

NIST SPECIAL PUBLICATION 1800-3

Attribute Based Access Control

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

Bill Fisher
Norm Brickman
Prescott Burden
Santos Jha
Brian Johnson
Andrew Keller
Ted Kolovos
Sudhi Umarji
Sarah Weeks

SECOND DRAFT

This publication is available free of charge from:
<https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control>



NIST SPECIAL PUBLICATION 1800-3

Attribute Based Access Control

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

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Norm Brickman
Prescott Burden
Santos Jha
Brian Johnson
Andrew Keller
Ted Kolovos
Sudhi Umarji
Sarah Weeks
*The MITRE Corporation
McLean, VA*

SECOND DRAFT

September 2017



U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Kent Rochford, Acting Undersecretary of Commerce for Standards and Technology and Director

NIST SPECIAL PUBLICATION 1800-3A

Attribute Based Access Control

Volume A: Executive Summary

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Norm Brickman
Prescott Burden
Santos Jha
Brian Johnson
Andrew Keller
Ted Kolovos
Sudhi Umarji
Sarah Weeks
The MITRE Corporation
McLean, VA

September 2017

SECOND DRAFT

This publication is available free of charge from:
<https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control>



1 Executive Summary

2 Traditionally, granting or revoking access to information technology (IT) systems or other networked
3 assets requires an administrator to manually enter information into a database—perhaps within several
4 systems. This method is inefficient and does not scale as organizations grow, merge, or reorganize.
5 Further, this approach may not be best for preserving privacy and security: all users of a database have
6 access to all its information, or administrators must limit access by constructing groups with specific
7 permissions.

8 Attribute based access control (ABAC) is an advanced method for managing access rights for people and
9 systems connecting to networks and assets. Its dynamic capabilities offer greater efficiency, flexibility,
10 scalability, and security than traditional access control methods, without burdening administrators or
11 users.

12 Despite ABAC's advantages and federal guidance that comprehensively defines ABAC and the
13 considerations for enterprise deployment ([NIST Special Publication 800-162](#)), adoption has been slow. In
14 response, the National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of
15 Standards and Technology (NIST), developed an example of an advanced access control system. Our
16 ABAC solution can manage access to networked resources more securely and efficiently, and with
17 greater granularity than traditional access management. It enables the appropriate permissions and
18 limitations for the same information system for each user based on individual attributes, and allows for
19 permissions to multiple systems to be managed by a single platform, without a heavy administrative
20 burden.

21 Our approach uses commercially available products that can be included alongside your current
22 products in your existing infrastructure.

23 This example solution is packaged as a “How To” guide that demonstrates implementation of standards-
24 based cybersecurity technologies in the real world. It can save organizations research and proof-of-
25 concept costs for mitigating risk through the use of context for access decisions.

26 CHALLENGE

27 Enterprises face the continual challenge of providing access control mechanisms for subjects requesting
28 access to corporate resources (e.g., applications, networks, systems, and data). The growth and
29 distributed nature of enterprise resources, increasing diversity in users, credentials, and access needs, as
30 well as the need to share information among stakeholders that are not managed directly by the
31 enterprise, has given rise to the demand for an access control system that enables fine-grained access
32 decisions based on a range of users, resources, and environmental conditions.

33 Consider a patient submitting a health insurance claim. A claims examiner needs to know just billing and
34 diagnostic codes and a few pieces of demographic data in order to permit reimbursement. Interacting
35 with the same system, the patient’s doctor needs to verify that the diagnosis and referral information is
36 for the correct patient, but does not need to see payment or address information. The patient needs
37 access to the claim’s status, while the patient’s employer only needs to see the number of claims

38 submitted by the employee. The insurance company provides a single service, claims processing, but
39 each user of the service has different access needs.

40 An advanced method of access management would increase security and efficiency by seamlessly
41 limiting some users' views to more granular data. It would enable the appropriate permissions and
42 limitations for the same information system for each user based on individual attributes, and allow for
43 permissions to multiple systems to be managed by a single platform, without a heavy administrative
44 burden.

45 **SOLUTION**

46 This document details our approach in developing a standards-based ABAC solution. Through
47 discussions with identity and access management (IdAM) experts and collaborating technology partners,
48 the NCCoE developed a set of security characteristics required to meet the IdAM risks facing today's
49 enterprises. The NCCoE mapped security characteristics to standards and best practices from NIST and
50 other standards organizations, then used products from our technology partners as modules in an end-
51 to-end example solution that mitigates IdAM risks.

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

58 **RISKS**

59 Access control systems implement a process for defining security policy and regulating access to
60 resources such that only authorized entities are granted access according to that policy. They are
61 fundamental to mitigating the risk of unauthorized access from malicious external users and insider
62 threats, as well as acts of misfeasance. In the absence of a robust access control system, enterprises
63 struggle to control and audit access to their most sensitive data and risk the loss or exposure of critical
64 assets, loss of trust in employees and from customers, and harm to brand reputation.

65 As technology pervades all business processes, access control systems must support increasing diversity
66 in users, credentials, and access needs, including digital identities from external security domains. This
67 increases the overhead associated with managing access control systems and introduces increased risk
68 of unauthorized access as organizational policies escalate in complexity.

69 **BENEFITS**

70 Our example implementation:

- 71 ■ allows products and capabilities to be adopted on a component-by-component basis, or as a
72 whole
- 73 ■ supports organizations with a diverse set of users and access needs, reducing the risks of
74 “privilege creep” (a user obtains access levels beyond those needed), and creating efficiencies in
75 the provisioning of accesses

- 76 ▪ reduces the number of identities managed by the enterprise, thereby reducing costs associated
77 with those management activities
- 78 ▪ enables a wider range of risk-mitigation decisions by allowing organizations to define attribute-
79 based policy on subjects and objects, and by using a variety of environmental decisions
- 80 ▪ supports business collaboration by allowing the enterprise to accept federated identities and
81 eliminating the need to pre-provision access for identities being federated
- 82 ▪ supports the centralization of auditing and access policy management, creating efficiencies of
83 policy management and reducing the complexity of regulatory compliance

84 **SHARE YOUR FEEDBACK**

85 You can view or download the guide at <https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control>. Help the NCCoE make this guide better by sharing your thoughts with us as you read the
86 guide. If you adopt this solution for your own organization, please share your experience and advice
87 with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so
88 we encourage organizations to share lessons learned and best practices for transforming the processes
89 associated with implementing this guide. To provide comments or to learn more by arranging a
90 demonstration of this example implementation, contact the NCCoE at abac-nccoe@nist.gov.

92 **TECHNOLOGY PARTNERS/COLLABORATORS**

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



98

99 Certain commercial entities, equipment, products, or materials may be identified by name or company
100 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an
101 experimental procedure or concept adequately. Such identification is not intended to imply special
102 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it
103 intended to imply that the entities, equipment, products, or materials are necessarily the best available
104 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 applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology.

LEARN MORE

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

NIST SPECIAL PUBLICATION 1800-3B

Attribute Based Access Control

Volume B:
Approach, Architecture, and Security Characteristics

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Norm Brickman
Prescott Burden
Santos Jha
Brian Johnson
Andrew Keller
Ted Kolovos
Sudhi Umarji
Sarah Weeks
The MITRE Corporation
McLean, VA

September 2017

SECOND DRAFT

This publication is available free of charge from:
<https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control>



DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-3b, Natl. Inst. Stand. Technol. Spec. Publ. 1800-3b, 48 pages, September 2017, CODEN: NSPUE2

FEEDBACK

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

Comments on this publication may be submitted to: abac-nccoe@nist.gov.

Public comment period: September 20, 2017 through October 20, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).

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

1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

2 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards
3 and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and
4 academic institutions work together to address businesses' most pressing cybersecurity issues. This
5 public-private partnership enables the creation of practical cybersecurity solutions for specific
6 industries, as well as for broad, cross-sector technology challenges. Through consortia under
7 Cooperative Research and Development Agreements (CRADAs), including technology partners—from
8 Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards
9 and best practices to develop modular, easily adaptable example cybersecurity solutions using
10 commercially available technology. The NCCoE documents these example solutions in the NIST Special
11 Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the
12 steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by
13 NIST in partnership with the State of Maryland and Montgomery County, Md.

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

16 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

26 **ABSTRACT**

27 Enterprises rely upon strong access control mechanisms to ensure that corporate resources (e.g.,
28 applications, networks, systems, and data) are not exposed to anyone other than an authorized user. As
29 business requirements change, enterprises need highly flexible access control mechanisms that can
30 adapt. The application of attribute based policy definitions enables enterprises to accommodate a
31 diverse set of business cases. This NCCoE practice guide details a collaborative effort between the
32 NCCoE and technology providers to demonstrate a standards-based approach to attribute based access
33 control (ABAC).

34 This guide discusses potential security risks facing organizations, benefits that may result from the
35 implementation of an ABAC system, and the approach the NCCoE took in developing a reference
36 architecture and build. It includes a discussion of major architecture design considerations, an
37 explanation of security characteristic achieved by the reference design, and a mapping of security
38 characteristics to applicable standards and security control families.

39 For parties interested in adopting all or part of the NCCoE reference architecture, this guide includes a
 40 detailed description of the installation, configuration, and integration of all components.

41 **KEYWORDS**

42 *access control; access management; attribute provider; authentication; authorization; identity
 43 federation; identity management; identity provider; relying party*

44 **ACKNOWLEDGMENTS**

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

Name	Organization
Nate Lesser	NIST National Cybersecurity Center of Excellence
Paul Timmel	NIST National Cybersecurity Center of Excellence
Paul Grassi	NIST National Strategy for Trusted Identities in Cyberspace
Mike Garcia	NIST National Strategy for Trusted Identities in Cyberspace
Naomi Lefkovitz	NIST National Strategy for Trusted Identities in Cyberspace
Rene Peralta	NIST National Strategy for Trusted Identities in Cyberspace
Dave Ferriaolo	NIST Computer Security Division
Vincent Hu	NIST Computer Security Division
Roger Wiggenstam	NextLabs Inc
John Conduit	NextLabs Inc
Srikanth Karanam	NextLabs Inc
Adam Madlin	Symantec Corporation
Steve Kruse	Symantec Corporation
Steve Schmalz	RSA
Ben Smith	RSA

Name	Organization
Andrew Whelchel	RSA
Chris Leggett	Ping Identity
Paul Fox	Microsoft Corporation
Derek Keatley	Microsoft Corporation
Hemma Prafullchandra	Hytrust
John McLeese	Hytrust
Dave Cox	ID/Dataweb
Chris Donovan	ID/Dataweb
Pete Romness	Cisco
Kevin McFadden	Cisco
John Eppish	Cisco
Chris Ceppi	Situational Corporation

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

Technology Partner/Collaborator	Build Involvement
Ping Identity	PingFederate Federation Server
NextLabs	Entitlements Management Policy Enforcement Point
Microsoft	Policy Controller Policy decision point
RSA	Control Center Policy Administration Point
Symantec	Active Directory

Technology Partner/Collaborator	Build Involvement
<u>Cisco</u>	SharePoint

Contents

51	1 Summary.....	1
52	1.1 Challenge	1
53	1.2 Solution.....	2
54	1.3 Risks	2
55	1.4 Benefits.....	2
56	2 How to Use This Guide	3
57	2.1 Typographical Conventions	5
58	3 Introduction	5
59	3.1 Background.....	6
60	3.2 ABAC and RBAC Considerations	6
61	3.3 ABAC Leveraging Identity Federation	7
62	3.4 Security Standards.....	9
63	4 Approach.....	12
64	4.1 Audience.....	12
65	4.2 Scope	12
66	4.3 Assumptions	12
67	4.3.1 Modularity	12
68	4.3.2 Business Policy Language.....	12
69	4.3.3 Attribute Semantics and Syntax.....	13
70	4.3.4 Attribute Provenance.....	13
71	4.3.5 Trust Relationships for Identity Federation	13
72	4.3.6 Human Resources Database/Identity Proofing	13
73	4.3.7 Technical Implementation	13
74	4.3.8 Limited Scalability Testing.....	14
75	4.4 Risk Assessment	14
76	4.4.1 Strategic Risks	14
77	4.4.2 Tactical Risks	15
78	4.4.3 Security Control Map	17
79	4.5 Technologies.....	18
80	5 Architecture	22
81	5.1 Overview.....	22

83	5.1.1	User Authentication and the Creation of an Authentication Context.....	22
84	5.1.2	Federation of a User Identity and Attributes.....	22
85	5.1.3	Fine-Grained Access Control through a PEP Closely Coupled with the Application	22
86	5.1.4	The Creation of Attribute-Based Policy Definitions	22
87	5.1.5	Secondary Attribute Requests	22
88	5.1.6	Allow RP Access Decisions on External Identities without the Need for Pre-Provisioning	23
90	5.2	ABAC Architecture Considerations.....	23
91	5.2.1	Industry Standards.....	23
92	5.2.2	PEP Placement	23
93	5.2.3	PDP Distribution.....	24
94	5.2.4	Multi-Vendor.....	24
95	5.2.5	Caching.....	24
96	5.2.6	Data Tagging	24
97	5.2.7	Policy Authoring.....	24
98	5.2.8	Attribute Retrieval	24
99	5.3	Technology and Architecture of the NCCoE Build.....	25
100	5.3.1	Architecture Diagram and Components	25
101	5.3.2	UML Diagram	28
102	5.3.3	NCCoE Design Considerations.....	32
103	5.4	Security Characteristics	34
104	5.5	Features and Benefits.....	35
105	5.5.1	Support Organizations with a Diverse Set of Users and Access Needs	35
106	5.5.2	Reduce the Number of Identities Managed by the Enterprise.....	35
107	5.5.3	Enable a Wider Range of Risk Decisions	35
108	5.5.4	Support Business Collaboration.....	35
109	5.5.5	Centralize Auditing and Access Policy Management.....	36
110	Appendix A	List of Acronyms	37
111	Appendix B	References.....	39

112 **List of Figures**

113	Figure 5-1 ABAC Build 1 Architecture	26
114	Figure 5-2 UML Sequence Diagram	29
115	Figure 5-3 Secondary Attribute Request Flow	31

116 **List of Tables**

117	Table 3-1 Related Security Standards and Best Practices	9
118	Table 4-1 Use Case Security Characteristics Mapped to Relevant Standards and Controls.....	17
119	Table 4-2 Security Characteristics Mapped to Relevant Build Products	19

1 Summary

Traditionally, granting or revoking access to information technology (IT) systems or other networked assets requires an administrator to manually enter information into a database—perhaps within several systems. This method is inefficient and does not scale as organizations grow, merge, or reorganize. Further, this approach may not be best for preserving privacy and security: all users of a database have access to all its information, or administrators must limit access by constructing groups with specific permissions.

Attribute based access control (ABAC) is an advanced method for managing access rights for people and systems connecting to networks and assets. Its dynamic capabilities offer greater efficiency, flexibility, scalability, and security than traditional access control methods, without burdening administrators or users.

Despite ABAC's advantages and federal guidance that comprehensively defines ABAC and the considerations for enterprise deployment [1], adoption has been slow. In response, the National Cybersecurity Center of Excellence (NCCoE), part of the National Institute of Standards and Technology (NIST), developed an example of an advanced access control system. Our ABAC solution can manage access to networked resources more securely and efficiently, and with greater granularity than traditional access management. It enables the appropriate permissions and limitations for the same information system for each user based on individual attributes, and allows for permissions to multiple systems to be managed by a single platform, without a heavy administrative burden.

Our approach uses commercially available products that can be included alongside your current products in your existing infrastructure.

This example solution is packaged as a “How To” guide that demonstrates implementation of standards-based cybersecurity technologies in the real world. It can save organizations research and proof-of-concept costs for mitigating risk through the use of context for access decisions.

1.1 Challenge

Enterprises face the continual challenge of providing access control mechanisms for subjects requesting access to corporate resources (e.g., applications, networks, systems, and data). The growth and distributed nature of enterprise resources, increasing diversity in users, credentials, and access needs, as well as the need to share information among stakeholders that are not managed directly by the enterprise, has given rise to the demand for an access control system that enables fine-grained access decisions based on a range of users, resources, and environmental conditions.

Consider a patient submitting a health insurance claim. A claims examiner needs to know just billing and diagnostic codes and a few pieces of demographic data in order to permit reimbursement. Interacting with the same system, the patient’s doctor needs to verify that the diagnosis and referral information is for the correct patient, but does not need to see payment or address information. The patient needs access to the claim’s status, while the patient’s employer only needs to see the number of claims submitted by the employee. The insurance company provides a single service, claims processing, but each user of the service has different access needs.

158 An advanced method of access management would increase security and efficiency by seamlessly
159 limiting some users' views to more granular data. It would enable the appropriate permissions and
160 limitations for the same information system for each user based on individual attributes, and allow
161 for permissions to multiple systems to be managed by a single platform, without a heavy
162 administrative burden.

163 **1.2 Solution**

164 This document details our approach in developing a standards-based ABAC solution. Through
165 discussions with identity and access management (IdAM) experts and collaborating technology partners,
166 the NCCoE developed a set of security characteristics required to meet the IdAM risks facing today's
167 enterprises. The NCCoE mapped security characteristics to standards and best practices from NIST and
168 other standards organizations, then used products from our technology partners as modules in an end-
169 to-end example solution that mitigates IdAM risks.

170 **1.3 Risks**

171 Access control systems implement a process for defining security policy and regulating access to
172 resources such that only authorized entities are granted access according to that policy. They are
173 fundamental to mitigating the risk of unauthorized access from malicious external users and insider
174 threats, as well as acts of misfeasance. In the absence of a robust access control system, enterprises
175 struggle to control and audit access to their most sensitive data and risk the loss or exposure of critical
176 assets, loss of trust in employees and from customers, and harm to brand reputation.

177 As technology pervades all business processes, access control systems must support increasing diversity
178 in users, credentials, and access needs, including digital identities from external security domains. This
179 increases the overhead associated with managing access control systems and introduces increased risk
180 of unauthorized access as organizational policies escalate in complexity.

181 **1.4 Benefits**

182 Our example implementation:

- 183 ■ allows products and capabilities to be adopted on a component-by-component basis, or as a
184 whole
- 185 ■ supports organizations with a diverse set of users and access needs, reducing the risks of
186 “privilege creep” (a user obtains access levels beyond those needed), and creating efficiencies in
187 the provisioning of accesses
- 188 ■ reduces the number of identities managed by the enterprise, thereby reducing costs associated
189 with those management activities
- 190 ■ enables a wider range of risk-mitigation decisions by allowing organizations to define attribute-
191 based policy on subjects and objects, and by using a variety of environmental decisions
- 192 ■ supports business collaboration by allowing the enterprise to accept federated identities and
193 eliminating the need to pre-provision access for identities being federated

- 194 ■ supports the centralization of auditing and access policy management, creating efficiencies of
195 policy management and reducing the complexity of regulatory compliance

196 2 How to Use This Guide

197 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides
198 users with the information they need to replicate this approach to identity and access management.
199 This reference design is modular and can be deployed in whole or in parts.

200 This guide contains three volumes:

- 201 ■ NIST SP 1800-3a: *Executive Summary*
202 ■ NIST SP 1800-3b: *Approach, Architecture, and Security Characteristics* – what we built and why
203 (you are here)
204 ■ NIST SP 1800-3c: *How-To Guides* – instructions for building the example solution

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

206 **Business decision makers, including chief security and technology officers** will be interested in the
207 *Executive Summary* (*NIST SP 1800-3a*), which describes the:

- 208 ■ challenges enterprises face in implementing and using access control mechanisms
209 ■ example solution built at the NCCoE
210 ■ benefits of adopting the example solution

211 **Technology or security program managers** who are concerned with how to identify, understand, assess,
212 and mitigate risk will be interested in this part of the guide, *NIST SP 1800-3b*, which describes what we
213 did and why. The following sections will be of particular interest:

- 214 ■ [Section 4.4](#), Risk Assessment, provides a description of the risk analysis we performed
215 ■ [Section 4.4.3, Security Control Map](#), maps the security characteristics of this example solution to
216 cybersecurity standards and best practices

217 You might share the *Executive Summary*, *NIST SP 1800-3a*, with your leadership team members to help
218 them understand the importance of adopting standards-based access management approaches to
219 protect your organization's digital assets.

220 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.
221 You can use the How-To portion of the guide, *NIST SP 1800-3c*, to replicate all or parts of the build
222 created in our lab. The How-To guide provides specific product installation, configuration, and
223 integration instructions for implementing the example solution. We do not recreate the product
224 manufacturers' documentation, which is generally widely available. Rather, we show how we
225 incorporated the products together in our environment to create an example solution.

226 This guide assumes that IT professionals have experience implementing security products within the
227 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
228 not endorse these particular products. Your organization can adopt this solution or one that adheres to
229 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing

SECOND DRAFT

230 parts of a solution that would support the deployment of an ABAC system and the corresponding
231 business processes. Your organization’s security experts should identify the products that will best
232 integrate with your existing tools and IT system infrastructure. We hope you will seek products that are
233 congruent with applicable standards and best practices. [Section 4.5, Technologies](#), lists the products we
234 used and maps them to the cybersecurity controls provided by this reference solution.

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

239 **2.1 Typographical Conventions**

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

241

242 **3 Introduction**

243 Any decision to implement ABAC within an organization must begin with a solid “business case.” An
 244 important set of inputs to the business case are the strategic and tactical risks to the organization from
 245 the standpoint of access control, as outlined in Sections [4.4.1](#) and [4.4.2](#). This business case could be an
 246 independent initiative or a component of the organization’s strategic planning cycle. Individual business
 247 units or functional areas typically derive functional or business unit strategies from the overall
 248 organization’s Strategic Plan. The business drivers for any ABAC project must originate in these Strategic
 249 Plans, and the decision to determine if an organization will invest in ABAC by implementing the solution
 250 in this practice guide will be based on the organization’s decision-making process for initiating new
 251 projects.

252 Some organizations use a systems engineering-based approach to the planning and implementation of
253 their IT projects. Organizations wishing to implement an ABAC system should conduct robust
254 requirements development, taking into consideration the operational needs of each system stakeholder.
255 Standards such as ISO/IEC 15288:2015, Systems and software engineering – System life cycle processes
256 [2], and NIST Special Publication (SP) 800-160, Systems Security Engineering: Considerations for a
257 Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [3], provide guidance in
258 this endeavor. With both these standards, organizations can choose to adopt only those sections of the
259 standard that are relevant to their environment and business context.

260 In addition to ABAC, basic read, write, and execute permissions, discretionary access control (DAC),
261 mandatory access control, and RBAC are some of the many access control solutions from which
262 organizations can choose. NIST SP 800-160 recommends a thorough analysis of alternative solution
263 classes accounting for security objectives, considerations, concerns, limitations, and constraints. An
264 analysis of alternatives may conclude that for a particular organization's requirements, RBAC or other
265 access control mechanism are most appropriate. In addition, while NCCoE has not implemented such
266 combinations, some authors have implemented and documented hybrid ABAC-RBAC solutions [4], [5].

267 **3.1 Background**

268 NIST SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*,
269 describes ABAC as a logical access control model that is distinguishable because it controls access to
270 objects by evaluating rules against the attributes of (a) the subject or user requesting access, (b) the
271 target object for which access or a transaction is being requested, and (c) the environment relevant to a
272 request. It continues:

273 “In its most basic form, ABAC relies upon the evaluation of attributes of the subject, attributes
274 of the object, environment conditions, and a formal relationship or access control rule defining
275 the allowable operations for subject-object attribute and environment condition combinations.
276 All ABAC solutions contain these basic core capabilities that evaluate attributes and
277 environment conditions, and enforce rules or relationships between those attributes and
278 environment conditions. ...”

279 The rules or policies that can be implemented in an ABAC model are limited only to the degree
280 imposed by the computational language. This flexibility enables the greatest breadth of subjects
281 to access the greatest breadth of objects without specifying individual relationships between
282 each subject and each object” [6], [1].

283 To enable ABAC implementations, the standards community has undertaken efforts to develop common
284 terminology and interoperability across access control systems. One such standard is the eXtensible
285 Access Control Markup Language (XACML) [7]. Built on an eXtensible Markup Language (XML)
286 foundation, XACML is designed to allow externalized, run-time access control decisions using attribute-
287 based policy definitions.

288 **3.2 ABAC and RBAC Considerations**

289 RBAC simplifies identity management by grouping users with similar access needs by role. Privileges can
290 then be assigned to a role rather than an individual user. This simplification has led to the widespread

291 adoption of RBAC for logical access control. However, many organizations face growing diversity in both
292 types of users and their access needs.

293 This diversity introduces a number of administrative and policy enforcement challenges. Administrators
294 manage access policy for multiple applications and security domains, each often requiring discrete
295 access control policies. Most systems implement access control in different ways, making it hard to
296 share information across systems and requiring administrators to configure access for like users
297 uniquely in each system, typically by using the roles or groups native to that system.

298 These roles are sometimes insufficient in the expression of real-world access control policies and cannot
299 handle real-time environmental considerations that may be relevant to access control decisions;
300 examples such as the location of access, time of day, threat level, and client patch level illustrate how
301 enterprises could be afforded a wider range of decisions based on the amount of risk they perceive or
302 are willing to accept. Similarly, RBAC does not readily support attributes relating to authentication
303 context, referring to assurance of a user's login process.

304 An organization facing the above challenges may meet them using an attribute-based system. Using
305 RBAC, access privileges are assigned to roles. Users are then provisioned those privileges by adding
306 them to a role. This differs from attribute-based systems, which use name:value pairs to establish user,
307 object, and environmental attributes and allow organizations to establish access policy via attribute
308 combinations. These access control policies are then evaluated at access request time for a specific user
309 and resource. Essentially, with RBAC, users arrive at the protected resource with their privileges via an
310 assigned role, while with ABAC, user resource privileges are determined just in time. It is this just-in-time
311 privilege determination that leverages the externalization of policy and enables the incorporation of
312 attributes with dynamic states – such as the environment, resource, user and authentication context.

313 Attribute policy definitions establish a relationship between subject and object that does not change as
314 attribute values change, thus reducing the opportunity for privilege creep and maintaining separation of
315 duties. ABAC systems have the ability to permit new types of access requests without the need to alter
316 the current set of subject/object relationships. Instead, the enterprise can define a new attribute or
317 attributes (or a combination of currently used attributes) that represents the new level of access needed
318 and then define an attribute-based policy that supports this level of access. Business logic to be
319 translated into attribute-based policies that govern access decisions, allowing for a common and
320 centralized way of expressing policy, and computing and enforcing decisions, over the access requests
321 for diverse systems.

322 **3.3 ABAC Leveraging Identity Federation**

323 As enterprises look to keep up with leading-edge technology solutions, they face the identity
324 management challenge of allowing a diverse set of digital identities to access many different
325 organizational applications and resources. Commonly, this requires recognizing digital identities from
326 external security domains, which are typically trusted strategic business stakeholders. Enterprises have
327 realized that supporting this wide range of users, which may not be known or managed by the
328 enterprise, requires attributes from external sources. One approach to meeting this requirement uses
329 federation profiles.

330 Identity federation profiles define the methods used to convey a set of user information from the
331 identity provider (IdP), or organization where the user is known, to the target location or relying party
332 (RP) that needs to acquire the information for some use such as access control. These technologies
333 leverage widely accepted, open, web-oriented, standardized communication languages, like the Security
334 Assertion Markup Language (SAML) version 2.0 standard from OASIS [8], which uses XML, or the OpenID
335 Connect (OIDC) standard from the OpenID Foundation [9] built upon JavaScript Object Notation, to carry
336 the assertions about a user. Federation profiles allow identity and attribute information to be sent over
337 Hypertext Transfer Protocol (HTTP) in a manner that can be understood and used by the receiving
338 organization (the RP) to make access control decisions.

339 In some cases, an RP may need to obtain attributes about a user from a source other than the user's IdP.
340 In such cases, the RP may receive a user's attributes from a trustworthy external source known as an
341 attribute provider (AP). Commonly, identity federation profiles are used to facilitate the federation of
342 attributes from the AP to the RP.

343 Enterprises wishing to participate in federation must have a degree of trust in the organization from
344 which they are receiving identity and attribute information. To facilitate these trust relationships,
345 nonprofit organizations such as the Kantara Initiative and the Open Identity Exchange have proposed or
346 issued trust framework specifications that provide a set of contracts, regulations, and commitments.
347 These specifications enable parties to a trust relationship to rely on identity and attribute assertions (via
348 federation profiles) from external entities.

349 Identity federation allows external users to gain access to web-based protected resources without the
350 need for the RP to manage the identity. When identities and access decisions are abstracted into a
351 common set of attributes, access decisions can be externalized and policies can be established across
352 business units or even organizational boundaries. Identity and attribute federation enables access
353 decisions for users from trusted IdPs, even if the users have not previously been provisioned by the RP
354 (sometimes referred to as the "unanticipated user" scenario).

355 **3.4 Security Standards**

356 Table 3-1 lists the security standards and best practices considered during the development of this practice guide.

357 **Table 3-1 Related Security Standards and Best Practices**

Related Technology	Relevant Standard	URL
General Cybersecurity	NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
	NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations	http://dx.doi.org/10.6028/NIST.SP.800-53r4
	ISO/IEC 27001, Information Security Management	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
	SANS Institute, Critical Security Controls	https://www.sans.org/critical-security-controls/
	ISACA, COBIT 5	http://www.isaca.org/COBIT/Pages/Product-Family.aspx
	Cloud Security Alliance, Cloud Controls Matrix v3.0.1	https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
Risk Management	NIST SP 800-30- r1, Risk Management Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
Requirements Engineering	ISO/IEC 15288:2015, Systems and software engineering – System life cycle processes	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711
	NIST SP 800-160 (Draft), Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems	http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf
Access Control (ABAC)	NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations	http://dx.doi.org/10.6028/NIST.SP.800-162

Related Technology	Relevant Standard	URL
Access Control (NGAC)	INCITS 499-2013, Information Technology – Next Generation Access Control – Functional Architecture (NGAC-FA)	http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+499-2013
Access Control (RBAC)	American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS) 359-2012, Information Technology – Role Based Access Control	http://www.techstreet.com/products/1837530
Language (OIDC)	OpenID Connect Core 1.0	http://openid.net/specs/openid-connect-core-1_0.html
Language (SAML)	OASIS Security Assertion Markup Language (SAML) V2.0	http://saml.xml.org/saml-specifications
Language (WS-Federation)	OASIS Web Services Federation Language (WS-Federation) Version 1.2	http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html
Language (XACML)	eXtensible Access Control Markup Language (XACML) Version 3.0	http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
Language (XML)	Extensible Markup Language (XML) 1.1 (Second Edition)	http://www.w3.org/TR/2006/REC-xml11-20060816/
Protocol (HTTP and HTTPS)	RFC 7230, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	https://tools.ietf.org/html/rfc7230
Protocol (LDAP)	RFC 4510, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	https://tools.ietf.org/html/rfc4510
Protocol (OAuth)	IETF Request for Comments 6749, The OAuth 2.0 Authorization Framework	http://tools.ietf.org/html/rfc6749

Related Technology	Relevant Standard	URL
Protocol (TLS)	NIST SP 800-52 Revision 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	http://dx.doi.org/10.6028/NIST.SP.800-52r1
	RFC 2246, TLS Protocol 1.0	https://tools.ietf.org/html/rfc2246
	RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1	https://tools.ietf.org/html/rfc4346
	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246
PKI	PKI Technical Standards	http://www.oasis-pki.org/resources/techstandards/

359 4 Approach

360 4.1 Audience

361 This guide is intended for individuals responsible for implementing IT security solutions.

362 4.2 Scope

363 This project began with discussions between the NCCoE, IdAM experts across NIST, and IT security
364 vendors partnered with the NCCoE. These discussions enumerated an array of technologies and
365 standards relevant to the ABAC space, but very few implementations of ABAC technology.

366 In response, the NCCoE drafted a white paper [10] that identified numerous desired solution
367 characteristics. After two rounds of public comments on the document, the NCCoE worked with its
368 NCEPs to design an architecture that would demonstrate an array of ABAC capabilities. This build does
369 not include every characteristic found in the white paper, but does include the relevant set of ABAC
370 capabilities based on the technology available to us through the portfolios of the NCCoE's NCEPs. The
371 scope of this build is the successful execution of the following capabilities:

- 372 ■ identity and attribute federation between trust partners
- 373 ■ user authentication and creation of an authentication context
- 374 ■ fine-grained access control through a policy enforcement point (PEP) closely coupled with the
375 application
- 376 ■ creation of attribute-based policy definitions
- 377 ■ secondary attribute requests
- 378 ■ allowing RP access decisions on external identities without the need for pre-provisioning

379 4.3 Assumptions

380 4.3.1 Modularity

381 This example solution is made of many commercially available parts. You might swap one of the
382 products we used for one that is better suited for your environment. We also assume that you already
383 have some IdAM solutions in place. The use of standard protocols such as SAML, LDAP, and Web Service
384 (WS)-Federation enhances the modularity of the architecture to improve your identity and
385 access/authorization functions without major impact to your existing infrastructure. For organizations
386 that want to limit their ABAC deployment to resources residing on Microsoft SharePoint, this solution
387 can be implemented alongside an RBAC implementation, with the lone configuration requirement of
388 enabling attributes inside Microsoft Active Directory (AD) or other identity stores as appropriate.

389 4.3.2 Business Policy Language

390 This build leverages NextLabs technology to decompose natural language business policy into attribute-
391 based digital policies. We implemented example business policies that we feel demonstrate the
392 capabilities of the solution that address business needs. When implementing an ABAC solution,

393 enterprises will need to determine the set of natural language business policies that best meet their
394 access control needs and risk tolerances.

395 **4.3.3 Attribute Semantics and Syntax**

396 An ABAC IdAM infrastructure by its nature is dependent on a predefined set of attribute name:value
397 pairs available for use within its set of rules to determine authorization privileges for users and web
398 service clients. The use of federation, as with this build, expands the domain of agreed-upon attributes
399 to include trusted federation partners. Often a common attribute dictionary is in use for all parties.
400 However, enterprises may look to a third-party service, typically called a trust broker, to facilitate
401 attribute exchange and normalization.

402 For the purposes of this build, we have chosen an example set of attribute values that we feel is
403 representative of business needs. When implementing an ABAC solution, enterprises will need to
404 determine the set of attribute syntax and semantics that best meets their unique access control needs.

405 **4.3.4 Attribute Provenance**

406 In this build, we utilize Microsoft AD, RSA Adaptive Authentication, and Microsoft SharePoint as sources
407 for attributes. Depending on the types of policy an enterprise wishes to implement in attribute-based
408 logic, there will be diversity in the appropriate sources of attribute information. When planning an ABAC
409 implementation, enterprises should consider their ability to collect the attributes required for access
410 decisions and the level of trust they have with the attribute provider and/or sources of attribute
411 information.

412 **4.3.5 Trust Relationships for Identity Federation**

413 The use of identity federation requires a degree of trust between pairs of sharing partners. When
414 establishing this trust relationship, enterprises need to agree upon the technical specification of the
415 trust relationship as well as the types of metadata to be exchanged. Enterprises should make a decision
416 based on their risk profile when determining the stakeholders with which they wish to establish trust
417 relationships.

418 This build establishes a trust relationship between two theoretical organizations through the exchange
419 of attribute and identity information between two Ping Federate instances using SAML 2.0. In order to
420 demonstrate federation capabilities, this build assumes complete trust between exchanging parties.

421 **4.3.6 Human Resources Database/Identity Proofing**

422 This build is based on a simulated environment. Rather than re-create a human resources database and
423 the entire identity proofing process in our lab, we assume that your organization has the processes,
424 databases, and other components necessary to establish a valid identity.

425 **4.3.7 Technical Implementation**

426 The guide is written from a technical perspective. Its foremost purpose is to provide details on how to
427 install, configure, and integrate components. We assume that enterprises have the technical resources
428 to implement all or parts of the build, or have access to companies that can perform the
429 implementation on their behalf.

430 **4.3.8 Limited Scalability Testing**

431 We experienced a major constraint in terms of replicating the volume of access requests that might be
432 generated through an enterprise deployment with a sizable user base. We do not identify scalability
433 thresholds in our builds, as those depend on the type and size of the implementation and are particular
434 to the individual enterprise.

435 **4.4 Risk Assessment**

436 NIST SP 800-30, *Risk Management Guide for Information Technology Systems* states, "Risk is the net
437 negative impact of the exercise of a vulnerability, considering both the probability and the impact of
438 occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce
439 risk to an acceptable level." The NCCoE recommends that any discussion of risk management,
440 particularly at the enterprise level, begin with a comprehensive review of NIST 800-37, *Guide for*
441 *Applying the Risk Management Framework to Federal Information Systems*, material available to the
442 public. The risk management framework (RMF) guidance as a whole proved invaluable in giving us a
443 baseline to assess risks, from which we developed the project, the security characteristics of the build,
444 and this guide.

445 According to NIST SP 800-30-r1, *Risk Management Guide for Information Technology Systems*, "A
446 measure of the extent to which an entity is threatened by a potential circumstance or event, and
447 typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and
448 (ii) the likelihood of occurrence."

449 Through a series of workshops held throughout the country and with industry input, NIST released the
450 *Framework for Improving Critical Infrastructure Cybersecurity* (CSF). The CSF provides industry with a
451 risk-based approach for developing and improving cybersecurity programs. Access control has been
452 identified as a core element of the CSF due to the risks posed by unauthorized access to sensitive data,
453 devices, or IT applications. NIST SP 800-39, *Managing Information Security Risk*, provides guidance on
454 organization-wide risk management. These documents proved invaluable in giving us a baseline to
455 assess risks, from which we developed the project, the security characteristics of the build, and this
456 guide.

457 **4.4.1 Strategic Risks**

458 Strategic risks are risks applicable to the enterprise or organizational level. The following sections
459 describe strategic risks from unauthorized access.

460 **4.4.1.1 Reputation Risk**

461 Public disclosure (by the attacker or through news reports) of an unauthorized access to sensitive
462 information could jeopardize an organization's reputation. Customers and partners could conclude that
463 the organization failed to put adequate access control restrictions in place. This could result in loss of
464 customers, credibility, and market share.

465 **4.4.1.2 Financial Risk**

466 The organization may incur financial losses directly from the theft of money or indirectly from the
467 additional cost of restoring data, equipment, and services. Intruders may blackmail the organization and

468 extort money by threatening to exploit the security breach or publicize the event. Customers may claim
469 that the organization was responsible for any financial loss they incurred due to lack of access controls.

470 ***4.4.1.3 Legal Risk***

471 Security or privacy breaches can expose an organization to lawsuits from employees, investors,
472 customers, or other affected parties.

473 ***4.4.1.4 Compliance Risk***

474 Many organizations have to deal with multiple regulations that require the implementation of
475 appropriate safeguards to protect customer and employee data. The lack of an adequate access control
476 mechanism could cause the organization to become noncompliant with applicable regulations.

477 ***4.4.1.5 Operational Risk***

478 A user who gains unauthorized access could introduce malicious code, using an initial breach as a
479 launching pad to attack the infrastructure, intentionally overload resources, and disrupt critical ongoing
480 operations. This could prevent legitimate users from access to critical resources in the course of their
481 duties, resulting in a loss of productivity. The intruder could modify or erase critical corporate data,
482 preventing normal operations. The delay from recovering data lost and fixing breaches may occupy
483 operation resources, thus degrading the quality of information services.

484 ***4.4.1.6 Intellectual Property Risk***

485 An intruder could rob an organization's intellectual property assets such as ideas, inventions, trade
486 secrets, and creative expressions.

487 ***4.4.1.7 Third Party Risks***

488 If the system is a part of a cooperated (or federated) operation, an intrusion due to ineffective access
489 control might cause a delay in operation or even result in a breach to the cooperated (or federated)
490 network. A breach from an originating system could propagate to an RP, where additional breaches
491 could occur.

492 ***4.4.2 Tactical Risks***

493 Tactical risks are risks applicable at the information system level. The following tactical risks result from
494 unauthorized access.

495 ***4.4.2.1 Insider Threat***

496 Individuals who have a legitimate need to access only a subset of applications and data may extend their
497 reach into domains that should be restricted. Lack of appropriate mechanisms to restrict such access
498 could result in improper use of resources or information.

499 ***4.4.2.2 Limited Provisioning***

500 Inappropriate access control mechanisms may be more prone to administrative errors due to
501 cumbersome workflows or procedures. For example, for a large number of users and resources, access
502 control lists are challenging to maintain as individuals are transferred or terminated. In addition,

503 delegation of provisioning may be available only to privileged users (e.g., system administrators), but
504 this functionality maybe necessary to support business needs.

505 ***4.4.2.3 Unanticipated Users***

506 Many access control mechanisms are unable to support unanticipated users or are prone to delays in
507 provisioning new users due to their inherent design. This might delay legitimate users from accessing
508 resources they need to perform critical functions within a reasonable timeframe.

509 ***4.4.2.4 Dynamic Access***

510 Many access control mechanisms are unable to support dynamic access decisions where risk holders
511 desire to change allowable access requests as environmental conditions change (e.g., Code Red).

512 ***4.4.2.5 Information Sharing***

513 Many access control mechanisms can only protect organizational information within the confines of
514 established system security boundaries. Such a capability may be required to facilitate information
515 sharing in a federation to support an organization's mission priorities.

516 ***4.4.2.6 Coarse-Grained Operations***

517 Many access control mechanisms can only protect resources where the context of the access applies to
518 fine atomic operations (e.g., Create, Read, Update Delete), whereas more comprehensive operations
519 that might include a sequence of steps to complete a workflow may not be supported.

520 ***4.4.2.7 Cost***

521 Some access control mechanisms may cost more than others, depending on the business and operation
522 requirements of the organization. The cost includes design, development, maintenance, and
523 interoperation with legacy or cooperated systems.

524 4.4.3 Security Control Map

525 Table 4-1 lists the major use case security characteristics. For each characteristic, the table provides the matching function, category, and
 526 subcategory from the NIST CSF [11], as well as mappings to controls from other relevant cybersecurity standards.

527 **Table 4-1 Use Case Security Characteristics Mapped to Relevant Standards and Controls**

Security Characteristics	CSF Function	CSF Category	CSF Subcategory	NIST SP 800-53 rev4 [12]	ISO/IEC 27001 [13]	SANS CSC [14]	ISACA COBIT 5 [15]	CSA CCMv3.0.1 [16]
Identity and Credentials	Protect	Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users.	AC-1, IA Family	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-12	DSS05.04, DSS06.03	IAM-02, IAM-03, IAM-04, IAM-08
Remote Access	Protect	Access Control	PR.AC-3: Remote access is managed.	AC-17, AC-19, AC-20	A.6.2.2, A.13.1.1, A.13.2.1	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	APO13.01, DSS01.04, DSS05.03	IAM-07, IAM-08
Access Permissions	Protect	Access Control	PR.AC-4: Access Permissions are managed, incorporating principles of least privilege and separation of duties.	AC-2, AC-3, AC-5, AC-6, AC-16	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12		IAM-01, IAM-02, IAM-05, IAM-06, IAM-09, IAM-10
Encryption and Digital Signature	Protect	Data Security	PR.DS-1 and PR.DS-2: Data-at-rest and data-in-transit are protected.	SC-28, SC-8	A.8.2.3, A.13.1.1, A.13.1.2, A.13.2.3, A.14.1.2, A.14.1.3	CSC 16-16, CSC 17-7		EKM-03, IVS-10, DSI-03

Security Characteristics	CSF Function	CSF Category	CSF Subcategory	NIST SP 800-53 rev4 [12]	ISO/IEC 27001 [13]	SANS CSC [14]	ISACA COBIT 5 [15]	CSA CCMv3.0.1 [16]
Provisioning	Protect	Information Protection Processes and Procedure	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	PS Family	A.7.1.1, A.7.3.1, A.8.1.4		APO07.01, APO07.02, APO07.03, APO07.04, APO07.05	IAM-02, IAM-09, IAM-11
Auditing and Logging	Protect	Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	AU family	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	CSC 4-2, CSC 12-1, CSC 12-10, CSC 14-2, CSC 14-3,	APO11.04	AAC-01
Access Control	Protect	Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	AC-3, CM-7	A.9.1.2	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	DSS05.02	IAM-03, IAM-05, IAM-13

528 **4.5 Technologies**

529 Table 4-2 lists all of the technologies used in this project and provides a mapping between the generic application term, the specific product
 530 used, and the security control(s) that the product provides. Refer to Table 4-1 for an explanation of the CSF Subcategory codes.

531 **Table 4-2 Security Characteristics Mapped to Relevant Build Products**

Security Characteristics	Product(s)	CSF Subcategory	NIST SP 800-53r4	ISO/IEC 27001
Identity and Credentials	Microsoft SharePoint, Ping Federate IdP, RSA Adaptive Authentication	PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-1, IA Family	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
Remote Access	Microsoft SharePoint, NextLabs Policy Controller and Control Center, Ping Federate RP, Ping Federate IdP	PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20	A.6.2.2, A.13.1.1, A.13.2.1
Access Permissions	Microsoft SharePoint and AD, NextLabs Policy Controller and Control Center	PR.AC-4 Access Permissions are managed, incorporating principles of least privilege and separation of duties.	AC-2, AC-3, AC-5, AC-6, AC-16	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
Encryption and Digital Signature	Microsoft SharePoint, NextLabs Policy Controller, Ping Federate RP, Ping Federate IdP, RSA Adaptive Authentication	PR.DS-1 and PR.DS-2: Data-at-rest and data-in-transit is protected	SC-28, SC-8	A.8.2.3, A.13.1.1, A.13.1.2, A.13.2.3, A.14.1.2, A.14.1.3
Provisioning	Microsoft AD	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	PS Family	A.7.1.1, A.7.3.1, A.8.1.4
Auditing and Logging	Microsoft SharePoint, NextLabs Policy Controller, Ping Federate RP, Ping Federate IdP, RSA Adaptive Authentication	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	AU family	A.12.4.1, A.12.4.2, A.12.4.3,

Security Characteristics	Product(s)	CSF Subcategory	NIST SP 800-53r4	ISO/IEC 27001
				A.12.4.4, A.12.7.1
Access Control	NextLabs Policy Controller and Entitlement Manager and Control Center	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	AC-3, CM-7	A.9.1.2

532

533 This build implements the security characteristics through available products, described below, from
534 NCEP organizations. [Section 5](#), Architecture, provides additional insight into the way we used the
535 products.

- 536 ▪ The build is centered on a resource server to be protected by the ABAC solution. In this case,
537 Microsoft SharePoint was used. It is a web-based application within the Windows operating
538 environment commonly deployed as a document management system for intranet, extranet, or
539 cloud repository purposes. SharePoint natively uses an RBAC authorization environment, but it
540 also supports the use of attributes within the user transaction request, a capability Microsoft
541 refers to as being “claims aware.” SharePoint also allows for tagging data within its repository,
542 which can be leveraged as object attributes.
- 543 ▪ Another important component of the build is identity management software, in this case
544 Microsoft AD. AD is a set of services that reside within the Windows server environment. AD
545 functions as an identity repository based on LDAP technology, but also provides authentication
546 and authorization services. AD also includes the ability to provision and de-provision user
547 identities and create, modify, and delete subject attributes.
- 548 ▪ The build needed PEP functionality, and it is provided by NextLabs Entitlement Management,
549 which interfaces and integrates with products such as SharePoint and SAP to provide finer
550 granularity of access decisions than that available using the native access control mechanisms.
551 Entitlement Management is closely coupled with the target application; it traps user access
552 requests and passes access decisions to the policy decision point (PDP).
- 553 ▪ Policy life-cycle management and auditing/reporting are facilitated by the NextLabs Control
554 Center, which hosts policy administration point (PAP) functionality, where attribute-based
555 policies are defined and deployed. The NextLabs Policy Controller, as an element of Control
556 Center, hosts the PDP, which uses the policy definitions and subject, object, and environmental
557 attributes to make an access accept-or-deny decision that the PEP enforces. Control Center also
558 includes dashboards, analytics, reports, and monitoring to offer insight into access patterns.
- 559 ▪ The build includes a federation server/platform for exchanging identities and attributes. Ping
560 Identity’s PingFederate serves as a federation identity system or trust broker, an identity
561 management component, and supports integrated single sign-on (SSO) within an enterprise
562 IdAM infrastructure. It supports standards-based protocols such as SAML, OAuth, and OpenID
563 Connect. Its trust broker capabilities allow for necessary transformation and interface options
564 between federated partners and internal proprietary target resources. When used within an
565 identity provider, it offers options for integrating with authoritative attribute sources.
- 566 ▪ The build has an authentication server that supports multifactor authentication. For this build,
567 RSA Adaptive Authentication (AA) provides this functionality. It is an authentication and
568 environmental analysis system. Its capabilities include a variety of adaptive opportunities, such
569 as Short Message Service (SMS) texting, fingerprint analysis, and knowledge-based
570 authentication. From an environmental perspective, AA collects information such as patch level,
571 operating system, and location, and generates a risk score associated with user authentication.
572 A risk score threshold can then be defined, which, if exceeded, can force a user to step up to an
573 additional authentication mechanism.
- 574 ▪ A final necessary component of the build is a certificate authority. In this case, Symantec’s
575 Managed PKI Service product is used for secure issuance of Public Key Infrastructure (PKI)-based
576 certificates. The Symantec certificates enable mutual transport layer security (TLS), digital

577 signatures, and any explicit encryption that is in use outside of TLS, such as for data-at-rest
578 within an IT environment.

579 **5 Architecture**

580 **5.1 Overview**

581 The following sections detail the ABAC and identity federation architecture that NCCoE staff members
582 and collaborators built. The architecture description details how components from five NCEPs were
583 integrated to achieve the following demonstrable capabilities:

584 **5.1.1 User Authentication and the Creation of an Authentication Context**

585 Our scenario starts with an unauthenticated user attempting to access a target resource for the first
586 time. The user's browser is redirected to his or her home organization (the IdP) for authentication and
587 includes, as required for the target resource, additional (step-up) authentication, and gathering of
588 environmental attributes and authentication context information about the user.

589 **5.1.2 Federation of a User Identity and Attributes**

590 This build demonstrates the federation of subject and environmental attributes between an IdP and an
591 RP. This means that, after the user is authenticated by his or her IdP, the federation protocol that
592 initially redirected the user to the IdP is now used to redirect the user back to the RP carrying the
593 requested identity and attribute information.

594 **5.1.3 Fine-Grained Access Control through a PEP Closely Coupled with the 595 Application**

596 Out of the box, SharePoint access control is more oriented to role-based or group-based DAC. In this
597 build, we enhance the SharePoint access control environment through the deployment of a closely
598 integrated policy enforcement, allowing for a finer degree of granularity based on subject, object, and
599 environmental attributes.

600 **5.1.4 The Creation of Attribute-Based Policy Definitions**

601 This build allows for the translation of business policies into a set of attribute-based policy definitions.
602 These policy definitions establish a relationship between subject, object, and environmental attributes
603 that controls a user's ability to access the RP's resources.

604 **5.1.5 Secondary Attribute Requests**

605 This build provides the ability to make runtime requests for additional attributes from the IdP, should
606 insufficient attributes be presented when making an access decision. When a user accesses a particular
607 resource, or returns to access additional resources, the access control components that we have
608 associated with SharePoint might find that additional subject attributes are needed beyond those that
609 were initially provided. Our build includes components able to search a local cache for the missing
610 attributes and, if not there, issue a new request to the IdP via a SAML attribute request/response for the
611 missing user attributes.

5.1.6 Allow RP Access Decisions on External Identities without the Need for Pre-Provisioning

This build relies upon the trust relationship between the IdP and RP, which enables identity and attribute federation. Once this trust relationship has been established between two organizations, the RP can make runtime access decisions on any individual presenting a credential from the IdP without the need to pre-provision that individual.

5.2 ABAC Architecture Considerations

There are many facets to architecting an ABAC system. As noted in [Section 4.3](#), Assumptions, these include the development of policy, procedure, and/or functional requirements before the selection of technology components. They also include an analysis of business drivers such as those in Section 2.

From a technical perspective, this section outlines a few of the options that an architect will face. [Section 5.3](#), Technology and Architecture of the NCCoE Build, presents the actual architecture chosen for this build.

5.2.1 Industry Standards

When selecting ABAC technologies, it is important to consider the protocols implemented by each technology and whether those protocols are defined by a standards organization. Utilizing standard protocols promotes product interoperability and modularity, and may offer standardized APIs in the event that system requirements drive the need for custom components.

As mentioned earlier, one of the standards for implementing ABAC is XACML. Built on top of XML, XACML offers a core set of rule capabilities for making attribute-based policy definitions and also specific request and response messages for exchange between PEPs and PDPs. Specific details of the XACML 3.0 architecture can be found in the OASIS documentation [7].

Although XACML was developed primarily to fill the need for a standard ABAC protocol, other standard protocols and architectures may be relevant to ABAC use cases. Next Generation Access Control [17], developed by the International Committee for Information Technology Standards, outlines an access control architecture that supports the use of attributes. OAuth 2.0 [18], ratified by the Internet Engineering Task Force (IETF), serves as a rights delegation protocol that grants access to protected resources by defining the allowable user actions for those resources, referred to as “scopes.”

When system requirements include identity federation, protocols such as SAML 2.0 and OpenID Connect can define the syntax and semantics for passing identity and attribute information across organization bounds.

5.2.2 PEP Placement

As it is in the XACML architecture, the PEP is a very important ABAC component, as it enforces the actual access control decision. The location of the PEP may affect the types of access requests the ABAC system can trap and send to the PDP for decisions. It may also contribute to how efficiently the system handles large numbers of access requests. Common options for PEP placement include:

- closely coupling it within a software program

649 ■ using an agent to front-end a web browser-based application
650 ■ placing it at an enterprise gateway position in order to ABAC-enable a set of applications
651 The PEP may also be asked to perform additional functions that require a specific PEP placement. Under
652 the XACML standard, the PEP can be configured to handle “out-of-band” instructions known as
653 obligations (mandatory directives) and advice (optional). These instructions trigger secondary actions in
654 addition to the access decision enforcement. An example of an obligation would be where a person is
655 allowed access to a target resource, but the PEP is directed to initiate a royalty payment for its use.

656 5.2.3 PDP Distribution

657 The PDP operates a rule-based engine that is called upon to adjudicate access permissions to a selected
658 resource. Typical ABAC installations get involved in deciding whether to locate PDPs centrally where
659 each PDP supports multiple PEPs, to dedicate one PDP to each PEP, or to pursue a hybrid of the two
660 approaches. Different PDP distributions can be associated with various performance and latency
661 characteristics.

662 5.2.4 Multi-Vendor

663 ABAC systems have traditionally been classified as proprietary or standards based. Those that are
664 standards based give the option of mixing and matching among system components rather than
665 requiring all components to come from the same vendor. A multi-vendor-implementation solution
666 sometimes needs some advance investigation to ensure that the standardized components will work
667 together as well as promised.

668 5.2.5 Caching

669 There are several locations in an ABAC system implementation for an architect to consider the use of
670 memory caching to improve performance. Considerations include caching decisions at the PEP, rules at
671 the PDP, and user attributes at the RP.

672 5.2.6 Data Tagging

673 If an organization is migrating from a non-ABAC legacy access control mechanism to ABAC, then the task
674 of going through every record and tagging the data with the applicable attributes must be addressed. If
675 the organization has a considerable corpus of legacy data and resources, this may be both a technical
676 and operational challenge.

677 5.2.7 Policy Authoring

678 An important consideration in the selection of an ABAC product is the tools available for creating and
679 modifying policies. Such tools can make understanding policies easier and help with overall policy
680 structure. Organizations could develop a library of sample policies identified by where they might apply
681 within the organization. Some integrated development environments support plug-ins that provide a
682 much more user-friendly syntax for XACML.

683 5.2.8 Attribute Retrieval

684 A design consideration in the implementation of ABAC is the mechanism for attribute retrieval by the
685 PDP. To render an access decision, the PDP needs the values of the attributes referenced by the
686 applicable policies. The PDP can obtain these attributes in one of three ways:

- 687 1. All the attribute values may be provided in the decision request.
- 688 2. If all the attributes are not provided to the PDP and it finds that attributes that are required to
689 make a decision are missing, it may return a decision value of Indeterminate-Missing Attributes
690 and specify what attributes are required. This allows the PEP to fetch the missing values and
691 retry the decision request with them added.
- 692 3. Many PDP implementations are able to pause in the middle of an evaluation and fetch missing
693 attribute values before completing the policy evaluation.

694 If the attributes are being retrieved in a federation scenario, privacy considerations may dictate the
695 choice of the retrieval options in order to ensure a more privacy-enhancing, secure, and efficient
696 implementation.

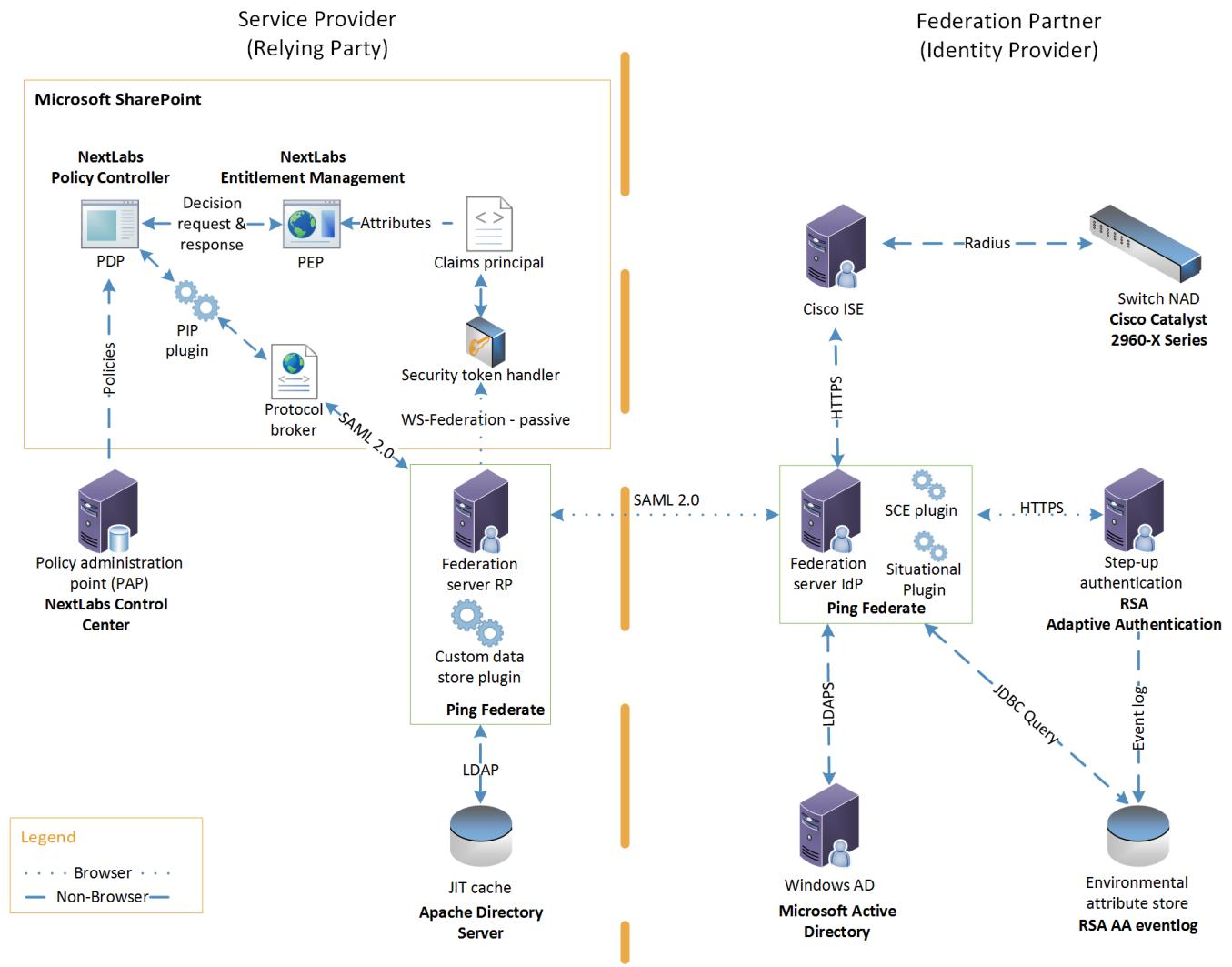
697 **5.3 Technology and Architecture of the NCCoE Build**

698 [Section 4.5](#) provides an overview of the technologies used in this architecture, while [Section 5.1](#) details
699 the functionality found in this build. This section documents how each of the technologies in this build
700 interoperate to achieve the build's functionality. Individuals interested in how these components were
701 installed, configured, or integrated should consult Volume C, How-To Guides, of this publication.

702 **5.3.1 Architecture Diagram and Components**

703 Figure 5-1 illustrates the logical interactions of the components in this build. Interactions are broken
704 down into browser-based or non-browser-based communications. All components in this build are
705 either commercially available through the applicable vendor or can be found publicly with the release of
706 this practice guide.

707 Figure 5-1 ABAC Build 1 Architecture



708

709 The components in Figure 5-1, which were available from NCEP organizations that met the build's
 710 functional requirements, provide the following capabilities to this build:

- 711 ▪ Microsoft AD acts as a user identity management repository for the IdP. This includes the ability
 712 to provision and de-provision user identities; the creation, modification, and deletion of subject
 713 attributes; and the provisioning and de-provisioning of subject attributes to specific user
 714 identities. In this build, AD is the only source for subject attributes.
- 715 ▪ RSA AA gathers environmental information about the user and the user's system or agent at the
 716 time of authentication. AA collects information such as patch level, operating system, and
 717 location, and it generates a risk score associated with the user authentication. A risk score
 718 threshold can then be defined in AA, which, if exceeded, can force a user to step up to one of
 719 the additional authentication mechanisms. In this build, information collected by AA to generate
 720 a risk score is also passed through PingFederate-IdP to the RP side of the operation to be used as
 721 environmental attributes.

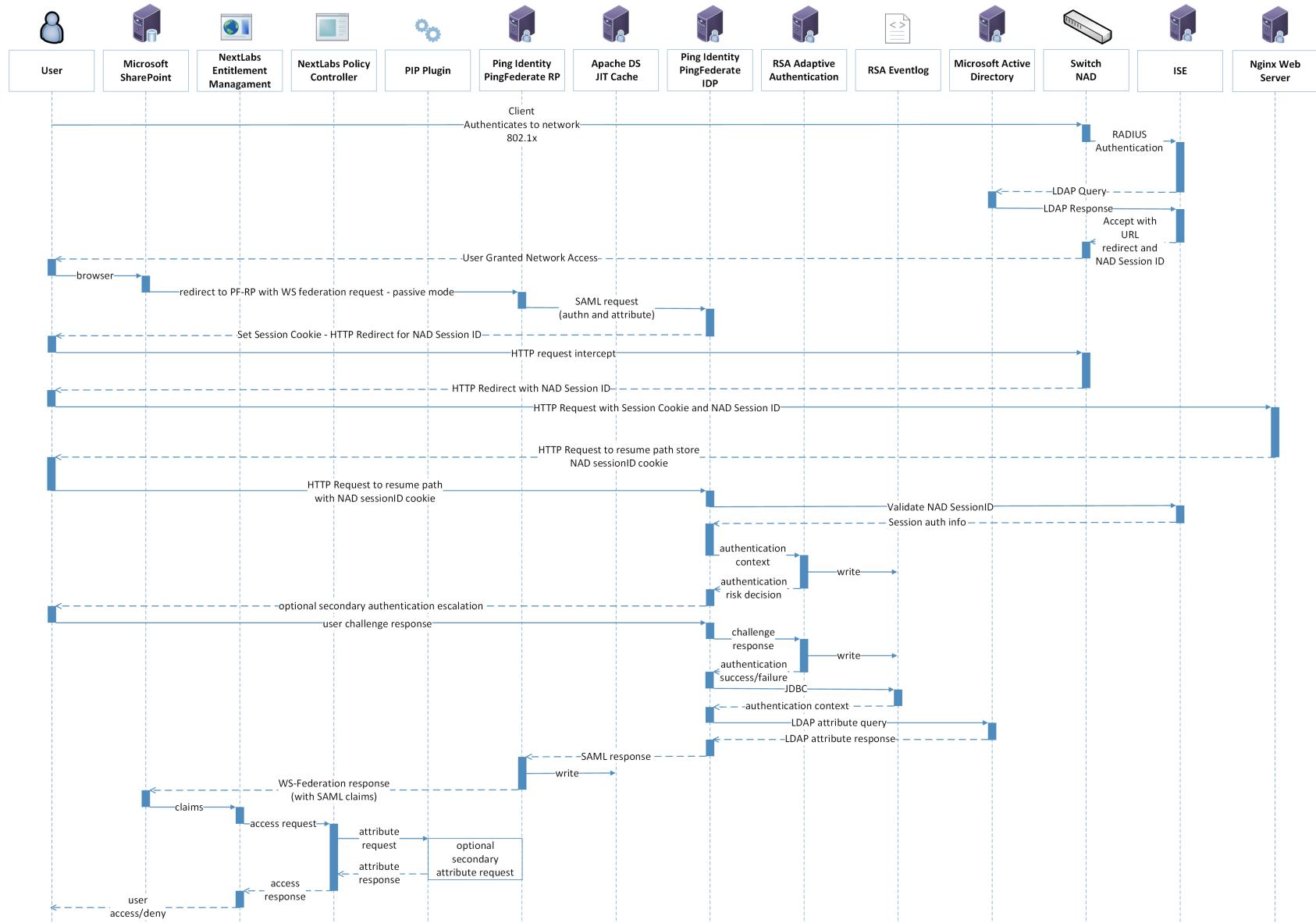
- 722 ■ The RSA AA event log contains the transaction identification (ID) of each user authentication and
723 the associated environmental information collected by RSA AA at the time of authentication.
- 724 ■ Ping Identity PingFederate-IdP serves as a federation system or trust broker for the IdP.
725 PingFederate-IdP provides initial user authentication and retrieval of user attributes to satisfy
726 SAML requests from the RP. Once the user has been authenticated, PingFederate-IdP queries
727 subject attributes from AD and environmental attributes from the RSA AA event log.
728 PingFederate-IdP packages both subject and environmental attributes in a SAML 2.0 token to be
729 sent to the RP.
- 730 ■ The SCE Plug-in is an RSA component that handles communications between the PingFederate-
731 IdP and the RSA AA. It is responsible for passing the RSA AA transaction ID for the user
732 authentication that PingFederate-IdP uses to query the RSA AA event log.
- 733 ■ Ping Identity PingFederate-RP serves as the trust broker for SharePoint. When the user requires
734 authentication, PingFederate-RP redirects the user to the IdP via a SAML request to get the
735 necessary assertions. Once authenticated, PingFederate-RP arranges for the browser's
736 Hypertext Transfer Protocol Secure (HTTPS) content to have the proper information in proper
737 format for acceptance at the target resource (SharePoint). PingFederate-RP has the option to
738 utilize the Apache Directory Server as a just-in-time (JIT) cache. Secondary attribute requests can
739 also be made by PingFederate-RP via a SAML query initiated by the PIP lug-in and the Protocol
740 Broker.
- 741 ■ Microsoft SharePoint serves as a typical enterprise repository. In this build, it stores the target
742 resources that users wish to access. SharePoint natively uses an RBAC authorization
743 environment, but it also supports the use of attributes, a capability Microsoft refers to as
744 “claims aware.” SharePoint accepts assertions from PingFederate-RP and stores asserted
745 attributes as claims. SharePoint also allows for the tagging of data within its repository, which
746 can then be leveraged as object attributes.
- 747 ■ Microsoft SharePoint Security Token Handler resides inside SharePoint, validating the token sent
748 by PingFederate-RP.
- 749 ■ Microsoft SharePoint Claims Principal is the object inside SharePoint where attribute assertions
750 are stored as claims.
- 751 ■ NextLabs Entitlement Management is closely coupled with SharePoint. It performs the PEP
752 functionality, trapping user access requests. As the PEP, Entitlement Management is responsible
753 for gathering object attributes from SharePoint and subject and environmental attributes from
754 the claims principal at the time of the access request. Entitlement management then passes this
755 information in the form of an access decision request to the NextLabs Policy Controller.
- 756 ■ NextLabs Policy Controller is a component of the NextLabs Control Center that is closely coupled
757 with the SharePoint instance. The Policy Controller is responsible for providing PDP capabilities.
758 The Policy Controller receives attribute-based policies from the Control Center and uses these
759 policies to respond to access requests from Entitlement Management.
- 760 ■ NextLabs Control Center serves as the PAP, where attribute-based policies are created, updated,
761 and deployed using a built-in graphical user interface (GUI). The Control Center also provides
762 auditing, logging, and reporting functions for the SharePoint access requests and decisions.

- 763 ■ Policy Information Point(PIP) Plug-in is a software extension of NextLabs Policy Controller that
764 enables it to acquire unavailable attributes required for policy evaluation at runtime from RP or
765 IdP by communicating with Protocol Broker on an HTTPS channel protected by mutual TLS.
- 766 ■ Protocol Broker is a web application that retrieves attribute values by accepting attributes to be
767 queried from the NextLabs Plug-in and querying the PingFederate-RP by issuing a SAML 2.0
768 Assertion Query/Request.
- 769 ■ The Custom Data Store is a plug-in built using PING software development kit (SDK) that enables
770 the RP to query the IdP and provides the resulting attribute value back to the Ping Federate RP.
- 771 ■ The Apache Directory Server is an LDAP version 3-compliant directory server developed by the
772 Apache Software Foundation that works as a JIT cache for PingFederate-RP. It stores subject
773 attributes and other relevant information from the SAML 2.0 response that an RP receives from
774 an IdP.
- 775 ■ Symantec Trust Center Account for Enterprise is used for secure issuance of PKI-based
776 certificates throughout this build. The Symantec certificates enable mutual TLS, digital
777 signatures, and any explicit encryption that is in use outside of TLS, such as for data-at-rest in
778 the RP's JIT cache.
- 779 ■ A Cisco Catalyst 2960-X series switch is used as a network access device (NAD) and provides
780 switching and routing to the network. When a user attempts to access the network, the NAD
781 challenges for credentials and upon successful authentication, a network session ID is created.
- 782 ■ Cisco Identity Services Engine (ISE) is used to provide 802.1X network authentication. In this
783 role, it accepts credentials from the user and verifies this information through radius
784 authentication. The service also collects attributes that are returned to Ping Federate IdP.
- 785 ■ The Situational Plug-In is a Ping Federate plug-in that is used as an adapter to retrieve attributes
786 from Cisco ISE. The plug-in communicates via the HTTP protocol.

787 5.3.2 UML Diagram

788 The architecture shown in [Figure 5-1](#) can, in practice, support different types of sequential operations.
789 We have chosen to initially implement, demonstrate, and document two generic types of sequential
790 ABAC operations as being representative of the core operations of the architecture. The ladder diagram
791 in Figure 5-2 contains represents the initial flow of the ABAC architecture, where an unauthenticated
792 user tries to access a resource on SharePoint.

793 Figure 5-2 UML Sequence Diagram



794

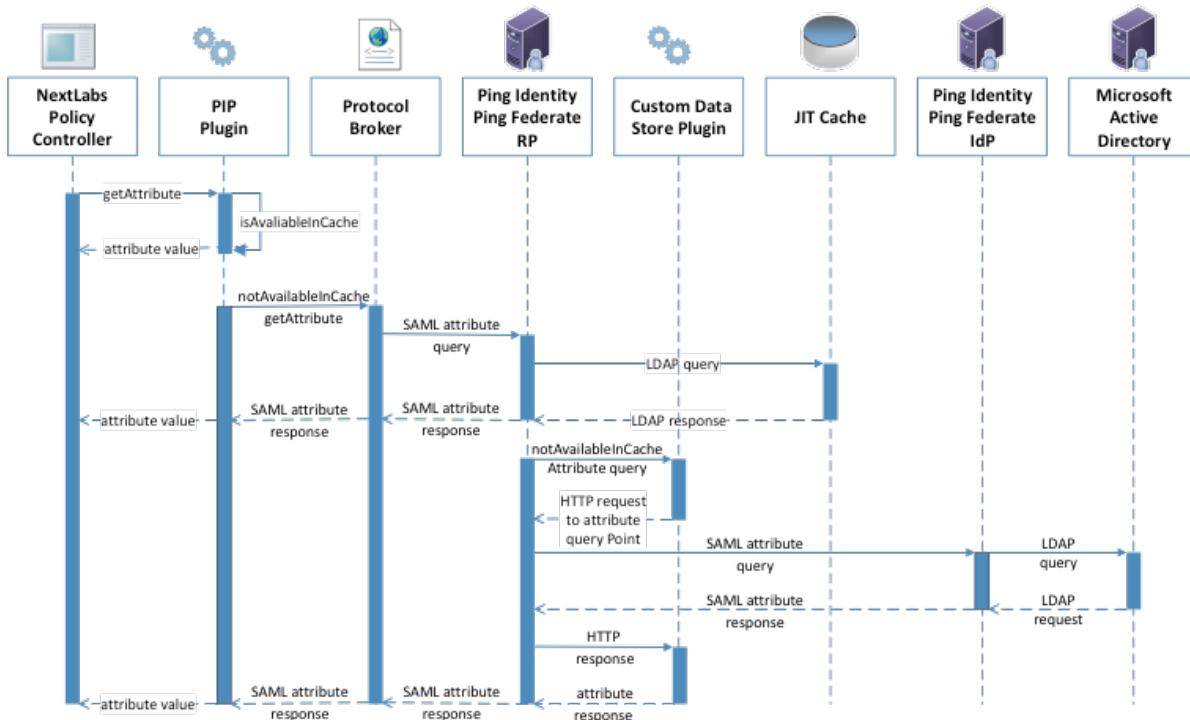
- 795 The sequence starts in the top of Figure 5-2 when a user joins the network and browses to, and
796 attempts to access, a protected resource in SharePoint.
- 797 1. The user attempts to join the network and is challenged for login credentials. These credentials
798 are validated by radius authentication to Active Directory. Upon successful authentication to the
799 network, a network session ID is created.
- 800 2. SharePoint inspects the user's HTTP content and finds that the user has not been previously
801 logged in (i.e., not authenticated), and therefore redirects the browser to PingFederate-RP via
802 use of the WS-Federation protocol.
- 803 3. PingFederate-RP interprets the WS-Federation request as a request for authentication and for
804 attributes, and the user is redirected to PingFederate-IdP carrying a SAML authentication request
805 and SAML attribute request.
- 806 4. PingFederate-IdP does an initial (single-factor) authentication of the user, and, if successful,
807 receives the requested subject attributes.
- 808 5. PingFederate-IdP then redirects the user's browser to RSA AA to enhance the initial
809 authentication.
- 810 Note: In practice this secondary authentication can be conditionally done based upon the type
811 of protected resource for which access is requested or upon other conditions such as
812 environment. The current installation always calls for the second level of authentication to
813 demonstrate what is known as multi-factor authentication (MFA), and, for this build, achieves it
814 by sending an SMS text message and expecting a particular response. The RSA AA product has
815 additional options that are not being demonstrated at this time.
- 816 6. Upon successful completion of the MFA operation, the user is redirected back to PingFederate-
817 IdP. At this time, PingFederate-IdP can query the RSA AA event log for environmental attributes
818 that add context to the authentication.
- 819 7. PingFederate-IdP issues a SAML 2.0 token containing the user's identity and attribute
820 information, and redirects the user's browser to PingFederate-RP.
- 821 8. PingFederate-RP accepts the SAML 2.0 response and issues a WS-Federation response back to
822 SharePoint with the HTTP carrying the authentication and attribute information.
- 823 At this point, the user's browser is issued a "FedAuth" cookie, establishing a session with
824 SharePoint, and resides there until the session is terminated. The rest of this flow occurs as
825 communications internal to the RP or as web service calls back to the IdP, without the user's
826 awareness. Once this session is established, the system is configured to allow the NextLabs
827 components to handle access requests to SharePoint. After the WS-Federation response, the
828 subject and environmental attributes from the IdP are stored in the SharePoint Claims Principal.
- 829 9. Access requests by the authenticated user are now trapped by the NextLabs Entitlement
830 Management PEP, which gathers the subject and environmental attributes stored in the Claims
831 Principal and the object attributes stored in SharePoint, and submits the access request to the
832 Policy Controller PDP for adjudication.
- 833 10. The Policy Controller uses the attributes provided by the PEP and the policy established by
834 Control Center to determine an access allow or deny. If the PDP is not presented with enough

835 attributes to make an access decision, it has the option of initiating a secondary attribute query,
 836 which is detailed in Figure 5-3 and discussed later.

837 11. Once an access decision has been made, the Policy Controller responds back to the Entitlement
 838 Management PEP, which enforces the decision.

839 The ladder diagram in Figure 5-3 represents a flow of this ABAC architecture where an authenticated
 840 user tries to access a resource on SharePoint but there is a need to initiate a secondary attribute
 841 request. If needed, this flow is initiated by the NextLabs Policy Controller in Step 9.

842 **Figure 5-3 Secondary Attribute Request Flow**



843

844 The basic steps of the Figure 5-3 flow are:

- 845 1. When the Policy Controller does not receive the attributes required to make a decision, a
 846 secondary attribute request will be initiated by calling the PIP Plug-in.
- 847 2. PIP Plug-in is a registered plug-in with the NextLabs Policy Controller. It implements the interface
 848 dictated by the NextLabs software. By virtue of this implementation, it receives the subject and
 849 name of the attribute that is required for the policy decision.
- 850 3. When the subject and attribute name are received, the PIP Plug-in checks its local short-term
 851 cache (in this build, configured to hold values for two seconds) to see if the needed attribute for
 852 the subject was recently requested.
- 853 4. If the attribute is still in cache, the value is returned to the Policy Controller. If the value is not in
 854 cache, the PIP Plug-in initiates an HTTPS request to the Protocol Broker.

- 855 5. The Protocol Broker receives the attribute name and subject from the HTTPS request and
856 forwards them as a signed SAML 2.0 Attribute Query to PingFederate-RP on a channel protected
857 by mutual TLS.
- 858 6. Once PingFederate-RP receives the SAML 2.0 attribute query, it sends an LDAP request to the JIT
859 cache to see if the attribute was previously queried in a secondary request.
- 860 7. If the subject does not have the attribute value assigned in the JIT cache, PingFederate-RP will
861 forward the subject and attribute name to the Custom Data Store plug-in. The Custom Data
862 Store plug-in acts as a pointer back to the PingFederate-IdP. To do this, the Custom Data Store
863 dispatches an HTTPS request to the PingFederate-RP with the PingFederate-IdP as the attribute
864 query point.
- 865 8. Ping Federate uses an HTTPS query to form a SAML 2.0 attribute query and dispatch it to the
866 Ping Federate at the IdP.
- 867 9. The Ping Federate at the IdP accepts the SAML 2.0 request, verifies whether the user has the
868 needed attribute, and replies to the PingFederate-RP with a SAML 2.0 response.
- 869 10. PingFederate-RP validates the SAML 2.0 response, retrieves attribute values, and responds to the
870 original Custom Data Store HTTP request with the attribute values.
- 871 11. The Custom Data Store then responds to the PingFederate-RP attribute request with an attribute
872 response.
- 873 12. The PingFederate-RP constructs a SAML 2.0 response and sends it to the Protocol Broker.
- 874 13. The Protocol Broker retrieves the attribute or exception from the SAML 2.0 response and
875 forwards it to the NextLabs plug-in, which passes the attribute or exception back to the Policy
876 Controller.

877 5.3.3 NCCoE Design Considerations

878 [Section 5.2](#) outlined the architectural topics and options that entered into our decision making for this
879 first ABAC build and demonstration. In this subsection, we summarize the architectural directions that
880 were chosen for this particular build, and why.

881 5.3.3.1 Industry Standards

882 The use of XACML and its importance to ABAC functionality were introduced in [Section 5.2.1](#). Its core
883 parts are the request/response protocol between PEP and PDP, the rule language, and the use of
884 obligation and advice that the PDP can forward to the PEP. Use of a standard like XACML yields potential
885 cost saving for an IdAM infrastructure implementation, as heterogeneous interchangeability of
886 operational components can be implemented more easily.

887 The use of SAML 2.0 provided advantages from several perspectives. From its documented set of
888 approved federation profiles, the Web Browser SSO Profile (referred to here as “Web SSO”) has a large
889 following in the industry and was chosen for the browser interface because its authentication
890 sequencing stepped between PingFederate-RP, PingFederate-IdP, and the RSA AA system.

891 SAML 2.0 core was used within the SAML Web SSO exchange, but was also used as a stand-alone for its
892 request/response protocol for backend attribute exchanges of NextLabs’ PIP Plug-in to and from

893 PingFederate-RP (via the Protocol Broker), and for backend attribute exchanges from PingFederate-IdP
894 to PingFederate-RP.

895 WS-Federation is a federation protocol that spans important federation functionality, ranging from
896 authentication to metadata, support for pseudonyms, and more. Our use is limited but still key: to carry
897 an authentication request from SharePoint to PingFederate-RP, and then to handle the return response
898 with its identity and user attribute information.

899 Lightweight Directory Access Protocol Secure (LDAPS), the TLS version of the LDAP standard for
900 interfacing to directory stores, is used in two places in this build. One is PingFederate-RP to its JIT cache
901 based on Apache Directory Server, and the other is PingFederate-IdP to the Microsoft AD LDAP store.
902 Other standards in use include PKI for the structure of the server certificates that are in use, and within
903 TLS operational algorithms. TLS itself is an important standard for promoting communications
904 confidentiality and integrity.

905 *5.3.3.2 PEP Placement*

906 There is a single PEP in this ABAC build for controlling the operations of the SharePoint authorization
907 functionality at a finer level of granularity than is available with the RBAC-oriented access control that
908 comes with SharePoint out of the box. The NextLabs Entitlement Management PEP product was chosen
909 because it meets our requirements, and by its nature it is integrated with and closely coupled with
910 SharePoint. The NextLabs PEP can be considered to be co-located with the SharePoint protected
911 resource.

912 *5.3.3.3 PDP Distribution*

913 With only one PEP in this build, the decisions on PDP quantity and location(s) for placement were
914 simpler than one would find in a typical enterprise installation. The NextLabs Policy Controller PDP is co-
915 located with SharePoint and the PEP.

916 *5.3.3.4 Multi-Vendor*

917 The ABAC implementation represented in this build is a heterogeneous set of IdAM components that
918 have been successfully integrated to achieve the system objectives. To accomplish this, we worked
919 closely with our NCEP collaborator to design an interoperable architecture. Each component performed
920 its functions as required, and Volume C of this guide describes the set of NCCoE experiences and
921 supplemental functionality that was incorporated to achieve the functional objectives.

922 *5.3.3.5 Caching*

923 Caching is a common topic in system integration work as architects work to achieve efficiencies required
924 for their particular functionality. In the current build, two caches have been explicitly implemented by
925 the NCCoE development team:

- 926 ■ NextLabs PIP Plug-in contains a local cache, developed using the EhCache library. This cache
927 stores attributes for two seconds and adds efficiency to the system should multiple requests for
928 the same subject and attribute value pairing occur in quick succession (with two seconds).

- 929 ▪ A JIT cache was developed for PingFederate-RP, using Apache Directory Server. It is used to
930 cache user attributes that are retrieved by PingFederate-RP for a finite time (such as up to 24
931 hours) to avoid future repeated secondary attribute calls to the IdP.

932 5.4 Security Characteristics

933 In this section, we re-introduce the security characteristics and security controls that were first
934 introduced in [Sections 4.4](#) and [4.4.1](#), and relate each to the NCEP's products used in this ABAC build.

- 935 ▪ Identity and Credentials and Their Use for Authorized Devices. In NIST SP 800-53, this is tied to
936 AC-1, and in NIST Cybersecurity Framework to PR.AC-1: "Identities and credentials are managed
937 for authorized devices and users." In this build, both user and system identities are managed to
938 ensure linkage with these security controls. Where applicable, systems are given PKI-based
939 credentials for use with TLS via the Symantec Managed PKI Service. User authentication in this
940 first build is multi-factor, with one factor being name and password via PingFederate-IdP and
941 AD, and the second an SMS text message sent to a cellular device conducted by the RSA AA. The
942 RSA AA system offers other options for use as the second factor of authentication through its
943 multi-credential framework.
- 944 ▪ Remote Access Being Managed. Several of the NCEP products are involved in ensuring efficient
945 and secure remote access. The two Ping Identity PingFederate installations have federation and
946 authentication features that allow the RP to accept external identities for remote access.
947 SharePoint via WS-Federation trusts external identities sent from PingFederate. NextLabs
948 products enable ABAC functionality for SharePoint access decisions and allow for the auditing
949 and logging of access requests.
- 950 ▪ Access Permissions. ABAC systems manage access permissions by defining attribute-based rules
951 that specify what subject attributes are needed to access resources with a given set of object
952 attributes, under a set of environmental conditions. In this build, this functionality is handled by
953 NextLabs products. A NextLabs Control Center allows for creation of attribute-based policies and
954 makes access decisions based on those policies via its Policy Controller.
- 955 ▪ Encryption and Digital Signature. Browser-based communications with SharePoint are HTTPS-
956 based, and LDAP is used for all interfacing with AD. All system endpoints are equipped with PKI
957 certificates issued by the Symantec Managed PKI Service, and TLS is used for system-level point-
958 to-point transactions. Examples include full encryption of SAML request/response transactions
959 such as between PingFederate-RP and PingFederate-IdP.
- 960 ▪ Provisioning. Identities are provisioned, stored, and de-provisioned inside AD. This process
961 occurs manually through the native Microsoft Windows Server GUI. AD also handles the
962 assigning of subject attributes to specific user identities.
- 963 Object attributes are provisioned via SharePoint. SharePoint sites or individual files can be
964 "tagged" with object attributes by adding columns to the SharePoint site table or document
965 library. The titles of these columns serve as attribute names and the content of the columns
966 serves as the values of attributes for the specific object.
- 967 ▪ Auditing and Logging. Each product in this build supports a logging mechanism detailing
968 activities occurring within that component. Access requests can be audited using the NextLabs
969 Reporter, where the user, access decision, and policy enforced can be viewed for each access
970 request.

- 971 ▪ Access Control. Fundamentally, this build enhances the native capabilities of SharePoint by
972 adding ABAC functionality. This is achieved through the NextLabs Entitlement Management PEP,
973 which traps access requests, and the Policy Controller PDP, which makes access decisions using
974 attribute-based policies. Organizations implement the concept of least privilege by defining
975 attribute-based policies in the NextLabs Control Center and assigning applicable attributes to
976 subjects and objects using AD and SharePoint. A wider range of access control decisions is
977 enabled through the use of environmental attributes, which can be obtained from RSA AA in this
978 build.

979 **5.5 Features and Benefits**

980 This section details some of an ABAC system's potential benefits through risk reductions, cost savings, or
981 access management efficiencies. As with any reference architecture, the exact benefits derived will
982 depend on the organization's individual implementation requirements and the scenarios to which an
983 organization wishes to apply an ABAC model.

984 **5.5.1 Support Organizations with a Diverse Set of Users and Access Needs**

985 RBAC meets practical limits as roles and their associated access requirements grow in diversity and
986 complexity. This often leads to the overloading of access privileges under a single role, the assignment of
987 multiple roles to a single user, or the escalation of the number of roles the enterprise needs to manage.
988 Moving to an ABAC model allows organizations to specify policy based on a single attribute or a
989 combination of attributes that represents the specific access an individual's needs. This helps eliminate
990 the potential for privilege creep.

991 **5.5.2 Reduce the Number of Identities Managed by the Enterprise**

992 When organizations wish to provide access to users from external security domains, they have the
993 option to provision local identities for these external users. These identities must then be managed by
994 the enterprise. This scenario incurs the costs associated with these management efforts and also
995 presents risk to the enterprise, because these accounts could be orphaned as the users' access privilege
996 requirements change at their home organization. Identity federation can address these issues by
997 allowing organizations to accept digital identities from external security domains, but leave the
998 management of these identities to the users' home organizations.

999 **5.5.3 Enable a Wider Range of Risk Decisions**

1000 The ability to define attribute-based policies affords organizations the extensibility to implement a wider
1001 range of risk-based decisions in access control policy, compared to an RBAC system. Specifically, the
1002 ability to leverage environmental attributes allows for relevant context such as location of access, time
1003 of day, threat level, and client patch level to be included in automated decision logic.

1004 **5.5.4 Support Business Collaboration**

1005 ABAC combined with identity federation helps reduce barriers to sharing resources and services with
1006 partner organizations. Under the ABAC model, a partner's user identities and appropriate access policies
1007 for those identities do not need to be pre-provisioned by the RP. Instead, access decisions can be made
1008 on partner identities using attributes provided by the partner.

1009 **5.5.5 Centralize Auditing and Access Policy Management**

1010 ABAC can improve the efficiency of access management by eliminating the need for multiple,
1011 independent, system-specific access management processes, replacing them with a centralized PDP and
1012 PAP. In this way, access decisions across multiple applications could be audited centrally at the PDP,
1013 while policies could be created and deployed centrally at the PAP, but enforced locally via an
1014 application-specific PEP. The ability to externalize and centrally manage access policies may also simplify
1015 compliance processes by reducing the number of places that need to be audited.

Appendix A List of Acronyms

AA	Adaptive Authentication
ABAC	Attribute Based Access Control
AD	Active Directory
AP	Attribute Provider
CSF	Framework for Improving Critical Infrastructure Cybersecurity
DAC	Discretionary Access Control
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IdAM	Identity and Access Management
IdP	Identity Provider
IETF	Internet Engineering Task Force
ISE	Identity Services Engine
IT	Information Technology
JIT	Just-in-Time
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
NAD	Network Access Device
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partner
NIST	National Institute of Standards and Technology
OIDC	OpenID Connect
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
RP	Relying Party
SAML	Security Assertion Markup Language
SMS	Short Message Service
SP	Special Publication
SSO	Single Sign-on
TLS	Transport Layer Security

SECOND DRAFT

WS	Web Service
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

Appendix B References

- [1] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, NIST Special Publication (SP) 800-162, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2014.
<http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf> [accessed 09/08/17].
- [2] International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers, *Systems and software engineering – System life cycle processes*, ISO/IEC/IEEE 15288:2015, 2015.
http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711 [accessed 09/08/17].
- [3] R. Ross, M. McEvilley, and J. C. Oren, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, NIST Special Publication (SP) 800-160 Second Public Draft, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2016.
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf [accessed 09/08/17].
- [4] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," *IEEE Computer*, vol. 43, no. 6, pp. 79-81, June 2010.
<http://ieeexplore.ieee.org/document/5481941/> [accessed 09/08/17].
- [5] E. Coyne and T.R. Weil, "ABAC and RBAC: Scalable flexible and auditable access management," *IT Professional*, vol. 15, no. 3, pp. 14-16, May-June 2013.
<https://www.computer.org/csdl/mags/it/2013/03/mit2013030014.html> [accessed 09/08/17].
- [6] *Attribute Based Access Control (ABAC) Overview*, National Institute of Standards and Technology: Computer Security Resource Center [Web site],
<http://csrc.nist.gov/projects/abac/> [accessed 09/08/17].
- [7] *eXtensible Access Control Markup Language (XACML) Version 3.0*, OASIS Standard, OASIS, January 2013. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html> [accessed 09/08/17].
- [8] *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, OASIS Standard, OASIS, March 2005. <http://saml.xml.org/saml-specifications> [accessed 09/08/17].
- [9] *OpenID Connect Core 1.0 incorporating errata set 1*, OpenID Foundation [Web site],
http://openid.net/specs/openid-connect-core-1_0.html [accessed 09/08/17].
- [10] W. Fisher, *Attribute Based Access Control*, Building Block Version 2, National Cybersecurity Center of Excellence. April 1, 2015.

<https://nccoe.nist.gov/sites/default/files/library/project-descriptions/abac-project-description-final.pdf> [accessed 09/08/17].

- [11] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, National Institute of Standards and Technology, February 12, 2014.
<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf> [accessed 09/08/17].
- [12] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST, SP 800-53 Revision 4, National Institute of Standards and Technology, April 2013. <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.
- [13] *ISO/IEC 27001 Information Security Management*, International Organization for Standardization [Web site], <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm> [accessed 09/08/17].
- [14] *SANS Institute - CIS Critical Security Controls*, SANS Institute [Web site], <https://www.sans.org/critical-security-controls/> [accessed 09/08/17].
- [15] COBIT 5 Publications Directory, ISACA [Web site],
<http://www.isaca.org/COBIT/Pages/Product-Family.aspx> [accessed 09/08/17].
- [16] *Cloud Controls Matrix v3.0.1 (10-6-16 Update)*, Cloud Security Alliance (CSA) [Web site],
<https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/> [accessed 09/08/17].
- [17] *Information Technology – Next Generation Access Control – Functional Architecture (NGAC-FA)*, ANSI INCITS 499-2013, American National Standards Institute, March 2013.
<http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+499-2013> [accessed 09/08/17].
- [18] D. Hardt, *The OAuth 2.0 Authorization Framework*, Internet Engineering Task Force (IETF) Network Working Group Request for Comments (RFC) 6749, October 2012.
<http://tools.ietf.org/html/rfc6749> [accessed 09/08/17].

NIST SPECIAL PUBLICATION 1800-3C

Attribute Based Access Control

Volume C:
How-to Guides

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Norm Brickman
Prescott Burden
Santos Jha
Brian Johnson
Andrew Keller
Ted Kolovos
Sudhi Umarji
Sarah Weeks
The MITRE Corporation
McLean, VA

September 2017

SECOND DRAFT

This publication is available free of charge from:
<https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control>



DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-3c, Natl. Inst. Stand. Technol. Spec. Publ. 1800-3c, 577 pages, September 2017, CODEN: NSPUE2

FEEDBACK

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

Comments on this publication may be submitted to: abac-nccoe@nist.gov.

Public comment period: September 20, 2017 through October 20, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).

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

1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

2 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards
3 and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and
4 academic institutions work together to address businesses' most pressing cybersecurity issues. This
5 public-private partnership enables the creation of practical cybersecurity solutions for specific
6 industries, as well as for broad, cross-sector technology challenges. Through consortia under
7 Cooperative Research and Development Agreements (CRADAs), including technology partners—from
8 Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards
9 and best practices to develop modular, easily adaptable example cybersecurity solutions using
10 commercially available technology. The NCCoE documents these example solutions in the NIST Special
11 Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the
12 steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by
13 NIST in partnership with the State of Maryland and Montgomery County, Md.

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

16 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

26 **ABSTRACT**

27 Enterprises rely upon strong access control mechanisms to ensure that corporate resources (e.g.,
28 applications, networks, systems, and data) are not exposed to anyone other than an authorized user. As
29 business requirements change, enterprises need highly flexible access control mechanisms that can
30 adapt. The application of attribute based policy definitions enables enterprises to accommodate a
31 diverse set of business cases. This NCCoE practice guide details a collaborative effort between the
32 NCCoE and technology providers to demonstrate a standards-based approach to attribute based access
33 control (ABAC).

34 This guide discusses potential security risks facing organizations, benefits that may result from the
35 implementation of an ABAC system, and the approach the NCCoE took in developing a reference
36 architecture and build. It includes a discussion of major architecture design considerations, an
37 explanation of security characteristic achieved by the reference design, and a mapping of security
38 characteristics to applicable standards and security control families.

39 For parties interested in adopting all or part of the NCCoE reference architecture, this guide includes a
 40 detailed description of the installation, configuration, and integration of all components.

41 **KEYWORDS**

42 *access control; access management; attribute provider; authentication; authorization; identity
 43 federation; identity management; identity provider; relying party*

44 **ACKNOWLEDGMENTS**

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

Name	Organization
Nate Lesser	NIST National Cybersecurity Center of Excellence
Paul Timmel	NIST National Cybersecurity Center of Excellence
Paul Grassi	NIST National Strategy for Trusted Identities in Cyberspace
Mike Garcia	NIST National Strategy for Trusted Identities in Cyberspace
Naomi Lefkovitz	NIST National Strategy for Trusted Identities in Cyberspace
Rene Peralta	NIST National Strategy for Trusted Identities in Cyberspace
Dave Ferriaolo	NIST Computer Security Division
Vincent Hu	NIST Computer Security Division
Roger Wiggenstam	NextLabs Inc
John Conduit	NextLabs Inc
Srikanth Karanam	NextLabs Inc
Adam Madlin	Symantec Corporation
Steve Kruse	Symantec Corporation
Steve Schmalz	RSA
Ben Smith	RSA

Name	Organization
Andrew Whelchel	RSA
Chris Leggett	Ping Identity
Paul Fox	Microsoft Corporation
Derek Keatley	Microsoft Corporation
Hemma Prafullchandra	Hytrust
John McLeese	Hytrust
Dave Cox	ID/Dataweb
Chris Donovan	ID/Dataweb
Pete Romness	Cisco
Kevin McFadden	Cisco
John Eppish	Cisco
Chris Ceppi	Situational Corporation

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

Technology Partner/Collaborator	Build Involvement
Ping Identity	PingFederate Federation Server
NextLabs	Entitlements Management Policy Enforcement Point
Microsoft	Policy Controller Policy decision point
RSA	Control Center Policy Administration Point

Technology Partner/Collaborator	Build Involvement
Symantec	Active Directory
Cisco	SharePoint

Contents

51	1	Introduction	1
52	1.1	Practice Guide Structure.....	1
53	1.2	Build Overview.....	2
54	1.3	Typographical Conventions	2
55	2	Setting Up the Identity Provider.	3
56	2.1	Components	3
57	2.1.1	Cisco Switch and Cisco Identity Services Engine	4
58	2.1.2	Microsoft AD.....	4
59	2.1.3	Nginx Web Server	4
60	2.1.4	PingFederate-IdP	4
61	2.1.5	PingFederate-RP	5
62	2.1.6	RSA Adaptive Authentication	5
63	2.1.7	SCE Plug-in	5
64	2.1.8	Situational Context Connector	5
65	2.1.9	Required or Recommended Files, Hardware, and Software	6
66	2.2	Configuring I PC for 802.1x Auth	7
67	2.2.1	Configure MS Native Suplicant for Wired 802.1x.....	10
68	2.3	Install Nginx Web Server	16
69	2.4	Install Microsoft AD	17
70	2.4.1	Create a User in Microsoft AD.....	17
71	2.4.2	Create the Lightweight Directory Access Protocol User for Federated Authentication.....	19
72	2.4.3	Create the LDAP User for Cisco ISE Administration.....	19
73	2.5	Configure the Cisco Switch	19
74	2.6	Install and Configure Cisco Identity Services Engine.....	23
75	2.6.1	Configure Cisco ISE with Microsoft AD	26
76	2.6.2	Add Network Device to ISE.....	26
77	2.6.3	Configure ISE for pxGrid	26
78	2.6.4	Enable ISE Policy Sets	27
79	2.6.5	Configure Authentication Policy.....	29
80	2.6.6	Configure Authorization Policy.....	32
81	2.6.7	Add Rule for Authorization Policy	37

84	2.7	Install RSA AA.....	54
85	2.8	Configure RSA AA Rules	58
86	2.8.1	Create Rule for Non-Persistent User Enrollment	59
87	2.8.2	Create Rule for Persistent User Enrollment	61
88	2.8.3	Create Rule for User Updates.....	61
89	2.8.4	Create Rule for Challenge SMS.....	62
90	2.8.5	Increase SMS Token Length.....	63
91	2.8.6	Create Policy for Session Sign-In	63
92	2.8.7	Create Lists for Session Sign-In.....	64
93	2.8.8	Create Rules for Session Sign-In	64
94	2.8.9	Create Rule to Allow Forced Sign-In for Payment	65
95	2.8.10	Create Custom Fact	65
96	2.9	Install and Configure PingFederate-RP	67
97	2.10	Install PingFederate-IdP.....	73
98	2.11	Install the SCE Plug-in for the PingFederate-IdP	73
99	2.12	Install the Situational Context Connector for the PingFederate-IdP.....	74
100	2.12.1	Install Situational Context Connector.....	74
101	2.12.2	Install Situational Session Validator	75
102	2.13	Configure PingFederate-IdP.....	76
103	2.13.1	Configure SAML Protocol	77
104	2.13.2	Create Data Store for Microsoft AD	77
105	2.13.3	Create Credential Validator for Microsoft AD	79
106	2.13.4	Create IdP Adapter for Authentication with Microsoft AD via Web Browser Form	83
107	2.13.5	Create IdP Adapter for Two-Factor Authentication with RSA AA	87
108	2.13.6	Create Composite IdP Adapter Integrating Microsoft AD and RSA AA	90
109	2.13.7	Create IdP Adapter for the Situational Context Connector and ISE Authentication	93
110	2.13.8	Configure the Federation Connection to the Relying Party	99
111	2.13.9	Configure ISE Composite Adapter	115
112	2.13.10	Applying the Composite Adapter	118
113	2.14	Certificates.....	127
114	2.14.1	Certificate Configuration PingFederate.....	128
115	2.15	Functional Test of All Configurations for Section 2	128
116	3	Setting up Federated Authentication Between the Relying Party and the Identity Provider	133

118	3.1	Introduction	133
119	3.2	Components	134
120	3.2.1	PingFederate-IdP	134
121	3.2.2	PingFederate-RP	135
122	3.3	Export Metadata from the Identity Provider	135
123	3.4	Configure PingFederate-RP Connection to the PingFederate-IdP	138
124	3.5	Functional Test of All Configurations for Section 3	160
125	4	Installing and Configuring Microsoft SharePoint Server and Related Components.....	162
127	4.1	Introduction	162
128	4.1.1	Components Used in this How-To Guide	162
129	4.1.2	Required or Recommended Files, Hardware, and Software.....	163
130	4.2	Installation of Required Components.....	164
131	4.2.1	Installing SQL Server 2012	164
132	4.2.2	Installing IIS 8.0 on the SharePoint Server	164
133	4.2.3	Installing Microsoft SharePoint Server 2013.....	164
134	4.3	Creating the Web Application (IIS site) in SharePoint.....	164
135	4.4	Creating and Installing SSL Certificate	172
136	4.4.1	Self-Signed Certificates.....	173
137	4.4.2	Certificates Signed by Local or Online Certificate Authority	197
138	4.5	Creating a Site Collection.....	205
139	4.6	Creating New Sub-Sites	211
140	5	Set Up Federated Authentication at the Relying Party's SharePoint ..	215
141	5.1	Introduction	215
142	5.2	Usage Notes on PingFederate	215
143	5.3	Configure a SharePoint Federated Logon Provider.....	216
144	5.3.1	Setting up the Certificate.....	216
145	5.3.2	Configuring the Trusted Identity Token Issuer.....	220
146	5.3.3	Configuring the Token Issuer as a Sign On Option	221
147	5.3.4	Configuring the Access Control Rule on SharePoint.....	222
148	5.3.5	Functional Test of the Federated Logon at the Resource Provider.....	225
149	5.4	Configure the PingFederate-RP Connection to SharePoint.....	229
150	5.5	Functional Test of All Configurations for Section 5	244

151	5.6 Troubleshooting SharePoint Federated Authentication Problems.....	248
152	6 Attribute Exchange between the Identity Provider and Relying Party 251	
153	6.1 Introduction.....	251
154	6.2 Create Custom User Attributes in Microsoft AD	251
155	6.2.1 Preparing the AD Schema for Creating New Custom Attributes.....	251
156	6.2.2 Set Values for Custom User Attributes in Microsoft AD	260
157	6.3 Configure PingFederate Servers to Pull User Attributes	268
158	6.3.1 Configure PingFederate-IdP to Pull User Attributes During Authentication.....	268
159	6.3.2 Configure PingFederate-IdP to Pull Environmental Attributes During Authentication	273
160	6.3.3 Configure PingFederate-RP to Pull Attributes from the Identity Provider's SAML Exchange.....	287
161	6.4 Configure PingFederate-RP and SharePoint to Pass and Read Attributes	293
162	6.4.1 Configure PingFederate-RP to Pass Attributes to SharePoint.....	293
163	6.4.2 Configure SharePoint to Read Custom Attributes from PingFederate-RP	301
164	6.5 Configure the Claims Viewer Web Part at the SharePoint Site.....	307
165	6.6 Functional Test of All Configurations for Section 6.....	314
166	6.6.1 Temporarily Disable SAML Encryption for Testing and Troubleshooting Message Exchanges	317
170	7 Setting Up NextLabs to Protect SharePoint..... 319	
171	7.1 Introduction	319
172	7.2 Components	320
173	7.2.1 NextLabs Control Center (release 7.5)	320
174	7.2.2 NextLabs Policy Studio: Enterprise Edition.....	321
175	7.2.3 NextLabs Policy Controller.....	321
176	7.2.4 NextLabs Entitlement Manager for Microsoft SharePoint Server.....	322
177	7.2.5 Required or Recommended Files, Hardware, and Software	323
178	7.3 Installation and Configuration of NextLabs Control Center (on the SQL Server)....	325
179	7.3.1 Installation and Configuration.....	325
180	7.4 Installation and Configuration of NextLabs Policy Studio: Enterprise Edition (PAP) 343	
181	7.4.1 Installation	343
182	7.5 Installation and Configuration of Policy Controller (PDP)	349
183	7.5.1 Installation	349

184	7.6	Installation and Configuration of NextLabs Entitlement Manager for SharePoint Server.....	354
185	7.6.1	Installation and Configuration.....	354
186	7.7	Functional Tests.....	363
187	7.7.1	Verify that the NextLabs Webpart for Policy Enforcement Has Been Successfully Enabled on the Site Collection in SharePoint.....	363
188	7.7.2	Test to Verify the NextLabs Service is Running	365
191	8	Defining Policies and Enforcing Access Decisions with NextLabs	366
192	8.1	Introduction	366
193	8.1.1	Components and Sub-Components Used in this How-To Guide.....	367
194	8.1.2	Pre-requisites to Complete Prior to this How-To Guide.....	367
195	8.2	Policy Strategy	367
196	8.2.1	Top-Level Blacklisting Deny Policy, Whitelisting Allow Sub-Policies	367
197	8.2.2	Global Policies.....	368
198	8.3	Translation of Business Logic into Policy	368
199	8.3.1	ABAC Build Scenario – Runabout Air Business Rules.....	368
200	8.3.2	Translation of Runabout Air Business Rules into ABAC Policies.....	369
201	8.4	Using the NextLabs Policy Studio GUI for Policy Definition and Deployment	370
202	8.4.1	Login and Initial Screen in Policy Studio	370
203	8.4.2	Policy Studio Menu Commands.....	372
204	8.4.3	Defining and Deploying Components.....	373
205	8.4.4	Defining Policy	385
206	8.4.5	Deploying Policy	416
207	8.4.6	Modifying and Re-Deploying Policies and Components	418
208	8.4.7	Deactivating Policies and Components	419
209	8.4.8	Deleting Policies and Components	421
210	8.5	Configuring Attributes in NextLabs	421
211	8.5.1	Stopping the NextLabs Policy Controller Service	421
212	8.5.2	Editing the Configuration File	422
213	8.5.3	Restarting IIS via Windows PowerShell	425
214	8.5.4	Restarting the NextLabs Policy Controller Service	426
215	8.6	Functional Test	426
216	8.6.1	Updated Bin File After Policy Creation/Modification.....	426
217	8.6.2	Reviewing NextLabs AgentLog to Illustrate History of Access Control Evaluations during SharePoint Access	429

219	9 Leveraging NextLabs Control Center Reporter for Reporting and Auditing Purposes	432
220	9.1 Introduction	432
221	9.1.1 Components Used in this How-To Guide	432
222	9.1.2 Pre-requisites to Complete Prior to this How-To Guide.....	432
223	9.2 Introduction to NextLabs Control Center Reporter	433
224	9.2.1 Opening Reporter.....	433
225	9.3 Introduction to Reporter Dashboard.....	435
226	9.3.1 Exploring the Dashboard	437
227	9.4 Introduction to Defining and Running Custom Reports in Reporter.....	439
228	9.4.1 Defining a Custom Report	440
229	9.4.2 Running a Custom Report.....	446
230	9.5 Example Custom Report and Available Formats	446
231	9.5.1 Defining the Example Custom Report	446
232	9.5.2 Format: Table of Event Data.....	450
233	9.5.3 Format: Bar Chart Grouped by Policy Chart.....	452
234	9.5.4 Format: Bar Chart Grouped by User Chart.....	453
235	9.5.5 Format: Pie Chart Grouped by Resource.....	455
236	9.6 Further Example Custom Reports from Our Build	457
237	9.6.1 Custom Report Illustrating All Access for One User During a Two-Month Period .	457
238	9.6.2 Viewing Access Attempts on Individual Resources	460
239		
240	10 Configuring a Secondary Attribute Provider	462
241	10.1 Introduction	462
242	10.1.1 Pre-Requisites.....	463
243	10.1.2 Criteria for Secondary Attribute Collection.....	463
244	10.1.3 Components	463
245	10.2 Component Software and Hardware Requirements.....	467
246	10.3 Ping Custom Data Store	468
247	10.3.1 Functionality and Architecture.....	468
248	10.3.2 Deploying the Ping Custom Data Store	469
249	10.3.3 Compilation	470
250	10.3.4 Configuration within PingFederate Administrative Console	471
251	10.4 NextLabs PIP Plugin	474
252	10.4.1 Architecture.....	474

253	10.4.2	Understanding How the NextLabs PIP Plugin Interacts with Build Components...	476
254	10.4.3	Compilation and Deployment	477
255	10.5	Protocol Broker.....	479
256	10.5.1	Architecture.....	479
257	10.5.2	Deployment	482
258	10.5.3	Example SAML Request and Response Output.....	486
259	10.6	Apache Directory Service (ApacheDS).....	488
260	10.6.1	Layout	488
261	10.6.2	Download	488
262	10.6.3	Installation.....	490
263	10.6.4	Starting and Stopping the Server	495
264	10.6.5	ApacheDS Configuration.....	496
265	10.7	PingFederate - Apache Integration.....	496
266	10.7.1	Provisioning of Server Credential	496
267	10.8	Configuration of PingFederate to Query the JIT Cache when Responding to Secondary Attribute Requests.....	515
269	10.8.1	Introduction.....	515
270	10.8.2	Prerequisites.....	515
271	10.9	ApacheDS Schema Extension	535
272	10.9.1	Pre-Requisites.....	536
273	10.9.2	Procedure	536
274	10.10	Functional Tests	556
275	10.10.1	Testing the Ready State of the NextLabs Policy Controller Service	556
276	10.10.2	Test the Successful Loading of the Custom Plugin Within the NextLabs Policy Controller Software Architecture	557
278	10.10.3	Testing That the Protocol Broker .war File Loads Correctly in Tomcat Server.....	558

279 **List of Figures**

280 Figure 2-1 Out-of-Band Token Length	63
281 Figure 2-2 Successful List Created	64
282 Figure 10-1 Architecture.....	465
283 Figure 10-2 Ping Custom Data Store Interaction Diagram	468
284 Figure 10-3 Ping Custom Data Store Class Diagram.....	469
285 Figure 10-4 NextLabs PIP Plugin Class Diagram.....	476
286 Figure 10-5 NextLabs PIP Plugin Interaction Diagram	477
287 Figure 10-6 Communication Between Plugin and Relying Party	481
288 Figure 10-7 Protocol Broker Interaction Diagram	481
289 Figure 10-8 Protocol Broker Class Diagram.....	482
290 Figure 10-9 ApacheDS Download	489

291 **List of Tables**

292 Table 2-1 Persistent User Enrollment.....	61
293 Table 2-2 User Update.....	61
294 Table 2-3 Out-of-Band SMS	62
295 Table 2-4 Session Sign-In – Low Risk	64
296 Table 2-5 Session Sign-In – Medium Risk.....	64
297 Table 2-6 Session Sign-In – High Risk.....	65
298 Table 2-7 Session Sign-In – Critical Risk	65
299 Table 2-8 Force Allow.....	67

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 an Attribute Based Access Control (ABAC) implementation. This reference design is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- NIST SP 1800-3a: *Executive Summary*
- NIST SP 1800-3b: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-3c: *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 1800-3a), which describes the:

- challenges enterprises face in access control solutions
- 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 this part of the guide, *NIST SP 1800-3b*, which describes what we did and why. The following sections will be of particular interest:

- Section 4.4.1, Risk, provides a description of the risk analysis we performed
- Section 4.4.3, 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 1800-3a*, with your leadership team members to help them understand the importance of adopting standards-based ABAC implementation.

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

You can use the How-To portion of the guide, *NIST SP 1800-3c*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

335 This guide assumes that IT professionals have experience implementing security products within the
 336 enterprise. While we have used a suite of commercial products to address this challenge, this guide does
 337 not endorse these particular products. Your organization can adopt this solution or one that adheres to
 338 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
 339 parts of an ABAC solution. Your organization's security experts should identify the products that will best
 340 integrate with your existing tools and IT system infrastructure. We hope you will seek products that are
 341 congruent with applicable standards and best practices. Volume B, Section 4.5, Technologies, lists the
 342 products we used and maps them to the cybersecurity controls provided by this reference solution.

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

347 1.2 Build Overview

348 The following section provides detailed instructions for implementing, configuring and integrating an
 349 ABAC solution coupled with identity and attribute federation. These instructions detail an example of an
 350 ABAC implementation using a policy enforcement point that is closely coupled with a SharePoint file
 351 server and two sources of environmental attributes. Before implementing this reference design,
 352 individuals should refer to NIST SP 1800-3b *Approach, Architecture, and Security Characteristics* to
 353 better understand the design decision that we made as part of this implementation.

354 1.3 Typographical Conventions

355 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

Typeface/ Symbol	Meaning	Example
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

356

357 2 Setting Up the Identity Provider

358 This guide details an attribute based access control (ABAC) implementation that leverages identity
 359 federation. In a federation model, the identity provider (IdP) authenticates the user requesting access
 360 and provides attributes assigned to that user to the relying party (RP). In addition to attributes assigned
 361 to the user, the IdP sends environmental and device attributes to the RP. The RP, which controls access
 362 to the resource requested by the user, utilizes the identity and attributes information to make runtime
 363 decisions to grant or deny access to the user.

364 In this section, we install and configure federation components at the identity provider. The
 365 components in this section facilitate federated, Security Assertion Markup Language (SAML)-based
 366 authentication using account credentials in the identity provider's Microsoft Active Directory Domain
 367 Services (referred to as Microsoft AD in this guide). The federated authentication between the RP and
 368 IdP is facilitated by Ping Identity's PingFederate application. This build also requires the user to
 369 authenticate with a second factor, which is handled by the RSA adaptive authentication server.

370 Each of the components used for the build are described in the Components section. Following the
 371 Components section are step-by-step instructions for installing, configuring, and integrating the
 372 components.

373 If you follow the instructions in this section, you will be able to perform a Functional Test to verify the
 374 successful completion of the steps for installing, configuring, and integrating the components.

375 2.1 Components

376 Federated Authentication at the IdP involves the following distinct components:

- 377 ■ **Cisco Switch (Catalyst 2960-X Series):** Acts as a switch and router in the build, routing traffic
 from users to the services and applications on another network segment
- 379 ■ **Cisco Identity Services Engine (ISE):** Authenticates users from other networks or network
 segments, and provides device and network attributes to the Ping-Federate IdP via the
 Situational Context Connector
- 382 ■ **Microsoft AD:** An LDAP directory service that stores user account and attribute information
- 383 ■ **Nginx Web Server:** A web server installed on a separate host that is required for handling
 Network Access Device (NAD) redirects for the Situational Context Connector. In this build, we
 used Nginx.
- 386 ■ **PingFederate-IdP:** A federation system or trust broker for the IdP
- 387 ■ **PingFederate-RP:** Serves as the trust broker for SharePoint

- 388 ▪ **RSA Adaptive Authentication (RSA AA):** Requires the user to authentication using a Short
389 Message Service (SMS) message sent to the user's mobile phone. Collects environmental
390 information about the user and the user's system or agent at the time of authentication.
391 ▪ **SCE Plug-in:** Handles communications between the PingFederate-IdP and the RSA AA
392 ▪ **Situational Context Connector:** IdP Adapter for PingFederate that integrates PingFederate with
393 the Cisco Identity Server Engine via the pxGrid Application Programming Interface (API)

394 2.1.1 Cisco Switch and Cisco Identity Services Engine

395 The Cisco Catalyst 2960-X Series switch serves as a switching and routing device, primarily for the
396 purpose of routing users' traffic from one network or network segment to another, where the protected
397 resources and services are located. The Cisco ISE authenticates users whose traffic comes from the
398 switch, and from that authentication provides device and network attributes to the PingFederate IdP via
399 the Situational Context Connector.

400 2.1.2 Microsoft AD

401 Microsoft AD acts as a user identity management repository for the IdP. It includes the ability to
402 provision and de-provision user identities; the creation, modification, and deletion of subject attributes;
403 and the provisioning and de-provisioning of subject attributes to specific user identities. In this build,
404 Microsoft AD is the only source for subject attributes from the IdP.

405 2.1.3 Nginx Web Server

406 Nginx acts as a web server that handles NAD redirects for the Situational Context Connector. It is used to
407 trigger the NAD (Cisco Switch in this case) to insert the session identification (ID) as a parameter to
408 create a secure browser cookie, which gets returned to PingFederate and then verified by the Context
409 Connector during authentication. When the Context Connector matches the session ID from the secure
410 browser cookie with the session ID from Cisco ISE, federation can continue, and a Security Assertion
411 Markup Language (SAML) response is returned to the browser. Finally, the browser POSTs a SAML
412 response to the PingFederate-RP.

413 2.1.4 PingFederate-IdP

414 Ping Identity PingFederate-IdP serves as a federation system or trust broker for the IdP. PingFederate-
415 IdP provides initial user authentication and retrieval of user attributes to satisfy SAML requests from the
416 RP. Once the user has been authenticated, PingFederate-IdP queries subject attributes from AD and
417 environmental attributes from the RSA AA event log. PingFederate-IdP packages both subject and
418 environmental attributes in a SAML 2.0 token to be sent to the RP.

419 PingFederate Usage Notes:

- 420 ▪ When using the PingFederate application to perform an administrative configuration, there is
421 usually a sequence of screens that require user entry, ending with a summary page. Once you
422 click Done on the summary page, you must also click Save on the following page to actually save
423 the configurations. If you forget to click Save, you may inadvertently lose changes to the
424 configuration.

- 425 ▪ In the PingFederate application and associated documentation, the RP is referred to as the
 426 Service Provider.
- 427 ▪ When using the PingFederate application to perform configuration, refer to the title of the tab
 428 with a small star icon to its left to identify the item you are currently configuring. For example, if
 429 you navigated to the following screen, you would be on the IdP Adapter screen.



430

431 2.1.5 PingFederate-RP

432 Ping Identity PingFederate-RP serves as the trust broker for SharePoint. When the user requires
 433 authentication, PingFederate-RP redirects the user to the IdP via a SAML request to get the necessary
 434 assertions. Once authenticated, PingFederate-RP arranges for the browser's Hypertext Transfer Protocol
 435 Secure (HTTPS) content to have the proper information in proper format for acceptance at the target
 436 resource (SharePoint).

437 2.1.6 RSA Adaptive Authentication

438 RSA AA gathers environmental information about the user and the user's system or agent at the time of
 439 authentication. RSA AA collects information such as patch level, operating system, and location, and it
 440 generates a risk score associated with the user authentication. A risk score threshold can then be
 441 defined in RSA AA, which, if exceeded, can force a user to step up to one of the additional
 442 authentication mechanisms. In this build, information collected by RSA AA to generate a risk score is also
 443 passed through PingFederate-IdP to the RP side of the operation to be used as environmental attributes.
 444 The RSA AA event log contains the transaction ID of each user authentication and the associated
 445 environmental information collected by RSA AA at the time of authentication.

446 2.1.7 SCE Plug-in

447 The SCE Plug-in handles communications between the PingFederate-IdP and the RSA AA. It is
 448 responsible for passing the RSA AA transaction ID for the user authentication that PingFederate-IdP uses
 449 to query the RSA AA event log.

450 2.1.8 Situational Context Connector

451 The Situational Context Connector is an IdP adapter for PingFederate that integrates PingFederate with
 452 the Cisco Identity Server Engine via the pxGrid API. Deploying this solution for PingFederate enables
 453 device-level authentication and authorization for web single sign-on (SSO) use cases. When a user
 454 attempts a SSO via PingFederate, the Context Connector queries Cisco ISE, retrieves the device context
 455 for the end-user device, and matches device context with the credentials of an authenticated user. The
 456 result is a session based on a combination of user and device information. The Context Connector
 457 enables real-time evaluation of Cisco ISE state-of-the-art device profiling. The Context Connector can
 458 provide information about the user and the session to the PingFederate IdP, which the PingFederate IdP
 459 includes in the SAML token sent to the PingFederate RP. The Context Connector relies on a web server
 460 for NAD redirects (implemented with Nginx on a separate server in this build), and a Session Validator
 461 that is included in the Situation Context Connector integration kit.

462

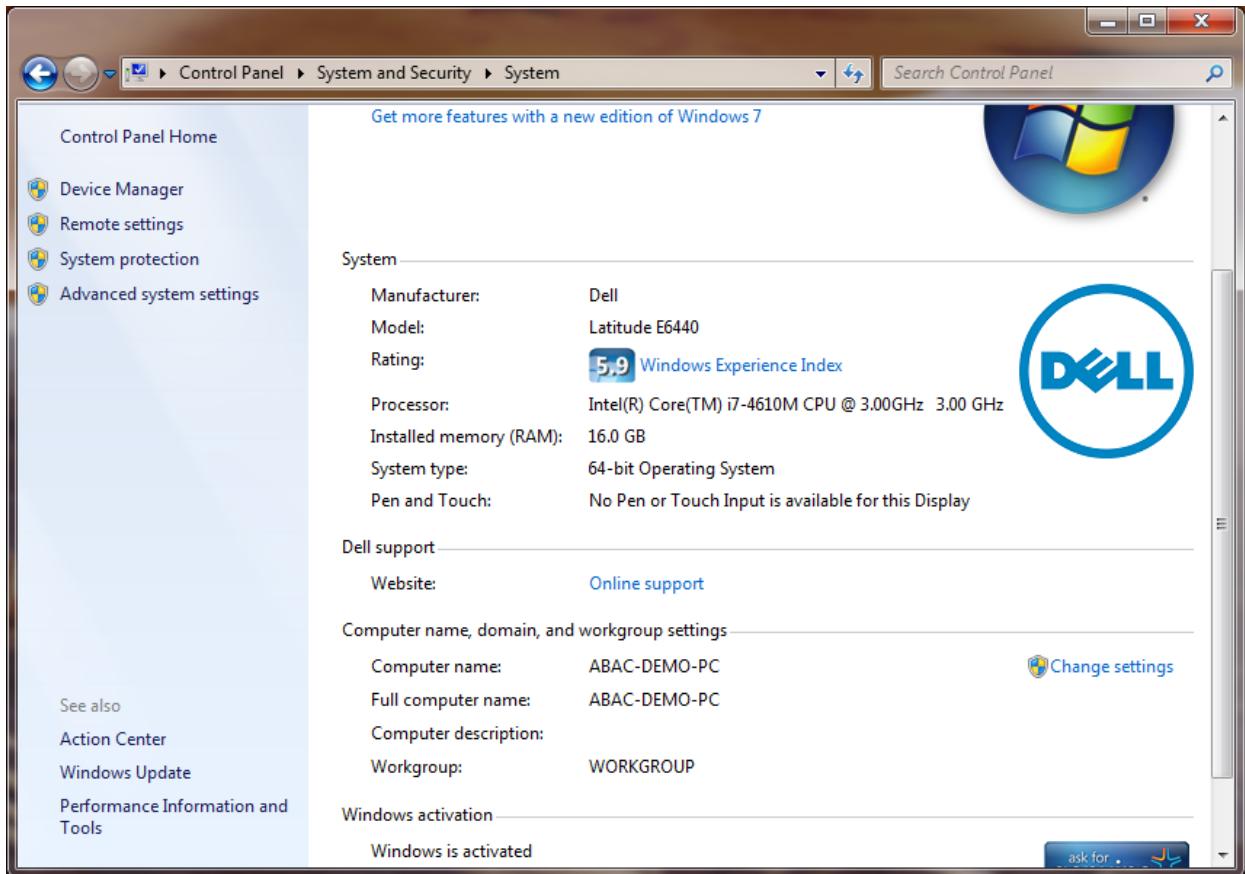
2.1.9 Required or Recommended Files, Hardware, and Software

Component	Required Files	Recommended or Minimum Hardware Requirements	Hardware Used in this Build	Recommended or Minimum Operating System or Other Software	Operating System or Other Software Used in this Build
Cisco ISE 2.1 (as Virtual Appliance)	ise-2.1.0.474.SPA.x86_64.iso	16GB RAM; 6 cores, 2GHz or faster; 200 GB free disk space	16GB RAM; 4 cores, 2GHz; 200 GB hard disk space	N/A	N/A
Microsoft AD	N/A	512MB RAM; 1.4GHz CPU; 32GB free disk space	4GB RAM; 2.2GHz CPU; 108GB free disk space	N/A	Microsoft Windows Server 2012
PingFederate	N/A	4GB RAM; 4 cores; 1.8 GHz or faster; 750 MB free disk space	4GB RAM; 2.2GHz CPU; 98 GB	Microsoft Windows Server 2008 R2	Microsoft Windows Server 2012
SCE Plug-in	sce-adapters-pingfederate-aa.1.1.jar	1GB RAM; 1.8GHz CPU; 250MB free disk space	4GB RAM; 2.2GHz CPU; 98 GB	N/A	Microsoft Windows Server 2012
RSA AA	Adaptive Authentication (On-Premise) 7.0.0.0-SNAPSHOT	6GB RAM; 2.2GHz CPU; 40GB free disk space	6GB RAM; 2.2GHz CPU; 150GB free disk space	Windows Server 2008; Apache Tomcat 7.0; Microsoft SQL Server 2008	Microsoft Windows Server 2008 (64-bit)
Situational Context Connector	Situational_Context_Connector_v21.zip (pf.plugins.ise-idp-adapter.jar; index.jsp); Situational_SessionValidator.zip	N/A	4GB RAM; 2.2GHz CPU; 98 GB	N/A	Microsoft Windows Server 2012
Nginx web server	nginx-1.11.4.zip	N/A	4GB RAM; 2.2 GHz CPU; 32GB	Windows XP, Linux 2.2, Free BSD 3	Microsoft Windows 7

463

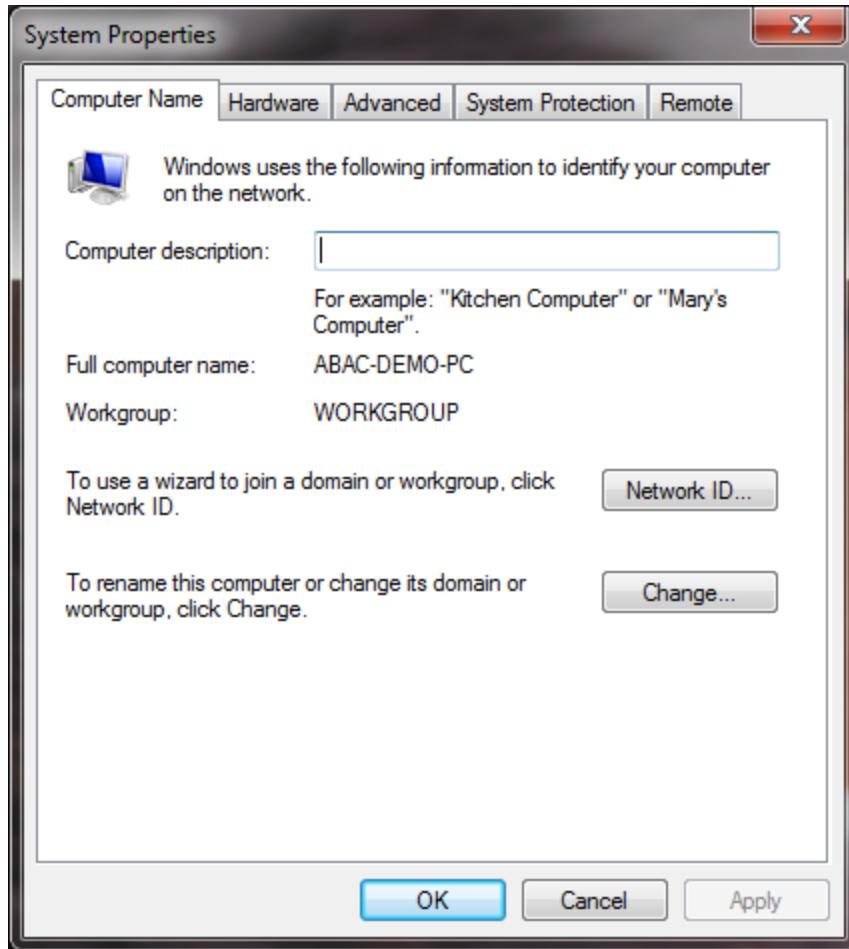
464 **2.2 Configuring I PC for 802.1x Auth**

- 465 1. On the client PC, go to **Control Panel > System and Security > System**.



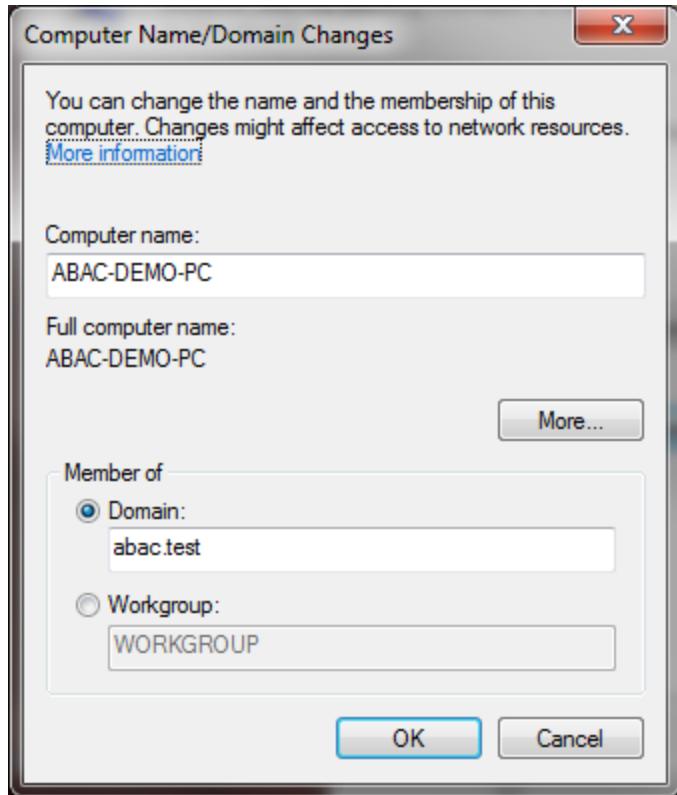
466

- 467 2. Click on **Change settings**.

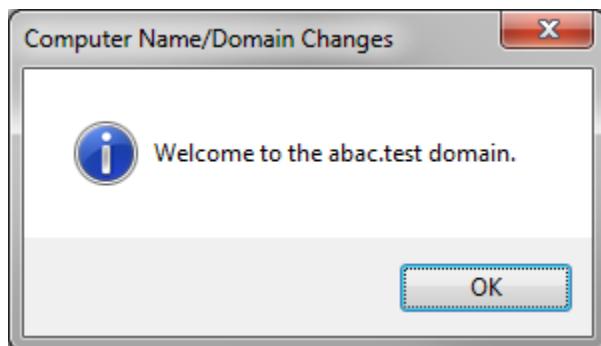


468

- 469 3. Click on the **Change** button.
- 470 4. Select **Domain**.
- 471 5. Enter the domain to join, "abac.test." It will require authentication using a user that's capable
472 of adding a computer to the domain controller.



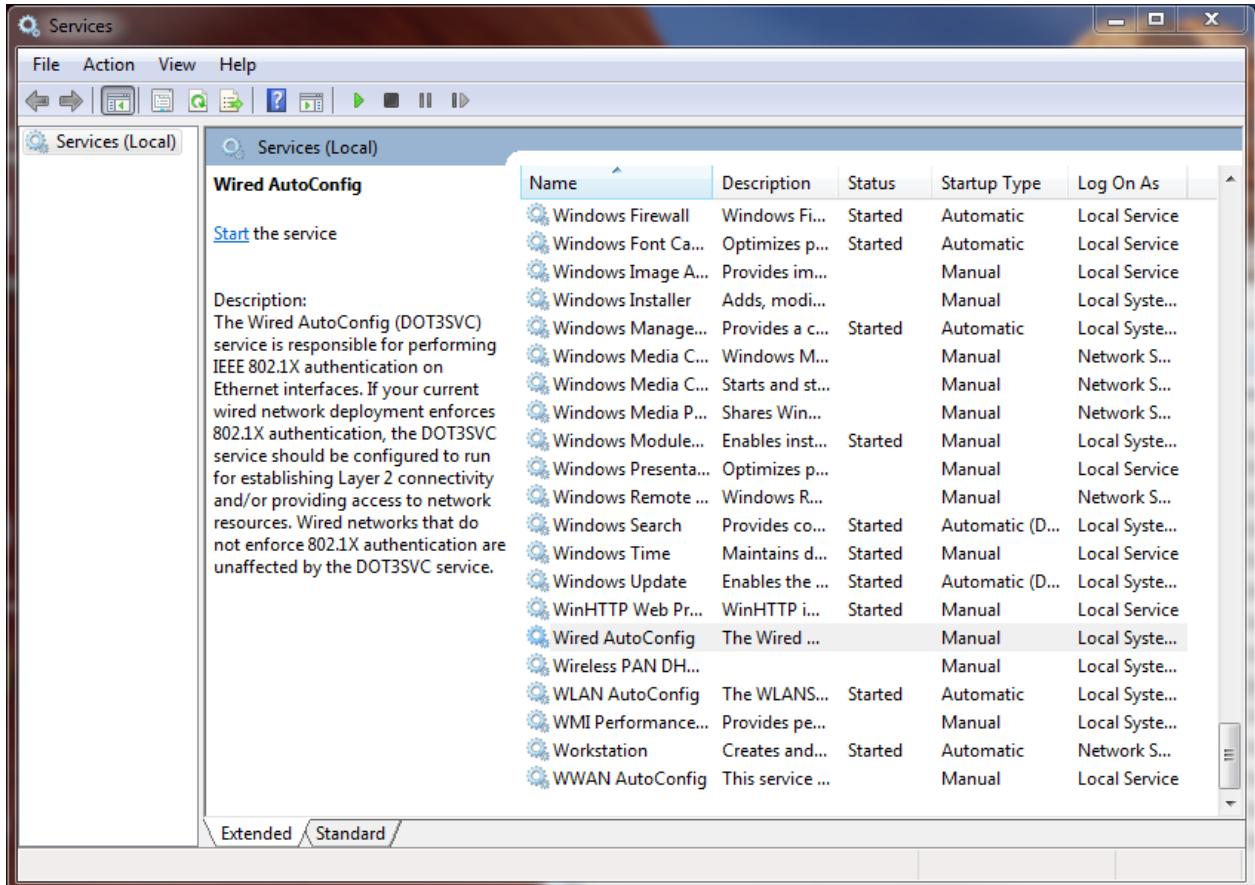
473



474

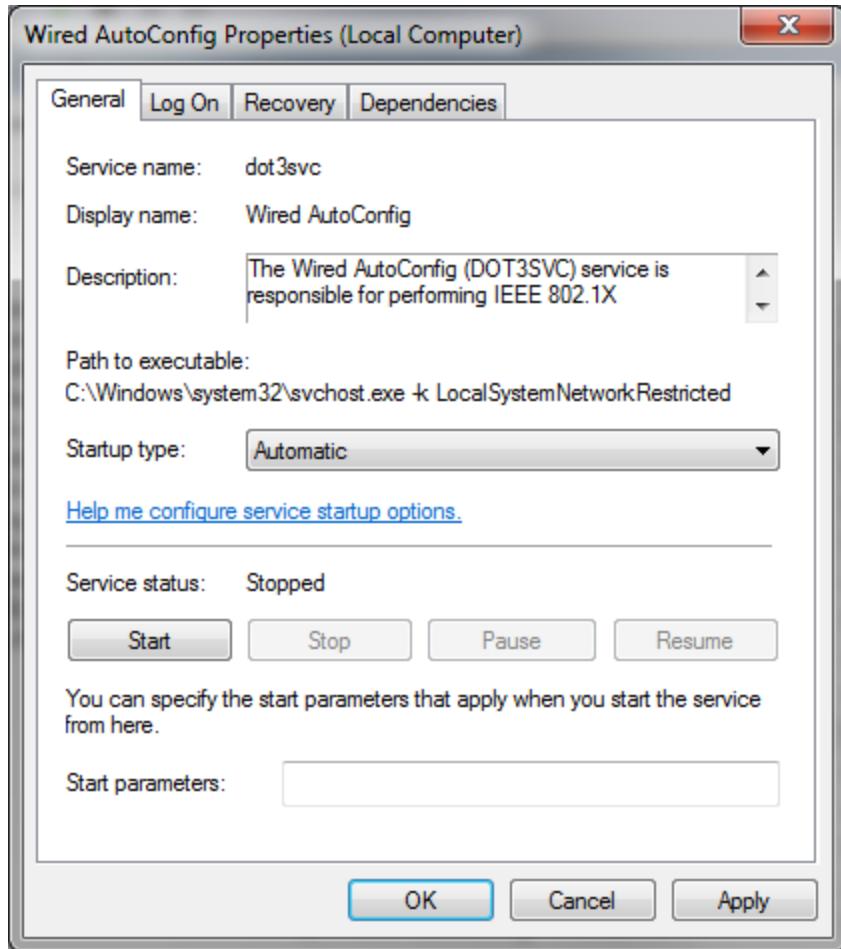
475 2.2.1 Configure MS Native Suplicant for Wired 802.1x

- 476 1. On the client PC, go to Control Panel > System and Security > Administrative Tools > Services.



477

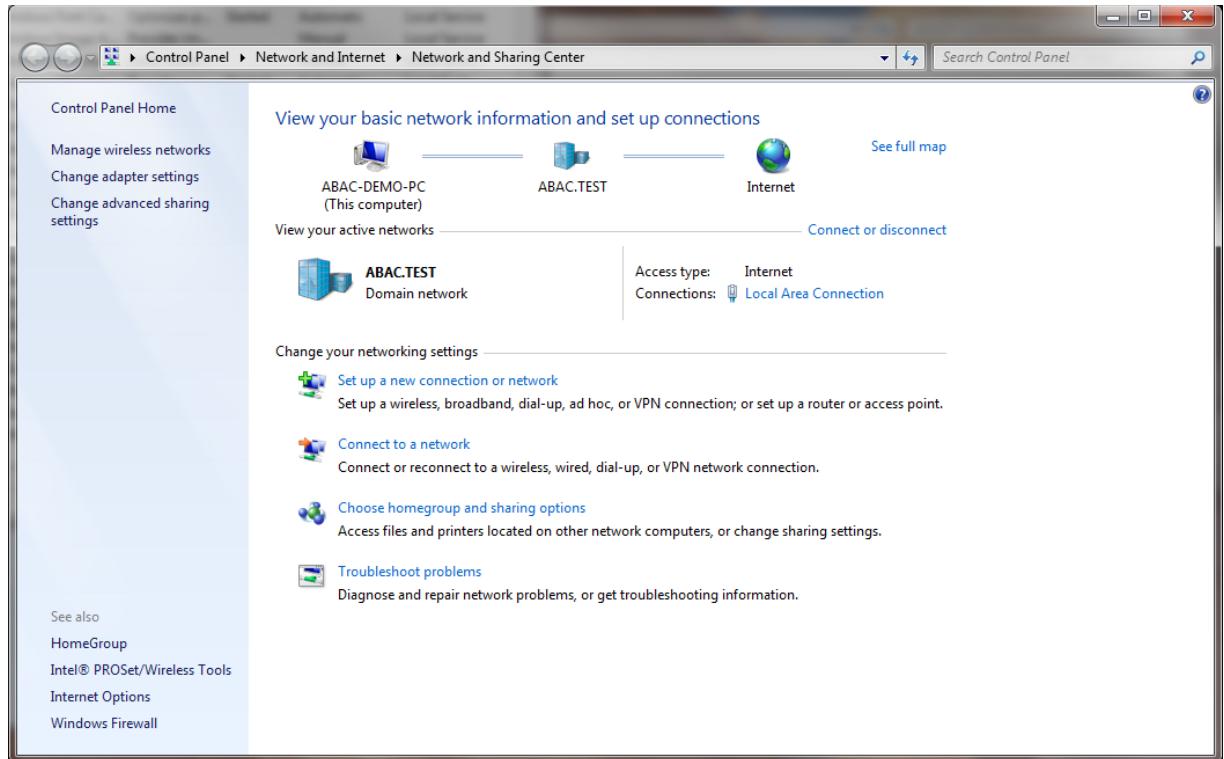
2. Right-click on **Wired AutoConfig**.
3. Select **Properties**.
4. Change the **Startup type** to **Automatic**.



481

- 482 5. Click **Apply**.
- 483 6. Click **OK**.
- 484 7. Go to **Control Panel > Network and Internet > Network and Sharing Center**.

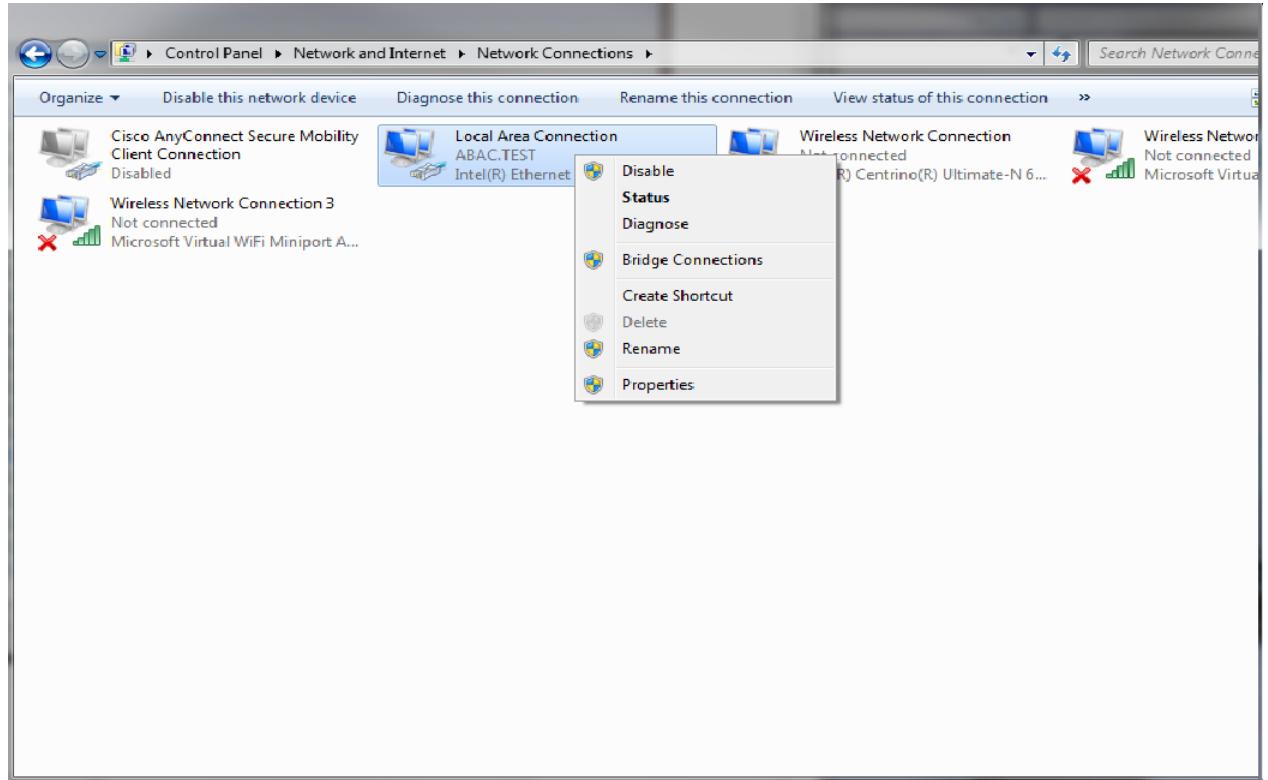
SECOND DRAFT



485

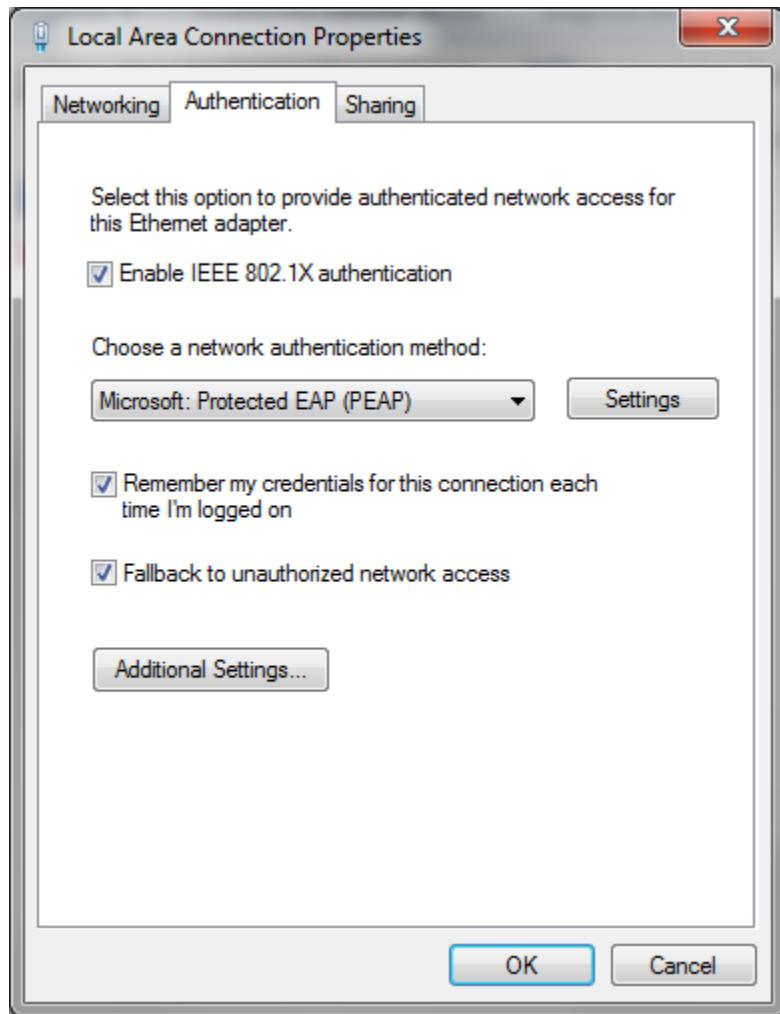
486 8. Click on **Change adapter settings**.

487 9. Right-click on your connection adapter and select **Properties**.



488

489 10. Click the **Authentication** tab.



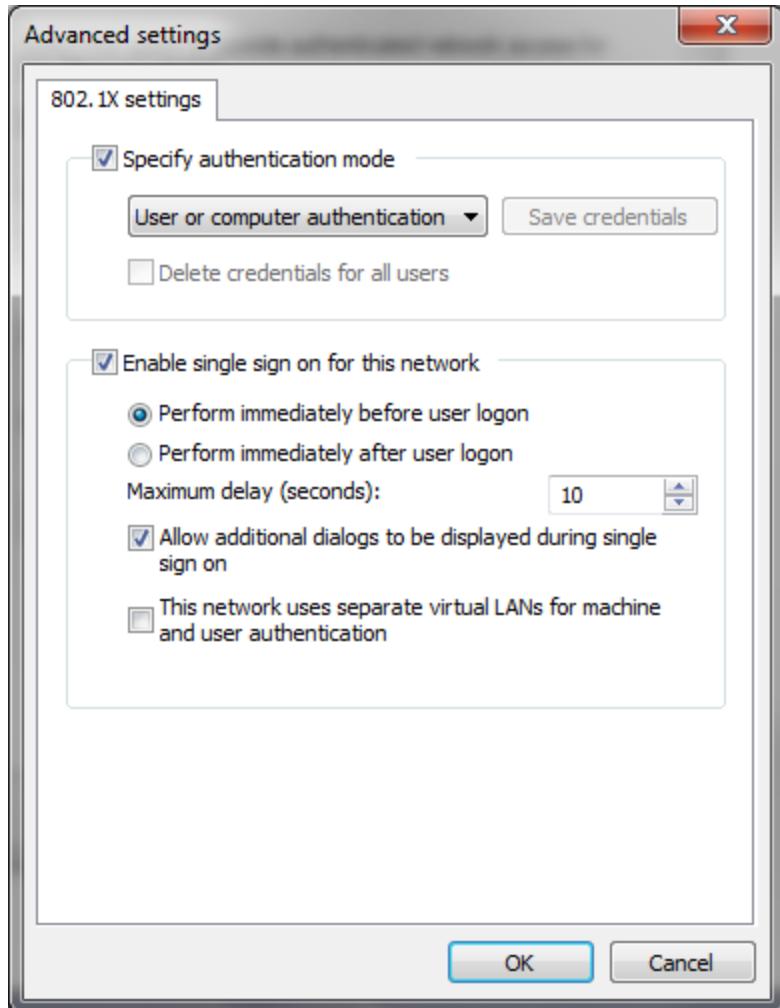
490

491 11. Click on **Additional Settings**.

492 12. Check the **Specify Authentication Mode** checkbox.

493 13. Select **User of computer authentication**.

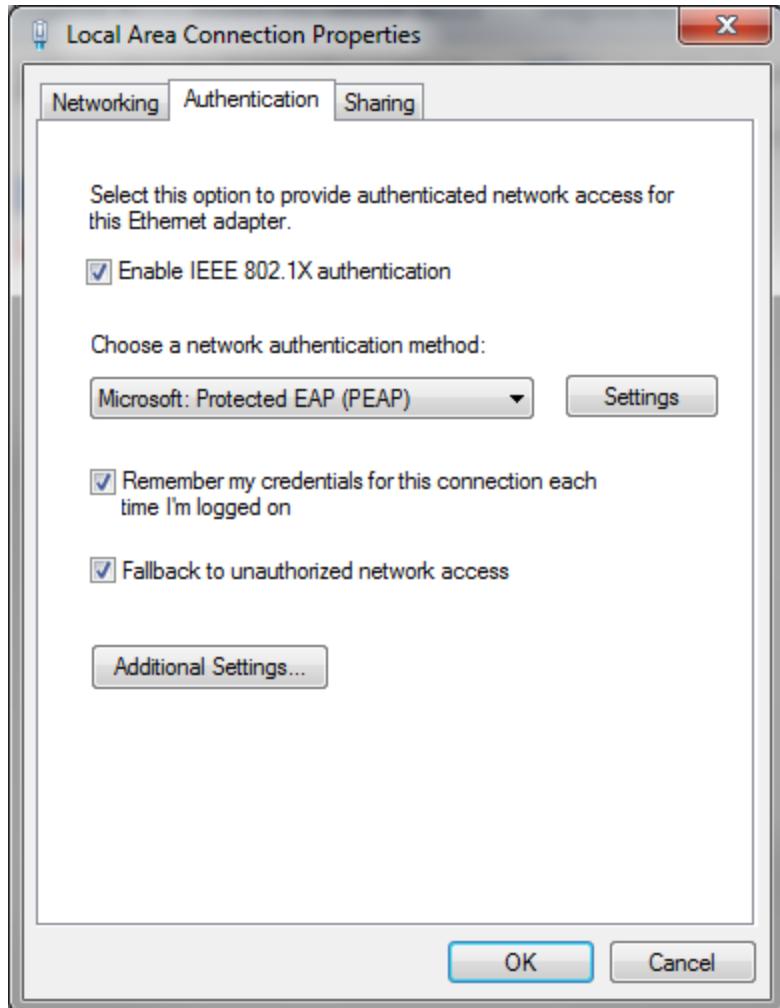
494 14. Check the **Enable single sign on for this network** checkbox.



495

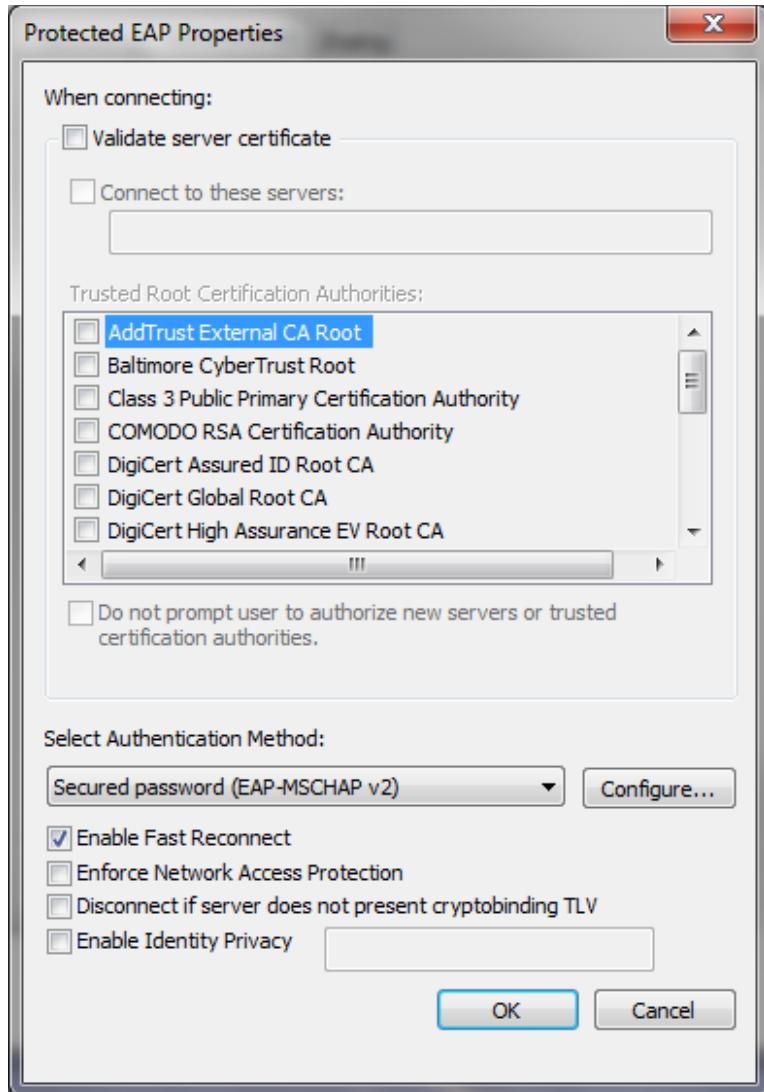
496 15. Click **OK**.

497 16. Click on **Settings** next to **Microsoft: Protected EAP (PEAP)**.



498

499 17. Uncheck **Validate server certificate**.



500

501 18. Click **OK** and proceed back to the desktop and log out.

502 **2.3 Install Nginx Web Server**

503 A web server is required for NAD redirects during the Situational Context Connector's authentication
504 flow. In our build, we implemented the web server using Nginx.

- 505 1. Log on to the server that will host the Nginx web server.
506 2. Follow the instructions at the link below to install Nginx on Windows.

507 <http://nginx.org/en/docs/windows.html>

508 **2.4 Install Microsoft AD**

509 Log on to the server that will host Microsoft AD.

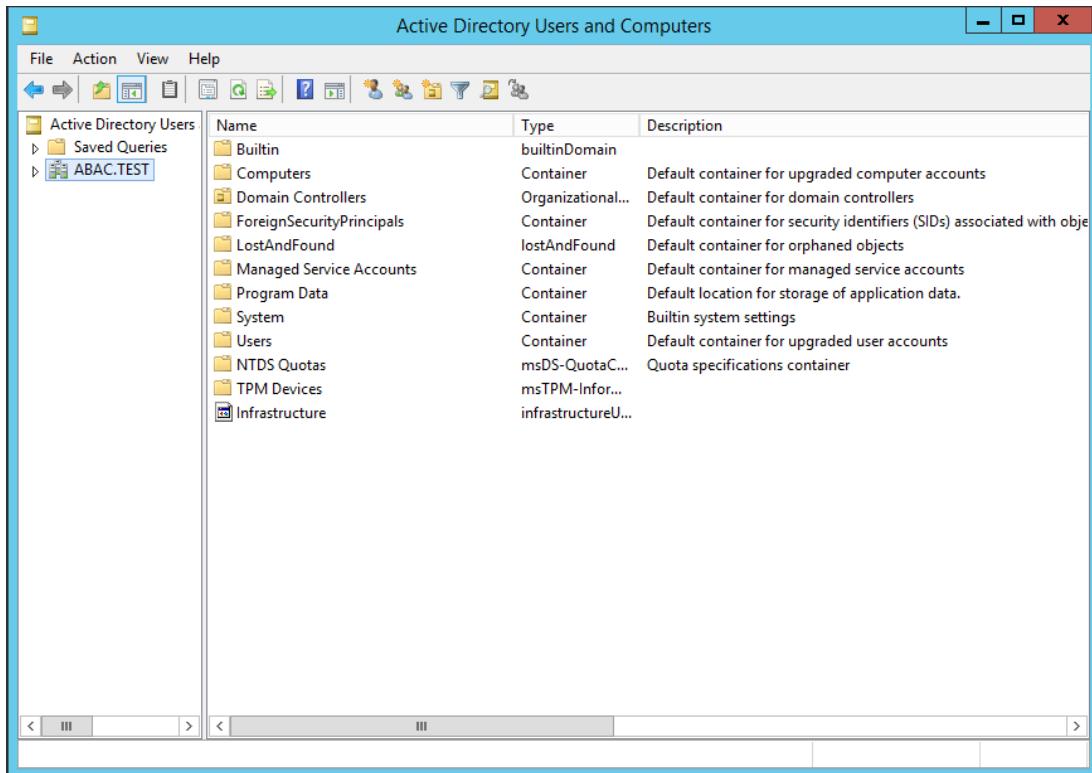
- 510 1. Follow the instructions at the link below to create a new Microsoft AD domain that will store the
511 accounts and identity information for the identity provider.
- 512 2. During setup, you will be asked to provide a name for your new domain.
513 The name of the domain used for this build is **ABAC.TEST**.

514 <https://technet.microsoft.com/en-us/library/jj574166.aspx>

515 **2.4.1 Create a User in Microsoft AD**

516 To create a user account in the Microsoft AD Domain:

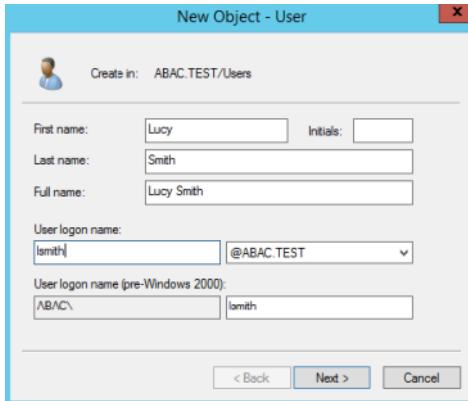
- 517 1. Launch the Active Directory Users and Computers program.



518

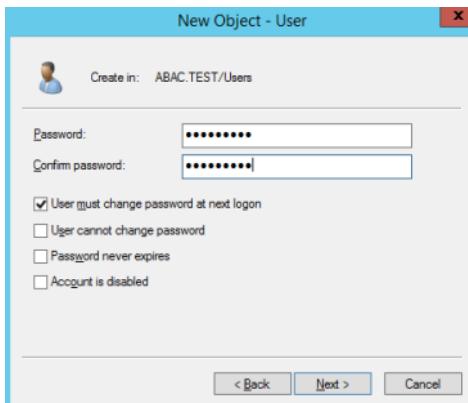
- 519 2. Click on the name of your domain in the left pane and then right-click on the Users folder in the
520 right pane. In this guide, the name of the domain is "ABAC.TEST."
- 521 3. In the pop-up menu that appears, select New, and then select User.
- 522 4. In the New Object - User screen that appears, type the **First** and **Last** name of the user, as well
523 as their **User logon name** (that is, the account name).

SECOND DRAFT



524

- 525 5. Click **Next**.
- 526 6. In the password screen that appears, type in the user's initial password. Then, type it again in the **Confirm password** field. When users log in for the first time, they will be prompted to create their own unique password.

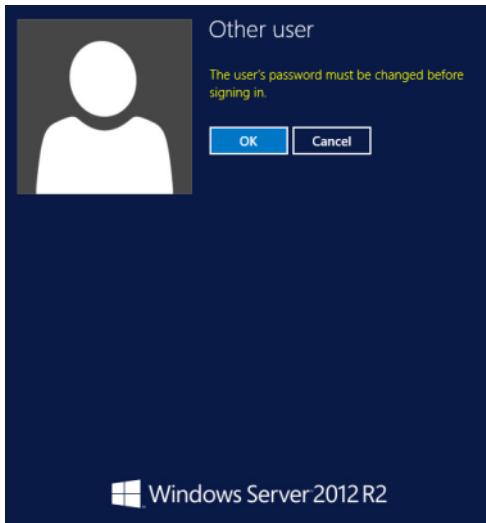


529

- 530 7. Click **Next**.
- 531 8. In the confirmation screen with information about the new user that appears, click **Finish** to complete the operation.

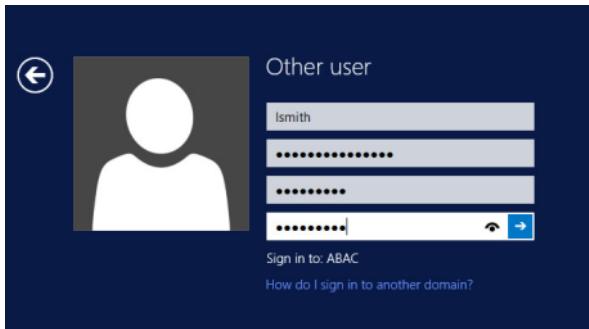
533 When the user logs on to the domain for the first time, the user will be prompted to create a
534 new, unique password.

535 The following illustrations demonstrate what the new password screens may look like on
536 Microsoft Windows Server 2012 when the user Lucy Smith attempts to log on to a computer in
537 the **ABAC.TEST** domain using her user name **lsmith** and the initial password.



538

539 When Lucy clicks **OK**, she will see the screen below. She will type in her new password, which
 540 adheres to the organization's password strength policy; then she will type the password in again
 541 to confirm.



542

543 When she presses Enter, Microsoft Windows will change her password.

544 2.4.2 Create the Lightweight Directory Access Protocol User for Federated 545 Authentication

546 Follow the steps in the previous section to create a user named Lightweight Directory Access Protocol
 547 (**LDAP**) user in Microsoft AD. The PingFederate-IdP will use this user account to perform LDAP queries in
 548 Microsoft AD.

549 2.4.3 Create the LDAP User for Cisco ISE Administration

550 Follow the steps in the previous section to create a user named **ciscoise_svc_account** in Microsoft AD.
 551 The Cisco ISE will use this user account to perform LDAP queries in Microsoft AD.

552 2.5 Configure the Cisco Switch

553 The Cisco Switch is configured in this build to represent realistic network segmentation separating users
 554 and protected network components and services on the IdP's network. Two virtual local area networks
 555 (VLANs) are configured, and traffic is routed between the user VLAN and the services VLAN.

- 556 1. Complete the initial setup of the switch with the *Running Express Setup* instructions found in the
557 document “Getting Started Guide for the Catalyst 2960-X and 2960-XR Switches,” available at
558 the link below.

559 http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/hardware/quick/guide/b_gsg_2960xr.html#task_0410FE6F6E3B4D9EB6175EBE40A03FD0

- 561 2. The switch in our build is configured as seen below.

```
562 service timestamps debug datetime msec
563 service timestamps log datetime msec
564 no service password-encryption
565 !
566 hostname Switch
567 !
568 boot-start-marker
569 boot-end-marker
570 !
571 !
572 username admin privilege 15 secret 5 $1$ZHMh$mD3FQRDvhAVbuFg49iOyq.
573 aaa new-model
574 !
575 !
576 aaa authentication login default local
577 aaa authentication dot1x default group radius
578 aaa authorization console
579 aaa authorization exec default local
580 aaa authorization network default group radius
581 aaa accounting update periodic 5
582 aaa accounting dot1x default start-stop group radius
583 !
584 !
585 !
586 !
587 !
588 aaa server radius dynamic-author
589   client 10.33.7.9 server-key [xxxxxxxxxxxxxx]
590 !
591 aaa session-id common
592 clock timezone EST -4 0
593 switch 1 provision ws-c2960x-24ts-l
594 !
595 !
596 !
597 !
598 ip dhcp excluded-address 10.33.50.193 10.33.50.194
599 ip dhcp excluded-address 10.33.7.1 10.33.7.230
600 !
601 ip dhcp pool CLIENTS
602   network 10.33.50.192 255.255.255.240
603   default-router 10.33.50.193
604   dns-server 10.97.74.8
605 !
606 ip dhcp pool NCCOE
607   network 10.33.7.0 255.255.255.0
608   default-router 10.33.7.1
609   dns-server 10.97.74.8
610 !
611 !
612   ip domain-name abac.test
613   ip name-server 10.33.7.230
```

```

614      vtp mode transparent
615      !
616      !
617      !
618      !
619      !
620      epm logging
621      !
622      !
623      crypto pki trustpoint TP-self-signed-1455706752
624          enrollment selfsigned
625          subject-name cn=IOS-Self-Signed-Certificate-1455706752
626          revocation-check none
627          rsakeypair TP-self-signed-1455706752
628      !
629      !
630      crypto pki certificate chain TP-self-signed-1455706752
631          certificate self-signed 01
632              3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
633              31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
634              69666963 6174652D 31343535 37303637 3532301E 170D3136 30383135 32313530
635              35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
636              4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 34353537
637              30363735 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
638              8100970B 2180DACE EC47660F 5DCEEB8 8E55475C 39A36018 FE770EFF 378662F6
639              8846AD8E D4F0E922 33E1B06E AA2526F0 16A8B451 07227347 2B82C6F6 EFA04BAC
640              D561EBA9 F0B85AE2 C50977DC 605D7573 489FD27B 0583F6FE 8D70DF0B CBD3162B
641              9E1FE937 371FA4AE 905EA47A 667ACC32 05D5DC7F 1E582001 DD40C159 3A21479C
642              D34F0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
643              551D2304 18301680 1457B47B 85B93B03 3557754B 9298D87C 89ED062 64301D06
644              03551D0E 04160414 57B47B85 B93B0335 57754B92 98D87C89 EED06264 300D0609
645              2A864886 F70D0101 05050003 81810079 9AE74655 14C450FE 6F6B4E63 1CBD9AF
646              15D8B911 2C55785A 020E18C7 4F3C28A7 A714E961 933DE0DF F3FB19F6 08AA2FD4
647              DCD95B9F 161317C0 3BDCD75F D4850E06 38153D02 260300D1 8D1D8794 9B9A0A3B
648              C69269C6 E83CD422 F24F3C17 1AE8F70A F75E7B0F A8FF7946 85328DFB 1C39F676
649              C3FC5B29 A1900D37 E7226576 183765
650          quit
651      dot1x system-auth-control
652      !
653      spanning-tree mode rapid-pvst
654      spanning-tree extend system-id
655      !
656      !
657      !
658      !
659      vlan internal allocation policy ascending
660      !
661      vlan 207,2084
662      !
663      !
664      !
665      !
666      !
667      !
668      !
669      !
670      !
671      !
672      !
673      !
674      interface FastEthernet0
675          no ip address
676          no ip route-cache

```

```
677      !
678      interface GigabitEthernet1/0/1
679          switchport access vlan 207
680          spanning-tree portfast edge
681      !
682      interface GigabitEthernet1/0/2
683          switchport access vlan 2084
684          switchport mode access
685          spanning-tree portfast edge
686      !
687      interface GigabitEthernet1/0/3
688          switchport access vlan 207
689          spanning-tree portfast edge
690      !
691      interface GigabitEthernet1/0/13
692          switchport access vlan 2084
693          spanning-tree portfast edge
694      !
695      interface GigabitEthernet1/0/20
696          switchport access vlan 2084
697          switchport mode access
698          authentication event fail action next-method
699          authentication order dot1x mab
700          authentication priority dot1x mab
701          authentication port-control auto
702          authentication violation restrict
703          snmp trap mac-notification change added
704          snmp trap mac-notification change removed
705          dot1x pae authenticator
706          dot1x timeout tx-period 10
707          spanning-tree portfast edge
708          spanning-tree bpduguard enable
709      !
710      interface GigabitEthernet1/0/21
711          switchport access vlan 207
712          switchport mode access
713          authentication event fail action next-method
714          authentication order dot1x mab
715          authentication priority dot1x mab
716          authentication port-control auto
717          authentication violation restrict
718          snmp trap mac-notification change added
719          snmp trap mac-notification change removed
720          dot1x pae authenticator
721          dot1x timeout tx-period 10
722          spanning-tree portfast edge
723          spanning-tree bpduguard enable
724      !
725      interface Vlan1
726          no ip address
727          no ip route-cache
728      !
729      interface Vlan207
730          ip address 10.33.7.2 255.255.255.0
731      !
732      interface Vlan2084
733          ip address 10.33.50.194 255.255.255.240
734          ip helper-address 10.33.7.9
735      !
736          ip default-gateway 10.33.7.1
737          ip http server
738          ip http authentication local
739          ip http secure-server
```

```
740      !
741      !
742      ip access-list extended ACL-REDIRECT
743          deny ip any host 10.33.7.9
744          permit ip any host 10.33.7.6
745      ip radius source-interface Vlan207
746      logging origin-id ip
747      logging source-interface Vlan207
748      logging host 10.33.7.9 transport udp port 20514
749      access-list 10 permit 10.33.7.9
750      access-list 10 deny any log
751      !
752      snmp-server community ciscoro RO 10
753      snmp-server trap-source Vlan207
754      snmp-server source-interface informs Vlan207
755      snmp-server enable traps snmp linkdown linkup
756      snmp-server enable traps mac-notification change move threshold
757      snmp-server host 10.33.7.9 version 2c cisco mac-notification
758      !
759      radius-server attribute 6 on-for-login-auth
760      radius-server attribute 8 include-in-access-req
761      radius-server attribute 25 access-request include
762      radius-server dead-criteria time 30 tries 5
763      !
764      radius server ABAC-CiscoISE
765          address ipv4 10.33.7.9 auth-port 1812 acct-port 1813
766          key [xxxxxxxxxxxxxxxxxx]
767      !
768      !
769      line con 0
770      line vty 0 4
771          exec-timeout 300 0
772          logging synchronous
773      line vty 5 15
774          logging synchronous
775      !
776      ntp server 10.97.74.8
777      mac address-table notification change
778      mac address-table notification mac-move
779      !
780      end
```

2.6 Install and Configure Cisco Identity Services Engine

- 782 1. On a Redhat or CentOS server, boot from the Cisco ISE iso file.
- 783 2. At the installation screen, choose your boot option and press **Enter**.

```
Welcome to the Cisco Identity Services Engine Installer  
Cisco ISE Version: 2.1.0.474  
  
Available boot options:  
[1] Cisco ISE Installation (Keyboard/Monitor)  
[2] Cisco ISE Installation (Serial Console)  
[3] System Utilities (Keyboard/Monitor)  
[4] System Utilities (Serial Console)  
<Enter> Boot existing OS from hard disk.  
  
Enter boot option and press <Enter>.  
boot: 1_
```

784

- 785 3. Once installation is complete, it restarts. Enter **setup** and press **Enter**.

```
*****  
Please type 'setup' to configure the appliance  
*****  
localhost login: setup_
```

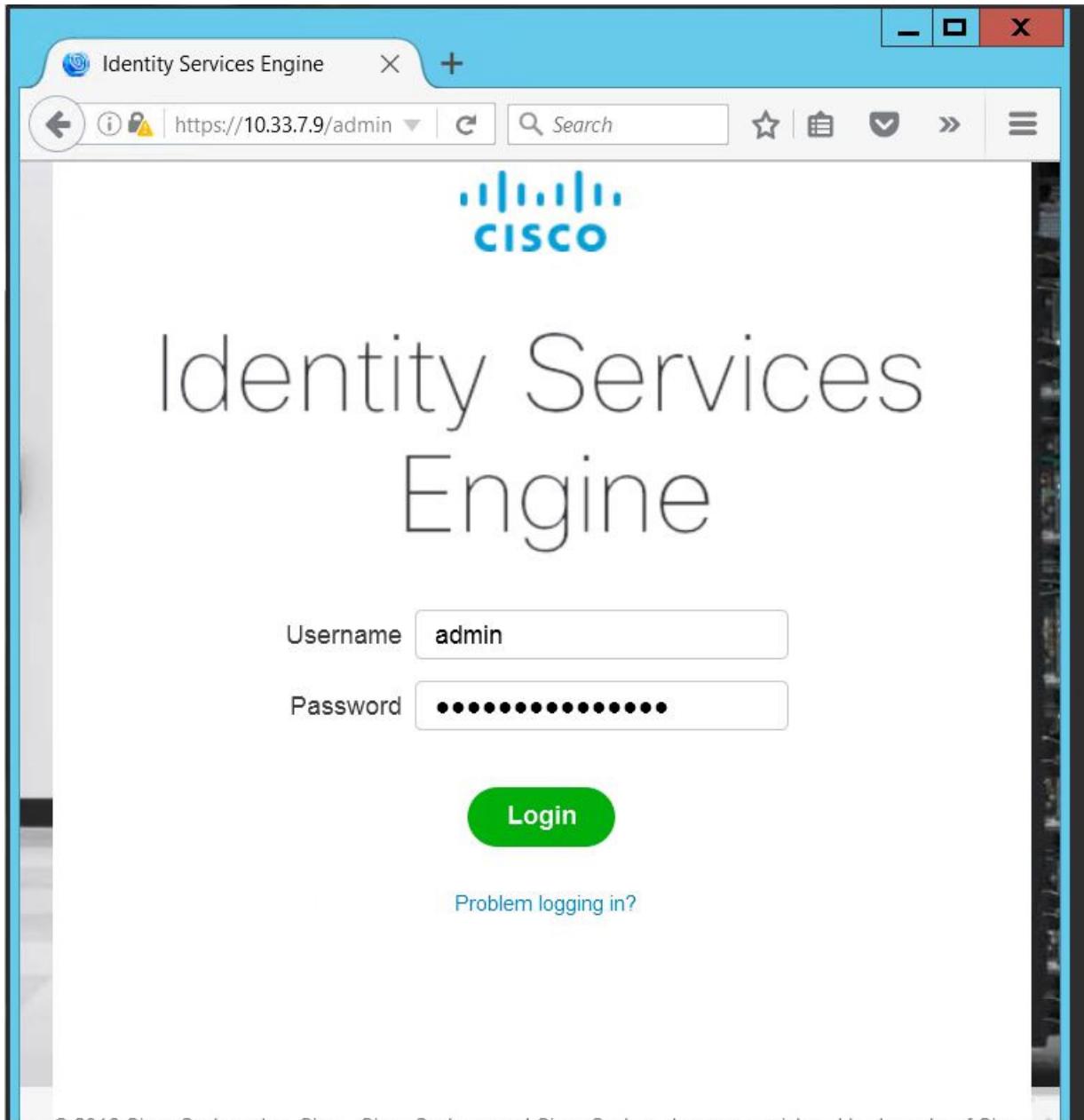
786

- 787 4. Enter ISE configuration information (ISE hostname, Internet Protocol [IP] addresses, domain
788 name service [DNS] domain and name servers, Network Time Protocol [NTP] server, time zone,
789 username, and password):

```
Press 'Ctrl-C' to abort setup  
Enter hostname[]: ABAC-CiscoISE  
Enter IP address[]: 10.33.7.9  
Enter IP netmask[]: 255.255.255.0  
Enter IP default gateway[]: 10.33.7.1  
Enter default DNS domain[]: abac.test  
Enter primary nameserver[]: 10.33.7.230  
Add secondary nameserver? Y/N [N]: Y  
Enter secondary nameserver[]: 8.8.8.8  
Add tertiary nameserver? Y/N [N]: Y  
Enter tertiary nameserver[]: 8.8.4.4  
Enter NTP server[time.nist.gov]: 129.6.15.30  
Add another NTP server? Y/N [N]: N  
Enter system timezone[UTC]: EST  
Enable SSH service? Y/N [N]: Y  
Enter username[admin]: admin  
Enter password:  
Enter password again:  
Copying first CLI user to be first ISE admin GUI user...  
Bringing up network interface...
```

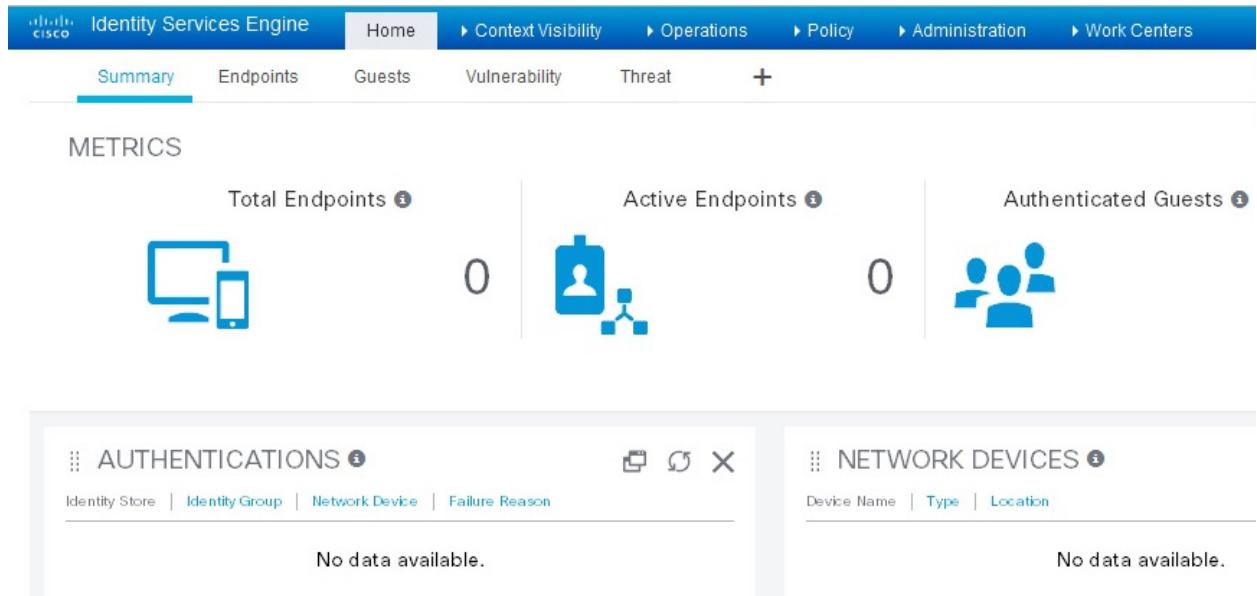
790

- 791 5. ISE will continue and create the database. ISE will automatically reboot after a successful
792 installation. After the reboot, you can log in to ISE via any browser reachable in your domain by
793 entering <https://<IP Address of ISE server>/admin>, as seen below:



794

795 6. After logging in, you will see the default ISE dashboard:



796

2.6.1 Configure Cisco ISE with Microsoft AD

- 797 1. While logged in to the ISE administration console, navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.
- 800 2. Follow the instructions at the link below, beginning on page 11, Steps 1-9, to configure Cisco ISE with Microsoft AD. Note: these instructions are in the section **Testing Environment > Cisco Identity Service Engine (ISE 2.0) VM Setup > Initial ISE Setup > AD User Setup**.
- 803 <https://developer.cisco.com/fileMedia/download/01d139d2-c08a-4f5d-a0ce-8d0473a021d9>
- 804 3. Note: At step 3, provide the credentials of the user account created earlier to join ISE to the existing AD domain (eg, **ciscoise_svc_account**).

2.6.2 Add Network Device to ISE

- 807 1. Follow the instructions at the link below, beginning on page 14, Steps 1-3, to register the NAD with ISE. Note: these instructions are in the section **Testing Environment > Cisco Identity Service Engine (ISE 2.0) VM Setup > Initial ISE Setup > Network Devices**.
- 810 <https://developer.cisco.com/fileMedia/download/01d139d2-c08a-4f5d-a0ce-8d0473a021d9>
- 811 2. Note: The shared secret used on Step 2, “Enable Radius Authentication Settings and enter the shared secrets,” must be the same key that was used for configuring aaa on the switch. If the switch has not yet been configured, remember to record the secret used here so that it can be used when configuring aaa on the switch.

2.6.3 Configure ISE for pxGrid

- 816 Follow the instructions at the link below, beginning on page 15, Steps 1-4, to enable a pxGrid persona, 817 used by the Situational Context Connector to query ISE for device and network attributes. Note: these 818 instructions are in the section **Configuring ISE for pxGrid**.

819 2.6.4 Enable ISE Policy Sets

- 820 1. Navigate to Administration > System > Settings.

The screenshot shows the Cisco ISE web interface. At the top, there's a navigation bar with tabs: Home, Context Visibility, Operations, Policy, Administration, and a quick search bar. Below the navigation bar is a sidebar with sections: TRICS (Summary, End), AUTHENTICATION (Identity Store, Identity Groups), and Device Portal Management (No data available). The main content area has a title 'System' and a sub-menu with options: Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings (which is highlighted with a blue background). To the right of the main content area, there are three columns of links: Network Resources (Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, Location Services), pxGrid Services (Feed Service, Profiler, PassiveID, AD Domain Controllers, Mapping Filters), and Threat Centric NAC (Third Party Vendors). At the bottom of the main content area, it says 'No data available.' next to two large circular icons.

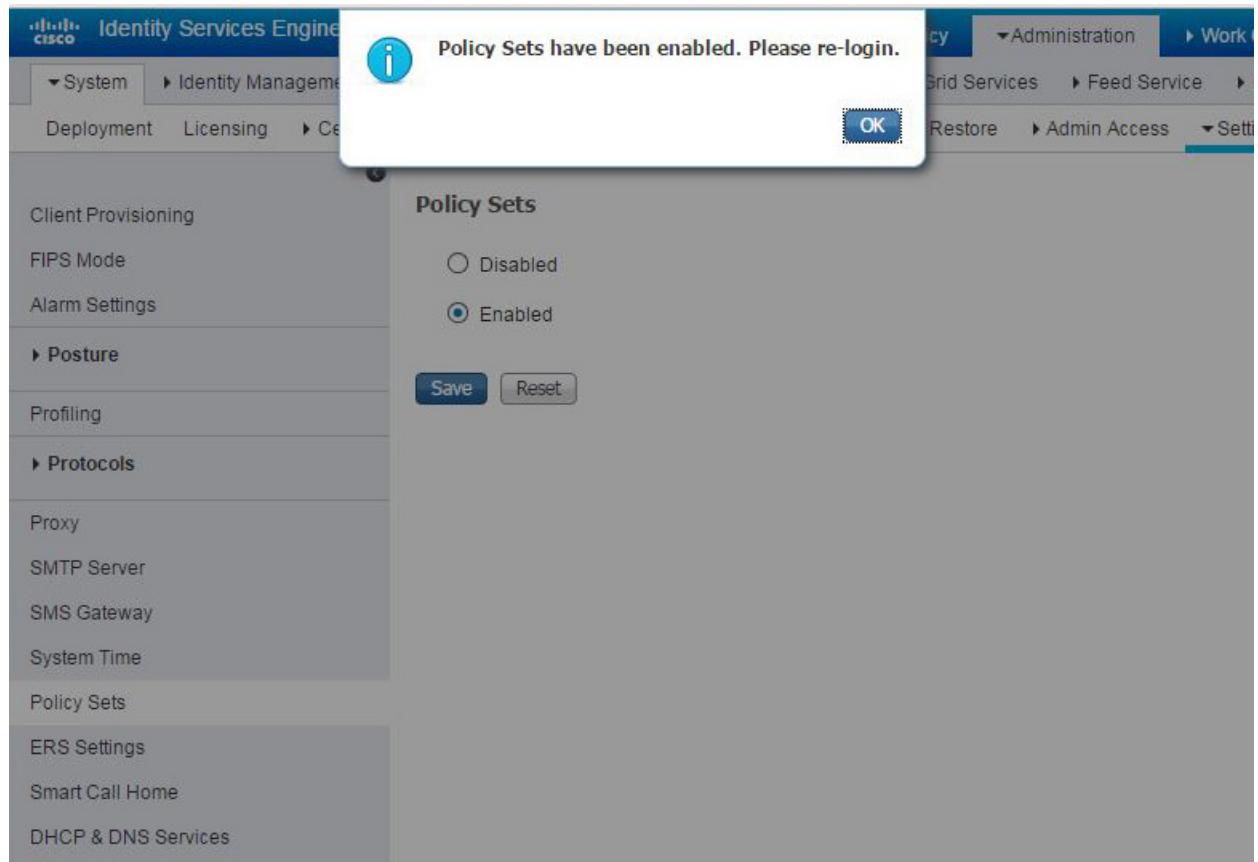
821

- 822 2. In the left sidebar, click on **Policy Sets**.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and more. The main menu on the left is expanded to show System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Policy. The Policy section is currently selected. The right-hand panel displays the 'Policy Sets' configuration. It features a radio button for 'Enabled' which is selected, and another for 'Disabled'. Below the radio buttons are 'Save' and 'Reset' buttons. A sidebar on the left lists various system settings: Client Provisioning, FIPS Mode, Alarm Settings, Posture, Profiling, Protocols, Proxy, SMTP Server, SMS Gateway (with a lock icon), System Time, Policy Sets (which is the current page), ERS Settings, Smart Call Home, and DHCP & DNS Services.

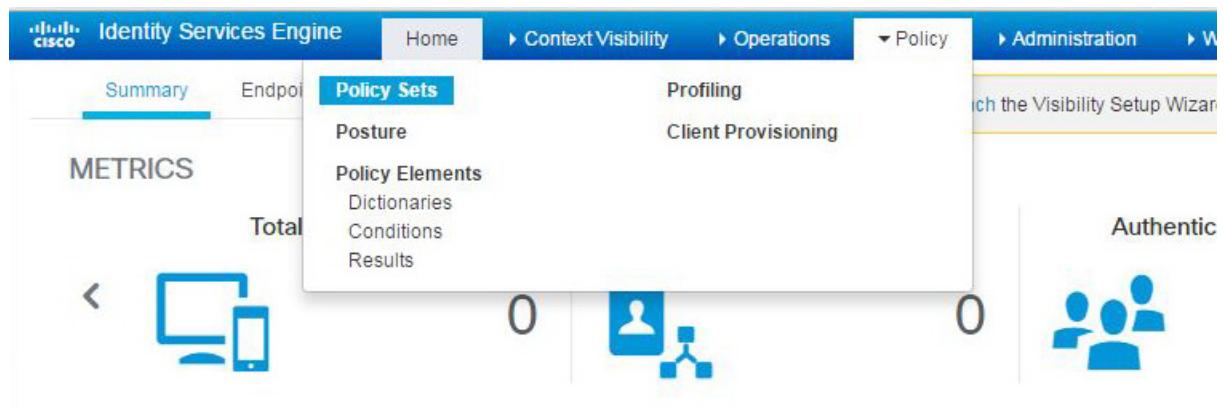
823

- 824 3. Click the **Enabled** radio button.
825 4. Click **Save**.
826 5. In the pop-up, click **OK** and log back into ISE.



828 2.6.5 Configure Authentication Policy

- 829 1. Navigate to **Policy > Policy Sets**.



SECOND DRAFT

The screenshot shows the Cisco Identity Services Engine (ISE) interface under the 'Policy Sets' tab. In the 'Authentication Policy' section, there are two rules: 'MAB' and 'Default'. The 'MAB' rule has conditions 'If Wired_MAB OR Wireless_MAB' and permissions 'Allow Protocols : Default Network Access and use Internal Endpoints'. The 'Default' rule has conditions 'If Wired_802.1X OR Wireless_802.1X' and permissions 'Allow Protocols : Default Network Access and use All_User_ID_Stores'. Below this, the 'Authorization Policy' section is shown with several exception rules listed.

832

833 3. Click on the **Dot1x** rule.

This screenshot is similar to the previous one but focuses on the 'Dot1x' rule within the 'Authentication Policy' section. The 'Dot1x' rule has conditions 'If Wired_802.1...' and permissions 'Allow Protocols : Default Network Access and use All_User_ID_Stores'. The 'Default' rule is also visible below it. The rest of the interface, including the 'Authorization Policy' section, remains the same.

834

835 4. Click on the plus icon.

SECOND DRAFT

The screenshot shows the Cisco Identity Services Engine (ISE) Policy Elements interface. On the left, there's a sidebar with 'Policy Sets' and a search bar. Below it is a 'Summary of Policies' section with 'Global Exceptions' and a selected 'Default' policy set. The main panel displays the 'Authentication Policy' configuration for the 'Default' policy set. It includes rules for 'MAB' and 'Dot1X'. The 'Dot1X' rule uses 'All_User_ID_Stores' as the identity source. A note at the bottom states: 'Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or RADIUS MSCHAP. It is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.' The 'Authorization Policy' section shows three exceptions: 'Wireless Black List Default', 'Profiled Cisco IP Phones', and 'Profiled Non Cisco IP Phon'.

836

837

5. Change the value of Identity Source to “pxGrid_Users.”

This screenshot is identical to the one above, but the 'Identity Source' field for the 'Dot1X' rule has been changed from 'All_User_ID_Stores' to 'pxGrid_Users'. The rest of the configuration remains the same, including the three exceptions listed under 'Authorization Policy'.

838

839

6. Scroll to the bottom of the page and click Save.

SECOND DRAFT

The screenshot shows the Cisco Identity Services Engine (ISE) interface under the 'Policy Elements' tab. In the 'Authentication Policy' section, there are three entries:

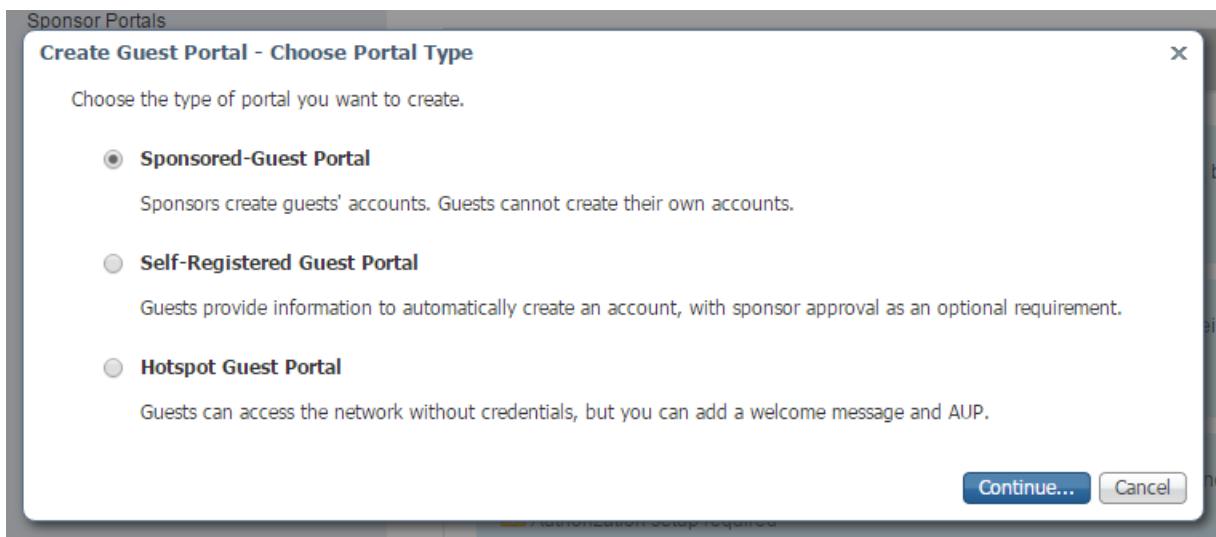
- MAB : If Wired_MAB OR Wireless_MAB then use Internal Endpoints
- Dot1X : If Wired_802.1... then Allow Protocols: Default Network Access
- Default : Use pxGrid_Users

At the bottom, a 'Default Rule (if no match)' is defined: Allow Protocols: Default Network Access and use: All_User_ID_Stores.

840

2.6.6 Configure Authorization Policy

1. Navigate to **Administration > Guest Access**.
2. In the sidebar, click on **Guest Portals**.
3. Click **Create**.
4. Choose **Sponsored Guest Portal**.



846

5. Click **Continue**.
6. Provide a name, **ABAC-Guest**.

SECOND DRAFT

849

- Under Portal settings, set the **HTTPS port** to **8000**.

The screenshot shows the Cisco Identity Services Engine interface. In the top navigation bar, 'Guest Access' is selected under 'Network Access'. In the left sidebar, 'Guest Portals' is selected. On the main page, there is a 'Customization' section with a 'Description' field and a 'Portal test URL' field. Below this is a 'Port and Flow Settings' section. A callout box highlights the 'Portal Settings' section where the 'HTTPS port' is set to '8000'. To the right, a 'Guest Flow (Based on settings)' diagram shows a flow from 'LOGIN' to 'AUP'. At the bottom right, a success message says 'Server Response Guest portal is saved successfully'.

850

851

- Click **Save**.

This screenshot shows the same Cisco Identity Services Engine interface as the previous one, but with a different focus. The 'Configure' tab is selected in the top navigation bar. The 'Guest Portals' section in the sidebar is still active. The main area displays various 'Page Settings' sections: 'Login Page Settings', 'Acceptable Use Policy (AUP) Page Settings', 'Guest Change Password Settings', 'Guest Device Registration Settings', 'BYOD Settings', 'Guest Device Compliance Settings', 'Post-Login Banner Page Settings', 'VLAN DHCP Release Page Settings', 'Authentication Success Settings', and 'Support Information Page Settings'. At the bottom right, a success message box is visible with the text 'Server Response Guest portal is saved successfully'.

