

**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**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce



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*



# 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-](https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control)  
86   [access-control](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  
87   guide. If you adopt this solution for your own organization, please share your experience and advice  
88   with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so  
89   we encourage organizations to share lessons learned and best practices for transforming the processes  
90   associated with implementing this guide. To provide comments or to learn more by arranging a  
91   demonstration of this example implementation, contact the NCCoE at [abac-nccoe@nist.gov](mailto: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](mailto: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](mailto: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](mailto: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 Lefkowitz	NIST National Strategy for Trusted Identities in Cyberspace
Rene Peralta	NIST National Strategy for Trusted Identities in Cyberspace
Dave Ferriolo	NIST Computer Security Division
Vincent Hu	NIST Computer Security Division
Roger Wiggensam	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
<a href="#">Ping Identity</a>	PingFederate Federation Server
<a href="#">NextLabs</a>	Entitlements Management Policy Enforcement Point
<a href="#">Microsoft</a>	Policy Controller Policy decision point
<a href="#">RSA</a>	Control Center Policy Administration Point
<a href="#">Symantec</a>	Active Directory

Technology Partner/Collaborator	Build Involvement
<a href="#">Cisco</a>	SharePoint

50

51 **Contents**

52 **1 Summary..... 1**

53 1.1 Challenge ..... 1

54 1.2 Solution..... 2

55 1.3 Risks ..... 2

56 1.4 Benefits..... 2

57 **2 How to Use This Guide ..... 3**

58 2.1 Typographical Conventions ..... 5

59 **3 Introduction ..... 5**

60 3.1 Background..... 6

61 3.2 ABAC and RBAC Considerations ..... 6

62 3.3 ABAC Leveraging Identity Federation ..... 7

63 3.4 Security Standards..... 9

64 **4 Approach..... 12**

65 4.1 Audience..... 12

66 4.2 Scope ..... 12

67 4.3 Assumptions ..... 12

68 4.3.1 Modularity ..... 12

69 4.3.2 Business Policy Language..... 12

70 4.3.3 Attribute Semantics and Syntax..... 13

71 4.3.4 Attribute Provenance..... 13

72 4.3.5 Trust Relationships for Identity Federation ..... 13

73 4.3.6 Human Resources Database/Identity Proofing ..... 13

74 4.3.7 Technical Implementation ..... 13

75 4.3.8 Limited Scalability Testing..... 14

76 4.4 Risk Assessment ..... 14

77 4.4.1 Strategic Risks ..... 14

78 4.4.2 Tactical Risks ..... 15

79 4.4.3 Security Control Map ..... 17

80 4.5 Technologies..... 18

81 **5 Architecture ..... 22**

82 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	
89		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	<b>Appendix A List of Acronyms .....</b>		<b>37</b>
111	<b>Appendix B References.....</b>		<b>39</b>

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**

## 120 **1 Summary**

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

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

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

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

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

### 144 **1.1 Challenge**

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

151 Consider a patient submitting a health insurance claim. A claims examiner needs to know just billing  
152 and diagnostic codes and a few pieces of demographic data in order to permit reimbursement.  
153 Interacting with the same system, the patient’s doctor needs to verify that the diagnosis and  
154 referral information is for the correct patient, but does not need to see payment or address  
155 information. The patient needs access to the claim’s status, while the patient’s employer only needs  
156 to see the number of claims submitted by the employee. The insurance company provides a single  
157 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



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](mailto: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> .
<b>Bold</b>	names of menus, options, com- mand buttons and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on-screen computer output, sample code examples, status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input con- trasted with computer output	<b><code>service sshd start</code></b>
<a href="#">blue text</a>	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 <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a>

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

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

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	<a href="http://dx.doi.org/10.6028/NIST.SP.800-52r1">http://dx.doi.org/10.6028/NIST.SP.800-52r1</a>
	RFC 2246, TLS Protocol 1.0	<a href="https://tools.ietf.org/html/rfc2246">https://tools.ietf.org/html/rfc2246</a>
	RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1	<a href="https://tools.ietf.org/html/rfc4346">https://tools.ietf.org/html/rfc4346</a>
	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2	<a href="https://tools.ietf.org/html/rfc5246">https://tools.ietf.org/html/rfc5246</a>
PKI	PKI Technical Standards	<a href="http://www.oasis-pki.org/resources/techstandards/">http://www.oasis-pki.org/resources/techstandards/</a>

358



## 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.

### 612 5.1.6 Allow RP Access Decisions on External Identities without the Need for 613 Pre-Provisioning

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

## 618 5.2 ABAC Architecture Considerations

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

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

### 625 5.2.1 Industry Standards

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

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

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

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

### 643 5.2.2 PEP Placement

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

- 648     ▪ 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.

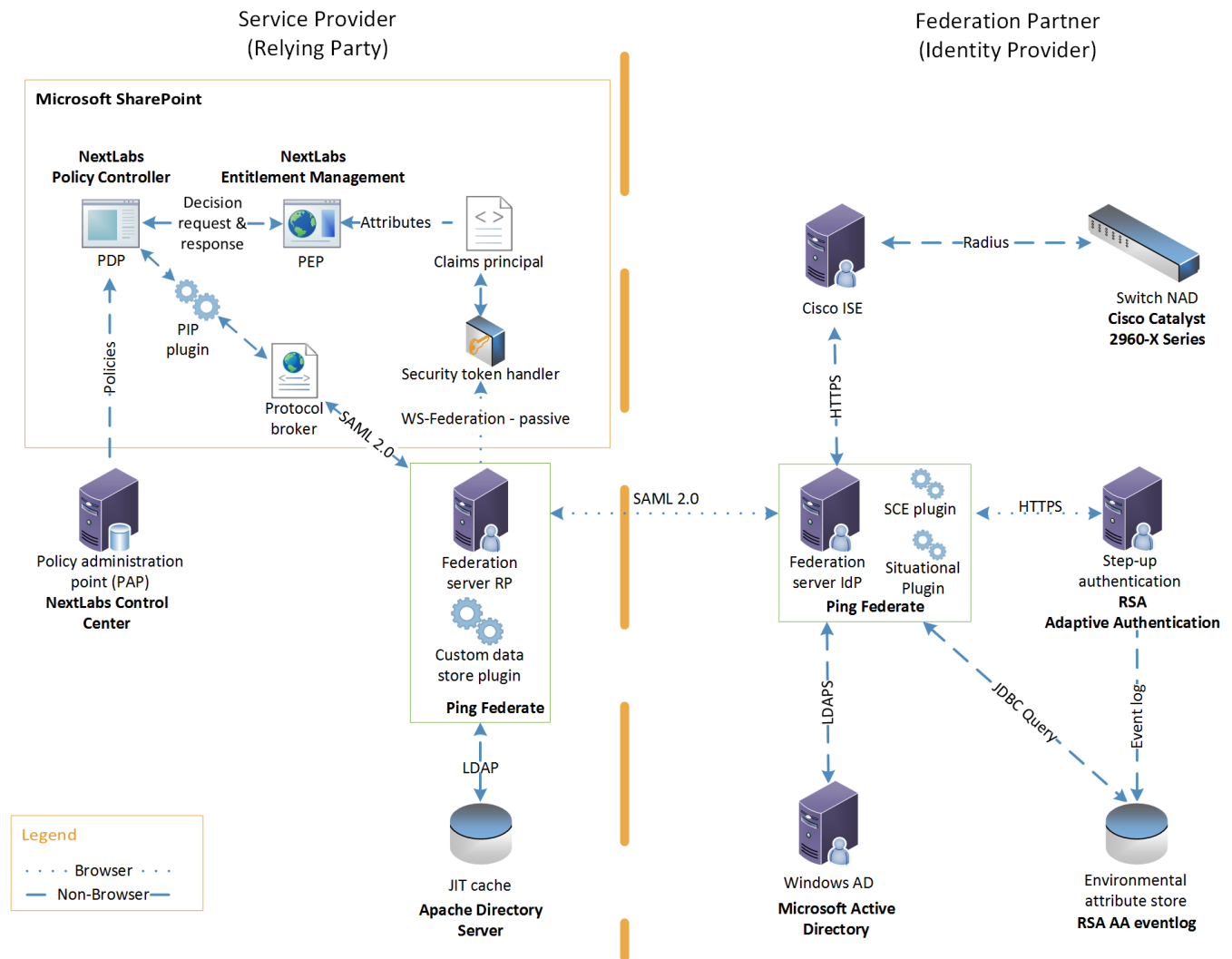
## 697 **5.3 Technology and Architecture of the NCCoE Build**

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.

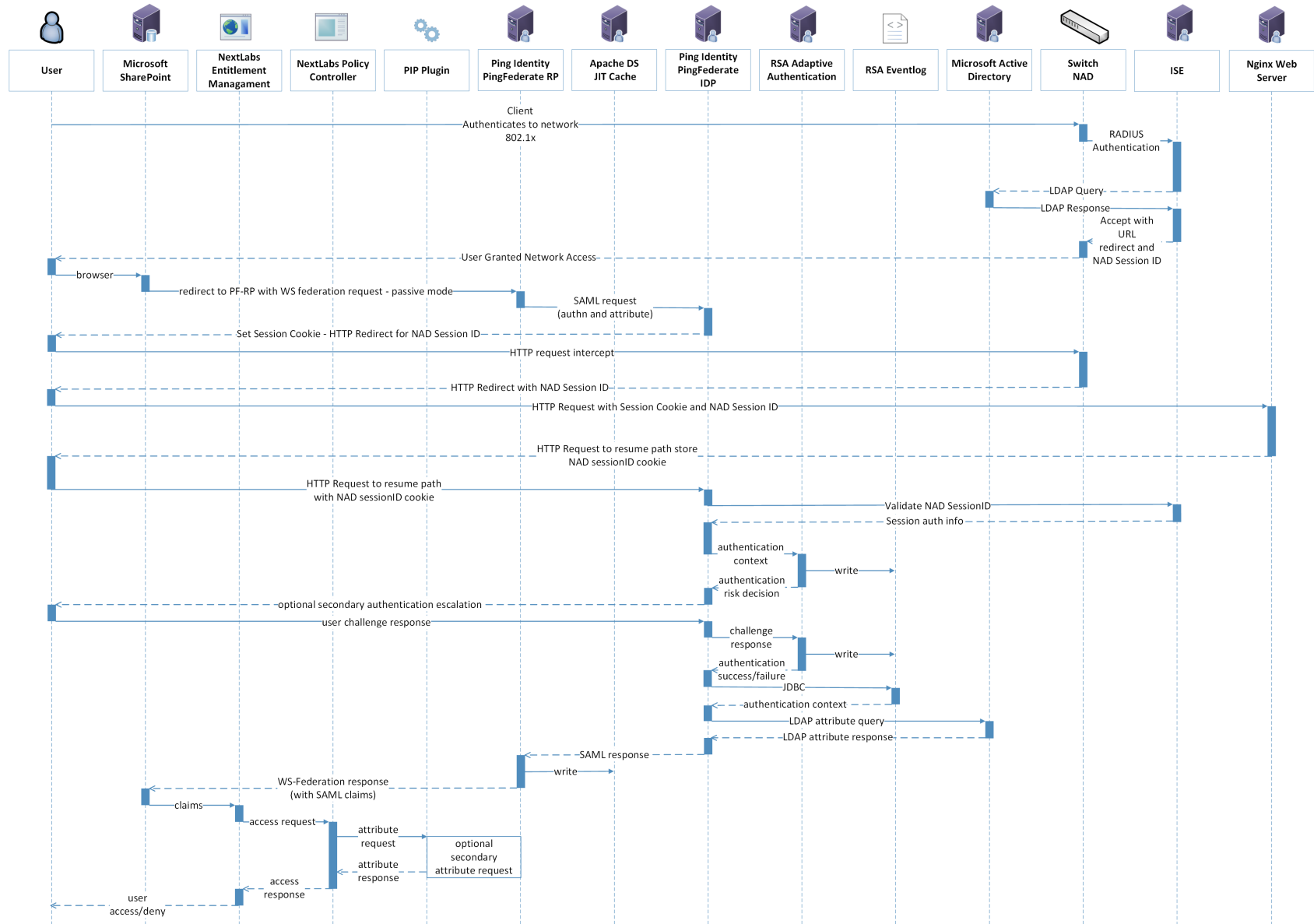


- 763       ▪ Policy Information Point(PIP) Plug-in is a software extension of NextLabs Policy Controller that  
764       enables it to acquire unavailable attributes required for policy evaluation at runtime from RP or  
765       IdP by communicating with Protocol Broker on an HTTPS channel protected 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.

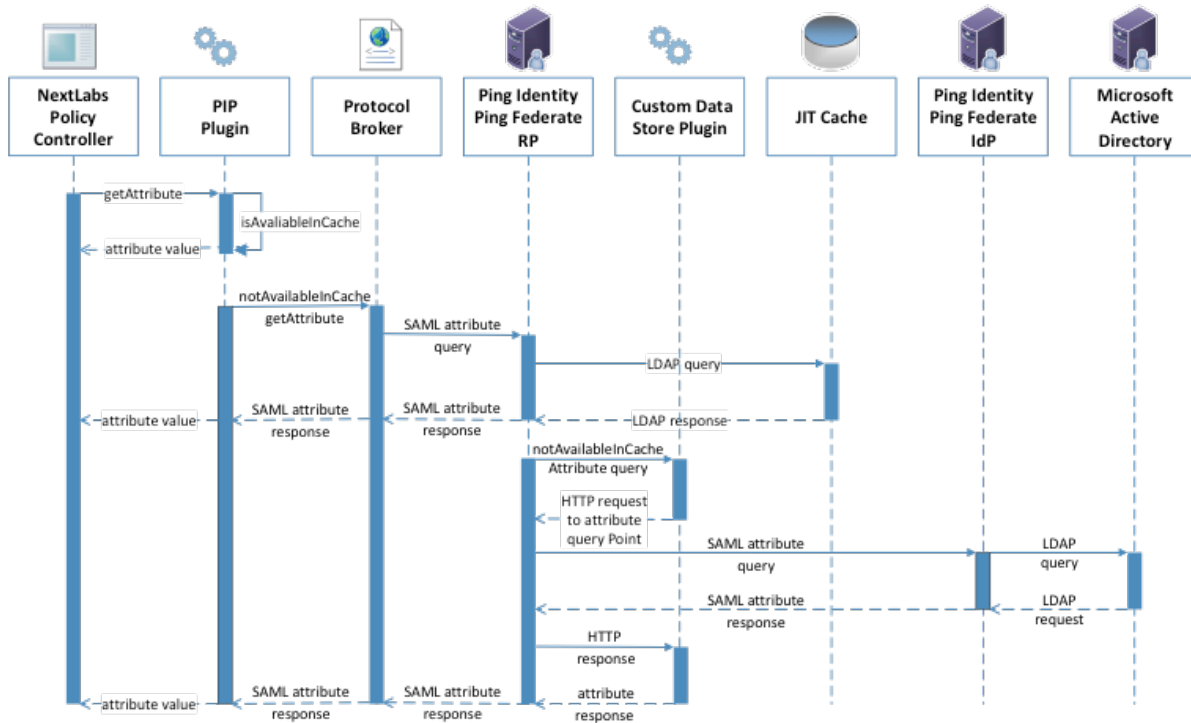
- 829 9. Access requests by the authenticated user are now trapped by the NextLabs Entitlement  
830 Management PEP, which gathers the subject and environmental attributes stored in the Claims  
831 Principal and the object attributes stored in SharePoint, and submits the access request to the  
832 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

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

<b>WS</b>	Web Service
<b>XACML</b>	eXtensible Access Control Markup Language
<b>XML</b>	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](http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711) [accessed 09/08/17].
- [3] R. Ross, M. McEvilly, 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](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](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](mailto: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](mailto: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 Lefkowitz	NIST National Strategy for Trusted Identities in Cyberspace
Rene Peralta	NIST National Strategy for Trusted Identities in Cyberspace
Dave Ferriolo	NIST Computer Security Division
Vincent Hu	NIST Computer Security Division
Roger Wiggensam	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
<a href="#">Ping Identity</a>	PingFederate Federation Server
<a href="#">NextLabs</a>	Entitlements Management Policy Enforcement Point
<a href="#">Microsoft</a>	Policy Controller Policy decision point
<a href="#">RSA</a>	Control Center Policy Administration Point

Technology Partner/Collaborator	Build Involvement
<a href="#">Symantec</a>	Active Directory
<a href="#">Cisco</a>	SharePoint

50

51	<b>Contents</b>	
52	<b>1 Introduction</b>	<b>1</b>
53	1.1 Practice Guide Structure	1
54	1.2 Build Overview	2
55	1.3 Typographical Conventions	2
56	<b>2 Setting Up the Identity Provider</b>	<b>3</b>
57	2.1 Components	3
58	2.1.1 Cisco Switch and Cisco Identity Services Engine	4
59	2.1.2 Microsoft AD	4
60	2.1.3 Nginx Web Server	4
61	2.1.4 PingFederate-IdP	4
62	2.1.5 PingFederate-RP	5
63	2.1.6 RSA Adaptive Authentication	5
64	2.1.7 SCE Plug-in	5
65	2.1.8 Situational Context Connector	5
66	2.1.9 Required or Recommended Files, Hardware, and Software	6
67	2.2 Configuring I PC for 802.1x Auth	7
68	2.2.1 Configure MS Native Supplicant for Wired 802.1x	10
69	2.3 Install Nginx Web Server	16
70	2.4 Install Microsoft AD	17
71	2.4.1 Create a User in Microsoft AD	17
72	2.4.2 Create the Lightweight Directory Access Protocol User for Federated	
73	Authentication	19
74	2.4.3 Create the LDAP User for Cisco ISE Administration	19
75	2.5 Configure the Cisco Switch	19
76	2.6 Install and Configure Cisco Identity Services Engine	23
77	2.6.1 Configure Cisco ISE with Microsoft AD	26
78	2.6.2 Add Network Device to ISE	26
79	2.6.3 Configure ISE for pxGrid	26
80	2.6.4 Enable ISE Policy Sets	27
81	2.6.5 Configure Authentication Policy	29
82	2.6.6 Configure Authorization Policy	32
83	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	<b>3</b>	<b>Setting up Federated Authentication Between the Relying Party and the</b>	
117		<b>Identity Provider .....</b>	<b>133</b>

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	<b>4</b>	<b>Installing and Configuring Microsoft SharePoint Server and Related</b>	
126		<b>Components.....</b>	<b>162</b>
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	<b>5</b>	<b>Set Up Federated Authentication at the Relying Party’s SharePoint ..</b>	<b>215</b>
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

160 ..... 273

161 6.3.3 Configure PingFederate-RP to Pull Attributes from the Identity Provider’s SAML

162 Exchange..... 287

163 6.4 Configure PingFederate-RP and SharePoint to Pass and Read Attributes ..... 293

164 6.4.1 Configure PingFederate-RP to Pass Attributes to SharePoint..... 293

165 6.4.2 Configure SharePoint to Read Custom Attributes from PingFederate-RP ..... 301

166 6.5 Configure the Claims Viewer Web Part at the SharePoint Site..... 307

167 6.6 Functional Test of All Configurations for Section 6..... 314

168 6.6.1 Temporarily Disable SAML Encryption for Testing and Troubleshooting Message

169 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  
 185 Server ..... 354  
 186 7.6.1 Installation and Configuration..... 354  
 187 7.7 Functional Tests..... 363  
 188 7.7.1 Verify that the NextLabs Webpart for Policy Enforcement Has Been Successfully  
 189 Enabled on the Site Collection in SharePoint..... 363  
 190 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  
 218 during SharePoint Access ..... 429



219 **9 Leveraging NextLabs Control Center Reporter for Reporting and**  
 220 **Auditing Purposes ..... 432**

221 9.1 Introduction ..... 432

222 9.1.1 Components Used in this How-To Guide ..... 432

223 9.1.2 Pre-requisites to Complete Prior to this How-To Guide..... 432

224 9.2 Introduction to NextLabs Control Center Reporter ..... 433

225 9.2.1 Opening Reporter ..... 433

226 9.3 Introduction to Reporter Dashboard..... 435

227 9.3.1 Exploring the Dashboard ..... 437

228 9.4 Introduction to Defining and Running Custom Reports in Reporter..... 439

229 9.4.1 Defining a Custom Report ..... 440

230 9.4.2 Running a Custom Report..... 446

231 9.5 Example Custom Report and Available Formats ..... 446

232 9.5.1 Defining the Example Custom Report ..... 446

233 9.5.2 Format: Table of Event Data..... 450

234 9.5.3 Format: Bar Chart Grouped by Policy Chart ..... 452

235 9.5.4 Format: Bar Chart Grouped by User Chart ..... 453

236 9.5.5 Format: Pie Chart Grouped by Resource..... 455

237 9.6 Further Example Custom Reports from Our Build ..... 457

238 9.6.1 Custom Report Illustrating All Access for One User During a Two-Month Period . 457

239 9.6.2 Viewing Access Attempts on Individual Resources ..... 460

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	
268		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	
277		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**

## 300 1 Introduction

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

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

### 307 1.1 Practice Guide Structure

308 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides  
309 users with the information they need to replicate an Attribute Based Access Control (ABAC)  
310 implementation. This reference design is modular and can be deployed in whole or in parts.

311 This guide contains three volumes:

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

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

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

- 318     ▪ challenges enterprises face in access control solutions
- 319     ▪ example solution built at the NCCoE
- 320     ▪ benefits of adopting the example solution

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

- 324     ▪ Section 4.4.1, Risk, provides a description of the risk analysis we performed
- 325     ▪ Section 4.4.3, Security Control Map, maps the security characteristics of this example solution to  
326     cybersecurity standards and best practices

327 You might share the *Executive Summary, NIST SP 1800-3a*, with your leadership team members to help  
328 them understand the importance of adopting standards-based ABAC implementation.

329 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.  
330 You can use the How-To portion of the guide, *NIST SP 1800-3c*, to replicate all or parts of the build  
331 created in our lab. The How-To guide provides specific product installation, configuration, and  
332 integration instructions for implementing the example solution. We do not recreate the product  
333 manufacturers' documentation, which is generally widely available. Rather, we show how we  
334 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-](mailto:abac-nccoe@nist.gov)  
 346 [nccoe@nist.gov](mailto: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> .
<b>Bold</b>	names of menus, options, command buttons and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on- screen computer output, sample code examples, sta- tus codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<code><b>service sshd start</b></code>

Typeface/ Symbol	Meaning	Example
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a>

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  
 378     from users to the services and applications on another network segment
- 379     ▪ **Cisco Identity Services Engine (ISE):** Authenticates users from other networks or network  
 380     segments, and provides device and network attributes to the Ping-Federate IdP via the  
 381     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  
 384     Network Access Device (NAD) redirects for the Situational Context Connector. In this build, we  
 385     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.

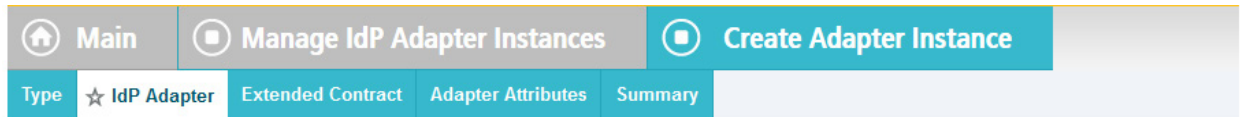
### 413   2.1.4   PingFederate-IdP

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.



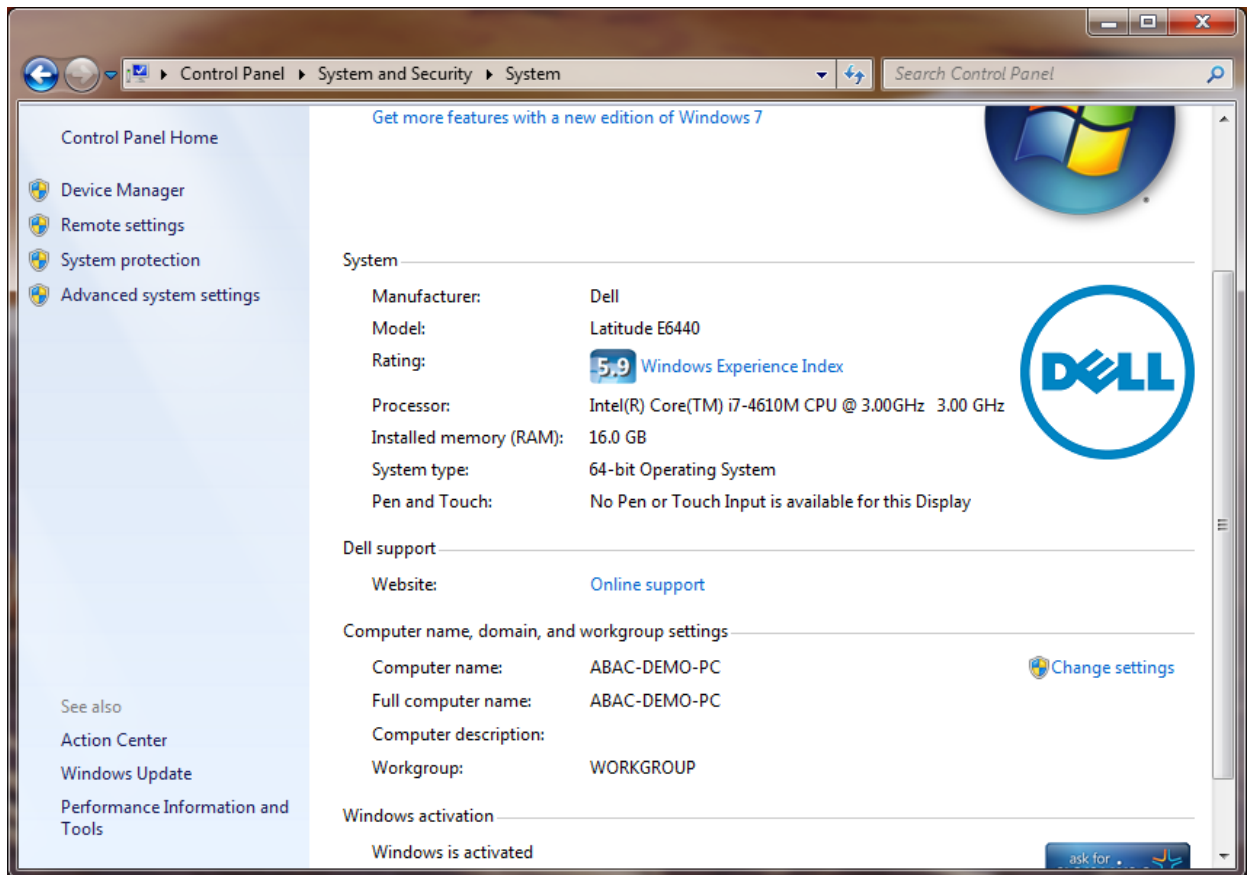
## 462 2.1.9 Required or Recommended Files, Hardware, and Software

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

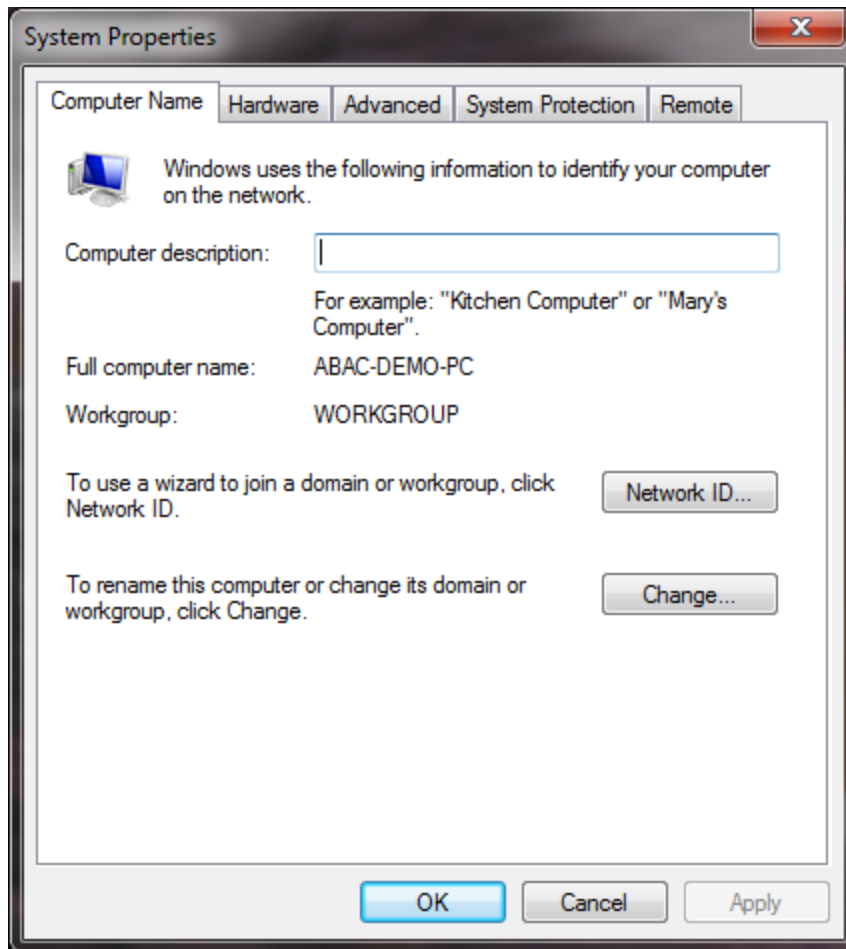
464 **2.2 Configuring I PC for 802.1x Auth**

- 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

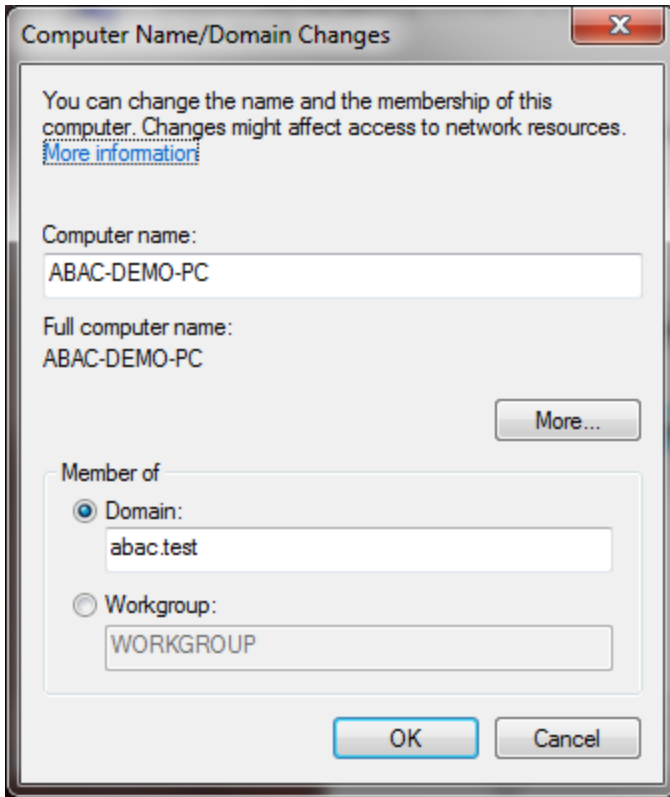
4. Select **Domain**.

471

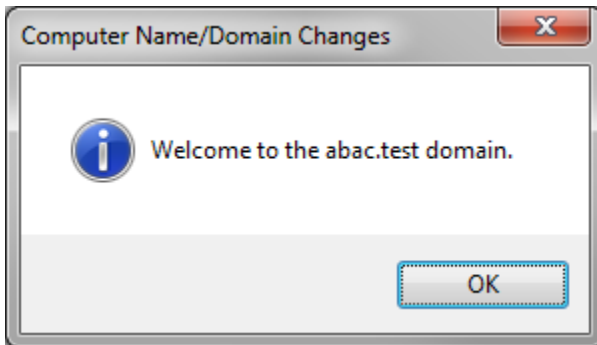
5. Enter the domain to join, "abac.test." It will require authentication using a user that' is capable

472

of adding a computer to the domain controller.



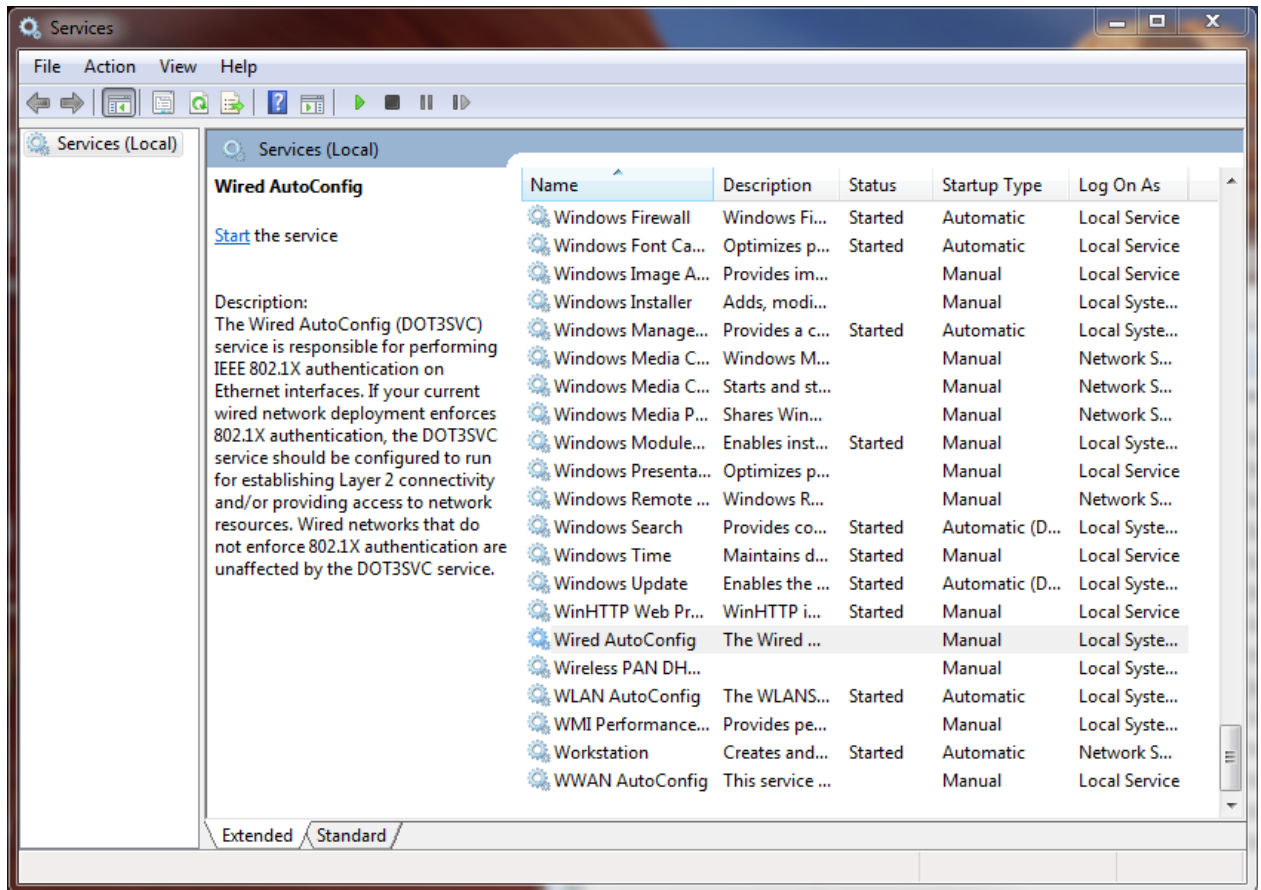
473



474

## 475 2.2.1 Configure MS Native Supplicant for Wired 802.1x

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

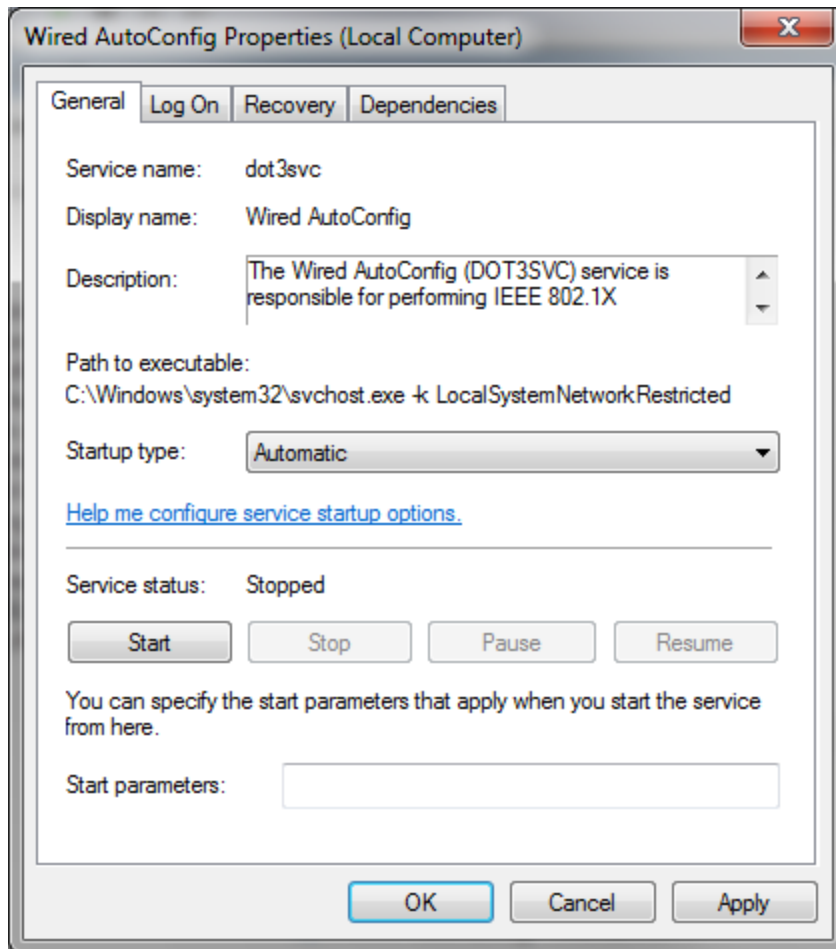


477

- 478 2. Right-click on
- Wired AutoConfig**
- .

- 479 3. Select
- Properties**
- .

- 480 4. Change the
- Startup type**
- to
- Automatic**
- .



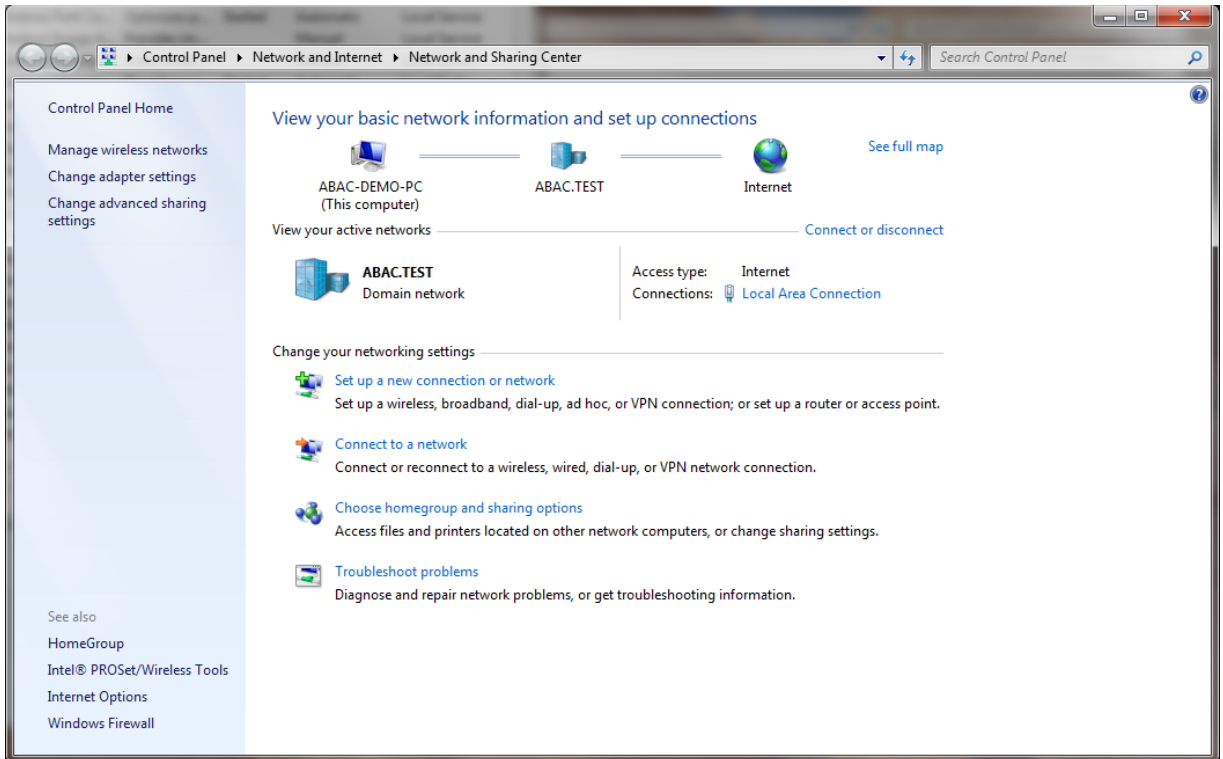
481

482

483

484

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

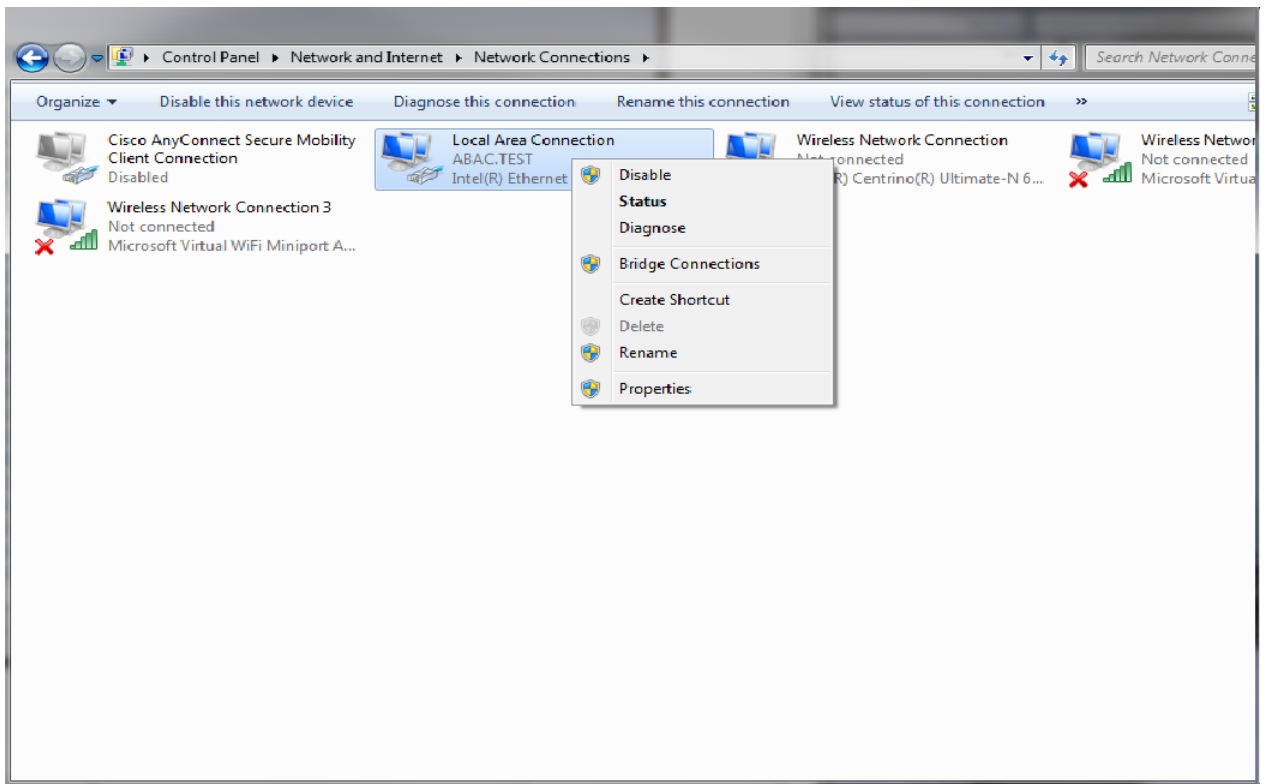


485

486

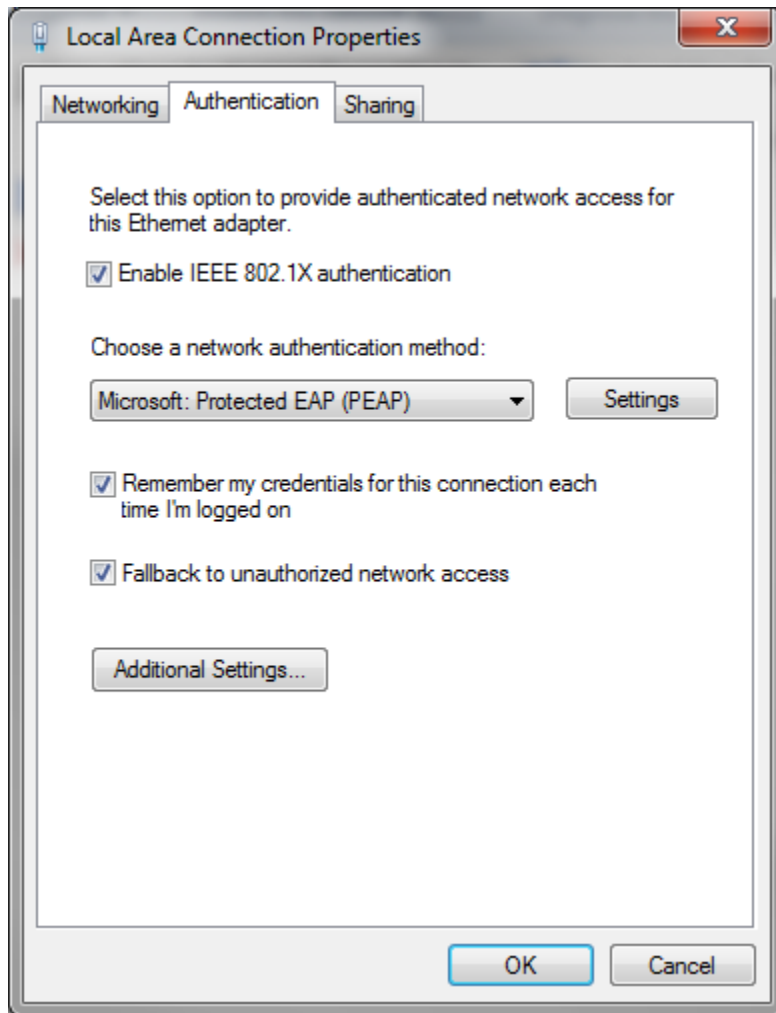
487

8. Click on **Change adapter settings**.
9. Right-click on your connection adapter and select **Properties**.



488

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



490

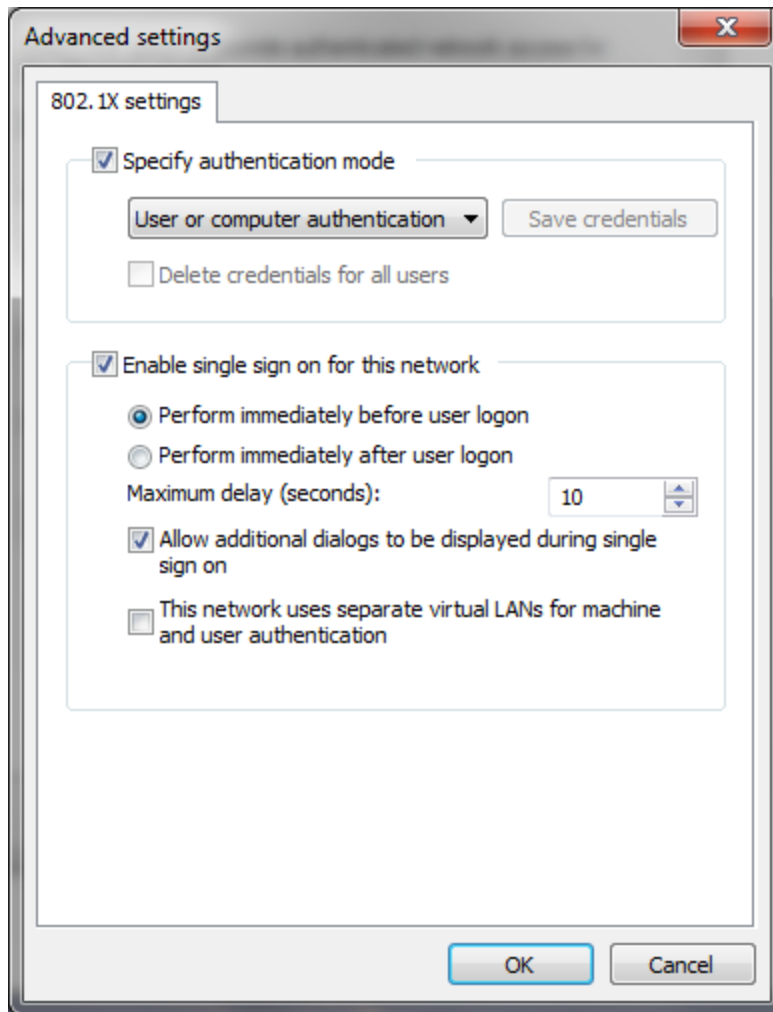
491 11. Click on **Additional Settings**.

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.





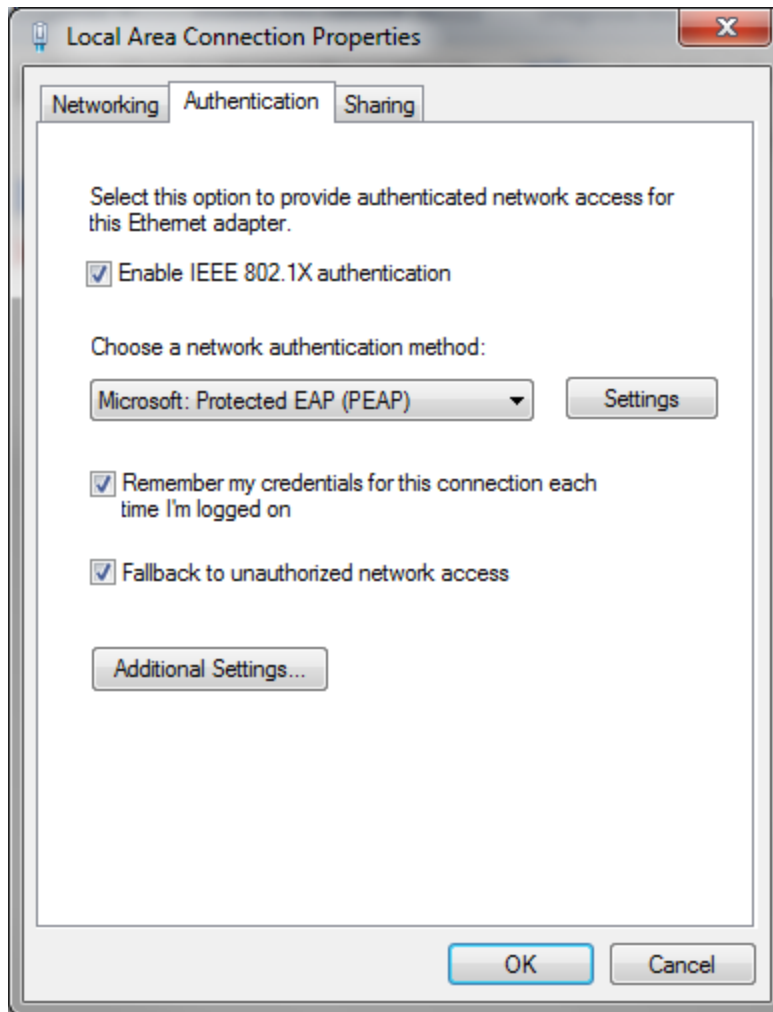
495

496

497

15. Click **OK**.

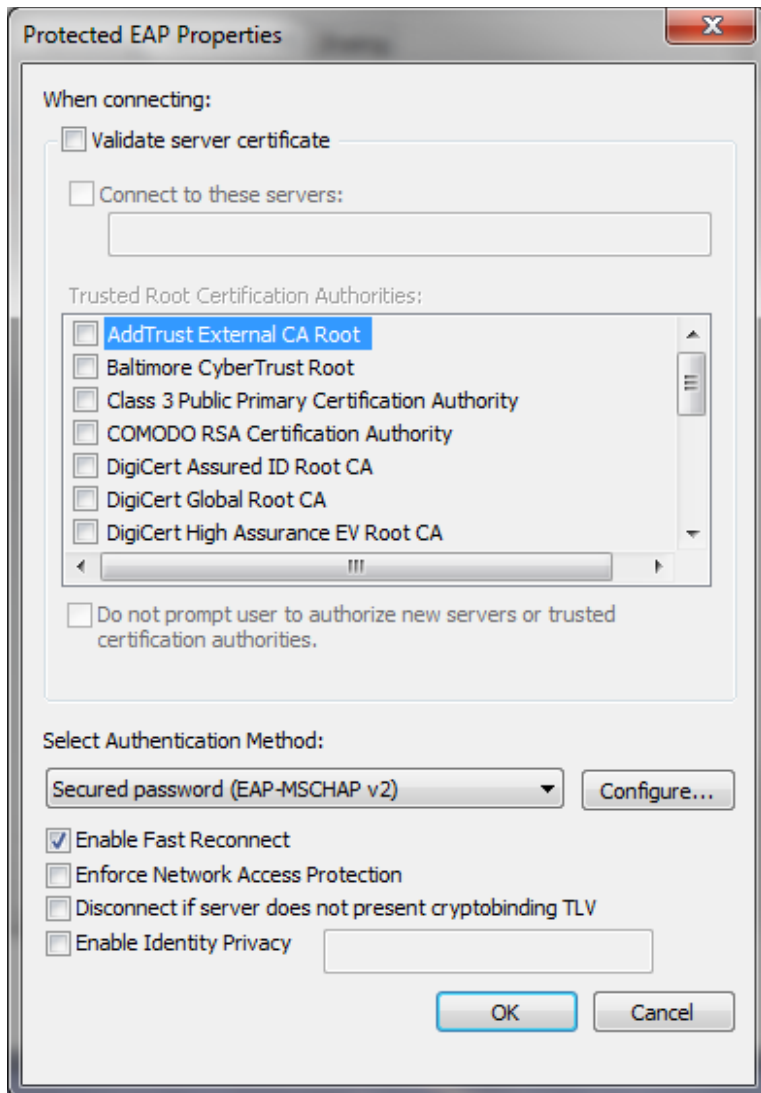
16. Click on **Settings** next to **Microsoft: Protected EAP (PEAP)**.



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.

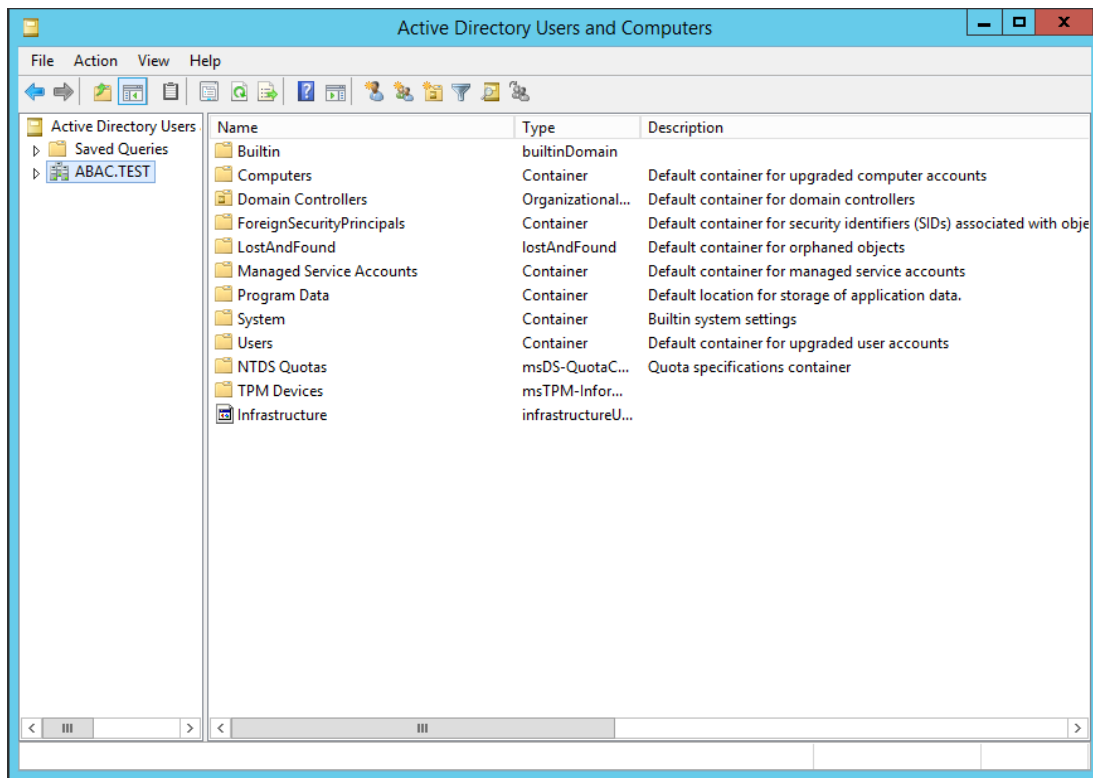
512 2. During setup, you will be asked to provide a name for your new domain.  
513 The name of the domain used for this build is **ABAC.TEST**.

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.

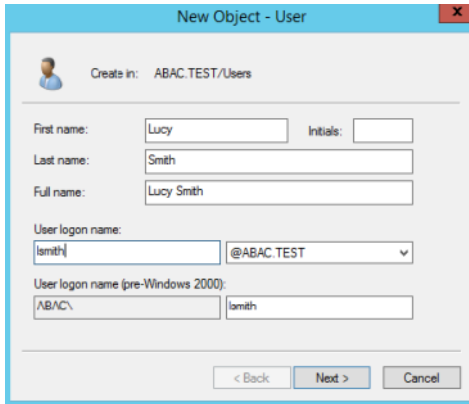


518

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).



524

525

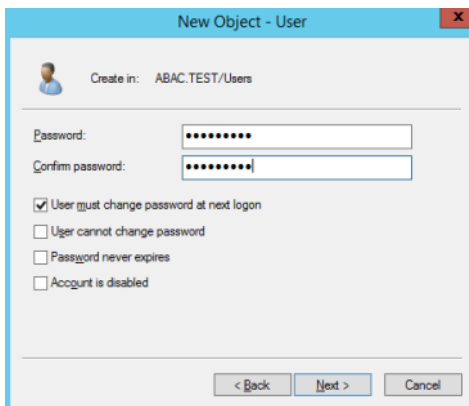
5. Click **Next**.

526

527

528

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

532

8. In the confirmation screen with information about the new user that appears, click **Finish** to complete the operation.

533

534

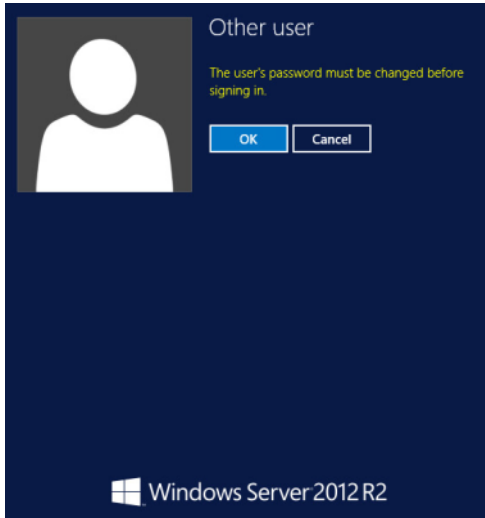
When the user logs on to the domain for the first time, the user will be prompted to create a new, unique password.

535

536

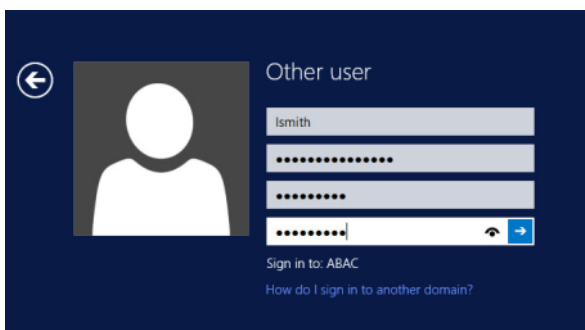
537

The following illustrations demonstrate what the new password screens may look like on Microsoft Windows Server 2012 when the user Lucy Smith attempts to log on to a computer in 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](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960xr/hardware/quick/guide/b_gsg_2960xr.html#task_0410FE6F6E3B4D9EB6175EBE40A03FD0)  
 560

- 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 [xxxxxxxxxxxxxxxxxxxx]
590 !
591 aaa session-id common
592 clock timezone EST -4 0
593 switch 1 provision ws-c2960x-24ts-1
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 5DCEEBC8 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 89EED062 64301D06
644         03551D0E 04160414 57B47B85 B93B0335 57754B92 98D87C89 EED06264 300D0609
645         2A864886 F70D0101 05050003 81810079 9AE74655 14C450FE 6F6B4E63 1CBCD9AF
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 [xxxxxxxxxxxxxxxxxxxx]
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
```

## 781 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):

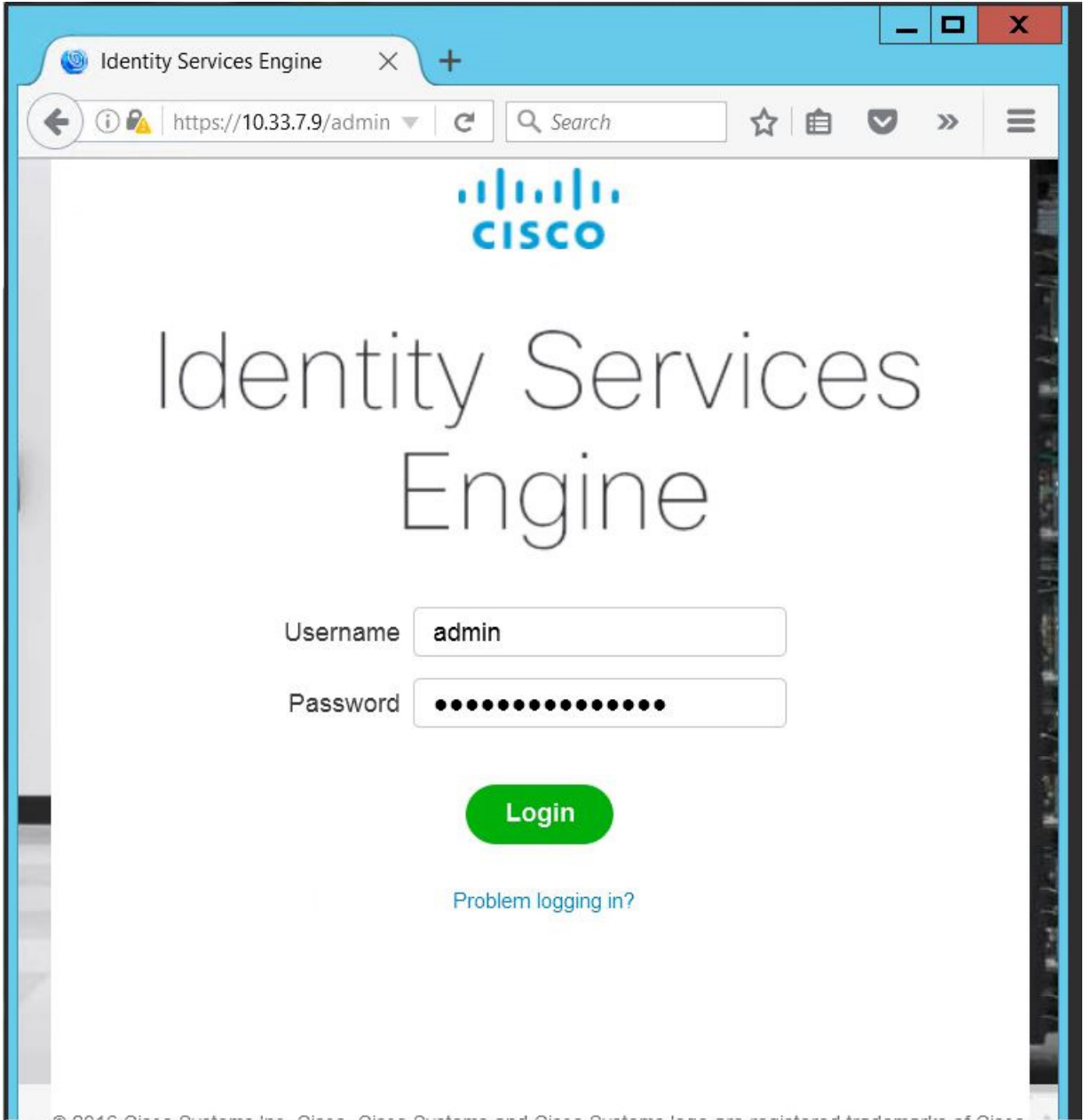
```

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

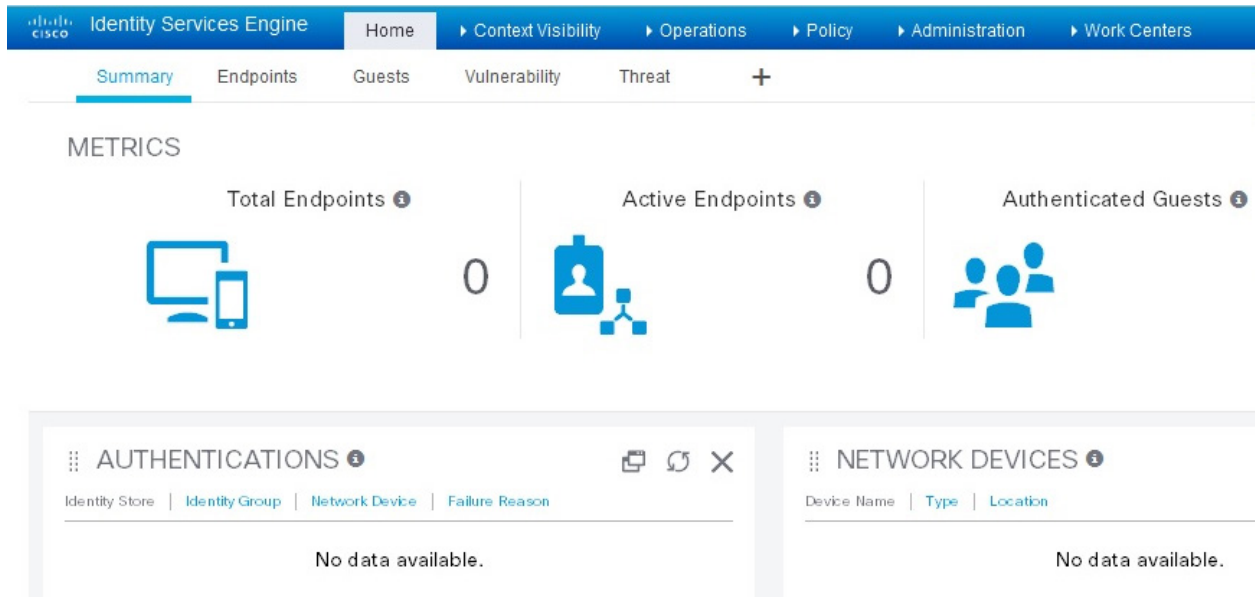
791 5. ISE will continue and create the database. ISE will automatically reboot after a successful  
792 installation. After the reboot, you can log in to ISE via any browser reachable in your domain by  
793 entering *https://<IP Address of ISE server>/admin*, as seen below:



794

795

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



796

### 797 2.6.1 Configure Cisco ISE with Microsoft AD

- 798 1. While logged in to the ISE administration console, navigate to **Administration > Identity**  
 799 **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  
 801 with Microsoft AD. Note: these instructions are in the section **Testing Environment > Cisco**  
 802 **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  
 805 existing AD domain (eg, `ciscoise_svc_account`).

### 806 2.6.2 Add Network Device to ISE

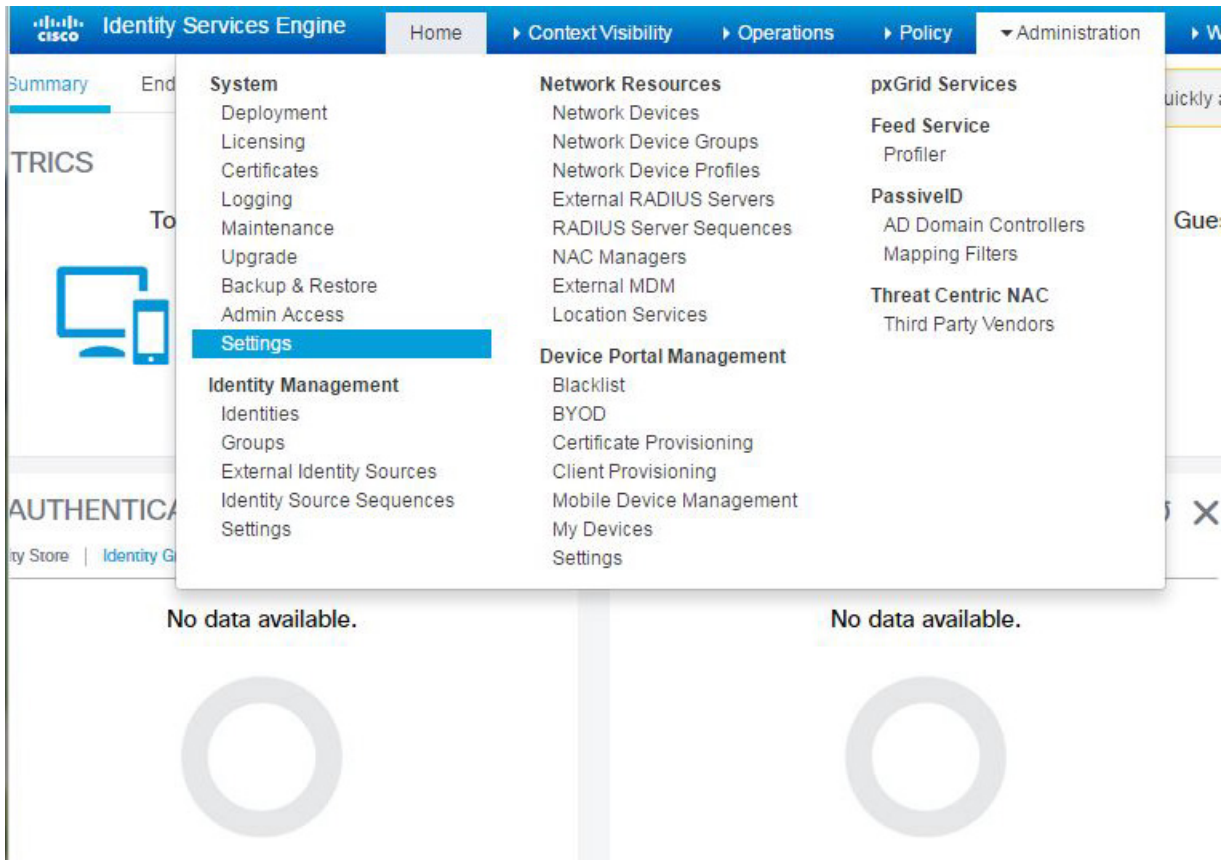
- 807 1. Follow the instructions at the link below, beginning on page 14, Steps 1-3, to register the NAD  
 808 with ISE. Note: these instructions are in the section **Testing Environment > Cisco Identity**  
 809 **Service Engine (ISE 2.0) VM Setup > Initial ISE Setup > Network Devices**.
- 810 <https://developer.cisco.com/fileMedia/download/01d139d2-c08a-4f5d-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

### 815 2.6.3 Configure ISE for pxGrid

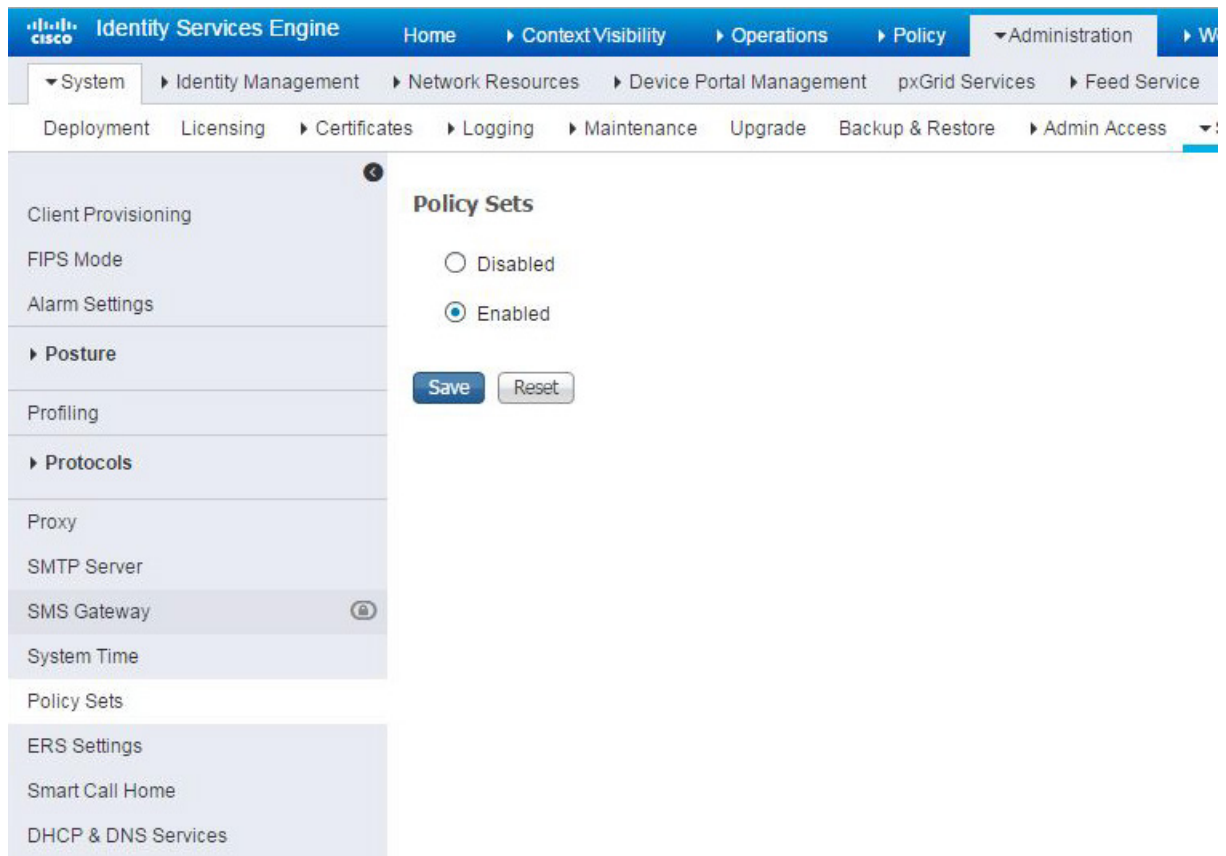
816 Follow the instructions at the link below, beginning on page 15, Steps 1-4, to enable a pxGrid persona,  
 817 used by the Situational Context Connector to query ISE for device and network attributes. Note: these  
 818 instructions are in the section **Configuring ISE for pxGrid**.

819 2.6.4 Enable ISE Policy Sets

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



- 821
- 822 2. In the left sidebar, click on **Policy Sets**.



823

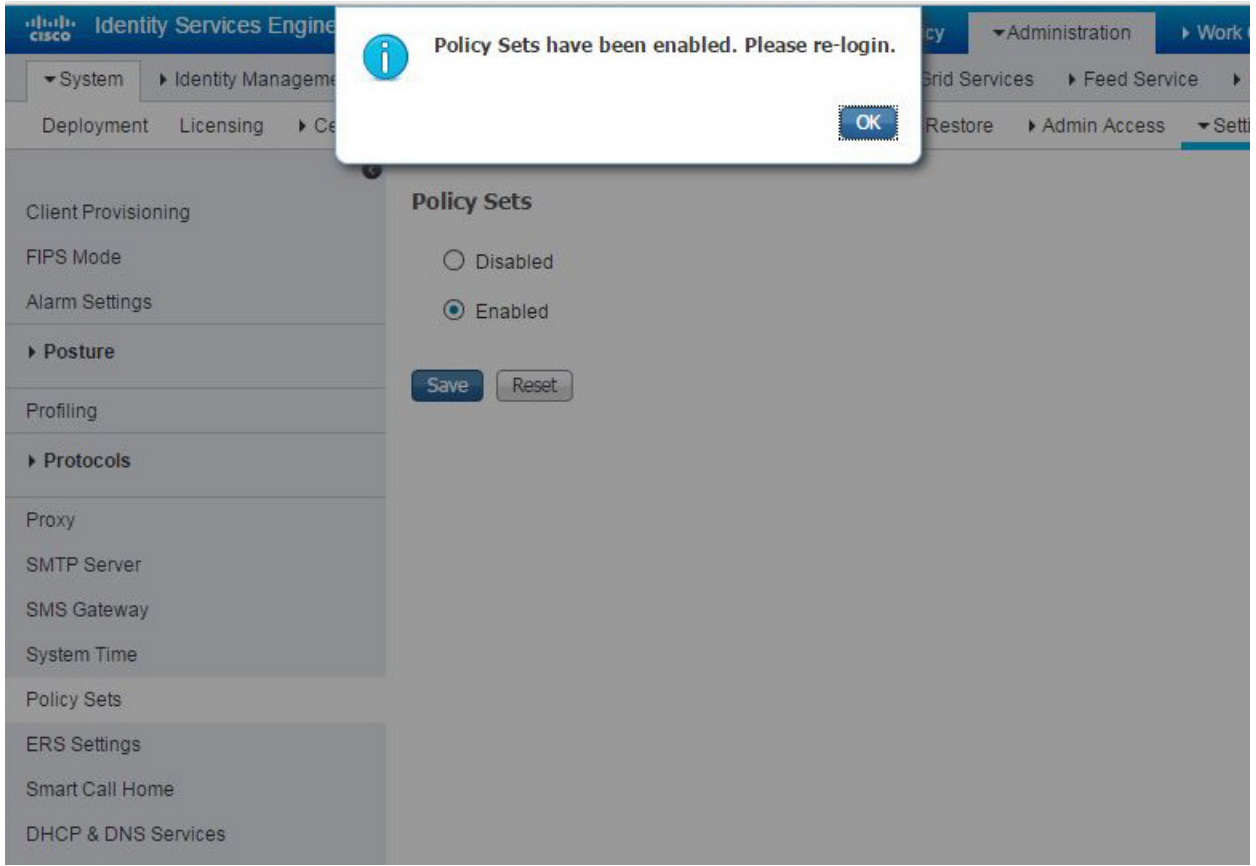
824

825

826

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

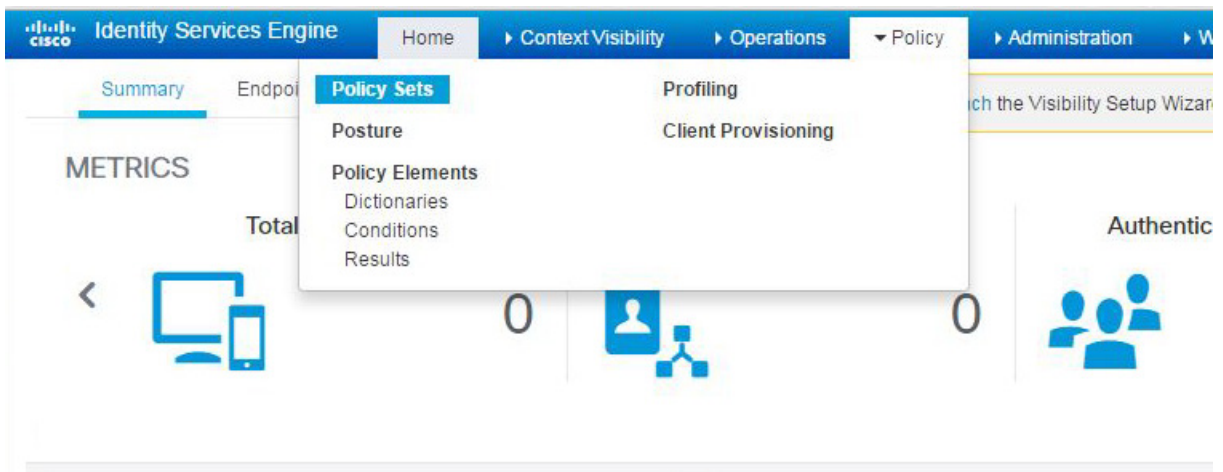




827

## 828 2.6.5 Configure Authentication Policy

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



830

- 831 2. In the left sidebar, click on **Default**.



Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
✓	Default	Default Policy Set

▼ Authentication Policy

✓	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access	and	Edit
✓	Default	: use Internal Endpoints			
✓	Dot1X	: If Wired_802.1X OR Wireless_802.1X	Allow Protocols : Default Network Access	and	Edit
✓	Default	: use All_User_ID_Stores			
✓	Default Rule (if no match)	: Allow Protocols : Default Network Access	and use : All_User_ID_Stores		Edit

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
⊗	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
⊗	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
⊗	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD
⊗	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAR)	then PermitAccess AND Guests

832

833

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

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
✓	Default	Default Policy Set

▼ Authentication Policy

✓	MAB	: If Wired_MAB OR Wireless_MAB	Allow Protocols : Default Network Access	and	
✓	Default	: use Internal Endpoints			
✓	Dot1X	: If Wired_802.1X	Allow Protocols : Default Network Access	and	
✓	Default	: Use All_User_ID_Stores			
✓	Default Rule (if no match)	: Allow Protocols : Default Network Access	and use : All_User_ID_Stores		

▼ Authorization Policy

► Exceptions (0)

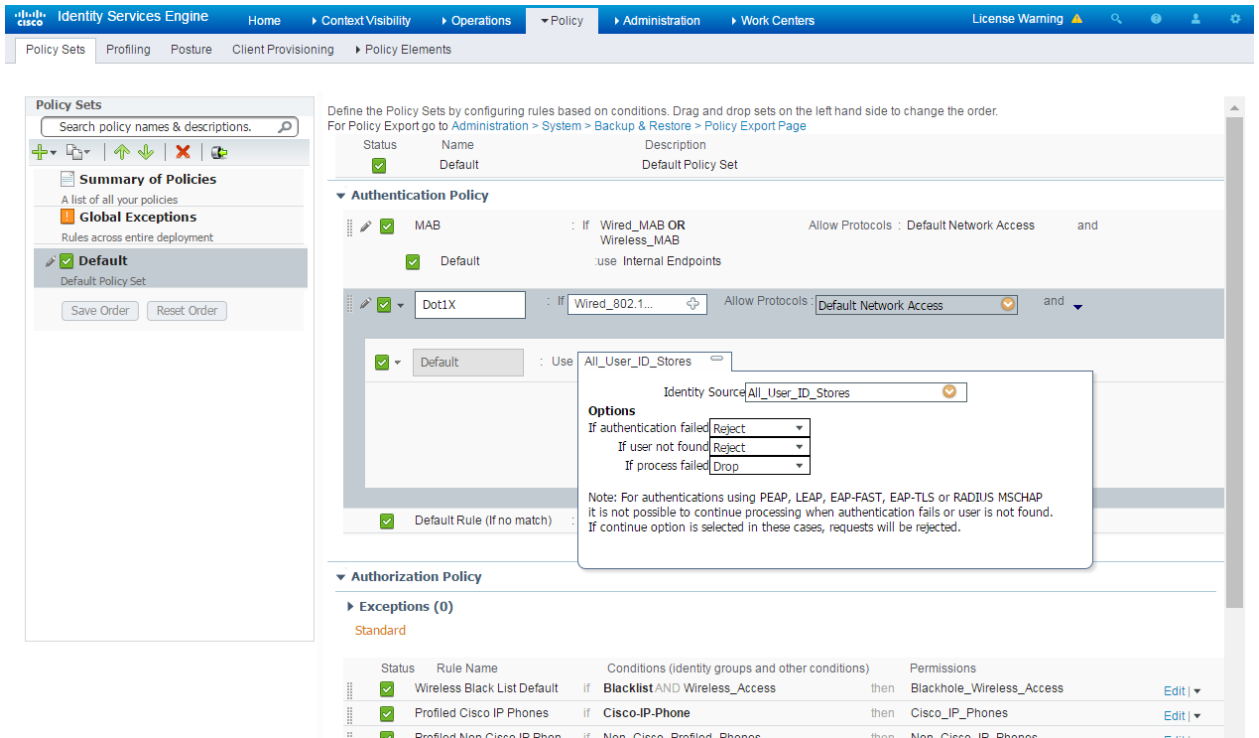
Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones

834

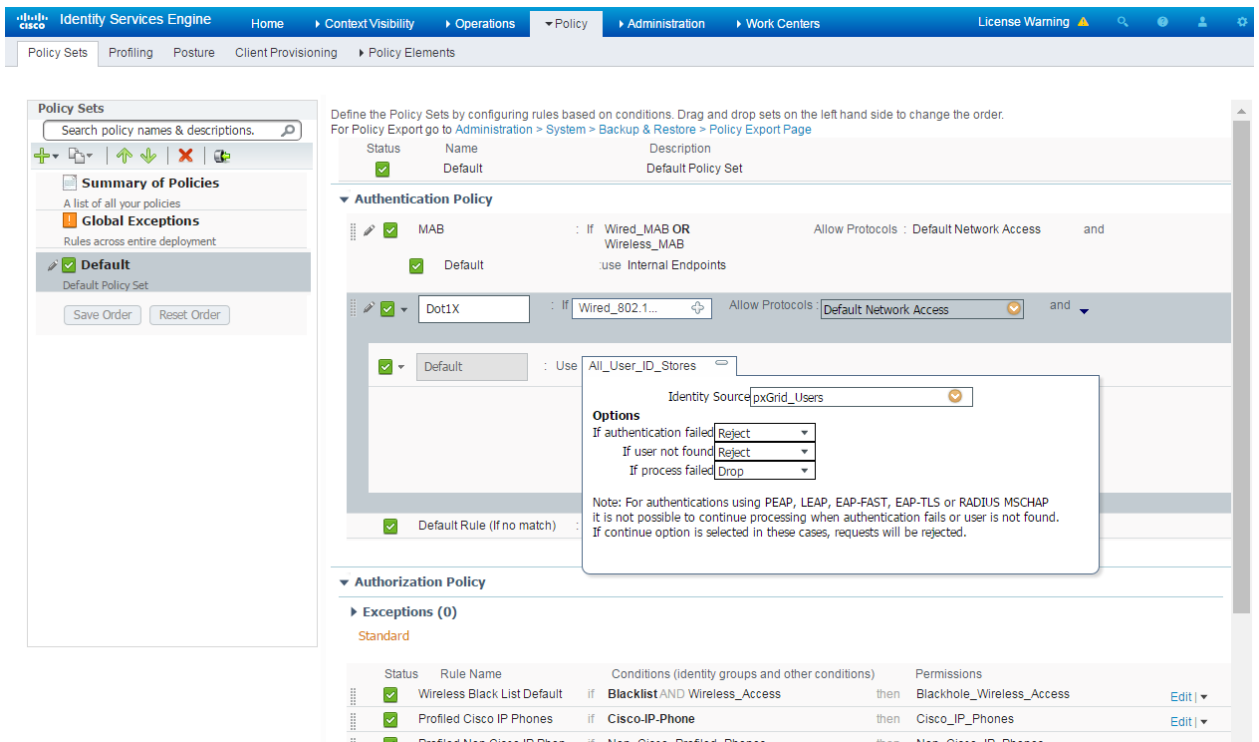
835

4. Click on the **plus icon**.



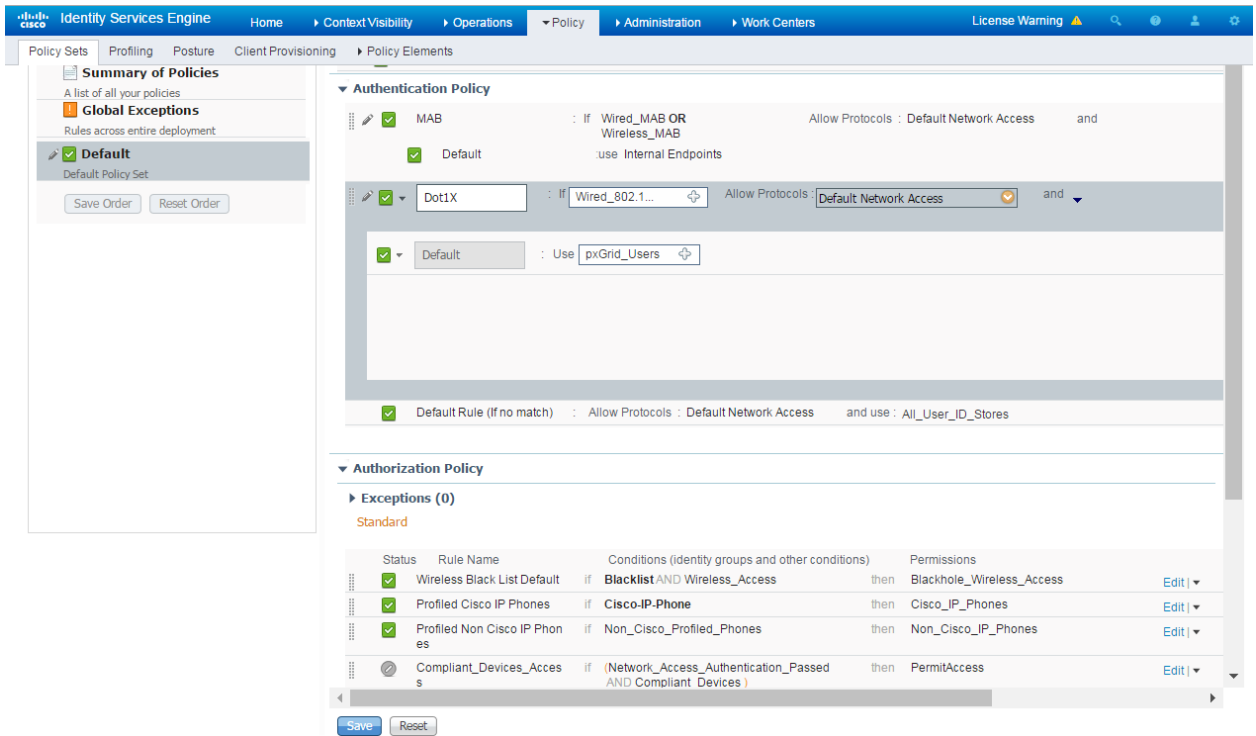
836

837 5. Change the value of Identity Source to “pxGrid\_Users.”



838

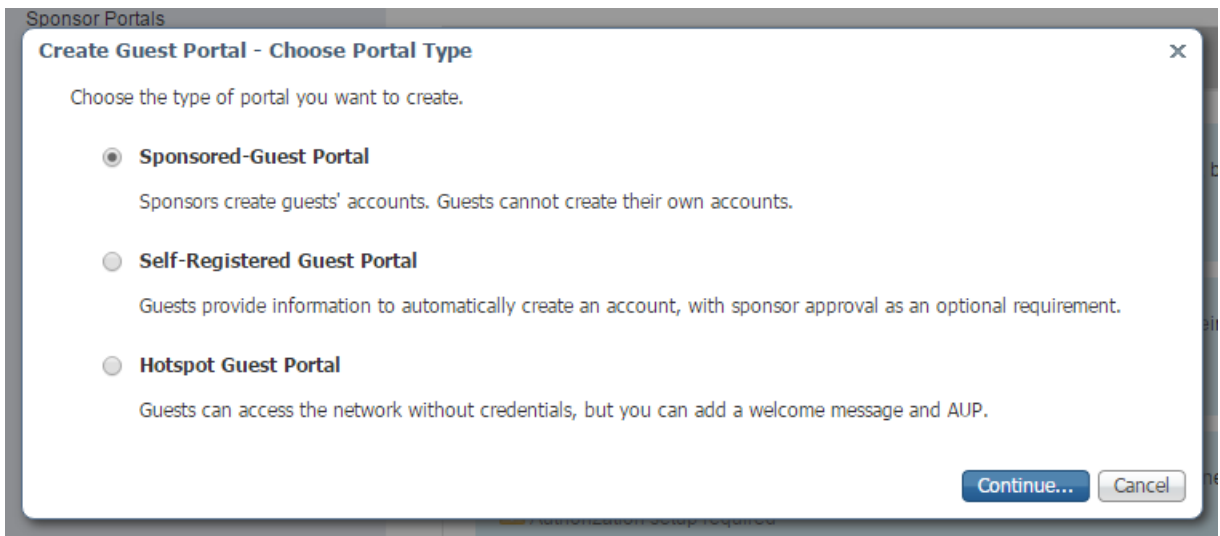
839 6. Scroll to the bottom of the page and click Save.



840

841 **2.6.6 Configure Authorization Policy**

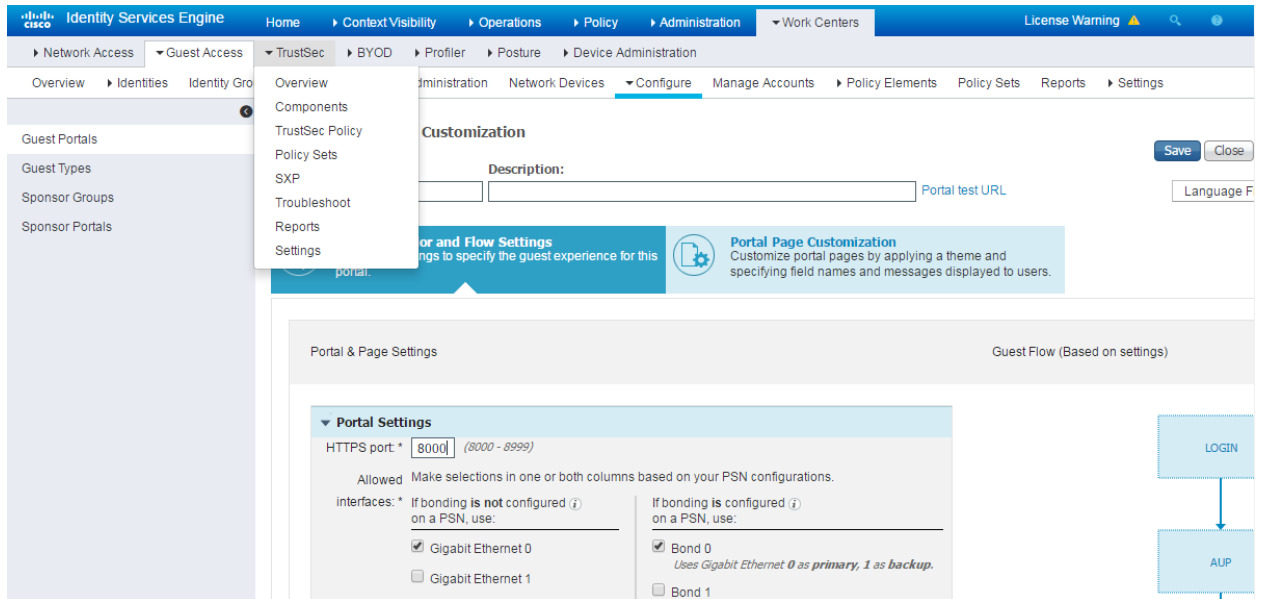
- 842 1. Navigate to **Administration > Guest Access**.
- 843 2. In the sidebar, click on **Guest Portals**.
- 844 3. Click **Create**.
- 845 4. Choose **Sponsored Guest Portal**.



846

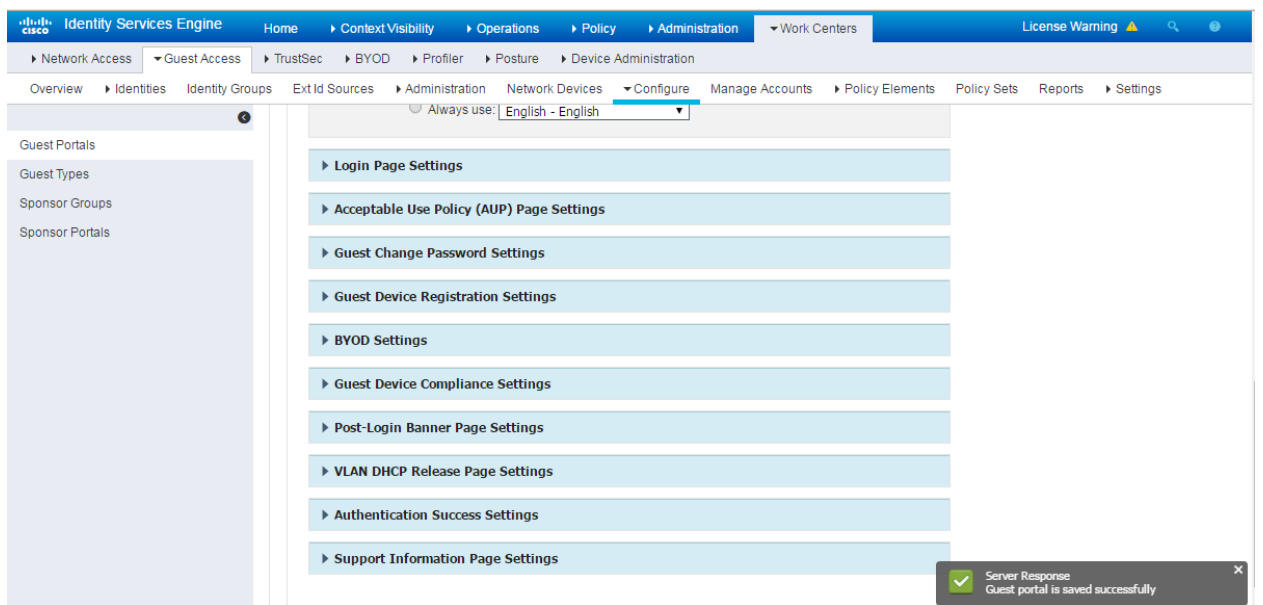
- 847 5. Click **Continue**.
- 848 6. Provide a name, **ABAC-Guest**.

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



850

851 8. Click **Save**.



852

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

**System Dictionaries**

Name	Description
<input type="checkbox"/> ACIDEX	Profiler ACIDEX
<input type="checkbox"/> ACTIVEDIRECTORY	Profiler ACTIVE
<input type="checkbox"/> APIC	Dictionary for A
<input type="checkbox"/> CDP	Profiler CDP dic
<input type="checkbox"/> CERTIFICATE	Cisco Certificate
<input type="checkbox"/> CWA	Cisco CWA Dicti
<input type="checkbox"/> CiscoPEP	Cisco PEP Dictic
<input type="checkbox"/> DEVICE	Cisco Device Dic
<input type="checkbox"/> DHCP	Profiler DHCP di
<input type="checkbox"/> ENDPOINTPURGE	Profiler ENDPOI
<input type="checkbox"/> EPS	EPS Dictionary
<input type="checkbox"/> EndPoints	System_Diction:
<input type="checkbox"/> Guest	Guest Dictionary
<input type="checkbox"/> GuestAccess	GuestAccess dic
<input type="checkbox"/> IOTASSET	Profiler IOTASSE
<input type="checkbox"/> IP	Profiler IP dictic
<input type="checkbox"/> Identity Mapping	Identity Mappin
<input type="checkbox"/> IdentityGroup	System_Diction:
<input type="checkbox"/> InternalCA	Dictionary for Ir
<input type="checkbox"/> InternalEndpoint	System_Diction:
<input type="checkbox"/> InternalUser	System_Diction:
<input type="checkbox"/> LLDP	Profiler LLDP di
<input type="checkbox"/> MAC	Profiler MAC dic
<input type="checkbox"/> MDM LOG	Dictionary for M

854

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

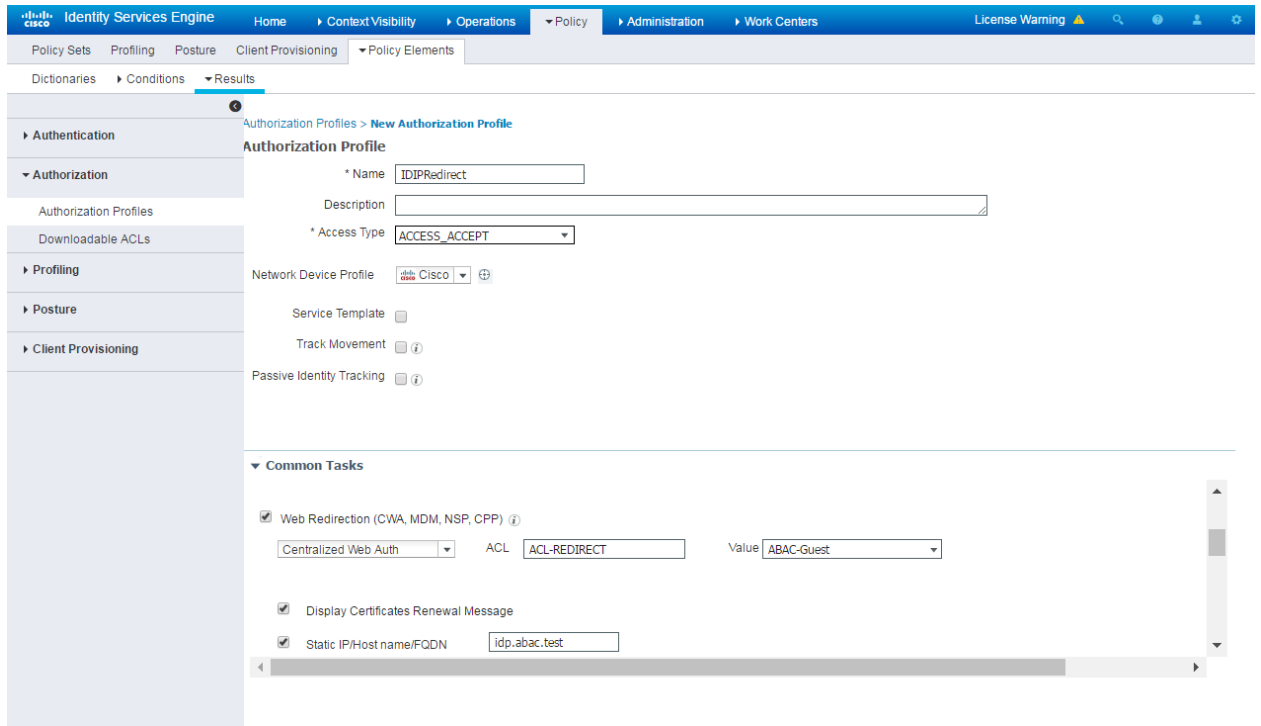
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', and 'Administration'. Below this, there are sub-menus for 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Results' sub-menu is currently selected. On the left side, there is a navigation pane with categories: Authentication, Authorization (expanded), Authorization Profiles, Downloadable ACLs, Profiling, Posture, and Client Provisioning. The main content area is titled 'Standard Authorization Profiles' and includes a sub-header 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. Below the title are action buttons: Edit, Add, Duplicate, and Delete. A table lists the following profiles:

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

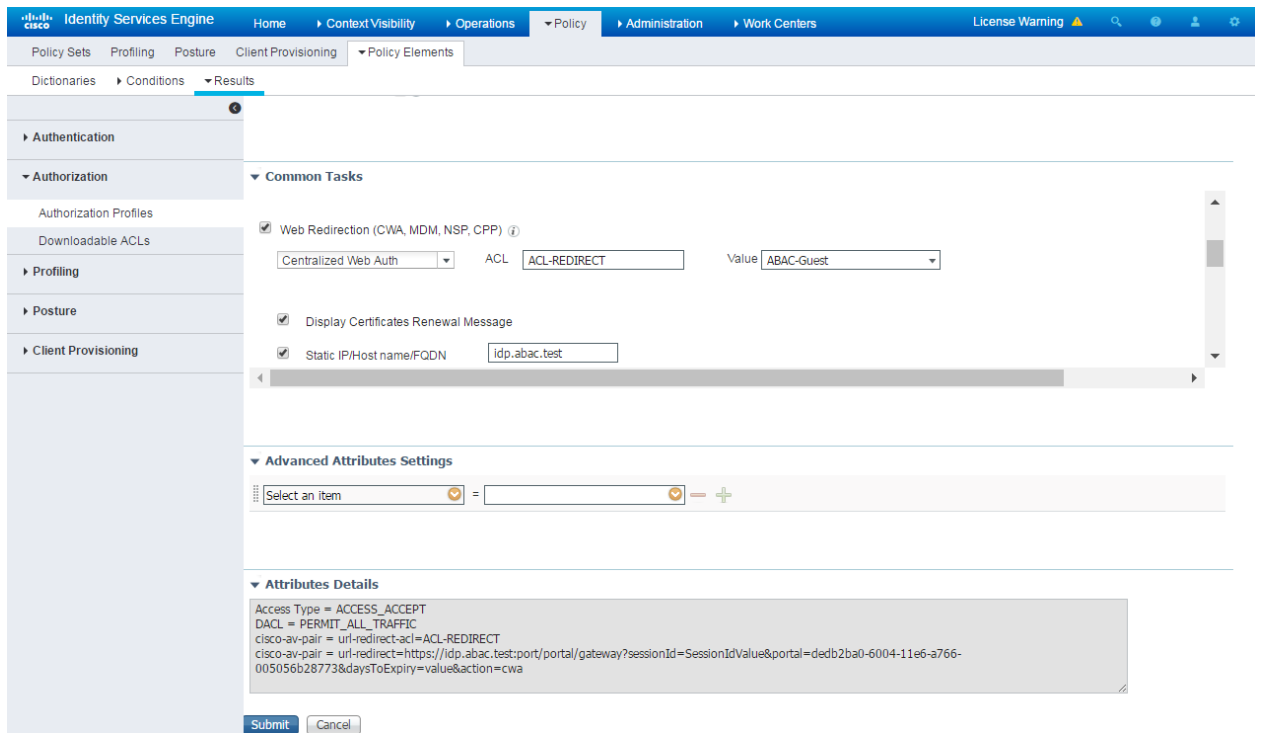
857 11. Click **Add**.858 12. In the **name field**, enter **"IDIPRedirect."**859 13. Set the **access type** to **"ACCESS\_ACCEPT."**860 14. Under **Common Tasks**, put a check next to **Web Redirection (CWA, MDM, NSP, CPP)**.861 15. In the revealed fields, choose **Centralized Web Auth**.862 16. Set 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**.

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



866

867 20. Click **Submit**.



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.

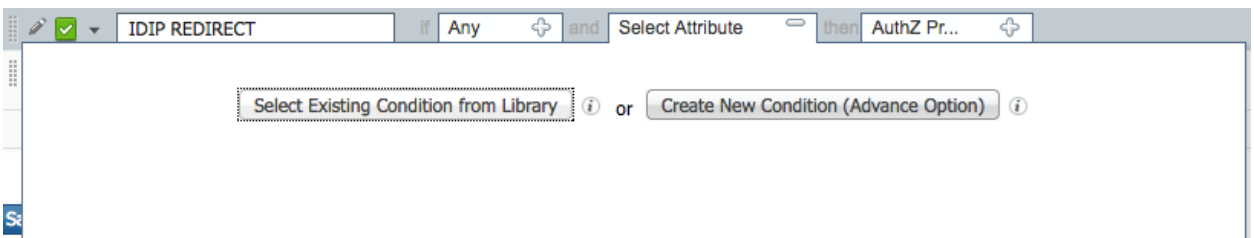
▼ Authorization Policy

► Exceptions (0)

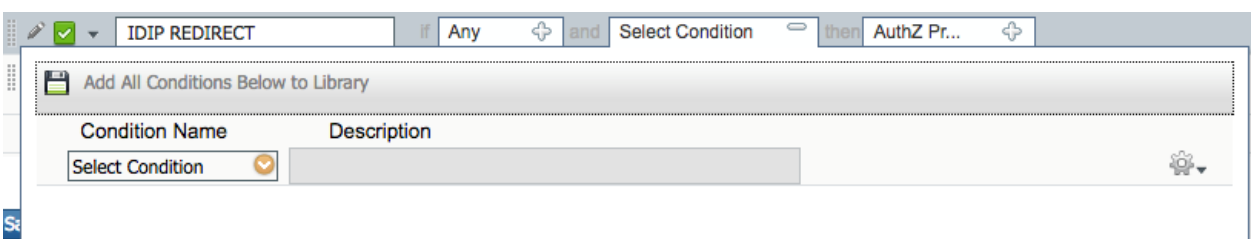
Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions	
✓	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_Access	then Blackhole_Wireless_Access	Edit   ▼
✓	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones	Edit   ▼
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Edit   ▼
⊘	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices )	then PermitAccess	Edit   ▼
⊘	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN )	then PermitAccess AND BYOD	Edit   ▼
⊘	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPV2 )	then NSP_Onboard AND BYOD	Edit   ▼
⊘	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB )	then PermitAccess AND Guest	Edit   ▼
⊘	Wi-Fi_Redirect_to_Guest_Logi n	if Wireless_MAB	then Cisco_WebAuth	Edit   ▼
✓	Basic_Authenticated_Acces s	if Network_Access_Authentication_Passed	then PermitAccess	Edit   ▼
✓	Default	if no matches, then	DenyAccess	Edit   ▼

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

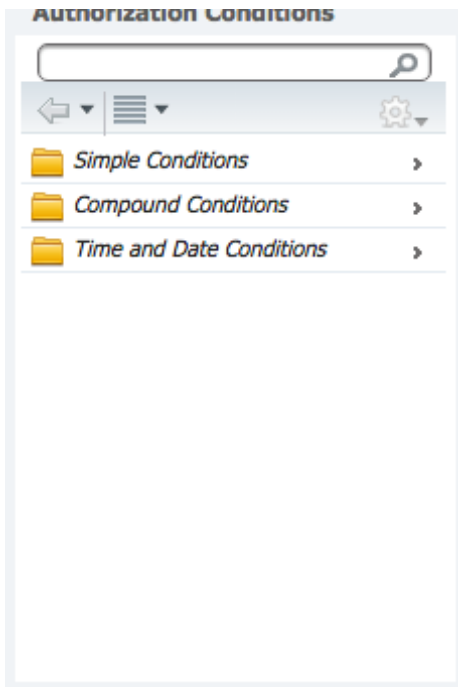


- 877
- 878 7. Click the **arrow** next to **Select Condition**



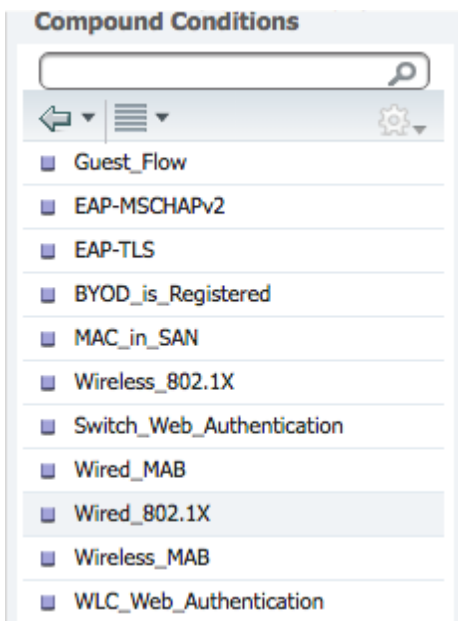
- 879
- 880 8. Choose **Compound Conditions.**





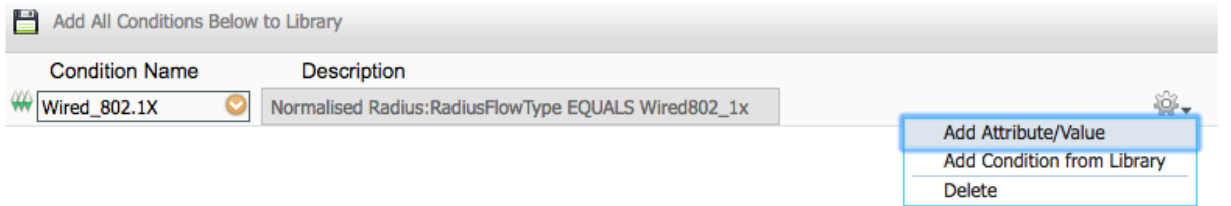
881

882 9. Choose **wired\_802.1x**.



883

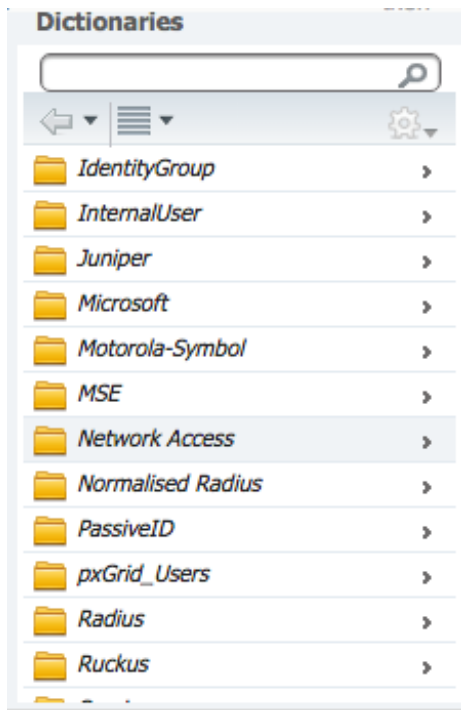
884 10. Click the **cog icon**.



885

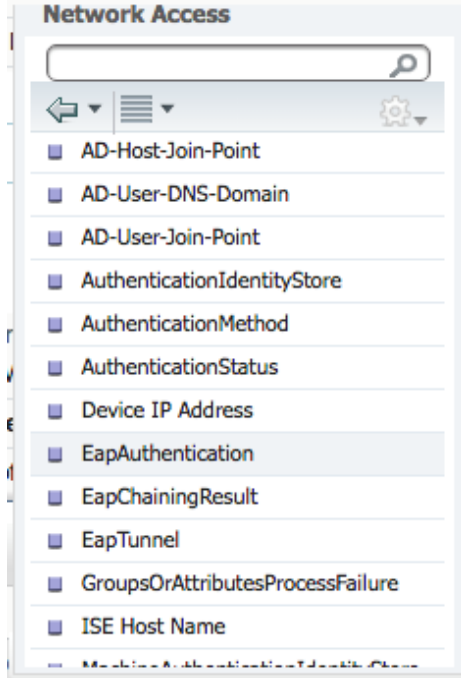
886 11. Choose **Add Attribute/Value**.

887 12. Select **Network Access**.



888

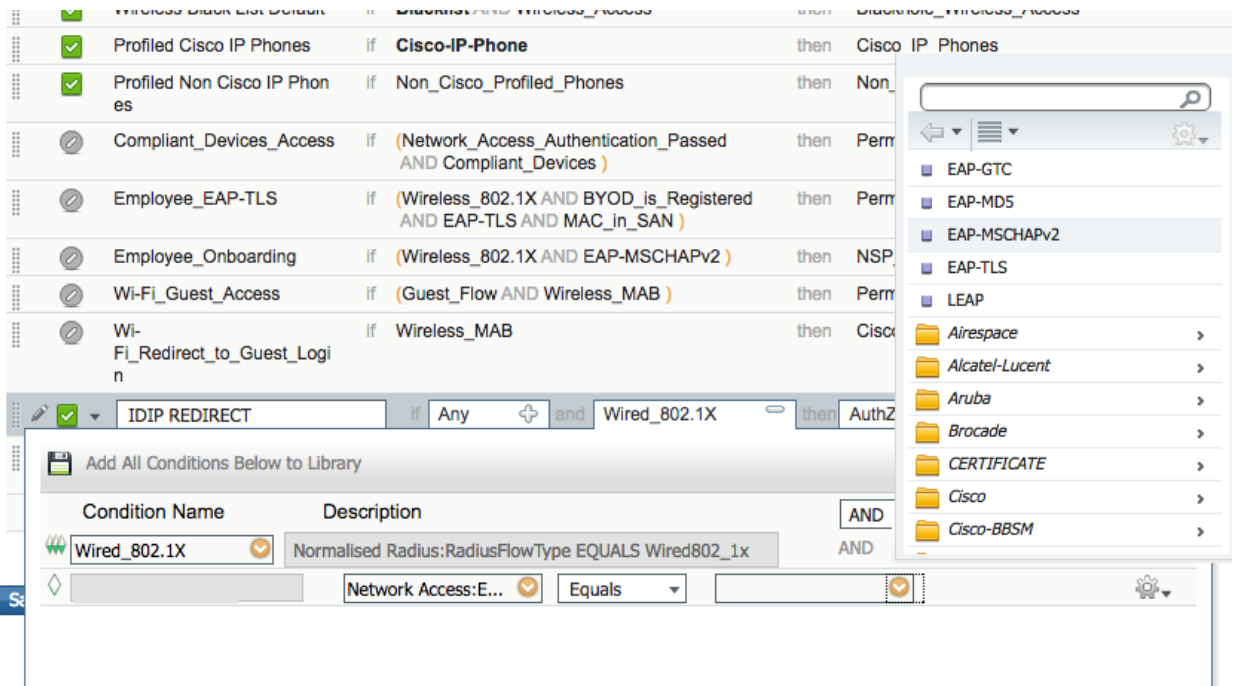
889 13. Select **EapAuthentication**.



890

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

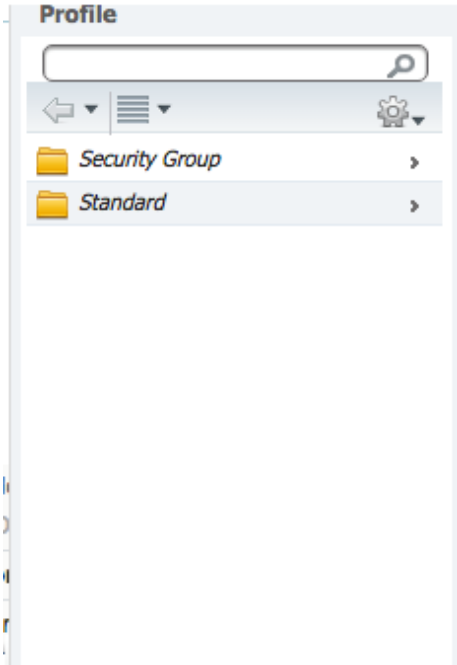
892 15. Select **EAP-MSCHAPv2**.



893

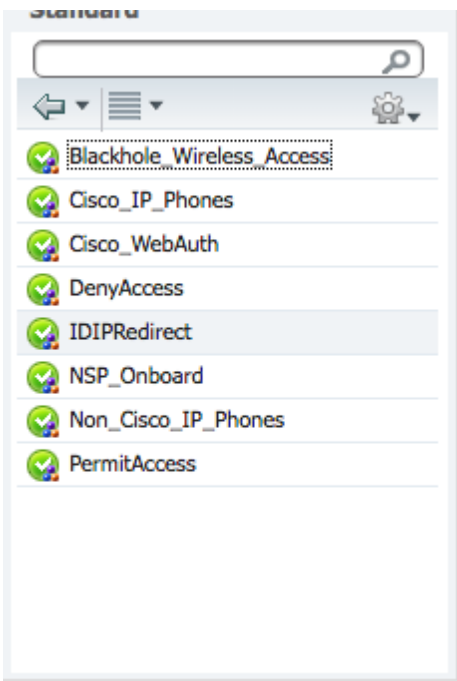
894 16. Click the **plus icon** in the **then** box.

895 17. Select **Standard**.



896

897 18. Select **IDIPRedirect**.

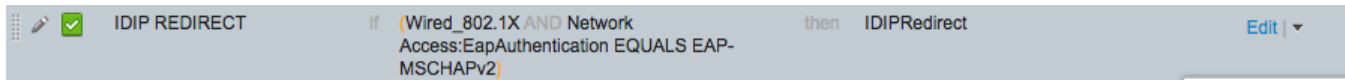


898

The screenshot displays a network policy configuration window. On the left, a list of policies is visible, including 'Compliant\_Dev', 'Employee\_EAP', 'Employee\_Ont', 'Wi-Fi\_Guest\_A', and 'Wi-Fi\_Redirect\_to\_n'. The main area shows a rule configuration for 'IDIP REDIRECT'. The rule is active, indicated by a green checkmark. The conditions are 'if Any' and 'and Wired\_802.1X...'. The action is 'then IDIPRedirect'. A dropdown menu is open, showing 'IDIPRedirect' as the selected action.

899

900 19. Click **Done**.



901

902 20. Click **Save**.

