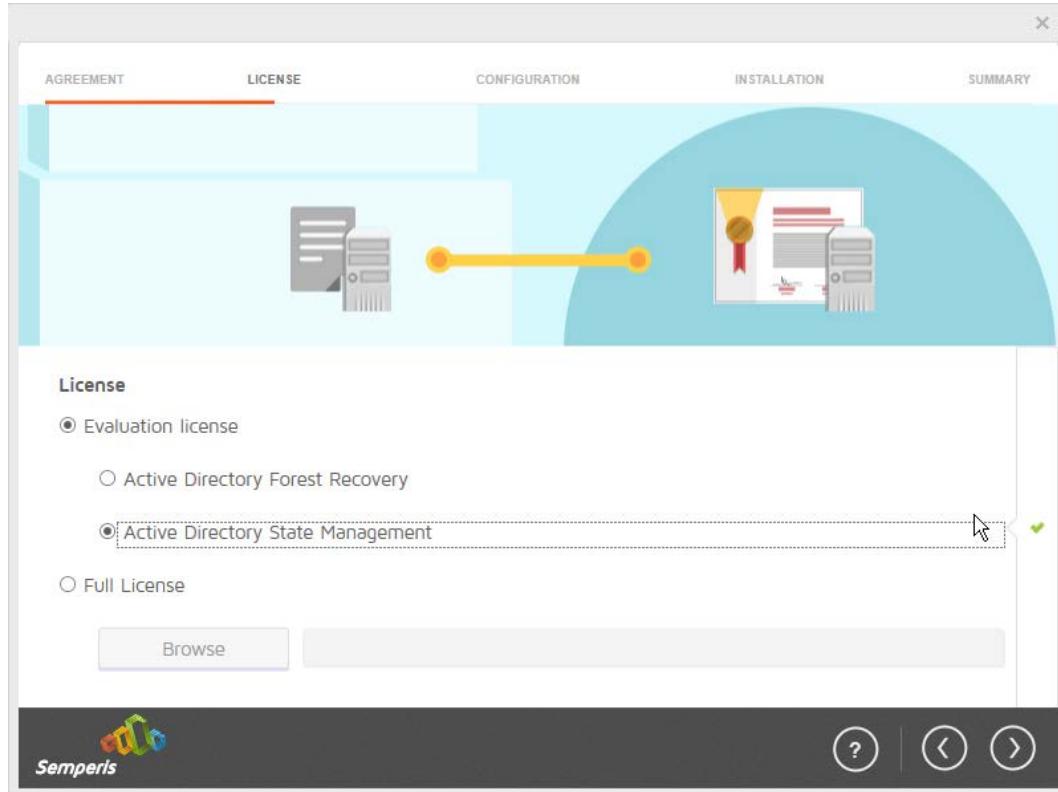


808
809

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



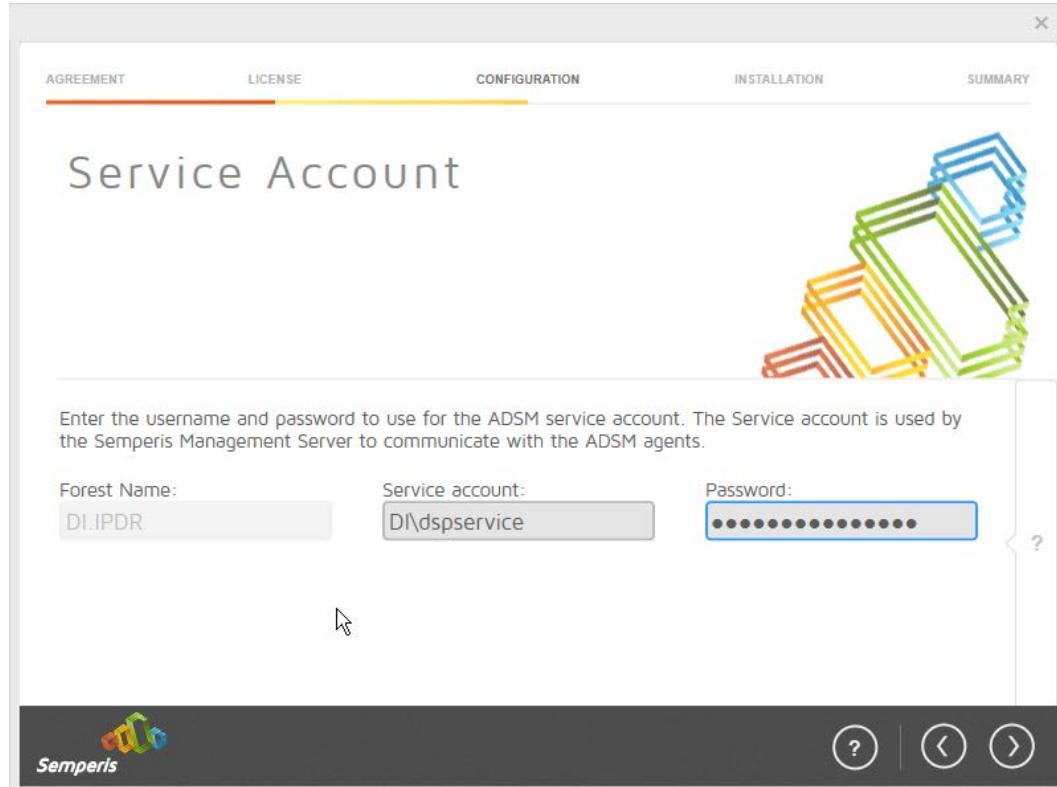
- 810
811 3. Click **I Agree**.
812 4. Select **Evaluation License**.
813 5. Select **Active Directory State Management**.

**License**

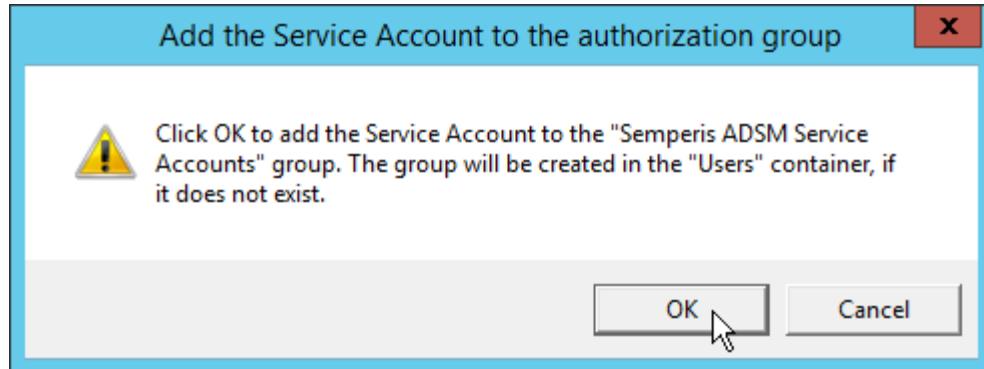
- Evaluation license
- Active Directory Forest Recovery
- Active Directory State Management
- Full License

Browse814
815
816

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

817
818

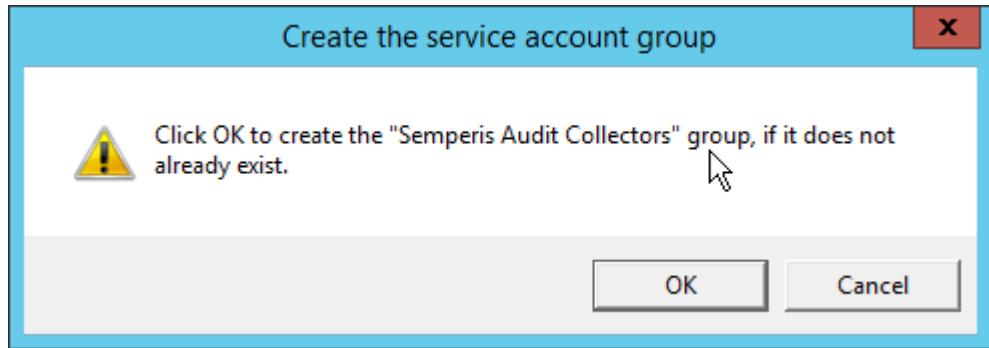
8. Click the > button.

819
820
821

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

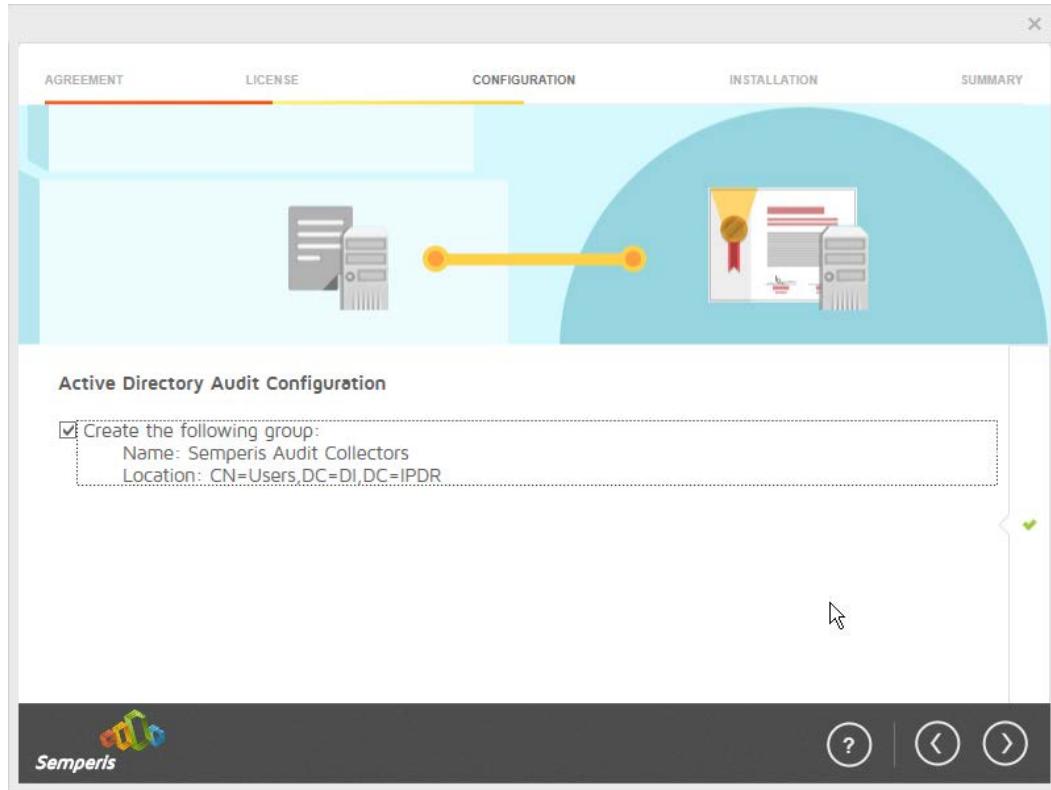
822
823

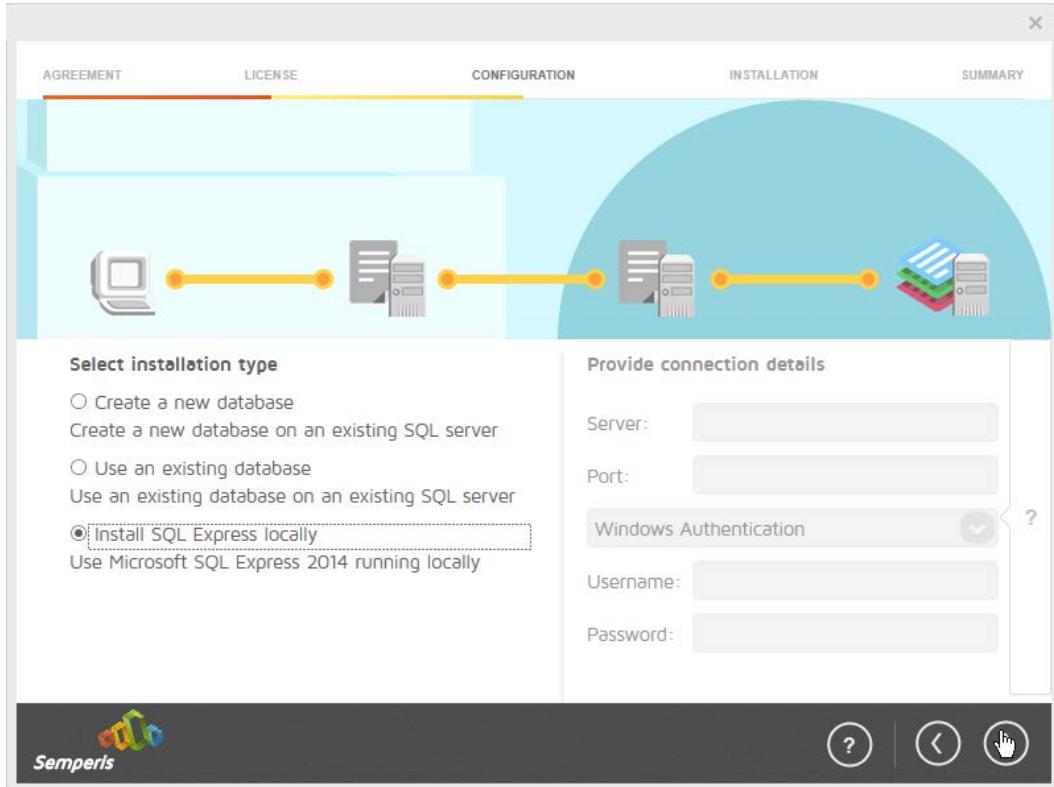
11. Click OK.



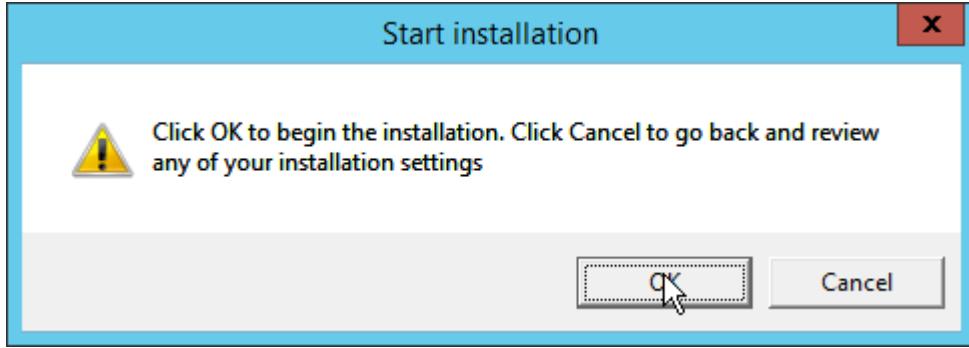
824
825
826

12. Click the > button.
13. Select the appropriate database option, and enter any required information.

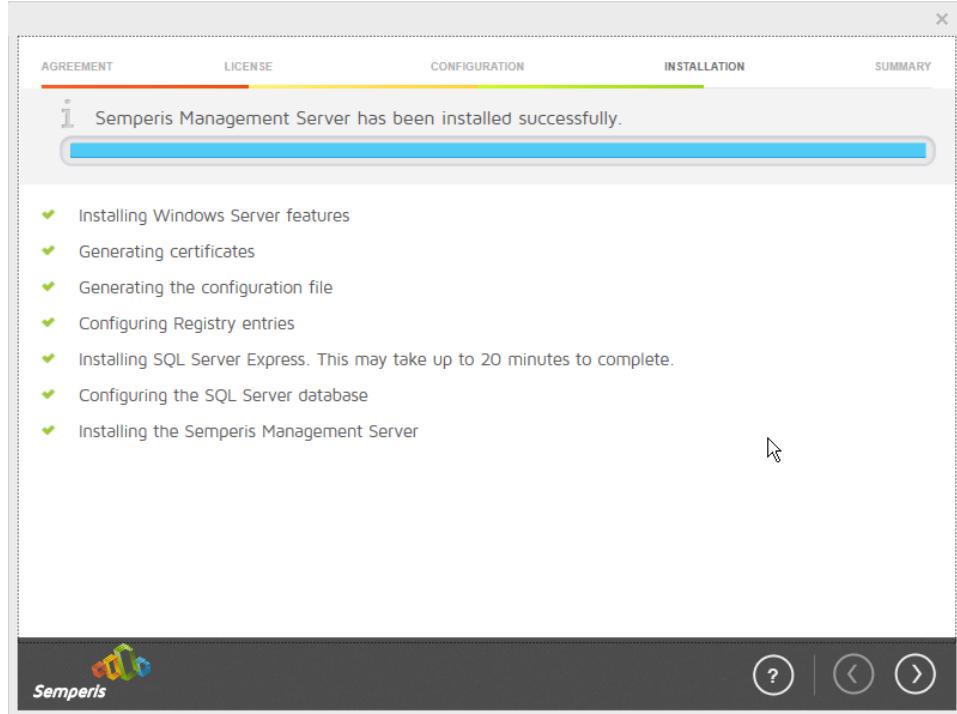


827
828

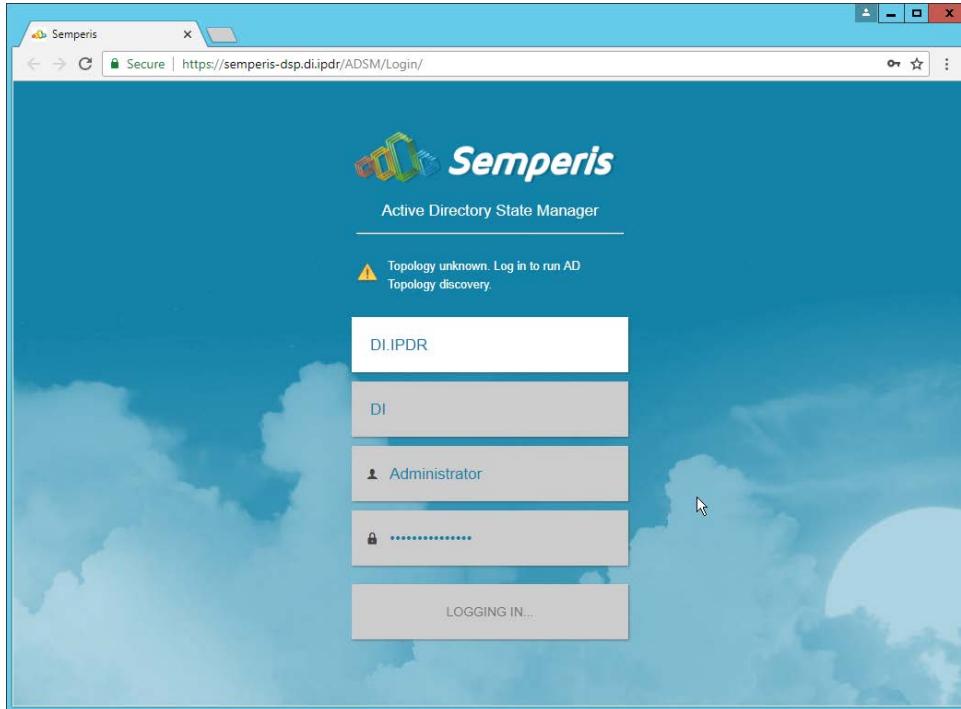
14. Click the > button.

829
830

15. Click OK.



- 831
832 16. Click the > button after the installation completes.
833 17. There should now be a shortcut on the desktop linking to the web console for **Semperis DS**
834 **Protector.**
835 18. On the login page, enter the full domain as well as the NetBIOS name.
836 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.

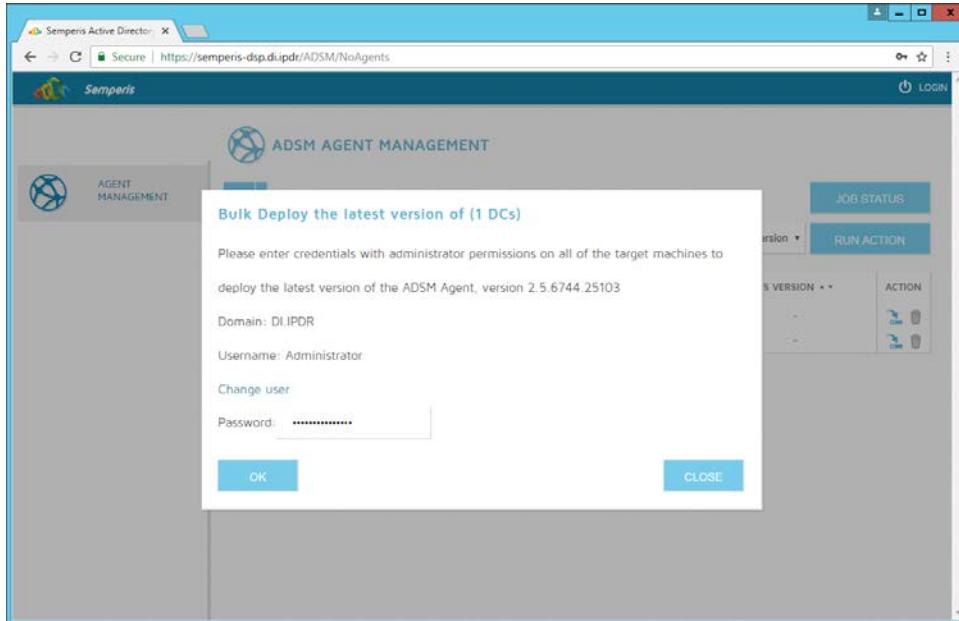
The screenshot shows the Semperis ADSM Agent Management interface. The title bar says 'Semperis Active Director' and the sub-page title is 'ADSM AGENT MANAGEMENT'. The main content area displays a table of agents. The table has columns: NAME, DOMAIN, STATUS, VERSION, OS VERSION, and ACTION. There are two rows in the table:

- Row 1: AD-DNS (checkbox checked), DI IPDR, No agent, 0.0.0.0, -, edit/delete icons.
- Row 2: AD-DNS08 (checkbox unchecked), DI IPDR, No agent, 0.0.0.0, -, edit/delete icons.

At the top right of the table area, there are buttons for 'JOB STATUS' and 'RUN ACTION'. On the left side, there is a sidebar titled 'AGENT MANAGEMENT' with a refresh icon.

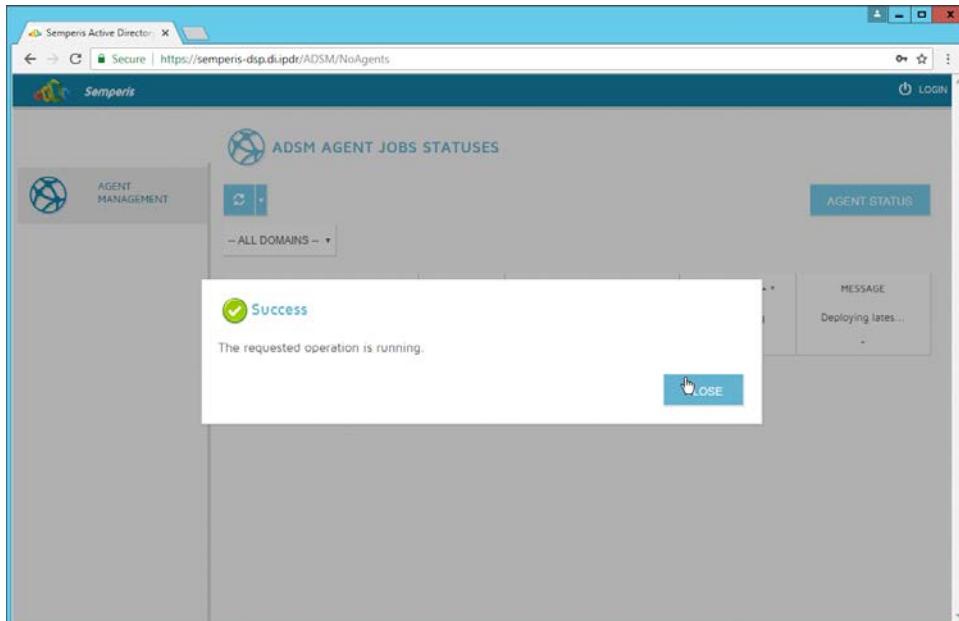
840
841
842

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



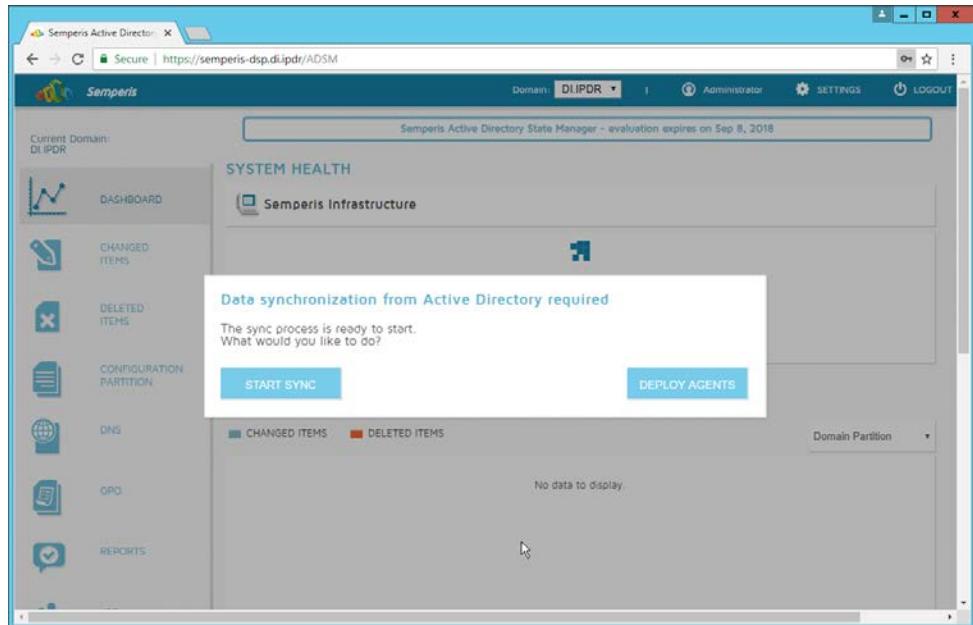
843
844

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.



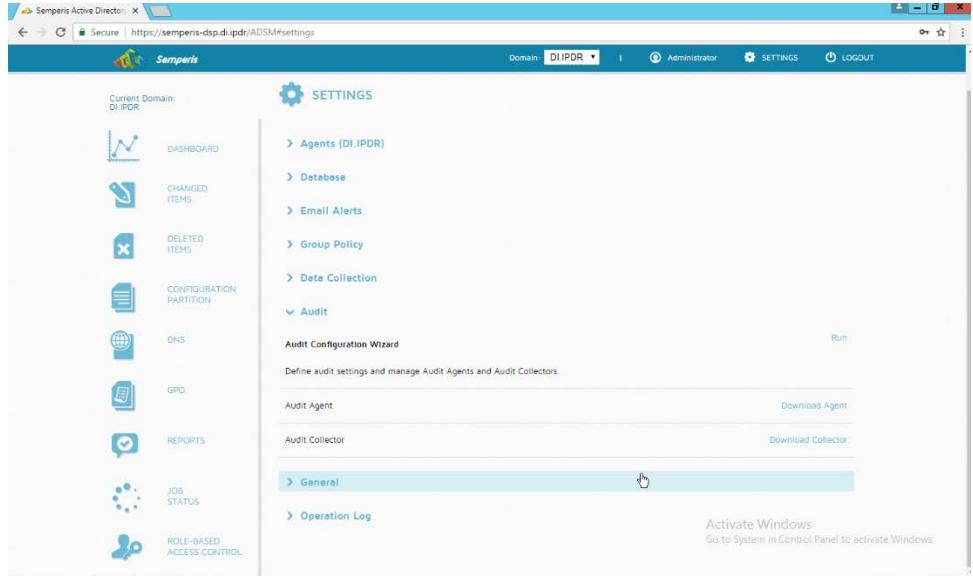
848

849

850

27. Click **Start Sync**.

28. After this completes, click **Settings** at the top of the page.



851

852

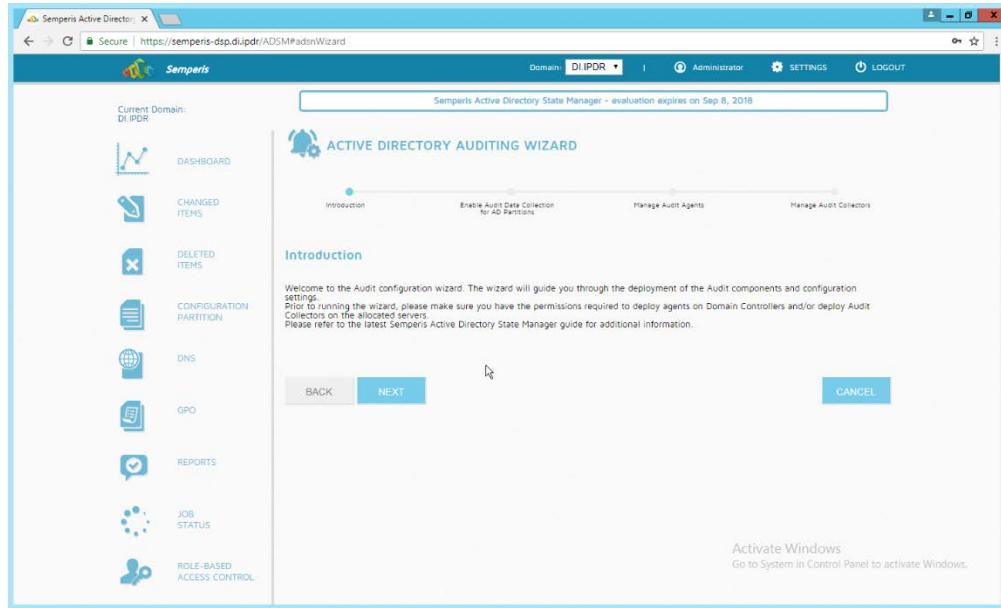
29. Click **Audit**.

853

30. Click **Run**.

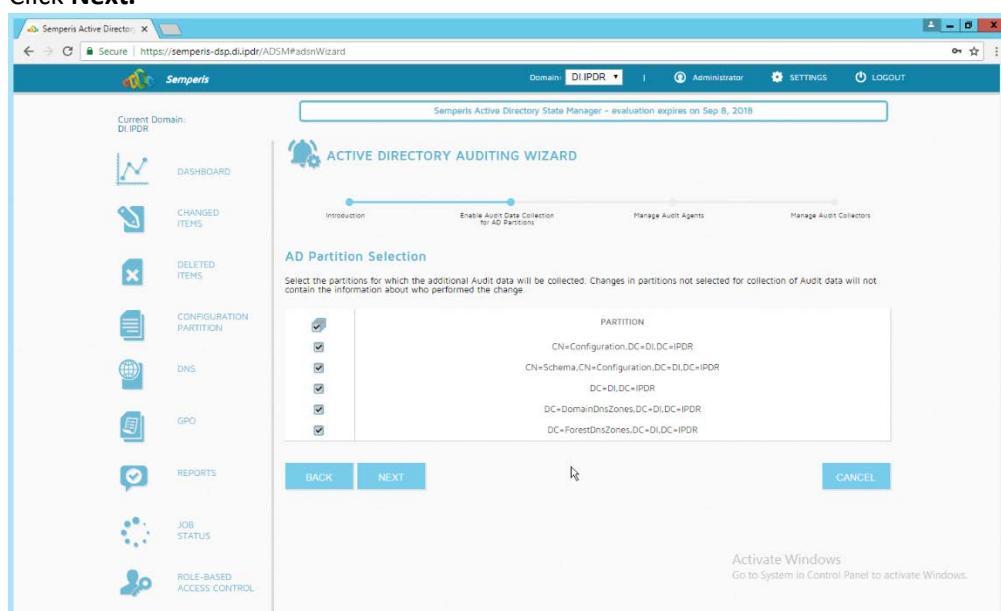
854
855

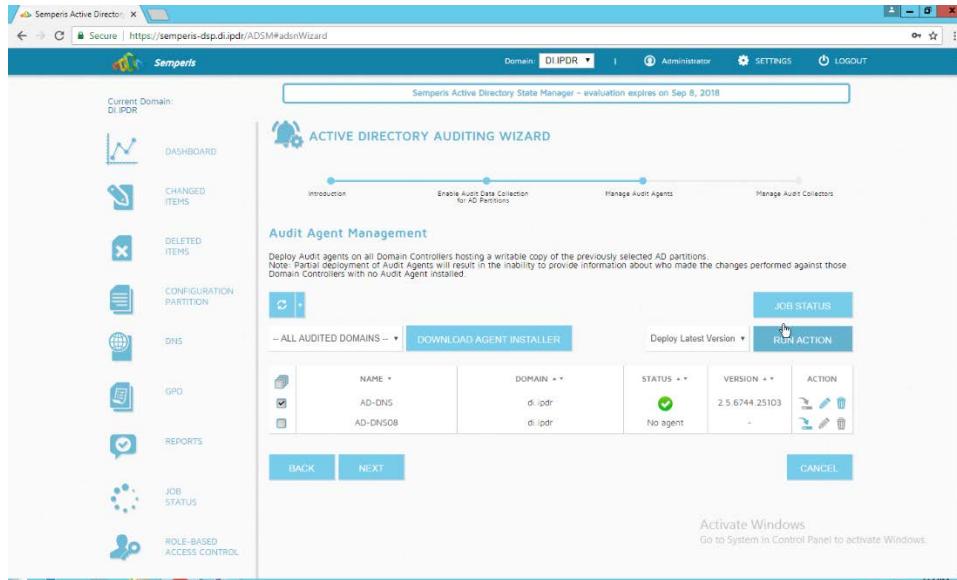
31. Click Next.

856
857
858

32. Click Next.

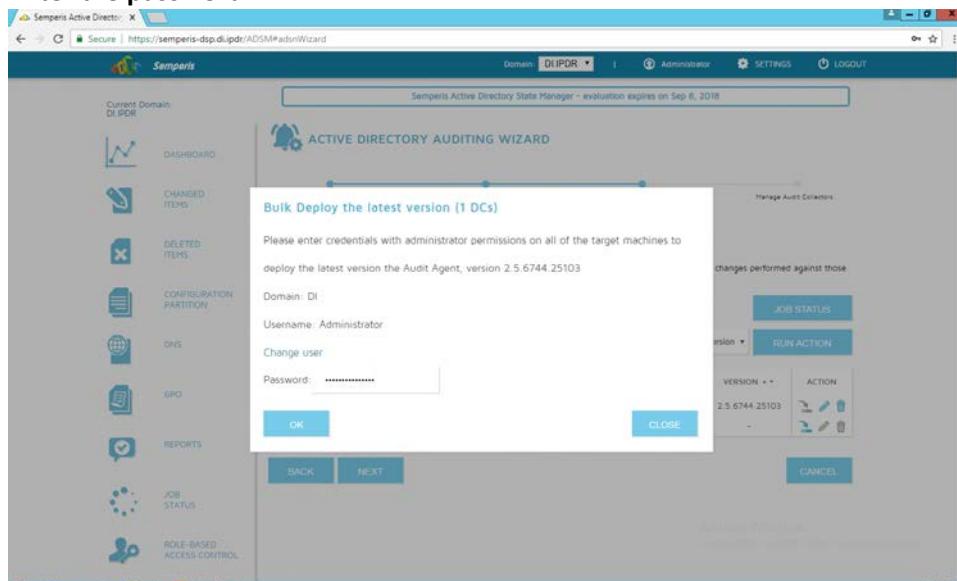
33. Check the boxes next to any Domain Controllers that should be monitored.





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.

2.6.3 Roll Back Changes with Semperis DSP

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

873
874

- Click **Undo Selected** to roll back these changes.

875

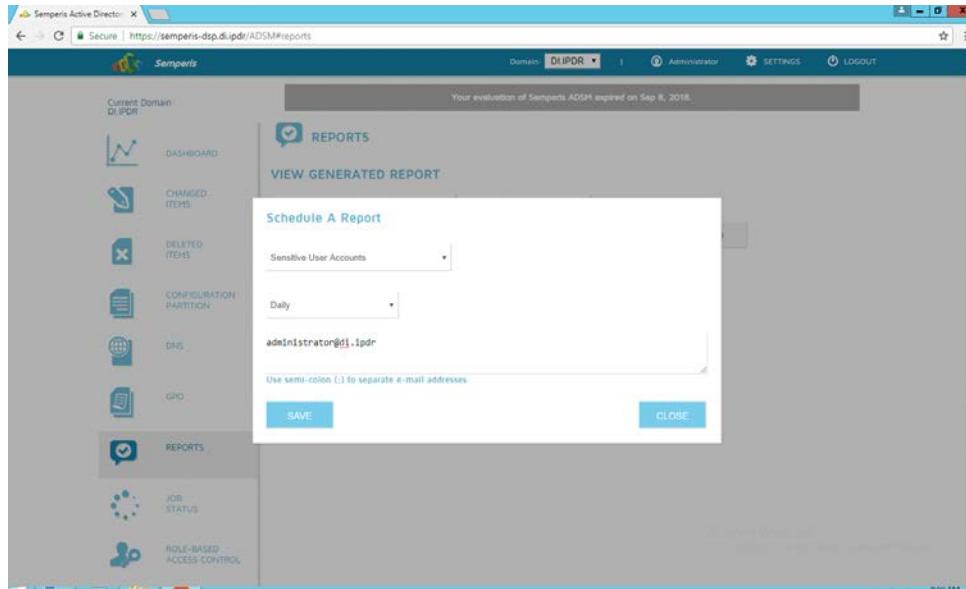
2.6.4 Configure Reporting with Semperis DSP

876
877
878

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

879
880
881
882

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

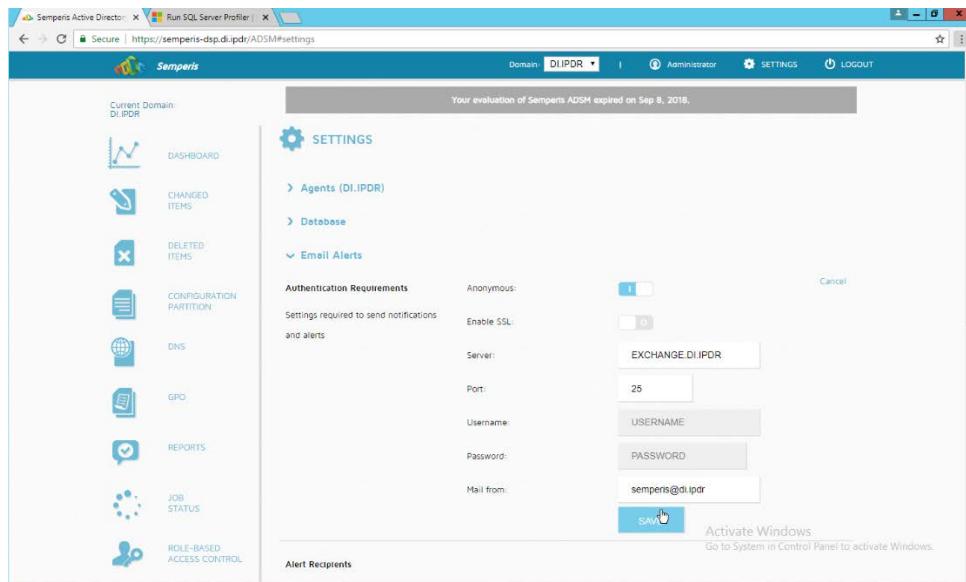


883
884

6. Click **Save**.

2.6.5 Configure Email Alerts with Semperis DSP

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.

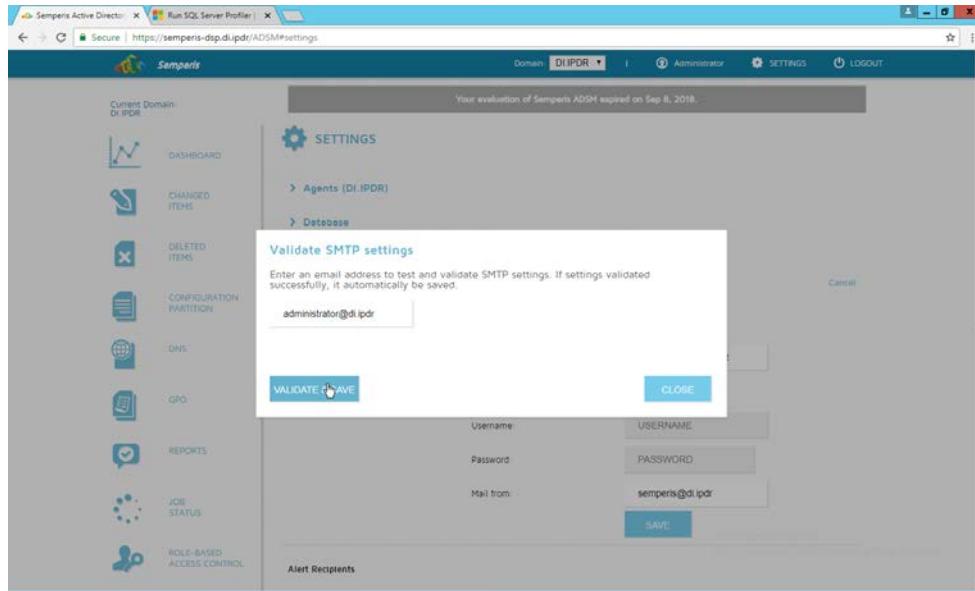


891
892

5. Click **Save**.

893

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



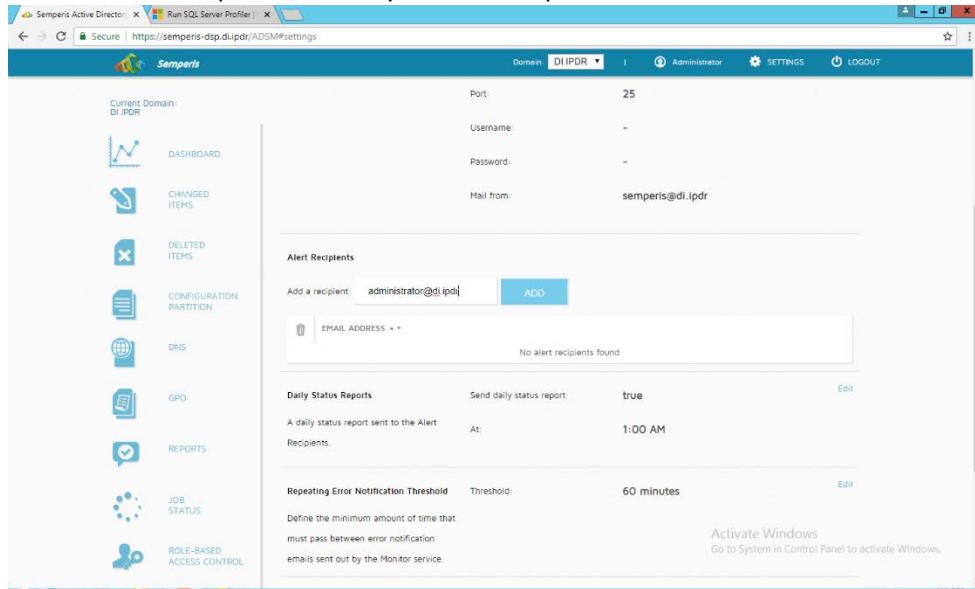
894

895

896

7. Click **Validate & Save**.

8. Under Alert Recipients, add any desired recipients of alerts.



897

898

899

9. Click **Add**.

10. Configure any schedule settings according to your organization's needs.

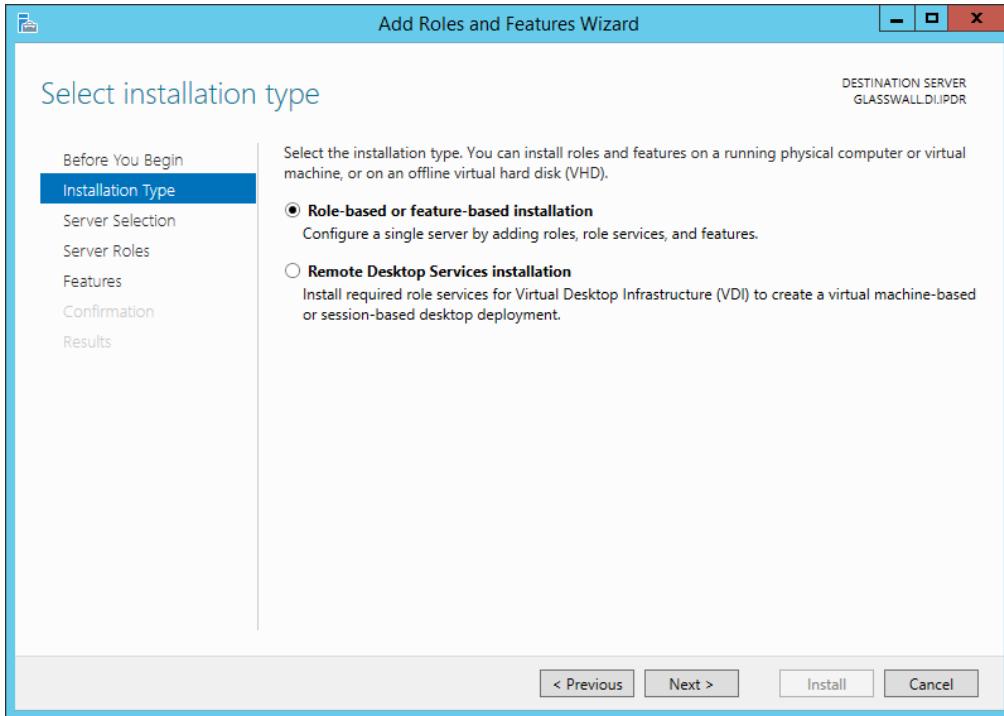
900 2.7 Glasswall FileTrust™ for Email

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.

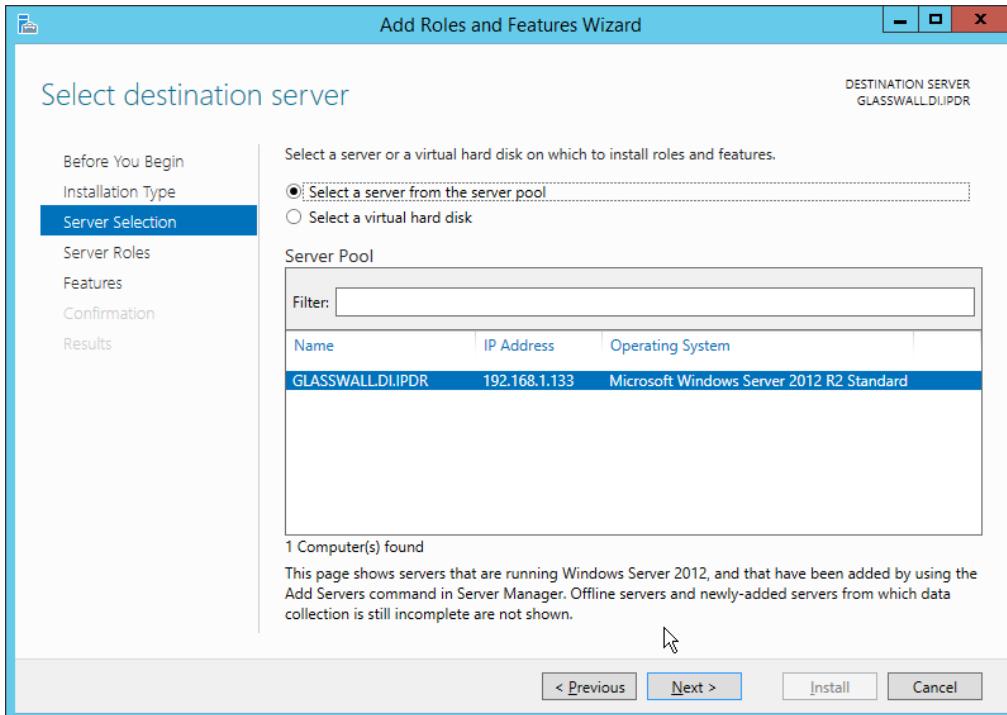
904 2.7.1 Install Prerequisites

905 2.7.1.1 *Install the IIS web server*

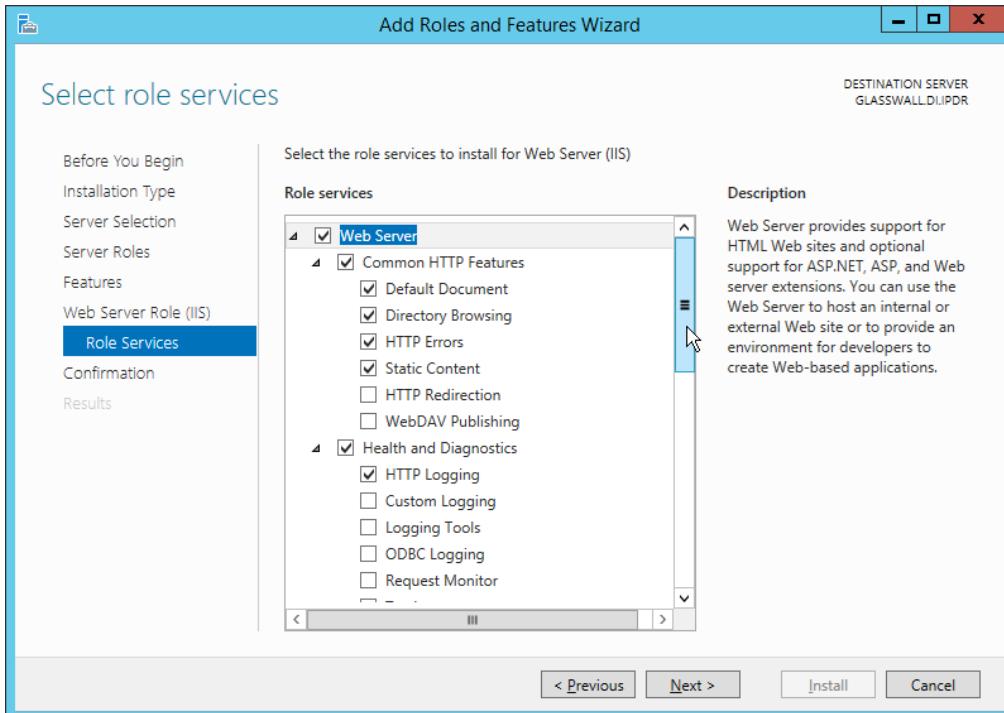
- 906 1. In **Server Manager**, click **Add Roles and Features**.
- 907 2. Click **Next**.
- 908 3. Select **Role-based or feature-based installation**.



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



- 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
925
926

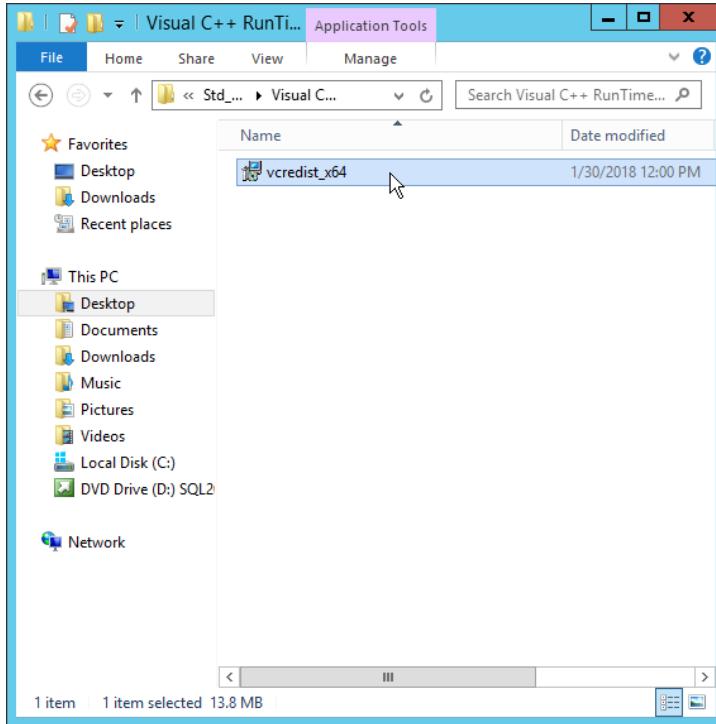
12. Click **Next**.
13. Check the box next to **Restart the destination server automatically if required**.
14. Click **Install**.

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.

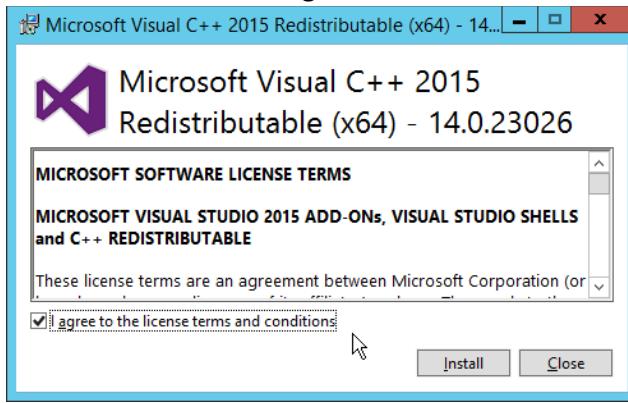
931 [**2.7.1.3 Install Microsoft Visual C++ 2015**](#)

1. Run the **vcredist_x64** installer.



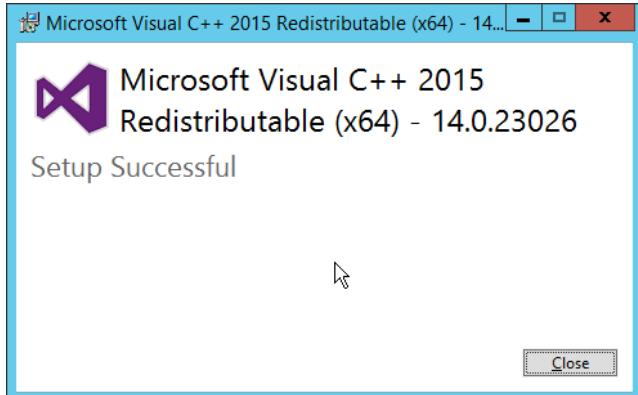
933
934

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**.

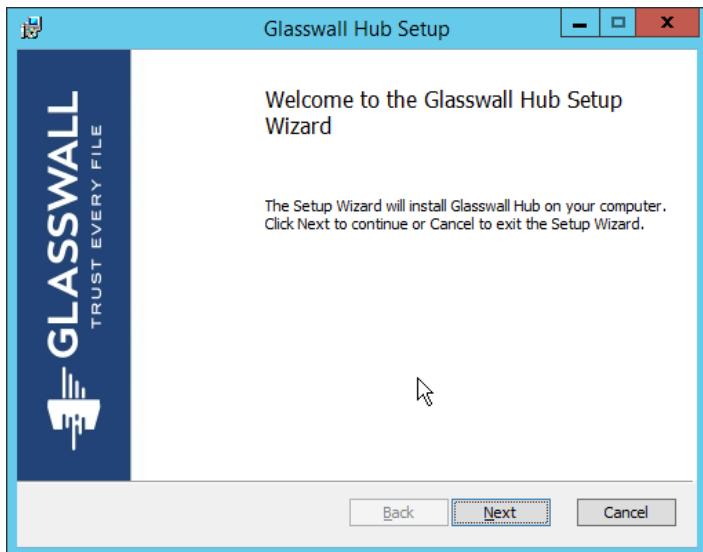


938

939 2.7.2 Install the Glasswall FileTrust Server Component

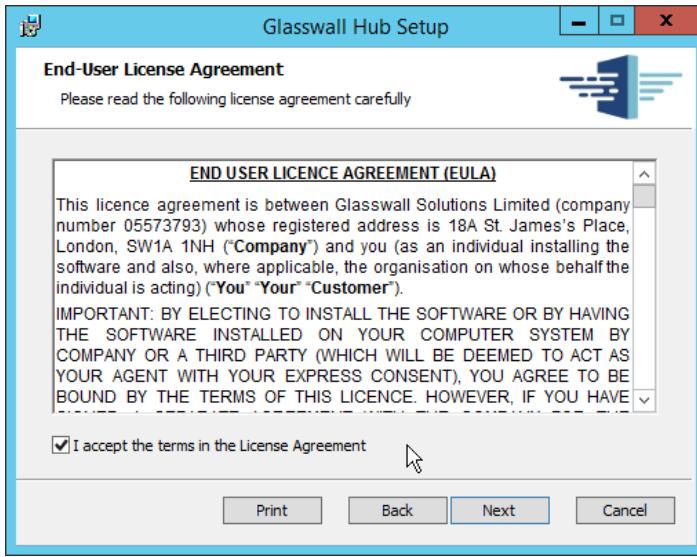
940 2.7.2.1 *Install Glasswall Hub*

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



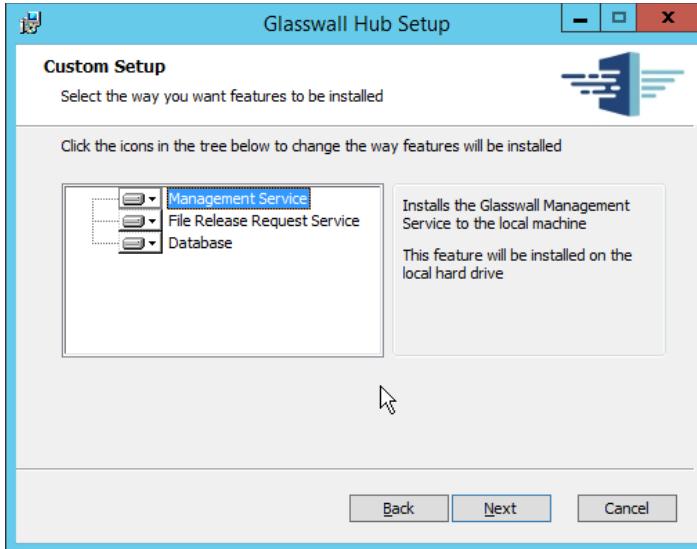
942

- 943 2. Click **Next**.



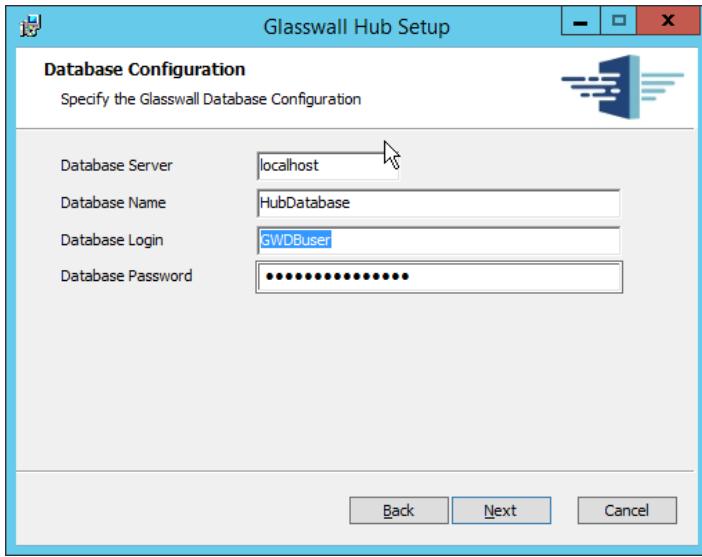
944
945
946

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



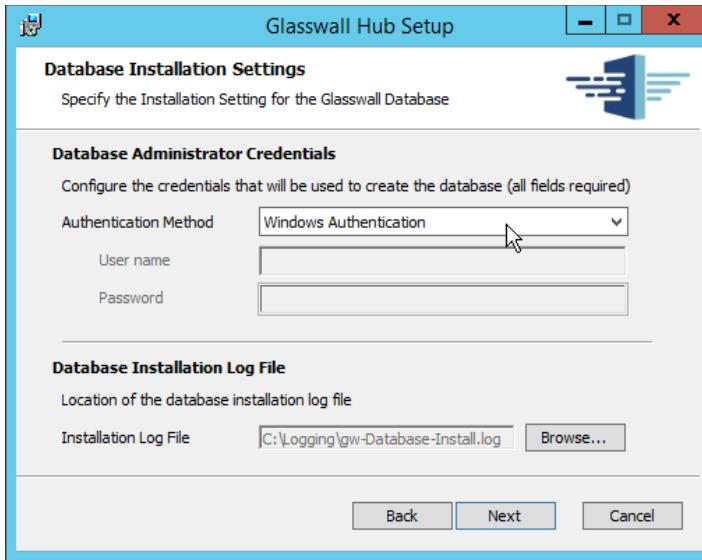
947
948
949
950
951

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).



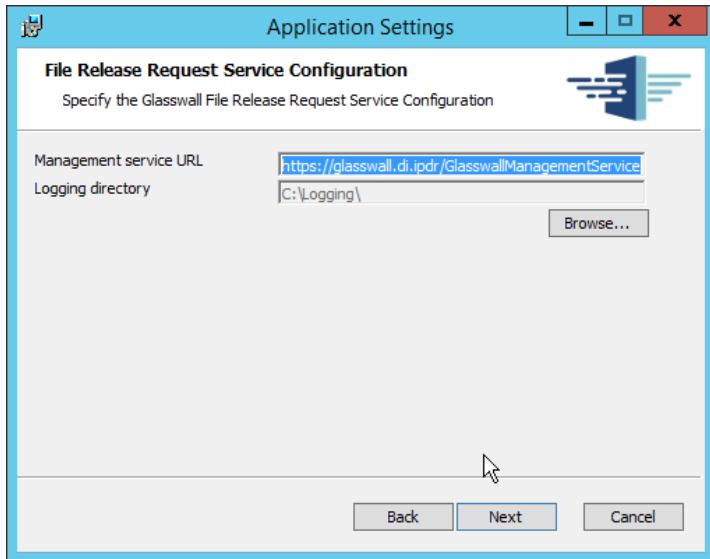
952
953
954

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



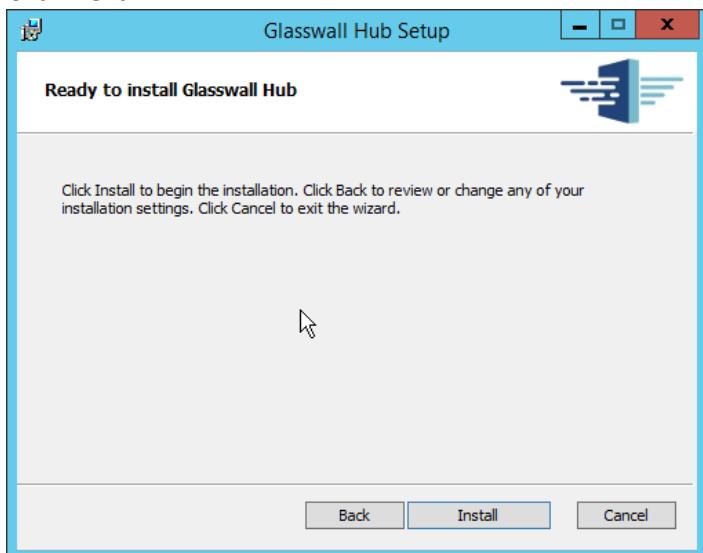
955
956
957
958

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



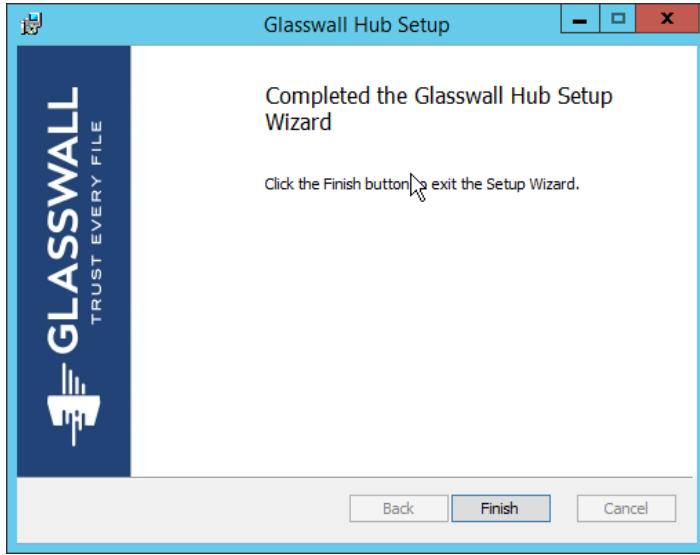
959
960

13. Click **Next**.



961
962

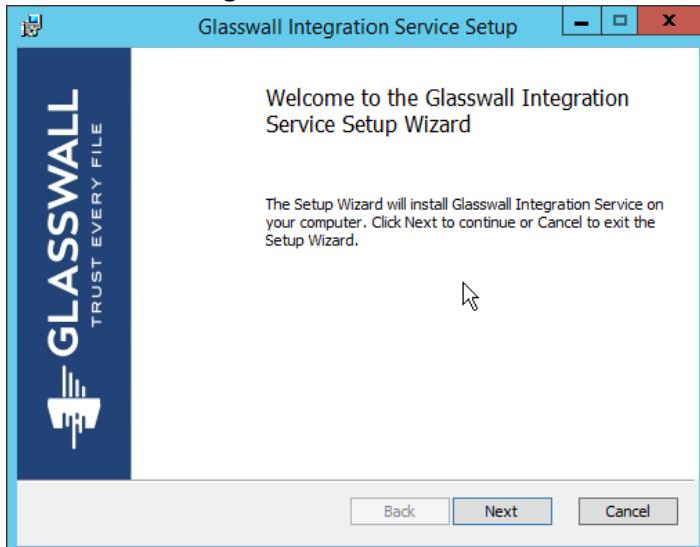
14. Click **Install**.



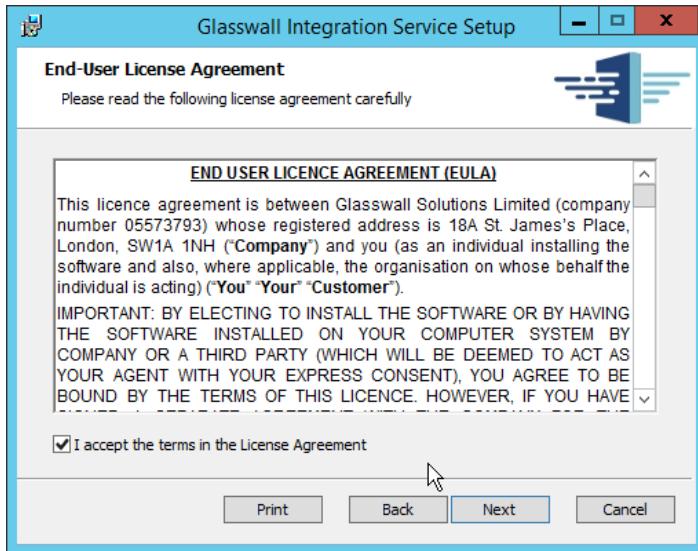
- 963
964 15. Click **Finish**.

2.7.2.2 *Install Glasswall Integration Service*

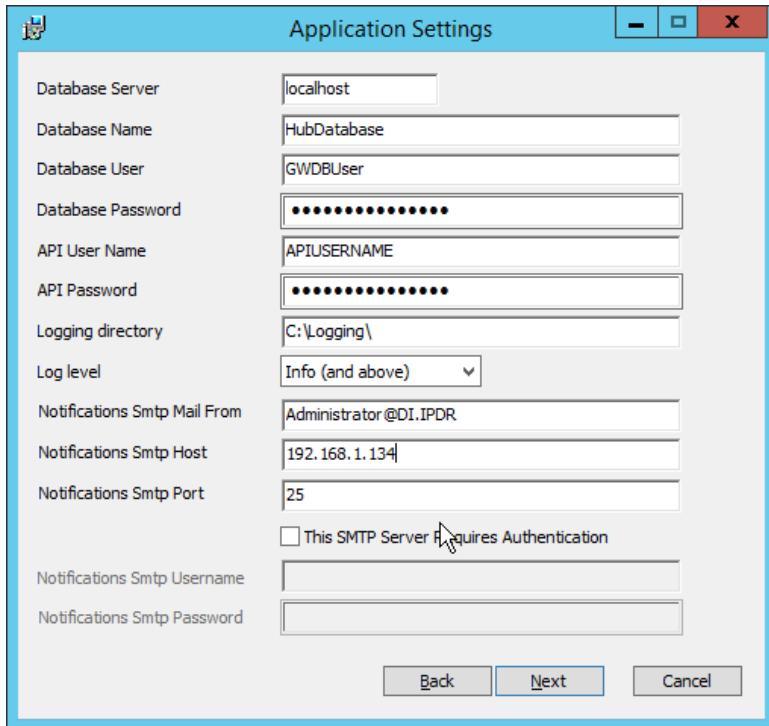
- 966 1. Run **GlasswallIntegrationService.msi**.



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

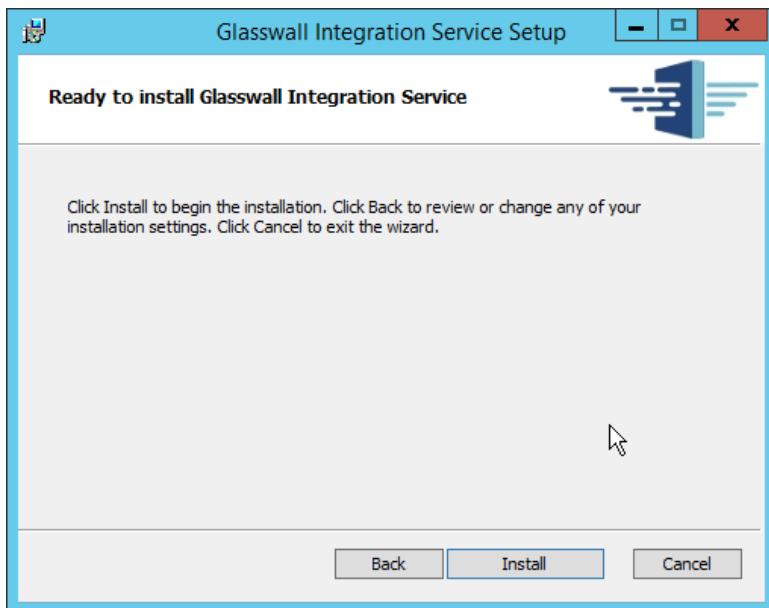


- 970
971 4. Click **Next**.
972 5. For **Database Server**, **Database Name**, **Database User**, and **Database Password**, enter the
973 information entered in the **Glasswall Hub Installer**.
974 6. Create a **username** and **password** for **API User Name** and **API Password**.
975 7. Enter an email address to be used for notifications in **Notifications Smtip Mail From**.
976 8. Enter the **address** for the mail server for **Notifications Smtip Host**.
977 9. Enter a **port** (25 is used here) for **Notifications Smtip Port**.



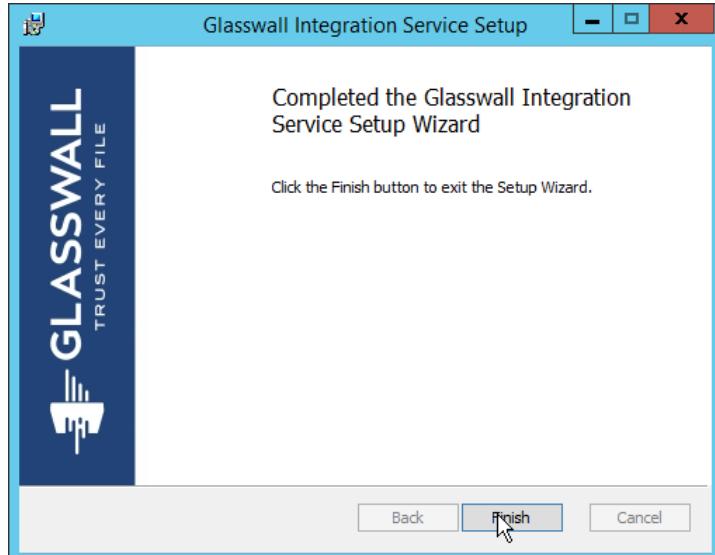
978
979

10. Click **Next**.



980
981

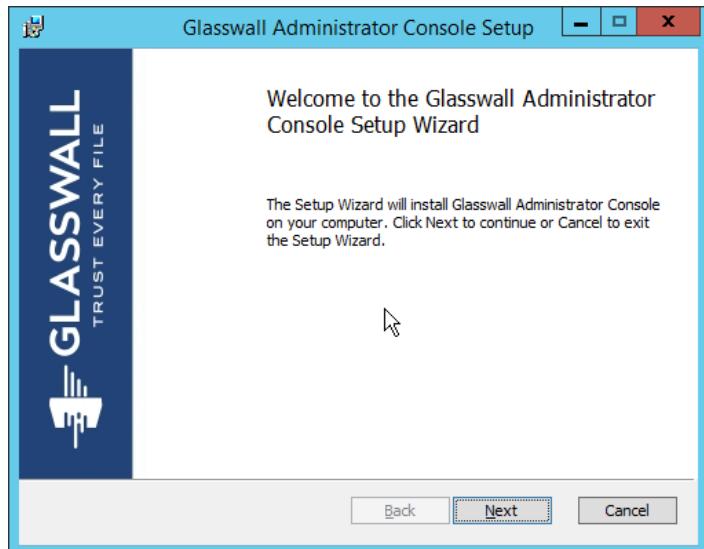
11. Click **Install**.



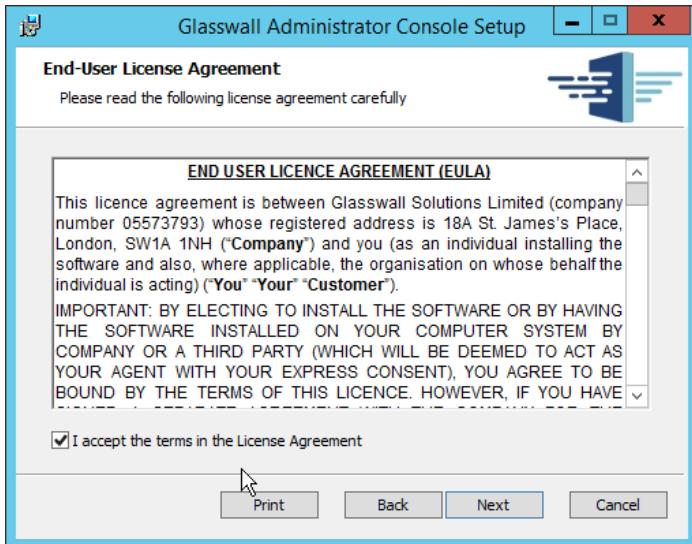
- 982
983 12. Click **Finish**.

2.7.2.3 *Install Glasswall Administrator Console*

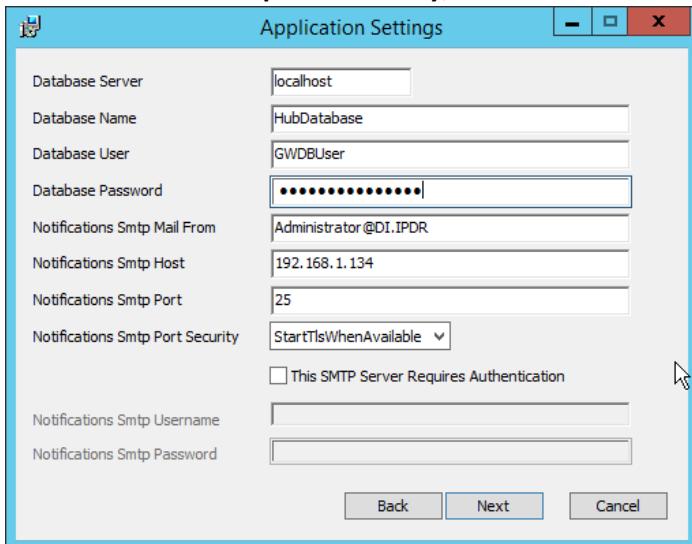
- 984 1. Run **AdministratorConsoleInstaller.msi**.



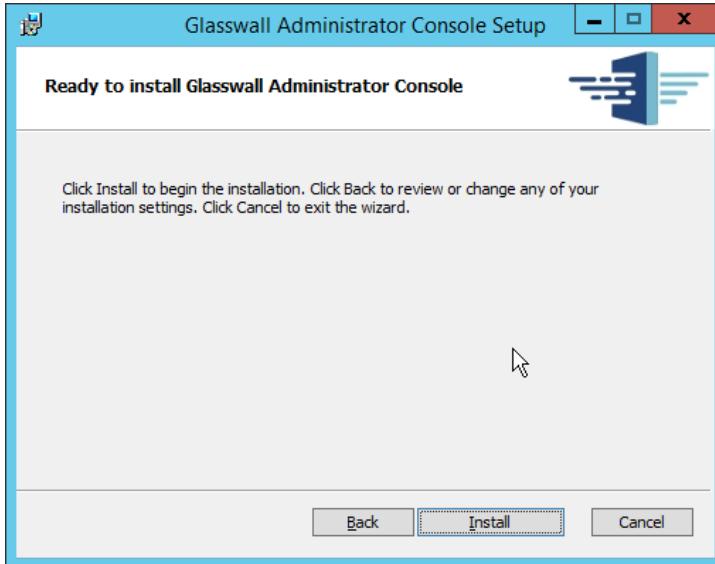
- 985
986 2. Click **Next**.
987 3. Check the box next to **I accept the terms in the License Agreement**.



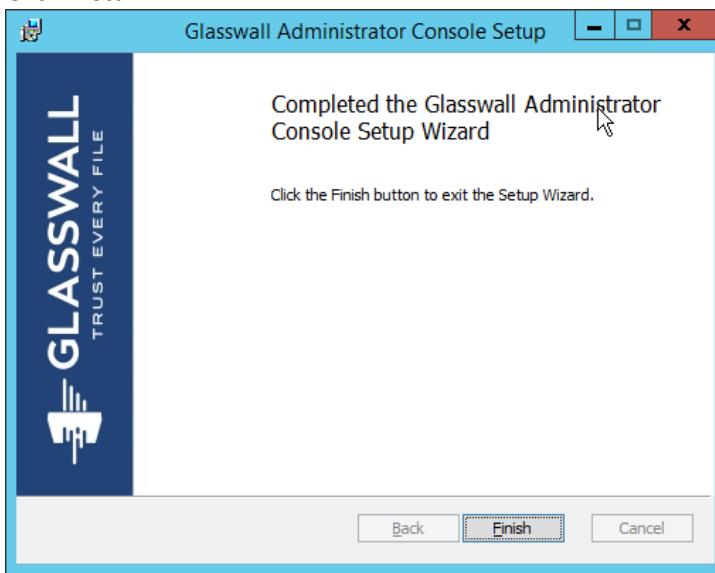
- 989
990 4. Click **Next**.
991 5. For **Database Server**, **Database Name**, **Database User**, and **Database Password**, enter the
992 information entered in the **Glasswall Hub Installer**.
993 6. For **Notifications Smtip Mail From**, **Notifications Smtip Host**, **Notifications Smtip Port**, enter the
994 information entered in the **Glasswall Integration Service Installer**.
995 7. For **Notifications Smtip Port Security**, select **StartTlsWhenAvailable**.



- 996
997 8. Click **Next**.

998
999

9. Click
- Install**
- .

1000
1001

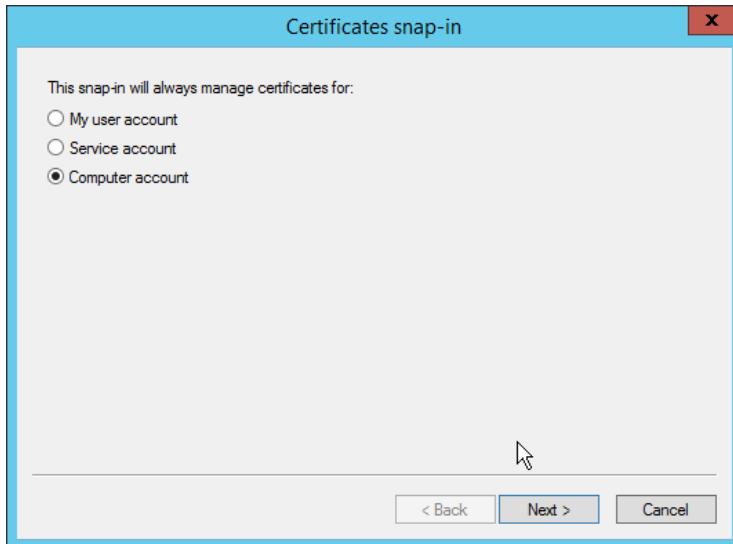
10. Click
- Finish**
- .

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

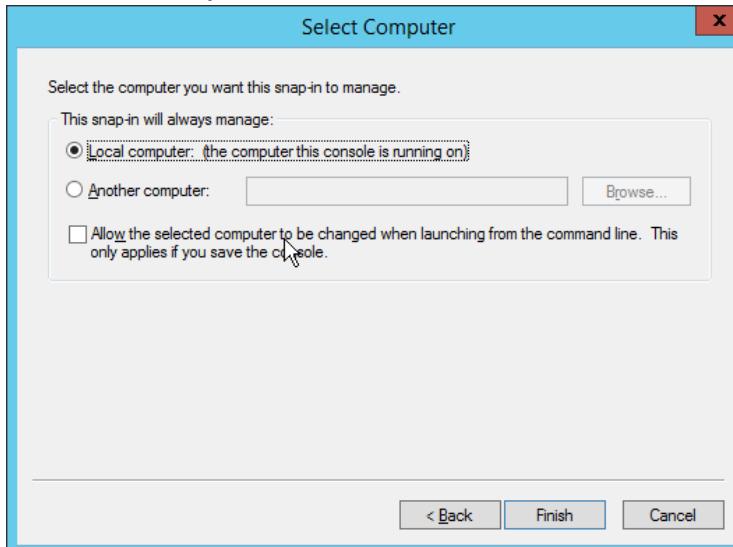


1011

1012 6. Click **Next**.

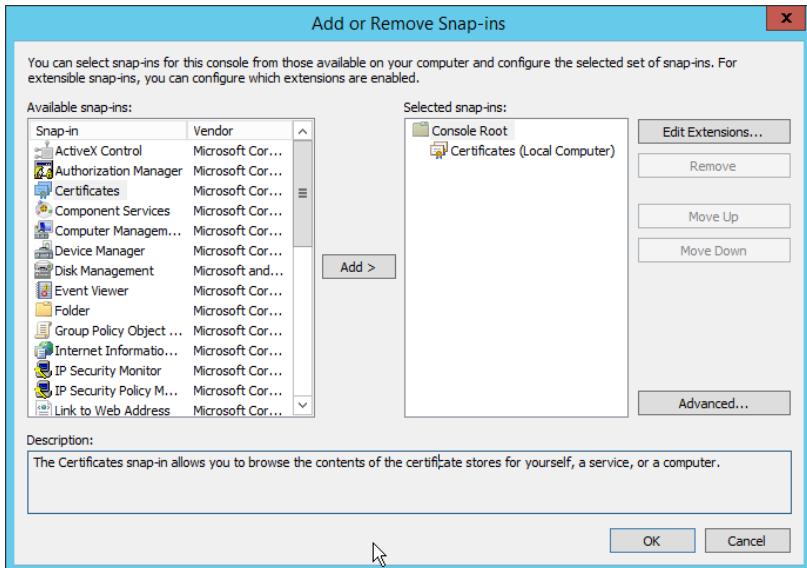
1013

7. Select **Local computer**.



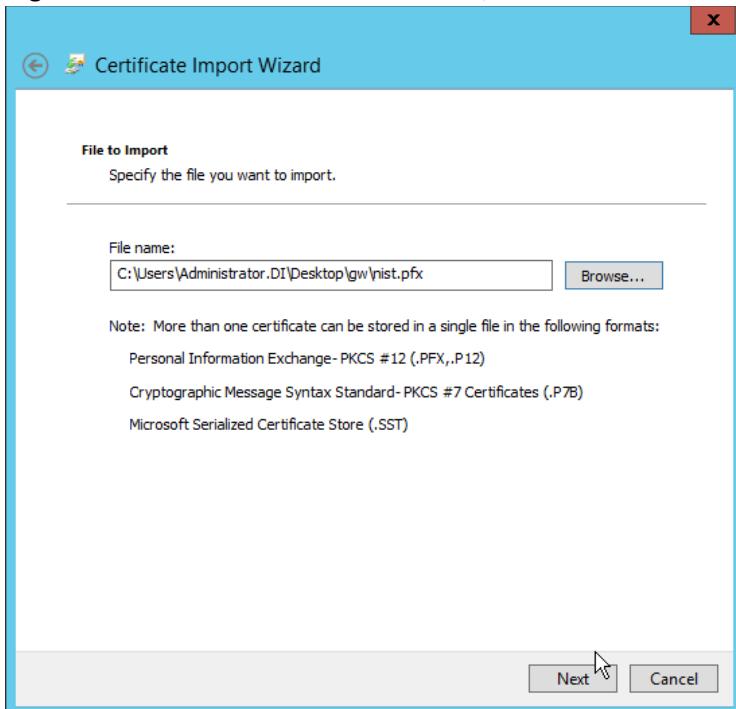
1014

1015 8. Click **Finish**.



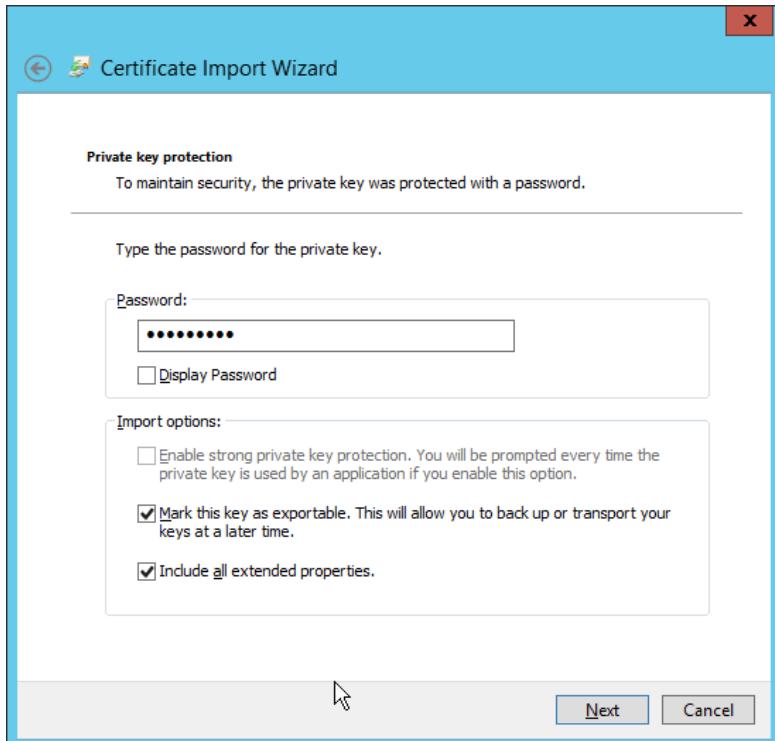
1016
1017
1018

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



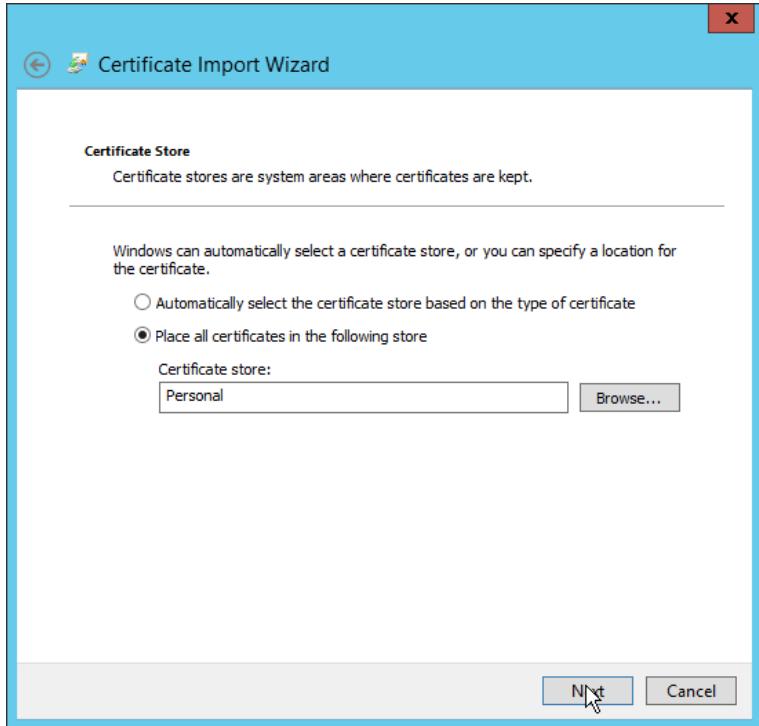
1019
1020
1021
1022
1023

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**.



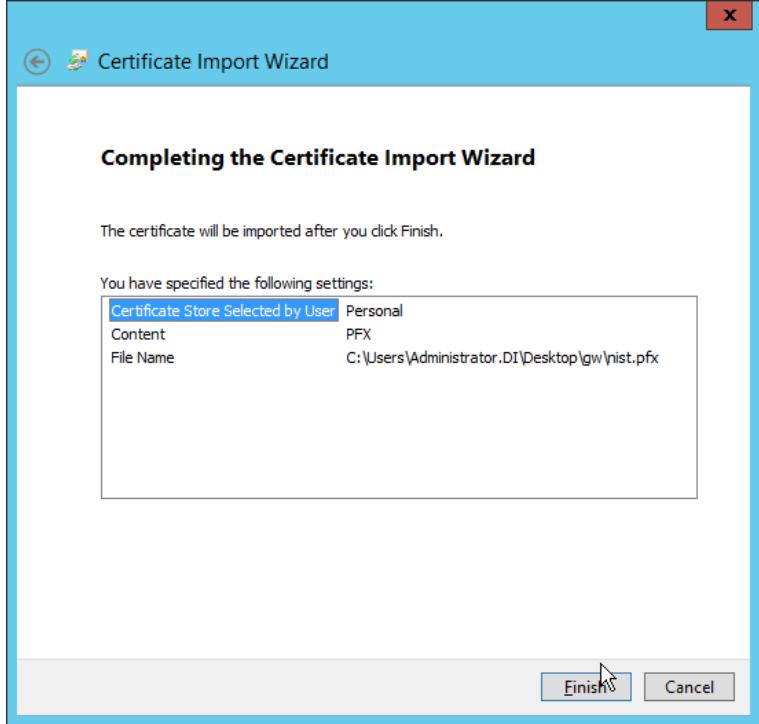
1024
1025
1026

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



1027
1028

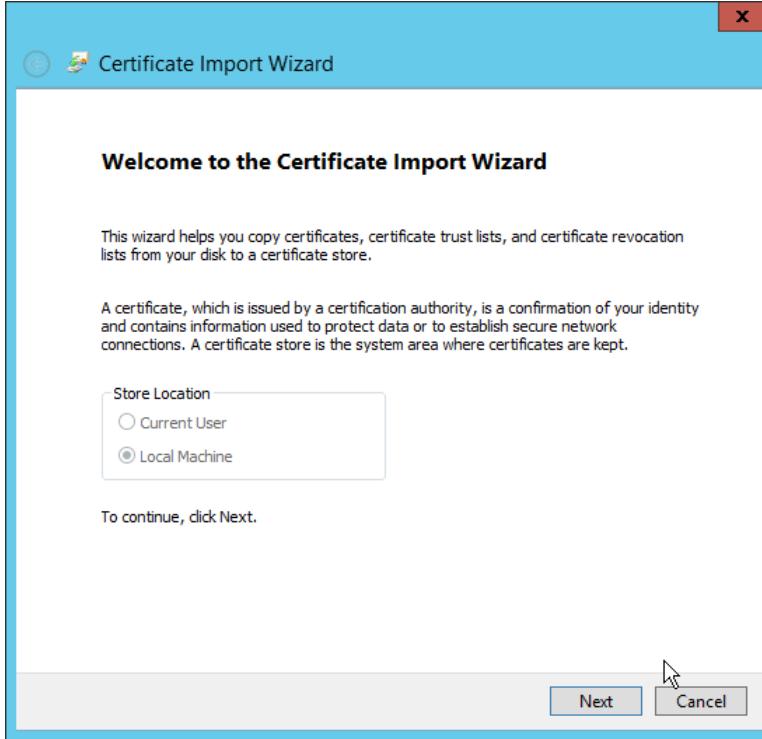
17. Click **Next**.



1029
1030

18. Click **Finish**.

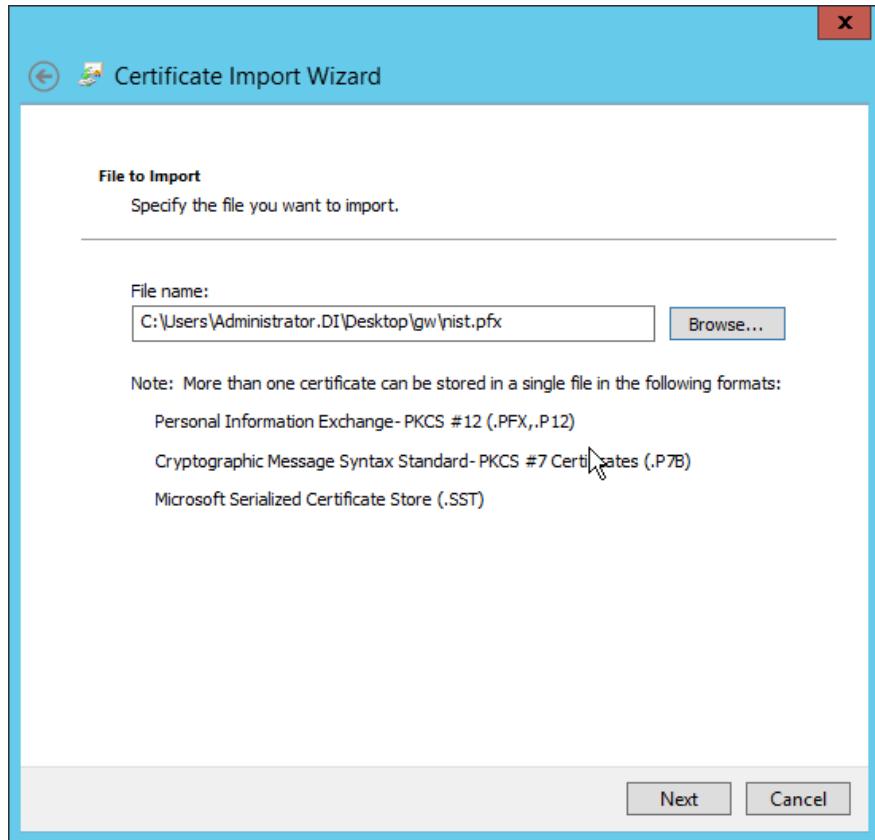
1031 19. Re-open the certificate import wizard but this time for **Trusted Root Certification Authorities**.



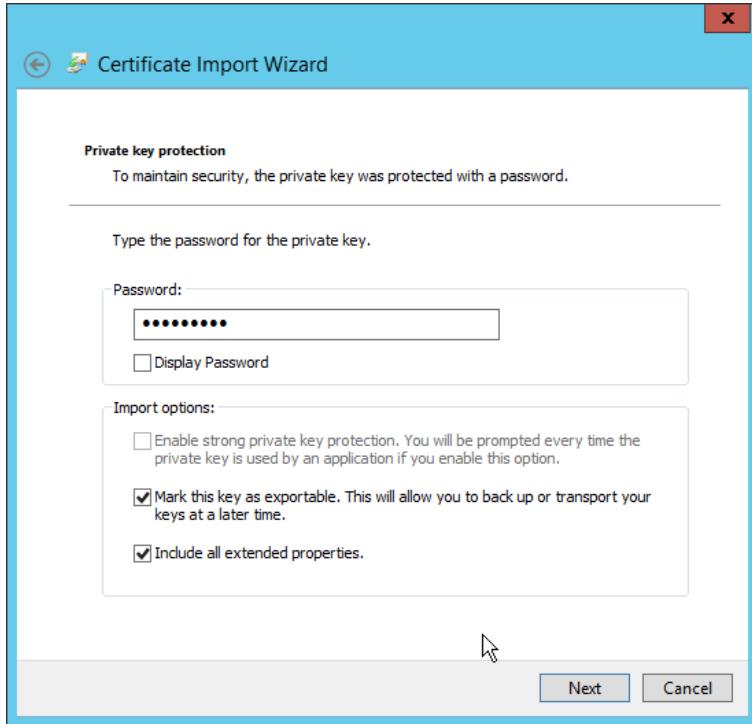
1032

1033 20. Click **Next**.

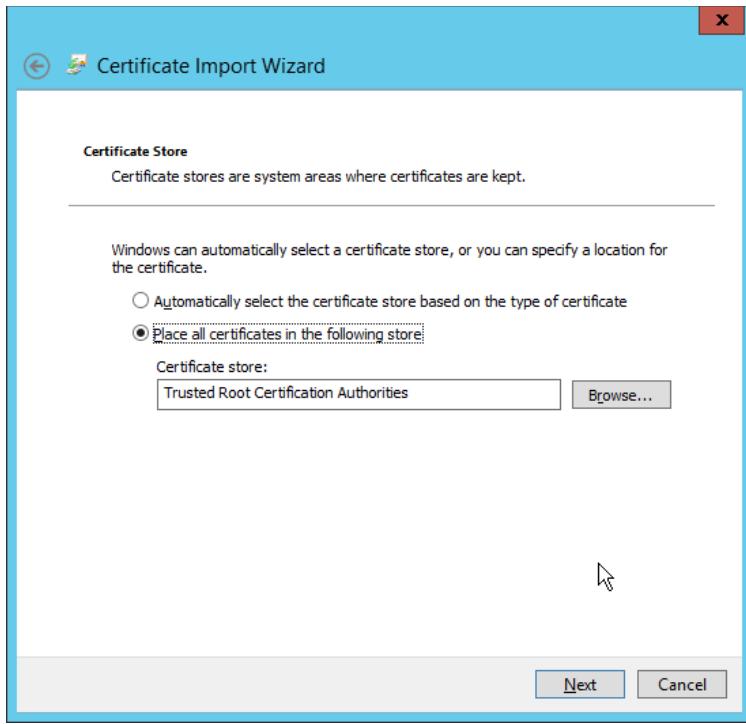
1034 21. Select the same certificate.



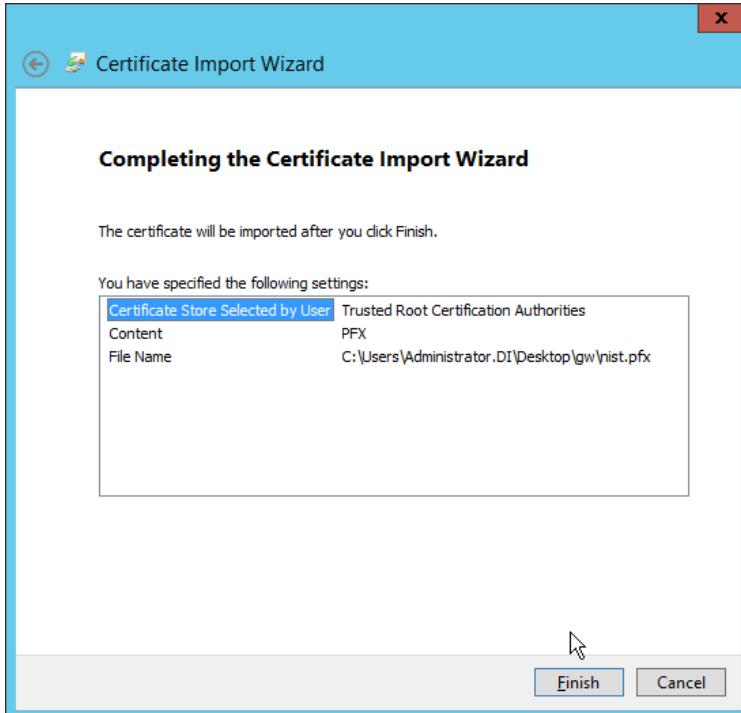
- 1035
1036 22. Click **Next**.
1037 23. Enter the certificate's **password**.
1038 24. Check the box next to **Mark this key as exportable**.

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.



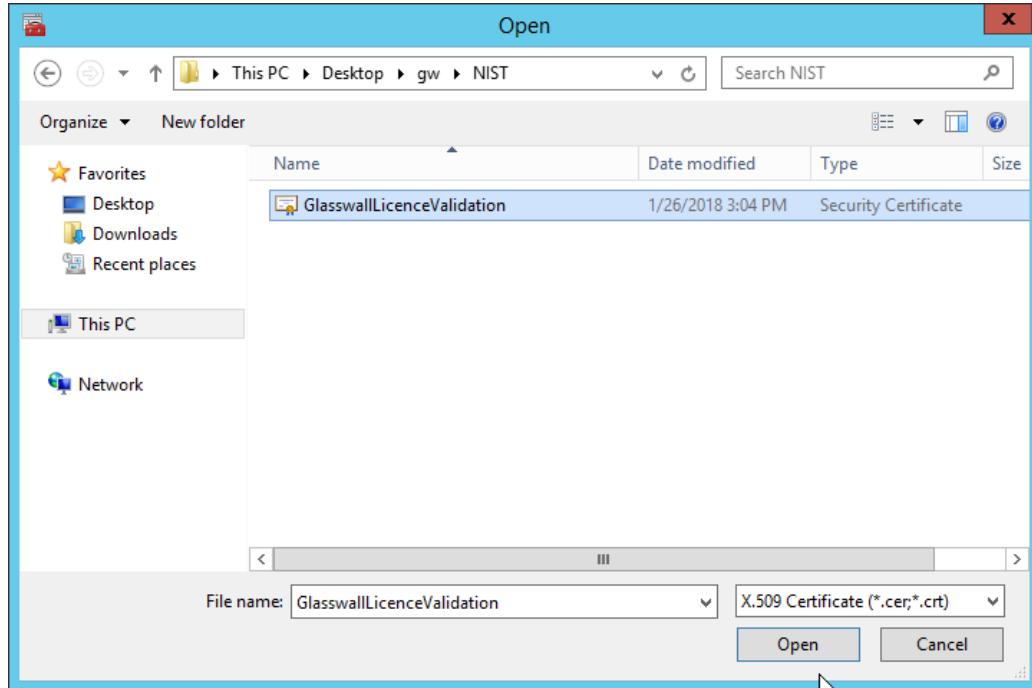
1046

1047

29. Click **Next**.

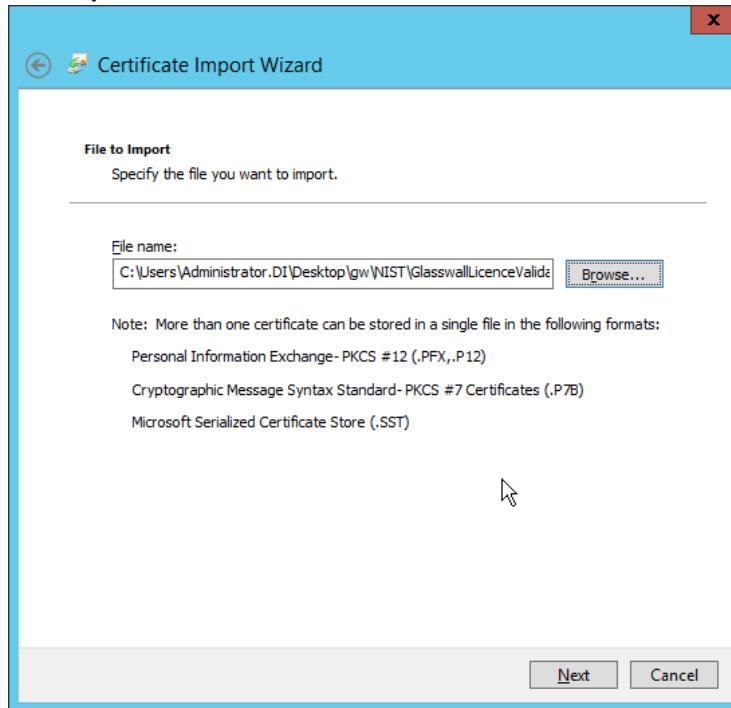
1048

30. Browse to the **GlasswallLicenseValidation** certificate.



1049

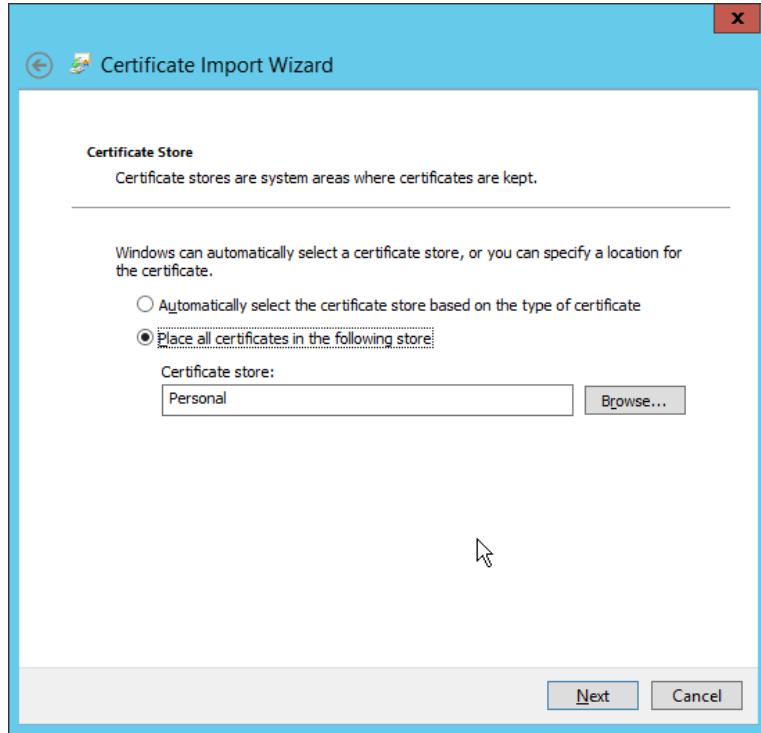
31. Click **Open**.



1051

1052

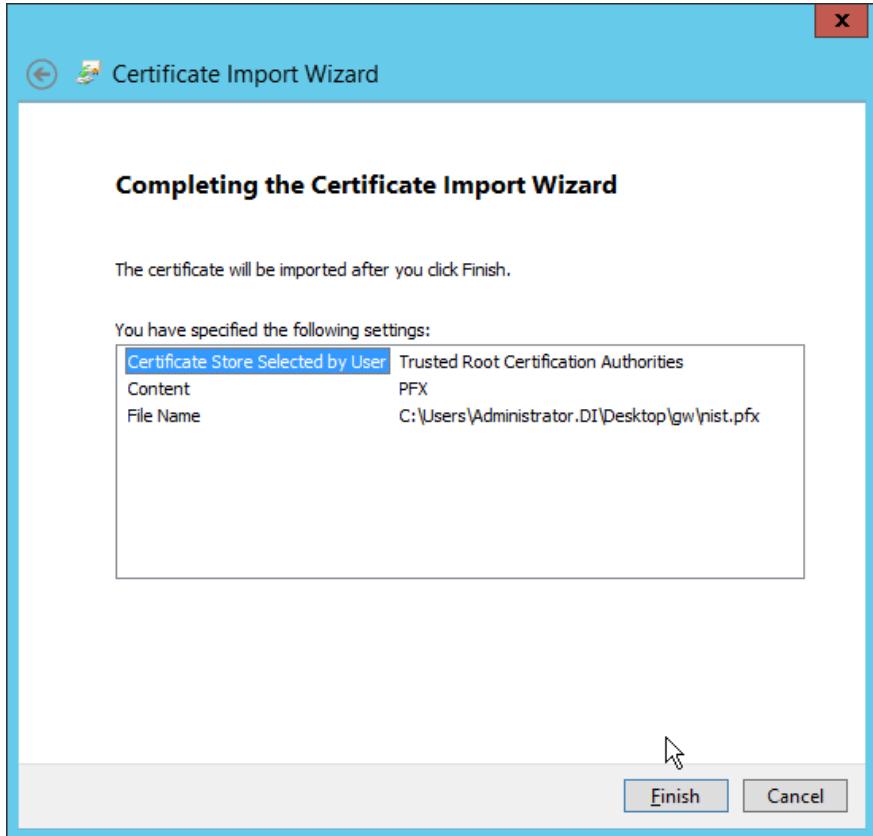
32. Click **Next**.



1053

1054

33. Click **Next**.



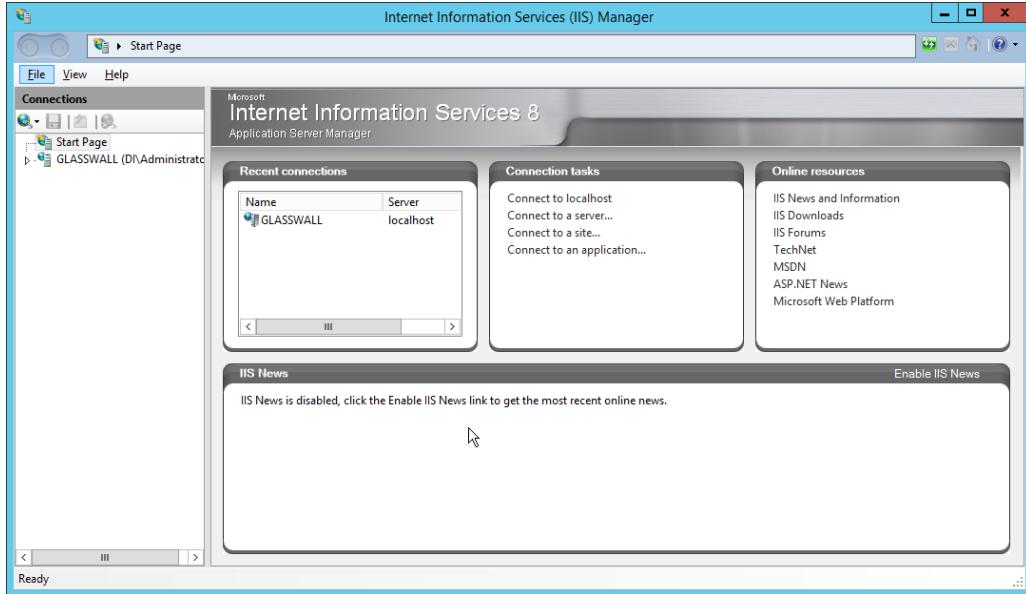
1055

1056

1057

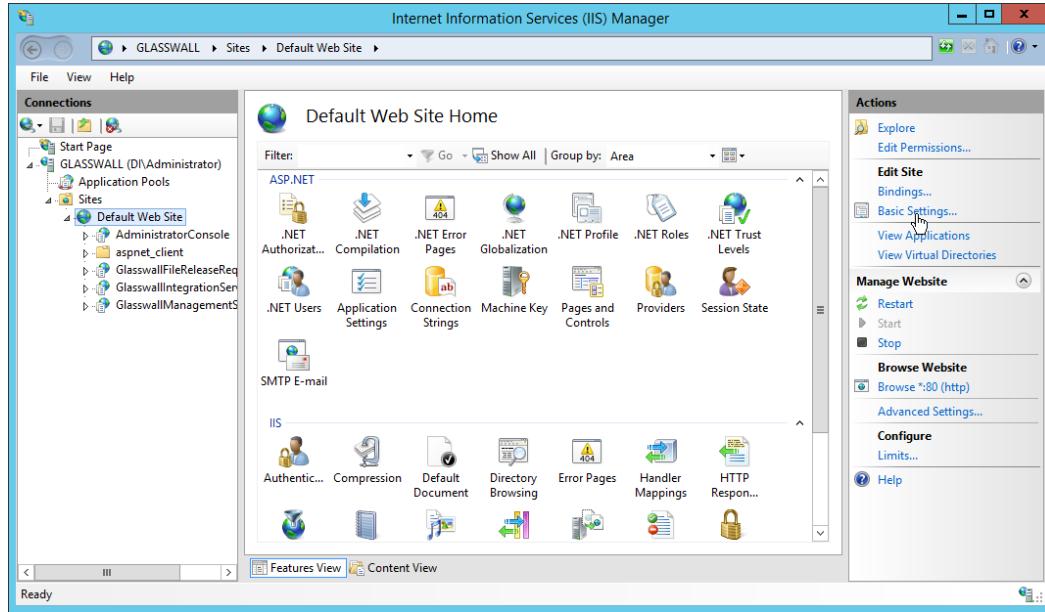
34. Click **Finish**.