852

853

- In the main menu, navigate to **Policy > Policy Elements**.

Dictionaries

Name	Description
ACIDEX	Profiler ACIDEX
ACTIVEDIRECTORY	Profiler ACTIVEDIRECTORY
APIC	Dictionary for APIC
CDP	Profiler CDP dictionary
CERTIFICATE	Cisco Certificate
CWA	Cisco CWA Dictionary
CiscoPEP	Cisco PEP Dictionary
DEVICE	Cisco Device Dictionary
DHCP	Profiler DHCP dictionary
ENDPOINTPURGE	Profiler ENDPOINTPURGE
EPS	EPS Dictionary
EndPoints	System_Dictionary
Guest	Guest Dictionary
GuestAccess	GuestAccess dictionary
IOTASSET	Profiler IOTASSET
IP	Profiler IP dictionary
Identity Mapping	Identity Mapping
IdentityGroup	System_Dictionary
InternalCA	Dictionary for Internal CA
InternalEndpoint	System_Dictionary
InternalUser	System_Dictionary
LLDP	Profiler LLDP dictionary
MAC	Profiler MAC dictionary
MDM_LOG	Dictionary for MDM Log

854

855 10. In the submenu, navigate to **Results > Authorization > Authorization Profiles**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Workspaces. Below this, a secondary navigation bar has tabs for Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements (which is selected). A sidebar on the left contains links for Authentication, Authorization (selected), Authorization Profiles, Downloadable ACLs, Profiling, Posture, and Client Provisioning. The main content area is titled "Standard Authorization Profiles" and includes a note: "For Policy Export go to Administration > System > Backup & Restore > Policy Export Page". Below this is a table with columns for Name, Profile, and a Cisco logo with a plus sign. The table lists several profiles: Blackhole_Wireless_Access, Cisco_IP_Phones, Cisco_WebAuth, NSP_Onboard, Non_Cisco_IP_Phones, DenyAccess, and PermitAccess.

	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco +
<input type="checkbox"/>	Cisco_IP_Phones	Cisco +
<input type="checkbox"/>	Cisco_WebAuth	Cisco +
<input type="checkbox"/>	NSP_Onboard	Cisco +
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco +
<input type="checkbox"/>	DenyAccess	
<input type="checkbox"/>	PermitAccess	

856

- 857 11. Click **Add**.
- 858 12. In the **name** field, enter “**IDIPRedirect**.”
- 859 13. Set the **access type** to “**ACCESS_ACCEPT**.”
- 860 14. Under **Common Tasks**, put a check next to **Web Redirection (CWA, MDM, NSP, CPP)**.
- 861 15. In the revealed fields, choose **Centralized Web Auth**.
- 862 16. Set the **ACL field** to “**ACL-REDIRECT**.”
- 863 17. Set the value such that it matches the created guest portal, “**ABAC-Guest**.”
- 864 18. Put a check next to **Static IP/Host name/FQDN**.

SECOND DRAFT

865

19. Enter the hostname of the server on which Ping Federate is running, "idp.abac.test."

The screenshot shows the 'Authorization Profiles > New Authorization Profile' screen. The 'Name' field is set to 'IDIPRedirect'. The 'Access Type' dropdown is set to 'ACCESS_ACCEPT'. The 'Network Device Profile' dropdown shows 'Cisco'. In the 'Common Tasks' section, 'Web Redirection' is checked, and the 'Value' dropdown is set to 'ABAC-Guest'. A static IP/Host name/FQDN 'idp.abac.test' is also listed.

866

867

20. Click **Submit**.

The screenshot shows the 'Advanced Attributes Settings' and 'Attributes Details' sections for the 'IDIPRedirect' profile. The 'Attributes Details' section contains a large block of text representing a URL with session and portal parameters. At the bottom, there are 'Submit' and 'Cancel' buttons.

868

869 2.6.7 Add Rule for Authorization Policy

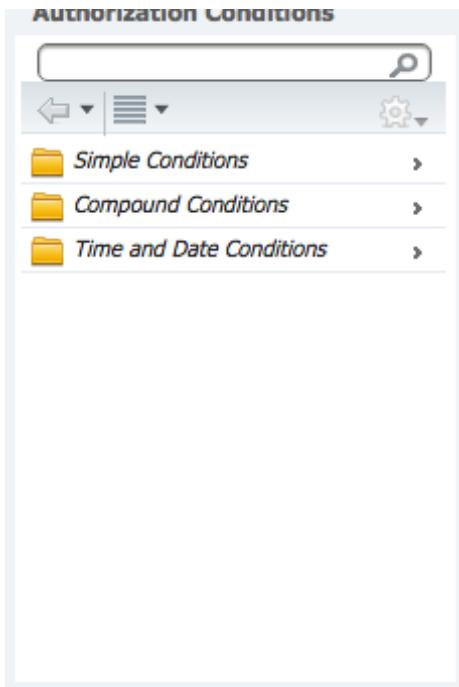
- 870 1. Navigate to **Policy > Policy Sets**.
- 871 2. In the right sidebar, click on **Default**.
- 872 3. Under the Authorization Policy section, click the **triangle** next to edit.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	Action
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access	Edit ▾
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit ▾
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Edit ▾
<input type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess	Edit ▾
<input type="checkbox"/>	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD	Edit ▾
<input type="checkbox"/>	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD	Edit ▾
<input type="checkbox"/>	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guest	Edit ▾
<input type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Logon	if Wireless_MAB	then Cisco_WebAuth	Edit ▾
<input checked="" type="checkbox"/>	Basic_Authenticated_Acces	if Network_Access_Authentication_Passed	then PermitAccess	Edit ▾
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess		Edit ▾

- 873 4. Provide a name for the rule, **IDIP REDIRECT**.
- 874 5. Click the **plus button** next to condition.
- 875 6. Choose, **Select Existing Condition from Library**.

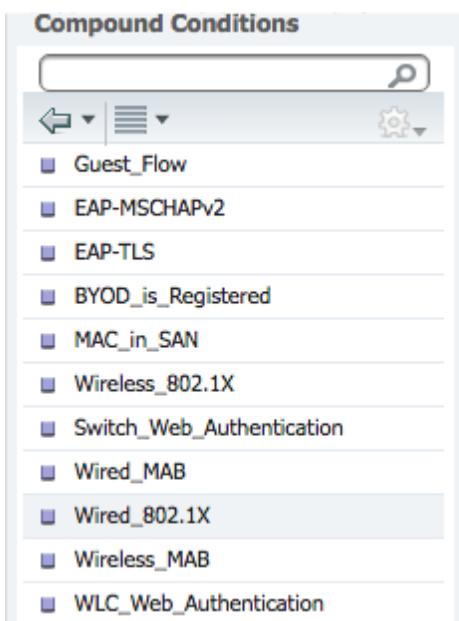
- 877 7. Click the **arrow** next to **Select Condition**

- 879 8. Choose **Compound Conditions**.



881

882 9. Choose **wired_802.1x**.



883

884 10. Click the **cog** icon.

Add All Conditions Below to Library

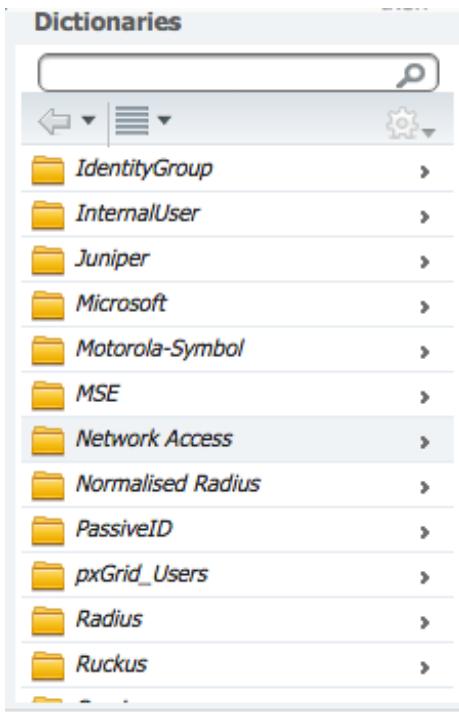
Condition Name	Description
Wired_802.1X	Normalised Radius:RadiusFlowType EQUALS Wired802_1x

Add Attribute/Value
Add Condition from Library
Delete

885

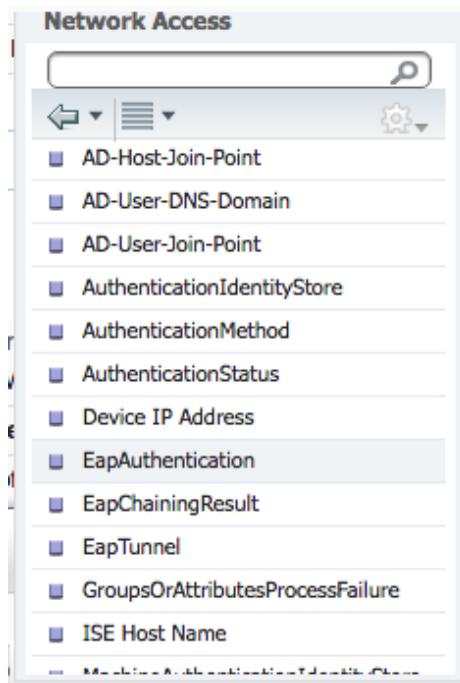
886 11. Choose **Add Attribute/Value**.

887 12. Select **Network Access**.



888

889 13. Select **EapAuthentication**.



890

891 14. Click the **arrow** in the box next to Equals.

892 15. Select **EAP-MSCHAPv2**.

The screenshot shows the Cisco ISE policy configuration interface. On the left, a list of authentication methods is shown in a tree view: EAP-GTC, EAP-MDS, EAP-MSCHAPv2 (selected and highlighted), EAP-TLS, LEAP, Airespace, Alcatel-Lucent, Aruba, Brocade, CERTIFICATE, Cisco, and Cisco-BBSM. In the center, a policy rule is displayed:

```

    Wireless_Basic_Elist_Default
    If Cisco-IP-Phone then Cisco IP Phones
    If Non_Cisco_Profiled_Phones then Non_Cisco_Profiled_Phones
    If (Network_Access_Authentication_Passed AND Compliant_Devices) then Perm
    If (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN) then Perm
    If (Wireless_802.1X AND EAP-MSCHAPv2) then NSP
    If (Guest_Flow AND Wireless_MAB) then Perm
    If Wireless_MAB then Cisco
    If Wi-Fi_Redirect_to_Guest_LogIn then Cisco
  
```

Below this, a condition editor is open for the 'IDIP REDIRECT' condition:

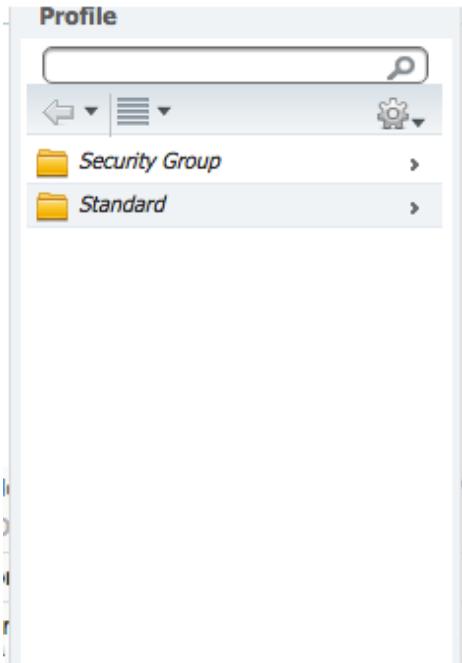
Condition Name	Description	Operator	Value
Wired_802.1X	Normalised Radius:RadiusFlowType EQUALS Wired802_1x	AND	
	Network Access:E...	Equals	

A sidebar on the right lists various vendor-specific modules: Airespace, Alcatel-Lucent, Aruba, Brocade, CERTIFICATE, Cisco, and Cisco-BBSM.

893

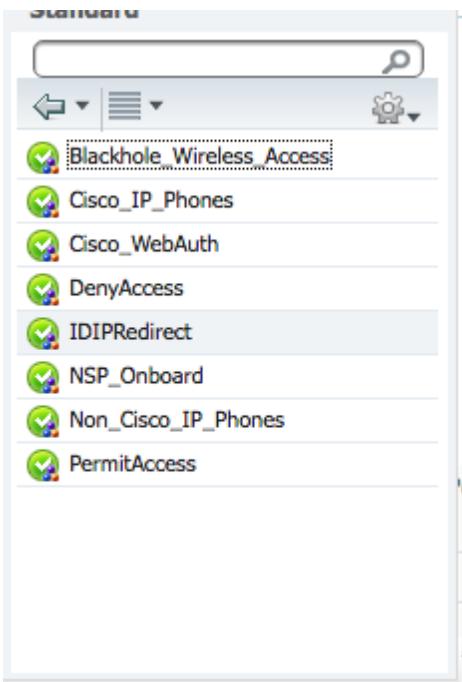
894 16. Click the **plus icon** in the **then** box.

895 17. Select **Standard**.



896

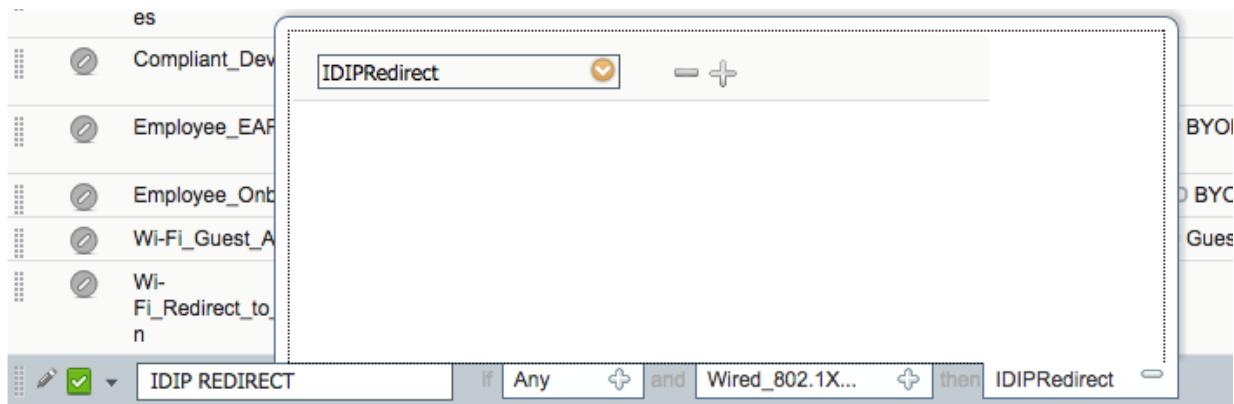
897 18. Select **IDIPRedirect**.



898

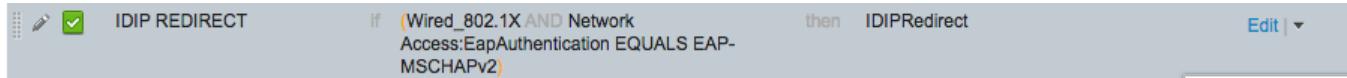
SECOND DRAFT

899



SECOND DRAFT

900 19. Click **Done**.



901

902 20. Click **Save**.



903

904 Machine Authorization Policy Rule

905 21. Navigate to **Policy > Policy Elements > Results**.

906 22. In the left sidebar, navigate to **Authorization > Downloadable ACLs**.

The screenshot shows the "Downloadable ACLs" section of the Cisco Identity Services Engine. The left sidebar has a tree view with nodes like "Authentication", "Authorization" (which is expanded to show "Authorization Profiles" and "Downloadable ACLs"), "Profiling", "Posture", and "Client Provisioning". The main area is titled "Downloadable ACLs" and contains a table with three rows:

Name	Description
DENY_ALL_TRAFFIC	Deny all traffic
PERMIT_ALL_TRAFFIC	Allow all Traffic

There are buttons for "Edit", "Add", "Duplicate", and "Delete" at the top of the table.

907

SECOND DRAFT

- 908 23. Click **Add**.
- 909 24. For **Name** enter **Wired_AD_ONLY**.
- 910 25. For **DACL Content** match the entry below.

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name

Description

* DACL Content

```
1 permit udp any eq 68 any eq 67
2 permit udp any any eq 53
3 permit tcp any eq 3389 any
4 permit ip any host 10.33.7.230
5
6
7
8
9
10
```

(i)

- 911
- 912 26. Click **Submit**.
- 913 27. Navigate back to **Policy > Policy Sets**.
- 914 28. Click on **Default** in the left sidebar.
- 915 29. Click the **triangle** next to the edit button on the IDIP REDIRECT line.
- 916 30. Click **Insert New Rule Above**.

917

IDIP REDIRECT If **(Wired_802.1X AND Network Access:EapAuthentication EQUALS EAP-MSCCHAPV2)** Then **IDIPRedirect**

Basic_Authenticated_Acces If **Network_Access_Authentication_Passed** Then **PermitAccess**

Default If no matches, then **DenyAccess**

Edit

Insert New Rule Above Insert New Rule Below

Duplicate Above Duplicate Below

Delete

- 918 31. Enter **Wired Machine** for the name.
- 919 32. Click the **plus button** next to condition.
- 920 33. Choose **Create New Condition**.

Select Attribute

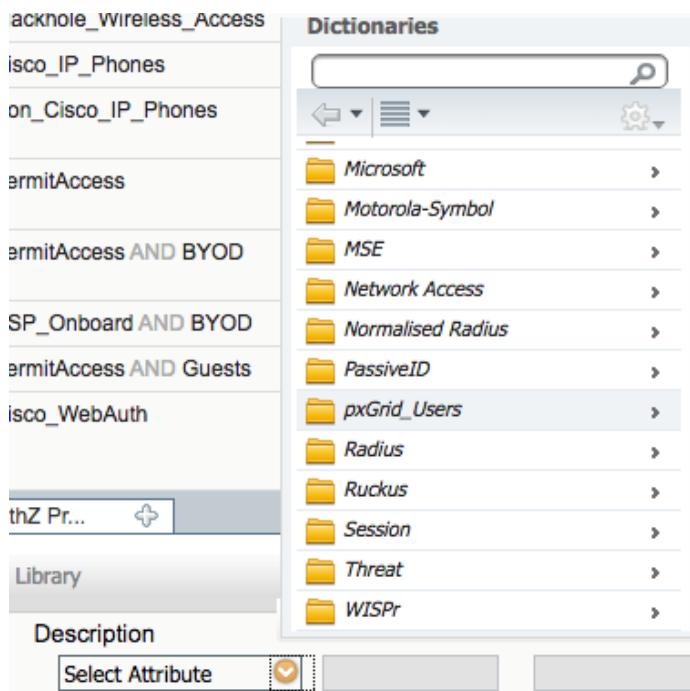
or

921

SECOND DRAFT

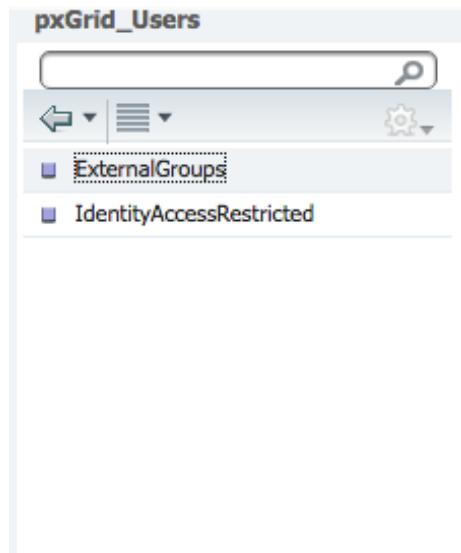
922 34. In the Select Attribute box, click the **arrow**.

923 35. Select **PxGrid_Users**.



924

925 36. Select **ExternalGroups**.

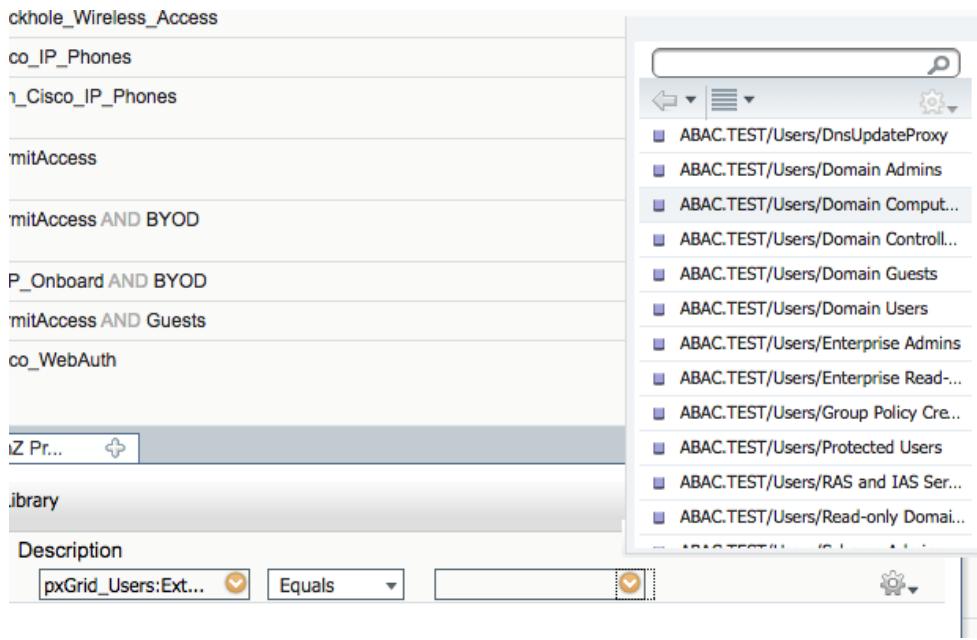


926

927 37. In the equals box, click the **arrow**.

928 38. Select **ABAC.TEST/Users/Domain Computers**.

SECOND DRAFT



929

- 930 39. In the Then box, click on the **plus icon**.
- 931 40. Click the **arrow** in the Select an Item box.
- 932 41. Click the **cog** in the top right of the pop-up window.
- 933 42. Select **Add New Standard Profile**.

The screenshot shows a Cisco Wireless LAN Controller (WLC) configuration interface. On the left, a tree view lists various configuration sections like 'Permissions', 'Blackhole_Wireless_Access', 'Cisco_IP_Phones', 'Non_Cisco_IP_Phones', 'PermitAccess', 'PermitAccess AND BYOD', 'NSP_Onboard AND BYOD', 'PermitAccess AND Guests', and 'Cisco_WebAuth'. A 'then' block is currently selected, showing a dropdown menu with 'Select an item' and a '+' button. On the right, a 'Profile' editor window is open, showing a list of profiles: 'Security Group' and 'Standard'. Two buttons are highlighted with blue boxes: 'Add New Security Group' and 'Add New Standard Profile'. The 'Standard' profile is also highlighted.

934

- 935 43. Name the profile **Wired_AD_ONLY**.
936 44. In the Common Tasks section, check the box next to **DACL Name**.
937 45. Select **Wired_AD_ONLY** from the drop-down.

SECOND DRAFT

Add New Standard Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement (i)

Passive Identity Tracking (i)

Common Tasks

DACL Name

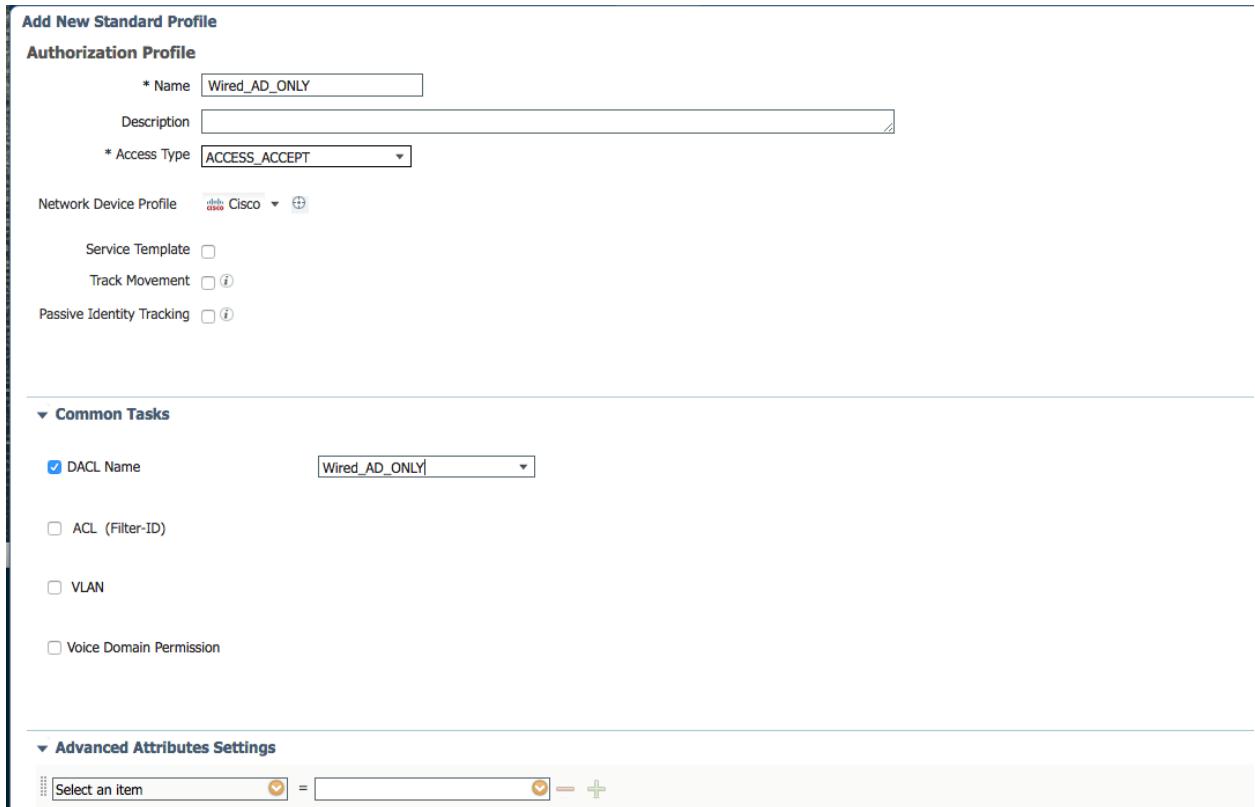
ACL (Filter-ID)

VLAN

Voice Domain Permission

Advanced Attributes Settings

= -



938

939

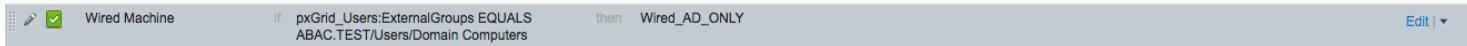
46. Click Save.



940

SECOND DRAFT

941 47. The completed rule should look similar to the one below.



942

943 User Authorization Policy Rule

944 48. Navigate back to **Policy > Policy Elements > Results**.

945 49. In the left sidebar, click on **Authorization > Downloadable ACLs**.

The screenshot shows the "Downloadable ACLs" page in the Cisco Identity Services Engine. The left sidebar has sections for Authentication, Authorization (which is expanded), Profiling, Posture, and Client Provisioning. The main area has tabs for Dictionaries, Conditions, and Results, with Results selected. There is a toolbar with Edit, Add, Duplicate, and Delete buttons. A table lists four downloadable ACLs:

Name	Description
DENY_ALL_TRAFFIC	Deny all traffic
PERMIT_ALL_TRAFFIC	Allow all Traffic
Wired_AD_ONLY	

946

SECOND DRAFT

- 947 50. Click **Add**.
- 948 51. In the Name field, type **Wired_PERMIT_ALL**.
- 949 52. In the DACL Content field, type **permit ip any any**.

Downloadable ACL List > [New Downloadable ACL](#)

Downloadable ACL

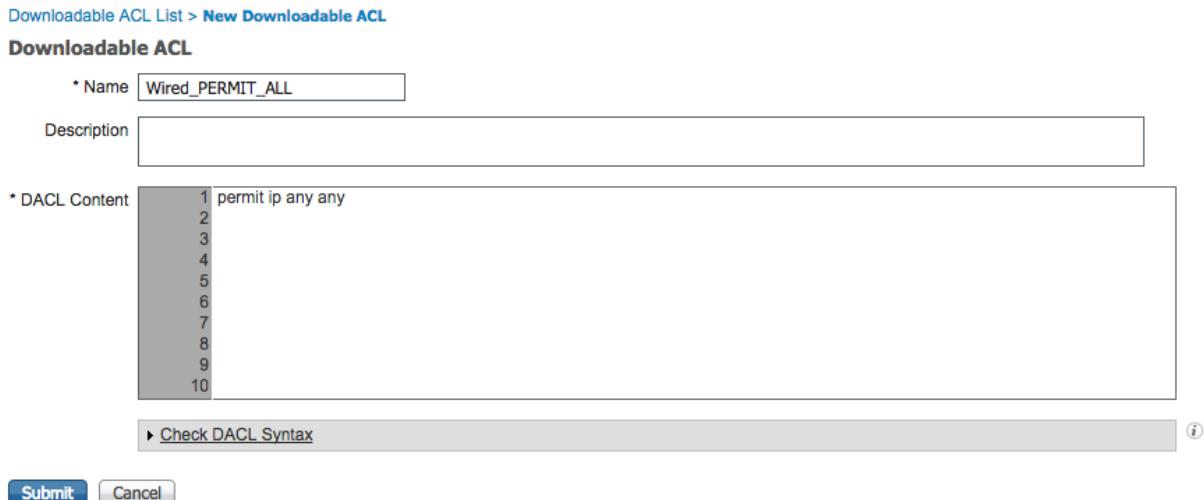
* Name

Description

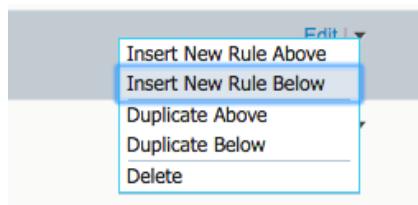
* DACL Content

[Check DACL Syntax](#) (i)

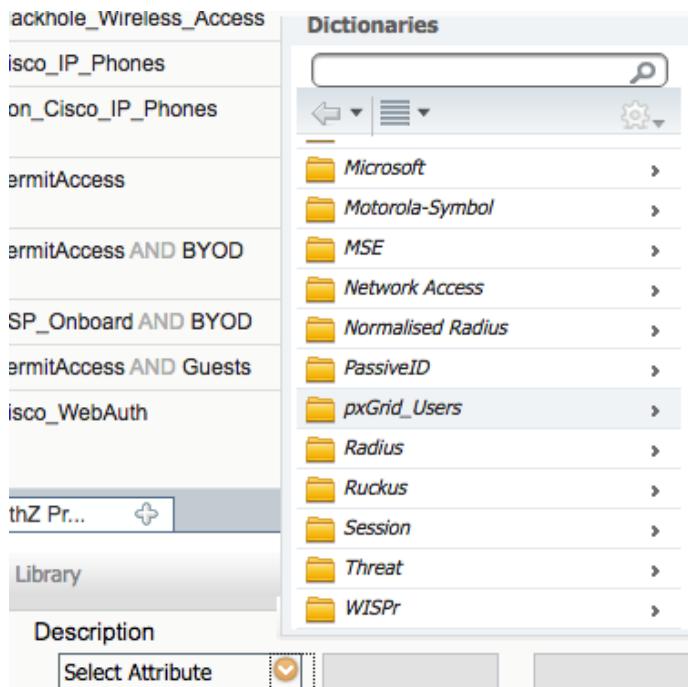
Submit **Cancel**



- 950
- 951 53. Click **Submit**.
- 952 54. Navigate back to **Policy > Policy Sets**.
- 953 55. Click on **Default** in the left sidebar.
- 954 56. Click the **triangle** next to the edit button on the IDIP REDIRECT line.
- 955 57. Click **Insert New Rule Below**.

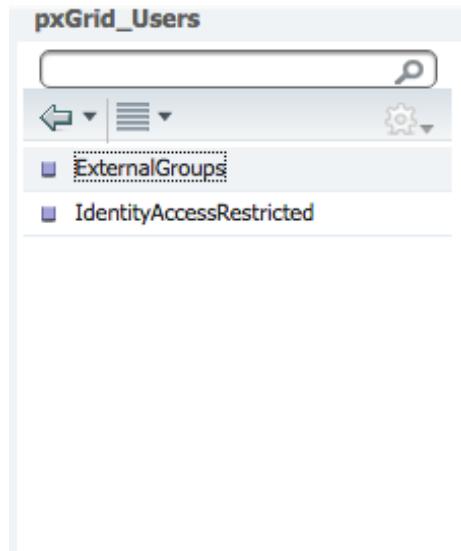


- 956
- 957 58. In the name field, type **Wired User**.
- 958 59. Click the **plus icon** in the condition box.
- 959 60. Select **Create New Condition**.
- 960 61. In the Select Attribute box, click the **arrow**.
- 961 62. Select **PxGrid_Users**.



962

963 63. Select **ExternalGroups**.



964

965 64. In the equals box, click the **arrow**.

966 65. Select **ABAC.TEST/USERS/Domain Users**.

The screenshot shows a software interface with a left sidebar containing a list of conditions and a right panel showing search results. The sidebar includes items like 'PermitAccess AND BYOD', 'SP_Onboard AND BYOD', 'PermitAccess AND Guests', 'sco_WebAuth', 'ired_AD_ONLY', and 'IPRedirect'. Below this is a toolbar with a plus sign and a 'Library' button. The main area has a 'Description' section with a dropdown menu set to 'pxGrid_Users:Ext... Equals ABAC.TEST/User...'. To the right is a search results panel titled 'Search' with a magnifying glass icon. It lists various user objects from the 'ABAC.TEST' domain, such as 'Cloneable Domain...', 'Denied RODC Pa...', 'DnsAdmins', 'DnsUpdateProxy', 'Domain Admins', 'Domain Comput...', 'Domain Controll...', 'Domain Guests', 'Domain Users', 'Enterprise Admins', 'Enterprise Read...', and 'Group Policy Cre...'.

967

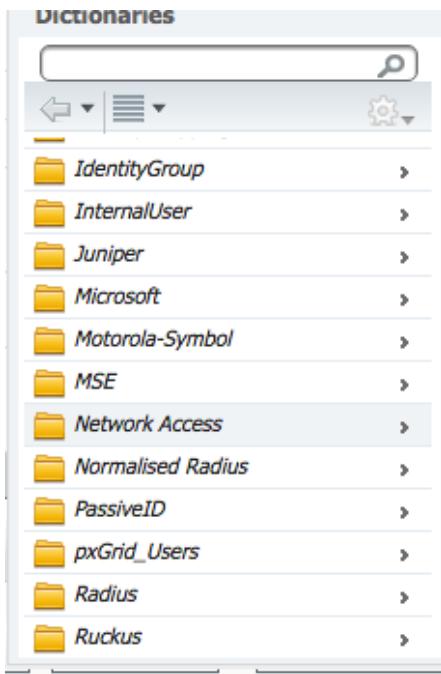
968 66. Click the **cog**.

969 67. Select **Add Attribute/Value**.

The screenshot shows a condition editor window. At the top, there's a header with 'Add All Conditions Below to Library' and two 'Edit | v' buttons. Below this is a table with columns 'Condition Name' and 'Description'. A single row is visible with the condition name 'pxGrid_Users:Ext...' and the description 'ABAC.TEST/User... Equals ABAC.TEST/User... AND'. To the right of the table is a context menu with options: 'Add Attribute/Value' (which is highlighted), 'Add Condition from Library', 'Duplicate', 'Add Condition to Library', and 'Delete'. The background of the window shows a faint grid of user data.

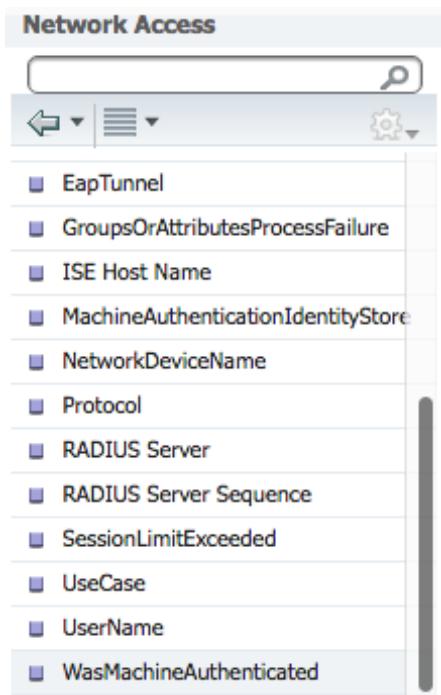
970

971 68. In the new attribute box, select **Network Access**.



972

973 69. Select **WasMachineAuthenticated**.



974

975 70. In the equals box, select **True**.

976 71. In the then box, click the **plus icon**.

977 72. Click **Select an item**.

978 73. Click the **cog**.

- 979 74. Select **Add New Standard Profile**
980 75. In the name field, put **Wired_PERMIT_ALL**.
981 76. In the Common Tasks section, check the box next to **DACL Name**.
982 77. In the box that appears, select **Wired_PERMIT_ALL**.
983 78. Click **Save**.



- 984
985 79. Back on the Policy page, click **Save** again. The final rule should look similar to the one below.

			Wired User	If	(pxGrid_Users:ExternalGroups EQUALS ABAC.TEST/Users/Domain Users AND Network Access:WasMachineAuthenticated EQUALS True)	then	Wired_PERMIT_ALL
--	--	--	------------	----	---	------	------------------

986

987 2.7 **Install RSA AA**

988 RSA AA (On-Premise) comes packaged as a virtual snapshot that must be installed on a virtual machine
989 (VM). A full installation requires core and back office applications, database scripts, and maintenance
990 tools – all necessary for this build. Follow these instructions to install RSA AA for the identity provider.

- 991 1. Log on to VMware and load the RSA AA virtual appliance (e.g., Adaptive Authentication [On-
992 Premise] 7.0.0.0-SNAPSHOT).
- 993 2. Start the RSA AA VM using VMware.
- 994 3. Log on to the server that hosts the new VM.
- 995 4. Launch the RSA AA installation file.
- 996 5. On the Installation Types screen, select **Full** to install all required components. Then, click **Next**.

SECOND DRAFT



997

998 6. Click Next in the Installation Components screen.



999

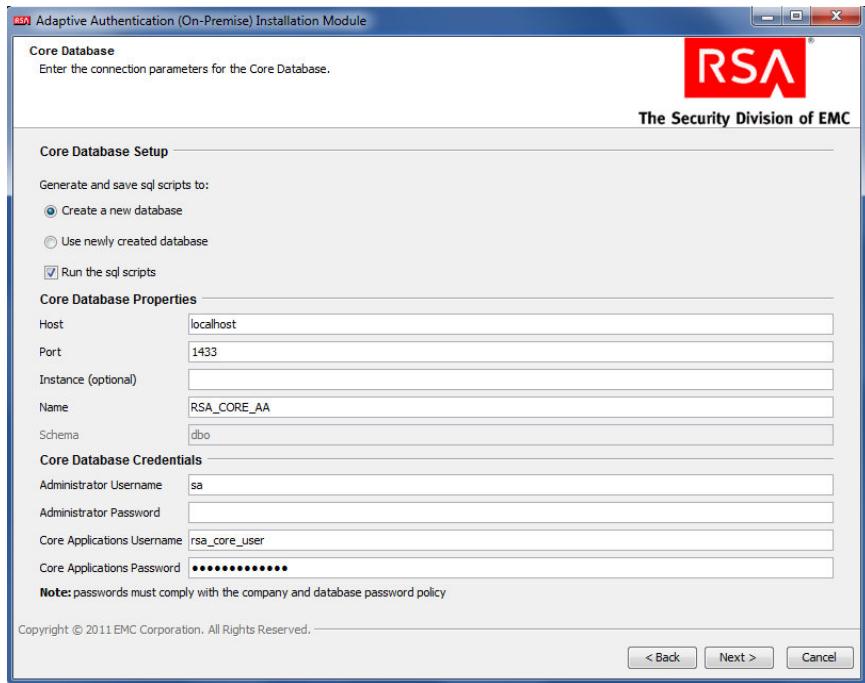
1000 7. In the environment screen, set the database type (MS SQL) and the JDBC driver file as shown in
1001 the following screenshot.

SECOND DRAFT



1002

- 1003 8. For the core database setup, create a new database, and set the core database properties and
1004 credentials.



1005

- 1006 9. On the Core Database screen, set parameters for the data and log files (directory, name, size,
1007 and growth).

SECOND DRAFT



1008

- 1009 10. On the Core Applications screen, select to install the image service, and provide the web service
1010 credentials and application server properties.



1011

- 1012 11. On the Site-to-User Authentication screen, select **Install site-to-user images**, which defines how
1013 the site authenticates users. **Select Save images in the Core Database** and select the directory
1014 shown in the following screenshot as the source directory. During enrollment, users are asked to
1015 select a personal image for authentication.



1016

- 1017 12. Review the configuration options on the Installation Parameters Summary and click **Install**. Once
1018 complete, you can confirm that the installation was successful by viewing the log files.



1019

1020 2.8 Configure RSA AA Rules

- 1021 RSA has a built-in policy management application that allows administrators to create and update rules
1022 for user login based on various scenarios. For example, high-risk users can be required to answer
1023 challenge questions or respond to an out-of-band SMS. For more information, see the Back Office User's
1024 Guide. This example shows how to create a challenge rule for users to confirm identity for large
1025 transactions using an out-of-band SMS code. RSA Back Office allows administrators to manage setup
1026 policy for enabling the enhanced features provided by the RSA adapter, such as answering challenge
1027 questions and providing SMS confirmation codes enabled through this interface.

2.8.1 Create Rule for Non-Persistent User Enrollment

RSA AA requires information for each user to help verify their identity. These users are classified into two groups: persistent and non-persistent users. A rule is created to request enrollment information for non-persistent users, those not kept in the user database.

1. Log in to the Back Office application
[http://xxx.xxx.xxx.xxx:8080/backoffice]
2. Once logged in, click **Manage Rules** under **Policy Management**. Select **New Rule**.
3. In the **Rule Details** (in the **General** tab):
 - a. Set **Rule Name** to **User Enrollment Not Persistent - Adapter**.
 - b. Set the **Status** to **Production**.

Note: The rule cannot be in production until it is created and approved by an administrator.
 - c. In **Event Type**, select **Create User** and **Enroll**.
 - d. Set the **Order** to **1**.

The screenshot shows the 'Edit Rule' interface in the 'General' tab. The 'Rule Name' field contains 'User Enrollment Not Persistent - Adapter'. The 'Status' dropdown is set to 'Production'. In the 'Event Type' section, 'CREATE_USER' and 'ENROLL' are checked. The 'Order' is set to 1. At the bottom, there are 'Next', 'Save & Exit', and 'Cancel' buttons. A note at the bottom left indicates that the rule cannot be in production until it is created and approved by an administrator.

4. Click **Next**.
5. In the **Rule Conditions** page, add a condition (**Condition 1**) and with one expression (**Expression 1**). Set **Expression 1** to **Account Details** such that **Persistent User** is **Equal to FALSE**.

SECOND DRAFT

The screenshot shows the 'Edit Rule' interface. At the top, there are three tabs: 'Policy Management', 'Administration' (which is selected), and 'Customer Service'. Below the tabs, a breadcrumb navigation bar shows 'Edit Rule > 1: General > 2: Conditions > 3: Actions > Summary'. A note below the breadcrumb states: 'Build the condition(s) for this rule using categories, facts, and operators. You must add at least one condition. Each condition must contain at least one expression.' The main area is titled 'Rule Conditions' and contains a section for 'Condition 1'. It shows an expression: 'Account Details' is compared to 'Persistent User' using the 'Equal to' operator, resulting in 'FALSE'. There are buttons for 'Remove Expression', 'Duplicate Expression', 'Join Multiple Expression By OR', 'Add New Expression', and 'Add New Condition'. At the bottom of the page are 'Back', 'Next', 'Save & Exit', and 'Cancel' buttons.

1046

1047 6. Click **Next**.

1048 7. In the **Rule Actions** page:

- 1049 a. Set **Action** to **Challenge**.
- 1050 b. Set **Authentication Methods** to **QUESTION**, **OOBSMS**, **OOBPHONE**, **SECURID**, and **TeleSign2FASms**.
- 1052 c. In **Create Case**, make sure that only **for when authentication fails** is selected.
1053 Then, click **Next**.

The screenshot shows the 'New Rule' interface. At the top, there are three tabs: 'Policy Management', 'Administration' (selected), and 'Customer Service'. Below the tabs, a breadcrumb navigation bar shows 'New Rule > 1: General > 2: Conditions > 3: Actions > Summary'. A note below the breadcrumb states: 'Define the action to occur when the rule conditions are met.' The main area is titled 'Rule Actions'. It shows an 'Action' dropdown set to 'Challenge'. Under 'Authentication Method(s)', there is a list of available methods: 'KBA', 'OOBEMAIL', and 'OTP'. To the right, a list of selected methods is shown: 'QUESTION', 'OOBSMS', 'OOBPHONE', 'SECURID', and 'TeleSign2FASms'. Below this, under 'Create Case:', there are two checkboxes: 'When authentication fails' (checked) and 'When authentication succeeds' (unchecked). At the bottom of the page are 'Back', 'Next', 'Save & Exit', and 'Cancel' buttons.

1054

1055 8. Review the rule settings in the **Summary** page. Then, click **Save and Finish**.

1056 Once created, a rule is in Work in Progress status until approved by an administrator.

1057 9. Click **Status** and **Approve Status**, then click **Approve** to set rule to **Production** status.

The screenshot shows a software interface for managing policies. At the top, there are tabs for 'Policy Management', 'Administration', and 'Customer Service'. Below the tabs, a section titled 'Manage Rules' displays a table of rules. A green success message box is overlaid on the table, stating 'User Enrollment Not Persistent - Adapter has been saved successfully.' The table has columns for 'Order', 'Rule Name', 'Event Type', 'Current Status', 'Pending Status', 'Action', and 'Date Modified'. One row is visible, showing Order 1, Rule Name 'User Enrollment Not Persistent - Adapter', Event Type 'CREATE_USER_ENROLL', Current Status 'Work In Progress', Pending Status 'None', Action 'Challenge', and Date Modified '2015-07-09 12:18 (GMT)'. Below the table, a detailed view of the selected rule ('User Enrollment Not Persistent - Adapter') is shown, including its details like Rule Name, Rule ID, Created By, Creation Date, and Description.

1058

1059 You can use these steps to create each of the rules in the following sections.

2.8.2 Create Rule for Persistent User Enrollment

1061 Persistent users are those that will be added to the user table.

1062 **Table 2-1 Persistent User Enrollment**

Rule Name	User Enrollment Persistent –Adapter
Event Type	Create User, Enroll
Rule Order	2
Rule Condition	IF (Account Details > Persistent User Equal to TRUE)
Rule Action	Allow
Authentication Method	
Create Case	No

1063

2.8.3 Create Rule for User Updates

1065 Once users are created, a rule is applied to allow persistent users to update their information.

1066 **Table 2-2 User Update**

Rule Name	User Update
Event Type	User Update
Rule Order	3
Rule Condition	IF (Account Details > Persistent User Equal to TRUE)
Rule Action	Allow
Authentication Method	
Create Case	No

1067

1068 2.8.4 Create Rule for Challenge SMS

1069 In this build, large transactions require users to respond to an out-of-band SMS challenge during
1070 authentication. When transactions meet the prerequisite, a random code will be sent to the user's SMS-
1071 enabled device that must be entered to confirm the transaction.

1072 **Table 2-3 Out-of-Band SMS**

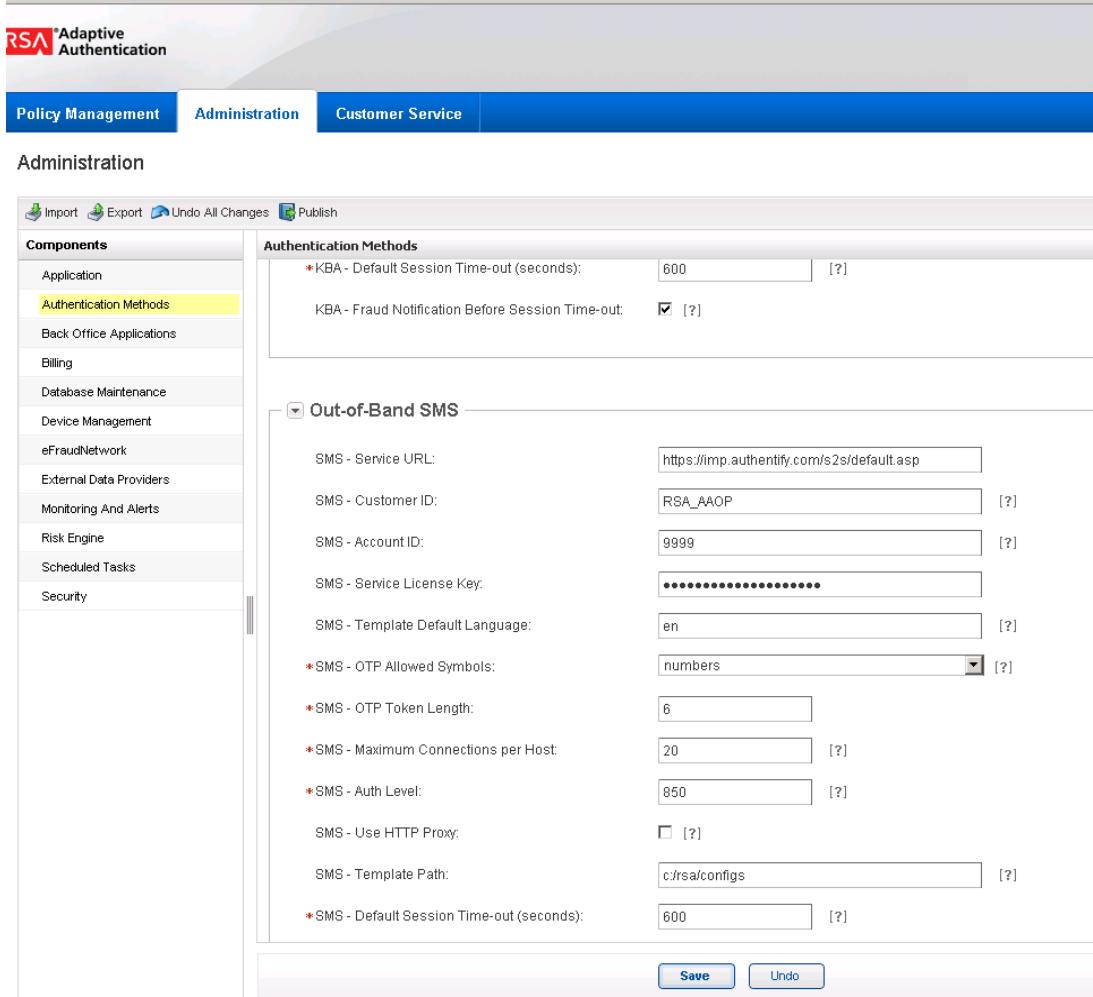
Rule Name	Challenge SMS for Payment
Event Type	Challenge
Rule Order	4
Rule Condition	IF (Transaction Details > Transaction Amount is BETWEEN 5000 and 10000)
Rule Action	Allow
Authentication Method	1. OOBSMS
Create Case	When Authentication Succeeds

1073

1074 **2.8.5 Increase SMS Token Length**

1075 The default token length for out-of-band SMS is currently set to four digits. Access the Administration
 1076 tab on the Back Office application. Under Components, select Authentication Methods and scroll down
 1077 to the Out-of-Band SMS section. Adjust the token length by changing the value of SMS - OTP Token
 1078 Length to six.

1079 **Figure 2-1 Out-of-Band Token Length**



The screenshot shows the RSA Adaptive Authentication Administration interface. The top navigation bar includes 'Policy Management' (selected), 'Administration' (current page), and 'Customer Service'. Below the navigation is a sub-header 'Administration'. The main content area has tabs for 'Components' (selected) and 'Authentication Methods'. Under 'Components', a list of modules like Application, Authentication Methods (highlighted in yellow), Back Office Applications, Billing, Database Maintenance, Device Management, eFraudNetwork, External Data Providers, Monitoring And Alerts, Risk Engine, Scheduled Tasks, and Security. Under 'Authentication Methods', the 'Out-of-Band SMS' section is expanded, showing fields for SMS - Service URL (https://imp.authentify.com/s2s/default.asp), SMS - Customer ID (RSA_AAOP), SMS - Account ID (9999), SMS - Service License Key (redacted), SMS - Template Default Language (en), SMS - OTP Allowed Symbols (numbers), SMS - OTP Token Length (6), SMS - Maximum Connections per Host (20), SMS - Auth Level (850), SMS - Use HTTP Proxy (unchecked), SMS - Template Path (c:/rsa/configs), and SMS - Default Session Time-out (seconds) (600). At the bottom are 'Save' and 'Undo' buttons.

1080

* Required Field

1081 **2.8.6 Create Policy for Session Sign-In**

1082 The following rules create different sign-in scenarios for users based on an RSA-generated risk score at
 1083 the time of login. RSA AA uses a risk engine to give users a risk score to determine a level of trust at the
 1084 time of access. See the tables in [Section 2.8.8](#) for the session sign-in parameters for each risk level.
 1085 Before the session sign-in rules are created, lists need to be created to group users together. This build
 1086 will group users into four categories based on risk level (low, medium, high, and critical).

1087 **2.8.7 Create Lists for Session Sign-In**

- 1088 1. Log in to the Back Office application.
- 1089 2. Go to **Policy Management** and select **Manage Lists**.
- 1090 3. Set List Name to **Low Risk Users**, List Type to **User ID**, and Status to **Enabled**.
- 1091 4. Under **List Content**, select **Add Value** and set the **Value** to **demolowrisk** and **Organization** to **default**.
- 1093 5. Click **Add Value**.
- 1094 6. Click **Save**.

1095 Repeat these steps to create a list for Medium, High, and Critical risk users.

1096 **Figure 2-2 Successful List Created**

The screenshot shows a web-based administrative interface for RSA Adaptive Authentication. At the top, there's a header bar with the RSA logo and navigation links for 'Policy Management', 'Administration', and 'Customer Service'. On the right side of the header, it says 'Logged in as admin' and has a 'Logout' button. Below the header, the main content area is titled 'Manage Lists' with a sub-instruction: 'Manage lists using the table below. To edit a list, click on the List Name.' A green success message box is displayed, stating 'Success! Low Risk Users has been saved successfully.' Below this message is a table with columns for 'List Name', 'List Type', 'Status', and 'Date Modified'. The table contains one row for 'Low Risk Users' with a User ID of 'demolowrisk' and a status of 'Enabled'. The bottom right corner of the interface shows pagination information: '1 items found. Showing 10 per page. 1 of 1'.

1097

1098 **2.8.8 Create Rules for Session Sign-In**

1099 Repeat the steps as in [Section 2.8.1](#) to create the session sign-in rules for different user groups.

1100 **Table 2-4 Session Sign-In – Low Risk**

Rule Name	Session Sign In – Low Risk
Event Type	Session Sign-in
Rule Order	5
Rule Condition	IF (Account Details>User ID within Low Risk Users)
Rule Action	Allow
Authentication Method	
Create Case	No

1101 **Table 2-5 Session Sign-In – Medium Risk**

Rule Name	Session Sign In – Medium Risk
Event Type	Session Sign-in
Rule Order	6
Rule Condition	IF (Account Details>User ID Within Medium Risk Users)

Rule Action	Allow
Authentication Method	1. Question
Create Case	When Authentication Fails

1102 **Table 2-6 Session Sign-In – High Risk**

Rule Name	Session Sign In – High Risk
Event Type	Session Sign-in
Rule Order	7
Rule Condition	IF (Account Details>User ID Within High Risk Users)
Rule Action	Challenge
Authentication Method	1. OOBSMS 2. OOBPhone
Create Case	When Authentication Fails

1103 **Table 2-7 Session Sign-In – Critical Risk**

Rule Name	Session Sign In – Critical Risk
Event Type	Session Sign-in
Rule Order	8
Rule Condition	IF (Account Details>User ID Within Critical Risk Users)
Rule Action	Challenge
Authentication Method	1. Securid
Create Case	When Authentication Fails

1104 **2.8.9 Create Rule to Allow Forced Sign-In for Payment**

1105 The rules for session sign-in in the preceding sections were based predefined facts built within RSA AA.
 1106 This build requires a rule that uses additional facts that are not within the build. Fortunately, new facts
 1107 can be created within the Back Office application. Once custom facts are created, they can be used to
 1108 build further rules.

1109 **2.8.10 Create Custom Fact**

- 1110 1. Log in to the Back Office application.
- 1111 2. Go to **Policy Management** and select **Manage Custom Facts**.
- 1112 3. Select **New** and set the **Field Name** to **Force Workflow**, **Field Type** to **String**, and **Status** to
 1113 **Enabled**.

SECOND DRAFT

The screenshot shows the RSA Adaptive Authentication interface under the 'Policy Management' tab. A modal window titled 'New Fact' is open, prompting the user to define a Custom Fact. The form includes fields for Category (Custom Facts), Fact Name (FORCE WORKFLOW), Field Type (String), Status (Enabled), and Description. The 'Save' button is visible at the bottom.

New Fact

Complete the fields below to define a Custom Fact in the system.

Custom Fact Details

Category:	Custom Facts
*Fact Name:	FORCE WORKFLOW [?]
*Field Type:	String [?]
*Status:	Enabled [?]
Description:	[?]

Save Cancel

1114

1115 4. Click Save.

The screenshot shows the 'Manage Custom Facts' page. A success message indicates that 'FORCE WORKFLOW has been saved successfully'. Below, a table lists the custom fact, showing it was created on 2015-07-10 18:17 (GMT) with a status of Enabled.

Manage Custom Facts

Success!

FORCE WORKFLOW has been saved successfully.

Custom Fact Name	Fact Type	Status	Date Modified
FORCE WORKFLOW	String	Enabled	2015-07-10 18:17 (GMT)

1116

1117 5. Create a new rule using this custom fact that allows payment if this fact is met. Use the settings
1118 in the following table.

1119 **Table 2-8 Force Allow**

Rule Name	Force Allow
Event Type	Payment, Session Sign-in
Rule Order	9
Rule Condition	IF (Custom Fact > Force Workflow Equal to Allow)
Rule Action	Allow
Authentication Method	
Create Case	No

1120

2.9 Install and Configure PingFederate-RP

1121 The PingFederate installation in this section is for the Federation Server at the RP. This is the only
 1122 component at the RP in this section. Even though the goal of this section is to set up the federation for
 1123 the IdP, the basic configuration of the PingFederate-RP in this section is necessary to produce metadata
 1124 that is exchanged with the IdP. A complete configuration of the PingFederate-RP will be performed in
 1125 [Section 3](#) of this guide.

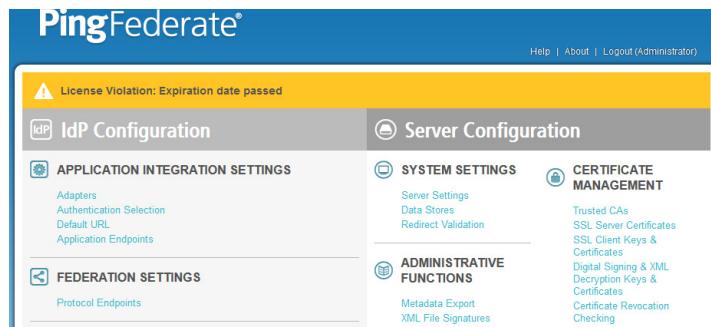
- 1126 1. Log on to the RP's server that will host the PingFederate service, and follow the instructions at
 1127 the link below to install PingFederate and run it as a Windows service.

1128 <https://documentation.pingidentity.com/display/PF73/Installation>

- 1129 2. Follow these steps to perform a basic configuration of the PingFederate-RP and export the
 1130 metadata.

- 1131 3. Launch your browser and navigate to the PingFederate app URL:
 1132 https://<DNS_NAME>:9999/pingfederate/app. Replace DNS_NAME with the fully qualified
 1133 name of the RP's PingFederate server (e.g., <https://rp.abac.test:9999/pingfederate/app>).

- 1134 4. Log on to the PingFederate application using the credentials you configured in the previous
 1135 installation section.



- 1136 5. On the **Main Menu** under **System Settings**, click **Server Settings**.
 1137 6. Click the **Roles and Protocols** tab.
 1138 7. Select **Enable Identity Provider (IdP) role and support the following**.

SECOND DRAFT

- 1140 8. Select SAML 2.0.
- 1141 9. Select WS-Federation.
- 1142 10. Select Enable Service Provider (SP) role and support the following.
- 1143 11. Select the SAML 2.0.

Select the role(s) and protocol(s) that you intend to use with your federation partners.

Enable OAuth 2.0 Authorization Server (AS) role

Enable Identity Provider (IdP) role and support the following:

SAML 2.0

Auto-Connect Profile

SAML 1.1

SAML 1.0

WS-Federation

Outbound Provisioning

WS-Trust

Enable Service Provider (SP) role and support the following:

SAML 2.0

Auto-Connect Profile

Attribute Requester Mapping for X.509 Attribute Sharing Profile (XASP)

SAML 1.1

SAML 1.0

WS-Federation

WS-Trust

Inbound Provisioning

Enable IdP Discovery role (SAML 2.0 only)

Cancel < Previous Next > Save

- 1144
- 1145 12. Click **Next**.
- 1146 13. On the Federation Info screen, enter the Base URL and SAML 2.0 Entity ID using the format
1147 *https://<DNS_NAME>:9031* (e.g., *https://rp.abac.test:9031*).
- 1148 14. Enter the WS-Federation Realm using the format *urn:<DNS_NAME>*
1149 (e.g., *urn:rp.abac.test*).
- 1150 Note: Keep a copy of the urn, because it will be used later to configure the WS-Federation
1151 relationship with SharePoint.

SECOND DRAFT

Base URL *

SAML 2.0 Entity ID *

WS-Federation Realm *

You must create a unique identifier for your server for use with your federation partners. A unique identifier is required for each protocol enabled. You will need to communicate this with your partners out-of-band or through metadata exchange. The Base URL is used to construct other URLs in the system and may be used as part of your system ID.

Cancel < Previous Next > Save

1152

1153 15. Click **Save**.

1154 16. On the **Main Menu** under **Administrative Functions**, click **Metadata Export**.

1155 17. On the Metadata Role screen, select **I am the Service Provider (SP)**.

This system is configured to act as both an IdP and an SP. For which role would you like to generate metadata?

I am the Identity Provider (IdP)
 I am the Service Provider (SP)

Cancel Next >

1156

1157 18. Click **Next**.

1158 19. On the Metadata Mode screen, select **Select information to include in metadata manually**.

Use a connection for metadata generation
 Select information to include in metadata manually
 Use the secondary port for SOAP channel

Cancel < Previous Next >

1159

1160 20. Click **Next**.1161 21. On the Protocol screen, make sure that **SAML 2.0** is listed.

For this metadata file, choose from among the federation protocols you have enabled that support metadata exchange with partners.

SAML 2.0

Cancel < Previous Next >

1162

1163 22. Click **Next**.1164 23. On the Attribute Contract screen, click **Next**.1165 24. On the Signing Key screen, select the certificate that will be used to sign communications with
1166 the IdP.

The screenshot shows a software interface titled "Export Metadata". At the top, there are tabs: "Main", "Export Metadata" (which is selected), "Metadata Role", "Metadata Mode", "Protocol", "Attribute Contract", "Signing Key" (with a star icon), "Metadata Signing", and "XML Encryption Certificate". Below these tabs, a button labeled "Export & Summary" is visible. A message box contains the text: "The metadata may contain a public key that this system uses for digital signatures. If you wish to include a key, please select from the list of available signature keys." Under the heading "DIGITAL SIGNATURE KEYS/CERTS", a dropdown menu shows the option "01:30:DB:8C:25:AB (cn=demo dsig new)". In the bottom right corner of the main window, there are buttons for "Cancel", "< Previous", and "Next >".

1167

1168 25. Click **Next**.1169 26. On the Metadata Signing screen, if you plan to sign the metadata file that will be exported,
1170 select the certificate that will be used to sign the file.

The screenshot shows a software interface titled "Export Metadata". At the top, there are tabs: "Main", "Export Metadata" (which is selected), "Metadata Role", "Metadata Mode", "Protocol", "Attribute Contract", "Signing Key" (with a star icon), "Metadata Signing" (which is selected), and "XML Encryption Certificate". Below these tabs, a button labeled "Export & Summary" is visible. A message box contains the text: "From this list of certificates, choose which one to use for signing the selected file." Under the heading "Signing Certificate", a dropdown menu is labeled "- SELECT -". In the bottom right corner of the main window, there are buttons for "Cancel", "< Previous", and "Next >".

1171

1172 27. Click **Next**.1173 28. On the XML Encryption Certificate screen, select the certificate that the Identity Provider will
1174 use to encrypt XML messages.

SECOND DRAFT

The screenshot shows the 'Export Metadata' interface. At the top, there are tabs: 'Main' (selected), 'Export Metadata', 'Metadata Role', 'Metadata Mode', 'Protocol', 'Attribute Contract', 'Signing Key', 'Metadata Signing', and 'XML Encryption Certificate'. Below these tabs, a button labeled 'Export & Summary' is visible. A note says: 'The metadata may contain a certificate that your partner can use to encrypt XML content. If you wish to include a certificate, please select one from the list.' Under the 'ENCRYPTION KEYS/CERTS' section, a dropdown menu shows '01:4C:09:35:30:19 (cn=demo-sp-enc)'. A 'Manage Certificates...' button is also present. At the bottom right, there are buttons for 'Cancel', '< Previous', and 'Next >'.

1175

1176

29. Click **Next**.

The screenshot shows the 'Export Metadata' interface. At the top, there are tabs: 'Main' (selected), 'Export Metadata', 'Metadata Role', 'Metadata Mode', 'Protocol', 'Attribute Contract', 'Signing Key', 'Metadata Signing', and 'XML Encryption Certificate'. Below these tabs, a note says: 'Click the Export button to export this metadata to the file system.' Under the 'Export Metadata' section, there are several configuration sections: 'METADATA ROLE' (Metadata role: Service Provider), 'METADATA MODE' (Metadata mode: Select information manually, Use the secondary port for SOAP channel: false), 'PROTOCOL' (Protocol: SAML 2.0), 'ATTRIBUTE CONTRACT' (Attribute: None defined), and 'SIGNING KEY'.

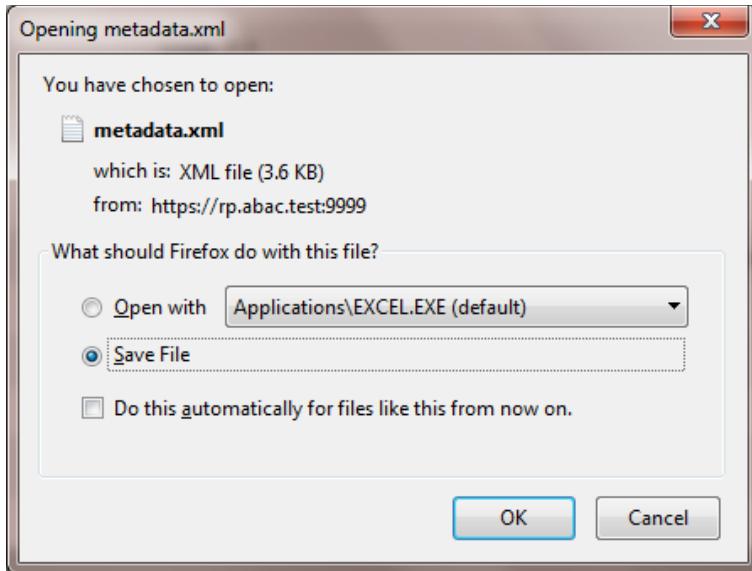
1177

1178

30. Click **Export**.

1179
1180
1181

This will create an export file that contains the metadata of the RP, which you can download using the browser. This file will be used later in the section, when configuring the PingFederate-IDP.



1182

2.10 Install PingFederate-IdP

1184 This PingFederate installation in this section is for the PingFederate-IdP.

1185 Log on to the server that will host the PingFederate service for the IdP, and follow the instructions at the
1186 link below to install PingFederate and run it as a Windows service.

1187 <https://documentation.pingidentity.com/display/PF73/Installation>

2.11 Install the SCE Plug-in for the PingFederate-IdP

1189 The SCE Plug-in integrates the features provided by RSA AA with PingFederate-IdP by providing a
1190 customizable user interface when RSA AA is accessed. New users will be enrolled into RSA's enhanced
1191 security features and be prompted to provide information such as security questions, a phone number,
1192 email address, and an SMS-enabled device. Follow the instructions below to install the SCE Plug-in
1193 adapter for the IdP. The variable <PF-install> used in the instructions corresponds to the PingFederate
1194 installation path. In this build, the PingFederate installation path was *c:\pingfederate-7.3.0*.

- 1195 1. Log on to the server that hosts the PingFederate service for the Identity provider.
- 1196 2. Download the SCE Plug-in adapter jar file (e.g., *sce-adapters-pingfederate-aa.1.1.jar*) to
1197 the local PingFederate server.
- 1198 3. Copy the jar file to **<PF-install>/server/default/deploy**
- 1199 4. From the adapter *dist/conf/template* folder, copy all .html files to
<PF-install>/server/default/conf/template.
- 1200 5. From the adapter *dist/conf/template/assets* folder, copy the *aa* folder to
<PF-install>/server/default/conf/template/assets
- 1203 6. From the adapter *dist/data/adapter-config* folder, copy the *aa* folder to

1204 **<PF-install>/server/default/data/adapter-config**
1205 7. From the adapter `dist/lib` folder, copy all .jar files to
1206 **<PF-install>/server/default/lib**

1207 **2.12 Install the Situational Context Connector for the PingFederate-IdP**

1208 The Situational Context Connector and a Session Validator must be installed. In this build, both are
1209 installed on the PingFederate-IdP Server.

1210 **2.12.1 Install Situational Context Connector**

1211 1. Log on to the server that hosts the PingFederate service for the Identity provider.
1212 2. Download the Situational Context Connector integration zip file (e.g.,
1213 `Situational_Context_Connector_v21.zip`) to the local PingFederate server.
1214 3. Stop the PingFederate service if it is running.
1215 4. Unzip the integration kit distribution file (`Situational_Context_Connector_v21.zip`) and copy
1216 the adapter file, `pf.plugins.ise-idp-adapter.jar`, from the `/dist` to the PingFederate
1217 “deploy” folder:
1218 **<PF_install>\pingfederate\server\default\deploy**
1219 5. Create a new sub-directory under the PingFederate `\deploy` folder called “portal.”
1220 **<PF_install>\pingfederate\server\default\deploy\portal**
1221 6. Create a new sub-directory under the new `\portal\` directory called “gateway.”
1222 **<PF_install>\pingfederate\server\default\deploy\portal\gateway**
1223 7. Copy the “index.jsp” from the Adapter .zip `/dist` folder to
1224 **<PF_install>\pingfederate\server\default\deploy\portal\gateway**
1225 8. Edit the **sessionIdCookie.setDomain** parameter in the `index.jsp` file to specify the cookie
1226 domain of your PingFederate server (Note: valid cookie domains must contain a minimum of
1227 two “dots.” For example “.company.com.”)

```

        response.addHeader("sessionId", request.getParameter("sessionId"));
        Cookie sessionIdCookie = new Cookie("sessionId", request.getParameter("sessionId"));
        sessionIdCookie.setSecure(true);
        sessionIdCookie.setPath("/");
        sessionIdCookie.setHttpOnly(true);
        sessionIdCookie.setDomain(".abac.test");
        response.addCookie(sessionIdCookie);

        List<Cookie> cookies = Arrays.asList(request.getCookies());
        String resumePath = new String();

        for(Cookie cookie : cookies){
            if (cookie.getName().equalsIgnoreCase("ResumePath")) {
                resumePath = cookie.getValue();
            }
        }
    }
}

```

1228 }

1229 9. Start or restart the PingFederate server.

1230 2.12.2 Install Situational Session Validator

- 1231 1. On the same PingFederate-IdP server, unpack the contents of the
1232 Situational_SessionValidator.zip file found in the Context Connector integration kit zip file
1233 (Situational_Context_Connector_v21.zip).
- 1234 2. Navigate to the folder where you unpacked the Situational Session Validator and locate the
1235 redirector.properties file.
- 1236 3. Edit the values in the redirector.properties file according to your environment.

```

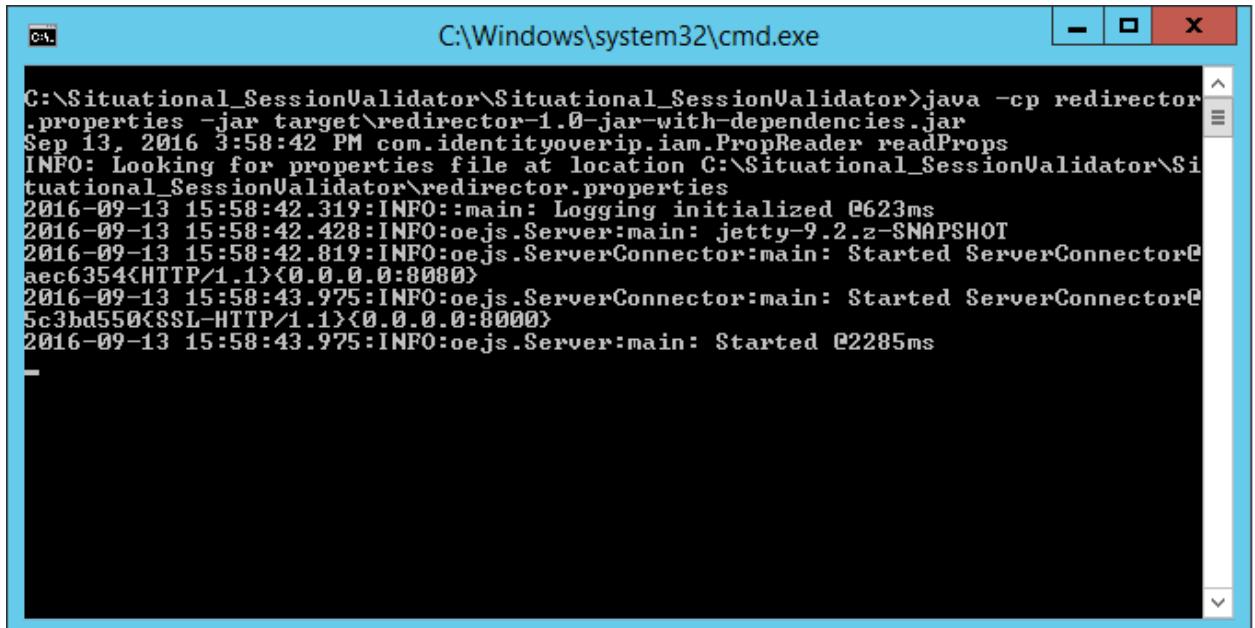
redirectorHTTPPort=8080
#redirectorSSLPot Number matches the Port configured in Cisco
ISE Guest Portal
redirectorSSLPort=8000
#redirectorDomain is the doamin for the PingFederate Server
redirectorDomain=abac.test
#pingFederateAddress is the resolvable URL for PingFederate
pingFederateAddress=https://10.33.7.4
#pingFederatePort is the port for the PingFederate Server
pingFederatePort=9031|

```

1237

1238 **Note:** As shown above, the **redirectorSSLPort** should be the same port number that you chose
1239 for the Guest Access Portal settings during the ISE configuration. For this build it is set to **8000**.

- 1240 4. Start the session validator by running the runme script, **runme.bat**. Afterward, you
1241 will see a Command Prompt window pop up running the script.



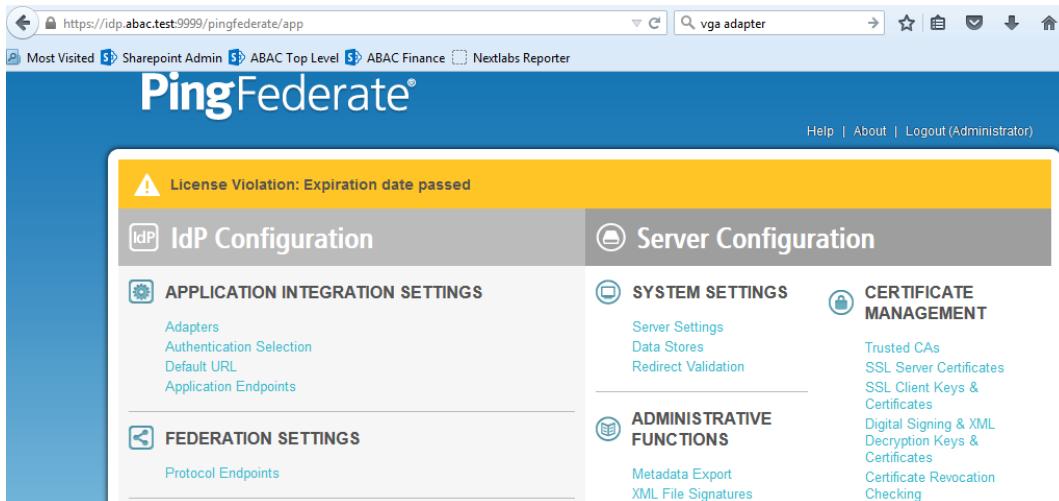
```
C:\Windows\system32\cmd.exe
C:\Situational_SessionValidator\Situational_SessionValidator>java -cp redirector.properties -jar target\redirector-1.0-jar-with-dependencies.jar
Sep 13, 2016 3:58:42 PM com.identityoverip.iam.PropReader readProps
INFO: Looking for properties file at location C:\Situational_SessionValidator\Situational_SessionValidator\redirector.properties
2016-09-13 15:58:42.319:INFO::main: Logging initialized @623ms
2016-09-13 15:58:42.428:INFO:oejs.Server:main: jetty-9.2.z-SNAPSHOT
2016-09-13 15:58:42.819:INFO:oejs.ServerConnector:main: Started ServerConnector@aec6354<HTTP/1.1>{0.0.0.0:8080}
2016-09-13 15:58:43.975:INFO:oejs.ServerConnector:main: Started ServerConnector@5c3bd550<SSL-HTTP/1.1>{0.0.0.0:8000}
2016-09-13 15:58:43.975:INFO:oejs.Server:main: Started @2285ms
```

1242

2.13 Configure PingFederate-IdP

Follow the instructions in the subsections below to configure PingFederate as the Federation Server for the IdP.

1. Launch your browser and go to https://<DNS_NAME>:9999/pingfederate/app.
2. Replace **DNS_NAME** with the fully qualified name of the IdP's PingFederate server (e.g., <https://idp.abac.test:9999/pingfederate/app>).
3. Log on to the PingFederate app using the credentials you configured during installation.

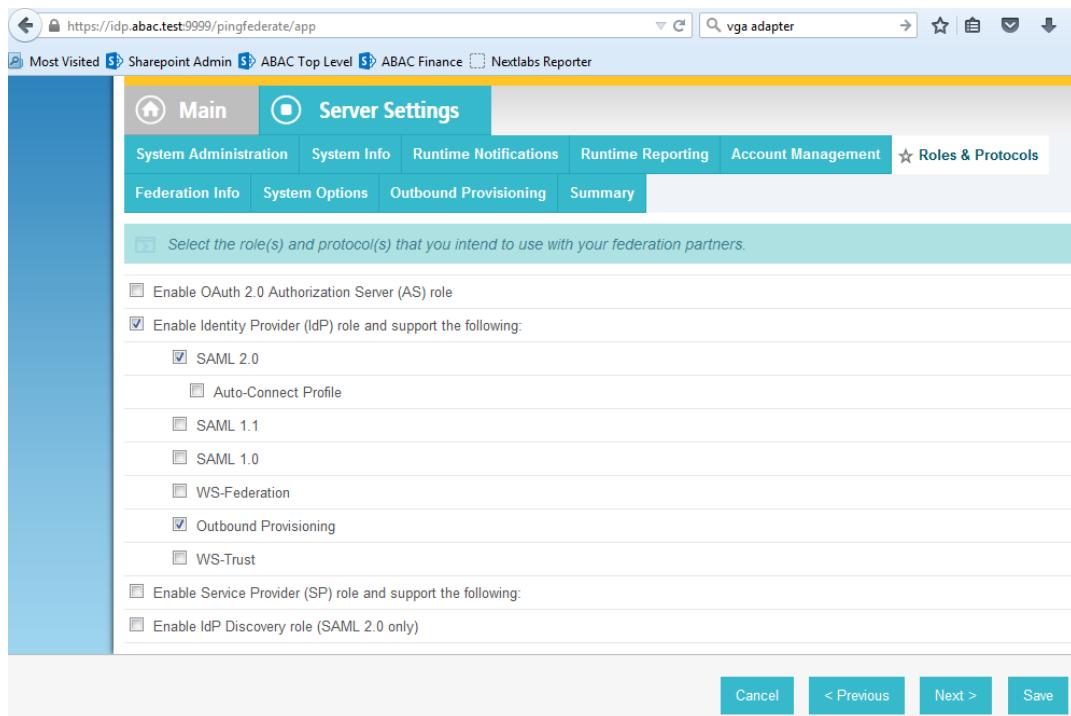


The screenshot shows the PingFederate web interface. At the top, there is a navigation bar with links for 'Sharepoint Admin', 'ABAC Top Level', 'ABAC Finance', and 'Nextlabs Reporter'. The main header says 'PingFederate' with a 'Logout (Administrator)' link. A yellow banner at the top left says 'License Violation: Expiration date passed'. The main content area has two main sections: 'IdP Configuration' on the left and 'Server Configuration' on the right. Under 'IdP Configuration', there are sections for 'APPLICATION INTEGRATION SETTINGS' (Adapters, Authentication Selection, Default URL, Application Endpoints) and 'FEDERATION SETTINGS' (Protocol Endpoints). Under 'Server Configuration', there are sections for 'SYSTEM SETTINGS' (Server Settings, Data Stores, Redirect Validation), 'ADMINISTRATIVE FUNCTIONS' (Metadata Export, XML File Signatures), and 'CERTIFICATE MANAGEMENT' (Trusted CAs, SSL Server Certificates, SSL Client Keys & Certificates, Digital Signing & XML Decryption Keys & Certificates, Certificate Revocation Checking).

1250

1251 **2.13.1 Configure SAML Protocol**

- 1252 1. On the Main Menu under System Settings, click **Server Settings**.
- 1253 2. Click the **Roles and Protocols** tab. Select **Enable Identity Provider (IdP) role and support the following**.
- 1254
- 1255 3. Select **SAML 2.0**.



1256

- 1257 4. Click **Save**.

1258 **2.13.2 Create Data Store for Microsoft AD**

- 1259 1. On the Main Menu under System Settings, click **Data Stores**.

The screenshot shows the PingFederate interface with the title "PingFederate®" at the top. A yellow banner at the top indicates a "License Violation: Expiration date passed". The main navigation bar includes "Main", "Manage Data Stores" (which is selected), and "Data Store". Below the navigation is a section titled "Manage data store definitions for use with attribute lookups." A table lists three data stores:

DESCRIPTION	SYSTEM ID	USER	TYPE	LDAP	ACTION
jdbc:sqlserver://10.33.7.12:1433;databaseName=RSA_CORE_AA	JDBC-B342DF1B15A101BDFAA22FB2A690588A4792B4B0	ping	Database		Delete (Check Usage)
jbchssqldb:\${boss.server.data.dir}\${/hypersonic\${/ProvisionerDefaultDB}	ProvisionerDS	sa	Database		Delete (Check Usage)
activedirectory.abac.test	LDAP-DFBE08A690B5467A07741DF51D756CB0737960	LDAP User	LDAP	Active	Delete (Check Usage)

At the bottom left is a button "Add New Data Store...". At the bottom right are "Cancel" and "Save" buttons.

1260

1261

2. Select **LDAP**.

The screenshot shows the "Data Store" configuration page. The title "PingFederate®" is at the top, followed by a yellow banner with a license violation message. The navigation bar includes "Main", "Manage Data Stores", and "Data Store" (selected). Below the navigation is a section titled "Please select a type of data store." with three radio buttons:

- Database
- LDAP
- Custom

At the bottom right are "Cancel" and "Next >" buttons.

1262

1263

3. Click **Next**.

1264

4. Enter the Hostname where the Microsoft AD is hosted (e.g., **activedirectory.abac.test**).

1265

5. For the **LDAP Type**, select **Active Directory**.

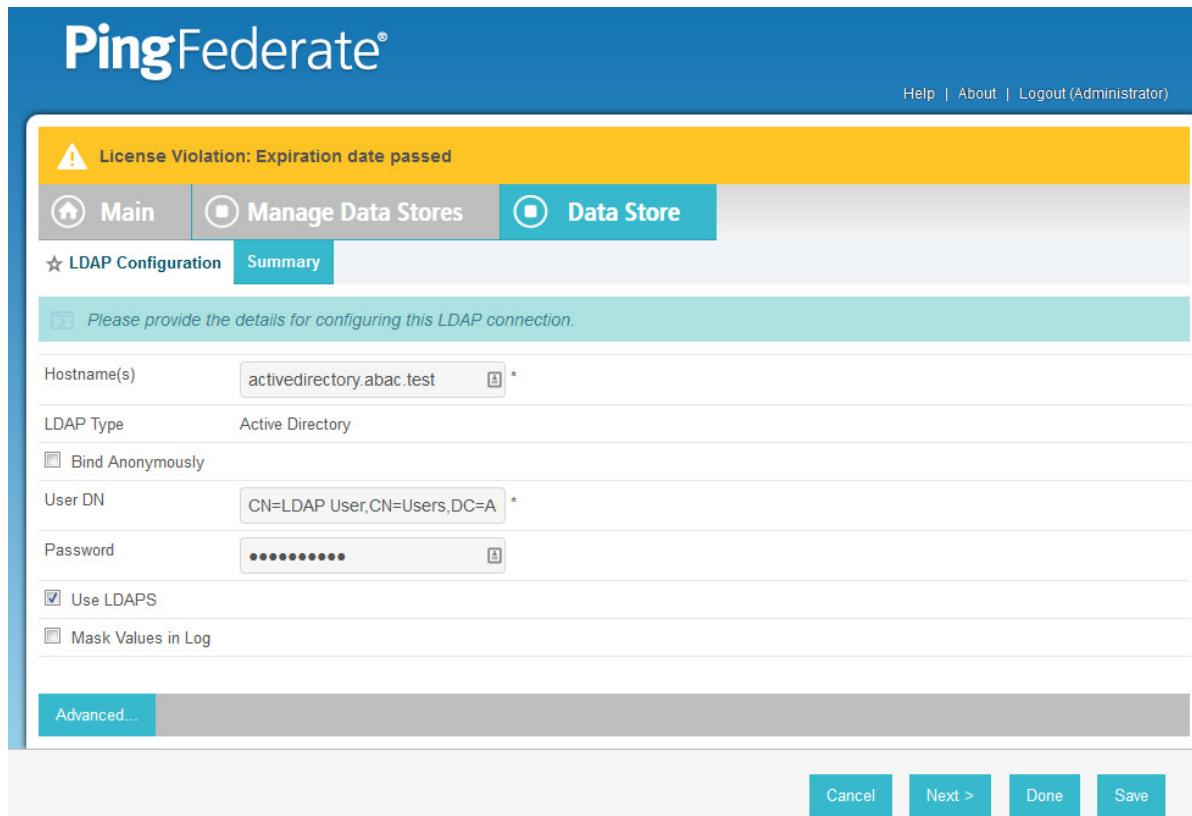
1266

6. Enter the **User DN** created in the earlier section named **Create the LDAP User for Federated Authentication** (e.g., **CN=LDAP User, CN=Users,DC=ABAC,DC=Test**).

1268

7. Enter the password associated with the **LDAP User DN**. Select the option to use **LDAPS**.

- 1269 8. Click **Next**. Then, click **Save** on the Summary screen.

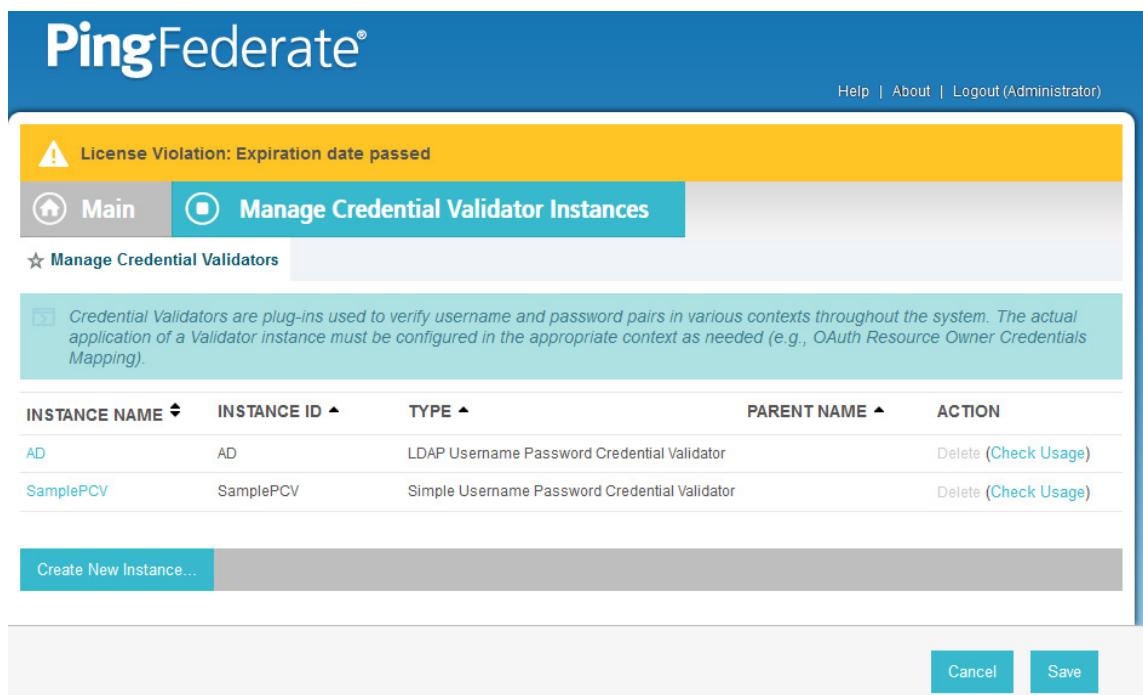


The screenshot shows the PingFederate web interface for configuring an LDAP connection. The title bar says "PingFederate". A yellow banner at the top left indicates a "License Violation: Expiration date passed". The main menu has tabs: Main (selected), Manage Data Stores, and Data Store. Below the tabs, there are two sub-tabs: LDAP Configuration (selected) and Summary. A message box says "Please provide the details for configuring this LDAP connection." The configuration form includes fields for Hostname(s) (active directory.abac.test), LDAP Type (Active Directory), Bind Anonymously (unchecked), User DN (CN=LDAP User,CN=Users,DC=A), Password (redacted), Use LDAPS (checked), and Mask Values in Log (unchecked). There is also an "Advanced..." button. At the bottom right are buttons for Cancel, Next >, Done, and Save.

1270

2.13.3 Create Credential Validator for Microsoft AD

- 1271 1. On the Main Menu under Authentication, click **Password Credential Validators**.



The screenshot shows the PingFederate web interface for managing credential validators. The title bar says "PingFederate". A yellow banner at the top left indicates a "License Violation: Expiration date passed". The main menu has tabs: Main (selected), Manage Credential Validator Instances (selected), and Manage Credential Validators. Below the tabs, there is a message box: "Credential Validators are plug-ins used to verify username and password pairs in various contexts throughout the system. The actual application of a Validator instance must be configured in the appropriate context as needed (e.g., OAuth Resource Owner Credentials Mapping)". A table lists existing credential validators:

INSTANCE NAME	INSTANCE ID	TYPE	PARENT NAME	ACTION
AD	AD	LDAP Username Password Credential Validator		Delete (Check Usage)
SamplePCV	SamplePCV	Simple Username Password Credential Validator		Delete (Check Usage)

At the bottom left is a "Create New Instance..." button. At the bottom right are buttons for Cancel and Save.

1273

- 1274 2. Click **Create New Instance**.
- 1275 3. Enter a unique **Instance Name** you would like to use to refer to this configuration (e.g., **AD**
1276 **username password**).
- 1277 4. Enter a unique **Instance Id** (typically the same as the Instance Name) without any spaces.
- 1278 5. For **Type**, select **LDAP Username Password Credential Validator**.

PingFederate®

Help | About | Logout (Administrator)

License Violation: Expiration date passed

Main Manage Credential Validator Instances Create Credential Validator Instance

Type Instance Configuration Extended Contract Summary

Identify this Credential Validator Instance. The Validator types available are limited to the plug-in implementations currently installed on your server.

Instance Name	AD username password *
Instance Id	ADusernamepassword *
Type	LDAP Username Password Credential Validator * Visit PingIdentity.com for additional types
Parent Instance	None

Cancel Next >

- 1279
- 1280 6. Click **Next**.
- 1281 7. For the **LDAP DATASTORE**, select the Active Directory data store you created earlier (e.g.,
1282 **activedirectory.abac.test**).
- 1283 8. Enter the **SEARCH BASE** (location in the directory where the LDAP search begins) for your
1284 Microsoft AD LDAP directory (e.g., **DC=ABAC,DC=TEST**).
- 1285 9. Enter the **SEARCH FILTER** (e.g., **sAMAccountName=\${username}**). The SEARCH FILTER allows Ping
1286 to search the LDAP directory, looking for a match where the attribute named sAMAccountName
1287 matches the username value passed from the PingIdentity server.

SECOND DRAFT

The screenshot shows a web-based configuration interface for a 'Credential Validator Instance'. The top navigation bar includes 'Main', 'Manage Credential Validator Instances', and 'Create Credential Validator Instance'. Below this, a sub-navigation bar shows 'Type' (selected), 'Instance Configuration', 'Extended Contract', and 'Summary'. A note at the top states: 'Complete the configuration necessary for this Password Credential Validator to check username/password pairs. This configuration was designed into, and is specific to, the selected Credential Validator plug-in.' The main content area describes a password credential validator that verifies credentials stored in a directory server via the LDAP protocol. It includes sections for 'AUTHENTICATION ERROR OVERRIDES' (a table of LDAP authentication error codes and customized matching expressions) and 'MATCH EXPRESSION' (the expression matched against the LDAP error message returned by the server). The configuration table includes fields for 'FIELD NAME', 'FIELD VALUE', and 'DESCRIPTION'. Key entries include:

FIELD NAME	FIELD VALUE	DESCRIPTION
LDAP DATASTORE	activedirectory.abac.test	Select the LDAP Datastore.
SEARCH BASE	DC=ABAC,DC=TEST	* The location in the directory from which the LDAP search begins.
SEARCH FILTER	sAMAccountName=\${username}	* You may use \${username} as part of the query. Example (for Active Directory): sAMAccountName=\${username}
SCOPE OF SEARCH	<input type="radio"/> One Level <input checked="" type="radio"/> Subtree	

At the bottom left is a button labeled 'Manage Data Stores...'. The right side of the interface includes columns for 'ERROR' and 'Action'.

1288

10. Click **Next**.

1289

You should see two attributes listed under **CORE CONTRACT**, **DN**, and **username**.

The screenshot shows the PingFederate interface. At the top, there's a yellow banner with a warning icon and the text "License Violation: Expiration date passed". Below this, the main navigation bar has tabs for "Main", "Manage Credential Validator Instances", and "Create Credential Validator Instance". The "Create Credential Validator Instance" tab is selected. A sub-navigation bar below it includes "Type", "Instance Configuration", "Extended Contract" (which is highlighted with a star icon), and "Summary". A message in a teal box says, "You can extend the attribute contract of this Password Credential Validator instance." The main content area is titled "CORE CONTRACT" and contains fields for "DN" and "username". Below this, there's a section titled "EXTEND THE CONTRACT" with an "ACTION" button and an "Add" button. At the bottom right are buttons for "Cancel", "< Previous", and "Next >".

1291

1292

11. Click **Next**.

1293

You should see a summary page.

The screenshot shows the "Create Credential Validator Instance" summary page. The top navigation bar has tabs for "Type", "Instance Configuration", "Extended Contract", and "Summary", with "Summary" being the active tab. A message in a teal box says, "Password Credential Validator configuration summary." The main content area is titled "Create Credential Validator Instance" and is divided into sections: "TYPE", "INSTANCE CONFIGURATION", and "EXTENDED CONTRACT". Under "TYPE", the configuration includes "Instance Name: AD username password", "Instance Id: ADusernamepassword", "Type: LDAP Username Password Credential Validator", "Class Name: org.sourceforge.saml20.domain.LDAPUsernamePasswordCredentialValidator", and "Parent Instance Name: None". Under "INSTANCE CONFIGURATION", the configuration includes "LDAP Datastore: activedirectory.abac.test", "Search Base: DC=ABAC,DC=TEST", "Search Filter: sAMAccountName=\${username}", and "Scope of Search: Subtree". Under "EXTENDED CONTRACT", the configuration includes "Attribute: DN" and "Attribute: username". At the bottom right are buttons for "Cancel", "< Previous", and "Done".

1294

- 1295 12. Click **Done**.
- 1296 You should see a list of the credential validator instances, including the newly added validator
1297 (e.g., **AD username password**).

INSTANCE NAME	INSTANCE ID	TYPE	PARENT NAME	ACTION
AD	AD	LDAP Username Password Credential Validator		Delete (Check Usage)
AD username password	ADusernamepassword	LDAP Username Password Credential Validator		Delete
SamplePCV	SamplePCV	Simple Username Password Credential Validator		Delete (Check Usage)

Create New Instance...

Cancel **Save**

- 1298
- 1299 13. Click **Save** to complete configuration of the credential validator.
- 1300 **2.13.4 Create IdP Adapter for Authentication with Microsoft AD via Web Browser Form**
- 1301 The IdP Adapter created in this section is the logical component PingFederate uses to authenticate a user with Microsoft AD via a web browser login page.
- 1304 1. On the Main Menu under Application Integration Settings, click **Adapters**.

INSTANCE NAME	INSTANCE ID	TYPE	PARENT NAME	ACTION
AdaptiveAuthentication	AdaptiveAuthentication	RSA Adaptive Authentication Adapter 2.0.0.0		Delete (Check Usage)
HTMLForms	HTMLForms	HTML Form IdP Adapter		Delete (Check Usage)
IdP Adapter	idpadapter	ReferenceID Adapter 1.0		Delete (Check Usage)
MultiFactorAuthentication	MultiFactorAuthentication	Composite Adapter		Delete (Check Usage)

1305

- 1306 2. Click **Create New Instance**.
- 1307 3. In **Instance Name**, enter a unique name for the instance. The name will be used to refer to this
1308 configuration (e.g., **AD HTML forms**).
- 1309 4. Enter a unique **Instance Id** (typically the same as the instance name) without any spaces. For
1310 **Type**, select **HTML Form IdP Adapter**.

1311

SECOND DRAFT

- 1312 5. Click **Next**.
- 1313 6. Under **PASSWORD CREDENTIAL VALIDATOR INSTANCE**, click on the **Add a new row to Credential Validator's** hyperlink. This will add a new selection box under the **PASSWORD CREDENTIAL VALIDATOR INSTANCE** with the value of “—Select One—” in it. In that new box, select the credential validator for Microsoft AD that was created in an earlier section (e.g., **AD username password**).

The screenshot shows the 'PASSWORD CREDENTIAL VALIDATOR INSTANCE' configuration page for an 'IdP Adapter'. The top navigation bar includes tabs for Type (selected), IdP Adapter, Extended Contract, Adapter Attributes, and Summary. A note at the top says: 'Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.' Below this is a table with columns for FIELD NAME, FIELD VALUE, and DESCRIPTION.

FIELD NAME	FIELD VALUE	DESCRIPTION
CHALLENGE RETRIES	3	* Max value of User Challenge Retries.
SESSION STATE	<input checked="" type="radio"/> Globally <input type="radio"/> Per Adapter <input type="radio"/> None	Determines how state is maintained within one adapter or between different adapter instances.
SESSION TIMEOUT	60	Session Idle Timeout (in minutes). If left blank the timeout will be the Session Max Timeout. Ignored if 'None' is selected for Session State.
SESSION MAX TIMEOUT	480	Session Max Timeout (in minutes). Leave blank for indefinite sessions. Ignored if 'None' is selected for Session State.
LOGIN TEMPLATE	html.form.login.template.html	* HTML template (in <pf_home>/server/default/conf/template) to render for login. The default value is html.form.login.template.html.
LOGOUT PATH		Path on the PingFederate server to end a user's IdP session. Must include the initial slash (example: /mylogoutpath). (Resulting URL will be http[s]://<pf_host>:<port>/ext<Logout Path>). If specified, the path should be unique across HTML Form IdP Adapter instances, including child instances.

At the bottom of the page, there is a note: 'A fully qualified IDI URL of the ID to which a user will be redirected after logout.'

- 1318
- 1319 7. Under **PASSWORD CREDENTIAL VALIDATOR INSTANCE**, click the **Update** hyperlink on the right side of the page. This will cause the selection box to turn grey.
- 1320

SECOND DRAFT

Main **Manage IdP Adapter Instances** **Create Adapter Instance**

Type **IdP Adapter** Extended Contract Adapter Attributes Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

CREDENTIAL VALIDATORS (A list of Password Credential Validators to be used for authentication.)

PASSWORD CREDENTIAL VALIDATOR INSTANCE		Action
AD username password	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Add a new row to 'Credential Validators'		

FIELD NAME	FIELD VALUE	DESCRIPTION
CHALLENGE RETRIES	3	* Max value of User Challenge Retries.
SESSION STATE	<input checked="" type="radio"/> Globally <input type="radio"/> Per Adapter <input type="radio"/> None	Determines how state is maintained within one adapter or between different adapter instances.
SESSION TIMEOUT	60	Session Idle Timeout (in minutes). If left blank the timeout will be the Session Max Timeout. Ignored if 'None' is selected for Session State.
SESSION MAX TIMEOUT	480	Session Max Timeout (in minutes). Leave blank for indefinite sessions. Ignored if 'None' is selected for Session State.
LOGIN TEMPLATE	html.form.login.template.html	* HTML template (in <pf_home>/server/default/conf/template) to render for login. The default value is html.form.login.template.html.
LOGOUT PATH		Path on the PingFederate server to end a user's IdP session. Must include the initial slash (example: /mylogoutpath). (Resulting URL will be https://<pf_host>:<port>/ext<Logout Path>). If specified, the path should be unique across HTML Form IdP Adapter instances, including child instances.

1321

1322 8. Click **Next**. Then, click **Next** again to bypass the Extended Contract screen.

1323 9. On the Adapter Attributes screen, select the **PSEUDONYM** check box in the **username** row.

Main **Manage IdP Adapter Instances** **Create Adapter Instance**

Type **IdP Adapter** **Extended Contract** **Adapter Attributes** Summary

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

ATTRIBUTE	PSEUDONYM	MASK LOG VALUES
username	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Mask all OGNL-expression generated log values		

Cancel **< Previous** **Next >**

1324

1325 10. Click **Next**. On the Summary screen, click **Done**.

INSTANCE NAME	INSTANCE ID	TYPE	PARENT NAME	ACTION
AD HTML forms	ADHTMLforms	HTML Form IdP Adapter		Delete
AdaptiveAuthentication	AdaptiveAuthentication	RSA Adaptive Authentication Adapter 2.0.0.0		Delete (Check Usage)
HTMLForms	HTMLForms	HTML Form IdP Adapter		Delete (Check Usage)
IdP Adapter	idpadapter	ReferenceID Adapter 1.0		Delete (Check Usage)
MultiFactorAuthentication	MultiFactorAuthentication	Composite Adapter		Delete (Check Usage)

1326

1327 11. Click **Save** to complete configuration of the new adapter.

2.13.5 Create IdP Adapter for Two-Factor Authentication with RSA AA

1329 The IdP Adapter created in this section is the logical component PingFederate uses to authenticate a
1330 user with RSA AA using a second factor.

1331 1. On the Main Menu under Application Integration Settings, click **Adapters**.

1332 2. On the Manage IdP Adapters screen, click **Create New Instance**.

1333 3. On the Type screen, enter an Instance Name and Instance ID.

1334 4. Set the following settings on the Adapter Type page before clicking **Next**:

1335 a. **Instance Name:** (Instance Name)

1336 b. **Instance ID:** (Instance ID)

1337 c. **Type:** RSA Adaptive Authentication Adapter 2.0

1338 d. **Class Name:**

1339 `com.thescegroup.adapters.aa.pingfederate.AdaptiveAuthenticationAdapter`

1340 e. **Parent Instance:** None

Instance Name: AdaptiveAuthentication
 Instance Id: AdaptiveAuthentication
 Type: RSA Adaptive Authentication Adapter 2.0.0.0
 Class Name: com thesecgroup adapters.aa.pingfederate.AdaptiveAuthenticationAdapter
 Parent Instance: None

Cancel Next > Done

© 2003-2015 Ping Identity Corporation All Rights Reserved
 Version 7.3.0.5

Activate Windows Go to System in Control Panel > Activate

1341

- 1342 5. On the IdP Adapter configuration page, click **Show Advanced Fields** and input the following
 1343 parameters while leaving the rest as default, before clicking **Next**:
- 1344 a. AA Web Service URL: *http://<RSA Server*
 1345 *DNS>:8080/AdaptiveAuthentication/services/AdaptiveAuthentication*
- 1346 b. AA Web Service Username: [username] (Credentials must match on RSA server.)
- 1347 c. AA Web Service Password: [password]

FIELD NAME	FIELD VALUE	DESCRIPTION
AA WEB SERVICE URL	http://10.53.7.12:8080/AdaptiveAuthentication/services/AdaptiveAuthentication	The Web Service URL of the Adaptive Authentication server.
AA WEB SERVICE USERNAME	demo	Adaptive Authentication Caller ID used to identify the service invoker.
AA WEB SERVICE PASSWORD	*****	Adaptive Authentication Caller ID password.
AA ORGANIZATION NAME		Adaptive Authentication Organization Name.
NUMBER OF QUESTIONS TO COLLECT	3	During enrollment, how many security questions should we collect from users? Set to 0 to disable security question collection.
NUMBER OF QUESTIONS TO ASK	1	During identity verification, how many security questions should we ask users to answer? This value must be less than the number of questions you collected.
NUMBER OF PHONE NUMBERS TO COLLECT	1	During enrollment, how many phone numbers should we collect from users? Set to 0 to disable out-of-band phone data collection.
NUMBER OF SMS-CAPABLE PHONE NUMBERS TO COLLECT	1	During enrollment, what is a minimum number of SMS-capable phone numbers should we collect from users? Set to 0 to disable out-of-band SMS data collection. This value cannot be greater than number of phone numbers you collected.
OUT-OF-BAND PHONE PROVIDER	<input checked="" type="radio"/> Authority <input type="radio"/> TeleSign	Selected which Out-of-Band Phone provider authentication you plan to use.
OUT-OF-BAND SMS PROVIDER	<input checked="" type="radio"/> Authority <input type="radio"/> TeleSign	Selected which Out-of-Band SMS provider authentication you plan to use.
NUMBER OF EMAIL ADDRESSES TO COLLECT	1	During enrollment, how many email addresses should we collect from users? Set to 0 to disable out-of-band email data collection.
DISPLAY DEVICE BINDING	<input checked="" type="checkbox"/>	During enrollment or identity verification, should we display device binding options to users?
DEFAULT DEVICE BINDING OPTION	No	If "Display Device Binding" is true, which option should we use as a default selection? If "Display Device Binding" is false, the setting is ignored.

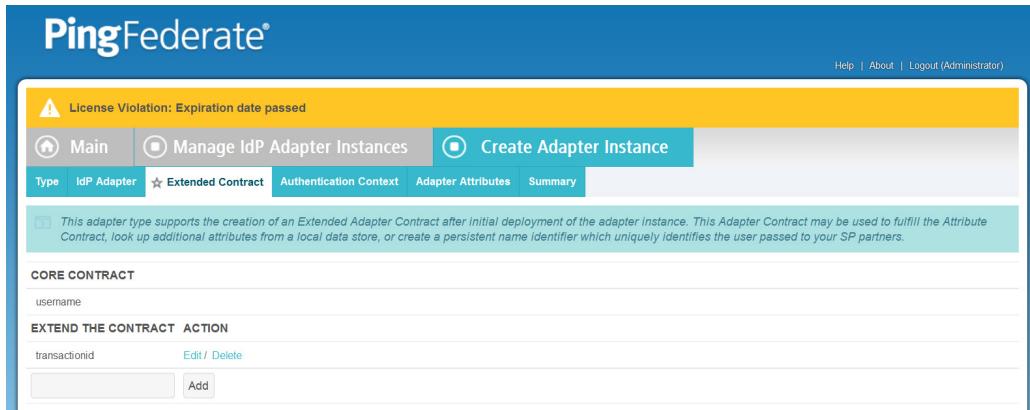
Show Advanced Fields

Cancel < Previous Next > Done

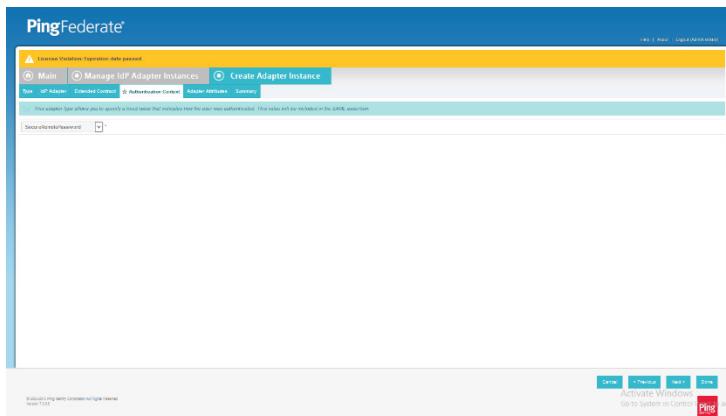
Activate Windows Go to System in Control Panel > Activate

1348

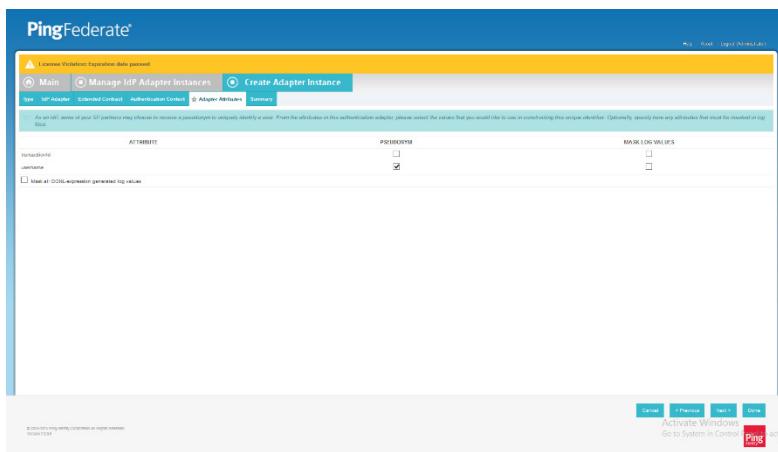
- 1349 6. On the Extended Contract screen, type **transactionid** (all lowercase). Then, click **Add**. By default,
 1350 username should already be listed under **Core Contract**.



1351

1352 7. Click **Next**.1353 8. On the **Authentication Context** screen, select *SecureRemotePassword* as the fixed value for authentication. This value will be included in the SAML assertion. Click **Next**.
1354

1355

1356 9. On the **Adapter Attributes** screen, select *username* as the **Pseudonym**. Click **Next**.

1357

1358 10. On the **Summary** screen, verify that the information is correct and click **Done**.1359 11. On the **Manager IdP Adapter Instances** screen, click **Save** to complete the Adapter configuration.
1360

2.13.6 Create Composite IdP Adapter Integrating Microsoft AD and RSA AA

The IdP Adapter created in this section is a composite adapter that integrates the two previously created adapters for Microsoft AD and RSA AA. When a user is directed to the PingFederate IdP server, the user will see a web form where they can enter their Microsoft AD credentials. Following authentication with Microsoft AD, PingFederate will initiate the second factor authentication with an SCE Plug-in. The SCE Plug-in will then present the user with a request for the second factor.

1. On the **Main** menu under **Application Integration Settings**, click **Adapters**.
2. On the Manage IdP Adapters screen, click **Create New Instance**.
3. Enter a unique **Instance Name** you would like to use to refer to this configuration (e.g., **RSA Multifactor**).
4. Enter a unique **Instance Id** (typically the same as the **Instance Name**) without any spaces.
5. For **Type**, select **Composite Adapter**.

Instance Name: RSA Multifactor *

Instance Id: RSAMultifactor *

Type: Composite Adapter * Visit [PingIdentity.com](#) for additional types

Parent Instance: None

Note: Enter an Adapter Instance Name and Id, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.

Cancel Next >

6. Click **Next**.
7. On the IdP Adapter screen, under **ADAPTER INSTANCE**, click on the **Add a new row to 'Adapters'**'s hyperlink. This will add a new selection box under the **ADAPTER INSTANCE** with the value of “—Select One—” into the box. In that new box, select the adapter instance for HTML forms with Microsoft AD that was created in an earlier section (e.g., **AD HTML forms**).
8. Under **ADAPTER INSTANCE**, click the **Update** hyperlink on the right side of the page. This will cause the selection box to turn grey.

SECOND DRAFT

Main **Manage IdP Adapter Instances** **Create Adapter Instance**

Type **IdP Adapter** Extended Contract Adapter Attributes Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

A Composite Adapter allows existing adapter instances to be chained together to execute in sequence. Each configured instance of a Composite Adapter is treated as a single logical adapter instance.

ADAPTERS (Chained adapters)

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
AD HTML forms	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	3		Edit Delete

Add a new row to 'Adapters'

INPUT USER ID MAPPING (Create mappings)

TARGET ADAPTER	USER ID SELECTION	Action
----------------	-------------------	--------

Add a new row to 'Input User Id Mapping'

1381

- 1382 9. Repeat the previous steps to add another row to **Adapters** using the hyperlink on the right side
 1383 of the page. This time, select the **AdaptiveAuthentication** adapter in the selection box. When
 1384 complete, the IdP Adapter screen will look similar to the screenshot below, with two adapters
 1385 configured under **ADAPTER INSTANCE**.

Main **Manage IdP Adapter Instances** **Create Adapter Instance**

Type **IdP Adapter** Extended Contract Adapter Attributes Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

A Composite Adapter allows existing adapter instances to be chained together to execute in sequence. Each configured instance of a Composite Adapter is treated as a single logical adapter instance.

ADAPTERS (Chained adapters)

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
AD HTML forms	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	3		Move down Edit Delete
AdaptiveAuthentication	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	3		Move up Edit Delete

Add a new row to 'Adapters'

1386

- 1387 10. Under **TARGET ADAPTER**, click on the **Add a new row to 'Input User Id Mapping'** hyperlink. This
 1388 will add a new selection box under the **TARGET ADAPTER** with the value of “—Select One—” in
 1389 the box.
 1390 11. In that new box, select the adapter instance for the RSA authentication that was created in an
 1391 earlier section (e.g., **AdaptiveAuthentication**).

SECOND DRAFT

- 1392 12. In the new **USER ID SELECTION** box, select **username**.
- 1393 13. Under **TARGET ADAPTER**, click the **Update** hyperlink on the right side of the page. This will
1394 cause the selection box to turn grey.

The screenshot shows the 'Manage IdP Adapter Instances' interface. At the top, there are tabs: Main, Manage IdP Adapter Instances (selected), and Create Adapter Instance. Below the tabs, a sub-tab bar includes Type, IdP Adapter (selected), Extended Contract, Adapter Attributes, and Summary. A note at the top says: 'Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.' The main content area is titled 'ADAPTERS (Chained adapters)'. It contains a table with columns: ADAPTER INSTANCE, POLICY, AUTHN CONTEXT WEIGHT, AUTHN CONTEXT OVERRIDE, and Action. Two rows are listed:

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
AD HTML forms	(radio) Required Sufficient *	3		Move down Edit Delete
AdaptiveAuthentication	(radio) Required Sufficient *	3		Move up Edit Delete

Below the table is a link: 'Add a new row to 'Adapters''.

Underneath is another section titled 'INPUT USER ID MAPPING (Create mappings)'. It has two columns: TARGET ADAPTER and USER ID SELECTION. A note above it says: 'This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. This Adapter Contract may be used to fulfill the Attribute Contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.' The 'TARGET ADAPTER' dropdown is set to 'AdaptiveAuthentication'. The 'USER ID SELECTION' dropdown is set to 'username'. Action buttons 'Edit' and 'Delete' are available.

Add a new row to 'Input User Id Mapping'

- 1395
- 1396 14. Click **Next**.
- 1397 15. On the Extended Contract screen, enter the value **username** in the **EXTEND THE CONTRACT** field.
1398

The screenshot shows the 'Manage IdP Adapter Instances' interface with the 'Extended Contract' tab selected. At the top, there are tabs: Main, Manage IdP Adapter Instances (selected), and Create Adapter Instance. Below the tabs, a sub-tab bar includes Type, IdP Adapter, Extended Contract (selected), Adapter Attributes, and Summary. A note at the top says: 'License Violation: Expiration date passed'. The main content area is titled 'EXTEND THE CONTRACT'. It contains a table with columns: EXTEND THE CONTRACT and ACTION. A note above it says: 'This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. This Adapter Contract may be used to fulfill the Attribute Contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.' The 'EXTEND THE CONTRACT' dropdown is set to 'username'. An 'Add' button is available. At the bottom right are buttons: Cancel, < Previous, and Next >.

- 1399
- 1400 16. Click **Add**. Enter the value **transactionid** (all lowercase) in the **EXTEND THE CONTRACT** field.

This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. This Adapter Contract may be used to fulfill the Attribute Contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.

EXTEND THE CONTRACT	ACTION
username	Edit / Delete
transactionId	Add

1401

- 1402 17. Click **Add**. Then, click **Next**.
- 1403 18. On the **Adapter Attributes** screen, in the **username** row, select the **PSEUDONYM** column.

ATTRIBUTE	PSEUDONYM	MASK LOG VALUES
transactionId	<input type="checkbox"/>	<input type="checkbox"/>
username	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Mask all OGNL-expression generated log values		

1404

- 1405 19. Click **Next**. On the **Summary** screen, click **Done**.
- 1406 20. Click **Save** to complete configuration of the new composite adapter.

2.13.7 Create IdP Adapter for the Situational Context Connector and ISE Authentication

The IdP Adapter created in this section is the logical component PingFederate uses to obtain connection (device and network) information obtained from ISE Authentication via the Situational Context Connector. These device and network attributes serve as environmental attributes in this build.

1. On the **Main** menu under **Application Integration Settings**, click **Adapters**.
2. On the **Manage IdP Adapters** screen, click **Create New Instance**.

- 1414 3. On the **Type** screen, enter an **Instance Name** and **Instance ID**.
- 1415 4. For Type, select **Context Connector v2.0**, and click **Next**.

Main Manage IdP Adapter Instances

Create Adapter Instance

Type IdP Adapter Extended Contract Adapter Attributes Summary

Enter an Adapter Instance Name and Id, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.

Instance Name	CiscoISE *
Instance Id	CiscoISE *
Type	Context Connector v2.0 * Visit PingIdentity.com for additional types
Parent Instance	None

Cancel Next >

- 1416
- 1417 5. Enter configuration information and click **Next**.

SECOND DRAFT

Type ★ **IdP Adapter** Extended Contract Adapter Attributes Summary

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

Set the details of the adapter

FIELD NAME	FIELD VALUE	DESCRIPTION
NETWORK BASE ADDRESS	10.33.7.0	Enter the base IPv4 address to identify the authenticated subnet
SUBNET MASK	255.255.255.0	Enter the IPv4 subnet mask to identify the authenticated subnet
ISE BASE URL	https://abac-ciscoise.abac.test	Enter the base URL for the ISE instance
ISE FAILOVER URL		Enter the failover URL for the ISE instance
ISE COMMAND	/admin/API/mnt/Session/EndPointIPAd	Enter the command to issue to the ISE instance
ISE USER NAME	admin	Enter the user name for the ISE instance
ISE PASSWORD	Enter the password for the ISE instance
NAD TRIGGER URL	http://10.33.7.6	Enter the URL used trigger the NAD to insert the sessionID as a parameter
RESUME PATH DOMAIN	abac.test	Enter the Domain to be used when passing along the session

Cancel **< Previous** **Next >**

1418

- 1419 6. On the **Extended Contract** screen, you can configure additional attributes for the adapter. We
 1420 retained the defaults and clicked **Next**.

Type **IdP Adapter** **Extended Contract** **Adapter Attributes** **Summary**

This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. This Adapter Contract may be used to fulfill the Attribute Contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.

CORE CONTRACT

- ip_address
- ise_audit_session
- ise_auth_acs_timestamp
- ise_auth_id
- ise_calling_station_id
- ise_identity_group
- ise_identity_store
- ise_message_code
- ise_network_device_name
- ise_selected_azn_profiles
- ise_user_name
- role

EXTEND THE CONTRACT **ACTION**

Add

Cancel **< Previous** **Next >**

1421

- 1422 7. On the **Adapter Attributes** screen, in the row for **ise_username**, check the box in the
 1423 **Pseudonym** column. Click **Next**. (Note: if you added other attributes in Step #6, you could check
 1424 the box under **Pseudonym** for those as well.)

Type	IdP Adapter	Extended Contract	Adapter Attributes	Summary
<p><input checked="" type="checkbox"/> As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.</p>				
ATTRIBUTE	PSEUDONYM	MASK LOG VALUES		
ip_address	<input type="checkbox"/>	<input type="checkbox"/>		
ise_audit_session	<input type="checkbox"/>	<input type="checkbox"/>		
ise_auth_acs_timestamp	<input type="checkbox"/>	<input type="checkbox"/>		
ise_auth_id	<input type="checkbox"/>	<input type="checkbox"/>		
ise_calling_station_id	<input type="checkbox"/>	<input type="checkbox"/>		
ise_identity_group	<input type="checkbox"/>	<input type="checkbox"/>		
ise_identity_store	<input type="checkbox"/>	<input type="checkbox"/>		
ise_message_code	<input type="checkbox"/>	<input type="checkbox"/>		
ise_network_device_name	<input type="checkbox"/>	<input type="checkbox"/>		
ise_selected_azn_profiles	<input type="checkbox"/>	<input type="checkbox"/>		
ise_user_name	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
role	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/> Mask all OGNL-expression generated log values				
		Cancel	< Previous	Next >

1425

1426 8. On the **Summary** screen, review the configuration and scroll down to click **Done**.

SECOND DRAFT

ISE User Name	admin
NAD Trigger URL	http://10.33.7.6
Resume Path Domain	abac.test
EXTENDED CONTRACT	
Attribute	ise_auth_acs_timestamp
Attribute	ise_audit_session
Attribute	role
Attribute	ise_network_device_name
Attribute	ise_calling_station_id
Attribute	ise_selected_azn_profiles
Attribute	ip_address
Attribute	ise_user_name
Attribute	ise_message_code
Attribute	ise_identity_store
Attribute	ise_identity_group
Attribute	ise_auth_id
ADAPTER ATTRIBUTES	
Mask all OGNL expression log values	false
Pseudonym	ise_user_name

Cancel < Previous Done

1427

1428 9. On the **Manage IdP Adapter Instances** screen, click **Save**.

INSTANCE NAME	INSTANCE ID	TYPE	PARENT NAME	ACTION
AD HTML forms	ADHTMLforms	HTML Form IdP Adapter		Delete (Check)
AdaptiveAuthentication	AdaptiveAuthentication	RSA Adaptive Authentication Adapter 2.0.0.0		Delete (Check)
CiscoISE	CiscoISE	Context Connector v2.0		Delete
HTMLForms	HTMLForms	HTML Form IdP Adapter		Delete (Check)
IdP Adapter	idpadapter	ReferenceID Adapter 1.0		Delete (Check)
MultiFactorAuthentication	MultiFactorAuthentication	Composite Adapter		Delete
RSA Multifactor	RSAMultifactor	Composite Adapter		Delete (Check)

1429

1430 2.13.8 Configure the Federation Connection to the Relying Party

1431 This PingFederate SP Connection at the PingFederate-IdP will configure the SAML exchange with a
 1432 server in the RP's environment. This connection will also enable a user to authenticate using the
 1433 composite adapter created in the previous section.

- 1434 1. On the **Main** Menu under **SP CONNECTIONS**, click **Create New**.
 1435 2. On the Connection Type screen, make sure **Browser SSO Profiles** is selected.

SECOND DRAFT

Main SP Connection

★ **Connection Type** Connection Options Import Metadata General Info Browser SSO Credentials Activation & Summary

Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all.

Connection Template	No Template
<input checked="" type="checkbox"/> Browser SSO Profiles	Protocol SAML 2.0
<input type="checkbox"/> WS-Trust STS	
<input type="checkbox"/> Outbound Provisioning	

Cancel **Next >**

1436

- 1437 3. Click **Next**. On the **Connection Options** screen, make sure **Browser SSO** is selected.

Main SP Connection

Connection Type ★ **Connection Options** Import Metadata General Info Browser SSO Credentials Activation & Summary

Please select options that apply to this connection.

<input checked="" type="checkbox"/> Browser SSO
<input type="checkbox"/> IdP Discovery
<input type="checkbox"/> Attribute Query

Cancel **< Previous** **Next >**

1438

- 1439 4. Click **Next**.
- 1440 5. On the **Import Metadata** screen, click **Browse** and select the metadata file that you exported from the RP's PingFederate server.
- 1441

SECOND DRAFT

If you received a metadata file from a partner SP describing this new connection, import the file here to populate many connection settings automatically.

Browse... metadata.xml

1442

- 1443 6. Click **Next**.
- 1444 7. On the **Metadata Summary** screen, click **Next**.
- 1445 8. On the **General Info** screen, you should see some configuration information (e.g., **Base URL**) about the RP that was taken from the metadata file that you selected earlier.
- 1446

This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints.

Partner's Entity ID (Connection ID): https://rp.abac.test:9031 *

Connection Name: https://rp.abac.test:9031 *

Virtual Server IDs:

Base URL: https://rp.abac.test:9031

Company:

Contact Name:

Contact Number:

Contact Email:

Application Name:

Application Icon URL:

Logging Mode: None Standard

1447

- 1448 9. Click **Next**. On the **Browser SSO** screen, click **Configure Browser SSO**.

SECOND DRAFT

1449

10. Select **IdP-Initiated SSO** and **SP-Initiated SSO**. Then, click **Next**.

The screenshot shows the Assertion Creation screen with the following interface elements:

- Top navigation bar: Main, SP Connection, Browser SSO.
- Sub-navigation bar: SAML Profiles, Assertion Lifetime, Assertion Creation (selected), Protocol Settings, Summary.
- Information message: A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported (bindings). As an IdP, you configure this information for your SP connection.
- Single Sign-On (SSO) Profiles section:
 - IdP-Initiated SSO
 - SP-Initiated SSO
- Single Logout (SLO) Profiles section:
 - IdP-Initiated SLO
 - SP-Initiated SLO
- Bottom right buttons: Save Draft, Cancel, Next >.

1450

11. On the **Assertion Lifetime** screen, click **Next**.

1452
1453

12. On the **Assertion Creation** screen, click **Configure Assertion Creation**. This will bring up a sequence of sub-screens, starting with the **Identity Mapping** screen.

1454

13. On the **Identity Mapping** screen, select the **Standard** option.

The screenshot shows the Identity Mapping screen with the following interface elements:

- Top navigation bar: Main, SP Connection, Browser SSO, Assertion Creation (selected).
- Sub-navigation bar: Identity Mapping (selected), Attribute Contract, Authentication Source Mapping, Summary.
- Information message: Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Select the type of name identifier that you will send to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.
- Options section:
 - Standard: Send the SP a known attribute value as the name identifier. The SP will often use account mapping to identify the user locally.
 - Pseudonym: Send the SP a unique, opaque name identifier that preserves user privacy. The identifier cannot be traced back to the user's identity at this IdP and may be used by the SP to make a persistent association between the user and a specific local account. The SP will often use account linking to identify the user locally.
 - Include attributes in addition to the pseudonym.
 - Transient: Send the SP an opaque, temporary value as the name identifier.
 - Include attributes in addition to the transient identifier.
- Bottom right buttons: Save Draft, Cancel, Next >.

1455

- 1456 14. Click **Next**. This will bring up the **Attribute Contract** screen.

SECOND DRAFT

The screenshot shows the PingFederate interface with the following navigation bar:

- Main
- SP Connection
- Browser SSO
- Assertion Creation

The current screen is "Attribute Contract". The sub-navigation bar includes:

- Identity Mapping
- Attribute Contract (selected)
- Authentication Source Mapping
- Summary

A message at the top states: "An Attribute Contract is a set of user attributes that this server will send in the assertion."

The main content area has two sections:

- ATTRIBUTE CONTRACT SUBJECT NAME FORMAT**: A table with one row. Column headers are "SAML_SUBJECT" and "ACTION". The value for SAML_SUBJECT is "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified". There is a dropdown arrow icon next to it.
- EXTEND THE CONTRACT**: A table with one row. Column headers are "ATTRIBUTE NAME FORMAT" and "ACTION". The value for ATTRIBUTE NAME FORMAT is "urn:oasis:names:tc:SAML:2.0:attrname-format:basic". There is a dropdown arrow icon next to it and an "Add" button.

At the bottom right are buttons: Save Draft, Cancel, < Previous, and Next >.

1457

1458

15. Click **Next**.

The screenshot shows the PingFederate interface with the following navigation bar:

- Main
- SP Connection
- Browser SSO
- Assertion Creation

The current screen is "Authentication Source Mapping". The sub-navigation bar includes:

- Identity Mapping
- Attribute Contract
- Authentication Source Mapping (selected)
- Summary

A message at the top states: "PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server."

The main content area has three columns:

- ADAPTER INSTANCE NAME
- VIRTUAL SERVER IDS
- ACTION

There is a button labeled "Map New Adapter Instance...".

At the bottom right are buttons: Save Draft, Cancel, < Previous, and Next >.

1459

1460

16. On the **Authentication Source Mapping** screen, click **Map New Adapter Instance**. This will launch a sequence of sub-screens, beginning with the **Adapter Instance** screen.

1461

1462

17. On the **Adapter Instance** screen, select the composite adapter created in an earlier section (e.g., **RSA Multifactor**).

SECOND DRAFT

The screenshot shows the 'IdP Adapter Mapping' section of a software interface. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, and IdP Adapter Mapping, with 'IdP Adapter Mapping' being the active tab. Below the tabs is a navigation bar with links for Adapter Instance, Assertion Mapping, Attribute Contract Fulfillment, Issuance Criteria, and Summary. A note in a callout box says: 'Select an IdP adapter instance that may be used to authenticate users for this partner. Attributes returned by the adapter instance you choose (the Adapter Contract) may be used to fulfill the Attribute Contract with your partner.' The 'ADAPTER INSTANCE' dropdown is set to 'RSA Multifactor'. Under 'ADAPTER CONTRACT', there are fields for transactionId and username, and a checkbox for 'Override Instance Settings'. At the bottom left is a 'Manage Adapter Instances...' button, and at the bottom right are 'Save Draft', 'Cancel', and 'Next >' buttons.

1464

- 1465 18. Click **Next**. On the Assertion Mapping screen, select **Use only the Adapter Contract values in the SAML assertion**.
- 1466

The screenshot shows the 'Assertion Mapping' section of a software interface. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, and IdP Adapter Mapping, with 'Assertion Mapping' being the active tab. Below the tabs is a navigation bar with links for Adapter Instance, Assertion Mapping, Attribute Contract Fulfillment, Issuance Criteria, and Summary. A note in a callout box says: 'You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "Composite Adapter" adapter, or you can use these values plus additional attributes retrieved from local data stores.' Under 'ADAPTER CONTRACT', there are fields for transactionId and username, and a radio button group for attribute retrieval: 'Retrieve additional attributes from multiple data stores using one mapping', 'Retrieve additional attributes from a data store--includes options to use alternate data stores and/or a failsafe mapping', and 'Use only the Adapter Contract values in the SAML assertion', which is selected. At the bottom right are 'Save Draft', 'Cancel', '< Previous', and 'Next >' buttons.

1467

- 1468 19. Click **Next**.

- 1469 20. On the **Attribute Contract Fulfillment** screen, for **SAML SUBJECT**, select **Adapter** for the **SOURCE** field and **username** for the **VALUE** field.
- 1470

SECOND DRAFT

The screenshot shows the PingFederate configuration interface. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, and IdP Adapter Mapping. Under IdP Adapter Mapping, the 'Attribute Contract Fulfillment' tab is active. Below the tabs, there are links for Adapter Instance, Assertion Mapping, Issuance Criteria, and Summary. A message box at the top says, "Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values." The main content area has a table with columns: ATTRIBUTE CONTRACT, SOURCE, VALUE, and ACTIONS. One row is shown: SAML_SUBJECT, Adapter, username, and "None available". At the bottom right are buttons for Save Draft, Cancel, < Previous, and Next >.

1471

1472

21. Click **Next**.

The screenshot shows the PingFederate configuration interface. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, and IdP Adapter Mapping. Under IdP Adapter Mapping, the 'Issuance Criteria' tab is active. Below the tabs, there are links for Adapter Instance, Assertion Mapping, Attribute Contract Fulfillment, Issuance Criteria, and Summary. A message box at the top says, "PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with this conditional authorization." The main content area has a table with columns: SOURCE, ATTRIBUTE NAME, CONDITION, VALUE, and ERROR RESULT. There are dropdown menus for SOURCE, ATTRIBUTE NAME, and CONDITION, and input fields for VALUE and ERROR RESULT.

1473

1474

22. Click **Next**.

SECOND DRAFT

The screenshot shows the 'IdP Adapter Mapping' configuration page. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, and IdP Adapter Mapping. Below these, sub-tabs include Adapter Instance, Assertion Mapping, Attribute Contract Fulfillment, Issuance Criteria, and Summary. A note at the top says 'Click a heading link to edit a configuration setting.' The main sections are:

- ADAPTER INSTANCE:** Selected adapter is RSA Multifactor.
- ASSERTION MAPPING:** Adapter is Composite Adapter; Data Store or Assertion uses only Adapter Contract values in the SAML assertion.
- ATTRIBUTE CONTRACT FULFILLMENT:** SAML_SUBJECT maps to username (Adapter).
- ISSUANCE CRITERIA:** Criterion is (None).

At the bottom right are buttons for Save Draft, Cancel, < Previous, and Done.

1475

- 1476 23. Click **Done**. This will bring you back to the **Authentication Source Mapping** screen, and you
1477 should see the composite adapter (e.g., **RSA Multifactor**) listed.

The screenshot shows the 'Authentication Source Mapping' configuration page. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, Identity Mapping, Attribute Contract, Authentication Source Mapping (which is selected), and Summary. A note at the top says 'PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server.' The main table lists adapter instances:

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION
RSA Multifactor		Delete

At the bottom right are buttons for Save Draft, Cancel, < Previous, and Next >. A button labeled 'Map New Adapter Instance...' is also present.

1478

- 1479 24. Click **Next**.

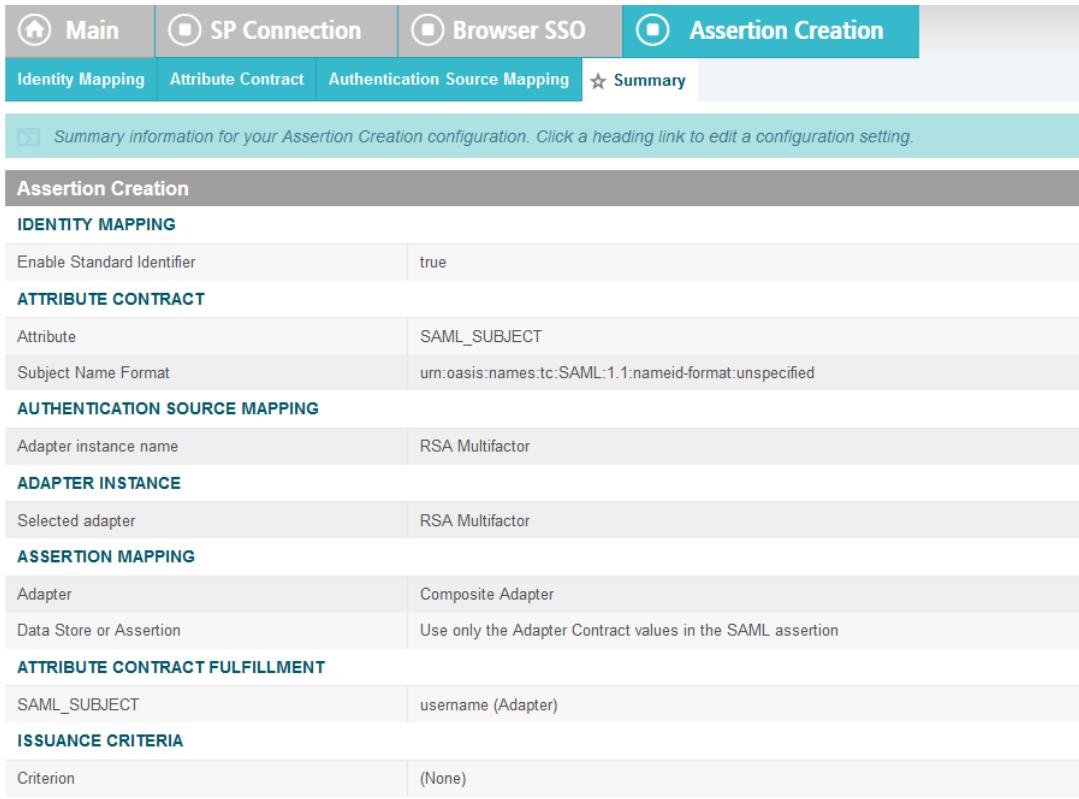
SECOND DRAFT

SECOND DRAFT

1480

1481 25. On the **Summary** screen, click **Done**. This will take you back to the **Configure Assertion Creation** screen.

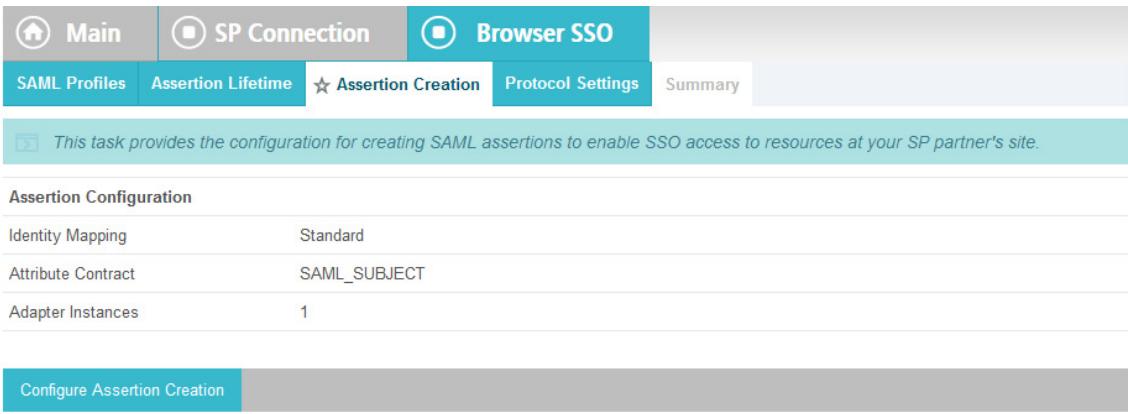
1482



1480

- 1481 25. On the **Summary** screen, click **Done**. This will take you back to the **Configure Assertion Creation** screen.

1482



1483

1484

26. Click **Next**.
- 

SECOND DRAFT

This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

Protocol Settings	
Outbound SSO Bindings	POST, Artifact
Inbound Bindings	POST, Redirect, Artifact, SOAP
Artifact Lifetime	60 second(s)
Signature Policy	SAML-standard, Authn requests over POST & Redirect
Encryption Policy	No Encryption

Configure Protocol Settings

Save Draft Cancel < Previous Next >

- 1485
- 1486 27. On the **Protocol Settings** screen, click **Configure Protocol Settings**. This will launch a sequence
1487 of sub-screens, beginning with the **Assertion Consumer Service URL** screen.
- 1488 28. On the **Assertion Consumer Service URL** screen, make sure that the **BINDING** field is set to **POST**
1489 and the **ENDPOINT URL** field is set to **/sp/ACS.saml2**.

As the IdP, you send SAML assertions to the SP's **Assertion Consumer Service**. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possible assertion consumer URLs below and select one to be the default.

DEFAULT	INDEX	BINDING	ENDPOINT URL	ACTION
default	0	POST	/sp/ACS.saml2	Edit / Delete
<input type="checkbox"/>	<input type="button" value=""/>	- SELECT - <input type="button" value="*"/>	<input type="text"/> *	<input type="button" value="Add"/>

Save Draft Cancel Next >

- 1490
- 1491 29. Click **Next**.
- 1492 30. On the **Allowable SAML Bindings** screen, select **POST** and **Redirect**.

SECOND DRAFT

When the SP sends messages, what SAML bindings do you want to allow?

- Artifact
- POST
- Redirect
- SOAP

Save Draft Cancel < Previous Next >

1493

1494 31. Click **Next**.

1495 32. On the **Signature Policy** screen, select **Require AuthN requests to be signed when received via the POST or Redirect bindings**.

Additional guarantees of authenticity may be agreed upon between you and your partner. For SP-initiated SSO, you can choose to require signed authentication requests sent via the POST or redirect bindings. You can also choose to sign assertions sent to this partner, regardless of the binding used.

- Require AuthN requests to be signed when received via the POST or Redirect bindings
- Always sign the SAML Assertion

Save Draft Cancel < Previous Next >

1497

1498 33. Click **Next**. On the **Encryption Policy** screen, select **The entire assertion**.

SECOND DRAFT

The screenshot shows the 'Protocol Settings' tab selected in a navigation bar. Below it is a sub-navigation bar with tabs: Assertion Consumer Service URL, Allowable SAML Bindings, Signature Policy, Encryption Policy (which is highlighted with a star), and Summary. A note at the top says: 'Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.' Below this note is a list of encryption policy options:

- None
- The entire assertion
- One or more attributes
- SAML_SUBJECT

At the bottom right are buttons: Save Draft, Cancel, < Previous, and Next >.

1499

1500 34. Click **Next**.

The screenshot shows the 'Summary' tab selected in a navigation bar. Below it is a sub-navigation bar with tabs: Assertion Consumer Service URL, Allowable SAML Bindings, Signature Policy, Encryption Policy (which is highlighted with a star), and Summary. A note at the top says: 'Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.'

Protocol Settings

ASSERTION CONSUMER SERVICE URL

Endpoint	URL: /sp/ACS.saml2 (POST)
----------	---------------------------

ALLOWABLE SAML BINDINGS

Artifact	false
POST	true
Redirect	true
SOAP	false

SIGNATURE POLICY

Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false

ENCRYPTION POLICY

Encrypt Entire Assertion	true
--------------------------	------

At the bottom right are buttons: Save Draft, Cancel, < Previous, and Done.

1501

1502 35. On the **Summary** screen, click **Done**.

SECOND DRAFT

The screenshot shows the 'SP Connection' tab selected in the top navigation bar. Below it, a sub-navigation bar includes 'SAML Profiles', 'Assertion Lifetime', 'Assertion Creation', 'Protocol Settings' (which is highlighted with a yellow star), and 'Summary'. A note at the top states: 'This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.' The 'Protocol Settings' section contains the following details:

Outbound SSO Bindings	POST
Inbound Bindings	POST, Redirect
Artifact Lifetime	60 second(s)
Signature Policy	SAML-standard, Authn requests over POST & Redirect
Encryption Policy	SAML Assertion

At the bottom are buttons for 'Configure Protocol Settings', 'Save Draft', 'Cancel', '< Previous', and 'Next >'.

1503

1504 This will take you back to the **Protocol Settings** screen.

1505 36. Click **Next**.

1506 37. On the **Summary** screen, click **Done**.

1507 This will take you back to the **Browser SSO** screen.

The screenshot shows the 'SP Connection' tab selected in the top navigation bar. Below it, a sub-navigation bar includes 'Connection Type', 'Connection Options', 'Import Metadata', 'Metadata Summary', 'General Info', 'Browser SSO' (which is highlighted with a yellow star), and 'Credentials'. A note at the top states: 'This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.' The 'Browser SSO Configuration' section contains a 'Configure Browser SSO' button.

1508

1509 38. Click **Next**.

1510 39. On the **Credentials** screen, click **Configure Credentials**.

1511 40. For the **Signing Certificate** field, select the certificate to be used to sign the SAML message.

1512 41. Select the certificate that you configured for the server in an earlier section.

1513 42. Select the **Signing Algorithm** for your environment (e.g., **RSA SHA256**).

SECOND DRAFT

01:30:DB:8C:25:AB (cn=demo dsig new) *

Include the certificate in the signature <KeyInfo> element.

RSA SHA256

Manage Certificates...

1514

1515

43. Click **Next**.

Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.

Manage Signature Verification Settings...

1516

1517

44. Click **Next**.

1518

1519

45. On the **Select XML Encryption Certificate** screen, select the **Block Encryption Algorithm** (e.g., **AES-128**), and the **Key Transport Algorithm** (e.g., **RSA-OAEP**).

1520

1521

46. For the selection box above the **Manage Certificates** button, select the RP's public key certificate to be used to encrypt the message content.

SECOND DRAFT

The screenshot shows the 'SP Connection' tab selected in the top navigation bar. Under the 'Credentials' section, the 'Select XML Encryption Certificate' tab is active. A note at the top says: 'Please select the partner certificate to use when encrypting message content as well as the preferred block encryption and key transport algorithms. Only RSA keys can be used for XML encryption.' Below this, there are two groups of options: 'Block Encryption Algorithm' (AES-128, AES-256, Triple DES) and 'Key Transport Algorithm' (RSA-v1.5, RSA-OAEP). A dropdown menu shows '01:4C:09:35:30:19 (cn=demo-sp-enc)' with an asterisk. At the bottom left is a 'Manage Certificates...' button.

1522

1523

47. Click **Next**.

The screenshot shows the 'Summary' tab selected in the top navigation bar. The main content area displays summary information for each section: 'DIGITAL SIGNATURE SETTINGS' (Selected Certificate: CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US; Include Certificate in KeyInfo: false; Selected Signing Algorithm: RSA SHA256), 'SIGNATURE VERIFICATION' (Trust Model: Unanchored), 'SIGNATURE VERIFICATION CERTIFICATE' (Selected Certificate: CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US), and 'SELECT XML ENCRYPTION CERTIFICATE' (Selected Block Encryption Algorithm: Aes_128; Selected Key Transport Algorithm: Rsa_oaep; Selected Encryption Certificate: CN=demo-sp-enc, O=NCCoE, C=US). At the bottom right are 'Save Draft', 'Cancel', '< Previous', and 'Next >' buttons.

1524

1525

48. On the **Summary** screen, click **Done**. This will take you back to the **Credentials** screen.

SECOND DRAFT

Digital Signature	Not Configured
Signature Verification Settings	Unanchored Certificate (Primary CN=demo dsig new, Secondary Not Configured)
Encryption Certificate	CN=demo-sp-enc

Configure Credentials

1526

1527 49. Click **Next**.

1528 50. On the **Activation & Summary** screen, select **Active** for the **Connection Status** field.

Connection Status	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
SSO Application Endpoint	https://idp.abac.test:9031/idp/startSSO.ping?PartnerSId=https://rp.abac.test:9031

SP Connection

CONNECTION TYPE

Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false

CONNECTION OPTIONS

Browser SSO	true
-------------	------

1529

- 1530 51. Copy the Identity Provider's SSO Application Endpoint URL (e.g.,
1531 <https://idp.abac.test:9031/idp/startSSO.ping?PartnerSId=https://rp.abac.test:9031>) to the
1532 clipboard and save it to a text file, because this URL will be used in the Functional Test section.
- 1533 52. Click **Done**. This will take you to a screen that lists the connections for the server, including the
1534 new connection you just created. Click **Save** to complete the configuration.

1535 **2.13.9 Configure ISE Composite Adapter**

- 1536 1. From the Main page, click on **Adapters**.
- 1537 2. Click **Create New Instance**.

INSTANCE NAME	INSTANCE ID
AD HTML forms	ADHTMLforms
AdaptiveAuthentication	AdaptiveAuthentication
CiscoISE	CiscoISE
HTMLForms	HTMLForms
IdP Adapter	idpadapter
ISE-RSA Composite Adapter	ISERSACCompositeAdapter
MultiFactorAuthentication	MultiFactorAuthentication
RSA Multifactor	RSAMultifactor

- 1538 3. In the Instance Name field, enter **ISE-RSA Composite Adapter**.
- 1539 4. In the Instance ID field, give the same name without spaces.
- 1540 5. In the Type field, choose **Composite Adapter**.

Instance Name: ISE-RSA Composite Adapter2 *

Instance Id: ISERSACompositeAdapter2 *

Type: Composite Adapter * Visit PingIdentity.com for additional types

Parent Instance: None

1542

1543 6. Click **Next**.1544 7. Click **Add a new row to 'Adapters'**.

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
CiscoSE	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	3		Move down Edit Delete
RSA Multifactor	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	3		Move up Edit Delete

1545

1546 8. Choose **CiscoSE**.1547 9. Click **Update**.1548 10. Click **Add a new row to 'Adapters'**.1549 11. Choose **RSA Multifactor**.1550 12. Click **Update**.

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
CiscoSE	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	1		Move down Edit Delete
RSA Multifactor	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	3		Move up Edit Delete

1551

1552 13. Click **Next**.

1553 14. Add the attributes from both the ISE and RSA adapters.

This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. You can either use the attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your System.

EXTEND THE CONTRACT ACTION	
ip_address	Edit / Delete
ise_audit_session	Edit / Delete
ise_auth_acs_timestamp	Edit / Delete
ise_auth_id	Edit / Delete
ise_calling_station_id	Edit / Delete
ise_identity_group	Edit / Delete
ise_identity_store	Edit / Delete
ise_message_code	Edit / Delete
ise_network_device_name	Edit / Delete
ise_selected_azn_profiles	Edit / Delete
ise_user_name	Edit / Delete
role	Edit / Delete
transactionid	Edit / Delete
username	Edit / Delete

[Add](#)

1554

15. Click **Next**.

1555

16. Check the **Pseudonym** box next to username.

The screenshot shows a user interface for creating an adapter instance. At the top, there are three tabs: 'Main' (selected), 'Manage IdP Adapter Instances', and 'Create Adapter Instance'. Below the tabs, there are five sub-tabs: 'Type' (selected), 'IdP Adapter', 'Extended Contract', 'Adapter Attributes' (with a star icon), and 'Summary'. A note below the tabs states: 'As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this list, you can select which attributes will be used for constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.' A table follows, listing attributes on the left and checkboxes for pseudonyms on the right.

ATTRIBUTE	PSEUDONYM
ip_address	<input type="checkbox"/>
ise_audit_session	<input type="checkbox"/>
ise_auth_acs_timestamp	<input type="checkbox"/>
ise_auth_id	<input type="checkbox"/>
ise_calling_station_id	<input type="checkbox"/>
ise_identity_group	<input type="checkbox"/>
ise_identity_store	<input type="checkbox"/>
ise_message_code	<input type="checkbox"/>
ise_network_device_name	<input type="checkbox"/>
ise_selected_azn_profiles	<input type="checkbox"/>
ise_user_name	<input type="checkbox"/>
role	<input type="checkbox"/>
transactionid	<input type="checkbox"/>
username	<input checked="" type="checkbox"/>
<input type="checkbox"/> Mask all OGNL-expression generated log values	

1557

17. Click **Next**.

1559

18. Click **Done**.

1560

19. Click **Save**.

1561

2.13.10 Applying the Composite Adapter

1562

1. From the main page, click on **rp.abac.test** under SP Connections.

The screenshot shows the 'IdP Configuration' page. Under 'APPLICATION INTEGRATION SETTINGS', there are links for Adapters, Authentication Selection, Default URL, and Application Endpoints. Under 'FEDERATION SETTINGS', there is a link for Protocol Endpoints. Under 'SP CONNECTIONS (3)', three entries are listed: SAML2.0 https://rp.abac.t..., SAML2.0 Demo SP, and SAML2.0 urn:nccoe:abac:rp. Below these are links for Manage All SP, Create New, and Import.

1563

- 1564 2. Scroll down and click on **Authentication Source Mapping**.

The screenshot shows the 'AUTHENTICATION SOURCE MAPPING' section. It displays two rows of mappings:

Adapter instance name	ISE-RSA Composite Adapter
Adapter instance name	RSA Multifactor

1565

1566 3. Click on **Map New Adapter Instance**.

The screenshot shows the 'Map New Adapter Instance...' interface. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, Identity Mapping, Attribute Contract, Authentication Source Mapping (which is highlighted), and Summary. A note below the tabs states: 'PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters.' The main table has columns for ADAPTER INSTANCE NAME and VIRTUAL SERVER IDS. Two rows are listed:

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS
ISE-RSA Composite Adapter	
RSA Multifactor	

A large button at the bottom left says 'Map New Adapter Instance...'

1567

1568 4. In the **Adapter Instance** box, select the composite adapter.

NIST SP 1800-3C: Attribute Based Access Control

119

SECOND DRAFT

>Main **IdP Adapter Mapping**

Adapter Instance Assertion Mapping Attribute Contract Fulfillment Issuance Criteria Summary

Select an IdP adapter instance that may be used to authenticate users for this partner. Attributes returned by the adapter instance you choose (the Adapter Contract) may be used with your partner.

ADAPTER INSTANCE ISE-RSA Composite Adapter2

ADAPTER CONTRACT

ip_address
ise_audit_session
ise_auth_acs_timestamp
ise_auth_id
ise_calling_station_id
ise_identity_group
ise_identity_store
ise_message_code
ise_network_device_name
ise_selected_azn_profiles
ise_user_name
role
transactionid
username

Override Instance Settings

Manage Adapter Instances...

1569

5. Click **Next**.

1570 6. Select the top radio button labeled **Retrieve additional attributes from multiple data stores using one mapping**.

SECOND DRAFT

ADAPTER CONTRACT

- ip_address
- ise_audit_session
- ise_auth_acs_timestamp
- ise_auth_id
- ise_calling_station_id
- ise_identity_group
- ise_identity_store
- ise_message_code
- ise_network_device_name
- ise_selected_azn_profiles
- ise_user_name
- role
- transactionid
- username

Retrieve additional attributes from multiple data stores using one mapping
 Retrieve additional attributes from a data store-includes options to use alternate data stores and/or a failsafe mapping
 Use only the Adapter Contract values in the SAML assertion

1573

1574 7. Click **Next**.

1575 8. Click **Add Attribute Source**.

DESCRIPTION

TYPE

ACTION

Add Attribute Source...

1576

1577 9. Enter **ActiveDirectory** for Source Id and Description.

1578 10. Select **activedirectory.abac.test** in the Active Data Store drop-down.

SECOND DRAFT

Attribute Source Id: ActiveDirectory *

Attribute Source Description: ActiveDirectory *

Active Data Store: activedirectory.abac.test *

Data Store Type: LDAP

1579

11. Click **Next**.

1580

12. In the BaseDN field, enter **DC=ABAC,DC=TEST**.

1581

13. Add all of the attributes from the LDAP Directory Search.

ROOT OBJECT CLASS	ATTRIBUTE	ACTION
	Subject DN	Remove
	accountNumber	Remove
	clearance	Remove
	company	Remove
	department	Remove
	planName	Remove
	role	Remove
	staffLevel	Remove
	state	Remove
	title	Remove
	userPrincipalName	Remove

<Show All Attributes> Enabled Add Attribute

1582

14. Click **Next**.

1583

15. In the Filter field, enter **sAMAccountName=\${ise_user_name}**.

1586

16. Click **Next**.

1588

17. Click **Save**.

1589

18. Click on **Attribute Sources & Data Store**.

! accountNumber must be mapped to something.
! browser_language must be mapped to something.
! browser_type must be mapped to something.
! browser_version must be mapped to something.
! challenge_auth_method must be mapped to something.
! challenge_successful must be mapped to something.
! clearance must be mapped to something.
! company must be mapped to something.
! department must be mapped to something.
! fullname must be mapped to something.
! geodistance must be mapped to something.
! groundspeed must be mapped to something.
! ip_address must be mapped to something.
! operating_system must be mapped to something.
! planName must be mapped to something.
! risk_score must be mapped to something.
! role must be mapped to something.
! SAML_SUBJECT must be mapped to something.
! stafflevel must be mapped to something.
! state must be mapped to something.
! timezone must be mapped to something.
! title must be mapped to something.
! upn must be mapped to something.

1590

19. Click on **Add Attribute Source**.

DESCRIPTION	TYPE	ACTION
ActiveDirectory	LDAP	Delete

1592

20. Enter **RSAAA** for Source Id and Description.

SECOND DRAFT

1594

21. Select **JDBC:sqlserver** in the Active Data Store drop-down.

The screenshot shows the 'Attribute Sources & User Lookup' configuration page. At the top, there are tabs: Main, SP Connection, Browser SSO, Assertion Creation, IdP Adapter Mapping, and Attribute Sources & User Lookup (which is selected). Below the tabs, there are four input fields: Attribute Source Id (RSAAA), Attribute Source Description (RSAAA), Active Data Store (jdbc:sqlserver://10.33.7.12:1433;databaseName=RSA_CORE_AA), and Data Store Type (JDBC). A note at the top states: 'This server uses local data stores to retrieve supplemental attributes to be sent in an assertion. Specify an Attribute Source name that will distinguish this user lookup.' A 'Manage Data Stores...' button is located at the bottom left of the form area.

1595

22. Click **Next**.

1596

23. Select **dbo** in the Scheme drop-down.

1597

24. Select **EVENT_LOG** in the Table drop-down.

1598

25. Add each of the columns from the table.

The screenshot shows the 'Database Table and Columns' configuration page. At the top, there are tabs: Data Store (selected), Database Table and Columns, Database Filter, and Summary. A note at the top states: 'Please select the table and columns you want to query. This information, along with the attributes supplied in the contract, will be used to fulfill the contract.' Below the tabs, there are two dropdown menus: Schema (dbo) and Table (EVENT_LOG). A list of columns is shown with 'Remove' links next to each: BROWSER_LANGUAGE, BROWSER_TYPE, BROWSER_VERSION, CHALLENGE_AUTH_METHOD, CHALLENGE_SUCCESSFUL, GEODISTANCE, GROUNDSPEED, IP_ADDRESS, OPERATING_SYSTEM, RISK_SCORE, and TIMEZONE. At the bottom, there is an input field for ACCEPT_LANGUAGE, an 'Add Attribute' button, and a 'Refresh' button.

1599

[View Attribute Contract](#)

- 1601 26. Click **Next**.
- 1602 27. In the Where field, enter **USER_ID=\${transactionid}**.

The screenshot shows a software interface for configuring attribute sources and user lookup. At the top, there are three tabs: 'Main' (selected), 'SP Connection', and 'Browser S'. Below them is another set of tabs: 'Attribute Sources & User Lookup' (selected, highlighted in blue), 'Data Store', 'Database Table and Columns', 'Database Filter' (with a star icon), and 'Summary'. A message box at the top says 'Please supply a WHERE clause to filter the data from your table.' Below this, a 'Where' field contains the value 'USER_ID=\${transactionid}'. Underneath, there's a section titled 'Adapter Values' which lists the value '\${ip_address}'.

- 1603 \${ip_address}
- 1604 28. Click **Next**.
- 1605 29. Click **Done**.
- 1606 30. Click **Next**.
- 1607 31. Map all the attributes as shown in the screenshot below.

SECOND DRAFT

Main	SP Connection	Browser SSO	Assertion Creation	IdP Adapter Mapping
Adapter Instance	Assertion Mapping	Attribute Sources & User Lookup	Attribute Contract Fulfillment	Issuance Criteria
			★	Summary
Fulfill your Attribute Contract with values from one or more data stores, the authentication adapter, or dynamic text values.				
ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS	
SAML SUBJECT	Adapter	ise_user_name	None available	
accountNumber	LDAP (ActiveDirectory)	accountNumber	None available	
browser_language	JDBC (RSAAA)	BROWSER_LANGUAGE	None available	
browser_type	JDBC (RSAAA)	BROWSER_TYPE	None available	
browser_version	JDBC (RSAAA)	BROWSER_VERSION	None available	
challenge_auth_method	JDBC (RSAAA)	CHALLENGE_AUTH_METHOD	None available	
challenge_successful	JDBC (RSAAA)	CHALLENGE_SUCCESSFUL	None available	
clearance	LDAP (ActiveDirectory)	clearance	None available	
company	LDAP (ActiveDirectory)	company	None available	
department	LDAP (ActiveDirectory)	department	None available	
fullname	LDAP (ActiveDirectory)	Subject DN	None available	
geodistance	JDBC (RSAAA)	GEODISTANCE	None available	
groundspeed	JDBC (RSAAA)	GEODISTANCE	None available	
ip_address	JDBC (RSAAA)	IP_ADDRESS	None available	
operating_system	JDBC (RSAAA)	OPERATING_SYSTEM	None available	
planName	LDAP (ActiveDirectory)	planName	None available	
risk_score	JDBC (RSAAA)	RISK_SCORE	None available	
role	LDAP (ActiveDirectory)	role	None available	
stafflevel	LDAP (ActiveDirectory)	staffLevel	None available	
state	LDAP (ActiveDirectory)	state	None available	
timezone	JDBC (RSAAA)	TIMEZONE	None available	
title	LDAP (ActiveDirectory)	title	None available	
upn	LDAP (ActiveDirectory)	userPrincipalName	None available	

1608

- 1609 32. Click **Next**.
- 1610 33. Click **Next**.
- 1611 34. Click **Save**.
- 1612 35. Back at the main page, click on **rp.abac.test** under SP Connections.

The screenshot shows the 'IdP Configuration' interface. Under 'APPLICATION INTEGRATION SETTINGS', there are links for Adapters, Authentication Selection, Default URL, and Application Endpoints. Under 'FEDERATION SETTINGS', there is a link for Protocol Endpoints. Under 'SP CONNECTIONS (3)', there are three entries: SAML2.0 https://rp.abac.t..., SAML2.0 Demo SP, and SAML2.0 urn:nccoe:abac:rp. Below these are links for Manage All SP, Create New, and Import.

1613

1614 36. Scroll down and click on **Database Filter**.1615 37. In the Where field, enter **EVENT_ID=\${transactionid}**.

The screenshot shows the 'Attribute Sources & User Lookup' tab selected. Below it, the 'Database Filter' tab is active. A message at the top says 'Please supply a WHERE clause to filter the data from your table.' Below that is a 'Where' field containing the value 'EVENT_ID = '\${transactionid}''. There is also a small asterisk (*) next to the input field.

1616

1617 38. Click **Save**.1618

2.14 Certificates

1619 Once you have installed the various products for this ABAC build, you can replace the default self-signed
 1620 certificates with certificates signed by a Certificate Authority (CA). For our build, we used Symantec's
 1621 Managed PKI Service to sign our certificates using a local CA. Certificates were used to support various
 1622 exchanges that require encryption, such as digital signature, SAML message encryption, and encryption
 1623 of TLS communications.

1624 Although the detailed instructions of configuring certificates signed by a CA vary by vendor product, the
1625 general process is described below. For each certificate, you perform the following high-level steps:

- 1626 1. Using the vendor product (e.g., PingFederate, SharePoint), generate a certificate signing request
1627 on the server where you want to use the certificate. Save the signing request to a file.
- 1628 2. Submit an enrollment request to your CA. You will need to provide the signing request that was
1629 generated in Step 1. This step is typically where you provide information such as the name of the
1630 server you intend to use the certificate on (e.g., “idp.abac.test”).
- 1631 3. A representative at the CA will examine the enrollment request and approve it. The
1632 representative will issue a certificate response signed with the CA’s key. You can download the
1633 signed response. If you are using a CA that is locally managed by your organization, you will also
1634 need to download the public key of the CA, because you will need to add this the Trusted
1635 Certificate Authorities on each server and client that will be using the certificates.
- 1636 4. Go back to the vendor product where you created the certificate signing request. If you are using
1637 a local CA, you will first need to add the Certificate Authority’s public key to the list of Trusted
1638 Certificate Authorities.
- 1639 5. Import the certificate file for your server that was signed by the CA.

2.14.1 Certificate Configuration PingFederate

1641 In the PingFederate app, on the main menu, under Certificate Management, click Trusted CAs to import
1642 the public key of your local CA. If you are using a well-known, external, major CA and that authority’s
1643 public key is already available in cacerts in the Java runtime, it is not necessary to import the same
1644 certificate into the PingFederate Trusted CA store.

- 1645 ▪ For SSL Server certificates, follow the instructions in the link below. The applicable sections are
1646 “To create a new certificate,” “To create a certificate-authority signing request,” and “To import
1647 a certificate authority response.” Once you have imported a signed certificate response, you will
1648 need to active the certificate on the PingFederate runtime server instance on which your
1649 applications are running. Follow the instructions in the section “To activate a certificate.”

1650 <https://documentation.pingidentity.com/display/PF73/SSL+Server+Certificates>

- 1651 ▪ For digital signatures and performing encryption / decryption, follow the instructions in the link
1652 below. The applicable sections are the same as for SSL Server certificates.

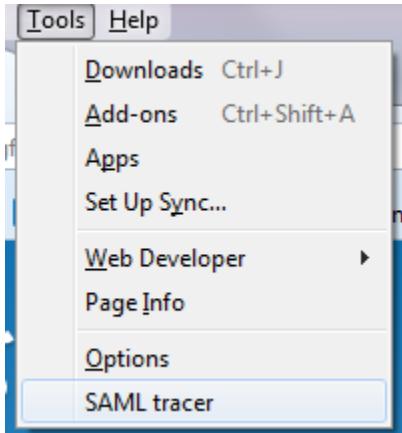
1653 <https://documentation.pingidentity.com/display/PF73/Digital+Signing+and+Decryption+Keys+an+Certificates>

2.15 Functional Test of All Configurations for Section 2

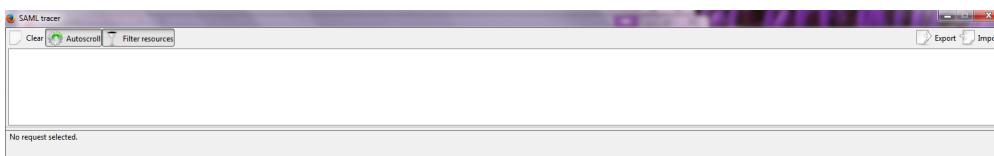
1656 The instructions in this section will help perform an integrated test all of the configurations in Section 2.
1657 Using the browser and PingFederate, a user will log on and validate that the federated authentication to
1658 Microsoft AD and RSA AA are properly configured.

1659 The test for this section was performed using the Mozilla Firefox browser and the “SAML tracer” add-on,
1660 which enables examination of HTTPS POST and SAML messages.

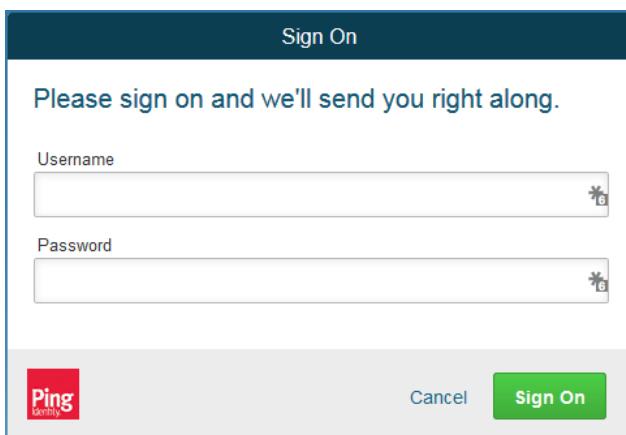
- 1661 1. Install the Firefox SAML tracer add-on from the link below.
1662 <https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/>
1663 2. Launch your Firebox browser and select **SAML tracer** from the Tools menu.



- 1664
1665 This will launch an empty SAML tracer window.



- 1666
1667 3. Minimize the SAML tracer window. The SAML tracer will automatically record the details of the
1668 HTTPS messages in the background.
1669 4. Go back to the main browser window and navigate to the Identity Provider's SSO Application
1670 Endpoint URL identified in the previous section (e.g.,
1671 <https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=https://rp.abac.test:9031>).
1672 Expected Result: You should see the PingFederate Sign On screen.



- 1673
1674 5. Enter the **Username** of the account created in Microsoft AD earlier in this section (e.g., **Ismith**).
1675 6. Enter an invalid password for the account. Do not enter the correct password.

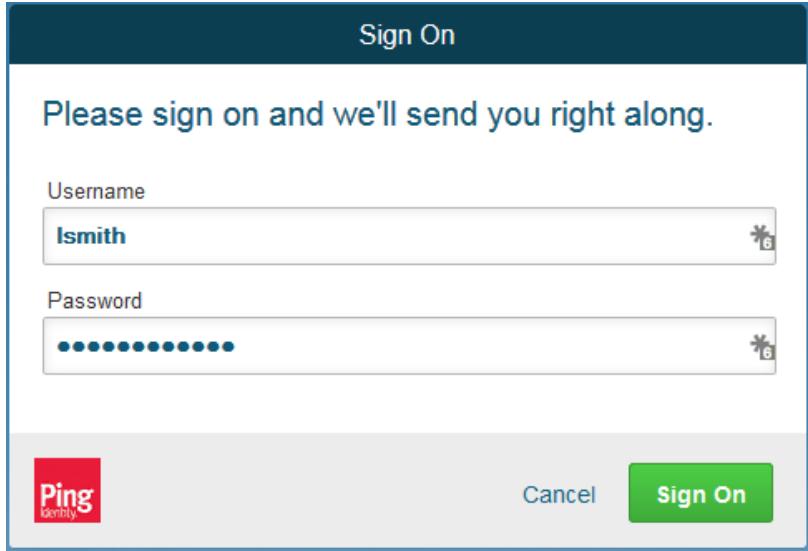
Sign On

Please sign on and we'll send you right along.

Username

Password

Ping Identity Cancel Sign On



1676

- 1677 7. Click **Sign On**.

1678 **Expected Result:** You should see an error message that states, “We didn’t recognize the
1679 username or password you entered.”

Sign On

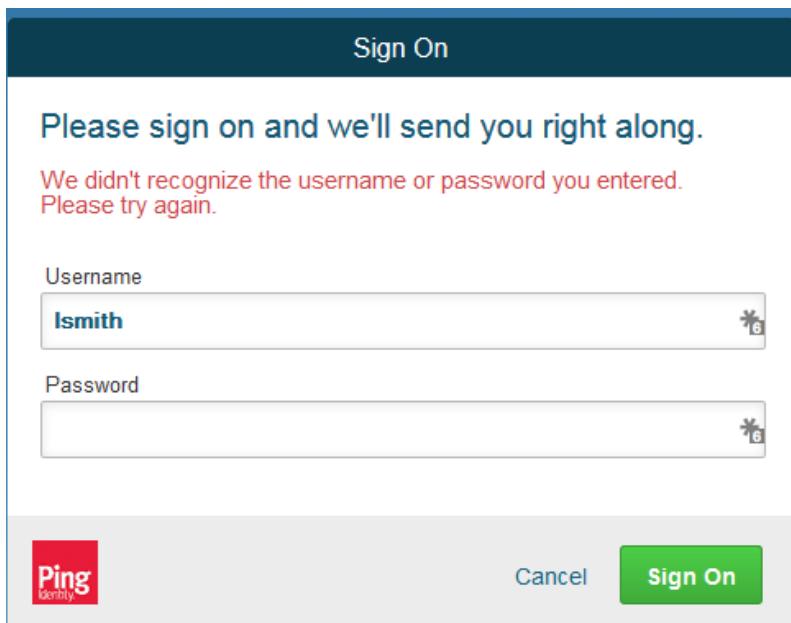
Please sign on and we'll send you right along.

We didn't recognize the username or password you entered.
Please try again.

Username

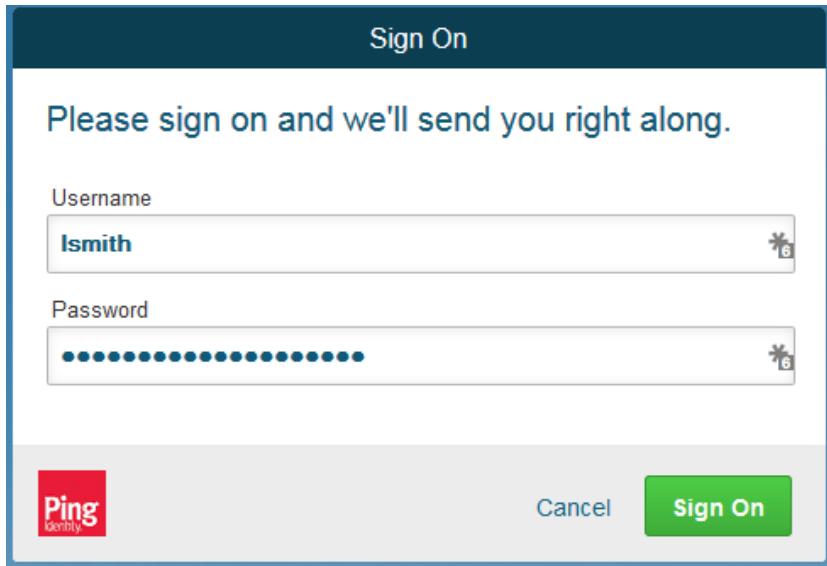
Password

Ping Identity Cancel Sign On



1680

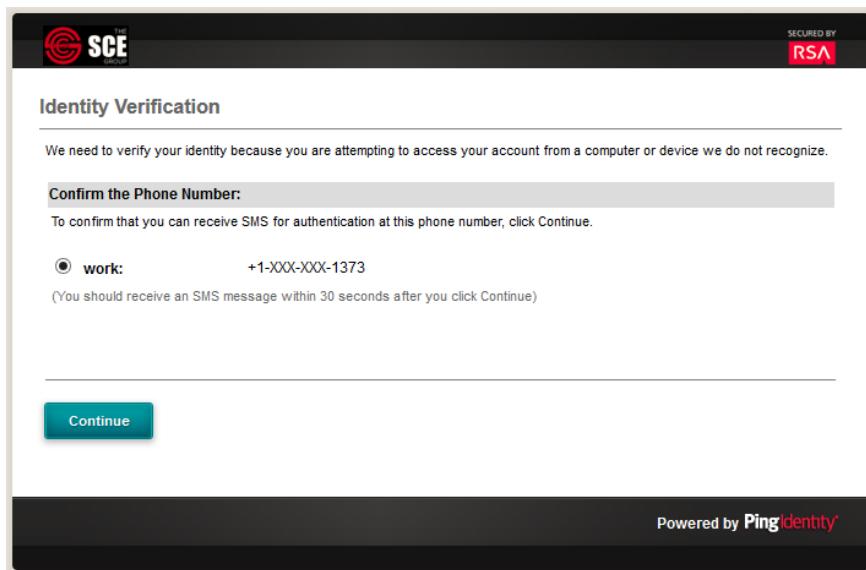
- 1681 8. Close the existing browser and launch a new browser.
- 1682 9. Navigate to the Identity Provider’s SSO Application Endpoint URL again.
- 1683 10. Enter the user name of the account created earlier in this section (e.g., **Ismith**). Then, enter the
1684 correct password.



1685

1686 11. Click **Sign On**.

1687 Expected Result: You should see the two-factor RSA AA plug-in screen. This screen prompts you
1688 to enter the SMS text validation code received by your mobile phone.



1689

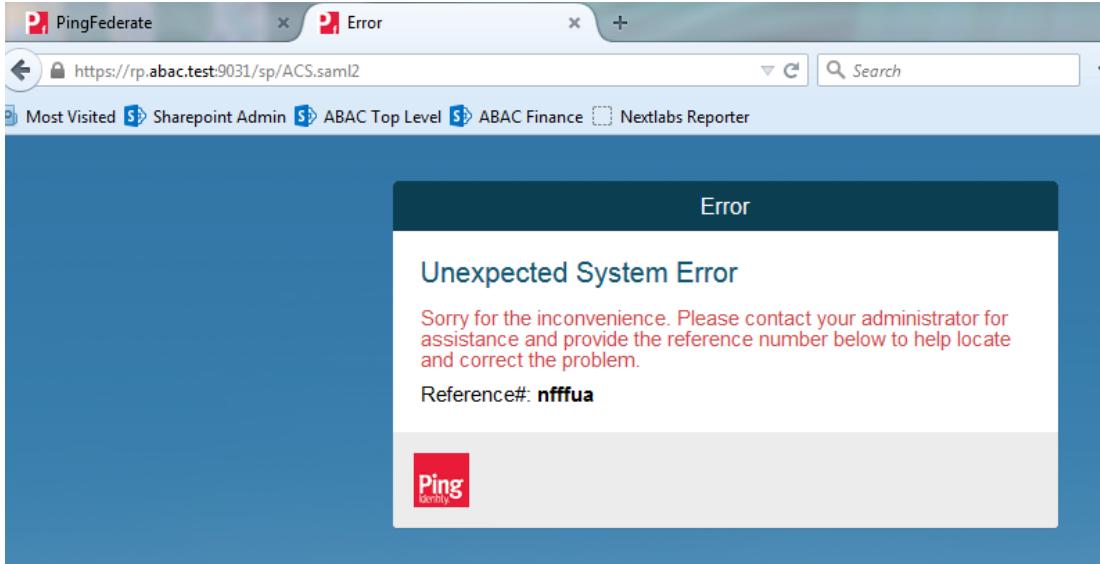
The screenshot shows a web page titled "Identity Verification". At the top, there are logos for "SCE" and "SECURED BY RSA". Below the title, a message states: "We are now sending an SMS message containing a confirmation code the following phone number you selected." A "Selected Phone Number" field contains "+1-XXX-XXX-1373" with "work:" preceding it. A note below says: "Enter the confirmation code below. After entering the confirmation code, you will be authorized to continue. If you didn't receive the SMS within 60 seconds or had other problems, please contact your administrator." A "Confirmation Code:" input field has a placeholder "123456". Under "Would You Like Us to Remember this Computer?", two radio buttons are shown: "Yes, I plan on using this computer to access my account in the future" (unchecked) and "No, This is a public computer or one I do not plan on using often to access my account" (checked). A "Continue" button is at the bottom left. A "Powered by PingIdentity" logo is at the bottom right.

1690

- 1691 12. Enter the SMS validation code received on your mobile phone and proceed. This will initiate a
1692 communication with the RSA AA server to validate the code that was entered.

1693
1694

Expected Result: The browser should redirect to the RP's Federation Server (e.g., **rp.abac.test**), and you should see an error message similar to the screenshot below.



1695

- 1696 13. Go back to the SAML tracer window. Scroll to the bottom of the list of messages in the upper
1697 pane. Click on the last message (e.g., POST <https://rp.abac.test:9031/sp/ACS.saml2>) that has a
1698 SAML icon associated with it. This will show the details of the POST message.

```

POST https://rp.abac.test:9031/sp/ACS.saml2 HTTP/1.1
Host: rp.abac.test:9031
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: application/saml+xml, application/xml;q=0.9, */*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://idp.abac.test:9031/idp/acsU/resumeSAML20/idp/startSSO.ping
Content-Type: application/x-www-form-urlencoded
Content-Length: 5169

HTTP/1.1 500 Server Error
Date: Mon, 20 Jul 2015 19:37:15 GMT
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
max-age: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1572

```

1699

Expected Result: In the details page at the bottom, on the **http** tab, you should see that the browser sent a **POST** message to the RP's PingFederate server **rp.abac.test**. The HTTP response status code (identified on the line that begins with **HTTP**) should be a **500 Server Error**.

1700 14. Click on the **SAML** tab.

```

<samlp:Response Version="2.0">
  <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
      <ds:Reference URI="#G0y0BRCNxWGBGfHe160.SbNu9" />
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldsig#sha256" />
      <ds:DigestValue>90QGFcSQuPspkaLD1PcAD37Nt7AfCMIcxEN0zkhak=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>Xg2q1quD93pJN1ZTfZMkTtcgH5ExKt6SFfMkT/1UJlsshe0uxlRuc/2/FCVdIH7FI+jI
  q76pqj3HK/+4DVN61qASD/mEED1Q46t1j3YduqgSc1HdCc0OfcSNE3oWi+w?M1dB6vuErvu0+Sjf1
  vWQg3j7+sGX/B26R2zQ=</ds:SignatureValue>
  </ds:Signature>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </samlp:Status>
</samlp:Response>

```

1704

Expected Result: You should see the details of the SAML message, including the Issuer. The Issuer should be the IdP's Federation server, **idp.abac.test**.

1705 3 Setting up Federated Authentication Between the Relying 1706 Party and the Identity Provider

1707 3.1 Introduction

1708 In the previous section of this How-To Guide we demonstrated how to set up federated, SAML-based authentication at the identity provider (IdP). Before continuing with this section, it is necessary to have a working federation service that will represent the identity provider and can receive and issue SAML 2.0 requests and responses. For instructions on how to set this up using Ping Federate, please refer to [Section 2](#) of this guide.

1715 In order to federate identities and attribute information between organizations a federation service
 1716 must exist at both the identity provider and the relying party (RP). A trust relationship between these
 1717 two services must then be instantiated to allow for identity and attribute requests and responses. In this
 1718 section we configure an instance of PingFederate (henceforth called PingFederate-RP) at the relying
 1719 party to act as a federation service and to redirect users to the PingFederate-IdP via a SAML request. We
 1720 then configure the trust relationship and federated authentication between the PingFederate-RP and
 1721 the PingFederate-IdP, allowing the SAML request to be processed by the identity provider and the
 1722 subsequent return of a SAML response containing identity and attribute assertions.

1723 If you follow the instructions in this How-To Guide section, you will be able to perform a functional test
 1724 to verify the successful completion of the steps for installing, configuring, and integrating the
 1725 components.

1726 **3.2 Components**

1727 Federated authentication between the relying party and the identity provider involves the following
 1728 distinct components:

- 1729 ▪ **PingFederate-IdP:** A federation system or trust broker for the identity provider
- 1730 ▪ **PingFederate-RP:** Serves as the trust broker for SharePoint

1731 **3.2.1 PingFederate-IdP**

1732 Ping Identity PingFederate-IdP serves as a federation system or trust broker for the IdP. PingFederate-
 1733 IdP provides initial user authentication and retrieval of user attributes to satisfy SAML requests from the
 1734 RP. Once the user has been authenticated, PingFederate-IdP queries subject attributes from AD and
 1735 environmental attributes from the RSA AA event log. PingFederate-IdP takes the name:value pairs of
 1736 both the subject and environmental attributes and stores them in a SAML 2.0 token to be sent to the RP.

1737 **PingFederate Usage Notes:**

- 1738 ▪ When using the PingFederate application to perform an administrative configuration, there is
 1739 usually a sequence of screens that require user entry, ending with a summary page. Once you
 1740 click **Done** on the summary page, you must also click **Save** on the following page to save the
 1741 configurations. If you forget to click **Save**, you may inadvertently lose changes to the
 1742 configuration.
- 1743 ▪ In the PingFederate application and associated documentation, the relying party is referred to as
 1744 the “Service Provider.”
- 1745 ▪ When using the PingFederate application to perform configuration, refer to the title of the tab
 1746 with a small star icon to its left, to identify the item you are currently configuring. For example,
 1747 if you navigated to the following screen, you would be on the IdP Adapter screen.



1748

1749

3.2.2 PingFederate-RP

1750 Ping Identity PingFederate-RP serves as the trust broker for SharePoint. When the user requires
 1751 authentication, PingFederate-RP redirects the user to the IdP via a SAML request to get the necessary
 1752 assertions. Once authenticated, PingFederate-RP arranges for the browser's HTTPS content to have the
 1753 proper information in proper format for acceptance at the target resource (SharePoint).

1754

3.3 Export Metadata from the Identity Provider

1755 Follow the instructions in this section to export a metadata file from the PingFederate-IdP.

- 1756 1. Logon to the server that hosts the PingFederate service for the Identity Provider.
- 1757 2. Launch your browser and navigate to the PingFederate application URL:
https://<DNS_NAME>:9999/pingfederate/app.
- 1759 3. Replace DNS_NAME with the fully qualified name of the Identity Provider's PingFederate server
 1760 (e.g., *https://idp.abac.test:9999/pingfederate/app*). Logon to the PingFederate application using
 1761 the credentials you configured during installation.
- 1762 4. On the **Main Menu** under **Administrative Functions**, click **Metadata Export**.
- 1763 5. On the Metadata Mode screen, select **Use a connection for metadata generation**.



1764

- 1765 6. Click **Next**. On the Connection Metadata screen, select the connection to the relying party that
 1766 you configured in the previous section (e.g., *https://rp.abac.test:9031*). This should
 1767 automatically populate some of the fields on the screen with information from the connection.

SECOND DRAFT

The screenshot shows the 'Export Metadata' interface. At the top, there are tabs for 'Main' and 'Export Metadata'. Below them, 'Metadata Mode' is selected, followed by 'Connection Metadata', 'Metadata Signing', and 'Export & Summary'. A note says 'Select a connection that contains the Attribute Contract and Digital Signature Key you wish to include in the metadata.' A dropdown menu shows 'https://rp.abac.test:9031'. Below this, sections for 'ATTRIBUTE CONTRACT' (SAML_SUBJECT) and 'DIGITAL SIGNATURE KEY' (CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US) are shown. An 'XML ENCRYPTION KEY' section notes 'No XML key available for this connection'. At the bottom right are 'Cancel', '< Previous', and 'Next >' buttons.

1768

- 1769 7. Click **Next**. On the Metadata Signing screen, if you plan to sign the metadata file that will be
1770 exported, select the certificate that will be used to sign the file.

The screenshot shows the 'Metadata Signing' interface. At the top, there are tabs for 'Main' and 'Export Metadata'. Below them, 'Connection Metadata' is selected, followed by 'Metadata Signing', 'Metadata Mode', and 'Export & Summary'. A note says 'From this list of certificates, choose which one to use for signing the selected file.' A dropdown menu labeled 'Signing Certificate' shows '- SELECT -'. At the bottom right are 'Cancel', '< Previous', and 'Next >' buttons.

1771

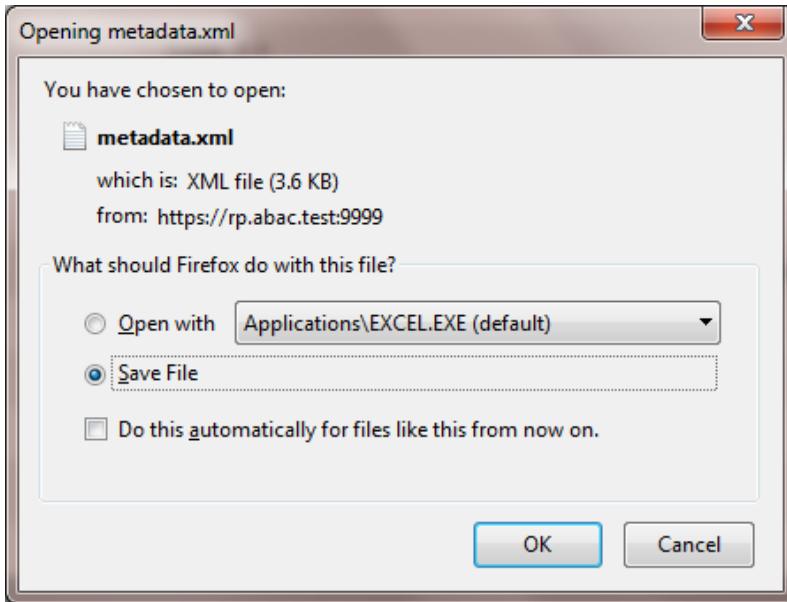
- 1772 8. Click **Next**. On the Export & Summary screen, you should see a summary of the options that
1773 were selected.

SECOND DRAFT

The screenshot shows the 'Export Metadata' configuration page. At the top, there are tabs: 'Main' (selected), 'Export Metadata' (highlighted in blue), 'Metadata Mode', 'Connection Metadata', 'Metadata Signing', and 'Export & Summary'. Below the tabs, a message says 'Click the Export button to export this metadata to the file system.' The main area is titled 'Export Metadata' and contains three sections: 'METADATA MODE', 'CONNECTION METADATA', and 'METADATA SIGNING'. Under 'METADATA MODE', 'Metadata mode' is set to 'Use connection' and 'Use the secondary port for SOAP channel' is set to 'false'. Under 'CONNECTION METADATA', 'Selected connection' is 'https://rp.abac.test:9031', 'Attribute' is 'SAML_SUBJECT', and 'Digital Signature Key' is 'CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US'. Under 'METADATA SIGNING', 'Signing Certificate' is 'None'. At the bottom, there is an 'Export' button and navigation buttons: 'Cancel', '< Previous', and 'Done'.

1774

- 1775 9. Click **Export**. This will create an export file that contains the metadata of the identity provider
1776 that you can download using the browser.



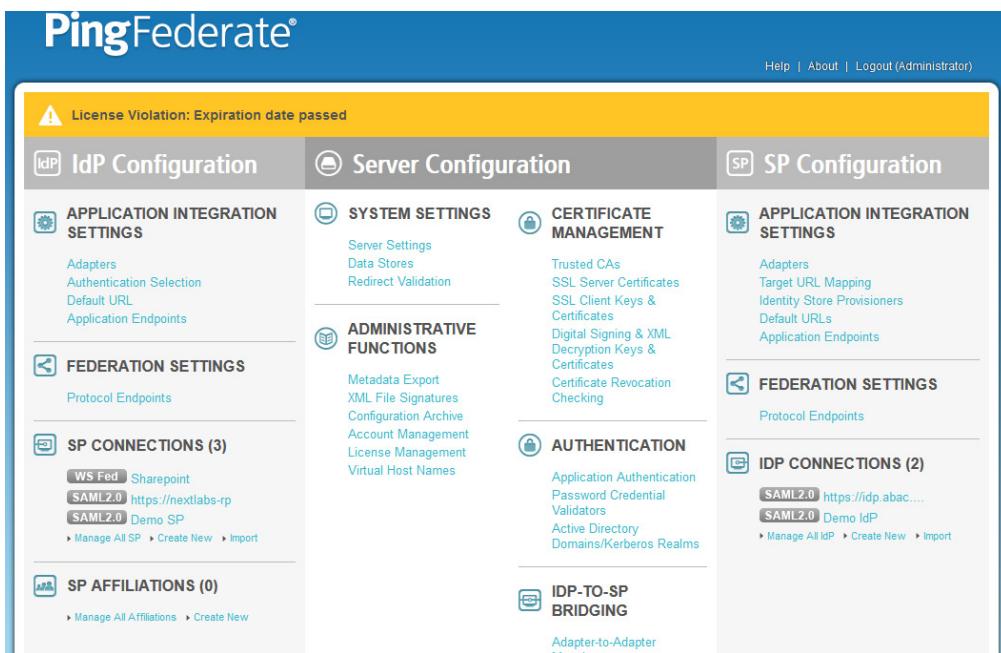
1777

- 1778 10. Copy the metatdata file to the server that hosts the PingFederate service for the relying party.

3.4 Configure PingFederate-RP Connection to the PingFederate-IdP

Follow the instructions in this section to configure a PingFederate connection from the relying party to the identity provider.

1. Logon to the server that hosts the PingFederate service for the relying party.
2. Launch your browser and go to: https://<DNS_NAME>:9999/pingfederate/app.
3. Replace DNS_NAME with the fully qualified name of the relying party's PingFederate server (e.g., <https://rp.abac.test:9999/pingfederate/app>). Logon to the PingFederate application using the credentials you configured in the previous installation section.



4. On the Main Menu under IDP CONNECTIONS, click **Create New**.
5. On the Connection Type screen, select **Browser SSO Profiles**.

SECOND DRAFT

As an SP, you are making a connection to a partner IdP. Select the type of connection needed for this IdP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), OAuth SAML Grant (for authenticating against the PingFederate Authorization Server), Inbound Provisioning (for integrating with SaaS partners) or all.

Browser SSO Profiles Protocol SAML 2.0

WS-Trust STS

OAuth SAML Grant

Inbound Provisioning

1790

1791 6. Click **Next**.

1792 7. On the Connection Options screen, make sure **Browser SSO** is selected.

Please select options that apply to this connection.

Browser SSO

JIT Provisioning

OAuth Attribute Mapping

Attribute Query

1793

1794 8. Click **Next**.

1795 9. On the Import Metadata screen, click **Browse** and select the metadata file that you exported
1796 from the Identity Provider's PingFederate server.

SECOND DRAFT

The screenshot shows the 'IdP Connection' configuration interface. The top navigation bar has tabs for 'Main' (selected), 'IdP Connection' (selected), 'Connection Type', 'Connection Options', 'Import Metadata' (with a star icon), 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. Below the tabs is a message: 'If you received a metadata file from a partner IdP describing this new connection, import the file here to populate many connection settings automatically.' A 'Browse...' button is shown next to a file path 'metadata idp.xml'.

1797

10. Click **Next**.

1798
1799
1800
1801

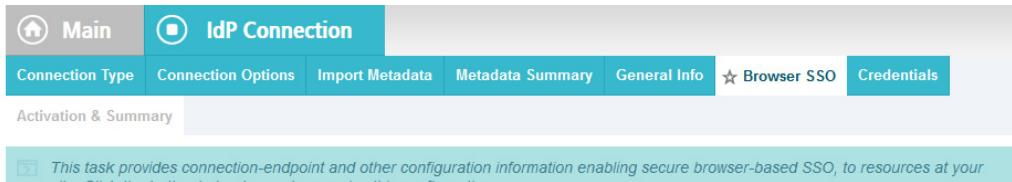
11. On the Metadata Summary screen, click **Next**. On the General Info screen, you should see some configuration information (e.g., Base URL) about the identity provider that was taken from the metadata file that you selected.