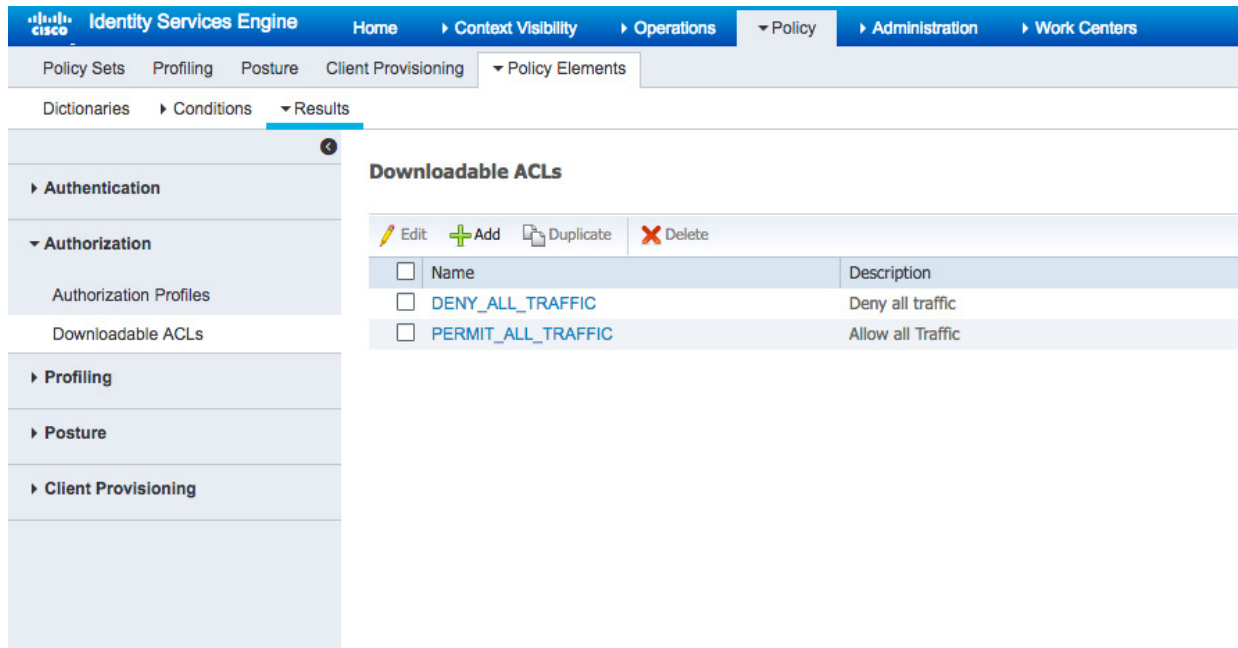


903

### 904 Machine Authorization Policy Rule

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

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



907

- 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
    
```

[▶ Check DACL Syntax](#) ⓘ

- 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**.

<input checked="" type="checkbox"/>	IDIP REDIRECT	if (Wired_802.1X AND Network Access:EapAuthentication EQUALS EAP-MSCHAPV2)	then	IDIPRedirect	<a href="#">Edit</a>
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then	PermitAccess	<a href="#">Insert New Rule Above</a> <a href="#">Insert New Rule Below</a> <a href="#">Duplicate Above</a> <a href="#">Duplicate Below</a> <a href="#">Delete</a>
<input checked="" type="checkbox"/>	Default	if no matches, then		DenyAccess	

- 917
- 918 31. Enter **Wired Machine** for the name.
- 919 32. Click the **plus button** next to condition.
- 920 33. Choose **Create New Condition**.

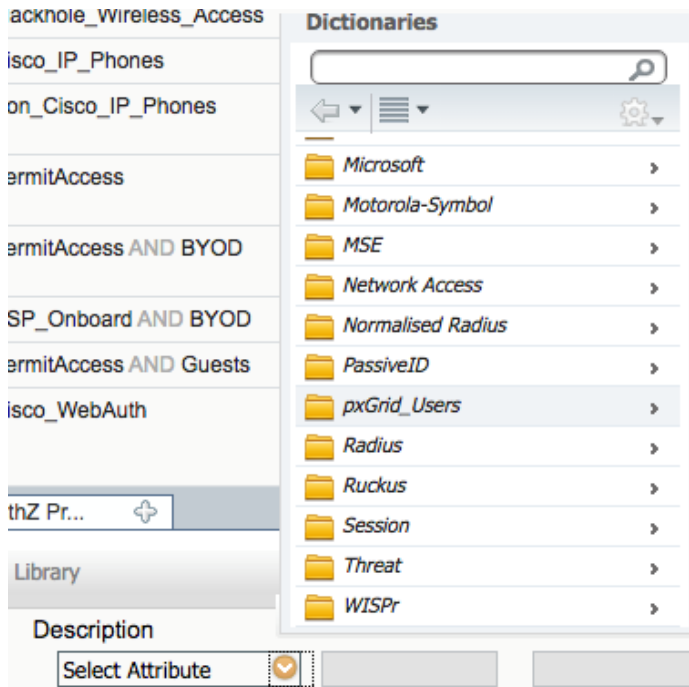
Select Attribute  [+](#)

ⓘ or  ⓘ

921

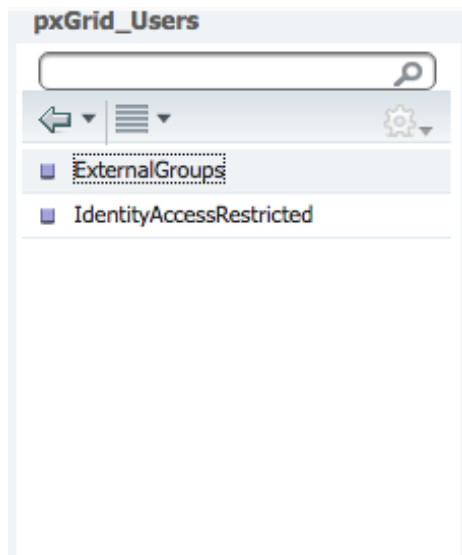
922 34. In the Select Attribute box, click the **arrow**.

923 35. Select **PxGrid\_Users**.



924

925 36. Select **ExternalGroups**.

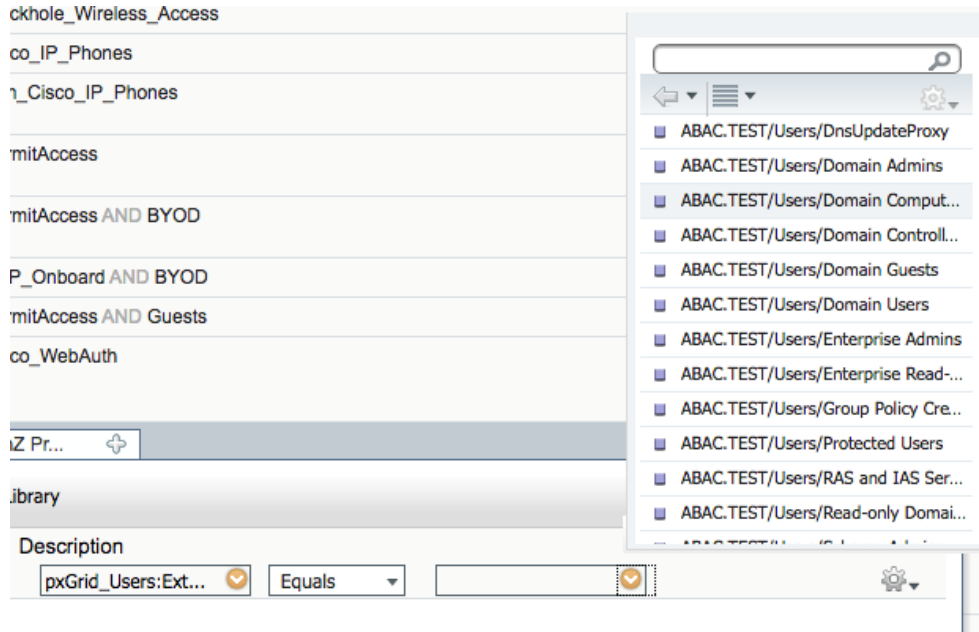


926

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

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





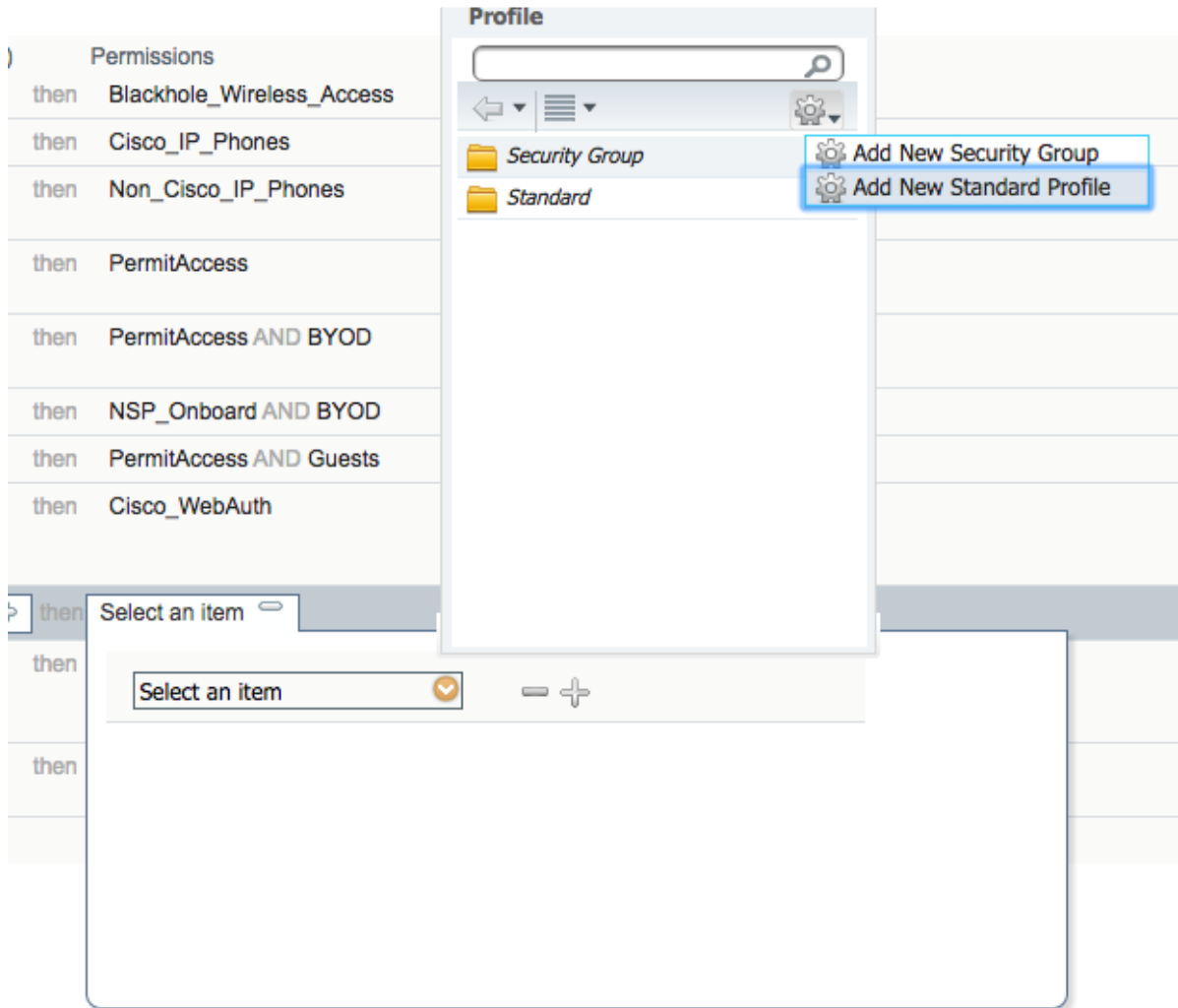
929

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**.



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.


**Add New Standard Profile**

**Authorization Profile**


\* Name


Description

\* Access Type

Network Device Profile  Cisco

Service Template

Track Movement  

Passive Identity Tracking  

---

**Common Tasks**

**DACL Name**



ACL (Filter-ID)

VLAN

Voice Domain Permission

---

**Advanced Attributes Settings**

 =   - +

938

939

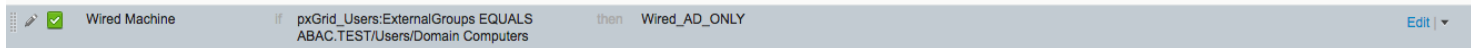
46. Click **Save**.

940

 **Authorization Profile "Wired\_AD\_ONLY" is created successfully.**



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

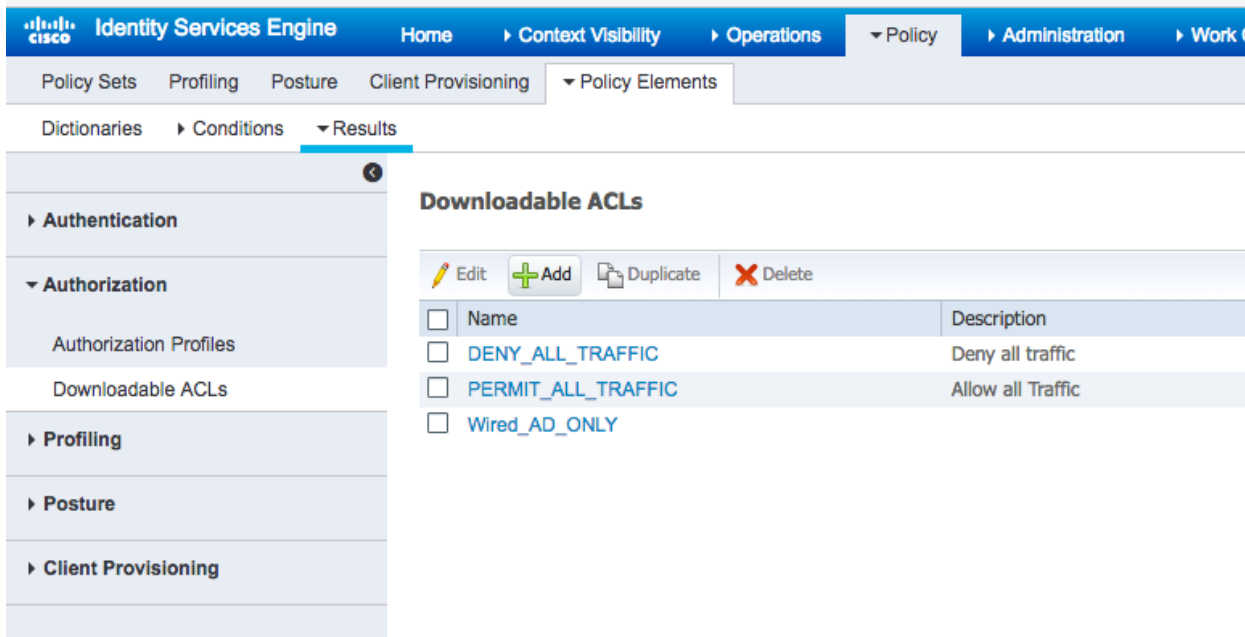


942

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**.



946

- 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

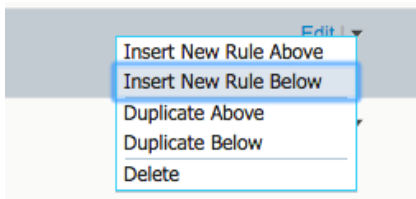
Description

\* DACL Content

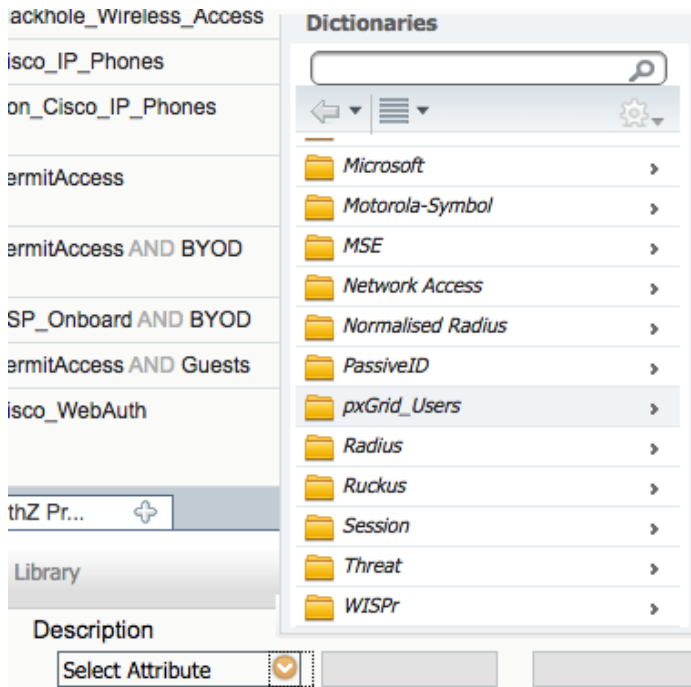
1	permit ip any any
2	
3	
4	
5	
6	
7	
8	
9	
10	

▶ Check DACL Syntax ⓘ

- 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**.

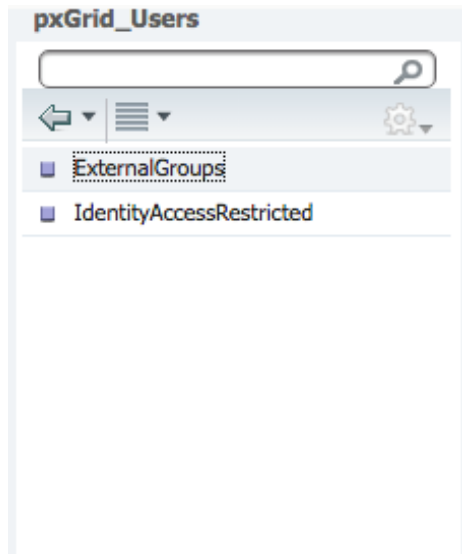


- 956
- 957 58. In the name field, type **Wired User**.
- 958 59. Click the **plus icon** in the condition box.
- 959 60. Select **Create New Condition**.
- 960 61. In the Select Attribute box, click the **arrow**.
- 961 62. Select **PxGrid\_Users**.



962

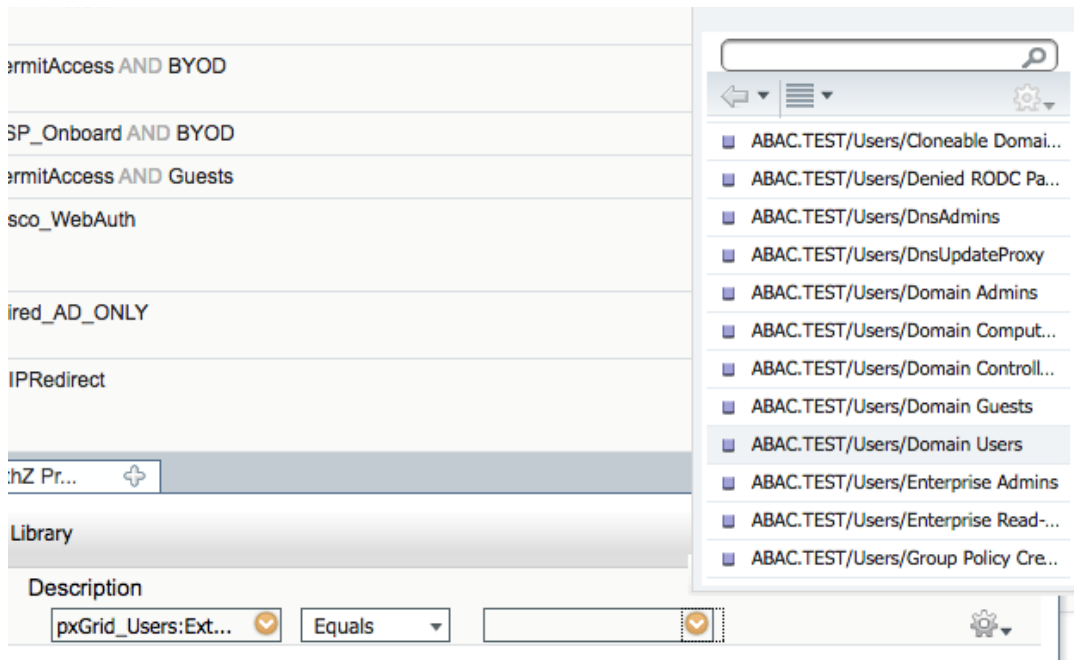
963 63. Select **ExternalGroups**.



964

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

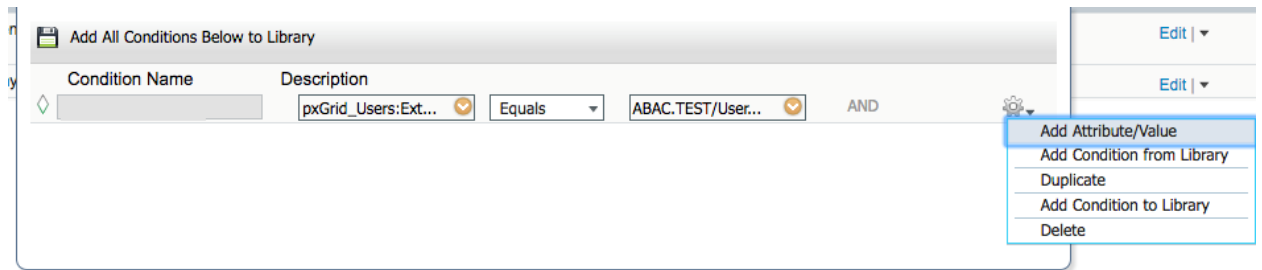
966 65. Select **ABAC.TEST/USERS/Domain Users**.



967

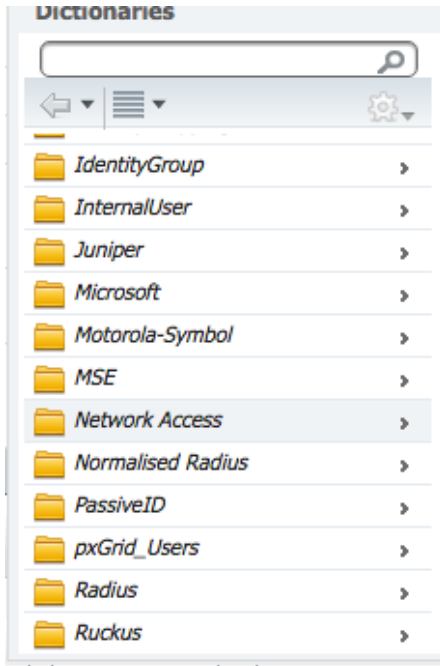
968 66. Click the cog.

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



970

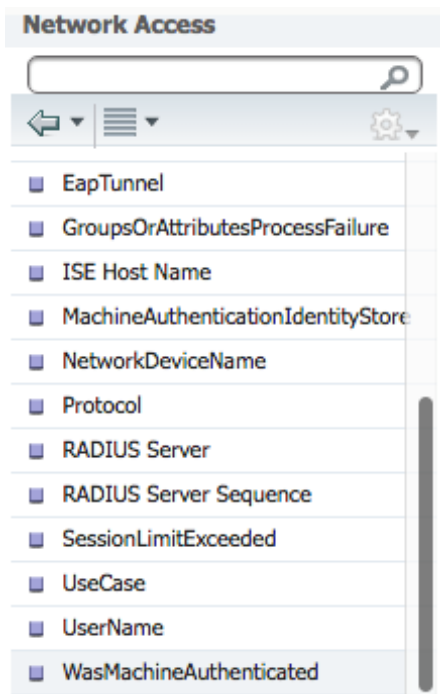
971 68. In the new attribute box, select **Network Access**.



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

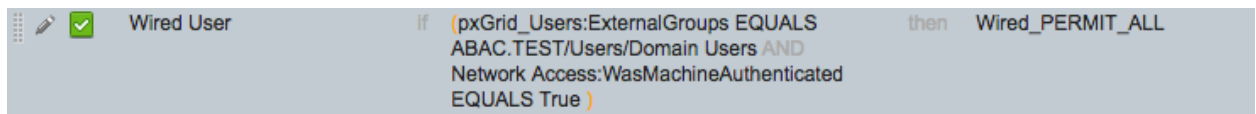
73. Click the **cog**.



- 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.



- 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**.



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.

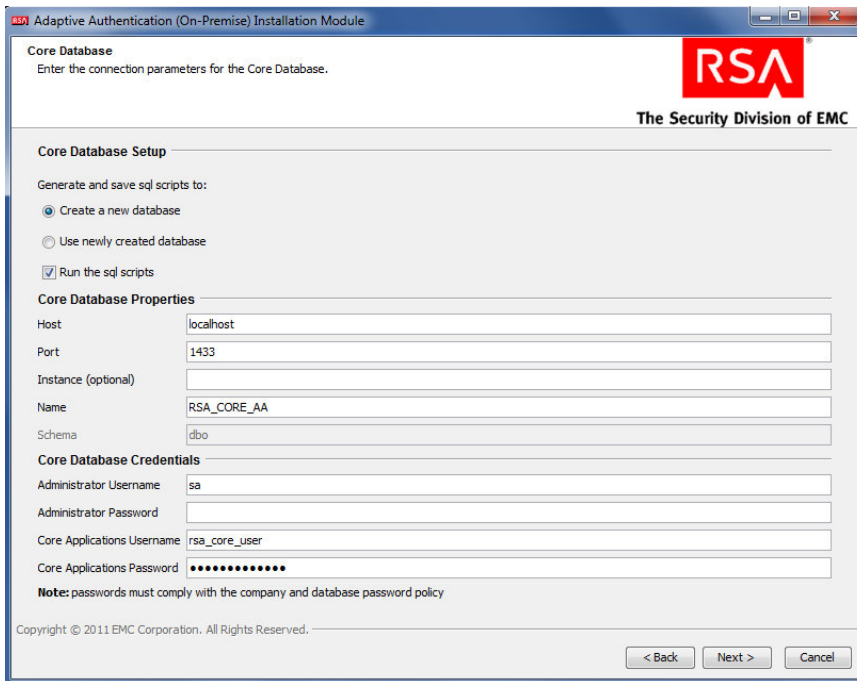


1002

1003

1004

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

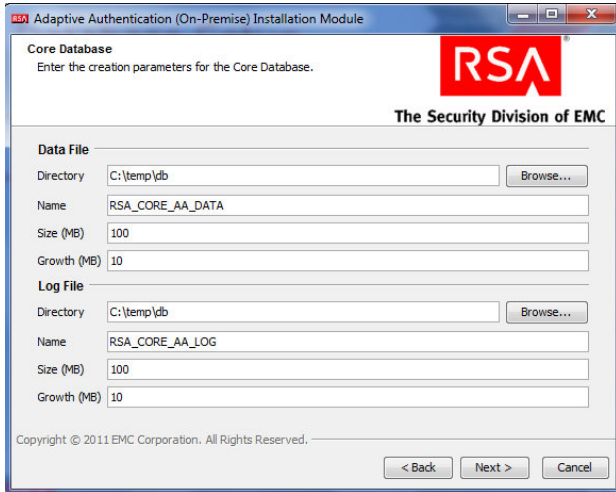


1005

1006

1007

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



1008

1009

1010

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



1011

1012

1013

1014

1015

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



1016

1017

1018

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



1019

1020

## 2.8 Configure RSA AA Rules

1021

1022

1023

1024

1025

1026

1027

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

## 1028 2.8.1 Create Rule for Non-Persistent User Enrollment

1029 RSA AA requires information for each user to help verify their identity. These users are classified into  
 1030 two groups: persistent and non-persistent users. A rule is created to request enrollment information for  
 1031 non-persistent users, those not kept in the user database.

- 1032 1. Log in to the Back Office application  
 1033 [http://xxx.xxx.xxx.xxx:8080/backoffice]
- 1034 2. Once logged in, click **Manage Rules** under **Policy Management**. Select **New Rule**.
- 1035 3. In the **Rule Details** (in the **General** tab):
  - 1036 a. Set **Rule Name** to **User Enrollment Not Persistent - Adapter**.
  - 1037 b. Set the **Status** to **Production**.
  - 1038 **Note:** The rule cannot be in production until it is created and approved by an  
 1039 administrator.
  - 1040 c. In **Event Type**, select **Create User** and **Enroll**.
  - 1041 d. Set the **Order** to **1**.

Policy Management Administration Customer Service

Edit Rule

1: General 2: Conditions 3: Actions Summary

Define the general details for this rule.

Rule Details

• Rule Name: User Enrollment Not Persistent - Adapter

Description:

• Status: Production [?]

Comment:

• Event Type:

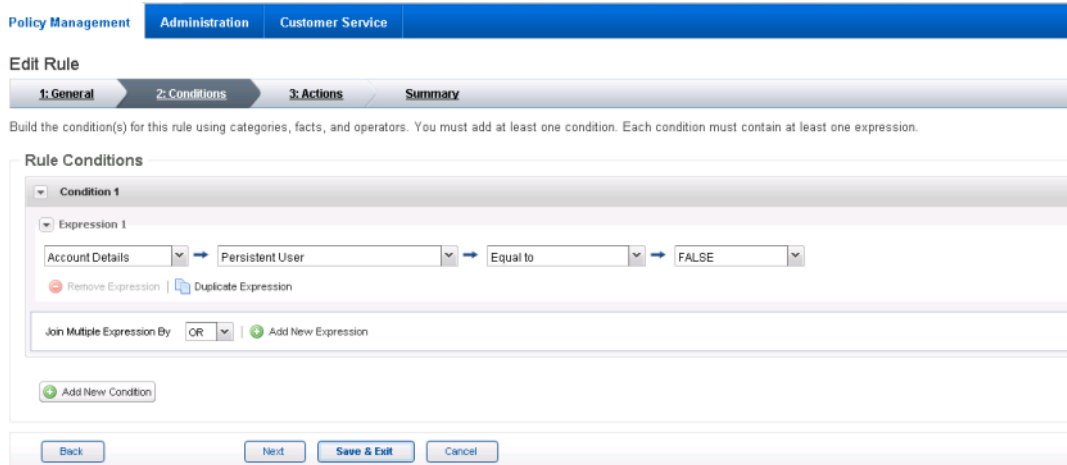
Event Type
<input type="checkbox"/> CHANGE_PHONE
<input type="checkbox"/> CHANGE_STATEMENT_SETTINGS
<input type="checkbox"/> CHANGE_STU
<input checked="" type="checkbox"/> CREATE_USER
<input type="checkbox"/> DEPOSIT
<input type="checkbox"/> EDIT_PAYEE
<input checked="" type="checkbox"/> ENROLL
<input type="checkbox"/> EXTRA_AUTH

• Order: 1 Available Range: 1 - 22 [?]

Next Save & Exit Cancel

• Required Field

- 1042
- 1043 4. Click **Next**.
- 1044 5. In the **Rule Conditions** page, add a condition (**Condition 1**) and with one expression  
 1045 (**Expression 1**). Set **Expression 1** to **Account Details** such that **Persistent User** is **Equal to FALSE**.



1046

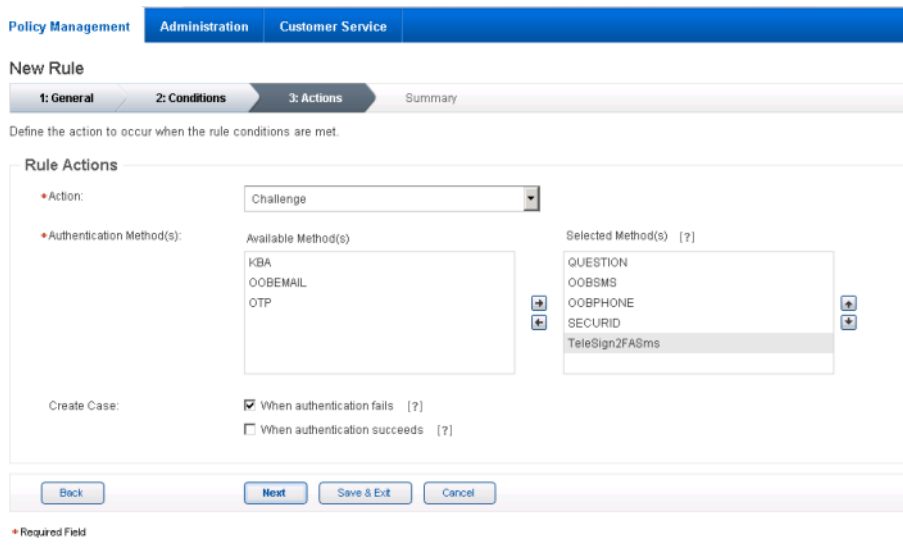
1047 6. Click **Next**.

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

1049 a. Set **Action** to **Challenge**.

1050 b. Set **Authentication Methods** to **QUESTION, OOB SMS, OOB PHONE, SECURID, and**  
 1051 **TeleSign2FASms**.

1052 c. In **Create Case**, make sure that only **for when authentication fails** is selected.  
 1053 Then, click **Next**.

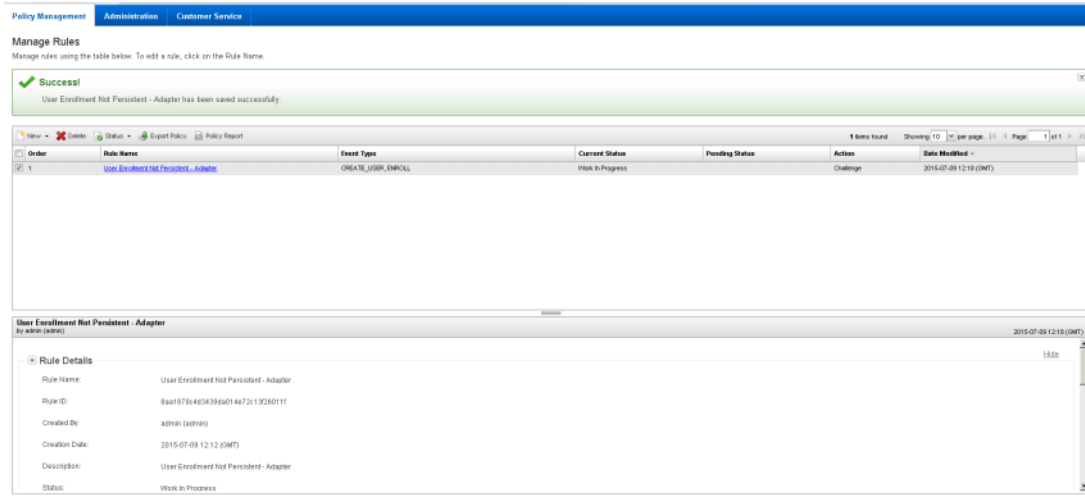


1054

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.



1058

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

1060 **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

1064 **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**

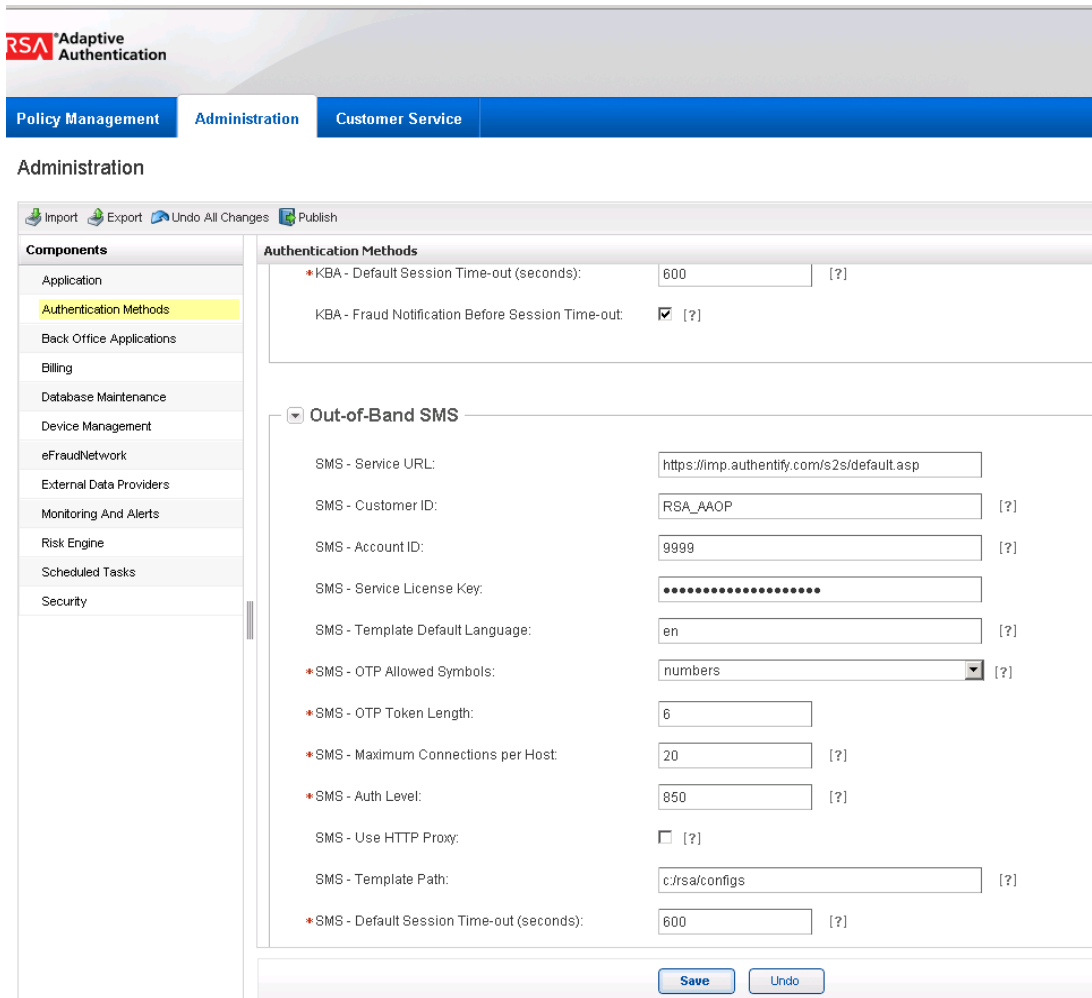
Rule Name	Challenge SMS for Payment
Event Type	Challenge
Rule Order	4
Rule Condition	IF (Transaction Details > Transaction Amount is BETWEEN 5000 and 10000)
Rule Action	Allow
Authentication Method	1. OOB SMS
Create Case	When Authentication Succeeds

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**



1080 \* Required Field

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

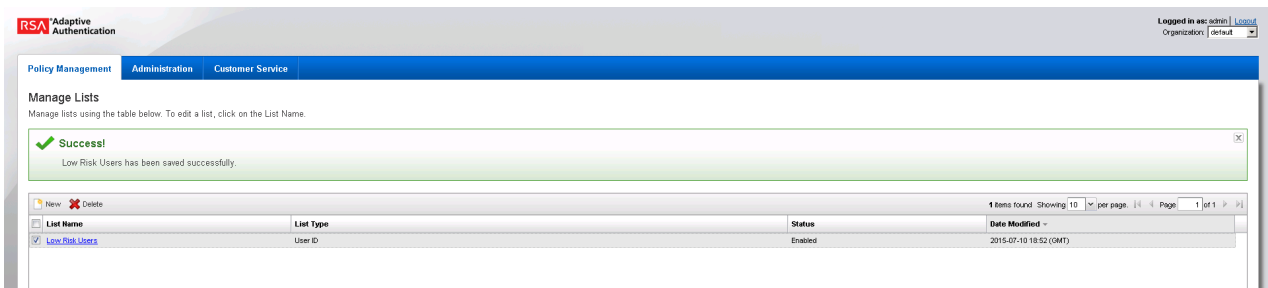
1082 The following rules create different sign-in scenarios for users based on an RSA-generated risk score at  
 1083 the time of login. RSA AA uses a risk engine to give users a risk score to determine a level of trust at the  
 1084 time of access. See the tables in [Section 2.8.8](#) for the session 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
- 1092 **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**



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**.

**Custom Fact Details**

Category: Custom Facts

\* Fact Name: FORCE WORKFLOW [?]

\* Field Type: String [?]

\* Status: Enabled [?]

Description: [?]

Save Cancel

1114

1115 4. Click **Save**.

**Manage Custom Facts**

Manage custom facts using the table below. To edit a fact, click on the Custom Fact Name. You may manage up to 1000 custom facts.

**Success!**  
FORCE WORKFLOW has been saved successfully.

Custom Fact Name	Fact Type	Status	Date Modified
<a href="#">FORCEWORKFLOW</a>	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.

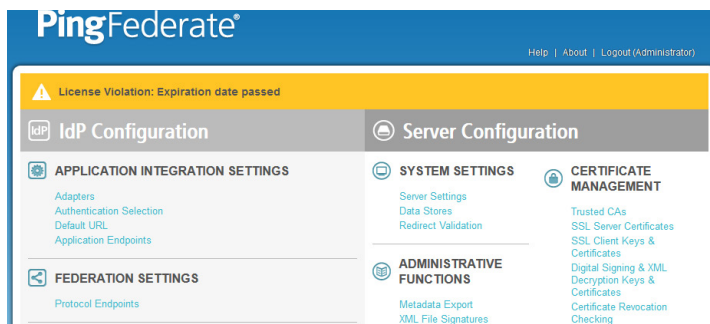
- 1126 1. Log on to the RP’s server that will host the PingFederate service, and follow the instructions at  
 1127 the link below to install PingFederate and run it as a Windows service.

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
- 1137 5. On the **Main Menu** under **System Settings**, click **Server Settings**.
- 1138 6. Click the **Roles and Protocols** tab.
- 1139 7. Select **Enable Identity Provider (IdP) role and support the following**.

- 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.

Main Server Settings

System Administration System Info Runtime Notifications Runtime Reporting Account Management Roles & Protocols

★ Federation Info System Options Summary

*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.*

Base URL  \*

SAML 2.0 Entity ID  \*

WS-Federation Realm  \*

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)**.

Main Export Metadata

★ Metadata Role Metadata Mode Connection Metadata Metadata Signing Export & Summary

*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)

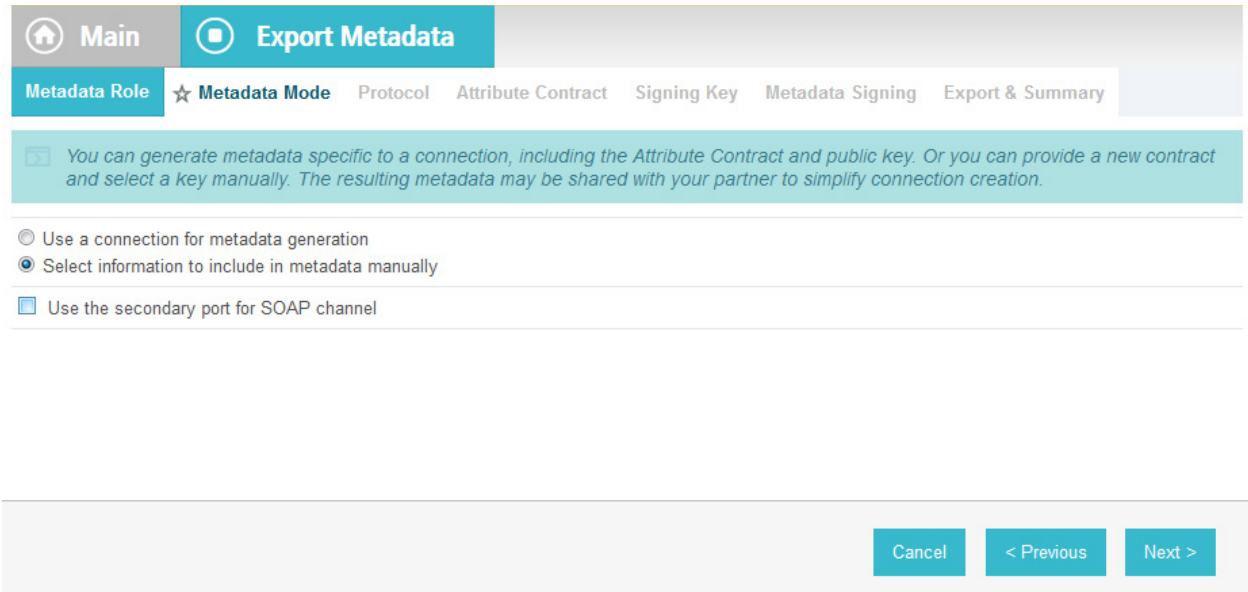
Cancel Next >

1156

1157 18. Click **Next**.

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





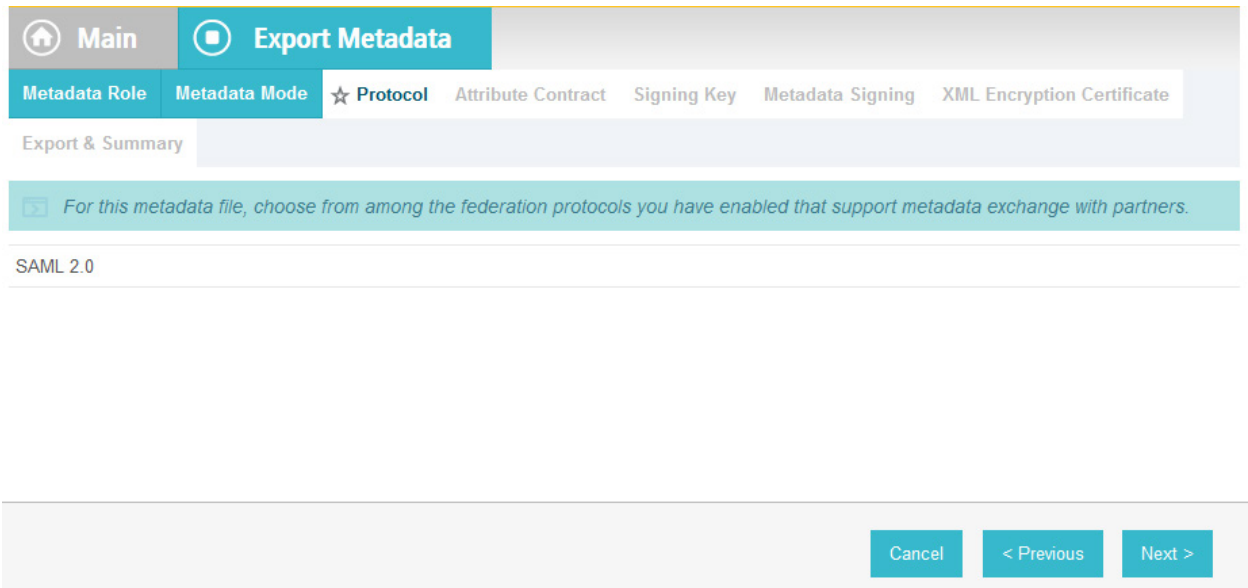
1159

1160

20. Click **Next**.

1161

21. On the Protocol screen, make sure that **SAML 2.0** is listed.



1162

1163

22. Click **Next**.

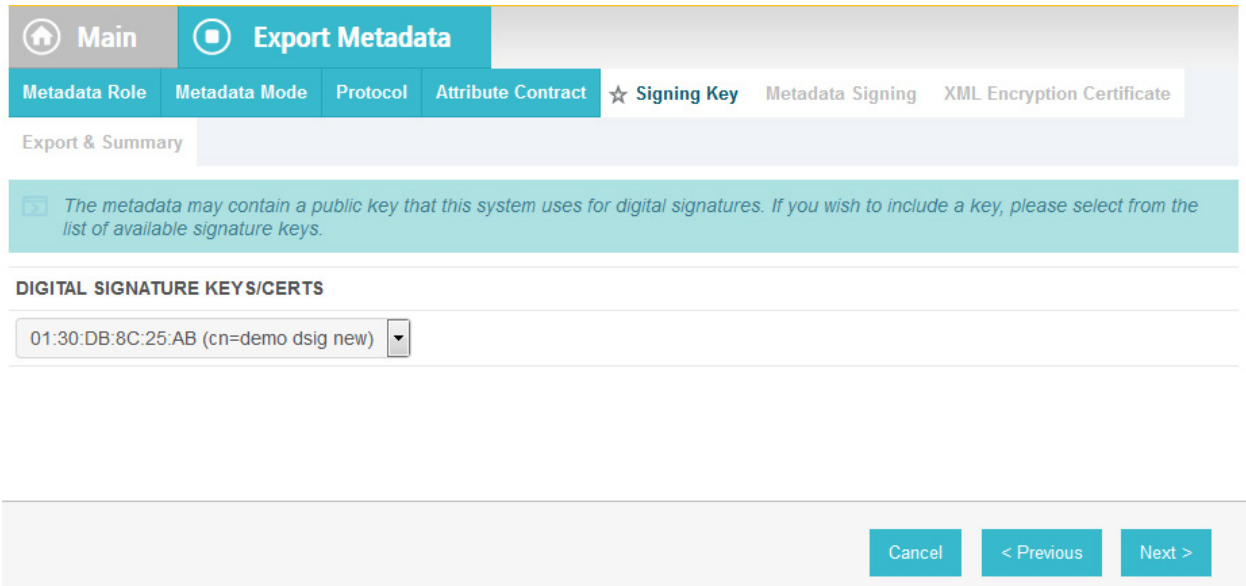
1164

23. On the Attribute Contract screen, click **Next**.

1165

1166

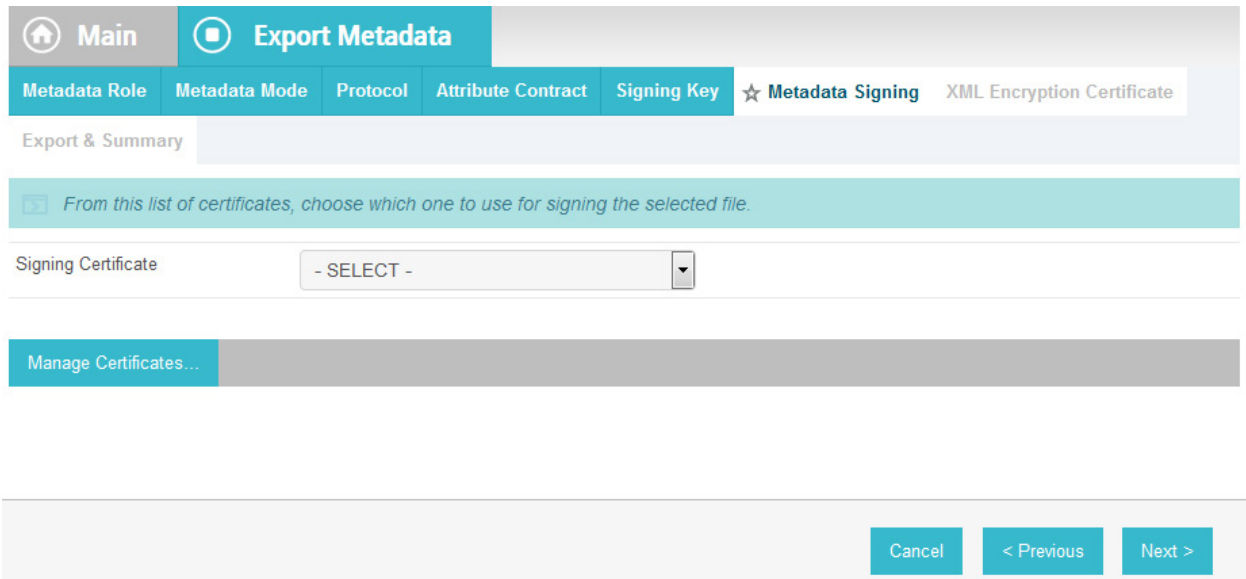
24. On the Signing Key screen, select the certificate that will be used to sign communications with the IdP.



1167

1168 25. Click **Next**.

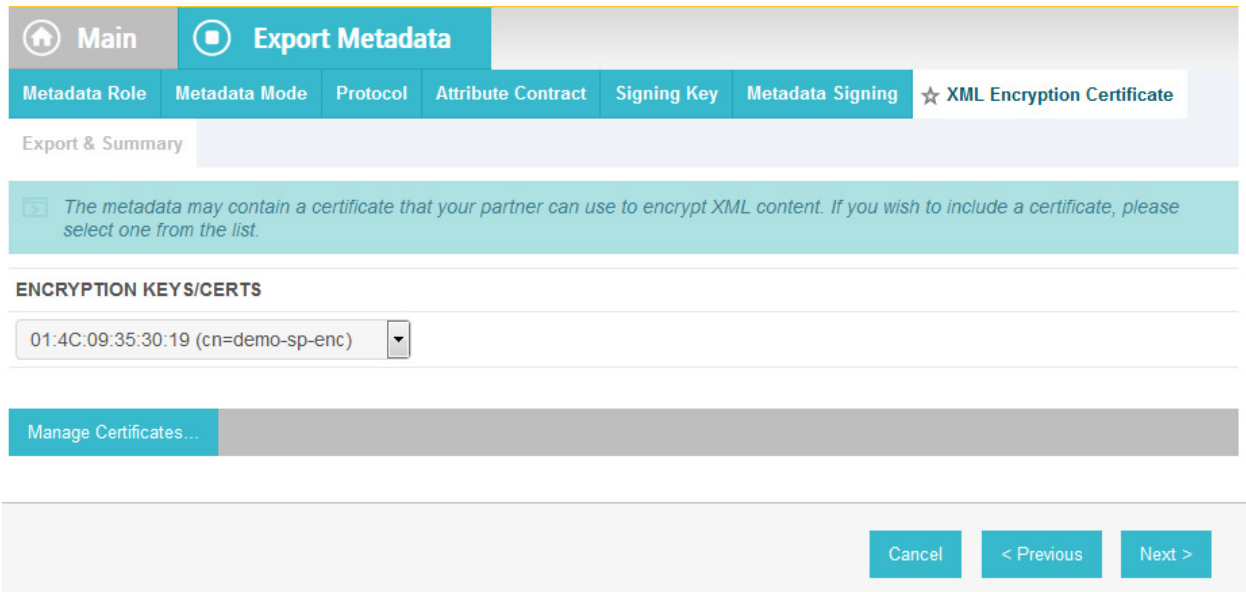
1169 26. On the Metadata Signing screen, if you plan to sign the metadata file that will be exported,  
 1170 select the certificate that will be used to sign the file.



1171

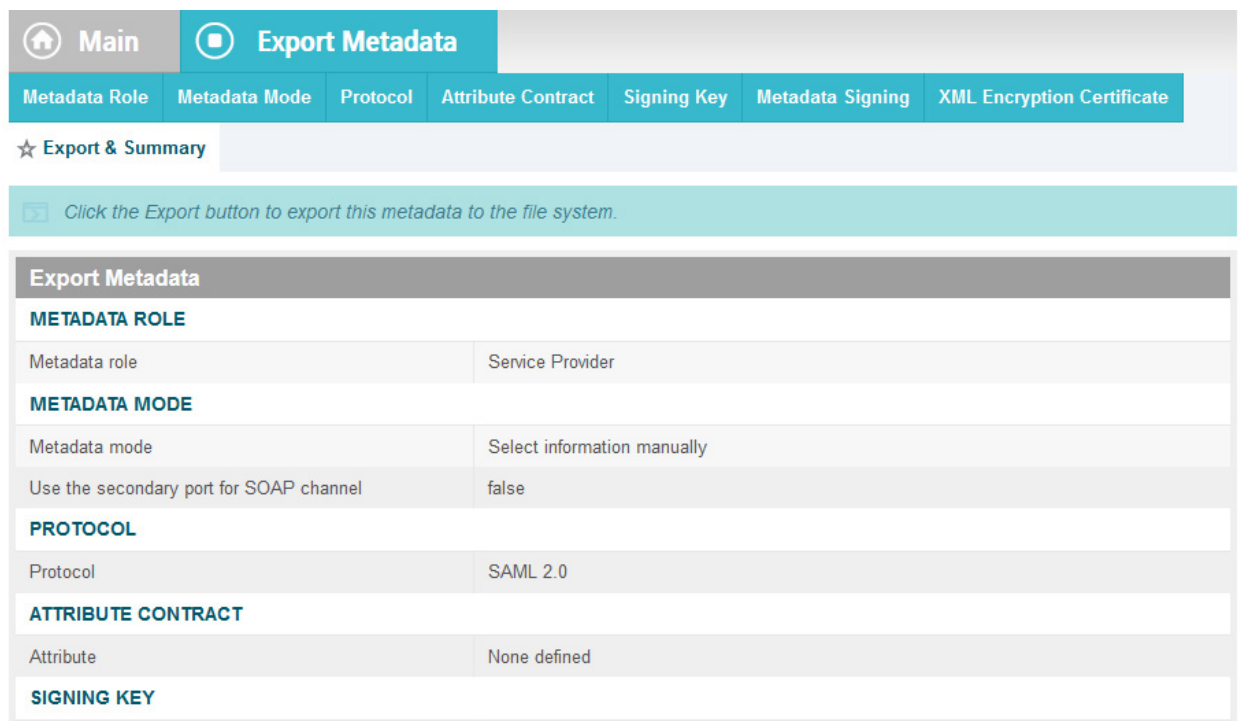
1172 27. Click **Next**.

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



1175

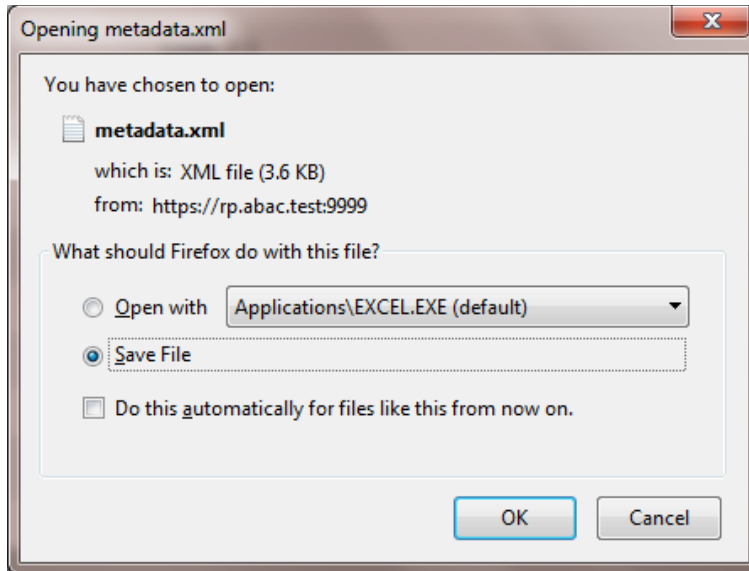
1176 29. Click **Next**.



1177

1178 30. Click **Export**.

1179 This will create an export file that contains the metadata of the RP, which you can download  
 1180 using the browser. This file will be used later in the section, when configuring the PingFederate-  
 1181 IDP.



1182

## 1183 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>

## 1188 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.1.1.1.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  
 1200 **<PF-install>/server/default/conf/template**.
- 1201 5. From the adapter *dist/conf/template/assets* folder, copy the *aa* folder to  
 1202 **<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
#redirectorSSLPort 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\Si
tuational_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

```

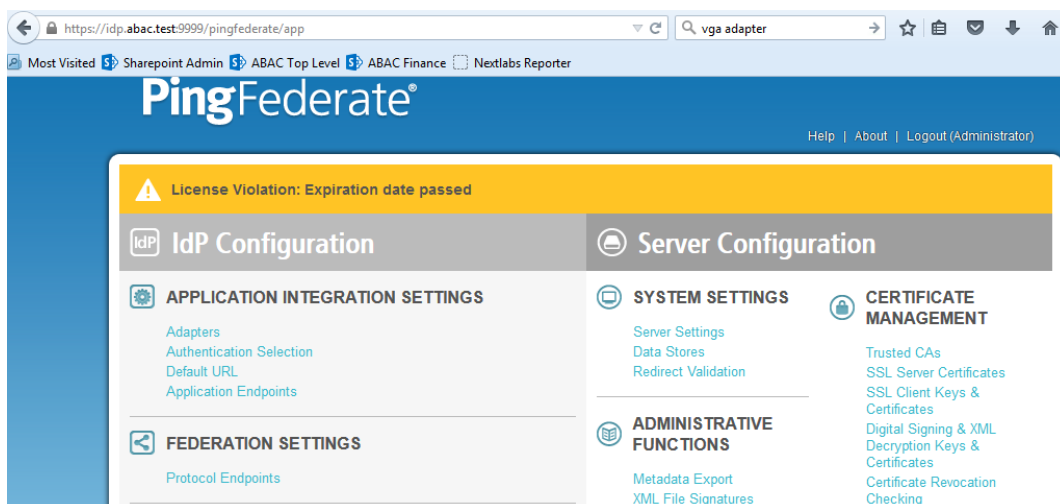
1242

## 1243 2.13 Configure PingFederate-IdP

1244 Follow the instructions in the subsections below to configure PingFederate as the Federation Server for  
 1245 the IdP.

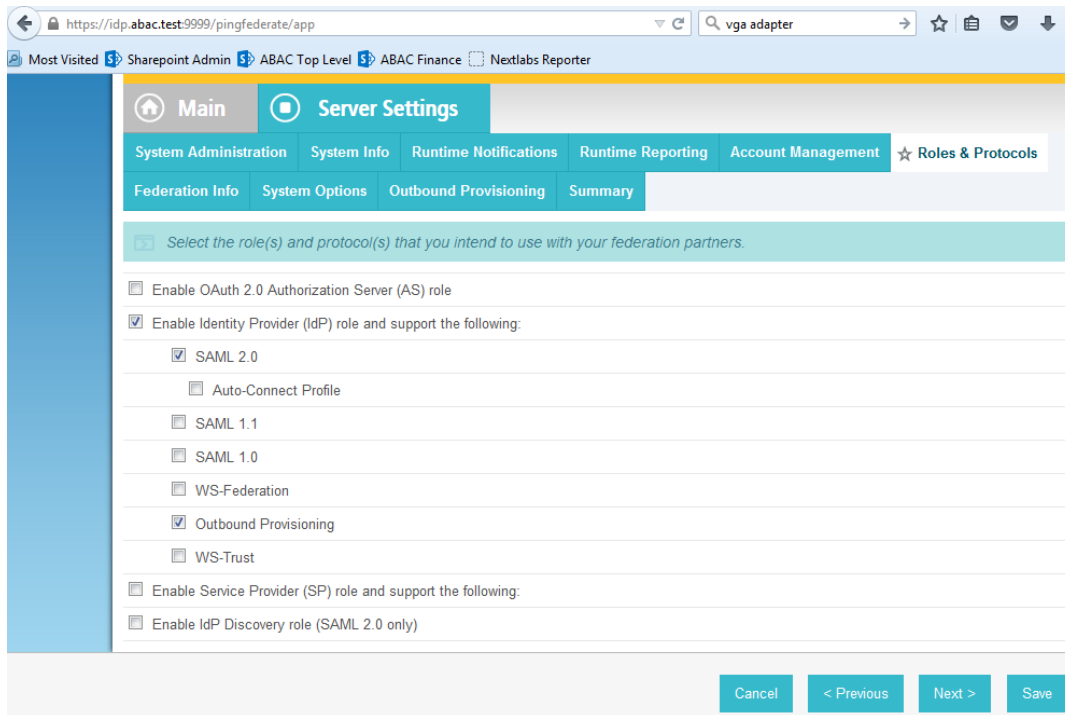
- 1246 1. Launch your browser and go to *https://<DNS\_NAME>:9999/pingfederate/app*.
- 1247 2. Replace **DNS\_NAME** with the fully qualified name of the IdP's PingFederate server (e.g.,  
 1248 *https://idp.abac.test:9999/pingfederate/app*).
- 1249 3. Log on to the PingFederate app using the credentials you configured during installation.

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**
- 1254 **following**.
- 1255 3. Select **SAML 2.0**.

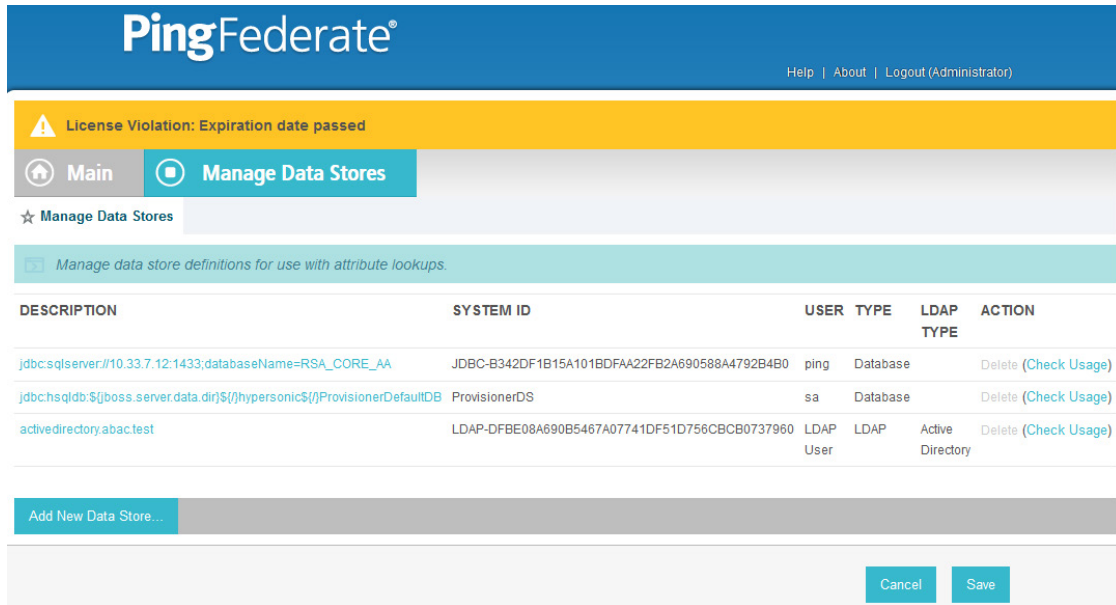


- 1256
- 1257 4. Click **Save**.

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

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

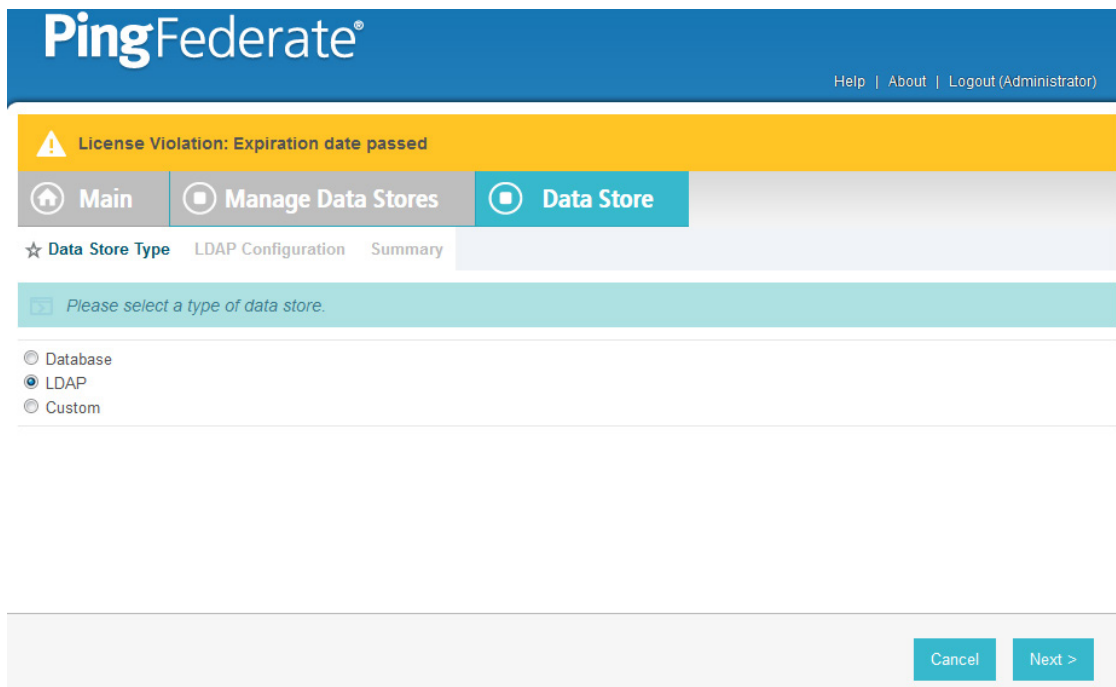




1260

1261

2. Select **LDAP**.



1262

1263

1264

1265

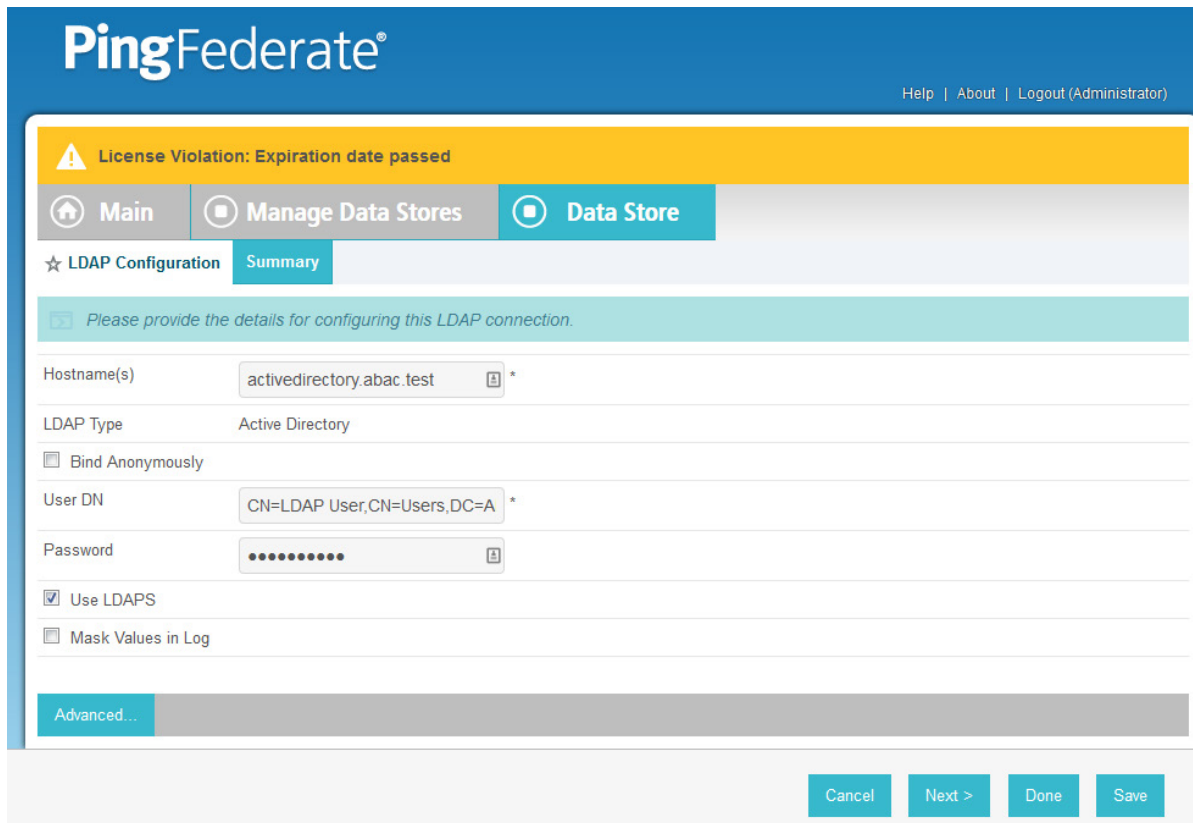
1266

1267

1268

3. Click **Next**.
4. Enter the Hostname where the Microsoft AD is hosted (e.g., **activedirectory.abac.test**).
5. For the **LDAP Type**, select **Active Directory**.
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**).
7. Enter the password associated with the **LDAP User DN**. Select the option to use **LDAPS**.

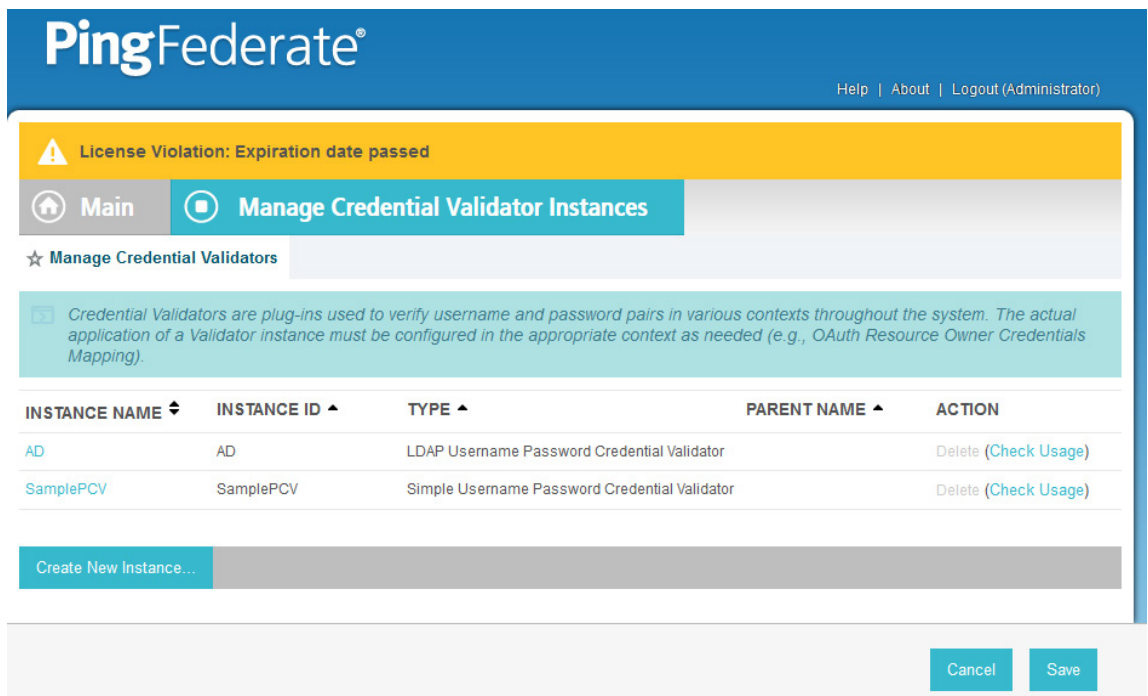
- 1269 8. Click **Next**. Then, click **Save** on the Summary screen.



1270

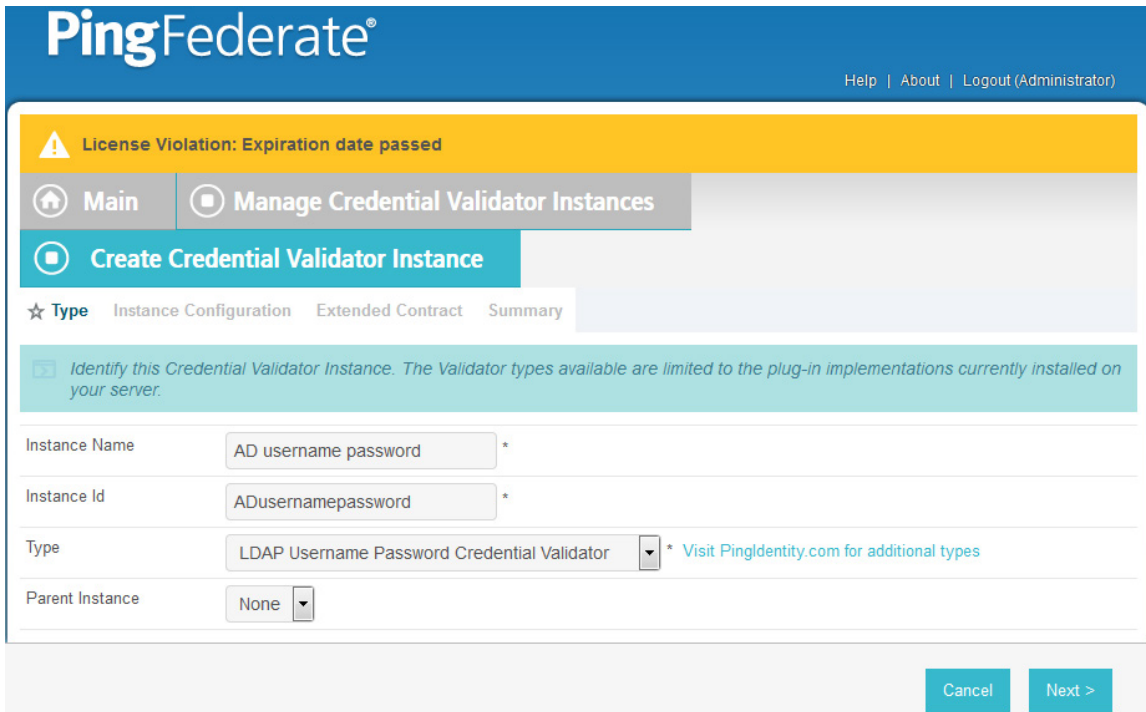
1271 2.13.3 Create Credential Validator for Microsoft AD

- 1272 1. On the Main Menu under Authentication, click **Password Credential Validators**.



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**.



- 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.

[Main](#) | [Manage Credential Validator Instances](#)

[Create Credential Validator Instance](#)

Type: [★ Instance Configuration](#) | [Extended Contract](#) | [Summary](#)

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.

This password credential validator provides a means of verifying credentials stored in a directory server via the LDAP protocol. Additional user attributes from the directory can also be returned by this PCV by adding the desired attribute names to the Extended Contract.

**AUTHENTICATION ERROR OVERRIDES** (A table of LDAP authentication error codes and customized matching expressions that will match the error code to an LDAP error message. These entries override the default individual mappings of messages to codes. Use the localization features to customize the error messages displayed to end users.)

MATCH EXPRESSION (The expression matched against the LDAP error message returned by the server.)	ERROR	Action
<a href="#">Add a new row to 'Authentication Error Overrides'</a>		

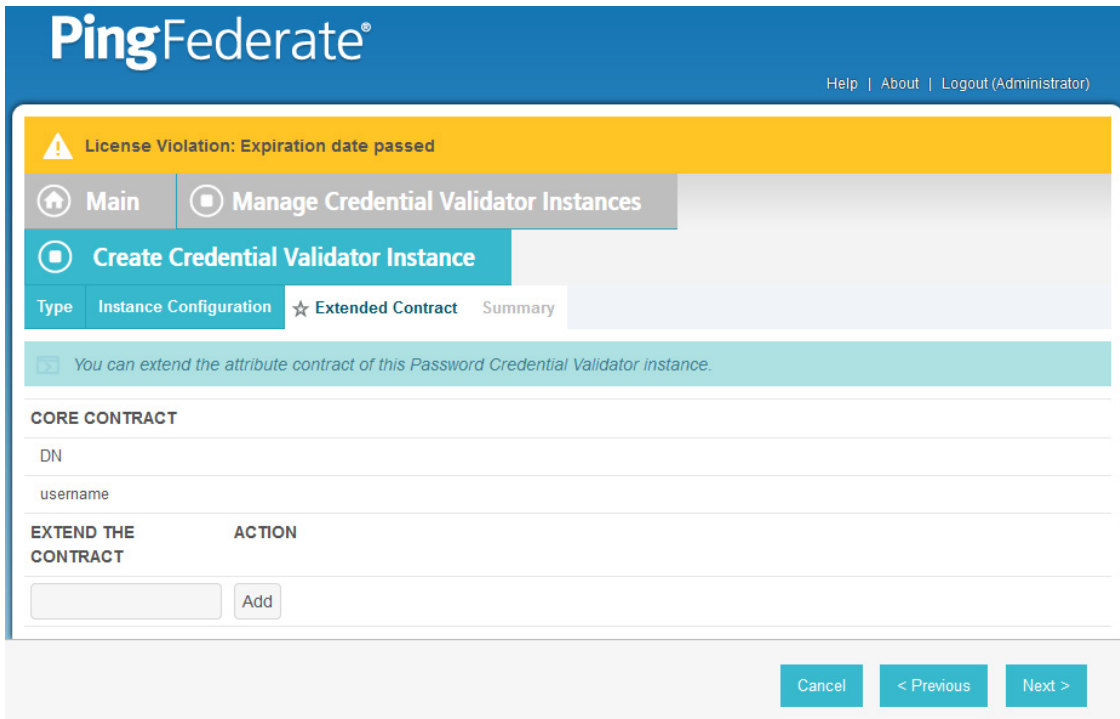
FIELD NAME	FIELD VALUE	DESCRIPTION
LDAP DATASTORE	activedirectory.abac.test *	Select the LDAP Datastore.
SEARCH BASE	DC=ABAC,DC=TEST *	The location in the directory from which the LDAP search begins.
SEARCH FILTER	sAMAccountName=\${username} *	You may use \${username} as part of the query. Example (for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

[Manage Data Stores...](#)

1288

1289 10. Click **Next**.

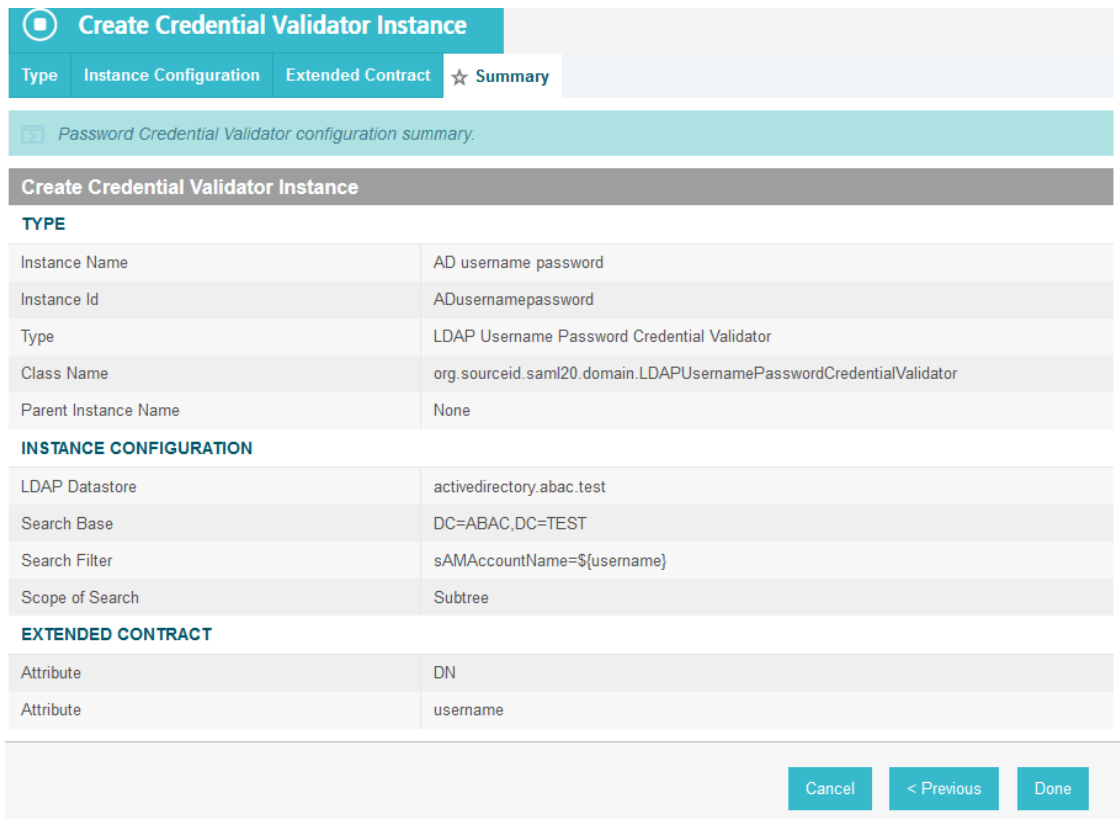
1290 You should see two attributes listed under **CORE CONTRACT**, **DN**, and **username**.



1291

1292 11. Click **Next**.

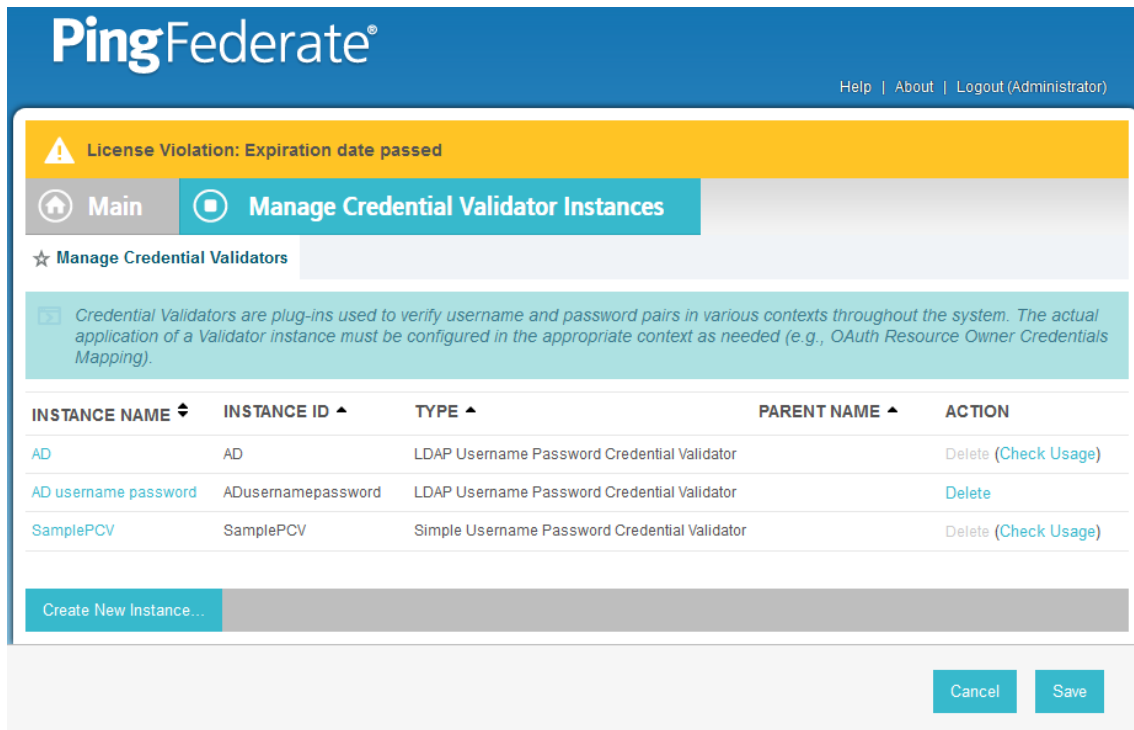
1293 You should see a summary page.



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**).

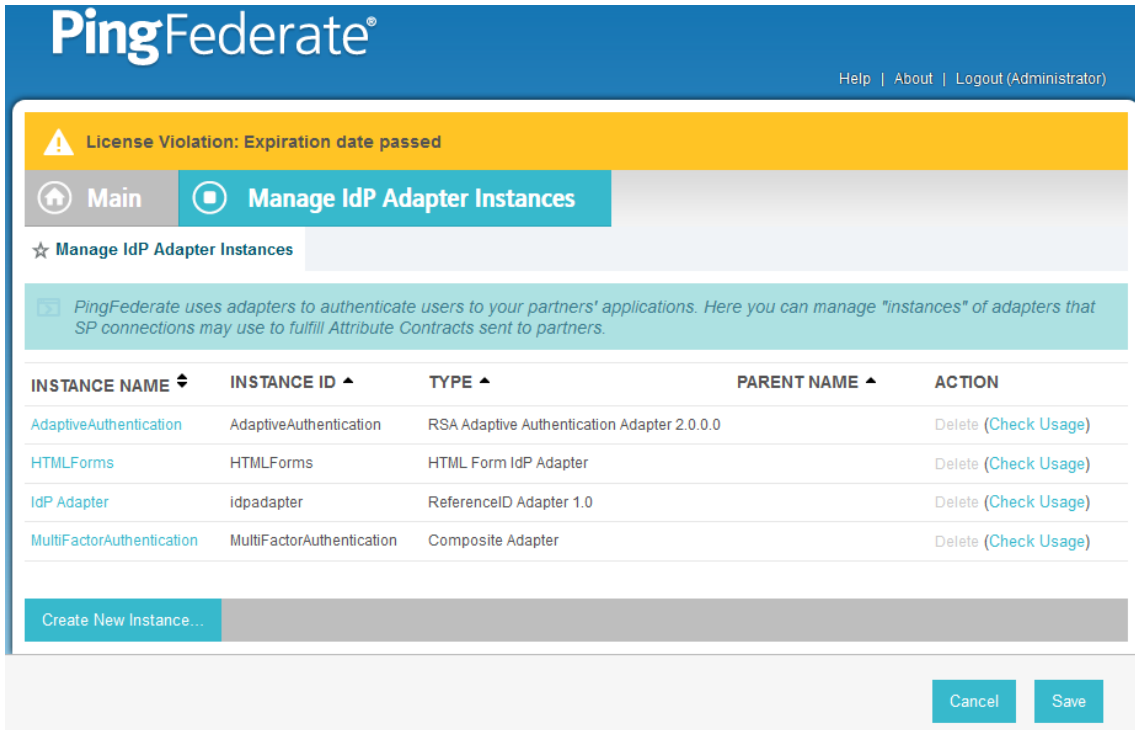


1298  
 1299 13. Click **Save** to complete configuration of the credential validator.

1300 **2.13.4 Create IdP Adapter for Authentication with Microsoft AD via Web Browser**  
 1301 **Form**

1302 The IdP Adapter created in this section is the logical component PingFederate uses to authenticate a  
 1303 user with Microsoft AD via a web browser login page.

1304 1. On the Main Menu under Application Integration Settings, click **Adapters**.



1305

1306

2. Click **Create New Instance**.

1307

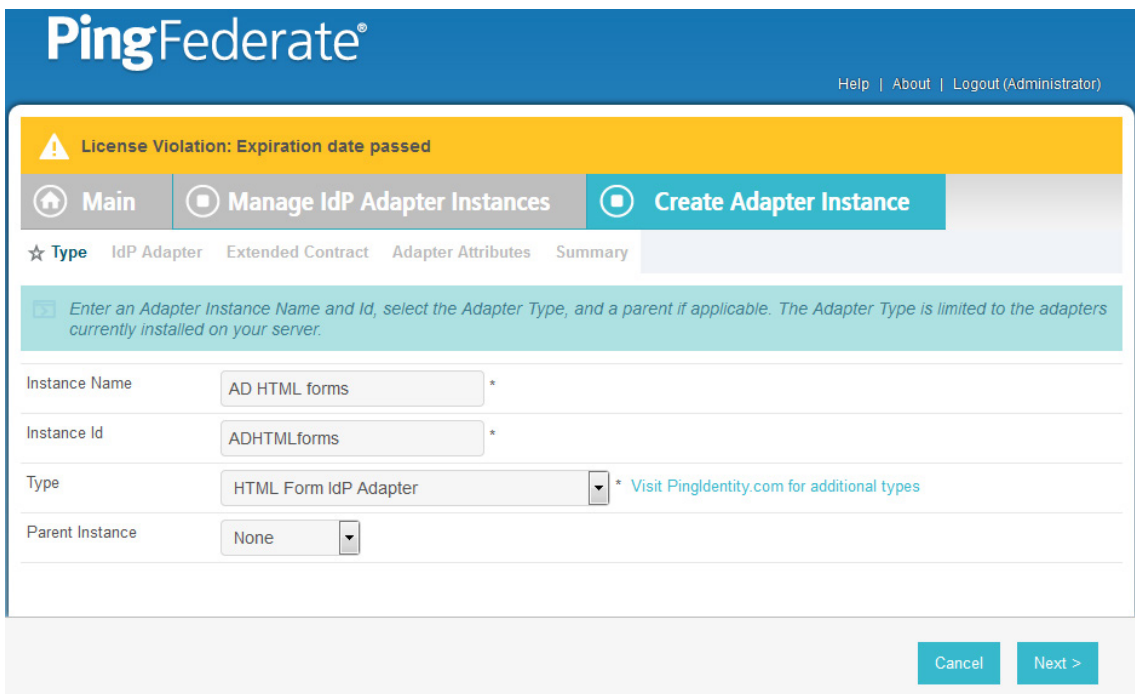
3. In **Instance Name**, enter a unique name for the instance. The name will be used to refer to this configuration (e.g., **AD HTML forms**).

1308

1309

4. Enter a unique **Instance Id** (typically the same as the instance name) without any spaces. For **Type**, select **HTML Form IdP Adapter**.

1310



1311

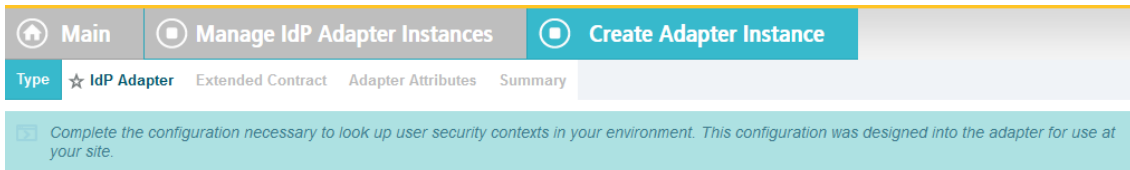
- 1312 5. Click **Next**.
- 1313 6. Under **PASSWORD CREDENTIAL VALIDATOR INSTANCE**, click on the **Add a new row to**
- 1314 **Credential Validator’s** hyperlink. This will add a new selection box under the **PASSWORD**
- 1315 **CREDENTIAL VALIDATOR INSTANCE** with the value of “—Select One—” in it. In that new box,
- 1316 select the credential validator for Microsoft AD that was created in an earlier section (e.g., **AD**
- 1317 **username password**).

The screenshot shows a configuration page for an IdP Adapter. At the top, there are tabs: Type, IdP Adapter (selected), Extended Contract, Adapter Attributes, and Summary. A teal banner contains a note: "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 the "CREDENTIAL VALIDATORS" section, which is a list of Password Credential Validators. The "PASSWORD CREDENTIAL VALIDATOR INSTANCE" section is active, showing a dropdown menu with "AD username password" selected. To the right of the dropdown are "Update" and "Cancel" buttons. Below the instance list is a link: "Add a new row to 'Credential Validators'". A table below contains configuration fields:

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: /mylogoutpast). (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.
LOGOUT REDIRECT		A fully qualified URL, usually at the SP to which a user will be redirected after logout

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





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

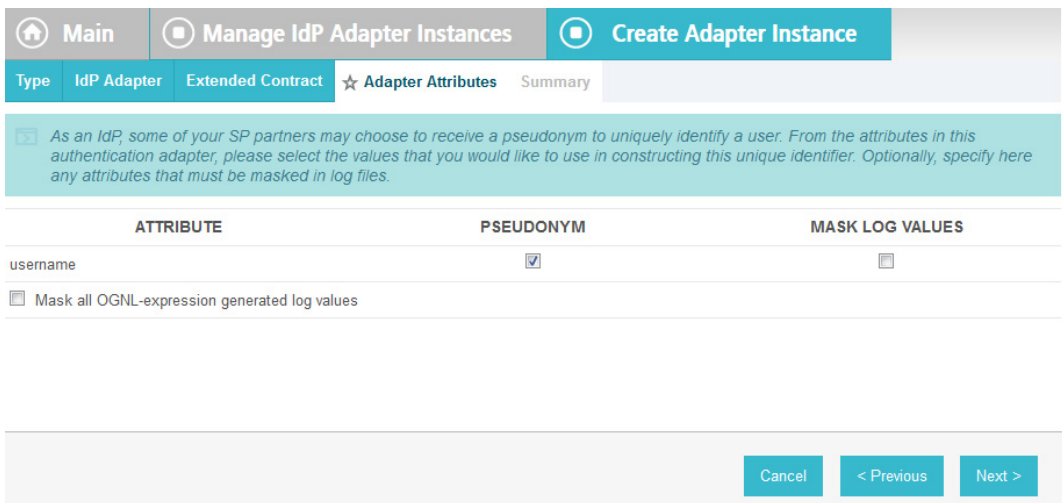
**PASSWORD CREDENTIAL VALIDATOR INSTANCE**

	Action
AD username password	<a href="#">Edit</a> <a href="#">Delete</a>

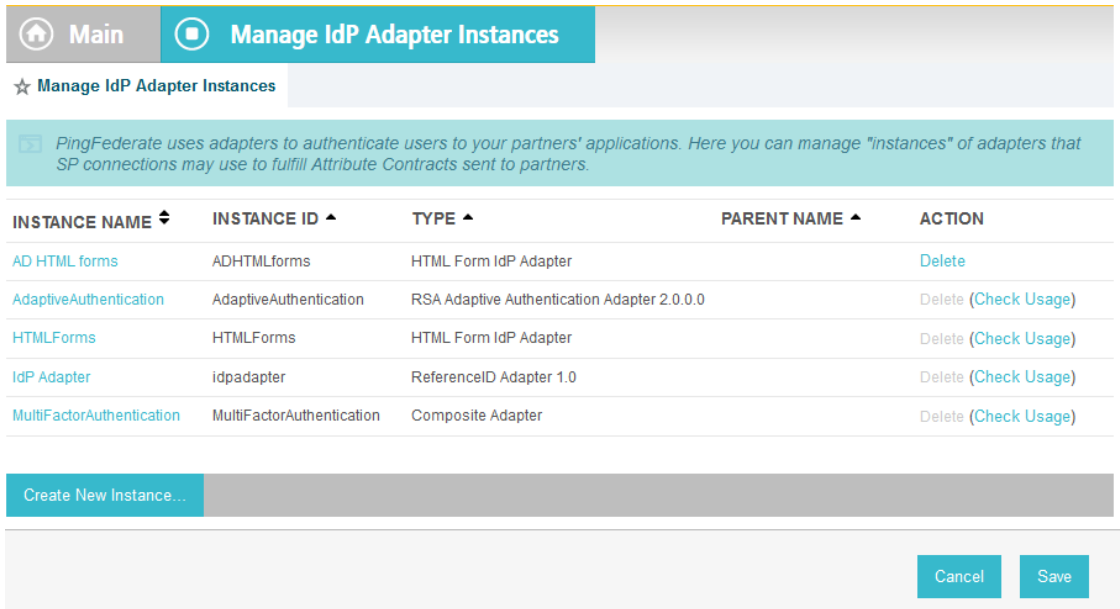
[Add a new row to 'Credential Validators'](#)

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: /mylogoutpast). (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.

- 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.



- 1324
- 1325 10. Click **Next**. On the Summary screen, click **Done**.



1326

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

### 1328 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**:

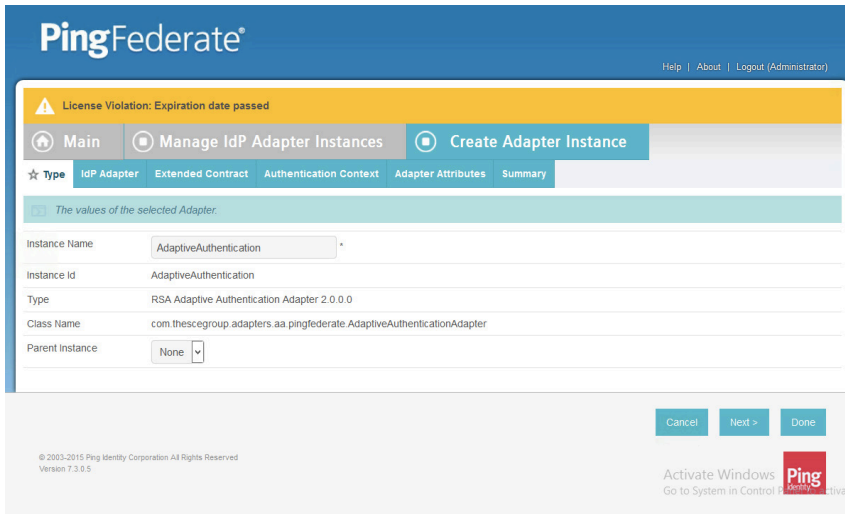
1335 a. **Instance Name:** (Instance Name)

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**



1341

1342

1343

5. On the IdP Adapter configuration page, click **Show Advanced Fields** and input the following parameters while leaving the rest as default, before clicking **Next**:

1344

a. AA Web Service URL: *http://<RSA Server*

1345

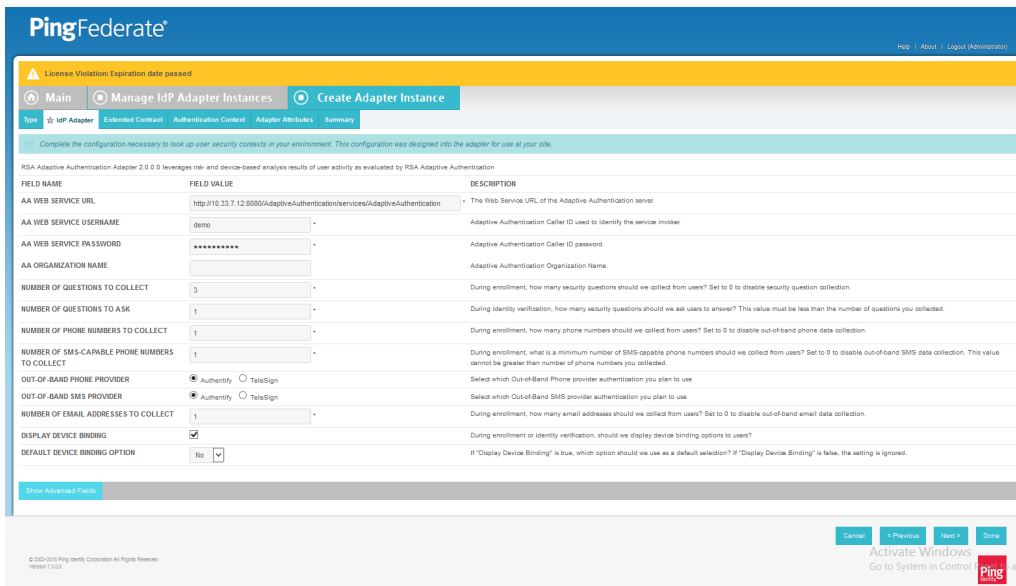
*DNS>:8080/AdaptiveAuthentication/services/AdaptiveAuthentication*

1346

b. AA Web Service Username: [username] (Credentials must match on RSA server.)

1347

c. AA Web Service Password: [password]

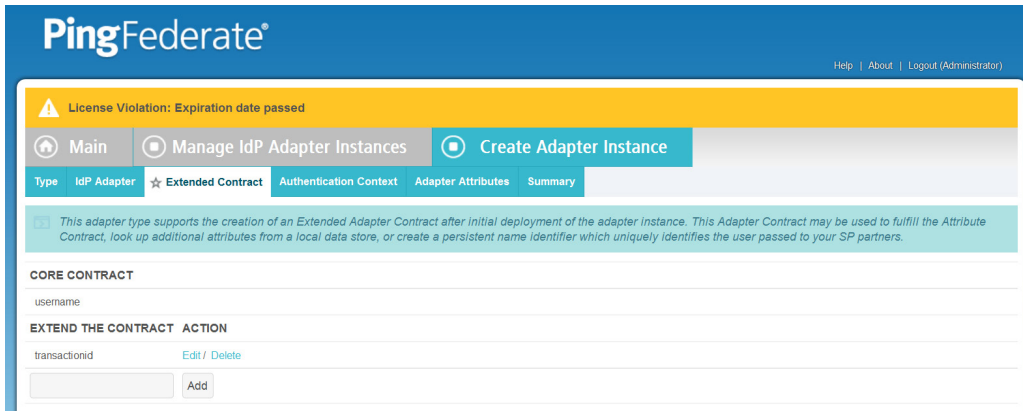


1348

1349

1350

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



1351

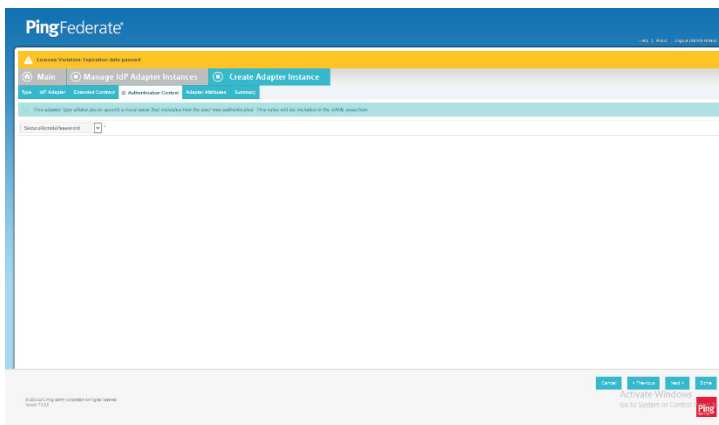
1352

7. Click **Next**.

1353

1354

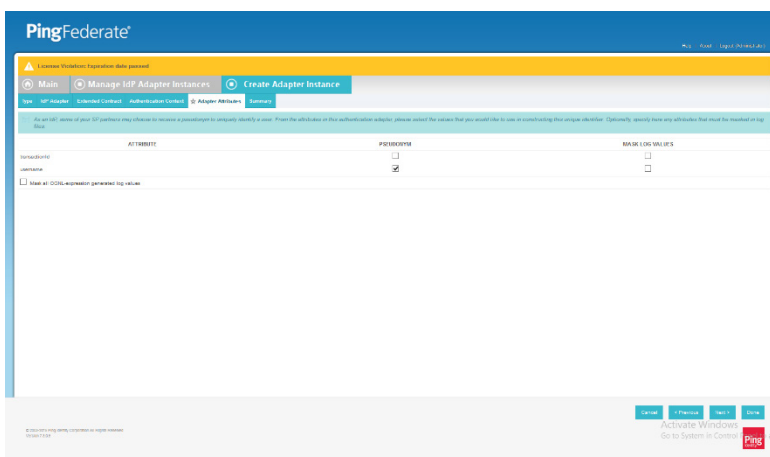
8. On the **Authentication Context** screen, select *SecureRemotePassword* as the fixed value for authentication. This value will be included in the SAML assertion. Click **Next**.



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

1360

11. On the **Manager IdP Adapter Instances** screen, click **Save** to complete the Adapter configuration.

### 1361 2.13.6 Create Composite IdP Adapter Integrating Microsoft AD and RSA AA

1362 The IdP Adapter created in this section is a composite adapter that integrates the two previously created  
 1363 adapters for Microsoft AD and RSA AA. When a user is directed to the PingFederate IdP server, the user  
 1364 will see a web form where they can enter their Microsoft AD credentials. Following authentication with  
 1365 Microsoft AD, PingFederate will initiate the second factor authentication with an SCE Plug-in. The SCE  
 1366 Plug-in will then present the user with a request for the second factor.

- 1367 1. On the **Main** menu under **Application Integration Settings**, click **Adapters**.
- 1368 2. On the Manage IdP Adapters screen, click **Create New Instance**.
- 1369 3. Enter a unique **Instance Name** you would like to use to refer to this configuration (e.g., **RSA**  
 1370 **Multifactor**).
- 1371 4. Enter a unique **Instance Id** (typically the same as the **Instance Name**) without any spaces.
- 1372 5. For **Type**, select **Composite Adapter**.

1373

- 1374 6. Click **Next**.
- 1375 7. On the IdP Adapter screen, under **ADAPTER INSTANCE**, click on the **Add a new row to**  
 1376 **'Adapters'** hyperlink. This will add a new selection box under the **ADAPTER INSTANCE** with the  
 1377 value of **"—Select One—"** into the box. In that new box, select the adapter instance for HTML  
 1378 forms with Microsoft AD that was created in an earlier section (e.g., **AD HTML forms**).
- 1379 8. Under **ADAPTER INSTANCE**, click the **Update** hyperlink on the right side of the page. This will  
 1380 cause the selection box to turn grey.

1381

1382

1383

1384

1385

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

1386

1387

1388

1389

1390

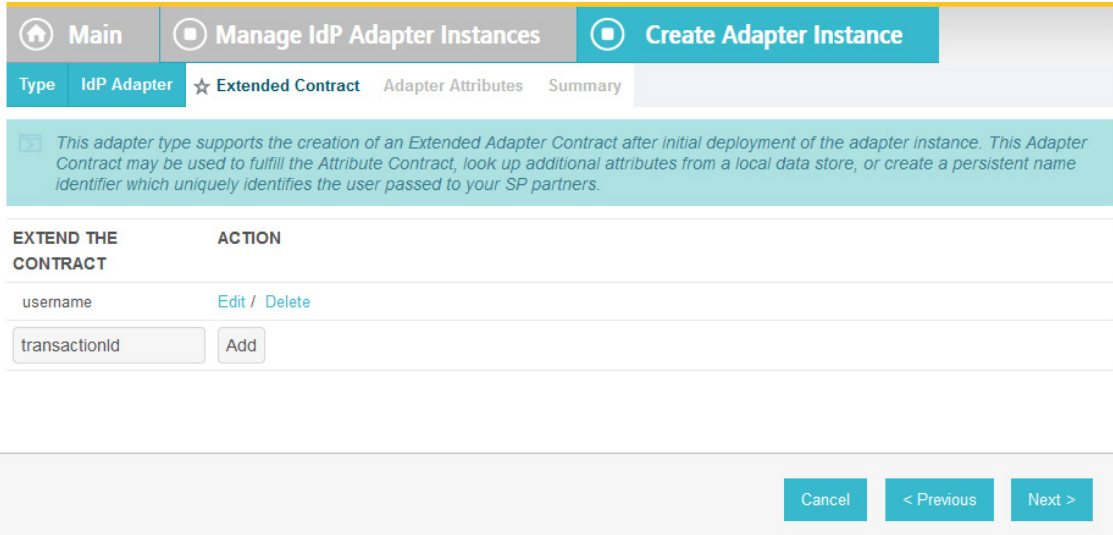
1391

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

- 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.

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

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



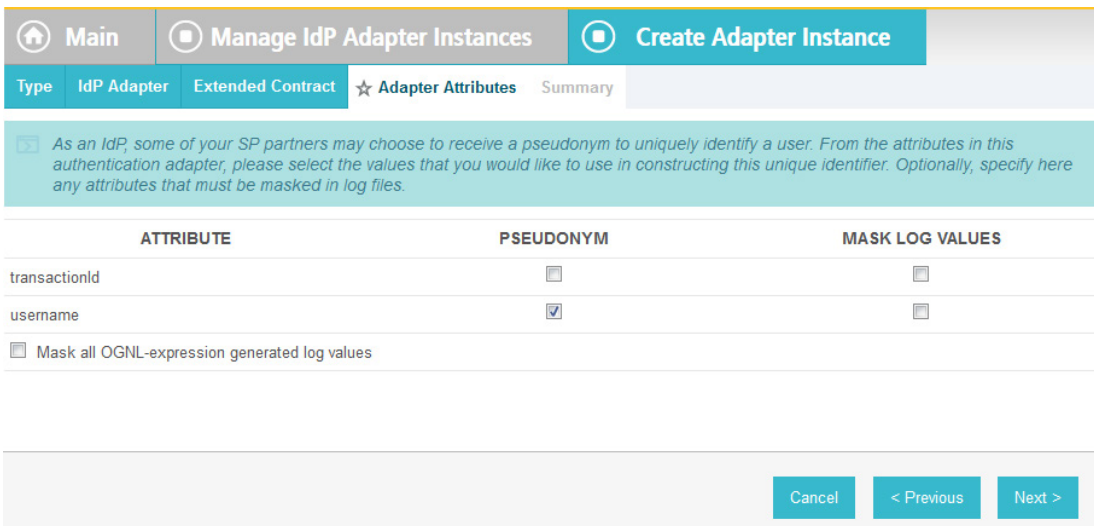
1401

1402

17. Click **Add**. Then, click **Next**.

1403

18. On the **Adapter Attributes** screen, in the **username** row, select the **PSEUDONYM** column.



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

1408

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.

1412

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

1413

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**.

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

1420

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

Type	IdP Adapter	★ Extended Contract	Adapter Attributes	Summary
<p> 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.</p>				
<b>CORE CONTRACT</b>				
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				
<b>EXTEND THE CONTRACT</b>		<b>ACTION</b>		
<input type="text"/>		<input type="button" value="Add"/>		
		<input type="button" value="Cancel"/> <input type="button" value=" &lt; Previous"/> <input type="button" value=" Next &gt;"/>		

- 1421
- 1422
- 1423
- 1424
- On the **Adapter Attributes** screen, in the row for **ise\_username**, check the box in the **Pseudonym** column. Click **Next**. (Note: if you added other attributes in Step #6, you could check the box under **Pseudonym** for those as well.)

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
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**.

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**.

★ Manage IdP Adapter Instances

*PingFederate uses adapters to authenticate users to your partners' applications. Here you can manage "instance adapters that SP connections may use to fulfill Attribute Contracts sent to partners.*

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)

Create New Instance...

Cancel Save

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.

The screenshot shows the 'SP Connection' configuration interface. At the top, there are two tabs: 'Main' and 'SP Connection'. Below the tabs is a navigation bar with the following items: '★ Connection Type', 'Connection Options', 'Import Metadata', 'General Info', 'Browser SSO', 'Credentials', and 'Activation & Summary'. A teal instruction bar reads: '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.' Below this, there are three rows of configuration options:

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	

At the bottom right of the form, there are two buttons: 'Cancel' and 'Next >'.

1436

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

The screenshot shows the 'SP Connection' configuration interface, now on the 'Connection Options' step. The navigation bar is updated: '★ Connection Type' is greyed out, and '★ Connection Options' is highlighted. The other navigation items remain. A teal instruction bar reads: 'Please select options that apply to this connection.' Below this, there are three rows of configuration options:

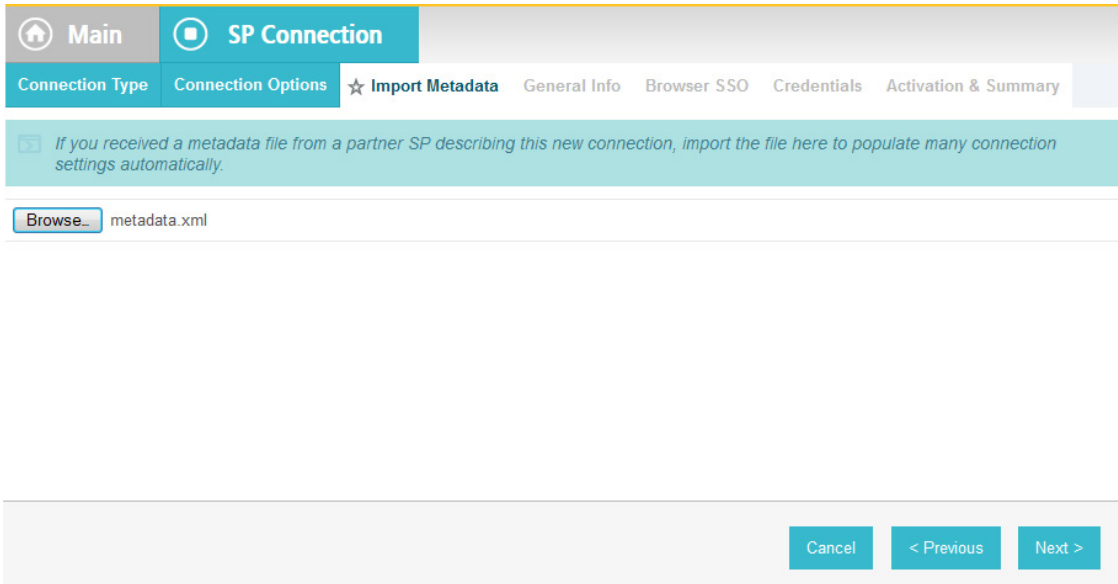
<input checked="" type="checkbox"/> Browser SSO
<input type="checkbox"/> IdP Discovery
<input type="checkbox"/> Attribute Query

At the bottom right of the form, there are three buttons: 'Cancel', '< Previous', and 'Next >'.

1438

- 1439 4. Click **Next**.

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



1442

1443

6. Click **Next**.

1444

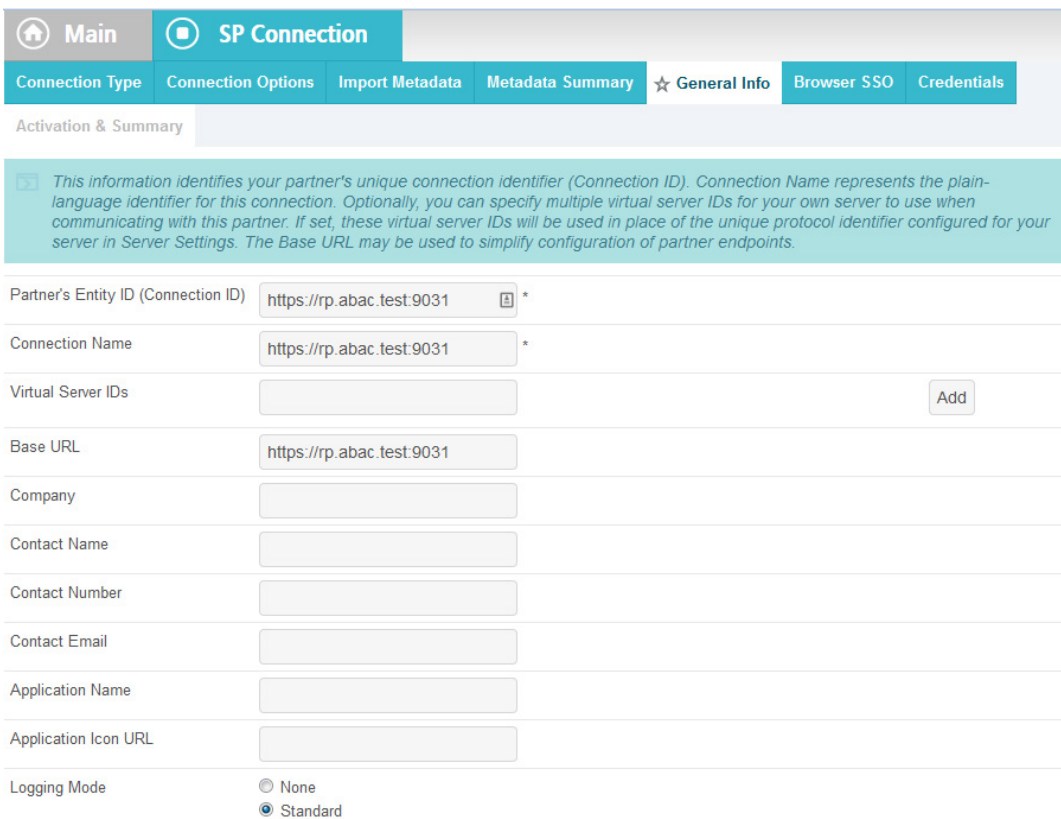
7. On the **Metadata Summary** screen, click **Next**.

1445

8. On the **General Info** screen, you should see some configuration information (e.g., **Base URL**)

1446

about the RP that was taken from the metadata file that you selected earlier.



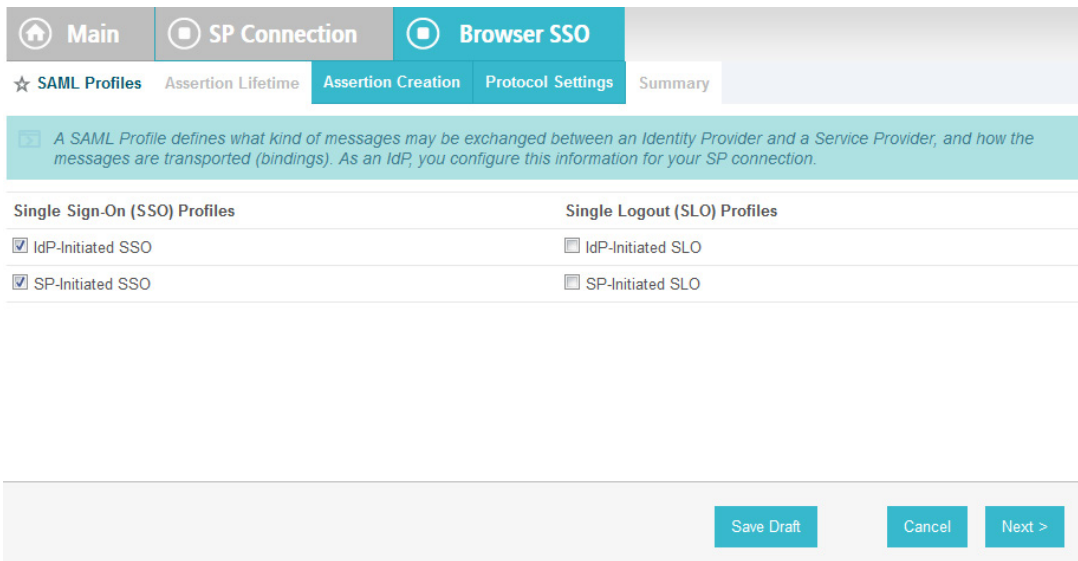
1447

1448

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



1449 10. Select **IdP-Initiated SSO** and **SP-Initiated SSO**. Then, click **Next**.

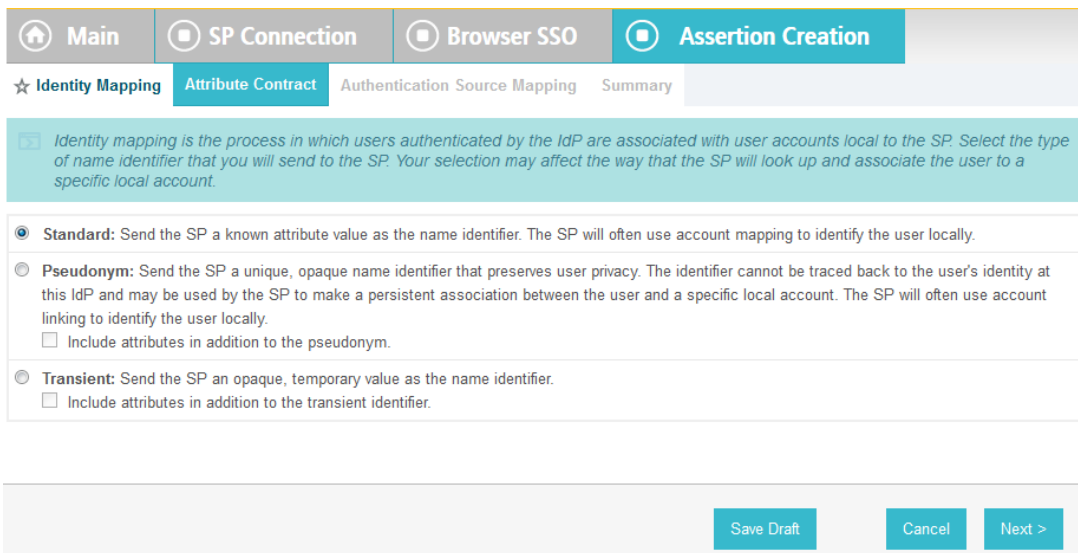


1450

1451 11. On the **Assertion Lifetime** screen, click **Next**.

1452 12. On the **Assertion Creation** screen, click **Configure Assertion Creation**. This will bring up a  
 1453 sequence of sub-screens, starting with the **Identity Mapping** screen.

1454 13. On the **Identity Mapping** screen, select the **Standard** option.



1455

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

1457

1458 15. Click **Next**.

1459

1460 16. On the **Authentication Source Mapping** screen, click **Map New Adapter Instance**. This will  
 1461 launch a sequence of sub-screens, beginning with the **Adapter Instance** screen.

1462 17. On the **Adapter Instance** screen, select the composite adapter created in an earlier section (e.g.,  
 1463 **RSA Multifactor**).

1464

1465

1466

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

1467

1468

1469

1470

19. Click **Next**.
20. On the **Attribute Contract Fulfillment** screen, for **SAML\_SUBJECT**, select **Adapter** for the **SOURCE** field and **username** for the **VALUE** field.

1471

1472 21. Click **Next**.

1473

1474 22. Click **Next**.

1475

1476

1477

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

1478

1479

24. Click **Next**.

1480

1481

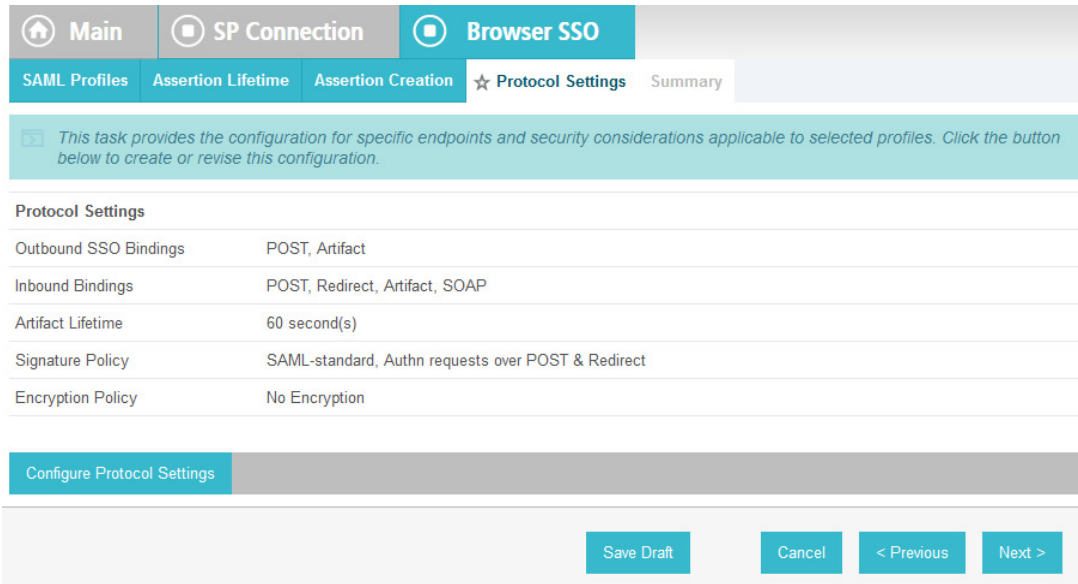
1482

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

1483

1484

26. Click **Next**.



1485

1486

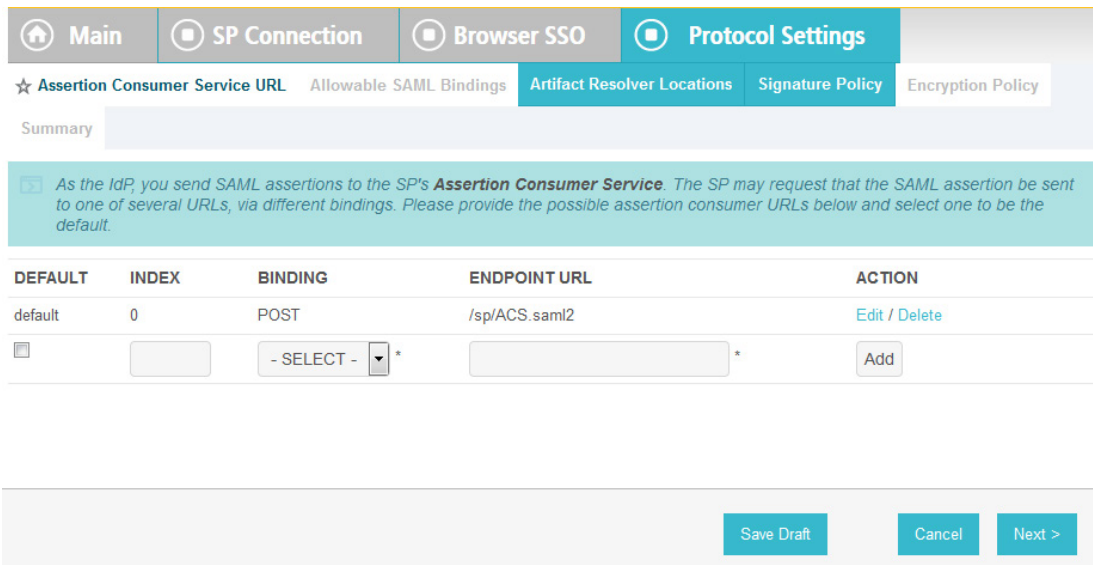
1487

27. On the **Protocol Settings** screen, click **Configure Protocol Settings**. This will launch a sequence of sub-screens, beginning with the **Assertion Consumer Service URL** screen.

1488

1489

28. On the **Assertion Consumer Service URL** screen, make sure that the **BINDING** field is set to **POST** and the **ENDPOINT URL** field is set to **/sp/ACS.saml2**.



1490

1491

1492

29. Click **Next**.

30. On the **Allowable SAML Bindings** screen, select **POST** and **Redirect**.

The screenshot shows a web interface with a top navigation bar containing 'Main', 'SP Connection', 'Browser SSO', and 'Protocol Settings'. Below this is a sub-navigation bar with 'Assertion Consumer Service URL', 'Allowable SAML Bindings', 'Signature Policy', 'Encryption Policy', and 'Summary'. The main content area has a teal header with the question: 'When the SP sends messages, what SAML bindings do you want to allow?'. Below this are four rows of checkboxes: 'Artifact' (unchecked), 'POST' (checked), 'Redirect' (checked), and 'SOAP' (unchecked). At the bottom right, there are four buttons: 'Save Draft', 'Cancel', '< Previous', and 'Next >'.

1493

1494 31. Click **Next**.

1495 32. On the **Signature Policy** screen, select **Require AuthN requests to be signed when received via**  
1496 **the POST or Redirect bindings**.

The screenshot shows the same web interface as above, but with the 'Signature Policy' tab selected in the sub-navigation bar. The teal header contains the text: '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.' Below this are two rows of checkboxes: 'Require AuthN requests to be signed when received via the POST or Redirect bindings' (checked) and 'Always sign the SAML Assertion' (unchecked). At the bottom right, there are four buttons: 'Save Draft', 'Cancel', '< Previous', and 'Next >'.

1497

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



1499

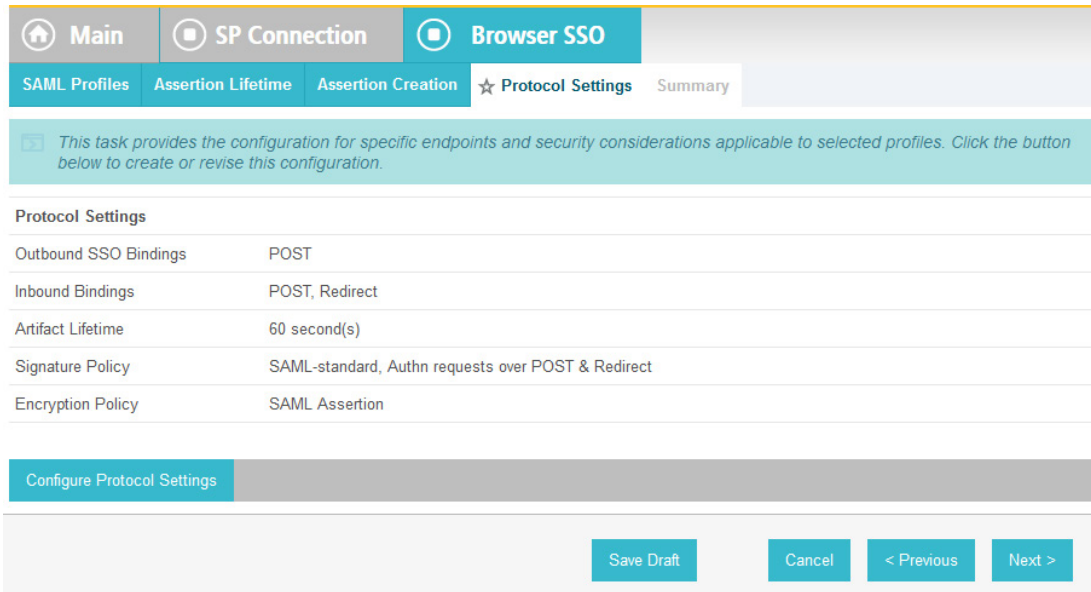
1500

34. Click **Next**.

1501

1502

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

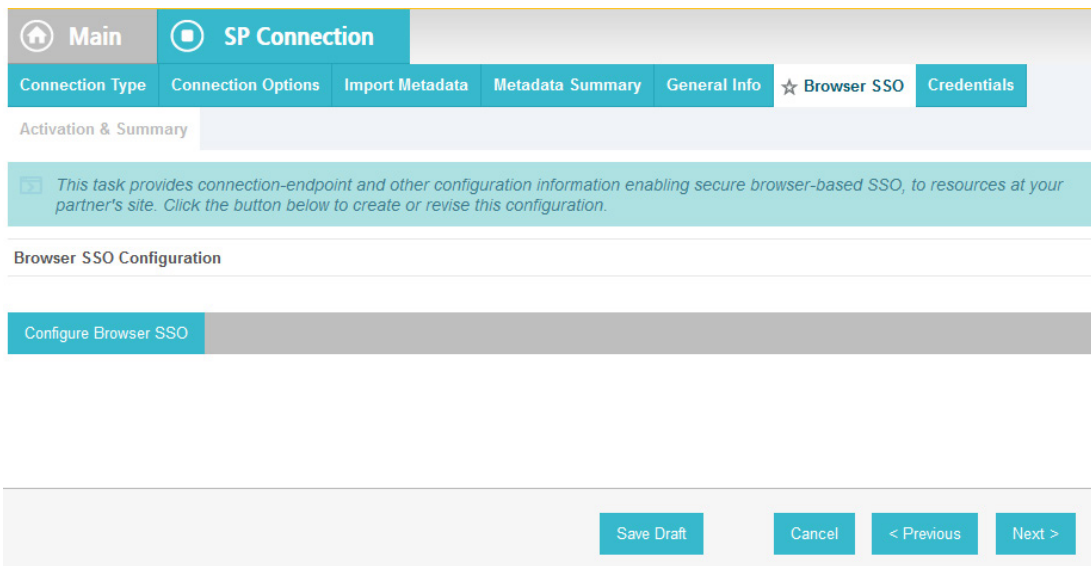


1503  
1504 This will take you back to the **Protocol Settings** screen.

1505 36. Click **Next**.

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

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



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**).

The screenshot shows a web interface with a top navigation bar containing 'Main', 'SP Connection', and 'Credentials'. Below this is a sub-navigation bar with 'Digital Signature Settings', 'Signature Verification Settings', 'Select XML Encryption Certificate', and 'Summary'. A teal banner contains the text: '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.' The main form area includes a 'Signing Certificate' dropdown menu with the value '01:30:DB:8C:25:AB (cn=demo dsig new)', a checkbox for 'Include the certificate in the signature <KeyInfo> element', and a 'Signing Algorithm' dropdown menu with the value 'RSA SHA256'. At the bottom right, there are three buttons: 'Save Draft', 'Cancel', and 'Next >'.

1514

1515

43. Click **Next**.

The screenshot shows the same web interface as above, but with the 'Signature Verification Settings' tab selected. A teal banner contains the text: '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. At the bottom right, there are four buttons: 'Save Draft', 'Cancel', '< Previous', and 'Next >'.

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.

1522

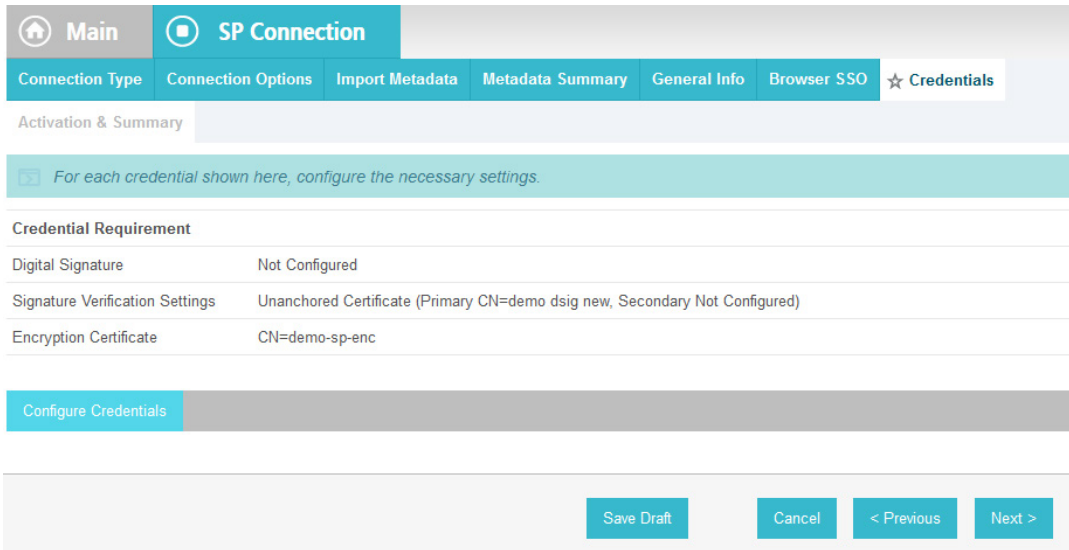
1523

47. Click **Next**.

1524

1525

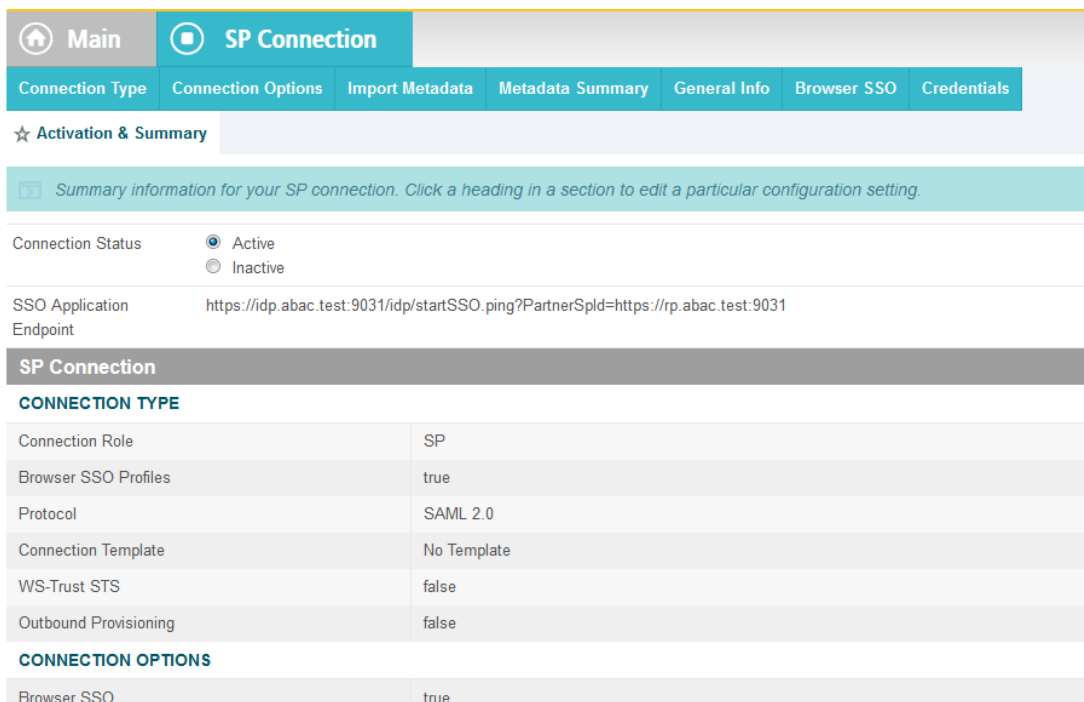
48. On the **Summary** screen, click **Done**. This will take you back to the **Credentials** screen.



1526

1527 49. Click **Next**.

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



1529

1530 51. Copy the Identity Provider’s SSO Application Endpoint URL (e.g.,  
 1531 *https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=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**.

★ Manage IdP Adapter Instances

*PingFederate uses adapters to authenticate users to your partners' applications. Here you*

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

Create New Instance...

- 1538
- 1539 3. In the Instance Name field, enter **ISE-RSA Composite Adapter**.
- 1540 4. In the Instance ID field, give the same name without spaces.
- 1541 5. In the Type field, choose **Composite Adapter**.

1542

1543 6. Click **Next**.

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

1545

1546 8. Choose **CiscoISE**.

1547 9. Click **Update**.

1548 10. Click **Add a new row to 'Adapters'**.

1549 11. Choose **RSA Multifactor**.

1550 12. Click **Update**.

1551

1552 13. Click **Next**.

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

[Main](#) | 
 [Manage IdP Adapter Instances](#) | 
 [Create Adapter Instance](#)

[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. It allows you to create adapter attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SAML service.

**EXTEND THE CONTRACT ACTION**

ip_address	<a href="#">Edit / Delete</a>
ise_audit_session	<a href="#">Edit / Delete</a>
ise_auth_acs_timestamp	<a href="#">Edit / Delete</a>
ise_auth_id	<a href="#">Edit / Delete</a>
ise_calling_station_id	<a href="#">Edit / Delete</a>
ise_identity_group	<a href="#">Edit / Delete</a>
ise_identity_store	<a href="#">Edit / Delete</a>
ise_message_code	<a href="#">Edit / Delete</a>
ise_network_device_name	<a href="#">Edit / Delete</a>
ise_selected_azn_profiles	<a href="#">Edit / Delete</a>
ise_user_name	<a href="#">Edit / Delete</a>
role	<a href="#">Edit / Delete</a>
transactionid	<a href="#">Edit / Delete</a>
username	<a href="#">Edit / Delete</a>

1554

1555

15. Click **Next**.

1556

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



🏠 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 a constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

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"/>

Mask all OGNL-expression generated log values

1557

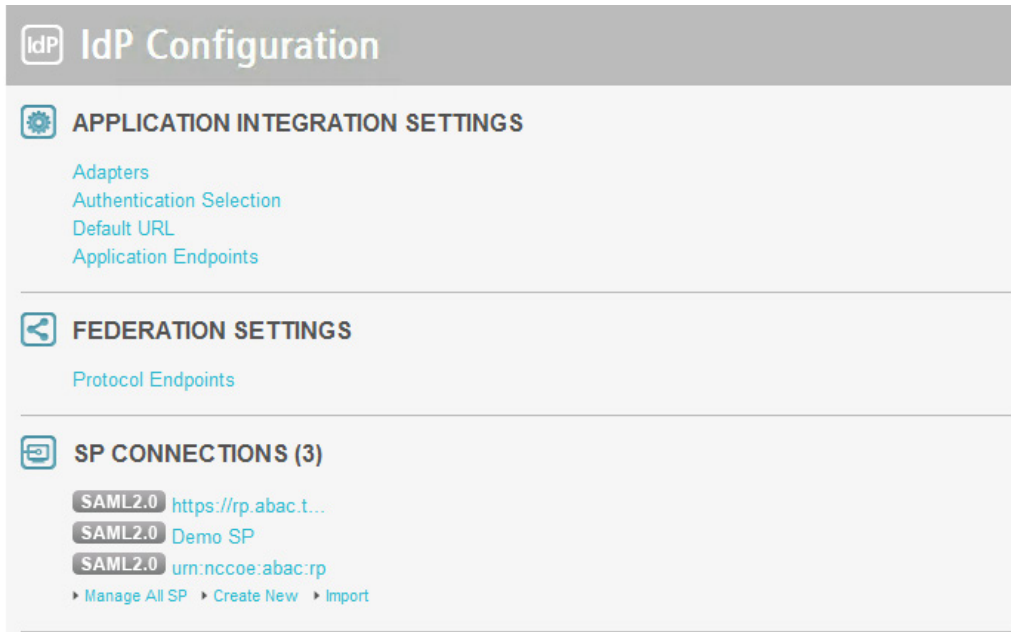
1558 17. Click **Next**.

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.



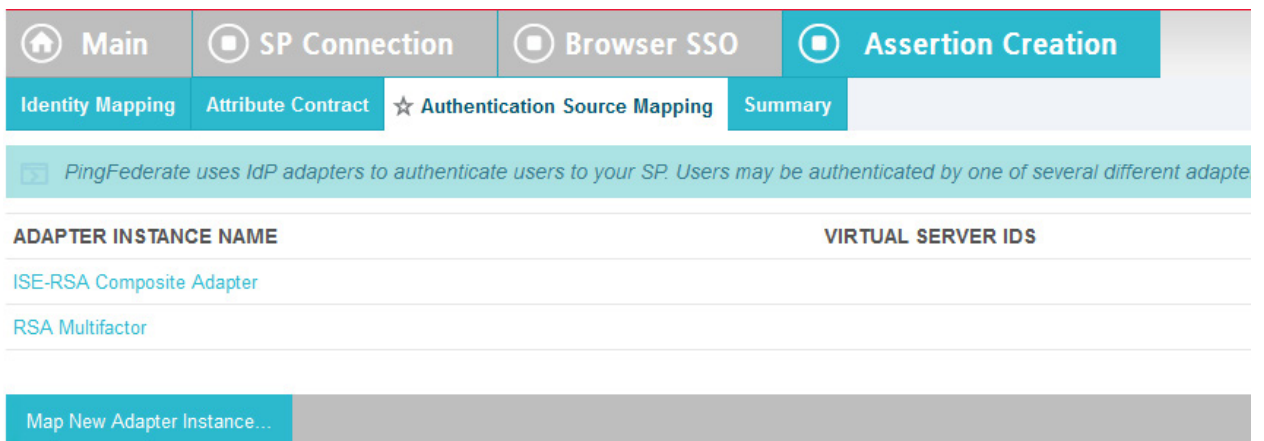
1563

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



1565

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



1567

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

★ **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

1570

1571

1572

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

1573

1574

7. Click **Next**.

1575

8. Click **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.

Home Main SP Connection Browser SSO Assertion Creation IdP Adapter Mapping

Attribute Sources & User Lookup

★ Data Store LDAP Directory Search LDAP Filter Summary

*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 for th*

Attribute Source Id:  \*

Attribute Source Description:  \*

Active Data Store:  \*

Data Store Type: LDAP

Manage Data Stores...

1579

1580 11. Click **Next**.

1581 12. In the BaseDN field, enter **DC=ABAC,DC=TEST**.

1582 13. Add all of the attributes from the LDAP Directory Search.

Attribute Sources & User Lookup

Data Store ★ LDAP Directory Search LDAP Filter Summary

*Please configure your directory search. This information, along with the attributes supplied in the contract, will be used to fulfill the contract.*

Base DN:

Search Scope:

Attributes to return from search

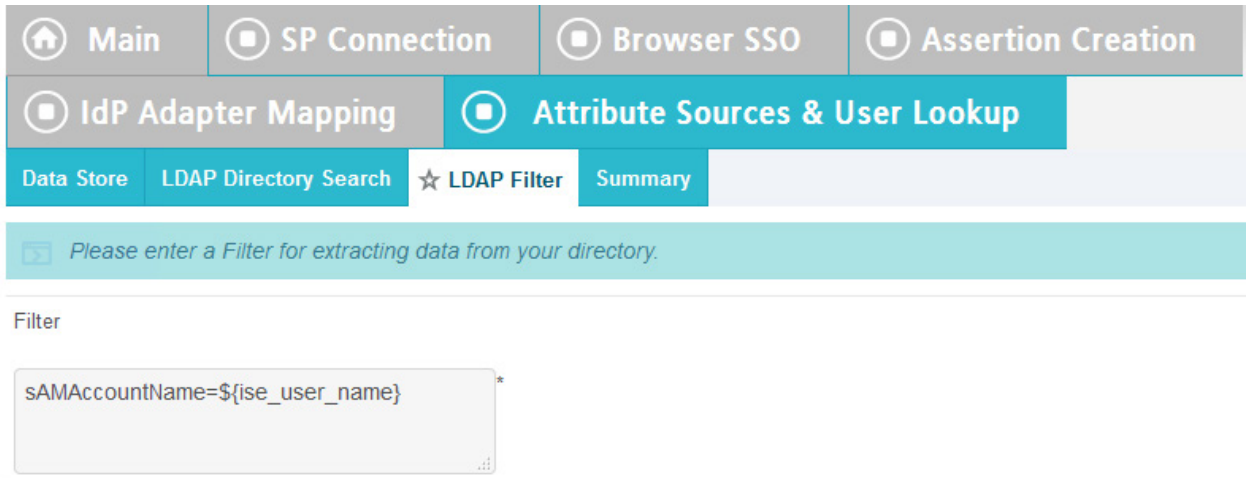
ROOT OBJECT CLASS	ATTRIBUTE	ACTION
	Subject DN	
	accountNumber	<a href="#">Remove</a>
	clearance	<a href="#">Remove</a>
	company	<a href="#">Remove</a>
	department	<a href="#">Remove</a>
	planName	<a href="#">Remove</a>
	role	<a href="#">Remove</a>
	staffLevel	<a href="#">Remove</a>
	state	<a href="#">Remove</a>
	title	<a href="#">Remove</a>
	userPrincipalName	<a href="#">Remove</a>

Enabled

1583

1584 14. Click **Next**.

1585 15. In the Filter field, enter **sAMAccountName=\${ise\_user\_name}**.

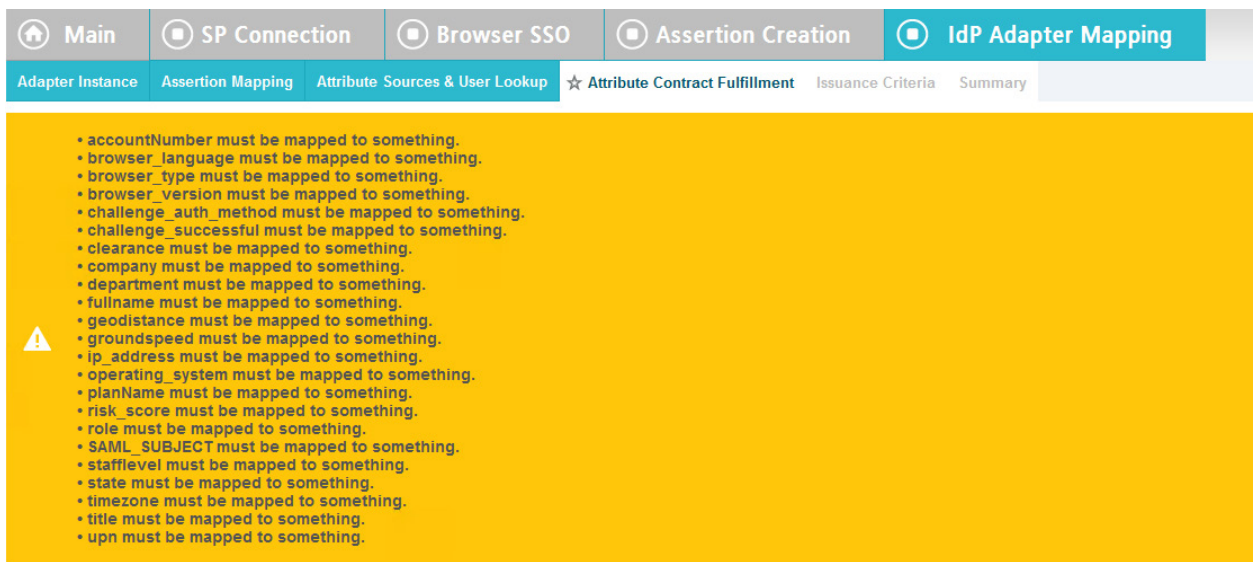


1586

1587 16. Click **Next**.

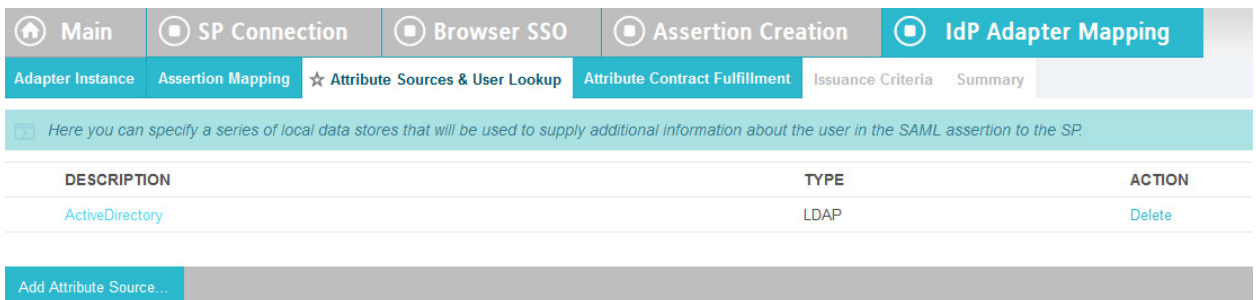
1588 17. Click **Save**.

1589 18. Click on **Attribute Sources & Data Store**.



1590

1591 19. Click on **Add Attribute Source**.