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



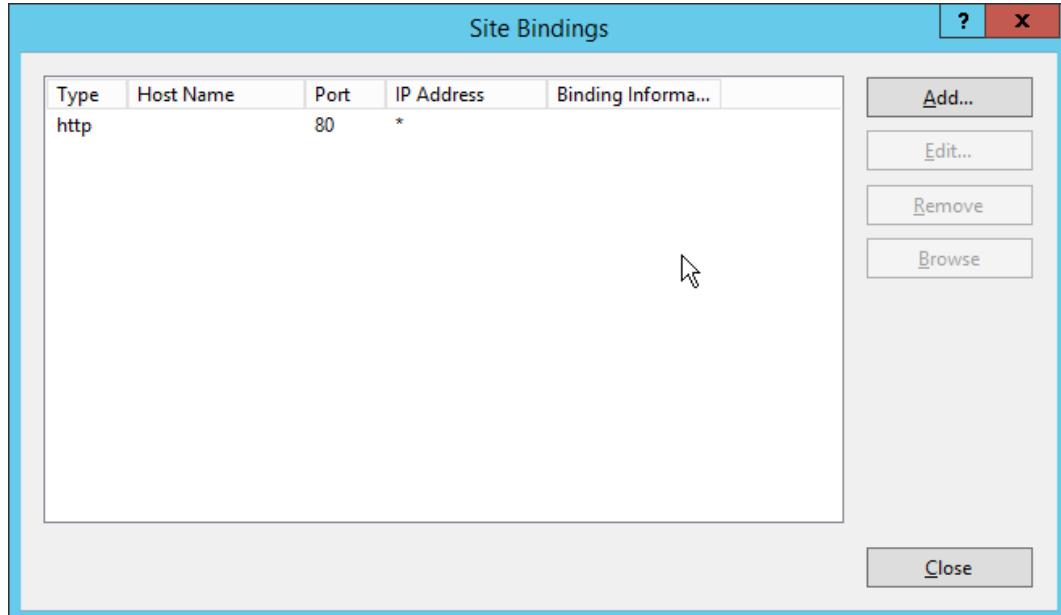
1058

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

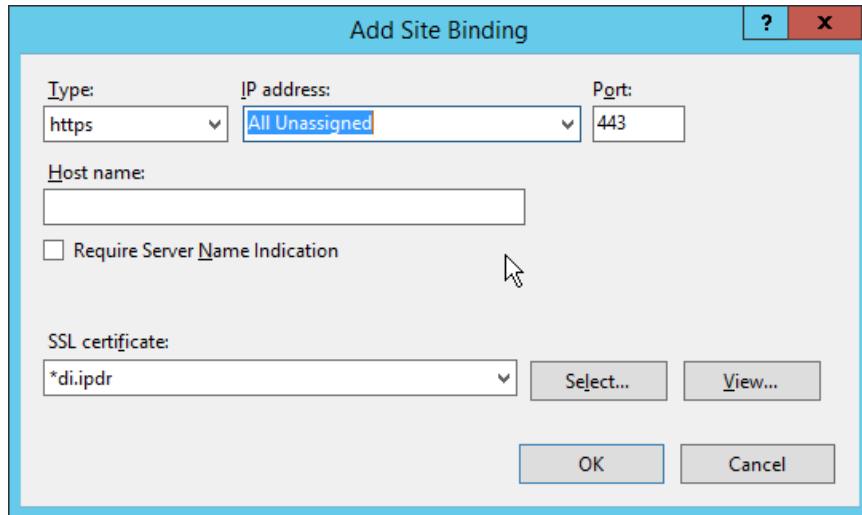
39. Select **https** for the **Type**.

1065

40. Select **All Unassigned** for **IP address**.

1066

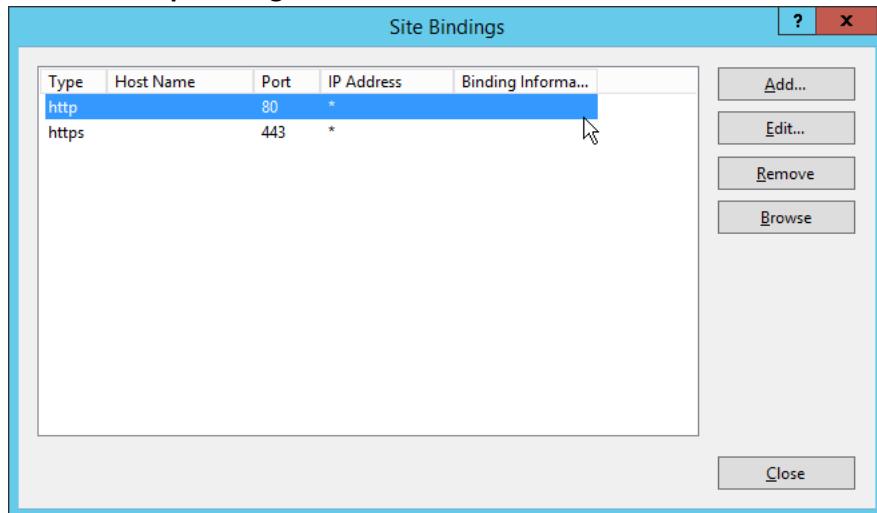
41. Select the **domain certificate** for **SSL certificate**.



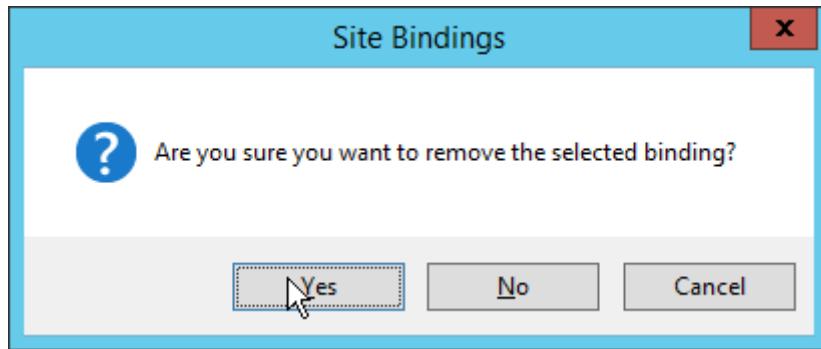
1067

42. Click **OK**.

1068

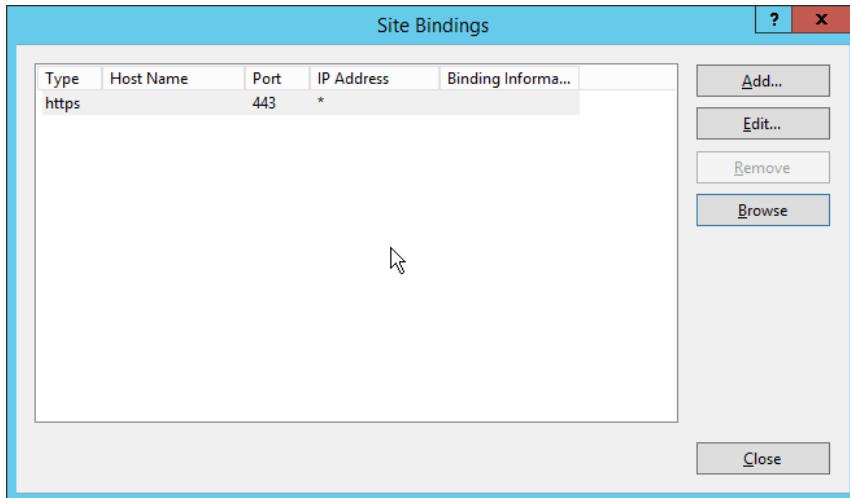
43. Select the **http binding**.

1069

44. Click **Remove**.

1070

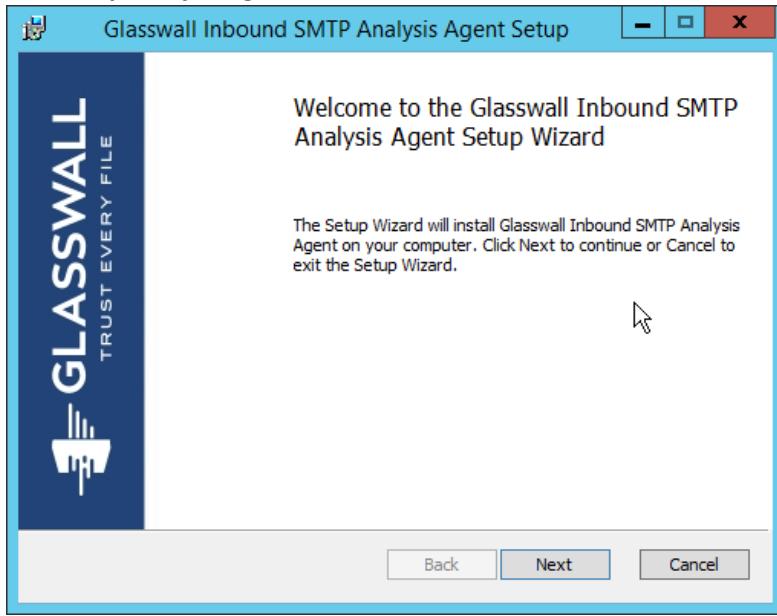
45. Click **Yes**.



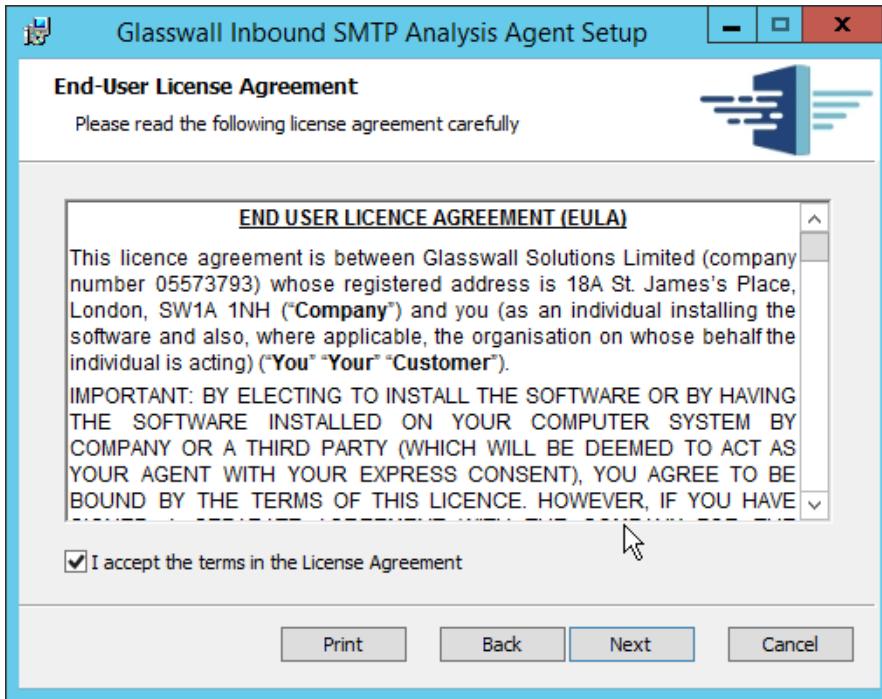
- 1074
1075 46. Click **Close**.
1076 47. Restart the IIS server. The Glasswall FileTrust console should now be accessible through a
1077 browser. (For example, <https://glasswall.di.ipdr/AdministratorConsole>). Ensure that there are
1078 no certificate errors.

2.7.2.5 *Install the Smtp Analysis Agent*

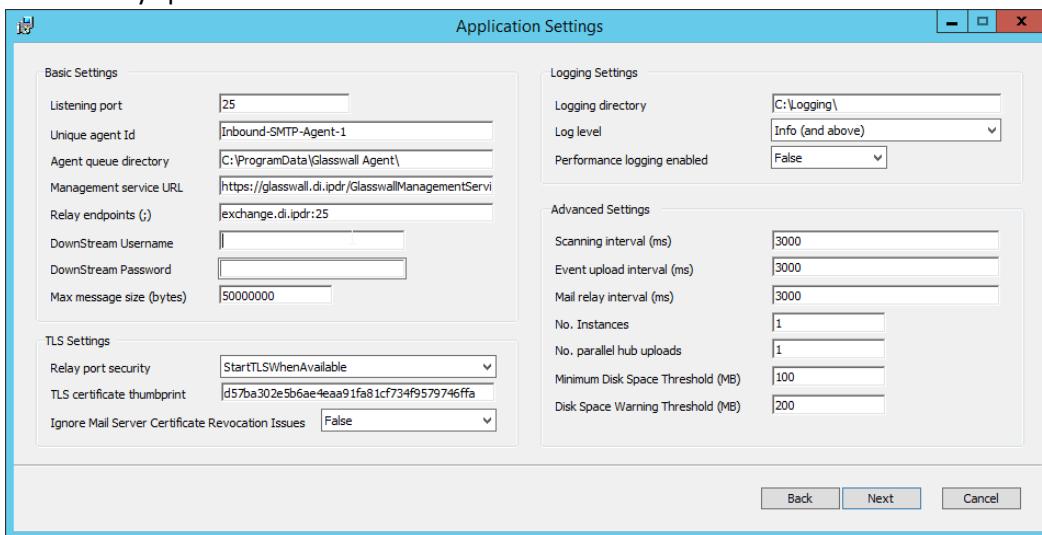
- 1080 1. Run **SmtpAnalysisAgentInstaller.msi**.



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



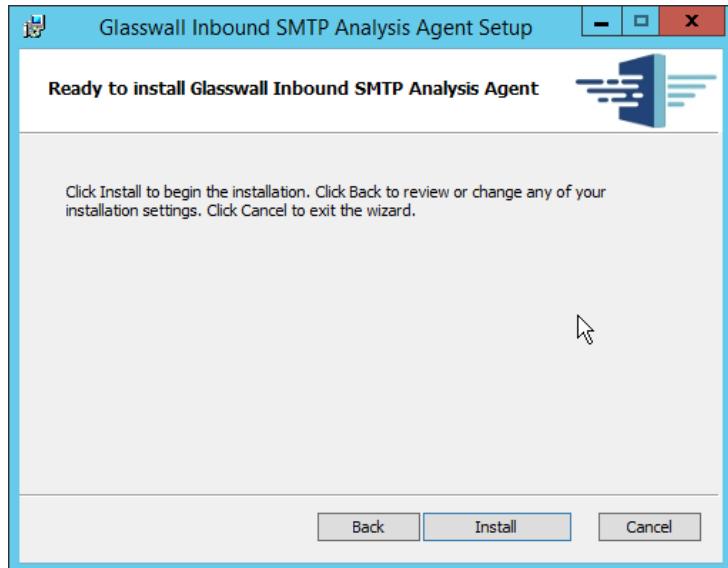
1084
1085 4. Click Next.
1086 5. For Listening port, enter 25.
1087 6. For Management service URL, correct the domain to be the web domain of the IIS server (for
1088 example, glasswall.di.ipdr).
1089 7. For the Relay endpoints, enter the address of the Exchange server, followed by the port (for
1090 example, exchange.di.ipdr:25).
1091 8. For the TLS certificate thumbprint, enter the value from the thumbprint field on the certificate,
1092 without any spaces.



1093

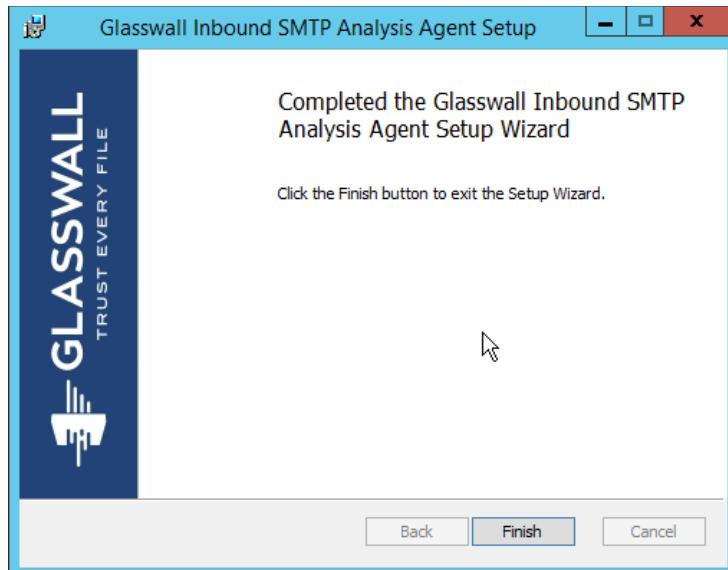
1094

9. Click **Next**.



1095
1096

10. Click **Install**.



1097
1098

11. Click **Finish**.

1099

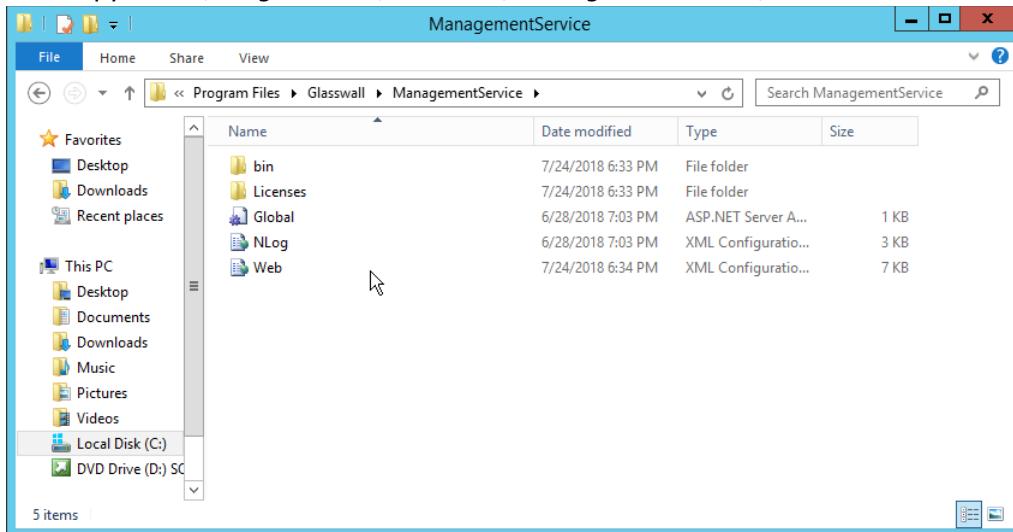
2.7.2.6 Distribute the Glasswall License File

1100
1101

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

1102
1103

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

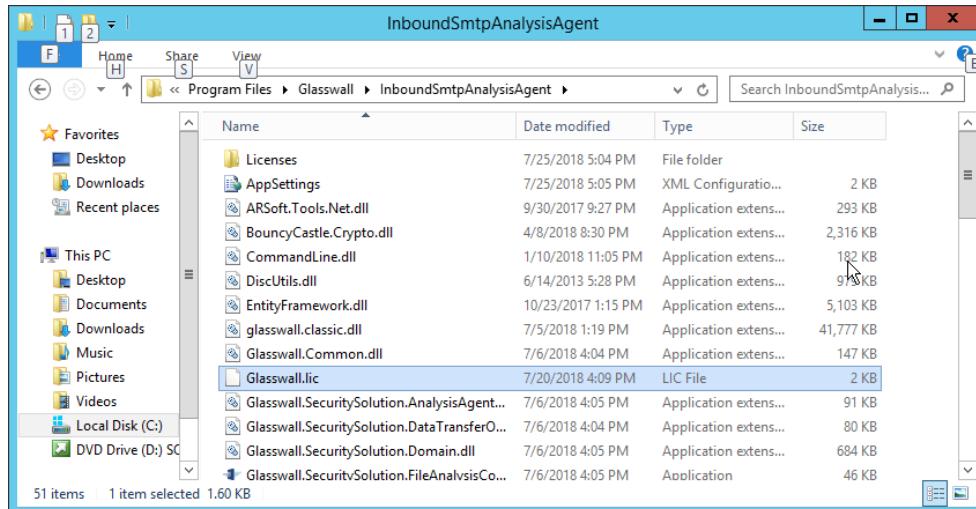


1104
1105

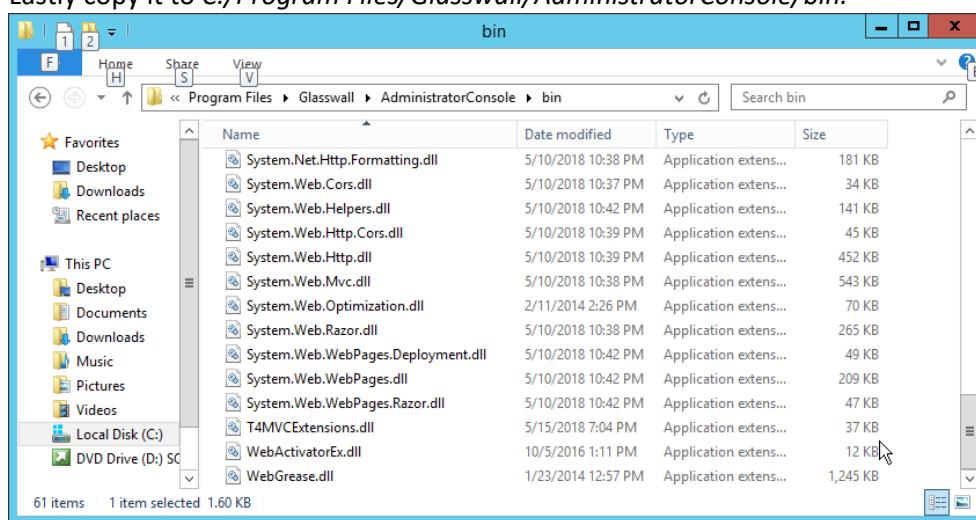
3. Then copy it to *C:/Program Files/Glasswall/InboundSmtpAnalysisAgent*.

1106
1107

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



1108



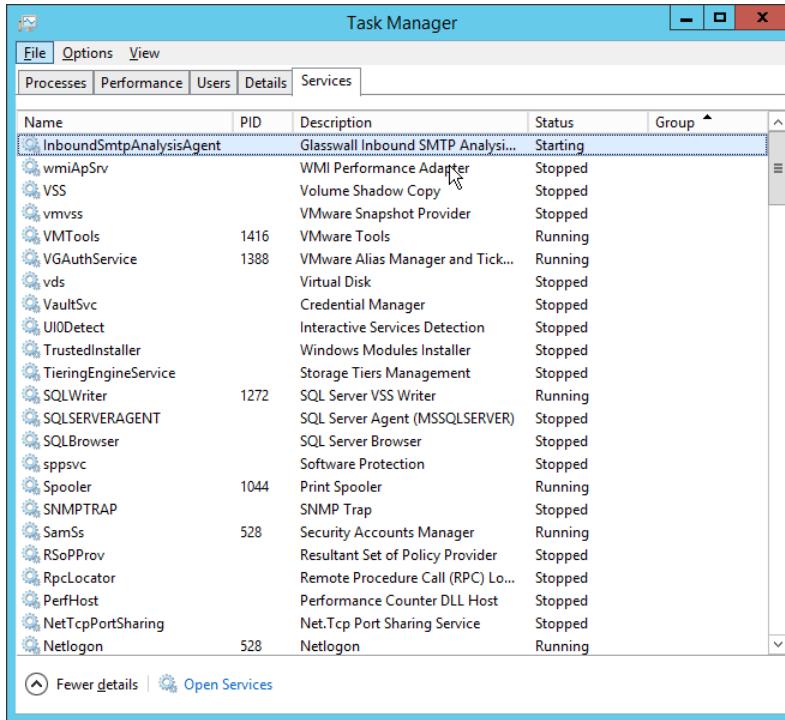
1109

2.7.3 Configure Glasswall FileTrust

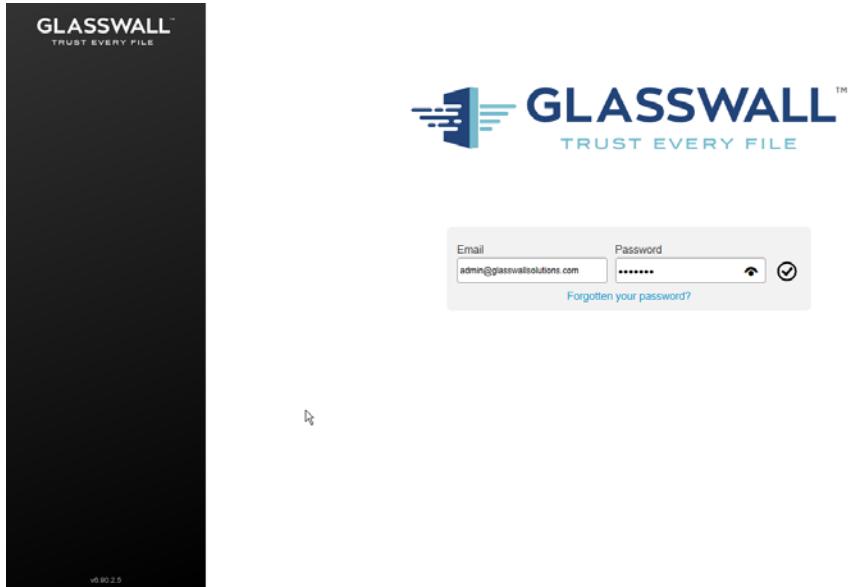
- 1110 Please see <https://docs.glasswallsolutions.com/#Configuring/Office%20365%20Integration.htm> for an example configuration that routes email with attachments from Office365 to Glasswall FileTrust.
- 1111 Glasswall then forwards email back to Office365, after processing. Note that this linked configuration does not work with on-premise Exchange setups.
- 1112 Instead, to achieve the goal of routing email through Glasswall, we redirect local MX records to Glasswall FileTrust. We implemented it this way because of limitations of the lab environment, but organizations should consult with the vendor for the best solution to route email through the email 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
- 1122 3. Close Task Manager.
- 1123 4. Open a browser and navigate to the **Glasswall Administration Console** (for example, <http://glasswall.di.ipdr/AdministratorConsole>).
- 1124
- 1125 5. If this is the first time logging in, the default account will be **admin@glasswallsolutions.com**, and the password is **Welcome1?**.
- 1126

1127
1128

6. Log in using these credentials.

Supported File Types		Other File Types	
Files 0	Sanitised / Remediated 0	Files 0	

Outbound Emails	
Total Emails 0	Total Files 0

Supported File Types		Other File Types	
Files 0	Sanitised / Remediated 0	Files 0	

Inbound SMTP Agent Status				
Active 1	Inactive 0	Inbound Queues 0	Scan Queues 0	Inspection Queues 0
Outbound Queues 0	Reporting Queues 0	Failed Queues 0	Unprocessable Queues 0	

Outbound SMTP Agent Status				
Active 0	Inactive 0	Inbound Queues 0	Scan Queues 0	Inspection Queues 0
Outbound Queues 0	Reporting Queues 0	Failed Queues 0	Unprocessable Queues 0	

1129
1130

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

Accounts

Name	Email	Security Group	Account Locked
Administrator	admin@glasswallsolutions.com	Principal Administrator	

Security Groups

Name	Security Roles
Principal Administrator	View Inbound Policy Catalogue Edit Inbound Policy Catalogue Request Publish of Inbound Policy Catalogue Approve Publish of Inbound Policy Catalogue View Outbound Policy Catalogue Edit Outbound Policy Catalogue Request Publish of Outbound Policy Catalogue Approve Publish of Outbound Policy Catalogue Account Administration Export Retained File Delete Retained File Approve File Release Request Request File Release View System Configuration Edit System Configuration Create Reports
Standard User	

Add Edit Delete

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**.

Create Account

Name	Administrator
Email	Administrator@di.ipdr
Security Group	Principal Administrator

Activate Windows
Go to System in Control Panel to activate Windows.

1135
1136

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

Name	Email	Security Group	Account Locked
Administrator	admin@glasswallsolutions.com	Principal Administrator	
Administrator	Administrator@di.ipdr	Principal Administrator	

Name	Security Roles
Principal Administrator	View Inbound Policy Catalogue Edit Inbound Policy Catalogue Request Publish of Inbound Policy Catalogue Approve Publish of Inbound Policy Catalogue View Outbound Policy Catalogue Edit Outbound Policy Catalogue Request Publish of Outbound Policy Catalogue Approve Publish of Outbound Policy Catalogue Account Administration Export Retained File Delete Retained File Approve File Release Request Request File Release View System Configuration Edit System Configuration Control Panel to activate Windows. Create Reports

1137
1138

12. The new administrator account should be created.

Your account has been created

Administrator@DI.PDR To: Administrator; <#>

Mik Un
hey hey lookie 3:37 PM
No preview is available.

Mik Un
(No subject) 11:23 PM
Tue 7/25/2018
No preview is available.

Mik Un
testing omg 11:23 PM
asdfghjklzxcvbnm
Tue 7/25/2018
From...

Mik Un
please work 11:22 PM
Tue 7/25/2018
No preview is available.

Mik Un
223542345 11:22 PM
Tue 7/25/2018
No preview is available.

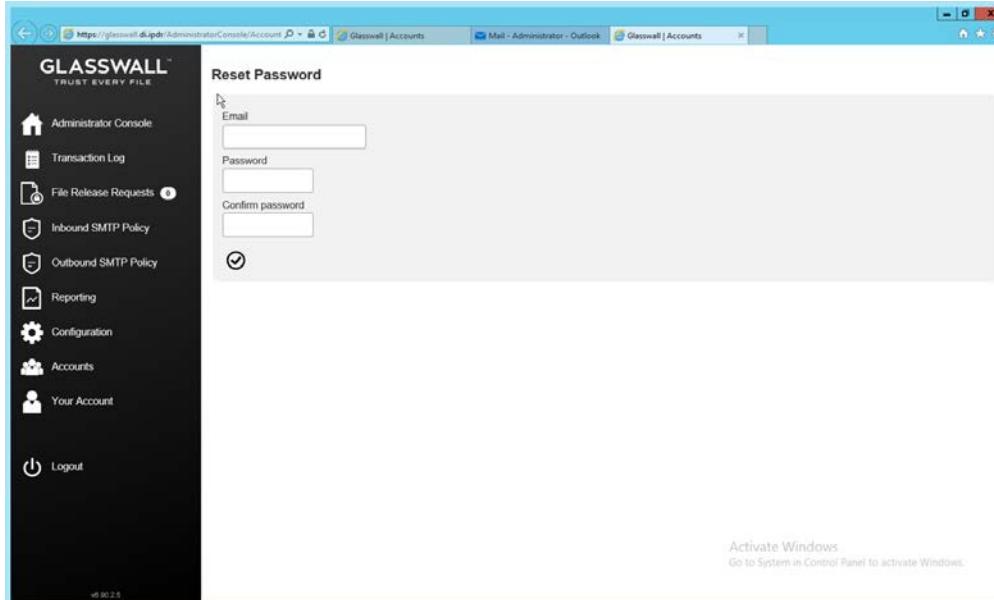
Mik Un
(No subject) 11:21 PM
Tue 7/25/2018

Would you like to store your password for exchange? [More info](#)

GLASSWALL™
Account Created
Your account has been created. Please confirm your email address and set up a password by clicking [here](#).
© 2018 Glasswall Solutions TRUST EVERY FILE

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.

Name	Email	Security Group	Account Locked
Administrator	admin@glasswallsolutions.com	Principal Administrator	
Administrator	Administrator@di.ipdr	Principal Administrator	

Name	Security Roles
Principal Administrator	View Inbound Policy Catalogue Edit Inbound Policy Catalogue Request Publish of Inbound Policy Catalogue Approve Publish of Inbound Policy Catalogue View Outbound Policy Catalogue Edit Outbound Policy Catalogue Request Publish of Outbound Policy Catalogue Approve Publish of Outbound Policy Catalogue Account Administration Export Retained File Delete Retained File Approve File Release Request Request File Release View System Configuration Edit System Configuration Create Reports
Standard User	Activate Windows Go to System in Control Panel to activate Windows.

1146
1147

17. Click **Delete**.

Name	Email	Security Group	Account Locked
Administrator	Administrator@di.ipdr	Principal Administrator	

Name	Security Roles
Principal Administrator	View Inbound Policy Catalogue Edit Inbound Policy Catalogue Request Publish of Inbound Policy Catalogue Approve Publish of Inbound Policy Catalogue View Outbound Policy Catalogue Edit Outbound Policy Catalogue Request Publish of Outbound Policy Catalogue Approve Publish of Outbound Policy Catalogue Account Administration Export Retained File Delete Retained File Approve File Release Request Request File Release View System Configuration Edit System Configuration <small>Create Reports</small> <small>Go to System in Control Panel to activate Windows.</small>
Standard User	

- 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.

The hostname to be used in hyperlinks within notification emails: https://glasswall.di.ipdr /AdministratorConsole

Subject Line: Your file has been released by Glasswall.

Quarantined File Alert: The attached file(s) were quarantined in accordance with Corporate Policy. Please contact IT support for more information.

Subject Line: The subject of the email used to release a file.

Body: The content of the email used to release a file.

Mail Footer Text: This mail has been protected by Glasswall.

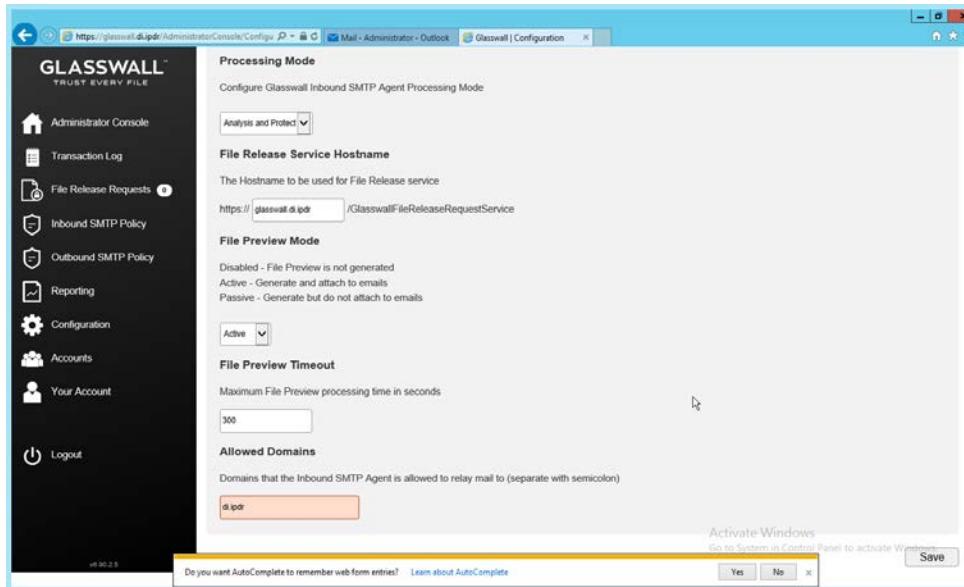
Subject Line: The subject of the email used to notify user of a file release denial.

Body: The content of the email used to deny a file release.

File Release Denied Notification: The following file(s) have been denied for release in accordance with organisation policy. %ReleaseDetails%
Please contact IT support for more information.

- 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
 1166 9. Click **Save**.

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
 1181 3. Under **Receiver Groups**, click **Add**.

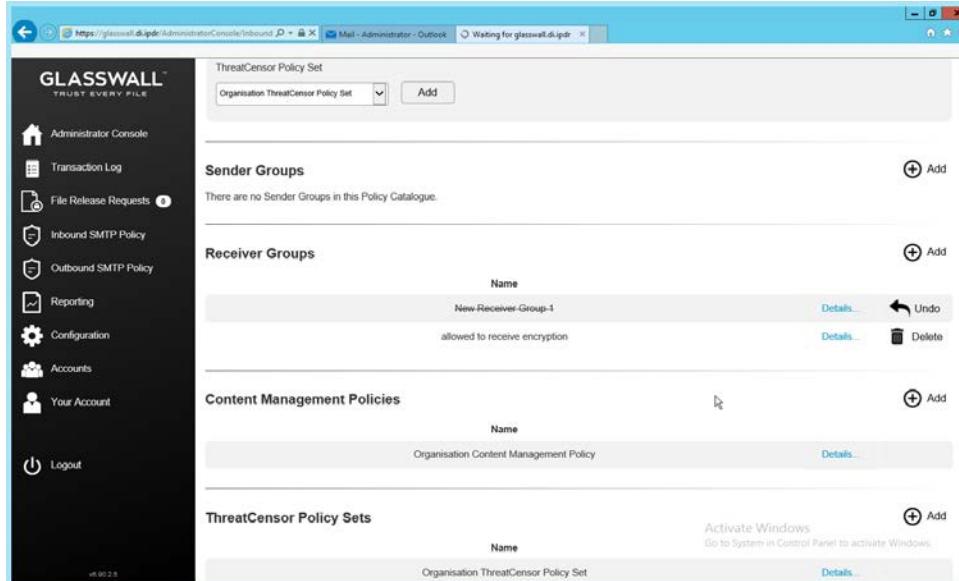
- 1182
 1183 4. Under **User Defined Mailboxes**, click **Edit**.

1184
1185

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

1186
1187
1188

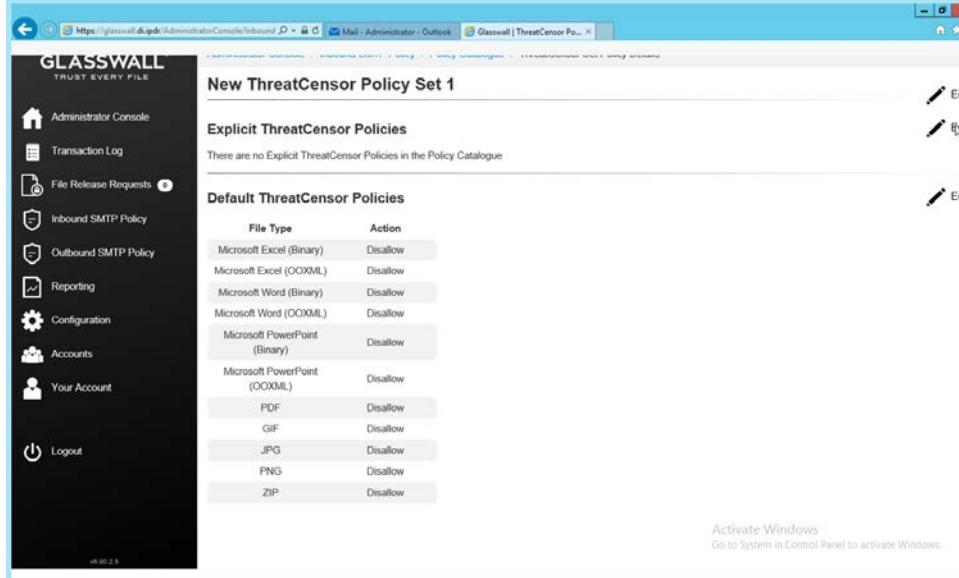
6. Click **Add**.
 7. When finished, return to the **Policy Catalogue** page.



1189

1190 2.7.3.5 *Create a ThreatCensor Policy Set*

- 1191 Under ThreatCensor Policy Sets, click Add.



1192

- 1193 Under Explicit ThreatCensor Policies, click Edit.

1194

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

1198 2.7.3.6 *Create a Processing Rule*

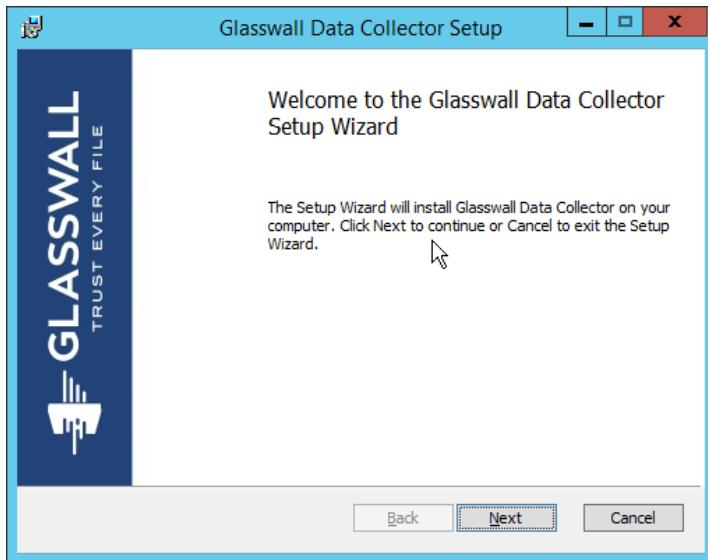
- 1199 1. Under Processing Rules, select the appropriate **Sender Group**, **Receiver Group**, **Content Management Policy**, and **ThreatCensor Policy Set**.
 1200

1201

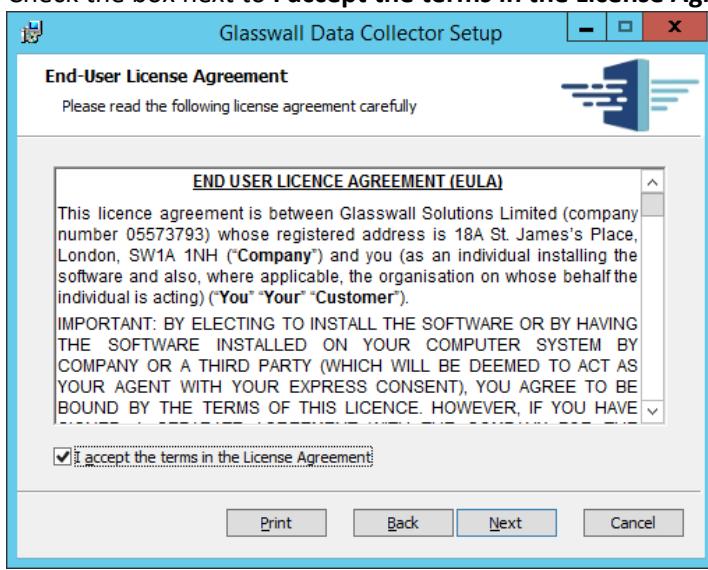
- 1202 2. Click **Add**.
 1203 3. This allows for granular policy for email inspection, quarantine, and reconstruction.

1204 **2.7.4 Configure Intelligence Sharing**

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

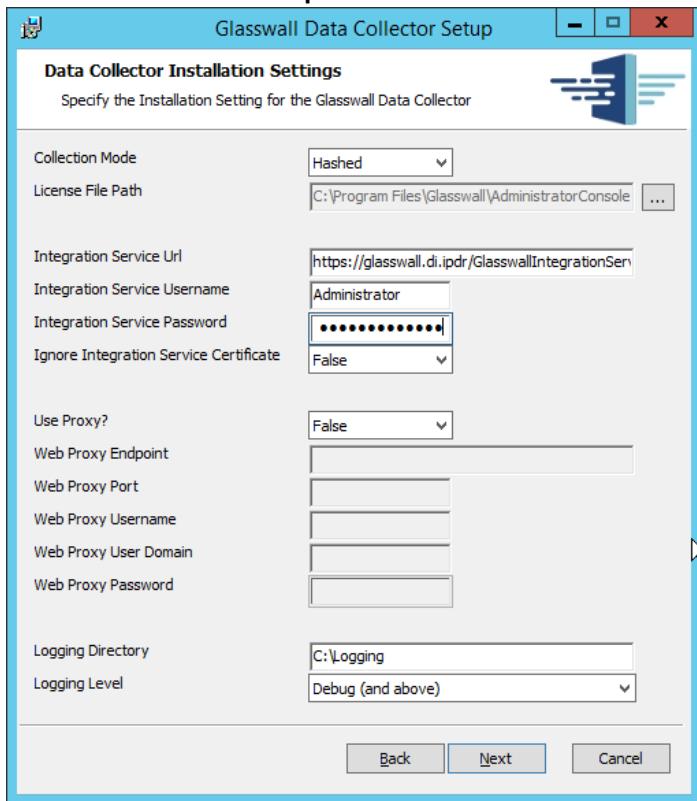


- 1206
 1207 2. Click **Next**.
 1208 3. Check the box next to **I accept the terms in the License Agreement**.

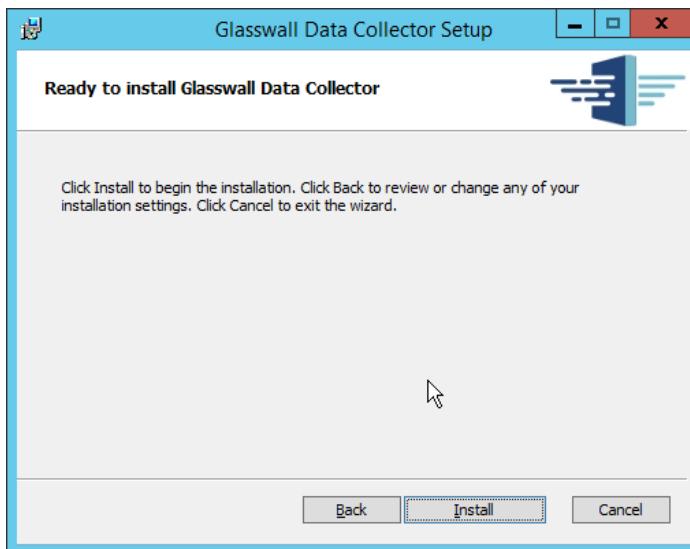


- 1209
 1210 4. Click **Next**.
 1211 5. Select **Hashed for Collection Mode** (especially if your data is sensitive; this will prevent the release of any identifying information).

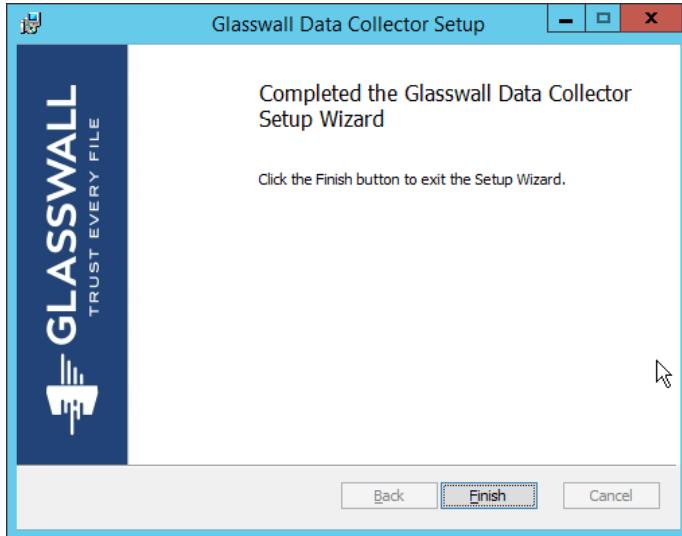
- 1213 6. For **Integration Service Url** replace **localhost** with the name of the computer running the
1214 **Integration Service**.
1215 7. Enter the **username** and **password**.



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



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



1220
1221

10. Click **Finish**.

1222 2.8 Micro Focus ArcSight Enterprise Security Manager

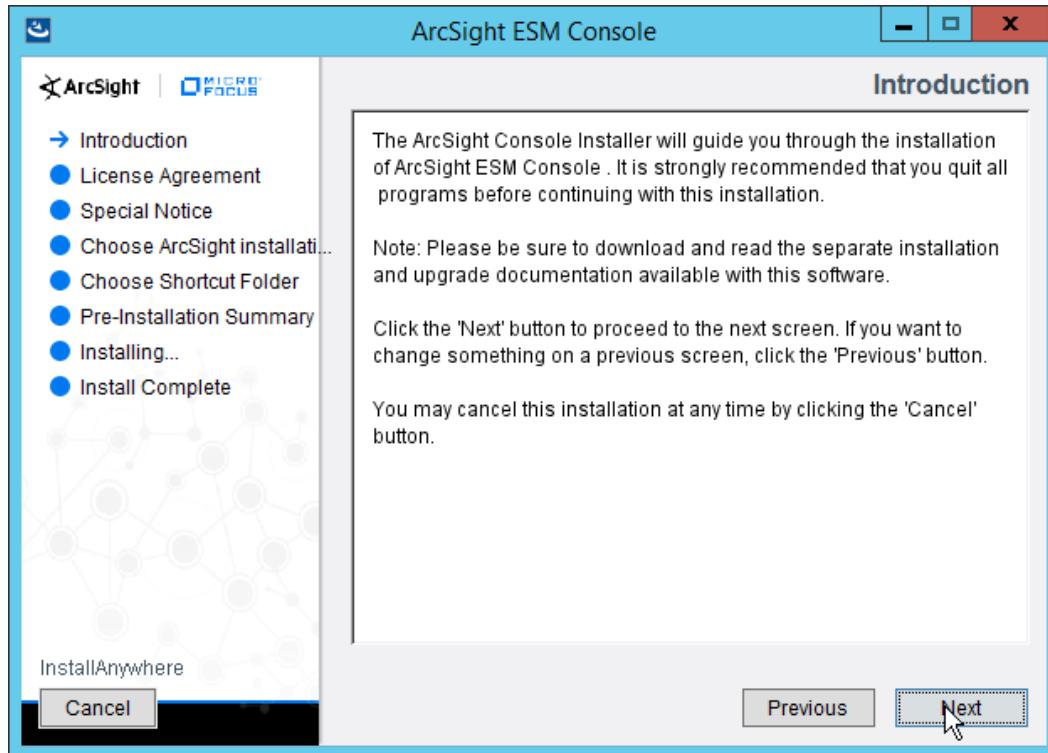
1223 Micro Focus ArcSight Enterprise Security Manager (ESM) is primarily a log collection/analysis tool with
1224 features for sorting, filtering, correlating, and reporting information from logs. It is adaptable to logs
1225 generated by various systems, applications, and security solutions.

1226 This installation guide assumes a pre-configured CentOS 7 machine with ESM already installed and
1227 licensed. This section covers the installation and configuration process used to set up ArcSight agents on
1228 various machines, as well as some analysis and reporting capabilities.

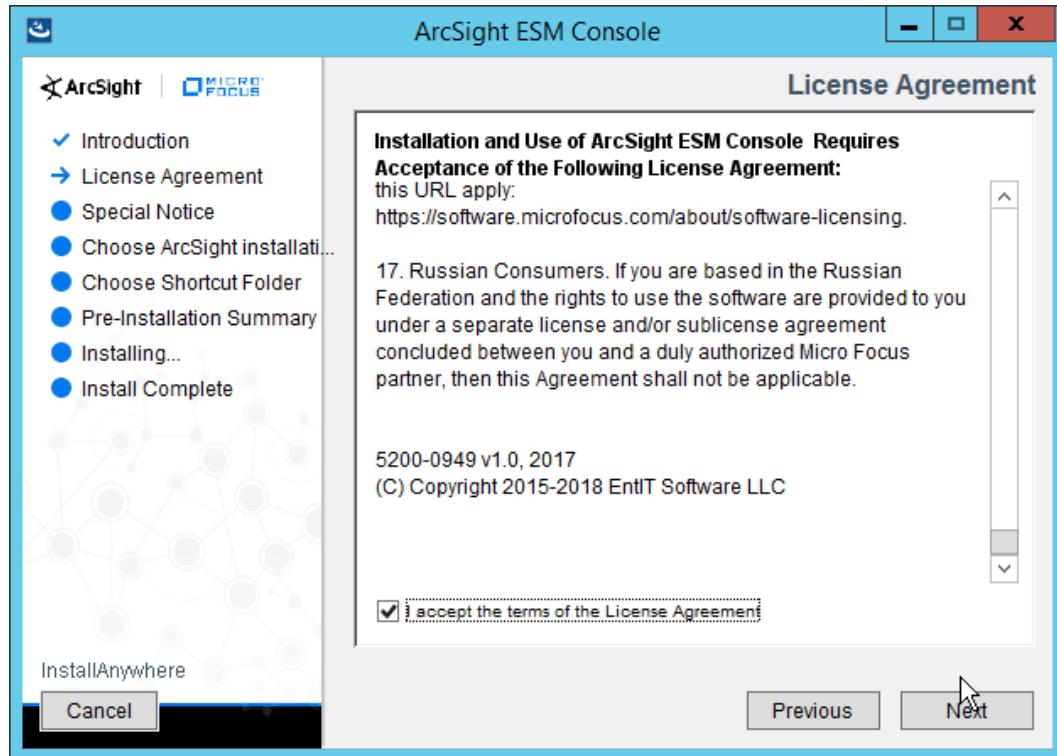
1229 Installation instructions are included for both Windows and UNIX machines, as well as for collecting
1230 from multiple machines. Furthermore, integrations with other products in the build are included in later
1231 sections.

1232 2.8.1 Install the ArcSight Console

1233 1. Run **ArcSight-7.0.0.2436.1-Console-Win.exe**.

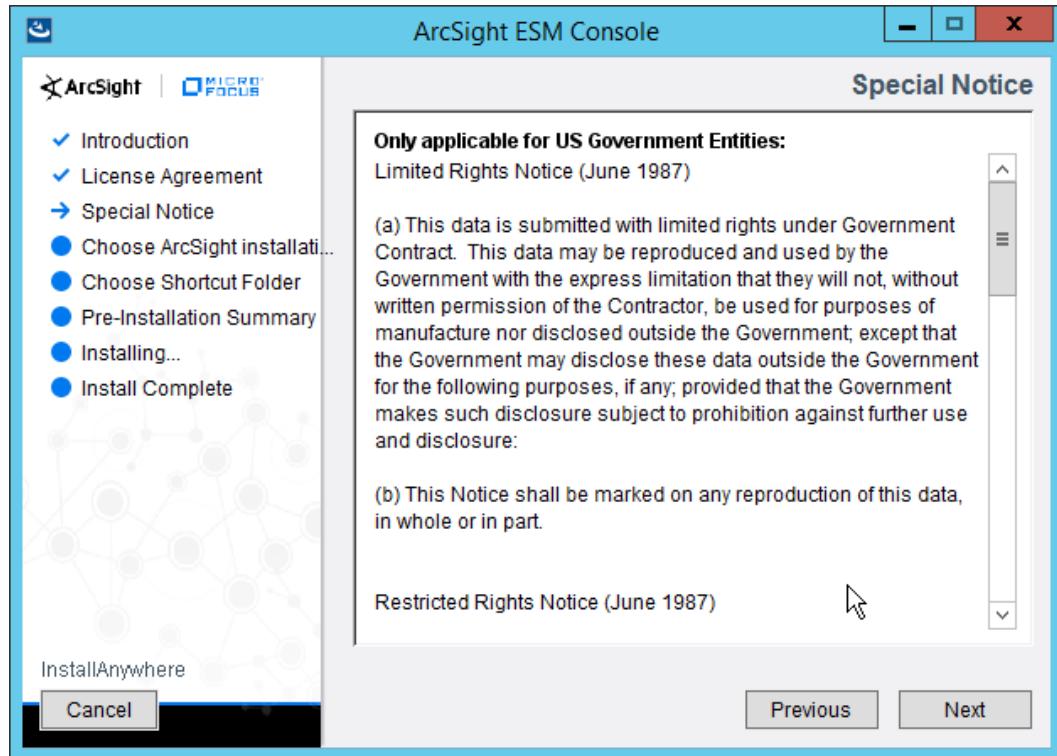


- 1234
1235 2. Click **Next**.
1236 3. Check the box next to **I accept the License Agreement**.



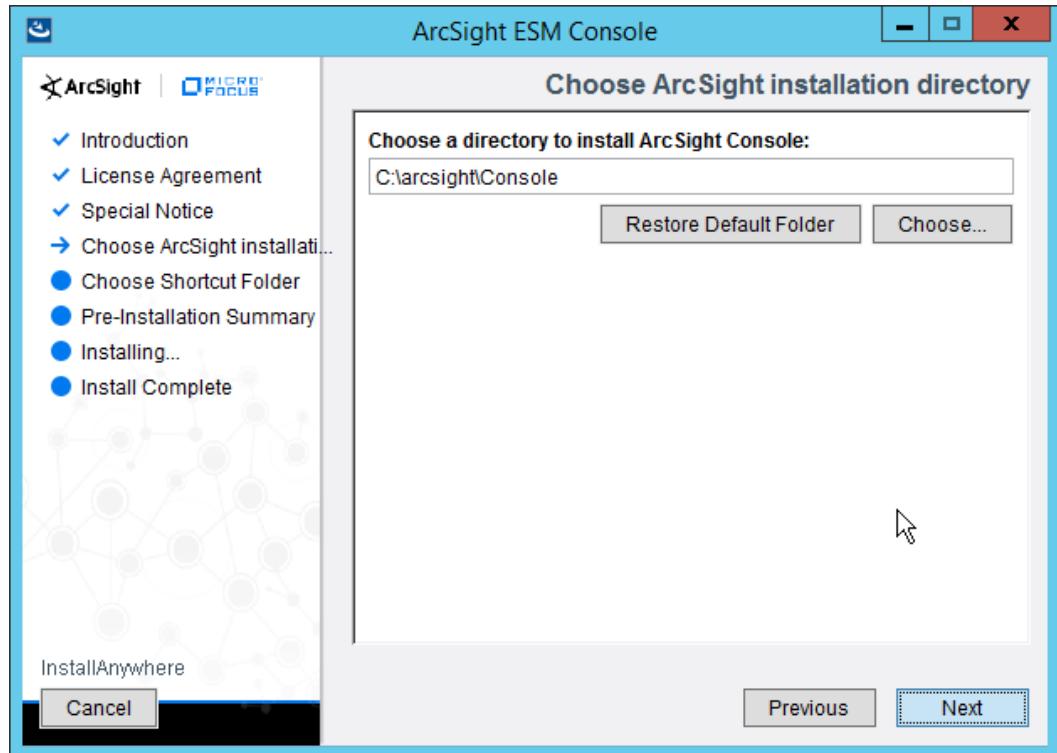
1237
1238

4. Click **Next**.



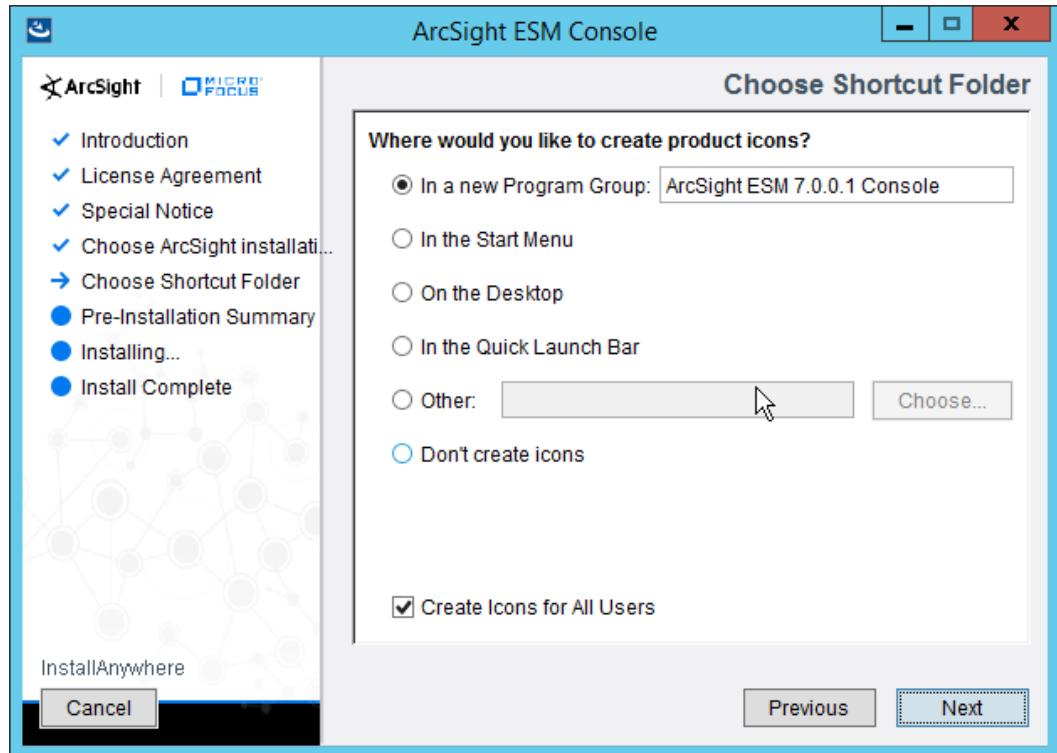
1239
1240

5. Click **Next**.



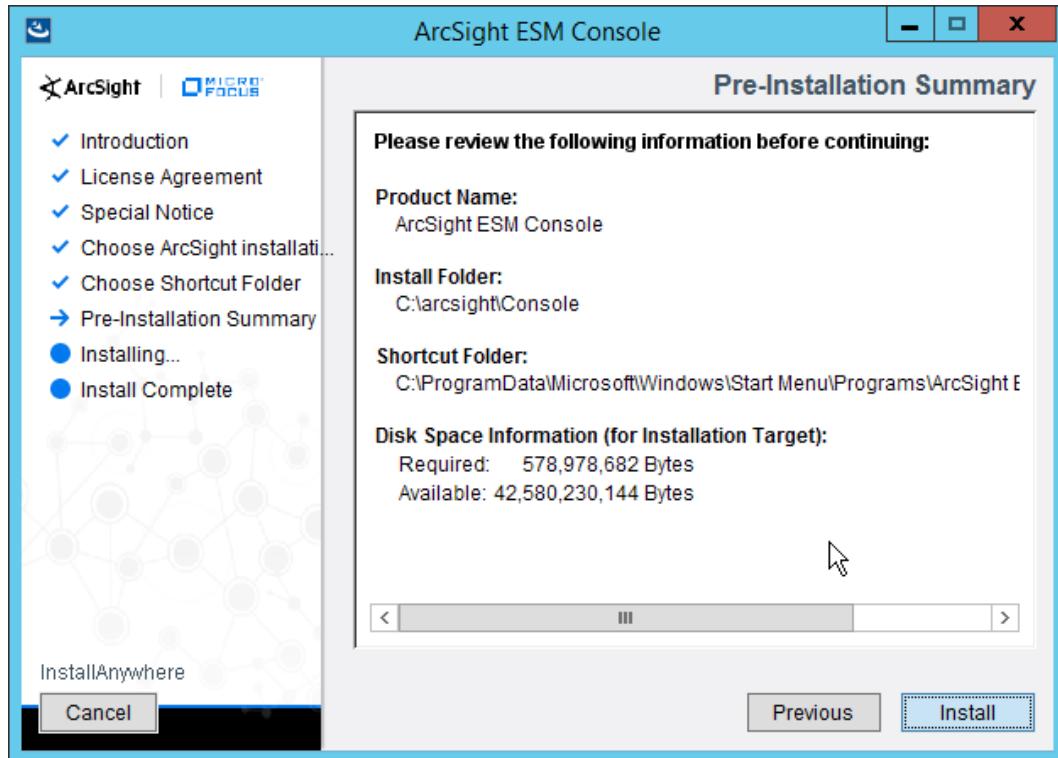
1241
1242

6. Click **Next**.

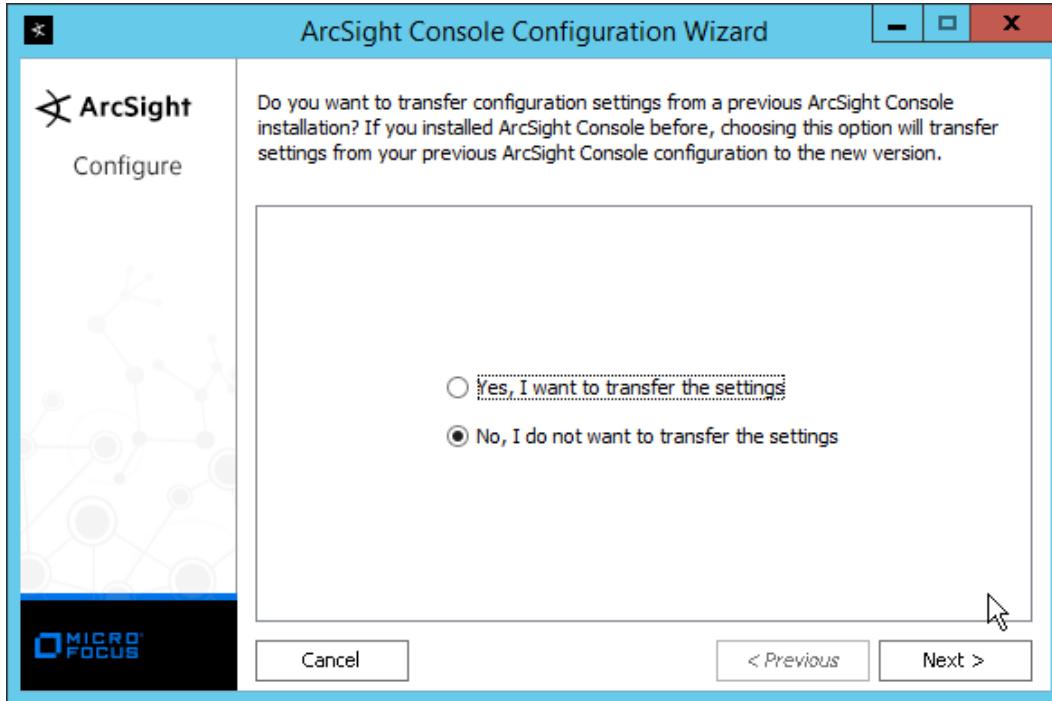


1243
1244

7. Click **Next**.

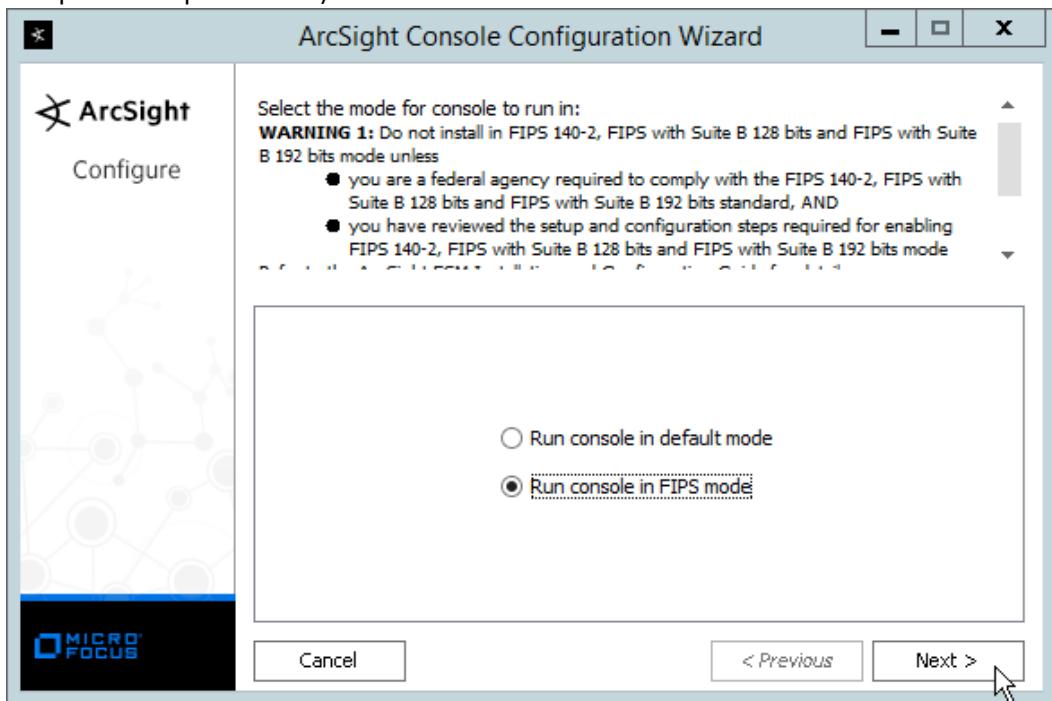


- 1245
1246 8. Click **Install**.
1247 9. Select **No, I do not want to transfer the settings**.



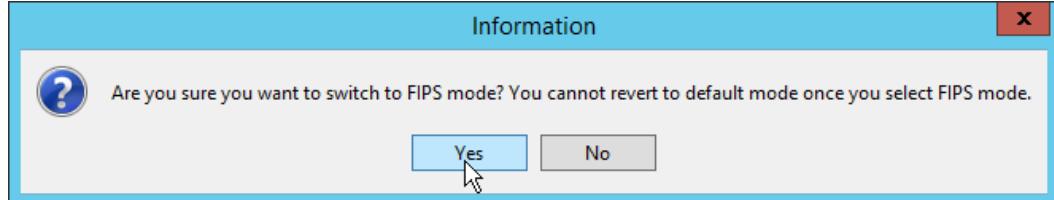
1248
1249
1250
1251

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



1252

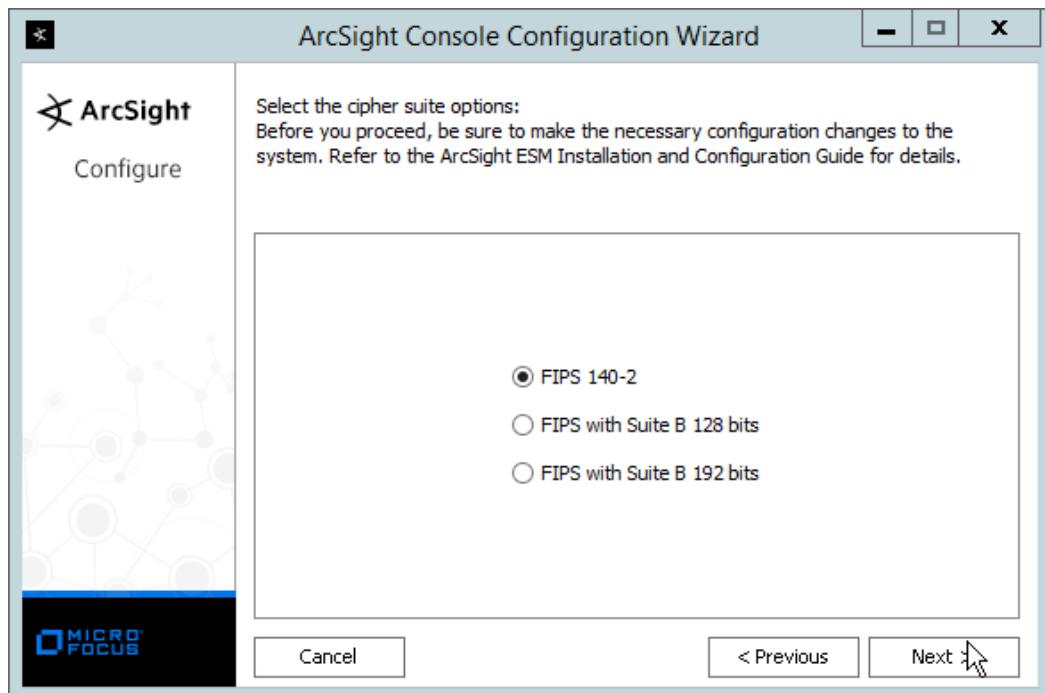
1253 12. Click **Next**.



1254

1255 13. Click **Yes**.

1256 14. Select **FIPS 140-2**.

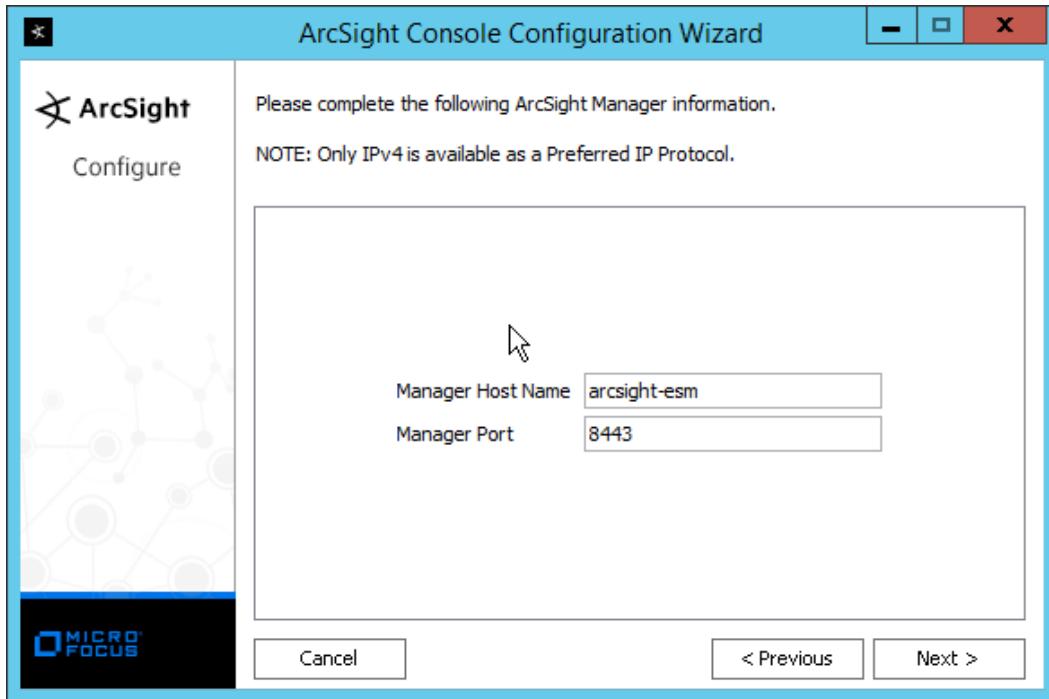


1257

1258 15. Click **Next**.

1259 16. Enter the **hostname** of the ESM server for **Manager Host Name**.

1260 17. Enter the **port** that ESM is running on for **Manager Port** (default: **8443**).



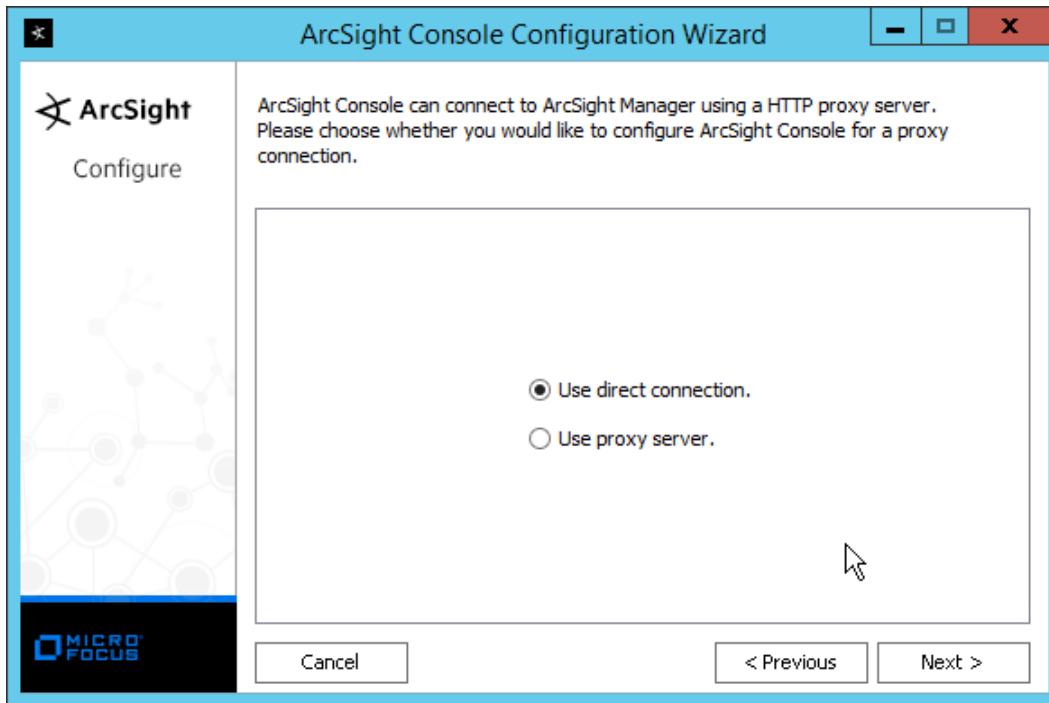
1261

1262

1263

18. Click **Next**.

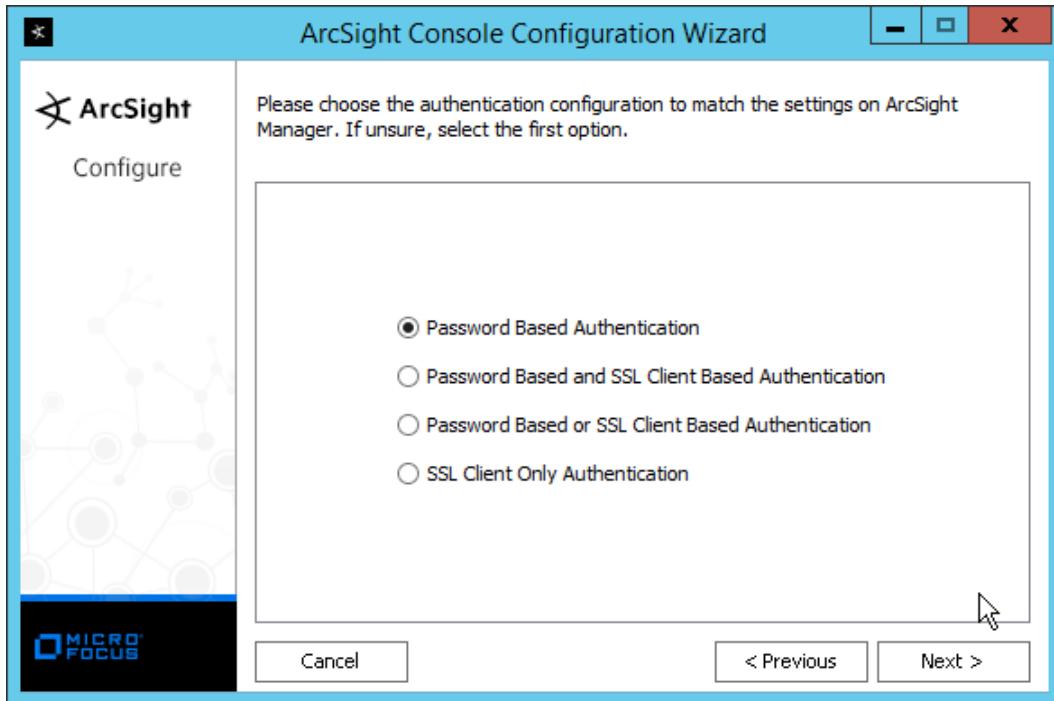
19. Select **Use direct connection**.



1264

1265

20. Click **Next**.

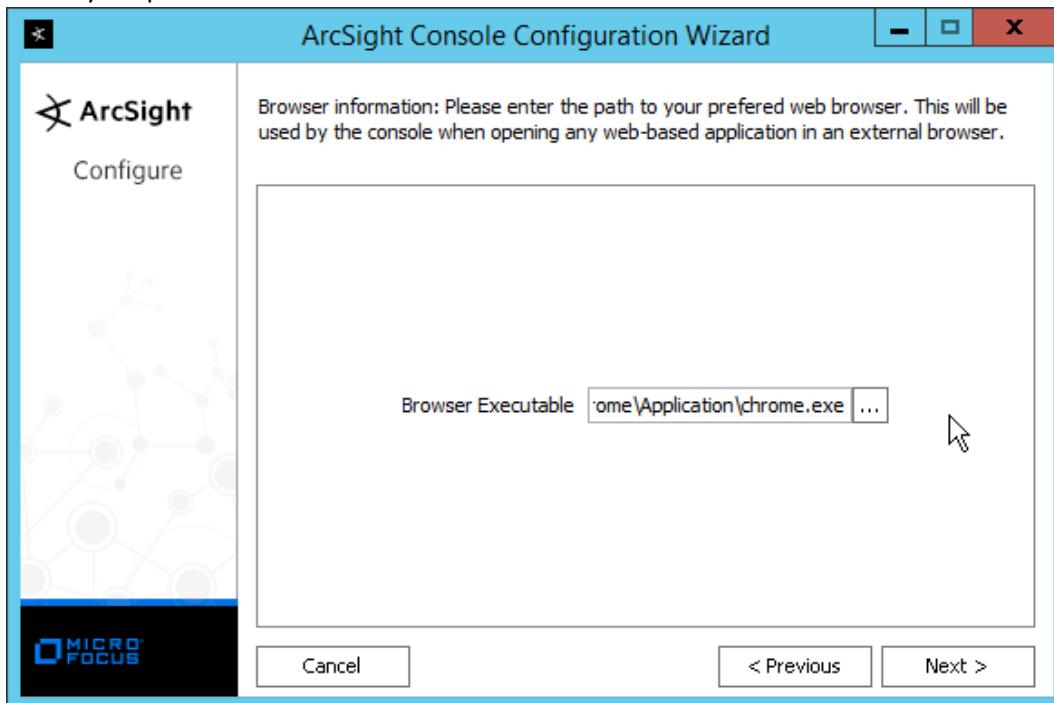


1266

1267

1268

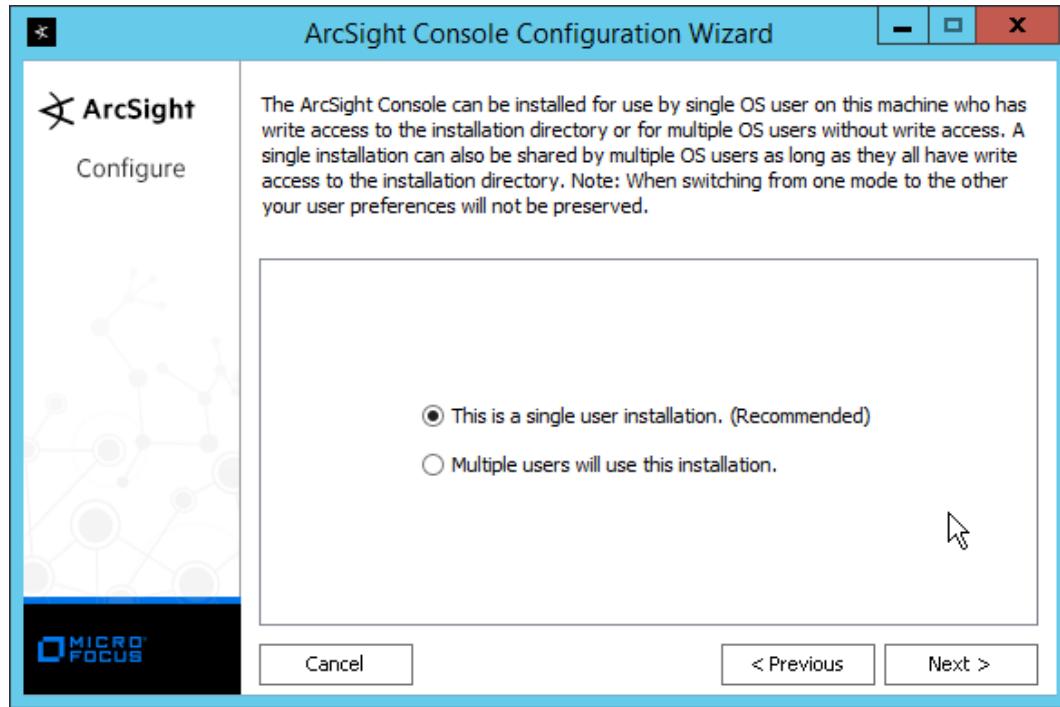
21. Click **Next**.
22. Select your preferred browser.



1269

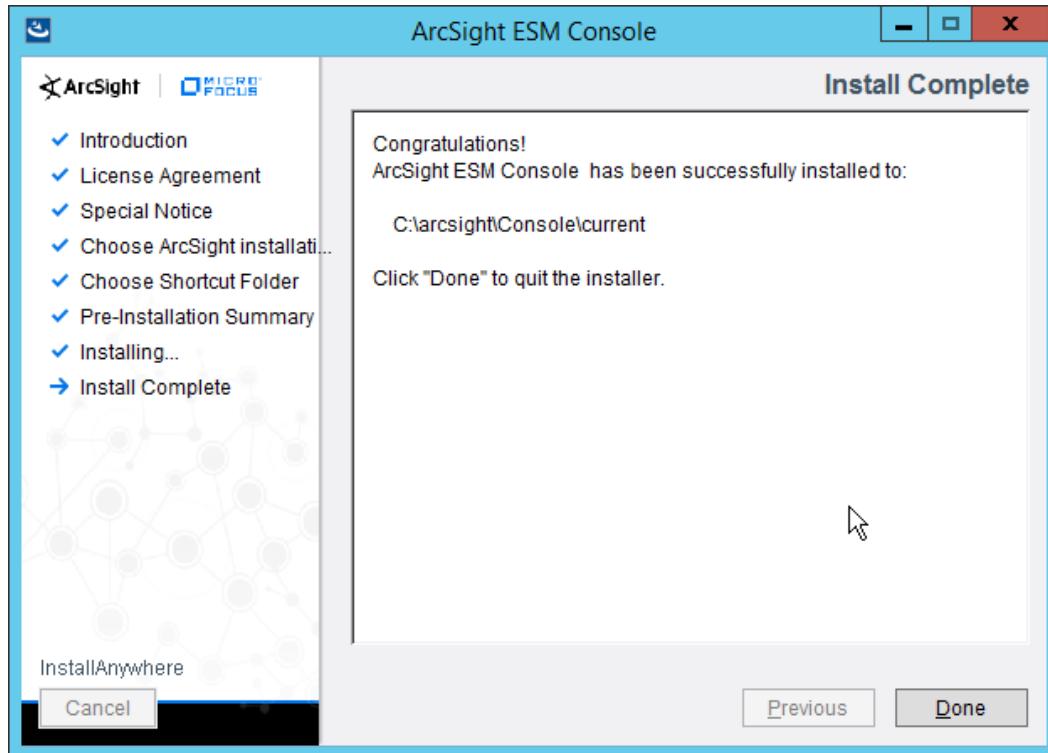
1270

23. Click **Next**.



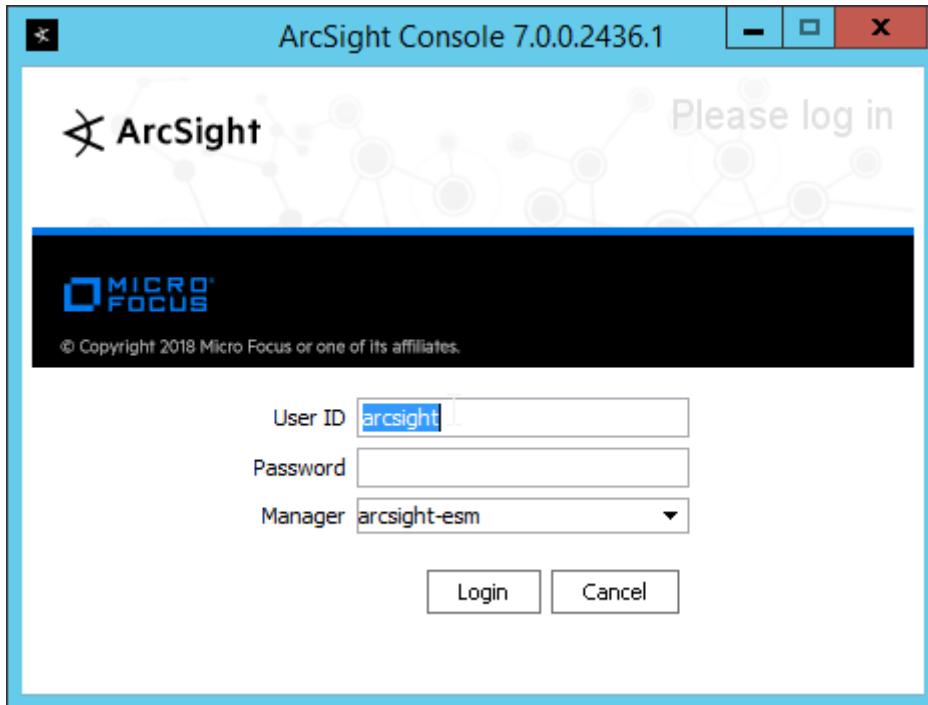
1271
1272
1273

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



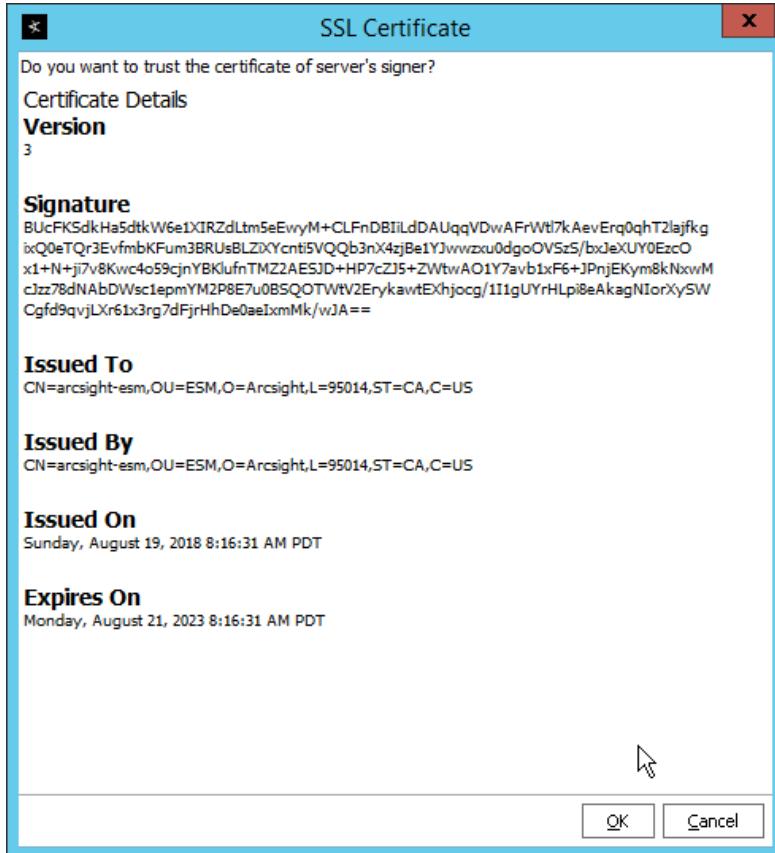
1274
1275
1276
1277

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



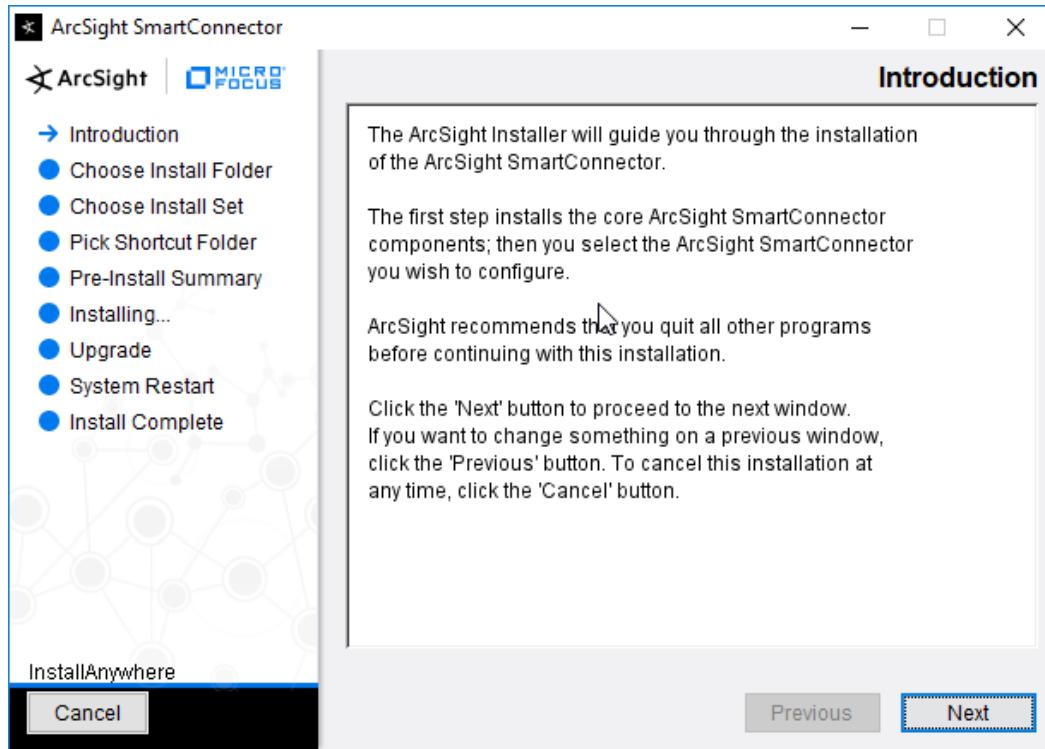
1278
1279
1280

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



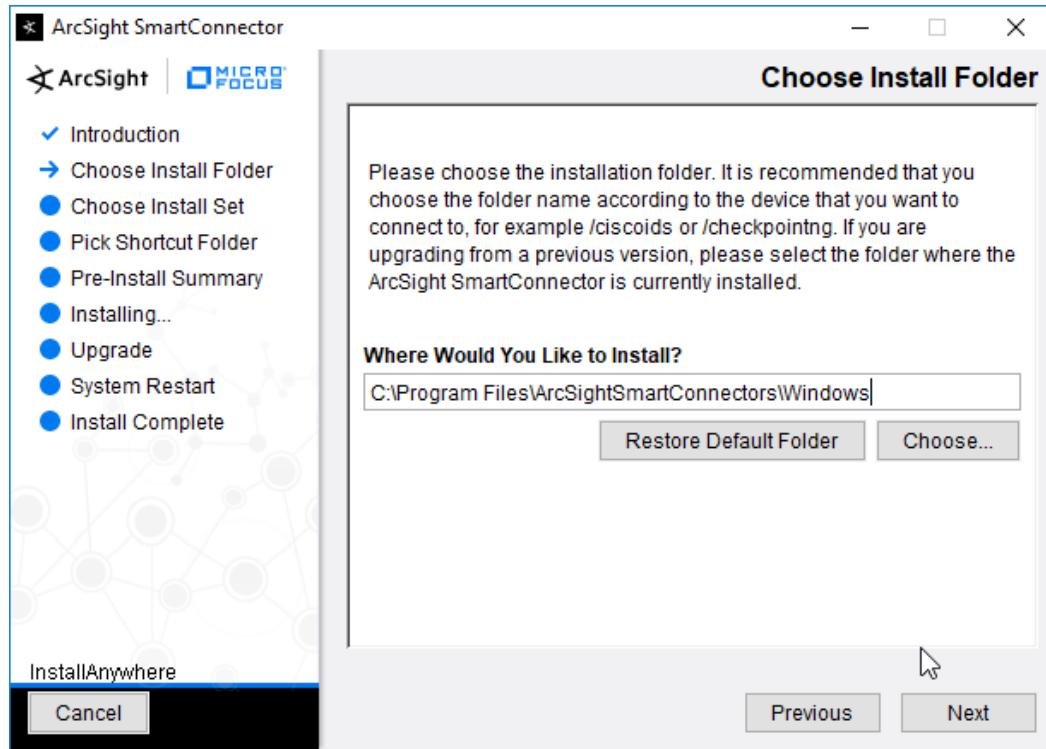
- 1281
1282 30. Click **OK**.

- 1283 2.8.2 Install Individual ArcSight Windows Connectors
1284 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe**.