The screenshot shows the 'Metadata Summary' configuration interface. The top navigation bar has tabs for 'Main' (selected), 'IdP Connection' (selected), 'Connection Type', 'Connection Options', 'Import Metadata', 'Metadata Summary' (selected), 'General Info' (with a star icon), 'Browser SSO', and 'Credentials'. Below the tabs is a message: 'This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints.' The form fields include: 'Partner's Entity ID (Connection ID)' with value 'https://idp.abac.test:9031' and a 'Browse...' button; 'Connection Name' with value 'https://idp.abac.test:9031'; 'Virtual Server IDs' (empty input field); 'Base URL' with value 'https://idp.abac.test:9031'; 'Company' (empty input field); 'Contact Name' (empty input field); 'Contact Number' (empty input field); 'Contact Email' (empty input field); and 'Error Message:' (empty input field).

1802
1803

12. Click **Next**.

SECOND DRAFT



1804

1805 13. On the Browser SSO screen, click **Configure Browser SSO**.

1806 14. On the SAML Profiles screen, select **IdP-Initiated SSO** and **SP-Initiated SSO**.



1807

1808 15. Click **Next >**.

SECOND DRAFT

The screenshot shows a top navigation bar with tabs: Main, IdP Connection, Browser SSO, SAML Profiles, User-Session Creation (which is selected and highlighted in blue), Protocol Settings, and Summary. A status message below the tabs reads: "This task provides the configuration for creating user sessions to enable SSO access to resources at your site." The main content area is titled "User-Session Configuration" and contains the following table:

Identity Mapping	Not Configured
Attribute Contract	SAML SUBJECT
Adapter Instances	0
Connection Contract Mappings	0

At the bottom of the configuration section is a blue button labeled "Configure User-Session Creation".

1809

1810

16. On the User-Session Creation screen, click **Configure User-Session Creation**.

The screenshot shows a top navigation bar with tabs: Main, IdP Connection, Browser SSO, and User-Session Creation (selected). Below the tabs, there are two sub-tabs: Identity Mapping (selected) and Attribute Contract. A status message below the tabs reads: "Identity mapping is the process whereby users authenticated by the IdP are associated with user accounts local to the SP. PingFederate supplies two modes for identity mapping of disparate user accounts between different domains. Choose which of these two styles to use to associate the user with a specific local account." The main content area contains three radio button options:

- Account Mapping: The IdP is sending a set of attributes that may be used to dynamically map the user to a specific local account.
- Account Linking: The IdP is sending a unique name identifier (possibly opaque). An opaque identifier preserves user privacy in that it cannot be traced back to a user's identity at the IdP. The name identifier is used by this SP to create a persistent association between the user and a specific local account.
- The assertion includes attributes in addition to the unique name identifier.

1811

1812

17. On the Identity Mapping screen, click **Next >**.

SECOND DRAFT

The screenshot shows the 'Attribute Contract' screen. At the top, there are four tabs: 'Main', 'IdP Connection', 'Browser SSO', and 'User-Session Creation'. The 'User-Session Creation' tab is highlighted with a teal background. Below the tabs, there are four sub-tabs: 'Identity Mapping' (selected), 'Attribute Contract' (highlighted with a star icon), 'Target Session Mapping', and 'Summary'. A note below the sub-tabs states: 'An Attribute Contract is a set of user attributes that the IdP will send in the assertion.' The main content area is titled 'ATTRIBUTE CONTRACT' and contains a table with one row. The table has three columns: 'EXTEND THE CONTRACT' (with a dropdown menu), 'MASK VALUES IN LOG' (with a checkbox), and 'ACTION' (with an 'Add' button). At the bottom right of the screen are buttons for 'Save Draft', 'Cancel', '< Previous', and 'Next >'.

1813

- 1814 18. On the Attribute Contract screen, click **Next**.

The screenshot shows the 'Target Session Mapping' screen. At the top, there are four tabs: 'Main', 'IdP Connection', 'Browser SSO', and 'User-Session Creation'. The 'User-Session Creation' tab is highlighted with a teal background. Below the tabs, there are four sub-tabs: 'Identity Mapping' (selected), 'Attribute Contract' (highlighted with a star icon), 'Target Session Mapping' (highlighted with a star icon), and 'Summary'. A note below the sub-tabs states: 'PingFederate can create sessions to internal applications and/or identity management system using adapters, or create sessions to partner SPs using connection mapping contracts. A session will be created based on attributes sent in an assertion. Map an adapter instance for each target application on your system. Likewise, map a connection contract for each partner SP(s).' The main content area contains two tables. The first table has columns 'ADAPTER INSTANCE NAME', 'VIRTUAL SERVER IDS', and 'ACTION'. The second table has columns 'CONNECTION MAPPING CONTRACT NAME', 'VIRTUAL SERVER IDS', and 'ACTION'. At the bottom left are buttons for 'Map New Adapter Instance...' and 'Map New Connection Contract Mapping...'. At the bottom right are buttons for 'Save Draft', 'Cancel', '< Previous', and 'Next >'.

1815

- 1816 19. On the Target Session Mapping screen, click **Map New Connection Contract Mapping**.

SECOND DRAFT

The screenshot shows a navigation bar with tabs: Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping (which is selected), and Connection Mapping Contract. Below the navigation bar, there are tabs for Attribute Retrieval, Contract Fulfillment, Issuance Criteria, and Summary. A message box says "Select the connection mapping contract you would like to activate for incoming SAML messages from this partner." A dropdown menu labeled "CONNECTION MAPPING CONTRACT" with the option "- SELECT -" is visible. A link "Manage Connection Mapping Contracts..." is at the bottom.

1817

- 1818 20. On the Connection Mapping Contract screen, click **Manage Connection Mapping Contracts**.

The screenshot shows a navigation bar with tabs: Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping, and Manage Connection Mapping Contracts (which is selected). Below the navigation bar, there is a message box: "Connection Mapping Contracts allow IdP Connections to map directly to SP Connections using a shared contract. This allows PingFederate to act as a federation hub between IdP and SP partners." A table lists contracts with columns: CONTRACT NAME, CONTRACT ID, and ACTION. One row shows "SharePoint" and "2TSYiibHRp5qs2t". A link "Create New Contract..." is at the bottom.

1819

- 1820 21. On the Manage Contracts screen, click **Create New Contract**.

- 1821 22. On the Contract Info screen, enter the **Contract Name** (e.g., SharePoint 2013).

SECOND DRAFT

The screenshot shows a navigation bar with several tabs: Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping, Manage Connection Mapping Contracts, and Connection Mapping Contract. The Connection Mapping Contract tab is selected and highlighted in blue. Below the tabs, there are three sub-tabs: Contract Info (selected), Contract Attributes, and Summary. A descriptive message at the top says, "Define the name of the contract. The ID is automatically generated by PingFederate." Below this, a field labeled "Contract Name" contains the value "Sharepoint 2013". At the bottom right of the screen are "Cancel" and "Next >" buttons.

1822

1823 23. Click **Next**.

The screenshot shows the same navigation bar and tabs as the previous screenshot. The Connection Attributes tab is selected. A descriptive message at the top says, "Define the set of attributes that the IdP connection will send to the SP connection." Below this, there is a section titled "ATTRIBUTE CONTRACT" with a table. The table has two columns: "EXTEND THE CONTRACT" and "ACTION". Under "EXTEND THE CONTRACT", there is a dropdown menu with an "Add" button next to it. At the bottom right of the screen are "Cancel", "< Previous", and "Next >" buttons.

1824

1825 24. Click **Next**.

Contract Info Contract Attributes ★ Summary

Connection mapping contract summary information.

Connection Mapping Contract

CONTRACT INFO

Contract Name	Sharepoint 2013
---------------	-----------------

CONTRACT ATTRIBUTES

Attribute	SAML_SUBJECT
-----------	--------------

Cancel < Previous Done

1826

1827

25. On the Summary screen, click **Done**.

★ Manage Contracts

Connection Mapping Contracts allow IdP Connections to map directly to SP Connections using a shared contract. This allows PingFederate to act as a federation hub between IdP and SP partners.

CONTRACT NAME	CONTRACT ID	ACTION
SharePoint	2TSYliBHRp5iqs2t	Delete (Check Usage)
Sharepoint 2013	pHDPDzxOTReXcnFp	Delete

Create New Contract...

Cancel Save

1828

1829

26. On the Manage Contracts screen, you should see the new contract listed. Click **Save**.

1830

1831

27. On the Connection Mapping Contract screen, for the CONNECTION MAPPING CONTRACT field select the name of the new contract that was created (e.g., **SharePoint 2013**).

SECOND DRAFT

The screenshot shows a navigation bar with five tabs: Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping (which is highlighted in blue), and Connection Mapping Contract. Below the tabs, there are five sub-tabs: Connection Mapping Contract, Attribute Retrieval, Contract Fulfillment, Issuance Criteria, and Summary. A message box at the top says "Select the connection mapping contract you would like to activate for incoming SAML messages from this partner." A dropdown menu labeled "CONNECTION MAPPING CONTRACT" shows "Sharepoint 2013". A section titled "CONTRACT ATTRIBUTES" contains a "subject" field. At the bottom is a button labeled "Manage Connection Mapping Contracts...".

1832

- 1833 28. Click **Next**. On the Attribute Retrieval screen, select **Use only the attributes available in the SSO Assertion**.
- 1834

The screenshot shows a navigation bar with the same tabs as the previous screen. Below the tabs, there are five sub-tabs: Connection Mapping Contract, Attribute Retrieval (which is highlighted in blue), Contract Fulfillment, Issuance Criteria, and Summary. A message box at the top says "You can fulfill the Connection Mapping Contract by using only the attributes from the SAML assertion or by using these attributes to look up additional information from a local data store." A section titled "CONNECTION MAPPING CONTRACT" contains a "subject" field and two radio buttons: "Use the SSO Assertion to look up additional information" (unchecked) and "Use only the attributes available in the SSO Assertion" (checked). At the bottom are "Cancel", "< Previous", and "Next >" buttons.

1835

- 1836 29. Click **Next**. On the Contract Fulfillment screen, for the SOURCE field select **Assertion**. For the
1837 VALUE field, select **SAML_SUBJECT**.

SECOND DRAFT

The screenshot shows the 'Connection Contract Mapping' screen. At the top, there are tabs for Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping, Connection Mapping Contract, Attribute Retrieval, Contract Fulfillment, Issuance Criteria, and Summary. The Connection Contract Mapping tab is selected. Below the tabs, a message says: "You can fulfill your Connection Mapping Contract with values from the assertion, dynamic text, expressions, or from a data-store lookup." A table lists a single mapping rule:

CONNECTION MAPPING CONTRACT	SOURCE	VALUE	ACTIONS
subject	Assertion	SAML_SUBJECT	None available

1838

1839 30. Click **Next**.

The screenshot shows the 'Issuance Criteria' screen. At the top, there are tabs for Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping, Connection Mapping Contract, Attribute Retrieval, Contract Fulfillment, Issuance Criteria, and Summary. The Issuance Criteria tab is selected. Below the tabs, a message says: "PingFederate can evaluate various criteria to determine whether to continue the SSO transaction. Use this optional screen to configure the criteria for use with this conditional authorization." A table allows defining issuance criteria:

SOURCE	ATTRIBUTE NAME	CONDITION	VALUE	ERROR RESULT	ACTION
- SELECT -	- SELECT -	- SELECT -	- SELECT -	- SELECT -	Add

[Show Advanced Criteria](#)

1840

1841 31. On the Issuance Criteria screen, click **Next**.

The screenshot shows the 'Connection Contract Mapping Summary' screen. At the top, there are tabs for Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping, Connection Mapping Contract, Attribute Retrieval, Contract Fulfillment, Issuance Criteria, and Summary. The Summary tab is selected. Below the tabs, a message says: "Connection Contract Mapping Summary". The screen displays the following configuration details:

- CONNECTION MAPPING CONTRACT**: Selected contract is Sharepoint 2013.
- ATTRIBUTE RETRIEVAL**: Attribute location is set to "Use only the attributes available in the SSO Assertion".
- CONTRACT FULFILLMENT**: subject is mapped to SAML_SUBJECT (Assertion).
- ISSUANCE CRITERIA**: Criterion is listed as (None).

1842

1843 32. On the Summary screen, click **Done**.

SECOND DRAFT

- 1844 33. On the Target Session Mapping screen, you should see new contract (e.g., **SharePoint 2013**)
1845 listed under the **CONNECTION MAPPING CONTRACT NAME** field.

The screenshot shows the 'Target Session Mapping' tab selected in the navigation bar. A note at the top states: 'PingFederate can create sessions to internal applications and/or identity management system using adapters, or create sessions to partner SPs using connection mapping contracts. A session will be created based on attributes sent in an assertion. Map an adapter instance for each target application on your system. Likewise, map a connection contract for each partner SP(s).'. Below this, there are two tables:

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		Delete

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		

At the bottom are buttons for 'Map New Adapter Instance...' and 'Map New Connection Contract Mapping...'. Navigation buttons 'Cancel', '< Previous', and 'Next >' are at the very bottom right.

- 1846
1847 34. Click **Next**.

The screenshot shows the 'User-Session Creation' tab selected in the navigation bar. A note at the top says: 'Summary information for Session Creation configuration. Click a heading link to edit a configuration setting.' Below this is a large configuration area with several sections:

- IDENTITY MAPPING:** Enable Account Mapping (true)
- ATTRIBUTE CONTRACT:** Attribute (SAML_SUBJECT)
- TARGET SESSION MAPPING:** Connection mapping contract name (Sharepoint 2013)
- CONNECTION MAPPING CONTRACT:** Selected contract (Sharepoint 2013)
- ATTRIBUTE RETRIEVAL:** Attribute location (Use only the attributes available in the SSO Assertion)
- CONTRACT FULFILLMENT:** subject (SAML_SUBJECT (Assertion))
- ISSUANCE CRITERIA:** Criterion ((None))

Navigation buttons 'Cancel', '< Previous', and 'Done' are at the bottom right.

- 1848
1849 35. Click **Done**.

SECOND DRAFT

The screenshot shows a top navigation bar with three tabs: Main (selected), IdP Connection, and Browser SSO. Below the tabs, there are four sub-tabs: SAML Profiles (selected), User-Session Creation, Protocol Settings, and Summary. A status message at the top says, "This task provides the configuration for creating user sessions to enable SSO access to resources at your site." The main content area is titled "User-Session Configuration" and contains the following table:

Identity Mapping	Not Configured
Attribute Contract	SAML_SUBJECT
Adapter Instances	0
Connection Contract Mappings	1

At the bottom of the screen is a blue button labeled "Configure User-Session Creation".

1850

1851

36. On the User-Session Creation screen, click **Next**.

The screenshot shows a top navigation bar with three tabs: Main (selected), IdP Connection, and Browser SSO. Below the tabs, there are four sub-tabs: SAML Profiles, User-Session Creation (selected), Protocol Settings, and Summary. A status message at the top says, "This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration." The main content area is titled "Protocol Settings Configuration" and contains the following table:

Outbound SSO Bindings	POST, Redirect
Inbound Bindings	POST, Redirect, Artifact, SOAP
Signature Policy	SAML-standard, Authn requests over POST & Redirect
Encryption Policy	No Encryption

At the bottom of the screen is a blue button labeled "Configure Protocol Settings".

1852

1853
1854

37. On the Protocol Settings screen, click **Configure Protocol Settings**. This will bring up a sequence of sub-screens.

SECOND DRAFT

The screenshot shows the 'Protocol Settings' tab selected in the top navigation bar. Under the 'SSO Service URLs' section, there is a table with three columns: 'BINDING', 'ENDPOINT URL', and 'ACTION'. The first row has 'POST' in 'BINDING', '/idp/SSO.saml2' in 'ENDPOINT URL', and 'Edit / Delete' in 'ACTION'. The second row has 'Redirect' in 'BINDING', '/idp/SSO.saml2' in 'ENDPOINT URL', and 'Edit / Delete' in 'ACTION'. Below the table is a dropdown menu labeled '- SELECT -' and an 'Add' button.

BINDING	ENDPOINT URL	ACTION
POST	/idp/SSO.saml2	Edit / Delete
Redirect	/idp/SSO.saml2	Edit / Delete

1855

38. On the SSO Service URLs screen, click **Next**.

1856

39. On the Allowable SAML Bindings screen, select **POST** and select **Redirect**.

The screenshot shows the 'Protocol Settings' tab selected in the top navigation bar. Under the 'Allowable SAML Bindings' section, there is a list of options with checkboxes. The 'POST' and 'Redirect' checkboxes are checked, while 'Artifact' and 'SOAP' are unchecked.

- Artifact
- POST
- Redirect
- SOAP

1858

40. Click **Next**.

SECOND DRAFT

The screenshot shows a top navigation bar with tabs: Main, IdP Connection, Browser SSO, and Protocol Settings. The Protocol Settings tab is active. Below the tabs, there are several sub-tabs: SSO Service URLs, Allowable SAML Bindings, Default Target URL (which is highlighted with a star), Signature Policy, Encryption Policy, and Summary. A note below the tabs states: " Optionally, you can specify a default target URL for this IdP connection. Entering a URL in the Default Target URL field overrides the SP Default URL SSO setting." A text input field labeled "Default Target URL" is present. At the bottom right are buttons for "Cancel", "< Previous", and "Next >".

1860

41. On the Default Target URL screen, click **Next**.
42. On the Signature Policy screen, make sure that the following are selected:
 - a. **Specify additional signature requirements** and
 - b. **Sign AuthN requests sent over POST and Redirect bindings**

The screenshot shows a top navigation bar with tabs: Main, IdP Connection, Browser SSO, and Protocol Settings. The Protocol Settings tab is active. Below the tabs, there are several sub-tabs: SSO Service URLs, Allowable SAML Bindings, Default Target URL (which is highlighted with a star), Signature Policy (which is also highlighted with a star), Encryption Policy, and Summary. A note below the tabs states: " Additional guarantees of authenticity may be agreed upon between you and your partner. For SP-initiated SSO, you can choose to sign authentication requests sent via the POST or redirect bindings. You can also choose to require signed assertions, regardless of the binding used." A section titled "Specify how message authenticity and integrity is ensured:" contains the following options:

- Use SAML-standard signature requirements
- Specify additional signature requirements
 - Sign AuthN requests sent over POST and Redirect bindings
 - Require signed SAML Assertions (rather than signed Responses — Assertions are contained inside SAML Responses)

1865

43. Click **Next**. On the Encryption Policy screen, select
 - a. **Allow encrypted SAML Assertions and SLO messages** and
 - b. **The entire assertion**

SECOND DRAFT

The screenshot shows the 'Protocol Settings' tab selected in a navigation bar. Below it is a sub-navigation bar with tabs: SSO Service URLs, Allowable SAML Bindings, Default Target URL, Signature Policy, Encryption Policy, and Summary. A note at the top says: 'Additional guarantees of message level privacy may be used between you and your partner through the use of XML encryption. Specify an encryption policy for the exchange of SAML messages.' Below this, there are several radio button options for encryption: 'None' (selected), 'Allow encrypted SAML Assertions and SLO messages' (selected), 'The entire assertion' (unchecked), 'SAML_SUBJECT (Name Identifier)' (unchecked), and 'One or more attributes' (unchecked). At the bottom right are 'Cancel', '< Previous', and 'Next >' buttons.

1869

1870 44. Click **Next**.

The screenshot shows the 'Summary' tab selected in a navigation bar. Below it is a sub-navigation bar with tabs: SSO Service URLs, Allowable SAML Bindings, Default Target URL, Signature Policy, Encryption Policy, and Summary. A note at the top says: 'Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.' Below this, there are several sections with configuration details:

- Protocol Settings**
- SSO SERVICE URLs**

Endpoint	URL: /idp/SSO.saml2 (POST)
Endpoint	URL: /idp/SSO.saml2 (Redirect)
- ALLOWABLE SAML BINDINGS**

Artifact	false
POST	true
Redirect	true
SOAP	false
- DEFAULT TARGET URL**
- SIGNATURE POLICY**

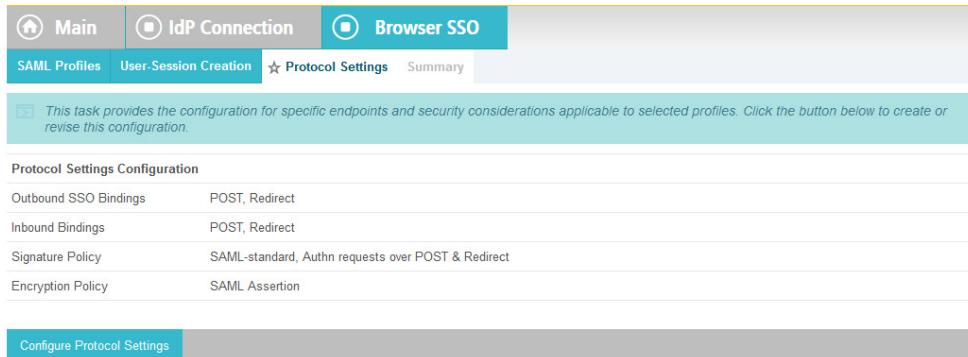
Sign AuthN requests over POST and Redirect	true
Require digitally signed SAML Assertion	false
- ENCRYPTION POLICY**

Encrypt Entire Assertion	true
Encrypt Name Identifier	false
Encrypt One or More Attributes	false

1871

1872 45. On the Summary screen, click **Done**.

SECOND DRAFT



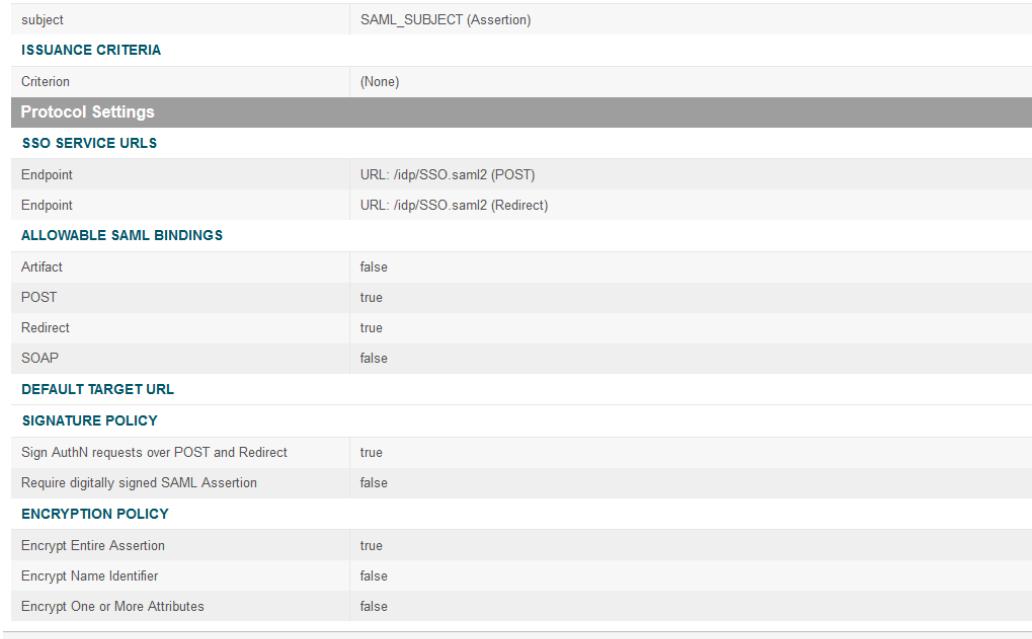
This screenshot shows the 'Protocol Settings Configuration' screen. At the top, there are three tabs: 'Main' (selected), 'IdP Connection', and 'Browser SSO'. Below the tabs, there are four navigation links: 'SAML Profiles', 'User-Session Creation', 'Protocol Settings' (selected), and 'Summary'. A note below the tabs states: 'This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.' The main content area displays several protocol settings:

Outbound SSO Bindings	POST, Redirect
Inbound Bindings	POST, Redirect
Signature Policy	SAML-standard, Authn requests over POST & Redirect
Encryption Policy	SAML Assertion

At the bottom left is a 'Configure Protocol Settings' button.

1873

1874 46. On the Protocol Settings screen, click **Next**.



This screenshot shows the 'Protocol Settings' screen with various configuration sections:

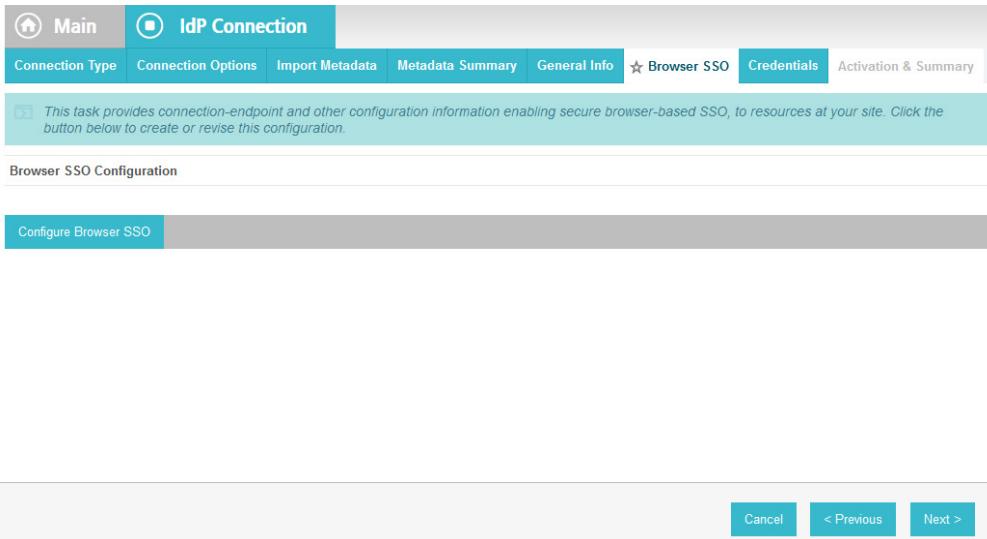
- ISSUANCE CRITERIA:** Criterion: (None)
- Protocol Settings:** This section is highlighted with a dark grey bar.
- SSO SERVICE URLs:** Endpoint: URL: /idp/SSO.saml2 (POST); Endpoint: URL: /idp/SSO.saml2 (Redirect).
- ALLOWABLE SAML BINDINGS:** Artifact: false; POST: true; Redirect: true; SOAP: false.
- DEFAULT TARGET URL:** (No visible configuration details shown)
- SIGNATURE POLICY:** Sign AuthN requests over POST and Redirect: true; Require digitally signed SAML Assertion: false.
- ENCRYPTION POLICY:** Encrypt Entire Assertion: true; Encrypt Name Identifier: false; Encrypt One or More Attributes: false.

At the bottom right are 'Cancel', '< Previous', and 'Next >' buttons.

1875

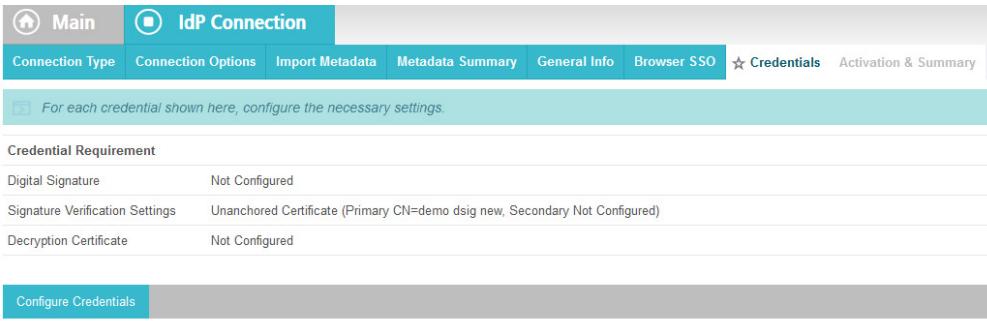
1876 47. On the Summary screen, click **Done**.

SECOND DRAFT



1877

- 1878 48. On the Browser SSO screen, click **Next**.



1879

- 1880 49. On the Credentials screen, click **Configure Credentials**.

- 1881 50. On the Digital Signature Settings screen, select

- 1882 a. **Signing Certificate for SAML messages** and
1883 b. **Signing Algorithm**

SECOND DRAFT

The screenshot shows the 'Digital Signature Settings' section of a configuration interface. At the top, there are tabs for 'Main', 'IdP Connection', 'Credentials', 'Digital Signature Settings' (which is selected), 'Signature Verification Settings', 'Select XML Decryption Key', and 'Summary'. A note at the top says: 'You may need to digitally sign SAML messages to protect against tampering. Please select a key/certificate to use from the list below.' Below this, there are two sections: 'Signing Certificate' (set to '01:30:DB:8C:25:AB (cn=demo dsig new) *') and 'Include the certificate in the signature <KeyInfo> element.' (unchecked). Another section for 'Signing Algorithm' is set to 'RSA SHA256'. At the bottom is a 'Manage Certificates...' button.

1884

1885 51. Click **Next**.

The screenshot shows the 'Signature Verification Settings' section of a configuration interface. At the top, there are tabs for 'Main', 'IdP Connection', 'Credentials', 'Digital Signature Settings' (disabled), 'Signature Verification Settings' (selected), 'Select XML Decryption Key', and 'Summary'. A note at the top says: 'Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.' Below this is a 'Manage Signature Verification Settings...' button.

1886

1887 52. On the Signature Verification Settings screen, click **Manage Signature Verification Settings**.

SECOND DRAFT

The screenshot shows the 'Signature Verification' tab selected in a navigation bar. Below it, a sub-menu bar includes 'Trust Model', 'Signature Verification Certificate', and 'Summary'. A note at the top says: 'Select the Trust Model to be used for verifying digital signatures received from this partner.' Two radio button options are shown: 'Anchored' (selected) and 'Unanchored'. At the bottom right are 'Cancel' and 'Next >' buttons.

1888

1889 53. On the Trust Model screen, click **Next**.

1890 54. On the Signature Verification Certificate screen, select the certificate to verify digital signatures.

The screenshot shows the 'Signature Verification' tab selected in a navigation bar. Below it, a sub-menu bar includes 'Trust Model', 'Signature Verification Certificate' (selected), and 'Summary'. A note at the top says: 'Please select the certificate(s) to use when verifying these digital signatures. When multiple certificates are chosen, each certificate is tried from the top of the list down until the signature is verified.' Under 'Primary', a dropdown menu is open with the value '01:30:DB:8C:25:AB (cn=demo dsig new)' and a required asterisk (*). Under 'Secondary', a dropdown menu is open with the value '- SELECT -'. At the bottom left is a 'Manage Certificates...' button, and at the bottom right are 'Cancel', '< Previous', and 'Next >' buttons.

1891

1892 55. Click **Next**.

SECOND DRAFT

The screenshot shows the 'Signature Verification' configuration page. The 'Signature Verification' tab is selected. Under 'SIGNATURE VERIFICATION CERTIFICATE', the 'Selected Certificate' dropdown is set to 'CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US'. The 'Trust Model' dropdown is set to 'Unanchored'.

- 1893
- 1894 56. On the Summary screen, click **Done**.
- 1895 57. On the Signature Verification Settings screen, click **Next**.
- 1896 58. On the Select XML Decryption Key screen, select the certificate associated with the private key
1897 that will decrypt messages from the identity provider.

The screenshot shows the 'Select XML Decryption Key' screen. The certificate '01:4C:09:35:30:19 (cn=demo-sp-enc)' is selected. A note at the top states: 'Please select the certificate that corresponds to the private key that you will use to decrypt message content sent to you from your partner. Only RSA keys can be used for XML encryption.'

- 1898
- 1899 59. Click **Next**.

SECOND DRAFT

The screenshot shows the 'Summary' tab selected in a navigation bar. Below it, a message says 'Summary information for your Credentials configuration. Click a heading link to edit a configuration setting.' The main content area is titled 'Credentials' and contains three sections: 'DIGITAL SIGNATURE SETTINGS', 'Signature Verification', and 'SELECT XML DECRYPTION KEY'. Each section has a table with configuration details. At the bottom right are buttons for 'Cancel', '< Previous', and 'Done'.

Selected Certificate	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256

Trust Model	Unanchored
-------------	------------

Selected Certificate	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
----------------------	--

Selected Decryption Certificate	CN=demo-sp-enc, O=NCCoE, C=US
---------------------------------	-------------------------------

Cancel < Previous Done

1900

- 1901 60. On the Summary screen, click **Done**.

The screenshot shows the 'Credentials' tab selected in a navigation bar. Below it, a message says 'For each credential shown here, configure the necessary settings.' The main content area lists 'Credential Requirement' with three items: 'Digital Signature' (CN=demo dsig new), 'Signature Verification Settings' (Unanchored Certificate (Primary CN=demo dsig new, Secondary Not Configured)), and 'Decryption Certificate' (CN=demo-sp-enc). At the bottom left is a 'Configure Credentials' button, and at the bottom right are buttons for 'Cancel', '< Previous', and 'Next >'.

Digital Signature	CN=demo dsig new
Signature Verification Settings	Unanchored Certificate (Primary CN=demo dsig new, Secondary Not Configured)
Decryption Certificate	CN=demo-sp-enc

Cancel < Previous Next >

1902

- 1903 61. On the Credentials screen, click **Next**.

- 1904 62. On the Activation and Summary screen, select **Active** for the **Connection Status** field.

The screenshot shows the 'IdP Connection' configuration page. The 'Activation & Summary' tab is active. Key visible information includes:

- Connection Status:** Active (radio button selected)
- SSO Application Endpoint:** https://rp.abac.test:9031/sp/startSSO.ping?PartnerIdpId=https://idp.abac.test:9031
- IdP Connection** section:
 - CONNECTION TYPE:**

Connection Role	IdP
Browser SSO Profiles	true
Protocol	SAML 2.0
WS-Trust STS	false
OAuth SAML Grant	false
Inbound Provisioning	false
 - CONNECTION OPTIONS:**

Browser SSO	true
JIT Provisioning	false
OAuth Attribute Mapping	false
Attribute Query	false

1905

1906 63. Copy the relying party's SSO Application Endpoint URL (e.g.,
 1907 *https://rp.abac.test:9031/sp/startSSO.ping?PartnerIdpId=https://idp.abac.test:9031*) to the
 1908 clipboard and save it to a text file, because this URL will be used in the Functional Test section.

1909

64. Click **Save** to save the configuration.

1910

3.5 Functional Test of All Configurations for Section 3

1911

This section provides instructions to perform an integrated test all of the configurations in Section 3.

1912

1. Using the browser and PingFederate, a user will logon at the identity provider, and then get redirected to the relying party.

1914

Note: This test is similar to the test in [Section 2](#), except this time the relying party has a destination endpoint connection that was configured in Section 3, so the response code from the relying party's Federation server (e.g., rp.abac.test), should be an HTTP 200 status code.

1917

2. Launch your browser and navigate to the relying party's SSO Application Endpoint URL identified in the previous section (e.g.,
 1919 *https://rp.abac.test:9031/sp/startSSO.ping?PartnerIdpId=https://idp.abac.test:9031*).

1920

3. Launch the SAML tracer as in [Section 2](#) and minimize the tracer window.

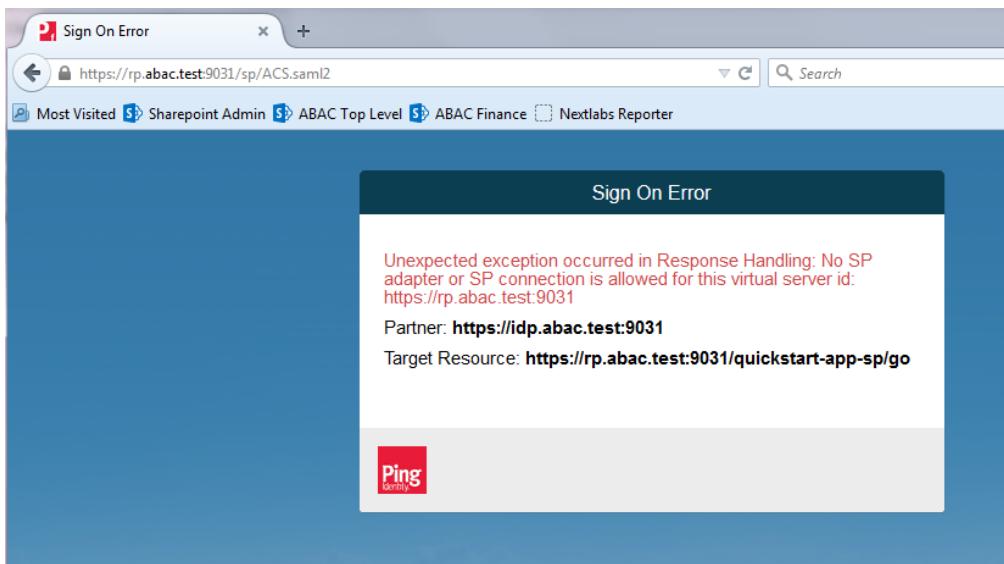
1921

Expected Result: You should see the PingFederate Sign On screen.

1922

- 1923 4. Enter the Username and Password of the account created in [Section 2](#) (e.g., “lsmith”) and click
1924 Sign On.
- 1925 5. When the RSA Adaptive Authentication screen comes up, enter the SMS text validation code.

1926 **Expected Result:** You should see the browser redirect to the relying party’s Federation Server
1927 (e.g., rp.abac.test) and an error message similar to the message in the following screenshot.



1928

- 1929 6. Return to the SAML tracer window.
1930 7. Scroll to the bottom of the list of message in the upper pane.
1931 8. Click on the last message (e.g., POST <https://rp.abac.test:9031/sp/ACS.saml2>) that has a SAML icon associated with it. This will show the details of the POST message.

```

POST https://rp.abac.test:9031/sp/ACS.saml2 HTTP/1.1
Host: rp.abac.test:9031
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://idp.abac.test:9031/idp/QtTk/resumeSAML20/idp/SSO.ping
Cookie: FF=20csp64v7QdVQ3D9C
X-Client-IP: 192.168.1.30729 (.NET CLR 4.0.30729; .NET4.0E)
Content-Type: application/x-www-form-urlencoded
Content-Length: 5319
Content-Length: 2263

HTTP/1.1 200 OK
Date: Mon, 20 Jul 2015 19:54:37 GMT
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache, no-store
Pragma: no-cache
max-age: 0
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 2263

```

1933

1934 **Expected Result:** In the details page at the bottom, on the **http** tab, you should see that the
 1935 browser sent a POST message to the relying party's PingFederate server (e.g., rp.abac.test). The
 1936 HTTP response status code (identified on the line that begins with "HTTP") should be a 200 OK
 1937 code.

1938 **4 Installing and Configuring Microsoft SharePoint Server and** 1939 **Related Components**

1940 **4.1 Introduction**

1941 In previous sections of this How-To Guide, we installed several products to establish RP and IdP
 1942 environments, their components, and the federation between them ([Section 2](#) and [Section 3](#)).

1943 In this section of the How-To Guide we will illustrate how to install IIS (Internet Information Services 8),
 1944 Microsoft SQL Server 2012, and Microsoft SharePoint Server 2013. Then, within SharePoint we will
 1945 illustrate how to create a web application, configure the web application to run SSL, create a site
 1946 collection, and create sub-sites.

1947 In our build, we used ABAC policies and policy enforcement to protect RP resources like SharePoint sites
 1948 and documents with the help of NextLabs products installed in subsequent How-To sections ([Section 7](#)
 1949 and [Section 8](#)).

1950 **4.1.1 Components Used in this How-To Guide**

- 1951 1. Internet Information Services (IIS) Manager - extensible web server created by Microsoft
 1952 (formerly Internet Information Server) and is pre-installed in most Windows editions though is
 1953 not active by default.
- 1954 2. Microsoft SharePoint 2013 - Microsoft SharePoint is a web-based application within the
 1955 Windows operating environment. Commonly, SharePoint is deployed as a document
 1956 management system for intranet, extranet, or cloud repository purposes. SharePoint natively
 1957 uses an RBAC authorization environment, but it also supports the use of attributes within the
 1958 user transaction request, a capability Microsoft refers to as being "claims aware." SharePoint
 1959 also allows for tagging data within its repository, which can be leveraged as object attributes.
- 1960 Microsoft SQL Server 2012 - relational database management system developed by Microsoft. As a
 1961 database server, it is a software product with the primary function of storing and retrieving data.

1962 4.1.2 Required or Recommended Files, Hardware, and Software

Component	Required Files	Required Other Software	Minimum Hardware Requirements	Recommended Hardware	Recommended or Minimum Operating System	Operating System or Other Software Used in this Build
Internet Information Services (IIS) 8	Built-in component in Windows Server 2012 operating system (inactive by default) – Windows Server 2012 ISO	N/A	For the Windows 2012 Server OS: 512 MB RAM, 1.4 GHz 64-bit CPU, 32 GB hard disk; Gigabit Ethernet adapter	For the Windows 2012 Server OS: 800+ MB RAM, >1.4 GHz 64-bit CPU, >32 GB hard disk	Windows Server 2012 R2 Standard 64-bit	Windows Server 2012 R2 Standard 64-bit
Microsoft SharePoint Server 2013	SharePoint Server 2013 installation setup file or DVD	Microsoft SQL Server 2012; Microsoft SQL Server Management Studio; IIS 7.0 or 8.0 (Web Server Role, 8.0 required for Windows Server 2012)	12 GB RAM, 4 core, 64 bit CPU, 80 GB hard disk space for system drive	8+ GB RAM, 4+core 64-bit CPU, >80 GB hard disk	The 64-bit edition of Windows Server 2008 R2 Service Pack 1 (SP1) Standard, Enterprise, or Datacenter or the 64-bit edition of Windows Server 2012 Standard or Datacenter	Windows Server 2012 R2 Standard 64-bit
Microsoft SQL Server 2012	SQL Server 2012 setup file or DVD	.NET 4.0 Framework (SQL Server installs .NET 4.0 during the feature installation step.)	1GB RAM, 1.4GHz CPU, 6 GB of hard-disk space	4 GB RAM (should be increased as database size increases to ensure optimal performance), >2.0 GHz CPU, 6 GH of hard-disk space	Windows Server 2008 R2 or Windows Server 2012, Windows 8.1, Windows 8, Windows 7 SP1, Windows Vista SP2	Windows Server 2012 R2 Standard 64-bit

1963

1964 **4.2 Installation of Required Components**

1965 **4.2.1 Installing SQL Server 2012**

1966 On the server where SQL Server 2012 is going to be installed, follow the steps from this link to install
1967 SQL Server 2012: [https://technet.microsoft.com/en-us/library/ms143219\(v=sql.110\).aspx](https://technet.microsoft.com/en-us/library/ms143219(v=sql.110).aspx)

1968 Note: in our build, this SQL Server instance is leveraged by SharePoint Server 2013 and by the NextLabs
1969 ABAC policy definition, deployment, and enforcement components. Two of these NextLabs components
1970 are also installed on the same server as SQL Server 2012 ([Section 7](#)). In our build, we call this server
1971 SQLServer.

1972 It is generally recommended by Microsoft regarding SharePoint Server and NextLabs regarding Control
1973 Center that the SQL Server be installed on a separate, dedicated server, which is why we chose that
1974 deployment in our build.

1975 **4.2.2 Installing IIS 8.0 on the SharePoint Server**

1976 On the separate server where SharePoint Server 2013 is going to be installed, follow the steps from this
1977 link to install IIS 8.0 (if not already installed; required for SharePoint Server 2013):
1978 <http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012>

1979 Note: in our build, we call this the SharePoint Server.

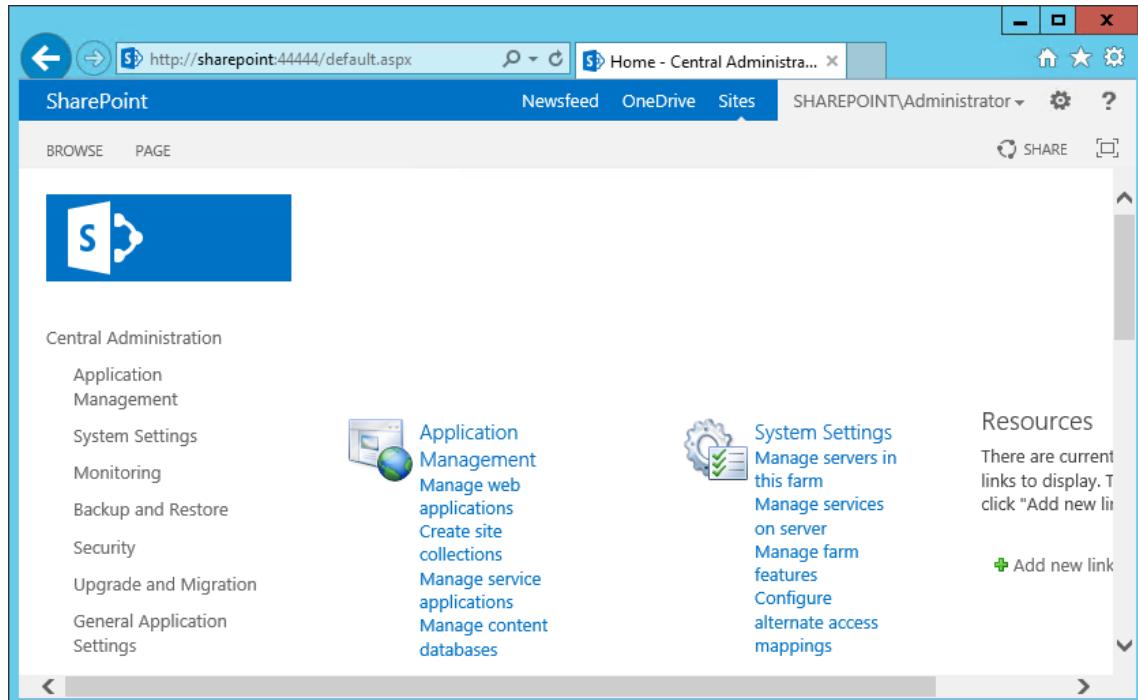
1980 **4.2.3 Installing Microsoft SharePoint Server 2013**

1981 On the separate server where SharePoint Server 2013 is going to be installed, follow the steps from this
1982 link to install SharePoint Server 2013:
1983 <http://social.technet.microsoft.com/wiki/contents/articles/14209.sharepoint-2013-installation-step-by-step.aspx>

1985 Note: in our build, we call this the SharePoint Server (same as step 2.2).

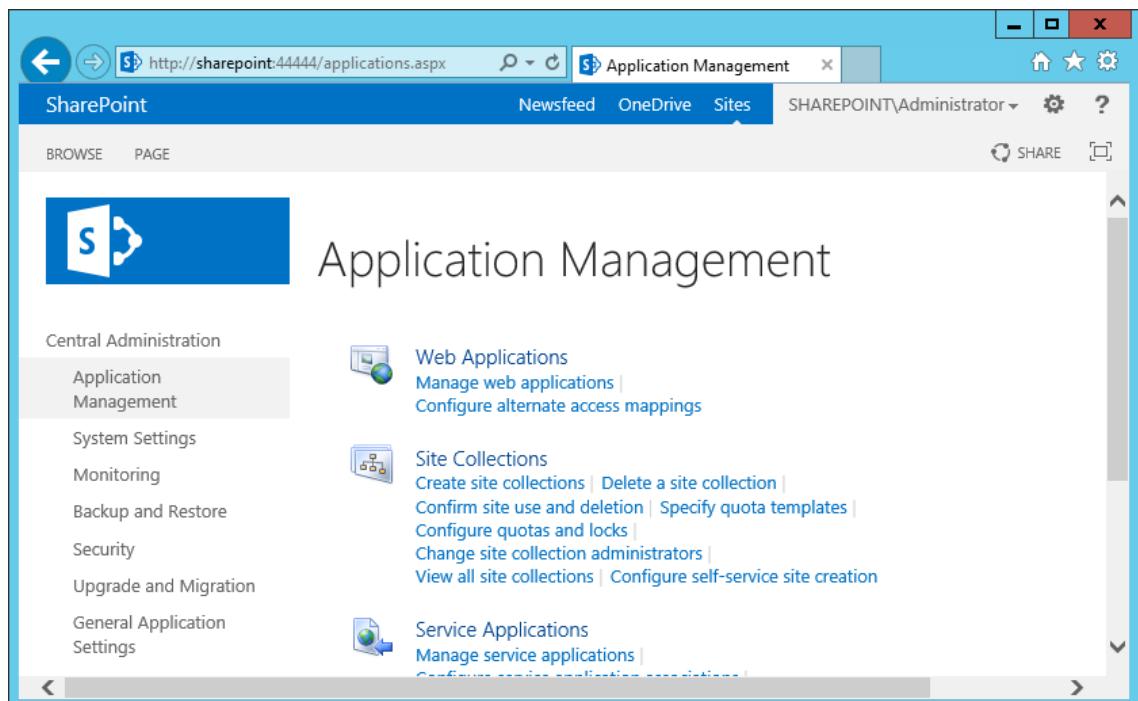
1986 **4.3 Creating the Web Application (IIS site) in SharePoint**

- 1987 1. On the SharePoint Server, open a web browser.
- 1988 2. In the URL address bar of the browser, enter the address for Central Administration and click
1989 Enter or Go: http://sharepoint:44444/default.aspx
- 1990 3. From the Central Administration page, click on **Application Management**.



1991

- 1992 4. On the Application Management Page, under the Web Applications section, click on **Manage web applications**.
- 1993



1994

- 1995 5. From the left-most end of the Web Applications ribbon menu click on **New**.

1996

The screenshot shows the SharePoint Web Applications Management interface. At the top, there are links for Newsfeed, OneDrive, and Sites. Below that is a ribbon with BROWSE and WEB APPLICATIONS tabs. Under the WEB APPLICATIONS tab, there are several icons for actions like New, Extend, Delete, Contribute, General Settings, Manage Features, Managed Paths, Service Connections, Authentication Providers, Self-Service Site Creation, Blocked File Types, User Permissions, Web Part Security, and User Policy.

1997

6. In the Create New Web Application window that automatically opens, in the IIS Web Site section, do the following steps to choose the web application's basic IIS configuration:

1999

a. Leave the radio button for **Create a new IIS web site** chosen (default).

2000

b. Leave the default **Name** or change the **Name** to something more memorable to you.

2001

c. Leave the default **Port** displayed or change the **Port** number to one that makes sense for your environment.

2002

Create New Web Application

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

Use an existing IIS web site
Default Web Site

Create a new IIS web site
Name:

Port:

Host Header:

If you select an existing IIS web site, that web site must exist on all servers in the farm and have the same name, or this action will not succeed.

If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.

2003

- d. Leave the **Host Header** blank and keep the default **Path**.

2004

Host Header:

Path:

2005

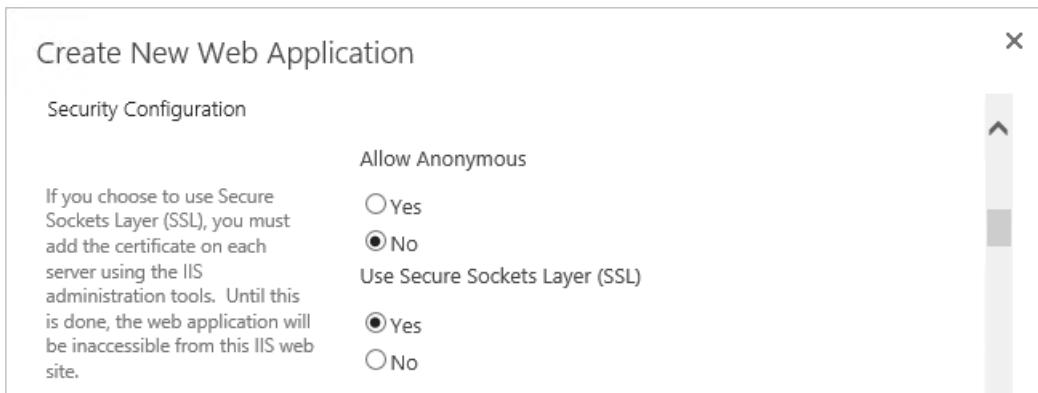
If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.

SECOND DRAFT

2006 7. Further down in the Create New Web Application window, in the Security Configuration section, do the following steps to configure the web application to run SSL,

2007 a. Under **Allow Anonymous** leave the **No** radio button chosen (default).

2008 b. Under **Use Secure Sockets Layer (SSL)**, click **Yes**.

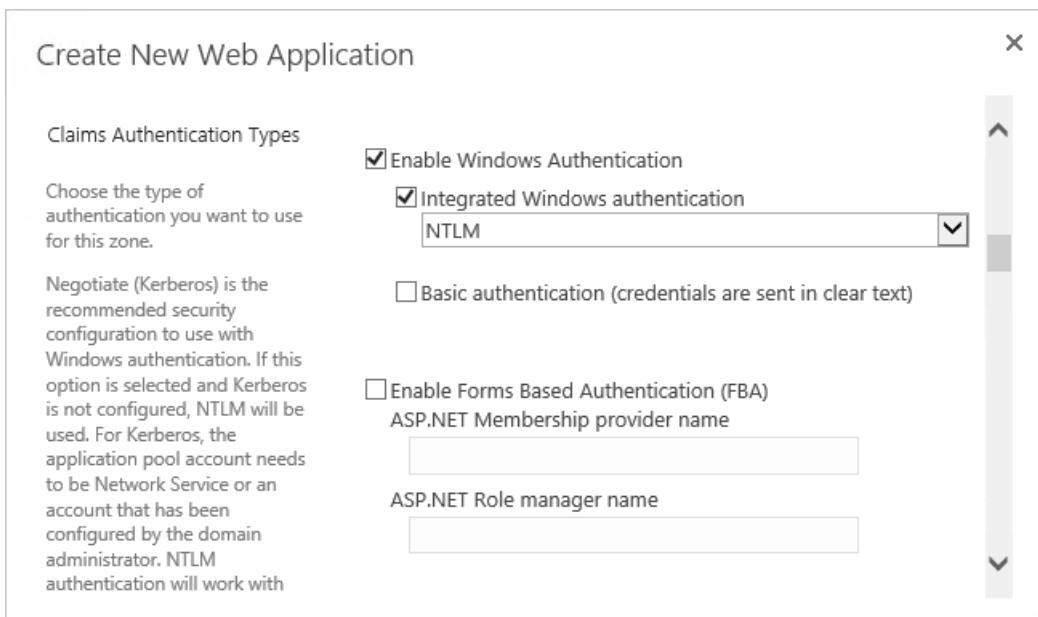


2009

2010 8. Further down in the Create New Web Application window, in the Claims Authentication Types section, do the following steps to enable Windows Authentication (as illustrated):

2011 a. Click on Enable Windows Authentication

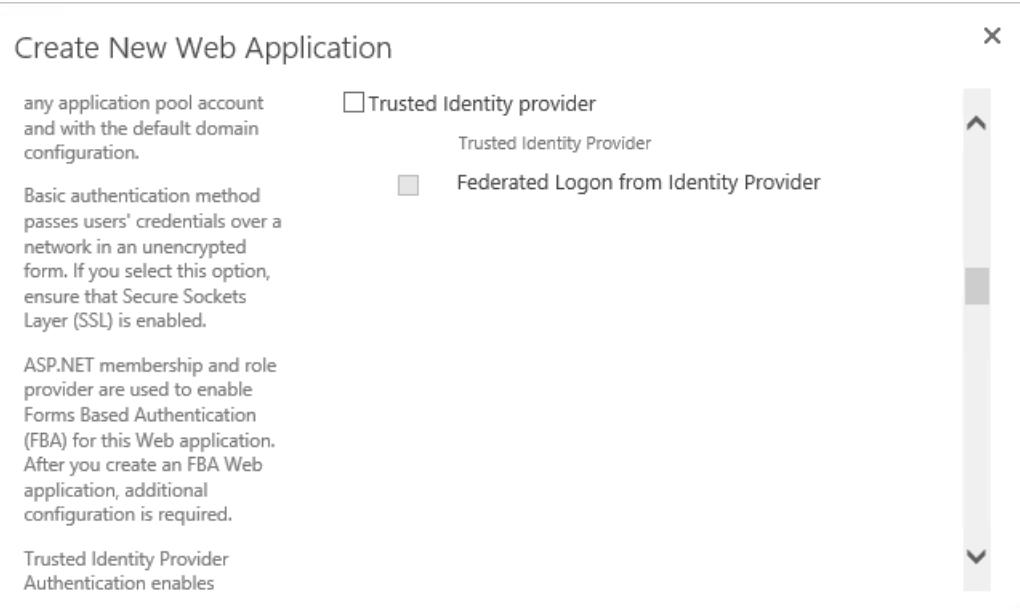
2012 b. Click on Integrated Windows authentication



2013

2014 9. Further down in the Create New Web Application window, in the Claims Authentication Types section, note that there is a **Trusted Identity provider** section. Do not select this option now, but later in our build and in other How-To guide sections there will be steps for setting up the federated logon.

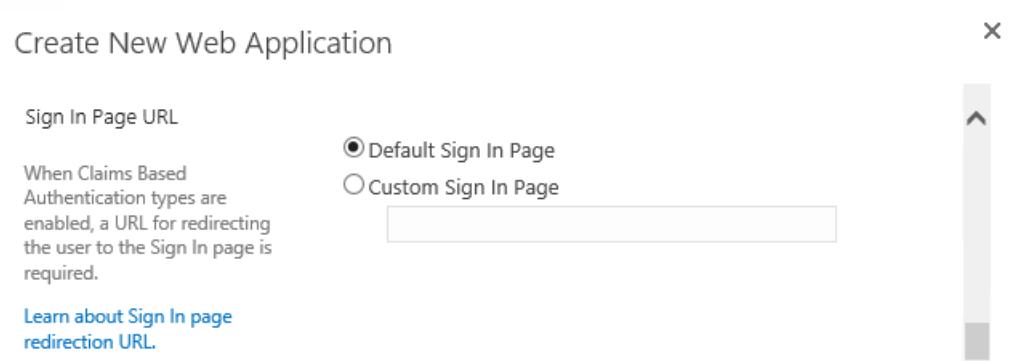
2020



2021

10. Further down in the Create New Web Application window, in the Sign In Page URL section, leave the **Default Sign In Page** radio button chosen (default).

2022

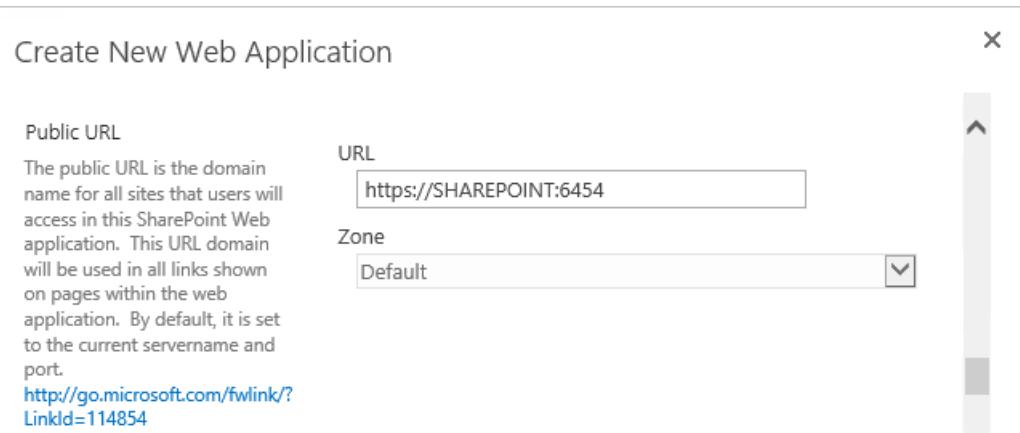


2023

11. Further down in the Create New Web Application window, in the Public URL section, change the **URL** or keep the default **URL**:

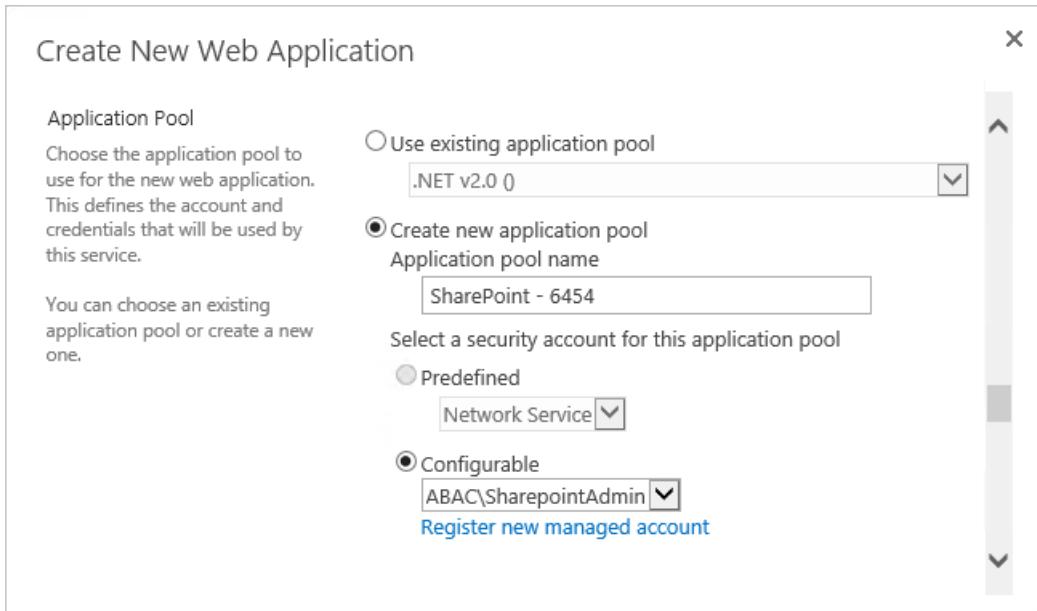
2024

2025

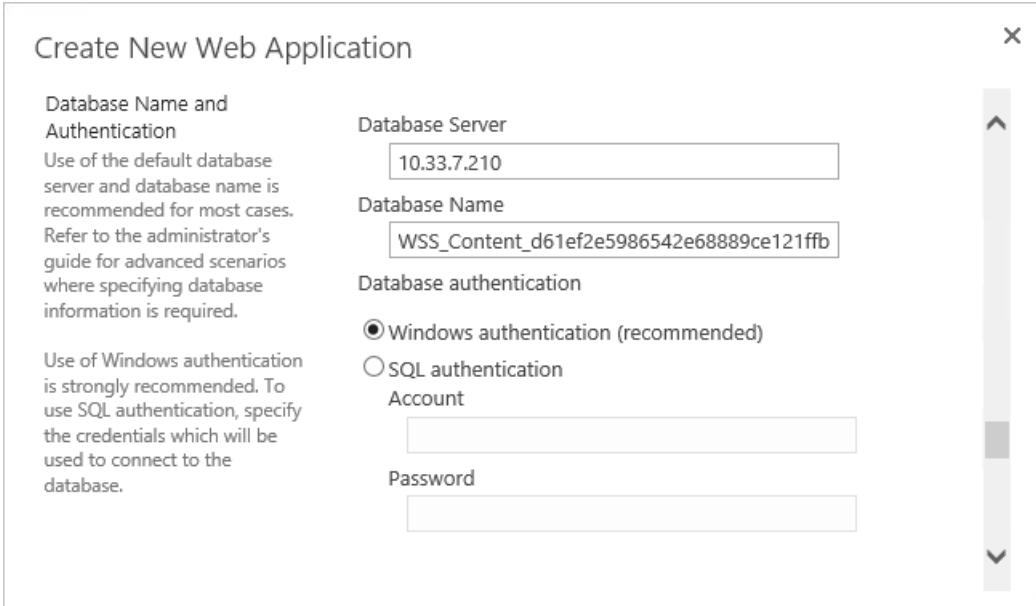


2026

- 2027 12. Further down in the Create New Web Application window, in the Application Pool section, leave
2028 the default values:
- 2029 a. Leave the radio button for **Create new application pool** chosen.
- 2030 b. Note that the **Configurable** button is already chosen to select an existing security
2031 account for the new application pool, an account called SharePointAdmin in this build
- 2032 i. If you do not already have a managed account for this purpose, click on the **Reg-**
2033 **ister new managed account** link and follow the prompts to create one.

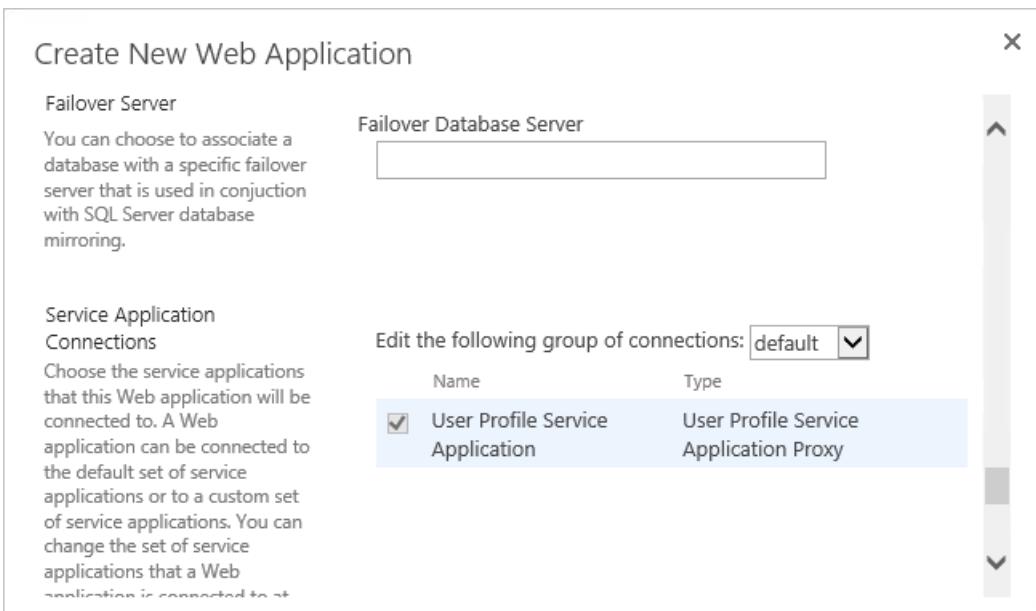


- 2034
- 2035 13. Further down in the Create New Web Application window, in the Database Name and
2036 Authentication section, leave the following fields filled in with the default information or enter
2037 your own manually:
- 2038 a. IP Address of the **Database Server**. In our build the separate, dedicated SQL Server IP
2039 address is 10.33.7.210
- 2040 b. **Database name**



2041

- 2042 14. Further down in the Create New Web Application window, in the Failover Server section, leave the **Failover Database Server** field blank.
- 2043
- 2044 15. Further down in the Create New Web Application window, in Service Application Connections, leave the default checkbox for **User Profile Service Application** checked.
- 2045



2046

- 2047 16. Further down in the Create New Application window, in Customer Experience Improvement Program, either keep the **Enable Customer Experience Improvement Program** radio button for **No** chosen, or click on **Yes**.
- 2048
- 2049
- 2050 17. At the bottom of the Create New Application window click **OK** to finish the web application creation process.
- 2051

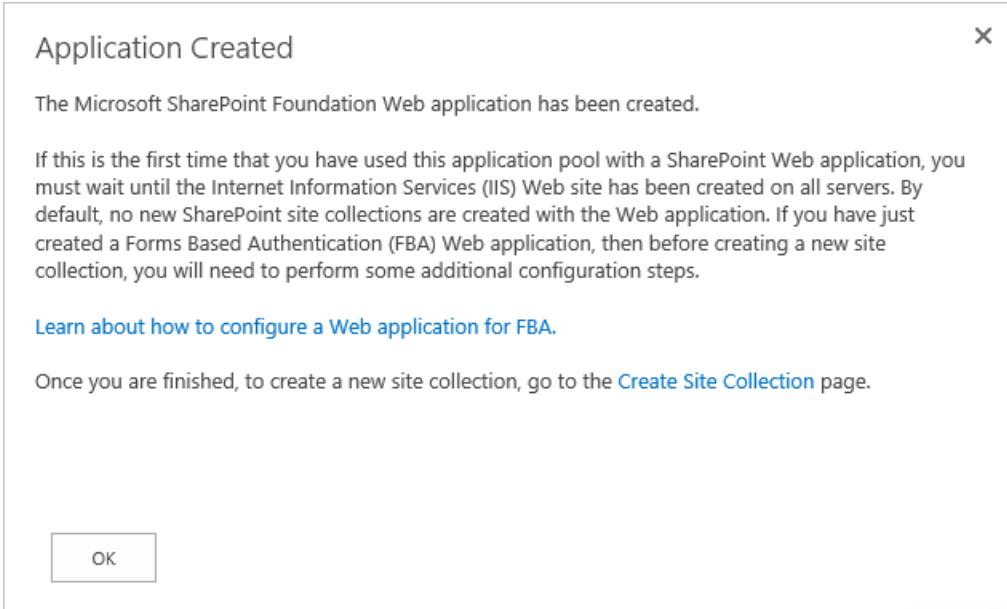
2052

- 2053 18. Wait for the new web application to be created.



2054

- 2055 19. In the Application Created window, click OK.



2056

- 2057 20. Back on the Web Applications page, verify that your new SharePoint web application is listed
2058 ("SharePoint – 6454" from this example).

The screenshot shows the SharePoint Central Administration interface under the 'Web Applications' tab. It lists four web applications:

	Name	URL	Port
Central Administration	SharePoint - 80	http://sharepoint/	80
Application Management	SharePoint Central Administration v4	http://sharepoint:44444/	44444
System Settings	SharePoint - 8888	http://sharepoint:8888/	8888
Monitoring	SharePoint - 6454	https://sharepoint:6454/	6454

2059

- 2060 21. In another browser window, navigate to your new web application (e.g.,
 2061 <https://sharepoint:6454>). Until the SSL certificate is installed as seen in the following section,
 2062 you will receive this error.

The screenshot shows a browser window displaying an error message: "Secure Connection Failed". The message indicates that the connection to the server was reset while the page was loading. It provides two options: "Try Again" and "Report this error".

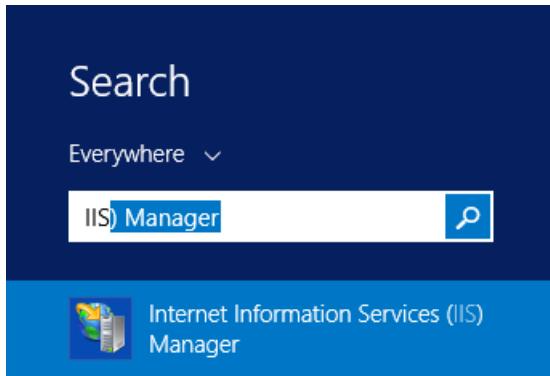
2063

2064 4.4 Creating and Installing SSL Certificate

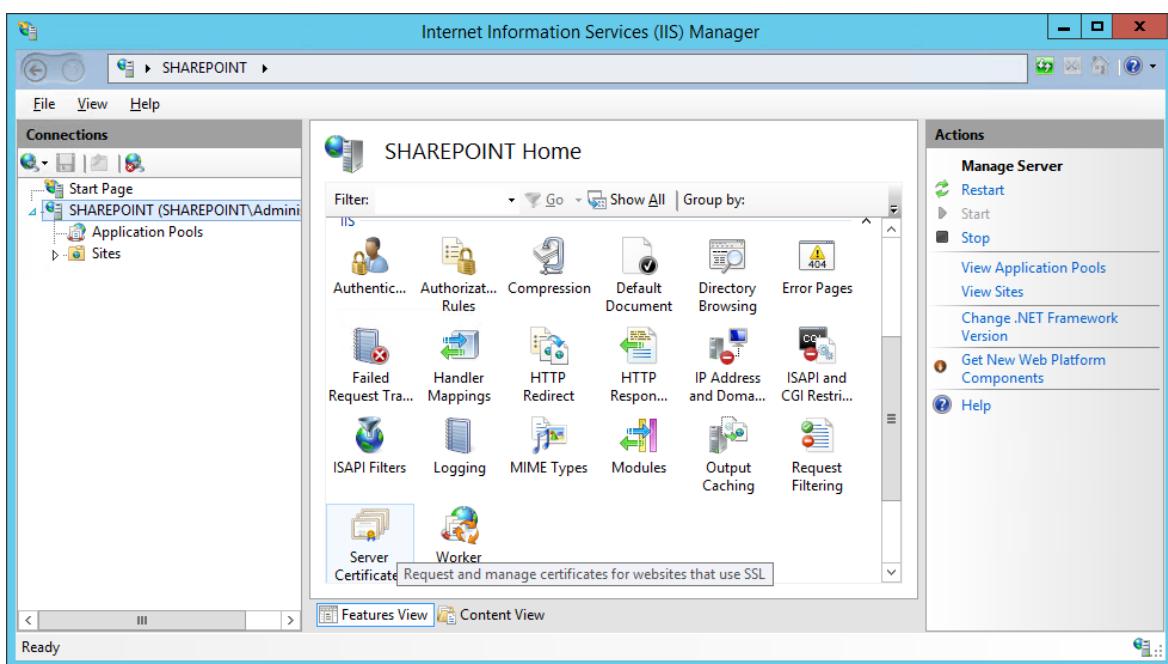
- 2065 For a protected lab environment, it is possible to use self-signed certificates, however for production
 2066 network deployments it is generally recommended to use certificates signed by a Certificate Authority.
 2067 Instructions related to both approaches are included in this section.

2068 **4.4.1 Self-Signed Certificates**2069 ***4.4.1.1 Creating a Self-Signed Certificate on IIS 8***

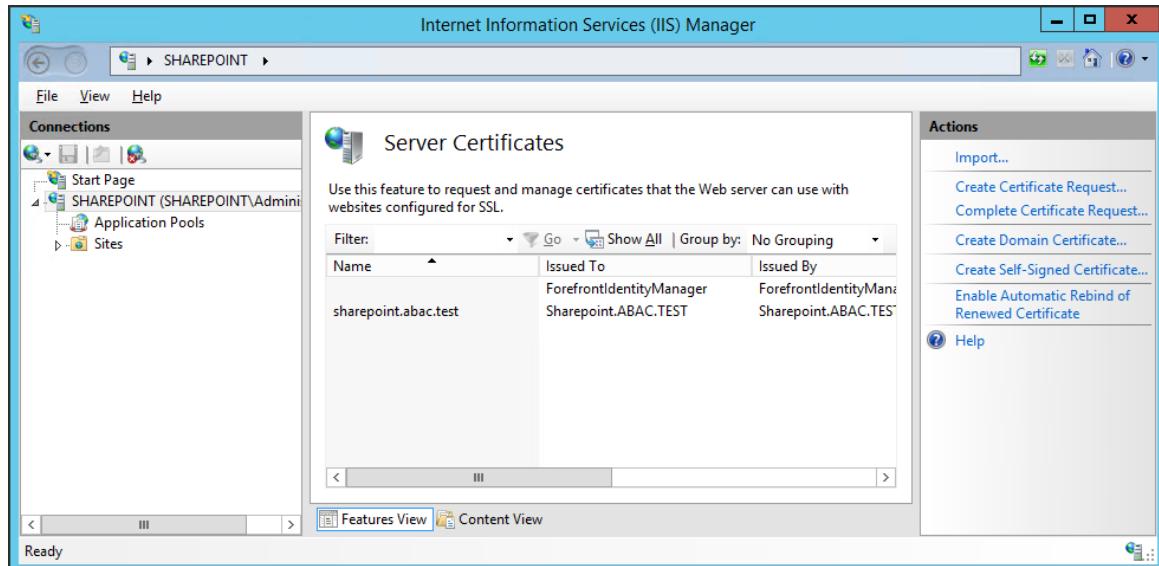
- 2070 1. On the SharePoint Server, click on the **Windows** icon in the bottom left corner of your screen.
- 2071 2. Begin typing **iis**.
- 2072 3. When the **Internet Information Services (IIS) Manager** appears, click on it.



- 2073
- 2074 4. Click on the **SharePoint Instance** to see its Features.
- 2075 5. Scroll down and double-click on **Server Certificates**.

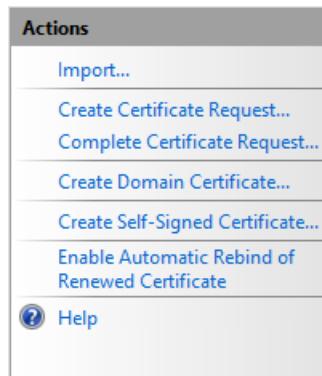


- 2076
- 2077 6. In the Server Certificates window, you will see any certificates that already exist.



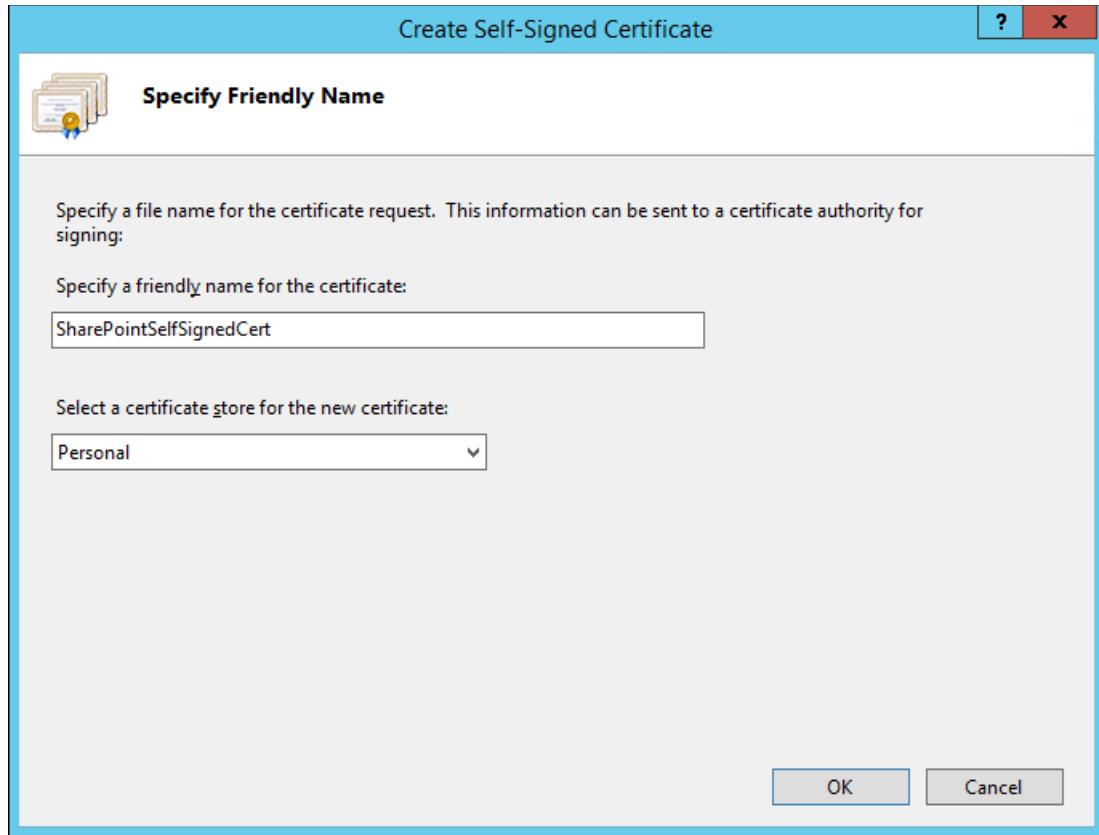
2078

- 2079 7. In the Actions panel on the right side of the IIS Manager window, next to the Server Certificates window, click on **Create Self-Signed Certificate**.



2081

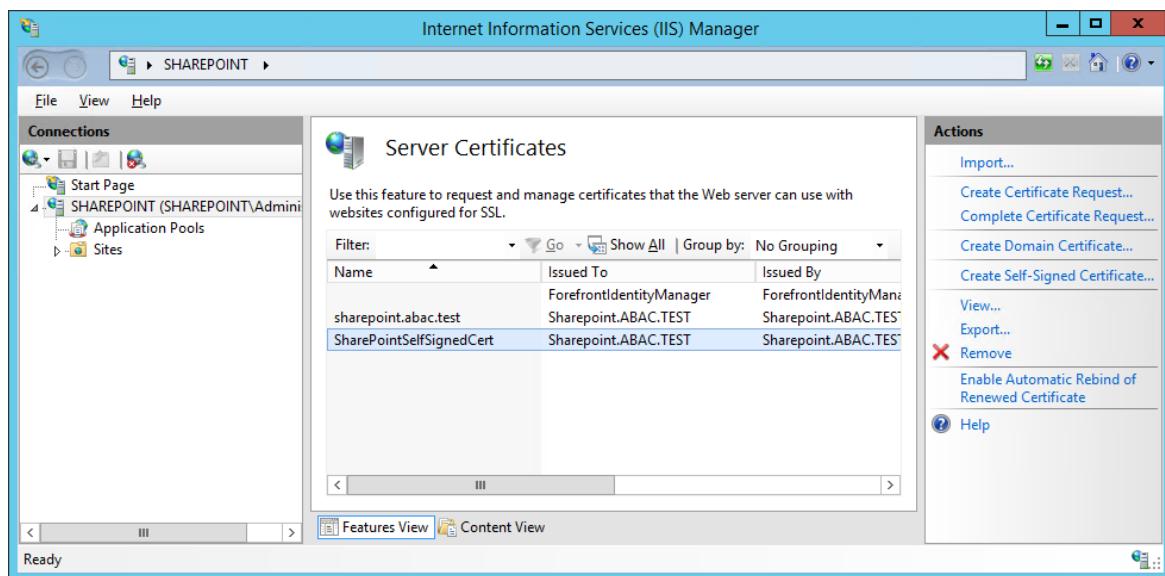
- 2082 8. In the Create Self-Signed Certificate window, **Specify a friendly name for the certificate** and
2083 **Select a certificate store for the new certificate**, then click **OK**.



2084

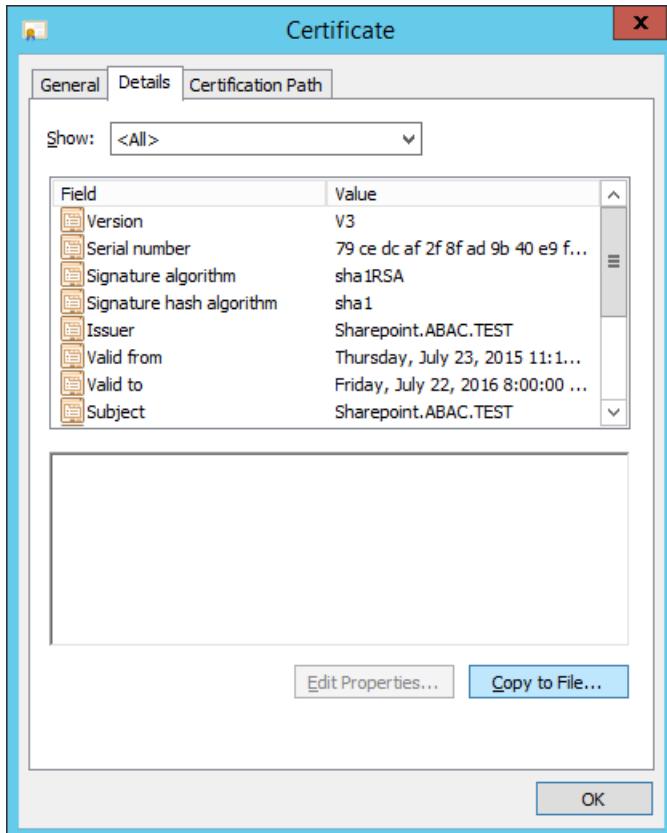
2085 4.4.1.2 Importing Self-Signed Certificate to SharePoint Certificate Store

- 2086 1. After creating the self-signed certificate and clicking **OK** in the previous sub-section, you will see
2087 your new certificate.
- 2088 2. Double-click on the new certificate.



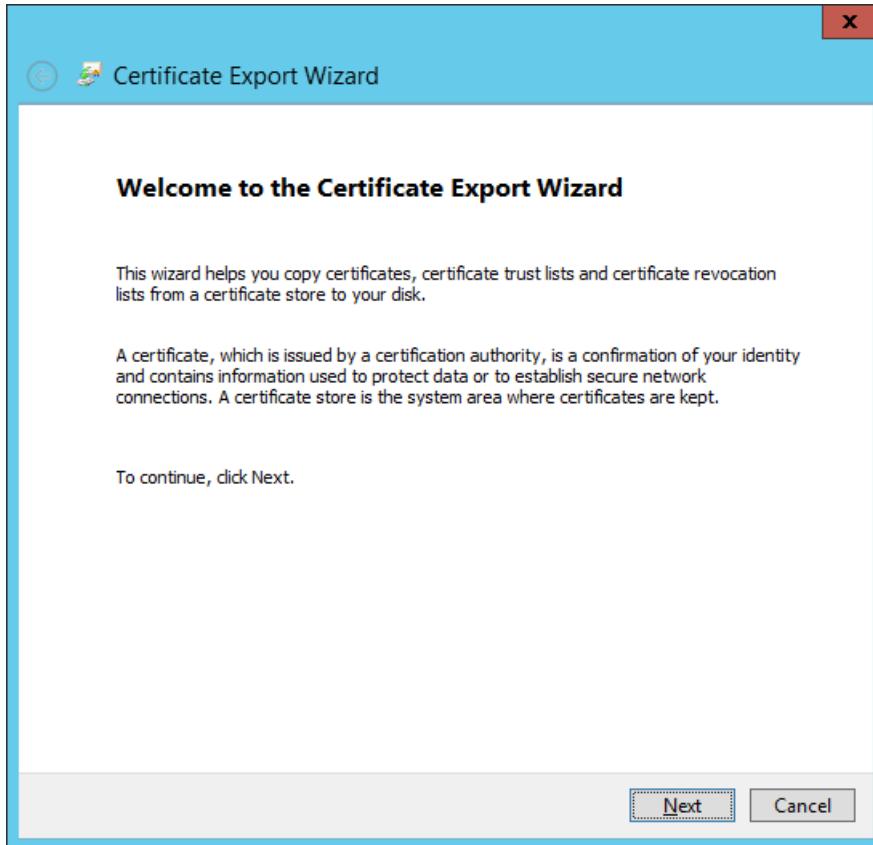
2089

- 2090 3. In the **Details** tab of the Certificate window, click on **Copy to File**.



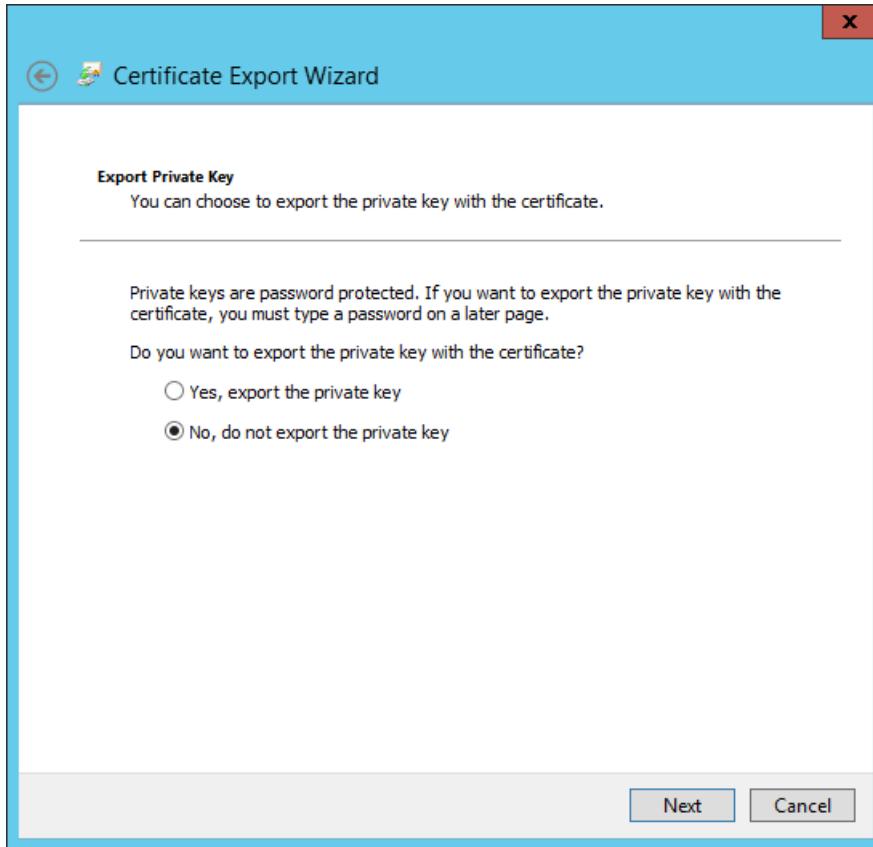
2091

2092 4. In the Certificate Export Wizard window that opens, click **Next**.



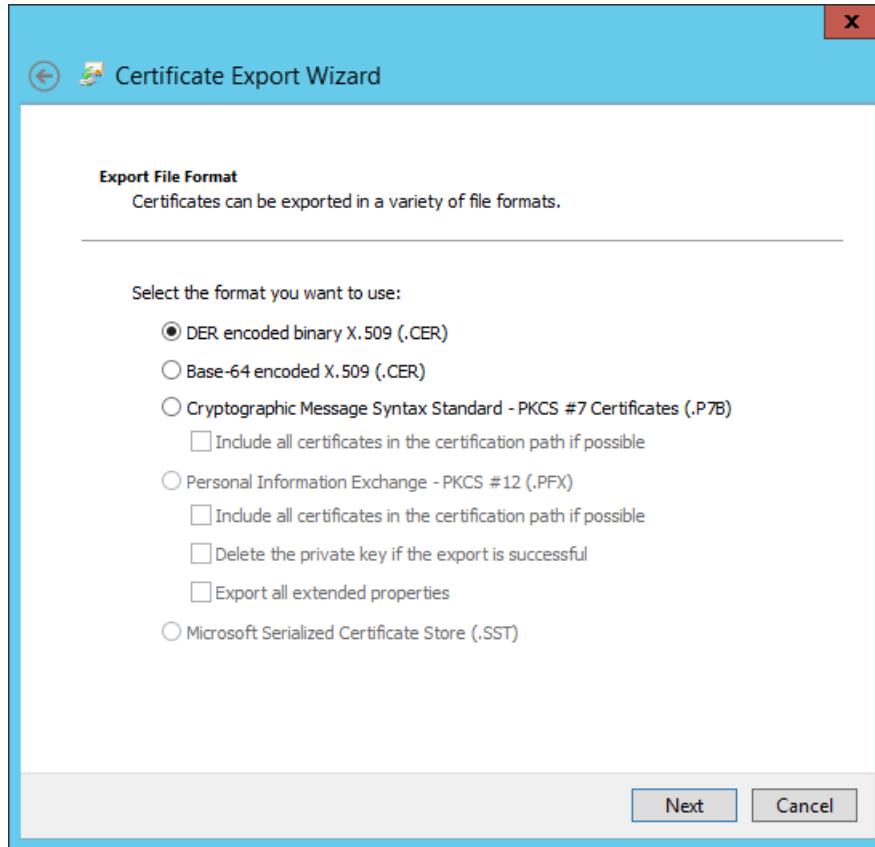
2093

- 2094 5. In the Certificate Export Wizard window on the Export Private Key screen, keep the selection
2095 **No, do not export the private key** and click **Next**.



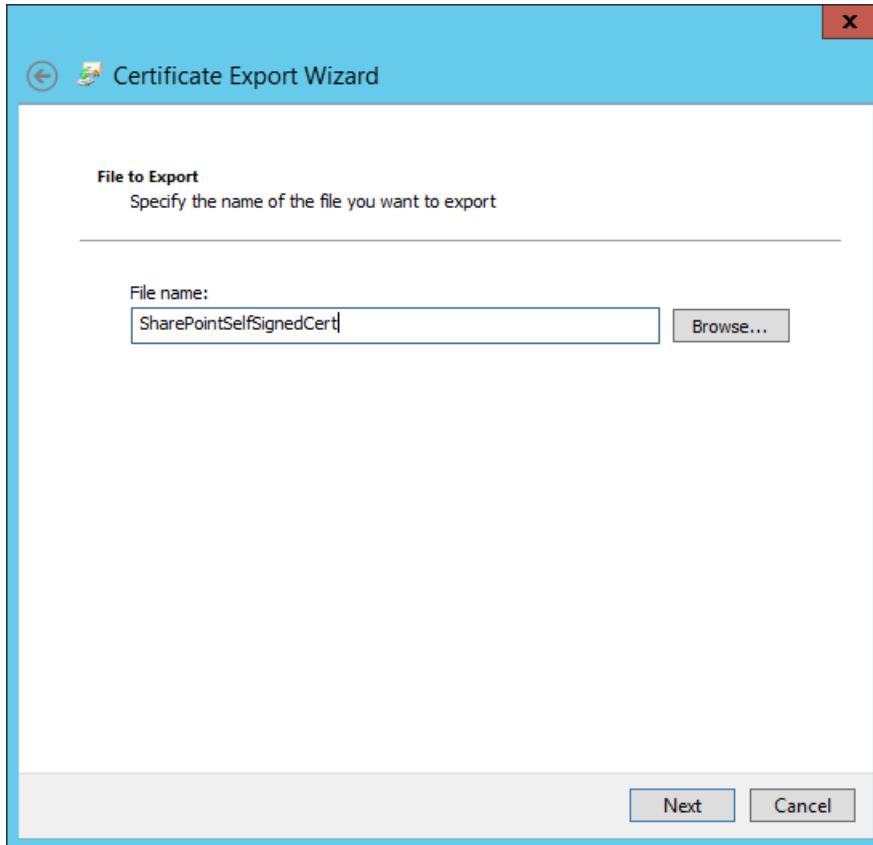
2096

- 2097 6. In the Certificate Export Wizard window on the Export File Format screen, select the format you
2098 want to use (**DER** in this example), then click **Next**.



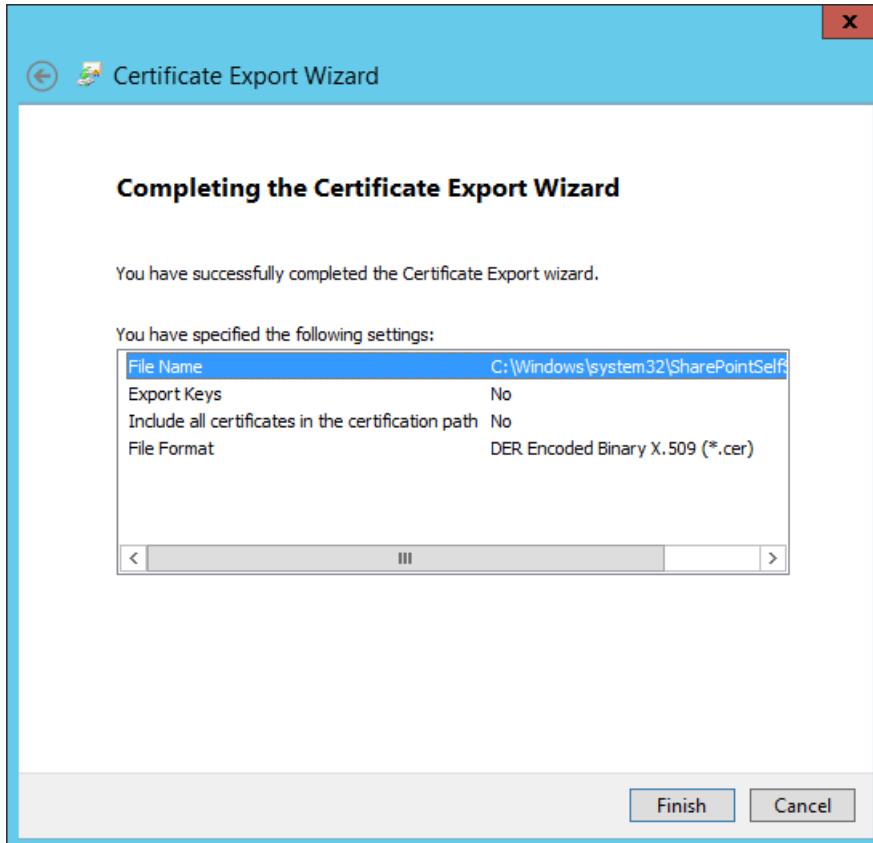
2099

- 2100 7. In the Certificate Export Wizard window on the File to Export screen, type in the certificate file
2101 name and click **Next**.



2102

- 2103 8. In the Certificate Export Window on the Completing the Certificate Export Wizard screen, click
2104 **Finish**.



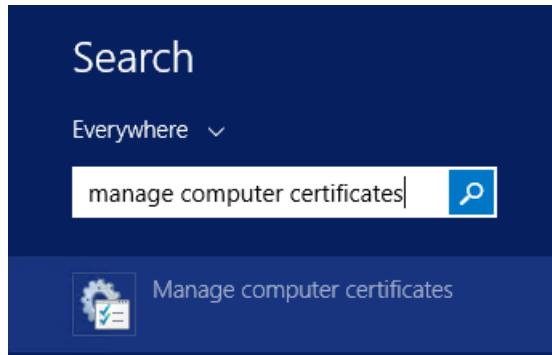
2105

- 2106 9. In another Certificate Export Wizard window that automatically opens, you will see that the
2107 export was successful. Click **OK**.



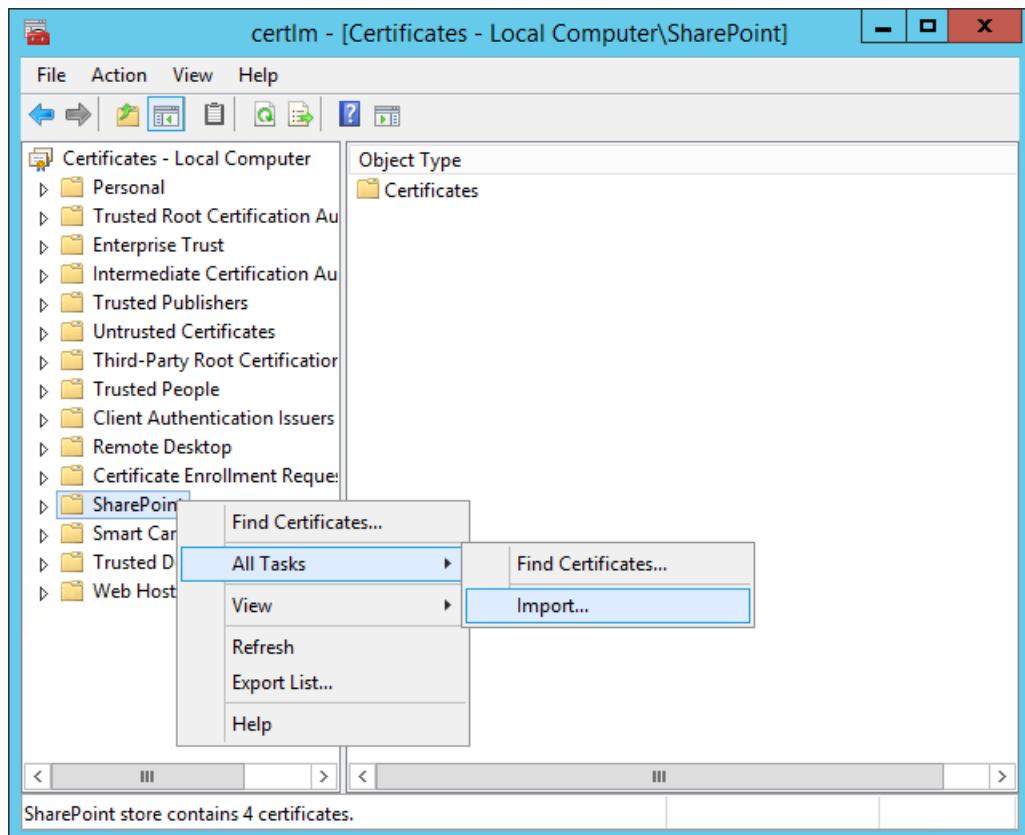
2108

- 2109 **4.4.1.3 Add the Self Signed Certificate to Trust management in Central Administration**
- 2110 1. Click on the Windows icon at the bottom left corner of your screen.
2111 2. Begin typing the words: manage computer certificates.
2112 3. Click on the Manage Computer Certificates icon.



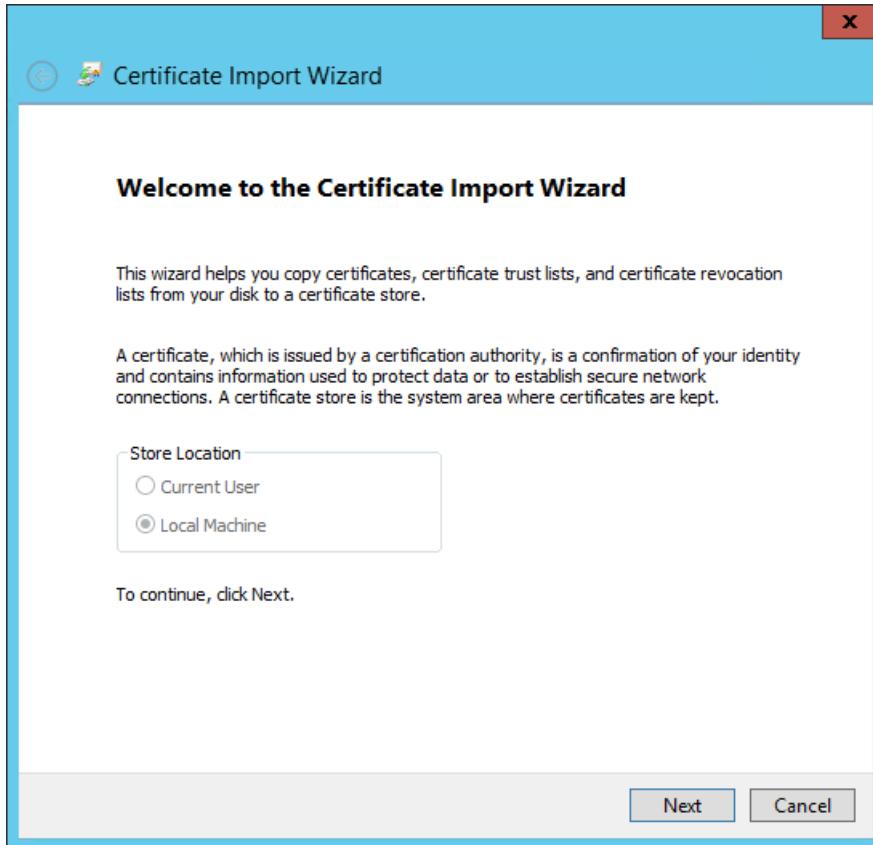
2113

- 2114 4. In the certlm window, right-click on the **SharePoint** node, hover over **All Tasks**, then click **Import**.
- 2115



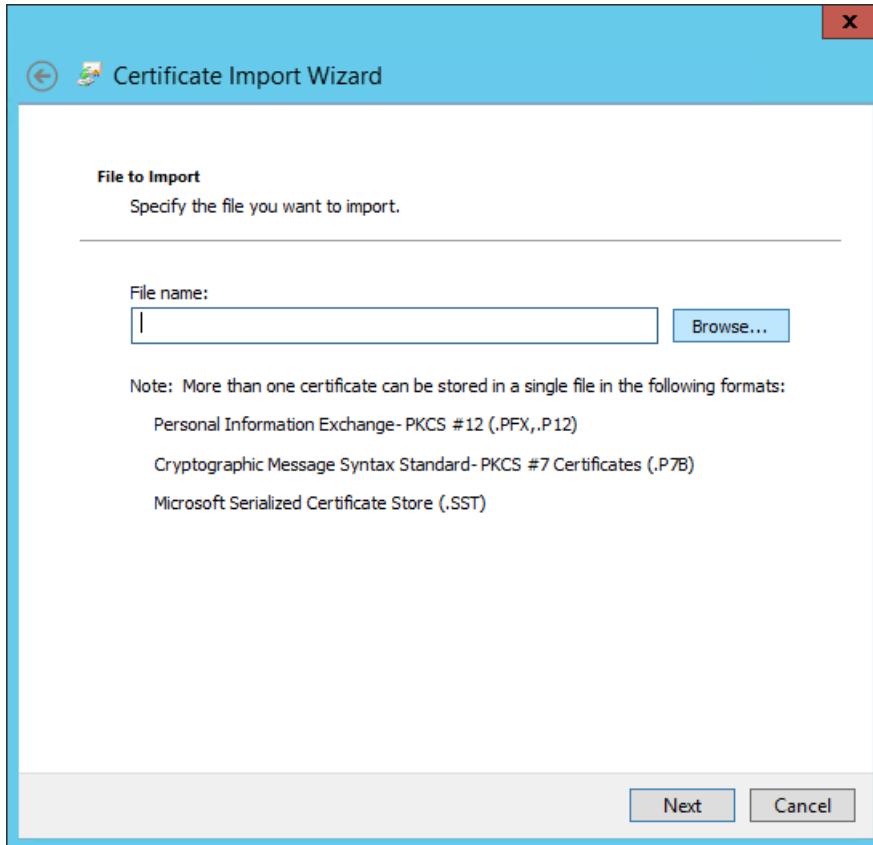
2116

- 2117 5. In the Certificate Import Wizard window that opens, click **Next**.



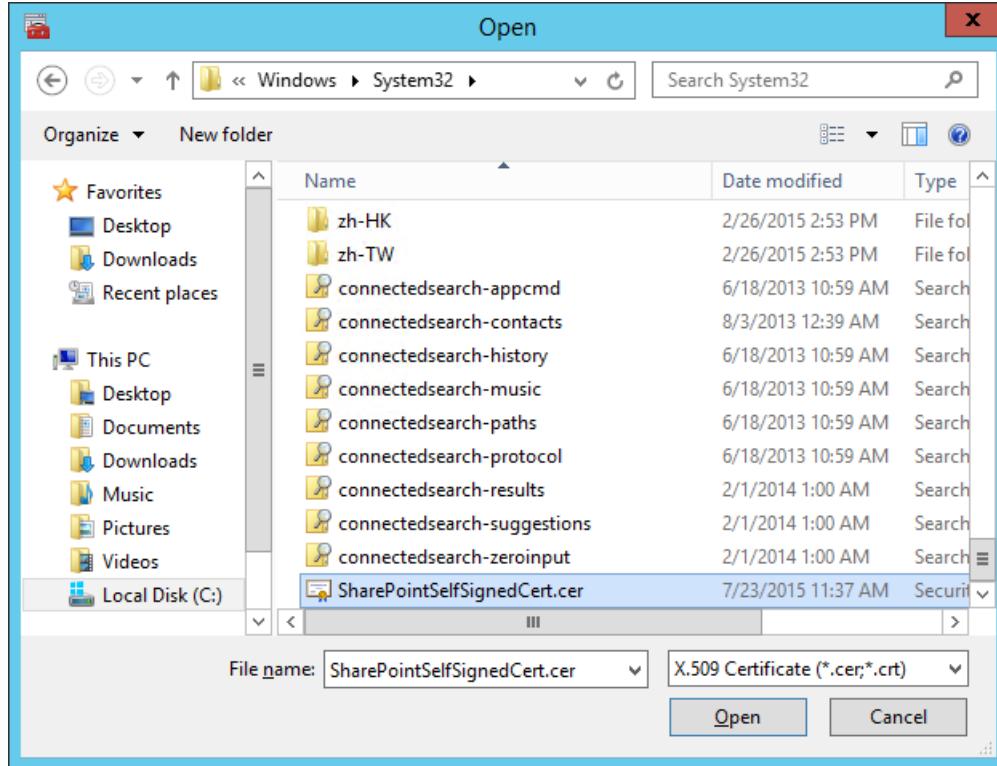
2118

- 2119 6. In the Certificate Import Wizard window, on the File to Import screen, click **Browse** to find the
2120 self-signed certificate we created in the previous sub-section.



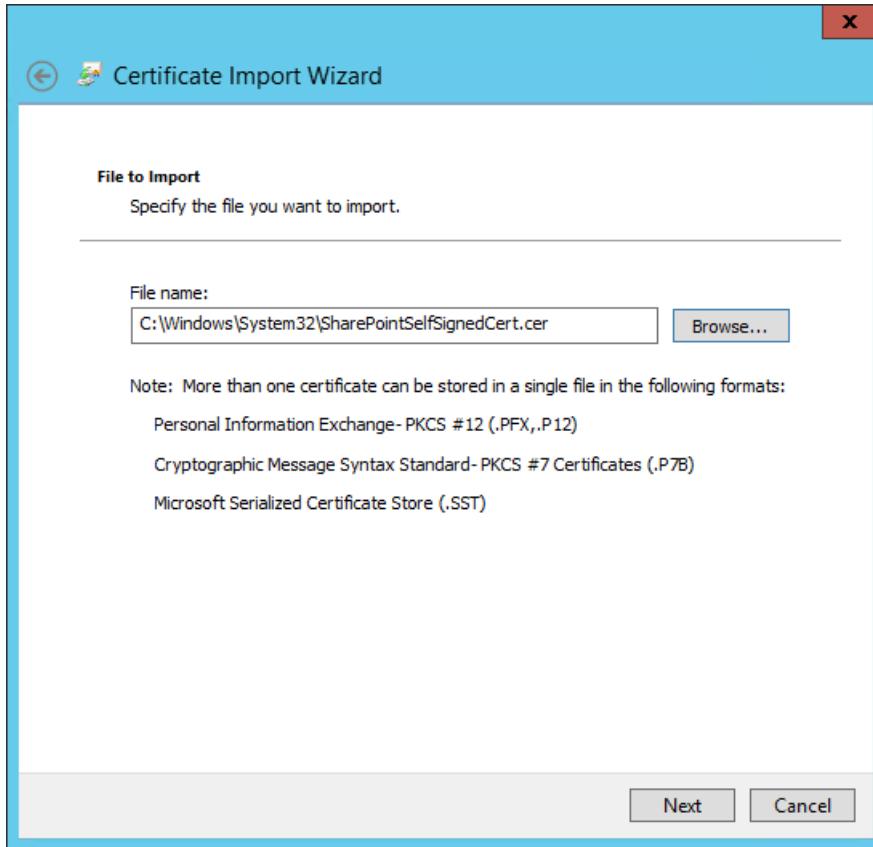
2121

- 2122 7. In the File Explorer window that opens automatically, click through location folders to find the
2123 self-signed certificate we created in the previous sub-section (example from this build:
2124 *C:/Windows/System32/*).
2125 8. Find the certificate and click to select it; then click **Open**.



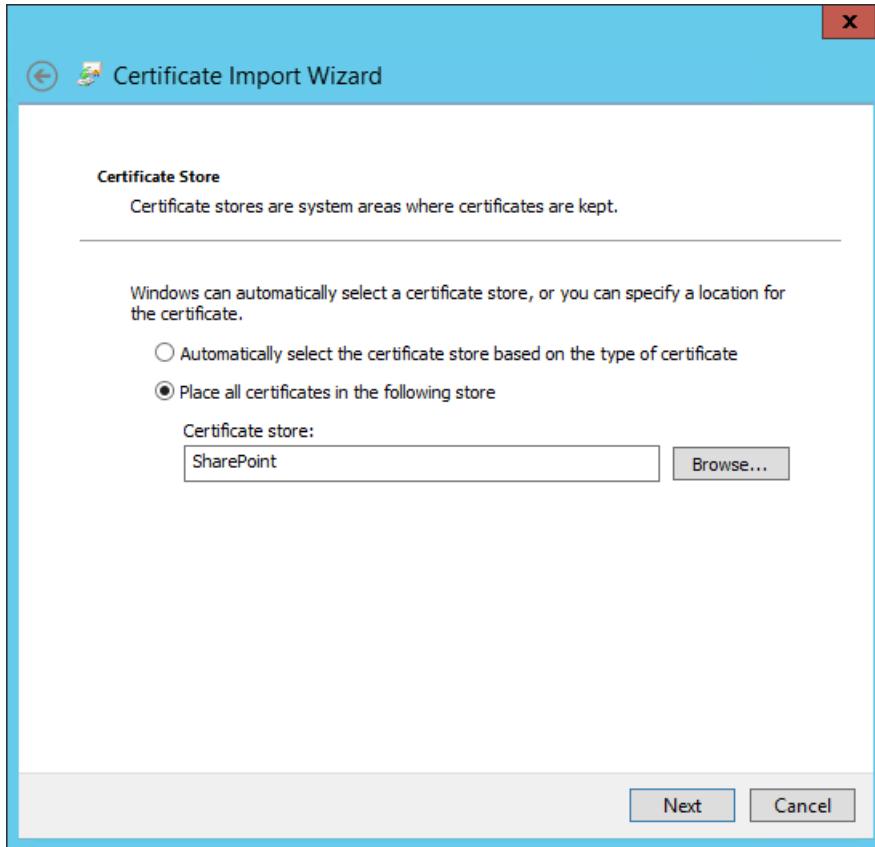
2126

- 2127 9. Back at the Certificate Import Wizard, on the File to Import screen, the location of the self-
2128 signed certificate will be in the **File name** field. Click **Next**.



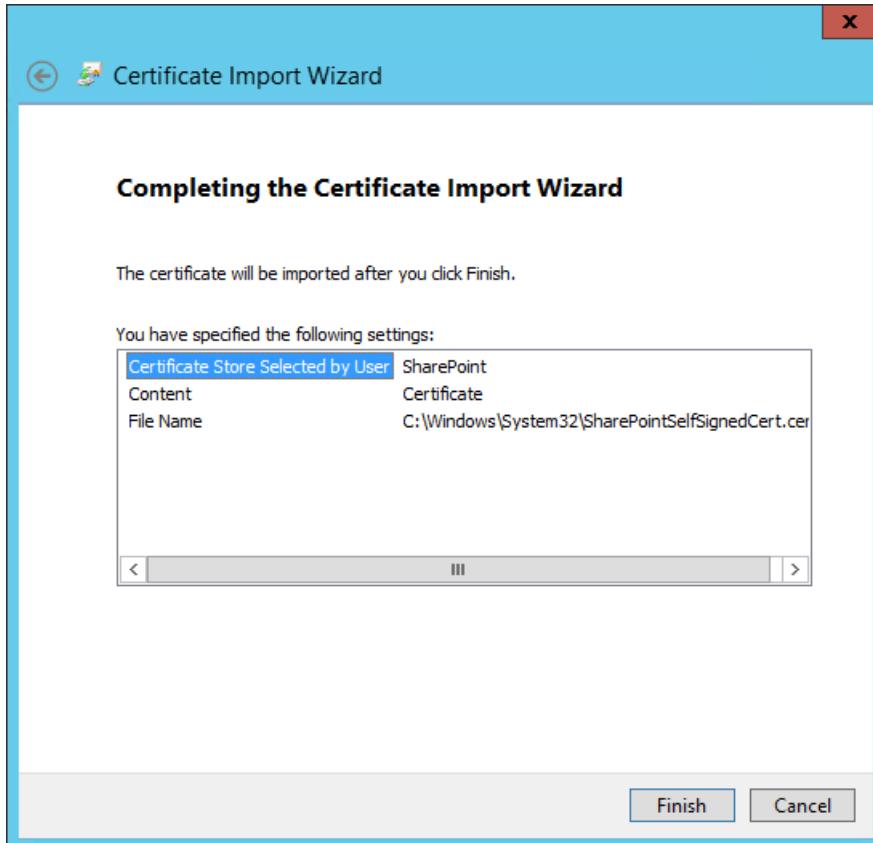
2129

- 2130 10. In the Certificate Import Wizard window on the Certificate Store screen, leave the default radio
2131 button for **Place all certificates in the following store** chosen. The **Certificate store** field should
2132 be set to SharePoint. Click **Next**.



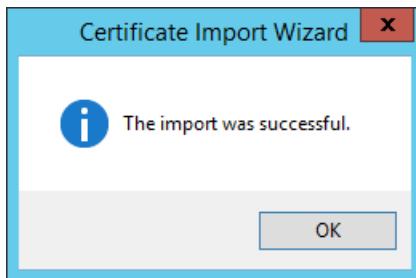
2133

2134 11. In the Certificate Import Wizard window, click **Finish**.



2135

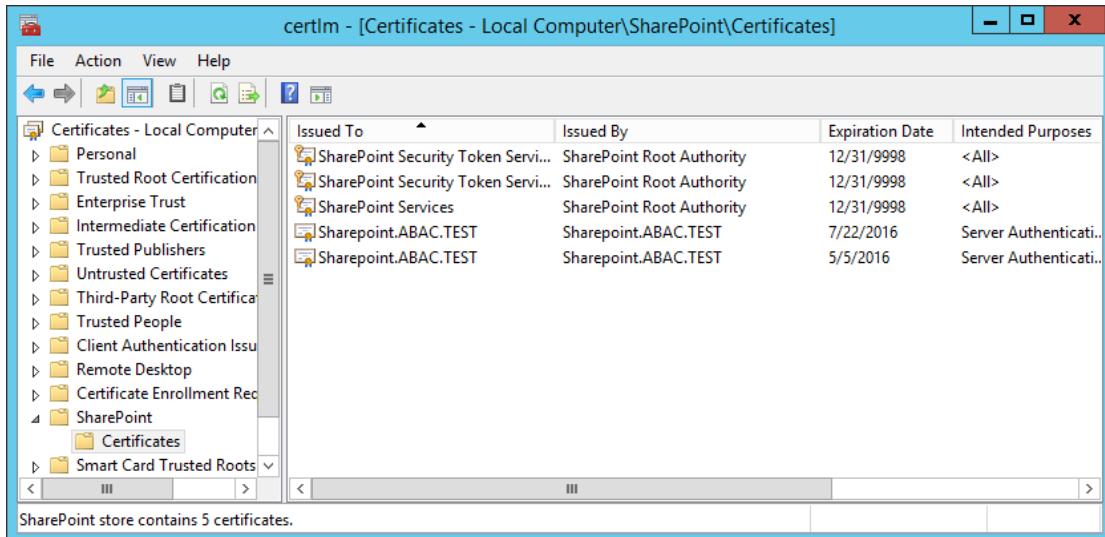
- 2136 12. In the Certificate Import Wizard window that automatically opens, you will see a message that
2137 the import was successful. Click **OK**.



2138

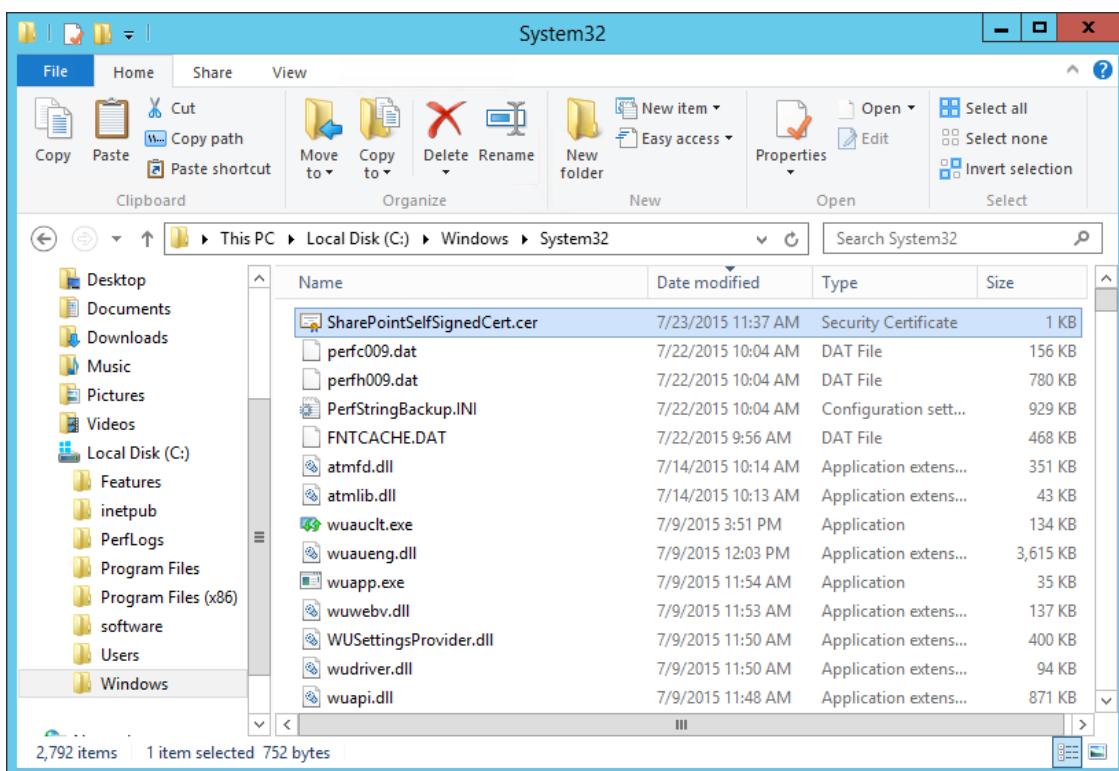
- 2139 13. In the certlm window, double-click on **Certificates** under the SharePoint node. The new self-
2140 signed certificate you created will be listed there.

SECOND DRAFT



2141

- 2142 14. Open **File Explorer** and click through locations to reach the location of your self-signed
2143 certificate (from this example: *C:/Windows/System32/*).

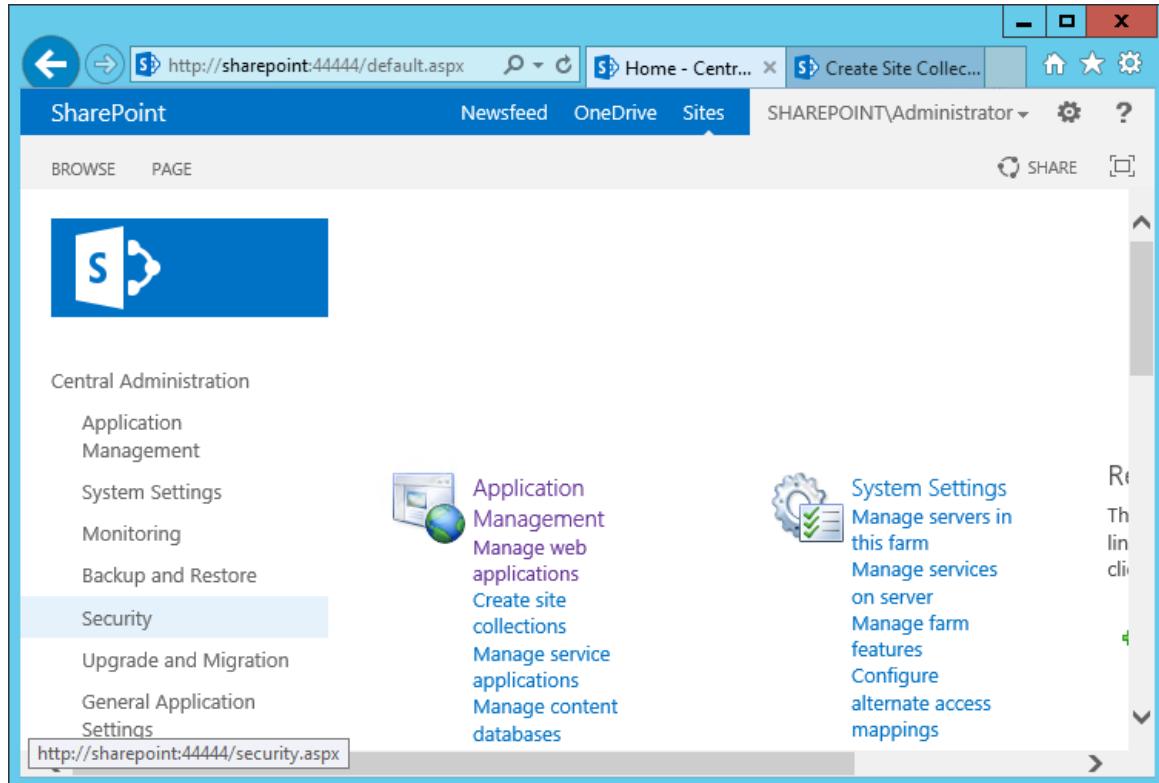


2144

- 2145 15. Right-click on the **self-signed certificate** and click on **Copy** or left-click on the self-signed
2146 certificate and press the keys Ctrl+C.
2147 16. Right-click on your **Desktop** and click **Paste**, or left-click on your Desktop and press the keys
2148 Ctrl+V to save a copy of the certificate in an accessible location.
2149 17. To Manage Trust via Central Administration, do the following steps: Open a **browser**.

SECOND DRAFT

- 2150 18. In the **URL address bar** of the browser, enter the address for Central Administration and click
2151 **Enter or Go:** *http://sharepoint:44444/default.aspx*
- 2152 19. From the Central Administration page, click on **Security** in the left-hand menu.



- 2153
- 2154 20. From the Security page, under the General Security section, click on **Manage Trust**.

The screenshot shows the SharePoint Central Administration interface. The left navigation menu is expanded, showing various administrative options like Application Management, System Settings, Monitoring, Backup and Restore, Security (which is selected), Upgrade and Migration, and General Application Settings. The main content area is titled "Security" and contains two sections: "Users" and "General Security". The "Users" section includes links to manage the farm administrators group, approve or reject distribution groups, and specify web application user policy. The "General Security" section includes links to configure managed accounts, service accounts, password change settings, authentication providers, trust, antivirus settings, blocked file types, web part security, and self-service site creation.

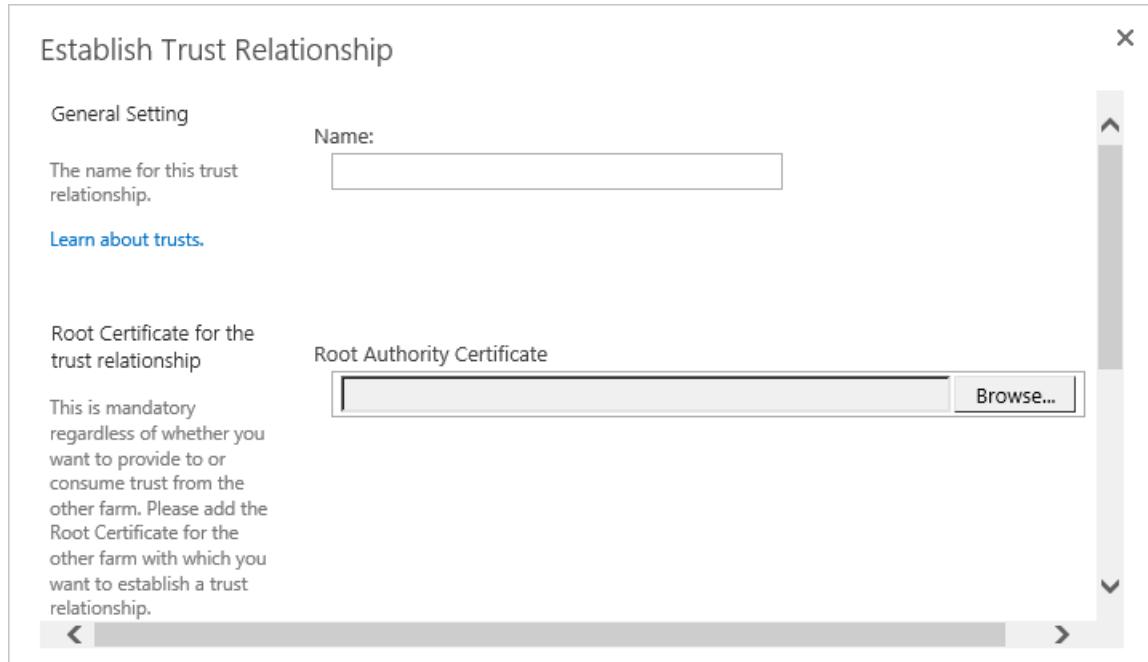
2155

2156 21. Under the Trust Relationships tab of the Manage Trust page, click **New**.

The screenshot shows the SharePoint Trust Relationships page. The top navigation bar has tabs for "BROWSE" and "TRUST RELATIONSHIPS", with "TRUST RELATIONSHIPS" being the active tab. Below the navigation is a toolbar with "New", "Edit", and "Delete" buttons, and a "Manage" link. The main content area displays a table with columns for "Central Administration", "Name", "Description", and "Type". There are currently no rows in the table.

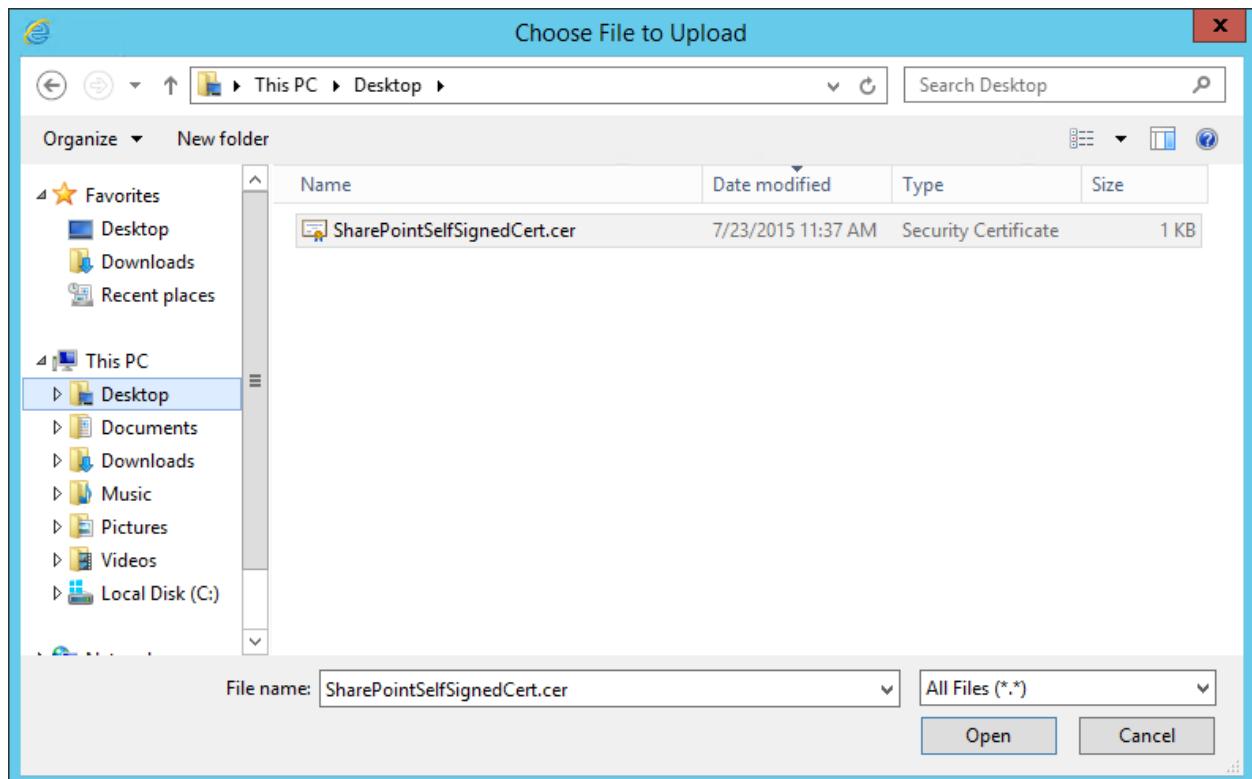
2157

2158 22. In the Establish Trust Relationship window that opens automatically, enter the **Name** for the
2159 trust relationship being created, then click **Browse** to find the certificate created in previous
2160 sub-sections.



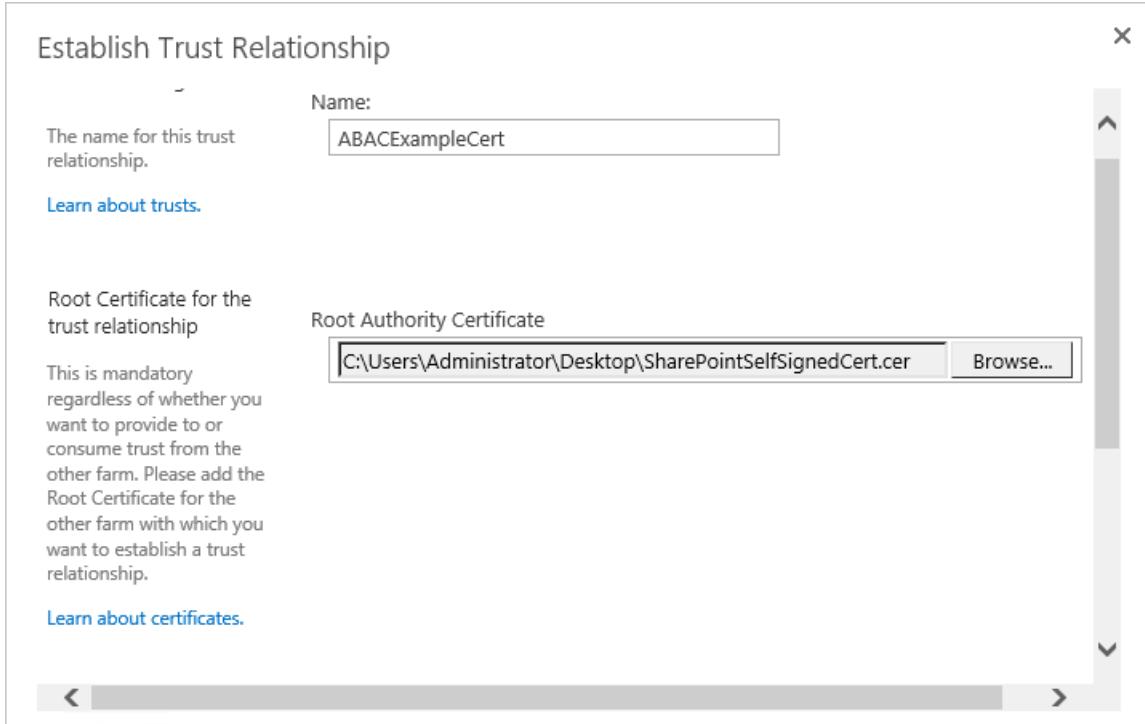
2161

- 2162 23. In the Choose File to Upload window that opens automatically, navigate to the copy of your
2163 certificate from [Section 4.4.1.1](#) (e.g., Desktop). Click on the certificate so its name automatically
2164 fills the **File name** field at the bottom of the window, then click **Open**.



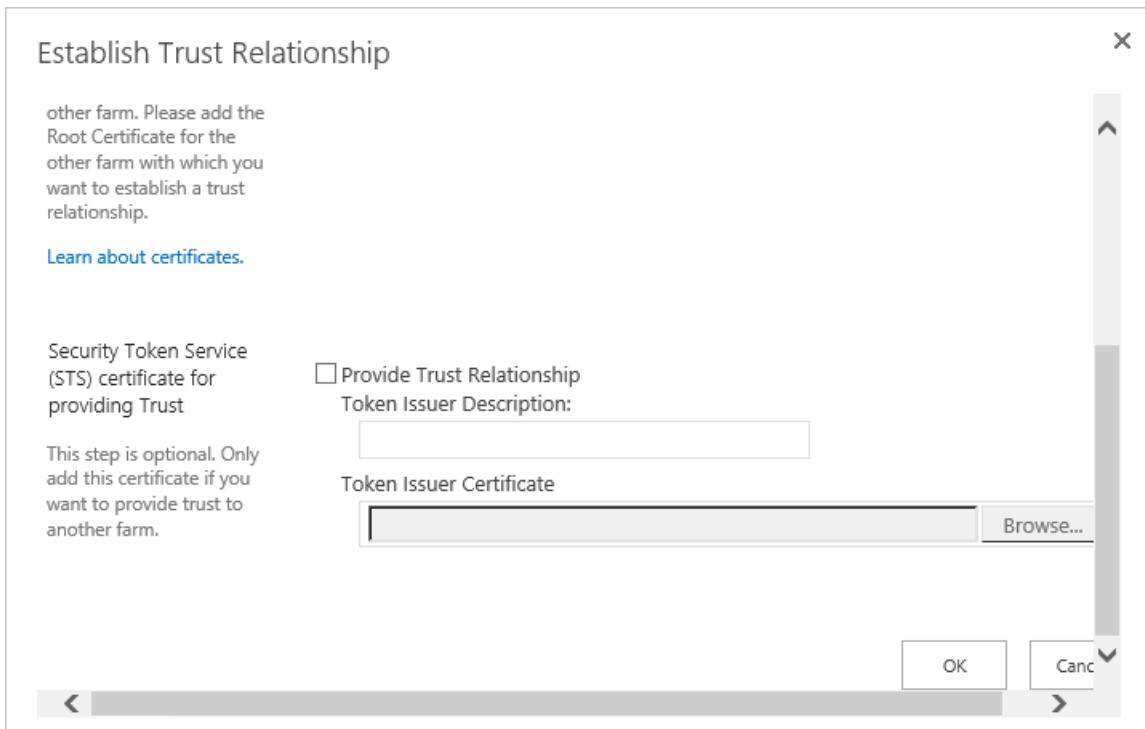
2165

- 2166 24. In the Establish Trust Relationship window, the certificate's location will be automatically
2167 entered as the **Root Authority Certificate**.



2168

- 2169 25. In the Establish Trust Relationship window, scroll down leaving the remaining fields empty, and click OK.
- 2170



2171

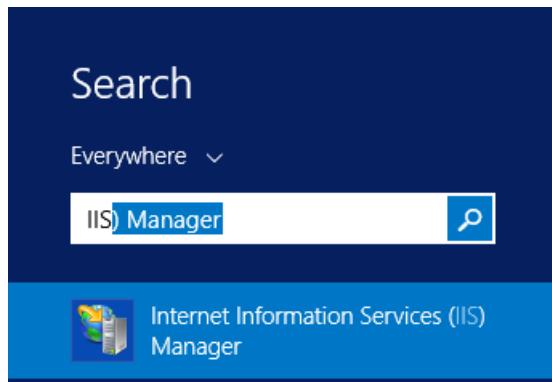
- 2172 26. Your new trust relationship will be listed under the Trust Relationships tab.

The screenshot shows the SharePoint Trust Relationships page. At the top, there are navigation links for SharePoint, Newsfeed, OneDrive, and Sites. The user is logged in as SHAREPOINT\Administrator. The main content area is titled "TRUST RELATIONSHIPS". It displays a table with columns: Central Administration, Name, Description, and Type. There is one entry: "ABACExampleCert" (Name), "Trusted Service Consumer" (Type). The left sidebar has sections for New, Edit, Delete, and Manage. The Manage section lists various SharePoint management options like Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, and Apps.

2173

2174 4.4.1.4 *Configure IIS Binding for the Self-Signed Certificate*

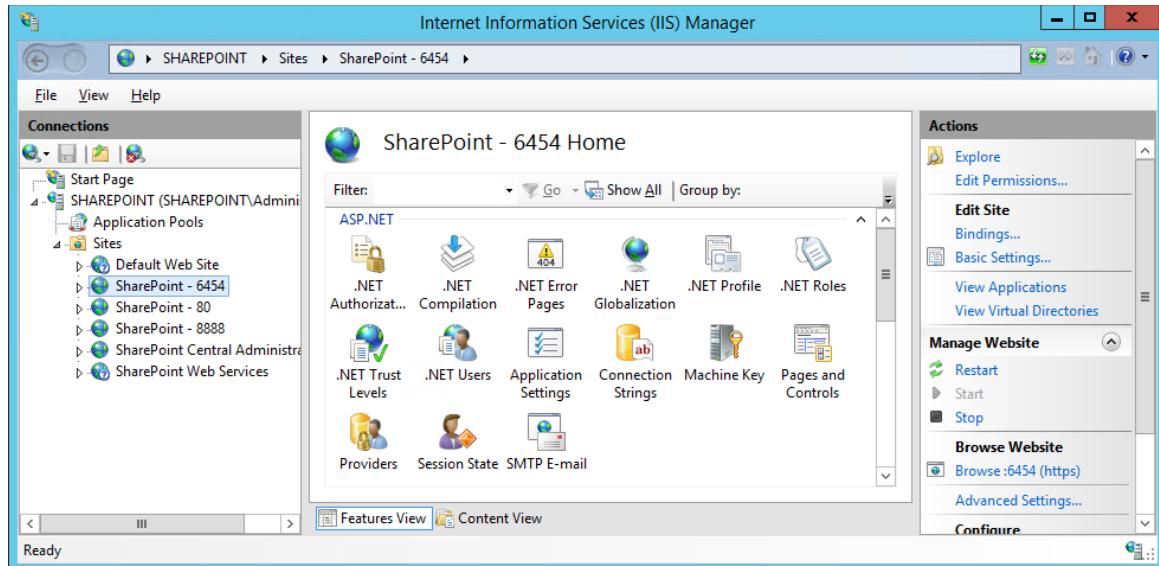
- 2175 1. Click on the **Windows** icon in the bottom left corner of your screen.
- 2176 2. Begin typing **iis**.
- 2177 3. When the **Internet Information Services (IIS) Manager** appears, click on it.



2178

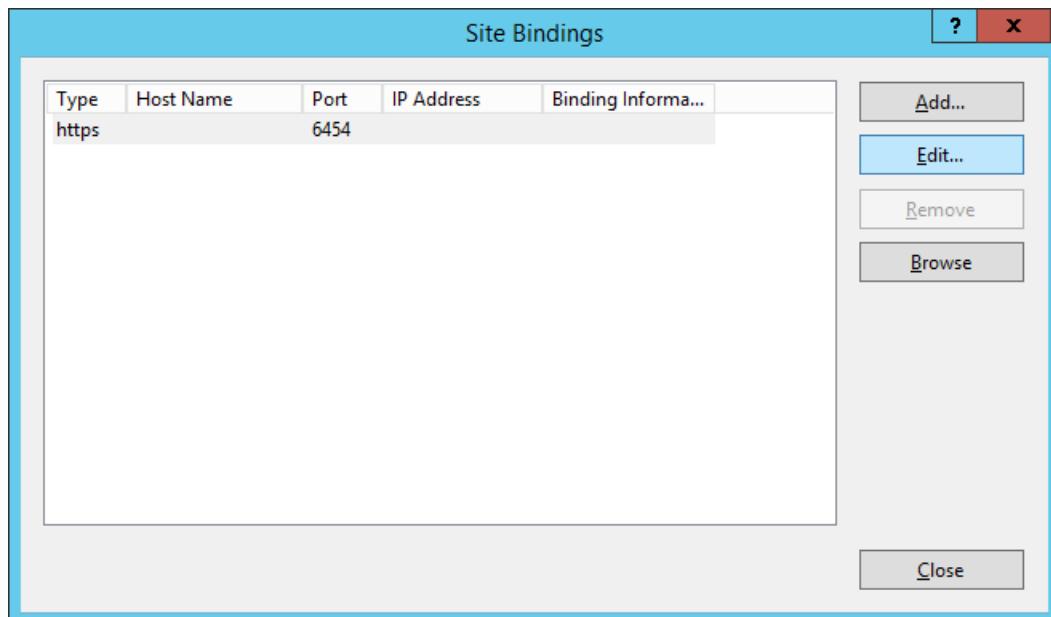
- 2179 4. On the left-hand side of the IIS Manager window, click on the **SharePoint web application** created in previous steps, then click **Bindings** in the Actions pane on the right.
- 2180

SECOND DRAFT



2181

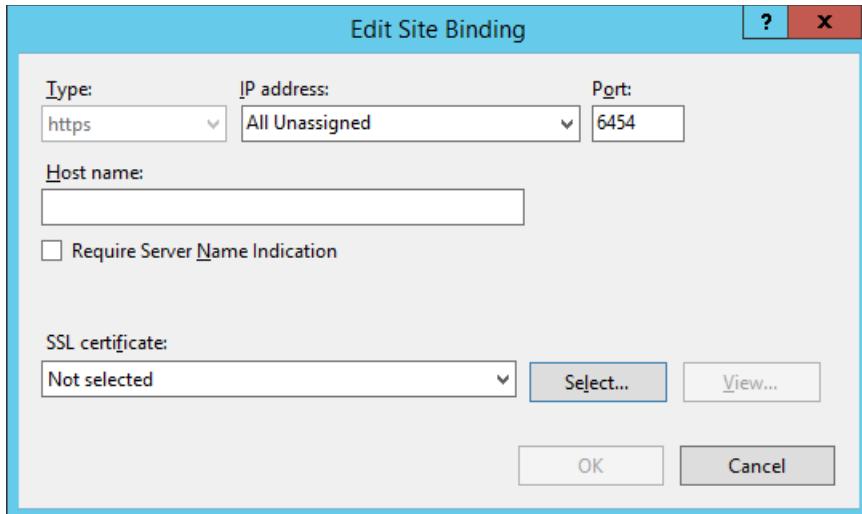
- 2182 5. In the Site Bindings window that opens, look for a binding type of https.
 - a. If a binding type of https does not exist, click on **Add**.
 - b. If a binding type of https does already exist, click on it, then click **Edit**.



2185

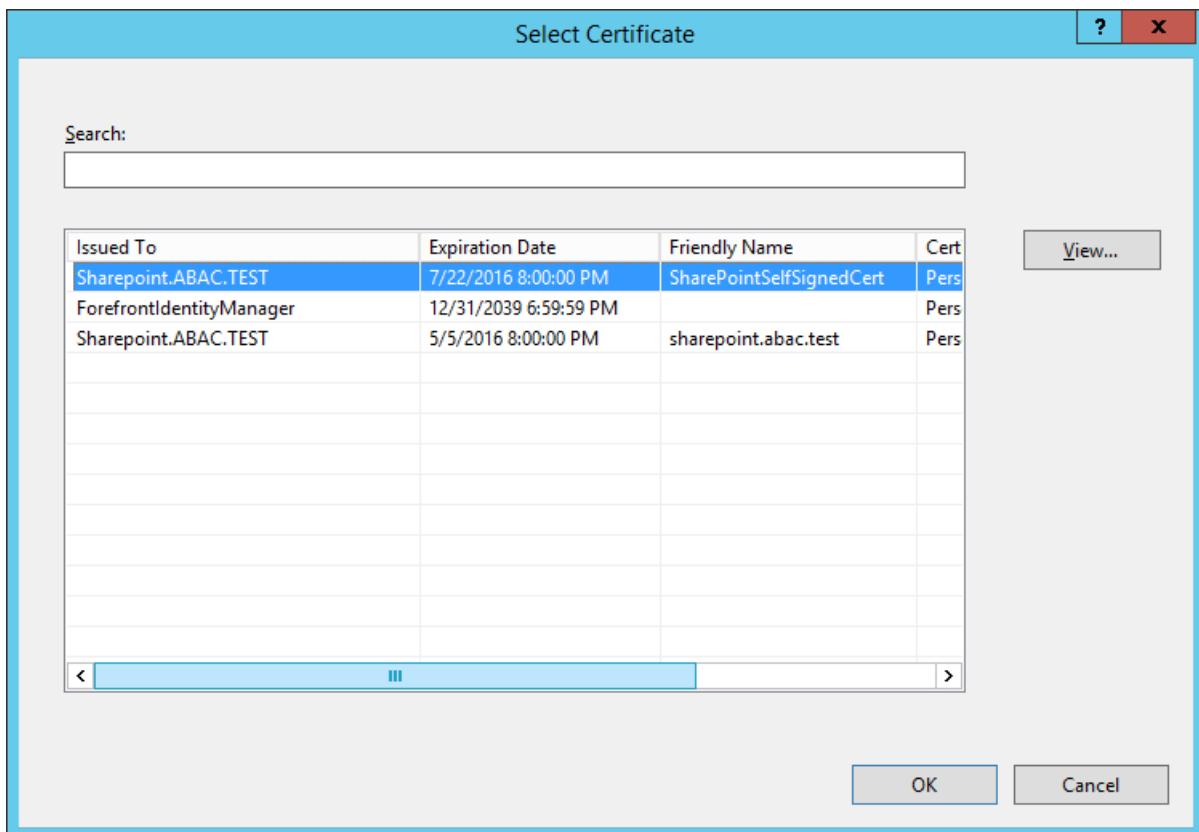
- 2186 6. In the Edit Site Binding window next to the SSL certificate field, click **Select**.

SECOND DRAFT



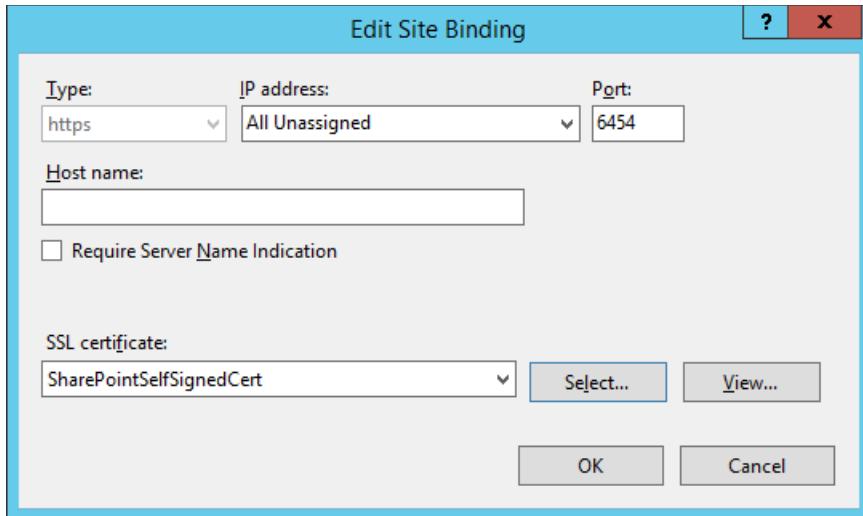
2187

- 2188 7. In the Select Certificate window, click on the certificate created in previous steps and click **OK**.

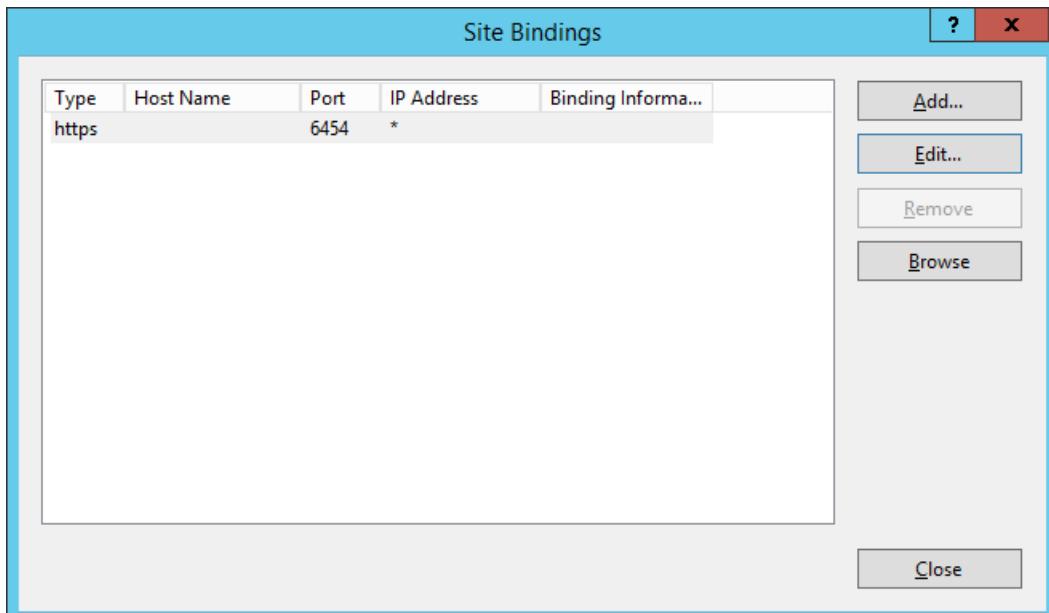


2189

- 2190 8. In the Edit Site Binding window, verify that your SSL certificate is listed, then click **OK**.



2191

2192 9. In the Site Bindings window, click **Close**.

2193

2194 4.4.2 Certificates Signed by Local or Online Certificate Authority

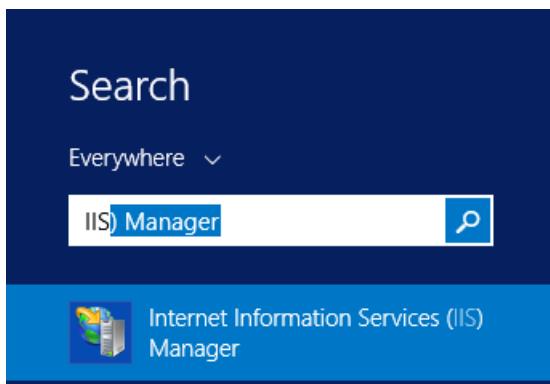
2195 Instead of using self-signed certificates which can be used in protected lab environments, it is
 2196 recommended that you use certificates signed by a Certificate Authority. For our build, we used
 2197 Symantec's Managed PKI Service to sign our certificates using a local Certificate Authority. Certificates
 2198 were used to support various exchanges that require encryption, such as digital signature, SAML
 2199 message encryption, and encryption of TLS communications.

2200 Although the detailed instructions of configuring certificates signed by a certificate authority vary by
2201 vendor product, the general process is described below. For each certificate, you perform the following
2202 high-level steps:

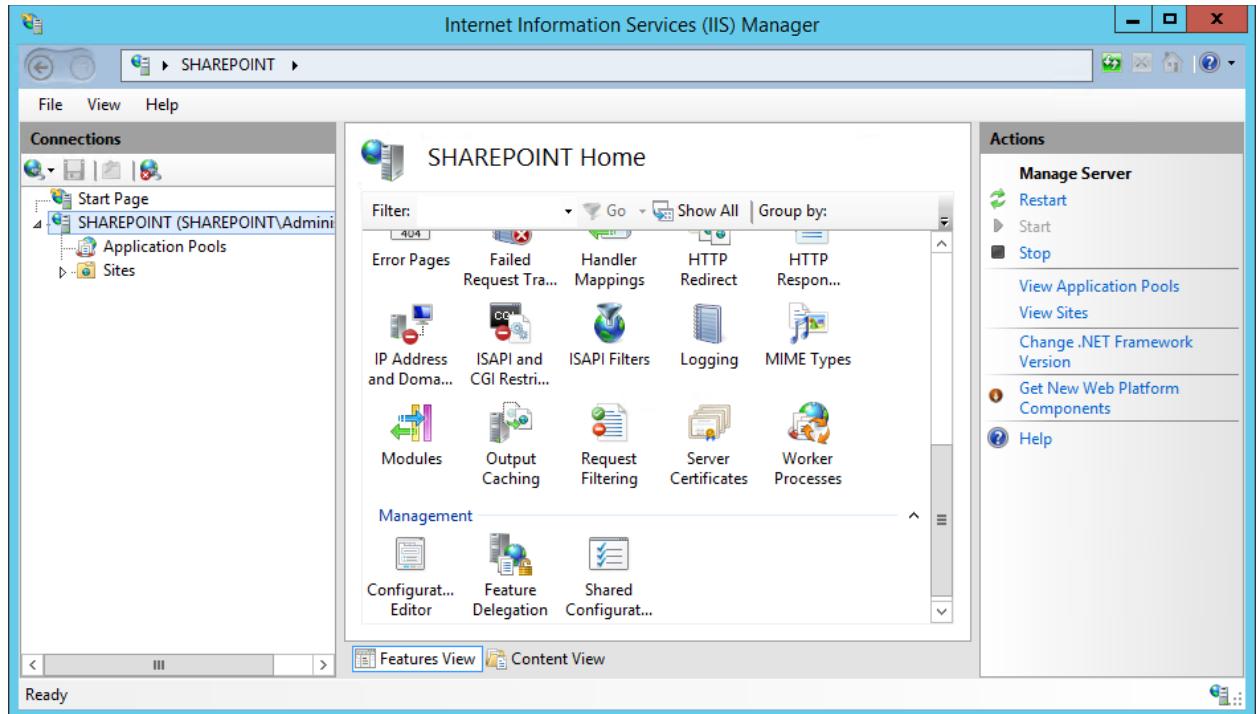
- 2203 1. Using the vendor product (e.g., SharePoint), generate a certificate signing request on the server
2204 where you want to use the certificate. Save the signing request to a file.
- 2205 2. Submit an enrollment request to your certificate authority. You will need to provide the signing
2206 request that was generated in step 1. This step is typically where you provide information such
2207 as the name of the server on which you intend to use the certificate (e.g.,
2208 "sharepoint.abac.test").
- 2209 3. A representative at the certificate authority will examine the enrollment request and approve it.
2210 The representative will issue a certificate response signed with the certificate authority's key.
2211 You can download the signed response. If you are using a certificate authority that is locally
2212 managed by your organization, you will also need to download the public key of the certificate
2213 authority because you will need to add this to the Trusted Certificate Authorities on each server
2214 and client that will be using the certificates.
- 2215 4. Go back to the vendor product where you created the certificate signing request. If you are using
2216 a local certificate authority, you will first need to add the certificate authority's public key to the
2217 list of Trusted Certificate Authorities.
- 2218 5. Import the certificate file for your server that was signed by the certificate authority.

2219 **4.4.2.1 Generating a Certificate Signing Request (CSR)**

- 2220 1. Log into the server where SharePoint Server 2013 is installed (e.g., SharePoint Server in our
2221 build).
- 2222 2. Click on the **Windows** icon in the bottom left corner of your screen.
- 2223 3. Begin typing **IIS**.
- 2224 4. When the **Internet Information Services (IIS) Manager** appears, click on it.

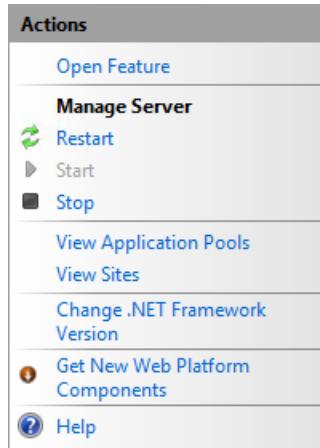


- 2225
- 2226 5. In the left-hand Connections column, left-click on your **SharePoint** instance.
 - 2227 6. Scroll down in the SharePoint Home pane and left-click on **Server Certificates**.



2228

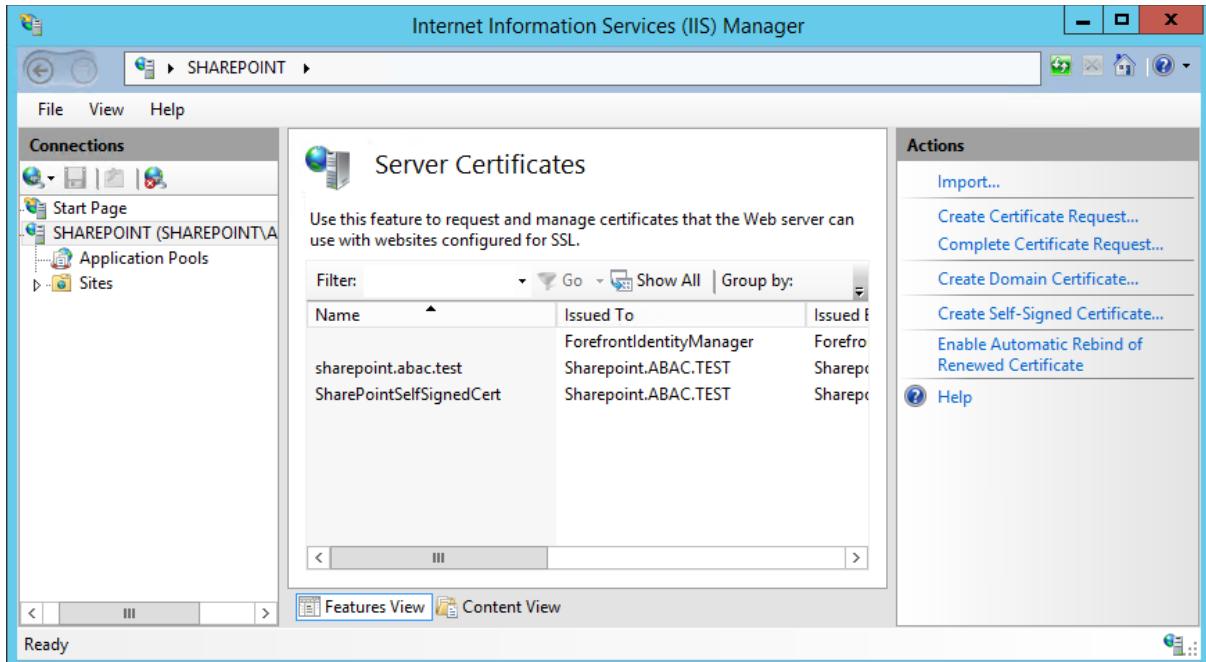
- 2229 7. In the right-hand Actions column, click on **Open Feature**.



2230

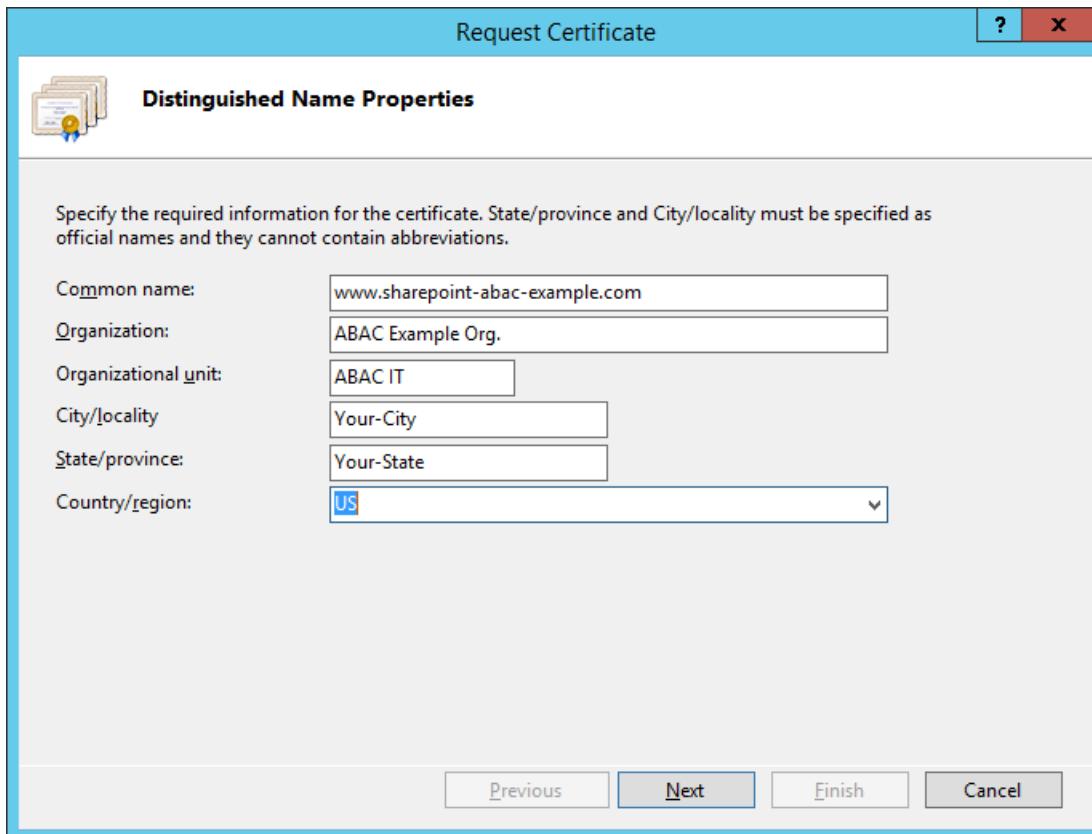
- 2231 8. In the Server Certificates pane, in the right-hand Actions column, click on **Create Certificate Request**.
- 2232

SECOND DRAFT



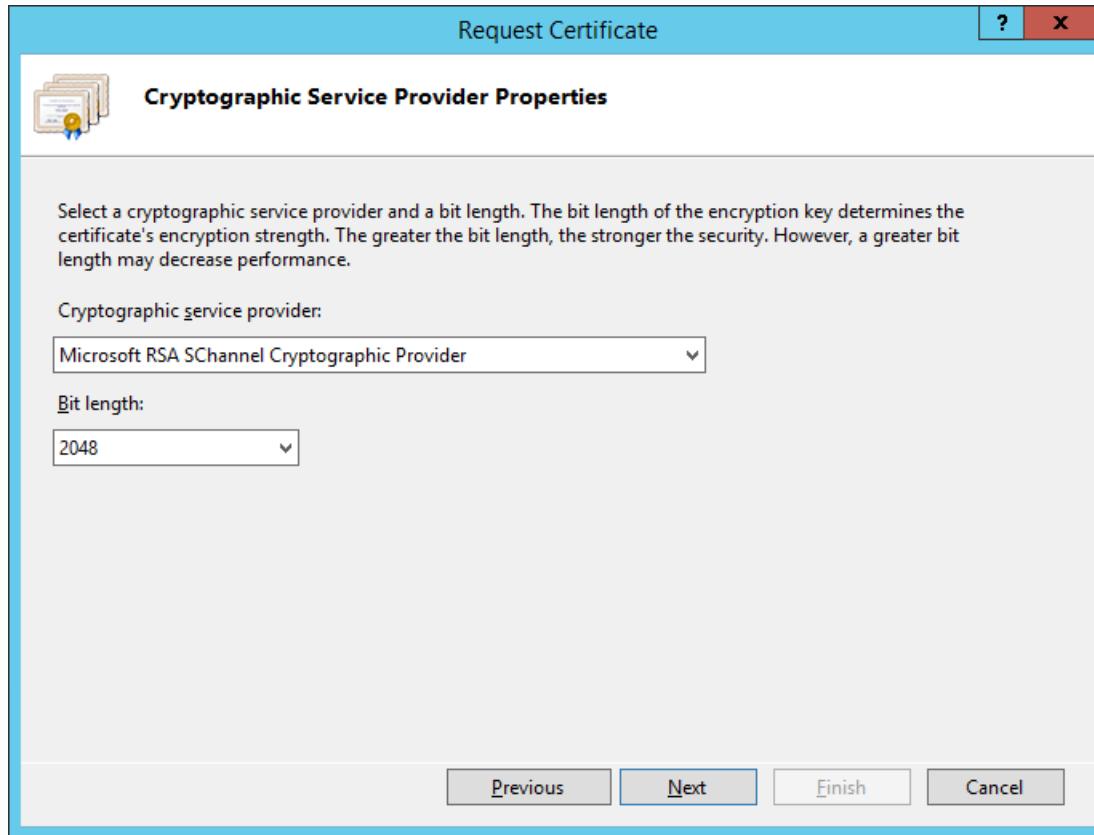
2233

- 2234 9. In the Distinguished Name Properties window that opens automatically, enter your
2235 organizational information and click **Next**.



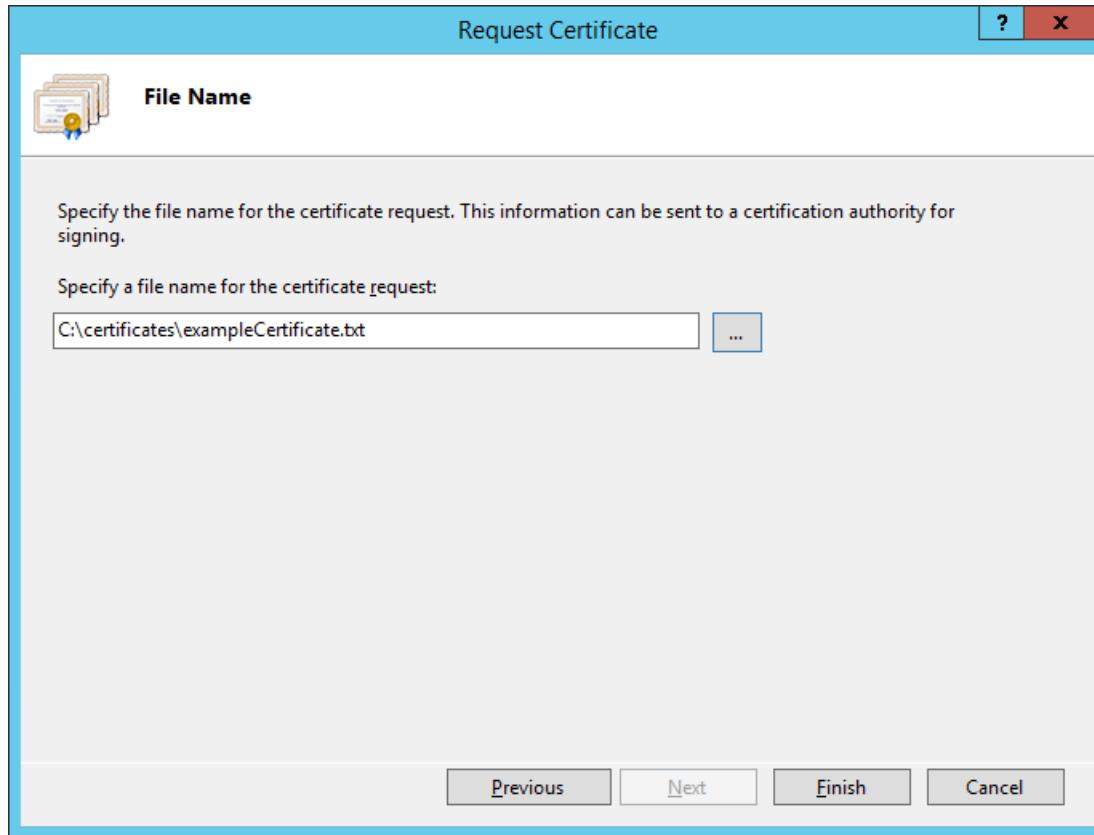
2236

- 2237 10. In the Cryptographic Service Provider Properties window that opens automatically, choose the
2238 **Cryptographic service provider** and a **Bit length**, then click **Next**.



2239

- 2240 11. On the File Name screen, browse to the location where you would like to save this certificate or
2241 type in the path, including a name for your certificate ending in ".txt," then click **Finish**.

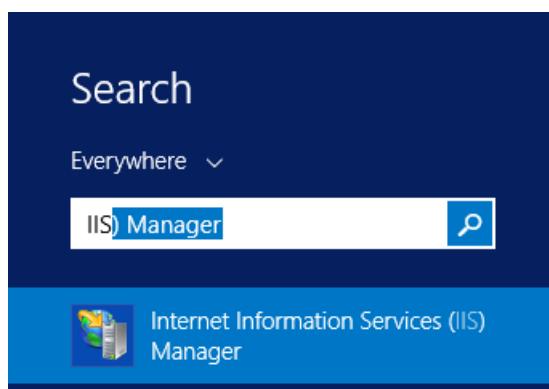


2242

2243 4.4.2.2 *Installing the new signed SSL Certificate*

2244 When the new signed SSL Certificate is available either from a local or online Certificate Authority, install
2245 the certificate using the instructions in this section.

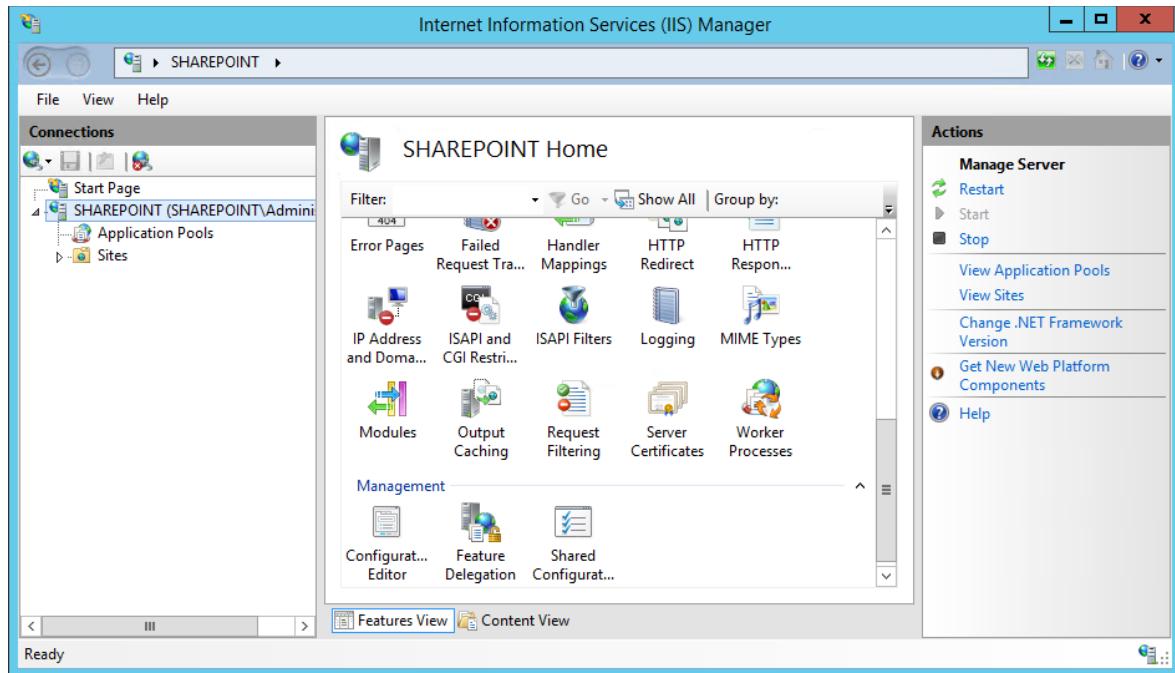
- 2246 1. Log onto the SharePoint Server and save the SSL certificate resulting from the CSR in [Section 4.2.1](#).
- 2247 2. Click on the **Windows** icon in the bottom left corner of your screen.
- 2248 3. Begin typing **iis**.
- 2249 4. When the **Internet Information Services (IIS) Manager** appears, click on it.



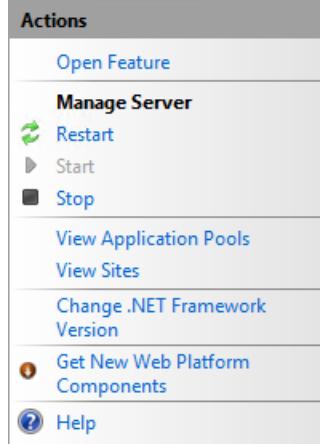
2251

SECOND DRAFT

- 2252 5. In the left-hand Connections column, left-click on your **SharePoint** instance.
- 2253 6. Scroll down in the SharePoint Home pane and left-click on **Server Certificates**.

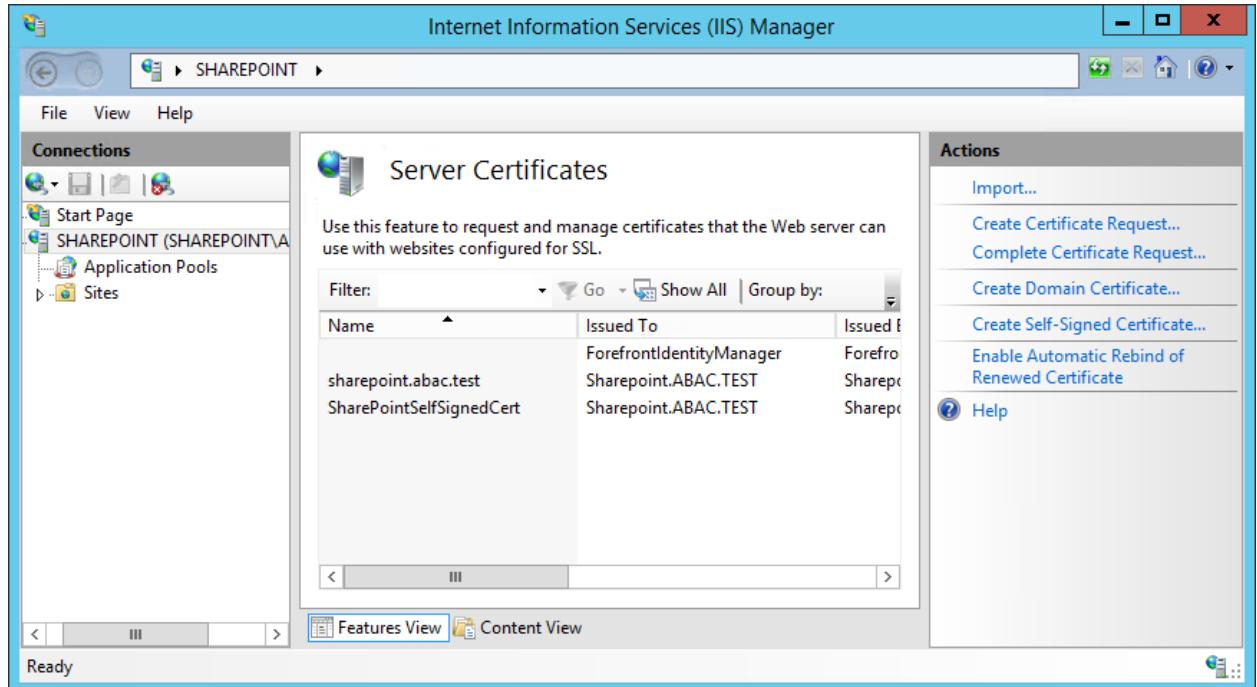


- 2254
- 2255 7. In the right-hand Actions column, click on **Open Feature**.



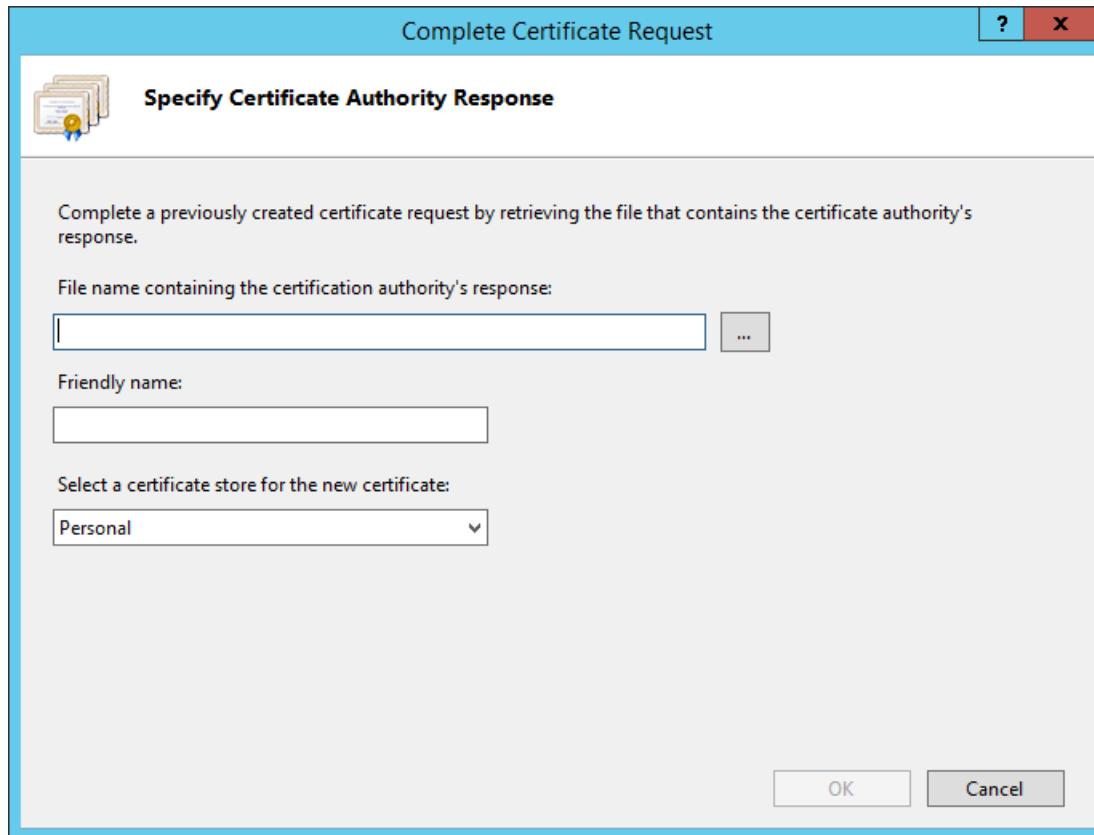
- 2256
- 2257 8. In the Server Certificates pane, in the right-hand Actions column, click on **Complete Certificate Request**.
- 2258

SECOND DRAFT



2259

- 2260 9. In the Complete Certificate Request wizard on the Specify Certificate Authority Response screen,
2261 browse to the location of the new SSL certificate generated from your CSR or type in its location,
2262 enter a friendly name, and choose a certificate store from the drop-down menu. Click **OK**.



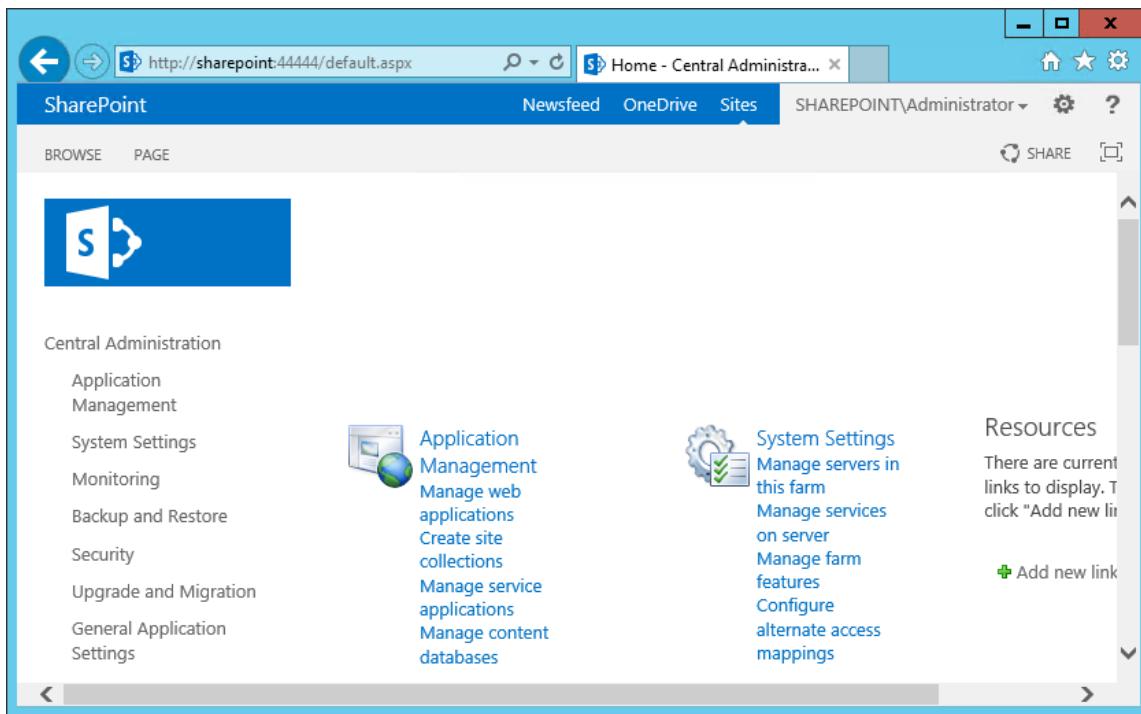
2263

2264 4.4.2.3 Configure the CA-Signed Certificate

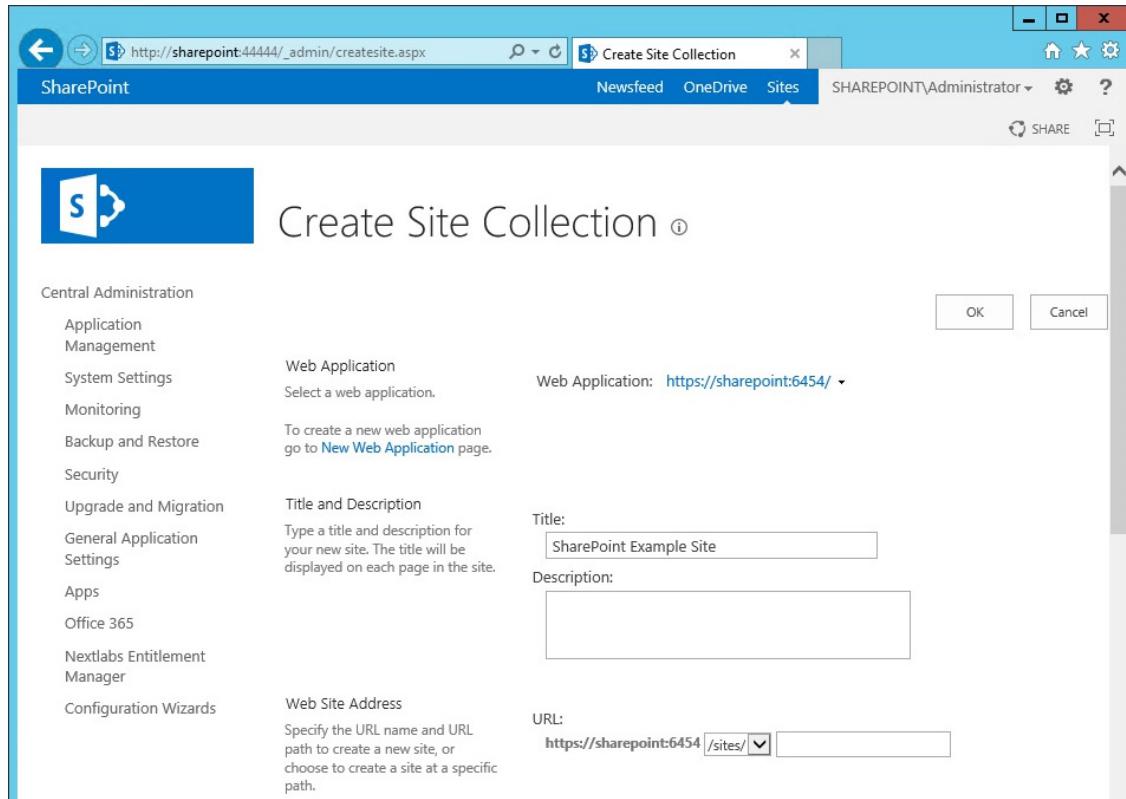
2265 Follow the steps listed in [Section 4.4.1.4](#) to configure IIS Binding for the new SSL certificate signed by a
 2266 local or online Certificate Authority. You can choose port 443 or any other available port if you prefer to
 2267 use a non-standard port for SSL traffic.

2268 4.5 Creating a Site Collection

- 2269 1. On the SharePoint Server, open a web browser.
- 2270 2. In the **URL address bar** of the browser, enter the address for Central Administration and click
 Enter or Go: `http://sharepoint:44444/default.aspx`
- 2272 3. From the Central Administration page, in the Application Management section, click on **Create**
 2273 **site collections**.



- 2274 4. On the Create Site Collection page, do the following:
- 2275 a. Verify that the web application under consideration is the one chosen.
- 2276 b. Enter a **Title** (required) and **Description** (optional).
- 2277 c. Choose the web site address you prefer for your site (in this build,
 2279 `https://sharepoint:6454/`).



2280

- 2281 5. In the browser, scroll down to the Template Selection area and Primary Site Collection
2282 Administrator area of the Create Site Selection page and do the following:
- 2283 a. Choose the **version** and **template** (e.g., 2013 Team Site)
- 2284 b. In the **User name** field, under the Primary Site Collection Administrator area, type in the
2285 name of your SharePoint Administrator account and click on the **Name check** icon. If the
2286 name is found, it will not give a warning and the name will be underlined.
- 2287 i. Alternatively, you can look up users by name using the address book people
2288 picker mechanism next to the user name text field.
- 2289 c. In the **User name** field under the Primary Site Collection Administrator area, type in the
2290 name of a secondary administrator if you so choose.
- 2291 i. Alternatively, you can look up users by name using the address book people
2292 picker mechanism next to the user name text field.

SECOND DRAFT

The screenshot shows the 'Create Site Collection' page in SharePoint. At the top, there's a navigation bar with 'SharePoint', 'Newsfeed', 'OneDrive', 'Sites', 'SHAREPOINT\Administrator', and a gear icon. Below the navigation, the page title is 'Template Selection'. A dropdown menu for 'Select experience version' shows '2013' selected. Under 'Select a template', the 'Team Site' tab is active, showing options like 'Blog', 'Developer Site', 'Project Site', and 'Community Site'. A description below says 'A place to work together with a group of people.' In the 'Primary Site Collection Administrator' section, the user name is set to 'SharepointAdmin'. In the 'Secondary Site Collection Administrator' section, the user name field is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

2293

2294 6. Scroll down in the browser to the Quota Template area of the Create Site Collection page. Leave the default choice **No Quota** chosen. Click **OK**.

2295

Quota Template

Select a predefined quota template to limit resources used for this site collection.

To add a new quota template, go to the [Manage Quota Templates](#) page.

Select a quota template:

No Quota

Storage limit:

Number of invited users:

OK Cancel

2296

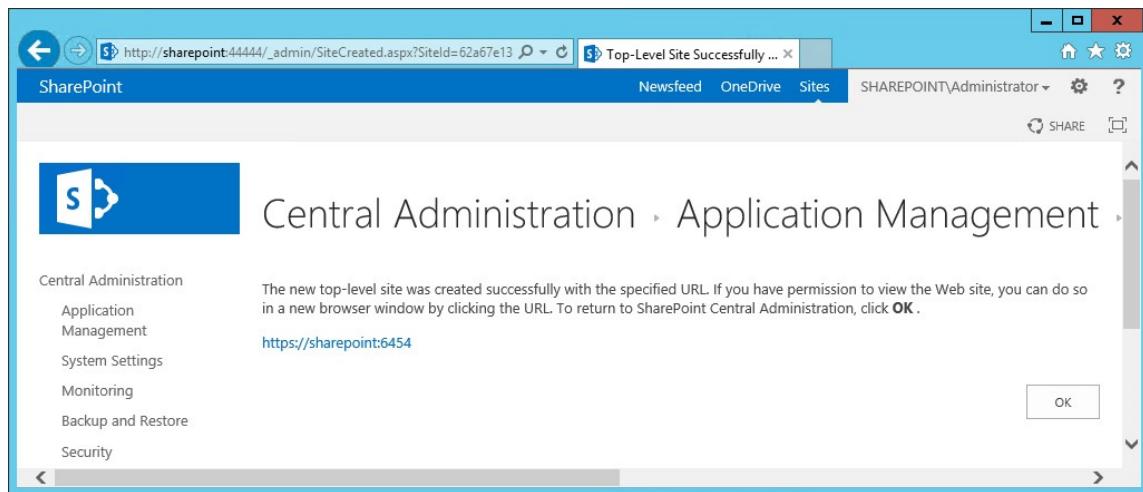
2297 7. Wait for the Site Collection to successfully complete.

Working on it...

⌚ This shouldn't take long.

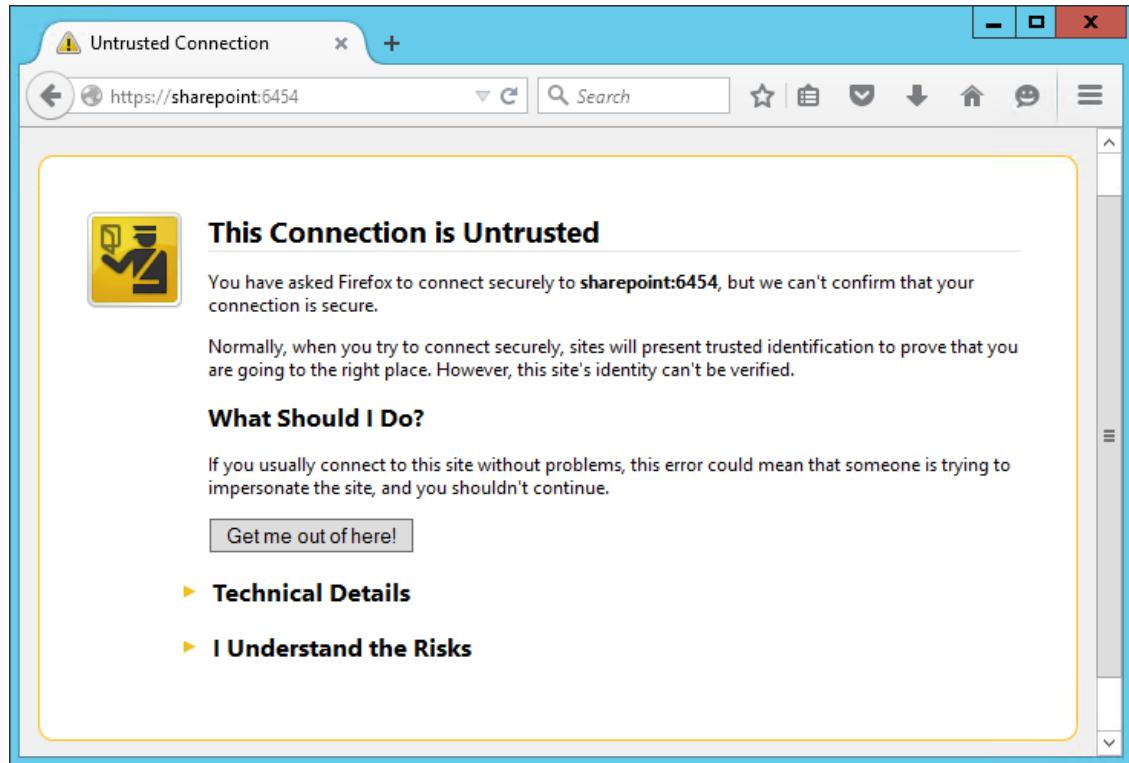
2298

- 2299 8. In the browser, on the page that indicates a new top-level site was created successfully, click
2300 OK.



2301

- 2302 9. Open a browser and navigate to the URL for your new web application (e.g.,
2303 <https://sharepoint:6454>)
2304 a. You may see a warning first because of the self-signing certificate.