1592

1593 20. Enter **RSAAA** for Source Id and Description.

1594 21. Select **JDBC:sqlserver** in the Active Data Store drop-down.

Main | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Attribute Sources & User Lookup

★ Data Store | Database Table and Columns | Database Filter | Summary

*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.*

Attribute Source Id: RSAAA \*

Attribute Source Description: RSAAA \*

Active Data Store: jdbc:sqlserver://10.33.7.12:1433;databaseName=RSA\_CORE\_AA \*

Data Store Type: JDBC

Manage Data Stores...

1595

1596 22. Click **Next**.

1597 23. Select **dbo** in the Scheme drop-down.

1598 24. Select **EVENT\_LOG** in the Table drop-down.

1599 25. Add each of the columns from the table.

Main | SP Connection | Browser SSO | Assertion Creation | IdP Adapter Mapping

Attribute Sources & User Lookup

Data Store | ★ Database Table and Columns | Database Filter | Summary

*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.*

Schema: dbo

Table: EVENT\_LOG \*

Columns to return from SELECT

BROWSER_LANGUAGE	Remove
BROWSER_TYPE	Remove
BROWSER_VERSION	Remove
CHALLENGE_AUTH_METHOD	Remove
CHALLENGE_SUCCESSFUL	Remove
GEODISTANCE	Remove
GROUNDSPEED	Remove
IP_ADDRESS	Remove
OPERATING_SYSTEM	Remove
RISK_SCORE	Remove
TIMEZONE	Remove

ACCEPT\_LANGUAGE | Add Attribute

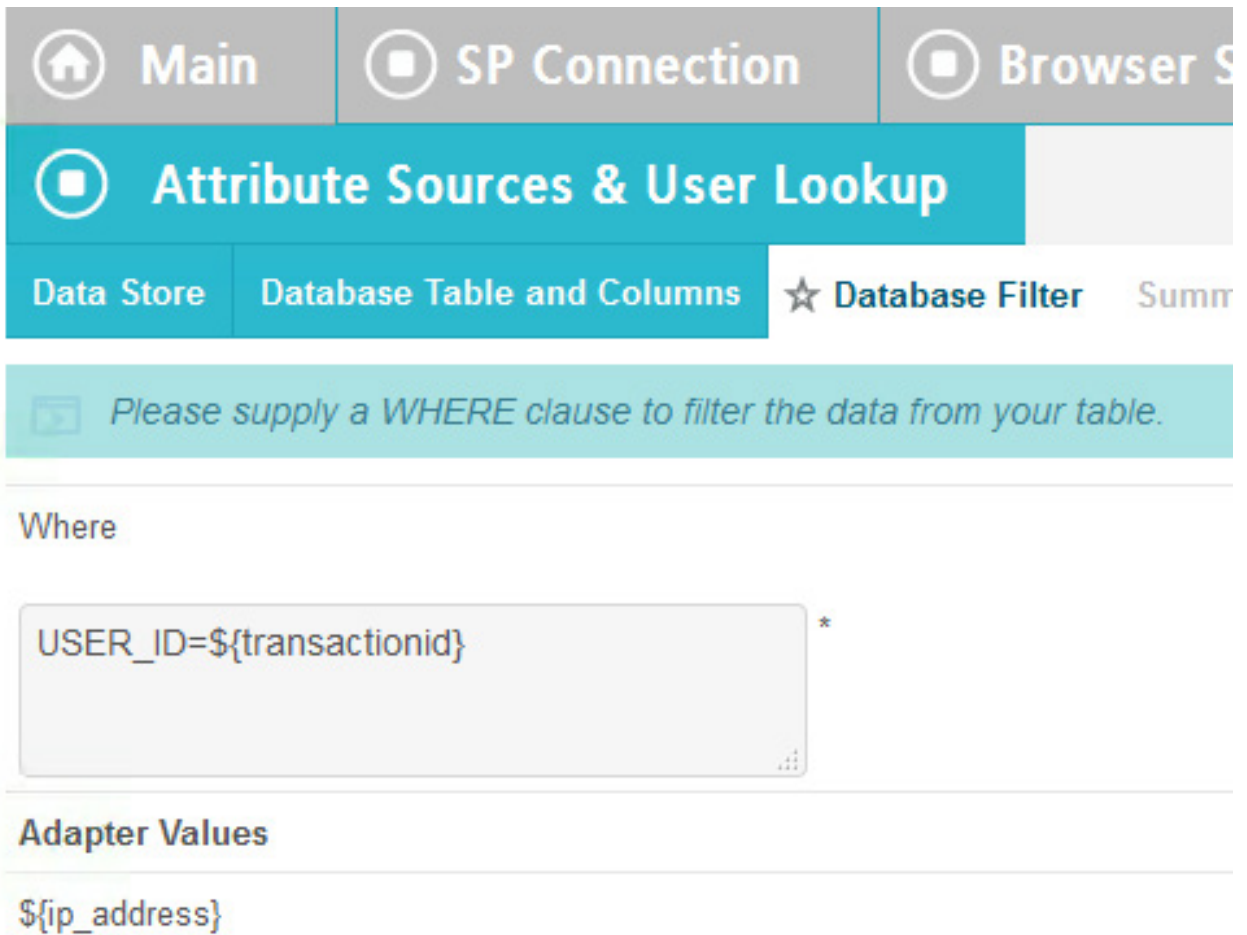
Refresh

[View Attribute Contract](#)

1600

1601 26. Click **Next**.

1602 27. In the Where field, enter **USER\_ID=\${transactionid}**.



1603

1604 28. Click **Next**.

1605 29. Click **Done**.

1606 30. Click **Next**.

1607 31. Map all the attributes as shown in the screenshot below.



Main		SP Connection		Browser SSO		Assertion Creation		IdP Adapter Mapping	
Adapter Instance		Assertion Mapping		Attribute Sources & User Lookup		★ Attribute Contract Fulfillment		Issuance Criteria	
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

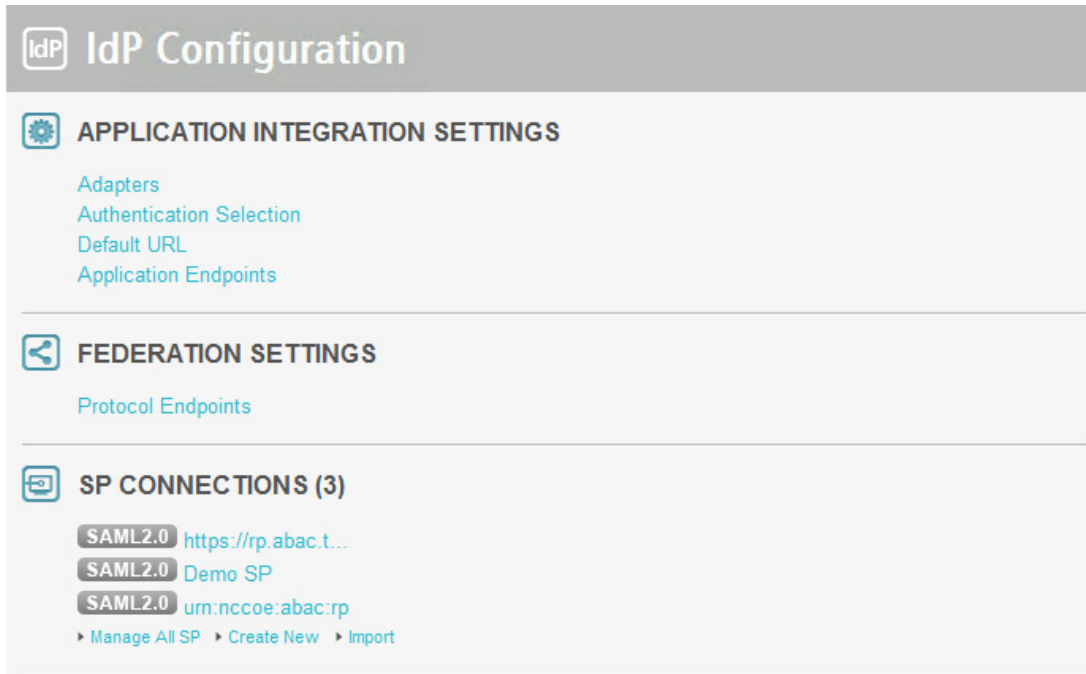
33. Click **Next**.

1611

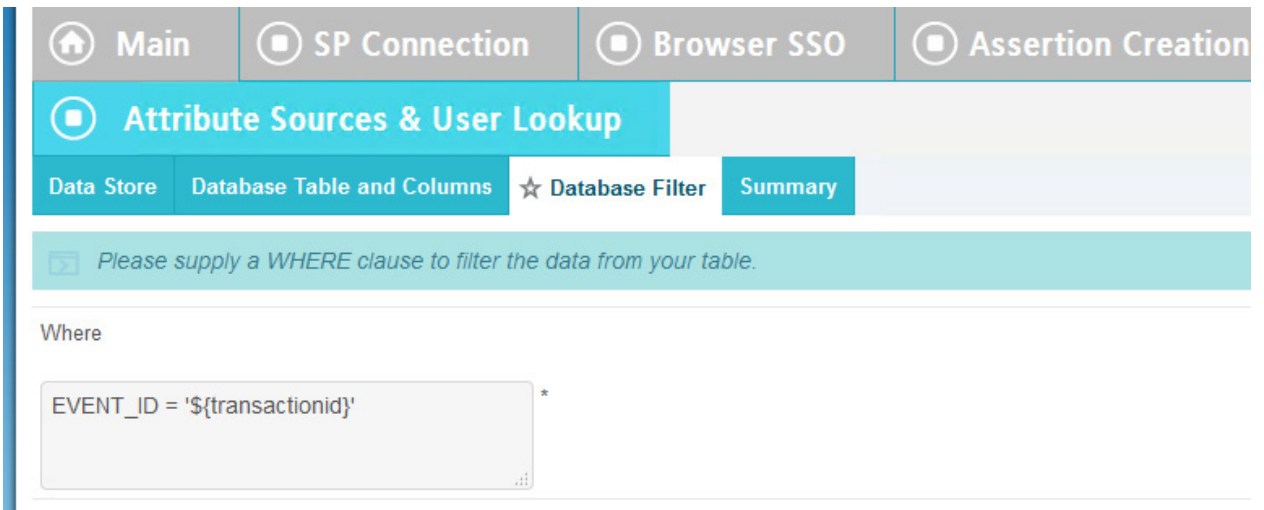
34. Click **Save**.

1612

35. Back at the main page, click on **rp.abac.test** under SP Connections.



1613

1614 36. Scroll down and click on **Database Filter**.1615 37. In the Where field, enter **EVENT\_ID=\${transactionid}**.

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.

### 1640 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.

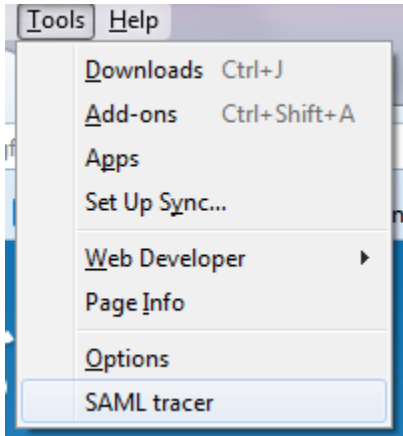
1653 [https://documentation.pingidentity.com/display/PF73/Digital+Signing+and+Decryption+Keys+a  
1654 nd+Certificates](https://documentation.pingidentity.com/display/PF73/Digital+Signing+and+Decryption+Keys+and+Certificates)

### 1655 2.15 Functional Test of All Configurations for Section 2

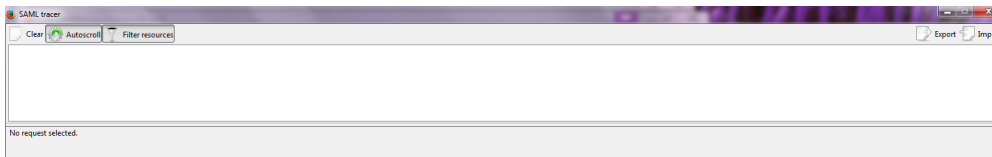
1656 The instructions in this section will help perform an integrated test all of the configurations in Section 2.  
1657 Using the browser and PingFederate, a user will log on and validate that the federated authentication to  
1658 Microsoft AD and RSA AA are properly configured.

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.

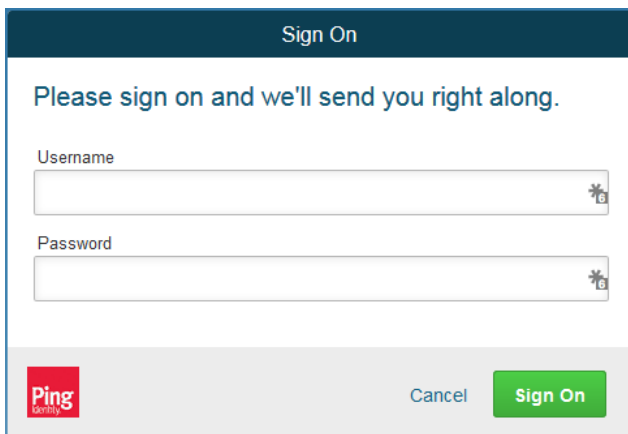


- 1664
- 1665 This will launch an empty SAML tracer window.



- 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., **lsmith**).
- 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  
lsmith

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 username or password you entered.”

1679

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  
lsmith

Password

Ping Identity

Cancel Sign On

1680

1681

8. Close the existing browser and launch a new browser.

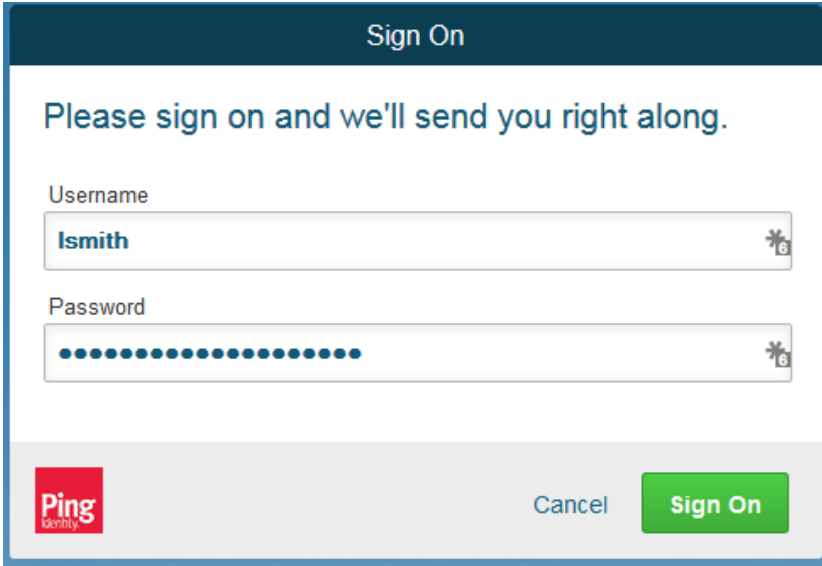
1682

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., **lsmith**). Then, enter the correct password.

1684



1685

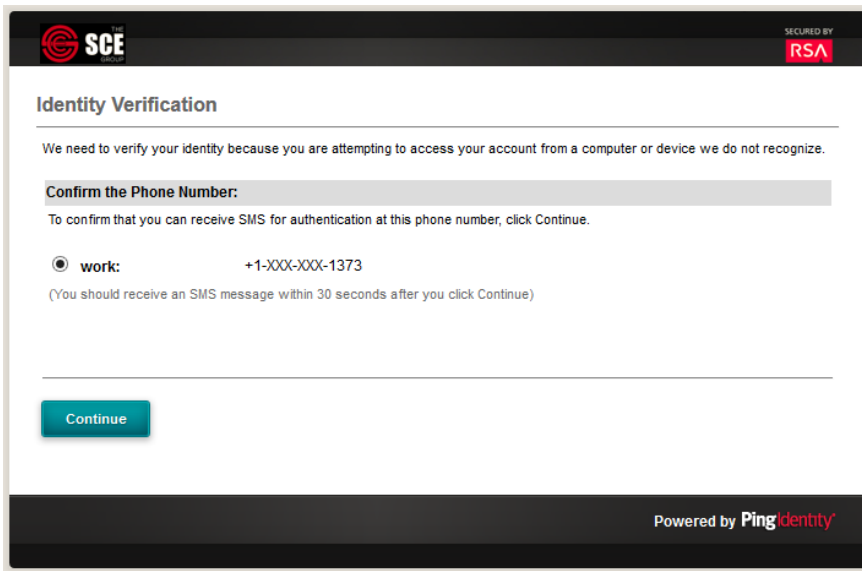
1686

11. Click **Sign On**.

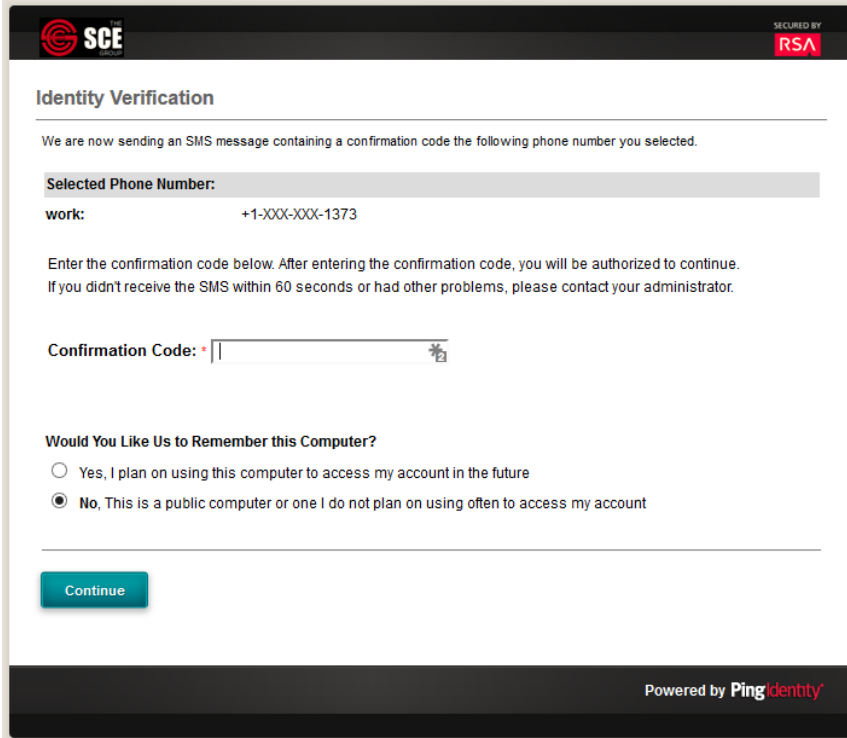
1687

Expected Result: You should see the two-factor RSA AA plug-in screen. This screen prompts you to enter the SMS text validation code received by your mobile phone.

1688



1689



1690

1691

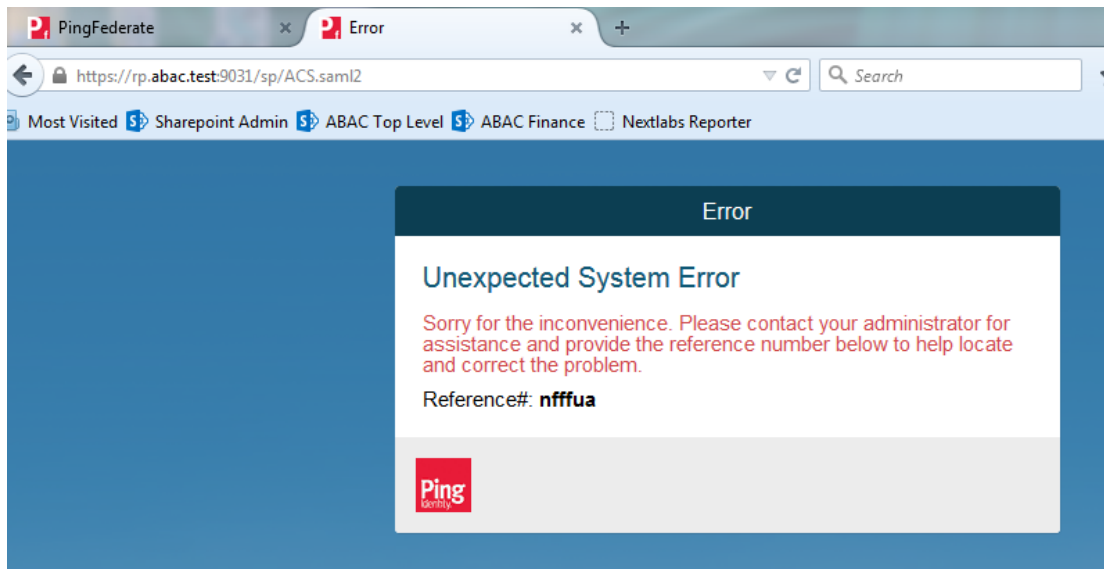
1692

12. Enter the SMS validation code received on your mobile phone and proceed. This will initiate a 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.



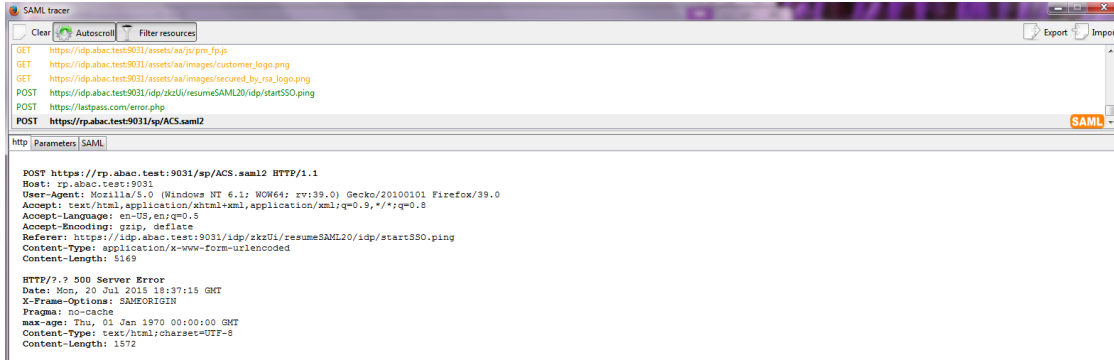
1695

1696

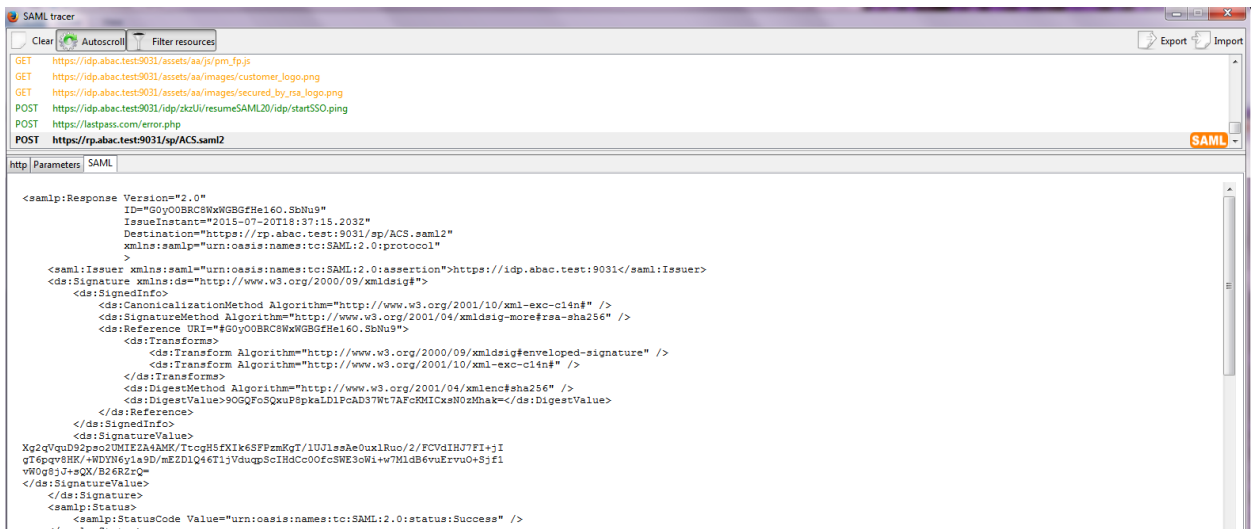
1697

1698

13. Go back to the SAML tracer window. Scroll to the bottom of the list of messages in the upper pane. 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.



- 1699
- 1700 Expected Result: In the details page at the bottom, on the **http** tab, you should see that the
- 1701 browser sent a **POST** message to the RP's PingFederate server **rp.abac.test**. The HTTP response
- 1702 status code (identified on the line that begins with **HTTP**) should be a **500 Server Error**.
- 1703 14. Click on the **SAML** tab.



- 1704
- 1705 Expected Result: You should see the details of the SAML message, including the Issuer. The
- 1706 Issuer should be the IdP's Federation server, **idp.abac.test**.

## 1707 3 Setting up Federated Authentication Between the Relying 1708 Party and the Identity Provider

### 1709 3.1 Introduction

1710 In the previous section of this How-To Guide we demonstrated how to set up federated, SAML-based  
1711 authentication at the identity provider (IdP). Before continuing with this section, it is necessary to have a  
1712 working federation service that will represent the identity provider and can receive and issue SAML 2.0  
1713 request and responses. For instructions on how to set this up using Ping Federate, please refer to  
1714 [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:

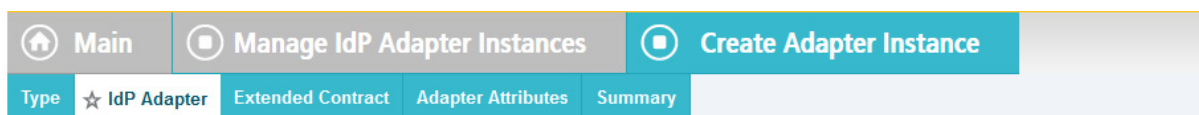
- 1729     ▪ **PingFederate-IdP:** A federation system or trust broker for the identity provider
- 1730     ▪ **PingFederate-RP:** Serves as the trust broker for SharePoint

### 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:  
 1758 *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**.

The screenshot shows the 'Export Metadata' interface. At the top, there are navigation tabs: 'Main', 'Export Metadata' (active), and 'Export & Summary'. Below the tabs, there are sub-tabs: 'Metadata Mode', 'Connection Metadata', 'Metadata Signing', and 'Export & Summary'. A teal banner contains the text: 'You can generate metadata specific to a connection, including the Attribute Contract and public key. Or you can provide a new contract and select a key manually. The resulting metadata may be shared with your partner to simplify connection creation.' Below the banner, there are three radio button options: 'Use a connection for metadata generation' (selected), 'Select information to include in metadata manually', and 'Use the secondary port for SOAP channel'.

- 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.

Main Export Metadata

Metadata Mode ☆ Connection Metadata Metadata Signing Export & Summary

Select a connection that contains the Attribute Contract and Digital Signature Key you wish to include in the metadata.

https://rp.abac.test.9031 \*

**ATTRIBUTE CONTRACT**

SAML\_SUBJECT

**DIGITAL SIGNATURE KEY**

CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US

**XML ENCRYPTION KEY**

No XML key available for this connection

Cancel < Previous Next >

1768

1769

1770

7. Click **Next**. On the Metadata Signing screen, if you plan to sign the metadata file that will be exported, select the certificate that will be use to sign the file.

Main Export Metadata

Metadata Mode Connection Metadata ☆ Metadata Signing Export & Summary

From this list of certificates, choose which one to use for signing the selected file.

Signing Certificate - SELECT -

Manage Certificates...

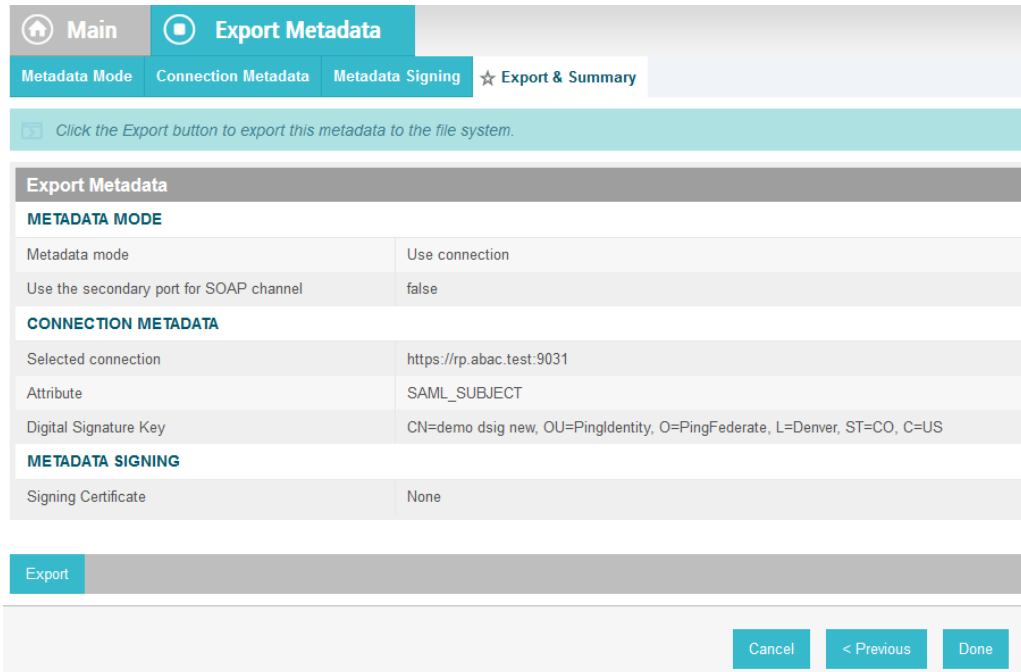
1771

1772

1773

8. Click **Next**. On the Export & Summary screen, you should see a summary of the options that were selected.

Cancel < Previous Next >

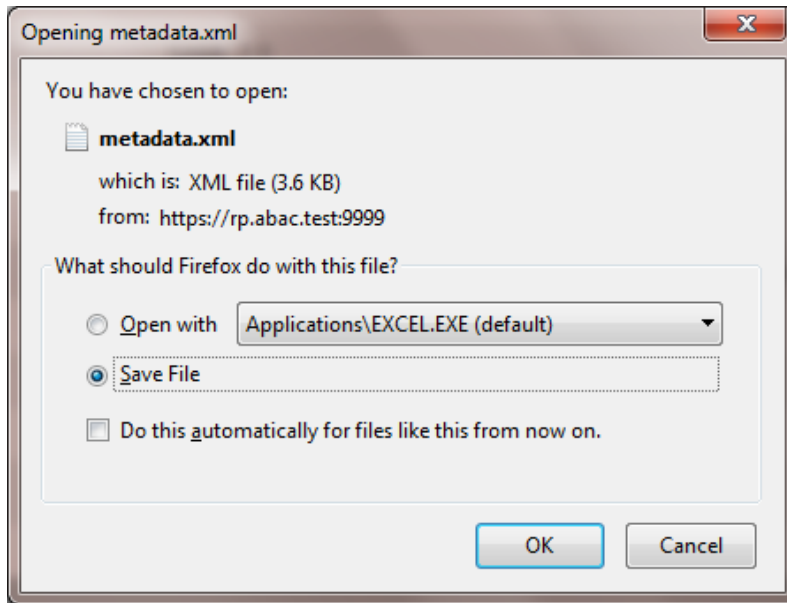


1774

1775

1776

9. Click **Export**. This will create an export file that contains the metadata of the identity provider that you can download using the browser.



1777

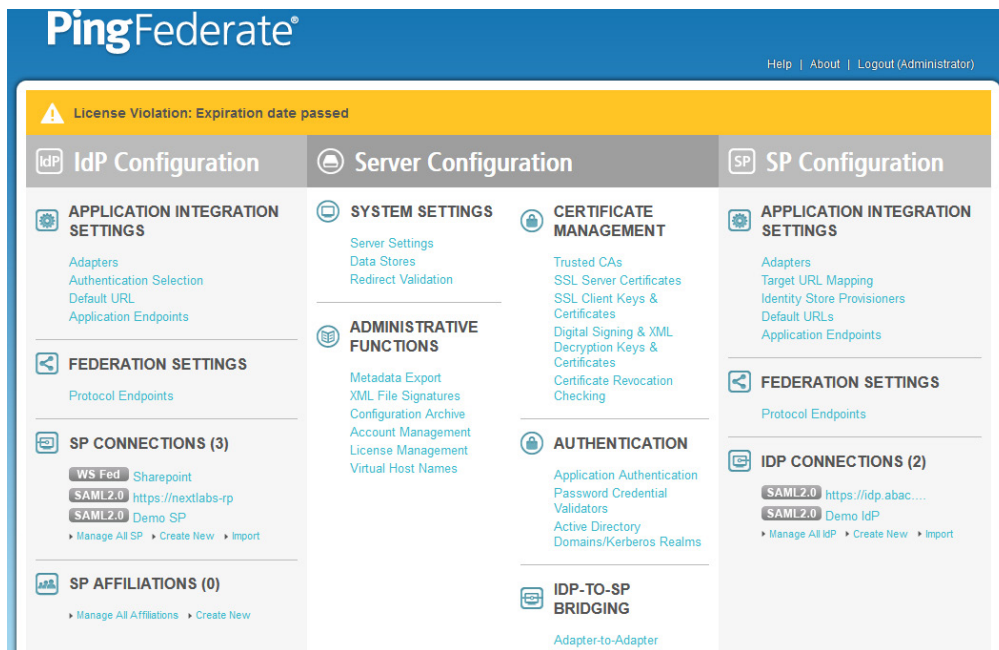
1778

10. Copy the metadata file to the server that hosts the PingFederate service for the relying party.

### 1779 3.4 Configure PingFederate-RP Connection to the PingFederate-IdP

1780 Follow the instructions in this section to configure a PingFederate connection from the relying party to  
1781 the identity provider.

- 1782 1. Logon to the server that hosts the PingFederate service for the relying party.
- 1783 2. Launch your browser and go to: *https://<DNS\_NAME>:9999/pingfederate/app*.
- 1784 3. Replace DNS\_NAME with the fully qualified name of the relying party's PingFederate server  
1785 (e.g., *https://rp.abac.test:9999/pingfederate/app*). Logon to the PingFederate application using  
1786 the credentials you configured in the previous installation section.



- 1787
- 1788 4. On the Main Menu under IDP CONNECTIONS, click **Create New**.
- 1789 5. On the Connection Type screen, select **Browser SSO Profiles**.

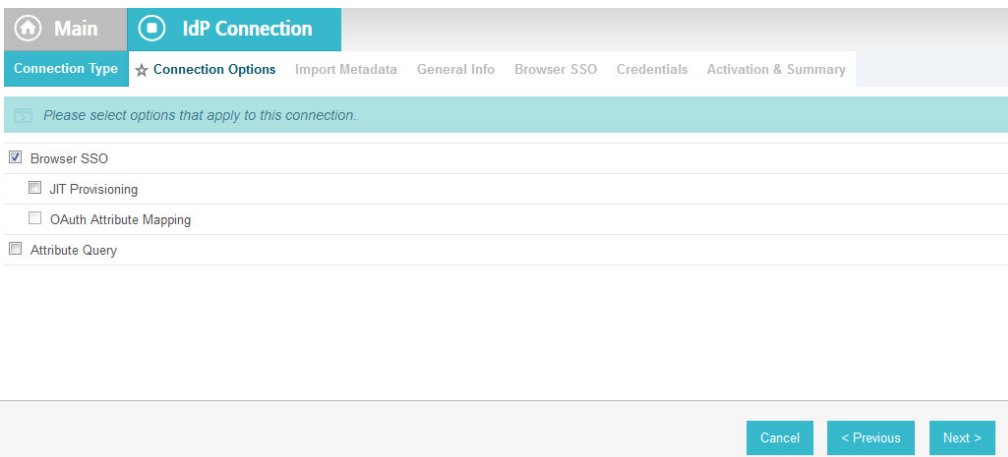


1790

1791

1792

6. Click **Next**.
7. On the Connection Options screen, make sure **Browser SSO** is selected.



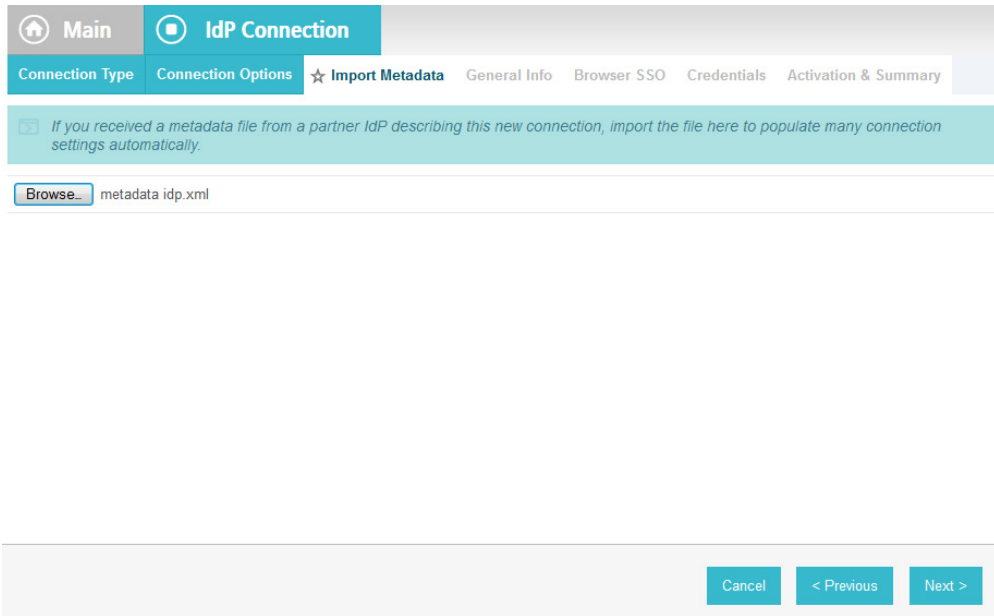
1793

1794

1795

1796

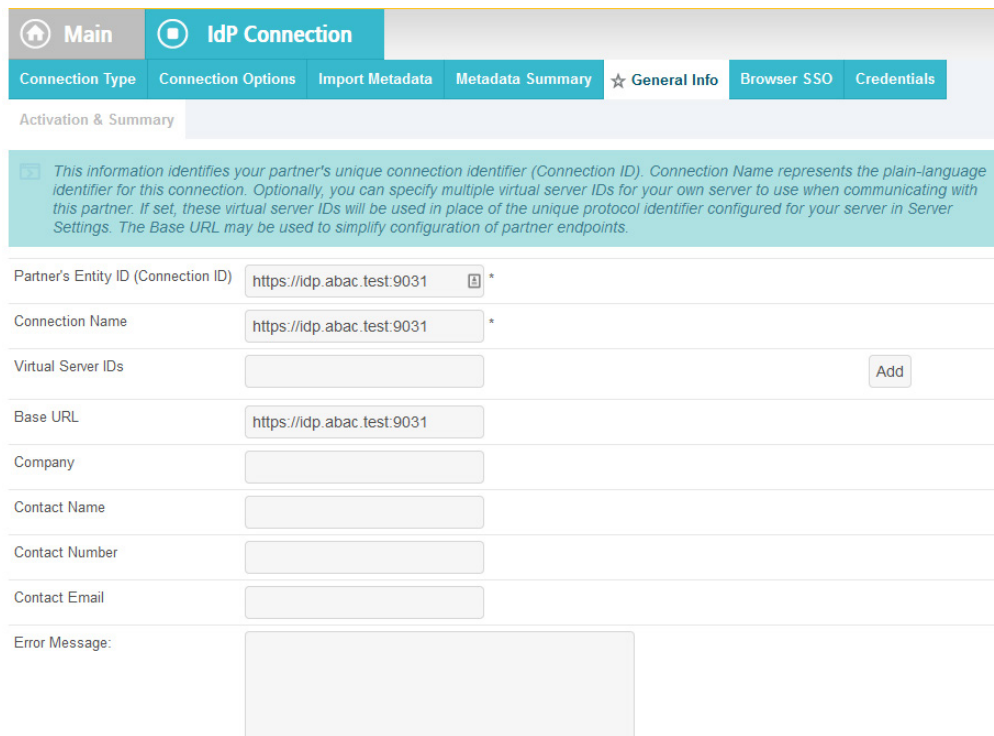
8. Click **Next**.
9. On the Import Metadata screen, click **Browse** and select the metadata file that you exported from the Identity Provider's PingFederate server.



1797

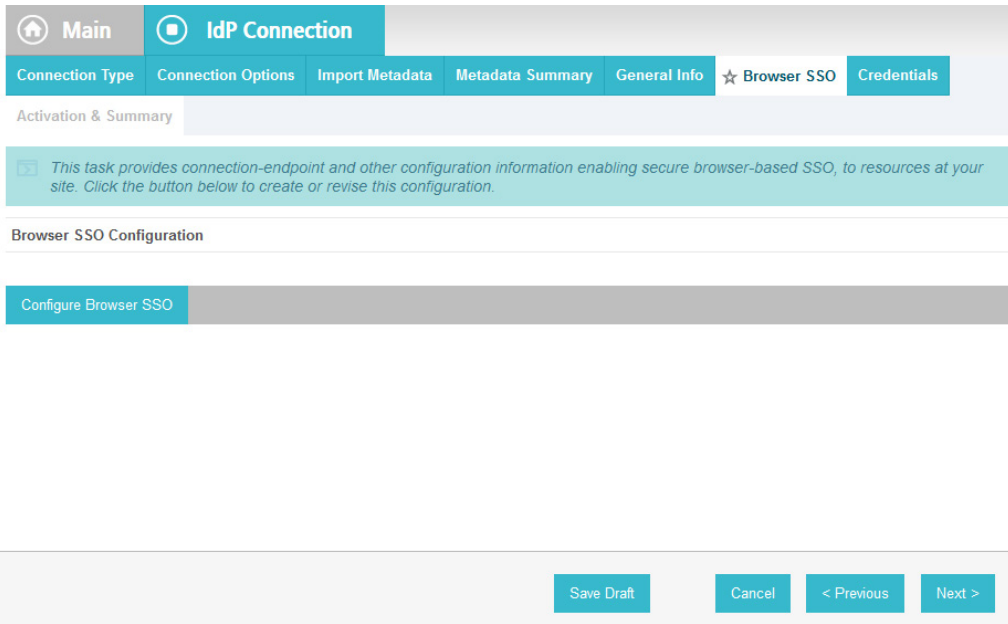
1798 10. Click **Next**.

1799 11. On the Metadata Summary screen, click **Next**. On the General Info screen, you should see some  
1800 configuration information (e.g., Base URL) about the identity provider that was taken from the  
1801 metadata file that you selected.



1802

1803 12. Click **Next**.



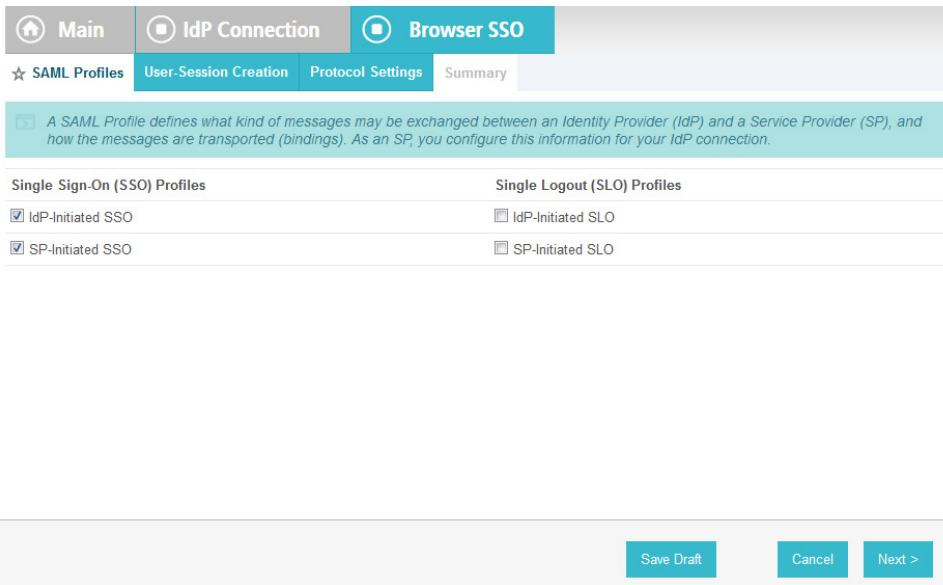
1804

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**.

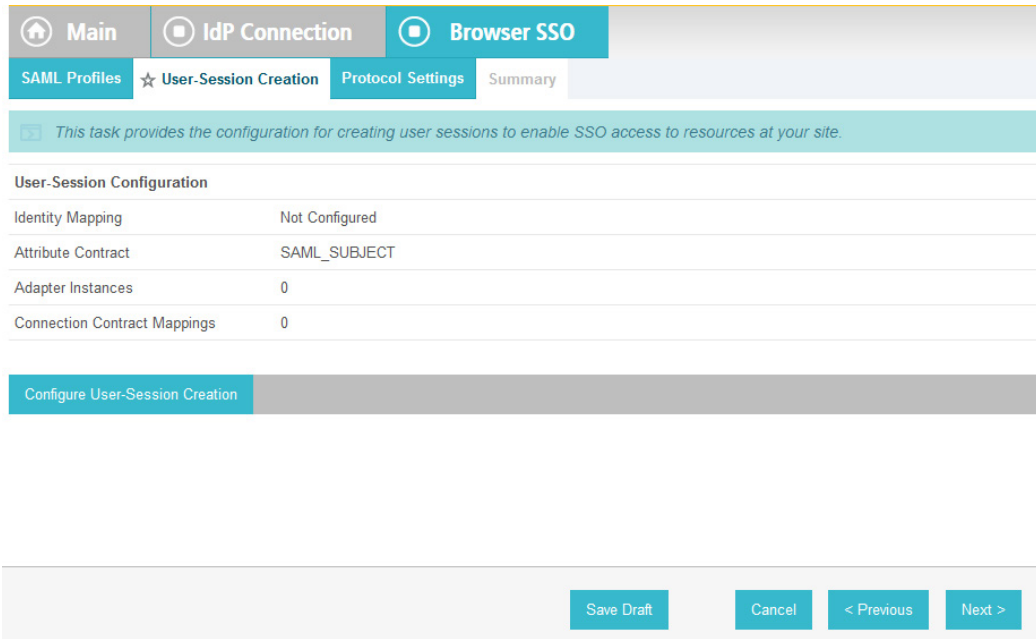


1807

1808

15. Click **Next**.

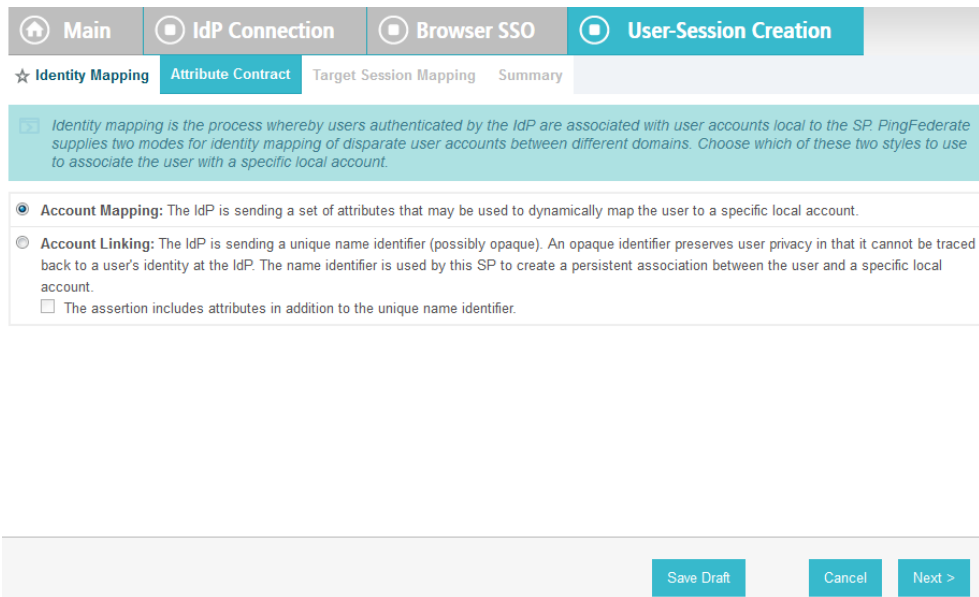




1809

1810

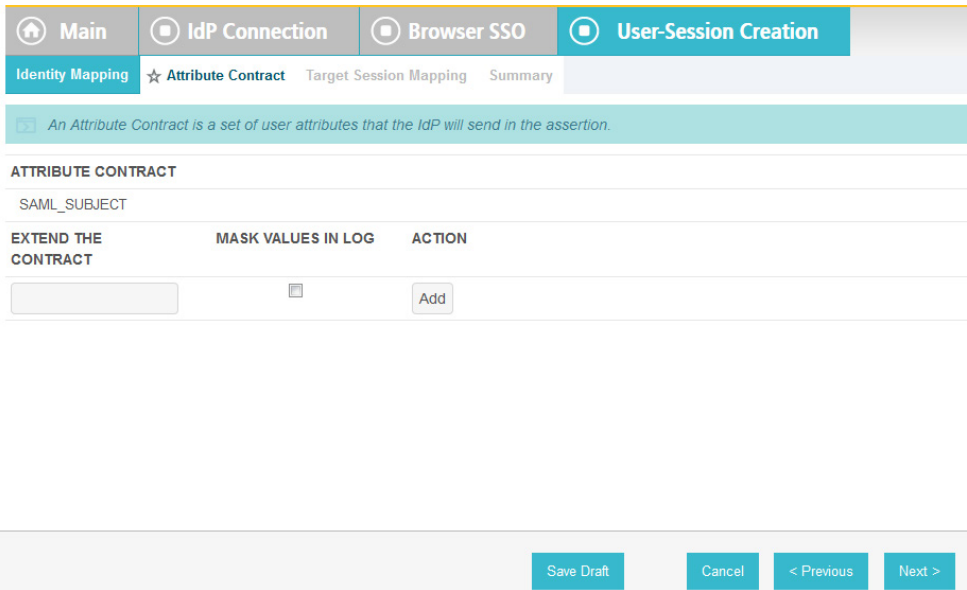
16. On the User-Session Creation screen, click **Configure User-Session Creation**.



1811

1812

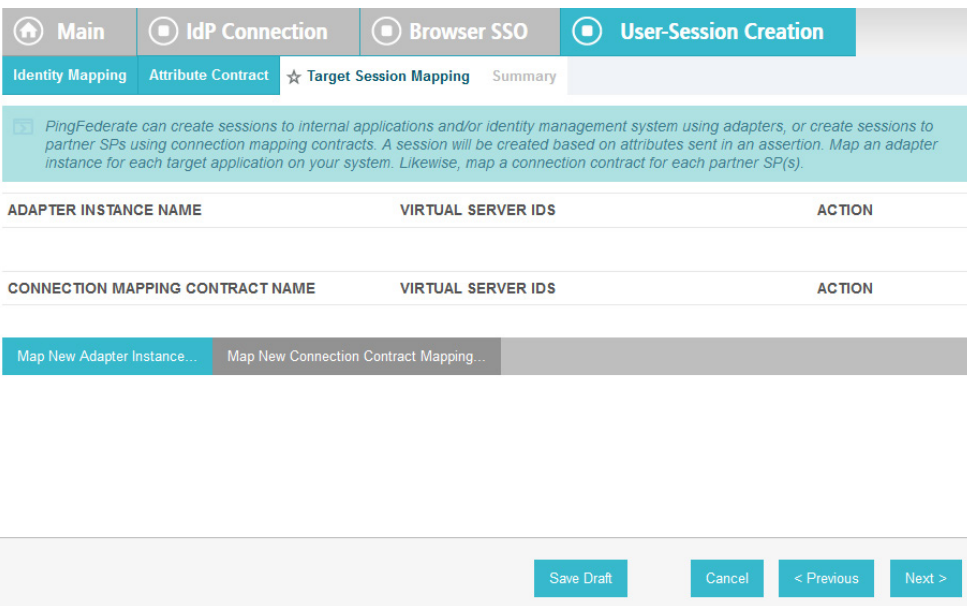
17. On the Identity Mapping screen, click **Next**.



1813

1814

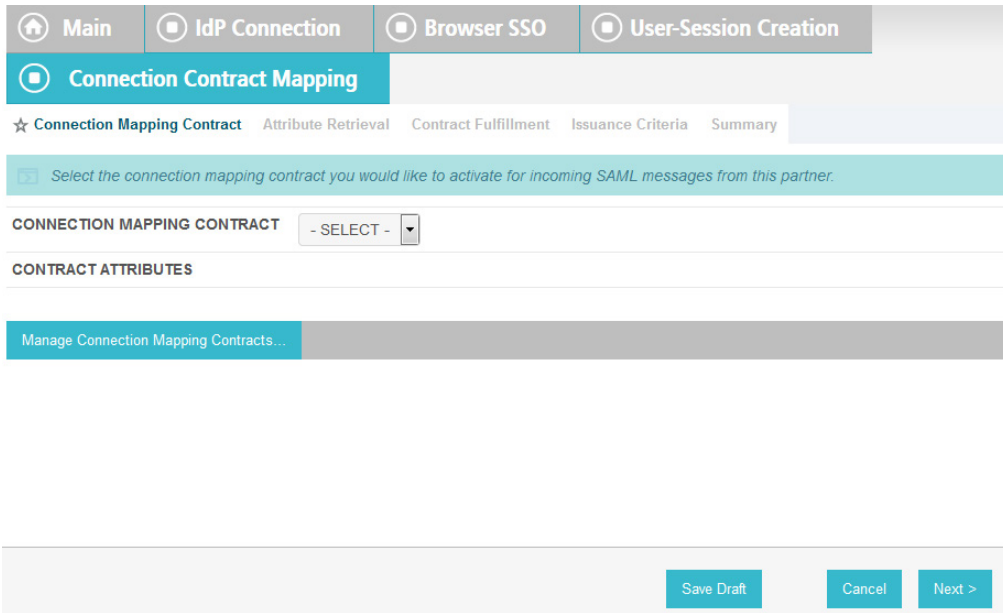
18. On the Attribute Contract screen, click **Next**.



1815

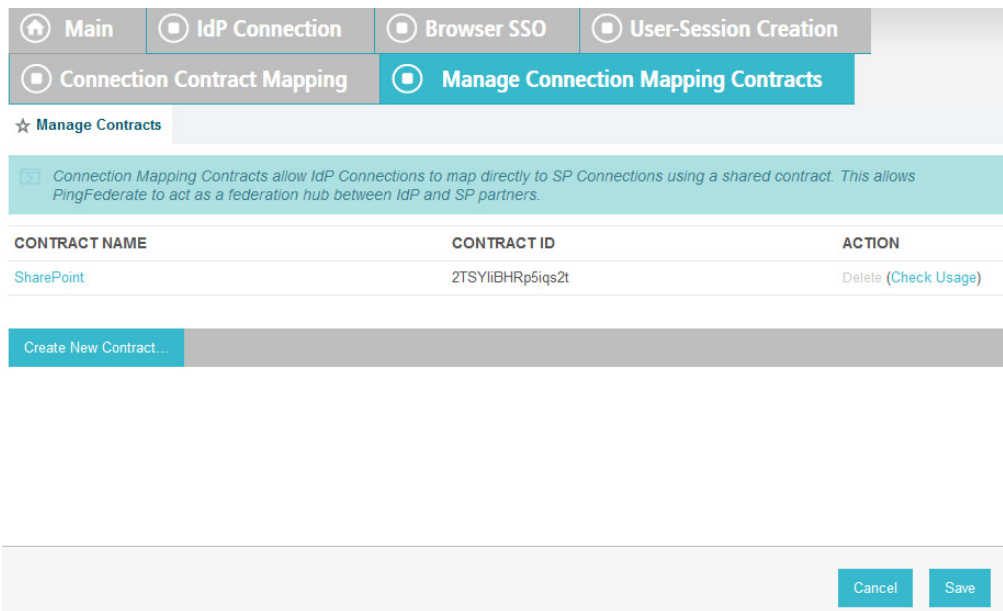
1816

19. On the Target Session Mapping screen, click **Map New Connection Contract Mapping**.



1817

1818 20. On the Connection Mapping Contract screen, click **Manage Connection Mapping Contracts**.



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).

Main IdP Connection Browser SSO User-Session Creation  
Connection Contract Mapping Manage Connection Mapping Contracts  
Connection Mapping Contract  
☆ Contract Info Contract Attributes Summary  
Define the name of the contract. The ID is automatically generated by PingFederate.  
Contract Name Sharepoint 2013 \*  
Cancel Next >

1822

1823

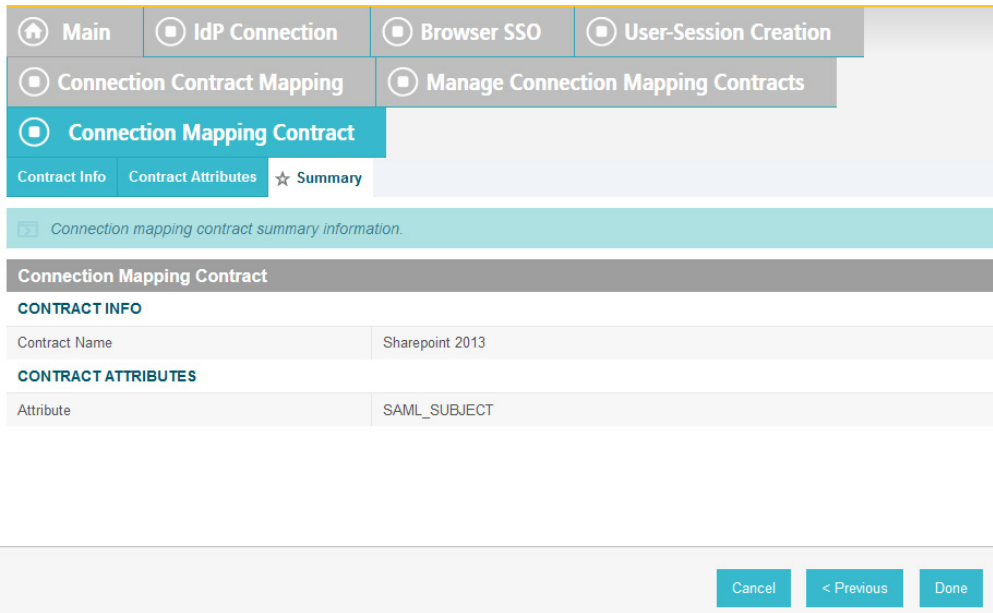
23. Click **Next**.

Main IdP Connection Browser SSO User-Session Creation  
Connection Contract Mapping Manage Connection Mapping Contracts  
Connection Mapping Contract  
Contract Info ☆ Contract Attributes Summary  
Define the set of attributes that the IdP connection will send to the SP connection.  
ATTRIBUTE CONTRACT  
SAML\_SUBJECT  
EXTEND THE CONTRACT ACTION  
Add  
Cancel < Previous Next >

1824

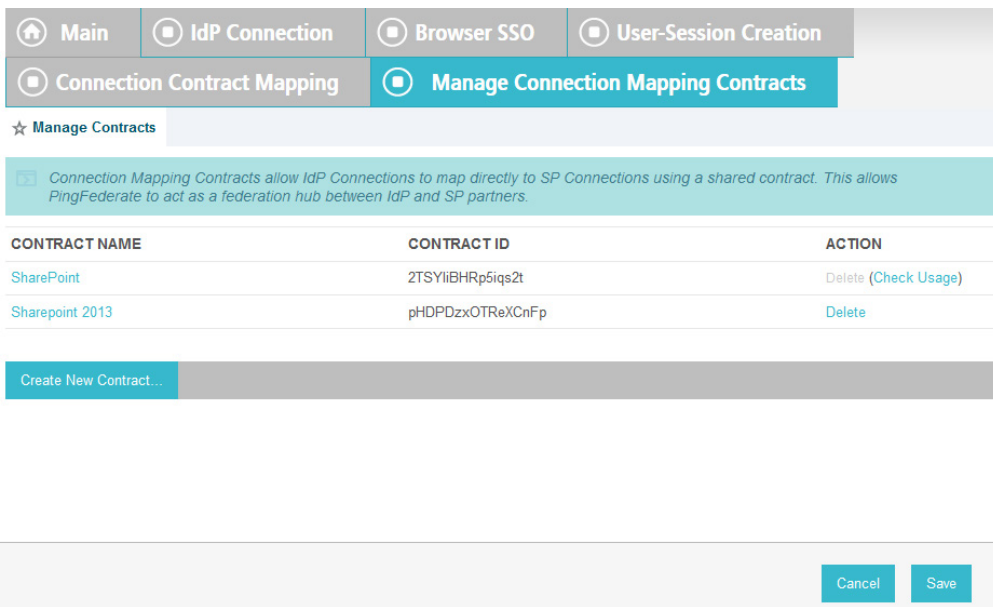
1825

24. Click **Next**.



1826

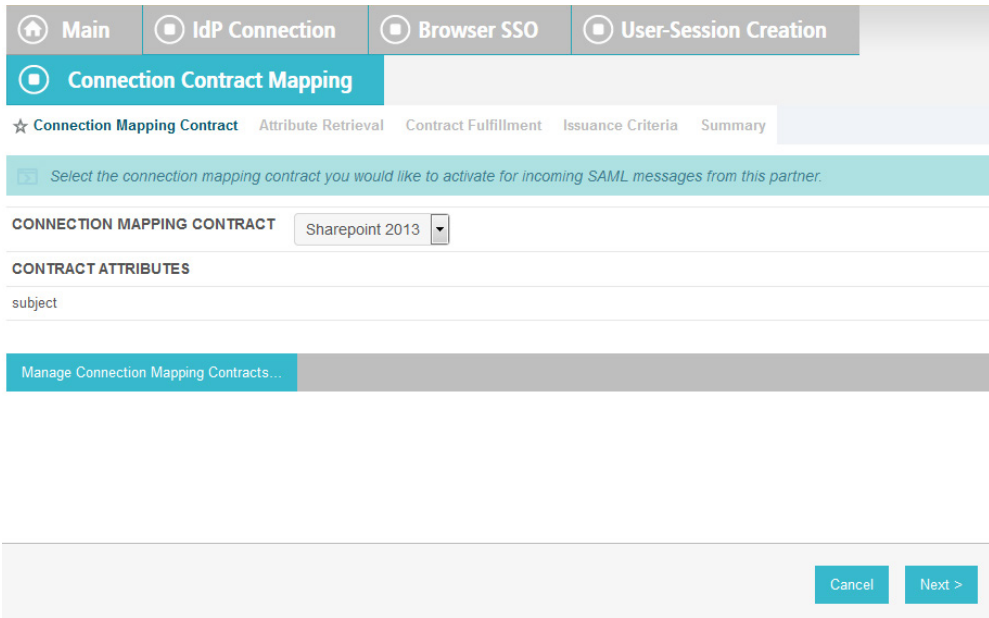
1827 25. On the Summary screen, click **Done**.



1828

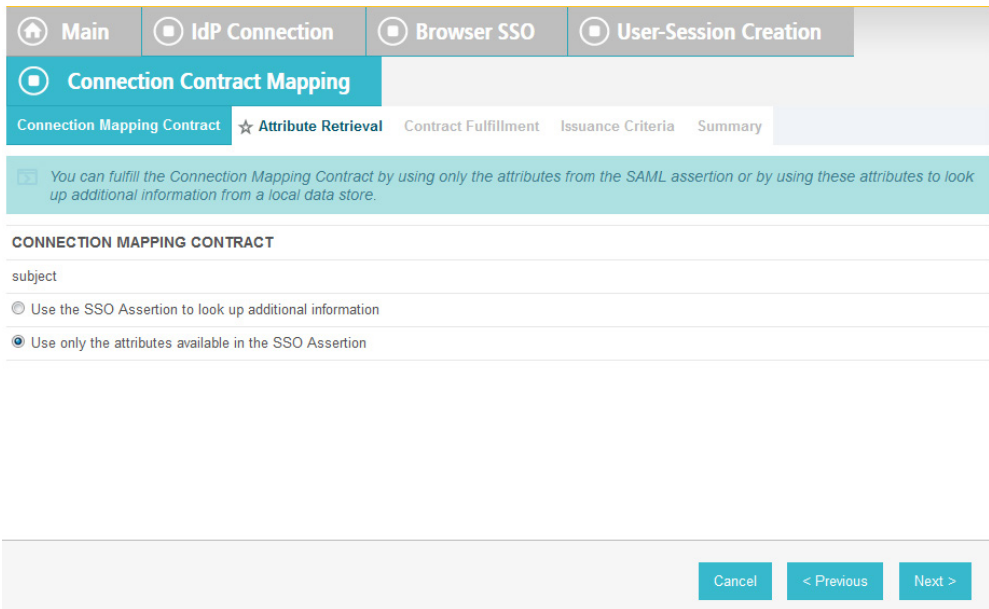
1829 26. On the Manage Contracts screen, you should see the new contract listed. Click **Save**.

1830 27. On the Connection Mapping Contract screen, for the CONNECTION MAPPING CONTRACT field  
 1831 select the name of the new contract that was created (e.g., **SharePoint 2013**).



1832

1833 28. Click **Next**. On the Attribute Retrieval screen, select **Use only the attributes available in the SSO**  
1834 **Assertion**.



1835

1836 29. Click **Next**. On the Contract Fulfillment screen, for the SOURCE field select **Assertion**. For the  
1837 VALUE field, select **SAML\_SUBJECT**.

1838

1839 30. Click **Next**.

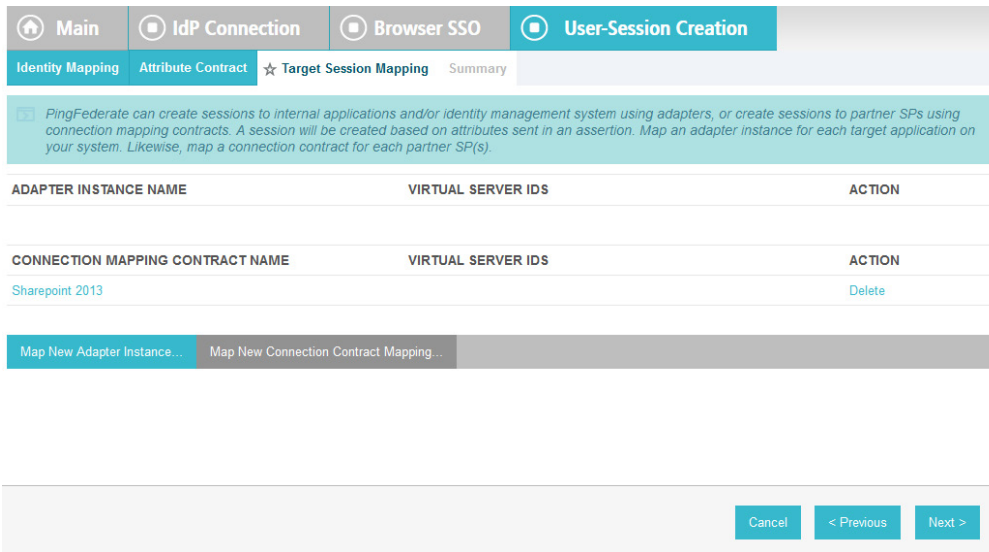
1840

1841 31. On the Issuance Criteria screen, click **Next**.

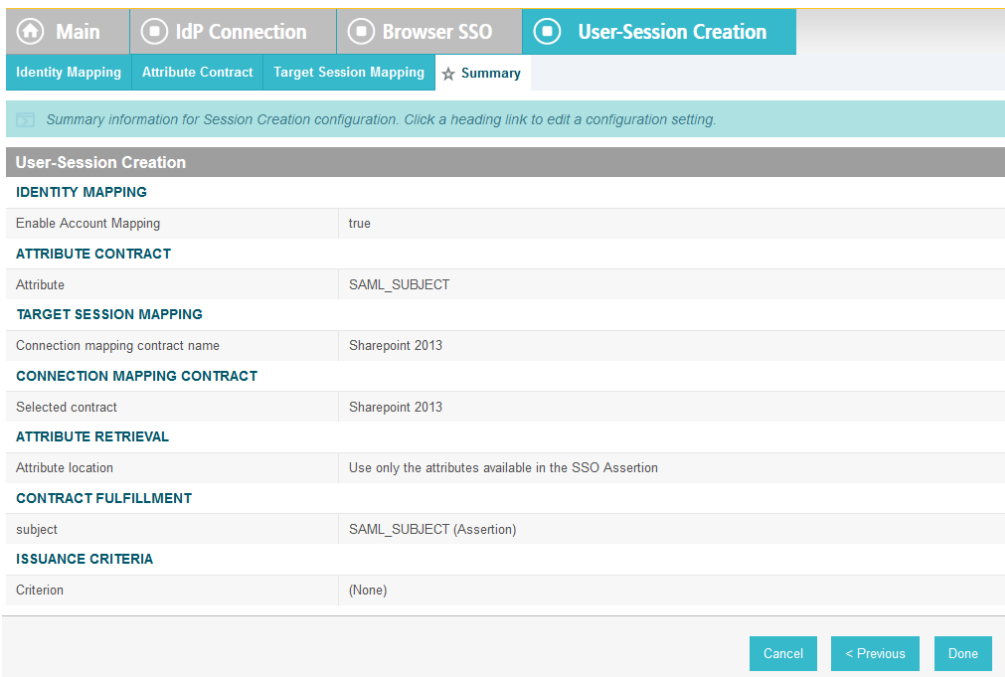
1842

1843 32. On the Summary screen, click **Done**.

- 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.

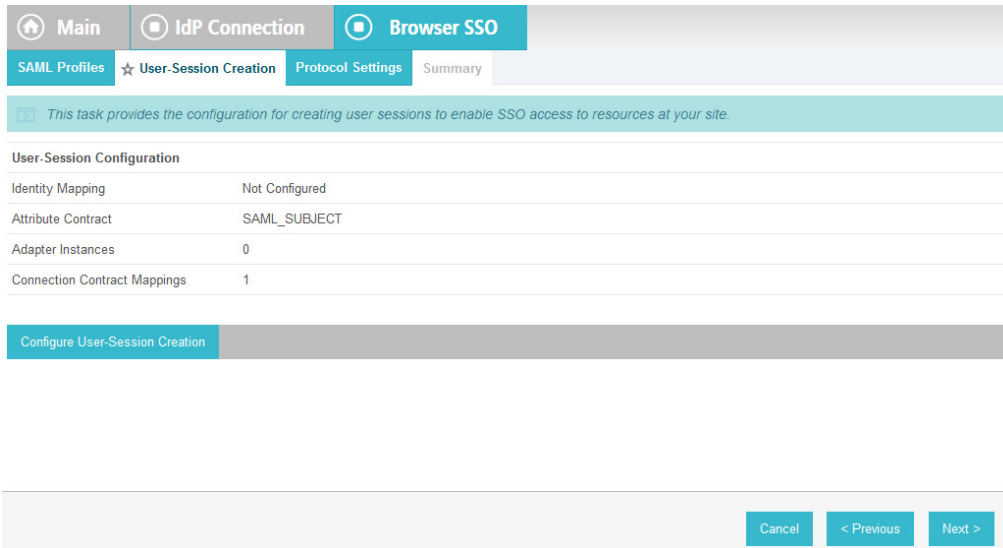


- 1846  
 1847 34. Click **Next**.



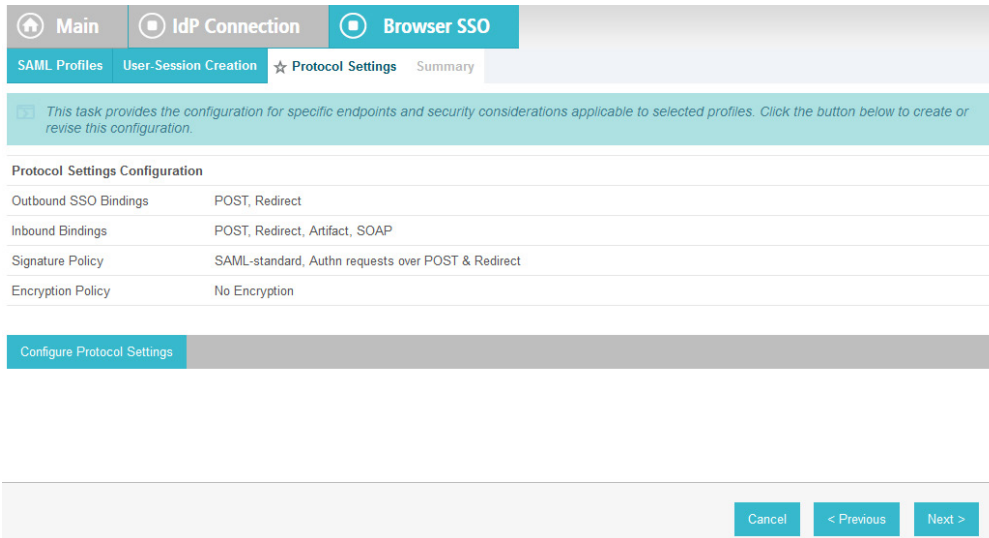
- 1848  
 1849 35. Click **Done**.





1850

1851 36. On the User-Session Creation screen, click **Next**.



1852

1853 37. On the Protocol Settings screen, click **Configure Protocol Settings**. This will bring up a sequence  
1854 of sub-screens.

As the SP, you send authentication requests (AuthnRequests) for single sign-on to the IdP's SSO Service. Depending on the situation, the IdP may have several endpoints available. Please provide the endpoints that you want to use when sending these requests.

BINDING	ENDPOINT URL	ACTION
POST	/idp/SSO.saml2	Edit / Delete
Redirect	/idp/SSO.saml2	Edit / Delete
- SELECT -		Add

Cancel Next >

1855

1856 38. On the SSO Service URLs screen, click **Next**.

1857 39. On the Allowable SAML Bindings screen, select **POST** and select **Redirect**.

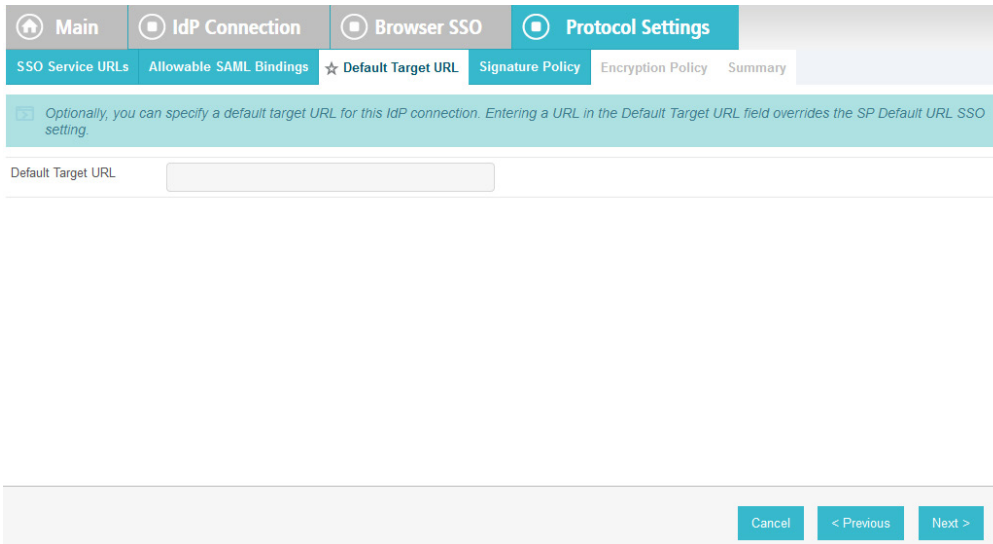
When the IdP sends messages, over what SAML bindings do you want to receive them?

- Artifact
- POST
- Redirect
- SOAP

Cancel < Previous Next >

1858

1859 40. Click **Next**.



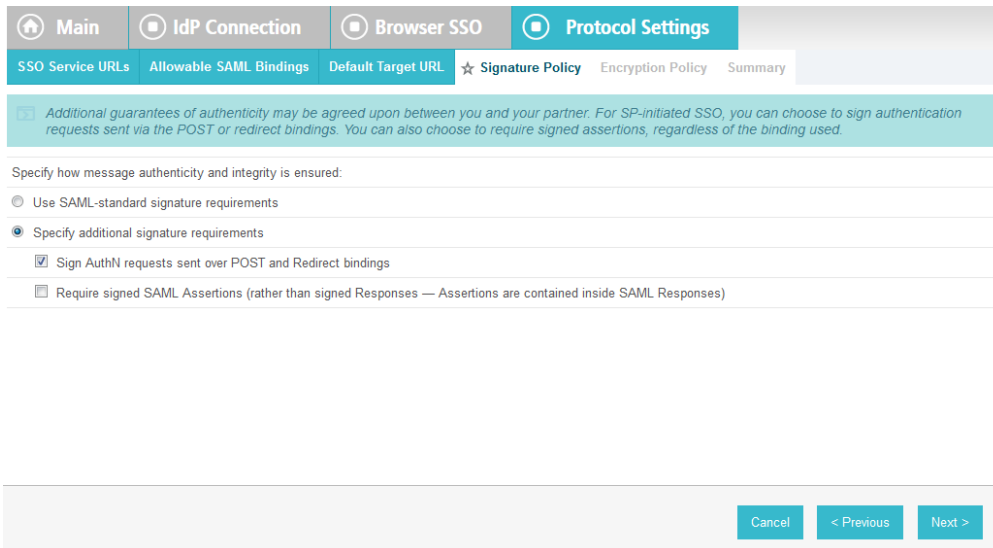
1860

1861 41. On the Default Target URL screen, click **Next**.

1862 42. On the Signature Policy screen, make sure that the following are selected:

1863 a. **Specify additional signature requirements and**

1864 b. **Sign AuthN requests sent over POST and Redirect bindings**



1865

1866 43. Click **Next**. On the Encryption Policy screen, select

1867 a. **Allow encrypted SAML Assertions and SLO messages and**

1868 b. **The entire assertion**

None  
 Allow encrypted SAML Assertions and SLO messages

The entire assertion  
 SAML\_SUBJECT (Name Identifier)  
 One or more attributes

[Cancel](#) [< Previous](#) [Next >](#)

1869

1870 44. Click **Next**.

[Main](#) [IdP Connection](#) [Browser SSO](#) [Protocol Settings](#)

[SSO Service URLs](#) [Allowable SAML Bindings](#) [Default Target URL](#) [Signature Policy](#) [Encryption Policy](#) [Summary](#)

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

**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**

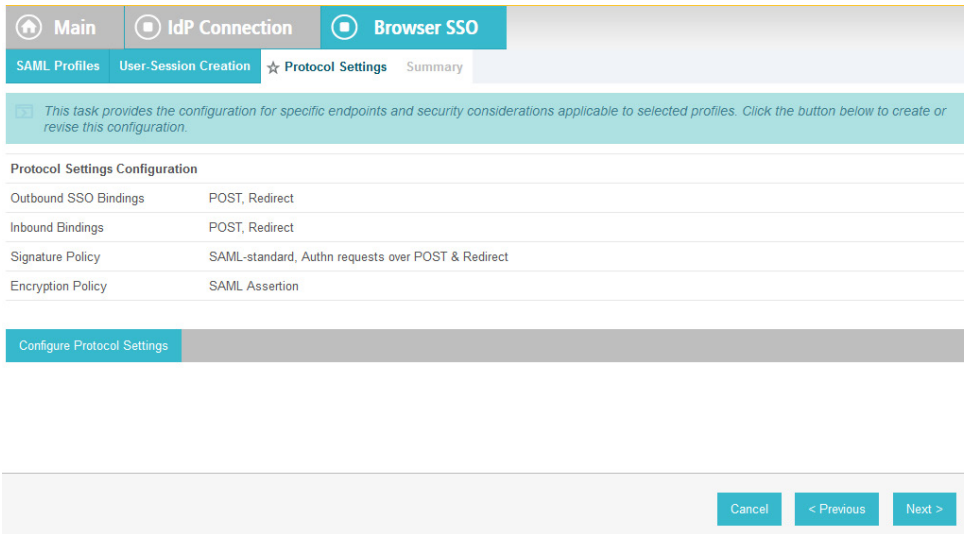
Sign AuthN requests over POST and Redirect	true
Require digitally signed SAML Assertion	false

**ENCRYPTION POLICY**

Encrypt Entire Assertion	true
Encrypt Name Identifier	false
Encrypt One or More Attributes	false

1871

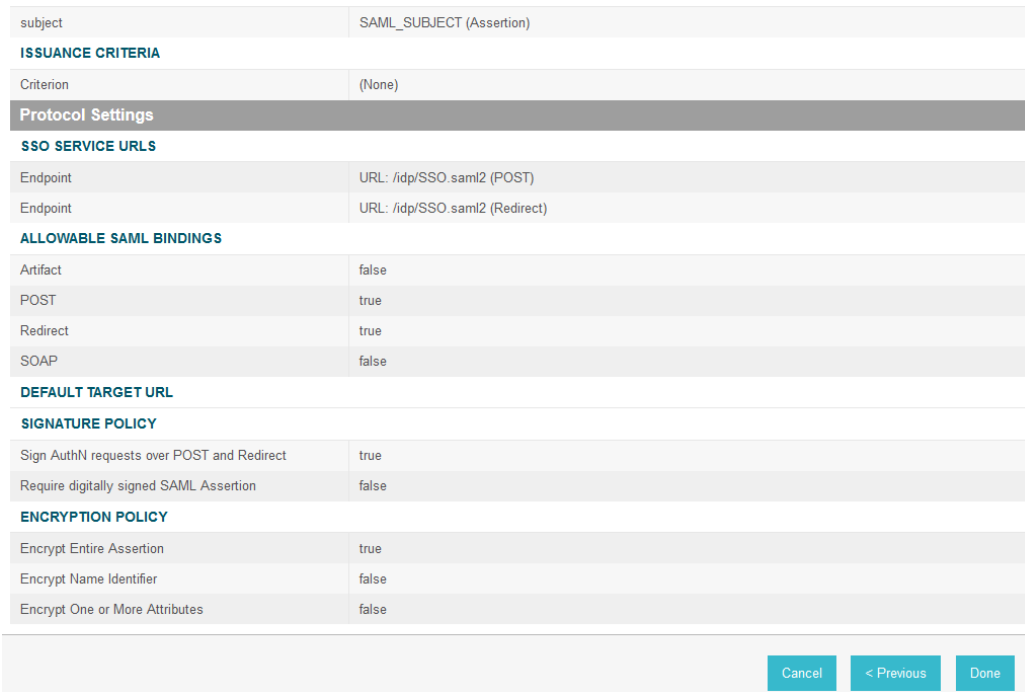
1872 45. On the Summary screen, click **Done**.



1873

1874

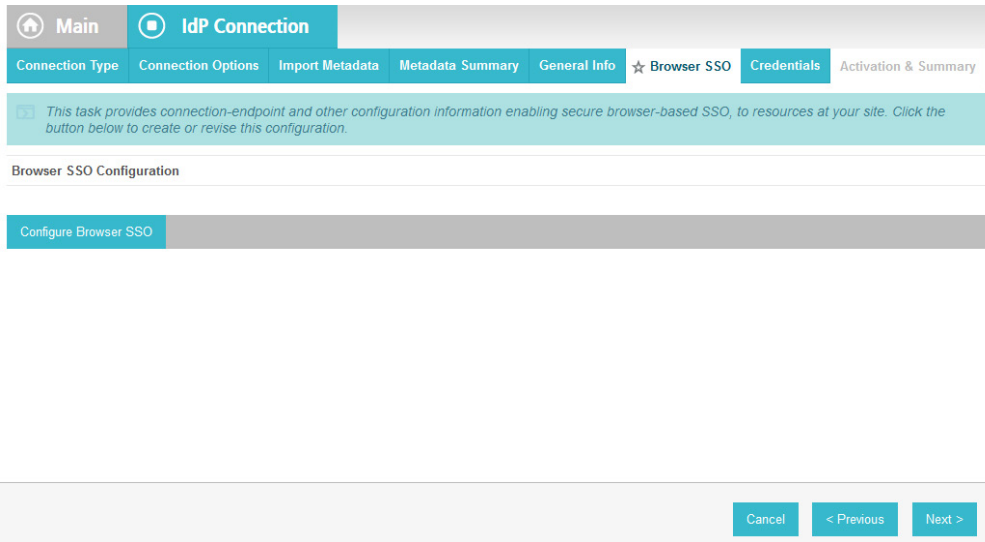
46. On the Protocol Settings screen, click **Next**.



1875

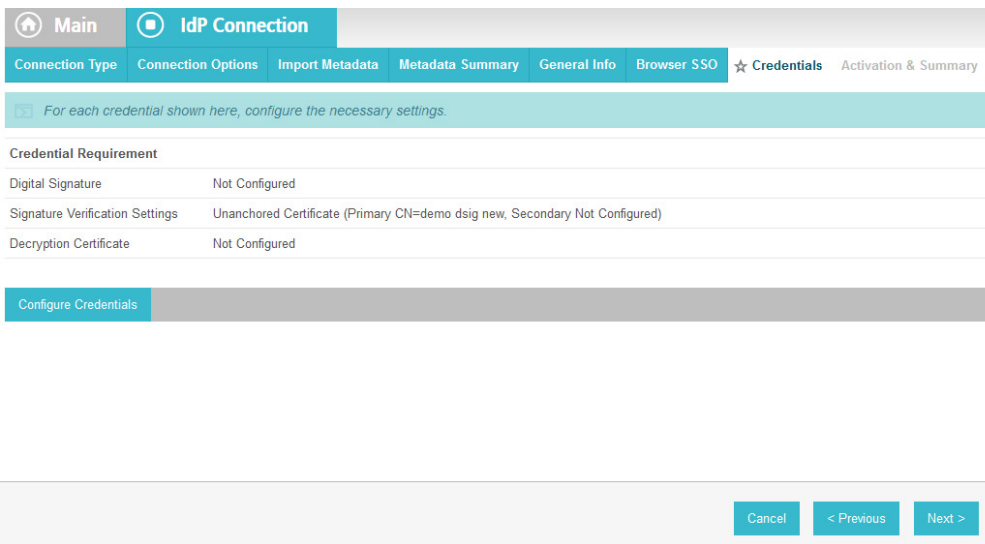
1876

47. On the Summary screen, click **Done**.



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**

The screenshot shows the 'Credentials' configuration screen with the 'Digital Signature Settings' tab selected. The breadcrumb trail is 'Main > IdP Connection > Credentials'. The sub-tabs are 'Digital Signature Settings', 'Signature Verification Settings', 'Select XML Decryption Key', and 'Summary'. A teal message box states: 'You may need to digitally sign SAML messages to protect against tampering. Please select a key/certificate to use from the list below.' The 'Signing Certificate' dropdown is set to '01:30:DB:8C:25:AB (cn=demo dsig new)'. Below it is a checkbox labeled 'Include the certificate in the signature <KeyInfo> element.' The 'Signing Algorithm' dropdown is set to 'RSA SHA256'. A 'Manage Certificates...' button is visible at the bottom left. At the bottom right, there are 'Cancel' and 'Next >' buttons.

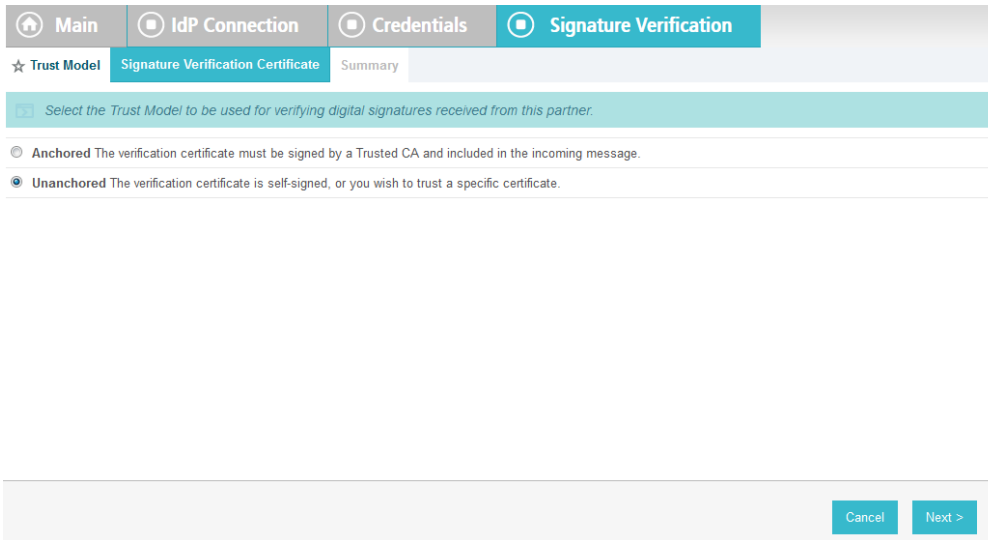
1884

1885 51. Click **Next**.

The screenshot shows the 'Signature Verification Settings' configuration screen. The breadcrumb trail is 'Main > IdP Connection > Credentials'. The sub-tabs are 'Digital Signature Settings', 'Signature Verification Settings', 'Select XML Decryption Key', and 'Summary'. A teal message box states: 'Incoming SAML messages or security tokens may be digitally signed. This configuration task provides options for verifying signatures.' A 'Manage Signature Verification Settings...' button is visible at the bottom left. At the bottom right, there are 'Cancel', '< Previous', and 'Next >' buttons.

1886

1887 52. On the Signature Verification Settings screen, click **Manage Signature Verification Settings**.



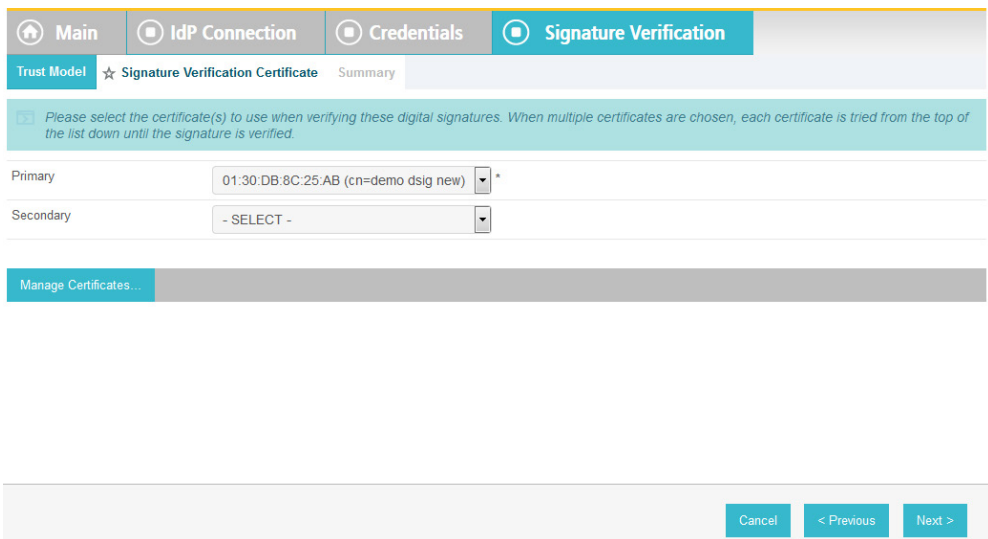
1888

1889

53. On the Trust Model screen, click **Next**.

1890

54. On the Signature Verification Certificate screen, select the certificate to verify digital signatures.

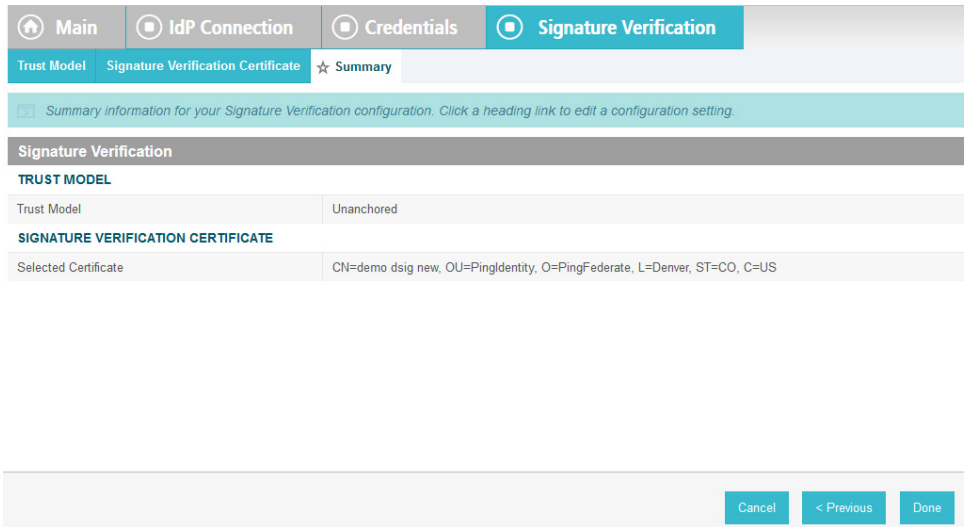


1891

1892

55. Click **Next**.





1893

1894

56. On the Summary screen, click **Done**.

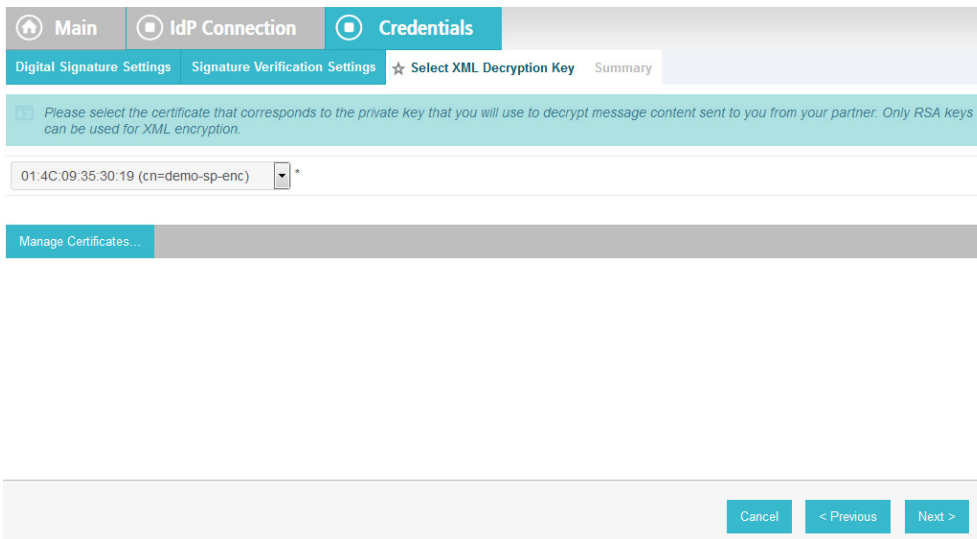
1895

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 that will decrypt messages from the identity provider.

1897



1898

1899

59. Click **Next**.

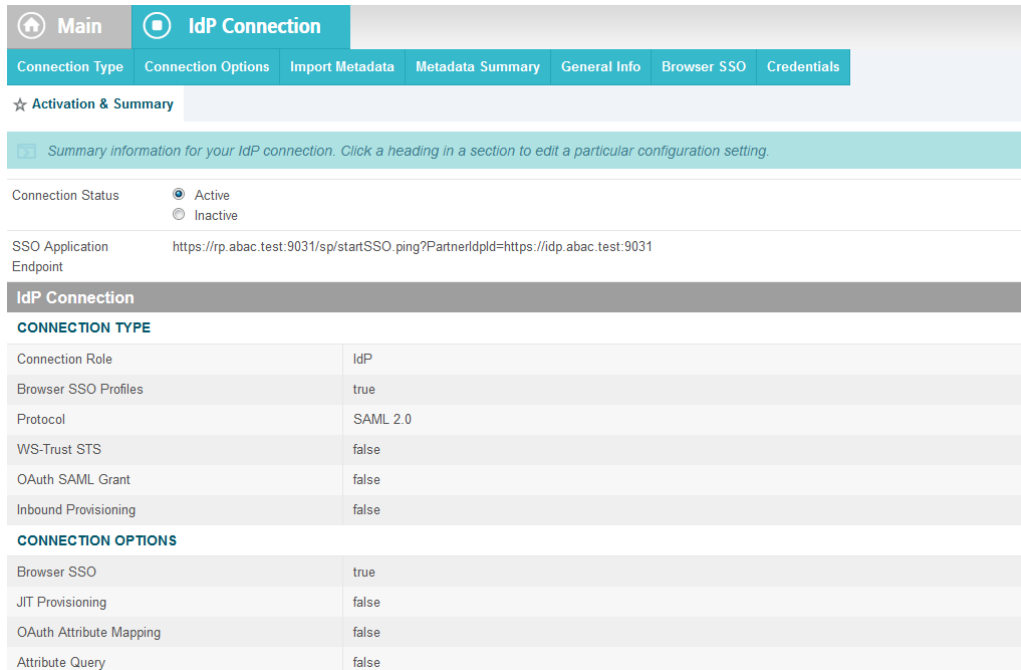
1900

1901 60. On the Summary screen, click **Done**.

1902

1903 61. On the Credentials screen, click **Next**.

1904 62. On the Activation and Summary screen, select **Active** for the **Connection Status** field.



1905

1906

1907

1908

63. Copy the relying party’s SSO Application Endpoint URL (e.g., *https://rp.abac.test:9031/sp/startSSO.ping?PartnerIdpid=https://idp.abac.test:9031*) to the 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

1913

1. Using the browser and PingFederate, a user will logon at the identity provider, and then get redirected to the relying party.

1914

1915

1916

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

1918

1919

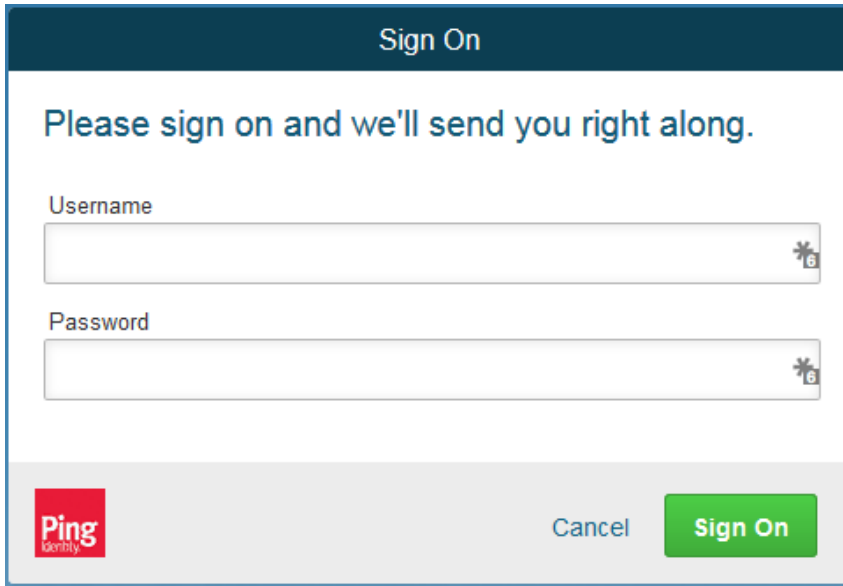
2. Launch your browser and navigate to the relying party’s SSO Application Endpoint URL identified in the previous section (e.g., *https://rp.abac.test:9031/sp/startSSO.ping?PartnerIdpid=https://idp.abac.test:9031*).

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

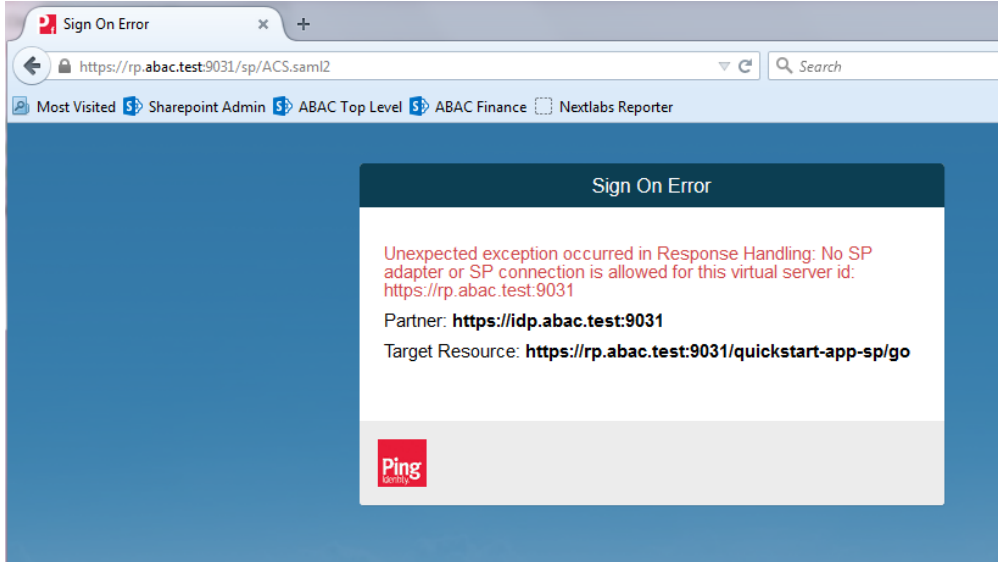
1924

1925

1926

1927

4. Enter the Username and Password of the account created in [Section 2](#) (e.g., “lsmith”) and click Sign On.
  5. When the RSA Adaptive Authentication screen comes up, enter the SMS text validation code.
- Expected Result:** You should see the browser redirect to the relying party’s Federation Server (e.g., rp.abac.test) and an error message similar to the message in the following screenshot.



1928

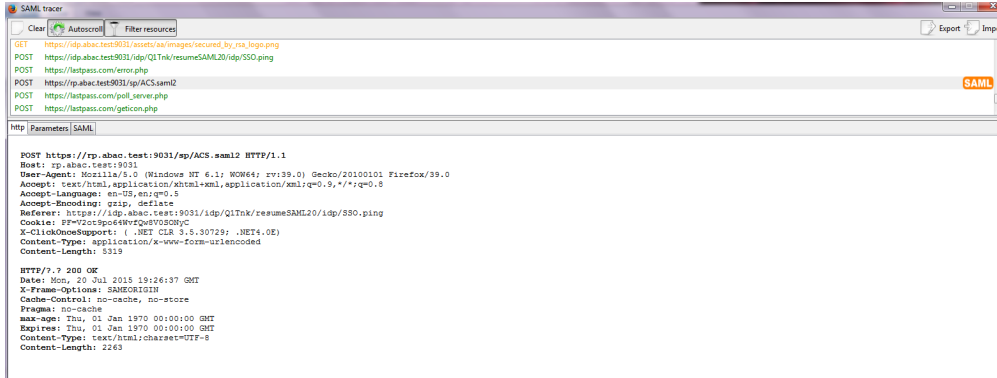
1929

1930

1931

1932

6. Return to the SAML tracer window.
7. Scroll to the bottom of the list of message in the upper pane.
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.



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
<b>Internet Information Services (IIS) 8</b>	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
<b>Microsoft SharePoint Server 2013</b>	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
<b>Microsoft SQL Server 2012</b>	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.

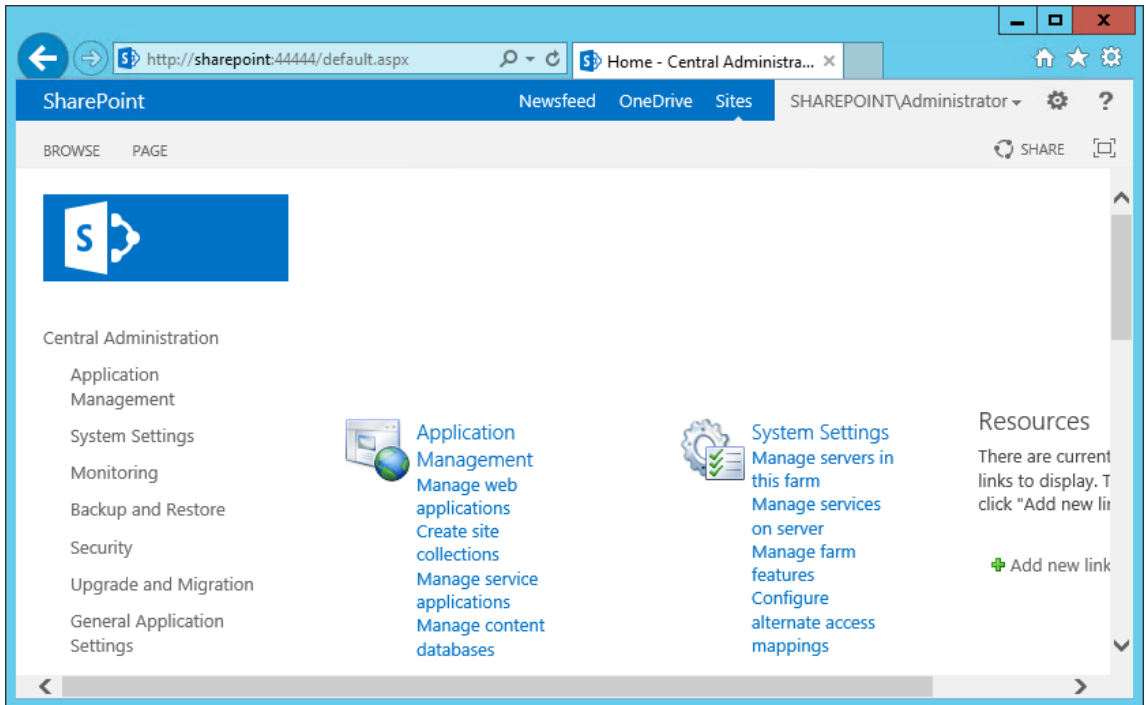
### 1980 4.2.3 Installing Microsoft SharePoint Server 2013

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-](http://social.technet.microsoft.com/wiki/contents/articles/14209.sharepoint-2013-installation-step-by-step.aspx)  
1984 [step.aspx](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**.

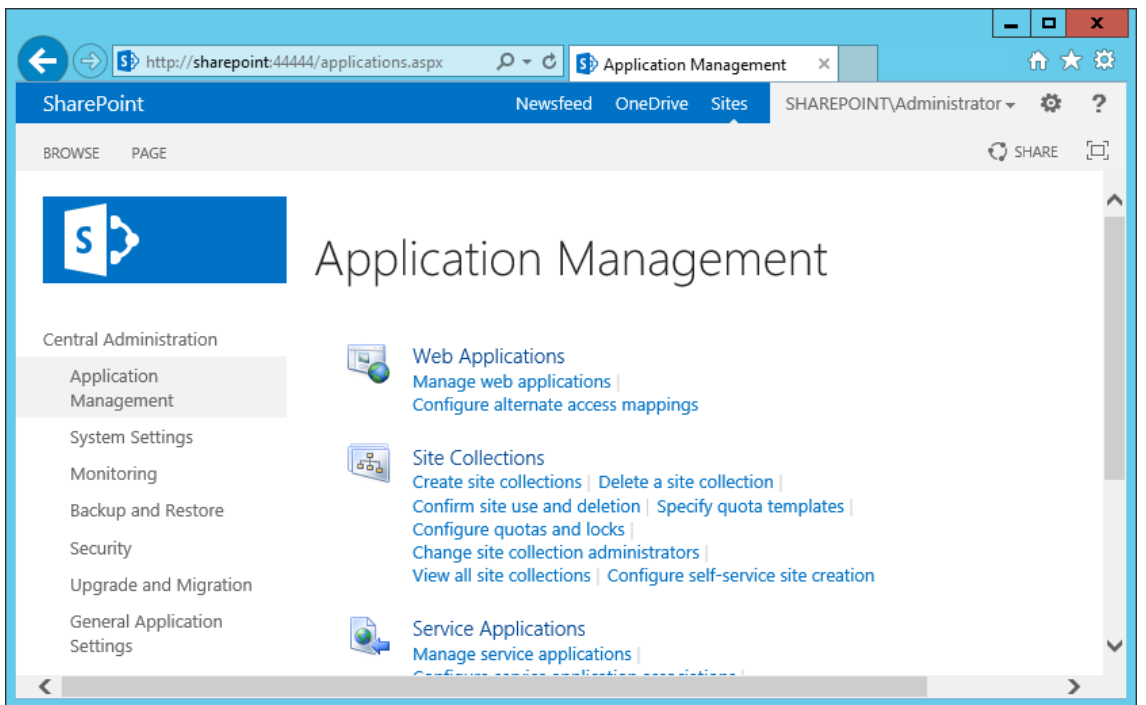


1991

1992

1993

4. On the Application Management Page, under the Web Applications section, click on **Manage web applications**.

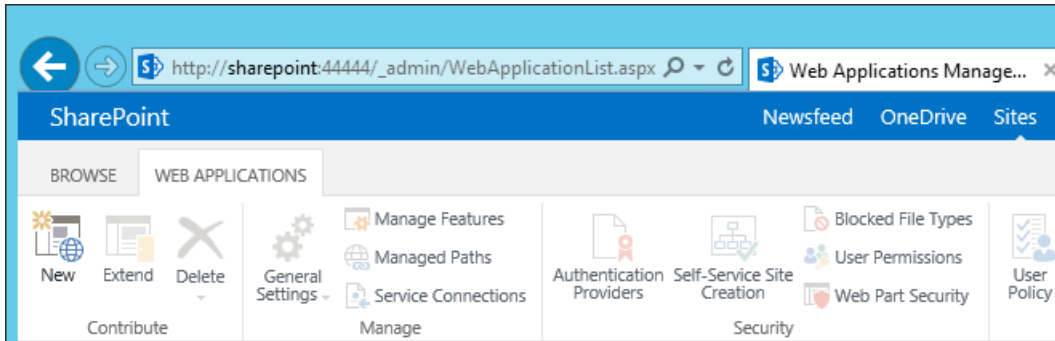


1994

1995

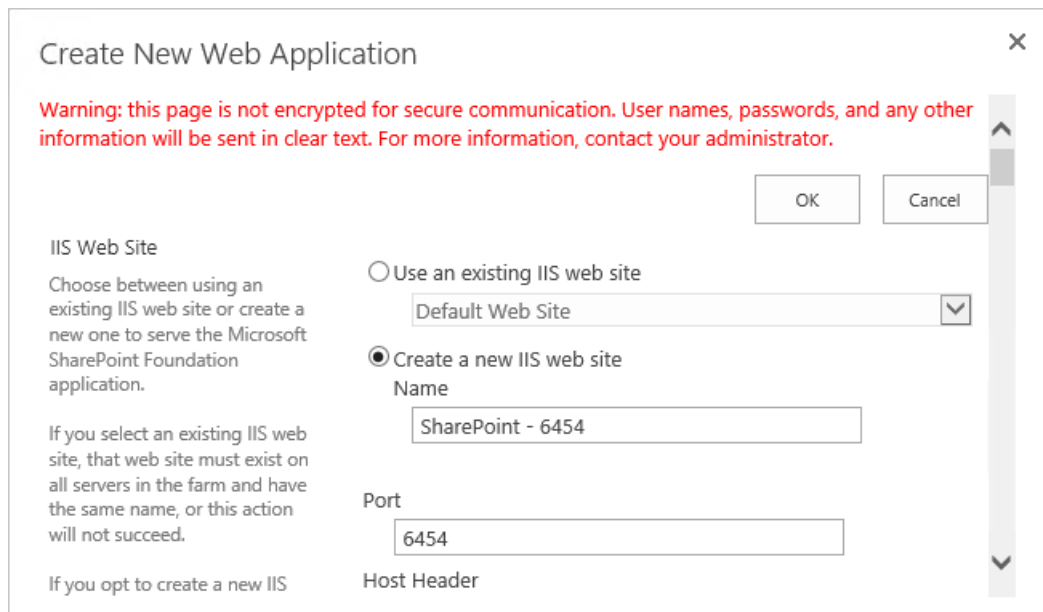
5. From the left-most end of the Web Applications ribbon menu click on **New**.





1996  
1997  
1998  
1999  
2000  
2001  
2002

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:
  - a. Leave the radio button for **Create a new IIS web site** chosen (default).
  - b. Leave the default **Name** or change the **Name** to something more memorable to you.
  - c. Leave the default **Port** displayed or change the **Port** number to one that makes sense for your environment.



2003  
2004

- d. Leave the **Host Header** blank and keep the default **Path**.

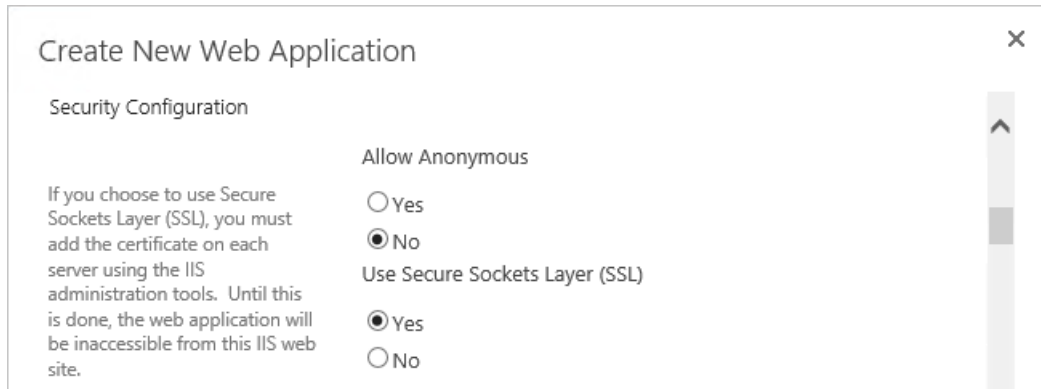
If you opt to create a new IIS web site, it will be automatically created on all servers in the farm. If an IIS setting that you wish to change is not shown here, you can use this option to create the basic site, then update it using the standard IIS tools.

Host Header

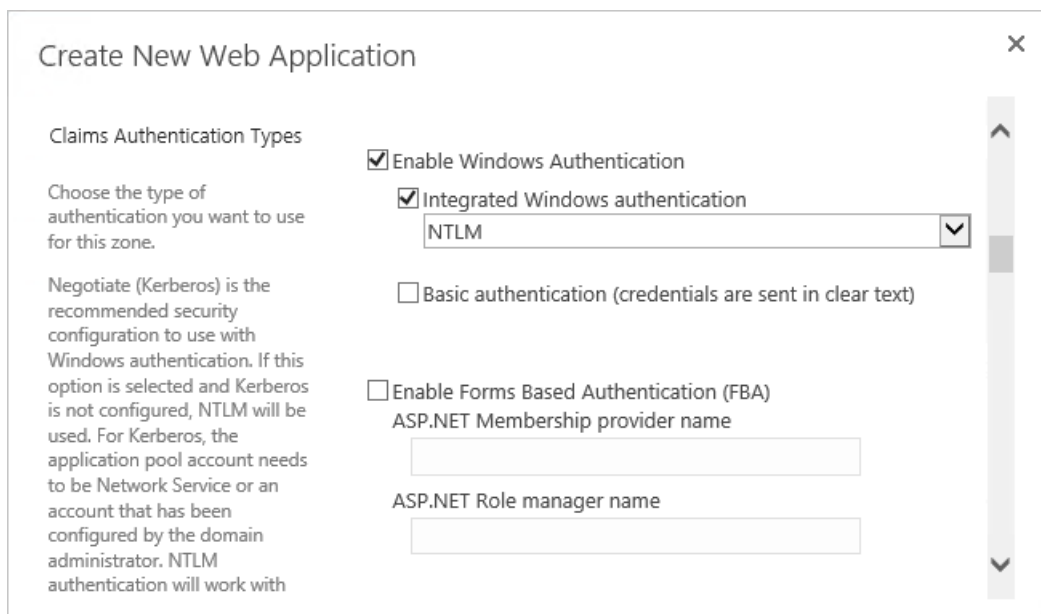
Path

2005

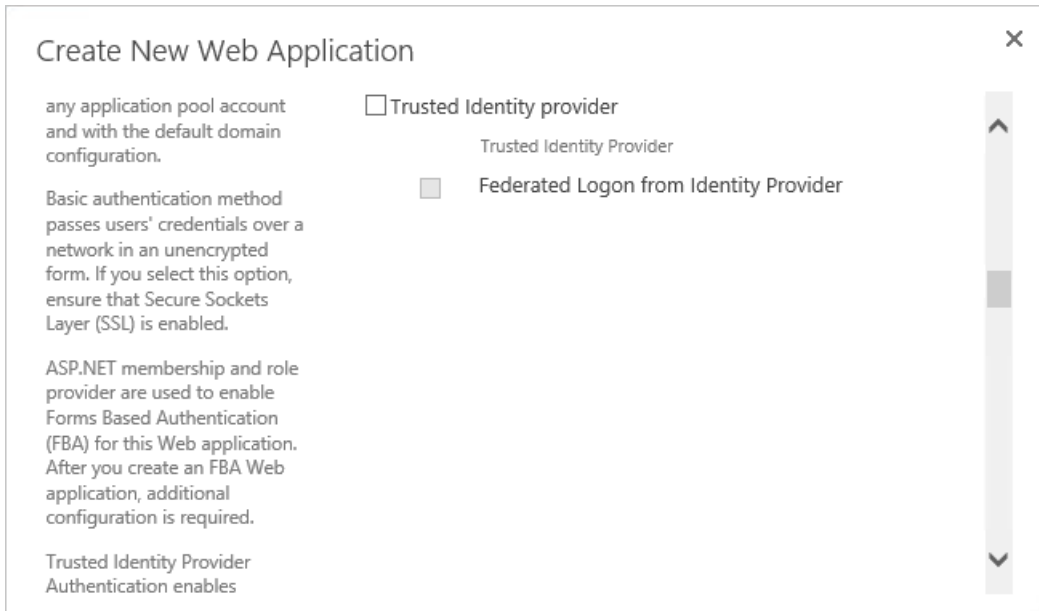
- 2006 7. Further down in the Create New Web Application window, in the Security Configuration section,  
 2007 do the following steps to configure the web application to run SSL:
- 2008 a. Under **Allow Anonymous** leave the **No** radio button chosen (default).
- 2009 b. Under **Use Secure Sockets Layer (SSL)**, click **Yes**.



- 2010
- 2011 8. Further down in the Create New Web Application window, in the Claims Authentication Types  
 2012 section, do the following steps to enable Windows Authentication (as illustrated):
- 2013 a. Click on Enable Windows Authentication
- 2014 b. Click on Integrated Windows authentication



- 2015
- 2016 9. Further down in the Create New Web Application window, in the Claims Authentication Types  
 2017 section, note that there is a **Trusted Identity provider** section. Do not select this option now, but  
 2018 later in our build and in other How-To guide sections there will be steps for setting up the  
 2019 federated logon.

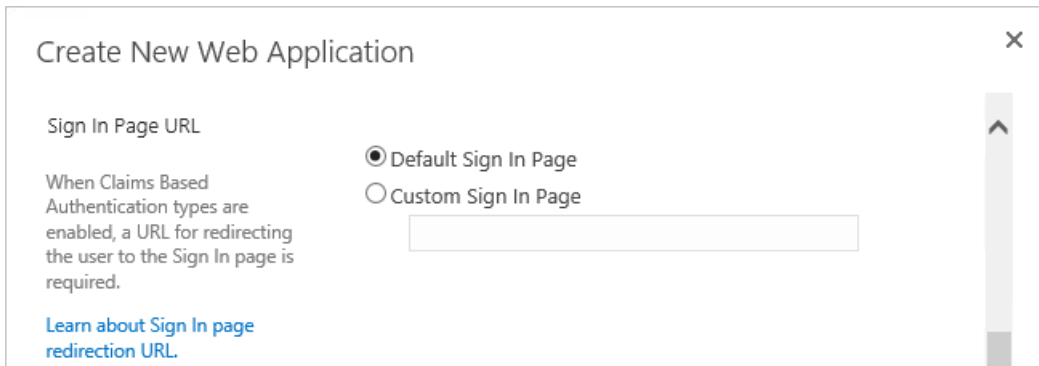


2020

2021

2022

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).

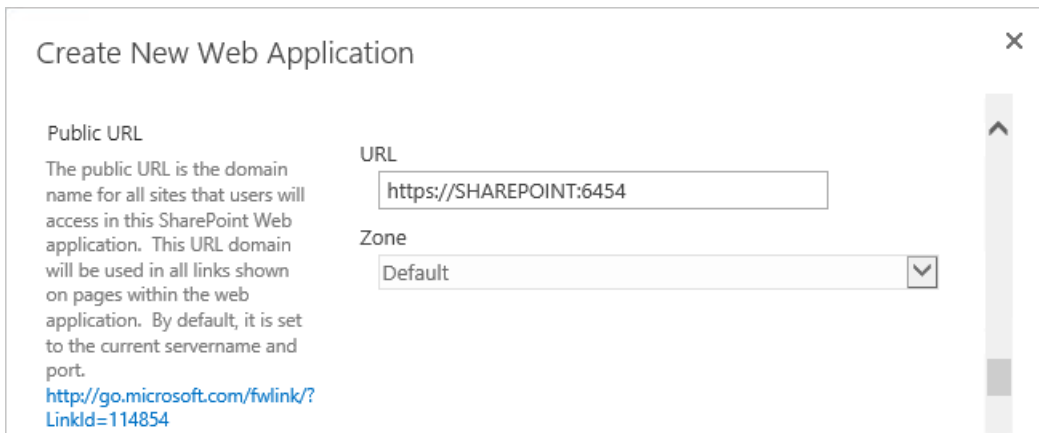


2023

2024

2025

11. Further down in the Create New Web Application window, in the Public URL section, change the **URL** or keep the default **URL**:



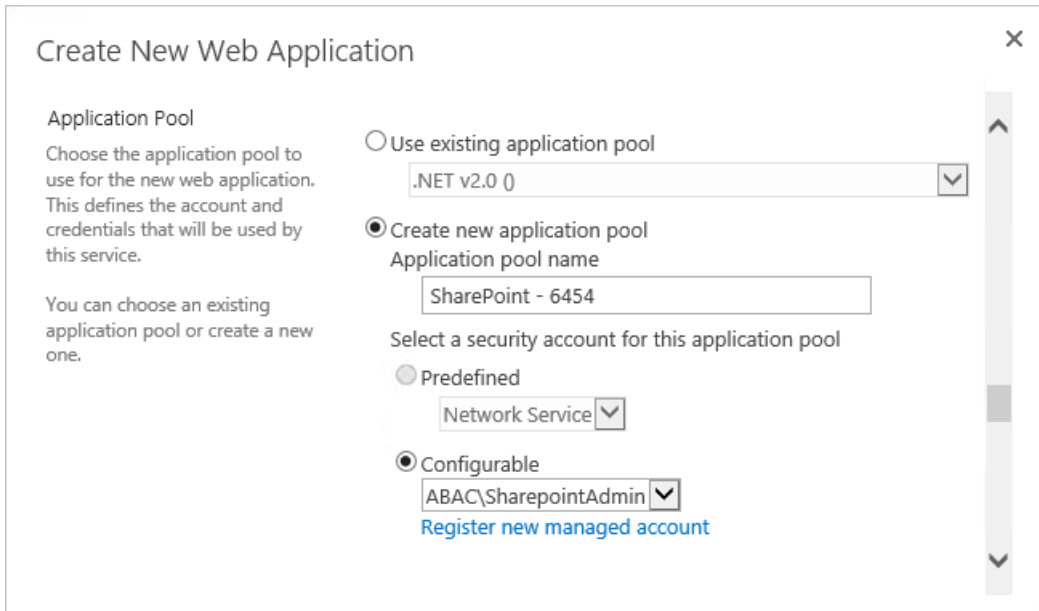
2026

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

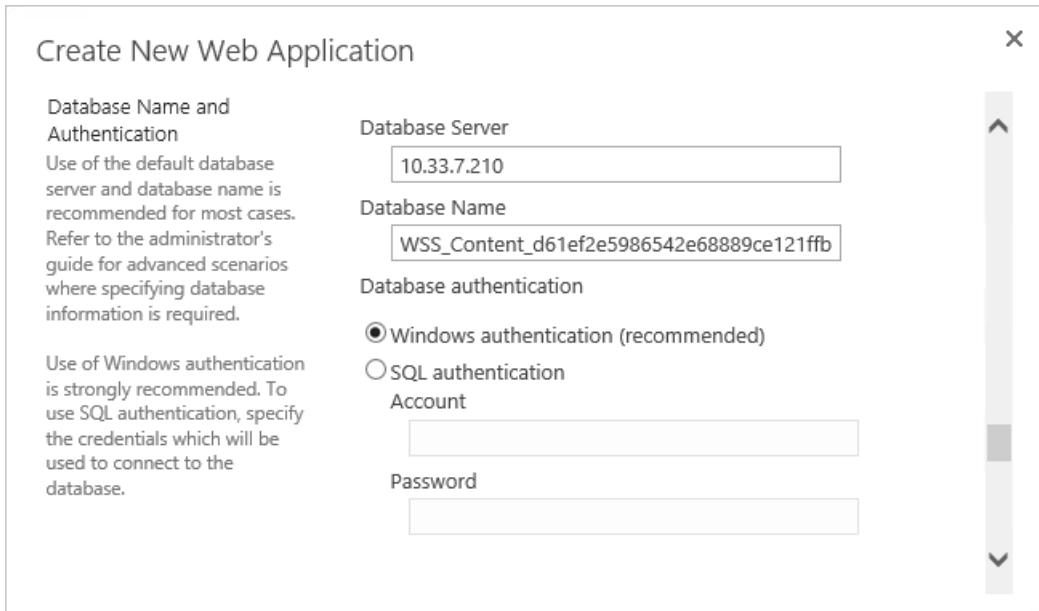
2032 i. If you do not already have a managed account for this purpose, click on the **Reg-**  
 2033 **ister new managed account** link and follow the prompts to create one.



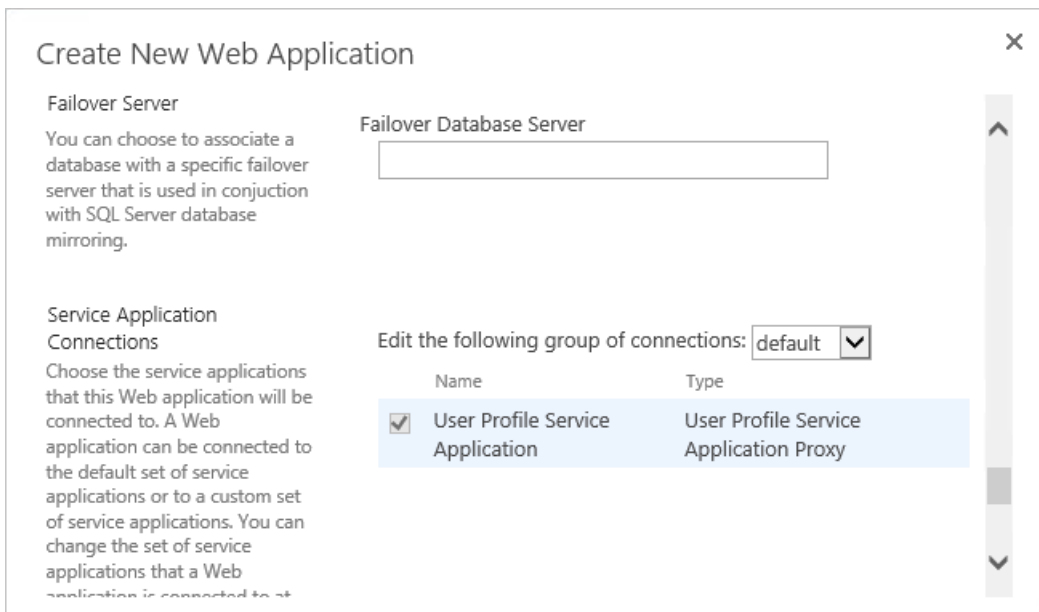
2034 13. Further down in the Create New Web Application window, in the Database Name and  
 2035 Authentication section, leave the following fields filled in with the default information or enter  
 2036 your own manually:  
 2037

2038 a. IP Address of the **Database Server**. In our build the separate, dedicated SQL Server IP  
 2039 address is 10.33.7.210

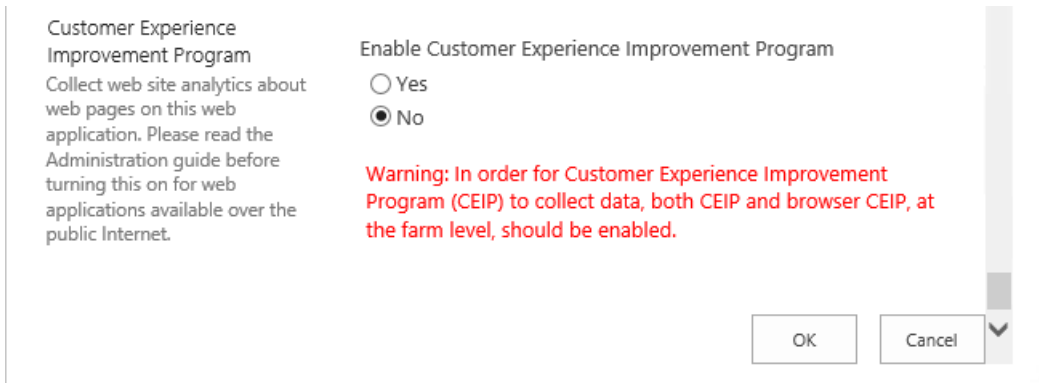
2040 b. **Database name**



- 2041
- 2042 14. Further down in the Create New Web Application window, in the Failover Server section, leave
- 2043 the **Failover Database Server** field blank.
- 2044 15. Further down in the Create New Web Application window, in Service Application Connections,
- 2045 leave the default checkbox for **User Profile Service Application** checked.

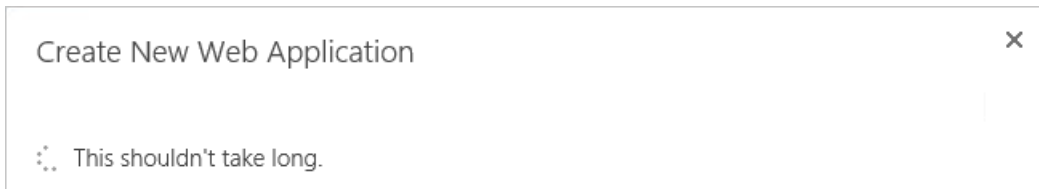


- 2046
- 2047 16. Further down in the Create New Application window, in Customer Experience Improvement
- 2048 Program, either keep the **Enable Customer Experience Improvement Program** radio button for
- 2049 **No** chosen, or click on **Yes**.
- 2050 17. At the bottom of the Create New Application window click **OK** to finish the web application
- 2051 creation process.



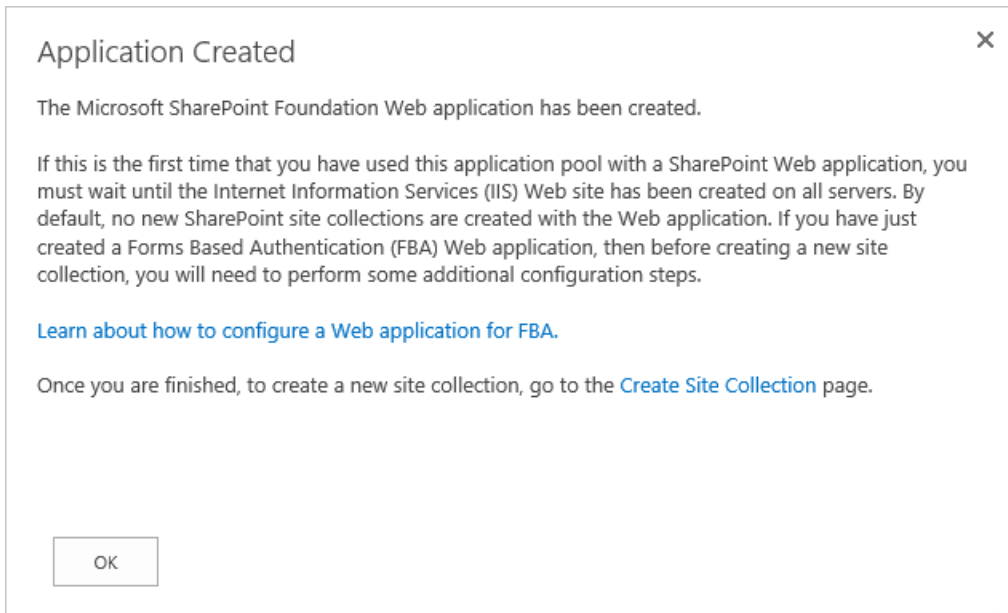
2052

2053 18. Wait for the new web application to be created.



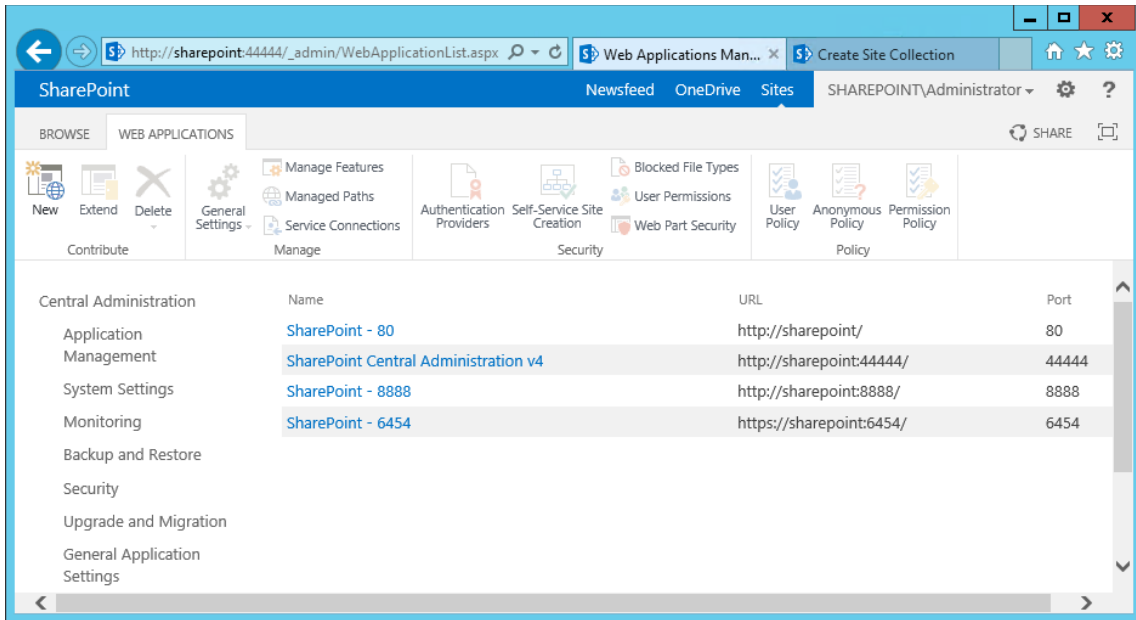
2054

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).



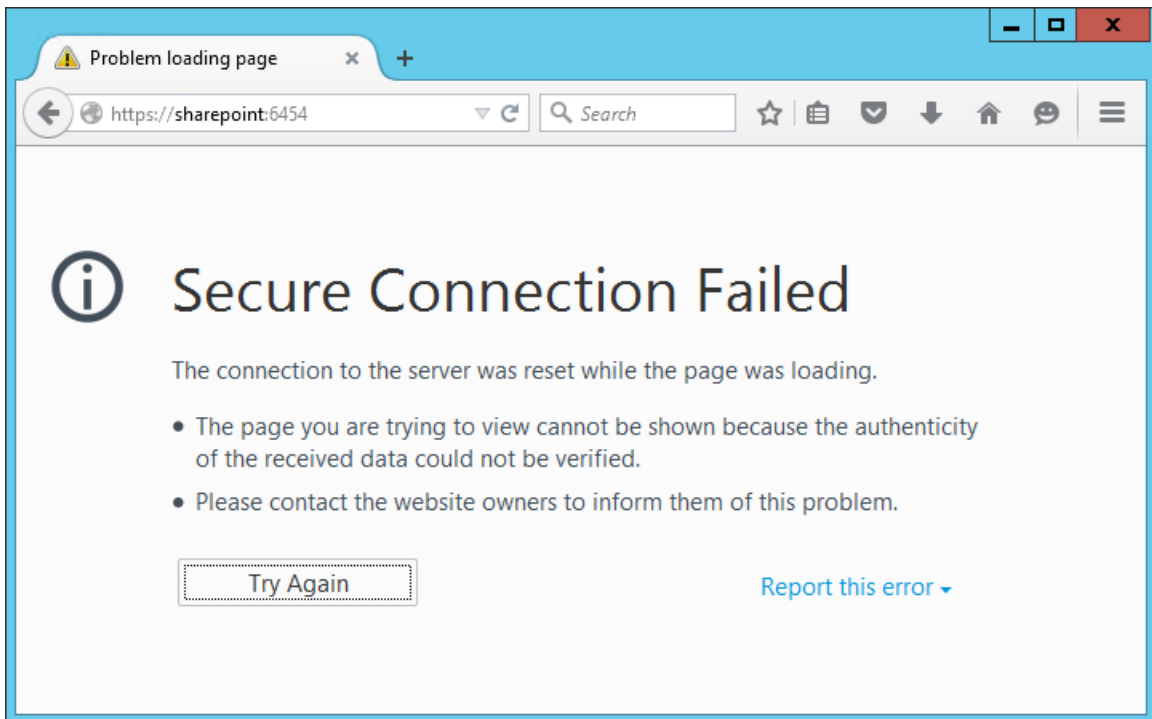
2059

2060

2061

2062

- In another browser window, navigate to your new web application (e.g., <https://sharepoint:6454>). Until the SSL certificate is installed as seen in the following section, you will receive this error.