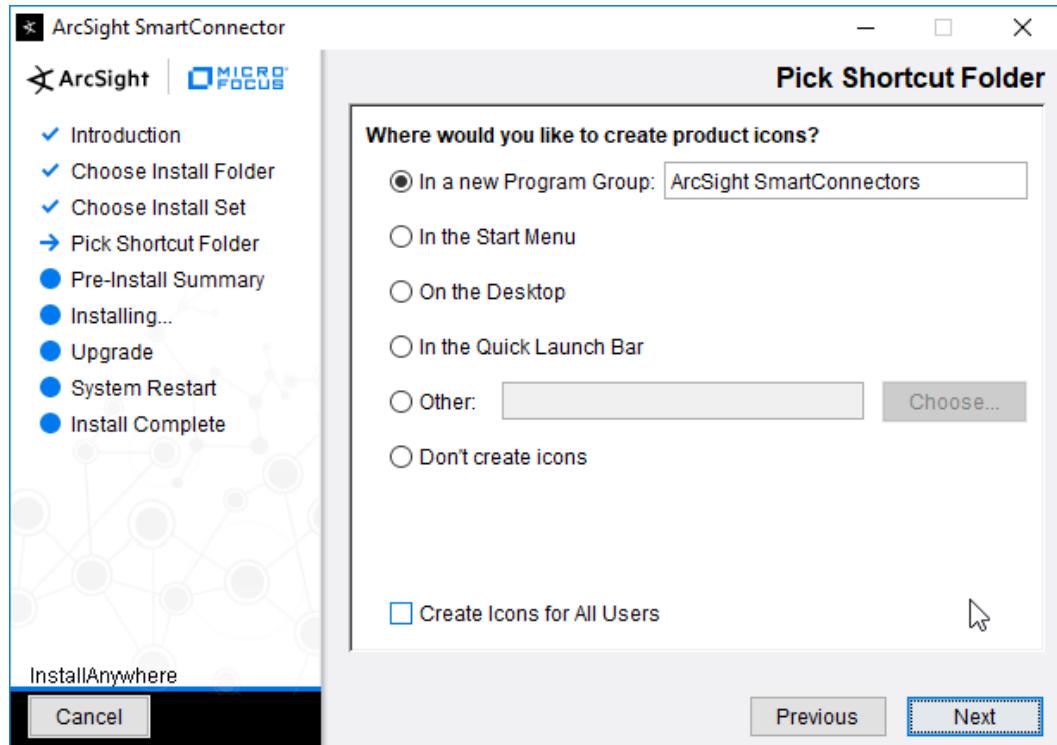


1285
1286
1287

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

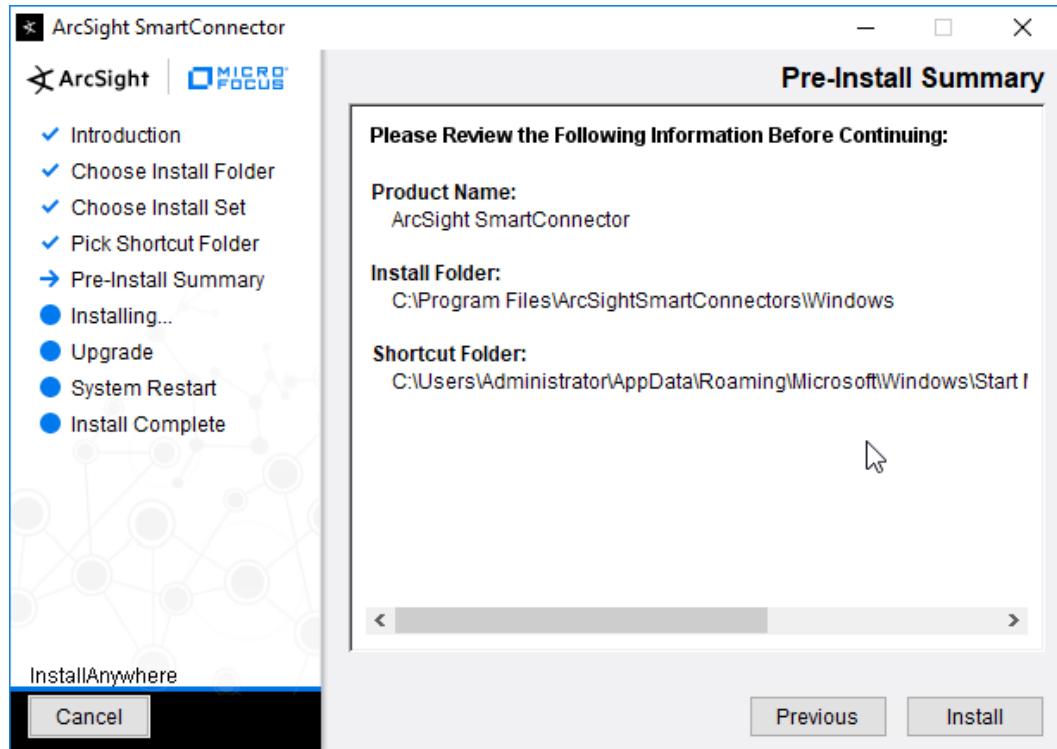
1288
1289

4. Click Next.



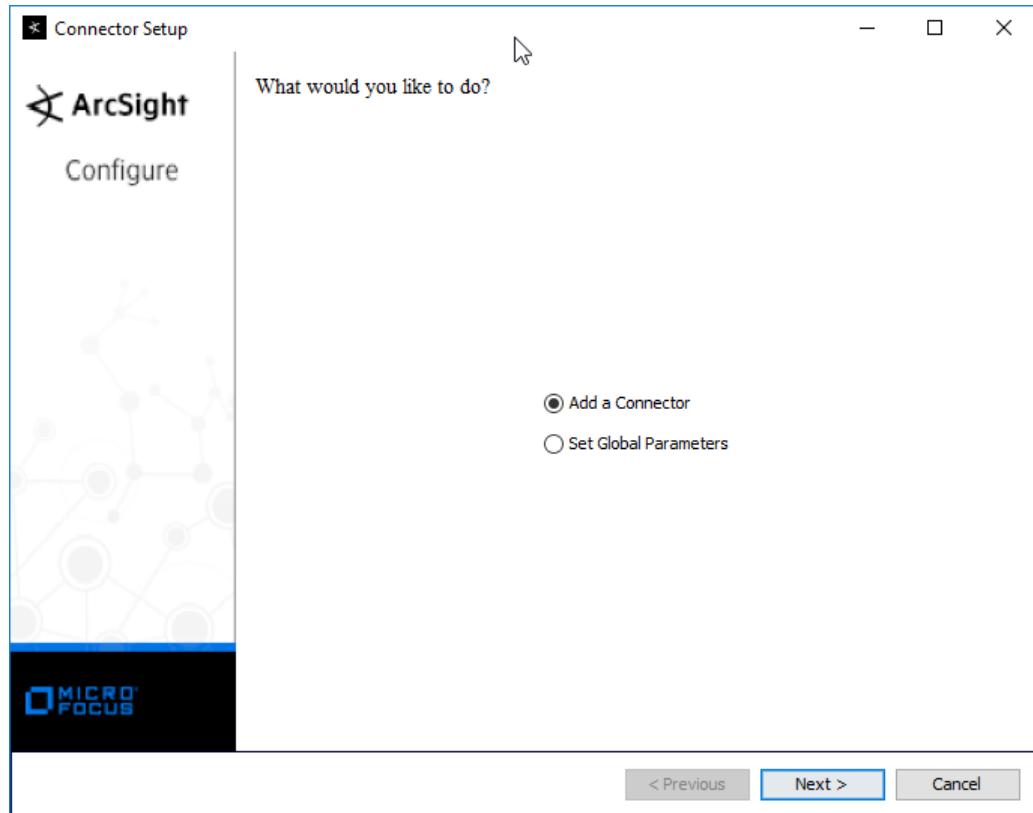
1290
1291

5. Click Next.



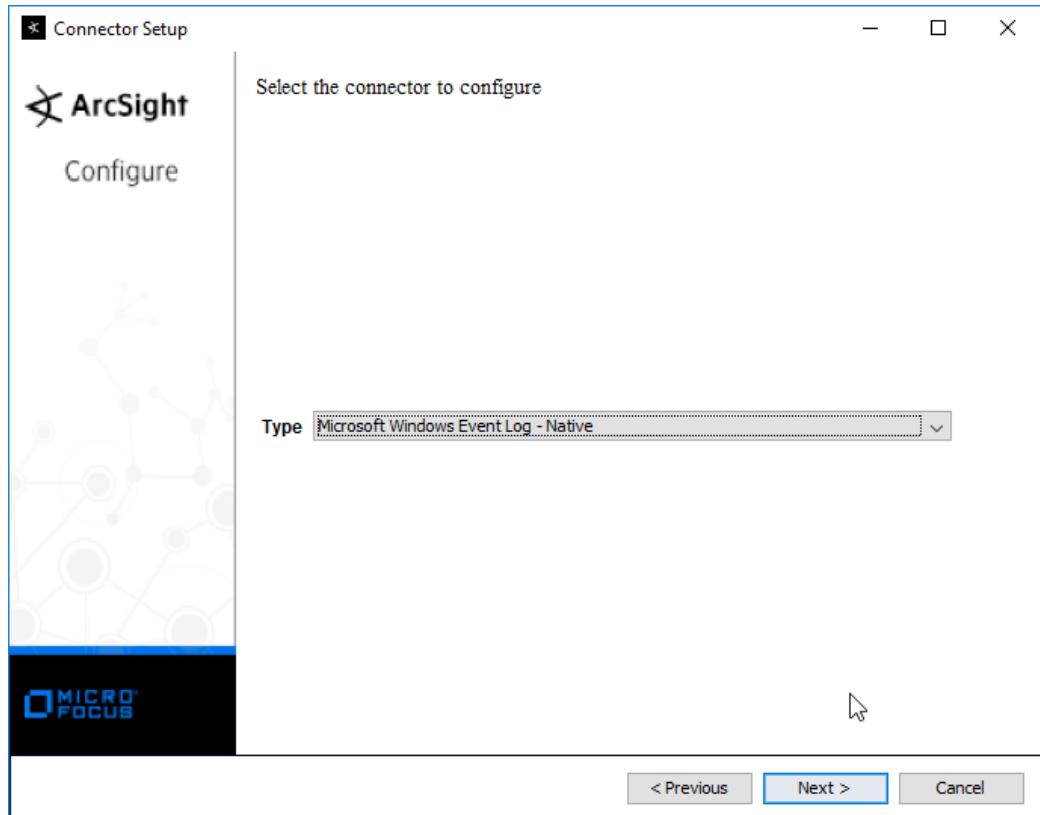
1292
1293
1294

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



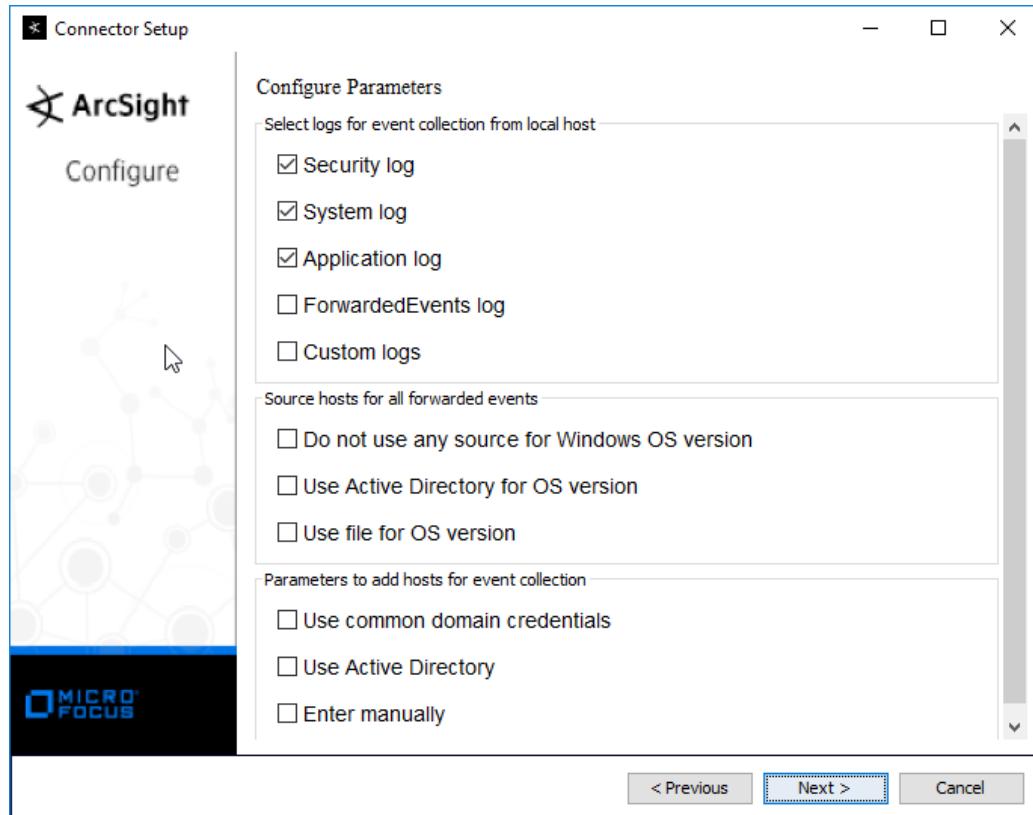
1295
1296
1297

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



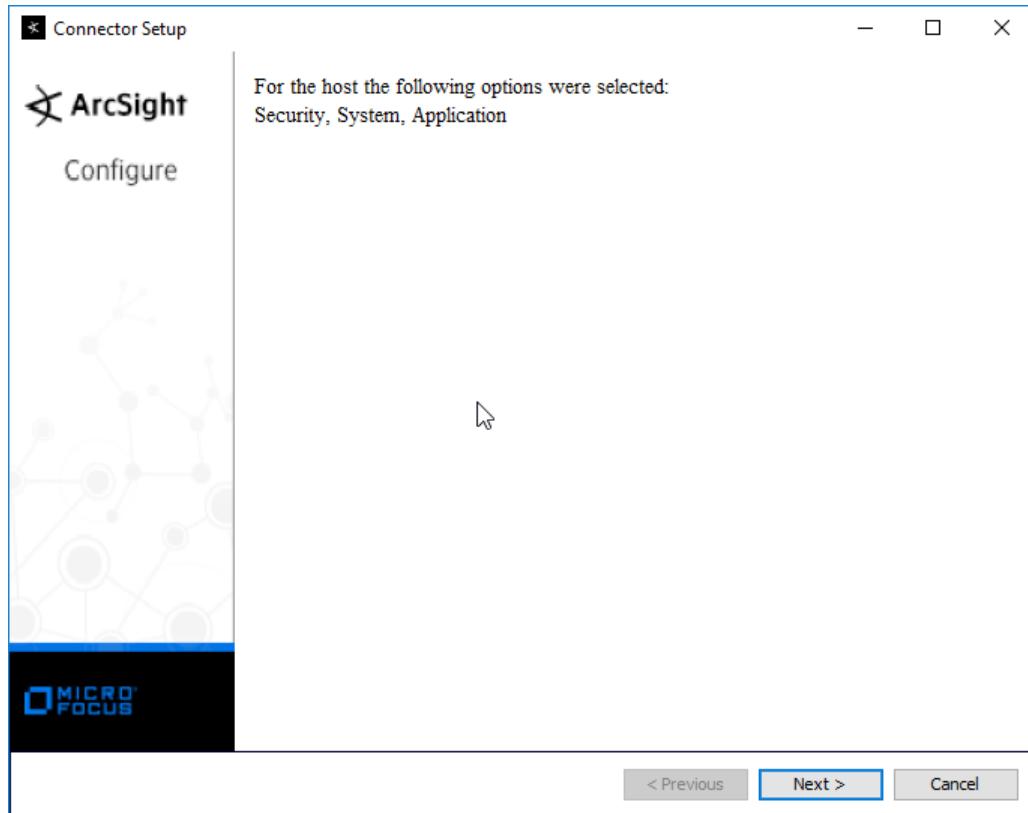
1298
1299

10. Click **Next**.



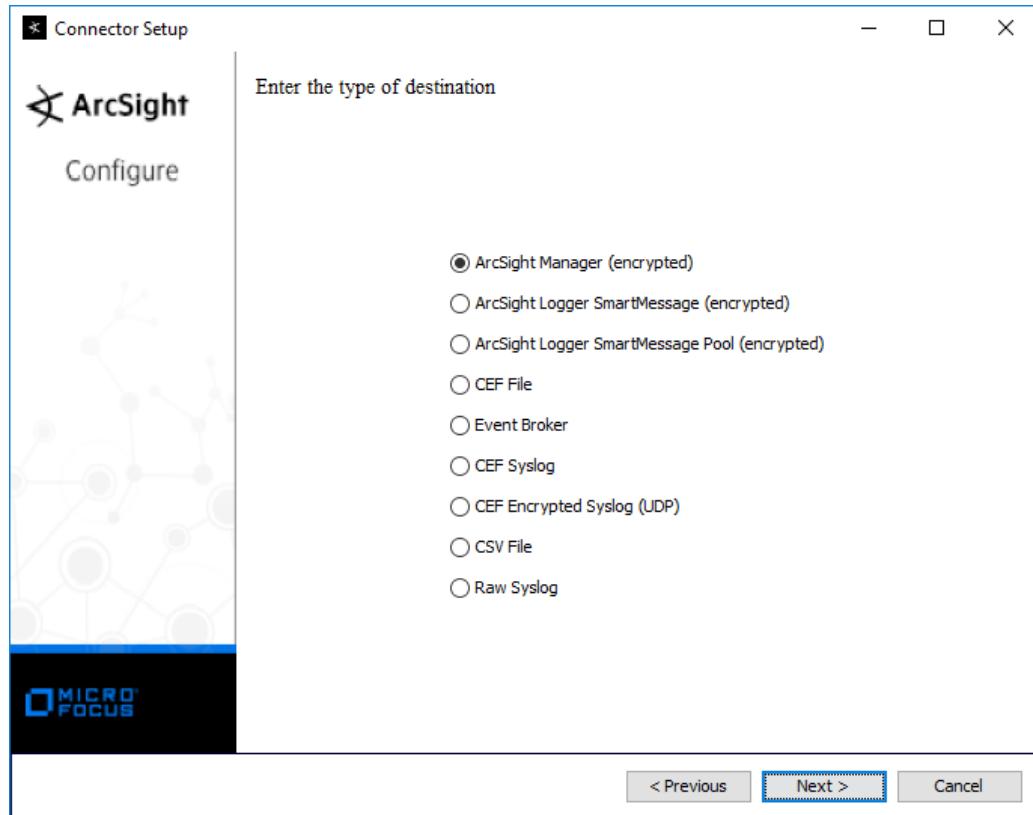
1300
1301

11. Click **Next**.



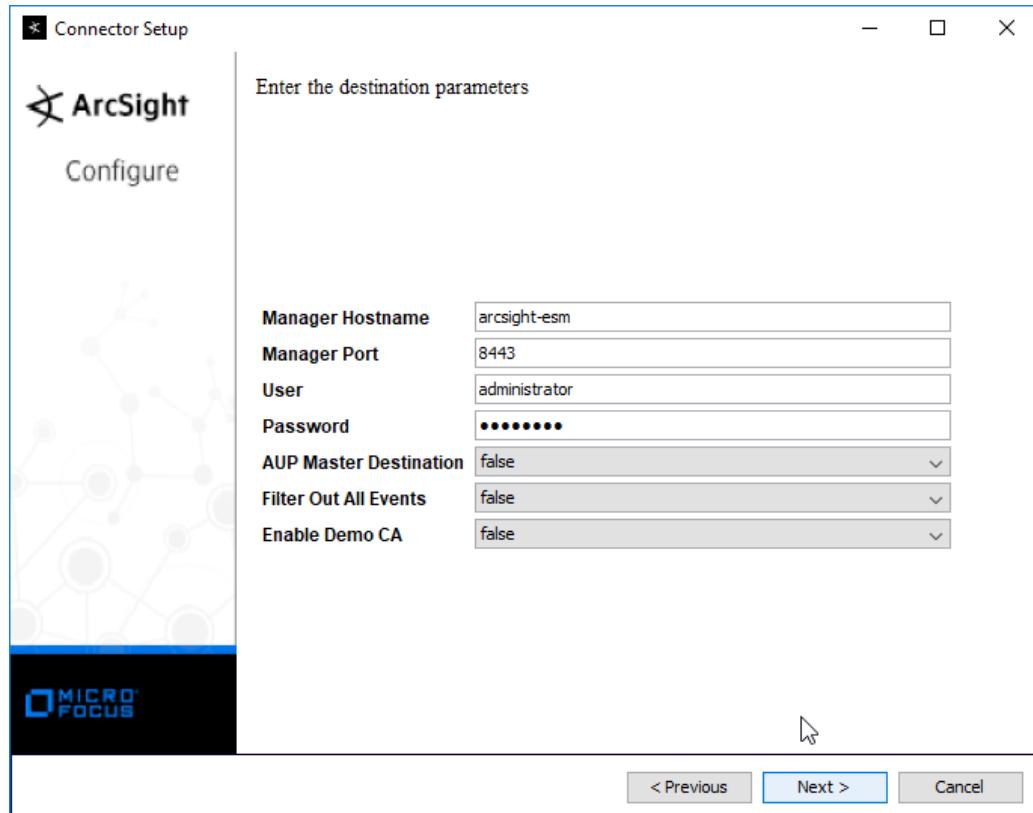
1302
1303
1304

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



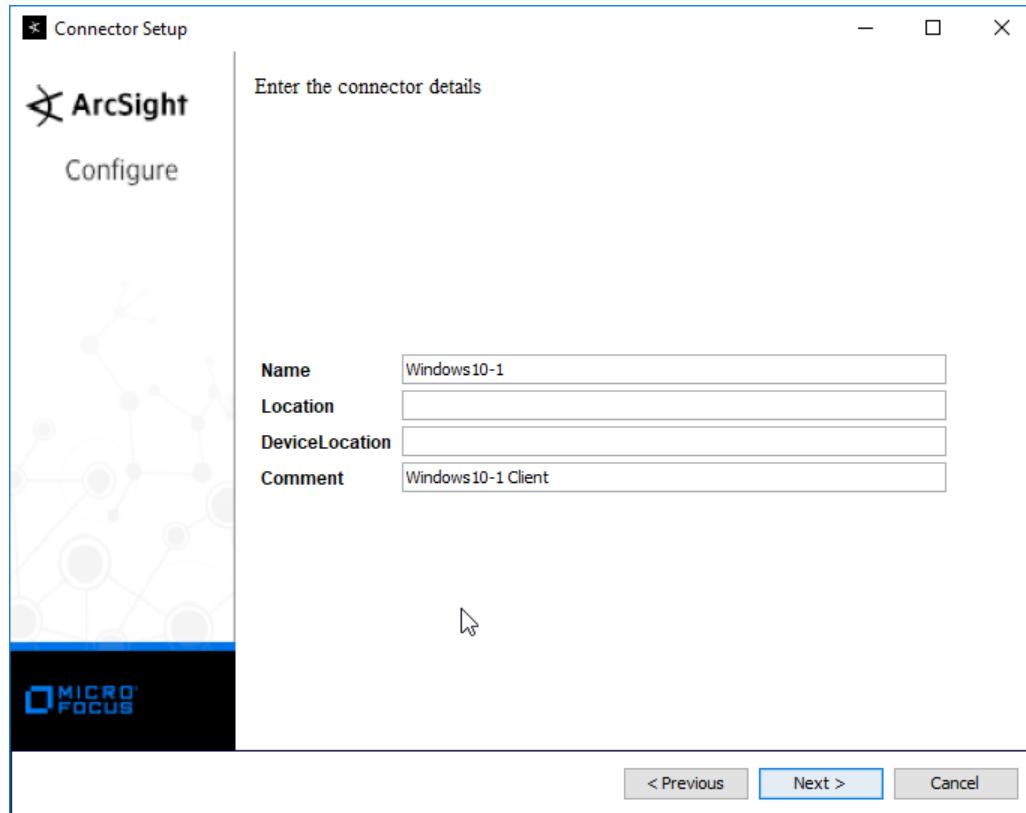
1305
1306
1307

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



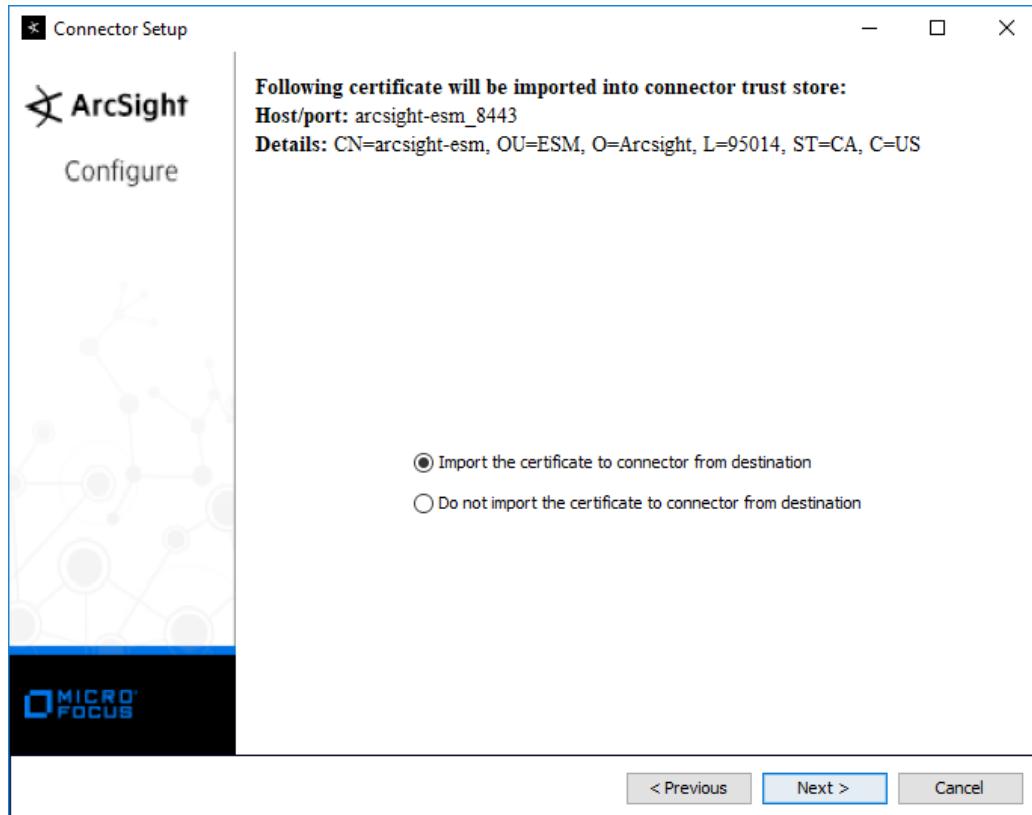
1308
1309
1310

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



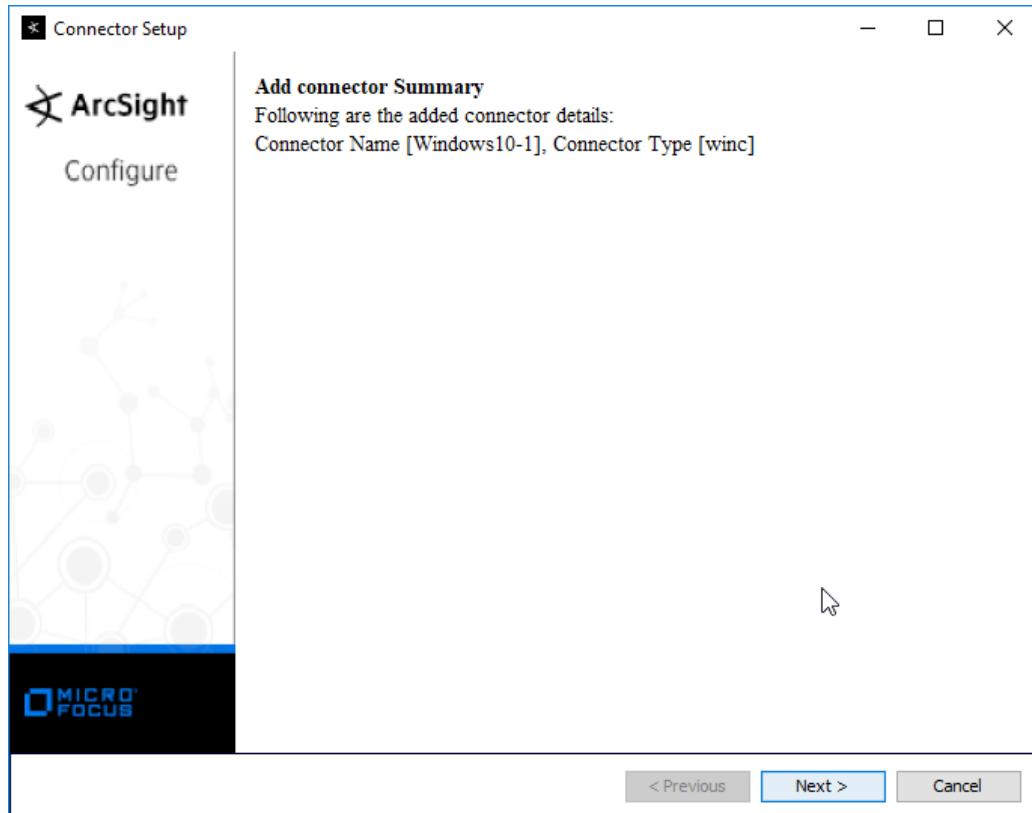
1311
1312
1313

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



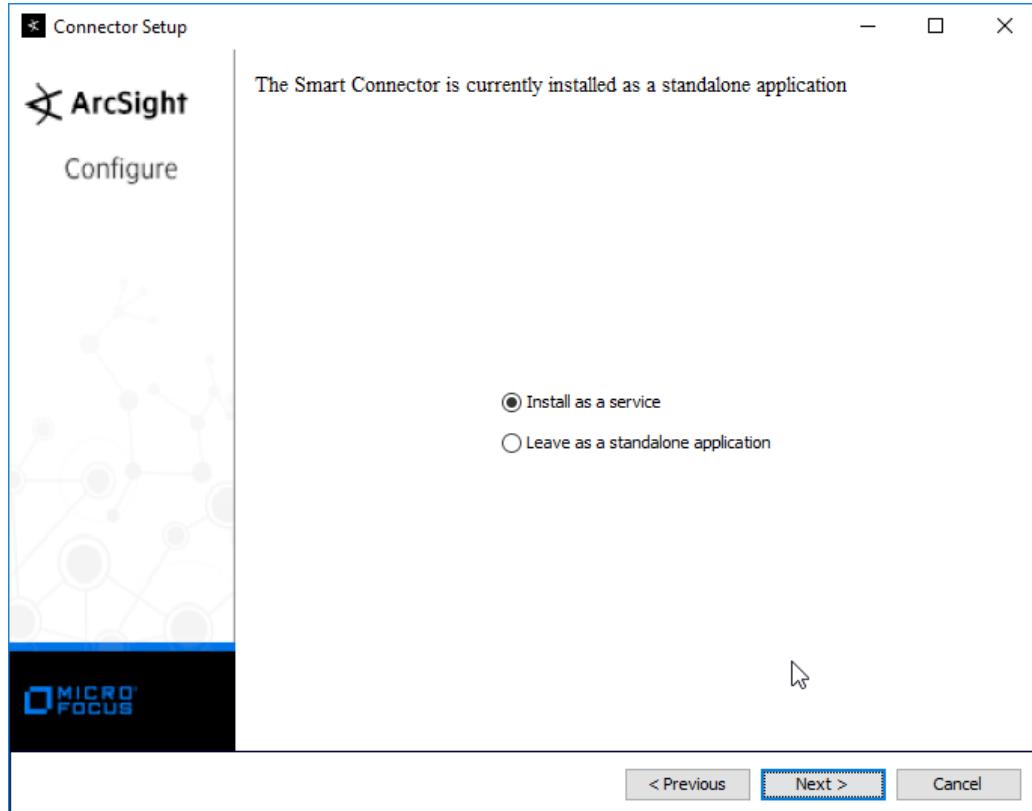
1314
1315

20. Click **Next**.



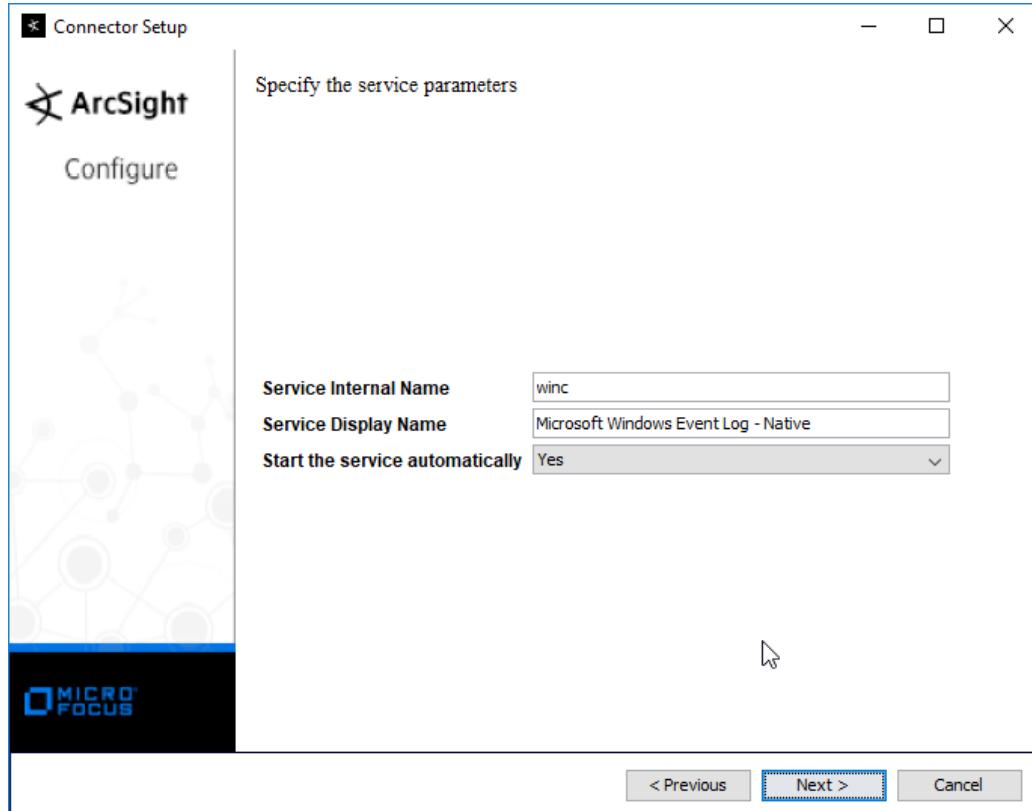
1316
1317
1318

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



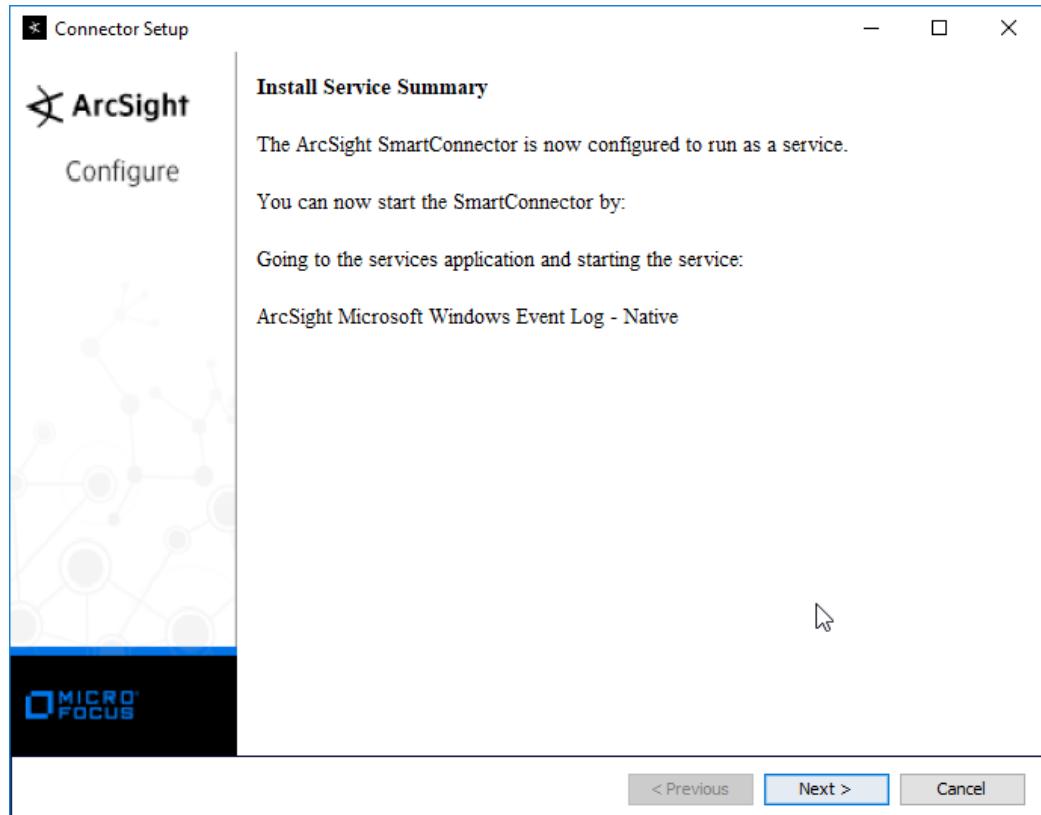
1319
1320

23. Click **Next**.



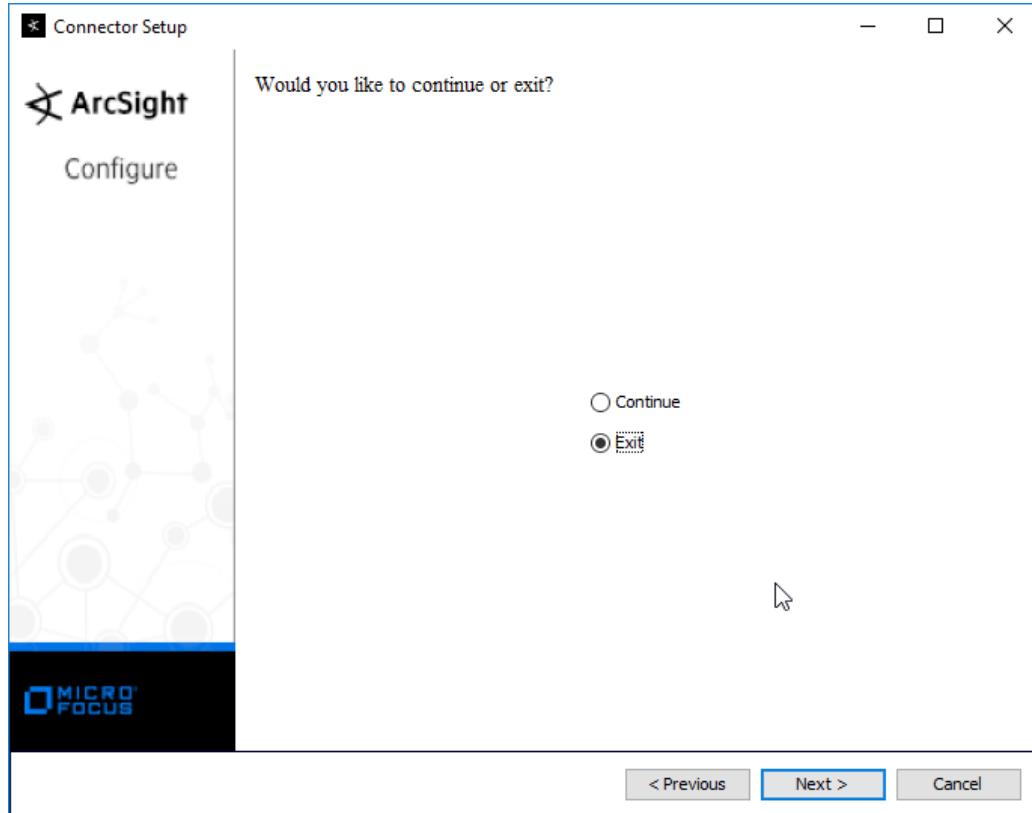
1321
1322

24. Click **Next**.



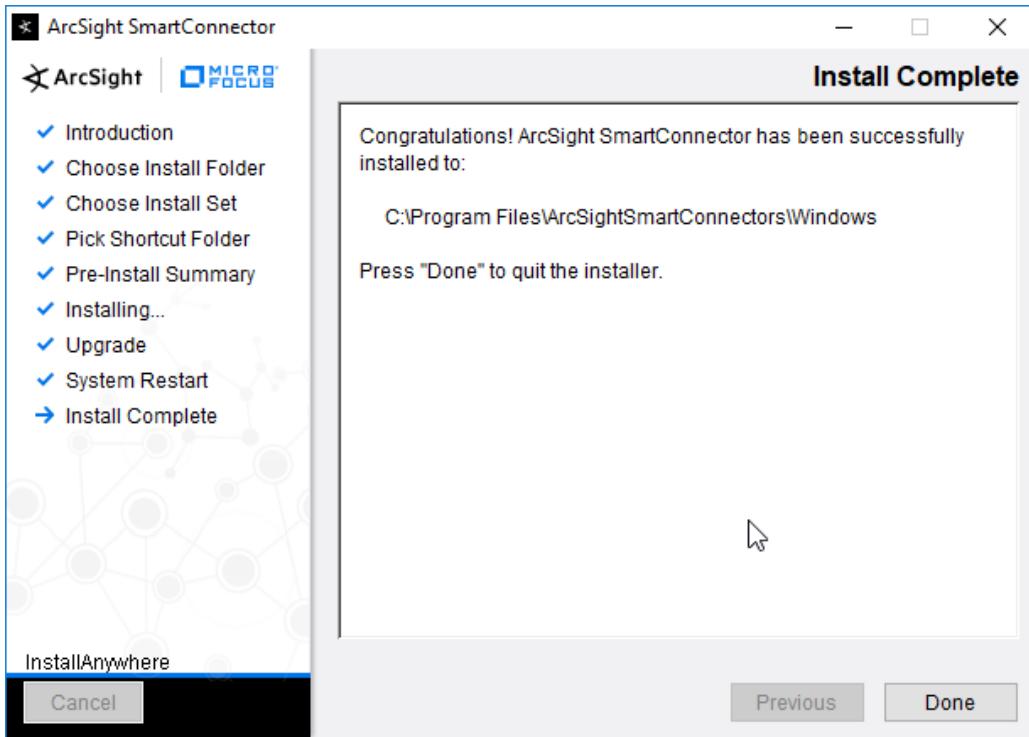
1323
1324
1325

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



1326
1327

27. Click **Next**.



1328

28. Click Done.

1329

2.8.3 Install Individual ArcSight Ubuntu Connectors

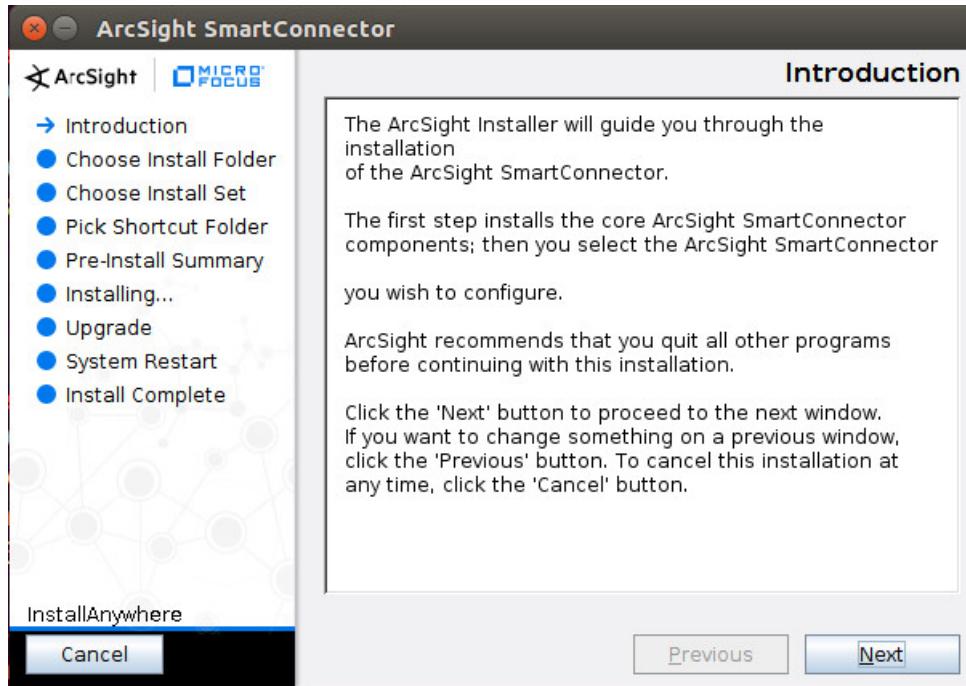
1331

1. From the command line, run:

```
> sudo ./ArcSight-7.9.0.8084.0-Connector-Linux64.bin
```

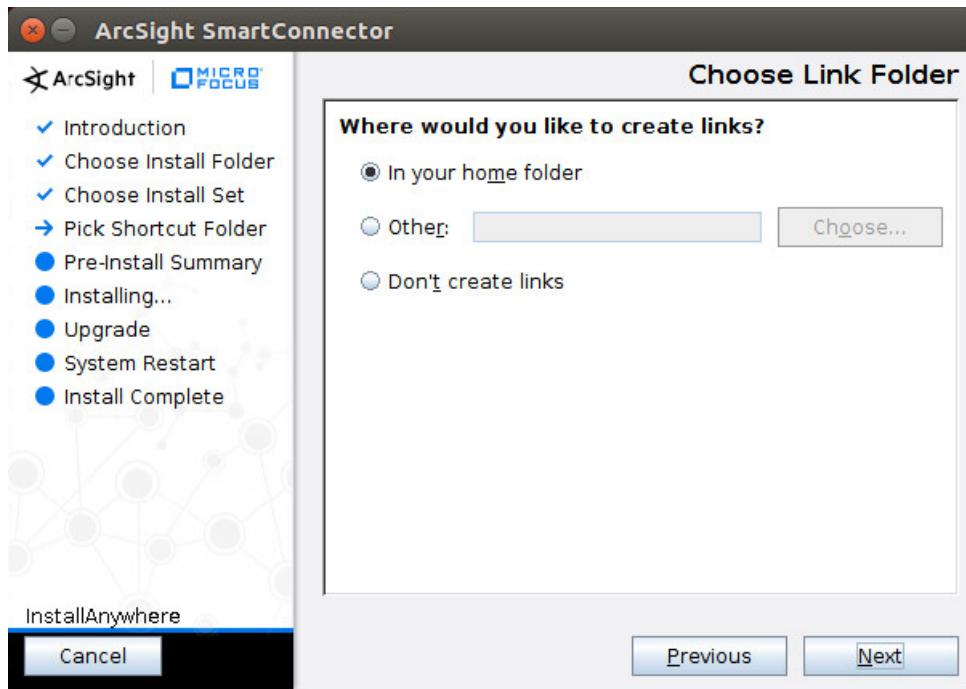
1332

2. Enter the **password** if prompted.



1334
1335
1336
1337
1338

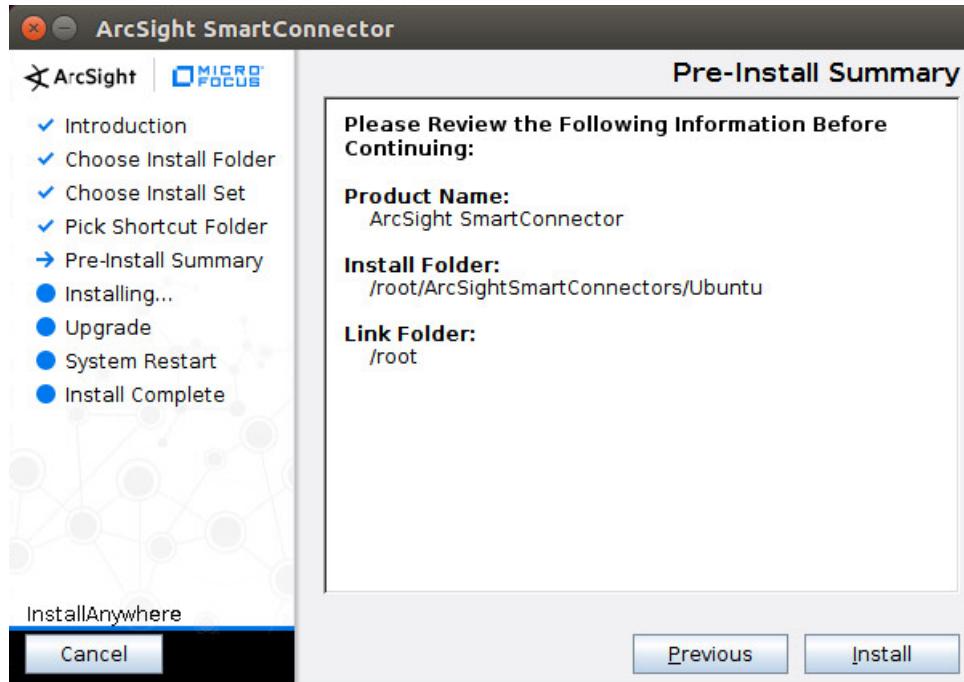
3. Click **Next**.
4. Enter */root/ArcSightSmartConnectors/Ubuntu*.
5. Click **Next**.



1339

1340

6. Click **Next**.

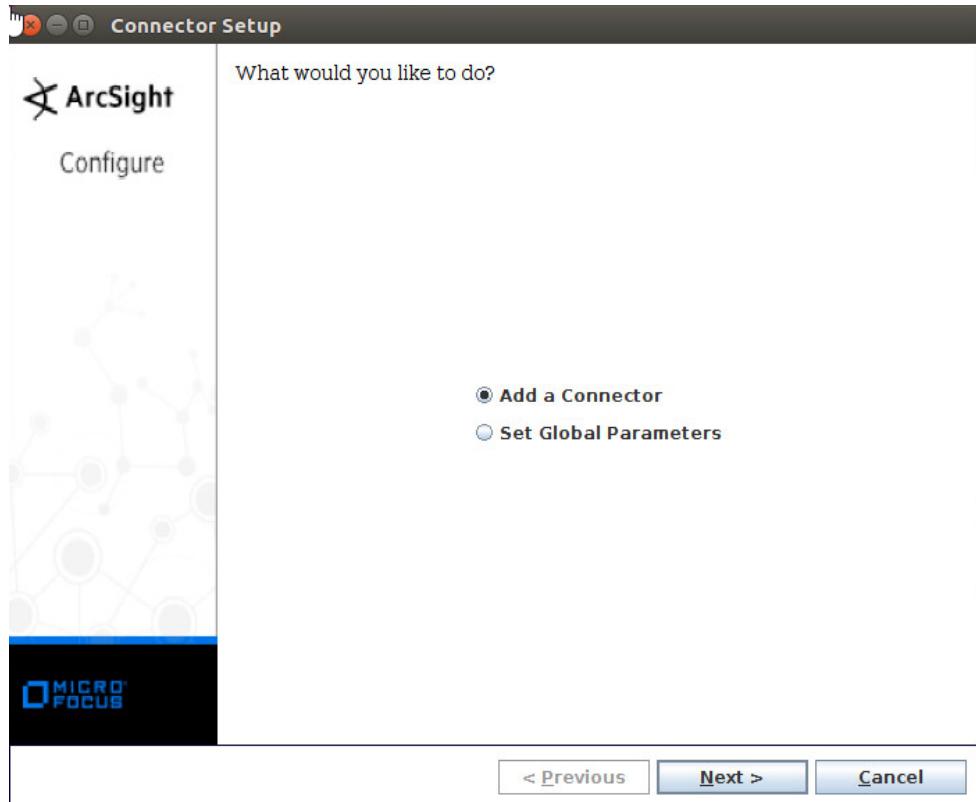


1341

7. Click **Install**.

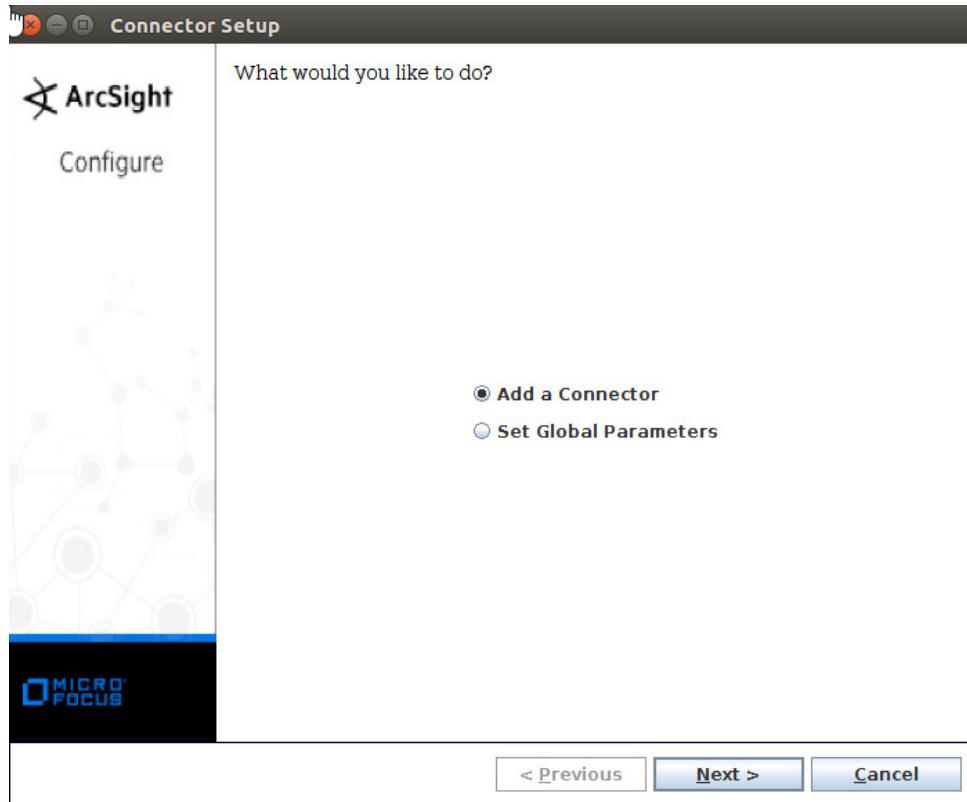
1342

8. Select **Add a Connector**.



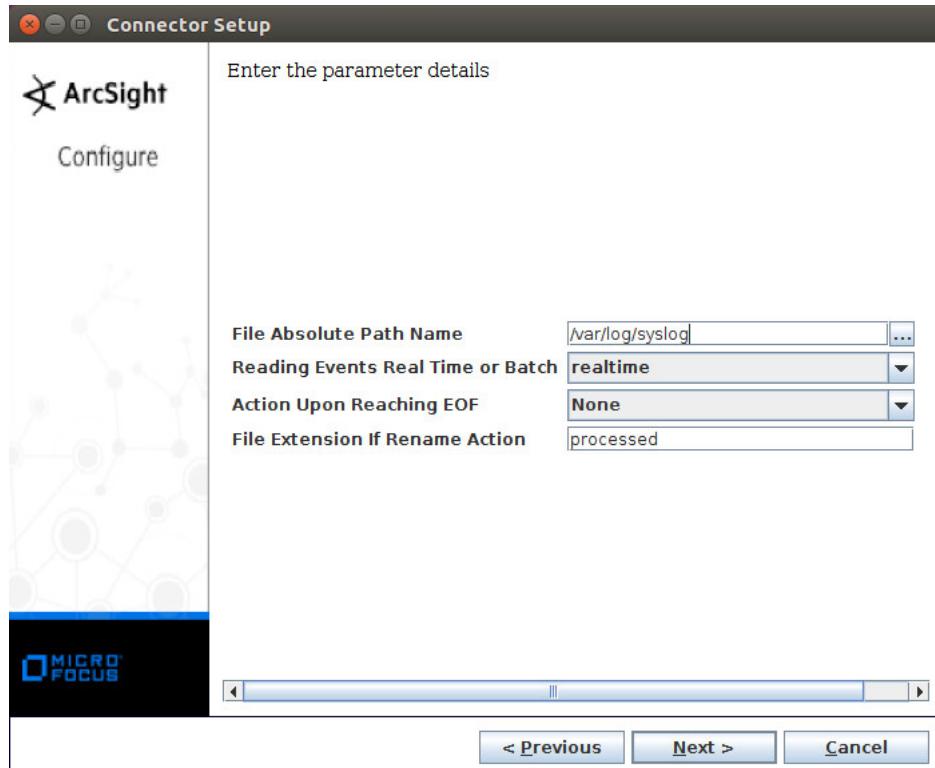
1344
1345
1346

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



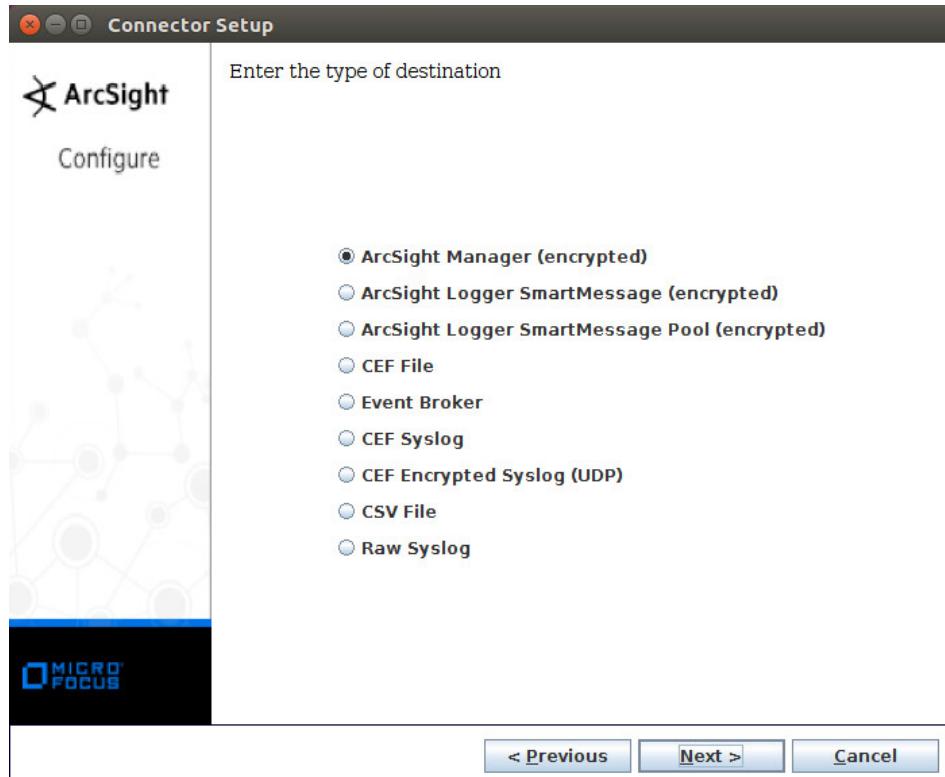
1347
1348
1349

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



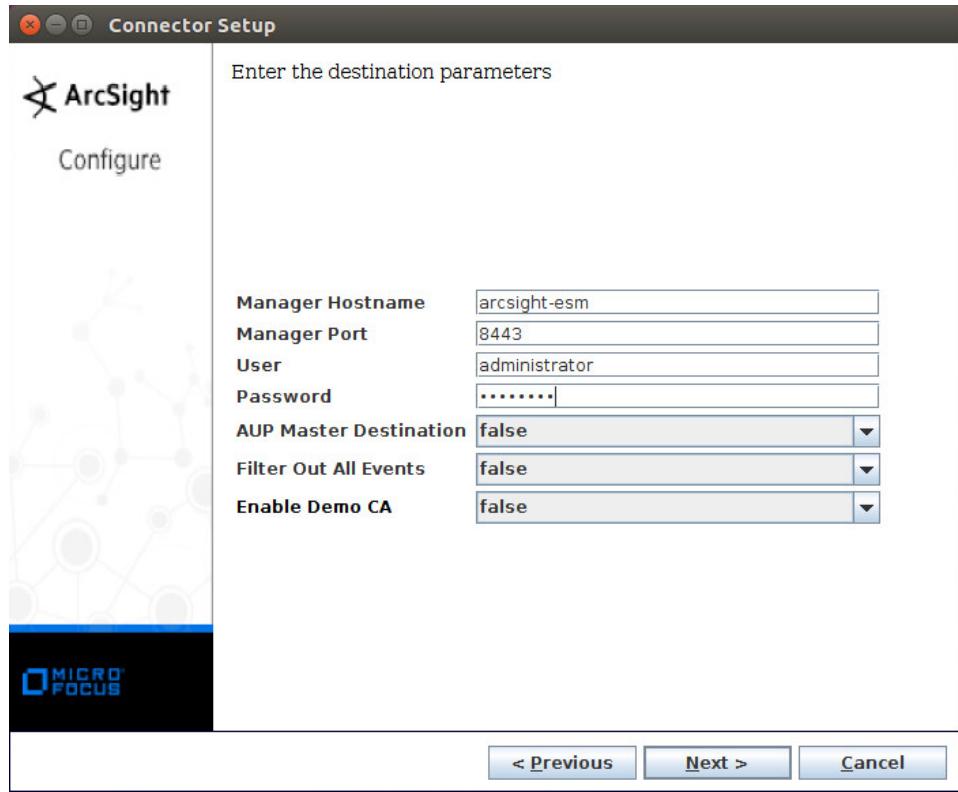
1350
1351
1352

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



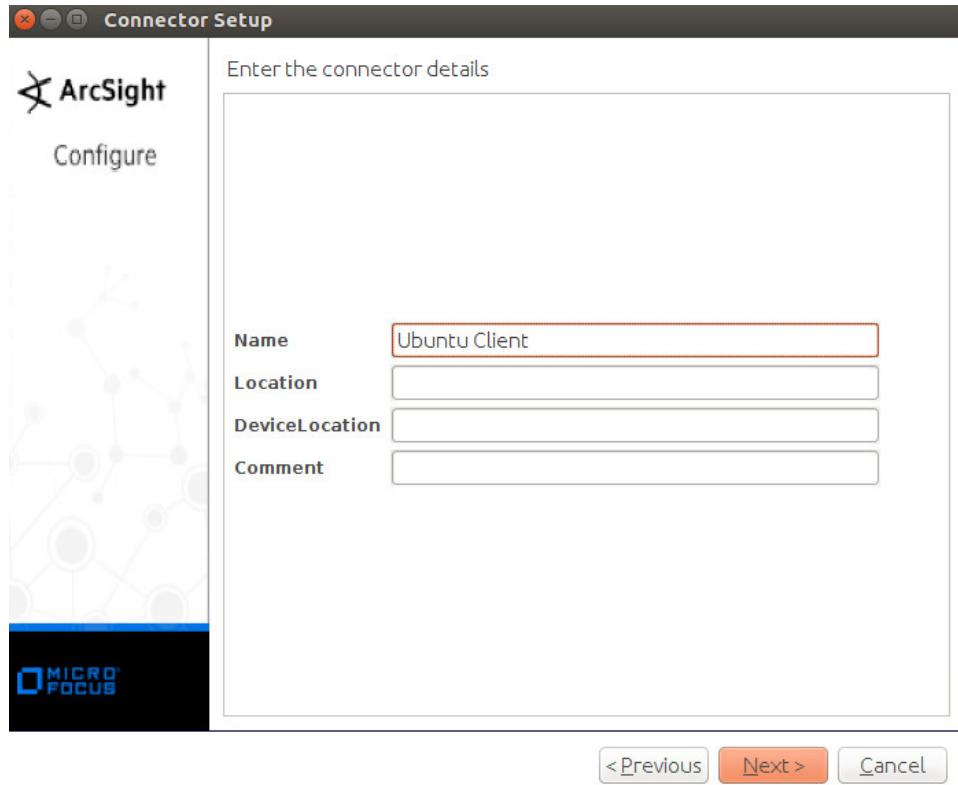
1353
1354
1355

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



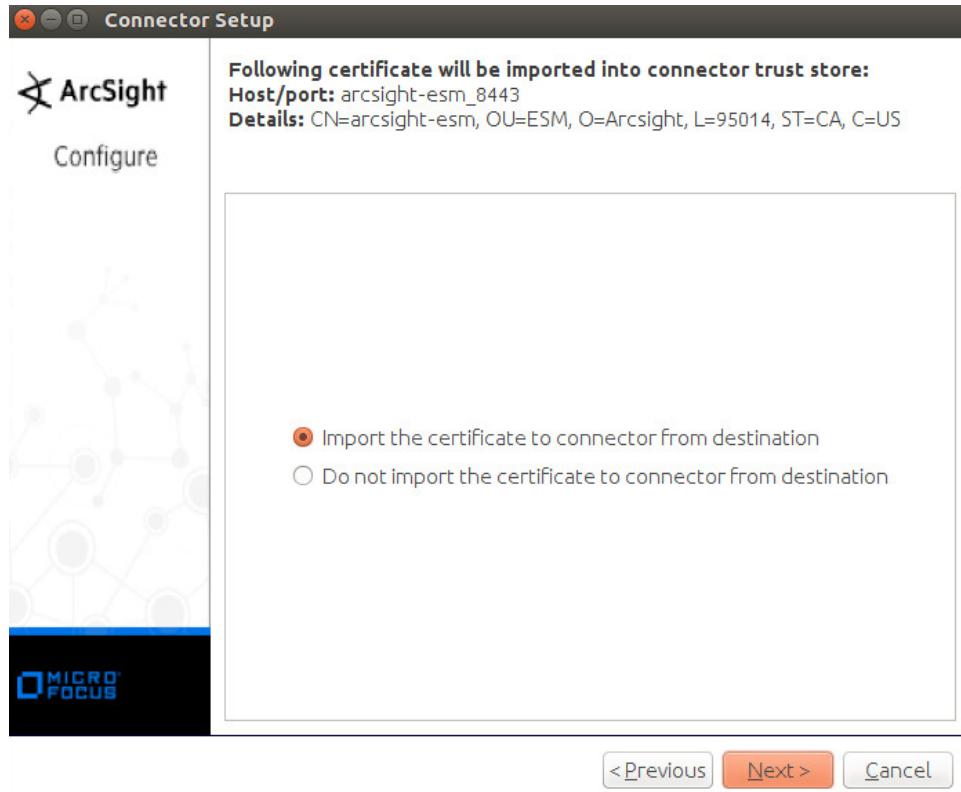
1356
1357
1358

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



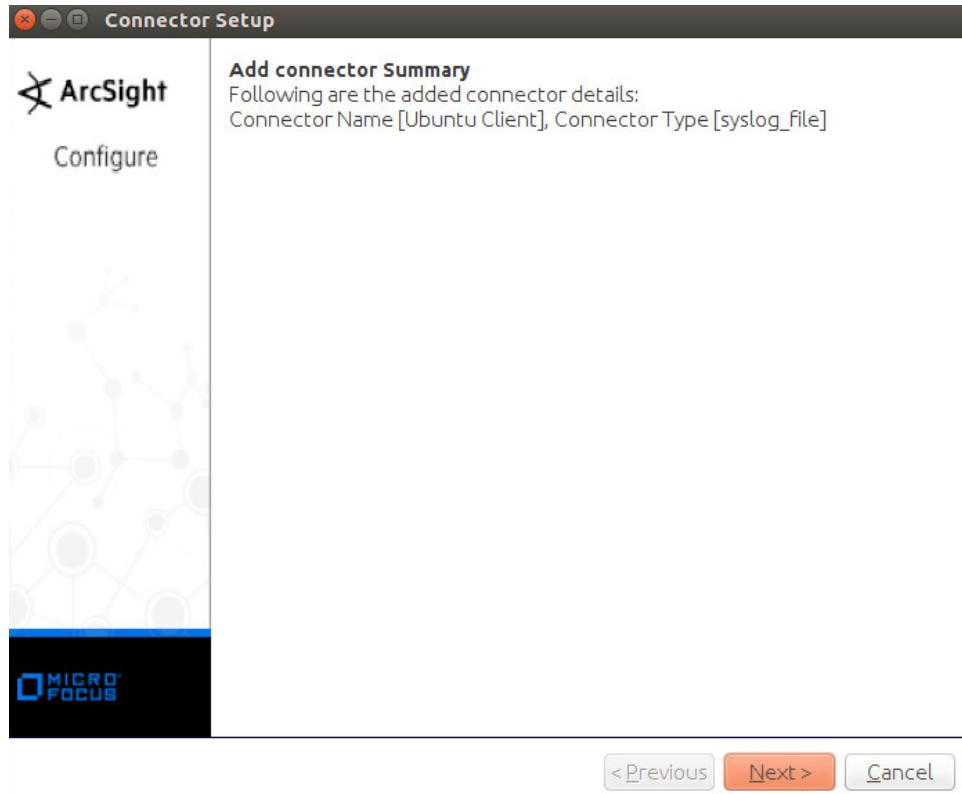
1359
1360
1361

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



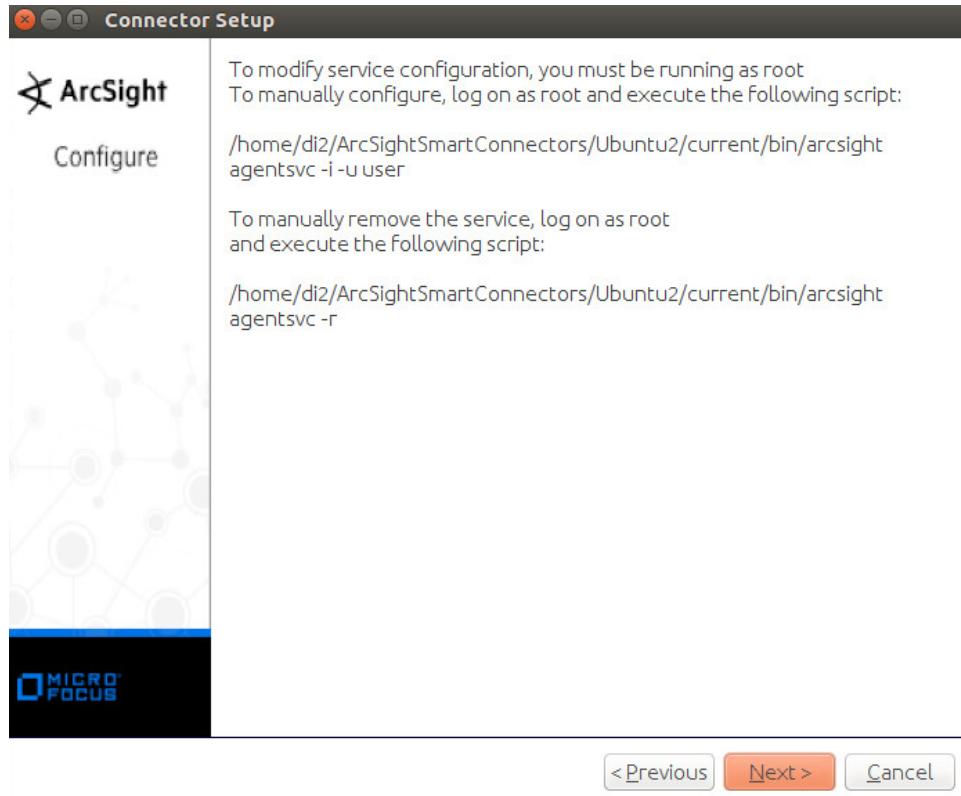
1362
1363

21. Click **Next**.

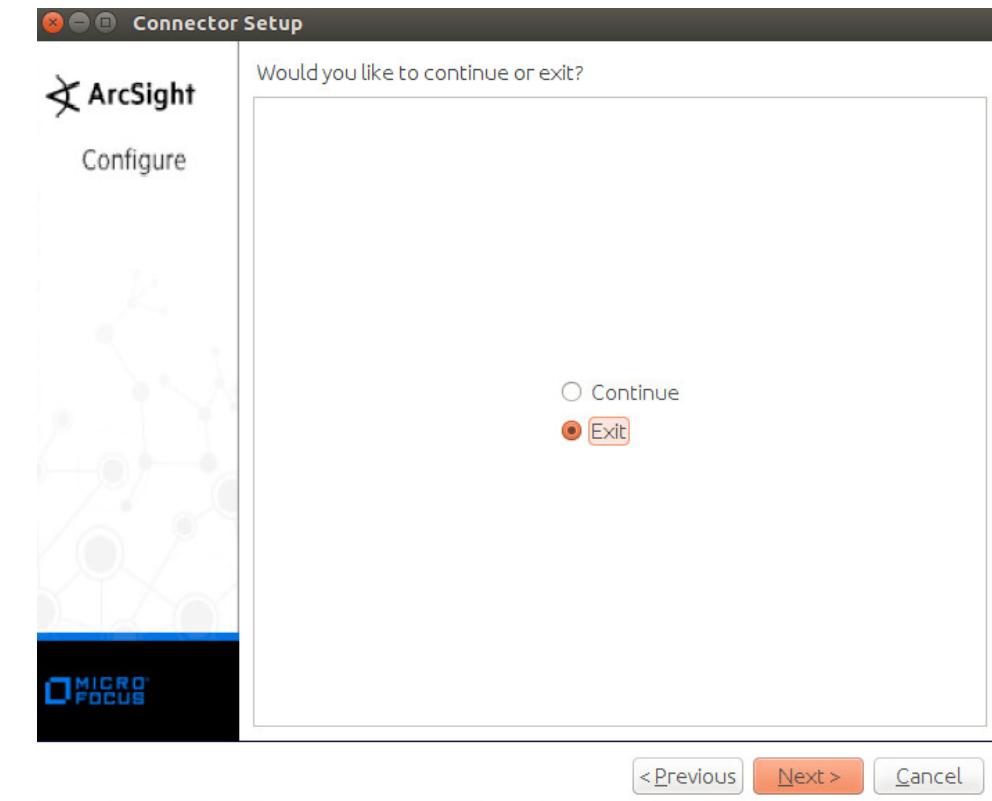
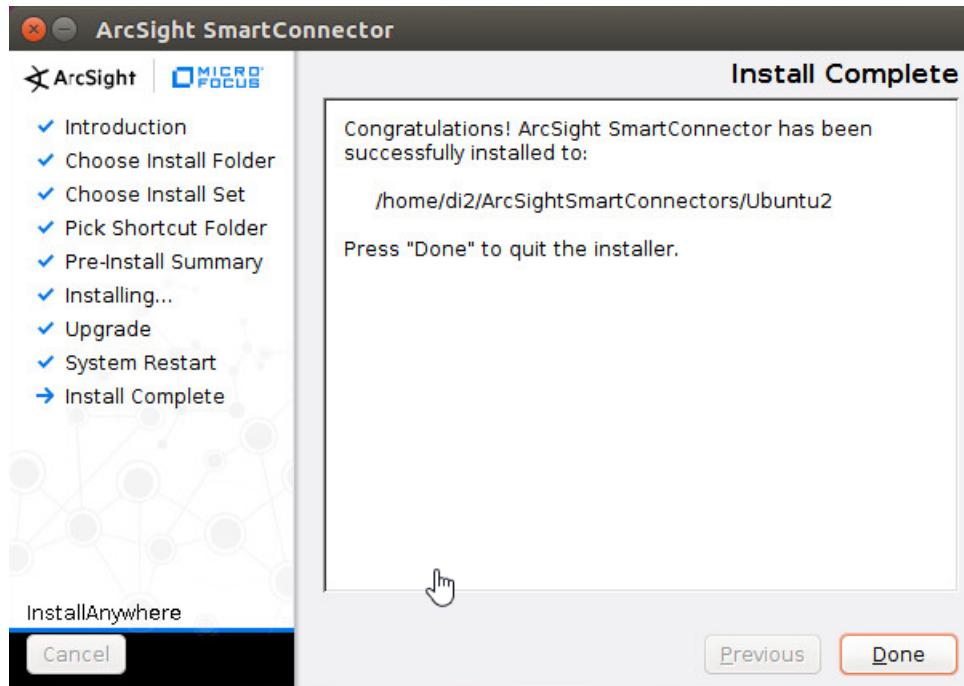


1364
1365

22. Click **Next**.



1366
1367 23. Click **Next**.
1368 24. Select **Exit**.

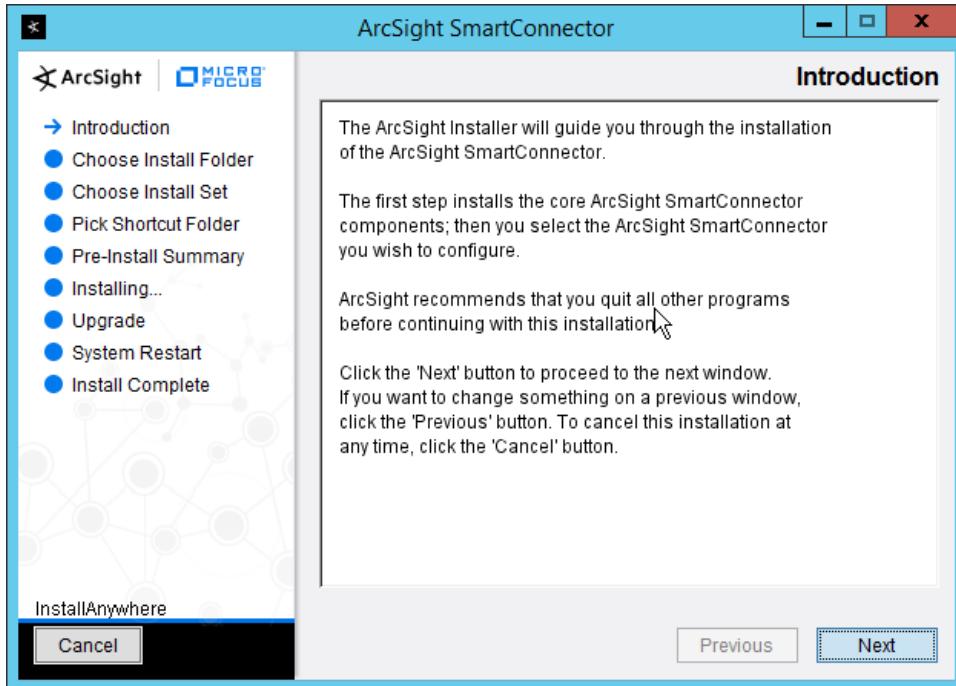
1369
137025. Click **Next**.

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**.



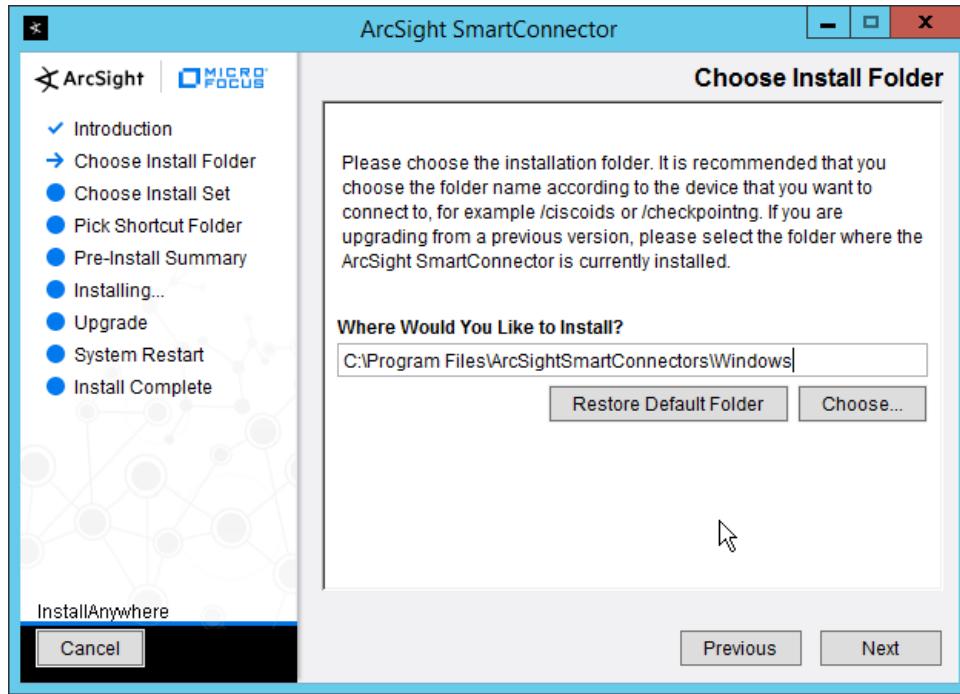
1375

1376 2. Click **Next**.

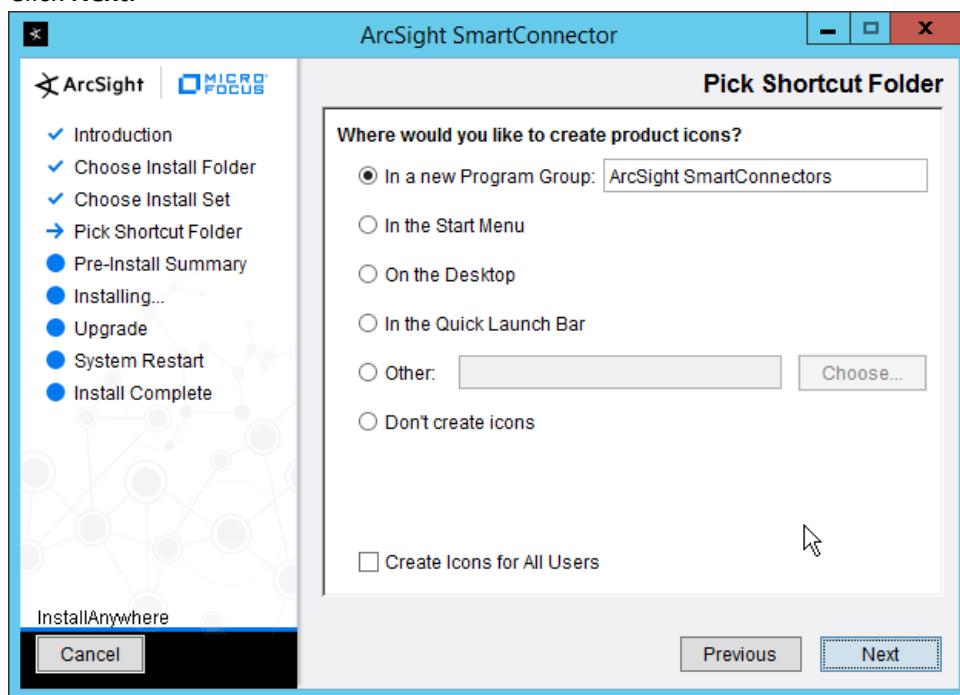
1377 3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows*.

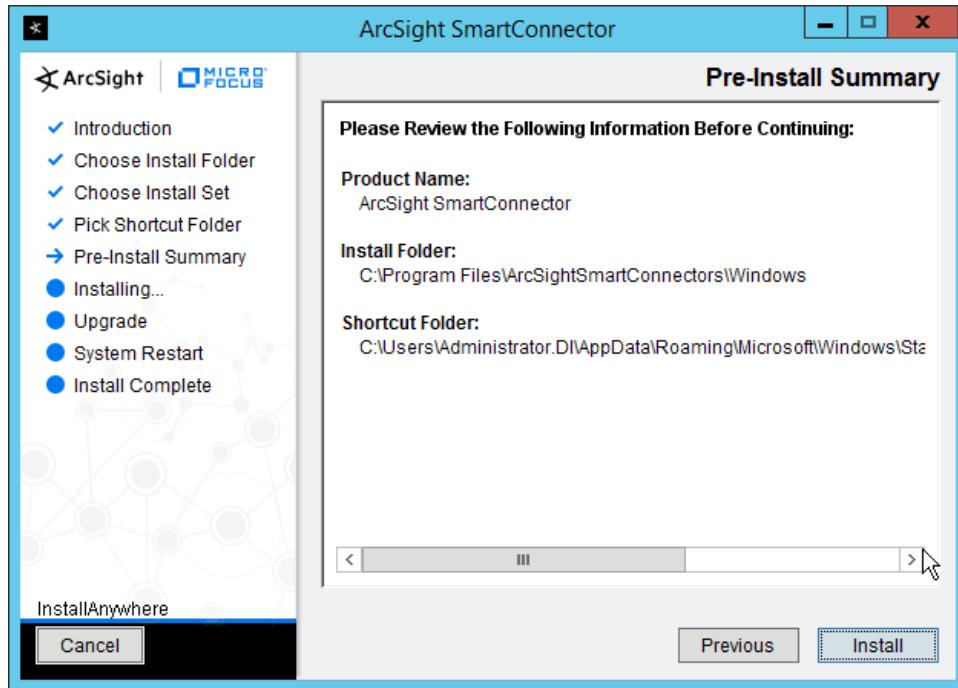
1378
1379

4. Click
- Next**
- .

1380
1381

5. Click
- Next**
- .



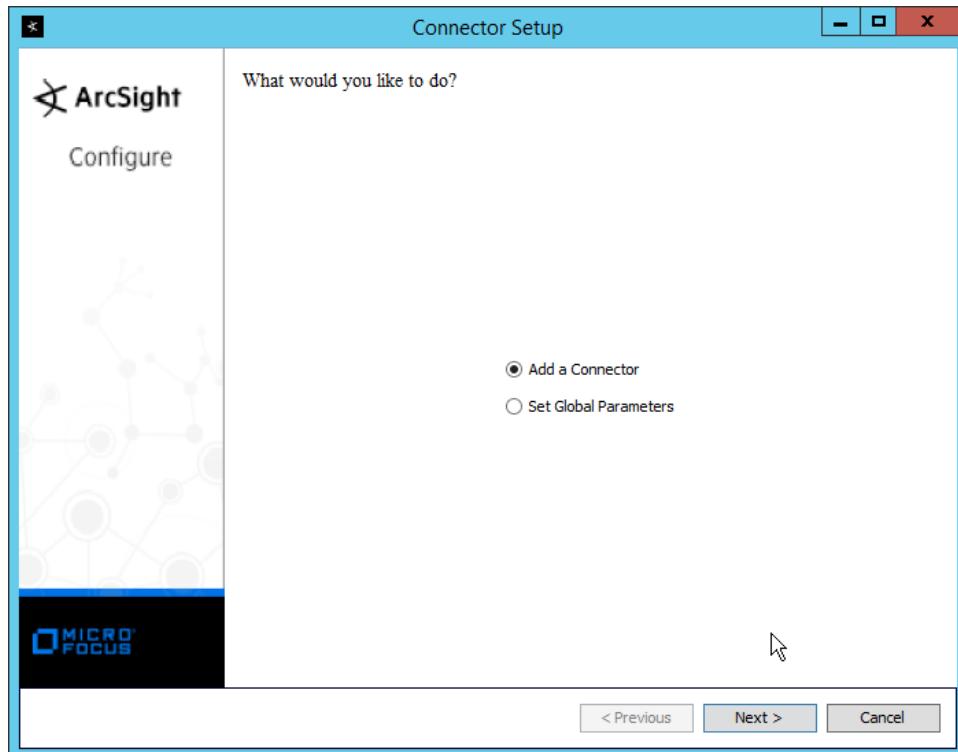


1382

1383

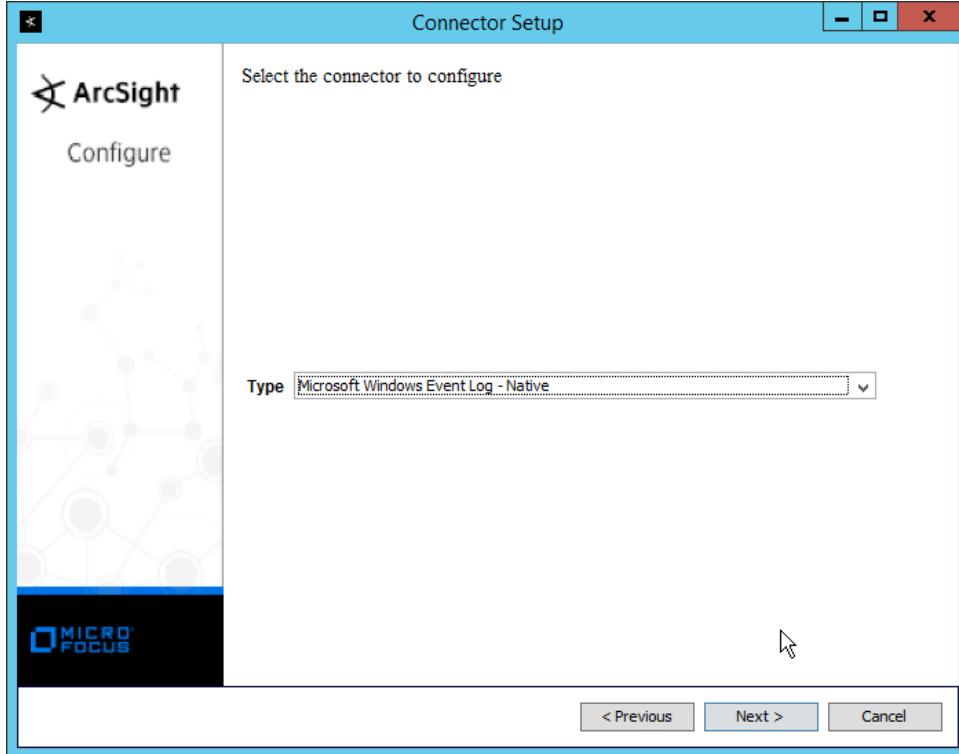
1384

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

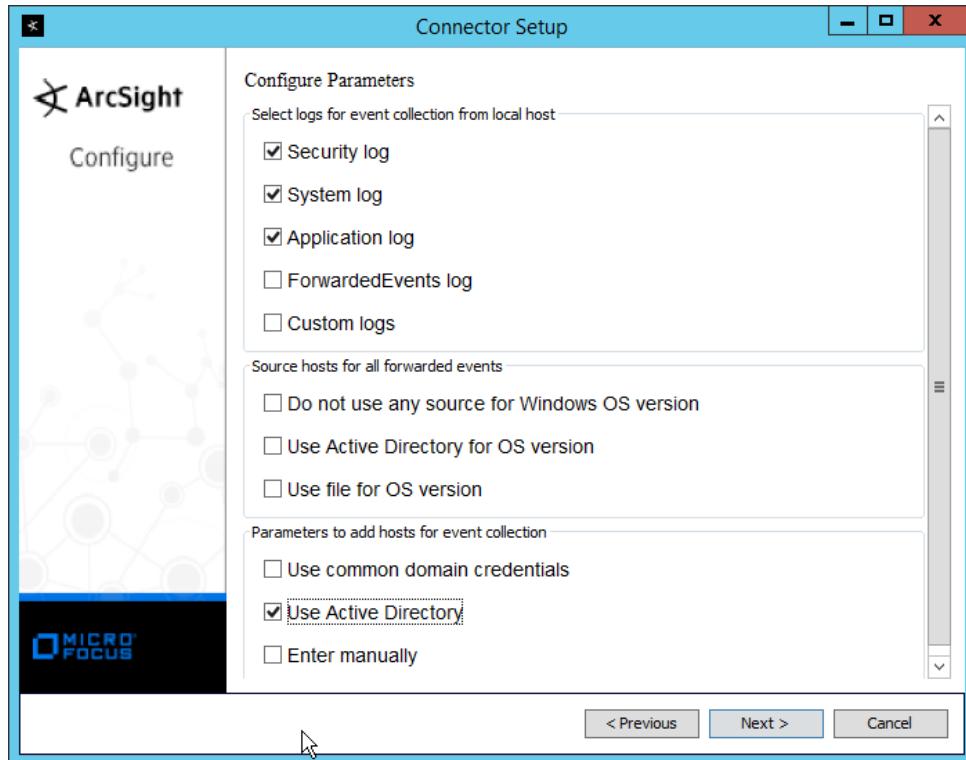


1385

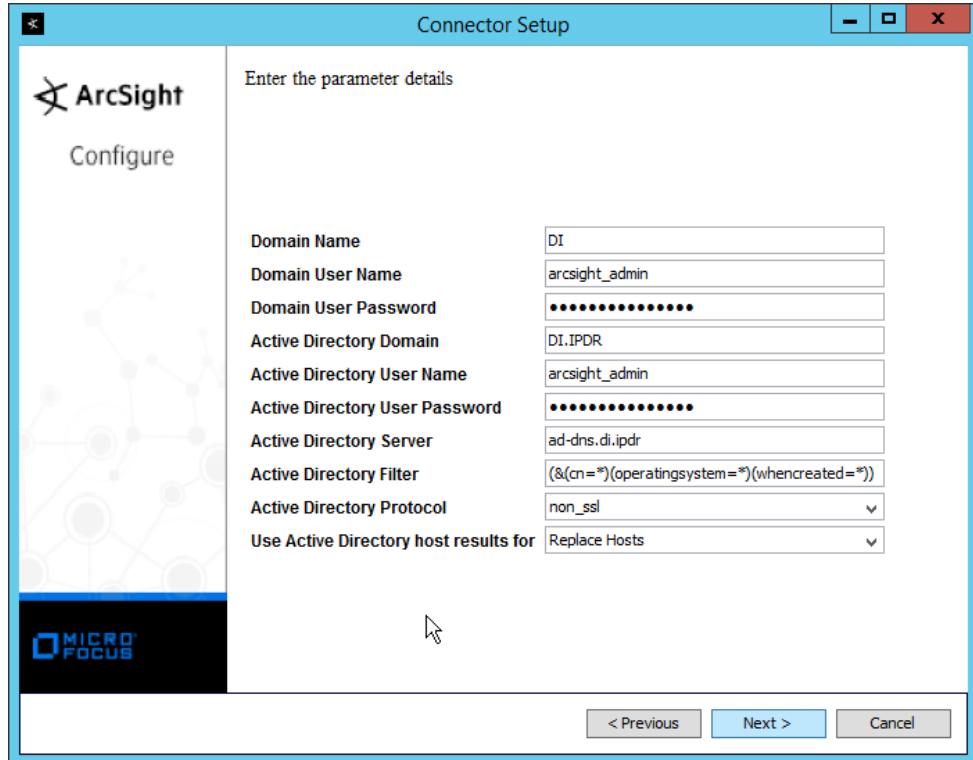
- 1386 8. Click **Next**.
1387 9. Select **Microsoft Windows Event Log – Native**.



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

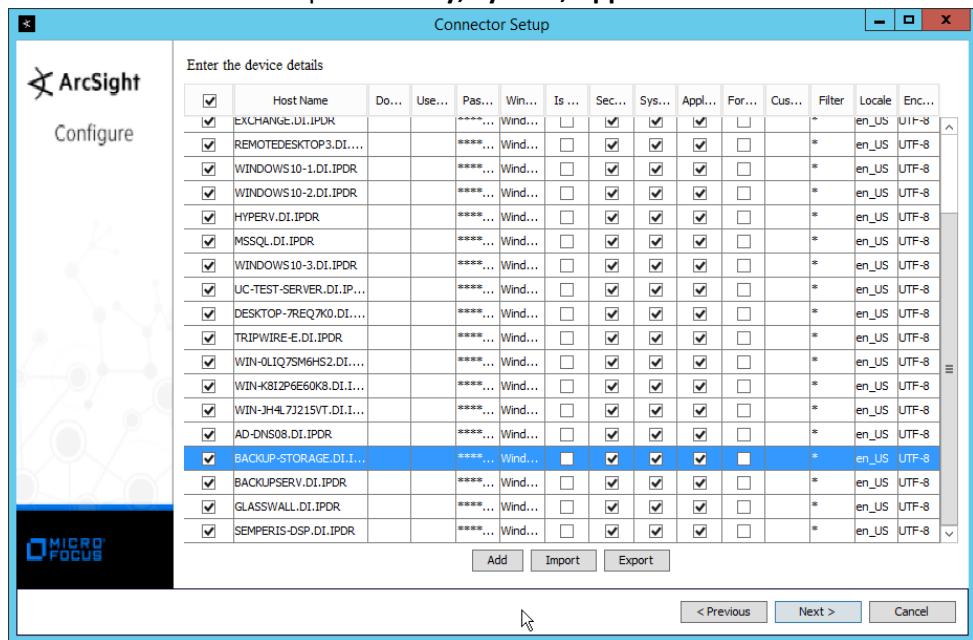


- 1391
1392 12. Click **Next**.
1393 13. Enter information about your Active Directory server (it is recommended to create a new
1394 administrator account for ArcSight to use).
1395 14. Set **Use Active Directory host results for to Replace Hosts**.



1396
1397
1398
1399

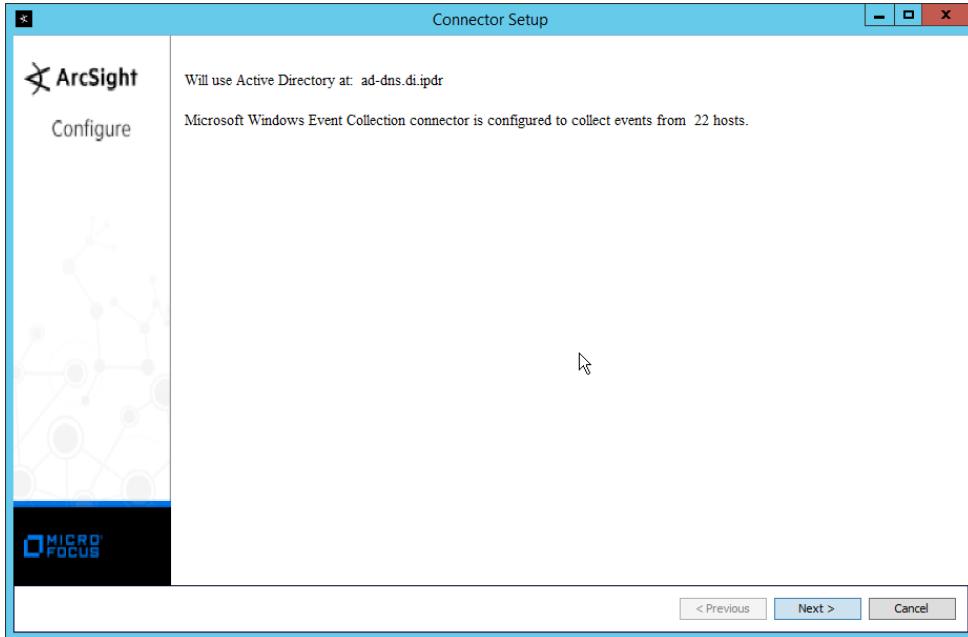
15. Click **Next**.
16. Check the boxes under any event types that should be forwarded to this connector, for each individual host. For example: **Security, System, Application**.



1400

1401

17. Click **Next**.

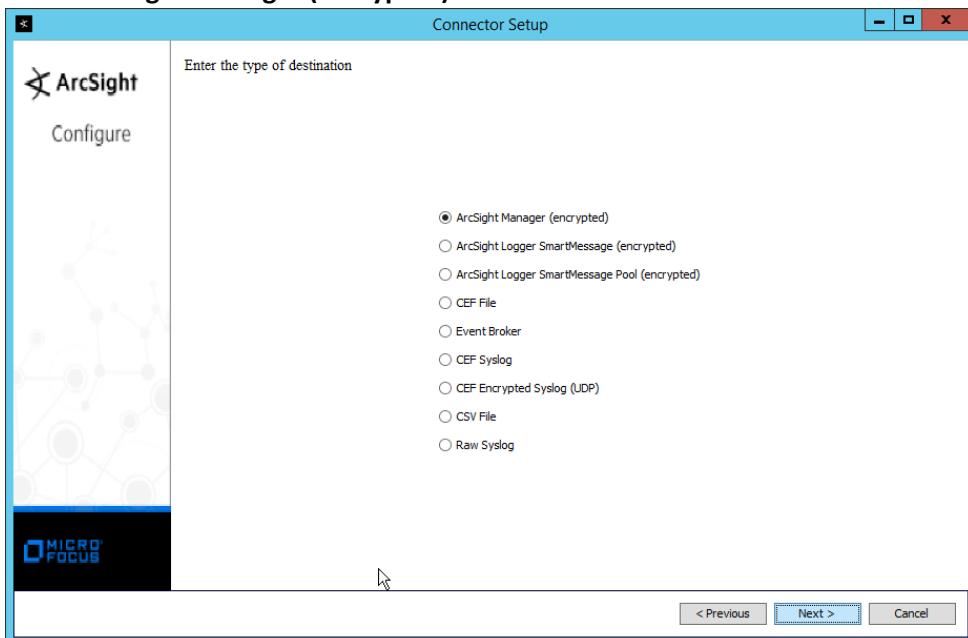


1402

18. Click **Next**.

1403

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

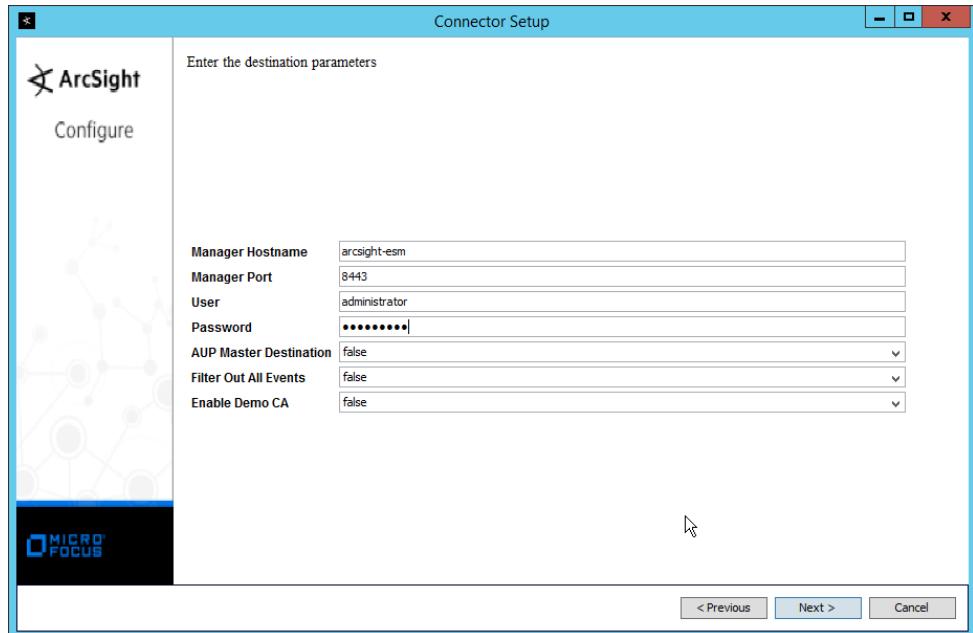


1405

20. Click **Next**.

1406

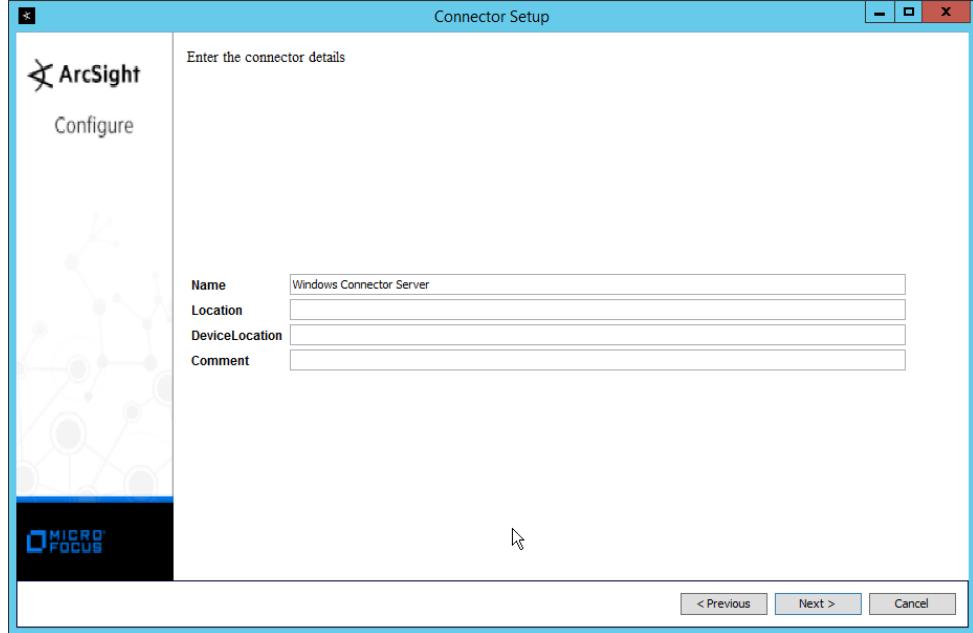
21. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.



1408

1409

1410

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

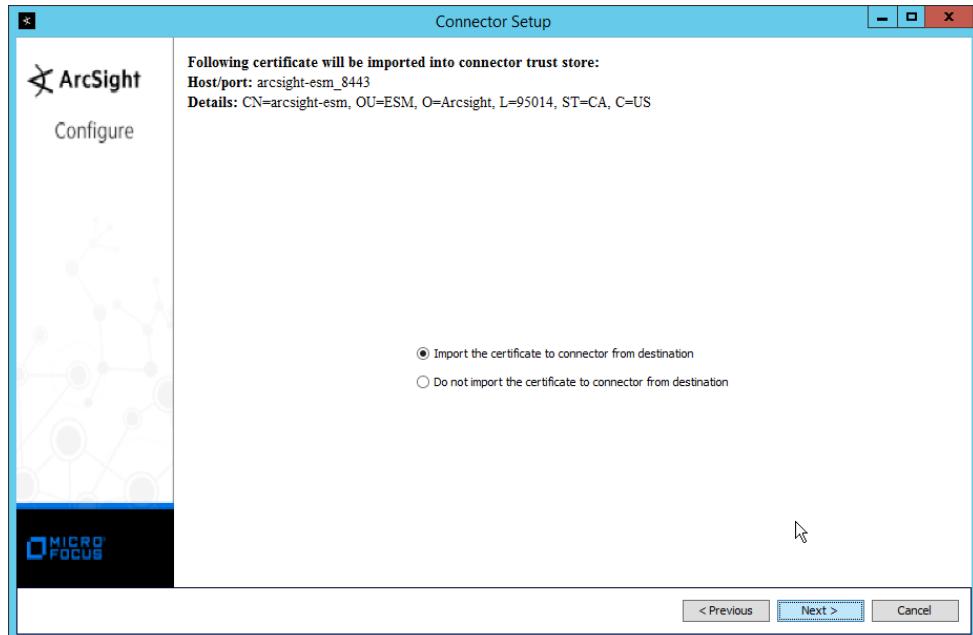
1411

1412

24. Click **Next**.

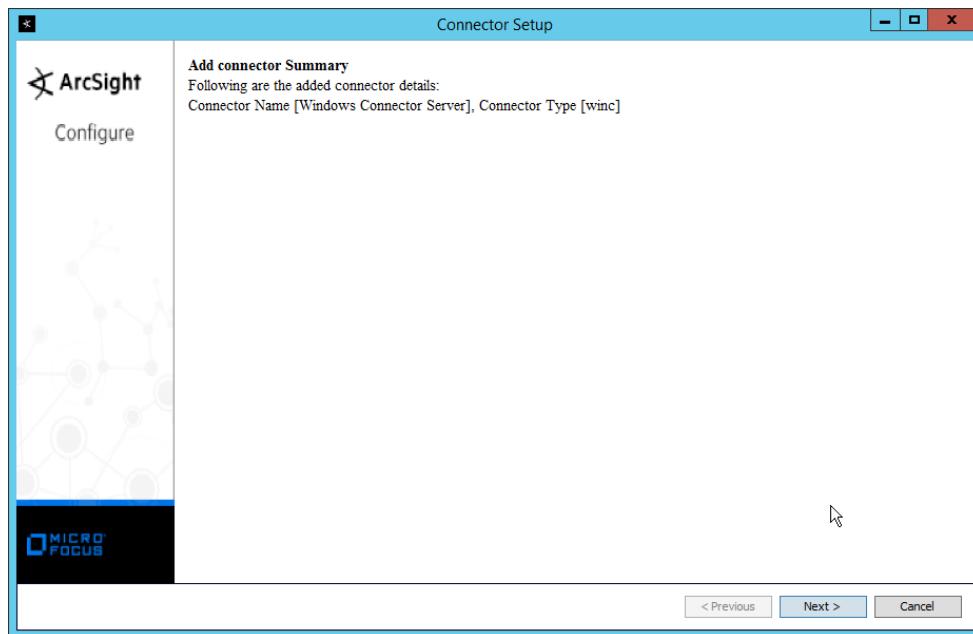
1413

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



1414
1415

26. Click **Next**.



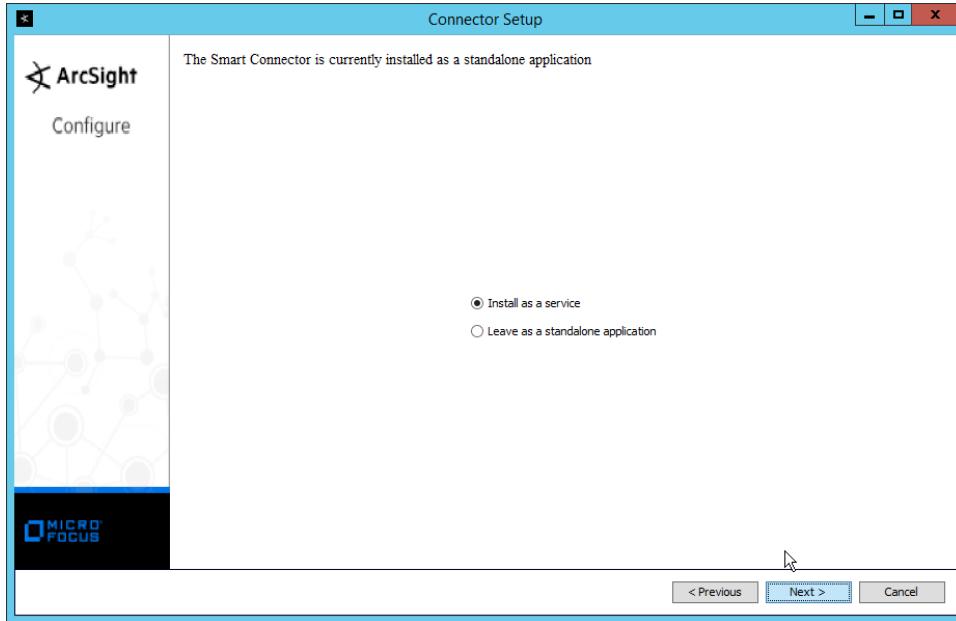
1416
1417
1418

27. Click **Next**.

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

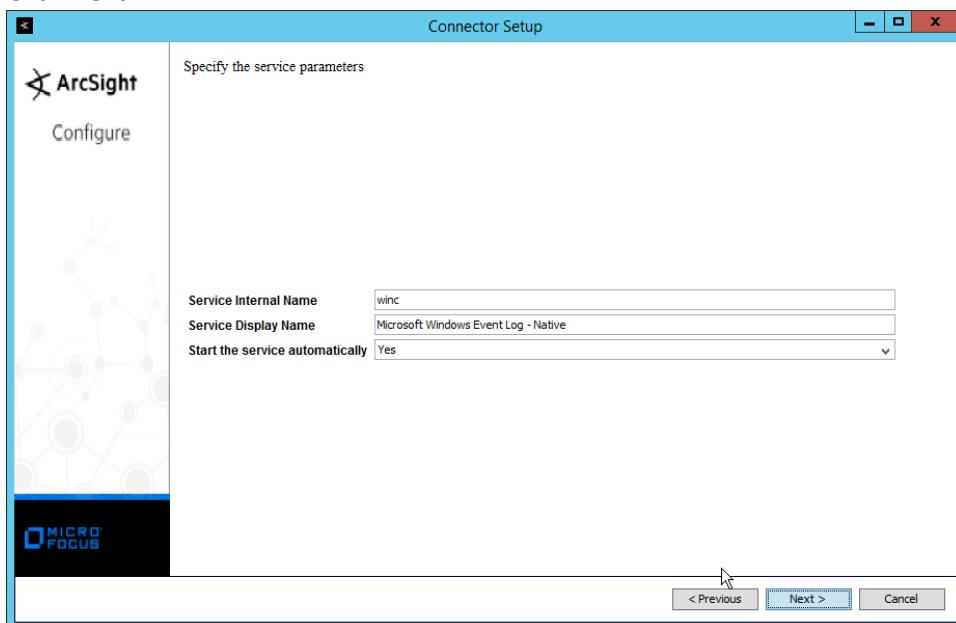
1419
1420

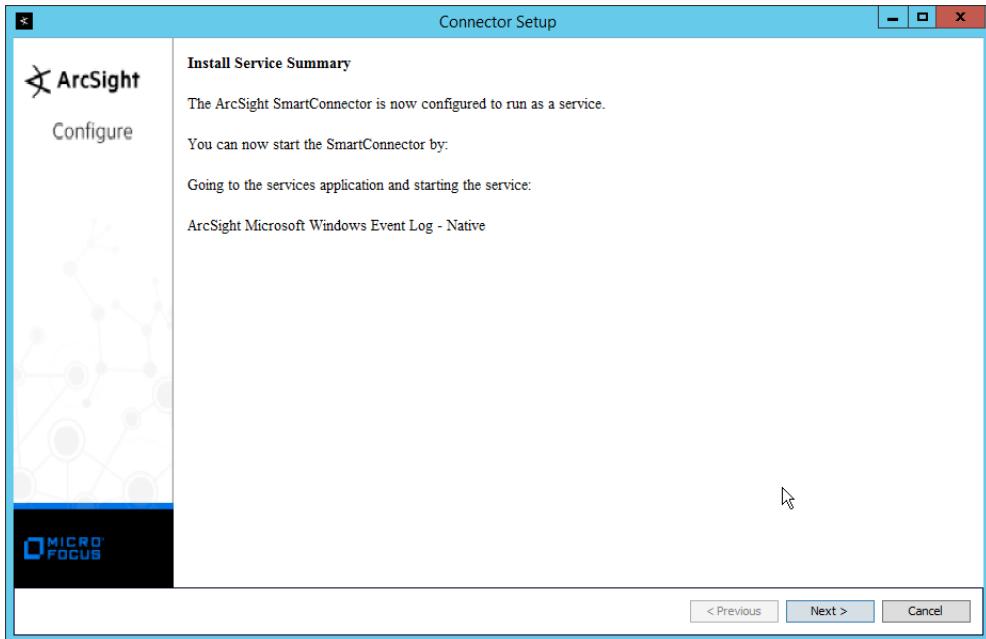
29. Click **Next**.



1421
1422

30. Click **Next**.





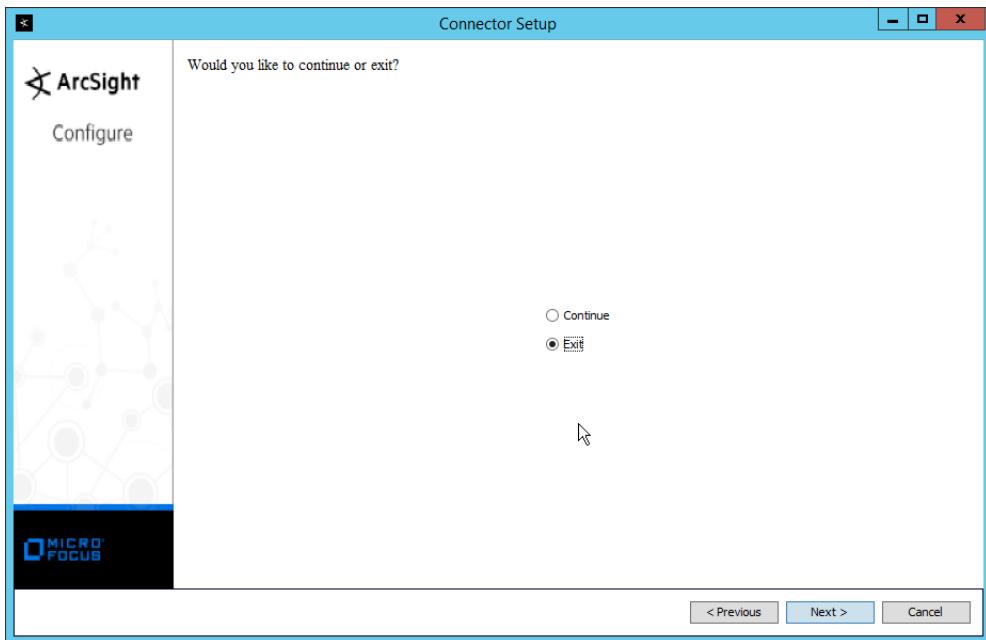
1423

1424

1425

31. Click **Next**.

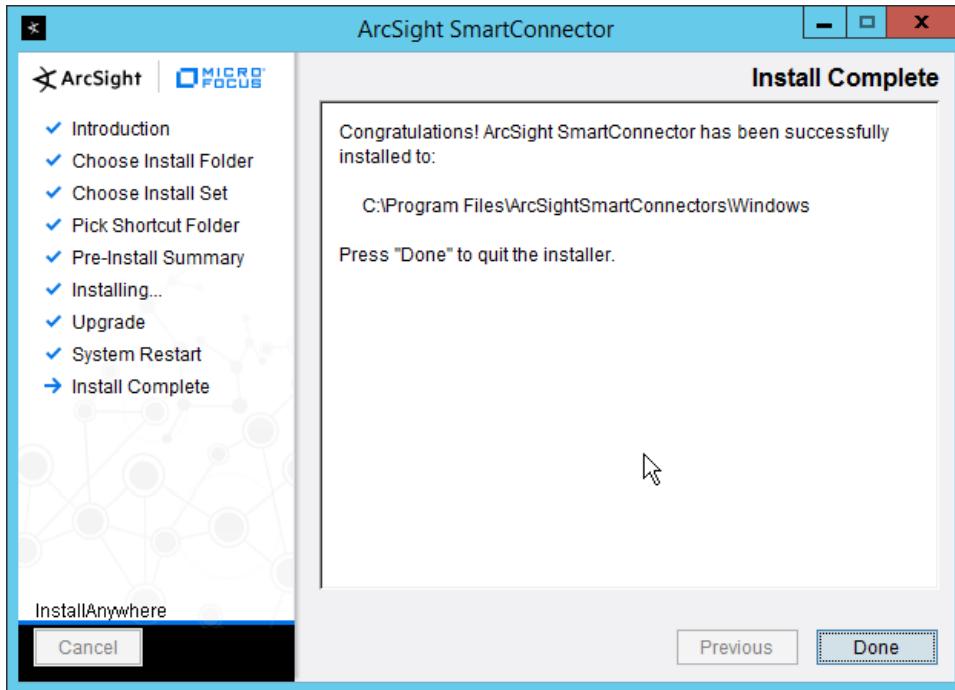
32. Select **Exit**.



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.

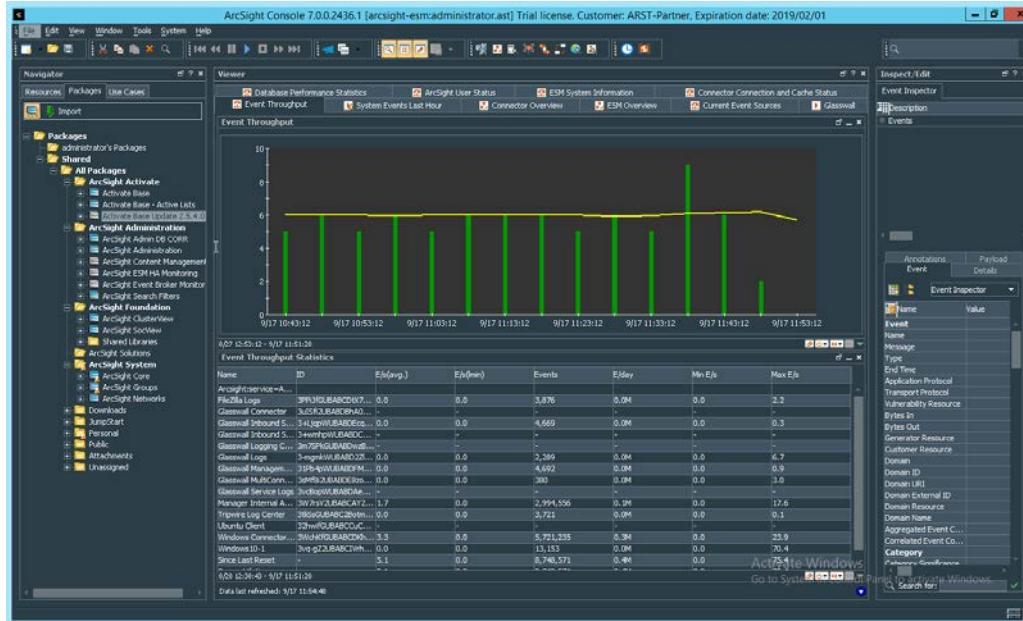


2. Click the **Download** link for the activate base. (Note: This package should be installed on the Arcsight Console, not on the ESM.)
3. Copy the contents of the zip file to *ARCSIGHT_HOME*. The default for this is *C:\arcsight\Console\current*, assuming a Windows Server.

- 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
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 2.5.4.0**, and select **Delete Package**.