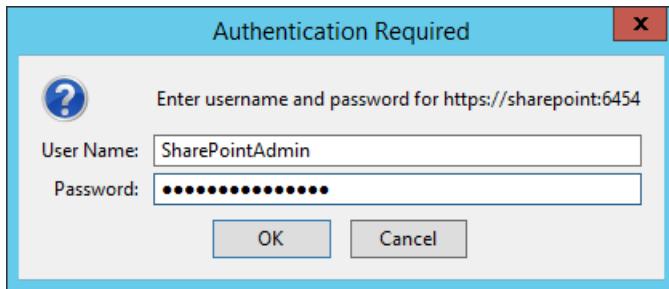
2305

- 2306 b. In the browser window, click on **I Understand the Risks**, then **Add Exception**.
- 2307 c. In the Add Security Exception window, click on **Confirm Security Exception**.



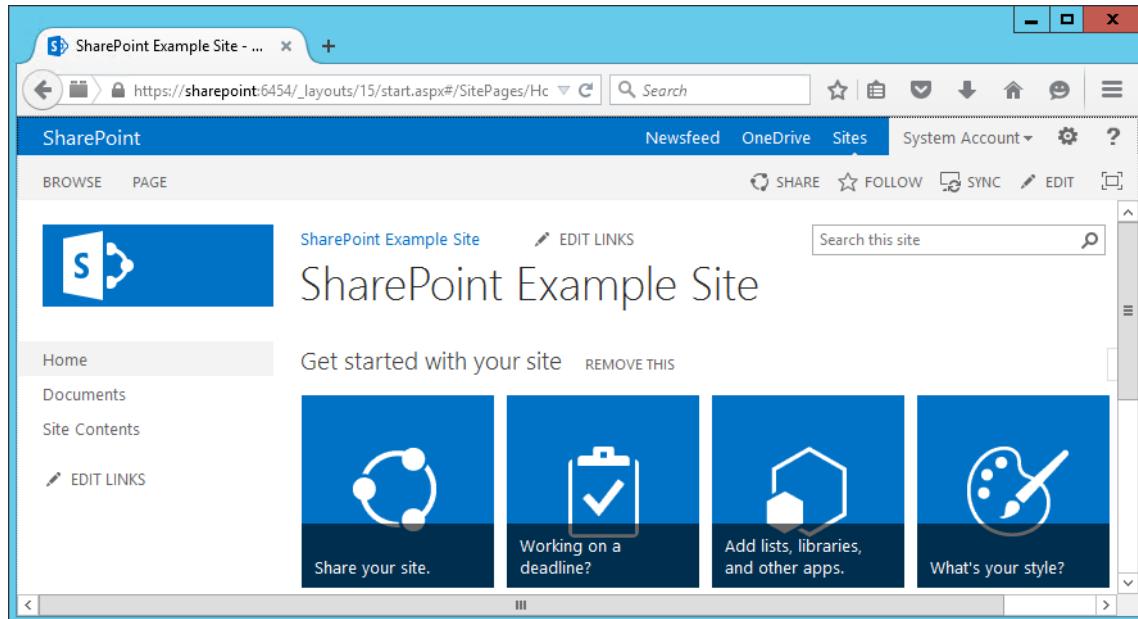
2308

- 2309 10. In the Authentication Required window that opens automatically, enter the administrator account **User Name** and **Password**, then click **OK**.
- 2310



2311

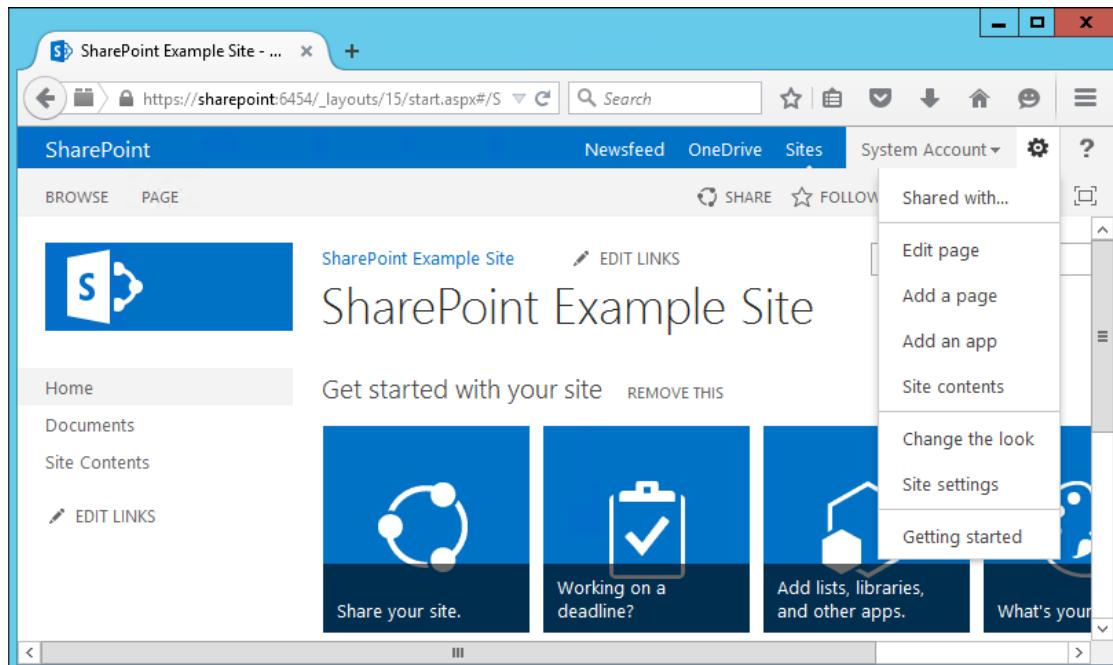
- 2312 11. Upon verification that the login was a success, you will see default site contents.



2313

2314 4.6 Creating New Sub-Sites

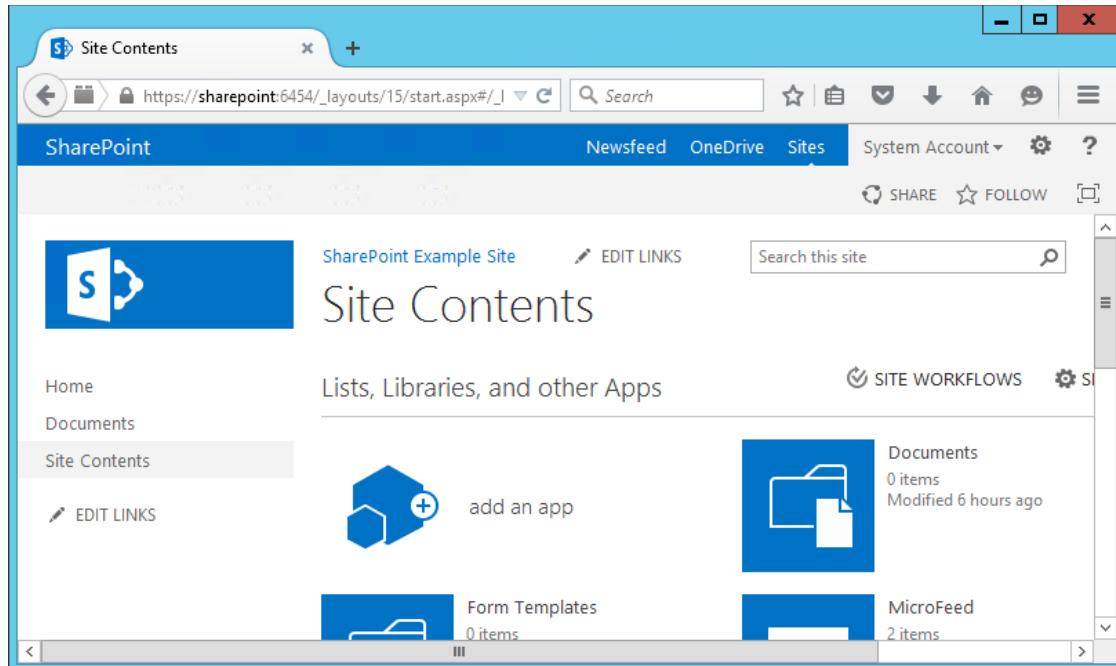
- 2315 1. After logging into your site, in your browser window click the **gear symbol** next to the
2316 Administrator login area, then click on **Site Contents**.



2317

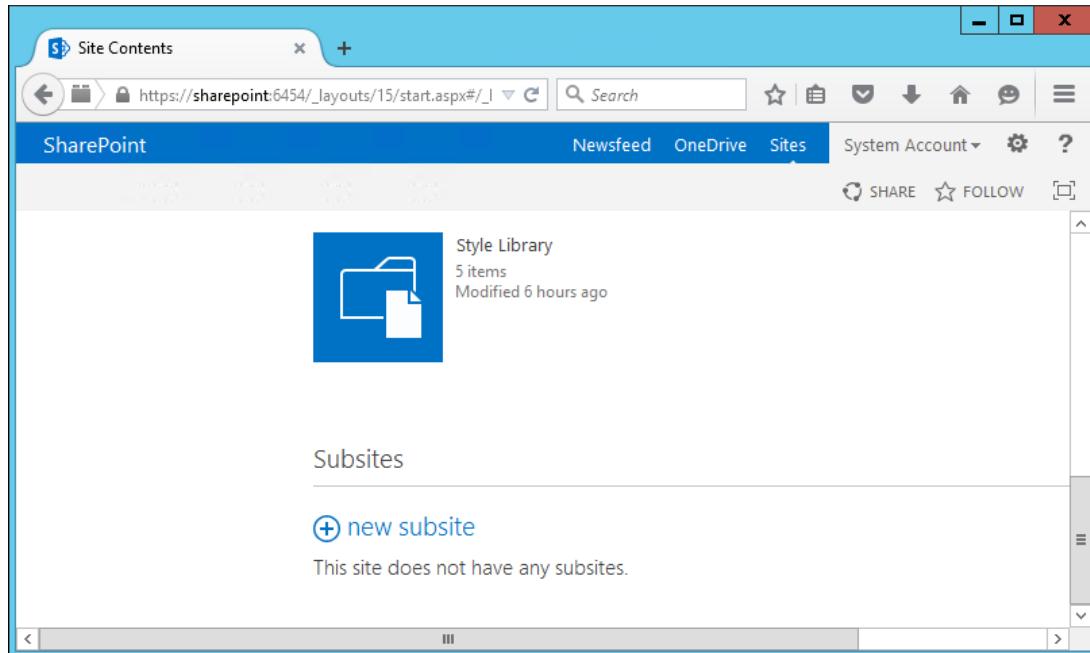
- 2318 2. In the browser window, the Site Contents page will open.

SECOND DRAFT



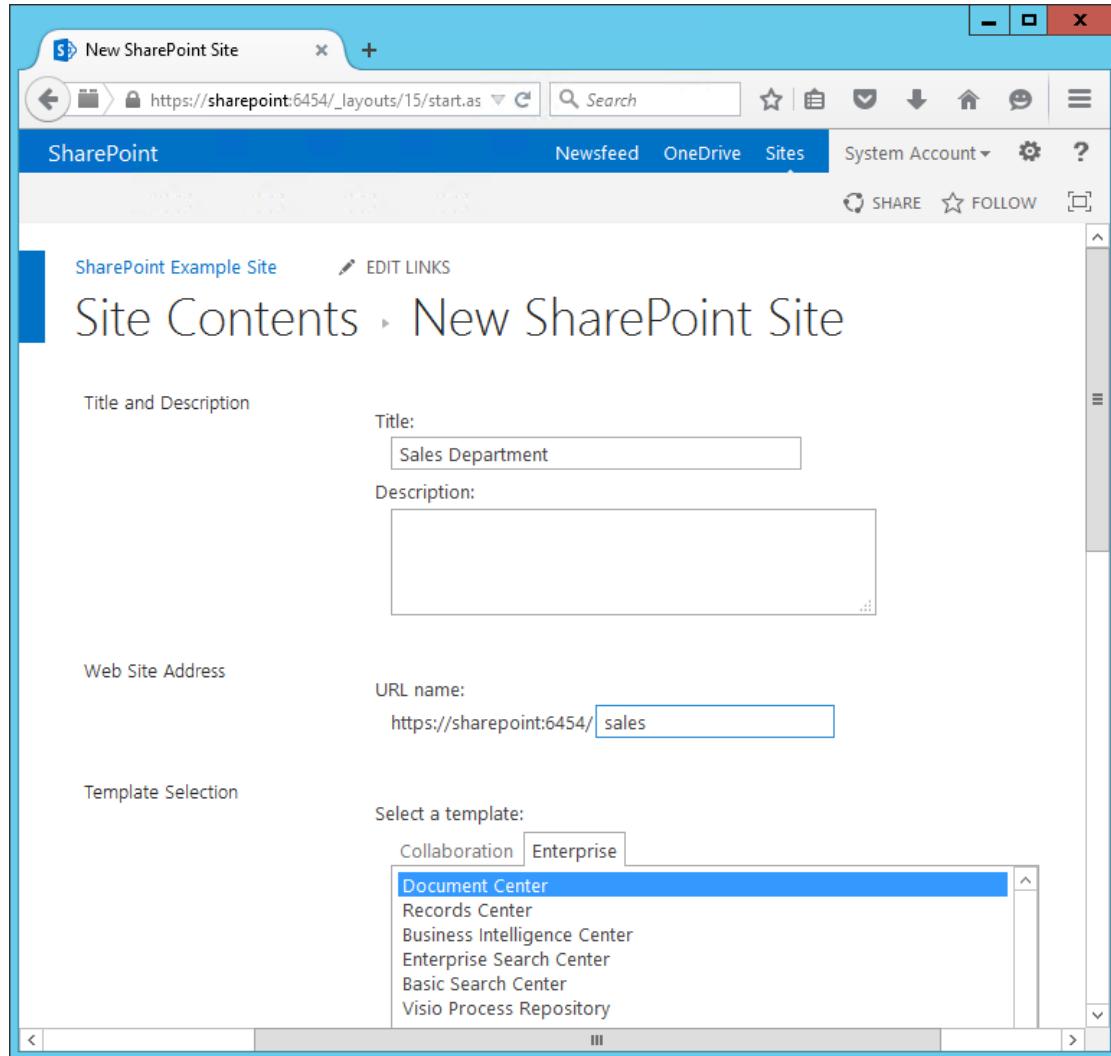
2319

- 2320 3. In the browser window, scroll down to the Subsites area and click the **plus sign button** next to
2321 new subsite.



2322

- 2323 4. In the browser window on the New SharePoint Site screen, do the following:
2324 a. Enter **Title** (required) and **Description** (optional).
2325 b. Enter a **URL name**.
2326 c. **Select a template**.



2328 5. In your browser, scroll down and do the following:

- 2329 a. Choose **User Permissions** (in our build, we left the Use same permissions as parent site
2330 radio button selected).
- 2331 b. Choose your **Navigation** and **Navigation Inheritance** settings.

SECOND DRAFT

The screenshot shows the 'Permissions' section where users can choose to give permission to access their new site to the same users who have access to the parent site or to give unique permissions. It also includes a note about selecting 'Use same permissions as parent site'. Below this is the 'Navigation' section, which includes options for displaying the site on the Quick Launch and top link bar of the parent site, both of which are set to 'Yes'. The 'Navigation Inheritance' section shows that the top link bar from the parent site will be used.

Permissions

You can give permission to access your new site to the same users who have access to this parent site, or you can give permission to a unique set of users.

Note: If you select **Use same permissions as parent site**, one set of user permissions is shared by both sites. Consequently, you cannot change user permissions on your new site unless you are an administrator of this parent site.

Navigation

Yes No

Yes No

Navigation Inheritance

Yes No

2332

2333 6. In the browser, scroll down and click **Create**.



2334

2335 7. Your new subsite will open in the browser.

The screenshot shows a SharePoint browser window titled 'Home - Sales Department'. The address bar shows the URL as https://sharepoint:6454/sales/default.aspx. The page header includes the SharePoint logo, navigation links for Newsfeed, OneDrive, and Sites, and a System Account dropdown. The main content area displays the 'Sales Department' subsite, featuring a 'Welcome to the Document Center' message and a 'Upload a Document' button. On the left, there is a navigation menu with links for Libraries, Lists, Recent, Documents, Tasks, and Site Contents. The SharePoint Example Site is also visible in the top navigation.

2336

2337 8. Return to the homepage URL <https://sharepoint:6454> and repeat the steps from [Section 4.6](#) to
 2338 create other subsites of interest.

2339 **5 Set Up Federated Authentication at the Relying Party's**
 2340 **SharePoint**

2341 **5.1 Introduction**

2342 In previous sections of this How-To Guide we demonstrated how to set up federated
 2343 authentication between the relying party and the identity provider and how to create the relying party's
 2344 SharePoint site. In this section, we demonstrate how to set up federated authentication between the
 2345 relying party's SharePoint and the PingFederate-RP. Before continuing with this section implementers
 2346 are required to have federation servers at both the identity provider and the relying party as well as a
 2347 working SharePoint instance that is claims-aware. For this build we provide instructions for setting up
 2348 these components in [Section 2](#), [Section 3](#), and [Section 4](#).

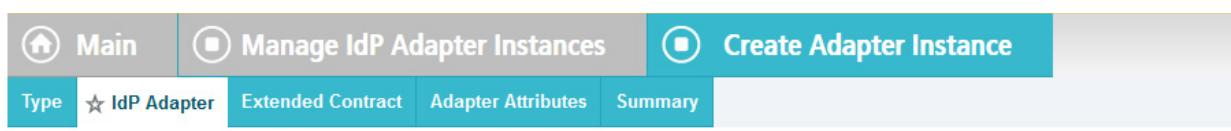
2349 We will demonstrate how to set up a trusted logon provider for the relying party' so that when a user
 2350 requests access to a SharePoint site, the user will be redirected to the PingFederate-RP for
 2351 authentication via WS-Federation. The Ping-Federate-RP will then forward the authentication request to
 2352 the PingFederate-IdP. The PingFederate-IdP will present a logon page to the user. Once the user
 2353 authenticates, the user will be redirected back to the original SharePoint site and will be able to access
 2354 the site because they have a valid authentication token.

2355 As you complete different steps in this section you will be able to verify the correctness or completeness
 2356 of your component configuration and integration in Functional Test sub-sections.

2357 If you follow the instructions in this How-To Guide section, you will be able to perform a Functional Test
 2358 to verify the successful completion of the steps for installing, configuring, and integrating the
 2359 components.

2360 **5.2 Usage Notes on PingFederate**

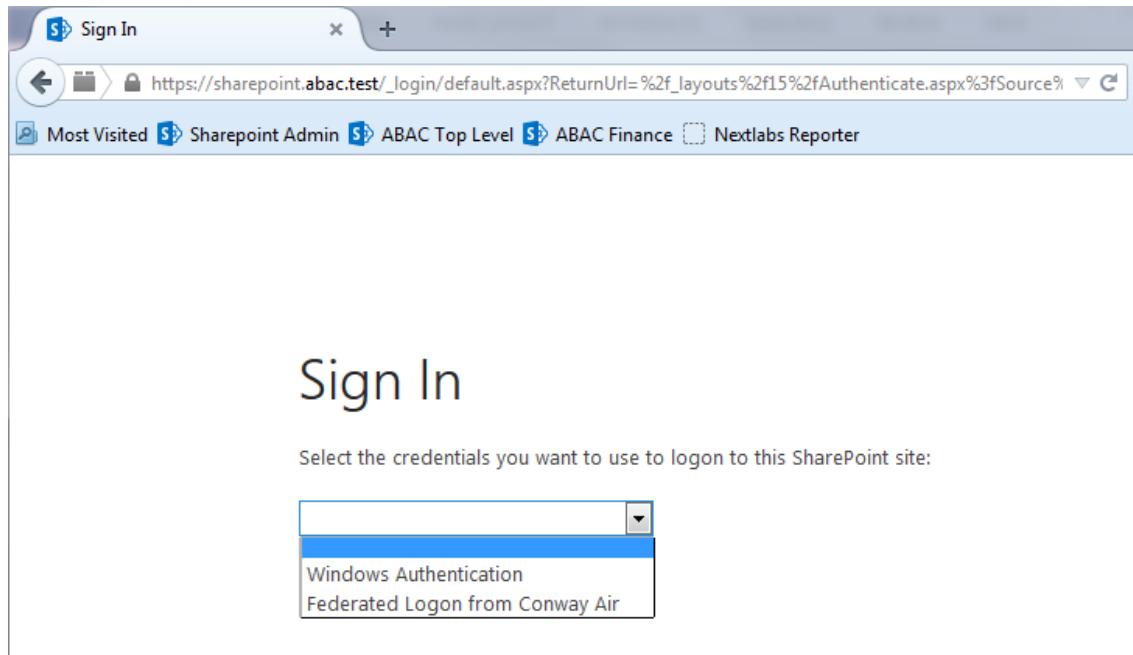
- 2361 ▪ When using the PingFederate application to perform an administrative configuration, there is
 2362 usually a sequence of screens, ending with a summary page. Once you click **Done** on the
 2363 summary page, you must also click **Save** on the following page to save the configurations. If you
 2364 forget to click **Save**, you may inadvertently lose changes to the configuration.
- 2365 ▪ Ping identity refers to the relying party as the **Service Provider** in their PingFederate product
 2366 and associated documentation.
- 2367 ▪ When using the PingFederate application to perform configuration, refer to the title of the tab
 2368 with a small star icon to its left, to easily identify the item you are currently configuring. For
 2369 example, if you navigated to the following screen, you would be on the IdP Adapter screen.



2370

2371 5.3 Configure a SharePoint Federated Logon Provider

2372 Follow the instructions in this section to configure the federated logon provider at the relying party's
 2373 SharePoint site. Once this configuration is complete, the user will see two authentication options when
 2374 first attempting to access the SharePoint site. The first option is to log on using the default **Windows**
 2375 **Authentication**. This option does not use federation. The second option is to use a federated logon.



2376

2377 In order to set up a federated logon, you will configure a trust relationship between the SharePoint
 2378 server and the PingFederate-RP that will facilitate the federated logon. Once a user authenticates via a
 2379 federated logon, the PingFederate-RP will cryptographically sign WS-Federation messages and send
 2380 them to the SharePoint server. The PingFederate-RP must be configured as a trusted identity token
 2381 Issuer in SharePoint, so that SharePoint will accept the messages sent by the PingFederate-RP and allow
 2382 the user access to the SharePoint site.

2383 5.3.1 Setting up the Certificate

2384 Setting up a certificate involves creating the certificate at the from the identity provider, exporting the
 2385 certificate, and importing it in the SharePoint site of the relying party.

- 2386 1. Logon to the server that hosts the PingFederate service for the relying party.
- 2387 2. Launch your browser and go to: *https://<DNS_NAME>:9999/pingfederate/app*.
- 2388 3. Replace **DNS_NAME** with the fully qualified name of the relying party's PingFederate server
 (e.g., *https://rp.abac.test:9999/pingfederate/app*).
- 2390 4. Logon to the PingFederate application using the credentials you configured during installation.

The screenshot shows the PingFederate main menu with three tabs: IdP Configuration, Server Configuration, and SP Configuration. A yellow banner at the top indicates a 'License Violation: Expiration date passed'. The IdP Configuration tab is active, showing sections for Application Integration Settings, Federation Settings, SP Connections (3), and SP Affiliations (0). The Server Configuration tab shows System Settings, Certificate Management, and Administrative Functions. The SP Configuration tab shows Application Integration Settings, Federation Settings, and IDP Connections (2).

2391

2392

- On the Main Menu, under **CERTIFICATE MANAGEMENT**, click **Digital Signing and XML**.

The screenshot shows the Certificate Management page. It has a header with 'Main' and 'Certificate Management'. Below is a section titled 'Manage Digital Signing Certificates' with a note: 'Establish and maintain your server's signing certificates, which may be used to sign assertions, security tokens, requests, and responses. These certificates may also be used for XML decrytion.' A table lists four certificates:

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTION
01:30:DB:8C:D4:83	CN=localhost, O=Quick Start App, C=US	Fri Jun 05 06:18:17 PDT 2111	RSA 1024	Valid	Export Certificate Signing Delete
01:30:DB:8C:25:AB	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US	Fri Jun 05 06:17:32 PDT 2111	RSA 1024	Valid	Export Certificate Signing Delete (Check Usage)
01:4C:09:35:30:19	CN=demo-sp-enc, O=NCCoE, C=US	Thu Mar 10 07:20:22 PST 2016	RSA 2048	Valid	Export Certificate Signing Delete (Check Usage)

At the bottom are buttons for 'Create New...' and 'Import...'

2393

2394

2395

2396

- Locate the certificate that will be used to sign messages that will be sent to the SharePoint server. In the example screenshot above, this certificate has CN with the value **demo dsig new**. Click on the **Export** link for this certificate in the **ACTION** column.

The screenshot shows a navigation bar with three tabs: 'Main', 'Certificate Management', and 'Export Certificate'. The 'Export Certificate' tab is active and highlighted in blue. Below the tabs, there is a breadcrumb trail: 'Export Certificate > Export & Summary'. A message box at the top states: 'You have a choice of exporting the certificate and the key or just the certificate.' Below this, there are two radio button options: 'Certificate Only' (selected) and 'Certificate and private key'. At the bottom right of the page are 'Cancel' and 'Next >' buttons.

2397

2398

7. Select **Certificate Only** and click **Next**.

The screenshot shows a navigation bar with three tabs: 'Main', 'Certificate Management', and 'Export Certificate'. The 'Export Certificate' tab is active and highlighted in blue. Below the tabs, there is a breadcrumb trail: 'Export Certificate > Export & Summary'. A message box at the top states: 'Click the Export button to export this certificate to the file system.' Below this, there is a section titled 'Export Certificate' with a sub-section 'EXPORT CERTIFICATE'. It displays the following certificate details in a table:

Subject DN	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
Issuer DN	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
Serial Number	01:30:DB:8C:25:AB
Expires	Fri Jun 05 06:17:32 PDT 2111

At the bottom left is an 'Export' button, and at the bottom right are 'Cancel', '< Previous', and 'Done' buttons.

2399

2400

8. On the Export & Summary page, click the **Export** button on the left side of the page. Save the file to the hard drive and rename it to **federation.cer**.

2402

2403

9. Using the SharePoint administrator credentials, logon to the server that hosts SharePoint for the relying party.

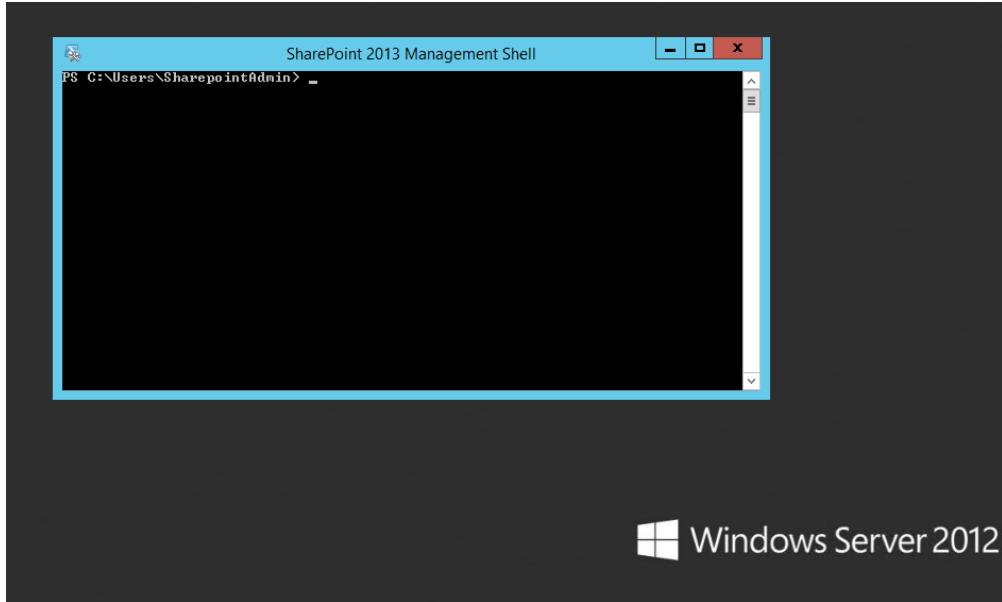
2404

10. Copy the **federation.cer** file to the desktop on the SharePoint server.

2405

2406

11. Click on the **Start** menu and navigate to the SharePoint 2013 Products group. Open the SharePoint 2013 Management Shell.



2407

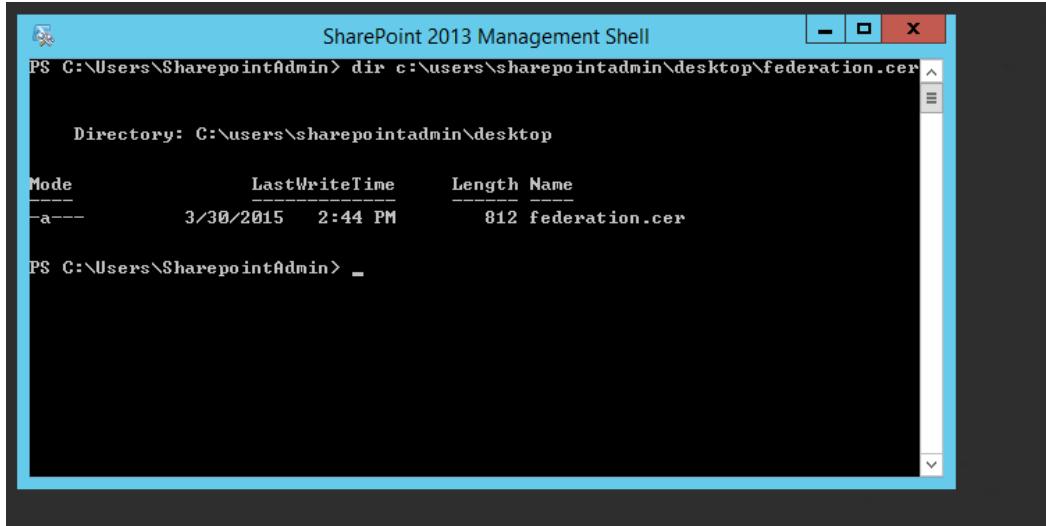
- 2408 12. To verify that you placed the federation.cer file to the desktop, enter the following command
2409 into the Management Shell (using the correct path for your server).

2410

```
dir c:\users\sharepointadmin\Desktop\federation.cer
```

2411

You should see information about the file such as the LastWriteTime.



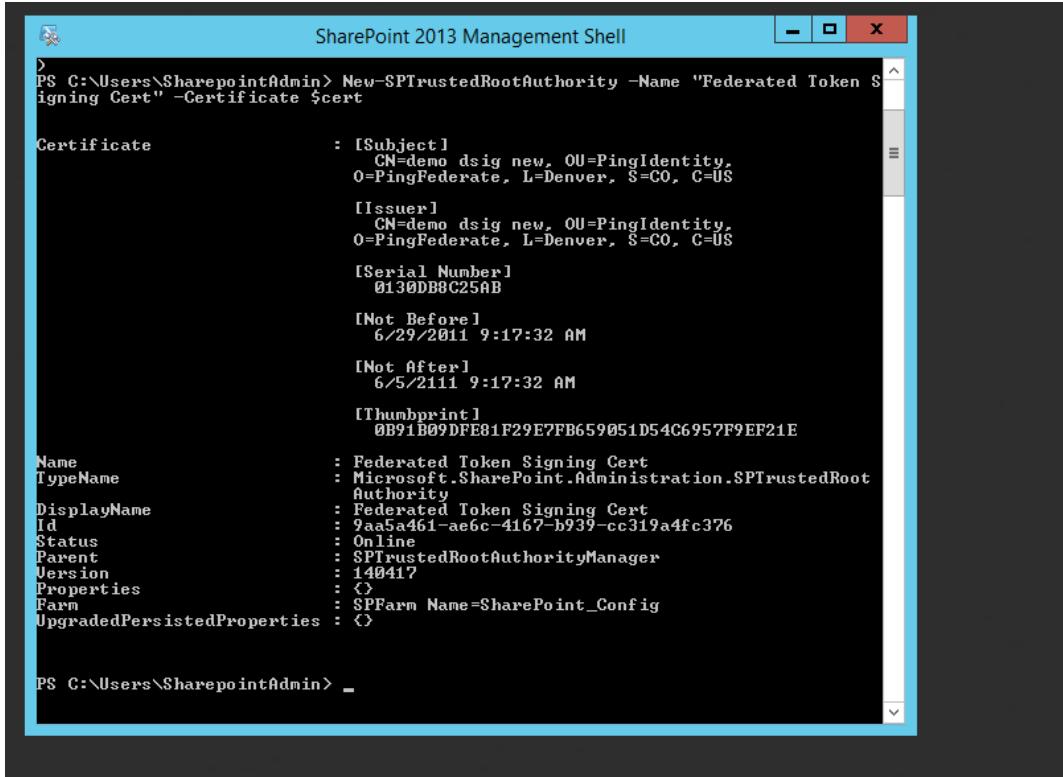
2412

- 2413 13. Enter the following commands into the Management Shell to import the PingFederate-RP's
2414 signing certificate (using the correct path for your server):

```
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate
$cate2 ("C:\users\sharepointadmin\Desktop\federation.cer")  
  
New-SPTtrustedRootAuthority -Name "Federated Token Signing Cert" -Certificate
$cert
```

2419

SharePoint responds by displaying details about the imported certificate.



```

SharePoint 2013 Management Shell
PS C:\Users\SharepointAdmin> New-SPTrustedRootAuthority -Name "Federated Token Signing Cert" -Certificate $cert

Certificate : [Subject]
              CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, S=CO, C=US

              [Issuer]
              CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, S=CO, C=US

              [Serial Number]
              0130DB8C25AB

              [Not Before]
              6/29/2011 9:17:32 AM

              [Not After]
              6/5/2111 9:17:32 AM

              [Thumbprint]
              0B91B09DFE81F29E7FB659051D54C6957F9EF21E

Name          : Federated Token Signing Cert
TypeName      : Microsoft.SharePoint.Administration.SPTrustedRootAuthority
DisplayName   : Federated Token Signing Cert
Id            : 9aa5a461-ae6c-4167-b939-cc319a4fc376
Status        : Online
Parent        : SPTrustedRootAuthorityManager
Version       : 14041?
Properties    : <>
Farm          : SPFarm Name=SharePoint_Config
UpgradedPersistedProperties : <>

PS C:\Users\SharepointAdmin> _

```

2420

5.3.2 Configuring the Trusted Identity Token Issuer

To configure a new Trusted Identity Token Issuer, enter each of the commands displayed below the next paragraph into the Management Shell to configure a new Trusted Identity Token Issuer. Enter each command separately, and enter a Carriage Return after the command. If the command executed successfully, Management Shell will not provide any feedback. If an error occurs, Management Shell will display the error.

In the example commands below, the attribute **upn** is configured. You can replace **upn** with an attribute that is appropriate for your environment. The realm value (e.g., **urn:SharePoint.abac.test**) must be identical to the realm value configured in the relying party's PingFederate Service Provider (SP) connection that will be configured later in this section. The signInURL should be configured with the PingFederate-RP WS-Federation URL (e.g., <https://rp.abac.test:9031/idp/prp.wsf>). In this example, the name given to this new token issuer in SharePoint is **Federated Logon from Identity Provider**. The issuer name will be displayed in SharePoint administration screens and to the end user on the Sign On screen.

```

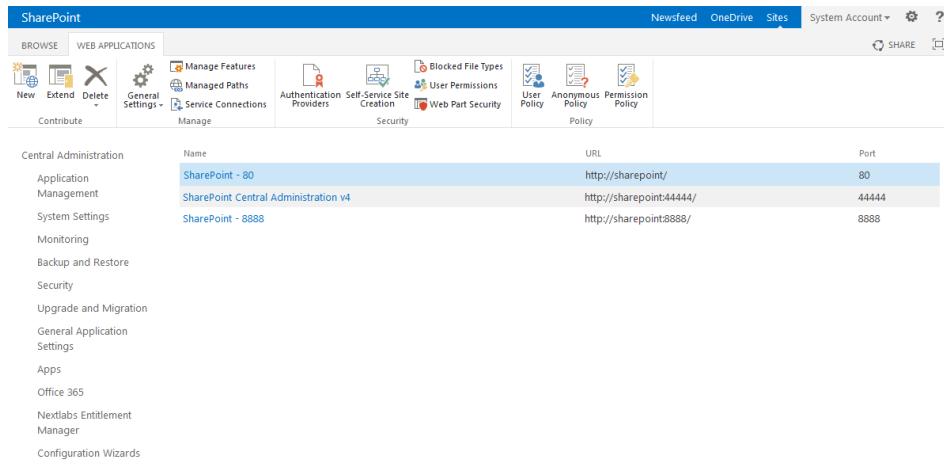
2434 $claimmap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" -IncomingClaimTypeDisplayName
2435 "upn" -SameAsIncoming
2436
2437 $realm = "urn:SharePoint.abac.test"
2438 $signInURL = https://rp.abac.test:9031/idp/prp.wsf
2439 $ap = New-SPTrustedIdentityTokenIssuer -Name "Federated Logon from Identity Provider" -Description "Federated Logon" -realm $realm -ImportTrustCertificate
2440 $cert -ClaimsMappings $claimmap -SignInUrl $signInURL -IdentifierClaim $claimmap.InputClaimType
2441
2442

```

2443 5.3.3 Configuring the Token Issuer as a Sign On Option

2444 After configuring the new Trusted Identity Token Issuer, configure the new token issuer as a Sign On
 2445 option for the SharePoint site.

- 2446 1. Launch your browser and go the SharePoint central administration page (e.g.,
 2447 <http://SharePoint.abac.test:44444/default.aspx>).
- 2448 2. Logon using the credentials of the SharePoint administrator
- 2449 3. In the **Application Management** group, click on **Manage web applications**.
- 2450 4. Click on the web application that contains the SharePoint site you are managing (e.g.,
 2451 **SharePoint – 80**). SharePoint will highlight the web application row that you clicked on.



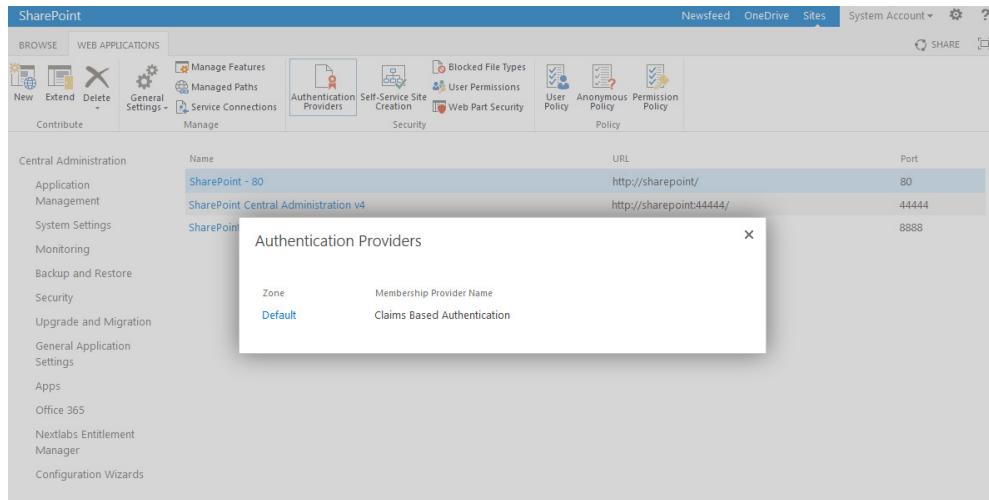
The screenshot shows the SharePoint Central Administration interface under the 'WEB APPLICATIONS' tab. The 'Manage Web Applications' section is active. A table lists three web applications:

	Name	URL	Port
Central Administration	SharePoint - 80	http://sharepoint/	80
	SharePoint Central Administration v4	http://sharepoint:44444/	44444
	SharePoint - 8888	http://sharepoint:8888/	8888

The left sidebar includes links for Central Administration, Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, Apps, Office 365, Nextlabs Entitlement Manager, and Configuration Wizards.

2452

- 2453 5. Click on the **Authentication Providers** button at the top of the page.



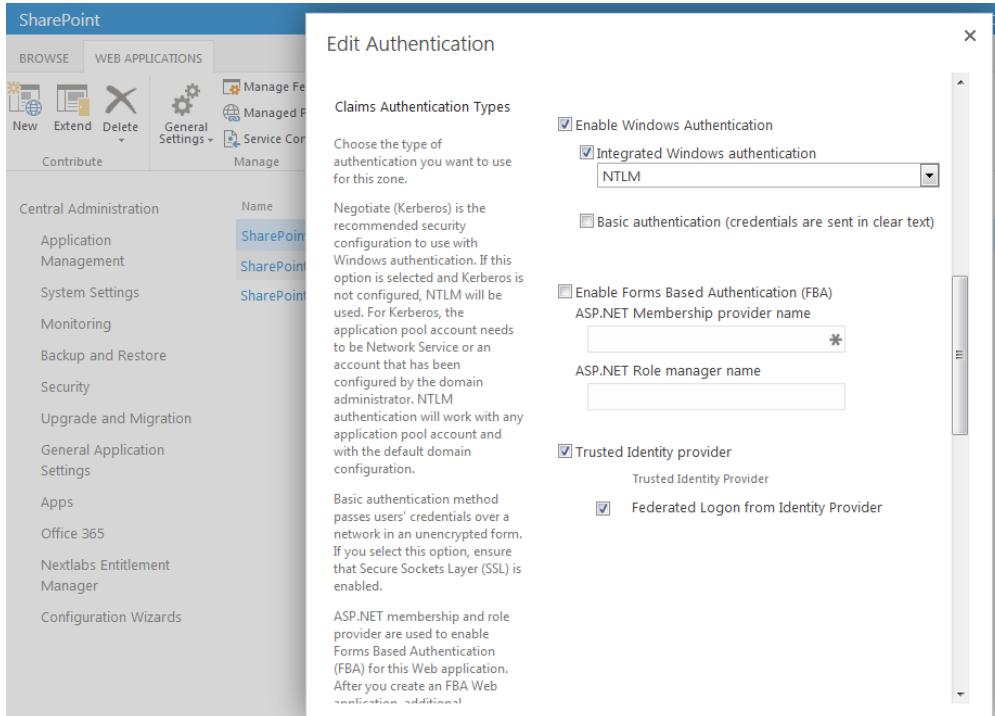
The screenshot shows the same SharePoint Central Administration interface as before, but with a modal dialog box titled 'Authentication Providers' overlaid on the 'SharePoint - 80' row. The dialog box contains the following information:

Zone	Membership Provider Name
Default	Claims Based Authentication

2454

- 2455 6. Click on the **Default** link in the **Zone** column.
- 2456 7. On the Edit Authentication screen, scroll down to the **Claims Authentication Types** group. Select
 2457 the **Trusted Identity provider** option.

- 2458 8. Under the **Trusted Identity provider** checkbox, select the name of the new token issuer that was
 2459 created using the Powershell commands (e.g., Federated Logon from Identity Provider).



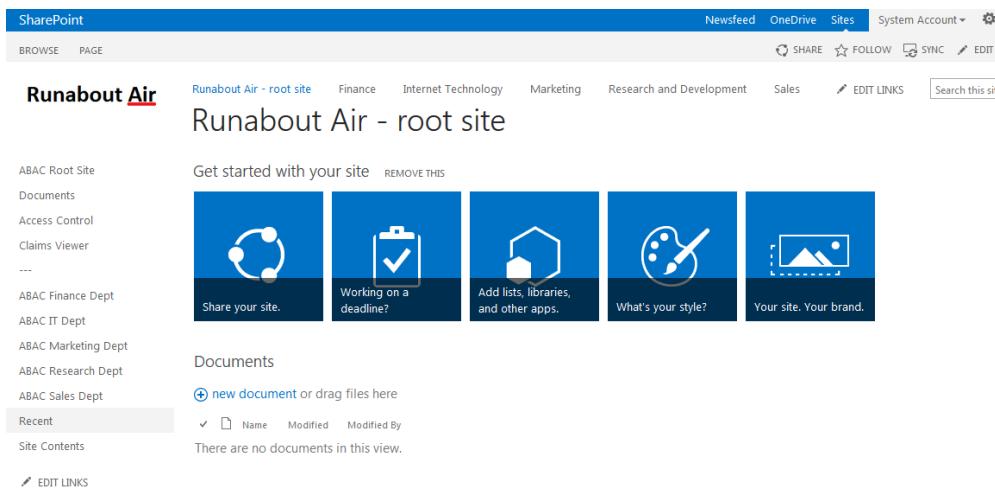
2460

- 2461 9. Scroll to the bottom of the page and click **Save**.

2462 5.3.4 Configuring the Access Control Rule on SharePoint

2463 After configuring the token issuer as a Sign On option for SharePoint, configure the access control rule
 2464 on the SharePoint site that is necessary for federated users to be able to access the site.

- 2465 1. Logon to the relying party's SharePoint site (e.g., <https://SharePoint.abac.test>) using the
 credentials of the SharePoint administrator.
- 2467 2. Select **Windows Authentication** in the Sign On screen.



2468

SECOND DRAFT

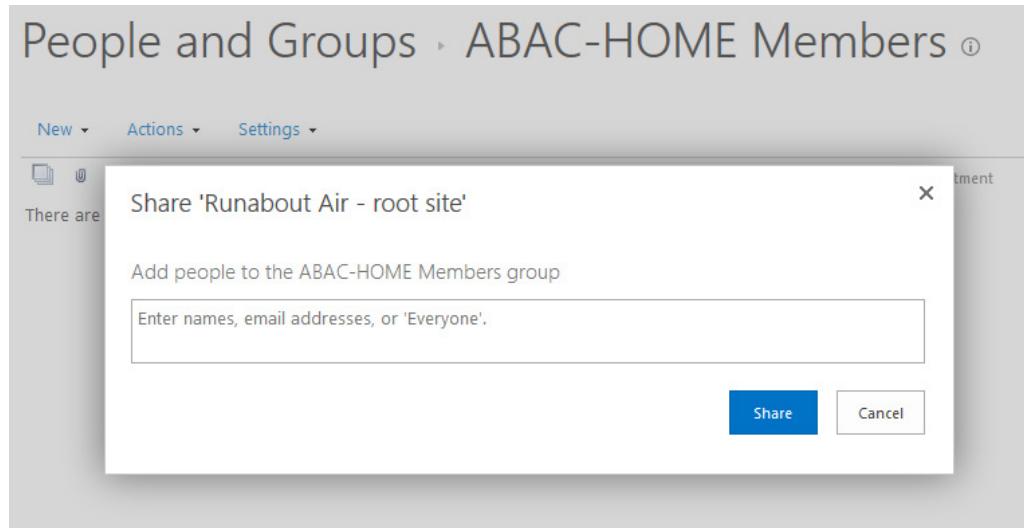
- 2469 3. Click the gear icon at the top right corner of the page and select the **Site Settings** link.
- 2470 4. On the Site Settings screen, in the **Users and Permissions** group, click **People and Groups**.
- 2471 5. Under the **Groups** heading on the left pane, click on the **HOME Members** group.

The screenshot shows a SharePoint 'People and Groups' page. The title bar includes 'Runabout Air - root site' and navigation links for Finance, Internet Technology, Marketing, Research and Development, and Sales. Below the title, it says 'People and Groups > ABAC-HOME Members'. A breadcrumb trail shows 'People and Groups > ABAC-HOME Members'. The main content area has a header 'Groups' with buttons for 'New', 'Actions', and 'Settings'. A table lists groups, with 'ABAC-HOME Members' selected and highlighted in blue. Other groups listed include 'Excel Services Viewers', 'ABAC-HOME Visitors', 'ABAC-HOME Owners', 'Style Resource Readers', 'Designers', 'Hierarchy Managers', 'Approvers', 'Restricted Readers', and 'Quick Deploy Users'. A 'More...' link is at the bottom. The 'Actions' menu is open, showing options 'Add Users' and 'Add users to this group.'

- 2472
- 2473 6. Under the page title, click on the **New** link and select the **Add Users** option from the popup menu.
- 2474

The screenshot shows a SharePoint 'People and Groups' page. The title bar includes 'Runabout Air - root site' and navigation links for Finance, Internet Technology, Marketing, Research and Development, and Sales. Below the title, it says 'People and Groups > ABAC-HOME Members'. A breadcrumb trail shows 'People and Groups > ABAC-HOME Members'. The main content area has a header 'Groups' with buttons for 'New', 'Actions', and 'Settings'. A table lists groups, with 'ABAC-HOME Members' selected and highlighted in blue. Other groups listed include 'Excel Services Viewers', 'ABAC-HOME Visitors', 'ABAC-HOME Owners', 'Style Resource Readers', 'Designers', 'Hierarchy Managers', 'Approvers', 'Restricted Readers', and 'Quick Deploy Users'. A 'More...' link is at the bottom. The 'Actions' menu is open, showing options 'Add Users' and 'Add users to this group.' The 'Add Users' option is highlighted with a blue box.

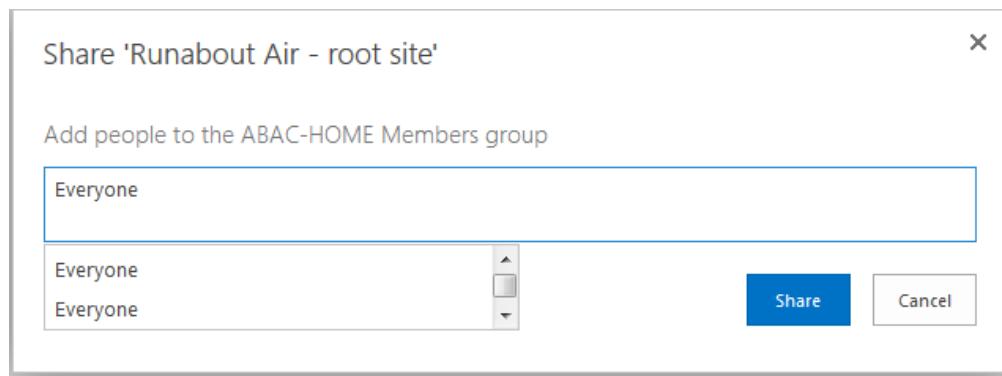
2475



2476

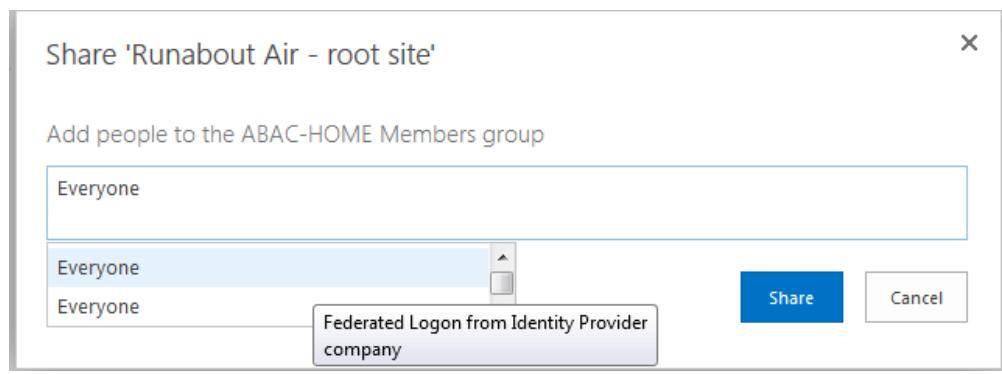
2477 7. On the Share popup screen, enter **Everyone** in the text field.

2478 SharePoint will display a List Box underneath the text field.



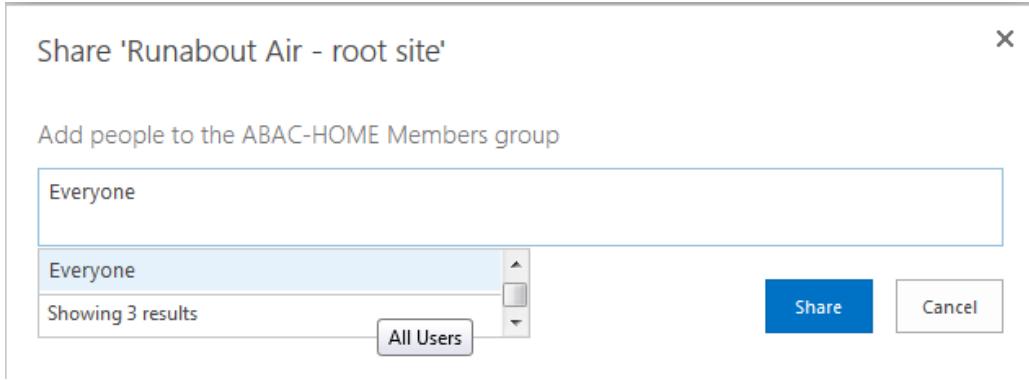
2479

2480 The list will contain multiple entries for the same value of **Everyone**. If you place your cursor
2481 over an entry in the list SharePoint will display details about the entry.



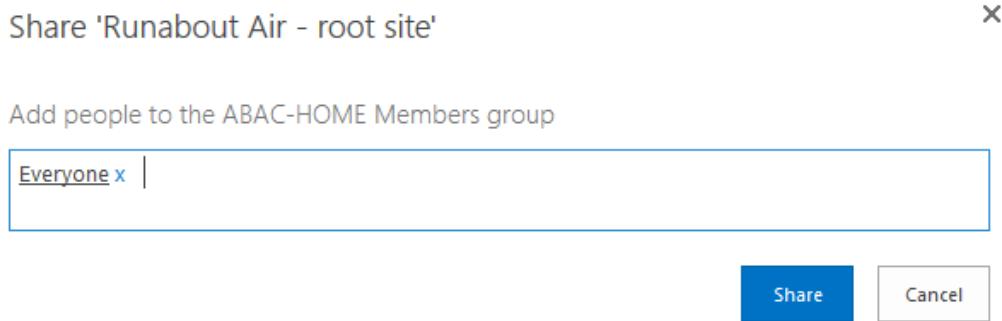
2482

2483 8. Locate the entry that is associated with **All Users**.



2484

- 2485 9. Click on the entry associated with **All Users**.



2486

- 2487 10. Click **Share**.

2488 When you go back to the People and Groups screen, you should see **Everyone** listed for the Home
2489 Members group.

Runabout Air Runabout Air - root site Finance Internet Technology Marketing Research and Development Sales EDIT LINKS

People and Groups > ABAC-HOME Members ⓘ

Groups	New	Actions	Settings	View:
ABAC-HOME Members	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Name	About me
Excel Services Viewers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> Everyone	Title
ABAC-HOME Visitors	<input type="checkbox"/>			Department

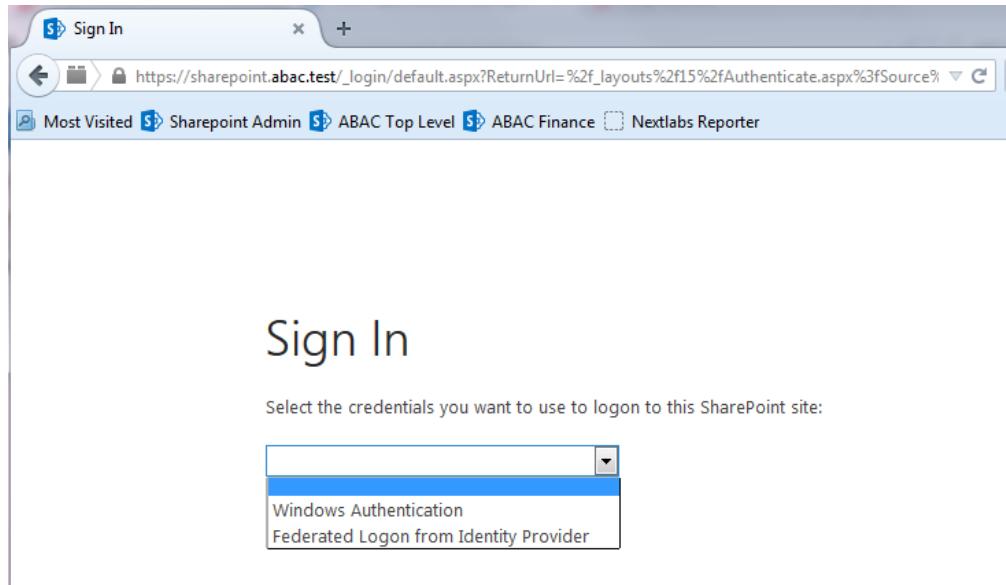
2490

2491 5.3.5 Functional Test of the Federated Logon at the Resource Provider

- 2492 1. Launch a new browser window and go to the relying party's SharePoint site (e.g.,
2493 <https://SharePoint.abac.test>).

2494 Expected Result: You should see two logon options in the dropdown box. One of the options
2495 should be the name of the new trusted token issuer that was configured in the previous section
2496 (e.g., Federated Logon from Identity Provider).

SECOND DRAFT



Sign In

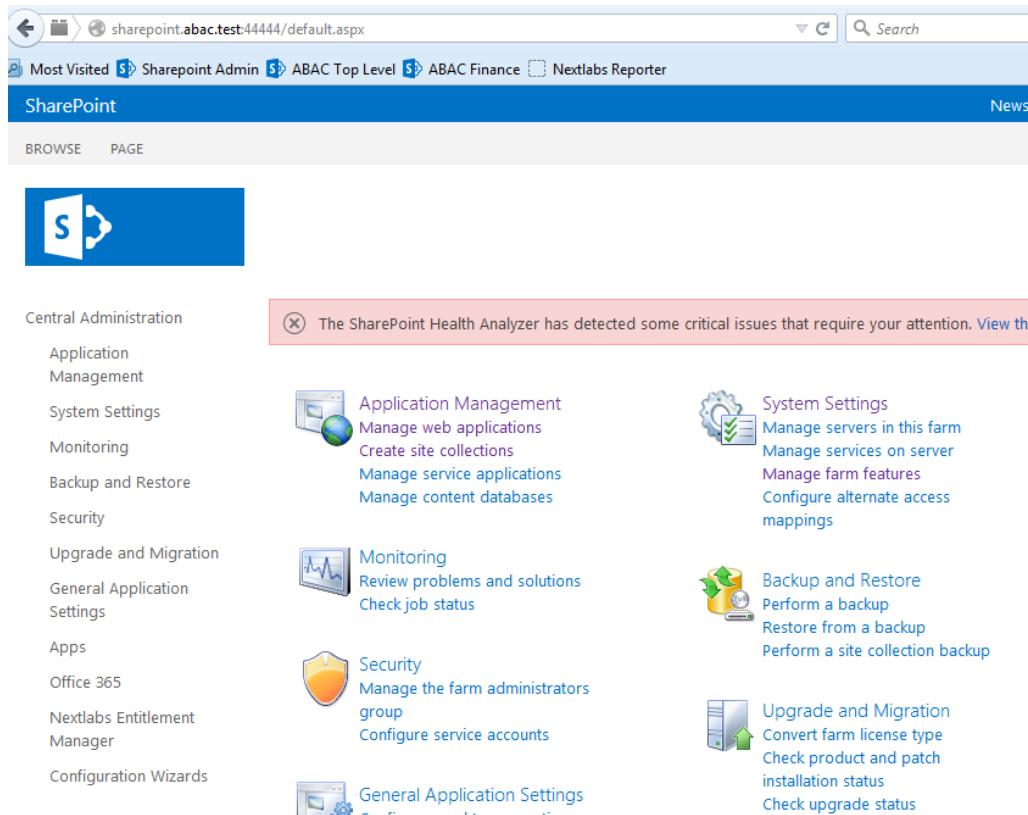
Select the credentials you want to use to logon to this SharePoint site:

Windows Authentication
Federated Logon from Identity Provider

2497

2498 Next you will verify that SharePoint is configured to read the **upn** attribute that was configured for the
2499 federated logon.

- 2500 2. Launch your browser and go the SharePoint central administration page (e.g.,
2501 <http://SharePoint.abac.test:44444/default.aspx>).
2502 3. Logon using the credentials of the SharePoint administrator.



The SharePoint Health Analyzer has detected some critical issues that require your attention. [View them](#)

Central Administration

Application Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Apps

Office 365

Nextlabs Entitlement Manager

Configuration Wizards

Application Management

Manage web applications
Create site collections
Manage service applications
Manage content databases

System Settings

Manage servers in this farm
Manage services on server
Manage farm features
Configure alternate access mappings

Monitoring

Review problems and solutions
Check job status

Security

Manage the farm administrators group
Configure service accounts

Backup and Restore

Perform a backup
Restore from a backup
Perform a site collection backup

Upgrade and Migration

Convert farm license type
Check product and patch installation status
Check upgrade status

General Application Settings

2503

SECOND DRAFT

- 2504 4. In the **Application Management** group, click on **Manage web applications**.
- 2505 5. Click on the web application that contains the SharePoint site you are managing (e.g., **SharePoint – 80**). SharePoint will highlight the web application row that you clicked on.

The screenshot shows the SharePoint Central Administration interface under the 'Web Applications' tab. The left navigation bar includes links like Central Administration, Application Management, System Settings, Monitoring, Security, Upgrade and Migration, General Application Settings, Apps, Office 365, Nextlabs Entitlement Manager, and Configuration Wizards. The main content area displays a table of web applications:

Name	URL	Port
SharePoint - 80	http://sharepoint/	80
SharePoint Central Administration v4	http://sharepoint:4444/	4444
SharePoint - 8888	http://sharepoint:8888/	8888
SharePoint - 6454	https://sharepoint:6454/	6454

2507

- 2508 6. Click on the **User Policy** button.

The screenshot shows the same SharePoint Central Administration interface as before, but with a modal dialog box titled 'Policy for Web Application' overlaid. The dialog box contains the following information:

Policy for Web Application

Adding or updating Web application policy with new users or groups will trigger a SharePoint Search crawl over all content covered by that policy. This can reduce search crawl freshness and increase crawl load. Consider using security groups at the policy level and add/remove users from security groups to avoid this.

Add Users | Delete Selected Users | Edit Permissions of Selected Users

Zone	Display Name	User Name	Permissions
(All zones)	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\LOCAL SERVICE	Full Read

2509

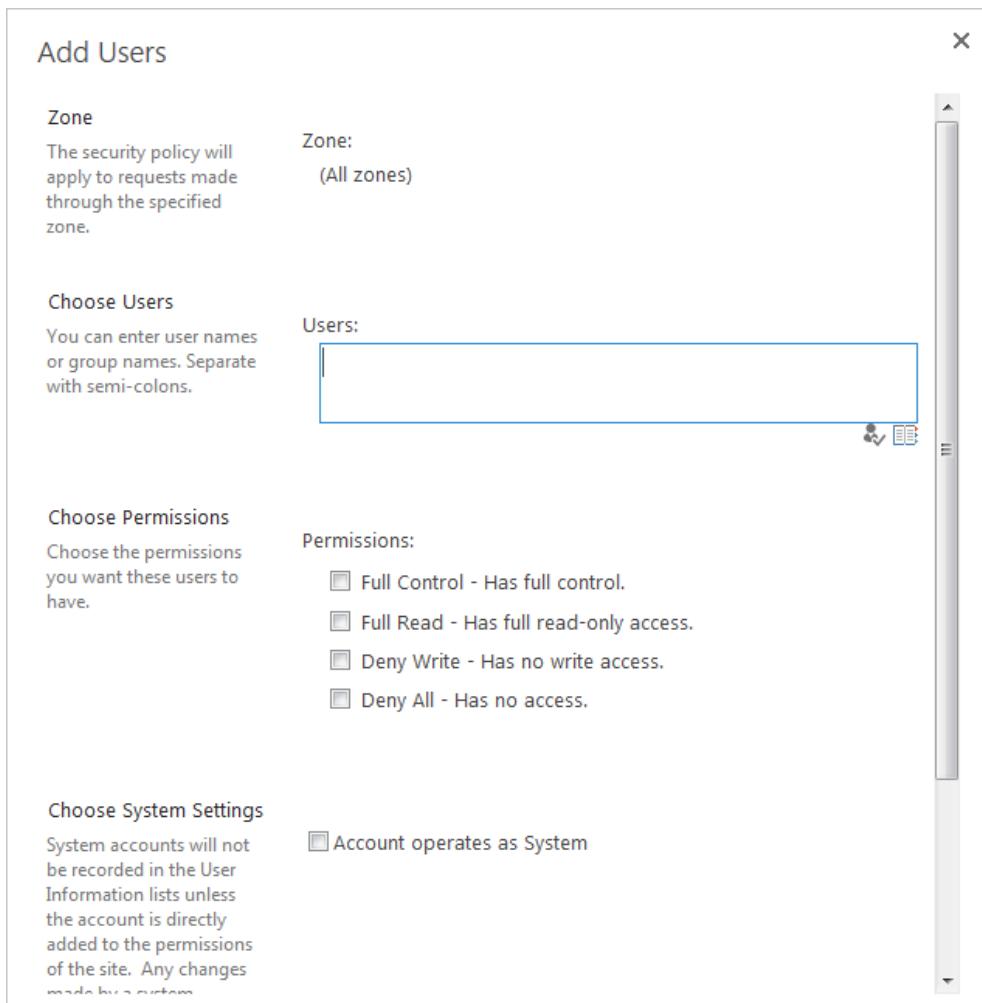
- 2510 7. Click **Add Users**.



2511

2512

8. Click **Next**.



2513

2514

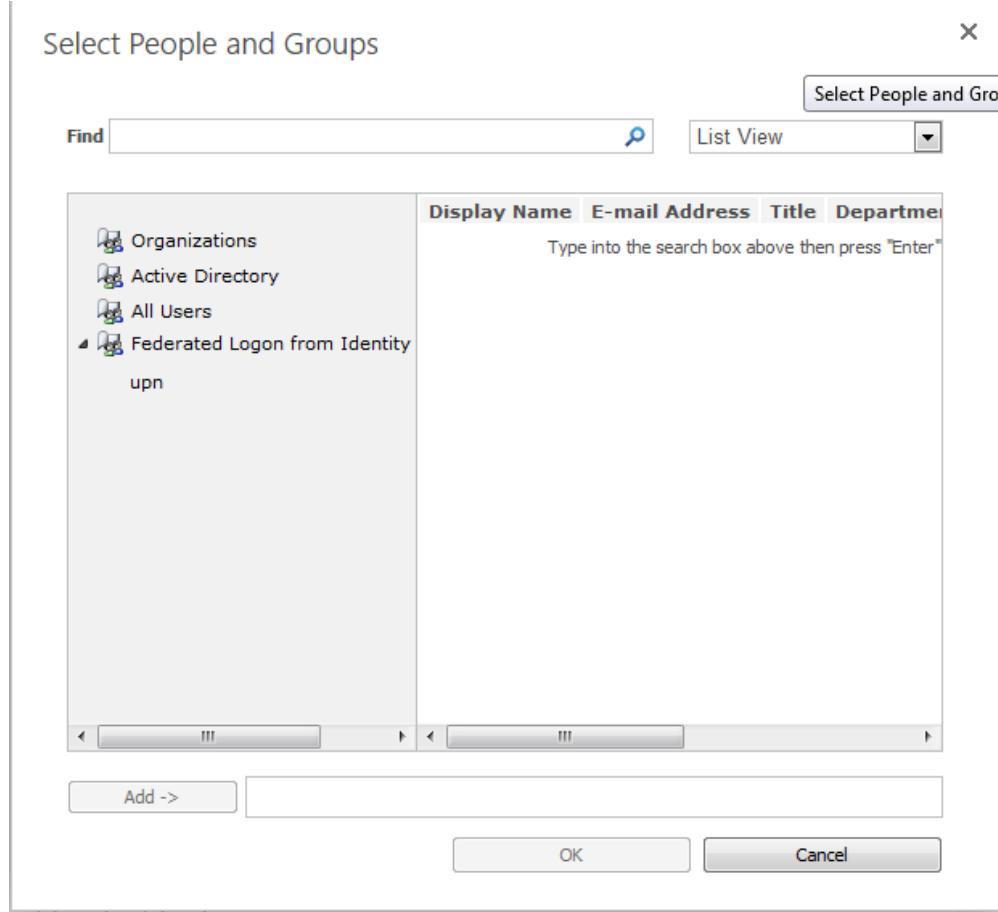
9. On the Add Users screen, click the small browse icon (looks like a book) under the Users field.

2515

2516

Expected Result: On the Select People and Groups screen, you should see a grouping with the name of the trusted token issuer that was configured via Powershell (e.g., **Federated**

2517 **Logon from Identity Provider).** You should also see the **upn** attribute listed under that
2518 grouping.



2519

2520

5.4 Configure the PingFederate-RP Connection to SharePoint

2521 Follow the instructions below to configure a PingFederate connection from the PingFederate-RP to the
2522 relying party's SharePoint.

2523

1. Logon to the server that hosts the PingFederate service for the relying party.
2. Launch your browser and go to: https://<DNS_NAME>:9999/pingfederate/app. Replace
2524 DNS_NAME with the fully qualified name of the relying party's PingFederate server (e.g.,
2525 <https://rp.abac.test:9999/pingfederate/app>). Logon to the PingFederate application using the
2526 credentials you configured during installation.

The screenshot shows the PingFederate web interface. At the top, there's a yellow banner with a warning icon and the text "License Violation: Expiration date passed". Below the banner, the main menu is divided into three main sections: "IdP Configuration", "Server Configuration", and "SP Configuration".

- IdP Configuration:**
 - APPLICATION INTEGRATION SETTINGS:** Adapters, Authentication Selection, Default URL, Application Endpoints.
 - FEDERATION SETTINGS:** Protocol Endpoints.
 - SP CONNECTIONS (3):** WS Fed (Sharepoint), SAML2.0 (https://nextlabs-rp), SAML2.0 (Demo SP). Sub-options: Manage All SP, Create New, Import.
 - SP AFFILIATIONS (0):** Sub-options: Manage All Affiliations, Create New.
- Server Configuration:**
 - SYSTEM SETTINGS:** Server Settings, Data Stores, Redirect Validation.
 - ADMINISTRATIVE FUNCTIONS:** Metadata Export, XML File Signatures, Configuration Archive, Account Management, License Management, Virtual Host Names.
 - CERTIFICATE MANAGEMENT:** Trusted CAs, SSL Server Certificates, SSL Client Keys & Certificates, Digital Signing & XML Decryption Keys & Certificates, Certificate Revocation Checking.
 - AUTHENTICATION:** Application Authentication, Password Credential Validators, Active Directory, Domains/Kerberos Realms.
 - IDP-TO-SP BRIDGING:** Adapter-to-Adapter.
- SP Configuration:**
 - APPLICATION INTEGRATION SETTINGS:** Adapters, Target URL Mapping, Identity Store Provisioners, Default URLs, Application Endpoints.
 - FEDERATION SETTINGS:** Protocol Endpoints.
 - IDP CONNECTIONS (2):** SAML2.0 (https://idp.abac....), SAML2.0 (Demo IdP). Sub-options: Manage All IdP, Create New, Import.

2528

3. On the **Main Menu** under SP CONNECTIONS, click **Create New**. On the Connection Type screen, select **Browser SSO Profiles**. For the Protocol field, select **WS-Federation**.

This screenshot shows the "Connection Type" step of a connection creation wizard. The top navigation bar includes "Main" and "SP Connection". Below the bar, tabs for "Connection Type", "Connection Options", "General Info", "Browser SSO", "Credentials", and "Activation & Summary" are visible. A note at the top says: "Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all." The "Connection Type" tab is selected. Under "Connection Template", "No Template" is listed. Under "Protocol", "WS-Federation" is selected from a dropdown menu. Other options shown are "Browser SSO Profiles" (selected), "WS-Trust STS", and "Outbound Provisioning". At the bottom right are "Cancel" and "Next >" buttons.

2531

4. Click **Next**. On the Connection Options screen, select **Browser SSO**.

SECOND DRAFT

The screenshot shows a software interface for managing connections. At the top, there are two tabs: "Main" and "SP Connection". The "SP Connection" tab is active and highlighted in blue. Below the tabs, a navigation bar includes "Connection Type", "Connection Options", "General Info", "Browser SSO", "Credentials", and "Activation & Summary". A message box at the top states: "Please select options that apply to this connection." Below this, there are three checkboxes: "Browser SSO" (which is checked), "IdP Discovery", and "Attribute Query". At the bottom right of the main area, there are three buttons: "Cancel", "< Previous", and "Next >".

2533

- 2534 5. Click **Next**. On the General Info screen, for the Partner's Realm field, enter the name of the
2535 Resource Provider's (SharePoint) realm (e.g., urn:SharePoint.abac.test). Keep a copy of the
2536 realm name because it will be used in a configuration of SharePoint later in the guide.
2537
2538 6. Enter a unique name for this new PingFederate configuration in the Connection Name field. For
2539 the Base URL field, enter the root destination URL at the SharePoint site where the PingFederate
will redirect a user once authenticated (e.g., <https://SharePoint.abac.test>).

The screenshot shows the "General Info" tab selected within the "SP Connection" configuration interface. The page includes a note: "This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints." Below the note, there are several input fields:

- Partner's Realm (Connection ID): urn:sharepoint.abac.test
- Connection Name: Sharepoint
- Virtual Server IDs: (empty input field with an "Add" button)
- Base URL: https://sharepoint.abac.test
- Company: (empty input field)
- Contact Name: (empty input field)
- Contact Number: (empty input field)
- Contact Email: (empty input field)
- Application Name: (empty input field)
- Application Icon URL: (empty input field)
- Logging Mode: (radio buttons for None, Standard, Enhanced, Full, with Standard selected)

At the bottom right, there are three buttons: "Cancel", "< Previous", and "Next >".

2540

- 2541 7. Click **Next**.

SECOND DRAFT

Connection Type Connection Options General Info ★ Browser SSO Credentials Activation & Summary

This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

Configure Browser SSO

2542

- 2543 8. On the Browser SSO screen, click **Configure Browser SSO**. On the Assertion Lifetime screen, 2544 enter a value of 20 for the Minutes After field.

Save Draft Cancel < Previous Next >

Assertion Lifetime Assertion Creation Protocol Settings Summary

When an assertion is issued to the SP, there is a timeframe of validity before and after issuance. Please specify these parameters below.

Minutes Before 5 *

Minutes After 20 *

2545

- 2546 9. Click **Next**.

Cancel Next > Done Save

Main SP Connection Browser SSO

Assertion Lifetime Assertion Creation Protocol Settings Summary

This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration

Identity Mapping	Email Address
Attribute Contract	SAML_SUBJECT
Adapter Instances	0
Connection Contract Mappings	0

Configure Assertion Creation

2547

SECOND DRAFT

- 2548 10. On the Assertion Creation screen, click **Configure Assertion Creation**. On the Identity Mapping
2549 screen, select **User Principal Name**.

Select the type of name identifier you will send to the SP. Your selection may affect the way the SP will look up and associate the user to a specific local account.

Email Address
 User Principal Name
 Common Name

- 2550
- 2551 11. Click **Next**. On the Attribute Contract screen, below the EXTEND THE CONTRACT FIELD, enter
2552 “upn” in the textbox. For the ATTRIBUTE NAME FORMAT select the **schemas.xmlsoap.org 2005**
2553 identity claims format.

An Attribute Contract is a set of user attributes that this server will send in the assertion.

EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
upn	http://schemas.xmlsoap.org/2005/05/identity/claims	<input type="button" value="Add"/>

- 2554
- 2555 12. Click **Add**.

SECOND DRAFT

The screenshot shows the Assertion Creation interface. At the top, there are tabs: Main, SP Connection, Browser SSO, and Assertion Creation (which is selected). Below the tabs, there are sub-tabs: Identity Mapping (selected), Attribute Contract, Authentication Source Mapping, and Summary. A note at the top says, "An Attribute Contract is a set of user attributes that this server will send in the assertion." The main area is titled "ATTRIBUTE CONTRACT" and contains a table:

SAML_SUBJECT	ATTRIBUTE NAME FORMAT	ACTION
EXTEND THE CONTRACT	upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims Edit / Delete
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	<input type="button" value="Add"/>

At the bottom right are buttons: Save Draft, Cancel, < Previous, and Next >.

2556

2557 13. Click **Next**.

The screenshot shows the Assertion Creation interface with the Authentication Source Mapping tab selected. A note at the top says, "PingFederate uses IdP adapters or partner IdPs to authenticate users to your SP. Users may be authenticated by one of several different adapters or connection mapping contracts, so map an adapter instance for each IDM system or a connection mapping contract for partner IdPs." The main area contains two tables:

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION

At the bottom are buttons: Map New Adapter Instance... (highlighted in blue), Map New Connection Contract Mapping..., Save Draft, Cancel, < Previous, and Next >.

2558

2559 14. On the Authentication Source Mapping screen, click **Map New Connection Contract Mapping**.
2560 On the Connection Contract Mapping screen, for the CONNECTION MAPPING CONTRACT field,
2561 select the name of the contract with the identity provider that was configured in a [Section 3](#)
2562 (e.g., SharePoint 2013).

SECOND DRAFT

The screenshot shows a user interface for managing connection contracts. At the top, there are tabs: Main, SP Connection, Browser SSO, Assertion Creation, and Connection Contract Mapping (which is highlighted). Below the tabs, a sub-menu bar includes Connection Mapping Contract, Assertion Mapping, Attribute Contract Fulfillment, Issuance Criteria, and Summary. A note at the top states: "Select a connection mapping contract that may be used to authenticate users for this partner. Attributes returned by the connection mapping contract you choose may be used to fulfill the Attribute Contract with your partner." A dropdown menu labeled "CONNECTION MAPPING CONTRACT" is open, showing "Sharepoint 2013". A section titled "CONTRACT ATTRIBUTES" contains a "subject" field. At the bottom left is a "Manage Connection Mapping Contracts..." button, and at the bottom right are Save Draft, Cancel, and Next > buttons.

2563

- 2564 15. Click **Next**. On the Assertion Mapping screen, select **Use only the Connection Mapping Contract values in the SAML assertion**.
- 2565

The screenshot shows the Assertion Mapping screen. The tabs at the top are Main, SP Connection, Browser SSO, Assertion Creation, and Connection Contract Mapping (highlighted). The sub-menu bar includes Connection Mapping Contract, Assertion Mapping (highlighted), Attribute Contract Fulfillment, Issuance Criteria, and Summary. A note at the top states: "You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "Sharepoint 2013" connection mapping contract, or you can use these values plus additional attributes retrieved from local data stores." A section titled "CONNECTION MAPPING CONTRACT" contains a "subject" field and three radio button options: "Retrieve additional attributes from multiple data stores using one mapping", "Retrieve additional attributes from a data store--includes options to use alternate data stores and/or a failsafe mapping", and "Use only the Connection Mapping Contract values in the SAML assertion" (which is selected). At the bottom right are Save Draft, Cancel, and Next > buttons.

2566

- 2567 16. Click **Next**.

SECOND DRAFT

The screenshot shows the 'Connection Contract Mapping' section of the PingFederate interface. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, and Connection Contract Mapping. Below these are sub-tabs for Connection Mapping Contract, Assertion Mapping, Attribute Contract Fulfillment (which is selected), Issuance Criteria, and Summary. A message bar at the top says, "Fulfill your Attribute Contract with values from the connection mapping contract or with dynamic text values." The main area displays two rows of attribute mappings:

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Connection Mapping Contract	subject	None available
upn	Connection Mapping Contract	subject	None available

At the bottom right are buttons for Save Draft, Cancel, < Previous, and Next >.

2568

2569

17. On the Attribute Contract Fulfillment screen, click **Next**.

The screenshot shows the 'Attribute Contract Fulfillment' section of the PingFederate interface. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, and Connection Contract Mapping. Below these are sub-tabs for Connection Mapping Contract, Assertion Mapping, Attribute Contract Fulfillment (selected), Issuance Criteria, and Summary. A message bar at the top says, "PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with this conditional authorization." The main area displays a table for defining issuance criteria:

SOURCE	ATTRIBUTE NAME	CONDITION	VALUE	ERROR RESULT	ACTION
- SELECT -	- SELECT -	- SELECT -			Add

At the bottom right are buttons for Save Draft, Cancel, < Previous, and Next >.

2570

2571

18. On the Issuance Criteria screen, click **Next**.

The screenshot shows the 'Connection Contract Mapping' section of the PingFederate interface. At the top, there are tabs for Main, SP Connection, Browser SSO, Assertion Creation, and Connection Contract Mapping. Below these are sub-tabs for Connection Mapping Contract, Assertion Mapping, Attribute Contract Fulfillment, Issuance Criteria (selected), and Summary. A message bar at the top says, "Click a heading link to edit a configuration setting." The main area displays several configuration sections:

- CONNECTION MAPPING CONTRACT**: Selected contract is Sharepoint 2013.
- ASSERTION MAPPING**: Connection Mapping Contract is Sharepoint 2013. Data Store or Assertion is "Use only the Connection Mapping Contract values in the SAML assertion".
- ATTRIBUTE CONTRACT FULFILLMENT**: upn is subject (Connection Mapping Contract). SAML_SUBJECT is subject (Connection Mapping Contract).
- ISSUANCE CRITERIA**: Criterion is (None).

At the bottom right are buttons for Save Draft, Cancel, < Previous, and Done.

2572

SECOND DRAFT

- 2573 19. On the Summary screen, click **Next**.



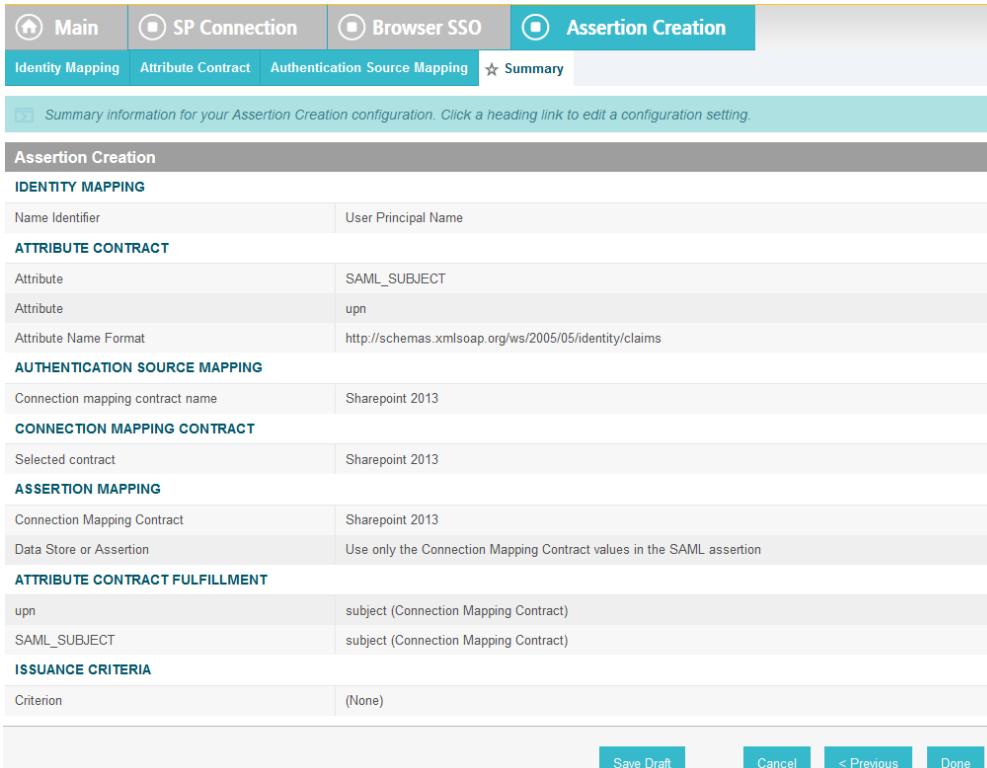
ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		Delete

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		

Map New Adapter Instance... Map New Connection Contract Mapping...

2574

- 2575 20. On the Authentication Source Mapping screen, click **Next**.



IDENTITY MAPPING	User Principal Name
Name Identifier	

ATTRIBUTE CONTRACT	
Attribute	SAML_SUBJECT
Attribute	upn
Attribute Name Format	http://schemas.xmlsoap.org/ws/2005/05/identity/claims

AUTHENTICATION SOURCE MAPPING	
Connection mapping contract name	Sharepoint 2013

CONNECTION MAPPING CONTRACT	
Selected contract	Sharepoint 2013

ASSERTION MAPPING	
Connection Mapping Contract	Sharepoint 2013
Data Store or Assertion	Use only the Connection Mapping Contract values in the SAML assertion

ATTRIBUTE CONTRACT FULFILLMENT	
upn	subject (Connection Mapping Contract)
SAML_SUBJECT	subject (Connection Mapping Contract)

ISSUANCE CRITERIA	
Criterion	(None)

Save Draft Cancel < Previous Done

2576

- 2577 21. On the Summary screen, click **Done**.

SECOND DRAFT

Assertion Configuration

Identity Mapping	User Principal Name
Attribute Contract	SAML_SUBJECT, upn
Adapter Instances	0
Connection Contract Mappings	1

Configure Assertion Creation

2578

2579

22. On the Assertion Creation screen, click **Next**.

Protocol Settings

Signature Policy	SAML-standard
------------------	---------------

Configure Protocol Settings

2580

2581 23. On the Protocol Settings screen, click **Configure Protocol Settings**. On the Service URL screen,
2582 for the Endpoint URL field, enter the name of the destination URL at the Service Provider
2583 (SharePoint) site (e.g., /_trust/). When PingFederate completes the authentication process, the
2584 user will be sent to a destination URL. The destination URL is a combination of two configuration
2585 fields. The first is the Base URL that was configured earlier, and the second is the Endpoint URL
2586 on this screen. The Endpoint URL will be appended to the Base URL. An example is provided
2587 below.

2588

Base URL: *https://SharePoint.abac.test/_trust/*

2589

Endpoint URL: /_trust/

2590

After authentication, PingFederate will redirect to the destination:

2591

https://SharePoint.abac.test/_trust/

SECOND DRAFT

The screenshot shows the 'Protocol Settings' tab selected in a navigation bar. Under the 'Service URL' section, there is a warning message: 'You must specify a URL in the URL field.' Below this, a note says: 'As the IdP, you send SAML assertions and SLO cleanup messages to the SP. Specify here the URL where the SP is expecting to receive these messages.' An 'Endpoint URL' input field contains the value '/_trust/'. A table below lists configuration options: 'Require HTTPS' (checkbox checked), 'Valid Domain Name (leading wildcard '*' allowed)' (input field empty), 'Valid Path (leave blank to allow any path)' (input field empty), 'Allow Any Query/Fragment' (checkbox checked), and an 'Action' column with a 'Add' button.

2592

2593 24. Click **Next >**.

The screenshot shows the 'Protocol Settings' tab selected in a navigation bar. Under the 'Service URL' section, there is a note: 'Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.' A 'Protocol Settings' section header is visible. An 'Endpoint URL' input field shows the value '/_trust/'. At the bottom are 'Save Draft', 'Cancel', and 'Next >' buttons.

2594

2595 25. On the Summary screen, click **Done**.

SECOND DRAFT

This screenshot shows the 'Protocol Settings' screen. At the top, there are three tabs: 'Main' (selected), 'SP Connection' (disabled), and 'Browser SSO'. Below the tabs, there are four sub-tabs: 'Assertion Lifetime', 'Assertion Creation' (selected), 'Protocol Settings' (disabled), and 'Summary'. A note below the tabs states: 'This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.' Under 'Protocol Settings', it shows 'Signature Policy' set to 'SAML-standard'. At the bottom, there is a blue button labeled 'Configure Protocol Settings'.

2596

2597 26. On the Protocol Settings screen, click **Next**.

This screenshot shows the 'Protocol Settings' screen with various configuration sections. The sections include:

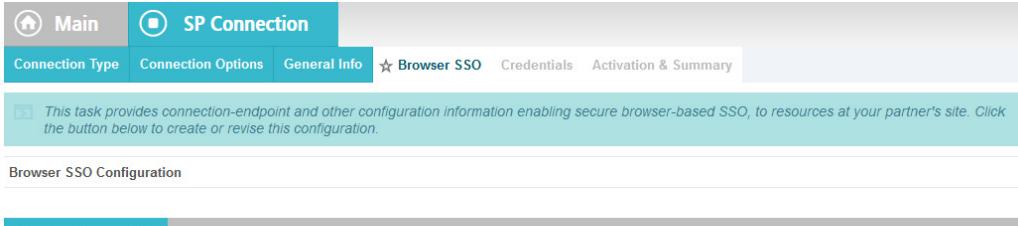
- IDENTITY MAPPING:** Name Identifier (User Principal Name)
- ATTRIBUTE CONTRACT:** Attribute (SAML_SUBJECT), Attribute (upn), Attribute Name Format (<http://schemas.xmlsoap.org/ws/2005/05/identity/claims>)
- AUTHENTICATION SOURCE MAPPING:** Connection mapping contract name (Sharepoint 2013)
- CONNECTION MAPPING CONTRACT:** Selected contract (Sharepoint 2013)
- ASSERTION MAPPING:** Connection Mapping Contract (Sharepoint 2013), Data Store or Assertion (Use only the Connection Mapping Contract values in the SAML assertion)
- ATTRIBUTE CONTRACT FULFILLMENT:** upn (subject (Connection Mapping Contract)), SAML_SUBJECT (subject (Connection Mapping Contract))
- ISSUANCE CRITERIA:** Criterion (None)
- Protocol Settings:** This section is highlighted with a dark grey background.
- SERVICE URL:** Endpoint URL (/_trust/)

At the bottom right, there are four buttons: 'Save Draft', 'Cancel', '< Previous', and 'Next >'.

2598

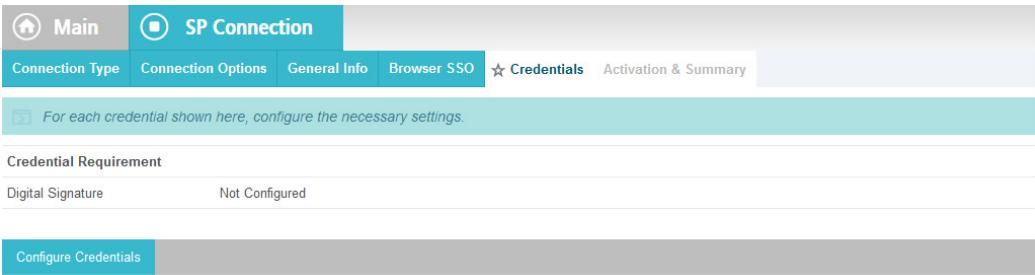
2599 27. On the Summary screen, click **Done**.

SECOND DRAFT



2600

2601 28. On the Browser SSO screen, click **Next**.



2602

2603 29. On the Credentials screen, click **Configure Credentials**. On the Digital Signature Settings screen,
2604 select the **Signing Certificate for SAML messages**.

SECOND DRAFT

The screenshot shows the 'Digital Signature Settings' configuration page. At the top, there are three tabs: 'Main' (disabled), 'SP Connection' (disabled), and 'Credentials' (selected). Below the tabs, a heading says '★ Digital Signature Settings Summary'. A note at the top states: 'You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.' Under 'Signing Certificate', a dropdown menu is open, showing '01:30:DB:8C:25:AB (cn=demo dsig new)' with an asterisk (*) next to it. There is also an unchecked checkbox for 'Include the raw key in the signature <KeyValue> element.' Under 'Signing Algorithm', a dropdown menu is open, showing 'RSA SHA256'. At the bottom left is a 'Manage Certificates...' button.

2605

2606 30. Click **Next**.

The screenshot shows the 'Summary' configuration page. At the top, there are three tabs: 'Main' (disabled), 'SP Connection' (disabled), and 'Credentials' (selected). Below the tabs, a heading says '★ Summary'. A note at the top states: 'Summary information for your Credentials configuration. Click a heading link to edit a configuration setting.' A large bold heading 'Credentials' is displayed. Below it, a section titled 'DIGITAL SIGNATURE SETTINGS' contains three items: 'Selected Certificate' (CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US), 'Include Raw Key in KeyValue' (false), and 'Selected Signing Algorithm' (RSA SHA256). At the bottom right are 'Save Draft', 'Cancel', and 'Next >' buttons.

2607

2608 31. On the Summary screen, click **Done**.

SECOND DRAFT

The screenshot shows the 'SP Connection' tab selected in the top navigation bar. Below it, a sub-navigation bar includes 'Connection Type', 'Connection Options', 'General Info', 'Browser SSO', 'Credentials' (which is highlighted with a star icon), and 'Activation & Summary'. A note at the top states: 'For each credential shown here, configure the necessary settings.' A section titled 'Credential Requirement' lists 'Digital Signature' with the value 'CN=demo dsig new'. At the bottom is a blue button labeled 'Configure Credentials'.

2609

- 2610 32. On the Credentials screen, click **Next**.

The screenshot shows the 'Activation & Summary' screen. It contains several sections: 'Attribute Name Format' (http://schemas.xmlsoap.org/ws/2005/05/identity/claims), 'AUTHENTICATION SOURCE MAPPING' (Connection mapping contract name: Sharepoint 2013), 'CONNECTION MAPPING CONTRACT' (Selected contract: Sharepoint 2013), 'ASSERTION MAPPING' (Connection Mapping Contract: Sharepoint 2013, Data Store or Assertion: Use only the Connection Mapping Contract values in the SAML assertion), 'ATTRIBUTE CONTRACT FULFILLMENT' (upn: subject (Connection Mapping Contract), SAML_SUBJECT: subject (Connection Mapping Contract)), 'ISSUANCE CRITERIA' (Criterion: (None)), 'Protocol Settings' (Endpoint URL: /_trust/), 'Credentials' (Selected Certificate: CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US, Include Raw Key in KeyValue: false, Selected Signing Algorithm: RSA SHA256), and 'DIGITAL SIGNATURE SETTINGS' (Selected Certificate: CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US, Include Raw Key in KeyValue: false, Selected Signing Algorithm: RSA SHA256). At the bottom are buttons for 'Save Draft', 'Cancel', '< Previous', and 'Next >'.

2611

- 2612 32. On the Activation and Summary screen, select **Active** for the Connection Status field and Click **Save** to
2613 complete the configuration.

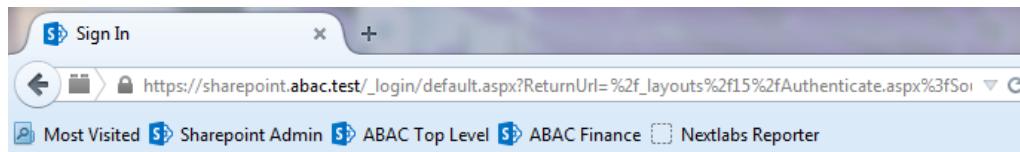
2614 5.5 Functional Test of All Configurations for Section 5

2615 The instructions in this section will perform an integrated test all of the configurations in Section 5.
 2616 Using the browser, you will logon using an account that was created in Active Directory and validate that
 2617 the complete federated authentication flow between SharePoint and the PingFederate servers at the
 2618 relying party and identity provider operates successfully.

2619 1. Launch your Firebox browser and select SAML tracer from the Tools menu.

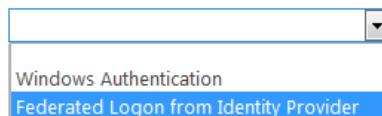
2620 This will launch an empty SAML tracer window. Minimize the SAML tracer window. The SAML
 2621 tracer will automatically record the details of the HTTPS messages in the background.

2622 2. Go back to the main browser window and go to the relying party's SharePoint site (e.g.,
 2623 <https://SharePoint.abac.test>).



Sign In

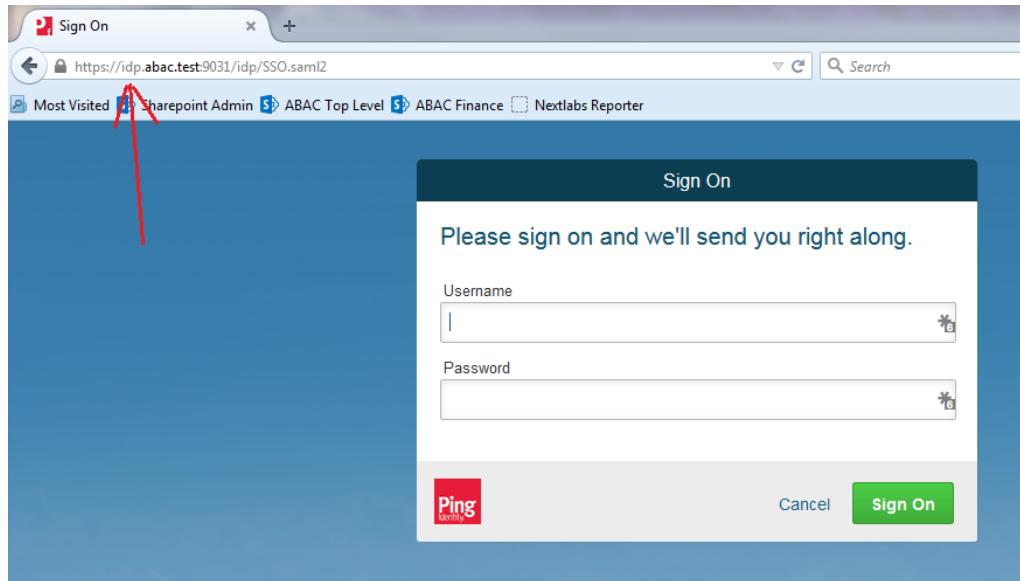
Select the credentials you want to use to logon to this SharePoint site:



2624

2625 3. Select the option to use the new trusted token issuer (e.g., Federated Logon from Identity
 2626 Provider) that was configured in this section.

2627 Expected Result: Your browser should be redirected to the PingFederate-IdP and you should see
 2628 the PingFederate Sign On screen. Examine the server name in the URL to ensure that it is the
 2629 identity provider's PingFederate server (e.g., idp.abac.test).



2630

- 2631 4. Enter the Username and Password of the Active Directory account created earlier in this guide
2632 (e.g., "lsmith").

A screenshot of a "Sign On" form. The title is "Sign On" and the sub-instruction is "Please sign on and we'll send you right along.". It has two input fields: "Username" containing "lsmith" and "Password" containing a series of dots. Below the fields are "Ping Identity" and "Cancel" buttons, and a large green "Sign On" button. The "Sign On" button is highlighted with a blue border.

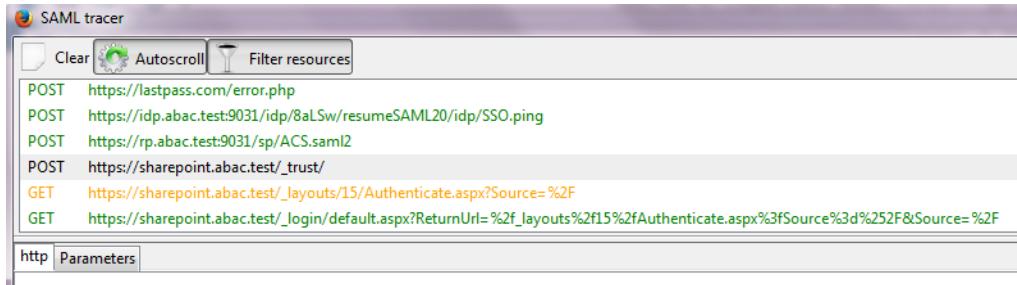
2633

- 2634 5. Click **Sign On**. On the RSA Adaptive Authentication screen, enter the SMS validation code
2635 received on your mobile phone. Click **Next**.

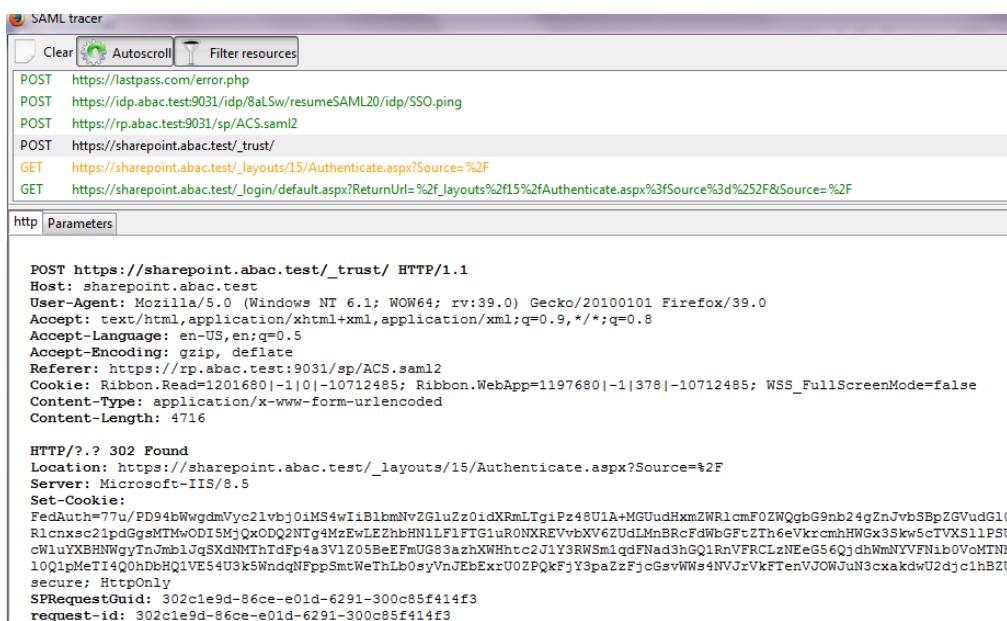
2636 Note: Once authenticated at the identity provider, your browser should automatically redirect
2637 to the PingFederate-RP (e.g., rp.abac.test) and then to the relying party's SharePoint
2638 (SharePoint.abac.test) site. Depending on the processing time of the servers in your
2639 environment, and other factors, it may take several seconds before your browser arrives back at
2640 the SharePoint site. The identity provider will redirect your browser to the PingFederate-RP first,
2641 and then the PingFederate-RP will redirect your browser to the SharePoint site, however you
2642 may not notice all of this activity if it happens quickly.

SECOND DRAFT

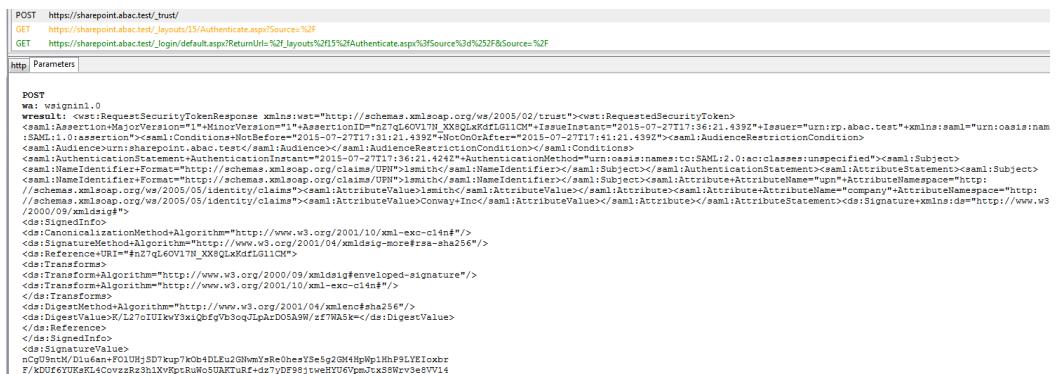
2643 **Expected Result:** Go back to the SAML tracer window. Scroll down the list of messages at the top
2644 and ensure there is a POST message to the SharePoint server to the _trust URL (e.g., POST
2645 `https://SharePoint.abac.test/_trust/`).



2646
2647 6. Click on the POST message to the SharePoint _trust URL to bring up the details of the message in
2648 the bottom pane.



2649
2650 7. Click on the Parameters tab for the bottom pane.



2651
2652 8. Copy all of the content (beginning with the POST line) in the bottom page and paste it into a text
2653 editor such as Notepad. Turn on Word Wrap to make it easier to see all of the XML content.

SECOND DRAFT

```
Untitled - Notepad
File Edit Format View Help

POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionId="n27ql60v17N_xx8QLxKdfLG1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp_abac_test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:Conditions+NotBefore="2015-
07-27T17:41:21.439Z"+NotOnOrAfter="2015-07-
27T17:36:21.424Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint_abac_test</saml:Audience></saml:AudienceRestrictionCondition></saml:Conditions><saml:AuthenticationStatement+AuthenticationInstant="2015-07-
27T17:36:21.424Z"><AuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:AuthenticationStatement><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="urn:attributeNamespace">http://schemas.xmlsoap.org/ws/2005/05/identity/claims"</saml:Attribute><saml:AttributeValue>Conway</saml:AttributeValue></saml:AttributeStatement><ds:Signature+xmldns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod+Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference+URI="#n27ql60v17N_xx8QLxKdfLG1CM">
<ds:Transforms>
<ds:Transform+Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod+Algorithm="http://www.w3.org/2001/04/xmldsig#sha256" />
<ds:DigestValue>K/L270iu1kwY3xiqbfgvb3oqJlpArD05A9W/zf7wASk=</ds:DigestValue>
```

2654

2655 9. Scroll down the SAML message and locate the AttributeStatement node and sub-nodes.

```
Untitled - Notepad
File Edit Format View Help

POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionId="n27ql60v17N_xx8QLxKdfLG1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp_abac_test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:Conditions+NotBefore="2015-
07-27T17:41:21.439Z"+NotOnOrAfter="2015-07-
27T17:36:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint_abac_test</saml:Audience></saml:AudienceRestrictionCondition></saml:Conditions><saml:AuthenticationStatement+AuthenticationInstant="2015-07-
27T17:36:21.424Z"><AuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:AuthenticationStatement><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="urn:attributeNamespace">http://schemas.xmlsoap.org/ws/2005/05/identity/claims"</saml:Attribute><saml:AttributeValue>Conway</saml:AttributeValue></saml:AttributeStatement><ds:Signature+xmldns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod+Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference+URI="#n27ql60v17N_xx8QLxKdfLG1CM">
```

2656

2657 10. For the AttributeStatement node and sub-nodes, enter some carriage returns before each XML
2658 tag to make it easier to examine the data. The goal is to be able to easily examine the Attribute
2659 nodes within the AttributeStatement node.

```
Untitled - Notepad
File Edit Format View Help

POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionId="n27ql60v17N_xx8QLxKdfLG1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp_abac_test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:Conditions+NotBefore="2015-07-27T17:41:21.439Z"+NotOnOrAfter="2015-07-27T17:36:21.424Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint_abac_test</saml:Audience></saml:AudienceRestrictionCondition></saml:Conditions><saml:AuthenticationStatement+AuthenticationInstant="2015-07-27T17:36:21.424Z"><AuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:AttributeStatement><saml:Subject><saml:NameIdentifier+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute><saml:AttributeName='urn:attributeNamespace'>http://schemas.xmlsoap.org/ws/2005/05/identity/claims"</saml:AttributeName><saml:AttributeValue>lsmith</saml:AttributeValue></saml:Attribute></saml:AttributeStatement>
```

2660

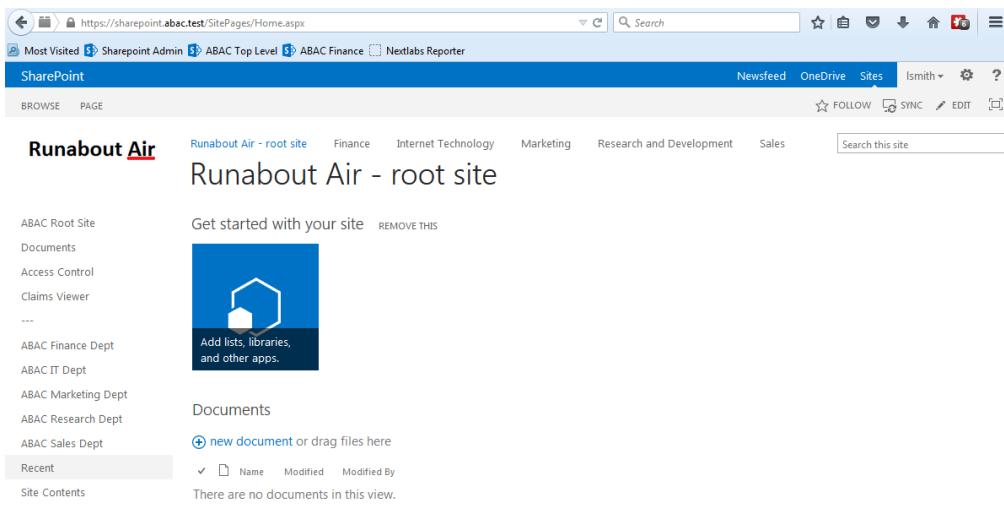
2661 Expected Result: Within the AttributeStatement node, there should be an Attribute sub-node.
2662 The Attribute sub-node should have an AttributeName value of “upn”. The AttributeNamespace
2663 value should be *http://schemas.xmlsoap.org/ws/2005/05/identity/claims*. There should be an
2664 AttributeValue sub-node and it should contain the account username (e.g., “lsmith”) that was

2665 used to authenticate at the identity provider (e.g.,
 2666 <saml:AttributeValue>Ismith</saml:AttributeValue>).

2667 **Expected Result:** Verify that the name (and case) of the attribute (noted by the AttributeName) is identical to the name configured at the SharePoint using Powershell earlier in this section.
 2668 Verify that the AttributeNamespace is identical to the IncomingClaimType option configured at the SharePoint using Powershell earlier in this section. If the name or namespace of the attribute being passed to SharePoint does not match with the SharePoint configuration, SharePoint will not allow access to the site, and direct your browser back to the SharePoint Sign On screen.

2674 11. If you verified that the name and namespace of the expected attribute match with the SharePoint configuration and SharePoint does not direct your browser to the site home page, follow the instructions in the Troubleshooting SharePoint Federated Authentication Problems section to determine the cause of the problem.

2678 **Expected Result:** Go back to the main browser window. The SharePoint server should present the site home page. You should see the account username of the user that authenticated in the upper right corner of the page.



2681

2682 5.6 Troubleshooting SharePoint Federated Authentication Problems

2683 If you encounter a situation where SharePoint is not allowing a federated user access to the site, you
 2684 may have a problem with the authentication configuration. A symptom that indicates you have an
 2685 authentication configuration problem is when a user successfully signs on at the identity provider, then
 2686 the user is redirected back to the SharePoint site, and instead of displaying the site home page,
 2687 SharePoint presents the SharePoint Sign On screen again. This section describes how to determine the
 2688 root cause of this type of authentication problem so that the problem can be resolved.

2689 **Note:** A SharePoint access control problem is a distinctly separate issue from authentication. A symptom
 2690 of an access control problem is when the user received a message that states "This site has not been
 2691 shared with you" upon successful authentication. Access control problems can be resolved by setting up

SECOND DRAFT

- 2692 SharePoint permissions on the People and Groups administration page, located in the Site Settings,
2693 Users and Permissions group.
- 2694 Follow the instructions below to troubleshoot federated authentication problems at the SharePoint site.
- 2695 Before you configure diagnostic logging for the SharePoint site to determine the root cause of the
2696 authentication problem, check the following items first:
- 2697
 - Verify that the relying party's PingFederate Server and the relying party's SharePoint Server
2698 synchronize their clocks from the same source. If both servers are on the same domain, they
2699 should be synchronized with the domain controller automatically. Logon to both servers and
2700 verify that the clocks display the same time.
 - Verify that the expiration time of the security token generated by the PingFederate Server is
2701 more than 10 minutes. SharePoint calculates the time length of its session using the formula:
2702 $\text{SharePointSessionTime} = \text{SecurityTokenLifeTime} - \text{LogonTokenCacheExpirationWindow}$.
2703 SecurityTokenLifeTime is the length of time the token is valid, and this time is generated by the
2704 PingFederate server when it issues the token. By default the SharePoint
2705 LogonTokenCacheExpirationWindow is set to 10 minutes, therefore the SecurityTokenLifeTime
2706 must be greater than 10 in order to generate a SharePointSessionTime greater than zero. In our
2707 build we set the SecurityTokenLifetime to 20 minutes in the PingFederate configuration.
 - The expiration time of the security token can be set in the configuration of the SP
2708 Connection on the relying party's PingFederate server. When you open the configuration for
2709 the SP Connection, click on the Assertion Lifetime link in the Browser SSO section. Enter a
2710 value for the Minutes After field that is greater than 10 (e.g., 20).

The screenshot shows the 'Assertion Lifetime' configuration page for a SharePoint connection. At the top, there are tabs for Main, SP Connection, and Browser SSO. Under the SP Connection tab, there are sub-tabs for Assertion Lifetime, Assertion Creation, Protocol Settings, and Summary. The Assertion Lifetime sub-tab is active, indicated by a teal background. Below the tabs, a note says: 'When an assertion is issued to the SP, there is a timeframe of validity before and after issuance. Please specify these parameters below.' There are two input fields: 'Minutes Before' with a value of '5' and 'Minutes After' with a value of '20'. At the bottom right are four buttons: Cancel, Next >, Done, and Save.

- 2713 2714 If you checked the items in the previous section and you are still encountering authentication problems,
2715 you will need to examine detailed authentication logs on the SharePoint server. Follow the instructions
2716 below to configure diagnostic logging on the SharePoint server and analyze the logs to determine the
2717 root of the authentication problem.
- 2718 1. Perform the instructions at the link below to change the levels of ULS authentication logging on
2719 the SharePoint server. Make sure that you perform the instructions in the following two sections
2720 of the article:
- 2721
 - "To configure SharePoint 2013 for the maximum amount of user authentication logging"

- 2722 ■ “To find the failed authentication attempt manually”
2723 <https://technet.microsoft.com/en-us/library/JJ906556.aspx>
- 2724 2. Once you configure the SharePoint diagnostic authentication logging, perform the sign on
2725 process to your SharePoint again to generate activity in the log.
- 2726 Since the SharePoint ULS log file contains many entries, it can be helpful to copy the file to
2727 another computer and analyze it offline.
- 2728 3. Open a copy of the log file and scroll to the bottom of the file. The bottom of the log contains
2729 the most recent activity.
- 2730 4. Starting at the bottom of the file, perform an upward search for the term “authentication”.
2731 Examine the entries that are labeled either “Claims Authentication” or “Authentication
2732 Authorization”.
- 2733 Look at the details for each of these two types of authentication entries to look for clues regarding what
2734 the source of the problem could be. You may have to look through several entries in the file to
2735 understand the sequence of events.
- 2736 We used this approach to troubleshoot an authentication problem in our lab. We found the following
2737 entry in the log file, that seemed as though it could be the source of the problem:
- 2738 ■ security token '0e.t|federated logon from identity provider|lsmithcc221cd9-23d7-4302-b029-
2739 ee81784754d2_Internet' is found in the local cache, but it is expired. Returing Null.
- 2740 Two lines further down in the file, we found the following entry as well:
- 2741 ■ token cache: Failed to find token for user '0e.t|federated logon from identity provider|lsmith'
2742 for cookie so signing out the user
- 2743 Based on the log file, we performed an Internet search for the term “security token is found in the local
2744 cache, but it is expired. Returing Null”. By researching various Internet blogs and forums, and
2745 performing additional analysis of the log file, we found a blog article on the PingIdentity website that
2746 described why the lifetime of the security token generated by the PingFederate-RP must be greater than
2747 10 minutes when issuing a token for SharePoint. Once we updated the associated configuration on the
2748 PingFederate-RP, the authentication problem was resolved.

6 Attribute Exchange between the Identity Provider and Relying Party

6.1 Introduction

In previous sections of this How-To Guide, we demonstrated foundational steps to building an ABAC solution:

- configuring federated authentication at the PingFederate-IdP
- configuring the SAML exchange between the PingFederate-IdP and PingFederate-RP
- configuring the Relying Party's SharePoint site
- configuring the federated logon at the SharePoint site

Building upon that foundation, this section describes how to:

- create custom attributes and set values for them in Microsoft AD
- configure the PingFederate-IdP to pull user and environmental attributes during authentication
- configure the PingFederate-RP to pass the user and environmental attributes to the RP's SharePoint
- configure SharePoint to load the user and environmental attributes passed from the PingFederate-RP into the web session

If you follow the instructions in this How-To Guide section, you will be able to perform a Functional Test to verify the successful completion of the steps for installing, configuring, and integrating the components.

6.2 Create Custom User Attributes in Microsoft AD

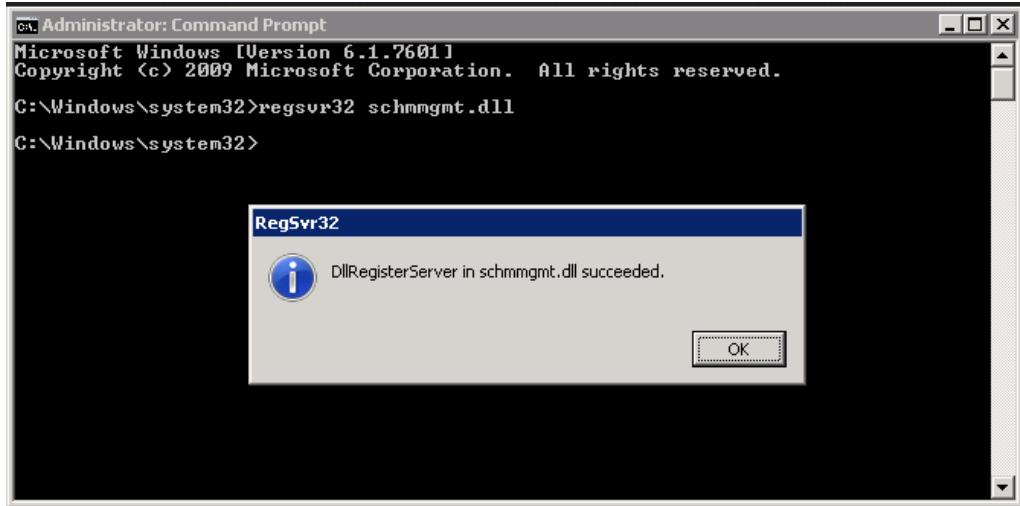
Follow the instructions in this section to create custom user attributes in the Microsoft AD schema. You will add a new attribute and add it to the “user” class. Microsoft AD user accounts inherit from the “user” class; therefore, the new attribute will be available to all of the users in the domain.

6.2.1 Preparing the AD Schema for Creating New Custom Attributes

6.2.1.1 Backing Up Your Directory before Making Schema Changes

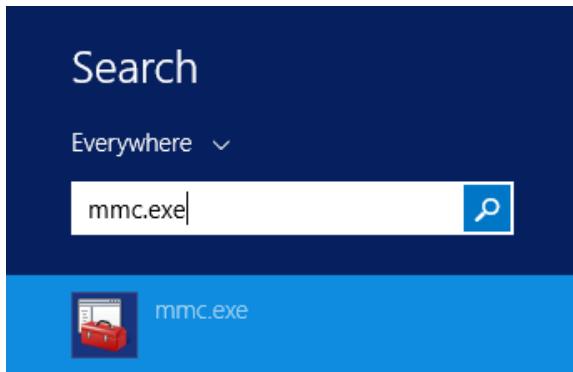
Microsoft recommends that you back up your directory before making schema changes. Choose the names of your new custom attributes carefully, because the creation of a new attribute is a permanent operation.

1. Log on to the server that contains the Microsoft AD schema (typically the schema is on the domain controller).
2. Launch a Command Prompt, using the Run as Administrator option.
3. Execute the following command:
`regsvr32 schmmgmt.dll`

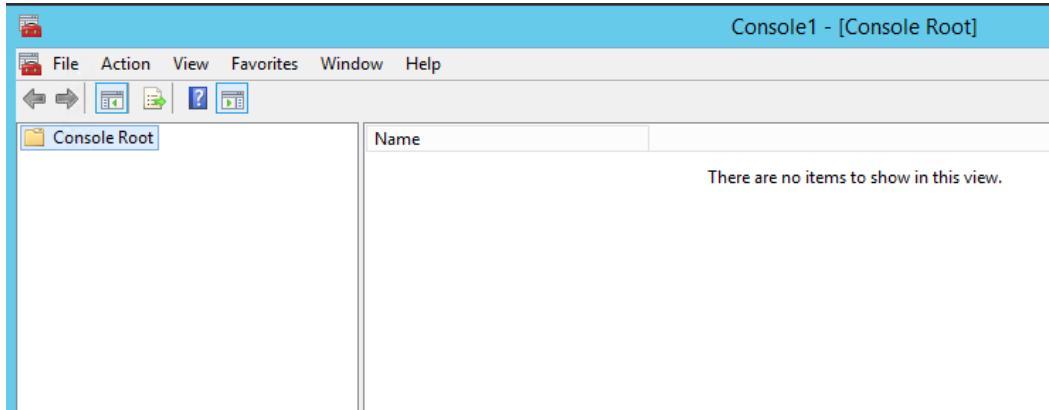


2782

- 2783 4. Click the **Start** button and enter **mmc.exe** in the search field.
2784 5. Launch the **mmc.exe** program.

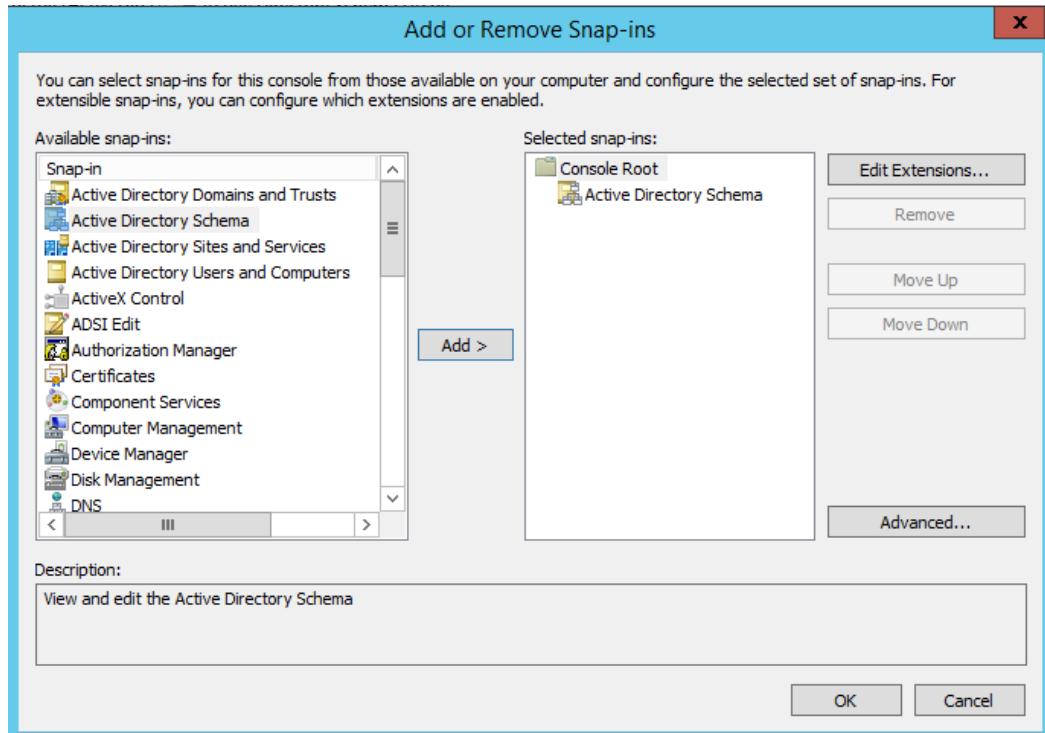


2785

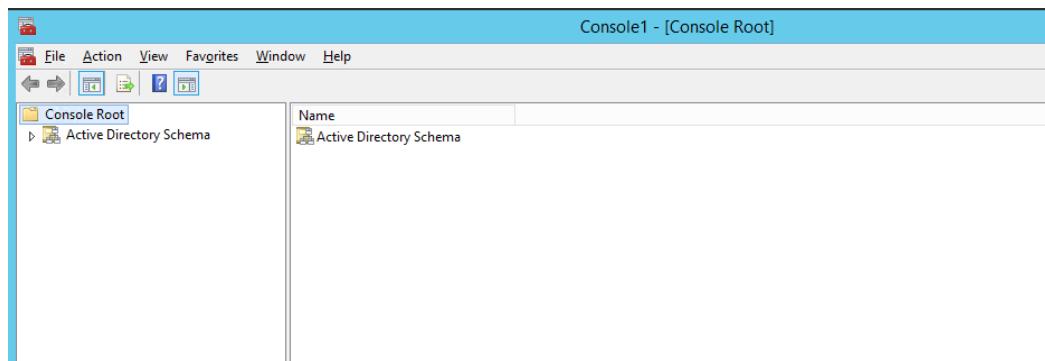


2786

- 2787 6. Click on the **File** menu. Then, click **Add / Remove Snap-in**.
2788 7. Click on **Active Directory Schema** in the list of **Available snap-ins** on the left; then, click **Add** to
2789 add it to the **Selected snap-ins** on the right.
2790 8. Click **OK**.



2791



2792

2793 9. Expand the **Active Directory Schema** on the left.

2794 **6.2.1.2 Reviewing Existing Attributes to Avoid Redundancies when Creating New Attributes**

2796 Before you create a new attribute, it is important to review existing user attributes in your Active
2797 Directory Schema. Under Active Directory Schema on the left, expand the Classes folder and scroll down
2798 to click on the **user** class. Examine the existing set of **user** class attributes listed on the right. These
2799 attributes are native to Active Directory, and can be assigned to users as subject attributes. These
2800 attributes may meet existing requirements for implementing subject attribute, alleviating the need to
2801 add custom attributes to the schema. You can list the attributes in alphabetical order by clicking on the
2802 **Name** column.

SECOND DRAFT

Console1 - [Console Root\Active Directory Schema [ActiveDirectory.ABAC.TEST]\Classes\user]

The screenshot shows the Active Directory Schema console with the 'user' class selected. The left pane displays a tree view of schema objects, and the right pane shows a table of attributes for the 'user' class. The table includes columns for Name, Type, System, Description, and Source Class.

Name	Type	System	Description	Source Class
accountExpires	Optional	Yes	Account-Expires	user
accountNameHistory	Optional	Yes	Account-Name-History	securityPrincipal
aCSPolicyName	Optional	Yes	ACS-Policy-Name	user
adminCount	Optional	Yes	Admin-Count	user
adminDescription	Optional	Yes	Admin-Description	top
adminDisplayName	Optional	Yes	Admin-Display-Name	top
allowedAttributes	Optional	Yes	Allowed-Attributes	top
allowedAttributesEffective	Optional	Yes	Allowed-Attributes-Effe...	top
allowedChildClasses	Optional	Yes	Allowed-Child-Classes	top
allowedChildClassesEffective	Optional	Yes	Allowed-Child-Classes-...	top
altSecurityIdentities	Optional	Yes	Alt-Security-Identities	securityPrincipal
assistant	Optional	Yes	Assistant	organizationalPerson
attributeCertificateAttribute	Optional	No	A digitally signed or cert...	person
audio	Optional	No	The Audio attribute type...	user
badPasswordTime	Optional	Yes	Bad-Password-Time	user
badPwdCount	Optional	Yes	Bad-Pwd-Count	user
bridgeheadServerListBL	Optional	Yes	Bridgehead-Server-List-BL	top
businessCategory	Optional	Yes	Business-Category	user
c	Optional	Yes	Country-Name	organizationalPerson
canonicalName	Optional	Yes	Canonical-Name	top
carLicense	Optional	No	Vehicle license or registr...	user
clearance	Optional	No	user	user
cn	Mandatory	Yes	Common-Name	mailRecipient
cn	Optional	No	Common-Name	posixAccount
cn	Mandatory	Yes	Common-Name	person
cn	Optional	Yes	Common-Name	top

2803

2804 If you wanted to create an attribute to store the user's cell phone number, you would look through the
2805 attributes and notice that the attribute **cellphone** does not exist. However, there is an attribute named
2806 **mobile** that could be used to store a cell phone number.

Console1 - [Console Root\Active Directory Schema [ActiveDirectory.ABAC.TEST]\Classes\user]

The screenshot shows the Active Directory Schema console with the 'user' class selected. The left pane displays a tree view of schema objects, and the right pane shows a table of attributes for the 'user' class. The table includes columns for Name, Type, System, Description, and Source Class.

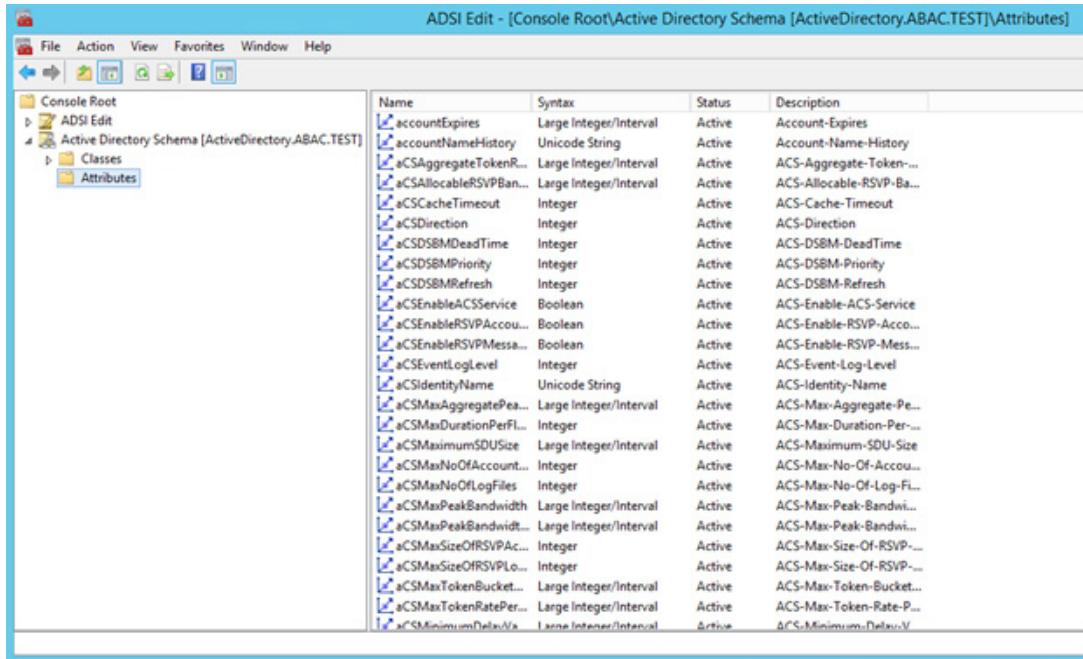
Name	Type	System	Description	Source Class
mobile	Optional	Yes	Phone-Mobile-Primary	organizationalPerson
modifyTimeStamp	Optional	Yes	Modify-Time-Stamp	top
ms-DS-ConsistencyChildCount	Optional	Yes	MS-DS-Consistency-Chi...	top
ms-DS-ConsistencyGuid	Optional	Yes	MS-DS-Consistency-Guid	top
ms-DS-CreatorSID	Optional	Yes	MS-DS-Creator-SID	user
msCOM-PartitionSetLink	Optional	Yes	Link from a Partition to ...	top
msCOM-UserLink	Optional	Yes	Link from a PartitionSet ...	top
msCOM-UserPartitionSetLink	Optional	Yes	Link from a User to a Par...	user
msDS-ComputerReferenceBL	Optional	No	Backlink attribute for ms...	top
msDS-MemberReferenceBL	Optional	No	Backlink attribute for ms...	top
msDRM-IdentityCertificate	Optional	Yes	The XML digital rights ...	user
msDS-AllowedToActOnBehalfOfO...	Optional	Yes	This attribute is used for...	organizationalPerson
msDS-AllowedToDelegateTo	Optional	Yes	Allowed-To-Delegate-T...	organizationalPerson
msDS-Approx-Immed-Subordinates	Optional	Yes	ms-DS-Approx-Immed-...	top
msDS-AssignedAuthNPolicy	Optional	Yes	This attribute specifies ...	user
msDS-AssignedAuthNPolicySilo	Optional	Yes	This attribute specifies ...	user
msDS-AuthenticatedAtDC	Optional	Yes	Forwardlink for ms-DS-...	user
msDS-AuthenticatedToAccountlist	Optional	Yes	Backlink for ms-DS-Aut...	top
msDS-AuthNPolicySiloMembersBL	Optional	Yes	This attribute is the back...	user
msDS-Cached-Membership	Optional	Yes	ms-DS-Cached-Membe...	user
msDS-Cached-Membership-Time-...	Optional	Yes	ms-DS-Cached-Membe...	user
msDS-ClaimSharesPossibleValues...	Optional	Yes	For a claim type object, ...	top
msDS-cloudExtensionAttribute1	Optional	No	An attribute used to hou...	msDS-CloudExtensions
msDS-cloudExtensionAttribute10	Optional	No	An attribute used to hou...	msDS-CloudExtensions
msDS-cloudExtensionAttribute11	Optional	No	An attribute used to hou...	msDS-CloudExtensions
msDS-cloudExtensionAttribute12	Optional	No	An attribute used to hou...	msDS-CloudExtensions

2807

2808 Once you have identified that the creation of a new attribute is warranted, proceed with the following
2809 instructions.

2810 ***6.2.1.3 Creating New Custom Attributes***

- 2811 1. Launch a browser window and go the Microsoft site:
<https://gallery.technet.microsoft.com/scriptcenter/56b78004-40d0-41cf-b95e-6e795b2e8a06>
- 2812 2. Copy the **oidgen.vbs** script code that is shown on the page to the clipboard.
- 2813 3. Open **Notepad** and paste the script into the editor.
- 2814 4. Save the script to a file on the desktop named **oidgen.vbs**.
- 2815 5. Go back to the Active Directory schema window.
- 2816 6. On the left pane, click on the **Attributes** folder.

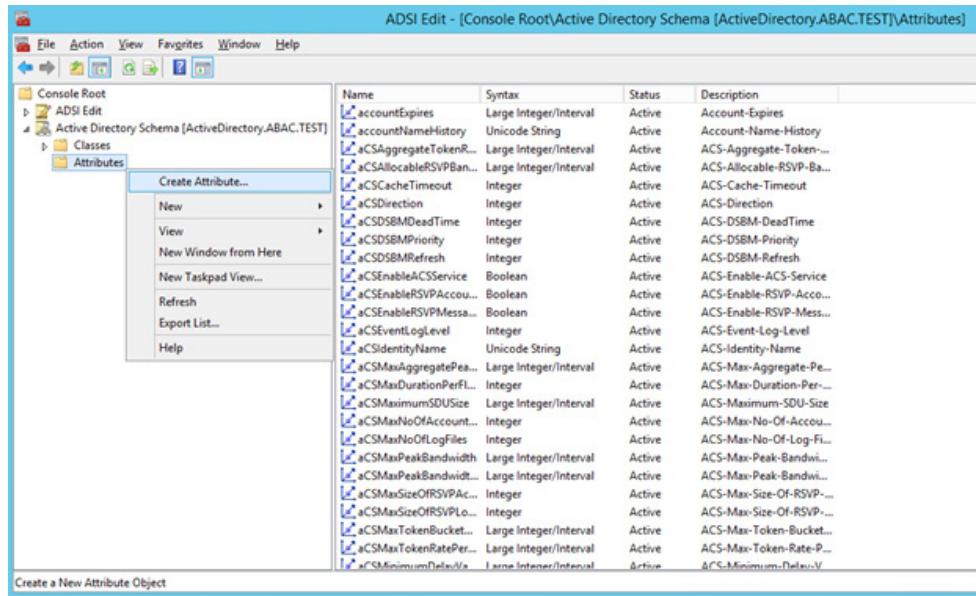


The screenshot shows the ADSI Edit interface with the title bar "ADSI Edit - [Console Root\Active Directory Schema [ActiveDirectory.ABAC.TEST]\Attributes]". The left pane displays a tree view with "Console Root", "ADSI Edit", "Active Directory Schema [ActiveDirectory.ABAC.TEST]", "Classes", and "Attributes". The "Attributes" folder is selected. The right pane is a table listing various attributes with their names, syntax, status, and descriptions. Some descriptions are truncated with ellipses.

Name	Syntax	Status	Description
aCSDSBRMPriority	Integer	Active	ACS-DSBM-Priority
aCSDSBRMRefresh	Integer	Active	ACS-DSBM-Refresh
aCSEnableACService	Boolean	Active	ACS-Enable-ACS-Service
aCSEnableRSVPAccou...	Boolean	Active	ACS-Enable-RSVP-Accou...
aCSEnableRSVPMessa...	Boolean	Active	ACS-Enable-RSVP-Messa...
aCSEventLogLevel	Integer	Active	ACS-Event-Log-Level
aCSIdentityName	Unicode String	Active	ACS-Identity-Name
aCSMaxAggregatePea...	Large Integer/Interval	Active	ACS-Max-Aggregate-Pe...
aCSMaxDurationPerFl...	Integer	Active	ACS-Max-Duration-Per...
aCSMaximumSDUSize	Large Integer/Interval	Active	ACS-Maximum-SDU-Size
aCSMaxNoOfAccount...	Integer	Active	ACS-Max-No-Of-Accou...
aCSMaxNoOfLogFiles	Integer	Active	ACS-Max-No-Of-Log-Fi...
aCSMaxPeakBandwidth	Large Integer/Interval	Active	ACS-Max-Peak-Bandwid...
aCSMaxPeakBandwidtht...	Large Integer/Interval	Active	ACS-Max-Peak-Bandwid...
aCSMaxSizeOfRSVPAc...	Integer	Active	ACS-Max-Size-Of-RSVP...
aCSMaxSizeOfRSVPLo...	Integer	Active	ACS-Max-Size-Of-RSVP...
aCSMaxTokenBucket...	Large Integer/Interval	Active	ACS-Max-Token-Bucket...
aCSMaxTokenRatePer...	Large Integer/Interval	Active	ACS-Max-Token-Rate-P...
aCSMinimumDelayVa...	Large Integer/Interval	Active	ACS-Minimum-Delay-V...

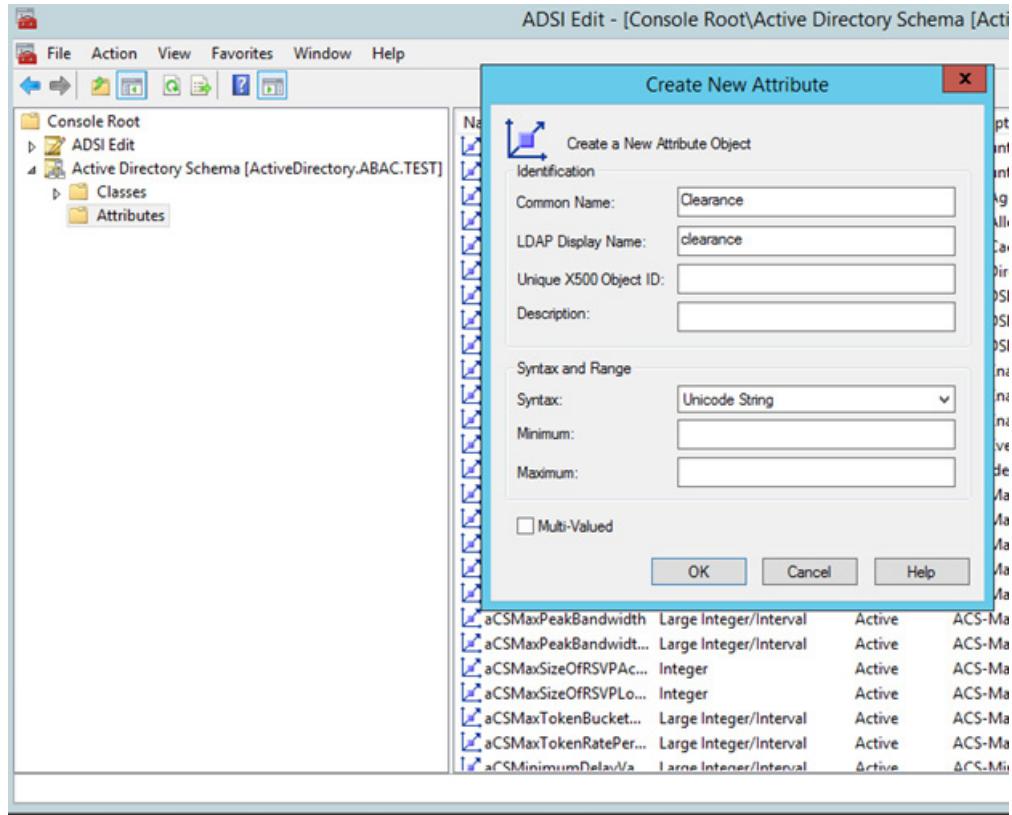
- 2818 7. Right-click on the **Attributes** folder and select Create Attribute.
- 2819 8. Click **Continue** on the warning window.

SECOND DRAFT



2821

- 2822 9. Enter the name of your new attribute and select the type of attribute in the Syntax field. In the
2823 example below, the name of the new attribute is **clearance** and the type of attribute is **Unicode
2824 String**.

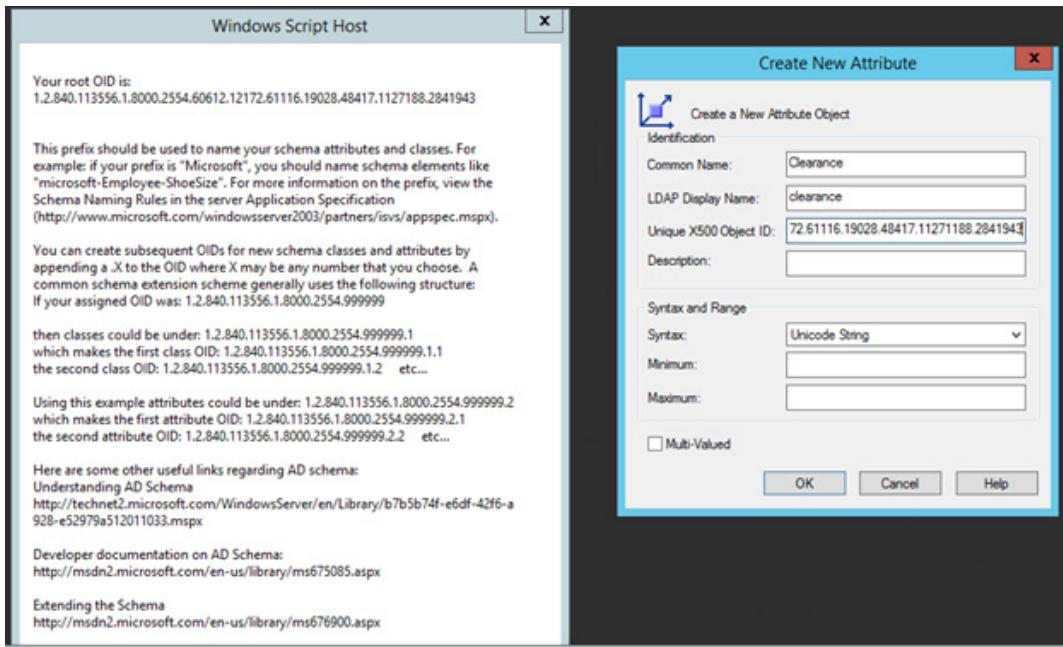


2825

2826 ***6.2.1.4 Generating an ID to Enter into the Unique X500 Object ID Field***

2827 Next, you need to generate an ID to enter into the Unique X500 Object ID field.

- 2828 1. Go to the desktop and double-click on the **oidgen.vbs** script that was saved earlier. This should
2829 execute the script to generate a unique Object ID.
- 2830 2. Enter this long Object ID into the **Unique X500 Object ID** field in the Active Directory Create New
2831 Attribute window.



- 2832
- 2833 3. Click **OK** to create the new attribute.
- 2834 4. Scroll down the list of attributes and make sure your newly added attribute is listed there.

Name	Syntax	Status	Description
clearance	Unicode String	Active	
c	Unicode String	Active	Country-Name
cACertificate	Octet String	Active	CA-Certificate
cACertificateDN	Unicode String	Active	CA-Certificate-DN
cAConnect	Unicode String	Active	CA-Connect
canonicalName	Unicode String	Active	Canonical-Name
canUpgradeScript	Unicode String	Active	Can-Upgrade-Script
carLicense	Unicode String	Active	Vehicle license or registr...
catalogs	Unicode String	Active	Catalogs
categories	Unicode String	Active	Categories
categoryld	Octet String	Active	Category-Id
cAUsages	Unicode String	Active	CA-Usages
cAWEBURL	Unicode String	Active	CA-WEB-URL
certificateAuthorityO...	Distinguished Name	Active	Certificate-Authority-O...
certificateRevocationL...	Octet String	Active	Certificate-Revocation-L...
certificateTemplates	Unicode String	Active	Certificate-Templates
classDisplayName	Unicode String	Active	Class-Display-Name
cn	Unicode String	Active	Common-Name
co	Unicode String	Active	Text-Country
codePage	Integer	Active	Code-Page
cOMClassID	Unicode String	Active	COM-ClassID
cOMCLSID	Unicode String	Active	COM-CLSID
cOMInterfaceID	Unicode String	Active	COM-InterfaceID
comment	Unicode String	Active	User-Comment
cOMOtherProgId	Unicode String	Active	COM-Other-Prog-Id
compliance	Unicode String	Active	Compliance

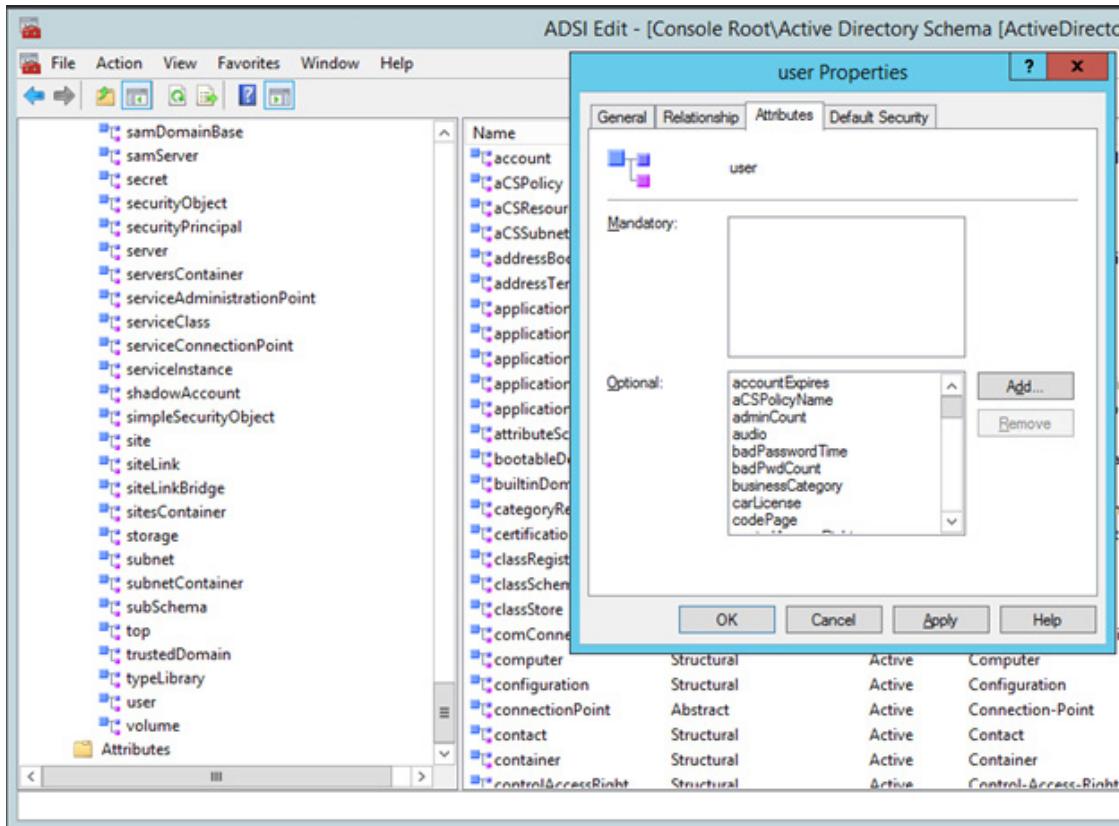
2835

2836 6.2.1.5 Adding the New Attribute to the User Class

2837 Next, you need to add the new attribute to the **user** class.

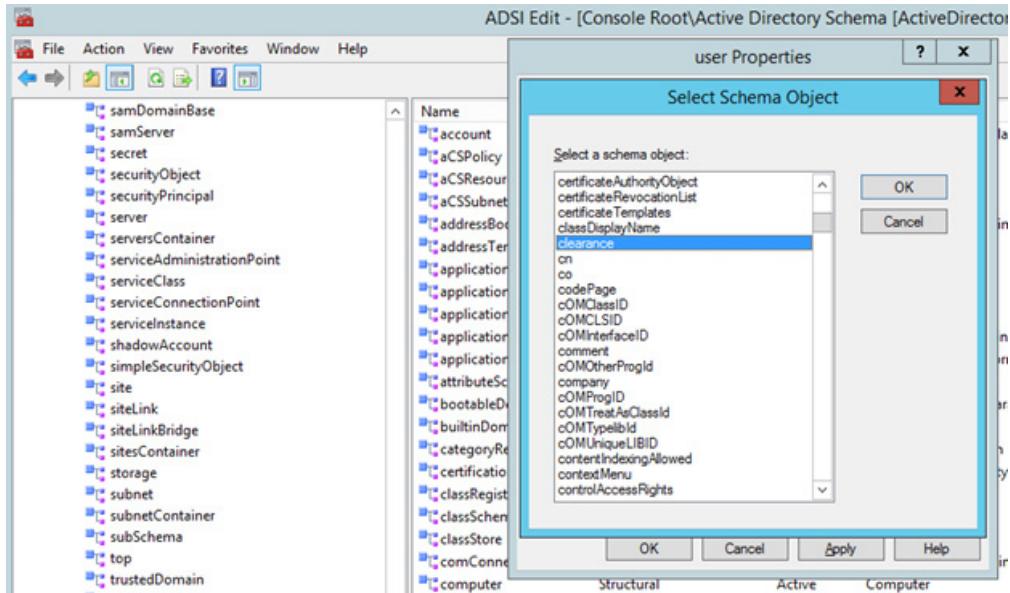
- 2838 1. In the left pane, expand the Classes folder. Scroll down the list of classes, right-click on the **user** class, and select **Properties**.
- 2839 2. Click on the **Attributes** tab.

SECOND DRAFT



2841

- 2842 3. Click **Add**. Scroll down and click on the new attribute.



2843

- 2844 4. Click **OK** on the Select Schema Object window, and then click **OK** one more time on the user properties window. At this point, you have added the new attribute to the **user** class.

2845
2846 When you examine the list of attributes for the **user** class, you should be able to see the new attribute.
2847

2848

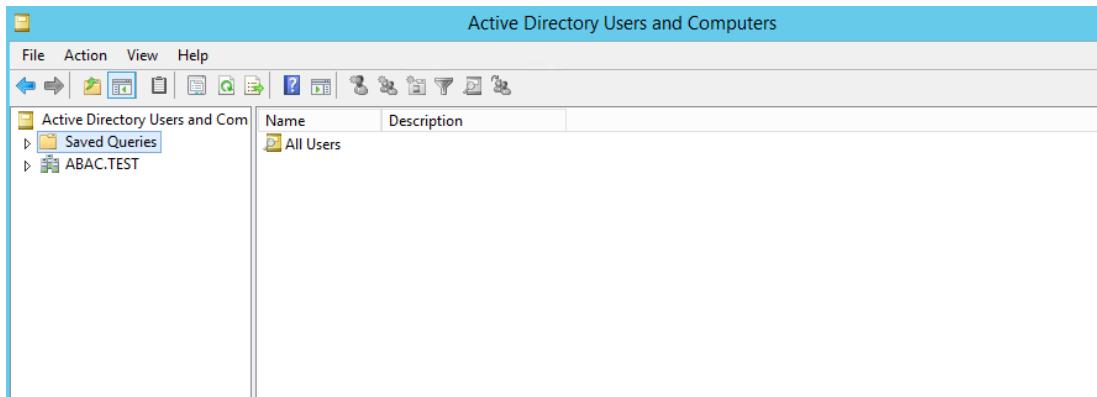
ADSI Edit - [Console Root\Active Directory Schema [ActiveDirectory.ABAC.TEST]\Classes\user]					
	Name	Type	System	Description	Source Class
	employeeType	Optional	No	Employee-Type	user
	employeeNumber	Optional	No	Employee-Number	user
	displayName	Optional	No	Display-Name	user
	departmentNumber	Optional	No	Identifies a department ...	user
	clearance	Optional	No		user
	carLicense	Optional	No	Vehicle license or registr...	user
	audio	Optional	No	The Audio attribute type...	user
	msDS-cloudExtensionAttribute20	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute19	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute18	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute17	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute16	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute15	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute14	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute13	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute12	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute11	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute10	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute9	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute8	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute7	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute6	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute5	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute4	Optional	No	An attribute used to hou...	msDS-CloudExter
	msDS-cloudExtensionAttribute3	Optional	No	An attribute used to hou...	msDS-CloudExter

2849 6.2.2 Set Values for Custom User Attributes in Microsoft AD

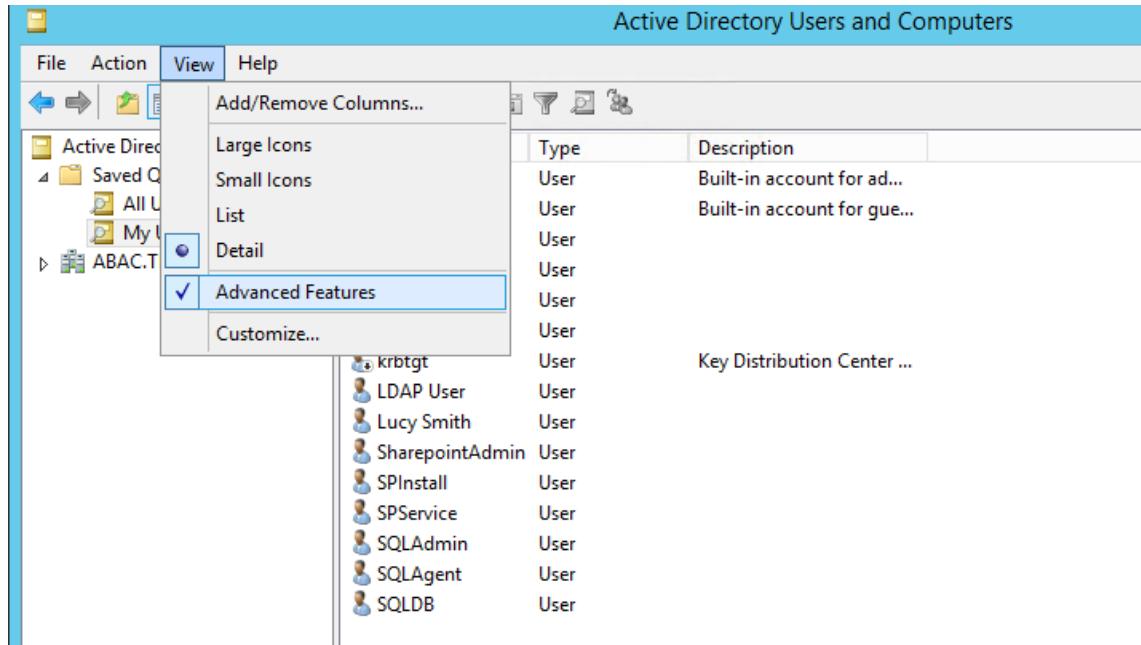
2850 Once you have created a new custom attribute in the Active Directory **user** class, that new attribute will
 2851 be available for all users in the domain. You will be able to set specific values for the new attribute for
 2852 each distinct user. Follow the instructions in this section to set a user-specific value for a new attribute
 2853 in Active Directory.

2854 1. Log on to the Microsoft AD server.

2855 2. Open the Active Directory Users and Computers program.

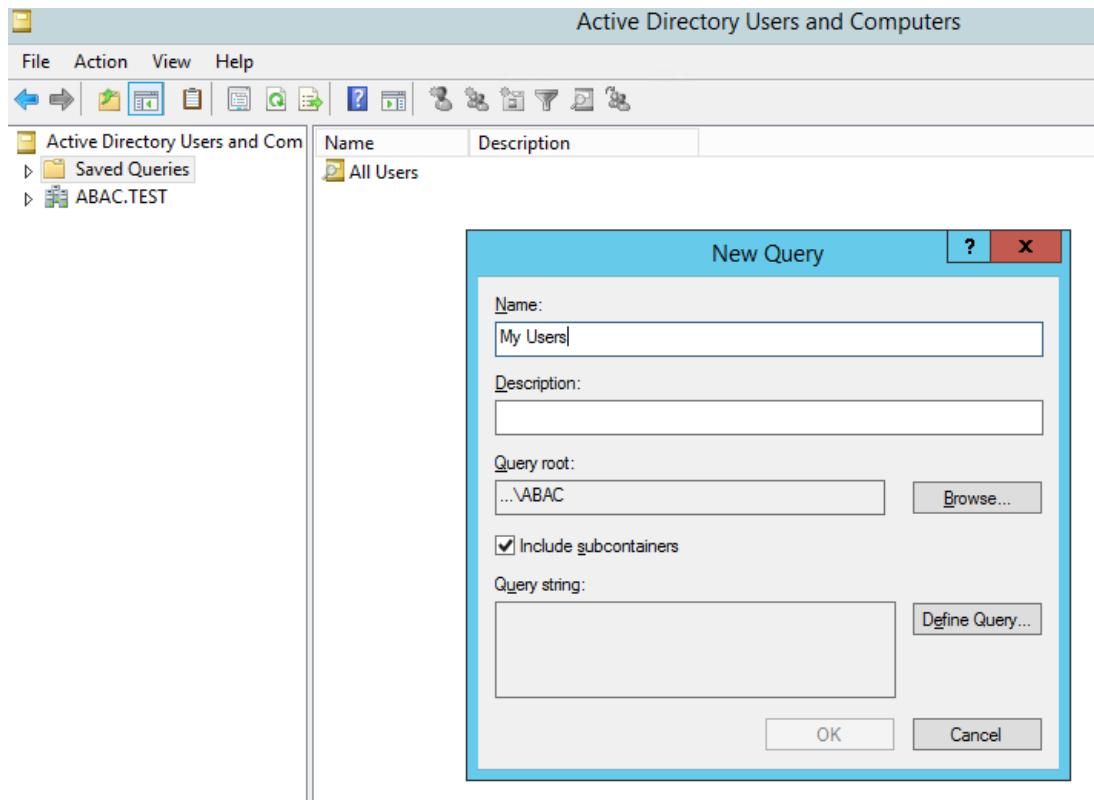


2857 3. Click on the **View** menu and select **Advanced Features**.



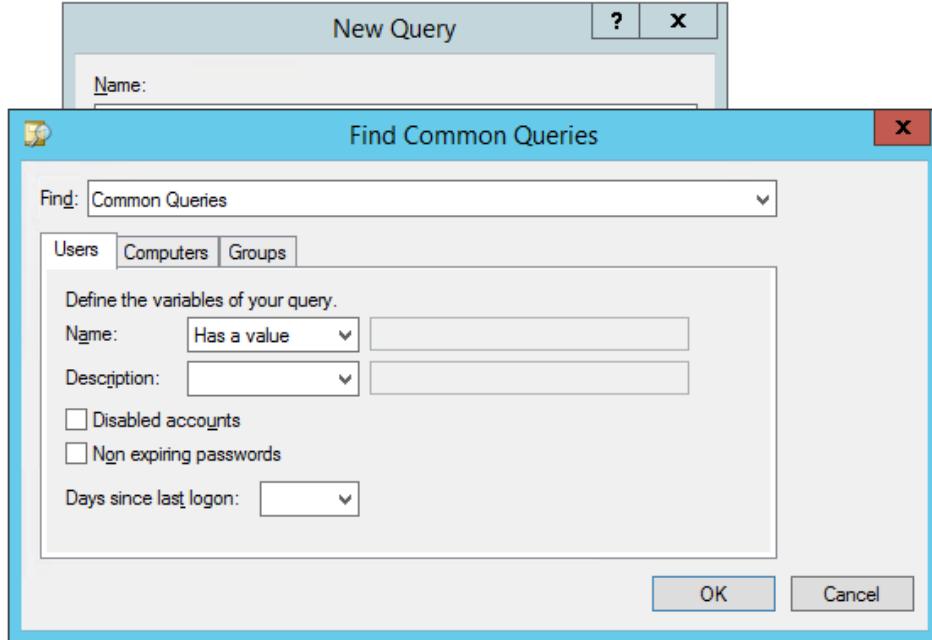
2858

- 2859 4. Right-click on Saved Queries and select **New > Query**. Enter a name for your query (e.g., **My
2860 Users**).



2861

- 2862 5. Click on **Define Query**. From the **Name** list, select **Has a value**.



2863

2864 6. Click **OK**. Then, click **OK** again to create your new query.

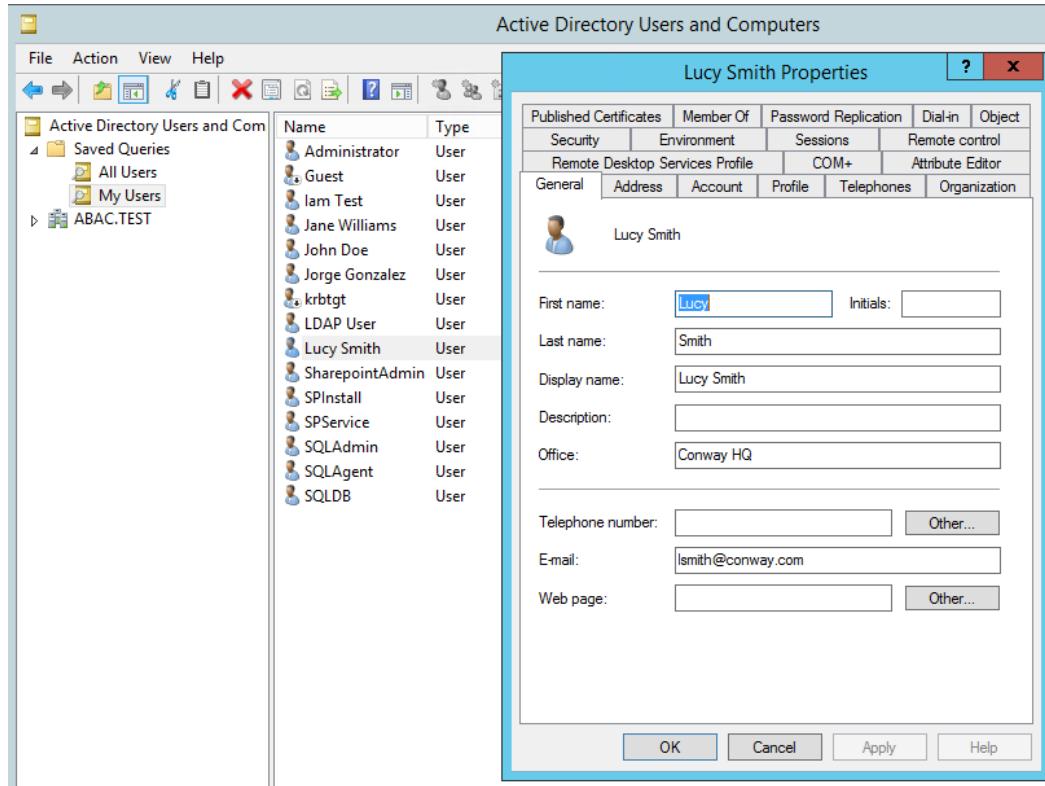
2865 You will see a list of Active Directory Users displayed in the right pane.

Name	Type	Description
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...
Iam Test	User	
Jane Williams	User	
John Doe	User	
Jorge Gonzalez	User	
krbtgt	User	Key Distribution Center ...
LDAP User	User	
Lucy Smith	User	
SharepointAdmin	User	
SPInstall	User	
SPService	User	
SQLAdmin	User	
SQLAgent	User	
SQLDB	User	

2866

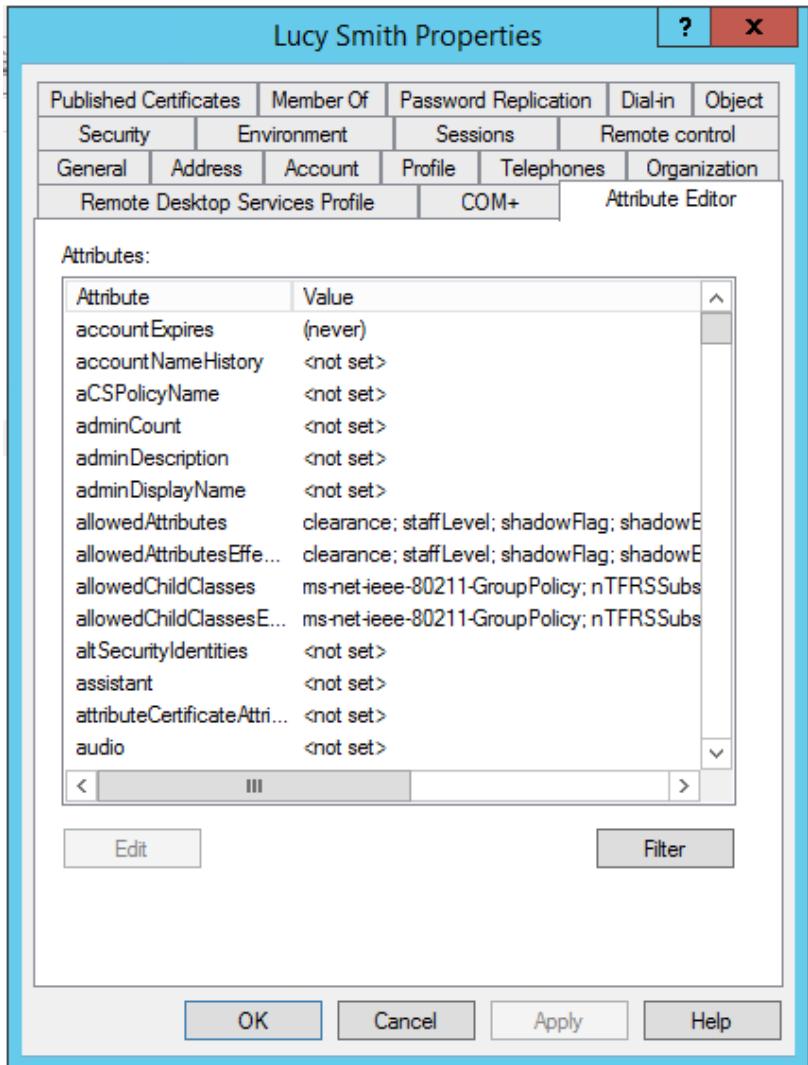
2867 7. Double-click on the specific user (e.g., **Lucy Smith**) that you want to modify to bring up the
2868 properties window.

SECOND DRAFT



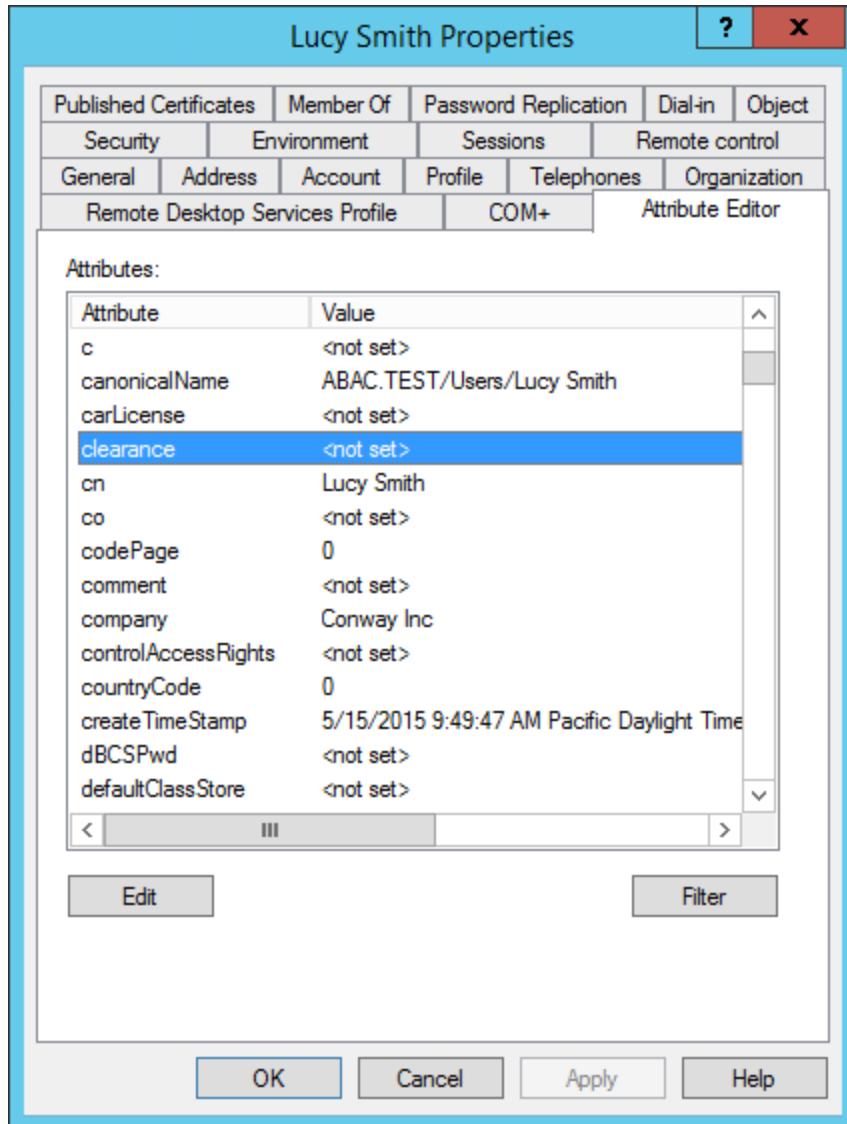
2869

2870 8. Click on the **Attribute Editor** tab.



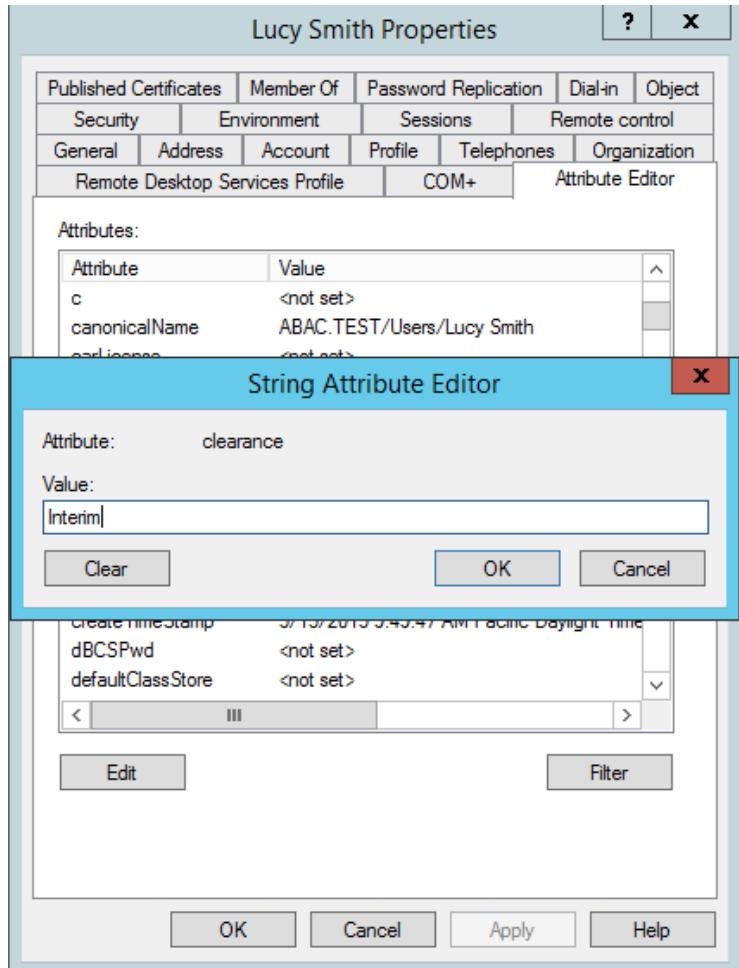
2871

- 2872 9. Scroll down and locate the new custom attribute for which you want to set a value (e.g.,
2873 **clearance**).



2874

- 2875 10. Double-click on the attribute, and enter a value suitable for your organization. In this example,
 2876 the **clearance** attribute will be set to a value of **Interim** for the user Lucy Smith in subsequent
 2877 steps.
- 2878 11. Click **OK** and then click **OK** again. The information is saved and the User Properties window
 2879 closes.



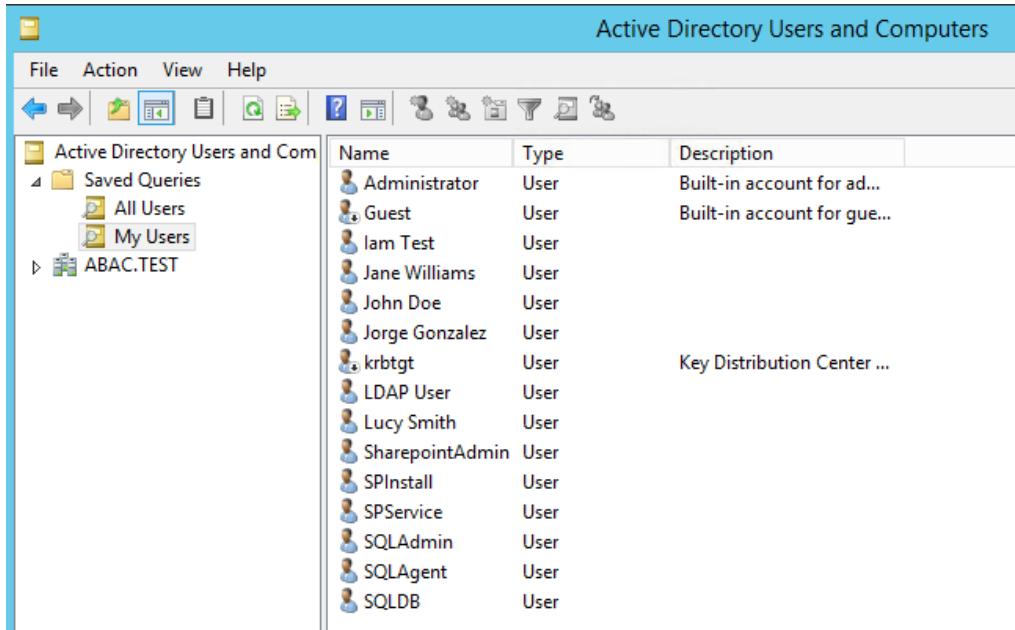
2880

2881 Note: When you set an attribute value in the attribute editor and then go back to the Users
 2882 query view, you have to press F5 or click the **Action menu > Refresh** to see the new value.

2883 *6.2.2.1 Adding New Columns to the Users Query View*

2884 Next you will add new columns to the Users query view to help monitor the custom attribute values for
 2885 each user in the directory. By default, the Users view only shows the attribute values for **Name, Type,**
 2886 and **Description**.

SECOND DRAFT



2887

- 2888 1. In the Saved Queries folder, click on the name of the query to be modified (e.g., **My Users**).
- 2889 2. Click on the **View** menu and select **Add/Remove Columns...**
- 2890 3. From the list of Available columns, scroll up or down to find desired columns.
- 2891 4. Click on column name and click on the **Add** button.
- 2892 5. When all desired columns have been chosen, click **OK**.

2893 The following screenshot shows a query view after adding custom attribute columns. The example
2894 contains new columns for the attributes **User Logon Name**, **Company**, **Department**, **Title**, **Staff Level**,
2895 and **Clearance**.

Name	User Logon Name	Type	Description	Company	Department	Title	Staff Level	Clearance
Administrator		User	Built-in ac...					
Guest		User	Built-in ac...					
Iam Test	itest@ABAC.TEST	User						
Jane Williams	jwilliams@ABAC.TEST	User		Conway Inc	Business Intelligence	Business Analyst		
John Doe	jdoe@ABAC.TEST	User						
Jorge Gonzalez	jgonzalez@ABAC.TEST	User		Conway Inc	Research & Development	Senior R&D Scientist		
krbtgt		User	Key Distrib...					
LDAP User	LDAPUser@ABAC.TEST	User						
Lucy Smith	lsmith@ABAC.TEST	User		Conway Inc	Business Intelligence	Business Analyst		Interim
SharepointAdmin	SharepointAdmin@ABAC.TEST	User						
SPInstall	SPInstall@ABAC.TEST	User						
SPService	SPService@ABAC.TEST	User						
SQLAdmin	SQLAdmin@ABAC.TEST	User						
SQLAgent	SQLAgent@ABAC.TEST	User						
SQLDB	SQLDB@ABAC.TEST	User						

2896

2897 6.3 Configure PingFederate Servers to Pull User Attributes

2898 6.3.1 Configure PingFederate-IdP to Pull User Attributes During Authentication

2899 Follow the instructions in this section to configure the PingFederate-IdP to pull user attribute values
 2900 from Microsoft AD and Cisco ISE during the authentication process. In the following example, the value
 2901 for the user attribute **company** is extracted from Microsoft AD.

- 2902 1. Launch your browser and go to https://<DNS_NAME>:9999/pingfederate/app.
- 2903 2. Replace **DNS_NAME** with the fully qualified name of the IdP's PingFederate server (e.g.,
 2904 <https://idp.abac.test:9999/pingfederate/app>).
- 2905 3. Log on to the PingFederate application using the credentials you configured during installation.
- 2906 4. On the Main Menu under **SP CONNECTION**, click **Manage All SP**.

CONNECTION NAME	CONNECTION ID	PROTOCOL	STATUS	ACTION
Demo SP	PF-DEMO	SAML2.0	Active	Delete Copy Export Connection Export Metadata
https://rp.abac.test:9031	https://rp.abac.test:9031	SAML2.0	Active	Delete Copy Export Connection Export Metadata
urn:nccoe:abac:rp	urn:nccoe:abac:rp	SAML2.0	Active	Delete Copy Export Connection Export Metadata

Buttons at the bottom: Create Connection..., Import Connection, Check All Connections For Errors

Logging Mode Override: Off (radio button selected), On

2907

- 2908 5. Click on the link for the connection created in [Section 3](#) (e.g., <https://rp.abac.test:9031>).

SECOND DRAFT

Main	SP Connections	SP Connection			
Connection Type	Connection Options	General Info	Browser SSO	Credentials	Activation & Summary
<p><input checked="" type="checkbox"/> Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.</p>					
Connection Status	<input checked="" type="radio"/> Active <input type="radio"/> Inactive				
SSO Application Endpoint	https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=https://rp.abac.test:9031				
SP Connection					
CONNECTION TYPE					
Connection Role	SP				
Browser SSO Profiles	true				
Protocol	SAML 2.0				
Connection Template	No Template				
WS-Trust STS	false				
Outbound Provisioning	false				
CONNECTION OPTIONS					
Browser SSO	true				
IdP Discovery	false				
Attribute Query	false				
GENERAL INFO					
Partner's Entity ID (Connection ID)	https://rp.abac.test:9031				

2909

2910 6. On the Activation & Summary screen, scroll down to the **Assertion Creation** group and click on the **ATTRIBUTE CONTRACT** link.

2911

Main	SP Connection	Browser SSO	Assertion Creation											
Identity Mapping	Attribute Contract	Authentication Source Mapping	Summary											
<p><input checked="" type="checkbox"/> An Attribute Contract is a set of user attributes that this server will send in the assertion.</p>														
ATTRIBUTE CONTRACT SUBJECT NAME FORMAT <table border="1"> <tr> <td>SAML_SUBJECT</td> <td>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</td> <td>*</td> </tr> <tr> <td>EXTEND THE CONTRACT</td> <td>ATTRIBUTE NAME FORMAT</td> <td>ACTION</td> </tr> <tr> <td></td> <td>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</td> <td><input type="button" value="Add"/></td> </tr> </table>						SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	*	EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION		urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<input type="button" value="Add"/>
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	*												
EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION												
	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	<input type="button" value="Add"/>												
<input type="button" value="Cancel"/> <input type="button" value="< Previous"/> <input type="button" value="Next >"/> <input type="button" value="Done"/> <input type="button" value="Save"/>														

2912

2913 7. On the **Attribute Contract** screen, under the **EXTEND THE CONTRACT** column, enter the name of the attributes to be extracted from Microsoft AD, Cisco ISE, and RSA AA (e.g., **company**) in the empty text field.

2914

2915

SECOND DRAFT

2916

2917 8. Click **Add**.

An Attribute Contract is a set of user attributes that this server will send in the assertion.

EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
company	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add

Cancel < Previous Next > Done Save

2918

2919 9. Click **Save** to complete the configuration.

PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION
RSA Multifactor		Delete

Map New Adapter Instance...

Cancel < Previous Next > Done Save

2920

2921 6.3.1.1 *Functional Test of Pulling User Attributes During Authentication*

2922 The instructions in this section will help you perform a test to ensure that the Identity Provider is getting
 2923 the configured attributes (e.g., **company**) from Active Directory and passing them in a SAML message to
 2924 the RP. The Firefox SAML tracer add-on is used to examine the SAML message.

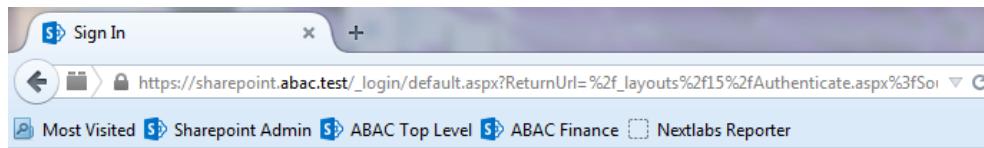
2925 Follow the instructions in the section Temporarily Disable SAML Encryption for Testing and
 2926 Troubleshooting Message Exchanges at the end of this section to disable SAML encryption. Once SAML
 2927 encryption has been disabled, you can proceed with the following functional test instructions.

- 2928 1. Launch your Firebox browser and select **SAML tracer** from the **Tools** menu.
 2929 This launches an empty SAML tracer window.

- 2930 2. Minimize the SAML tracer window.

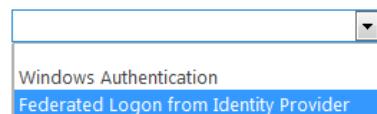
2931 The SAML tracer automatically records the details of the HTTPS messages in the background.

- 2932 3. Go back to the main browser window and go to the RP's SharePoint site (e.g.,
 2933 <https://SharePoint.abac.test>).



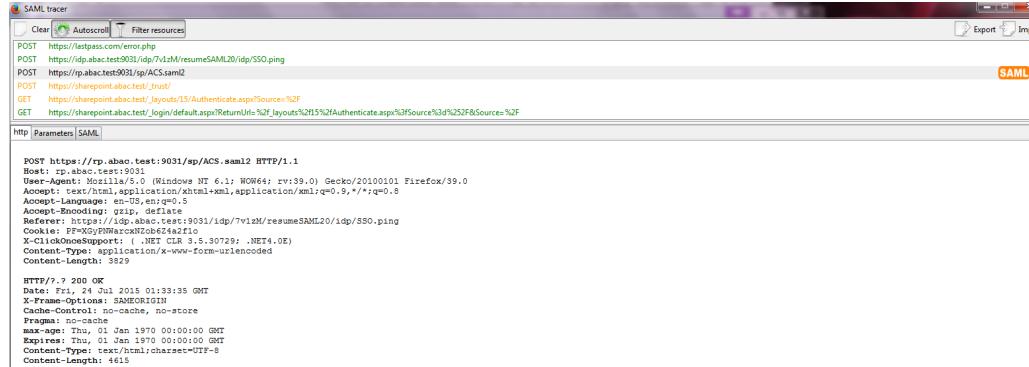
Sign In

Select the credentials you want to use to logon to this SharePoint site:



- 2934
- 2935 4. Select **Federated Logon from Identity Provider**.
- 2936 5. In the Identity Provider's PingFederate Sign On screen, enter the credentials for the account you
 2937 are testing with (e.g., **Ismith**) and click **Sign On**.
- 2938 6. On the RSA two-factor authentication screen, enter the validation code and proceed.
 2939 The browser redirects you to the PingFederate-RP and then to the RP's SharePoint site. You may
 2940 not notice the redirection to the PingFederate-RP if it happens quickly.
- 2941 7. Go back to the SAML tracer window. Scroll down and click on the last **POST** message that
 2942 contains a SAML icon.