2063

#### 2064 4.4 Creating and Installing SSL Certificate

2065

2066

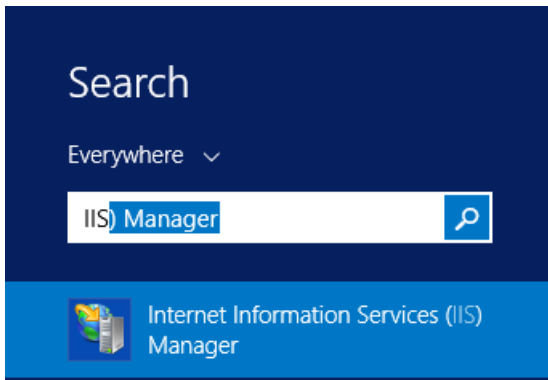
2067

For a protected lab environment, it is possible to use self-signed certificates, however for production network deployments it is generally recommended to use certificates signed by a Certificate Authority. Instructions related to both approaches are included in this section.

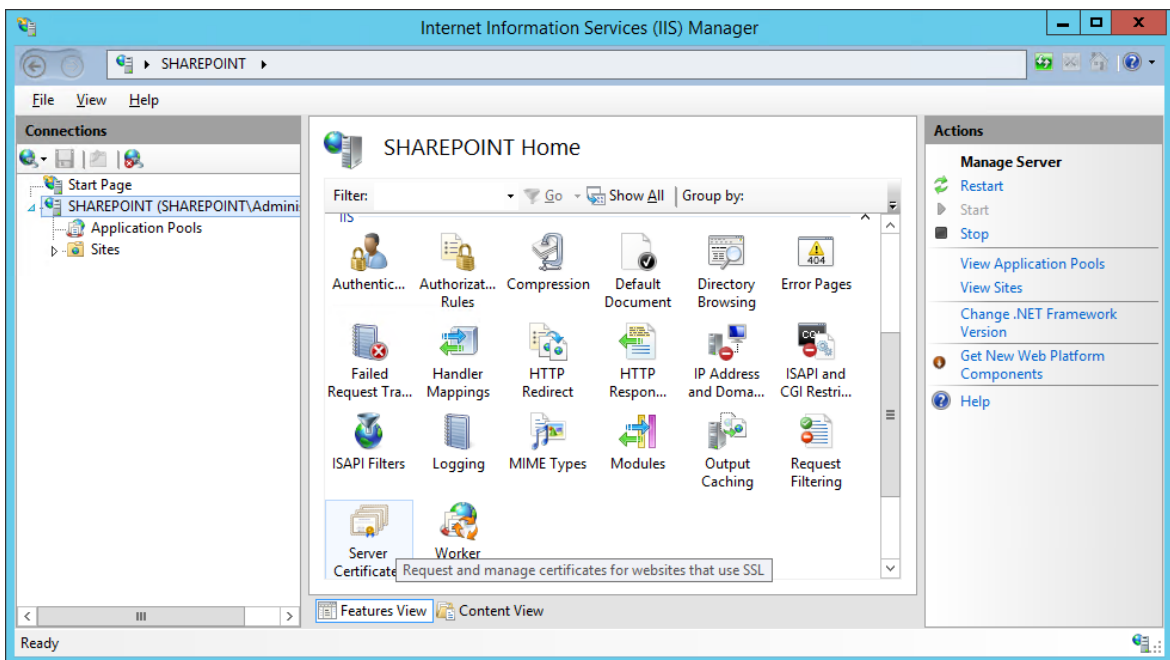
2068 **4.4.1 Self-Signed Certificates**

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.

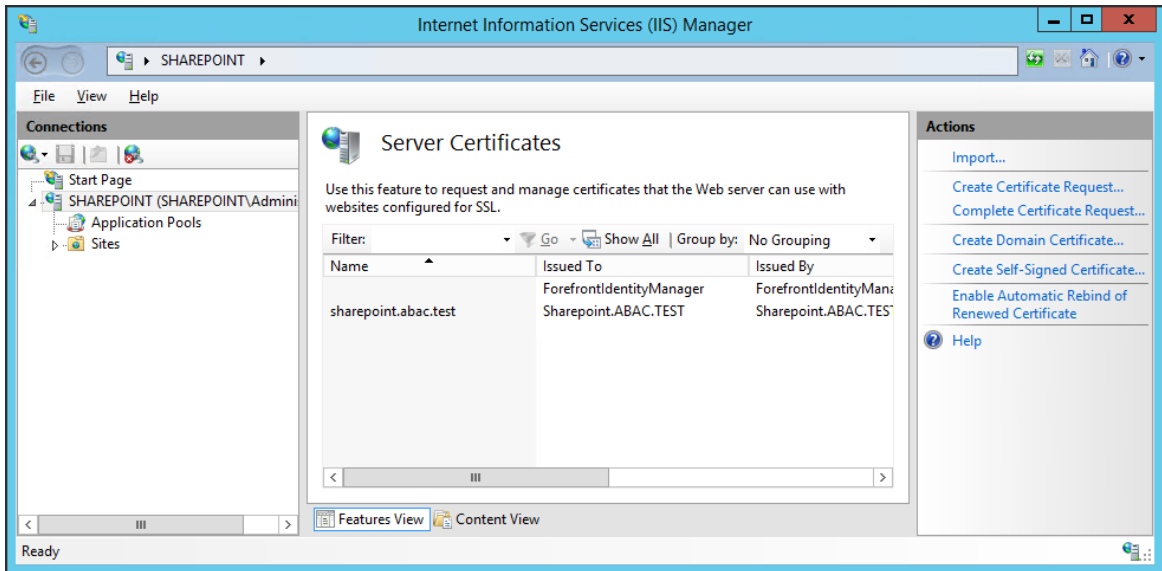


- 2073
- 2074 4. Click on the **SharePoint Instance** to see its Features.
- 2075 5. Scroll down and double-click on **Server Certificates**.



- 2076
- 2077 6. In the Server Certificates window, you will see any certificates that already exist.



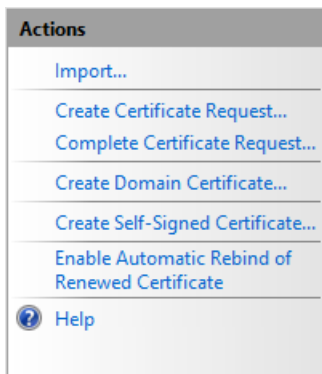


2078

2079

2080

- 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**.

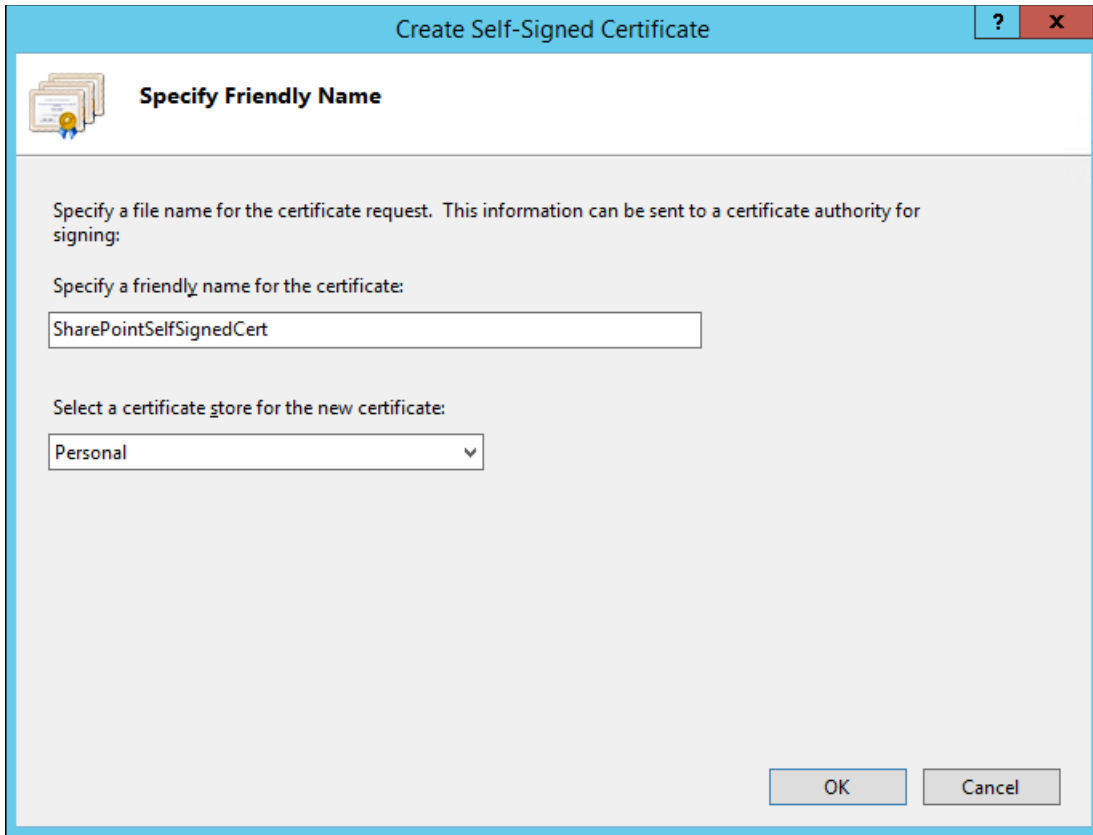


2081

2082

2083

- In the Create Self-Signed Certificate window, **Specify a friendly name for the certificate** and **Select a certificate store for the new certificate**, then click **OK**.

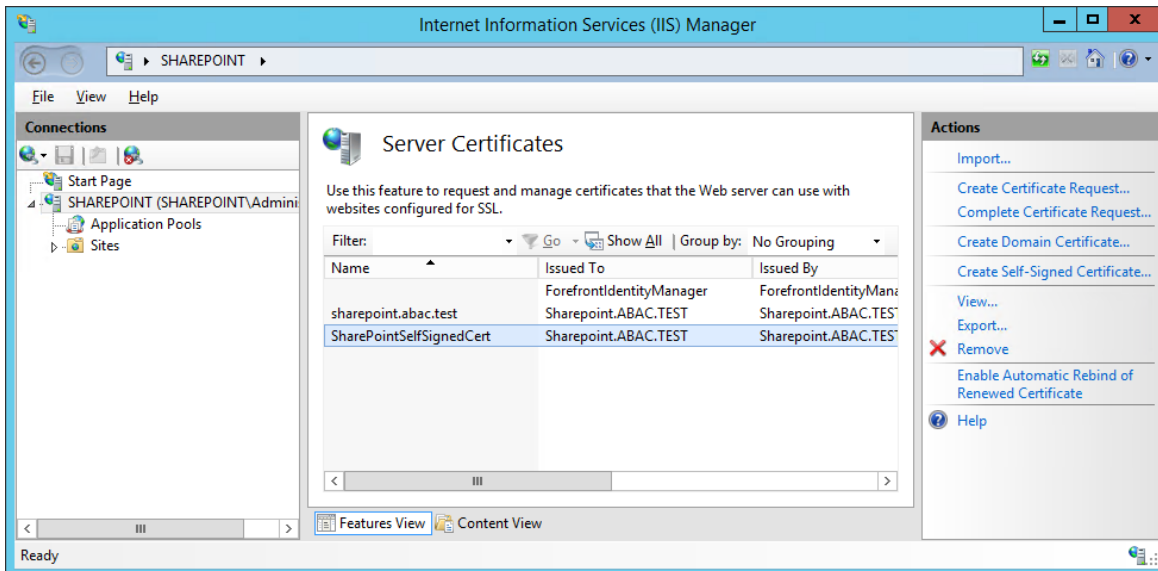


2084

2085 *4.4.1.2 Importing Self-Signed Certificate to SharePoint Certificate Store*

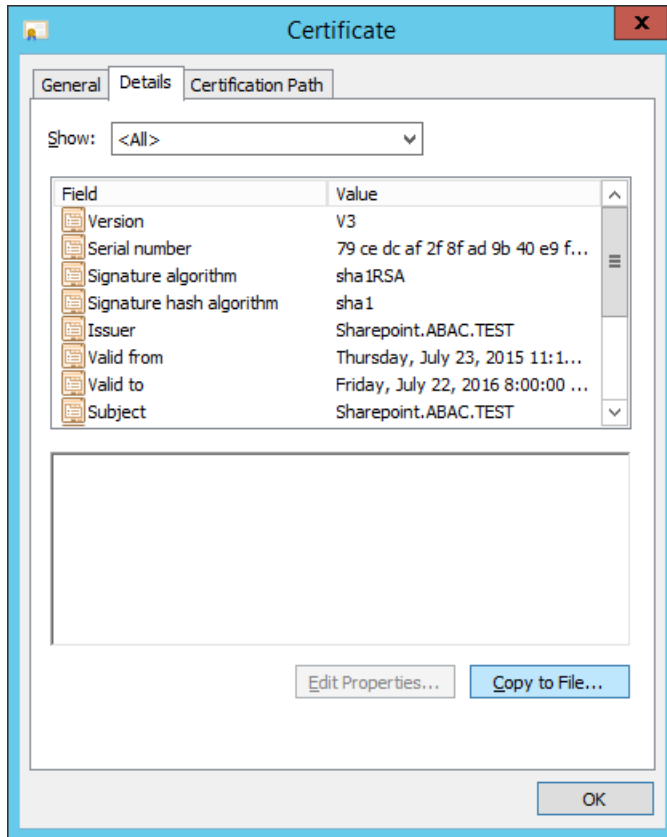
2086 1. After creating the self-signed certificate and clicking **OK** in the previous sub-section, you will see  
 2087 your new certificate.

2088 2. Double-click on the new certificate.



2089

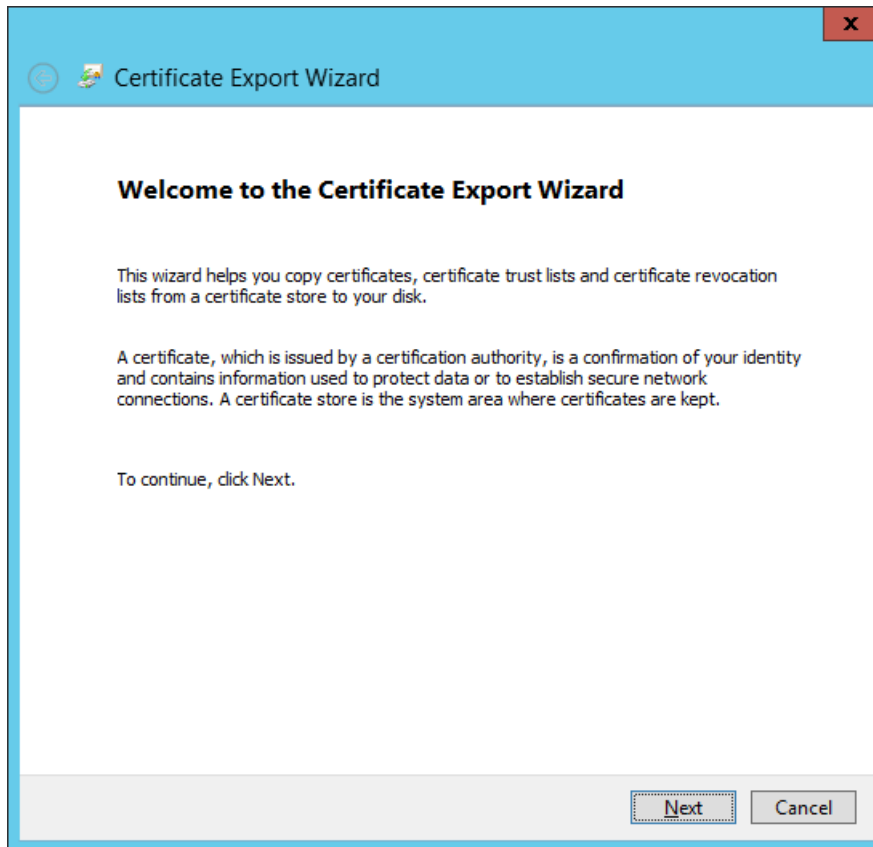
2090 3. In the **Details** tab of the Certificate window, click on **Copy to File**.



2091

2092

4. In the Certificate Export Wizard window that opens, click **Next**.

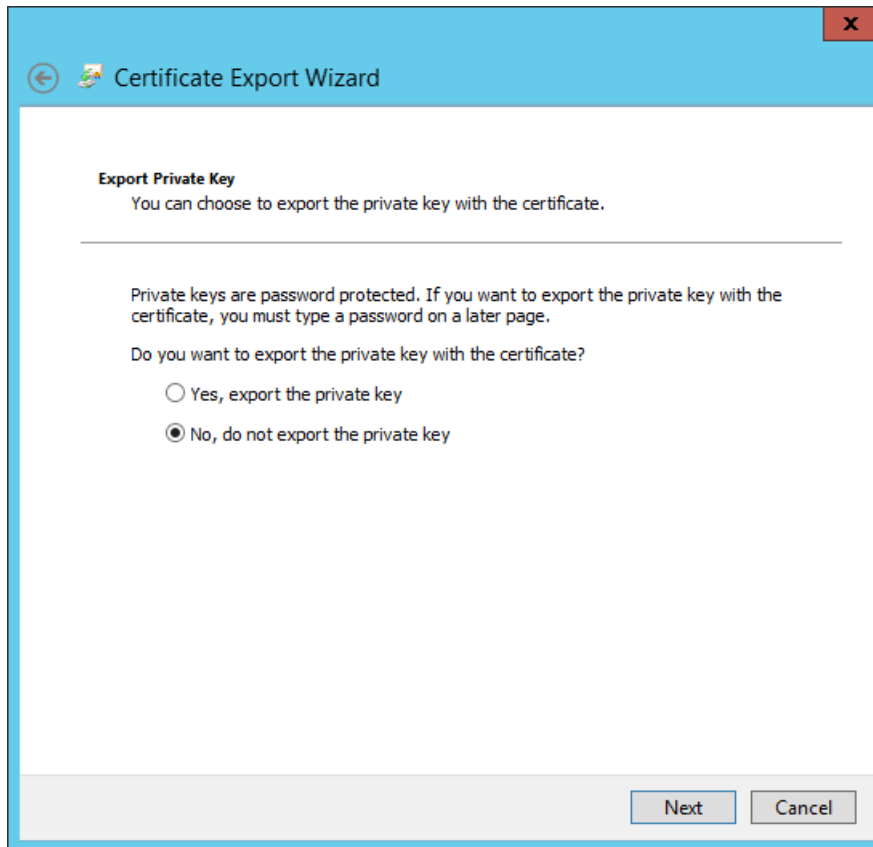


2093

2094

2095

5. In the Certificate Export Wizard window on the Export Private Key screen, keep the selection **No, do not export the private key** and click **Next**.

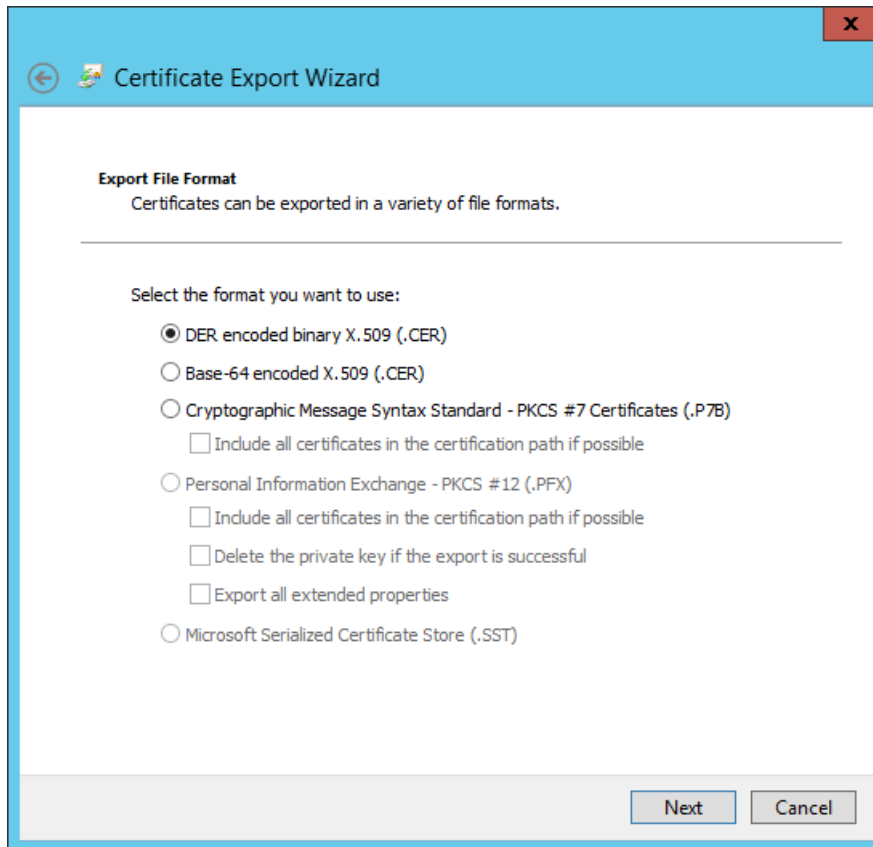


2096

2097

2098

6. In the Certificate Export Wizard window on the Export File Format screen, select the format you want to use (**DER** in this example), then click **Next**.

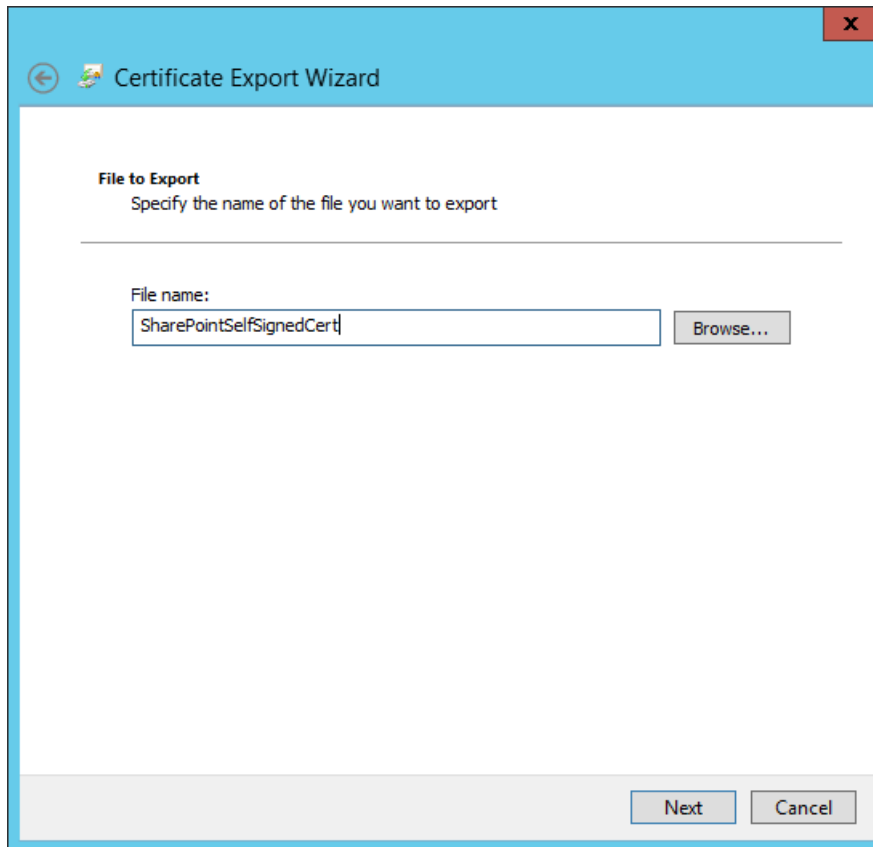


2099

2100

2101

7. In the Certificate Export Wizard window on the File to Export screen, type in the certificate file name and click **Next**.

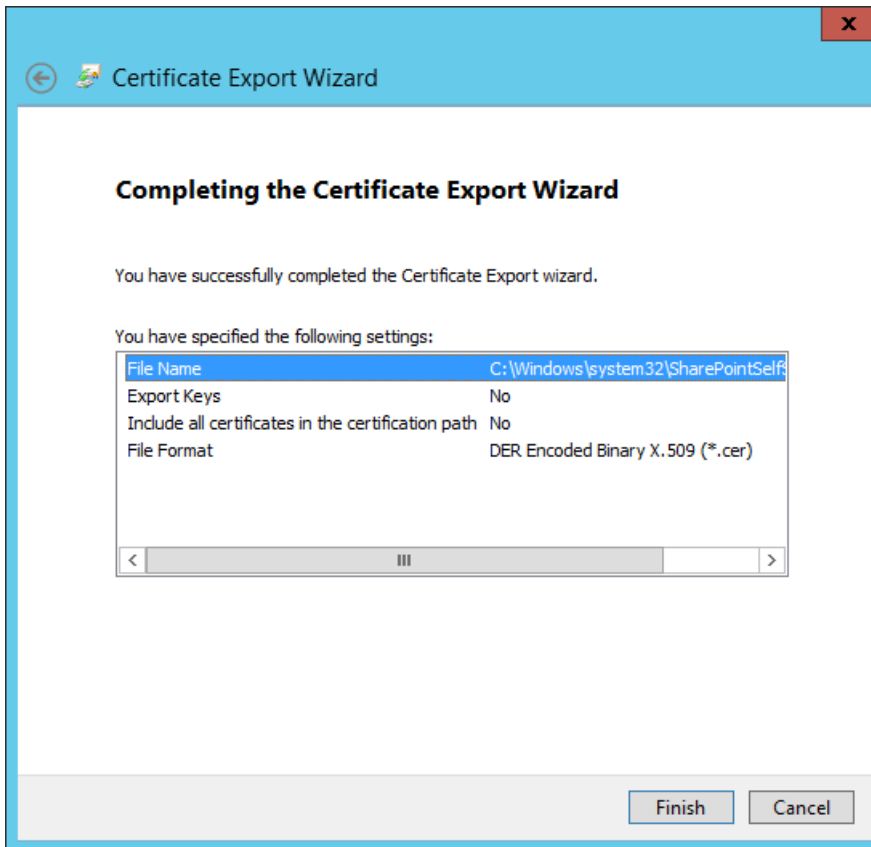


2102

2103

2104

8. In the Certificate Export Window on the Completing the Certificate Export Wizard screen, click **Finish**.

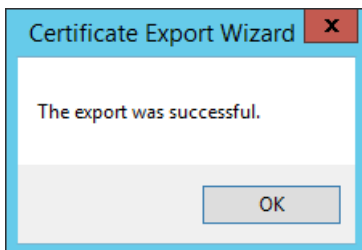


2105

2106

2107

- In another Certificate Export Wizard window that automatically opens, you will see that the export was successful. Click **OK**.



2108

2109

#### 4.4.1.3 Add the Self Signed Certificate to Trust management in Central Administration

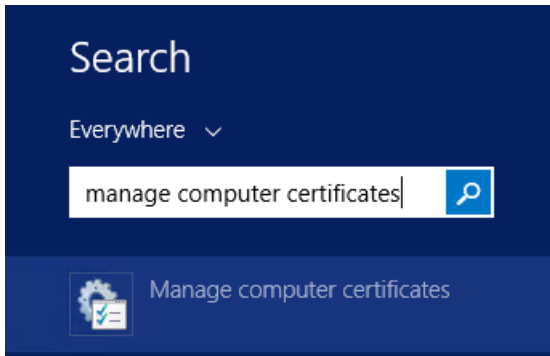
2110

2111

2112

- Click on the Windows icon at the bottom left corner of your screen.
- Begin typing the words: manage computer certificates.
- Click on the Manage Computer Certificates icon.



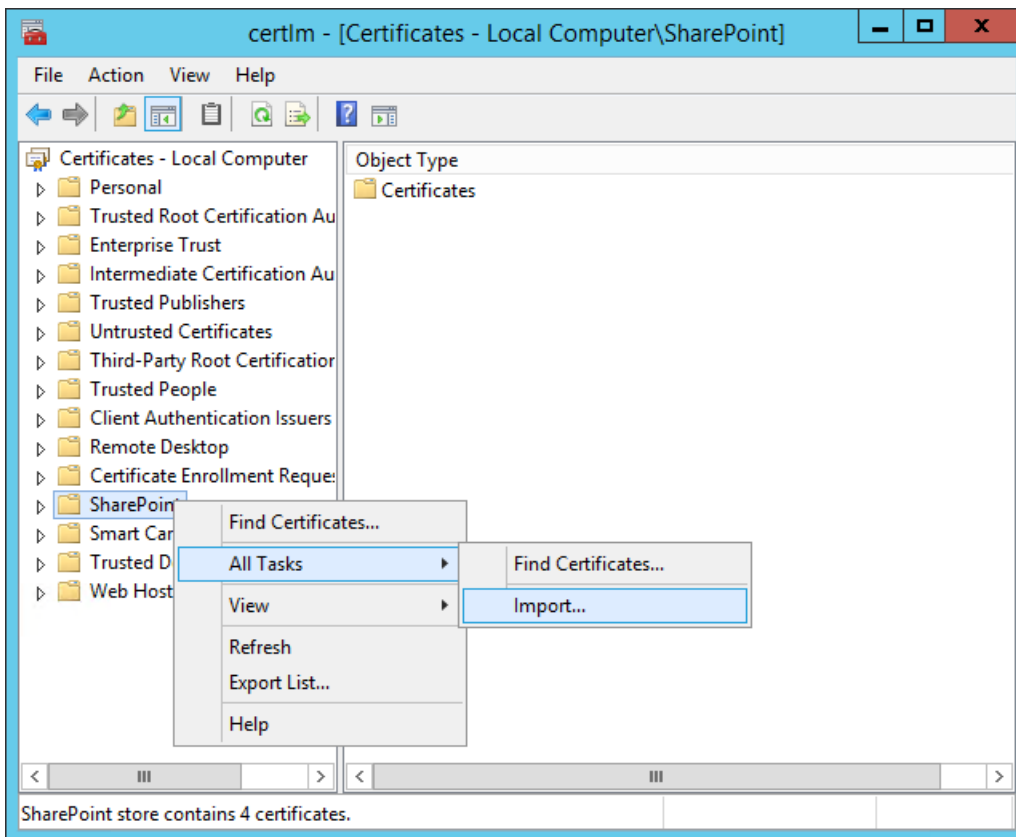


2113

2114

2115

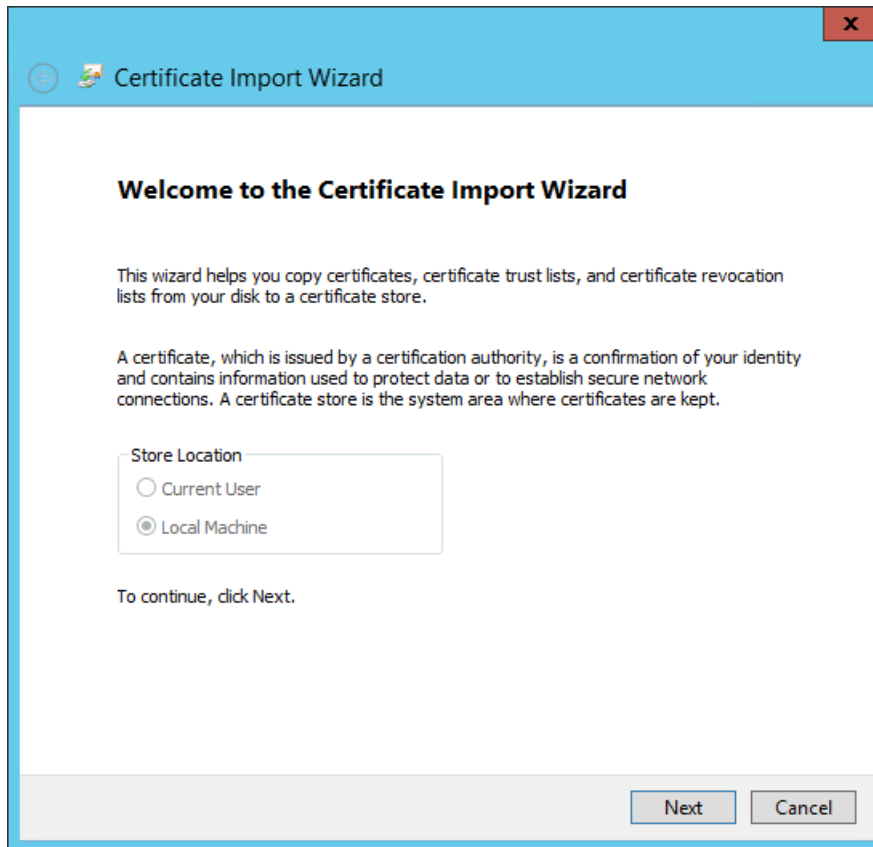
4. In the certlm window, right-click on the **SharePoint** node, hover over **All Tasks**, then click **Import**.



2116

2117

5. In the Certificate Import Wizard window that opens, click **Next**.

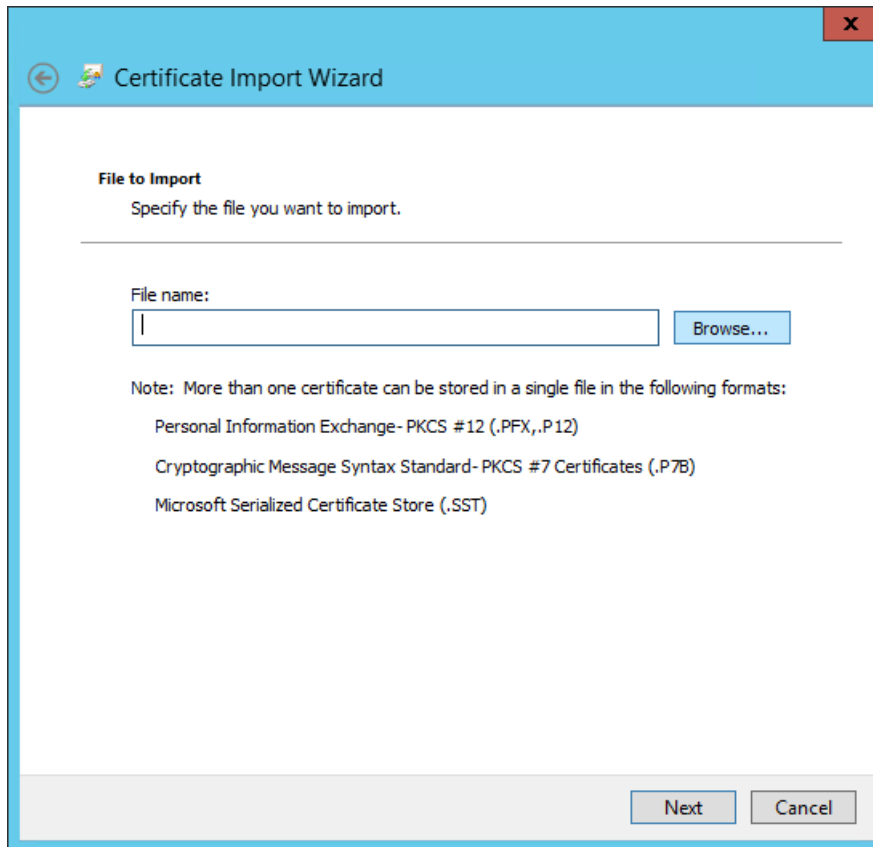


2118

2119

2120

6. In the Certificate Import Wizard window, on the File to Import screen, click **Browse** to find the self-signed certificate we created in the previous sub-section.



2121

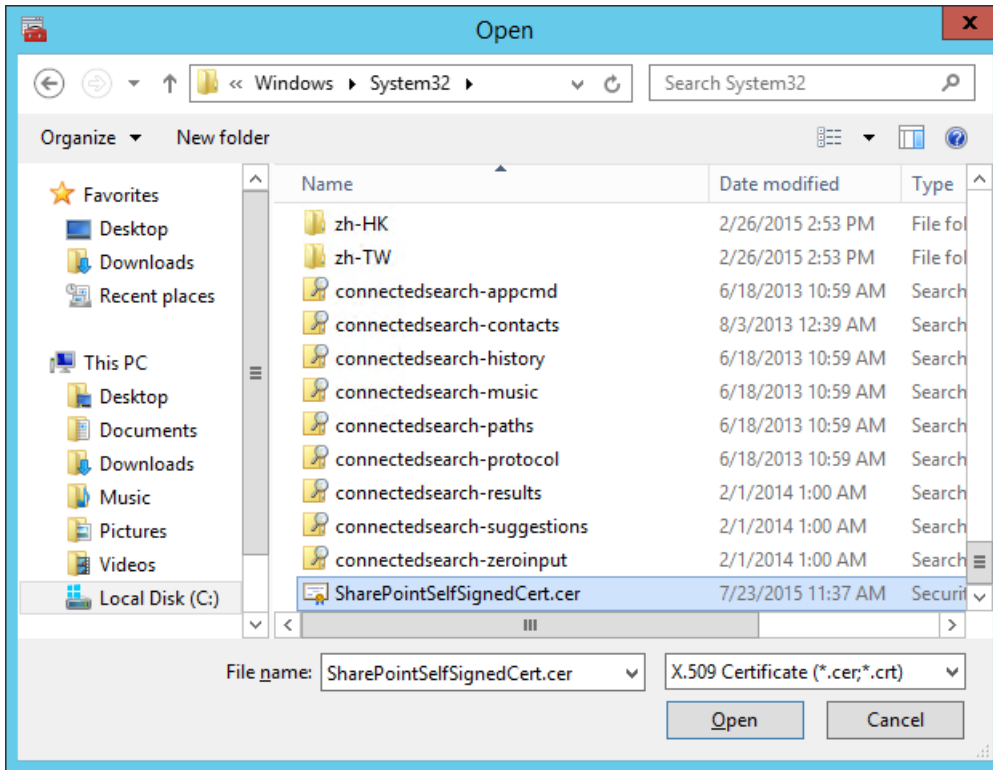
2122

2123

2124

2125

7. In the File Explorer window that opens automatically, click through location folders to find the self-signed certificate we created in the previous sub-section (example from this build: *C:/Windows/System32/*).
8. Find the certificate and click to select it; then click **Open**.

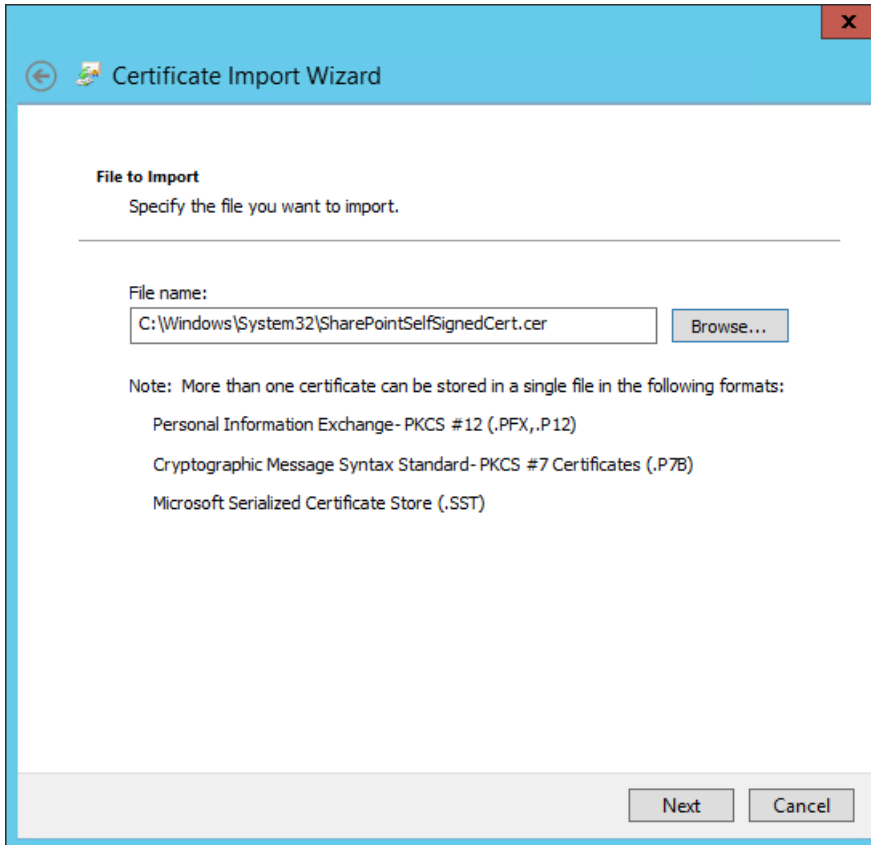


2126

2127

2128

- Back at the Certificate Import Wizard, on the File to Import screen, the location of the self-signed certificate will be in the **File name** field. Click **Next**.



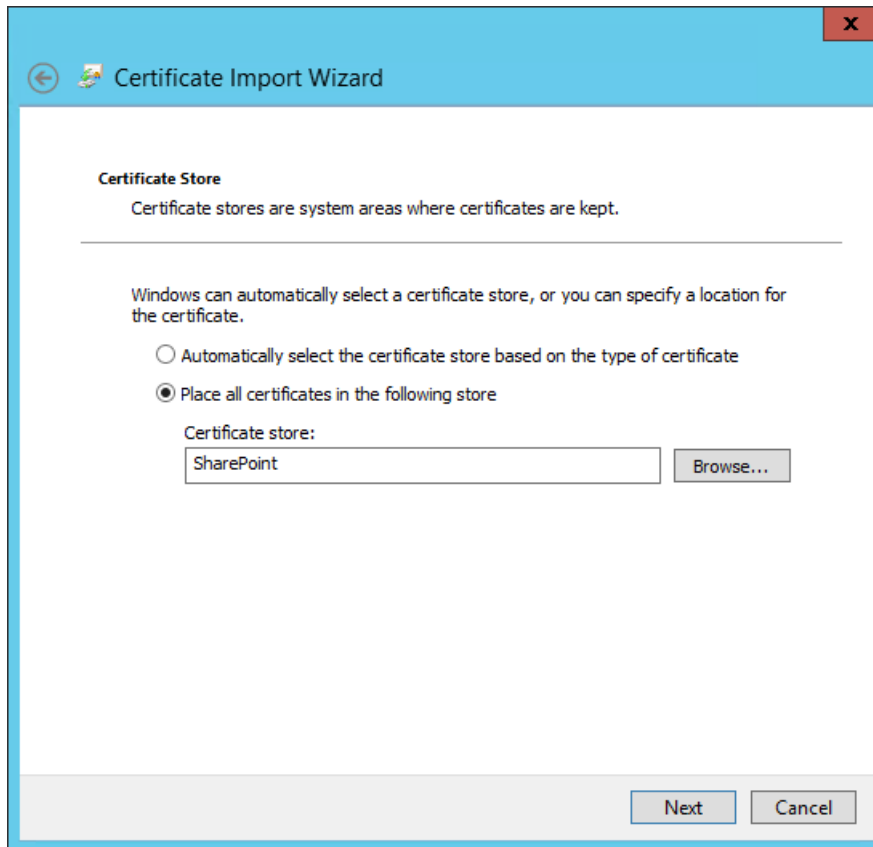
2129

2130

2131

2132

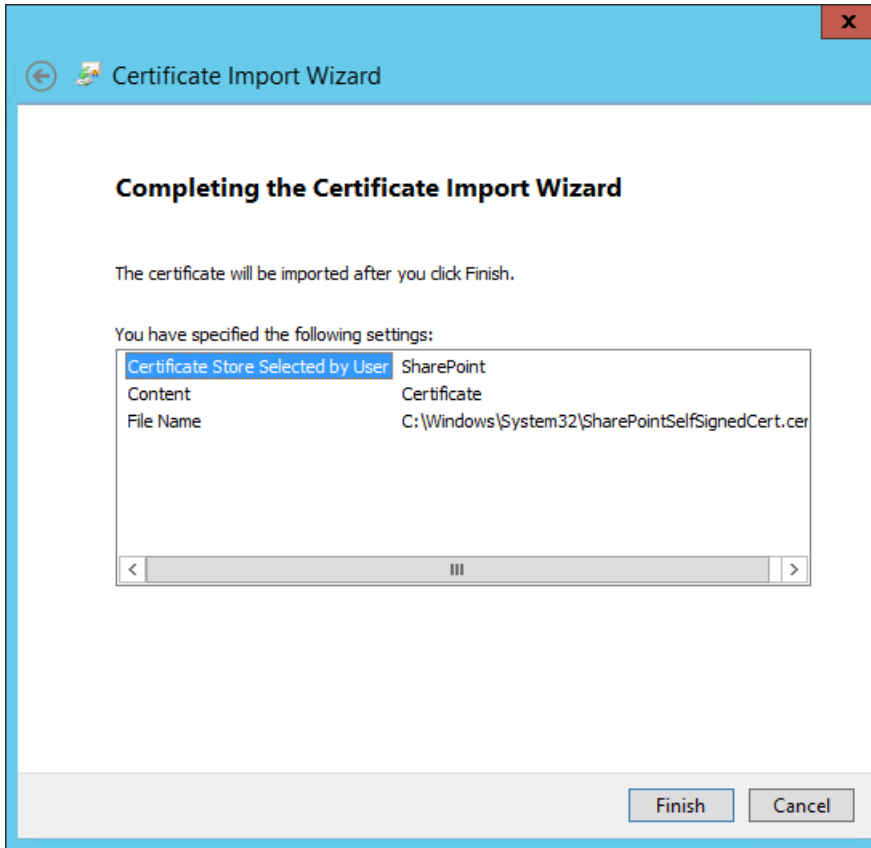
10. In the Certificate Import Wizard window on the Certificate Store screen, leave the default radio button for **Place all certificates in the following store** chosen. The **Certificate store** field should be set to SharePoint. Click **Next**.



2133

2134

11. In the Certificate Import Wizard window, click **Finish**.

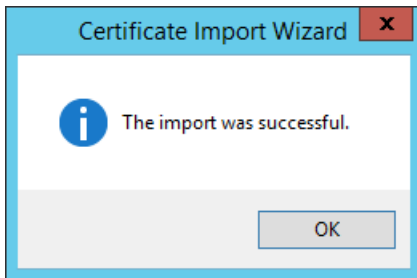


2135

2136

2137

12. In the Certificate Import Wizard window that automatically opens, you will see a message that the import was successful. Click **OK**.

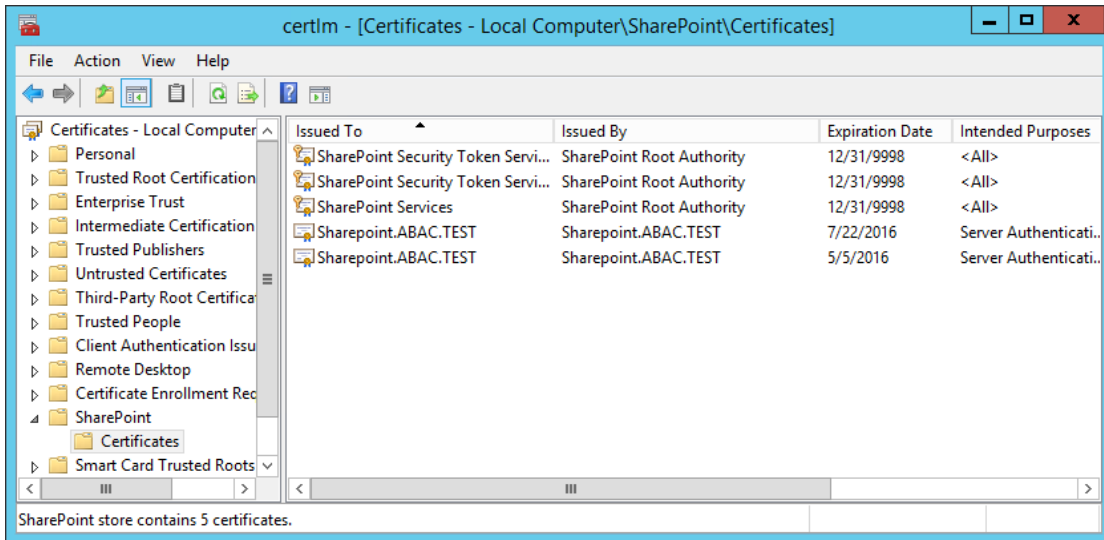


2138

2139

2140

13. In the certlm window, double-click on **Certificates** under the SharePoint node. The new self-signed certificate you created will be listed there.

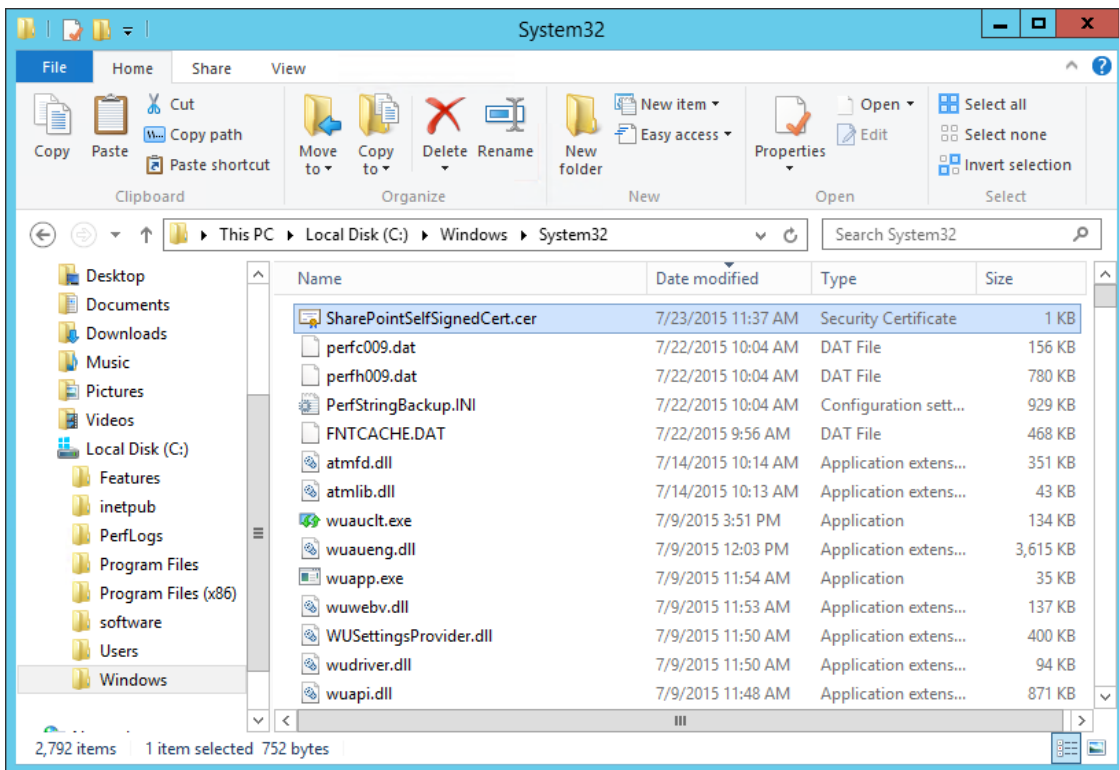


2141

2142

2143

14. Open **File Explorer** and click through locations to reach the location of your self-signed certificate (from this example: *C:/Windows/System32/*).



2144

2145

2146

15. Right-click on the **self-signed certificate** and click on **Copy** or left-click on the self-signed certificate and press the keys Ctrl+C.

2147

2148

16. Right-click on your **Desktop** and click **Paste**, or left-click on your Desktop and press the keys Ctrl+V to save a copy of the certificate in an accessible location.

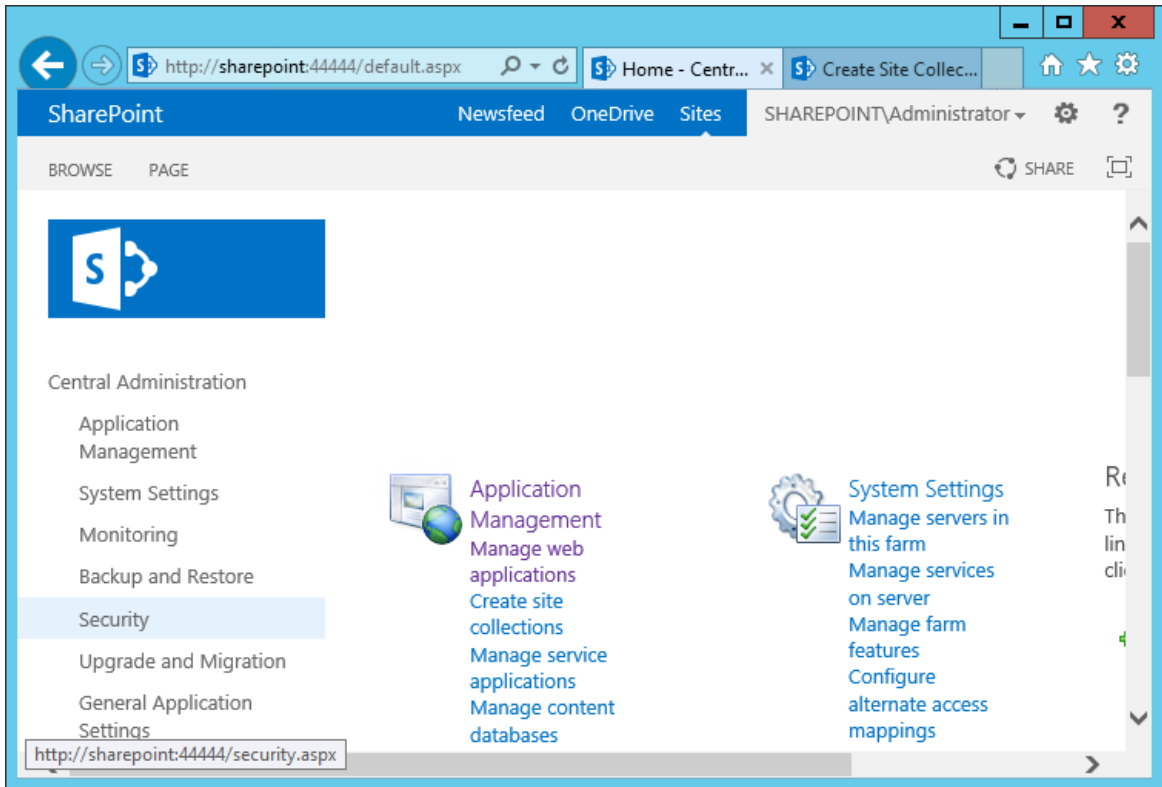
2149

17. To Manage Trust via Central Administration, do the following steps: Open a **browser**.



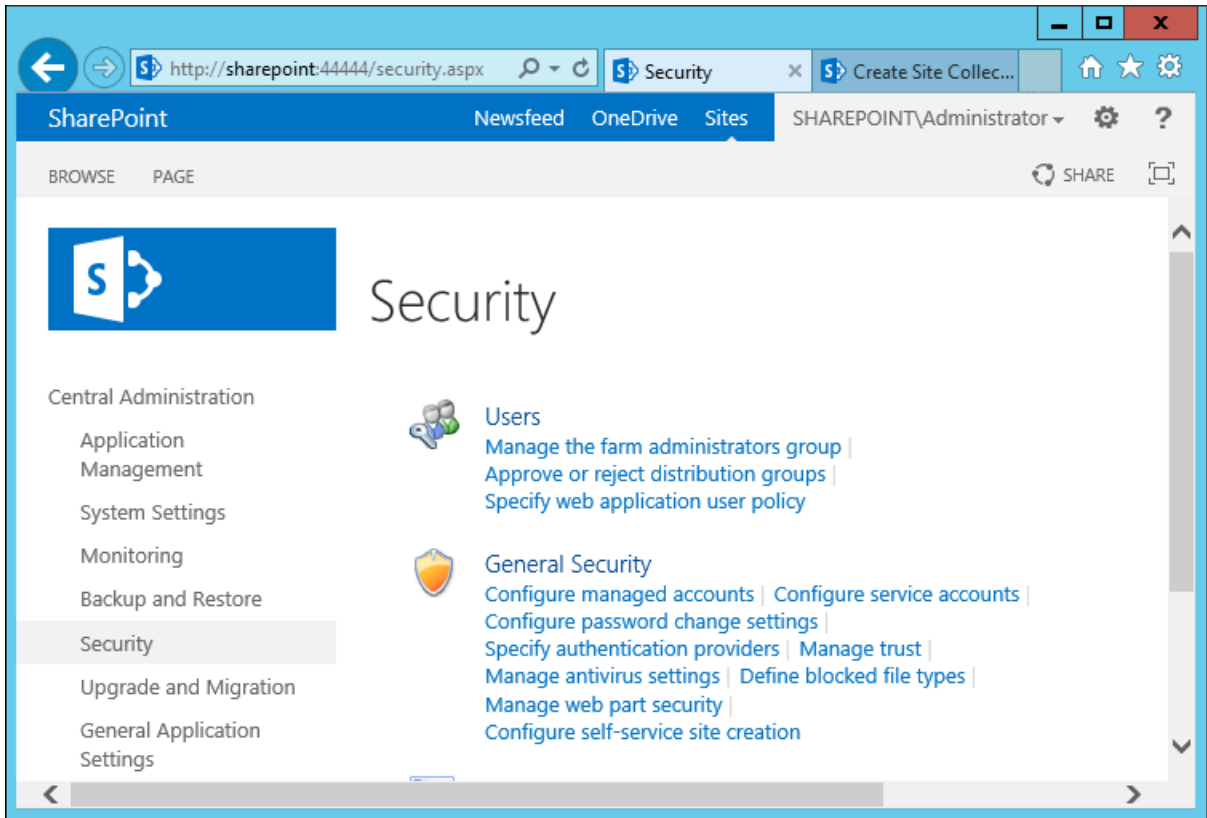
2150 18. In the **URL address bar** of the browser, enter the address for Central Administration and click  
2151 **Enter** or Go: *http://sharepoint:44444/default.aspx*

2152 19. From the Central Administration page, click on **Security** in the left-hand menu.



2153

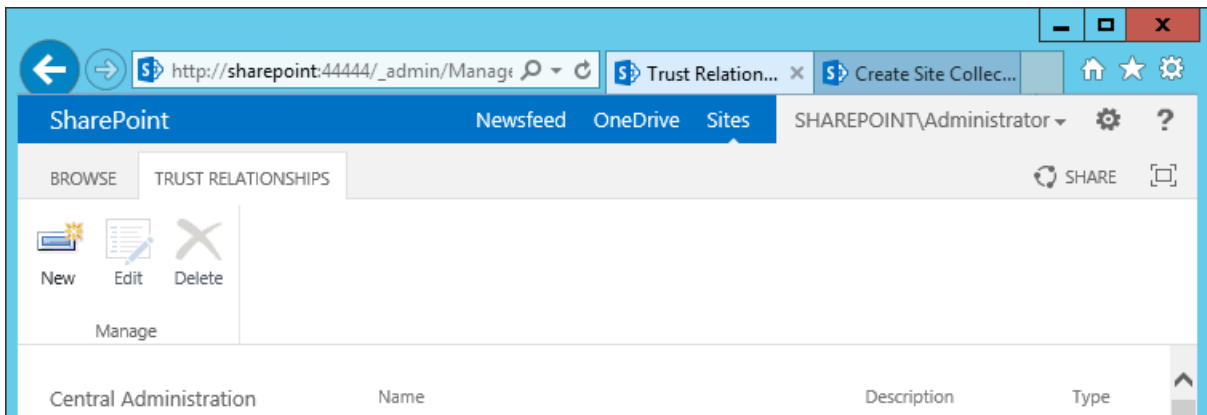
2154 20. From the Security page, under the General Security section, click on **Manage Trust**.



2155

2156

21. Under the Trust Relationships tab of the Manage Trust page, click **New**.



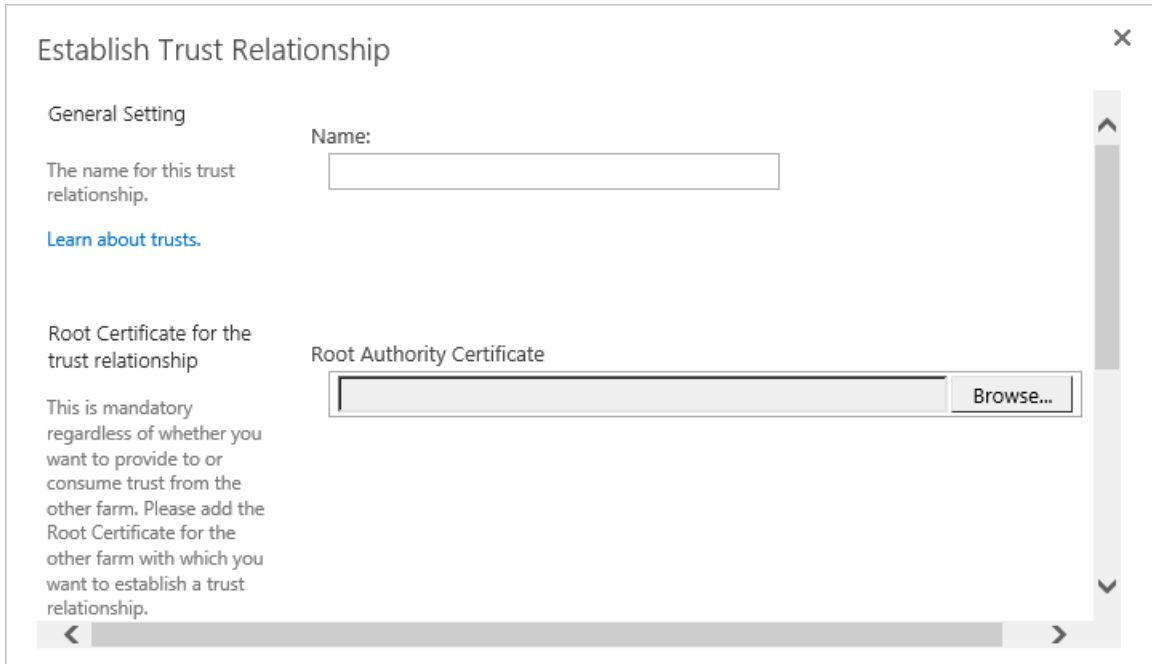
2157

2158

2159

2160

22. In the Establish Trust Relationship window that opens automatically, enter the **Name** for the trust relationship being created, then click **Browse** to find the certificate created in previous sub-sections.



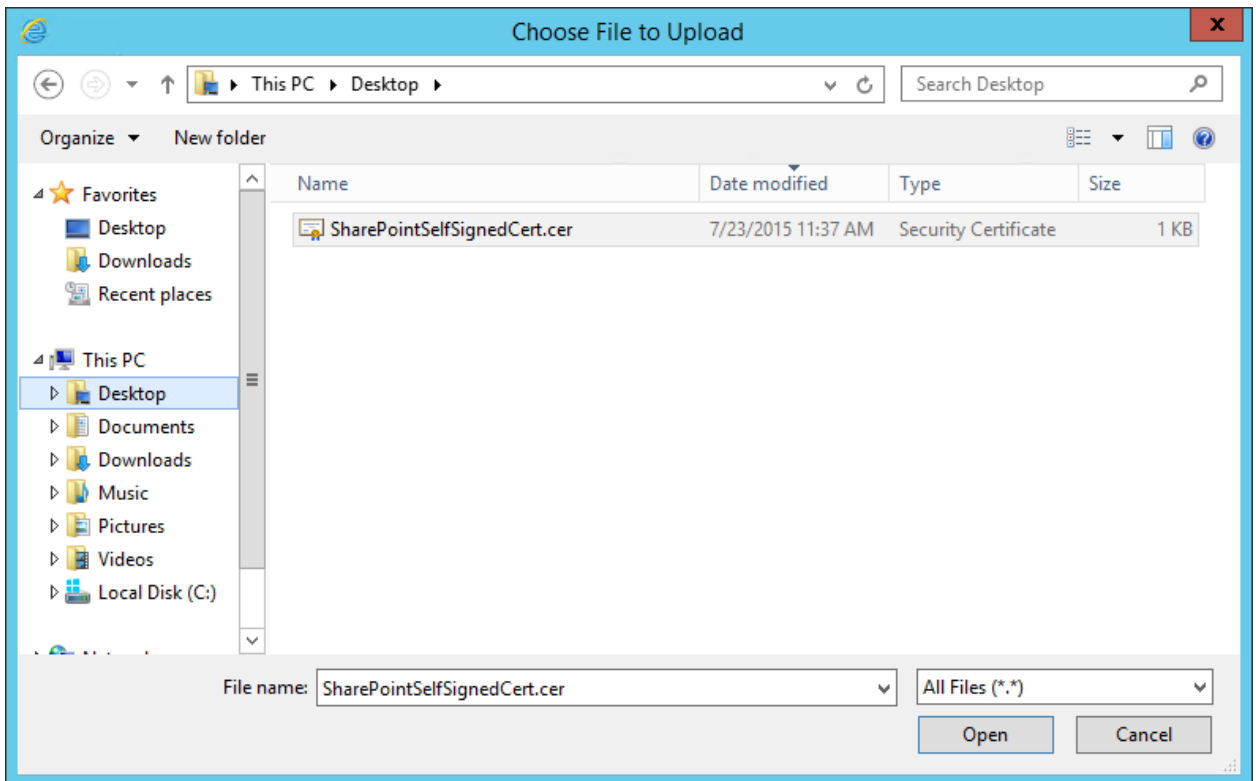
2161

2162

2163

2164

23. In the Choose File to Upload window that opens automatically, navigate to the copy of your certificate from [Section 4.4.1.1](#) (e.g., Desktop). Click on the certificate so its name automatically fills the **File name** field at the bottom of the window, then click **Open**.

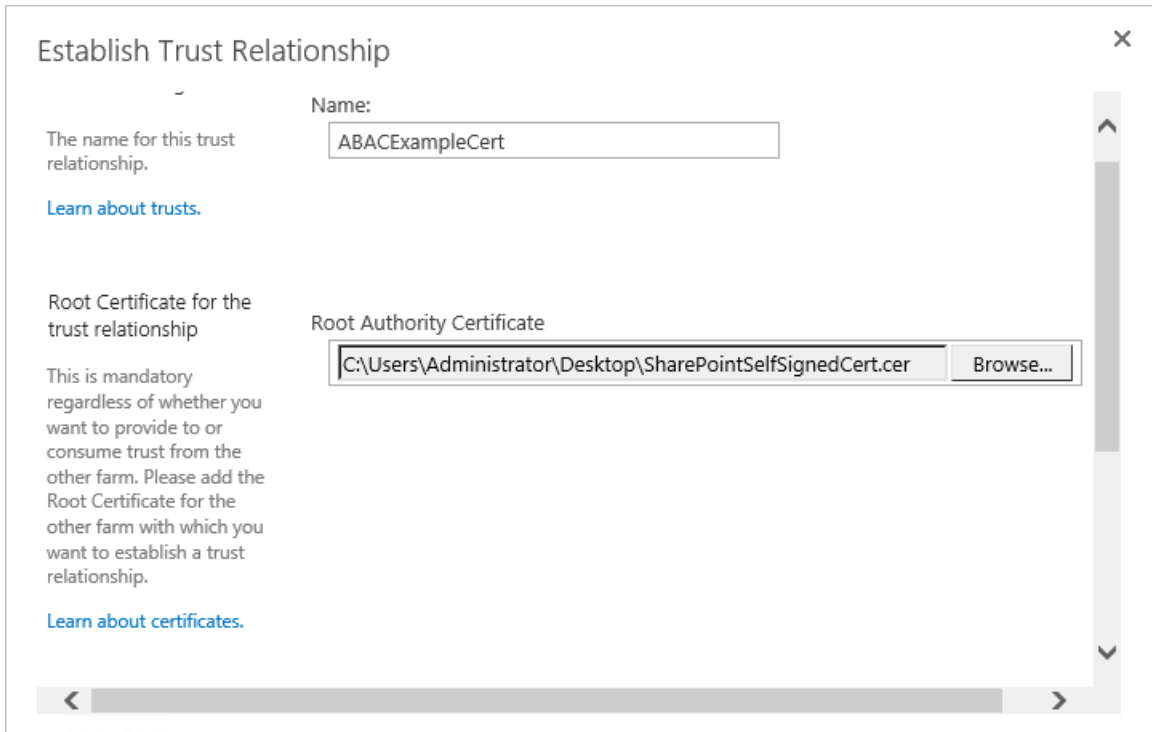


2165

2166

2167

24. In the Establish Trust Relationship window, the certificate's location will be automatically entered as the **Root Authority Certificate**.

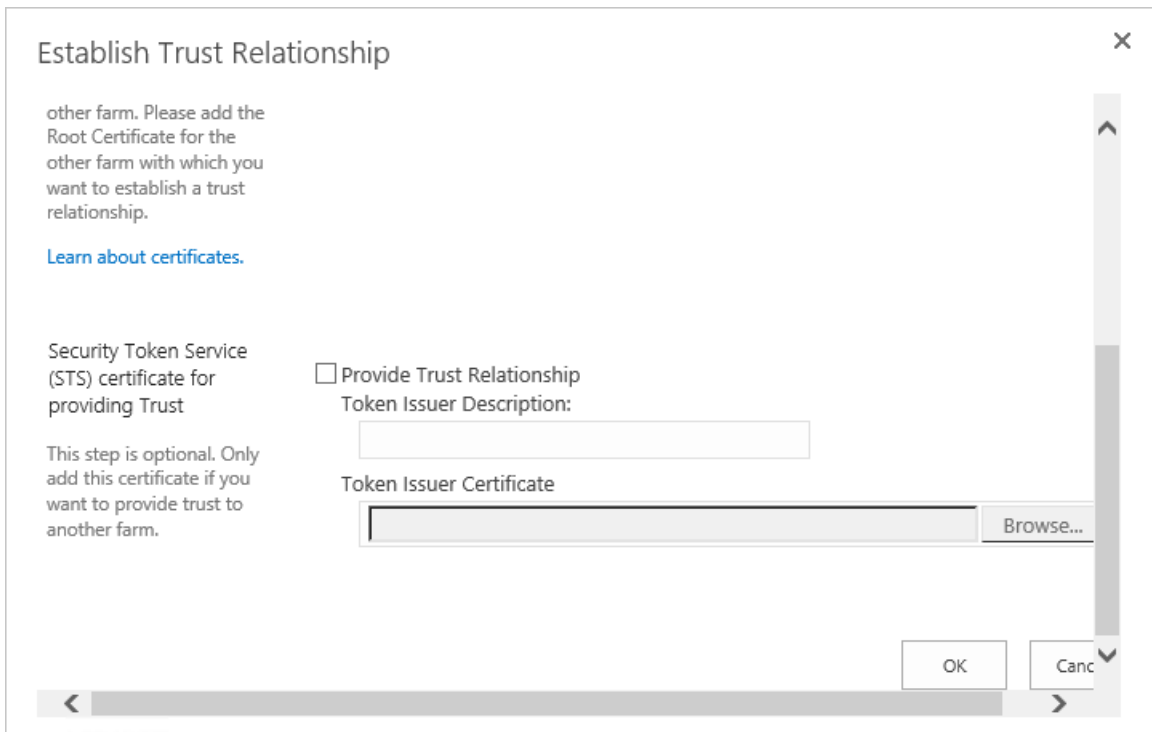


2168

2169

2170

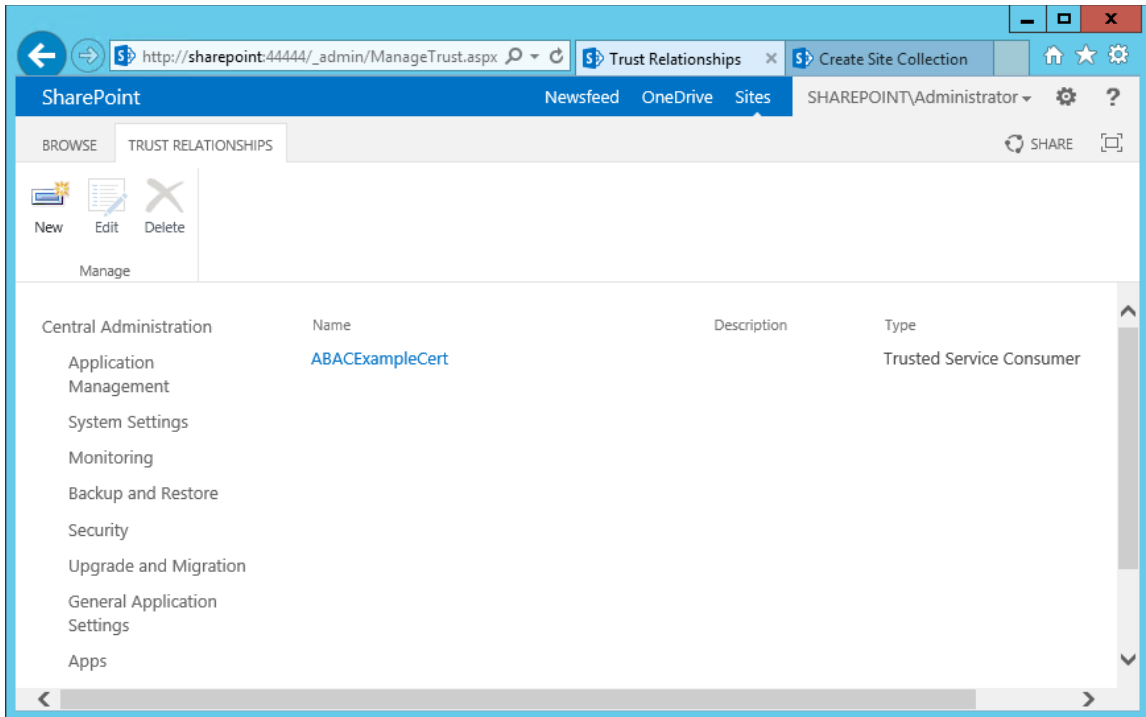
25. In the Establish Trust Relationship window, scroll down leaving the remaining fields empty, and click **OK**.



2171

2172

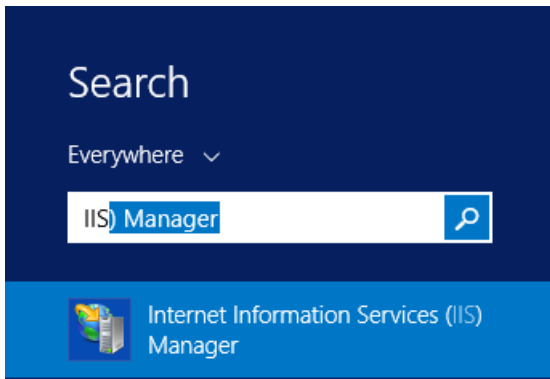
26. Your new trust relationship will be listed under the Trust Relationships tab.



2173

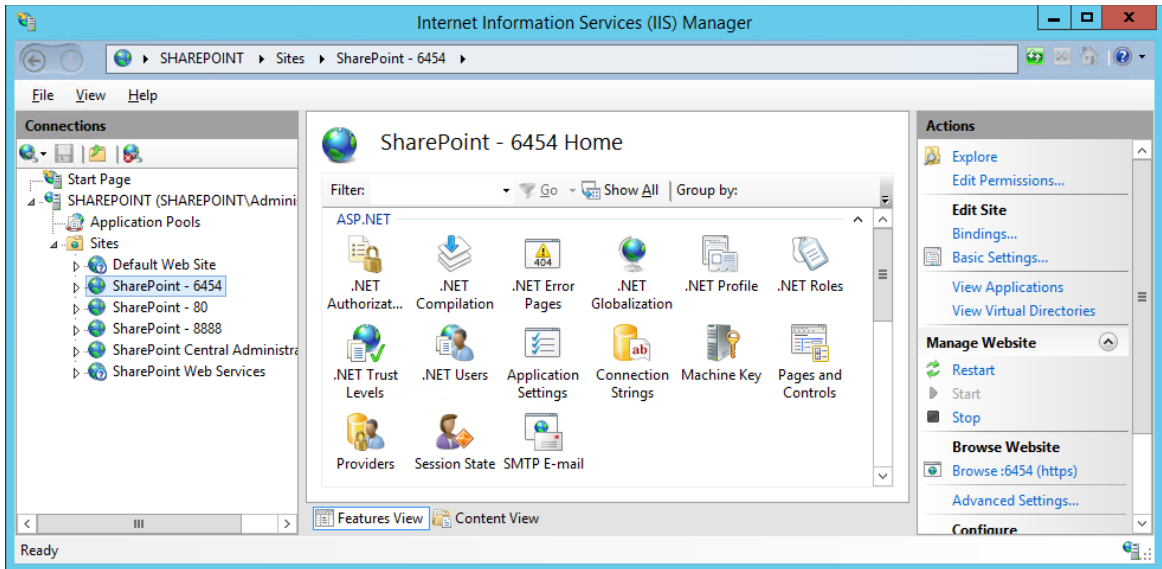
2174 *4.4.1.4 Configure IIS Binding for the Self-Signed Certificate*

- 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**
- 2180 created in previous steps, then click **Bindings** in the Actions pane on the right.



2181

2182

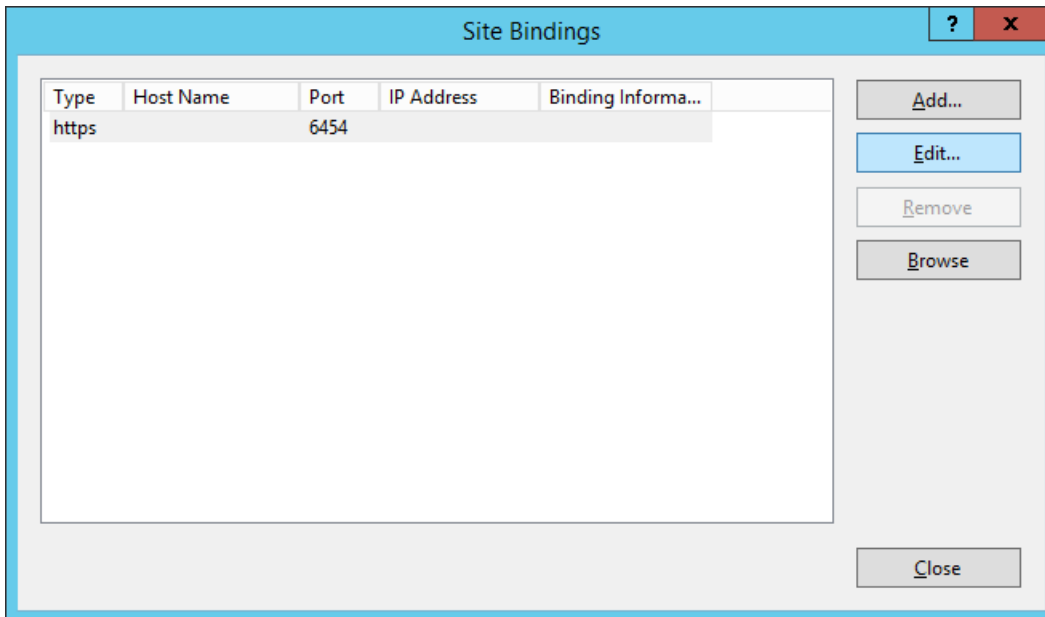
5. In the Site Bindings window that opens, look for a binding type of https.

2183

a. If a binding type of https does not exist, click on **Add**.

2184

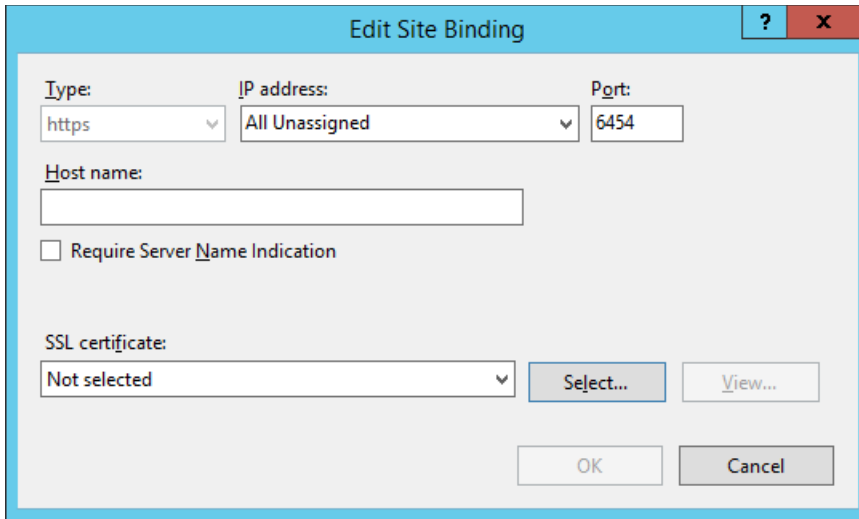
b. If a binding type of https does already exist, click on it, then click **Edit**.



2185

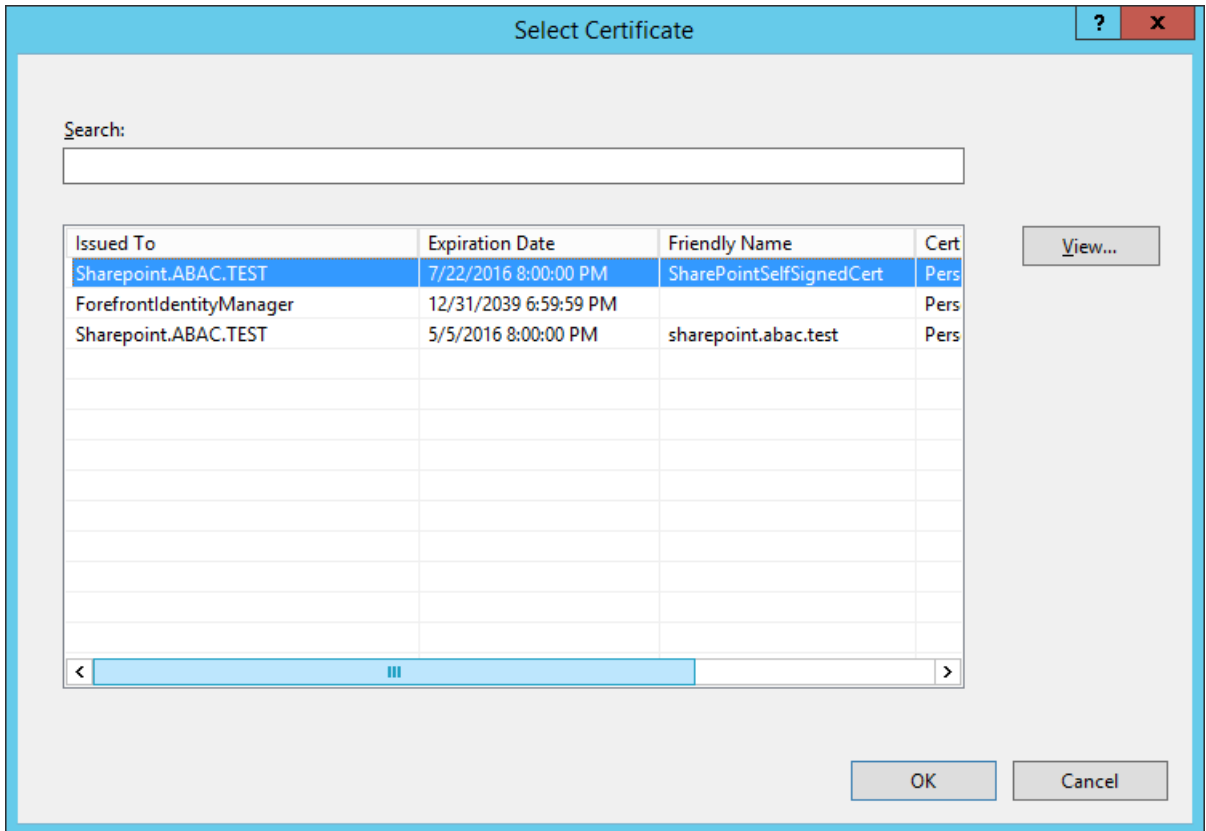
2186

6. In the Edit Site Binding window next to the SSL certificate field, click **Select**.



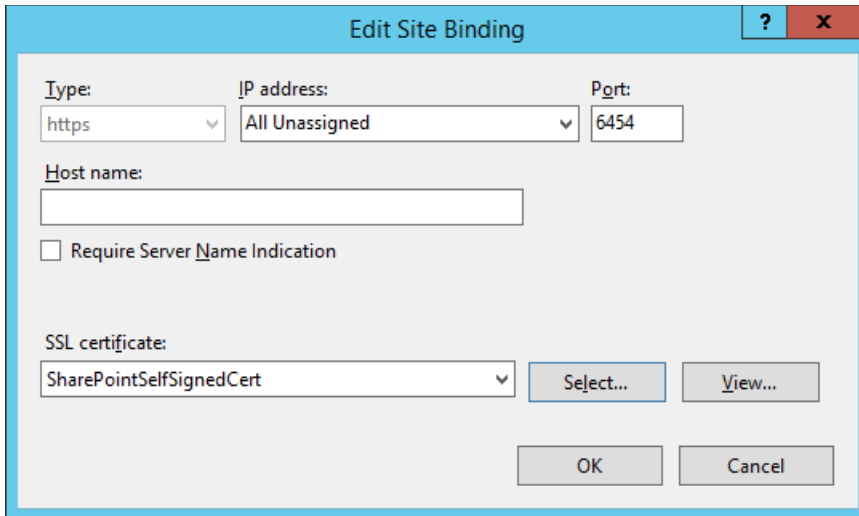
2187

2188 7. In the Select Certificate window, click on the certificate created in previous steps and click **OK**.



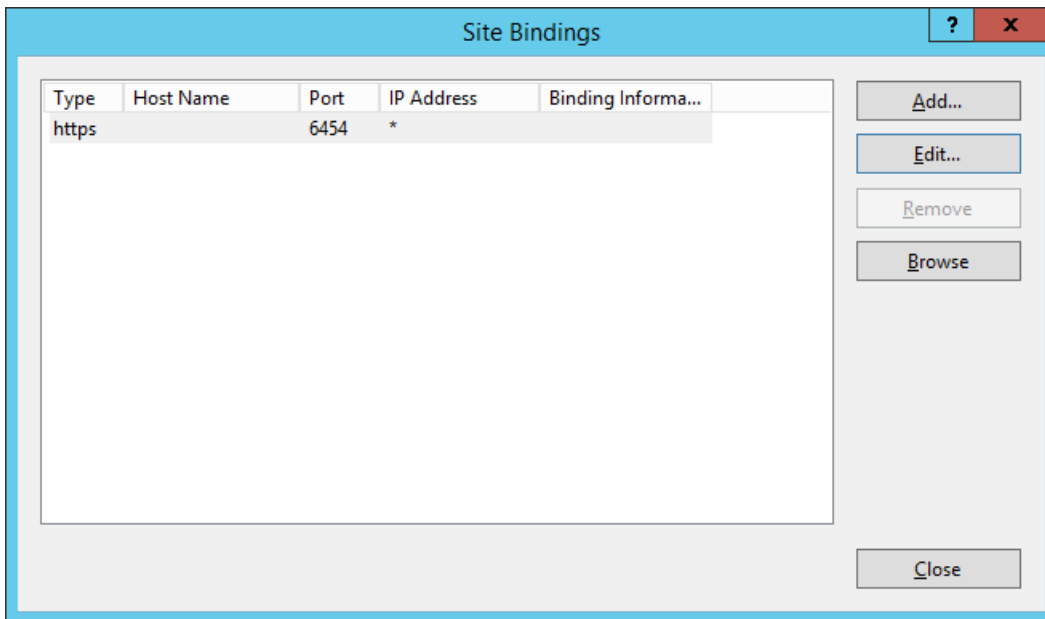
2189

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.

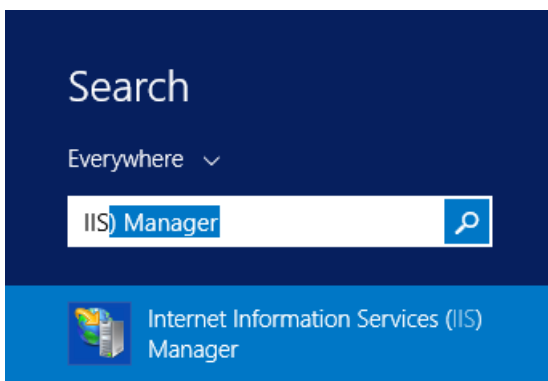


2200 Although the detailed instructions of configuring certificates signed by a certificate authority vary by  
 2201 vendor product, the general process is described below. For each certificate, you perform the following  
 2202 high-level steps:

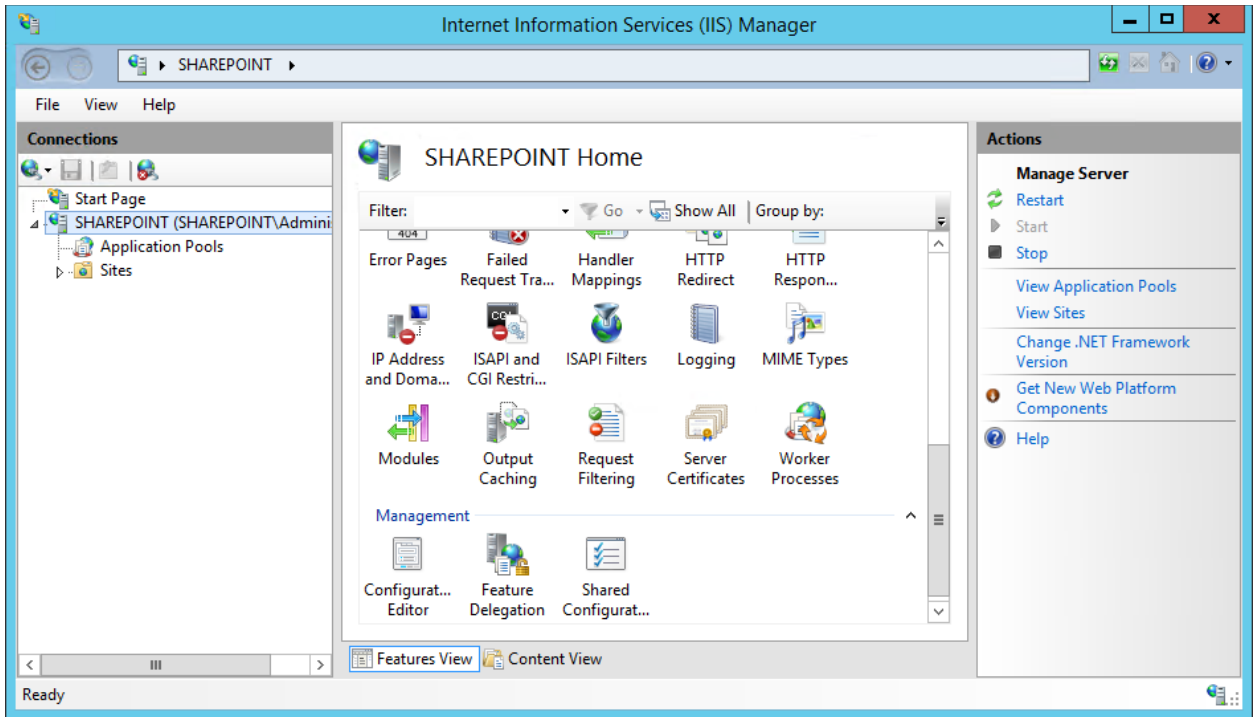
- 2203 1. Using the vendor product (e.g., SharePoint), generate a certificate signing request on the server  
 2204 where you want to use the certificate. Save the signing request to a file.
- 2205 2. Submit an enrollment request to your certificate authority. You will need to provide the signing  
 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.

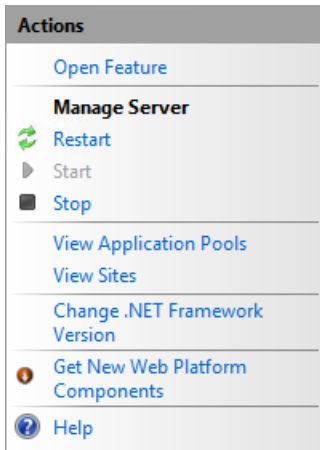


- 2225
- 2226 5. In the left-hand Connections column, left-click on your **SharePoint** instance.
- 2227 6. Scroll down in the SharePoint Home pane and left-click on **Server Certificates**.



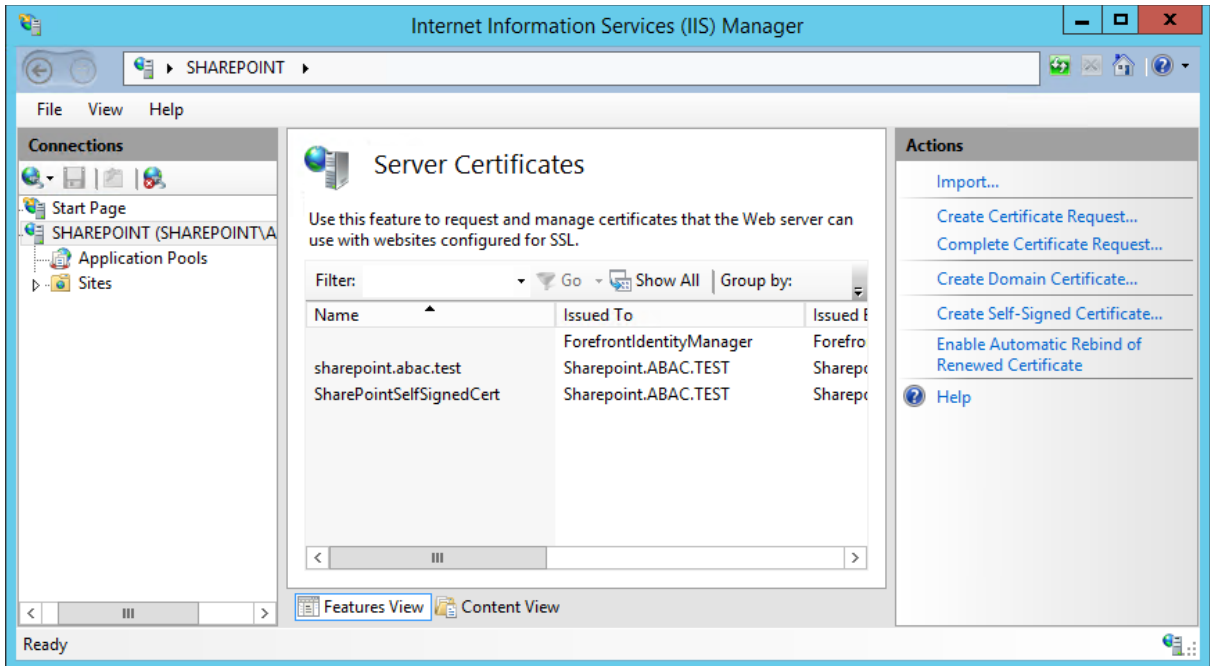
2228

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**  
2232 **Request**.

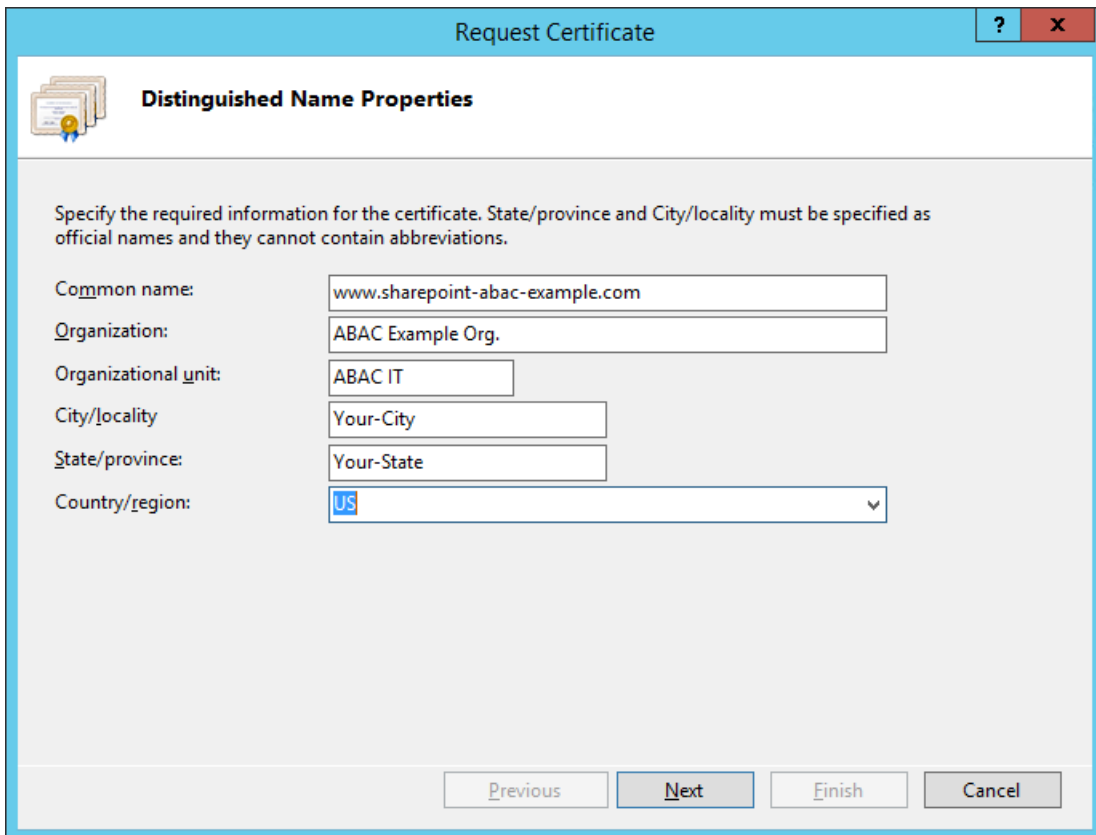


2233

2234

2235

- In the Distinguished Name Properties window that opens automatically, enter your organizational information and click **Next**.

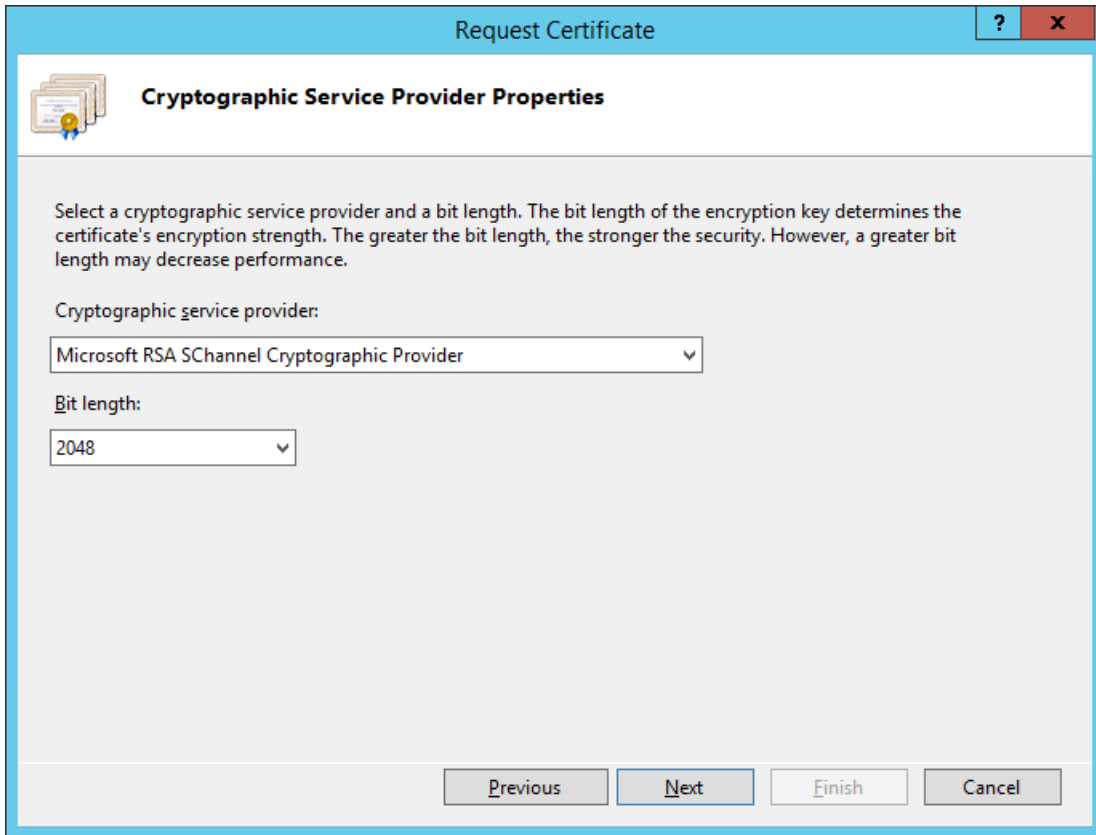


2236

2237

2238

- In the Cryptographic Service Provider Properties window that opens automatically, choose the **Cryptographic service provider** and a **Bit length**, then click **Next**.

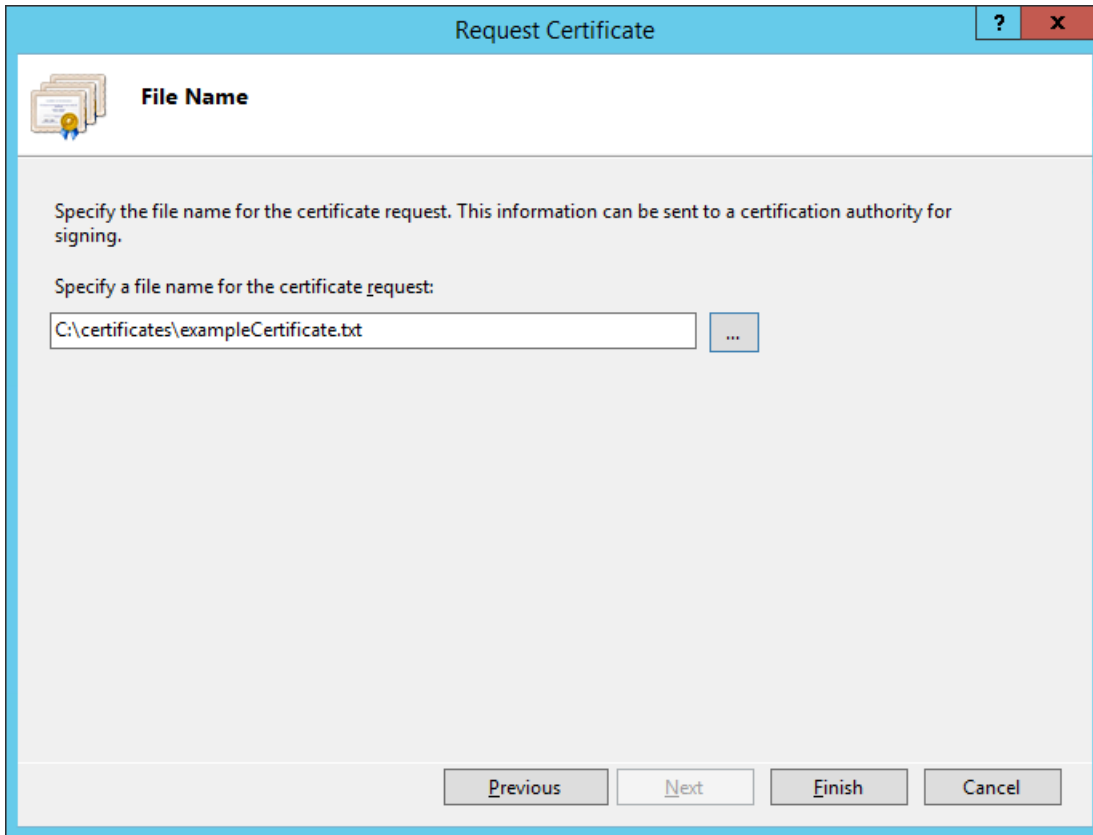


2239

2240

2241

11. On the File Name screen, browse to the location where you would like to save this certificate or type in the path, including a name for your certificate ending in “.txt,” then click **Finish**.

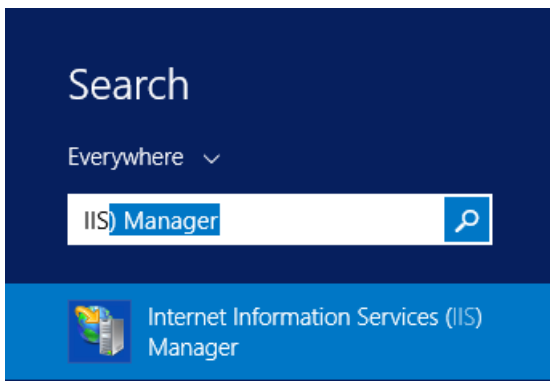


2242

2243 *4.4.2.2 Installing the new signed SSL Certificate*

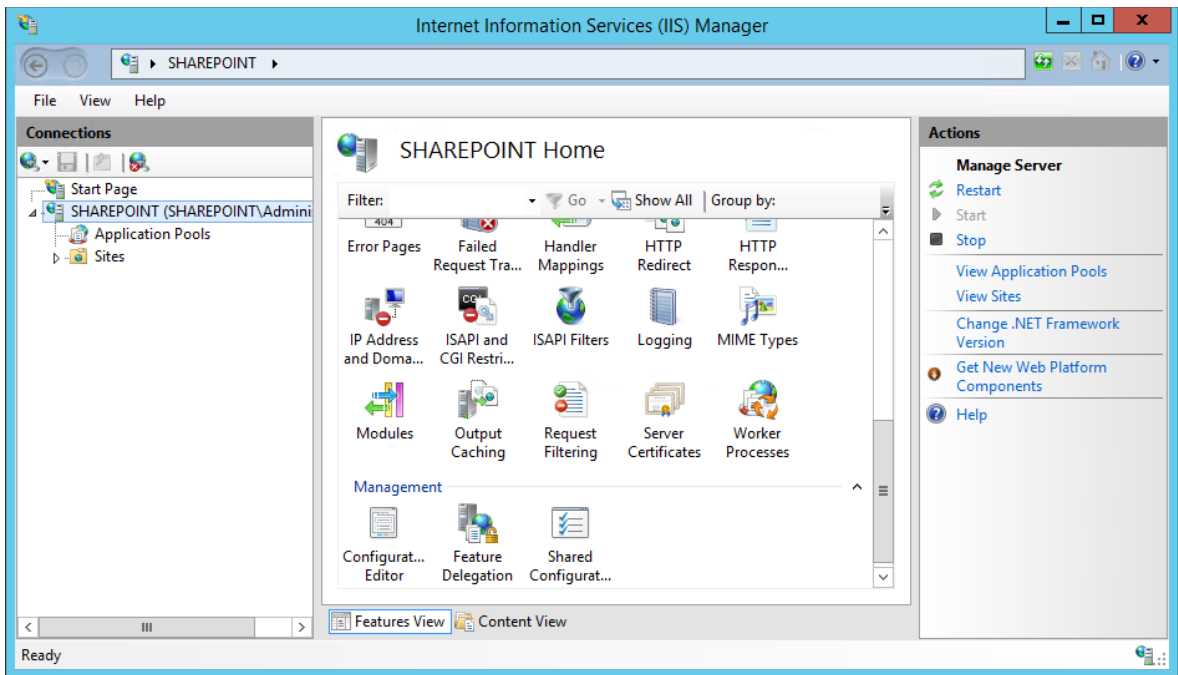
2244 When the new signed SSL Certificate is available either from a local or online Certificate Authority, install  
 2245 the certificate using the instructions in this section.

- 2246 1. Log onto the SharePoint Server and save the SSL certificate resulting from the CSR in [Section](#)  
 2247 [4.2.1](#).
- 2248 2. Click on the **Windows** icon in the bottom left corner of your screen.
- 2249 3. Begin typing **IIS**.
- 2250 4. When the **Internet Information Services (IIS) Manager** appears, click on it.

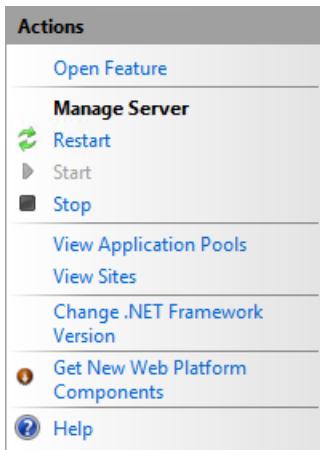


2251

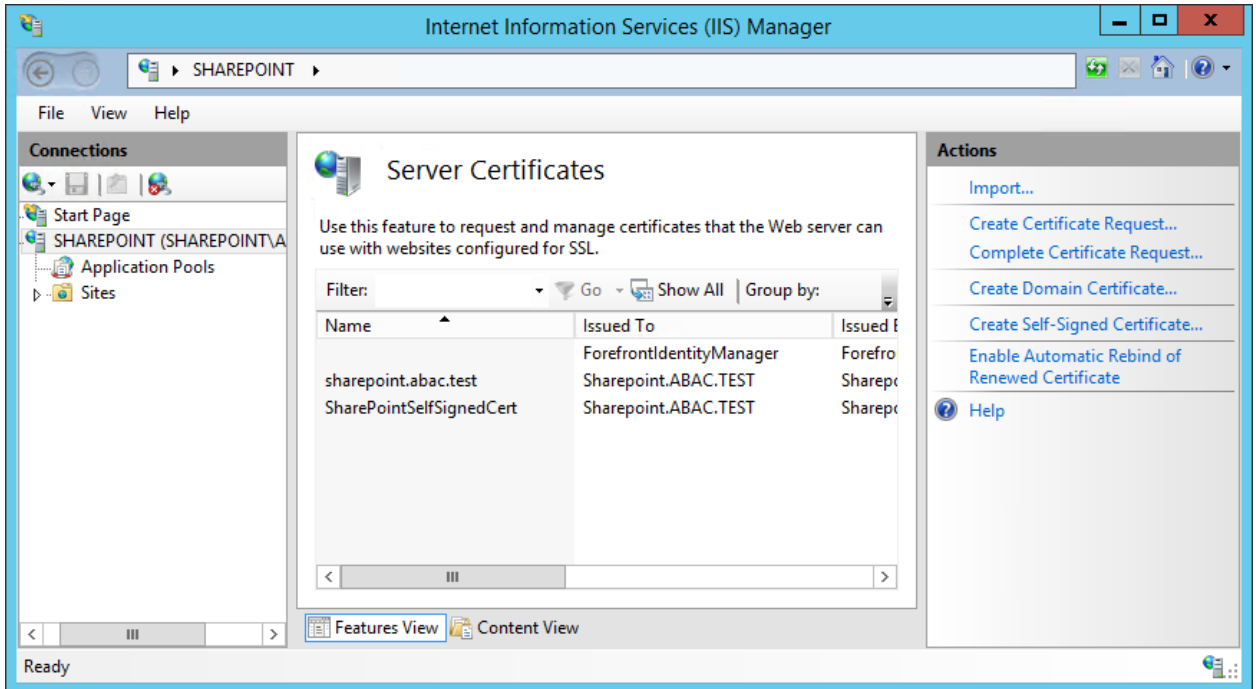
- 2252 5. In the left-hand Connections column, left-click on your **SharePoint** instance.
- 2253 6. Scroll down in the SharePoint Home pane and left-click on **Server Certificates**.



- 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**
- 2258 **Request.**



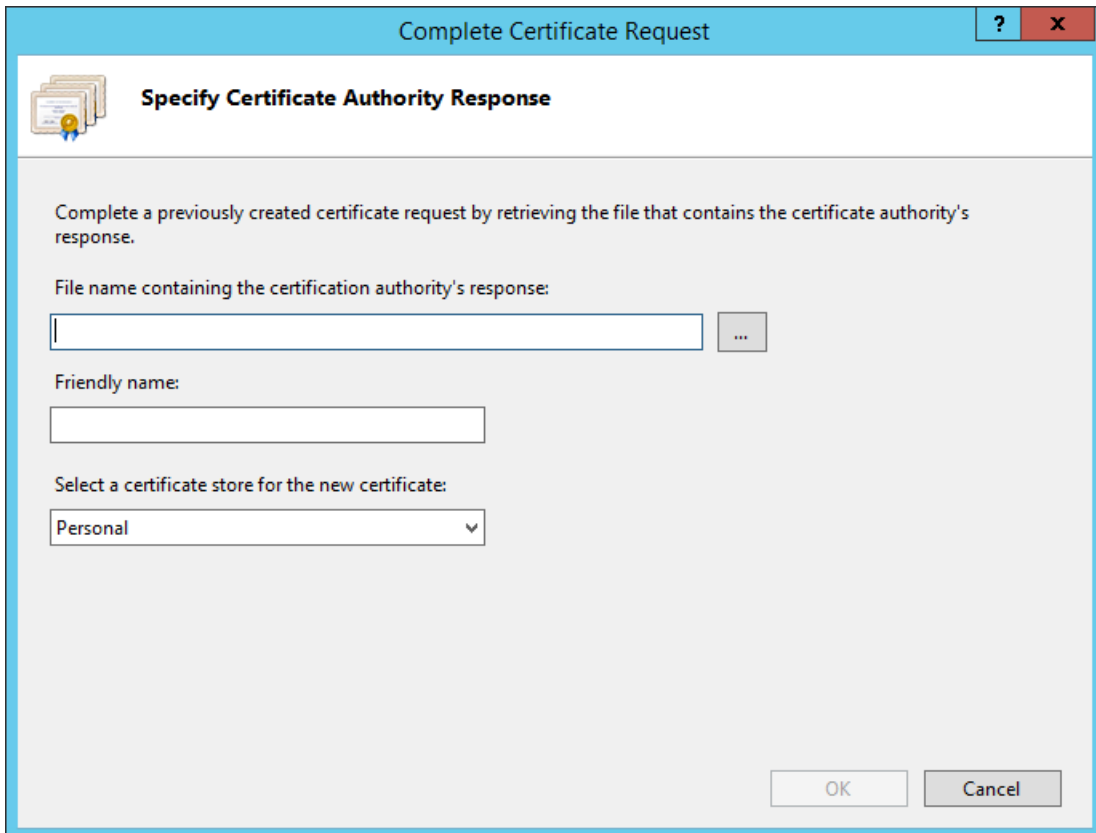
2259

2260

2261

2262

- In the Complete Certificate Request wizard on the Specify Certificate Authority Response screen, browse to the location of the new SSL certificate generated from your CSR or type in its location, enter a friendly name, and choose a certificate store from the drop-down menu. Click **OK**.



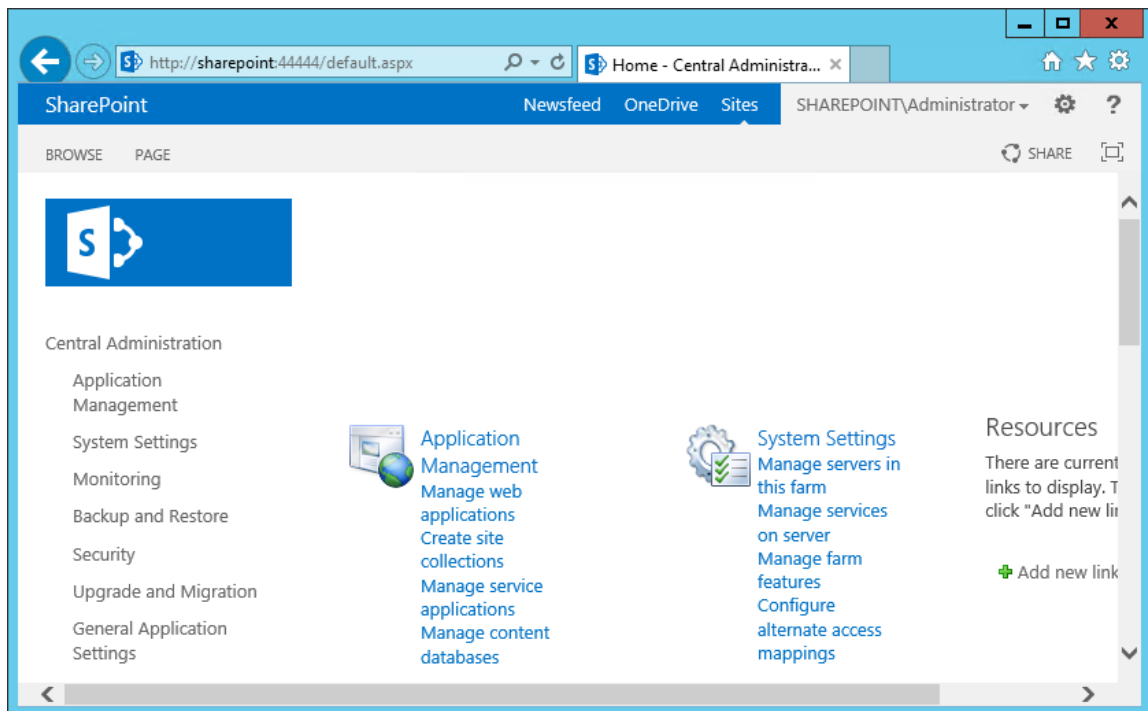
2263

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.

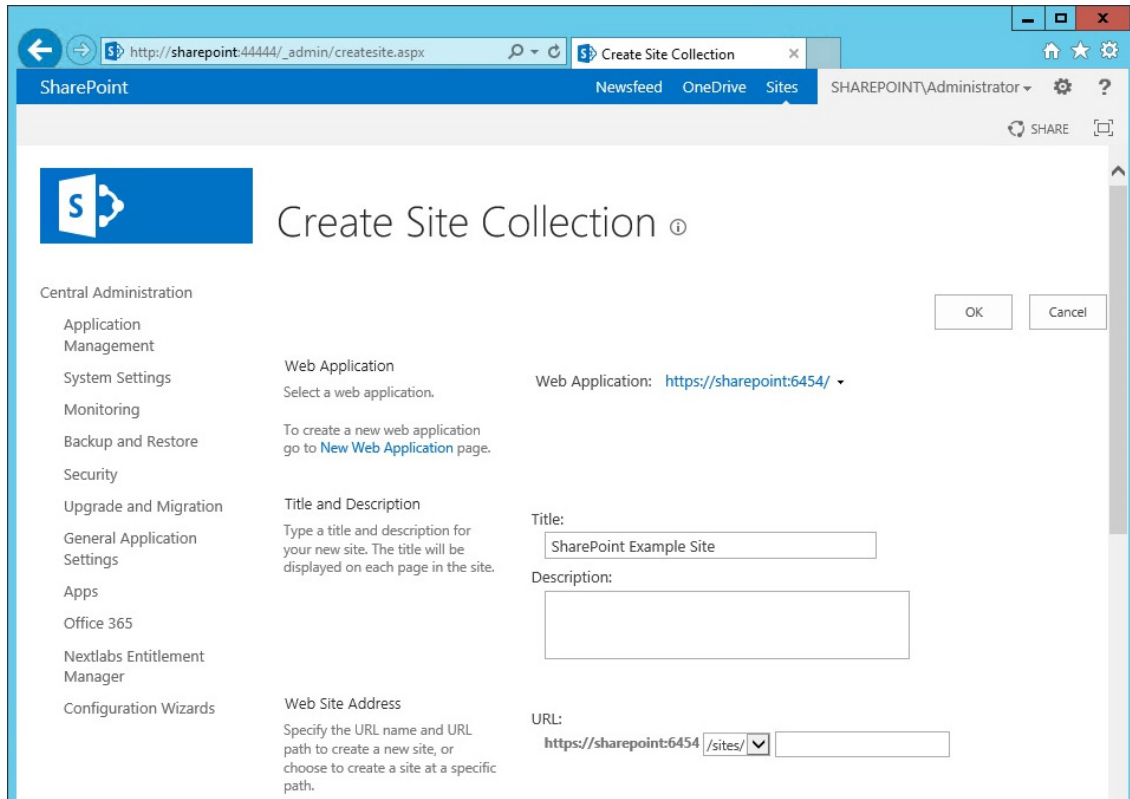
2268 **4.5** **Creating a Site Collection**

- 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  
 2271 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
- 2275 4. On the Create Site Collection page, do the following:
- 2276 a. Verify that the web application under consideration is the one chosen.
- 2277 b. Enter a **Title** (required) and **Description** (optional).
- 2278 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 name of your SharePoint Administrator account and click on the **Name check** icon. If the name is found, it will not give a warning and the name will be underlined.

2285

2286

2287

i. Alternatively, you can look up users by name using the address book people picker mechanism next to the user name text field.

2288

2289

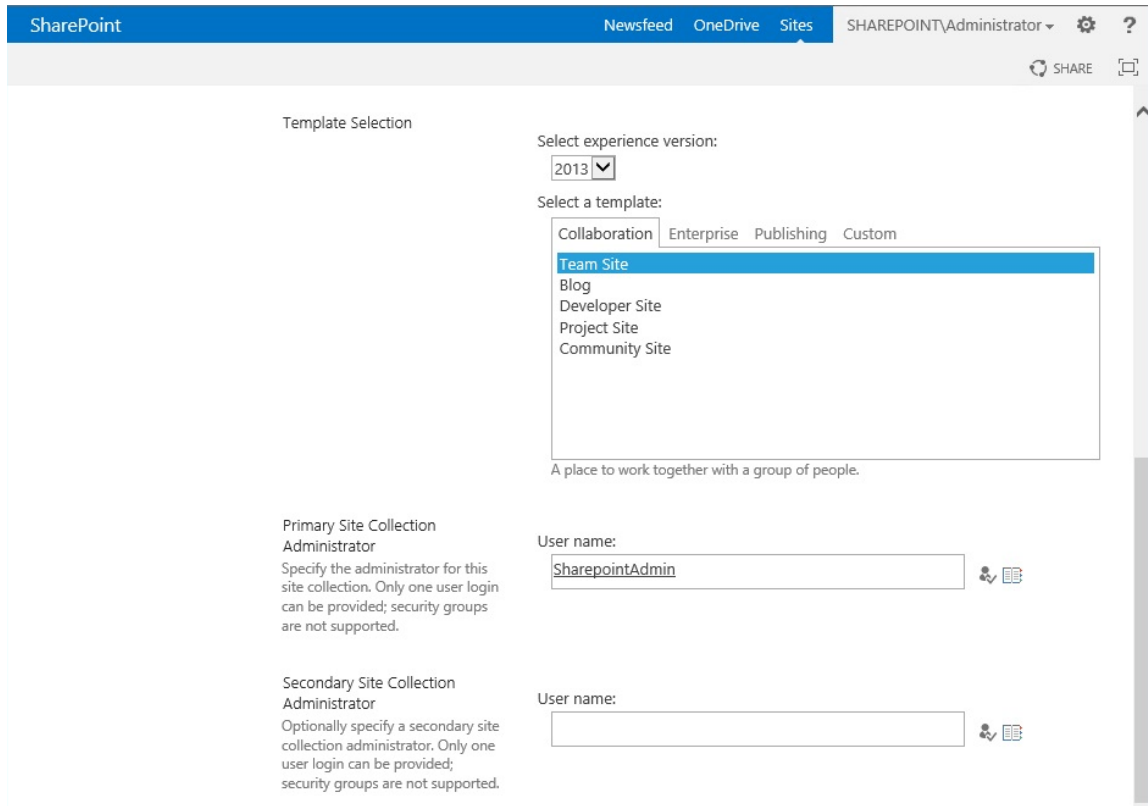
c. In the **User name** field under the Primary Site Collection Administrator area, type in the name of a secondary administrator if you so choose.

2290

2291

i. Alternatively, you can look up users by name using the address book people picker mechanism next to the user name text field.

2292

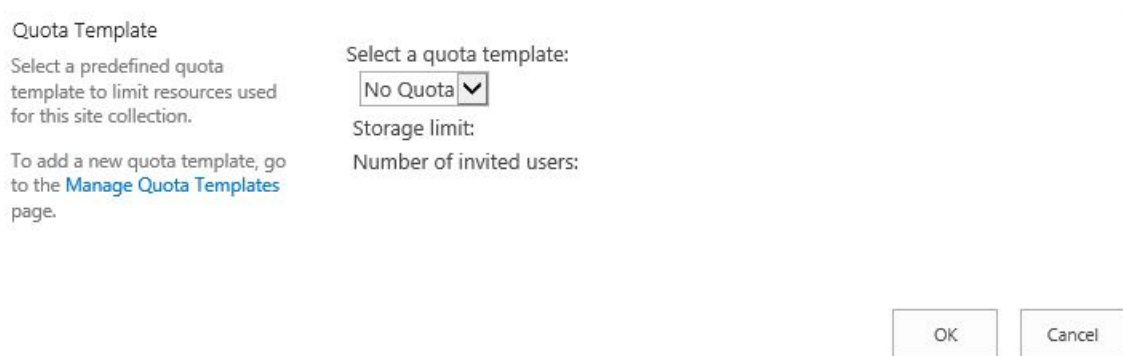


2293

2294

2295

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**.



2296

2297

7. Wait for the Site Collection to successfully complete.

Working on it...

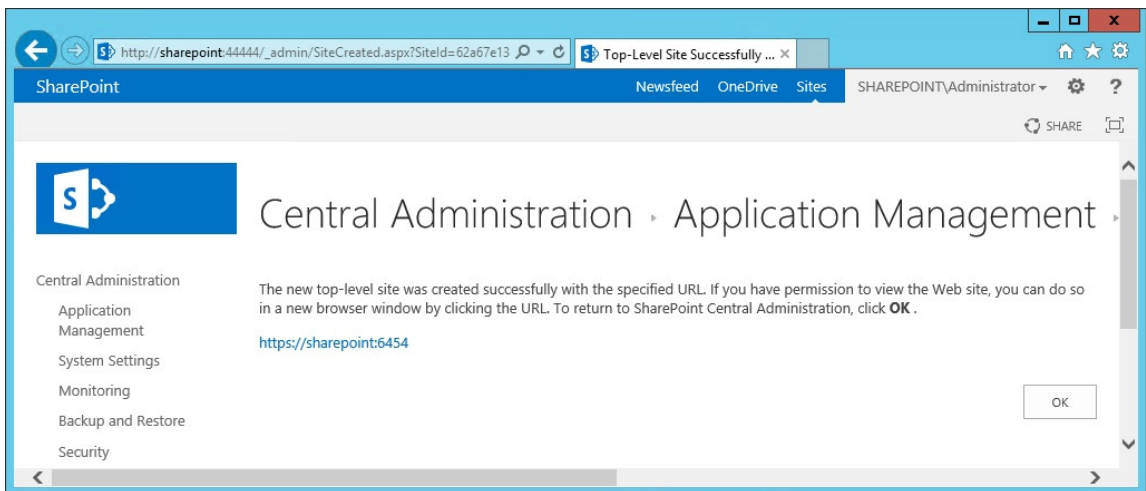
⋮ This shouldn't take long.

2298

2299

2300

8. In the browser, on the page that indicates a new top-level site was created successfully, click **OK**.



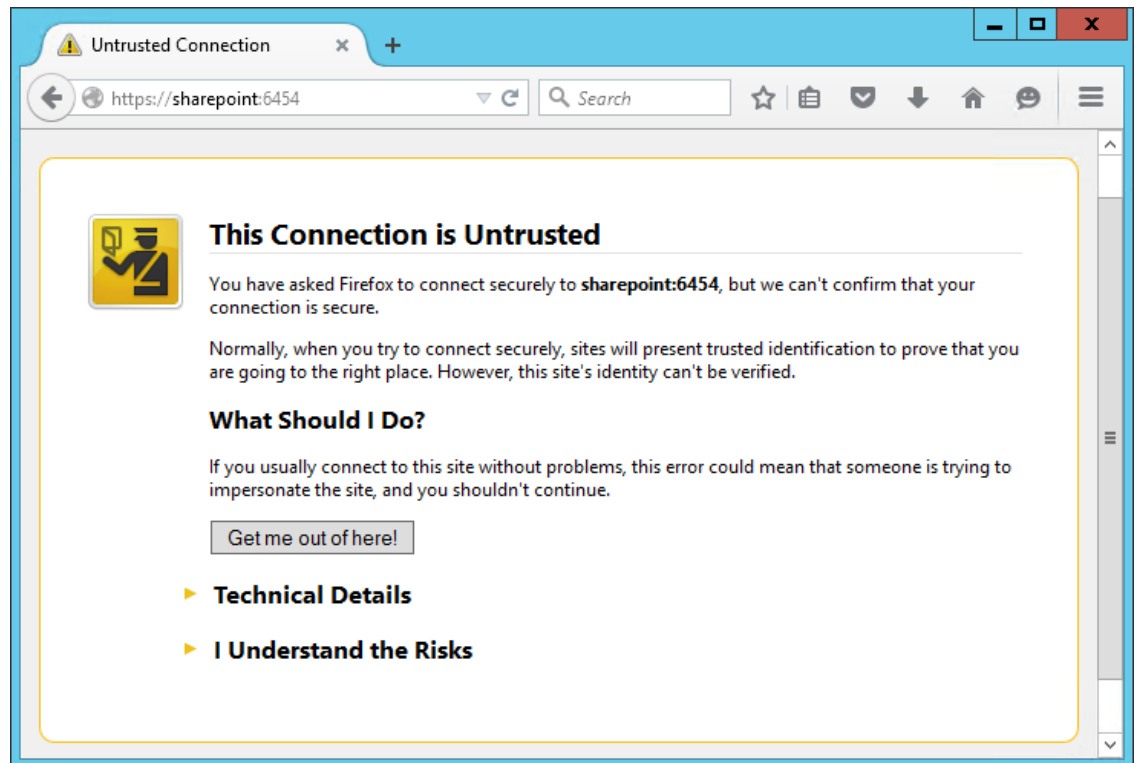
2301

2302

2303

2304

9. Open a browser and navigate to the URL for your new web application (e.g., *https://sharepoint:6454*)
  - a. You may see a warning first because of the self-signing certificate.

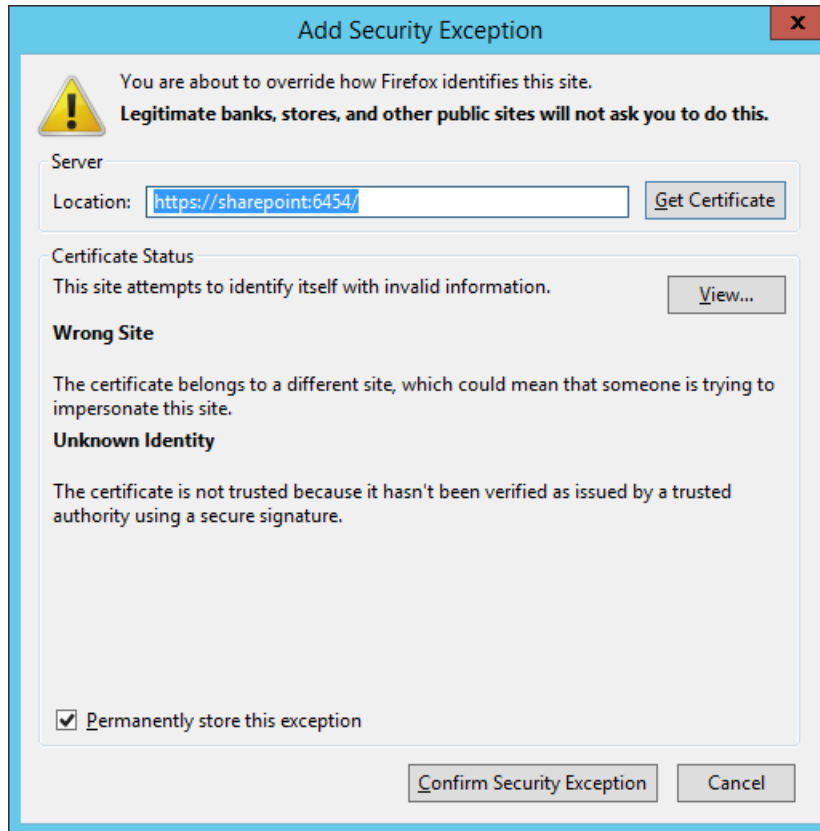


2305

2306

2307

- b. In the browser window, click on **I Understand the Risks**, then **Add Exception**.
- c. In the Add Security Exception window, click on **Confirm Security Exception**.

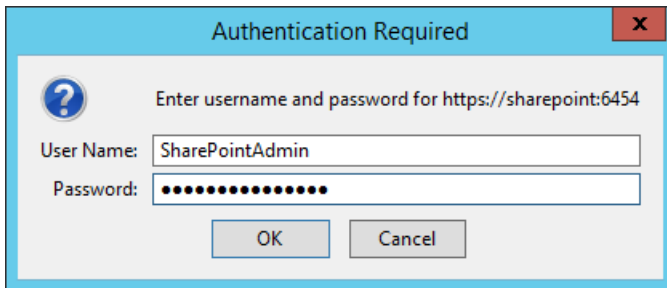


2308

2309

2310

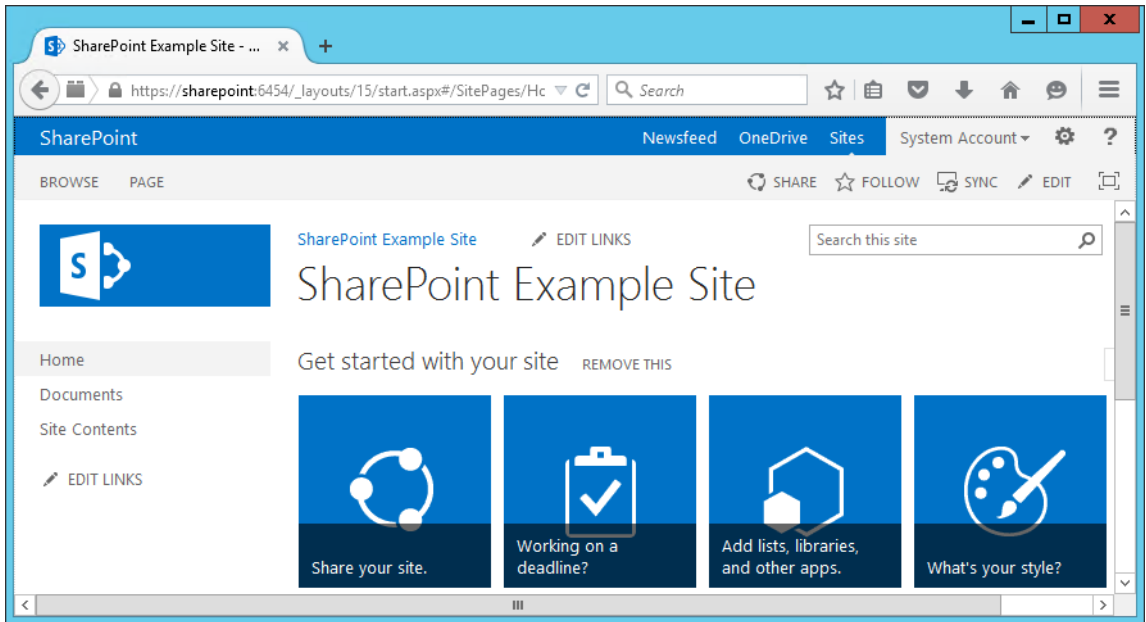
10. In the Authentication Required window that opens automatically, enter the administrator account **User Name** and **Password**, then click **OK**.