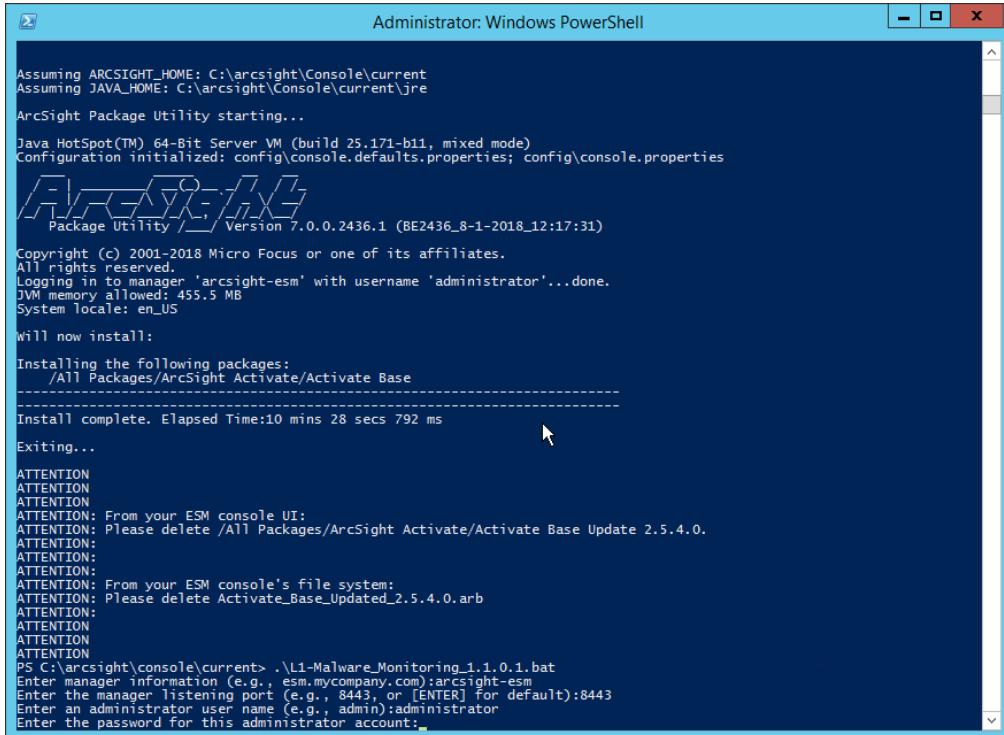
1454 2.8.5.2 Install Packages

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\current*, assuming a Windows Server.
 1466
 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



```

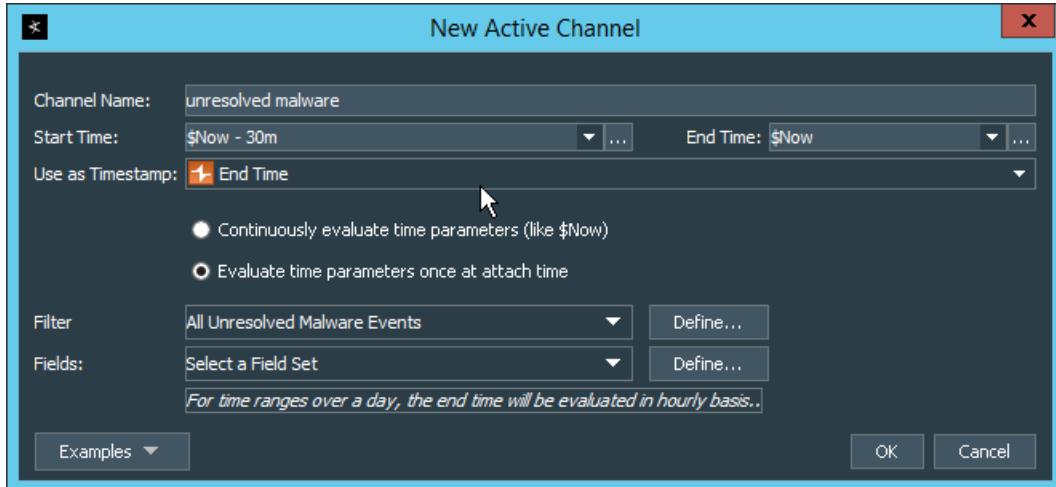
Administrator: Windows PowerShell
Assuming ARCSIGHT_HOME: C:\arcsight\Console\current
Assuming JAVA_HOME: C:\arcsight\Console\current\jre
ArcSight Package Utility starting...
Java HotSpot(TM) 64-Bit Server VM (build 25.171-b11, mixed mode)
Configuration initialized: config\Console.defaults.properties; config\Console.properties
[Progress Bar]
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 'arcsgith-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:
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):arcsgith-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 6. Enter the **hostname** of the ArcSight machine, the **port** (default: **8443**), and the **username** and
 1471 **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.

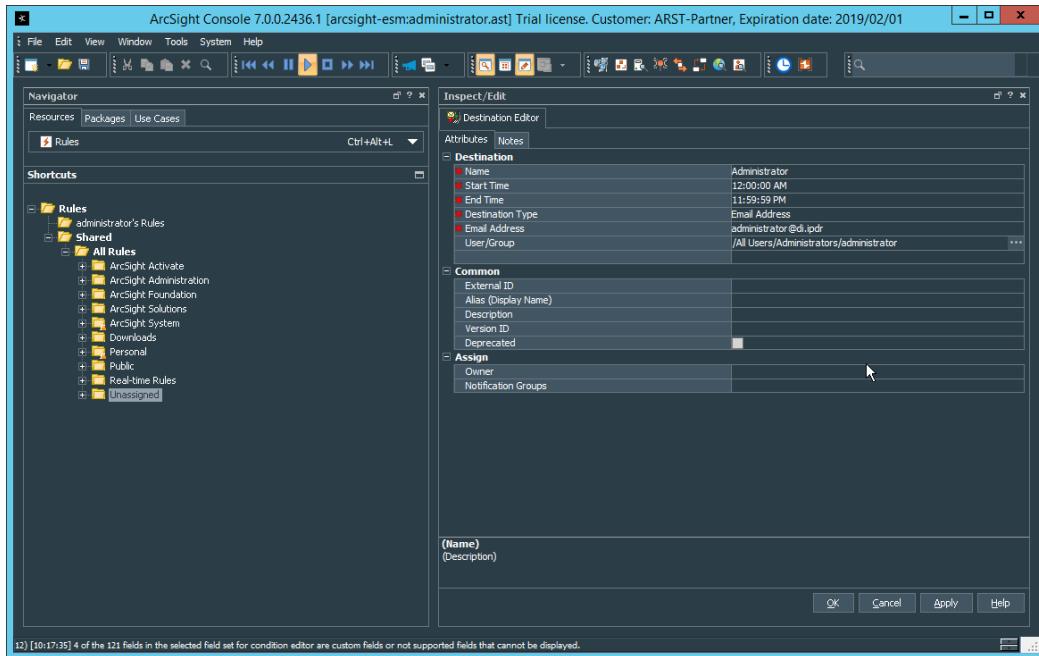


- 1478
1479 5. Click **OK**. All events that match the filter can be displayed in the newly created channel. Filters
1480 from imported packages can be found under **Filters > Shared > All Filters > ArcSight Activate >**
1481 **Solutions.**

1482 2.8.7 Configure Email Alerts in ArcSight

1483 2.8.7.1 *Configure a New Destination*

- 1484 1. In **ArcSight Console**, click **File > New > Destination**.
1485 2. Enter a name for the **Destination**.
1486 3. For **Destination Type**, select **Email Address**.
1487 4. For **Email Address**, enter the email that should be associated with this destination.



1488

5. Click **OK**.

1489

6. Select a place to save the new **Destination**.

1490

7. Click **OK**.

1491

2.8.7.2 *Configure a New Rule*

1492

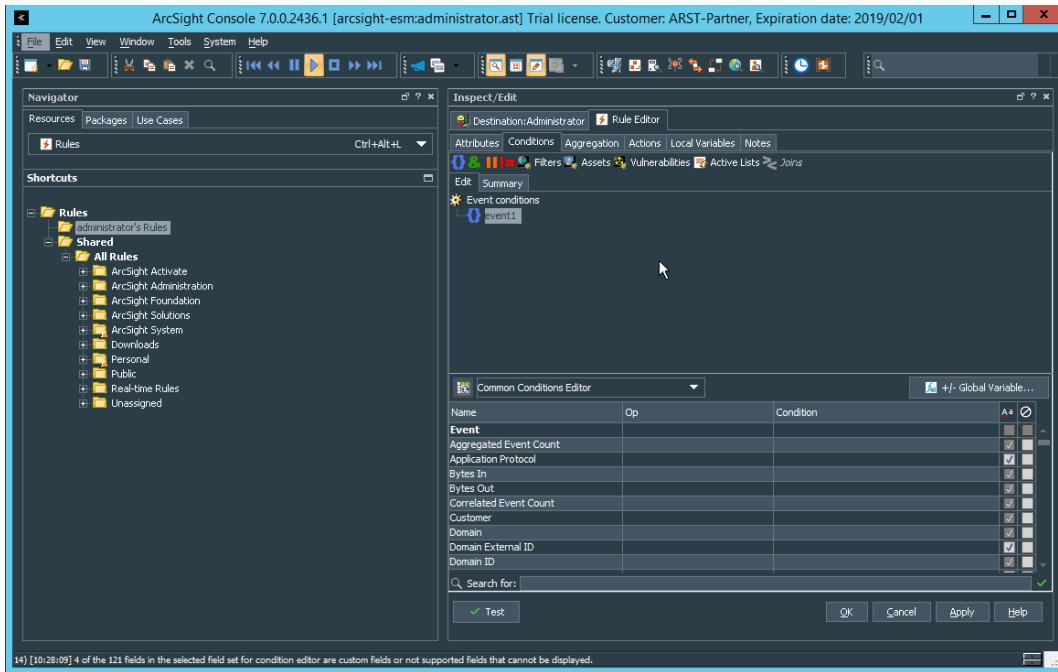
1. Click **File > New > Rule > Standard Rule**.

1493

2. Enter a name for the rule.

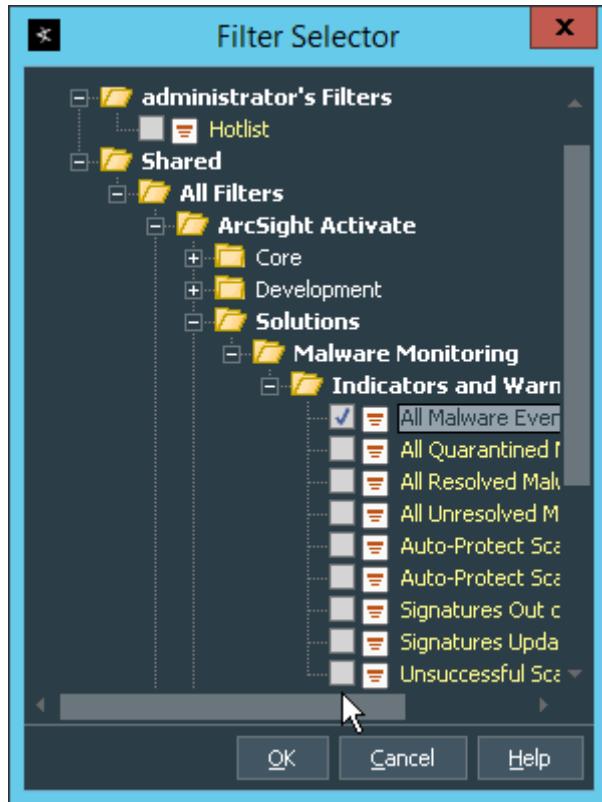
1495
1496

3. Click the **Conditions** tab.



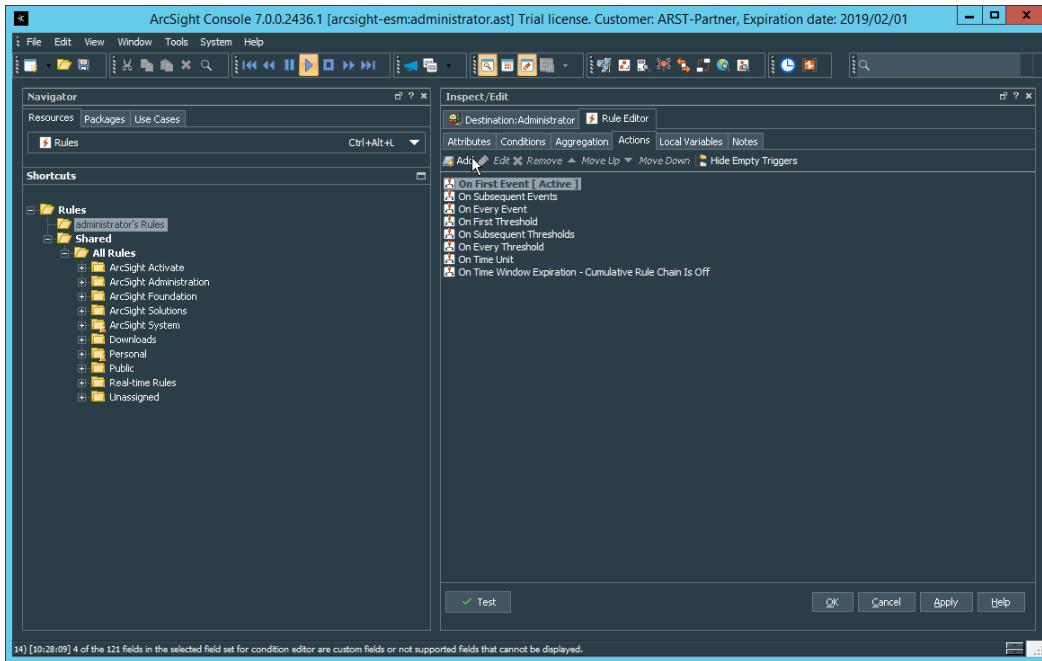
1497
1498
1499
1500

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.

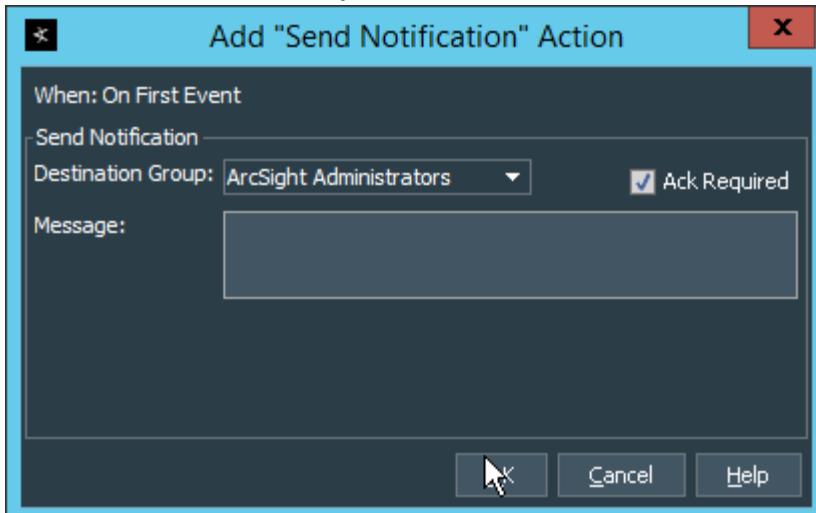


1504

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

1513 2.9.1 Install Tripwire Enterprise

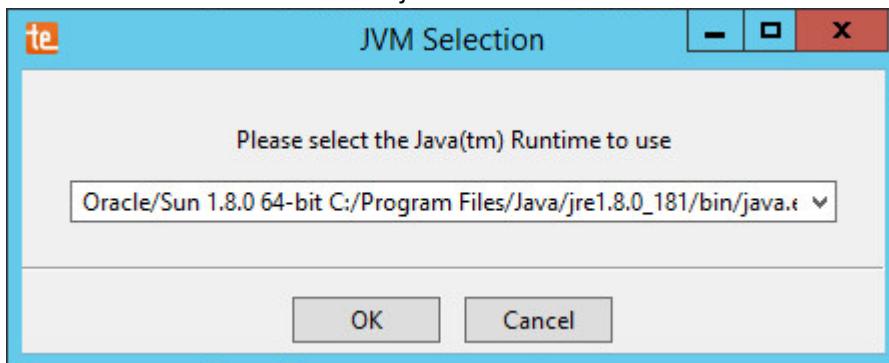
- 1514 1. Ensure that you have a current version of Oracle Java. You must install both the Java Runtime
 1515 Environment (JRE) and the Java Cryptography Extension (JCE).
 1516 2. Download and run the **JRE installer**.



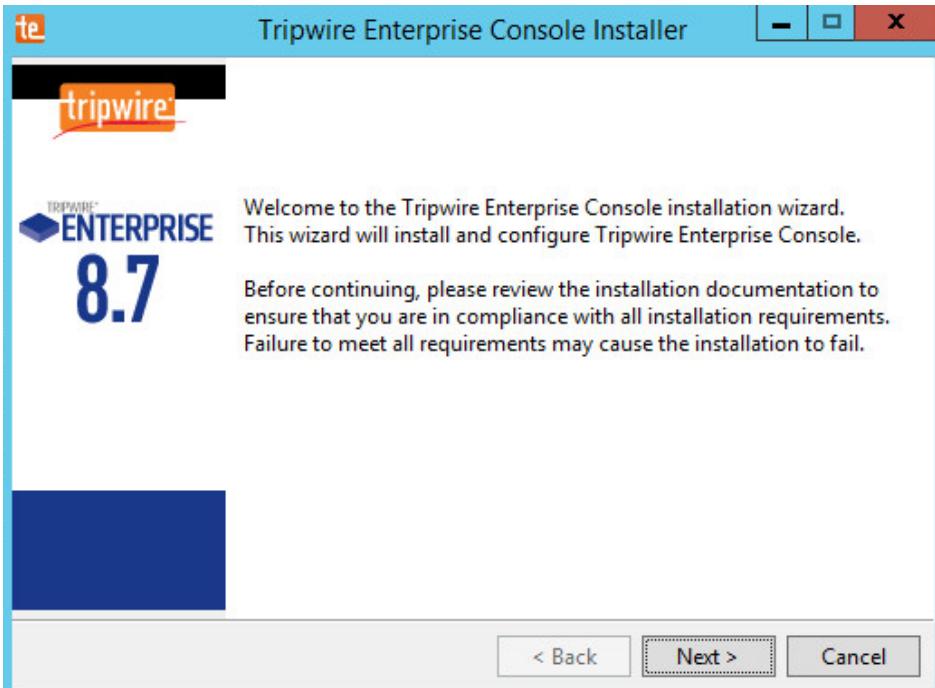
- 1517 3. Click **Install**.
 1518 4. Download the JCE, and extract the files.

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.



- 1525 8. Click **OK**.



1527

1528

1529

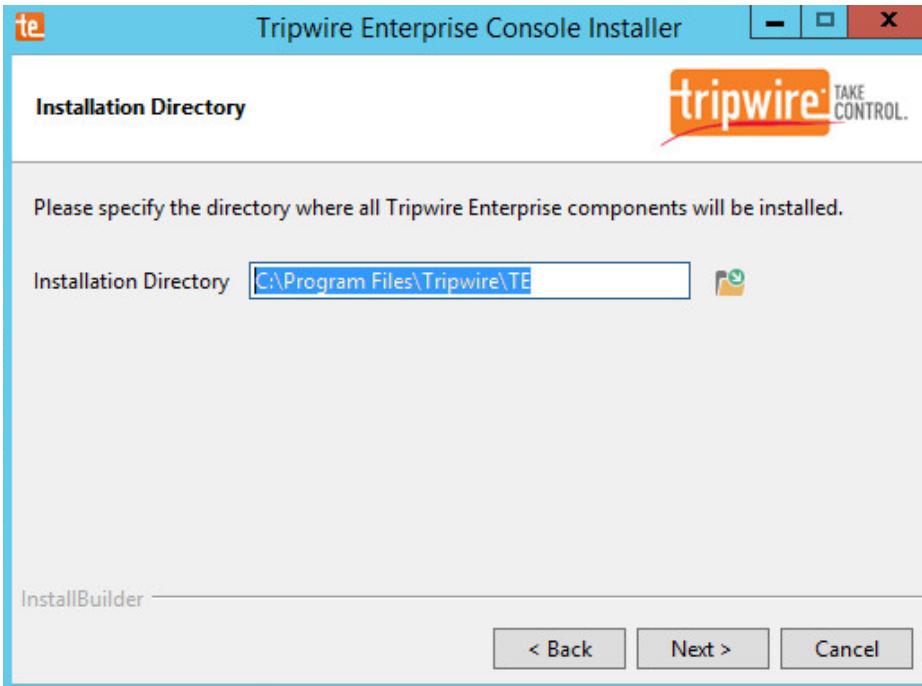
9. Click **Next**.
10. Select **I accept the agreement**.



1530

1531

11. Click **Next**.



1532

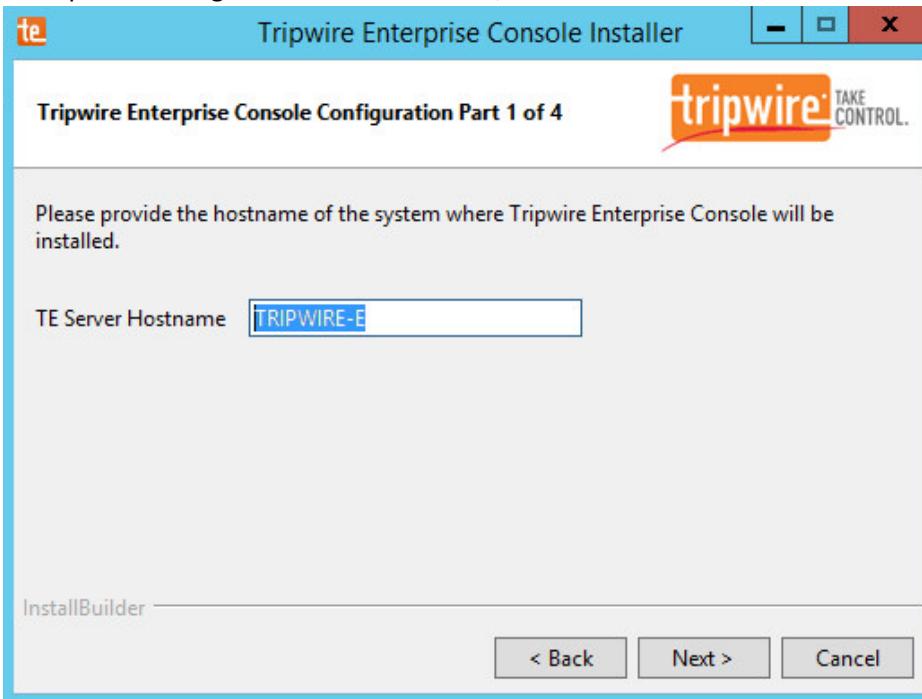
1533

12. Click **Next**.

1534

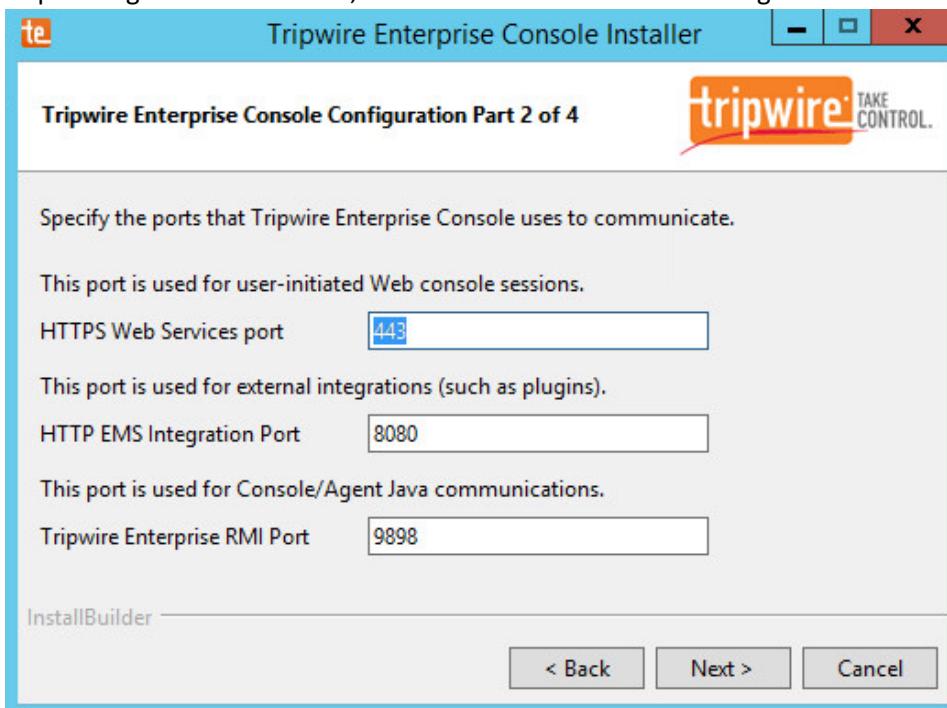
1535

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.

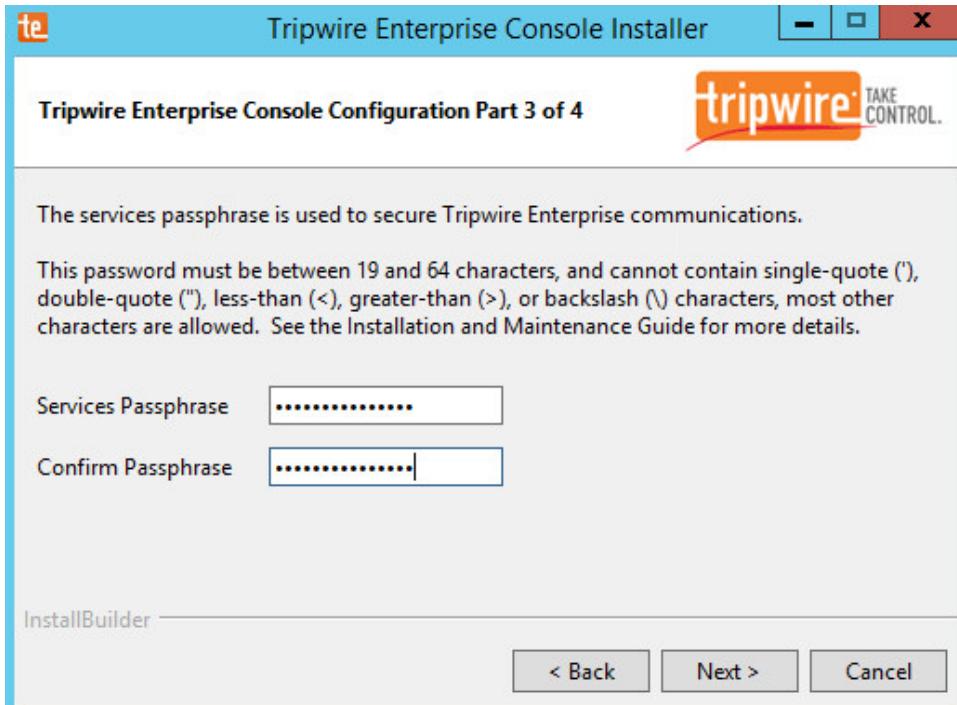


1536

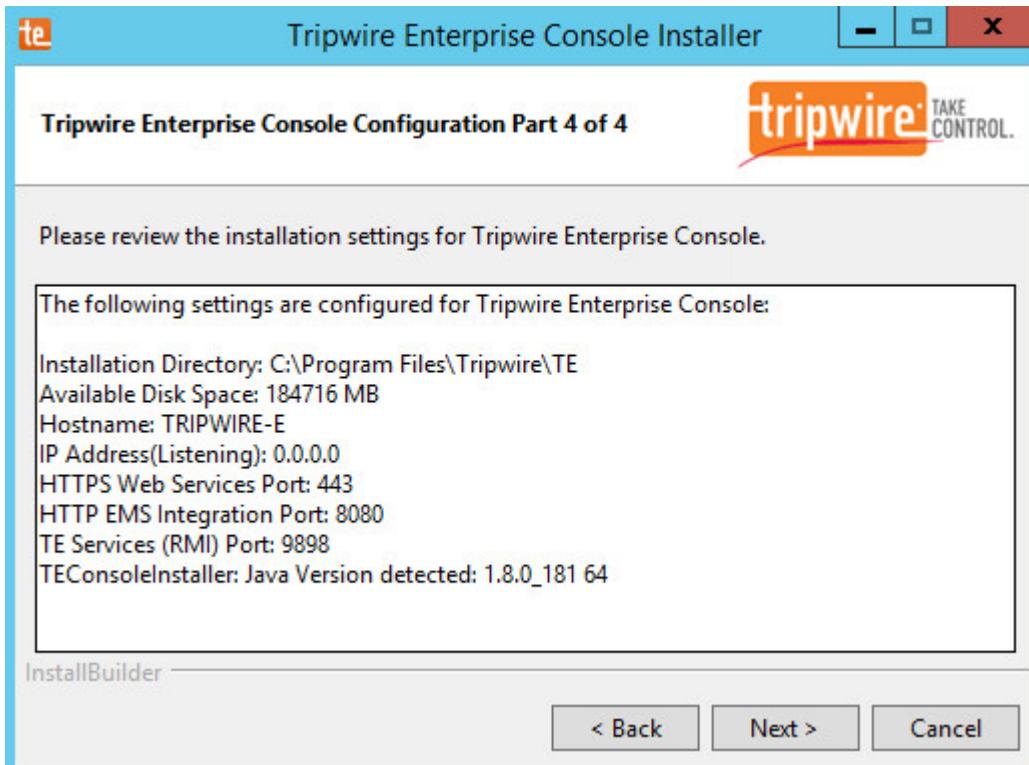
- 1537 14. Click **Next**.
1538 15. Enter the port numbers to use for each of the **HTTPS Web Services port**, **HTTP EMS Integration**
1539 **Port**, and **Tripwire Enterprise RMI port**. The RMI port is used for inbound communication from
1540 Tripwire agents to the server, so ensure that it is allowed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



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

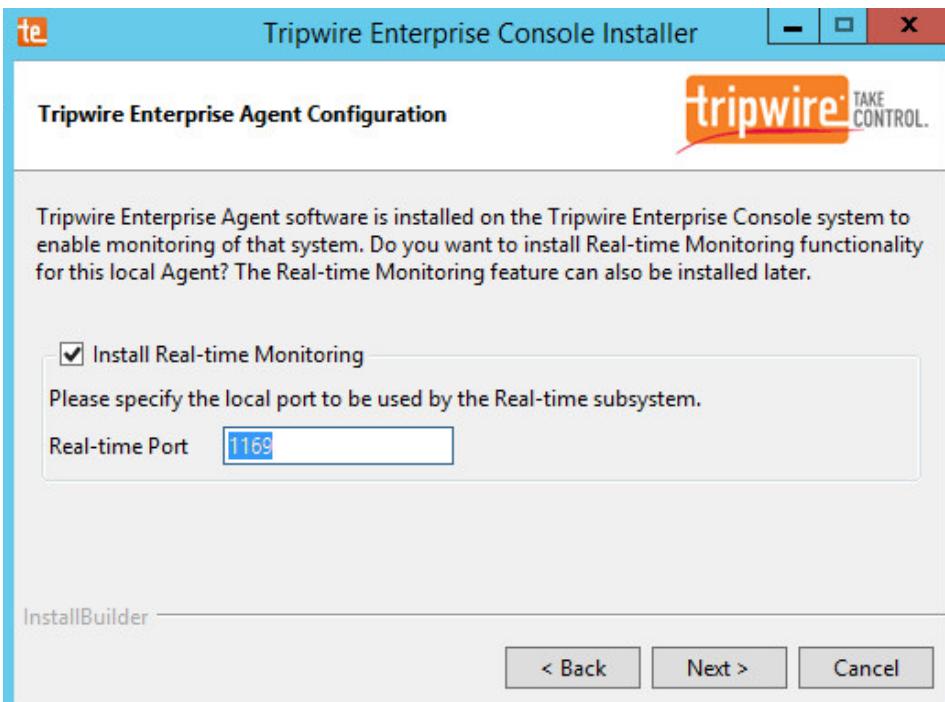
1544
1545

18. Click Next.

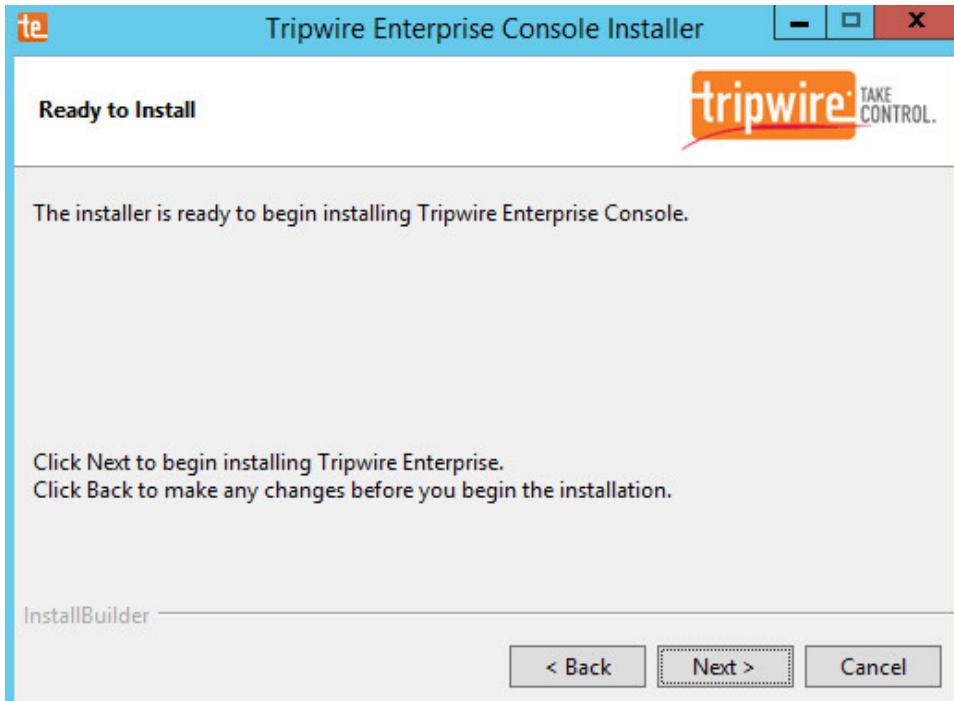


1546

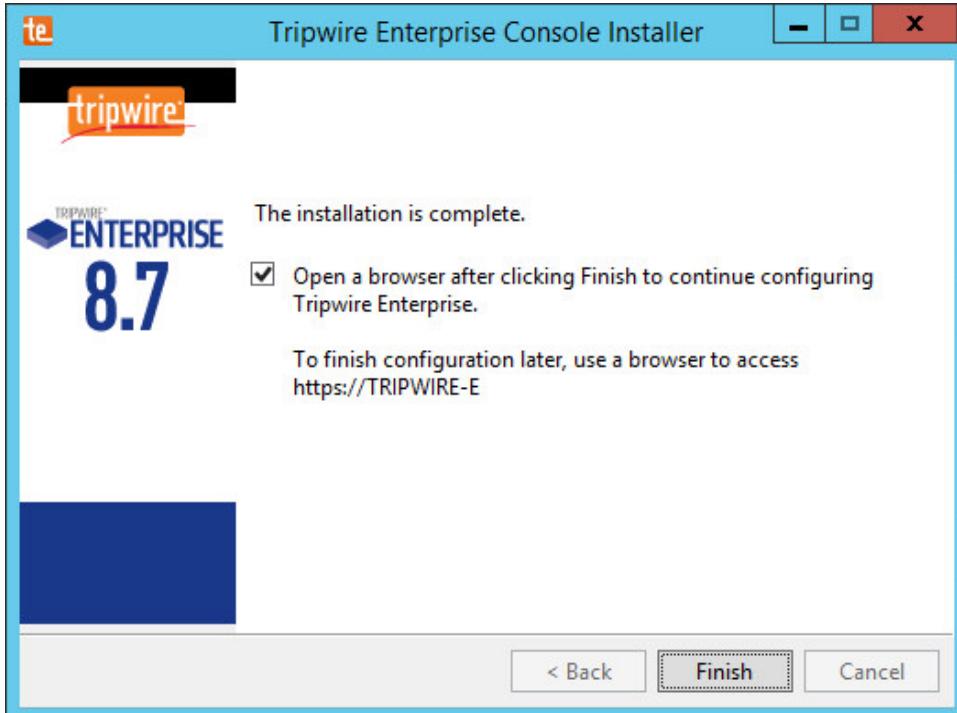
- 1547 19. Click **Next**.
1548 20. Check the box next to **Install Real-time Monitoring**.
1549 21. Enter **1169** for **Real-time Port**.



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



- 1552
1553 23. Click **Next**.
1554 24. Check the box next to **Open a browser after clicking Finish to continue configuring Tripwire Enterprise.**
1555



1556

1557

1558

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

Tripwire Enterprise Post-Install Configuration

Tripwire Enterprise needs additional configuration.
To finish installing, please enter your Services Passphrase for authentication. The Services Passphrase was created when you installed Tripwire Enterprise.

Services Passphrase:

1559

1560

27. Click **Login**.

Tripwire Enterprise Post-Install Configuration

Database Configuration Settings

These settings control how the TE Console connects to a remote database that stores data for all TE operations. You can check the current configuration here, and make any necessary changes in the fields below.

Remote Database Type: <input type="button" value="Microsoft SQL Server"/> Microsoft SQL Server Microsoft SQL Server Oracle Oracle RAC MySQL	Remote Database Type: The type of remote database used by TE
--	--

1561

1562

28. Select **Microsoft SQL Server** for **Remote Database Type**.

1563

29. Select **SQL Server** for **Authentication Type**.

1564

30. Enter login details for the account created during the MSSQL setup.

1565

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 the 'Database Configuration' section of the Tripwire Enterprise configuration tool. It includes fields for Authentication Type (SQL Server), Login Name (twadmin), Password, Database Host (192.168.78.125), Port (1433), Database Name (TE_DB), Instance Name (Optional), and SSL (Off). A detailed description of each field is provided to the right of the input fields.

Authentication Type:	SQL Server	Authentication Type: Specifies whether the database login should authenticate using a Windows account (typically of the format domain\user), or an SQL Server account (an account defined only in SQL Server). With the Windows authentication type, NTLMv2 should be used, as it is cryptographically superior to the first version of NTLM. However, as NTLMv2 is configured in the operating system, not in the database or application, TE can be used with NTLM to ensure compatibility.
Login Name:	twadmin	Login Name: The login name that TE will use to authenticate with the database.
Password:	*****	Password: The password that TE will use to authenticate with the database.
Database Host:	192.168.78.125	Database Host: The fully qualified domain name, hostname or IP address of the system where the database is installed.
Port (default 1433):	1433	Port: The TCP port that the database is listening on. If an Instance Name is specified here, then the database connection will use UDP 1434 to connect to the SQL Server Browser Service, and this Port field will be disabled. The SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance.
Database Name:	TE_DB	Database Name: The name of the database that TE should use when connecting to the remote database. Note that the login name in SQL Server should have this database set as the default, and the login name should be mapped to this database.
Instance Name (Optional):		Instance Name (Optional): The location/name of the database instance on the server. Ask your DBA if a non-default instance should be used for TE.
SSL:	Off	SSL (Secure Sockets Layer): Specifies whether the database connection should request, require or authenticate SSL. <ul style="list-style-type: none">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.

Activate Windows
Go to System in Control Panel

Test Database Login ✓

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

The screenshot shows the 'Test Results' section of the configuration tool. It displays a message: 'Connection Succeeded.' Below this, there is a 'Save Configuration and Restart Console' button and a 'Logout' button.

Test Results:	Connection Succeeded.
---------------	-----------------------

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

Save Configuration and Restart Console Logout

Activate Windows
Go to System in Control Panel

- 1571 36. Click **Save Configuration and Restart Console**.
- 1572 37. After the reboot, enter a new administrator password.

1574
1575

38. Click Confirm and Continue.

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:

[Confirm and Continue](#)

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?](#)

[Generate Support Bundle](#)

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

[Logout](#)1576
1577

39. Click Configure Tripwire Enterprise.

Tripwire Enterprise Fast Track

Welcome to Tripwire Enterprise Fast Track!

tripwire 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.

[Configure Tripwire Enterprise](#) [Private](#) [Cancel](#)

1578
1579
1580

- Step 1: Add your Tripwire Enterprise license (*.cert)**
- No file chosen
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

- Step 2: Configure Change Auditing and/or Policy Management**
- | | |
|----------------------|--|
| Monitoring Solutions | <input checked="" type="checkbox"/> Change Auditing
<input checked="" type="checkbox"/> Policy Management |
| Available Policies | <input type="checkbox"/> CIS
<input checked="" type="checkbox"/> PCI
<input type="checkbox"/> DISA
<input type="checkbox"/> NIST 800-53 (FISMA) |
42. Select any available policies desired.

Step 3: Specify the platforms to monitor

Note: You are licensed for the **Highlighted** platforms.

Available Platforms:

Operating System <input checked="" type="checkbox"/> Microsoft Windows Server 2008 R2 <input checked="" type="checkbox"/> Microsoft Windows Server 2012 R2 <input checked="" type="checkbox"/> Oracle Solaris 10 <input checked="" type="checkbox"/> Oracle Solaris 11 <input checked="" type="checkbox"/> Red Hat Enterprise Linux 6 <input checked="" type="checkbox"/> Red Hat Enterprise Linux 7 Virtual Infrastructure <input checked="" type="checkbox"/> VMware ESXi 5.5 Server	Selected Platforms: <input checked="" type="checkbox"/> Microsoft Windows Server 2008 R2 <input checked="" type="checkbox"/> Microsoft Windows Server 2012 R2 <input checked="" type="checkbox"/> Oracle Solaris 10 <input checked="" type="checkbox"/> Oracle Solaris 11 <input checked="" type="checkbox"/> Red Hat Enterprise Linux 6 <input checked="" type="checkbox"/> Red Hat Enterprise Linux 7 <input checked="" type="checkbox"/> VMware ESXi 5.5 Server
--	--

1583
1584

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

Step 4: Set up a schedule for running checks and reports

Change Audit Scheduling Checks How frequently would you like to run checks on your assets? <input type="button" value="Daily"/> Run the checks at <input type="button" value="1:00"/> <input type="button" value="AM"/>	Reports How frequently would you like to run reports on your assets? <input type="button" value="Daily"/> Run the reports at <input type="button" value="4:00"/> <input type="button" value="AM"/>
---	--

Policy Scheduling Checks How frequently would you like to run checks on your assets? <input type="button" value="Weekly"/> on <input type="button" value="Sundays"/> Run the checks at <input type="button" value="1:00"/> <input type="button" value="AM"/>	Reports How frequently would you like to run reports on your assets? <input type="button" value="Weekly"/> on <input type="button" value="Sundays"/> Run the reports at <input type="button" value="4:00"/> <input type="button" value="AM"/>
--	---

Enable Checks and Reports (Optional)

Note: Tripwire does not recommend enabling checks and reports until after you have installed Tripwire Agent software on the systems that you want to monitor.

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.**

Step 5: Configure an email server for sending reports and alerts

Set up the email server now
 Set up the email server at another time

Before Tripwire Enterprise can deliver alerts or reports, an email server must be created. You can set up the server now, or you can wait and do it later using the Tripwire Enterprise Console.

1590
1591
1592
1593**46. Enter a username and password for a new administrator account for TE Console.**
47. Click Preview Configuration.

Tripwire Enterprise Configuration

These tasks will be applied to your configuration

- Critical Change Audit Check - RHEL 6
- Critical Change Audit Check - RHEL 7
- Critical Change Audit Check - Solaris 10
- Critical Change Audit Check - Solaris 11
- Critical Change Audit Check - Windows
- Policy Check - RHEL 6
- Policy Check - RHEL 7
- Policy Check - Solaris 10
- Policy Check - Solaris 11
- Policy Check - VMware ESX
- Policy Check - Windows
- Report Task - Daily File System Changes by Node
- Report Task - Daily File System Changes by Rule
- Report Task - Test Result Summary - Red Hat - PCI v3.1
- Report Task - Test Result Summary - Solaris - PCI v3.1
- Report Task - Test Result Summary - VMware ESX - PCI v3.1
- Report Task - Test Result Summary - Windows - PCI v3.1
- Report Task - Test Results by Node - Red Hat - PCI v3.1
- Report Task - Test Results by Node - Solaris - PCI v3.1
- Report Task - Test Results by Node - VMware ESX - PCI v3.1
- Report Task - Test Results by Node - Windows - PCI v3.1
- Report Task - Top 5 Nodes with Daily Changes
- Report Task - Waivers - Red Hat - PCI v3.1
- Report Task - Waivers - Solaris - PCI v3.1
- Report Task - Waivers - VMware ESX - PCI v3.1
- Report Task - Waivers - Windows - PCI v3.1

These home pages will be applied to your configuration

Change Audit

Customer Center Home Page

PCI Overview - Red Hat

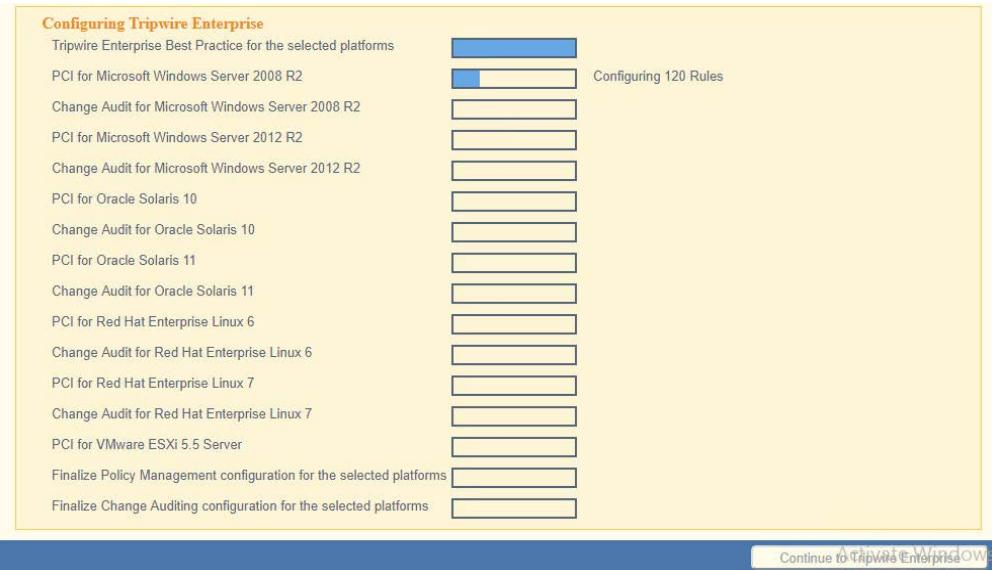
PCI Overview - Solaris

PCI Overview - VMware ESX

PCI Overview - Windows

Tripwire Enterprise Administrator

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
1600
1601
1602
1603
1604
1605
1606
1607
1608

1. Ensure that TCP traffic on port 5670 is allowed through the firewall.
2. Navigate to the TE Console installation directory, to the `/server/data/config` folder. Copy `bridge_sample.properties` to `bridge.properties`.
3. In the `bridge.properties` file, find the line that says:
`#tw.cap.bridge.registrationPreSharedKey=`
 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.
4. Restart the TE console by running the following command from an administrator command prompt, where `<te_root>` is the TE installation directory:
`> <te_root>/server/bin/twserver restart`

1609

2.9.3 Install the Axon Agent (Windows)

1610
1611
1612
1613
1614
1615
1616

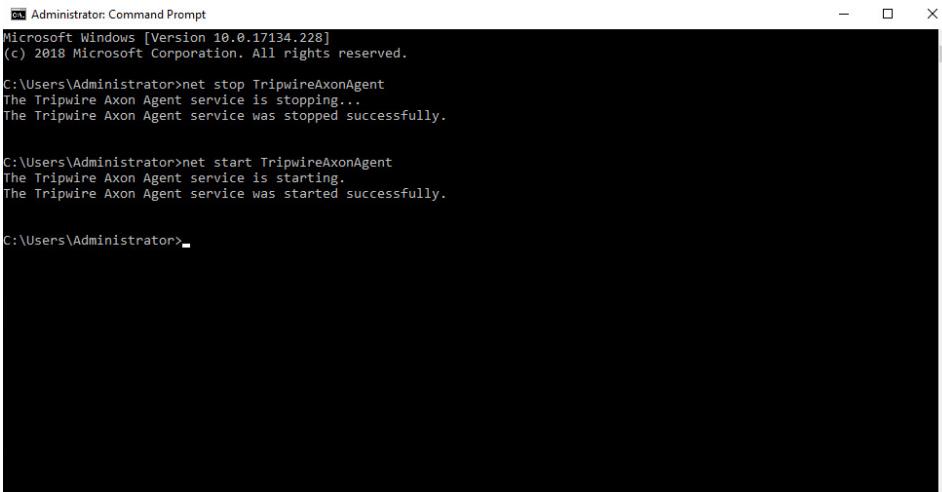
1. Download the *Axon Agent* .zip file from the Tripwire customer website (<https://tripwireinc.force.com/customers>), under the **Product Downloads** tab.
2. Unzip the file.
3. To begin the installation, double-click the `.msi` file in the extracted folder. Note: No installation wizard will appear; the installation happens automatically.
4. After the Axon Agent is installed, navigate to `C:\ProgramData\Tripwire\agent\config`, and copy `twagent_sample.conf` to `twagent.conf`.

```

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

```

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



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The window displays the following text:

```

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 2.9.4 Install the Axon Agent (Linux)

- 1628 1. Download the Axon Agent *.tgz* file from the Tripwire customer website
1629 (<https://tripwireinc.force.com/customers>), under the **Product Downloads** tab.
- 1630 2. To install the software, run the following commands:
1631 RHEL or CentOS: > `rpm -ivh <installer_file>`
1632 Debian or Ubuntu: > `dpkg -i <installer_file>`
- 1633 3. Navigate to */etc/tripwire/* and copy *twagent_sample.conf* to *twagent.conf*.
- 1634 4. Open *twagent.conf*, and find the line that says `bridge.host`. Remove the # character, and enter
1635 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 Family, Primary Function**). Click **Add** if adding your own tag set.

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

Create and Edit Tag Sets

Add a new tag set

x Location (Add tags)

Add a new tag Add

x ▾ Owner (1 tag)

Add a new tag Add

x DI Testing

x ▾ Platform Family (4 tags)

Add a new tag Add

x Red Hat
x Solaris
x VMware ESX
x Windows

x ▾ Primary Function (1 tag)

Add a new tag Add

x Domain Controller

x Tutorial (Add tags)

Tutorial tag Add

1677

1678 6. Click **Add**.

1679 7. Navigate to **Nodes > Asset View > Filter Assets**.

1680 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

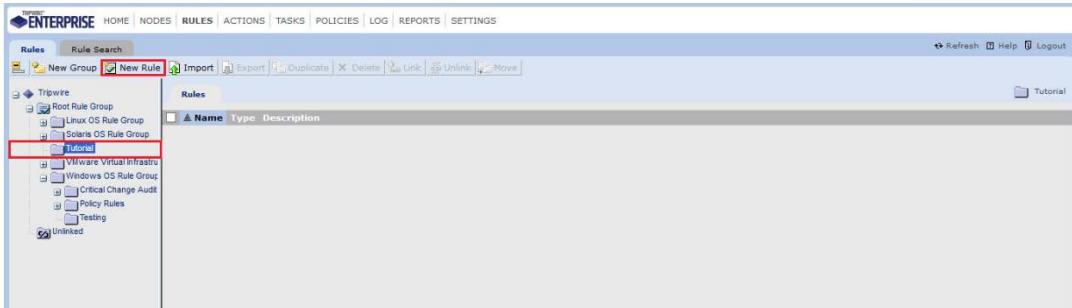
1687 This section will describe how to create a rule.

- 1688 1. Click **Rules**.

1689

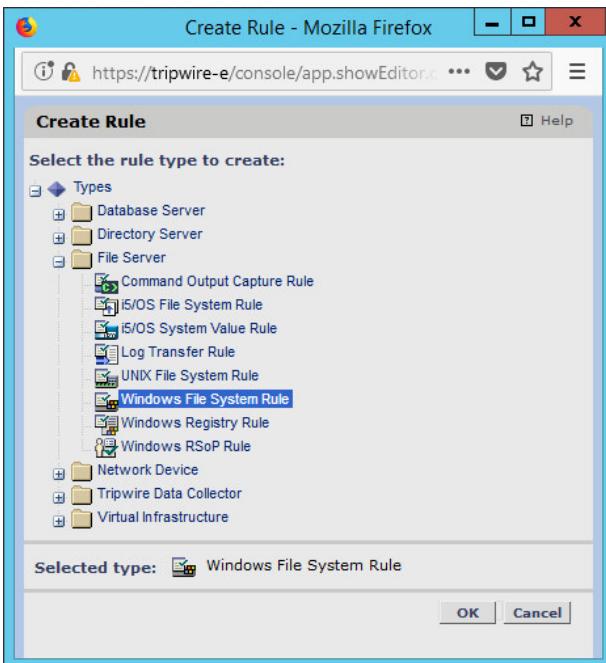
1690

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**.

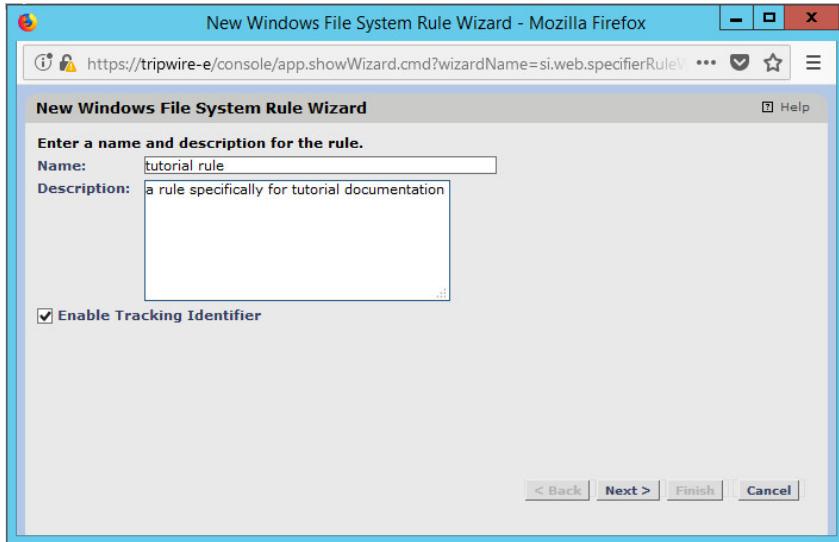


1696
1697
1698

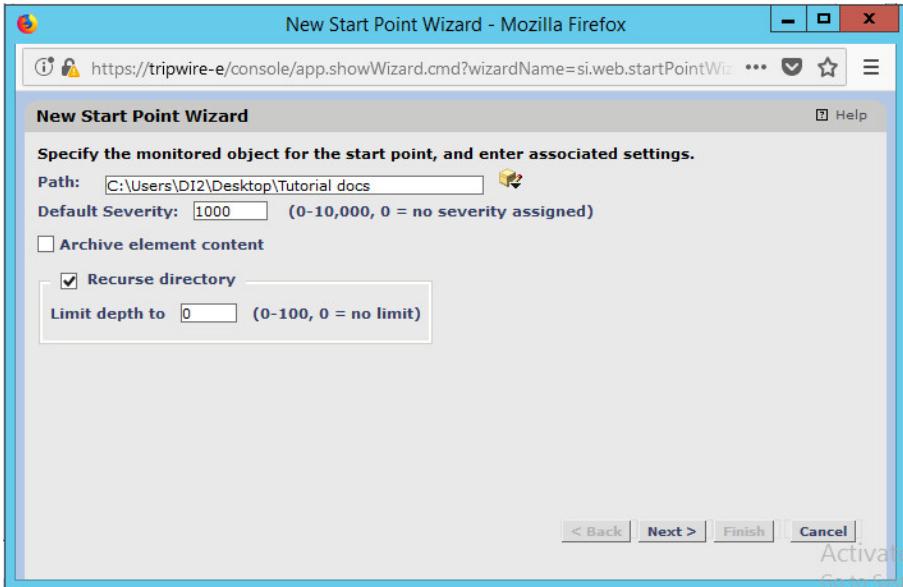
5. Click **OK**.
6. Enter a **name** and **description** for the rule.

1699
1700

7. Click **Next**.

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.

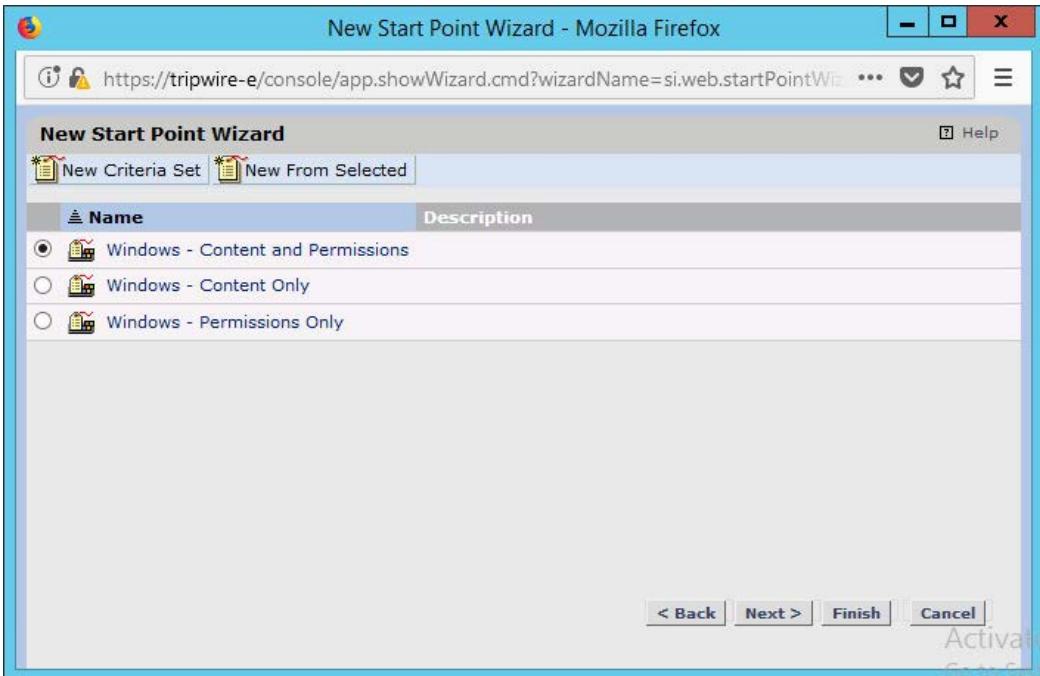


1707

1708

11. Click **Next**.

1709

12. Select **Windows Content and Permissions**.

1710

1711

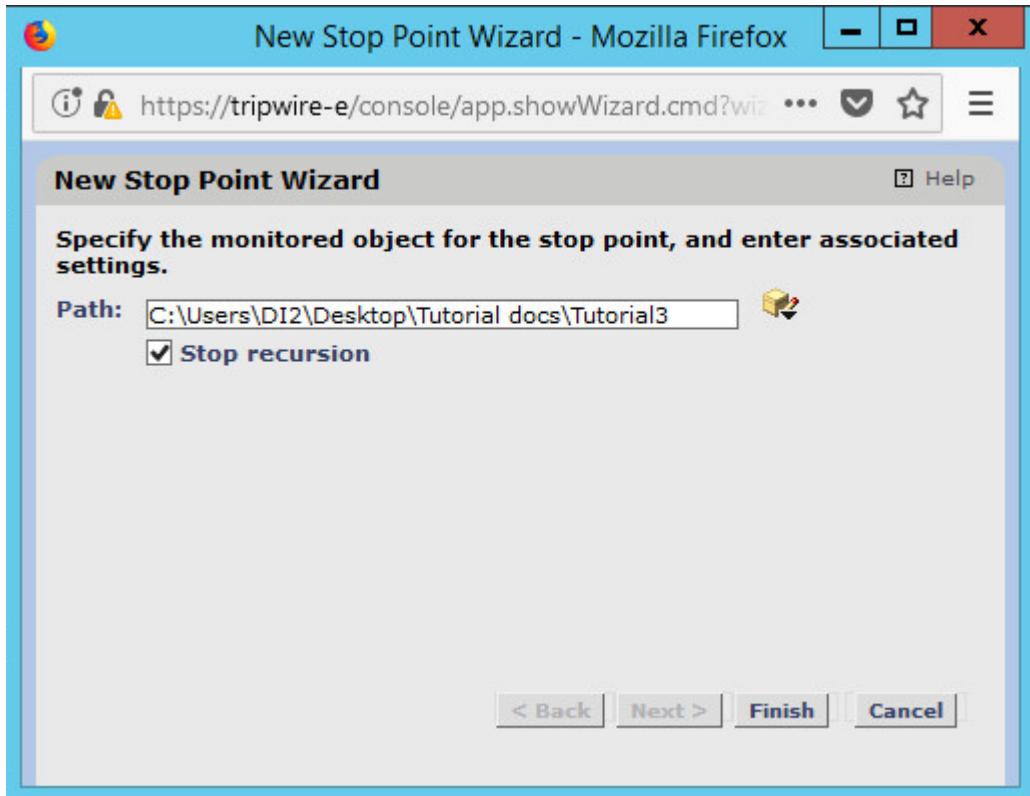
13. Click **Finish**.

1712

14. Click **New Stop Point**.

1713

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.
1714



1715
1716
1717
1718
1719

16. Click **Finish**.
17. Click **Next**.
18. Click **Next**.
19. Click **Finish**.

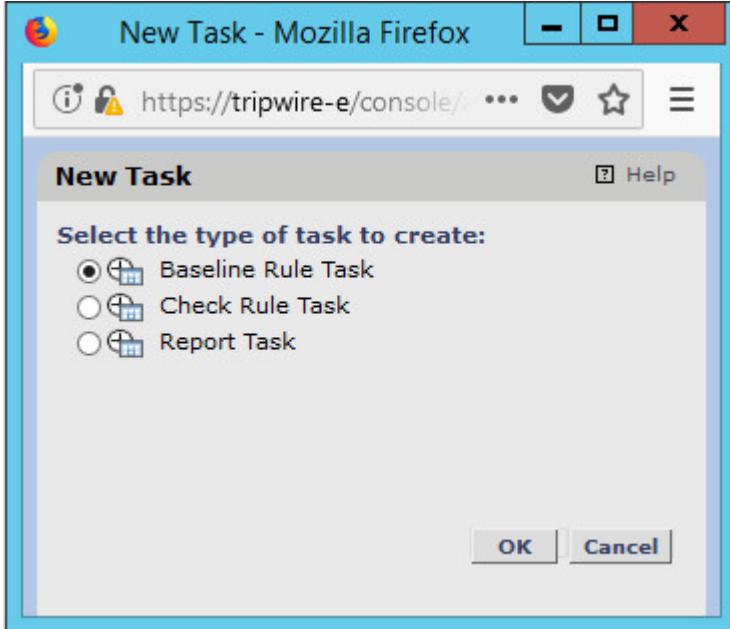
1720 **2.9.5.4 Tasks**

1721 This section will describe how to create a task.

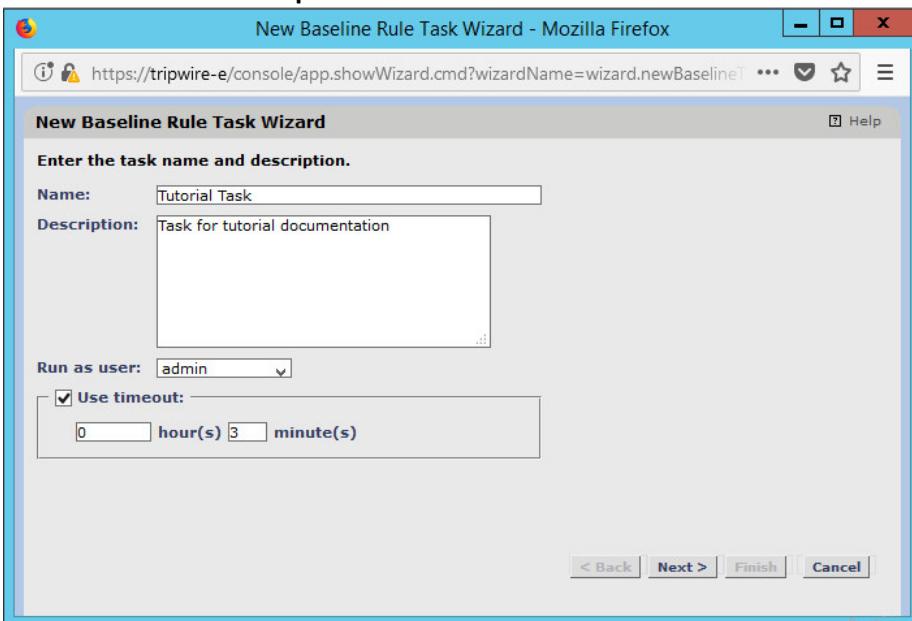
- 1722 1. Click **Tasks**.

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

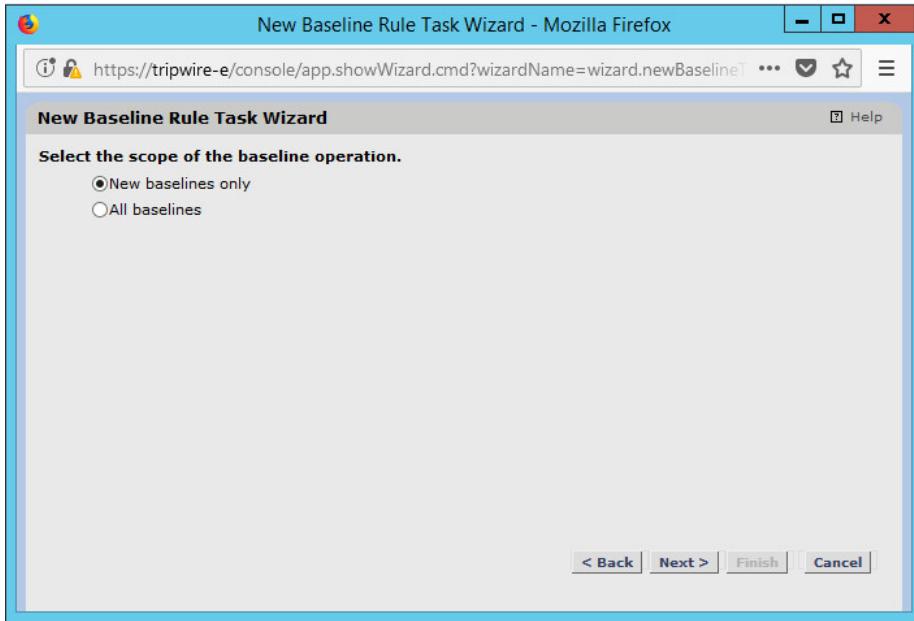
- 1727 4. Select **Baseline Rule Task** or **Check Rule Task** (Note: Both are needed: baseline creates the
1728 initial state of the monitored object, and check updates the state and reports any changes).



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

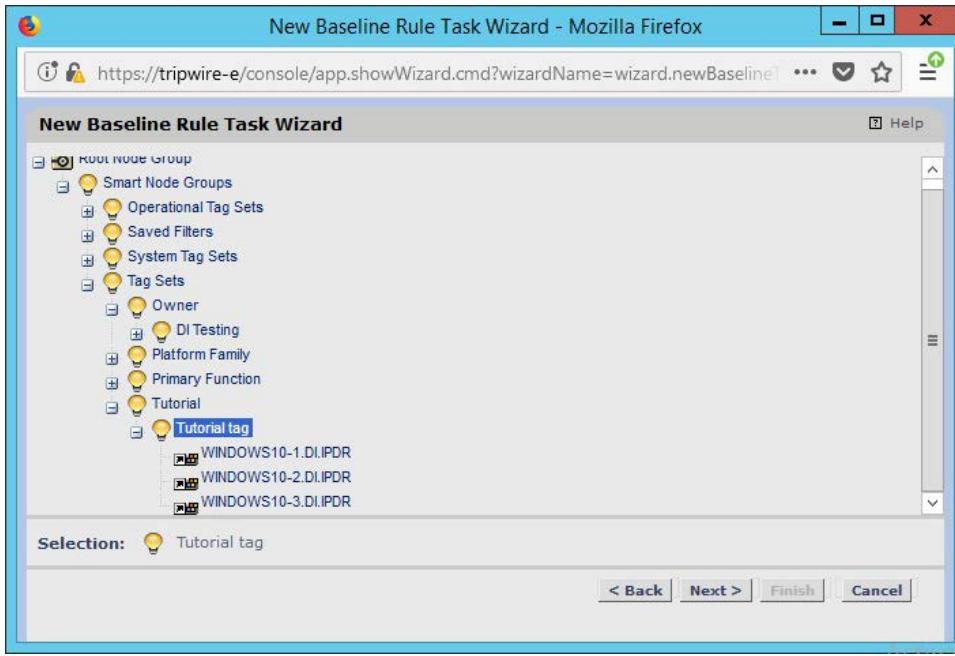


- 1732 7. Click **Next**.
1733 8. Select whether you want all baselines to be updated or to only create new baselines.



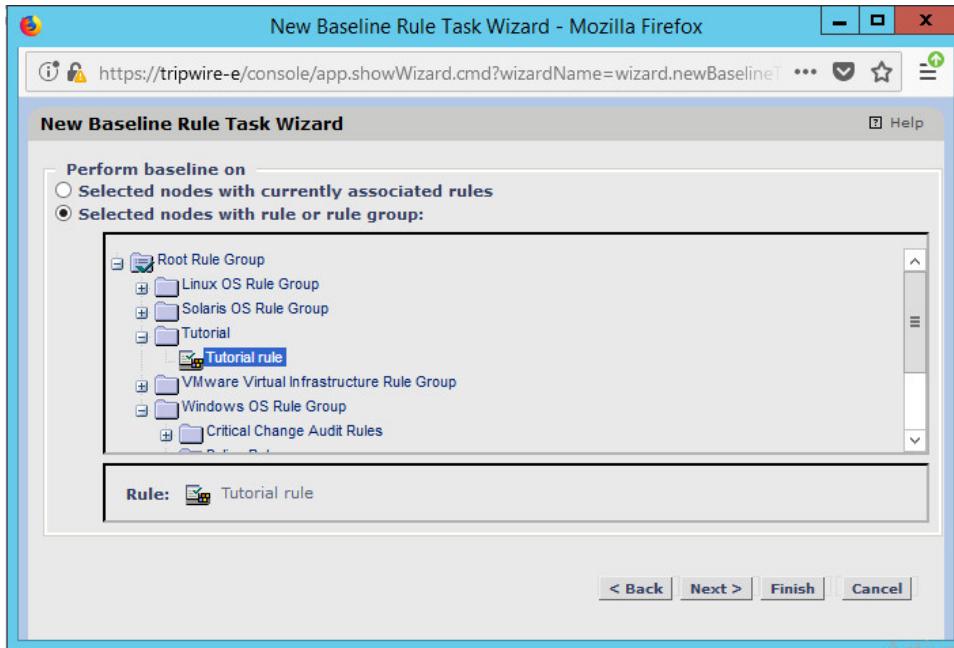
1735
1736
1737
1738

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.



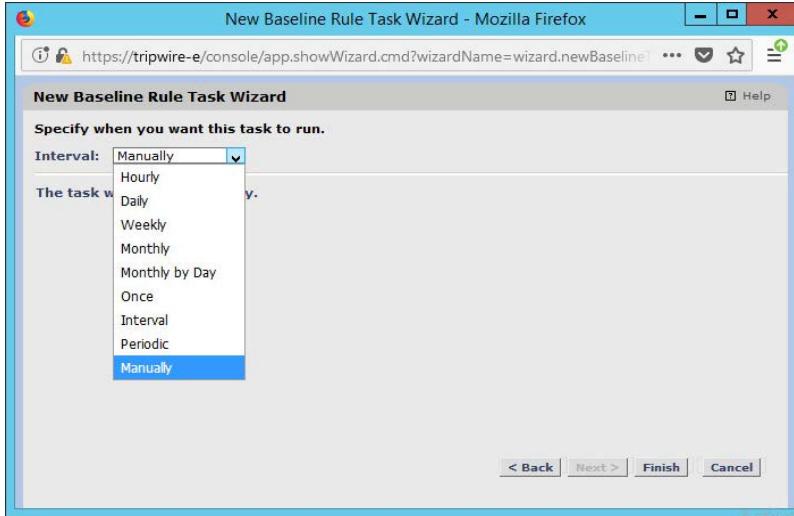
1742

1743

13. Click **Next**.

1744

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

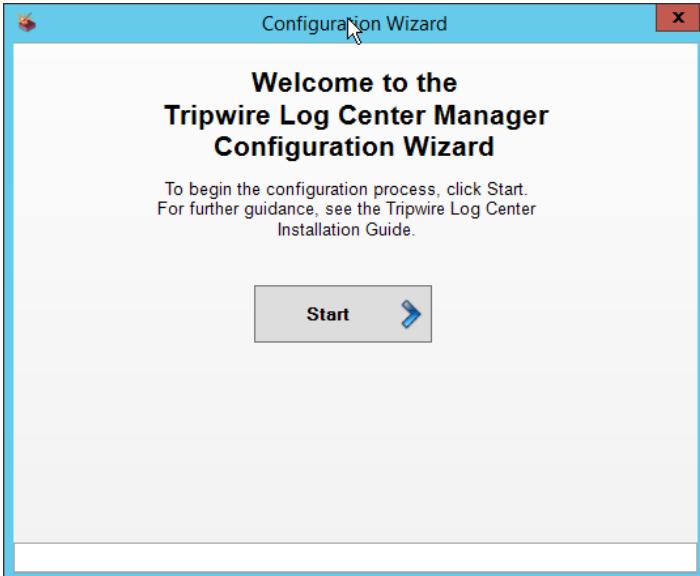
See the *Tripwire Log Center 7.3.1 Installation Guide* that should accompany the installation media for instructions on how to install **Tripwire Log Center**. Use the **Tripwire Log Center Manager** installer.

1751 Notes:

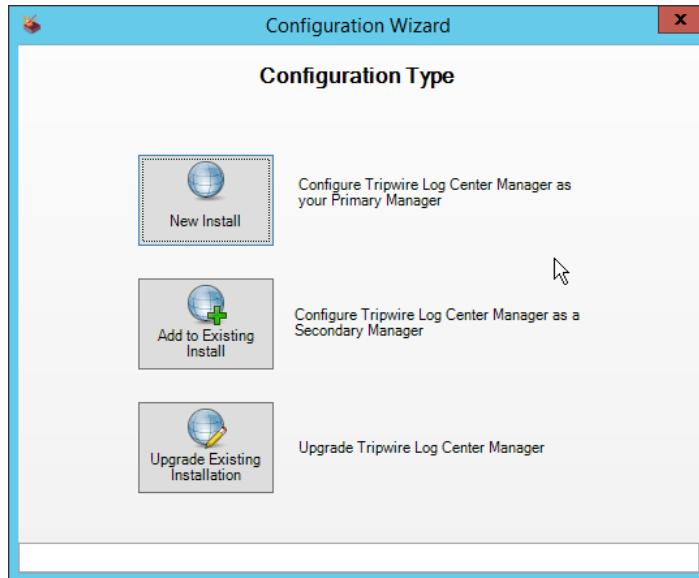
- 1752 a. It is recommended that you install **Tripwire Log Center** on a separate system from **Tripwire Enterprise**.
- 1753 b. You will need to install **JRE8** and the **Crypto** library. Instructions are also in the *Tripwire Log Center 7.3.1 Installation Guide*.
- 1754 c. .NET Framework 3.5 is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

1762 2.10.2 Configure Tripwire Log Center Manager

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

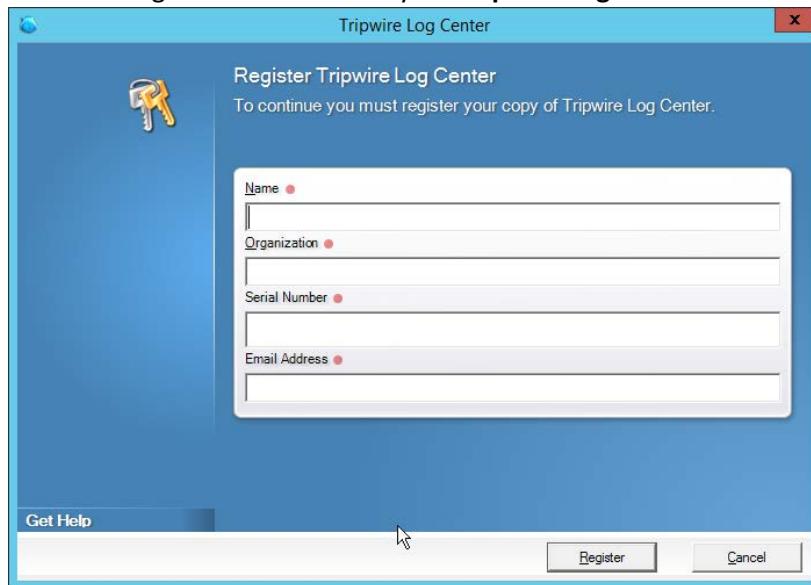


- 1764 2. Click **Start**.
- 1765



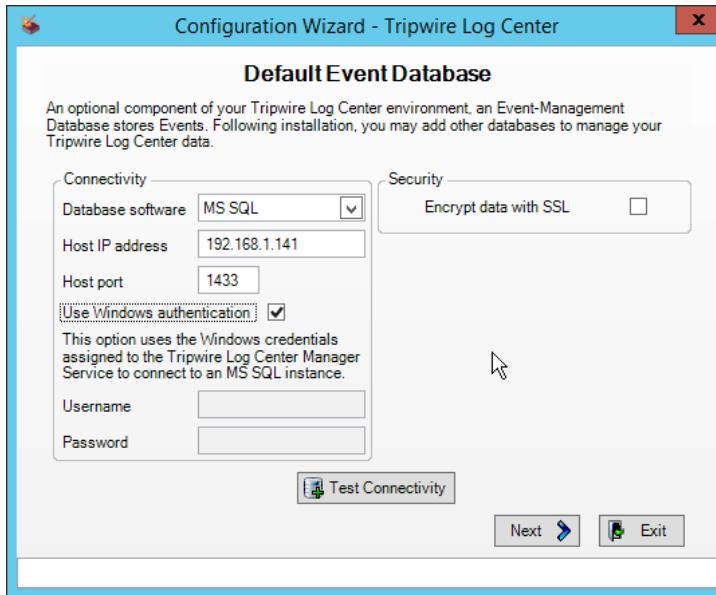
1766
1767
1768

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



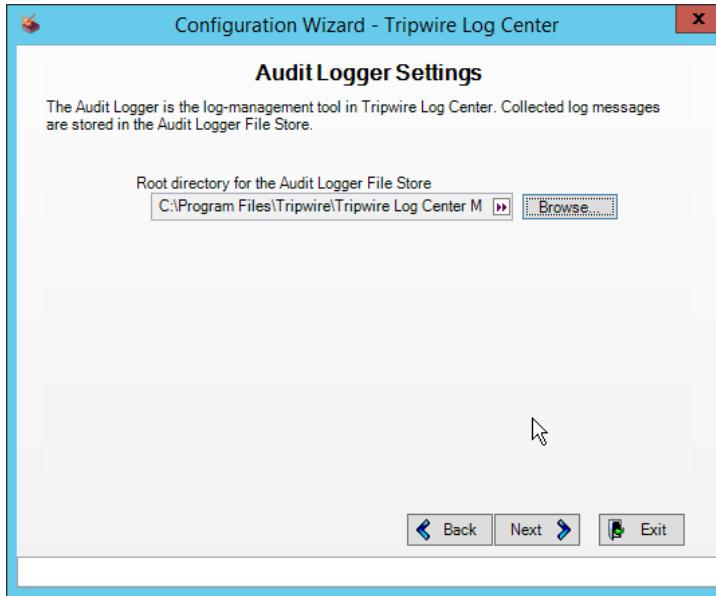
1769
1770
1771

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



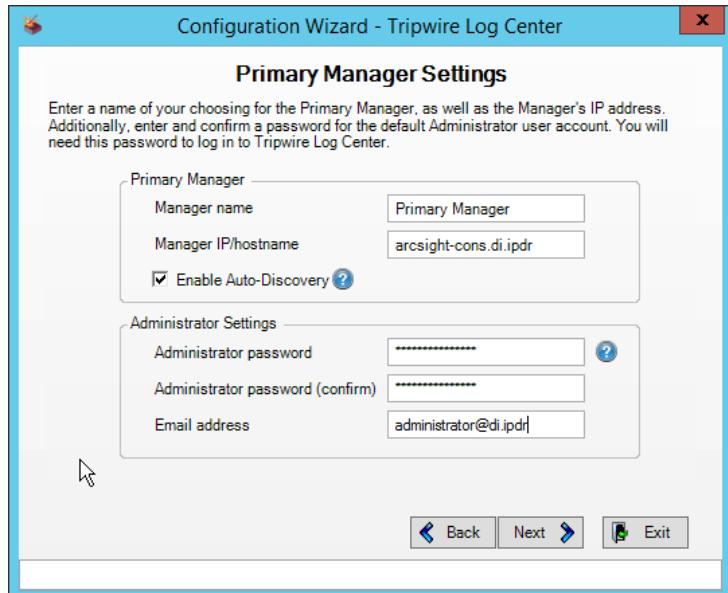
1772
1773
1774
1775

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



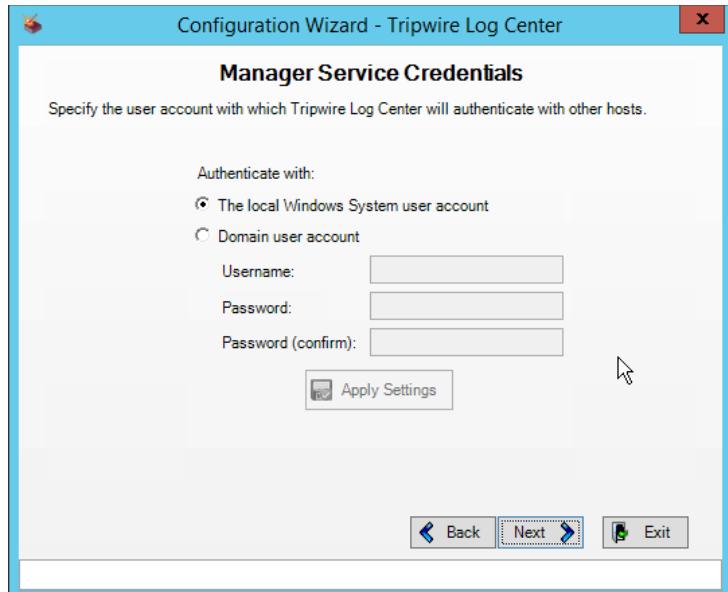
1776
1777
1778
1779

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



1780
1781

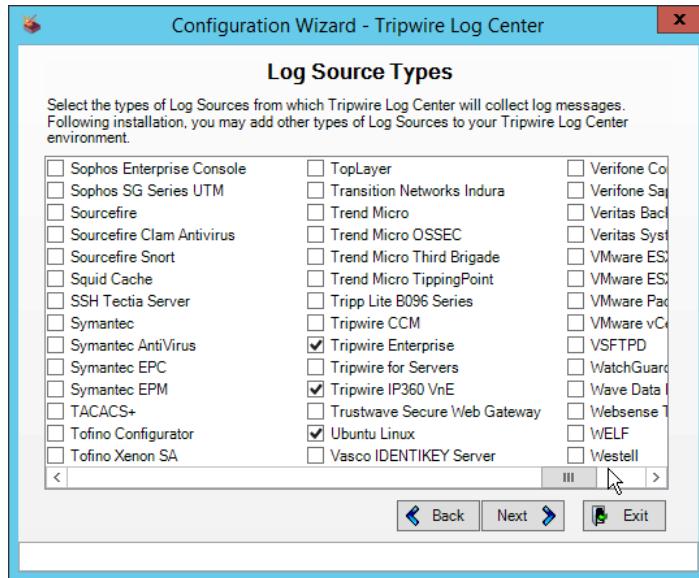
12. Click Next.



1782
1783
1784
1785
1786

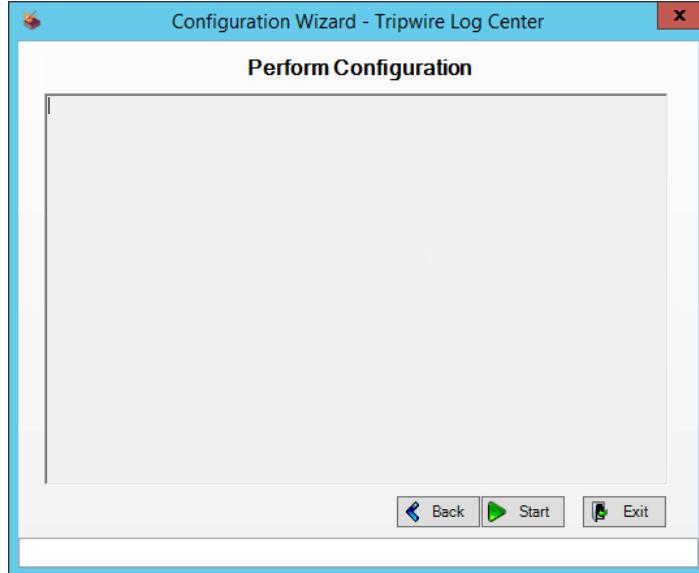
13. Click Next.

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

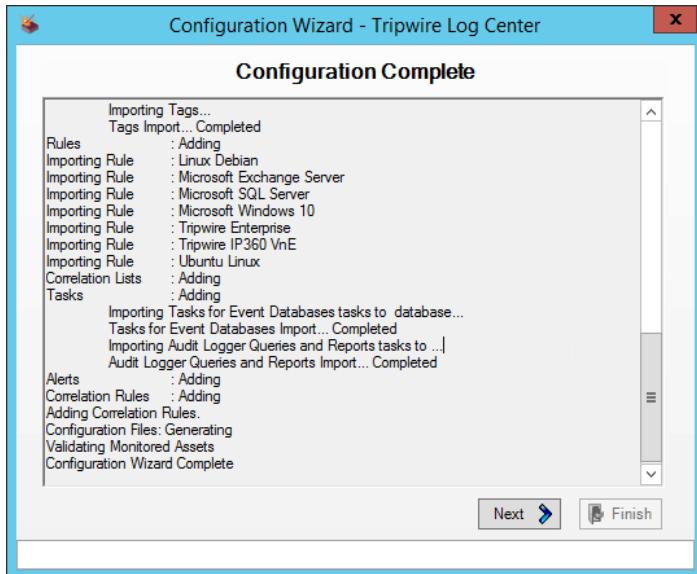
1788

15. Click **Next**.

1789

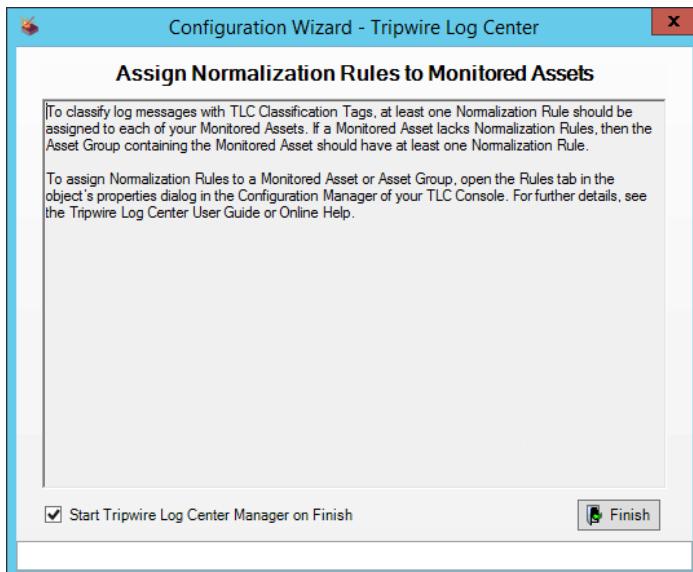
1790

16. Click **Start**.



1791
1792

17. Click **Next**.



1793
1794

18. Click **Finish**.

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 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

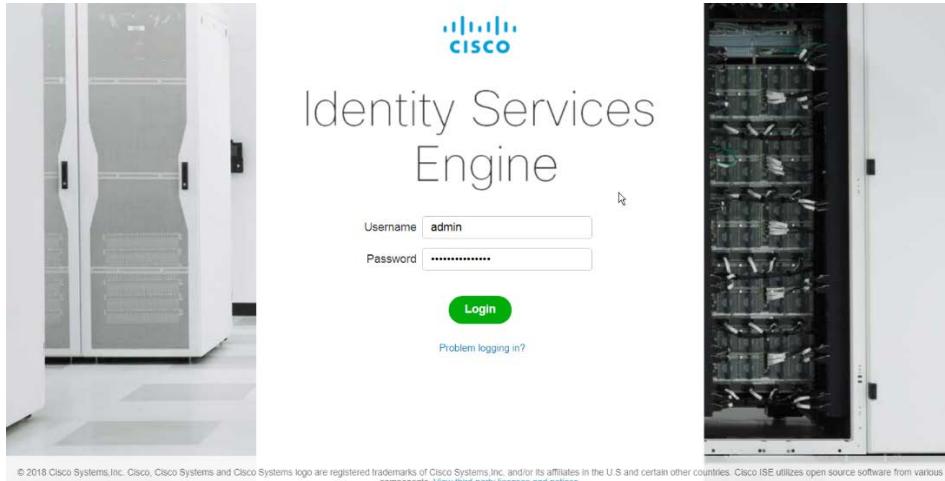
- 1803 1. When prompted to log in for the first time, enter **setup**. (You can use the command **reset-**
1804 **config** to change these values later.)
- 1805 2. Enter the desired **hostname** for the machine.
- 1806 3. Enter the desired **IP address** for the machine. (Ensure that the specified hostname 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.

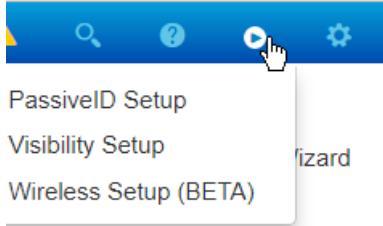
1821 2.11.3 Inventory: Configure Device Detection

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



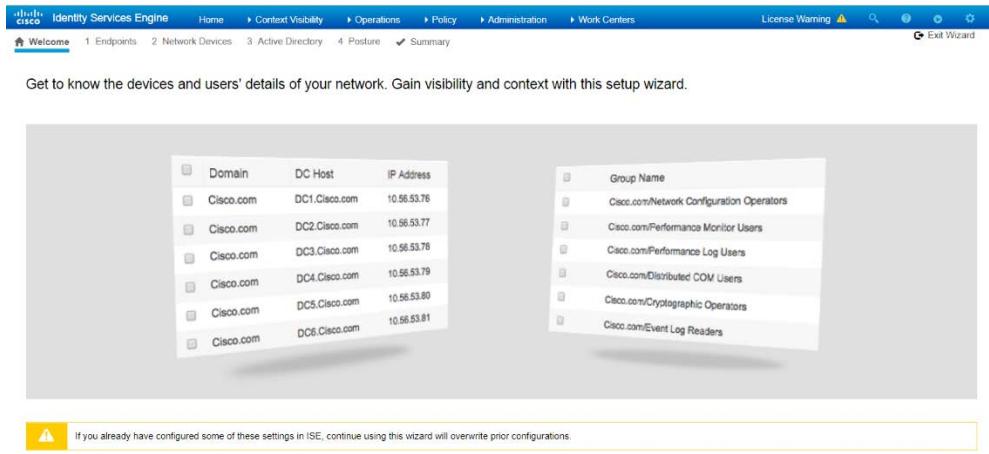
1824
1825

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. A 'License Warning' icon is visible. The main content area is titled 'Endpoints Discovery' and contains a form for specifying an IP address range. The 'IP Address Range' field is set to '192.103.0.0/16'. Below it, there's a note: 'We are going to discover the endpoints using the IP range(s) below.' An 'Active Scanning' checkbox is checked. At the bottom right are 'Skip', 'Back', and a green 'Next' button.

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.

The screenshot shows the 'Add Network Device' dialog box from the Cisco ISE Network Device Discovery interface. The 'Name' field is filled with 'GATEWAYROUTER'. The 'IP Address' field is filled with '192.168.1.1'. The 'SNMP Settings' section shows 'SNMP Version' set to '1' and 'RO Community' set to '*****'. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

1838
1839

12. Click **OK**.

ISE VISIBILITY SETUP WIZARD

1 Endpoints 2 Network Devices 3 Active Directory 4 Posture ✓ Summary

Network Device Discovery

Name	IP Address	Device Type	Location	Description	Action
GATEWAYROUT...	192.168.1.1				Edit

Total Added (1) Failed (0)

Scan Add Remove Add Location Filter

Back Next

- 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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Connect to Active Directory (AD)

Display Name * ADDNS

Domain FQDN * DI.IPDR

ISE Node * cisco-ise di ipdr

Username * Administrator

Password *

Organization Unit e.g. CN=COMPUTERS,DC= CISCO,DC=COM

Test Connection Successfully Connected

Add another Active Directory server Skip Back Next

- 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**.

ISE VISIBILITY SETUP WIZARD

Posture Discovery

Discover posture on endpoints using common administrative account and same IP range(s) from step 1

Username * Administrator

Password *

Enable Endpoint Logging

IP Address Range * 192.168.0.0/16

Include Range

Skip Back Next

1852
185323. Click **Next**.

Active Scanning true

Network Device Discovery

Total Devices Added 1

Active Directory Information

Display Name ADONIS
Domain FQDN DI IPDR
ISE Node cisco-ise.di.ipdr
Username

Test Connection Successfully Connected.

Posture Discovery

IP Scanning Range 192.168.0.0/16

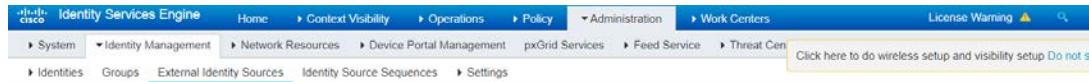
Included true

Back Done

1854
1855 24. Verify the settings, and click **Done**. (This should begin importing endpoints connected to the
1856 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**.

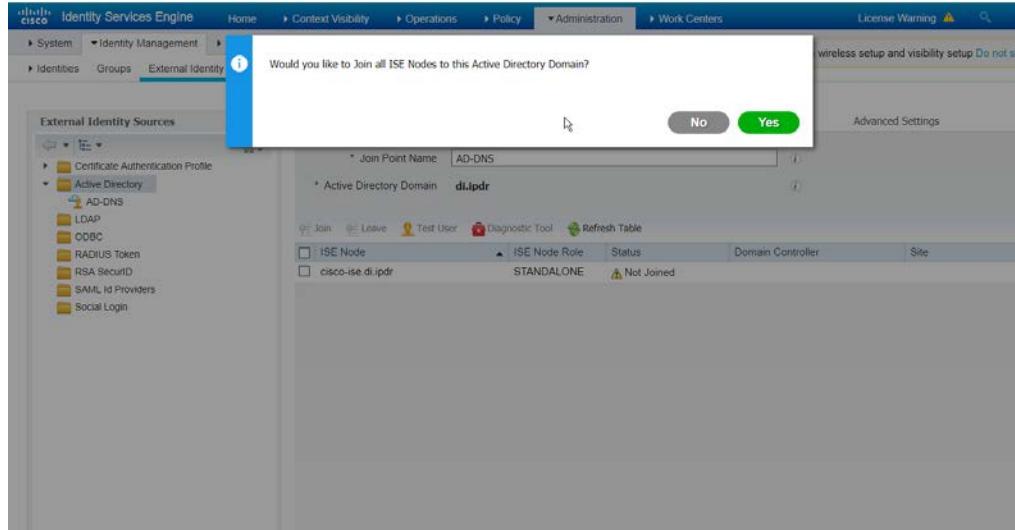
The screenshot shows the 'Connection' configuration dialog for Active Directory. The left sidebar lists the same external identity sources as the previous screenshot. The main dialog has two fields: 'Join Point Name' set to 'AD-DNS' and 'Active Directory Domain' set to 'di.ipdr'. At the bottom are 'Submit' and 'Cancel' buttons.

1864
1865

5. Click **Submit**.

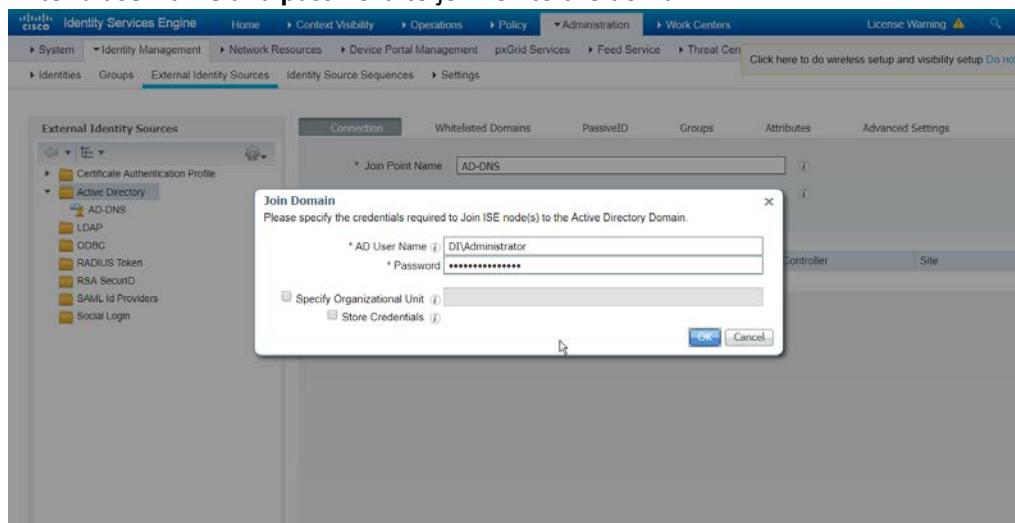
1866
1867
1868

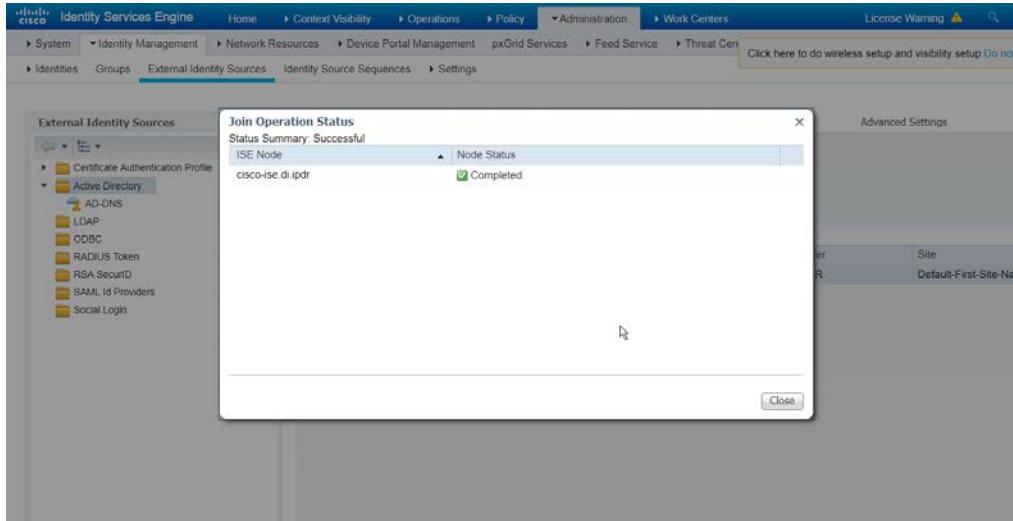
6. Click Yes.
7. Enter a **username** and **password** to join ISE to the domain.



1869
1870

8. Click OK.





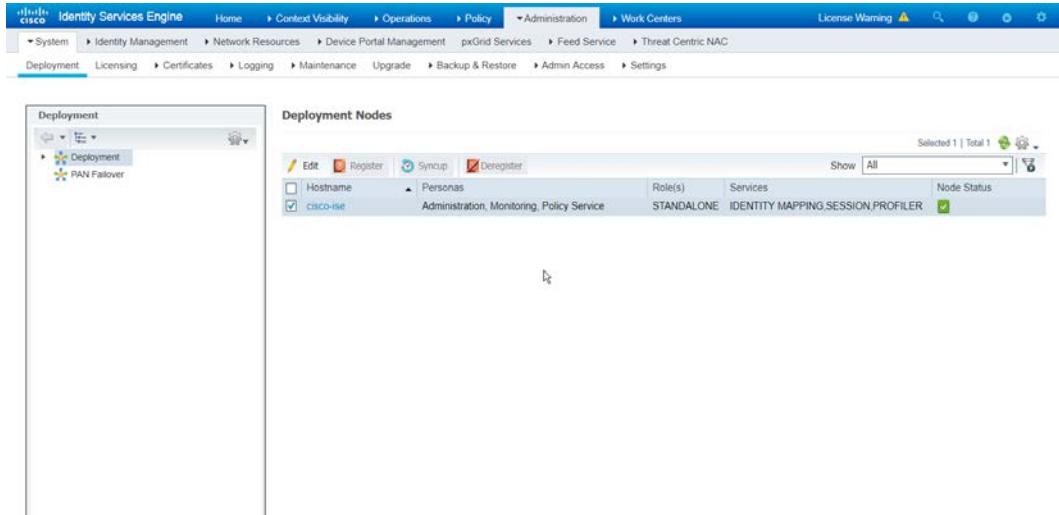
1871

1872 9. Click **Close** when the join is finished.1873

2.11.5 Policy Enforcement: Enable Passive Identity with AD

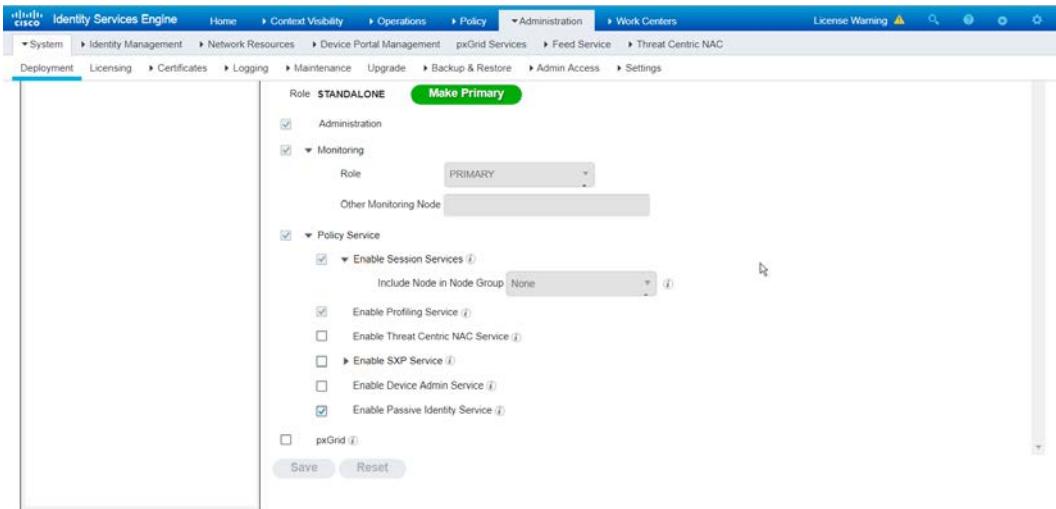
1874 This configuration allows users to use Active Directory usernames/passwords as authentication for the
 1875 portal. The web portal will allow clients to download profiling software to ensure that clients have up to
 1876 date software and can be trusted on the network.

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



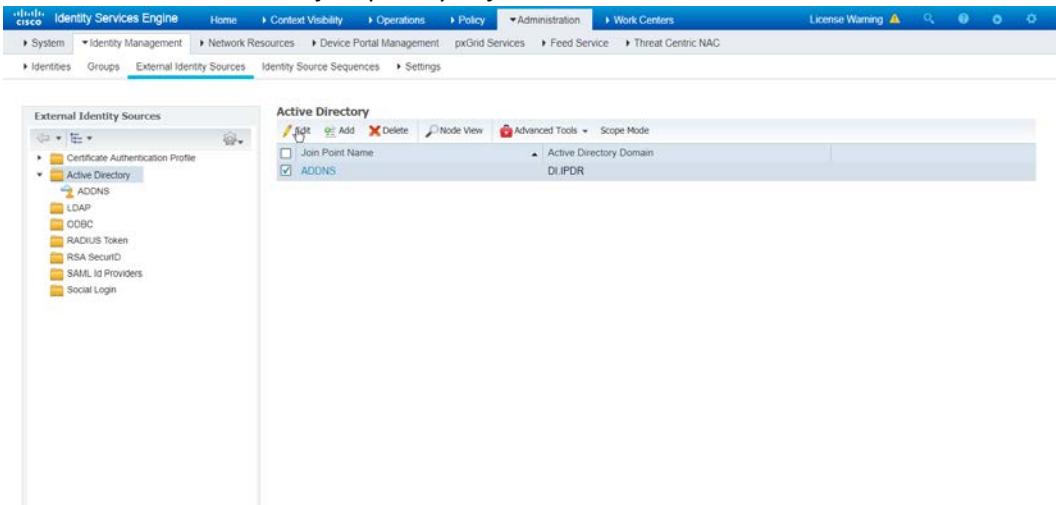
1879

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



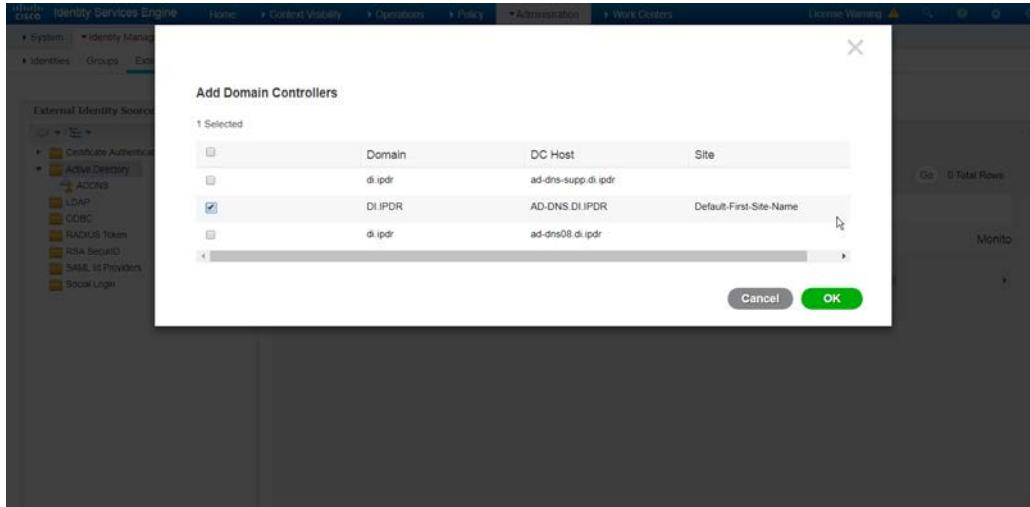
1882

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.



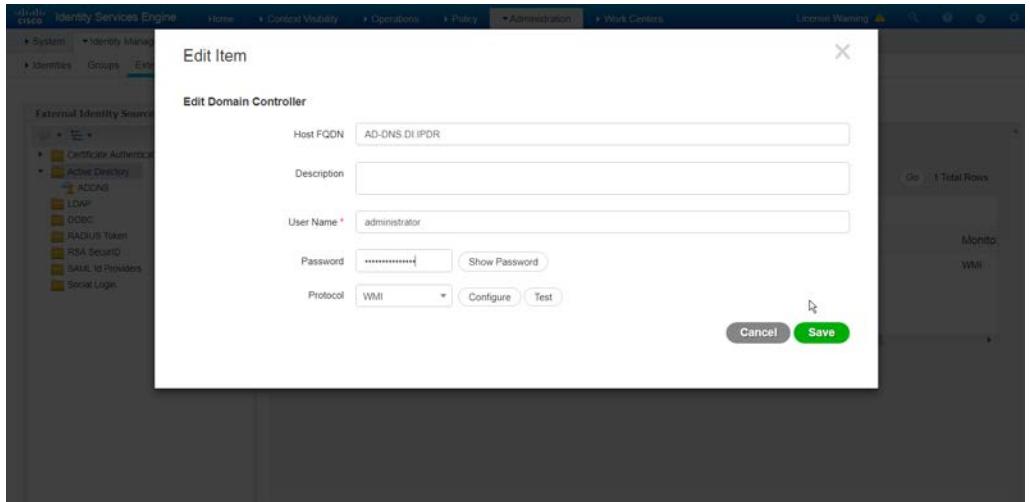
1888

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



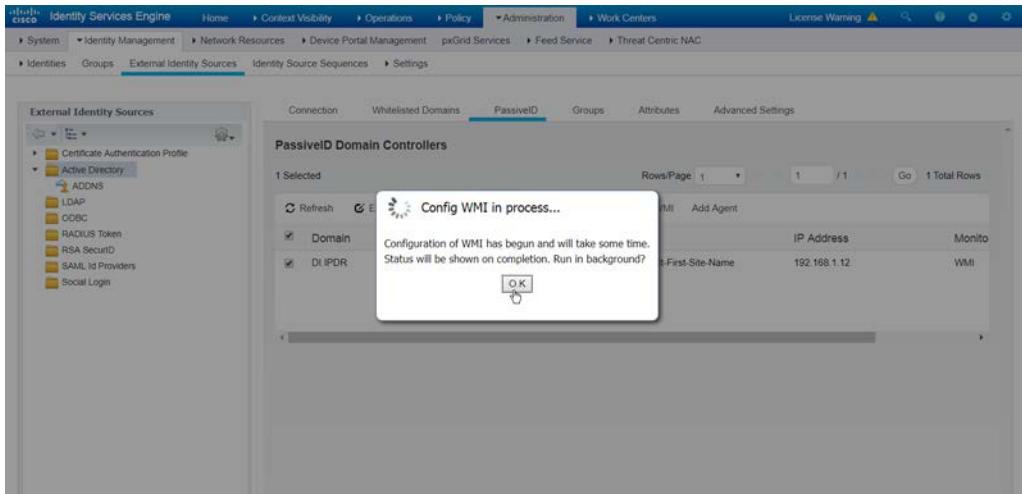
1892
1893
1894
1895
1896
1897

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

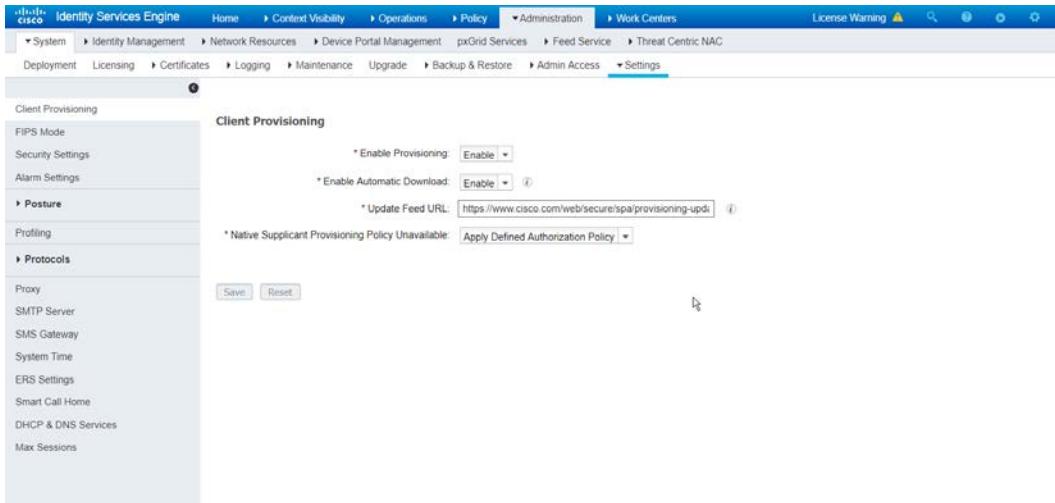
20. Click **OK** when this configuration finishes.

1903

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

1904

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



1905

23. Click **Save**.

1906

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

1907

25. Click the **Groups** tab.

1908

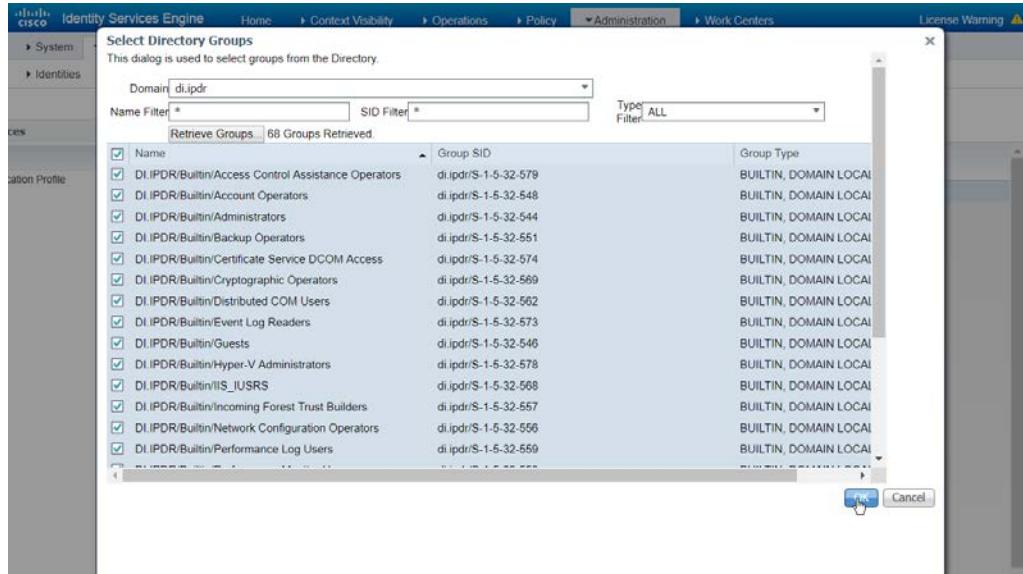
26. Click **Add > Select Groups from Directory**.

1909

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

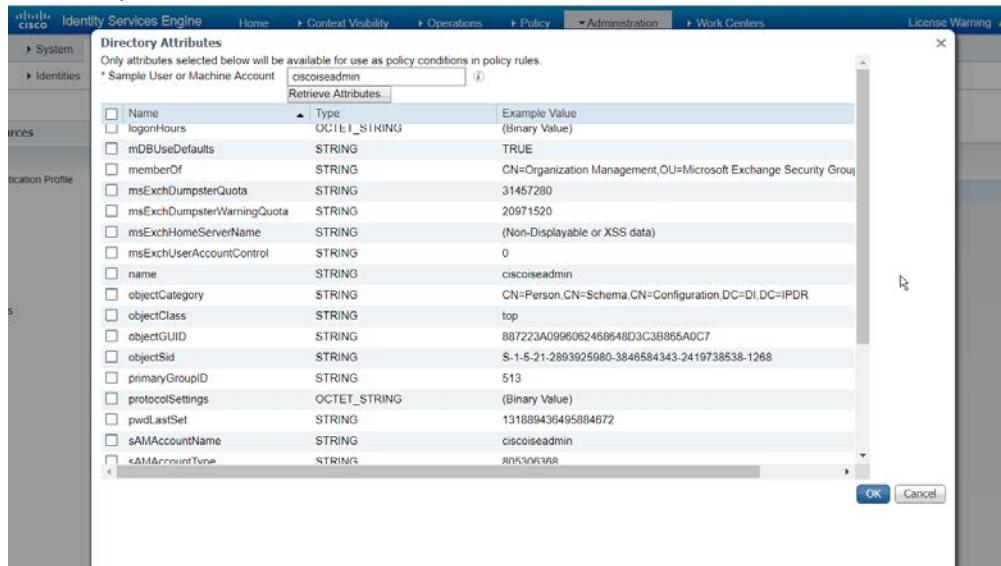
1910

28. Select them all.



1915
1916
1917
1918
1919
1920
1921
1922
1923
1924

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



1925
1926

36. Click **OK**.

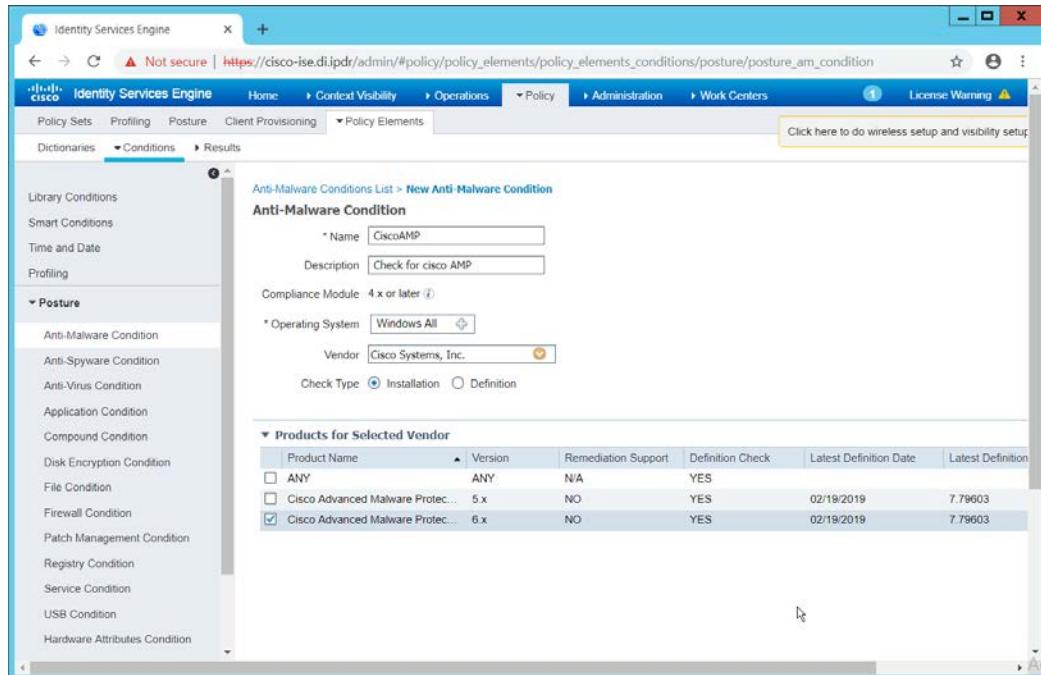
1927 37. Click **Save**.