SECOND DRAFT



The screenshot shows the SAML tracer interface. The top menu bar includes 'Clear', 'Autoscroll', 'Filter resources', 'Export', and 'Import'. A 'SAML' tab is selected. Below the tabs, there's a list of requests:

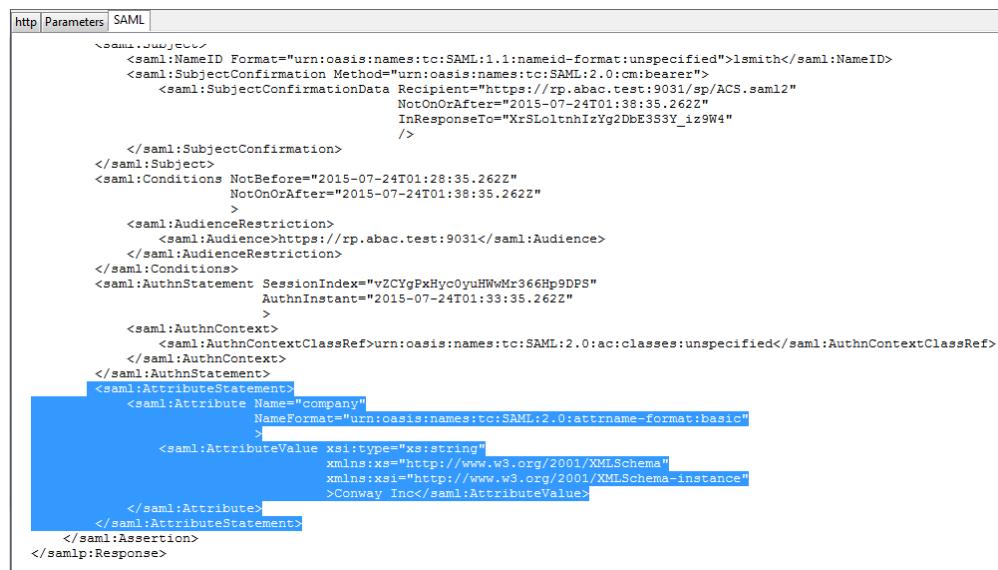
- POST https://rp.abac.test:9031/sp/ACS.saml2 HTTP/1.1
- POST https://idp.abac.test:9031/idp/v1/m/resumeSAML20/idp/SSO.ping
- POST https://rp.abac.test:9031/sp/ACS.saml2
- POST https://sharepoint.abac.test/_trust/
- GET https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
- GET https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2F.layouts%2FAuthenticate.aspx%3d%252F&Source=%2F

Below the requests, there are two tabs: 'Http Parameters' and 'SAML'. The 'Http Parameters' tab is currently active, showing the following request details:

```
Host: rp.abac.test:9031
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://idp.abac.test:9031/idp/v1/m/resumeSAML20/idp/SSO.ping
Cookie: PHPSESSID=jc6o2zaflo
X-ClickOnceSupport: (.NET CLR 3.5.30729; .NETA;0E)
Content-Type: application/x-www-form-urlencoded
Content-Length: 329
```

HTTP/1.1 200 OK
Date: Fri, 03 Jul 2015 01:38:35 GMT
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache, no-store
Pragma: no-cache
max-age: 0
Expires: Mon, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 4616

- 2943
- 2944 8. Click on the **SAML** tab. Scroll down the SAML message and locate the AttributeStatement node and sub nodes.
- 2945



The screenshot shows the SAML tracer interface with the 'SAML' tab selected. The message content is displayed as XML. A blue box highlights the `<saml:AttributeStatement>` node, specifically the `<saml:Attribute Name="company">` section. The XML code is as follows:

```
<saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">lsmith</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData Recipient="https://rp.abac.test:9031/sp/ACS.saml2"
      NotOnOrAfter="2015-07-24T01:38:35.262Z"
      InResponseTo="XrSLoitnh1zYg2DBE3S3Y_iz9W4">
  </saml:SubjectConfirmation>
  <saml:Conditions NotBefore="2015-07-24T01:28:35.262Z"
    NotOnOrAfter="2015-07-24T01:38:35.262Z">
  </saml:Conditions>
  <saml:AuthnStatement SessionIndex="vZYgPxHyo0yuHWMr366Hp9DBS"
    AuthnInstant="2015-07-24T01:33:35.262Z">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
  </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute Name="company">
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema"
          xmlns:xsd="http://www.w3.org/2001/XMLSchema-instance">Conway Inc</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

- 2946
- 2947 **Expected Result:** Ensure that the attribute you configured from Microsoft AD contains a node. In
2948 the example screenshot above, you can see that there is an Attribute node for the **company**
2949 attribute because of the line `<saml:Attribute Name= "company"`.

- 2950 **Expected Result:** Ensure that the `AttributeValue` node contains the expected value for the
2951 attribute from ActiveDirectory. In the example screenshot above, you can see there is an
2952 `AttributeValue` node for the **company** attribute and the value is **Conway Inc**. This is correct,
2953 because in our Microsoft AD environment, the user account we tested with is **lsmith** (Lucy
2954 Smith), and Lucy's **company** attribute in Microsoft AD is set to a value of **Conway Inc**.

- 2955 When you complete this functional test, you must enable SAML encryption between the IdP and RP
2956 again. Follow the instructions in the section Temporarily Disable SAML Encryption for Testing and
2957 Troubleshooting Message Exchanges, subsection Enable SAML Encryption at the end of this section
2958 again to enable SAML encryption.

2959 **6.3.2 Configure PingFederate-IdP to Pull Environmental Attributes During**
2960 **Authentication**

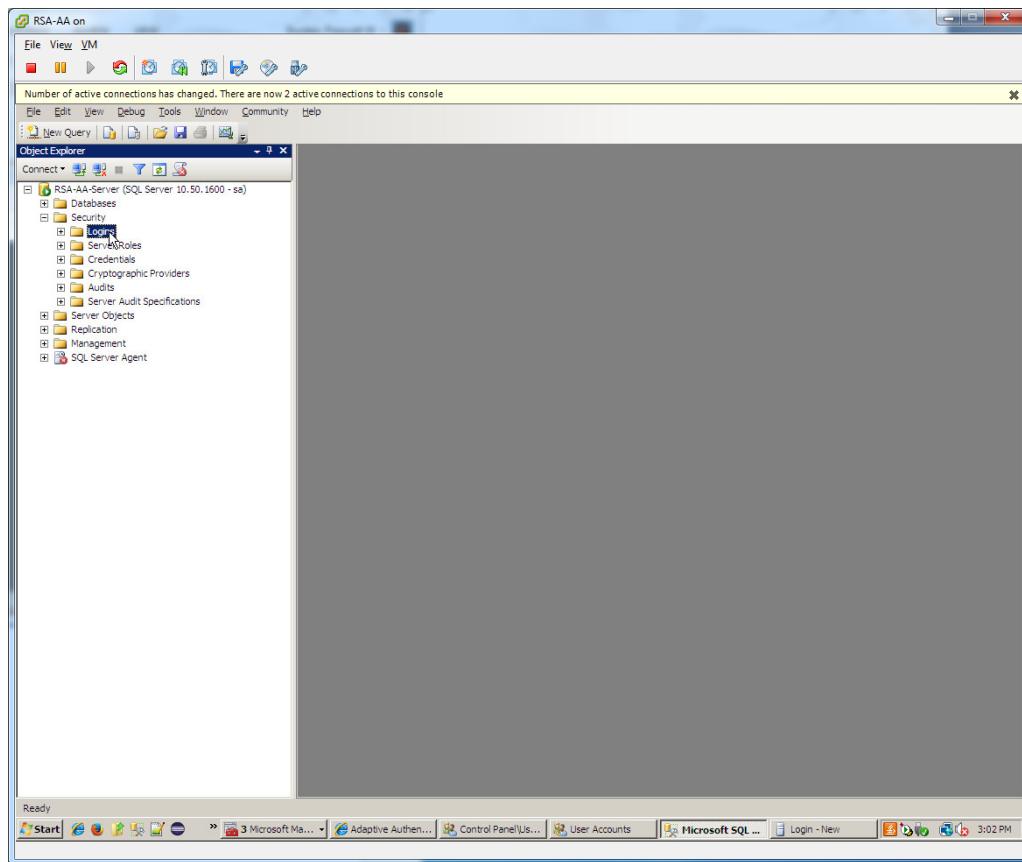
2961 Follow the instructions in this section to configure the PingFederate-IdP to get environmental attribute
2962 values from the RSA Adaptive Authentication system during the authentication process. The
2963 environmental attributes are passed along with the user attributes in the SAML messages that is sent to
2964 the RP. In the example below, the environmental attribute **ip_address** will be pulled from RSA Adaptive
2965 Authentication.

2966 RSA Adaptive Authentication stores environmental attributes about the user's web transactions in a SQL
2967 Server database named **RSA_CORE_AA**. The PingFederate-IdP will be configured to query to the
2968 **RSA_CORE_AA** database and get the value of **ip_address** from the **EVENT_LOG** table.

2969 Before you can configure the query for **ip_address**, you must first create an account for the
2970 PingFederate application in the **RSA_CORE_AA** database. Follow the instructions below to create the
2971 account in the SQL Server database.

2972 Log on to the server that hosts the RSA Adaptive Authentication SQL Server database engine.

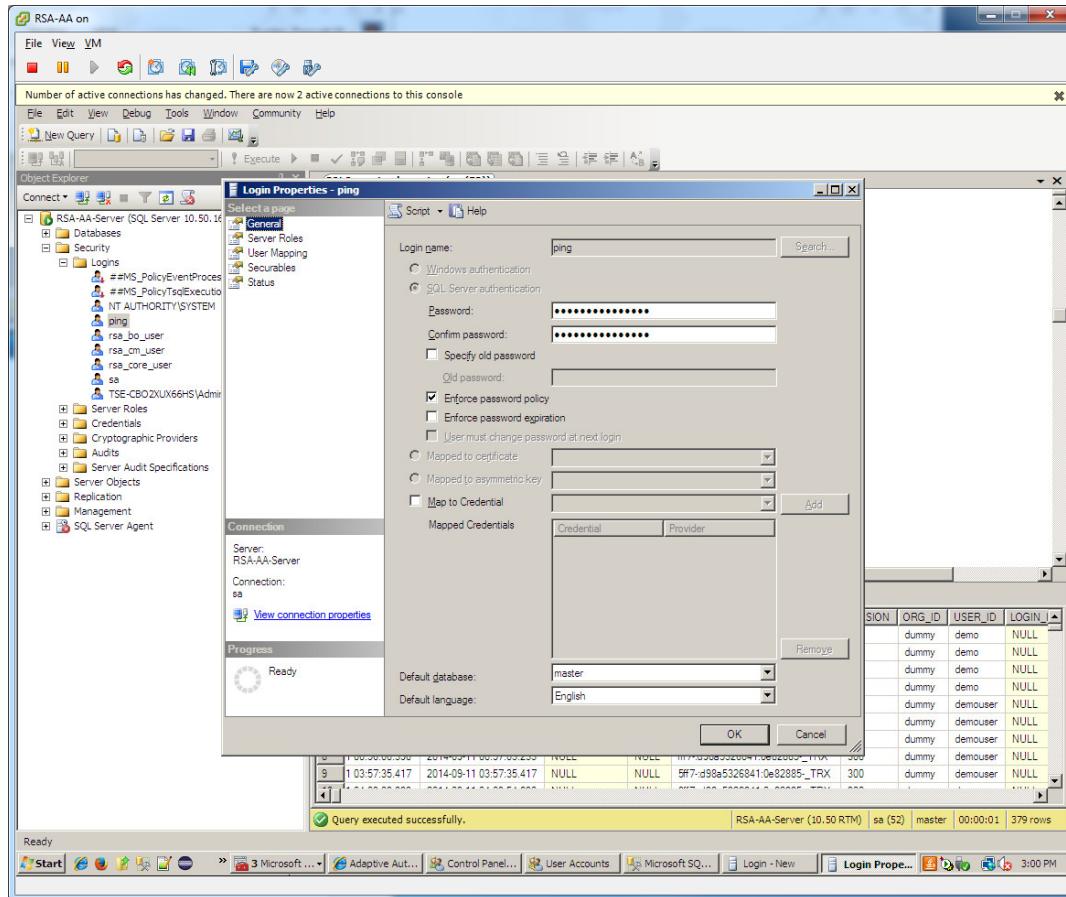
- 2973 1. Open SQL Server Management Studio.
2974 2. Expand the **RSA-AA-Server** folder, then the **Security** folder.
2975 3. Right-click on **Logins** and select **New Login**.



2976

SECOND DRAFT

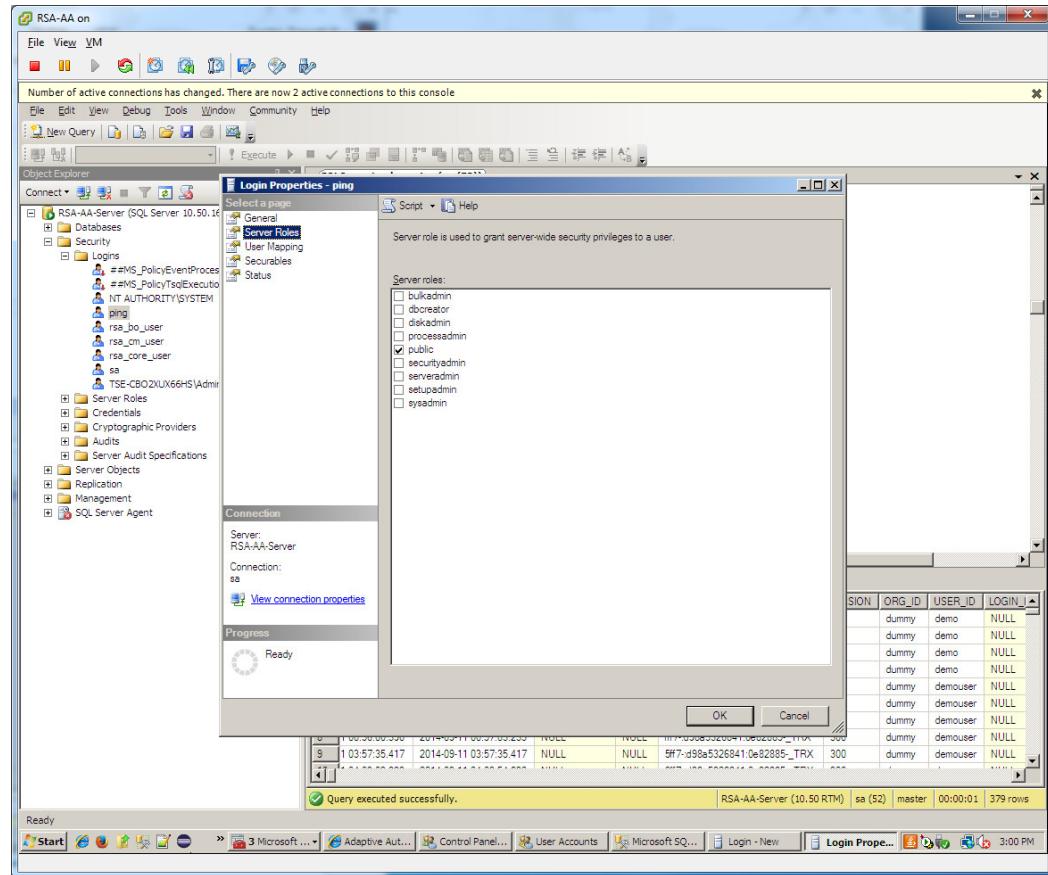
- 2977 4. Set the **Login name** (e.g., ping), under **SQL Server authentication** and choose a password that
2978 meets the Windows password policy.



2979

- 2980 5. Under **Server Roles**, select **public**.

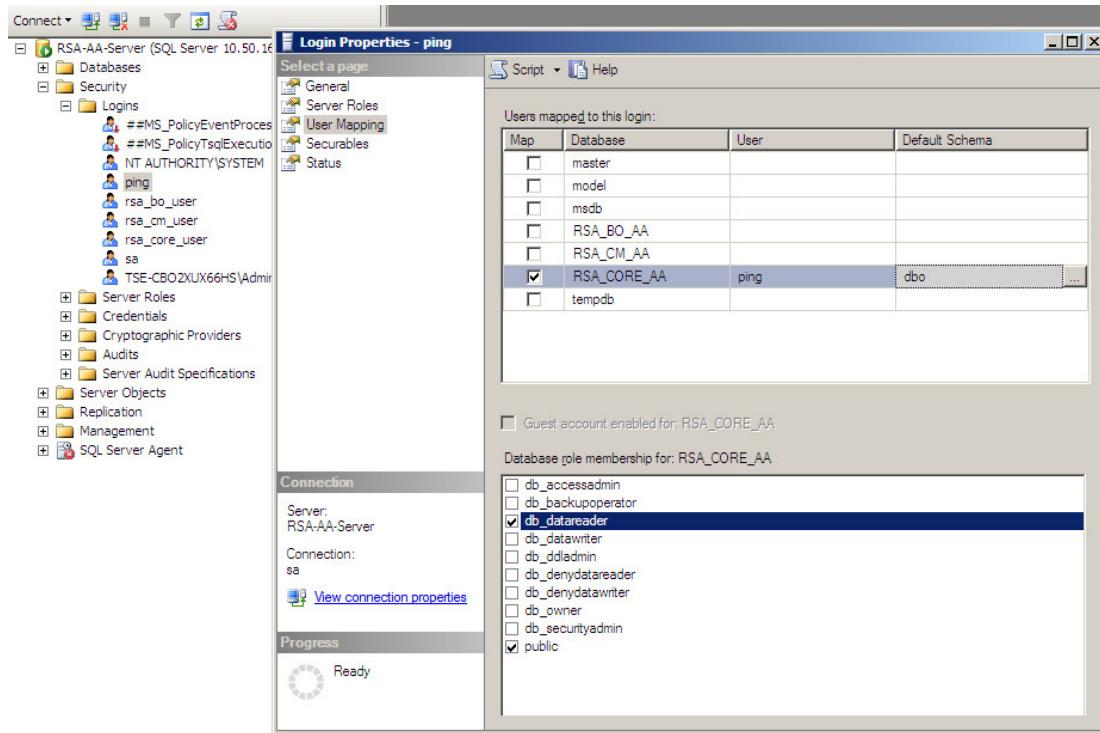
SECOND DRAFT



2981

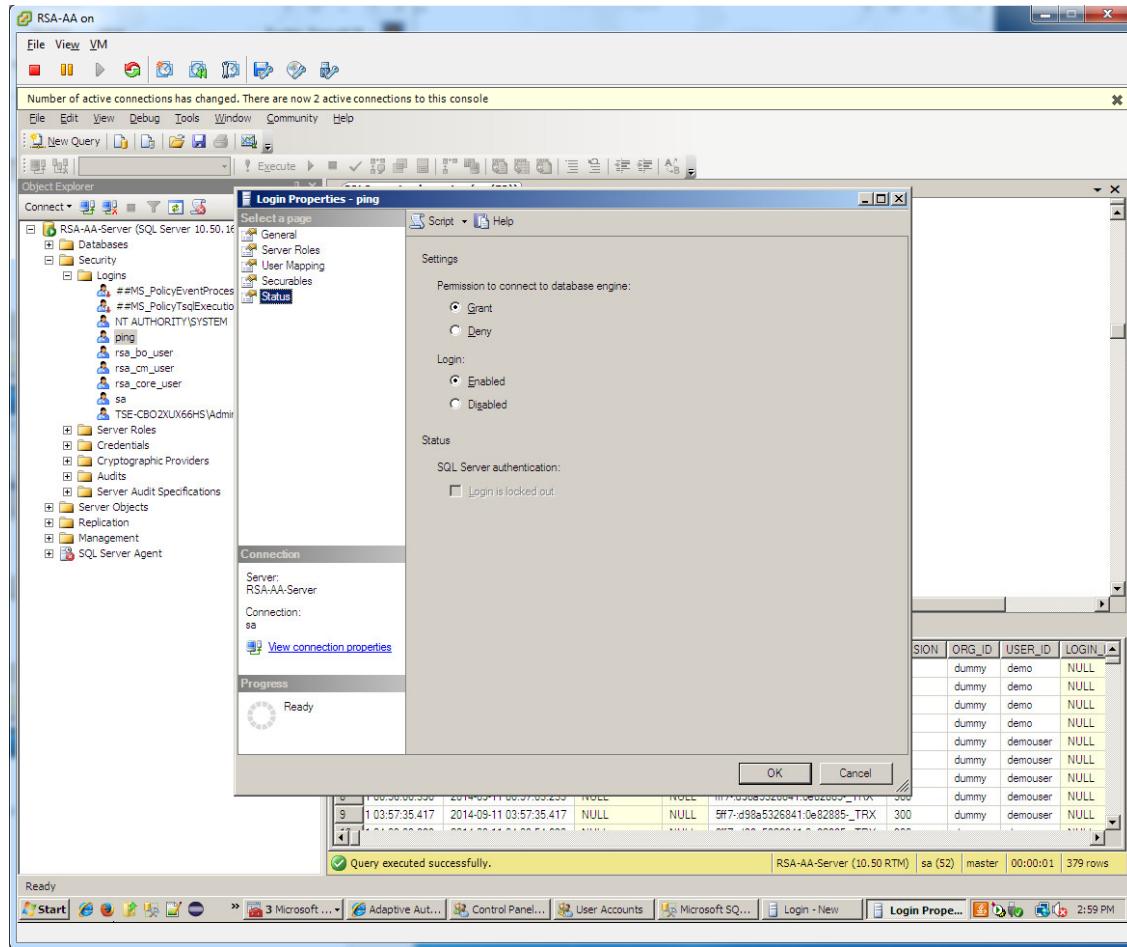
2982 Under User Mapping, check the Map box next to **RSA_CORE_AA**. In the bottom pane, under
2983 **Database role membership**, check the box next to **db_datareader**.

SECOND DRAFT



2984

- 2985 6. Under **Status**, set permission to connect to database engine to **Grant** and **Login to Enabled**. Click
2986 **OK**.



2987

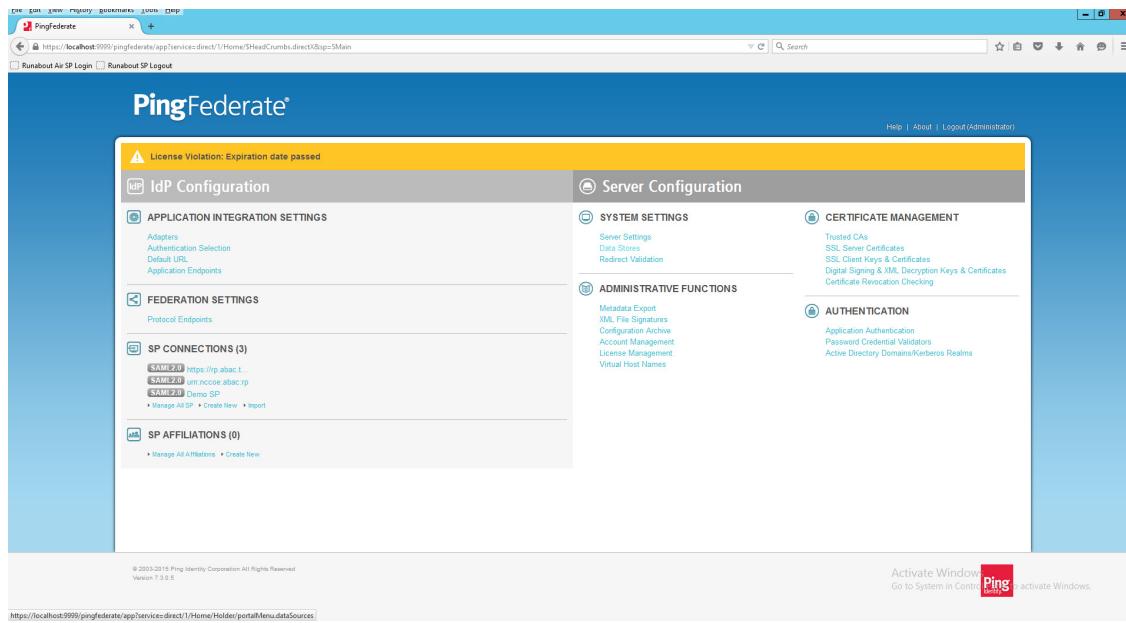
6.3.2.1 Configuring a New Data Store that Connects to the RSA database

2988 Next, you will configure a new Data Store that connects to the **RSA_CORE_AA** database on the Identity
 2989 Provider's PingFederate server. This new data store will be used in the RP Connection to query the
 2990 EVENT_LOG table during the authentication process.

2991 Follow the instructions below to create a new Data Store for the **RSA_CORE_AA** database.

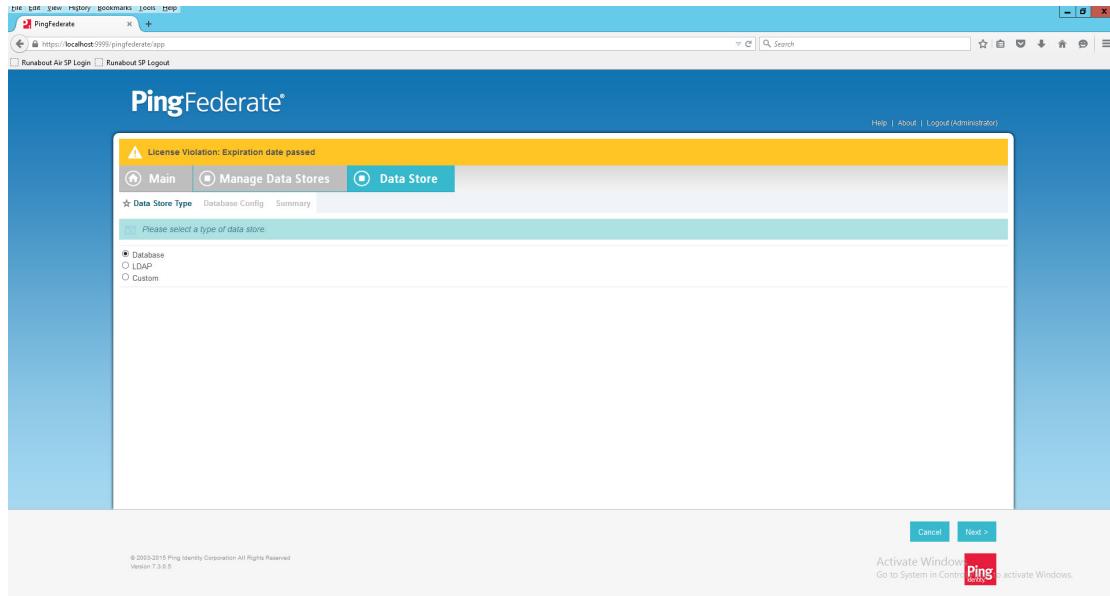
- 2992 1. Launch your browser and go to https://<DNS_NAME>:9999/pingfederate/app. Replace <DNS_NAME> with the fully qualified name of the IdP's PingFederate server (e.g., <https://idp.abac.test:9999/pingfederate/app>).
- 2993 2. Log on to the PingFederate application using the credentials you configured during installation.
- 2994 3. Under **Server configuration**, select **Data Stores**.

SECOND DRAFT



2998

- 2999 4. Under **Manage data stores**, select **Add new data store**. Select **Database** as type of data store.
3000 Click **Next**.



3001

- 3002 5. On the database config page, set the **JDBC URL** to:
3003 **jdbc:sqlserver://<RSA_SERVER_IP_ADDRESS>:1433;databaseName=rsa_core_aa**
3004 a. Replace <RSA_SERVER_IP_ADDRESS> with the IP address of the server that hosts the
3005 RSA_CORE_AA database.
3006 6. Set the driver class to **com.microsoft.sqlserver.jdbc.SQLServerDriver**
3007 7. In the **Username** and **Password** fields, enter the credentials for the Ping user created in the SQL
3008 server RSA Database.

SECOND DRAFT

- 3009 8. Under **Validate Connection SQL**, type **SELECT 1=1**.
- 3010 9. Check the box to allow multi-value attributes. Click **Next**.

The screenshot shows the 'Data Store' configuration page. At the top, there are tabs: Main, Manage Data Stores, and Data Store (which is selected). Below the tabs, there are sub-tabs: Data Store Type (selected), Database Config, and Summary.

The main content area has a message: "Please provide the details for configuring this database connection." It contains the following fields:

- JDBC URL: databaseName=RSA_CORE_AA *
- Driver Class: .sqlserver.jdbc.SQLServerDriver *
- Username: ping *
- Password: [REDACTED] ⓘ
- Validate Connection SQL: SELECT 1=1

Below these fields are two checkboxes:
☐ Mask Values in Log
☑ Allow Multi-Value Attributes

At the bottom right of the configuration section are buttons: Cancel, < Previous, and Next >.

- 3011
- 3012 10. Review the settings on the summary page. Then, click **Save**.

The screenshot shows the 'Summary' configuration page. At the top, there are tabs: Main, Manage Data Stores, and Data Store (selected). Below the tabs, there are sub-tabs: Data Store Type (selected), Database Config, and Summary.

The main content area has a message: "Click a heading link to edit a configuration setting." It displays the following configuration settings under the 'Data Store' heading:

DATA STORE TYPE	
Type of Data Store	Database

DATABASE CONFIG	
JDBC URL	jdbc:sqlserver://10.33.7.12:1433;databaseName=RSA_CORE_AA
Driver	com.microsoft.sqlserver.jdbc.SQLServerDriver
Username	ping
Validate Connection SQL	SELECT 1=1
Allow Multi-Value Attributes	true

At the bottom right of the configuration section are buttons: Cancel, < Previous, Done, and Save.

- 3013
- 3014 *6.3.2.2 Modifying the SP Connection to the RP to Add New Environmental Attribute*
- 3015 Next, you will modify the SP Connection to the RP and add a new environmental attribute, **ip_address**,
- 3016 from the RSA_CORE_AA database.
- 3017 1. Go to the PingFederate main menu. On the **Main** menu under **SP CONNECTION**, click **Manage All SP**.

SECOND DRAFT

SP Connections

Manage Connections

On this screen you can manage connections to your partner SPs. Use the drop-downs to filter the connection list. You can also override the logging mode for all SP connections by specifying a single, global logging mode.

Connection Name	Connection ID	Protocol	Status	Action
Demo SP	PF-DEMO	SAML2.0	Active	Delete Copy Export Connection Export Metadata
https://rp.abac.test:9031	https://rp.abac.test:9031	SAML2.0	Active	Delete Copy Export Connection Export Metadata
urn:nccoe:abac:rp	urn:nccoe:abac:rp	SAML2.0	Active	Delete Copy Export Connection Export Metadata

Create Connection... Import Connection Check All Connections For Errors

3019

3020

- Click on the link for the SP connection created in [Section 2](#) (e.g., <https://rp.abac.test:9031>).

SP Connection

Connection Type Connection Options General Info Browser SSO Credentials Activation & Summary

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status	<input checked="" type="radio"/> Active <input type="radio"/> Inactive
SSO Application Endpoint	https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=https://rp.abac.test:9031

SP Connection

CONNECTION TYPE

Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false

CONNECTION OPTIONS

Browser SSO	true
IdP Discovery	false
Attribute Query	false

GENERAL INFO

Partner's Entity ID (Connection ID)	https://rp.abac.test:9031
-------------------------------------	---------------------------

3021

- On the **Activation & Summary** screen, scroll down to the **Assertion Creation** group and click on the **ATTRIBUTE CONTRACT** link.

SECOND DRAFT

3024

3025 4. On the **Attribute Contract** screen, under the **EXTEND THE CONTRACT** column, enter the name of
3026 the environmental attribute to be pulled from the RSA_CORE_AA database (e.g., **ip_address**) in
3027 the empty text field.

3028 5. Click **Add**.

3029 6. Click **Next >**.

3030

The screenshot shows the 'Attribute Contract' screen with the 'Subject Name Format' tab selected. At the top, there are tabs for Main, SP Connection, Browser SSO, and Assertion Creation. Below the tabs, there is a sub-tab for Identity Mapping, followed by Attribute Contract, Authentication Source Mapping, and Summary. A note at the top says, 'An Attribute Contract is a set of user attributes that this server will send in the assertion.' The main area has sections for 'ATTRIBUTE CONTRACT' and 'SUBJECT NAME FORMAT'. Under 'ATTRIBUTE CONTRACT', there is a table with columns for 'EXTEND THE CONTRACT' (containing 'company' and 'ip_address') and 'ACTION' (containing 'Edit / Delete'). Under 'SUBJECT NAME FORMAT', there is a table with columns for 'SAML SUBJECT' (containing 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified') and 'ATTRIBUTE NAME FORMAT' (containing 'urn:oasis:names:tc:SAML:2.0:attrname-format:basic'). At the bottom right, there are buttons for Cancel, < Previous, Next >, Done, and Save.

- 3024
- 3025 4. On the **Attribute Contract** screen, under the **EXTEND THE CONTRACT** column, enter the name of
3026 the environmental attribute to be pulled from the RSA_CORE_AA database (e.g., **ip_address**) in
3027 the empty text field.
- 3028 5. Click **Add**.

3029 6. Click **Next >**.

3030

The screenshot shows the 'Attribute Contract' screen with the 'Subject Name Format' tab selected. At the top, there are tabs for Main, SP Connection, Browser SSO, and Assertion Creation. Below the tabs, there is a sub-tab for Identity Mapping, followed by Attribute Contract, Authentication Source Mapping, and Summary. A note at the top says, 'An Attribute Contract is a set of user attributes that this server will send in the assertion.' The main area has sections for 'ATTRIBUTE CONTRACT' and 'SUBJECT NAME FORMAT'. Under 'ATTRIBUTE CONTRACT', there is a table with columns for 'EXTEND THE CONTRACT' (containing 'company' and 'ip_address') and 'ACTION' (containing 'Edit / Delete'). Under 'SUBJECT NAME FORMAT', there is a table with columns for 'SAML SUBJECT' (containing 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified') and 'ATTRIBUTE NAME FORMAT' (containing 'urn:oasis:names:tc:SAML:2.0:attrname-format:basic'). At the bottom right, there are buttons for Cancel, < Previous, Next >, Done, and Save.

The screenshot shows the Assertion Creation interface. The top navigation bar has tabs for Main, SP Connection, Browser SSO, and Assertion Creation, with Assertion Creation selected. Below the tabs are sub-tabs: Identity Mapping, Attribute Contract, Authentication Source Mapping, and Summary, with Authentication Source Mapping selected. A note at the top says: "PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server." A table lists an adapter instance named "RSA Multifactor" under the columns Adapter Instance Name, Virtual Server IDs, and Action (Delete). At the bottom is a button labeled "Map New Adapter Instance...".

3031

- 3032 7. On the **Authentication Source Mapping** screen, click on the name of the **ADAPTER INSTANCE**
3033 (e.g., **RSA Multifactor**).

The screenshot shows the IdP Adapter Mapping interface. The top navigation bar has tabs for Main, SP Connection, Browser SSO, Assertion Creation, and IdP Adapter Mapping, with IdP Adapter Mapping selected. Below the tabs are sub-tabs: Adapter Instance, Assertion Mapping, Attribute Sources & User Lookup, Attribute Contract Fulfillment, Issuance Criteria, and Summary, with Attribute Contract Fulfillment selected. A note at the top says: "ip_address must be mapped to something." A table lists attribute contracts with their sources and values, and actions available:

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Adapter	username	None available
company	LDAP (Attrs from MS AD)	company	None available
ip_address	- SELECT -		None available

At the bottom are buttons for Cancel, < Previous, Next >, Done, and Save.

3034

- 3035 8. Click on the **Attribute Sources & User Lookup** tab.

The screenshot shows the 'Attribute Sources & User Lookup' tab selected in a navigation bar. Below it is a table with one row containing the following data:

DESCRIPTION	TYPE	ACTION
Atts from MS AD	LDAP	Delete

Below the table is a button labeled 'Add Attribute Source ...'. At the bottom right are five buttons: 'Cancel', '< Previous', 'Next >', 'Done', and 'Save'.

3036

- 3037 9. Click **Add Attribute Source**.
- 3038 10. On the **Attribute Sources & User Lookup** screen, enter a unique name in the **Attribute Source Id** field (e.g., **RSAEventLog**).
- 3039 11. Enter a description (e.g., **Atts from RSA**).
- 3040 12. For the **Active Data Store** field, select the existing Data Store that connects to the **RSA_CORE_AA** database.

The screenshot shows the 'Attribute Sources & User Lookup' tab selected. The configuration fields are as follows:

- Attribute Source Id:** RSAEventLog *
- Attribute Source Description:** Atts from RSA *
- Active Data Store:** jdbc:sqlserver://10.33.7.12:1433;databaseName=RSA_CORE_AA *
- Data Store Type:** JDBC

Below the fields is a button labeled 'Manage Data Stores...'. At the bottom right are two buttons: 'Cancel' and 'Next >'.

3043

- 3044 13. Click **Next**.
- 3045 14. On the **Database Table and Columns** screen, select the **dbo** Schema.
- 3046 15. Select the **EVENT_LOG** table.
- 3047 16. Under the **Columns to return from SELECT**, select the **IP_ADDRESS** column and click **Add Attribute**.

SECOND DRAFT

The screenshot shows the 'Attribute Sources & User Lookup' tab selected in a navigation bar. Below it, the 'Database Table and Columns' tab is active. A message box at the top says: 'Please select the table and columns you want to query. This information, along with the attributes supplied in the contract, will be used to fulfill the contract.' The 'Schema' dropdown is set to 'dbo'. The 'Table' dropdown is set to 'EVENT_LOG'. Under 'Columns to return from SELECT', there are two entries: 'IP_ADDRESS' and 'ACCEPT_LANGUAGE'. There is a 'Remove' link next to 'IP_ADDRESS' and an 'Add Attribute' button next to 'ACCEPT_LANGUAGE'. A 'Refresh' button is also present. At the bottom right are 'Cancel', '< Previous', and 'Next >' buttons.

3049

3050 17. Click **Next**.

3051 18. On the **Database Filter** screen, enter the text on the following line into the text field for the
3052 **Where**. Make sure to include the quotes.

3053 **EVENT_ID = '\${transactionid}'**

The screenshot shows the 'Database Filter' tab selected in a navigation bar. Below it, the 'Data Store' tab is active. A message box at the top says: 'Please supply a WHERE clause to filter the data from your table.' Under the 'Where' section, there is a text input field containing the value 'EVENT_ID = '\${transactionid}''. Below this, under 'Adapter Values', are listed '\${transactionid}' and '\${username}'. Under 'Previous Attribute Source Values', are listed '\${ds.ActiveDirectory.Subject DN}' and '\${ds.ActiveDirectory.company}'. At the bottom right are 'Cancel', '< Previous', and 'Next >' buttons.

3054

3055 19. Click **Next**.

SECOND DRAFT

SECOND DRAFT

Attribute Sources & User Lookup

Data Store Database Table and Columns Database Filter Summary

Attribute Source Summary

Attribute Sources & User Lookup

DATA STORE

Attribute Source	Atts from RSA
Attribute Source Id	RSAEventLog
Type of Data Store	JDBC
Data Store	jdbc:sqlserver://10.33.7.12:1433;databaseName=RSA_CORE_AA

DATABASE TABLE AND COLUMNS

Schema	dbo
Table	EVENT_LOG
Column	IP_ADDRESS

DATABASE FILTER

Filter	EVENT_ID = \${transactionId}
--------	------------------------------

Cancel < Previous Done Save

3056

3057

20. On the **Summary** screen, click **Done**.

Main SP Connection Browser SSO Assertion Creation

IdP Adapter Mapping

Adapter Instance Assertion Mapping Attribute Sources & User Lookup Attribute Contract Fulfillment Issuance Criteria Summary

Here you can specify a series of local data stores that will be used to supply additional information about the user in the SAML assertion to the SP.

DESCRIPTION	TYPE	ACTION
▼ Atts from MS AD	LDAP	Delete
▲ Atts from RSA	JDBC	Delete

Add Attribute Source...

Cancel < Previous Next > Done Save

3058

3059

21. On the **Attribute Sources & User Lookup** screen, click **Done**.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML SUBJECT	Adapter	username	None available
company	LDAP (Atts from MS AD)	company	None available
ip_address	- SELECT -		None available

Cancel < Previous Next > Done Save

3060

- 3061 22. On the **Attribute Contract Fulfillment** screen, for the **ip_address** attribute, select the **SOURCE**
 3062 and **VALUE**. For the **SOURCE**, select **JDBC (Atts from RSA)**. For **VALUE**, select **IP_ADDRESS**.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML SUBJECT	Adapter	username	None available
company	LDAP (Atts from MS AD)	company	None available
ip_address	JDBC (Atts from RSA)	IP_ADDRESS	None available

Cancel < Previous Next > Done Save

3063

- 3064 23. Click **Save** to complete the configuration.

3065 *6.3.2.3 Functional Test of Pulling Environmental Attributes during Authentication*

3066 To test that the Identity Provider's PingFederate server is successfully getting the environmental
 3067 attributes during the authentication process, follow the instructions in the section Functional Test of
 3068 Pulling User Attributes during Authentication. The only exception to those instructions is that when you
 3069 examine the SAML message, you need to look for the environmental attribute that is being pulled from
 3070 the RSA_CORE_AA database. See below for an example.

- 3071 1. Once you have the message open in the SAML tracer window, scroll down the message and
 3072 locate the **AttributeStatement** node and sub-nodes.

http Parameters SAML

```

</saml:Subject>
<saml:Conditions NotBefore="2015-07-30T20:09:53.495Z"
                  NotOnOrAfter="2015-07-30T20:19:53.495Z"
                >
  <saml:AudienceRestriction>
    <saml:Audience>https://rp.abac.test:9031</saml:Audience>
  </saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement SessionIndex="xgoiCeKQSAr5WzpM_tTuga.sZ1L"
                      AuthnInstant="2015-07-30T20:14:53.495Z"
                    >
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
  <saml:Attribute Name="company"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                >
    <saml:AttributeValue xsi:type="xs:string"
                        xmlns:xs="http://www.w3.org/2001/XMLSchema"
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                      >Conway Inc</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="ip_address"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                >
    <saml:AttributeValue xsi:type="xs:string"
                        xmlns:xs="http://www.w3.org/2001/XMLSchema"
                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                      >10.255.207.19</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>

```

3073

3074 **Expected Result:** Ensure that the attribute you configured to be pulled from the RSA_CORE_AA
 3075 database contains a node. In the example screenshot above, you can see that there is an
 3076 Attribute node for the **ip_address** attribute because of the line **<saml:Attribute**
 3077 **Name="ip_address"**.

3078 **Expected Result:** Ensure that the AttributeValue node contains the expected value for the
 3079 attribute from the RSA_CORE_AA database. In the example screenshot above, you can see that
 3080 there is an AttributeValue node for the **ip_address** attribute, and the value is **10.255.207.19**.

3081 6.3.3 Configure PingFederate-RP to Pull Attributes from the Identity Provider's 3082 SAML Exchange

3083 Once the PingFederate-IdP completes the authentication for a user, the IdP will send a SAML message to
 3084 the PingFederate-RP. That SAML message will contain attributes.

3085 Follow the instructions below to configure the PingFederate-RP to get attributes and their associated
 3086 values from the SAML message exchange with the IdP. In the example below, the attribute being
 3087 configured at the RP is the **company** attribute.

- 3088 1. Launch your browser and go to *https://<DNS_NAME>:9999/pingfederate/app*. Replace
 3089 DNS_NAME with the fully qualified name of the Relying Party's PingFederate server (e.g.,
 3090 *https://rp.abac.test:9999/pingfederate/app*). Log on to the PingFederate application using the
 3091 credentials you configured during installation.
- 3092 2. On the main menu, under **IDP CONNECTIONS**, click on the connection that was configured to
 3093 the IdP in [Section 3](#) (e.g., *https://idp.abac.test:9031*).

User-Session Creation	
IDENTITY MAPPING	
Enable Account Mapping	true
ATTRIBUTE CONTRACT	
Attribute	SAML_SUBJECT
Attribute	stafflevel
TARGET SESSION MAPPING	
Connection mapping contract name	Sharepoint 2013
CONNECTION MAPPING CONTRACT	
Selected contract	Sharepoint 2013
ATTRIBUTE RETRIEVAL	
Attribute location	Use only the attributes available in the SSO Assertion
CONTRACT FULFILLMENT	
subject	SAML_SUBJECT (Assertion)
stafflevel	stafflevel (Assertion)
ISSUANCE CRITERIA	
Criterion	(None)
Protocol Settings	
SSO SERVICE URLs	
Endpoint	URL: /idp/SSO.saml2 (POST)
Endpoint	URL: /idp/SSO.saml2 (Redirect)

3094

- 3095 3. On the **Activation & Summary** screen, scroll down to the **User-Session Creation** group and click
 3096 on the **ATTRIBUTE CONTRACT** link.

ATTRIBUTE CONTRACT		
EXTEND THE CONTRACT	MASK VALUES IN LOG	ACTION
<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add"/>

An Attribute Contract is a set of user attributes that the IdP will send in the assertion.

Buttons at the bottom: Cancel, < Previous, Next >, Done, Save.

3097

- 3098 4. On the **Attribute Contract** screen, under the **EXTEND THE CONTRACT** column, enter the name of
 3099 the attribute to be pulled from the IdP's message (e.g., **company**) in the empty text field. In the
 3100 **ACTION** column, click **Add**.

SECOND DRAFT

The screenshot shows the 'User-Session Creation' tab selected in a navigation bar. Below it, the 'Attribute Contract' section is active. A note says: 'An Attribute Contract is a set of user attributes that the IdP will send in the assertion.' Under 'ATTRIBUTE CONTRACT', there's a table with columns 'EXTEND THE CONTRACT', 'MASK VALUES IN LOG', and 'ACTION'. It contains one row for 'company' with an 'Edit / Delete' link and an 'Add' button. At the bottom are 'Cancel', '< Previous', 'Next >', 'Done', and 'Save' buttons.

3101

3102

- Click Done.

The screenshot shows the 'User-Session Configuration' screen. It lists four items: 'Identity Mapping' (Not Configured), 'Attribute Contract' (SAML_SUBJECT, company), 'Adapter Instances' (0), and 'Connection Contract Mappings' (1). Below this is a 'Configure User-Session Creation' button and a set of navigation buttons: 'Cancel', '< Previous', 'Next >', 'Done', and 'Save'.

3103

3104

- On the **User-Session Creation** screen, click **Configure User-Session Creation**.

The screenshot shows the 'User-Session Creation' configuration page. It includes sections for 'IDENTITY MAPPING' (Enable Account Mapping: true), 'ATTRIBUTE CONTRACT' (Attribute: SAML_SUBJECT, Attribute: company), 'TARGET SESSION MAPPING' (Connection mapping contract name: Sharepoint 2013), 'CONNECTION MAPPING CONTRACT' (Selected contract: Sharepoint 2013), and 'ATTRIBUTE RETRIEVAL' (Attribute location: Use only the attributes available in the SSO Assertion). At the bottom are 'Cancel', '< Previous', 'Next >', 'Done', and 'Save' buttons.

3105

3106
3107

- On the **Summary** page, under **User-Session Creation**, click on the **CONNECTION MAPPING CONTRACT** link.

SECOND DRAFT

The screenshot shows a software interface for managing connection contracts. At the top, there are tabs: Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping (which is selected), Connection Mapping Contract, Attribute Retrieval, Contract Fulfillment, Issuance Criteria, and Summary. Below the tabs, a message says "The list of attributes below, is required for the selected contract." Under "CONNECTION MAPPING CONTRACT", it shows "Sharepoint 2013". In the "CONTRACT ATTRIBUTES" section, there is a "subject" field. At the bottom right are buttons for Cancel, Next >, Done, and Save.

3108

- 3109 8. On the **Connection Mapping Contract** screen, make note of the **CONNECTION MAPPING CONTRACT** being used, because you will need to modify it by adding new attributes. In the example screenshots, the contract name is **SharePoint 2013**.
- 3110
- 3111
- 3112 9. Click on **Manage Connection Mapping Contracts**.

The screenshot shows a list of connection contracts. At the top, there are tabs: Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping, and Manage Connection Mapping Contracts (which is selected). Below the tabs, a message says "Manage Contracts". A table lists contracts with columns: CONTRACT NAME, CONTRACT ID, and ACTION. The table contains three rows: "SharePoint" (Contract ID: 2TSYliBHRp5iqs2t, Action: Delete), "Sharepoint 2013" (Contract ID: pHDPDzxOTReXnFp, Action: Delete (Check Usage)), and "Ted" (Contract ID: t59CO6fJWH6sZ8xW, Action: Delete). At the bottom left is a "Create New Contract..." button, and at the bottom right are buttons for Cancel and Save.

3113

- 3114 10. On the **Manage Contracts** screen, click on the name of the contract that is being used for the current configuration (e.g., **SharePoint 2013**).
- 3115

SECOND DRAFT

The screenshot shows a navigation bar with five items: Main, IdP Connection, Browser SSO, User-Session Creation, Connection Contract Mapping, Manage Connection Mapping Contracts, Connection Mapping Contract (which is selected and highlighted in blue). Below the navigation bar, there are three tabs: Contract Info (selected), Contract Attributes, and Summary. A status message at the top says "Connection mapping contract summary information." The main content area is titled "Connection Mapping Contract" and contains two sections: "CONTRACT INFO" (Contract Name: Sharepoint 2013) and "CONTRACT ATTRIBUTES" (Attribute: SAML_SUBJECT). At the bottom right are buttons for Cancel, < Previous, and Done.

3116

- 3117 11. On the **Summary** screen, click on the **Contract Attributes** link.
- 3118 12. On the **Contract attributes** screen, under the **EXTEND THE CONTRACT** column, enter the name
3119 of the attribute to be shared with the PingFederate service provider connection (e.g., **company**).
- 3120 13. In the **ACTION** column, click **Add**.

The screenshot shows a navigation bar with the same items as the previous screenshot. Below the navigation bar, there are three tabs: Contract Info, Contract Attributes (selected and highlighted in blue), and Summary. A status message at the top says "Define the set of attributes that the IdP connection will send to the SP connection." The main content area is titled "ATTRIBUTE CONTRACT" and shows a table with one row: "SAML_SUBJECT". Under "EXTEND THE CONTRACT", it says "company". Under "ACTION", there is a "Edit / Delete" link and an "Add" button. At the bottom right are buttons for Cancel, < Previous, Next >, and Done.

3121

- 3122 14. Click **Done**.
 - 3123 15. On the **Manage Contracts** screen, click **Save**.
- 3124 On the **Connection Mapping Contract** screen, you should see the new attribute (e.g., **company**)
3125 listed on the page.

SECOND DRAFT

The screenshot shows the 'Connection Contract Mapping' interface. At the top, there are four tabs: Main, IdP Connection, Browser SSO, and User-Session Creation. Below them, another set of tabs includes Connection Mapping Contract (which is highlighted in blue), Attribute Retrieval, Contract Fulfillment, Issuance Criteria, and Summary. A note below the tabs states: 'The list of attributes below, is required for the selected contract.' Under 'CONNECTION MAPPING CONTRACT', it says 'Sharepoint 2013'. In the 'CONTRACT ATTRIBUTES' section, there are two entries: 'company' and 'subject'. At the bottom, there is a 'Manage Connection Mapping Contracts...' button and a row of buttons: Cancel, Next >, Done, and Save.

3126

- 3127 16. Click on the **Contract Fulfillment** tab.

The screenshot shows the 'Connection Contract Mapping' interface with the 'Contract Fulfillment' tab selected. The tabs at the top are Main, IdP Connection, Browser SSO, and User-Session Creation. Below them, the tabs are Connection Mapping Contract, Attribute Retrieval, Contract Fulfillment (which is highlighted in blue), Issuance Criteria, and Summary. A note below the tabs states: 'You can fulfill your Connection Mapping Contract with values from the assertion, dynamic text, expressions, or from a data-store lookup.' The 'CONNECTION MAPPING CONTRACT' section contains two rows: 'company' with a dropdown menu showing '- SELECT -' and 'subject' with dropdown menus showing 'Assertion' and 'SAML_SUBJECT'. At the bottom, there is a row of buttons: Cancel, < Previous, Next >, Done, and Save.

3128

- 3129 17. On the **Contract Fulfillment** screen, for the new attribute (e.g., **company**), select **Assertion** for the **SOURCE** field and select **company** for the **VALUE** field.
3130

The screenshot shows the 'Connection Contract Mapping' interface with the 'Contract Fulfillment' tab selected. The tabs at the top are Main, IdP Connection, Browser SSO, and User-Session Creation. Below them, the tabs are Connection Mapping Contract, Attribute Retrieval, Contract Fulfillment (which is highlighted in blue), Issuance Criteria, and Summary. A note below the tabs states: 'You can fulfill your Connection Mapping Contract with values from the assertion, dynamic text, expressions, or from a data-store lookup.' The 'CONNECTION MAPPING CONTRACT' section contains two rows: 'company' with 'Assertion' selected in the SOURCE dropdown and 'company' selected in the VALUE dropdown, and 'subject' with 'Assertion' selected in the SOURCE dropdown and 'SAML_SUBJECT' selected in the VALUE dropdown. At the bottom, there is a row of buttons: Cancel, < Previous, Next >, Done, and Save.

3131

- 3132 18. Click **Save** to complete the configuration.

3133 6.4 Configure PingFederate-RP and SharePoint to Pass and Read 3134 Attributes

3135 6.4.1 Configure PingFederate-RP to Pass Attributes to SharePoint

3136 Once the PingFederate-IdP completes the authentication for a user, the IdP will send a SAML message to
3137 the PingFederate-RP. That SAML message will contain attributes. The PingFederate-RP will then take the
3138 attributes and send them to SharePoint via WS-Federation.

3139 Follow the instructions below to configure the PingFederate-RP to pass attributes and their associated
3140 values from the IdP to SharePoint. In the example below, the attribute being configured to be passed to
3141 SharePoint is the **company** attribute.

- 3142 1. Launch your browser and go to https://<DNS_NAME>:9999/pingfederate/app. Replace
3143 DNS_NAME with the fully qualified name of the RP's PingFederate server (e.g.,
3144 <https://rp.abac.test:9999/pingfederate/app>).
- 3145 2. Log on to the PingFederate application using the credentials you configured during installation.
- 3146 3. On the **Main** menu under **SP CONNECTION**, click **Manage All SP**.
- 3147 4. Click on the link for the WS-Federation connection to the SharePoint instance created in
3148 [Section 3](#) (e.g., **SharePoint**).
- 3149 5. On the **Activation & Summary** screen, scroll down to the Assertion Creation group.

Assertion Creation	
IDENTITY MAPPING	
Name Identifier	User Principal Name
ATTRIBUTE CONTRACT	
Attribute	SAML_SUBJECT
Attribute	upn
Attribute Name Format	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
AUTHENTICATION SOURCE MAPPING	
Connection mapping contract name	Sharepoint 2013
CONNECTION MAPPING CONTRACT	
Selected contract	Sharepoint 2013
ASSERTION MAPPING	
Connection Mapping Contract	Sharepoint 2013
Data Store or Assertion	Use only the Connection Mapping Contract values in the SAML assertion
ATTRIBUTE CONTRACT FULFILLMENT	
upn	subject (Connection Mapping Contract)
SAML_SUBJECT	subject (Connection Mapping Contract)
ISSUANCE CRITERIA	
Criterion	(None)
Protocol Settings	
SERVICE URL	
Endpoint URL	/_trust/

- 3150 6. Click on the **ATTRIBUTE CONTRACT** link. On the Attribute Contract screen, under the EXTEND
3151 THE CONTRACT column, enter the name of the attribute (e.g., "company") to be passed from

SECOND DRAFT

3153 the PingFederate-RP to SharePoint in the empty text field. For the ATTRIBUTE NAME FORMAT,
3154 select the schemas.xmlsoap.org 2005 identity claims format.

An Attribute Contract is a set of user attributes that this server will send in the assertion.

EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Edit / Delete
company	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Add

Cancel < Previous Next > Done Save

3155

3156 7. Click Add.

An Attribute Contract is a set of user attributes that this server will send in the assertion.

EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
company	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Edit / Delete
upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Edit / Delete
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Add

Cancel < Previous Next > Done Save

3157

3158 8. Click Done.

PingFederate uses IdP adapters or partner IdPs to authenticate users to your SP. Users may be authenticated by one of several different adapters or connection mapping contracts, so map an adapter instance for each IDM system or a connection mapping contract for partner IdPs.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		Delete

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		Delete

[Map New Adapter Instance...](#) [Map New Connection Contract Mapping...](#)

[Cancel](#) [< Previous](#) [Next >](#) [Done](#) [Save](#)

3159

- 3160 9. On the Authentication Source Mapping screen, under the CONNECTION MAPPING CONTRACT NAME heading, click on the name of the connection mapping contract (e.g., SharePoint 2013) between this PingFederate SP connection and the PingFederate IdP connection that was configured in the earlier section, Configure Relying Party to Pull Attributes from the Identity Provider's SAML Exchange.

⚠ company must be mapped to something.

Fulfill your Attribute Contract with values from the connection mapping contract or with dynamic text values.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Connection Mapping Contract	subject	None available
company	- SELECT -		None available
upn	Connection Mapping Contract	subject	None available

[Cancel](#) [< Previous](#) [Next >](#) [Done](#) [Save](#)

3165

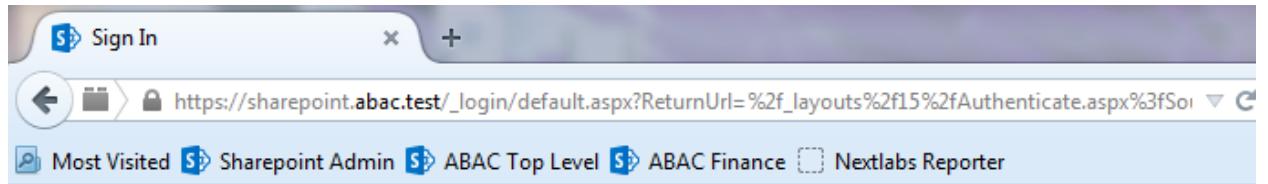
- 3166 10. On the Attribute Contract Fulfillment screen, for the “company” attribute, select **Connection Mapping Contract** for the SOURCE field. Select **company** for the VALUE field.
- 3167

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Connection Mapping Contract	subject	None available
company	Connection Mapping Contract	company	None available
upn	Connection Mapping Contract	subject	None available

Cancel < Previous Next > Done Save

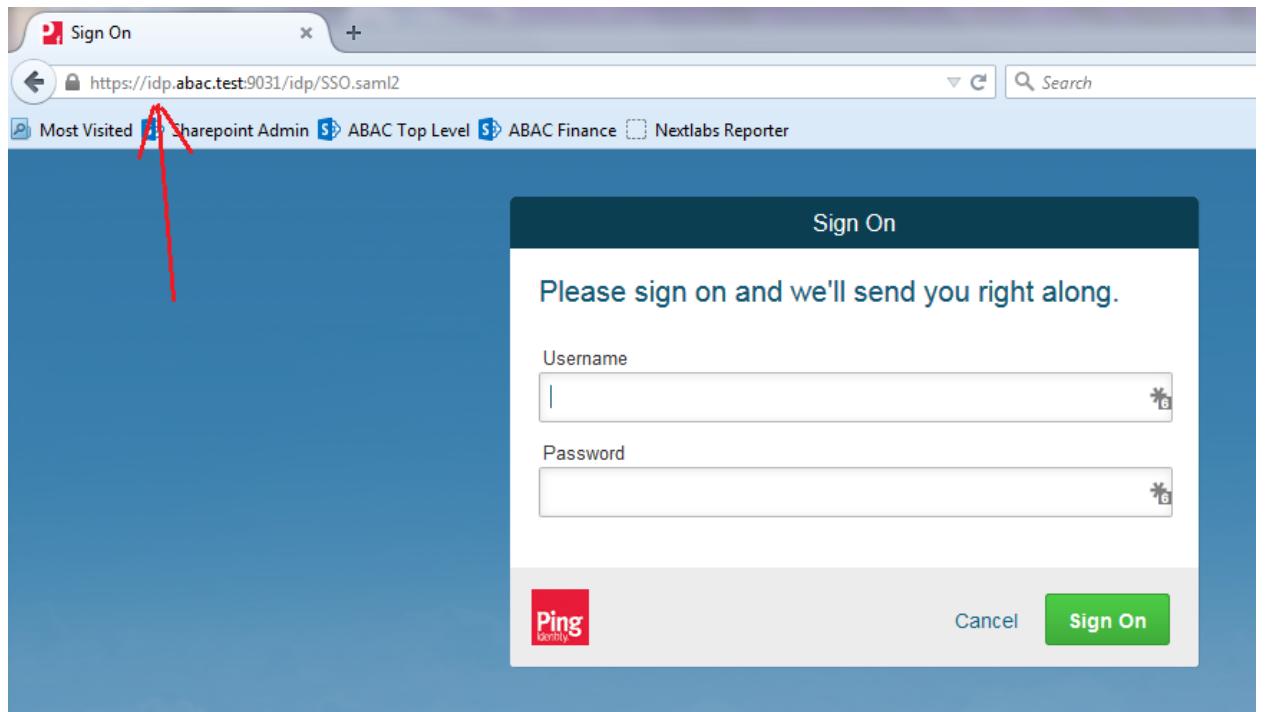
3168

3169 11. Click **Save** to complete the configuration.3170 **6.4.1.1 Functional Test of PingFederate-RP Passing Attributes to SharePoint**3171 The instructions in this section will help you perform a test to ensure that the PingFederate-RP is
3172 sending the correct attributes to SharePoint. The Firefox SAML tracer add-on is used to examine the
3173 SAML message.3174 1. Launch your Firefox browser and select **SAML tracer** from the Tools menu.3175 This will launch an empty SAML tracer window. Minimize the SAML tracer window. The SAML
3176 tracer will automatically record the details of the HTTPS messages in the background.3177 2. Go back to the main browser window and go to the RP's SharePoint site (e.g.,
3178 <https://SharePoint.abac.test>).



3179

- 3180 3. Select the option to use the federated logon (e.g., Federated Logon from Identity Provider).
3181 Your browser should be redirected to the PingFederate-IdP, and you should see the
3182 PingFederate Sign On screen.



3183

- 3184 4. Enter the Username and Password of the Microsoft AD account created earlier in this guide
3185 (e.g., lsmith). Note: If CISCO ISE has already been set up and 802.1x authentication has already
3186 occurred, this login is not necessary.

The screenshot shows a 'Sign On' page from Ping Identity. The top bar is dark blue with the word 'Sign On' in white. Below it, a message reads 'Please sign on and we'll send you right along.' There are two input fields: 'Username' with the value 'lsmith' and 'Password' with a masked value consisting of several blue dots. In the bottom left corner, there is a red square containing the 'Ping Identity' logo. On the right side, there are two buttons: 'Cancel' in blue and 'Sign On' in green. The entire form is set against a light gray background.

- 3187
- 3188 5. Click **Sign On**. On the RSA Adaptive Authentication screen, enter the SMS validation code
3189 received on your mobile phone. Click **Continue**.
- 3190 Once authenticated at the IdP, your browser should automatically redirect to the PingFederate-
3191 RP (e.g., *rp.abac.test*) and then to the RP's SharePoint (*SharePoint.abac.test*) site.
- 3192 6. Go back to the SAML tracer window. Scroll down the list of messages and click on the **POST**
3193 message to *SharePoint_trust* URL to bring up the details of the message in the bottom pane.

SAML tracer

Clear Autoscroll Filter resources

```

POST https://lastpass.com/error.php
POST https://idp.abac.test:9031/idp/8aLSw/resumeSAML20/idp/SSO.ping
POST https://rp.abac.test:9031/sp/ACS.saml2
POST https://sharepoint.abac.test/_trust/
GET https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
GET https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F

```

http Parameters

```

POST https://sharepoint.abac.test/_trust/ HTTP/1.1
Host: sharepoint.abac.test
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://rp.abac.test:9031/sp/ACS.saml2
Cookie: Ribbon.Read=1201680|-1|0|-10712485; Ribbon.WebApp=1197680|-1|378|-10712485; WSS_FullScreenMode=false
Content-Type: application/x-www-form-urlencoded
Content-Length: 4716

HTTP/1.1 302 Found
Location: https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
Server: Microsoft-IIS/8.5
Set-Cookie:
FedAuth=77u/PD94bWwgdmVyc2lvbj0iMS4wIiB1bmNvZGluZz0idXRmLTgiPz48U1A+MGUudHxmZWR1cmF0ZWQgbG9nb24gZnJvbSBpZGVudG10Rlcnxsc21pdGgsMTMwOD15MjQxODQ2NTg4MzEwLEZhbnL1F1FTGiURONXREVvbXV6ZUdLMnBrCfdWbGFtZTh6eVkrcmhHWGx3Skw5cTVX511PSUcWluYXBHNWgyTnJmb1JqSXdnMTMhTdFp4a3V1205BeEFmUG83azhXWHhtc2J1Y3RWSm1qdFNad3hGQ1RnVFRCLzNEeG56QjdhNmNYVFNibOVoMTNh10Q1pMeTI4Q0hDbU3k5WndqNFppSmtWeThLb0syVnJEbExrU0ZPQkFjY3paZzFjcgSvWws4NVJrVkJTenVJOWJuN3cxakdwU2djchBZU
secure: HttpOnly
SPRequestGuid: 302c1e9d-86ce-e01d-6291-300c85f414f3
request-id: 302c1e9d-86ce-e01d-6291-300c85f414f3

```

3194

3195

7. Click on the **Parameters** tab for the bottom pane.

POST https://sharepoint.abac.test/_trust/
GET https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
GET https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F

http Parameters

```

POST
wa:wsignin1.0
wst:RequestSecurityTokenResponse xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken>
<saml:Assertion:MajorVersion="1"><MinorVersion="1"><SubjectID="#27ql60V17N_XX8QlKdflG1CM"><IssuedInstant>2015-07-27T17:36:21.439Z</IssuedInstant>
<saml:Subject><saml:Audience>urn:sharepoint_abac_test</saml:Audience></saml:Subject><saml:AttributeStatement><saml:Condition>
<saml:Audience>urn:sharepoint_abac_test</saml:Audience></saml:Condition></saml:AttributeStatement><saml:AttributeStatement><saml:NameIdentifier>urn:uuid:12345678-1234-1234-1234-123456789012</saml:NameIdentifier>
<saml:NameIdentifierFormat>http://schemas.xmlsoap.org/claims/UPN</saml:NameIdentifierFormat><saml:Subject><saml:Attribute><saml:AttributeName>urn:</saml:AttributeName><saml:AttributeValue>Company</saml:AttributeValue></saml:Attribute><saml:Attribute><saml:AttributeName>http://schemas.xmlsoap.org/ws/2005/05/identity/claims</saml:AttributeName><saml:AttributeValue>ConwayIn</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><ds:Signature><ds:KeyInfo><ds:X509Certificate>MIIEvQIBAAKCAQDw0u...</ds:X509Certificate></ds:KeyInfo></ds:Signature><ds:SignedInfo><ds:CanonicalizationMethodAlgorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<ds:SignatureMethodAlgorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
<ds:Reference URI="#n27ql60V17N_XX8QlKdflG1CM"><ds:Transforms>
<ds:TransformAlgorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:TransformAlgorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
</ds:Transforms>
<ds:DigestMethodAlgorithm="http://www.w3.org/2001/04/xmldsig#sha256"/>
<ds:DigestValue>K/L27oIUkwY3xiQbfqVb3oqJUpArD05a9W/zf7WA5k</ds:DigestValue>
</ds:Reference>
</ds:Signature>
<ds:SignatureValue>
nGQUnnM/DiuEan+P0LWj3SD7kup7kOb+4DELu2GNwmYeRe0hesYSe5g2GM4Hpw1HbP9LYElowbrF/kDjf6V1KeKL4CovzzRz3h1YhKptohkuo5UAkTRf+d7jyDF8jtwehYU6VpmJtxs0Wv3e8VV14

```

3196

3197
3198

8. Copy all of the content (beginning with the POST line) in the bottom page and paste it into a text editor such as Notepad. Turn on Word Wrap to make it easier to see all of the XML content.

SECOND DRAFT

```
Untitled - Notepad
File Edit Format View Help

POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionID="nZ7qL6oV17N_XX8QLxKdfLG1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp.abac.test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:conditions+NotBefore="2015-
07-31:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint.abac.test</saml:Audience></saml:AudienceRestrictionCondition></saml:Conditions><saml:AuthenticationStatement+AuthenticationInstant="2015-07-
27T17:36:21.424Z"><AuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:AttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="urn:Identity&gt;<saml:AttributeValue>lsmith</saml:AttributeValue></saml:Attribute
+AttributeName="company"><saml:AttributeValue>Conway</saml:AttributeValue></saml:AttributeStatement><ds:Signature+xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
+Inc</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><ds:Signature+xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod+Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference+URI="#nZ7qL6oV17N_XX8QLxKdfLG1CM">
<ds:Transforms>
<ds:Transform+Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod+Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
<ds:DigestValue>K/L27oIUIkwY3xiQbfvb3oqJLpArD05A9w/zf7wA5k=</ds:DigestValue>
```

3199

- 3200 9. Scroll down the SAML message and locate the AttributeStatement node and sub-nodes.

```
Untitled - Notepad
File Edit Format View Help

POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionID="nZ7qL6oV17N_XX8QLxKdfLG1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp.abac.test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:conditions+NotBefore="2015-
07-27T17:31:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint.abac.test</saml:Audience></saml:AudienceRestrictionCondition></saml:Conditions><saml:AuthenticationStatement+AuthenticationInstant="2015-07-
27T17:36:21.424Z"><AuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:AttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="urn:Identity"><saml:AttributeValue>lsmith</saml:AttributeValue></saml:Attribute
+AttributeName="company"><saml:AttributeValue>Conway</saml:AttributeValue></saml:AttributeStatement><ds:Signature+xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
+Inc</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><ds:Signature+xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod+Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference+URI="#nZ7qL6oV17N_XX8QLxKdfLG1CM">
```

3201

- 3202 10. For the AttributeStatement node and sub-nodes, enter some carriage returns before each XML
3203 tag to make it easier to examine the data. The goal is to be able to easily examine the Attribute
3204 nodes within the AttributeStatement node.

Untitled - Notepad

File Edit Format View Help

```

POST
wa: wsse:signin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionID="nz7qL6ovl7N_XX8QLxKdfLG1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp:abac.test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:Conditions+NotBe
07-27T17:31:21.439Z">+NotOnOrAfter="2015-07-
27T17:41:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint.abac.test</saml:Audience></saml:Audie
ctionCondition></saml:Conditions><saml:AuthenticationStatement+AuthenticationInstant="2015-07-
27T17:36:21.424Z">+AuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"><saml:Subject><saml:NameI
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationState
<saml:AttributeStatement>
<saml:Subject>
<saml:NameIdentifier+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject>
<saml:Attribute AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
<saml:AttributeValue>lsmith</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute+AttributeName="company"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
<saml:AttributeValue>Conway+Inc</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>

```

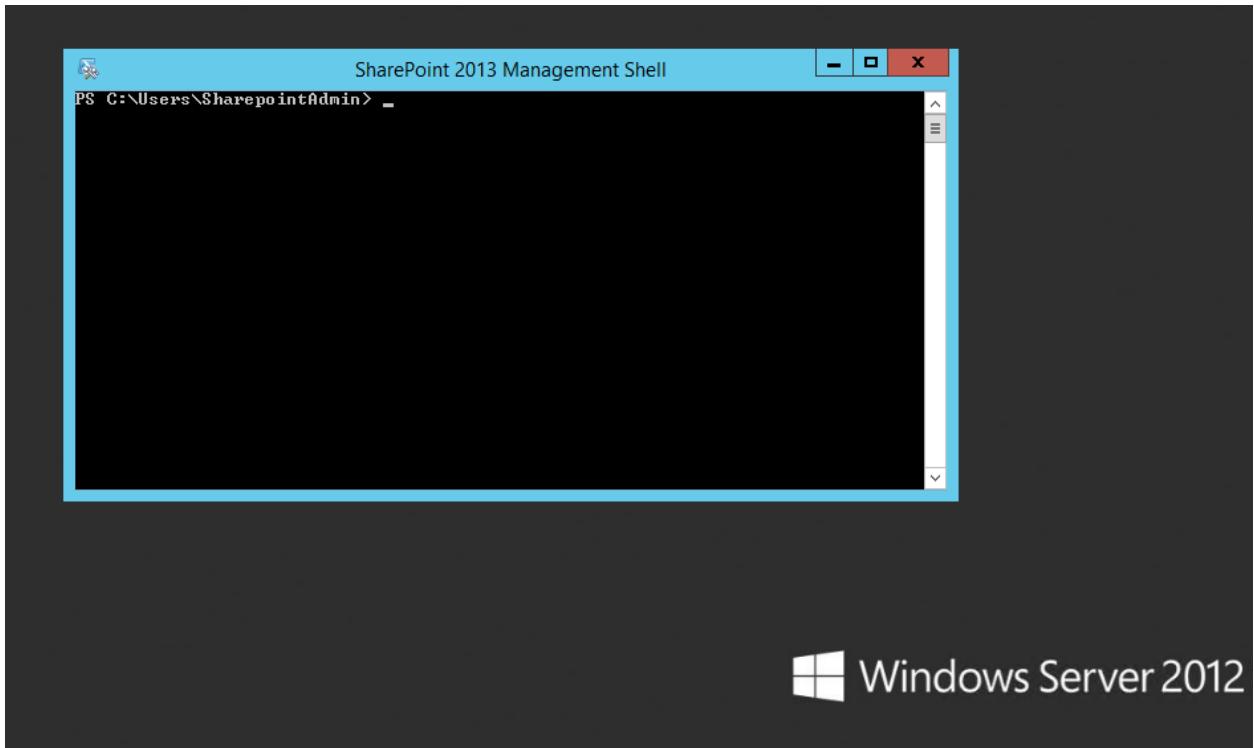
3205

3206 Expected Result: Within the AttributeStatement node, there should be multiple Attribute sub-nodes. There should be an Attribute sub-node that has an AttributeName value of “company.”
 3207 The AttributeNamespace value should be
 3208 *http://schemas.xmlsoap.org/ws/2005/05/identity/claims*. There should be an AttributeValue
 3209 sub-node, which should contain the expected value (e.g., Conway Inc) for the “company”
 3210 attribute that was pulled from Microsoft AD (e.g., <saml:AttributeValue> Conway+Inc
 3211 </saml:AttributeValue>) for the specific user (e.g., lsmith) who authenticated at the Sign On
 3212 screen.

3214 6.4.2 Configure SharePoint to Read Custom Attributes from PingFederate-RP

3215 The PingFederate-RP will send attributes to SharePoint via WS-Federation. Follow the instructions below
 3216 to configure SharePoint to read the attributes and load them into the web session. In the example
 3217 below, the attribute being configured to be read by SharePoint is the “company” attribute.

- 3218 1. Using SharePoint administrator credentials, log on to the server that hosts SharePoint for the
 3219 Relying Party.
- 3220 2. Click on the Start menu and navigate to SharePoint 2013 Products group. Open SharePoint 2013
 3221 Management Shell.



3222

- 3223 3. Enter each of the commands displayed below the next paragraph into the Management Shell to
3224 configure a new attribute, "company," for the existing Trusted Identity Token Issuer named
3225 "Federated Logon from Identity Provider." Enter each command separately, and enter a carriage
3226 return after the command. If the command executed successfully, Management Shell will not
3227 provide any feedback. If an error occurs, Management Shell will display the error.

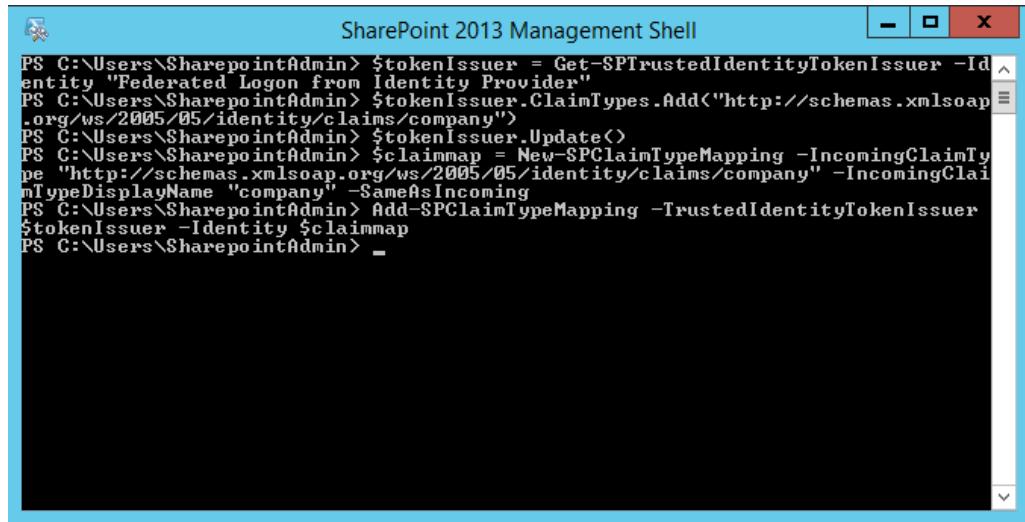
3228 \$tokenIssuer = Get-SPTrustedIdentityTokenIssuer -Identity "Federated Logon from
3229 Identity Provider"

3230 \$tokenIssuer.ClaimTypes.Add("http://schemas.xmlsoap.org/ws/2005/05/identity/cla
3231 ims/company")

3232 \$tokenIssuer.Update()

3233 \$claimmap = New-SPClaimTypeMapping -IncomingClaimType
3234 "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company" -
3235 IncomingClaimTypeDisplayName "company" -SameAsIncoming

- 3236 4. Add-SPClaimTypeMapping -TrustedIdentityTokenIssuer \$tokenIssuer -Identity \$claimmap