2311

2312

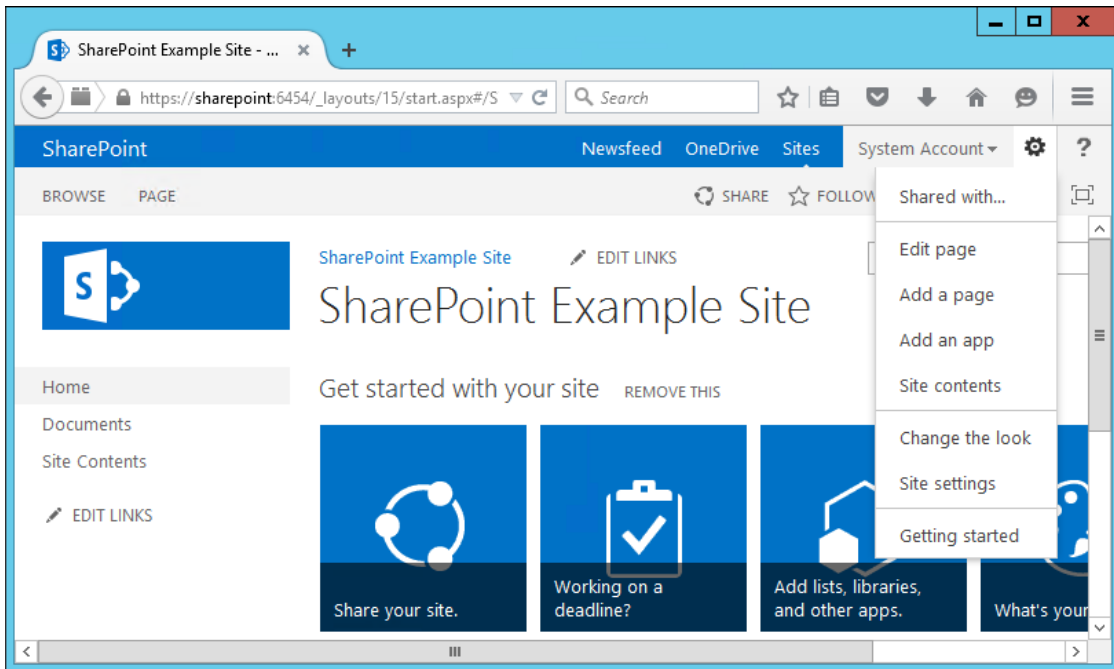
11. Upon verification that the login was a success, you will see default site contents.



2313

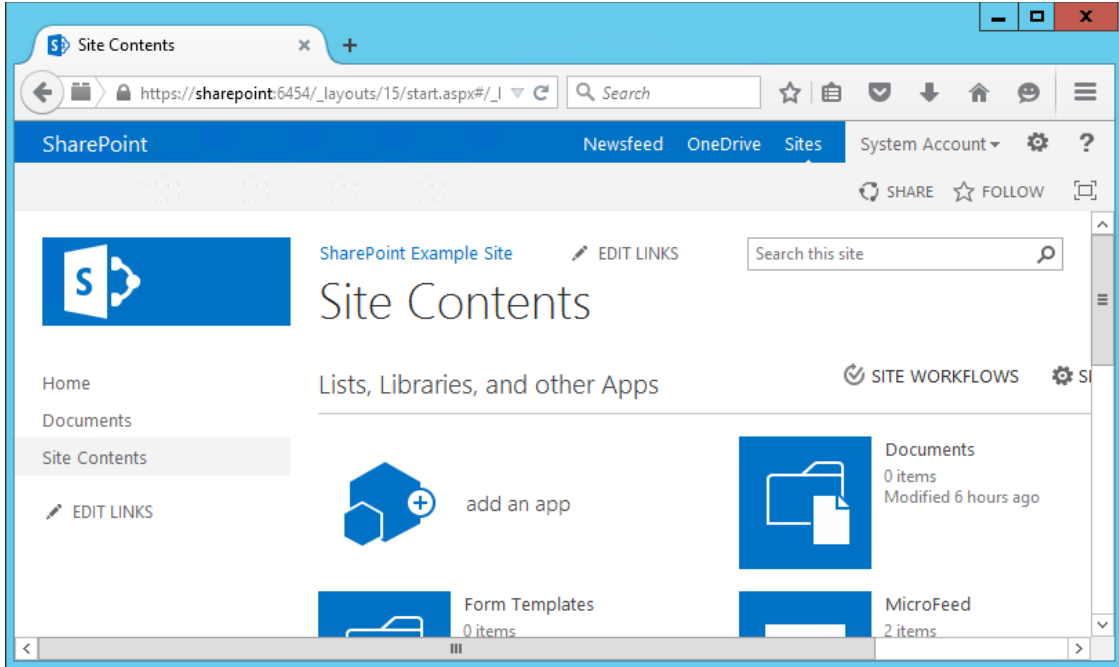
#### 2314 4.6 Creating New Sub-Sites

- 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.

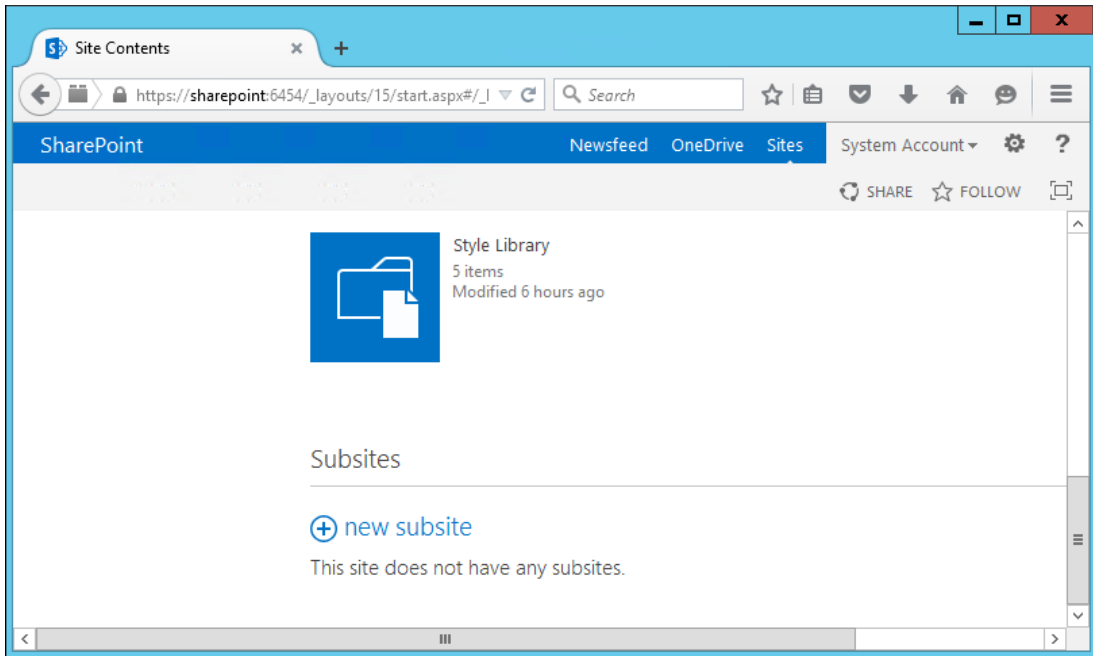


2319

2320

2321

3. In the browser window, scroll down to the Subsites area and click the **plus sign button** next to new subsite.



2322

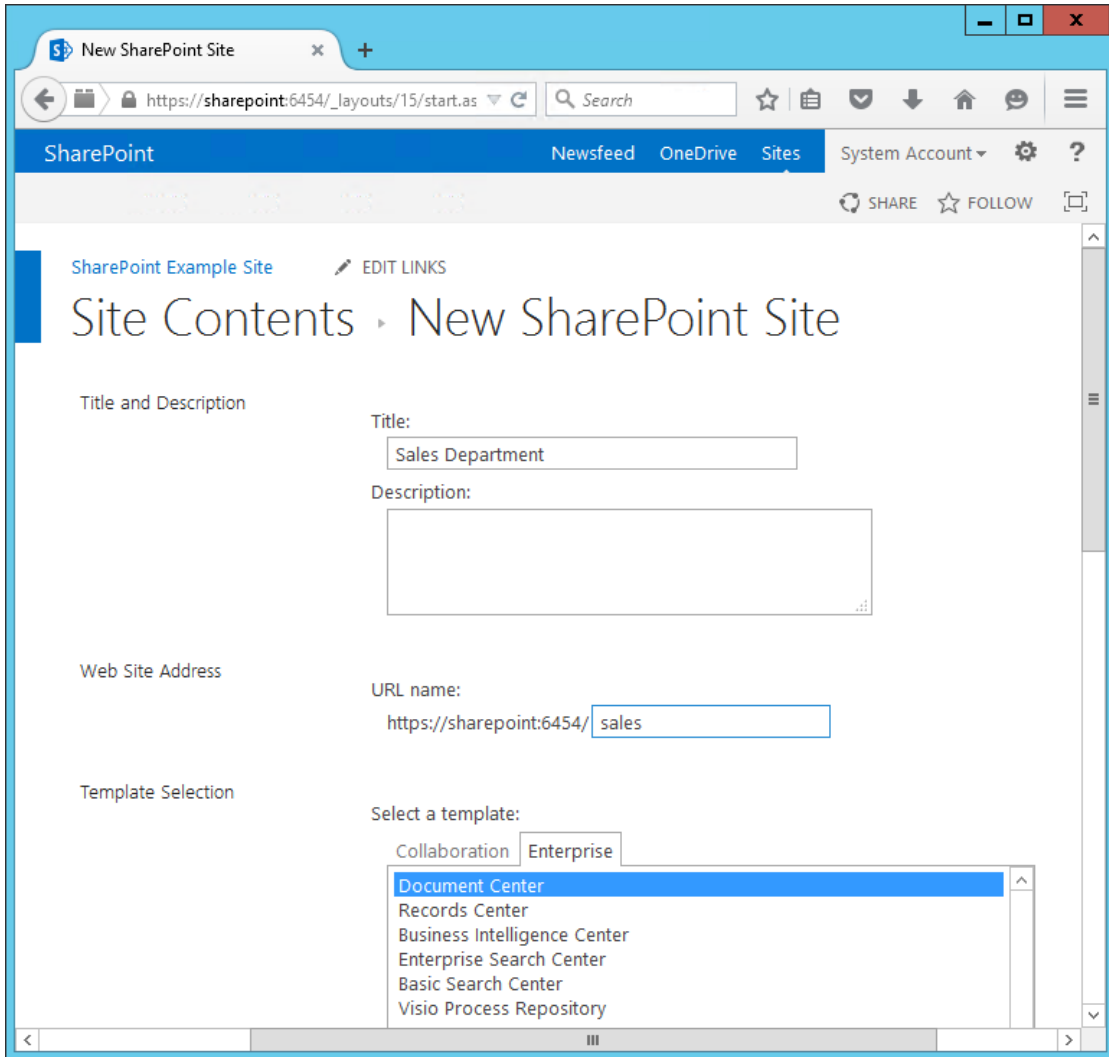
2323

2324

2325

2326

4. In the browser window on the New SharePoint Site screen, do the following:
  - a. Enter **Title** (required) and **Description** (optional).
  - b. Enter a **URL name**.
  - c. **Select a template**.



2327

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 radio button selected).

2330

2331

b. Choose your **Navigation** and **Navigation Inheritance** settings.



**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.

**User Permissions:**

Use same permissions as parent site  
 Use unique permissions

**Navigation**

Display this site on the Quick Launch of the parent site?  
 Yes  No

Display this site on the top link bar of the parent site?  
 Yes  No

**Navigation Inheritance**

Use the top link bar from the parent site?  
 Yes  No

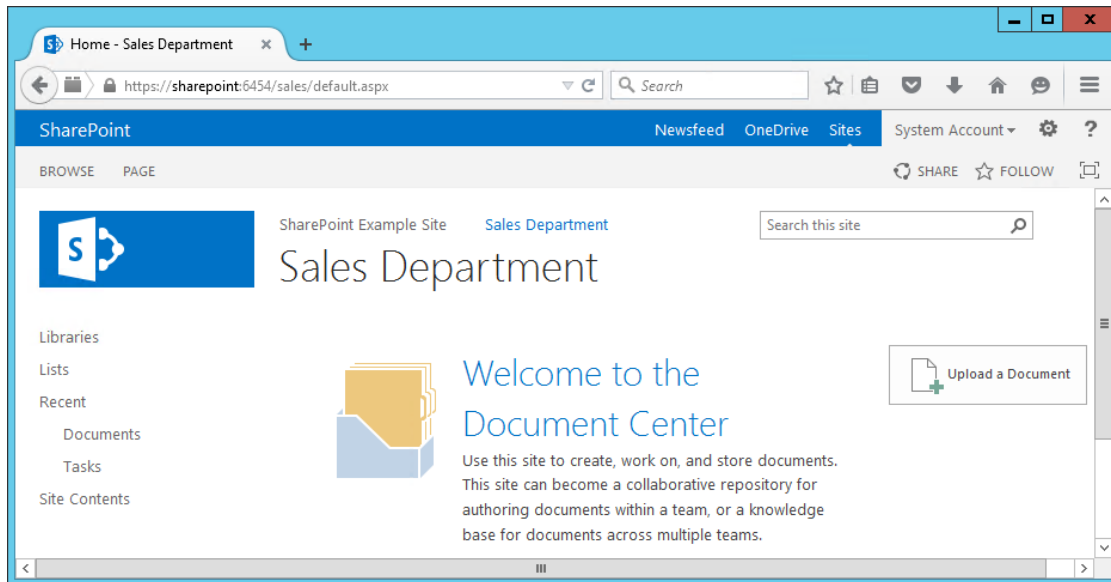
2332

2333 6. In the browser, scroll down and click **Create**.



2334

2335 7. Your new subsite will open in the browser.



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 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](#).

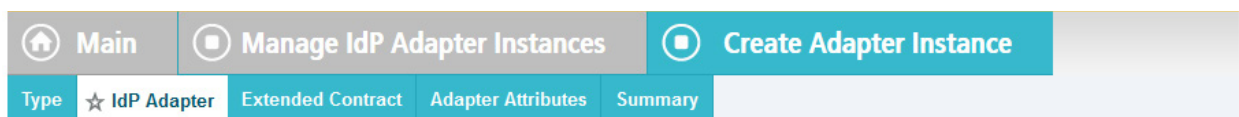
2349 We will demonstrate how to set up a trusted logon provider for the relying party' so that when a user  
2350 requests access to a SharePoint site, the user will be redirected to the PingFederate-RP for  
2351 authentication via WS-Federation. The Ping-Federate-RP will then forward the authentication 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

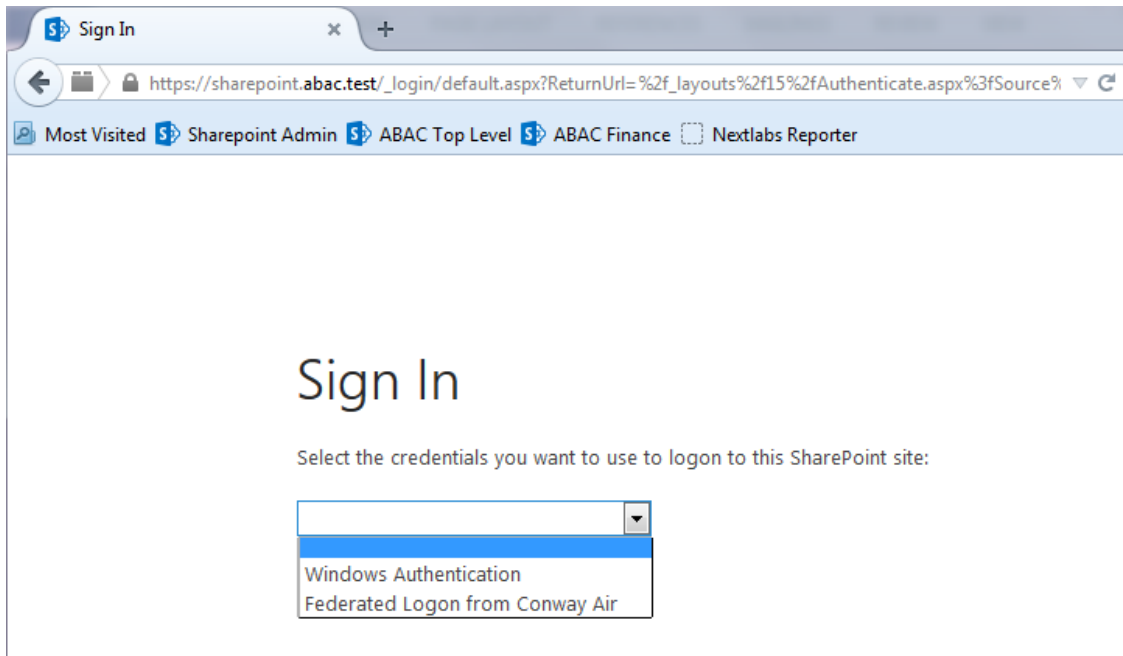
- 2361  When using the PingFederate application to perform an administrative configuration, there is  
2362 usually a sequence of screens, ending with a summary page. Once you click **Done** on the  
2363 summary page, you must also click **Save** on the following page to save the configurations. If 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.

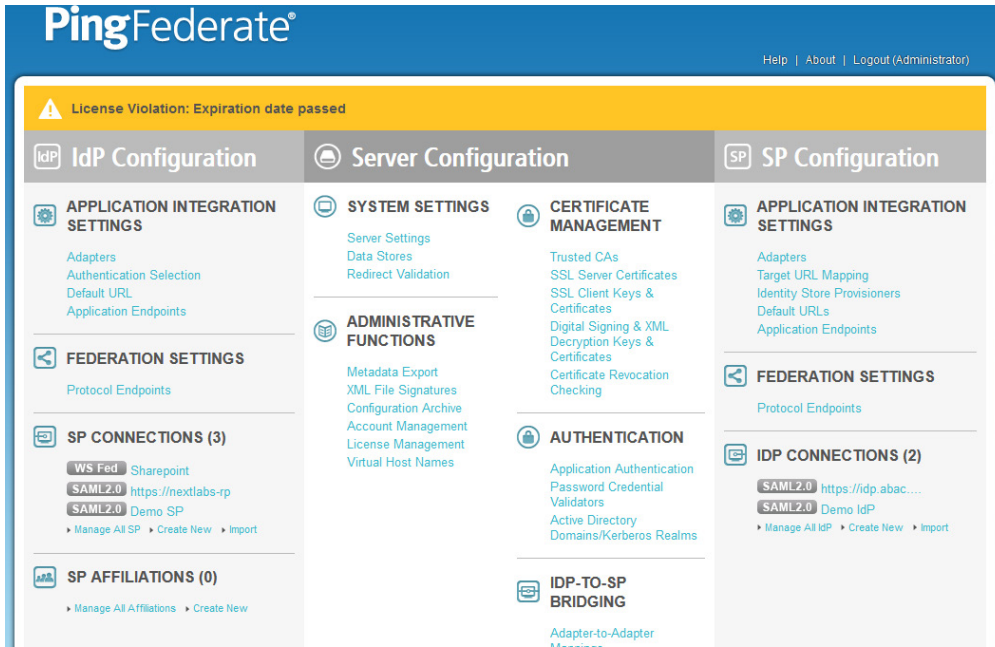


2376  
 2377 In order to set up a federated logon, you will configure a trust relationship between the SharePoint  
 2378 server and the PingFederate-RP that will facilitate the federated logon. Once a user authenticates via a  
 2379 federated logon, the PingFederate-RP will cryptographically sign WS-Federation 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.

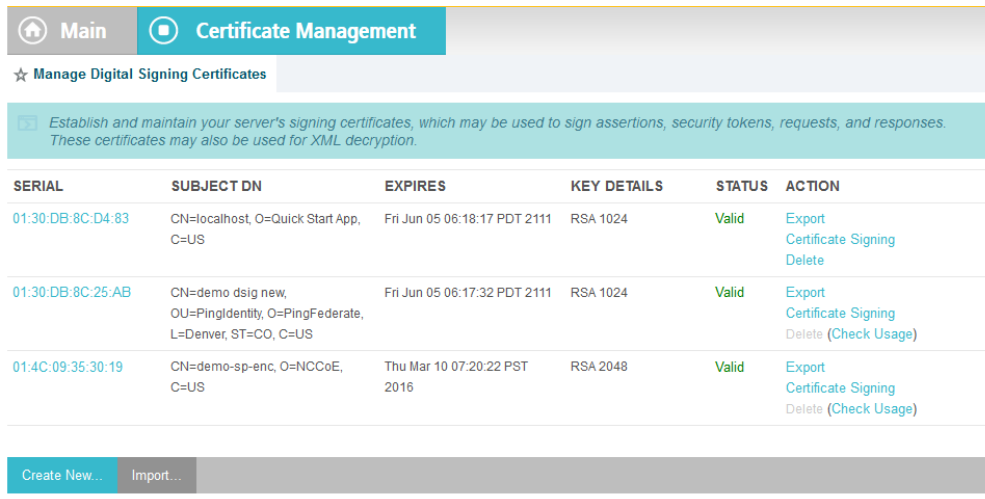
### 2383 5.3.1 Setting up the Certificate

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.

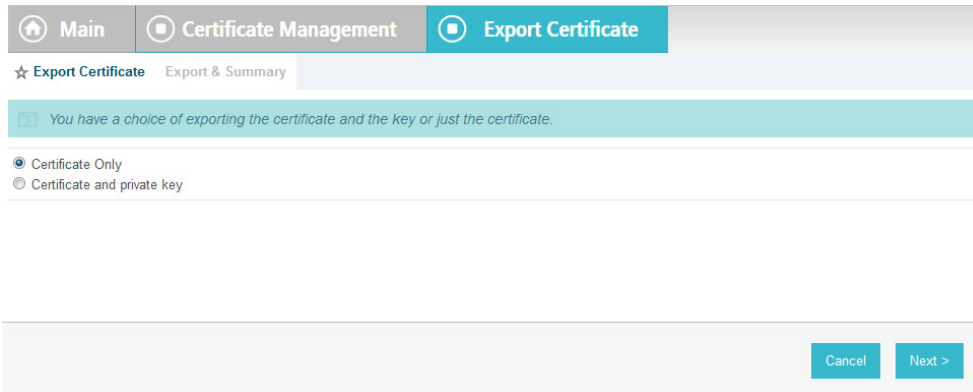
- 2386 1. Logon to the server that hosts the PingFederate service for the relying party.
- 2387 2. Launch your browser and go to: *https://<DNS\_NAME>:9999/pingfederate/app*.
- 2388 3. Replace **DNS\_NAME** with the fully qualified name of the relying party's PingFederate server  
 2389 (e.g., *https://rp.abac.test:9999/pingfederate/app*).
- 2390 4. Logon to the PingFederate application using the credentials you configured during installation.



- 2391
- 2392 5. On the Main Menu, under **CERTIFICATE MANAGEMENT**, click **Digital Signing and XML**.

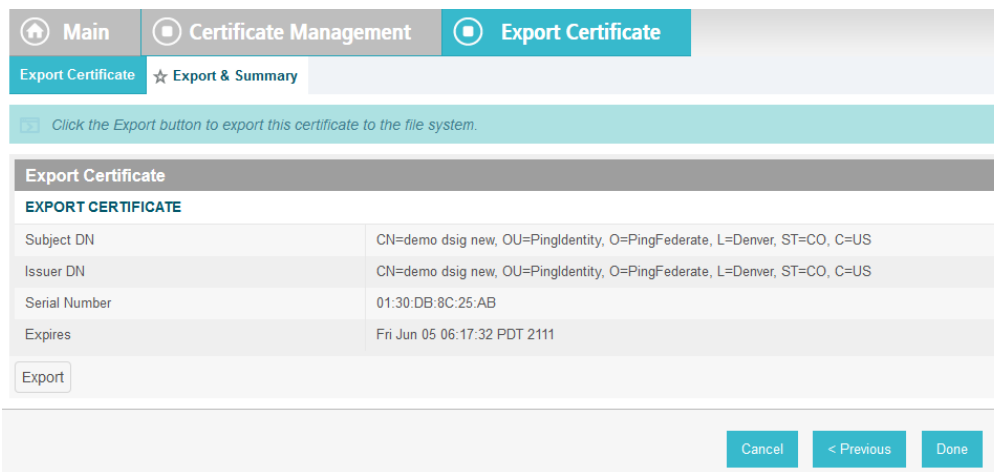


- 2393
- 2394 6. Locate the certificate that will be used to sign messages that will be sent to the SharePoint
- 2395 server. In the example screenshot above, this certificate has CN with the value **demo dsig new**.
- 2396 Click on the **Export** link for this certificate in the **ACTION** column.



2397

2398 7. Select **Certificate Only** and click **Next**.



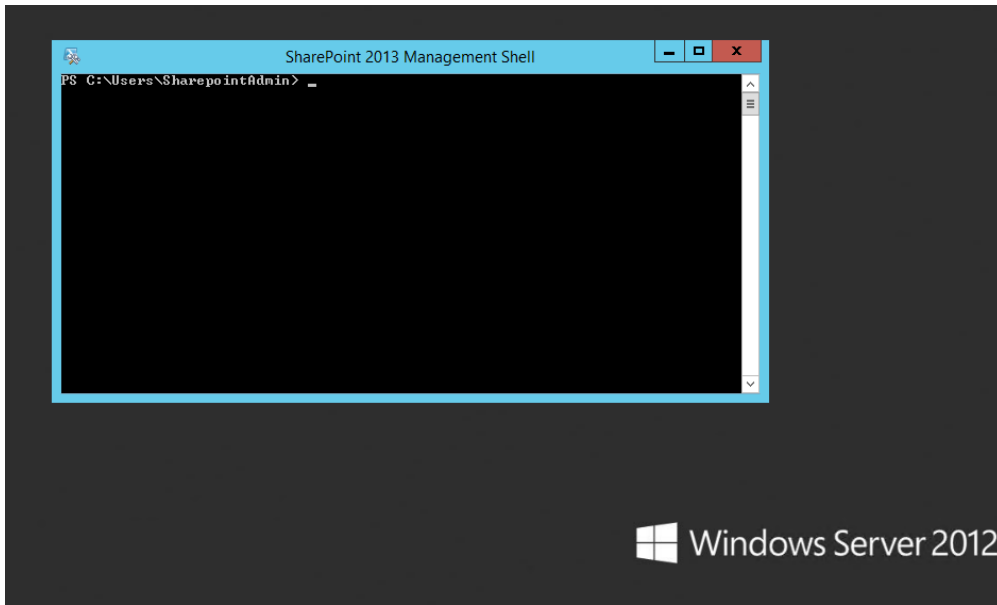
2399

2400 8. On the Export & Summary page, click the **Export** button on the left side of the page. Save the file  
 2401 to the hard drive and rename it to **federation.cer**.

2402 9. Using the SharePoint administrator credentials, logon to the server that hosts SharePoint for the  
 2403 relying party.

2404 10. Copy the **federation.cer** file to the desktop on the SharePoint server.

2405 11. Click on the **Start** menu and navigate to the SharePoint 2013 Products group. Open the  
 2406 SharePoint 2013 Management Shell.

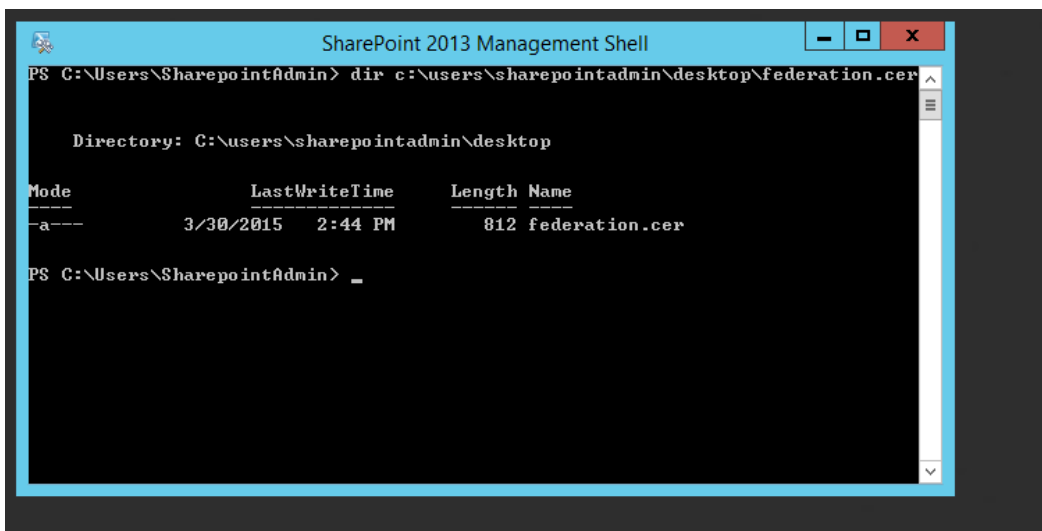


2407

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):

2415 `$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certifi-`  
2416 `cate2("C:\Users\SharePointadmin\Desktop\ federation.cer")`

2417 `New-SPTrustedRootAuthority -Name "Federated Token Signing Cert" -Certificate`  
2418 `$cert`

2419 SharePoint responds by displaying details about the imported certificate.

```

SharePoint 2013 Management Shell
PS C:\Users\SharepointAdmin> New-SPTTrustedRootAuthority -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]
      0B91B09DFE01F29E7FB659051D54C6957F9EF21E

Name
Type
  : Federated Token Signing Cert
  : Microsoft.SharePoint.Administration.SPTTrustedRootAuthority
DisplayName
Id
  : Federated Token Signing Cert
  : 2aa5a461-ae6c-4167-b939-cc319a4fc376
Status
  : Online
Parent
  : SPTTrustedRootAuthorityManager
Version
  : 140417
Properties
  : <>
Farm
  : SPSFarm Name=SharePoint_Config
UpgradedPersistedProperties
  : <>

PS C:\Users\SharepointAdmin>

```

2420

### 2421 5.3.2 Configuring the Trusted Identity Token Issuer

2422 To configure a new Trusted Identity Token Issuer, enter each of the commands displayed below the next  
 2423 paragraph into the Management Shell to configure a new Trusted Identity Token Issuer. Enter each  
 2424 command separately, and enter a Carriage Return after the command. If the command executed  
 2425 successfully, Management Shell will not provide any feedback. If an error occurs, Management Shell will  
 2426 display the error.

2427 In the example commands below, the attribute **upn** is configured. You can replace **upn** with an attribute  
 2428 that is appropriate for your environment. The realm value (e.g., **urn:SharePoint.abac.test**) must be  
 2429 identical to the realm value configured in the relying party's PingFederate Service Provider (SP)  
 2430 connection that will be configured later in this section. The signInURL should be configured with the  
 2431 PingFederate-RP WS-Federation URL (e.g., **https://rp.abac.test:9031/idp/prp.wsf**). In this example, the  
 2432 name given to this new token issuer in SharePoint is **Federated Logon from Identity Provider**. The issuer  
 2433 name will be displayed in SharePoint administration screens and to the end user on the Sign On screen.

```

2434 $claimmap = New-SPClaimTypeMapping -IncomingClaimType "http://sche-
2435 mas.xmlsoap.org/ws/2005/05/identity/claims/upn" -IncomingClaimTypeDisplayName
2436 "upn" -SameAsIncoming

2437 $realm = "urn:SharePoint.abac.test"

2438 $signInURL = https://rp.abac.test:9031/idp/prp.wsf

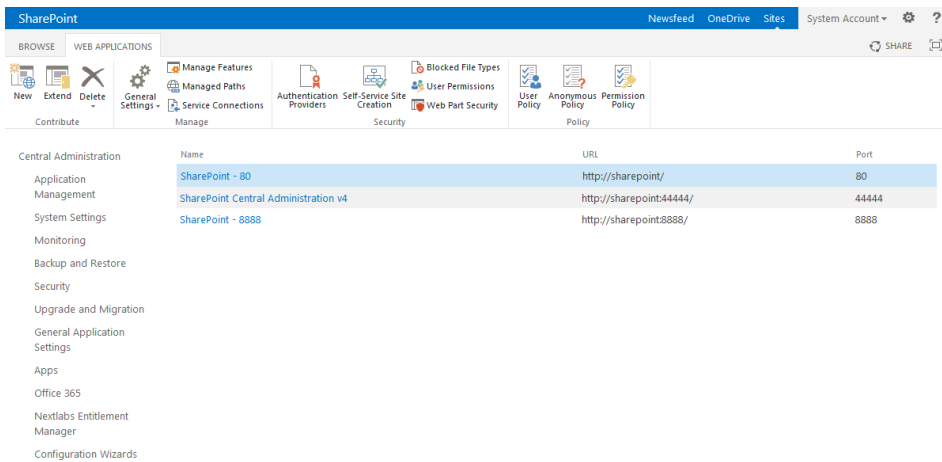
2439 $ap = New-SPTTrustedIdentityTokenIssuer -Name "Federated Logon from Identity
2440 Provider" -Description "Federated Logon" -realm $realm -ImportTrustCertificate
2441 $cert -ClaimsMappings $claimmap -SignInUrl $signInURL -IdentifierClaim $claim-
2442 map.InputClaimType

```

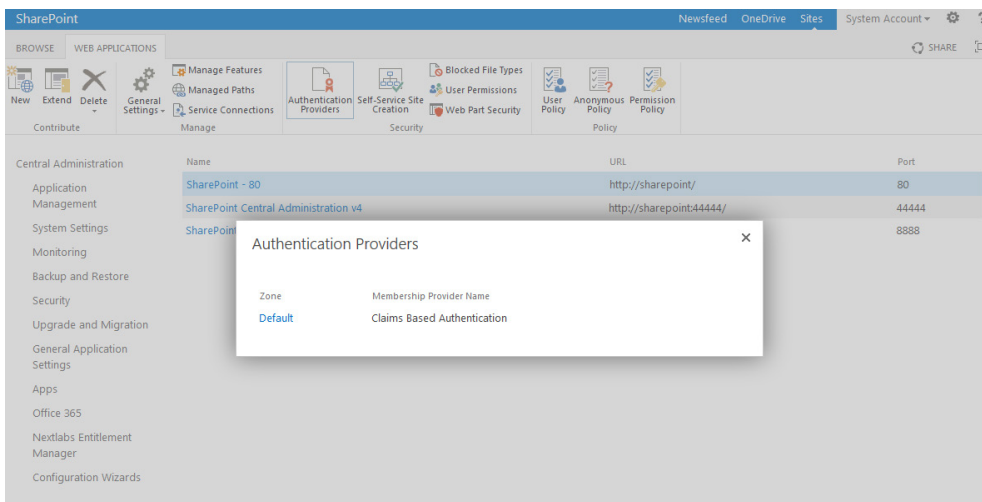
2443 **5.3.3 Configuring the Token Issuer as a Sign On Option**

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.



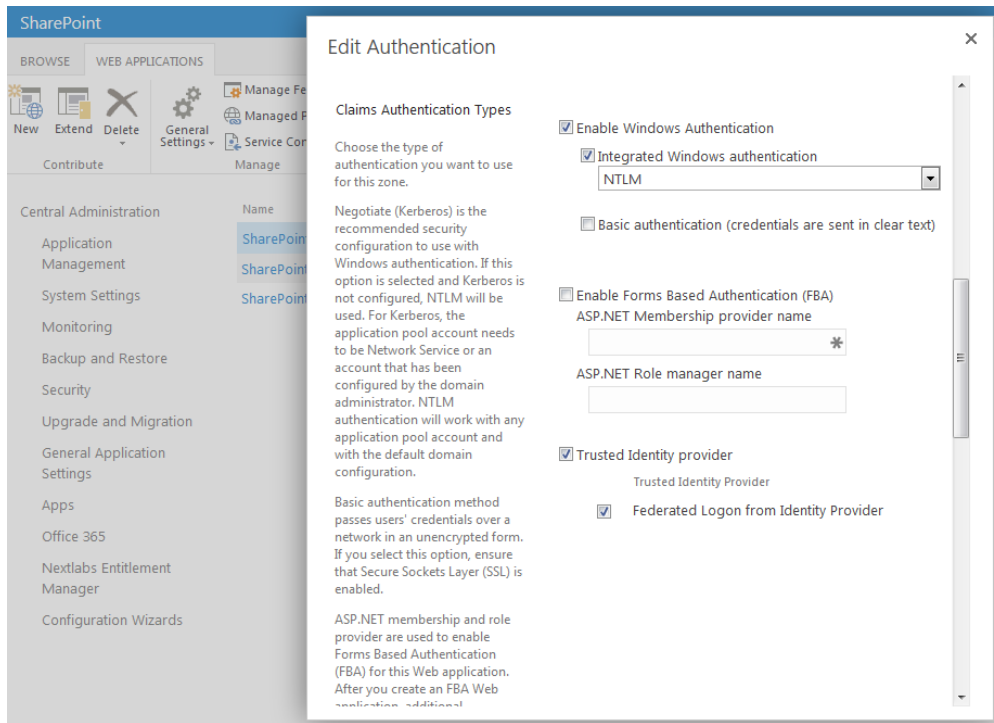
- 2452
- 2453 5. Click on the **Authentication Providers** button at the top of the page.



- 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).

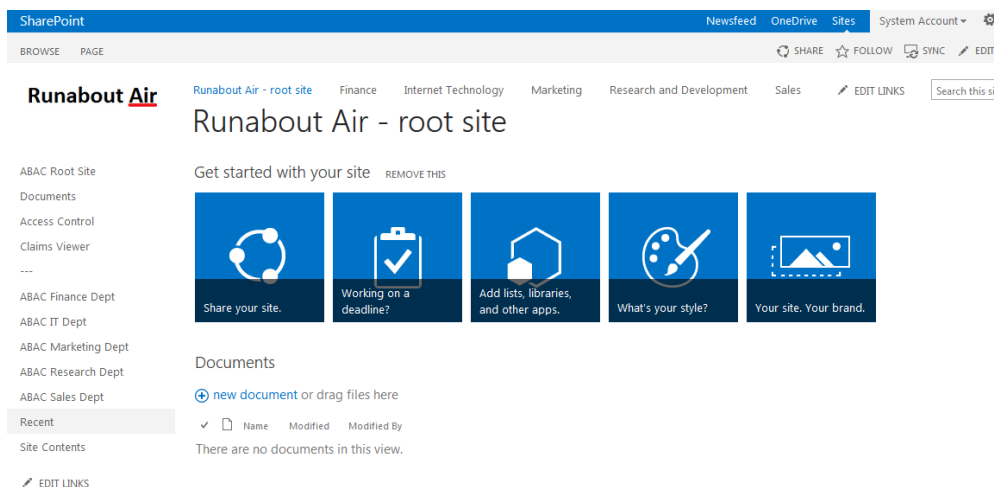


- 2460  
 2461 9. Scroll to the bottom of the page and click **Save**.

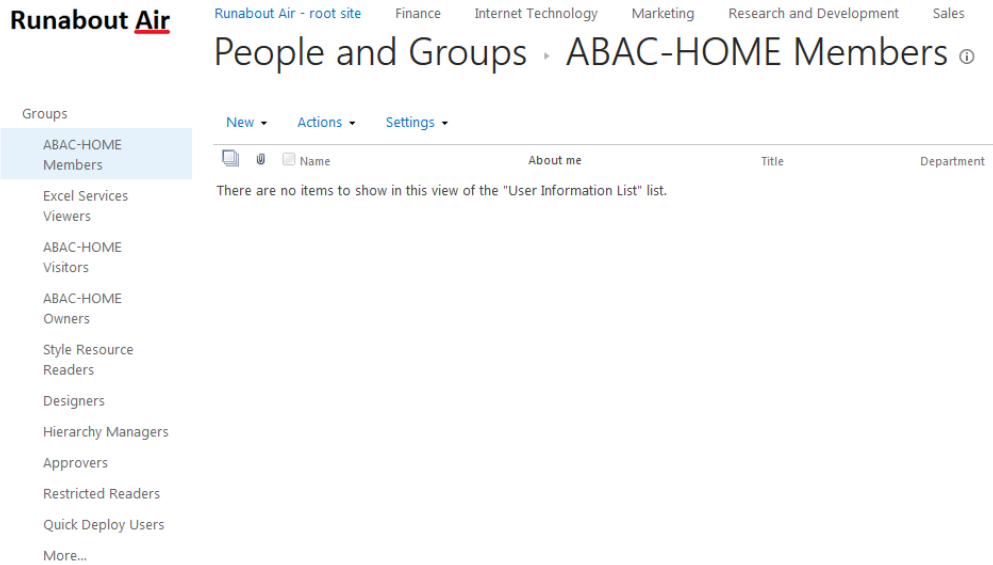
### 5.3.4 Configuring the Access Control Rule on SharePoint

2462 After configuring the token issuer as a Sign On option for SharePoint, configure the access control rule  
 2463 on the SharePoint site that is necessary for federated users to be able to access the site.  
 2464

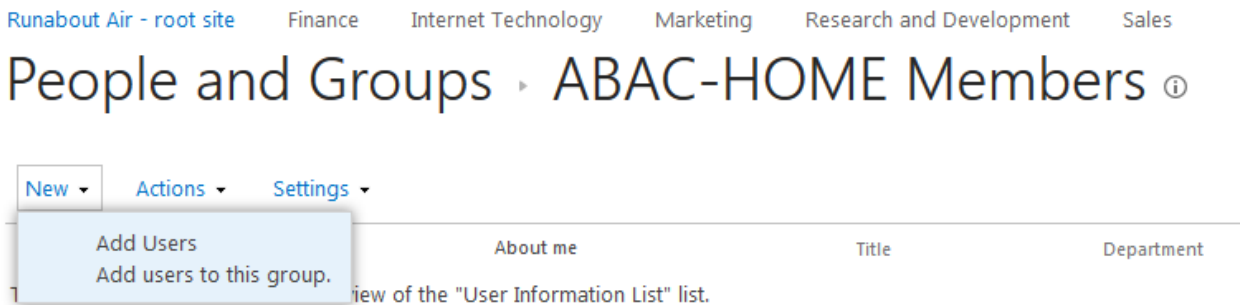
- 2465 1. Logon to the relying party's SharePoint site (e.g., *https://SharePoint.abac.test*) using the  
 2466 credentials of the SharePoint administrator.  
 2467 2. Select **Windows Authentication** in the Sign On screen.



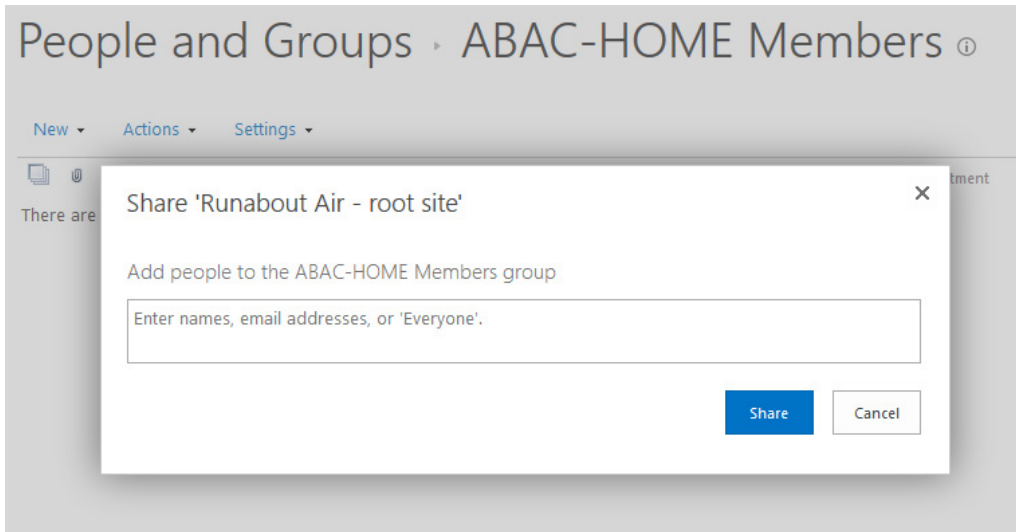
- 2469 3. Click the gear icon at the top right corner of the page and select the **Site Settings** link.
- 2470 4. On the Site Settings screen, in the **Users and Permissions** group, click **People and Groups**.
- 2471 5. Under the **Groups** heading on the left pane, click on the **HOME Members** group.



- 2472
- 2473 6. Under the page title, click on the **New** link and select the **Add Users** option from the popup
- 2474 menu.



2475



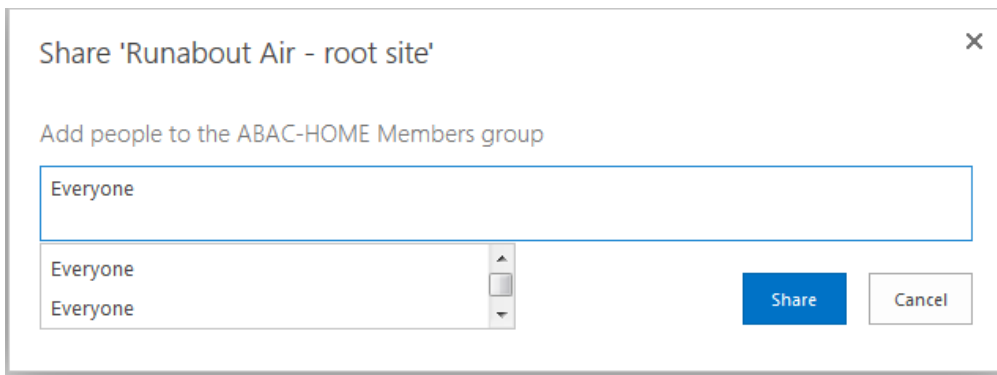
2476

2477

7. On the Share popup screen, enter **Everyone** in the text field.

2478

SharePoint will display a List Box underneath the text field.

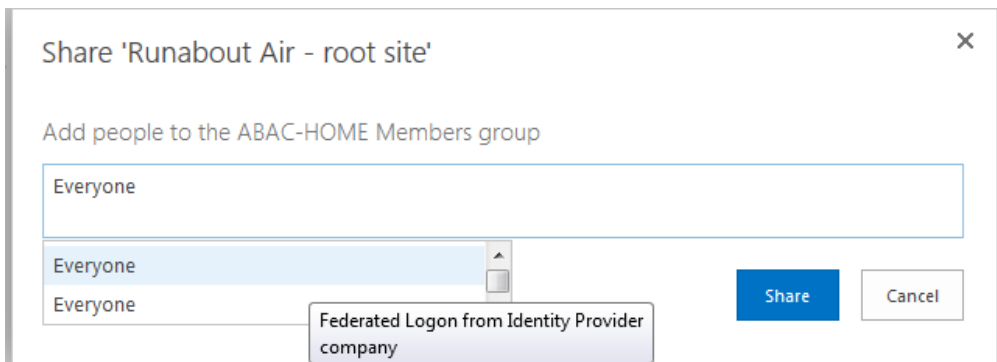


2479

2480

The list will contain multiple entries for the same value of **Everyone**. If you place your cursor over an entry in the list SharePoint will display details about the entry.

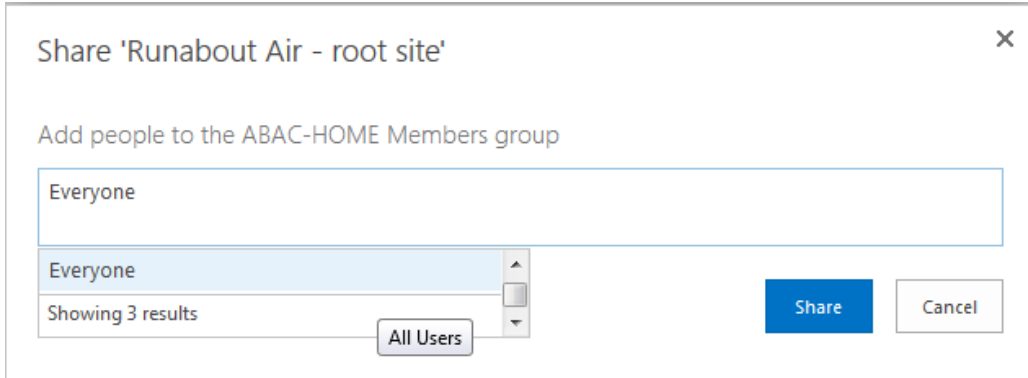
2481



2482

2483

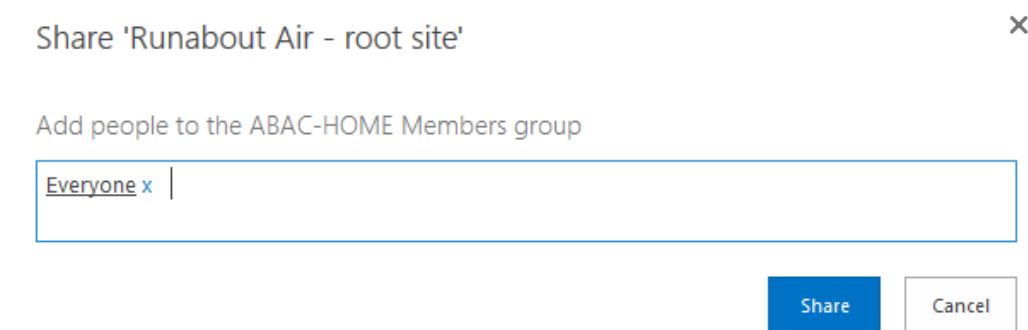
8. Locate the entry that is associated with **All Users**.



2484

2485

9. Click on the entry associated with **All Users**.



2486

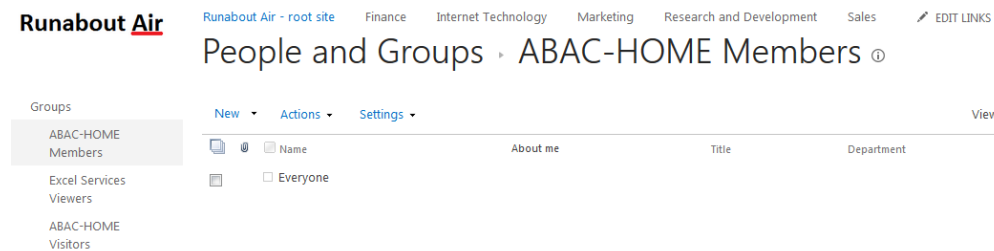
2487

10. Click **Share**.

2488

2489

When you go back to the People and Groups screen, you should see **Everyone** listed for the Home Members group.



2490

2491

2492

2493

### 5.3.5 Functional Test of the Federated Logon at the Resource Provider

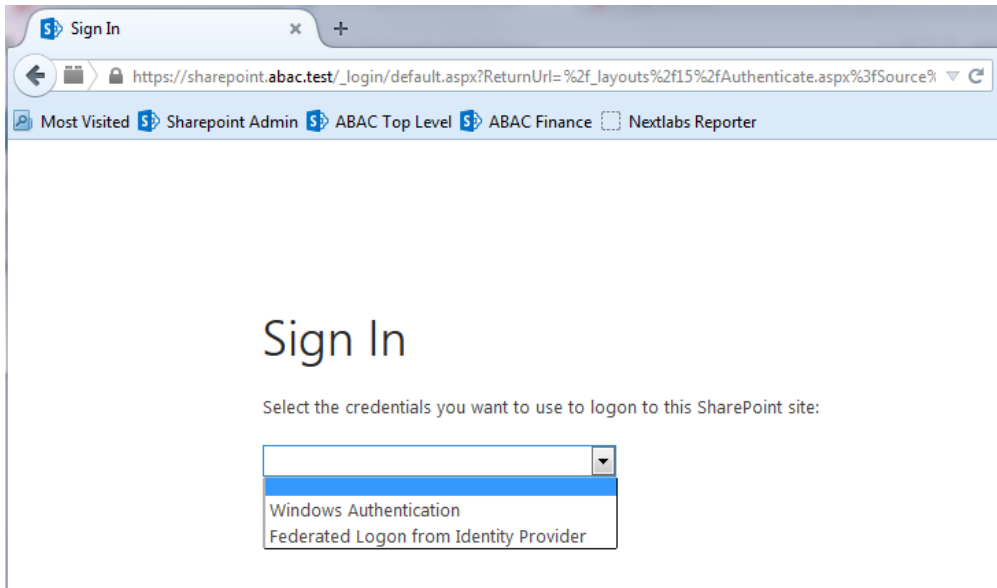
1. Launch a new browser window and go to the relying party's SharePoint site (e.g., <https://SharePoint.abac.test>).

2494

2495

2496

Expected Result: You should see two logon options in the dropdown box. One of the options should be the name of the new trusted token issuer that was configured in the previous section (e.g., Federated Logon from Identity Provider).

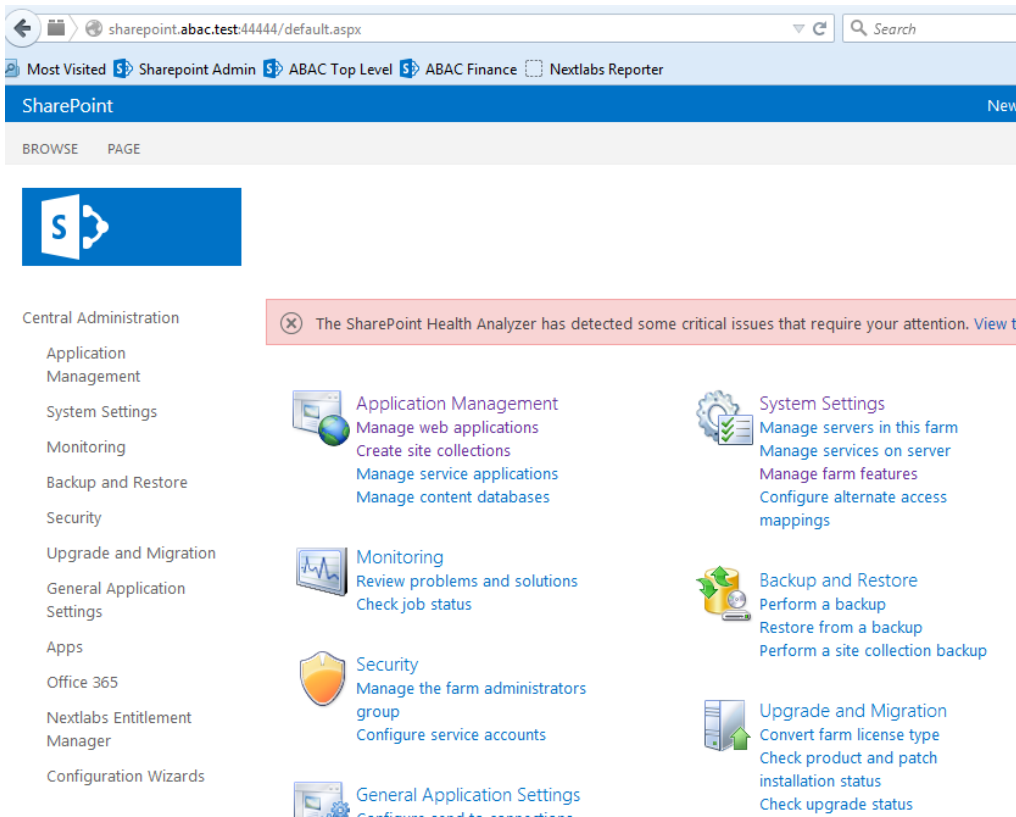


2497

2498 Next you will verify that SharePoint is configured to read the **upn** attribute that was configured for the  
2499 federated logon.

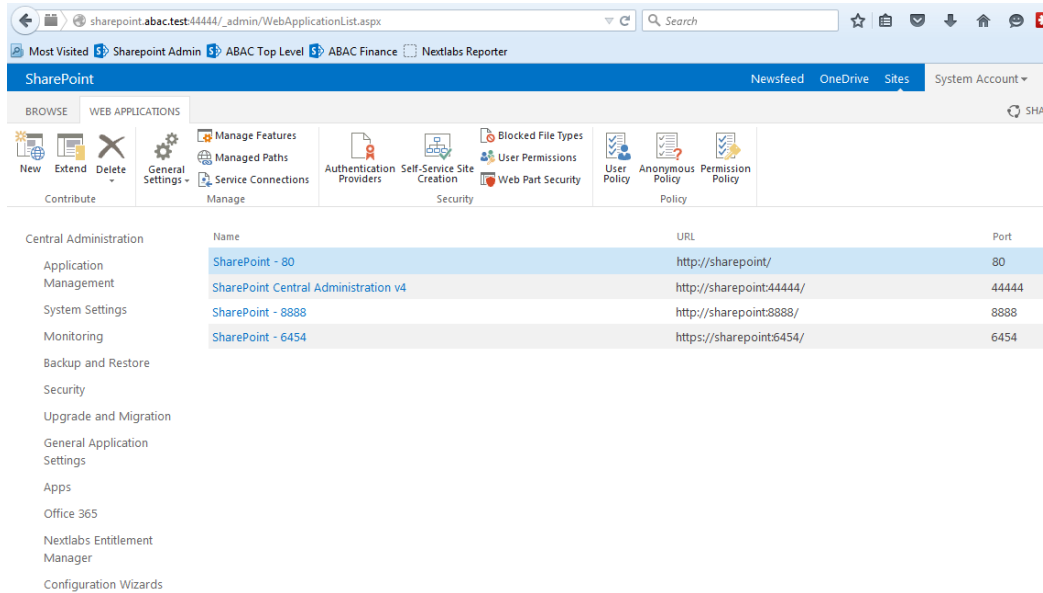
2500 2. Launch your browser and go the SharePoint central administration page (e.g.,  
2501 <http://SharePoint.abac.test:44444/default.aspx>).

2502 3. Logon using the credentials of the SharePoint administrator.

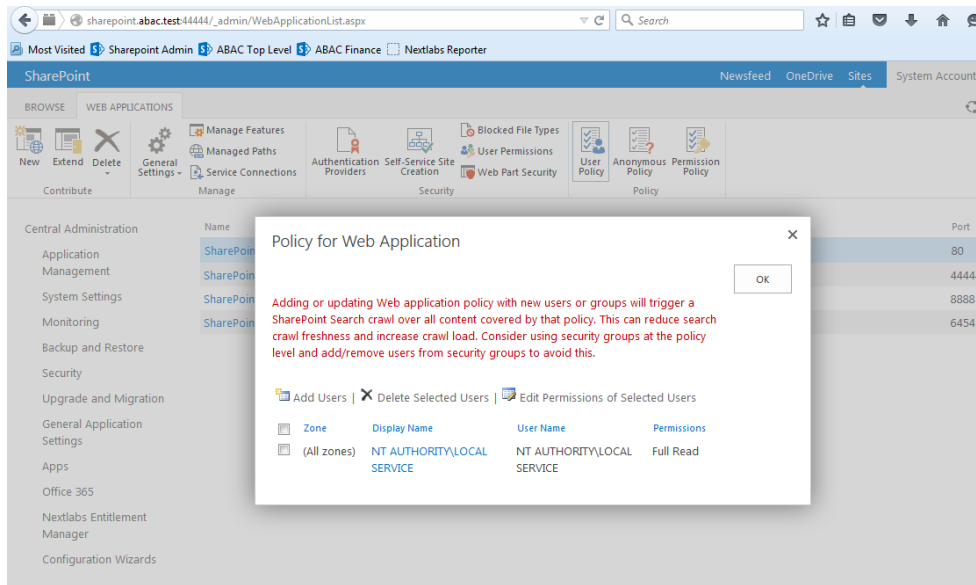


2503

- 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.,
- 2506 **SharePoint – 80**). SharePoint will highlight the web application row that you clicked on.



- 2507
- 2508 6. Click on the **User Policy** button.



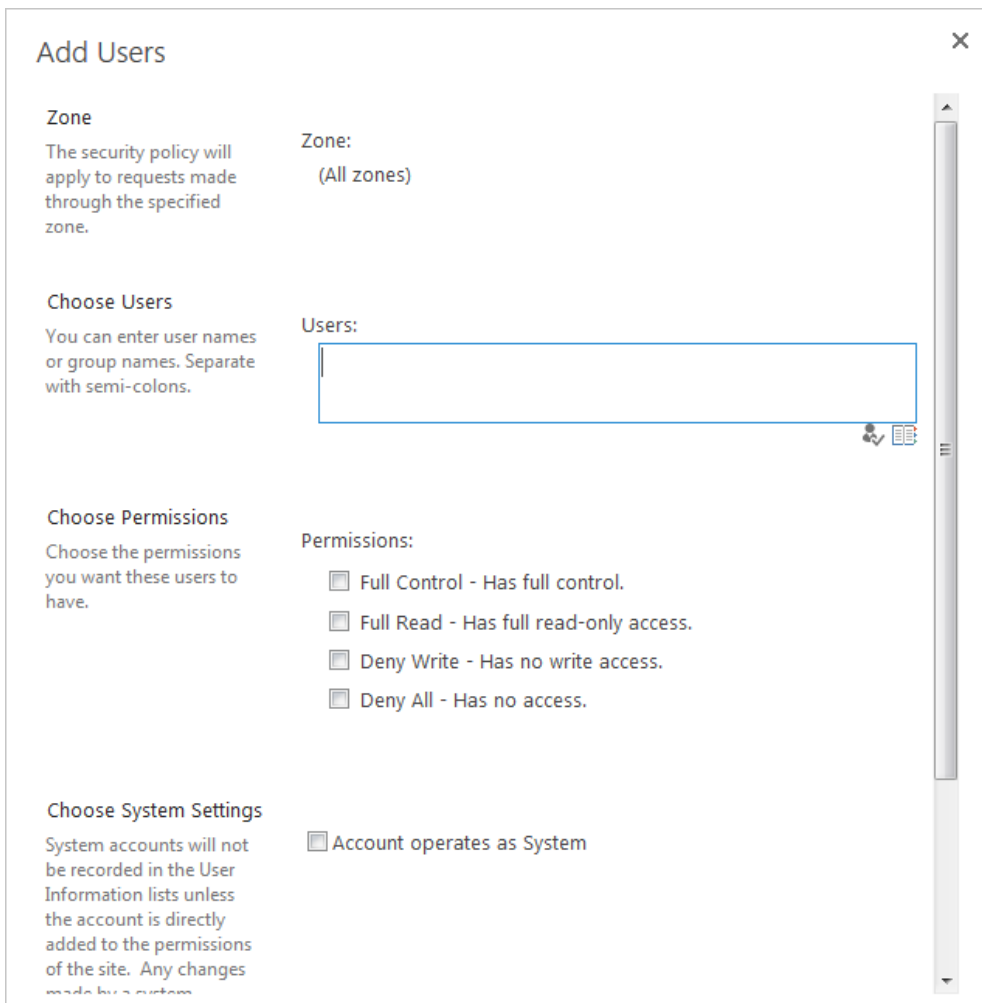
- 2509
- 2510 7. Click **Add Users**.



2511

2512

8. Click **Next**.



2513

2514

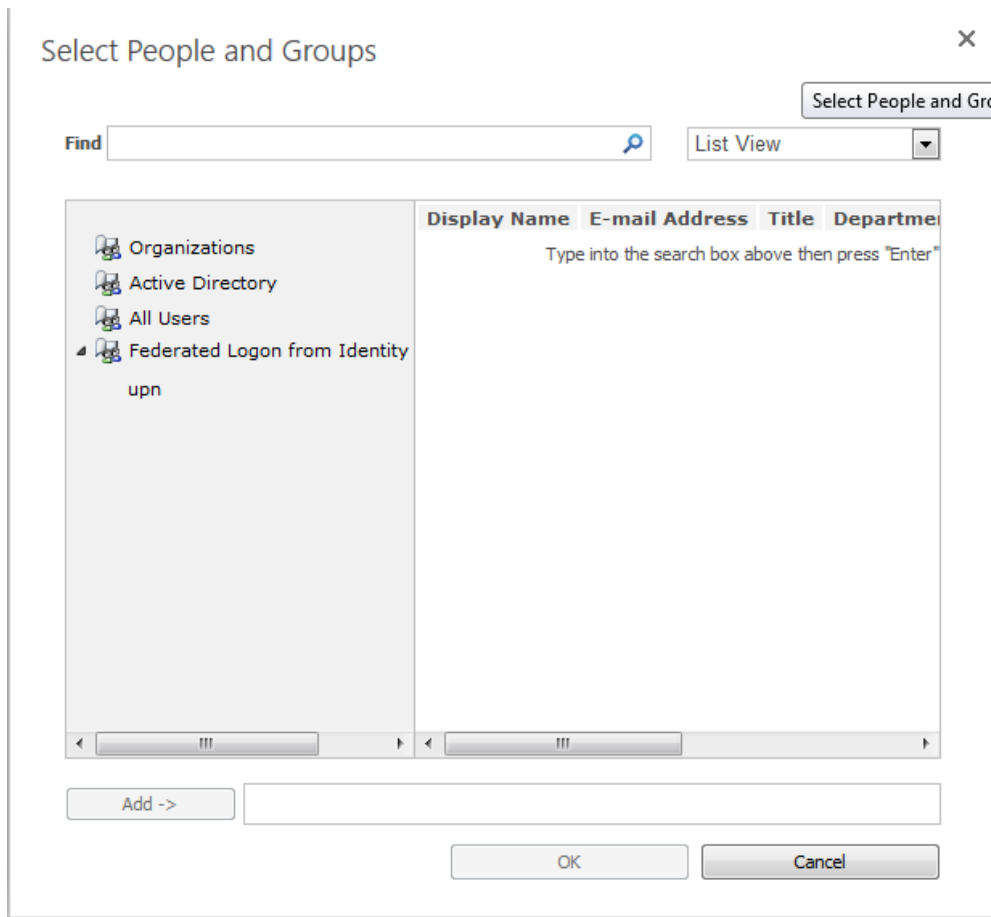
9. On the Add Users screen, click the small browse icon (looks like a book) under the Users field.

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.



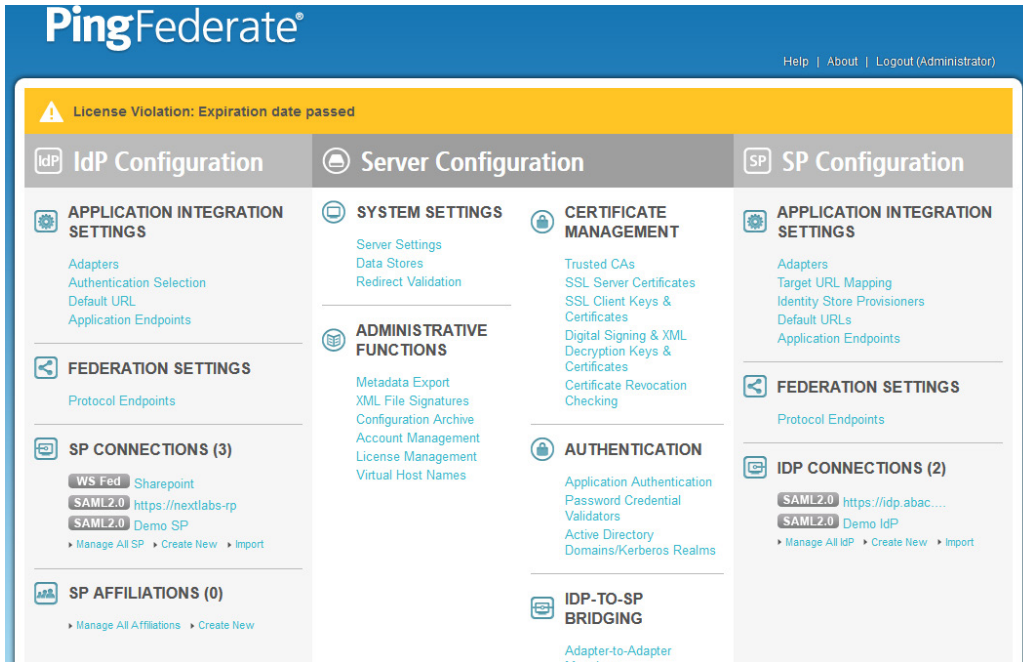
2519

## 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.
- 2524 2. Launch your browser and go to: *https://<DNS\_NAME>:9999/pingfederate/app*. Replace  
 2525 DNS\_NAME with the fully qualified name of the relying party's PingFederate server (e.g.,  
 2526 *https://rp.abac.test:9999/pingfederate/app*). Logon to the PingFederate application using the  
 2527 credentials you configured during installation.



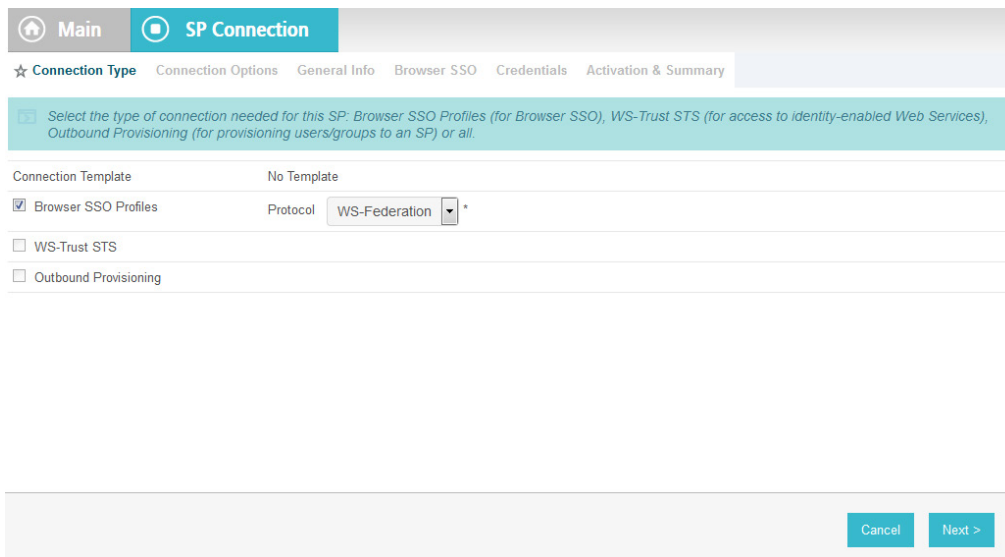


2528

2529

2530

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**.



2531

2532

4. Click **Next**. On the Connection Options screen, select **Browser SSO**.

2533

2534

2535

2536

5. Click **Next**. On the General Info screen, for the Partner’s Realm field, enter the name of the Resource Provider’s (SharePoint) realm (e.g., urn:SharePoint.abac.test). Keep a copy of the realm name because it will be used in a configuration of SharePoint later in the guide.

2537

2538

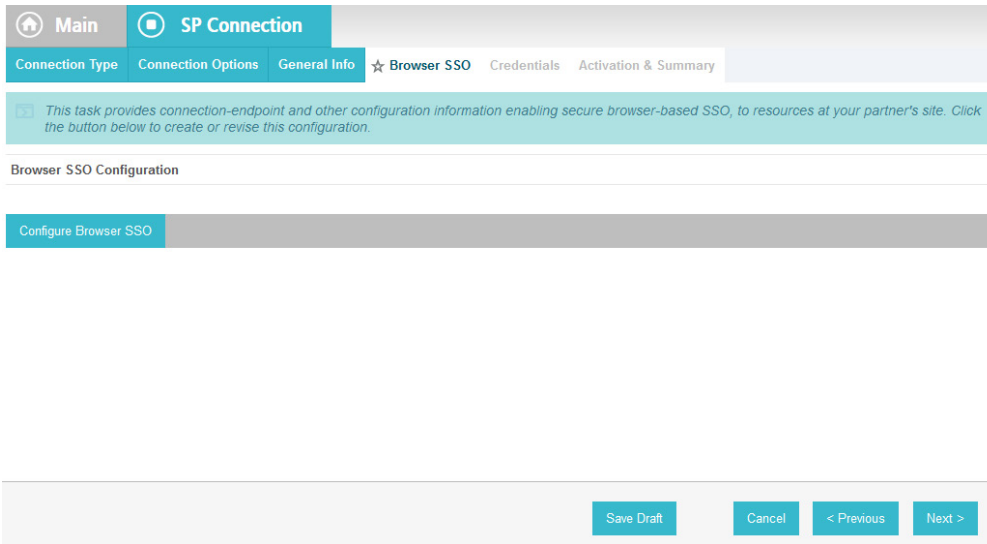
2539

6. Enter a unique name for this new PingFederate configuration in the Connection Name field. For 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*).

2540

2541

7. Click **Next**.

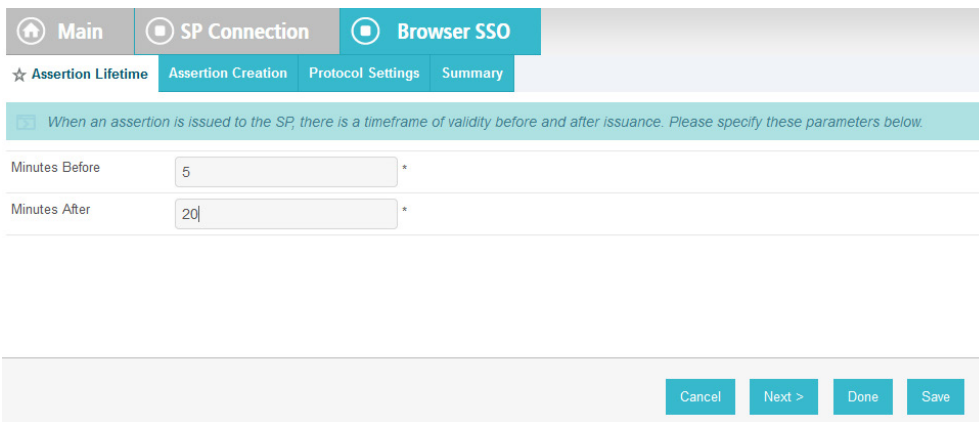


2542

2543

2544

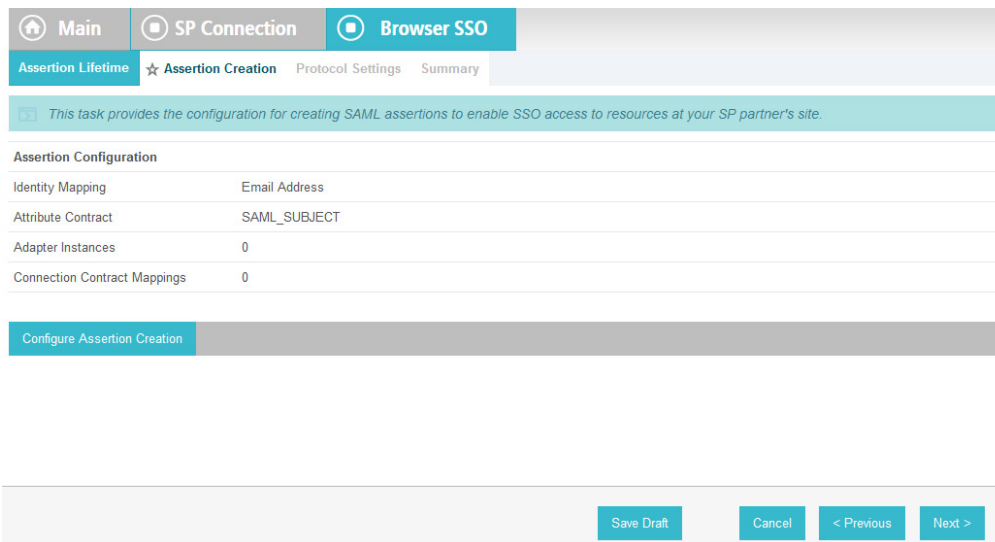
8. On the Browser SSO screen, click **Configure Browser SSO**. On the Assertion Lifetime screen, enter a value of 20 for the Minutes After field.



2545

2546

9. Click **Next**.



2547

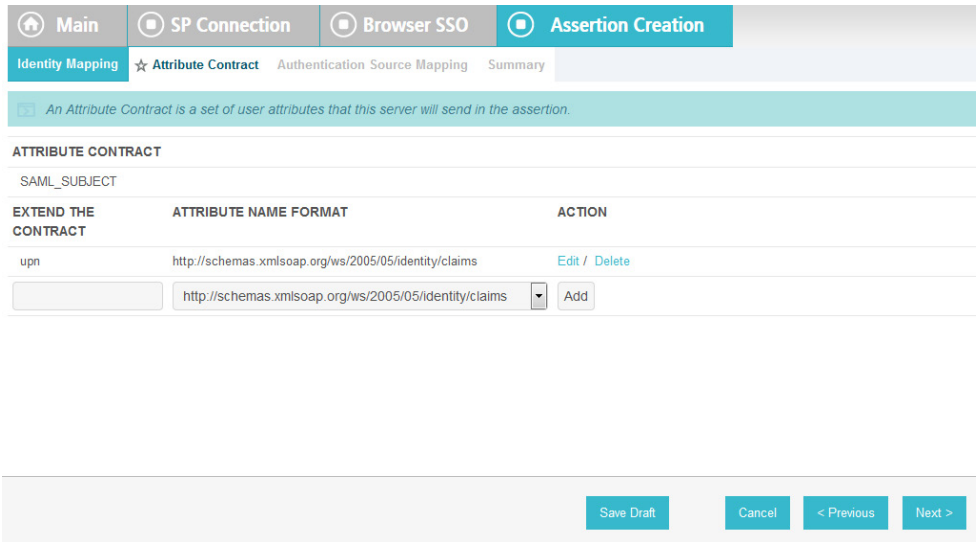
- 2548 10. On the Assertion Creation screen, click **Configure Assertion Creation**. On the Identity Mapping  
 2549 screen, select **User Principal Name**.

The screenshot shows a web interface with a breadcrumb trail: Main > SP Connection > Browser SSO > Assertion Creation. Below this is a sub-breadcrumb trail: Identity Mapping > Attribute Contract > Authentication Source Mapping > Summary. A teal instruction box reads: "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." Below this are three radio button options: "Email Address", "User Principal Name" (which is selected), and "Common Name". At the bottom right of the form are three buttons: "Save Draft", "Cancel", and "Next >".

- 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.

The screenshot shows the same breadcrumb trail as the previous screen, but the sub-breadcrumb trail is: Identity Mapping > Attribute Contract > Authentication Source Mapping > Summary. A teal instruction box reads: "An Attribute Contract is a set of user attributes that this server will send in the assertion." Below this is the "ATTRIBUTE CONTRACT" section with "SAML\_SUBJECT" set to "SAML\_SUBJECT". A table titled "EXTEND THE CONTRACT" has three columns: "EXTEND THE CONTRACT", "ATTRIBUTE NAME FORMAT", and "ACTION". The first row contains the text "upn" in the first column, "http://schemas.xmlsoap.org/ws/2005/05/identity/claims" in the second column (with a dropdown arrow), and "Add" in the third column. At the bottom right of the form are four buttons: "Save Draft", "Cancel", "< Previous", and "Next >".

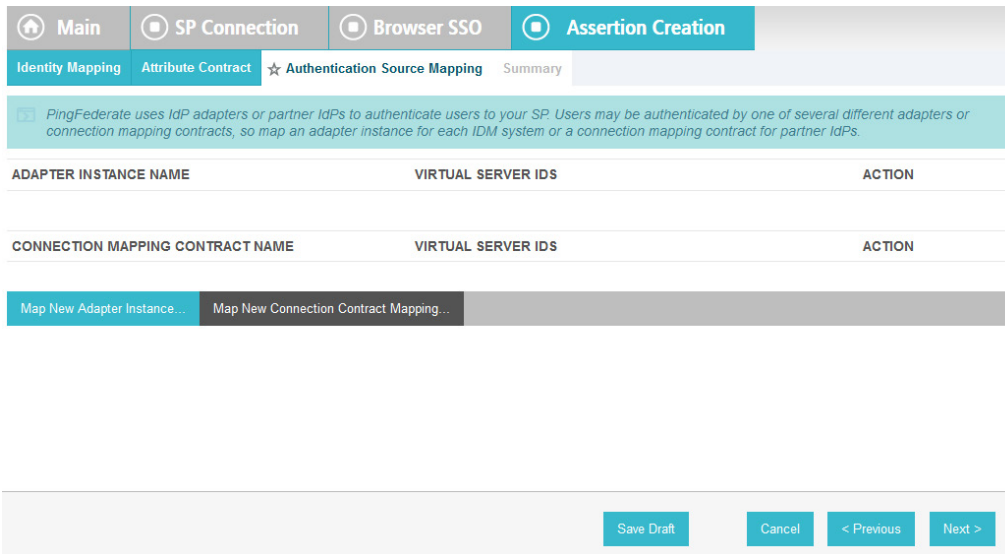
- 2554  
 2555 12. Click **Add**.



2556

2557

13. Click **Next**.



2558

2559

2560

2561

2562

14. On the Authentication Source Mapping screen, click **Map New Connection Contract Mapping**. On the Connection Contract Mapping screen, for the CONNECTION MAPPING CONTRACT field, select the name of the contract with the identity provider that was configured in a [Section 3](#) (e.g., SharePoint 2013).

2563

2564

2565

15. Click **Next**. On the Assertion Mapping screen, select **Use only the Connection Mapping Contract values in the SAML assertion**.

2566

2567

16. Click **Next**.

2568

2569 17. On the Attribute Contract Fulfillment screen, click **Next**.

2570

2571 18. On the Issuance Criteria screen, click **Next**.

2572

2573 19. On the Summary screen, click **Next**.

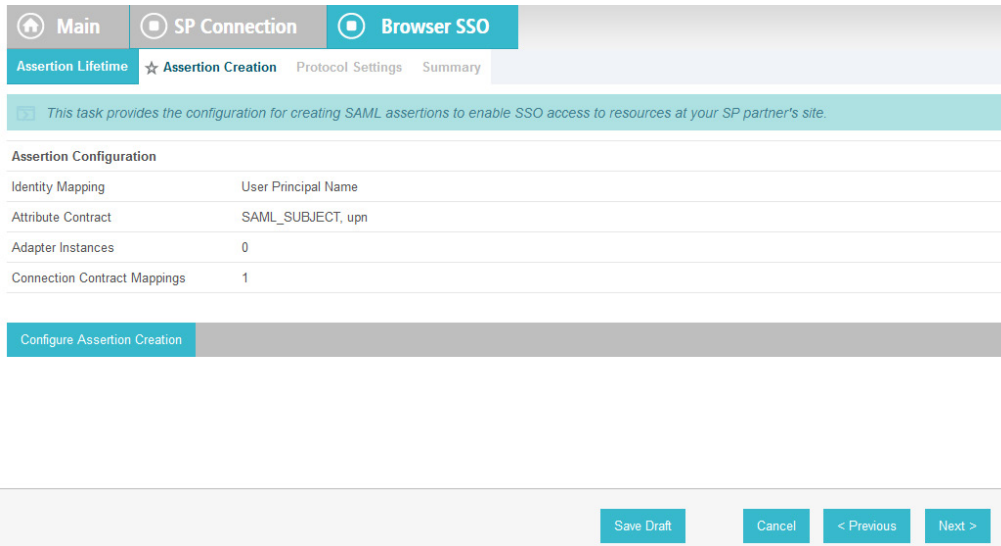
2574

2575 20. On the Authentication Source Mapping screen, click **Next**.

2576

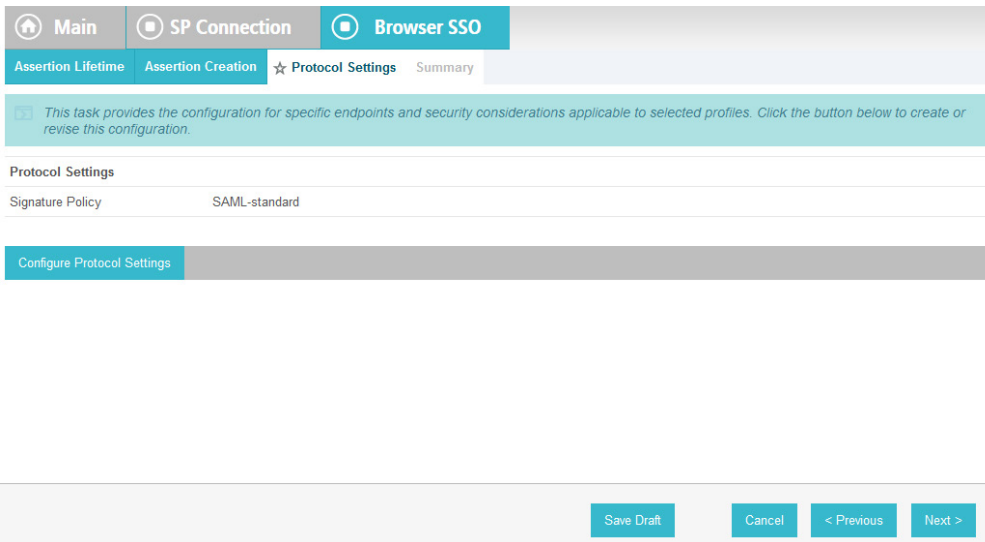
2577 21. On the Summary screen, click **Done**.





2578

2579 22. On the Assertion Creation screen, click **Next**.



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

Require HTTPS	Valid Domain Name (leading wildcard *. allowed)	Valid Path (leave blank to allow any path)	Allow Any Query/Fragment	Action
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	Add

2592

2593

24. Click **Next**.

Protocol Settings
<b>SERVICE URL</b>
Endpoint URL: /_trust/

2594

2595

25. On the Summary screen, click **Done**.

2596

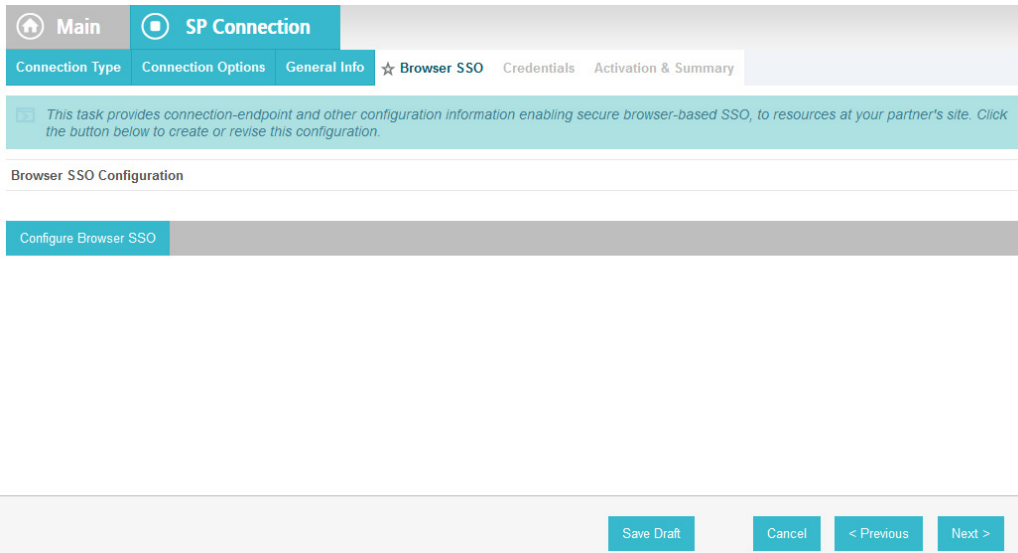
2597

26. On the Protocol Settings screen, click **Next**.

2598

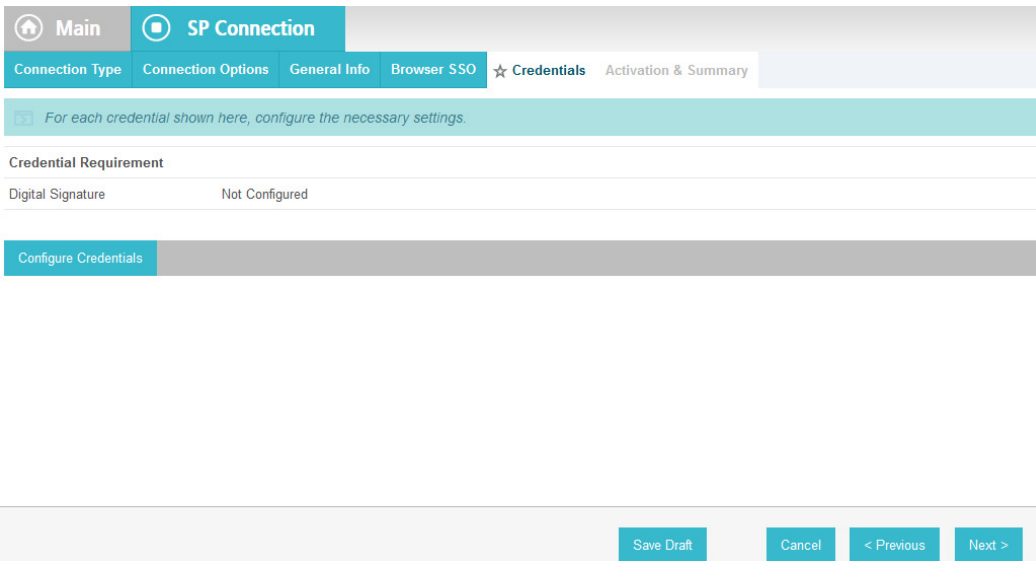
2599

27. On the Summary screen, click **Done**.



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**.

Main SP Connection **Credentials**

☆ Digital Signature Settings Summary

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.

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

Include the raw key in the signature <KeyValue> element.

Signing Algorithm RSA SHA256

Manage Certificates...

Save Draft Cancel Next >

2605

2606 30. Click **Next**.

Main SP Connection **Credentials**

Digital Signature Settings ☆ Summary

Summary information for your Credentials configuration. Click a heading link to edit a configuration setting.

**Credentials**

**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

Save Draft Cancel < Previous Done

2607

2608 31. On the Summary screen, click **Done**.

Main | **SP Connection**

Connection Type | Connection Options | General Info | Browser SSO | **Credentials** | Activation & Summary

For each credential shown here, configure the necessary settings.

**Credential Requirement**

Digital Signature: CN=demo dsig new

Configure Credentials

Save Draft | Cancel | < Previous | Next >

2609

2610

32. On the Credentials screen, click **Next**.

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/

**Credentials**

**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

Cancel | < Previous | Save

2611

2612

2613

On the Activation and Summary screen, select **Active** for the Connection Status field and Click **Save** to complete the configuration.

## 2614 5.5 Functional Test of All Configurations for Section 5

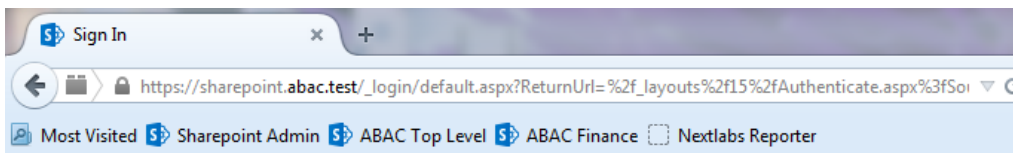
2615 The instructions in this section will perform an integrated test all of the configurations in Section 5.

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 Firefox 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

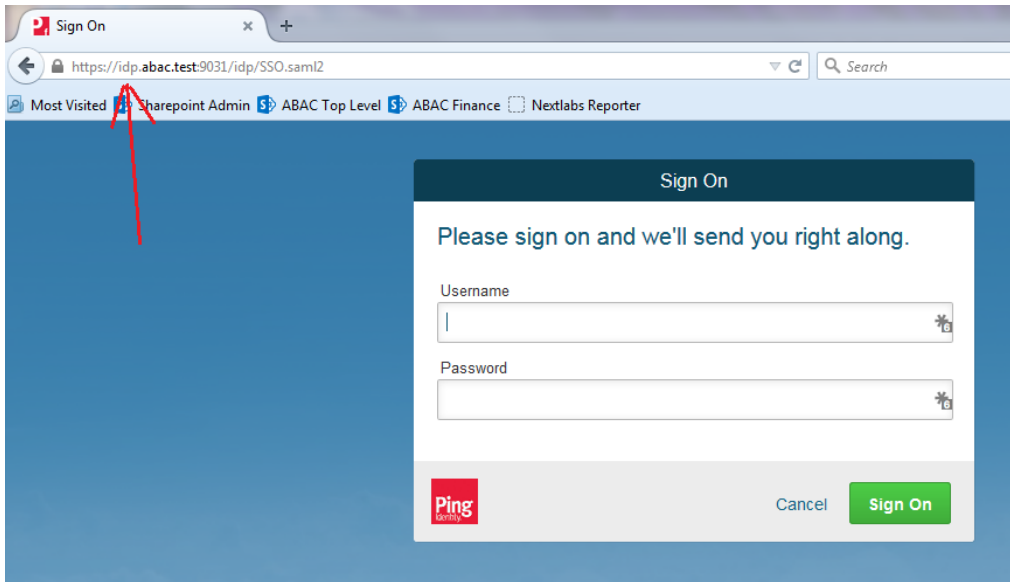
Select the credentials you want to use to logon to this SharePoint site:

- Windows Authentication
- Federated Logon from Identity Provider

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).

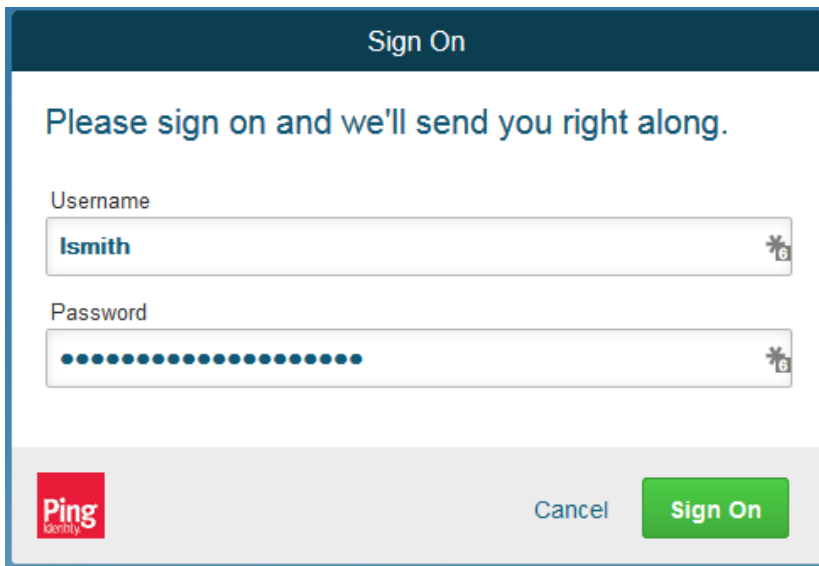


2630

2631

2632

4. Enter the Username and Password of the Active Directory account created earlier in this guide (e.g., "lsmith").



2633

2634

2635

5. Click **Sign On**. On the RSA Adaptive Authentication screen, enter the SMS validation code received on your mobile phone. Click **Next**.

2636

2637

2638

2639

2640

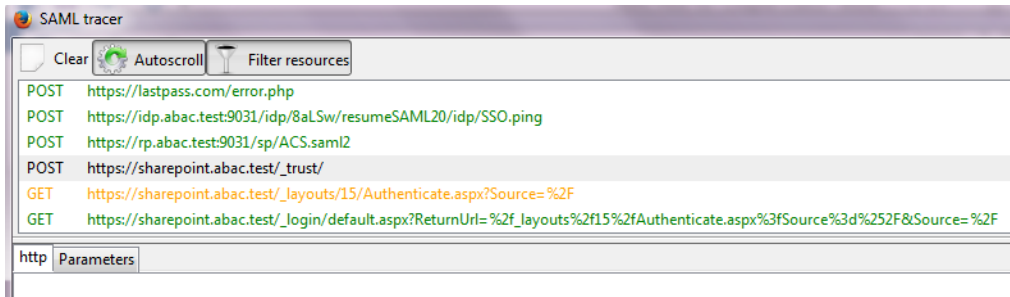
2641

2642

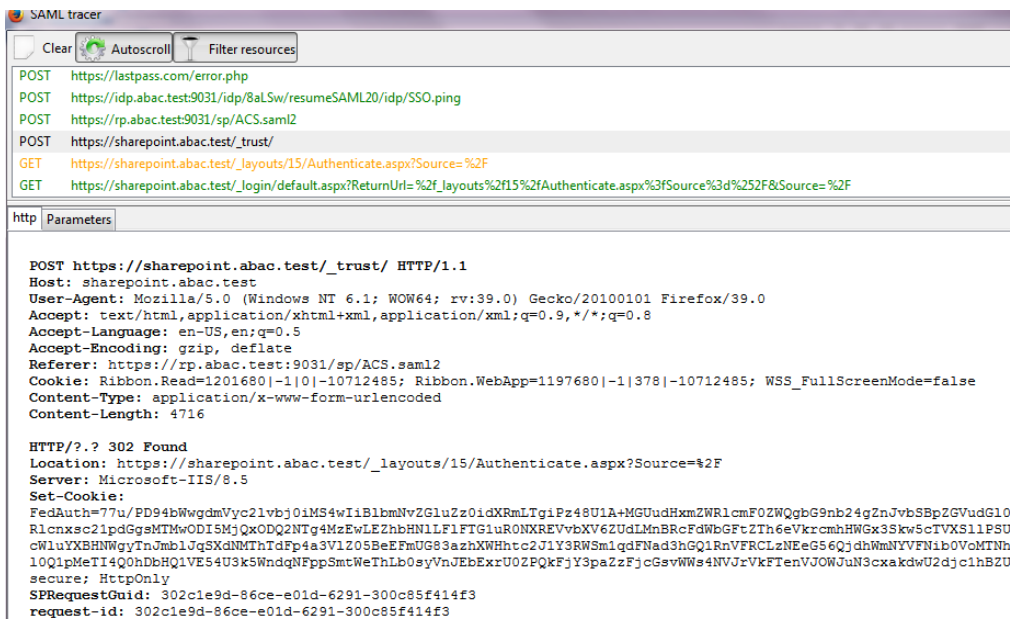
Note: Once authenticated at the identity provider, your browser should automatically redirect to the PingFederate-RP (e.g., rp.abac.test) and then to the relying party's SharePoint (SharePoint.abac.test) site. Depending on the processing time of the servers in your environment, and other factors, it may take several seconds before your browser arrives back at the SharePoint site. The identity provider will redirect your browser to the PingFederate-RP first, and then the PingFederate-RP will redirect your browser to the SharePoint site, however you may not notice all of this activity if it happens quickly.



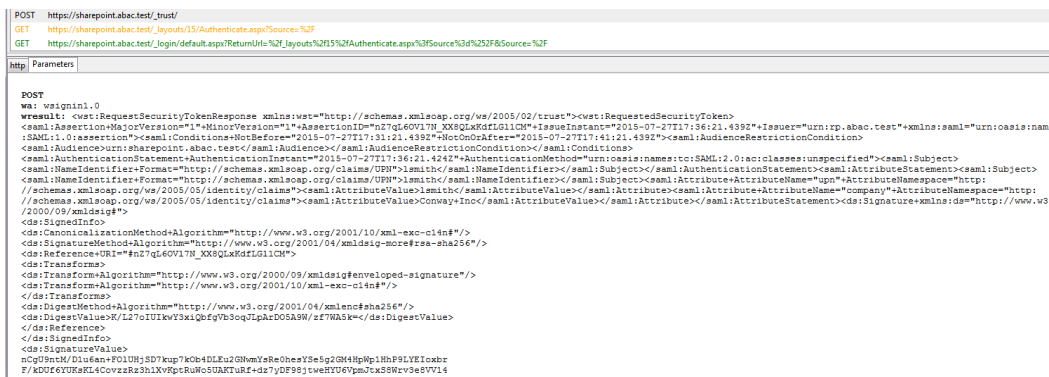
2643 Expected Result: Go back to the SAML tracer window. Scroll down the list of messages at the top  
 2644 and ensure there is a POST message to the SharePoint server to the \_trust URL (e.g., POST  
 2645 [https://SharePoint.abac.test/\\_trust/](https://SharePoint.abac.test/_trust/)).



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.

```

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="nZ7QL60V17N_XX8QLXKDFLG11CM"+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"+NotOnOrAfter="2015-07-
27T17:41:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint.abac.test</saml:Audience></saml:AudienceRestri
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:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">ismith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:A
ttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">ismith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>ismith</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><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="#nZ7QL60V17N_XX8QLXKDFLG11CM">
<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/xmenc#sha256"/>
<ds:DigestValue>K/L270iUikwY3xiQbfgyb3oqJLPArD05A9w/Zf7WASk=</ds:DigestValue>

```

2654

2655

9. Scroll down the SAML message and locate the AttributeStatement node and sub-nodes.

```

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="nZ7QL60V17N_XX8QLXKDFLG11CM"+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"+NotOnOrAfter="2015-07-
27T17:41:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint.abac.test</saml:Audience></saml:AudienceRestri
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:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">ismith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:A
ttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">ismith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>ismith</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><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="#nZ7QL60V17N_XX8QLXKDFLG11CM">

```

2656

2657

2658

2659

10. For the AttributeStatement node and sub-nodes, enter some carriage returns before each XML tag to make it easier to examine the data. The goal is to be able to easily examine the Attribute nodes within the AttributeStatement node.

```

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="nZ7QL60V17N_XX8QLXKDFLG11CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp.abac.test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><saml:Conditions+
07-27T17:31:21.439Z"+NotOnOrAfter="2015-07-
27T17:41:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint.abac.test</saml:Audience></saml:AudienceRestri
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:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">ismith</saml:NameIdentifier></saml:Subject></saml:Authentication
Statement><saml:AttributeStatement>
<saml:Subject>
<saml:NameIdentifier+Format="http://schemas.xmlsoap.org/claims/UPN">ismith</saml:NameIdentifier></saml:Subject>
<saml:Attribute AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
<saml:AttributeValue>ismith</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>

```

2660

2661

2662

2663

2664

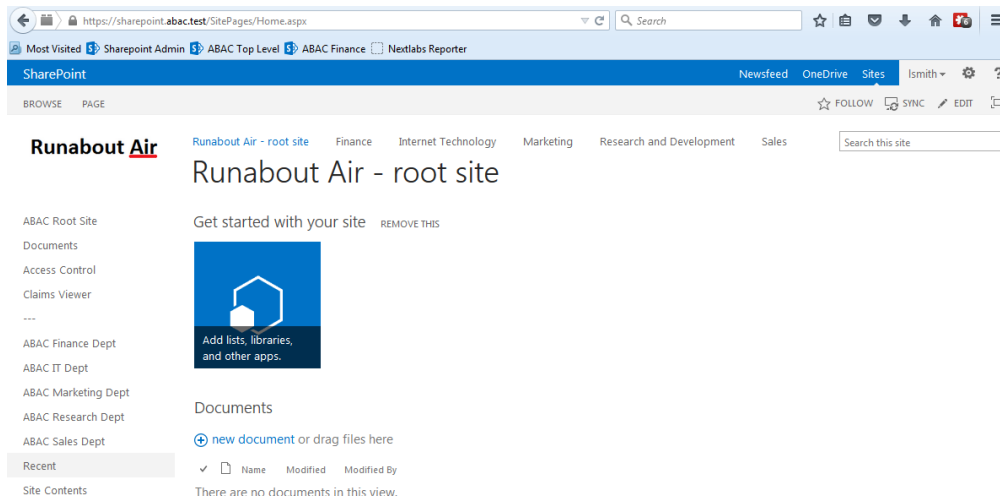
Expected Result: Within the AttributeStatement node, there should be an Attribute sub-node. The Attribute sub-node should have an AttributeName value of “upn”. The AttributeNamespace value should be *http://schemas.xmlsoap.org/ws/2005/05/identity/claims*. There should be an AttributeValue sub-node and it should contain the account username (e.g., “ismith”) 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)  
2668 is identical to the name configured at the SharePoint using Powershell earlier in this section.  
2669 Verify that the AttributeNamespace is identical to the IncomingClaimType option configured at  
2670 the SharePoint using Powershell earlier in this section. If the name or namespace of the  
2671 attribute being passed to SharePoint does not match with the SharePoint configuration,  
2672 SharePoint will not allow access to the site, and direct your browser back to the SharePoint Sign  
2673 On screen.

2674 11. If you verified that the name and namespace of the expected attribute match with the  
2675 SharePoint configuration and SharePoint does not direct your browser to the site home page,  
2676 follow the instructions in the Troubleshooting SharePoint Federated Authentication Problems  
2677 section to determine the cause of the problem.

2678 **Expected Result:** Go back to the main browser window. The SharePoint server should present  
2679 the site home page. You should see the account username of the user that authenticated in the  
2680 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.

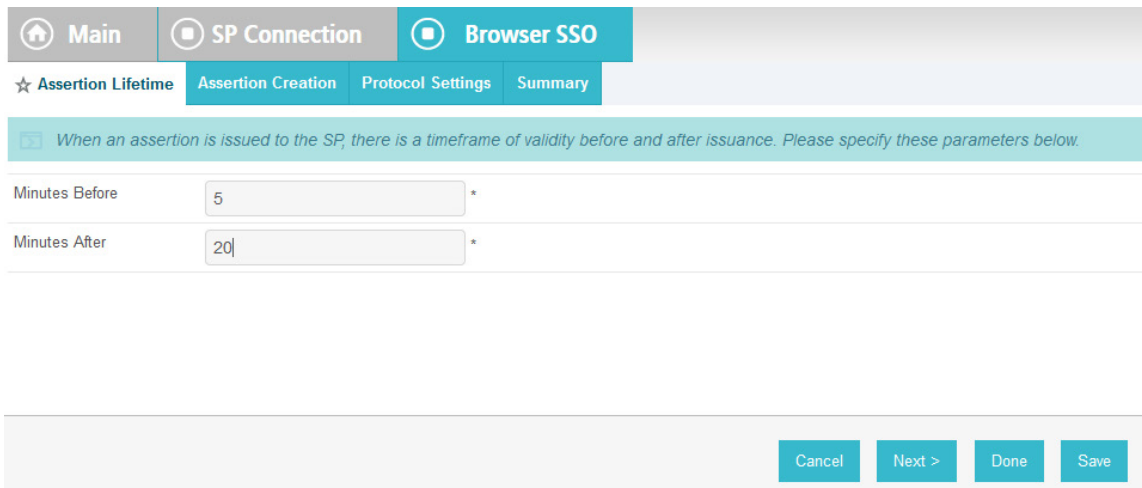
2689 **Note:** A SharePoint access control problem is a distinctly separate issue from authentication. A symptom  
2690 of an access control problem is when the user received a message that states “This site has not been  
2691 shared with you” upon successful authentication. Access control problems can be resolved by setting up

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.
  
- 2701       ▪ Verify that the expiration time of the security token generated by the PingFederate Server is  
 2702       more than 10 minutes. SharePoint calculates the time length of its session using the formula:  
 2703       SharePointSessionTime = SecurityTokenLifeTime – LogonTokenCacheExpirationWindow.  
 2704       SecurityTokenLifeTime is the length of time the token is valid, and this time is generated by the  
 2705       PingFederate server when it issues the token. By default the SharePoint  
 2706       LogonTokenCacheExpirationWindow is set to 10 minutes, therefore the SecurityTokenLifeTime  
 2707       must be greater than 10 in order to generate a SharePointSessionTime greater than zero. In our  
 2708       build we set the SecurityTokenLifetime to 20 minutes in the PingFederate configuration.
  
- 2709       • The expiration time of the security token can be set in the configuration of the SP  
 2710       Connection on the relying party’s PingFederate server. When you open the configuration for  
 2711       the SP Connection, click on the Assertion Lifetime link in the Browser SSO section. Enter a  
 2712       value for the Minutes After field that is greater than 10 (e.g., 20).



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 'Oe.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 'Oe.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.

## 2749 6 Attribute Exchange between the Identity Provider and 2750 Relying Party

### 2751 6.1 Introduction

2752 In previous sections of this How-To Guide, we demonstrated foundational steps to building an ABAC  
2753 solution:

- 2754     ▪ configuring federated authentication at the PingFederate-IdP
- 2755     ▪ configuring the SAML exchange between the PingFederate-IdP and PingFederate-RP
- 2756     ▪ configuring the Relying Party's SharePoint site
- 2757     ▪ configuring the federated logon at the SharePoint site

2758 Building upon that foundation, this section describes how to:

- 2759     ▪ create custom attributes and set values for them in Microsoft AD
- 2760     ▪ configure the PingFederate-IdP to pull user and environmental attributes during authentication
- 2761     ▪ configure the PingFederate-RP to pass the user and environmental attributes to the RP's  
2762         SharePoint
- 2763     ▪ configure SharePoint to load the user and environmental attributes passed from the  
2764         PingFederate-RP into the web session

2765 If you follow the instructions in this How-To Guide section, you will be able to perform a Functional Test  
2766 to verify the successful completion of the steps for installing, configuring, and integrating the  
2767 components.

### 2768 6.2 Create Custom User Attributes in Microsoft AD

2769 Follow the instructions in this section to create custom user attributes in the Microsoft AD schema. You  
2770 will add a new attribute and add it to the "user" class. Microsoft AD user accounts inherit from the  
2771 "user" class; therefore, the new attribute will be available to all of the users in the domain.

#### 2772 6.2.1 Preparing the AD Schema for Creating New Custom Attributes

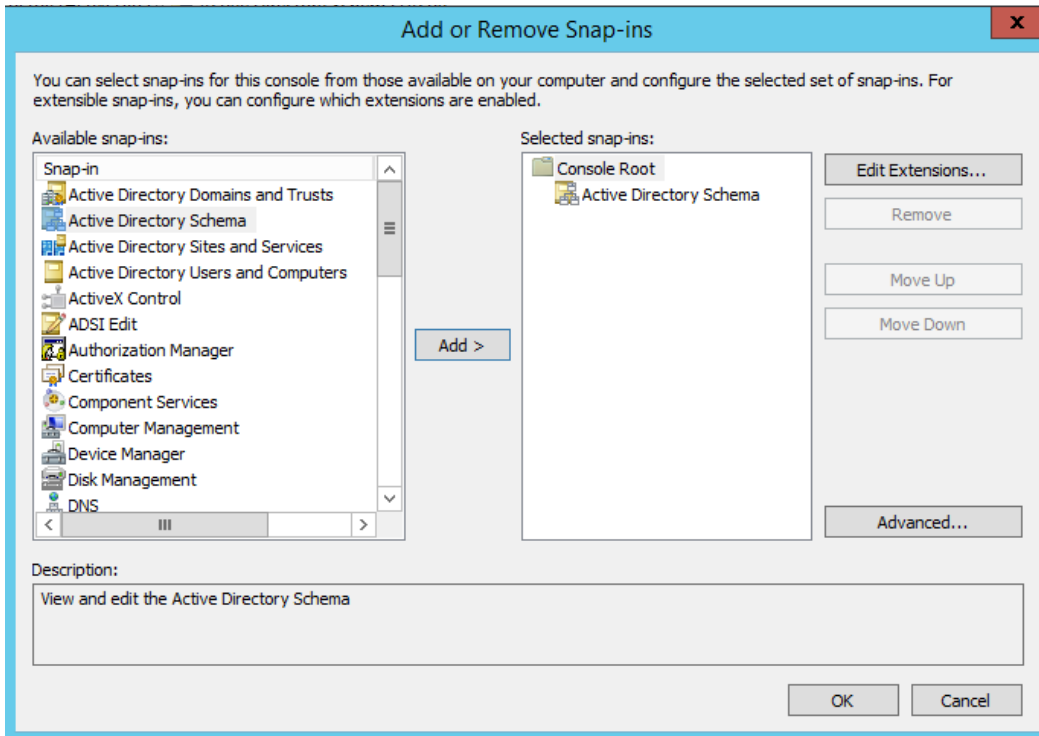
##### 2773 6.2.1.1 *Backing Up Your Directory before Making Schema Changes*

2774 Microsoft recommends that you back up your directory before making schema changes. Choose the  
2775 names of your new custom attributes carefully, because the creation of a new attribute is a permanent  
2776 operation.

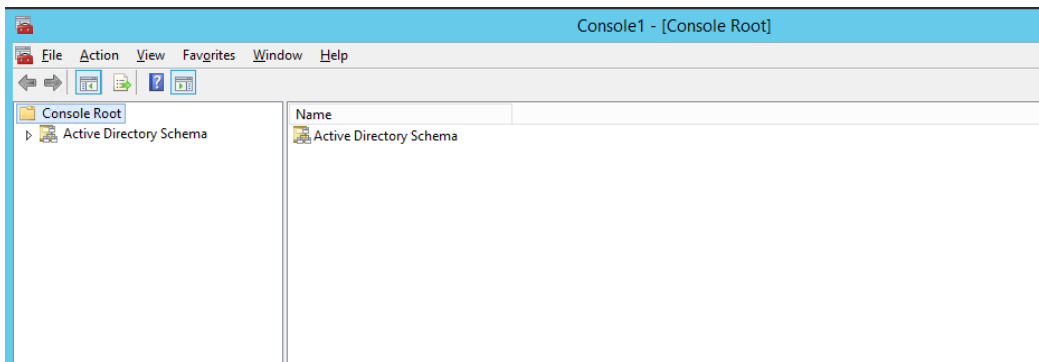
- 2777     1. Log on to the server that contains the Microsoft AD schema (typically the schema is on the  
2778         domain controller).
- 2779     2. Launch a Command Prompt, using the Run as Administrator option.
- 2780     3. Execute the following command:  
2781         **regsvr32 schmmgmt.dll**







2791



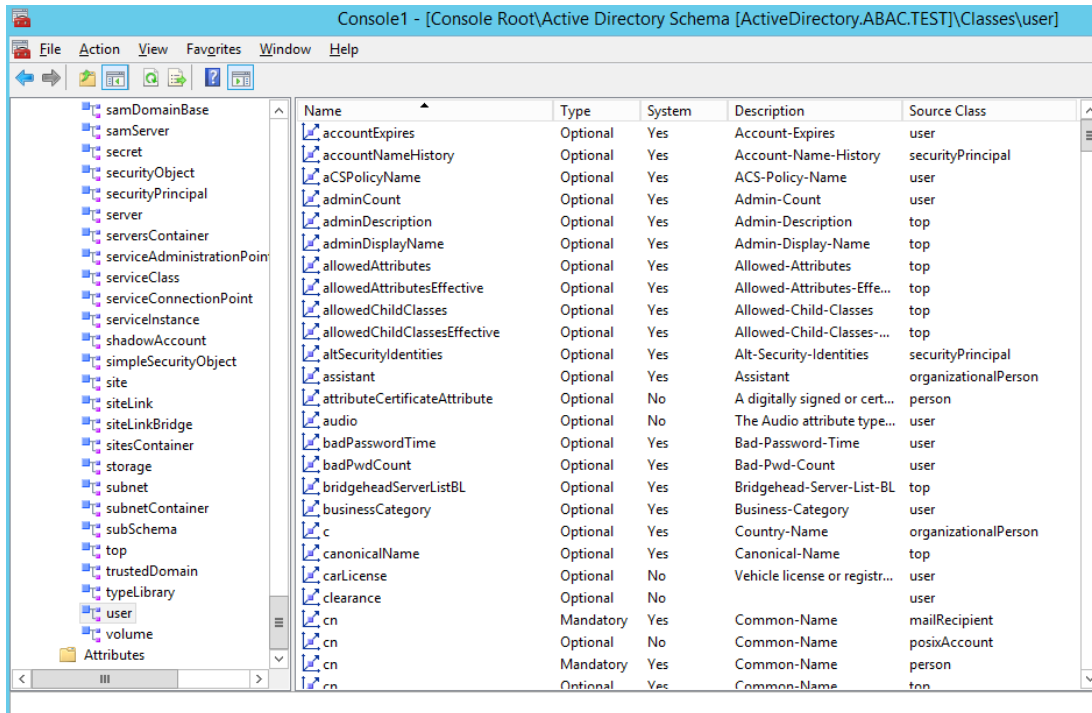
2792

2793 9. Expand the **Active Directory Schema** on the left.

2794 *6.2.1.2 Reviewing Existing Attributes to Avoid Redundancies when Creating New*  
 2795 *Attributes*

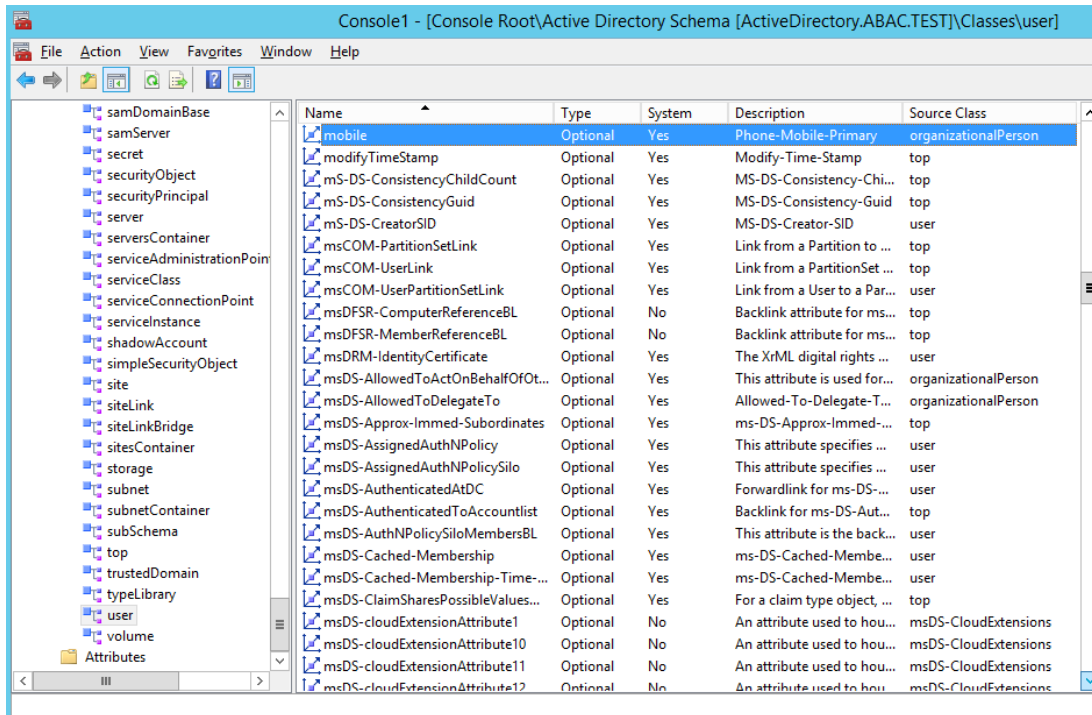
2796 Before you create a new attribute, it is important to review existing user attributes in your Active  
 2797 Directory Schema. Under Active Directory Schema on the left, expand the Classes folder and scroll down  
 2798 to click on the **user** class. Examine the existing set of **user** class attributes 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.





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.

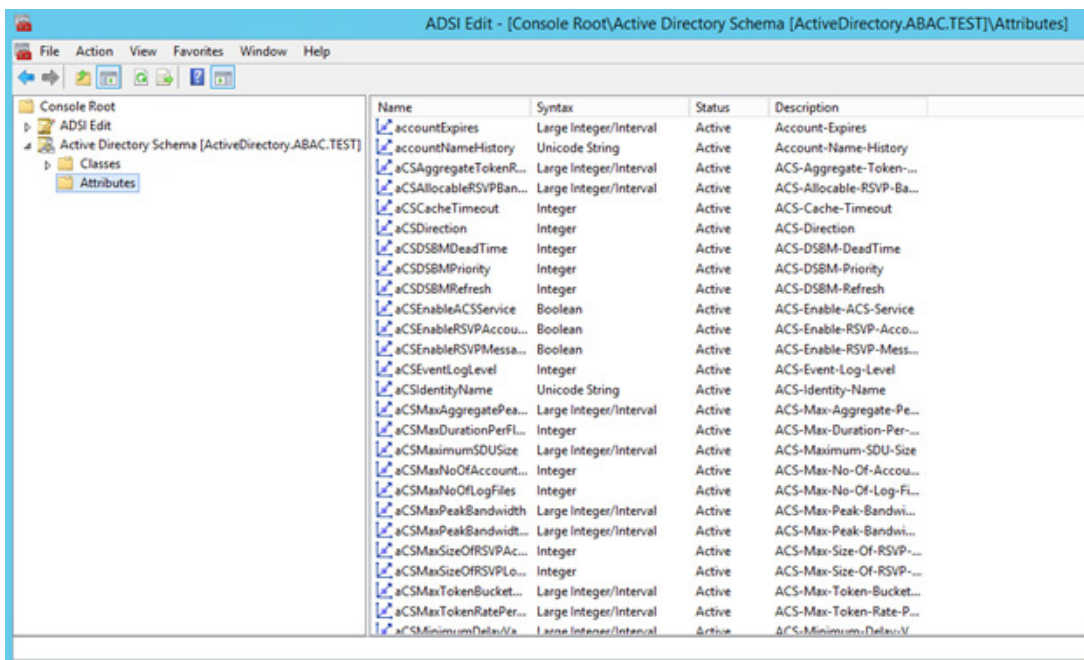


2807

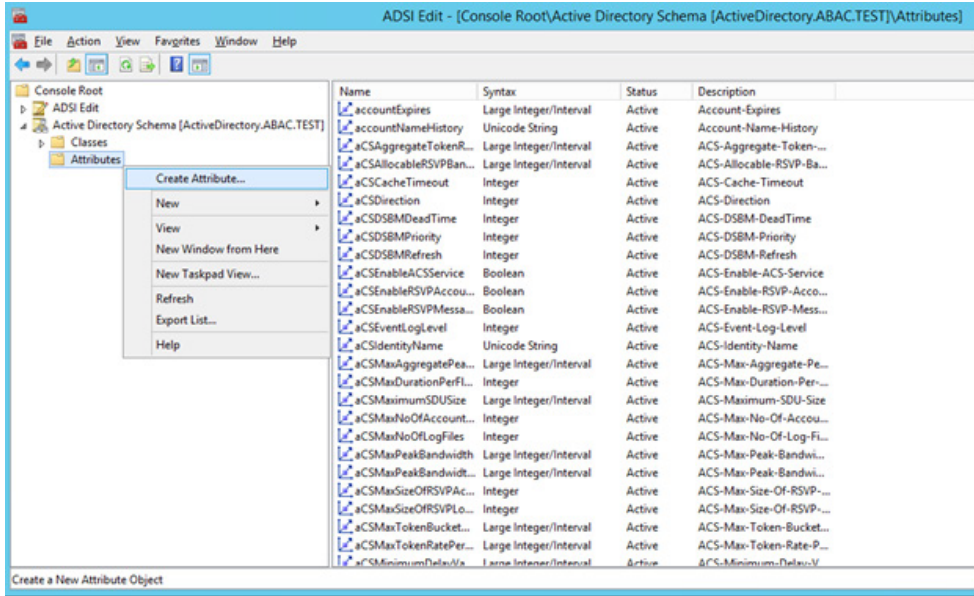
2808 Once you have identified that the creation of a new attribute is warranted, proceed with the following  
 2809 instructions.

2810 **6.2.1.3** *Creating New Custom Attributes*

- 2811 1. Launch a browser window and go the Microsoft site:
- 2812 <https://gallery.technet.microsoft.com/scriptcenter/56b78004-40d0-41cf-b95e-6e795b2e8a06>
- 2813 2. Copy the **oidgen.vbs** script code that is shown on the page to the clipboard.
- 2814 3. Open **Notepad** and paste the script into the editor.
- 2815 4. Save the script to a file on the desktop named **oidgen.vbs**.
- 2816 5. Go back to the Active Directory schema window.
- 2817 6. On the left pane, click on the **Attributes** folder.



- 2818
- 2819 7. Right-click on the **Attributes** folder and select Create Attribute.
- 2820 8. Click **Continue** on the warning window.



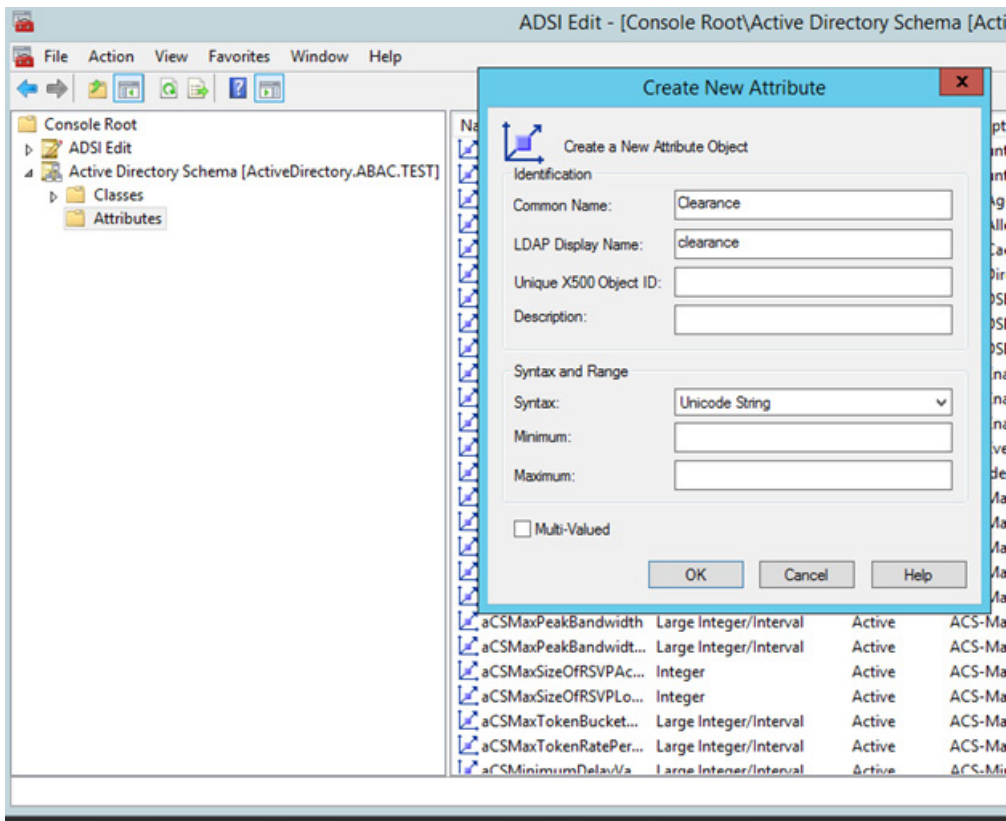
2821

2822

2823

2824

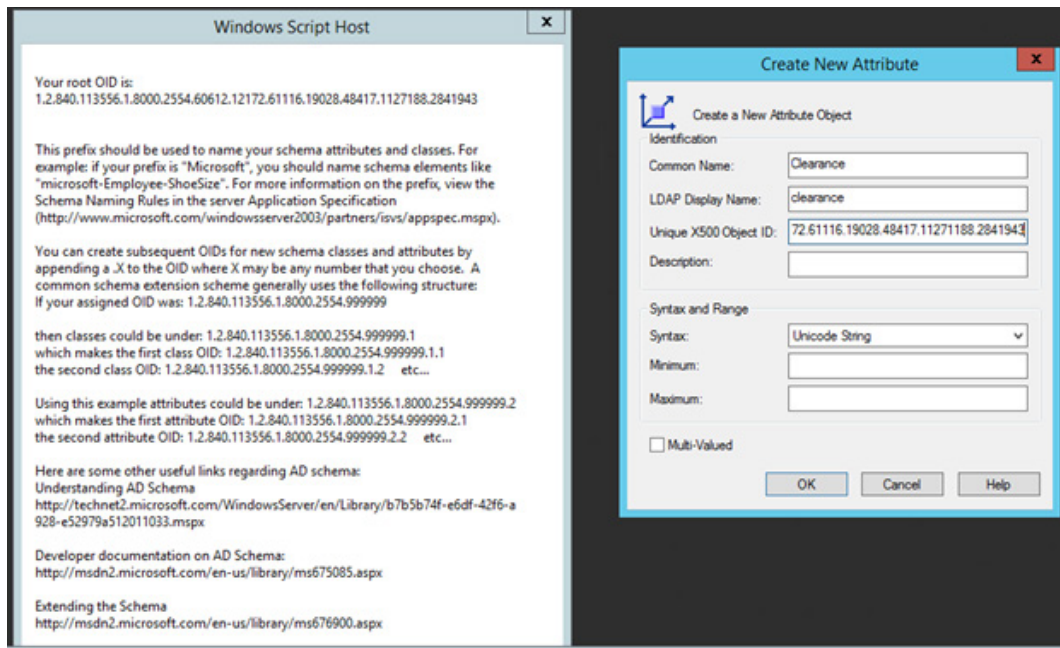
- Enter the name of your new attribute and select the type of attribute in the Syntax field. In the example below, the name of the new attribute is **clearance** and the type of attribute is **Unicode String**.



2825

2826 **6.2.1.4** *Generating an ID to Enter into the Unique X500 Object ID Field*

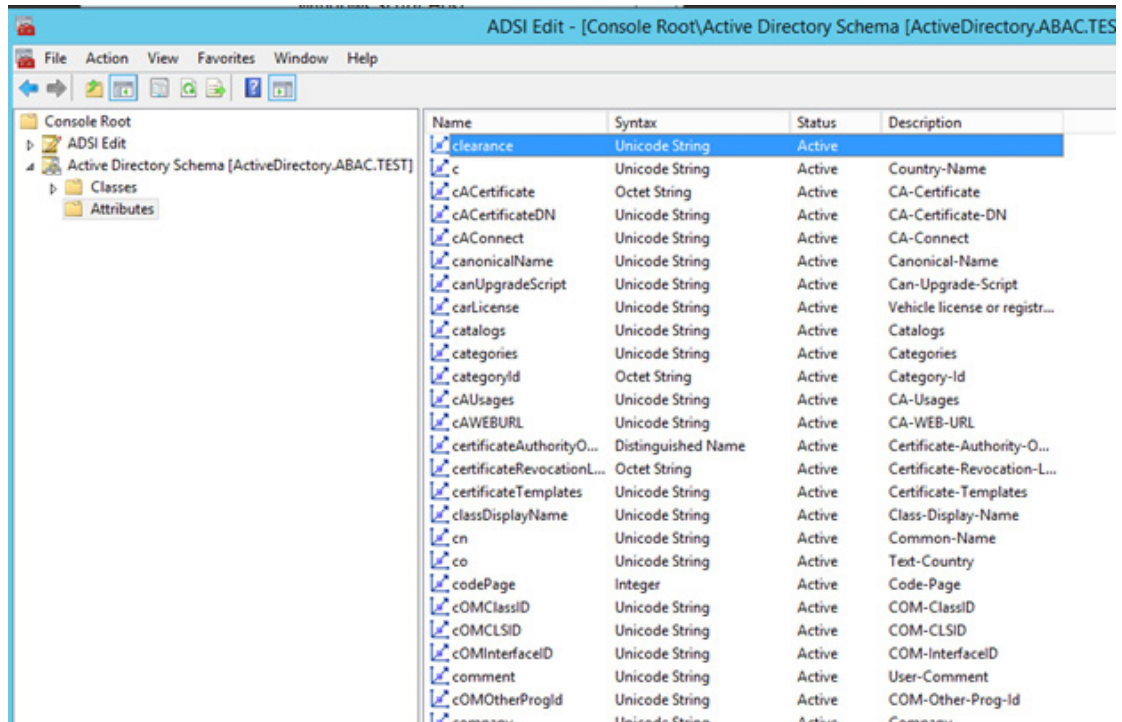
2827 Next, you need to generate an ID to enter into the Unique X500 Object ID field.

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.



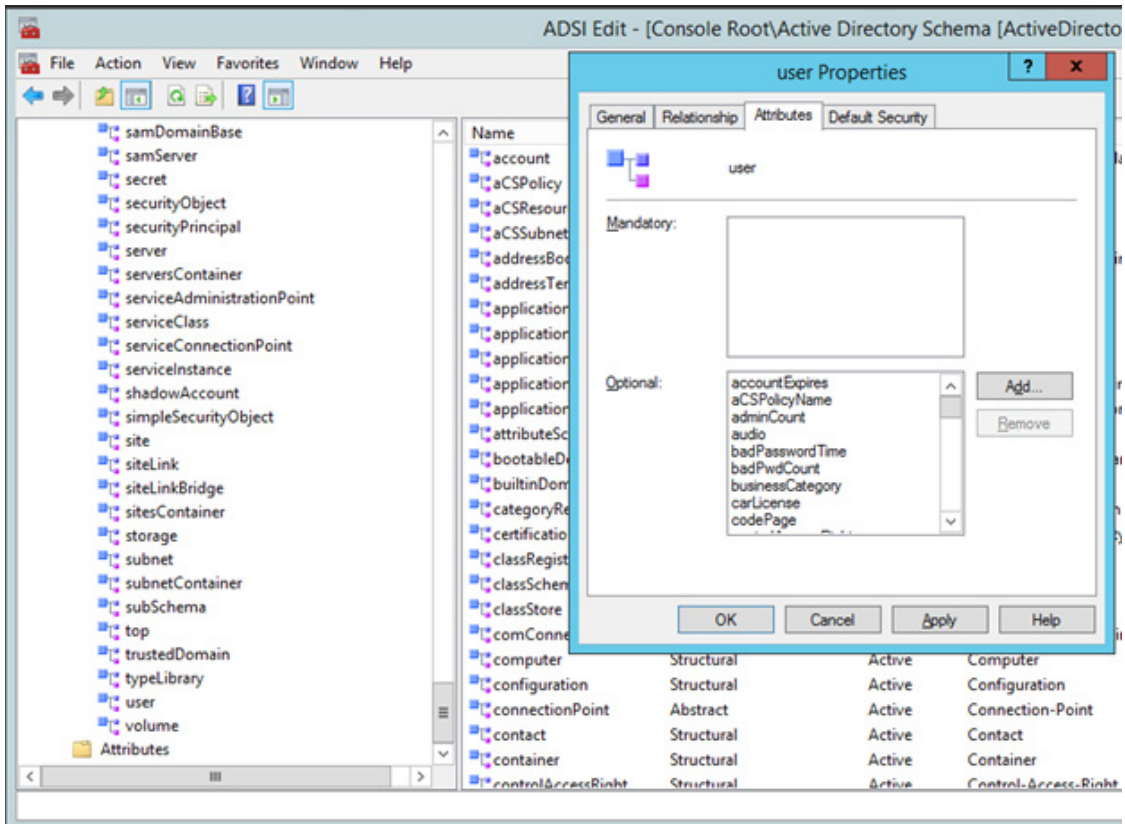
2835

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**  
 2839 class, and select **Properties**.

2840 2. Click on the **Attributes** tab.

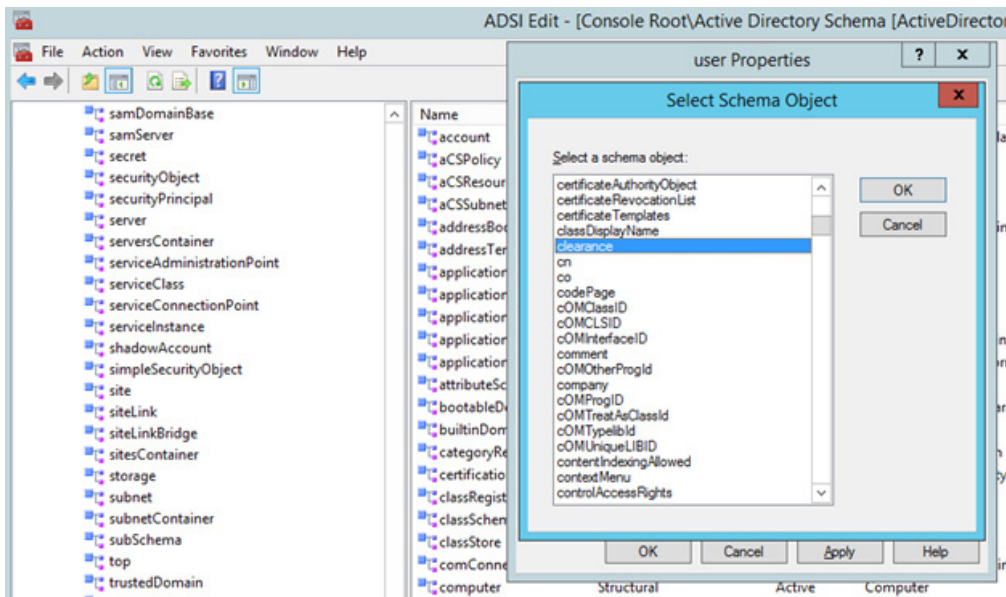




2841

2842

3. Click **Add**. Scroll down and click on the new attribute.



2843

2844

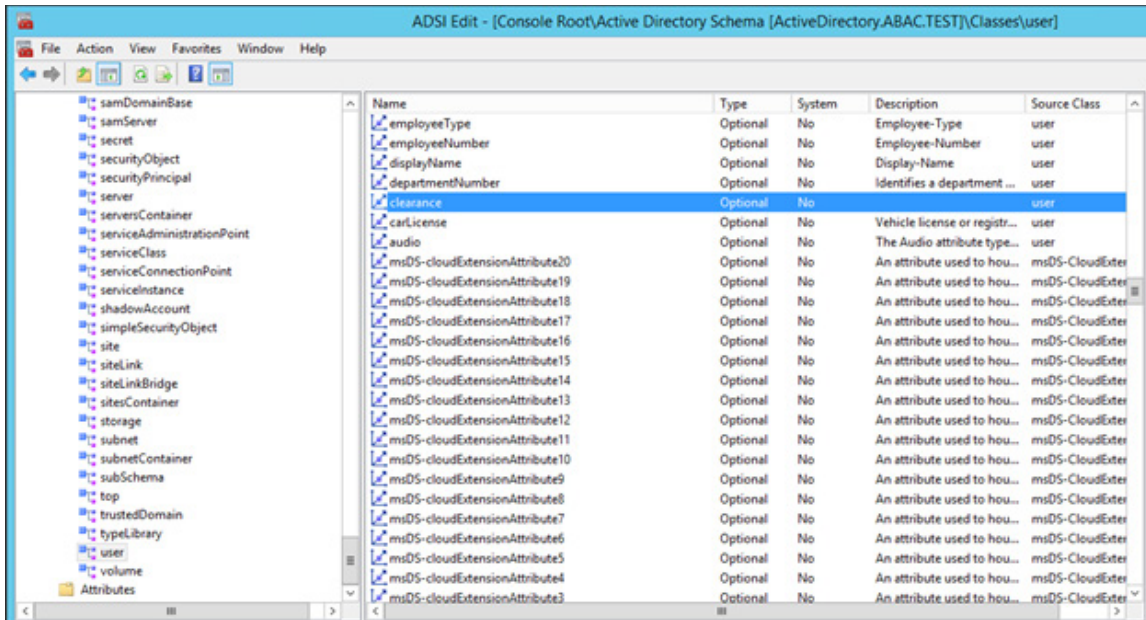
2845

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.