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 conditions allow you to select or define requirements that endpoints should meet. In typical enterprises these conditions can be used as requirements to gain network access; however, this strongly depends on the capabilities of your network device. Furthermore, the network device
- 1931 3. As an example, we will require that Cisco AMP be installed on all Windows devices. If you are
- 1932 using a different anti-malware software, locate that instead. Click **Anti-Malware Condition**.

Name	Description
ANY_am_win_inst	Any AM installation check on Win...
ANY_am_win_def	Any AM definition check on Wind...
ANY_am_mac_inst	Any AM installation check on Mac
ANY_am_mac_def	Any AM definition check on Mac
Cisco-AMP	Requires Cisco AMP

- 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 Protection**, with the version number you have installed.



1944
1945

10. Click **Submit**.

2.11.7 Policy Enforcement: Developing Policy Results

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

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The URL is https://cisco-ise.d1.ipdr/admin/#policy/policy_elements/policy_elements_permissions/posture_permissions/posture_requirements_policy. The page title is "Identity Services Engine". The navigation bar includes "Home", "Operations", "Administration", and "Work Centers". On the left, a sidebar lists categories: Authentication, Authorization, Profiling, Posture, and Remediation Actions. Under "Posture", there is a "Requirements" section. The main content area displays a table of policy elements. A new row is being edited, with the "Condition" field set to "AMP_CHECK" and the "Action" field set to "Message". The "Operating System" is set to "Windows All", "Compliance Module" is set to "4.x or later", "Posture Type" is set to "Temporal Agent", and the "Requirement" is set to "Cisco AMP". The table also lists other policy elements for various operating systems and compliance modules.

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**.

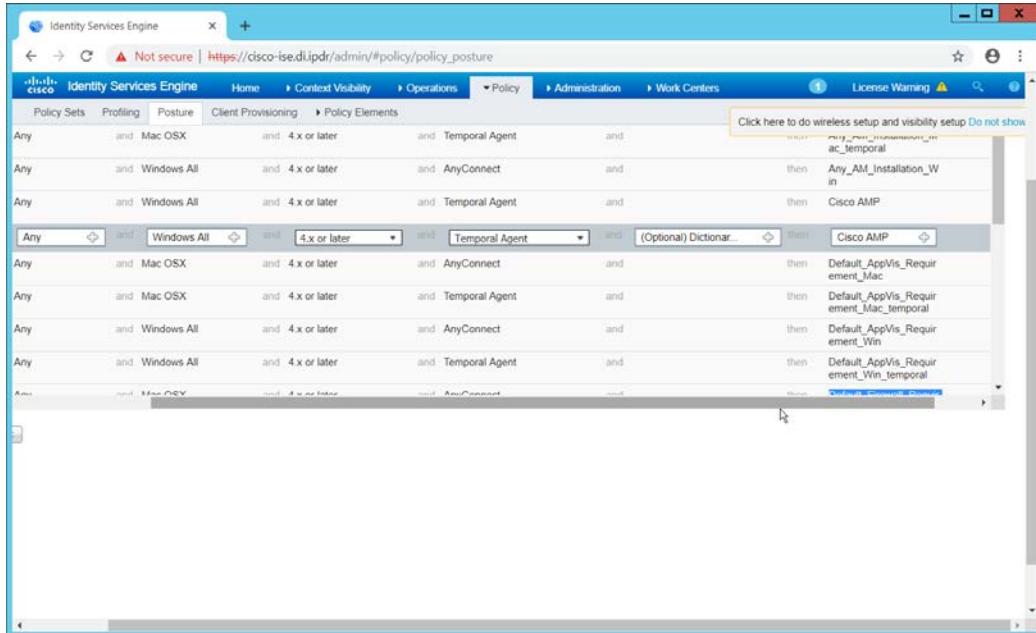
1964 3. Enter a **name**.

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

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.

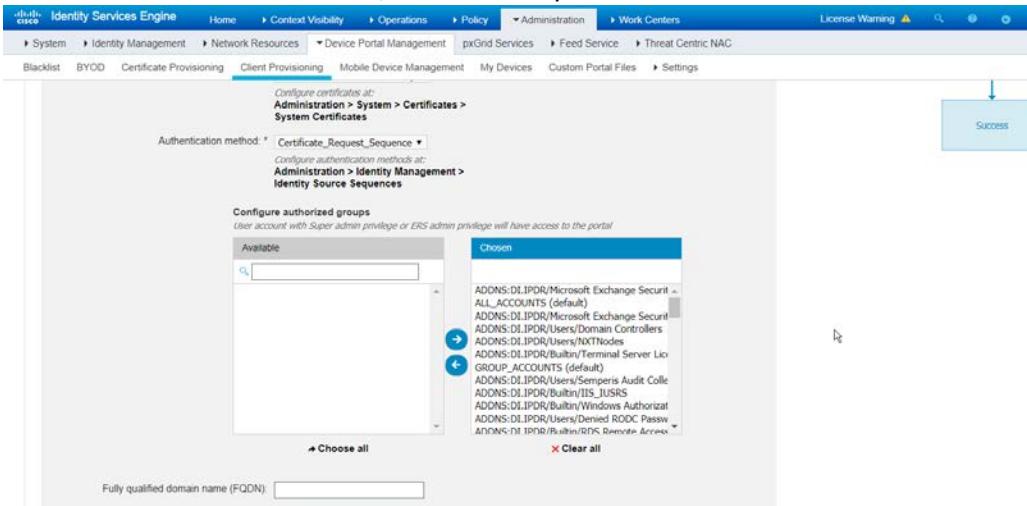
1973 2.11.9 Policy Enforcement: Configuring a Web Portal

- 1974 1. Navigate to **Administration > Device Portal Management > Client Provisioning**.
- 1975 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**.

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.

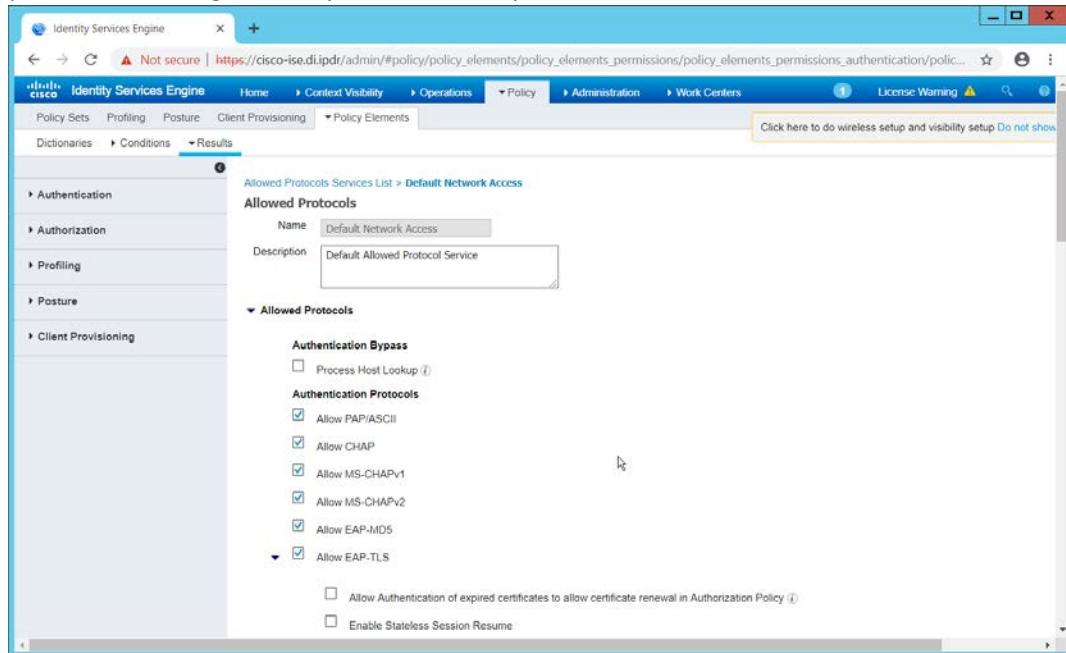
2009 3. The two steps above detail the **authentication** phase. Once authenticated, the network device
 2010 must redirect the user to the client provisioning portal (or to a guest portal), depending on the
 2011 setup. The URL for this can be acquired from the active **Authorization Profile** in ISE.

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.

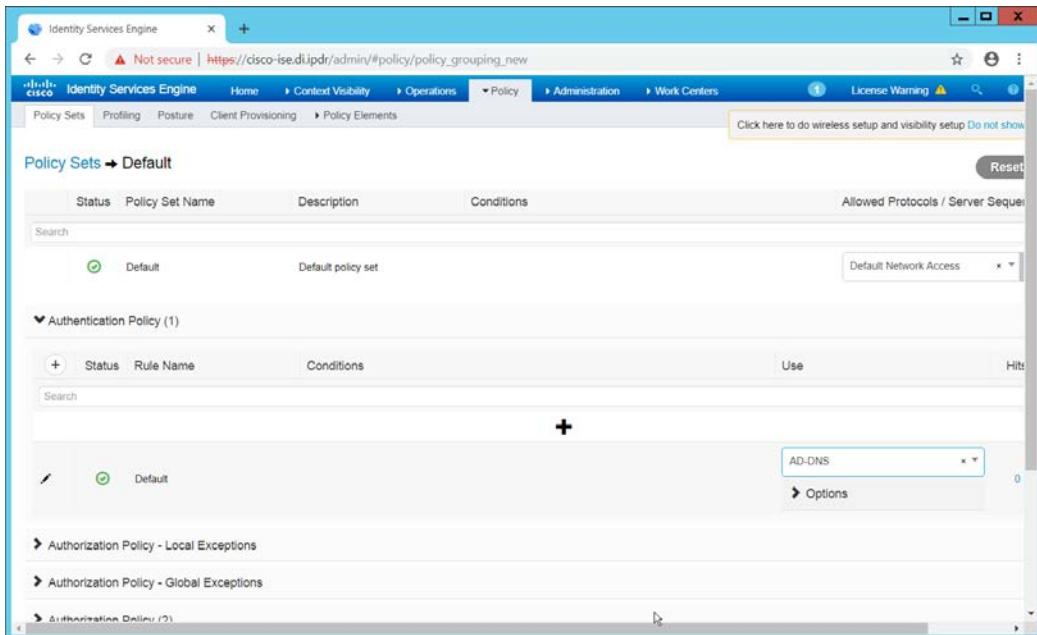
2014 5. The executable will *first* check for the existence of a RADIUS session in Cisco ISE for the user
 2015 who downloaded the executable. It will primarily check the MAC address that visited the ISE
 2016 web portal against the MAC addresses of existing sessions. *If and only if a session exists*, 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 created/edited.
- 2029 8. Expand the **Authentication Policy** section, and select the ID stores from which to authenticate users. For example, if you set up an Active Directory integration, it may be desirable to authenticate users from there.
- 2030
- 2031
- 2032



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

2.11.12 Configuring an Authorization Policy

- 2035
- 2036 1. The Authorization Profile is likely dependent on your network device, but it is possible that the **Cisco_Temporal_Onboard** profile will work even for non-Cisco devices. You can edit the authorization policy by navigating to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
- 2037
- 2038
- 2039
- 2040 2. The temporal onboard profile will attempt to redirect the user to a client provisioning portal—this redirection will most likely only happen automatically on compatible Cisco network devices.
- 2041
- 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.

Status	Rule Name	Conditions	Results
<input checked="" type="radio"/>	Basic_Authenticated_Access	machineuserauth Cisco_Temporal_Onboard	Profiles: Guests, Cisco_Temporal_Onboard Security Groups: Unknown
<input checked="" type="radio"/>	Default		

- 2052 7. Click **Save**.

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:

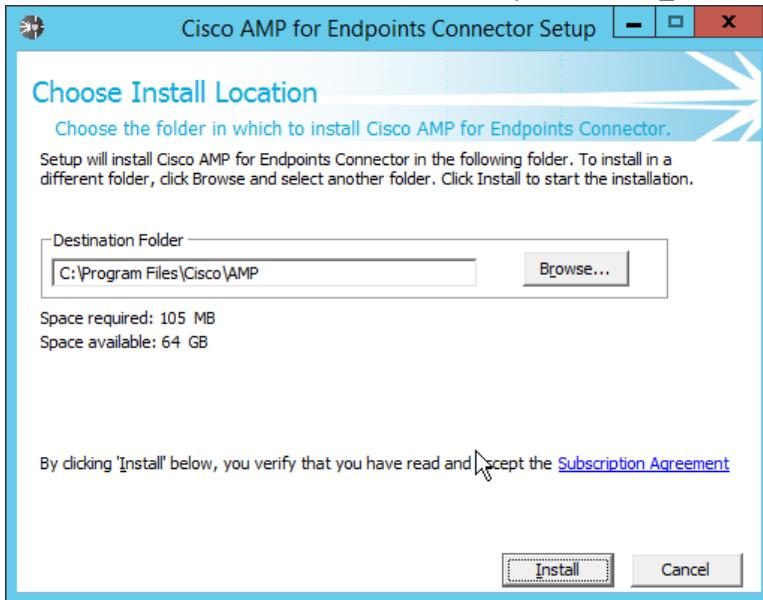
2059 <https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/213681-best-practices-for-amp-for-endpoint-excl.html>.

2.12.1 Dashboard Configuration

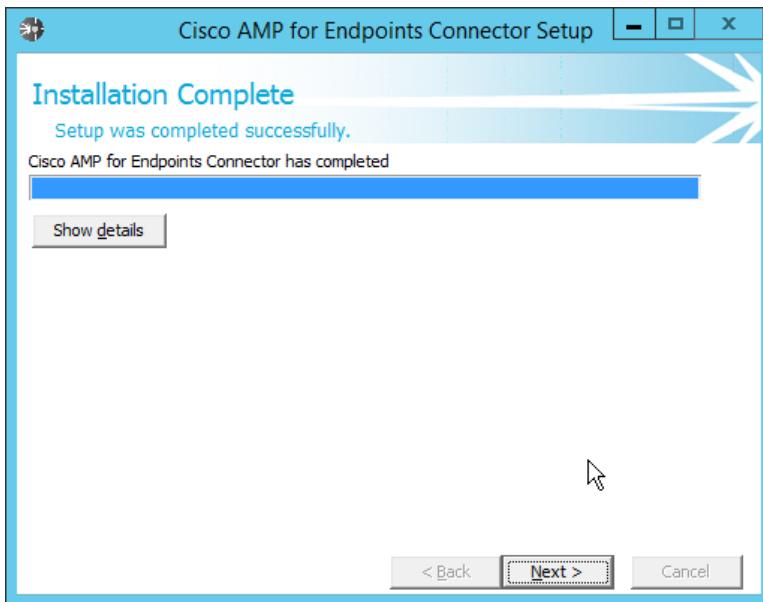
- From the Cisco AMP dashboard, located at <https://console.amp.cisco.com/dashboard>, click **Set Up Windows Connector**.
- The configuration of this will be different for each enterprise, so consult your Cisco representative for the proper way to set this up. For the purposes of this build, we accepted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

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

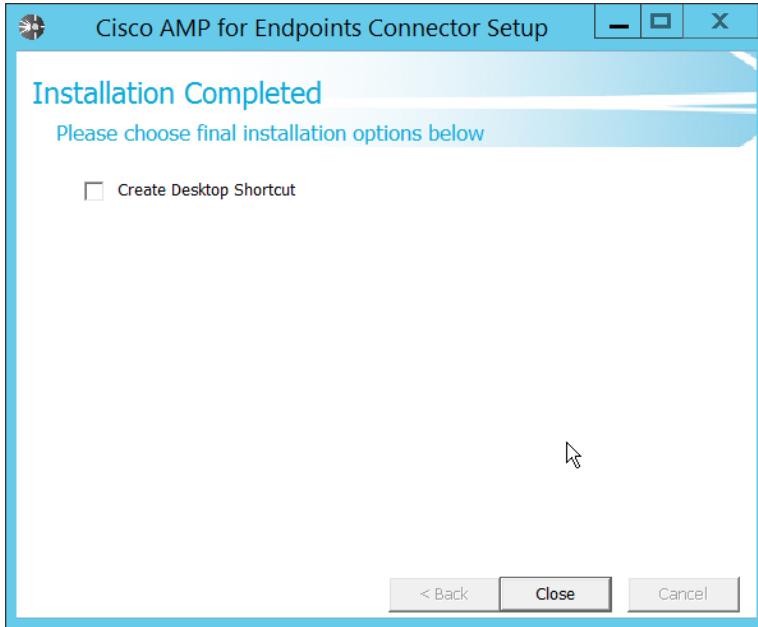
- 2068 1. On the Cisco AMP dashboard, navigate to **Management > Download Connector**.
2069 2. Select the AMP group in which to put the machine. For example, when installing on an Active
2070 Directory machine, we chose **Domain Controller**.
2071 3. Find the correct OS version of the installer, and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



- 2073 5. Click **Install**.



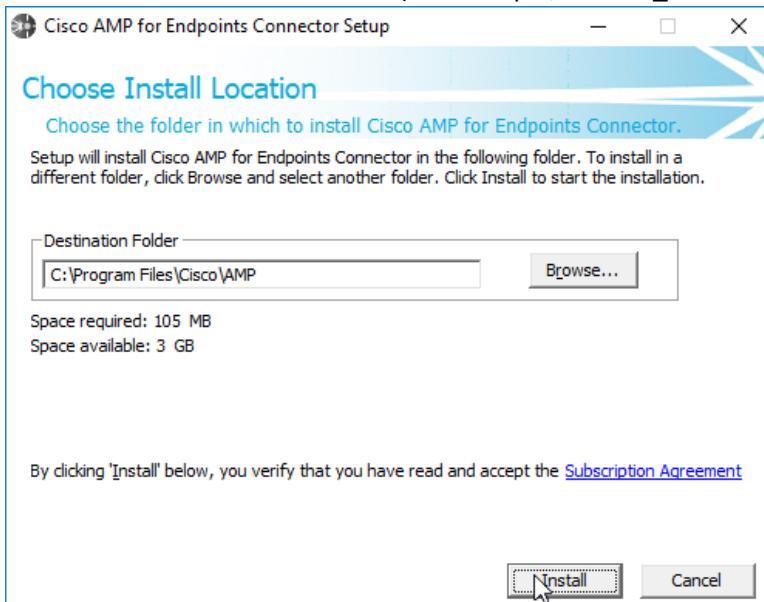
- 2075 6. Click **Next**.



- 2077
2078 7. Click Close.

2.12.3 Installing the Connector on a Windows 10 Machine

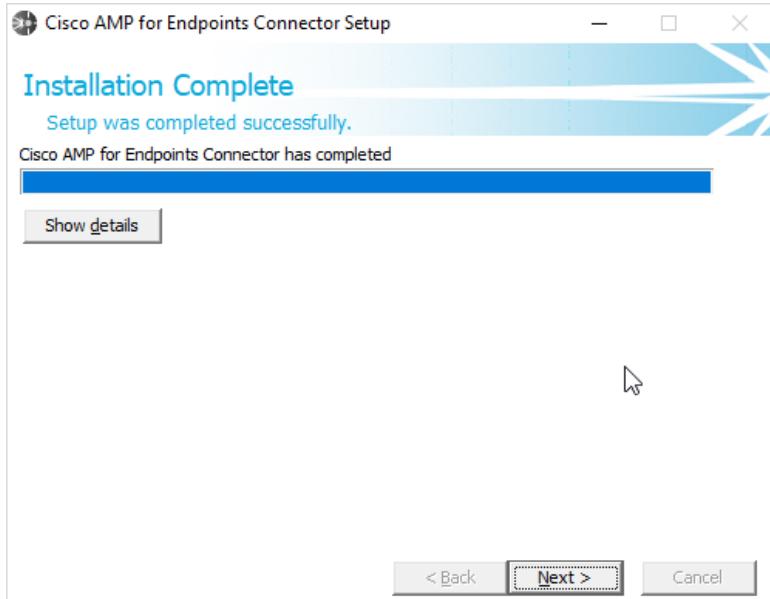
- 2080 1. On the Cisco AMP dashboard, navigate to **Management > Download Connector**.
 2081 2. Select the AMP group in which to put the machine. For this installation we chose **Protect**.
 2082 3. Find the correct OS version of the installer, and click **Download**.
 2083 4. Run the downloaded executable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



- 2084

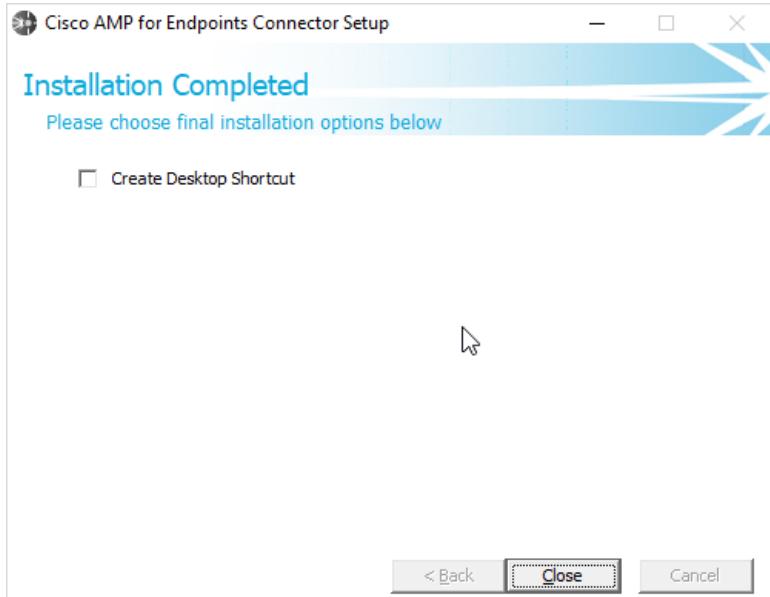
2085

5. Click **Install**.



2086
2087

6. Click **Next**.



2088
2089

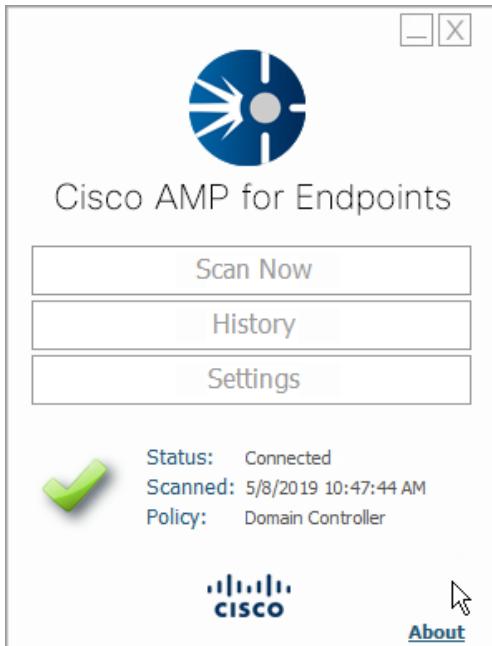
7. Click **Close**.

2090

2.12.4 Scanning using AMP

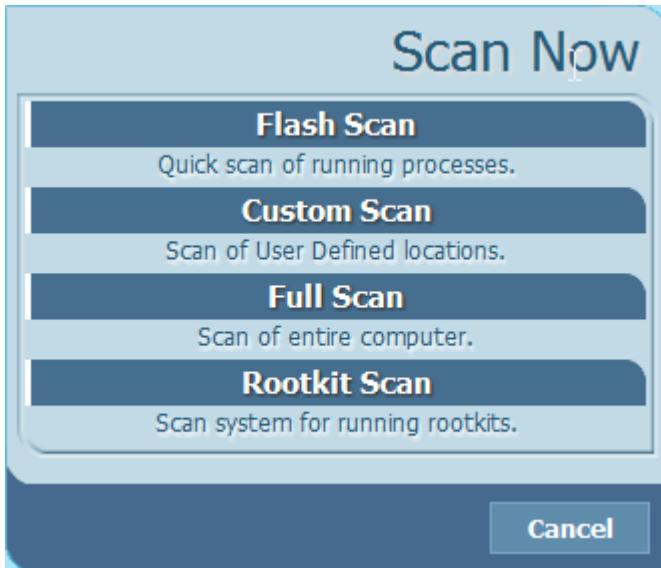
2091

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.

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...](#) [Edit](#) [Delete](#)

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 Network Disabled Malicious Activity Prote... Disabled System Process Protection Protect	Altiris by Symantec AVAST Avira Diebold Warsaw	Not Configured	Domain Controller
Outbreak Control			
Custom Detections - Simple File Blacklist	Custom Detections - Advanced Not Configured	Application Control Execution Blacklist File Whitelist Blocked Allowed	Network
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 <input type="button" value="25"/> / page <input type="button" value="←"/> 1 <input type="button" value="of 1"/> <input type="button" value="→"/>			

- 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 • **Audit** is a detection/logging approach that does not take any action other than logging
 the activity.
 - 2106 • **Quarantine** involves the move of the offending file to its own folder, where it is
 monitored and deleted after a certain amount of time. Quarantining can also be applied
 to processes, in which the process is monitored and prevented from affecting system
 operations.
 - 2107 • **Block** involves the deletion of the file or the stopping of the process or network traffic.
- 2108 5. “Detection Engines” refer to the actual detection of the suspicious activity.
- 2109 • **TETRA** is intended to be an anti-malware engine and recommends that it not be used
 when other antimalware software is in use.
 - 2110 • **Exploit Prevention** refers to an engine that defends endpoints against memory injection
 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

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

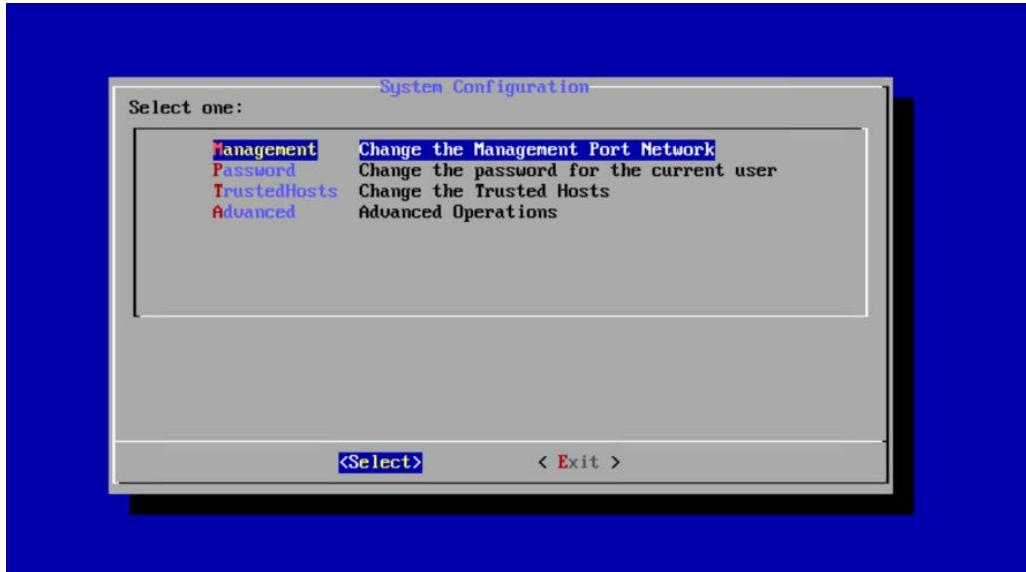
6. Click **Save**.

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.

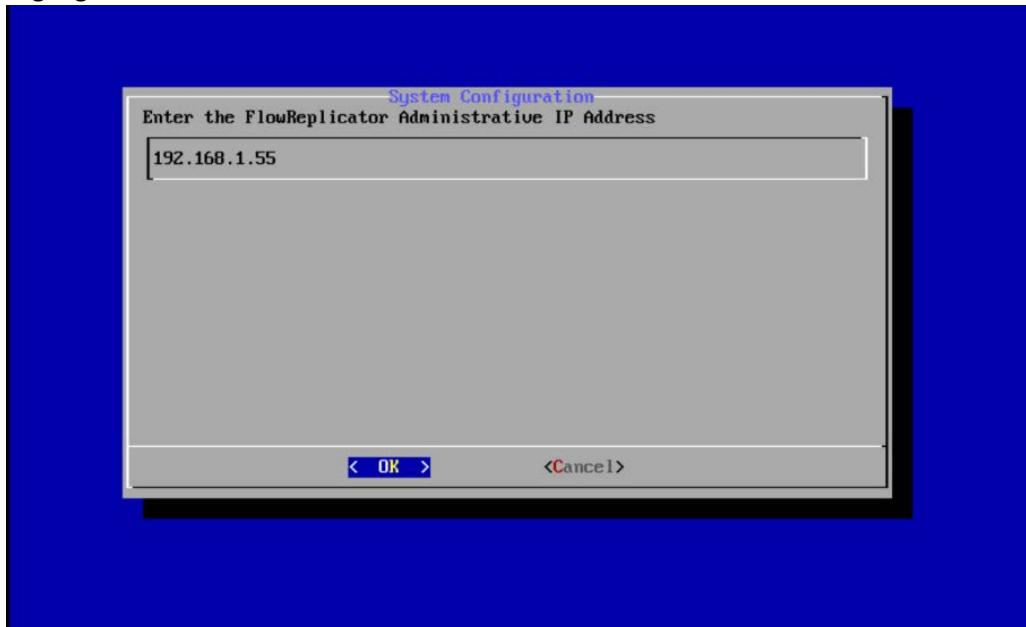
2123 **2.13.1 Configure Stealthwatch Flow Collector, Stealthwatch Management 2124 Console, Stealthwatch UDP Director and Stealthwatch Flow Sensor**

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



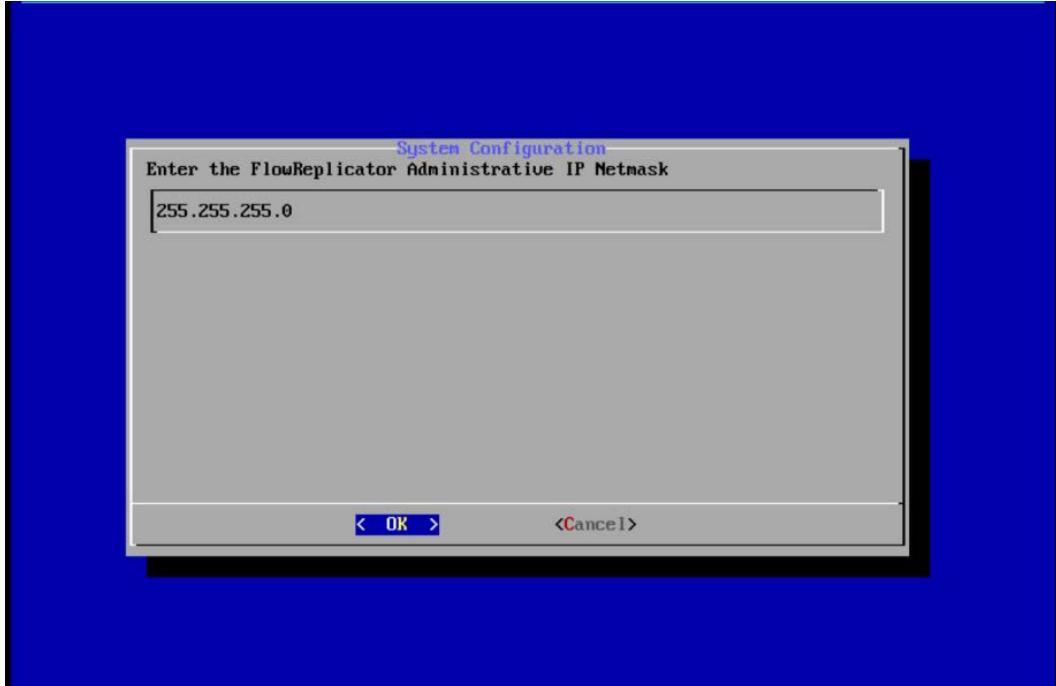
2127
2128
2129
2130

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**.

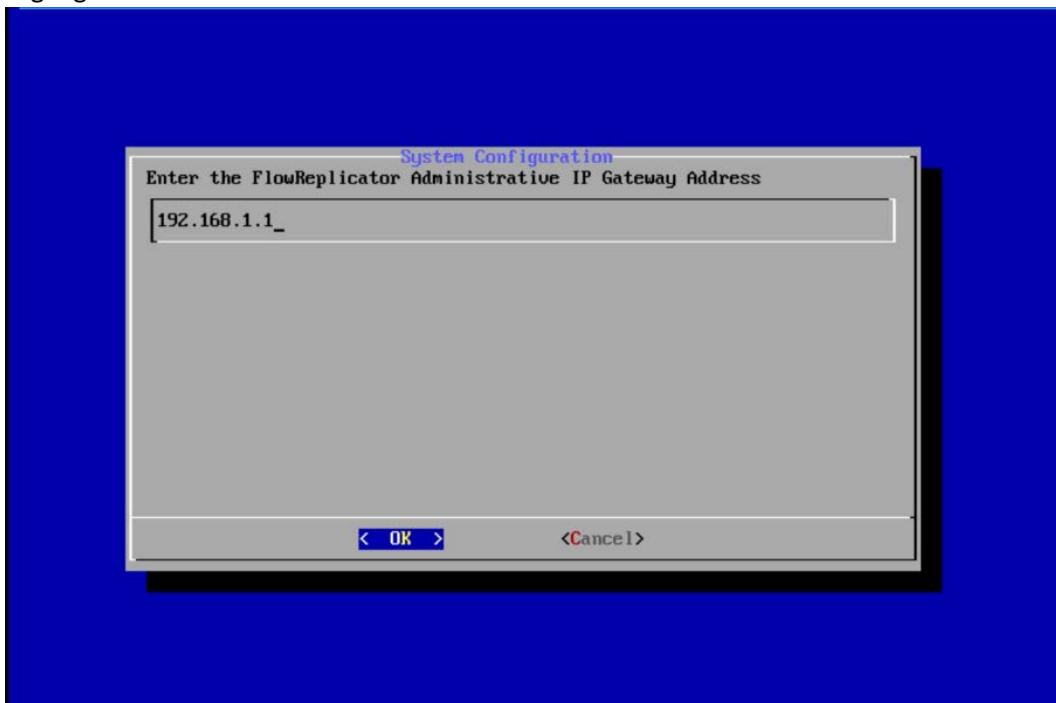


2135

2136 9. Press **Enter**.

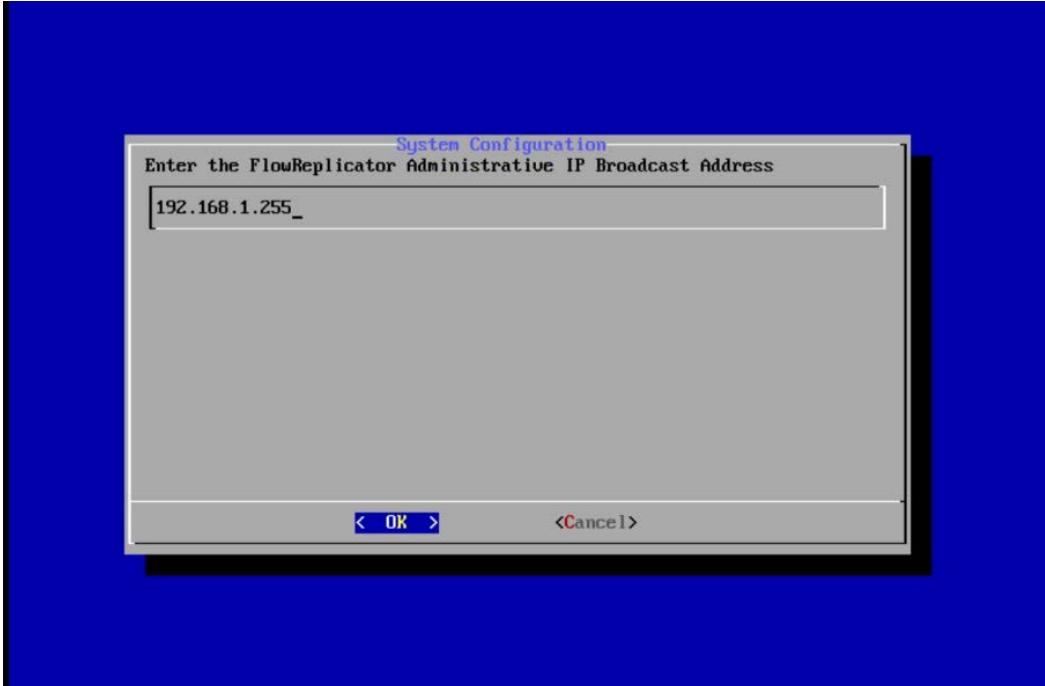
2137 10. Enter the network **gateway**.

2138 11. Highlight **OK**.

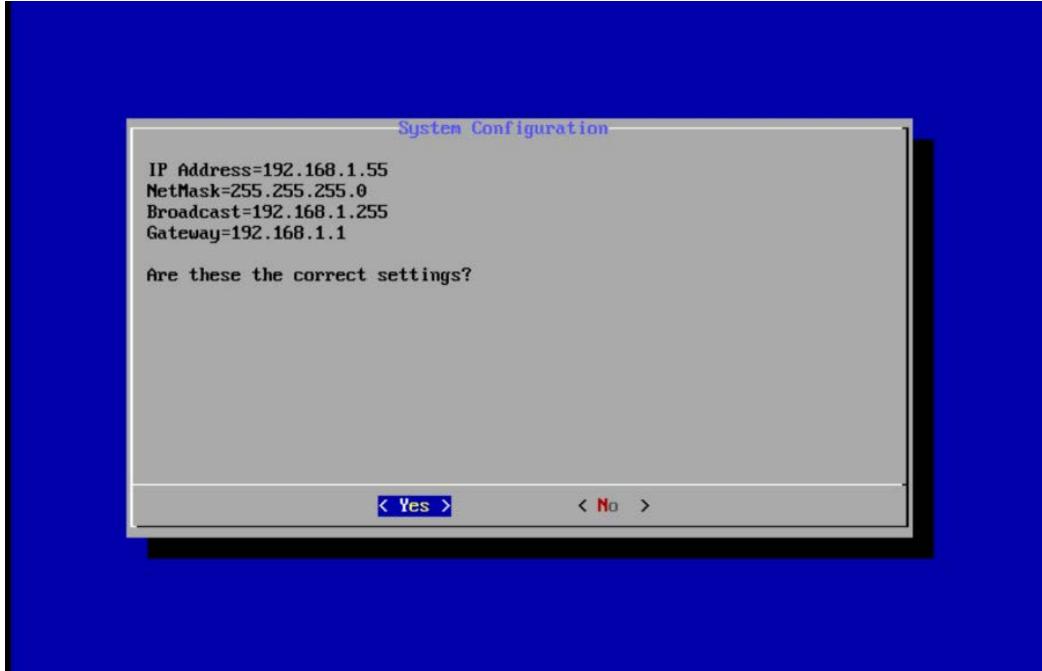


2139

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



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



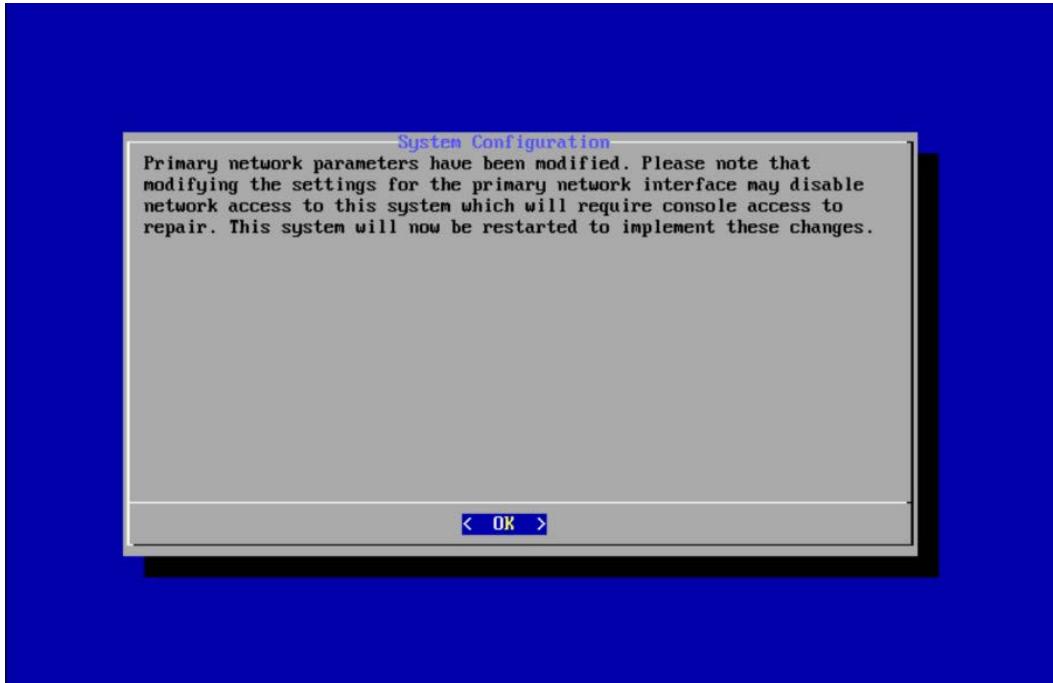
2146

2147

17. Press **Enter**.

2148

18. Highlight **OK**.



2149

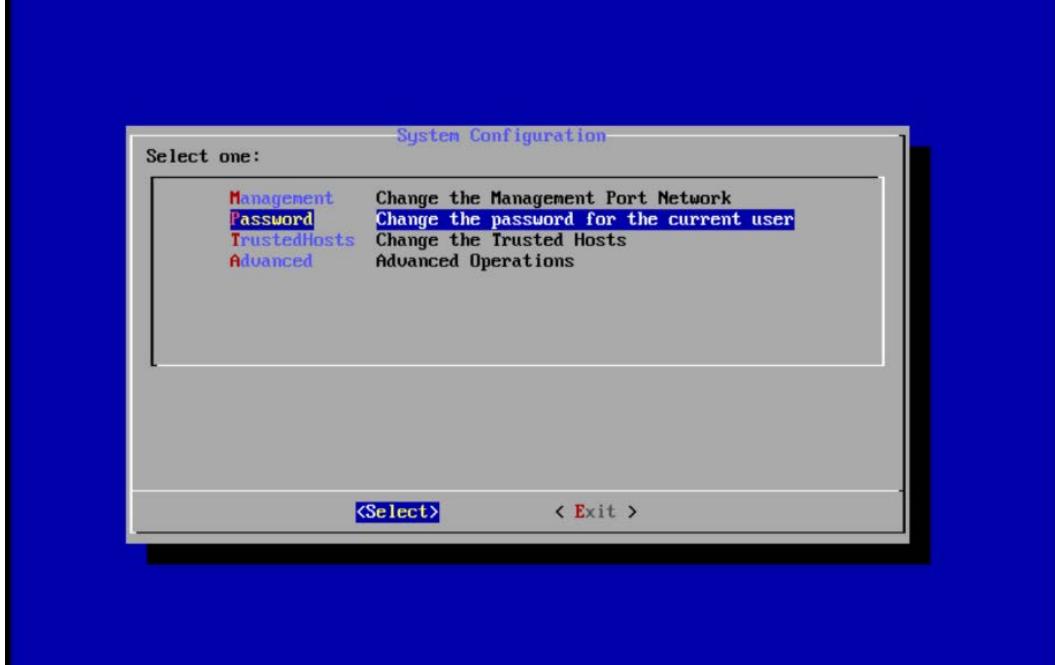
2150

19. Press **Enter**.

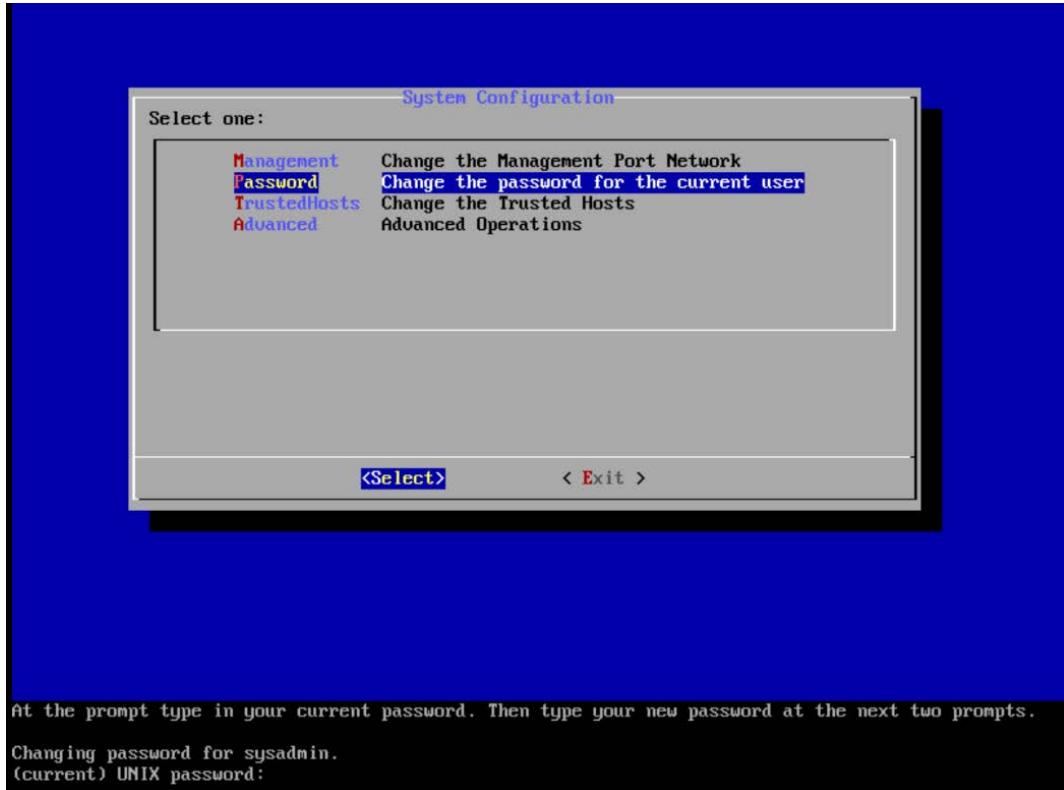
2151 **20.** Repeat steps 1-19 for each of the **Stealthwatch Management Console**, **Stealthwatch UDP**
2152 **Director**, **Stealthwatch Flow Sensor**, and **Stealthwatch Flow Collector**.

2153 2.13.2 Change Default Stealthwatch Console Passwords

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

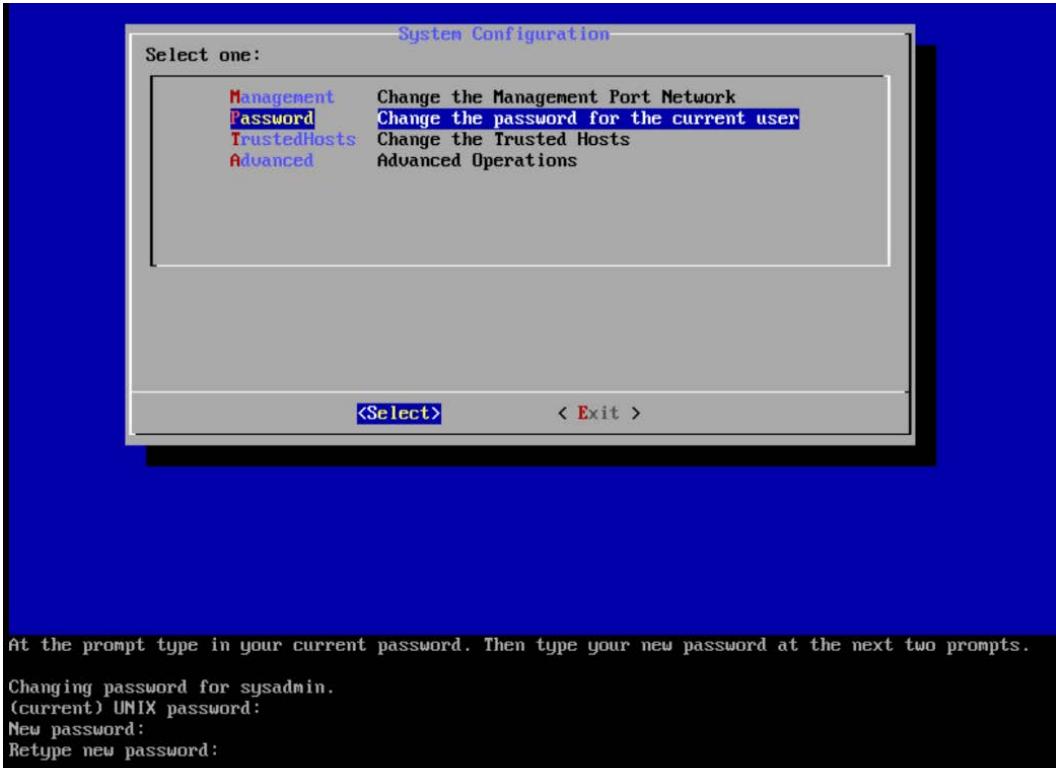


2155
2156 2. Press **Enter**.
2157 3. Enter the original password.

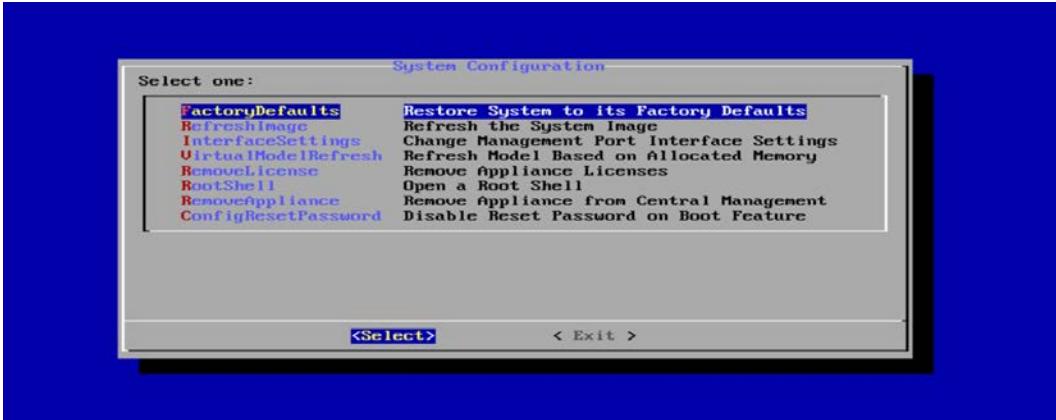


2158
2159
2160

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



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



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

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:  
smc-01:~# passwd root  
New password:  
Retype new password:  
passwd: password updated successfully  
smc-01:~#
```

2172
2173

2174

2175 14. Press **Enter**.

2176 15. Repeat steps 1-14 for each console.

2177

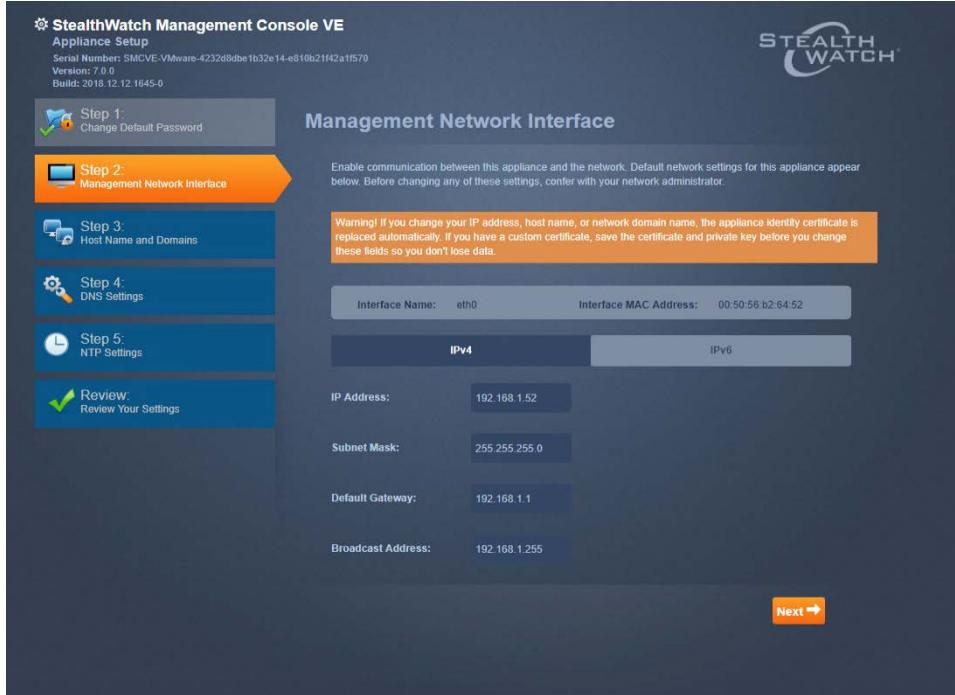
2.13.3 Configure the Stealthwatch Management Console Web Interface

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



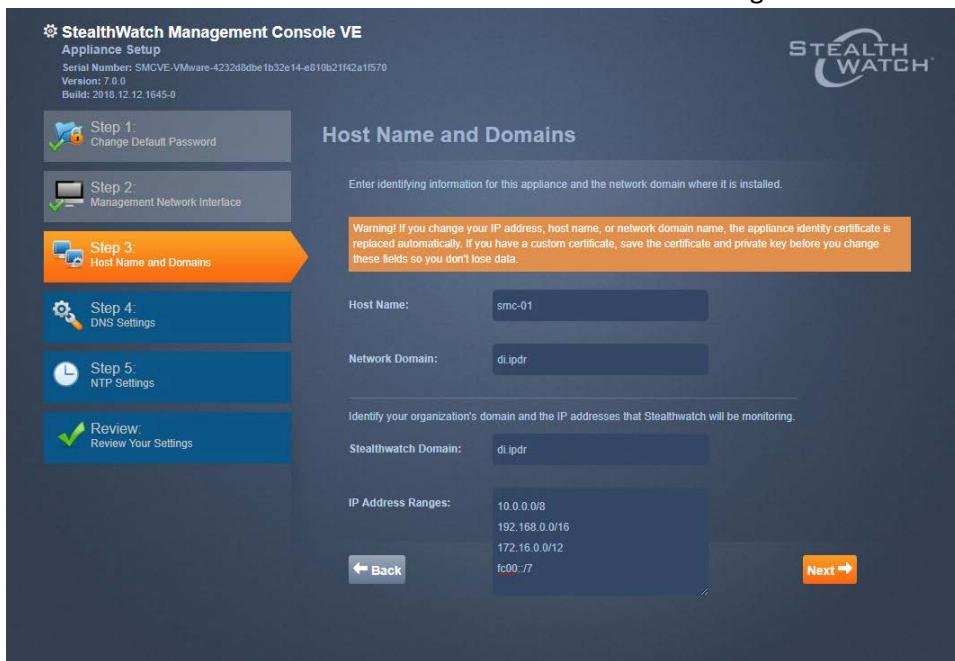
2180

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

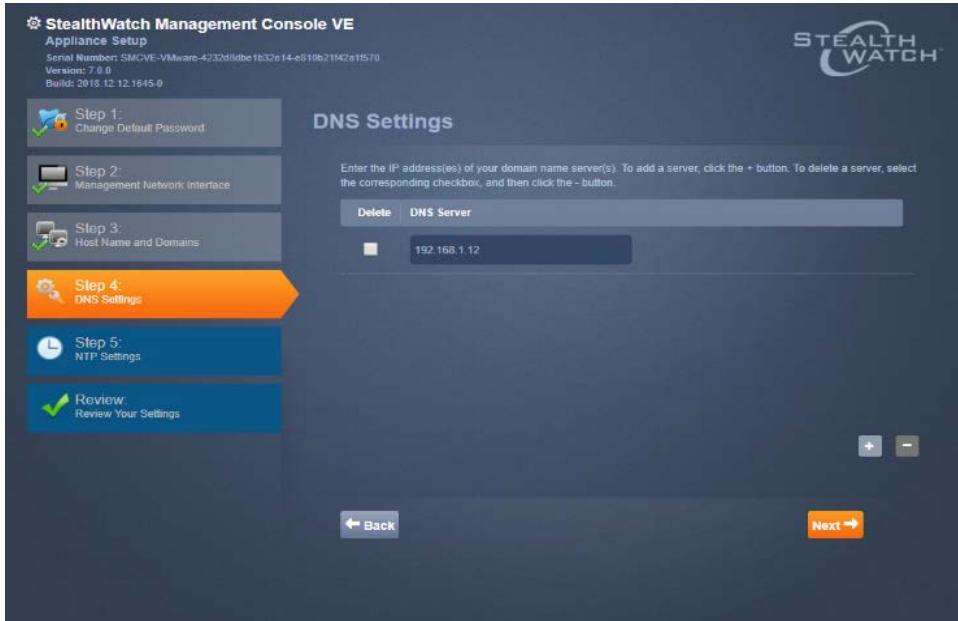
4. Click **Next**.
5. Enter a **host name**.
6. Enter the network domain that Stealthwatch is in for **Network Domain**.
7. Enter the network domain that Stealthwatch will be monitoring for **Stealthwatch Domain**.



2189

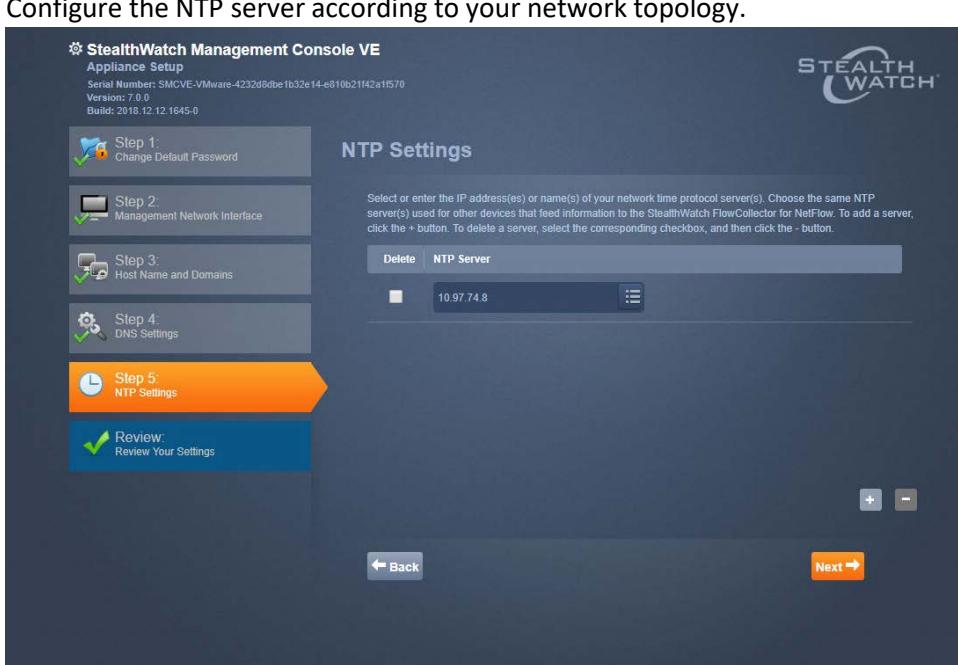
2190 8. Click **Next**.

2191 9. Enter a **DNS Server**.



2192 10. Click **Next**.

2193 11. Configure the NTP server according to your network topology.



2195 12. Click **Next**.

2196 13. Select **Restart**.



2198
2199

14. Click Apply.



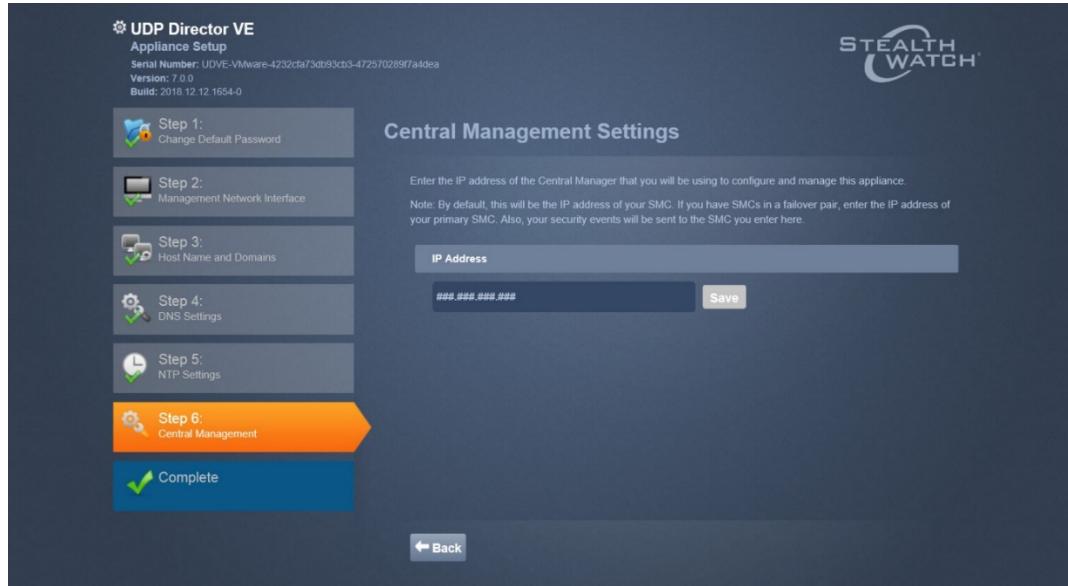
2200
2201

15. After the restart, click Next.

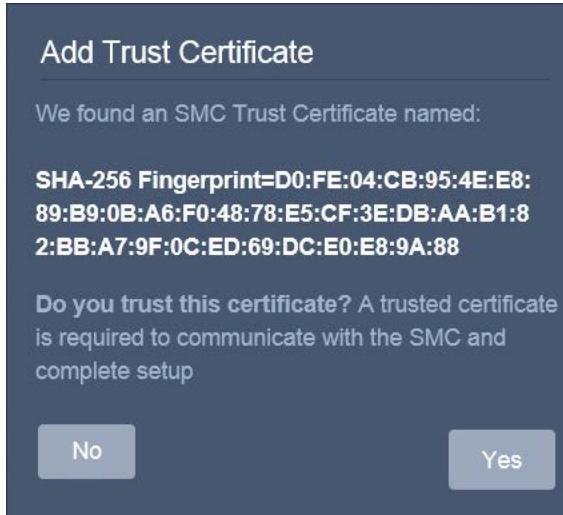
- 2202 **2.13.4 Configure the Stealthwatch UDP Director, Stealthwatch Flow Collector and Stealthwatch Flow Sensor Web Interfaces**
- 2203
- 2204 1. Repeat steps 1-12 from *Configure the Stealthwatch Management Console Web Interface*.

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**.

Please enter your administration credentials below.

In order to be added for management you must enter your SMC administration credentials below.

User ID: [Redacted]

Password: [Redacted]

Cancel Next ➔

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 0xfbbe00000-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 0xfbbe20000-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 0xfbbe40000-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 0xfbbe60000-fbe7ffff

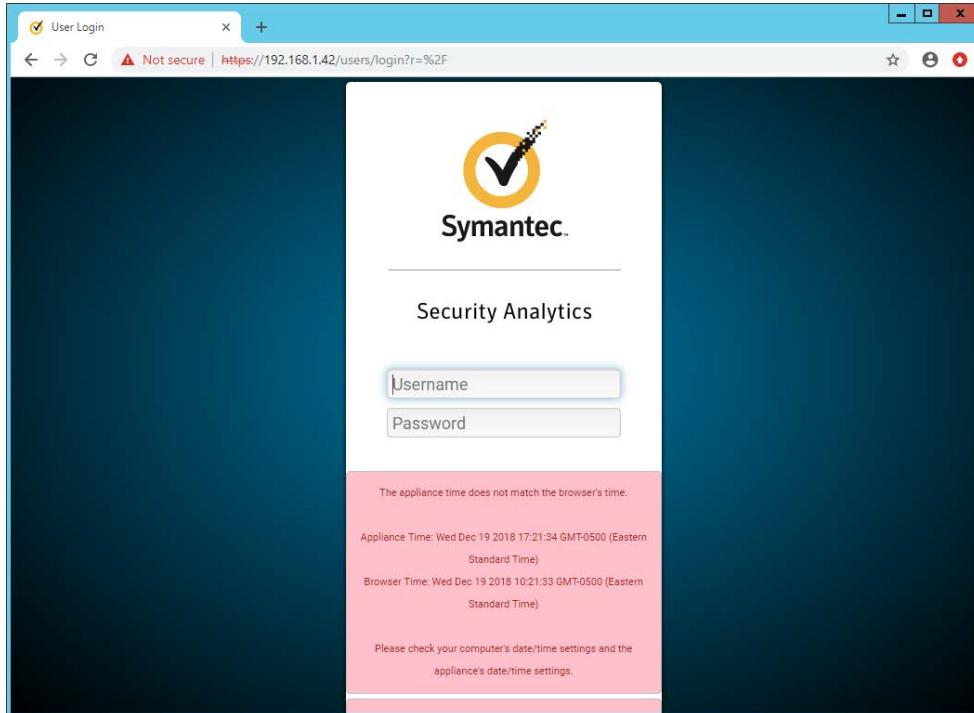
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 1165 bytes 428654 (418.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1165 bytes 428654 (418.6 KiB)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

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

```

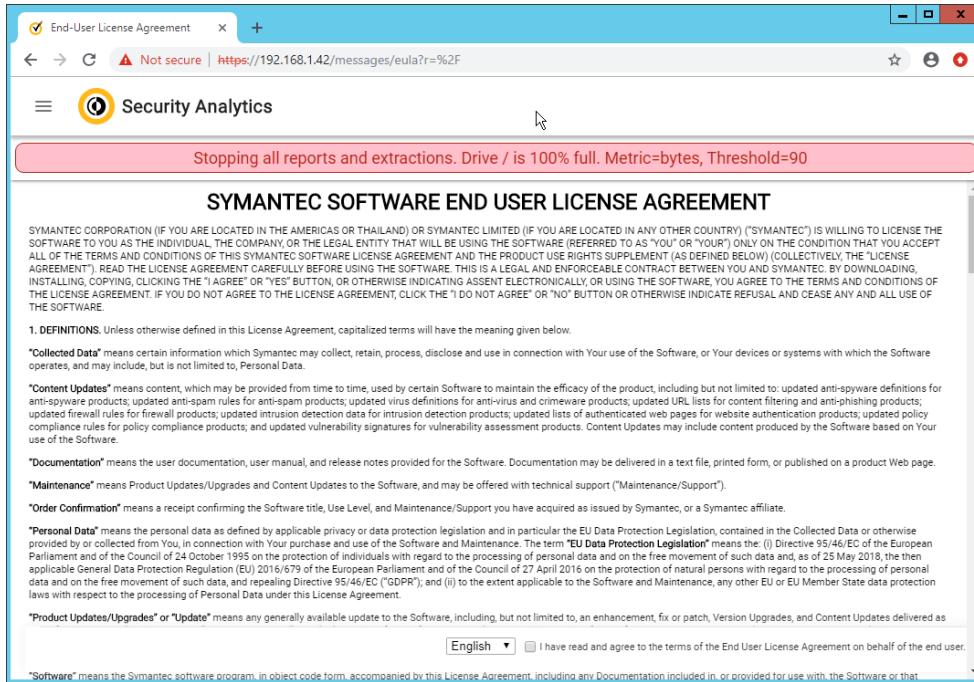
2226

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



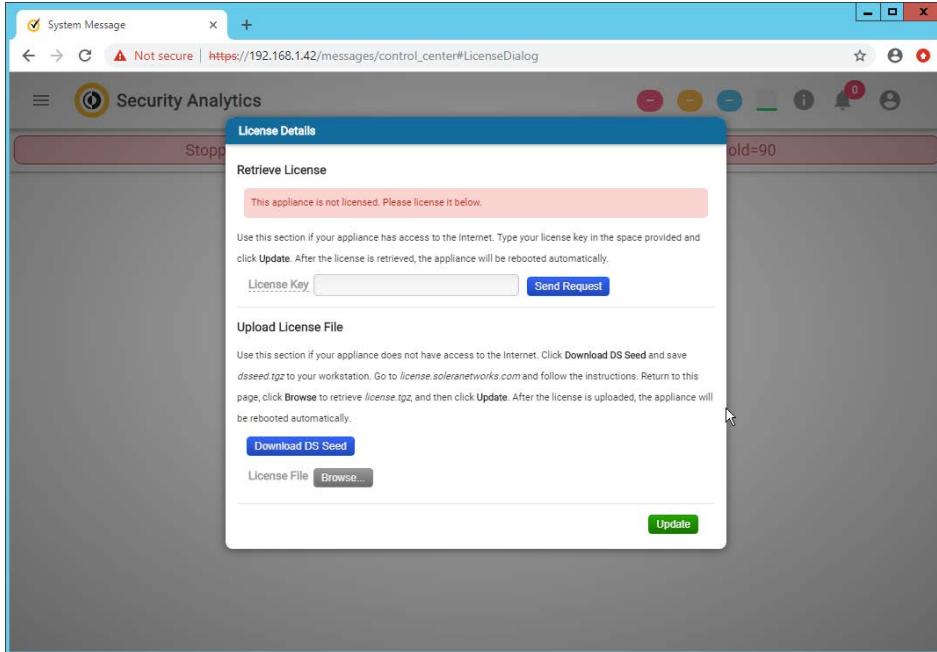
2228
2229
2230
2231

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.**

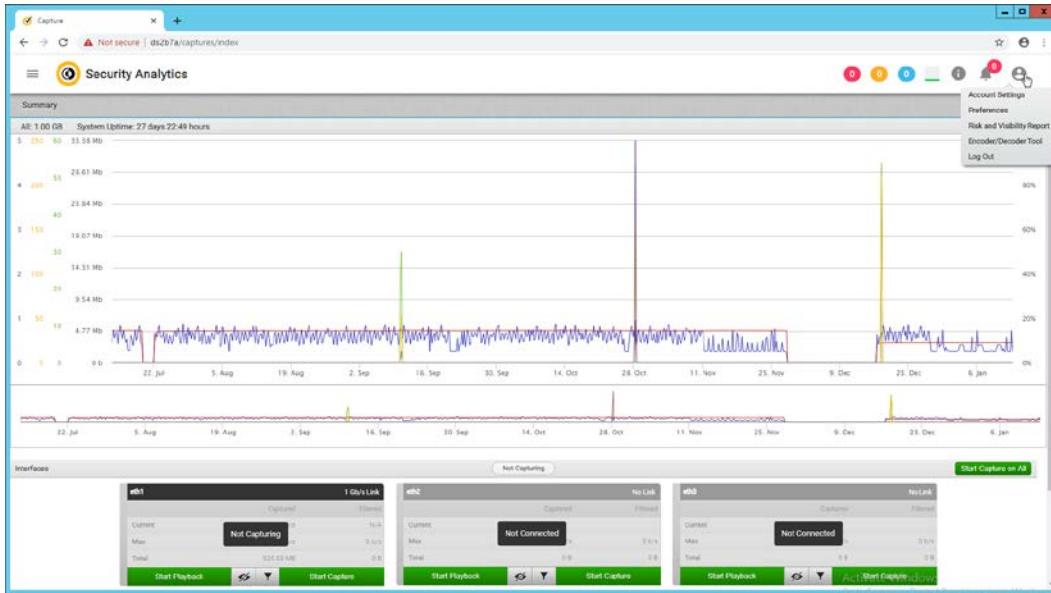


2232

- 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**. Otherwise, click **Send Request**.



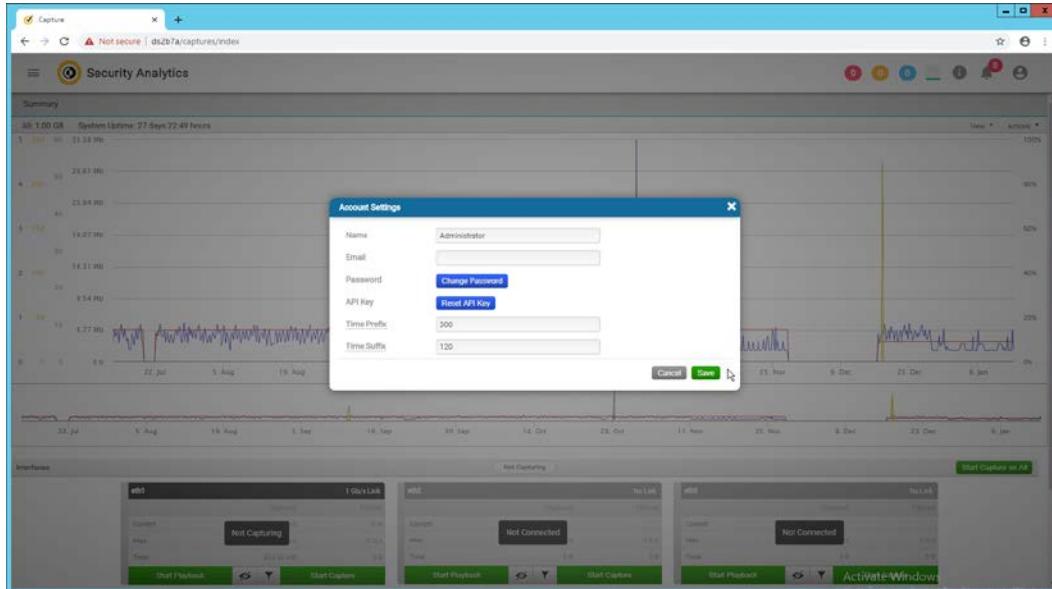
- 2237 9. Click **Update**. The device will reboot.
- 2238 10. Log in to the web page again.
- 2239 11. Click the silhouette in the top right corner and click **Account Settings**.



2241

2242

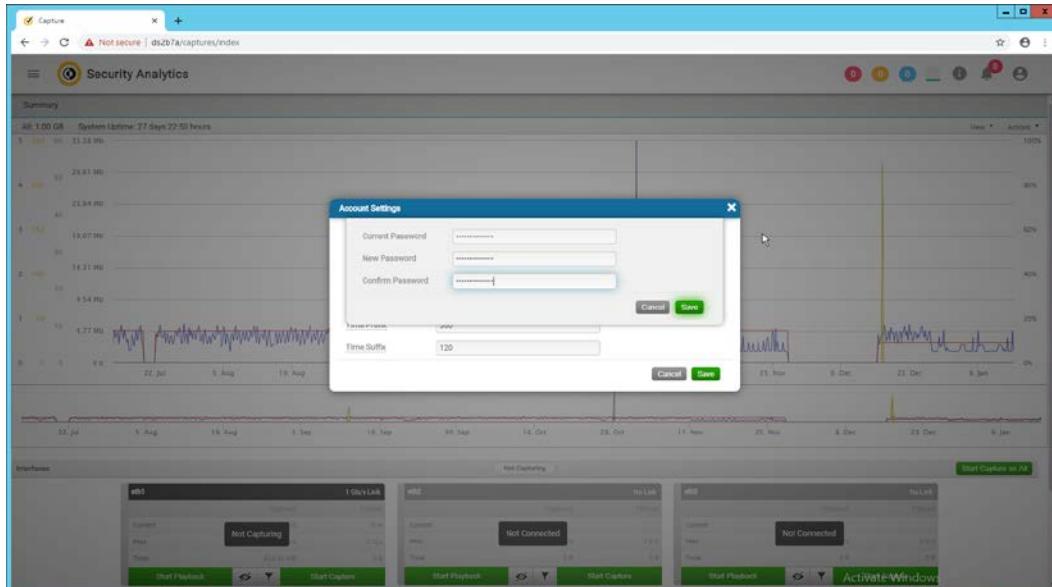
12. Click Change Password.



2243

2244

13. Enter a new password. Click Save.



2245

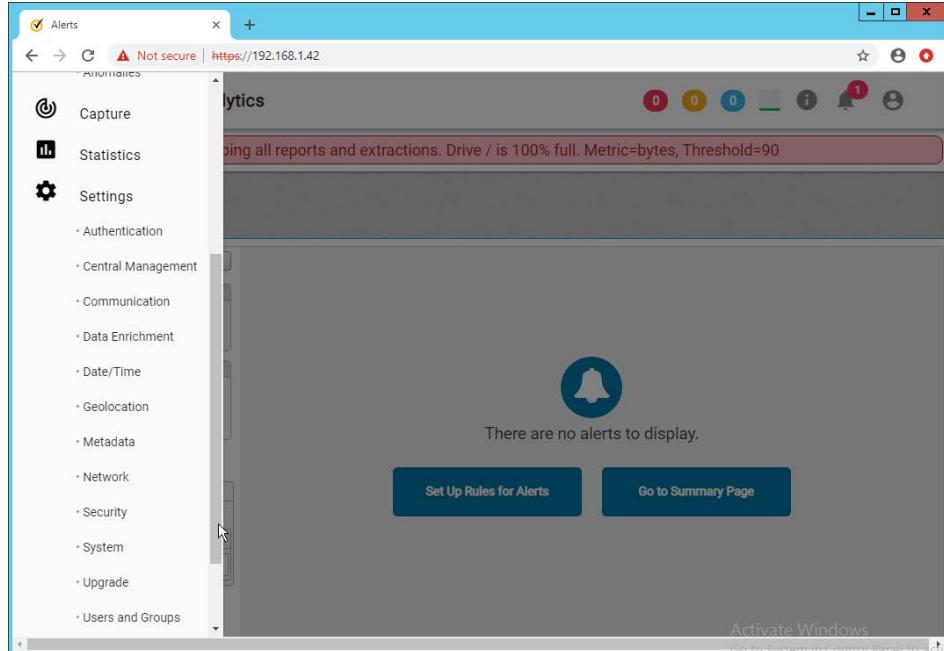
2246

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.

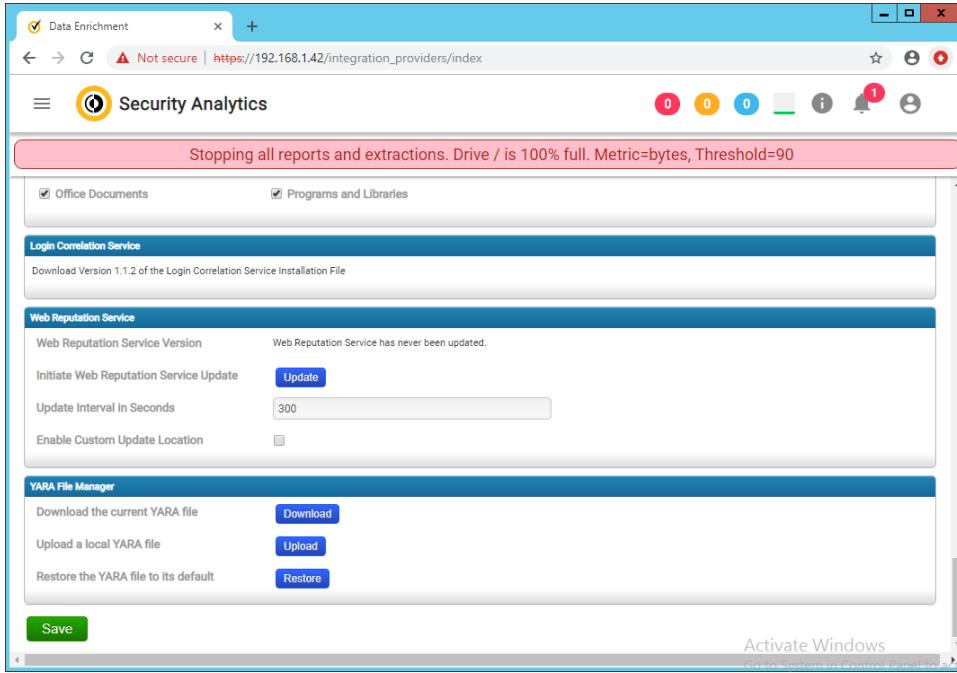
The screenshot shows the Symantec Security Analytics interface with the following details:

- Symantec Intelligence Services:**
 - Symantec Web Reputation Service: Licensed, Yes, -/n/a-, Actions: Power (red), Edit, Info.
 - Symantec File Reputation Service: Archives, Binaries, Debian Packages, Office Documents, Programs and Libraries, JAR Archives, Adobe PDF, Yes, Actions: Power (red), Edit, Info.
- Data Enrichment Profiles:** A dropdown menu shows "Full Data Enrichment (No Anomaly Detection)".
- Symantec Analysis Providers:**
 - ICAP: Default filters, Actions: Power (red), Edit, Info.
 - Malware Analysis Appliance: Archives, Debian Packages, Office Documents, Programs and Libraries, Adobe PDF, Actions: Power (red), Edit, Info.
- Symantec On-Demand Providers:**
 - ATP: -/n/a-, Actions: Power (red), Edit, Info.
 - DeepSight: -/n/a-, Actions: Power (red), Edit, Info.

The status bar at the bottom of the interface displays the message: "Stopping all reports and extractions. Drive / is 100% full. Metric=bytes, Threshold=90".

2256
2257
2258

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

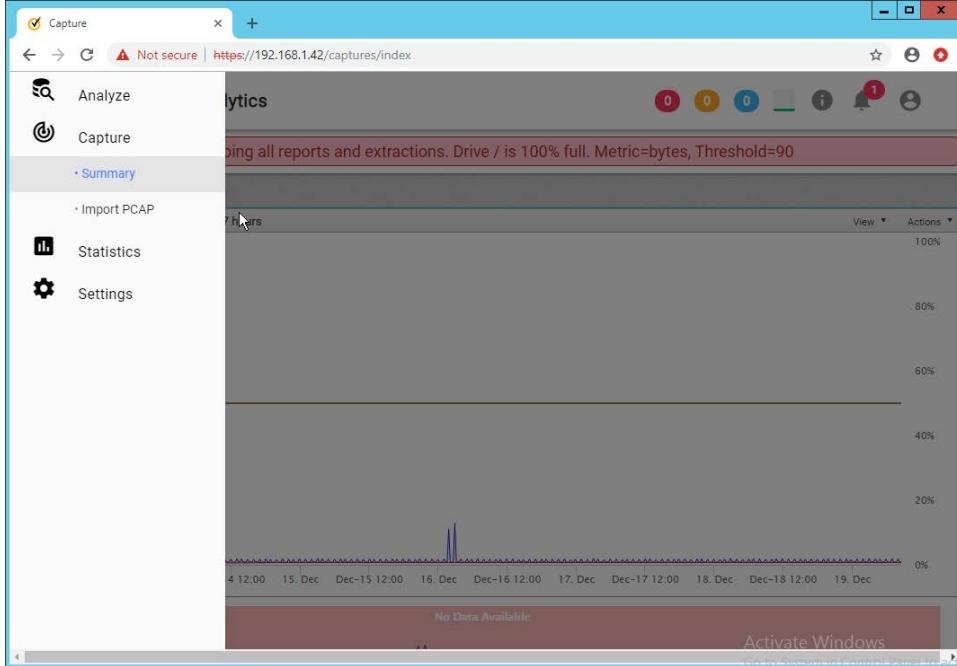


2259
2260

19. Click **Save**.

2.14.2 Capturing Data

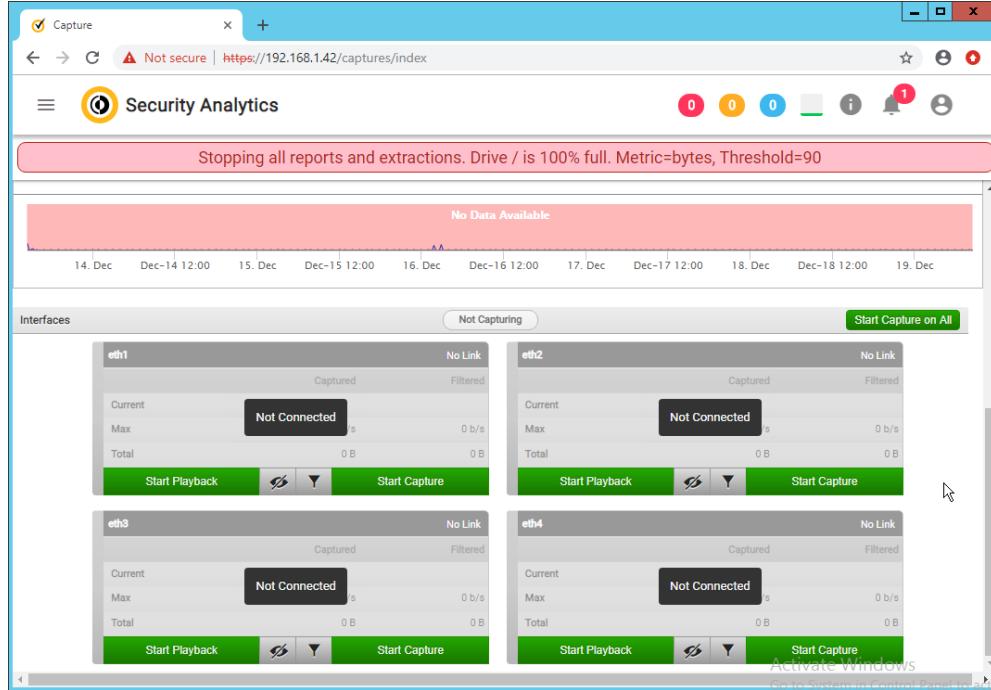
2261 1. Navigate to **Capture > Summary** in the menu.



2263

2264

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



2265

2.15 Symantec Information Centric Analytics

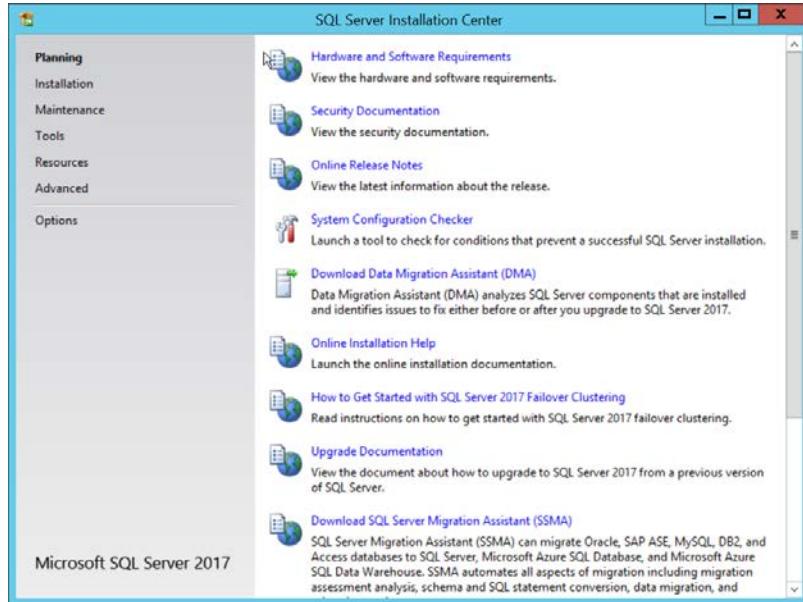
2266 This section describes the installation and configuration of Symantec Information Centric Analytics (ICA).

2.15.1 Installing MS SQL 2017

- 2269 1. Launch the SQL Setup Wizard.

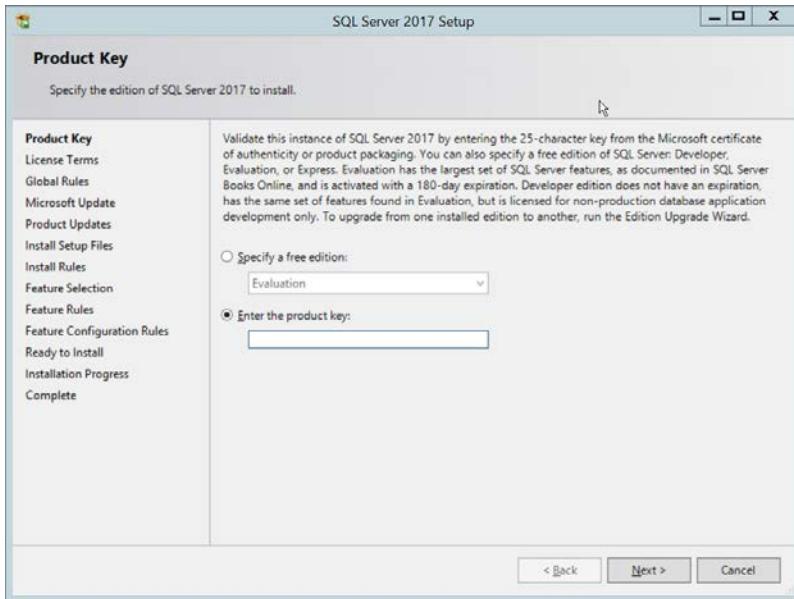
2271
2272

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**.

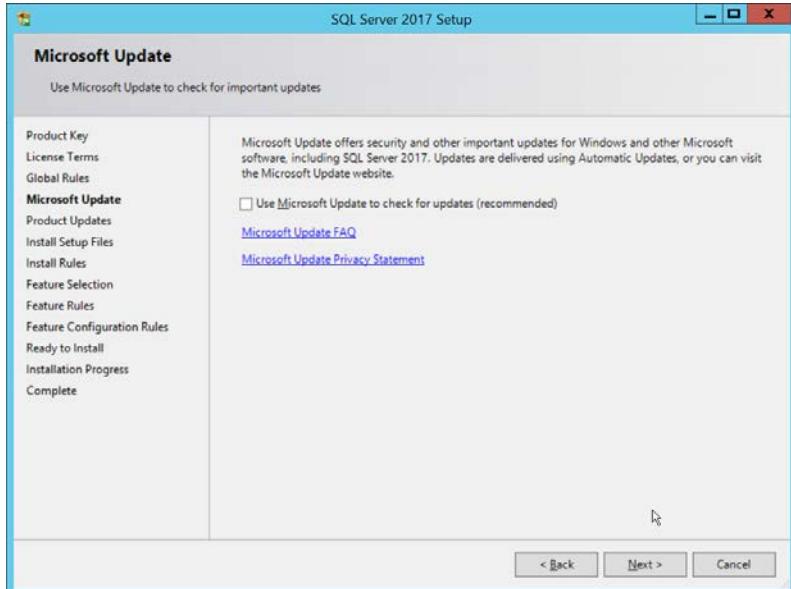


2279
2280

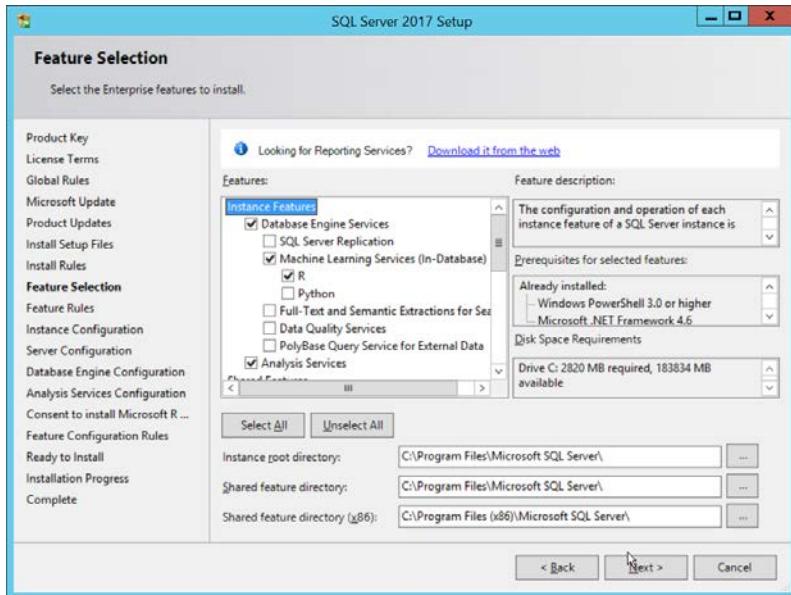
7. Click **Next**.

2281
2282

8. Click **Next**.

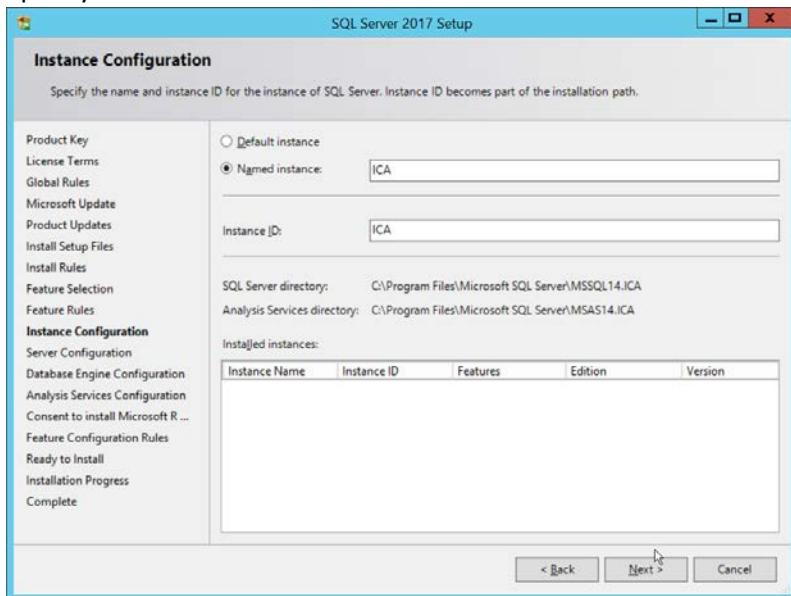
2283
2284
2285

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



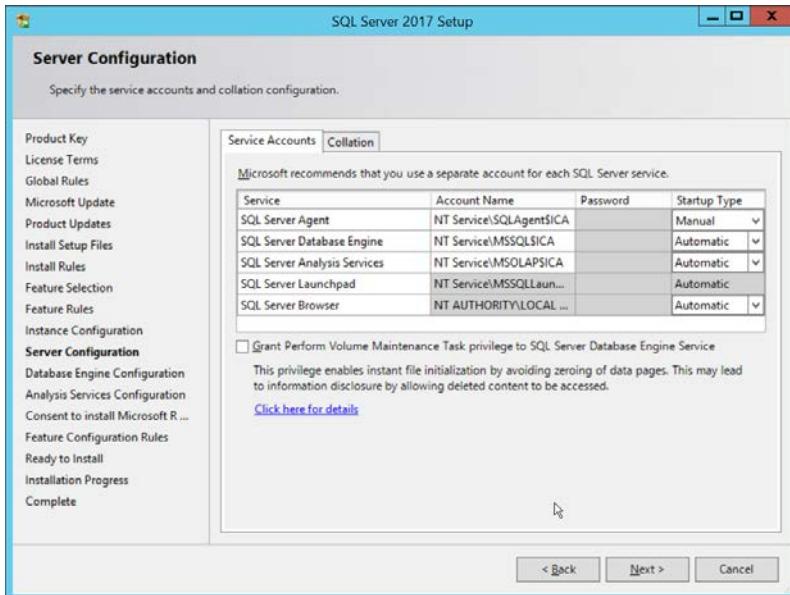
2286
2287
2288
2289

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



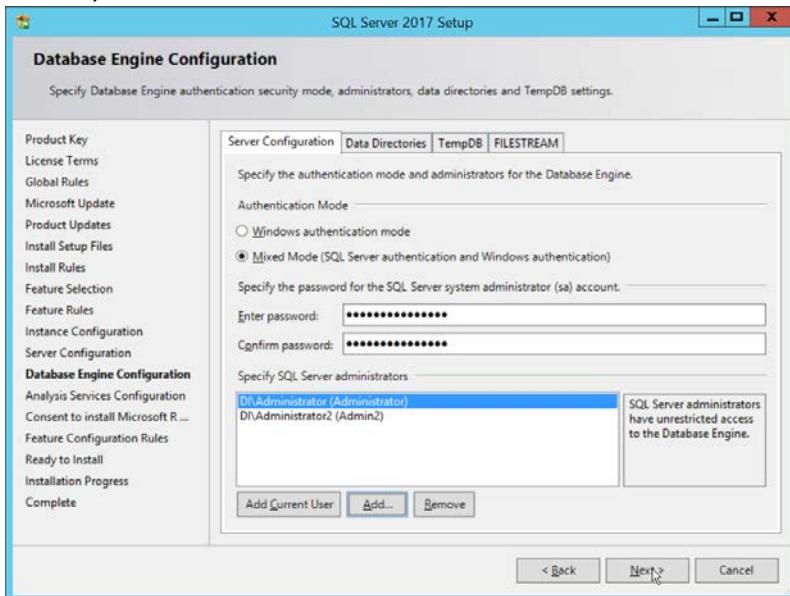
2290
2291

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.

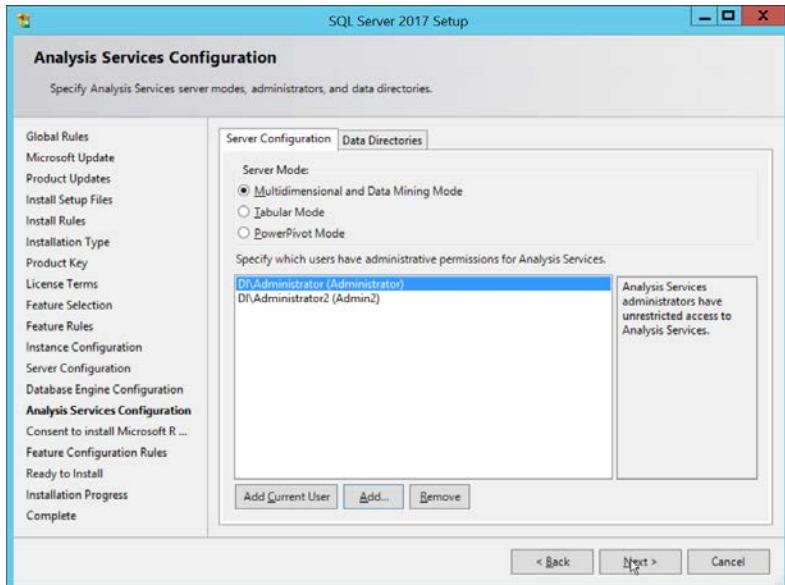


2297
2298
2299
2300

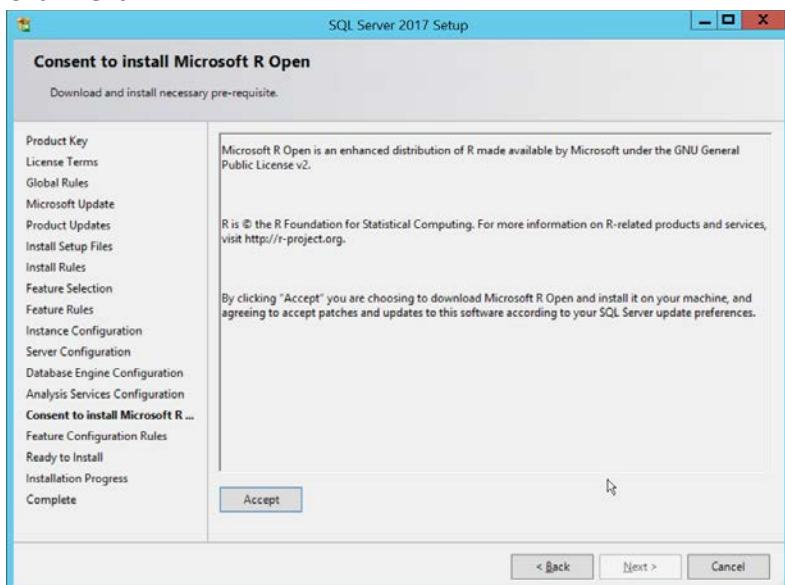
19. Click Next.
20. Select **Multidimensional and Data Mining Mode**.
21. Add any users who should be administrators of the Analysis Services.

2301
2302

22. Click Next.

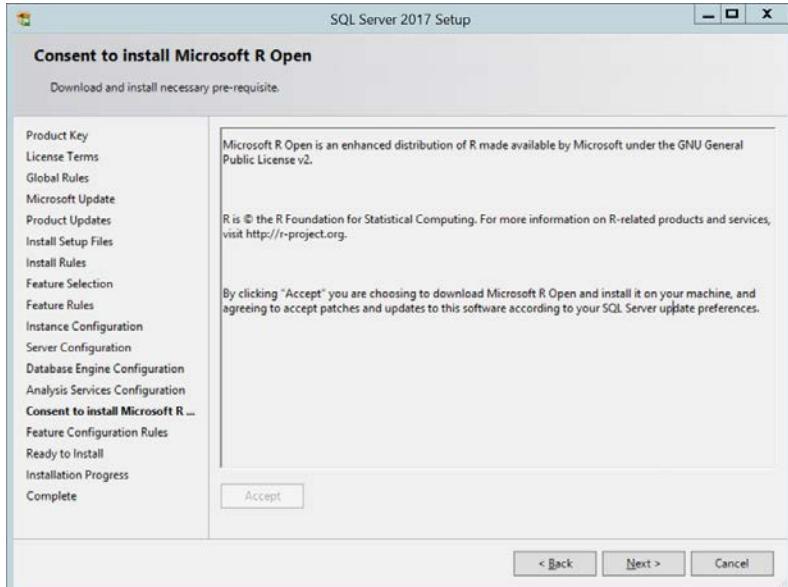
2303
2304

23. Click Accept.

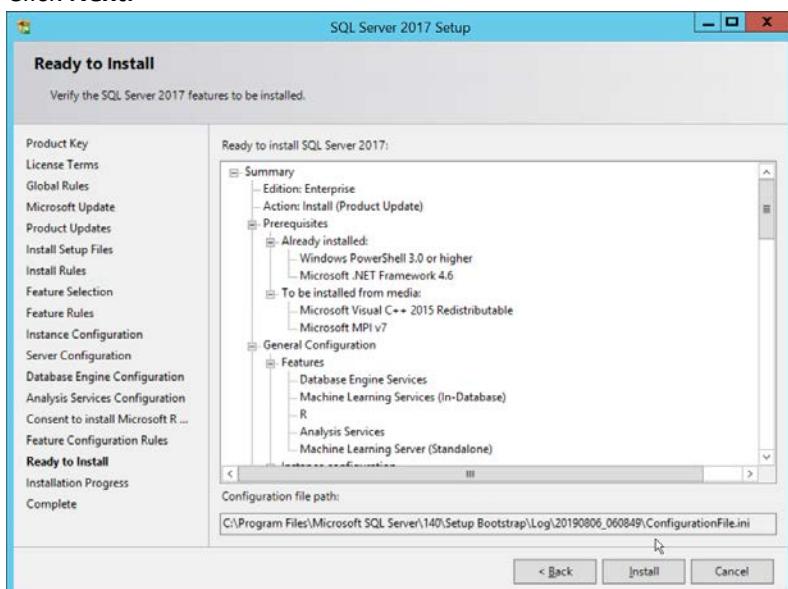


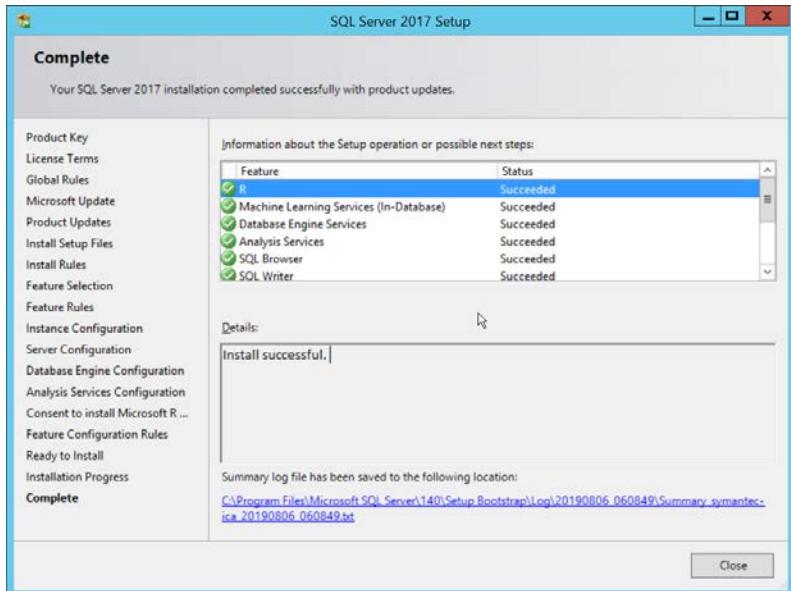
2305
2306

24. Click Next.

2307
2308

25. Click Install.



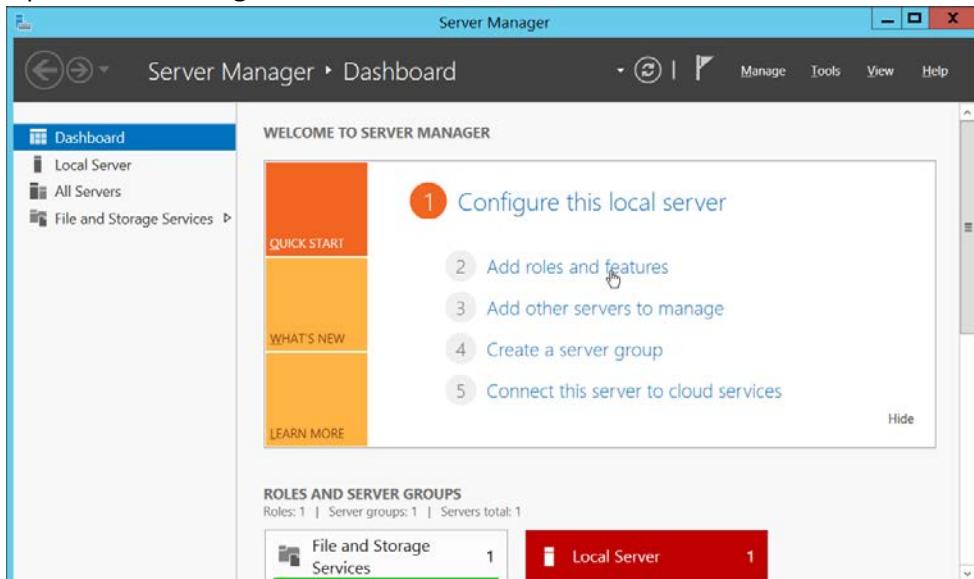


2309
2310

26. Click **Close**.

2.15.2 Install Windows Services

2311 1. Open **Server Manager**.

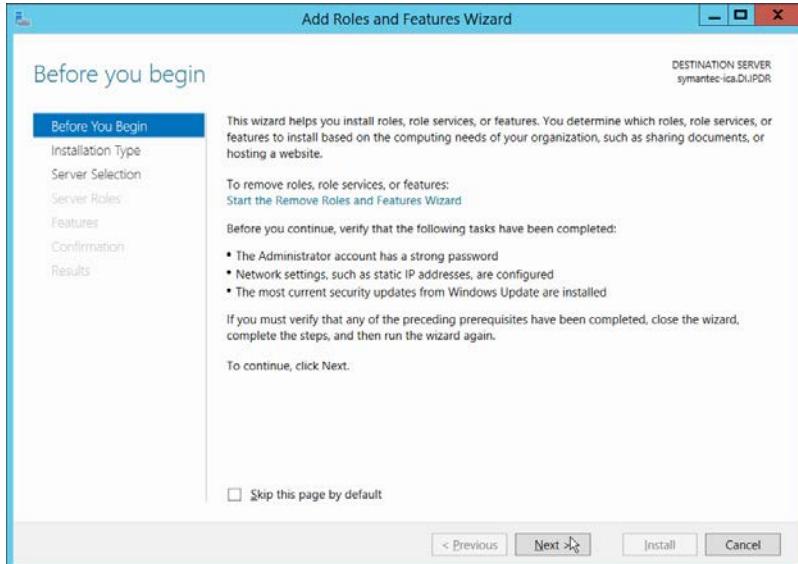


2313
2314

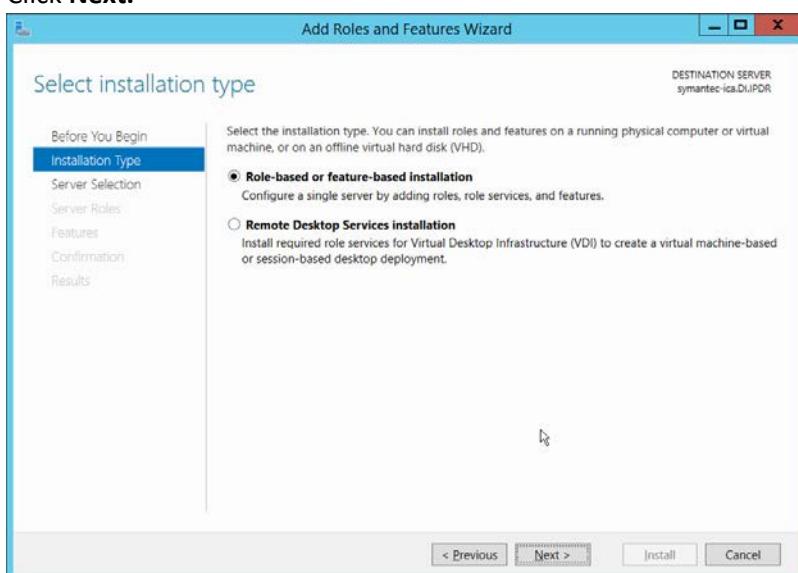
2. Click **Add Roles and Features**.