```
SharePoint 2013 Management Shell
PS C:\Users\SharepointAdmin> $tokenIssuer = Get-SPTrustedIdentityTokenIssuer -Id entity "Federated Logon from Identity Provider"
PS C:\Users\SharepointAdmin> $tokenIssuer.ClaimTypes.Add("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company")
PS C:\Users\SharepointAdmin> $tokenIssuer.Update()
PS C:\Users\SharepointAdmin> $claimmap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company" -IncomingClaimTypeDisplayName "company" -SameAsIncoming
PS C:\Users\SharepointAdmin> Add-SPClaimTypeMapping -TrustedIdentityTokenIssuer $tokenIssuer -Identity $claimmap
PS C:\Users\SharepointAdmin> _
```

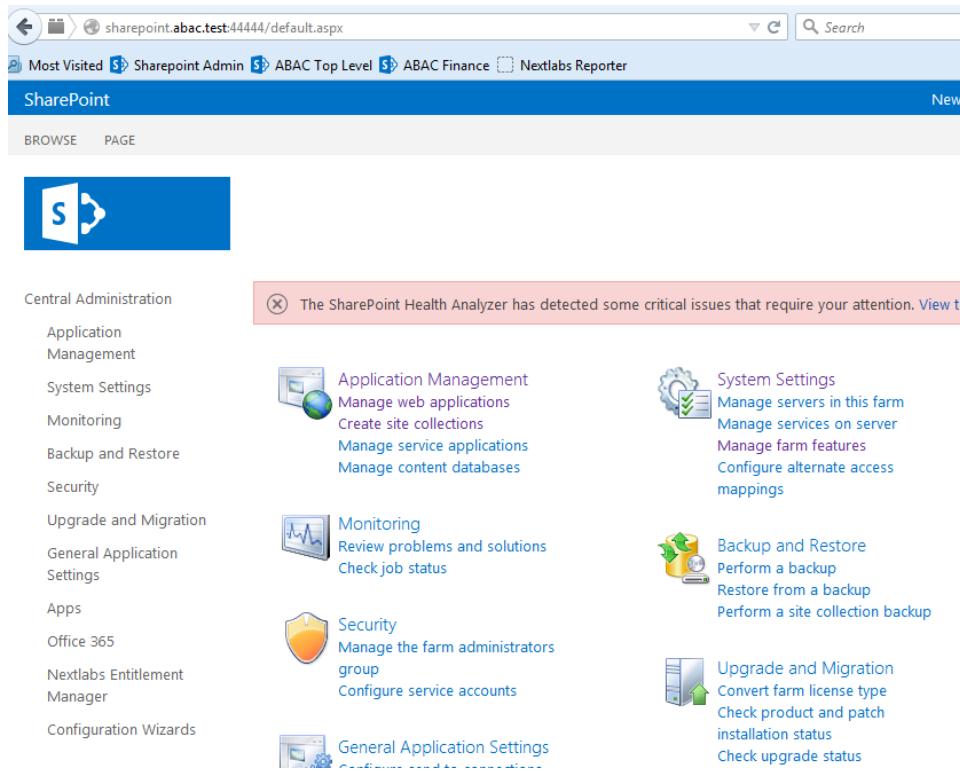
3237

3238 **6.4.2.1 Functional Test of SharePoint Reading Attributes from PingFederate-RP**

3239 The instructions in this section will help you perform a test to ensure that SharePoint can read the
3240 attributes sent in messages from the PingFederate-RP.

- 3241 1. First, follow the instructions in this section to ensure that SharePoint is configured to read the
3242 newly configured attributes from PingFederate-RP.
- 3243 2. Launch your browser and go the SharePoint central administration page (e.g.,
3244 <http://SharePoint.abac.test:44444/default.aspx>).
- 3245 3. Log on using the credentials of the SharePoint administrator.

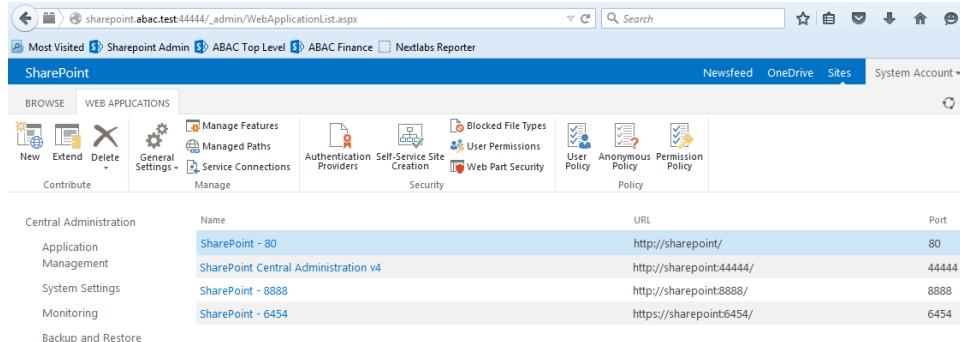
SECOND DRAFT



The screenshot shows the SharePoint Central Administration interface. On the left, there's a navigation menu with links like Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, Apps, Office 365, Nextlabs Entitlement Manager, and Configuration Wizards. In the center, there's a large blue button with the SharePoint logo. To the right, a red alert box from the SharePoint Health Analyzer states: "The SharePoint Health Analyzer has detected some critical issues that require your attention. View the details". Below the alert, there are several sections with icons and links: Application Management (Manage web applications, Create site collections, Manage service applications, Manage content databases), System Settings (Manage servers in this farm, Manage services on server, Manage farm features, Configure alternate access mappings), Monitoring (Review problems and solutions, Check job status), Security (Manage the farm administrators group, Configure service accounts), Backup and Restore (Perform a backup, Restore from a backup, Perform a site collection backup), Upgrade and Migration (Convert farm license type, Check product and patch installation status, Check upgrade status), and General Application Settings.

3246

- 3247 4. Under the Application Management group, click on **Manage Web Applications**.
- 3248 5. Click on the web application that contains the SharePoint site you are managing (e.g., **SharePoint - 80**). SharePoint highlights the web application row that you clicked.
- 3249



The screenshot shows the SharePoint Admin Center with the "WEB APPLICATIONS" tab selected. The top navigation bar includes links for Newsfeed, OneDrive, Sites, and System Account. Below the navigation, there are tabs for New, Extend, Delete, General Settings, Manage Features, Managed Paths, Authentication Providers, Self-Service Site Creation, Blocked File Types, User Permissions, Web Part Security, User Policy, Anonymous Policy, and Permission Policy. The main content area displays a table of web applications:

Name	URL	Port
SharePoint - 80	http://sharepoint/	80
SharePoint Central Administration v4	http://sharepoint:44444/	44444
SharePoint - 8888	http://sharepoint:8888/	8888
SharePoint - 6454	https://sharepoint:6454/	6454

3250

- 3251 6. Click **User Policy**.

SECOND DRAFT

The screenshot shows the SharePoint Central Administration interface. In the center, a modal dialog box titled "Policy for Web Application" is displayed. The dialog contains a warning message: "Adding or updating Web application policy with new users or groups will trigger a SharePoint Search crawl over all content covered by that policy. This can reduce search crawl freshness and increase crawl load. Consider using security groups at the policy level and add/remove users from security groups to avoid this." Below the message, there are three buttons: "Add Users", "Delete Selected Users", and "Edit Permissions of Selected Users". A table lists users with their zones and permissions:

Zone	Display Name	User Name	Permissions
(All zones)	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\LOCAL SERVICE	Full Read

At the bottom right of the dialog is an "OK" button. The background of the Central Administration page shows a list of management links on the left and a table of ports on the right.

3252

3253

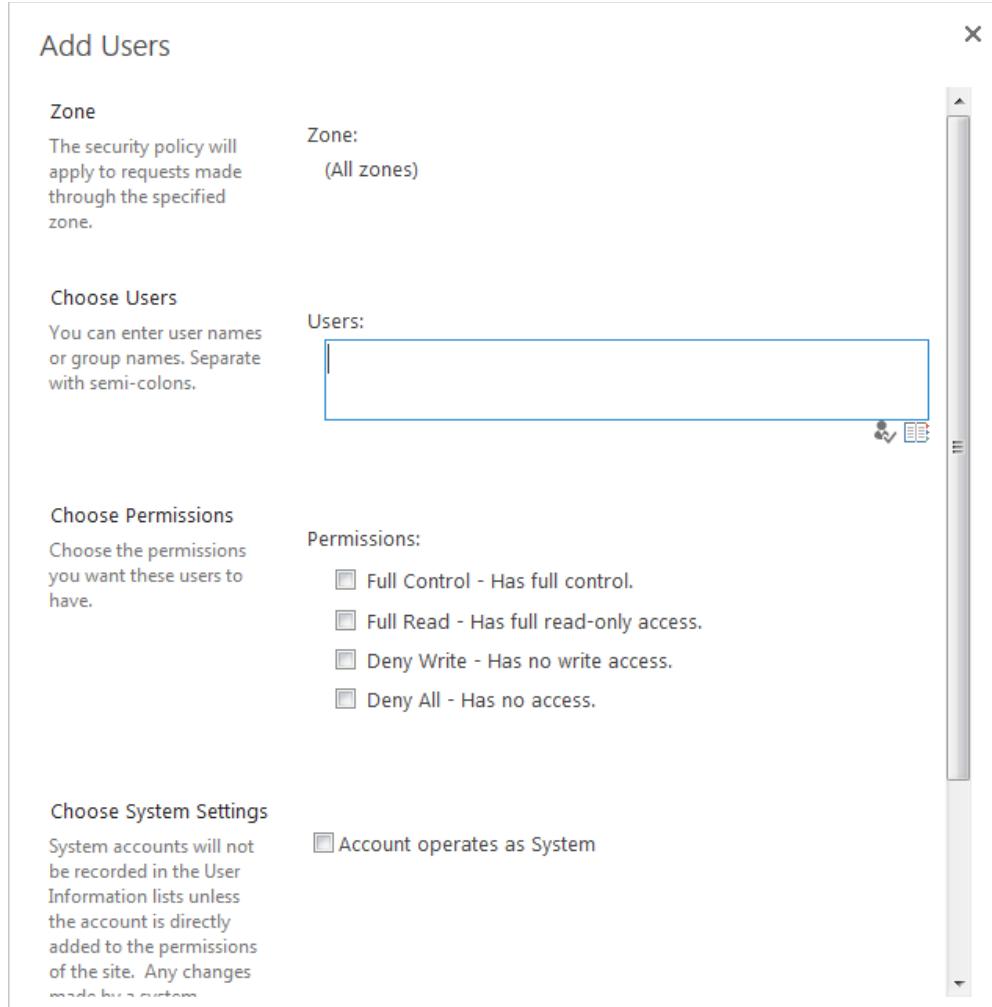
7. Click the **Add users** link.

The screenshot shows the "Add Users" dialog box. It has a header "Add Users" and a close button. Below the header is a section titled "Select the Zone" with a descriptive text: "The security policy will apply to requests made through the specified zone. To apply a policy to all zones, select '(All zones)'. All zone policies are only valid for Windows users." To the right of this text is a "Zones:" label followed by a dropdown menu set to "(All zones)". At the bottom right of the dialog are "Next >" and "Cancel" buttons.

3254

3255

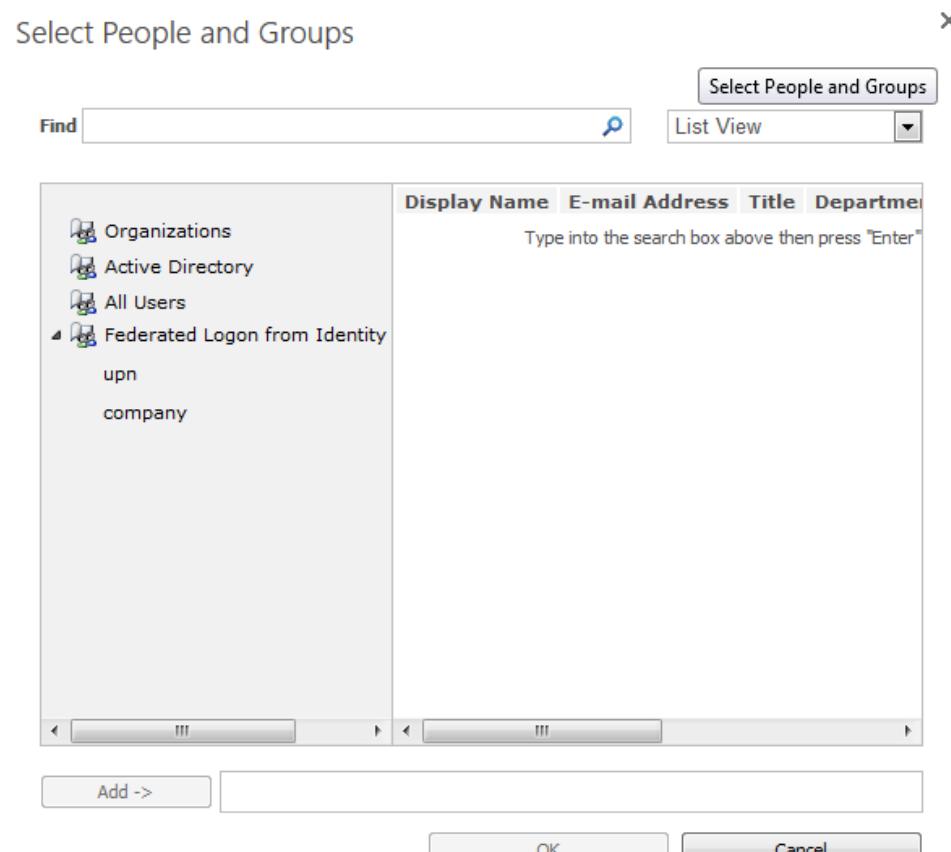
8. Click **Next**.



3256

- 3257 9. On the **Add Users** screen, click the small browse icon (looks like an open book) under the **Users** field.

3259 **Expected Result:** On the Select People and Groups screen, you should see a grouping with the
 3260 name of the trusted token issuer (e.g., Federated Logon from Identity Provider). You should also
 3261 see the newly configured attribute (e.g., company) listed under that grouping.



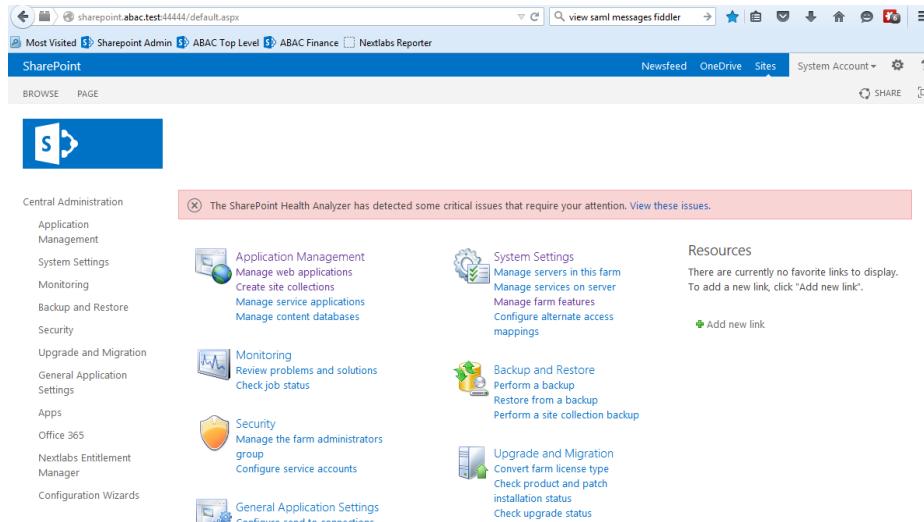
3262

3263 6.5 Configure the Claims Viewer Web Part at the SharePoint Site

3264 Follow the instructions below to configure the Claims Viewer web part at the SharePoint site. The Claims
 3265 Viewer is a component that is useful to the SharePoint administrator because it displays a list of the
 3266 attributes that are loaded into the web session. This list can be used to validate that the correct set of
 3267 attributes and associated values are being passed from the PingFederate-RP, and that SharePoint is
 3268 correctly configured to read the attributes.

- 3269 1. Log on to the server that hosts SharePoint for the RP.
- 3270 2. Launch your browser and go the SharePoint central administration page (e.g.,
 3271 <http://SharePoint.abac.test:44444/default.aspx>). Log on using the credentials of the SharePoint
 3272 administrator.
- 3273 The central administration home page displays.

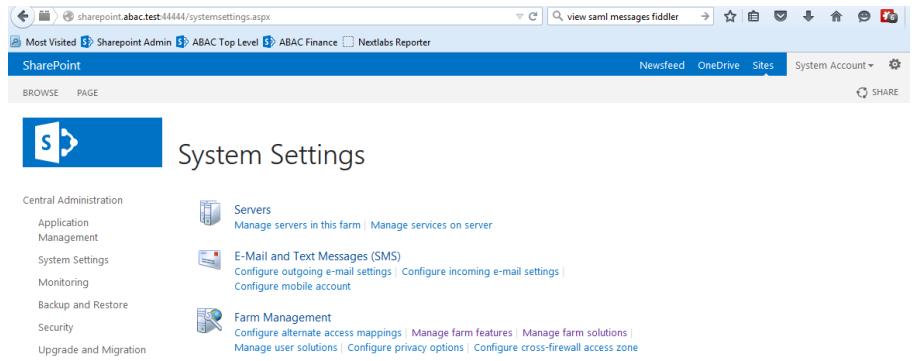
SECOND DRAFT



The screenshot shows the SharePoint Central Administration interface. On the left, there's a navigation menu with links like Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, Apps, Office 365, Nextlabs Entitlement Manager, and Configuration Wizards. A red alert box at the top right says: "The SharePoint Health Analyzer has detected some critical issues that require your attention. View these issues." Below the alert, there are several sections: Application Management, System Settings, Resources, Monitoring, Security, and General Application Settings. Each section has a brief description and some links.

3274

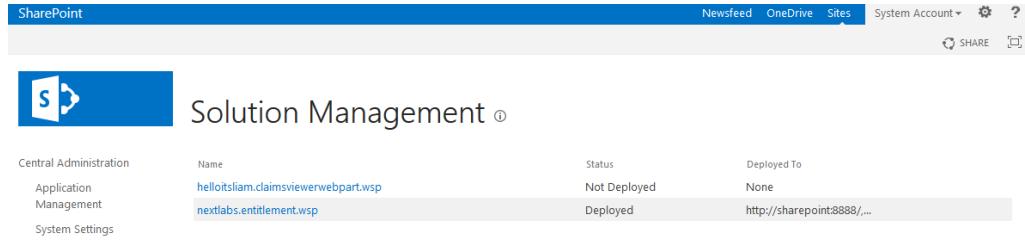
3. On the **Central Administration** menu on the left, click **System Settings**.



The screenshot shows the SharePoint System Settings page. The left sidebar includes links for Application Management, System Settings, Monitoring, Backup and Restore, Security, and Upgrade and Migration. The main content area is titled "System Settings" and contains sections for Servers, E-Mail and Text Messages (SMS), and Farm Management, each with their respective management links.

3276

4. On the **Farm Management** menu, click **Manage Farm Solutions**.

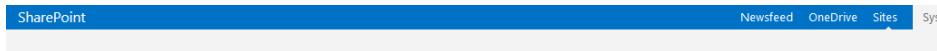


The screenshot shows the SharePoint Solution Management page. The left sidebar lists Central Administration, Application Management, System Settings, Monitoring, and Backup and Restore. The main content area is titled "Solution Management" and displays a table of solutions. One solution, "helloitsliam.claimsviewerwebpart.wsp", is highlighted in blue.

Name	Status	Deployed To
helloitsliam.claimsviewerwebpart.wsp	Not Deployed	None
nextlabs.entitlement.wsp	Deployed	http://sharepoint:8888/...

3278

5. Click on the **helloitsliam.claimsviewerwebpart.wsp** link.



Solution Properties

Central Administration

Application Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Apps

Office 365

Nextlabs Entitlement Manager

Configuration Wizards

[Deploy Solution](#) | [Remove Solution](#) | [Back to Solutions](#)

Name: helloitsliam.claimsviewerwebpart.wsp

Type: Core Solution

Contains Web Application Resource: Yes

Contains Global Assembly: Yes

Contains Code Access Security Policy: No

Deployment Server Type: Front-end Web server

Deployment Status: Not Deployed

Deployed To: None

Last Operation Result: The solution was successfully retracted.

SHAREPOINT : http://sharepoint/ : The solution was successfully retracted.

SHAREPOINT : http://sharepoint:8888/ : The solution was successfully retracted.

SHAREPOINT : http://sharepoint/ : The solution was successfully retracted.

SHAREPOINT : http://sharepoint:8888/ : The solution was successfully retracted.

Last Operation Details: 7/20/2015 7:08 PM

3280

3281

6. Click on the **Deploy Solution** link at the top of the page.



Deploy Solution ①

Central Administration

Application Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Apps

Office 365

Nextlabs Entitlement Manager

Configuration Wizards

Solution Information

Information on the solution you have chosen to deploy.

Name: helloitsliam.claimsviewerwebpart.wsp

Locale: 0

Deployed To: None

Deployment Status: Not Deployed

Deploy When?

A timer job is created to deploy this solution. Please specify the time at which you want this solution to be deployed.

Choose when to deploy the solution:

 Now At a specified time:7/20/2015 11 PM 00

Deploy To?

The solution contains Web application scoped resources and should be deployed to specific Web applications. Please choose the Web application where you want the solution to be deployed.

Choose a Web application to deploy this solution:

Warning: Deploying this solution will place assemblies in the global assembly cache. This will grant the solution assemblies full trust. Do not proceed unless you trust the solution provider.

3282

3283

7. Click **OK** at the bottom of the page.

3284

The claimsviewerwebpart should be shown as deployed on the **Solution Management** page.

SECOND DRAFT

The screenshot shows the SharePoint Central Administration interface. On the left, there is a navigation menu with items like Central Administration, Application Management, System Settings, Monitoring, Backup and Restore, Security, Upgrade and Migration, General Application Settings, Apps, Office 365, NextLabs Entitlement Manager, and Configuration Wizards. The main content area is titled "Solution Management" and displays a table with two rows. The first row has columns: Name (helloitsliam.claimsviewerwebpart.wsp), Status (Deployed), and Deployed To (http://sharepoint:3888/...). The second row has the same structure. At the bottom of the table, there is a "View All" link.

Name	Status	Deployed To
helloitsliam.claimsviewerwebpart.wsp	Deployed	http://sharepoint:3888/...
nextlabs.entitlement.wsp	Deployed	http://sharepoint:3888/...

3285

3286 This completes the portion of the claims viewer web part configuration at the SharePoint central administration page.
3287

3288 *6.5.1.1 Configure SharePoint Claims Viewer*

3289 This section explains how to add a new page to the SharePoint site to view the claims.

- 3290 1. Log on to the RP's SharePoint site (e.g., <https://SharePoint.abac.test>) using the credentials of the SharePoint administrator. Select **Windows Authentication** at the Sign On screen.
3291

The screenshot shows the SharePoint site "Runabout Air - root site". The top navigation bar includes links for Newsfeed, OneDrive, Sites, System Account, Share, Follow, Sync, and Edit. Below the navigation, there is a search bar labeled "Search this site". The main content area features a "Get started with your site" section with five cards: "Share your site.", "Working on a deadline?", "Add lists, libraries, and other apps.", "What's your style?", and "Your site. Your brand.". On the left, there is a sidebar with a navigation menu including ABAC Root Site, Documents, Access Control, Claims Viewer, ABAC Finance Dept, ABAC IT Dept, ABAC Marketing Dept, ABAC Research Dept, ABAC Sales Dept, Recent, and Site Contents. The "Recent" item is highlighted. The "Documents" section shows a "new document" button and a table for sorting by Name, Modified, and Modified By. A message states "There are no documents in this view."

3292

- 3293 2. Click the gear icon at the top right corner of the page and select the **Site Contents** link.

SECOND DRAFT

Runabout Air

Runabout Air - root site Finance Internet Technology Marketing Research and Development Sales EDIT LINKS Search this site

Site Contents

Lists, Libraries, and other Apps SITE WORKFLOWS SETTINGS RECYCLE BIN (0)

ABAC Root Site	Documents	Content and Structure Reports	Documents
Access Control	Form Templates	7 items Modified 3 months ago	0 items Modified 7 weeks ago
Claims Viewer	Reusable Content	3 items Modified 3 months ago	2 items Modified 7 weeks ago
...	Site Collection Documents	0 items Modified 3 months ago	Site Assets
ABAC Finance Dept	Style Library	0 items Modified 3 months ago	Site Pages
ABAC IT Dept		28 items Modified 3 months ago	Workflow Tasks
ABAC Marketing Dept			0 items Modified 3 months ago
ABAC Research Dept			
ABAC Sales Dept			
Recent			
Site Contents			
EDIT LINKS			

3294

- 3295 3. Click on the Site Pages library. This will show a list of the existing pages on the site.

Runabout Air

Runabout Air - root site Finance Internet Technology Marketing Research and Development Sales EDIT LINKS Search this site

Site Pages

+ new Wiki page

All Pages By Author By Editor ... Find a file

ABAC Root Site	Name	...
Documents	test2	...
Access Control	test1	...
Claims Viewer	Home	...
...	ClaimsViewer	...
ABAC Finance Dept	How To Use This Library	...
ABAC IT Dept		
ABAC Marketing Dept		
ABAC Research Dept		
ABAC Sales Dept		
Recent		
Site Contents		
EDIT LINKS		

3296

- 3297 4. Click the new Wiki page link to add a new page. This link may be named differently, depending
3298 on your site's SharePoint template. Enter a name for the new page (e.g., ClaimsView).

Runabout Air

Runabout Air - root site Finance Internet Technology Marketing Research and Development Sales EDIT LINKS Search this site

New Item

New page name:

ClaimsView

Find it at <https://sharepoint.abac.test/SitePages/ClaimsView.aspx>

Create Cancel

ABAC Root Site	New page name:
Documents	ClaimsView
Access Control	
Claims Viewer	
...	
ABAC Finance Dept	
ABAC IT Dept	
ABAC Marketing Dept	
ABAC Research Dept	
ABAC Sales Dept	
Recent	
Site Contents	
EDIT LINKS	

3299

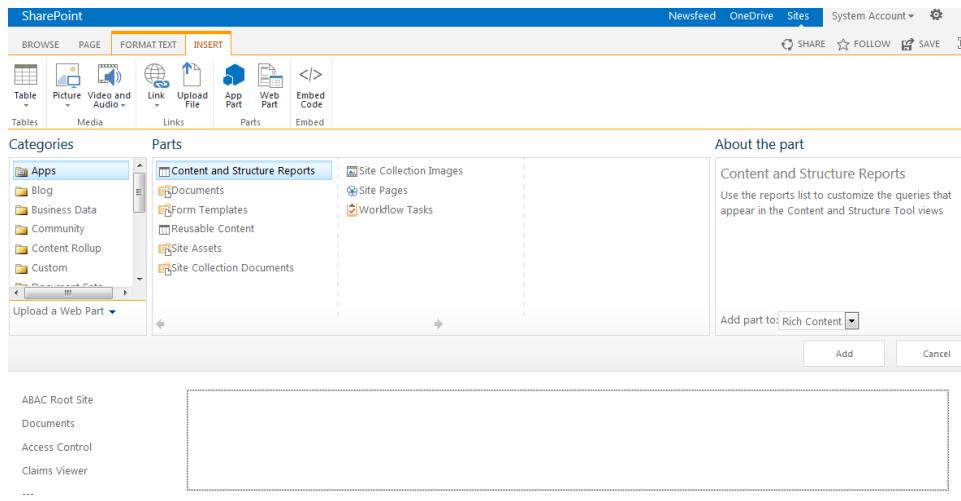
- 3300 5. Click **Create**. The SharePoint page editor for the newly added page displays.

SECOND DRAFT

3301

3302

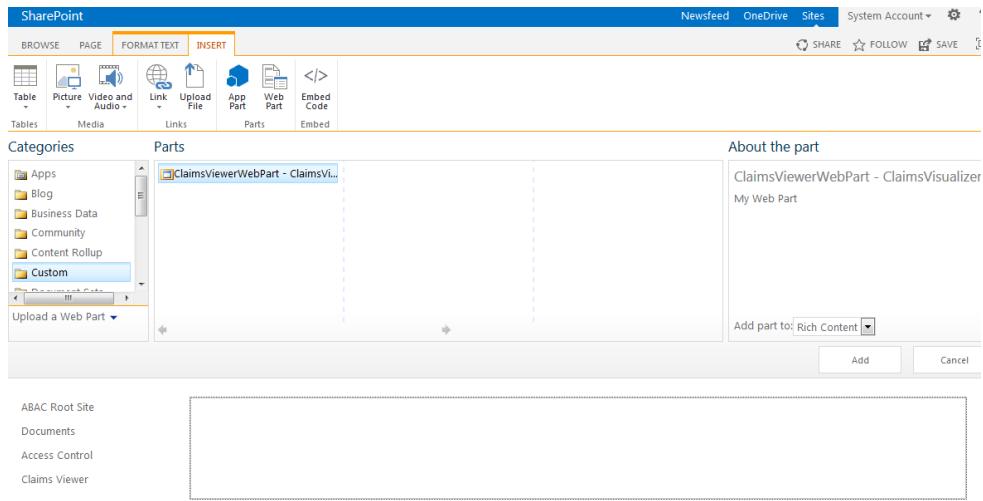
6. Click on the **INSERT** tab at the top of the page. Click on the **Web Part** button.



3303

3304

7. In the **Categories** list, select **Custom**. In the **Parts** list, select **ClaimsViewerWebPart**.

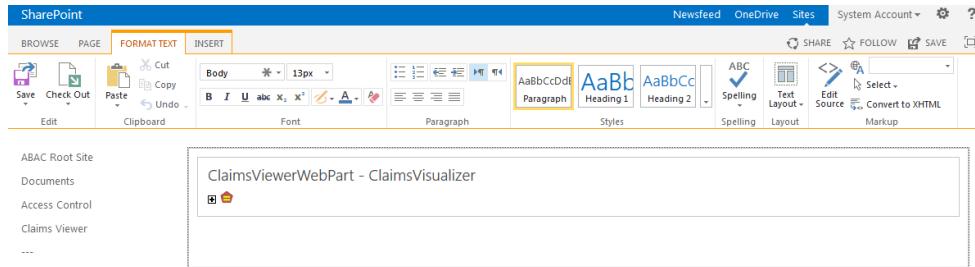


3305

3306

8. Click **Add**.

SECOND DRAFT



3307

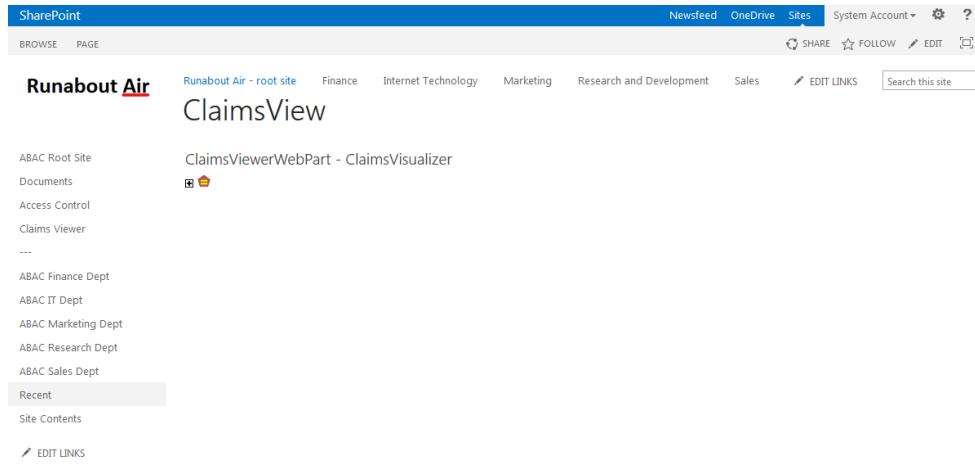
9. Click the **SAVE** button at the top right corner of the page.

3309

SharePoint launches the new page (e.g., ClaimsView) that was just created. Save the URL of the new page (e.g., <https://SharePoint.abac.test/SitePages/ClaimsView.aspx>), because you will use it later in a functional test.)

3312

The Claims Viewer Web Part on the page displays. It is collapsed by default.



3313

10. Click on the + sign under **ClaimsViewerWebPart** to view the claims data. You will see a list of claim values and information about the SAML token at the bottom of the page.

The screenshot shows a SharePoint page titled "Runabout Air - root site" with a navigation bar for Finance, Internet Technology, Marketing, Research and Development, Sales, and Edit Links. The main content area is titled "ClaimsView" and displays a table titled "Issued Identity". The table has two columns: "Claim Type" and "Claim Value". The data in the table is as follows:

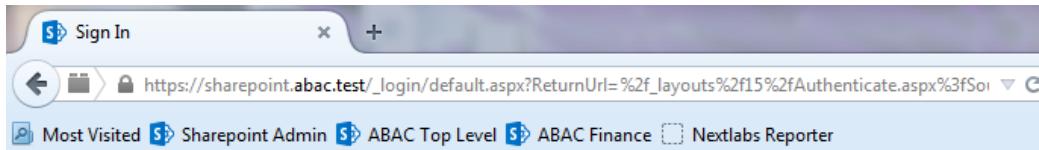
Claim Type	Claim Value
http://schemas.xmlsoap.org/.ws/2005/05/identity/claims/nameidentifier	abac\sharepointadmin
http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupid	S-1-5-21-972639958-268376111-2639239546-1108
http://schemas.microsoft.com/ws/2008/06/identity/claims/primarygroupname	S-1-5-21-972639958-268376111-2639239546-513
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	SharepointAdmin@ABAC.TEST
http://schemas.microsoft.com/sharepoint/2009/08/claims/userlogonname	ABAC\sharepointadmin
http://schemas.microsoft.com/sharepoint/2009/08/claims/userid	0# w\abac\sharepointadmin
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/username	0# w\abac\sharepointadmin

3316

3317 6.6 Functional Test of All Configurations for Section 6

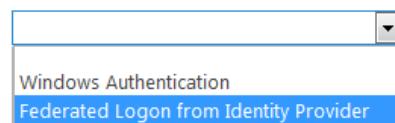
3318 The instructions in this section will perform an integrated test all of the configurations in Section 6.
 3319 Using the browser, you will log on using an account that was created in Microsoft AD. Then you will use
 3320 the SharePoint claims viewer to validate that the newly configured attributes are passed from the IdP to
 3321 the RP and that the attributes are successfully loaded into the SharePoint web session.

3322 1. Launch your browser and go to the RP's SharePoint site (e.g., <https://SharePoint.abac.test>).



Sign In

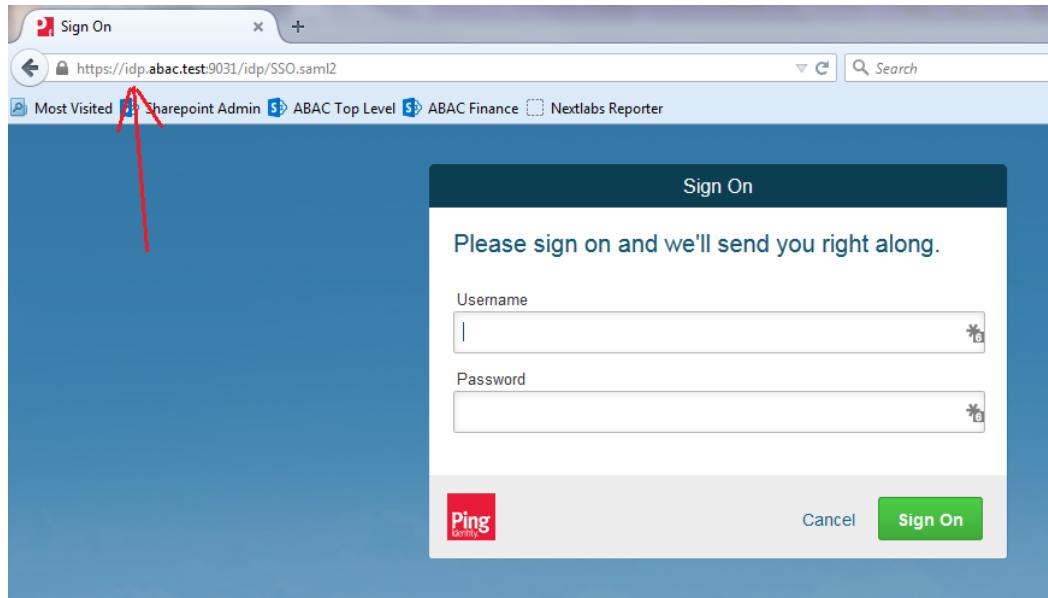
Select the credentials you want to use to logon to this SharePoint site:



3323

3324 2. Select **Federated Logon from Identity Provider**.

3325 Your browser is redirected to the PingFederate-IdP, and you see the PingFederate Sign On
 3326 screen.



3327

- 3328 3. Enter the credentials of the Microsoft AD account created earlier in this guide (e.g., **Ismith**).

A screenshot of a sign-on page titled "Sign On". The page instructs the user to "Please sign on and we'll send you right along.". It has fields for "Username" and "Password". The "Username" field contains "Ismith". The "Password" field contains a series of dots representing a password. At the bottom are "Cancel" and "Sign On" buttons, with the "Ping Identity" logo on the left.

3329

- 3330 4. Click **Sign On**. On the **RSA Adaptive Authentication** screen, enter the SMS validation code
3331 received on your mobile phone. Then, click **Continue**.

3332 Once authenticated at the IdP, your browser automatically redirects to the PingFederate-RP
3333 (e.g., *rp.abac.test*) and then to the RP's SharePoint (*SharePoint.abac.test*) site.

SECOND DRAFT

Get started with your site [REMOVE THIS](#)

Add lists, libraries, and other apps.

Documents

[+ new document](#) or drag files here

✓	Name	Modified	Modified By
There are no documents in this view.			

3334

- 3335 5. Once you arrive at the SharePoint site home page, navigate to the claims viewer page that was
 3336 created in the earlier section (e.g., <https://SharePoint.abac.test/SitePages/ClaimsView.aspx>).
 3337 Expand the claims viewer web part on the page to see a list of claims.

3338 **Expected Result:** You should see the newly configured attribute (e.g., **company**) and its
 3339 associated claim value. The claims viewer shows the name of each attribute (i.e., **claim**) using a
 3340 long format such as <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company>.

Issued Identity	
Claim Type	Claim Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	lsmith
http://schemas.xmlsoap.org/ws/2005/05/identity/upn	lsmith
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company	Conway Inc.
http://schemas.microsoft.com/sharepoint/2009/08/claims/used	0e:t:federated logon from identity provider lsmith
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0e:t:federated logon from identity provider lsmith
http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider	trusted:Federated Logon from Identity Provider

3341

3342 **6.6.1 Temporarily Disable SAML Encryption for Testing and Troubleshooting**
 3343 **Message Exchanges**

3344 Follow the instructions below to temporarily disable the encryption of SAML messages between the IdP
 3345 and the RP. You should perform the steps in this section only when explicitly instructed to do so in
 3346 another section of the guide (e.g., during a functional test). You may also need to refer back to this
 3347 section in the future to test or troubleshoot SAML message exchanges in your environment.

3348 Temporarily disabling the encryption can help test that the expected attributes are being exchanged
 3349 between the IdP and the RP. By temporarily disabling the encryption, you will be able to see the
 3350 attributes and their associated values in the SAML messages using the Firefox SAML tracer add-on or a
 3351 comparable software tool. When testing or troubleshooting is completed, you can enable the encryption
 3352 again.

3353 **6.6.1.1 Disable SAML Encryption**

- 3354 1. Launch your browser and go to https://<DNS_NAME>:9999/pingfederate/app. Replace
 3355 **DNS_NAME** with the fully qualified name of the IdP's PingFederate server (e.g.,
 3356 <https://idp.abac.test:9999/pingfederate/app>). Log on to the PingFederate application using the
 3357 credentials you configured during installation.
- 3358 2. On the **Main** menu under **SP CONNECTION**, click **Manage All SP**.
- 3359 3. Click on the link for the SP connection for which you want to disable the encryption (e.g.,
 3360 <https://rp.abac.test:9031>).
- 3361 4. Scroll down to the **Protocol Settings** group.

Protocol Settings	
ASSERTION CONSUMER SERVICE URL	
Endpoint	URL: /sp/ACS.saml2 (POST)
ALLOWABLE SAML BINDINGS	
Artifact	false
POST	true
Redirect	true
SOAP	false
SIGNATURE POLICY	
Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false
ENCRYPTION POLICY	
Encrypt Entire Assertion	true

- 3362 5. Click on the **ENCRYPTION POLICY** link.
- 3363 6. On the **Encryption Policy** screen, select **None**.

Protocol Settings

Assertion Consumer Service URL Allowable SAML Bindings Signature Policy **Encryption Policy** Summary

Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.

None
 The entire assertion
 One or more attributes
 SAML_SUBJECT
 company

Cancel < Previous Next > Done Save

3365

3366 7. Click **Save**.

3367 At this point, you have disabled SAML encryption at the IdP for this specific connection to the RP. You
 3368 can perform authentication testing using the Firefox SAML tracer to examine the SAML messages being
 3369 sent by the IdP to the RP.

3370 *6.6.1.2 Enable SAML Encryption again*

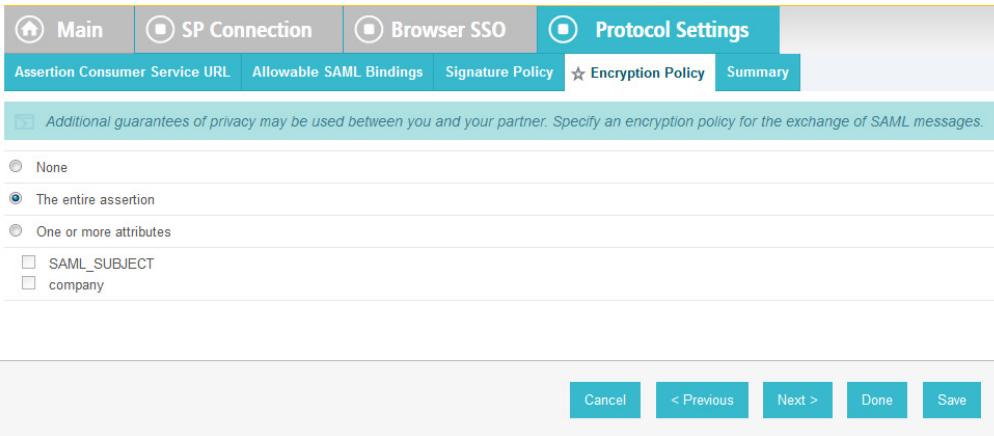
3371 Once testing is completed, follow the instructions below to enable the encryption once again.

- 3372 1. On the PingFederate Main Menu under SP CONNECTION, click **Manage All SP**.
- 3373 2. Click on the link for the SP connection for which you want to enable the encryption (e.g.,
 3374 <https://rp.abac.test:9031>).
- 3375 3. Scroll down to the Protocol Settings group.

Protocol Settings	
ASSERTION CONSUMER SERVICE URL	
Endpoint	URL: /sp/ACS.saml2 (POST)
ALLOWABLE SAML BINDINGS	
Artifact	false
POST	true
Redirect	true
SOAP	false
SIGNATURE POLICY	
Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false
ENCRYPTION POLICY	
Status	Inactive
Credentials	

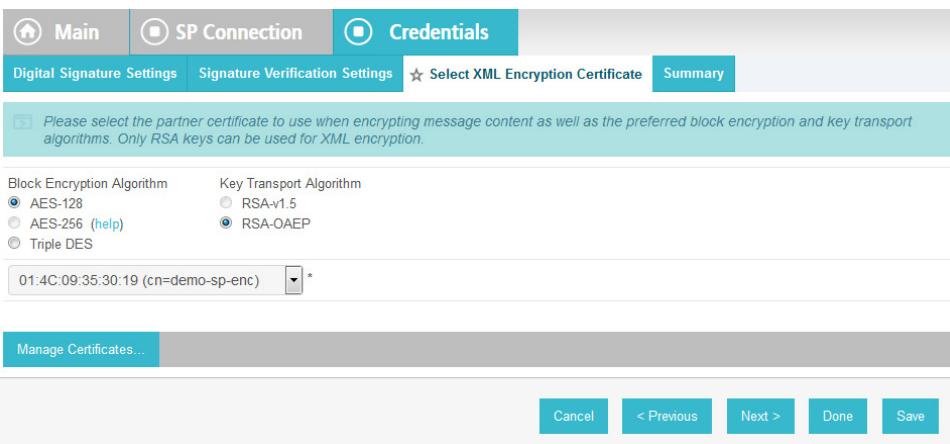
3376

- 3377 4. Click on the **ENCRYPTION POLICY** link.
- 3378 5. On the **Encryption Policy** screen, select **The entire assertion**.



3379

- 3380 6. Click **Save**.
- 3381 7. On the Select XML Encryption Certificate screen, select the **Block Encryption Algorithm** (e.g.,
3382 **AES-128**), and the **Key Transport Algorithm** (e.g., **RSA-OAEP**). For the selection box above
3383 **Manage Certificates**, select the RP's public key certificate to be used to encrypt the message
3384 content.



3385

- 3386 8. Click **Save**.
- 3387 You have now enabled the encryption for the connection again.

3388 7 Setting Up NextLabs to Protect SharePoint

3389 7.1 Introduction

- 3390 In this build we are using an ABAC architecture to protect resources on a Microsoft SharePoint instance.
3391 In this section, we will install the NextLabs Control Center, Policy Studio, Policy Controller, and
3392 Entitlement Manager for SharePoint Server. Before getting started installing these components, you
3393 must prepare your environment. At a minimum, Windows Server 2012 must be set up with a configured
3394 Active Directory, and SharePoint must be installed and configured with a Site Collection. If you haven't
3395 already completed the basic installation and configuration of Windows Server 2012 and Active
3396 Directory, please refer back to [Section 2](#), "Setting up the Identity Provider." If you haven't already

3397 completed the installation and configuration of SharePoint, please refer to [Section 4](#), “Installing and
3398 Configuring Microsoft SharePoint Server and Related Components.”

3399 The four NextLabs components installed in this How-To section provide an Information Control Platform
3400 (ICP), Policy Administration Point (PAP), Policy Decision Point (PDP), and Policy Enforcement Point (PEP)
3401 in the ABAC Architecture. Each component will be described generally in the Components section. Then
3402 there will be separate sections illustrating installation and configuration of each component. Finally, the
3403 Functional Test section will give some guidance for verifying the correct installation and configuration of
3404 the various components presented in this section.

3405 7.2 Components

- 3406 ▪ **NextLabs Control Center (release 7.5):** enterprise-level Information Control Platform (ICP) for
3407 policy-driven data loss prevention and entitlement management; can contain many software
3408 components, including the following two in this build:
 - 3409 • **Policy Studio: Enterprise Edition (PAP):** application for policy lifecycle management,
3410 provides a graphical user interface (GUI) for defining and deploying ABAC policies. This
3411 product is installed on an instance of SQL Server.
 - 3412 • **Policy Controller (PDP):** distributed component of the Control Center that evaluates policies
3413 created in the PAP to determine a deny or allow decision when users attempt to access
3414 protected resources. This product is installed on an instance of Microsoft SharePoint Server.
- 3415 ▪ **NextLabs Entitlement Manager for Microsoft SharePoint Server (PEP):** enforces the decisions
3416 from the PDP to deny or allow access to SharePoint resources. this product is installed on an
3417 instance of Microsoft SharePoint Server.

3418 7.2.1 NextLabs Control Center (release 7.5)

3419 The NextLabs Control Center is an enterprise-level Information Control Platform (ICP). It integrates into
3420 existing IT infrastructure, and applications and can be used to digitally manage policies to govern data
3421 classification, access, sharing, and automate security compliance procedures. In order to fulfill its diverse
3422 capabilities, the Control Center can be configured to incorporate and coordinate many NextLabs
3423 software components. It is also possible to develop your own custom access control enforcers for
3424 applications that do not already have an available enforcer built by NextLabs. In this build, we take
3425 advantage of the Policy Studio, Policy Controller, and Entitlement Manager for Microsoft SharePoint
3426 Server, which are discussed in the following sub-sections.

3427 In order to support administrative and configuration activities necessary for its many components,
3428 NextLabs Control Center provides a web application user interface called Administrator. Some of the
3429 system monitoring and administrative tasks available via Administrator include: checking how many
3430 policies are deployed in the network, finding out on which hosts the Control Center components are
3431 installed, checking the status of Control Center server components, finding out how many enforcers are
3432 currently running, finding out if any enforcers are disconnected, and finding out or modifying the
3433 current heartbeat setting for an enforcer, among others.

3434 Another key component of the Control Center is the Policy Server. The Policy Server runs continuously
3435 from the moment of startup as a Windows service. As new policy is defined or policies are updated, the
3436 Policy Server pushes these policy sets to the Policy Controller on the SharePoint Server.

3437 The Control Center platform is installed and configured on the same server as the build's SQL database,
3438 which we refer to as the SQL Server.

3439 **7.2.2 NextLabs Policy Studio: Enterprise Edition**

3440 The NextLabs Policy Studio component of the Control Center is intended for administrators and policy
3441 designers responsible for converting the general data access and usage management goals of the
3442 enterprise into deployable, active policies. Depending on a company's business rules, policies can be
3443 defined to evaluate user (subject) attributes, resource (object) attributes, and environmental
3444 (contextual) attributes.

3445 The Policy Studio provides a graphical user interface with which you can create an abstract model
3446 representing the various parts of the enterprise environment (users, applications, computers, and
3447 environmental context), construct policies with these modeled components, and fine-tune policies using
3448 advanced conditions that can change based on dynamic comparisons, evaluations, and contextual
3449 factors. For example, policy designers can select pre-defined conditions including the time of day, day of
3450 the week, connection type, and IP address, among many others. In addition to defining which attributes
3451 to evaluate when making an enforcement decision, the policy construction process can also determine
3452 notification obligations such that when a policy is allowed or denied, a user can be notified with a
3453 default or custom message, a statement can be added to the application's log file, and an email can be
3454 sent to an administrator.

3455 Like the Control Center platform, the Policy Studio is installed and configured on the SQL Server.

3456 **7.2.3 NextLabs Policy Controller**

3457 Each NextLabs Policy Controller provides the interface to the Policy Server component of the Control
3458 Center (installed on the SQL Server), and serves as a distributed Policy Decision Point (PDP). It comprises
3459 a set of software modules delivered with Control Center, ready-to-install on the enforcer host or
3460 development machine. Because it is not specific to any adapter type, it requires no customization. In this
3461 build, the Policy Controller is installed and configured on the same server as the SharePoint instance,
3462 which we refer to as the SharePoint Sever.

3463 In general, the logical architecture of a NextLabs enforcer that protects an application (such as the
3464 Entitlement Manager for SharePoint Server, covered in the next sub-section) consists of two parts, the
3465 Policy Controller and the Policy Adapter.

3466 The Policy Controller consists of the following functional components:

- 3467 ■ The **Policy Evaluation Engine** evaluates whether or not each user action is covered by any of the
3468 policies currently cached at that enforcement point. It bases its evaluation on multiple criteria
3469 such as who the user is, what host he is using, how he is connected to the network, which action
3470 is being attempted, on what resource, the date, the time, and so on. It does this in real time,
3471 and operates continuously whether the host is connected to the network or not. Note that while
3472 disconnected from the network the local encrypted bundle.bin policy cache would not be able
3473 to be updated from policy changes made in the PAP.

3474 Note: Policies are authored in the PAP GUI on the SQL Server, and any modifications to the
3475 policy set are transmitted by the Policy Server, also installed on the SQL Server, to the Policy

- 3476 Controller on the SharePoint Server. It takes a heartbeat length of time for the updates to take
3477 effect on the SharePoint Server. By default, the heartbeat rate of the desktop enforcer is set to
3478 60 minutes, which is appropriate for a live production environment. For testing and learning
3479 purposes, however, you should change this to 1 minute, which will allow you to define, deploy
3480 and test policies with shorter delays. A heartbeat can be configured via the Control Center
3481 Administrator web application.
- 3482 ■ The **Context Manager** keeps constant track of the environmental context of all events, and
3483 provides it to the Policy Engine and Policy Adapter. The context includes user identity, computer
3484 host name, network connection type, and date and time.
- 3485 ■ For any policy that evaluates as True, the **Obligation Manager** initiates an obligation by sending
3486 a request to a policy adapter's obligation services or executing built-in obligations. It contains
3487 three sub-components:
- 3488 ● **Policy Logger** - collects and logs all activity details and policy decision results
- 3489 ● **Messaging Services** - sends message to recipients or targets listed in a policy
- 3490 ● **Application Extender** - launches an application or custom executable that performs some
3491 custom obligation
- 3492 ■ The **Controller Manager** records non-policy activities, updates the configuration, and secures
3493 the controller. Components include:
- 3494 ● **Activity Recorder** - records activities tracked by the policy adapter in real time.
- 3495 ● **Configuration Manager** - applies profile and system configuration changes in real time
- 3496 ● **Policy Authentication** - authenticates the policy set from the Policy Server and encrypts it
3497 on the local file system
- 3498 Note: It is the responsibility of the Controller Manager to encrypt the bundle.bin file on the
3499 local file system for use during policy evaluation by the PDP.
- 3500 ● **Tamper Resistance Module** - protects all Entitlement Manager processes, installed files, and
3501 registry settings from tampering by users or other processes, and governs the automatic
3502 start-up and restart features. The Policy Controller runs as a Windows service continuously
3503 from the moment of startup, called **Control Center Enforcer Service**.
- 3504 ■ The **ICENet Client** provides the interface for all communication with the Policy Server. It is used
3505 for deploying new or changed policies, periodically sending activity logs from each control point,
3506 and providing controller health status.

3507 7.2.4 NextLabs Entitlement Manager for Microsoft SharePoint Server

3508 The NextLabs Entitlement Manager for SharePoint is designed to enforce the policies that control
3509 whether and how users can access, download, and use data stored on a SharePoint server. SharePoint
3510 policies can apply to entire portals or to any parts thereof, and allow some users to view all webparts on
3511 a page while blocking other users from viewing some subset of the webparts on the same page.

7.2.5 Required or Recommended Files, Hardware, and Software

Component	Required Files	Recommended or Minimum Hardware Requirements	Hardware Used in this Build	Recommended or Minimum Operating System or Other Software	Operating System or Other Software Used in this Build
Control Center (CC)	license.dat; ControlCenter-64-7.5.0.0-64-201410211146.zip	1GB RAM; 1GHz CPU; 4GB free disk space		Windows Server 2008, Enterprise Edition, R2, 64-bit, or Windows Server 2012; Java bundled and installed within NextLabs CC; Microsoft SQL Server 2012; Microsoft SQL Server Management Studio	Windows Server 2012; Java bundled and installed within NextLabs software architecture; Microsoft SQL Server 2012; Microsoft SQL Server Management Studio
External Data-base	N/A	500 GB for table space	500 GB for table space	Internal PostgreSQL; External, PostgreSQL, External Oracle, or External MS SQL Server	External MS SQL Server 2012
Policy Studio	PolicyStudio-setup64-7.5.0.0-10-201410291227.zip	i3 or above, 1.5 GHz, dual-core CPU; 2GB; 10 GB free disk space		Windows XP, Service Pack 3, 32-bit, Windows 7, 32-bit and 64-bit, or Windows Server 2008, Enterprise Edition, R2, 64-bit; Microsoft SQL Server 2012; Microsoft SQL Server Management Studio	Windows Server 2012; Microsoft SQL Server 2012; Microsoft SQL Server Management Studio
Policy Controller	PolicyController-CE-64-7.0.1.0-1-201405191624.zip	2GB RAM; i3 or above, 1.5 GHz, dual-core CPU; 10 GB free disk space		Windows XP, Service Pack 3, 32-bit Windows 2003, 32-bit, Windows 7, 32-bit and 64-bit, Windows Server 2008, Enterprise Edition, R2, 64-bit, or Red Hat Linux Release 1, Updates 1-3	Windows Server 2012

Component	Required Files	Recommended or Minimum Hardware Requirements	Hardware Used in this Build	Recommended or Minimum Operating System or Other Software	Operating System or Other Software Used in this Build
Entitlement Manager for SharePoint Server	SharePointEnforcer-2013-64-7.1.3.0-7-201410101427.zip			<ul style="list-style-type: none"> • Microsoft Office SharePoint Server 2007 on <ul style="list-style-type: none"> - Windows Server 2003, Enterprise Edition, 32-bit, Service Pack 2, or - Windows Server 2008, Enterprise Edition, 64-bit, R2 • Microsoft Office SharePoint Server 2010 on <ul style="list-style-type: none"> - Windows Server 2008, Enterprise Edition, 64-bit, R2 • Microsoft SharePoint Server 2013 on <ul style="list-style-type: none"> - Windows Server 2008, Enterprise Edition, 64-bit, R2 	Microsoft SharePoint Server 2013 on Windows Server 2012

3513

3514 **7.3 Installation and Configuration of NextLabs Control Center (on the SQL**
3515 **Server)**

3516 **7.3.1 Installation and Configuration**

3517 ***7.3.1.1 Install the Microsoft SQL Server via Microsoft SQLServer 2012***

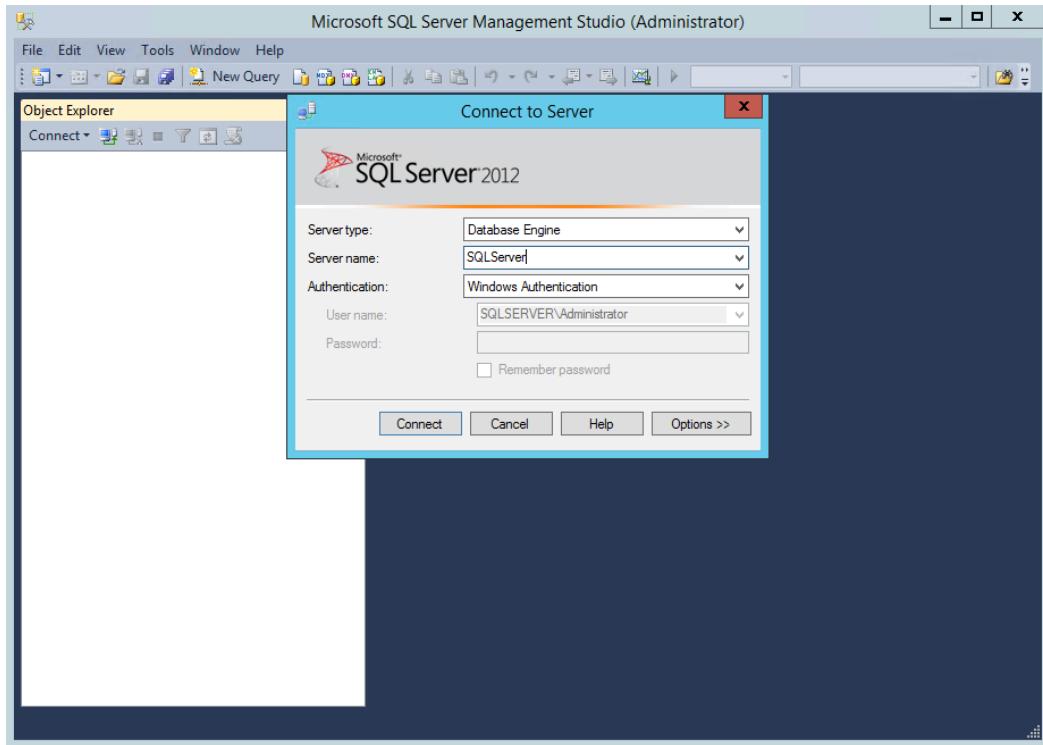
3518 Instructions available at the Microsoft SQLServer site: [https://technet.microsoft.com/en-us/library/hh231622\(v=sql.110\).aspx](https://technet.microsoft.com/en-us/library/hh231622(v=sql.110).aspx).

3520 Notes:

- 3521 1. Regarding installation of Microsoft SQLServer 2012: if you already completed the [Section 4](#),
3522 “Installing and Configuring Microsoft SharePoint Server and Related Components,” this step will
3523 already have been completed.
- 3524 2. Regarding having a database dedicated to NextLabs: NextLabs recommends that for anything but
3525 a demo or testing environment, you should use a database running on its own dedicated server
3526 to store all system data, rather than rely on Control Center’s internal database. A dedicated
3527 database server is strongly recommended because policy enforcement data accumulates quickly
3528 and can reach a significant volume. The problem is not necessarily storage space, but the
3529 performance drag on other processes caused by database queries of large amounts of data.

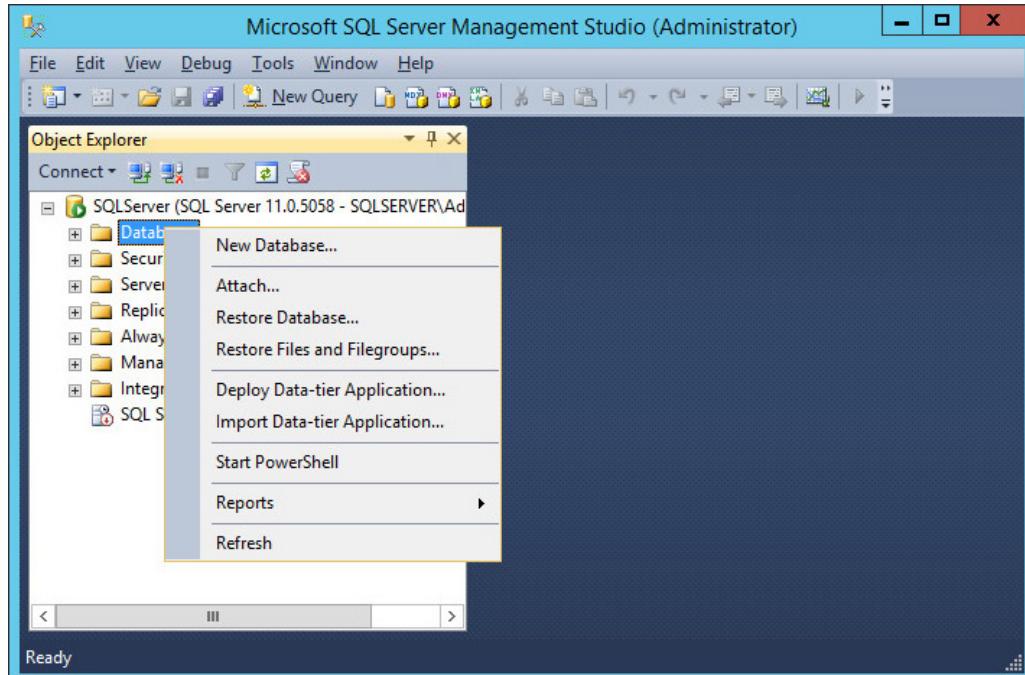
3530 ***7.3.1.2 Create a New Database and Database User for the NextLabs Control Center***
3531 ***Installation and Administration***

- 3532 1. Open Microsoft SQL Server Management Studio and login to Microsoft SQL Server.



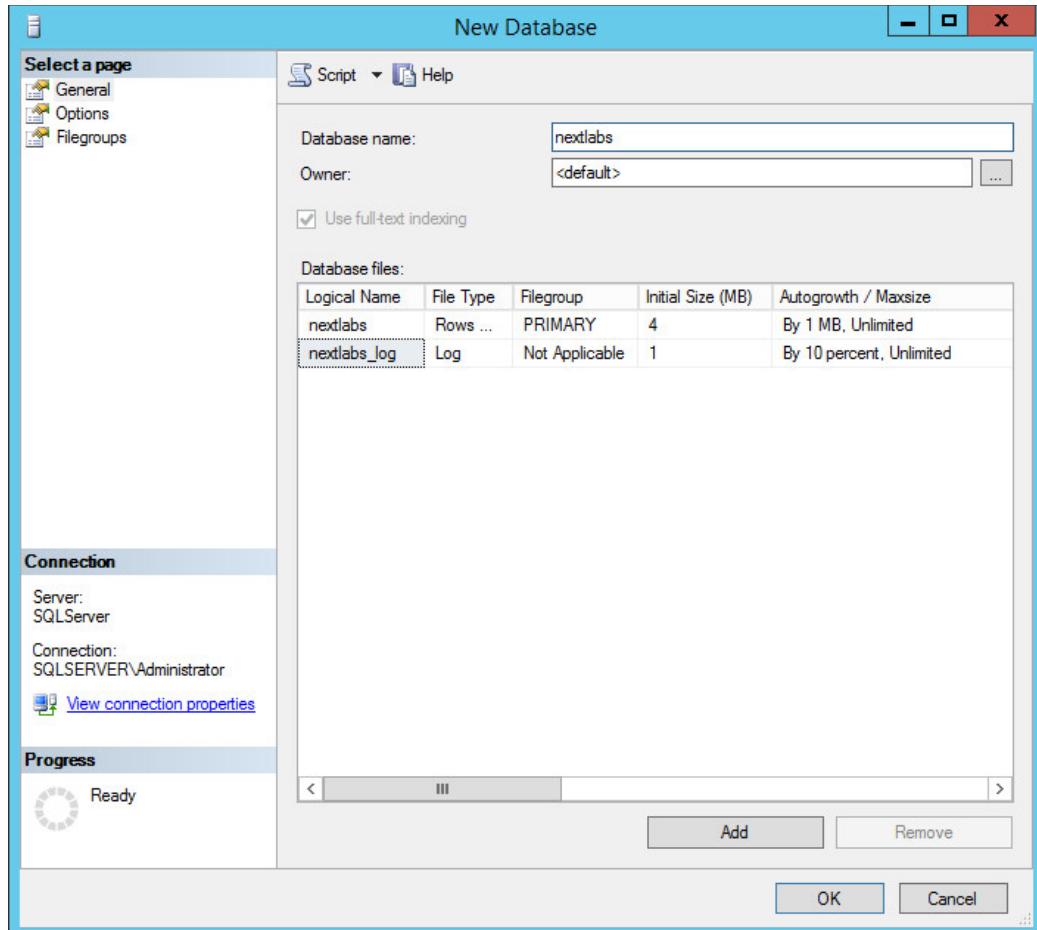
3533

- 3534 2. Right-click on **Databases**, left-click on **New Database**.



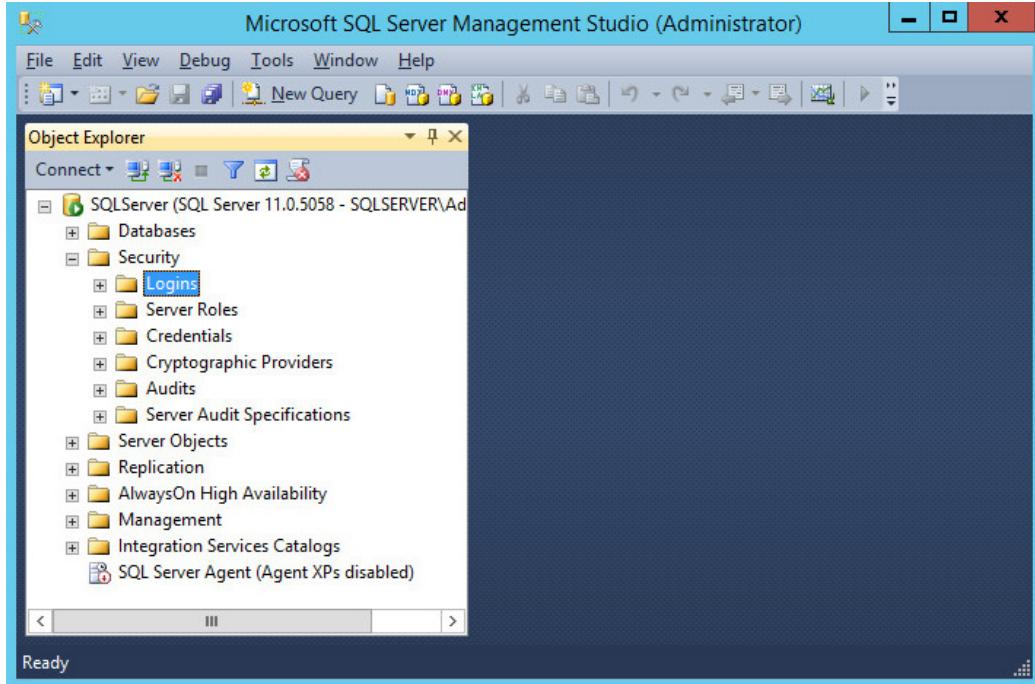
3535

- 3536 3. In the New Database window, specify a **Database name** that works for you. The application
3537 automatically copies this into the **Logical Names** of the **Database files**. Click **OK**. Example name
3538 from this build: **nextlabs**



3539

- 3540 4. Click on the menu box next to **Security** to begin the process for creating a new login for the new
3541 NextLabs database's administrator.

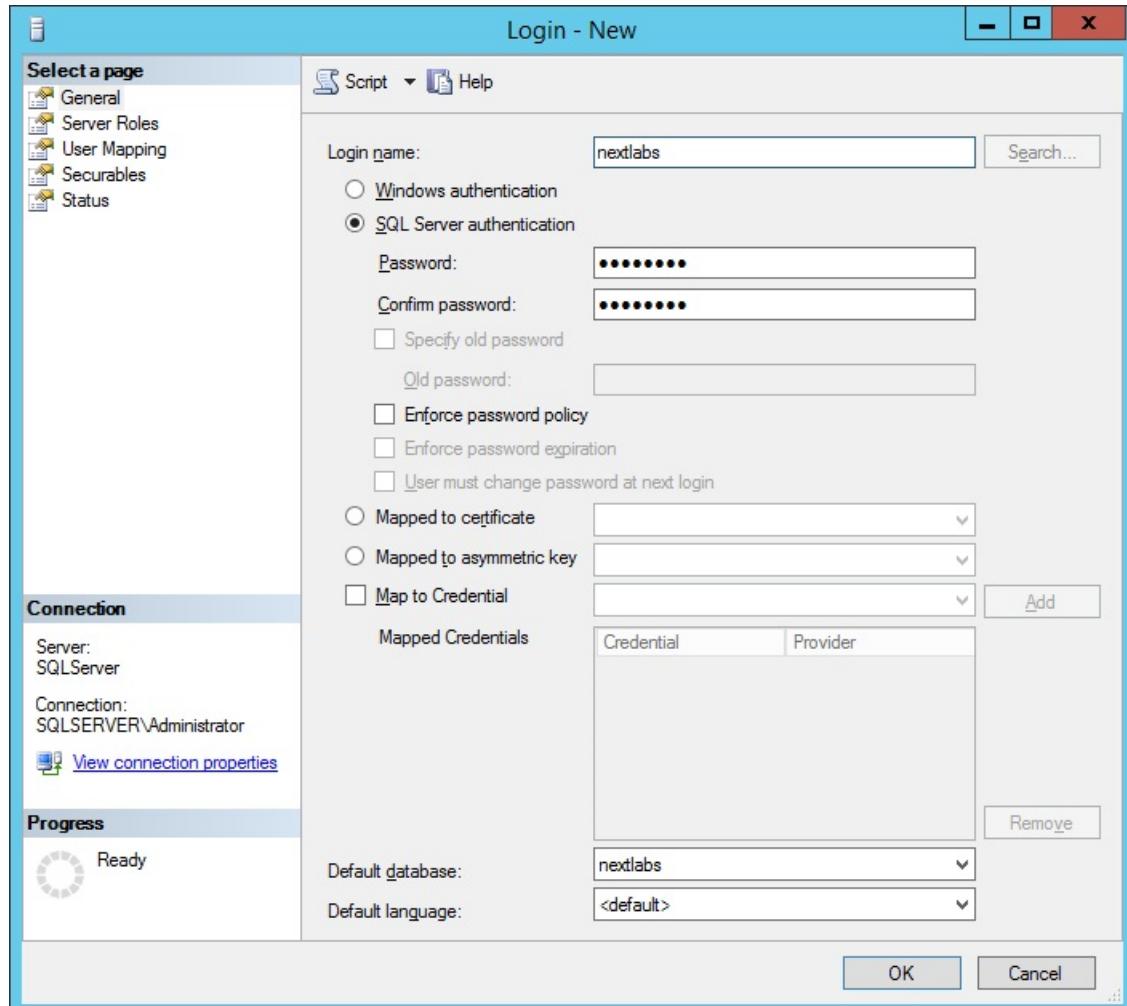


3542

3543 5. Right-click **Logins**. Left-click **New Login**.

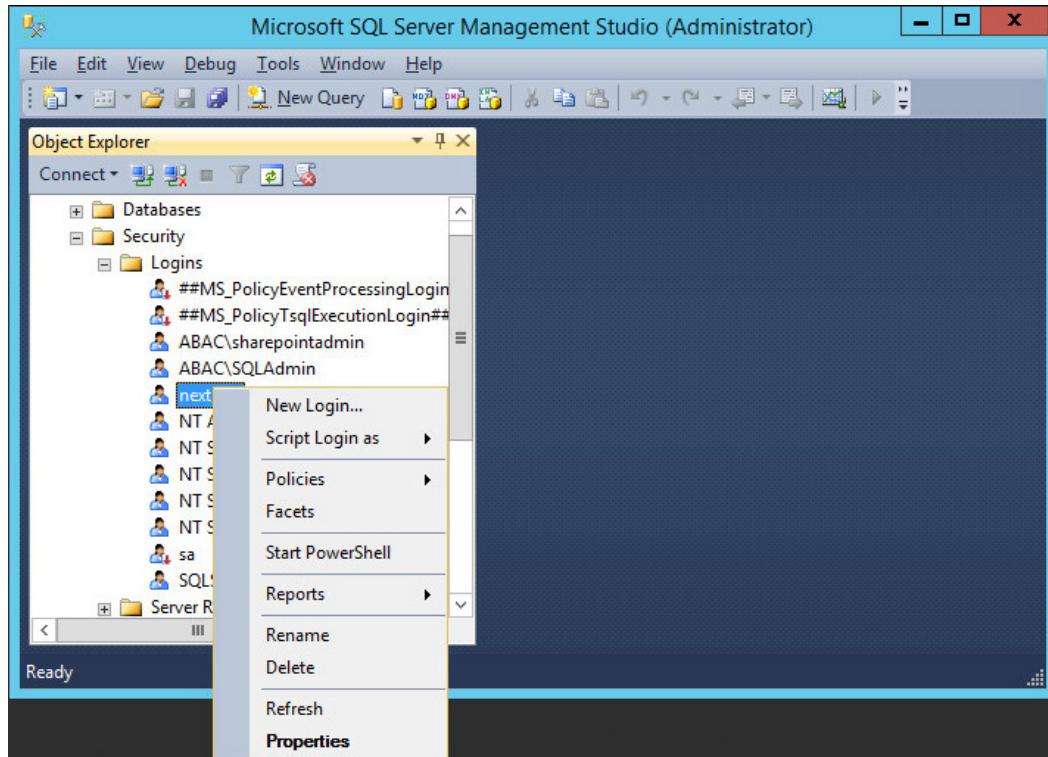
3544

6. Click on **SQL Server authentication**, and enter a new **Login name** and **Password**.



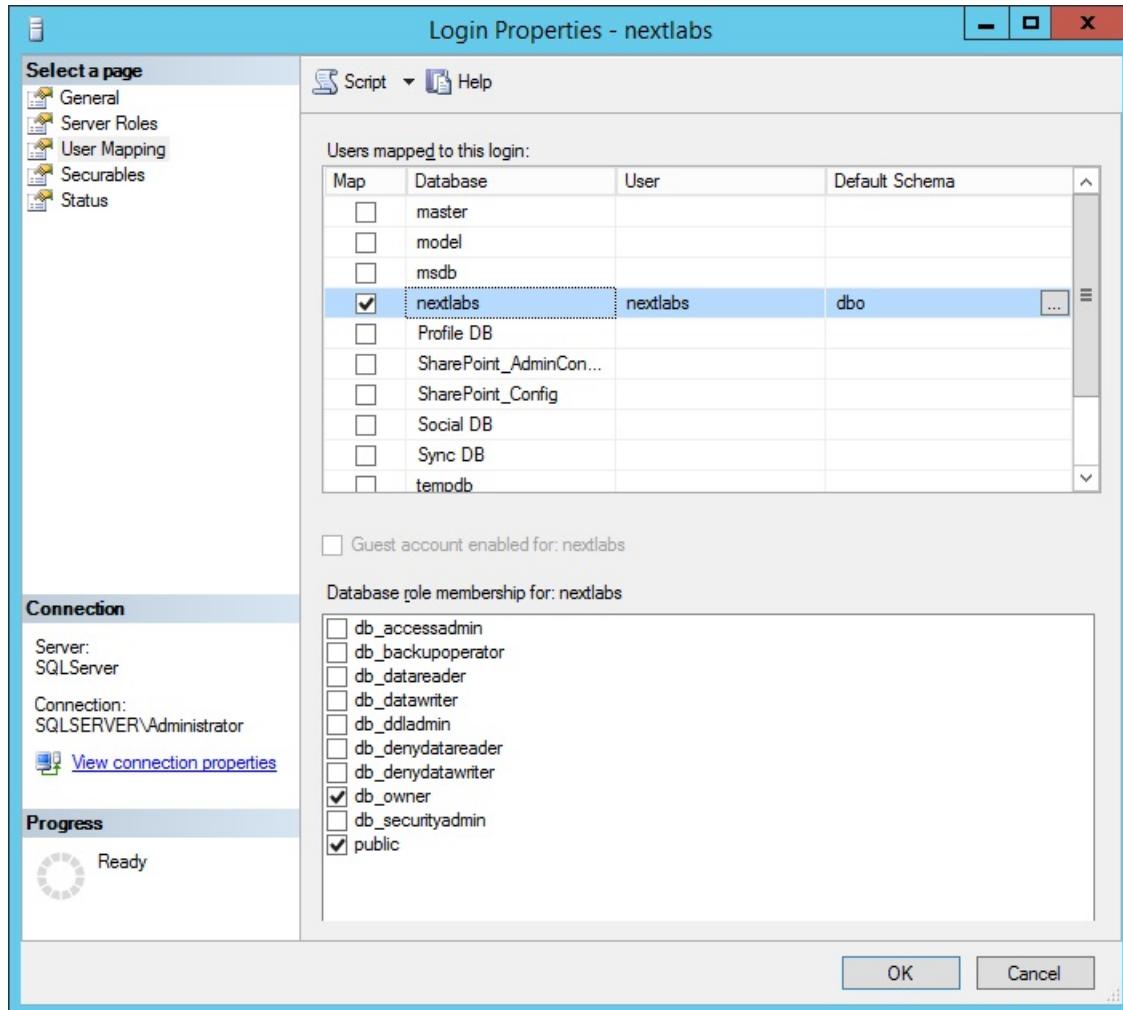
3545

- 3546 7. Click the menu box next to **Logins**. Right-click on the new user created in the previous step. Click
3547 **Properties**.



3548

- 3549 8. Click on **User Mapping**, then **New Database**. Under **Database role membership** for:
3550 [**database_name**], check the box next to **db_owner**.



3551

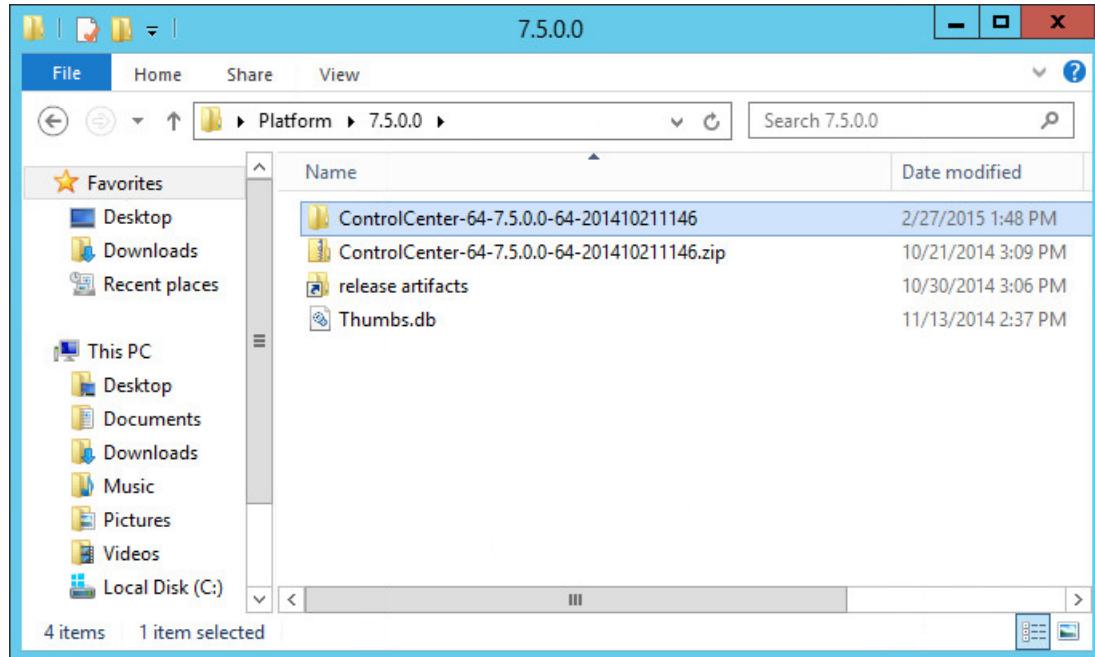
3552 7.3.1.3 Install and Configure the NextLabs Control Center

3553 Complete standard Control Center installation per NextLabs documentation available to customers,
3554 using the following steps:

- 3555 1. Go to your Desktop or other known location where the required NextLabs Control Center
3556 installation files are stored. Example:
3557 **C:\Users\Administrator\Desktop\NextLabs\Platform\7.5.0.0**
- 3558 Note the location of the required license.dat file which will be needed later; example:
3559 **C:\Users\Administrator\Desktop\NextLabs\Platform\License\license.dat**
- 3560 2. Right-click on **ControlCenter-64-7.5.0.0-64-201410211146.zip** and select **Extract All** from the
3561 floating menu. Wait for the files to be extracted.
- 3562 3. Double-click to open the **ControlCenter-64-7.5.0.0-64-201410211146** folder.

SECOND DRAFT

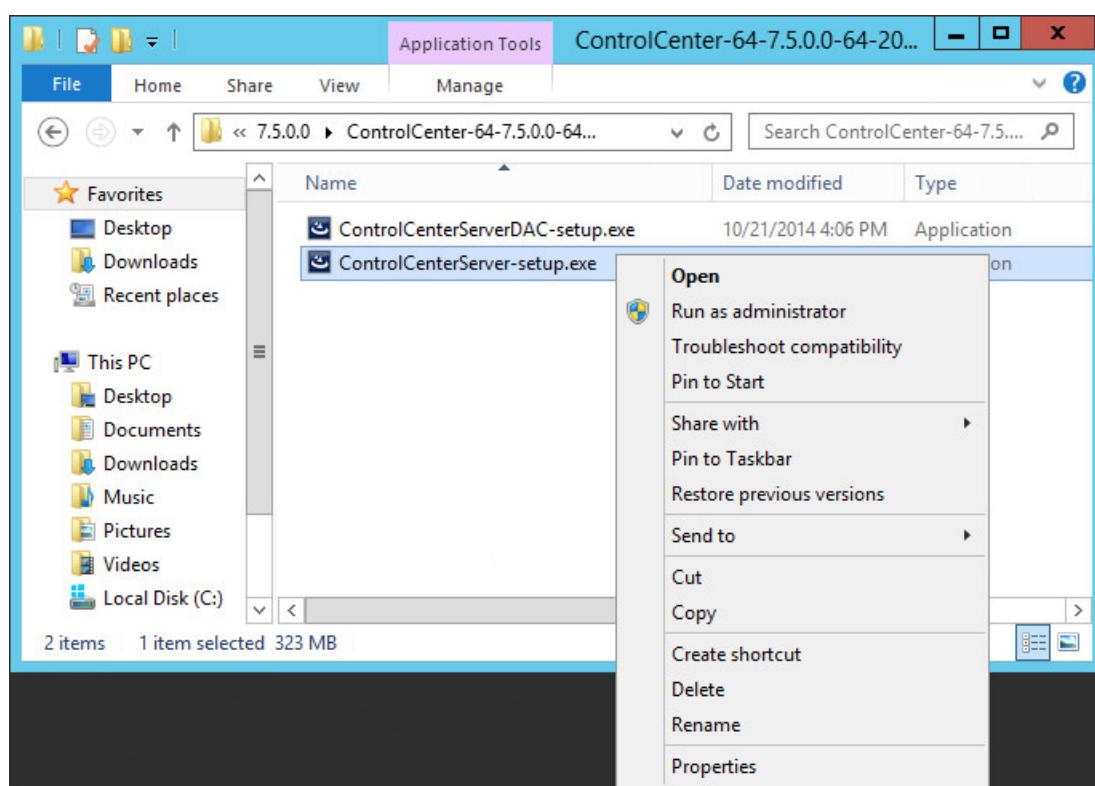
3563



3564

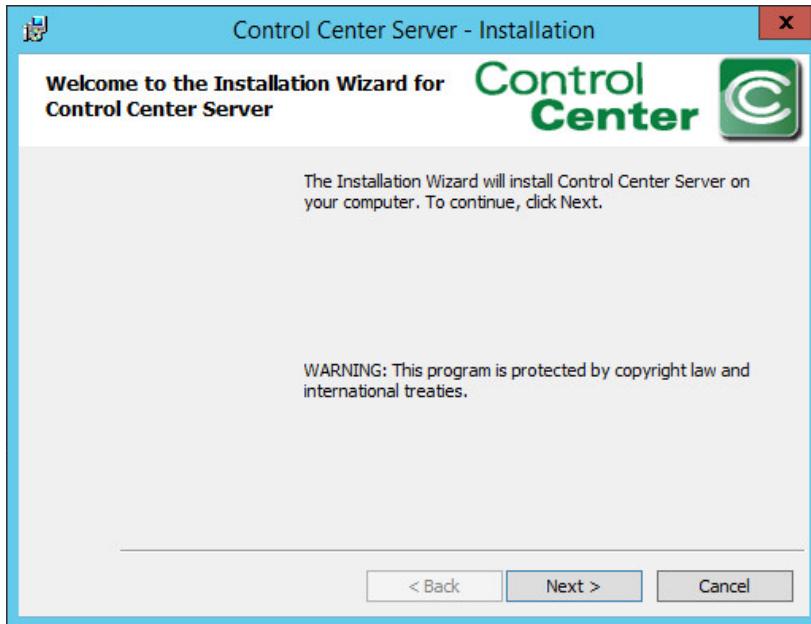
4. Right-click on **ControlCenterServer-setup.exe**, and select **Run as administrator**.

3565



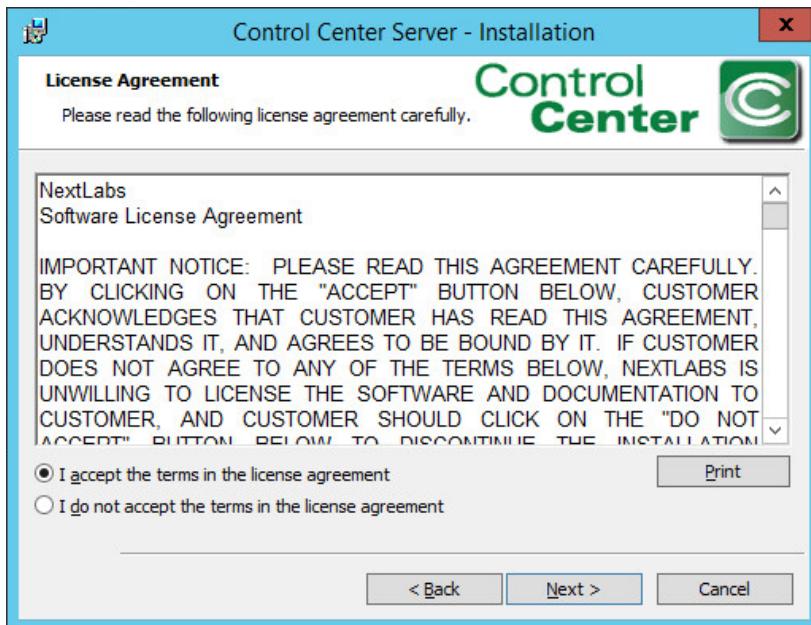
3566

5. Click **Next**.



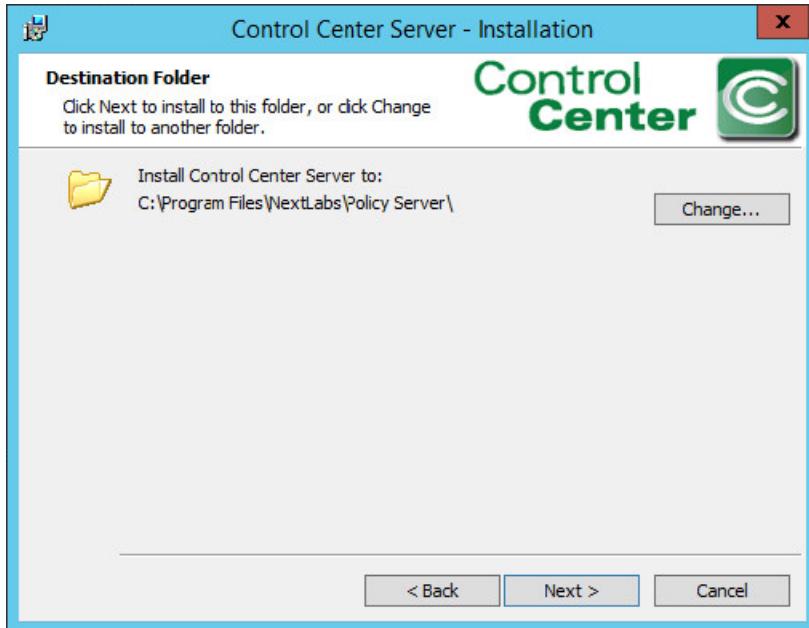
3567

- 3568 6. Select **I accept the terms in the license agreement**, then click **Next**.



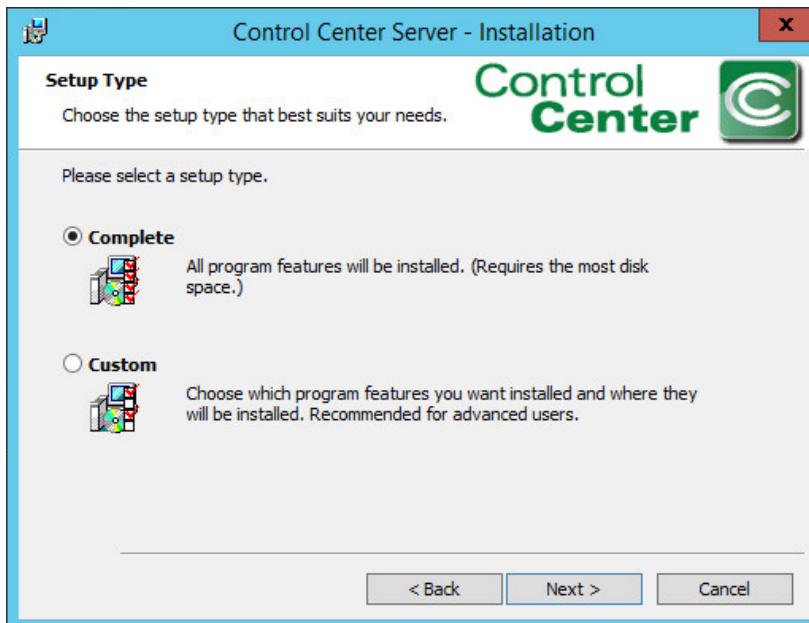
3569

- 3570 7. Click **Next**.



3571

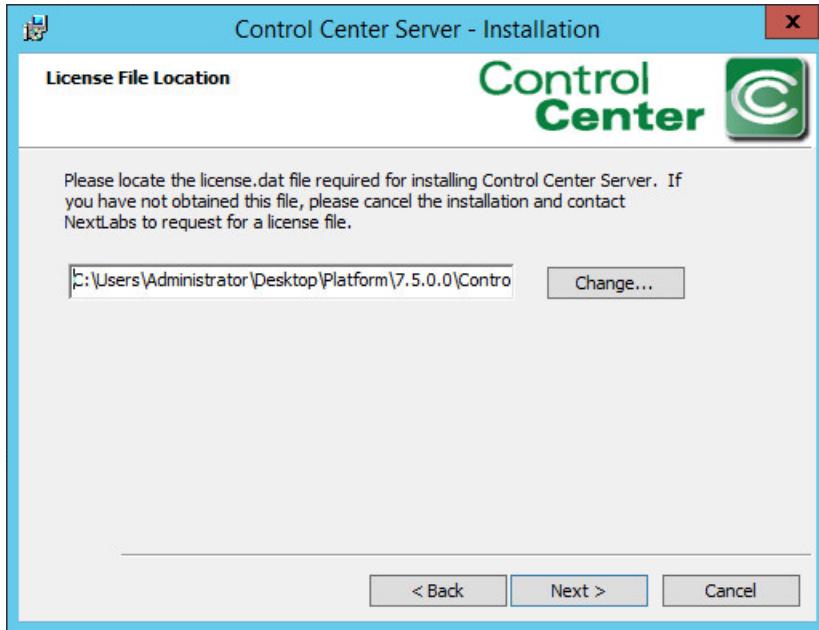
- 3572 8. Select the **Complete** setup type. Then, click **Next**.



3573

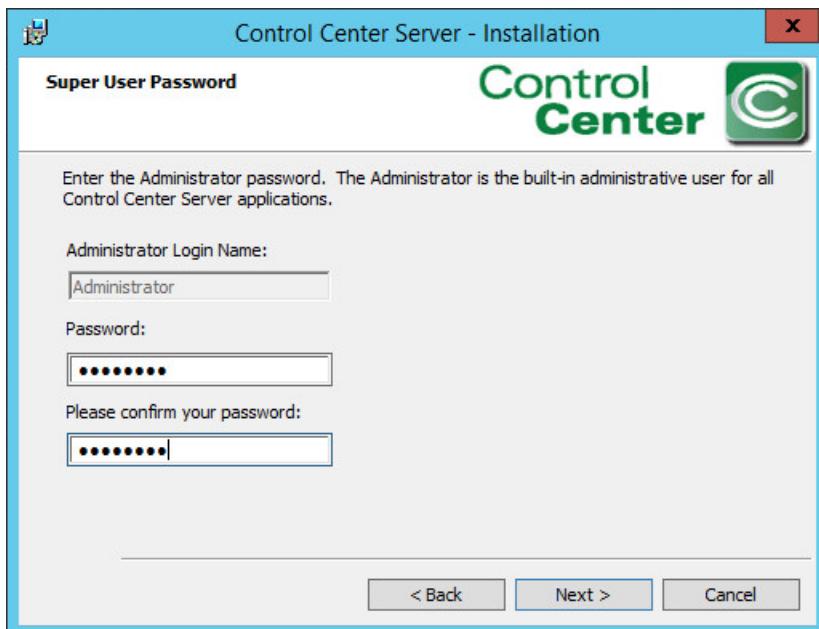
- 3574 9. Enter the location of the license file in the **License File Location** field, or click **Change** to navigate to its location in Windows File Explorer. Click **Next**.

3575
3576 Example location: C:\Users\Administrators\Desktop\Platform\7.5.0.0\ControlCenter-64-7.5.0.0-
3577 64-201410211146\license.dat



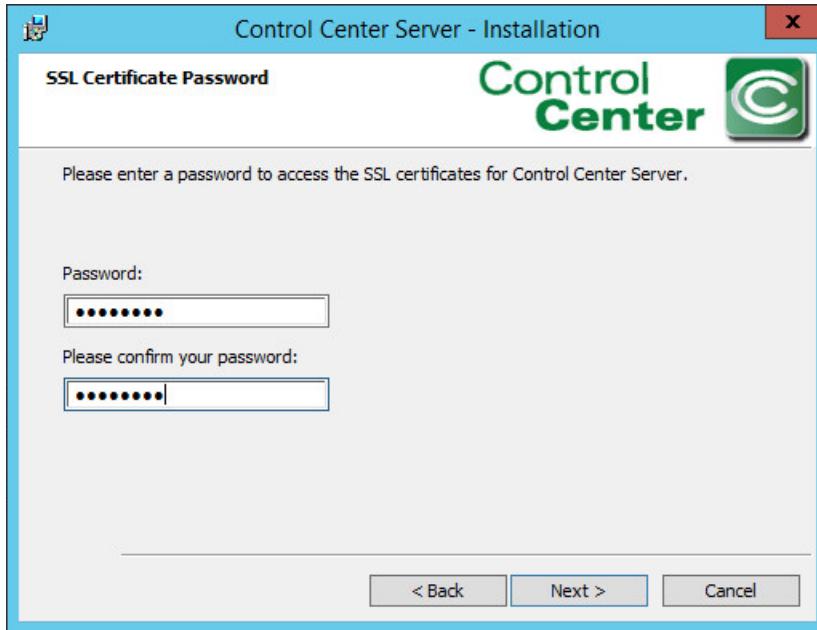
3578

- 3579 10. In the configuration wizard Super User password screen, enter a **Password** for the built-in
3580 administrative user for all Control Center Server applications. Click **Next**.



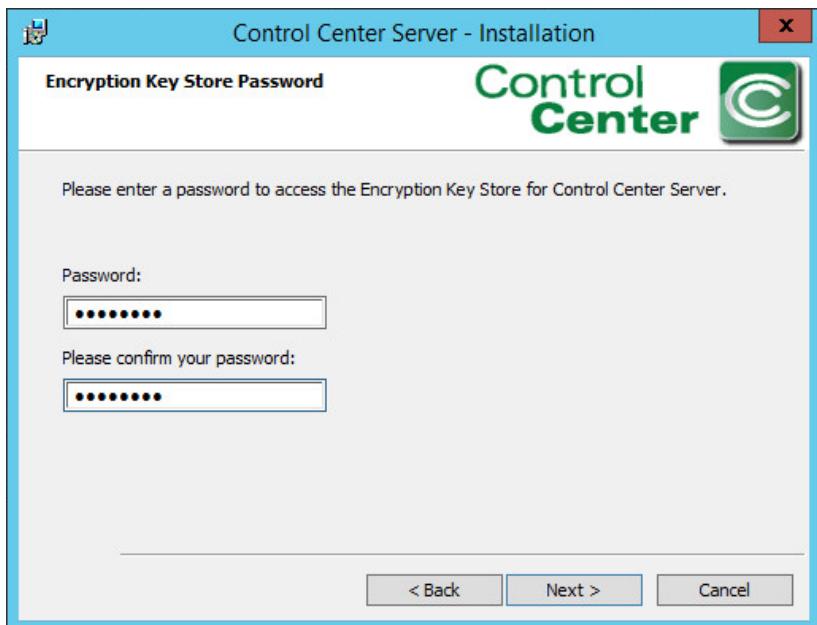
3581

- 3582 11. At the SSL Certificate Password screen, enter a **Password** to access the SSL certificates for the
3583 Control Center Server. Click **Next**.



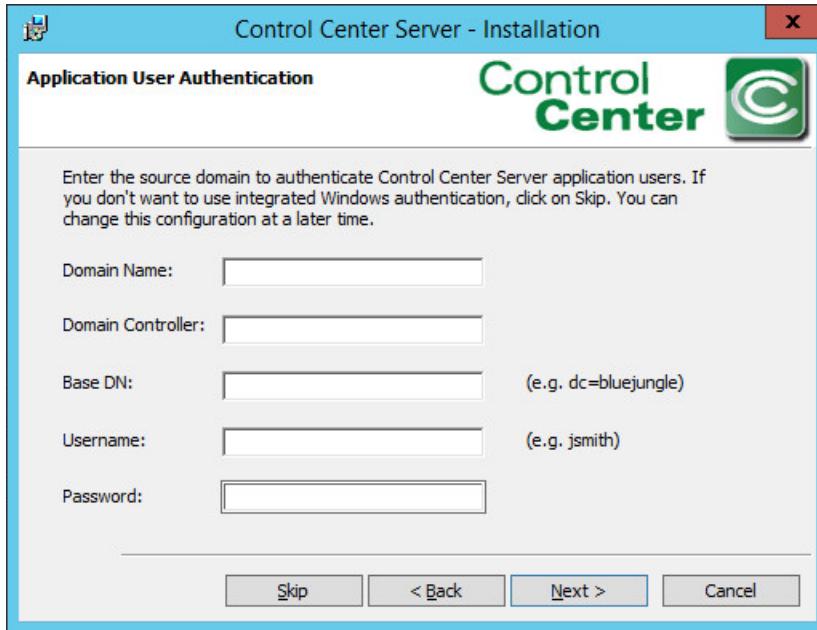
3584

- 3585 12. At the Encryption Key Store Password screen, enter a **Password** to access the Encryption Key
3586 Store for the Control Center Server. Click **Next**.



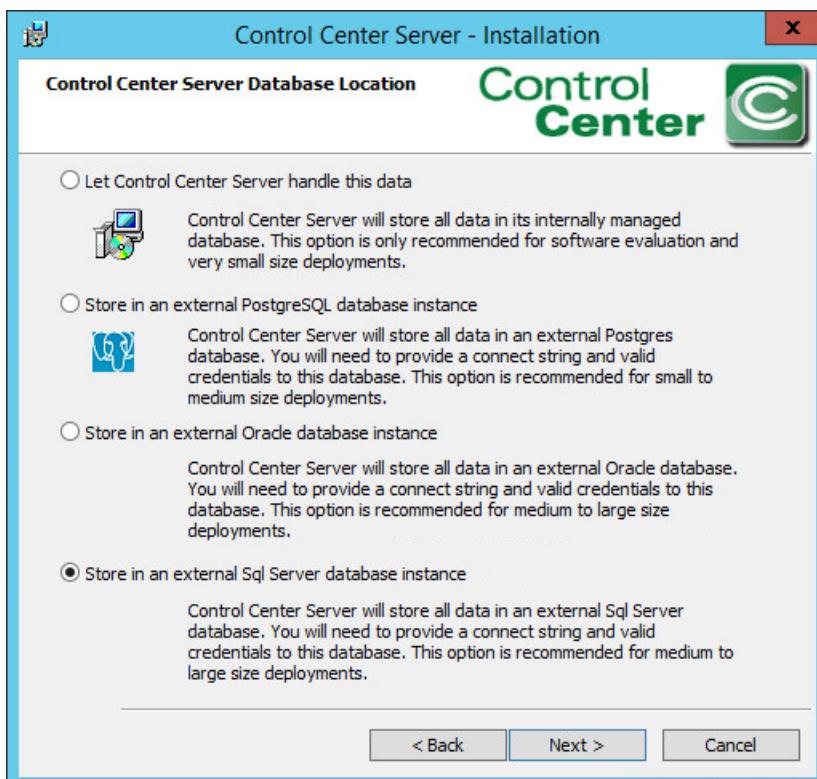
3587

- 3588 13. At the Application User Authentication screen, click **Skip**.



3589

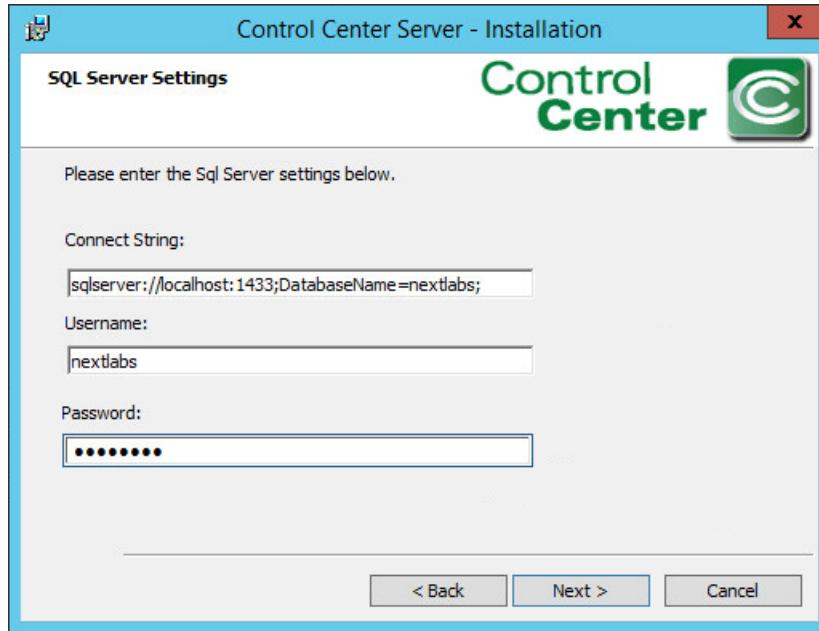
- 3590 14. At the Control Center Server Database Location screen, select Store in an external **Sql Server**
3591 **database instance**. Click **Next**.



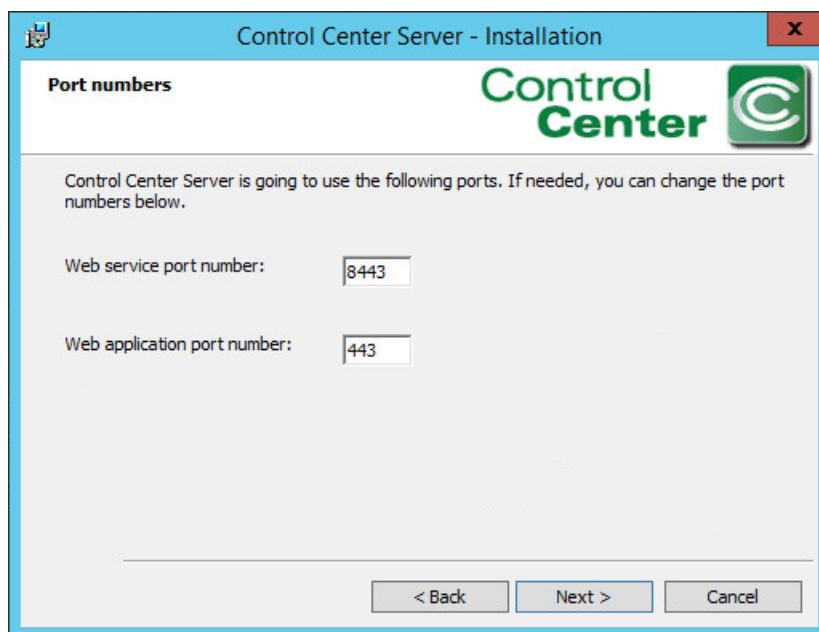
3592

- 3593 15. At the SQL Server Settings screen, do the following:
3594 a. Specify the **Connect String**, including the name of the new SQL database created.
3595 Example: **nextlabs**

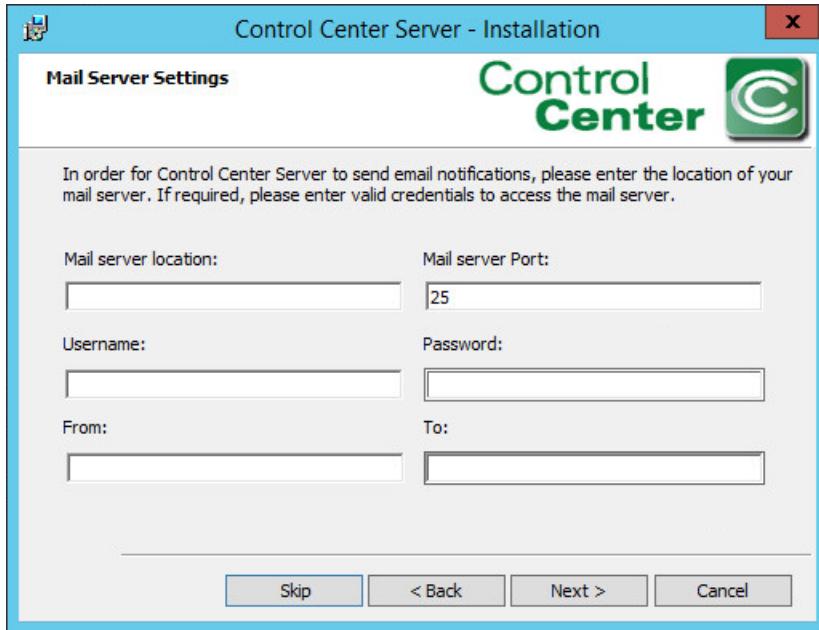
- 3596 b. Specify **Username** (non-Super User) and **Password**.
3597 c. Click **Next**. Note: If the error **Connection to the SQL database could not be established properly** appears, it may help to restart the SQL Server.
3598



- 3599
3600 16. At the Port numbers window, the default port numbers are already entered: Web service port number: 8443, Web application port number: 443. Click **Next**.
3601

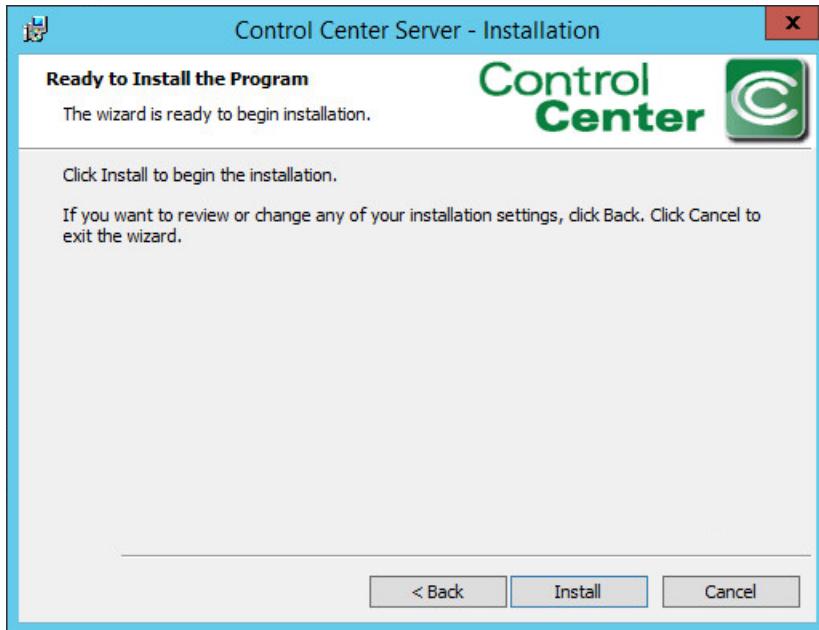


- 3602
3603 17. At the Mail Server Settings screen, click **Skip**.



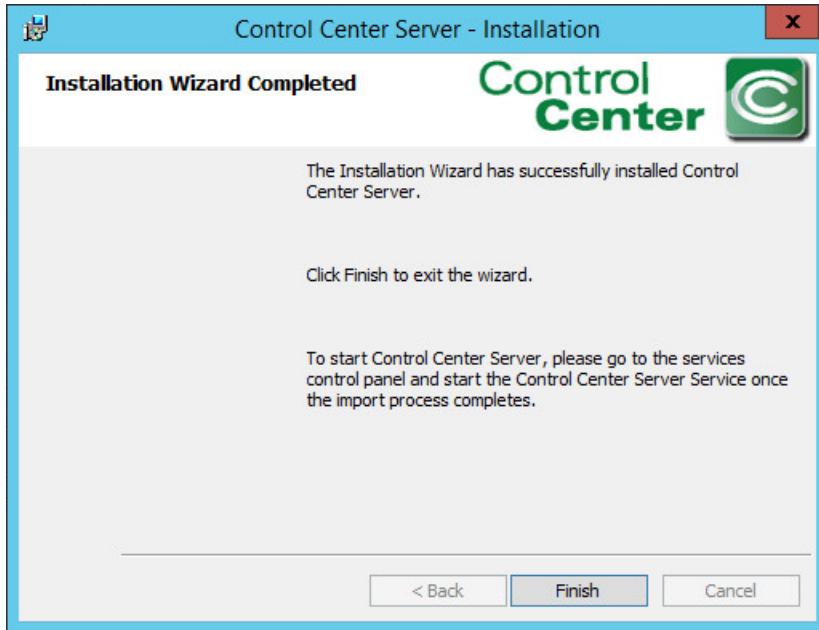
3604

3605 18. At the Ready to Install the Program screen, click **Install**.



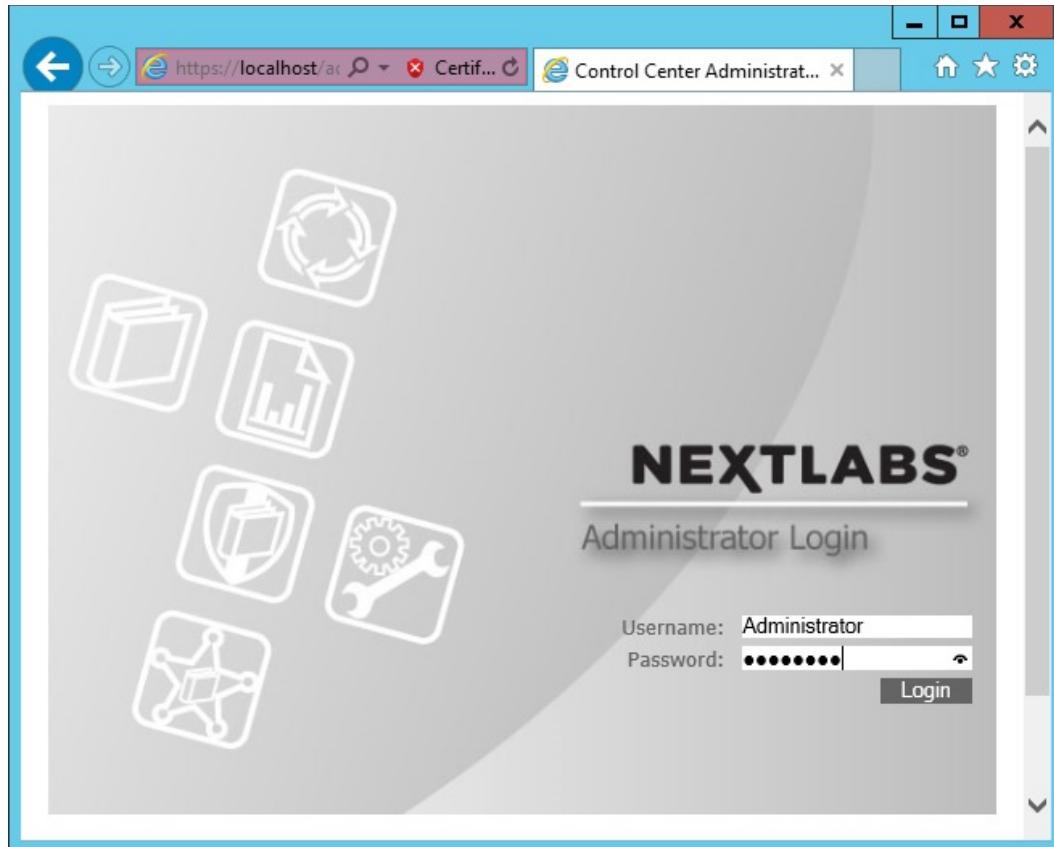
3606

3607 19. At the Installation Wizard Completed screen, click **Finish**.



3608

- 3609 20. Open an Internet browser and navigate to the following URL: <https://localhost/administrator> to
3610 login to the Control Center Administrator web application.
- 3611 a. If a security certificate warning comes up, click **Continue to this website**.
- 3612 b. Enter the Administrator (Super User) **Username** and **Password**.
- 3613 c. Click **Login**.



3614

3615 21. Once logged into the Control Center Administrator web application in your browser, you can
 3616 verify that the NextLabs Control Center is installed and configured correctly on the SQL Server,
 3617 and view the following information:

3618 a. Fully qualified domain name (FQDN) of the server hosting the NextLabs Control Center.

3619 Example: **SQLServer.ABAC.TEST**

3620 b. Services running on the host server, including but not limited to:

3621 i. Intelligence Server

3622 ii. Dynamic Access Control

3623 iii. Key Management Server

3624 iv. Management Server

3625 v. Policy Management Server

3626 For more information about these or other services running continuously via NextLabs
 3627 Control Center on the SQL Server, please refer to NextLabs support documentation.

3628 c. Port via which the above services are running. Example: 8443, default for web services

3629 d. For each of the listed services, the default heartbeat period is 60 minutes, and can be
 3630 modified via the Administrator (See step 23).

Status Overview

System Status		Server Status				
Policy Enforcer Status (Last 24 Hours)		Server	Type	Host	Port	Last Heartbeat
Policy enforcers not connecting	0	SQLSERVER.ABAC.TEST_dac	Intelligence Server	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:27 AM
Policy consistency	0	SQLSERVER.ABAC.TEST_ddac	Dynamic Access Control	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:27 AM
System Statistics		SQLSERVER.ABAC.TEST_dkms	Key Management Server	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:27 AM
Policy Enforcers		SQLSERVER.ABAC.TEST_dem	Enrollment Manager	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:17 AM
Desktop Enforcers Registered	0	SQLSERVER.ABAC.TEST_dabs	ICENet Server	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:35:15 AM
Portal Enforcers Registered	1	SQLSERVER.ABAC.TEST_dms	Management Server	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:35:02 AM
Active Directories Registered	0	SQLSERVER.ABAC.TEST_dpms	Policy Management	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:52 AM
File Server Enforcers Registered	0					

3631

- 3632 22. Click on the **Policy Enforcer Configuration** tab. The default Profile to open is the **Desktop Enforcer Portal**, with the **Settings** sub-tab defaulted also open. To change the heartbeat frequency for testing or debugging purposes, edit the **Heartbeat Frequency** field (minimum time is 1 minute). Click **Save**.
- 3633
- 3634
- 3635

Desktop Enforcer Default Profile

Settings

Title:	Desktop Enforcer Defal
ICENet Server:	https://SQLSERVER.ABAC.TEST:8443/dabs - or - <input type="text"/>
Heartbeat Frequency:	1 hours
Audit Log Upload Frequency:	30 seconds
Max Log Size:	2 MB
Enable Push:	<input type="checkbox"/> Default Port: 2000
Administrative Password:	<input type="password"/>
Confirm Password:	<input type="password"/>

Hosts

©2009-2014 NextLabs, Inc. All rights Reserved.

3636

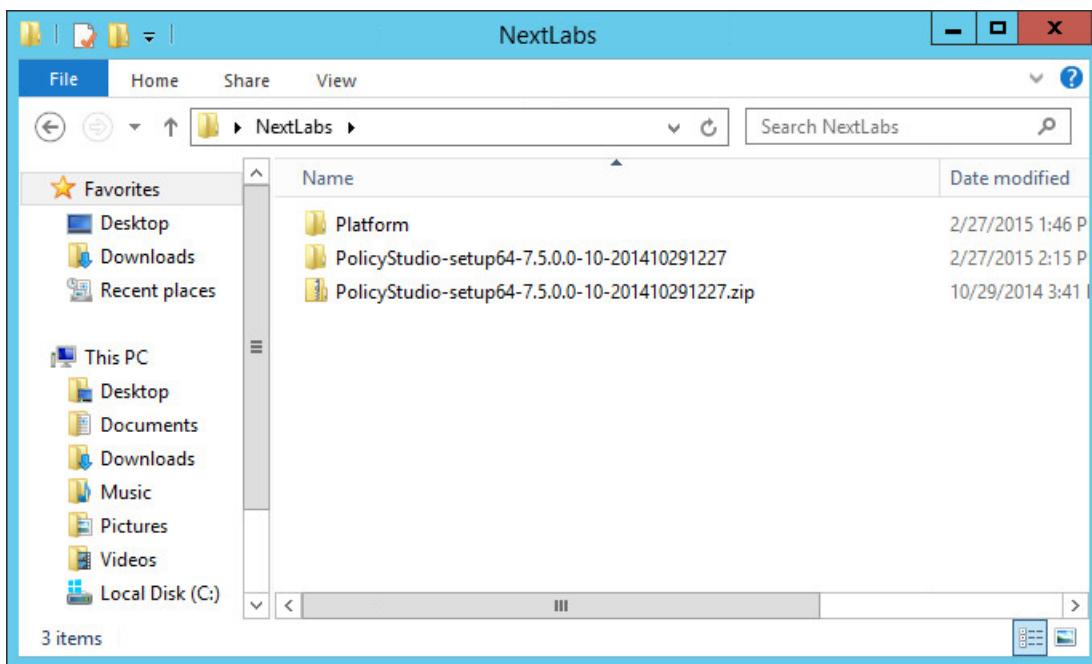
3637 **7.4 Installation and Configuration of NextLabs Policy Studio: Enterprise**
3638 **Edition (PAP)**

3639 **7.4.1 Installation**

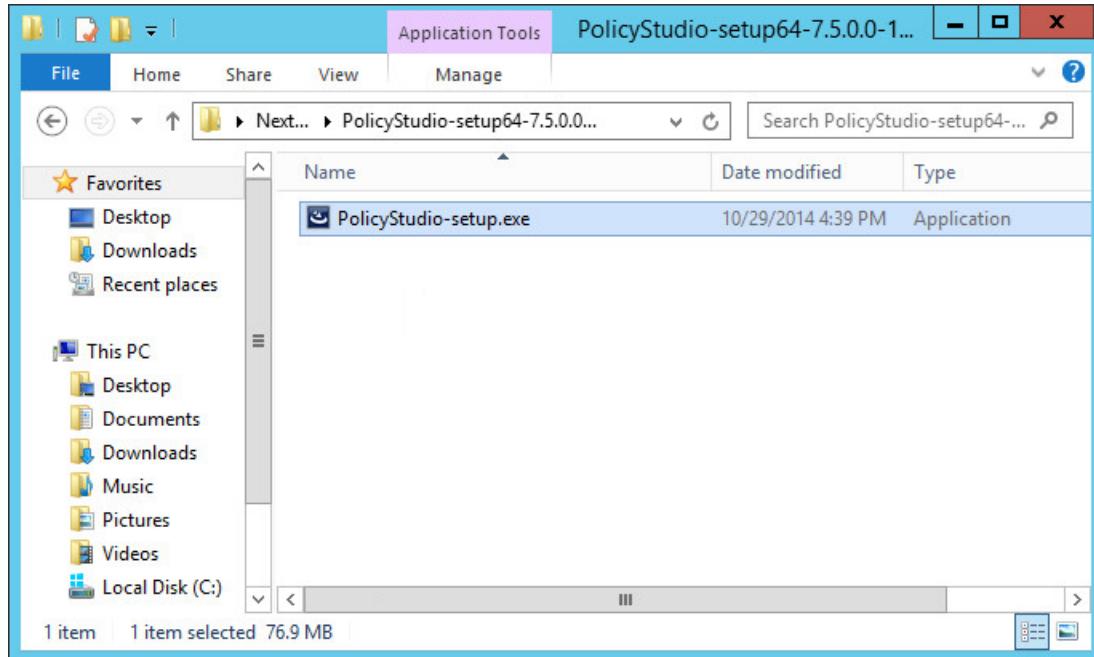
3640 Complete the standard Policy Studio installation per NextLabs documentation available to customers
3641 using the following steps:

- 3642 1. On the SQLServer, go to your Desktop or other known location where the required NextLabs
3643 Policy Studio installation files are stored. Example: *C:\Users\Administrator\Desktop\NextLabs*

3644 2. Right-click on **PolicyStudio-setup64-7.5.0.0-10-201410291227.zip** and select **Extract All**. Wait
3645 for files to be extracted.

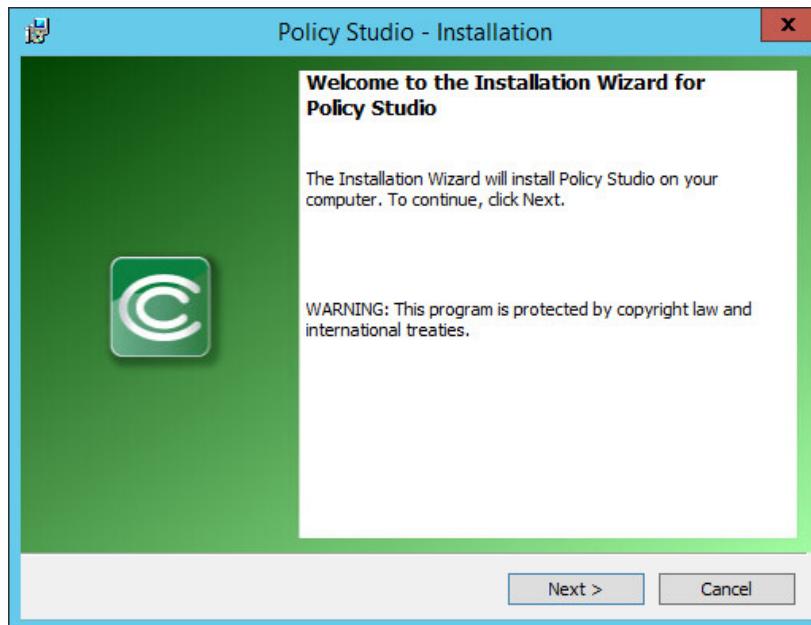


- 3646
3647 3. Double-click to open the **PolicyStudio-setup64-7.5.0.0-10-201410291227** folder.
3648 4. Right-click on **PolicyStudio-setup.exe** and select Run as **Administrator**.



3649

- 3650 5. At the Welcome to the Installation Wizard for Policy Studio screen of the Policy Studio
3651 Installation Window, click **Next**.



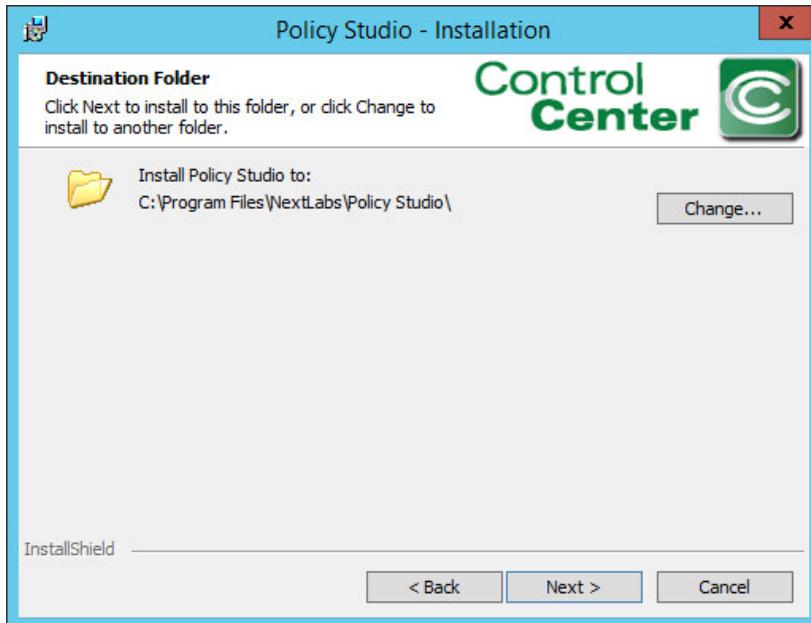
3652

- 3653 6. At the License Agreement screen, select **I accept the terms in the license agreement**, and click
3654 Next.



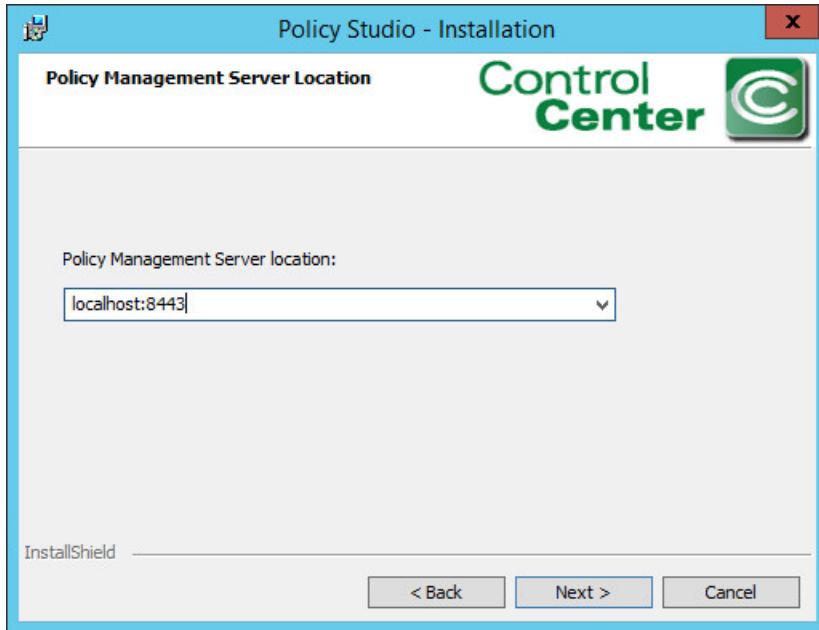
3655

- 3656 7. At the Destination Folder screen, click **Next**.



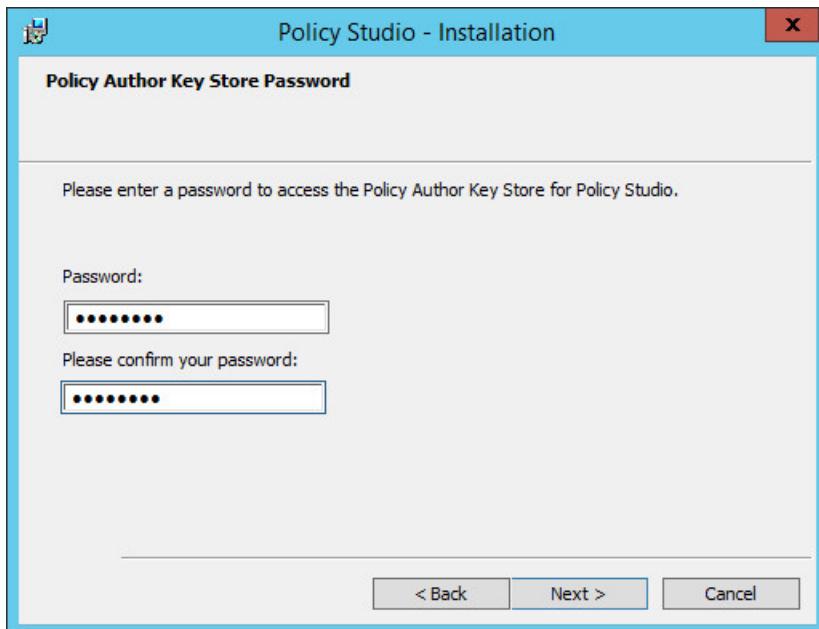
3657

- 3658 8. At the Policy Management Server Location screen, enter the default location **localhost:8443**.
3659 Click **Next**.



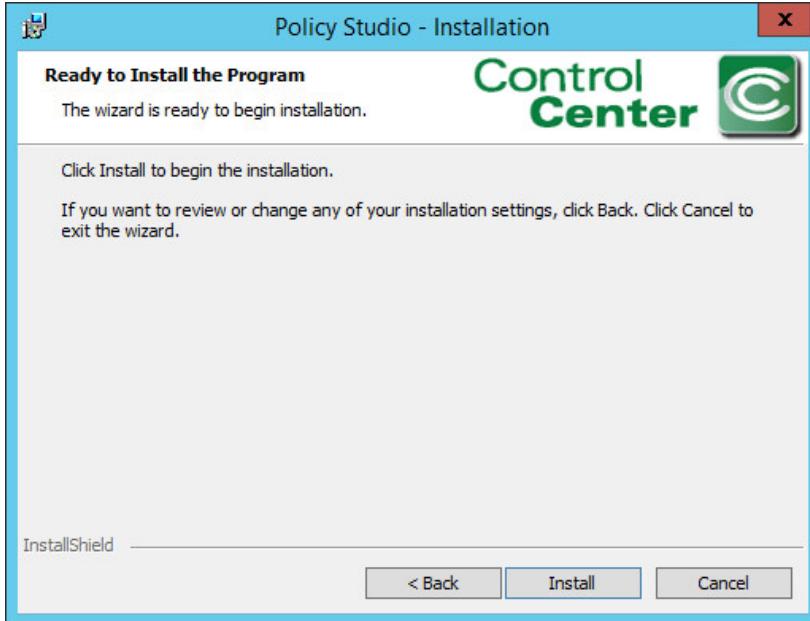
3660

- 3661 9. At the Policy Author Key Store Password screen, enter a **Password** and click **Next**.



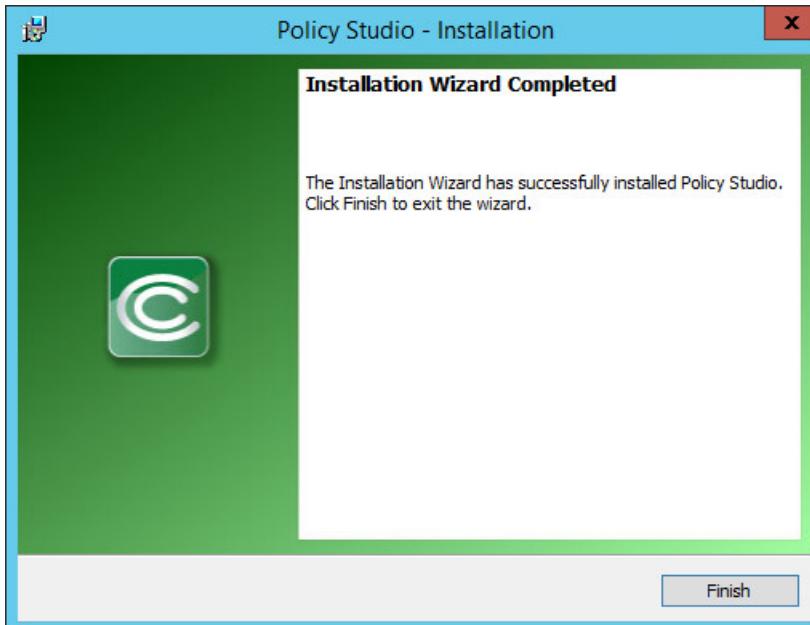
3662

- 3663 10. At the Ready to Install the Program screen, click **Install**.



3664

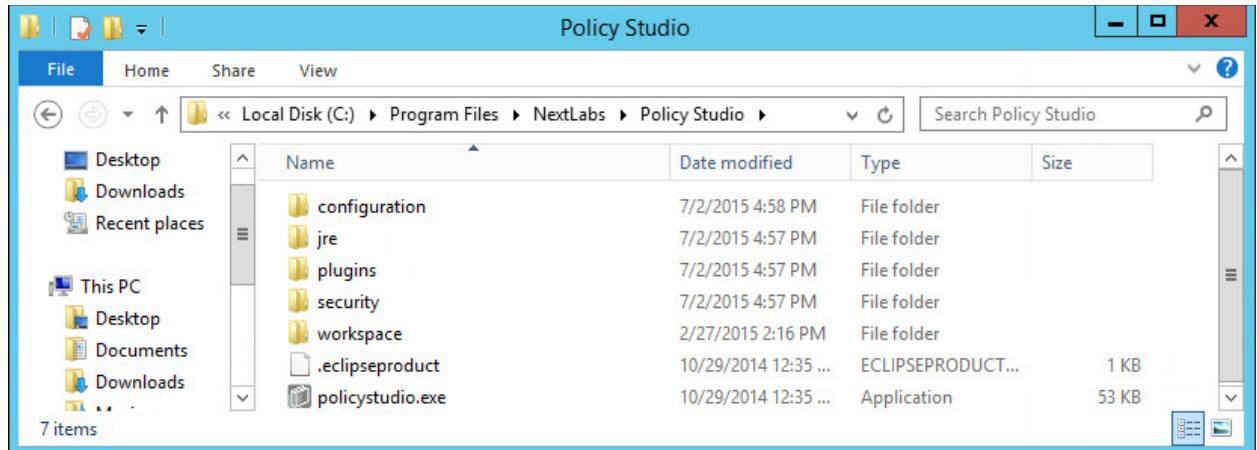
3665 11. At the Installation Wizard Completed screen, click **Finish**.



3666

3667 12. In Windows Explorer, find and open the **policystudio.exe** application file.

- 3668 a. Double-click the **C:/ drive**.
- 3669 b. Double-click **Program Files**.
- 3670 c. Double-click **NextLabs**.
- 3671 d. Double-click **Policy Studio**.
- 3672 e. Double-click **policystudio.exe**.



3673

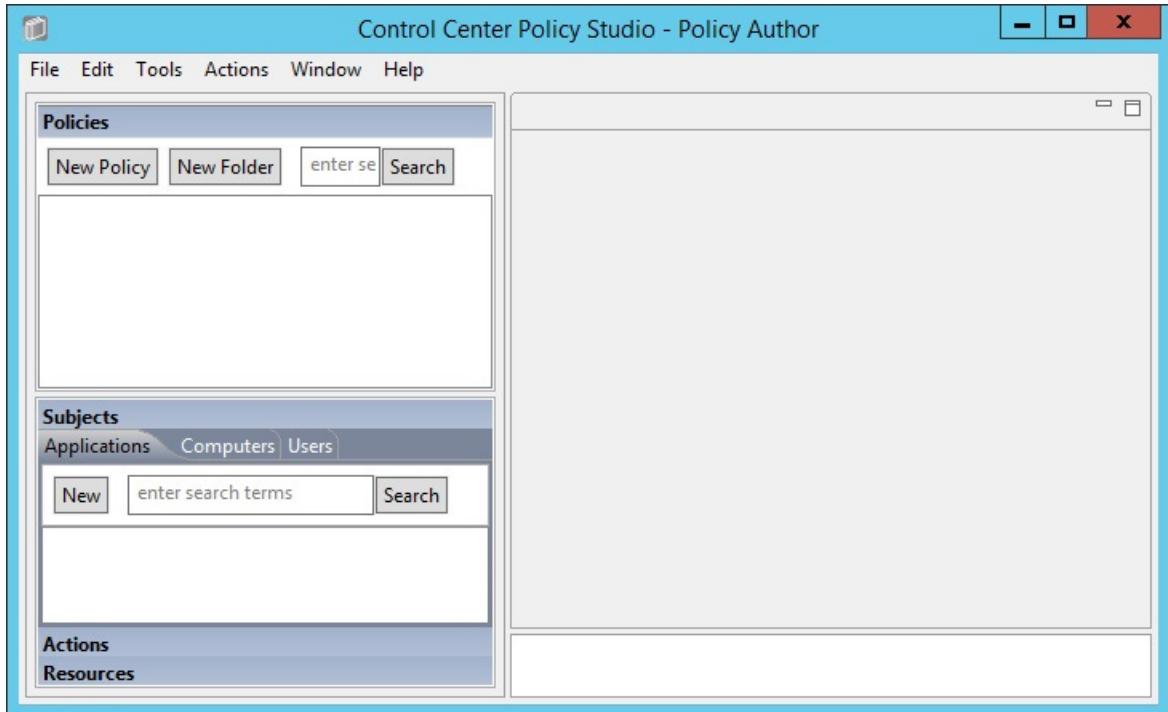
- 3674 13. In the Control Center Policy Studio window, enter a **User Name** and **Password** to connect to the
3675 Policy Management Server



3676

- 3677 14. If the connection is successful, the Control Center Policy Studio - Policy Author window will
3678 open.

- 3679 a. Policies are defined and deployed in this interface, to be covered in [Section 8](#).



3680

3681 7.5 Installation and Configuration of Policy Controller (PDP)

3682 7.5.1 Installation

3683 To complete standard Policy Controller installation per NextLabs documentation available to customers,
3684 use the following steps:

- 3685 1. On the SharePoint Server, go to your Desktop or other known location where the required
3686 NextLabs Policy Controller installation files are stored. Example:
3687 C:\Users\Administrator\Desktop\SharePoint\
- 3688 2. Right-click on **PolicyController-CE-64-7.0.1.0-1-201405191624.zip** and select **Extract All** from
3689 the floating menu. Wait for files to be extracted.
- 3690 3. Double-click on **PolicyController-CE-64-7.0.1.0-1-201405191624** folder to open it.
- 3691 4. Double-click **CE-PolicyController-setup64.msi** to begin installation.
- 3692 5. At the Welcome to the InstallShield Wizard for NextLabs Policy Controller Installation screen,
3693 click **Next**.



3694

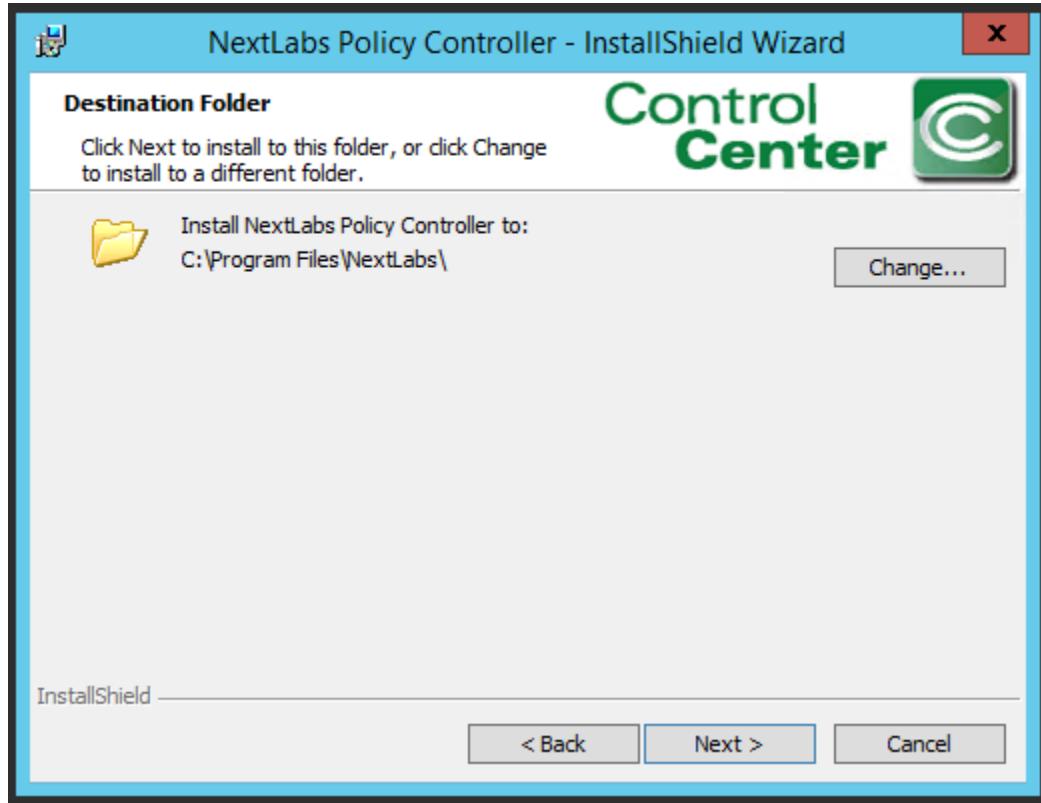
- 3695 6. At the License Agreement screen, select **I accept the terms in the license agreement** and click
3696 **Next**.



3697

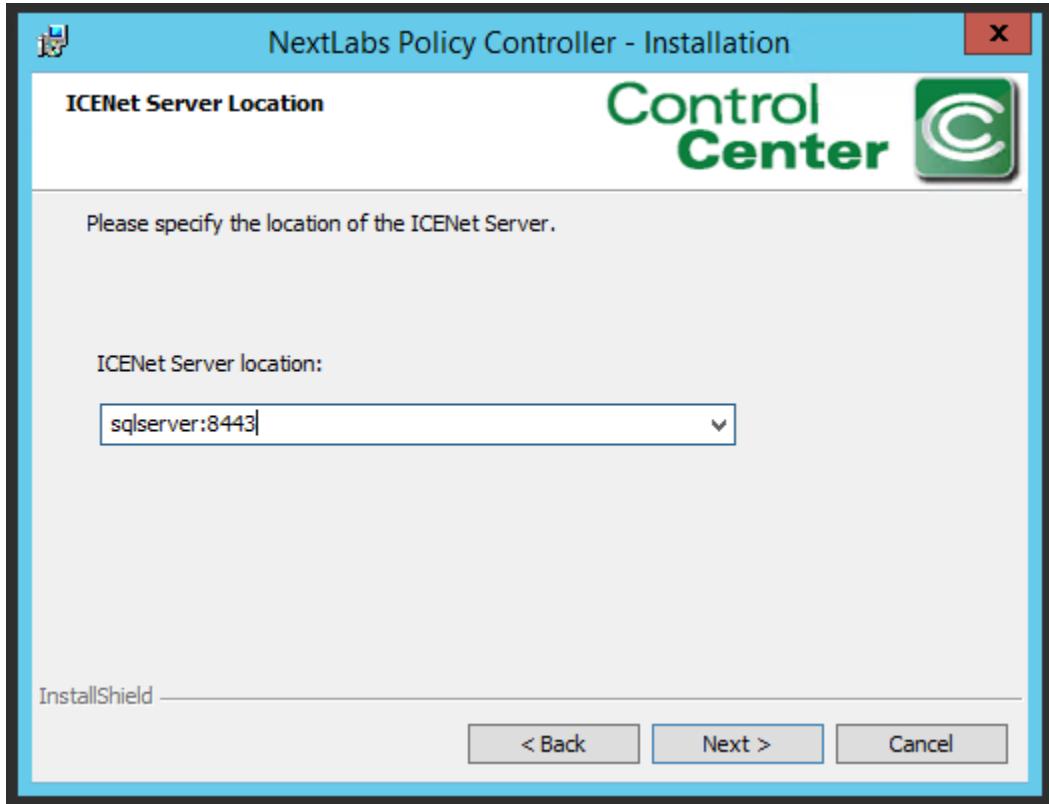
3698

7. At the Destination Folder screen, click **Next**.

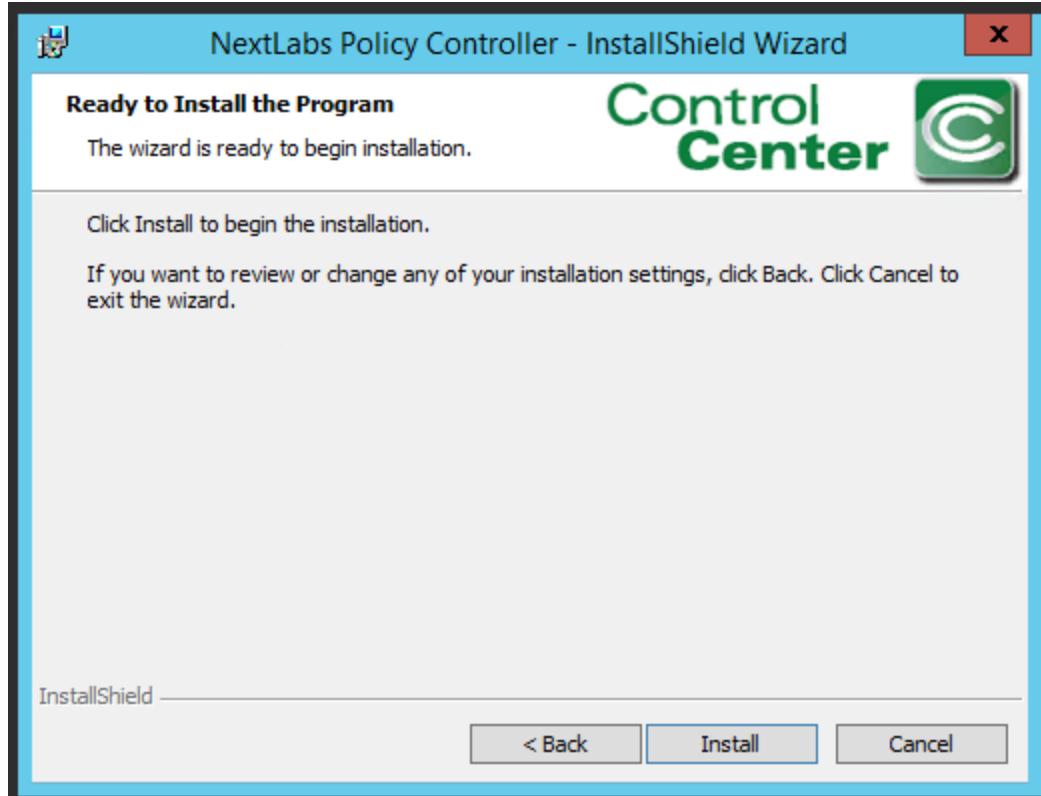


3699

- 3700 8. At the ICENet Server Location screen, enter the default ICENet Server Location: **sqlserver:8443**.
3701 Click **Next**.

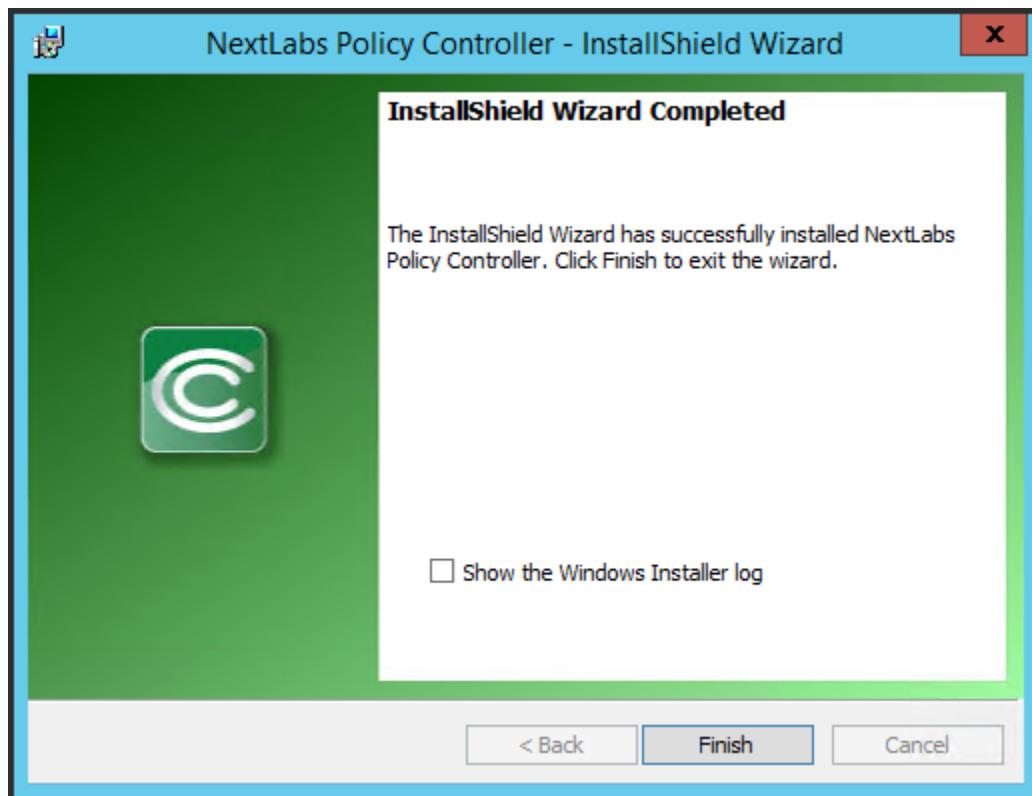


- 3702
3703 9. At the Ready to Install the Program screen, click **Install**.



3704

3705 10. At the InstallShield Wizard Completed screen, click **Finish**.



3706

- 3707 11. In the window that immediately opens, click **Yes** to restart the computer, or click **No** to wait and
 3708 restart after installing the PEP (see Section 7.6).

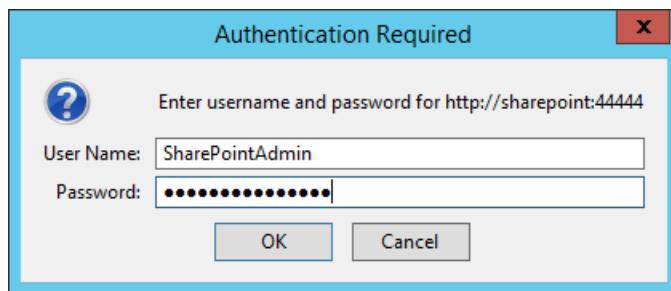
3709 **7.6 Installation and Configuration of NextLabs Entitlement Manager for**
 3710 **SharePoint Server**

3711 **7.6.1 Installation and Configuration**

3712 Note: Prior to installing the Entitlement Manager for SharePoint Server, it is necessary to install the
 3713 NextLabs Policy Controller on the SharePoint Server. If you have not already installed the Policy
 3714 Controller, please refer to [Section 7.5](#) before proceeding.

3715 **7.6.1.1 Verify that a Web Application Site and Site Collection Already Exist in SharePoint**

- 3716 1. On the SharePoint Server, open an Internet browser and navigate to the following URL:
 <http://sharepoint:44444> to login to the SharePoint Central Administration portal.
- 3718 2. Enter the **User Name** and **Password** for your SharePoint Central Administration account, and
 click **OK**.



- 3720
- 3721 3. At the Central Administration page, click on **Manage web applications** under Application
 Management.

3723

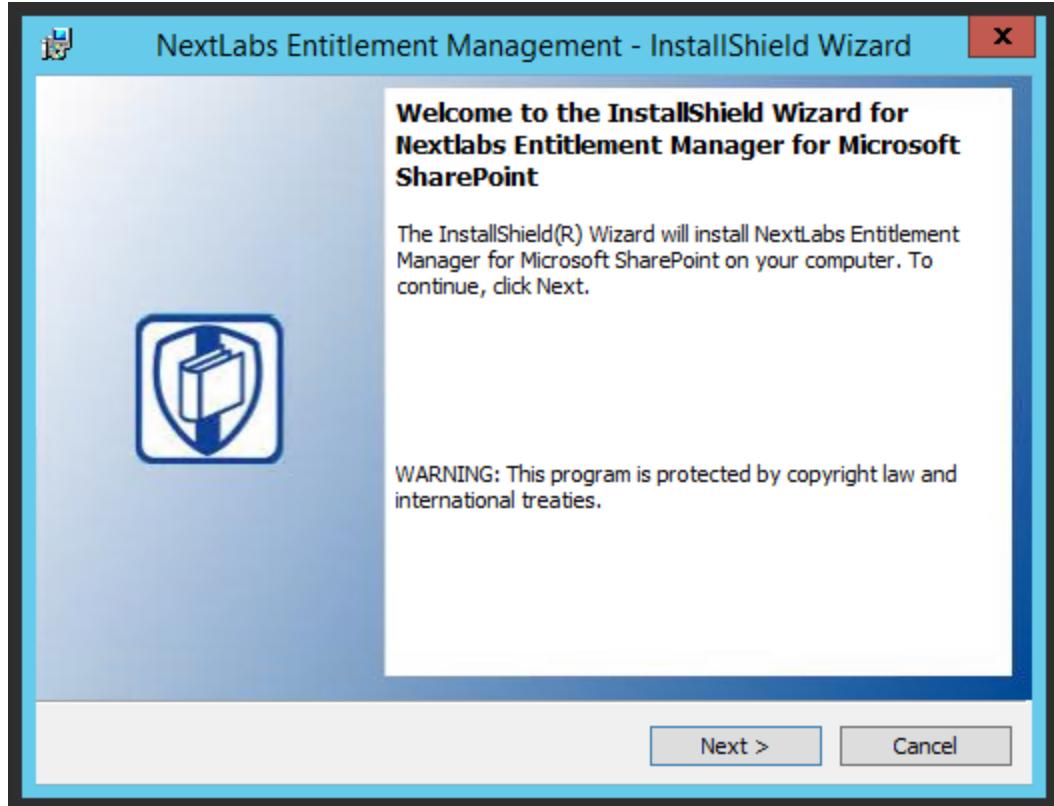
- 3724 a. If they do not already exist, create a default **Web Application** site and add it to a basic
 3725 Site Collection in SharePoint via Central Administration (See [Section 4](#)).

Central Administration	Name	URL	Port
Application Management	SharePoint - 80	http://sharepoint/	80
	SharePoint Central Administration v4	http://sharepoint:4444/	4444

3726 **7.6.1.2 *Install NextLabs Entitlement Manager for SharePoint Server***

3727 Complete the standard Entitlement Manager for SharePoint Server installation per NextLabs
 3728 documentation available to customers using the following steps:

- 3730 1. On the SharePoint Server, go to your Desktop or other known location where the required
 3731 NextLabs Policy Controller installation files are stored. Example:
 3732 C:\Users\Administrator\Desktop\SharePoint\
- 3733 2. Right-click on **SharePointEnforcer-2013-64-7.1.3.0-7-201410101427.zip** and select **Extract All**
 3734 from the floating menu. Wait for the files to be extracted.
- 3735 3. Double-click on the **SharePointEnforcer-2013-64-7.1.3.0-7-201410101427** folder.
- 3736 4. Double-click on **SharePointEnforcer-2013-64-7.1.3.0-7.msi** to begin the installation.
- 3737 5. At the Welcome to the InstallShield Wizard for NextLabs Entitlement Manager for Microsoft
 3738 SharePoint screen, click **Next**.



3739

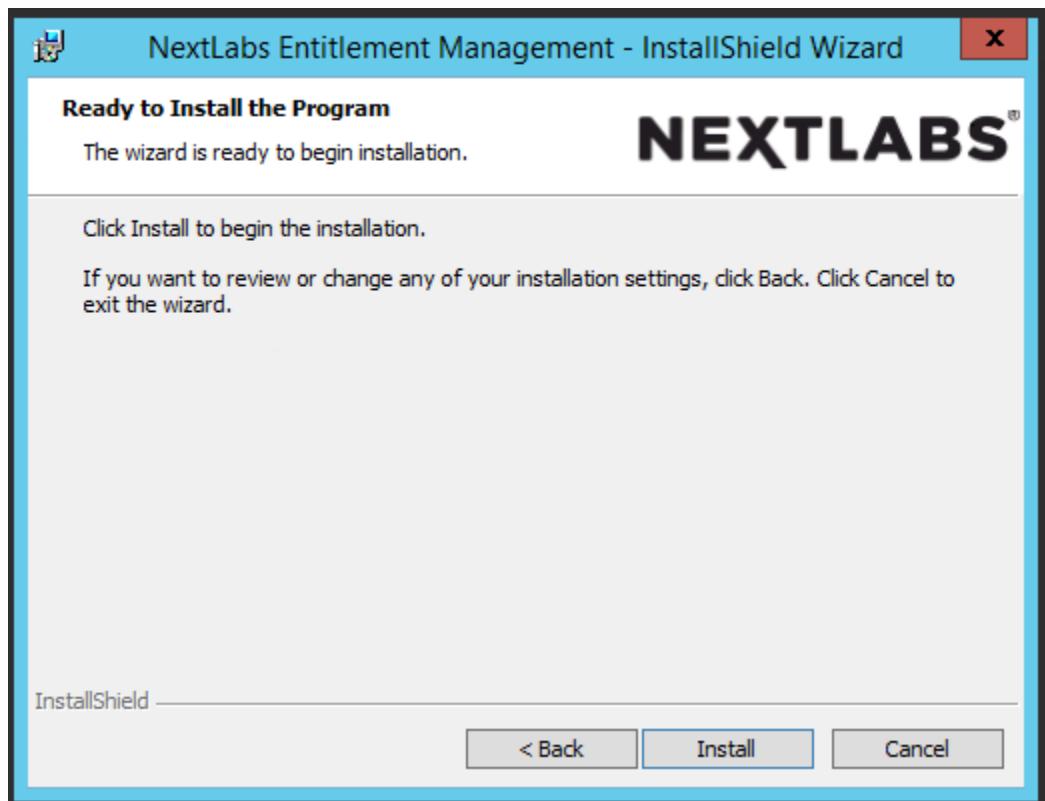
- 3740 6. At the License Agreement screen, select **I accept the terms in the license agreement** and click
3741 **Next**.



3742

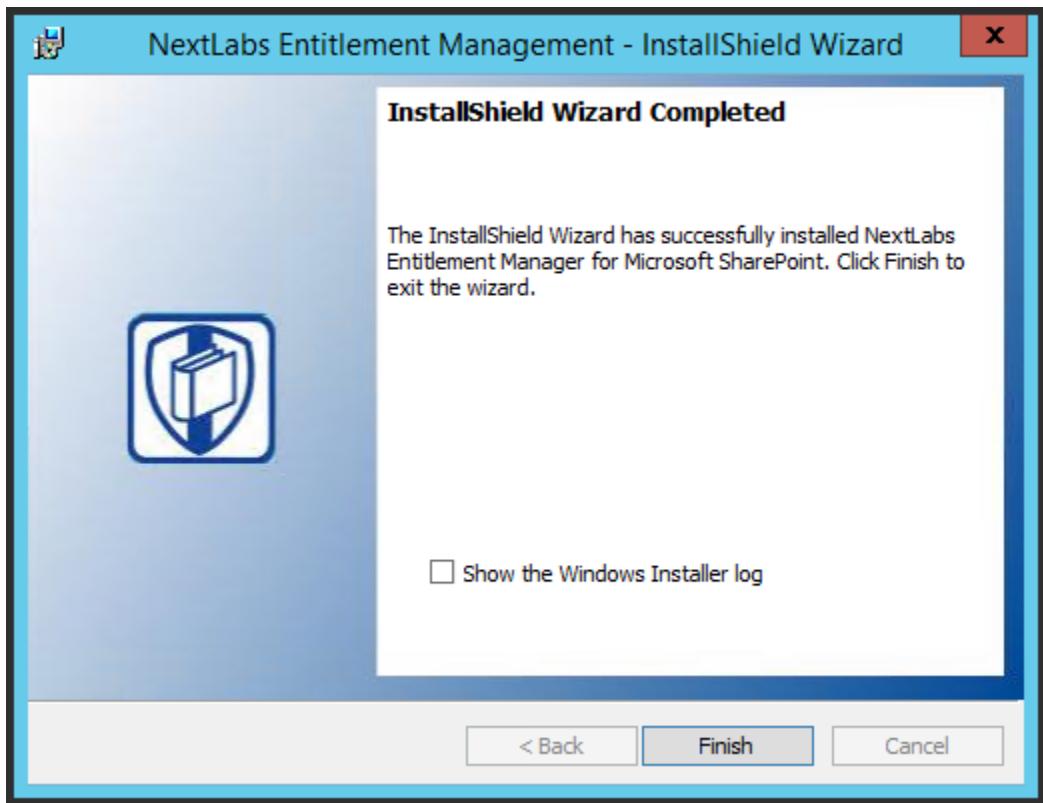
3743

7. At the Ready to Install the Program screen, click **Install**.



3744

3745 8. At the InstallShield Wizard Completed screen, click **Finish**.



3746

3747 9. After installing the IIS server must be reset:

3748 a. Click on the Windows icon and begin typing the word **PowerShell**

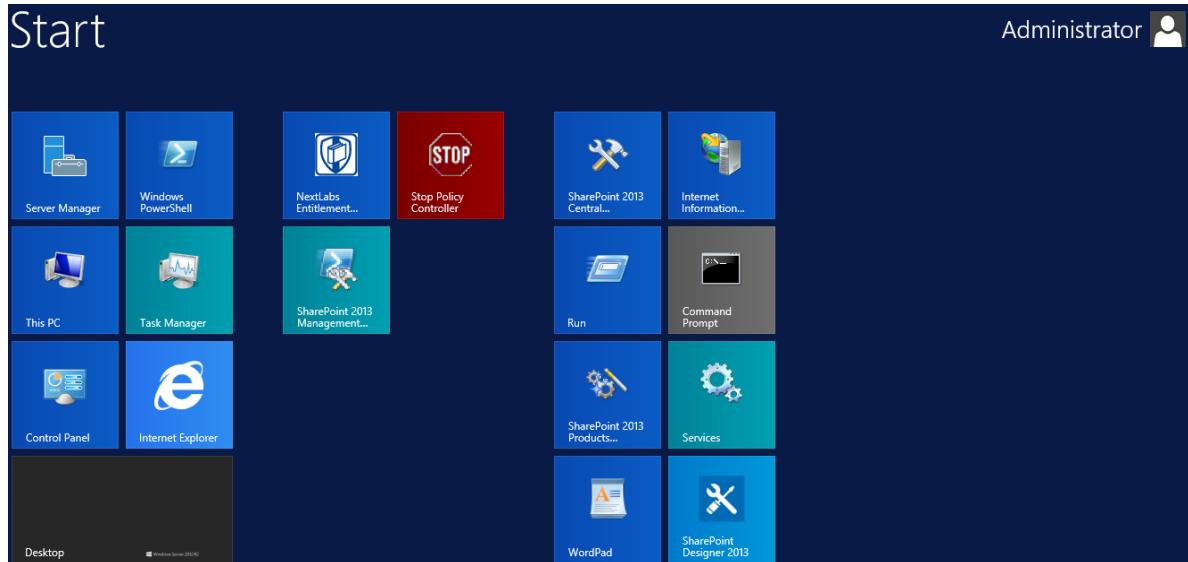
3749 b. When the Windows PowerShell application icon appears, double-click on the icon to
3750 open the Windows PowerShell

3751 c. From within the Windows PowerShell window, type in this command and press Enter to
3752 reset Internet Information Services: **iisreset**

3753 *7.6.1.3 Deploy Entitlement Manager for SharePoint Server to your SharePoint Farm*

3754 On the SharePoint Server, complete standard Entitlement Manager for SharePoint Server deployment
3755 per NextLabs documentation available to customers using the following steps:

3756 1. On the SharePoint Server, click the **Start** icon to see the applications pinned to the **Start** menu.

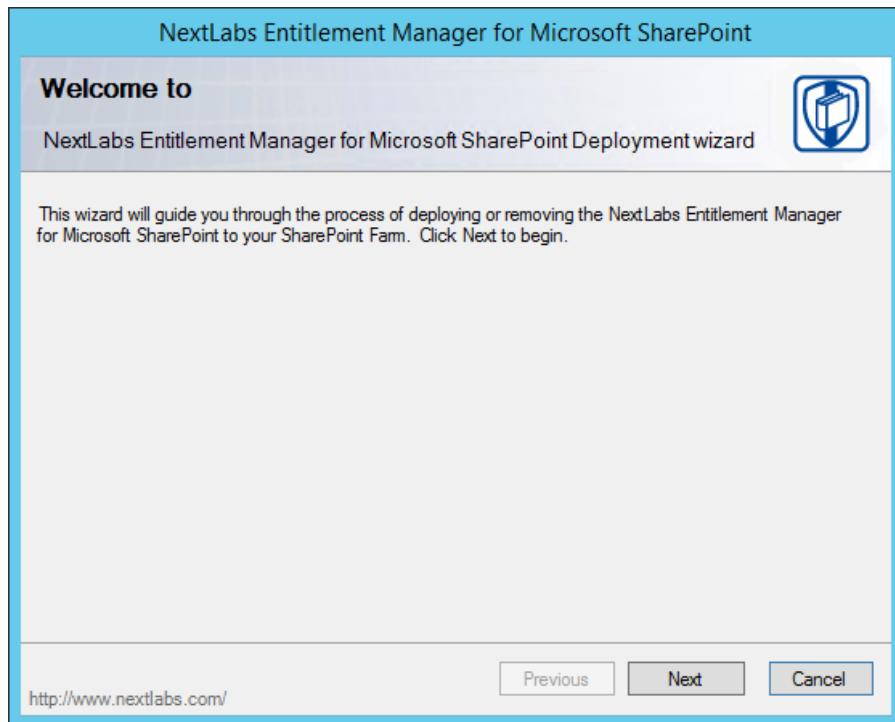


3757

- 3758 2. Click on the NextLabs Entitlement Manager for SharePoint Server Deployment icon.

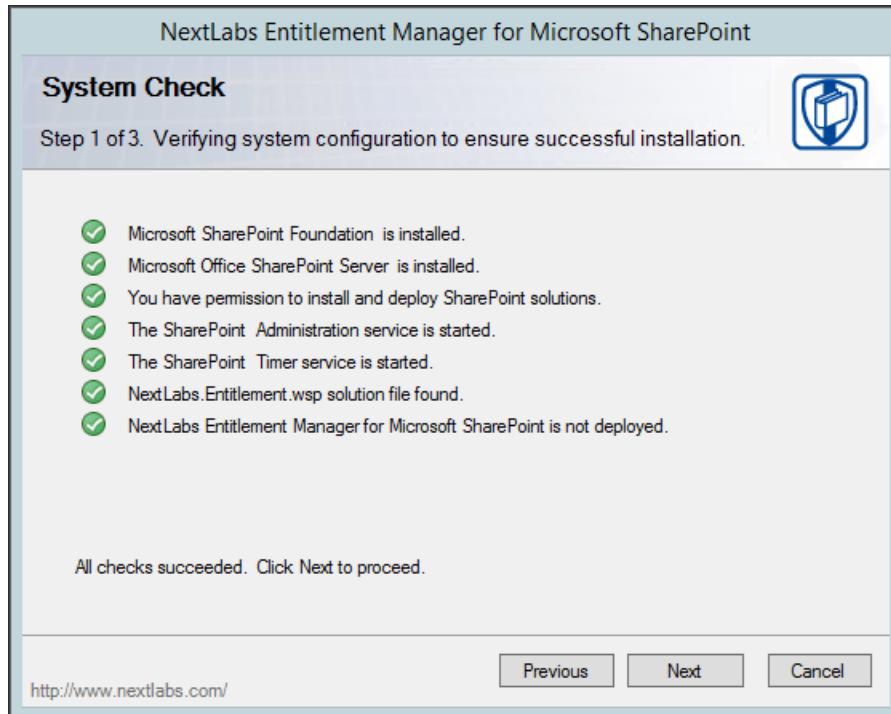
3759 This shortcut is automatically pinned during the initial installation. In case the shortcut is not
 3760 created automatically, the application can be opened from File Explorer at the location:
 3761 *C:\Program Files\NextLabs\SharePoint Enforcer\bin\NextLabs.Entitlement.Wizard.exe*

- 3762 3. At the Welcome to NextLabs Entitlement Manager for Microsoft SharePoint Deployment wizard
 3763 screen, click **Next**.



3764

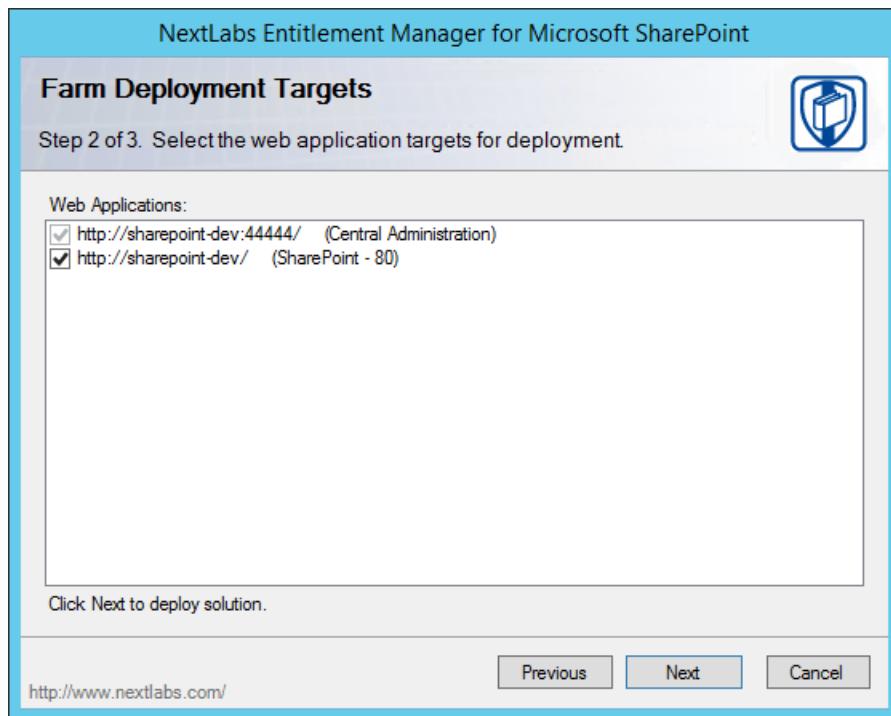
- 3765 4. At the System Check screen, after the system check is complete, click **Next**.



3766

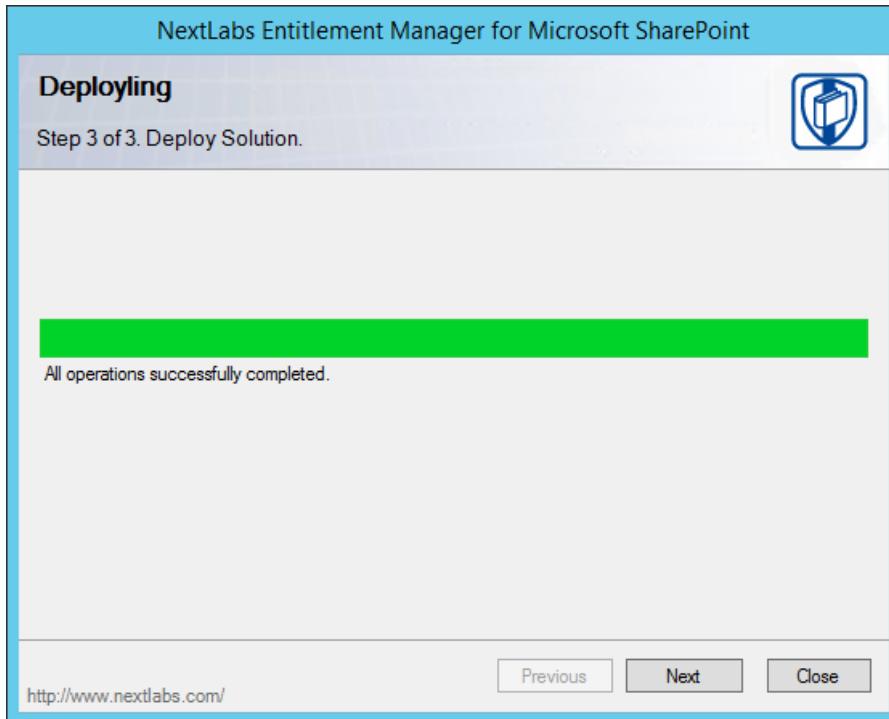
- 3767 5. At the Farm Deployment Targets screen, select the applicable web application on which to
3768 deploy.

3769
3770

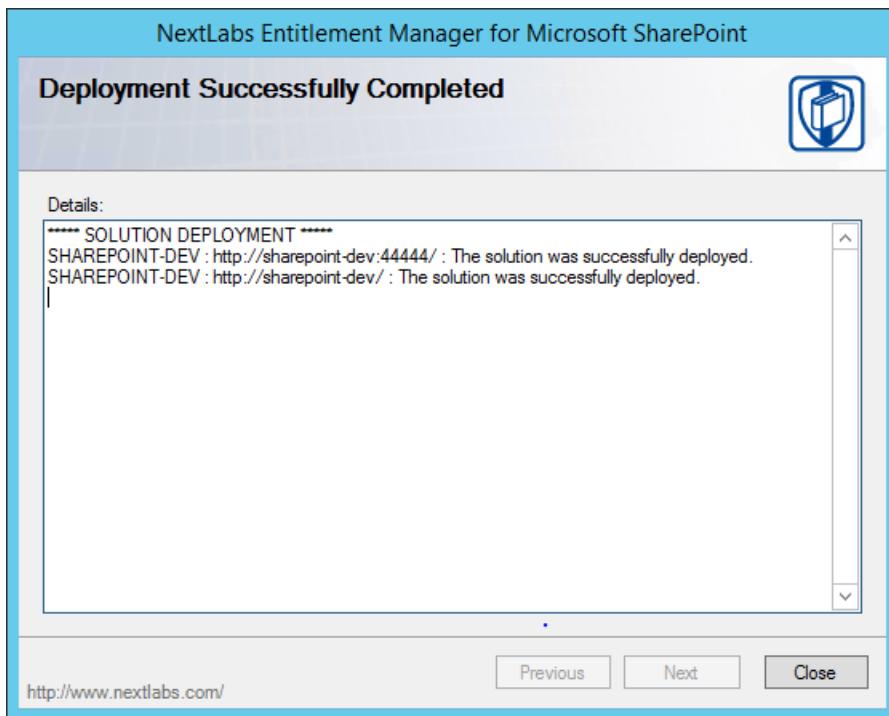


3771

- 3772 6. At the Deploying Step 3 of 3 screen, click **Next**.



- 3774 7. At the Successful Deployment Completed screen, click **Close**.

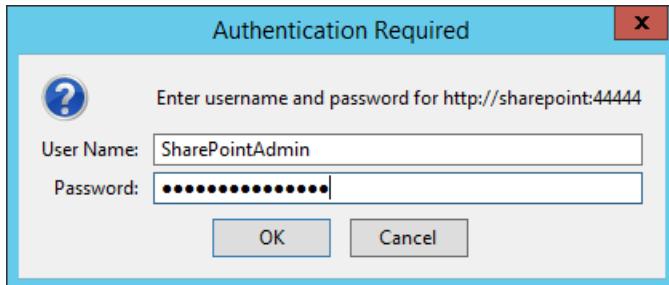


3776 **7.6.1.4 Enable Policy Enforcement on your Web Application via SharePoint Central Administration**

- 3777
- 3778 1. On the SharePoint Server, open an Internet browser and navigate to the following URL:
3779 <http://sharepoint:44444> to login to the SharePoint Central Administration portal.

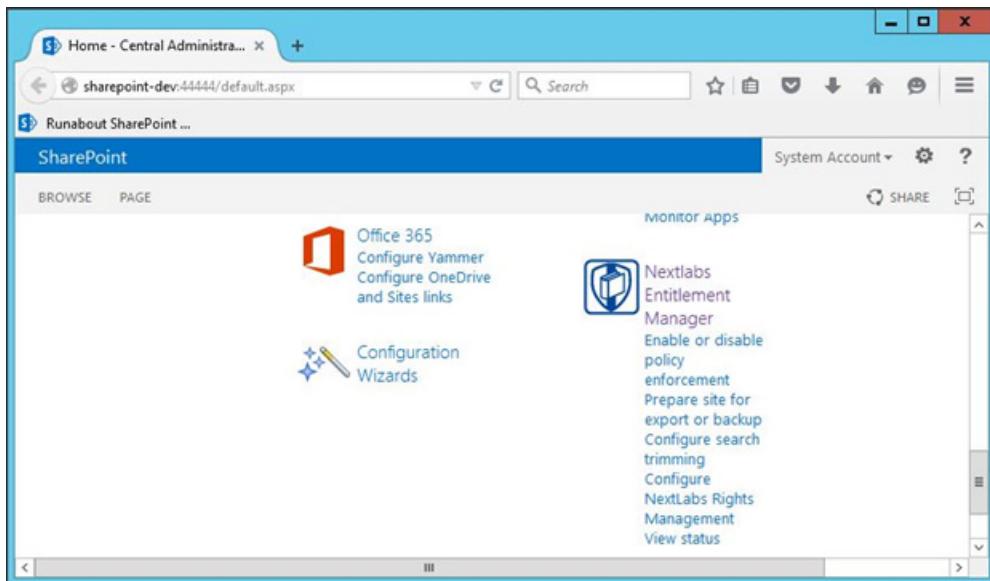
SECOND DRAFT

- 3780 2. Enter the **User Name** and **Password** for your SharePoint Central Administration account, and
3781 click **OK**.



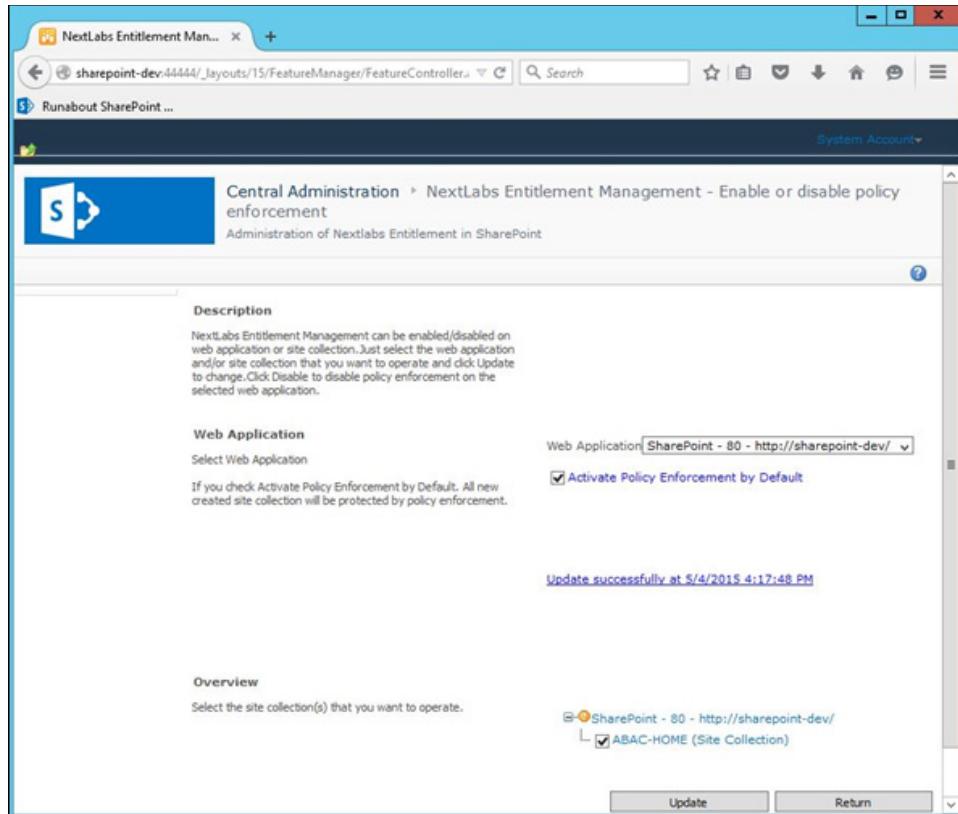
3782

- 3783 3. Click on the **NextLabs Entitlement Manager** icon.



3784

- 3785 4. In the page that opens, scroll down to verify that the correct **Web Application** is chosen and the
3786 service is **Enabled**.

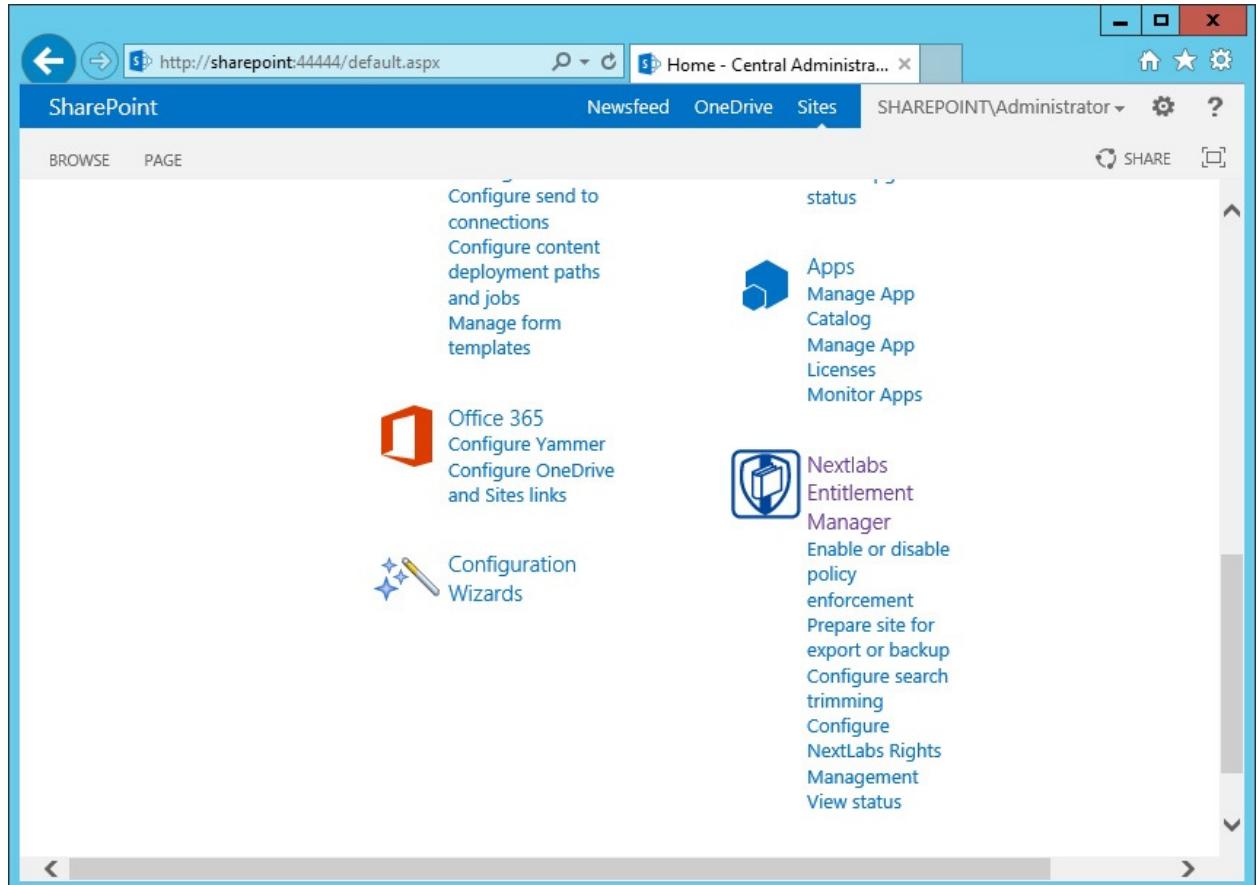


3787

3788 7.7 Functional Tests

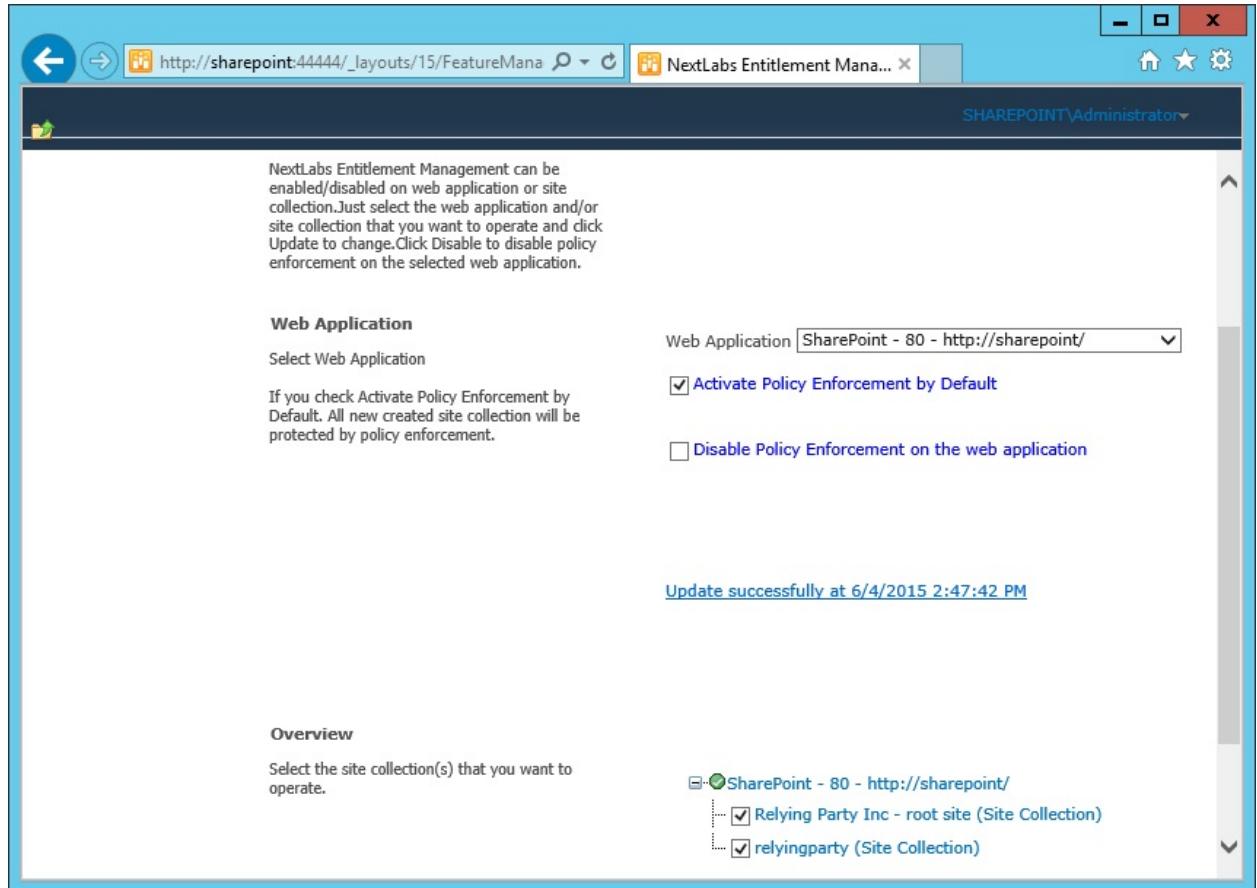
3789 7.7.1 Verify that the NextLabs Webpart for Policy Enforcement Has Been 3790 Successfully Enabled on the Site Collection in SharePoint

- 3791 1. Similar to [Section 7.6.1.4](#), complete the following steps to login to SharePoint Central
3792 Administration:
 - 3793 a. Click on the Start icon.
 - 3794 b. Click the NextLabs Entitlement Manager for SharePoint icon.
 - 3795 c. Open SharePoint Central Administration and login as Administrator.
- 3796 2. Click on **Enable or disable policy enforcement** under the NextLabs Entitlement Manager
3797 webpart.



3798

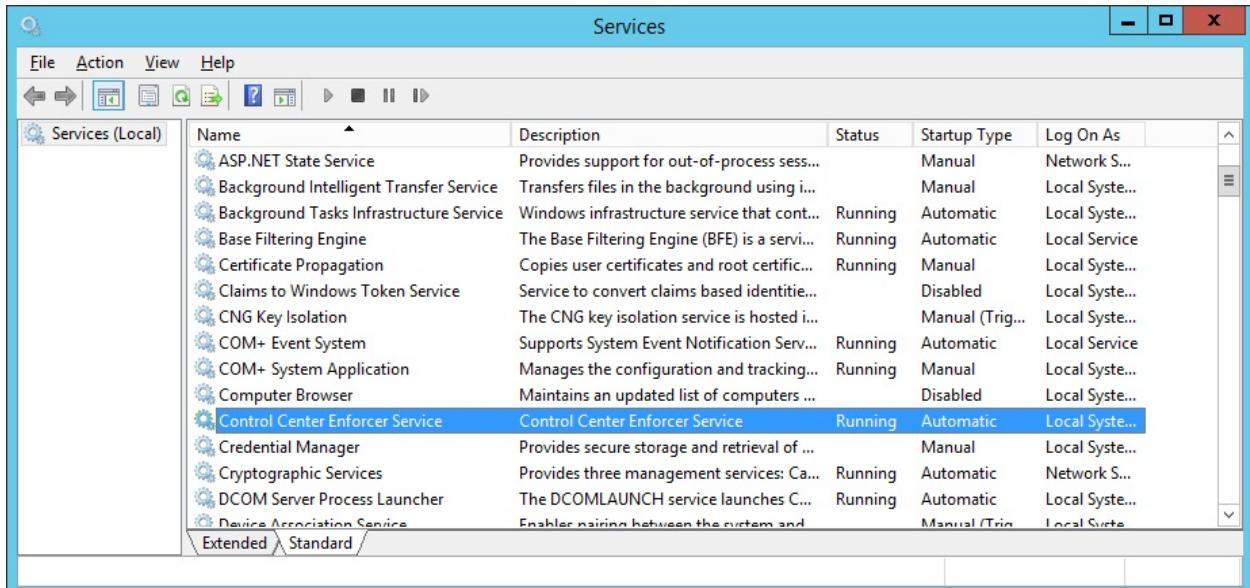
- 3799 3. Scroll down to the **Web Application** area to verify that the Entitlement Manager is activated for
3800 the correct SharePoint web application.



3801

3802 7.7.2 Test to Verify the NextLabs Service is Running

- 3803 1. Click on the Windows Start icon.
- 3804 2. Start typing the word **Services**.
- 3805 3. Click on the Windows Services icon to open the list of running services.
- 3806 4. Look for the NextLabs Policy Controller service called **Control Center Enforcer Service**.
- 3807 5. Verify that the status is **Running**.



The screenshot shows the Windows Services window with the title bar 'Services'. The menu bar includes 'File', 'Action', 'View', and 'Help'. Below the menu is a toolbar with icons for search, refresh, and various actions. A grid table lists services under the heading 'Services (Local)'. The columns are 'Name', 'Description', 'Status', 'Startup Type', and 'Log On As'. The 'Control Center Enforcer Service' is highlighted in blue. Other services listed include ASP.NET State Service, Background Intelligent Transfer Service, Background Tasks Infrastructure Service, Base Filtering Engine, Certificate Propagation, Claims to Windows Token Service, CNG Key Isolation, COM+ Event System, COM+ System Application, Computer Browser, Control Center Enforcer Service, Credential Manager, Cryptographic Services, DCOM Server Process Launcher, and Device Association Service.

Name	Description	Status	Startup Type	Log On As
ASP.NET State Service	Provides support for out-of-process sess...	Manual	Network S...	
Background Intelligent Transfer Service	Transfers files in the background using ...	Manual	Local Syste...	
Background Tasks Infrastructure Service	Windows infrastructure service that cont...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Filtering Engine (BFE) is a servi...	Running	Automatic	Local Service
Certificate Propagation	Copies user certificates and root certific...	Running	Manual	Local Syste...
Claims to Windows Token Service	Service to convert claims based identifie...	Disabled	Local Syste...	
CNG Key Isolation	The CNG key isolation service is hosted i...	Manual (Trig...	Local Syste...	
COM+ Event System	Supports System Event Notification Serv...	Running	Automatic	Local Service
COM+ System Application	Manages the configuration and tracking...	Running	Manual	Local Syste...
Computer Browser	Maintains an updated list of computers ...	Disabled	Local Syste...	
Control Center Enforcer Service	Control Center Enforcer Service	Running	Automatic	Local Syste...
Credential Manager	Provides secure storage and retrieval of ...	Manual	Local Syste...	
Cryptographic Services	Provides three management services: Ca...	Running	Automatic	Network S...
DCOM Server Process Launcher	The DCOMLAUNCH service launches C...	Running	Automatic	Local Syste...
Device Association Service	Enables pairing between the system and...	Manual (Trig...	Local Syste...	

3808

3809 8 Defining Policies and Enforcing Access Decisions with 3810 NextLabs

3811 8.1 Introduction

3812 In previous sections of this How-To Guide, we installed several NextLabs products that can be used to
 3813 define and deploy Attribute Based Access Control (ABAC) policies, and enforce decisions regarding user
 3814 access to Microsoft SharePoint resources based on user, object, and environmental attributes, and the
 3815 corresponding policies in place. This How-To Guide will illustrate how to use and configure NextLabs
 3816 Policy Studio, the product responsible for Policy Lifecycle Management, and discuss policy strategy and
 3817 the translation of business logic into policy.

3818 Within Policy Studio, we will define and deploy policies and policy components. In NextLabs, the word
3819 Component is a named definition that represents a category or class of entities, such as users, data
 3820 resources, or applications; or of actions, such as Open or Copy. Components are similar to using parts of
 3821 speech to construct policy statements. For example:

- 3822 ▪ Noun: All employees in the human resources department or Any file with an .xls extension
- 3823 ▪ Verb: Copy, Print, or Rename File

3824 **Deployment** is simply the distribution of new or modified policies and policy components to the
 3825 appropriate enforcement points on desktop PCs, laptops, and file servers throughout the organization.
 3826 This means you can create, review and refine policies as long as you like, but they are not enforced until
 3827 you actually deploy them.

3828 Finally, the Functional Test section will illustrate how to ensure that policies are being updated,
 3829 evaluated, and enforced on Microsoft SharePoint.

8.1.1 Components and Sub-Components Used in this How-To Guide

1. NextLabs Policy Studio –provides the Policy Administration Point of the ABAC architecture. This component was installed with the rest of the NextLabs product suite used in this implementation in [Section 7](#). Policy Studio provides the graphical user interface for Policy Lifecycle Management (defining, deploying, modifying, and deactivating policies).
 - a. Located on the SQL Server
2. NextLabs Policy Server SharePoint Enforcer configuration file
 - a. Automatically exists after NextLabs Control Center installation
 - b. Located within the NextLabs software architecture on the SQL Server
3. NextLabs AgentLog and bundle.bin files
 - a. Automatically exist after NextLabs Policy Controller installation
 - b. Located within the NextLabs software architecture on the SharePoint Server

8.1.2 Pre-requisites to Complete Prior to this How-To Guide

1. If you intend to do a setup without identity federation and federated logins, you must:
 - a. Install and configure Active Directory (see [Section 2](#)).
 - b. Install and configure Microsoft SharePoint (see [Section 4](#)).
 - c. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see [Section 7](#)).
2. If you intend to incorporate a trust relationship between an IdP and RP, and use federated logins into SharePoint, you must:
 - a. Install and configure Active Directory (see [Section 2](#)).
 - b. Setup and configure the RP and IdP (see [Section 3](#)).
 - c. Install and configure Microsoft SharePoint (see [Section 4](#)).
 - d. Configure the SharePoint federated login with the RP (see [Section 5](#)).
 - e. Configure the attribute flow between all endpoints (see [Section 6](#)).
 - f. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see [Section 7](#)).

8.2 Policy Strategy

8.2.1 Top-Level Blacklisting Deny Policy, Whitelisting Allow Sub-Policies

In order to demonstrate a policy set with high security and fine-grained control, we employed a general blacklisting, then fine grained whitelisting sub-policy strategy for the policies. We chose this strategy because we considered it a more secure paradigm for securing SharePoint resources. Using this strategy, the access control logic initially applies a general deny all access decision at the top level for a given set of related attributes, then specifies conditions under which access can be allowed in various sub-policies based on sufficient correlating user, resource, and/or environment attributes. For example, later in this

3865 guide we will describe a policy set in which we initially deny all users on resources that have a sensitivity
3866 level attribute, however there is a sub-policy that specifies that a for resources at sensitivity level 2,
3867 allow users with a clearance attribute of **Secret** during regular business hours. The alternative to this
3868 approach would be to apply a general allow all access decision at the top level initially, then specify
3869 conditions under which users should be denied access. Because there can be many unforeseen edge
3870 cases that may not be anticipated by a business protecting its assets, we consider the general
3871 blacklisting, then whitelisting sub-policies approach a more feasibly secure solution. According to our
3872 strategy, any time a user, resource, or environment attribute does not comply with a whitelisting sub-
3873 policy to allow access, the access decision will default to deny.

3874 8.2.2 Global Policies

3875 In addition to the blacklisting versus whitelisting approach taken in our policy strategy, we also
3876 employed the use of global policies. The term **global policy** refers to the general applicability of the
3877 policy sets to more than one user and more than one resource at a given time. We defined our policies
3878 such that they have global effects and do not apply only to very specific use cases by themselves. The
3879 collective logic taken from the multiple global policies in place applies to the many kinds of access
3880 events that must be controlled according to a business's complex and distributed business rules, which
3881 we describe below in Section 8.3.

3882 8.3 Translation of Business Logic into Policy

3883 8.3.1 ABAC Build Scenario – Runabout Air Business Rules

3884 In previous sections of our Practice Guide we have constructed an example business scenario where an
3885 airline company, Runabout Air, has acquired another airline company, Conway Airlines. In this scenario
3886 the two companies have not yet merged their active directory forest and established a trust relationship
3887 such that historically Conway Airlines employees will be able to access resources on the Runabout Air
3888 SharePoint according to policies that correspond to Runabout Air's business rules. The business rules we
3889 based our policies on are, generally:

- 3890 1. Some documents are more sensitive than others, and should be marked in SharePoint at
3891 different sensitivity levels. These documents should be strictly protected, and access should be
3892 restricted to Runabout Air's normal business hours. Also, users should only be granted access to
3893 sensitive documents if they have sufficient clearance.
- 3894 2. Users should only be able to access documents that belong to their department, or to the
3895 departments relevant to them in the case of some instances of a need for cross-department
3896 access, i.e., business intelligence employees should have access to both sales and marketing
3897 department documents.
- 3898 3. Some documents are time-sensitive and pertain to system or other business maintenance, and
3899 should be marked in SharePoint as maintenance documents. These documents should only be
3900 accessed outside of Runabout Air's normal business hours, so as to reduce the likelihood of
3901 disruption of normal business operation.
- 3902 4. There are times when a suspicious IP address or range of addresses should be blocked from
3903 accessing any SharePoint resources, or when a user from a particular IP address or range of IP
3904 addresses should only have access to low-sensitivity documents. There must be a mechanism in

3905 place to ensure access is denied for users attempting to access any high-sensitivity documents
3906 from an environment with that IP address or within a given IP address range.

3907 8.3.2 Translation of Runabout Air Business Rules into ABAC Policies

3908 ABAC Policies created from the above business rules might look like this:

- 3909 1. Top-level sensitivity policy: default to deny access to all users attempting to access resources
3910 that have a sensitivity level attribute defined in SharePoint as greater than **0**, unless explicitly
3911 allowed access by a sub-policy.
 - 3912 a. For documents whose sensitivity attribute is defined as **1**, allow access any time of day,
3913 any day of the week, to users with a clearance attribute of **None, Secret, or Top Secret**.
 - 3914 b. For documents whose sensitivity attribute is defined as **2**, allow access between the
3915 hours of 6am and 6pm for users with a clearance attribute of **Secret or Top Secret**.
 - 3916 c. For documents whose sensitivity attribute is defined as **3**, allow access between the
3917 hours of 6am and 6pm for users with a clearance attribute of **Top Secret**.
- 3918 2. Top-level department policy: default to deny access to all users attempting to access resources
3919 that have a department attribute and project status defined in SharePoint.
 - 3920 a. For users whose department attribute is defined as a value equal to the document's de-
3921 partment attribute value, allow access for documents with a project status of any value.
 - 3922 b. For users whose department attribute is **Business Intelligence**, allow access for docu-
3923 ments with a department attribute of **Sales or Marketing** and with a Project status of
3924 any value.

3925 Note: The Project status metric is necessary because the department attribute is defined at the
3926 site level within SharePoint. Restricting users based only on the resource's department attribute
3927 in this policy set results in the user being stuck in a deny access loop, no longer being able to
3928 access the Runabout Air root site and navigate to their correct department's documents.
3929 Because each document has a project status attribute defined in addition to the department
3930 attribute, the policies can specify the targets of this policy as having both project status and
3931 department attributes defined, even though the department attribute is the most pertinent
3932 attribute for enforcing the access control relating to department access rules.

- 3933 3. Top-level maintenance policy: default to deny access to all users attempting to access resources
3934 that have a maintenance attribute defined in SharePoint
 - 3935 a. For documents whose maintenance attribute is defined as **no**, allow access to users, any
3936 time of day, any day of the week.
 - 3937 b. For documents whose maintenance attribute is defined as **yes**, allow access to users be-
3938 tween 6pm and 6am, any day of the week.
- 3939 4. Top-level IP Address policy: default to deny access to all users attempting to access resources
3940 that have a sensitivity attribute defined in SharePoint.
 - 3941 a. For documents whose sensitivity attribute is defined as **1**, allow access to any user from
3942 an environment with any IP address defined.

- 3943 b. For documents whose sensitivity attribute is defined as **2** or **3**, allow access to users
 3944 coming from an environment with an IP address other than a restricted IP or one within
 3945 a restricted IP range.

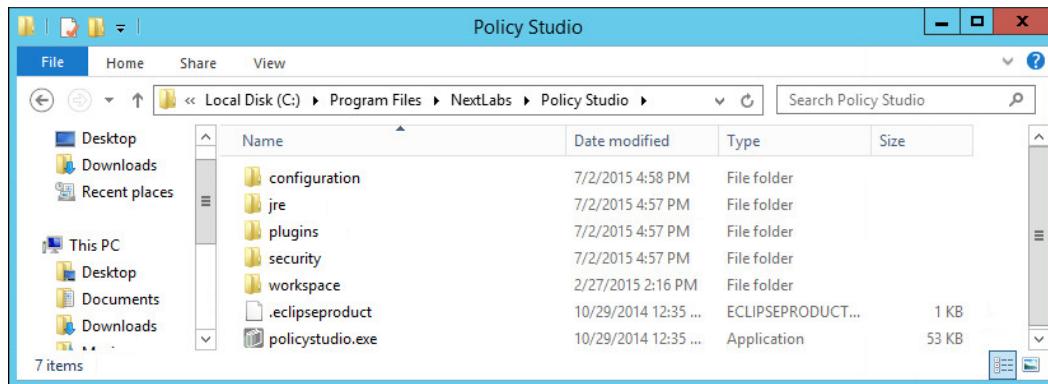
3946 8.4 Using the NextLabs Policy Studio GUI for Policy Definition and 3947 Deployment

3948 In this section, we will provide step-by-step instructions for how to define, deploy, modify and re-
 3949 deploy, and deactivate necessary policy components and policies within Policy Studio. The examples we
 3950 will use correspond to the Runabout Air business rules and ABAC policies described in [Section 8.3.1](#) and
 3951 [Section 8.3.2](#). Note that Policy Studio was installed on the SQL Server, which is where all of the activity in
 3952 Section 8.4 occurs.

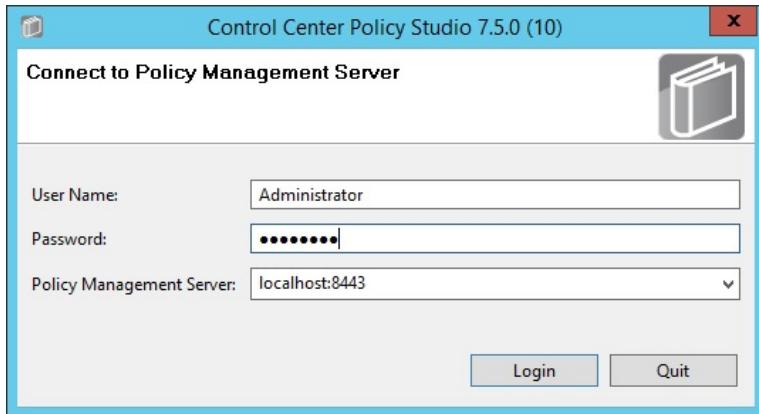
3953 8.4.1 Login and Initial Screen in Policy Studio

3954 Given you have followed the instructions found in [Section 7](#), follow these instructions to login to the
 3955 NextLabs Policy Studio:

- 3956 1. In Windows Explorer, find and open the **policystudio.exe** application file:
 - 3957 a. Double-click the **C:/** drive.
 - 3958 b. Double-click **Program Files**.
 - 3959 c. Double-click **NextLabs**.
 - 3960 d. Double-click **Policy Studio**.
 - 3961 e. Double-click **policystudio.exe**.

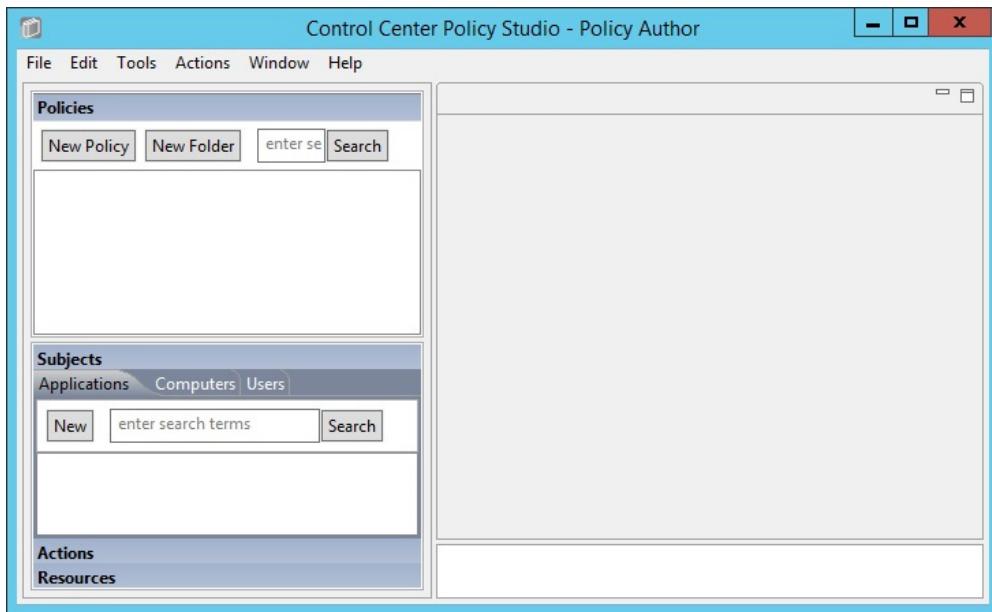


- 3962 2. In the Control Center Policy Studio window, enter **User Name** and **Password**, then click **Login** to
 3963 connect to the Policy Management Server.



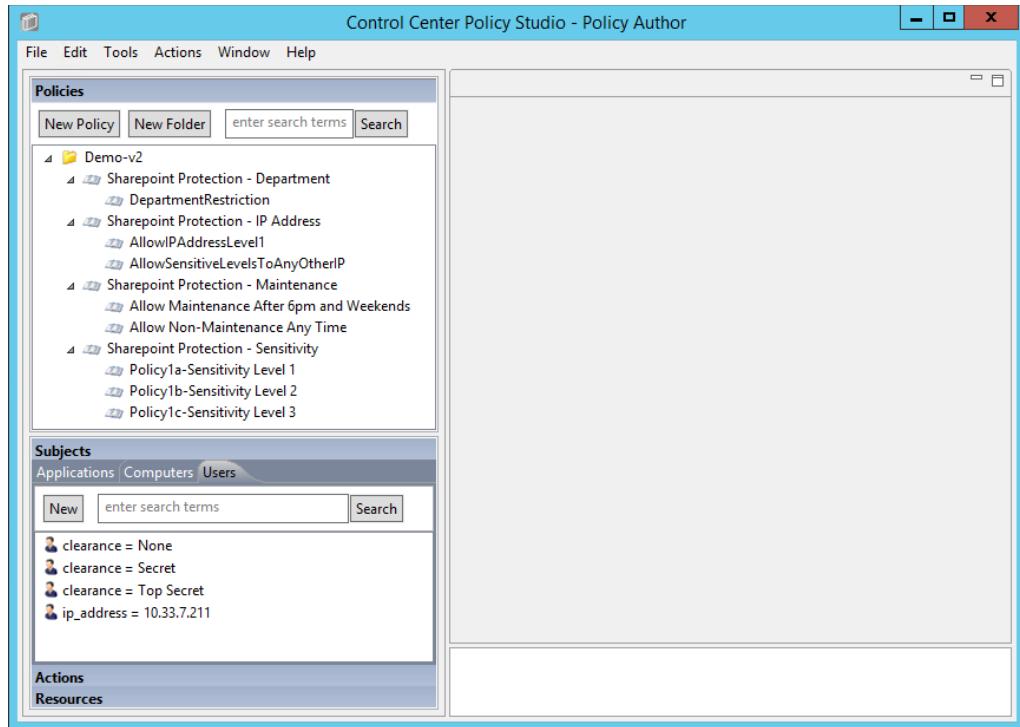
3965

- 3966 3. If login was successful, you will see the Policy Studio's graphical user interface, specifically the
 3967 main screen where new policies and new components are defined, deployed, modified, and
 3968 deactivated. Note the **Policies** panel in the top-left, the **Components** panel in the bottom-left,
 3969 and an open space to the right where editing panels emerge for editing the policies and
 3970 components.



3971

- 3972 4. After following the instructions in this section to define and deploy several user and resource
 3973 components, as well as four policy sets, the Policy Studio interface will show the new
 3974 components and policies populated in the left-side panel.



3975

3976 8.4.2 Policy Studio Menu Commands

3977 Below are some of the Policy Studio menu commands used in this How-To Guide, along with
3978 explanations for what action they perform.

3979 Extracted from the NextLabs Policy Studio User guide available to customers:

Menu	Command	Function
File	Exit	Closes Policy Studio.
Edit	Delete	Deletes the currently selected item or items.
	Duplicate	Creates a clone of the selected component

3980

Menu	Command	Function
Actions	Modify	Changes the status of the currently displayed component or policy to Draft. You must do this whenever you want to make any changes to a component or policy that has been submitted. Function is the same as the Modify button at the bottom of the Editing pane.
	Submit	Submits the currently selected components or policies for changing from one status to another—for example, from Draft status to Submitted for Deployment. Function is the same as the Submit button at the bottom of the Editing pane. Disabled if no object is selected, or if any of the selected objects is not currently in Modify state.
	Deploy	Deploys the currently displayed component or policy. Function is the same as the Deploy button at the bottom of the Editing pane. As with individually deployed objects, you can specify a scheduled deployment, or choose Now. Disabled if no object is selected, or if the selected object has not been submitted for deployment.
	Deploy All	Deploys all currently submitted components or policies. Function is the same as the Deploy button at the bottom of the Editing pane.
	Deactivate	Changes the status of the currently selected policies or components from Active to Deactivated. Disabled if no object is selected, or if any of the selected objects is not currently in Active state.
Window	Preview	Opens the Preview pane, at the right side of the Editor pane. The Preview pane allows you to test the actual content that would result from the current definition of a component.
	Policy Manager	Toggles to the Policy Manager interface. You can also type Ctrl + Tab.
	Policy Author	Disabled

3981

3982 8.4.3 Defining and Deploying Components

3983 8.4.3.1 Explanation of Components in NextLabs

3984 According to the NextLabs Policy Studio User Guide available to customers, it is necessary to define
 3985 components to represent various kinds of entities in your information environment. There are several
 3986 times when you might want to define a new component:

- 3987 1. After setting up your Control Center system, before constructing policies for the first time (which
 3988 is the reason here at this point in our How-To literature)
- 3989 2. When new classes of information or users come under the control of information policy
- 3990 3. When a new policy requires a policy component that has not yet been created
- 3991 4. When conditions at the organization change in any way that adds new items to be covered by
 3992 information control policies. For example, if the company reorganizes and adds a new division,
 3993 you might need a new policy component to represent the employees in that division.

3994 Furthermore, when you are constructing a component, you do not need to save your work explicitly.
 3995 Work is automatically saved as you go. If you are interrupted while working on a policy component, or
 3996 want to work on another task and return to constructing the policy component later, you can stop and
 3997 continue the constructing process as desired. Your work will be saved in draft status. You can find the
 3998 policy component later in the appropriate component panel.

3999 8.4.3.2 Defining and Deploying User Components

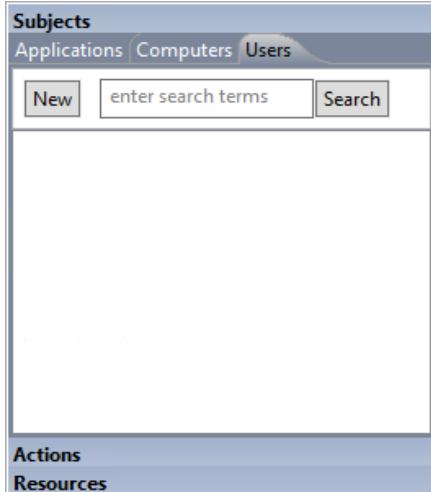
4000 According to the Runabout Air business rules in [Section 8.3.1](#) and ABAC policies in [Section 8.3.2](#), it is
 4001 possible that you may need to create a User Component to match the following conditions: user
 4002 clearance attribute, user department attribute, and user IP address. This is correct, except for the user
 4003 department attribute. Because of the cross-departmental access of Runabout Air's Business Intelligence
 4004 employees, we use logical syntax instead of graphical components while defining that policy. Also, a

4005 note regarding the user IP address component: even though IP address is an environmental attribute, it
 4006 can be configured in NextLabs as a user attribute coming from SharePoint Claims, or as a resource
 4007 attribute, which requires different configuration in NextLabs. For our example, we use the IP Address
 4008 from SharePoint Claims, which is handled as a user attribute.

4009 [8.4.3.2.1 Clearance Components](#)

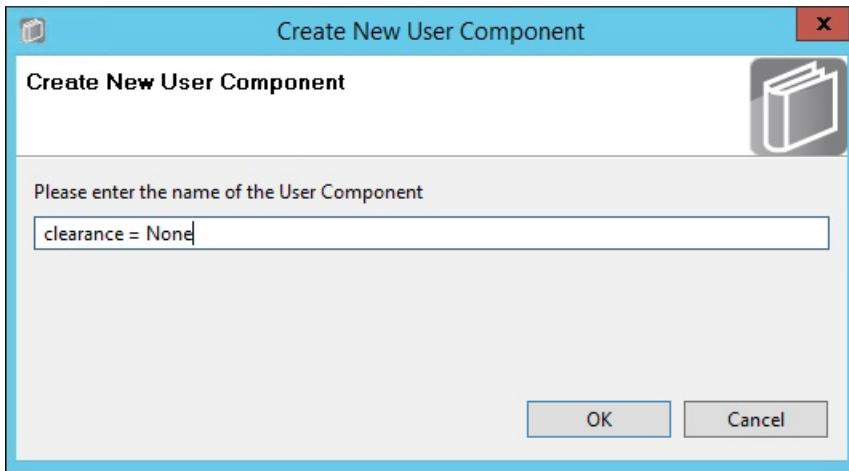
4010 [8.4.3.2.1.1 CLEARANCE = NONE](#)

- 4011 1. In the Components panel in the bottom-left of the Policy Studio window, click on the **Subjects** heading, and then click on the **Users** tab. Then click **New** to create a new component.



4013

- 4014 2. In the Create New User Component window, enter a descriptive component name, such as
 4015 **clearance = None**. Click **OK**.

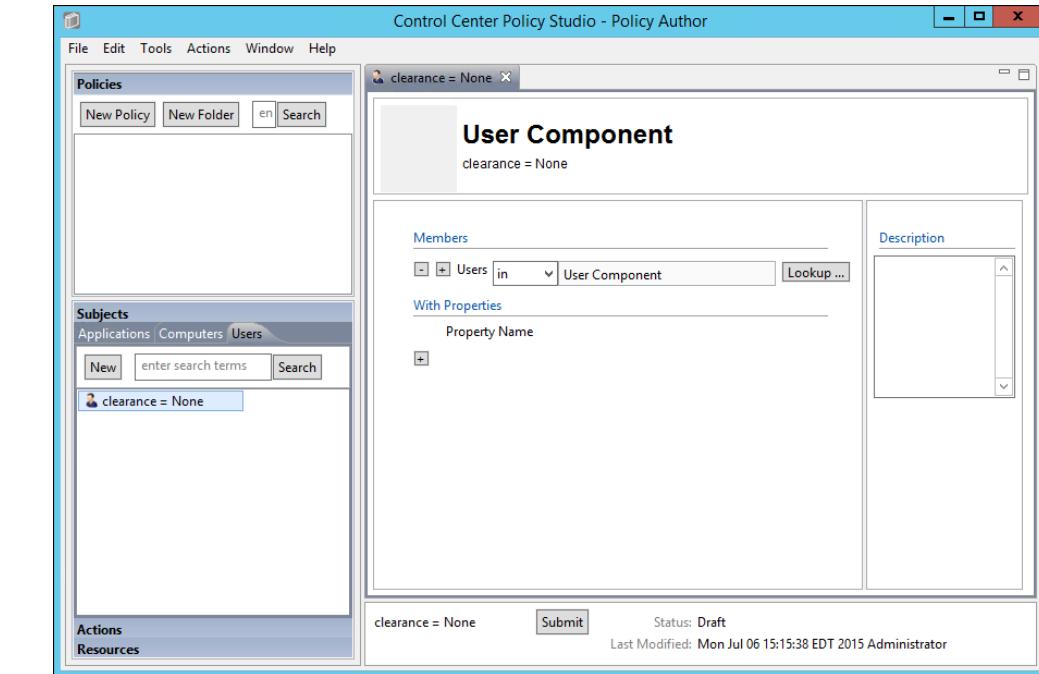


4016

- 4017 3. In the component editing panel you will see the following:

SECOND DRAFT

4018

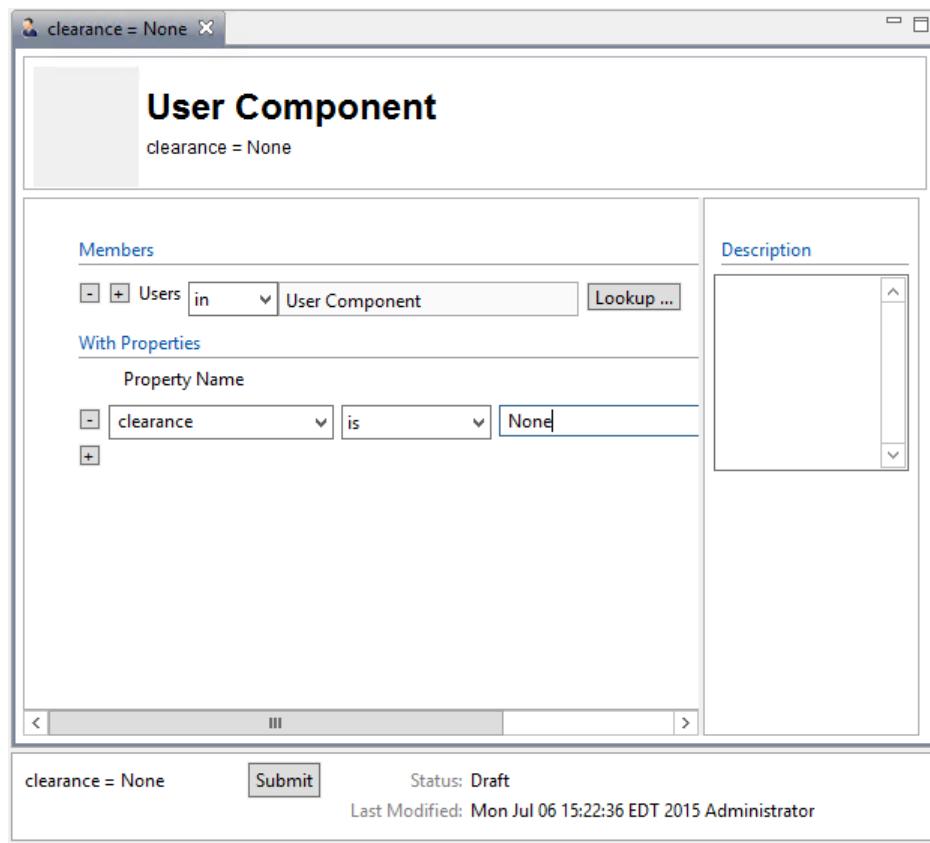


4019

4. In the editing panel, click on the **plus sign** box under Property Name and enter **clearance** in the property name text box, keep the default **is** as the action, then enter **None** into the value text box. Click **Submit**.

4020

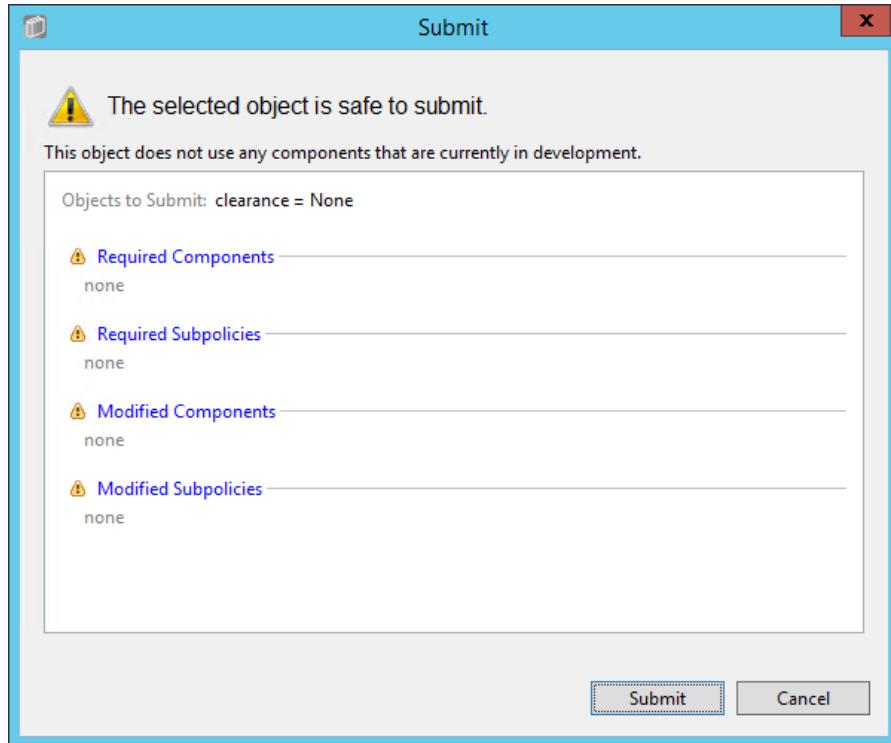
4021



4022

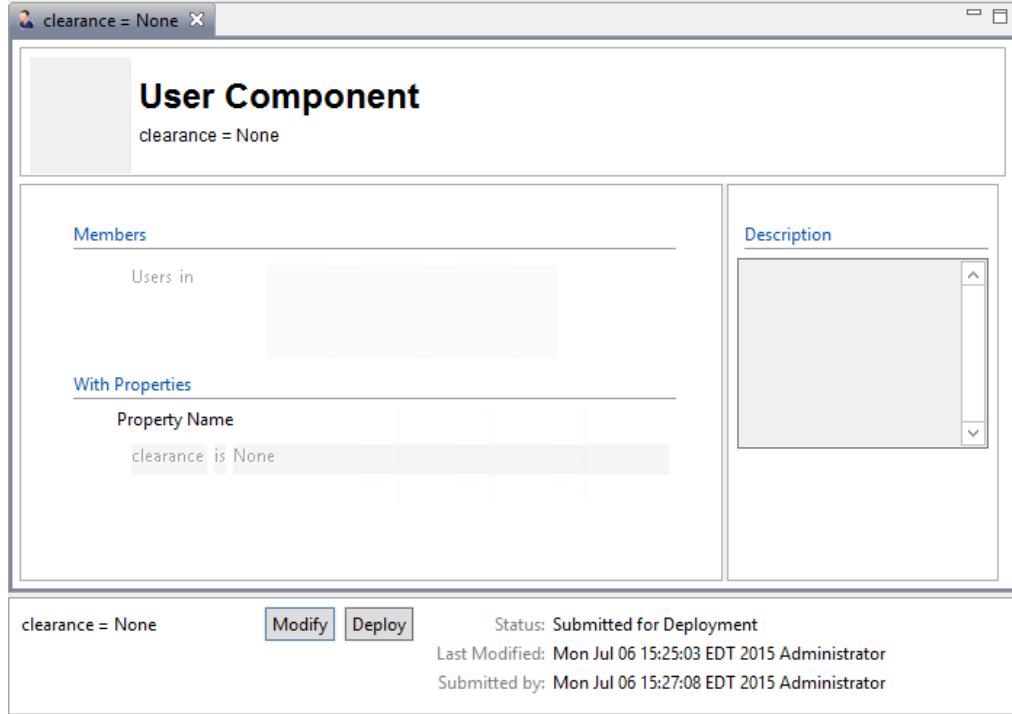
SECOND DRAFT

- 4023 5. In the Submit window, click **Submit**.

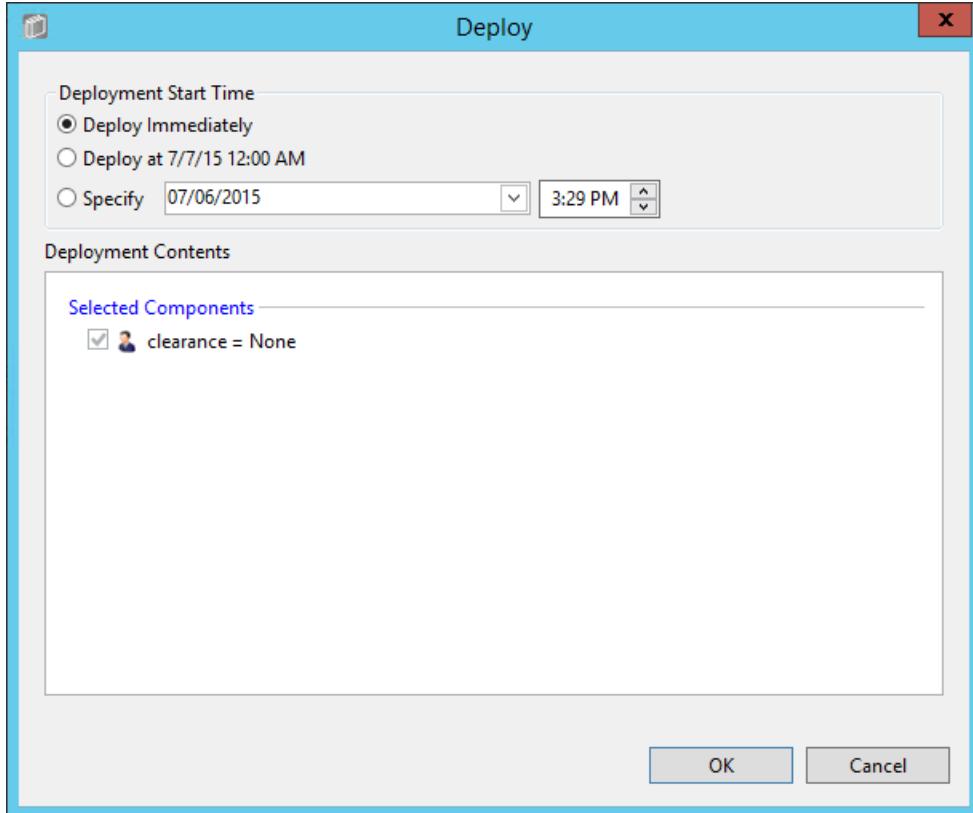


4024

- 4025 6. From the component editing panel, note the differences. The new status reads **Submitted for Deployment**. Click **Deploy**.
- 4026



- 4028 7. In the Deploy window, click **OK**. Note: You may deploy immediately, which we choose in our
 4029 example. You could also deploy the following day at midnight, or at a different specific date and
 4030 time.



- 4031
 4032 8. Verify at the bottom of the component editing panel that the Status now reads **Pending Deployment**. This will remain for the duration of the heartbeat (described in [Section 7](#)).
 4033

clearance = None	Modify	Deploy	Status: Pending Deployment
Last Modified: Mon Jul 06 15:25:03 EDT 2015 Administrator			
Submitted by: Mon Jul 06 15:27:08 EDT 2015 Administrator			

- 4034
 4035 9. After the duration of the heartbeat has passed, Status will then read as **Deployed**. This indicates
 4036 that the component is actively deployed in your ABAC system.

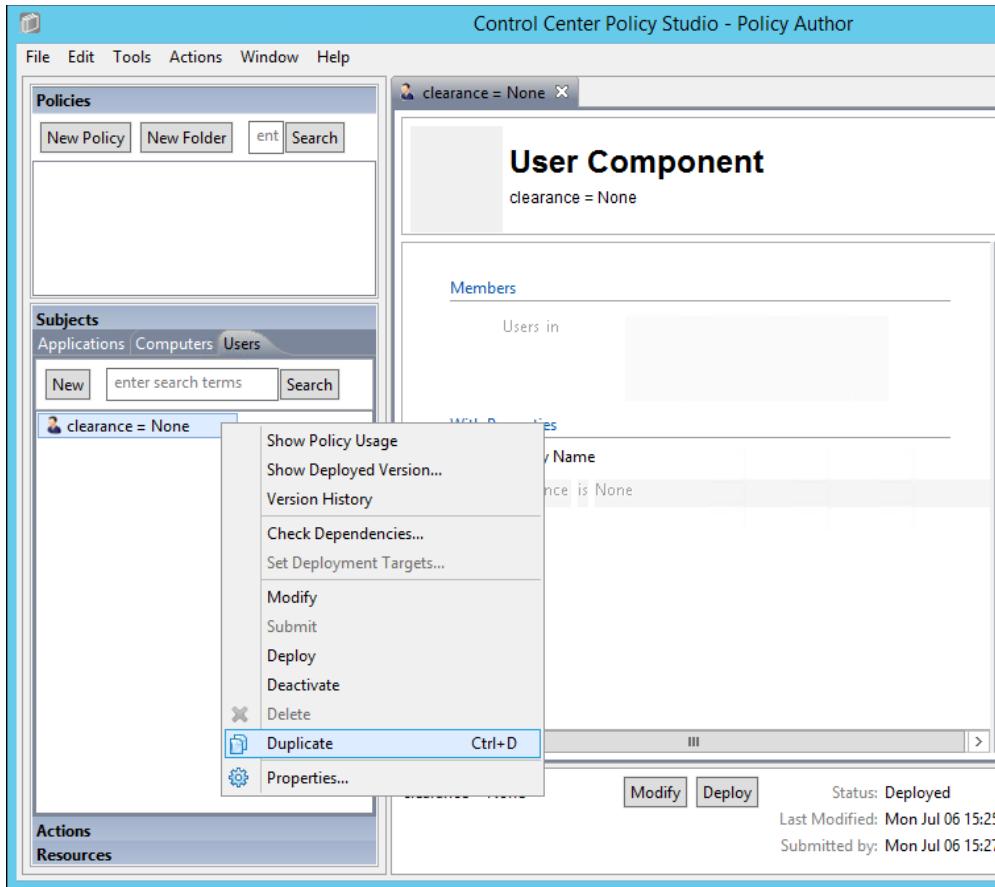
clearance = None	Modify	Deploy	Status: Deployed
Last Modified: Mon Jul 06 15:25:03 EDT 2015 Administrator			
Submitted by: Mon Jul 06 15:27:08 EDT 2015 Administrator			

- 4037

4038 8.4.3.2.1.2 CLEARANCE = SECRET

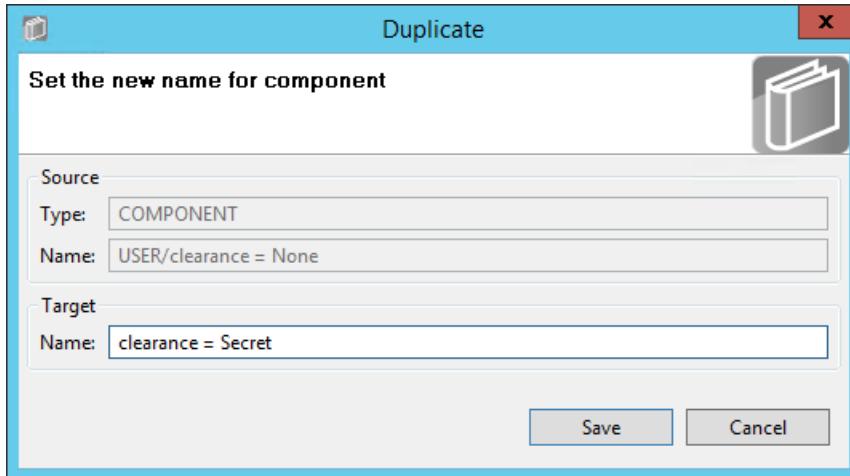
4039 The easiest way to create additional attribute components is to duplicate existing ones. To duplicate the
 4040 existing user attribute component:

- 4041 1. From the Component panel, highlight the name of the existing component, i.e., clearance =
 4042 **None**
- 4043 2. Click on **Edit** from the menu toolbar at the top of the window and select **Duplicate** from the
 4044 drop-down menu, or right-click on the component and select **Duplicate** from the floating menu:



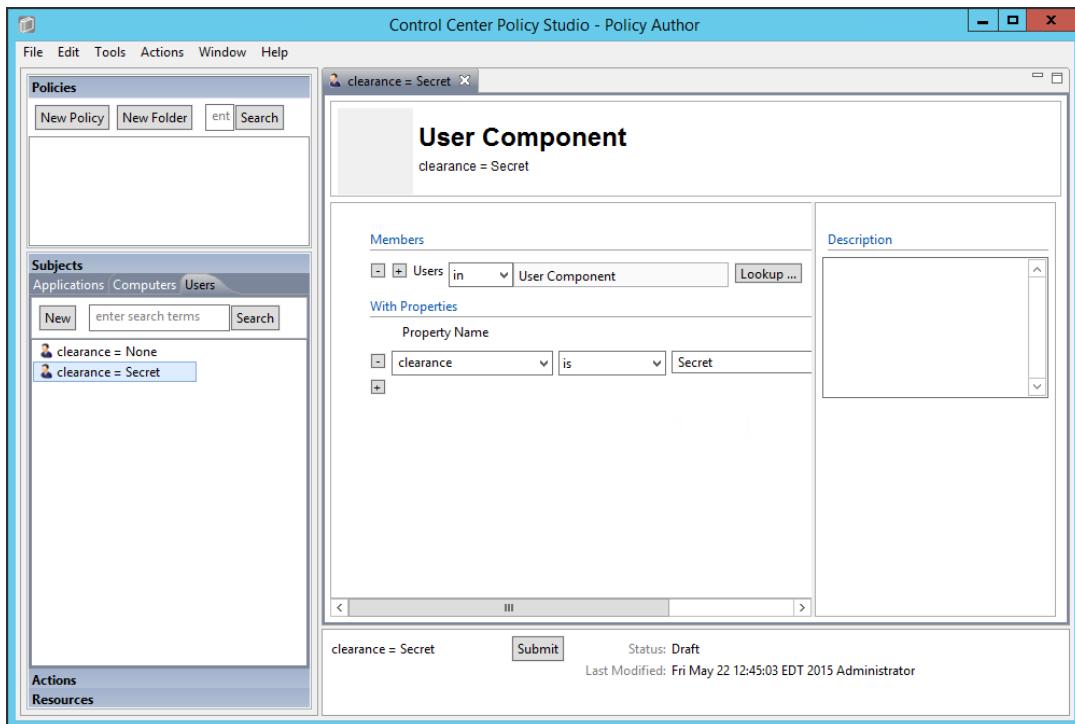
4045

- 4046 3. In the Duplicate window, edit the name of the new component, i.e., clearance = **Secret**. Click
 4047 **Save**.



4048

- 4049 4. Edit the property value to match the component's purpose, i.e., **Secret**. Click **Submit**.



4050

- 4051 5. Repeat steps 5-9 from [Section 8.4.3.2.1.1](#) to Submit and Deploy this component.

4052 8.4.3.2.1.3 CLEARANCE = TOP SECRET

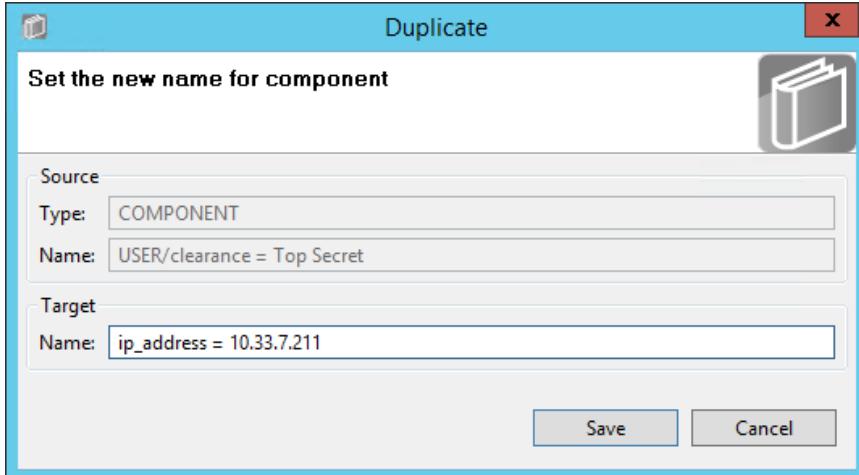
- 4053 1. Repeat steps 1-5 in [Section 8.4.3.2.1.2](#) for duplicating a new user attribute component. The new component should be named **clearance = Top Secret**, and the property value should equal **Top Secret**.

4056 8.4.3.2.2 IP Address component

- 4057 1. Repeat steps 1-3 in [Section 8.4.3.2.1.2](#) for duplicating a new user attribute component. The new component should be named **ip_address = 10.33.7.211**.

4059

- 4060 2. From the component editing panel, edit the **Property Name** to **ip_address** and the value to
 4061 **10.33.7.211**, leaving the default action **is**. Then click **Submit**.



ip_address = 10.33.7.211

User Component

ip_address = 10.33.7.211

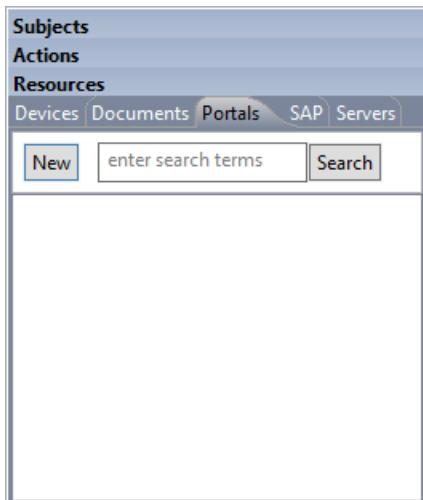
Members	Description
<input type="checkbox"/> <input type="checkbox"/> Users <input type="button" value="in"/> User Component <input type="button" value="Lookup ..."/>	
With Properties	
Property Name <input type="checkbox"/> ip_address <input type="button" value="is"/> <input type="text" value="10.33.7.211"/>	

ip_address = 10.33.7.211 Status: Draft
 Last Modified: Fri Jun 19 16:52:34 EDT 2015 Administrator

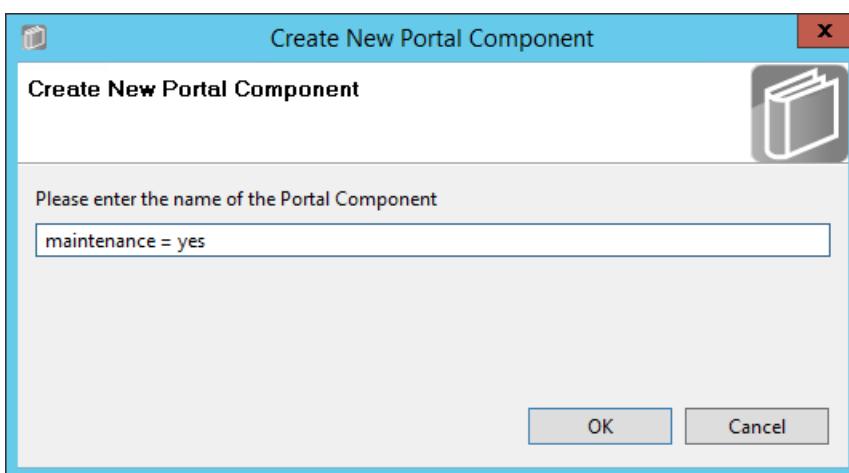
4062

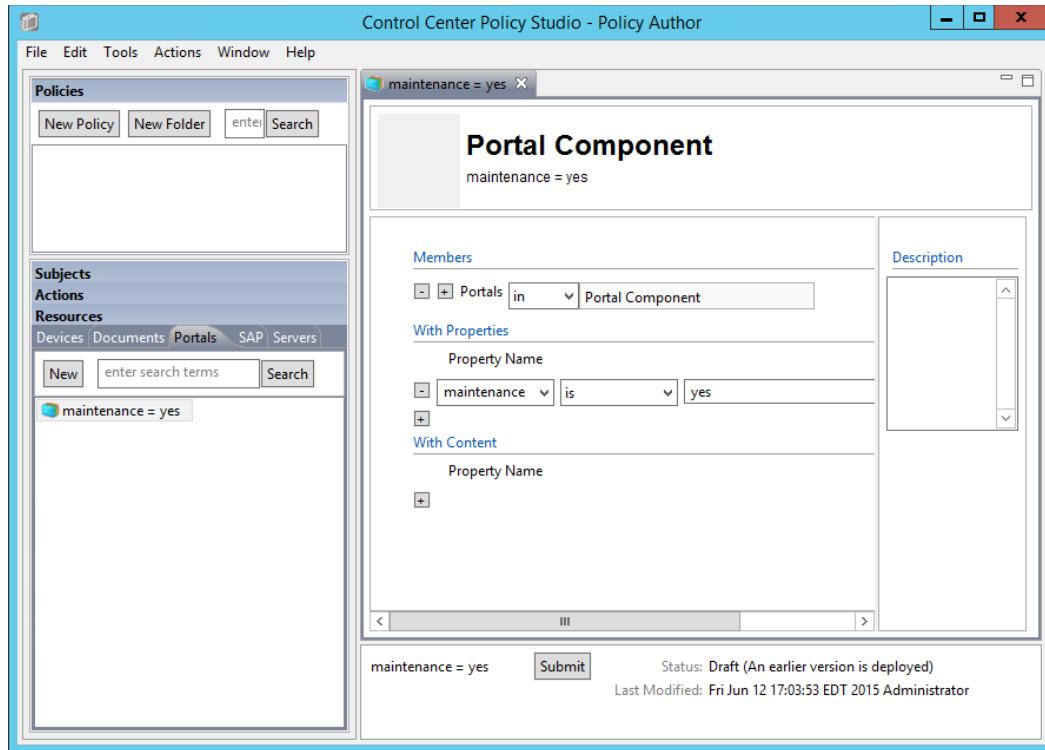
- 4063 3. Repeat steps 5-9 from [Section 8.4.3.2.1.1](#) to Submit and Deploy this component.

- 4064 **8.4.3.3 Defining and Deploying Resource Components**
- 4065 **8.4.3.3.1 Maintenance components**
- 4066 **8.4.3.3.1.1 MAINTENANCE = YES**
- 4067 1. In the Components panel in the bottom-left of the Policy Studio window, click on the **Resources** heading, and then click on the **Portals** tab. Then, click **New** to create a new component.
- 4068



- 4069
- 4070 2. Enter a descriptive component name, such as **maintenance = yes**, then click **OK**.
- 4071
- 4072 3. In the editing panel, click on the **plus sign** box under Property Name and enter **maintenance** in the **Property Name** text box, keep the default **is** as the action, and enter **yes** into the value text box. Then click **Submit**.
- 4073
- 4074





4075

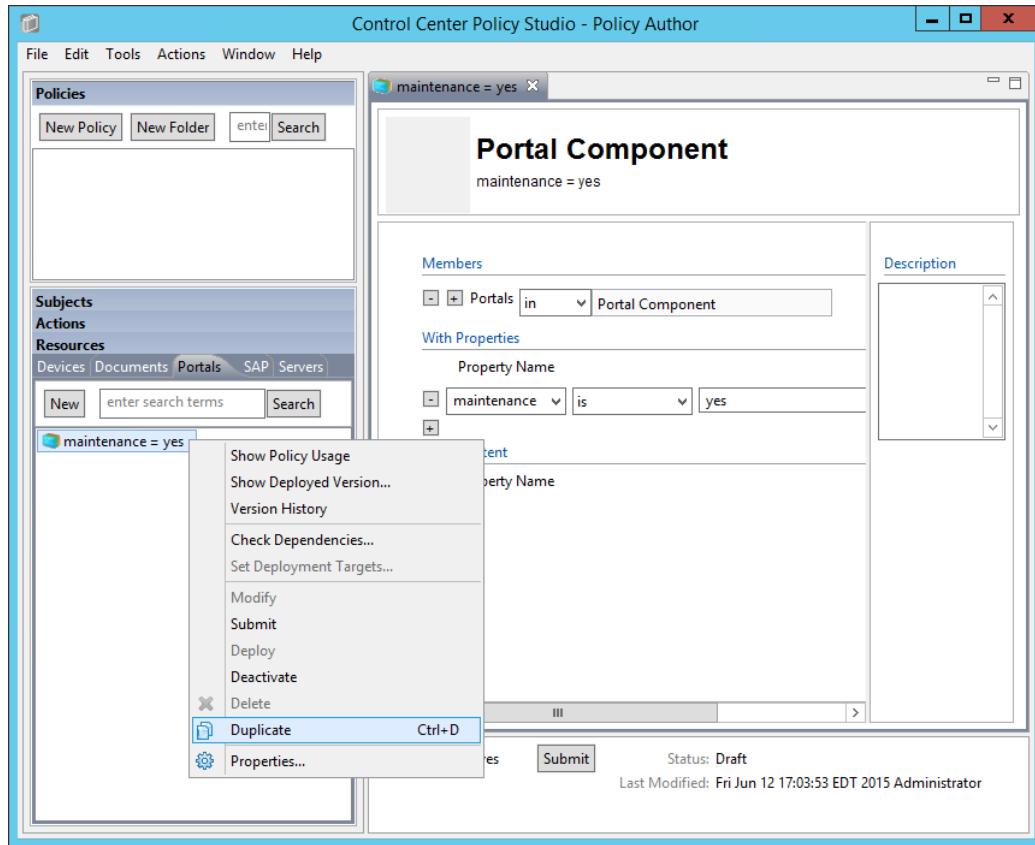
4076 4. Repeat steps 5-9 from [Section 8.4.3.2.1.1](#) to Submit and Deploy this component.

4077 [8.4.3.3.1.2 MAINTENANCE = NO](#)

4078 Similar to the steps taken for duplicating user components, do the following to duplicate the existing
4079 resource maintenance component to create the other resource components.

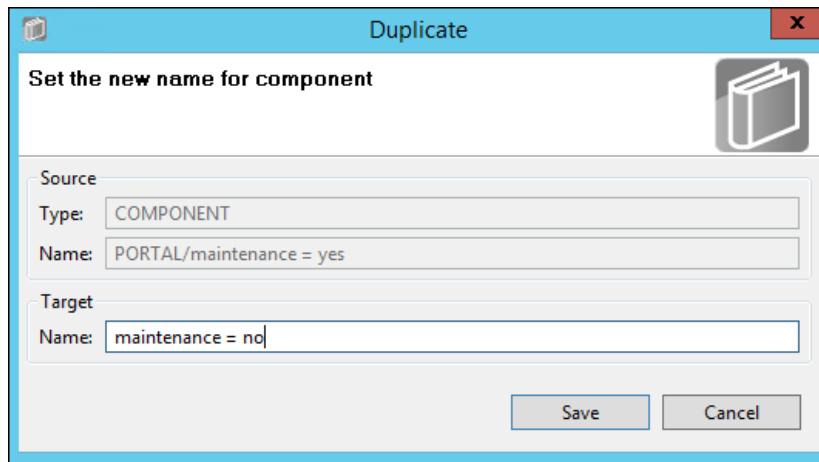
- 4080 1. In the Component panel in the bottom-left corner of the Policy Studio interface, right-click on
4081 the **maintenance = yes** component. In the floating menu, select **Duplicate**.

SECOND DRAFT



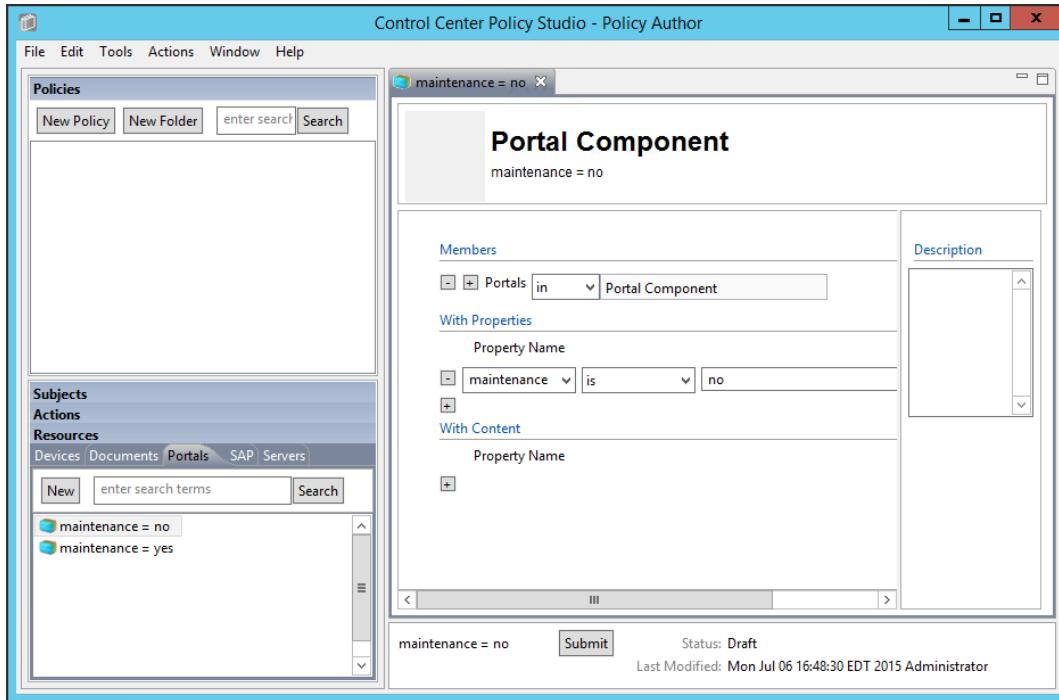
4082

- 4083 2. In the Duplicate window, edit the name of the new component. Example: **maintenance = no**.



4084

- 4085 3. In the component editing panel, change the property value to **no** and click **Submit**.



4086

4087 4. Repeat steps 5-9 from [Section 8.4.3.2.1.1](#) to Submit and Deploy this component.

4088 8.4.3.3.2 Sensitivity components

4089 8.4.3.3.2.1 SENSITIVITY = 1

4090 Repeat steps 1-4 from [Section 8.4.3.3.1.2](#) to duplicate an existing resource component to create the
4091 Sensitivity = 1 component.

4092 8.4.3.3.2.2 SENSITIVITY = 2

4093 Repeat steps 1-4 from [Section 8.4.3.3.1.2](#) to duplicate an existing resource component to create the
4094 Sensitivity = 2 component.

4095 8.4.3.3.2.3 SENSITIVITY = 3

4096 Repeat steps 1-4 from [Section 8.4.3.3.1.2](#) to duplicate an existing resource component to create the
4097 Sensitivity = 3 component.

4098 8.4.3.3.3 Project status component

4099 8.4.3.3.3.1 PROJECT STATUS = ANY

4100 Repeat steps 1-4 from [Section 8.4.3.3.1.2](#) to duplicate an existing resource component to create the
4101 Project status = any component.

4102 Note: Before the Submit step, in the component editing panel, enter the property value as *.

Portal Component

Project status = any

<p>Members</p> <p>- + Portals in ▾ Portal Component</p> <p>With Properties</p> <p>Property Name</p> <p>- project status ▾ is * +</p> <p>With Content</p> <p>Property Name</p> <p>+ [empty]</p>	<p>Description</p> <p>[Empty text area with scroll bars]</p>
<input type="button" value="Project status = any"/> <input type="button" value="Submit"/> Status: Draft <small>Last Modified: Fri Jun 12 15:13:49 EDT 2015 Administrator</small>	

4103

4104 8.4.4 Defining Policy

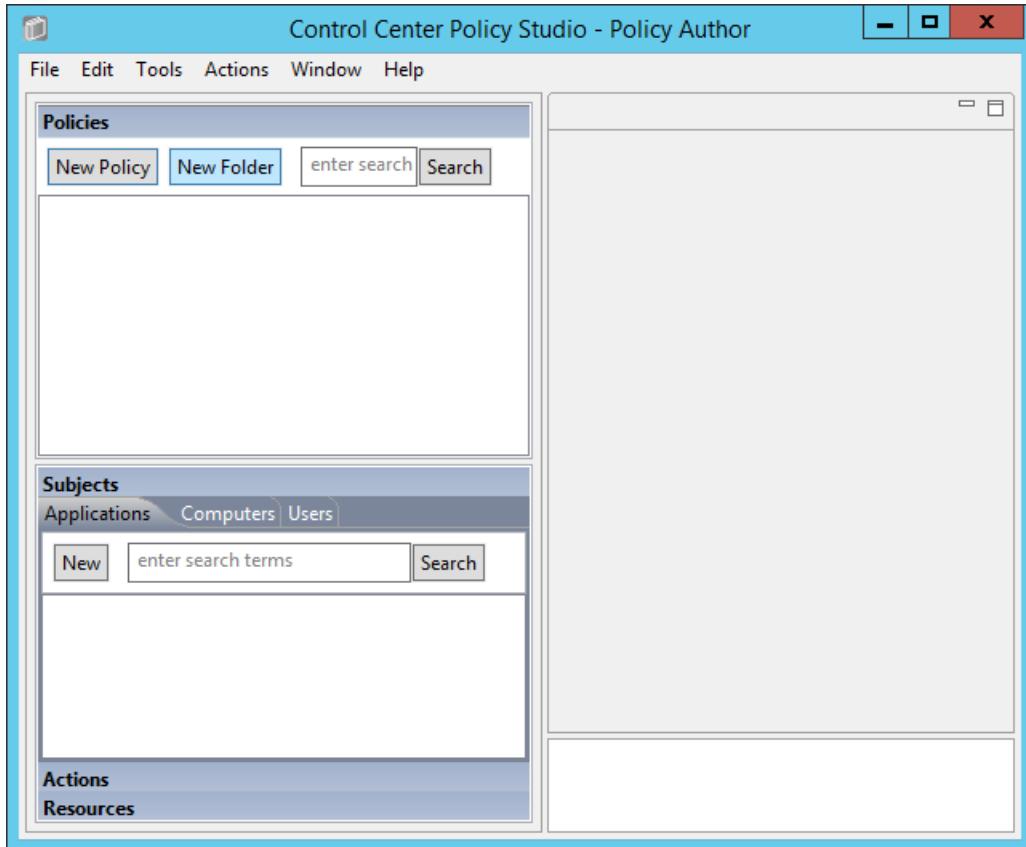
4105 After following the steps to define and deploy components in [Section 8.4.3](#), you can continue on to
 4106 define policies that relate to the Runabout Air scenario business rules discussed in [Section 8.3](#). In order
 4107 to define policies in Policy Studio, login as described in [Section 8.4.1](#).

4108 8.4.4.1 Creating a Policy Set Folder

4109 Before being able to create any policies in Policy Studio, first you must create a folder, or choose an
 4110 existing one.

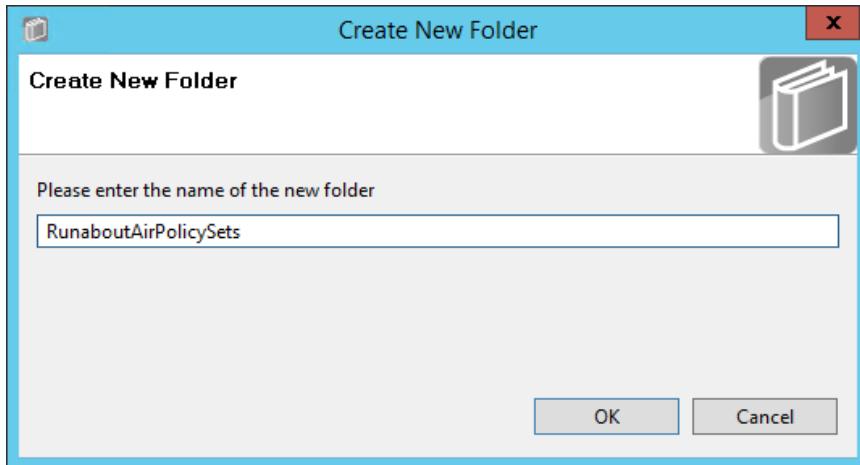
- 4111 1. From the main Policy Studio window, click **New Folder**.

SECOND DRAFT



4112

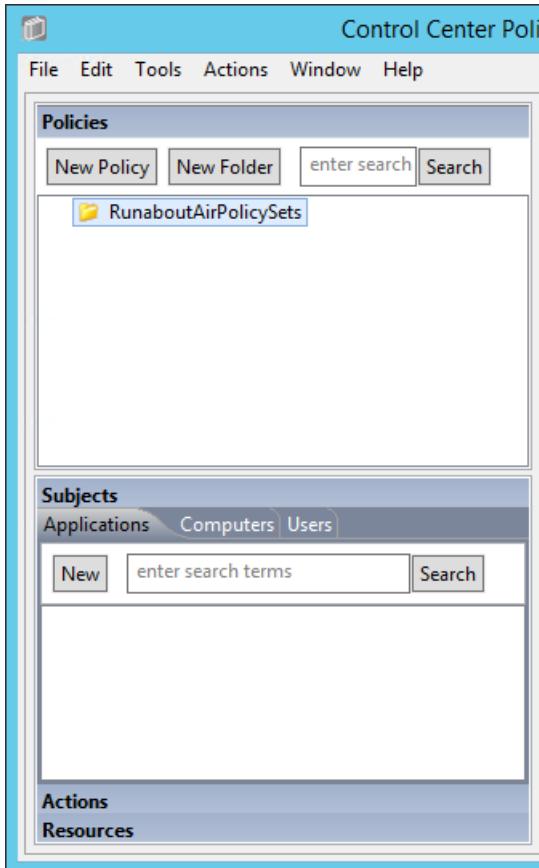
- 4113 2. Enter the **name** of your folder and click **OK**.



4114

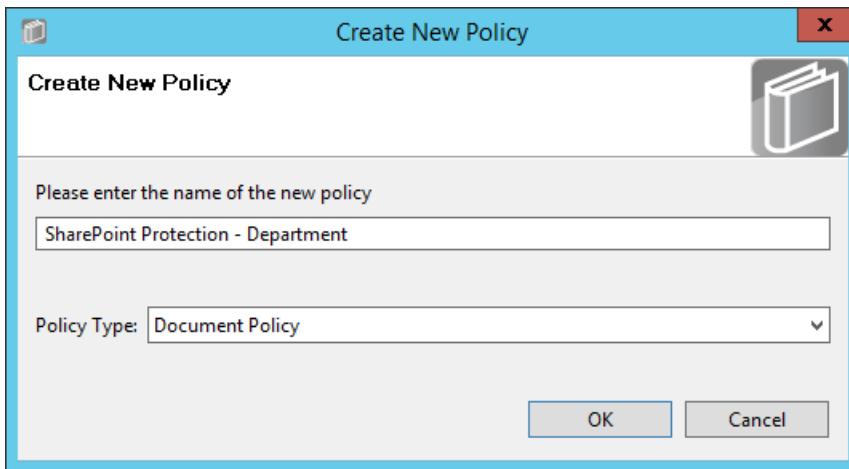
4115 ***8.4.4.2 Defining Department-based Policy Set***4116 ***8.4.4.2.1 Defining the Top-level Department Policy that Enforces a General Deny Decision***

- 4117 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
 4118 folder to highlight it. Then click **New Policy**.



4119

- 4120 2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-down menu, select **Document Policy** (which applies to all SharePoint policies). Click **OK**.



4122

- 4123 3. The new policy opens automatically in an editing panel. For this policy, keep the default **Deny**
4124 enforcement. Make these edits:
- 4125 a. In the On Resources area, click on the **plus sign** box next to **Target**. This automatically
4126 populates **in** and **Resource Component**.
- 4127 b. In the **Condition Expression** enter the ACPL: **(resource.portal.department = "*" AND**
4128 **resource.portal.project status = "*")**
- 4129 c. In the Obligations area, check the **Display User Alert** box in order to customize the deny
4130 message displayed to the user when access is denied.
- 4131 4. In the policy editing panel, your policy should look like this:

SECOND DRAFT

SharePoint Protection - Department

Document Policy

SharePoint Protection - Department

Enforcement: Deny

Subject

- User
- Computer
- Application

Perform the Following

- Action

On Resources

Target
Moved, Renamed or Copied:

Conditions

- Connection Type
- Heartbeat
- Date/Time
 - Start:
 - End:
- Recurrence
 - Time:
 - Day:
- Condition Expression
`(resource.portal.department = "*" AND resource.portal."project status" = "*")`

Subpolicy

Subpolicy

Obligations

On Deny Log
 Display User Alert

SharePoint ... Department Status: Draft
Last Modified: Tue Jul 07 11:34:07 EDT 2015 Administrator

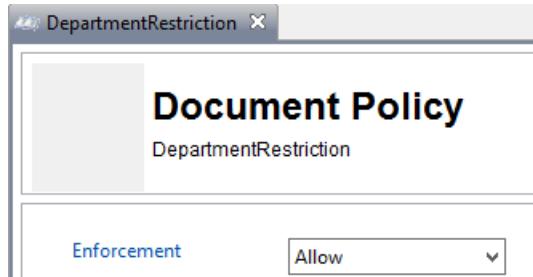
4132

4133

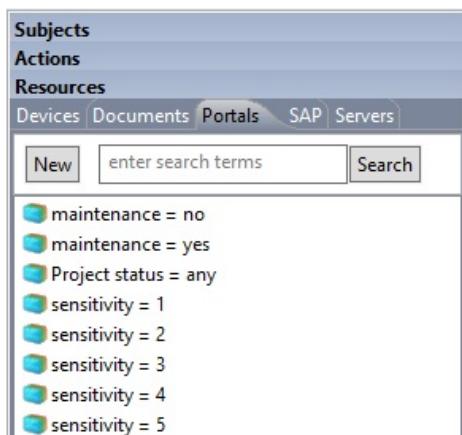
5. To deploy this policy, follow the steps in [Section 8.4.5](#).

4134 8.4.4.2.2 Defining a Department-based Sub-policy that Enforces an Allow Decision when Certain
 4135 Conditions are met

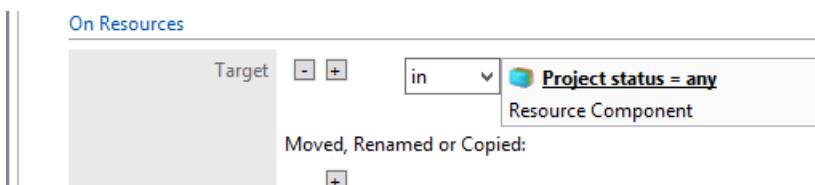
- 4136 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
 4137 policy to highlight it. Then click on **New Policy** to create a sub-policy.
- 4138 2. Select a **name** for the new sub-policy then click **OK**.
- 4139 3. In the policy editing panel, make the following edits:
- 4140 a. From the Enforcement drop-down menu, select **Allow**.



- 4141
- 4142 b. In the On Resources area, click on the **plus sign** box next to **Target**.
- 4143 i. In the Components panel, click on **Resources**, then the **Portals** tab to see the
 4144 components you created earlier.



- 4145
- 4146 ii. From the Portals tab, left-click and hold the **Project status = any** component and
 4147 drag it onto the **Target** field.



- 4148
- 4149 c. In the Conditions area, in the **Condition Expression** text box, enter the ACPL:
- 4150 `(user.department = resource.portal.department OR (user.department =`
 4151 `"Business Intelligence" AND (resource.portal.department = "Marketing" OR`
 4152 `resource.portal.department = "Sales")))`

4153

4154

4. In the Policy Editing panel, your policy should look like this:

The screenshot shows the 'Policies' interface on the left and the 'DepartmentRestriction' policy configuration on the right.

Policies View:

- New Policy
- New Folder
- enter
- Search
- RunaboutAirPolicySets
- SharePoint Protection - Department
- DepartmentRestriction

DepartmentRestriction Policy Configuration:

Conditions:

- Connection Type
- Heartbeat
- Date/Time
 - Start: []
 - End: []
- Recurrence
- Day: []
- Condition Expression
 - (user.department = resource.portal.department OR (user.department = "Business Intelligence" AND (resource.portal.department = "Marketing" OR resource.portal.department = "Sales"))))

Document Policy Configuration:

Enforcement: Allow

Subject:

- User []
- Computer []
- Application []

Perform the Following:

Action []

On Resources:

Target [] in [] Project status = any
Resource Component

Moved, Renamed or Copied: []

Conditions:

- Connection Type
- Heartbeat
- Date/Time
 - Start: []
 - End: []
- Recurrence
- Day: []
- Condition Expression
 - (user.department = resource.portal.department OR (user.department = "Business Intelligence" AND (resource.portal.department = "Marketing" OR resource.portal.department = "Sales"))))

Subpolicy:

Subpolicy [] Subpolicy []

Obligations:

On Allow, Monitor Log
 Display User Alert
 Send Email

DepartmentRestriction Status: Draft
Last Modified: Tue Jul 07 11:20:01 EDT 2015 Administrator

4155

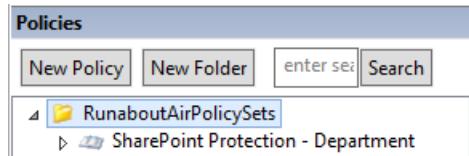
4156 5. To deploy this policy, follow the steps in [Section 8.4.5](#).

4157 **8.4.4.3 Defining a Sensitivity-based Policy Set**

4158 In order to define a sensitivity-based policy set, follow instructions similar to defining the department-
4159 based policy set in [Section 8.4.4.2](#):

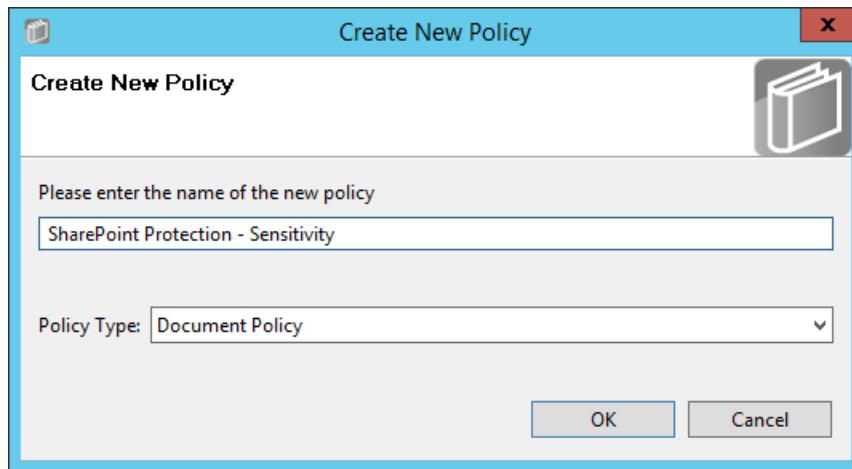
4160 **8.4.4.3.1 Defining the Top-level Sensitivity Policy that Enforces a General Deny Decision**

4161 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your folder
4162 to highlight it. Then click on **New Policy**.



4163

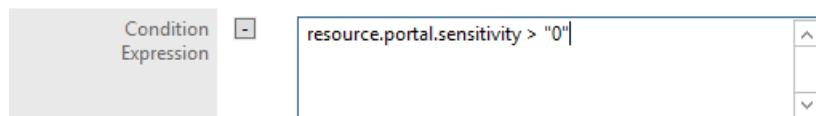
4164 2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-
4165 down menu, select **Document Policy** (which applies to all SharePoint policies). Click **OK**.



4166

4167 3. The new policy opens automatically in an editing panel. For this policy, keep the default **Deny**
4168 enforcement. Make these edits:

- 4169 a. In the On Resources area, click on the **plus sign** box next to **Target**. This automatically
4170 populates **in** and **Resource Component**.
- 4171 b. In Condition Expression enter the ACPL: **resource.portal.sensitivity > "0"**



4172

4173 4. In the Obligations area, check the **Display User Alert** box in order to customize the deny
4174 message displayed to the user when access is denied.

Obligations

On Deny	<input checked="" type="checkbox"/> Log <input checked="" type="checkbox"/> Display User Alert <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">Access denied. Contact your administrator.<div style="text-align: right; margin-top: -10px;">^▼</div></div> <input type="checkbox"/> Send Email <input type="checkbox"/> Custom Obligation
On Allow, Monitor	<input type="checkbox"/> Log <input type="checkbox"/> Display User Alert <input type="checkbox"/> Send Email <input type="checkbox"/> Custom Obligation

4175

4176 5. In the policy editing panel, your policy should look like this:

Document Policy

SharePoint Protection - Sensitivity

Enforcement	Deny
Subject	
User	[+]
Computer	[+]
Application	[+]
Perform the Following	
Action	[+]
On Resources	
Target	[+]
Moved, Renamed or Copied:	
[+]	
Conditions	
Connection Type	[+]
Heartbeat	[+]
Date/Time	Start: [+] End: [+]
Recurrence	Time: [+] Day: [+]
Condition Expression	- resource.portal.sensitivity > "0"
Subpolicy	
Subpolicy	
Obligations	
On Deny	<input checked="" type="checkbox"/> Log <input checked="" type="checkbox"/> Display User Alert

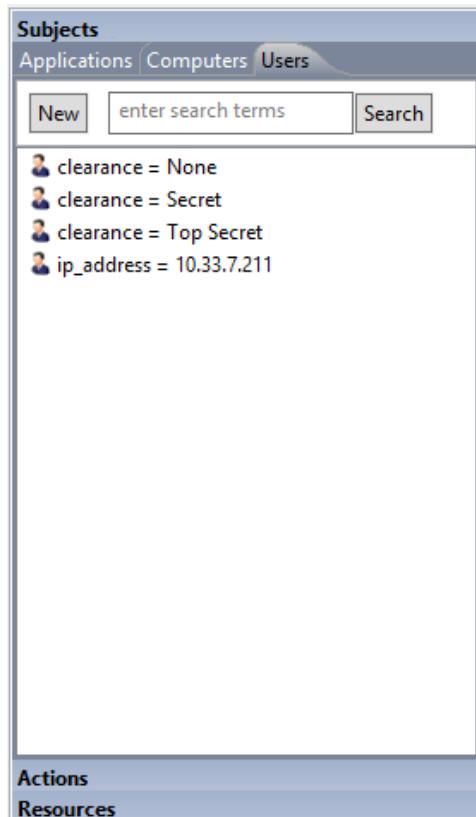
SharePoint Pr...- Sensitivity **Submit** Status: Draft
Last Modified: Tue Jul 07 11:33:41 EDT 2015 Administrator

4177

4178

- To deploy this policy, follow the steps in [Section 8.4.5](#).

- 4179 8.4.4.3.2 Defining a Sensitivity-based Sub-policy that Enforces an Allow Decision when Certain
 4180 Conditions are met for Access to Sensitivity Level 1 Documents
 4181 Similar to the steps in [Section 8.4.4.2.2](#) for creating the Department-based sub-policy, do the following:
- 4182 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
 policy to highlight it. Then click **New Policy** to create a sub-policy.
 - 4184 2. Select a **name** for the new sub-policy then click **OK**.
 - 4185 3. In the policy editing panel, make the following edits:
 - 4186 a. From the **Enforcement** drop-down menu, select **Allow**.
 - 4187 b. In the Subject area, click on the **plus sign** next to User.
 - 4188 i. In the Components panel in the bottom-left corner of the Policy Studio window,
 click on **Subjects**, then the **Users** tab to see the components you created earlier.



- 4190
- 4191 ii. Left-click and hold the **clearance = None** component to drag it onto the **User** field.
 - 4192
 - 4193 iii. Left-click and hold the **clearance = Secret** component to drag it onto the **User** field.
 - 4194
 - 4195 iv. Left-click and hold the **clearance = Top Secret** component to drag it onto the **User** field.
 - 4196

- 4197 c. In the On Resources area, click on the **plus sign** box next to **Target**.
- 4198 i. In the Components panel in the bottom-left corner of the Policy Studio window,
4199 click on **Resources**, then the **Portals** tab to see the components you created
4200 earlier.
- 4201 ii. Left-click and hold the **sensitivity = 1** component to drag it onto the **Target** field.
- 4202 d. In the policy editing panel, your policy should look like this:

Policy1a-Sensitivity Level 1

Document Policy

Policy1a-Sensitivity Level 1

Enforcement Allow

Subject

User in clearance = None
 clearance = Secret
 clearance = Top Secret
User Component

Computer

Application

Perform the Following

Action

On Resources

Target in sensitivity = 1
Resource Component

Moved, Renamed or Copied:

Conditions

Connection Type

Heartbeat

Date/Time Start:
End:

Recurrence Time:
Day:

Condition Expression

Subpolicy

Subpolicy

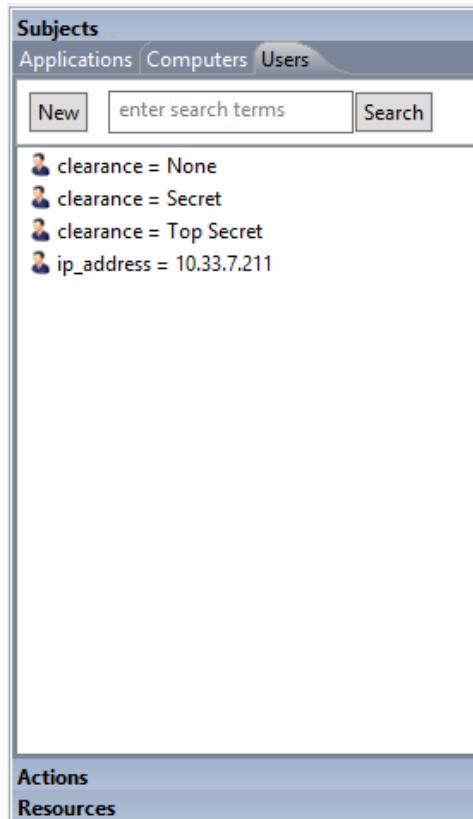
Obligations

Policy1a-Sensitivity Level 1 Status: Draft
Last Modified: Tue Jul 07 11:20:27 EDT 2015 Administrator

4203
4204

- e. To deploy this policy, follow the steps in [Section 8.4.5](#).

- 4205 [8.4.4.3.3 Defining a Sensitivity-based Sub-policy that Enforces an Allow Decision when Certain](#)
4206 [Conditions are met for Access to Sensitivity Level 2 Documents](#)
- 4207 Similar to the steps in [Section 8.4.4.3.2](#) for creating the sensitivity-based sub-policy for sensitivity level 1
4208 documents, do the following:
- 4209 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
4210 policy to highlight it. Then click **New Policy** to create a sub-policy.
 - 4211 2. Select a **name** for the new sub-policy then click **OK**.
 - 4212 3. In the policy editing panel, make the following edits:
 - 4213 a. From the **Enforcement** drop-down menu, select **Allow**.
 - 4214 b. In the Subject area, click on the **plus sign** next to User.
 - 4215 i. In the Components panel in the bottom-left corner of the Policy Studio window,
4216 click on **Subjects**, then the **Users** tab to see the components you created earlier.



- 4217
- 4218 ii. Left-click and hold the **clearance = Secret** component to drag it onto the **User** field.
 - 4219 iii. Left-click and hold the **clearance = Top Secret** component to drag it onto the **User** field.
- 4220
- 4221 c. In the On Resources area, click on the **plus sign** box next to **Target**.

- 4223 i. In the Components panel in the bottom-left corner of the Policy Studio window,
4224 click on **Resources**, then the **Portals** tab to see the components you created
4225 earlier.
- 4226 ii. Left-click and hold the **sensitivity = 2** component to drag it onto the **Target** field.
- 4227 d. In the Conditions area, click on the **plus sign** boxes next to **Time** and **Day**. Edit those
4228 fields to match below:

Conditions

Connection Type	[+]																		
Heartbeat	[+]																		
Date/Time	Start: [+] End: [+]																		
Recurrence	Time: [-] From 6:00 AM [^] To 6:00 PM [^] Day: [-] <table border="1"><tr><td>Sun</td><td>Mon</td><td>Tue</td><td>Wed</td><td>Thu</td><td>Fri</td><td>Sat</td></tr><tr><td><input checked="" type="radio"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td><input type="radio"/></td><td>Day <input type="text" value="1"/> of every month</td></tr><tr><td><input type="radio"/></td><td>The <input type="text" value="First"/> <input type="text" value="Sunday"/> of every month</td></tr></table>	Sun	Mon	Tue	Wed	Thu	Fri	Sat	<input checked="" type="radio"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>	Day <input type="text" value="1"/> of every month	<input type="radio"/>	The <input type="text" value="First"/> <input type="text" value="Sunday"/> of every month
Sun	Mon	Tue	Wed	Thu	Fri	Sat													
<input checked="" type="radio"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>													
<input type="radio"/>	Day <input type="text" value="1"/> of every month																		
<input type="radio"/>	The <input type="text" value="First"/> <input type="text" value="Sunday"/> of every month																		
Condition Expression	[+]																		

- 4229
- 4230 4. In the policy editing panel, your policy should look like this:

Policy1b-Sensitivity Level 2

Document Policy

Policy1b-Sensitivity Level 2

Enforcement: Allow

Subject

- User: in **clearance = Secret**, **clearance = Top Secret** User Component
- Computer: +
- Application: +

Perform the Following

Action: +

On Resources

- Target: in **sensitivity = 2** Resource Component

Moved, Renamed or Copied: +

Conditions

Connection Type: +

Heartbeat: +

Date/Time

- Start: +
- End: +
- Time: From 6:00 AM To 6:00 PM
- Day: +

Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Day 1 of every month						
<input type="radio"/>	The First Sunday of every month					

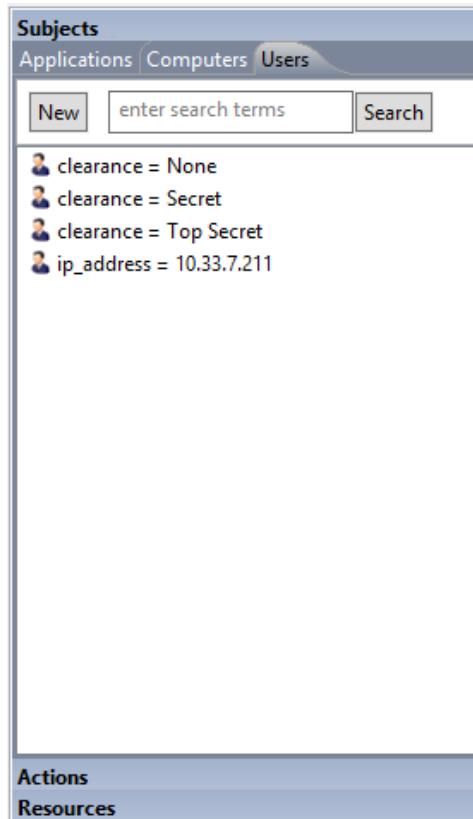
Condition Expression: +

Policy1b-Sensitivity Level 2 **Submit** Status: Draft
Last Modified: Tue Jul 07 11:20:27 EDT 2015 Administrator

4231

4232 5. To deploy this policy, follow the steps in [Section 8.4.5](#).

- 4233 8.4.4.3.4 Defining a Sensitivity-based Sub-policy that Enforces an Allow Decision when Certain
 4234 Conditions are met for Access to Sensitivity Level 3 Documents
 4235 Similar to the steps in [Section 8.4.4.3.2](#) for creating the sensitivity-based sub-policy for sensitivity level 1
 4236 documents, do the following:
- 4237 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
 4238 policy to highlight it. Then click **New Policy** to create a sub-policy.
 - 4239 2. Select a **name** for the new sub-policy then click **OK**.
 - 4240 3. In the policy editing panel, make the following edits:
 - 4241 a. From the **Enforcement** drop-down menu, select **Allow**.
 - 4242 b. In the Subject area, click on the **plus sign** next to User.
 - 4243 i. In the Components panel in the bottom-left corner of the Policy Studio window,
 4244 click on **Subjects**, then the **Users** tab to see the components you created earlier.



- 4245
- 4246 ii. Left-click and hold the **clearance = Top Secret** component to drag it onto the
 4247 **User** field.
 - 4248 c. In the On Resources area, click on the **plus sign** box next to **Target**.
 - 4249 i. In the Components panel in the bottom-left corner of the Policy Studio window,
 4250 click on **Resources**, then the **Portals** tab to see the components you created
 4251 earlier.

- 4252 ii. Left-click and hold the **sensitivity = 3** component to drag it onto the **Target** field.
- 4253 d. In the Conditions area, click on the **plus sign** boxes next to **Time** and **Day**. Edit those
4254 fields to match below:

Conditions

Connection Type	[+]																																			
Heartbeat	[+]																																			
Date/Time	Start: [+] End: [+]																																			
Recurrence	Time: [-] From 6:00 AM [^] To 6:00 PM [^] Day: [-] <table border="1"><tr><td>Sun</td><td>Mon</td><td>Tue</td><td>Wed</td><td>Thu</td><td>Fri</td><td>Sat</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td></tr><tr><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td></tr><tr><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td><td><input type="radio"/></td></tr></table> <input type="radio"/> Day <input type="text" value="1"/> of every month <input type="radio"/> The <input type="text" value="First"/> <input type="text" value="Sunday"/> of every month	Sun	Mon	Tue	Wed	Thu	Fri	Sat	<input checked="" type="checkbox"/>	<input type="radio"/>																										
Sun	Mon	Tue	Wed	Thu	Fri	Sat																														
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																														
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>																														
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>																														
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>																														
Condition Expression	[+]																																			

- 4255
- 4256 4. In the policy editing panel, your policy should look like this:

Document Policy
Policy1c-Sensitivity Level 3

Enforcement: Allow

Subject:

- User: clearance = Top Secret
- Computer: [+] (disabled)
- Application: [+] (disabled)

Perform the Following:

Action: [+]

On Resources:

Target: sensitivity = 3

Moved, Renamed or Copied:

Conditions:

Connection Type: [+]

Heartbeat: [+]

Date/Time:

- Start: [+]
- End: [+]
- Time: From 6:00 AM To 6:00 PM
- Day: [+]
 - Sun Mon Tue Wed Thu Fri Sat
 - Mon, Tue, Wed, Thu, Fri, Sun are checked
 - Sat is unchecked
 - Day 1 of every month
 - The First Sunday of every month

Condition Expression: [+]

Description: (empty)

Tags:

Name: (empty)

Value: (empty)

Name: (empty)

< >

Policy1c-Sensitivity Level 3 Submit Status: Draft
Last Modified: Tue Jul 07 11:20:27 EDT 2015 Administrator

4257

4258 5. To deploy this policy, follow the steps in [Section 8.4.5](#).

8.4.4.4 Defining a Maintenance-based Policy Set

4260 In order to define a maintenance-based policy set, follow instructions similar to defining the
 4261 department-based policy set in [Section 8.4.4.2](#):

4262 8.4.4.4.1 Defining the Top-level Maintenance Policy that Enforces a General Deny Decision

- 4263 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
4264 folder to highlight it. Then click **New Policy**.
- 4265 2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-
4266 down menu, select **Document Policy** (which applies to all SharePoint policies). Click **OK**.
- 4267 3. The new policy opens automatically in an editing panel. For this policy, keep the default **Deny**
4268 enforcement. Make these edits:
- 4269 a. In the On Resources area, click on the **plus sign** box next to **Target**. This automatically
4270 populates **in** and **Resource Component**.
- 4271 b. In **Condition Expression**, enter the ACPL: **resource.portal.maintenance = “*”**
- 4272 c. In the Obligations area, check the **Display User Alert** box in order to customize the deny
4273 message displayed to the user when access is denied.
- 4274 4. In the policy editing panel, your policy should look like this:

Document Policy

SharePoint Protection - Maintenance

Enforcement	Deny	Description
Subject	User Computer Application	Tags
Perform the Following	Action On Resources Target Moved, Renamed or Copied: +	Name: Value:
Conditions	Connection Type Heartbeat Date/Time Start: End: Recurrence Time: Day: Condition Expression resource.portal.maintenance = "*"	Name
Subpolicy	Subpolicy	
Obligations	On Deny <input checked="" type="checkbox"/> Log <input checked="" type="checkbox"/> Display User Alert	
<input type="button" value="SharePoint ...Maintenance"/> <input type="button" value="Submit"/> Status: Draft Last Modified: Tue Jul 07 11:20:18 EDT 2015 Administrator		

4275

4276 5. To deploy this policy, follow the steps in [Section 8.4.5](#).

4277 8.4.4.4.2 Defining a Maintenance-based Sub-policy that Enforces an Allow Decision when Certain
 4278 Conditions are met for Access to Documents whose Maintenance Attribute is defined as Yes
 4279 Similar to the instructions in [Section 8.4.4.2.2](#) for defining a Department-based sub-policy, do the
 4280 following:

- 4281 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
 4282 policy to highlight it. Click **New Policy** to create a sub-policy under this main policy.
- 4283 2. Select a **name** for the new sub-policy, then click **OK**.
- 4284 3. In the policy editing panel, make the following edits:
 - 4285 a. From the **Enforcement** drop-down menu, select **Allow**.
 - 4286 b. In the On Resources area, click on the **plus sign** box next to **Target**.
 - 4287 i. In the Components panel in the bottom-left corner of the Policy Studio window,
 4288 click on **Resources**, then the **Portals** tab to see the components you created
 4289 earlier.
 - 4290 ii. Left-click and hold the **maintenance = yes** component to drag it onto the **Target**
 4291 field.
 - 4292 c. In the Conditions area, click on the **plus sign** boxes next to **Time** and **Day**. Edit those
 4293 fields to match below:

Conditions

Connection Type	[+]
Heartbeat	[+]
Date/Time	Start: [+] End: [+]
Recurrence	Time: [-] From 6:00 PM To 6:00 AM Day: [-] <div style="border: 1px solid #ccc; padding: 5px; width: fit-content;"> Sun <input checked="" type="radio"/> Mon <input checked="" type="radio"/> Tue <input checked="" type="radio"/> Wed <input checked="" type="radio"/> Thu <input checked="" type="radio"/> Fri <input checked="" type="radio"/> Sat <input checked="" type="radio"/> Day <input type="text" value="1"/> of every month The <input type="text" value="First"/> <input type="text" value="Sunday"/> of every month </div>
Condition Expression	[+]

4294

- 4295 4. In the policy editing panel, your policy should look like this:

Allow Maintenance After 6pm and Weekends

Document Policy

Allow Maintenance After 6pm and Weekends

Enforcement Allow

Subject

- User +
- Computer +
- Application +

Perform the Following

Action +

On Resources

Target in **maintenance = yes**
Resource Component

Moved, Renamed or Copied: +

Conditions

Connection Type +

Heartbeat +

Date/Time Start: + End: +

Recurrence Time: From 6:00 PM To 6:00 AM
Day: Sun Mon Tue Wed Thu Fri Sat
 Sun Mon Tue Wed Thu Fri Sat
 Day 1 of every month
 The First Sunday of every month

Condition Expression +

Subpolicy

Allow Maintenance After 6pm and Weekends **Submit** Status: Draft
Last Modified: Tue Jul 07 11:20:18 EDT 2015 Administrator

4296

4297

5. To deploy this policy, follow the steps in [Section 8.4.5](#).

- 4298 8.4.4.4.3 Defining a Maintenance-based Sub-policy that Enforces an Allow Decision when Certain
4299 Conditions are met for Access to Documents whose Maintenance Attribute is defined as No
4300 Similar to the instructions in [Section 8.4.4.2.2](#) for defining a Department-based sub-policy, do the
4301 following:
- 4302 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
4303 policy to highlight it. Click **New Policy** to create a sub-policy.
- 4304 2. Select a **name** for the new sub-policy, then click **OK**.
- 4305 3. In the policy editing panel, make the following edits:
- 4306 a. From the **Enforcement** drop-down menu, select **Allow**.
- 4307 b. In the On Resources area, click on the **plus sign** box next to **Target**.
- 4308 i. In the Components panel in the bottom-left corner of the Policy Studio window,
4309 click on **Resources**, then the **Portals** tab to see the components you created
4310 earlier.
- 4311 ii. Left-click and hold the **maintenance = no** component to drag it onto the **Target**
4312 field.
- 4313 4. In the policy editing panel, your policy should look like this:

SECOND DRAFT

Allow Non-Maintenance Any Time

Document Policy

Allow Non-Maintenance Any Time

Enforcement: Allow

Subject:

- User
- Computer
- Application

Perform the Following:

Action: +

On Resources:

Target: +
Moved, Renamed or Copied: +

Conditions:

- Connection Type: +
- Heartbeat: +
- Date/Time:
 - Start: +
 - End: +
- Recurrence:
 - Time: +
 - Day: +
- Condition Expression: +

Subpolicy:

Subpolicy: Subpolicy

Obligations:

On Allow, Monitor:

- Log
- Display User Alert
- Send Email
- Custom Obligation

Allow Non-Maintenance Any Time

Status: Draft

Last Modified: Tue Jul 07 16:10:37 EDT 2015 Administrator

4314

4315 5. To deploy this policy, follow the steps in [Section 8.4.5](#).

4316 **8.4.4.5 Defining an IP Address-based Policy Set**

4317 In order to define an IP address-based policy set, follow instructions similar to defining the department-
4318 based policy set in [Section 8.4.4.2](#).

4319 **8.4.4.5.1 Defining the top-level IP Address Policy that Enforces a General Deny Decision**

4320 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
4321 folder to highlight it. Then click **New Policy**.

4322 2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-
4323 down menu, select Document Policy (which applies to all SharePoint policies). Click **OK**.

4324 3. The new policy opens automatically in an editing panel. For this policy, keep the default **Deny**
4325 enforcement. Make these edits:

4326 4. In the **Condition Expression**, enter the ACPL: **resource.portal.sensitivity = “*”**

4327 5. In the Obligations area, check the **Display User Alert** box in order to customize the deny
4328 message displayed to the user when access is denied.

4329 6. In the policy editing panel, your policy should look like this:

Document Policy
SharePoint Protection - IP Address

Enforcement: Deny

Subject

- User
- Computer
- Application

Perform the Following

Action: [+] Moved, Renamed or Copied: [+]

On Resources

Target: [+] Moved, Renamed or Copied: [+]

Conditions

- Connection Type
- Heartbeat
- Date/Time

 - Start: [+]
 - End: [+]

- Recurrence

 - Time: [+]
 - Day: [+]

- Condition Expression: resource.portal.sensitivity = "*" [-]

Subpolicy

Obligations

On Deny: Log Display User Alert

SharePoint P...- IP Address Status: Draft
Last Modified: Tue Jul 07 12:38:19 EDT 2015 Administrator

4330

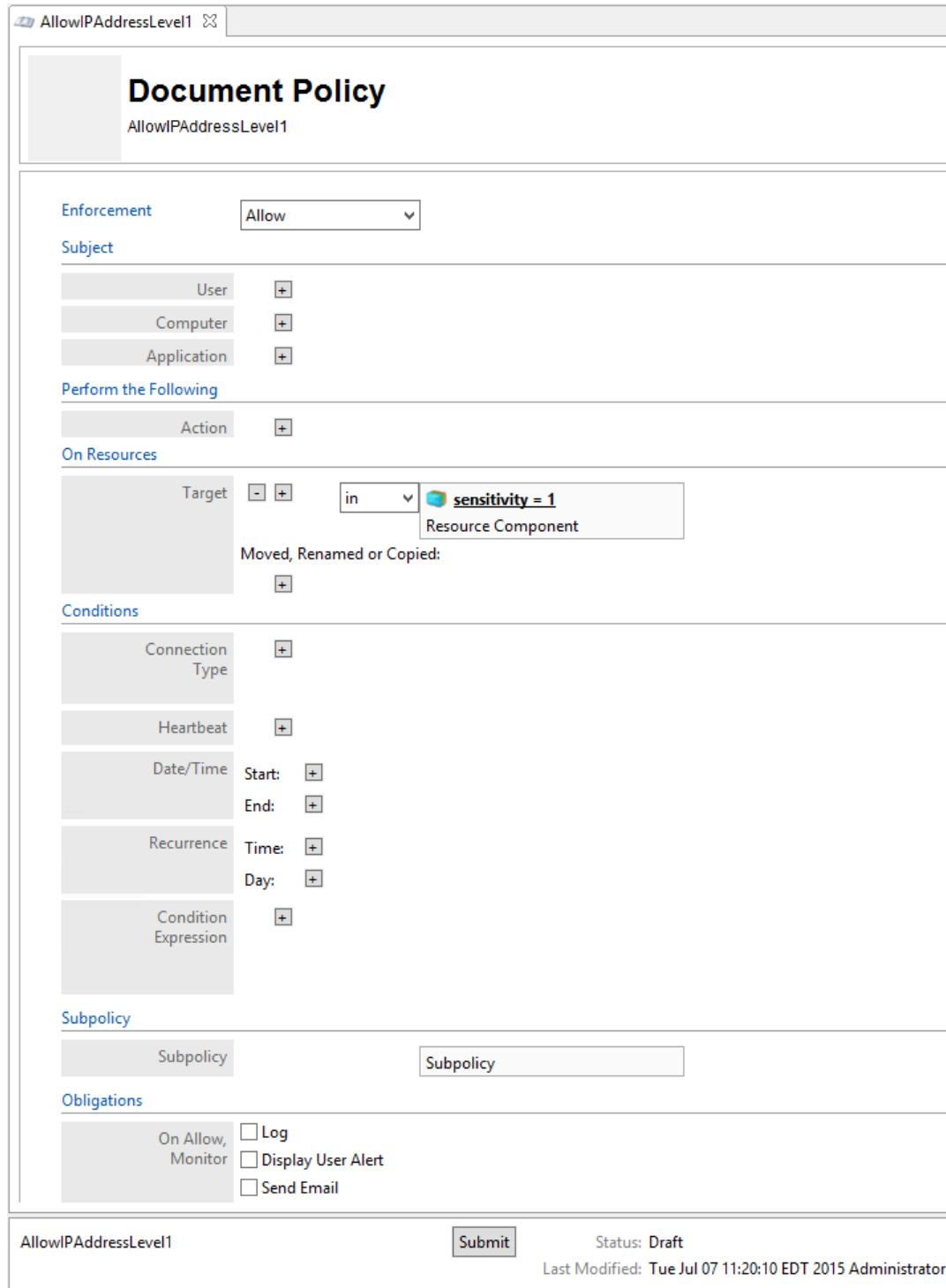
4331 7. To deploy this policy, follow the steps in [Section 8.4.5](#).

4332 8.4.4.5.2 Defining an IP Address-based Sub-policy that Enforces an Allow Decision for Access to
 4333 Resources at any Sensitivity Level when a User does not come from an Environment with a
 4334 Restricted IP Address (ex: 10.33.7.211)

4335 Similar to the instructions in [Section 8.4.4.2.2](#) for defining a Department-based sub-policy, do the
 4336 following:

4337 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
 4338 policy to highlight it. Click **New Policy** to create a sub-policy.

- 4339 2. Select a **name** for the new sub-policy, then click **OK**.
- 4340 3. In the policy editing panel, make the following edits:
- 4341 a. From the **Enforcement** drop-down menu, select **Allow**.
- 4342 b. In the On Resources area, click on the **plus sign** box next to **Target**.
- 4343 i. In the Components panel in the bottom-left corner of the Policy Studio window,
4344 click on **Resources**, then the **Portals** tab to see the components you created
4345 earlier.
- 4346 ii. Left-click and hold the **sensitivity = 1** component to drag it onto the **Target** field.
- 4347 4. In the policy editing panel, your policy should look like this:

A screenshot of a software interface titled "AllowIPAddressLevel1" showing the configuration of a "Document Policy". The policy is named "AllowIPAddressLevel1". The interface includes sections for Enforcement (set to "Allow"), Subject (User, Computer, Application), Perform the Following (Action), On Resources (Target set to "in" with a sensitivity level of 1, Resource Component), Conditions (Connection Type, Heartbeat, Date/Time, Recurrence, Condition Expression), Subpolicy (Subpolicy), and Obligations (On Allow, Monitor options: Log, Display User Alert, Send Email). The status is listed as "Draft" with a last modified date of "Tue Jul 07 11:20:10 EDT 2015" and author "Administrator".

Allow	Enforcement
User Computer Application	Subject
Action	Perform the Following
Target in sensitivity = 1 Resource Component	On Resources
Connection Type Heartbeat Date/Time Start: End: Recurrence Time: Day: Condition Expression	Conditions
Subpolicy	Subpolicy
On Allow, Monitor Log Display User Alert Send Email	Obligations
AllowIPAddressLevel1	Status: Draft Last Modified: Tue Jul 07 11:20:10 EDT 2015 Administrator

4348

4349 5. To deploy this policy, follow the steps in [Section 8.4.5](#).

4350 8.4.4.5.3 Defining an IP Address-based Sub-policy that Enforces an Allow Decision for Access to
 4351 Resources at Only Sensitivity Level 1 when a User comes from an Environment with a
 4352 Restricted IP Address (ex: 10.33.7.211)

4353 Similar to the instructions in [Section 8.4.4.2.2](#) for defining a Department-based sub-policy, do the
 4354 following:

4355 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new
 4356 policy to highlight it. Then click **New Policy** to create a sub-policy.

4357 2. Select a **name** for the new sub-policy, then click **OK**.

4358 3. In the policy editing panel, make the following edits:

4359 a. From the **Enforcement** drop-down menu, select **Allow**.

4360 b. In the Subject area, click on the **plus sign** box next to **User**.

4361 i. From the drop-down menu, select **not in**.

4362 ii. In the Components panel in the bottom-left corner of the Policy Studio window,
 4363 click on **Subjects**, then the **Users** tab to see the components you created earlier.

4364 1. Left-click and hold the **ip_address=10.33.7.211** component to drag it
 4365 onto the **User** field.



4366

4367 c. In the On Resources area, click on the **plus sign** box next to **Target**.

4368 i. In the Components panel in the bottom-left corner of the Policy Studio window,
 4369 click on **Resources**, then the **Portals** tab to see the components you created
 4370 earlier.

4371 ii. Left-click and hold the **sensitivity = 1** component to drag it onto the **Target** field.

4372 iii. Left-click and hold the **sensitivity = 2** component to drag it onto the **Target** field.

4373 iv. Left-click and hold the **sensitivity = 3** component to drag it onto the **Target** field.

4374 4. In the policy editing panel, your policy should look like this:

SECOND DRAFT

AllowSensitiveLevelsToAnyOtherIP

Document Policy

AllowSensitiveLevelsToAnyOtherIP

Enforcement: Allow

Subject:

User: not in ip address = 10.33.7.211 (User Component)

Computer: +

Application: +

Perform the Following:

Action: +

On Resources:

Target: in sensitivity = 2, sensitivity = 3, sensitivity = 1 (Resource Component)

Moved, Renamed or Copied: +

Conditions:

Connection Type: +

Heartbeat: +

Date/Time: Start: +, End: +

Recurrence: Time: +, Day: +

Condition Expression: +

Subpolicy:

Subpolicy: Subpolicy

Obligations:

On Allow: Log

AllowSensitiveLevelsToAnyOtherIP

Status: Draft

Last Modified: Tue Jul 07 11:20:10 EDT 2015 Administrator

4375

4376

5. To deploy this policy, follow the steps in [Section 8.4.5](#).

4377 **8.4.5 Deploying Policy**

4378 In order to deploy policies, follow steps similar to those for deploying a component (see
 4379 [Section 8.4.3.2.1.1](#)):

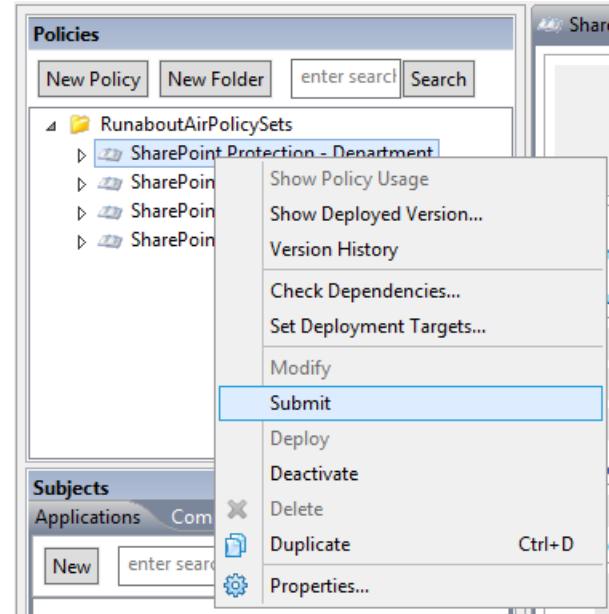
- 4380 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on the policy
 4381 you want to deploy. In the policy editing panel, click **Submit**.

The screenshot shows the 'Document Policy' configuration window in the Policy Studio. The window title is 'SharePoint Protection - Department'. The left panel contains sections for 'Enforcement' (set to 'Deny'), 'Subject' (User, Computer, Application), 'Perform the Following' (Action), 'On Resources' (Target, Moved, Renamed or Copied), and 'Conditions' (Connection Type). The right panel contains sections for 'Description' (empty), 'Tags' (Name and Value fields, Add button), and a table for conditions. At the bottom, there are buttons for 'SharePoint...Department' and 'Submit' (disabled), and status information: 'Status: Draft' and 'Last Modified: Tue Jul 07 12:44:16 EDT 2015 Administrator'.

4382

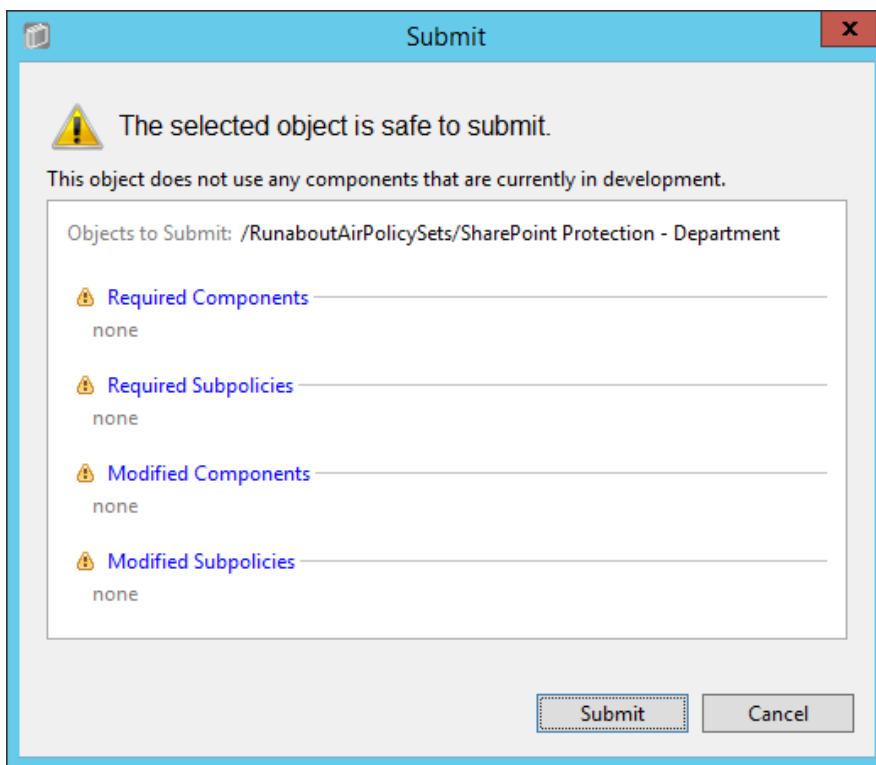
- 4383 a. Or, in the Policies panel in the top-left corner of the main Policy Studio window, right-click the policy you want to deploy. Select **Submit** from the floating menu.

4385



4386

2. In the Submit window, click **Submit**.



4387

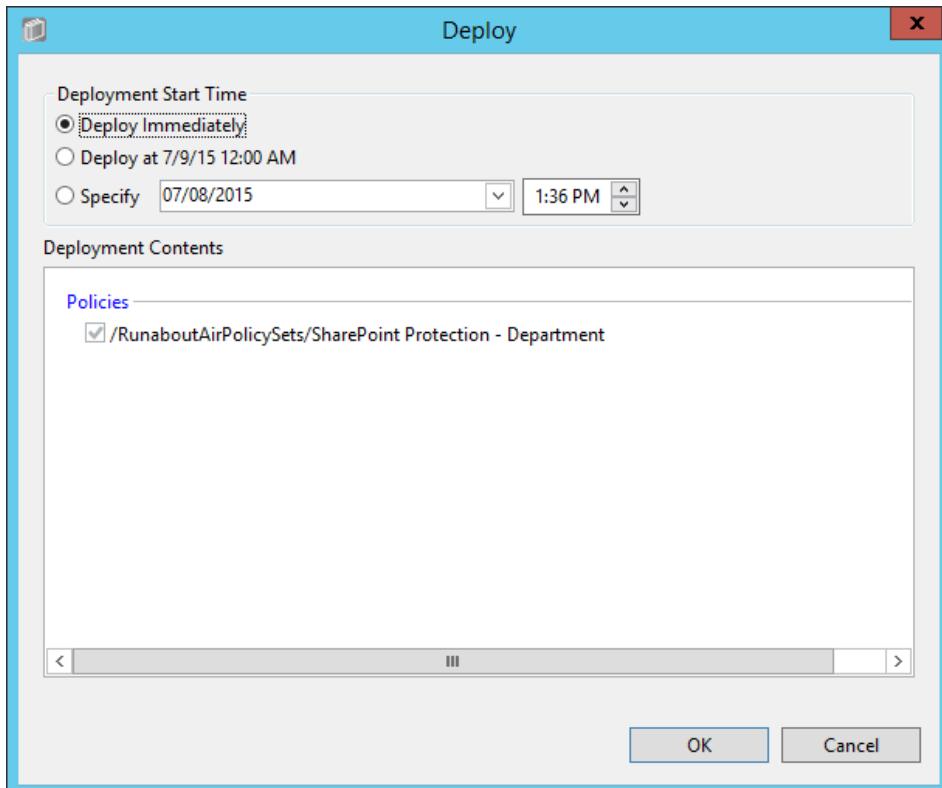
3. From the component editing panel, note the differences. The new status reads **Submitted for Deployment**. Click **Deploy**.
 - a. Or, in the Policies panel in the top-left corner of the main Policy Studio window, right-click the policy you want to deploy. Select **Deploy** from the floating menu.

4392

SharePoint ... Department	Modify	Deploy	Status: Submitted for Deployment
			Last Modified: Tue Jul 07 12:44:16 EDT 2015 Administrator
			Submitted by: Wed Jul 08 13:32:11 EDT 2015 Administrator

4393

- 4394 4. In the Deploy window, click **OK**. Note: You may specify to deploy immediately, which we choose
 4395 in our example. You may also deploy at the following day at midnight, or at a different specific date and time.



4396

- 4397 5. At the bottom of the policy editing panel, verify that the **Status** is now **Pending Deployment**.
 4398 This will remain for the duration of the heartbeat (described in [Section 7](#)).
 4399 6. After the duration of the heartbeat has passed, **Status** should read as **Deployed**. This indicates
 4400 that the component is actively deployed in your ABAC system.

4401 8.4.6 Modifying and Re-Deploying Policies and Components

4402 In order to modify existing policies and re-deploy them, do the following:

4403 8.4.6.1 Modifying and Deploying Existing Policies

- 4404 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on the policy
 4405 you want to modify. In the policy editing panel, click **Modify**.
 4406 a. Or, right-click the policy you want to modify and select **Modify** from the floating menu.
 4407 2. In the policy editing panel, make the desired changes and click **Submit**.

4408 3. Follow the deploy instructions from [Section 8.4.5](#) to deploy the modified policy.

4409 *8.4.6.2 Modifying and Deploying Existing Components*

4410 1. In the Components panel in the bottom-left corner of the main Policy Studio window, click on
4411 the component you want to modify. In the policy editing panel, click **Modify**.

4412 a. Or, right-click the component you want to modify and select **Modify** from the floating
4413 menu.

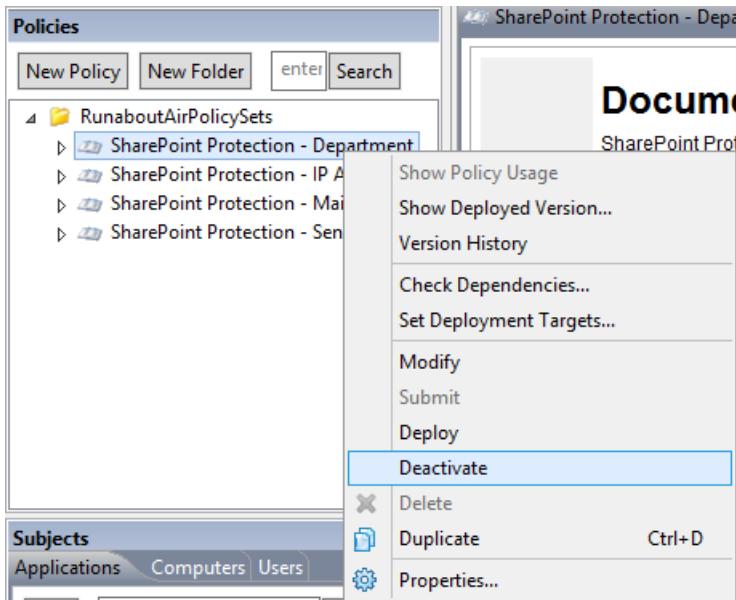
4414 2. In the component editing panel, make the desired changes and click **Submit**.

4415 3. Follow the deploy instructions from [Section 8.4.5](#) to deploy the modified component.

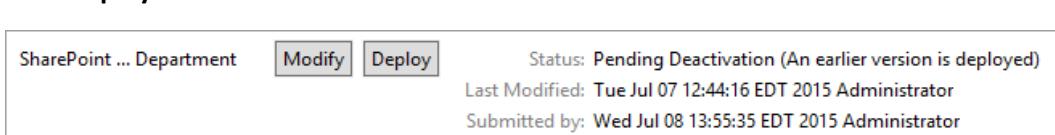
4416 *8.4.7 Deactivating Policies and Components*

4417 *8.4.7.1 Deactivating Policies*

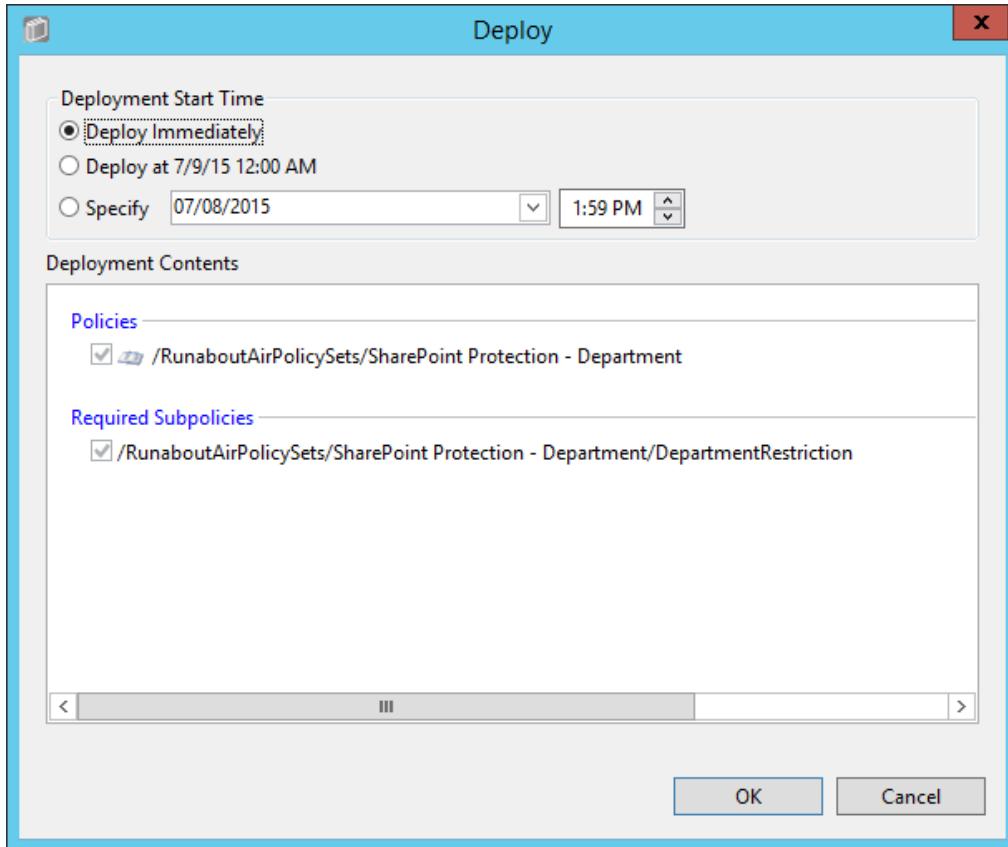
4418 1. In the Policies panel in the top-left corner of the main Policy Studio window, right-click the
4419 policy you want to deactivate. Select **Deactivate** from the floating menu.



4420 2. At the bottom of the policy editing panel, note the change in **Status to Pending Deactivation**.
4421 Click **Deploy**.

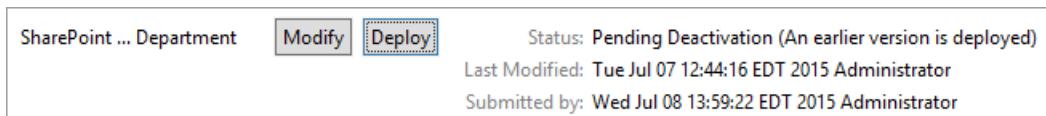


4423 3. In the Deploy window, click **OK**. Note: You may specify to deploy immediately, which we choose
4424 in our example. You may also deploy the following day at midnight, or at a different specific date
4425 and time.



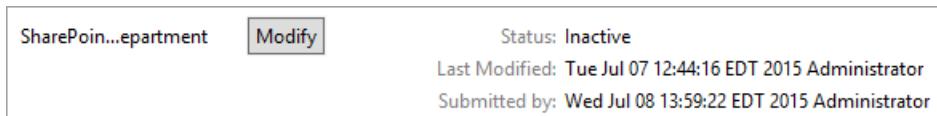
4427

- 4428 4. Verify at the bottom of the policy editing panel that the **Status** is now **Pending Deactivation**.
 4429 This will remain for the duration of the heartbeat (described in [Section 7](#)).



4430

- 4431 5. After the duration of the heartbeat has passed, **Status** should read as **Inactive**. This indicates
 4432 that the component is currently inactive in your ABAC system.



4433

4434 *[8.4.7.2 Deactivating Components](#)*

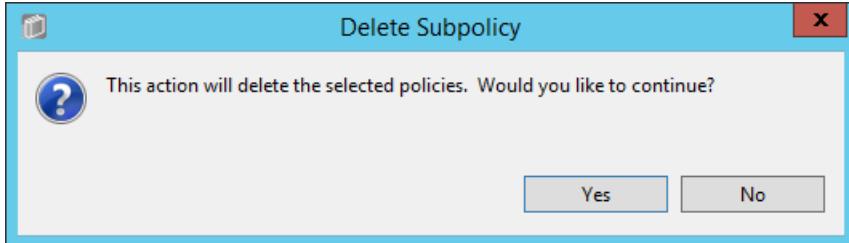
- 4435 1. In the Components panel in the bottom-left corner of the main Policy Studio window, right-click
 4436 on the component you want to deactivate. Select **Deactivate** from the floating menu.
 4437 2. Follow steps 2-5 in [Section 8.4.7.1](#) for deactivating policies.

4438 **8.4.8 Deleting Policies and Components**

4439 Note: In order to delete a policy or component, you must first deactivate the item and any related sub-
4440 items.

4441 **8.4.8.1 Deleting Policies**

- 4442 1. In the Policies panel in the top-left corner of the main Policy Studio window, right-click on the
4443 policy you want to delete. Select **Delete** from the floating menu.
4444 2. In the Delete window, click **Yes**.



4445

4446 **8.4.8.2 Deleting Components**

- 4447 1. In the Components panel in the bottom-left corner of the main Policy Studio window, right-click
4448 on the policy you want to delete. Select **Delete** from the floating menu.

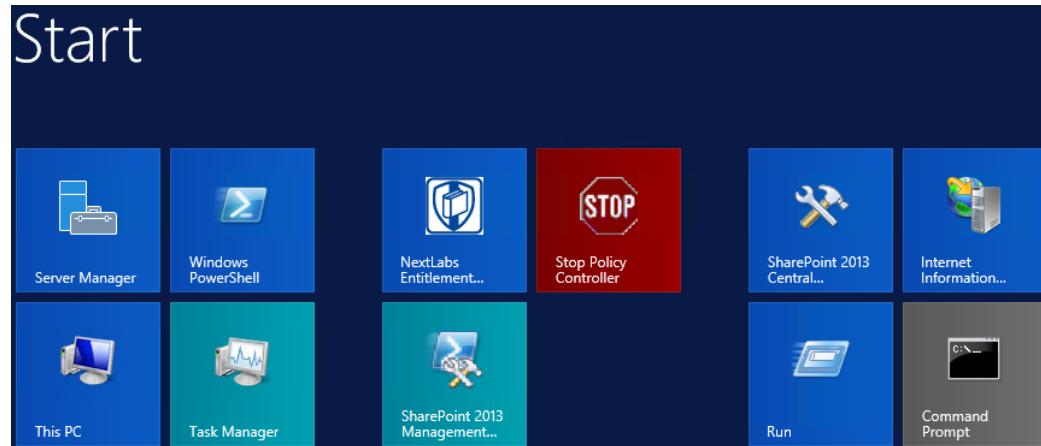
4449 **8.5 Configuring Attributes in NextLabs**

4450 [Section 6](#) illustrated how to configure the attribute flow between several of the servers and components
4451 in the ABAC architecture. Note that the NextLabs Entitlement Manager was installed on the SharePoint
4452 Server, which is where all of the activity in Section 8.5 occurs.

4453 In order to configure NextLabs to enforce policy on all of the attributes coming from the front-channel
4454 as SharePoint Claims, you must first stop the NextLabs Policy Controller service, edit the
4455 configuration.xml file in the SharePoint Enforcer software architecture, restart Internet Information
4456 Services (IIS), then restart the NextLabs Policy Controller service using the following instructions.

4457 **8.5.1 Stopping the NextLabs Policy Controller Service**

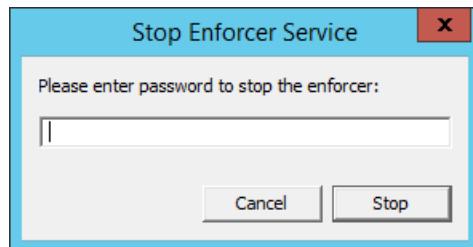
- 4458 1. On the SharePoint Server, click the Windows icon and begin typing the word **Services**.
4459 2. Double-click on the icon to open the Services application.
4460 3. Within the Services application window, in the list of services, click on the **Name** column to sort
4461 by alphabetical order, and look for **Control Center Enforcer Service**.
4462 4. If the **status** of the Control Center Enforcer Service is **Running**, stop it.
4463 a. Click the Windows icon.
4464 b. Double-click the **Stop Policy Controller** shortcut icon.



4465

4466

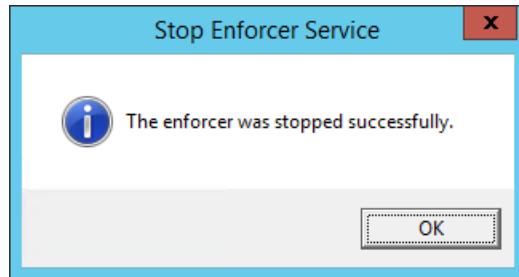
- c. Enter your NextLabs Administrator credentials. Then click **Stop**.



4467

4468

- d. In the Stop Enforcer Service success window, click **OK**.



4469

4470 8.5.2 Editing the Configuration File

4471 8.5.2.1 Locating and Opening the SharePoint Enforcer configuration.xml File

4472 1. In Windows Explorer, find and open the SharePoint Enforcer configuration.xml file.

4473 a. Double-click the **C:/** drive.

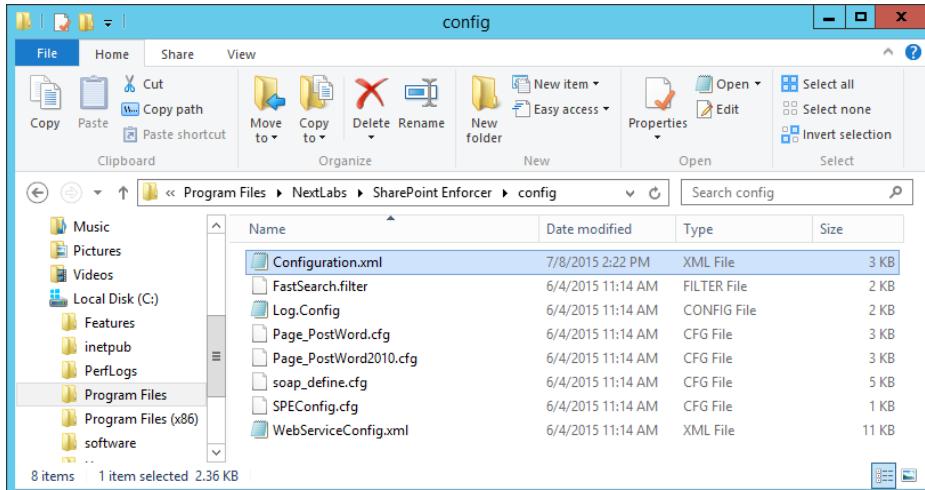
4474 b. Double-click **Program Files**.

4475 c. Double-click **NextLabs**.

4476 d. Double-click **SharePoint Enforcer**.

4477 e. Double-click **config**.

4478 f. Right-click **Configuration.xml** to edit the file in a text editor.



4479

8.5.2.2 Configuring Resource Attributes from SharePoint Metadata

1. Within the **configuration.xml** file, look for the **<SPEConfiguration>** tag.
2. Under that tag, but above a **<User Attribute>** tag, insert tags for each site-level or sub-site level resource attribute of interest.
 - a. For example, in our build we created policies based on the **department** resource attribute, so in our configuration.xml file we included the following:

```

<PropertyBag disabled="false" level="SiteCollection">
  <Property disabled="false" name="department" attributename="department" />
</PropertyBag>
<PropertyBag disabled="false" level="SubSite">
  <Property disabled="false" name="department" attributename="department" />
</PropertyBag>

```
- b. From the example above, the top of the **configuration.xml** file looks like this:

4495

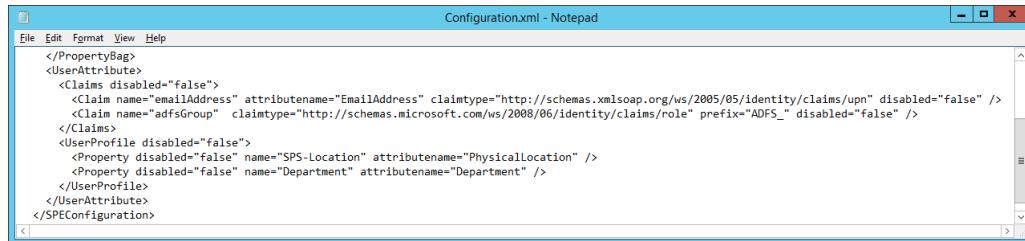
```

<?xml version="1.0" encoding="utf-8"?>
<Configuration name="test" xmlns="http://www.nextlabs.com/configurationSchema">
  <SPEConfiguration>
    <PropertyBag disabled="false" level="SiteCollection">
      <Property disabled="false" name="department" attributename="department" />
    </PropertyBag>
    <PropertyBag disabled="false" level="SubSite">
      <Property disabled="false" name="department" attributename="department" />
    </PropertyBag>
  </SPEConfiguration>
</Configuration>

```

4496 8.5.2.3 Configuring User Attributes from SharePoint Claims

- 4497 1. Within the **configuration.xml** file directly under any **<PropertyBag>** closing tags, find the **<User Attribute> </User Attribute>** portion of the document. Initially, its default contents in that area
 4498 may look like this, containing some default user attributes such as “**emailAddress**” or
 4499 “**adfsGroup**”:



```

</PropertyBag>
<UserAttribute>
  <Claims disabled="false">
    <Claim name="emailAddress" attributename="EmailAddress" claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" disabled="false" />
    <Claim name="adfsGroup" claimtype="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" prefix="ADFS_" disabled="false" />
  </Claims>
<UserProfile disabled="false">
  <Property disabled="false" name="SPS-Location" attributename="PhysicalAllocation" />
  <Property disabled="false" name="Department" attributename="Department" />
</UserProfile>
</UserAttribute>
</SPEConfiguration>

```

- 4501 4502 2. In the **User Attribute** area, add more claims here to include all the attributes you will be
 4503 expecting to evaluate in NextLabs policies for access control decisions.

- 4504 a. For example, in our build we created policies based on users’ “**clearance**”,
 4505 “**department**”, and “**ip_address**”, so in our **configuration.xml** file we included the
 4506 following, among others:

```

<Claim name="department" attributename="department"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/department" disabled="false" />

<Claim name="ip_address" attributename = "ip_address"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ip_address" disabled="false" />

<Claim name="clearance" attributename = "clearance"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/clearance" disabled="false" />

```

- 4516 b. From the example above, the rest of our **configuration.xml** file looks like this:



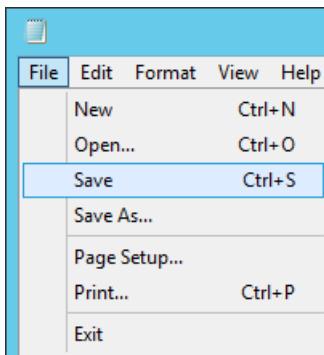
```

</PropertyBag>
<UserAttribute>
  <Claims disabled="false">
    <Claim name="upn" attributename="upn"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" disabled="false" />
    <Claim name="emailaddress" attributename="emailaddress"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress" disabled="false" />
    <Claim name="adfsGroup"
claimtype="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" prefix="ADFS_" disabled="false" />
    <Claim name="department" attributename="department"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/department" disabled="false" />
    <Claim name="staffLevel" attributename="staffLevel"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/staffLevel" disabled="false" />
    <Claim name="employer" attributename="employer"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/employer" disabled="false" />
    <Claim name="role" attributename="role"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role" disabled="false" />
    <Claim name="ip_address" attributename = "ip_address"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ip_address" disabled="false" />
    <Claim name="clearance" attributename = "clearance"
claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/clearance" disabled="false" />
  </Claims>
</UserAttribute>
</SPEConfiguration>

```

4518 **8.5.2.4 Saving Changes to the Configuration File**

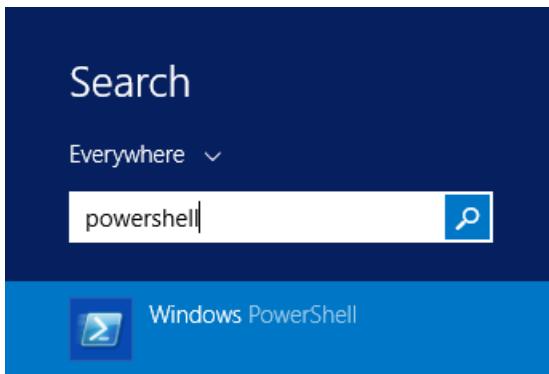
- 4519 1. From the File menu, click **Save**, or Ctrl+S on your keyboard.



4520

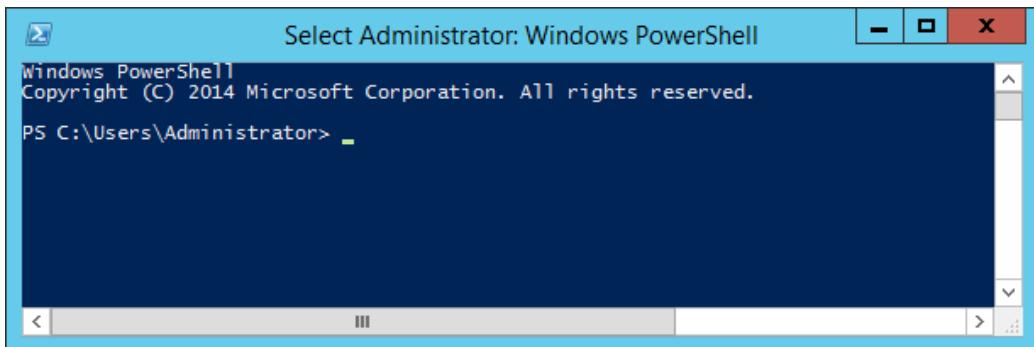
4521 **8.5.3 Restarting IIS via Windows PowerShell**

- 4522 1. Click the Windows icon.
- 4523 2. In the Search text box, begin typing **PowerShell**.



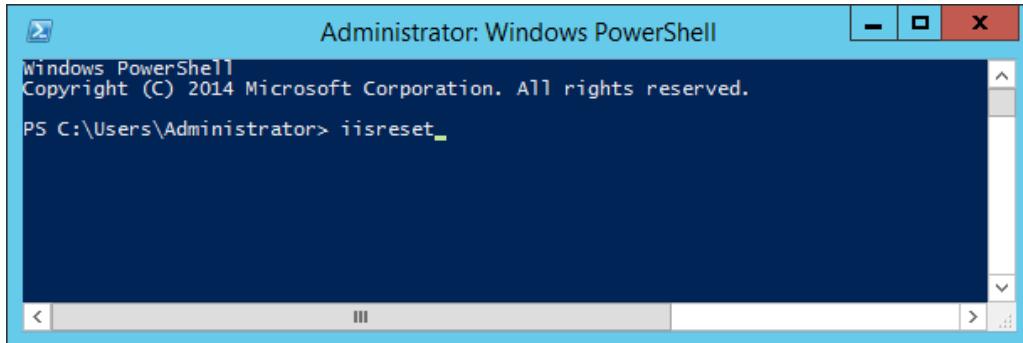
4524

- 4525 3. Click on **Windows PowerShell**.



4526

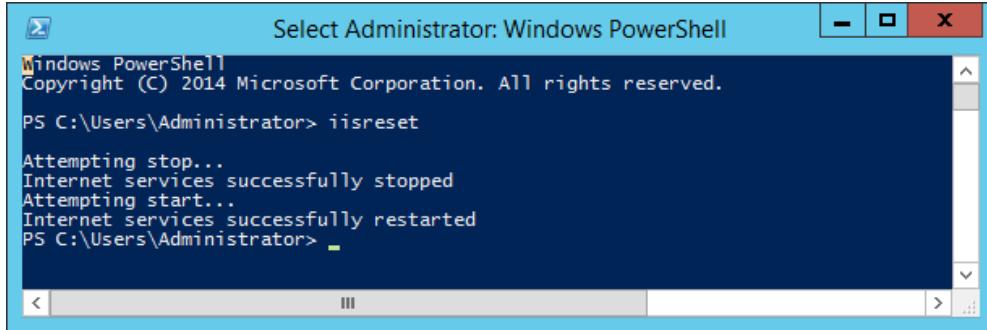
- 4527 4. In the PowerShell window, type the command: **iisreset**. Press **Enter**.



Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> iisreset

4528

- 4529 5. In the PowerShell window, verify that services stopped and restarted successfully.



Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> iisreset
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
PS C:\Users\Administrator>

4530

8.5.4 Restarting the NextLabs Policy Controller Service

1. Click on the Windows icon and begin typing the word **Services**.
2. Double-click the **Services** icon to open the application.
3. Within the Services application window in the list of services, click on the **Name** column to sort by alphabetical order and look for **Control Center Enforcer Service**.
4. Right-click **Control Center Enforcer Service** and click **Start**.
 - a. It may be necessary to click the **Refresh** icon in order to see the **Control Center Enforcer Service** status change to **Running**.

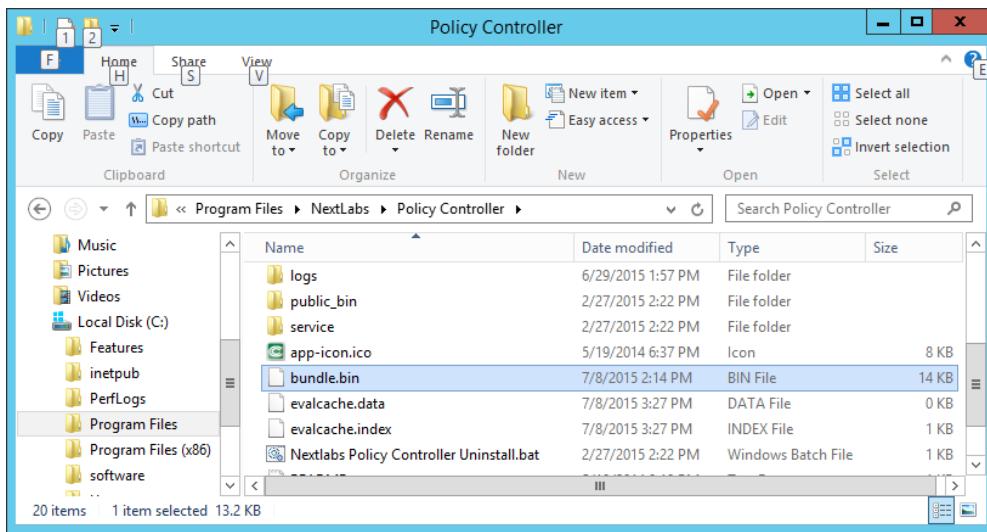
8.6 Functional Test

8.6.1 Updated Bin File After Policy Creation/Modification

- After a policy or component is deployed for the first time, or modified and re-deployed within Policy Studio on the SQL Server, an encrypted bundle.bin file on the SharePoint Server will be updated after one heartbeat. As explained in [Section 7](#), on the SharePoint Server it is the responsibility of the Controller Manager component of the NextLabs Policy Controller (PDP) to encrypt the bundle.bin file on the local file system for use during policy evaluation by the PDP.
- To ensure the policy logic is being correctly sent from the NextLabs Policy Studio (PAP) on the SQL Server to the bundle.bin file on the SharePoint Server for use by the NextLabs Policy Controller (PDP), you can find the bundle.bin file and decrypt its contents to see your policy logic decrypted there.

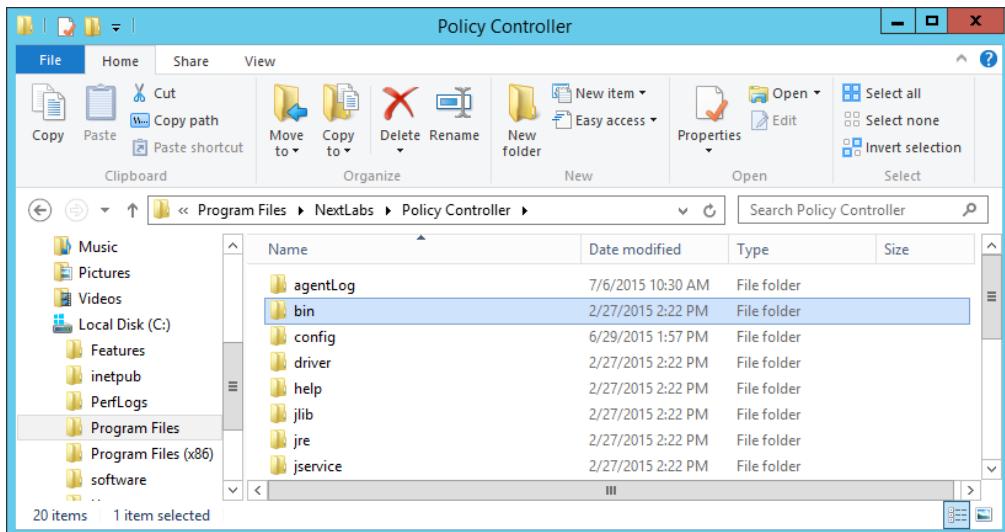
4549 8.6.1.1 *On the SharePoint Server Note Timestamp of the Bundle.bin File and Decrypt Its
4550 Contents*

- 4551 1. Double-click the **C:/** drive.
- 4552 2. Double-click **Program Files**.
- 4553 3. Double-click **NextLabs**.
- 4554 4. Double-click **Policy Controller**.
- 4555 5. Scroll down to find **bundle.bin** and note the timestamp in the **Date Modified** column. This
4556 would be the last time policies or components were deployed.



4557

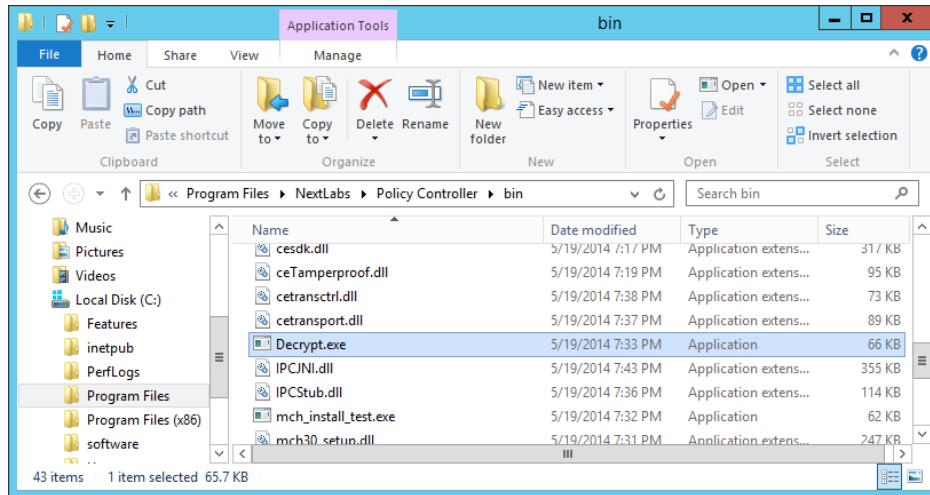
- 4558 6. Scroll back up and double-click on the **bin** folder.



4559

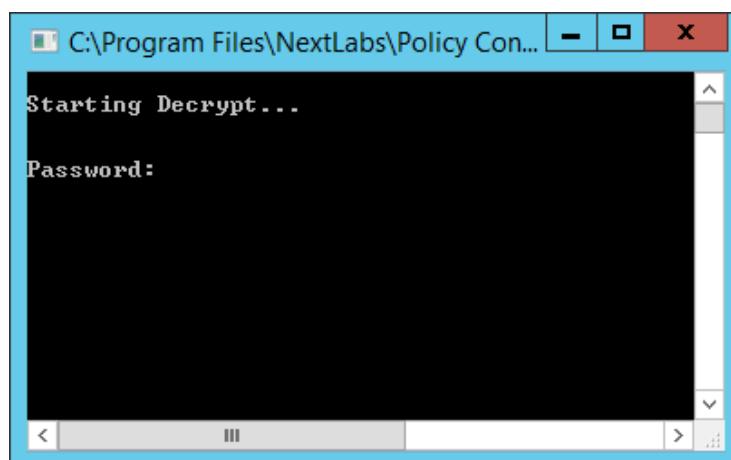
- 4560 7. Scroll down to find **Decrypt.exe**.

SECOND DRAFT



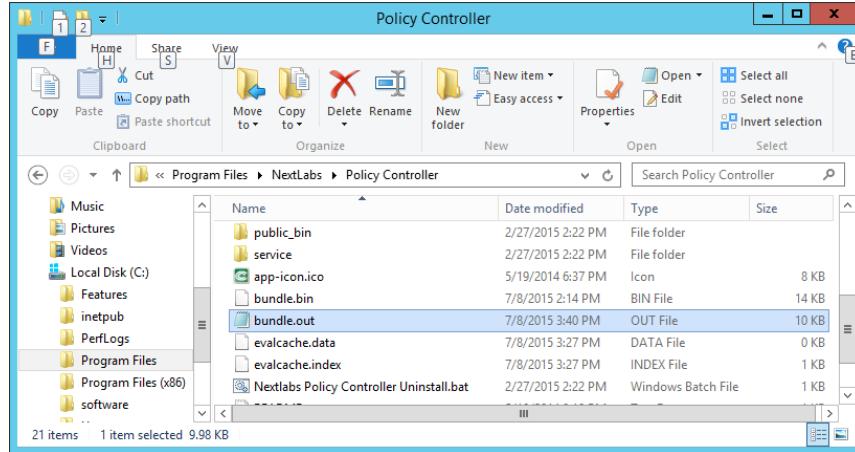
4562

- In the Decrypt window, enter the administrator's **Password** and press **Enter**.



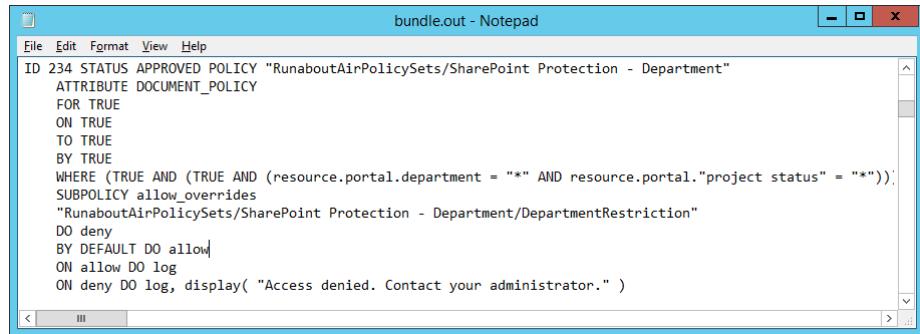
4563

- 4564 b. After the Decrypt window disappears, click on Policy Controller to return to that folder.
4565 Scroll down and double-click the **bundle.out** file.



- 4567 c. In the text editor window, scroll down to find policies that you have created previously.
4568 Example: **RunaboutAirPolicySets/SharePoint Protection – Department** top-level policy

4569



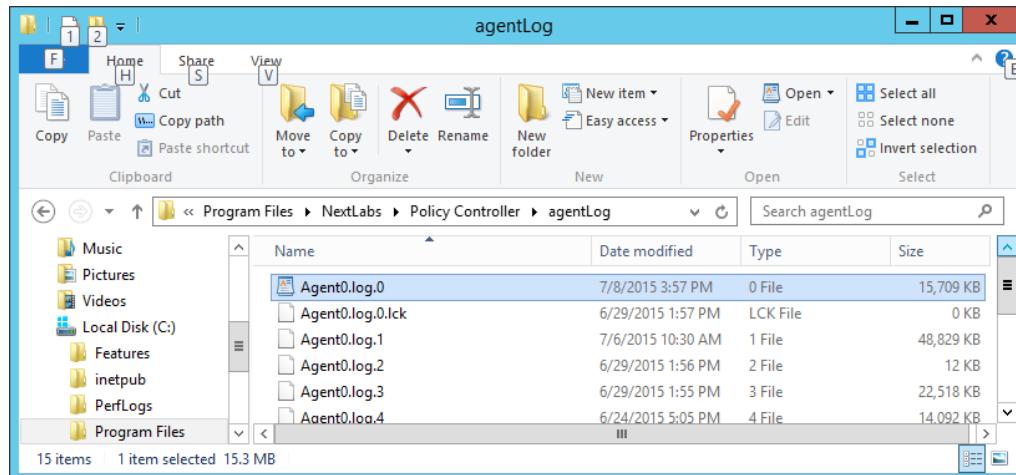
The screenshot shows a Notepad window titled "bundle.out - Notepad". The content of the window is a policy definition in XML-like syntax:

```
ID 234 STATUS APPROVED POLICY "RunaboutAirPolicySets/SharePoint Protection - Department"
  ATTRIBUTE DOCUMENT_POLICY
  FOR TRUE
  ON TRUE
  TO TRUE
  BY TRUE
  WHERE (TRUE AND (TRUE AND (resource.portal.department = "*" AND resource.portal."project status" = "*")));
  SUBPOLICY allow_overrides
    "RunaboutAirPolicySets/SharePoint Protection - Department/DepartmentRestriction"
    DO deny
    BY DEFAULT DO allow
    ON allow DO log
    ON deny DO log, display( "Access denied. Contact your administrator." )
```

4570 8.6.2 **Reviewing NextLabs AgentLog to Illustrate History of Access Control Evaluations during SharePoint Access**

- 4571
- 4572 1. Double-click the **C:/** drive.
 - 4573 2. Double-click **Program Files**.
 - 4574 3. Double-click **NextLabs**.
 - 4575 4. Double-click **Policy Controller**.
 - 4576 5. Double-click **AgentLog**.
 - 4577 6. Right-click the **Agento.log.0** locked file and select **Copy**.

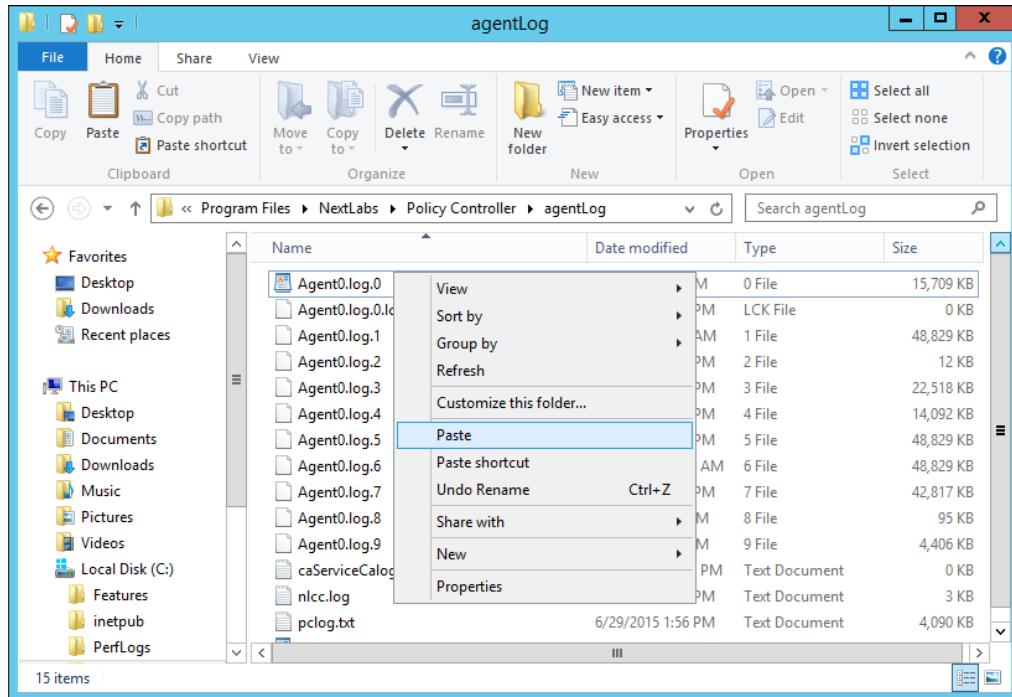
4578



4579

7. Within the **agentLog** folder, right-click in an empty space and select **Paste**.

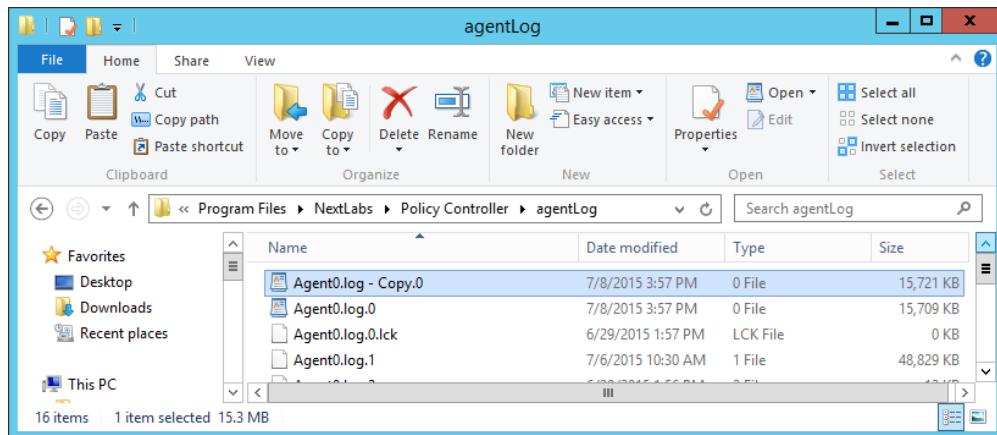
SECOND DRAFT



4580

4581

8. Double-click the **Agent0.log-Copy.0** file to view its contents.



4582

4583

9. Scroll down to view the contents. You can press Ctrl+F to find keywords such as any identifying word from your policy definitions, words common to ABAC activity such as **allow** or **deny**, or words native to NextLabs logging such as **effect =**.

4584

4585

- a. Examples of information found in this **Agent0.log-Copy.0** file:

4586

- i. All of the policies evaluated during one instance of access:

4587

```
Jul 7, 2015 4:29:53 PM com.bluejungle(pf.engine.destiny.f
performContentAnalysis
FINEST: No from resource found. Ignoring
Jul 7, 2015 4:29:53 PM
com.bluejungle(pf.engine.destiny.EvaluationEngine evaluate
INFO: Matching policies for 2342972204282387:
X: RunaboutAirPolicySets/SharePoint Protection -
Department/DepartmentRestriction
```

```

4596      A: RunaboutAirPolicySets/SharePoint Protection - Department
4597      X: RunaboutAirPolicySets/SharePoint Protection - IP
4598      Address/AllowIPAddressLevel1
4599      X: RunaboutAirPolicySets/SharePoint Protection - IP
4600      Address/AllowSensitiveLevelsToAnyOtherIP
4601      A: RunaboutAirPolicySets/SharePoint Protection - IP Address
4602      X: RunaboutAirPolicySets/SharePoint Protection - Maintenance/Allow
4603      Maintenance After 6pm and Weekends
4604      A: RunaboutAirPolicySets/SharePoint Protection - Maintenance/Allow
4605      Non-Maintenance Any Time
4606      A: RunaboutAirPolicySets/SharePoint Protection - Maintenance
4607      X: RunaboutAirPolicySets/SharePoint Protection -
4608      Sensitivity/Policyla-Sensitivity Level 1
4609      X: RunaboutAirPolicySets/SharePoint Protection -
4610      Sensitivity/Policylb-Sensitivity Level 2
4611      X: RunaboutAirPolicySets/SharePoint Protection -
4612      Sensitivity/Policylc-Sensitivity Level 3
4613      A: RunaboutAirPolicySets/SharePoint Protection - Sensitivity

```

- 4614 ii. An allow decision was evaluated when this example user, Jorge Gonzalez,
 4615 logged into the Runabout Air SharePoint:

```

4616 Jul 7, 2015 4:29:53 PM
4617 com.bluejungle.destiny.agent.controlmanager.PolicyEvaluatorImpl
4618 queryDecisionEngine
4619 INFO: Request 2342972204282387 input params
4620     to
4621     application
4622         pid: 5140
4623     environment
4624         request_id: 2342972204282387
4625         time_since_last_successful_heartbeat: 31
4626     host
4627         inet_address: 184536844
4628     operating-system-user
4629         id: S-1-5-21-972639958-268376111-2639239546-1138
4630     action
4631         name: OPEN
4632     sendto
4633     from
4634         title: relying party inc - root site
4635         ce::id: sharepoint://sharepoint.abac.test/
4636         name: relying party inc - root site
4637         sub_type: site
4638         type: site
4639         ce::destinytype: portal
4640         url: sharepoint://sharepoint.abac.test/
4641     user
4642         :
4643         id: S-1-5-21-972639958-268376111-2639239546-1138
4644         title: Scientist
4645         department: Research and development
4646         stafflevel: Senior
4647         upn: jgonzalez@ABAC.TEST
4648         company: Conway
4649         name: abac\jgonzalez
4650         clearance: Top Secret
4651     Ignore obligation = false

```

```
4652          Process Token = 984
4653          LogLevel = 3
4654          Result: Effect = allow (total:4608ms, setup:4605ms,
4655          obligations:0ms)
4656          Obligations:
4657          From file list: [sharepoint://sharepoint.abac.test/]
4658          To filename list: null
```

9 Leveraging NextLabs Control Center Reporter for Reporting and Auditing Purposes

9.1 Introduction

In previous sections of this How-To Guide ([Section 7](#)), we installed several NextLabs products that can be used to define and deploy Attribute Based Access Control policies and enforce decisions regarding user access to Microsoft SharePoint resources based on user, object, environmental attributes, and the corresponding policies in place. We also illustrated how to use and configure the NextLabs Policy Studio, the product responsible for Policy Lifecycle Management, and discussed policy strategy and the translation of business logic into policy ([Section 8](#)).

In this section of the How-To Guide, we will illustrate how to use the NextLabs Control Center Reporter, a component of the previously installed NextLabs Control Center ([Section 7](#)), in order to generate reports and provide a graphical user interface for prior policy evaluation and access control decisions in your environment.

Reporter is automatically installed during the NextLabs Control Center installation, which was detailed in [Section 7](#). In this How-To section, we will introduce Reporter, its purpose, interface, and capabilities, then illustrate some example uses based on our build.

9.1.1 Components Used in this How-To Guide

NextLabs Control Center Reporter v7.5.0 (64) – web application and graphical user interface for evaluating prior policy evaluation access control decisions and generating reports for monitoring and auditing.

9.1.2 Pre-requisites to Complete Prior to this How-To Guide

1. If you intend to do a setup without identity federation and federated logins, you must:
 - a. Install and configure Active Directory (see [Section 2](#))
 - b. Install and configure Microsoft SharePoint (see [Section 4](#))
 - c. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see [Section 7](#))
 - d. Define and deploy policies based on your business rules (see [Section 8](#))
2. If you intend to incorporate a trust relationship between an IdP and RP and use federated logins into SharePoint, you must:

- 4688 a. Install and configure Active Directory (see [Section 2](#))
- 4689 b. Setup and configure the RP and IdP (see [Section 3](#))
- 4690 c. Install and configure Microsoft SharePoint (see [Section 4](#))
- 4691 d. Configure the SharePoint federated login with the RP (see [Section 5](#))
- 4692 e. Configure the attribute flow between all endpoints (see [Section 6](#))
- 4693 f. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see
4694 [Section 7](#))
- 4695 g. Define and deploy policies based on your business rules (see [Section 8](#))

4696 **9.2 Introduction to NextLabs Control Center Reporter**

4697 The NextLabs Control Center Reporter is a web application that can be used to generate reports on how
4698 information is being used in your environment. You can use Reporter to define and run custom queries
4699 about policy enforcement activities that are recorded in the Activity Journal, a native, automatic logging
4700 mechanism built into the NextLabs SQL database that was configured during installation of the NextLabs
4701 Control Center ([Section 7](#)). These queries are referred to as **reports**. Reports can be designed to answer
4702 a wide variety of questions, such as who has access to certain documents, who is using which resources
4703 and when, what types of policy enforcement is taking place, what activity occurred within a given
4704 department, and so on.

4705 In addition to reports, you can also use Reporter to create monitors that trigger alerts when specified
4706 policy enforcement criteria are met. You can design monitors to cover a wide range of scenarios, such as
4707 sending an alert through email when access to a certain resource has been denied more than a specified
4708 number of times in a given time period; or when the volume of classified documents that have been
4709 downloaded in a given time period exceeds a specific file size. Together, monitors and alerts can provide
4710 continuous coverage of critical policy enforcements in an enterprise, as well as a notification system that
4711 lets you know when action is required.

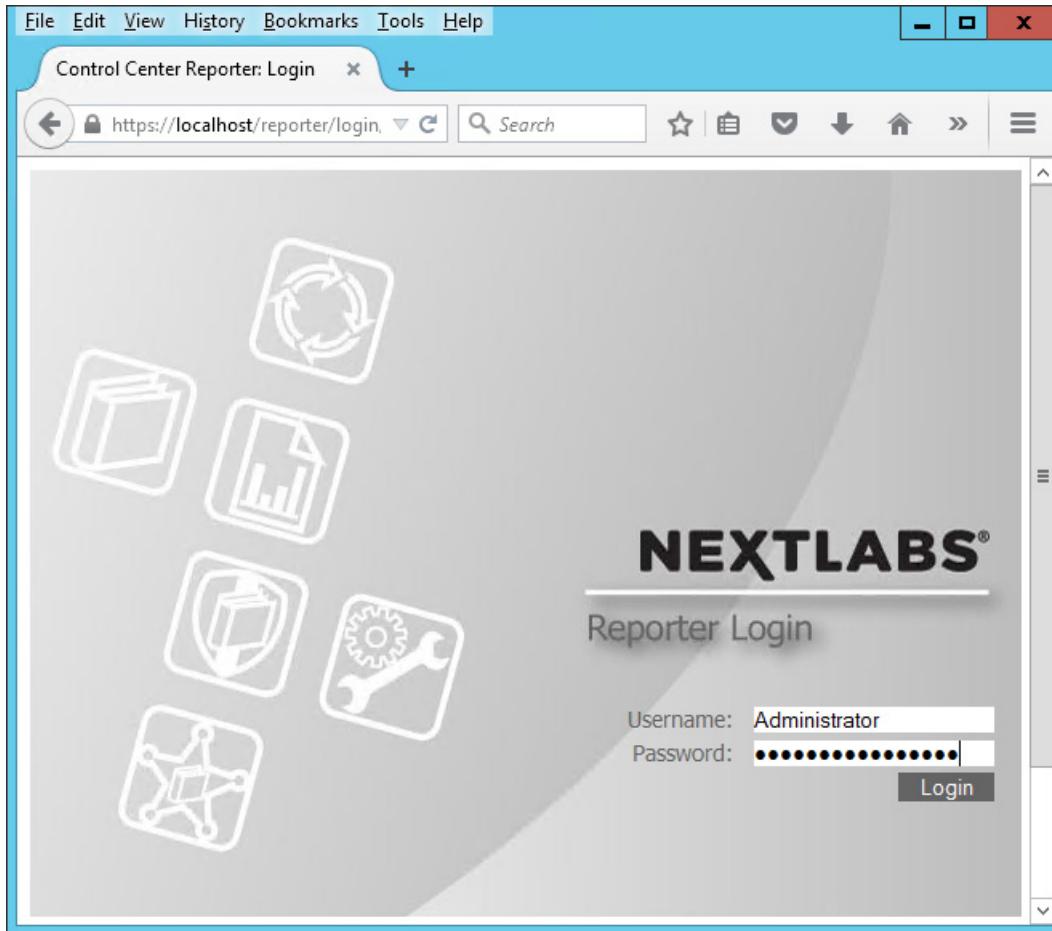
4712 Reporter is intended for use by whoever is responsible for monitoring and reporting on compliance,
4713 gathering statistics about document usage, and investigating any suspected incidents of information
4714 mishandling. This may include administrators, IT staff, managers, executives, and auditors, or any other
4715 authorized personnel.

4716 User permissions are defined in the Administrator application (another component of Control Center
4717 installed in [Section 7](#)), by creating a new User and assigning one of the four available roles to it. By
4718 default, all roles include permission to open and use the reporting functionality of Reporter.

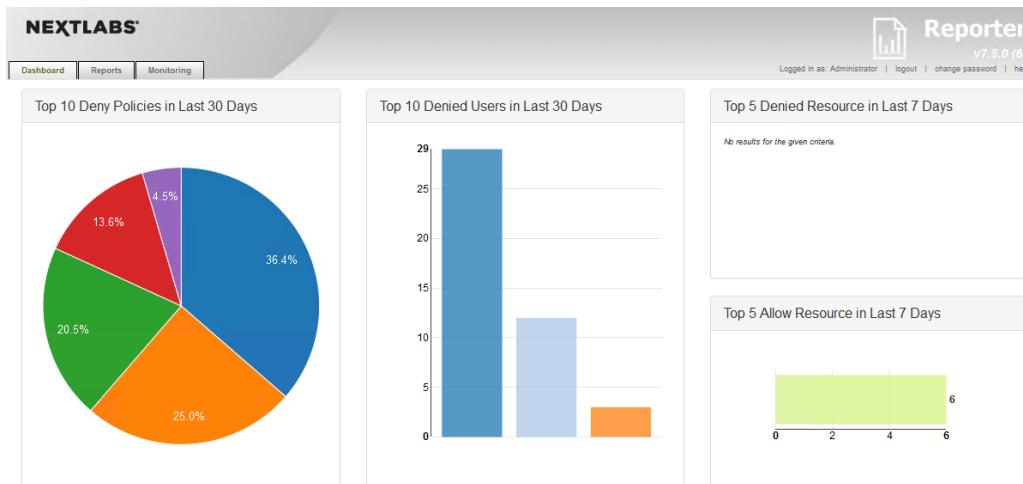
4719 **9.2.1 Opening Reporter**

- 4720 1. On the server where NextLabs Control Center was installed, open a web browser (i.e., SQL
4721 Server in this build).
- 4722 2. Enter the URL and press Enter: *https://<hostname>/reporter*, i.e., *https://localhost/reporter*

- 4723 3. At the Reporter login screen, enter valid credentials, such as the Control Center Administrator
 4724 account created in [Section 7](#). Click **Login**.



- 4725
 4726 4. In your browser, the Reporter opening view defaults to the **Dashboard** tab. The **Dashboard** tab,
 4727 **Reports** tab, and **Monitoring** tab will be discussed more thoroughly in subsequent sections of
 4728 this How-To Guide.



4729

4730 9.3 Introduction to Reporter Dashboard

4731 The Reporter Dashboard is divided into panes, each displaying a predefined statistical view of data that
 4732 provides a snapshot of policy enforcement trends. In the default configuration of Reporter, these panes
 4733 display data in the following graphs (from the NextLabs Control Center Reporter User Guide, available
 4734 only to customers at this time):

Graph	Description	May Indicate
Top Five Deny Policies (Month)	Pie chart representing the five Deny policies that were most frequently enforced over the previous thirty days.	<ul style="list-style-type: none"> • Misunderstanding of access level: users being blocked from a resource they believe they should use • Incorrectly defined entitlements: users should have access, but policies are not updated or correctly designed
Top Ten Denied Users (Month)	Bar chart representing the ten users who have had the most instances of any Deny policy enforced against them.	<ul style="list-style-type: none"> • Users who habitually snoop into resources they are not authorized to use • Incorrectly defined entitlements: users or group should have access, but policies are not updated or are incorrectly designed
Top Five Deny Resources (Week)	Bar chart representing the five resources that any users have most frequently attempted to access and been blocked by an active policy, over the previous seven days.	<ul style="list-style-type: none"> • Resources of broad interest to users who should not be using them • Incorrectly designed resource or user component, blocking users who should have access
Top Five Allow Resources (Week)	Bar chart representing the five resources that users have most frequently attempted to access and been allowed by an active policy, over the previous seven days.	<ul style="list-style-type: none"> • Improperly designed resource component or policies, which allow inappropriate users access to sensitive resources
Deny Policy Enforcement Trends (Month)	Bar chart representing the trend, over the previous 30 days, of the daily total instances of any deny policy being enforced on any user, for any resource.	<ul style="list-style-type: none"> • Progress (or lack thereof) in educating users about access policies and individual/group entitlements, at a broad level • Improperly designed policies that are blocking too many users who expect and are entitled to access or use

Graph	Description	May Indicate
Recent Allows	<p>List of details about the most recent ten instances of any allow policy being enforced against any user, for any resource. Details listed include:</p> <ul style="list-style-type: none"> • Date of enforcement • Name of enforced policy • User who triggered the policy • Action that triggered the policy • Resource the user was trying to access 	<ul style="list-style-type: none"> • Instances where some urgent action is required, such as users being allowed access to some resource they should not be using, due to lack of policy coverage or an incorrectly defined policy
Recent Denys	<p>List of details about the most recent ten instances of any deny policy being enforced against any user, for any resource. Details listed include:</p> <ul style="list-style-type: none"> • Date of enforcement • Name of enforced policy • User who triggered the policy • Action that triggered the policy • Resource the user was trying to access 	<ul style="list-style-type: none"> • Instances where many users are attempting to get at data they are not authorized to use • Instances where some urgent correction is required to allow appropriate access, such as multiple authorized users being blocked from some resource they need by an incorrectly defined policy
Alerts this Week: Group by Tags	<p>Treemap representing volume of alerts in the current week. Alerts are grouped by monitor tags.</p>	<ul style="list-style-type: none"> • Policies being watched by monitors that are tagged are being enforced at a rate that demands attention. Further review or action may be required.
Today's Alerts: Details	<p>List of details about the alerts raised in the current day. Details include:</p> <ul style="list-style-type: none"> • Alert level • Monitor name • Alert message • Date and time the alert was raised 	<ul style="list-style-type: none"> • Policies being monitored are being enforced at a rate that demands attention. Further review or action may be required.

4736 These panels are configurable such that an administrator can choose which panels and data are visible
4737 and how they are laid out within the Dashboard according to the business's business logic, policies, and
4738 priorities.

4739 The data displayed in all panes of the dashboard is refreshed from the Activity Journal each time you
4740 open the Dashboard tab. This means that data is updated on demand; for example, if a pane shows
4741 some statistic for the past week, that reflects not the last seven whole calendar days, but the last seven
4742 24-hour periods starting from the top of the current hour.

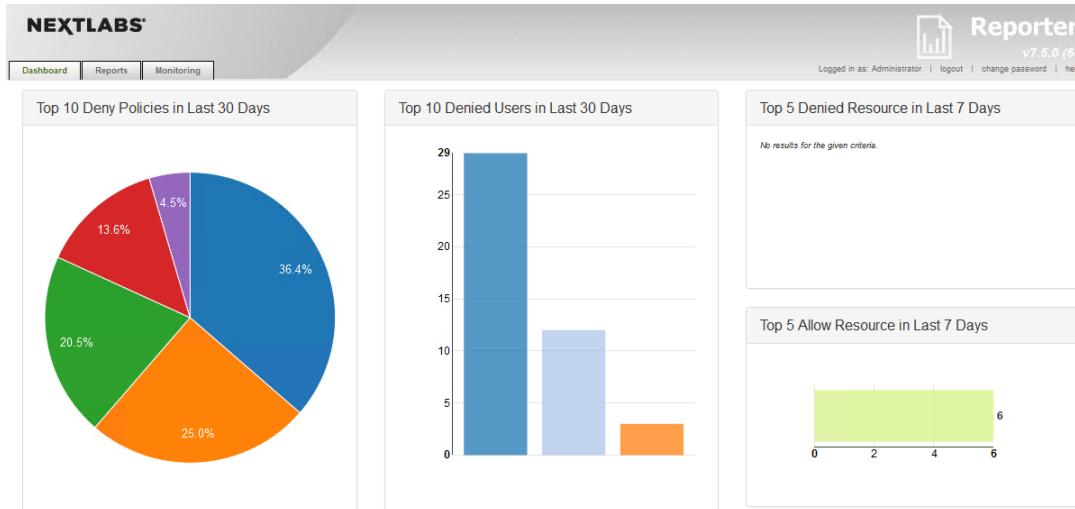
4743 **9.3.1 Exploring the Dashboard**

- 4744 1. On the server where NextLabs Control Center was installed, open a web browser, i.e., SQL
4745 Server in this build
- 4746 2. Enter the URL and press Enter: *https://<hostname>/reporter*, i.e., *https://localhost/reporter*
- 4747 3. At the Reporter login screen, enter valid credentials such as the Control Center Administrator
4748 account created in [Section 7](#). Click **Login**.



4749

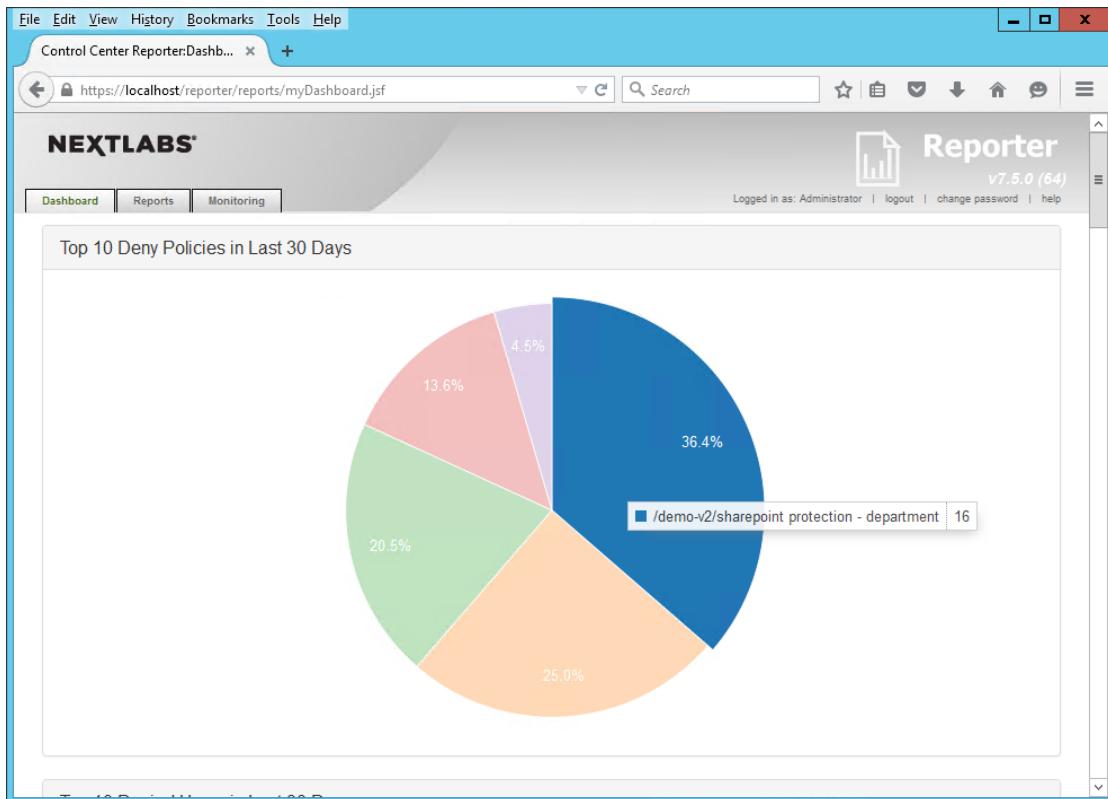
- 4750 4. In your browser, the Reporter will default to the **Dashboard tab**.



4751

4752 The charts and graphs on the Dashboard are interactive. When you move your cursor over a bar in a bar chart or a slice in the pie chart, a tooltip displays information about that value series.

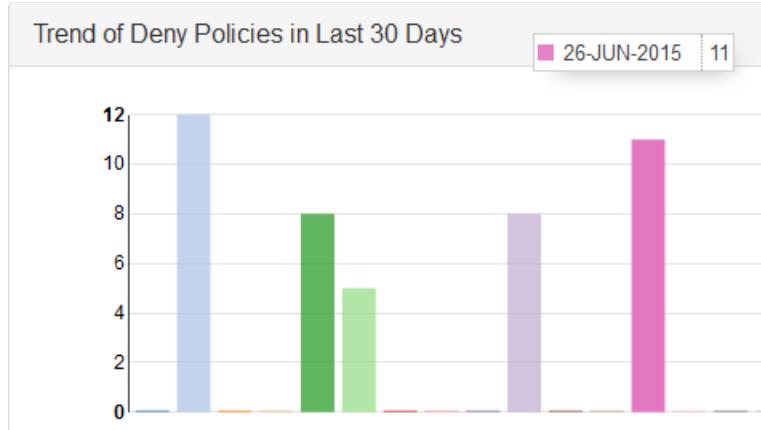
4753
4754 Example seen in the image below: 36.4% of the Deny policies evaluated in the last 30 days
4755 belonged to the SharePoint Protection – Department policy set.



4756

4757 Another example from this build seen in the image below: in the Deny Policies trend in the last
4758 30 days, June 26, 2015 saw an unusually large number of Deny Policies relative to other days.

4759



4760 9.4 Introduction to Defining and Running Custom Reports in Reporter

4761 In Reporter, you can define and run reports in the Reports tab. This tab is divided into two panes, **Saved Reports** on the left side of the Reports tab window and **Report Details** on the right.

The screenshot shows the NEXTLABS Reporter application. The top navigation bar includes 'Dashboard', 'Reports' (which is selected), and 'Monitoring'. The left sidebar is titled 'Saved Reports' and lists several report entries:

- Allow Enforcement in Last 7 Days (S)
- Allow Resource in Last 7 Days (S)
- Attempted Access Classified Documents
- Denied Resource in Last 7 Days (S)
- Denied Users in Last 30 Days (S)
- Deny Enforcement in Last 7 Days (S)
- Deny Policies in Last 30 Days (S)

The main 'Report Details' pane contains the following configuration fields:

- Report Query:** From: 2015-07-15 00:00:00; To: 2015-07-15 23:59:59
- Event Level:** User Events (Level 3)
- Policy Decision:** Both
- Action:** A dropdown menu listing: Ask Question, Attach to Item, Change Attributes, Change File Permissions, Copy / Embed File.
- User:** Search input field with a magnifying glass icon.
- User Criteria:** Fields for User Name and Value, with operators Equals and Max 255 characters, and a '+' button.
- Resource Name:** Input field for Resource Name.
- Resource Criteria:** Fields for Resource Name and Value, with operators Equals and Max 255 characters, and a '+' button.

4763

4764 The Saved Reports pane provides a list of all saved reports available to you. This includes all reports you
4765 create and save, all reports saved by other users and marked as Shared, and the sample reports used to
4766 generate data that is displayed in the Dashboard tab. When you click on any item in Saved Reports, the
4767 details of that report are displayed in Report Details on the right. This is also where you work when you
4768 create a new report.

4769 In the Report Details pane, define the following:

- 4770 ■ the time period of the policy activity data to cover in the report
4771 ■ the criteria, or filters, that determine what policy activity data to include in the report
4772 ■ the output format of the report

4773 The default settings in Report Details display when you click the Reports tab or when you click New in
4774 the Saved Reports pane. By default, the time period for the report is the current day, all policy activity
4775 data at the user level is included, and the data is presented in table format.

4776 After defining a new report or editing an existing report, click **Run** at the bottom of the Report Details
4777 pane to view the results, which we will illustrate in the following two subsections.

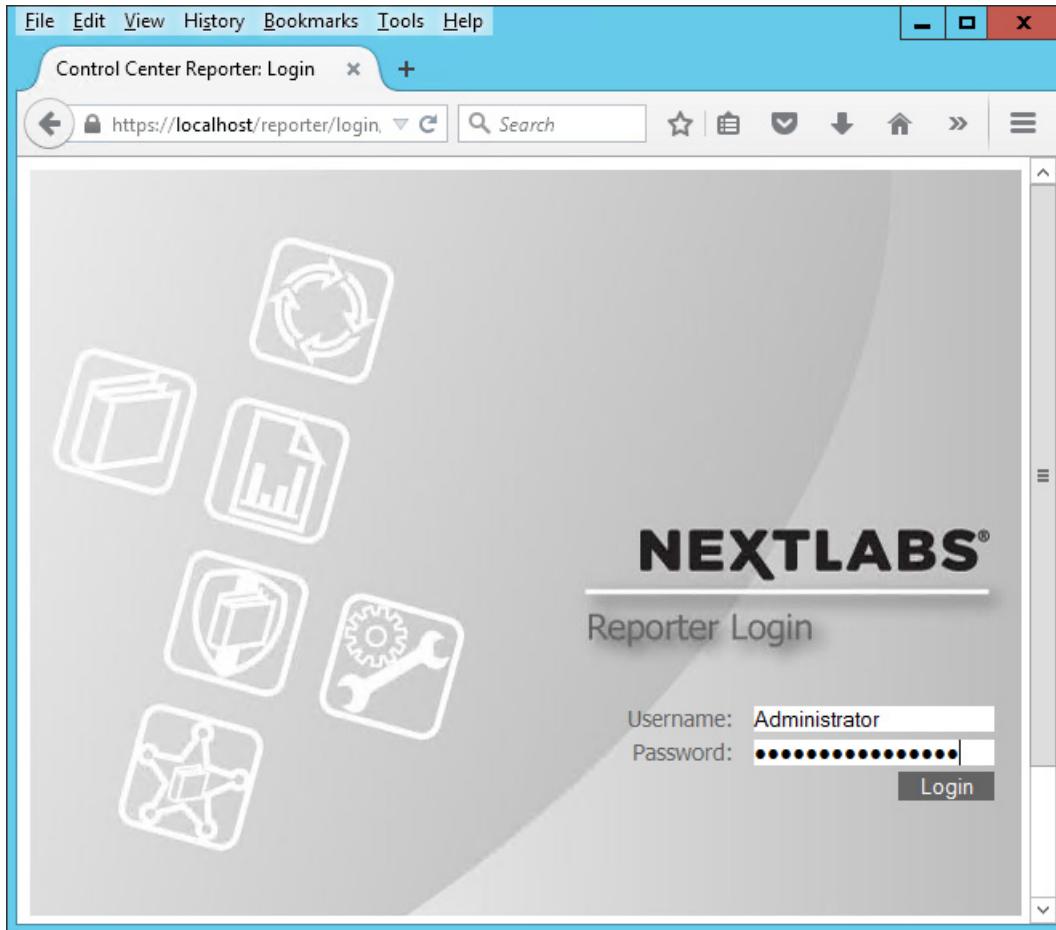
4778 **9.4.1 Defining a Custom Report**

4779 In this subsection, we will list the standard steps for creating a custom report. In [Section 9.5](#) of this How-
4780 To Guide we will illustrate some example custom report sections that demonstrate Reporter's report
4781 capabilities.

4782 *9.4.1.1 Logging into Reporter*

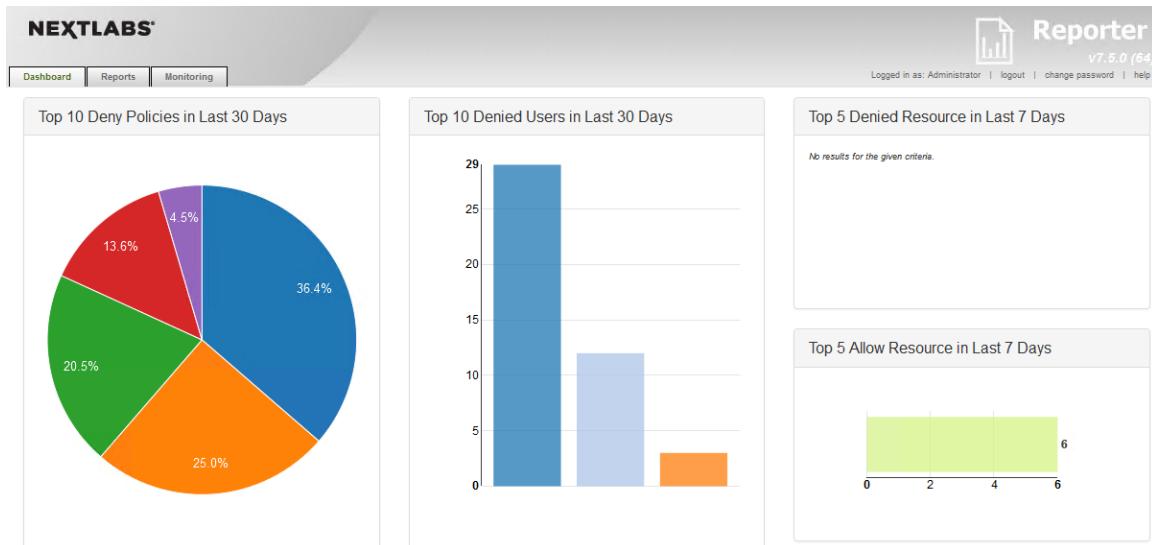
4783 Before being able to define a custom report, you must first log in to Reporter and click on the Reports
4784 tab as seen in the steps below:

- 4785 1. On the server where NextLabs Control Center was installed in [Section 7](#), open a web browser,
4786 i.e., SQL Server in this build.
- 4787 2. Enter the URL and press Enter: *https://<hostname>/reporter*, i.e., *https://localhost/reporter*
- 4788 3. At the Reporter login screen, enter valid credentials, such as the Control Center Administrator
4789 account created in [Section 7](#). Click **Login**.



4790

- 4791 4. In your browser, the Reporter user interface will default to the **Dashboard tab**. The Dashboard
4792 tab, Reports tab, and Monitoring tab will be discussed more thoroughly in subsequent sections
4793 of this How-To Guide.



4794

- 4795 5. Click on the **Reports tab** to open the Reports tab window.

The screenshot shows the NextLabs interface with the following components:

- Top Navigation:** Dashboard, Reports (highlighted in green), Monitoring.
- Saved Reports (Left Pane):**
 - Search bar:
 - Report Name dropdown menu:
 - Allow Enforcement in Last 7 Days (S)
 - Allow Resource in Last 7 Days (S)
 - Attempted Access Classified Documents
 - Denied Resource in Last 7 Days (S)
 - Denied Users in Last 30 Days (S)
 - Deny Enforcement in Last 7 Days (S)
 - Deny Policies in Last 30 Days (S)
 - Buttons: < / > / New
 - Text: Showing 1 to 7 of 7 entries
 - Buttons: Previous / Next
- Report Details (Right Pane):**
 - Report Query:**
 - From: 2015-07-15 00:00:00
 - To: 2015-07-15 23:59:59
 - Event Level: User Events (Level 3)
 - Policy Decision: Both
 - Action:** A list of actions with a scroll bar:
 - Ask Question
 - Attach to Item
 - Change Attributes
 - Change File Permissions
 - Copy / Embed File
 - User:** Text input field with a search icon.
 - User Criteria:** Text input field with dropdowns for operator (Equals) and value (Max 255 characters), and a plus sign (+).
 - Resource Name:** Text input field.
 - Resource Criteria:** Text input field with dropdowns for operator (Equals) and value (Max 255 characters), and a plus sign (+).

4796

4797 9.4.1.2 Defining the Custom Report

4798 In order to define a custom or new report, you must specify filters and change default settings within
 4799 the Report Details – Report Query pane. If you don't specify any filters or change any of the default
 4800 settings, the report retrieves all policy activity data categorized as user-level events for the current day.

Report Details

Report Query

From: **To:**

Event Level: **Policy Decision:**

Action:

Ask Question
Attach to Item
Change Attributes
Change File Permissions
Copy / Embed File

User:

User Criteria: Equals Max 255 characters

Resource Name:

Resource Criteria: FROM_RESOURCE Equals Max 255 characters

Policy Full Name:

Policy Criteria: POLICY_NAME Equals Max 255 characters

Other Criteria: APPLICATION_NAME Equals Max 255 characters

4801

- 4802 1. In the Report Details - Report Query pane, define the report query by filling in data or using drop-down menus to define your desired report.
- 4803
- 4804 a. Note: Many of the fields are optional. Required fields contain default values.
 - 4805 i. In the **From** and **To** fields, specify the start date and time, and end date and time, respectively, of the time period you want the report to cover. Click in the field to choose a date and time from the calendar. When specifying a report period, be sure to consider the time zone where Control Center is installed, and the time period of data stored in the Activity Journal.
 - 4806 ii. In **Event Level**, select the level of event verbosity the report contains:
 - 4807 1. User Events (default): Logged in the Activity Journal as Level 1
 - 4808 2. Application Events (application and user-level events): Logged in the Ac-
 - 4809 tivity Journal as Level 2
 - 4810 3. All System Events (system, application, and user-level events): Logged in the Activity Journal as Level 3

4816 Note: As a rule, you should leave this setting at User Events. This setting
4817 significantly reduces the amount of system noise. Application- or
4818 system-level events generally are not useful in monitoring policy or user
4819 activities.

4820 2. In **Decision**, select the type of enforcement effect to include in this report:

4821 a. Allow: Instances when the policy permitted the user to perform the action covered by
4822 the policy. Note that the report results always depend on what information is logged. If
4823 the policy does not have any On Allow logging obligation specified, this report will not
4824 return any On Allow data whether or not you select this option.

4825 b. Deny: Instances when the policy did not allow the user to perform the action. Deny
4826 decisions are always logged.

4827 c. Both: All instances when the policy was enforced, with either Allow or Deny effect.

4828 3. In **Action**, select the user action or actions to include in this report. The list shows all currently
4829 defined actions.

4830 a. To select multiple actions, hold Ctrl and click each action. If you do not make any
4831 selections, all actions are included.

4832 Note: Policies involving Paste actions do not support logging obligations, therefore,
4833 instances of their enforcement are not included in reports.

4834 4. In **User**, specify one or more users on which to filter the activity data, or leave this field blank to
4835 include all users. Use the User Lookup window (magnifying glass icon) to browse through all
4836 users currently defined in your Information Network Directory, and select the users you want.

4837 5. In **User Criteria**, specify additional user criteria by creating one or more conditions. Each
4838 condition consists of a user attribute, an operator, and a value. You must click the + button to
4839 add a condition to the query.

4840 6. In **Resource Path**, type the network path of the resource on which to filter, or leave this field
4841 blank to include all resources.

4842 7. In **Resource Criteria**, specify additional resource criteria by creating one or more conditions.
4843 Each condition consists of a resource attribute, an operator, and a value. Click the + button to
4844 add a condition to the query.

4845 8. In **Policy Name**, specify one or more policies on which to filter, or leave this field blank to
4846 include all policies. Use the Policy Lookup window to browse through and select which policies
4847 you want to include.

4848 9. In **Policy Criteria**, specify additional policy criteria by creating one or more conditions. Each
4849 condition consists of a policy attribute, an operator, and a value. Click the + button to add a
4850 condition to the query.

4851 10. In **Other Criteria**, specify additional criteria by creating one or more conditions. Each condition
4852 consists of a general attribute (for example, host name, host IP, and application name), an
4853 operator, and a value. Click the + button to add a condition to the query.

4854 ***9.4.1.3 Setting the Custom Report Display Options***

4855 Within the Report Details – Report Query pane, directly below the Other Criteria filter, continue with
 4856 these steps to set the display options for your custom report:

The screenshot shows the 'Report Details - Report Query' pane. It contains several configuration fields:
Report Type : A dropdown menu set to 'Table'.
Show : A dropdown menu set to '-- Group by options --'.
Sort By: A dropdown menu set to 'DATE', with radio buttons for 'Asc' and 'Desc' where 'Desc' is selected.
Max Results : A dropdown menu set to '100'.
Display Columns : A list box containing 'USER_NAME, HOST_NAME, APPLICATION_NAME, POLICY_FULLNAME, ...'.
At the bottom are two buttons: a blue 'Run' button with a play icon, and a blue 'Options' button with a dropdown arrow.

4857

- 4858 1. In **Report Type**, select the output format in which to display the data: Table, Bar Chart,
 4859 Horizontal Bar Chart, or Pie Chart. Use a table to display policy activity details in a row-and-
 4860 column format. Use a chart to display a summary of policy activities.
- 4861 2. If you selected one of the charts in Report Type, in **Show**, select a grouping option. Grouping is
 4862 not available to a table.
 - 4863 a. Group by User: The chart shows the number of enforcement events for each user
 4864 covered by the report.
 - 4865 b. Group by Resource: The chart shows the number of enforcement events for each
 4866 resource covered by the report.
 - 4867 c. Group by Policy: The chart shows the number of enforcement events for each policy
 4868 covered by the report.
 - 4869 d. Group by Month: The chart shows the number of enforcement events for each month
 4870 covered by the report. Select this option only if the time period you specified spans
 4871 more than one month.
 - 4872 e. Group by Day: The chart shows the number of enforcement events for each day covered
 4873 by the report.
- 4874 3. In **Sort By**, select a field on which to sort the data, then select Asc to sort in ascending order or
 4875 Desc to sort in descending order. If the report is a table, you can sort the data by any attribute. If
 4876 the report is a chart, you can sort either by the grouping item (user, resource, policy, month, or
 4877 day) or by Result Count (the number of enforcement events for each user, resource, policy,
 4878 month, or day).
- 4879 4. In **Max Results**, specify the maximum number of results to display in the table or chart. For
 4880 charts, this number represents the maximum number of bars in a bar chart, or slices in a pie

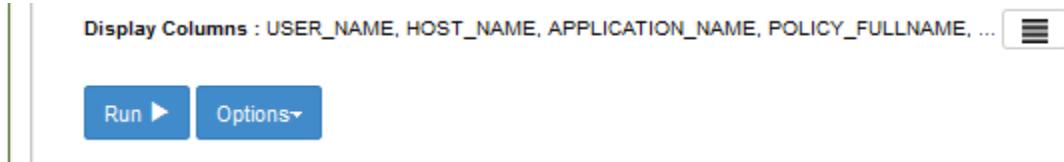
4881 chart. For readability reasons, charts should display a limited number of bars or slices. For a
 4882 table, the number represents the maximum number of rows (each row represents an event).
 4883 Tables that show a large number of rows present the data on multiple pages.

4884 5. In **Display Columns**, select the columns to display in a table. This setting applies to tables only.
 4885 **USER_NAME**, **POLICY_FULLNAME**, **POLICY_DECISION**, **HOST_NAME**, and **APPLICATION_NAME**
 4886 are selected by default. To remove any of those columns or to add other columns, click  and
 4887 use the arrow icons to move columns out of, or into, the Selected pane.

4888 9.4.2 Running a Custom Report

4889 Directly beneath the filters and data fields for defining the report and setting its display settings, do the
 4890 following in order to run the report and/or save it for the future:

4891 1. At the bottom of the Report Details – Report Query pane, click **Run** to generate the new report.



4892 2. If you want to run this report again in the future, save the report. Click **Options**, and select **Save**.



4894

4895 9.5 Example Custom Report and Available Formats

4896 In this section, we will present examples of different report formats, all representing a small set of event
 4897 data, returned by the same custom report from our build. By comparing the example formats, you will
 4898 gain a better understanding of the way the different formats can be used to highlight different aspects
 4899 of the same data depending on your business rules or priorities.

4900 The custom report used in this section will result from a query that requests all events by users on all
 4901 resources for one week (June 7, 2015 to June 13, 2015). We include columns that are relevant for our
 4902 example business logic and the ABAC policies we put in place in [Section 8](#). For example, we chose to
 4903 include the “Department” and “Sensitivity” columns, which were custom attributes in the metadata we
 4904 added to the documents uploaded to the RP’s SharePoint sites.

4905 9.5.1 Defining the Example Custom Report

4906 9.5.1.1 Customizing Report Query Fields for this Report

4907 1. In the Report Query pane, change the fields for the **From** and **To** date to match the desired
 4908 query for the week of June 7, 2015 to June 13, 2015.

SECOND DRAFT

- 4909 2. In the Report Query pane, click on the **Max Results** field to open the drop-down menu. We
4910 chose 11 for demonstration purposes.
- 4911 3. In the Report Query pane, leave the rest of the fields in the default query settings.

Report Query

From: 2015-06-07 00:00:00 **To:** 2015-06-13 23:59:59

Event Level: User Events (Level 3) **Policy Decision:** Both

Action:

- Ask Question
- Attach to Item
- Change Attributes
- Change File Permissions
- Copy / Embed File

User:

User Criteria: Equals Max 255 characters

Resource Name:

Resource Criteria: FROM_RESOURCE_PATH Equals Max 255 characters

Policy Full Name:

Policy Criteria: POLICY_NAME Equals Max 255 characters

Other Criteria: APPLICATION_NAME Equals Max 255 characters

Report Type : Table **Show :**

Sort By: DATE Asc Desc

Max Results : 11

Display Columns : USER_NAME, POLICY_NAME, POLICY_DECISION, FROM_RESOURCE_NAME, ...

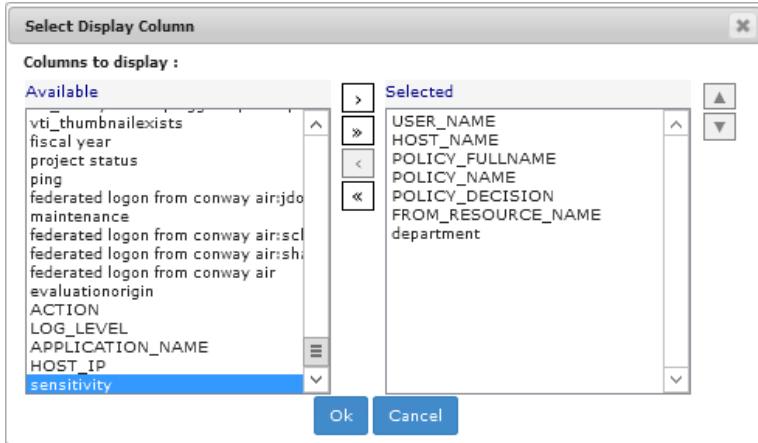
4912

4913 9.5.1.2 *Editing the Columns for Custom Views*

- 4914 1. Toward the bottom of the Report Query pane, click on the columns icon at the end of the
4915 Display Columns line of text to open the Select Display Column window.

4916

- 4917 2. In the Select Display Column window, in the **Available** attribute list, review standard attributes (i.e. Action, Log_Level, Host_IP, etc) and custom attributes (department, sensitivity).

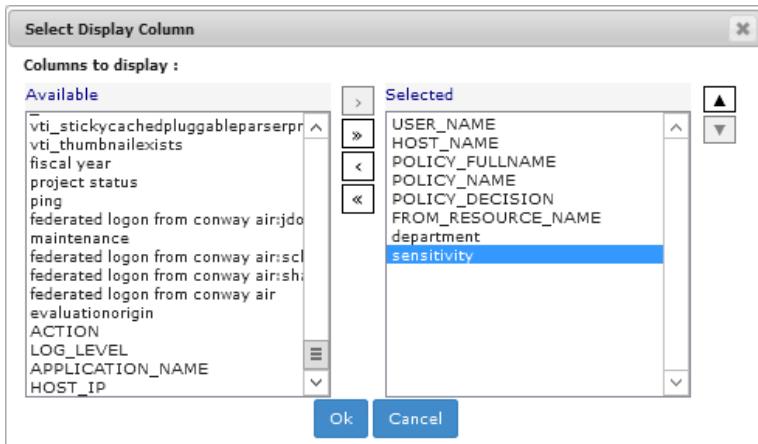


4919

- 4920 3. Click on any available attribute of interest to highlight it, then click the single right arrow button to add it to the list of **Selected** attributes.

4922 The attribute name will move from the **Available** list to the **Selected** list.

4923 **Note:** Attributes can be added and removed individually by using the single arrow buttons between lists, or as a group by using the double arrow buttons between lists.



4925

4926 *9.5.1.3 Running the Report Query*

- 4927 1. At the bottom of the Report Query pane, click **Run** to run the query. (**Tip:** You can click on **Options** and **Save** or **Save As** to save the query for future use.)

SECOND DRAFT

4929

- 4930 2. Scroll down in your browser window to see the Results pane illustrated in the following section.

4931 **9.5.2 Format: Table of Event Data**

4932 The default results pane with the display columns you selected displays showing the query results. This is illustrated in the following image.

Date	USER_NAME	POLICY_NAME	POLICY_DECISION	FROM_RESOURCE_NAME	department	sensitivity
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Denied	sharepoint://sharepoint.abac.test/internettechnology/documents/it dept - system configuration -level 3.rtf	Internet Technology	3
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint://sharepoint.abac.test/internettechnology	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint://sharepoint.abac.test/internettechnology	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint://sharepoint.abac.test/internettechnology	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint://sharepoint.abac.test/style library/en-us/themeable/core styles/controls15.css	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint://sharepoint.abac.test/style library/en-us/themeable/core styles/controls15.css	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint://sharepoint.abac.test/style library/en-us/themeable/core styles/controls15.css	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint://sharepoint.abac.test/sites/assets/runabout air logo.png	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint://sharepoint.abac.test/sites/assets/runabout air logo.png	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint://sharepoint.abac.test/sites/assets/runabout air logo.png	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air joe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Denied	sharepoint://sharepoint.abac.test/internettechnology/documents/it dept - onboarding doc -level 1.rtf	Internet Technology	1

4933
4934 This excerpt from the query results shows that:

- 4935 ▪ 13 pages of policy enforcement events were logged.
- 4936 ▪ All events in this excerpt occurred on June 12, 2015 (as illustrated in the **Date** column).
- 4937 ▪ Each event from this excerpt was triggered by the same user, who had logged in with a federated identity from the IdP (Sections 2 through 5)
- 4938
- 4939 ▪ Each event corresponds to one of three policies: SharePoint Protection – Sensitivity, SharePoint Protection – Maintenance Denied 5am-5pm, or SharePoint Protection – Department.
- 4940
- 4941 ▪ Five resources were involved:
 - 4942 • The first row shows that the resource was an .rtf document from the Internet Technology department's SharePoint sub-site, marked at sensitivity level 3.
 - 4943
 - 4944 • The second through fourth rows show that the resource was the Internet Technology department site.
 - 4945 • The fifth through seventh rows show that the resources were the underlying .css style sheet and logo used on the SharePoint site.
 - 4946 • The seventh through tenth rows (up to the second to last) show that the resources were the underlying .css style sheet and logo used on the SharePoint site.
 - 4947
 - 4948 • The eleventh and final row from this excerpt shows that the resource was another .rtf document from the Internet Technology department SharePoint sub-site, marked at sensitivity level 1.
 - 4949

SECOND DRAFT

- 4950 ■ In the case of three out of the five resources, the enforcement decision was Allow, as shown in the fourth column (second through tenth
4951 rows).
4952 ■ In the case of two out of the five resources, the enforcement decision was Deny, as shown in the fourth column (first and last rows).
4953 Keep these details in mind as you analyze the data in the following charts.

4954 **9.5.3 Format: Bar Chart Grouped by Policy Chart**

4955 Grouping events by policy is useful for identifying policies that are being triggered with unexpected
 4956 frequency, which may be an indication that they are improperly designed and cover users, resources or
 4957 actions that they should not. It can also indicate concentrated efforts at unauthorized data access. To
 4958 examine the latter possibility, it is often helpful to switch to the Group by User option in order to focus
 4959 on who is performing the activity, as seen in [Section 9.5.2](#).

4960 ***9.5.3.1 Customizing the Display Settings***

4961 1. Using the Report Details – Report Query window from [Section 9.5.2](#) for displaying the results in
 4962 **Table** format, make the following edits to display results in a **Bar Chart** grouped by **Policy**:

4963 a. From the **Report Type** list, select **Bar Chart**.

4964 b. From the **Show** list, select **Group by Policy**

4965 c. From the **Sort By** list, select **Policy**.

4966 d. From the **Max Results** list, choose a number or type one in the field.

4967 Example: The value 6 means that our bar chart will display up to six policies, including
 4968 but not limited to the number of policies displayed in the Table format.

4969 e. Click on the **Asc** (Ascending) radio button to set the sorting order.

The screenshot shows a configuration interface for a report query. It includes fields for 'Report Type' (set to 'Bar Chart'), 'Show' (set to 'Group by Policy'), 'Sort By' (set to 'Policy'), and 'Max Results' (set to '6'). The 'Asc' radio button is selected for sorting order.

4970

4971 ***9.5.3.2 Running the Report Query***

4972 1. At the bottom of the Report Query pane, click **Run** to run the query

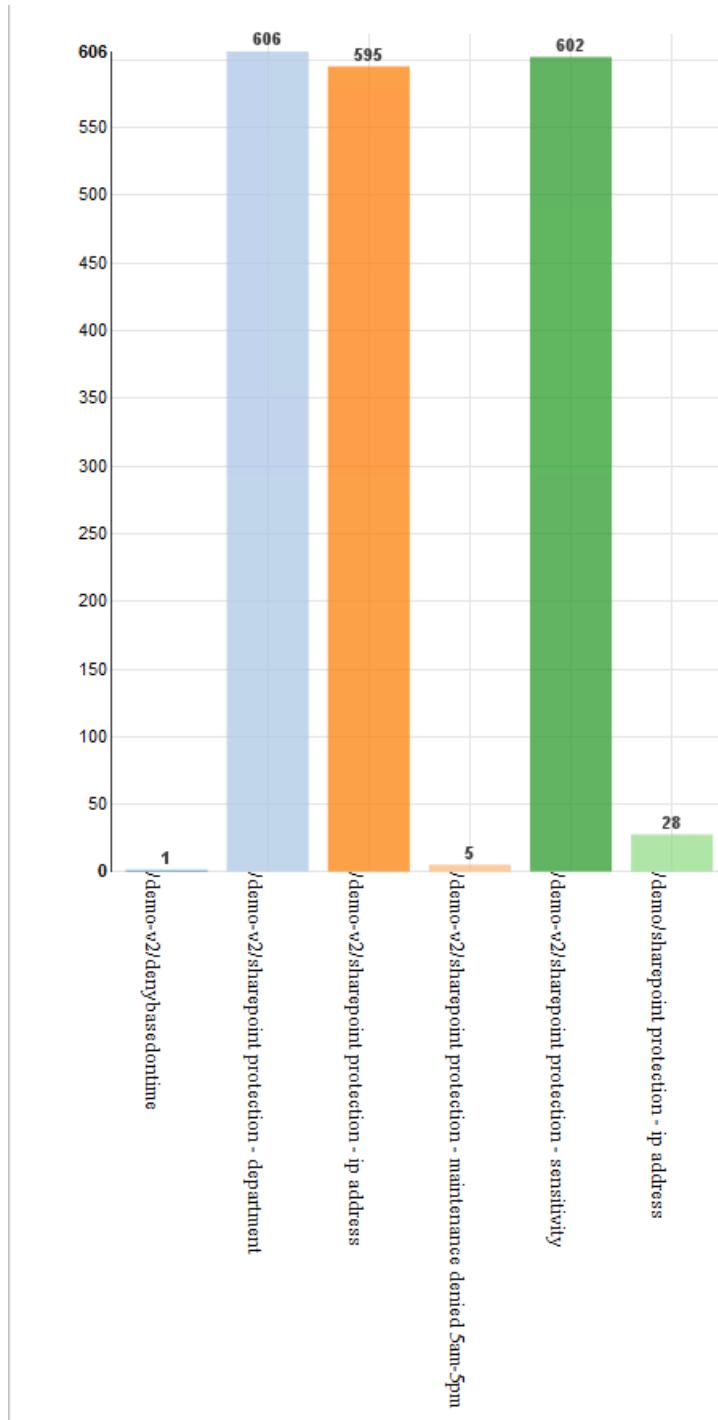
The screenshot shows the bottom pane of the report query window. It features a 'Run' button with a play icon and an 'Options' dropdown menu.

4973

4974 ***9.5.3.3 Viewing the Results as a Bar Chart Grouped by Policy***

4975 1. In the same browser window, scroll down if necessary. Under the **Run** button, review the
 4976 resulting Bar Chart Grouped by Policy.

4977 As illustrated below, hundreds of enforcement decisions were logged during the week, and the
 4978 three most commonly evaluated policies include two that were included in the table from
 4979 [Section 9.5.2](#), formatting results by Table.



4980

4981 **9.5.4 Format: Bar Chart Grouped by User Chart**

4982 When the same data is grouped by user, and the bar chart is selected, the following chart is generated.
4983 As noted previously, the four policies were each triggered by a different user, so the graph shows four
4984 bars—each representing one user. Each is labeled with a user name. In this example, the bars are the
4985 same height, since each of the four users triggered a policy once.

4986 ***9.5.4.1 Customizing the display settings***

4987 1. Using the same Report Details – Report Query window from the previous subsection, make the
 4988 following edits to display results in a Bar Chart Grouped by Policy.

4989 a. From the **Report Type** list, select **Bar Chart**.

4990 b. From the **Show** list, select **Group by User**.

4991 c. From the **Sort By** list, select **User**.

4992 d. From the **Max Results** list, choose a number or type one in the field.

4993 Example: The value 6 indicates that this will be the maximum number of users reflected
 4994 in our Bar Chart.

4995 e. Leave **Asc** selected.

The screenshot shows the 'Report Type' set to 'Bar Chart', 'Show' set to 'Group by User', 'Sort By' set to 'User' with 'Asc' selected, 'Max Results' set to 6, and 'Display Columns' showing 'USER_NAME, POLICY_NAME, POLICY_DECISION, FROM_RESOURCE_NAME, ...'. There are 'Run' and 'Options' buttons at the bottom.

4996

4997 ***9.5.4.2 Running the Report Query***

4998 1. At the bottom of the Report Query pane, click **Run** to run the query.

The screenshot shows the 'Display Columns' list and the 'Run' and 'Options' buttons at the bottom.

4999

5000 ***9.5.4.3 Viewing the Results as a Bar Chart Grouped by User***

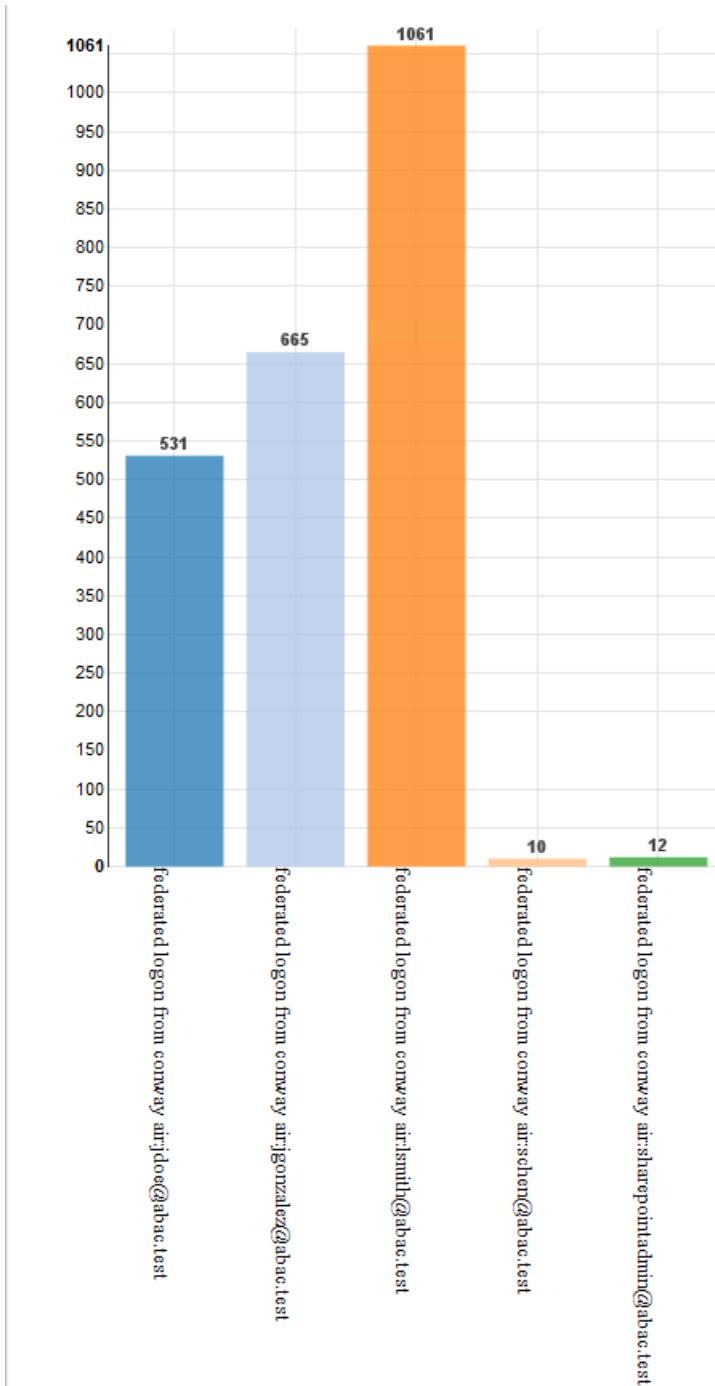
5001 1. In the same browser window, scroll down if necessary. Under the **Run** button, review the
 5002 resulting Bar Chart Grouped by User:

5003 As illustrated below, only five users were accessing the protected RP SharePoint resources
 5004 during this week period, and all logged in via federated identity from the IdP.

5005 ▪ Two users had very minimal activity logged during this week: schen@abac.test and
 5006 sharepointadmin@abac.test

5007 ▪ Two users had relatively similar activity logged during this week: jdoe@abac.test and
 5008 jgonzalez@abac.test

5009 ▪ One user had an extremely large amount of activity logged during this week:
 5010 lsmith@abac.test



5011

5012 9.5.5 Format: Pie Chart Grouped by Resource

5013 The Group by Resource option shows the extent of specified events—in this case, policies being
 5014 triggered—per individual resource covered by the report.

5015 Because policies often cover large numbers of individual documents or other resources, grouping by
 5016 resource is only helpful when the number of events has already been narrowed down to a smaller set by
 5017 various report filters, such as policies or users. A pie charts is ideal here, because in the context of

5018 resource use, the *relative* access activity regarding some single file or other resource as compared to all
 5019 others is generally of more interest than any *absolute* number of instances of access.

5020 **9.5.5.1 Customizing the Display Settings**

5021 1. Using the same Report Details – Report Query window from the previous subsection, make the
 5022 following edits to display results in a Bar Chart grouped by Policy

5023 a. From the **Report Type** list, select **Pie Chart**.

5024 b. From the **Show** list, select **Group by Resource**.

5025 c. From the **Sort By** list, select **Resource**.

5026 d. From the **Max Results** list, select a number or type one.

5027 Example: The value 10 means that will be the maximum number of resources displayed
 5028 in our Pie Chart.

5029 e. Leave **Asc** selected.

The screenshot shows the 'Report Type' dropdown set to 'Pie Chart', the 'Show' dropdown set to 'Group by Resource', the 'Sort By' dropdown set to 'Resource' with 'Asc' selected, and the 'Max Results' input field set to '10'. Below these, a 'Display Columns' section lists 'USER_NAME', 'POLICY_NAME', 'POLICY_DECISION', 'FROM_RESOURCE_NAME', and an ellipsis. At the bottom are 'Run' and 'Options' buttons.

5030

5031 **9.5.5.2 Running the Report Query**

5032 1. At the bottom of the Report Query pane, click **Run** to run the query.

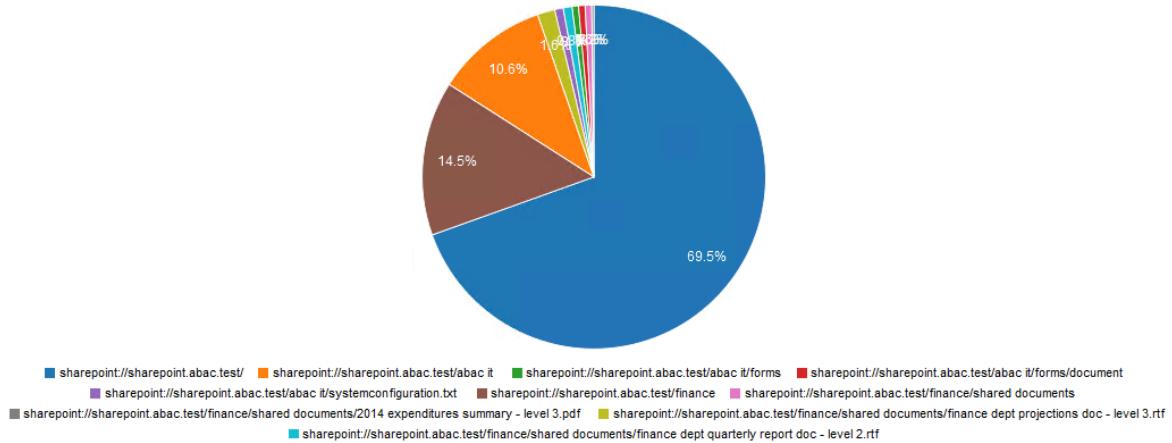
5033 **9.5.5.3 Viewing the Results as a Bar Chart Grouped by User**

5034 1. In the same browser window, scroll down if necessary. Under the **Run** button, review the
 5035 resulting Bar Chart Grouped by Policy:

5036 As illustrated below, the maximum of ten resources are displayed in the pie chart.

- 5037 ■ The most commonly accessed resource during this week period (69.5%) was our build's
 5038 SharePoint home page.
- 5039 ■ The two second-most accessed resources during this week period were the ABAC IT
 5040 department and its forms sub-site (where documents are stored).
- 5041 ■ The remaining seven most-accessed resources during this week after the top three have
 5042 relatively very minimal access, and the majority of those are documents that belong to

5043 specific department sub-sites, such as Finance Dept Quarterly Reports, IT Dept System
 5044 Configuration documents, etc.



5045

5046 9.6 Further Example Custom Reports from Our Build

5047 In this section, we will illustrate how to define custom reports that will provide a graphical
 5048 representation of particular kinds of activity that could be of interest to our RP business.

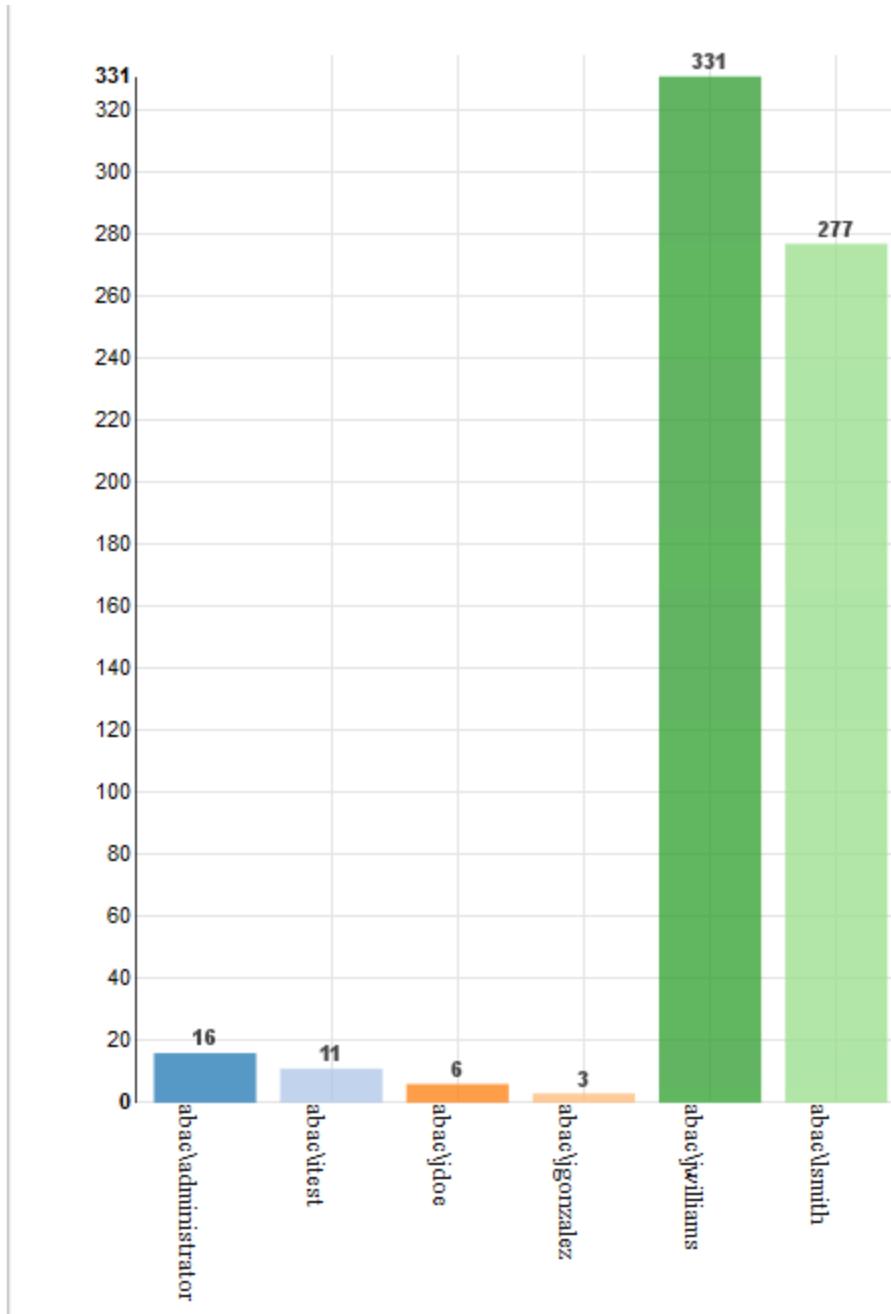
5049 For our first additional example, we will use a fictitious user from our build's IdP and check her activity
 5050 on the RP SharePoint site within a specific time period. The report we define will focus on the user Lucy
 5051 Smith (username: **Ismith**) and all of her Allowed and Denied access during a specific timeframe, such as
 5052 May 1, 2015 – June 30, 2015.

5053 For our second additional example, we will use a document on the RP SharePoint site that has been
 5054 marked with a metadata attribute called sensitivity. The document's sensitivity value is set to 3, which
 5055 according to our example ABAC policies requires that 1) the user accessing the document belongs to the
 5056 same or appropriate department for accessing it, 2) the access occurs during regular business hours
 5057 Monday-Friday, and 3) the user has a clearance attribute value of **Top Secret**. The report we define will
 5058 focus on the access attempts on that document for the months of May and June 2015.

5059 9.6.1 Custom Report Illustrating All Access for One User During a Two-Month 5060 Period

- 5061 1. Follow the steps for [Section 9.5.4](#), Format: Bar Chart Grouped by User, and change the **From**
 5062 field to May 1, 2015 and the **To** field to June 30, 2015.
- 5063 2. Within the browser, in the results area at the bottom of the Report Details window, click on the
 5064 vertical bar that represents the user **Ismith@abac.test** or **abac\Ismith** (light green, the far-right
 5065 bar in our chart below).

5066 The Report window of your browser will automatically refresh, and a default query on the User
 5067 will run automatically.



5068

5069 3. Within the browser window, scroll up to Report Details and verify that the User: field was
5070 automatically populated with **abac\lsmith**.

5071 In the Report Query pane, you will see that the default query pertaining to the User has a Report
5072 type of Table, sorted by date in descending order, with a maximum of 100 results.

Report Query

From: 2015-05-01 00:00:00 **To:** 2015-06-30 23:59:59

Event Level: User Events (Level 3) **Policy Decision:** Both

Action:

- Ask Question
- Attach to Item
- Change Attributes
- Change File Permissions
- Copy / Embed File

User: abacismith **Search:**

User Criteria: Equals Max 255 characters **Add:**

Resource Name:

Resource Criteria: FROM_RESOURCE_PATH Equals Max 255 characters **Add:**

Policy Full Name: **Search:**

Policy Criteria: POLICY_NAME Equals Max 255 characters **Add:**

Other Criteria: APPLICATION_NAME Equals Max 255 characters **Add:**

Report Type : Table **Show :** -- Group by options --

Sort By: DATE **Asc:** **Desc:**

Max Results : 100

5073

- 5074 4. Within the browser window, scroll back down to the resulting Table to review its data. See the
5075 excerpt below.

5076 If desired, you can change the Display Columns, Report Type, etc. to customize your view as
5077 illustrated in previous subsections.

Date	USER_NAME	ACTION	POLICY_FULLNAME	POLICY_DECISION
May 15, 2015 9:59 AM	abacismith	Open	testboxccosemail	Allows
May 15, 2015 12:18 PM	abacismith	Open	/scenario 1/scenario 1-1	Denied
May 15, 2015 12:20 PM	abacismith	Open	/scenario 1/scenario 1-1	Denied
May 18, 2015 12:21 PM	abacismith	Open	/scenario 1/scenario 1-1	Denied
May 20, 2015 11:42 AM	abacismith	Open	/scenario 1/scenario 1-1	Denied
May 20, 2015 11:47 AM	abacismith	Open	/scenario 1/scenario 1-1	Denied

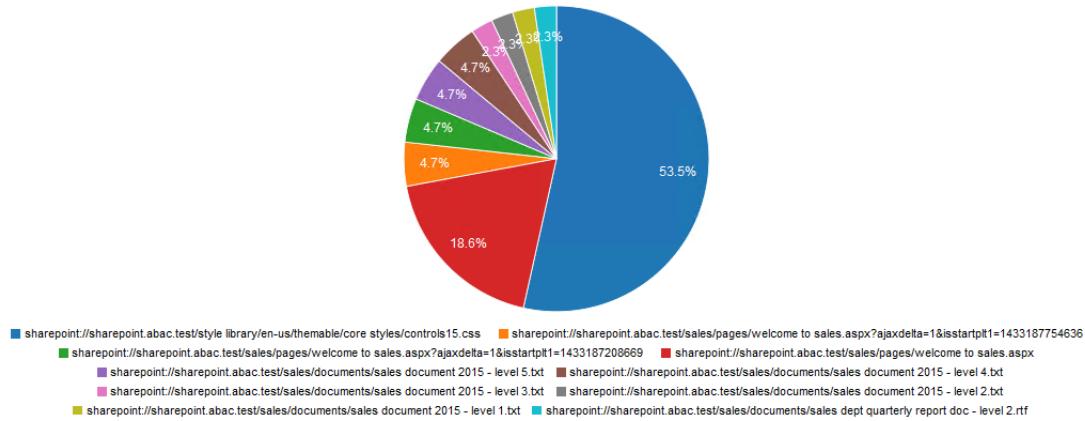
5078

5079 9.6.2 Viewing Access Attempts on Individual Resources

5080 This section provides instructions for creating a custom report that shows the access attempts of a
5081 single resource for a period of two months.

- 5082 1. Follow the steps for [Section 9.5.5](#), Format: Pie Chart Grouped by Resource, and change the **From**
5083 field to May 1, 2015 and the **To** field to June 30, 2015.
- 5084 2. From the resulting list of resources under the pie chart, find the color of a resource with a name
5085 including **level 3**, which according to our schema means in SharePoint metadata the sensitivity
5086 level attribute is equal to 3.
- 5087 3. Click on that resource in the pie chart (example: light pink area of 2.3% is for a Sales Dept
5088 document called **sales document 2015 – level 3.txt**).

5089 This will begin an automatic default query for that resource similar to the one done above based
5090 on the user **Ismith**.



- 5091 4. Within the browser window, scroll up to Report Details and verify that the Resource Name: field
5092 was automatically populated with the name **Sales document 2015 – level 3.txt**.

5094 In the Report Query pane, you will see that the default query pertaining to the resource has a
5095 Report type of Table, sorted by date in descending order, with a maximum of 100 results.

Report Query

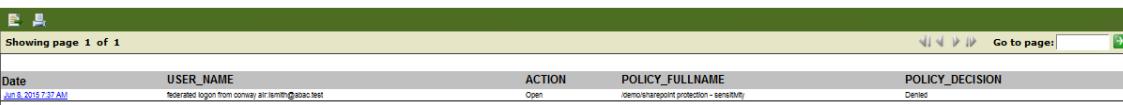
From:	To:
2015-06-01 00:00:00	2015-06-30 23:59:59
Event Level:	Policy Decision:
User Events (Level 3)	Deny
Action:	
Ask Question Attach to Item Change Attributes Change File Permissions Copy / Embed File	
User:	<input type="text"/> <input type="button" value="Q"/>
User Criteria:	<input type="text"/> Equals <input type="text"/> Max 255 characters <input type="button" value="+"/>
Resource Name:	sharepoint://sharepoint.abac.test/sales/documents/sales document 2015 - level 3.txt
Resource Criteria:	<input type="text"/> Equals <input type="text"/> Max 255 characters <input type="button" value="+"/>
Policy Full Name:	<input type="text"/> <input type="button" value="Q"/>
Policy Criteria:	<input type="text"/> Equals <input type="text"/> Max 255 characters <input type="button" value="+"/>
Other Criteria:	<input type="text"/> Equals <input type="text"/> Max 255 characters <input type="button" value="+"/>
Report Type :	Show :
Table	-- Group by options -- <input type="button" value="▼"/>
Sort By:	<input type="text"/> <input type="radio"/> Asc <input checked="" type="radio"/> Desc
Max Results :	<input type="text"/> 100

5096

- 5097 5. Within the browser window, scroll back down to the resulting table to review its data. See the
5098 excerpt below.

5099
5100

If desired, you can change the Display Columns, Report Type, etc. to customize your view as illustrated in previous subsections.



The screenshot shows a table with the following data:

Date	USER_NAME	ACTION	POLICY_FULLNAME	POLICY_DECISION
Jun 8 2015 11:37 AM	federated logon from conway air lsmith@abac.test	Open	demo/sharepoint protection - sensitivity	Denied

10 Configuring a Secondary Attribute Provider

10.1 Introduction

This section provides a description of the architecture, compilation, and deployment instructions for a secondary attribute provider and its components, which we describe as a custom Policy information point (PIP), to be included as part of the ABAC infrastructure. We also demonstrate how to configure the Relying Party server to accommodate the custom PIP and its component JIT provisioning mechanism.

The secondary attribute provider comes into the picture when a user tries to access a resource at the Relying Party's Resource Provider, and the Policy decision point (PDP) finds that an essential attribute needed to make the access control decision is missing from the initial set of attributes sent from the Identity Provider. In our build, this would mean a user with a federated identity (via PingFederate Identity Provider, IdP, augmented with two-factor authentication by RSA AA) has already logged into Microsoft SharePoint (Relying Party's Resource Provider), but when trying to open a particular resource on the site, the NextLabs Policy Controller (PDP) makes a run-time decision that additional subject attributes are needed before the access decision can be made. The PDP determines this while evaluating the existing ABAC policies (created in the NextLabs Policy Studio, PAP in our ABAC build) against the user, resource, and environmental attributes at play at the time of requested access.

Providing the secondary attribute collection capability in our build required the implementation of new components and related features, which we will describe more in detail later in the section:

- NextLabs Policy Information Point (PIP) Plugin to extend the NextLabs Policy Controller (PDP) when additional attribute(s) are needed
- Protocol broker to initiate and receive a SAML attribute query and SAML response
- Custom data store plugin for PingFederate on the Relying Party (RP) server which will cache attributes in order to limit the number of secondary requests to the PingFederate Identity Provider (IdP) server
- Apache Directory Server (ApacheDS), an LDAP in which PingFederate can create and update local user accounts and associated attributes based on the attributes contained in SAML assertions received after authentication from IdP
- PingFederate RP configuration must be modified so that it can serve as an IdP as needed, such as when checking its JIT cache (Apache DS LDAP) before sending requests to the IdP

In later sub-sections of this section we will discuss in detail the purpose of each of these new components and features, and how they are developed, configured, compiled, and deployed.

Note: The custom PIP we have developed involves new custom components, open source components, and commercially available components. For open source and commercial components, the related descriptions in this section have been limited to installation and relevant configuration required for the desired functionality of our build. If you are interested in other details or additional capabilities of this software, explore the referenced product literature or contact that organization.

10.1.1 Pre-Requisites

In order to follow the instructions of this How-To section, it is necessary that seven of the previous How-To sections have been successfully completed. The required components that must be installed and configured before continuing in this How-To section include:

- Installation and Configuration of Active Directory ([Section 2](#))
- Installation and Configuration of RSA AA ([Section 2](#))
- Installation and Configuration of RSA AA Plugin ([Section 2](#))
- Installation and Configuration of PingFederate on both the RP and IdP federation servers ([Section 2](#) and [Section 3](#)),
- Installation and Configuration of Microsoft SharePoint ([Section 4](#) and [Section 5](#))
- Configuration of the attribute flow ([Section 6](#))
- Installation and Configuration of NextLabs Control Center, Policy Studio, Policy Controller, and Entitlement Manager for SharePoint Server ([Section 7](#))

10.1.2 Criteria for Secondary Attribute Collection

At the time of ABAC policy evaluation, required attributes may not be available or the system may not find it appropriate to use for various reasons, including, but not limited to:

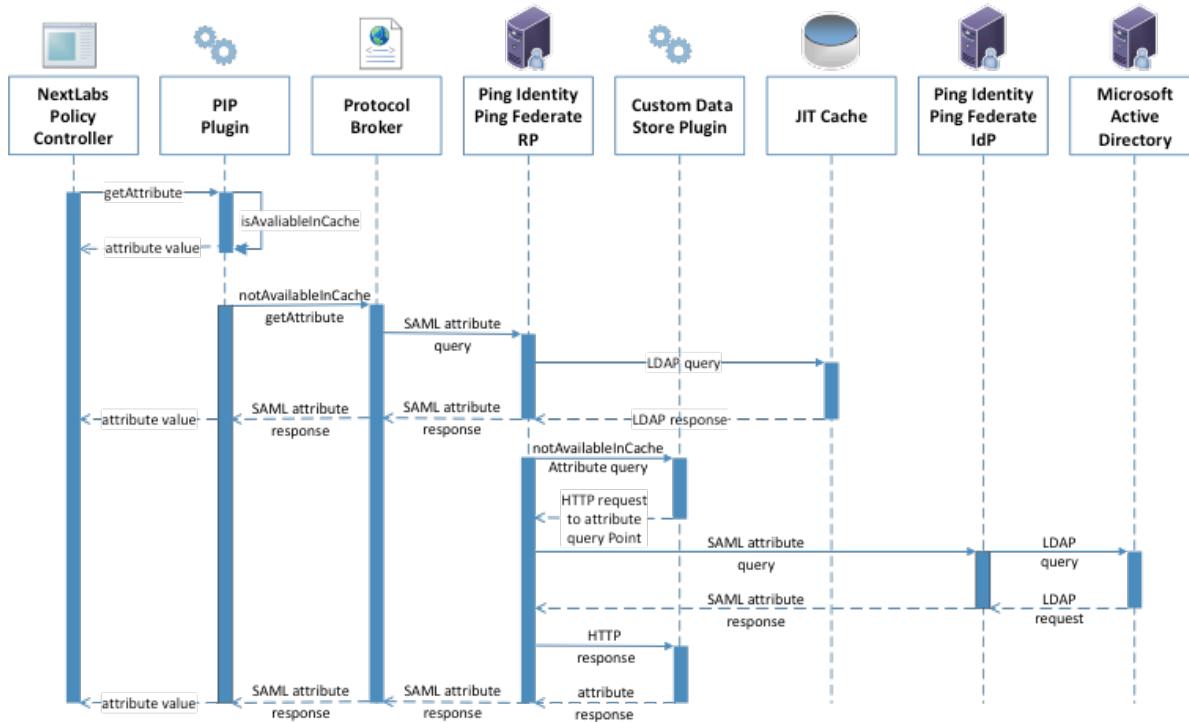
- For security and privacy purposes it is not ideal to acquire all known attributes for a subject when the session is created. Some attributes maybe PII or of higher sensitivity and should not be sent to the relying party until an access request made by the user requires those attributes.
- Depending on the longevity of a session, attributes risk becoming stale. Because of this potential for staleness, it is essential to procure attributes as needed, depending on the freshness criteria established by the system. The freshness of attributes is sometimes guided by the policies established for a local cache.
- The attribute needed for a specific attribute request may not an attributed owned by the Identity provider but rather may need to be acquired from an external party attribute provider.

10.1.3 Components

The custom PIP described in this section is composed of four new components and mechanisms which interact or integrate with different existing components in our ABAC build as extensions, plugins, or web applications:

- **NextLabs Plugin:** This plugin extends the NextLabs Policy Controller to make attributes available based on the criteria mentioned in Section 10.1.2, when the PDP determines that attribute values needed to evaluate an ABAC policy are insufficient or unavailable. Following the recommendation in the software development framework provided by NextLabs, the NCCoE implemented this PIP plugin in Java, and deployed the plugin within the NextLabs Policy Controller software architecture on the server we call SharePoint server in our build. Due to the requirements of the Policy Controller architecture, the plugin can request the values of multiple missing attributes sequentially, one at a time.

- 5175 ■ **Protocol Broker:** This agent, in the form of [servlet](#) local to the NextLabs installation, is
5176 responsible for facilitating communication between the NextLabs PIP Plugin and the
5177 PingFederate RP server following an Assertion Query/Request SAML2 Profile. This web
5178 application is deployed on a tomcat server that listens on localhost(127.0.0.1) and only
5179 communicates using https with mutual TLS. Similar to the NextLabs PIP Plugin, this component is
5180 also installed on the SharePoint server.
- 5181 ■ **Ping Custom Data store:** This custom data store is an extension built using Ping SDK. It enables
5182 the RP server to query the IdP server and coordinates resulting attribute values back to the RP.
5183 When it is chained with a built-in data store to query JIT Cache (LDAP), it enables RP to provide
5184 data from and configuration to various data stores (JIT in this build). This helps the custom data
5185 store to query and coordinate the result from local JIT and remote Active Directory at the
5186 PingFederate IdP.
- 5187 ■ [Just-in-Time provisioning](#) is a feature provided by PingFederate to store attributes of a subject
5188 for a limited time. We implemented JIT provisioning using [ApacheDS](#). ApacheDS 2.0 is an
5189 embeddable, extendable, standards compliant, modern LDAP server written entirely in Java, and
5190 available under the [Apache Software License](#). It also supports network protocols like Kerberos
5191 and NTP. PingFederate RP acts as an IdP for the secondary attribute provider. To fulfill in this
5192 role, the PingFederate administrative console provides mechanisms to configure SP and IdP
5193 connections. These configurations manage connection settings to support the exchange of
5194 federation-protocol messages. It also allows configuration of data stores within the connection
5195 and an attribute contract that acts as the medium to convey attribute mapping from one entity
5196 to another.

5197 **10.1.3.1 Sequence Diagram of Custom PIP Component Interactions**5198 **Figure 10-1 Architecture**

5199

5200 **10.1.3.1.1 Description**

5201 Nextlabs PDP (Policy Controller) is the arbitrator for all access decisions at the SharePoint portal. It
 5202 controls access to SharePoint URL(s) by evaluating rules against the attributes of the entities (subject
 5203 and object), actions, and the environment relevant to a request. It may be possible that the attribute
 5204 required for the decision is not available at run time. In that case, it looks for the registered plugin that
 5205 will fetch the attribute using the following flow:

- 5206 1. When the policy controller does not receive the attributes required to make a decision, a
 5207 secondary attribute request will be initiated by calling the PIP Plugin.
- 5208 2. PIP Plugin is a registered plugin with the NextLabs Policy Controller. It implements the interface
 5209 dictated by the NextLabs software. By virtue of this implementation, it receives the subject and
 5210 name of the attribute that is required for the policy decision.
- 5211 3. When the subject and attribute name are received, the PIP Plugin checks its local short-term
 5212 cache (in this build, configured to hold values for two seconds) to see if the needed attribute for
 5213 the subject was recently requested.
- 5214 4. If the attribute is still in cache, the value is returned to the Policy Controller. If the value is not in
 5215 cache, the PIP Plugin initiates an HTTPS request to the Protocol Broker.

- 5216 5. The Protocol Broker receives the attribute name and subject from the HTTPS request and
5217 forwards them as a signed SAML 2.0 Attribute Query to PingFederate-RP on a channel protected
5218 by mutual TLS.
- 5219 6. Once PingFederate-RP receives the SAML 2.0 attribute query, it sends an LDAP request to the JIT
5220 cache to see if the attribute was previously queried in a secondary request.
- 5221 7. If the subject does not have the attribute value assigned in the JIT cache, PingFederate-RP will
5222 forward the subject and attribute name to the Custom Data Store plugin. The Custom Data Store
5223 plugin acts as a pointer back to the PingFederate-IdP. To do this, the Custom Data Store
5224 dispatches an HTTPS request to the PingFederate-RP with the PingFederate-IdP as the attribute
5225 query point.
- 5226 8. Ping Federate uses an HTTPS query to form a SAML 2.0 attribute query and dispatch it to the
5227 Ping Federate at the IdP.
- 5228 9. The Ping Federate at the IdP accepts the SAML 2.0 request, verifies if the user has the attribute
5229 of need, and replies back to the PingFederate-RP with a SAML 2.0 response.
- 5230 10. PingFederate-RP validates the SAML 2.0 response, retrieves attribute values, and responds to the
5231 original Custom Data Store HTTP request with the attribute values.
- 5232 11. The Custom Data Store then responds to the PingFederate-RP attribute request with an attribute
5233 response.
- 5234 12. The PingFederate-RP constructs a SAML 2.0 response and sends it to the Protocol Broker.
- 5235 13. The Protocol Broker retrieves the attribute or exception from the SAML 2.0 response and
5236 forwards it to the NextLabs plugin, which passes the attribute or exception back to the Policy
5237 Controller.

5238

10.2 Component Software and Hardware Requirements

Component	Server where component is installed	Compilation method	Required software or hardware	Operating System	Optional Software
Ping Custom Data Store	PingFederate RP server	Ant 1.9.2	PingFederate 7.3.2; Java version same as PingFederate installed	Windows Server 2012	
NextLabs Plugin	SharePoint server	Apache Maven 3.2.5	SharePoint 2013; NextLabs Entitlement Manager for SharePoint Server, NextLabs Policy Controller, NextLabs Control Center, NextLabs Policy Studio; SQL Server 2012; Java version same as NextLabs Policy Controller installed (1.6)	Windows Server 2012	BareTail (used here as a log file annotator) Copyright Bare Metal Software Pty Ltd. Download 05/22/2015.
Protocol Broker	SharePoint server	Apache Maven 3.2.5	PingFederate 7.3.2; SharePoint 2013; NextLabs Entitlement Manager for SharePoint Server, NextLabs Policy Controller, NextLabs Control Center, NextLabs Policy Studio; SQL Server 2012;	Windows Server 2012	
Apache Directory Server		N/A	PingFederate 7.3.2; Java 7.0 (recommended by Oracle's JDK . Some issues have been reported with Java 8); 384 MB of memory by default, can be changed using Apache Directory Studio (included)	Windows Server 2012	

5239 **10.3 Ping Custom Data Store**

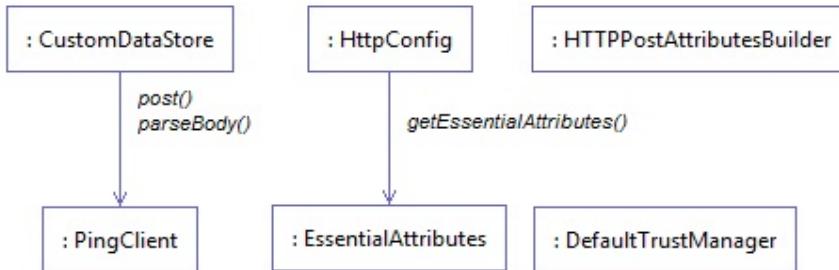
5240 **10.3.1 Functionality and Architecture**

5241 This data store was developed according to the guidelines from the Ping Identity provided [here](#). It has
5242 three functionalities:

- 5243 ▪ Configuration
 - 5244 • HttpConfig class is used to read in a configuration file for the custom data store.
5245 Configuration parameters, like truststore location, password and attribute names can be
5246 defined in a file and read in as a configuration by HttpConfig class. The structure of the
5247 HttpConfig class configuration is based on [spring](#) annotation.
 - 5248 • Other sets of configuration can be read via a web interface. A detailed description of these
5249 parameters is provided in step 9 of [Section 10.3.4](#) in this how-to guide.
- 5250 ▪ Communication
 - 5251 • Similarly, dispatching the http request relies on PingClient class. PingClient uses classes
5252 under the [spring](#) http package. PingClient sends an https query to Attribute Query End Point.
5253 All of the parameters for the https URL are provided by the web interface.
- 5254 ▪ Custom Data Store
 - 5255 • CustomDataStore is a class that implements
5256 com.pingidentity.sources.CustomDataSourceDriver.
 - 5257 • It implements all methods specified by the contract, i.e.:
 - 5258 – boolean testConnection(): This method tests whether a host and port is reachable or
5259 not. It is assumed that if host and port is reachable, a URL will be available.
 - 5260 – java.util.List<java.lang.String> getAvailableFields():
 - 5261 – java.util.Map<java.lang.String,java.lang.Object> retrieveValues(
5262 java.util.Collection<java.lang.String> attributeNamesToFill,
5263 SimpleFieldList filterConfiguration)

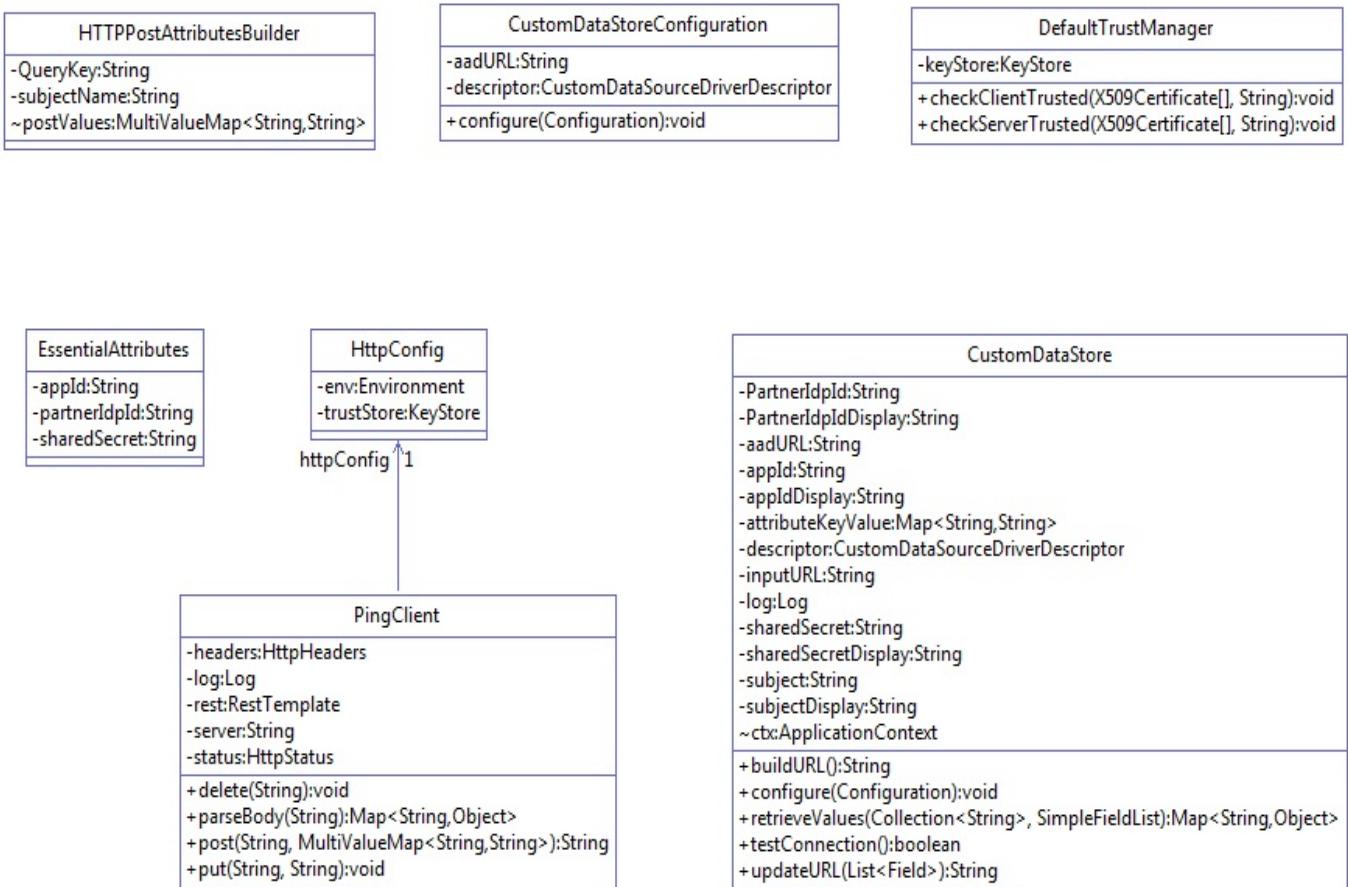
5264 The Class Structure and their interactions are provided in the Interaction Diagram and Class Diagram.

5265 **Figure 10-2 Ping Custom Data Store Interaction Diagram**



5266

5267 Figure 10-3 Ping Custom Data Store Class Diagram



5268

5269 10.3.2 Deploying the Ping Custom Data Store

5270 Note: PingFederate [administrator's manual](#) provides detailed steps for every platform. In our build, we
5271 used the Windows Server 2012 platform.

- 5272 1. Log on to the PingFederate RP server.
- 5273 2. Click on the Windows icon and begin typing **Services**.
- 5274 3. Double-click the Services application icon.
- 5275 4. Click on the Name column to sort by alphabetical order, and look for **PingFederateService**.
- 5276 5. If the status column reads **running**, right-click on **PingFederateService** and click **Stop**.
- 5277 6. Prepare environment based on [PingFederate documentation](#). This may involve going to
5278 `../pingfederate-7.3.0/pingfederate/sdk folder`
- 5279 7. Click on the Windows icon and begin typing **Cmd**.
- 5280 8. Double-click the icon to open the Command Prompt.

- 5281 9. In Command Prompt, navigate to your installation of PingFederate and its sdk folder by typing
 5282 the following command and pressing Enter. Example: `cd C:/pingfederate-`
 5283 `7.3.0/pingfederate/sdk/`
- 5284 10. Within the sdk folder, locate **build.local.properties** and open it with your default text editor. For
 5285 example, enter the following command and press Enter: `notepad build.local.properties`
- 5286 11. In your default text editor (Notepad in our example), set or update **target-plugin.name** to **idp-**
 5287 **query-data-store**, i.e., # Please set the 'target-plugin.name' property to the name of the
 5288 directory (under plugin-src) that # contains the source code of the plugin you want to build.
`target-plugin.name=idp-query-data-store`
- 5289 12. Within the Command Prompt window, navigate to your **idp-query-data-store** folder by entering
 5290 a cd command with a path to your **idp_query_data_store** and pressing Enter. Example: `cd C:/--`
 5291 `path-to-your-idp_query_data_store`
- 5292 13. Within the Command Prompt window, copy **idp-query-data-store** along with all subfolders to
 5293 your PingFederate installation's **sdk/plugin-src** folder by entering a cp command and pressing
 5294 Enter. Example: `cp -rf idp_query_data_store C:/pingfederate-`
 5295 `7.3.0/pingfederate/sdk/plugin-src`
- 5296 14. Within the Command Prompt window, run the following command and press enter in order to
 5297 make sure all relevant subfolders exist: `ls -ltr ./idp-query-data-store/`

- 5299 a. Example results from the above command:

```
5300            total 4
5301            drwxrwxr--. 3 t... t.... 16 Apr 29 11:34 java
5302            drwxrwxr--. 2 t... t.... 4096 Apr 29 12:59 lib
5303            drwxrwxr-x. 4 t... t.... 30 May 15 17:52 build
5304            drwxrwxr--. 2 t... t.... 51 May 29 09:26 conf
```

5305 10.3.3 Compilation

5306 The [Building and Deploying with Ant](#) section of the [SDK Developer's Guide](#) by Ping provides a detailed
 5307 description of compiling and deploying the project using Apache Ant. For current deployment, it may be
 5308 sufficient.

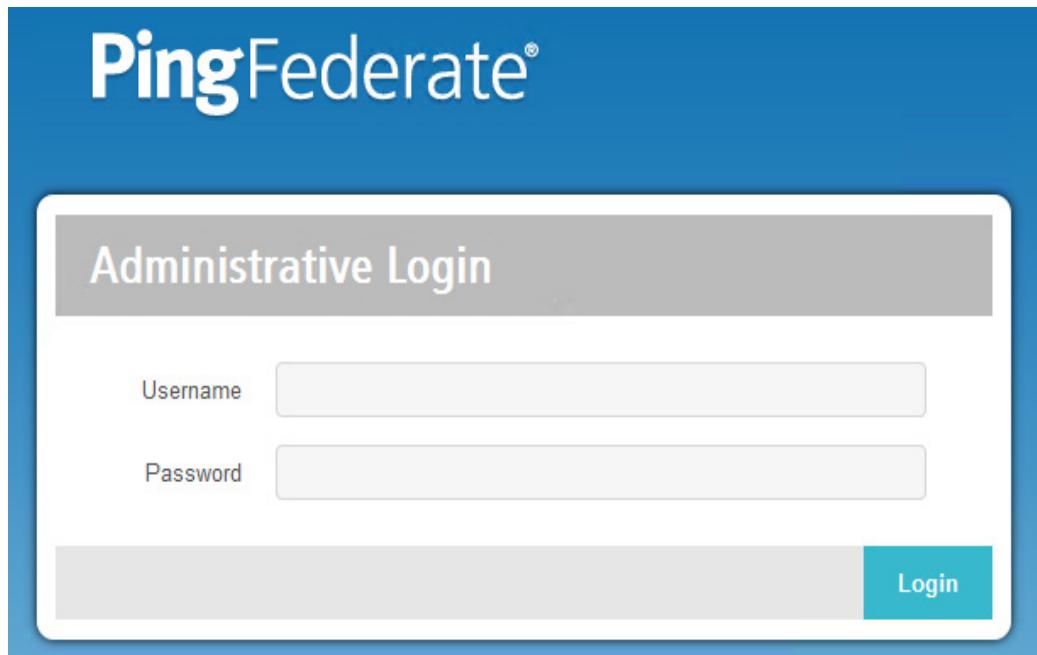
- 5309 1. Click on the Windows icon and begin typing the word `cmd`.
- 5310 2. Double-click the icon to open the Command Prompt.
- 5311 3. It is essential to know about the attributes that this data store will return. PingFederate calls the
 5312 `getAvailableFields()` method to determine the available fields that could be returned from a
 5313 query of this data source. These fields are displayed to the PingFederate administrator during
 5314 the configuration of a data source lookup. The administrator can then select the attributes from
 5315 the data source and map them to the adapter or attribute contract. PingFederate requires at
 5316 least one field returned from this method.
- 5317 4. To change it, go to your ping installation directory. From that directory, navigate to
 5318 `..\pingfederate-7.3.0\pingfederate\ sdk\plugin-src\idp-query-data-store\conf`. Open

5319 .\config.properties with your favorite editor. Change the value for the attribute called
 5320 **NameOfAttributes:**
 5321 NameOfAttributes=fullname,username,stafflevel,role,division,employer,clearance
 5322 Use a comma to separate attribute names. More attributes can be added by adding subsequent
 5323 commas and attribute names.
 5324 5. Navigate to your PingFederate sdk folder, i.e., cd C:/pingfederate-
 5325 7.3.0/pingfederate/sdk/
 5326 6. Within the Command prompt window, type the following compilation command and press
 5327 Enter: ant deploy-plugin

5328 10.3.4 Configuration within PingFederate Administrative Console

5329 The end of successful execution of ant deploy-plugin signals the installation of the data-store driver. Its
 5330 configuration is provided in detail by [Ping documentation](#). In summary, it spans the following process:

- 5331 1. Logon to the Ping RP server.
- 5332 2. Open an internet browser.
- 5333 3. Enter the following URL and press Enter: <https://localhost:9999/pingfederate/app>
- 5334 4. Enter your PingFederate administrator username and password, then click **Login**.



- 5335
- 5336 5. In the browser window, under the main menu area, find **Server Configuration > System Settings**
 5337 > **Data Stores**. Double-click on **Data Stores**.

The screenshot shows the 'Server Configuration' interface. Under 'SYSTEM SETTINGS', there are links for 'Server Settings', 'Data Stores', and 'Redirect Validation'. Under 'ADMINISTRATIVE FUNCTIONS', there are links for 'Metadata Export', 'XML File Signatures', 'Configuration Archive', 'Account Management', 'License Management', and 'Virtual Host Names'.

5338

- 5339 6. At the bottom of the browser window, click **Add New Data Store**.

The screenshot shows the 'Manage Data Stores' screen. It lists three data stores: 'ProvisionerDS' (System ID: ProvisionerDS, User Type: Database), 'LDAP' (System ID: LDAP-0227B4508E324006450B3ED0FF3BD44ACA4EC421, User Type: LDAP), and 'idpquery' (System ID: 02B340D2D9277F16295261175FE339153276D4CD, User Type: Custom). Below the table is a teal button labeled 'Add New Data Store...'

5340

- 5341 7. On the Data Store Type screen, select **Custom** and click **Next**.

The screenshot shows the 'Data Store Type' screen. It has three tabs: 'Data Store Type' (selected), 'Database Config', and 'Summary'. A teal message bar says 'Please select a type of data store.' Below are three radio buttons: 'Database', 'LDAP', and 'Custom' (which is selected). At the bottom right are 'Cancel' and 'Next >' buttons.

5342

- 5343 8. On the Custom Data Store Type screen, specify **Data Store Instance Name** and **Data Store Type**.
 5344 The name can be arbitrary, but you must select **IDP Attribute Query** from the **Data Store Type**
 5345 drop-down. Click **Next**.

5346

- 5347 9. To configure the data store, the following parameters must be configured. These parameters
 5348 are guided by the requirements of the end point (/sp/startAttributeQuery.ping) defined by Ping
 5349 documentation [here](#):

5350 <https://10.33.7.5:9031/sp/startAttributeQuery.ping?AppId=appid&SharedSecret=3Federate&PartnerId=partnerId=https://idp.abac.test:9031&Subject=lsmith@abac.test>

- 5352 ▪ **Attribute Query URL:** the URL specifying the endpoint inside RP (Relying Party) that will
 query the IdP, i.e., <https://rp.abac.test:9031/sp/startAttributeQuery.ping>
- 5353 ▪ **AppId field used in query:** the unique identity of the initiating application, i.e., **appid**
- 5354 ▪ **Shared Secret field used in query:** used to authenticate the initiating application. The
 AppId and SharedSecret must both match the application authentication settings within
 the PingFederate server, i.e. **!23234Federate**
- 5355 ▪ **Partner IDP ID:** used to identify the specific IdP partner to which the Attribute Query
 should be sent. If this parameter is not present, the Subject and Issuer are used to
 determine the correct IdP, i.e., <https://idp.abac.test:9031>

The screenshot shows a navigation bar with 'Main', 'Manage Data Stores', and 'Data Store' tabs. The 'Data Store' tab is active, showing sub-options: 'Data Store Type', 'Custom Data Store Type', 'Configure Attribute Source Adapter Instance' (which is selected and highlighted in blue), and 'Summary'. Below this is a header bar with a 'Configure the Custom Source Adapter' button. The main content area is titled 'Configuration Settings IDP Attribute Query' and contains a table with four rows:

FIELD NAME	FIELD VALUE	DESCRIPTION
ATTRIBUTE QUERY URL	<input type="text"/>	The URL specifies the endpoint inside SP that will query IDP
APPID FIELD USED IN QUERY	<input type="text"/>	AppId field used in Query parameter of URL
SHARED SECRET FIELD USED IN QUERY	<input type="text"/>	SharedSecret field used in Query parameter of URL
PARTNET IDP ID	<input type="text"/>	Partner Idp ID field used in Query parameter of URL

At the bottom right are 'Cancel', '< Previous', and 'Next >' buttons.

5361

5362 10.4 NextLabs PIP Plugin

5363 10.4.1 Architecture

5364 The NextLabs Control Center can support custom PIP plugin extensions for dynamic user and resource
 5365 attribute retrieval during runtime. In order to install and deploy a PIP plugin such as the one described in
 5366 this section, it is necessary to have previously installed and deployed the NextLabs Control Center, Policy
 5367 Controller, Policy Studio, and the NextLabs Entitlement Manager ([Section 7](#)).

5368 According to the NextLabs PDP Policy Extension documentation, which is only available to NextLabs
 5369 customers at this time, one method for leveraging this PIP extension capability is by way of a
 5370 `getAttribute()` function within a `UserAttrProviderMod` class. The PIP Plugin implements methods defined
 5371 by the `ISubjectAttributeProvider` interface. The `ISubjectAttributeProvider` interface declares the method
 5372 `getAttribute()` function which enables querying for a single subject attribute sequentially until all missing
 5373 required attributes have been requested.

5374 *10.4.1.1 Required classes of the NextLabs PIP Plugin:*

- 5375 ▪ UserAttrProviderMod class must exist and must contain a `getAttribute()` function.
 - 5376 • The `getAttribute()` function must accept two arguments (`IDSubject` and `String`) and return an `EvalValue`. The `EvalValue` is created using its `build()` function and the attribute value ultimately returned from the Protocol Broker (see [Section 10.5](#)).
- 5379 ▪ `HTTPSTransmitter` class
 - 5380 • makes an HTTPS request to the Protocol Broker using a `doPost()` function

- CacheKey class, implementing a local Ehcache
 - The CacheKey class constructor takes two parameters, the subjectId and the attributeName, which serve as a compound cache key for storing and retrieving the value of a given user's attribute within the plugin's local Ehcache.

10.4.1.2 Other Required Files or Deployment Notes:

- The three above classes must be compiled into a .jar file.
 - Our method of compilation in this build was using Apache Maven 3.2.5. Maven compilations are directed by a pom.xml (“Project Object Model”), which is an XML representation of a Maven project. More information about Apache Maven and its pom file requirements can be found here: <https://maven.apache.org/pom.html>
 - According to NextLabs support, be sure to include within the pom.xml file configuration a statement that specifies the Provider-Class. The Provider-Class is the UserAttrProviderMod class that contains the getAttribute() method. Example pom.xml excerpt from the pom.xml file in this implementation:

```
<configuration>
  <archive>
    <manifest>
      <mainClass>nist.pdppugin.UserAttrProviderMod</mainClass>
    </manifest>
  <manifestEntries>
    <Provider-Class>nist.pdppugin.UserAttrProviderMod</Provider-
Class>
  </manifestEntries>
  </archive>
</configuration>
```

- Also required per NextLabs support documentation, for any custom plugin you must include a properties file.
 - The configuration file should end with the “.properties” file extension. Example from this implementation: *nlsamlpluginService.properties*
 - Contents should be similar to our example copied below. You must include a *category = ADVANCED CONDITION* statement per NextLabs deployment and loading requirements:

```
name = NLSAMLPlugin_Service
jar-path = [NextLabs]/Policy
Controller/jservice/jar/nlsamlplugin/NLSAMLPlugin-0.0.1-SNAPSHOT-jar-
with-dependencies.jar
friendly_name = NLSAMLPlugin Service
description = NLSAMLPlugin Service
```

10.4.1.3 Notes on Jar and Properties File Deployment within NextLabs Policy Controller Software Architecture:

- The jar file containing the three classes must be deployed on the SharePoint server within the NextLabs Policy Controller software architecture in a specific location. Under the *C:/Program Files/NextLabs/Policy Controller/jservice/jar* folder you must create a folder specifically for your custom jar, i.e., *C:/Program Files/NextLabs/Policy Controller/jservice/jar/custom_jar_folder_you_create*

- 5425 ▪ Any other required supporting jars can be compiled within the same jar as the
 5426 UserAttrProviderMod class and other classes deployed as described in the previous step.
- 5427 • Otherwise, any additional required supporting jars can be compiled into a separate jar which
 5428 is deployed elsewhere within the NextLabs Policy Controller software architecture on the
 5429 SharePoint server, i.e., *C:/Program Files/NextLabs/Policy Controller/jre/lib/ext/*
- 5430 ▪ The properties file must be deployed on the SharePoint server within the NextLabs Policy
 5431 Controller software architecture in a specific location, under the *C:/Program*
 5432 *Files/NextLabs/Policy Controller/jservice/config* folder, i.e., *C:/Program Files/NextLabs/Policy*
 5433 *Controller/jservice/config/jarpropertiesfile.properties*

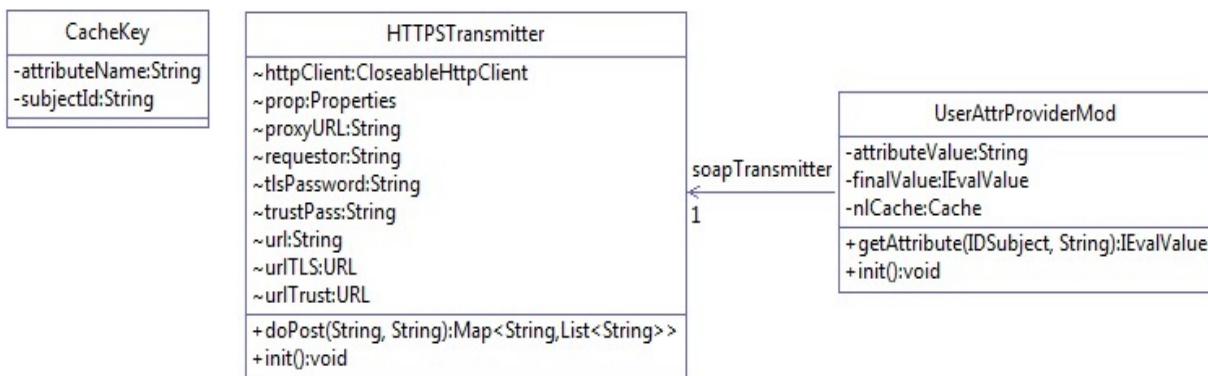
5434 10.4.2 Understanding How the NextLabs PIP Plugin Interacts with Build 5435 Components

5436 When a policy is executed and the NextLabs Policy Controller PDP determines that attributes sent in the
 5437 initial set up of the session are insufficient, the `getAttribute()` function in the `UserAttrProviderMod`
 5438 within the NextLabs Plugin jar is automatically executed sequentially for each missing attribute.

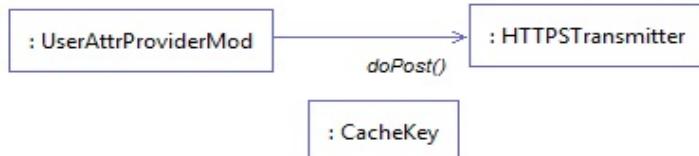
5439 As described above, when the initial set of attributes is insufficient, the NextLabs PIP Plugin first checks a
 5440 local cache, implemented using the Ehcache library and a `CacheKey` class illustrated above. If the
 5441 requested attribute exists within the local cache, the NextLabs PIP Plugin retrieves and returns it
 5442 immediately for use during policy evaluation by the Policy Controller (PDP).

5443 If the requested attribute does not exist within the local cache, the NextLabs PIP Plugin's
 5444 `HTTPSTransmitter` class makes an https request to the Protocol Broker using a `doPost()` function. The
 5445 Protocol Broker performs its functions and returns either the desired attribute or an exception back to
 5446 the NextLabs PIP Plugin, where the Policy Controller (PDP) can evaluate the relevant ABAC policy and
 5447 determine an access decision. In the case that the requested attribute does not exist, the NextLabs
 5448 Policy Controller PDP is configured to default to Deny access in our build. The NextLabs Policy Controller
 5449 PDP is also configured to Deny Access whenever the Protocol Broker or the NextLabs PIP Plugin
 5450 produces an exception.

5451 Figure 10-4 NextLabs PIP Plugin Class Diagram



5453 **Figure 10-5 NextLabs PIP Plugin Interaction Diagram**



5454

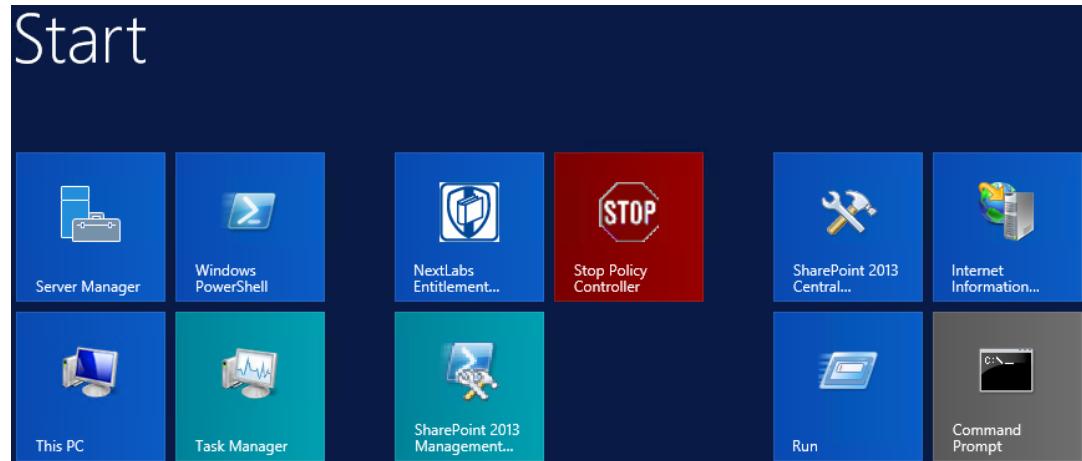
5455 **10.4.3 Compilation and Deployment**

5456 ***10.4.3.1 Compiling the NextLabs PIP Plugin Jar***

- 5457 1. Verify that you are on the server hosting your SharePoint instance, called the SharePoint server in our build.
- 5458
- 5459 2. Click on the Windows icon and begin typing **Cmd**.
- 5460 3. Double-click the icon to open the Command Prompt.
- 5461 4. In the Command Prompt window, navigate to the folder where your pom.xml exists and click Enter, i.e., `cd C:/software/java/plugin/`
- 5462
- 5463 5. In the Command Prompt window, run the following command and press Enter to compile your files and jar(s) into a single jar: `mvn clean install`
- 5464

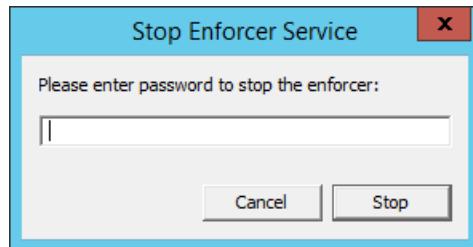
5465 ***10.4.3.2 Stopping the NextLabs Policy Controller Service Before NextLabs PIP Plugin Jar Deployment***

- 5466 1. Still on the SharePoint server, click on the Windows icon and begin typing **Services**.
- 5467
- 5468 2. Double-click the icon to open the Services application.
- 5469 3. In the Services application window, in the list of services, click on the **Name** column to sort by alphabetical order and look for **Control Center Enforcer Service**.
- 5470
- 5471 4. If the status of the **Control Center Enforcer Service** is **running**, stop it by following these steps:
 - a. Click on the Windows icon.
 - 5472 b. On your main screen, double-click the **Stop Policy Controller** shortcut.
- 5473



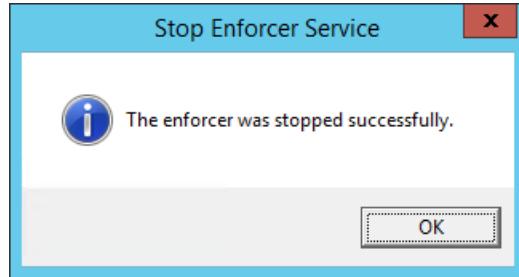
5474

- 5475 c. Enter your NextLabs Administrator credentials, then click **Stop**.



5476

- 5477 d. Click **OK**.



5478

10.4.3.3 Deploying the NextLabs PIP Plugin Jar and its Configuration File

- 5480 1. Still on the SharePoint server, Click on the Windows icon and begin typing **Cmd**.
- 5481 2. Double-click the icon to open the Command Prompt.
- 5482 3. In the Command Prompt window, navigate to the folder where your NextLabs Policy Controller installation exists, and into its **/jservices/jar** folder where custom plugins are required to be stored, then press Enter. i.e., `cd C:/Program Files/NextLabs/Policy Controller/jservice/jar/`
- 5486 4. In the Command Prompt window, enter a command similar to the following and press Enter to create an empty folder named after your plugin: `mkdir nlsamlplugin`
- 5487 5. In the Command Prompt window, enter a command similar to the following and press Enter to copy your plugin jar from its existing location (example `C:/software/java/plugin/target/`) to the

5490 new plugin folder you just created: `copy "C:/software/java/plugin/target/plugin.jar"`
5491 `"nlsamlplugin/"`

5492 6. In the Command Prompt window, enter a command to navigate to the folder where your
5493 NextLabs Policy Controller installation exists, and into its **jservices** folder which contains the
5494 config folder where custom plugin .properties files are required to be stored, then press Enter.
5495 i.e., `cd C:/Program Files/NextLabs/Policy Controller/jservice/`

5496 7. In the Command Prompt window, enter a command similar to the following and press Enter to
5497 copy your plugin .properties file from its existing location (example *C:/software/java/plugin/*) to
5498 the config folder: `copy "C:/software/java/plugin/nlsamlpluginService.properties"`
5499 `"config/"`

5500 *10.4.3.4 Resetting IIS and Restarting the NextLabs Policy Controller Service*

- 5501 1. Click on the Windows icon and begin typing **PowerShell**.
- 5502 2. Double-click the icon to open Windows PowerShell.
- 5503 3. In the Windows PowerShell window, type in this command and press Enter to reset Internet
5504 Information Services: `iisreset`
- 5505 4. Click on the Windows icon and begin typing **Services**.
- 5506 5. Double-click the icon to open the Services application.
- 5507 6. Within the Services application window, in the list of services, click on the **Name** column to sort
5508 by alphabetical order and look for **Control Center Enforcer Service**.
- 5509 7. Right-click **Control Center Enforcer Service** and click **Start**.

5510 It may be necessary to click the Refresh icon in order to see the **Control Center Enforcer Service**
5511 status change to **running**.

5512 **10.5 Protocol Broker**

5513 **10.5.1 Architecture**

5514 The Protocol Broker decouples communication between the NextLabs Plugin and PingFederate RP. As
5515 noted earlier, the Protocol Broker is a web application hosted on a tomcat server installed on the
5516 SharePoint server. It communicates using mutual TLS and listens on the localhost. This ensures that the
5517 service provided by Protocol Broker is not available on the network, and the requester must be
5518 authenticated during each request.

5519 SAMLProxy extends the [HttpServlet](#) class, which is an abstract class. This enables SAMLProxy class to
5520 read/write the http request/response, and determines the [http method](#) of the request (i.e. HTTP GET,
5521 POST, PUT, DELETE, HEAD etc) and calls one of the corresponding methods. The SAMLProxy class only
5522 implements the POST method.

5523 The SAMLProxy class constructs an object of the SoapHTTPTransmitter class. This class reads
5524 **abacClient.jks** and **truststore.jks** which are used for mutual TLS communication initiated by the

5525 SoapHTTPTransmitter with PingFederate. It also reads **abacSigningClient.jks**, which is used to sign the
5526 SAML AttributeQuery, and metadata to verify the SAML Response signature. The jks extension stands
5527 for Java Key store, which is a storage facility for cryptographic keys and certificates.

5528 The Protocol Broker facilitates secure communication between the NextLabs PIP Plugin and
5529 PingFederate RP. This coordination consists of two parts:

- 5530 1. Communication between the NextLabs PIP Plugin and the Protocol Broker
- 5531 2. Communication between the Protocol Broker and the PingFederate RP server

10.5.1.1 Communication Between NextLabs PIP Plugin and Protocol Broker

5533 The Protocol Broker's doPost() method expects the following parameters:

- 5534 ▪ Requester
- 5535 ▪ SubjectId
- 5536 ▪ AttributeName

5537 On successful receipt of a request, SAMLProxy uses the SoapHTTPTransmitter class to transmit the
5538 request to the PingFederate RP server. The response received from SOAPHTTPTransmitter is dispatched
5539 back to the NextLabs PIP Plugin, which then hands the result off to the PDP for policy evaluation and
5540 access decision making.

10.5.1.2 Communication Between Protocol Broker and PingFederate RP Server

5542 The PingFederateRP and ProtocolBroker communicate using Assertion Query/Request Profile. As shown
5543 in Figure 10-6, Protocol Broker initiates the secured communication on a mutual TLS channel with the
5544 Relying Party, and sends a signed SAML2 AttributeQuery. The message format and structure of the
5545 AttributeQuery is defined by SAMLCore Section 3.3.2.3. Binding for the profile is defined by SAMLBind
5546 Section 3.2.3. Processing rules governing the profile are provided by Section 3.3 of SAMLCore. In
5547 response, Protocol Broker expects a SAML response back.

5548 OpenSAML is used to implement an Assertion Query/Request Profile. OpenSAML is a set of open source
5549 libraries meant to support developers working with Security Assertion Markup Language (SAML). The
5550 configuration required to use the OpenSAML library is provided in [Section 10.5.2.2](#).

5551 Figure 10-6 Communication Between Plugin and Relying Party

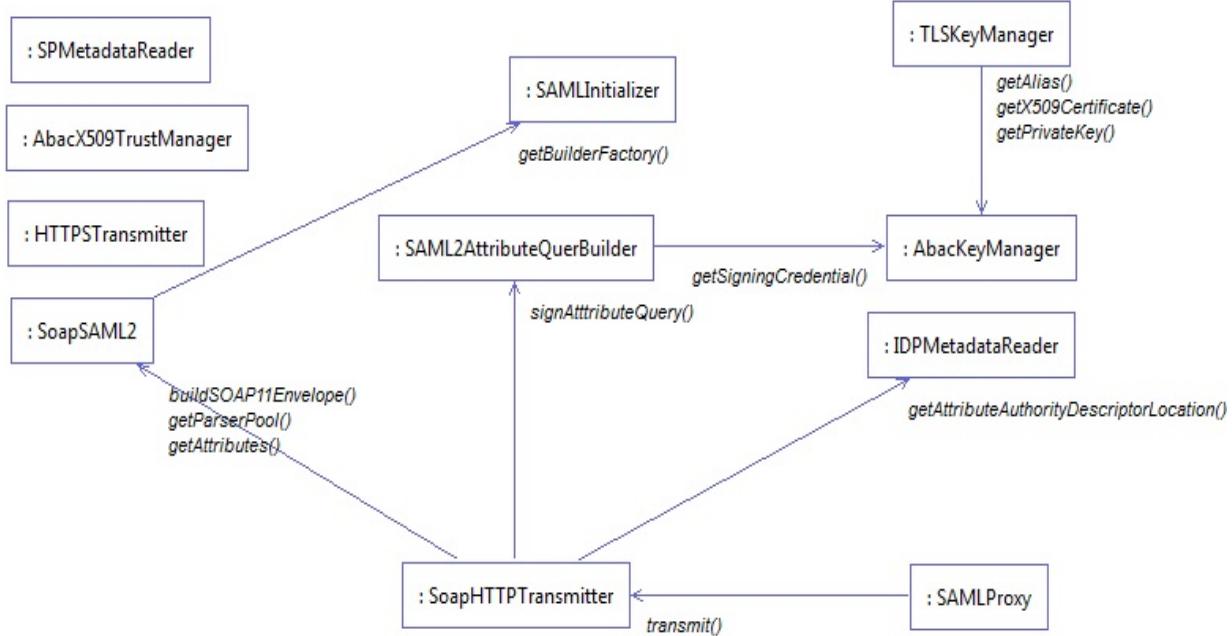


5552

5553 Based on keystores and configuration read during initialization, SoapHTTPTransmitter creates a
 5554 SAML2AttributeQuerBuilder class to build a Signed SAML 2.0 Attribute Query. Attribute names received
 5555 earlier in the doPost() method are used to build the AttributeQuery. A SOAPSAML2 object is used to
 5556 provide SOAP parameters for the SAML message created earlier. It reads SAML 2.0 metadata to find the
 5557 location of the Attribute Authority end point. It uses HttpSOAPClient to dispatch the request to the end
 5558 point using mutual TLS.

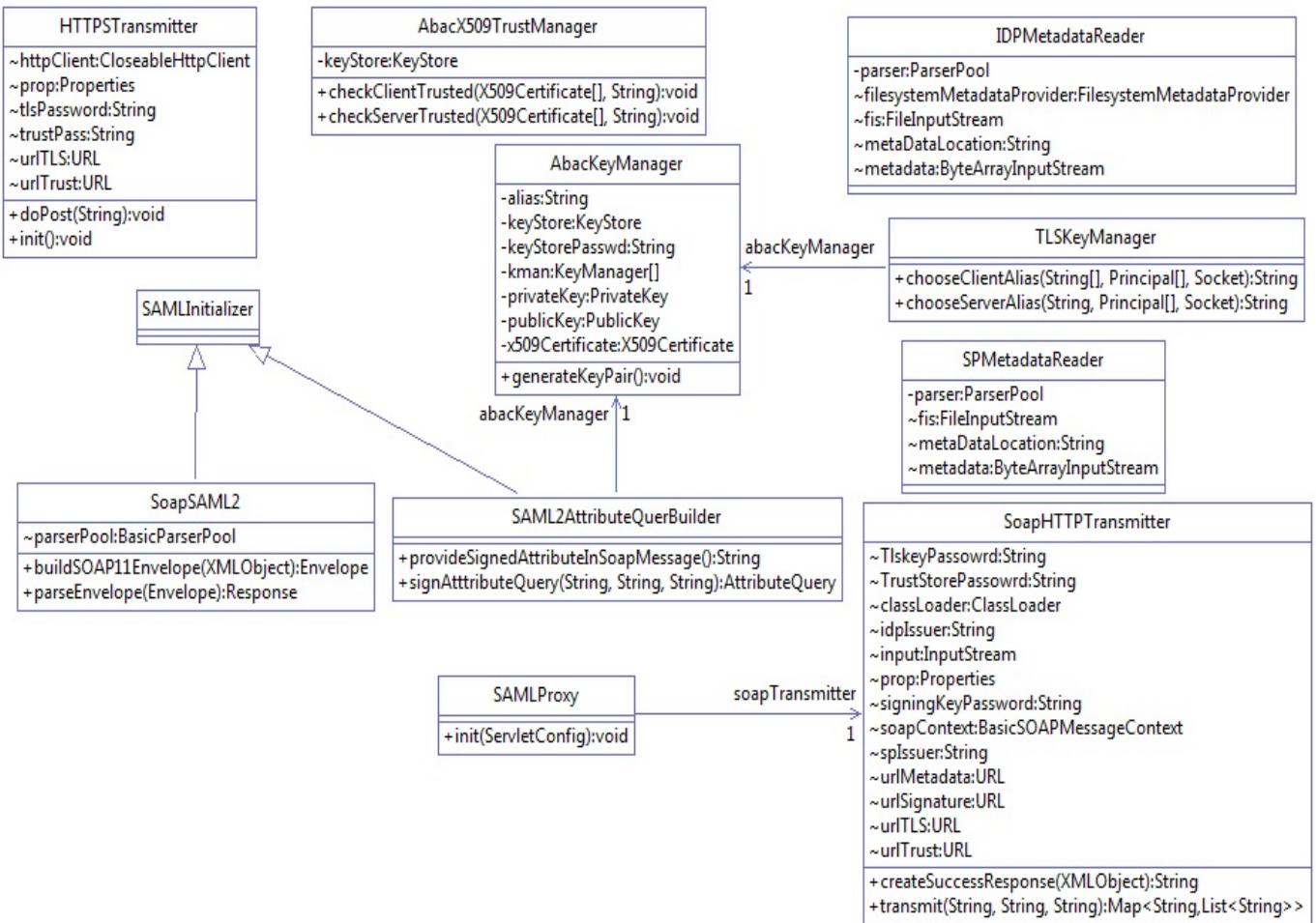
5559 HTTPSoapClient is also responsible for receiving the Attribute response, verifying the signature and
 5560 sending the attributes back to the Nextlab Plugin.

5561 Figure 10-7 Protocol Broker Interaction Diagram



5562

5563 Figure 10-8 Protocol Broker Class Diagram



5564

5565 **10.5.2 Deployment**5566 **10.5.2.1 System and Environment Requirements**5567 The Protocol Broker is deployed on [tomcat 8.0.22](#) on the SharePoint server, and uses [OpenSAML 2.6.4](#).5568 **10.5.2.2 Configuration**

5569 In order to accept traffic only on the channel protected by mutual TLS:

- 5570 1. Install tomcat on the SharePoint server. The tomcat installation procedure is provided [here](#).
- 5571 2. Open the configuration file **server.xml** inside the configuration directory of the tomcat installation. Comment out the section:

```

5573 <!--
5574     <Connector port="8080" protocol="HTTP/1.1"
5575         connectionTimeout="20000"
5576         redirectPort="8443" />
5577 -->
  
```

5578 3. Update/insert the following line:

```
5579      <Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
5580      maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
5581      keystoreFile="C:\Users\<name>\Documents\softwares\tomcat\apache-tomcat-
5582      8.0.22\conf\abacTomcat.jks" keystorePass="....password" clientAuth="true"
5583      sslProtocol="TLS"
5584      truststoreFile="C:\Users\sjha\Documents\softwares\tomcat\apache-tomcat-
5585      8.0.22\conf\truststore.jks" truststoreType="JKS" truststorePass="...password" />
```

5586 The configuration details for OpenSAML are provided [here](#). In this demonstration, a folder called
 5587 **endorsed** is created inside the **lib** directory of tomcat installation.

5588 Add the following libraries to the endorsed folder created in the above step:

- 5589 ■ xml-apis-2.10.0.jar
- 5590 ■ xml-resolver-1.2.jar
- 5591 ■ xercesImpl-2.10.0.jar
- 5592 ■ xalan-2.7.1.jar
- 5593 ■ serializer-2.10.0.jar

10.5.2.3 Preparation and Compilation

5595 In our build, we used [Apache Maven](#) for Protocol Broker compilation. In order to prepare and compile
 5596 the Protocol Broker, follow these steps:

10.5.2.3.1 Preparation

- 5598 1. On the SharePoint server, click on the Windows icon and begin typing **Cmd**.
- 5599 2. Double-click the icon to open the Command Prompt.
- 5600 3. In the Command Prompt window, navigate to the folder where your pom.xml for the Protocol
 Broker exists, and press Enter. i.e., **cd C:/software/java/samlNewPlugin/**
- 5602 4. Type the following command, then press Enter to prepare for compilation of the new Protocol
 Broker: **.war file: mvn clean**
- 5604 5. Verify that your results are similar to the following, including the **Build Success** statement:

```
5605 [INFO] Scanning for projects...
5606 [INFO]
5607 [INFO] -----
5608 [INFO] Building SAMLProxy 0.0.1-SNAPSHOT
5609 [INFO] -----
5610 [INFO]
5611 [INFO] --- maven-clean-plugin:2.5:clean (default-clean) @ SAMLProxy ---
5612 [INFO] Deleting /home/sjha/pdpPlugins/SAMLProxy/target
5613 [INFO] -----
```

```
5614      [INFO] BUILD SUCCESS
5615      [INFO] -----
5616      [INFO] Total time: 1.333 s
5617      [INFO] Finished at: 2015-06-29T10:24:27-04:00
5618      [INFO] Final Memory: 5M/15M
5619      [INFO] -----
```

10.5.2.3.2 Compiling the .war File

1. After following the instructions above to prepare for compiling, within the Command Prompt window, enter the following command and press Enter to create the Protocol Broker: **.war file: mvn package**
2. Verify that your results are similar to the following, including the **Failures: 0** and **Build Success** portions:

```
5620
5621      [INFO] Scanning for projects...
5622
5623      [INFO]
5624      [INFO] -----
5625
5626      [INFO] Building SAMLProxy 0.0.1-SNAPSHOT
5627
5628      [INFO] -----
5629
5630      [INFO] -----
5631
5632      [INFO] --- maven-resources-plugin:2.6:resources (default-resources) @ SAMLProxy
5633  ---
5634
5635      [INFO] Using 'UTF-8' encoding to copy filtered resources.
5636
5637      [INFO] Copying 9 resources
5638
5639      [INFO]
5640      [INFO] --- maven-compiler-plugin:3.1:compile (default-compile) @ SAMLProxy ---
5641
5642      [INFO] Nothing to compile - all classes are up to date
5643
5644      [INFO]
5645
5646      [INFO] --- maven-resources-plugin:2.6:testResources (default-testResources) @ SAMLProxy
5647  ---
5648
5649      [INFO] Using 'UTF-8' encoding to copy filtered resources.
5650
5651      [INFO] skip non existing resourceDirectory
5652      /home/sjha/pdpPlugins/SAMLProxy/src/test/resources
5653
5654      [INFO]
5655
5656      [INFO] --- maven-compiler-plugin:3.1:testCompile (default-testCompile) @ SAMLProxy
5657  ---
5658
5659      [INFO] Nothing to compile - all classes are up to date
5660
5661      [INFO]
```

SECOND DRAFT

```
5650      [INFO] --- maven-surefire-plugin:2.12.4:test (default-test) @ SAMLProxy ---
5651      [INFO] Surefire report directory:
5652      /home/sjha/pdpPlugins/SAMLProxy/target/surefire-reports
5653
5654 -----
5655      T E S T S
5656 -----
5657      Running nist.pdpplugin.AppTest
5658      Tests run: 1, Failures: 0, Errors: 0, Skipped: 0, Time elapsed: 0.03 sec
5659
5660      Results :
5661
5662      Tests run: 1, Failures: 0, Errors: 0, Skipped: 0
5663
5664      [INFO]
5665      [INFO] --- maven-war-plugin:2.6:war (default-war) @ SAMLProxy ---
5666      [INFO] Packaging webapp
5667      [INFO] Assembling webapp [SAMLProxy] in
5668      [/home/sjha/pdpPlugins/SAMLProxy/target/SAMLProxy-0.0.1-SNAPSHOT]
5669      [INFO] Processing war project
5670      [INFO] Copying webapp resources [/home/sjha/pdpPlugins/SAMLProxy/WebContent]
5671      [INFO] Webapp assembled in [440 msec]
5672      [INFO] Building war: /home/sjha/pdpPlugins/SAMLProxy/target/SAMLProxy-0.0.1-
5673      SNAPSHOT.war
5674      [INFO] -----
5675      [INFO] BUILD SUCCESS
5676      [INFO] -----
5677      [INFO] Total time: 6.281 s
5678      [INFO] Finished at: 2015-06-29T10:27:14-04:00
5679      [INFO] Final Memory: 11M/26M
5680      [INFO] -----
```

5681 10.5.3 Example SAML Request and Response Output

5682 10.5.3.1 Example of Tomcat Output from our Build that Illustrates a SAML Request

```

5683 <saml2p:AttributeQuery ID="_7a41be2e3d0d1abea13e857a80b3cfbc" IssueInstant="2015-05-
5684 26T18:14:39.405Z" Version="2.0" xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
5685 xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
5686   <saml2:Issuer
5687     xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:nccoe:abac:plugin</saml2:Issue
5688   r>
5689   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
5690     <ds:SignedInfo>
5691       <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
5692       <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
5693       <ds:Reference URI="#_7a41be2e3d0d1abea13e857a80b3cfbc">
5694         <ds:Transforms>
5695           <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
5696           <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
5697         </ds:Transforms>
5698         <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
5699         <ds:DigestValue>hz3JxkkIsCL/BV1kRCrgUykjaho=</ds:DigestValue>
5700       </ds:Reference>
5701     </ds:SignedInfo>
5702     <ds:SignatureValue>O8Gc8CSVKeYoNsR8bWaiExEpumeO2bLaMwlWC6LNaqf9ydvMPw/gcZbAEATCgK/RXVY
5703 gTe7ikYKKC80/GiO7NrUKZPO861n5LINX5Gw5iTOeb6S4zUTWEfp2PQTfmSTB6rZe5OBuUDEpWFJ4T/3E1KpI4
5704 H7sxoaYhcZ3J2i1ZxPheMEJ014zvicAzlsefiirftnlvWirOdjub9VE0SicC111FJB13Wla+c8JA5Nbbsnc3H6
5705 h5oDeapEOD9bX41KZtj2sGbh6k+F3vunYpd3m69KW6z8CJQeBWOCGCMdt4Dyf/avg61z7o0PYjPYxFIvws1OY
5706 YU2QzLtOpHT8e/RRQ==</ds:SignatureValue>
5707
5708     <ds:KeyInfo>
5709       <ds:KeyValue>
5710         <ds:RSAKeyValue>
5711         <ds:Modulus>uzxrL5iAIpNyEXHmGTDW1mzx7YJa1/c9Ruxag3sifjzuUdBjEznFJJxaagM2pzTUI5JCaLzgm7
5712 1V
5713
5714 SBmuVL+6PzTxReM3i5XzWjapgRMIIizadnQT0wmCryKuNaQiBIFLoMbi+ySdBvu+M/xhH1RxuFjY9N
5715 PSE1MHL8YaLoKW2SFIM/3bhJ/xF7q7FGHMcJH4Zzr2QpQmBERyoZJV3z4ZvVro/MfyLg1VER0pu
5716 36e32hIyzsf2gKizv00qY2ecD1BCNTITsA2HWSTf50kpvt4qupCnXVKVqzDPZON0XCsjJCcwWsUi9
5717 pRvkGtVBXqhh2820Dyzcl3nkpgs15F8hR7kOjQ==</ds:Modulus>
5718       <ds:Exponent>AQAB</ds:Exponent>

```

```

5719      </ds:RSAKeyValue>
5720      </ds:KeyValue>
5721      </ds:KeyInfo>
5722      </ds:Signature>
5723      <saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
5724          <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
5725          format:unspecified">jdoe</saml2:NameID>
5726      </saml2:Subject>
5727      <saml2:Attribute Name="firstname" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
5728      format:basic" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"/>
5729  </saml2p:AttributeQuery>

```

5730 10.5.3.2 *Example of Tomcat Output from our Build that Illustrates a SAML Response*

```

5731  <?xml version="1.0" encoding="UTF-8"?><S11:Envelope
5732  xmlns:S11="http://schemas.xmlsoap.org/soap/envelo
5733  pe/">
5734  <S11:Body>
5735      <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
5736      ID="LkF9NevJONpgbE56hszqbo2V
5737          FZH" InResponseTo="_13caab0c0aa8b70946be278ff32376ad" IssueInstant="2015-06-
5738          29T14:46:35.617Z" Version
5739          ="2.0">
5740          <saml:Issuer
5741          xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://rp.abac.test:9031</saml:Iss
5742          user>
5743          <samlp:Status>
5744              <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
5745          </samlp:Status>
5746          <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="P-
5747          nmuwJENgb_aVjhd5Dpy
5748              dfN2IU" IssueInstant="2015-06-29T14:46:35.945Z" Version="2.0">
5749              <saml:Issuer>https://rp.abac.test:9031</saml:Issuer>
5750              <saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
5751              xmlns:saml2p="urn:oasi
5752                  s:names:tc:SAML:2.0:protocol"
5753                  xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
5754                      <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
5755                      format:unspecified">lsmith@ab
5756                          ac.test</saml2:NameID>
5757                      </saml2:Subject>
5758                      <saml:Conditions NotBefore="2015-06-29T14:41:35.945Z" NotOnOrAfter="2015-06-
5759                      29T14:51:35.9
5760                          45Z">
5761                          <saml:AudienceRestriction>
5762                              <saml:Audience>https://nextlabs-rp</saml:Audience>
5763                          </saml:AudienceRestriction>
5764                      </saml:Conditions>
5765                      <saml:AttributeStatement>
5766                          <saml:Attribute Name="stafflevel"
5767                          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-for
5768                          mat:basic">
5769                          <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema">
```

```

5770    xmlns:xsi="http://
5771        www.w3.org/2001/XMLSchema-instance"
5772    xsi:type="xs:string">Junior</saml:AttributeValue>
5773        </saml:Attribute>
5774        </saml:AttributeStatement>
5775    </saml:Assertion>
5776    </samlp:Response>
5777    </S11:Body>
5778 </S11:Envelope>
```

5779 **10.6 Apache Directory Service (ApacheDS)**

5780 ApacheDS is included in [Apache Directory Studio](#), which has multiple functionalities with ApacheDS
 5781 Server, i.e., LDAP Browser, Schema Editor, Apache Configurator, LDIF Editor, Embedded ApacheDS, and
 5782 ACI Editor.

5783 **10.6.1 Layout**

5784 Before installation, it is important to consider system needs and match them with the installation layout.
 5785 The general layout for ApacheDS consists of two major concepts:

- 5786 1. Installation Layout: The installation is where all files essential to ApacheDS are stored, i.e.,
 5787 launch script, libraries, and a service wrapper (depending on the kind of installer used).
- 5788 2. Instance Layout: ApacheDS is built to run multiple instances of the server at the same time,
 5789 which means that an optional instances folder can be found in the installation layout (or
 5790 elsewhere on the disk, depending on the platform). In that folder you will find one or multiple
 5791 directories, all sharing the same layout, corresponding to all ApacheDS instances (one directory
 5792 per instance, with names corresponding to the ID of the instance).

5793 A detailed discussion of these concepts can be found [here](#).

5794 **10.6.2 Download**

5795 ApacheDS can be downloaded as binary or as source, and compiled on a given platform. Source can be
 5796 downloaded [here](#).

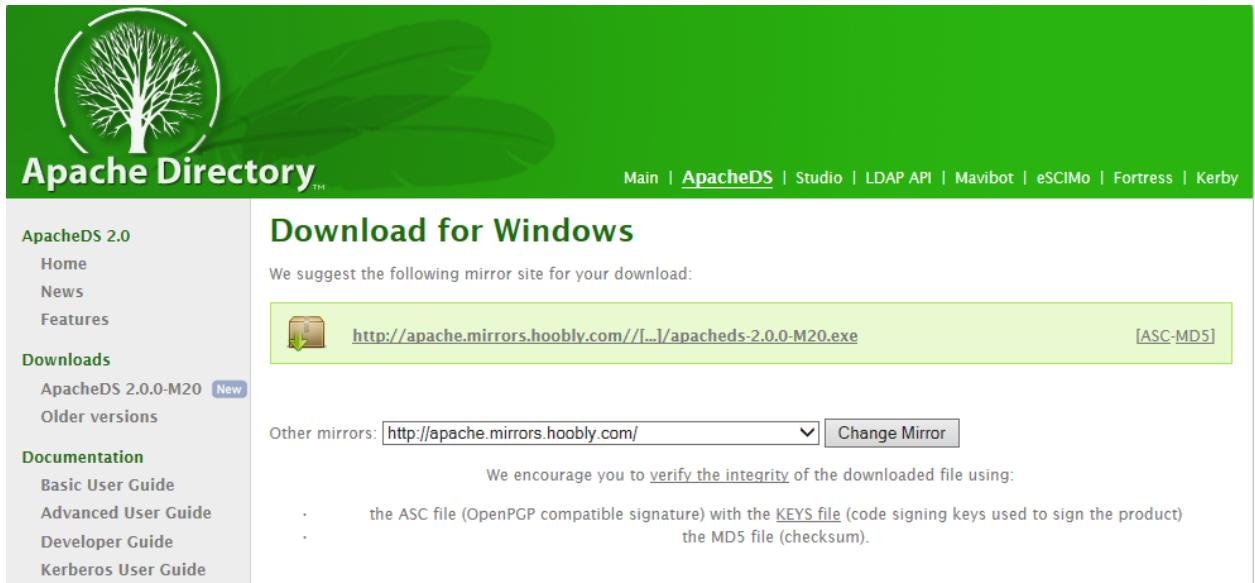
5797 In this project, ApacheDS was downloaded as a packaged Windows installer from this [location](#). Native
 5798 installers are available in the following formats, and their download links are available at following [site](#).

Platform	Installer Format
Window	Exe
Mac OS X	Dmg
Debian	Deb
Linux	Rpm,bin

5799

5800 1. At the download [location](#), you will see a URL as shown in the example below. Click the link
 5801 above to download Apache Directory Server for Windows.

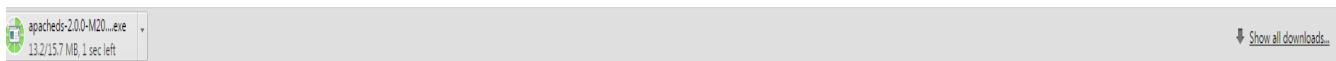
5802 **Figure 10-9 ApacheDS Download**



5803
 5804 2. During the software download, different installation graphics will be displayed depending on
 5805 which browser you use. Example from Windows Internet Explorer:



5806
 5807 On Chrome, it may display as below (if you are not using command line tools):



5809 *10.6.2.1 Verify the Integrity of the Downloaded File*

5810 It is essential to verify the integrity of the file when the download completes.

5811 The file's integrity can be verified with PGP signatures using PGP or GPG. First, download the [KEYS](#) and
 5812 the [asc](#) signature file for the relevant distribution. Both **KEYS** and **asc** can be found to the right of the
 5813 download link, as shown in Figure 10-9 above.

5814 Verify the signatures using the following commands in the Command Prompt:

```
5815        $ pgpk -a KEYS
  5816        $ pgpv apacheds-2.0.0-M20.exe.asc
  5817        or
  5818        $ pgp -ka KEYS
  5819        $ pgp apacheds-2.0.0-M20.exe.asc
  5820        or
```

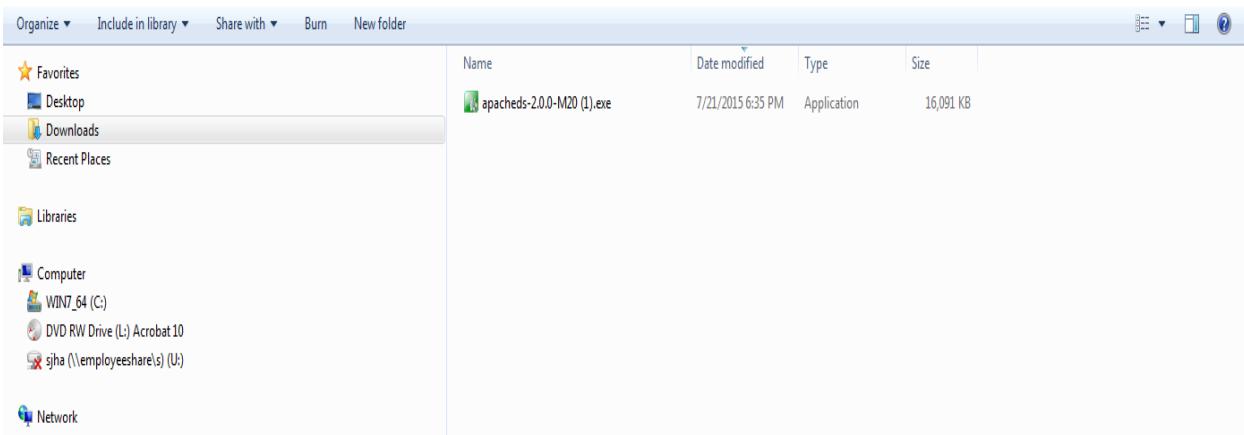
5821 \$ gpg --import KEYS
5822 \$ gpg --verify apacheds-2.0.0-M20.exe.asc

5823 Alternatively, you can verify the MD5 signature on the files. A Unix program called **md5** or **md5sum** is
5824 included in many Unix distributions. It is also available as part of [GNU Textutils](#). Windows users can get
5825 binary md5 programs from [here](#), [here](#), or [here](#).

5826 10.6.3 Installation

5827 Note: To install ApacheDS as a Windows service, you need administrative privileges. We installed
5828 ApacheDS on Windows Server 2012. The ApacheDS installation procedure for other operating systems
5829 can be found [here](#).

- 5830 1. Once ApacheDS is downloaded and verified, double-click the installer to open it. Note: It may
5831 have already been opened by your web browser.

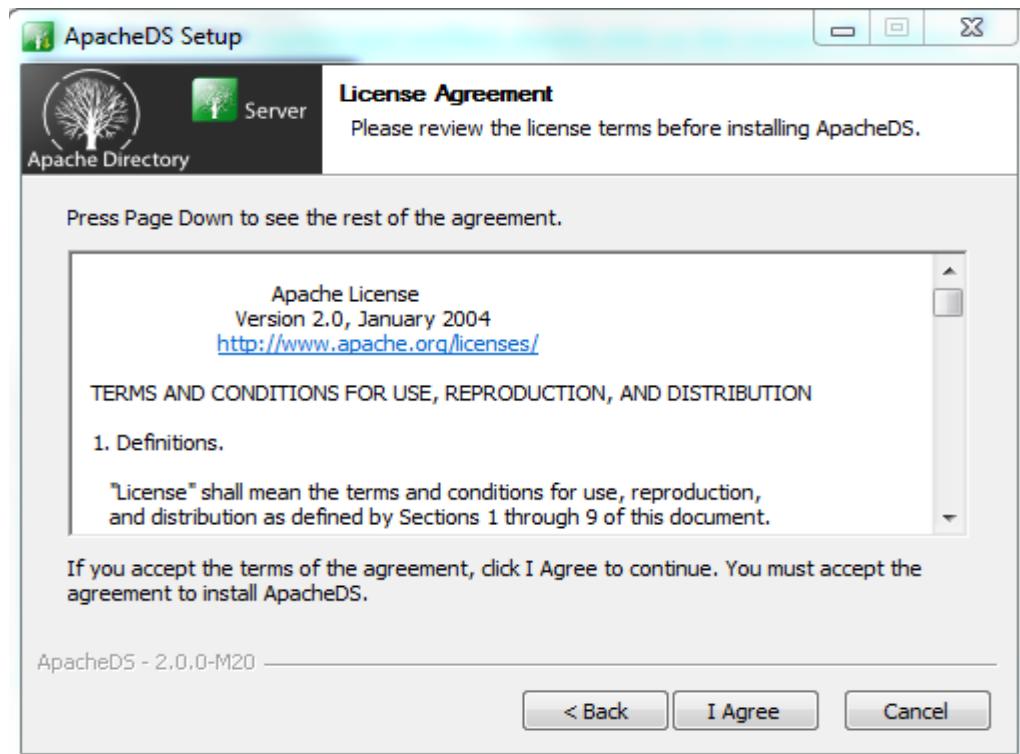


- 5832
5833 2. When the following screen appears, click **Next**.



5834

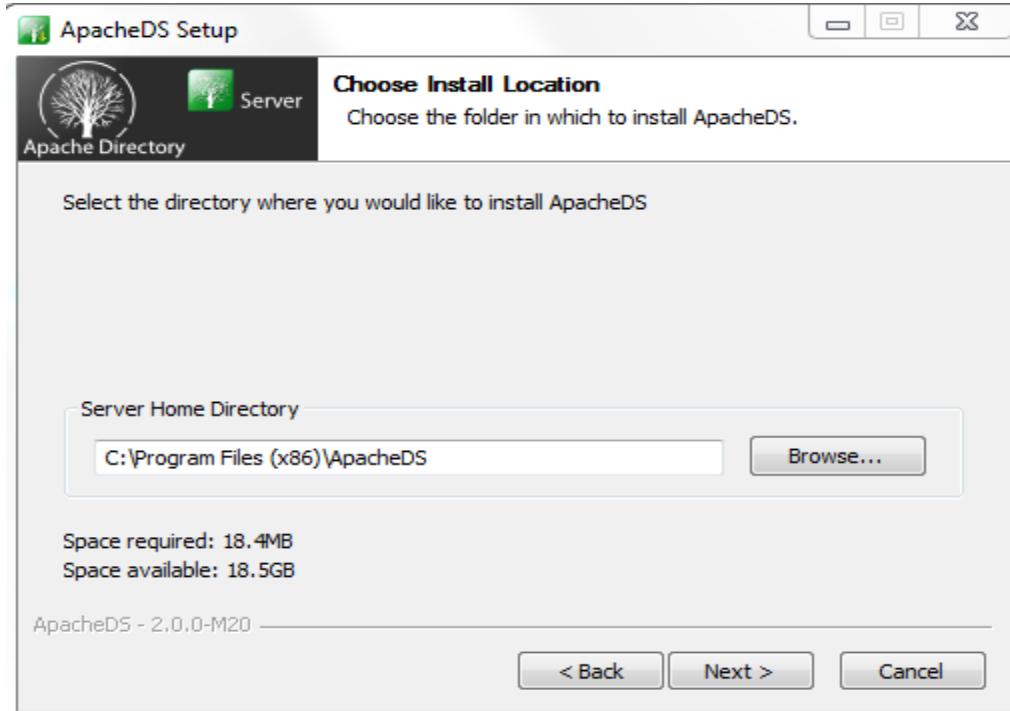
- 5835 3. Review the License agreement and click I Agree.



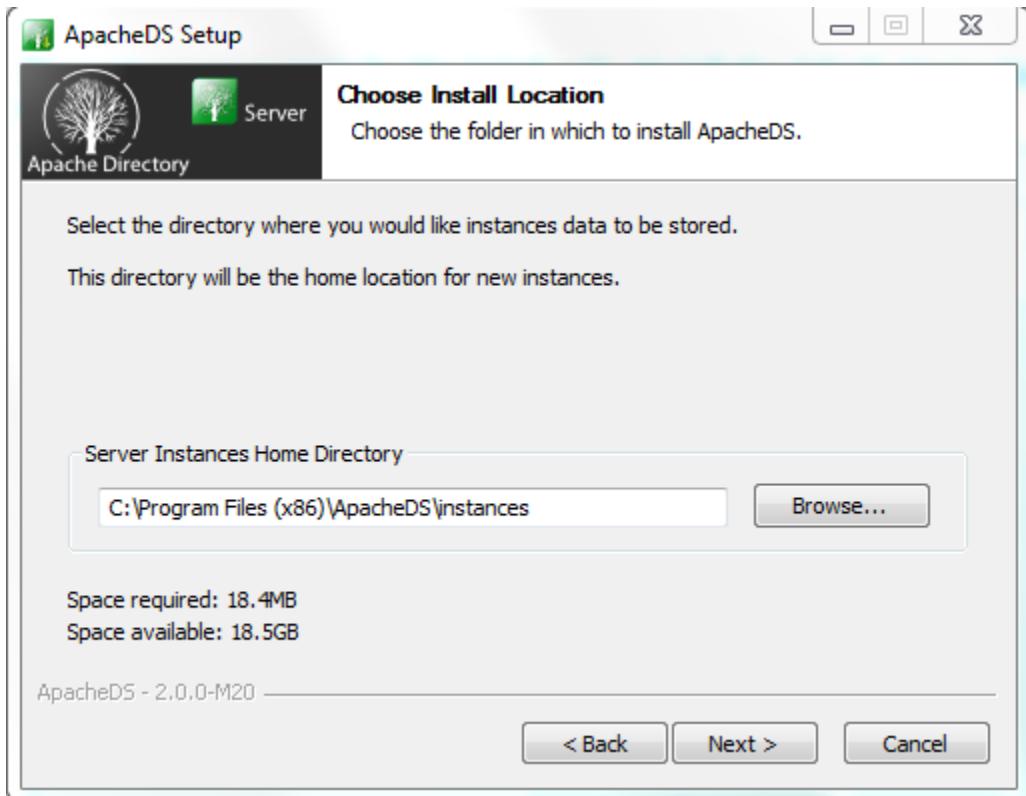
5836

SECOND DRAFT

- 5837 4. The next screen prompts you for the install path. In our build, we left the default install path.
5838 Specify an install path of your choosing, and click **Next**.

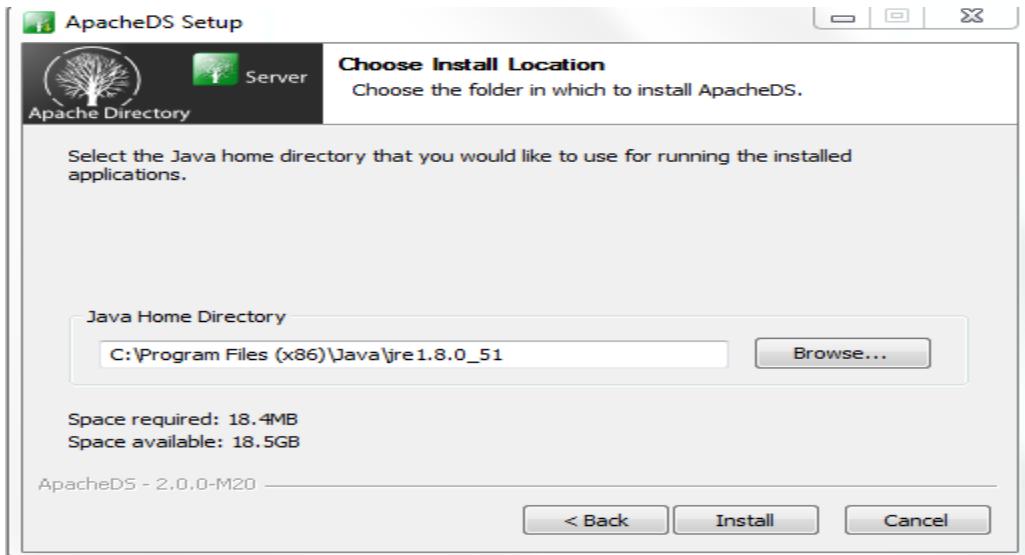


- 5839
5840 5. Specify a location for storing ApacheDS instances, then click **Next**.



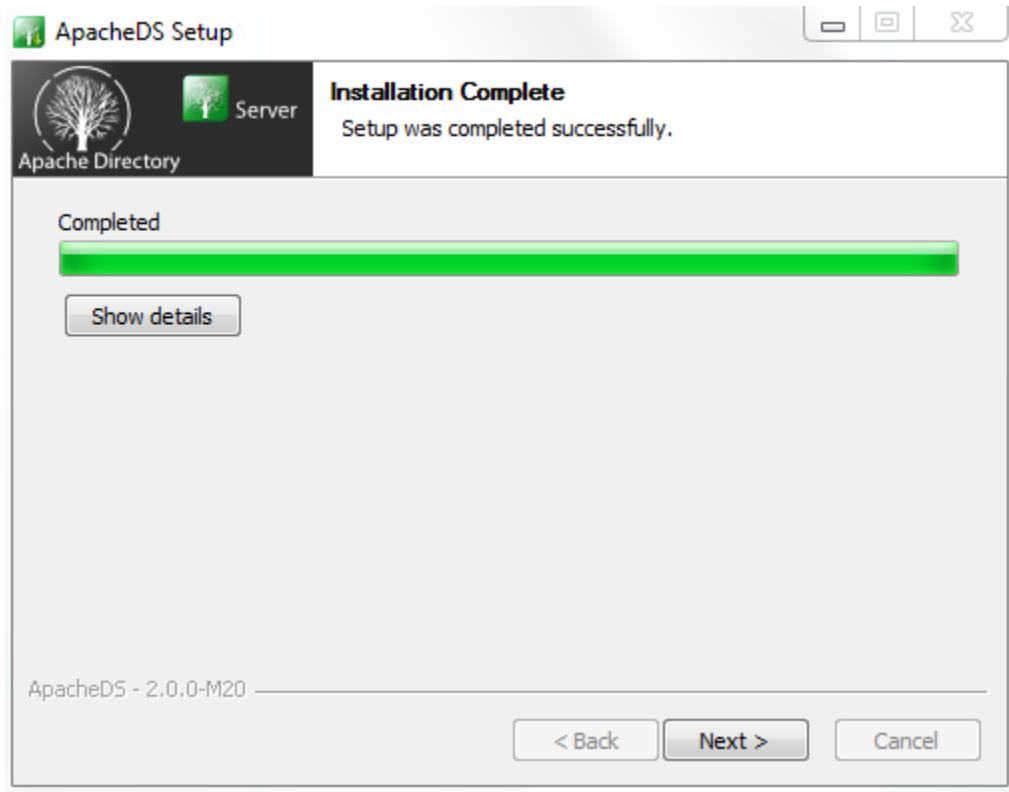
5841

5842 6. The next screen asks for the location of your java run time. It is assumed, based on the earlier
5843 description in [Section 10.8.2](#), that users will have the proper java environment prior to
5844 attempting to install ApacheDS. Users who have no JRE installed should abandon the install by
5845 clicking **Cancel**. Install the JRE and re-run the ApacheDS install. We accepted the default as
5846 shown.



5847

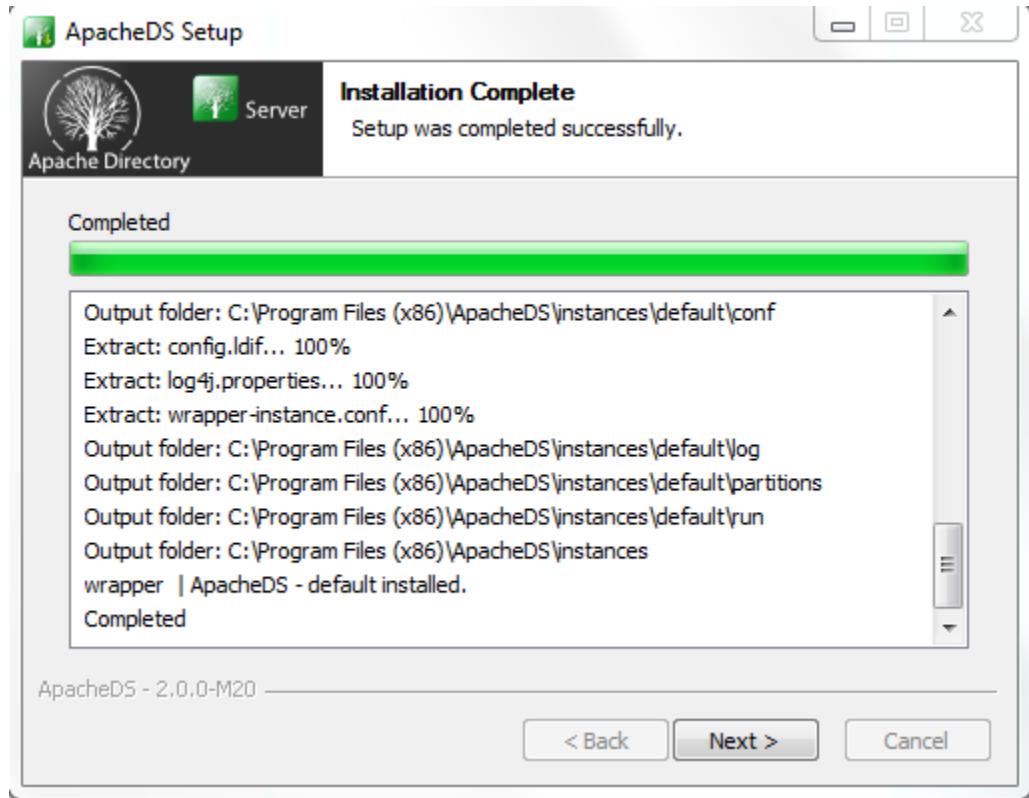
5848 7. Click **Install**. Once the installation is complete, you will receive the following prompt:



5849

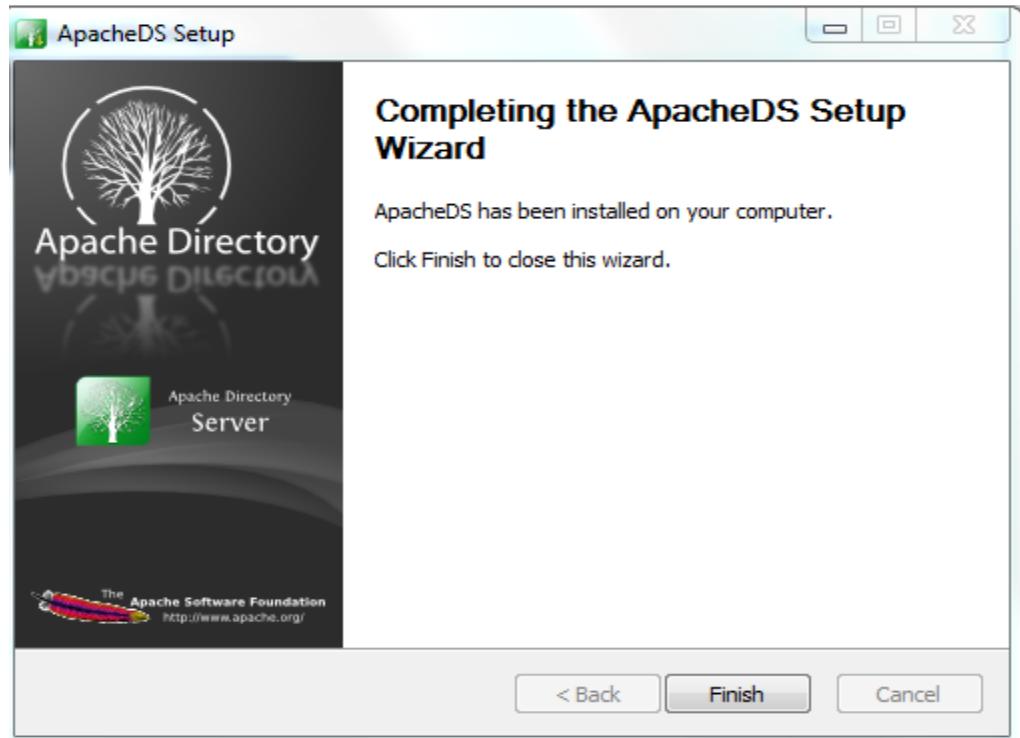
5850 **10.6.3.1 Functional Test of the ApacheDS Installation**

- 5851 1. Click **Show Details** in above diagram to see details of installation. Make sure all of the folders
5852 exist, then click **Next**.



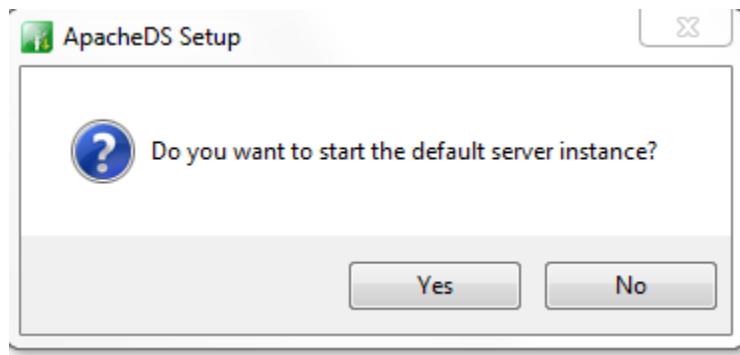
5853

- 5854 2. Click **Finish** to end the installation.



5855

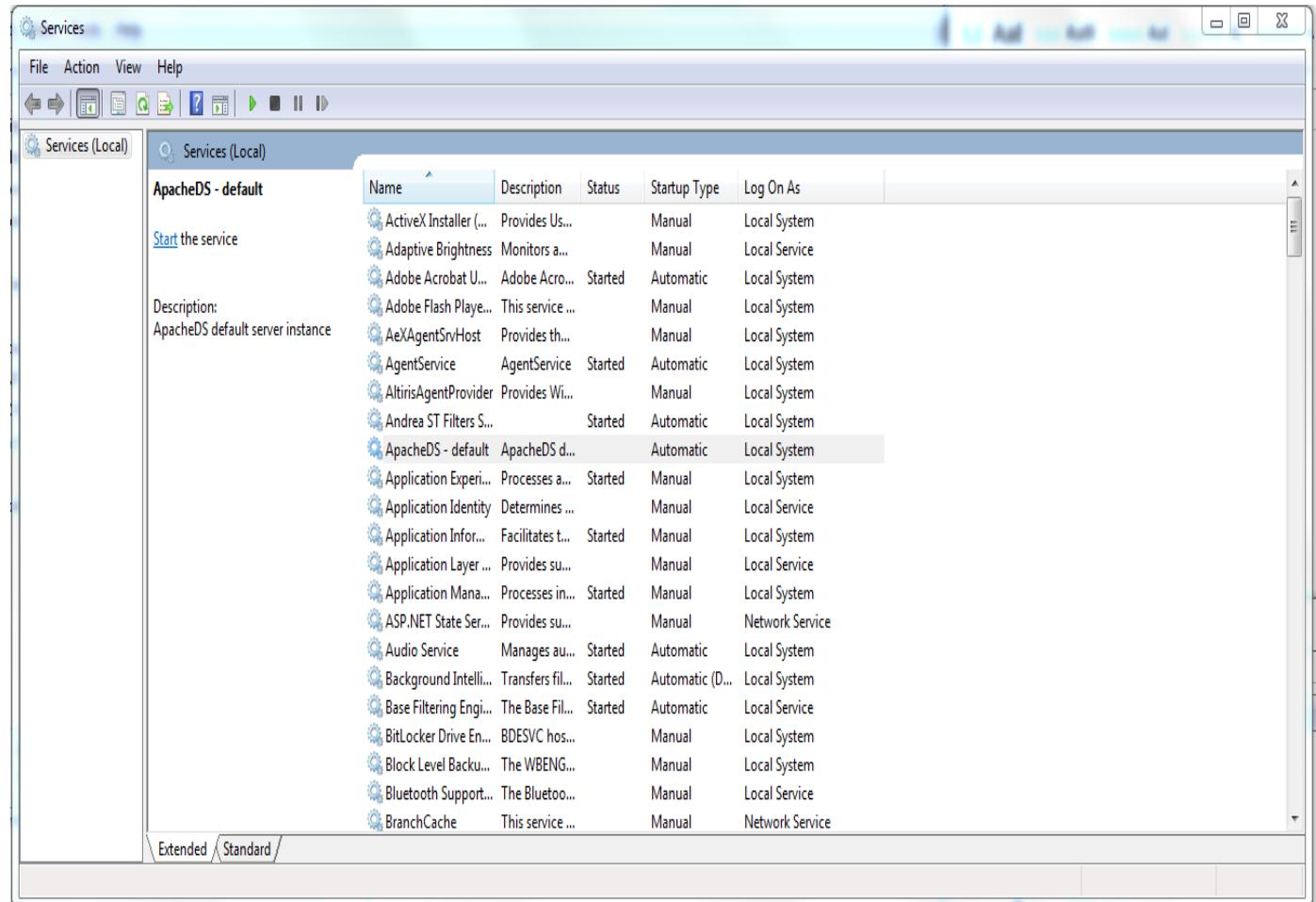
- 5856 3. Click **Yes** to start the ApacheDS server. Instructions are provided in [Section 10.6.2](#).



5857

10.6.4 Starting and Stopping the Server

5858 The server can be started and stopped with the Windows Services manager (**Control Panel > Administrative Tools > Services**). The user must have administrative privileges.



5861

5862 From here, ApacheDS can be started, stopped, or restarted.

5863 The process for starting and stopping ApacheDS on other operating systems is described [here](#).

10.6.5 ApacheDS Configuration

5865 ApachdDS Server and Schema configuration details are provided [here](#).

10.7 PingFederate - Apache Integration

5867 This section requires knowledge of the following pieces of information:

- 5868 ▪ Server IP address or hostname
- 5869 ▪ Server port where it is listening on
- 5870 ▪ Server credentials (i.e., private key and certificate) to be provisioned on directory server

10.7.1 Provisioning of Server Credential

5872 Start Apache Directory Server Studio and open a new connection.

5873 ***10.7.1.1 Creation of Server Connection***

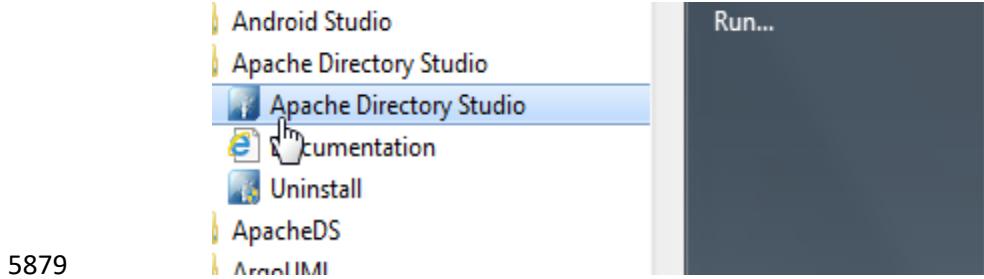
5874 1. To create a new LDAPS connection, complete the following steps:

5875 a. Define network parameters.

5876 b. Define authentication parameters.

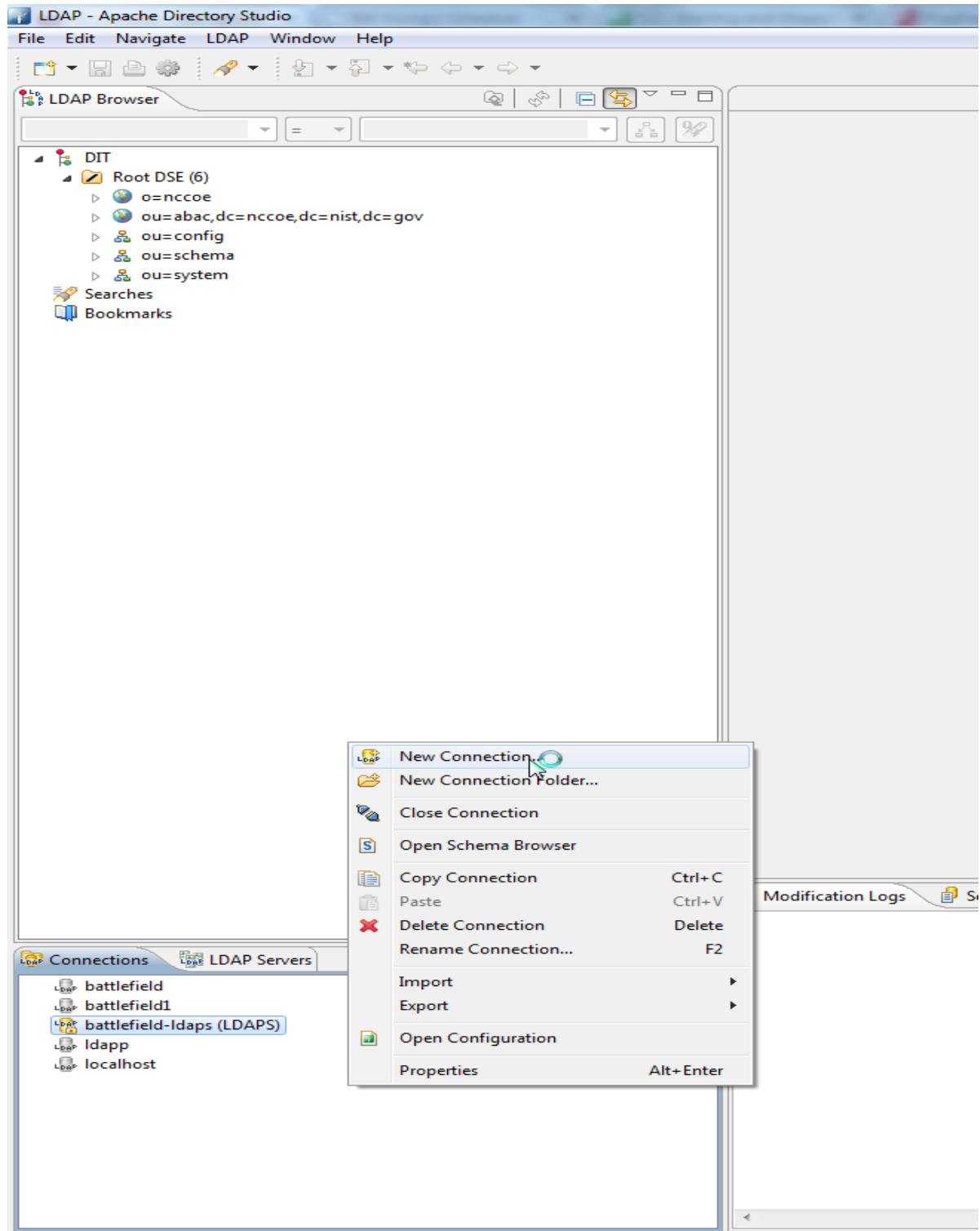
5877 c. Define additional browser options (optional).

5878 d. Define additional edit options (optional).



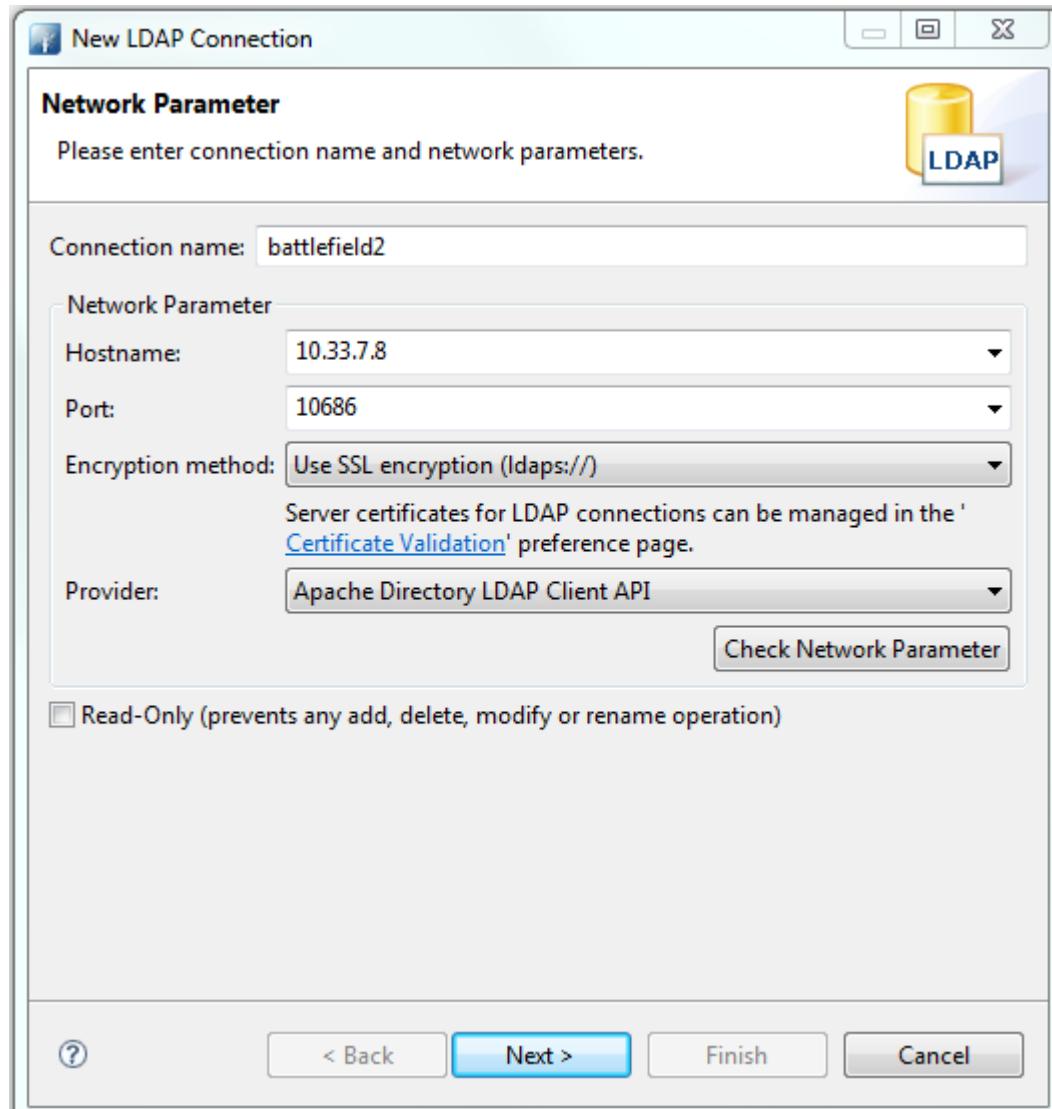
5879

SECOND DRAFT



5880

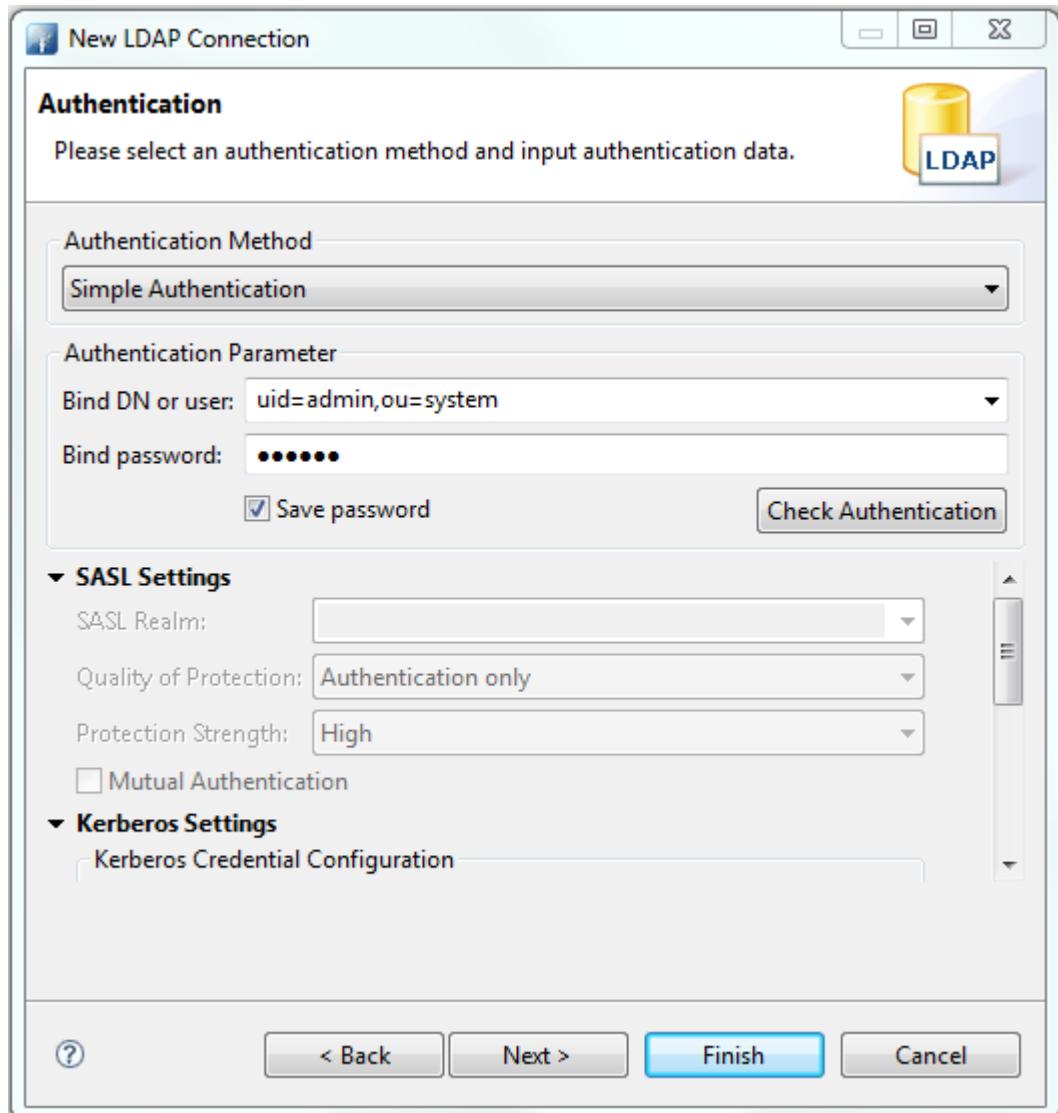
- 5881 2. Once a new connection is opened, the following screen appears. Fill in **Hostname** and **Port**.
5882 Select the encryption method **Use SSL encryption(ldaps://)**, then click **Next**.



5883

Option	Description	Default
Connection name	The name of the connection. In the Connections view, the connection is listed with this name. The name must be unique.	empty
Hostname	The hostname or IP address of the LDAP server. A history of recently used hostnames is available through the drop-down list.	empty
Port	The port of the LDAP server. The default port for non-encrypted connections is 389. The default port for ldaps:// connections is 636. A history of recently used ports is available through the drop-down list.	10636
Encryption method	The encryption to use. Possible values are: No encryption, ldaps:// and StartTLS extension.	No encryption
Provider	Option to choose either JNDI or Apache Directory LDAP client API	
Check network parameter	Use this function if you want validate that the entered information is correct, and the server is reachable.	
Read-Only	If this option is chosen, any attempts to modify will return an error.	

5884

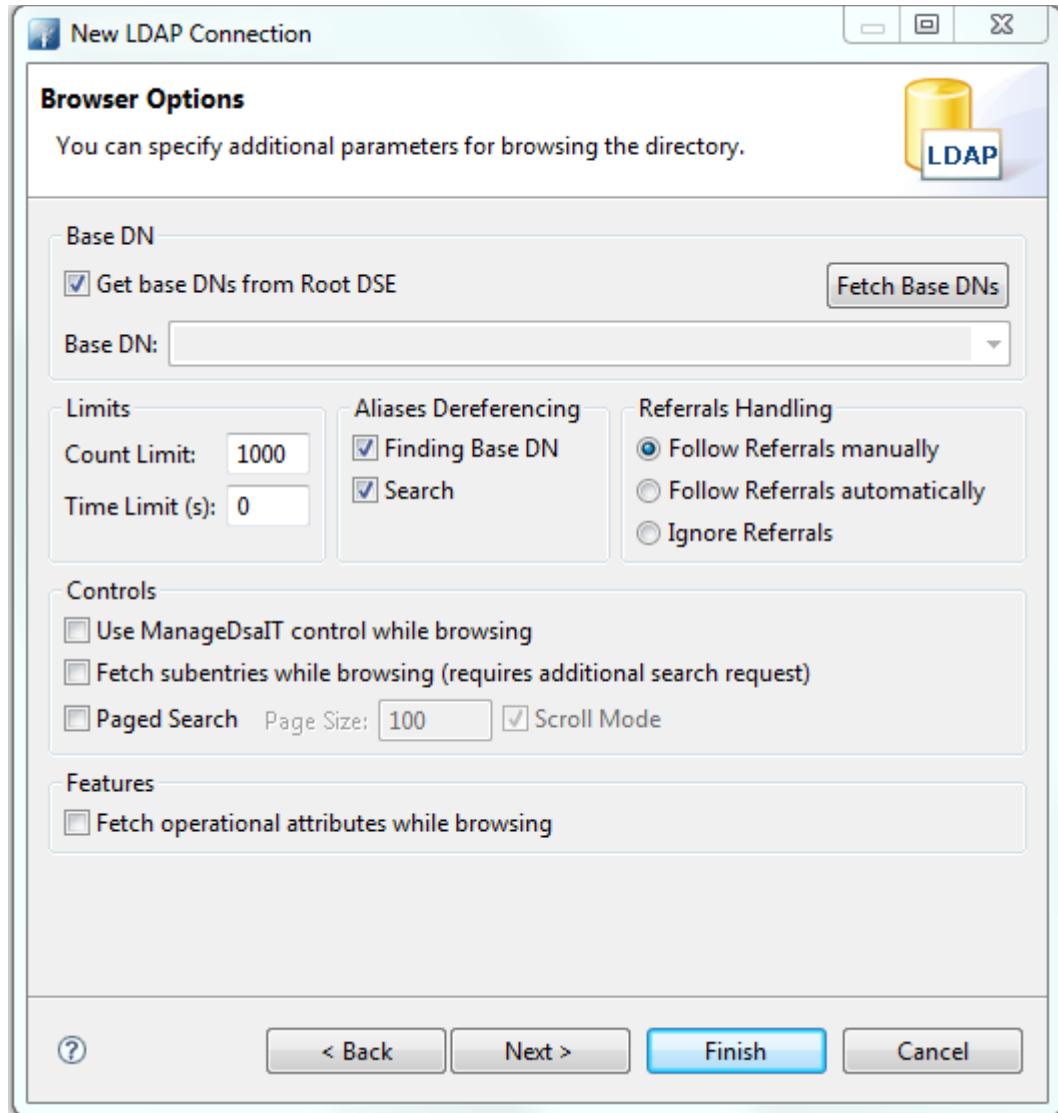


5885

Option	Description	Default
Authentication Method	Select your authentication method: <ul style="list-style-type: none"> Anonymous Authentication: connects to the directory without authentication. Simple Authentication: uses simple authentication using a bind DN and password. The credentials are transmitted in clear-text over the network. CRAM-MD5 (SASL): authenticates to the directory using a challenge-response authentication mechanism. The credentials are not transmitted in clear-text over the network. DIGEST-MD5 (SASL): another challenge-response authentication mechanism. Additionally, you could define your realm and QoP parameters. GSSAPI (Kerberos): user Kerberos-based authentication. Additional parameters can be defined. 	Simple Authentication
Bind DN or user	The distinguished name or user ID used to bind. Previously entered DNs can be selected from drop-down list.	empty
Bind Password	The password used to bind.	empty
Save password	If checked, the password will be saved in configuration. If not checked, you must enter the password whenever you connect to the server. Warning: The password is saved as plain text.	checked
Check Authentication	Use this function to attempt a connection plus a bind to the host upon completion of the wizard. It will validate that the entered information is correct.	

5886

This project does not use SASL or Kerberos.



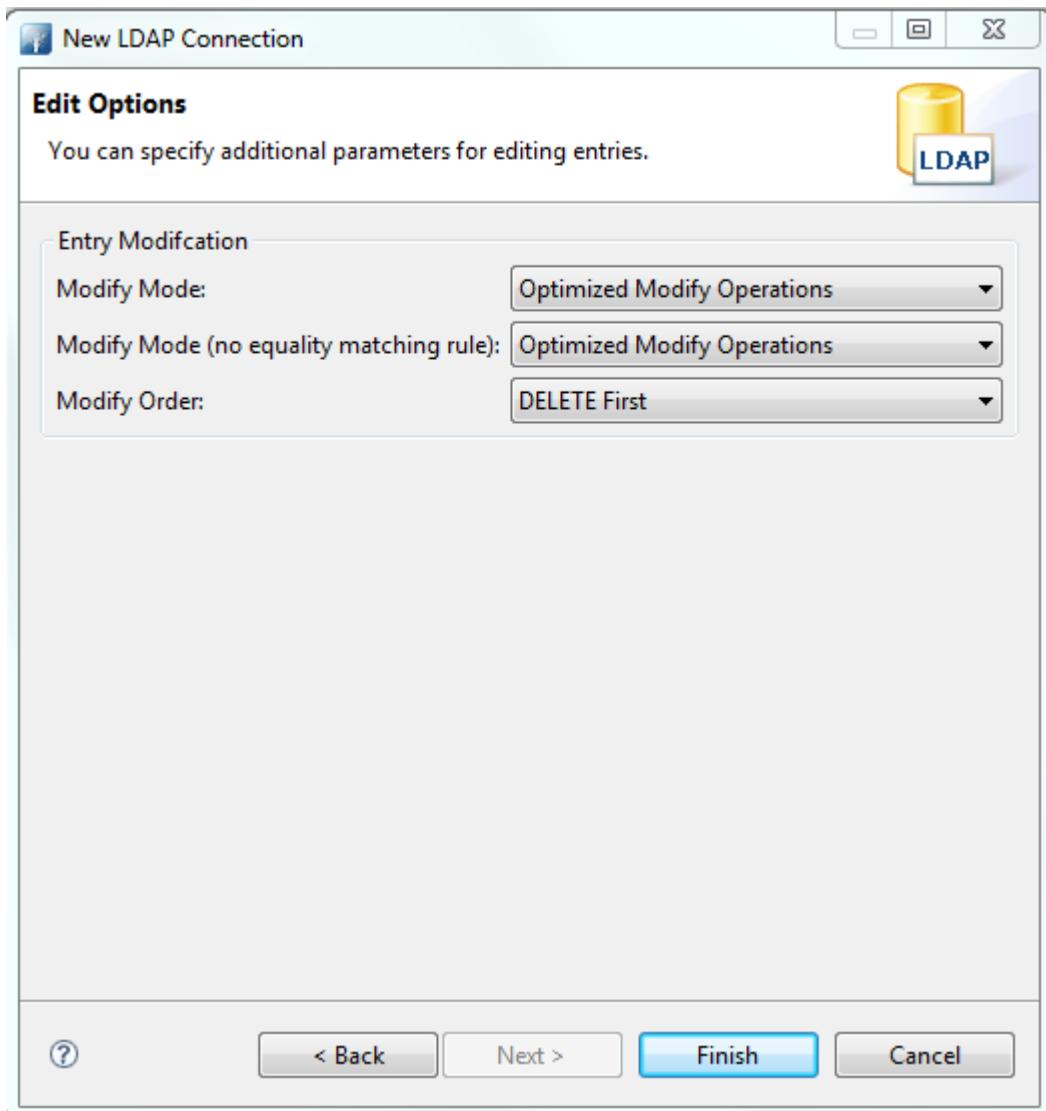
5887

Option	Description	Default
Get base DNs from Root DSE	If checked, the base DNs are fetched from the namingContexts attribute of the Root DSE.	checked
Fetch Base DNs	Use this function to get the namingContext values from the Root DSE. The returned values will appear in the Base DN drop-down list.	-
Base DN	The Base DN to use. You may enter a DN manually or select one from the drop-down list. This field is only enabled if the option Get base DNs from root DSE is off.	empty
Count Limit	Maximum number of entries returned from the server when browsing the directory. It is also used as default value when searching the	1000

Option	Description	Default
	directory. A value of 0 means no count limit. Note that this value is a client-side value. It is also possible to use a server-side limit.	
Time Limit	The maximum time in seconds the server searches for results. This is used as default value when browsing or searching the directory. A value of 0 means no limit. Note that this value is a client-side value. It is also possible to use a server-side limit.	0
Alias Dereferencing	Specifies whether aliases should be dereferenced while finding the search base entry, when performing the search, or both. To manage (create, modify, delete) alias objects you must uncheck both options.	Both finding and searching
Referrals Handling	<p>Specifies the referral handling.</p> <ul style="list-style-type: none"> Follow Referrals Manually: Received referrals and search continuations are displayed in the browser. When you open or expand a search continuation, the search is continued. Specify which connection you want to use to follow a specific referral URL. You will have full control regarding encryption and authentication options when following referrals. Follow Referrals Automatically: Follows referrals and search continuations immediately if they are received from the directory server. Specify which connection you want to use to follow a specific referral URL. You will have full control regarding encryption and authentication options when following referrals. Ignore Referrals: Any referral or search continuation received from the directory server is silently ignored. No error is logged, no dialog appears, no special entry is displayed in the DIT, and no ManageDsAIT control is sent to the server. 	Follow Referrals manually
Use ManageDsAIT control while browsing	If enabled, the ManageDsAIT control is sent to the server in each request. This signals the directory server not to send referrals and search continuations, but return the special referral objects. Note: This is only applicable if the directory server supports the ManageDsAIT control.	unchecked
Fetch subentries while browsing	If enabled, both normal and subentries according to RFC 3672 are fetched. This causes additional search requests while browsing the directory.	unchecked
Paged Search	If enabled, the simple paged result control is used while browsing the directory. With page size you can define how many entries should be retrieved in one request. If Scroll Mode is enabled, only one page is fetched from the server at a time. While browsing, you can scroll through the pages by using next page and top page . If	unchecked

Option	Description	Default
	disabled, all entries are fetched from the server. The paged result control is only used in the background to avoid server-side limits.	
Fetch operational attributes while browsing	If enabled, both user attributes and operational attributes are retrieved while browsing. If the server supports the feature All Operational Attributes , use + to retrieve operational attributes. Otherwise, all operational attributes defined in the schema are requested.	unchecked

5888

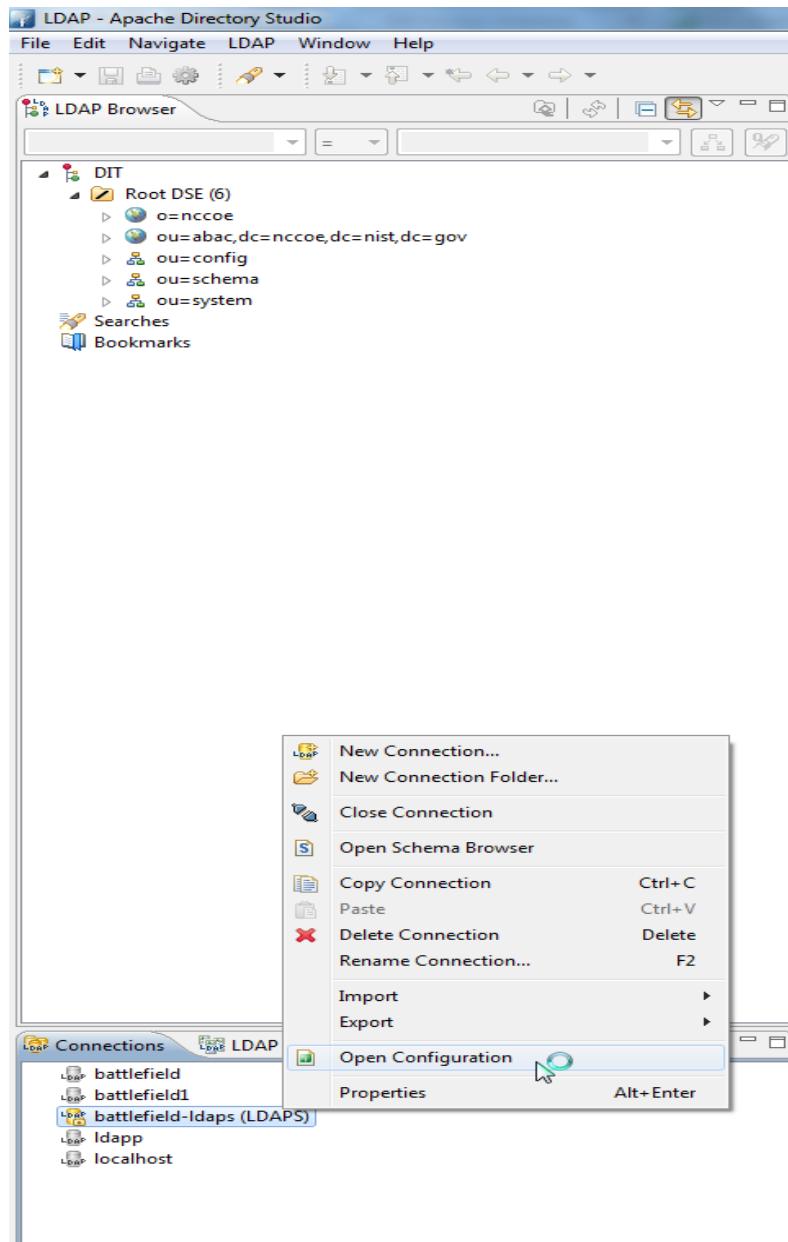


5889

Option	Description	Default
Modify Mode	<p>Specify the modify mode for attributes with an equality matching rule. Options:</p> <ul style="list-style-type: none"> • Optimized Modify Operations: uses add/delete by default, uses replace if operation count is less • Always REPLACE: always uses replace operations to perform entry modifications • Always ADD/DELETE: always uses add and/or delete operations to perform entry modifications 	Optimized Modify Operations
Modify Mode (no equality matching rule)	<p>Specify the modify mode for attributes with no equality matching rule. Options:</p> <ul style="list-style-type: none"> • Optimized Modify Operations: uses add/delete by default, uses replace if operation count is less • Always REPLACE: always uses replace operations to perform entry modifications • Always ADD/DELETE: always uses add and/or delete operations to perform entry modifications <p>Recommended values for various LDAP servers:</p> <ul style="list-style-type: none"> • ApacheDS: Optimized Modify Operations or REPLACE • OpenLDAP: REPLACE • OpenDS / SunDS: Optimized Modify Operations or REPLACE • FedoraDS / 389DS: Optimized Modify Operations (missing equality matching rules for many standard attribute types) • Active Directory: Optimized Modify Operations (exposes no equality matching rules at all) • eDirectory: Optimized Modify Operations (exposes no equality matching rules at all) 	Optimized Modify Operations
Modify Order	Specify the modify order when using add and delete operations.	Delete first

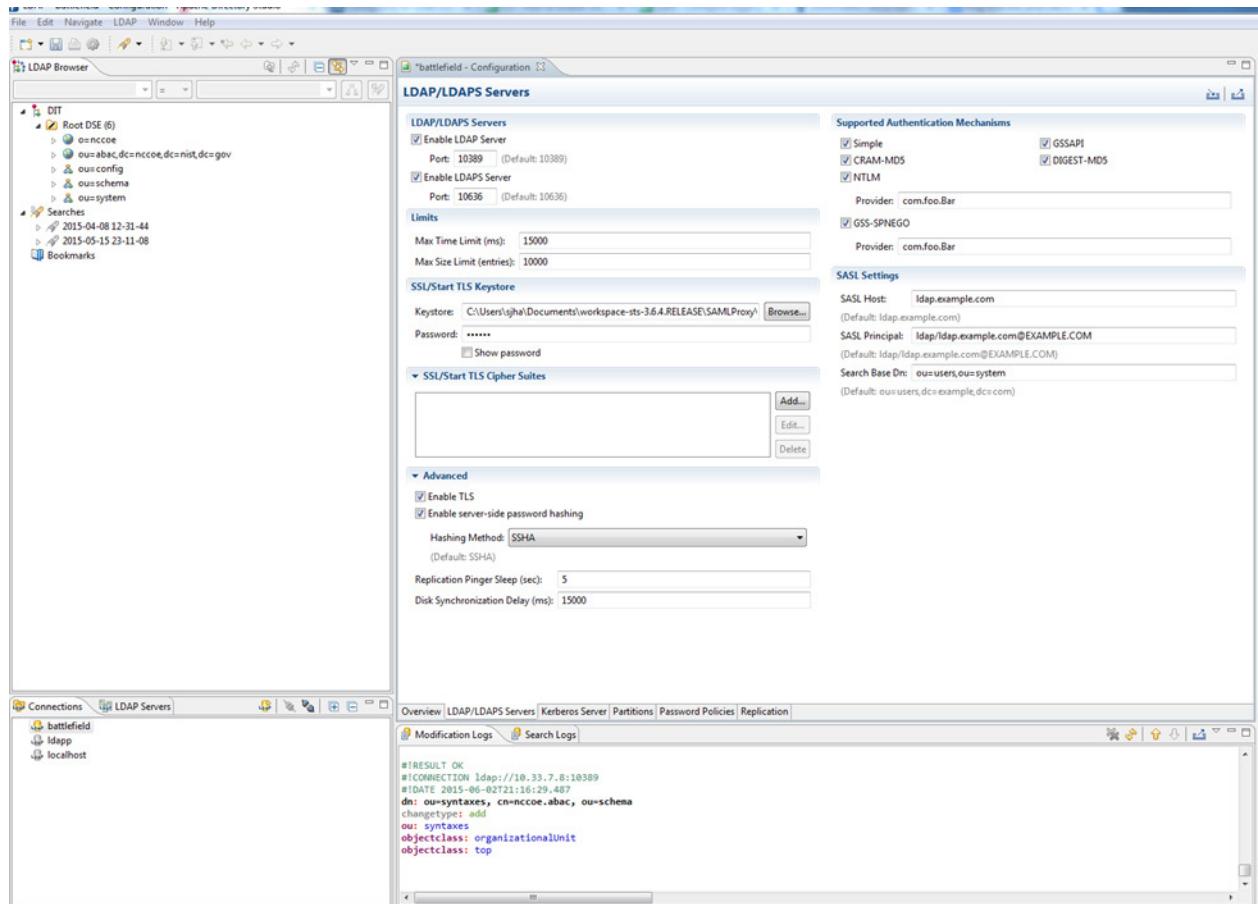
SECOND DRAFT

5890 3. Go to **Open Configuration** for the newly created connection.



5891

SECOND DRAFT



5892

Property	Default Value	Description
keystoreFile	none	Path of the X509 (or JKS) certificate file for LDAPS
certificatePassword	changeit	Password used to load the LDAPS certificate file
port	10636	LDAPS TCP/IP port number to listen to
enableSSL	true	Sets if SSL is enabled or not

5893

- 5894 4. Make sure **Enable LDAPS Server** is checked, and **Port** is the same as provided during creation of
5895 the connection.
- 5896 5. Go to SSL/Start TLS Keystore.
- 5897 6. Provide the **location** of the Keystore file and the **password** for the certificate.
- 5898 7. **Save** the configuration.
- 5899 8. **Restart** the server.

5900 **10.7.1.2 Verification**

5901 OpenSSL was used to acquire the server public certificate.

5902 >openssl s_client -showcerts -connect 10.33.7.8:10636 < /dev/null | openssl x509 -

5903 outform PEM > dir.pem

5904 depth=0 C = US, O = ASF, OU = Directory, CN = battlefield.bb-abac-bb1.nccoe.lab

5905 verify error:num=20:unable to get local issuer certificate

5906 verify return:1

5907 depth=0 C = US, O = ASF, OU = Directory, CN = battlefield.bb-abac-bb1.nccoe.lab

5908 verify error:num=27:certificate not trusted

5909 verify return:1

5910 depth=0 C = US, O = ASF, OU = Directory, CN = battlefield.bb-abac-bb1.nccoe.lab

5911 verify error:num=21:unable to verify the first certificate

5912 verify return:1

5913 DONE

5914 [sjha@battlefield ~]\$ more dir.pem

5915 -----BEGIN CERTIFICATE-----

5916 MIIBjDCCATYCBgFMlJE24DANBgkqhkiG9w0BAQUFADBCMQswCQYDVQQGEwJVUzEM

5917 MAoGA1UEChMDQVNGMRIwEAYDVQQLEw1EaXJ1Y3RvcnkxETAPBgNVBAMTCEFwYWNo

5918 ZURTMB4XDTE1MDQwNzE1NDgwN1oXDTE2MDQwNjE1NDgwN1owWzELMAkGA1UEBhMC

5919 VVMxDDAKBgNVBAoTA0FTRjESMBAGA1UECxMJRG1yZWN0b3J5MSowKAYDVQQDEyFi

5920 YXR0bGVmaWVsZC5iYi1hYmFjLWJiMS5uY2NvZS5sYWIwXDANBgkqhkiG9w0BAQEF

5921 AANLADBIAkEALLYJY8PJgMS82IqrW4uTVobkNqi2oJBoFAvOGMF7o1PCQ4x5vrgS

5922 6GEq9gUHk1ZZzymIIq6BMxoEb80161PY/wIDAQABMA0GCSqGSIb3DQEBBQUAA0EA

5923 hXNpaGff2Aboemwzt6U/fvSNyl+KRdeKFm0liWbseBk8OPvdOEmW96HVLvlbxSlc

5924 JpSznkLFhFOe0fimwB6GEg==

5925 -----END CERTIFICATE-----

5926 1. Verify the **certificate** received from the directory server against the certificate that was loaded earlier.

5928 **10.7.1.3 Configuration Steps on PingFederate RP Server**

CERTIFICATE MANAGEMENT

- Trusted CAs
- SSL Server Certificates
- SSL Client Keys & Certificates
-
- Digital Signing & XML Decryption Keys & Certificates
- Certificate Revocation Checking

AUTHENTICATION

- Application Authentication
- Password Credential Validators
- Active Directory Domains/Kerberos Realms

IDP-TO-SP BRIDGING

- Adapter-to-Adapter Mappings
- Connection Mapping Contracts

5929

5930 1. The following screen will appear, displaying all certificates on the server's global trust list.

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTION
0130.DB.8C.D4.83	CN=localhost, O=Quick Start App, C=US	Fri Jun 05 09:18:17 EDT 2111	RSA 1024	Valid	Export Delete
44.DC.CD.D7	CN=localhost, OU=Brian Campbell, O=Pingidentity, L=Denver, ST=CO, C=US	Tue Dec 27 13:35:03 EST 2033	RSA 1024	Valid	Export Delete
0130.DB.8C.25.AB	CN=demo dsig new, OU=Pingidentity, O=PingFederate, L=Denver, ST=CO, C=US	Fri Jun 05 09:17:32 EDT 2111	RSA 1024	Valid	Export Delete
014C.94.91.36.E0	CN=battlefield.bb-abac-bb1.nccoe.lab, OU=Directory, O=ASF, C=US	Wed Apr 06 11:48:07 EDT 2016	RSA 512	Valid	Export Delete
014C.DC.85.7F.1F	CN=idp.abac.test, O=NCCoE, C=US	Wed Apr 20 11:07:58 EDT 2016	RSA 2048	Valid	Export Delete

Import...

5931

5932 2. Select Import Certificate.

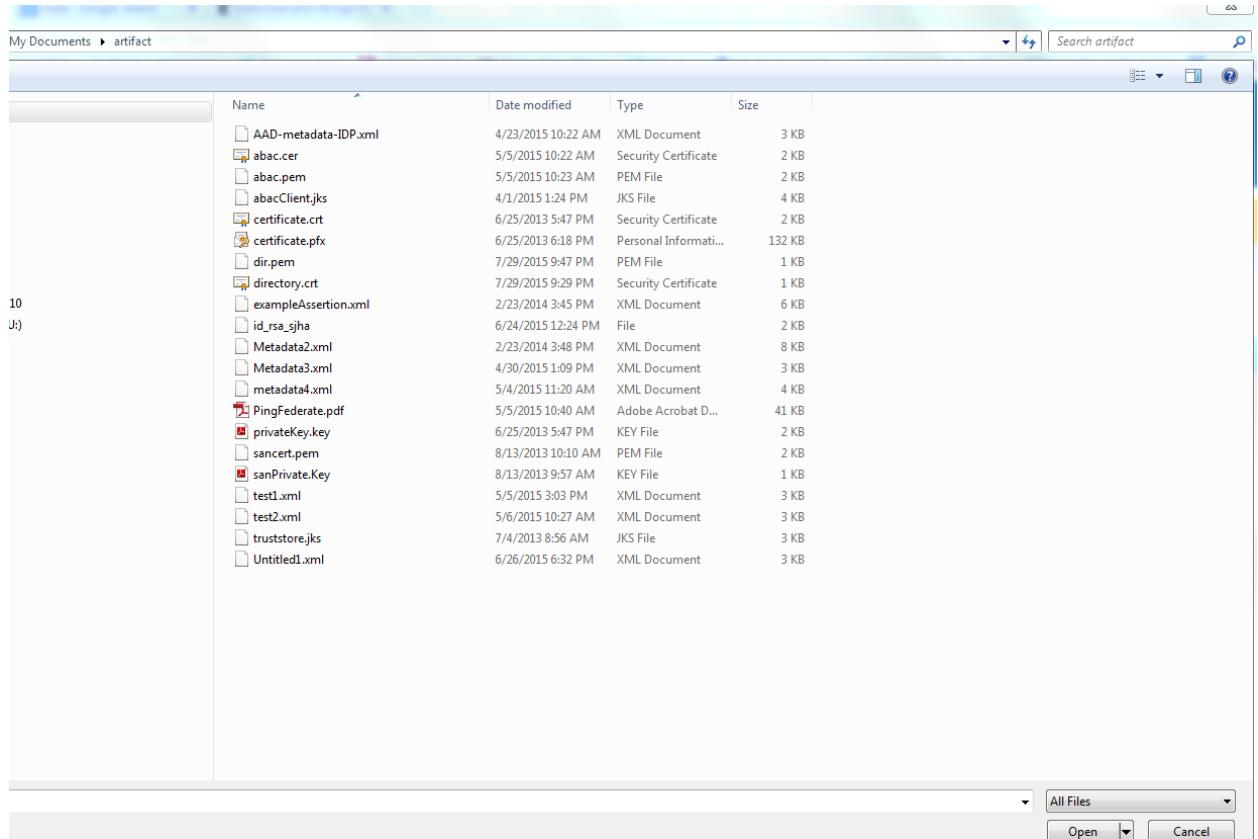
Please select the file containing the desired certificate.

Filename Choose File No file chosen *

5933

5934 3. Choose a file to import.

SECOND DRAFT



5935

5936

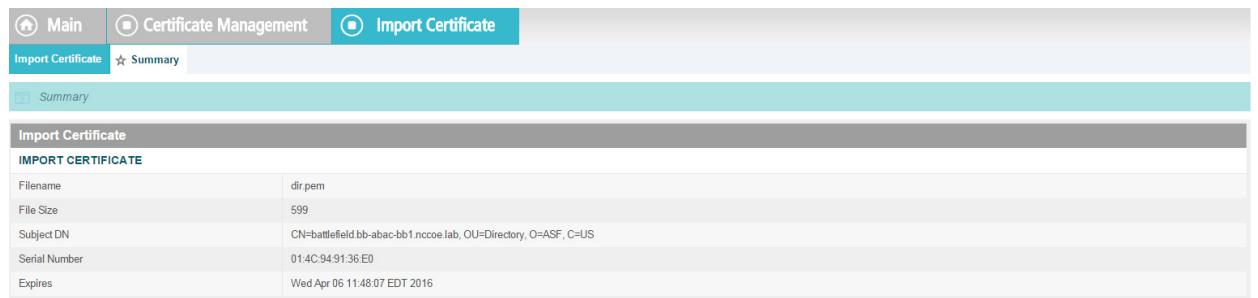
- Once your chosen file appears in the **Filename** field, click **Next**.



5937

5938

- View the **Summary** of the imported certificate.



5939

5940

- Click **Done**. The main screen will display a list of certificates. Click **Save**.

SECOND DRAFT

5941

5942 [10.7.1.3.1 Creation of Data Store to Connect to ApacheDS](#)

5943

5944 [7. Click on Data Stores.](#)

5945

5946 [8. In the Manage Data Stores window, click Add New Data Store.](#)

The screenshot shows a table of certificates with columns: SERIAL, SUBJECT DN, EXPIRES, KEY DETAILS, STATUS, and ACTION. The table contains six rows of certificate information. At the bottom left is a blue 'Import...' button.

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTION
0130DB8C4D483	CN=localhost, O=Quick Start App, C=US	Fri Jun 05 09:18:17 EDT 2111	RSA 1024	Valid	Export Delete
44DCCD:D7	CN=localhost, OU=Brian Campbell, O=PingIdentity, L=Denver, ST=CO, C=US	Tue Dec 27 13:35:03 EST 2033	RSA 1024	Valid	Export Delete
0130DB8C25AB	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US	Fri Jun 05 09:17:32 EDT 2111	RSA 1024	Valid	Export Delete
014CDC857F1F	CN=idp.abac.test, O=NCCoE, C=US	Wed Apr 20 11:07:58 EDT 2016	RSA 2048	Valid	Export Delete
014C949136E0	CN=battlefield bb-abac-bb1.nccoe.lab, OU=Directory, O=ASF, C=US	Wed Apr 06 11:48:07 EDT 2016	RSA 512	Valid	Export Delete

Server Configuration

SYSTEM SETTINGS

Server Settings

Data Stores

Redirect Validation

ADMINISTRATIVE FUNCTIONS

Metadata Export

XML File Signatures

Configuration Archive

Account Management

License Management

Virtual Host Names

Add New Data Store...

Main Manage Data Stores

Manage Data Stores

Manage data store definitions for use with attribute lookups.

DESCRIPTION	SYSTEM ID	USER	TYPE	LDAP TYPE	ACTION
jdbc:hsqldb:\$[boss.server.data.dir]\$[/hyperonic]\$[/ProvisionerDefaultDB	ProvisionerDS	sa	Database		Delete (Check Usage)
10.33.7.8:10389	LDAP-6399779A7D7C14C2F0880D7BDB27AC87C8ECE0FD		LDAP	Generic	Delete (Check Usage)
activedirectory.abac.test	LDAP-DFBE08A690B5467A07741DF51D756CBCB0737960		LDAP User	Active Directory	Delete (Check Usage)
idpQuery	Custom-B5051E1EF5F0684652FFE2B53F171E79D7BCF856		Custom		Delete (Check Usage)

Add New Data Store...

SECOND DRAFT

The screenshot shows a table of data stores with columns: DESCRIPTION, SYSTEM ID, USER, TYPE, LDAP TYPE, and ACTION. The data includes:

DESCRIPTION	SYSTEM ID	USER	TYPE	LDAP TYPE	ACTION
jdbc:hsqldb:\$@boss server data.dir\$/hypersonic\$//ProvisionerDefaultDB	ProvisionerDS	sa	Database		Delete (Check Usage)
10.33.7.8.10389	LDAP-6399779A7D7C14C2F0886D7BDB27AC87C8ECE0FD		LDAP	Generic	Delete (Check Usage)
activedirectory.abac.test	LDAP-DFBE08A690B5467A07741DF51D756C8CB0737960		LDAP User	Active Directory	Delete (Check Usage)
ldpQuery	Custom-B5051E1EF5F0684652FE2B53F171E79D7BCF856			Custom	Delete (Check Usage)

At the bottom left is a button labeled "Add New Data Store...".

5947

- 5948 9. Choose LDAP, and click Next.

The screenshot shows a "Data Store Type" tab selected. It displays a message: "Please select a type of data store." Below are three radio buttons: Database, LDAP (selected), and Custom.

5949

- 5950 10. Provide a Hostname and Ldaptype.

The screenshot shows the "LDAP Configuration" tab selected. It includes fields for Hostname(s) (battlefield.bb-abac-bb1.nccoe.lab:103), LDAP Type (Generic), Bind Anonymously (unchecked), User DN (uid=admin,ou=system), Password (*****), Use LDAPS (checked), and Mask Values in Log (unchecked). At the bottom left is an "Advanced..." button.

5951

- 5952 11. It may be necessary to configure connection pooling. It is important to select Verify LDAPS
5953 Hostname if the directory server certificate is bound to a hostname, and this hostname can be
5954 verified.

SECOND DRAFT

This screenshot shows the 'Advanced LDAP Options' configuration screen. At the top, there are tabs for Main, Manage Data Stores, Data Store, and Advanced LDAP Options, with 'Advanced LDAP Options' being the active tab. Below the tabs, there is a note: 'Manage LDAP connection-pooling settings on this screen as needed.' There are several configuration options with checkboxes:

- Test Connection on Borrow
- Test Connection on Return
- Create New Connections if Necessary
- Verify LDAPS Hostname

Below these are input fields for connection pooling parameters:

Minimum Connections	10
Maximum Connections	100
Maximum Wait (Milli)	-1
Time Between Eviction (Milli)	60000
Read Timeout (Milli)	3000
Connection Timeout (Milli)	3000

At the bottom left is a button labeled 'Apply Defaults...'.

5955

5956 12. If there is any binary data, enter it in the **Binary Attribute Name** Field, and click **Add**.

This screenshot shows the 'LDAP Binary Attributes' configuration screen. At the top, there are tabs for Main, Manage Data Stores, Data Store, and Advanced LDAP Options, with 'Advanced LDAP Options' being the active tab. Below the tabs, there is a note: 'Specify the LDAP attributes to be handled as binary data.' A table is used to manage binary attributes:

BINARY ATTRIBUTE NAME	ACTION
(empty field)	<input type="button" value="Add"/>

5957

5958 13. A **summary** of the LDAP configuration will appear.

This screenshot shows the 'LDAP Configuration' summary screen. At the top, there are tabs for Main, Manage Data Stores, Data Store, and Data Store Type, with 'Data Store Type' being the active tab. Below the tabs, there is a note: 'Please provide the details for configuring this LDAP connection.' The configuration details are listed in a form:

Hostname(s)	10.33.7.8:10636
LDAP Type	Generic
<input type="checkbox"/> Bind Anonymously	
User DN	uid=admin,ou=system
Password	*****
<input checked="" type="checkbox"/> Use LDAPS	
<input type="checkbox"/> Mask Values in Log	

At the bottom left is a button labeled 'Advanced...'.

5959

5960 14. A **Summary** of the **connection** will appear as following. Click **Save**. You will then return to the
5961 Main Admin console.

This screenshot shows the 'LDAP Configuration' summary screen. At the top, there are tabs for Main, Manage Data Stores, Data Store, and Data Store Type, with 'Data Store Type' being the active tab. Below the tabs, there is a note: 'Click a heading link to edit a configuration setting.' The configuration details are listed in a form:

Data Store	
DATA STORE TYPE	
Type of Data Store	LDAP
LDAP CONFIGURATION	
Hostname(s)	10.33.7.8:10636
Username	uid=admin,ou=system

5962

5963 10.8 Configuration of PingFederate to Query the JIT Cache when 5964 Responding to Secondary Attribute Requests

5965 10.8.1 Introduction

5966 This section will cover all the configuration steps required to enable PingFederate RP to communicate
5967 with the Secondary attribute Provider and respond to its queries. The SP connection section will cover
5968 communication channel protection and message protection. To fulfill the query request from the
5969 NextLabs PIP Plugin and Protocol Broker, PingFederate queries its local LDAP server called Just in Time
5970 (JIT) cache. Note that PingFederate RP may not have data to fulfill the query. In that case, PingFederate
5971 RP extends the query to PingFederate IdP using a unique method (Ping Data source).

5972 A Data Store is any type of source for digitized data, i.e., database, file, stream, etc. PingFederate
5973 administration console uses this term for system settings. In the Java software platform, [data source](#) is a
5974 factory for connections to the physical data source that this data source object represents. Thus, data
5975 source is the logical manifestation of a physical data store in a java application. Due to this, the terms
5976 will be used interchangeably below.

5977 This section provides the configuration needed to query JIT cache, i.e., creation of the data source for
5978 the LDAP Server. We have already discussed the configuration of Ping Data Source in Custom Data Store
5979 section. SP connection describes how both of these data stores are chained together to fetch the result
5980 of the attribute query.

5981 10.8.2 Prerequisites

5982 Before starting this configuration, the following steps must have already been completed:

- 5983 1. Sections 2-7
 - 5984 a. Complete Installation of PingFederate, both RP and Idp
 - 5985 2. Installation and configuration of ApacheDS
 - 5986 3. Installation of Ping Custom Data Store
 - 5987 4. Availability of Ping web administration console (automatically included in the PingFederate
5988 installation from previous How-To Guide sections)

5989 10.8.2.1 SP Connection

5990 As described above, PingFederate (RP) acts as an IdP for the Secondary attribute provider. In order to
5991 enable support for exchange of federation-protocol messages and provide channel protection, it is
5992 essential to configure the SP (Service Provider) connection. Note: Ping Identity's documentation uses the
5993 term **Service Provider** and **SP** where the rest of our ABAC documentation uses the term **Relying Party**
5994 and **RP**. In this document, please consider these terms interchangeable.

5995 The following goals are achieved by configuration of the SP connection:

- 5996 ▪ Specification of connection and associated security protocol (i.e., TLS/SSL)
- 5997 ▪ Specification of SAML profile t including detailed security specifications (the use of digital
5998 signatures, signature verification, XML encryption)

SECOND DRAFT

- 5999 ▪ Specification of Attributes that may be sent using the SAML2 Attribute Query profile
6000 ▪ Specification of Data Store(s), if agreement between Idp and SP includes sending a SAML
6001 response containing attribute values from a local data store

10.8.2.1.1 Specification of Profile

6002 Instructions on how to create a new connection can be found [here](#).

- 6004 1. Click on **Manage on All SP** in the first column on the left hand side.

The screenshot shows the 'IdP Configuration' interface with the 'SP Connections' section selected. It displays two entries: 'WS Fed SharePoint' and 'SAML2.0 Demo SP'. Below each entry are links for 'Manage All SP', 'Create New', and 'Import'. To the right of the screenshot is a detailed view of the 'SP Configuration' interface, which includes sections for Certificate Management, Authentication, and IDP Connections, mirroring the structure of the 'IdP Configuration' interface.

6005

- 6006 2. The following screen will appear. Click on **Create Connection**.

The screenshot shows the 'SP Connections' management screen. It lists two existing connections: 'Demo SP' (Protocol: SAML2.0) and 'SharePoint' (Protocol: WS Fed). Below the table are buttons for 'Create Connection...' and 'Import Connection'. At the bottom, there is a 'Logging Mode Override' section with radio buttons for 'Off' and 'On'.

6007

- 6008 3. Check the box for **Browser SSO Profiles** and select **SAML 2.0** as protocol from the drop-down
6009 menu.

SECOND DRAFT

The screenshot shows the 'SP Connection' configuration interface. The top navigation bar has tabs for 'Main', 'SP Connections', and 'SP Connection'. The 'SP Connection' tab is active. Below it, a sub-navigation bar includes 'Connection Type' (selected), 'Connection Options', 'Import Metadata', 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. A note at the top says: 'Select the type of connection needed for this SP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), Outbound Provisioning (for provisioning users/groups to an SP) or all.' Under 'Connection Type', 'Browser SSO Profiles' is checked. The 'Protocol' dropdown is set to 'SAML 2.0'. Other options like 'WS-Trust STS' and 'Outbound Provisioning' are also listed.

6010

- 6011 4. Uncheck **Browser SSO**, check **Attribute Query**, and click **Next**.

The screenshot shows the 'Connection Options' configuration interface. The top navigation bar includes 'Connection Type' (selected), 'Connection Options', 'Import Metadata', 'General Info', 'Attribute Query', 'Credentials', and 'Activation & Summary'. A note at the top says: 'Please select options that apply to this connection.' Under 'Connection Options', the 'Attribute Query' checkbox is checked, while 'Browser SSO' and 'IdP Discovery' are unchecked.

6012

- 6013 5. Choose a metadata file and click **Next**.

The screenshot shows the 'Import Metadata' configuration interface. The top navigation bar includes 'Main', 'SP Connections' (selected), and 'SP Connection'. Below it, a sub-navigation bar includes 'Connection Type', 'Connection Options', 'Import Metadata' (selected), 'General Info', 'Attribute Query', 'Credentials', and 'Activation & Summary'. A note at the top says: 'If you received a metadata file from a partner SP describing this new connection, import the file here to populate many connection settings automatically.' A 'Choose File' button shows 'metadata4.xml'.

6014

- 6015 6. SAML2 metadata has its own [specification](#). As per this specification, KeyDescriptor is an optional
6016 sequence of elements that provides information about the cryptographic keys that the entity
6017 uses when acting in this role. However, for message authentication and integrity, it is essential
6018 to provide the certificate so that signed messages coming from the secondary attribute provider
6019 can be verified. A relevant part of metadata is shown here:

6020 <md:KeyDescriptor use="signing">

6021 <ds:KeyInfo>

6022 <ds:X509Data>

6023 <ds:X509Certificate>

6024 MIIE4jCCAsqgAwIBAgICEAMwDQYJKoZIhvCNQELBQAwyjELMAkGA1UEBhMCVVMx

6025 ETAPBgNVBAgMCE1hcnlSYW5kMRIwEAYDVQQHDA1Sb2NrdmlsbGUxDjAMBgNVBAoM

6026 BU5DQ29FMQ0wCwYDVQQLDARBQkFDMQ0wCwYDVQQDDARBQkFDMB4XDTE1MDQwMTE4

6027 MTA1Nl0XDTE2MDMzMTE4MTA1Nl0wejELMAkGA1UEBhMCVVMxETAPBgNVBAgMCE1h

SECOND DRAFT

```
6028      cnlsYW5kMQ4wDAYDVQQKDAVOQ0NvRTENMAsGA1UECwwEQUJBQzEUMBIGA1UEAwL
6029      TU0xOTU1OTITUEMxIzAhBgkqhkiG9w0BCQEWFHNqaGFATU0xOTU1OTITUEMu3Jn
6030      MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEauzxrl5iAIpNyEXHmGTDW
6031      1mzx7YJal/c9Ruxag3sifjzuUdBjEznFJJxaagM2pzTUI5JCaLzgm71VSBmuVL+6
6032      PzTxReM3i5XzWjpgRMIizadnQT0wmCryKuNaQiBIFLoMbi+ySdBvu+M/xhH1RxuF
6033      jY9NPSE1MHL8YaLoKW2SFIm/3bhJ/xF7q7FGHMcJH4Zzr2QpQmBERyozJJV3z4Zv
6034      Vro/MfyLg1VER0pu36e32hIyzsf2gKizv00qY2ecD1BCNTITsA2HWSTf50kpvt4q
6035      upCnXVKVqzDPZON0CsJJcwWsUi9pRvkGtVBXqhh282ODyzcl3nkpgs15F8hR7kO
6036      jQIDAQABo4GJMIGGMAkGA1UdEwQCMAwCwYDVR0PBAQDAgXgMCwGCWCGSAGG+EIB
6037      DQQfFh1PcGVuU1NMIEdlbmVyYXR1ZCBDZXJ0aWZpY2F0ZTAdbgNVHQ4EFgQURPRr
6038      8BNghnDip40B1sy6AWpWJmcwHwYDVR0jBBgwFoAUyZ5WFptCW/BOjVxvof8eNcBo
6039      5c8wDQYJKoZIhvcNAQELBQADggIBAGhVmD47uFNi1z8oEYgwDInZDAtfujvkfTu2
6040      Dtr7dvkvB2x6uW481ffIKDKb48yKVbMO0kSwU4esPHgMWowJJs37XFo9PYJ1kaE/
6041      NCD7e8V4p3xhzXux6JqKpaholxHifzEsdKqOyNj00ZXqmRMstbw6UC+IFCNUWJZQ
6042      zJ+Dwciaxa9kq/huv8BMbYzcL8r1fE3x9nUwwuFuXudpnED0B+Rmmod1G5fVG1j
6043      agMWakXscGJ9rpT8wgfJGjU4Sct3Eocp5roRGopUVBrW6jljZD4dYEuleJ1LJqcW
6044      mDiYdZIvu0z393HApNpwC4XSaMoTN7xq4Z+Xwe0zdt1HVM0aeAiglrDB3XKuiYQT
6045      Ab899WBgK/TixTLJ+Nf6FkAl2apkVkaxxl+35DZrkDOHo3HQTORQFNYcb1LlrsfP
6046      A5r0PPVi6XE6h4k9/CgO03Q6fzpgl7avCrw8s1m/WnmQjfc0K+op717zsYrnsxdB
6047      wQsnaT6GX2csy99jOpfLK1Sh6ja1uFdRPMEwjhNyqTy2xoLfuYK5bxMzlpfaoZE
6048      sVURPCFiC0G97xn8ffjjhv5Kby8JIRWV2QhXicf5FsWoiWZIhtHo0L9WEQXKPTO1
6049      +8310xJDW6bosdNww8IbRft1MYqGWYCTnwmBshURCXSJrjpE/MInE5nw/7QWA/OR
6050          U3r4Pv6s
6051      </ds:X509Certificate>
6052      </ds:X509Data>
6053      </ds:KeyInfo>
6054      </md:KeyDescriptor>
6055      7. Verify the metadata content.
```

Main **SP Connections** **SP Connection**

Connection Type **Connection Options** **Import Metadata** **Metadata Summary** **General Info** **Attribute Query**

Credentials Activation & Summary

Use the information below to evaluate the authenticity of the imported metadata.

Metadata File	unsigned
---------------	----------

Main **SP Connections** **SP Connection**

Connection Type **Connection Options** **Import Metadata** **Metadata Summary** **General Info** **Attribute Query**

Credentials Activation & Summary

This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these virtual server IDs will be used in place of the unique protocol identifier configured for your server in Server Settings. The Base URL may be used to simplify configuration of partner endpoints.

Partner's Entity ID (Connection ID)	urn:nccoe:abac:plugin *
Connection Name	urn:nccoe:abac:plugin *
Virtual Server IDs	<input type="button" value="Add"/>
Base URL	http://10.33.7.8:8080
Company	The National Cybersecurity Center of
Contact Name	John Smith
Contact Number	+1 (240) 314-6800
Contact Email	john.smith@nccoe.nist.gov
Application Name	
Application Icon URL	
Logging Mode	<input type="radio"/> None <input checked="" type="radio"/> Standard <input type="radio"/> Enhanced <input type="radio"/> Full

8. Click on Configure Attribute Query Profile.

The screenshot shows the 'SP Connection' tab selected in the top navigation bar. Below it, a sub-menu bar includes 'Connection Type', 'Connection Options', 'Import Metadata', 'Metadata Summary', 'General Info', and 'Attribute Query'. The 'Attribute Query' option is highlighted with a star icon. A secondary menu at the bottom of this bar includes 'Credentials' and 'Activation & Summary'. A callout box in the center states: 'The Attribute Query Profile supports SPs in requesting user attributes. Click the button below to configure the necessary settings to support this profile.' A large blue button labeled 'Configure Attribute Query Profile' is visible.

6059

- 6060 9. Specify the list of attributes that may be returned to the SP in response to an attribute request.

The screenshot shows the 'Attribute Query' tab selected in the top navigation bar. Below it, a sub-menu bar includes 'Retrievable Attributes', 'Attribute Sources & User Lookup', 'Attribute Mapping Fulfillment', and 'Issuance Criteria'. The 'Retrievable Attributes' option is highlighted with a star icon. A secondary menu at the bottom of this bar includes 'Security Policy' and 'Summary'. A callout box in the center states: 'Specify the list of attributes that may be returned to the SP in the response to an attribute request.' A table lists attributes with edit/delete actions:

RETRIEVABLE ATTRIBUTES	ACTION
clearance	Edit / Delete
division	Edit / Delete
employer	Edit / Delete
fullname	Edit / Delete
role	Edit / Delete
stafflevel	Edit / Delete
username	Add

6061

SECOND DRAFT

6062 10.8.2.1.2 Specify a series of data stores.

6063 1. In the **Attribute Source Id** field, specify **JIT (LDAP)**.

The screenshot shows the 'Attribute Sources & User Lookup' configuration page. The 'Attribute Source Id' is set to 'JIT (LDAP)' and the 'Attribute Source Description' is 'Just in Time cache source'. The 'Active Data Store' is '10.33.7.8:10389' and the 'Data Store Type' is 'LDAP'. A 'Manage Data Stores...' button is visible at the bottom left.

Attribute Source Id	JIT (LDAP)
Attribute Source Description	Just in Time cache source
Active Data Store	10.33.7.8:10389
Data Store Type	LDAP

Manage Data Stores...

6064

6065 2. Specify **Attributes** for the JIT Cache.

The screenshot shows the 'LDAP Directory Search' configuration page. The 'Base DN' is 'ou=users,ou=system' and the 'Search Scope' is 'Subtree'. Below this, a table lists attributes to return from search:

ROOT OBJECT CLASS	ATTRIBUTE	ACTION
	Subject DN	
	employeeType	Remove
<Show All Attributes>	givenName	Add Attribute

[View Retrievable Attributes](#)

6066

3. Specify **LDAP Filter**.

The screenshot shows the 'Attribute Sources & User Lookup' section of a web-based configuration tool. At the top, there are tabs for 'Main', 'SP Connection', 'Attribute Query', and 'Attribute Sources & User Lookup'. Below these, sub-tabs include 'Data Store', 'LDAP Directory Search', 'LDAP Filter', and 'Summary'. A note below the tabs says: 'Define a filter for extracting data from your directory. In qualifying the search, you should use only those values passed in the DN from the SP.' A 'Filter' input field contains the value 'uid=\${SAML SUBJECT}' with an asterisk (*) indicating it is required. A link 'View List of Available LDAP Attributes' is also present.

6068

- 6069 4. Verify that your data is correct.

The screenshot shows the 'Attribute Sources & User Lookup' section with tabs for 'Data Store', 'LDAP Directory Search', 'LDAP Filter', and 'Summary'. The 'Attribute Source Summary' section is visible. Below it is a large 'Attribute Sources & User Lookup' header. The interface is divided into several sections: 'DATA STORE' (Attribute Source: JIT (LDAP), Attribute Source Id: JIT, Type of Data Store: LDAP, Data Store: 10.33.7.8:10389); 'LDAP DIRECTORY SEARCH' (Base DN: ou=users,ou=system, Search scope: SUBTREE_SCOPE, Attribute: Subject DN, Attribute: employeeType); and 'LDAP FILTER' (Filter: uid=\${SAML SUBJECT}).

6070

- 6071 5. Specify a custom **Data Store**.

SECOND DRAFT

Attribute Source Id: aaquery *

Attribute Source Description: Attribute Query *

Active Data Store: idpQuery *

Data Store Type: Custom

This server uses local data stores to retrieve user attributes in response to an attribute request.

6072

6. Define a filter for extracting data from this data store.

FIELD NAME	FIELD VALUE	DESCRIPTION
SUBJECT	\${SAML_SUBJECT}	Subject field used in Query parameter of URL

Define a filter for extracting data from this data store.

6074

7. Based on the data elements available from this data store, select the ones pertinent to this connection. Note that these are the attributes you previously selected to return from Ping Custom Data.

Based upon the data elements available from this data store, select the ones to retrieve.

- fullname
- username
- stafflevel
- role
- division
- employer
- clearance

6078

8. Click **Retrieve**.

SECOND DRAFT

DATA STORE

Attribute Source	aaquery
Attribute Source Id	aaquery
Type of Data Store	Custom
Data Store	idpQuery

CONFIGURE CUSTOM SOURCE FILTERS

Subject	\$(SAML_SUBJECT)
---------	------------------

CONFIGURE CUSTOM SOURCE FIELDS

Field	fullname
Field	username
Field	stafflevel
Field	role
Field	division
Field	employer
Field	clearance

6080

6081

9. Click on **Attribute Mapping Fulfillment**.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
clearance	Text	#clearance = #this.get("ds.JIT.carLicense"), #queryclearance = #this.get("ds.aaquery.clearan	None available
division	Text	#division = #this.get("ds.JIT.physicalDeliveryOfficeName"), #querydivision = #this.get("ds.aaq	None available
employer	Text	#employer = #this.get("ds.JIT.member"), #queryemployer = #this.get("ds.aaquery.employe	None available
fullname	Text	#fullname = #this.get("ds.JIT.cn"), #queryfullname = #this.get("ds.aaquery.fullname"), (#fullna	None available
role	Text	#role = #this.get("ds.JIT.title"), #queryrole = #this.get("ds.aaquery.role"), (#role == null #role	None available
stafflevel	Text	#stafflevel = #this.get("ds.JIT.employeeType"), #querystafflevel= #this.get("ds.aaquery.staffle	None available
username	Text	#username= #this.get("ds.JIT.givenName"), #queryusername= #this.get("ds.aaquery.username")	None available

6082

6083

10. **Issuance Criteria:** PingFederate can evaluate various criteria to determine whether to issue an attribute query response. Use this optional screen to configure the criteria for use with this conditional authorization.

SOURCE	ATTRIBUTE NAME	CONDITION	VALUE	ERROR RESULT	ACTION
- SELECT -	- SELECT -	- SELECT -			Add

6086

6087

11. Click on **Security Policy**.

SECOND DRAFT

The screenshot shows the 'Attribute Query' tab selected in a navigation bar. Below it, a sub-navigation bar includes 'Retrievable Attributes', 'Attribute Sources & User Lookup', 'Attribute Mapping Fulfillment', 'Issuance Criteria', 'Security Policy' (which is highlighted with a star), and 'Summary'. A note at the top says 'Specify the attribute requester profile's security policy with your partner.' Below this are several checkboxes: 'Sign the Response' (unchecked), 'Sign the Assertion' (checked), 'Encrypt the Assertion' (unchecked), 'Require signed Attribute Query' (checked), and 'Require an encrypted Name Identifier' (unchecked).

6088

6089 12. Check the **Summary**.

The screenshot shows the 'Attribute Query' configuration page with the 'Summary' tab selected. It displays various configuration sections: 'RETRIEVABLE ATTRIBUTES' (listing attributes like clearance, division, employer, fullname, role), 'ATTRIBUTE SOURCES & USER LOOKUP' (listing Data Stores: JIT (LDAP) (LDAP) and Attribute Query (Custom)), 'DATA STORE' (listing Attribute Source, Attribute Source Id, Type of Data Store, and Data Store details), and 'LDAP DIRECTORY SEARCH' (listing Base DN, Search scope, Attribute, and Attribute values). A note at the top says 'Click a heading link to edit a configuration setting.'

6090

6091 13. Provide **Credentials** for the back channel attribute request.

The screenshot shows the 'SP Connection' configuration page with the 'Credentials' tab selected. A note at the top says 'The Attribute Query Profile supports SPs in requesting user attributes. Click the button below to configure the necessary settings to support this profile.' Below is a 'Configure Attribute Query Profile' button.

6092

6093 14. Specify **Inbound Back-Channel Authentication** and **Digital Signature** on the message.

The screenshot shows the 'SP Connection' configuration page with the 'Connection Type' tab selected. A note at the top says 'For each credential shown here, configure the necessary settings.' Below is a table of credential requirements:

Credential Requirement	
Inbound Back-Channel Authentication	Not Configured
Digital Signature	Not Configured
Signature Verification Settings	Unanchored Certificate (Primary CN=MM195592-PC, Secondary Not Configured)

Below the table is a 'Configure Credentials' button.

6094

SECOND DRAFT

6095 10.8.2.1.3 Back Channel Authentication Configuration

1. Use the default **Transport Layer Authentication** with **SSL Client Certificate**.

The screenshot shows the 'Back-Channel Authentication' tab selected in a navigation bar. Below it, the 'Inbound Authentication Type' section is highlighted. Under 'Select the SOAP authentication method(s) to use when your partner sends an Attribute Query request using the SOAP back channel.', the 'Transport Layer Authentication' radio button is selected. Other options like 'No Client Authentication', 'HTTP Basic', and 'SSL Client Certificate' are shown but not selected.

6097

2. It is encouraged to use the **Anchored** verification method.

The screenshot shows the 'Back-Channel Authentication' tab selected in a navigation bar. Below it, the 'Inbound Authentication Type' section is highlighted. Under 'Select the method of certificate verification to use when the remote party connects to the SOAP endpoint and begins SSL client certificate authentication.', the 'Anchored' radio button is selected. A note states 'The client certificate must be signed by a Trusted CA.' The 'Unanchored' option is also listed.

6099

3. You will be prompted to select an **SSL Verification Certificate**. In our build, a certificate has not been previously imported. Click on **Manage Certificate**.

The screenshot shows the 'Manage Certificate...' button highlighted. Below it, a dropdown menu is open with the text '- SELECT - *'.

6102

4. Click **Import**.

The screenshot shows the 'Certificate Management' tab selected in a navigation bar. Below it, the 'Manage Verification Certificates' section is highlighted. At the bottom left, there is a blue 'Import...' button.

6104

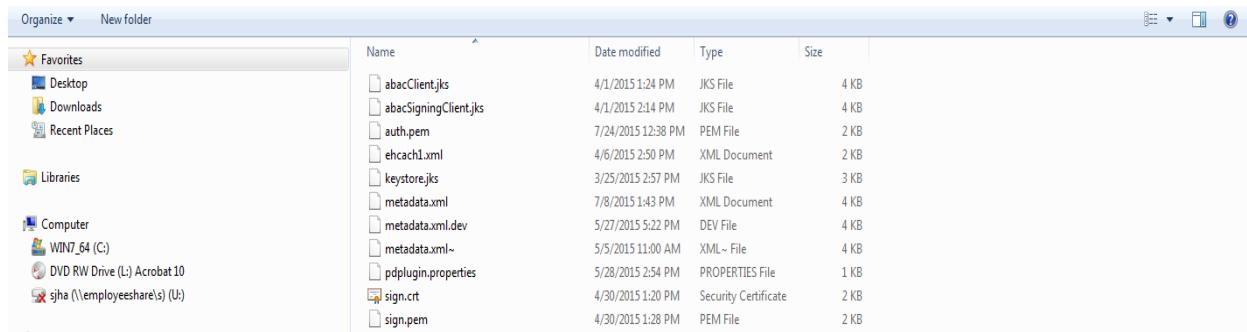
5. Click **Choose File**.

SECOND DRAFT

The screenshot shows a software interface with a top navigation bar containing tabs: Main, SP Connections, SP Connection, Credentials, Back-Channel Authentication, Certificate Management, and Import Certificate. The Import Certificate tab is selected. Below the tabs, there are two buttons: 'Import Certificate' and 'Summary'. A message box says 'Please select the file containing the desired certificate.' A 'Filename' field contains 'Choose File' and 'No file chosen'. The background shows a Windows-style file explorer window.

6106

- 6107 6. Select your certificate file from the Explorer window.



6108

- 6109 7. The file name will appear in the **Filename** field.

The screenshot shows the same software interface as the first one, but the 'Import Certificate' tab is now active. It displays a message 'Please select the file containing the desired certificate.' and a 'Filename' field with 'Choose File' and 'auth.pem'. The background shows a Windows-style file explorer window.

6110

- 6111 8. Click **Next**. This will display details of parts of certificate.

6112

9. Check **Make this the active certificate** and click **Done**.

The screenshot shows the 'Import Certificate' interface. At the top, it says 'Summary information for your new certificate. Select the checkbox to make this new certificate the active certificate. Unselecting the checkbox preserves the current active certificate.' Below this, there is a checked checkbox labeled 'Make this the active certificate'. The main area is titled 'Import Certificate' and contains a 'IMPORT CERTIFICATE' section. It shows the following details:

Filename	auth.pem
File Size	1764
Subject DN	CN=MM1955, OU=ABAC, O=NCCoE, ST=Maryland, C=US
Serial Number	1002
Expires	Thu Mar 31 13:19:27 EDT 2016

6113

- 6114 10. Verify the certificate.

SECOND DRAFT

This screenshot shows the 'Manage Verification Certificates' section within the 'SP Connection' tab. It displays a table of certificates with columns for SERIAL, SUBJECT DN, EXPIRES, KEY DETAILS, STATUS, ACTIVE, and ACTION. A single certificate is listed:

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTIVE	ACTION
10:02	CN=MM195592-PC, OU=ABAC, O=NCCoE, ST=Maryland, C=US	Thu Mar 31 13:19:27 EDT 2016	RSA 2048	Valid	<input checked="" type="checkbox"/>	Activate - Certificate already active Export Delete - Certificate in use

6115

6116 11. Under **Action**, select **Activate**.

This screenshot shows the 'Certificate Verification Method' section within the 'SP Connection' tab. It includes tabs for Inbound Authentication Type, Certificate Verification Method, SSL Verification Certificate, and Summary. The 'SSL Verification Certificate' tab is selected, showing a dropdown menu with the option '10:03 (cn=MM195592-PC) *'. Below the tabs is a 'Manage Certificates...' button.

6117

6118 12. View a **Summary** of the verification.

This screenshot shows the 'Summary' section within the 'SP Connection' tab. It includes tabs for Inbound Authentication Type, Certificate Verification Method, SSL Verification Certificate, and Summary. The 'SSL Verification Certificate' tab is selected, showing a note 'Click a heading link to edit a configuration setting'. Below the tabs are sections for INBOUND AUTHENTICATION TYPE (Authentication Type: SSL Client Certificate), CERTIFICATE VERIFICATION METHOD (Cert Verification Method: Unanchored), and SSL VERIFICATION CERTIFICATE (Selected Certificate: CN=MM195592, OU=ABAC, O=NCCoE, ST=Maryland, C=US).

6119

6120 13. Return to the **Back Channel Authentication** tab.

This screenshot shows the 'Digital Signature Settings' section within the 'Back-Channel Authentication' tab. It includes tabs for Back-Channel Authentication, Digital Signature Settings, Signature Verification Settings, and Summary. The 'Digital Signature Settings' tab is selected, showing a note 'You selected one or more bindings that require additional security for communication with your partner. Please ensure that security settings are properly configured.' Below the tabs are sections for 'Receive from your partner' (Configure button) and 'Attribute Query requests'.

6121

6122 14. Select **Digital Signature Settings** for outgoing messages, then click **Next**.

This screenshot shows the 'Digital Signature Settings' section within the 'Back-Channel Authentication' tab. It includes tabs for Back-Channel Authentication, Digital Signature Settings, Signature Verification Settings, and Summary. The 'Digital Signature Settings' tab is selected, showing a note 'You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.' Below the tabs are sections for 'Signing Certificate' (a dropdown menu with '- SELECT -'), 'Include the certificate in the signature <KeyInfo> element' (checked), and 'Include the raw key in the signature <KeyValue> element' (unchecked). At the bottom is a 'Manage Certificates...' button.

6123

6124 15. Go to **Digital Signature settings**. Click **Configure**.

SECOND DRAFT

The screenshot shows the 'Digital Signature Settings' tab selected in a navigation bar. A dropdown menu for 'Signing Certificate' is open, showing '01:4C:09:4C:8D:9B (cn=demo-idp-enc)' as the selected item. There are two checkboxes below it: 'Include the certificate in the signature <KeyInfo> element.' (checked) and 'Include the raw key in the signature <KeyValue> element.' Below that, a dropdown for 'Signing Algorithm' is set to 'RSA SHA256'. At the bottom left is a 'Manage Certificates...' button.

6125

16. Select **Digital Signature Settings** on incoming messages.

The screenshot shows the 'Signature Verification Settings' tab selected in a navigation bar. A note at the top says 'Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.' Below is a 'Manage Signature Verification Settings...' button.

6127

17. Click on **Manage Signature Verification Settings**.

The screenshot shows the 'Signature Verification' tab selected in a navigation bar. Under 'Trust Model', there are two radio buttons: 'Anchored' (selected) and 'Unanchored'. A note at the top says 'Select the Trust Model to be used for verifying digital signatures received from this partner.'

6129

18. Select the certificate(s) to use when verifying these digital signatures. When multiple certificates are chosen, each certificate is tried from the top of the list down until the signature is verified. It is assumed that signed certificates have already been imported. If not, click on **Manage Certificate** and complete the steps detailed earlier for importing a certificate.

The screenshot shows the 'Signature Verification' tab selected in a navigation bar. Under 'Primary', a dropdown shows '10:02 (cn=MM195592-PC)'. Under 'Secondary', another dropdown shows '10:03 (cn=MM195592-PC)'. A note at the top says 'Please select the certificate(s) to use when verifying these digital signatures. When multiple certificates are chosen, each certificate is tried from the top of the list down until the signature is verified.'

6134

19. Verify the **Summary**.

SECOND DRAFT

The screenshot shows the 'Signature Verification' tab selected in a navigation bar. Below it, a summary message reads: 'Summary information for your Signature Verification configuration. Click a heading link to edit a configuration setting.' Under the 'SIGNATURE VERIFICATION CERTIFICATE' section, there are two tabs: 'Primary Certificate' and 'Secondary Certificate'. The Primary Certificate tab displays the details: CN=MM1955, OU=ABAC, O=NCCoE, ST=Maryland, C=US. The Secondary Certificate tab displays the details: CN=MM1955, OU=ABAC, O=NCCoE, ST=Maryland, C=US.

6136

6137 20. This completes the signature verification credential settings.

The screenshot shows the 'Signature Verification Settings' tab selected in a navigation bar. Below it, a summary message reads: 'Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.' Under the 'Digital Signature Settings' section, there is a link: 'Manage Signature Verification Settings...'. The 'Back-Channel Authentication' section is also visible.

6138

6139 21. Verify the **Summary**.

The screenshot shows the 'Credentials' tab selected in a navigation bar. Below it, a summary message reads: 'Summary information for your Credentials configuration. Click a heading link to edit a configuration setting.' Under the 'INBOUND AUTHENTICATION TYPE' section, 'Authentication Type' is set to 'SSL Client Certificate'. Under the 'CERTIFICATE VERIFICATION METHOD' section, 'Cert Verification Method' is set to 'Unanchored'. Under the 'SSL VERIFICATION CERTIFICATE' section, 'Selected Certificate' is EMAILADDRESS=sjha@MM195592-PC.org, CN=MM195592-PC, OU=ABAC, O=NCCoE, ST=Maryland, C=US. Under the 'DIGITAL SIGNATURE SETTINGS' section, 'Selected Certificate' is CN=demo-idp-enc, O=NCCoE, C=US. 'Include Certificate in KeyInfo' is set to 'true', 'Include Raw Key in KeyValue' is set to 'false', and 'Selected Signing Algorithm' is RSA SHA256. Under the 'Signature Verification' section, the 'TRUST MODEL' is 'Unanchored'. Under the 'SIGNATURE VERIFICATION CERTIFICATE' section, both 'Primary Certificate' and 'Secondary Certificate' are listed with the same details: EMAILADDRESS=sjha@MM195592-PC.org, CN=MM195592-PC, OU=ABAC, O=NCCoE, ST=Maryland, C=US.

6140

6141 22. **Activate** the connection and **Save**.

SECOND DRAFT

The screenshot shows the 'SP Connection' configuration page. At the top, there are tabs for Main, SP Connections, and SP Connection. Under SP Connection, there are sub-tabs: Connection Type, Connection Options, Import Metadata, Metadata Summary, General Info, Attribute Query, Credentials, and Activation & Summary. The 'Activation & Summary' tab is currently selected. A summary message at the top says: "Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting." Below this, there are sections for Connection Status (Active), Connection Type (SP), and various configuration parameters like Browser SSO Profiles, Protocol (SAML 2.0), and Connection Template (No Template). There are also sections for Connection Options (Browser SSO, IdP Discovery, Attribute Query) and Import Metadata (Metadata File: unsigned). The General Info section contains partner details: Partner's Entity ID (Connection ID): urn:nccoe:abac:plugin1, Base URL: http://10.33.7.8:8080, Company: The National Cybersecurity Center of Excellence, Contact Name: John Smith, Contact Number: +1 (240) 314-6800, and Contact Email: john.smith@nccoe.nist.gov. The Attribute Query section lists retrievable attributes: clearance and division.

6142

6143 23. Save again.

The screenshot shows the 'Manage Connections' page under the 'SP Connections' tab. It displays a table of existing connections. The columns are: CONNECTION NAME, CONNECTION ID, VIRTUAL ID, PROTOCOL, STATUS, and ACTION. The table contains five rows:

CONNECTION NAME	CONNECTION ID	VIRTUAL ID	PROTOCOL	STATUS	ACTION
Demo SP	FF-DEMO		SAML2.0	Active	Delete Copy Export Connection Export Metadata
https://rp.abac.test:9031	https://rp.abac.test:9031		SAML2.0	Inactive	Delete Copy Export Connection Export Metadata
urn:nccoe:abac:plugin	urn:nccoe:abac:plugin		SAML2.0	Inactive	Delete Copy Export Connection Export Metadata
urn:nccoe:abac:plugin1	urn:nccoe:abac:plugin1		SAML2.0	Active	Delete Copy Export Connection Export Metadata
urn:nccoe:abac:rp	urn:nccoe:abac:rp	urn:nccoe:abac:idp	SAML2.0	Active	Delete Copy Export Connection Export Metadata

At the bottom of the page, there are buttons for 'Create Connection...' and 'Import Connection'. A 'Logging Mode Override' section with radio buttons for 'Off' and 'On' is also present.

6144

6145 *10.8.2.2 IDP Connection*

6146 As an SP, you are making a connection to a partner IdP. Follow these steps to select the type of connection needed for this IdP:
6147

- 6148 1. On the righthand side of the administrative console, click **Manage All IdP** under **IdP Connections**.
- 6149

The screenshot shows the 'SP Configuration' interface. Under 'APPLICATION INTEGRATION SETTINGS', there are links for Adapters, Target URL Mapping, Default URLs, and Application Endpoints. Under 'FEDERATION SETTINGS', there is a link for Protocol Endpoints. In the 'IDP CONNECTIONS (2)' section, two SAML2.0 connections are listed: 'https://idp.abac...' and 'urn:nccoe:abac:idp'. Below these are links for 'Manage All IdP', 'Create New', and 'Import'.

6150

- 6151 2. Open the connection that was created in [Section 6](#). Click on **Connection Option**. It my default to
6152 **Browser SSO**. Additionally, select **Attribute Query** and **JIT Provisioning**.

The screenshot shows the 'IdP Connection' configuration page. The 'Connection Type' tab is selected, showing 'Connection Options' and other tabs like Import Metadata, General Info, Browser SSO, Attribute Query, JIT Provisioning, Credentials, Activation & Summary. A note says 'Please select options that apply to this connection.' with checkboxes for Browser SSO, JIT Provisioning, OAuth Attribute Mapping, and Attribute Query, all of which are checked.

6153

- 6154 3. Click **Next**. Verify that the information in the **General Info** tab is correct.

SECOND DRAFT

6155

6156 4. Click **Next**.

6157

6158 5. Click on **Configure Attribute Query Profile**.

6159

6160 6. Specify an **Attribute Authority Service URL**.

6161

SECOND DRAFT

- 6162 7. Attributes requested by your application may not match exactly the attributes supplied by the
6163 IdP. Specify the mapping between these sets of attributes.

The screenshot shows the 'Attribute Name Mapping' tab selected within the 'Attribute Query' section of a web-based configuration tool. At the top, there are tabs for Main, IdP Connections, IdP Connection, Attribute Query, Attribute Request Service URL, Attribute Name Mapping, Security Policy, and Summary. A status message at the top indicates: 'Attributes requested by your application may not match exactly the attributes supplied by the IdP. Specify the mapping between these sets of attributes.' Below this, there is a table with columns for LOCAL NAME, REMOTE NAME, and ACTION. There is one row in the table with empty fields and an 'Add' button.

6164

- 6165 8. Select **Sign the Attribute Query**.

The screenshot shows the 'Security Policy' tab selected within the 'Attribute Query' section. At the top, there are tabs for Main, IdP Connection, Attribute Query, Attribute Request Service URL, Attribute Name Mapping, Security Policy, and Summary. A status message at the top indicates: 'Specify the attribute authority profile's security policy with your partner.' Below this, there is a list of checkboxes for security policies:

- Require signed Response
- Require signed Assertion
- Require encrypted Assertion
- Sign the Attribute Query
- Encrypt the Name Identifier
- Mask attributes in log files

6166

- 6167 9. Verify that the **Summary** is correct, then click **Done**.

The screenshot shows the 'Summary' tab selected within the 'Attribute Query' section. At the top, there are tabs for Main, IdP Connection, Attribute Query, Attribute Request Service URL, Attribute Name Mapping, Security Policy, and Summary. A status message at the top indicates: 'Click a heading link to edit a configuration setting.' Below this, there is a summary table:

Attribute Query	
ATTRIBUTE REQUEST SERVICE URL	
Endpoint URL	https://rp.abac.test:8443/fidp/attrsvc.ssaml2
ATTRIBUTE NAME MAPPING	
SECURITY POLICY	
Require signed Response	false
Require signed Assertion	true
Require encrypted Assertion	false
Sign the Attribute Query	true
Encrypt the Name Identifier	false
Mask attributes in log files	false

6168

- 6169 10. When the following screen appears, click **Next**.

The screenshot shows the 'JIT Provisioning' tab selected within the 'IdP Connection' section. At the top, there are tabs for Main, IdP Connection, Connection Type, Connection Options, General Info, Browser SSO, Attribute Query, JIT Provisioning, Credentials, and Activation & Summary. A status message at the top indicates: 'The Attribute Query Profile supports local applications in requesting user attributes from an Attribute Authority. Click the button below to configure the necessary settings to support this profile.' Below this, there is a button labeled 'Configure Attribute Query Profile'.

6170

- 6171 11. JIT provisioning details have been provided by PingFederate [here](#).

6172 12. **Save** the configuration.

6173 13. Select **Application Authentication**.

CERTIFICATE MANAGEMENT

- Trusted CAs
- SSL Server Certificates
- SSL Client Keys & Certificates
- Digital Signing & XML Decryption Keys & Certificates
- Certificate Revocation Checking

AUTHENTICATION

- Application Authentication
- Password Credential Validators
- Active Directory Domains/Kerberos Realms

IDP-TO-SP BRIDGING

- Adapter-to-Adapter Mappings
- Connection Mapping Contracts

6174

SERVICE	ID	SHARED SECRET	CONFIRM SHARED SECRET	ACTION
Attribute Query	Attribute Query	heuristics	heuristics	Activate
JMX	JMX	heuristics	heuristics	Activate
Connection Management	Connection Management	heuristics	heuristics	Activate
SSO Directory Service	heuristics	heuristics	heuristics	Deactivate

6175

6176 14. Enter **appid** in the **ID** field, and use the shared secret that you input during custom data store configuration, then save the configuration.

6177

6178 15. Select **Browser SSO** and **Attribute Query**.

6179 **10.9 ApacheDS Schema Extension**

6180 At a high level, LDAP Schema is the collection of attribute type definitions, object class definitions, and
6181 other information which a server uses to determine how to match a filter or attribute value assertion (in
6182 a compare operation) against the attributes of an entry, and whether to permit add and modify
6183 operations. For a more formal definition, look into Section 4.1 of [RFC 4512](#).

6184 ApacheDS comes with a comprehensive set of predefined, standardized schema elements. Specification
6185 of many of these elements can be found in [RFC 4519](#). Generally, these predefined schema satisfy most

6186 of the needs of a project. However, you may sometimes be required to define additional attributes or
6187 object classes that are not included in the server provided schema.

6188 Each attribute and object class has an associated unique Object Identifier. Generally, An Object
6189 Identifier is a tree of nodes where each node is simply a sequence of digits. The rules roughly state that
6190 once an entity is assigned a node in the Object Identifier (OID) tree, it has sole discretion to further
6191 delegate sub-trees off of that node. Some examples of OIDs include: 1.3.6.1 - the Internet OID,
6192 1.3.6.1.4.1 - IANA-assigned company OIDs. It is formally defined using the ITU-T's ASN.1 standard, X.690.

6193 The IANA OID registry contains a list of registered entities that use OIDs to reference internal structures.
6194 In this section, we have used OIDs that are not registered anywhere. For this reason, we are using the
6195 subtree 2.25, as per recommendation by [ITU](#). UUID is generated by the program found [here](#).

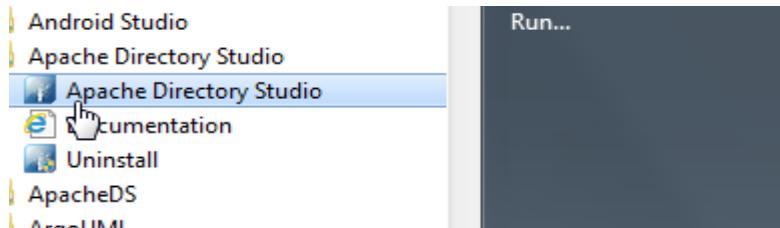
6196 In the following section, we will demonstrate how to create an attribute. Similar procedures can be used
6197 to create many attributes and object classes.

6198 [10.9.1 Pre-Requisites](#)

6199 For Schema extension, this project used ApacheDS studio. ApacheDS installation and configuration is
6200 detailed in [Section 10.6](#) of this guide.

6201 [10.9.2 Procedure](#)

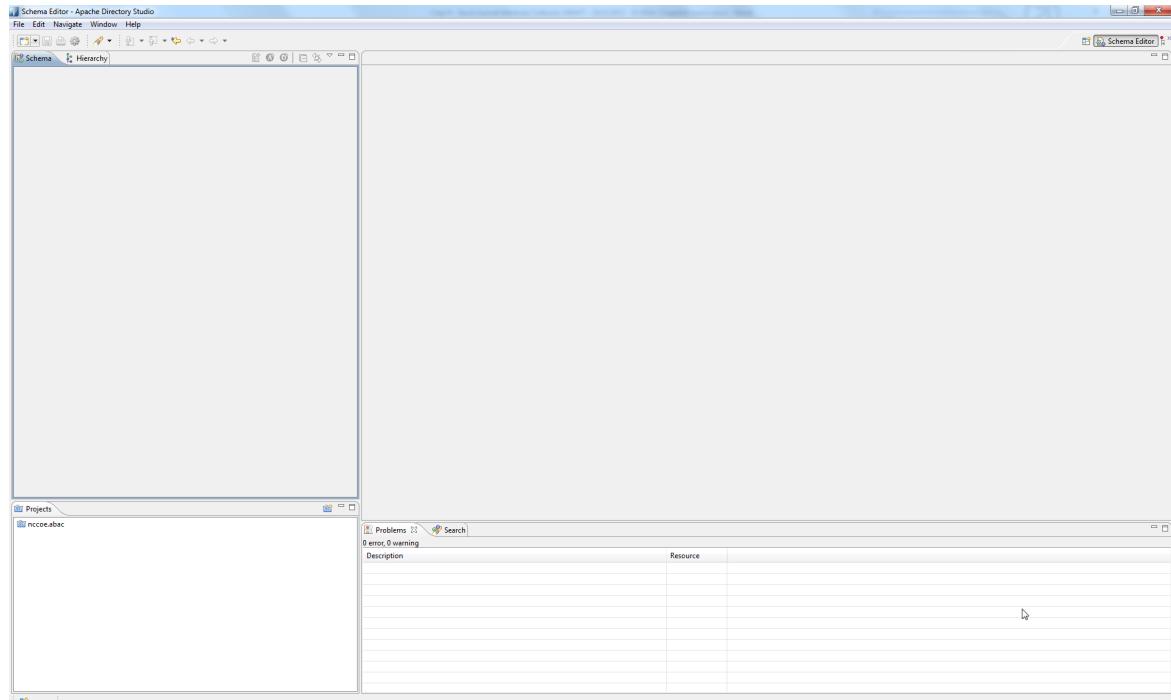
6202 1. Start ApacheDS Studio from the Start menu.



6203

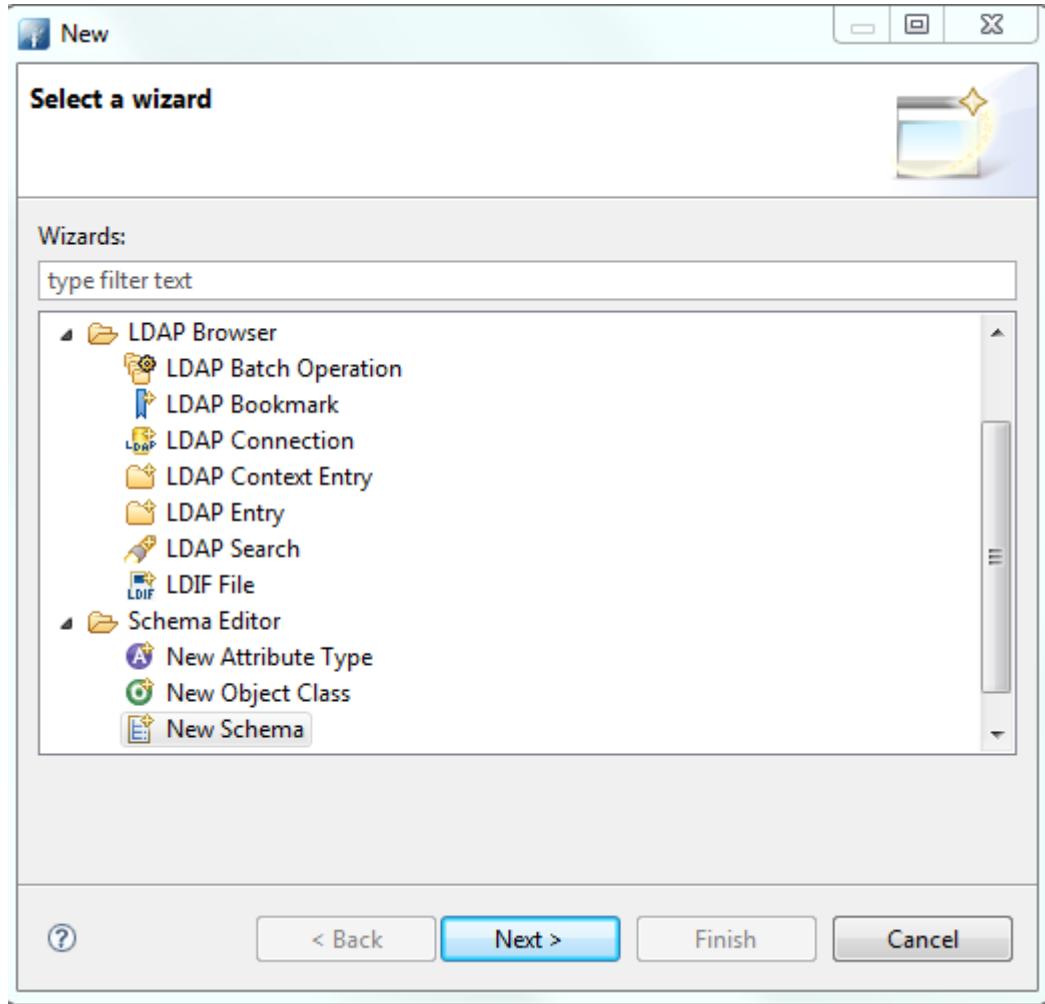
6204 2. The following screen will appear:

SECOND DRAFT



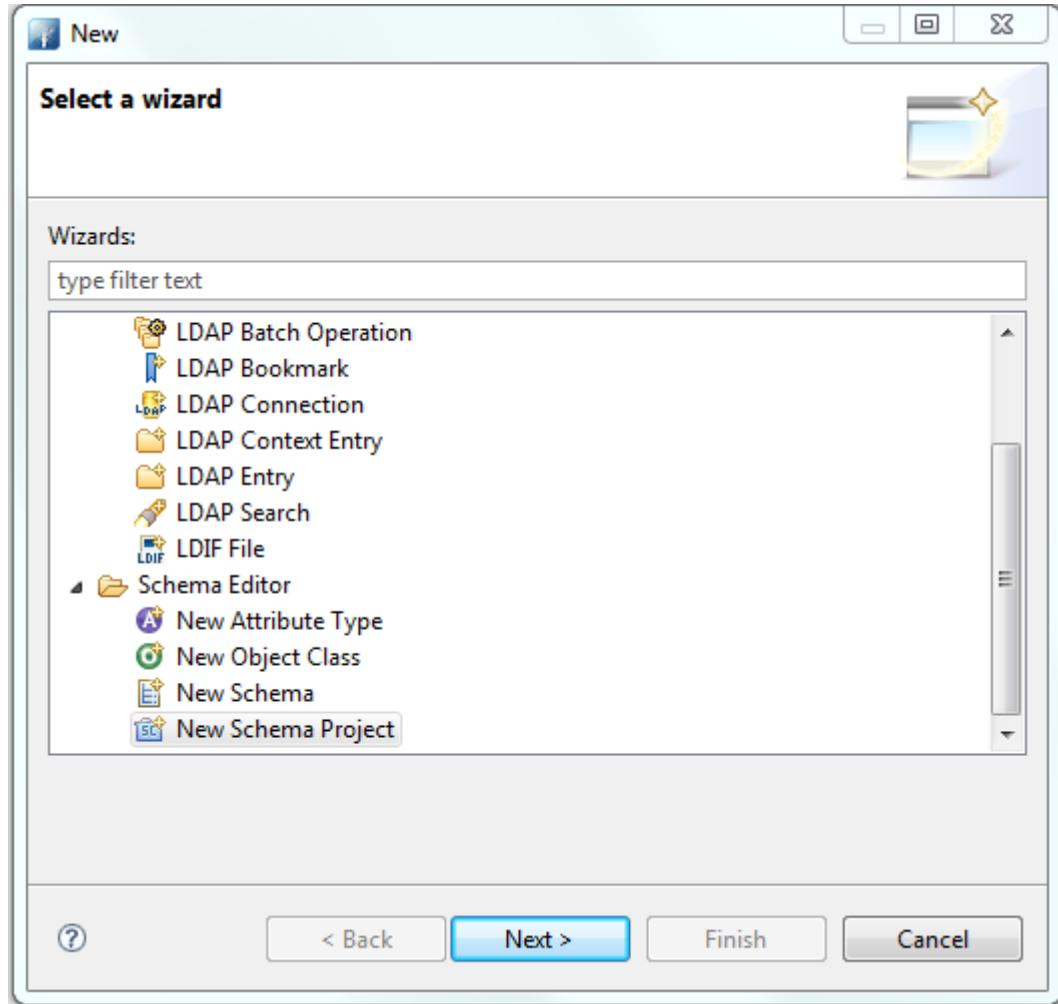
6205

6206 3. Select **File > New**.



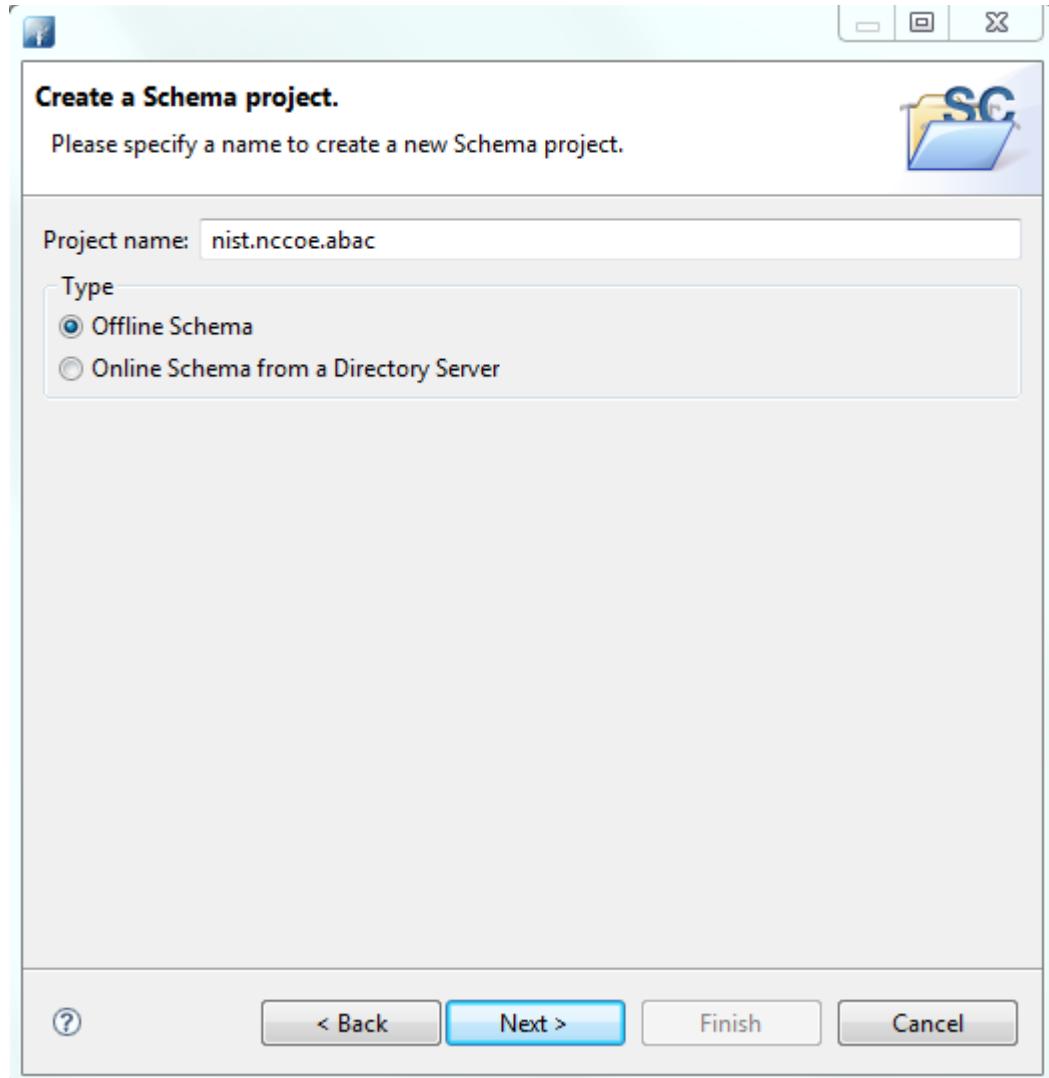
6207

6208 4. Select the **New Schema Project** wizard.



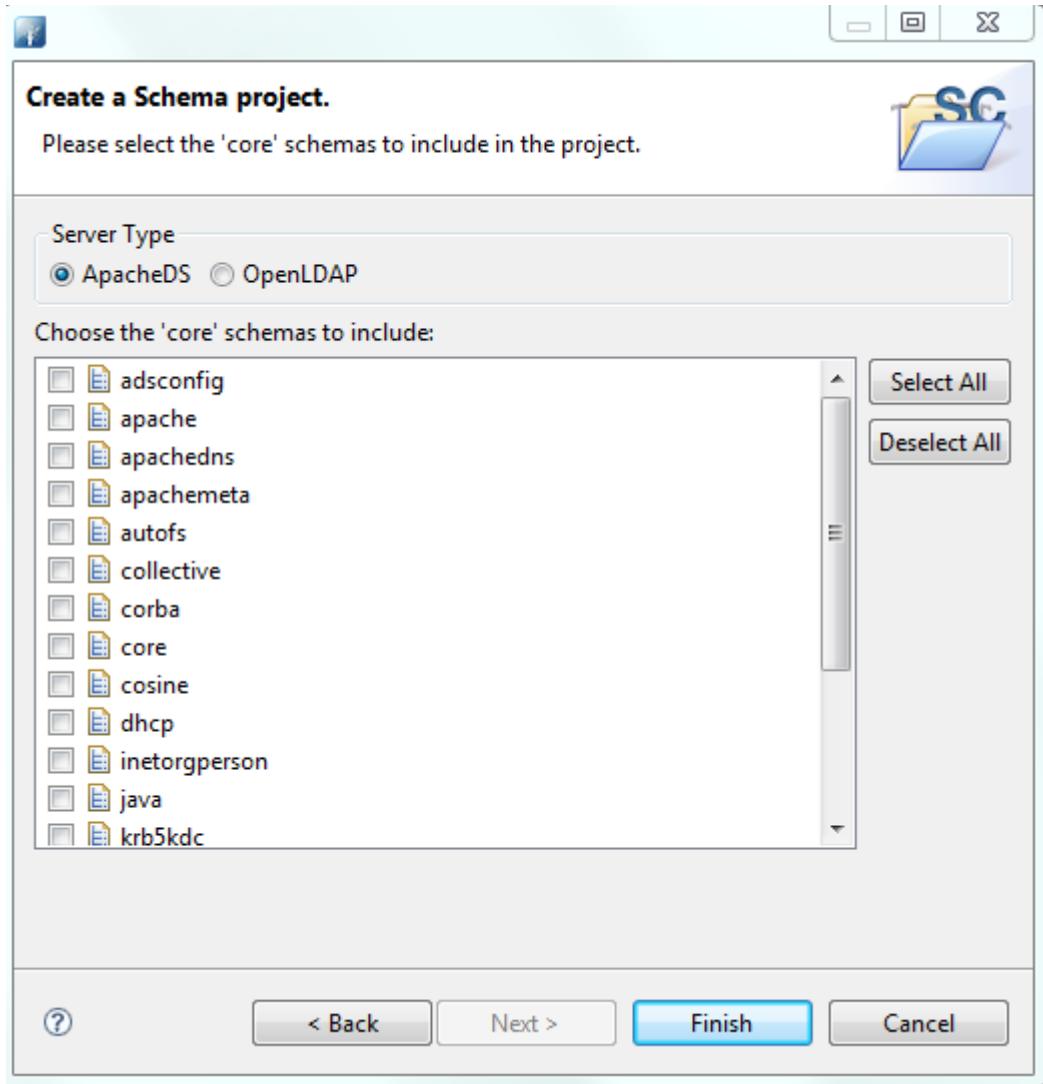
6209

6210 5. Specify a **Project name**, i.e., **nist.nccoe.abac** in our build.



6211

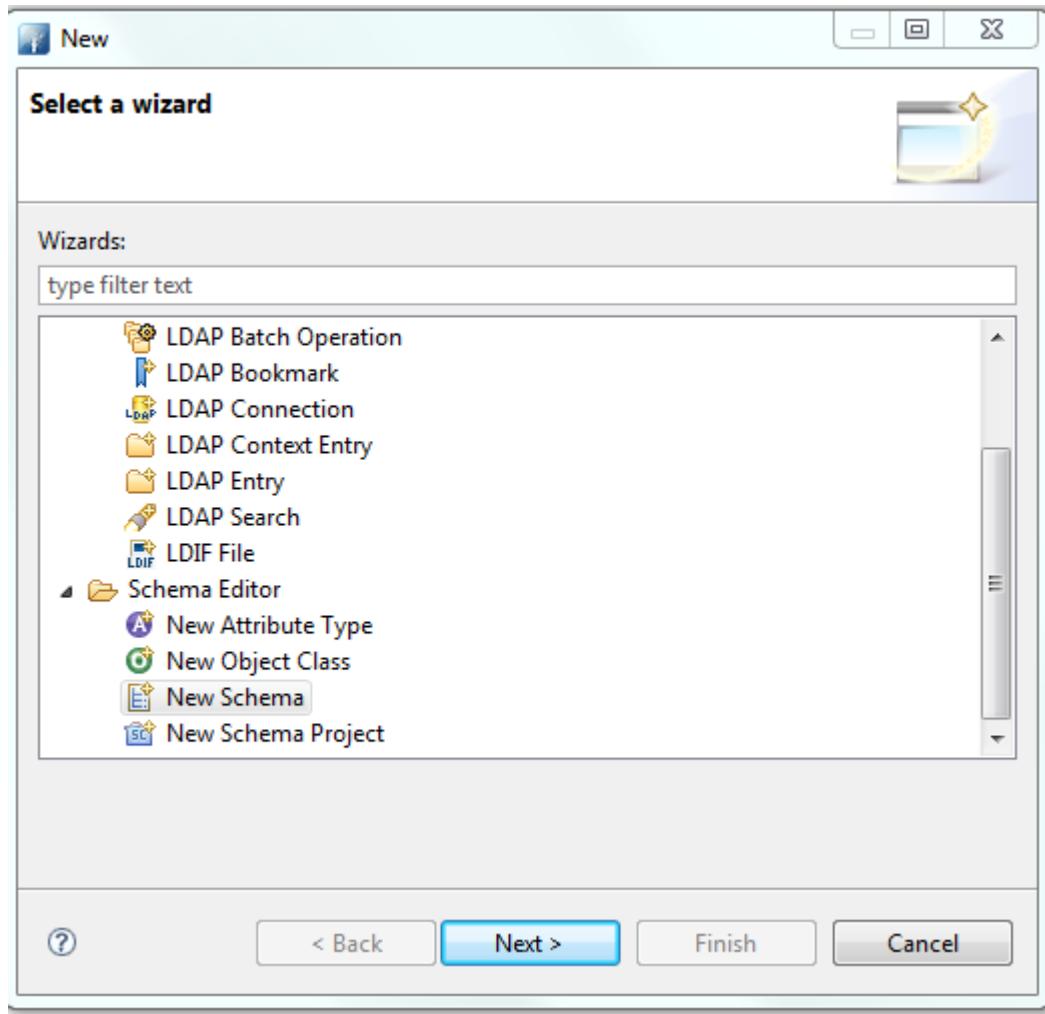
- 6212 6. Select **Offline Schema**, then click **Next**. On the next screen, **Choose the 'core' schemas to include**.
- 6213



6214

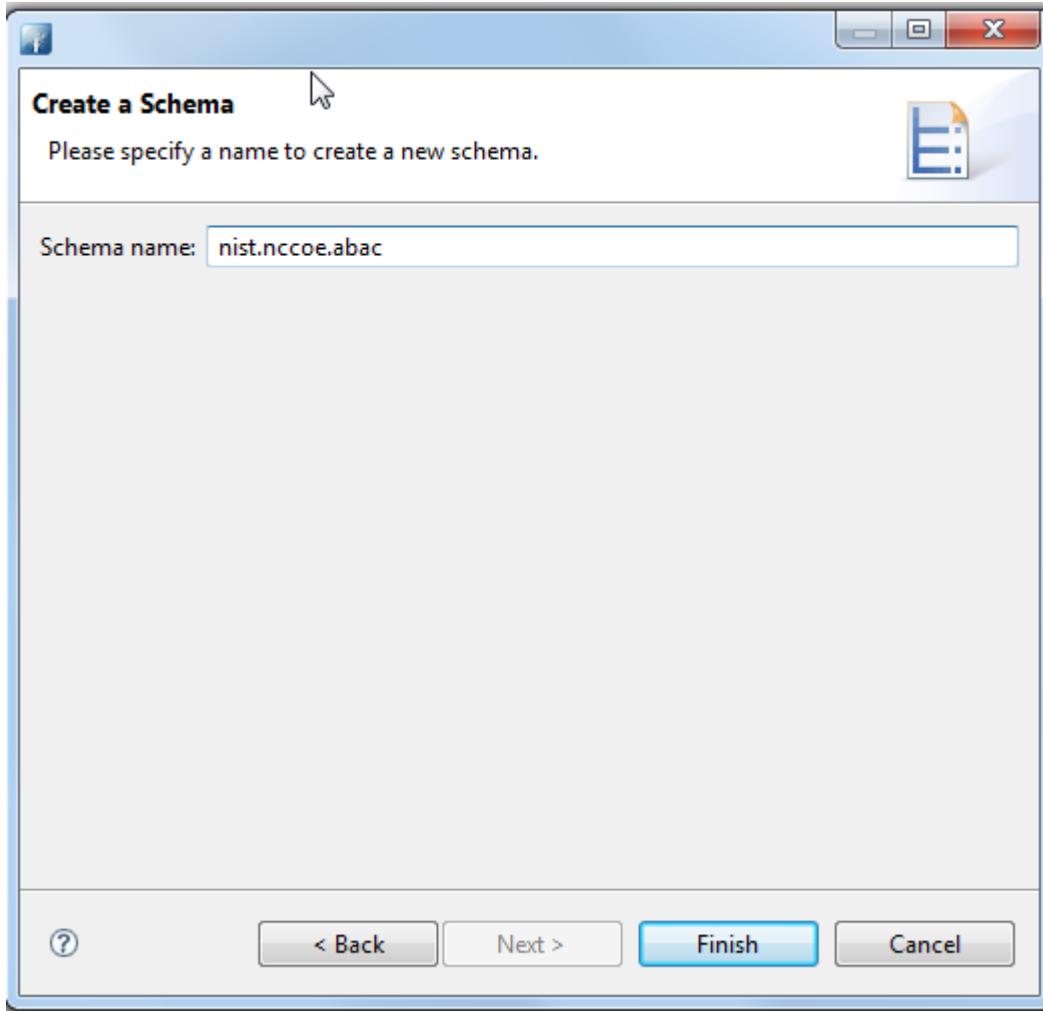
6215

7. Click **File > New** and select **New Schema**.



6216

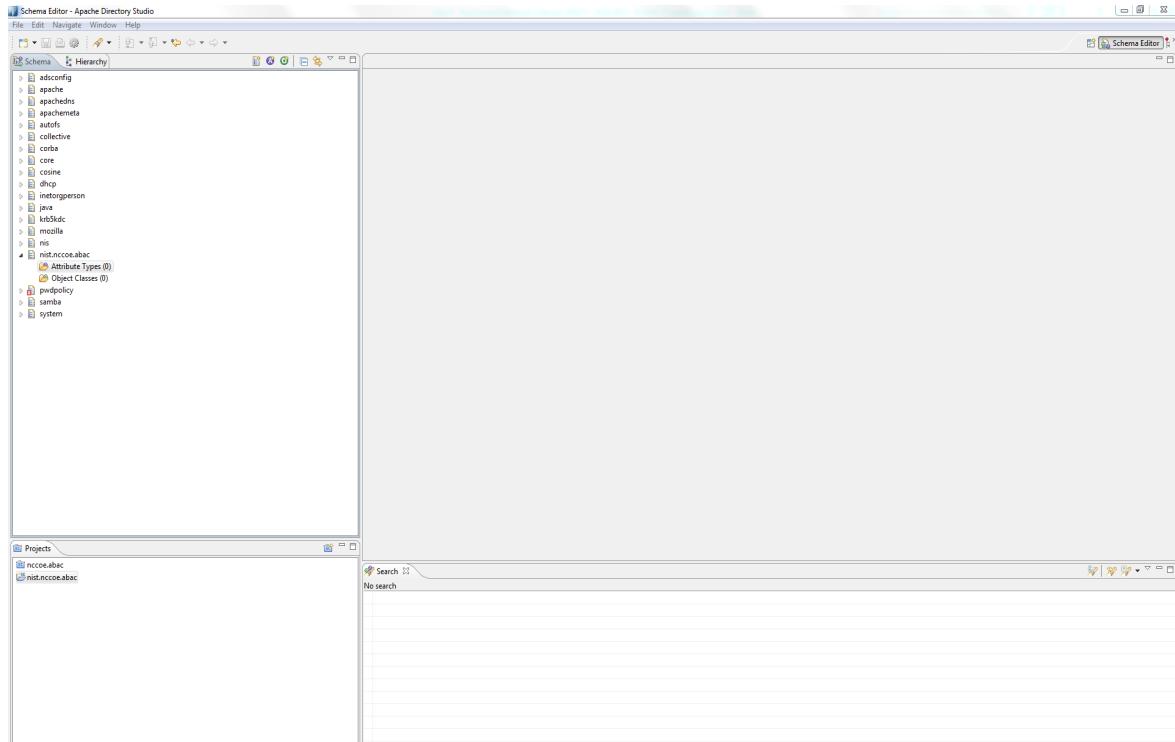
6217 8. Specify a **Schema name**, i.e., **nist.nccoe.abac** in our build.



6218

6219 9. The following screen will appear:

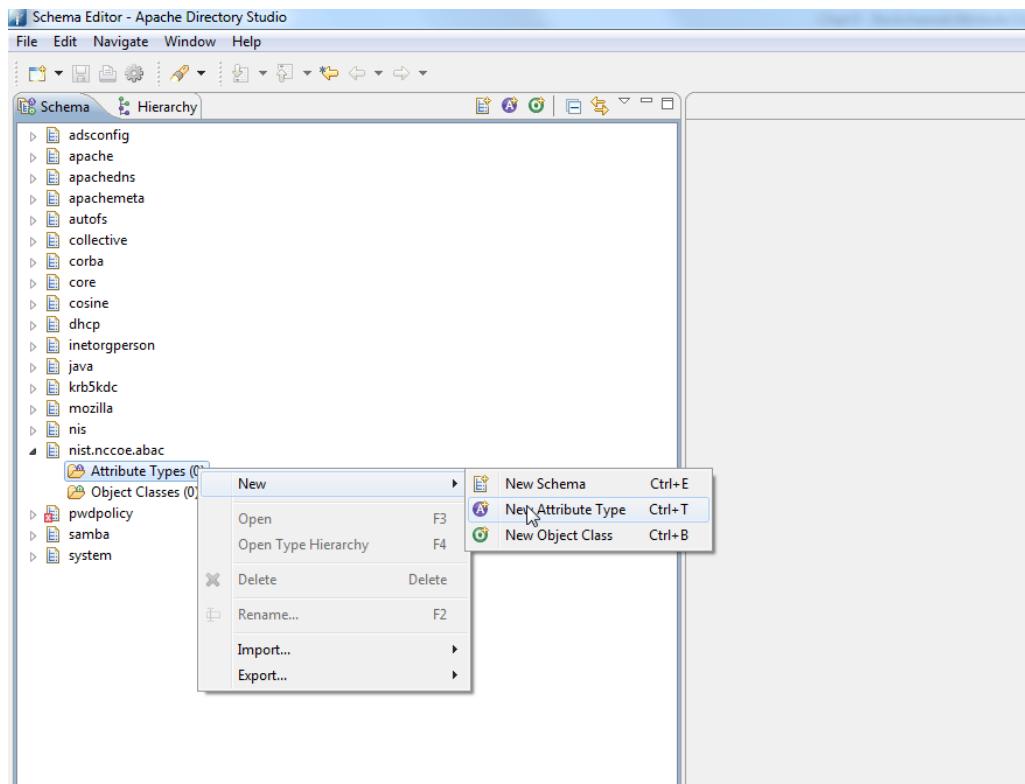
SECOND DRAFT



6220

6221

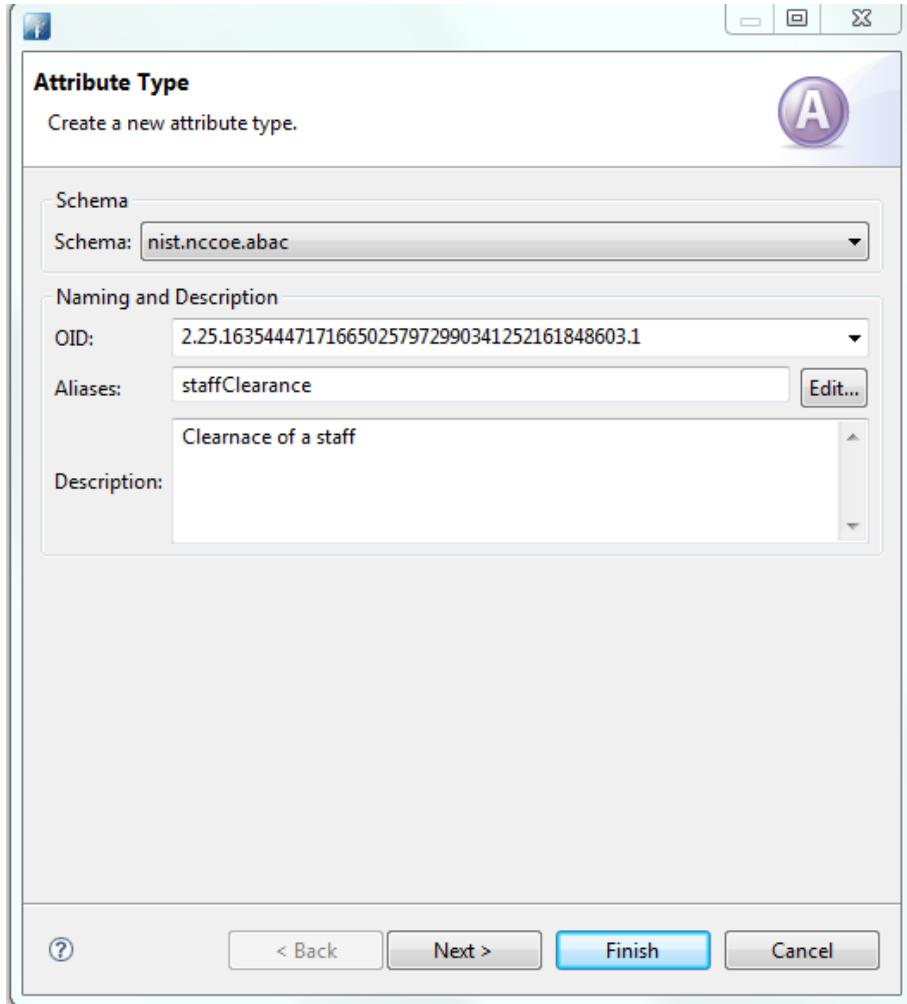
10. Select **Attribute Types** > **New** > **New Attribute Type**.



6222

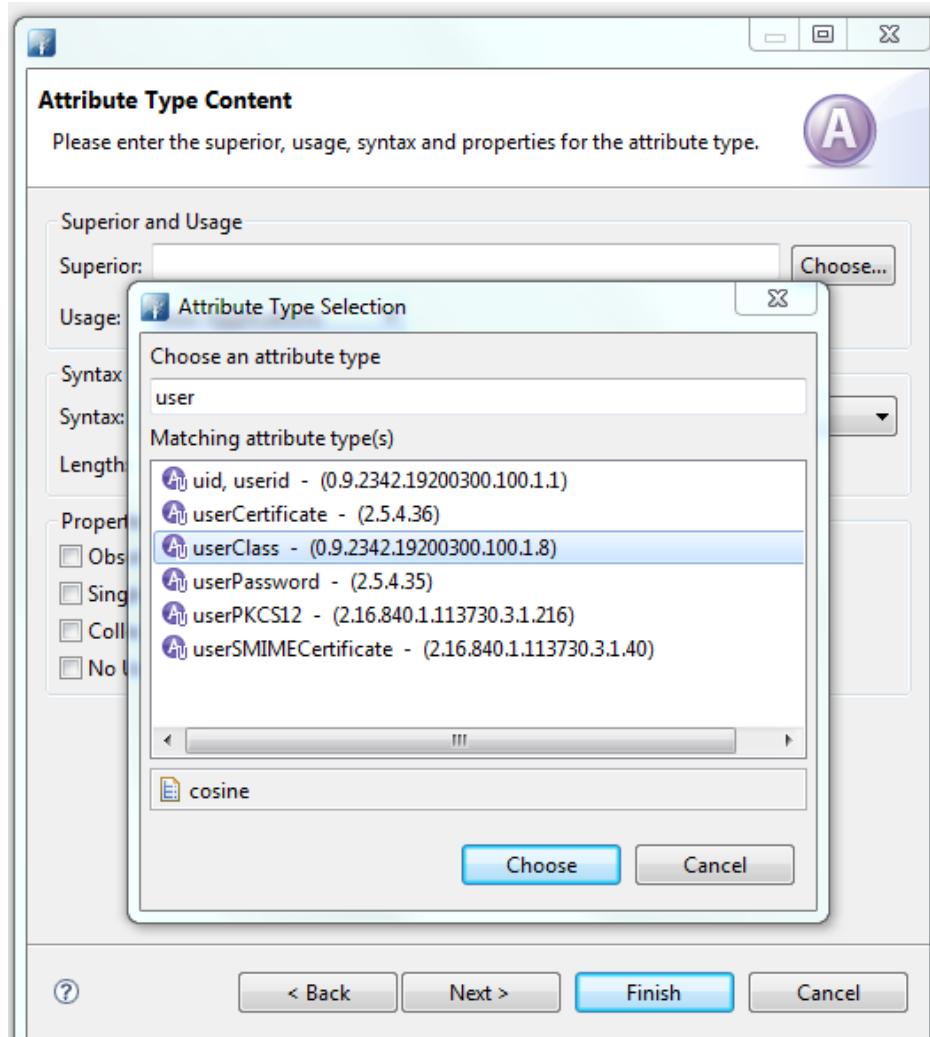
6223

11. In the new window, choose the **OID** from the previous instructions.



6224

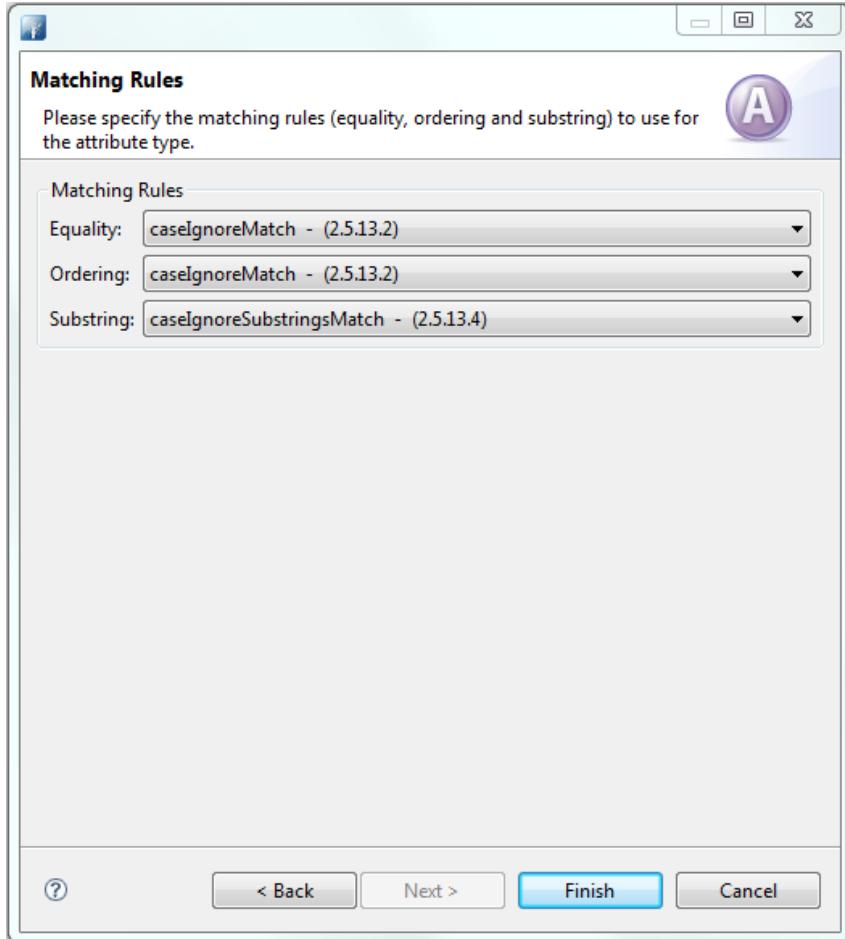
6225 12. Click **Next** to choose the superior type of this attribute.



6226

6227

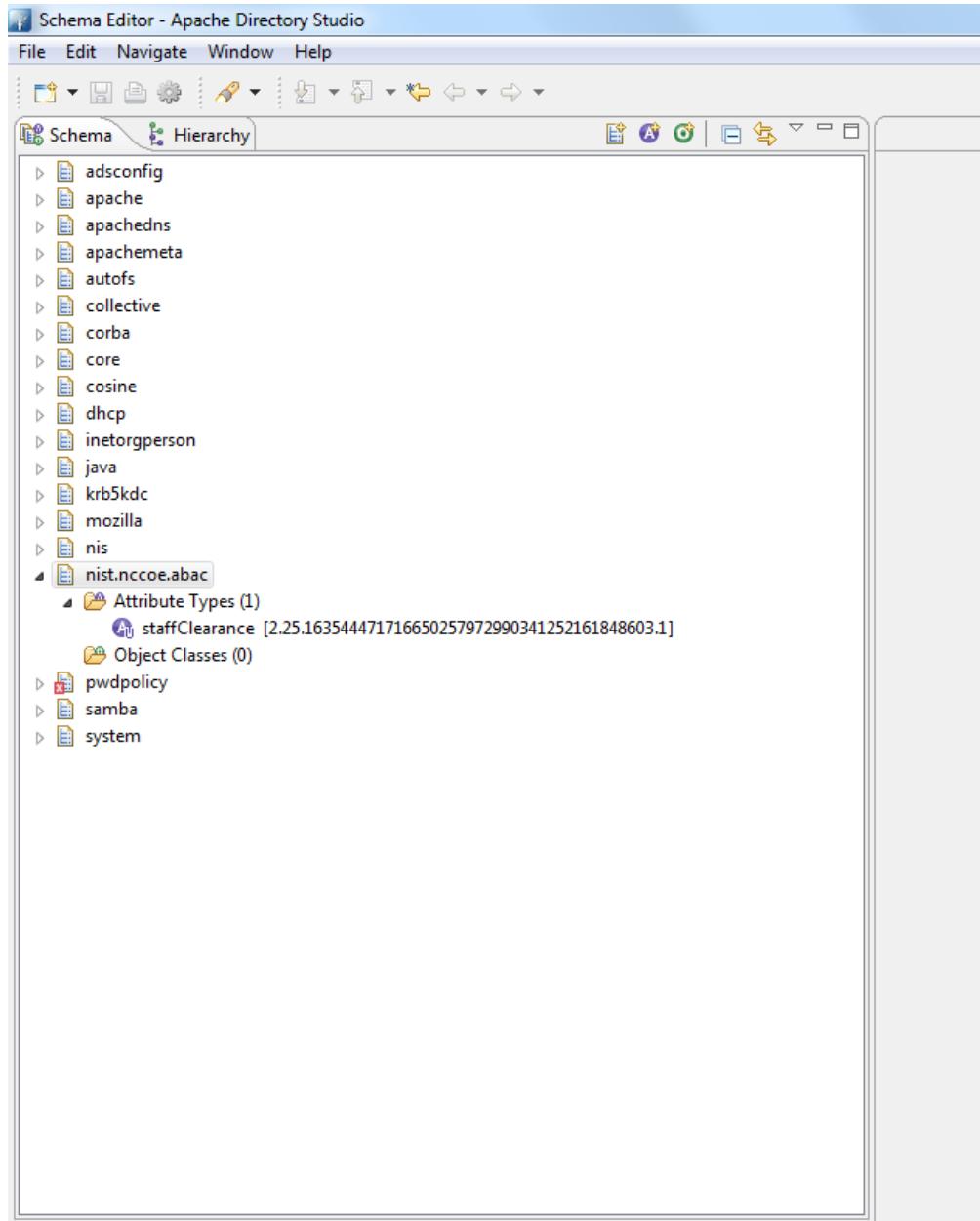
13. Specify **Matching Rules**. Since it is a string, case insensitivity is chosen in our build.



6228

6229 14. The following screen will appear:

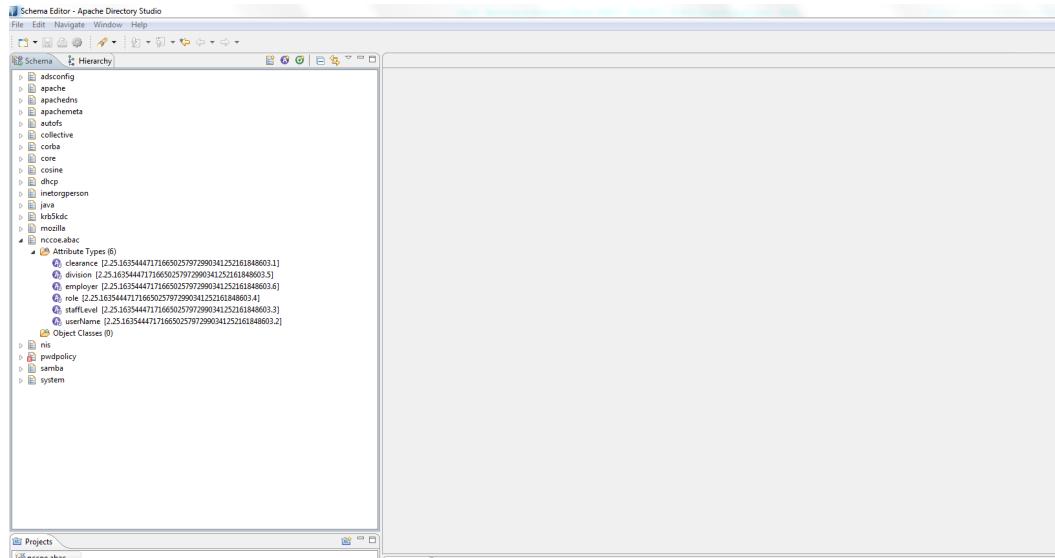
SECOND DRAFT



6230

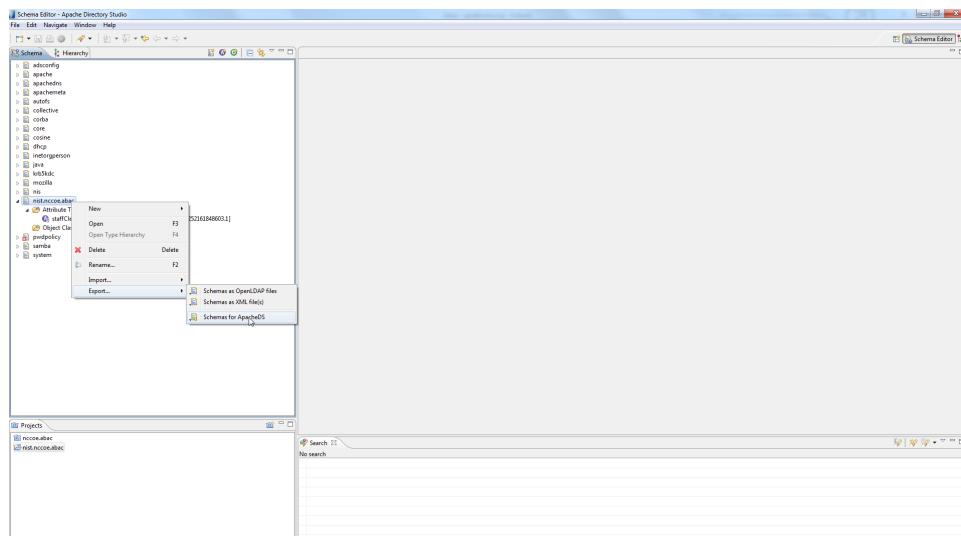
6231 15. You can create other attributes by following process described above.

SECOND DRAFT



6232

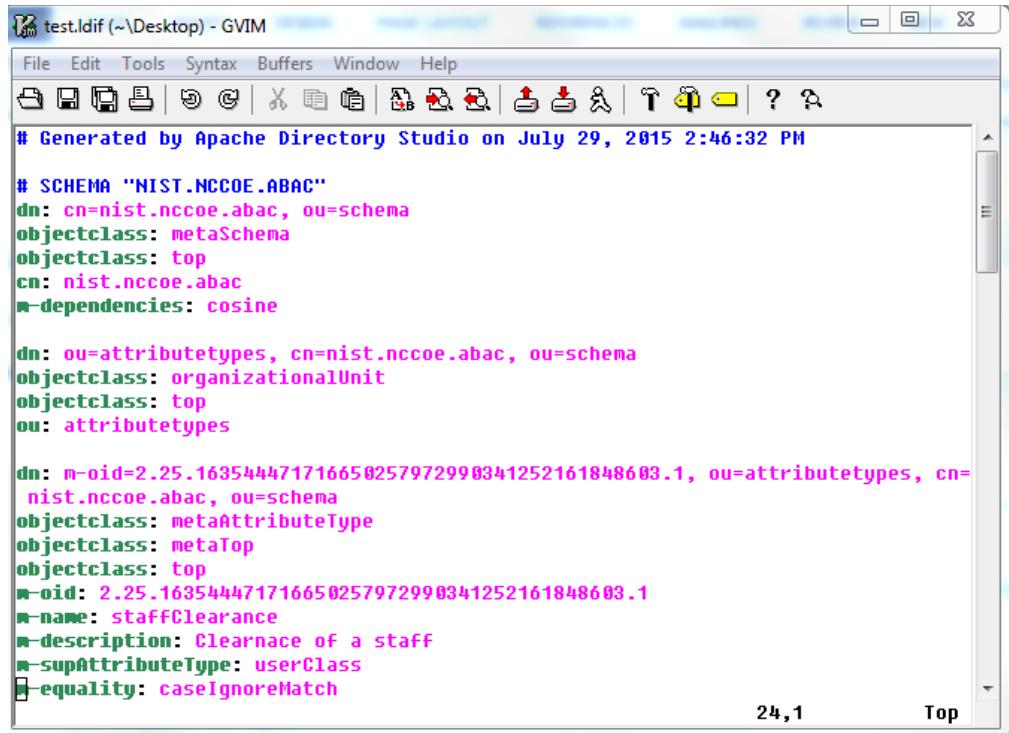
6233 16. Export the schema by selecting **Export > Schemas for ApacheDS**. It will create an LDIF file.



6234

6235 17. LDIF files are specified by their own RFC. In a text editor, it displays as following:

SECOND DRAFT



The screenshot shows a GVIM window titled "test.ldif (~\Desktop) - GVIM". The window contains an LDIF file with the following content:

```
# Generated by Apache Directory Studio on July 29, 2015 2:46:32 PM

# SCHEMA "NIST.NCCOE.ABAC"
dn: cn=nist.nccoe.abac, ou=schema
objectclass: metaSchema
objectclass: top
cn: nist.nccoe.abac
m-dependencies: cosine

dn: ou=attributetypes, cn=nist.nccoe.abac, ou=schema
objectclass: organizationalUnit
objectclass: top
ou: attributetypes

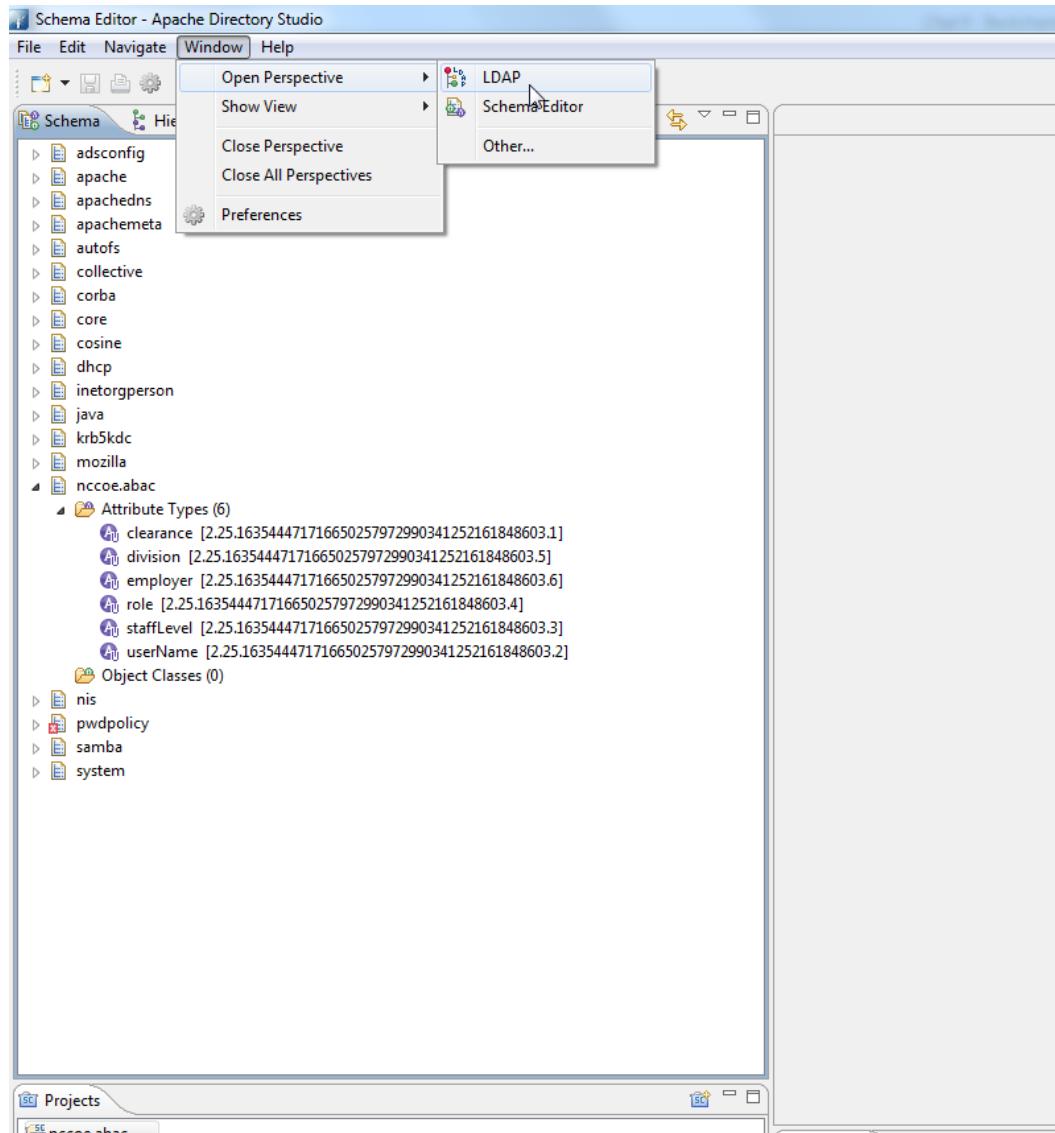
dn: m-oid=2.25.163544471716650257972990341252161848603.1, ou=attributetypes, cn=
nist.nccoe.abac, ou=schema
objectclass: metaAttributeType
objectclass: metaTop
objectclass: top
m-oid: 2.25.163544471716650257972990341252161848603.1
m-name: staffClearance
m-description: Clearnace of a staff
m-supAttributeType: userClass
m-equality: caseIgnoreMatch
```

The status bar at the bottom right of the GVIM window displays "24,1" and "Top".

6236

6237 18. To import the file, first select **Window > Open Perspective > LDAP**.

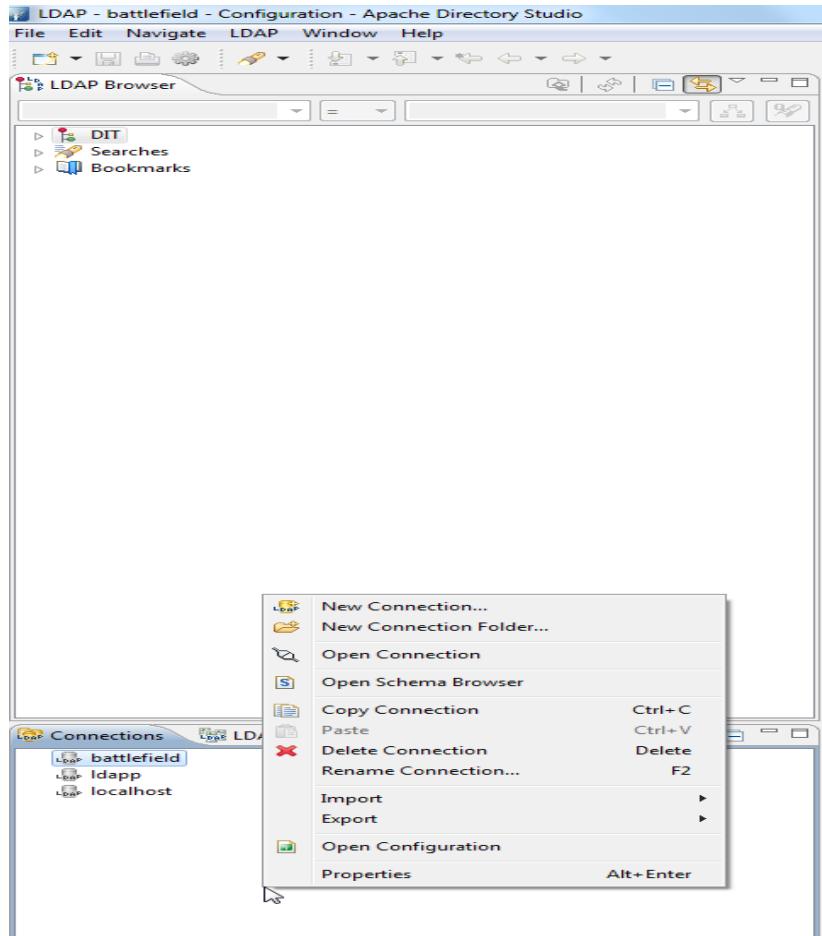
SECOND DRAFT



6238

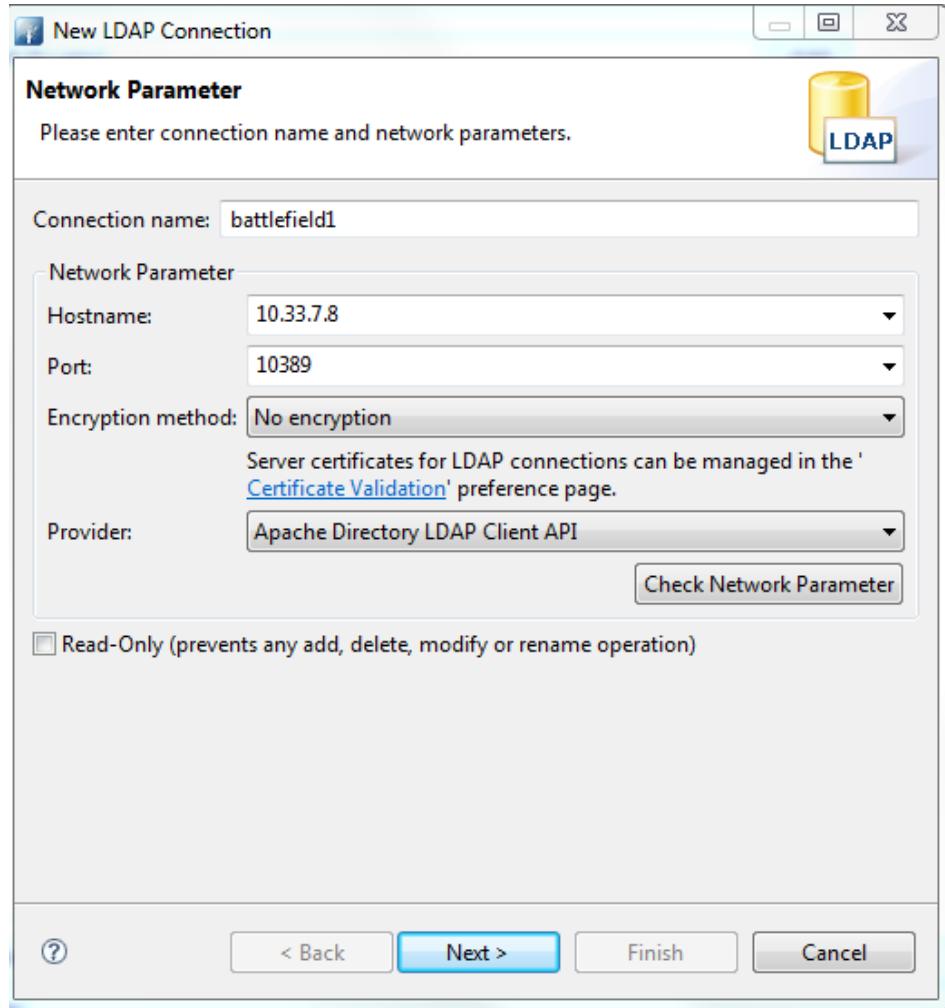
6239 19. Click on the left bottom corner of the window and select **New Connection**.

SECOND DRAFT



6240

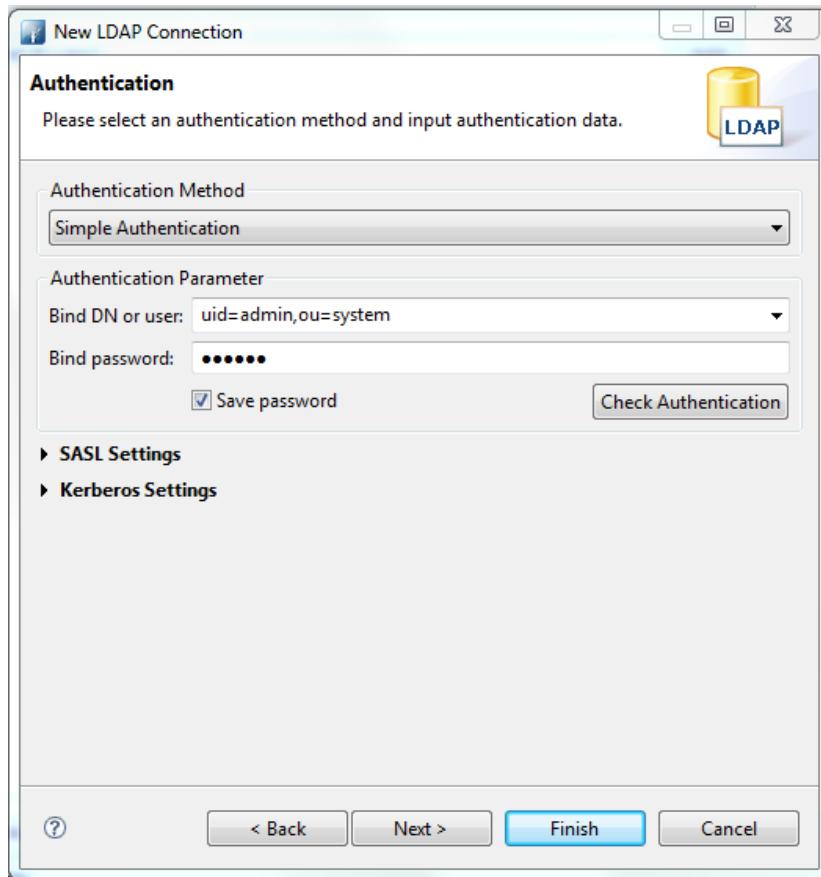
6241 20. Fill in the network parameters and click **Next**.



6242

6243 21. Provide credentials and click **Finish**.

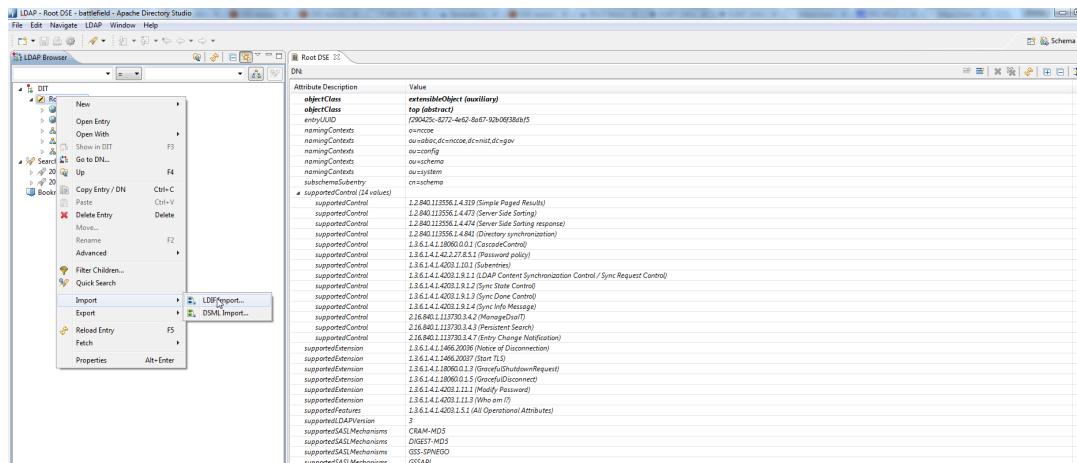
SECOND DRAFT



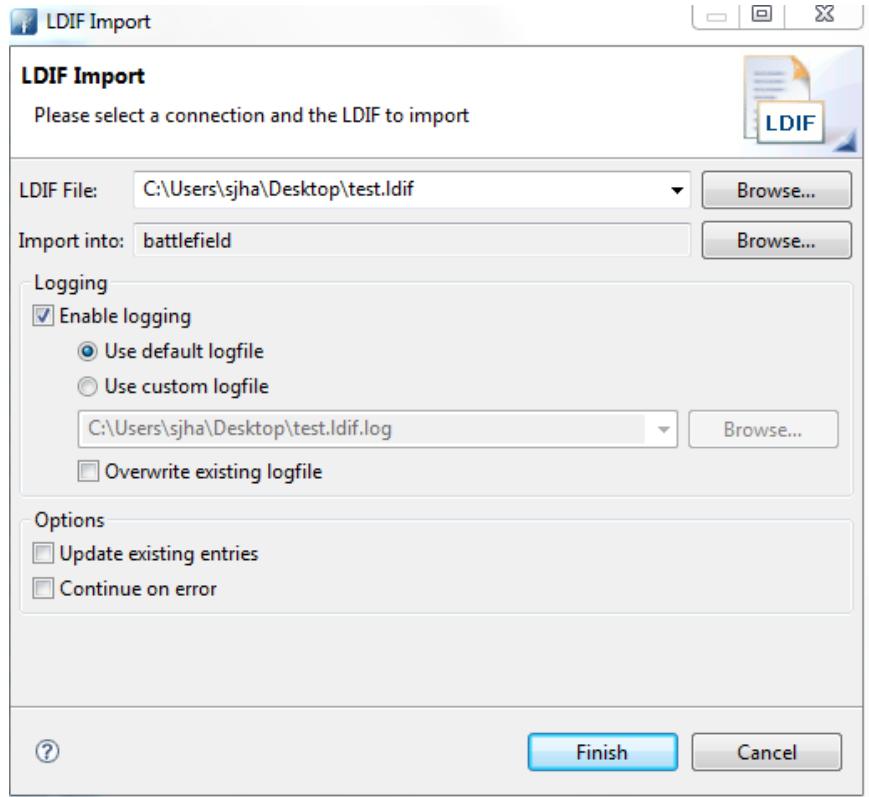
6244

6245

22. Open Schema Editor Browser and import the LDIF file created in the previous step.



6246



6247

6248

23. Click **Finish**.

6249

24. To verify success, the log file generated at the end of the import should show **RESULT OK**.

```

nccoe.abac.ldif.log - Notepad
File Edit Format View Help
# Generated by Apache Directory Studio on July 29, 2015 12:14:30 PM# SCHEMA "NIST.NCCOE.ABAC"#!RESULT OK
#!CONNECTION ldap://10.33.7.8:10389
#!DATE 2015-07-29T17:50:35.069
dn: cn=nccoe.abac, ou=schema
objectclass: metaSchema
objectclass: top
cn: nccoe.abac
m-dependencies: core
m-dependencies: cosine

#!RESULT OK
#!CONNECTION ldap://10.33.7.8:10389
#!DATE 2015-07-29T17:50:35.122
dn: ou=attributetypes, cn=nccoe.abac, ou=schema
objectclass: organizationalUnit
objectclass: top
ou: attributetypes

#!RESULT OK
#!CONNECTION ldap://10.33.7.8:10389
#!DATE 2015-07-29T17:50:35.274
dn: m-oid=2.25.163544471716650257972990341252161848603.1, ou=attributetypes,
cn=nccoe.abac, ou=schema
objectclass: metaAttributeType
objectclass: metaTop
objectclass: top
m-oid: 2.25.163544471716650257972990341252161848603.1
m-name: clearance
m-supAttributeType: userClass
m-equality: caseIgnoreMatch
m-substr: caseIgnoreSubstringsMatch
m-syntax: 1.3.6.1.4.1.1466.115.121.1.15

#!RESULT OK
#!CONNECTION ldap://10.33.7.8:10389
#!DATE 2015-07-29T17:50:35.345
dn: m-oid=2.25.163544471716650257972990341252161848603.2, ou=attributetypes,
cn=nccoe.abac, ou=schema
objectclass: metaAttributeType
objectclass: metaTop
objectclass: top
m-oid: 2.25.163544471716650257972990341252161848603.2
m-name: userName
m-obsolete: TRUE
m-supAttributeType: uid
m-equality: caseIgnoreMatch
m-substr: caseIgnoreSubstringsMatch
m-syntax: 1.3.6.1.4.1.1466.115.121.1.15
m-singleValue: TRUE

#!RESULT OK
#!CONNECTION ldap://10.33.7.8:10389
#!DATE 2015-07-29T17:50:35.487

```

6250

6251 10.10 Functional Tests

6252 Once all requirements have been met and all steps in this How-To Guide have been executed, a few
 6253 functional tests will ensure that the key components of this How-To Guide were correctly deployed and
 6254 are communicating with other ABAC components as desired.

6255 The first functional test will check the ready state of the NextLabs Policy Controller (ensures that it is
 6256 running after being paused for plugin deployment).

6257 The second test will check that the plugin was successfully loaded into the NextLabs software
 6258 architecture, that an attribute request is sent to the Protocol Broker from the NextLabs PIP plugin's
 6259 `getAttribute()` function, and that the Protocol Broker responds with an expected attribute value.

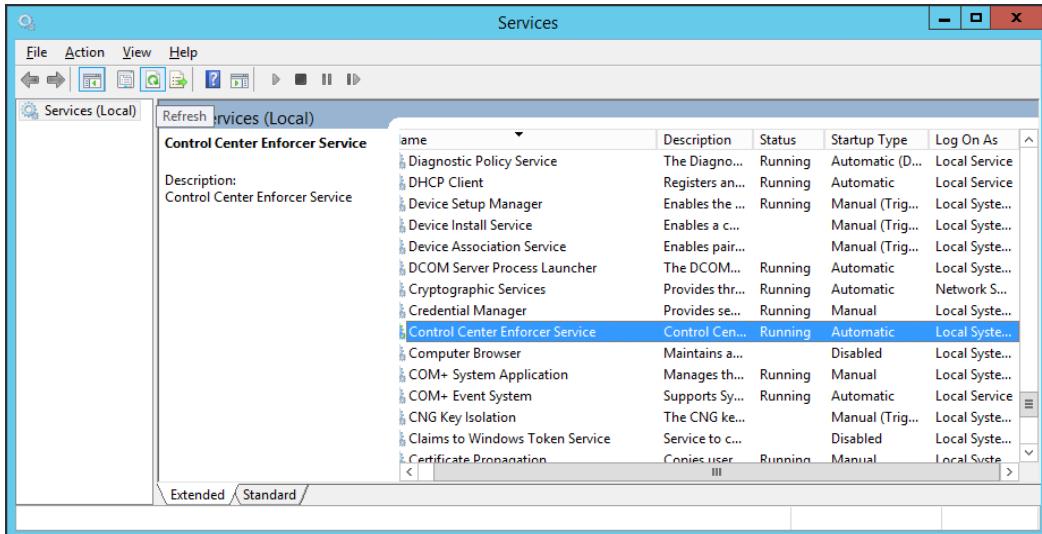
6260 The second functional test will ensure that the Protocol Broker is successfully loaded and deployed
 6261 within the tomcat server instance.

6262 Both of these functional tests can be done on the SharePoint server.

6263 10.10.1 Testing the Ready State of the NextLabs Policy Controller Service

- 6264 1. Click on the Windows icon and begin typing the word **services**.
- 6265 2. When the Services application icon appears, double-click to open the Services application.
- 6266 3. Within the Services application window, click on the Name column and look for **Control Center**
Enforcer Service.

6268 4. Verify that the status column reads **Running**.



6269

10.10.2 Test the Successful Loading of the Custom Plugin Within the NextLabs Policy Controller Software Architecture

- 6270 1. Click on the Windows icon.
- 6271 2. Begin typing **Windows Explorer**.
- 6272 3. Click on the Windows Explorer application icon.
- 6273 4. Navigate to *C:/Program Files/NextLabs/Policy Controller/agentLog/*.
- 6274 5. Within the **agentLog** folder, note the **Agentlog0.0** file.
- 6275 6. Within the **agentLog** folder, copy and paste the locked file **Agentlog0.log0** to open it for review.
 - 6276 a. Left-click on the file name, and hold down Ctrl+C.
 - 6277 b. Left-click anywhere in the **agentLog** folder, right-click and hold down Ctrl+V.

- 6278 7. Double-click the **Agent0.log-Copy.0** file to open it in your default text editor.
- 6279 8. Within your default text editor, use a search function to search for standard NextLabs logging terminology to verify that the plugin was loaded correctly. Example:

```

6280 Jul 13, 2015 4:59:21 PM com.bluejungle(pf.domain.destiny.serviceprovider.c A
6281 FINE: Loading C:\Program Files\NextLabs\Policy
6282 Controller\.jservice\config\nlsamlpluginService.properties
6283 Jul 13, 2015 4:59:21 PM com.bluejungle(pf.domain.destiny.serviceprovider.c A
6284 FINE: Loading C:\Program Files\NextLabs\Policy
6285 Controller\jservice\jar\nlsamlplugin/NLSAMLPPlugin-0.0.1-SNAPSHOT-jar-with-
6286 dependencies.jar
  
```

```

6287
6288
6289
6290 Jul 13, 2015 4:59:22 PM
6291 com.bluejungle(pf.domain.destiny.serviceprovider.ServiceProviderManager
6292 register
6293 INFO: A new Service 'NLSAMLPPlugin_Service' is registered.
  
```

6294 9. Within your default text editor, use a search function to search for logging statements you
 6295 included in your plugin code to verify that the init() methods are called while the jar is loaded
 6296 within NextLabs (standard according to NextLabs support). Example:

```
6297 Jul 13, 2015 4:59:21 PM gov.nist.NLSAMLPlugin.UserAttrProviderMod init
6298 INFO: NLSAMLPlugin UserAttrProviderMod code -- init method
6299 Jul 13, 2015 4:59:21 PM gov.nist.NLSAMLPlugin.HTTPSTransmitter init
```

6300 You can copy and paste the locked file, or keep a live annotating tool open that will display the
 6301 contents of Agent0.log0 as new log statements are recorded. Example from this
 6302 implementation: **BareTail by Bare Metal Software Pty Ltd.**

6303 Example screenshot using BareTail to open the **Agent0.log0** file, with optional highlighting
 6304 illustrating evaluated policies in yellow:

The screenshot shows the BareTail application interface. The title bar reads "Agent0.log0 (13.8 MB) - BareTail". The menu bar includes "File", "Edit", "View", "Preferences", "Help", "Open", "Highlighting", "Follow Tail", and "ANSI". The status bar at the bottom shows the file path "C:\Program Files\NextLabs\Policy Controller\agentLog\Agent0.log0 (13.8 MB)". The main window displays a list of log entries in yellow, which are highlighted to indicate evaluated policies. Some entries include timestamps and log levels like INFO and FINEST.

```

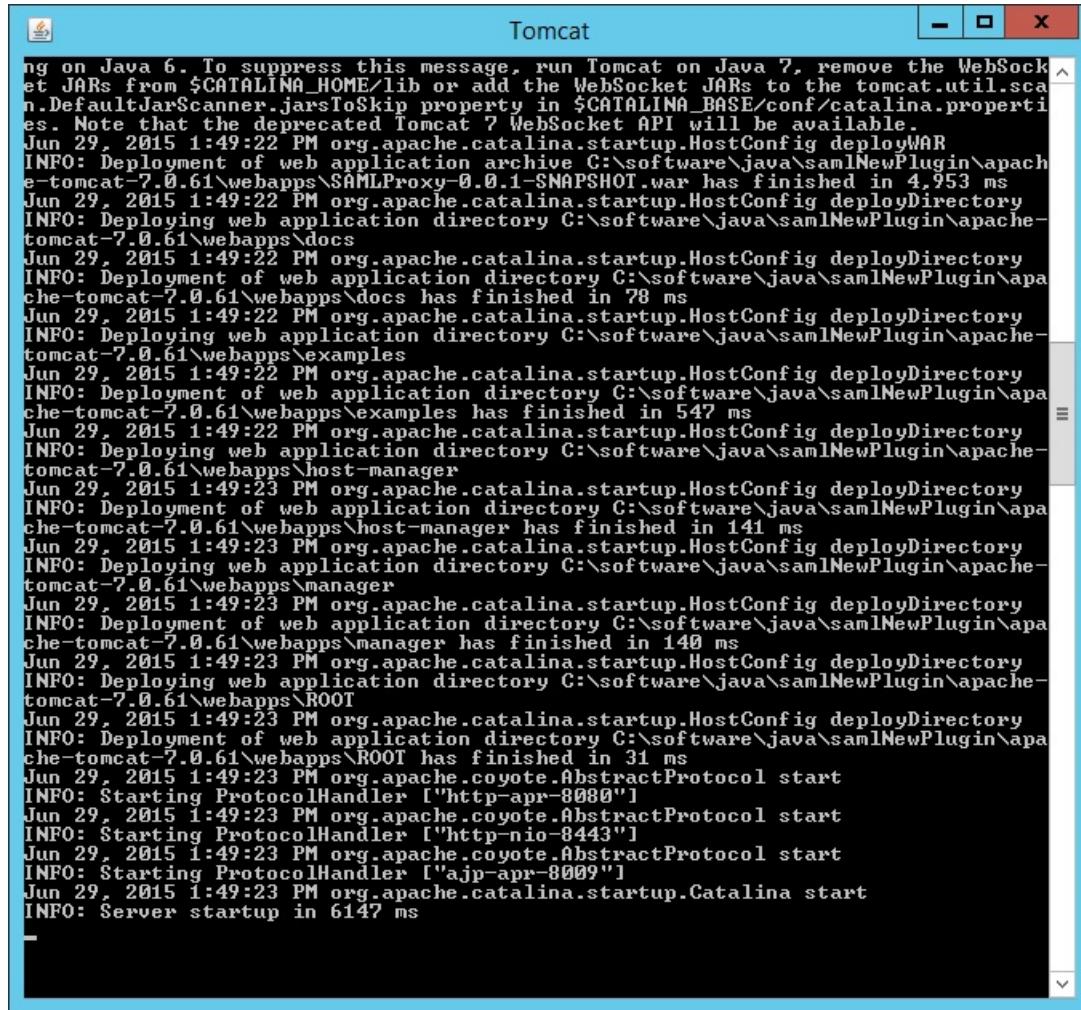
INFO: Executing log command: Time: 1435082292667
Jun 23, 2015 1:58:12 PM com.bluejungle.destiny.agent.commandengine.LogCommand execute
INFO: User ID: 9223372036854775806 Action: OPEN Effect: allow
Jun 23, 2015 1:58:12 PM com.bluejungle.framework.threading.WorkerThread run
FINEST: CommandExecutor-0: Queue size: 2
Jun 23, 2015 1:58:12 PM com.bluejungle.destiny.agent.commandengine.LogCommand execute
INFO: Executing log command: Time: 1435082292667
Jun 23, 2015 1:58:12 PM com.bluejungle.destiny.agent.commandengine.LogCommand execute
INFO: User ID: 9223372036854775806 Action: OPEN Effect: allow
Jun 23, 2015 1:58:12 PM com.bluejungle.framework.threading.WorkerThread run
FINEST: CommandExecutor-0: Queue size: 1
Jun 23, 2015 1:58:12 PM com.bluejungle.destiny.agent.commandengine.LogCommand execute
INFO: Executing log command: Time: 1435082292667
Jun 23, 2015 1:58:12 PM com.bluejungle.destiny.agent.commandengine.LogCommand execute
INFO: User ID: 9223372036854775806 Action: OPEN Effect: allow
Jun 23, 2015 1:58:12 PM com.bluejungle.framework.threading.WorkerThread run
FINEST: CommandExecutor-0: Queue size: 0
Jun 23, 2015 1:58:12 PM com.bluejungle.pf.engine.destiny.f performContentAnalysis
FINEST: No from resource found. Ignoring
Jun 23, 2015 1:58:12 PM com.bluejungle.pf.engine.destiny.EvaluationEngine evaluate
INFO: Matching policies for 1124308778098403:
X: Demo-v2/Sharepoint Protection - Department/DepartmentRestriction
A: Demo-v2/Sharepoint Protection - Department

```

6305

10.10.3 Testing That the Protocol Broker .war File Loads Correctly in Tomcat Server

1. On the SharePoint Server, open Services, and ensure that the **Control Center Enforcer Service** is listed as **Running**.
2. Using Windows Explorer, navigate to your Apache tomcat installation within the Windows file structure. Example: *C:/software/apache-tomcat-7.0.61*
3. **Double-click to open the bin folder.** Example: *C:/software/apache-tomcat-7.0.61/bin*
4. Double-click **startup.bat** to start the bat, and wait for startup to complete.



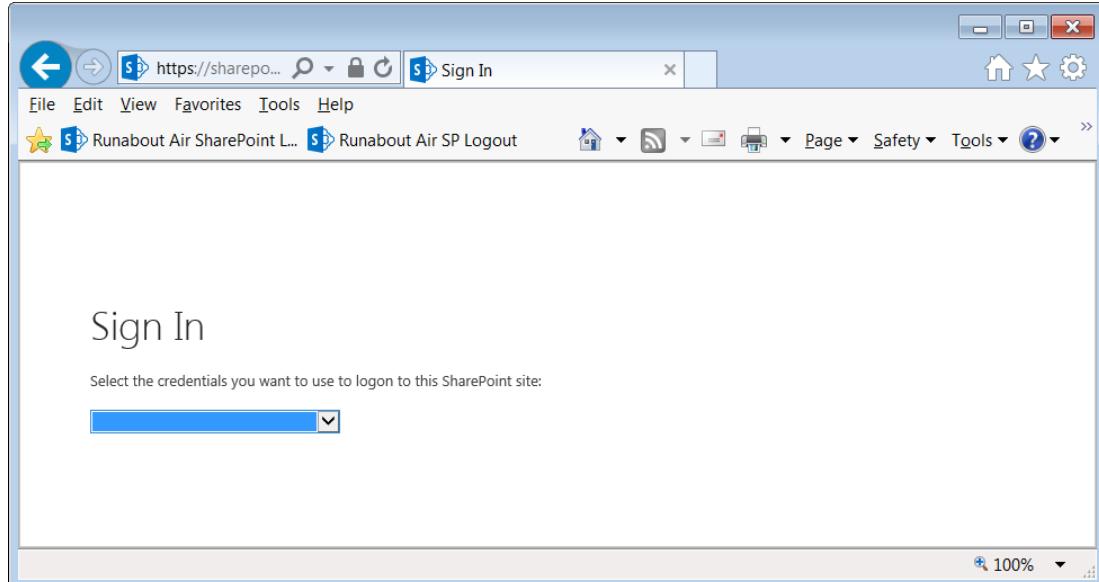
```

Tomcat
ng on Java 6. To suppress this message, run Tomcat on Java 7, remove the WebSock
et JARs from $CATALINA_HOME/lib or add the WebSocket JARs to the tomcat.util.sca
n.DefaultJaxScanner.jarsToSkip property in $CATALINA_BASE/conf/catalina.properti
es. Note that the deprecated Tomcat 7 WebSocket API will be available.
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployWAR
INFO: Deployment of web application archive C:\software\java\samlNewPlugin\apach
e-tomcat-7.0.61\webapps\SAMLProxy-0.1-SNAPSHOT.war has finished in 4,953 ms
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\docs
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\docs has finished in 78 ms
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\examples
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\examples has finished in 547 ms
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\host-manager
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\host-manager has finished in 141 ms
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\manager
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\manager has finished in 140 ms
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\ROOT
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\ROOT has finished in 31 ms
Jun 29, 2015 1:49:23 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["http-apr-8080"]
Jun 29, 2015 1:49:23 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["http-nio-8443"]
Jun 29, 2015 1:49:23 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["ajp-apr-8009"]
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 6147 ms

```

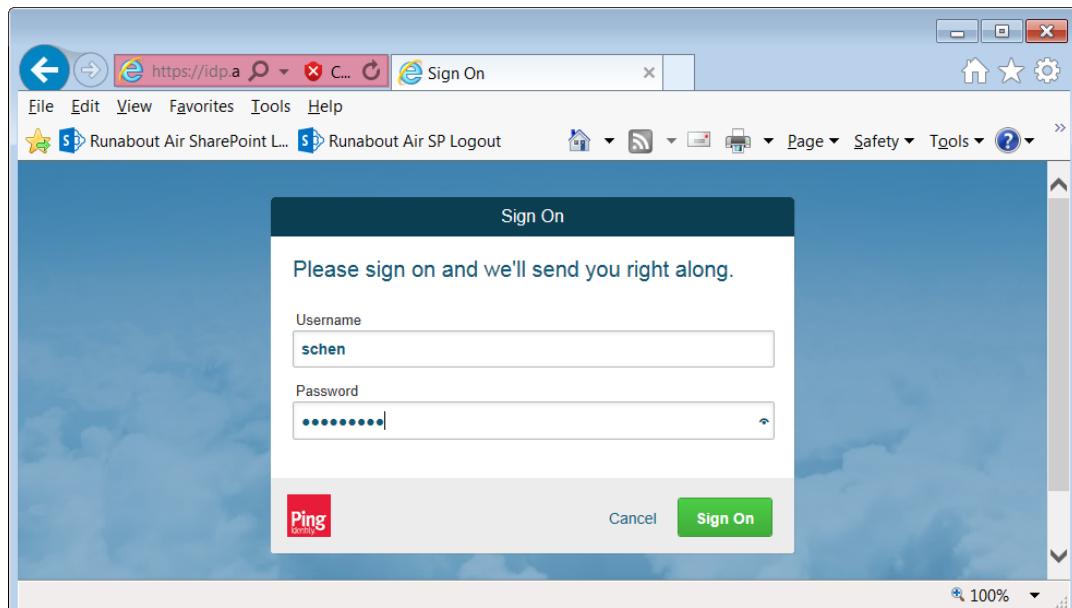
6313

- 6314 5. From any computer connected to this network, open an internet browser.
- 6315 6. In the address field, type <https://sharepoint.abac.test/> and press **Enter**.
- 6316 7. Choose **Federated Logon** from the drop-down menu.



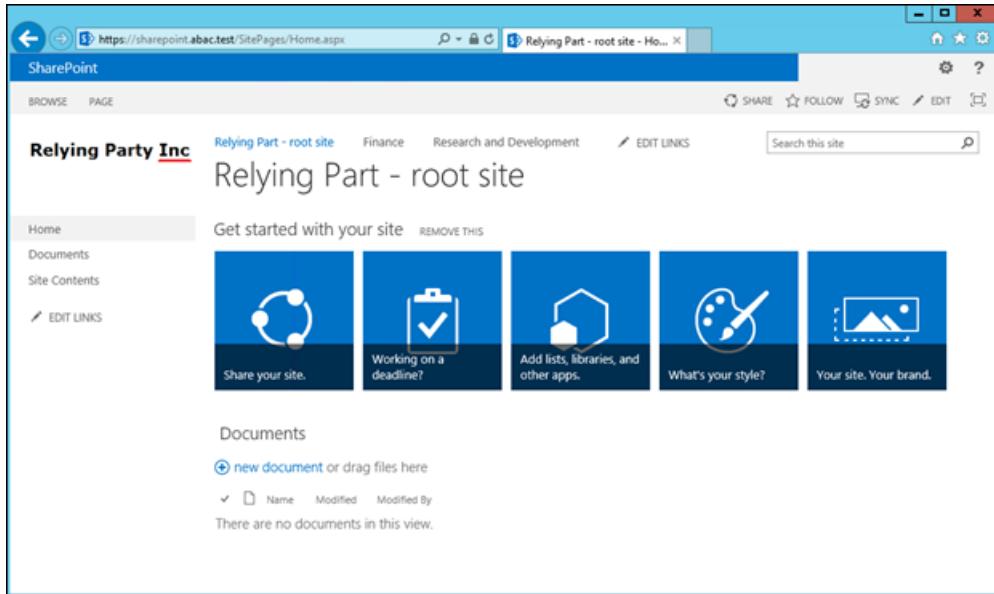
6317

- 6318 8. At the login screen, enter the credentials of a user that exists in your IdP Active Directory
6319 ([Section 2](#)), and click **Sign On**.



6320

- 6321 9. Verify that the user was able to access the main page of the RP's SharePoint. Example:



6322

- 6323 10. In the SharePoint site, double-click on an object for which you know the user will be missing an
 6324 attribute in order to be granted access, but that can be retrieved via a secondary attribute
 6325 request using the NextLabs PIP plugin, Protocol broker, and Ping custom data store.
- 6326 11. Follow the remaining steps 15-18 to verify through standard and custom logging that the
 6327 Protocol Broker was loaded, that the getAttribute() from the NextLabs PIP plugin was sent, and
 6328 an expected attribute value was returned.
- 6329 12. In Windows Explorer, navigate to your installation of Apache tomcat and locate its log files, i.e.,
 6330 *C:/software/apache-tomcat-7.0.61/logs*
- 6331 13. Open a catalina._____.log file using your default text editor and use a search function to find
 6332 standard Apache tomcat logging that indicates the .war file was correctly deployed and loads
 6333 without error. For example, in *C:/software/apache-tomcat-7.0.61/logs/catalina.2015-06-29.log*:
- ```

 6334 Jun 29, 2015 1:49:16 PM org.apache.catalina.startup.VersionLoggerListener log
 6335 INFO: Server version: Apache Tomcat/7.0.61
 6336 Jun 29, 2015 1:49:16 PM org.apache.catalina.startup.VersionLoggerListener log
 6337 Jun 29, 2015 1:49:16 PM org.apache.catalina.startup.VersionLoggerListener log
 6338 INFO: CATALINA_BASE: C:\software\java\samlNewPlugin\apache-tomcat-7.0.61
 6339 Jun 29, 2015 1:49:16 PM org.apache.catalina.startup.VersionLoggerListener log
 6340 INFO: CATALINA_HOME: C:\software\java\samlNewPlugin\apache-tomcat-7.0.61
 6341 Jun 29, 2015 1:49:16 PM org.apache.catalina.startup.VersionLoggerListener log
 6342 INFO: Command line argument: -
 6343 Djava.util.logging.config.file=C:\software\java\samlNewPlugin\apache-tomcat-
 6344 7.0.61\conf\logging.properties
 6345 Jun 29, 2015 1:49:16 PM org.apache.catalina.startup.VersionLoggerListener log
 6346 INFO: Command line argument: -
 6347 Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
 6348 Jun 29, 2015 1:49:16 PM org.apache.catalina.startup.VersionLoggerListener log
 6349 INFO: Command line argument: -
 6350 Djava.endorsed.dirs=C:\software\java\samlNewPlugin\apache-tomcat-
 6351 7.0.61\endorsed
 6352 Jun 29, 2015 1:49:17 PM org.apache.catalina.startup.HostConfig deployWAR

```

```

6353 INFO: Deploying web application archive C:\software\java\samlNewPlugin\apache-
6354 tomcat-7.0.61\webapps\SAMLProxy-0.0.1-SNAPSHOT.war
6355 Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployWAR
6356 INFO: Deployment of web application archive
6357 C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\SAMLProxy-0.0.1-
6358 SNAPSHOT.war has finished in 4,953 ms
6359 Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
6360 INFO: Deploying web application directory
6361 C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\docs
6362 Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
6363 INFO: Deployment of web application directory
6364 C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\docs has finished
6365 in 78 ms
6366 Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
6367 INFO: Deploying web application directory
6368 C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\examples
6369 Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
6370 INFO: Deployment of web application directory
6371 C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\examples has
6372 finished in 547 ms
6373 Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
6374 INFO: Deploying web application directory
6375 C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\host-manager
6376 Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
6377 INFO: Deployment of web application directory
6378 C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\host-manager has
6379 finished in 141 ms

```

- 6380 14. While the same file is open, use another search function to find custom logging that indicates  
 6381 that the Protocol Broker was used for a SAML Attribute query request and response. Example  
 6382 custom log files from this build:

```

Jun 29, 2015 1:59:00 PM nist.pdpplugin.transport.SoapHTTPTransmitter transmit
INFO: START SoapHTTPTransmitter method. Start time: 1435600740151
Jun 29, 2015 1:59:08 PM nist.pdpplugin.transport.SoapHTTPTransmitter transmit
INFO: START SoapHTTPTransmitter method. Start time: 1435600748229
Jun 29, 2015 1:59:11 PM nist.pdpplugin.transport.SoapHTTPTransmitter transmit
INFO: END SoapHTTPTransmitter transmit Method: 1435600751682
Jun 29, 2015 1:59:11 PM nist.pdpplugin.transport.SoapHTTPTransmitter transmit
INFO: END SoapHTTPTransmitter transmit Method. Total Execution time: 11531

```

- 6391 15. Within the **Agent0.log0**, another search function to find custom logging statements that verify  
 6392 from within the NextLabs Policy Controller software execution side that the plugin's  
 6393 `getAttribute()` function was called and that the requested attribute was returned.

- 6394 a. Example from this build:

- 6395 i. user: schen@abac.test
- 6396 ii. requested attribute: clearance
- 6397 iii. expected returned value: Secret
- 6398 iv. actual returned value: Secret

```

Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
getAttribute

```

## SECOND DRAFT

```
6401 INFO: NLSAMLPlugin UserAttrProviderMod getAttribute() function called.
6402 Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6403 getAttribute
6404 INFO: START getAttribute method. Start time: 1433345957517
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6405 getAttribute
6406 INFO: NLSAMLPlugin UserAttrProviderMod getAttribute Line00-72 - subjectID
6407 param: schen@abac.test
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6408 getAttribute
6409 INFO: NLSAMLPlugin UserAttrProviderMod getAttribute Line00-73 -
6410 attributeName param: clearance
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6411 getAttribute
6412 INFO: NLSAMLPlugin Trying to check if there exist a prior entry in cache.
6413 -- UserAttrProviderMod Line00-79
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6414 getAttribute
6415 INFO: NLSAMLPlugin Using soapHTTPTransmitter object and calling its
6416 transmit() function.
Jun 3, 2015 11:39:22 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6417 getAttribute
6418 INFO: NLSAMLPlugin UserAttrProviderMod getAttribute() Line00-114 --
6419 attributeValue returned: Secret
6420
6421
6422
6423
6424
```