2846

2847

When you examine the list of attributes for the **user** class, you should be able to see the new attribute.



2848

### 6.2.2 Set Values for Custom User Attributes in Microsoft AD

2849

2850

Once you have created a new custom attribute in the Active Directory **user** class, that new attribute will be available for all users in the domain. You will be able to set specific values for the new attribute for each distinct user. Follow the instructions in this section to set a user-specific value for a new attribute in Active Directory.

2851

2852

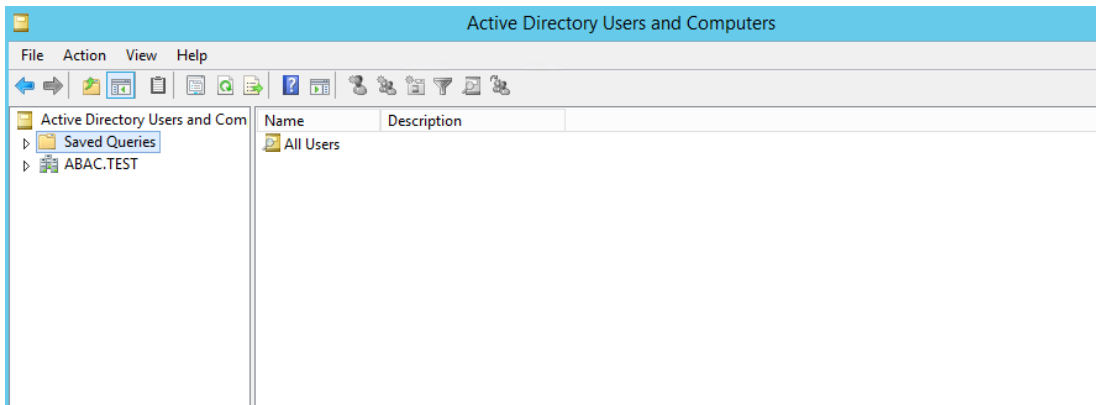
2853

2854

1. Log on to the Microsoft AD server.

2855

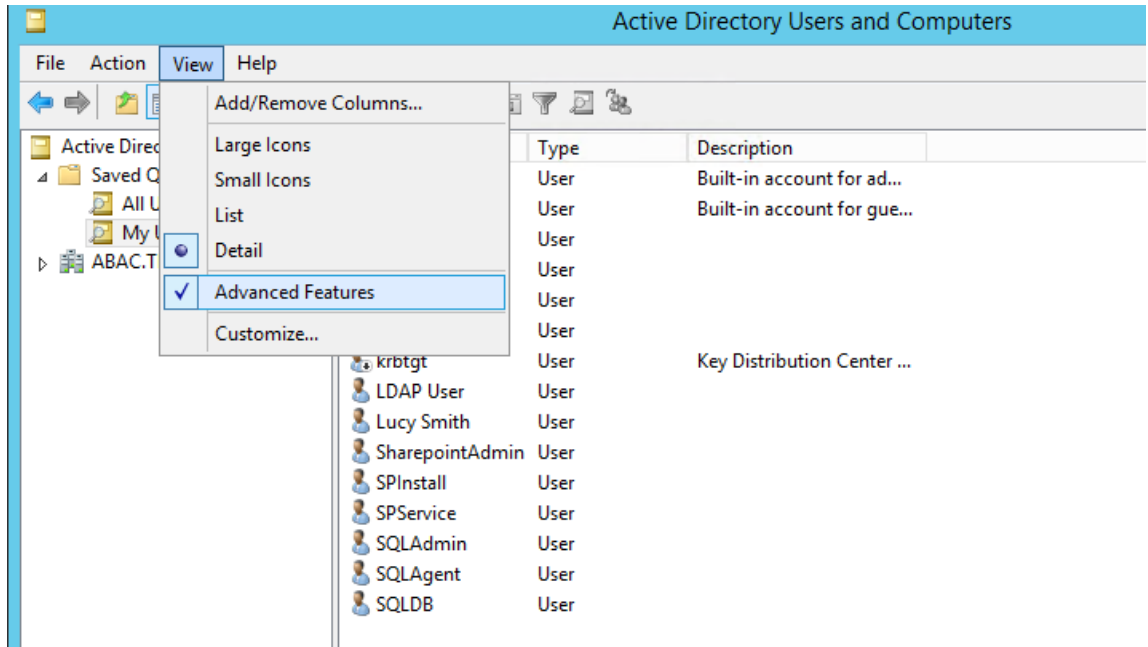
2. Open the Active Directory Users and Computers program.



2856

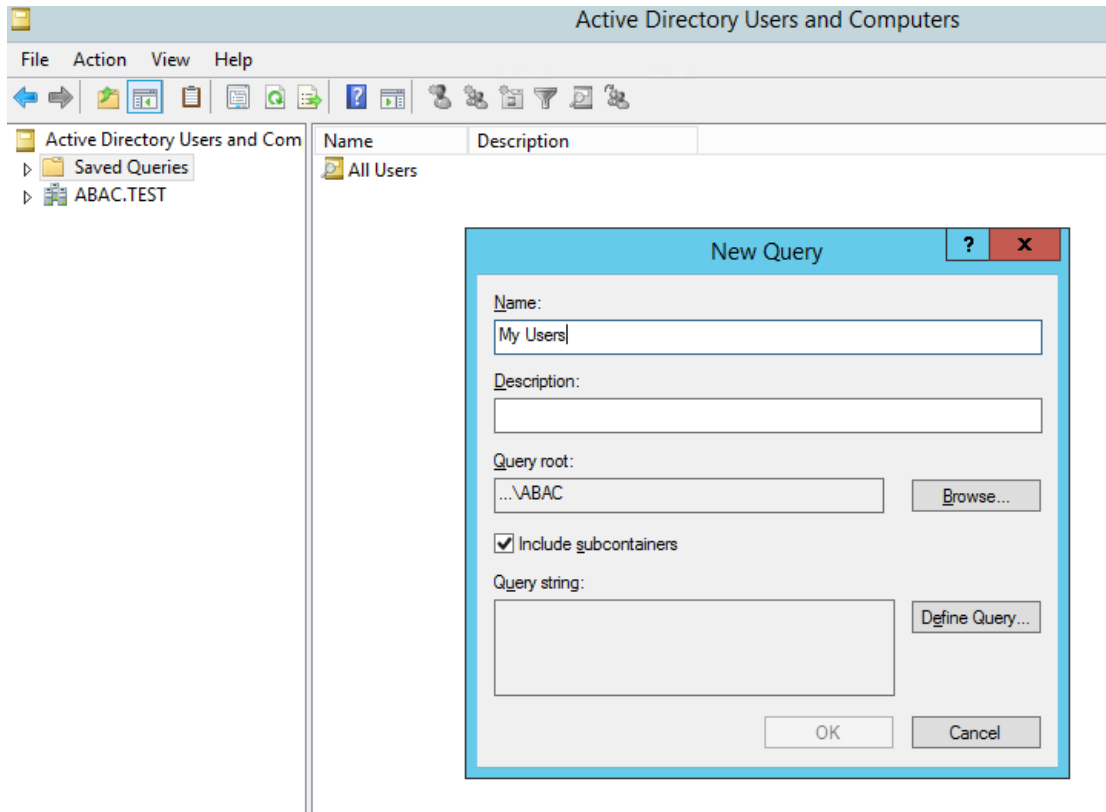
2857

3. Click on the **View** menu and select **Advanced Features**.



2858

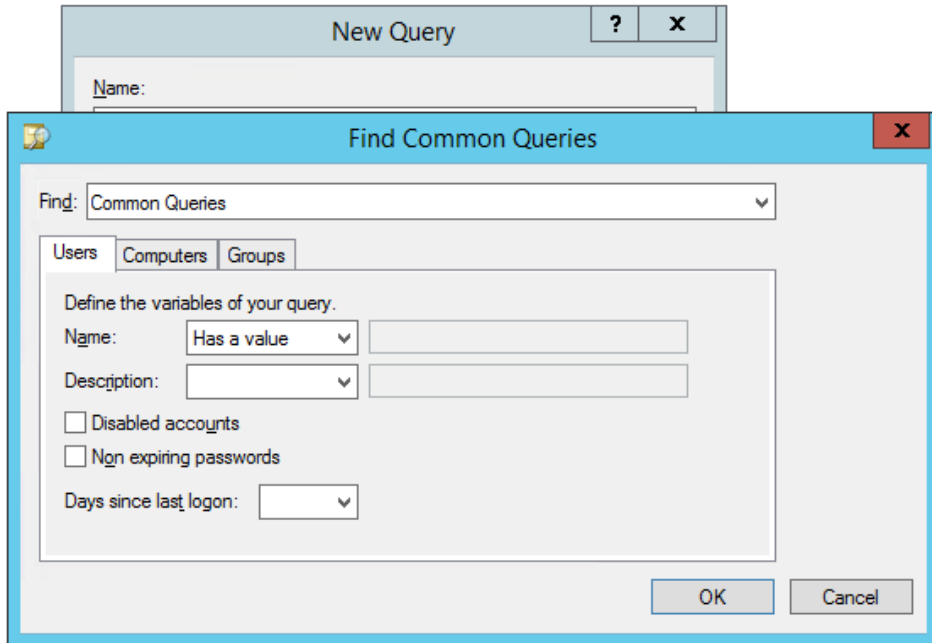
- 2859 4. Right-click on Saved Queries and select **New > Query**. Enter a name for your query (e.g., **My**  
 2860 **Users**).



2861

- 2862 5. Click on **Define Query**. From the **Name** list, select **Has a value**.





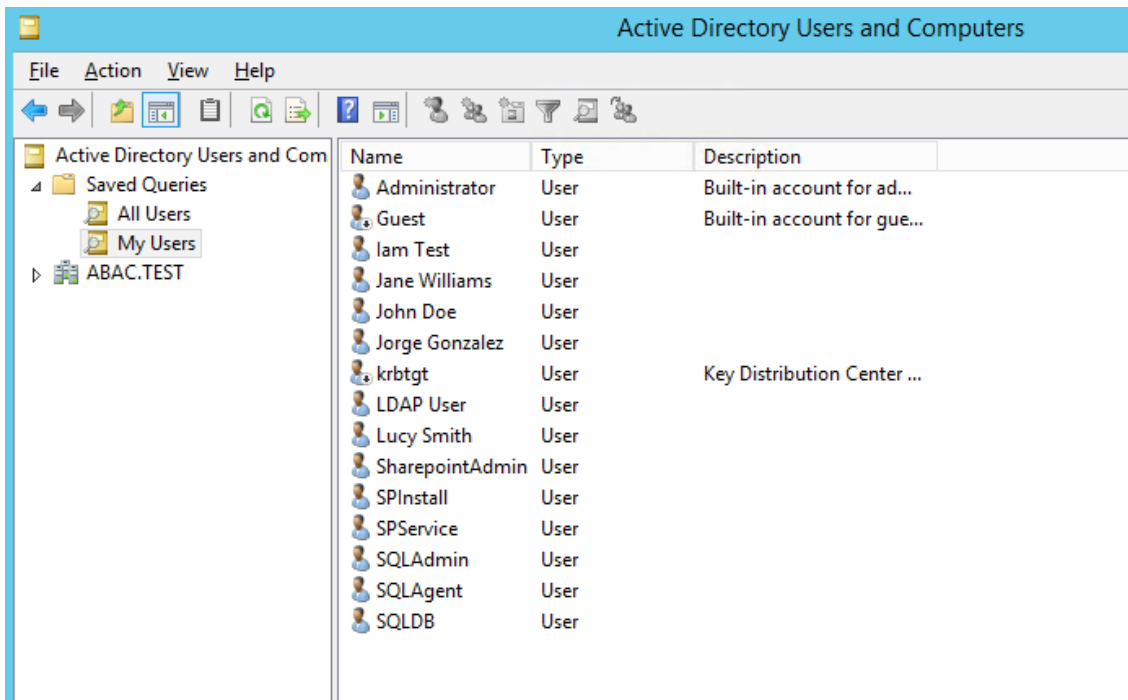
2863

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.

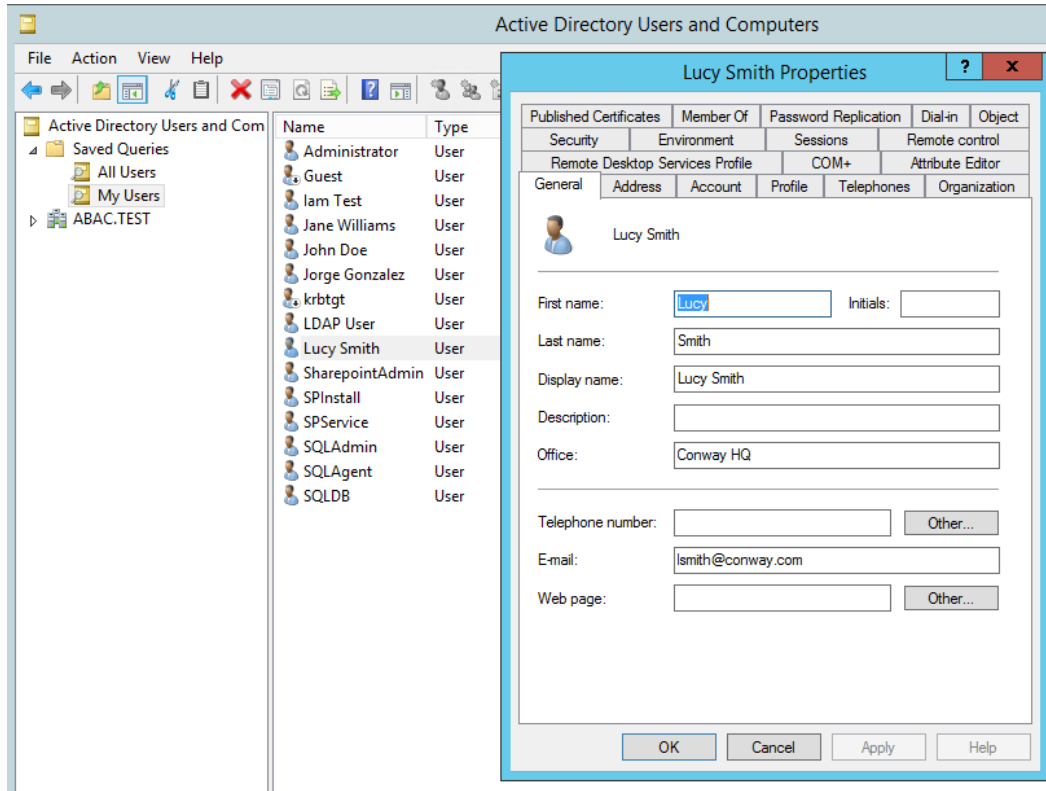


2866

2867

2868

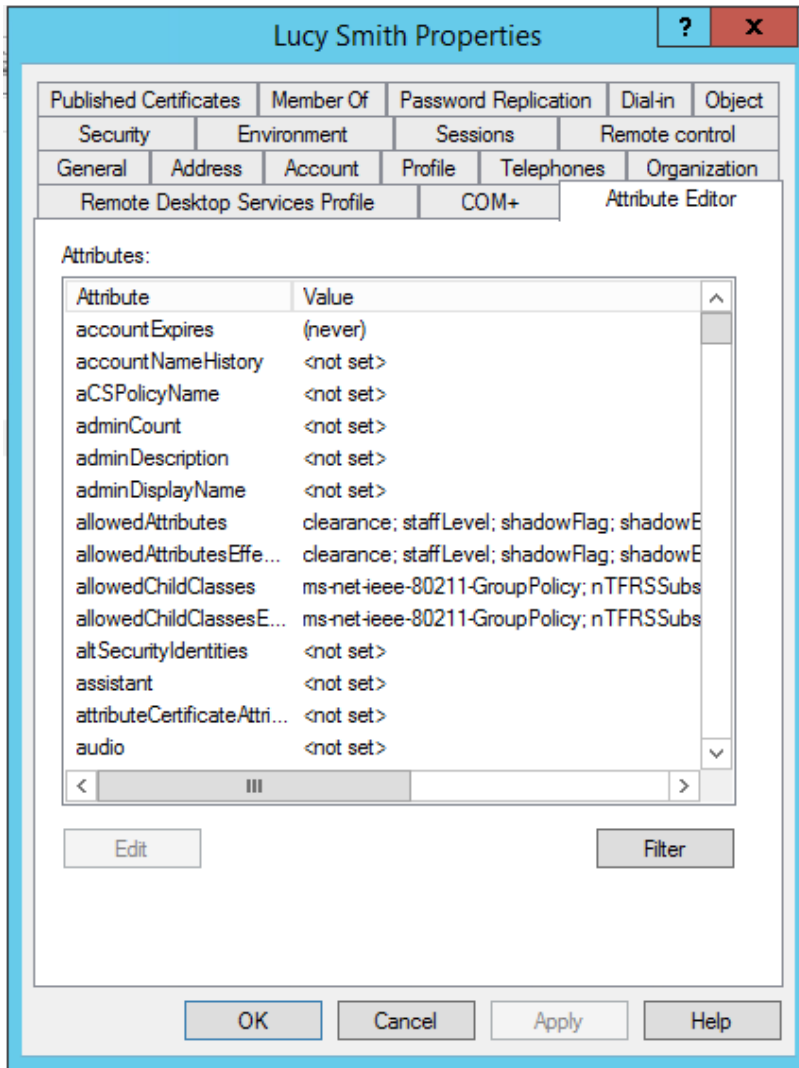
7. Double-click on the specific user (e.g., **Lucy Smith**) that you want to modify to bring up the properties window.



2869

2870

8. Click on the **Attribute Editor** tab.

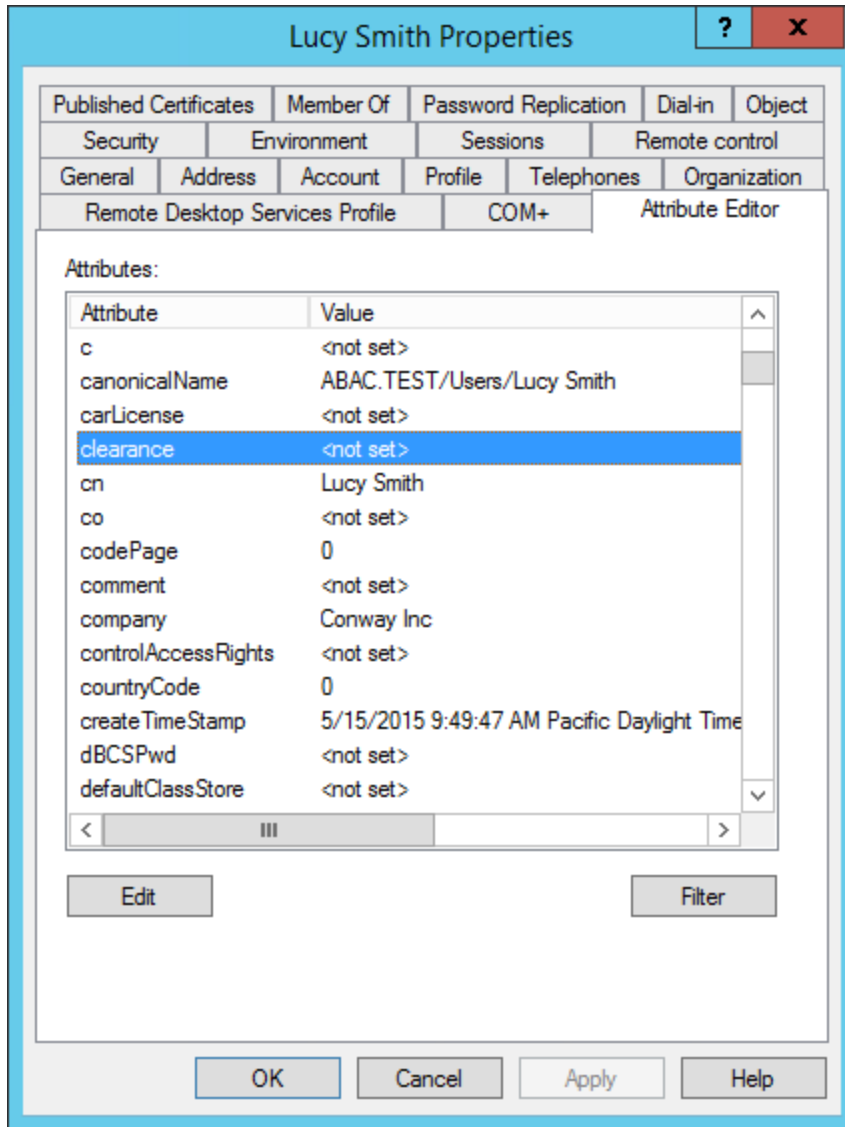


2871

2872

2873

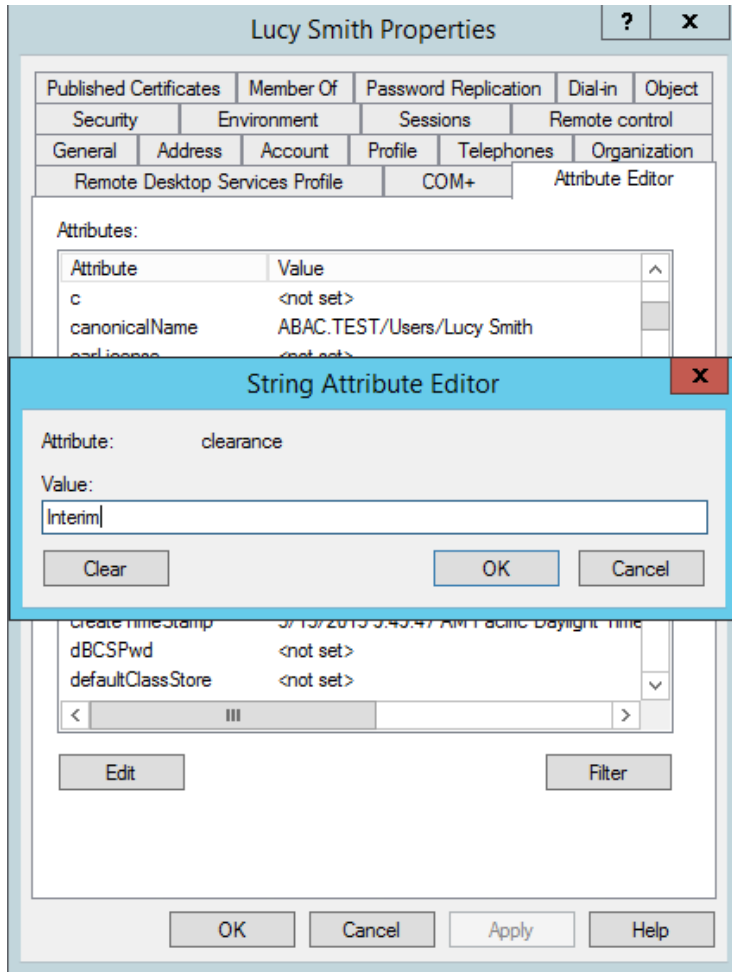
9. Scroll down and locate the new custom attribute for which you want to set a value (e.g., **clearance**).



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

2882

Note: When you set an attribute value in the attribute editor and then go back to the Users query view, you have to press F5 or click the **Action menu > Refresh** to see the new value.

2883

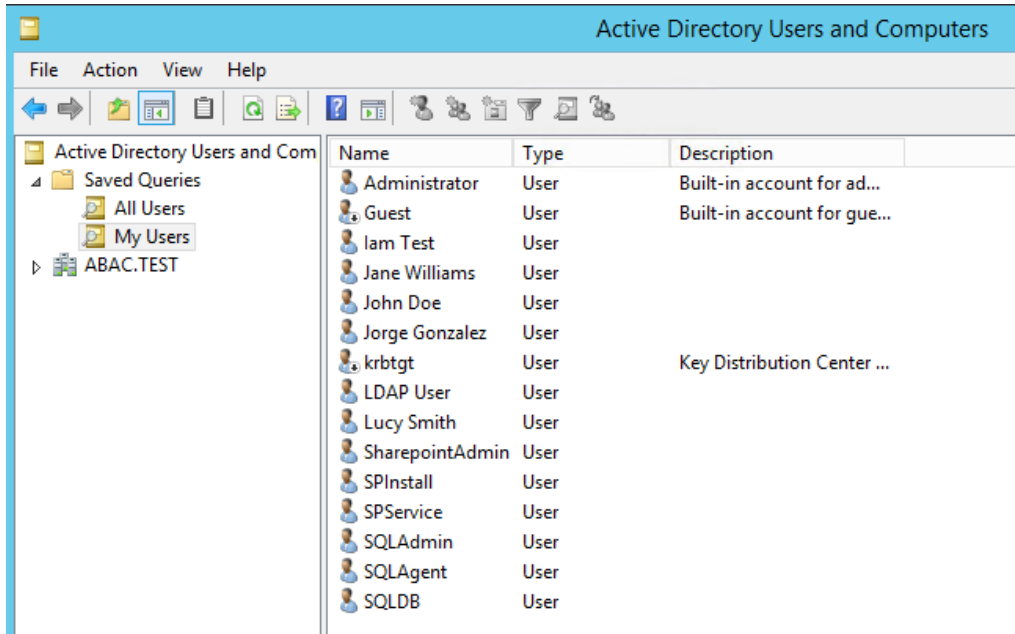
### 6.2.2.1 Adding New Columns to the Users Query View

2884

2885

2886

Next you will add new columns to the Users query view to help monitor the custom attribute values for each user in the directory. By default, the Users view only shows the attribute values for **Name**, **Type**, and **Description**.



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**.

★ Manage Connections

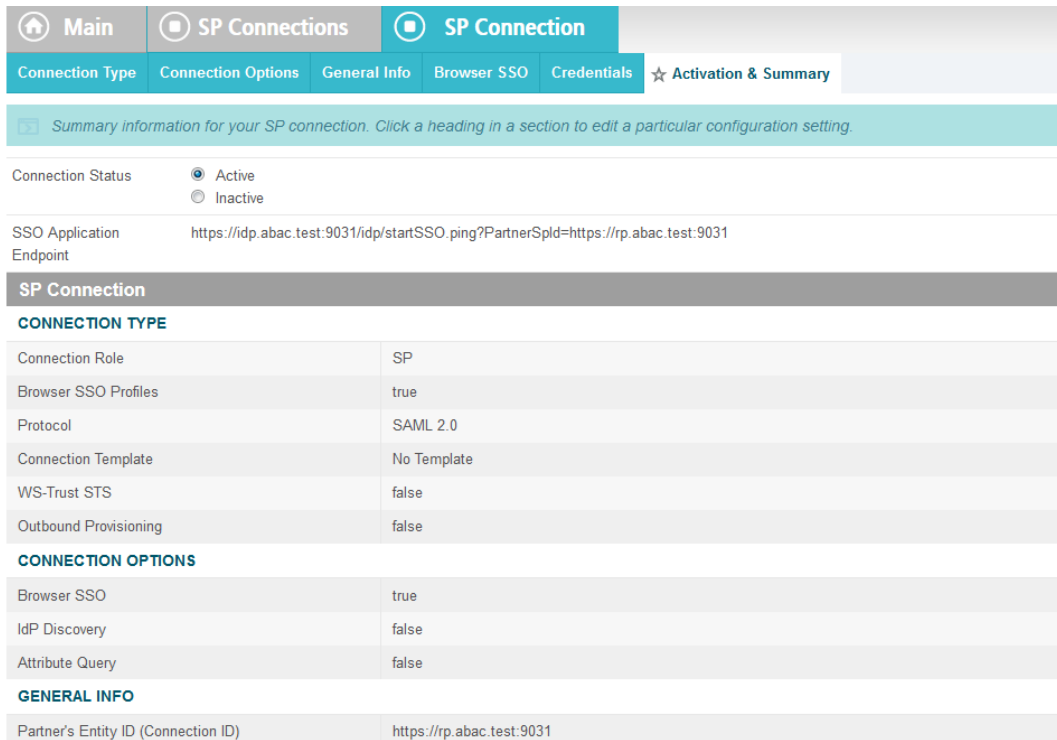
On this screen you can manage connections to your partner SPs. Use the drop-downs to filter the connection list. You can also override the logging mode for all SP connections by specifying a single, global logging mode.

CONNECTION NAME ▲	CONNECTION ID ▲	PROTOCOL ▲	STATUS ▲	ACTION
Demo SP	PF-DEMO	SAML 2.0	Active	Delete   Copy Export Connection   Export Metadata
https://rp.abac.test:9031	https://rp.abac.test:9031	SAML 2.0	Active	Delete   Copy Export Connection   Export Metadata
urn:nccoe:abac:rp	urn:nccoe:abac:rp	SAML 2.0	Active	Delete   Copy Export Connection   Export Metadata

Create Connection... Import Connection Check All Connections For Errors

Logging Mode Override  
 Off  
 On

- 2907
- 2908 5. Click on the link for the connection created in [Section 3](#) (e.g., *https://rp.abac.test:9031*).

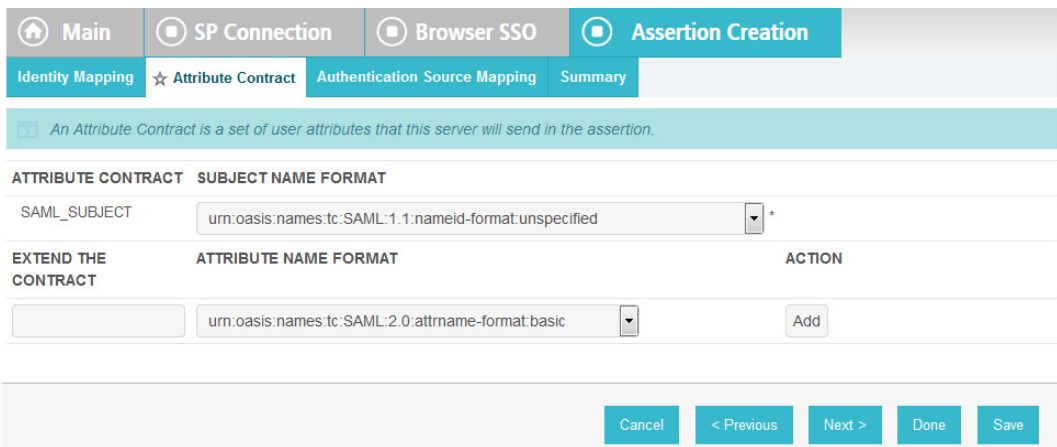


2909

2910

2911

- On the Activation & Summary screen, scroll down to the **Assertion Creation** group and click on the **ATTRIBUTE CONTRACT** link.



2912

2913

2914

2915

- 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.



2916

2917 8. Click **Add**.

2918

2919 9. Click **Save** to complete the configuration.

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.

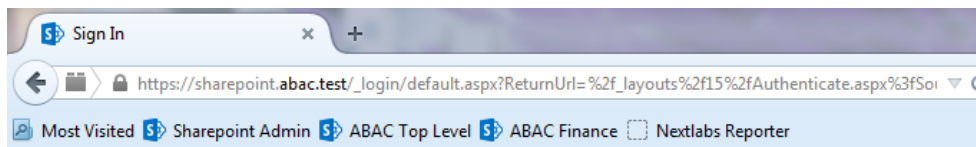
2925 Follow the instructions in the section Temporarily Disable SAML Encryption for Testing and  
 2926 Troubleshooting Message Exchanges at the end of this section to disable SAML encryption. Once SAML  
 2927 encryption has been disabled, you can proceed with the following functional test instructions.

2928 1. Launch your Firefox browser and select **SAML tracer** from the **Tools** menu.  
 2929 This launches an empty SAML tracer window.

2930 2. Minimize the SAML tracer window.

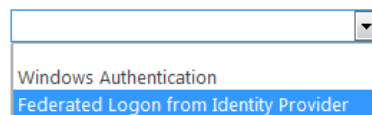
2931 The SAML tracer automatically records the details of the HTTPS messages in the background.

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:



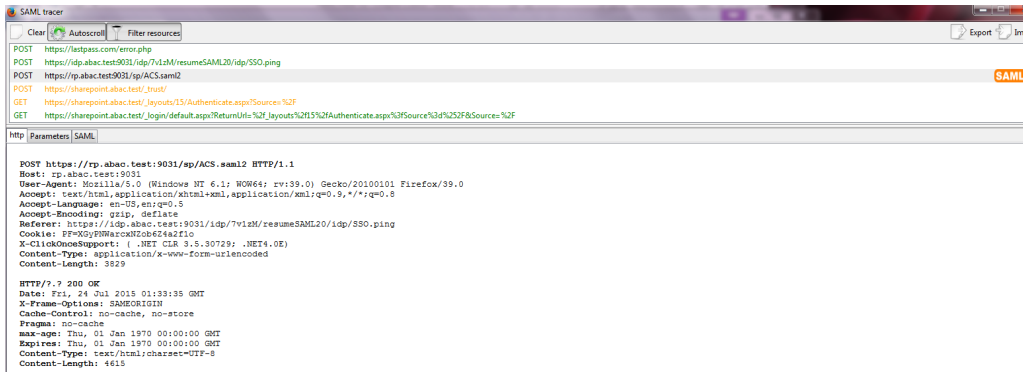
2934

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., **lsmith**) 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.



2943

2944

2945

8. Click on the **SAML** tab. Scroll down the SAML message and locate the AttributeStatement node and sub nodes.



2946

2947

2948

2949

**Expected Result:** Ensure that the attribute you configured from Microsoft AD contains a node. In the example screenshot above, you can see that there is an Attribute node for the **company** attribute because of the line **<saml:Attribute Name= "company"**.

2950

2951

2952

2953

2954

**Expected Result:** Ensure that the AttributeValue node contains the expected value for the attribute from ActiveDirectory. In the example screenshot above, you can see there is an AttributeValue node for the **company** attribute and the value is **Conway Inc**. This is correct, because in our Microsoft AD environment, the user account we tested with is **lsmith** (Lucy Smith), and Lucy's **company** attribute in Microsoft AD is set to a value of **Conway Inc**.

2955

2956

2957

2958

When you complete this functional test, you must enable SAML encryption between the IdP and RP again. Follow the instructions in the section Temporarily Disable SAML Encryption for Testing and Troubleshooting Message Exchanges, subsection Enable SAML Encryption at the end of this section again to enable SAML encryption.

### 2959 6.3.2 Configure PingFederate-IdP to Pull Environmental Attributes During 2960 Authentication

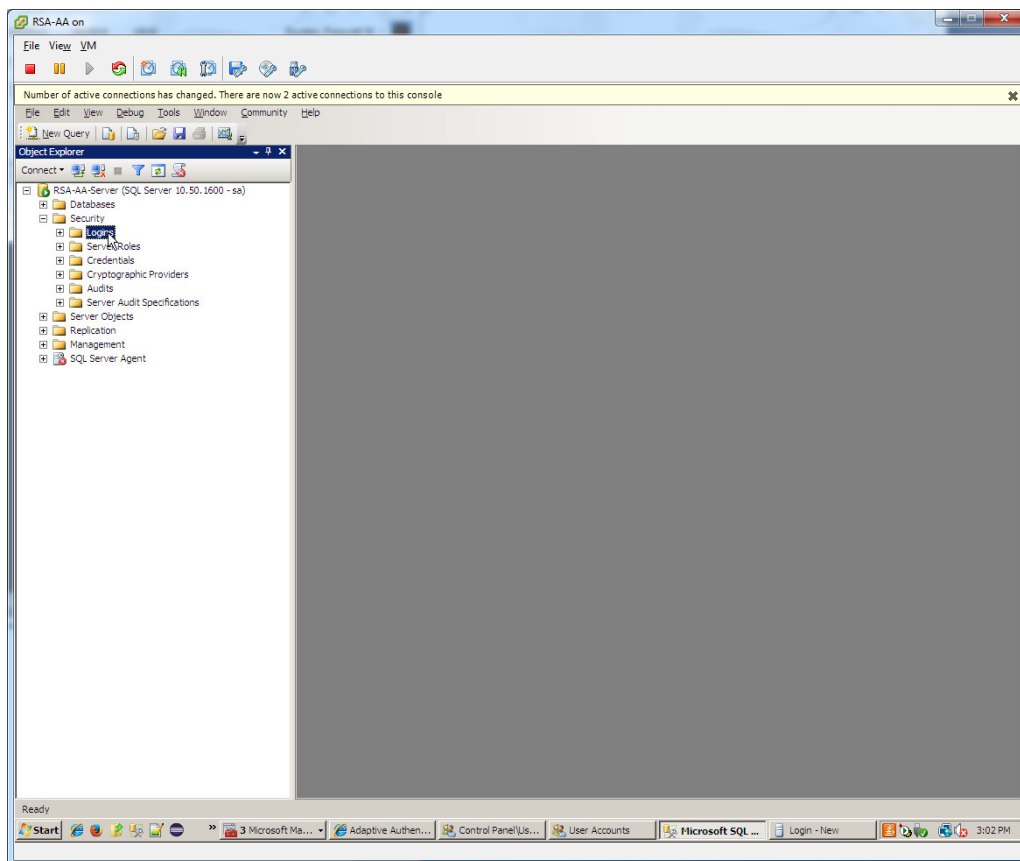
2961 Follow the instructions in this section to configure the PingFederate-IdP to get environmental attribute  
2962 values from the RSA Adaptive Authentication system during the authentication process. The  
2963 environmental attributes are passed along with the user attributes in the SAML messages 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.

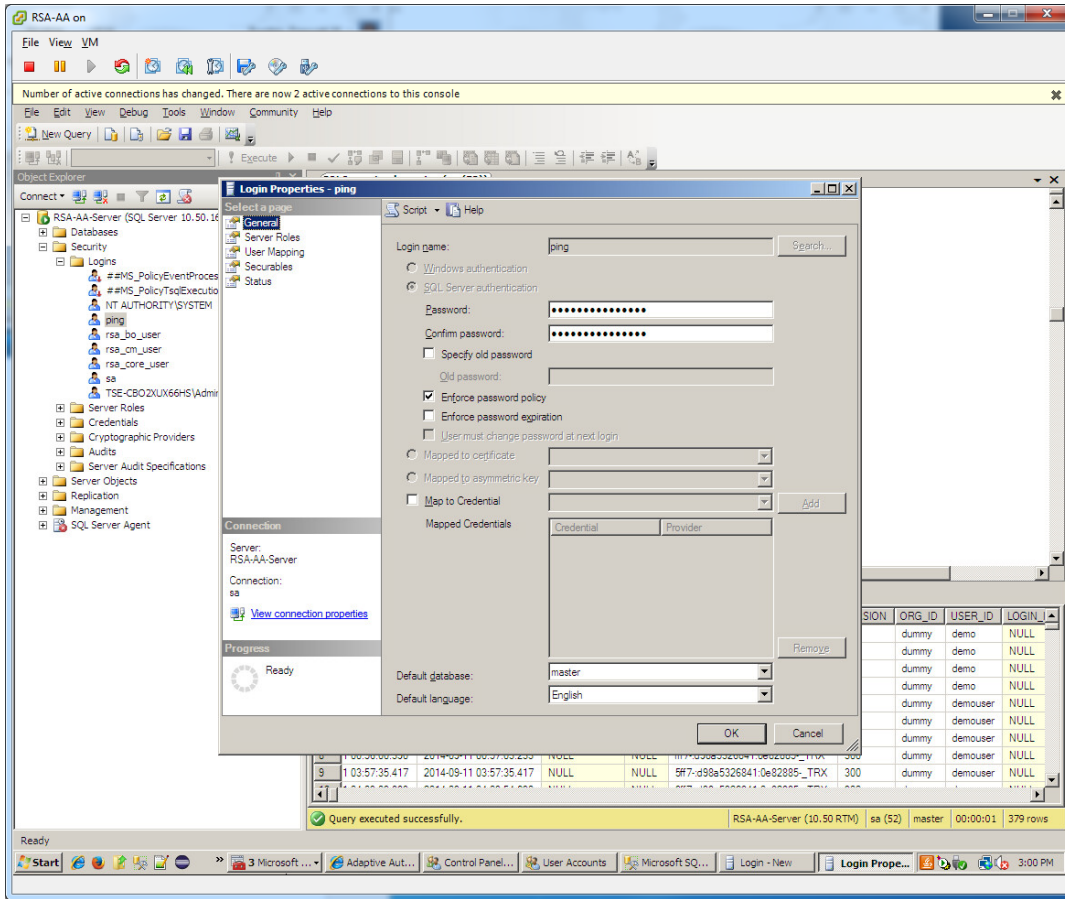
2972 Log on to the server that hosts the RSA Adaptive Authentication SQL Server database engine.

- 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**.



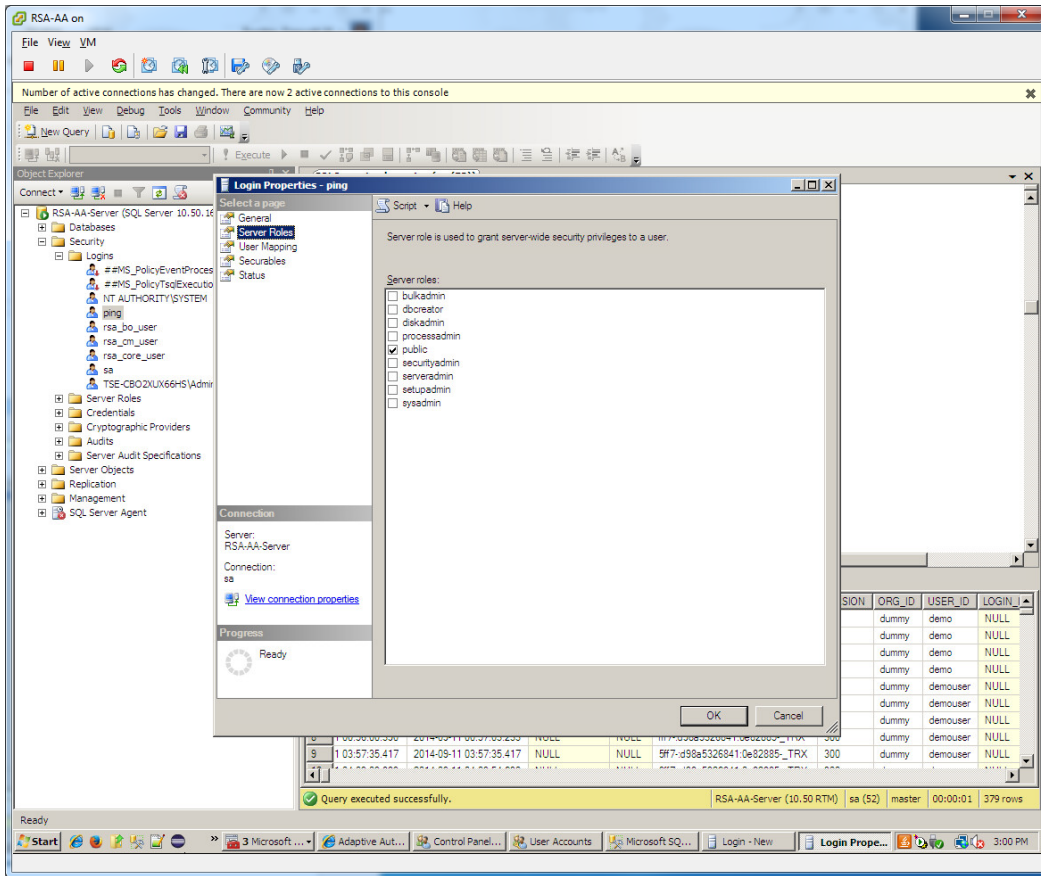
2976

- 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**.

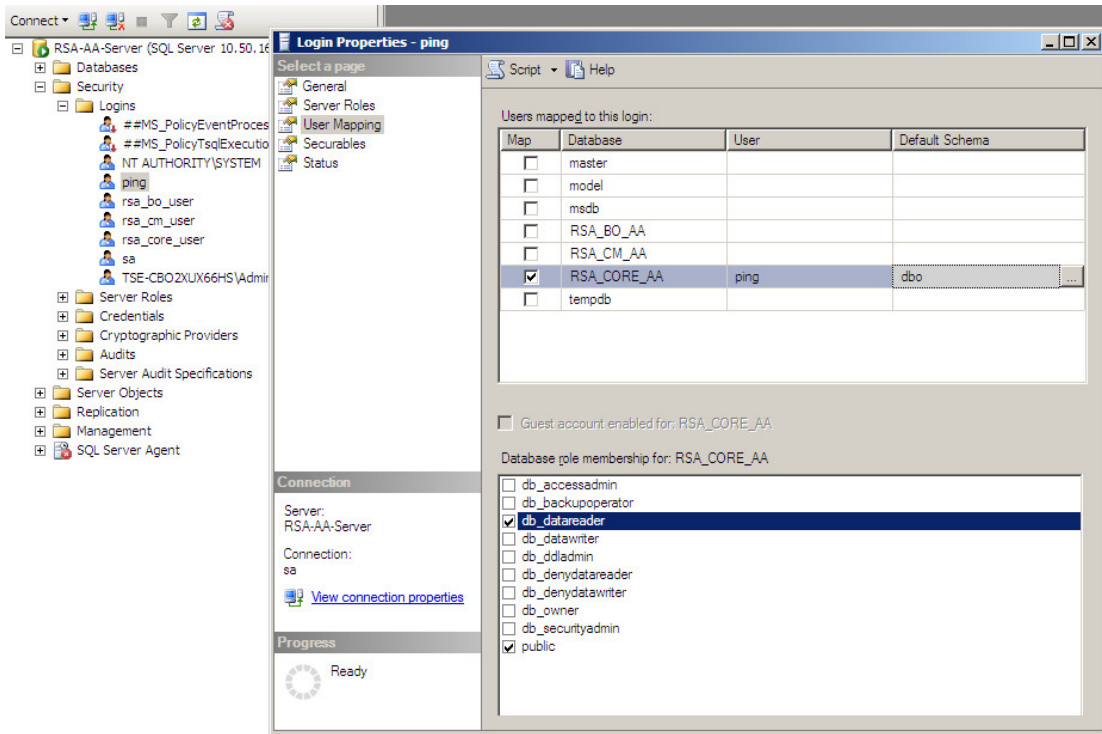


2981

2982

2983

Under User Mapping, check the Map box next to **RSA\_CORE\_AA**. In the bottom pane, under **Database role membership**, check the box next to **db\_datareader**.



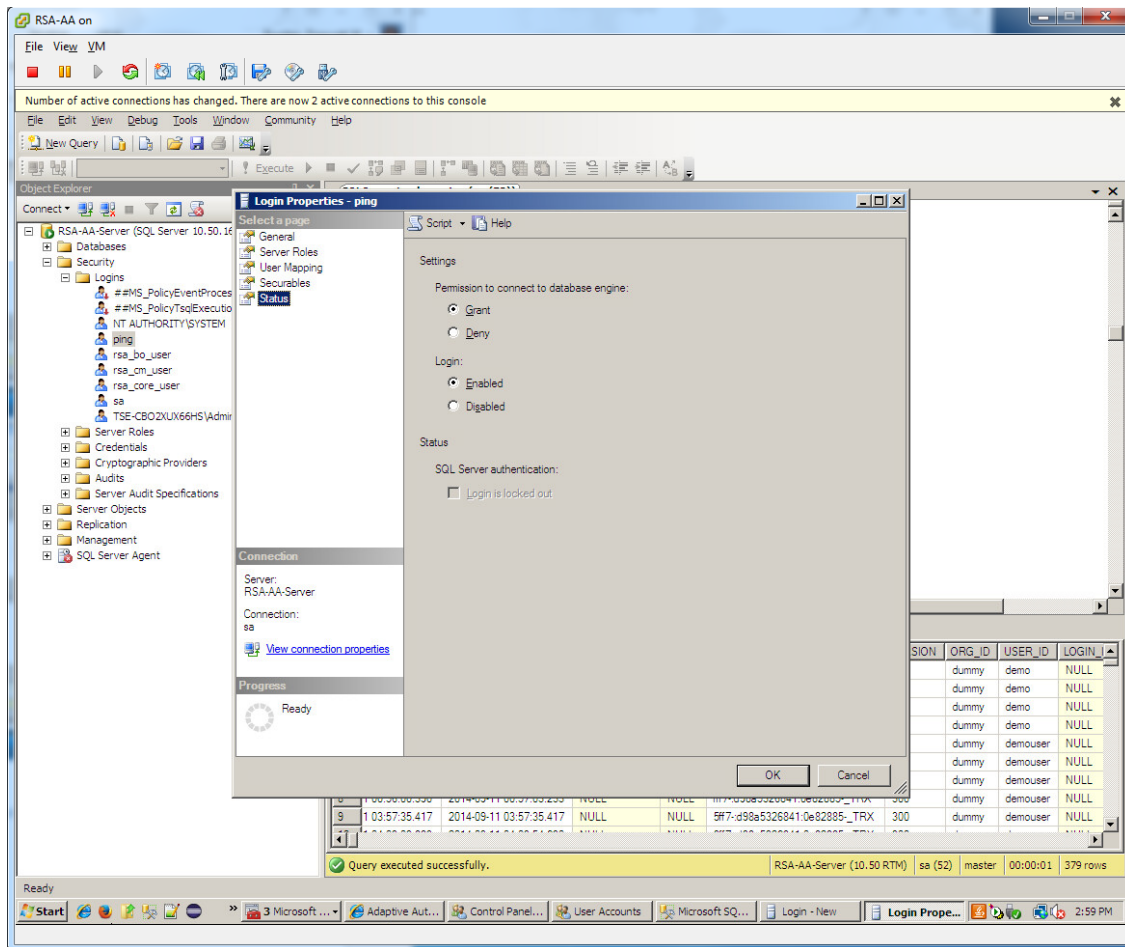
2984

2985

2986

- Under **Status**, set permission to connect to database engine to **Grant** and **Login** to **Enabled**. Click **OK**.





2987

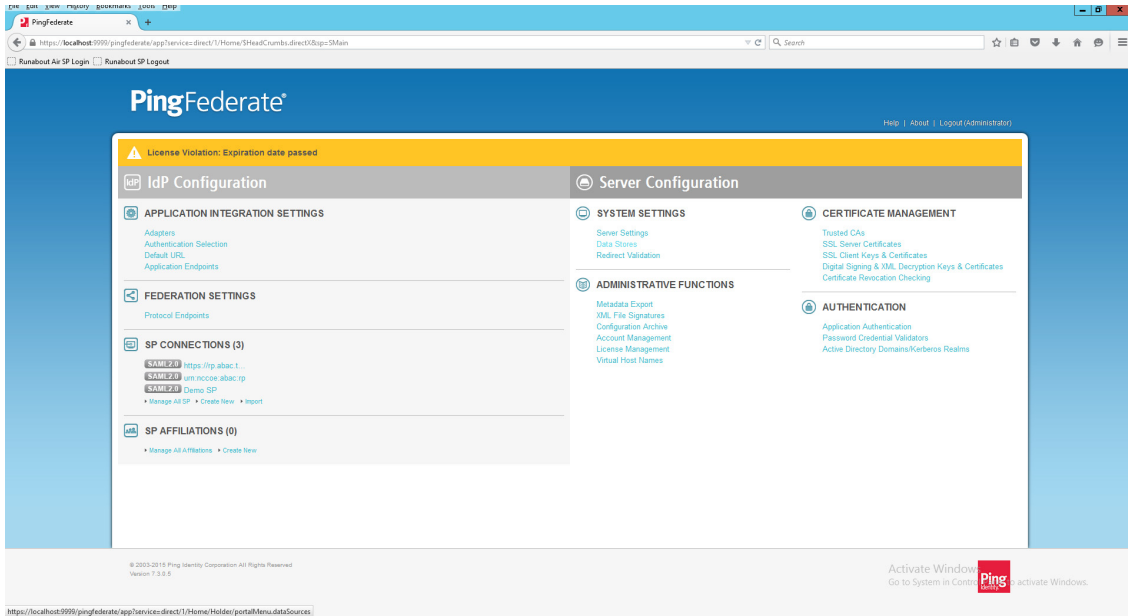
### 2988 6.3.2.1 Configuring a New Data Store that Connects to the RSA database

2989 Next, you will configure a new Data Store that connects to the **RSA\_CORE\_AA** database on the Identity  
 2990 Provider's PingFederate server. This new data store will be used in the RP Connection to query the  
 2991 EVENT\_LOG table during the authentication process.

2992 Follow the instructions below to create a new Data Store for the **RSA\_CORE\_AA** database.

- 2993 1. Launch your browser and go to *https://<DNS\_NAME>:9999/pingfederate/app*. Replace  
 2994 <DNS\_NAME> with the fully qualified name of the IdP's PingFederate server (e.g.,  
 2995 *https://idp.abac.test:9999/pingfederate/app*).
- 2996 2. Log on to the PingFederate application using the credentials you configured during installation.
- 2997 3. Under **Server configuration**, select **Data Stores**.



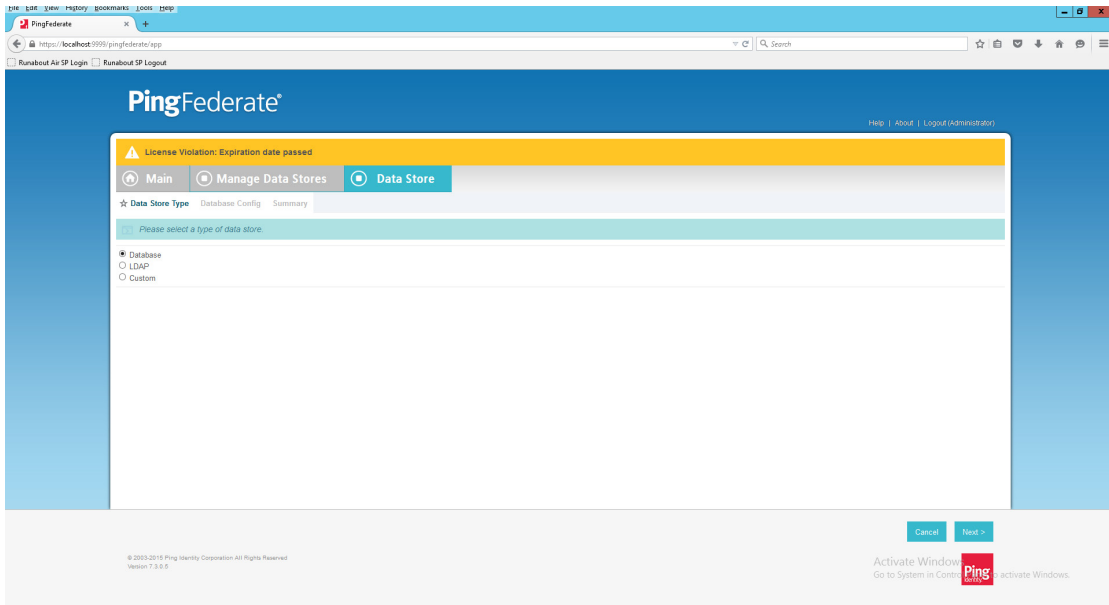


2998

2999

3000

4. Under **Manage data stores**, select **Add new data store**. Select **Database** as type of data store. Click **Next**.



3001

3002

3003

5. On the database config page, set the **JDBC URL** to:  
**jdbc:sqlserver://<RSA\_SERVER\_IP\_ADDRESS>:1433;databaseName=RSA\_CORE\_AA**

3004

3005

- a. Replace **<RSA\_SERVER\_IP\_ADDRESS >** with the IP address of the server that hosts the RSA\_CORE\_AA database.

3006

6. Set the driver class to **com.microsoft.sqlserver.jdbc.SQLServerDriver**

3007

3008

7. In the **Username** and **Password** fields, enter the credentials for the Ping user created in the SQL server RSA Database.

- 3009 8. Under **Validate Connection SQL**, type **SELECT 1=1**.
- 3010 9. Check the box to allow multi-value attributes. Click **Next**.

Please provide the details for configuring this database connection.

JDBC URL:  \*

Driver Class:  \*

Username:  \*

Password:  ⓘ

Validate Connection SQL:

Mask Values in Log

Allow Multi-Value Attributes

Advanced...

Cancel < Previous Next >

- 3011
- 3012 10. Review the settings on the summary page. Then, click **Save**.

Click a heading link to edit a configuration setting.

**Data Store**

**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

Cancel < Previous Done 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**  
 3018 **All SP**.

3019

3020

2. Click on the link for the SP connection created in [Section 2](#) (e.g., <https://rp.abac.test:9031>).

3021

3022

3023

3. On the **Activation & Summary** screen, scroll down to the **Assertion Creation** group and click on the **ATTRIBUTE CONTRACT** link.

The screenshot shows the 'Assertion Creation' interface. At the top, there are navigation tabs: 'Main', 'SP Connection', 'Browser SSO', and 'Assertion Creation' (which is active). Below these are sub-tabs: 'Identity Mapping', 'Attribute Contract' (active), 'Authentication Source Mapping', and 'Summary'. A teal banner contains the text: 'An Attribute Contract is a set of user attributes that this server will send in the assertion.' Below this, there are two sections: 'ATTRIBUTE CONTRACT' and 'SUBJECT NAME FORMAT'. The 'ATTRIBUTE CONTRACT' section has a 'SAML\_SUBJECT' field with a dropdown menu showing 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified'. The 'EXTEND THE CONTRACT' section is a table with columns 'ATTRIBUTE NAME FORMAT' and 'ACTION'. It contains one row with 'company' and 'urn:oasis:names:tc:SAML:2.0:attname-format:basic'. Below this table is an empty text field, a dropdown menu with 'urn:oasis:names:tc:SAML:2.0:attname-format:basic', and an 'Add' button. At the bottom right, there are buttons for 'Cancel', '< Previous', 'Next >', 'Done', and 'Save'.

3024

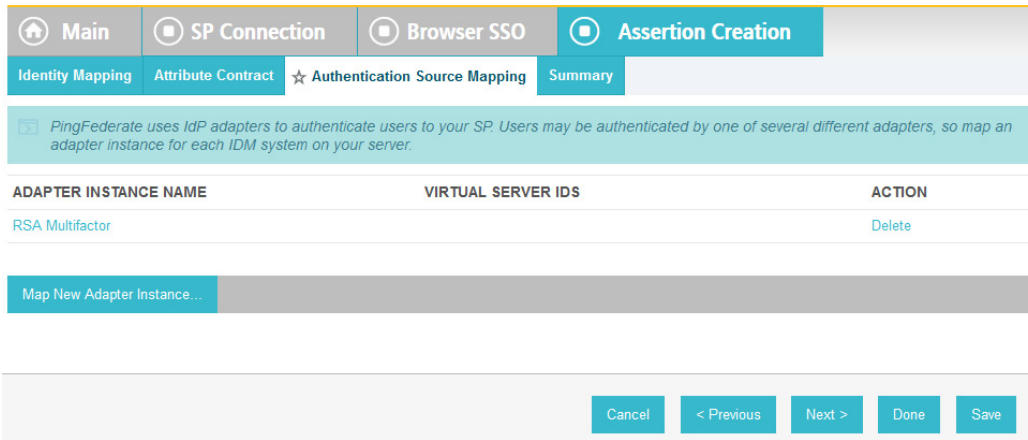
3025 4. On the **Attribute Contract** screen, under the **EXTEND THE CONTRACT** column, enter the name of  
 3026 the environmental attribute to be pulled from the RSA\_CORE\_AA database (e.g., **ip\_address**) in  
 3027 the empty text field.

3028 5. Click **Add**.

This screenshot is identical to the previous one, but the empty text field in the 'EXTEND THE CONTRACT' section now contains the text 'ip\_address'. The 'Add' button is still visible, and the rest of the interface remains the same.

3029

3030 6. Click **Next**.

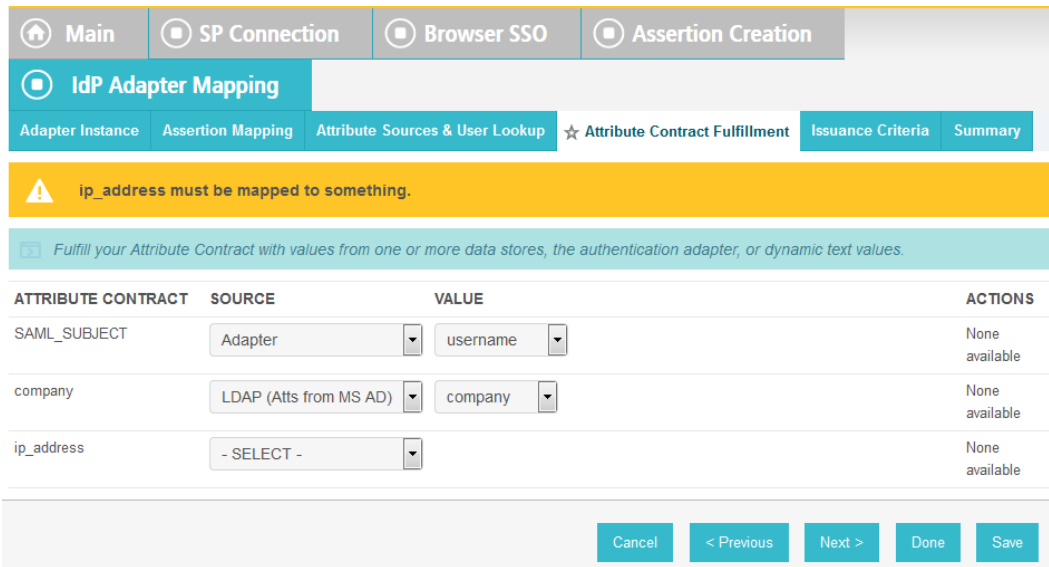


3031

3032

3033

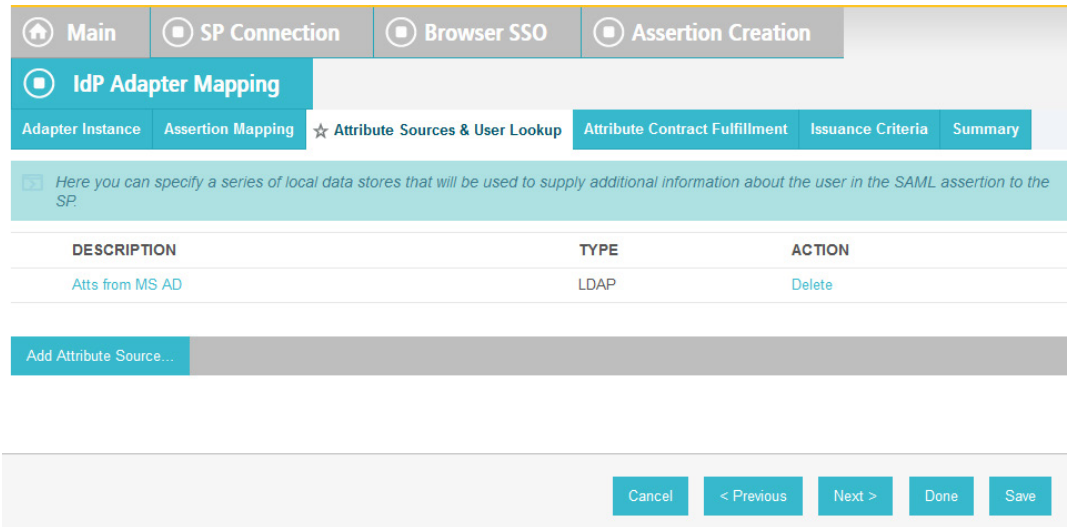
7. On the **Authentication Source Mapping** screen, click on the name of the **ADAPTER INSTANCE** (e.g., **RSA Multifactor**).



3034

3035

8. Click on the **Attribute Sources & User Lookup** tab.



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., **RSAAEventLog**).

3039

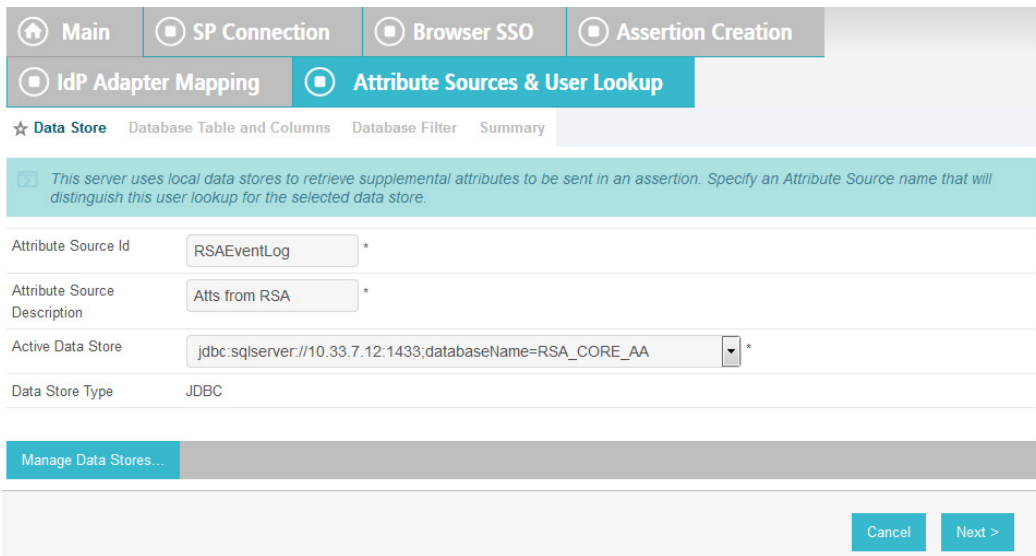
3040

11. Enter a description (e.g., **Atts from RSA**).

3041

12. For the **Active Data Store** field, select the existing Data Store that connects to the **RSA\_CORE\_AA** database.

3042



3043

13. Click **Next**.

3044

14. On the **Database Table and Columns** screen, select the **dbo** Schema.

3045

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**.

3048

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}'**

3054

3055 19. Click **Next**.

**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**.



The screenshot shows the 'Attribute Contract Fulfillment' screen in the 'IdP Adapter Mapping' section. A yellow warning banner at the top states: 'ip\_address does not have a value mapped.' Below this, a teal instruction box says: 'Fulfill your Attribute Contract with values from one or more data stores, the authentication adapter, or dynamic text values.' The main table lists attributes with their sources and values:

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

At the bottom, there are buttons for 'Cancel', '< Previous', 'Next >', 'Done', and 'Save'.

3060

22. On the **Attribute Contract Fulfillment** screen, for the **ip\_address** attribute, select the **SOURCE** and **VALUE**. For the **SOURCE**, select **JDBC (Atts from RSA)**. For **VALUE**, select **IP\_ADDRESS**.

3061

3062

This screenshot shows the same 'Attribute Contract Fulfillment' screen, but now the 'ip\_address' attribute is configured. The 'SOURCE' dropdown is set to 'JDBC (Atts from RSA)' and the 'VALUE' dropdown is set to '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

The buttons at the bottom remain the same: 'Cancel', '< Previous', 'Next >', 'Done', and 'Save'.

3063

23. Click **Save** to complete the configuration.

3064

### 6.3.2.3 Functional Test of Pulling Environmental Attributes during Authentication

3065

To test that the Identity Provider’s PingFederate server is successfully getting the environmental attributes during the authentication process, follow the instructions in the section Functional Test of Pulling User Attributes during Authentication. The only exception to those instructions is that when you examine the SAML message, you need to look for the environmental attribute that is being pulled from the RSA\_CORE\_AA database. See below for an example.

3066

3067

3068

3069

3070

1. Once you have the message open in the SAML tracer window, scroll down the message and locate the **AttributeStatement** node and sub-nodes.

3071

3072

http	Parameters	SAML
		<pre> &lt;/saml:Subject&gt; &lt;saml:Conditions NotBefore="2015-07-30T20:09:53.495Z"   NotOnOrAfter="2015-07-30T20:19:53.495Z"   &gt;   &lt;saml:AudienceRestriction&gt;     &lt;saml:Audience&gt;https://rp.abac.test:9031&lt;/saml:Audience&gt;   &lt;/saml:AudienceRestriction&gt; &lt;/saml:Conditions&gt; &lt;saml:AuthnStatement SessionIndex="xgoiCeKQSAr5Wzpm_tTuga.sZ1L"   AuthnInstant="2015-07-30T20:14:53.495Z"   &gt;   &lt;saml:AuthnContext&gt;     &lt;saml:AuthnContextClassRef&gt;urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified&lt;/saml:AuthnContextClassRef&gt;   &lt;/saml:AuthnContext&gt; &lt;/saml:AuthnStatement&gt; &lt;saml:AttributeStatement&gt;   &lt;saml:Attribute Name="company"     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"     &gt;     &lt;saml:AttributeValue xsi:type="xs:string"       xmlns:xs="http://www.w3.org/2001/XMLSchema"       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"       &gt;Conway Inc&lt;/saml:AttributeValue&gt;     &lt;/saml:Attribute&gt;     &lt;saml:Attribute Name="ip_address"       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"       &gt;       &lt;saml:AttributeValue xsi:type="xs:string"         xmlns:xs="http://www.w3.org/2001/XMLSchema"         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"         &gt;10.255.207.19&lt;/saml:AttributeValue&gt;       &lt;/saml:Attribute&gt;     &lt;/saml:AttributeStatement&gt;   &lt;/saml:Assertion&gt; &lt;/samlp:Response&gt; </pre>

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	
<b>IDENTITY MAPPING</b>	
Enable Account Mapping	true
<b>ATTRIBUTE CONTRACT</b>	
Attribute	SAML_SUBJECT
Attribute	stafflevel
<b>TARGET SESSION MAPPING</b>	
Connection mapping contract name	Sharepoint 2013
<b>CONNECTION MAPPING CONTRACT</b>	
Selected contract	Sharepoint 2013
<b>ATTRIBUTE RETRIEVAL</b>	
Attribute location	Use only the attributes available in the SSO Assertion
<b>CONTRACT FULFILLMENT</b>	
subject	SAML_SUBJECT (Assertion)
stafflevel	stafflevel (Assertion)
<b>ISSUANCE CRITERIA</b>	
Criterion	(None)
Protocol Settings	
<b>SSO SERVICE URLS</b>	
Endpoint	URL: /idp/SSO.saml2 (POST)
Endpoint	URL: /idp/SSO.saml2 (Redirect)

3094

3095

3096

3. On the **Activation & Summary** screen, scroll down to the **User-Session Creation** group and click on the **ATTRIBUTE CONTRACT** link.

Main	IdP Connection	Browser SSO	User-Session Creation
Identity Mapping	★ Attribute Contract	Target Session Mapping	Summary
<p><i>An Attribute Contract is a set of user attributes that the IdP will send in the assertion.</i></p>			
<b>ATTRIBUTE CONTRACT</b>			
SAML_SUBJECT			
<b>EXTEND THE CONTRACT</b>	<b>MASK VALUES IN LOG</b>	<b>ACTION</b>	
<input type="text"/>	<input type="checkbox"/>	<input type="button" value="Add"/>	
<p style="text-align: right;"> <input type="button" value="Cancel"/> <input type="button" value=" &lt; Previous"/> <input type="button" value=" Next &gt;"/> <input type="button" value=" Done"/> <input type="button" value=" Save"/> </p>			

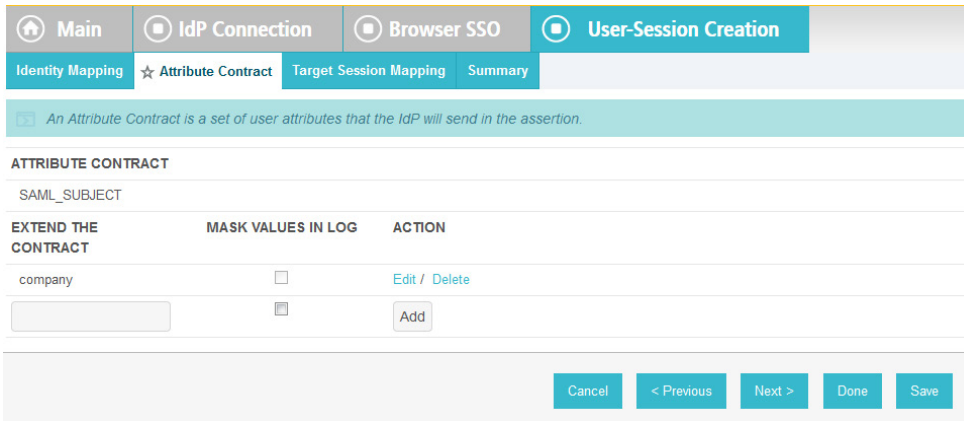
3097

3098

3099

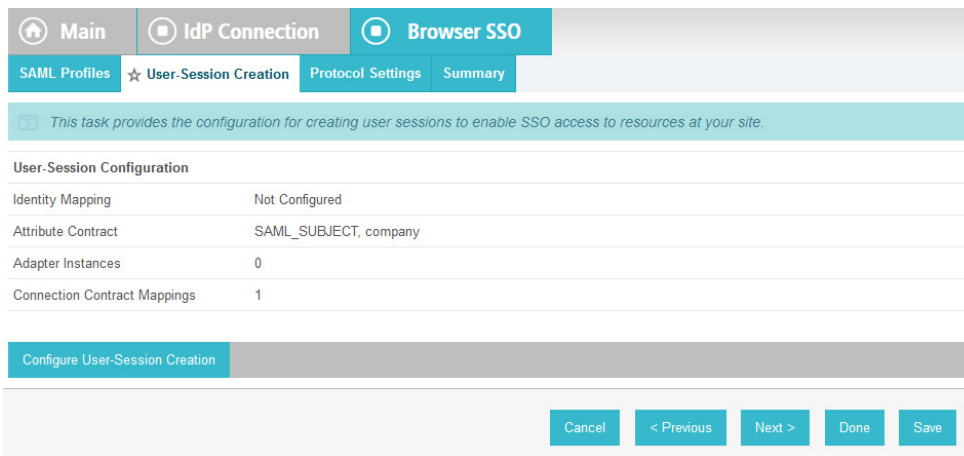
3100

4. On the **Attribute Contract** screen, under the **EXTEND THE CONTRACT** column, enter the name of the attribute to be pulled from the IdP's message (e.g., **company**) in the empty text field. In the **ACTION** column, click **Add**.



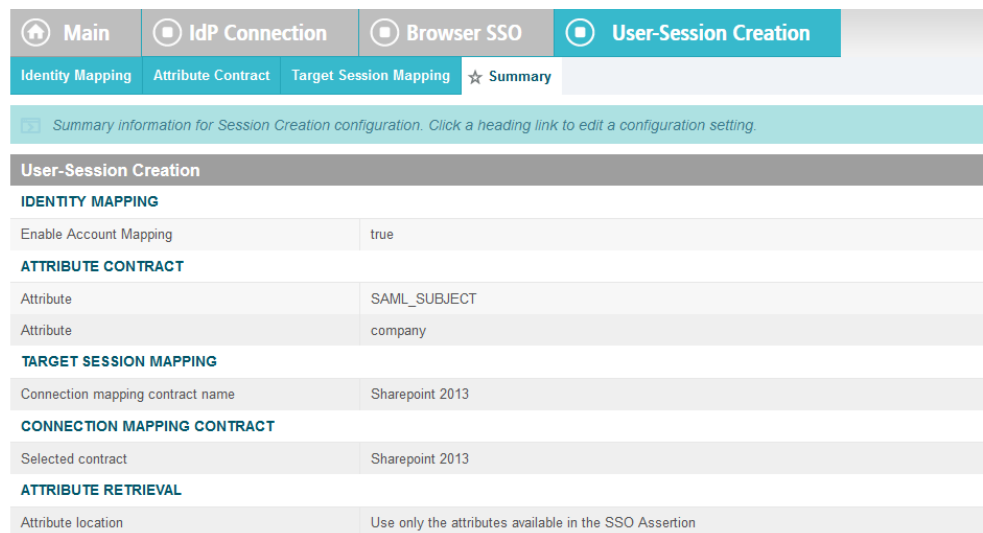
3101

3102 5. Click **Done**.



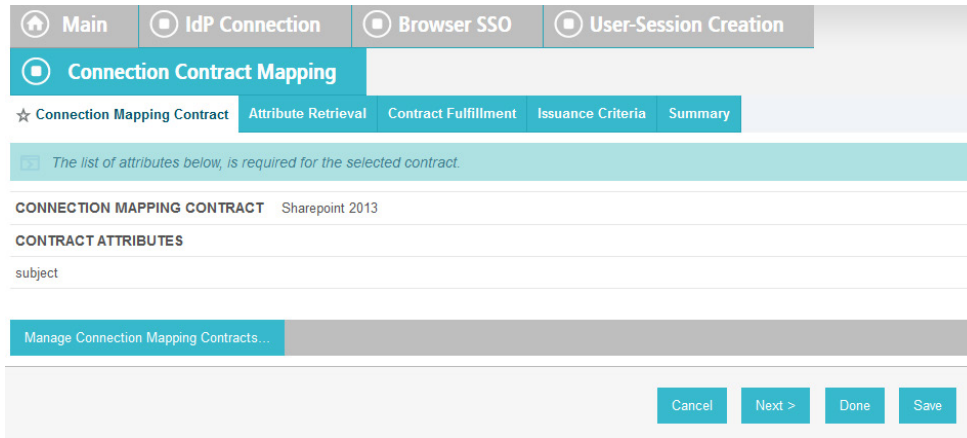
3103

3104 6. On the **User-Session Creation** screen, click **Configure User-Session Creation**.



3105

3106 7. On the **Summary** page, under **User-Session Creation**, click on the **CONNECTION MAPPING**  
3107 **CONTRACT** link.



3108

3109

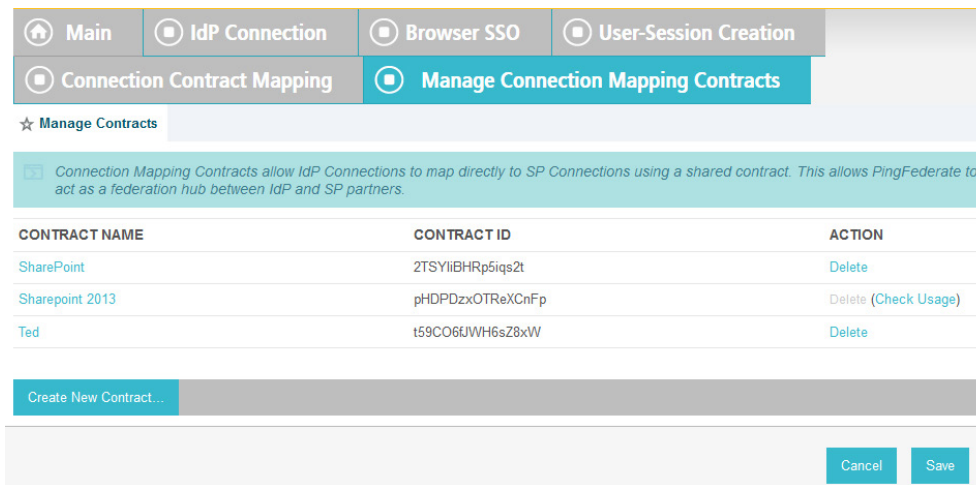
3110

3111

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**.

3112

9. Click on **Manage Connection Mapping Contracts**.

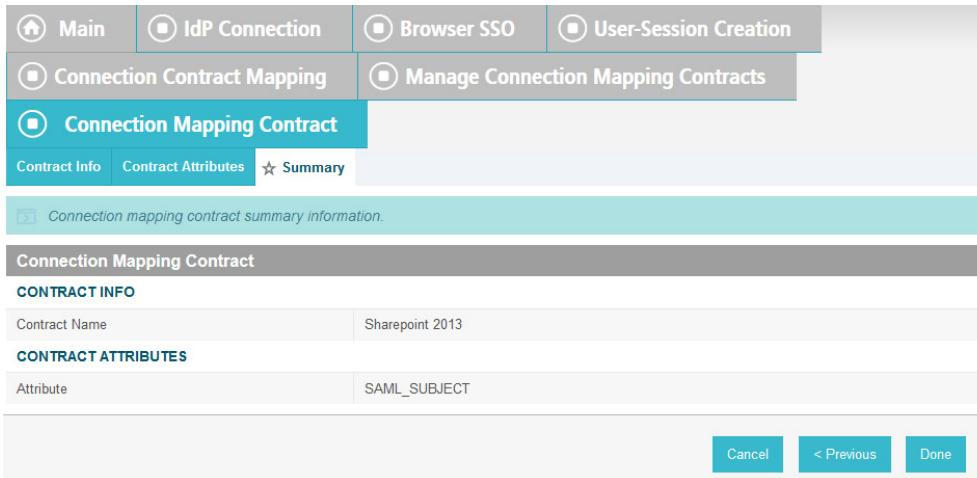


3113

3114

3115

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**).



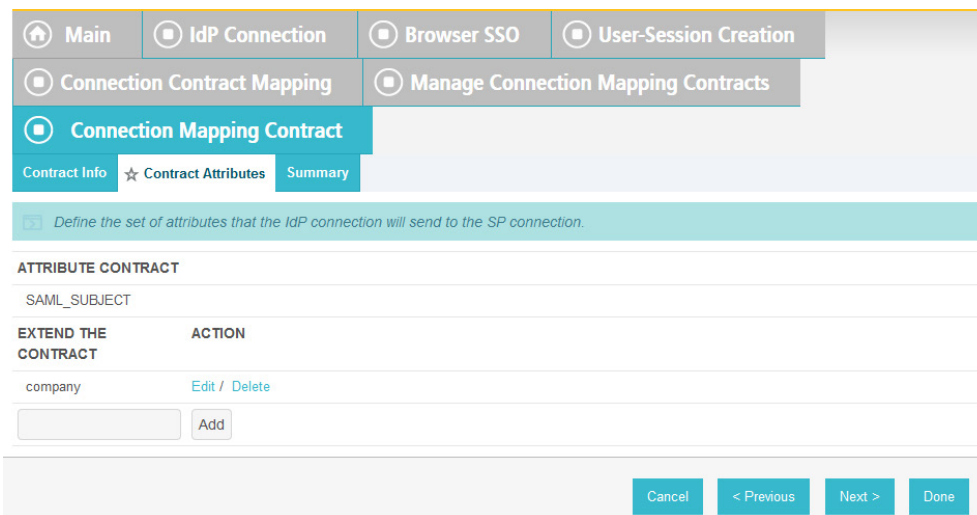
3116

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**.



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.

3126

3127 16. Click on the **Contract Fulfillment** tab.

CONNECTION MAPPING CONTRACT	SOURCE	VALUE	ACTIONS
company	- SELECT -		None available
subject	Assertion	SAML_SUBJECT	None available

At the bottom, there are navigation 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  
3130 the **SOURCE** field and select **company** for the **VALUE** field.

CONNECTION MAPPING CONTRACT	SOURCE	VALUE	ACTIONS
company	Assertion	company	None available
subject	Assertion	SAML_SUBJECT	None available

At the bottom, there are navigation 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	
<b>IDENTITY MAPPING</b>	
Name Identifier	User Principal Name
<b>ATTRIBUTE CONTRACT</b>	
Attribute	SAML_SUBJECT
Attribute	upn
Attribute Name Format	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
<b>AUTHENTICATION SOURCE MAPPING</b>	
Connection mapping contract name	Sharepoint 2013
<b>CONNECTION MAPPING CONTRACT</b>	
Selected contract	Sharepoint 2013
<b>ASSERTION MAPPING</b>	
Connection Mapping Contract	Sharepoint 2013
Data Store or Assertion	Use only the Connection Mapping Contract values in the SAML assertion
<b>ATTRIBUTE CONTRACT FULFILLMENT</b>	
upn	subject (Connection Mapping Contract)
SAML_SUBJECT	subject (Connection Mapping Contract)
<b>ISSUANCE CRITERIA</b>	
Criterion	(None)
Protocol Settings	
<b>SERVICE URL</b>	
Endpoint URL	/_trust/

- 3150
- 3151 6. Click on the **ATTRIBUTE CONTRACT** link. On the Attribute Contract screen, under the EXTEND  
3152 THE CONTRACT column, enter the name of the attribute (e.g., "company") to be passed from



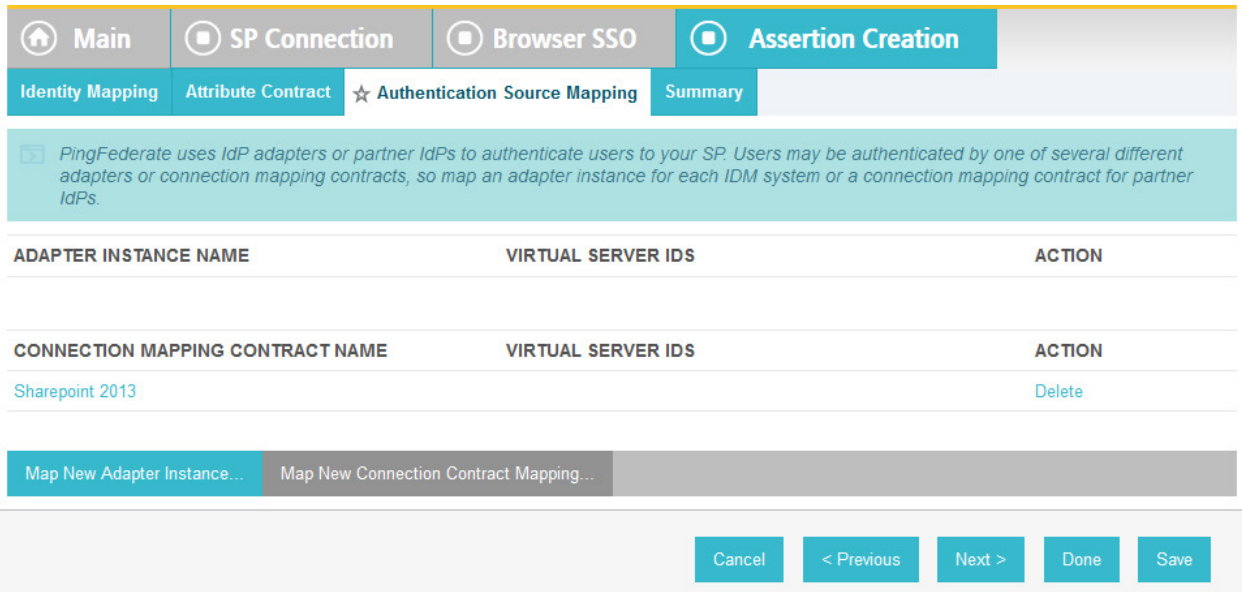
3153 the PingFederate-RP to SharePoint in the empty text field. For the ATTRIBUTE NAME FORMAT,  
 3154 select the schemas.xmlsoap.org 2005 identity claims format.

The screenshot shows the 'Assertion Creation' tab in a web application. The breadcrumb trail includes 'Main', 'SP Connection', 'Browser SSO', and 'Assertion Creation'. The sub-tab is 'Attribute Contract'. A teal banner contains the text: 'An Attribute Contract is a set of user attributes that this server will send in the assertion.' Below this, the 'ATTRIBUTE CONTRACT' section shows 'SAML\_SUBJECT' as 'SAML\_SUBJECT'. A table with columns 'EXTEND THE CONTRACT', 'ATTRIBUTE NAME FORMAT', and 'ACTION' is present. The table contains two rows: one for 'upn' with format 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims' and 'Edit / Delete' action; and one for 'company' with the same format and 'Add' action. Below the table is an input field with 'company' and a dropdown menu with the selected format 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims' and an 'Add' button. At the bottom right are buttons for 'Cancel', '< Previous', 'Next >', 'Done', and 'Save'.

3155  
 3156 7. Click **Add**.

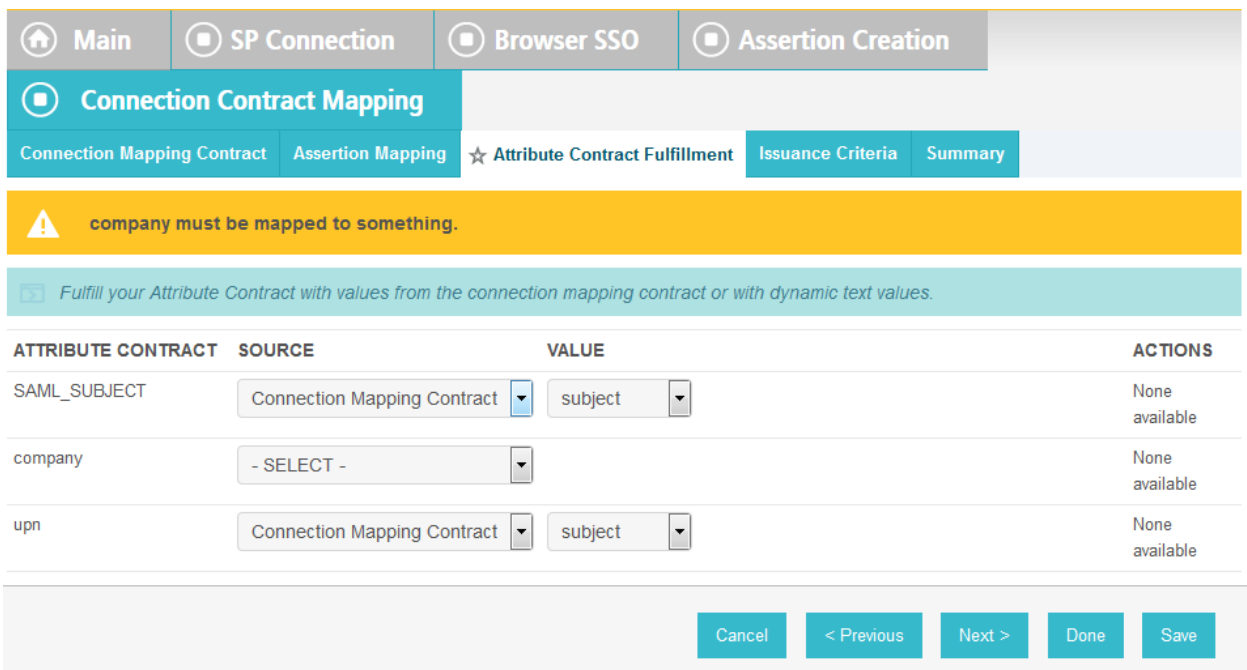
This screenshot is similar to the previous one but shows the state after clicking 'Add'. The 'company' entry is now listed in the table with 'Edit / Delete' action. The 'upn' entry is also present with 'Edit / Delete' action. The input field at the bottom is now empty, and the dropdown menu still shows the selected format 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims' with an 'Add' button. The navigation buttons at the bottom right remain the same.

3157  
 3158 8. Click **Done**.



3159

- 3160 9. On the Authentication Source Mapping screen, under the CONNECTION MAPPING CONTRACT
- 3161 NAME heading, click on the name of the connection mapping contract (e.g., SharePoint 2013)
- 3162 between this PingFederate SP connection and the PingFederate IdP connection that was
- 3163 configured in the earlier section, Configure Relying Party to Pull Attributes from the Identity
- 3164 Provider’s SAML Exchange.



3165

- 3166 10. On the Attribute Contract Fulfillment screen, for the “company” attribute, select **Connection**
- 3167 **Mapping Contract** for the SOURCE field. Select **company** for the VALUE field.

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

3168

3169 11. Click **Save** to complete the configuration.

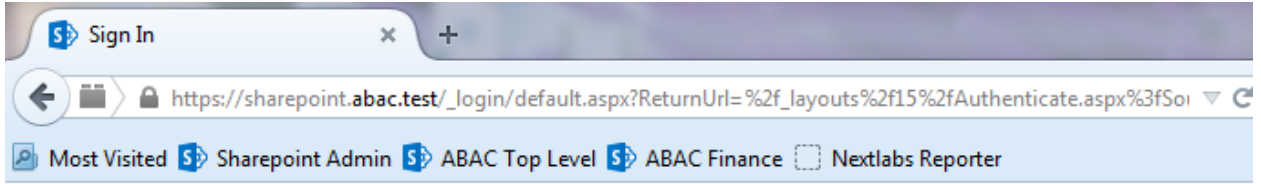
3170 *6.4.1.1 Functional Test of PingFederate-RP Passing Attributes to SharePoint*

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*).



# Sign In

Select the credentials you want to use to logon to this SharePoint site:

Windows Authentication  
Federated Logon from Identity Provider

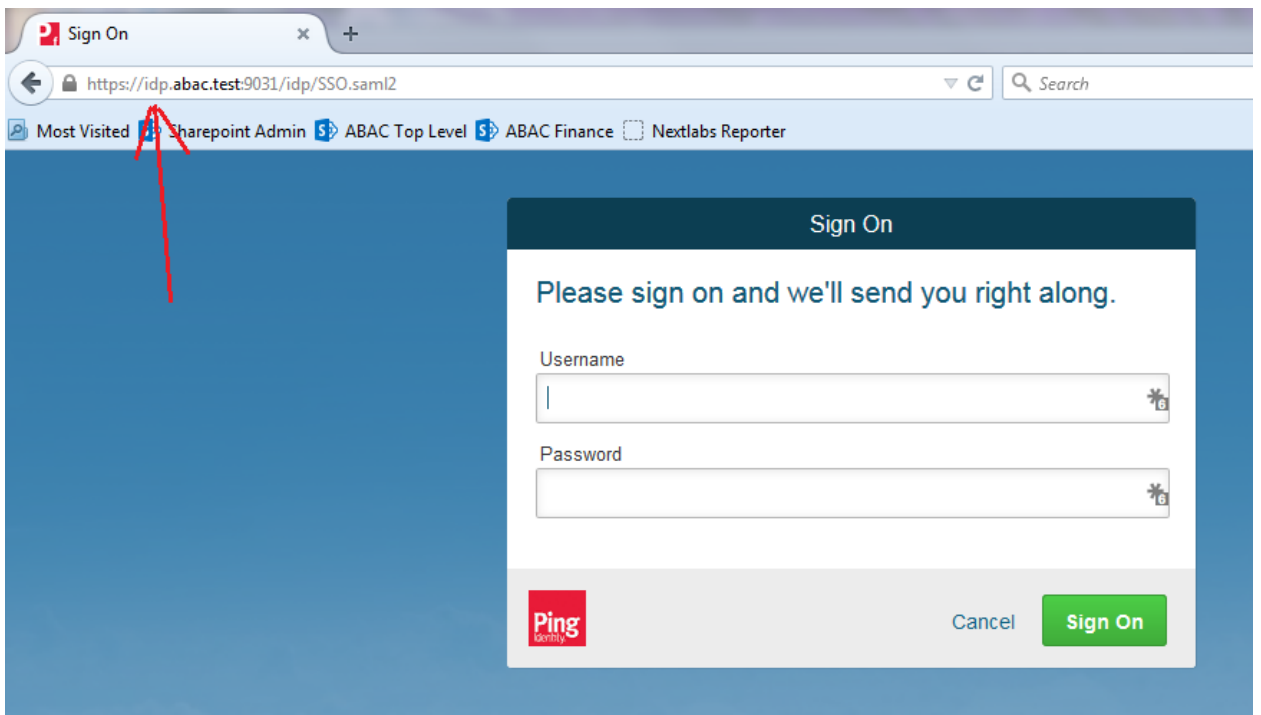
3179

3180

3181

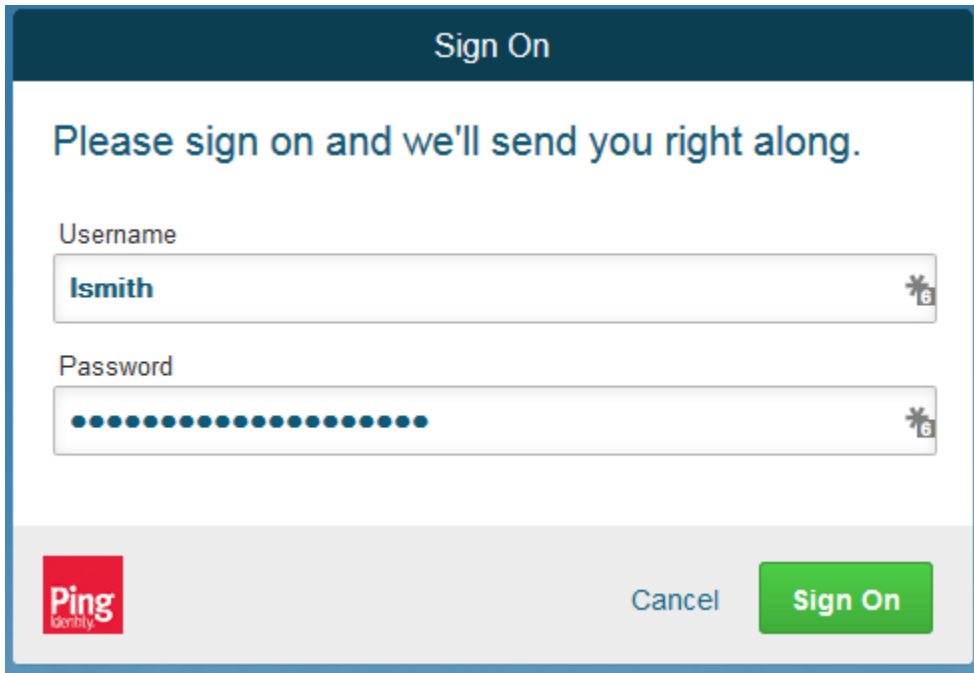
3182

3. Select the option to use the federated logon (e.g., Federated Logon from Identity Provider). Your browser should be redirected to the PingFederate-IdP, and you should see the PingFederate Sign On screen.

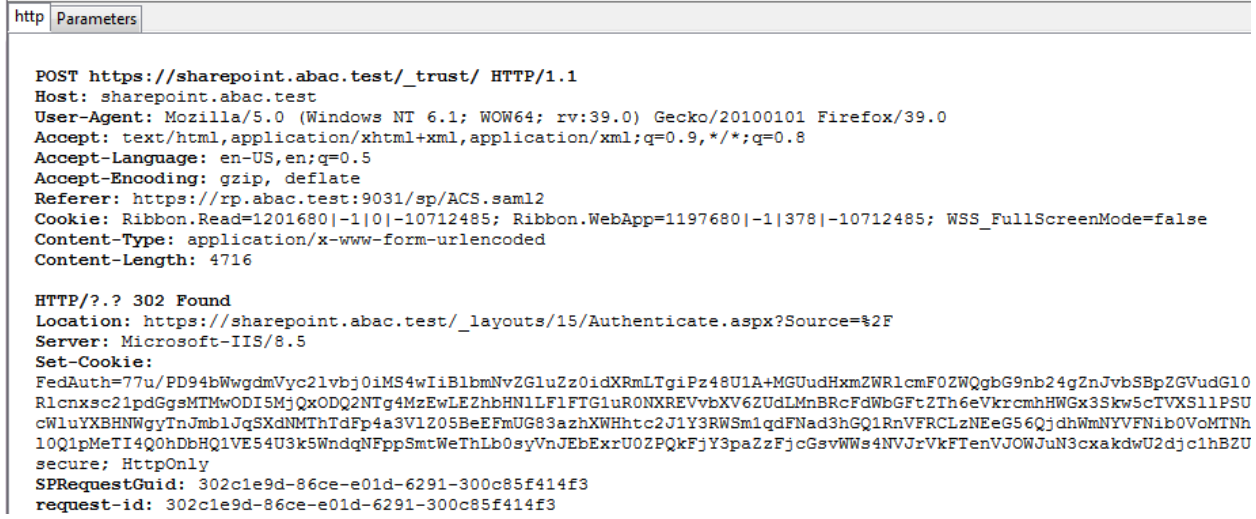
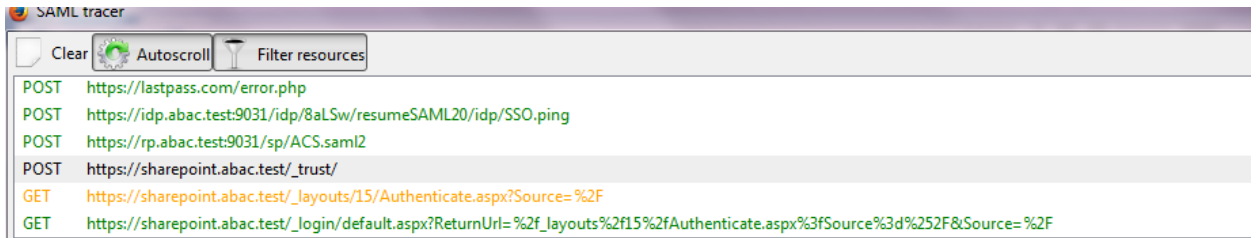


3183

- 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.



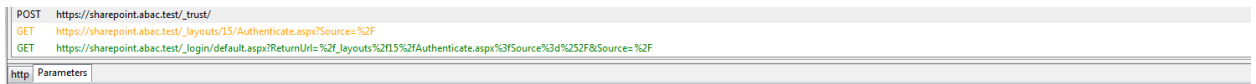
- 3187
- 3188 5. Click **Sign On**. On the RSA Adaptive Authentication screen, enter the SMS validation code  
 3189 received on your mobile phone. Click **Continue**.
- 3190 Once authenticated at the IdP, your browser should automatically redirect to the PingFederate-  
 3191 RP (e.g., *rp.abac.test*) 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.



3194

3195

7. Click on the **Parameters** tab for the bottom pane.



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.

```

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-
07-27T17:31:21.439Z"+NotOnOrAfter="2015-07-
27T17:41:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint.abac.test</saml:Audience></saml:AudienceRestri
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:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">Ismith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:A
ttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">Ismith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="upn"+AttributeNameNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Ismith</saml
:AttributeValue></saml:Attribute><saml:Attribute
+AttributeName="company"+AttributeNameNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Conway
+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="#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/xmenc#sha256"/>
<ds:DigestValue>K/L27oIUIkwY3xiqbfGvb3oqJLPArDO5A9W/zf7WA5k=</ds:DigestValue>

```

3199

3200 9. Scroll down the SAML message and locate the AttributeStatement node and sub-nodes.

```

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-
07-27T17:31:21.439Z"+NotOnOrAfter="2015-07-
27T17:41:21.439Z"><saml:AudienceRestrictionCondition><saml:Audience>urn:sharepoint.abac.test</saml:Audience></saml:AudienceRestri
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:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">Ismith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:A
ttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">Ismith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="upn"+AttributeNameNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Ismith</saml
:AttributeValue></saml:Attribute><saml:Attribute
+AttributeName="company"+AttributeNameNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Conway
+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="#n27qL60V17N_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: 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_XX8QLxKdFLG11CM"+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:Au
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
dentifier+Format="http://schemas.xmlsoap.org/claims/UPN">Ismith</saml:NameIdentifier></saml:Subject></saml:AuthenticationState
ment></saml:AuthenticationStatement></wst:RequestedSecurityToken></wst:RequestSecurityTokenResponse>

<saml:AttributeStatement>
<saml:Subject>
<saml:NameIdentifier+Format="http://schemas.xmlsoap.org/claims/UPN">Ismith</saml:NameIdentifier></saml:Subject>

<saml:Attribute+AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
<saml:AttributeValue>Ismith</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

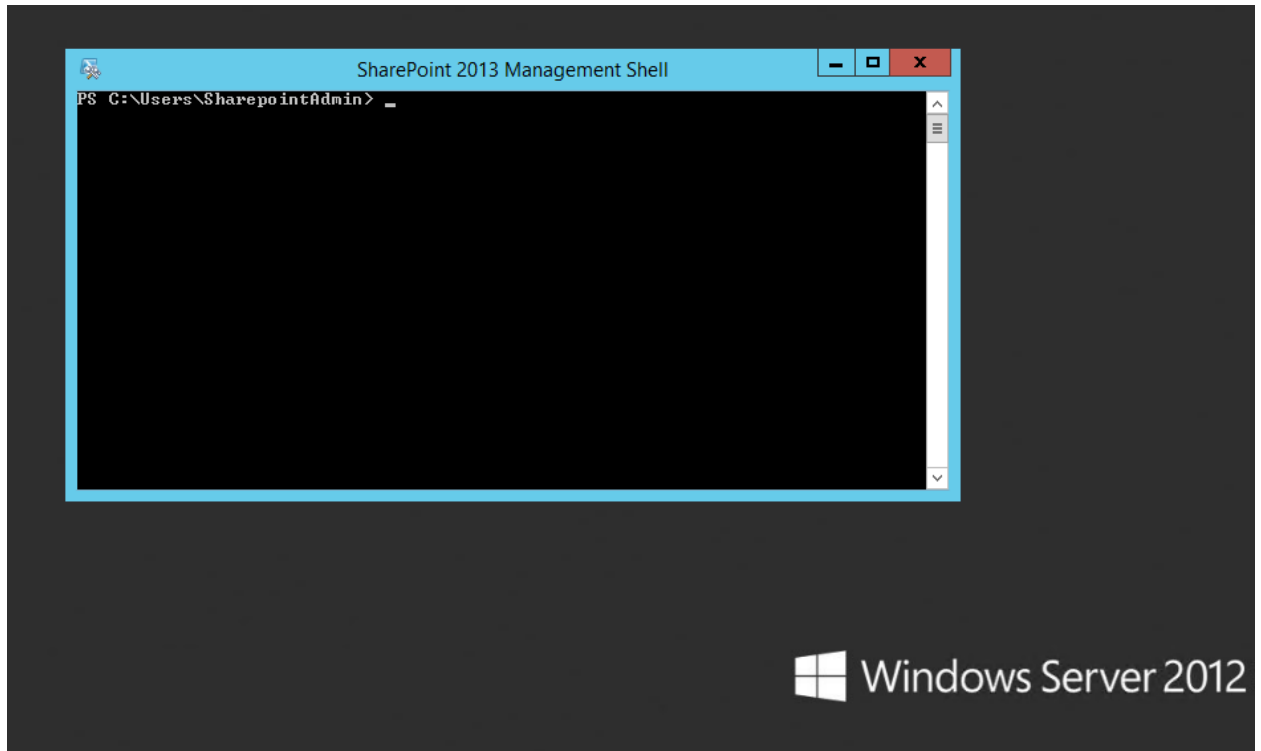
3206 Expected Result: Within the AttributeStatement node, there should be multiple Attribute sub-  
3207 nodes. There should be an Attribute sub-node that has an AttributeName value of “company.”  
3208 The AttributeNamespace value should be  
3209 *http://schemas.xmlsoap.org/ws/2005/05/identity/claims*. There should be an AttributeValue  
3210 sub-node, which should contain the expected value (e.g., Conway Inc) for the “company”  
3211 attribute that was pulled from Microsoft AD (e.g., <saml:AttributeValue> Conway+Inc  
3212 </saml:AttributeValue>) for the specific user (e.g., Ismith) who authenticated at the Sign On  
3213 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 -Identity "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> _

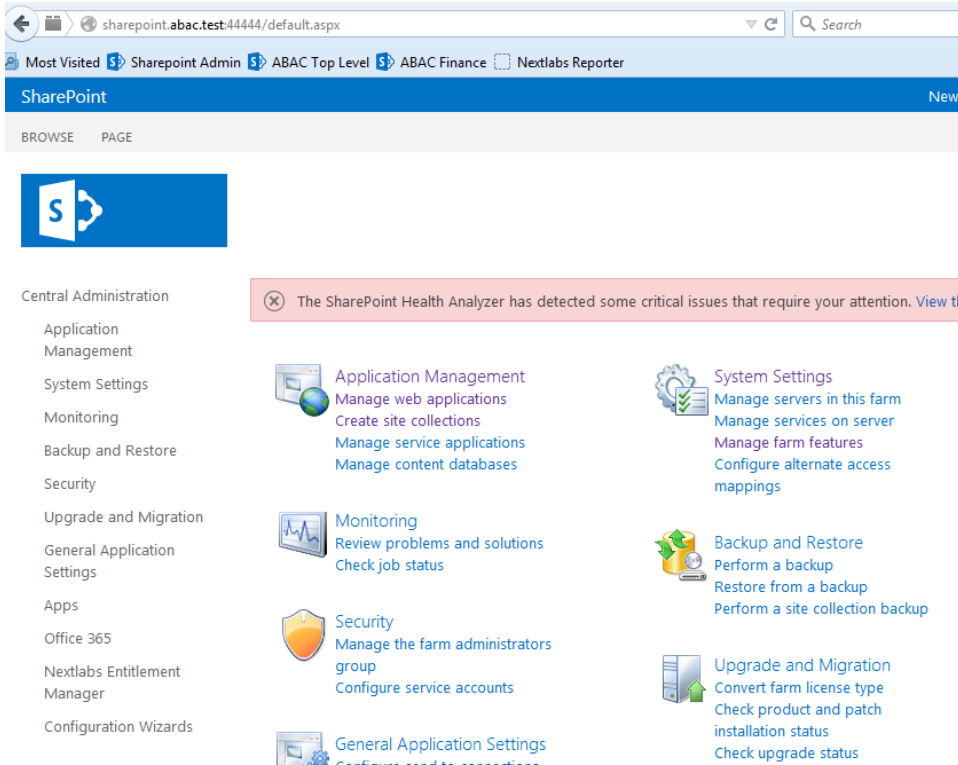
```

3237

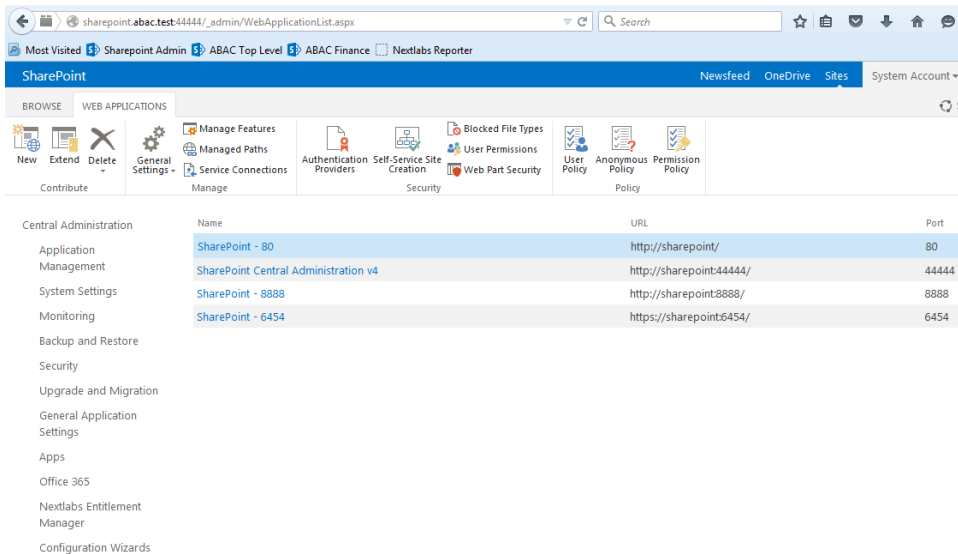
#### 3238 *6.4.2.1 Functional Test of SharePoint Reading Attributes from PingFederate-RP*

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.

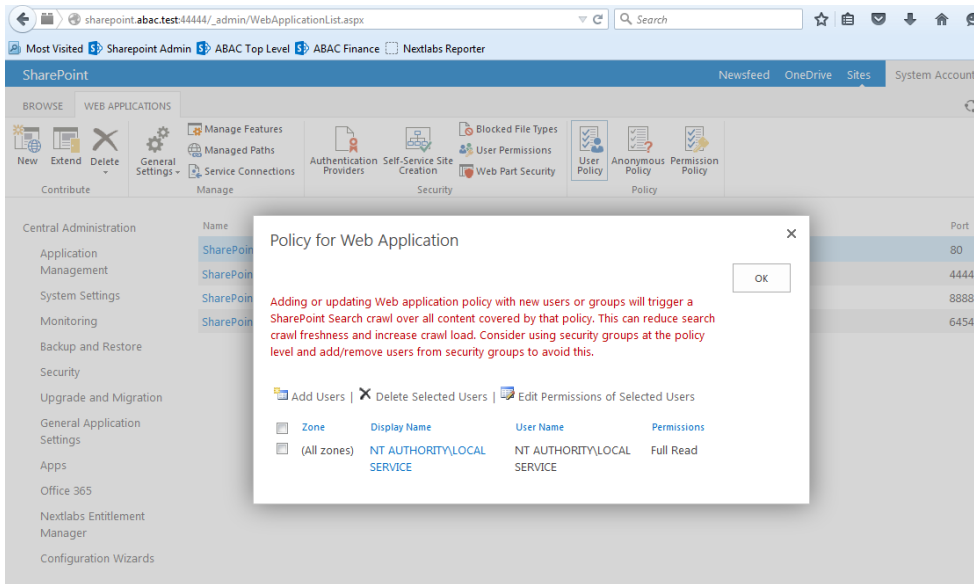
- 3241 1. First, follow the instructions in this section to ensure that SharePoint is configured to read the  
 3242 newly configured attributes from PingFederate-RP.
- 3243 2. Launch your browser and go the SharePoint central administration page (e.g.,  
 3244 <http://SharePoint.abac.test:44444/default.aspx>).
- 3245 3. Log on using the credentials of the SharePoint administrator.



- 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.,
- 3249 **SharePoint – 80**). SharePoint highlights the web application row that you clicked.



- 3250
- 3251 6. Click **User Policy**.



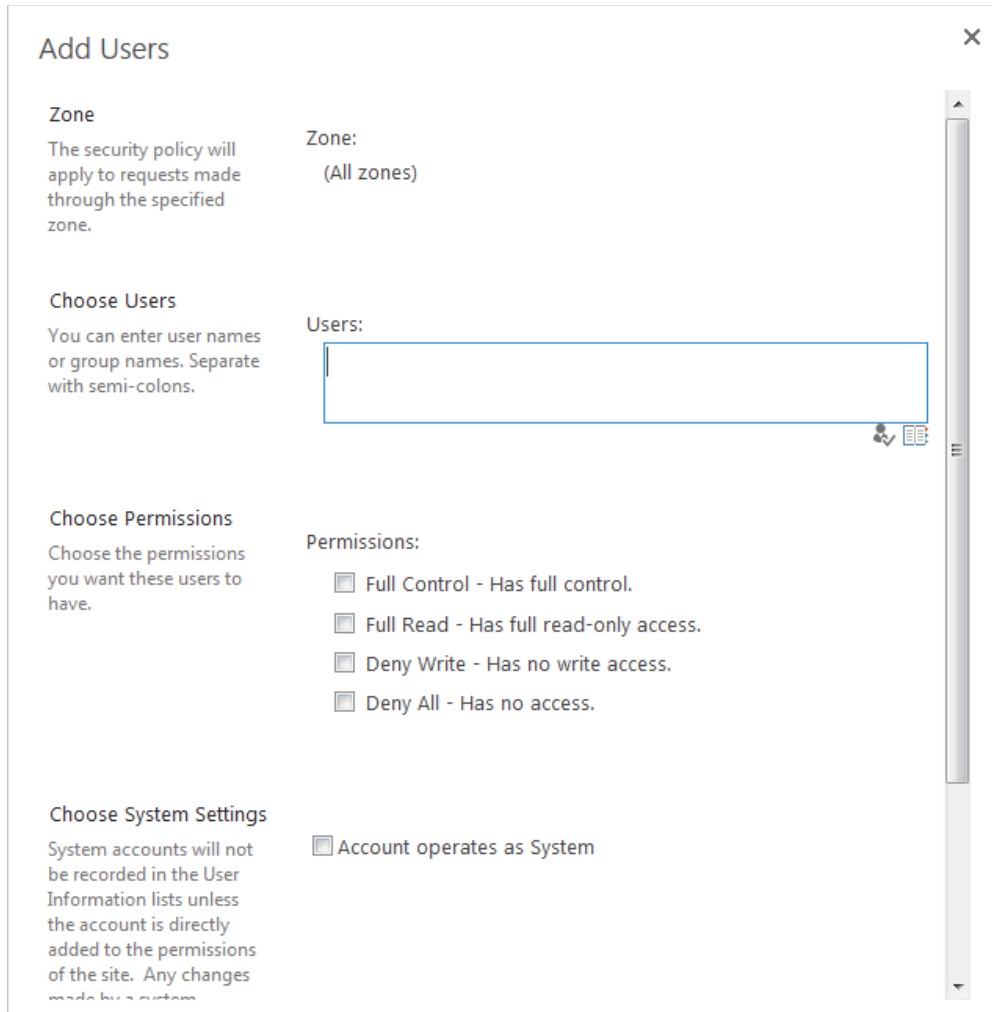
3252

3253 7. Click the **Add users** link.



3254

3255 8. Click **Next**.



3256

3257

3258

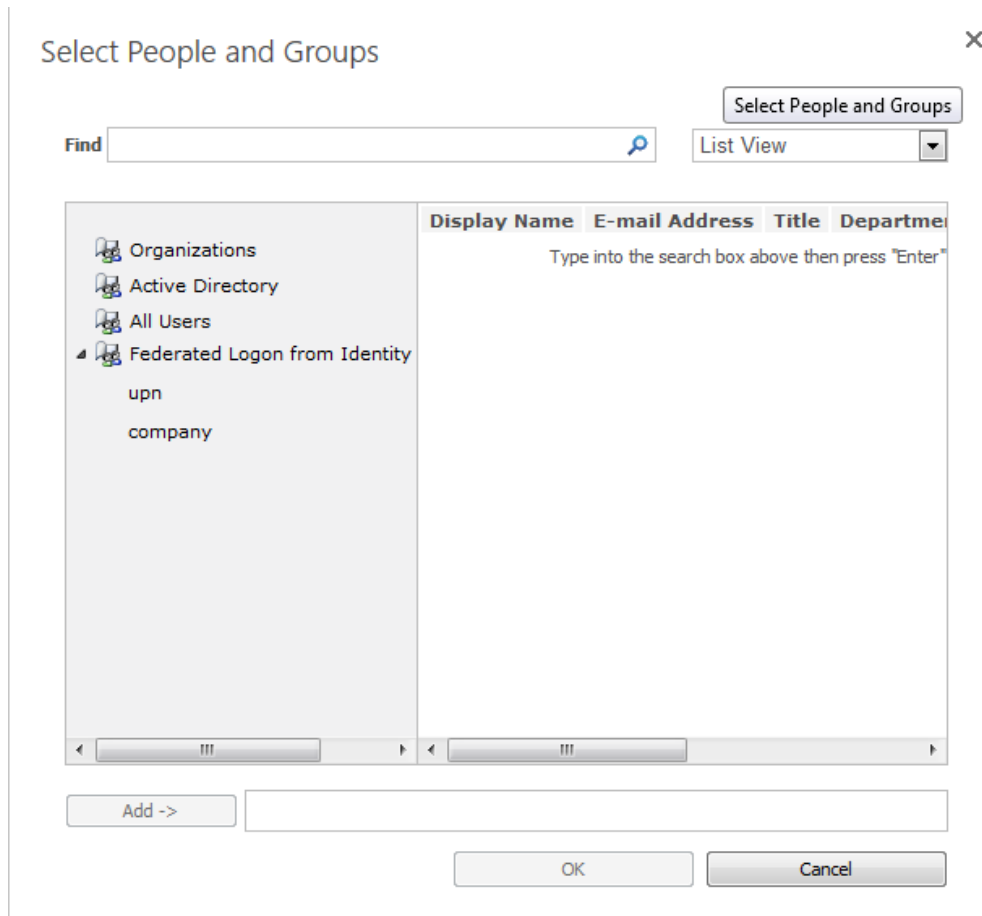
9. On the **Add Users** screen, click the small browse icon (looks like an open book) under the **Users** field.

3259

3260

3261

Expected Result: On the Select People and Groups screen, you should see a grouping with the name of the trusted token issuer (e.g., Federated Logon from Identity Provider). You should also see the newly configured attribute (e.g., company) listed under that grouping.



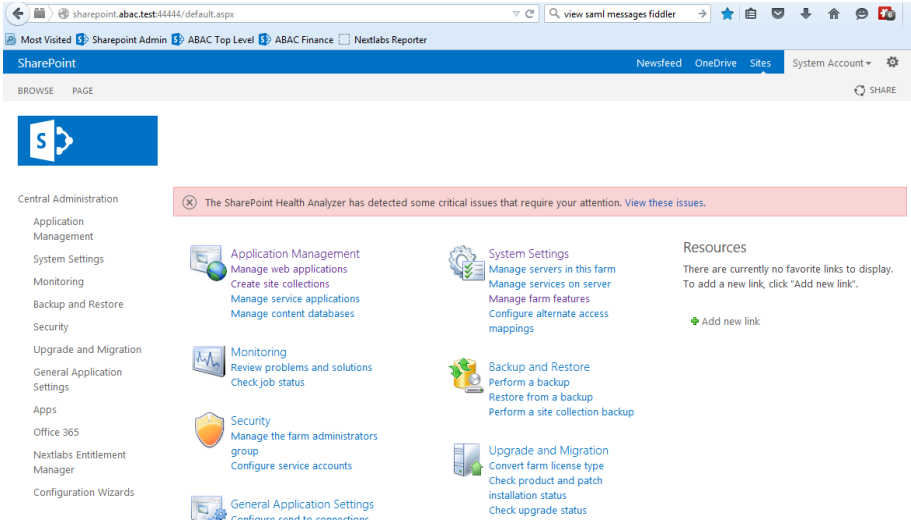
3262

## 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.

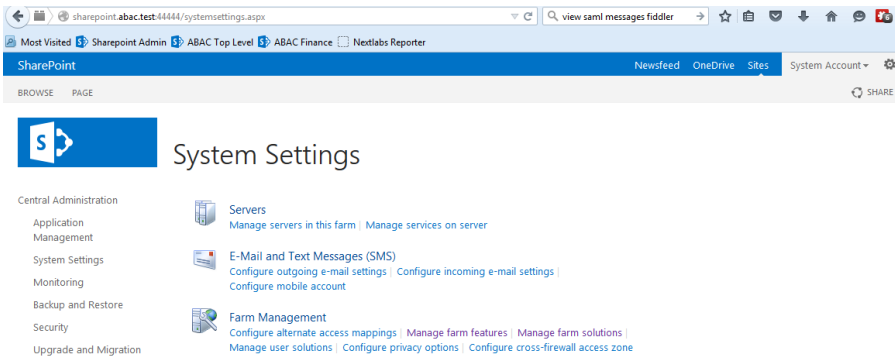
- 3269 1. Log on to the server that hosts SharePoint for the RP.
- 3270 2. Launch your browser and go the SharePoint central administration page (e.g.,  
 3271 <http://SharePoint.abac.test:44444/default.aspx>). Log on using the credentials of the SharePoint  
 3272 administrator.

3273 The central administration home page displays.



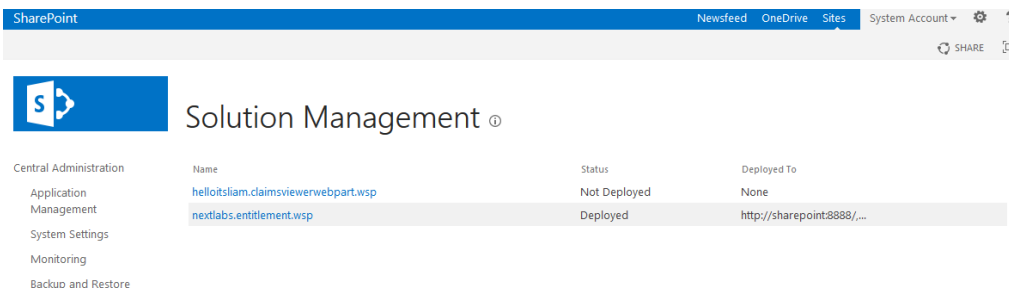
3274

3275 3. On the **Central Administration** menu on the left, click **System Settings**.



3276

3277 4. On the **Farm Management** menu, click **Manage Farm Solutions**.



3278

3279 5. Click on the **helloitsliam.claimsviewerwebpart.wsp** link.

SharePoint Newsfeed OneDrive Sites Sys

## 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: helloitslam.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.

Last Operation Details: 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 Time: 7/20/2015 7:08 PM

3280

3281

6. Click on the **Deploy Solution** link at the top of the page.

## Deploy Solution

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: helloitslam.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:

All content Web applications

**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

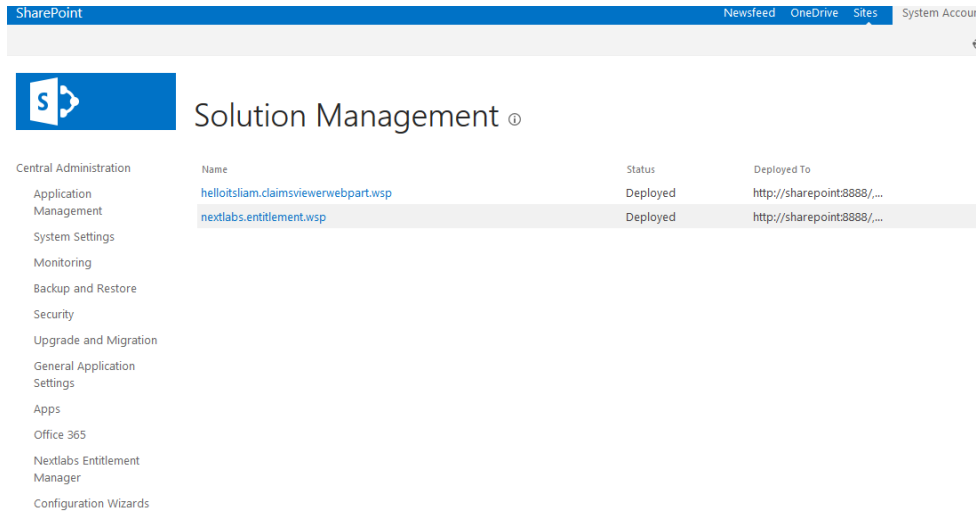
3283

3284

7. Click **OK** at the bottom of the page.

The claimsviewerwebpart should be shown as deployed on the **Solution Management** page.





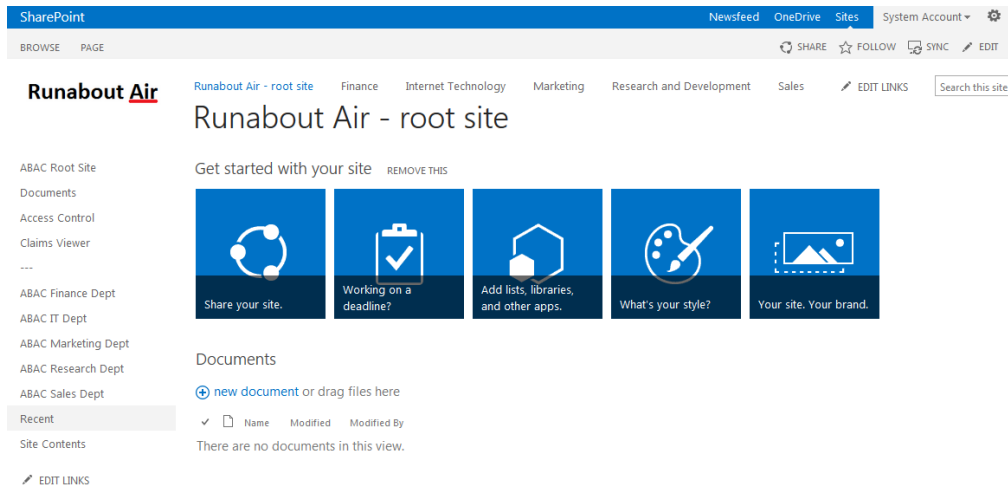
3285

3286 This completes the portion of the claims viewer web part configuration at the SharePoint central  
 3287 administration page.

3288 *6.5.1.1 Configure SharePoint Claims Viewer*

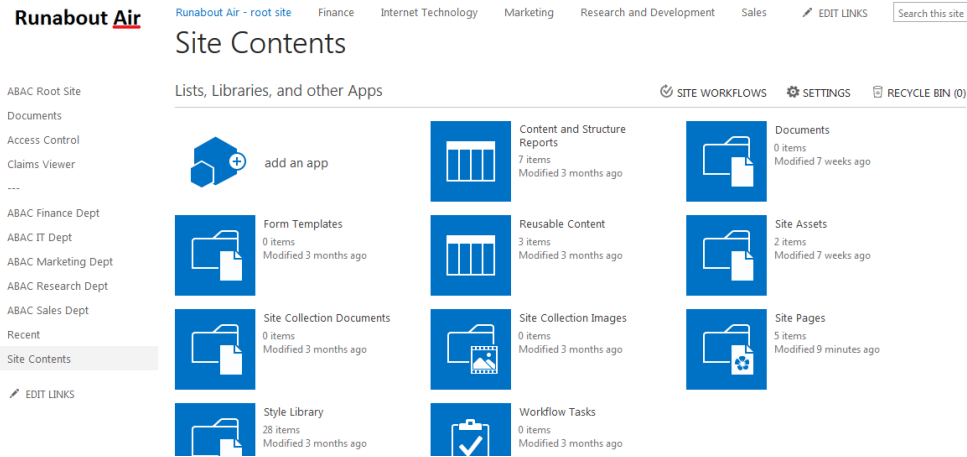
3289 This section explains how to add a new page to the SharePoint site to view the claims.

- 3290 1. Log on to the RP’s SharePoint site (e.g., *https://SharePoint.abac.test*) using the credentials of the  
 3291 SharePoint administrator. Select **Windows Authentication** at the Sign On screen.



3292

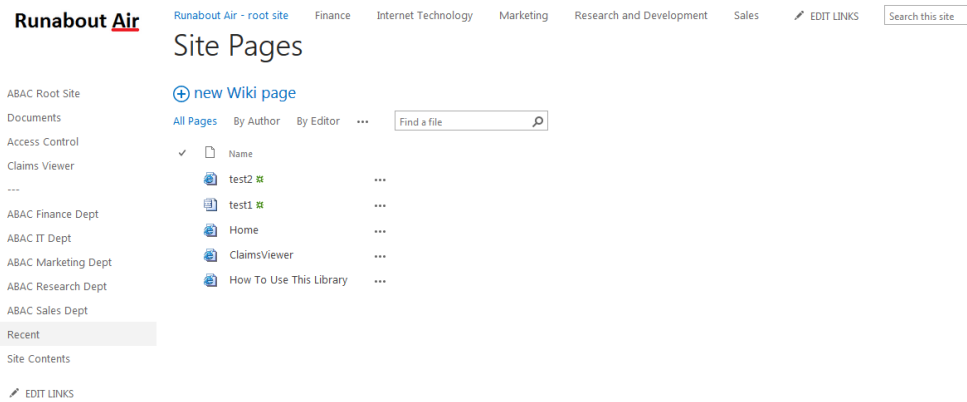
- 3293 2. Click the gear icon at the top right corner of the page and select the **Site Contents** link.



3294

3295

3. Click on the Site Pages library. This will show a list of the existing pages on the site.

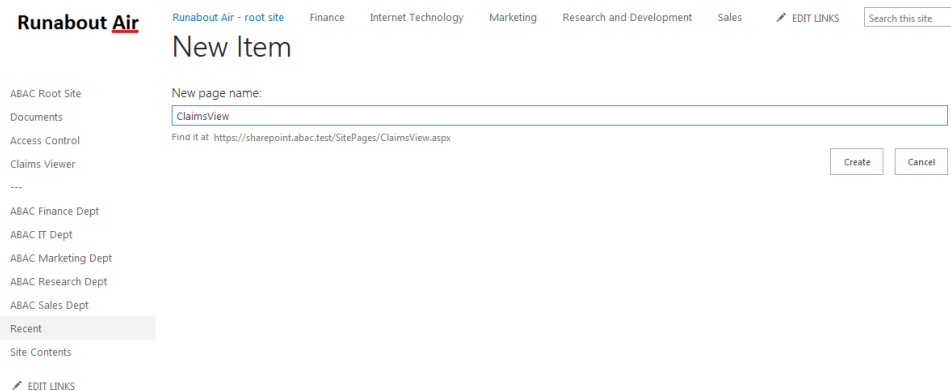


3296

3297

3298

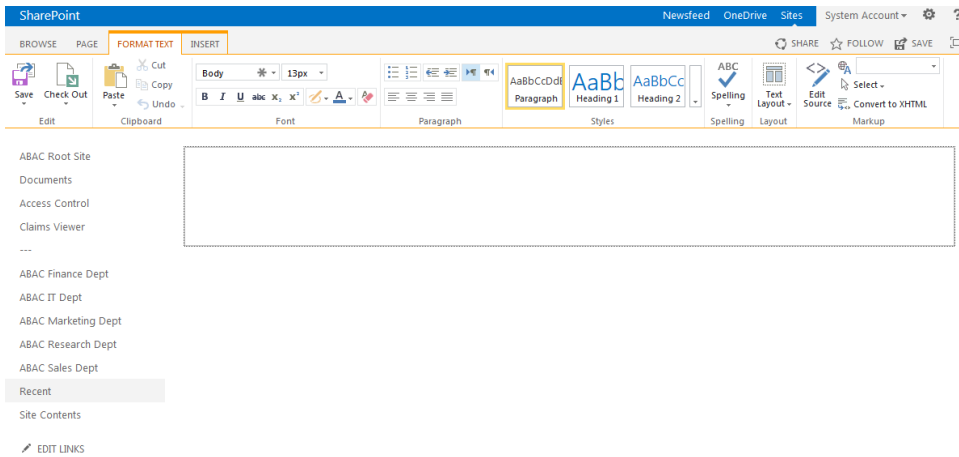
4. Click the new Wiki page link to add a new page. This link may be named differently, depending on your site's SharePoint template. Enter a name for the new page (e.g., ClaimsView).



3299

3300

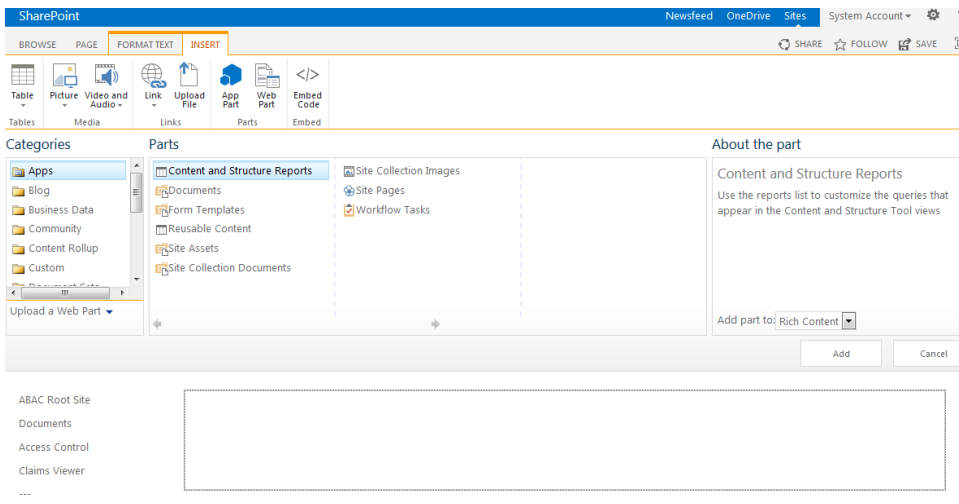
5. Click **Create**. The SharePoint page editor for the newly added page displays.