2315
2316

3. Click **Next**.

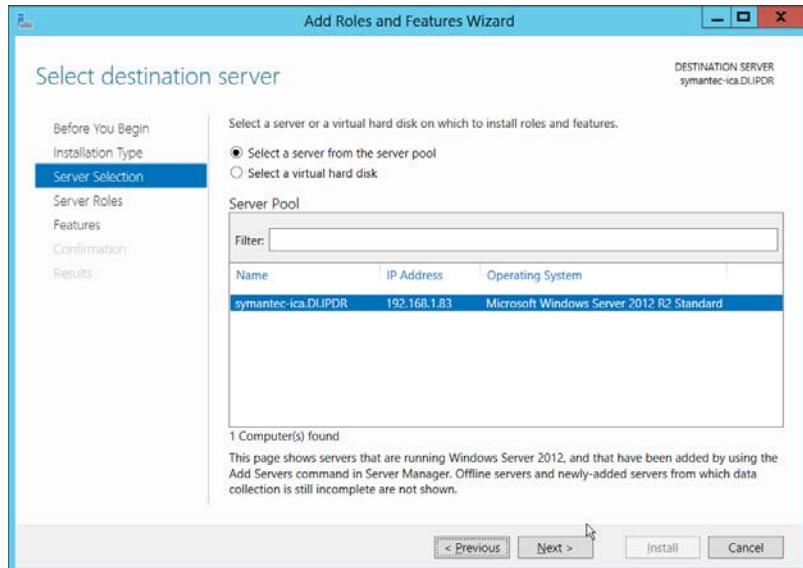
2317
2318

4. Click **Next**.

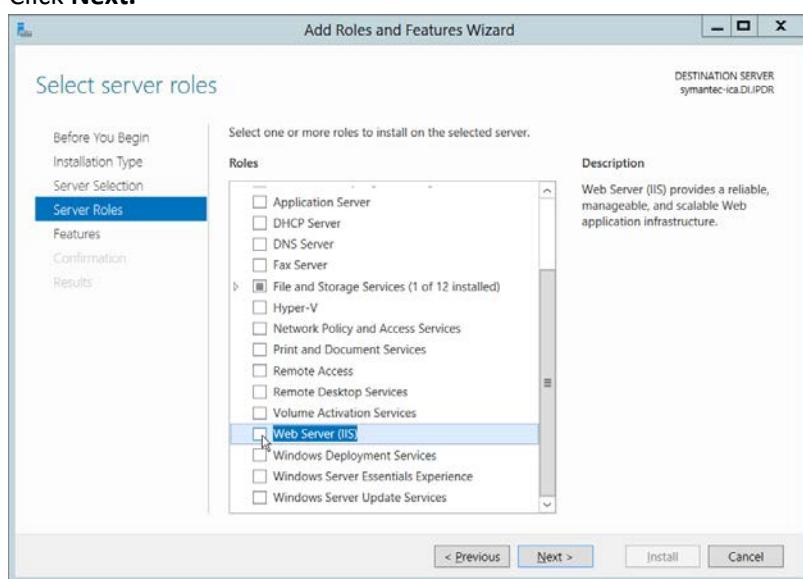


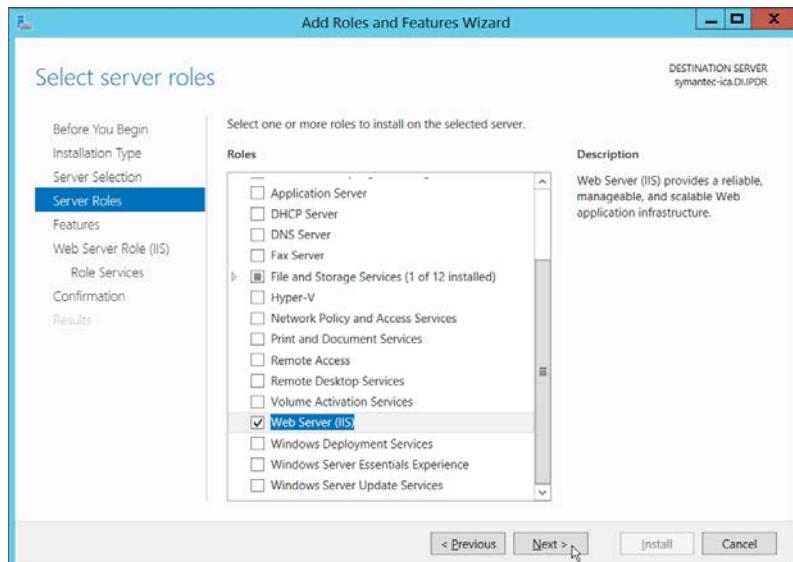
2319
2320

5. Click **Next**.

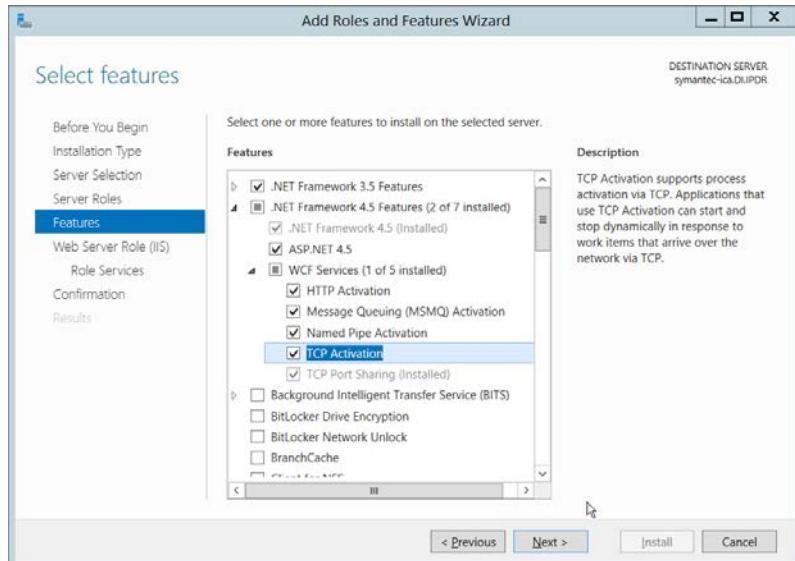
2321
2322

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



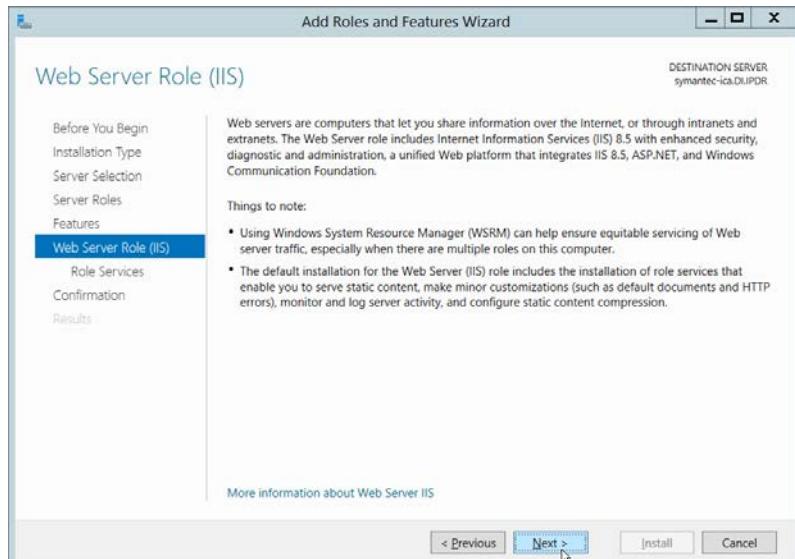
2323
23247. Click **Add Features**.2325
2326
2327
2328

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**.



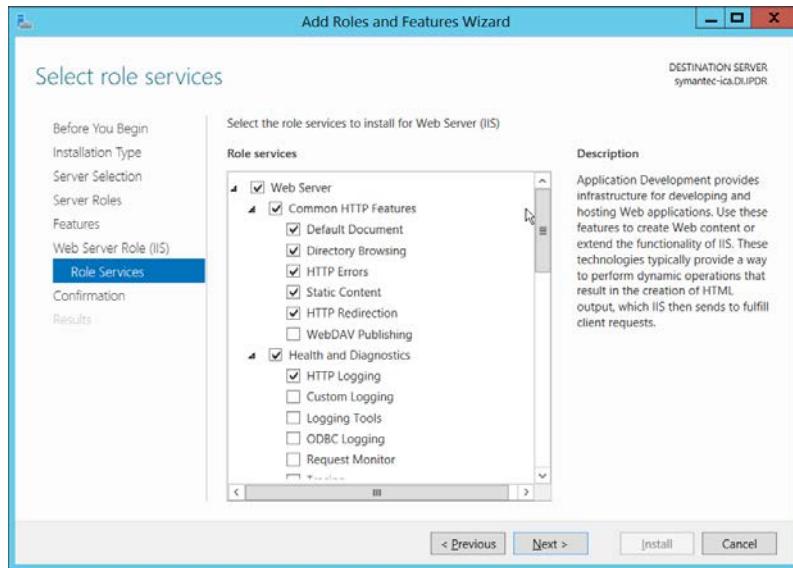
2331
2332

12. Click **Next**.

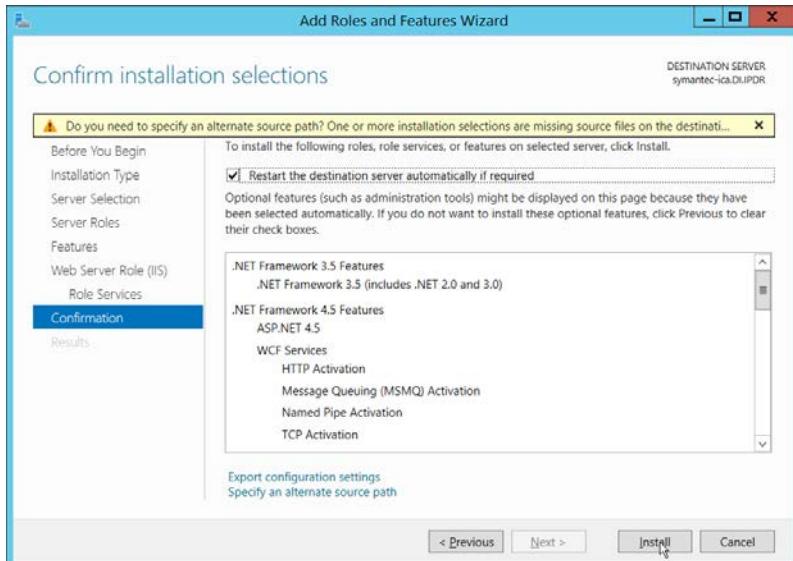
13. Ensure that the following **Role Services** are selected:

- 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**

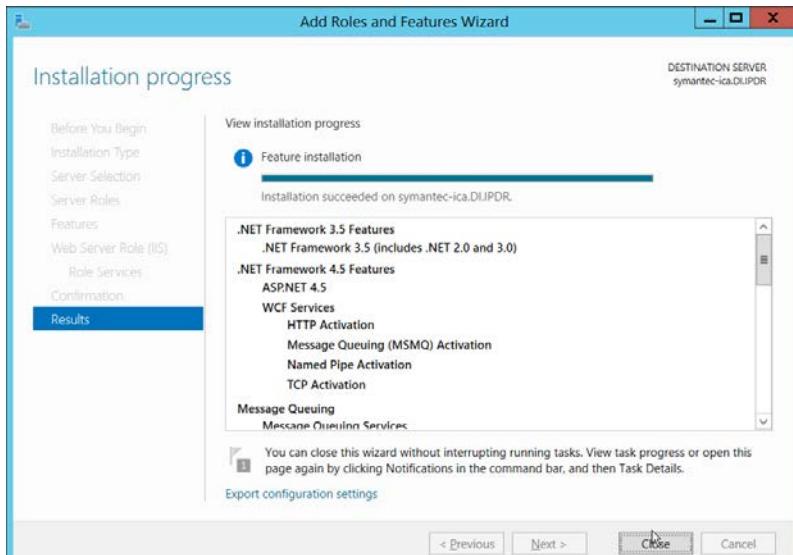


- 2349 14. Click **Next**.
 2350 15. If necessary, specify a path to **/Sources/SxS**, which is found in the Windows Installation Media.
 2351 16. Check the box next to **Restart the destination server automatically if required**.



2353
2354

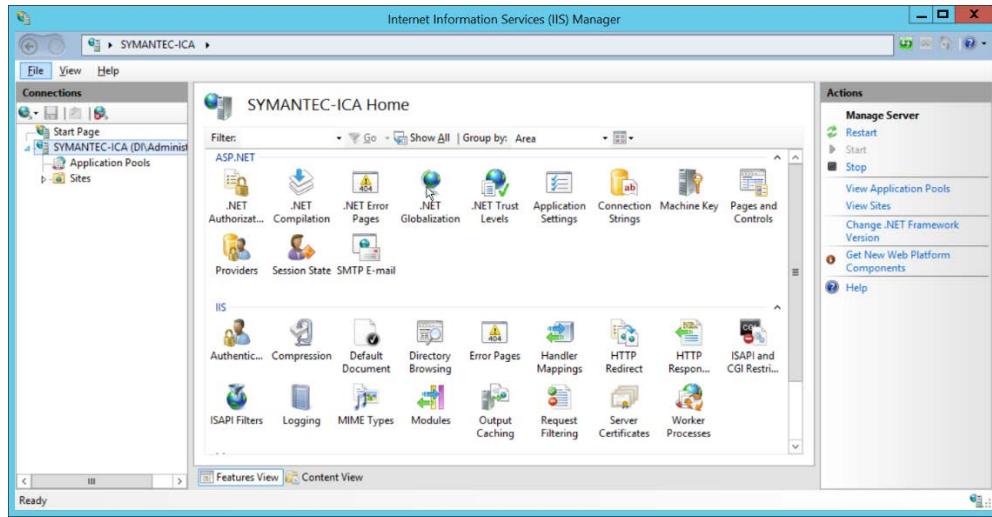
17. Click Install.



2355
2356
2357

18. Click Close when the installation finishes.

19. Open Internet Information Services Manager.



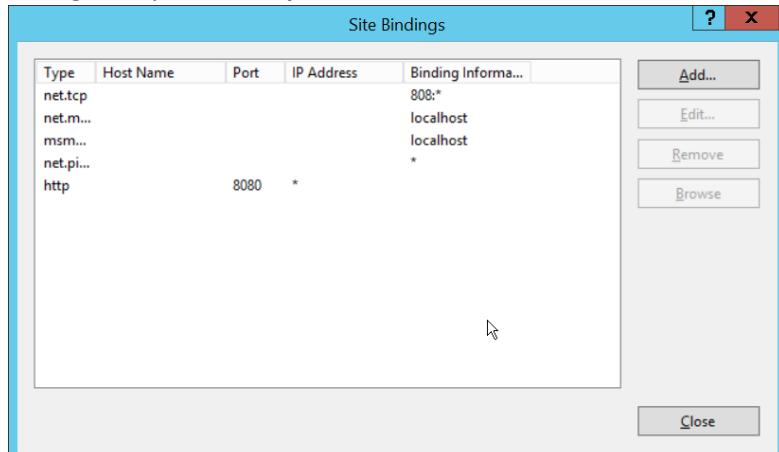
2358

2359

2360

2361

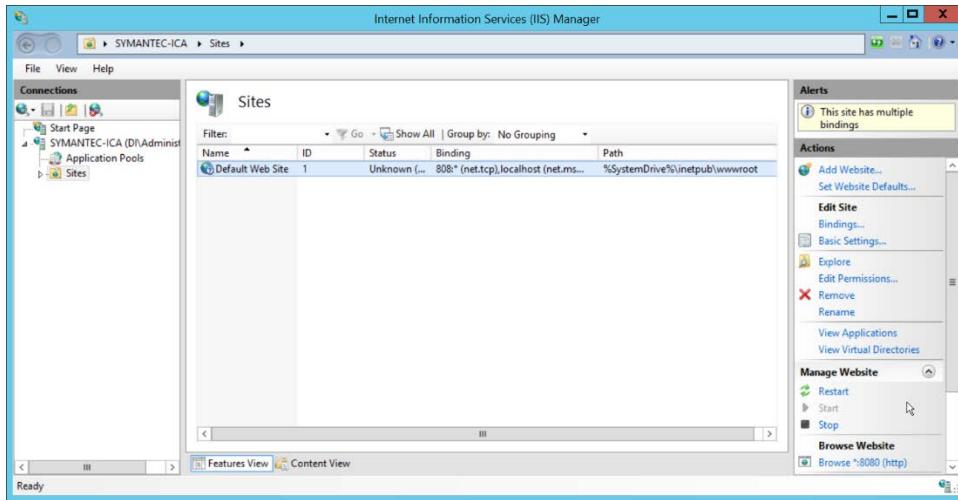
20. Navigate to **SERVER-NAME > Sites**.
21. Right-click the **Default Web Site**, and select **Bindings**.
22. Change the port for **http** to **8080**.



2362

2363

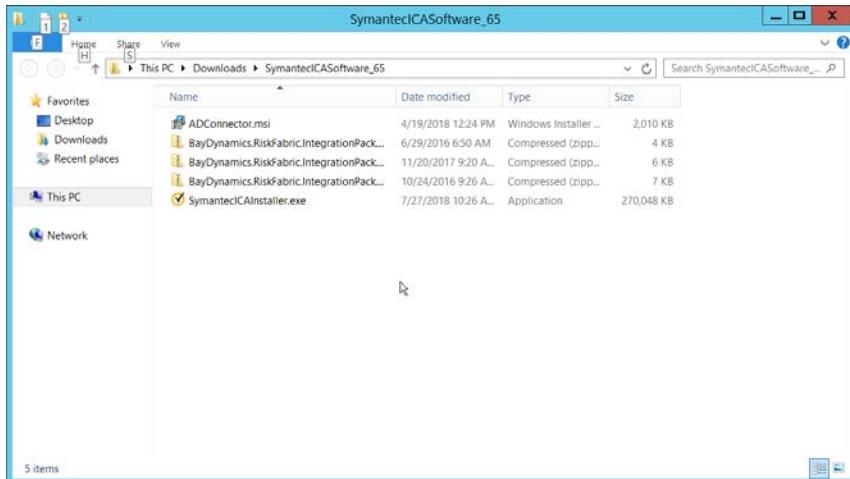
23. Click **Close**.



2364

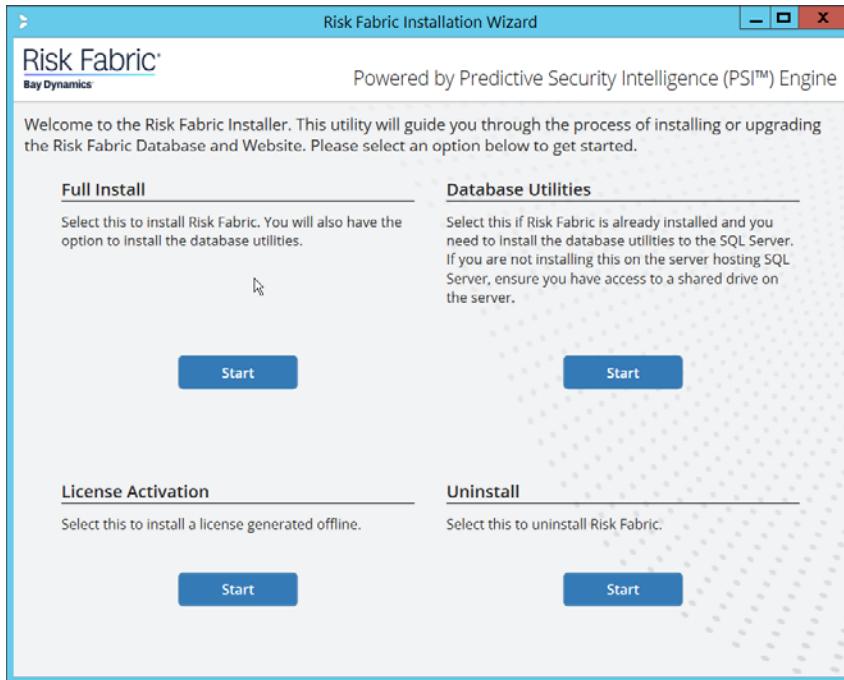
2365 24. Click **Restart** under **Manage Website**.2366 2.15.3 **Installing Symantec ICA**

- 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.



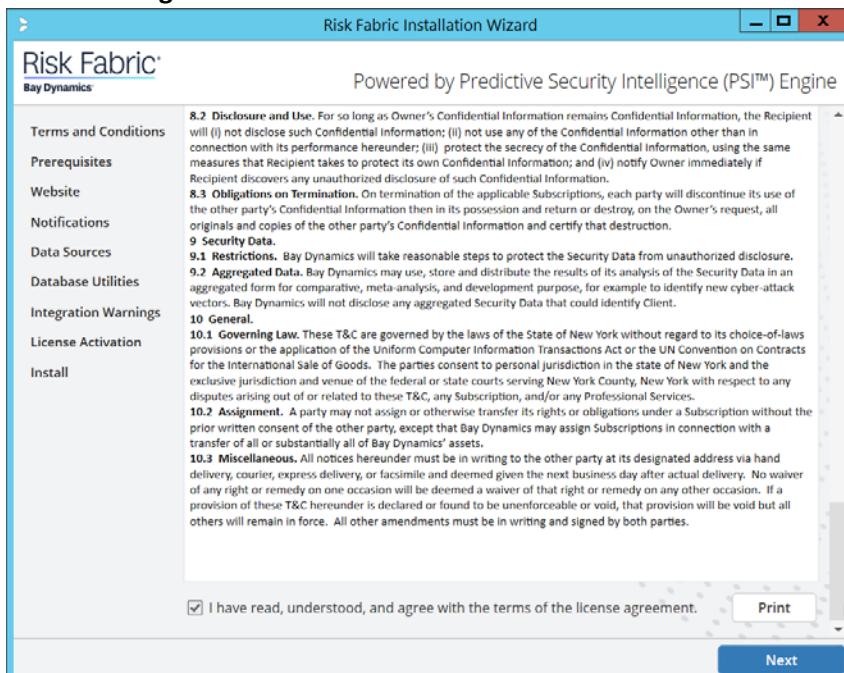
2370

2371 4. Run **SymantecICAInstaller.exe**.



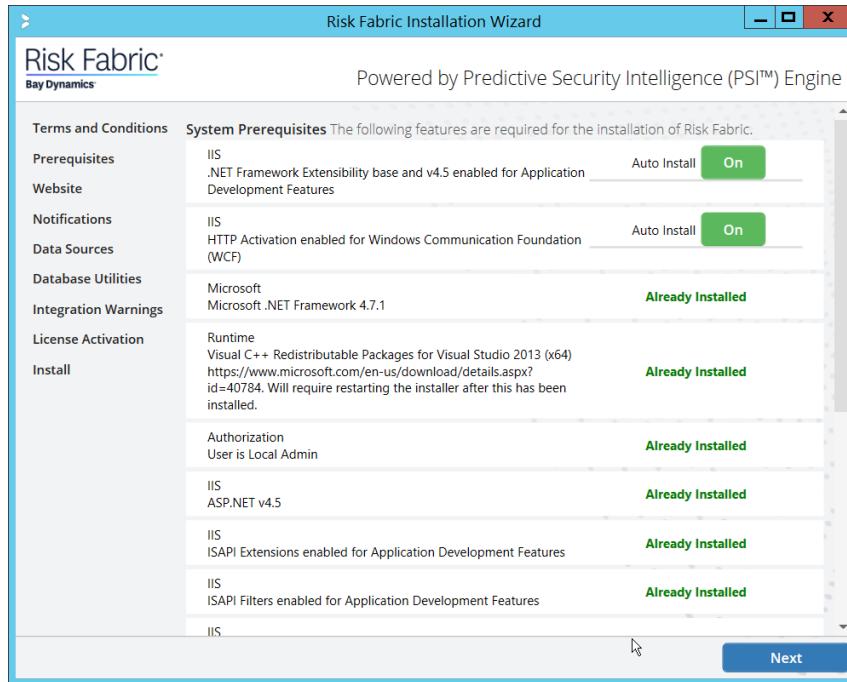
2372
2373
2374
2375

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**.

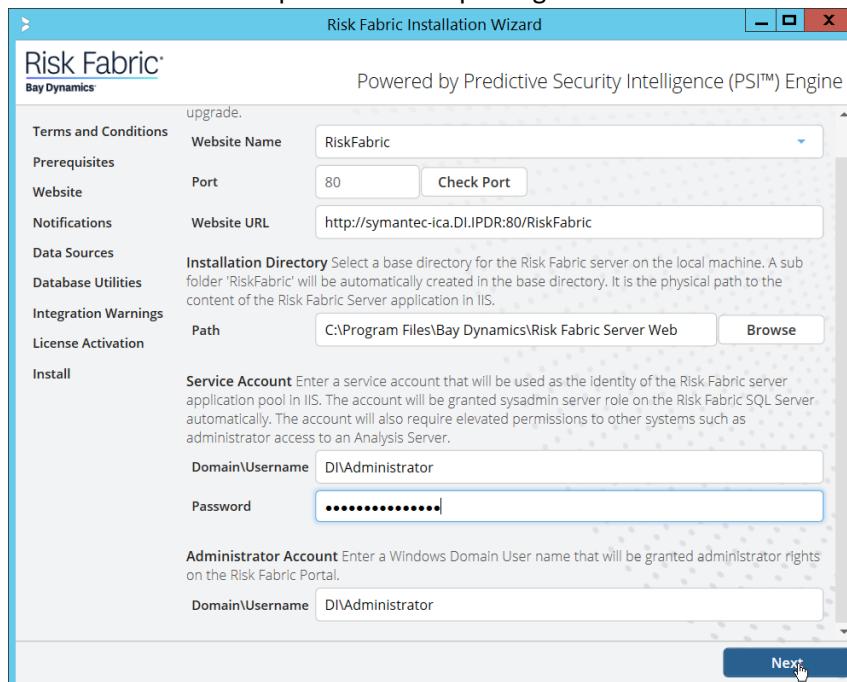


2378

2379

2380

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

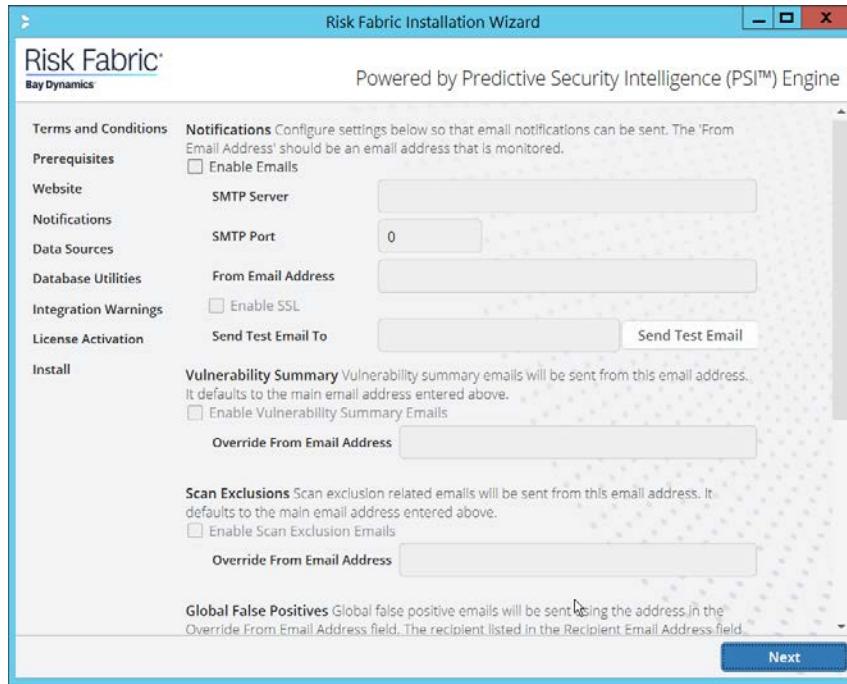


2381

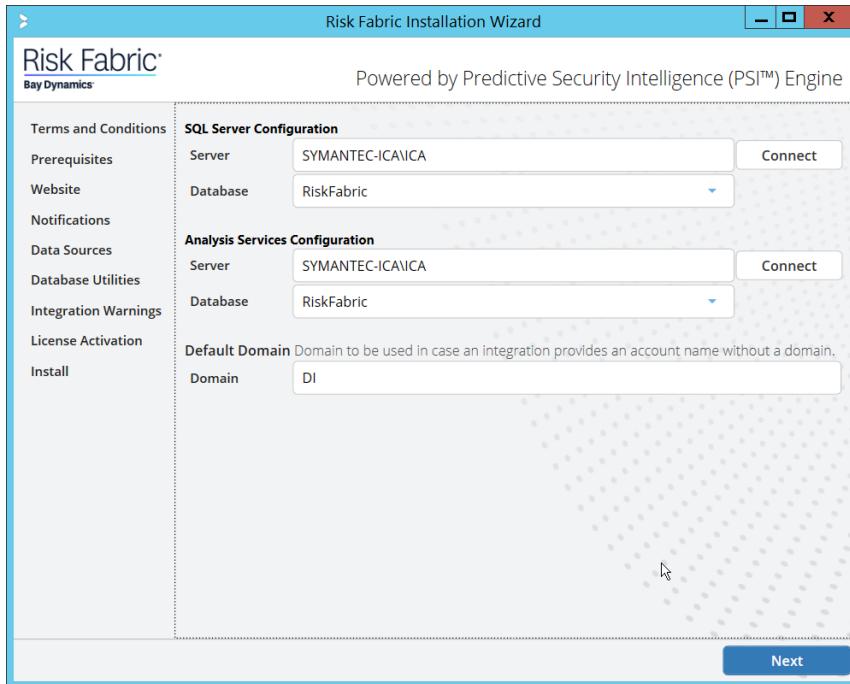
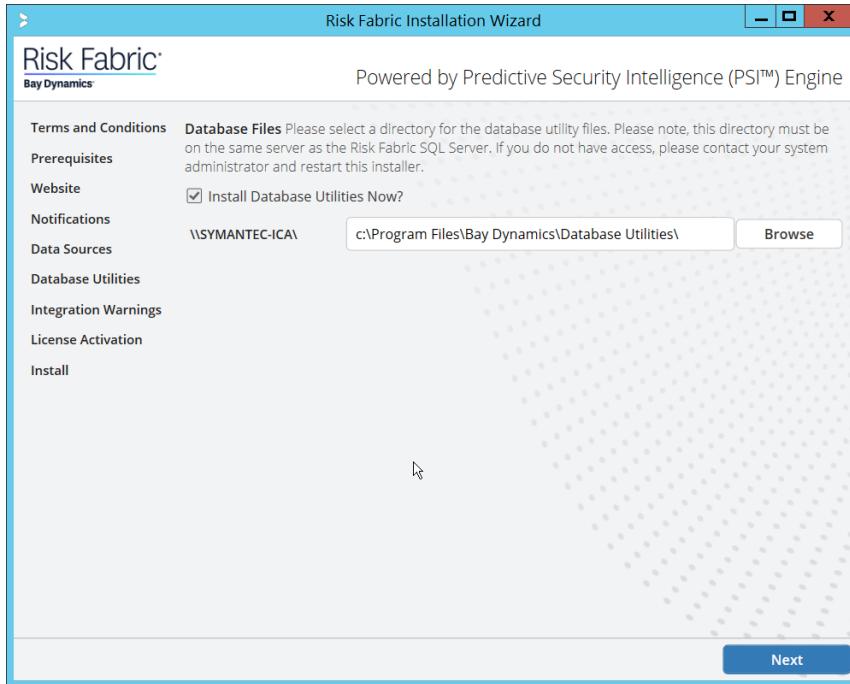
2382

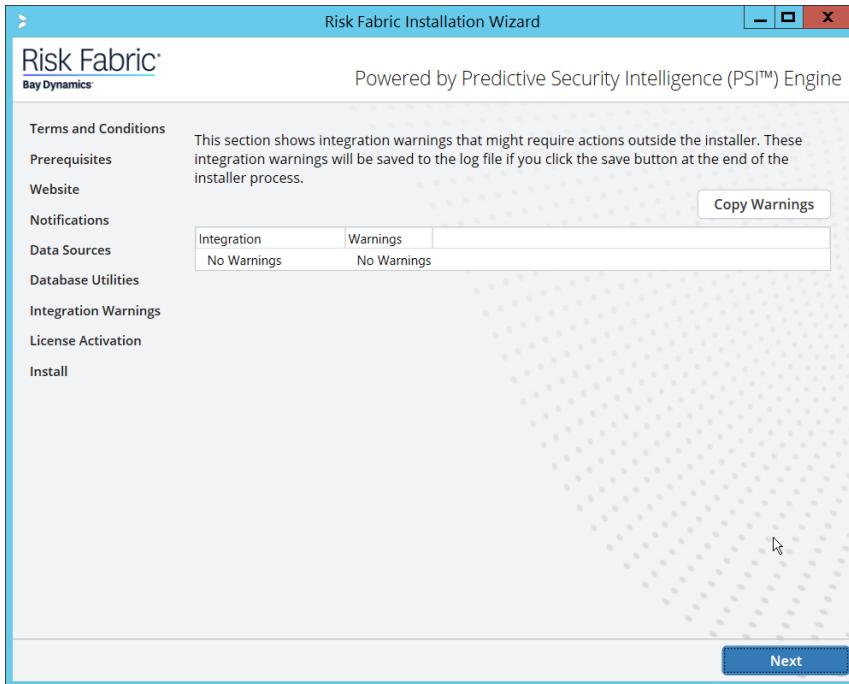
2383

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



2384
2385 12. Click **Next**.
2386 13. Enter the name of the SQL Server you created in the format <SERVER-DOMAIN-NAME>\<SQL-
2387 SERVER-NAME>. 14. Click **Connect**, and verify that there are no connection issues.
2388 15. Enter the name of the SQL Analysis Services server you created in the format <SERVER-
2389 DOMAIN-NAME>\<SQL-SERVER-NAME>. (It may be the same as the SQL Server).
2390 16. Click **Connect**, and verify that there are no connection issues.
2391

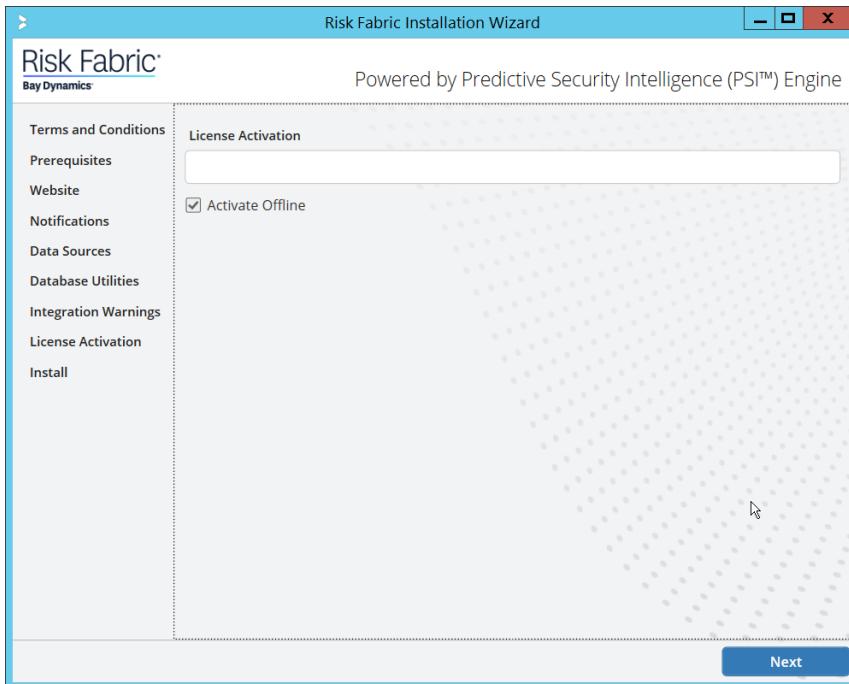
2392
239317. Click **Next**.2394
239518. Click **Next**.



2396

2397

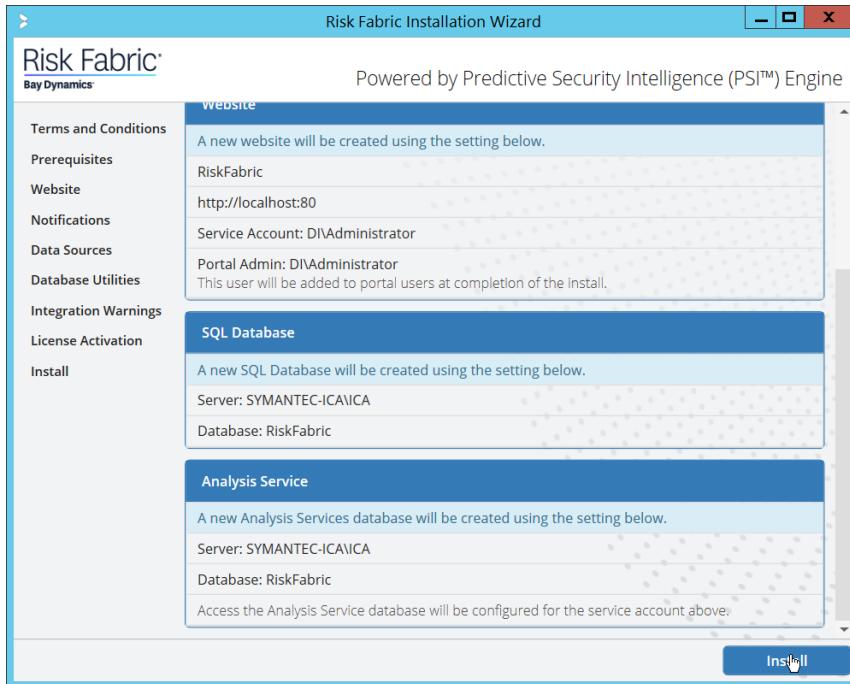
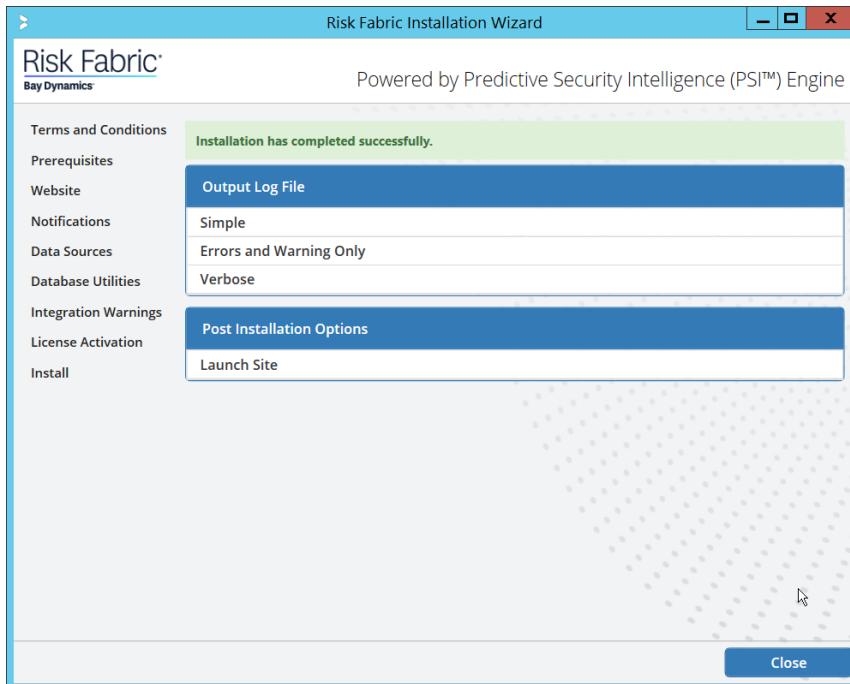
2398

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

2399

2400

21. Click Next.

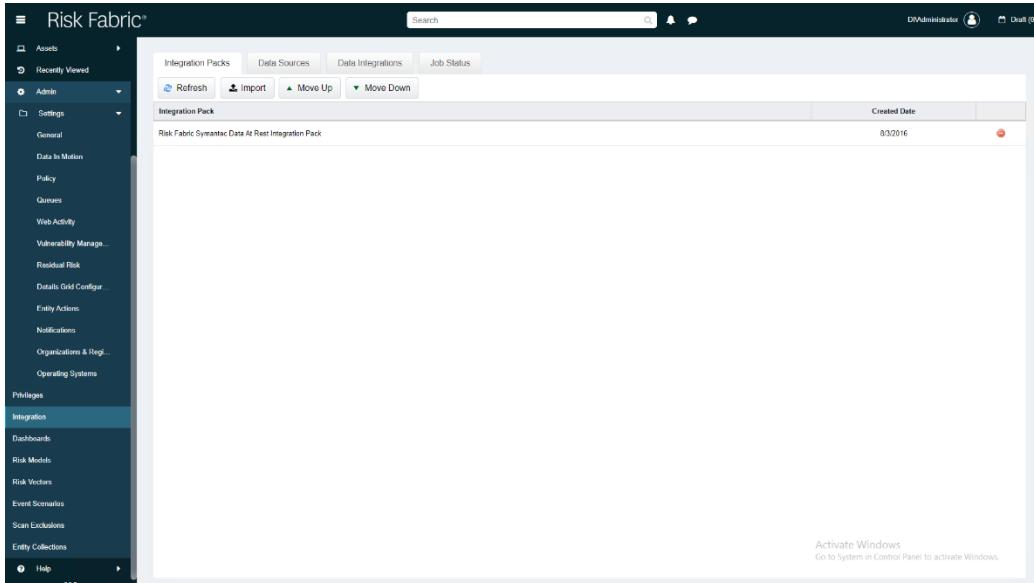
2401
2402**22. Click Install.**2403
2404**23. Click Close.**

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***

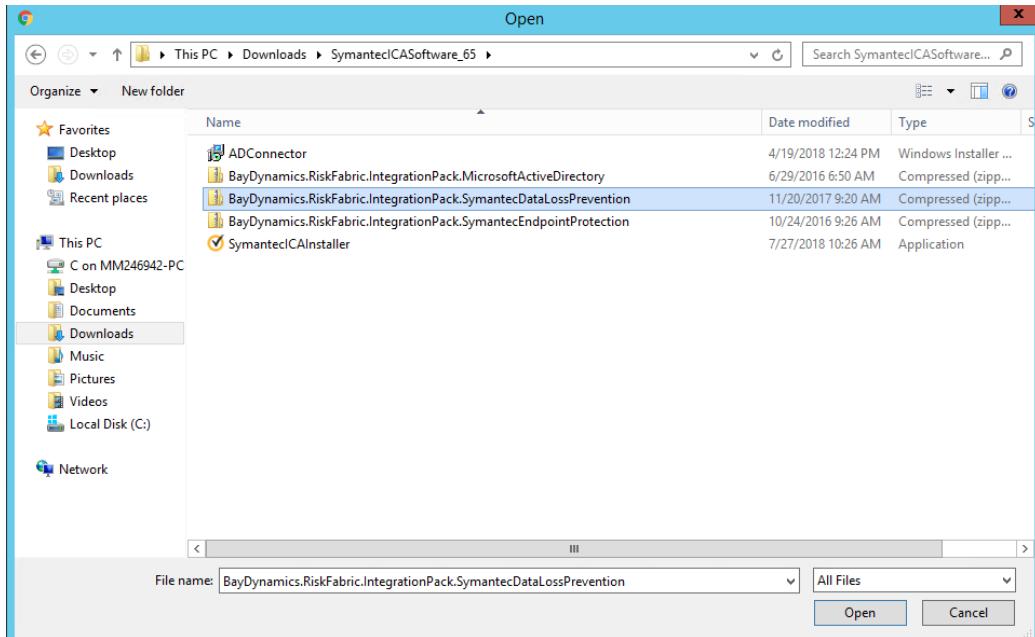
- 2410 1. Download the relevant integration packs to someone on the local system. These are typically
 2411 provided by Symantec, in a zip file. The zip file should be titled in the format of
`BayDynamics.RiskFabric.IntegrationPack.<productName>`.
- 2412 2. Log in to the Risk Fabric web interface.
-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



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

2418
2419

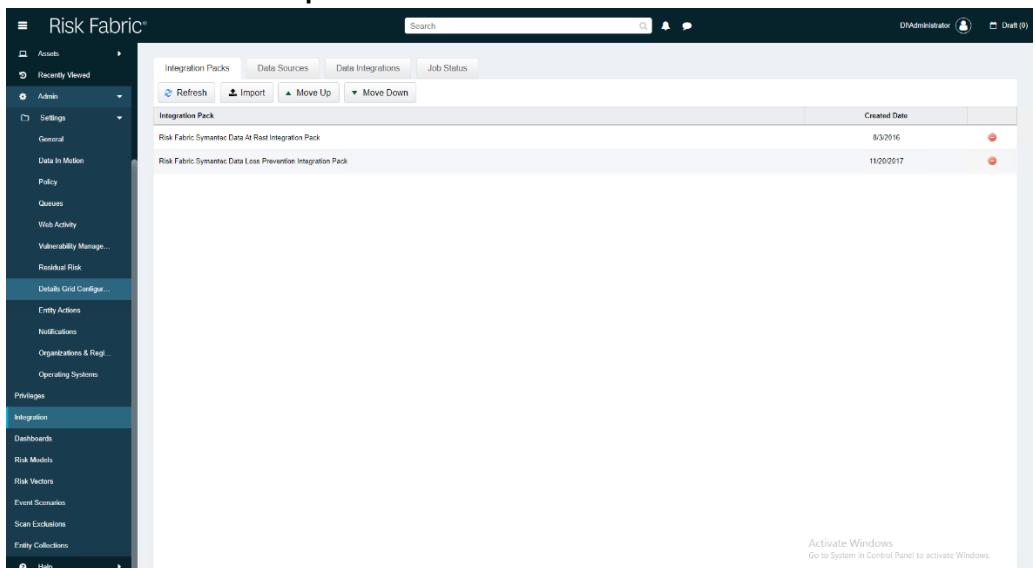
6. Select the file and click Open.

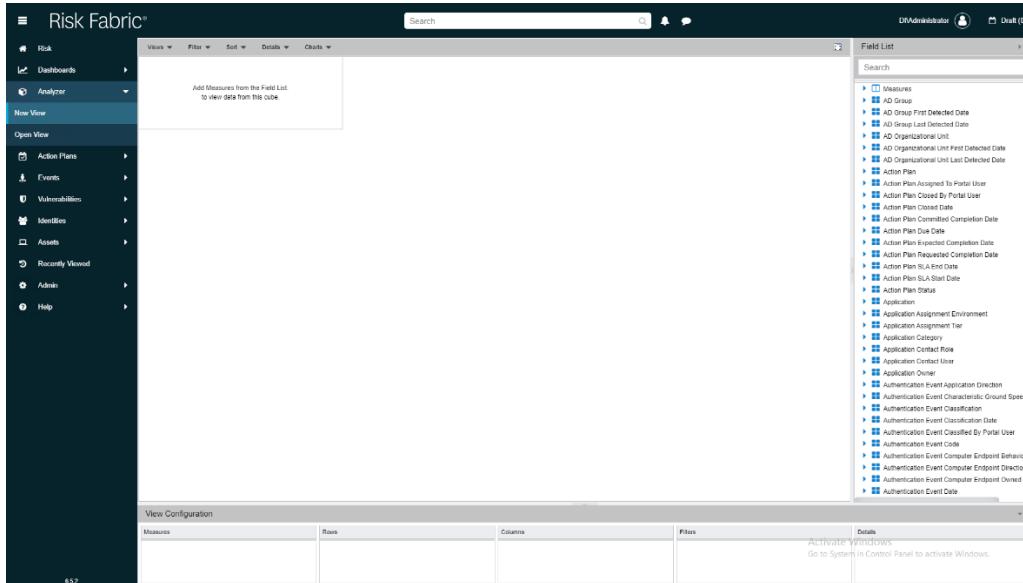


2420

2.15.4.2 Create a View

1. Navigate to Analyzer > New View.





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

Save View

Create new View Overwrite existing View

View Name:

Type:

Existing View Name:

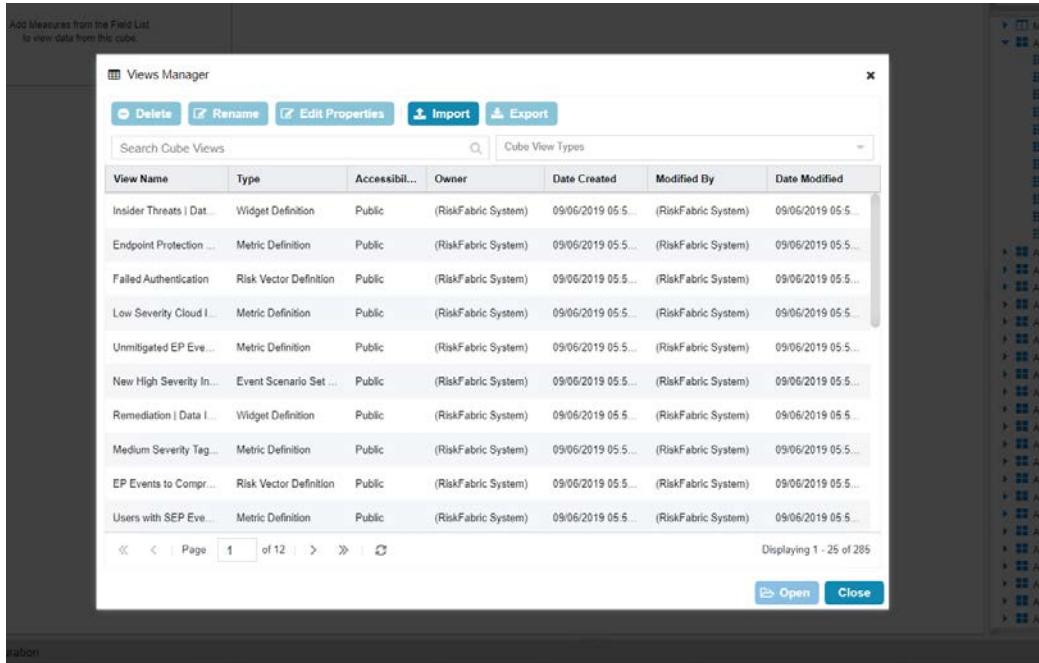
This view is accessible by all Users (Public)

Save **Cancel**

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

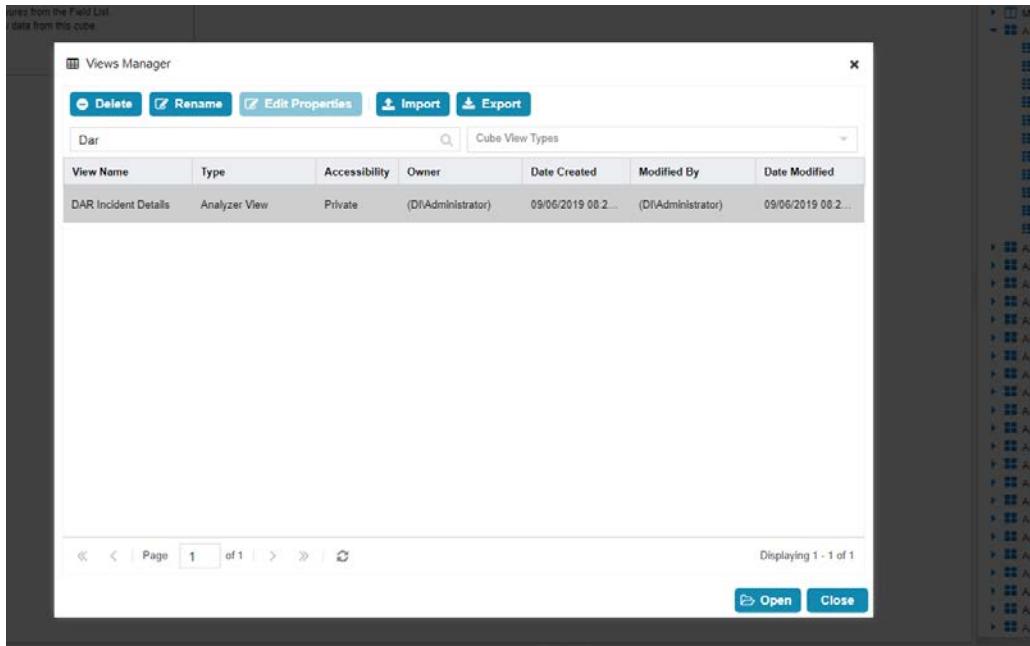
2.15.4.3 Open an Existing View

- 2435 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.

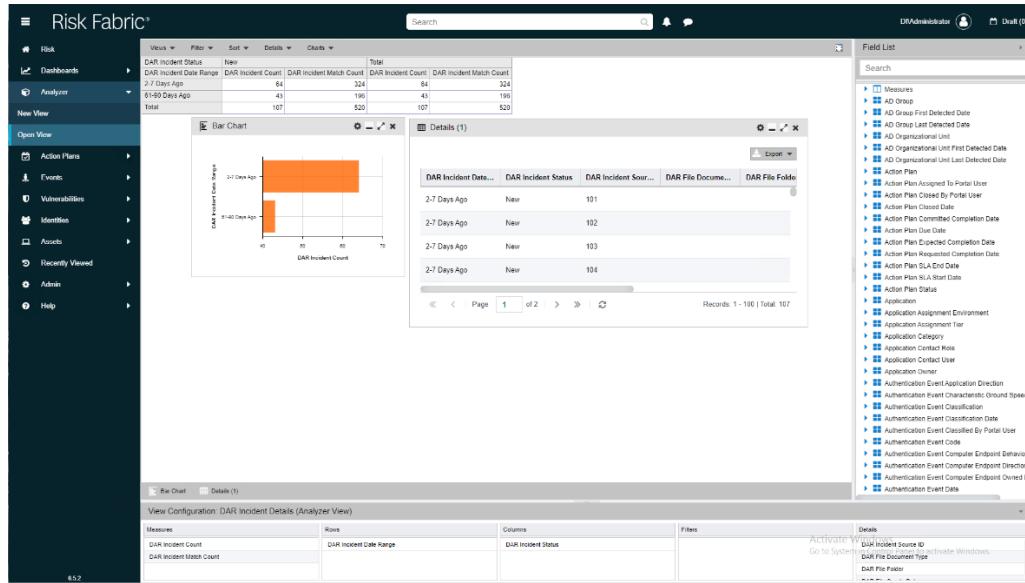


2442
2443

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** button in the details tab.
- 2446



- 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
- 2451 4. The entire view format can be exported as a .json file from the **Open View** option.

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

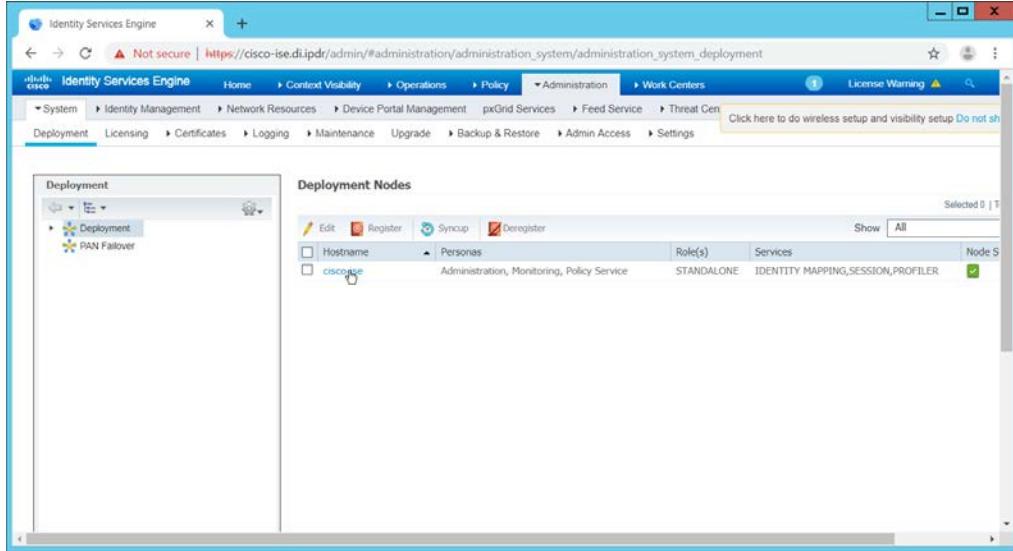
2457 details and other potential uses of the integration.

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**.

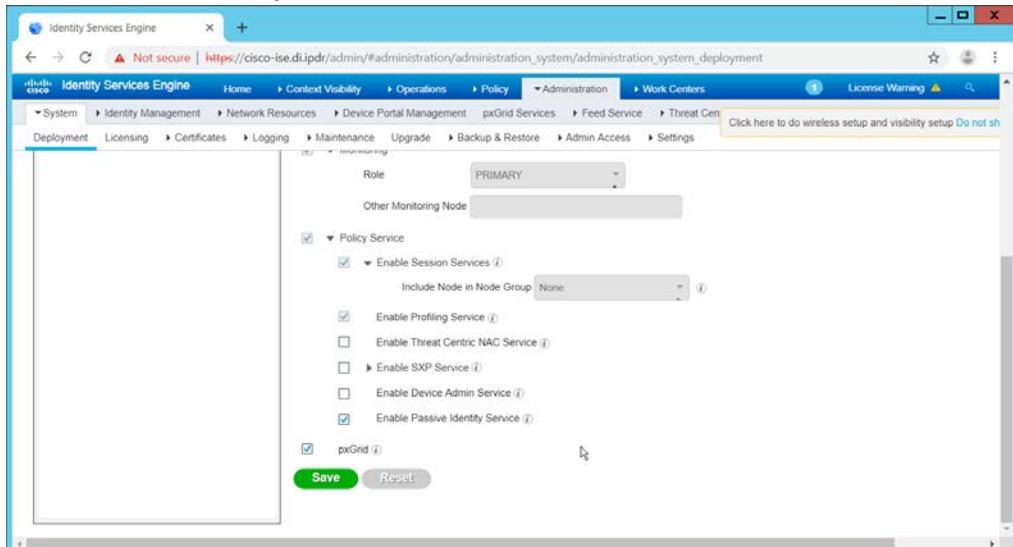
2461
2462
2463

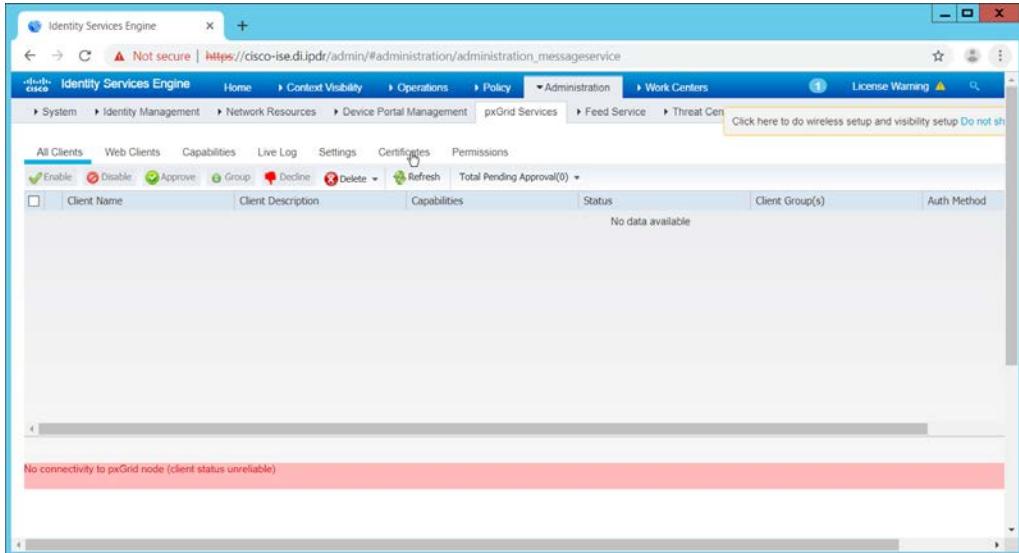
3. Click the hostname of the Cisco ISE machine.
4. Check the box next to **pxGrid**.



2464
2465
2466

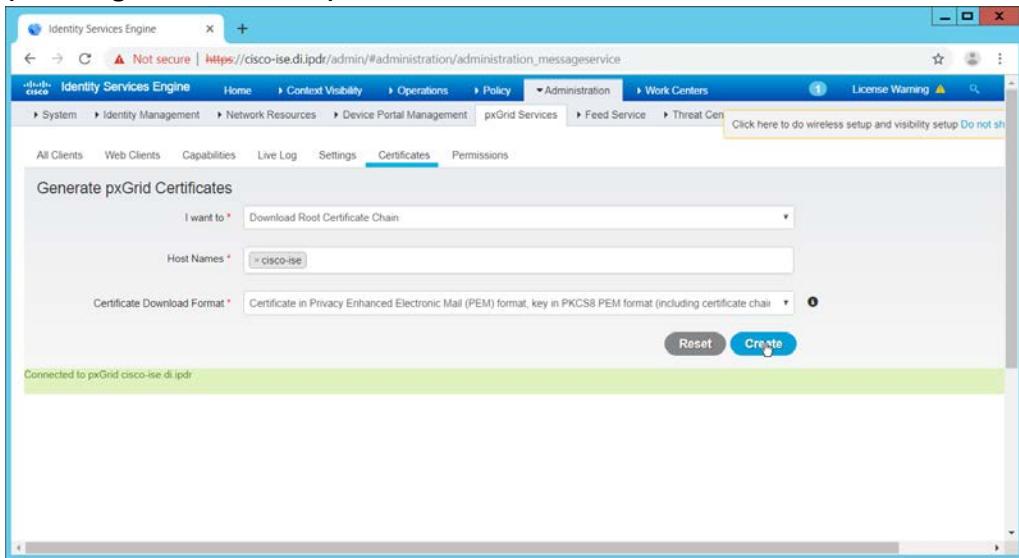
5. Click **Save**.
6. Navigate to **Administration > pxGrid Services**.





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

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

The screenshot shows a web browser window for the Identity Services Engine. The title bar says "Not secure | https://192.168.1.52/ic-landing-page/smci.html#/dashboard". The main content area is titled "Stealthwatch" and "Security Insight Dashboard | Inside Hosts". At the top right, there is a gear icon with a dropdown menu. The menu is titled "Desktop Client" and includes options: Global Settings, Central Management (which is highlighted with a yellow background), Packet Analyzer Configuration, UDP Director Configuration, and External Lookup Configuration. Below the gear icon, there is a section for "Alarming Hosts" with various metrics like Concern Index, Target Index, Recon, C&C, Exploitation, DDoS Source, DDoS Target, Data Hoarding, Exfiltration, and P2P User Management, all showing values of 0. There are also sections for "Top Alarming Hosts" (No data to display) and "Alarms by Type" and "Today's Alarms" (both also show No data to display).

2480
2481
2482

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

The screenshot shows a web browser window for the Identity Services Engine. The title bar says "Not secure | https://192.168.1.52/central-mgmt/#/inventory". The main content area is titled "Stealthwatch Central Management" and has tabs for "Appliance Manager", "Update Manager", and "App Manager". The "Appliance Manager" tab is selected. It displays a table titled "4 Appliances found" with the following data:

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	60 Days or Less	smc-01	SMC SMCI-VE-VMware- 4232d8dbe1b32e14- e610621f42a1f570	192.168.1.52	
Up	90 Days or Less	fcnf-01	Flow Collector FCNF-VE-VMware- 4232d8f162c01ea4- f1b1edb64da9166b	192.168.1.54	
Up	90 Days or Less	fr-01	UDP Director UDVE-VMware- 4232cfa73db93cb3- 472570289794deaa	192.168.1.55	
Up	90 Days or Less	fsae-01	Flow Sensor FSVE-VMware-	192.168.1.53	

4 Appliances found

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE
Up	60 Days or Less	smc-01	SMC SMCvE-VMware- 423208be1b32e14- e910b21f42a1f570
Up	90 Days or Less	fcnf-01	Flow Collector FCNvE-VMware- 42320bf162c01ea4- 7fb1edb64da9166b
Up	90 Days or Less	fr-01	UDP Director UDvE-VMware- 4232cfa73d093cb3- 472570289f7a4de8
Up	90 Days or Less	fsae-01	Flow Sensor FSvE-VMware-

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.

Appliance Configuration - SMC
smc-01 (192.168.1.52) / Last Updated: 06/27/2019 8:34 AM by admin

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
ota0ndfywl2m2e wzjhmnixkotdmzd mzjm/m5ntrknza... tq2ywmxzdc1ngu 5mtcnja0ymeznjl wodvmndhhyw== cert	smc-01.di.ipdr	smc-01.di.ipdr	2019-06-25 07:50:35	2024-06-25 07:50:35	64c2d2753702e5 538e85593013b1 28332c2b41e8	8192 bits	Delete
fr-01.di.ipdr	fr-01.di.ipdr	fr-01.di.ipdr	2019-06-18 05:51:57	2024-06-18 05:51:57	633aa308a37cba2 3e511c486d1f2c9 8b6e1b93bd	8192 bits	Delete

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.**

Appliance Configuration - SMC

smc-01 (192.168.1.52) / Last Updated: 06/27/2019 8:34 AM by admin

General

Trust Store

Add New

FRIENDLY NAME *: CiscoISE

CERTIFICATE FILE *: cisco-ise.di.ipdr_cisco-ise.di.ipdr.cer

Choose File

Add Certificate

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMB...	KEY LENGTH	ACTIONS
nt0001@fsae-01.d...	nt0001@fsae-01.d...	nt0001@fsae-01.d...	2010-06-26	2024-06-26	e5f8f969219	8192 bits	Delete

2494
2495**24. Click Apply Settings.**

Appliance Configuration - SMC

smc-01 (192.168.1.52) / Last Updated: 06/27/2019 8:34 AM by admin

General

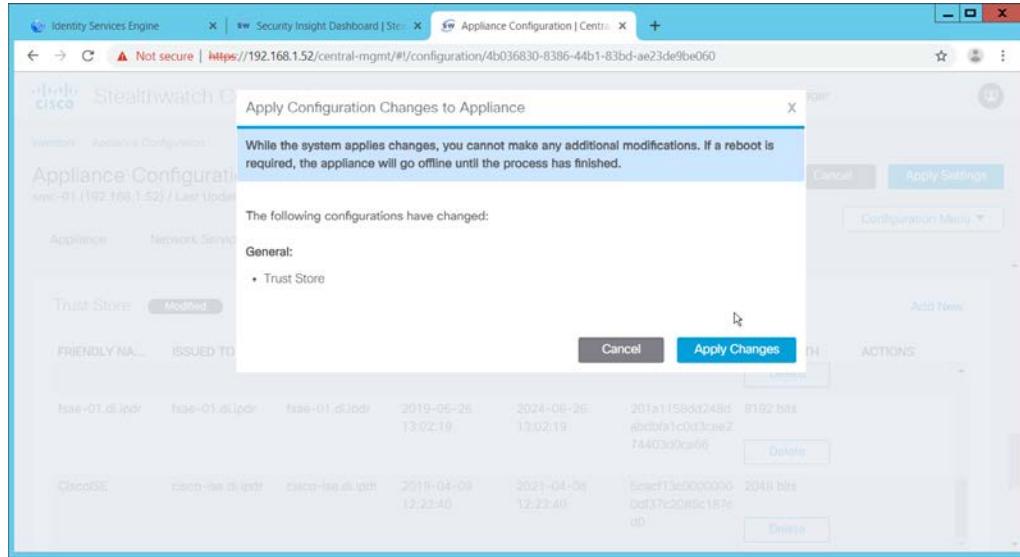
Trust Store

Modified

Add New

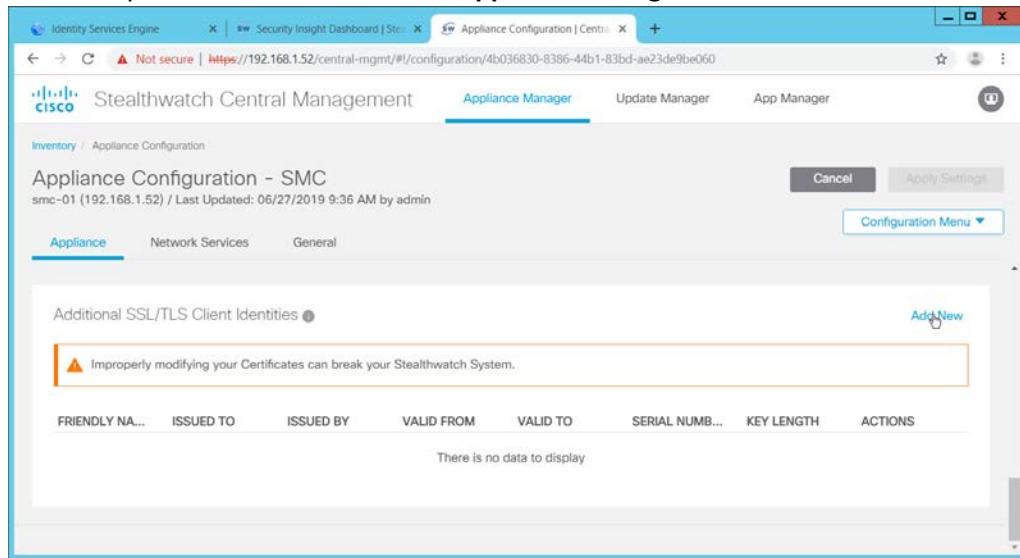
FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
fsae-01.di.ipdr	fsae-01.di.ipdr	fsae-01.di.ipdr	2019-06-26 13:02:19	2024-06-26 13:02:19	201a1158dd248d abdbfa1c0d3cee2 74403d0ca66	8192 bits	Delete
CiscoISE	cisco-ise.di.ipdr	cisco-ise.di.ipdr	2019-04-09 12:23:40	2021-04-08 12:23:40	5cadf13c0000000 0df37c2085c187c d0	2048 bits	Delete

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 **ellipsis 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.**

Appliance Configuration - SMC

sw-smc (192.168.1.150) / Last Updated: 08/08/2019 6:55 AM by admin

Appliance Network Services General

Generate a CSR

RSA KEY LENGTH * 2048 bits 4096 bits 8192 bits

COMMON NAME

ORGANIZATION

LOCALITY OR CITY

COUNTRY CODE

ORGANIZATIONAL UNIT

STATE OR PROVINCE

EMAIL ADDRESS

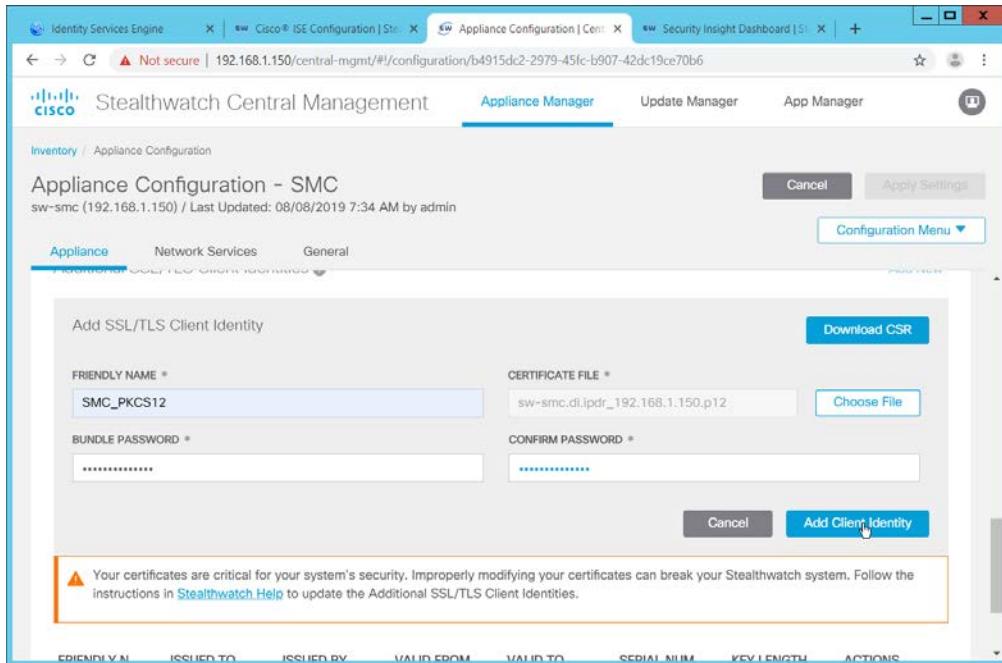
Cancel **Generate CSR**

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**.

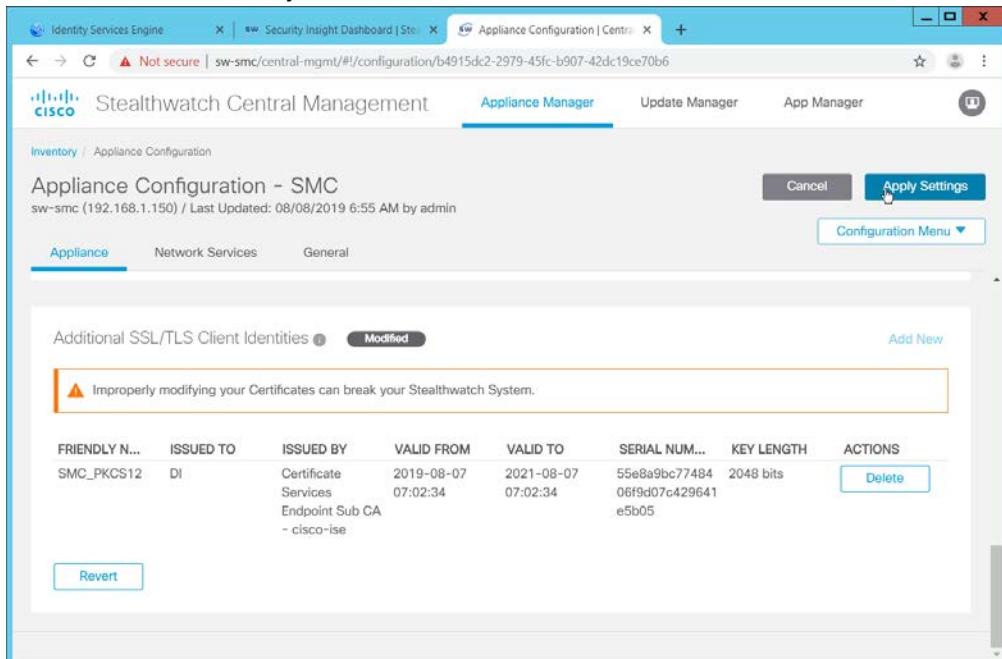
- 2513 36. Select **Generate a single certificate (with certificate signing request)** for I want to.
 2514 37. Paste the copied text into the **Certificate Signing Request Details**.
 2515 38. Enter a description such as **SMC** for the **Description**.
 2516 39. Select **IP Address** for **Subject 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 key)** for **Certificate Download Format**.
 2519
 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 Identities** (where you downloaded the CSR), click **Choose File**.
 2524 46. Upload the certificate file from the zip file that has the hostname of the SMC in it; the file extension should be **.p12**.
 2525
 2526 47. Enter a name for **Friendly Name**.
 2527
 2528 48. Enter the password used in ISE when generating the certificate.



2530
2531

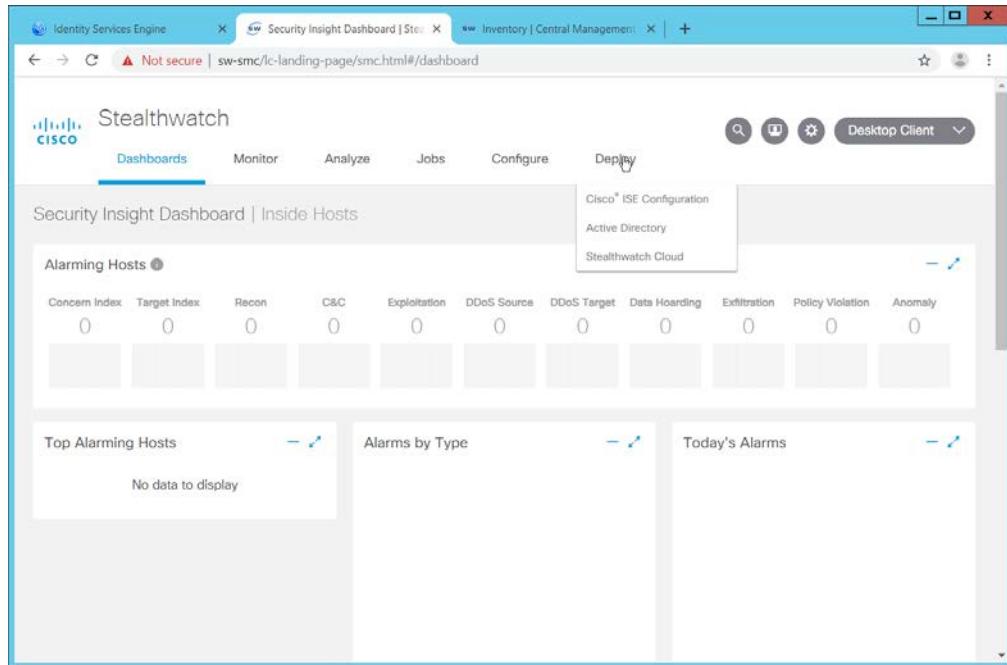
49. Click Add Client Identity.



2532
2533
2534

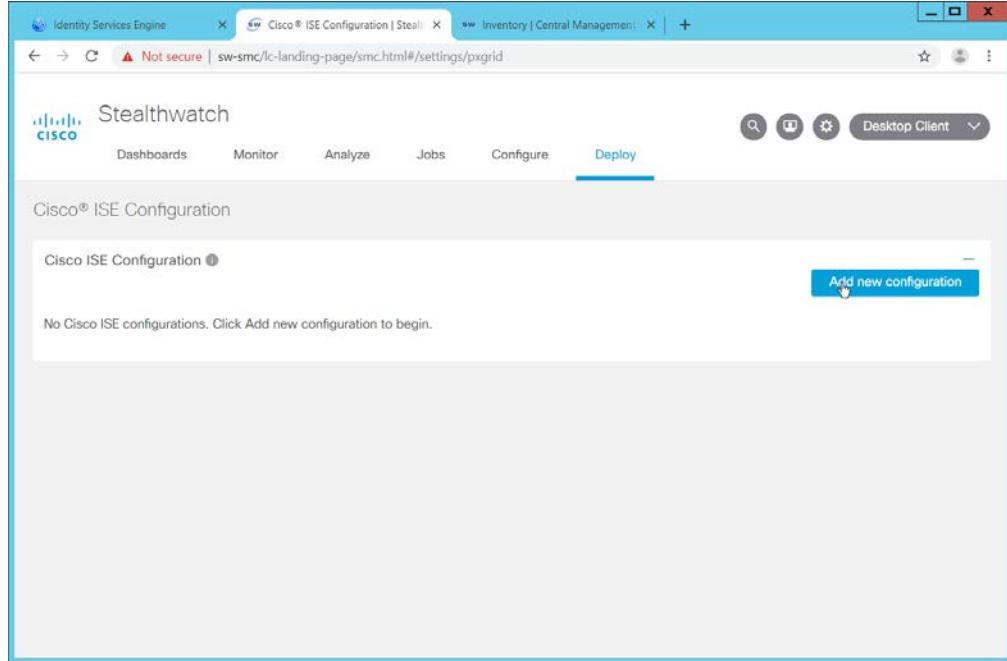
50. Click Apply Settings.

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.

Cisco ISE Configuration Setup

CLUSTER NAME: cisco-ise

CERTIFICATE: SMC_PKCS12

PRIMARY PXGRID NODE: 192.168.1.61

SECONDARY PXGRID NODE: ex. 10.10.10.10

USER NAME: SMC

Integration options:

- Adaptive Network Control
- Static SGT Classifications
- User sessions

Save

2543

2544

2545

58. Click **Save**.

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

	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth
<input type="checkbox"/>	ise-fanout-cisco-ise		Capabilties(0 Pub, 0 Sub)	Online (XMPP)	Internal	Cert
<input type="checkbox"/>	ise-admin-cisco-ise		Capabilties(4 Pub, 2 Sub)	Online (XMPP)	Internal	Cert
<input type="checkbox"/>	ise-pubsub-cisco-ise		Capabilties(0 Pub, 0 Sub)	Online (XMPP)	Internal	Cert
<input type="checkbox"/>	ise-bridge-cisco-ise		Capabilties(0 Pub, 4 Sub)	Online (XMPP)	Internal	Cert
<input type="checkbox"/>	ise-mint-cisco-ise		Capabilties(2 Pub, 1 Sub)	Online (XMPP)	Internal	Cert
<input checked="" type="checkbox"/>	smc		Capabilties(0 Pub, 0 Sub)	Online (XMPP)		Cert

Connected to pxGrid cisco-ise.di.ipdr

2546

2547

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

The screenshot shows a web browser window with three tabs: 'Identity Services Engine', 'Cisco® ISE Configuration | Stealthwatch', and 'Inventory | Central Management'. The central tab displays the 'Stealthwatch' interface. At the top, there are navigation links: Dashboards, Monitor, Analyze, Jobs, Configure, Deploy, and a 'Desktop Client' dropdown. Below this is a search bar and a toolbar with icons for search, refresh, and settings. The main content area is titled 'Cisco® ISE Configuration' and contains a table with one row. The table columns are: Cluster Name, Primary pxGrid Node, Secondary pxGrid Node, User Name, Status, and Actions. The data row shows: 'cisco-ise', '192.168.1.61', ' ', 'SMC', 'Green status icon', and a blue 'Edit' button.

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

2.16.2 Configuring Stealthwatch to Quarantine through ISE

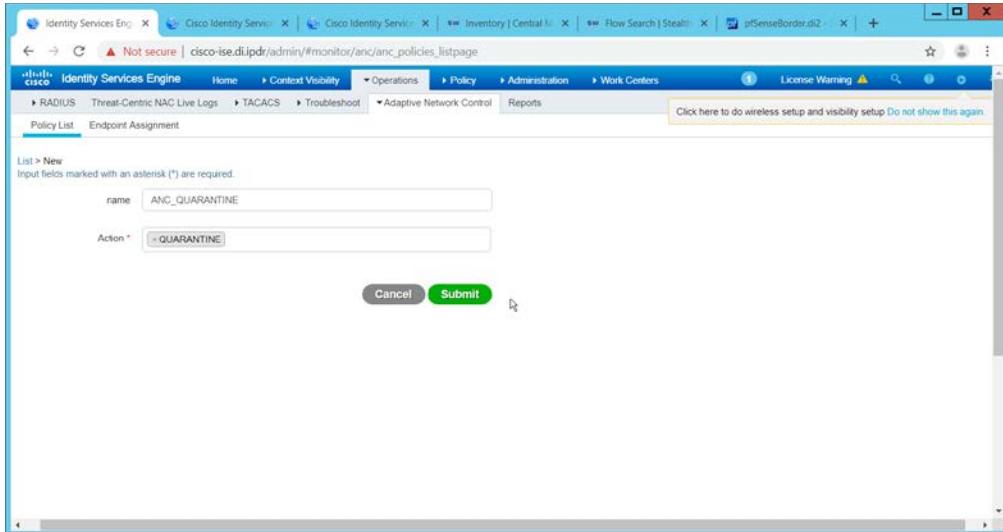
- 2551 1. Navigate to Operations > Adaptive Network Control > Policy List.

The screenshot shows a web browser window with multiple tabs: 'Identity Services Engine', 'Cisco Identity Services Engine', 'Cisco Identity Services Engine', 'Inventory | Central Management', 'Flow Search | Stealthwatch', and 'pfSenseBorder.d2'. The main content area is titled 'Policy List' under the 'Adaptive Network Control' section. It has a toolbar with 'Refresh', 'Add', 'Trash', and 'Edit' buttons. The table below has columns: 'Policy Name' and 'ANC Actions'. A message at the bottom says 'No data found.'

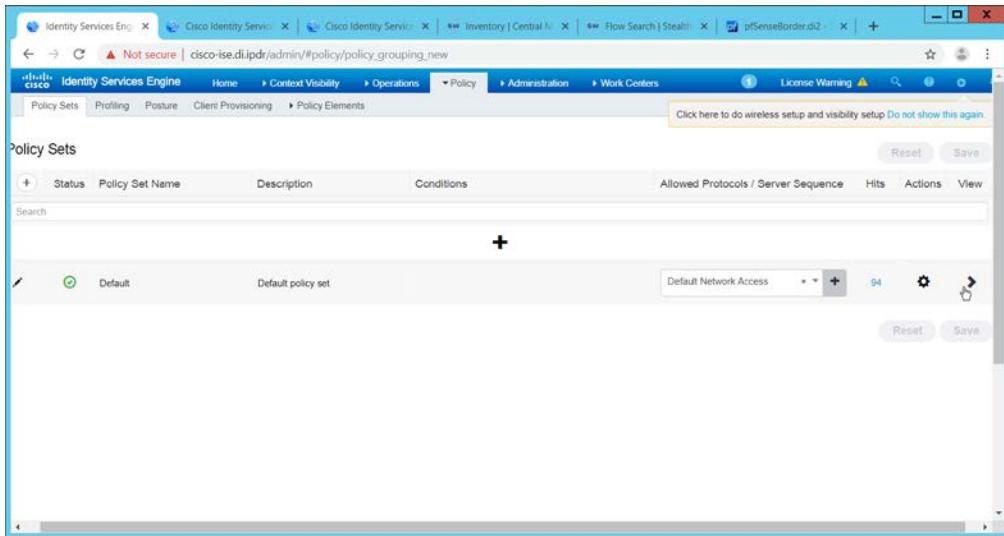
- 2553
2554 2. Click Add.
2555 3. Enter a name for a quarantine action.

2556
2557

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

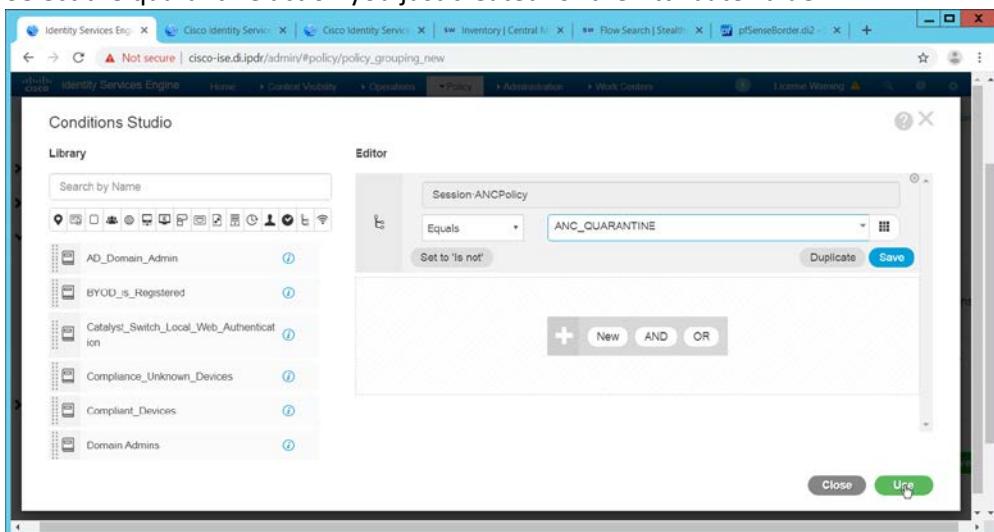
2558
2559
2560

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.

Host	Name	Group	Location	Count	Start	End
192.168.8.102	--	Catch All	RFC 1918	34	8/8/19 9:25 AM	★ Current

2580
2581
2582

20. Click **Edit** next to ISE ANC Policy.
21. From the drop down, select the quarantine action you created earlier.

Host Groups:	192.168.8.102
Location:	RFC 1918
First Seen:	--
Last Seen:	--
Policies:	Inside
MAC Address:	00:50:56:b2:8c:ad (VMware, Inc.)
ISE ANC Policy:	-- Edit

Top Security Events for 192.168.8.102

No events were found. If you are sure this result is incorrect, contact your Stealthwatch administrator.

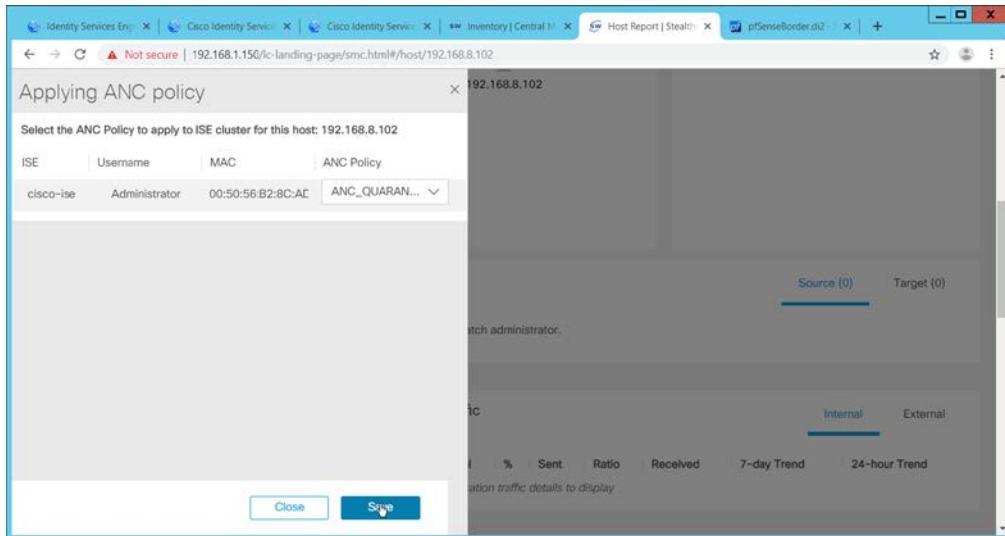
Source (0) Target (0)

Users & Sessions Application Traffic

MAC Address:	MAC Vendor:	Device Type:	Internal	External
00:50:56:b2:8c:ad	VMware, Inc.	Microsoft-Workstation		
User	Start	End		
Administrator	8/8/19 9:25 AM	★ Current		

Application Total % Sent Ratio Received 7-day Trend 24-hour Trend

There are no application traffic details to display



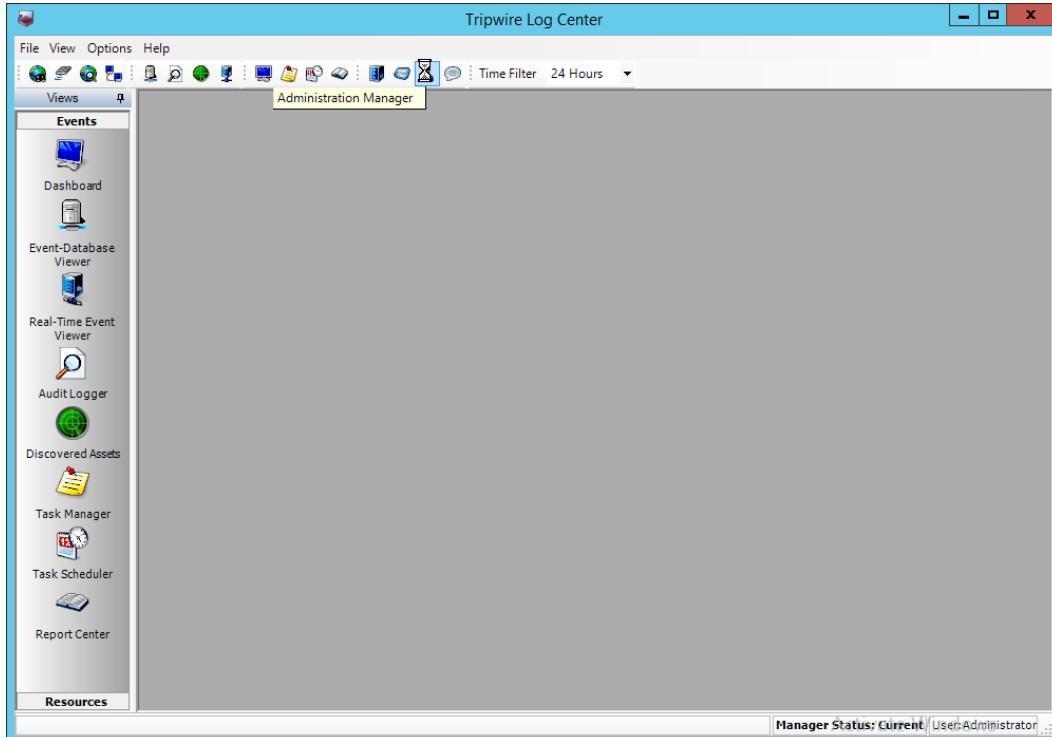
2583

2584 22. Click **Save**.

2585 23. This will apply the quarantine action to the machine.

2.17 Integration: Tripwire Log Center and Tripwire Enterprise

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

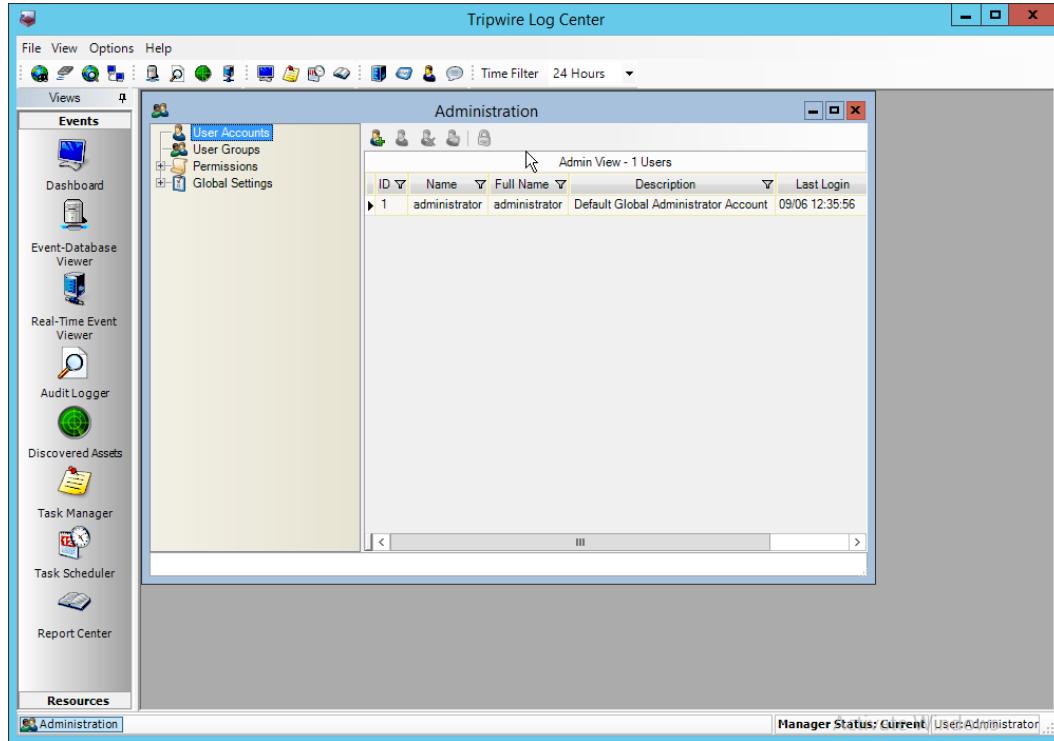


2588

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

2590

3. Click User Accounts.



2591

2592

4. Click the Add button.

2593

5. Enter the details of the user.

A screenshot of the "Add New User" dialog box. It has a "Username" field containing "tweuser" and a "Settings" tab. Under the Settings tab, there are fields for "Full name" (empty), "Description" (empty), and "Authentication method" set to "Tripwire Log Center". Below the settings are fields for "Password" and "Password Verify", both containing masked text. At the bottom are "Add" and "Cancel" buttons.

2594

2595

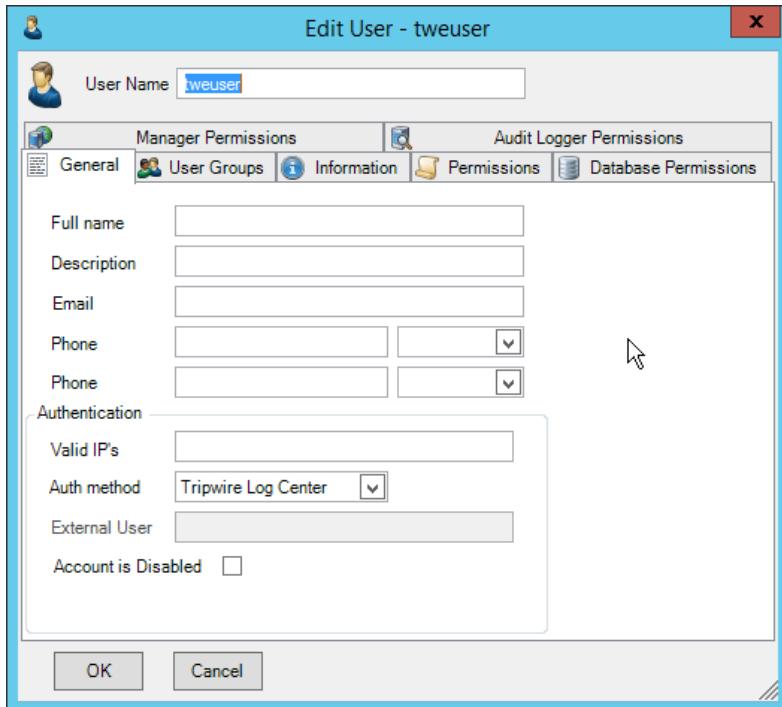
6. Click Add.

2596

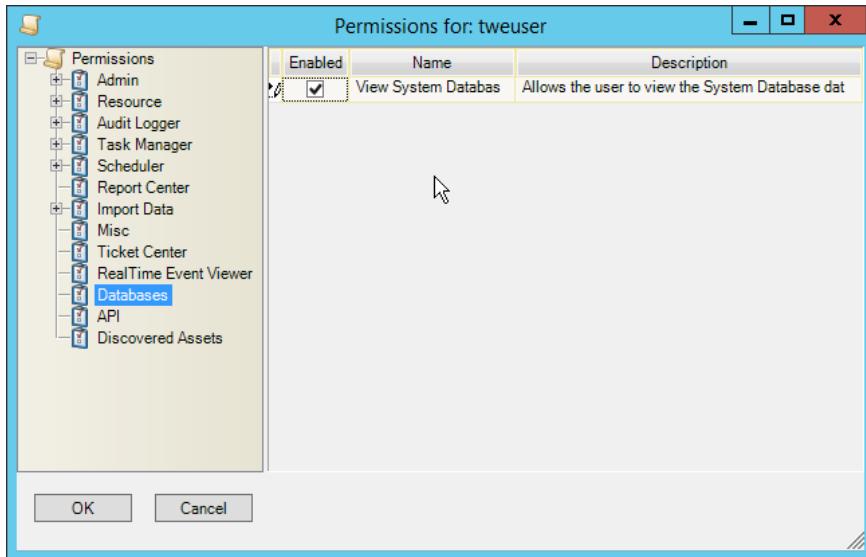
7. Double-click the user account.

2597
2598

8. Click the **Permissions** tab.

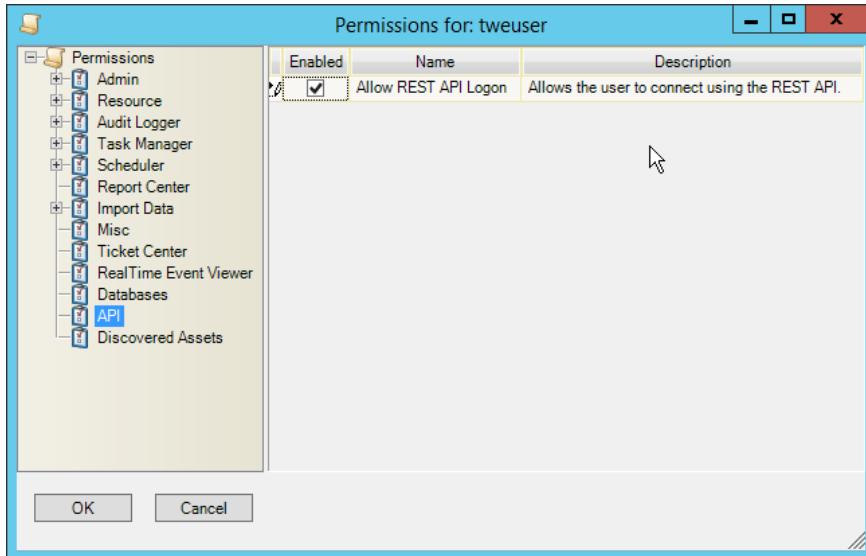
2599
2600
2601

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



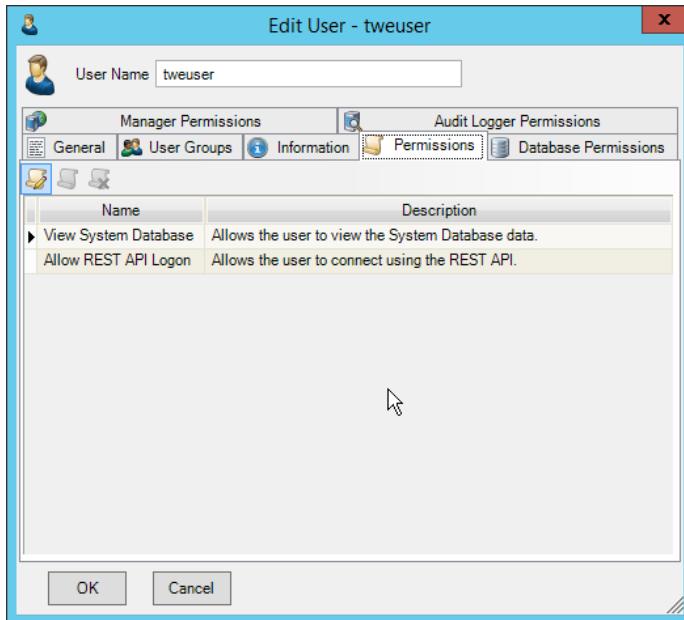
2602
2603
2604

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

14. Click **OK**.

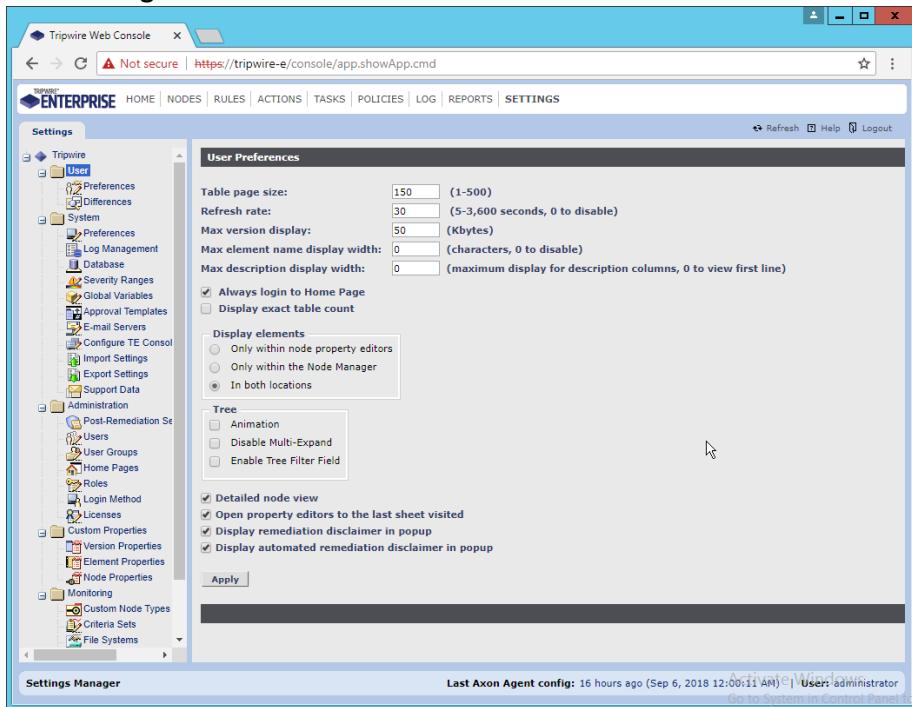
2608

15. Click **OK**.

2609

16. Log in to the **Tripwire Enterprise** web console.

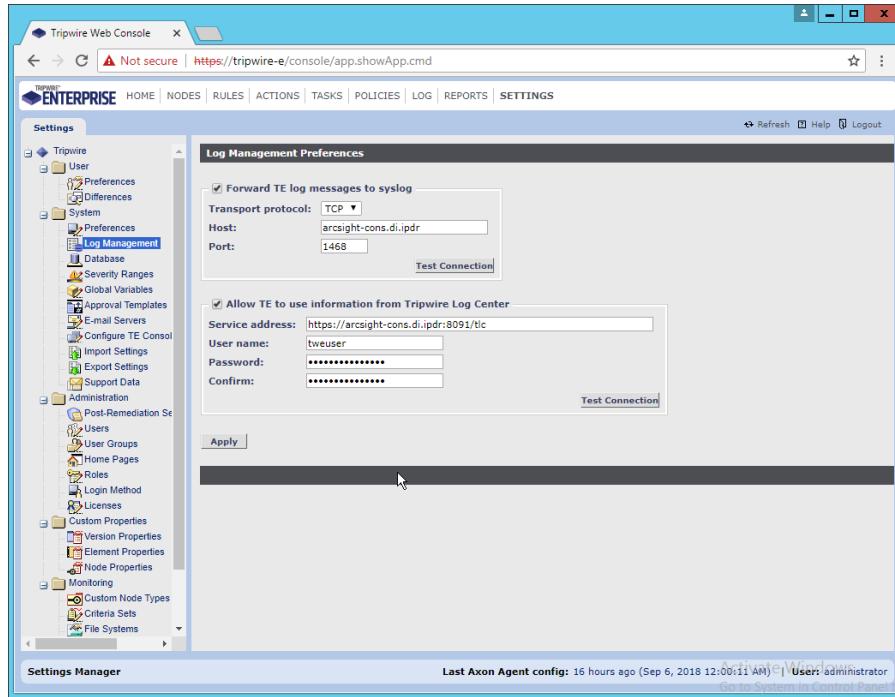
2610

17. Click **Settings**.

2611

18. Go to **System > Log Management**.

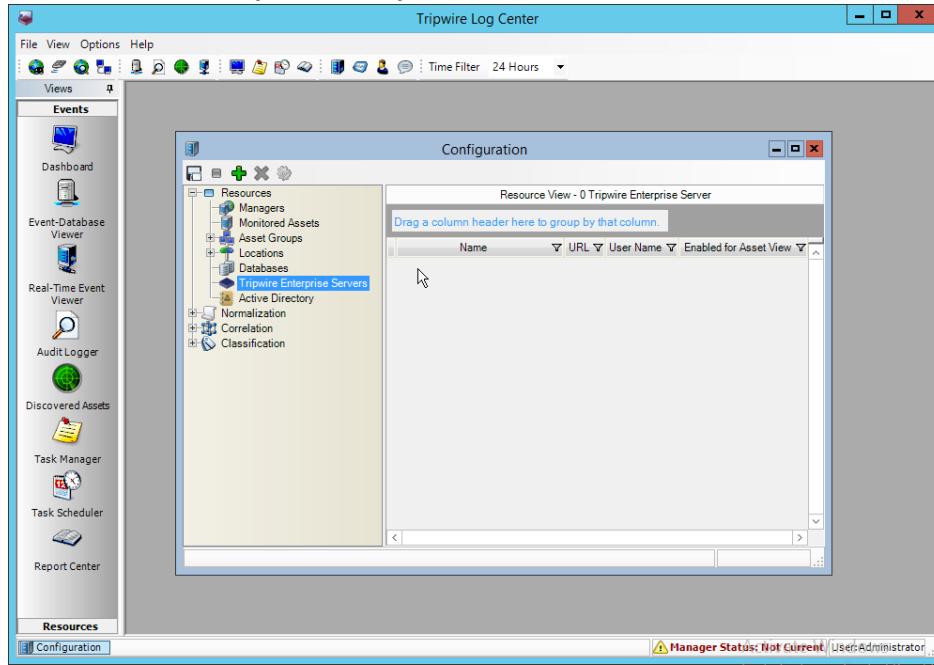
- 2614 19. Check the box next to **Forward TE log messages to syslog**.
 2615 20. Enter the **hostname** and **port** of the **Tripwire Log Center** server. The default port is **1468**.
 2616 21. Check the box next to **Allow TE to use information from Tripwire Log Center**.
 2617 22. Enter the **service 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**.

2624
2625
2626

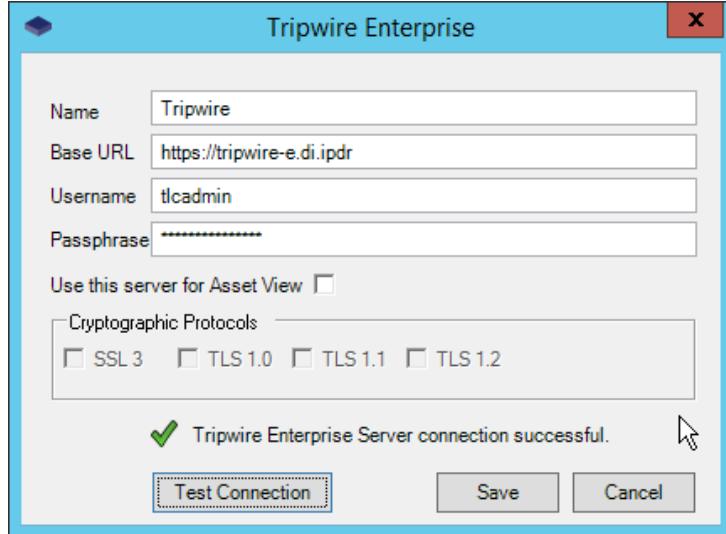
27. Click Configuration Manager.
28. Click Resources > Tripwire Enterprise Servers.



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 33. Click **Save**.

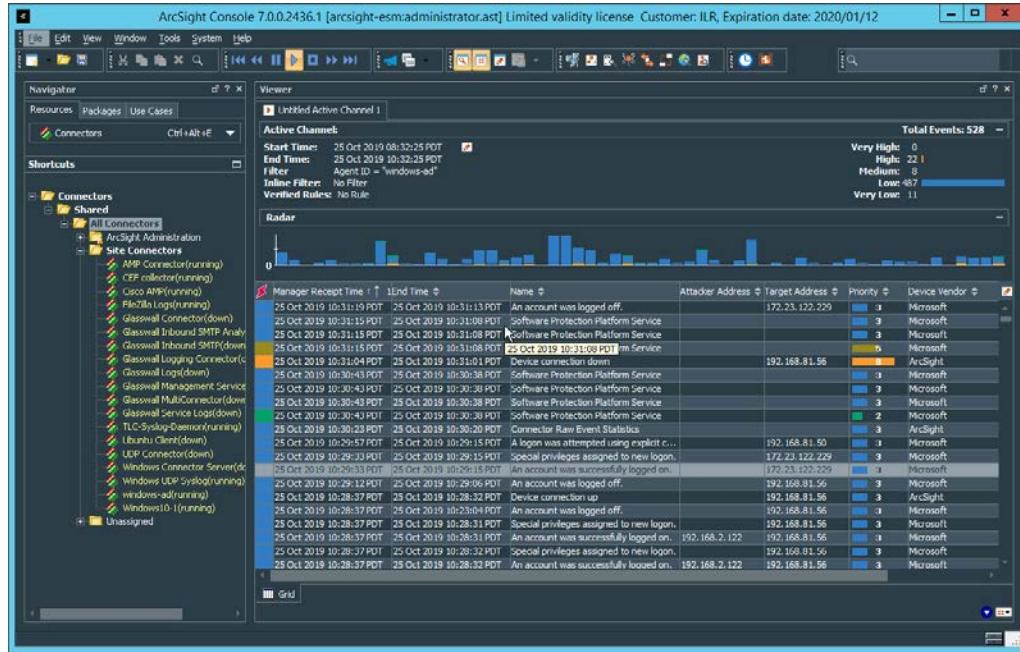
2.18 Integration: Symantec ICA and ArcSight ESM

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:

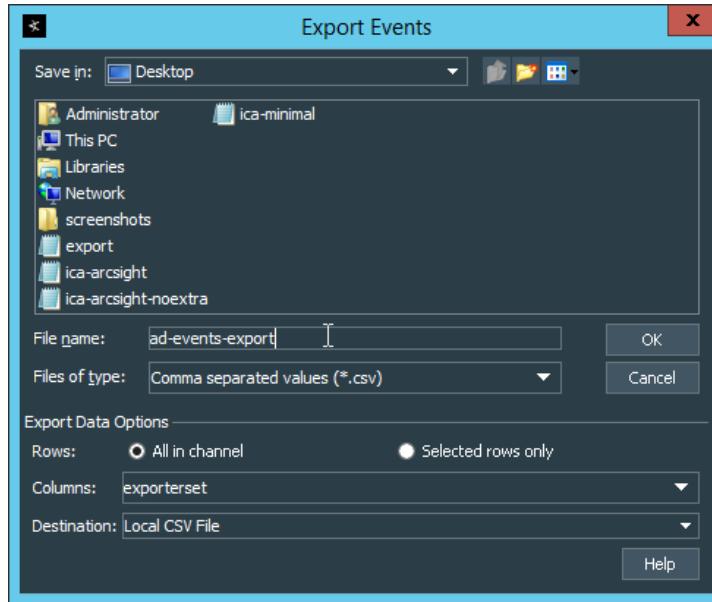
- 2641 • On the version of Symantec ICA we are using, it is required to replace empty fields in the CSV
 2642 with NULL. This may be unnecessary in future updates.
- 2643 • The CSV file should be in a location accessible to the ICA server. You can replace this file with a
 2644 new CSV file on a daily 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.