3301

3302

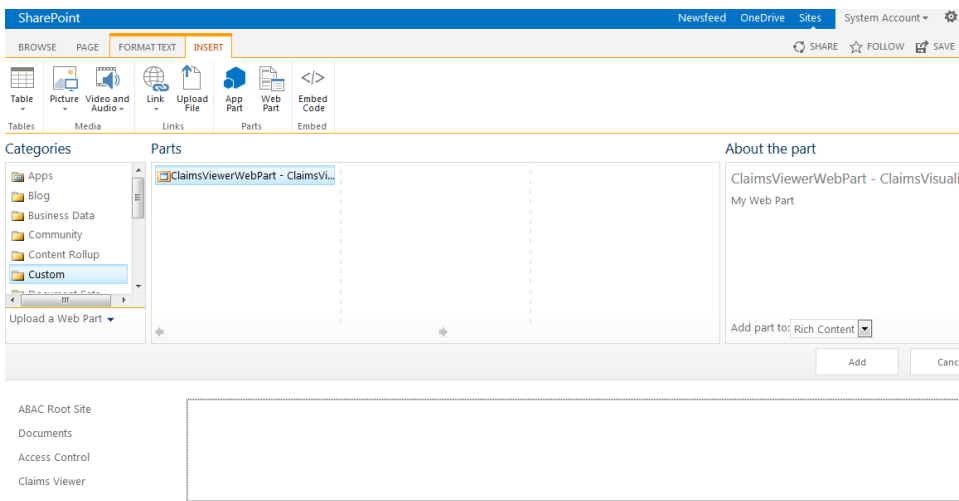
6. Click on the **INSERT** tab at the top of the page. Click on the **Web Part** button.



3303

3304

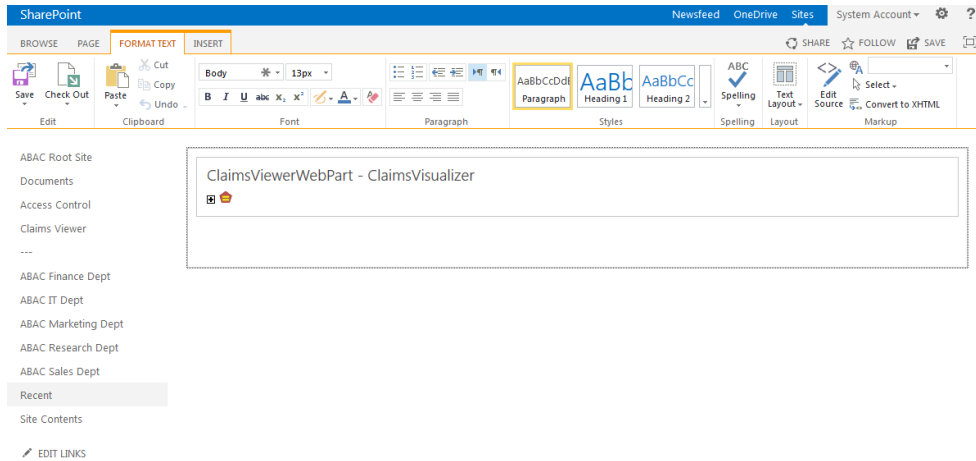
7. In the **Categories** list, select **Custom**. In the **Parts** list, select **ClaimsViewerWebPart**.



3305

3306

8. Click **Add**.

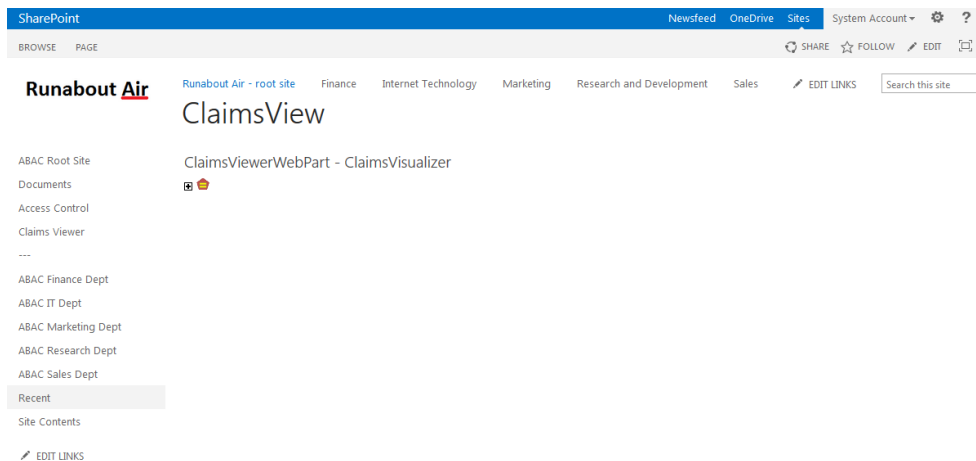


3307

3308 9. Click the **SAVE** button at the top right corner of the page.

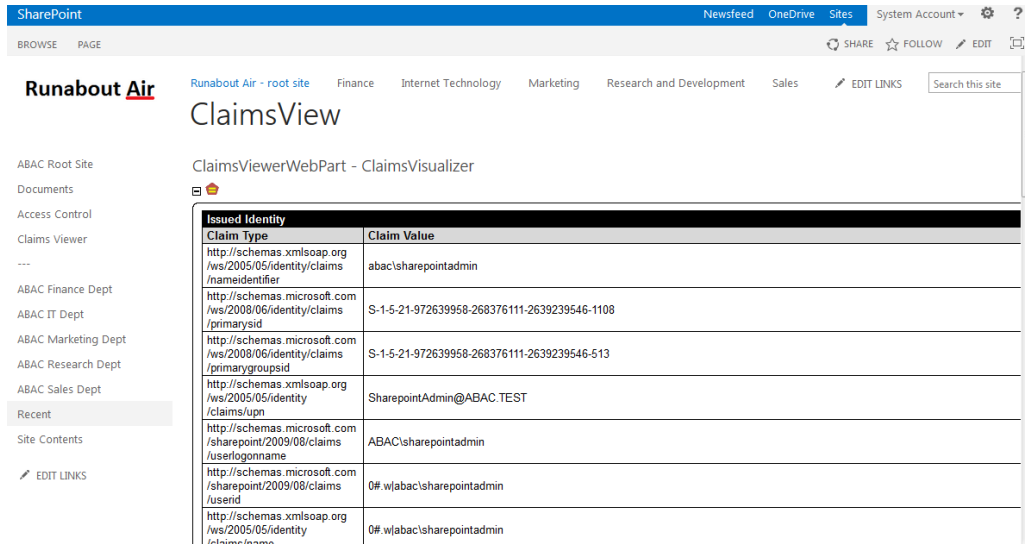
3309 SharePoint launches the new page (e.g., ClaimsView) that was just created. Save the URL of the  
3310 new page (e.g., <https://SharePoint.abac.test/SitePages/ClaimsView.aspx>), because you will use  
3311 it later in a functional test.)

3312 The Claims Viewer Web Part on the page displays. It is collapsed by default.



3313

3314 10. Click on the **+** sign under **ClaimsViewerWebPart** to view the claims data. You will see a list of  
3315 claim values and information about the SAML token at the bottom of the page.

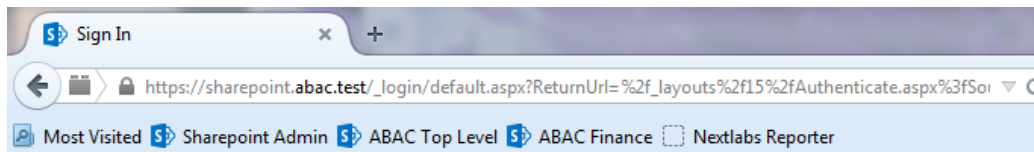


3316

## 3317 6.6 Functional Test of All Configurations for Section 6

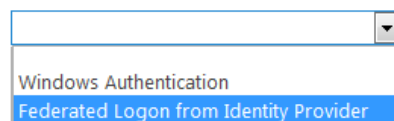
3318 The instructions in this section will perform an integrated test all of the configurations in Section 6.  
 3319 Using the browser, you will log on using an account that was created in Microsoft AD. Then you will use  
 3320 the SharePoint claims viewer to validate that the newly configured attributes 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

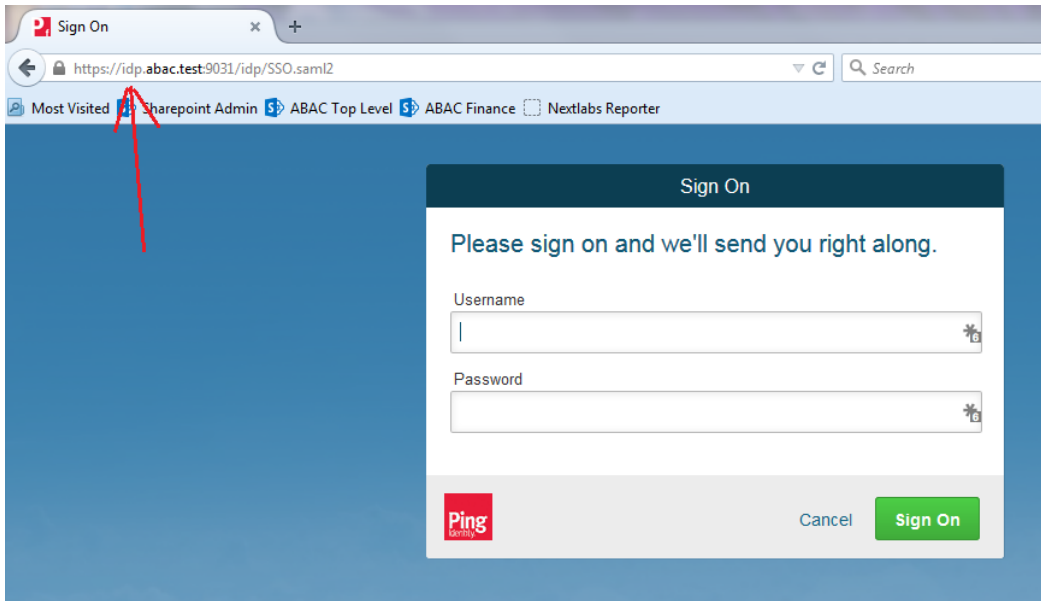
Select the credentials you want to use to logon to this SharePoint site:



3323

- 3324 2. Select **Federated Logon from Identity Provider**.

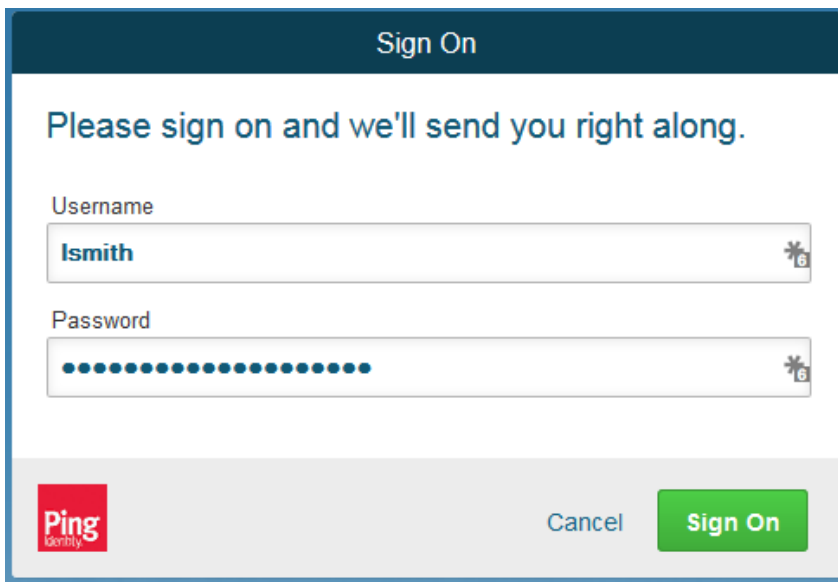
3325 Your browser is redirected to the PingFederate-IdP, and you see the PingFederate Sign On  
 3326 screen.



3327

3328

3. Enter the credentials of the Microsoft AD account created earlier in this guide (e.g., **lsmith**).



3329

3330

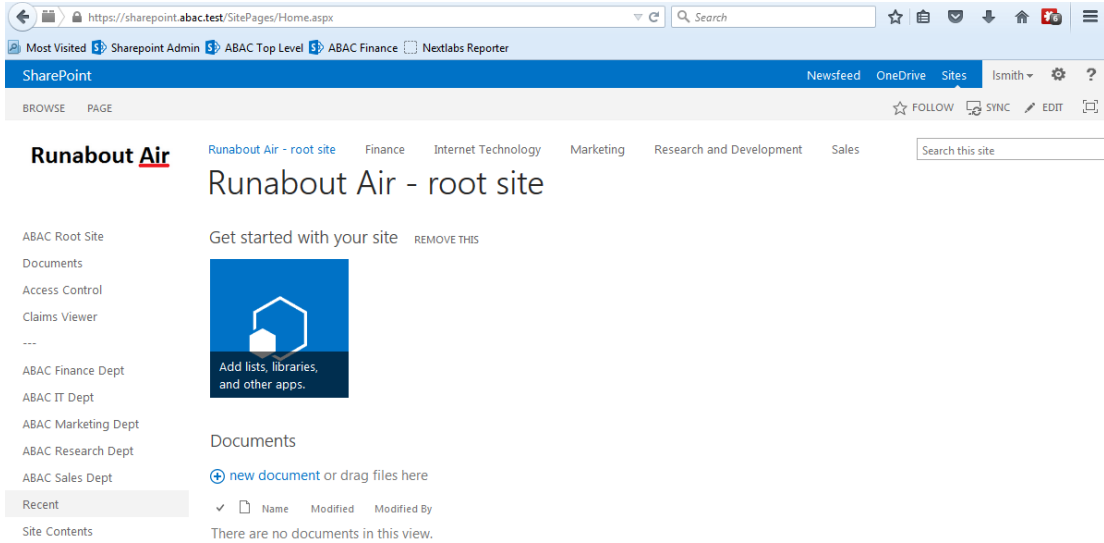
3331

4. Click **Sign On**. On the **RSA Adaptive Authentication** screen, enter the SMS validation code received on your mobile phone. Then, click **Continue**.

3332

3333

Once authenticated at the IdP, your browser automatically redirects to the PingFederate-RP (e.g., *rp.abac.test*) and then to the RP's SharePoint (*SharePoint.abac.test*) site.



3334

3335

3336

3337

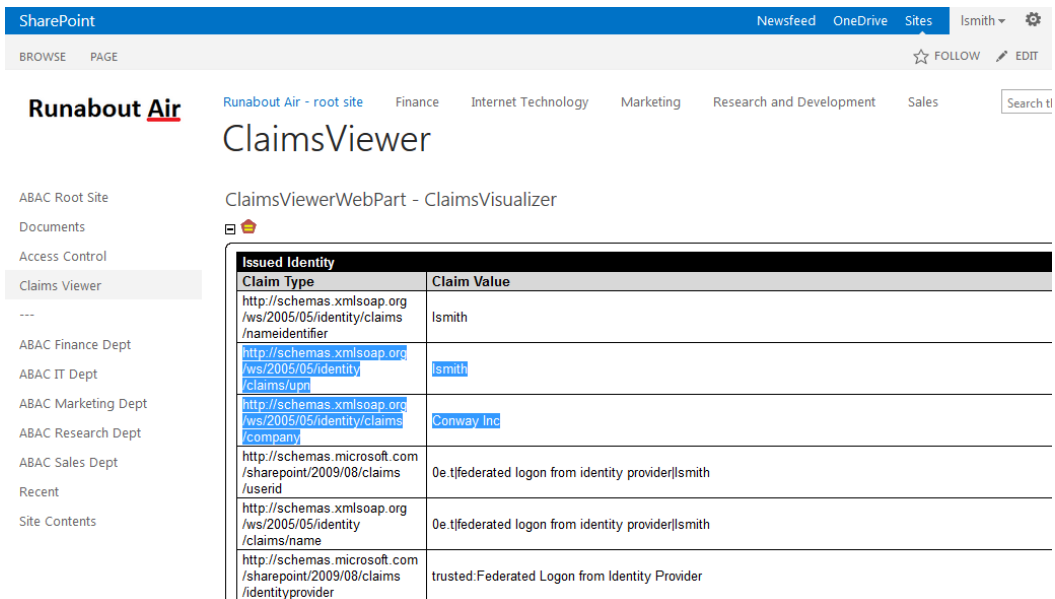
- Once you arrive at the SharePoint site home page, navigate to the claims viewer page that was created in the earlier section (e.g., <https://SharePoint.abac.test/SitePages/ClaimsView.aspx>). Expand the claims viewer web part on the page to see a list of claims.

3338

3339

3340

**Expected Result:** You should see the newly configured attribute (e.g., **company**) and its associated claim value. The claims viewer shows the name of each attribute (i.e., **claim**) using a long format such as <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company>.



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.

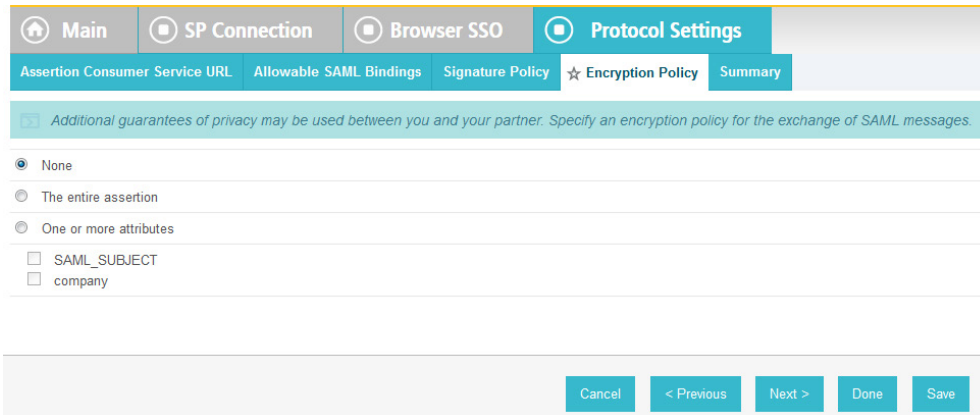
#### 3353 6.6.1.1 Disable SAML Encryption

- 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	
<b>ASSERTION CONSUMER SERVICE URL</b>	
Endpoint	URL: /sp/ACS.saml2 (POST)
<b>ALLOWABLE SAML BINDINGS</b>	
Artifact	false
POST	true
Redirect	true
SOAP	false
<b>SIGNATURE POLICY</b>	
Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false
<b>ENCRYPTION POLICY</b>	
Encrypt Entire Assertion	true

- 3362
- 3363 5. Click on the **ENCRYPTION POLICY** link.
- 3364 6. On the **Encryption Policy** screen, select **None**.





3365

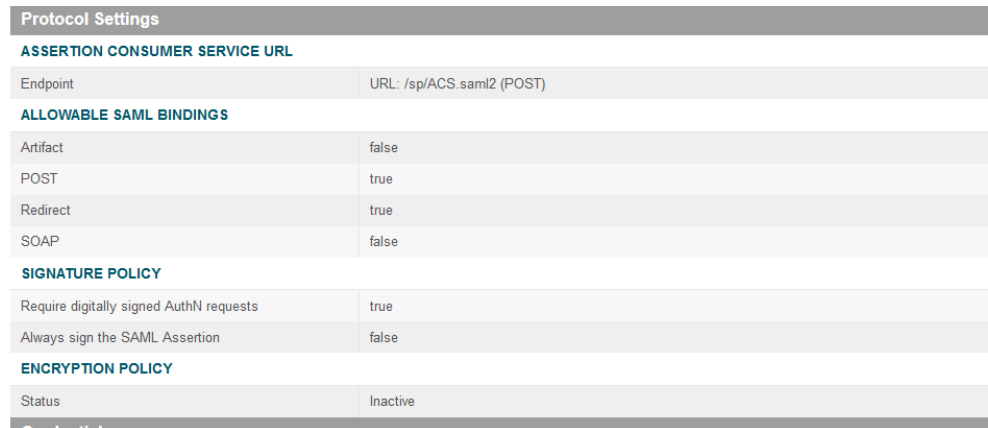
3366 7. Click **Save**.

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.

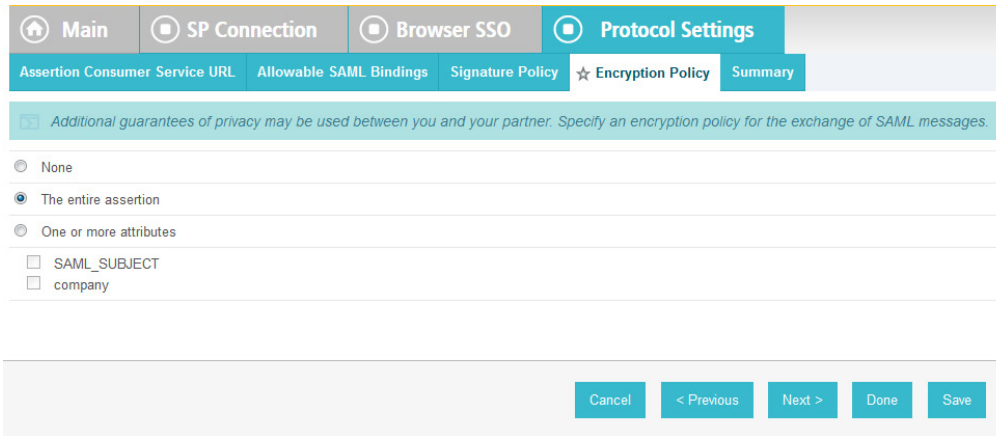
- 3372 1. On the PingFederate Main Menu under SP CONNECTION, click **Manage All SP**.
- 3373 2. Click on the link for the SP connection for which you want to enable the encryption (e.g.,  
 3374 *https://rp.abac.test:9031*).
- 3375 3. Scroll down to the Protocol Settings group.



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**.

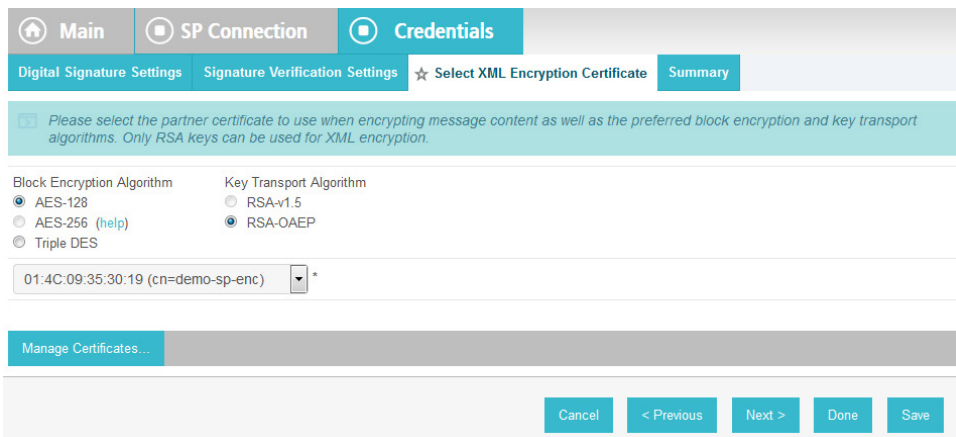
3381

7. On the Select **XML Encryption Certificate** screen, select the **Block Encryption Algorithm** (e.g., **AES-128**), and the **Key Transport Algorithm** (e.g., **RSA-OAEP**). For the selection box above **Manage Certificates**, select the RP’s public key certificate to be used to encrypt the message content.

3382

3383

3384



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, read-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.

## 3512 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
<b>Control Center (CC)</b>	license.dat; ControlCenter-64-7.5.0.0-64-2014102111146.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
<b>External Database</b>	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
<b>Policy Studio</b>	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
<b>Policy Controller</b>	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
<b>Entitlement Manager for SharePoint Server</b>	SharePointEnforcer-2013-64-7.1.3.0-7-201410101427.zip			<ul style="list-style-type: none"> <li>• Microsoft Office SharePoint Server 2007 on                             <ul style="list-style-type: none"> <li>- Windows Server 2003, Enterprise Edition, 32-bit, Service Pack 2, or</li> <li>- Windows Server 2008, Enterprise Edition, 64-bit, R2</li> </ul> </li> <li>• Microsoft Office SharePoint Server 2010 on                             <ul style="list-style-type: none"> <li>- Windows Server 2008, Enterprise Edition, 64-bit, R2</li> </ul> </li> <li>• Microsoft SharePoint Server 2013 on                             <ul style="list-style-type: none"> <li>- Windows Server 2008, Enterprise Edition, 64-bit, R2</li> </ul> </li> </ul>	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*

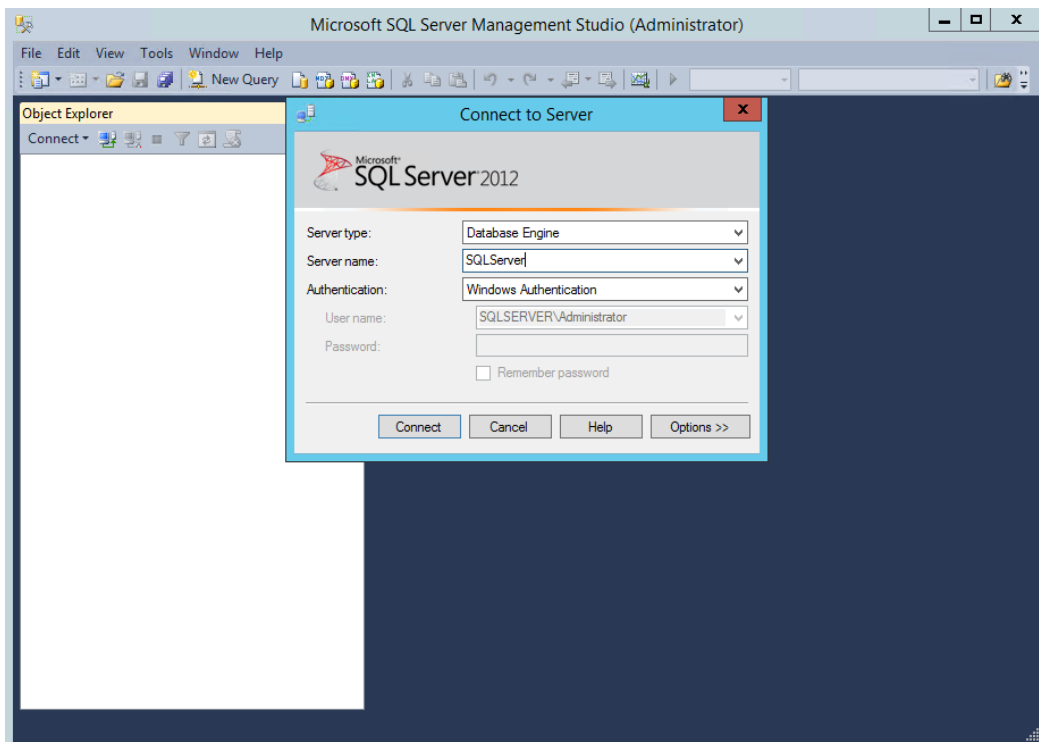
3518 Instructions available at the Microsoft SQLServer site: [https://technet.microsoft.com/en-](https://technet.microsoft.com/en-us/library/hh231622(v=sql.110).aspx)  
3519 [us/library/hh231622\(v=sql.110\).aspx](https://technet.microsoft.com/en-us/library/hh231622(v=sql.110).aspx).

#### 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*

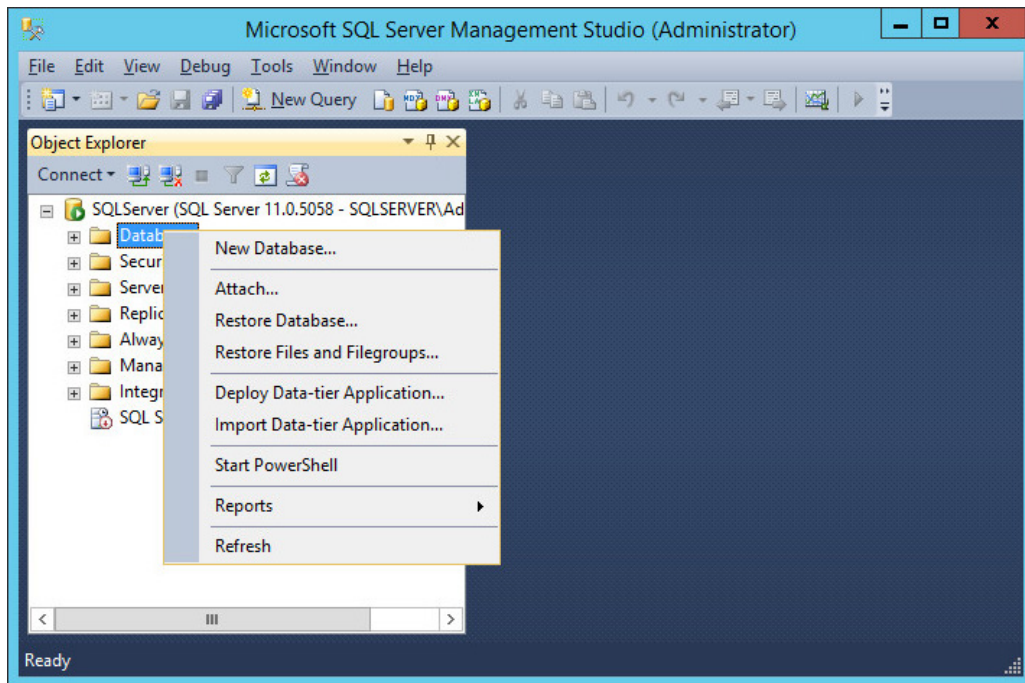
- 3532 1. Open Microsoft SQL Server Management Studio and login to Microsoft SQL Server.



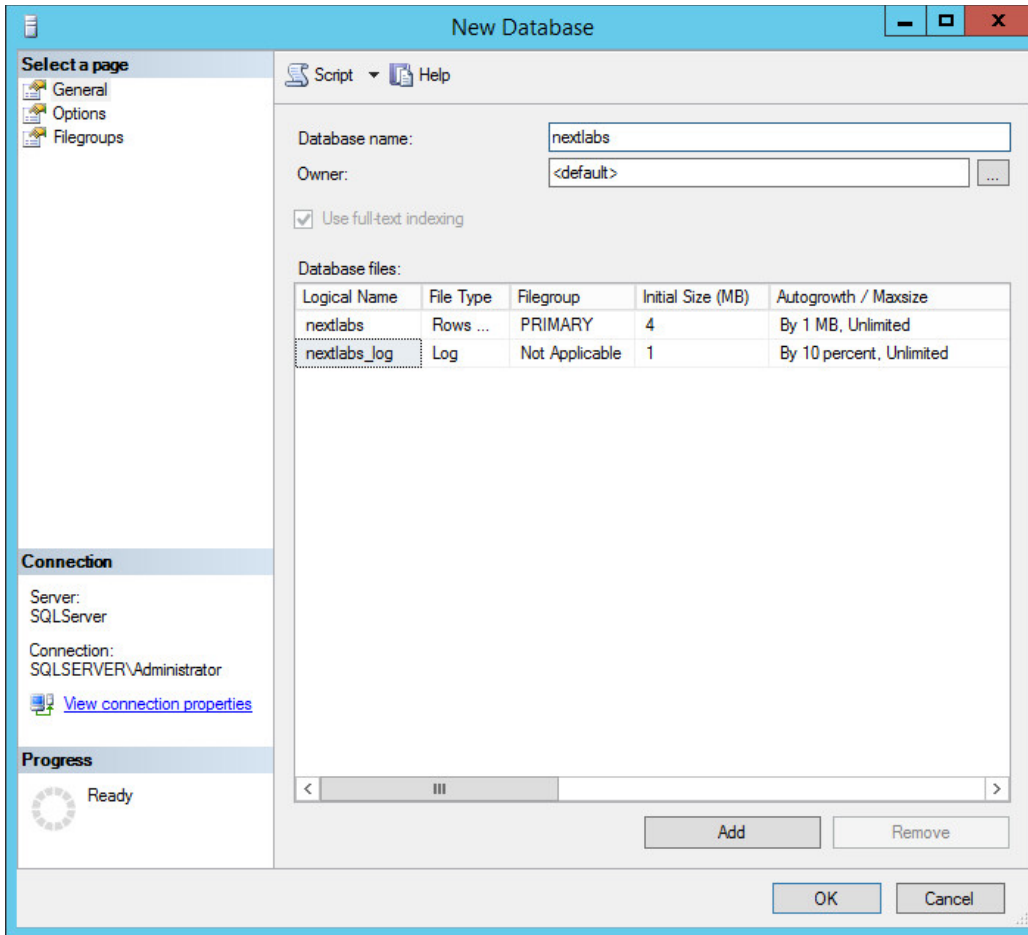
3533



- 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**

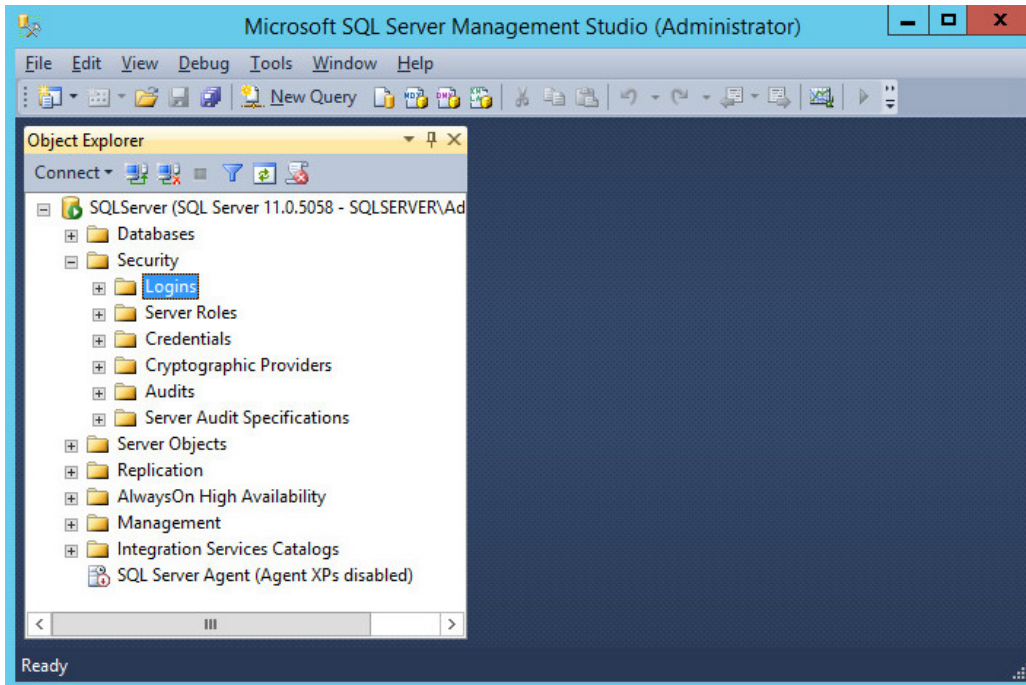


3539

3540

3541

4. Click on the menu box next to **Security** to begin the process for creating a new login for the new NextLabs database’s administrator.



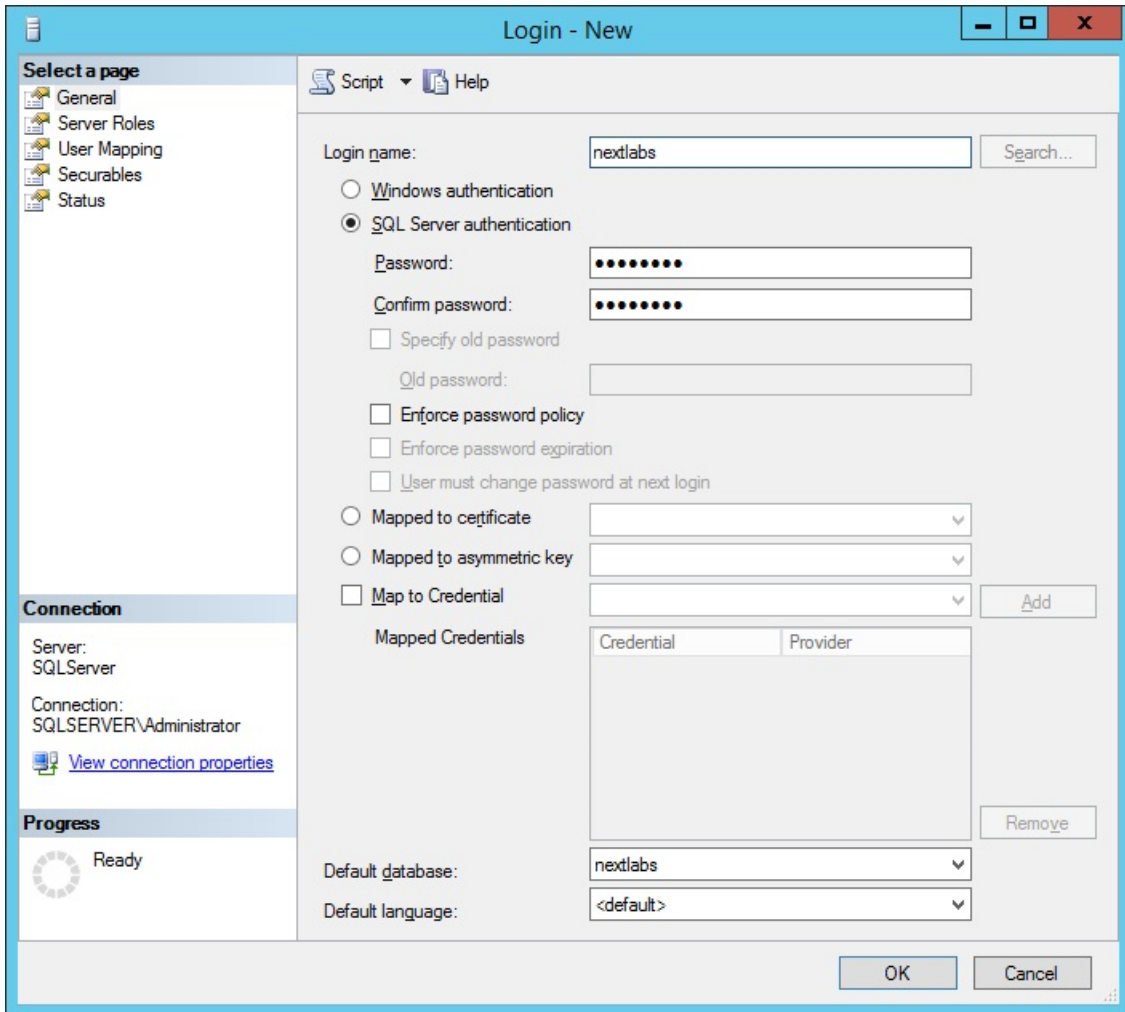
3542

3543

5. Right-click **Logins**. Left-click **New Login**.

3544

6. Click on **SQL Server authentication**, and enter a new **Login name** and **Password**.

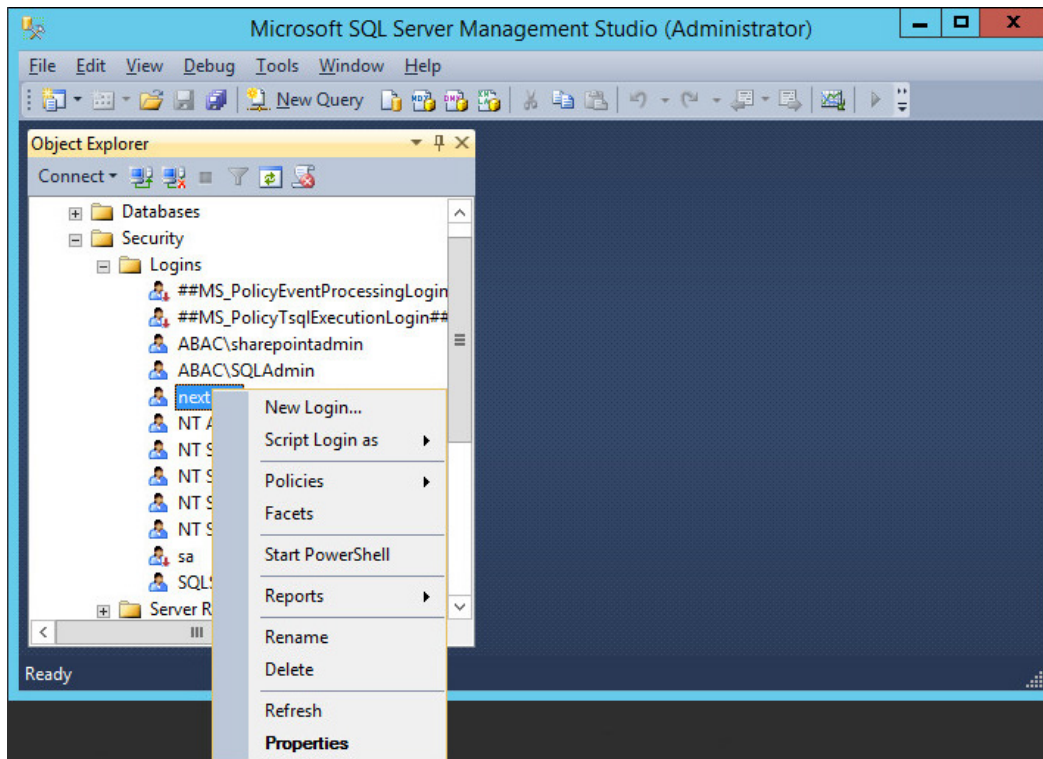


3545

3546

3547

7. Click the menu box next to **Logins**. Right-click on the new user created in the previous step. Click **Properties**.

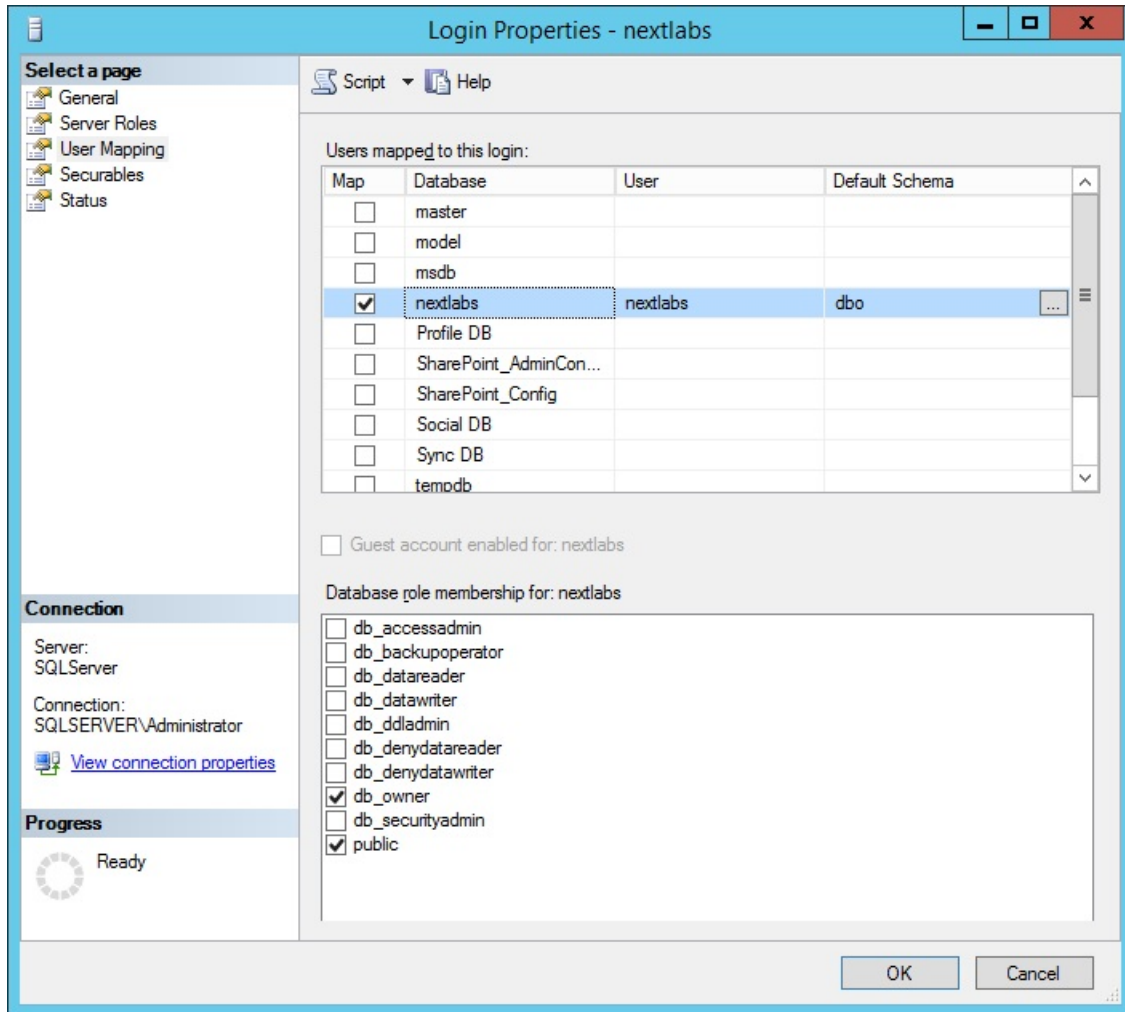


3548

3549

3550

8. Click on **User Mapping**, then **New Database**. Under **Database role membership for: [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:

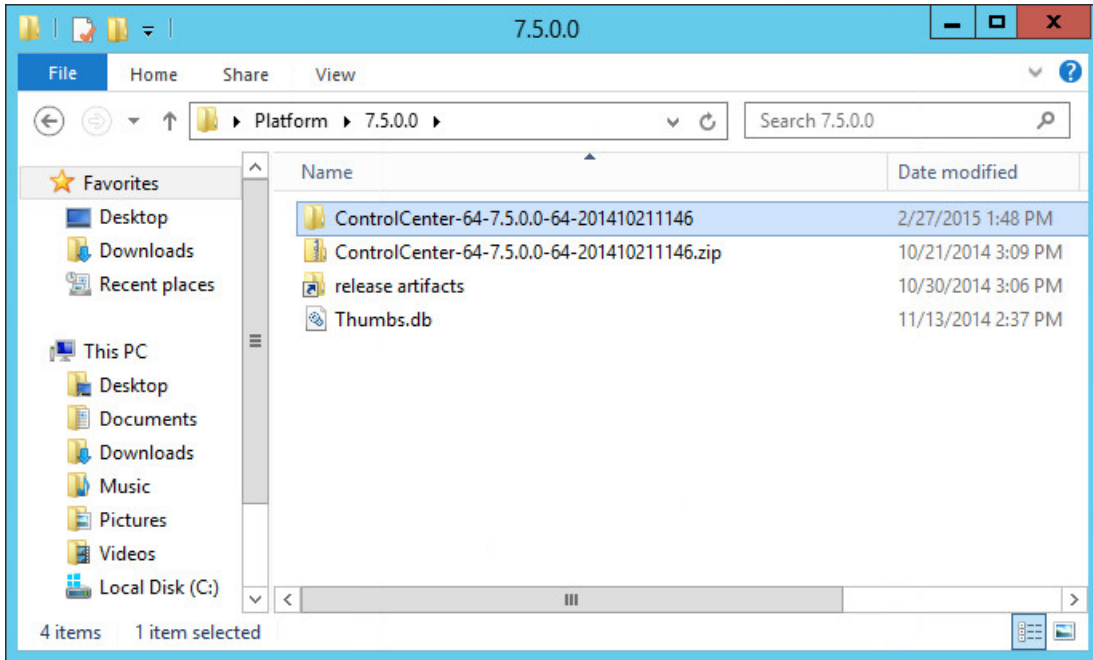
3557 **C:\Users\Administrator\Desktop\NextLabs\Platform\7.5.0.0\**

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.

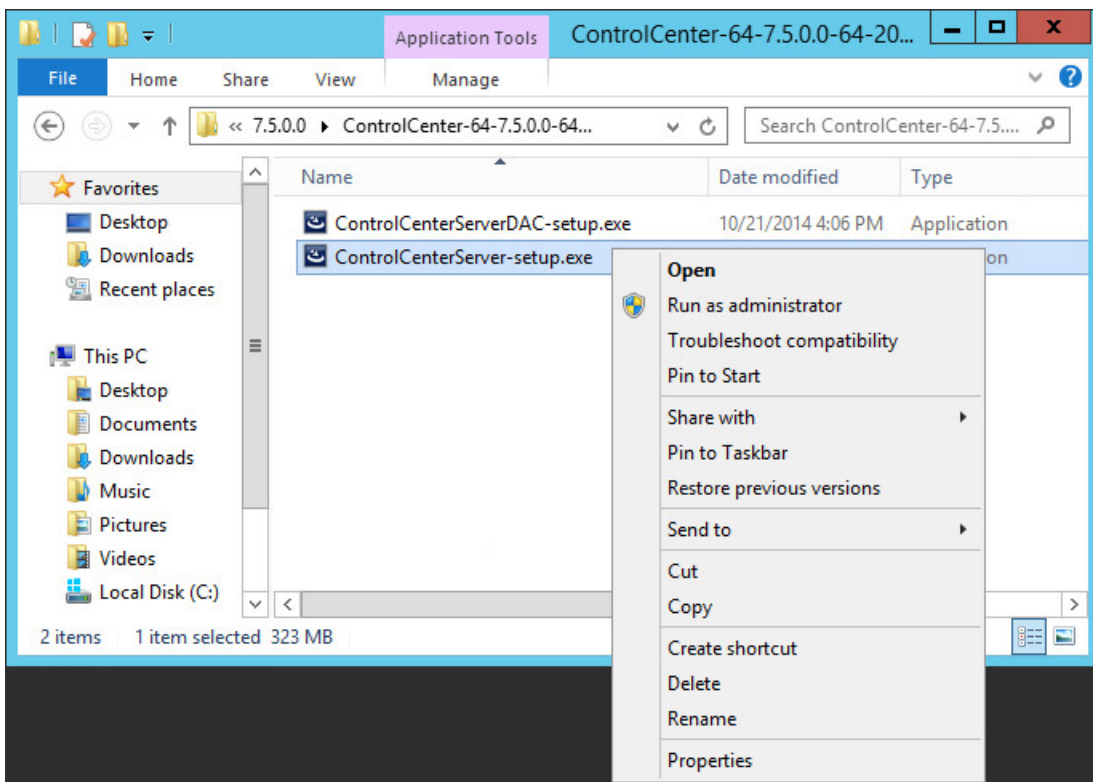
3562 3. Double-click to open the **ControlCenter-64-7.5.0.0-64-201410211146** folder.



3563

3564

4. Right-click on **ControlCenterServer-setup.exe**, and select **Run as administrator**.

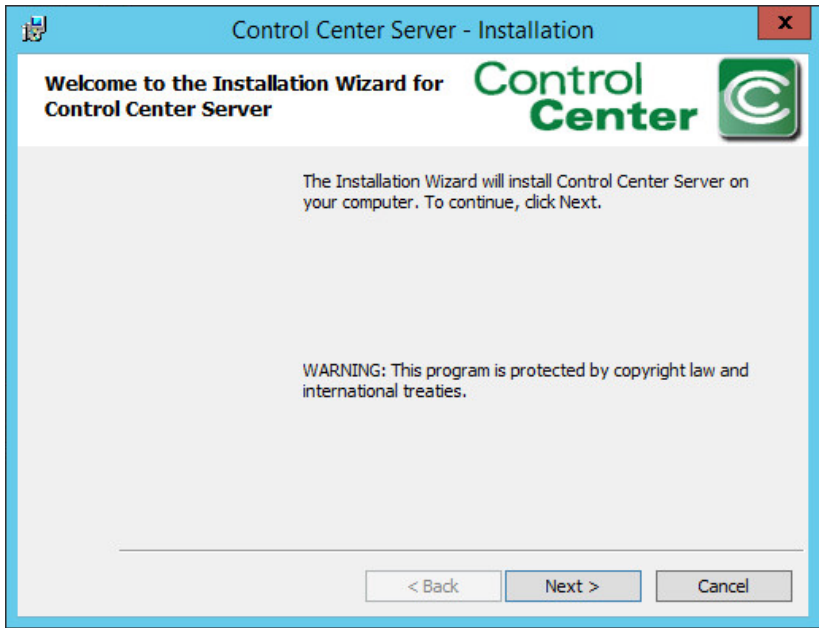


3565

3566

5. Click **Next**.

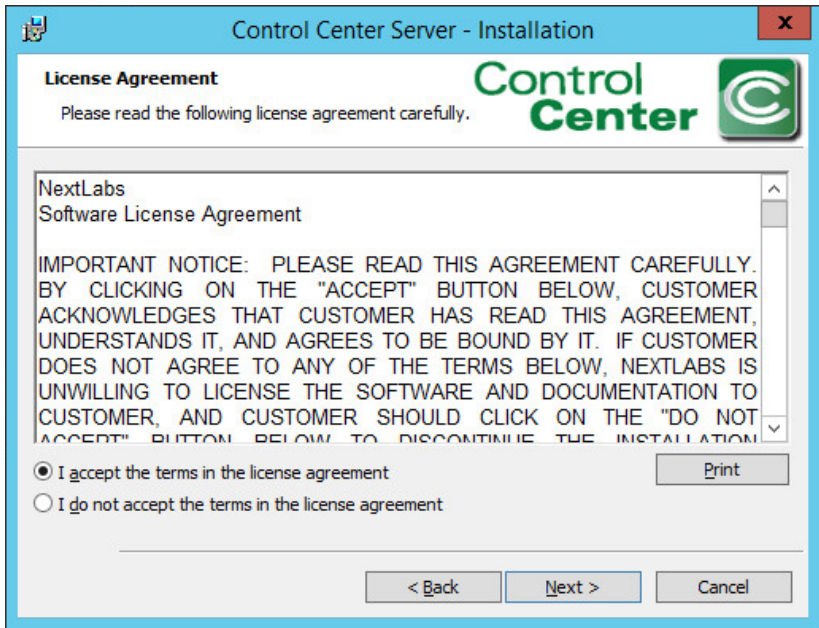




3567

3568

6. Select **I accept the terms in the license agreement**, then click **Next**.

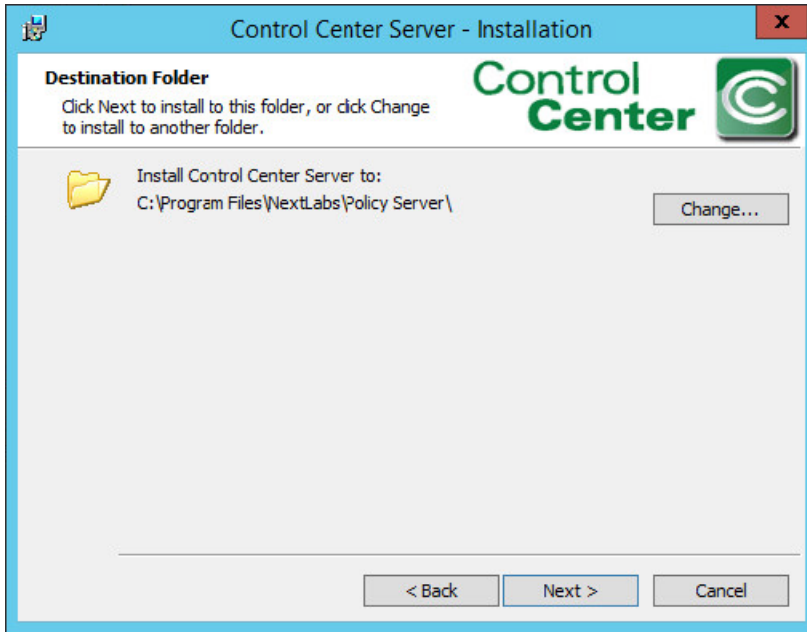


3569

3570

7. Click **Next**.

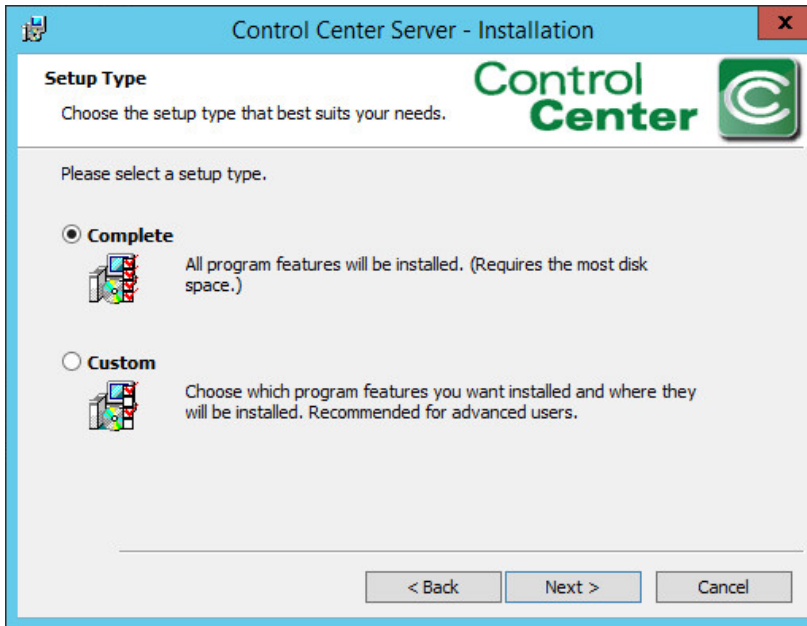




3571

3572

8. Select the **Complete** setup type. Then, click **Next**.



3573

3574

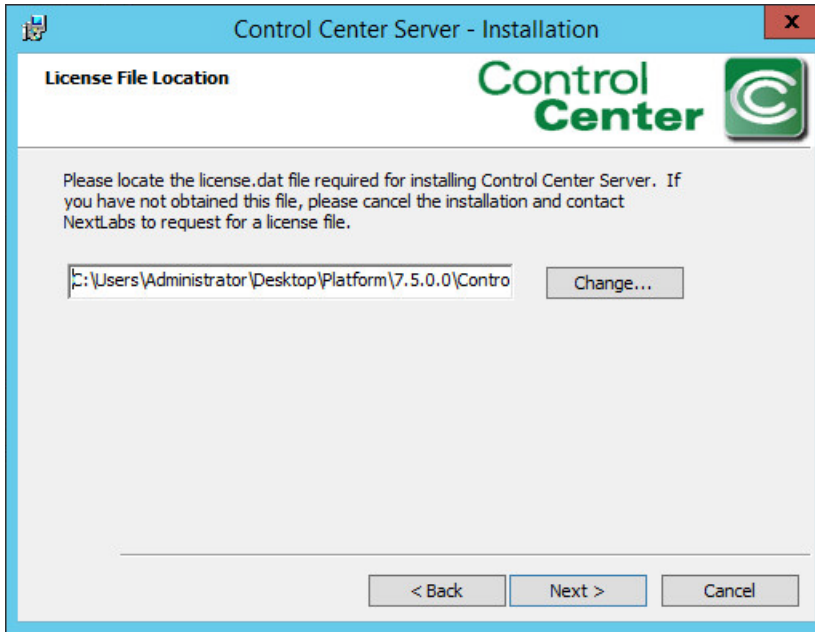
3575

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**.

3576

3577

Example location: *C:\Users\Administrators\Desktop\Platform\7.5.0.0\ControlCenter-64-7.5.0.0-64-201410211146\license.dat*

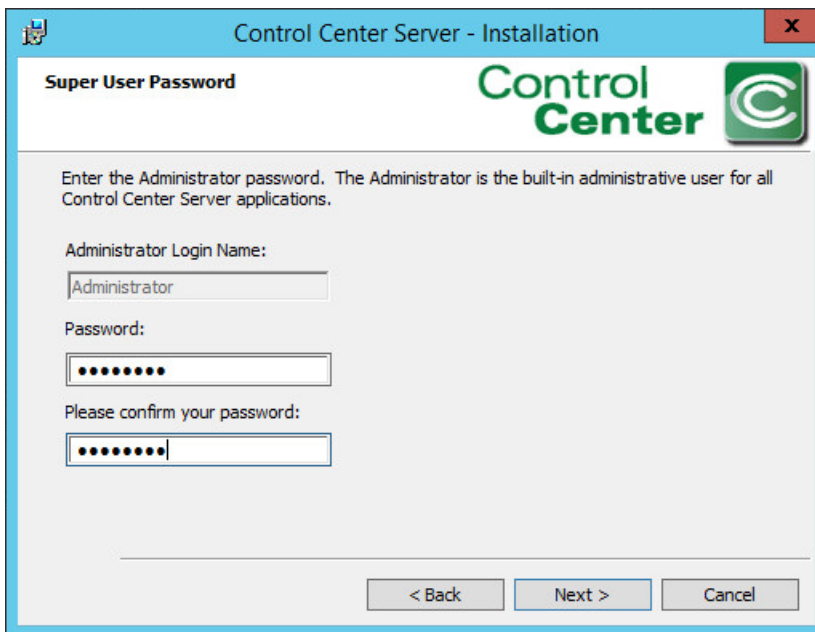


3578

3579

3580

10. In the configuration wizard Super User password screen, enter a **Password** for the built-in administrative user for all Control Center Server applications. Click **Next**.

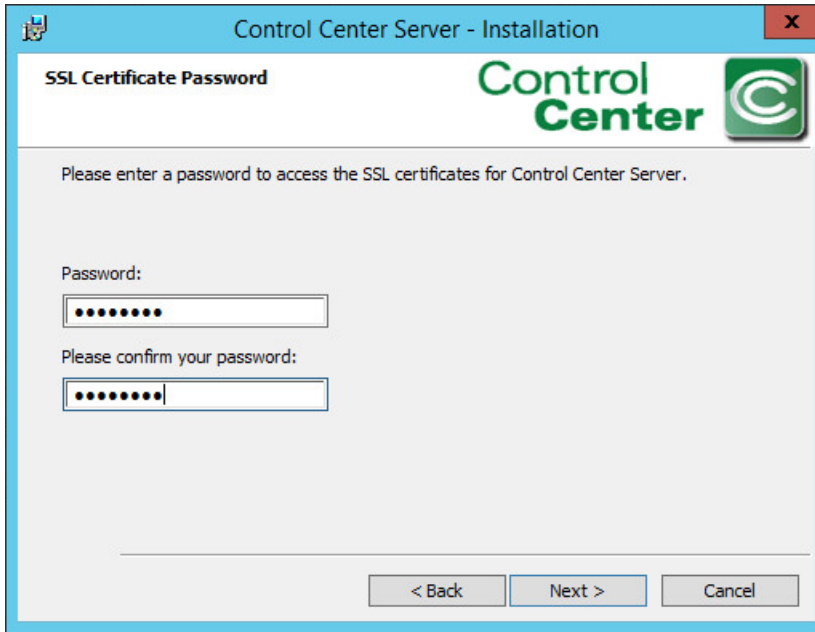


3581

3582

3583

11. At the SSL Certificate Password screen, enter a **Password** to access the SSL certificates for the Control Center Server. Click **Next**.

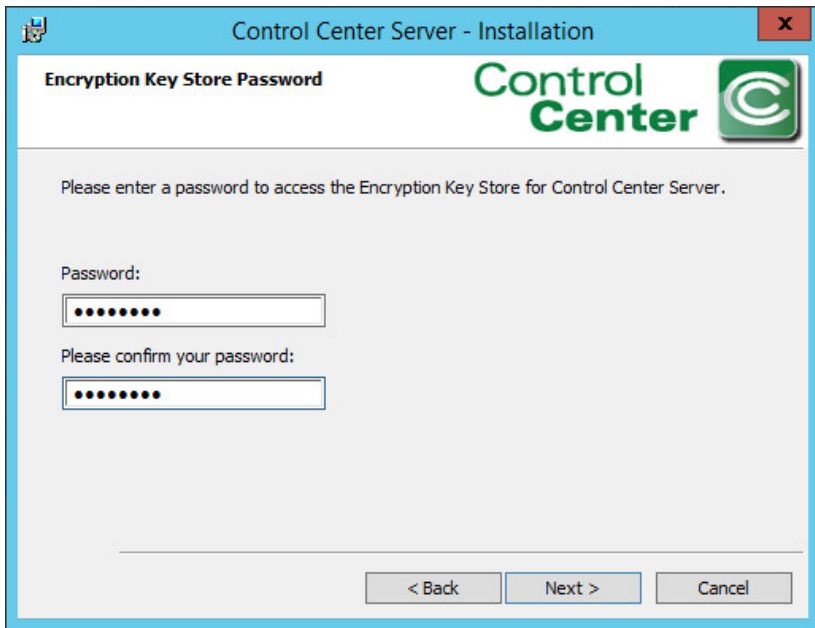


3584

3585

3586

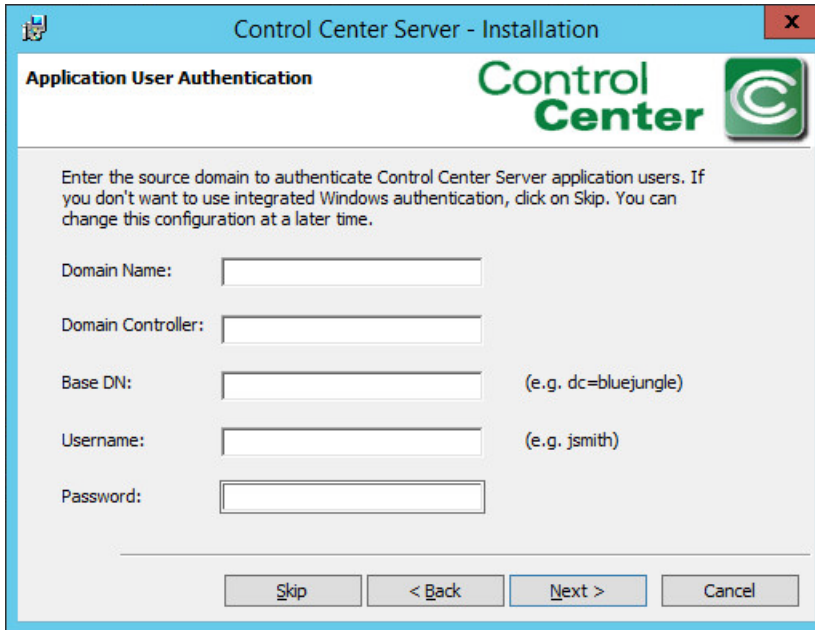
12. At the Encryption Key Store Password screen, enter a **Password** to access the Encryption Key Store for the Control Center Server. Click **Next**.



3587

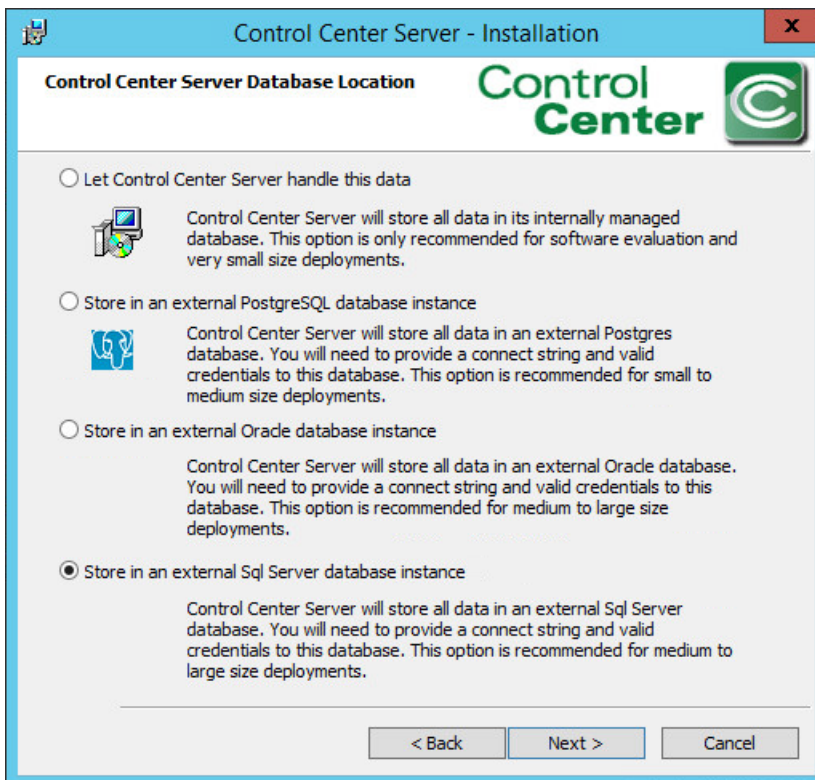
3588

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**.

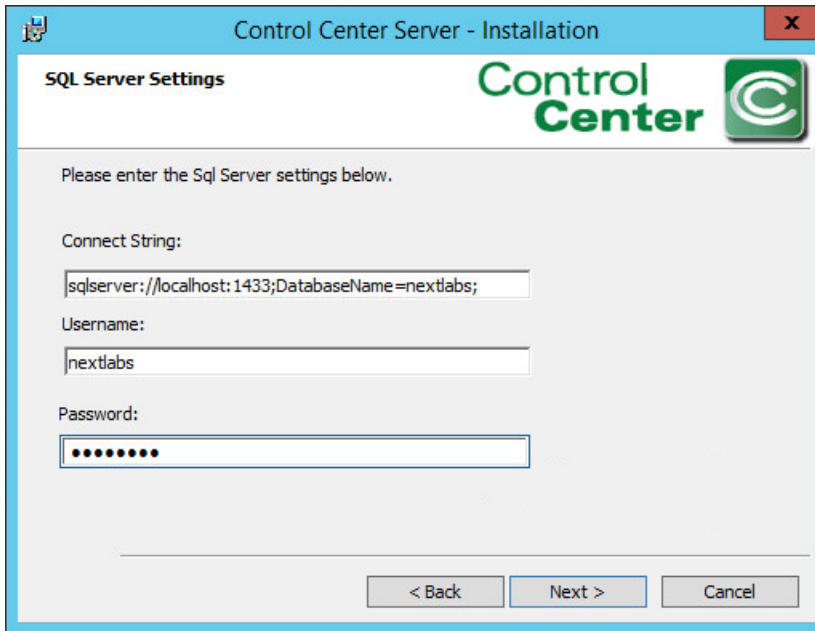


3592

- 3593 15. At the SQL Server Settings screen, do the following:

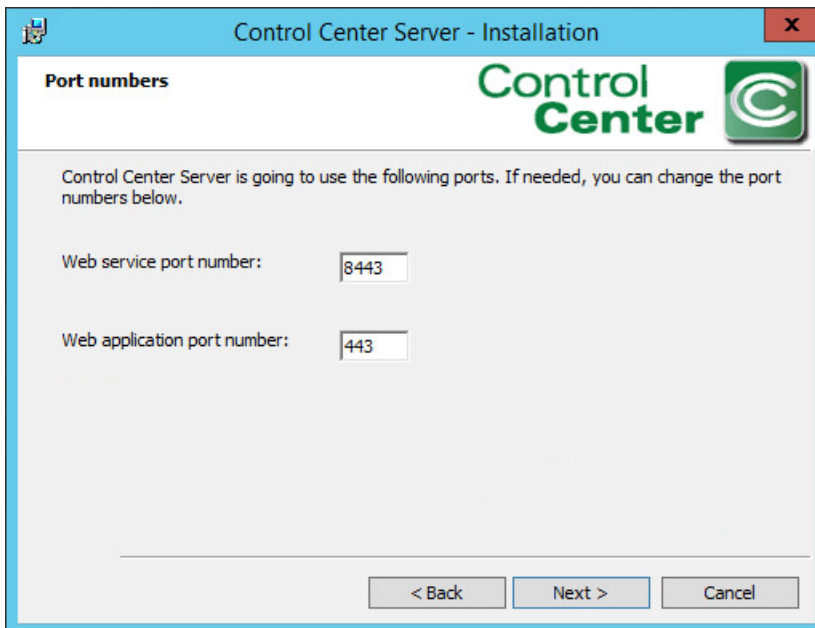
- 3594 a. Specify the **Connect String**, including the name of the new SQL database created.  
 3595 Example: **nextlabs**

- 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**
- 3598                    **properly** appears, it may help to restart the SQL Server.



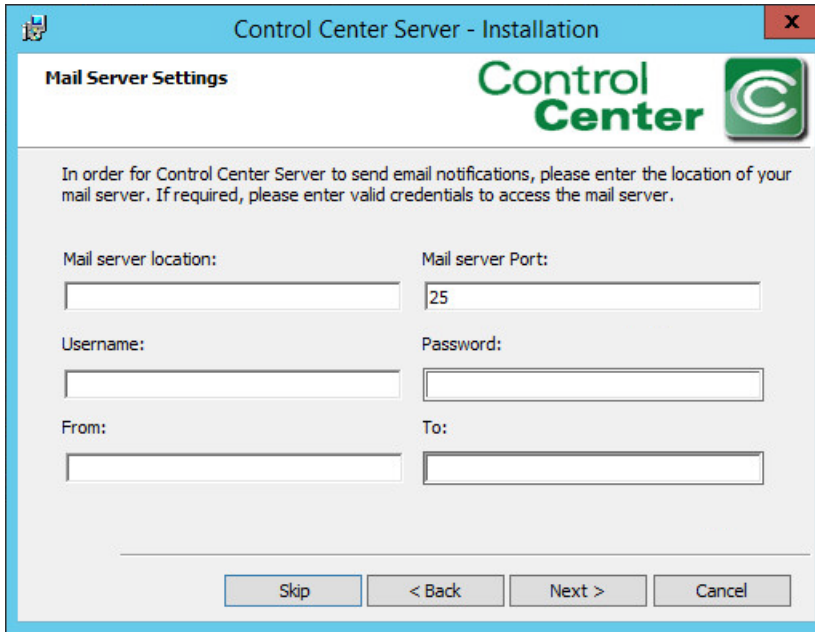
3599

- 3600                    16. At the Port numbers window, the default port numbers are already entered: Web service port
- 3601                    number: 8443, Web application port number: 443. Click **Next**.



3602

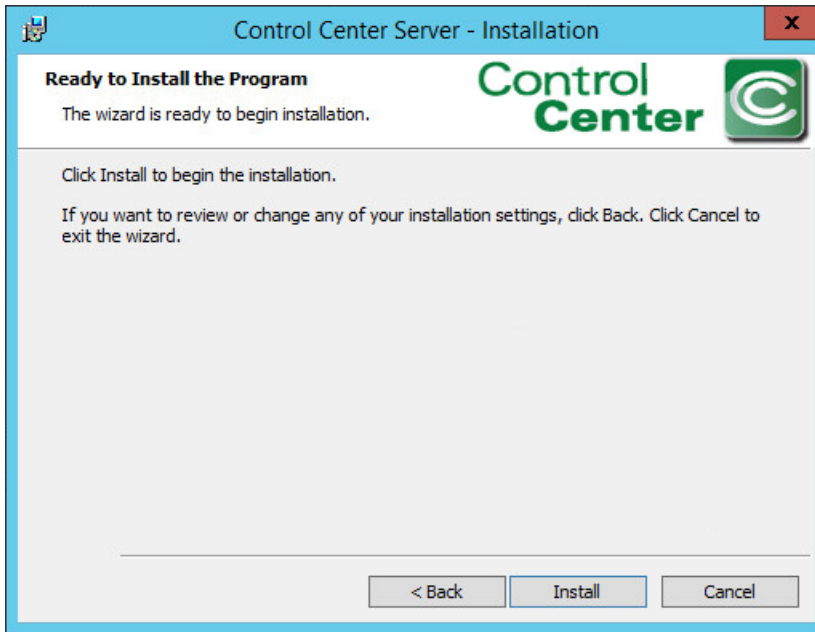
- 3603                    17. At the Mail Server Settings screen, click **Skip**.



3604

3605

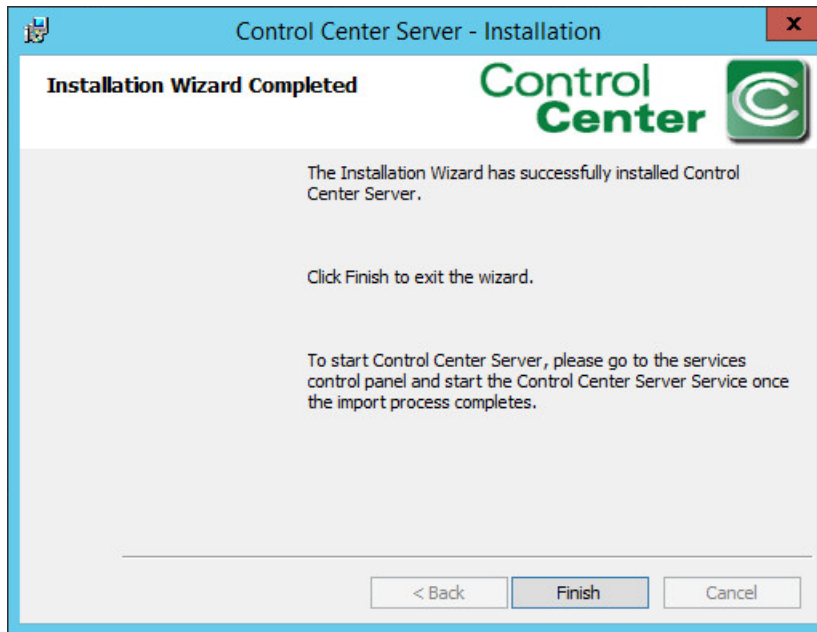
18. At the Ready to Install the Program screen, click **Install**.



3606

3607

19. At the Installation Wizard Completed screen, click **Finish**.



3608

3609

3610

20. Open an Internet browser and navigate to the following URL: *https://localhost/administrator* to 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

3616

3617

21. Once logged into the Control Center Administrator web application in your browser, you can verify that the NextLabs Control Center is installed and configured correctly on the SQL Server, and view the following information:

3618

3619

- a. Fully qualified domain name (FQDN) of the server hosting the NextLabs Control Center. 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 Control Center on the SQL Server, please refer to NextLabs support documentation.

3627

3628

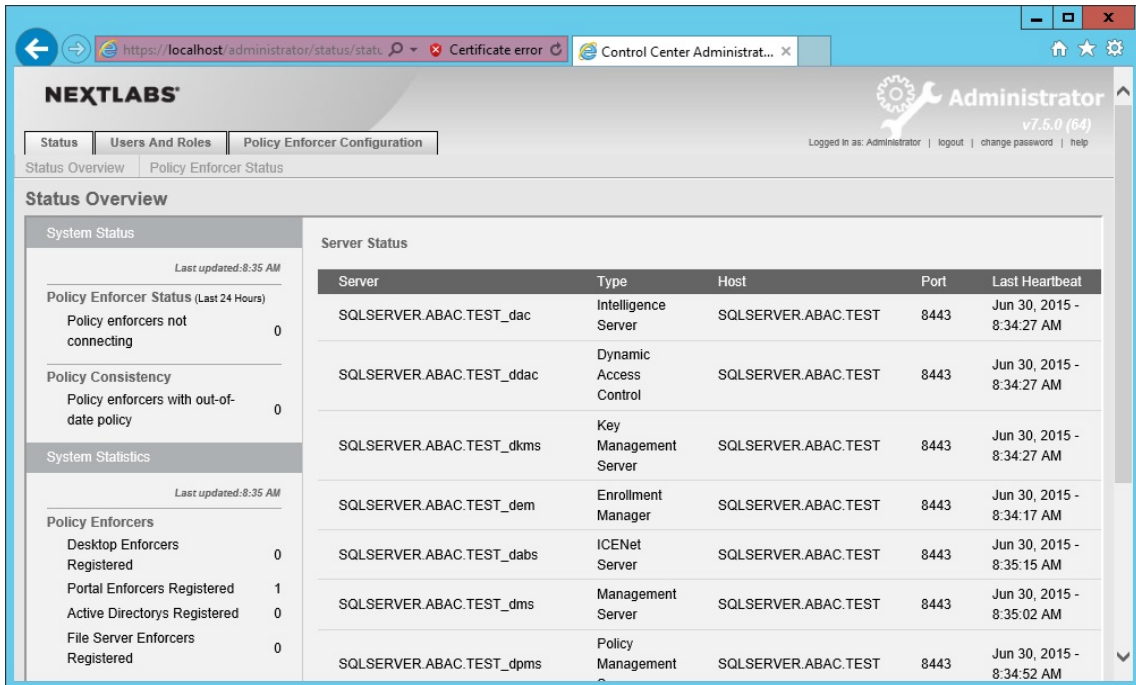
- c. Port via which the above services are running. Example: 8443, default for web services

3629

- d. For each of the listed services, the default heartbeat period is 60 minutes, and can be modified via the Administrator (See step 23).

3630





3631

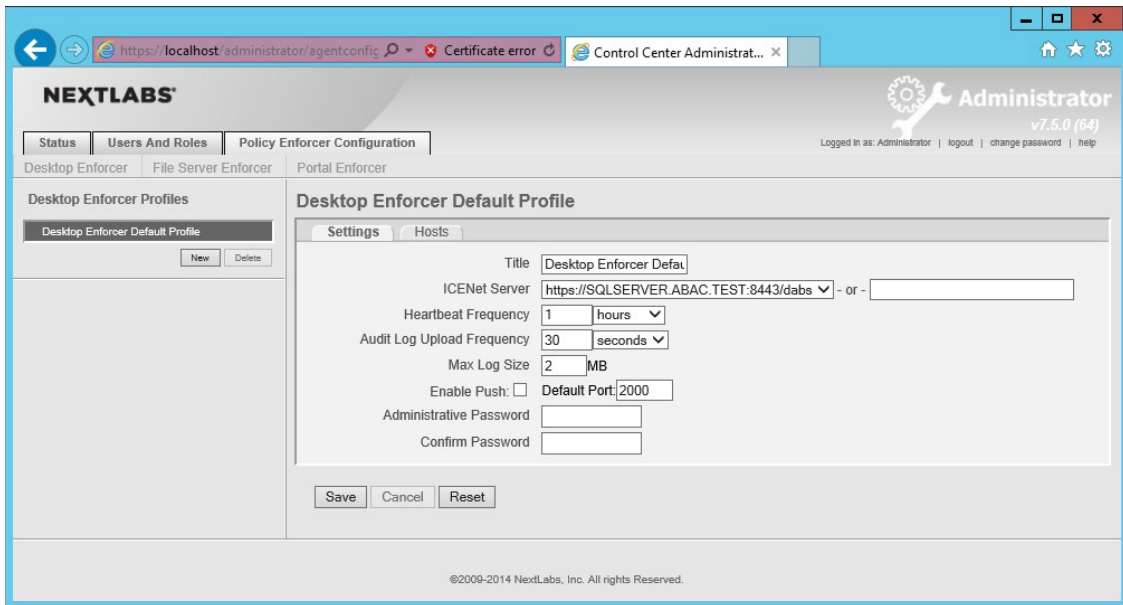
3632

3633

3634

3635

- 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**.



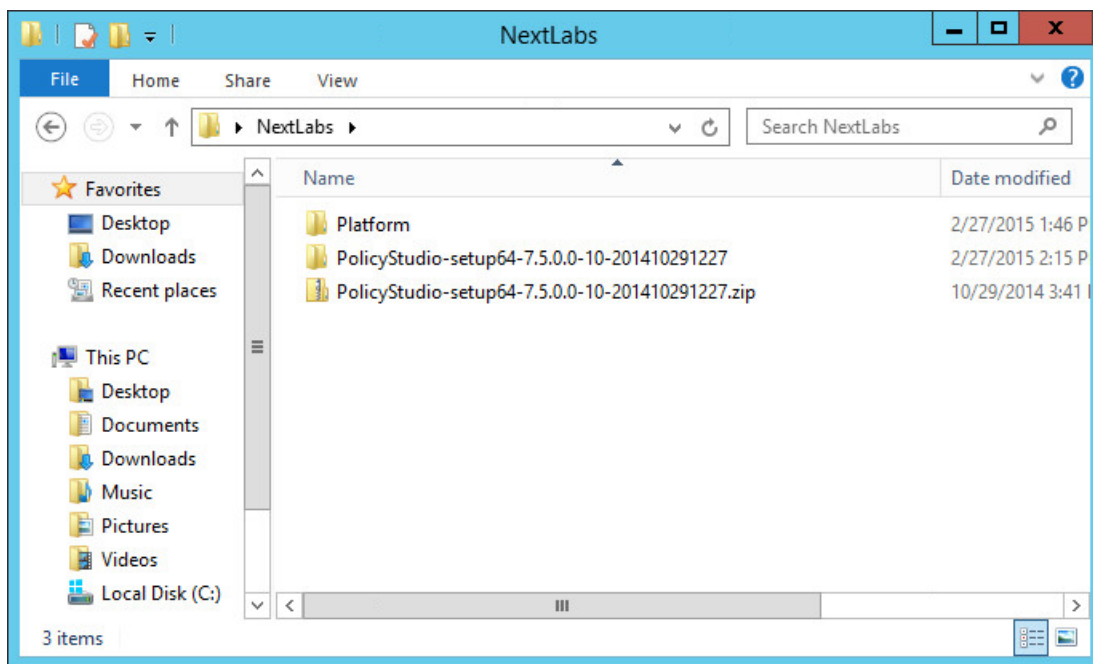
3636

3637 **7.4 Installation and Configuration of NextLabs Policy Studio: Enterprise**  
3638 **Edition (PAP)**

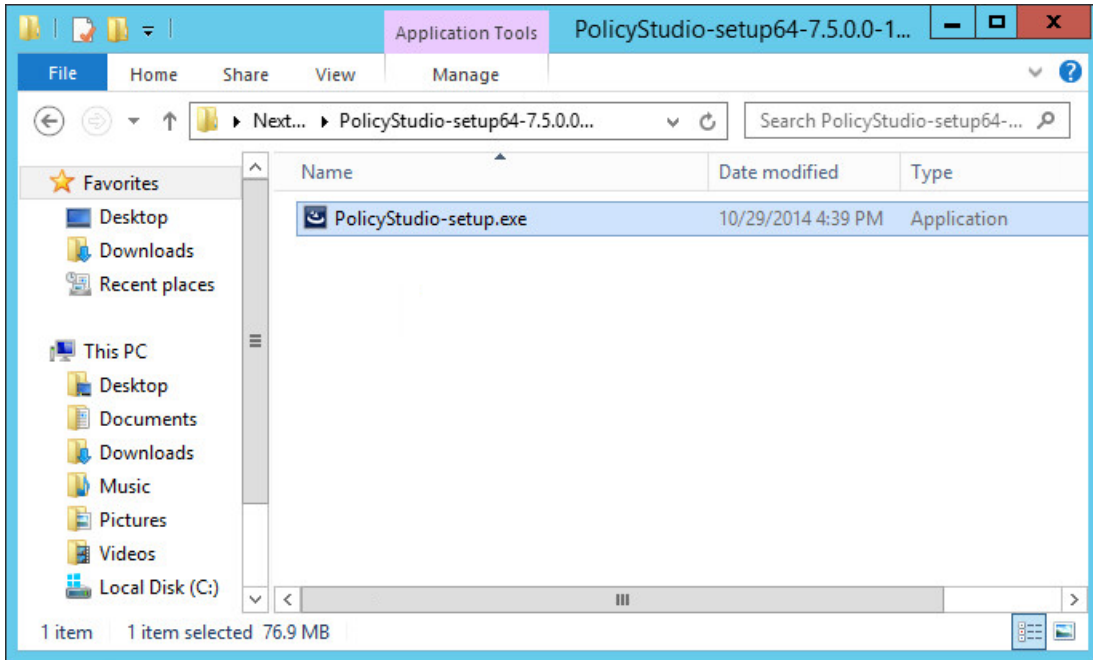
3639 **7.4.1 Installation**

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 3. Double-click to open the **PolicyStudio-setup64-7.5.0.0-10-201410291227** folder.
- 3647 4. Right-click on **PolicyStudio-setup.exe** and select Run as **Administrator**.

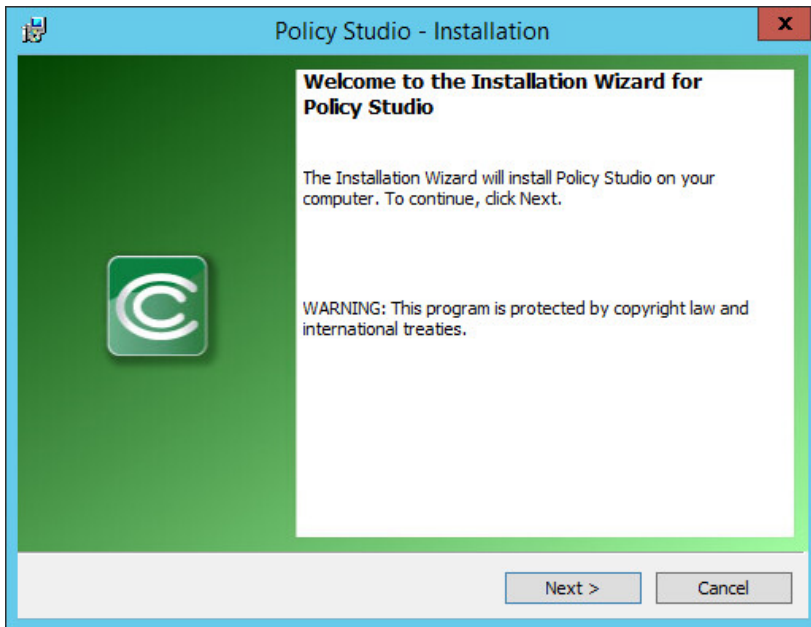


3649

3650

3651

5. At the Welcome to the Installation Wizard for Policy Studio screen of the Policy Studio Installation Window, click **Next**.



3652

3653

3654

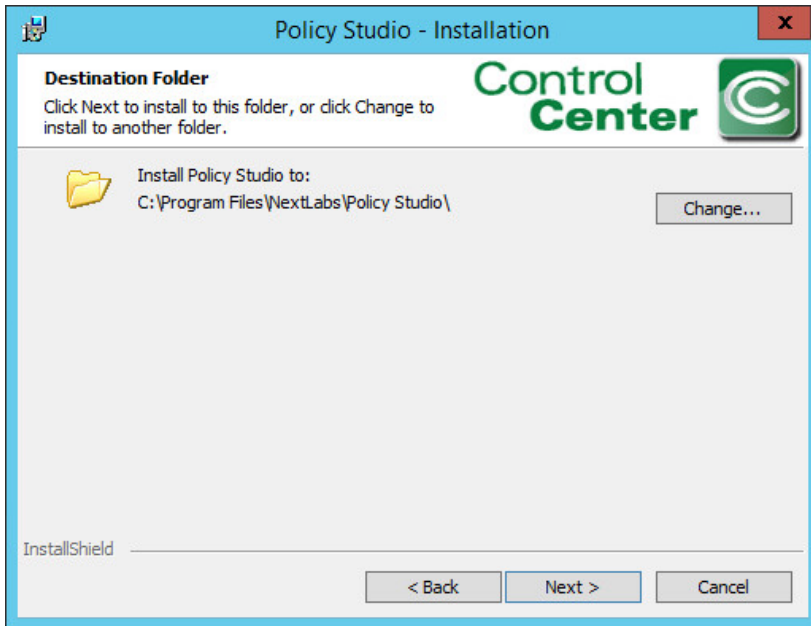
6. At the License Agreement screen, select **I accept the terms in the license agreement**, and click **Next**.



3655

3656

7. At the Destination Folder screen, click **Next**.

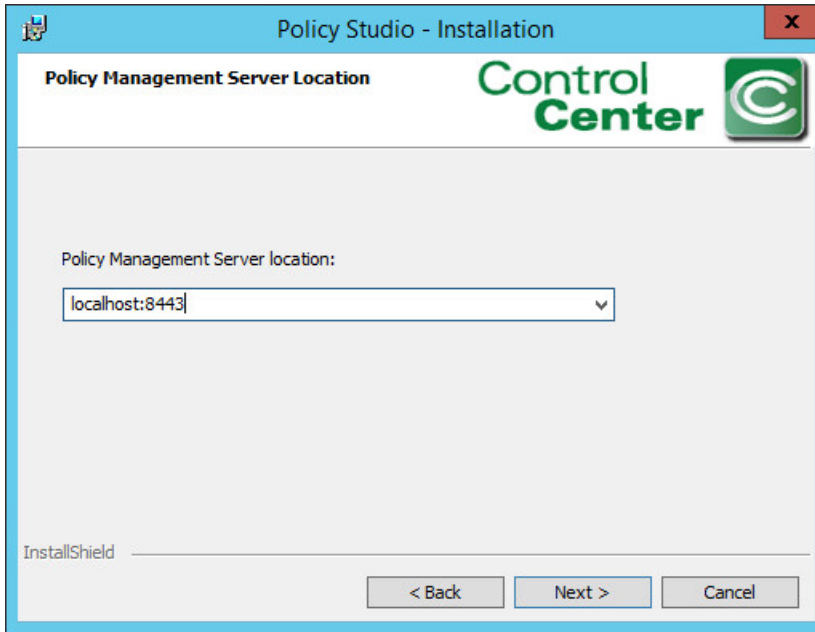


3657

3658

3659

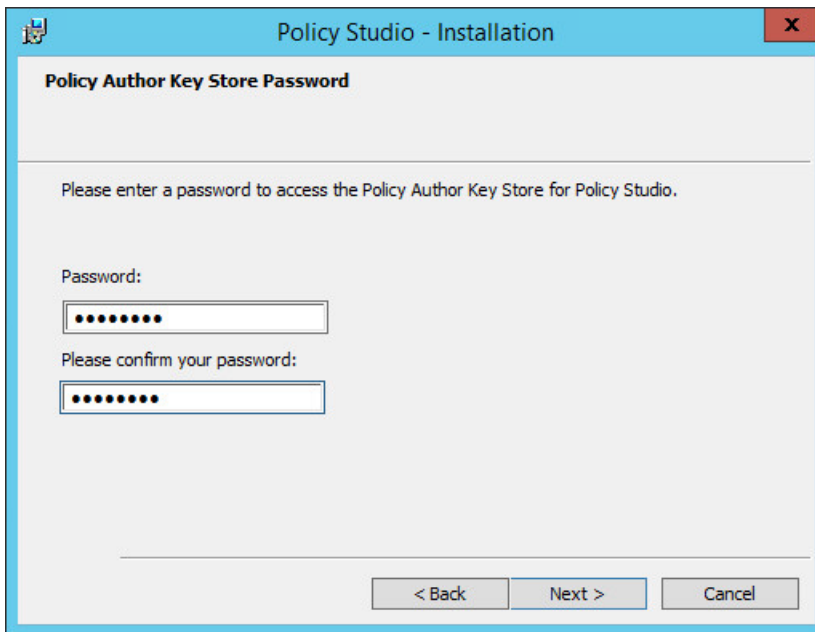
8. At the Policy Management Server Location screen, enter the default location **localhost:8443**. Click **Next**.



3660

3661

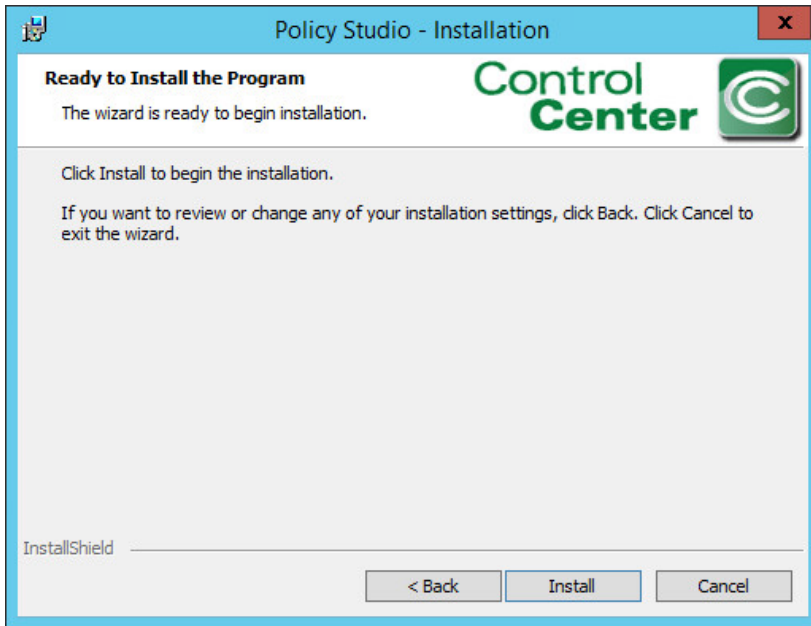
9. At the Policy Author Key Store Password screen, enter a **Password** and click **Next**.



3662

3663

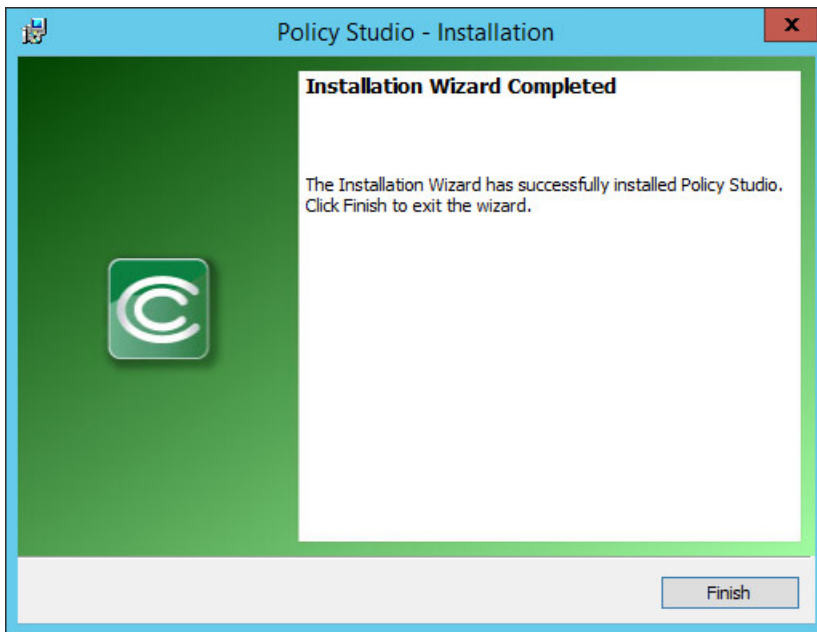
10. At the Ready to Install the Program screen, click **Install**.



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

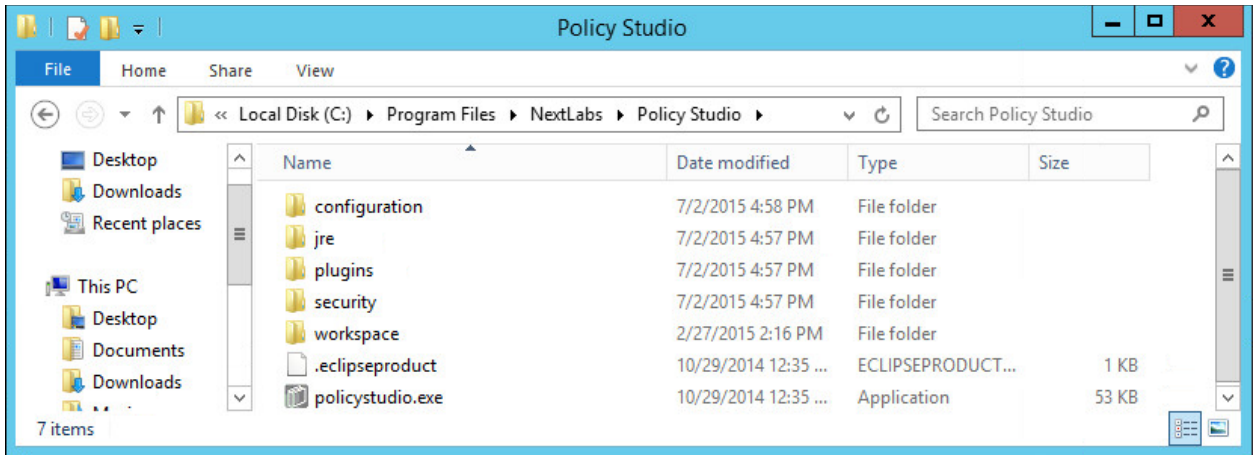
c. Double-click **NextLabs**.

3671

d. Double-click **Policy Studio**.

3672

e. Double-click **policystudio.exe**.

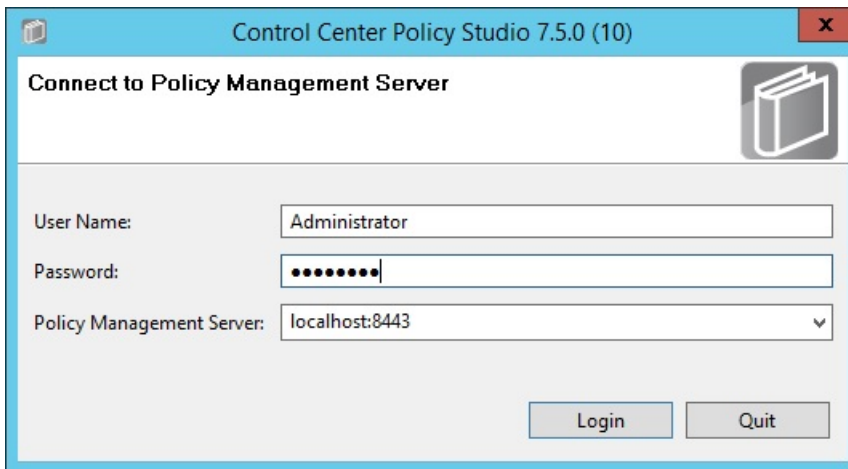


3673

3674

3675

13. In the Control Center Policy Studio window, enter a **User Name** and **Password** to connect to the Policy Management Server



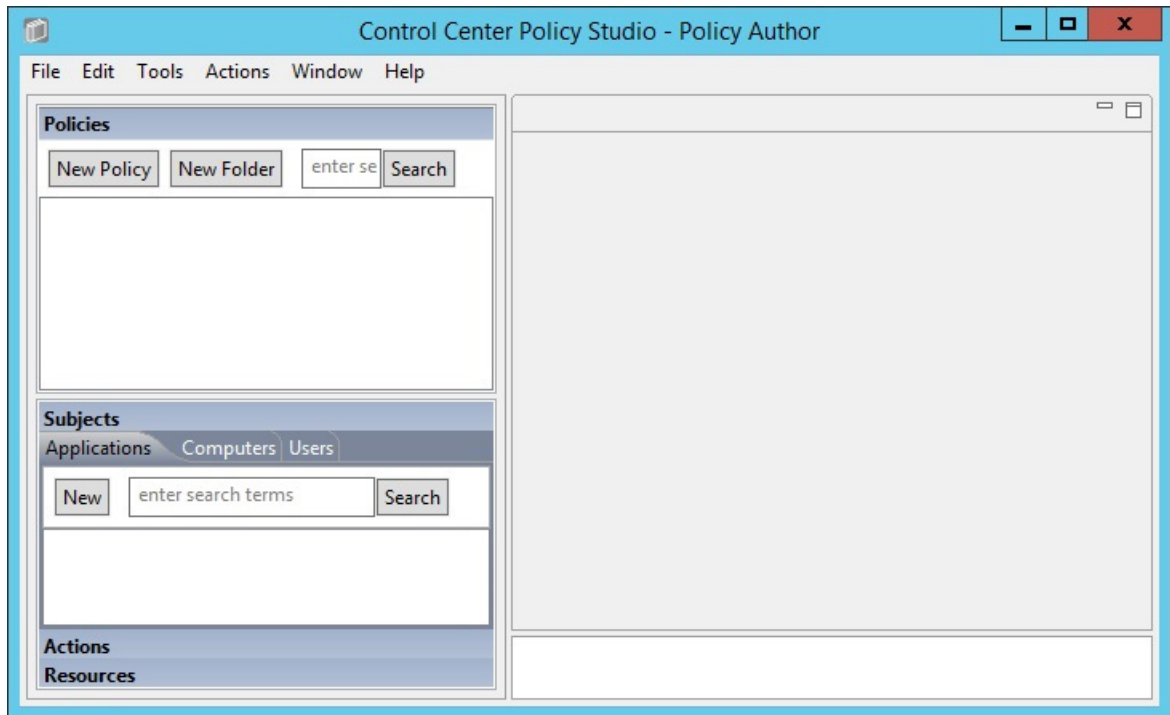
3676

3677

3678

3679

14. If the connection is successful, the Control Center Policy Studio - Policy Author window will open.
  - a. Policies are defined and deployed in this interface, to be covered in [Section 8](#).



3680

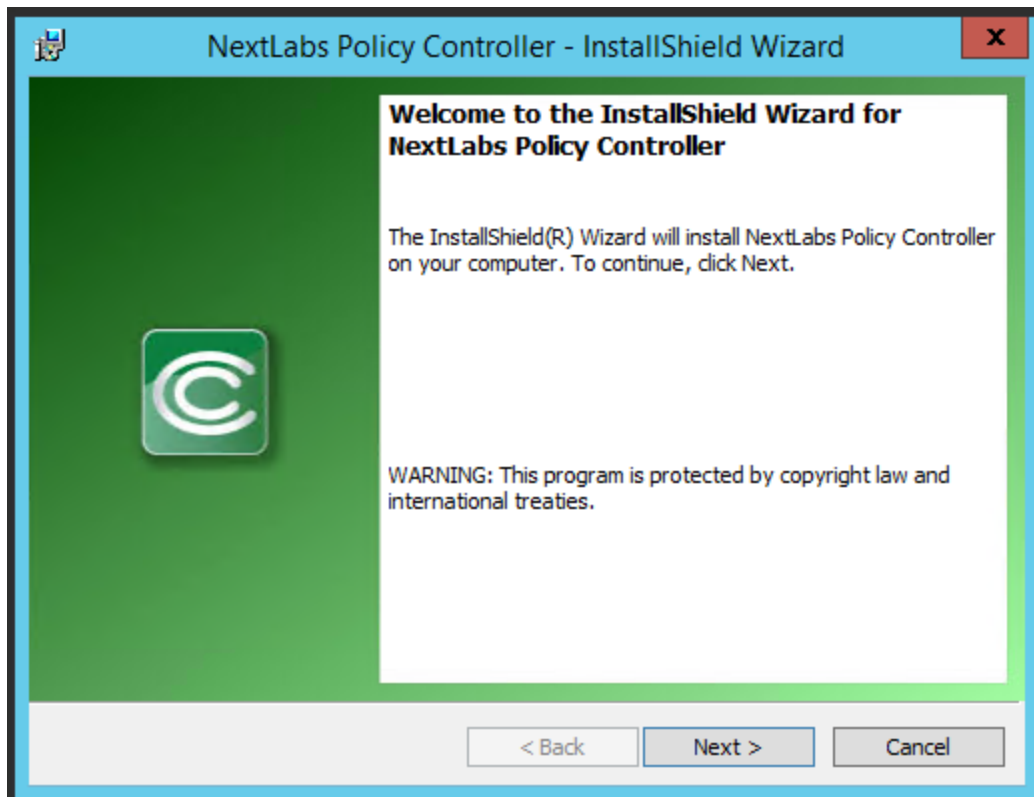
## 3681 7.5 Installation and Configuration of Policy Controller (PDP)

### 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

3696

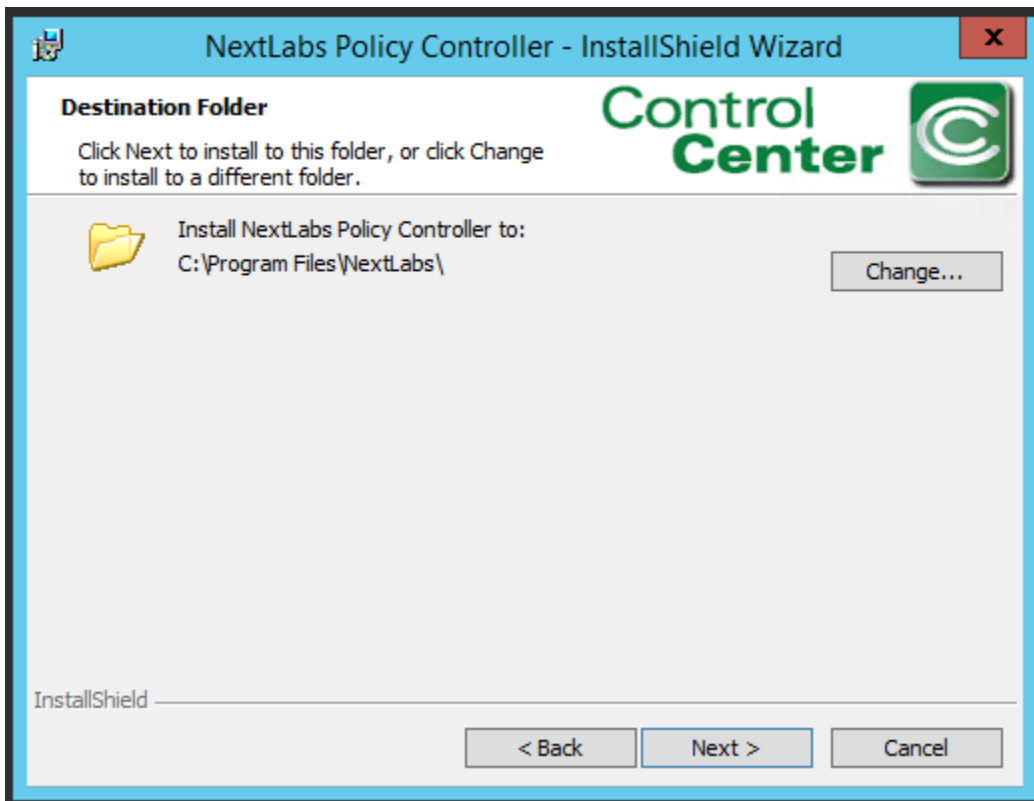
6. At the License Agreement screen, select **I accept the terms in the license agreement** and click **Next**.



3697

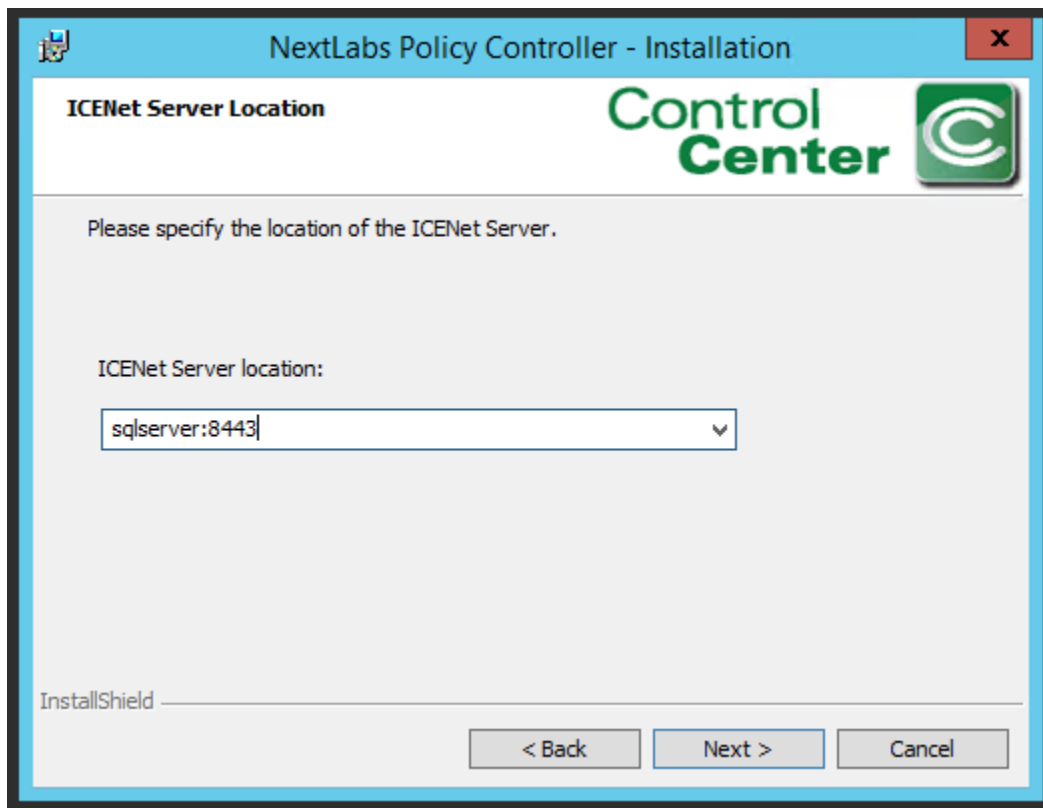
3698

7. At the Destination Folder screen, click **Next**.

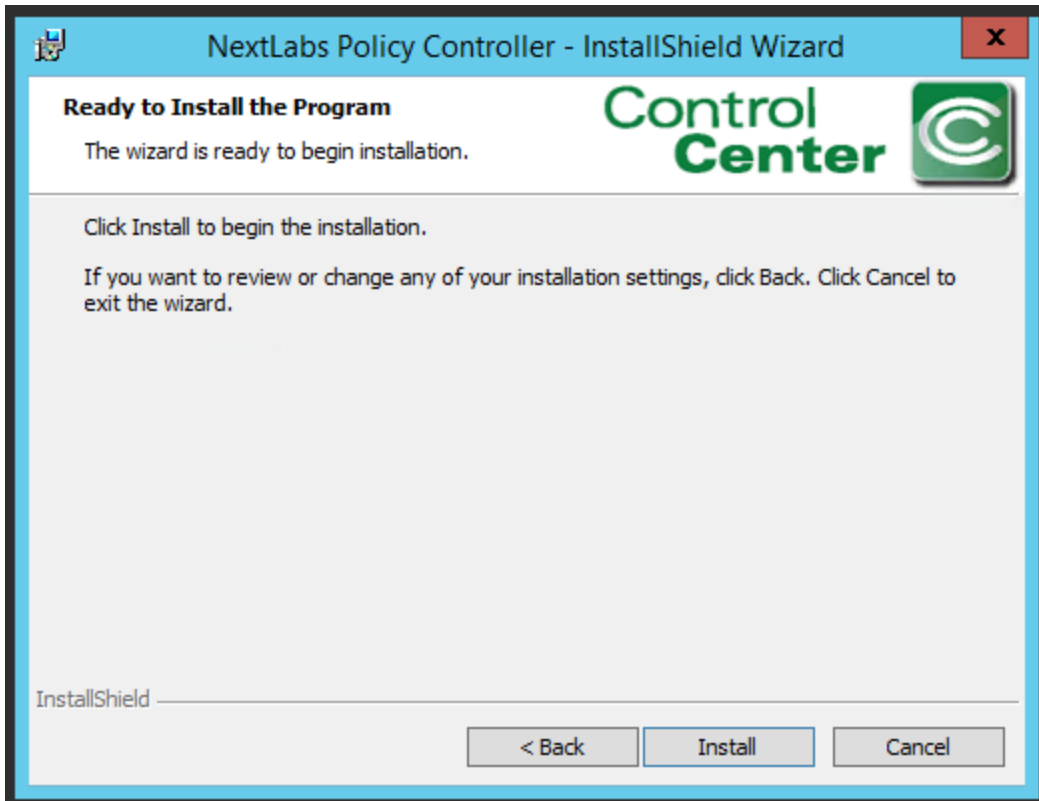


3699

- 3700 8. At the ICENet Server Location screen, enter the default ICENet Server Location: **sqlserver:8443**.  
3701 Click **Next**.



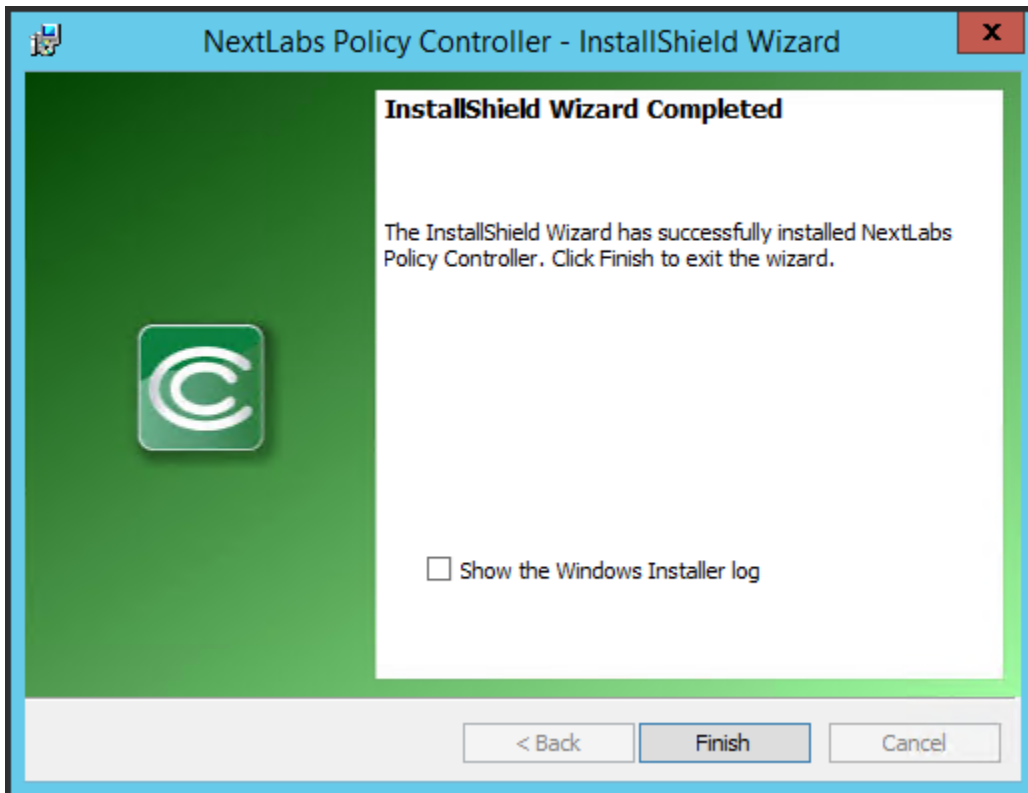
- 3702  
3703 9. At the Ready to Install the Program screen, click **Install**.



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).

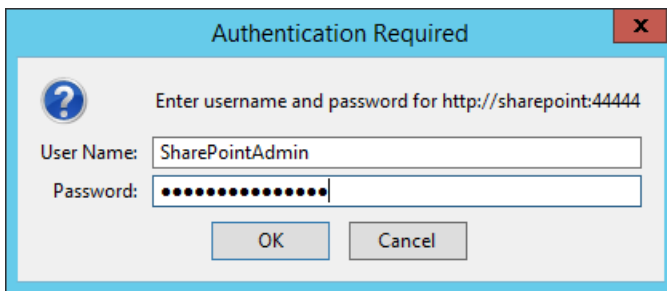
3709 **7.6 Installation and Configuration of NextLabs Entitlement Manager for**  
 3710 **SharePoint Server**

3711 **7.6.1 Installation and Configuration**

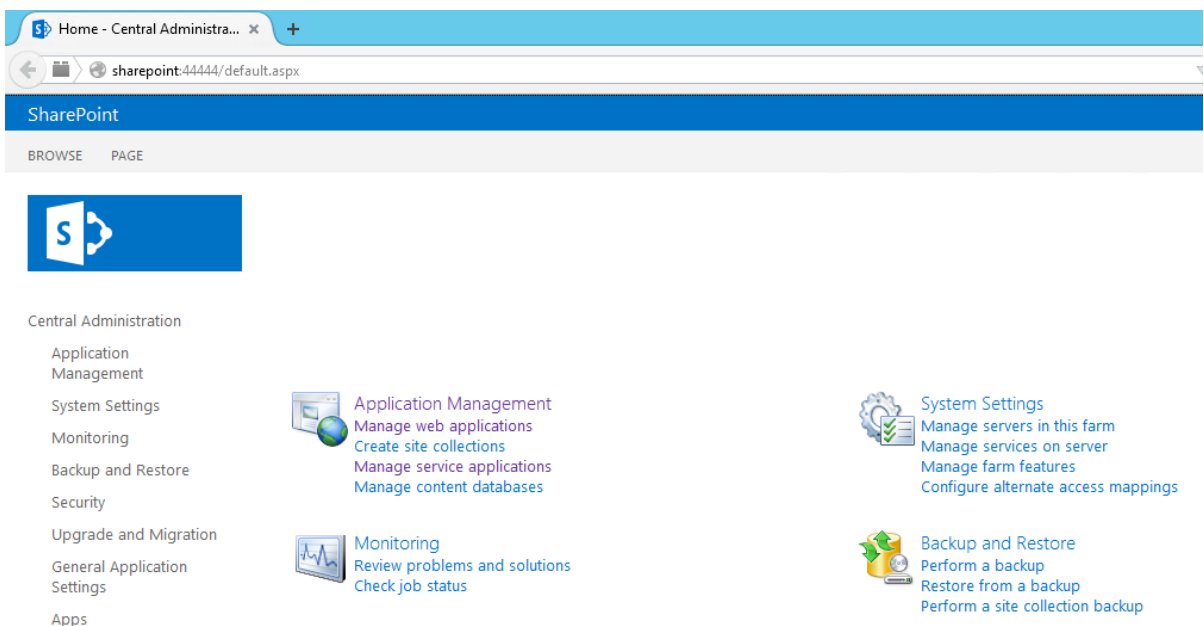
3712 Note: Prior to installing the Entitlement Manager for SharePoint Server, it is necessary to install the  
 3713 NextLabs Policy Controller on the SharePoint Server. If you have not already installed the Policy  
 3714 Controller, please refer to [Section 7.5](#) before proceeding.

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:  
 3717 <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  
 3719 click **OK**.

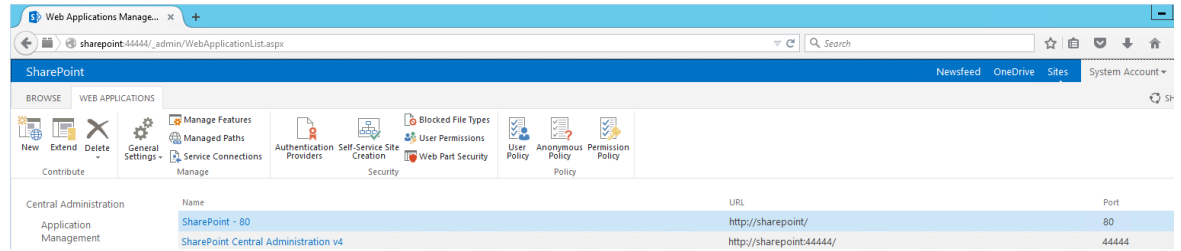


- 3720
- 3721 3. At the Central Administration page, click on **Manage web applications** under Application  
 3722 Management.



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](#)).

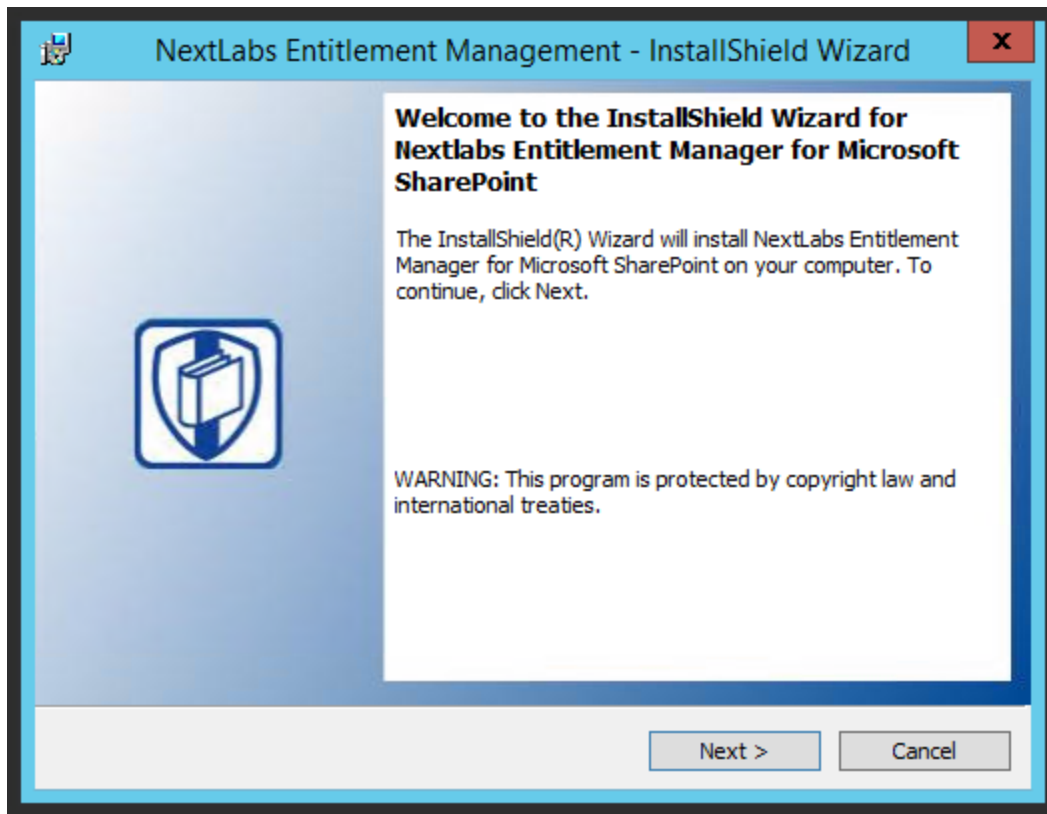


3726

3727 **7.6.1.2 Install NextLabs Entitlement Manager for SharePoint Server**

3728 Complete the standard Entitlement Manager for SharePoint Server installation per NextLabs  
 3729 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

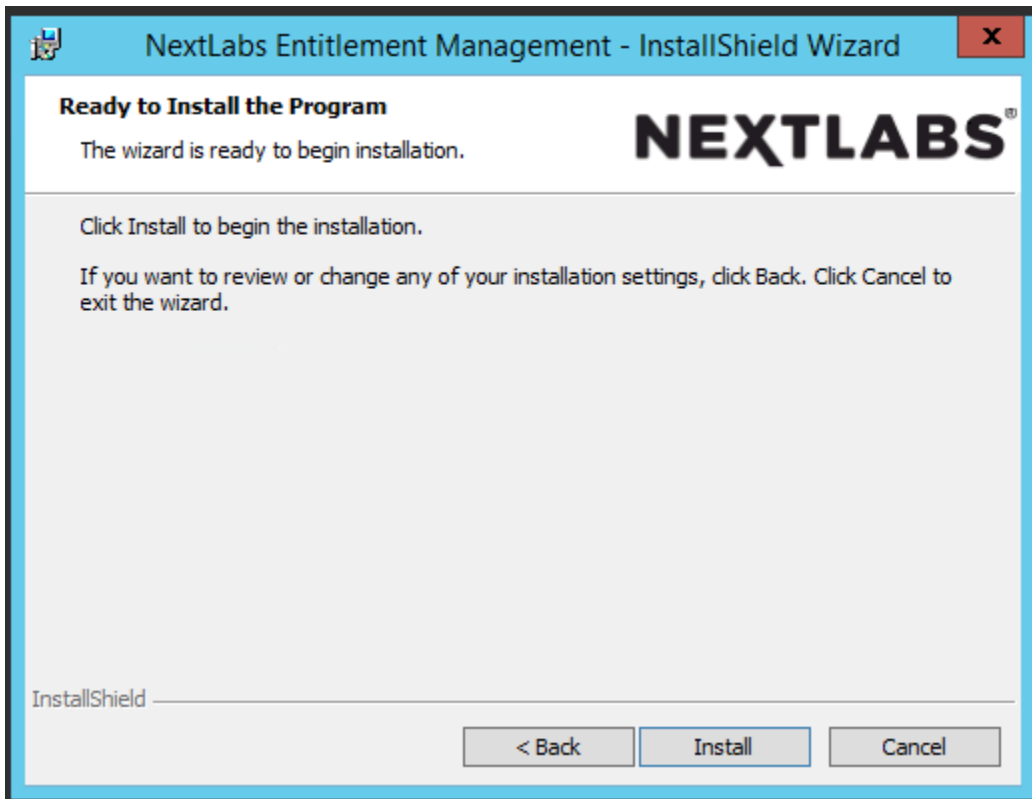
3741

6. At the License Agreement screen, select **I accept the terms in the license agreement** and click **Next**.



3742

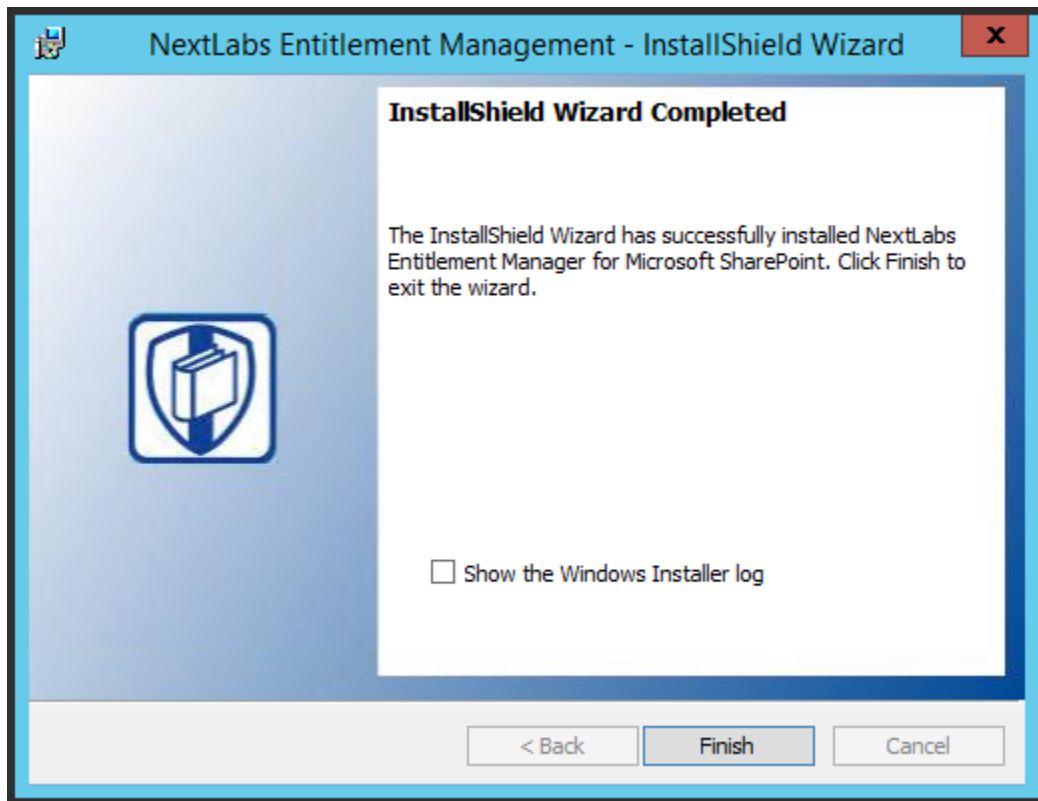
3743 7. At the Ready to Install the Program screen, click **Install**.



3744



- 3745 8. At the InstallShield Wizard Completed screen, click **Finish**.



3746

- 3747 9. After installing the IIS server must be reset:

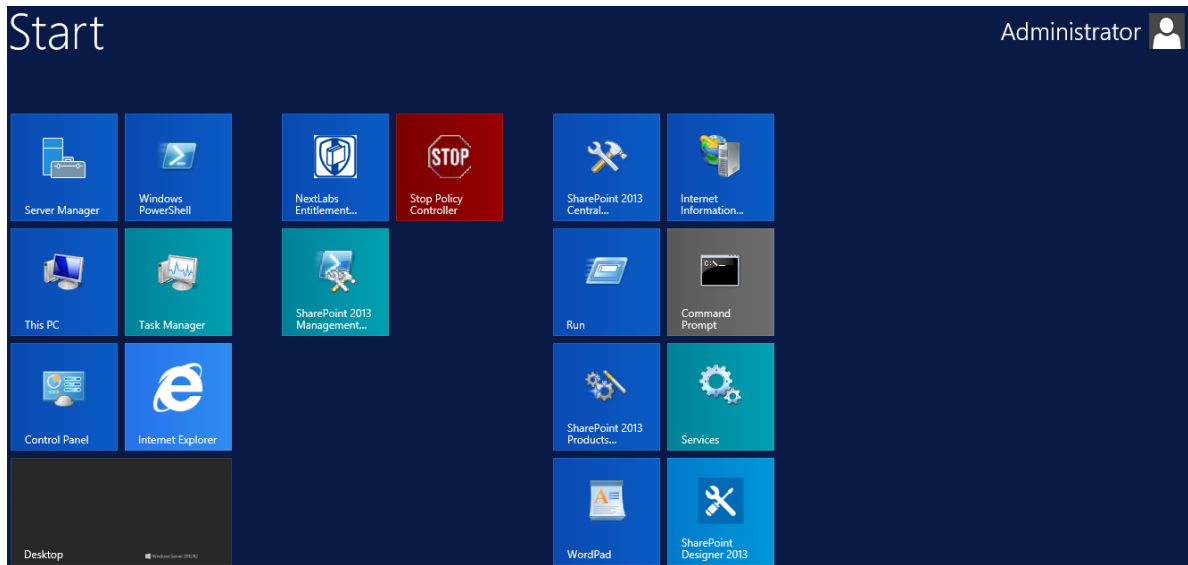
- 3748 a. Click on the Windows icon and begin typing the word **PowerShell**
- 3749 b. When the Windows PowerShell application icon appears, double-click on the icon to
- 3750 open the Windows PowerShell
- 3751 c. From within the Windows PowerShell window, type in this command and press Enter to
- 3752 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 created automatically, the application can be opened from File Explorer at the location:

3760

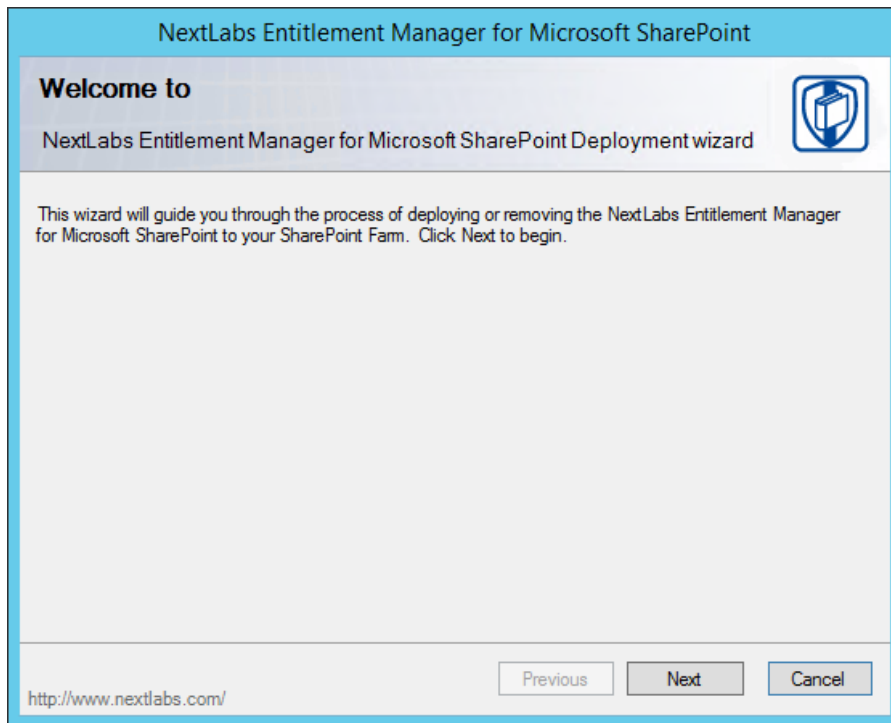
3761

*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 screen, click **Next**.