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

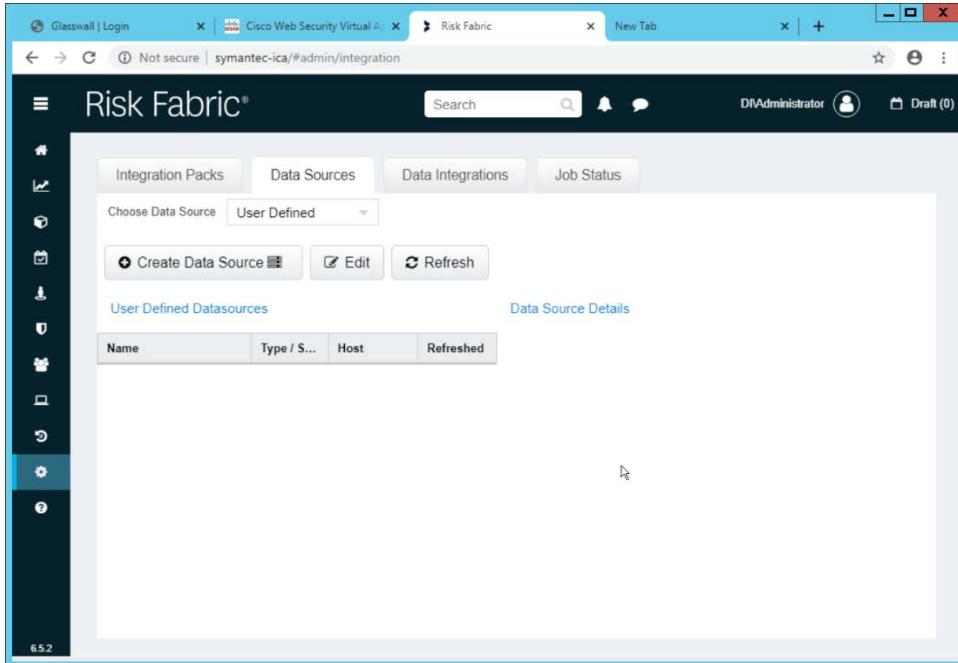


- 2658
 2659 7. Click **OK**.

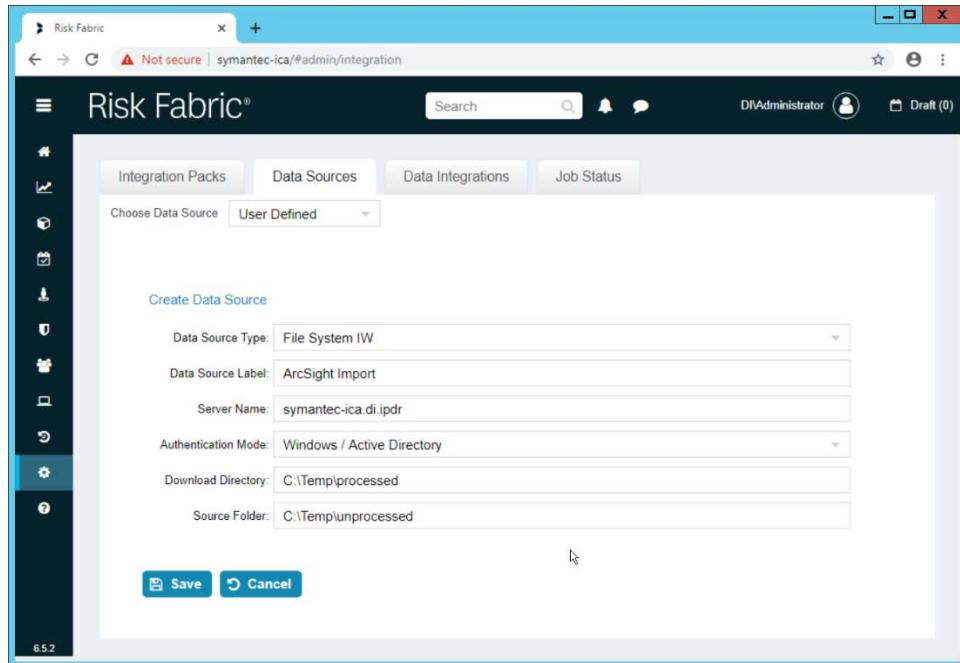
2660 8. Move the file to the desired location for ICA to collect. (Ensure that if required for your version
2661 of Symantec ICA, all empty fields are replaced with "NULL") For the purposes of this
2662 demonstration, we moved it to *C:\Temp\unprocessed* on the Symantec ICA server.

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.

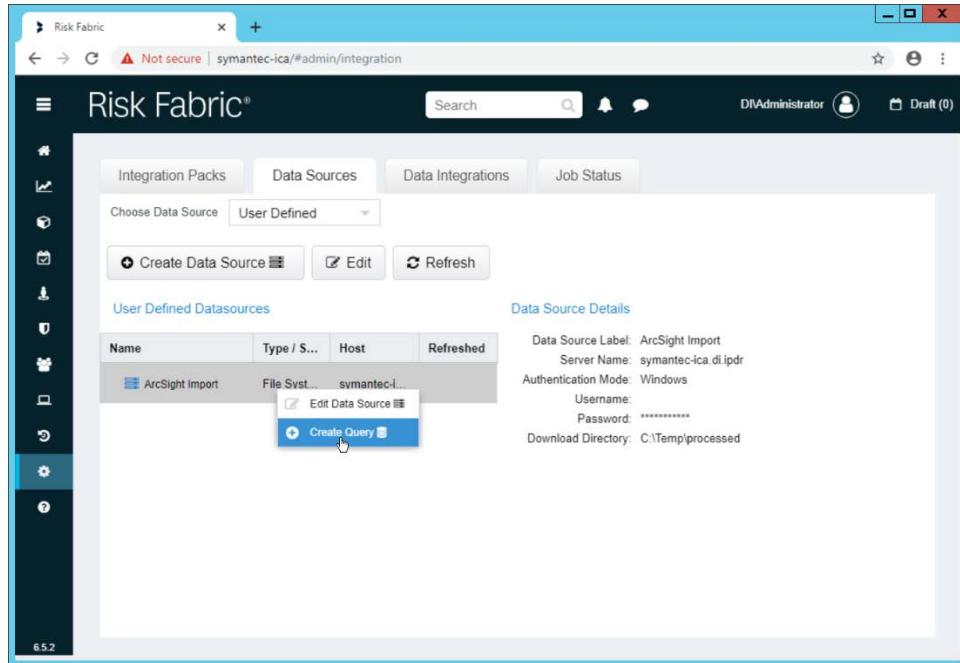


- 2666 3. Select **User Defined** for **Choose Data Source**.
2667 4. Click **Create Data Source**.
2668 5. Select **File System IW** for the **Data Source Type**.
2669 6. Enter a name for the data source for **Data Source Label**.
2670 7. Enter the hostname of the Symantec ICA server for **Server Name**.
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



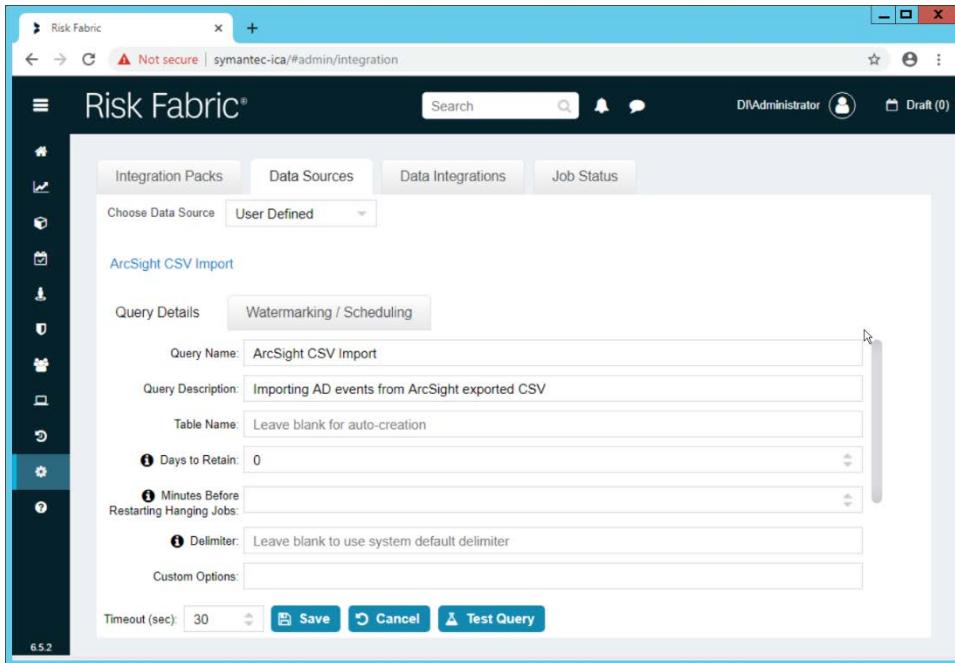
2677
2678

11. Click Save.



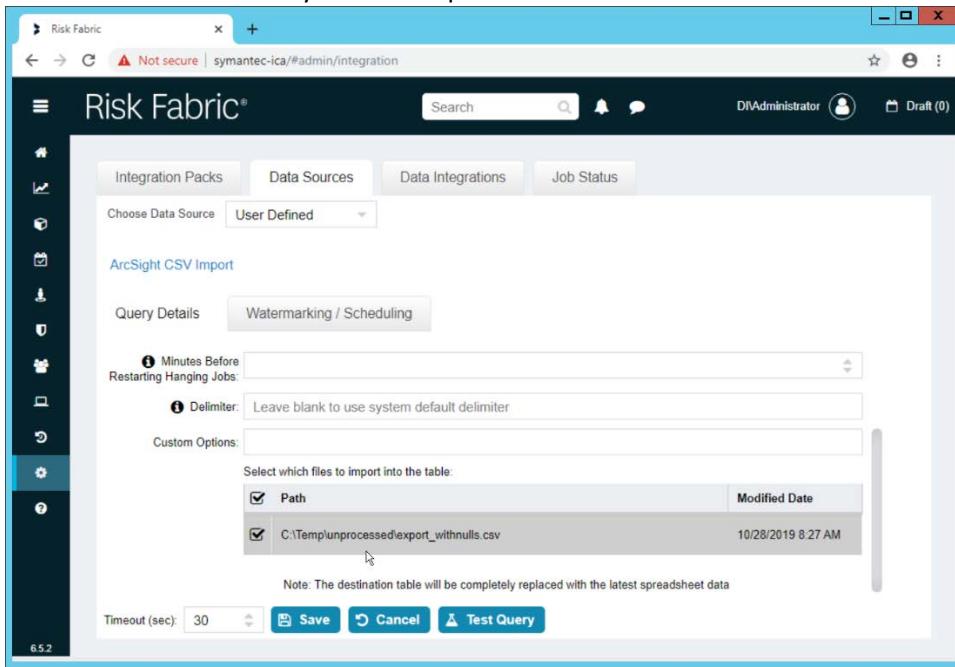
2679
2680
2681

12. Right-click the newly created data source and select **Create Query**.
13. Enter a **Query Name** and **Query Description**.



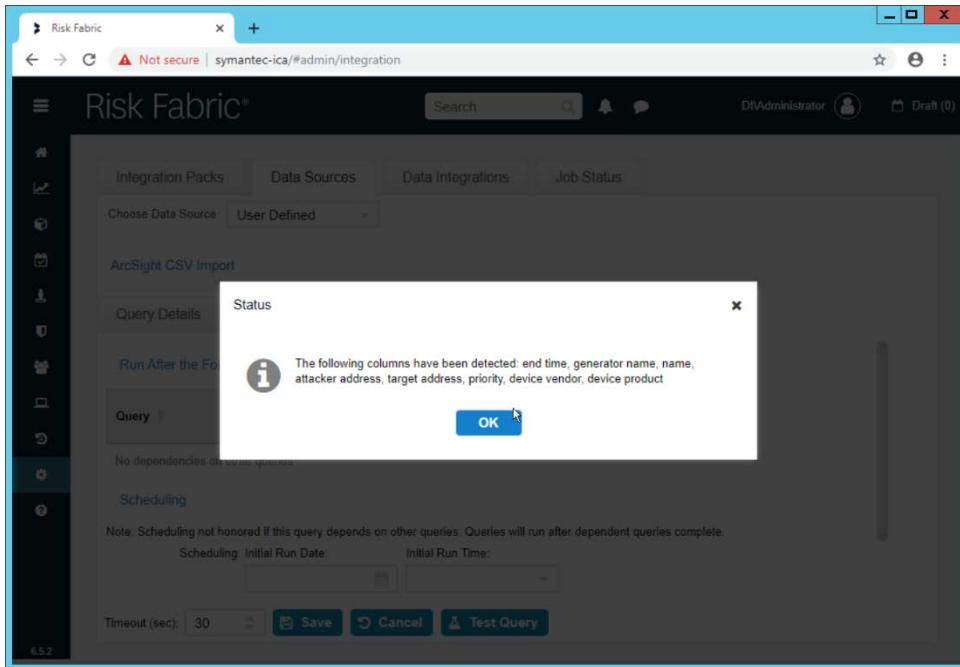
2682
2683
2684

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**.



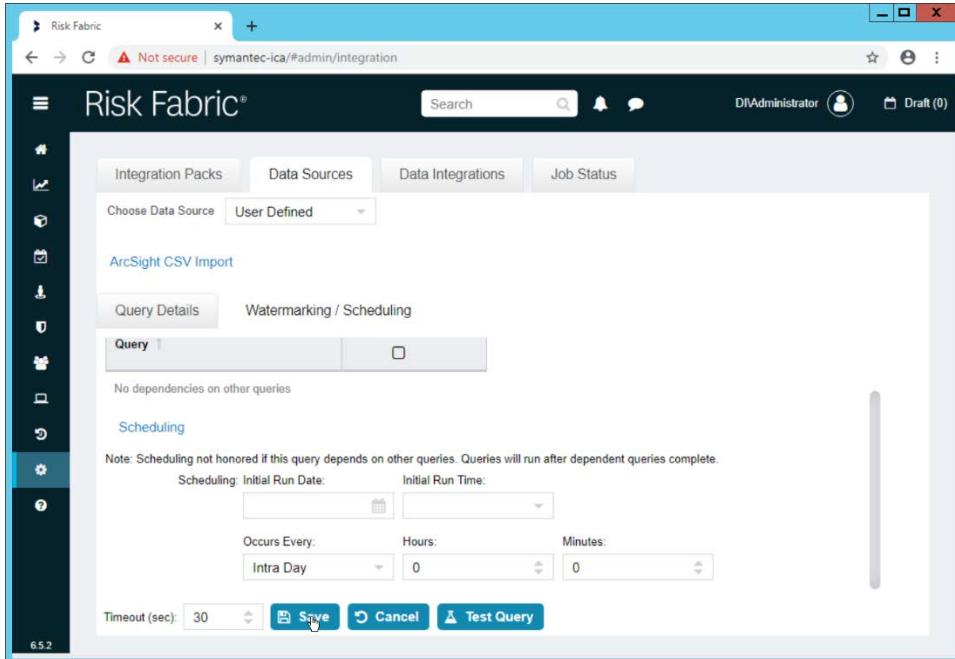
2687

2688

2689

17. Click OK.

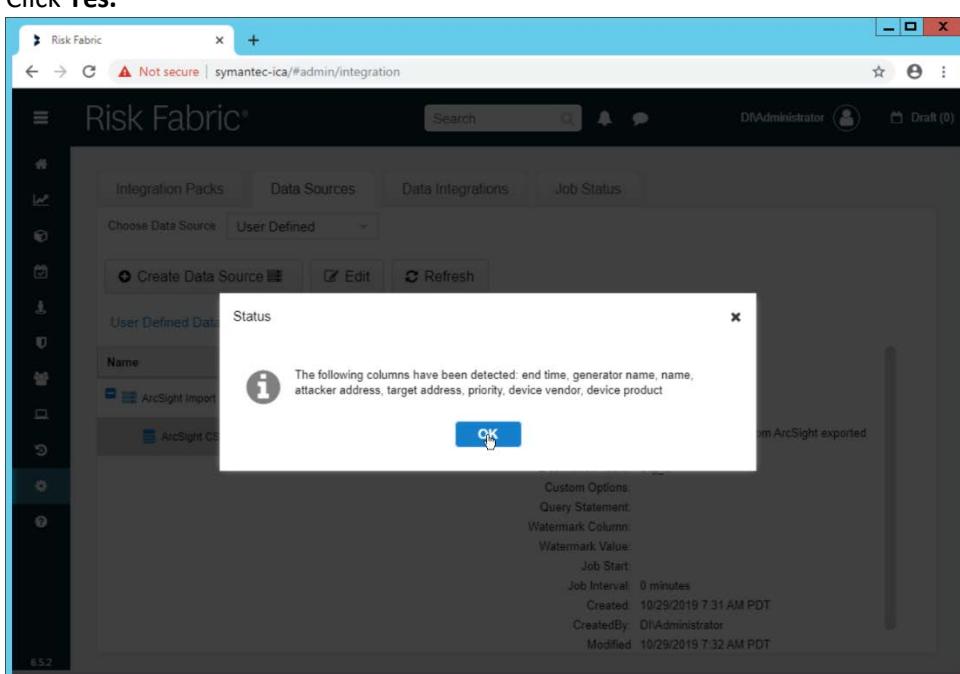
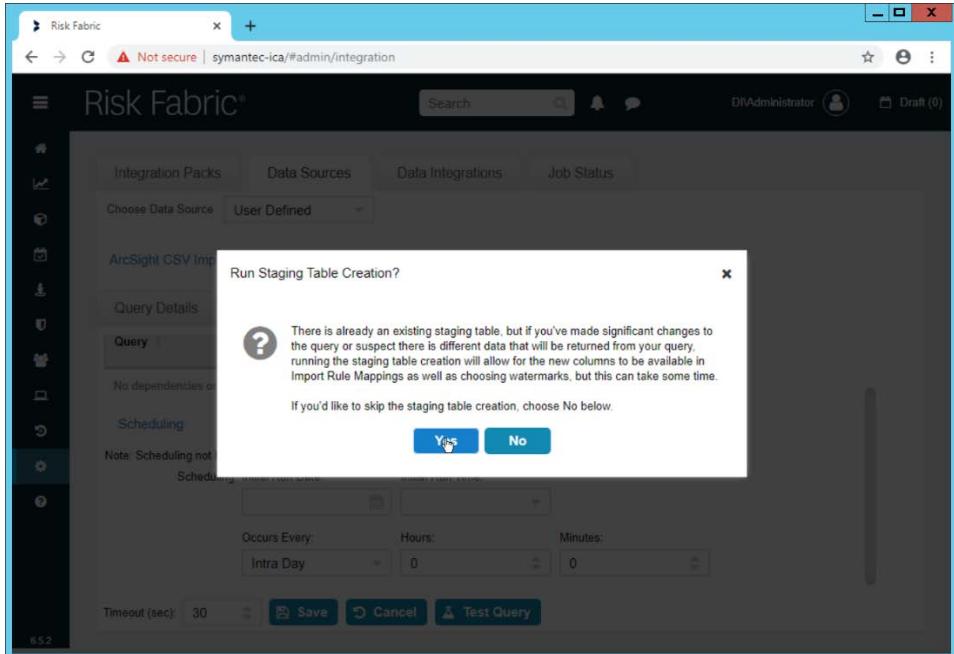
18. If desired, set a schedule for this import.



2690

2691

19. Click Save.

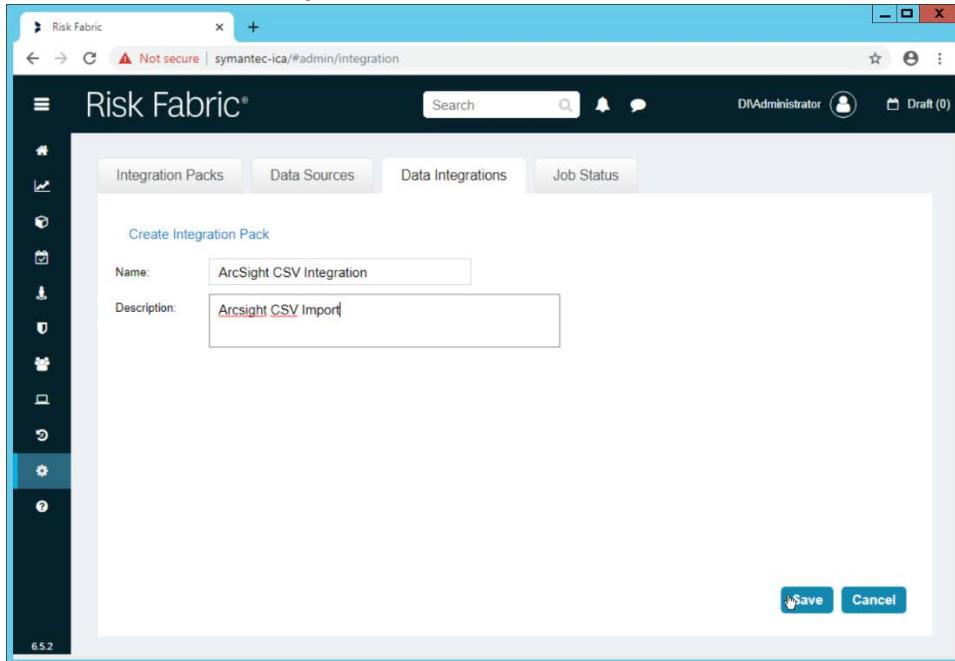


2.18.3 Create a Mapping between ArcSight events and Symantec ICA

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

2698
2699
2700

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

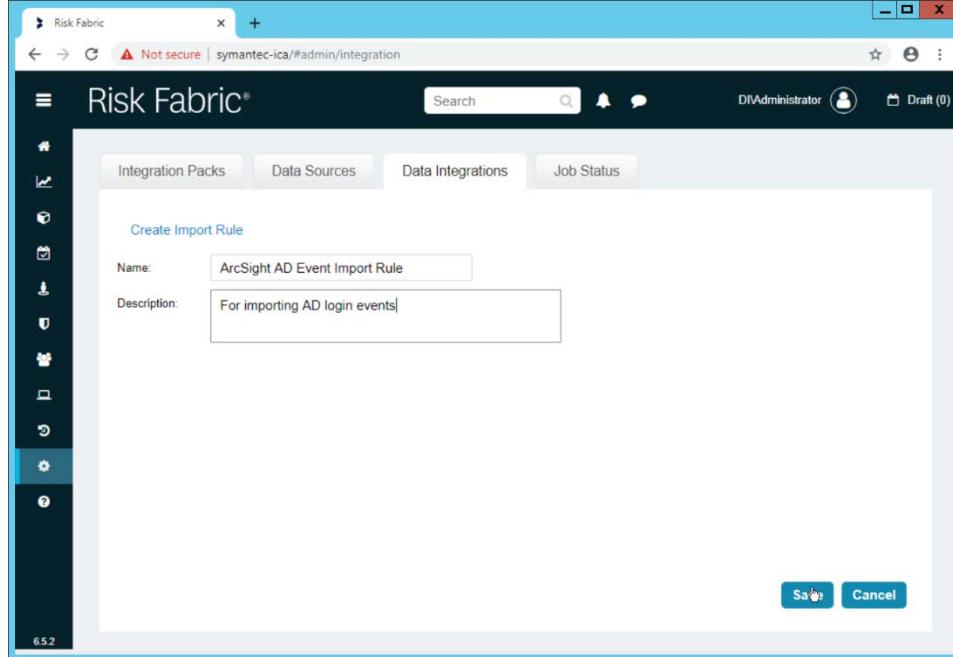


2701
2702

4. Click **Save**.

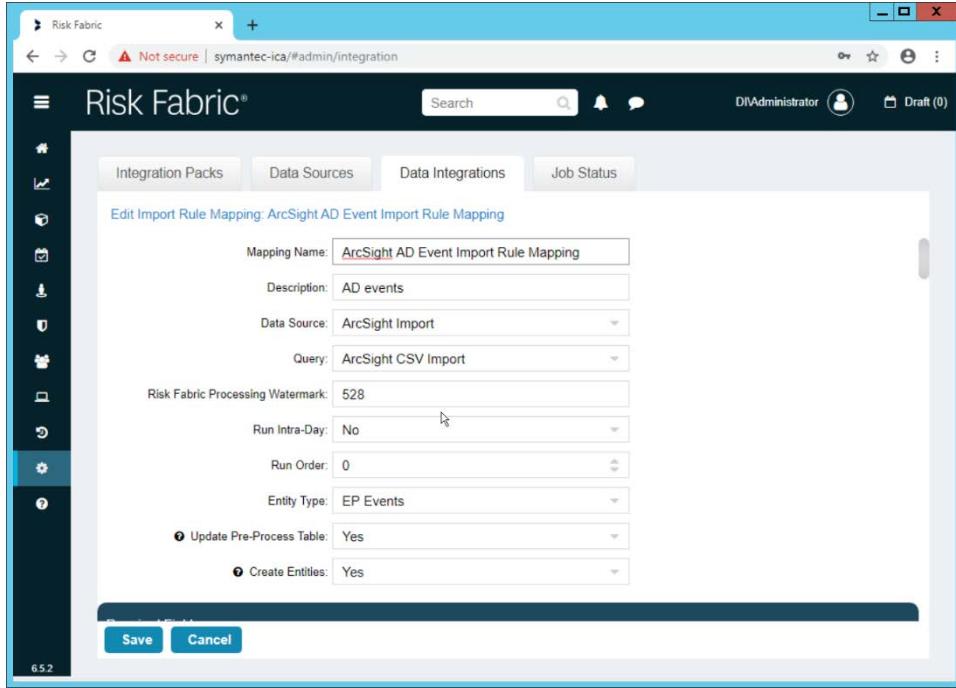
2703
2704
2705

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 events you are importing).



- 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 15. For example, **EventDate** in ICA corresponds directly to the **End Time** in ArcSight, so we select
2718 that value directly as a **Source Column** for the mapping.

Integration Packs Data Sources Data Integrations Job Status

Edit Import Rule Mapping: ArcSight AD Event Import Rule Mapping

Required Fields

Entity Column	Type	Value	Default Value
EventDate	datetime	Source Column	End Time
SourceEventID	nvarchar(50)	Formula	Convert unique \$

Optional Fields

Entity Column	Type	Value	Default Value
---------------	------	-------	---------------

Save Cancel

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.

Integration Packs Data Sources Data Integrations Job Status

Create Import Rule Mapping

EventObjectType	Source Column		
-----------------	---------------	--	--

Create and Associate Event Activity Type

Entity Column	Type	Value	Default Value
EventActivityType	Source Column		

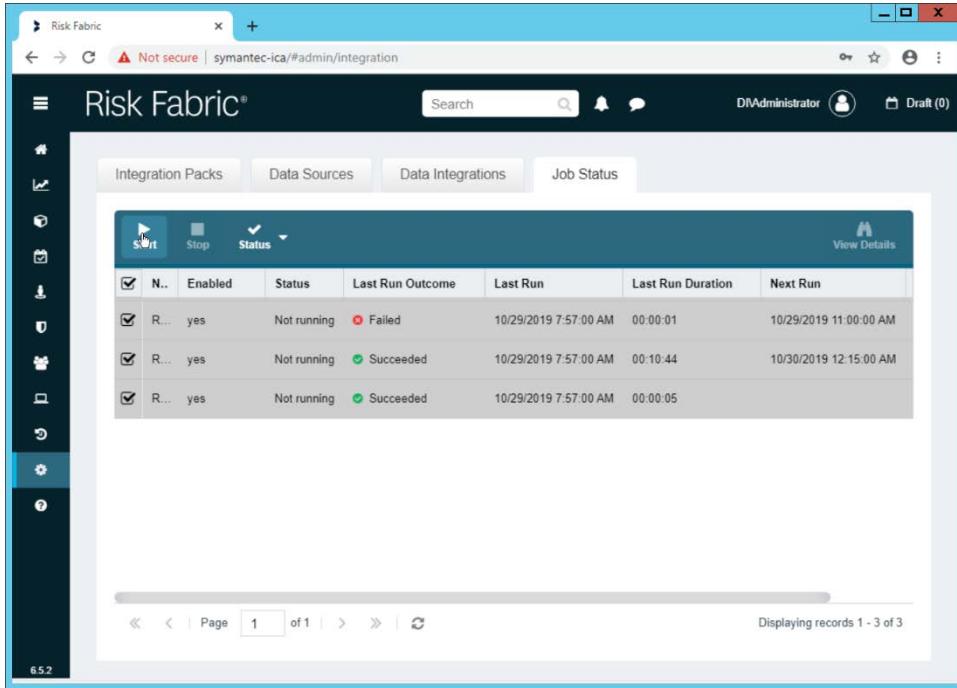
Create and Associate Event Rule

Entity Column	Type	Value	Default Value
EventRule	Source Column		

Save Cancel

2726

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



The screenshot shows the Risk Fabric interface with the 'Job Status' tab selected. A table displays three processing jobs. The columns are: N., Enabled, Status, Last Run Outcome, Last Run, Last Run Duration, and Next Run. The data is as follows:

N.	Enabled	Status	Last Run Outcome	Last Run	Last Run Duration	Next Run
R...	yes	Not running	Failed	10/29/2019 7:57:00 AM	00:00:01	10/29/2019 11:00:00 AM
R...	yes	Not running	Succeeded	10/29/2019 7:57:00 AM	00:10:44	10/30/2019 12:15:00 AM
R...	yes	Not running	Succeeded	10/29/2019 7:57:00 AM	00:00:05	

Below the table, a message indicates "Displaying records 1 - 3 of 3".

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

2.18.4 View ArcSight Events in the Analyzer

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

The screenshot shows the Risk Fabric web application interface. At the top, there's a header with the title 'Risk Fabric', a search bar, and a user dropdown for 'DAdministrator'. Below the header is a navigation bar with options like 'Views', 'Filter', 'Sort', 'Details', and 'Charts'. The main content area features a table titled 'Details' showing event data. The table has columns for 'EP Event Date Ra...', 'Action Taken', 'EP Event Date', and 'EP Event Count'. Two rows of data are visible: one for a logon attempt and another for an account failure. To the right of the table is a 'Field List' sidebar containing a hierarchical tree of various system and security-related fields. At the bottom of the main content area is a 'View Configuration' section for 'arcsight (Analyzer View)', which includes tabs for 'Measures', 'Rows', 'Columns', 'Filters', and 'Details', along with specific field mappings.

2734
2735
2736

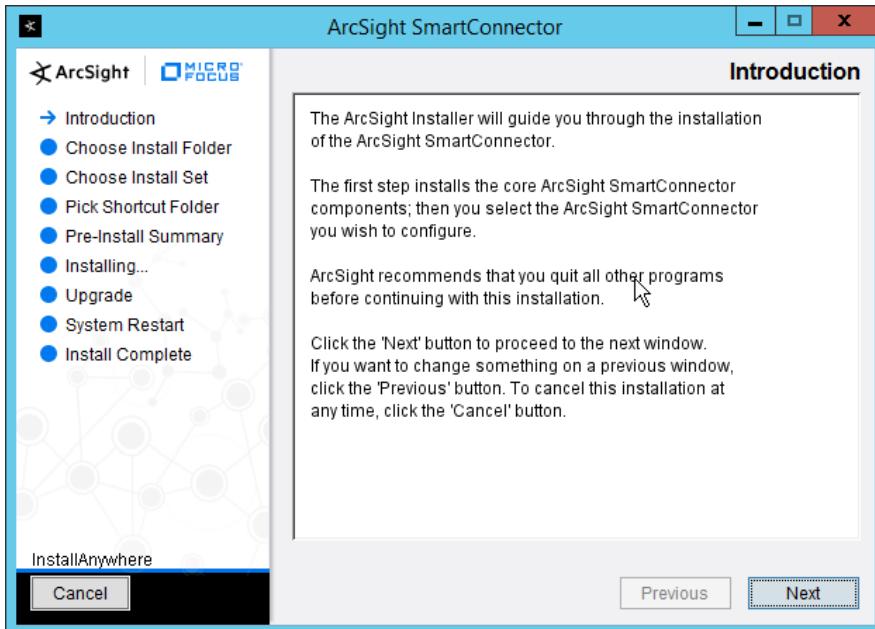
2. Drag mapped columns (from the import rule mapping you created) from the list on the right to view them in the analyzer.

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**.

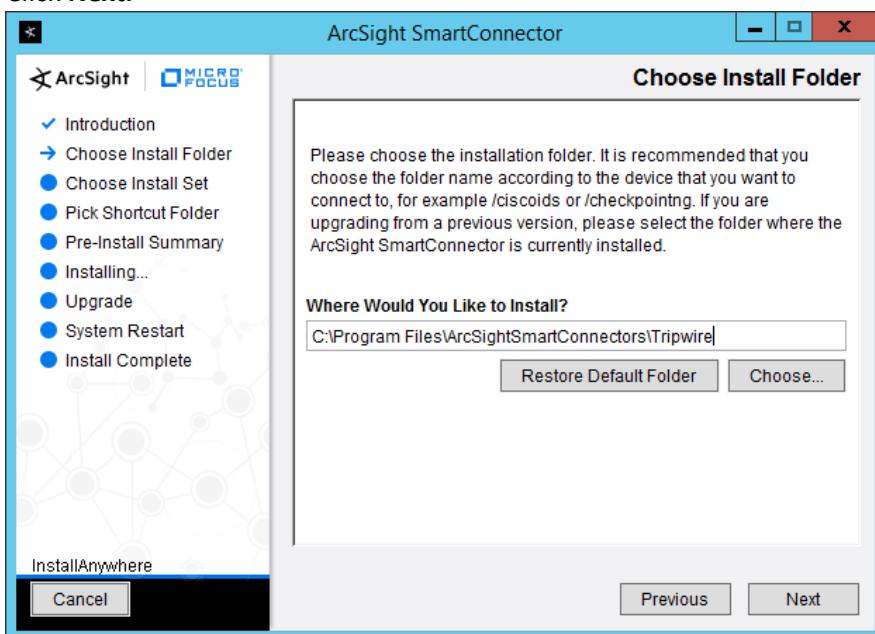
2741 2.19.1 Install Micro Focus ArcSight

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



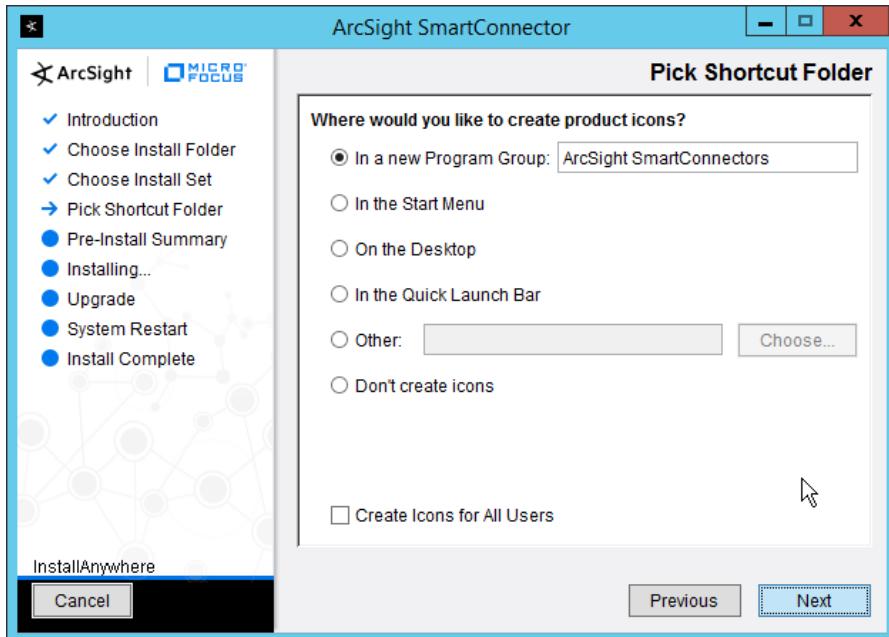
2744
2745

2. Click **Next**.

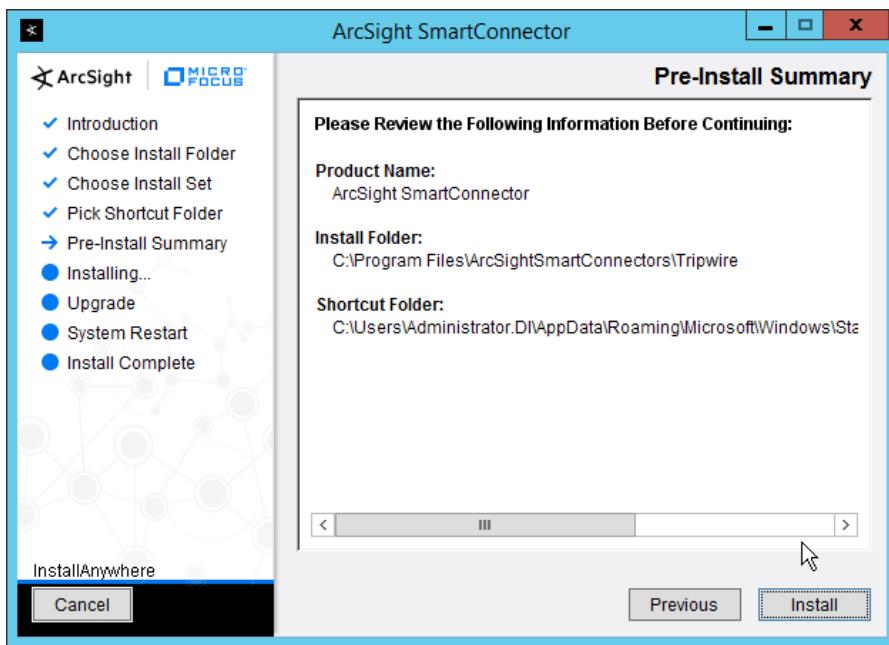


2746
2747

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

2748
2749

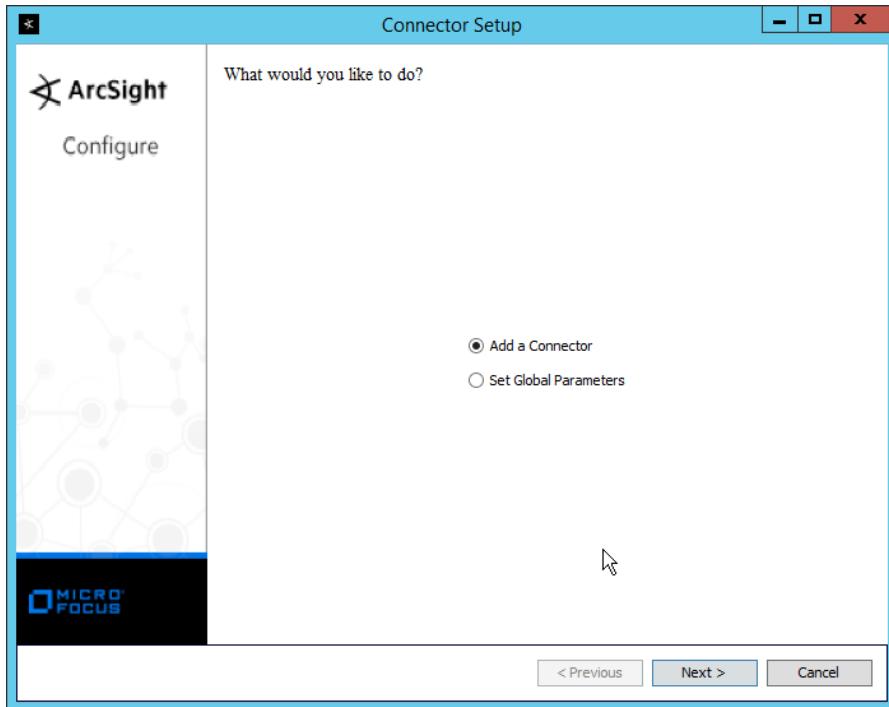
4. Click
- Next**
- .

2750
2751
2752

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

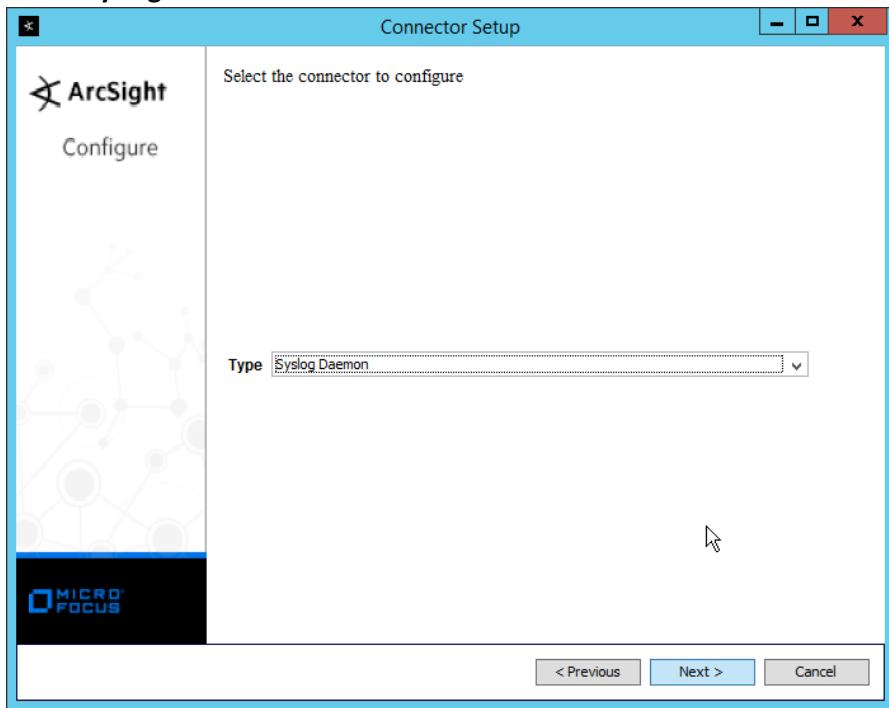
2753
2754
2755

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

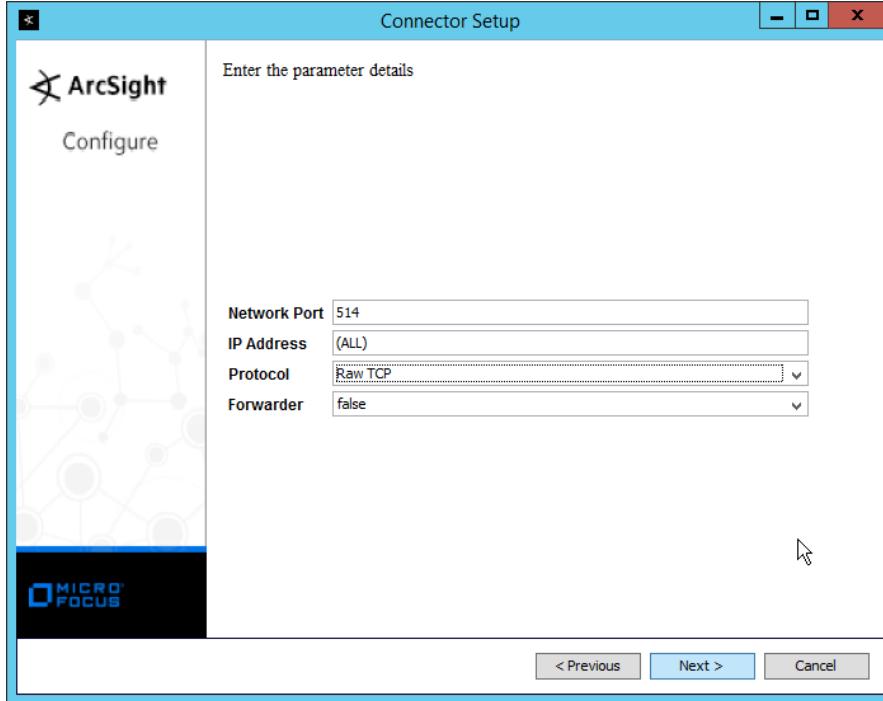


2756
2757

9. Click **Next**.



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

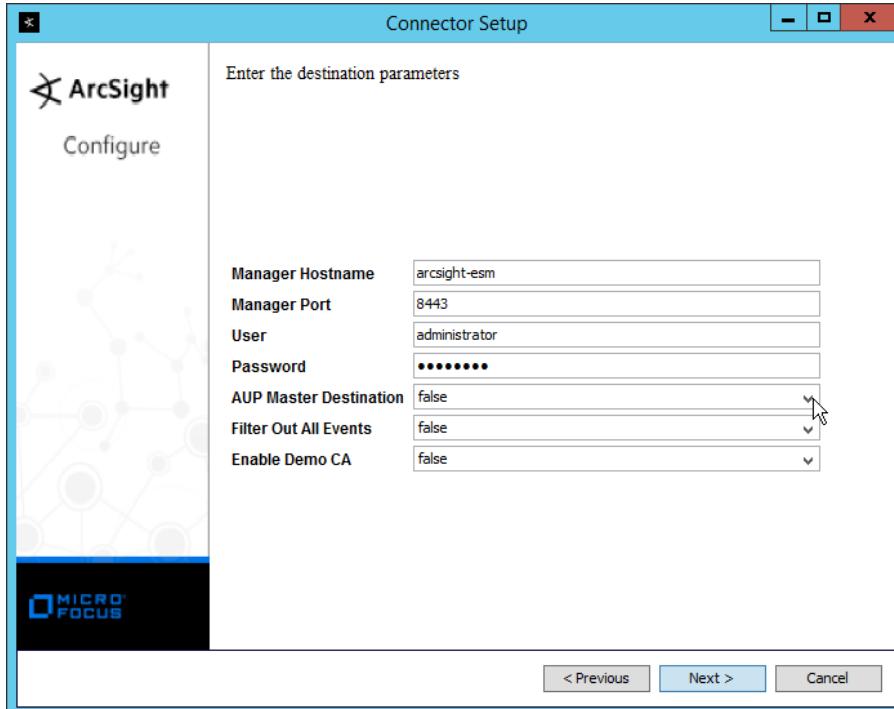


- 2760
2761 12. Click **Next**.
2762 13. Select **ArcSight Manager (encrypted)**.

2763
2764
2765

14. Click Next.

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



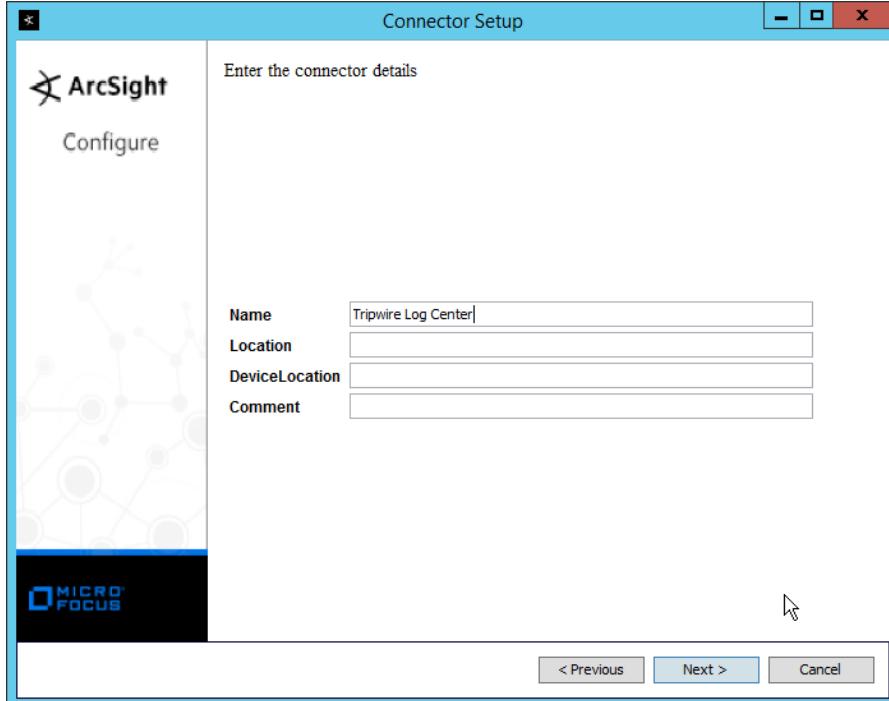
2766

2767

16. Click **Next**.

2768

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

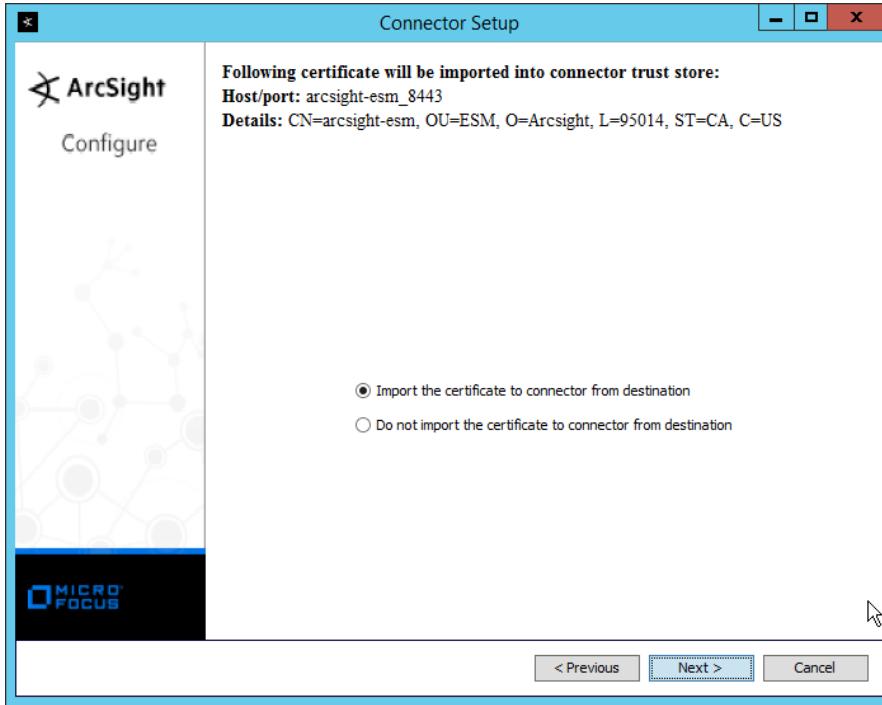


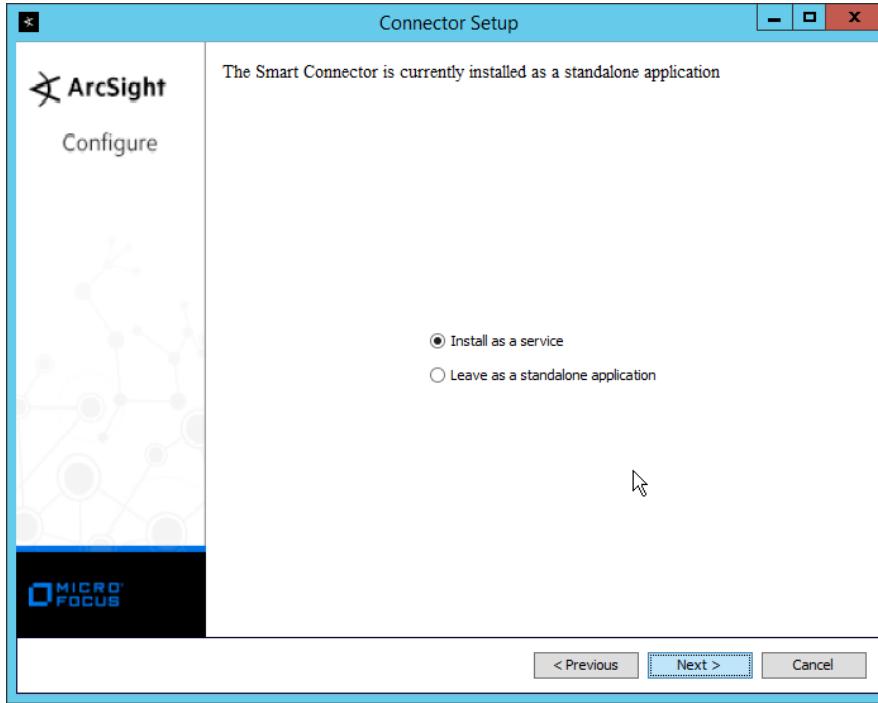
2769

18. Click **Next**.

2770

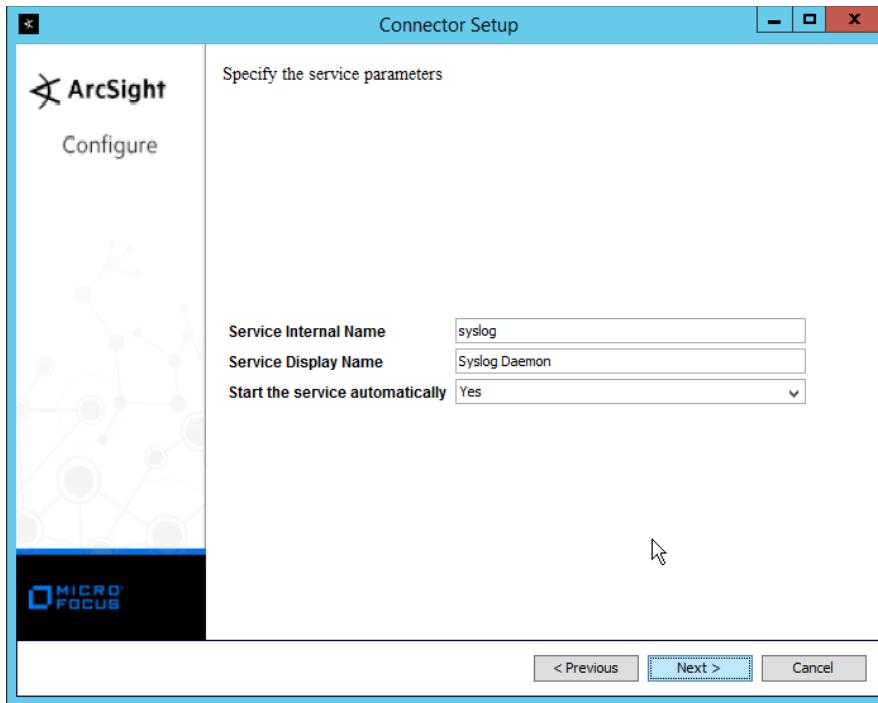
19. Select **Import the certificate to connector from destination**.

2772
277320. Click **Next**.2774
2775
277621. Click **Next**.22. Select **Install as a service**.



2777
2778

23. Click **Next**.

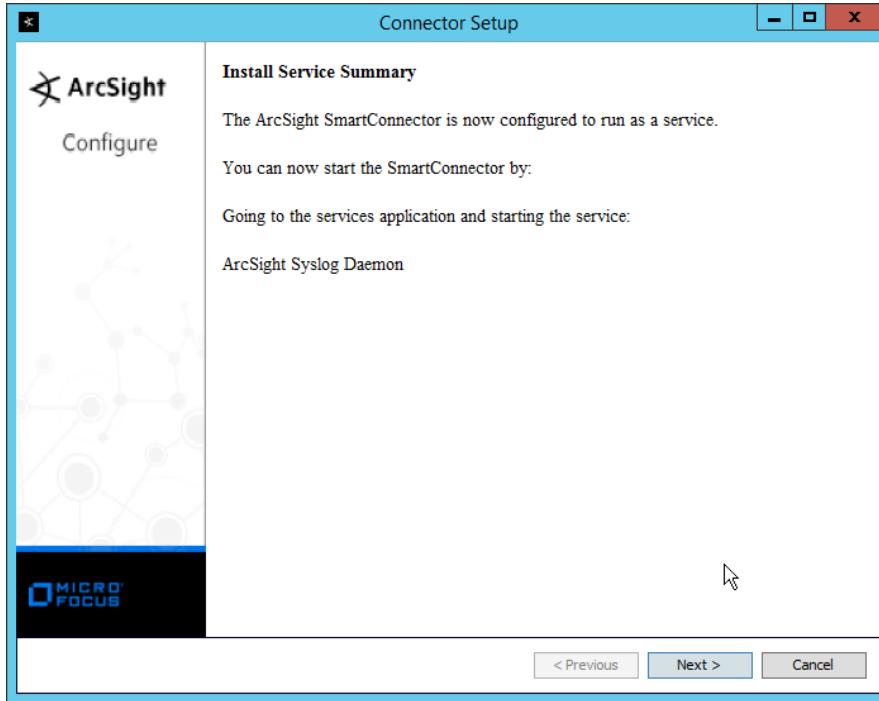


2779
2780

24. Click **Next**.

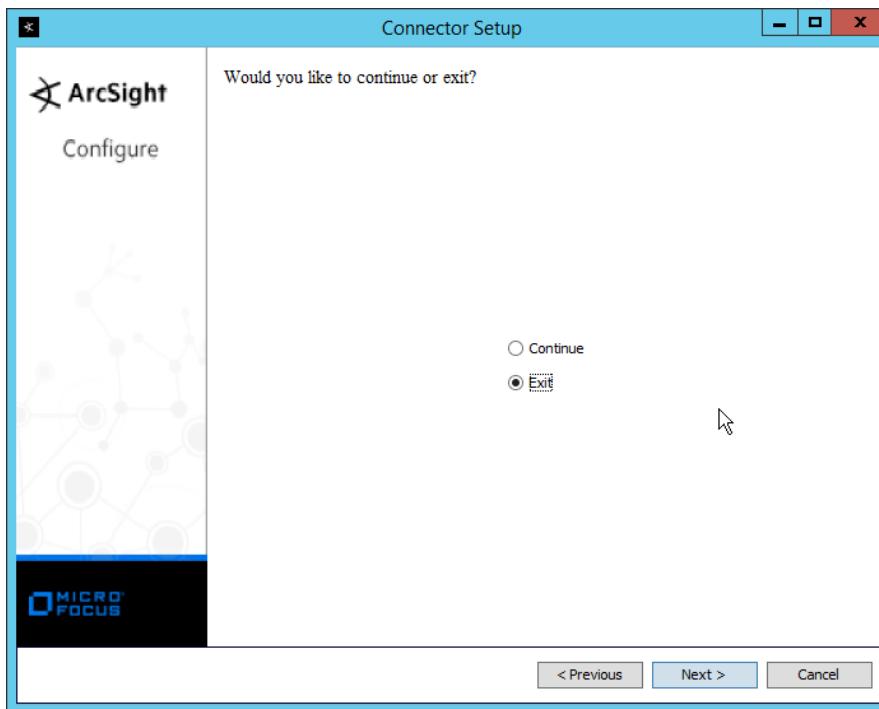
2781
2782
2783

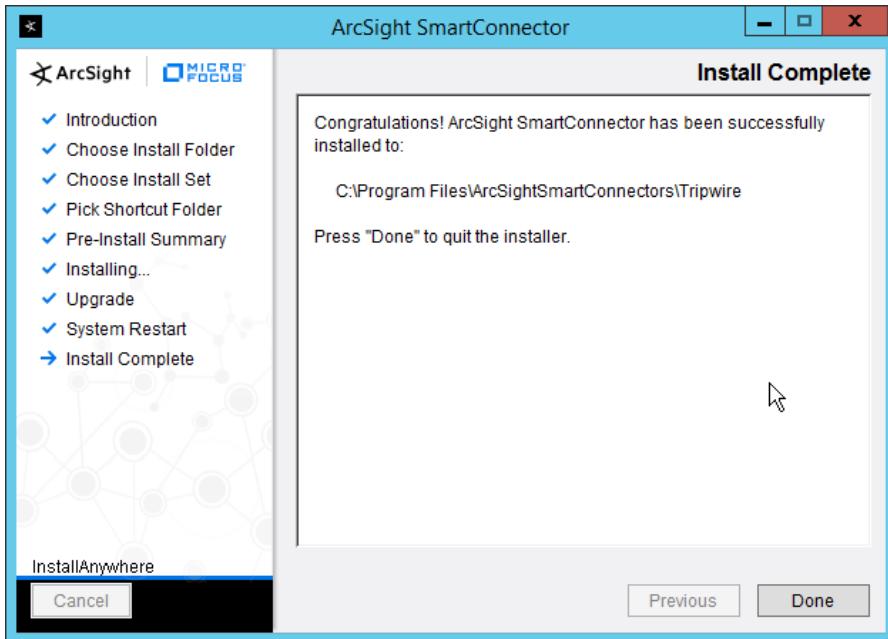
25. Click **Next**.
26. Select **Exit**.



2784
2785

27. Click **Next**.





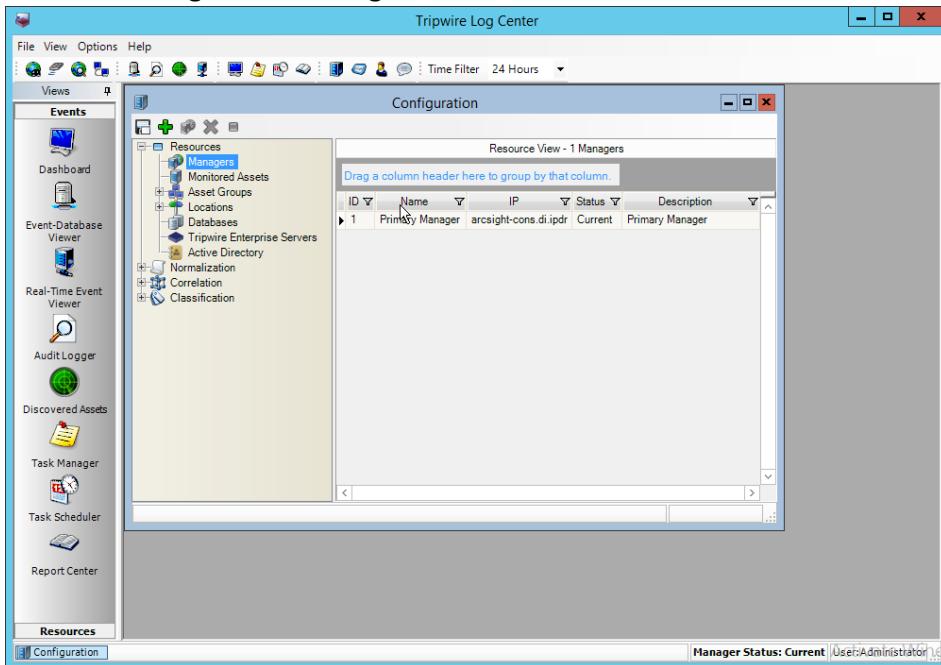
2786

2787

2788

2789

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



2790

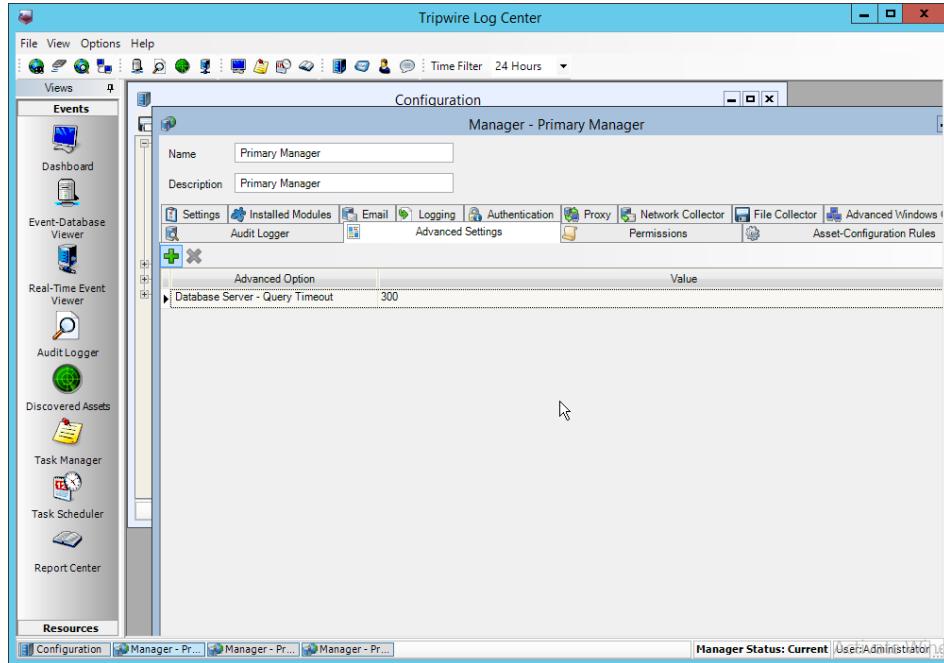
2791

2792

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

2793

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



2794

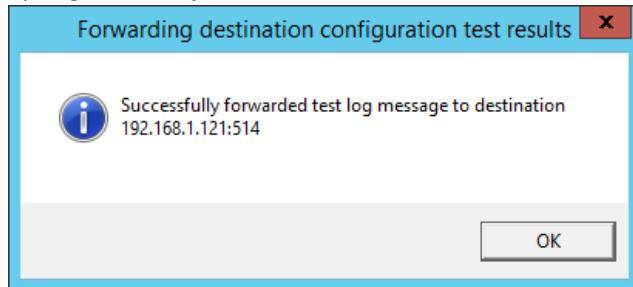
34. Click the **Add** button.

2795

35. In the **Advanced Option** box select **Log Message Forwarding – Destinations**.

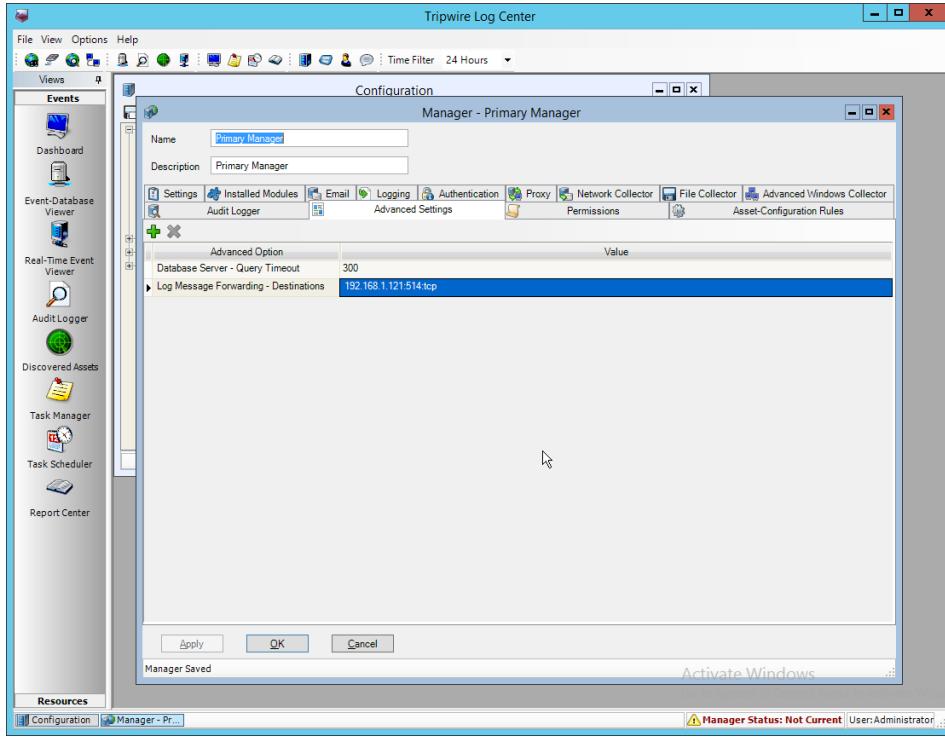
2796

36. In the **Value** box next to it, type <ip_address>:<port>:tcp with the **IP address** and **port** of the syslog daemon just created.



2797

37. Click **OK**.



2801

38. Click **OK**.

2803

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**.

The screenshot shows the Cisco AMP web console with the 'API Credentials' page open. The top navigation bar includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Management', and 'Accounts'. The 'Accounts' tab is selected. Below the navigation is a search bar and a 'View API Documentation' link. The main area is titled 'API Credentials' and contains a table with three rows. Each row has columns for 'Name', 'Type', 'Last used', and 'Actions'. The first row is 'ArcSight' (Read/Write, last used 2019-06-17 15:17:04 UTC). The second row is 'ArcSight Read/Write' (Read/Write, last used 2019-06-17 15:17:04 UTC). The third row is 'CTR' (Read/Write, last used 2019-06-17 15:17:04 UTC). At the top of the table are buttons for 'New API Credential' and 'Delete'.

2808

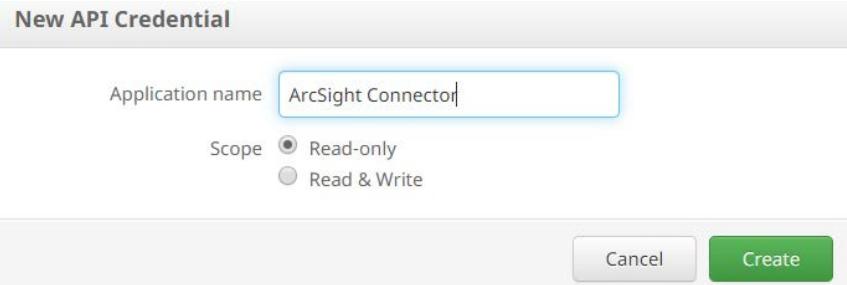
2. Click **New API Credential**.

2809

3. Enter a name for the credential.

2810

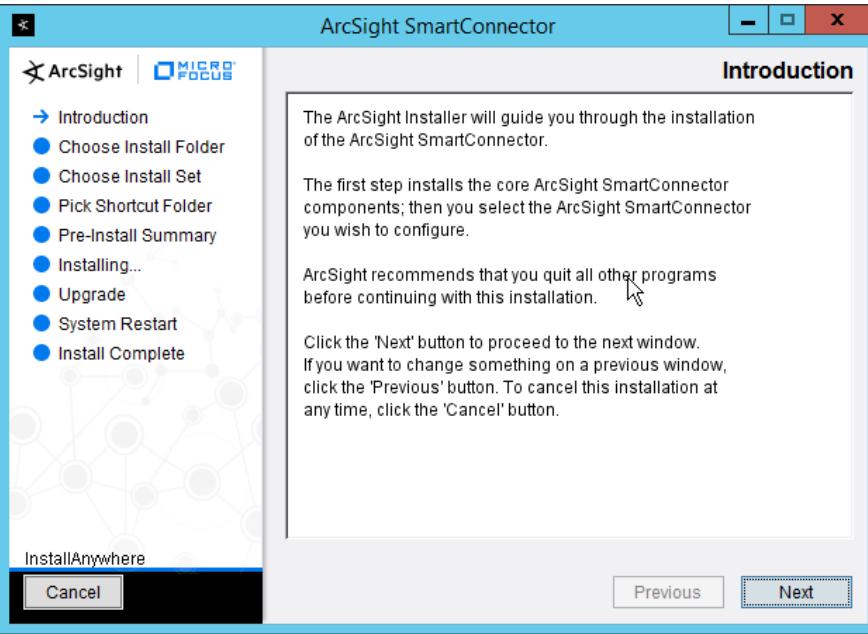
4. Select **Read-only**.



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

2.20.2 Install Micro Focus ArcSight

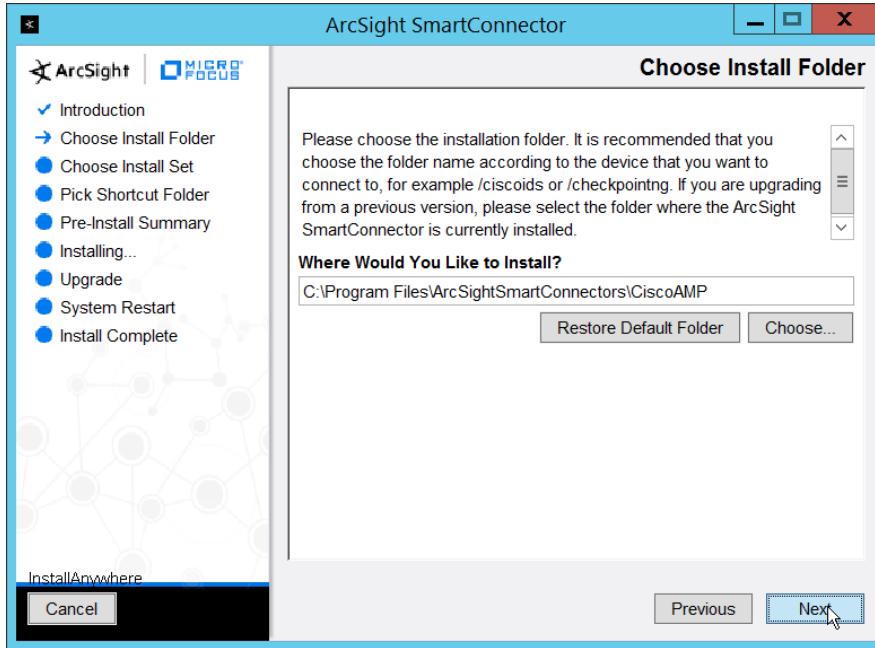
- 2816 1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server.



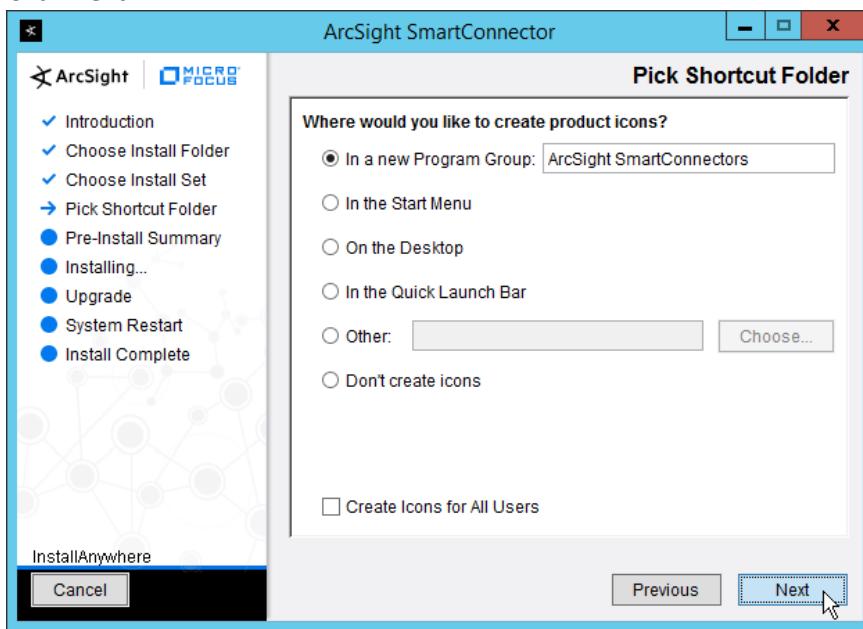
- 2817 2. Click **Next**.
- 2818 3. Enter **C:\Program Files\ArcSightSmartConnectors\CiscoAMP**.
- 2819
- 2820

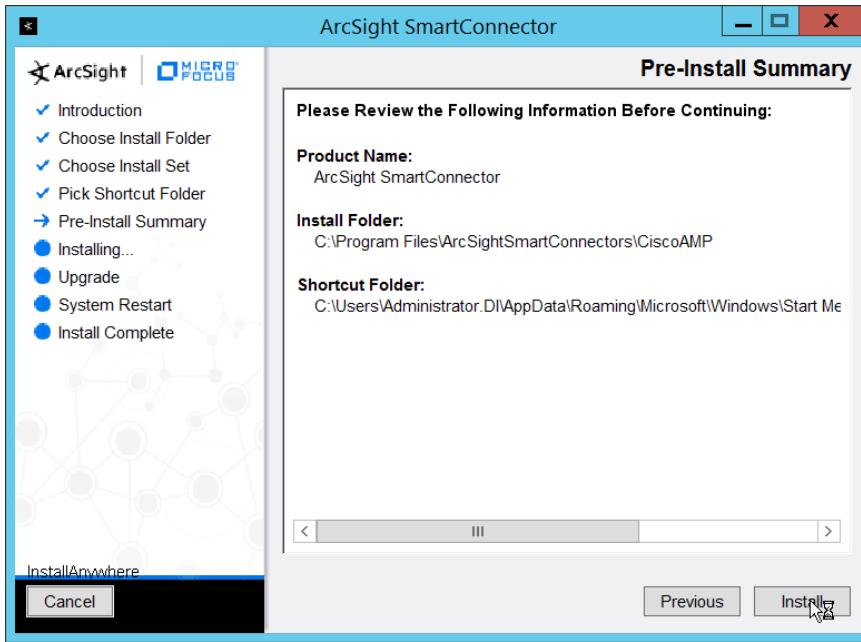
2821
2822

4. Click **Next**.

2823
2824

5. Click **Next**.

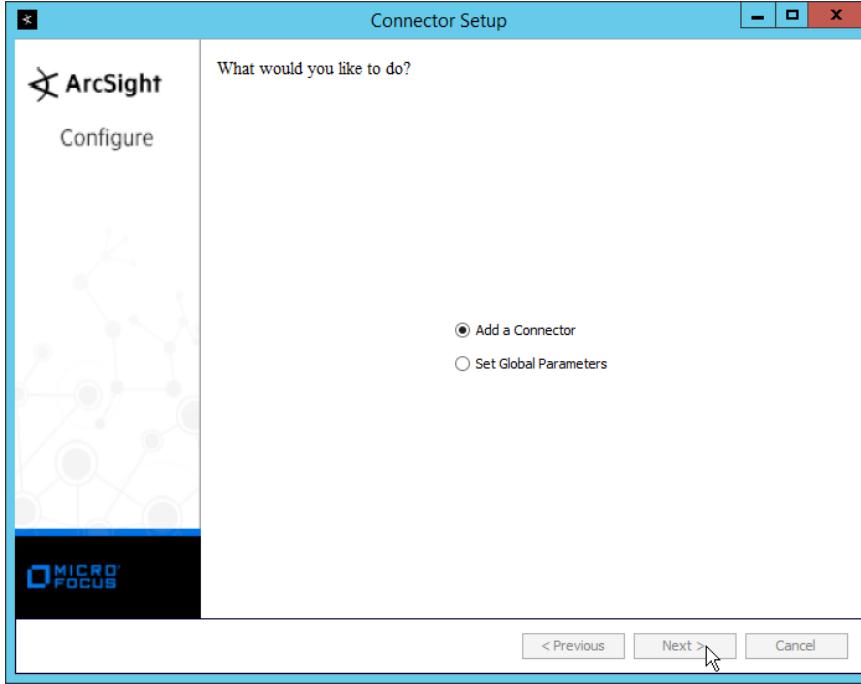




2825

2826

2827

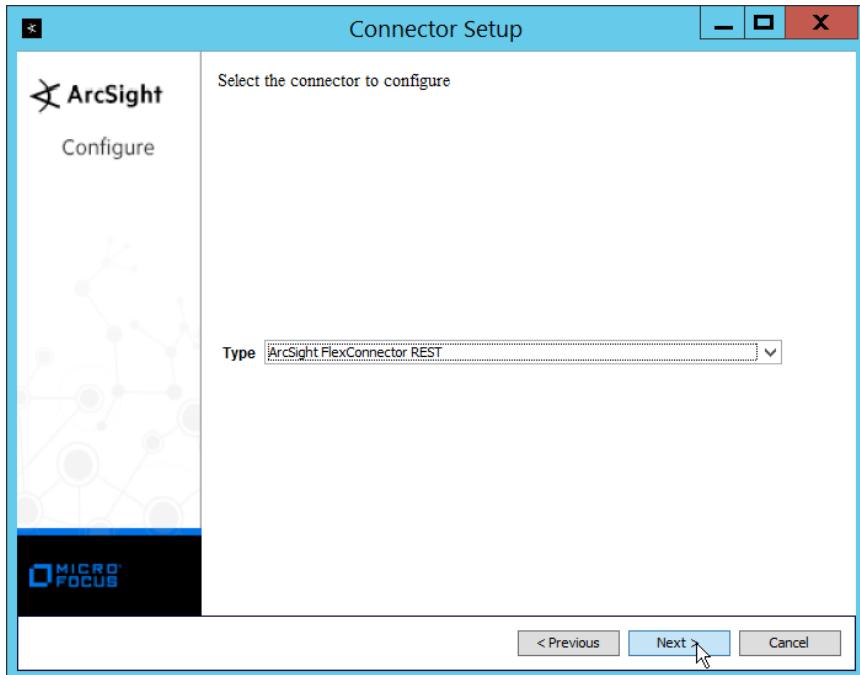
6. Click **Install**.7. Select **Add a Connector**.

2828

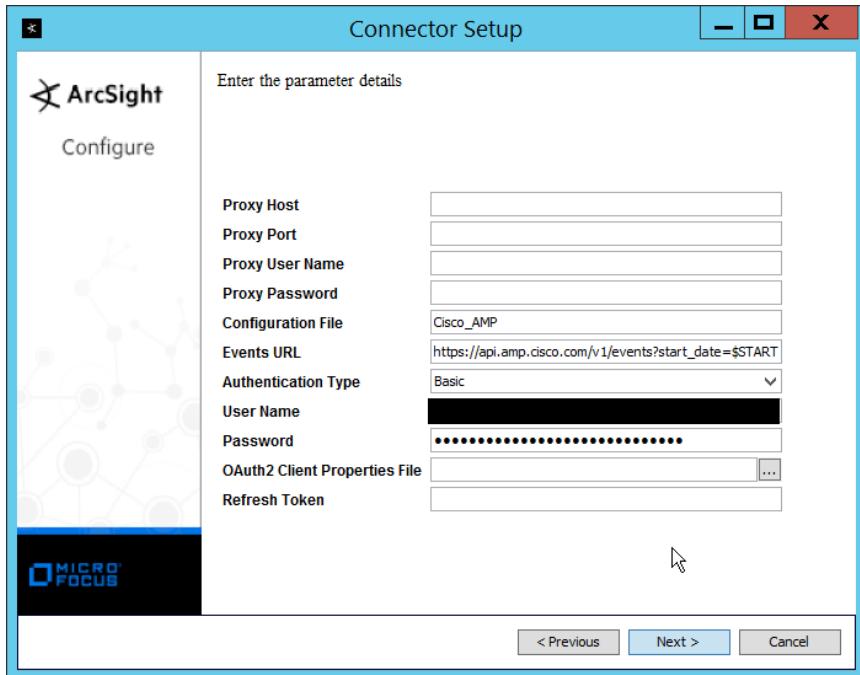
2829

2830

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



- 2831
2832 10. Click **Next**.
2833 11. Enter *Cisco_AMP* for the **Configuration File**.
2834 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**.
2835 (Note: You can see the Cisco AMP REST API documentation for more information on how to
2836 formulate this URL for things other than events.)
2837 13. Enter the username and password from the credential generated on Cisco AMP in Section
2838 2.20.1.



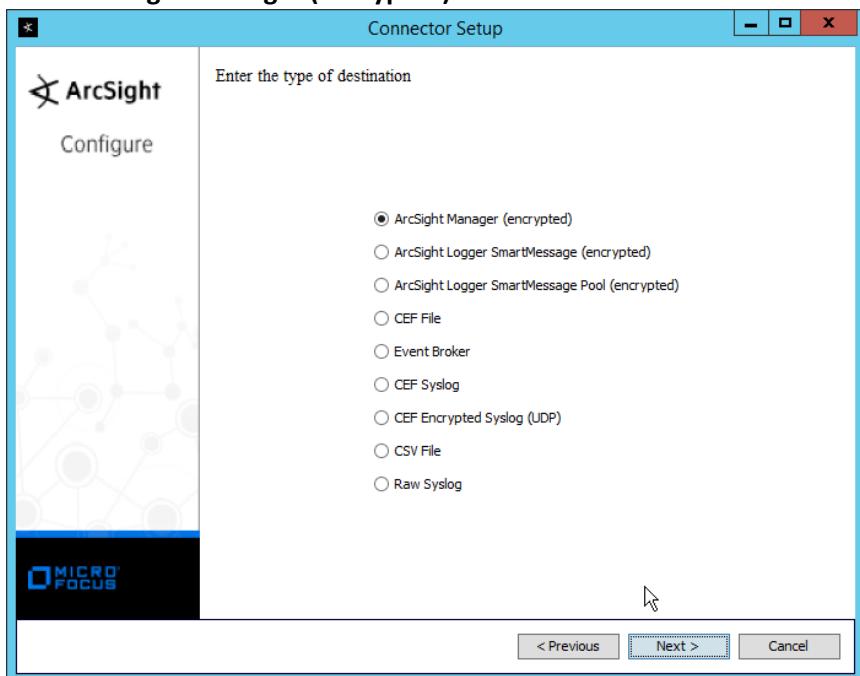
2839

2840

2841

14. Click **Next**.

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



2842

2843

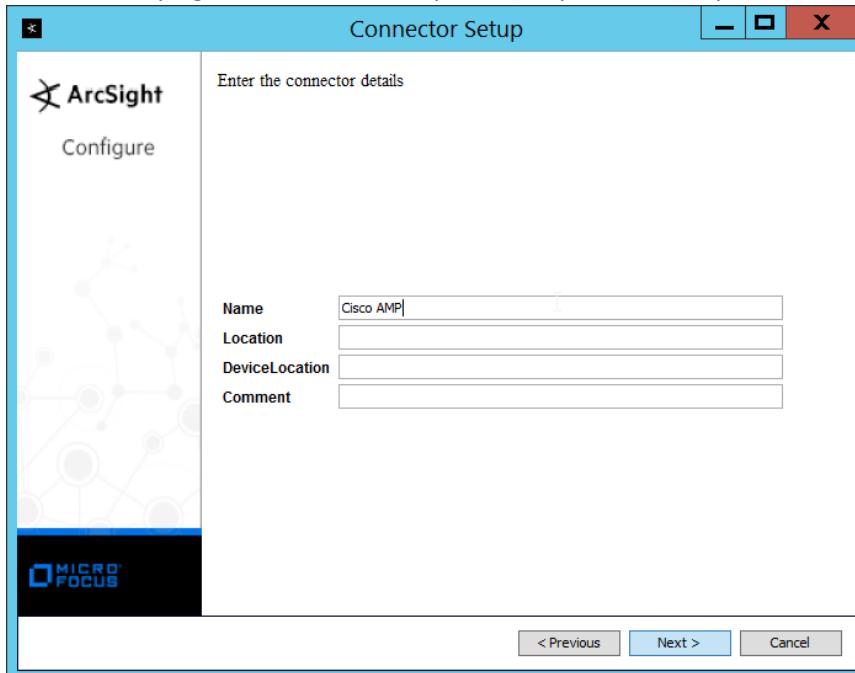
2844

16. Click **Next**.

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

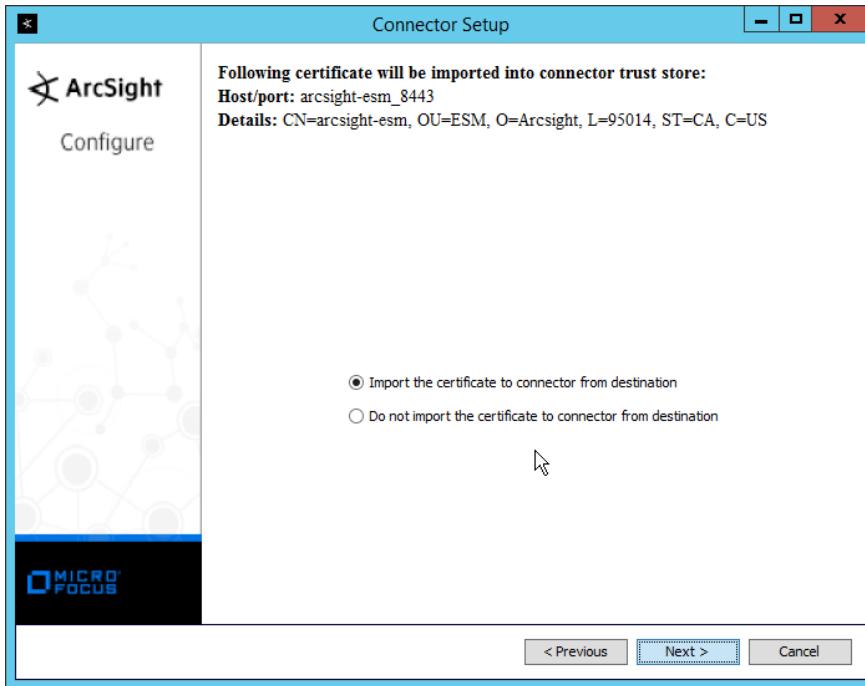
2845
2846
2847

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

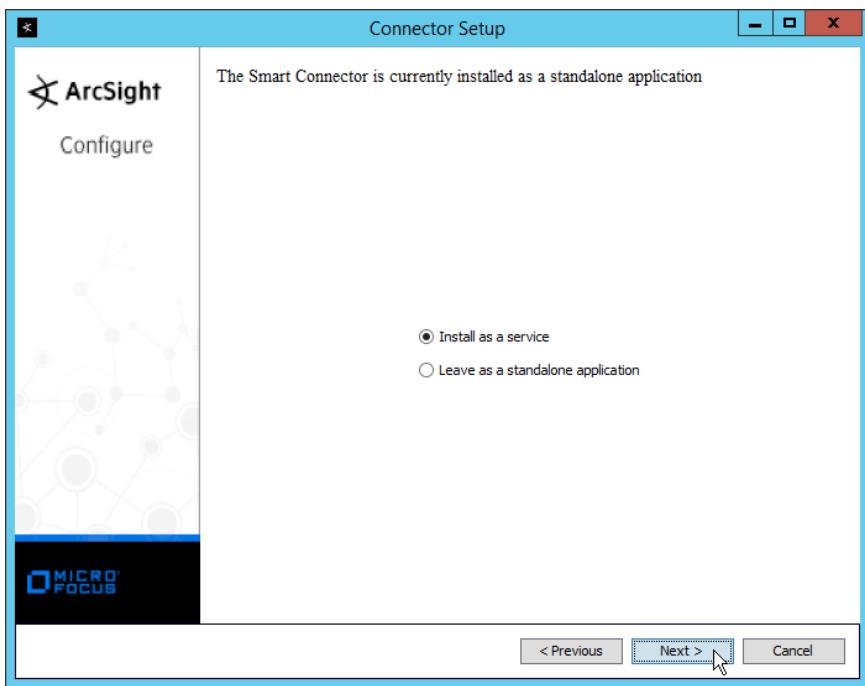


2848
2849
2850

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



2851

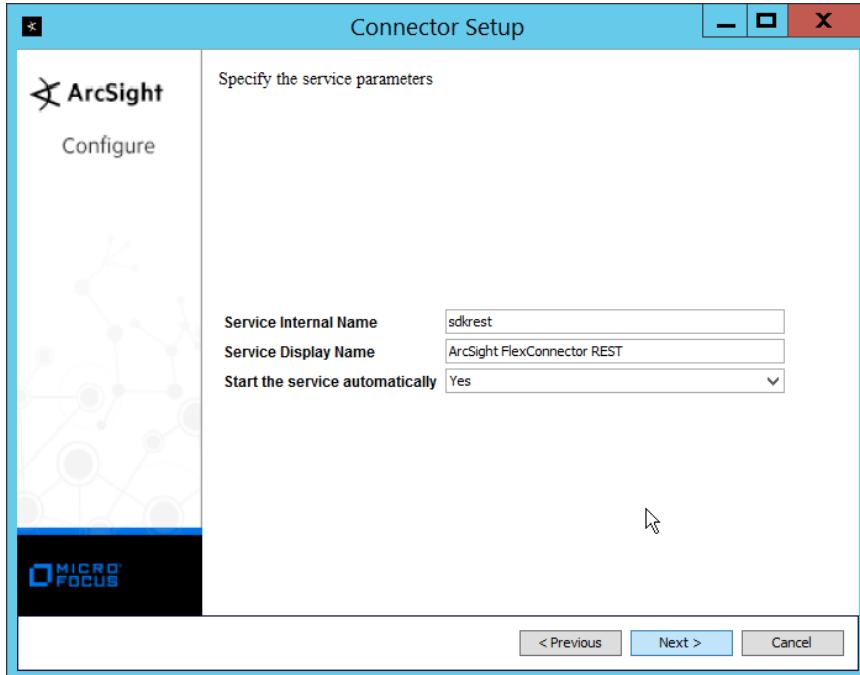
2852 22. Click **Next**.2853 23. Click **Next**.2854 24. Select **Install as a service**.

2855

2856 25. Click **Next**.

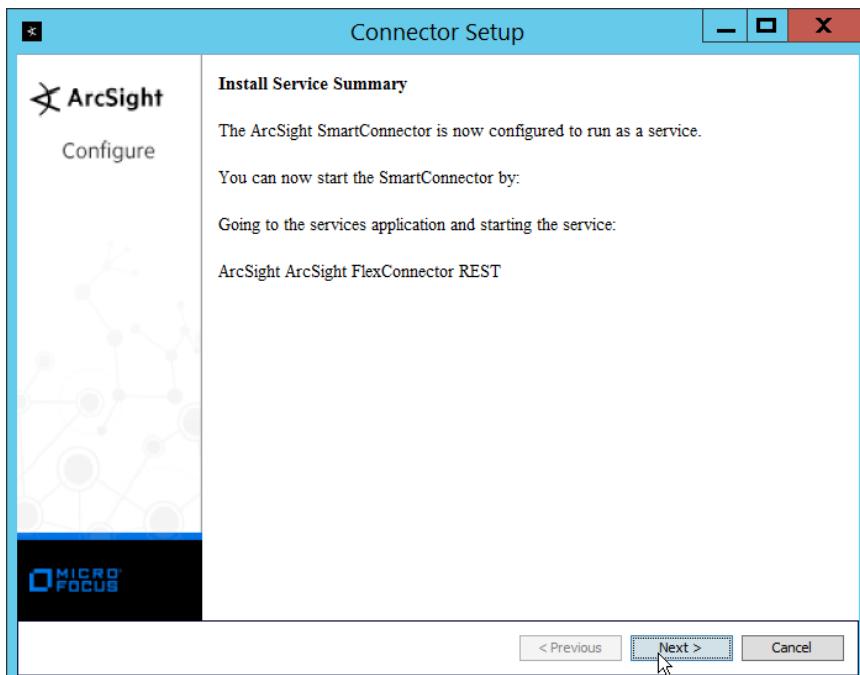
2857

26. Enter a service name and display name.



2858

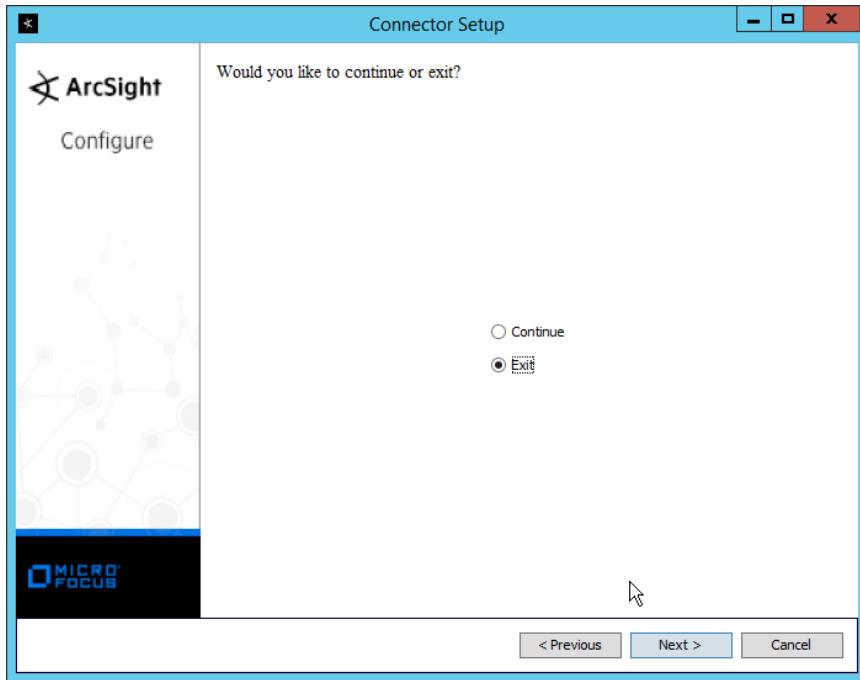
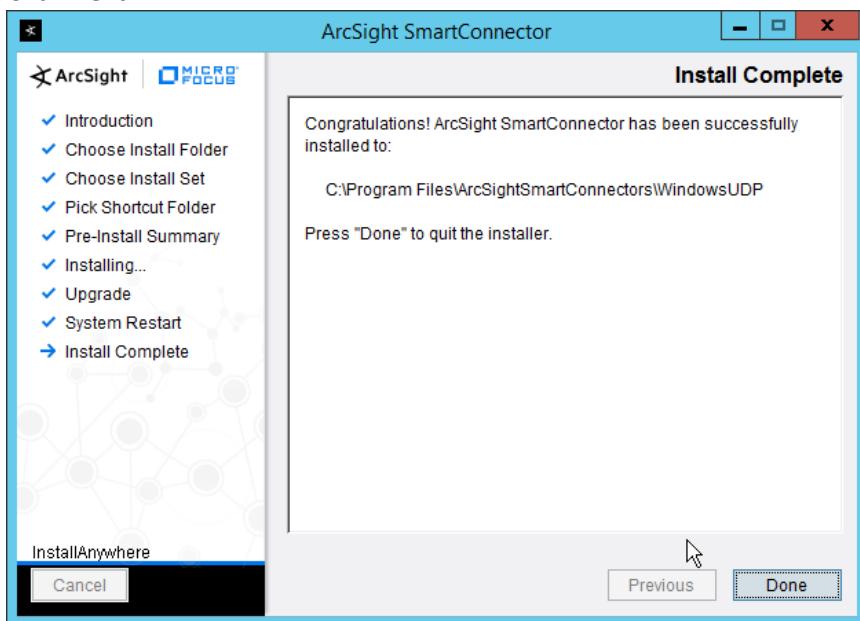
2859 27. Click **Next**.



2860

2861 28. Click **Next**.

2862 29. Select **Exit**.

2863
286430. Click **Next**.2865
286631. Click **Done**.2867
2868

2.20.3 Create a Parser for Cisco AMP REST events

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")
2909

```
- 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

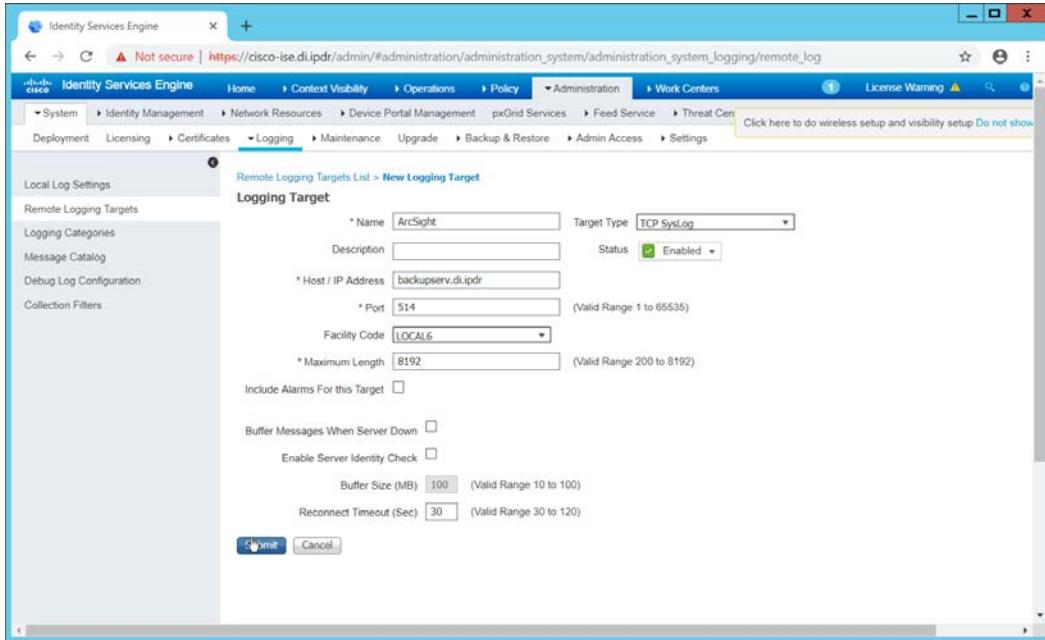
2917 collector. If a server is already configured, you do not need to install a new one—simply use the address  
 2918 of that server to which to forward logs.

### 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**.

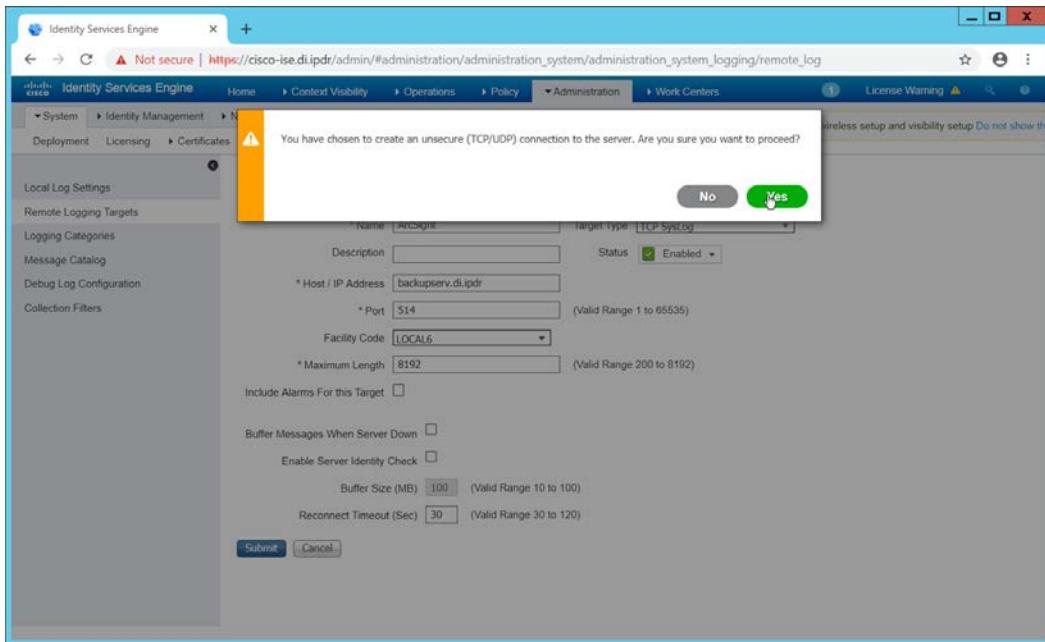
| Name                  | IP Address | Port  | Type            | Description                             | Status |
|-----------------------|------------|-------|-----------------|-----------------------------------------|--------|
| LogCollector          | 127.0.0.1  | 20514 | UDP SysLog      | Syslog Target for Log Collector         | En     |
| ProfilerRadiusProbe   | 127.0.0.1  | 30514 | Profiler SysLog | Syslog Target for Profiler RADIUS Probe | En     |
| SecureSyslogCollector | 127.0.0.1  | 6514  | Secure SysLog   | Secure Syslog Collector                 | En     |
| TCPLogCollector       | 127.0.0.1  | 1468  | TCP SysLog      | TCP SysLog collector                    | De     |

- 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**.



2931  
2932

9. Click **Submit**.

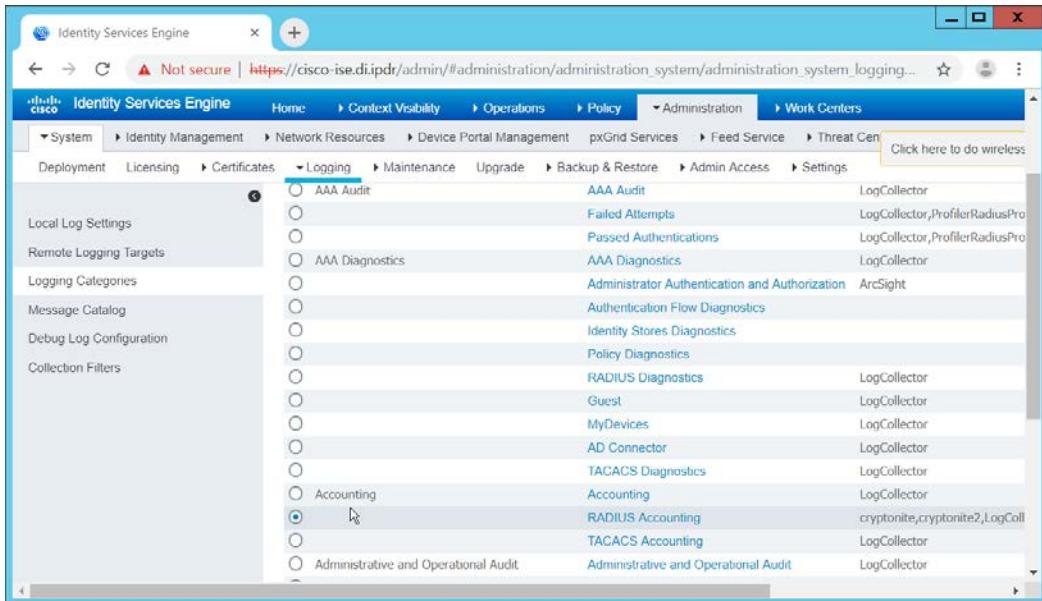


2933  
2934

10. Click **Yes**.

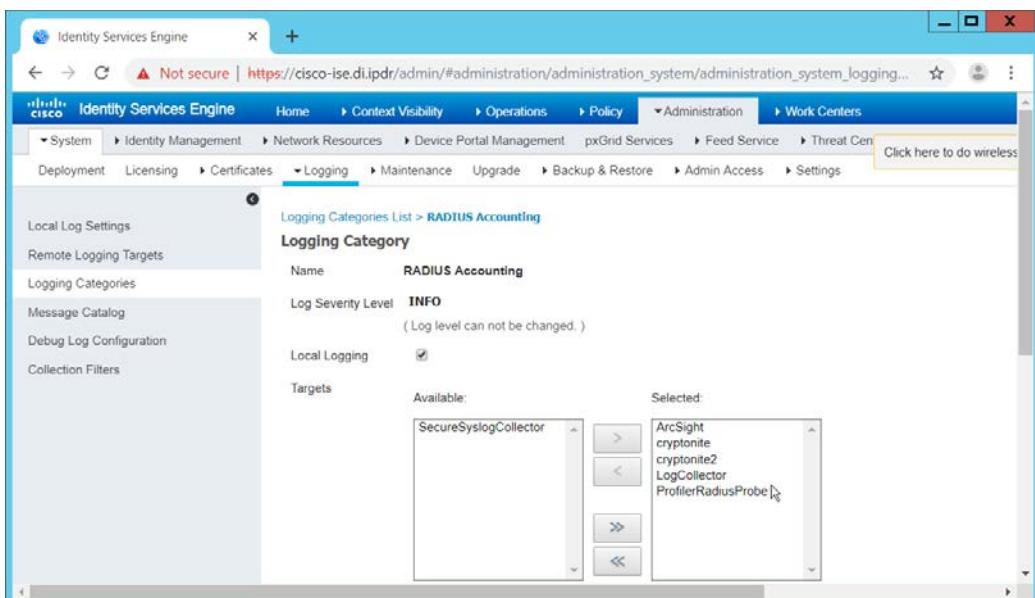
## 2.21.2 Select Logs for Forwarding

2935 1. Navigate to **System > Logging > Logging Categories**.



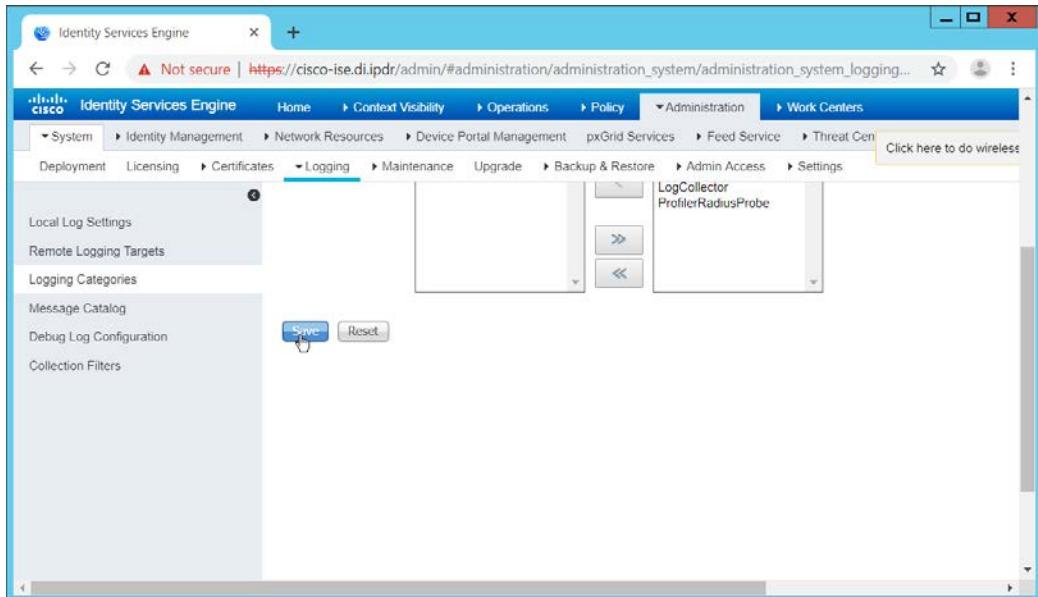
2937  
2938  
2939

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.

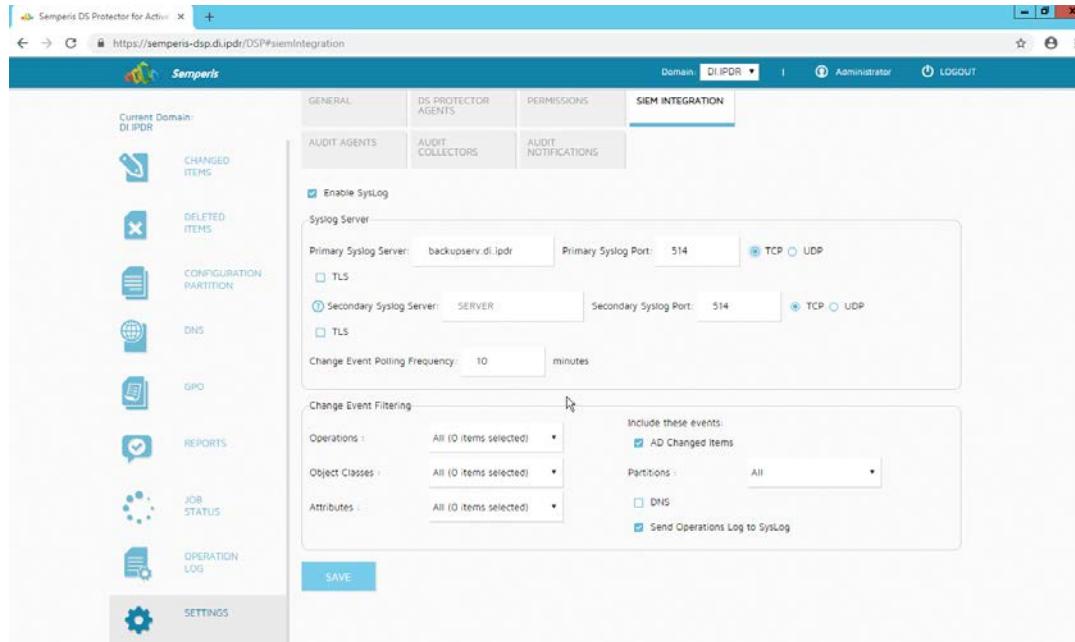
## 2.22 Integration: Micro Focus ArcSight and Semperis DSP

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.

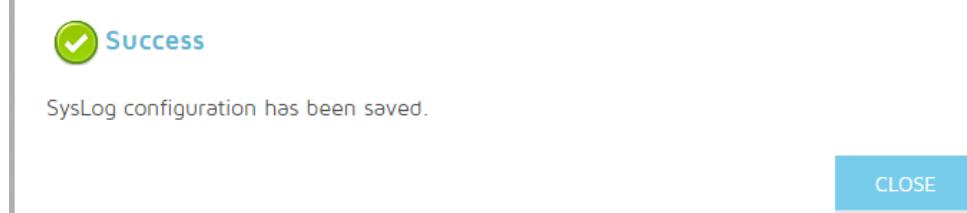
2950 Note: This integration requires Semperis DSP version 2.6.

### 2.22.1 Configure Semperis DSP to Forward Logs

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.

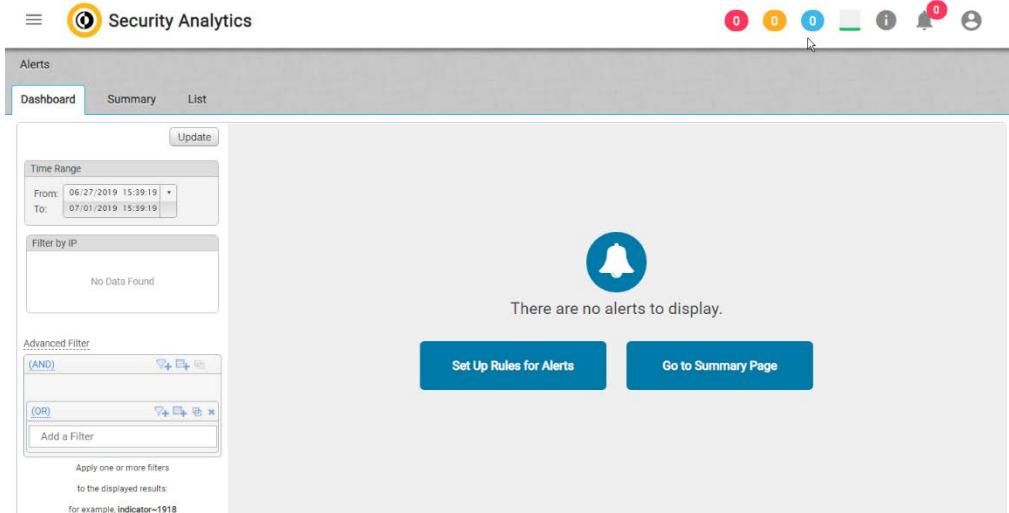
## 2.23 Integration: Micro Focus ArcSight and Symantec Analytics

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

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

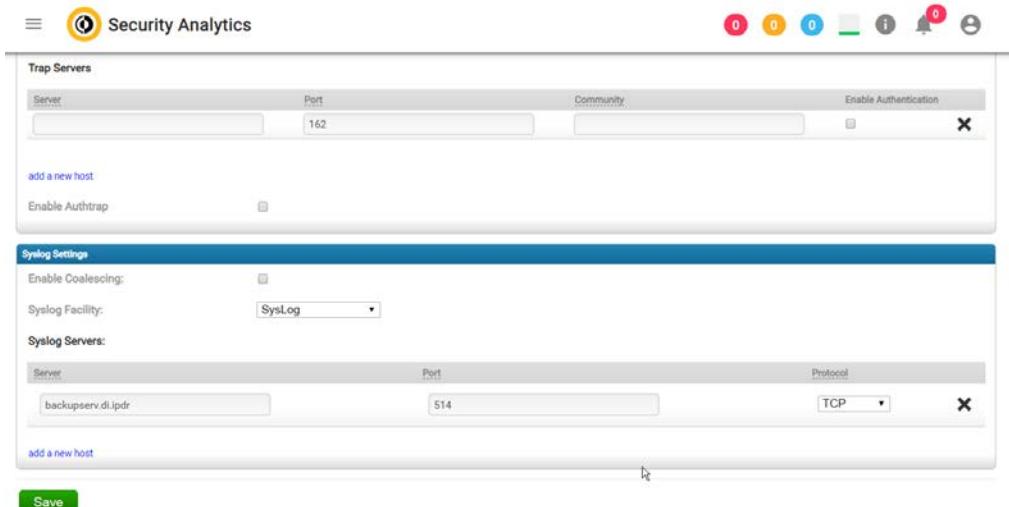
### 2.23.1 Configure Symantec Analytics to Forward Logs

1. Log in to the Symantec Analytics web console.



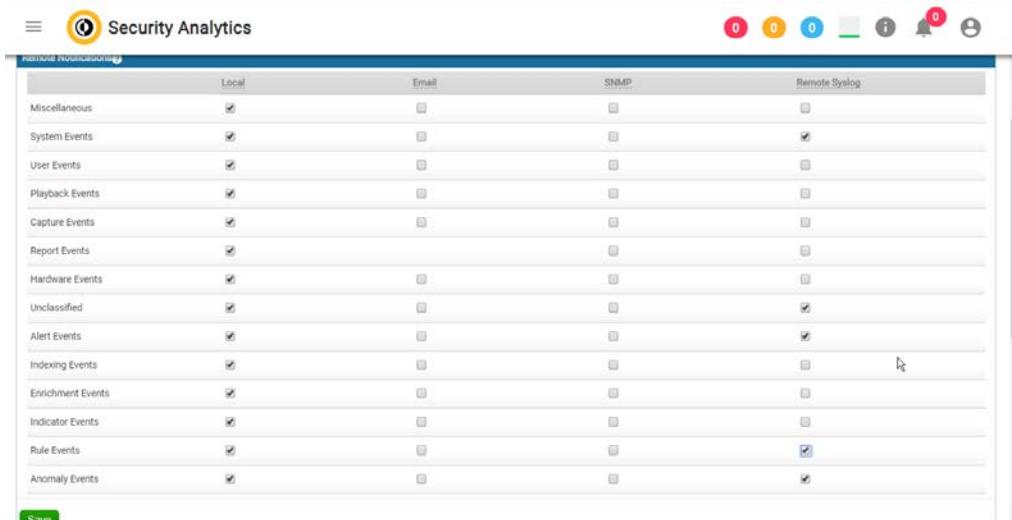
2975  
2976  
2977  
2978  
2979  
2980  
2981  
2982

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

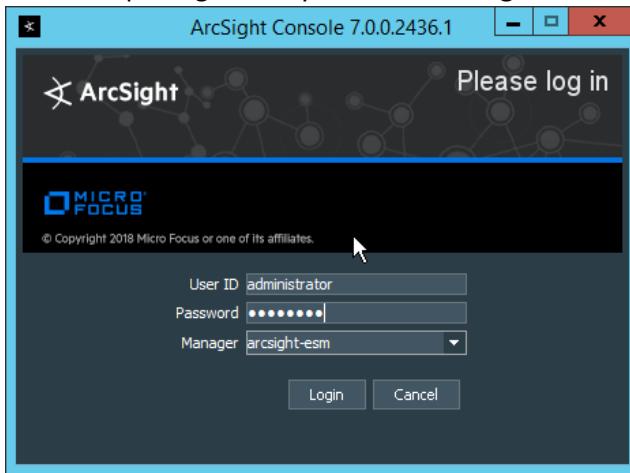
12. Click Save.

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 ArcSight. It may be available here: <https://marketplace.microfocus.com/arcsight/content/blue-coat-security-analytics-platform> but not please contact your ArcSight representative to get the package. The package should be called **Blue\_Coat\_SA\_HP\_ArcSight-3.0.arb**.
2. Place this package on a system with **ArcSight ESM Console** installed.



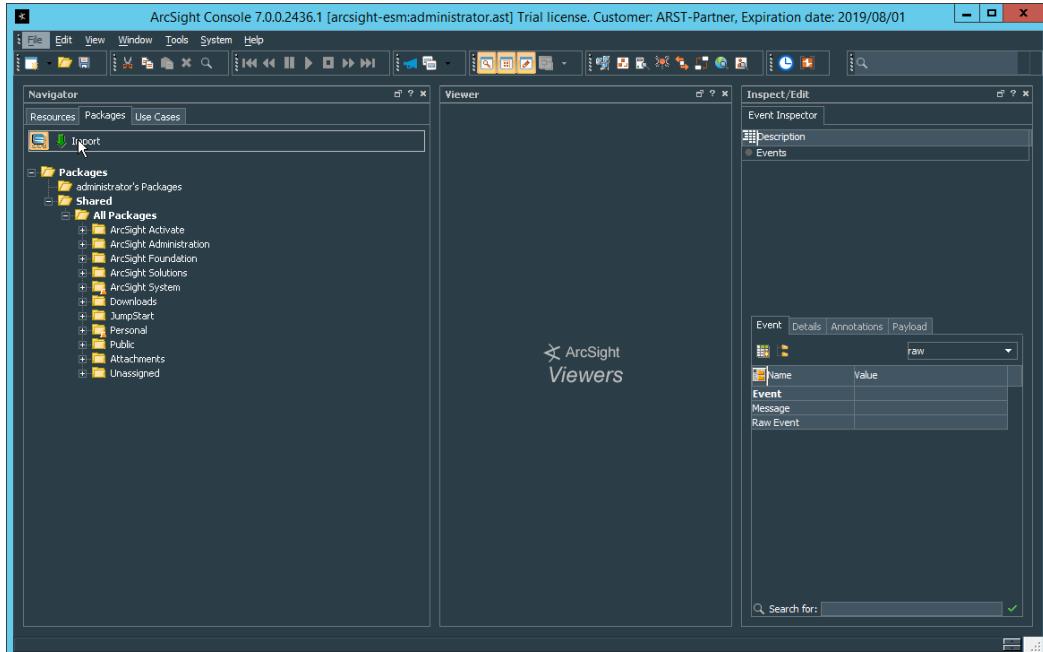
2997

2998

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

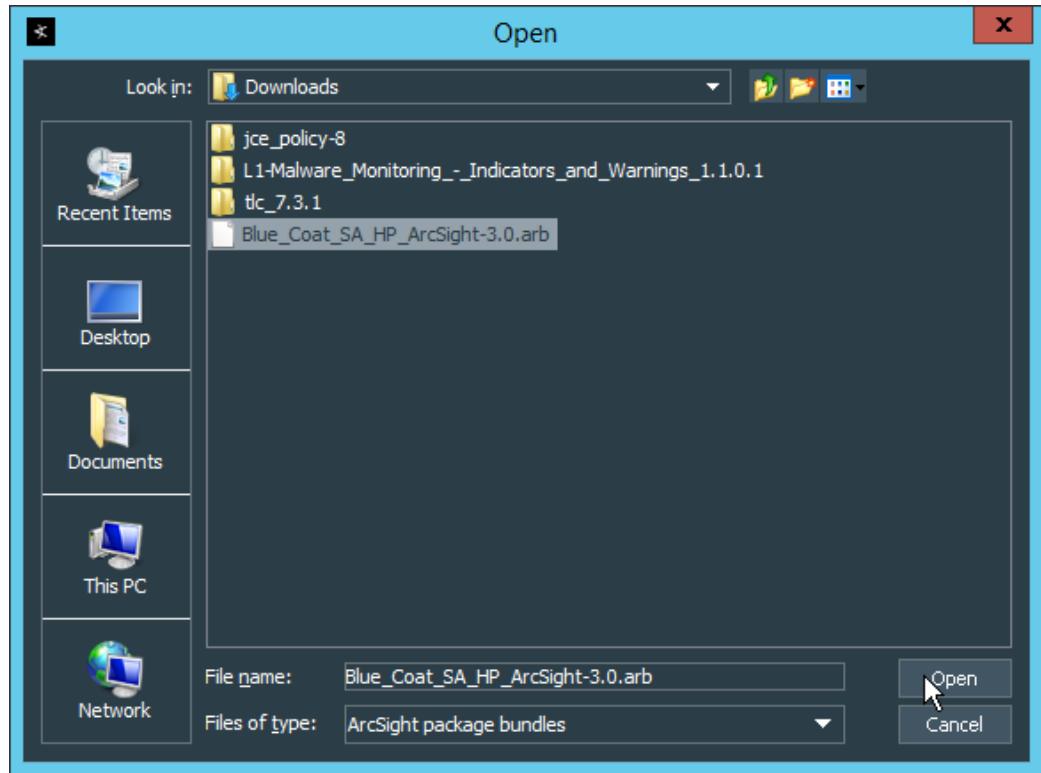
2999  
3000

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



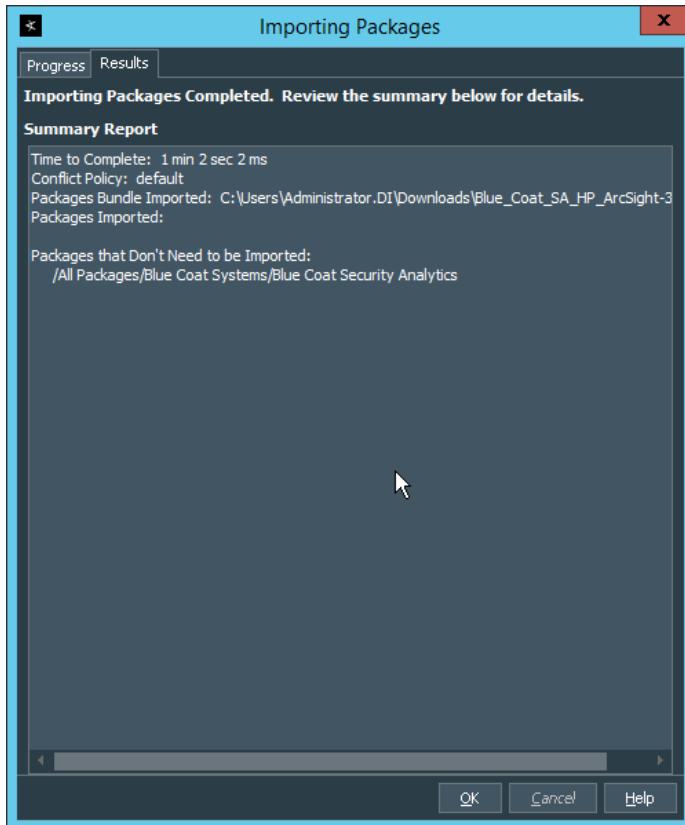
3001  
3002  
3003

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



3004  
3005

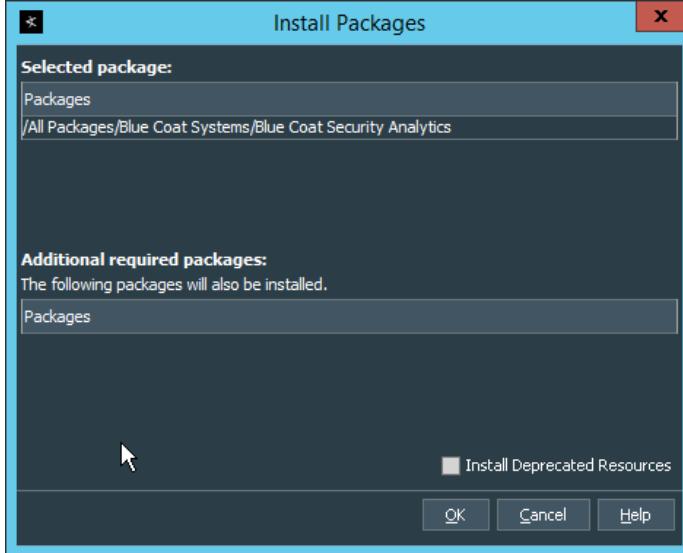
7. Click **Open**.



- 3006  
3007     8. Click **OK** when the import finishes.  
3008  
3009     9. Under the **Packages** tab in the **Navigator** pane, navigate to **Packages > Shared > All Packages > Blue Coat Systems > Blue Coat Security Analytics**.

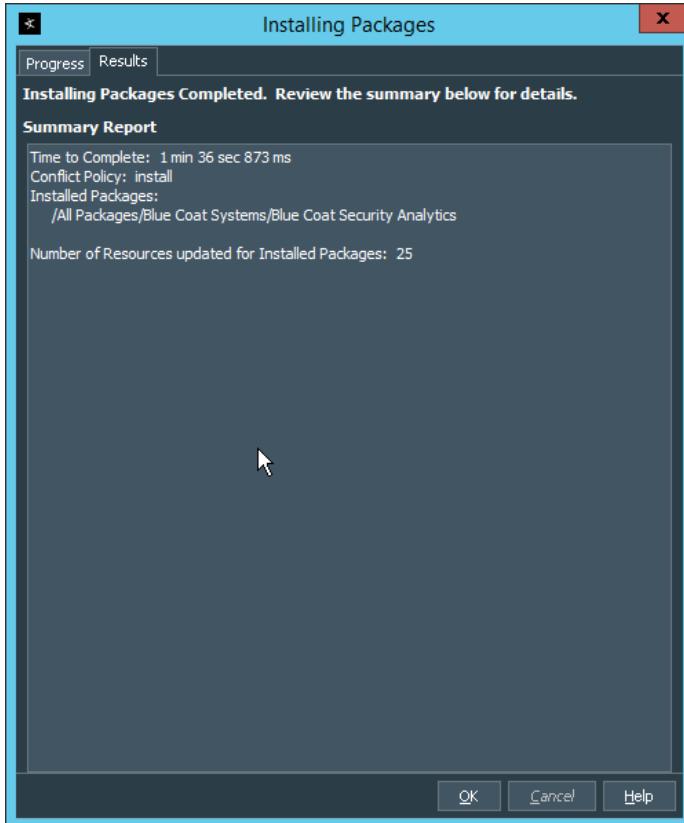
3010  
3011

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



3012  
3013

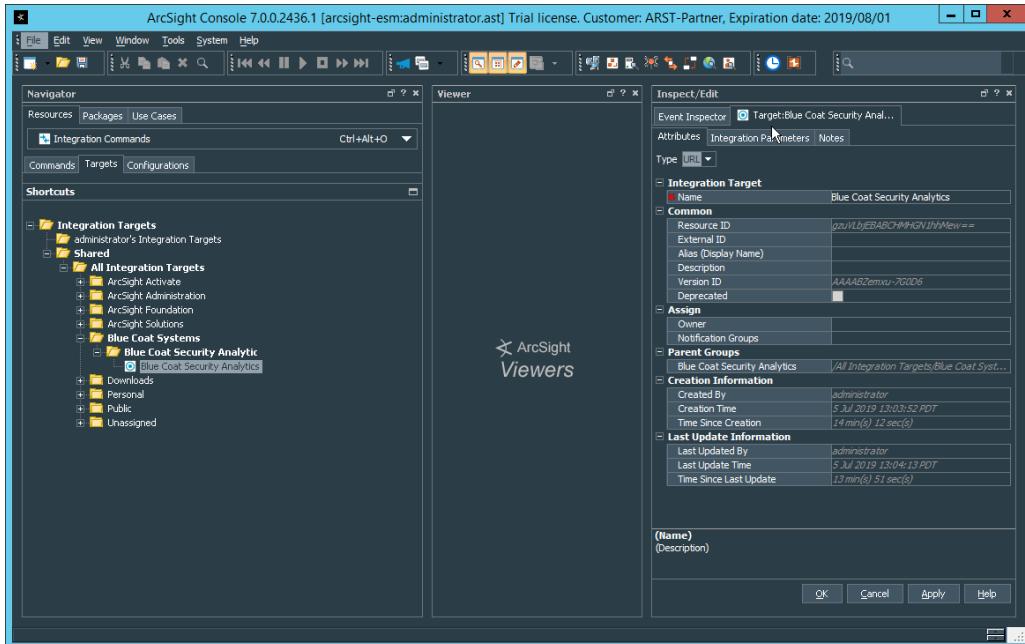
11. Click **OK**.



- 3014  
3015 12. Click **OK**.
- 3016 13. When this completes, you can verify that the installation was successful by the existence of a  
3017 **Blue Coat Systems** folder when you navigate to **Resources > Integration Commands >**  
3018 **Commands > Shared > All Integration Commands**.
- 3019 14. In the **Resources** tab of the **Navigation** pane, under **Integration Commands**, select the **Targets**  
3020 tab.
- 3021 15. Navigate to **Integration Targets > Shared > All Integration Targets > Blue Coat Systems > Blue**  
3022 **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

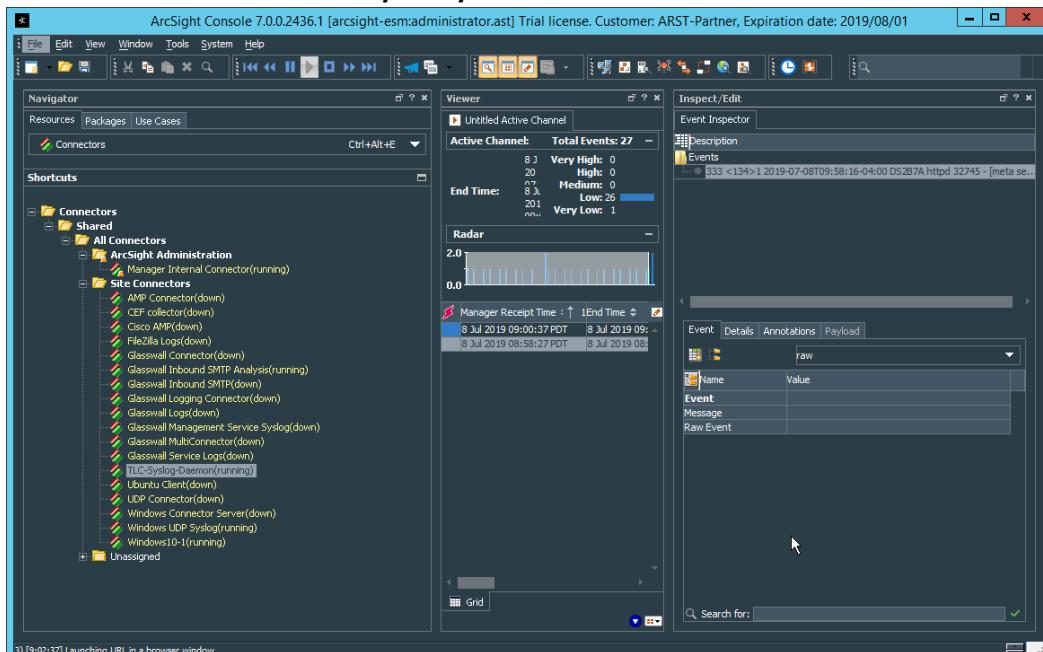
3029

3030

3031

19. Click **OK**.

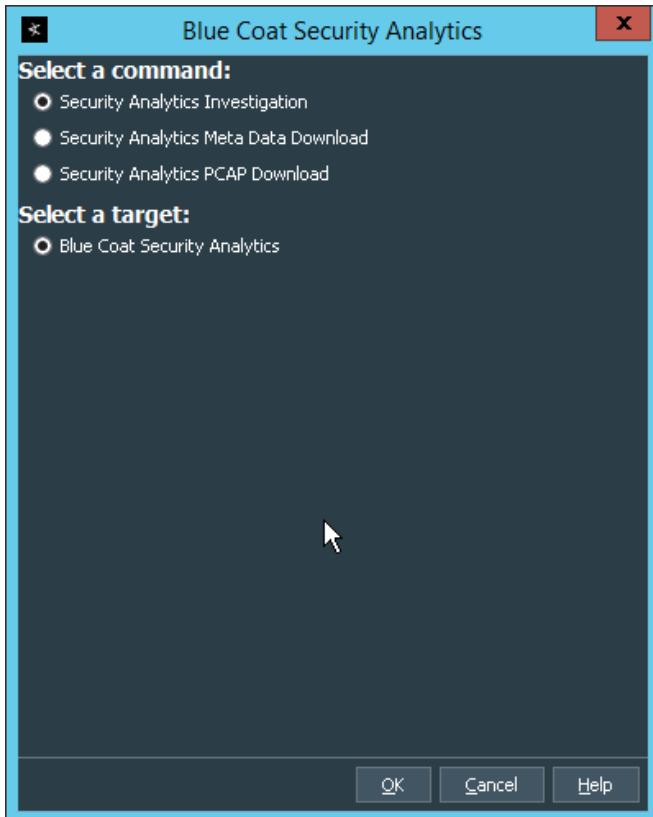
20. To verify the functionality, right-click an event in any channel, and select **Integration Commands > Blue Coat Security Analytics**.



3032

3033

21. Select **Security Analytics Investigation**.



3034  
3035        22. Click **OK**. This will open Security Analytics in the browser and perform a packet search based on  
3036        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**

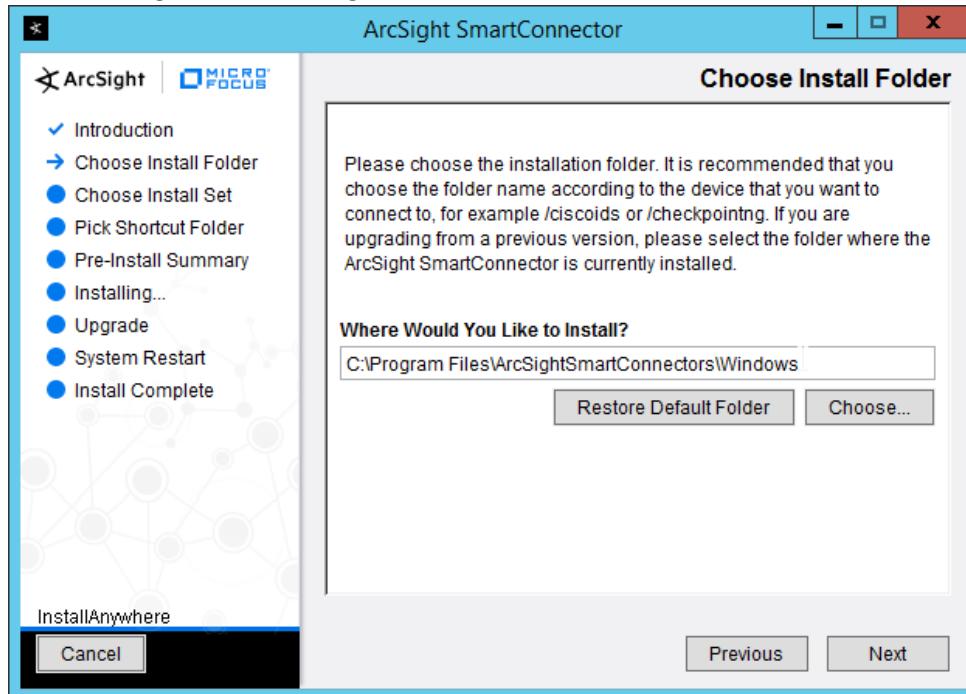
3040        1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on the same server as **Glasswall FileTrust**.

3041

3042

3043

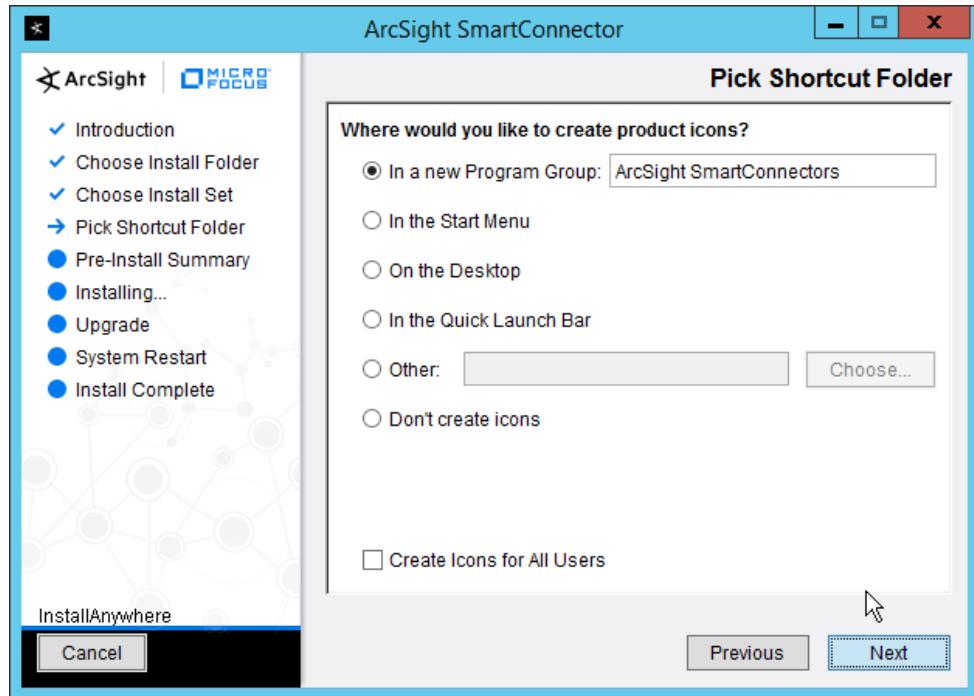
2. Click **Next**.
3. Enter *C:\Program Files\ArcSightSmartConnectors\Windows*.



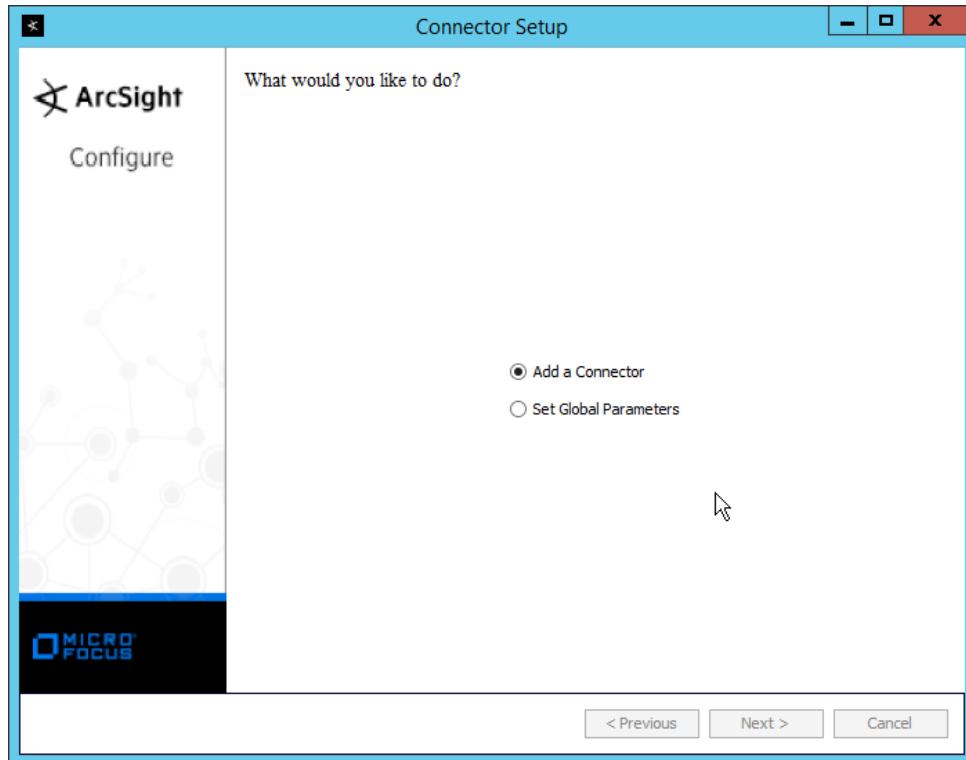
3044

3045

4. Click **Next**.

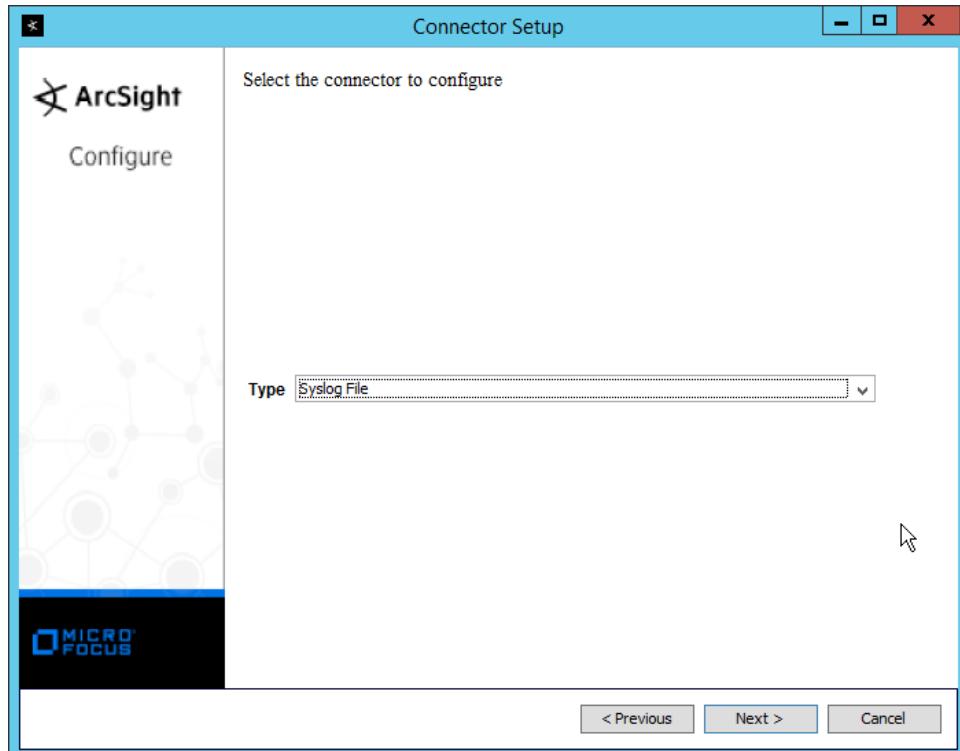


3046  
3047 5. Click **Next**.  
3048 6. Click **Install**.  
3049 7. Select **Add a Connector**.



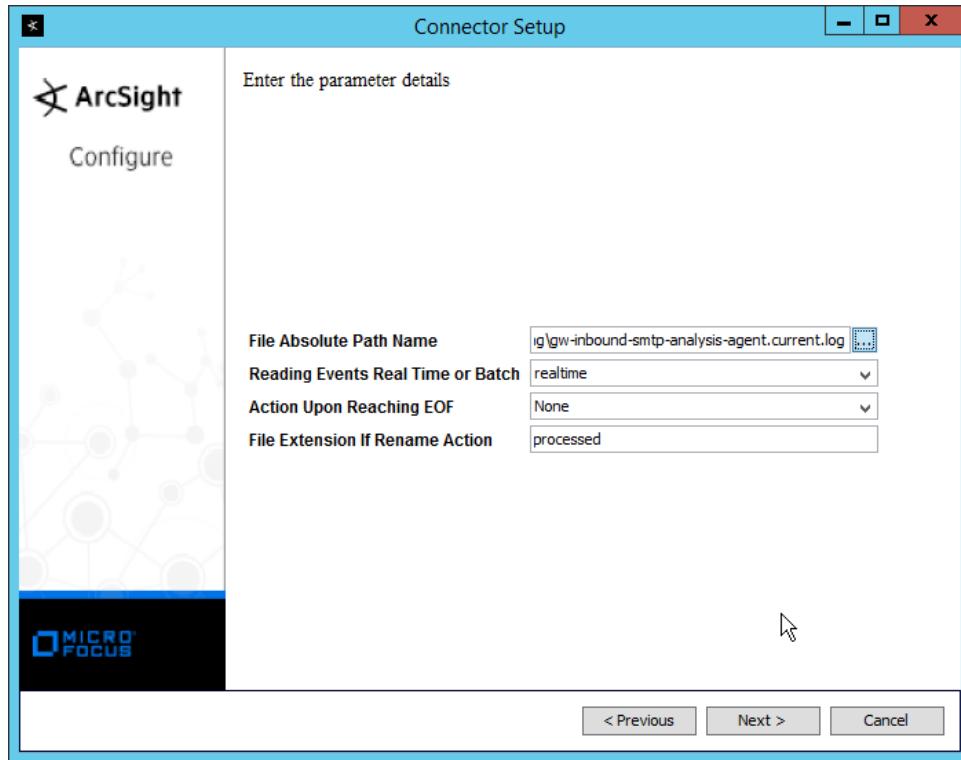
3050  
3051  
3052

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



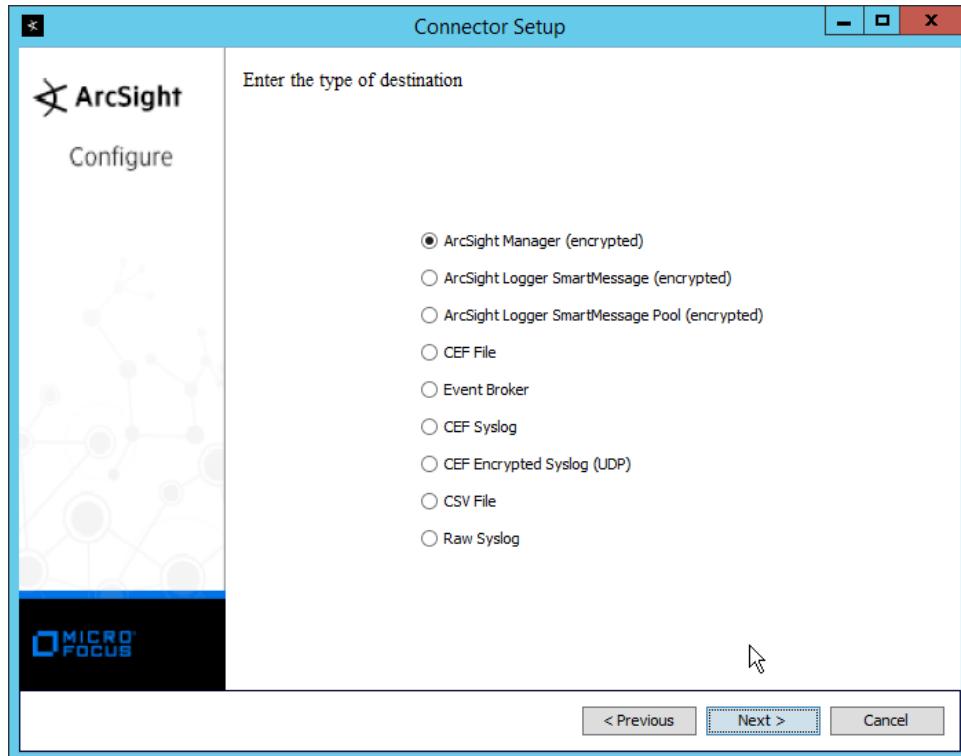
3053  
3054  
3055

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



3056  
3057  
3058

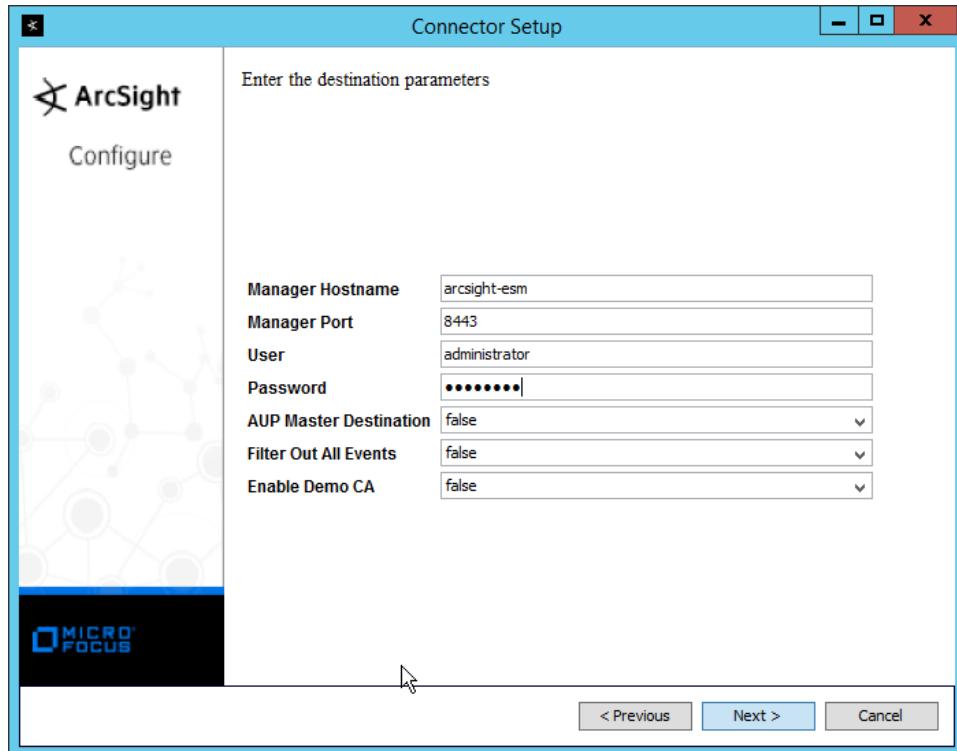
12. Click **Next**.
13. Select **ArcSight Manager (encrypted)**.



3059  
3060  
3061

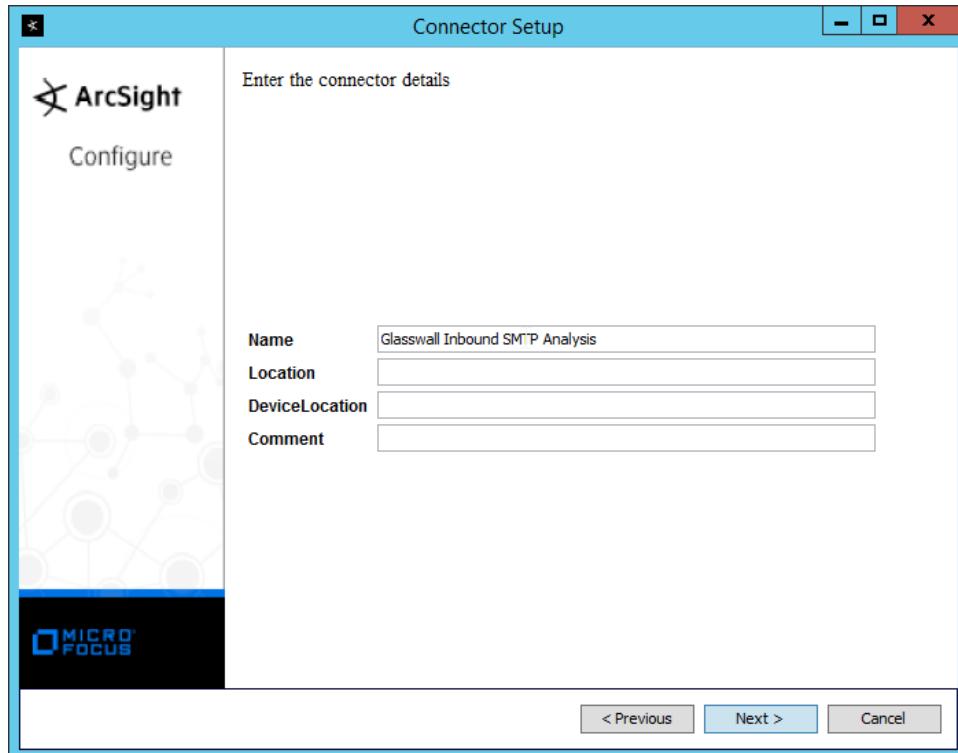
14. Click **Next**.

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



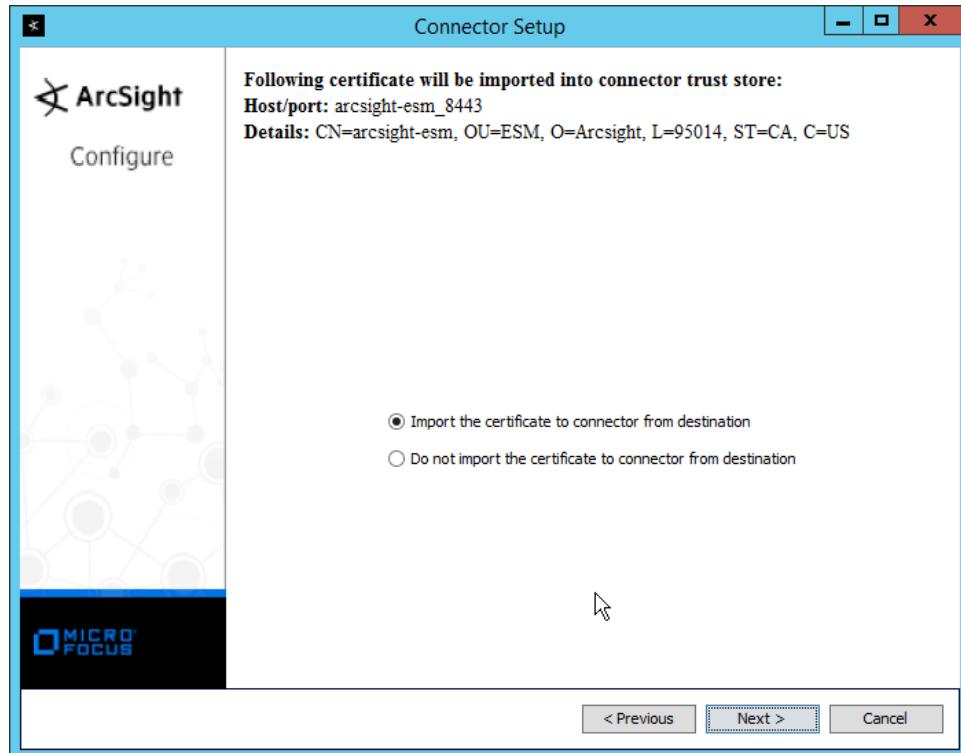
3062  
3063  
3064

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



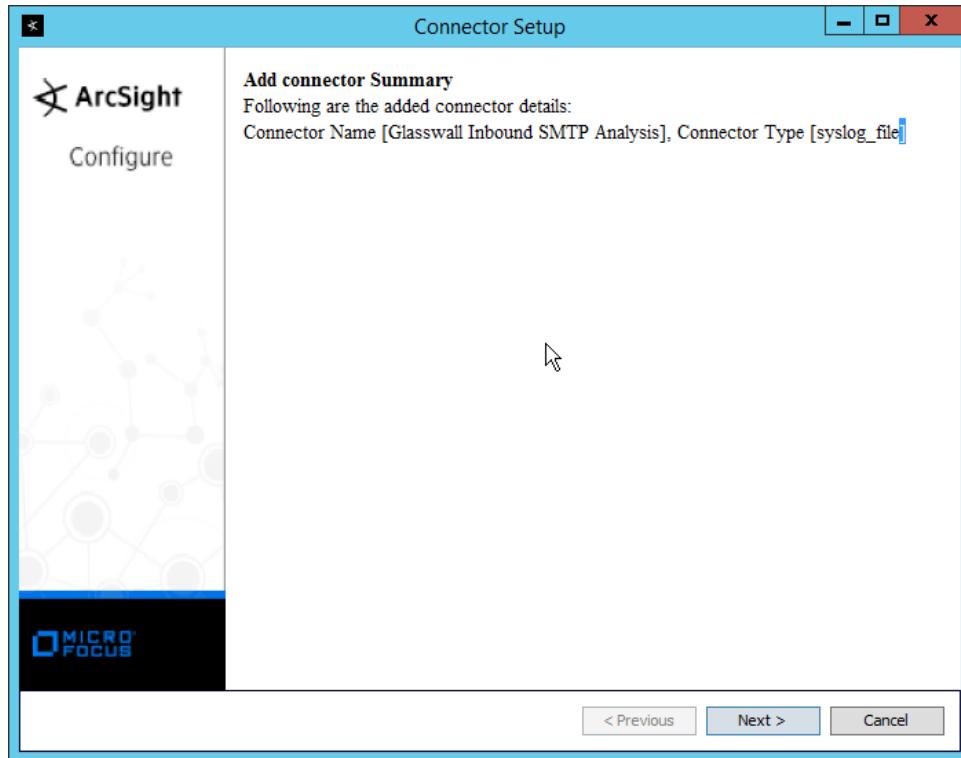
3065  
3066  
3067

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



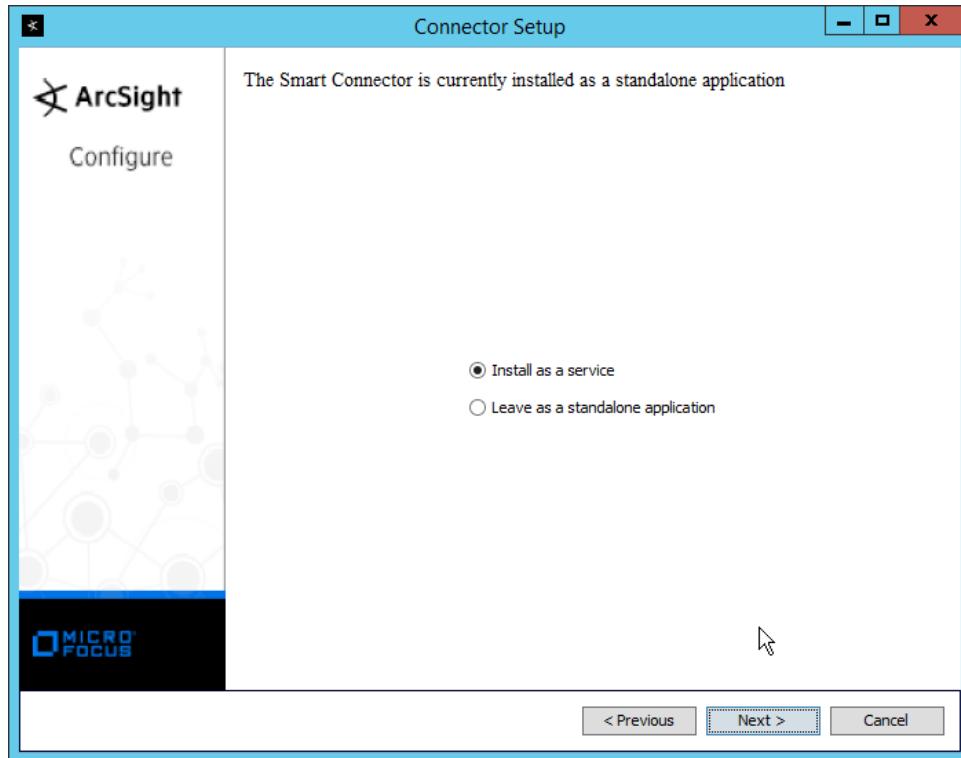
3068  
3069

20. Click **Next**.



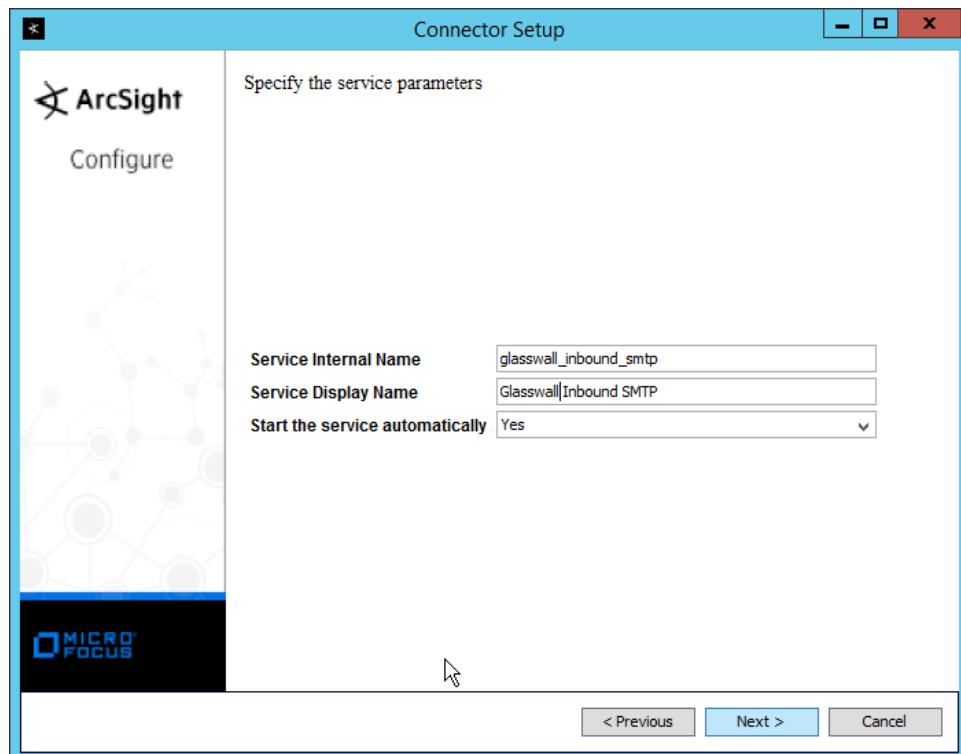
3070  
3071  
3072

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



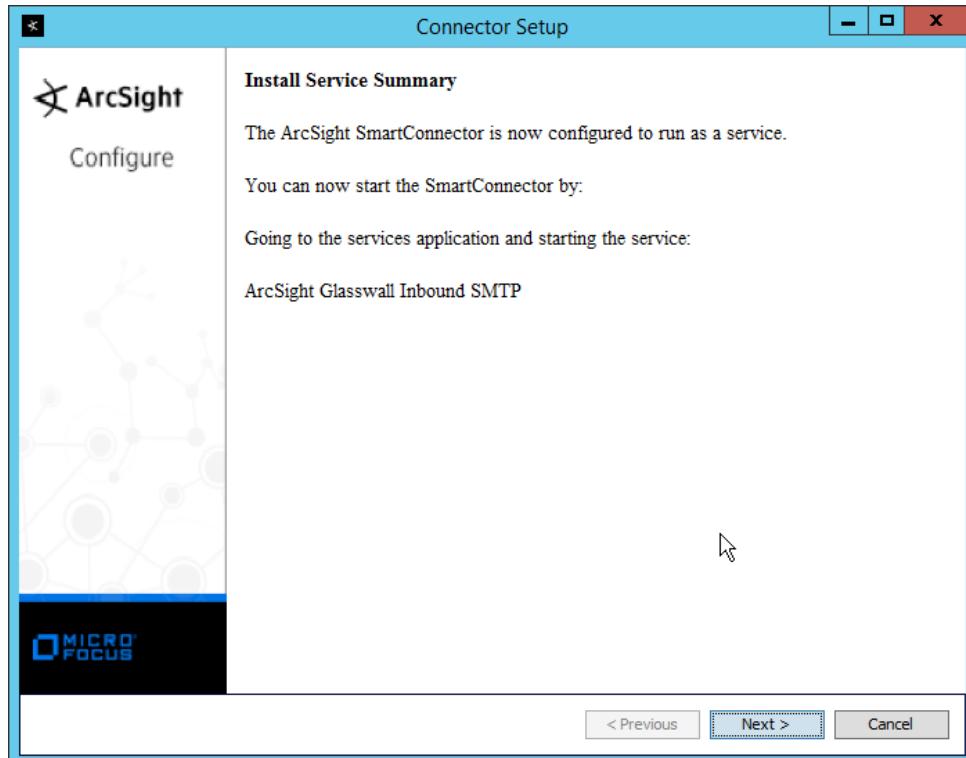
3073  
3074  
3075  
3076

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**.

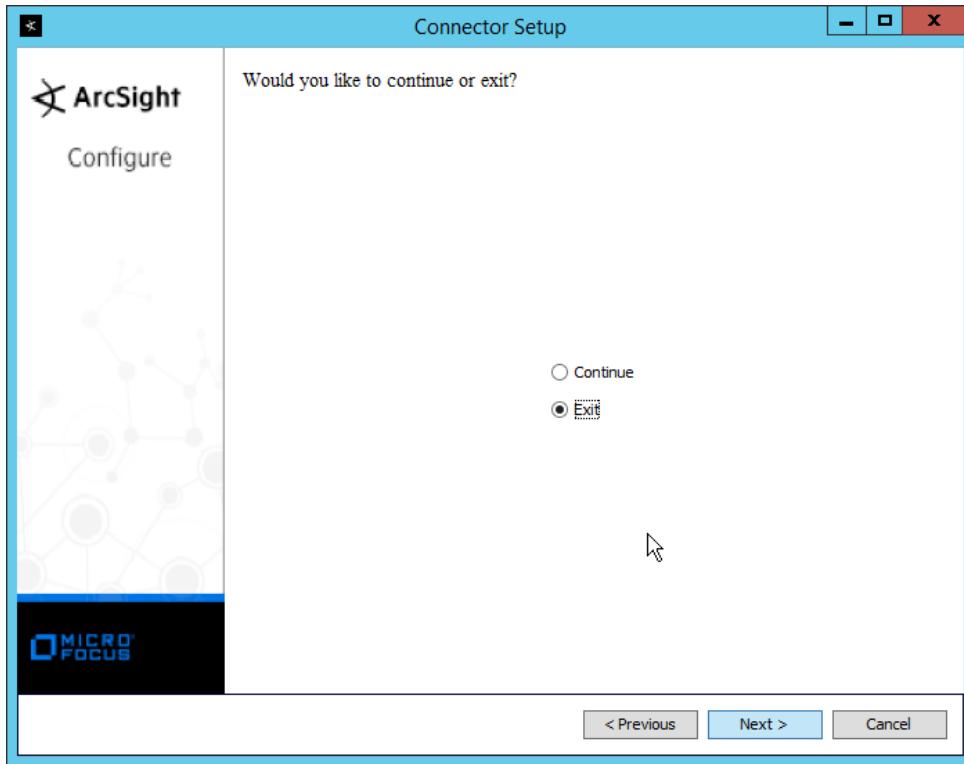


3079  
3080  
3081

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

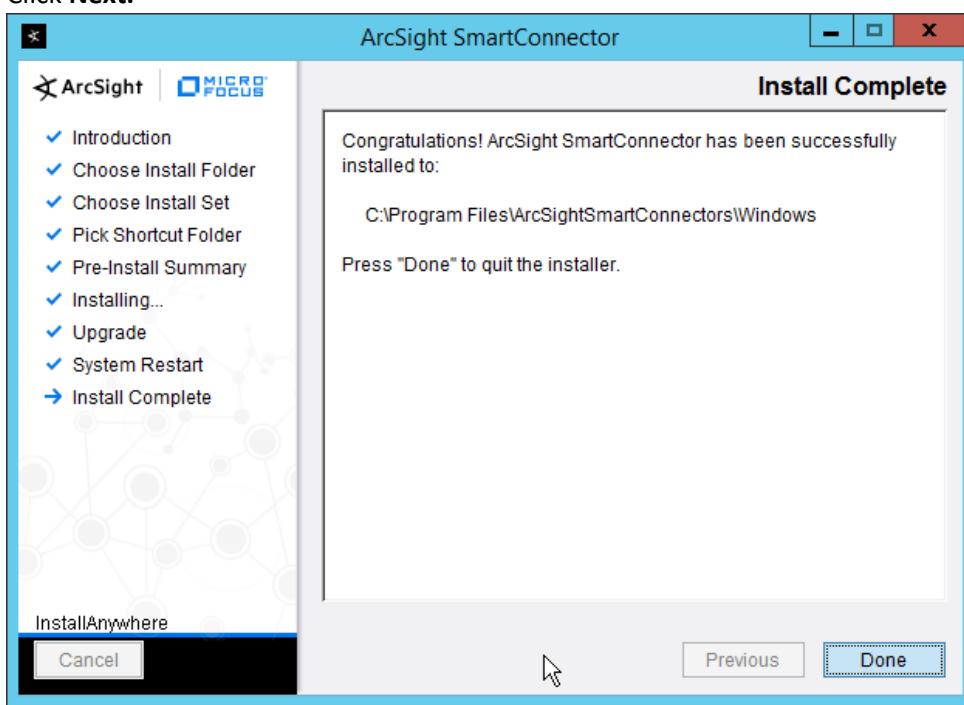
3082  
3083

28. Click **Next**.



3084  
3085

29. Click **Done**.



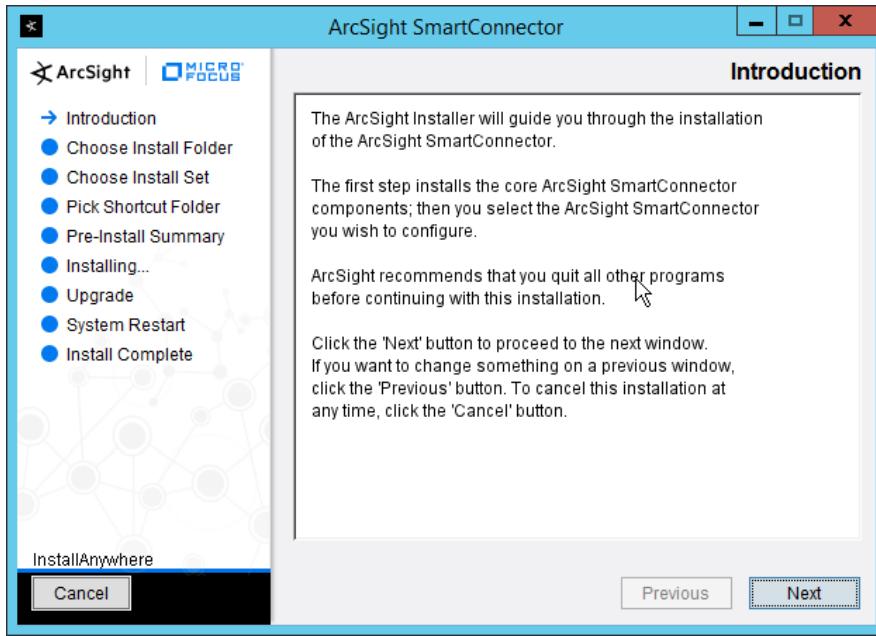
- 3086        30. Repeat steps 1-29 for the other three “current” log files in *C:\Logging*, with the following  
 3087        caveats:
- 3088            a. Replace *C:\Program Files\ArcSightSmartConnectors\Windows* with a different folder  
 3089              name for each connector.
- 3090            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

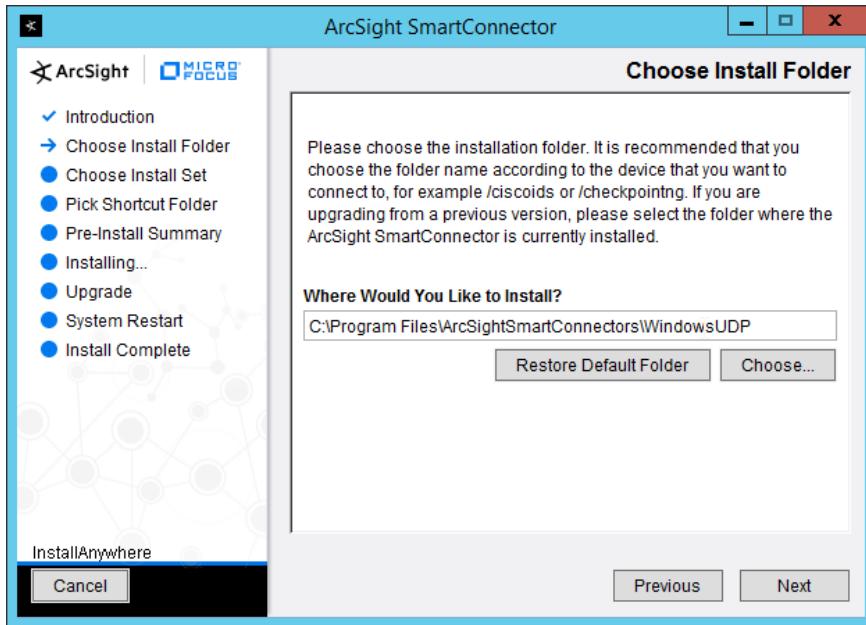
- 3101        1. Run **ArcSight-7.9.0.8084.0-Connector-Win64.exe** on any server except the one running **Cisco**  
 3102        **Stealthwatch**.



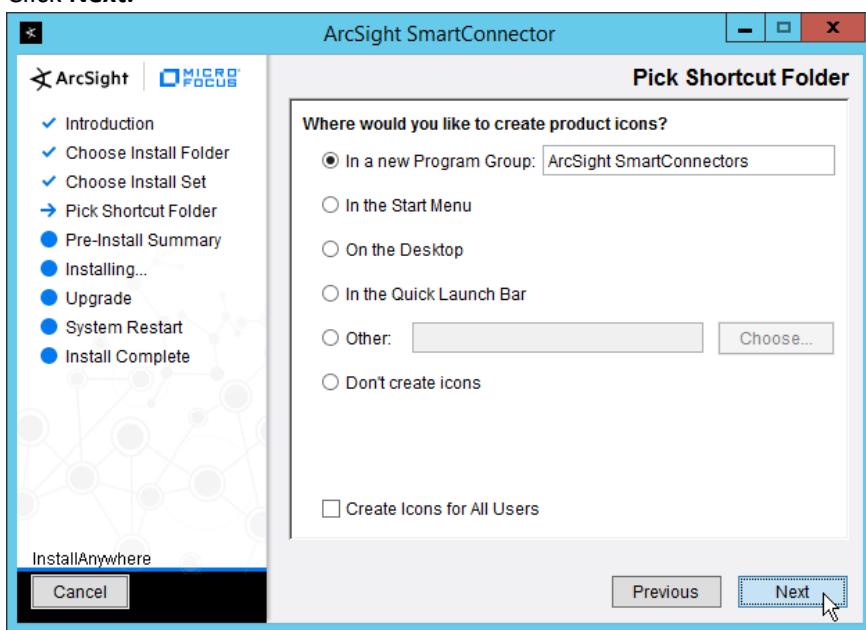
- 3103        2. Click **Next**.  
 3104        3. Enter *C:\Program Files\ArcSightSmartConnectors\WindowsUDP*.

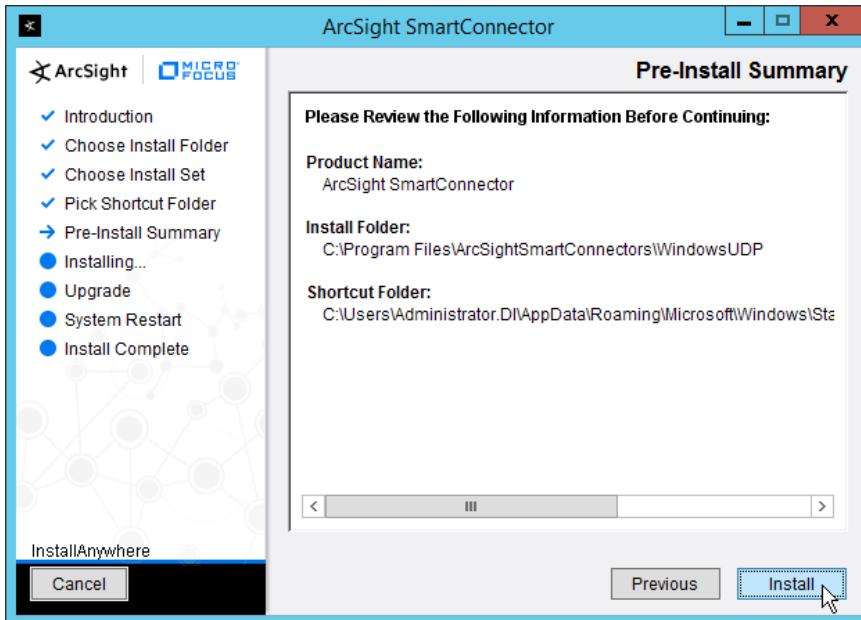
3106  
3107

4. Click Next.

3108  
3109

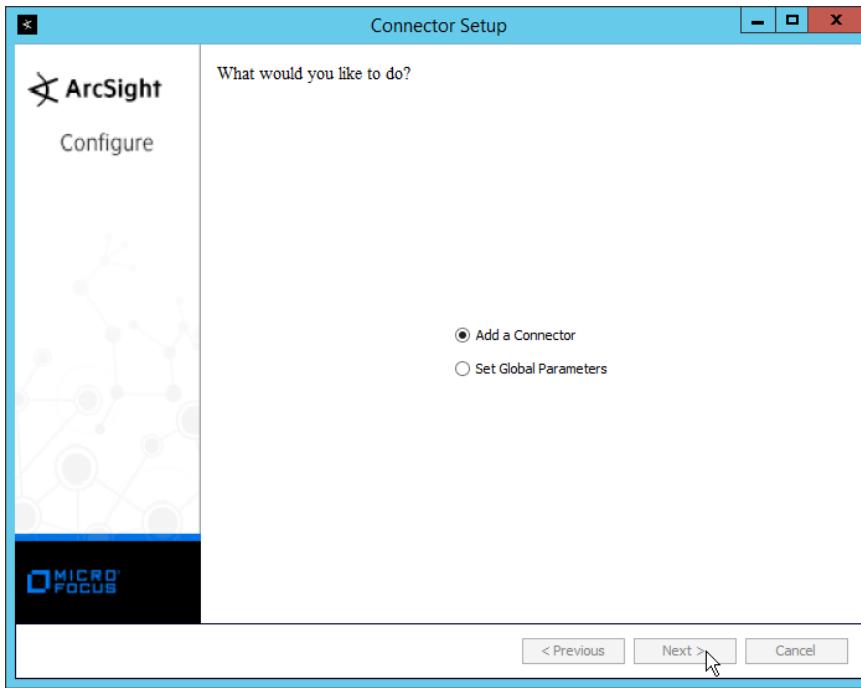
5. Click Next.





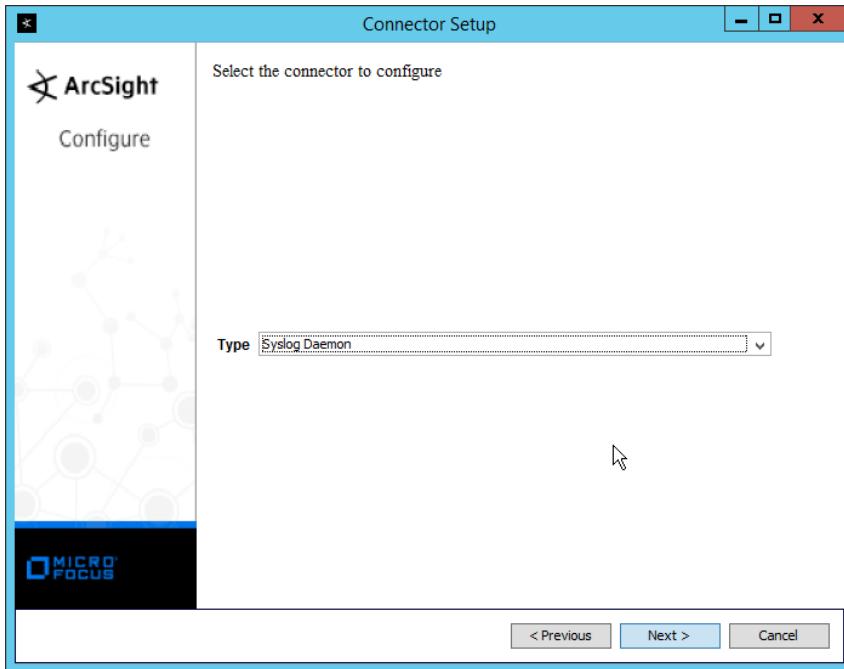
3110  
3111  
3112

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



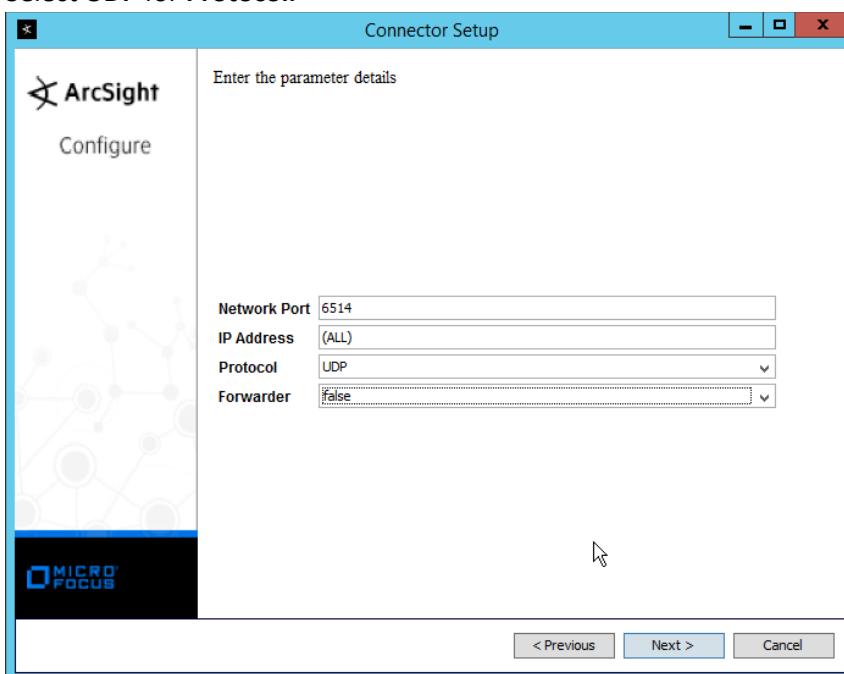
3113  
3114  
3115

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**.

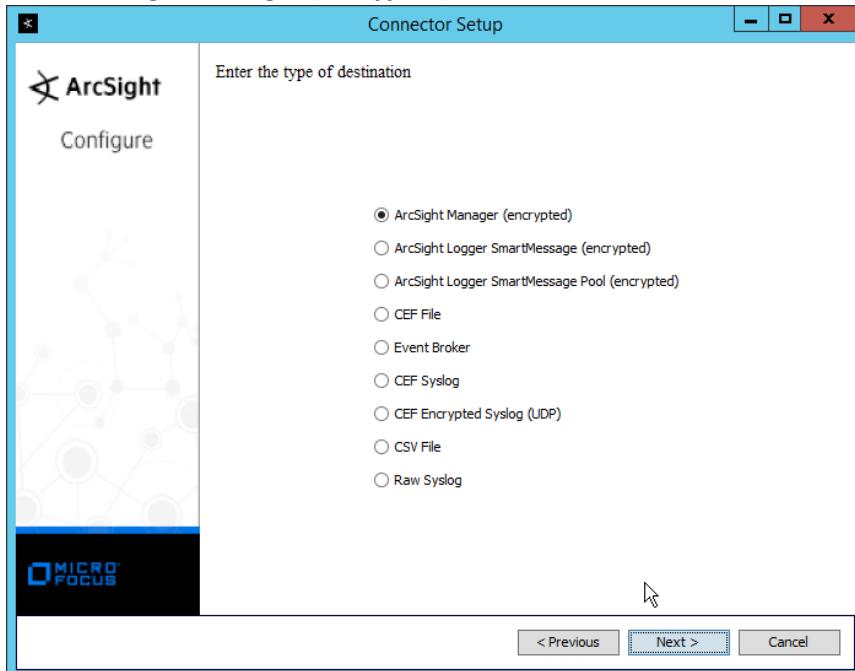


3121  
3122

13. Click **Next**.

3123

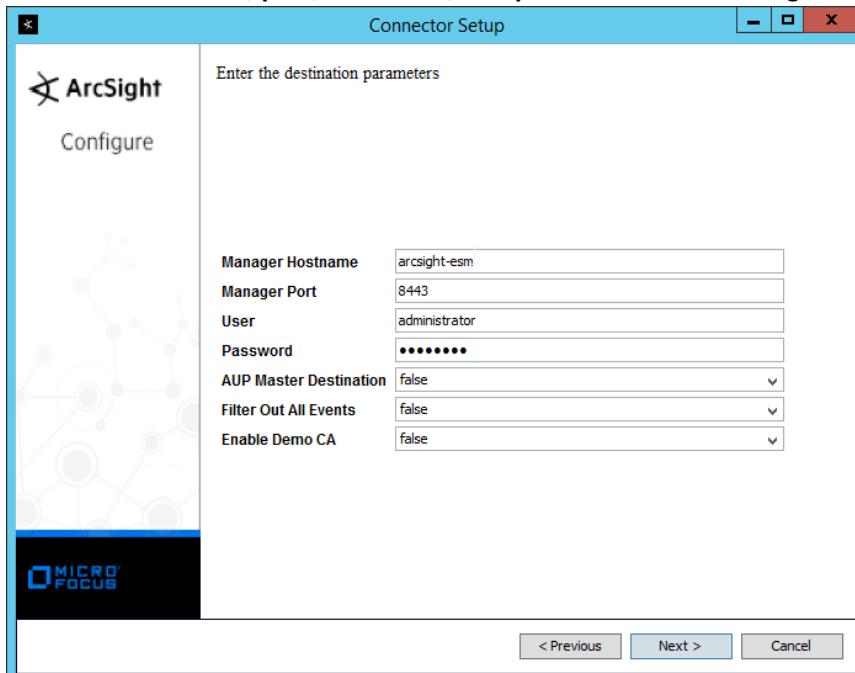
## 14. Select ArcSight Manager (encrypted).



3124

15. Click Next.

3125

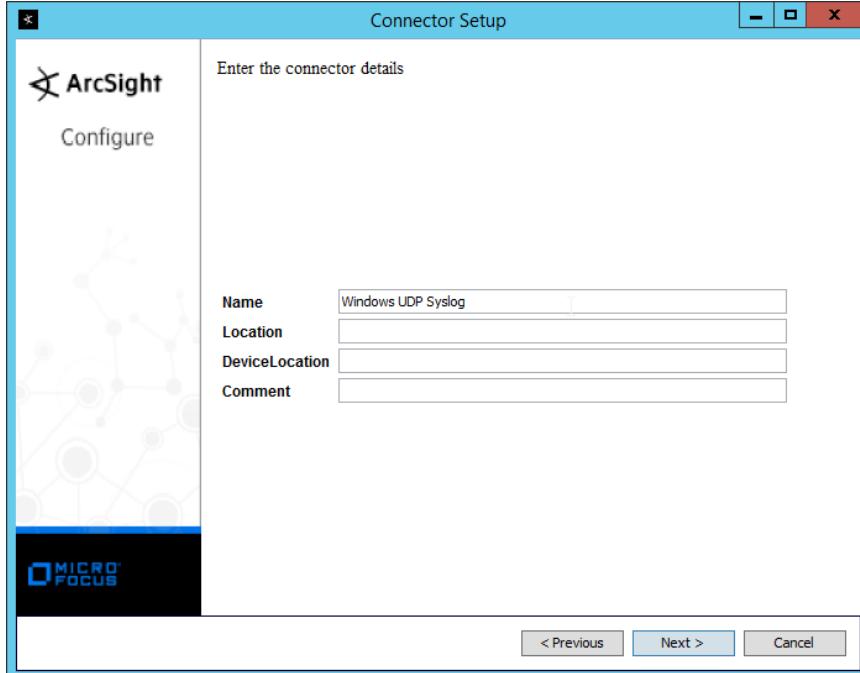
16. Enter the **hostname**, **port**, **username**, and **password** for the ArcSight ESM server.

3127

17. Click Next.

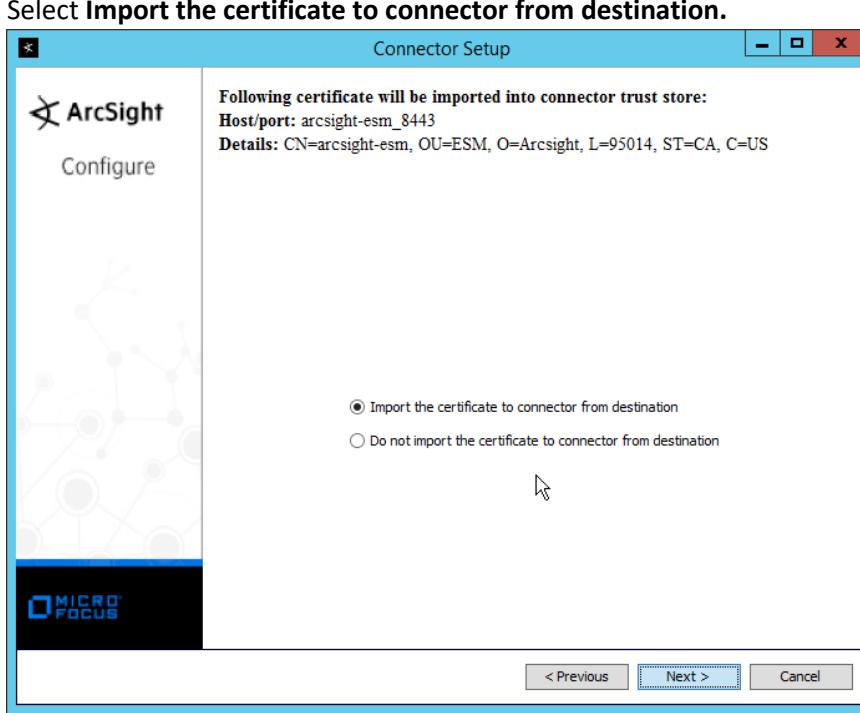
3128

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

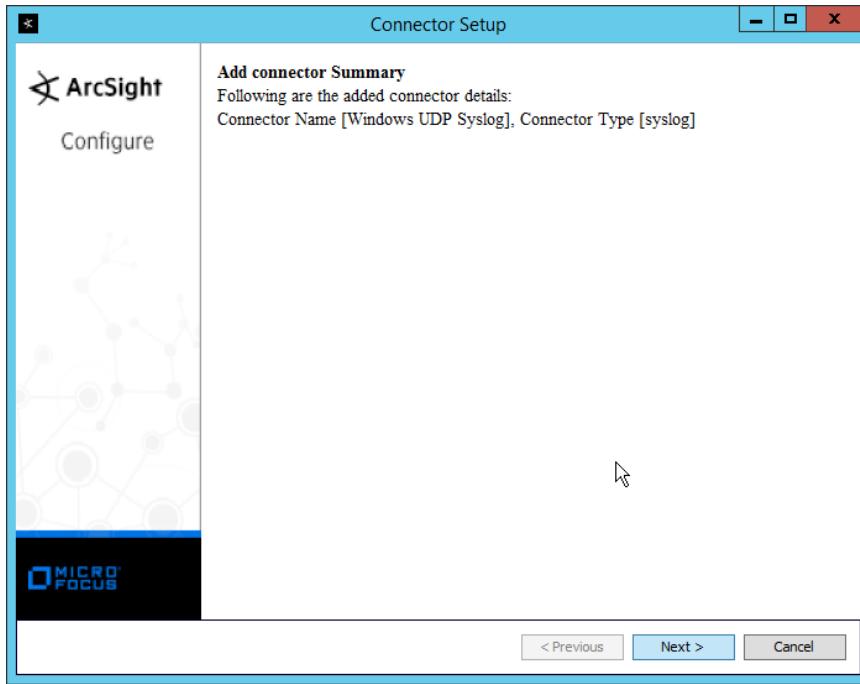


- 3130 19. Click **Next**.

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

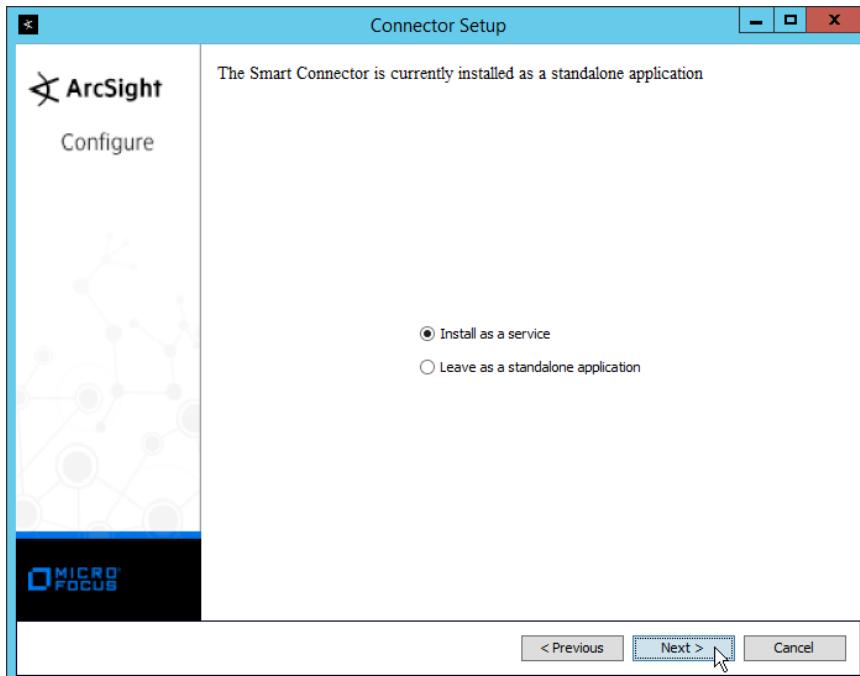


- 3133 21. Click **Next**.



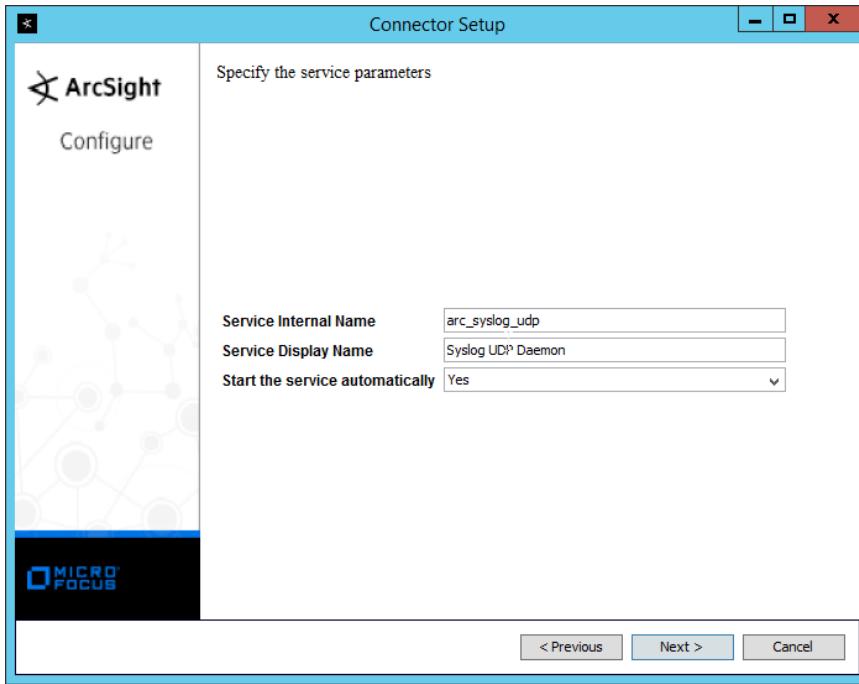
3135      22. Click **Next**.

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



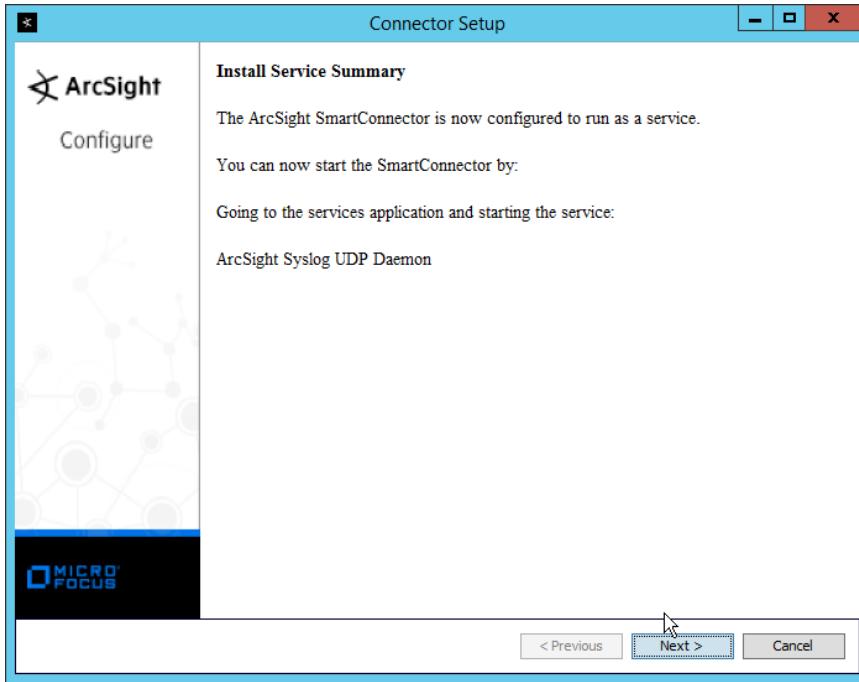
3137      24. Click **Next**.

3138      25. Enter a service name and display name.



3139

26. Click **Next**.

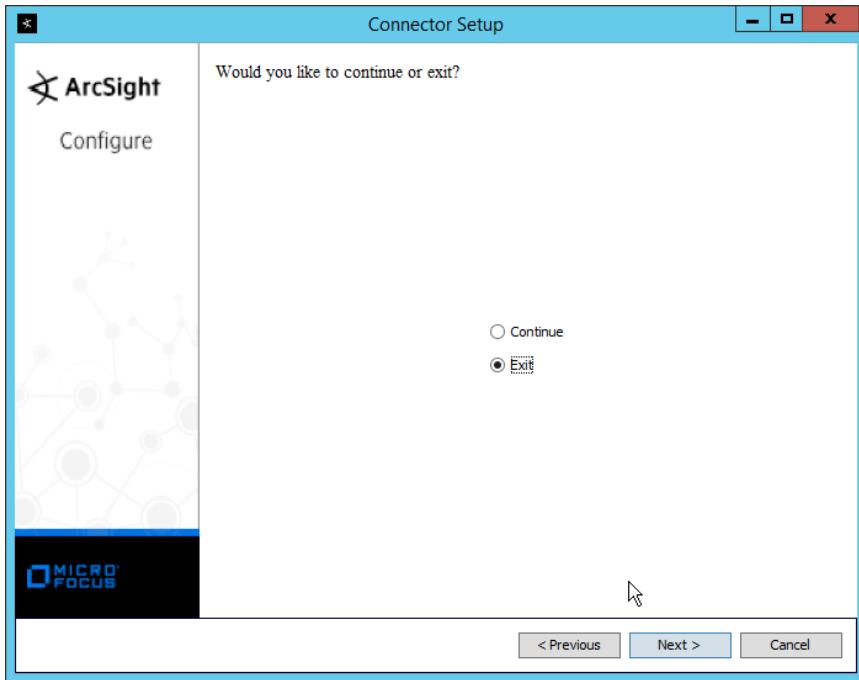


3140

27. Click **Next**.

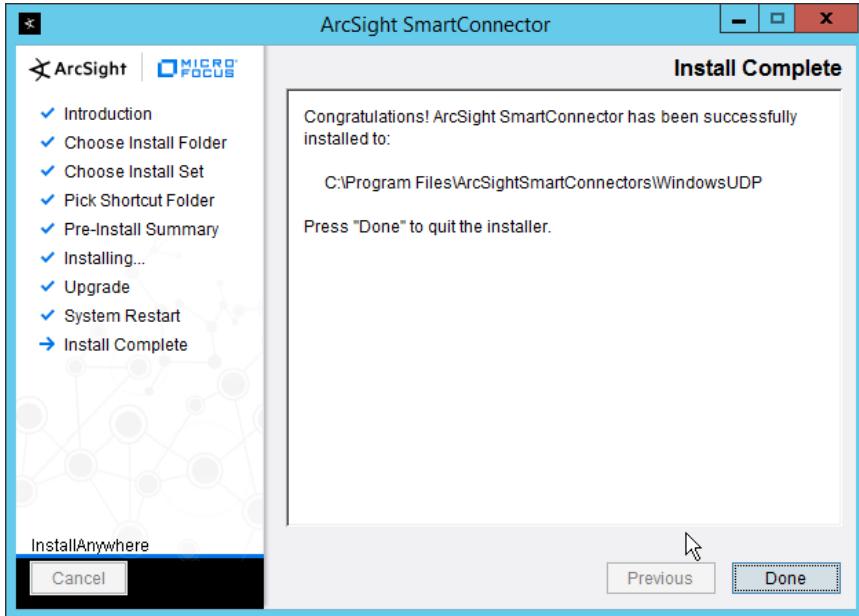
3141

28. Select **Exit**.



3142

29. Click **Next**.

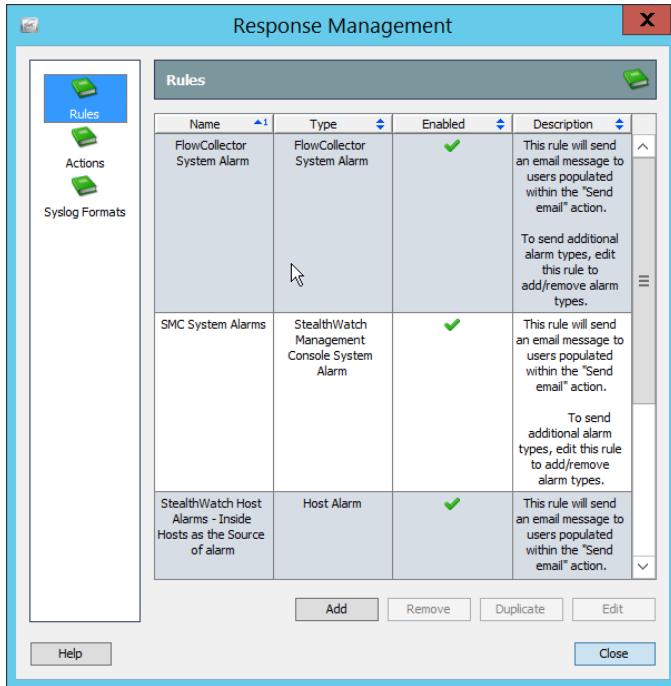


3143

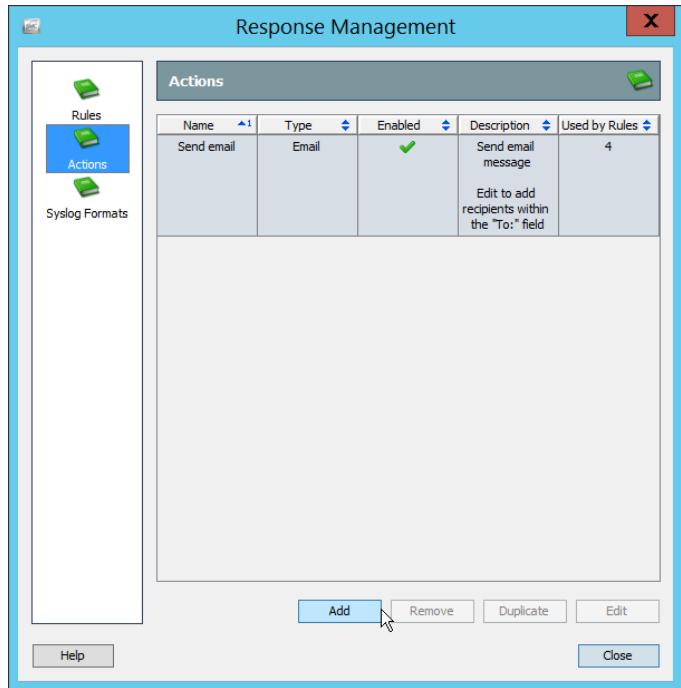
30. Click **Done**.

### 3144 2.25.2 Configure Cisco Stealthwatch

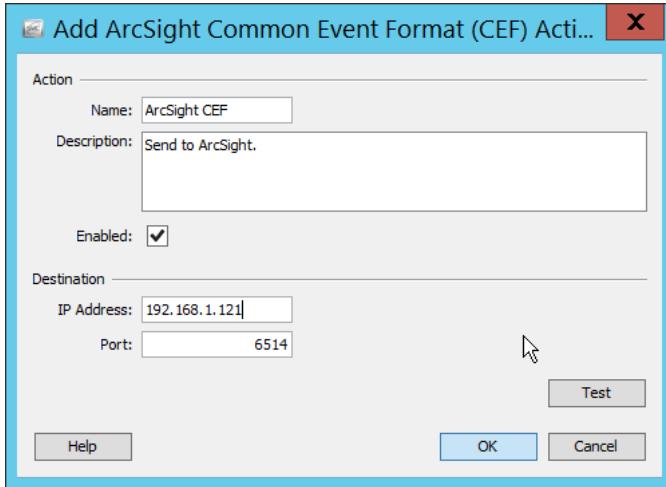
- 3145 1. Log in to the **Cisco Stealthwatch Management Console** desktop interface. (This can be  
3146 downloaded from the web interface and run using **javaws.exe**. You may need to add the site to  
3147 your Java exceptions in **Control Panel > Java**.)  
3148 2. Click **Configuration > Response 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 message.
- 3158

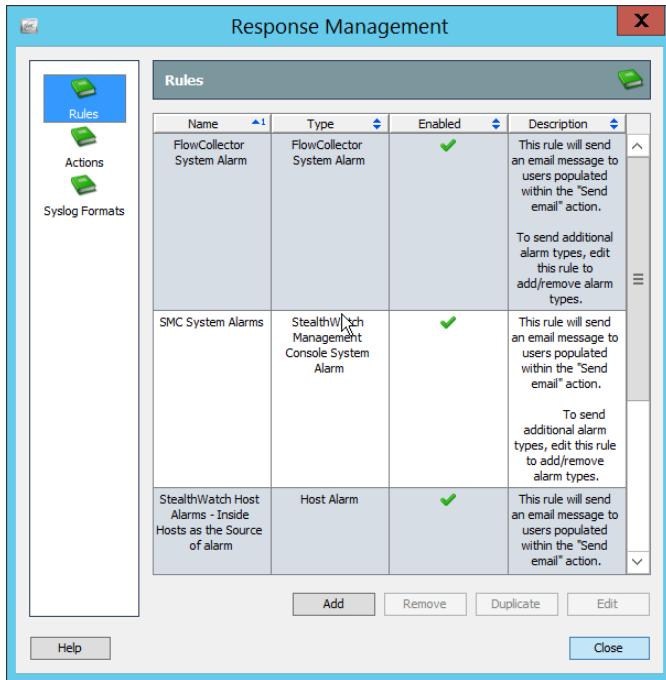


3159 12. Click **OK**.

3160 13. Verify that the action was created properly.

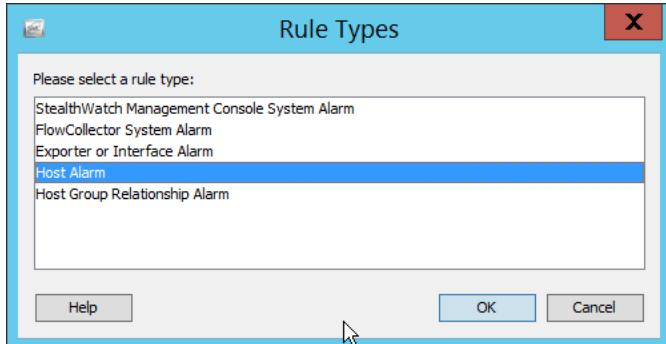
| Actions      |                                    |         |                                                                     |               |
|--------------|------------------------------------|---------|---------------------------------------------------------------------|---------------|
| Name         | Type                               | Enabled | Description                                                         | Used by Rules |
| ArcSight CEF | Arcsight Common Event Format (CEF) | ✓       | Send to ArcSight.                                                   |               |
| Send email   | Email                              | ✓       | Send email message<br>Edit to add recipients within the "To:" field | 4             |

3161 14. Click **Rules**.



3162 15. Click **Add**.

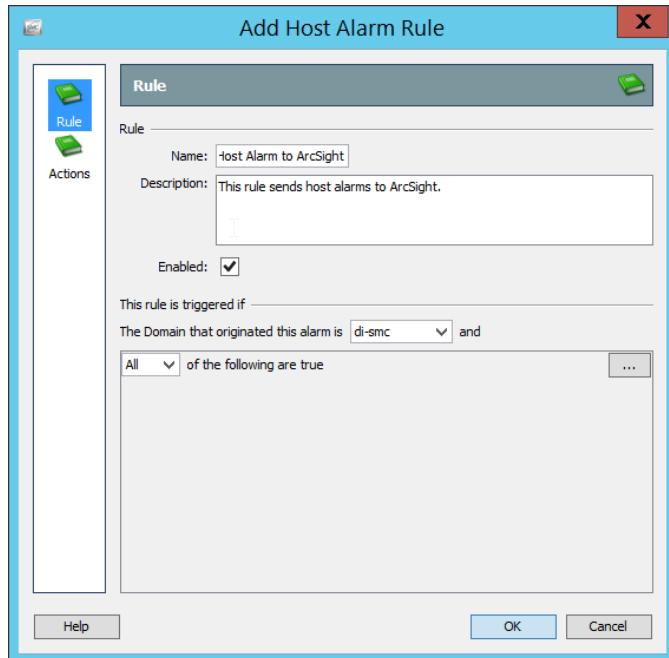
3163 16. Select **Host Alarm**.



3164 17. Click **OK**.

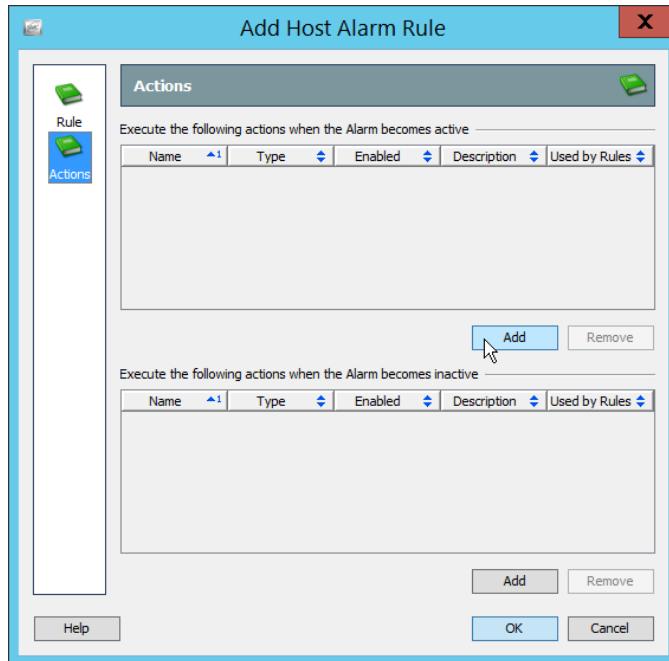
3165 18. Enter a **name**.

3166 19. Enter a **description**.



3167

## 20. Click Actions.

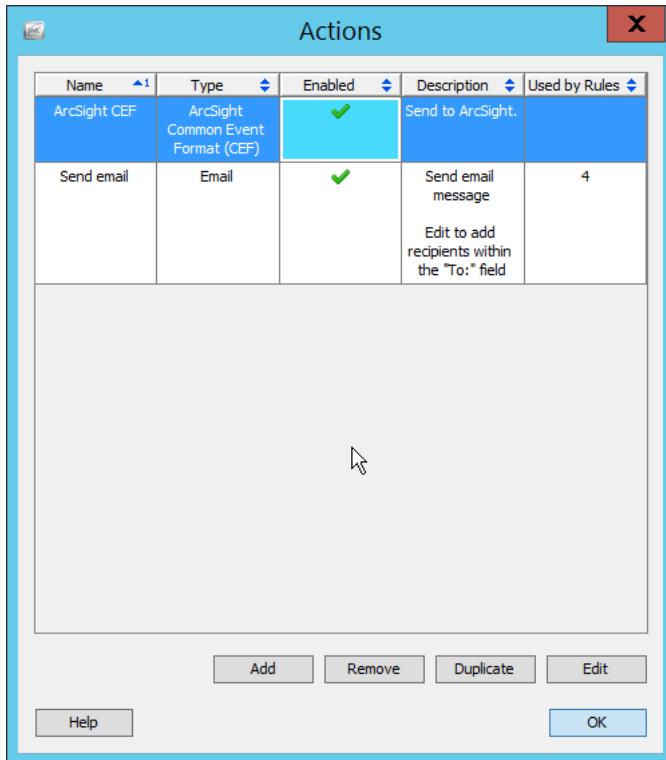


3168

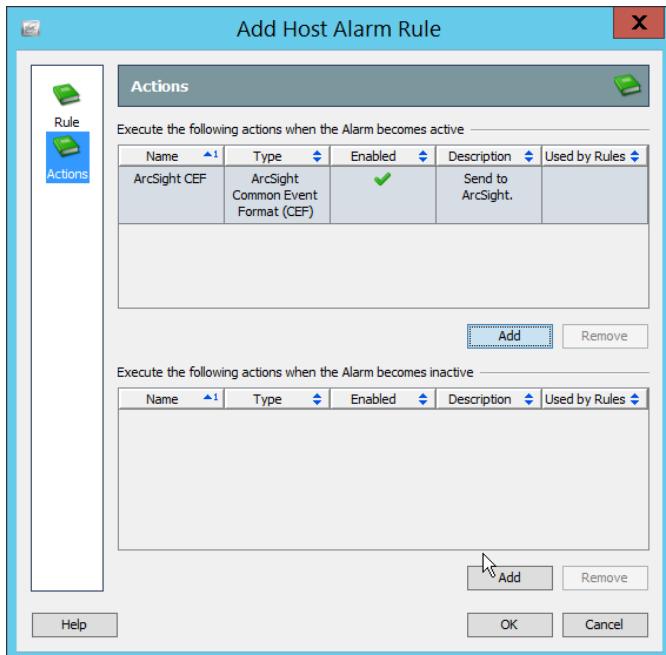
21. Click the Add button for the top section; this adds an action when the alarm becomes active.

3169

22. Select the ArcSight CEF rule you just created.



3170

23. Click **OK**.

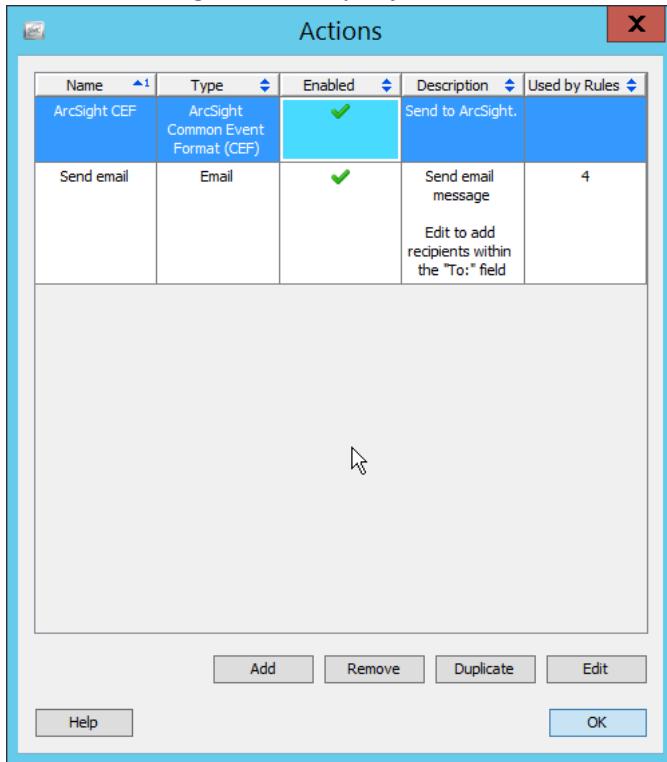
3171

24. Click the **Add** button for the bottom section; this adds an action when the alarm becomes inactive.

3172

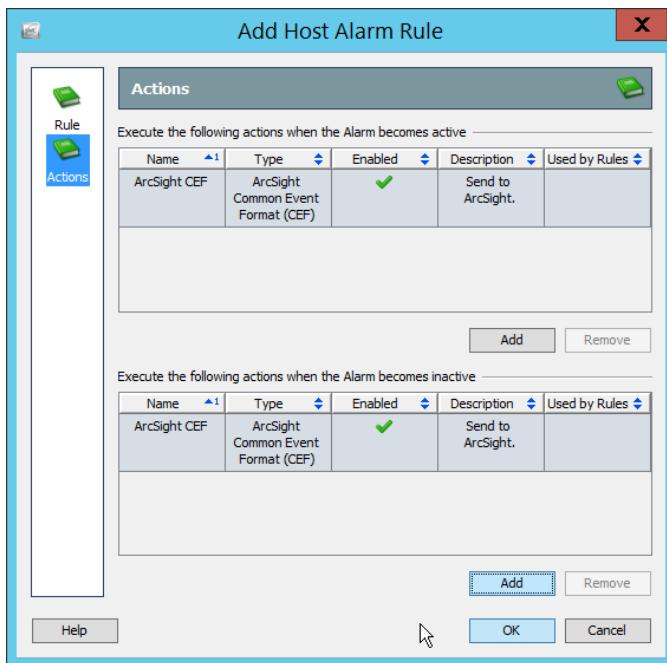
3173

25. Select the ArcSight CEF rule you just created.

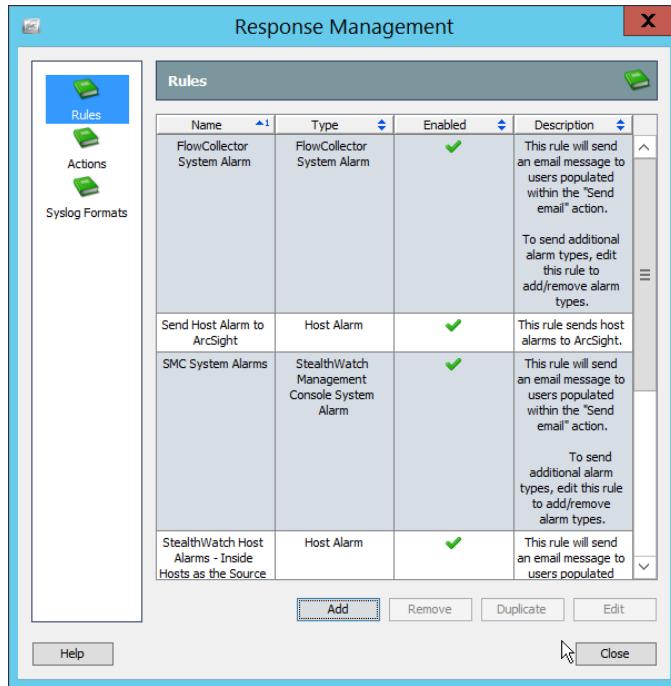


3174

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                |