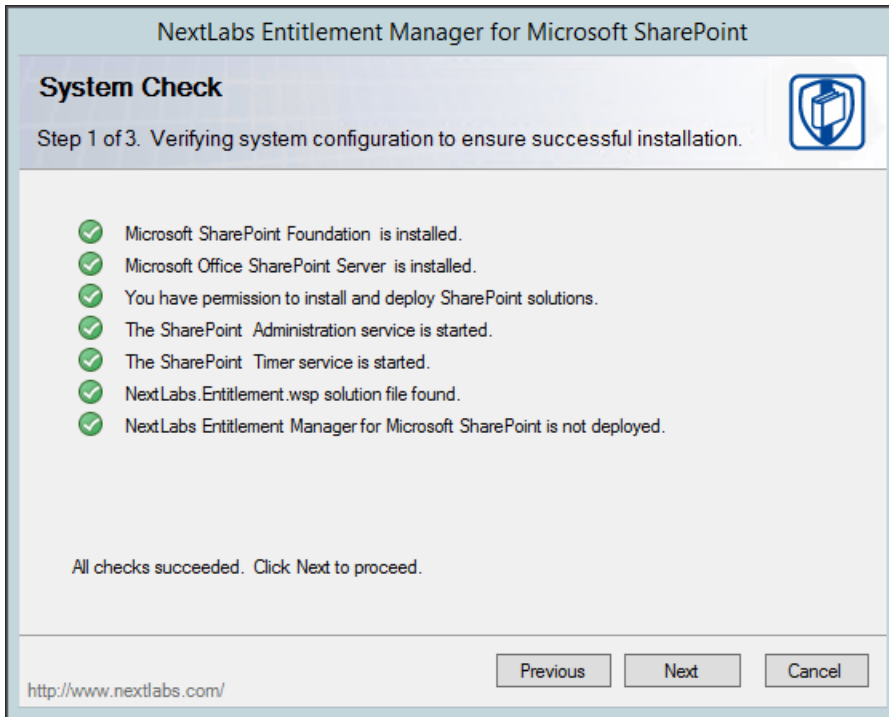
3763



3764

3765

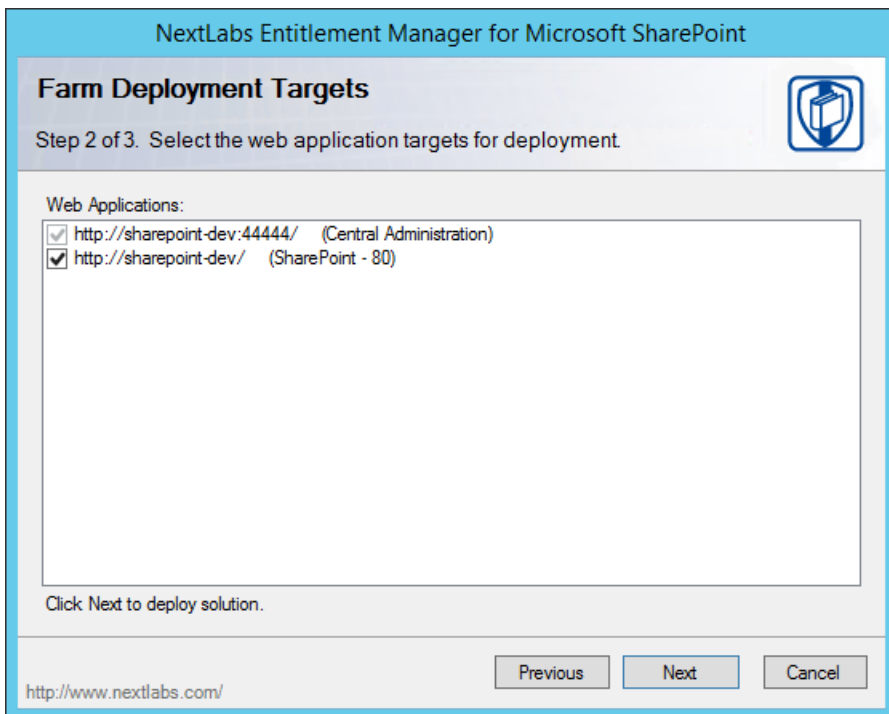
4. At the System Check screen, after the system check is complete, click **Next**.



3766

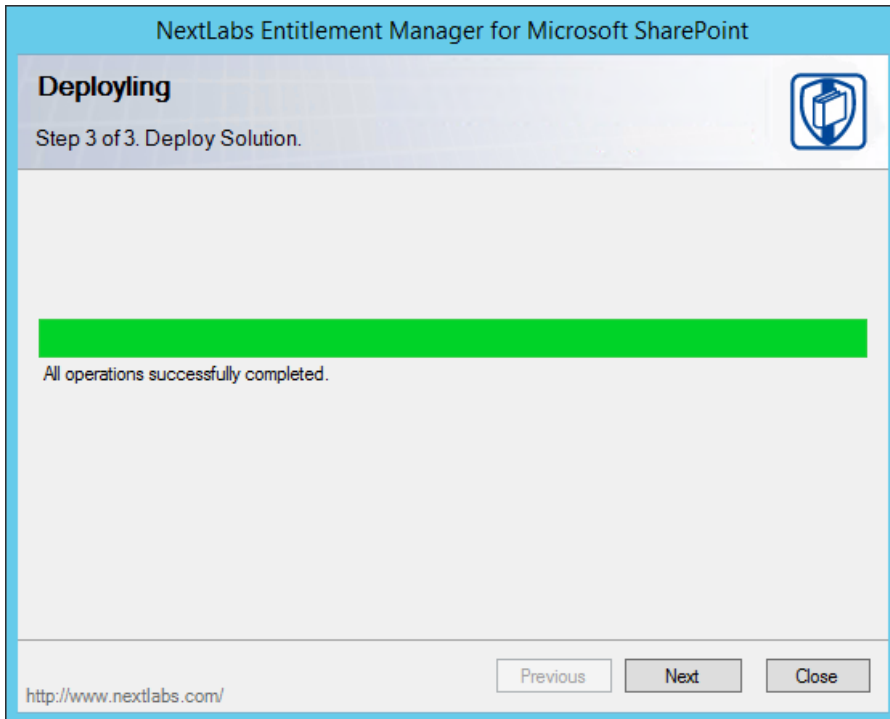
- 3767 5. At the Farm Deployment Targets screen, select the applicable web application on which to  
 3768 deploy.

3769 Note: if there is only one entry listed, i.e., *http://sharepoint:44444/Central Administration*, no  
 3770 web applications have been created. In that case, refer back to [Section 7.6.1.1](#).



3771

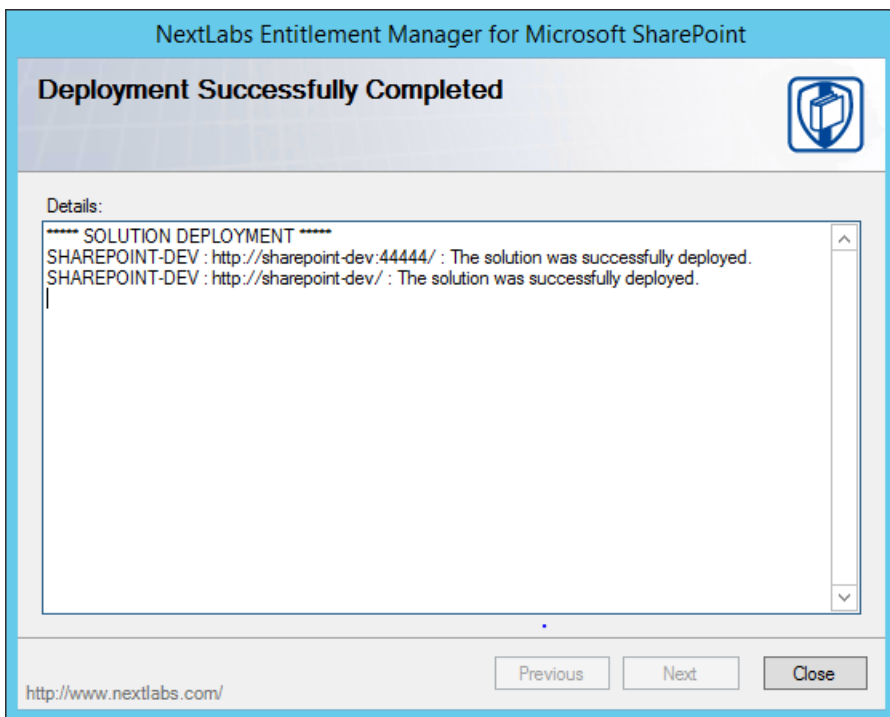
- 3772 6. At the Deploying Step 3 of 3 screen, click **Next**.



3773

3774

7. At the Successful Deployment Completed screen, click **Close**.



3775

3776

3777

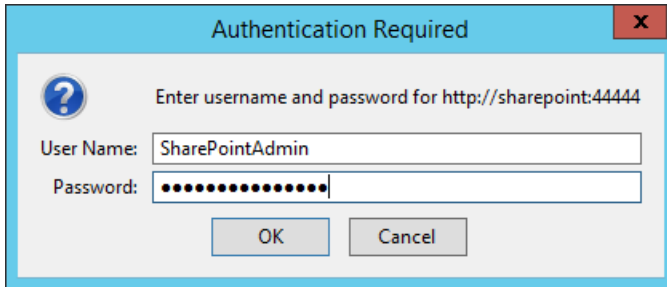
#### 7.6.1.4 *Enable Policy Enforcement on your Web Application via SharePoint Central Administration*

3778

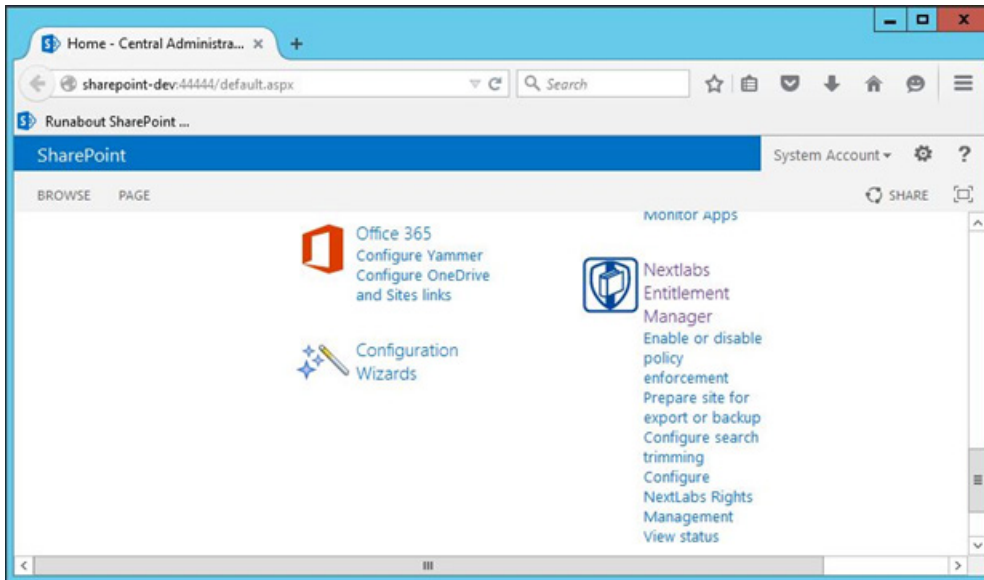
3779

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.

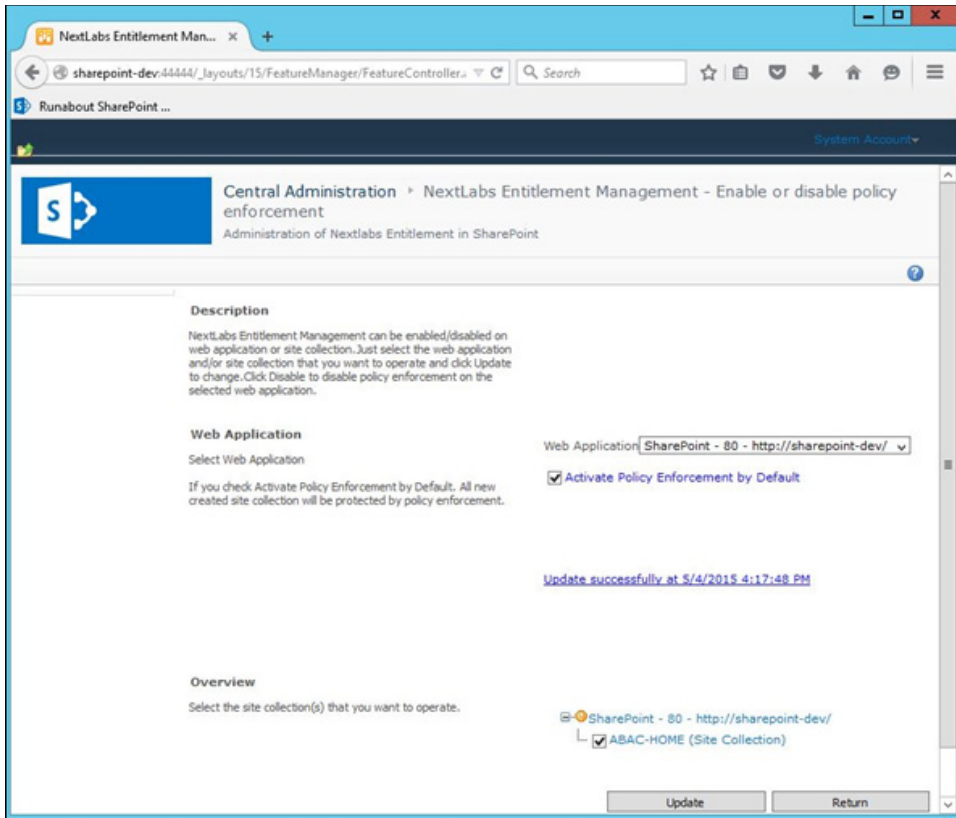
- 3780 2. Enter the **User Name** and **Password** for your SharePoint Central Administration account, and  
3781 click **OK**.



- 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**.

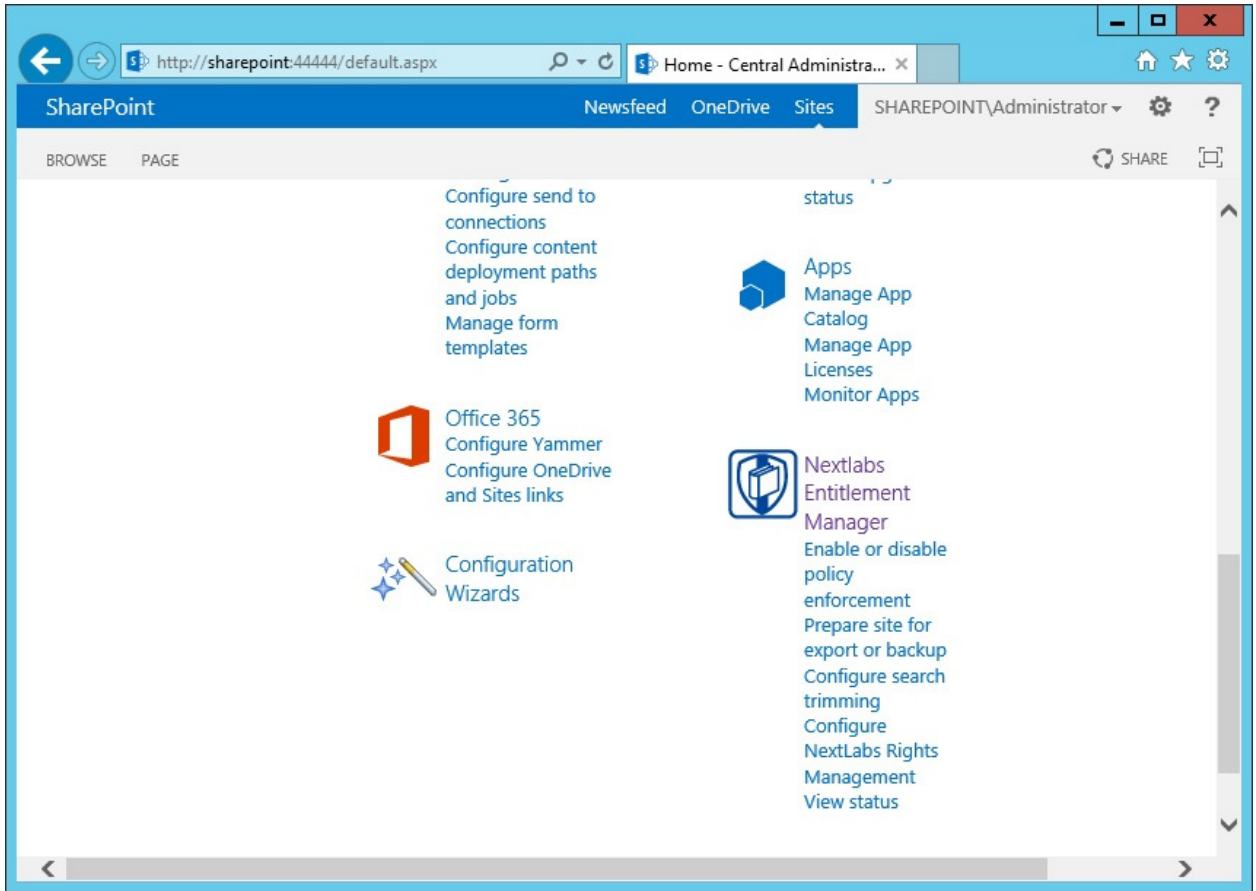


3787

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.

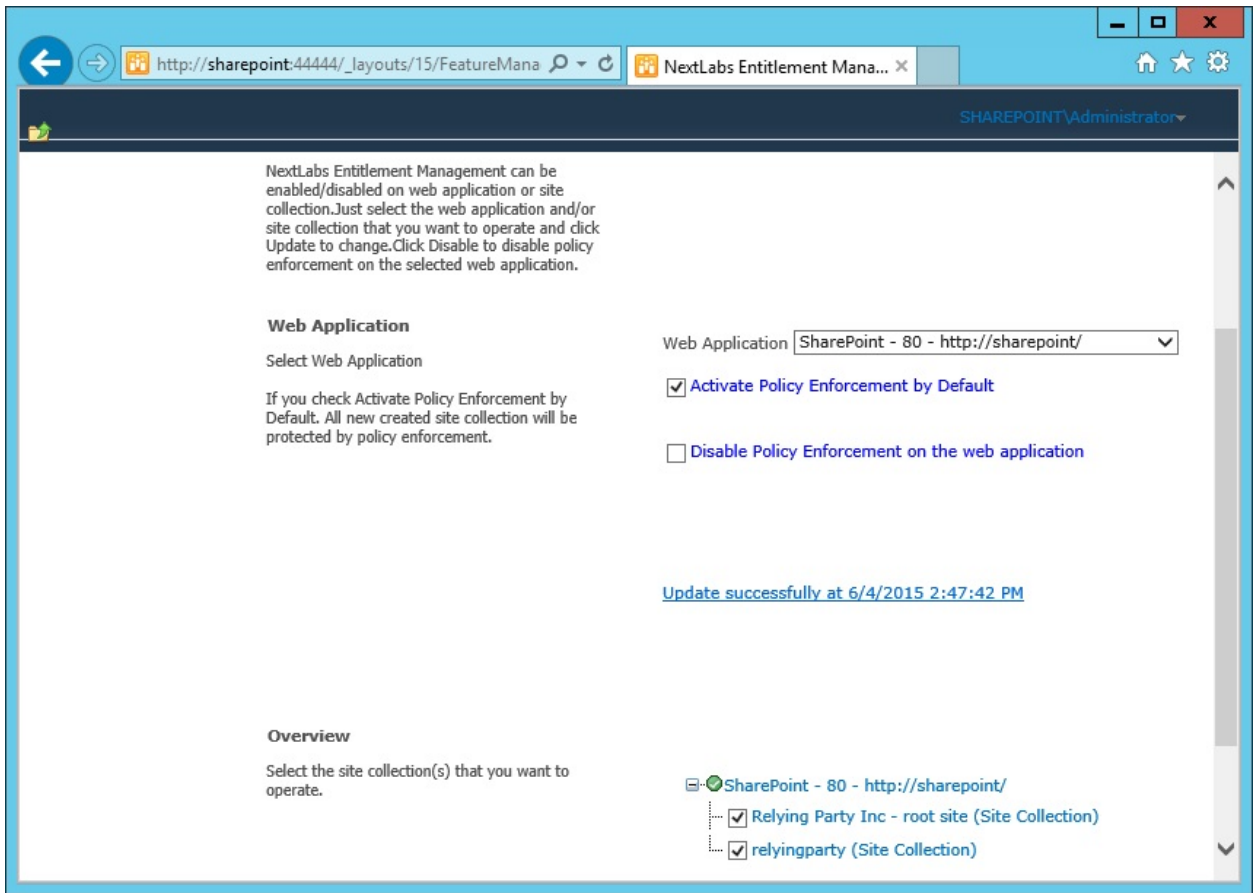


3798

3799

3800

3. Scroll down to the **Web Application** area to verify that the Entitlement Manager is activated for the correct SharePoint web application.

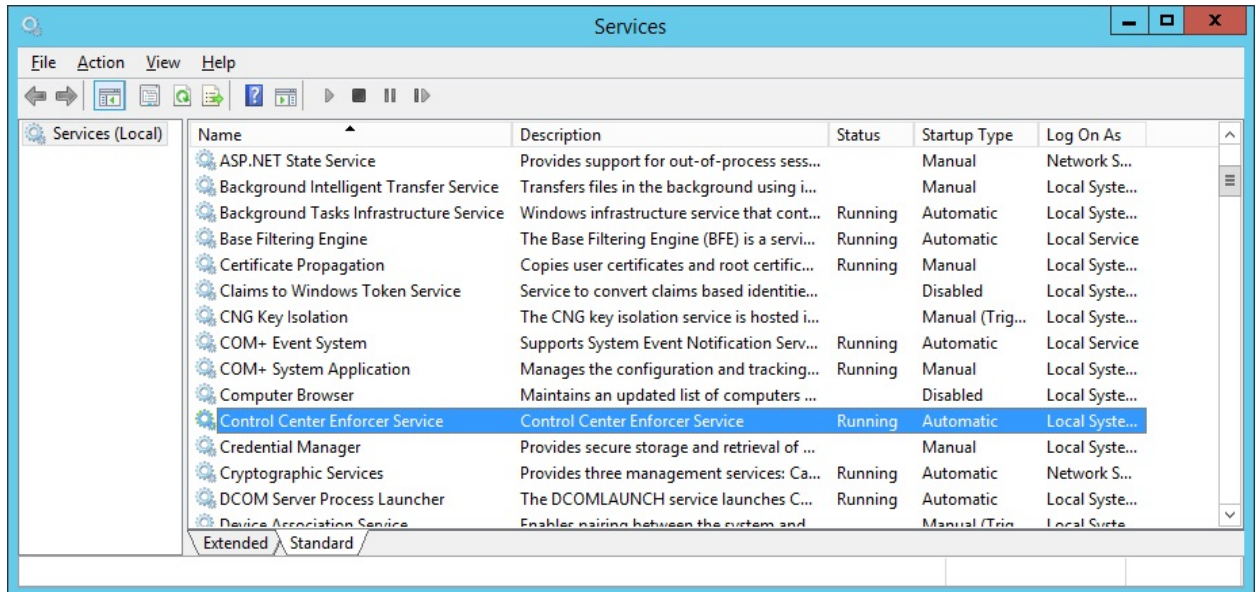


3801

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**.





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.

### 3830 8.1.1 Components and Sub-Components Used in this How-To Guide

- 3831 1. NextLabs Policy Studio –provides the Policy Administration Point of the ABAC architecture. This  
 3832 component was installed with the rest of the NextLabs product suite used in this  
 3833 implementation in [Section 7](#). Policy Studio provides the graphical user interface for Policy  
 3834 Lifecycle Management (defining, deploying, modifying, and deactivating policies).
- 3835 a. Located on the SQL Server
- 3836 2. NextLabs Policy Server SharePoint Enforcer configuration file
- 3837 a. Automatically exists after NextLabs Control Center installation
- 3838 b. Located within the NextLabs software architecture on the SQL Server
- 3839 3. NextLabs AgentLog and bundle.bin files
- 3840 a. Automatically exist after NextLabs Policy Controller installation
- 3841 b. Located within the NextLabs software architecture on the SharePoint Server

### 3842 8.1.2 Pre-requisites to Complete Prior to this How-To Guide

- 3843 1. If you intend to do a setup without identity federation and federated logins, you must:
- 3844 a. Install and configure Active Directory (see [Section 2](#)).
- 3845 b. Install and configure Microsoft SharePoint (see [Section 4](#)).
- 3846 c. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see  
 3847 [Section 7](#)).
- 3848 2. If you intend to incorporate a trust relationship between an IdP and RP, and use federated logins  
 3849 into SharePoint, you must:
- 3850 a. Install and configure Active Directory (see [Section 2](#)).
- 3851 b. Setup and configure the RP and IdP (see [Section 3](#)).
- 3852 c. Install and configure Microsoft SharePoint (see [Section 4](#)).
- 3853 d. Configure the SharePoint federated login with the RP (see [Section 5](#)).
- 3854 e. Configure the attribute flow between all endpoints (see [Section 6](#)).
- 3855 f. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see  
 3856 [Section 7](#)).

## 3857 8.2 Policy Strategy

### 3858 8.2.1 Top-Level Blacklisting Deny Policy, Whitelisting Allow Sub-Policies

3859 In order to demonstrate a policy set with high security and fine-grained control, we employed a general  
 3860 blacklisting, then fine grained whitelisting sub-policy strategy for the policies. We chose this strategy  
 3861 because we considered it a more secure paradigm for securing SharePoint resources. Using this strategy,  
 3862 the access control logic initially applies a general deny all access decision at the top level for a given set  
 3863 of related attributes, then specifies conditions under which access can be allowed in various sub-policies  
 3864 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.

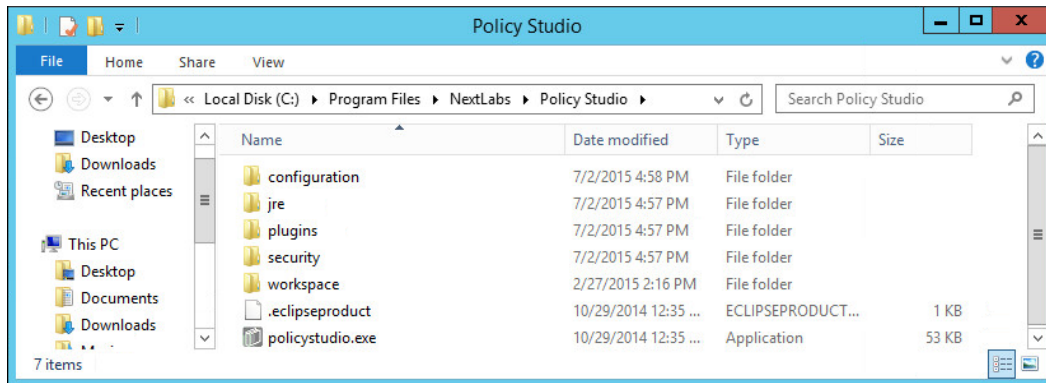
## 3946    **8.4    Using the NextLabs Policy Studio GUI for Policy Definition and** 3947                    **Deployment**

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.

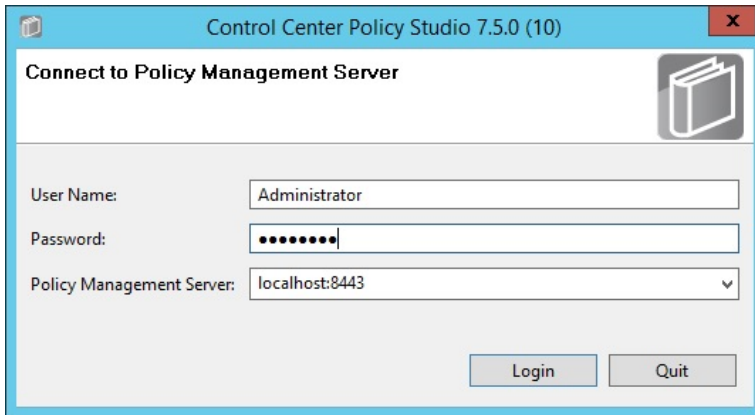
### 3953    **8.4.1    Login and Initial Screen in Policy Studio**

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 **polycystudio.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 **polycystudio.exe**.



- 3962
- 3963            2. In the Control Center Policy Studio window, enter **User Name** and **Password**, then click **Login** to  
 3964            connect to the Policy Management Server.



3965

3966

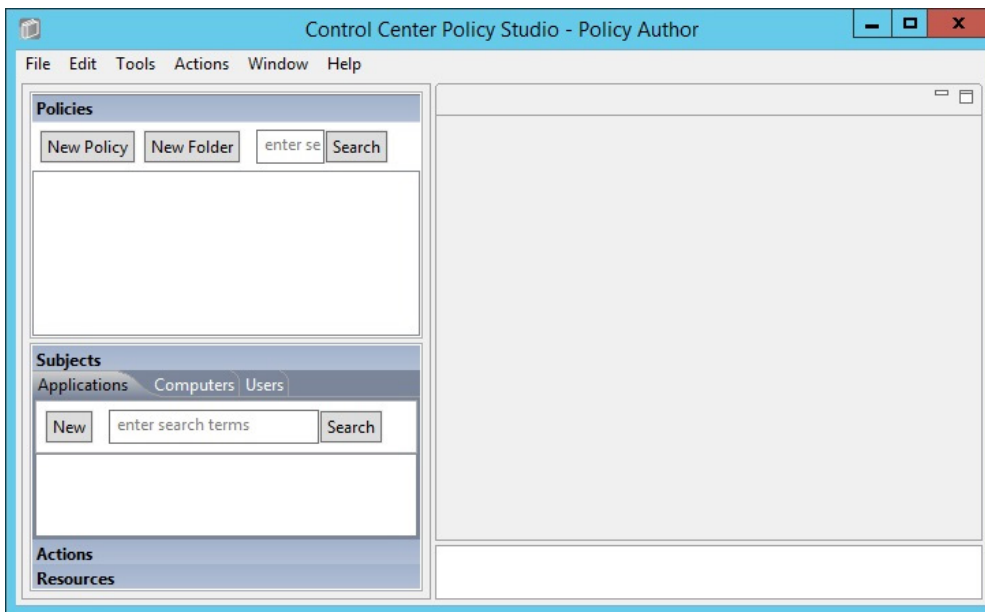
3967

3968

3969

3970

3. If login was successful, you will see the Policy Studio’s graphical user interface, specifically the main screen where new policies and new components are defined, deployed, modified, and deactivated. Note the **Policies** panel in the top-left, the **Components** panel in the bottom-left, and an open space to the right where editing panels emerge for editing the policies and components.



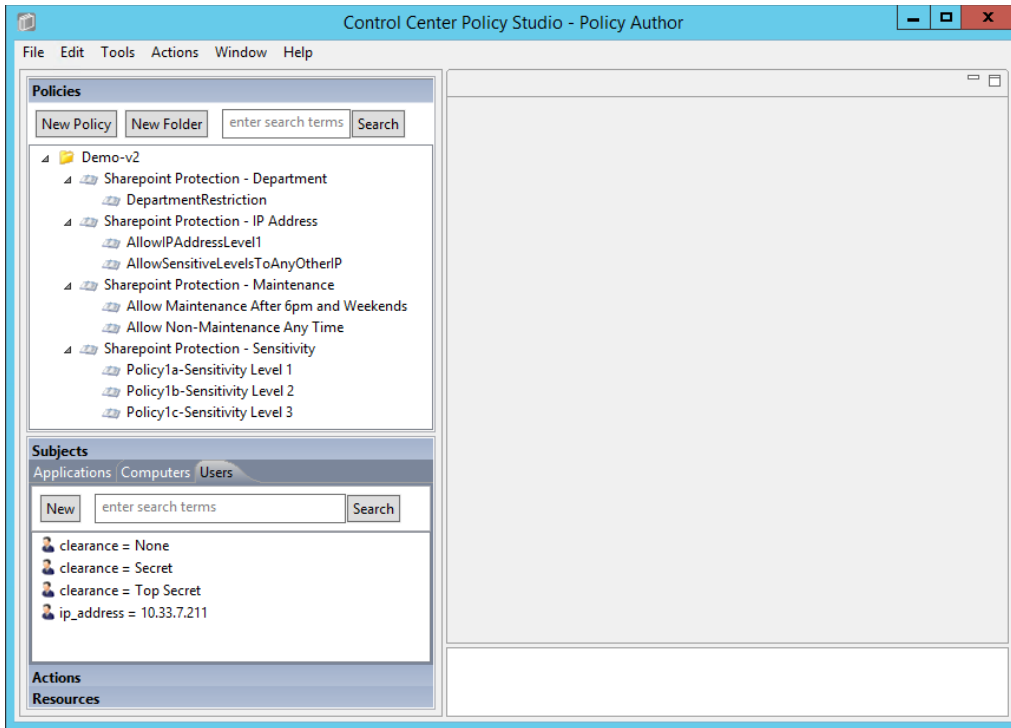
3971

3972

3973

3974

4. After following the instructions in this section to define and deploy several user and resource components, as well as four policy sets, the Policy Studio interface will show the new 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

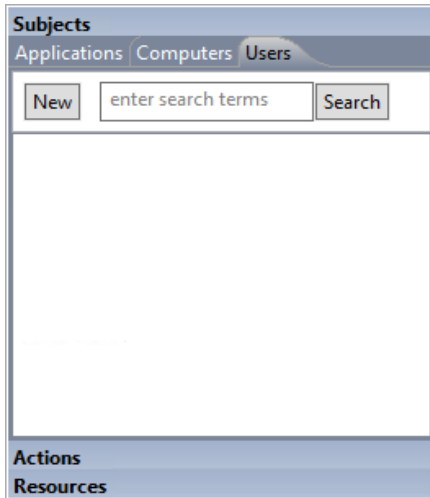


4005 note regarding the user IP address component: even though IP address is an environmental attribute, it  
4006 can be configured in NextLabs as a user attribute coming from SharePoint Claims, or as a resource  
4007 attribute, which requires different configuration in NextLabs. For our example, we use the IP Address  
4008 from SharePoint Claims, which is handled as a user attribute.

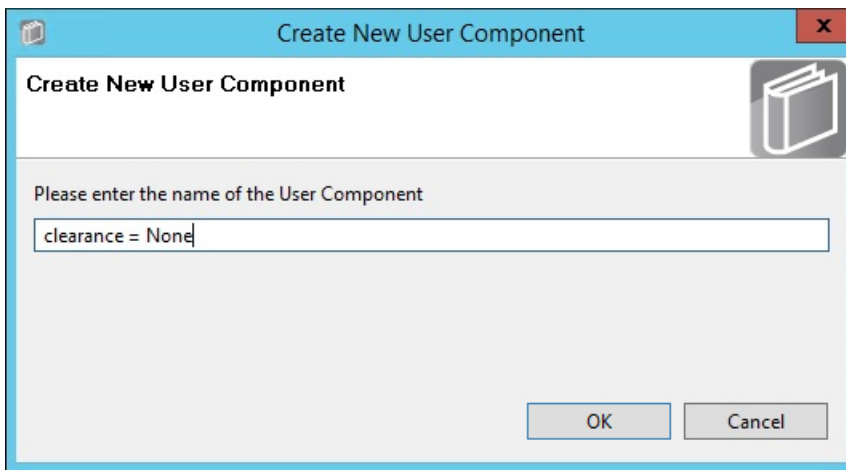
4009 [8.4.3.2.1 Clearance Components](#)

4010 [8.4.3.2.1.1 CLEARANCE = NONE](#)

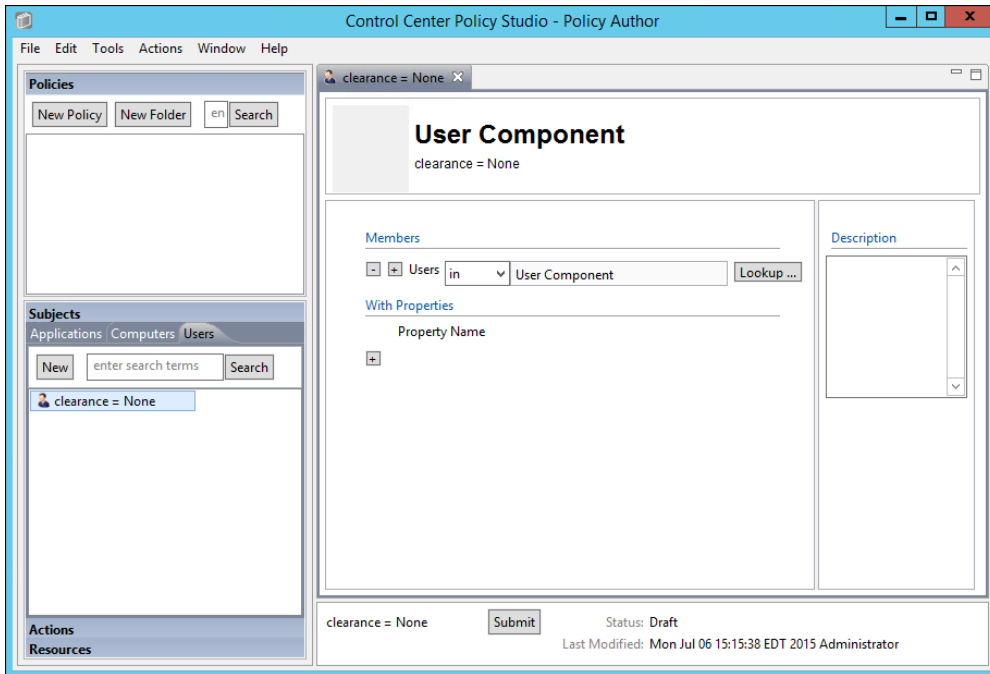
- 4011 1. In the Components panel in the bottom-left of the Policy Studio window, click on the **Subjects**  
4012 heading, and then click on the **Users** tab. Then click **New** to create a new component.



- 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:



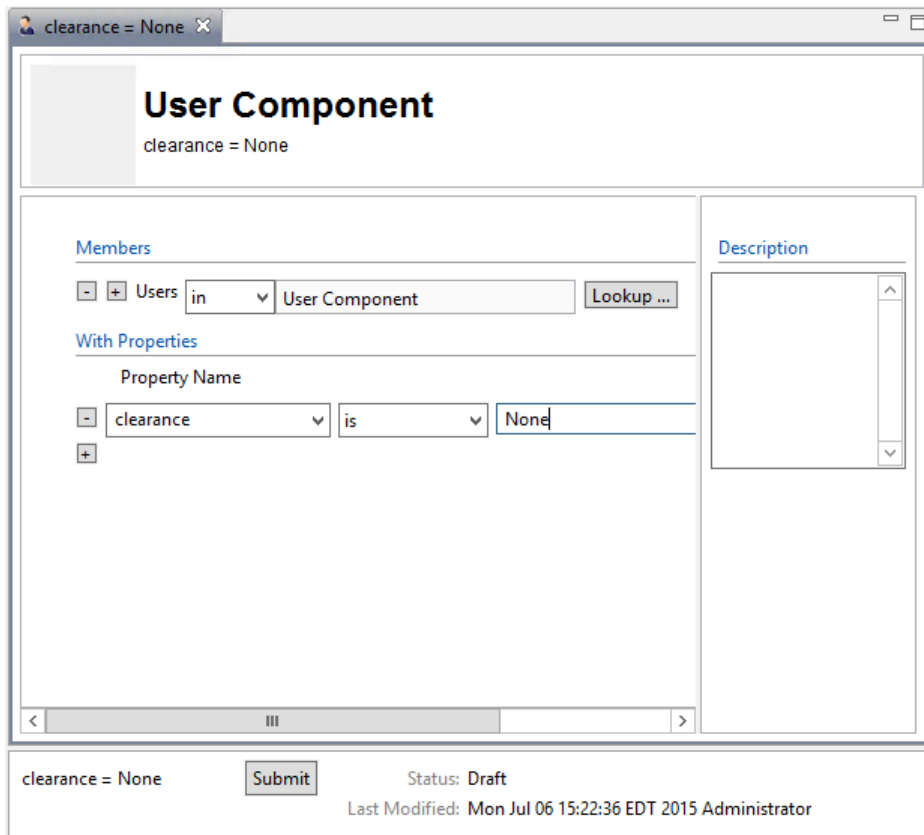
4018

4019

4020

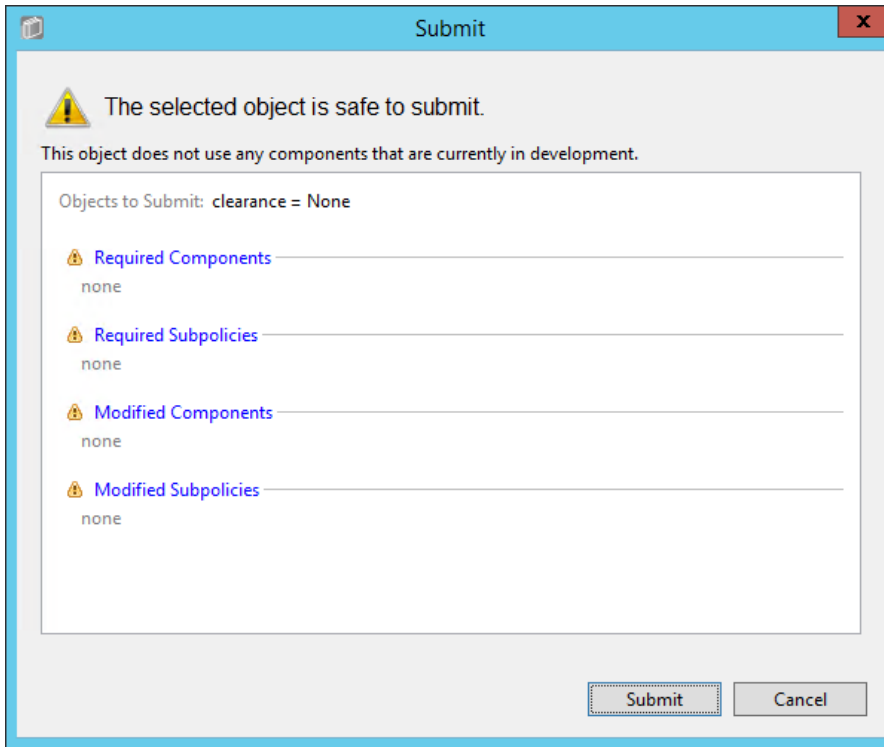
4021

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**.



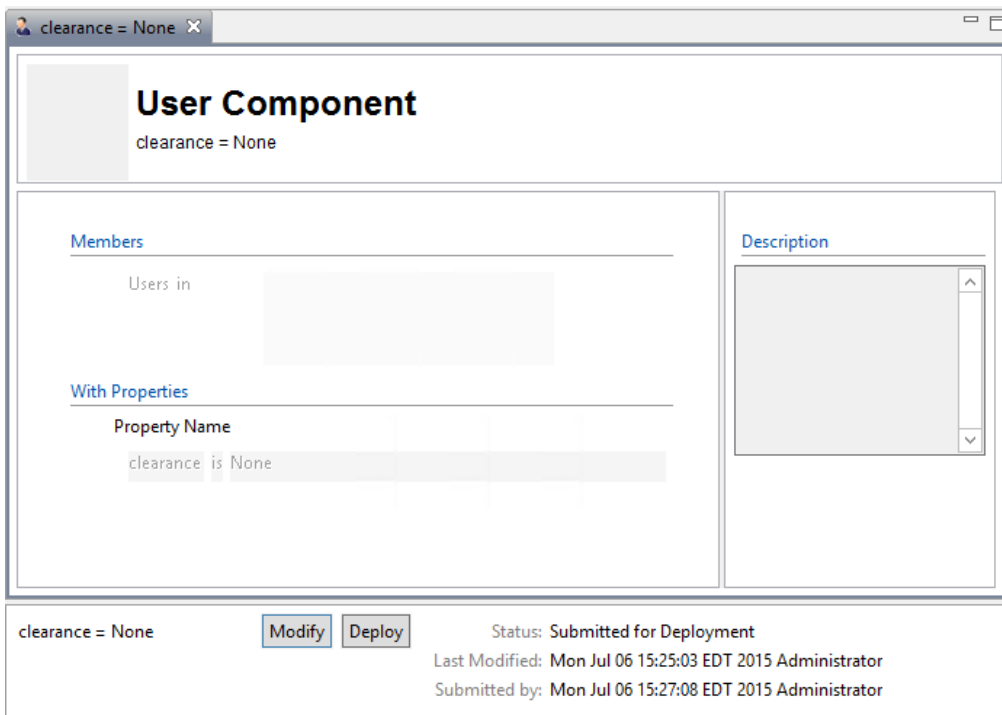
4022

4023 5. In the Submit window, click **Submit**.



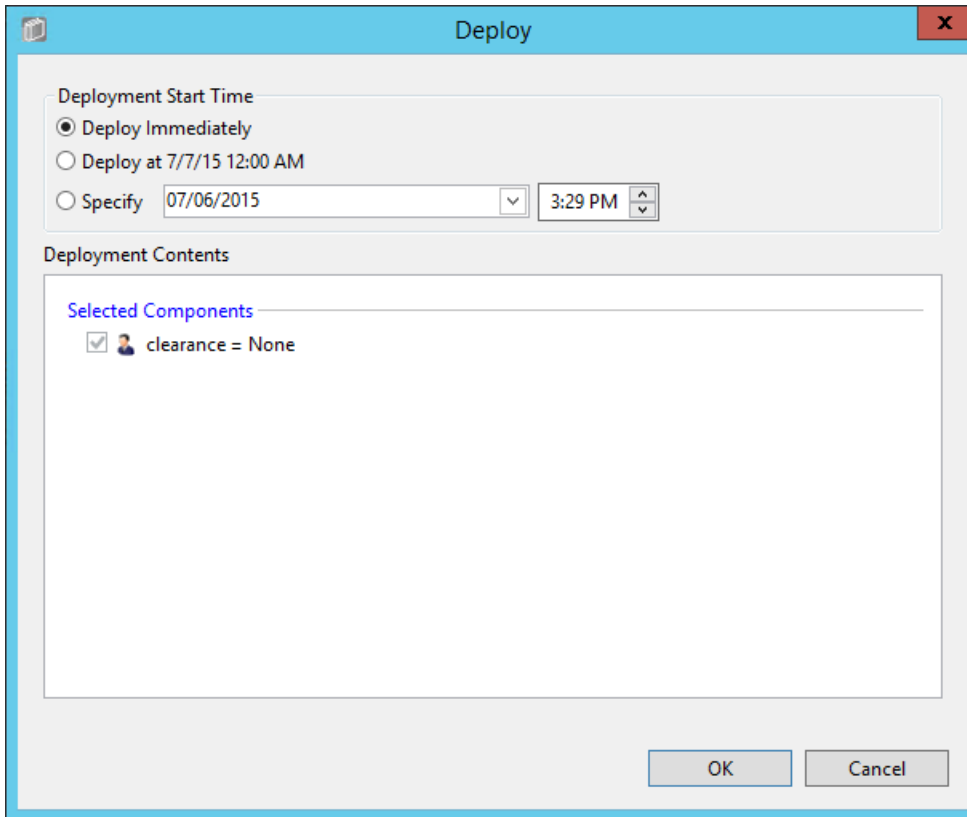
4024

4025 6. From the component editing panel, note the differences. The new status reads **Submitted for**  
4026 **Deployment**. Click **Deploy**.

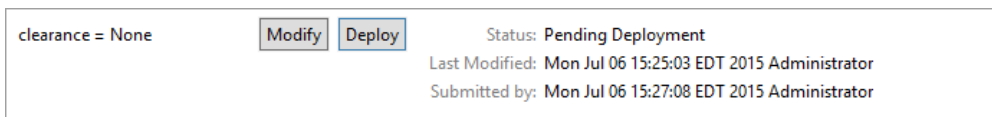


4027

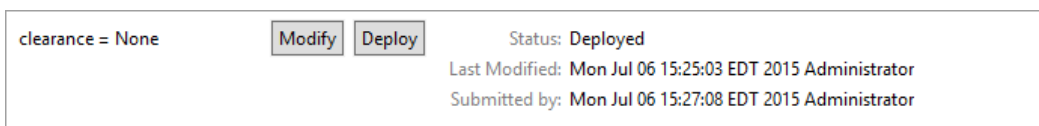
- 4028 7. In the Deploy window, click **OK**. Note: You may deploy immediately, which we choose in our  
 4029 example. You could also deploy the following day at midnight, or at a different specific date and  
 4030 time.



- 4031  
 4032 8. Verify at the bottom of the component editing panel that the Status now reads **Pending**  
 4033 **Deployment**. This will remain for the duration of the heartbeat (described in [Section 7](#)).



- 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.

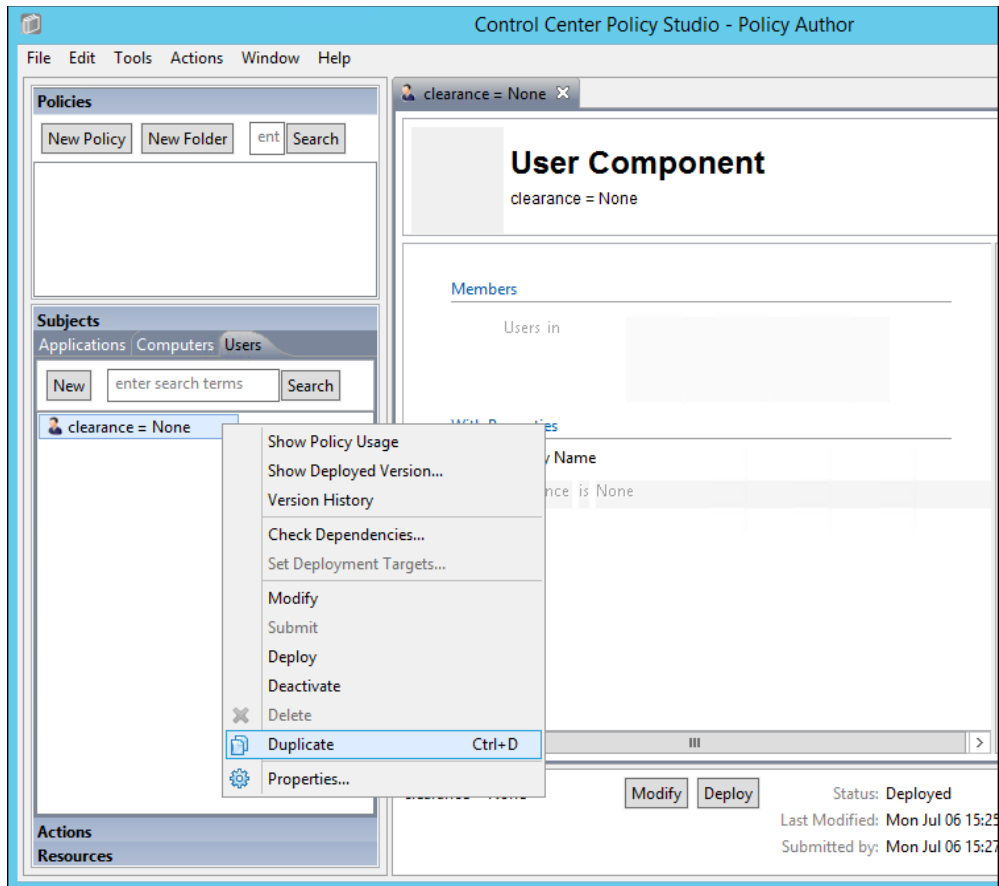


4037

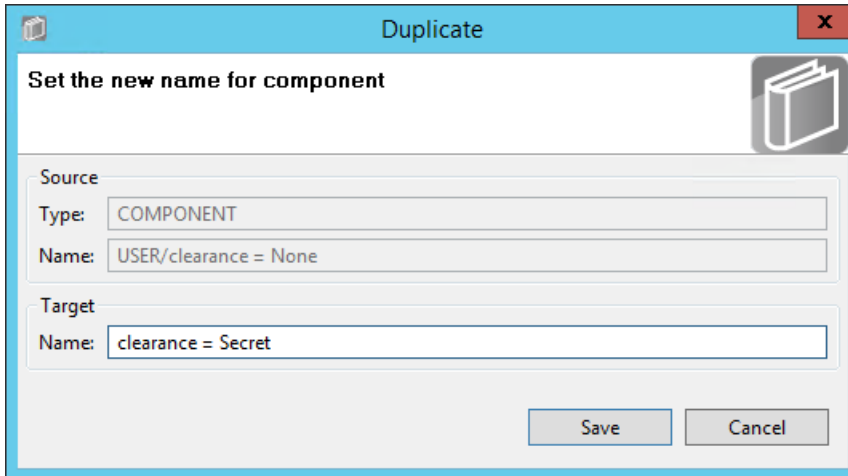
## 4038 8.4.3.2.1.2 CLEARANCE = SECRET

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:



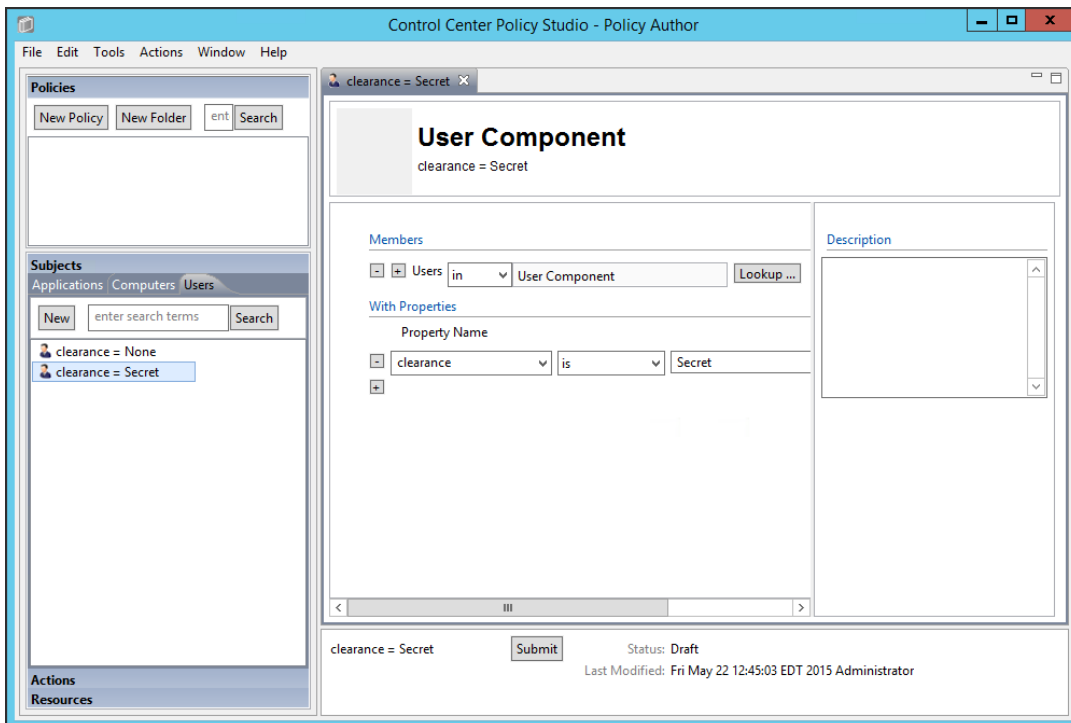
- 4045 3. In the Duplicate window, edit the name of the new component, i.e., clearance = **Secret**. Click  
4046 **Save**.  
4047



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

4054

4055

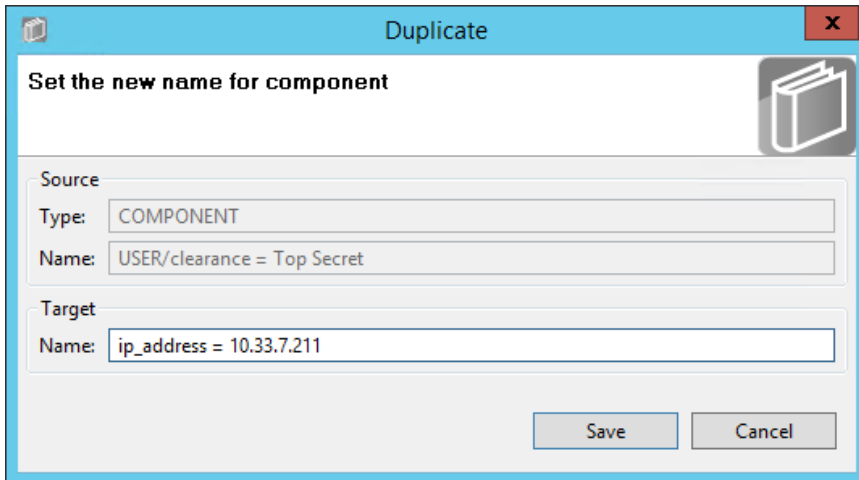
1. Repeat steps 1-5 in [Section 8.4.3.2.1.2](#) for duplicating a new user attribute component. The new component should be named **clearance = Top Secret**, and the property value should equal **Top Secret**.

4056 **8.4.3.2.2 IP Address component**

4057

4058

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**.

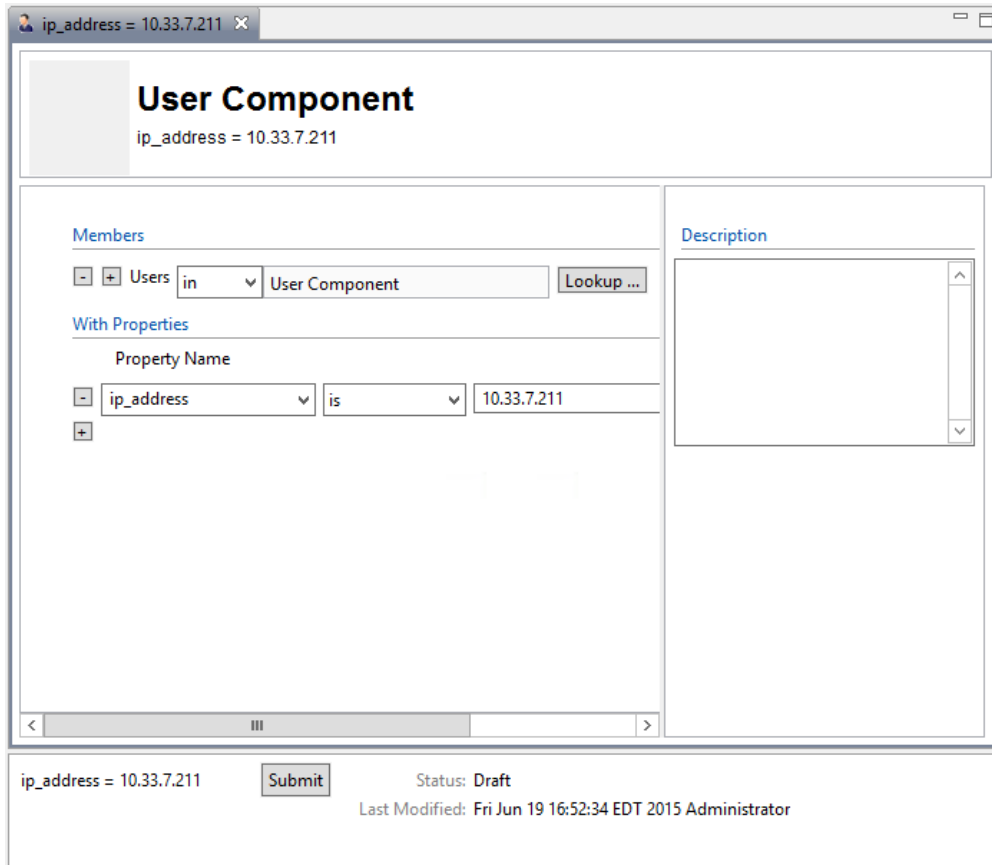


4059

4060

4061

- From the component editing panel, edit the **Property Name** to **ip\_address** and the value to **10.33.7.211**, leaving the default action **is**. Then click **Submit**.



4062

4063

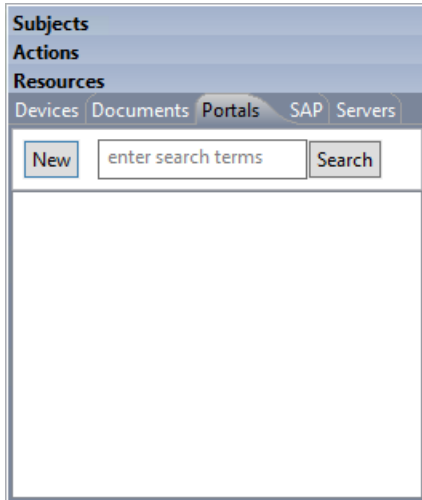
- Repeat steps 5-9 from [Section 8.4.3.2.1.1](#) to Submit and Deploy this component.

4064 *8.4.3.3 Defining and Deploying Resource Components*

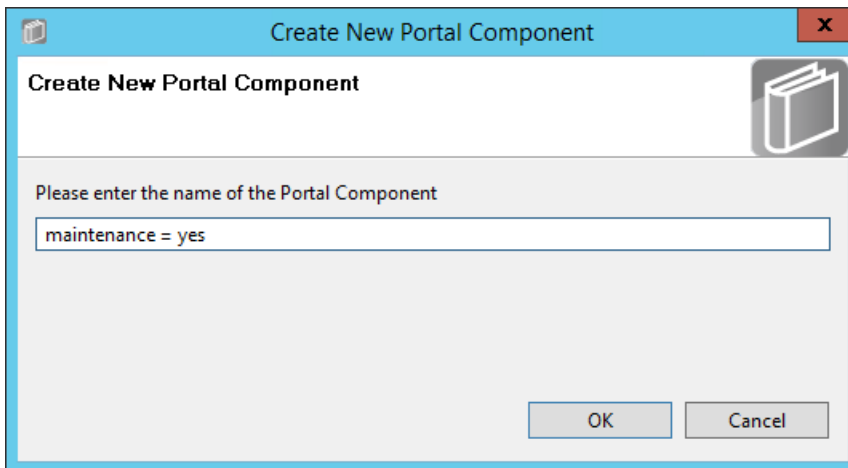
4065 8.4.3.3.1 Maintenance components

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**
- 4068 heading, and then click on the **Portals** tab. Then, click **New** to create a new component.

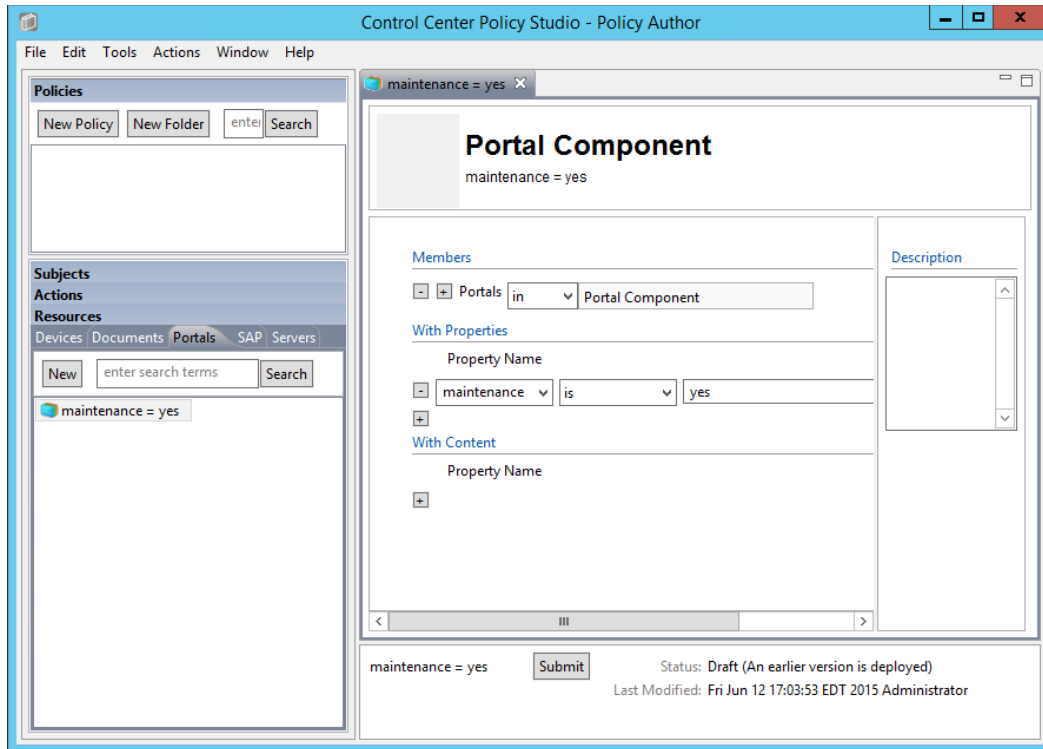


- 4069
- 4070 2. Enter a descriptive component name, such as **maintenance = yes**, then click **OK**.



- 4071
- 4072 3. In the editing panel, click on the **plus sign** box under Property Name and enter **maintenance** in
- 4073 the **Property Name** text box, keep the default **is** as the action, and enter **yes** into the value text
- 4074 box. Then click **Submit**.





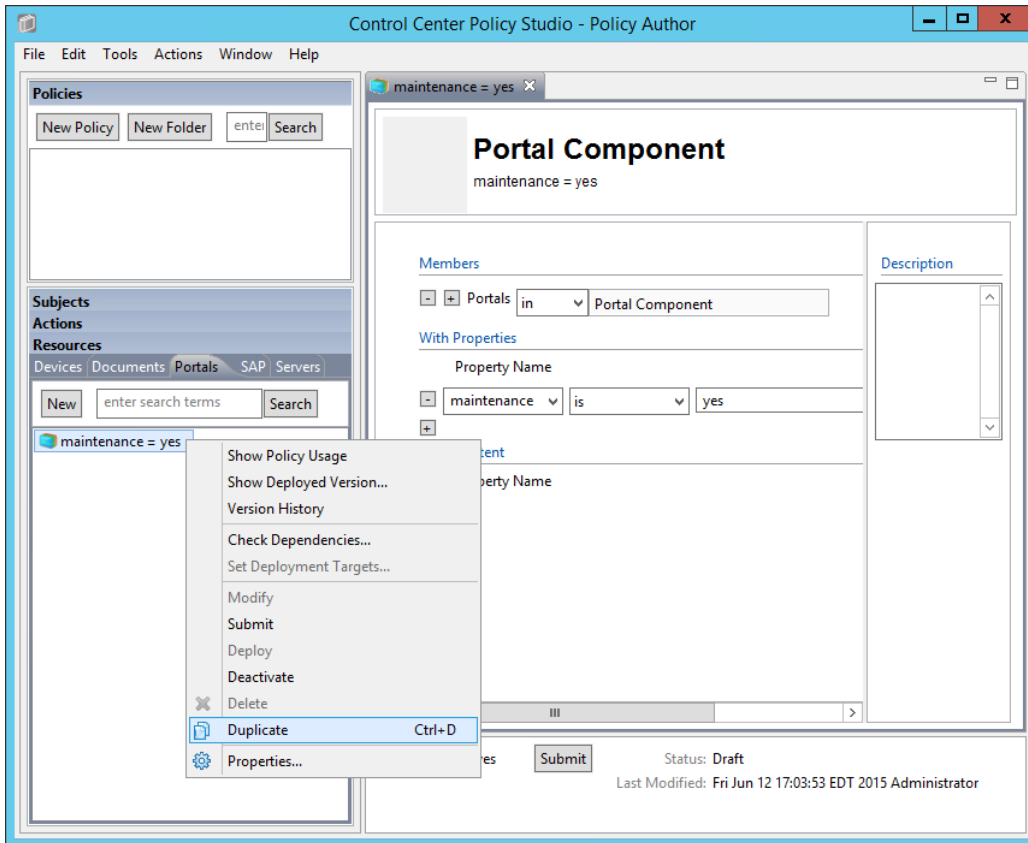
4075

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.

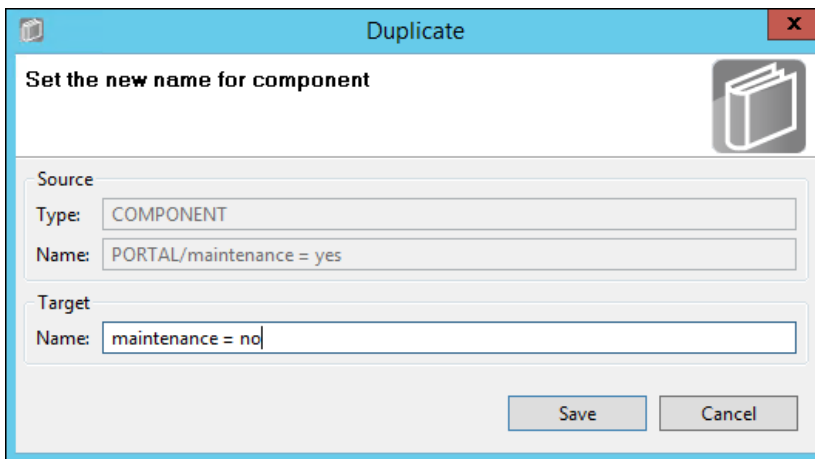
- 4080 1. In the Component panel in the bottom-left corner of the Policy Studio interface, right-click on  
 4081 the **maintenance = yes** component. In the floating menu, select **Duplicate**.



4082

4083

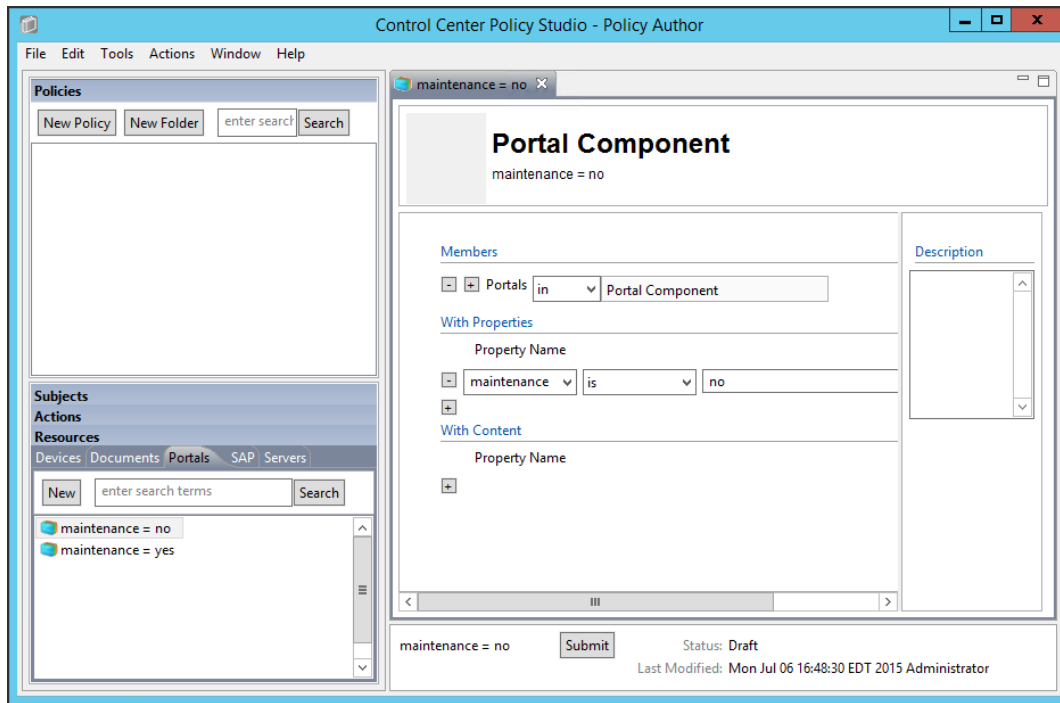
2. In the Duplicate window, edit the name of the new component. Example: **maintenance = no**.



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 \*.

Project status = any

## Portal Component

Project status = any

**Members**

- + Portals in Portal Component

**With Properties**

Property Name

- project status is \*

+

**With Content**

Property Name

+

**Description**

Project status = any  Status: Draft  
Last Modified: Fri Jun 12 15:13:49 EDT 2015 Administrator

4103

4104 

## 8.4.4 Defining Policy

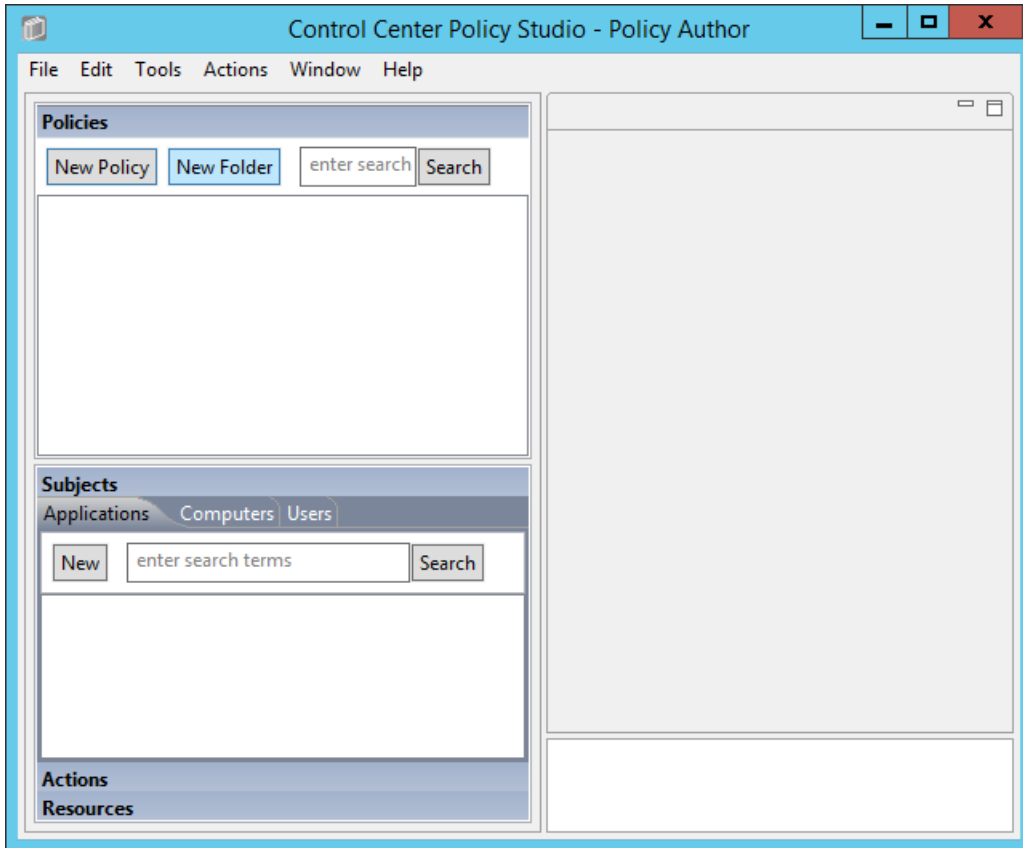
4105 After following the steps to define and deploy components in [Section 8.4.3](#), you can continue on to  
 4106 define policies that relate to the Runabout Air scenario business rules discussed in [Section 8.3](#). In order  
 4107 to define policies in Policy Studio, login as described in [Section 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.

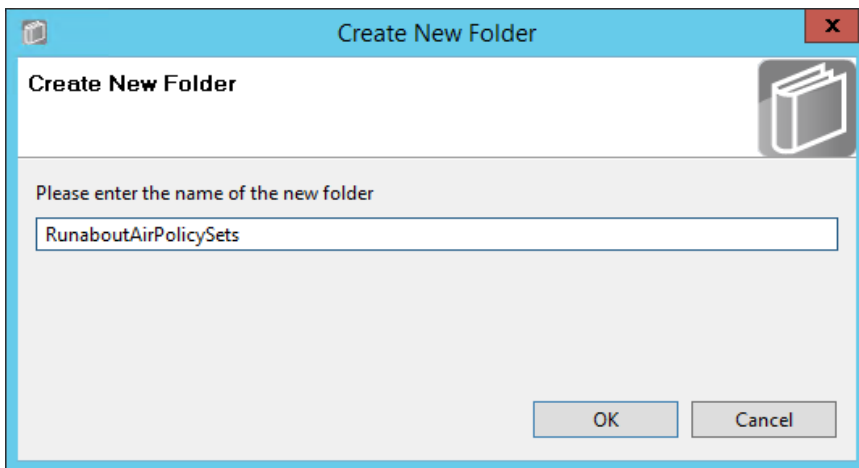
- 4111 1. From the main Policy Studio window, click **New Folder**.



4112

4113

2. Enter the **name** of your folder and click **OK**.

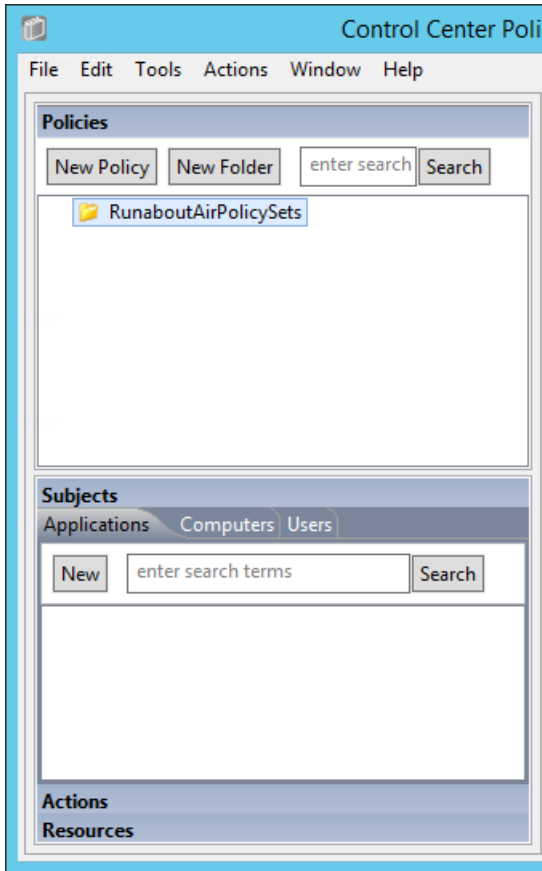


4114

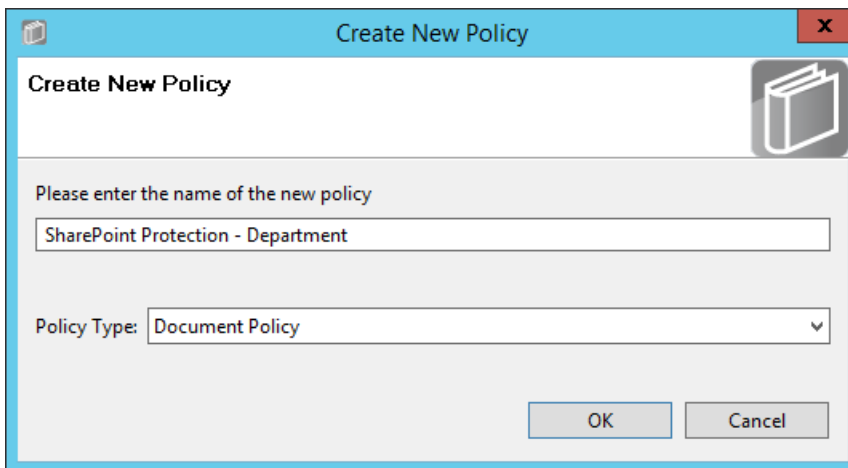
4115 *8.4.4.2 Defining Department-based Policy Set*

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-  
 4121 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:

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

Submit

Status: Draft

Last Modified: Tue Jul 07 11:34:07 EDT 2015 Administrator

4132

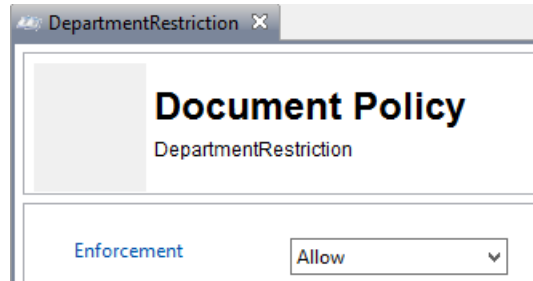
4133

5. To deploy this policy, follow the steps in [Section 8.4.5](#).

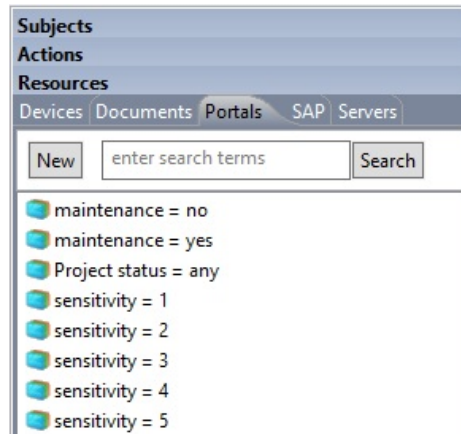


4134 8.4.4.2.2 Defining a Department-based Sub-policy that Enforces an Allow Decision when Certain  
 4135 Conditions are met

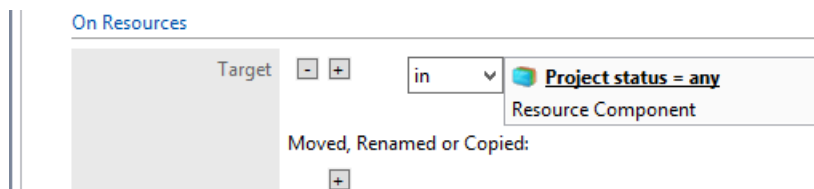
- 4136 1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new  
 4137 policy to highlight it. Then click on **New Policy** to create a sub-policy.
- 4138 2. Select a **name** for the new sub-policy then click **OK**.
- 4139 3. In the policy editing panel, 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

**Conditions**

Connection Type	<input type="button" value="+"/>
Heartbeat	<input type="button" value="+"/>
Date/Time	Start: <input type="button" value="+"/> End: <input type="button" value="+"/>
Recurrence	Time: <input type="button" value="+"/> Day: <input type="button" value="+"/>
Condition Expression	<input type="button" value="-"/> (user.department = resource.portal.department OR (user.department = "Business Intelligence" AND (resource.portal.department = "Marketing" OR resource.portal.department = "Sales")))

4154 4. In the Policy Editing panel, your policy should look like this:

The screenshot displays the Policy Editor interface. On the left, the 'Policies' pane shows a tree view with 'RunaboutAirPolicySets' > 'SharePoint Protection - Department' > 'DepartmentRestriction'. Below it, the 'Subjects' pane shows a list of subjects including 'maintenance = no', 'Project status = any', and various 'sensitivity' levels. The main editing area is titled 'Document Policy' for 'DepartmentRestriction'. It includes sections for 'Enforcement' (set to 'Allow'), 'Subject' (with 'User', 'Computer', and 'Application' options), 'Perform the Following' (with an 'Action' option), and 'On Resources' (with a 'Target' set to 'in' and 'Project status = any'). The 'Conditions' section is identical to the one shown in the previous image. At the bottom, there are 'Subpolicy' and 'Obligations' sections, and a 'Submit' button with a 'Status: Draft' indicator and a timestamp.

4155

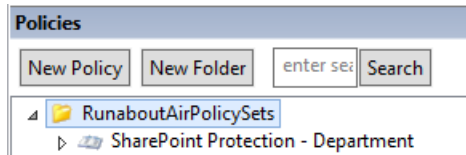
4156 5. To deploy this policy, follow the steps in [Section 8.4.5](#).

4157 **8.4.4.3 Defining a Sensitivity-based Policy Set**

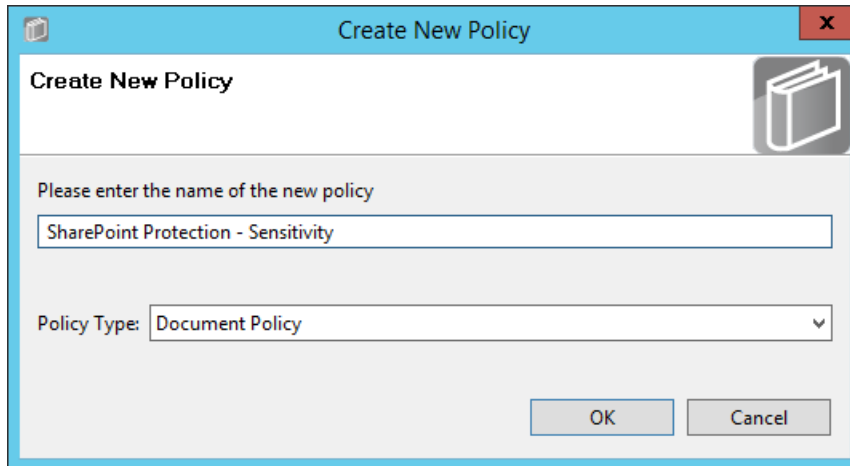
4158 In order to define a sensitivity-based policy set, follow instructions similar to defining the department-  
4159 based policy set in [Section 8.4.4.2](#):

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**.



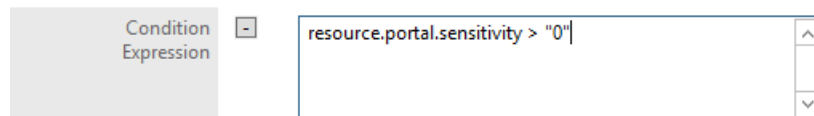
4163  
4164 2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-  
4165 down menu, select **Document Policy** (which applies to all SharePoint policies). Click **OK**.



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 gray; padding: 2px; display: inline-block;">Access denied. Contact your administrator. <span style="float: right;">^ v</span></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:

The screenshot shows the 'Document Policy' configuration page for 'SharePoint Protection - Sensitivity'. The page is divided into several sections:

- Enforcement:** A dropdown menu is set to 'Deny'.
- Subject:** Three expandable sections for 'User', 'Computer', and 'Application', each with a plus sign (+).
- Perform the Following:** An expandable section for 'Action' with a plus sign (+).
- On Resources:** An expandable section for 'Target' with a plus sign (+), containing the text 'Moved, Renamed or Copied:' and another plus sign (+).
- Conditions:** Multiple expandable sections: 'Connection Type' (+), 'Heartbeat' (+), 'Date/Time' (with 'Start:' and 'End:' sub-sections, each with a plus sign (+)), 'Recurrence' (with 'Time:' and 'Day:' sub-sections, each with a plus sign (+)), and 'Condition Expression' (-) containing the text 'resource.portal.sensitivity > "0"'. A minus sign (-) is next to the 'Condition Expression' header.
- Subpolicy:** An expandable section for 'Subpolicy'.
- Obligations:** A section with 'On Deny' containing two checked checkboxes: 'Log' and 'Display User Alert'.
- Right Sidebar:** Contains 'Description' (a text area), 'Tags' (with 'Name' and 'Value' input fields), and a 'Name' field with a list of empty rows and navigation arrows.

At the bottom of the page, there is a 'Submit' button, the status 'Draft', and the text 'Last Modified: Tue Jul 07 11:33:41 EDT 2015 Administrator'.

4177

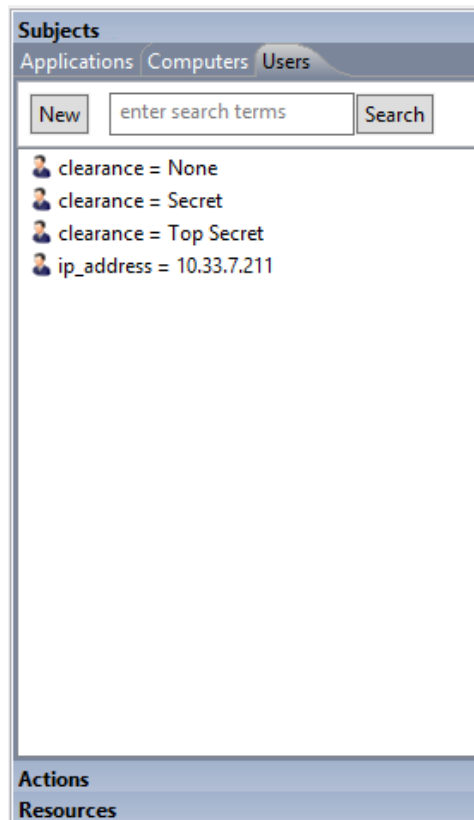
4178

6. 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  
 4183 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,  
 4189 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**  
 4192 field.
- 4193 iii. Left-click and hold the **clearance = Secret** component to drag it onto the **User**  
 4194 field.
- 4195 iv. Left-click and hold the **clearance = Top Secret** component to drag it onto the  
 4196 **User** field.

- 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**

**Subject**

User    
  
  
User Component

Computer

Application

**Perform the Following**

Action

**On Resources**

Target    
Resource Component

Moved, Renamed or Copied:

**Conditions**

Connection Type

Heartbeat

Date/Time Start:   
End:

Recurrence Time:   
Day:

Condition Expression

**Subpolicy**

Subpolicy

Subpolicy

**Obligations**

Policy1a-Sensitivity Level 1  Status: Draft  
Last Modified: Tue Jul 07 11:20:27 EDT 2015 Administrator

4203  
4204

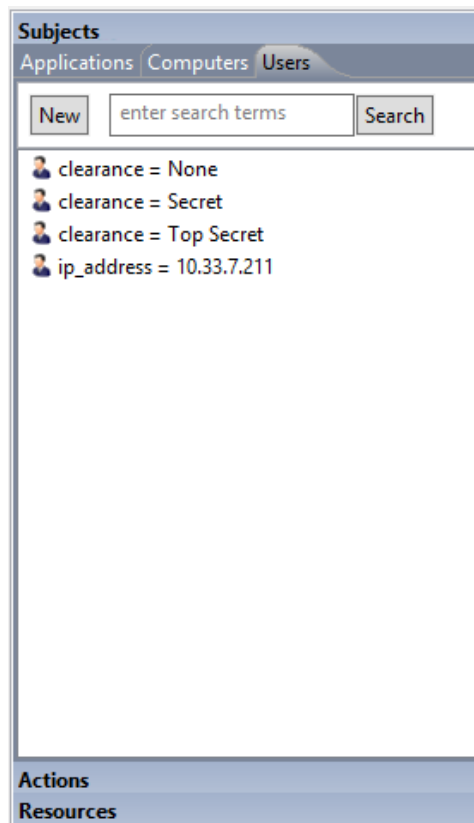
- e. To deploy this policy, follow the steps in [Section 8.4.5](#).



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**  
 4219 field.
- 4220 iii. Left-click and hold the **clearance = Top Secret** component to drag it onto the  
 4221 **User** field.
- 4222 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: - <input checked="" type="radio"/> Sun <input type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="radio"/> Day 1 of every month <input type="radio"/> The First Sunday of every month
Condition Expression	+

4229

- 4230 4. In the policy editing panel, your policy should look like this:

**Document Policy**  
Policy1b-Sensitivity Level 2

**Enforcement**

**Subject**

User  **clearance = Secret**  
**clearance = Top Secret**  
User Component

Computer

Application

**Perform the Following**

Action

**On Resources**

Target  **sensitivity = 2**  
Resource Component

Moved, Renamed or Copied:

**Conditions**

Connection Type

Heartbeat

Date/Time Start:   
End:

Recurrence Time:  From  To   
Day:

Sun  Mon  Tue  Wed  Thu  Fri  Sat  
 Day  of every month  
 The   of every month

Condition Expression

Policy1b-Sensitivity Level 2  Status: Draft  
Last Modified: Tue Jul 07 11:20:27 EDT 2015 Administrator

4231

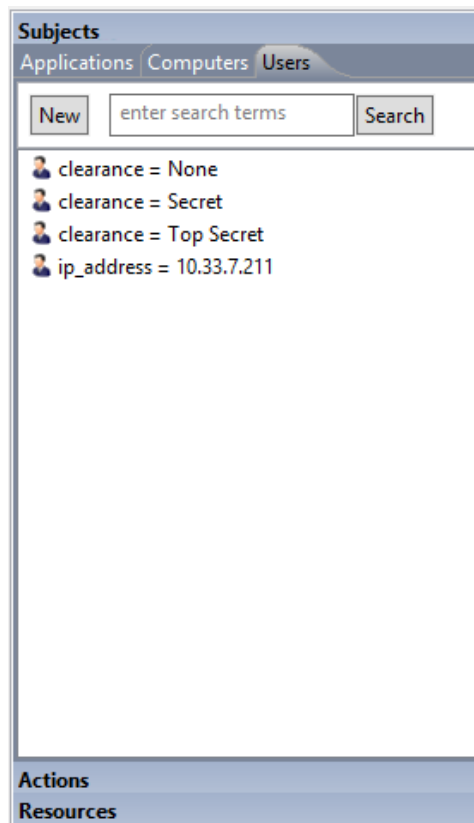
4232

- 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 <input type="text"/> To: 6:00 PM <input type="text"/>																							
	Day: - <table border="1"><tr><td><input checked="" type="radio"/></td><td>Sun</td><td><input type="checkbox"/></td><td>Mon</td><td><input checked="" type="checkbox"/></td><td>Tue</td><td><input checked="" type="checkbox"/></td><td>Wed</td><td><input checked="" type="checkbox"/></td><td>Thu</td><td><input checked="" type="checkbox"/></td><td>Fri</td><td><input checked="" type="checkbox"/></td><td>Sat</td><td><input type="checkbox"/></td></tr><tr><td><input type="radio"/></td><td>Day</td><td>1</td><td>of every month</td></tr><tr><td><input type="radio"/></td><td>The</td><td>First</td><td>Sunday</td><td>of every month</td></tr></table>	<input checked="" type="radio"/>	Sun	<input type="checkbox"/>	Mon	<input checked="" type="checkbox"/>	Tue	<input checked="" type="checkbox"/>	Wed	<input checked="" type="checkbox"/>	Thu	<input checked="" type="checkbox"/>	Fri	<input checked="" type="checkbox"/>	Sat	<input type="checkbox"/>	<input type="radio"/>	Day	1	of every month	<input type="radio"/>	The	First	Sunday
<input checked="" type="radio"/>	Sun	<input type="checkbox"/>	Mon	<input checked="" type="checkbox"/>	Tue	<input checked="" type="checkbox"/>	Wed	<input checked="" type="checkbox"/>	Thu	<input checked="" type="checkbox"/>	Fri	<input checked="" type="checkbox"/>	Sat	<input type="checkbox"/>										
<input type="radio"/>	Day	1	of every month																					
<input type="radio"/>	The	First	Sunday	of every month																				
Condition Expression	+																							

- 4255
- 4256                    4. In the policy editing panel, your policy should look like this:

**Document Policy**  
Policy1c-Sensitivity Level 3

**Enforcement**

**Subject**

User  **clearance = Top Secret**  
User Component

Computer

Application

**Perform the Following**

Action

**On Resources**

Target  **sensitivity = 3**  
Resource Component

Moved, Renamed or Copied:

**Conditions**

Connection Type

Heartbeat

Date/Time Start:  End:

Recurrence Time: From  To

Day:  Sun  Mon  Tue  Wed  Thu  Fri  Sat

Day  of every month

The   of every month

Condition Expression

**Tags**

Name:

Value:

**Description**

Policy1c-Sensitivity Level 3  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](#).

4259 **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  
4264
1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new 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**

**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.maintenance = "\*\*"

**Subpolicy**

- Subpolicy

**Obligations**

- On Deny  Log  Display User Alert

**Description**

**Tags**

Name:   
Value:

Name

Name

SharePoint ...Maintenance  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 <input type="text"/> To 6:00 AM <input type="text"/>
	Day: -
	<input checked="" type="radio"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat <input type="radio"/> Day 1 of every month <input type="radio"/> The First Sunday of every month
Condition Expression	+

- 4294
- 4295 4. In the policy editing panel, your policy should look like this:

#44: 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:** -

SunMonTueWedThuFriSat

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:

Allow Non-Maintenance Any Time

### Document Policy

Allow Non-Maintenance Any Time

Enforcement:

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

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

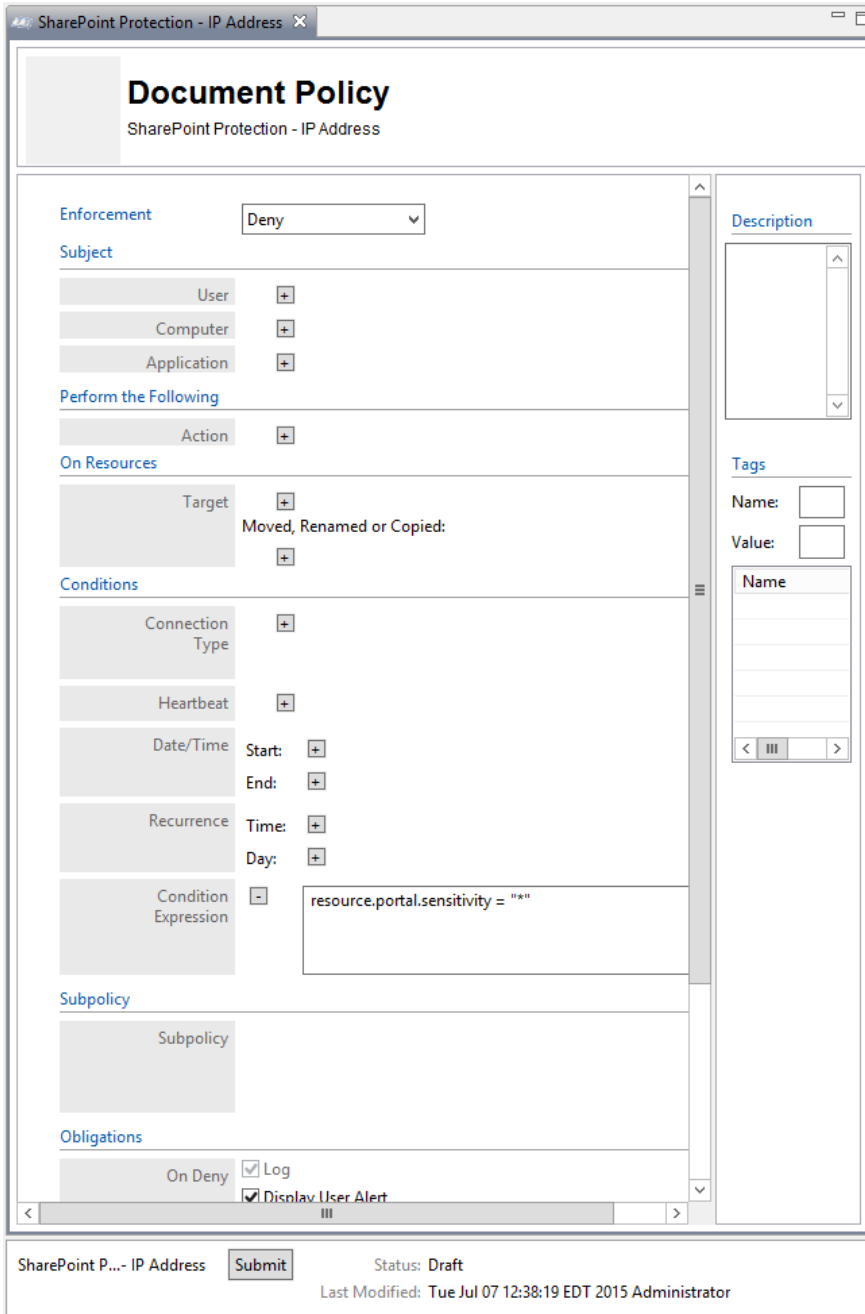
- To deploy this policy, follow the steps in [Section 8.4.5](#).

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:



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:

AllowIPAddressLevel1

## Document Policy

AllowIPAddressLevel1

**Enforcement**

**Subject**

User

Computer

Application

**Perform the Following**

Action

**On Resources**

Target      
Resource Component

Moved, Renamed or Copied:

**Conditions**

Connection Type

Heartbeat

Date/Time Start:   
End:

Recurrence Time:   
Day:

Condition Expression

**Subpolicy**

Subpolicy

**Obligations**

On Allow, Monitor  Log  
 Display User Alert  
 Send Email

AllowIPAddressLevel1  Status: Draft  
Last Modified: Tue Jul 07 11:20:10 EDT 2015 Administrator

4348

4349

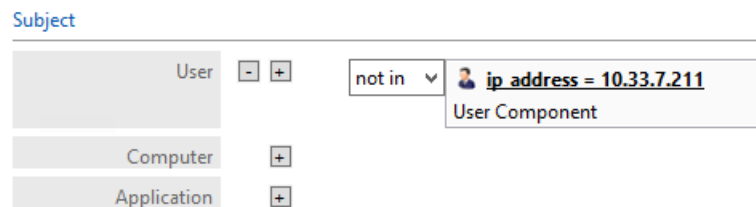
5. To deploy this policy, follow the steps in [Section 8.4.5](#).



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 c. In the On Resources area, click on the **plus sign** box next to **Target**.
  - 4367 i. In the Components panel in the bottom-left corner of the Policy Studio window,  
 4368 click on **Resources**, then the **Portals** tab to see the components you created  
 4369 earlier.
  - 4370 ii. Left-click and hold the **sensitivity = 1** component to drag it onto the **Target** field.
  - 4371 iii. Left-click and hold the **sensitivity = 2** component to drag it onto the **Target** field.
  - 4372 iv. Left-click and hold the **sensitivity = 3** component to drag it onto the **Target** field.
- 4373 4. In the policy editing panel, your policy should look like this:  
 4374

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

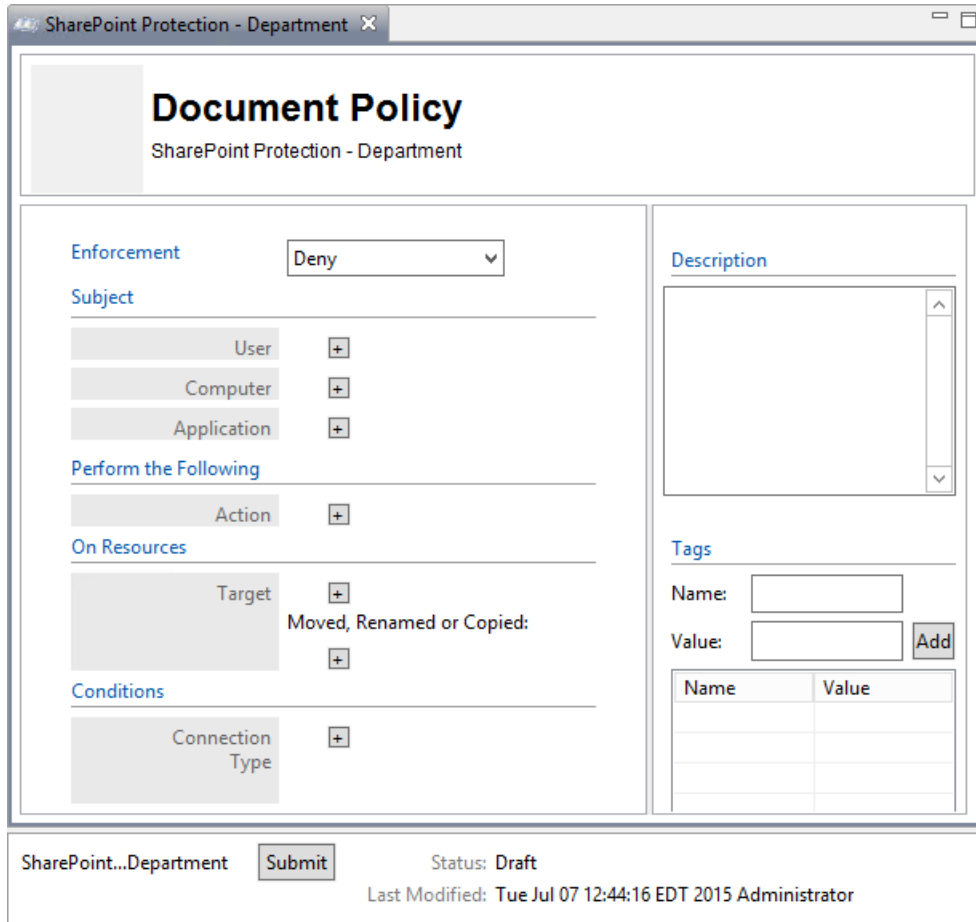
4376

5. To deploy this policy, follow the steps in [Section 8.4.5](#).

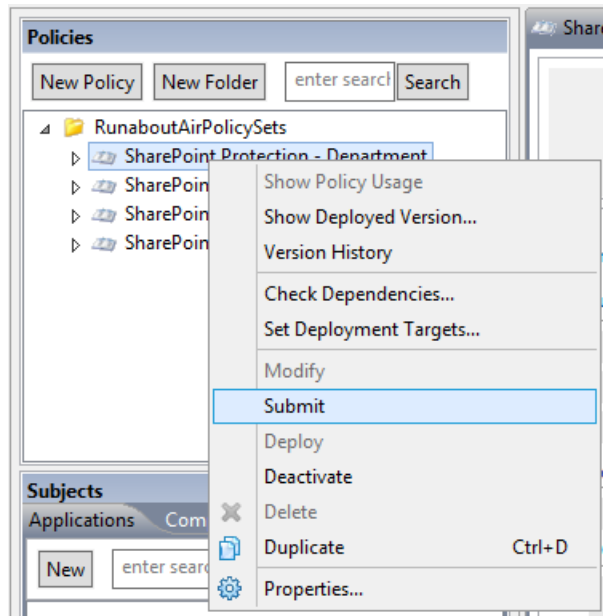
4377 **8.4.5 Deploying Policy**

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**.

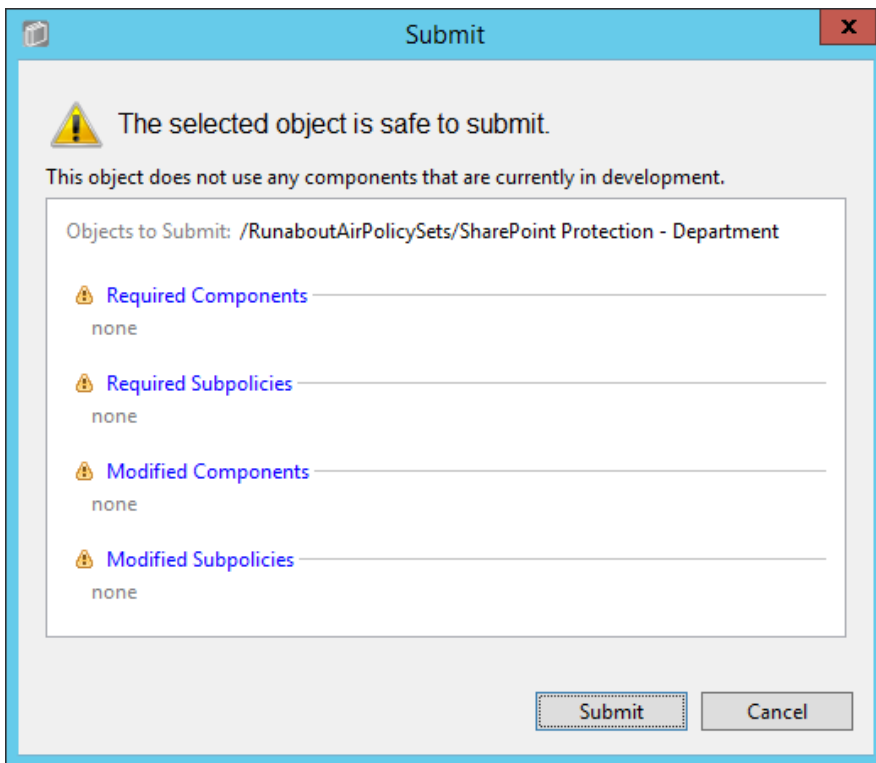


- 4382
- 4383 a. Or, in the Policies panel in the top-left corner of the main Policy Studio window, right-  
 4384 click the policy you want to deploy. Select **Submit** from the floating menu.



4385

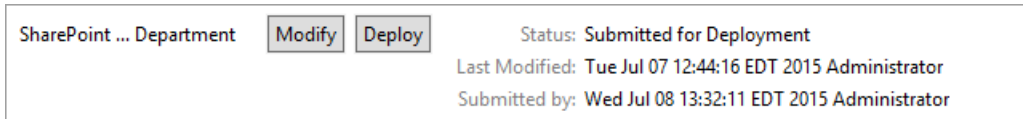
4386 2. In the Submit window, click **Submit**.



4387

4388 3. From the component editing panel, note the differences. The new status reads **Submitted for**  
 4389 **Deployment**. Click **Deploy**.

4390 a. Or, in the Policies panel in the top-left corner of the main Policy Studio window, right-  
 4391 click the policy you want to deploy. Select **Deploy** from the floating menu.



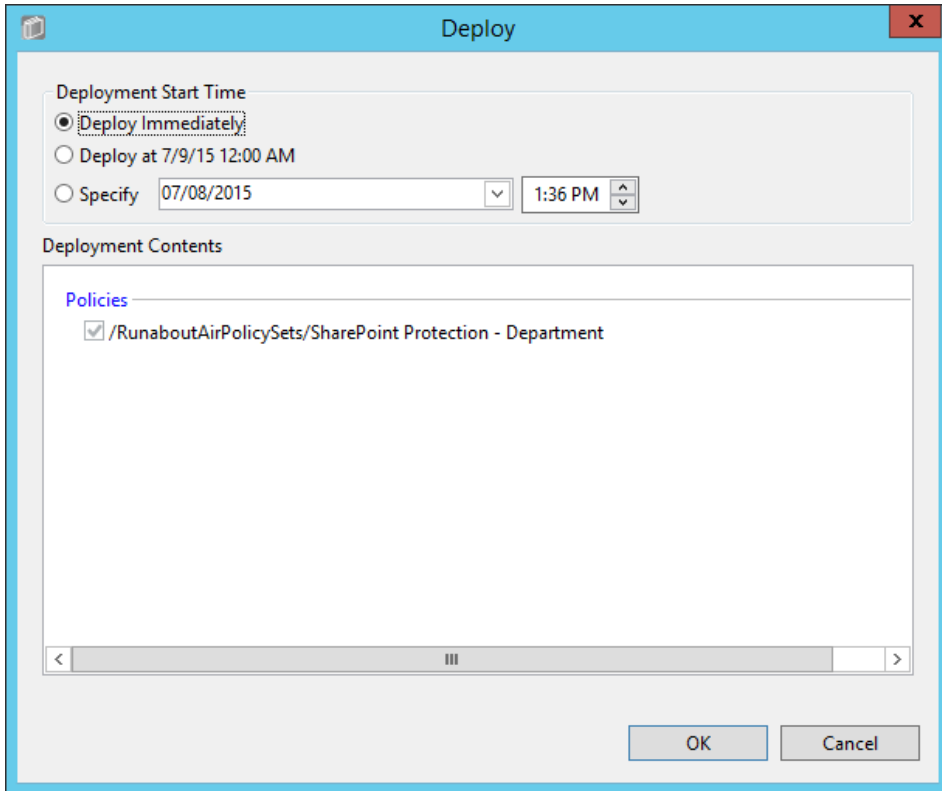
4392

4393

4394

4395

4. In the Deploy window, click **OK**. Note: You may specify to deploy immediately, which we choose in our example. You may also deploy at the following day at midnight, or at a different specific date and time.



4396

4397

4398

4399

4400

5. At the bottom of the policy editing panel, verify that the **Status** is now **Pending Deployment**. This will remain for the duration of the heartbeat (described in [Section 7](#)).
6. After the duration of the heartbeat has passed, **Status** should read as **Deployed**. This indicates 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

4405

4406

4407

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on the policy you want to modify. In the policy editing panel, click **Modify**.
  - a. Or, right-click the policy you want to modify and select **Modify** from the floating menu.
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.

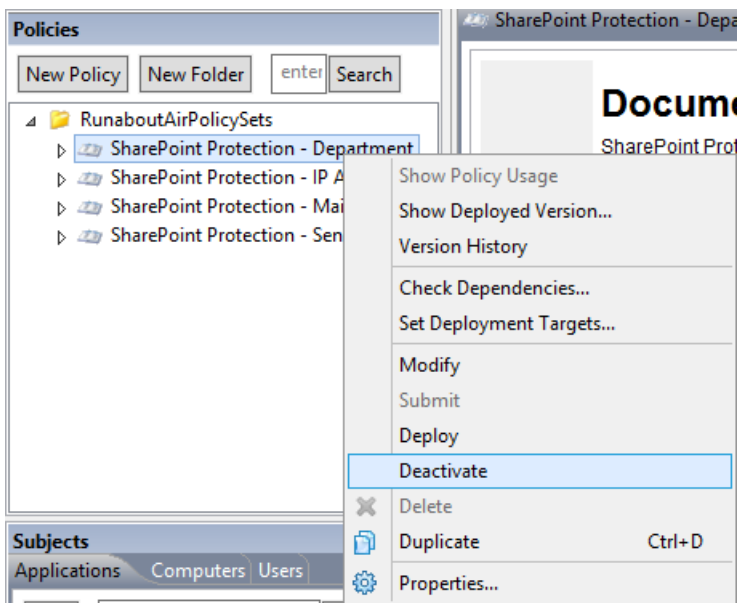
4414 2. In the component editing panel, make the desired changes and click **Submit**.

4415 3. Follow the deploy instructions from [Section 8.4.5](#) to deploy the modified component.

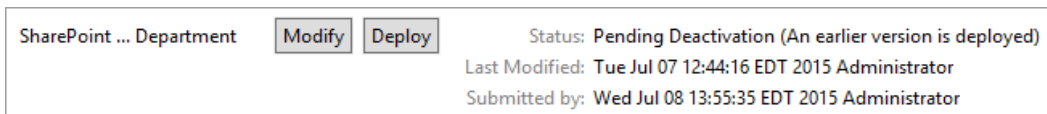
4416 **8.4.7 Deactivating Policies and Components**

4417 *8.4.7.1 Deactivating Policies*

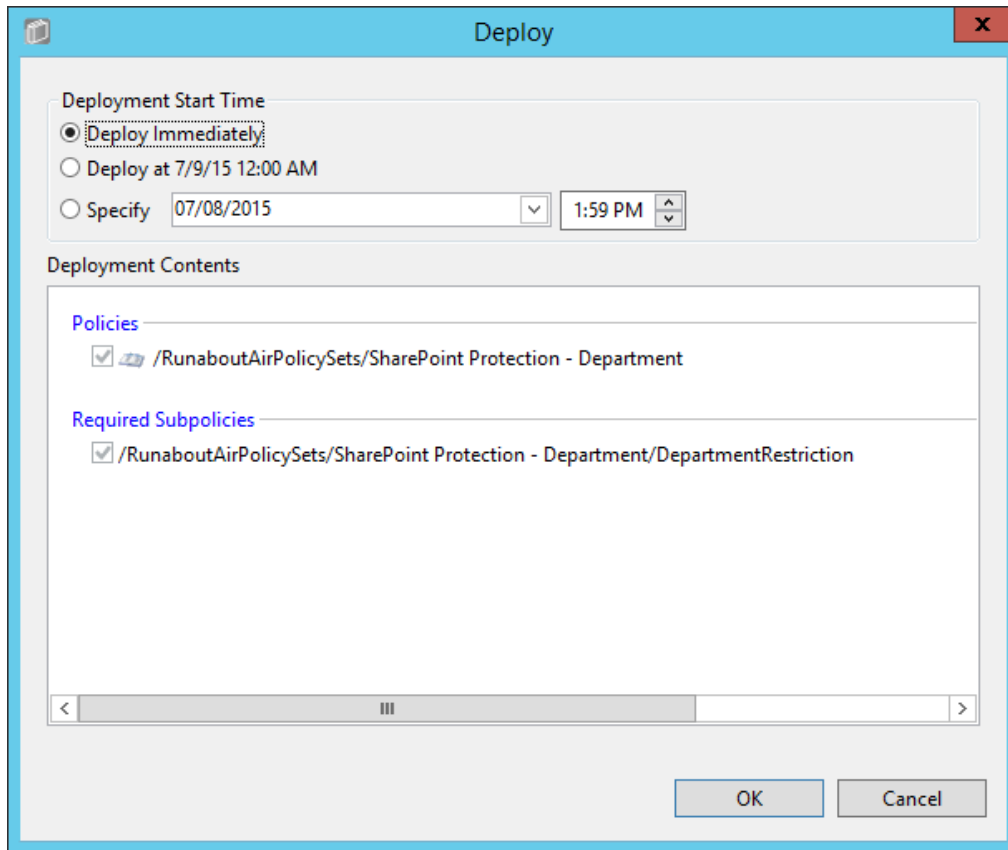
4418 1. In the Policies panel in the top-left corner of the main Policy Studio window, right-click the  
4419 policy you want to deactivate. Select **Deactivate** from the floating menu.



4420  
4421 2. At the bottom of the policy editing panel, note the change in **Status to Pending Deactivation**.  
4422 Click **Deploy**.

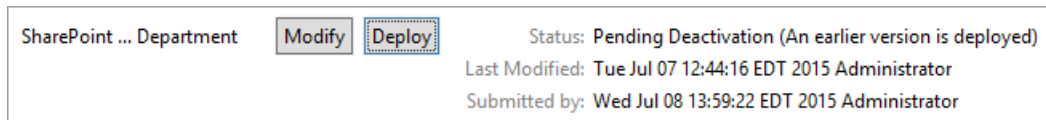


4423  
4424 3. In the Deploy window, click **OK**. Note: You may specify to deploy immediately, which we choose  
4425 in our example. You may also deploy the following day at midnight, or at a different specific date  
4426 and time.



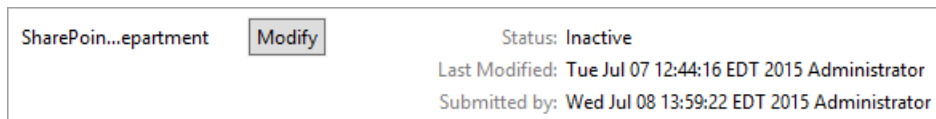
4427

- 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**

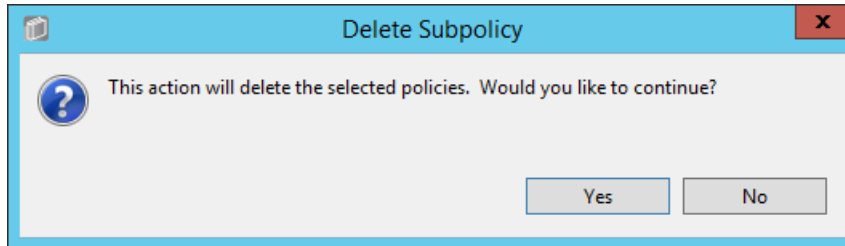
- 4435 1. In the Components panel in the bottom-left corner of the main Policy Studio window, right-click  
 4436 on the component you want to deactivate. Select **Deactivate** from the floating menu.  
 4437 2. Follow steps 2-5 in [Section 8.4.7.1](#) for deactivating policies.

## 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

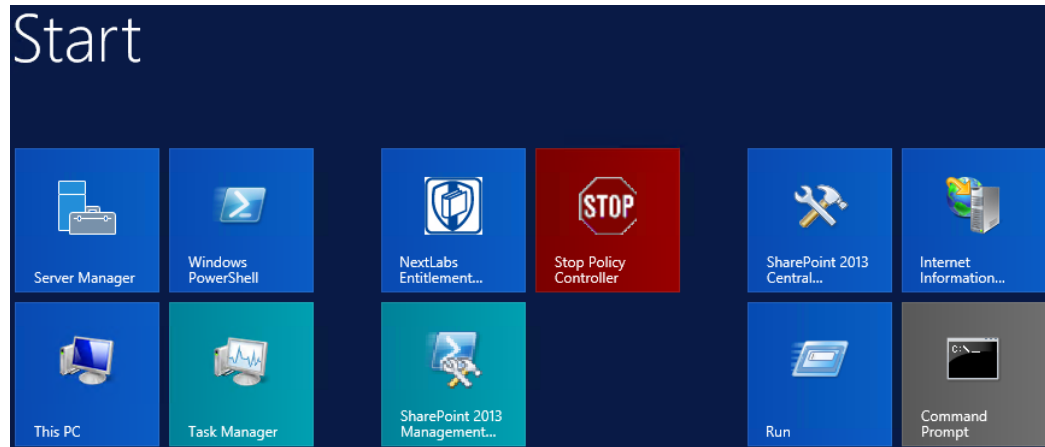
4450 [Section 6](#) illustrated how to configure the attribute flow between several of the servers and components  
4451 in the ABAC architecture. Note that the NextLabs Entitlement Manager was installed on the SharePoint  
4452 Server, which is where all of the activity in Section 8.5 occurs.

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.

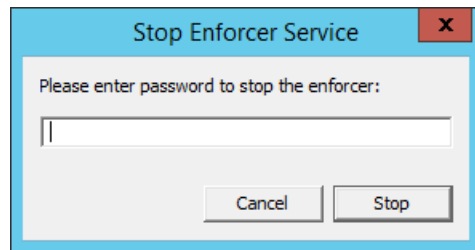




4465

4466

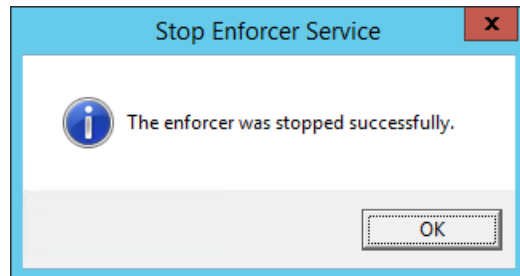
- c. Enter your NextLabs Administrator credentials. Then click **Stop**.



4467

4468

- d. In the Stop Enforcer Service success window, click **OK**.

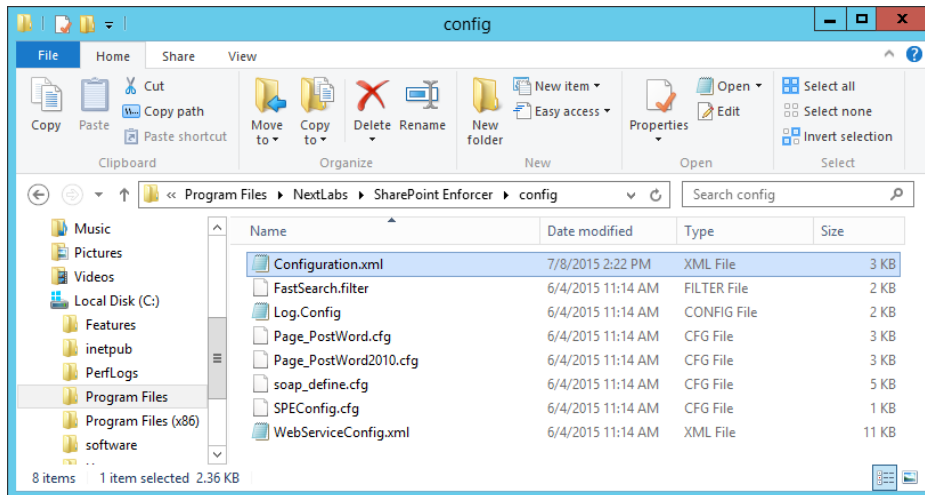


4469

## 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

4480 

### 8.5.2.2 *Configuring Resource Attributes from SharePoint Metadata*

- 4481 1. Within the **configuration.xml** file, look for the **<SPEConfiguration>** tag.
- 4482 2. Under that tag, but above a **<User Attribute>** tag, insert tags for each site-level or sub-site level
- 4483 resource attribute of interest.

- 4484 a. For example, in our build we created policies based on the **department** resource
- 4485 attribute, so in our configuration.xml file we included the following:

4486 `<PropertyBag disabled="false" level="SiteCollection">`

4487 `<Property disabled="false" name="department" attributename="department"`

4488 `/>`

4489 `</PropertyBag>`

4490 `<PropertyBag disabled="false" level="SubSite">`

4491 `<Property disabled="false" name="department" attributename="department"`

4492 `/>`

4493 `</PropertyBag>`

- 4494 b. From the example above, the top of the **configuration.xml** file looks like this:

```

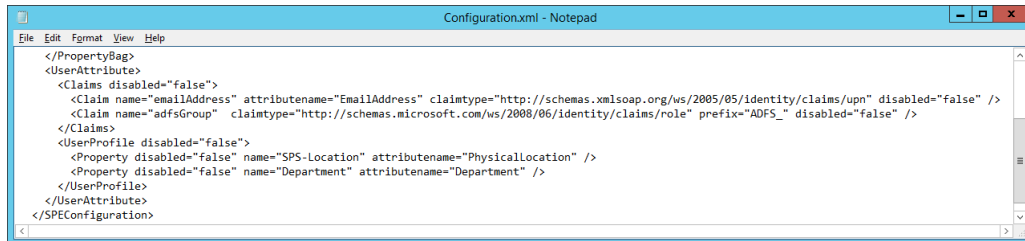
<?xml version="1.0" encoding="utf-8"?>
<Configuration name="test" xmlns="http://www.nextlabs.com/configurationSchema">
  <SPEConfiguration>
    <PropertyBag disabled="false" level="SiteCollection">
      <Property disabled="false" name="department" attributename="department" />
    </PropertyBag>
    <PropertyBag disabled="false" level="SubSite">
      <Property disabled="false" name="department" attributename="department" />
    </PropertyBag>
  </SPEConfiguration>
</Configuration>

```

4495

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**  
 4498 **Attribute>** **</User Attribute>** portion of the document. Initially, its default contents in that area  
 4499 may look like this, containing some default user attributes such as **“emailAddress”** or  
 4500 **“adfsGroup”**:



- 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:

```
4507 <Claim name="department" attributename="department"
4508 claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/departme
4509 nt" disabled="false" />
```

```
4510 <Claim name="ip_address" attributename = "ip_address"
4511 claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ip_adre
4512 ss" disabled="false" />
```

```
4513 <Claim name="clearance" attributename = "clearance"
4514 claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/clearanc
4515 e" disabled="false" />
```

- 4516 b. From the example above, the rest of our **configuration.xml** file looks like this:

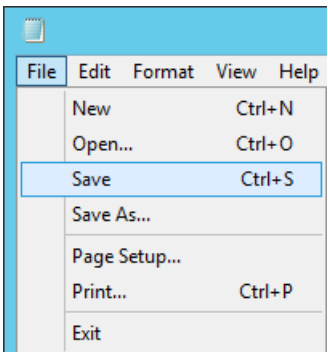
```

  </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>
```

4517

4518 **8.5.2.4** *Saving Changes to the Configuration File*

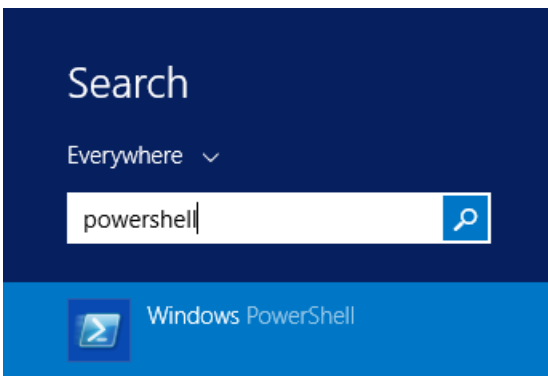
- 4519
1. From the File menu, click **Save**, or Ctrl+S on your keyboard.



4520

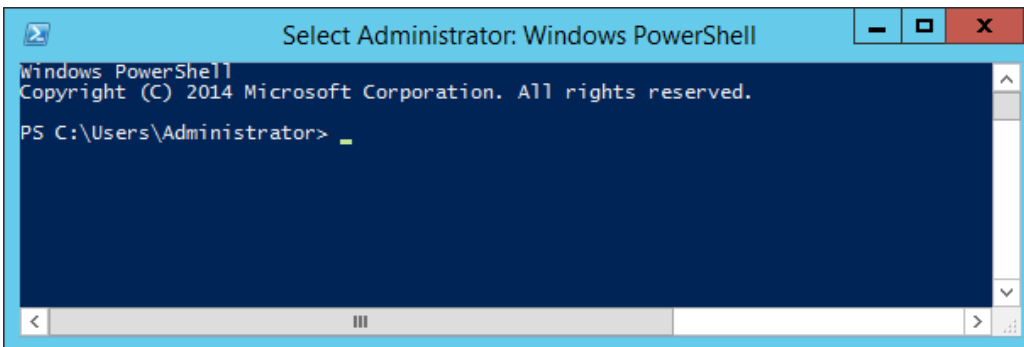
4521 **8.5.3** *Restarting IIS via Windows PowerShell*

- 4522
  1. Click the Windows icon.
- 4523
  2. In the Search text box, begin typing **PowerShell**.



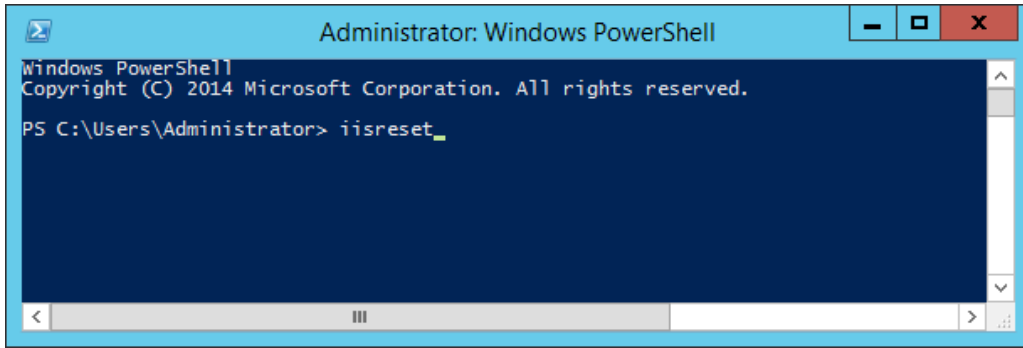
4524

- 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.

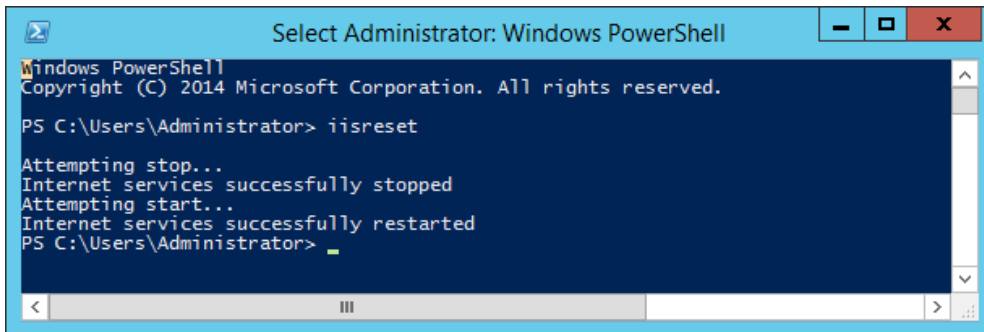
PS C:\Users\Administrator> iisreset_

```

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

#### 4531 8.5.4 Restarting the NextLabs Policy Controller Service

4532

1. Click on the Windows icon and begin typing the word **Services**.

4533

2. Double-click the **Services** icon to open the application.

4534

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**.

4535

4536

4. Right-click **Control Center Enforcer Service** and click **Start**.

4537

- a. It may be necessary to click the **Refresh** icon in order to see the **Control Center Enforcer Service** status change to **Running**.

4538

## 4539 8.6 Functional Test

### 4540 8.6.1 Updated Bin File After Policy Creation/Modification

4541

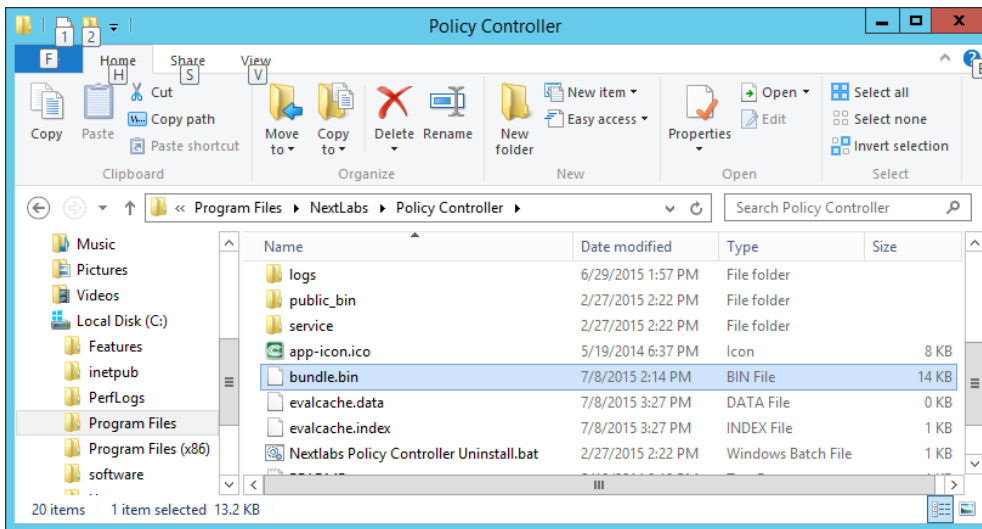
4542 After a policy or component is deployed for the first time, or modified and re-deployed within Policy  
 4543 Studio on the SQL Server, an encrypted bundle.bin file on the SharePoint Server will be updated after  
 4544 one heartbeat. As explained in [Section 7](#), on the SharePoint Server it is the responsibility of the  
 4545 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.

4546

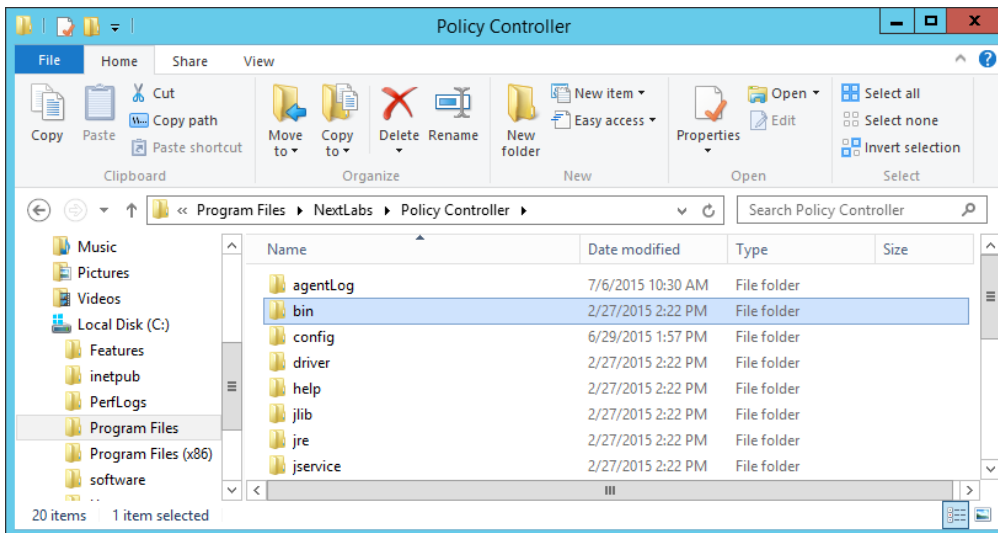
To ensure the policy logic is being correctly sent from the NextLabs Policy Studio (PAP) on the SQL Server  
 4547 to the bundle.bin file on the SharePoint Server for use by the NextLabs Policy Controller (PDP), you can  
 4548 find the bundle.bin file and decrypt its contents to see your policy logic decrypted there.

4549 *8.6.1.1 On the SharePoint Server Note Timestamp of the Bundle.bin File and Decrypt Its*  
 4550 *Contents*

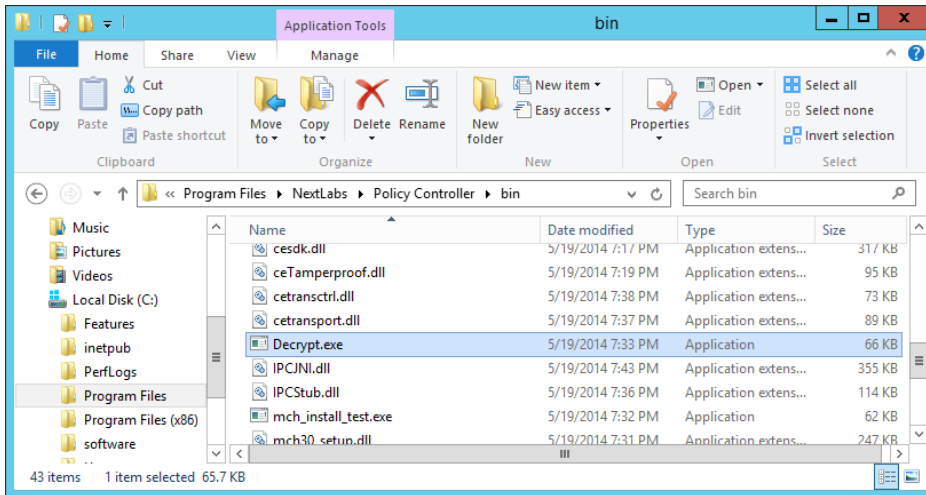
- 4551 1. Double-click the **C:/** drive.
- 4552 2. Double-click **Program Files**.
- 4553 3. Double-click **NextLabs**.
- 4554 4. Double-click **Policy Controller**.
- 4555 5. Scroll down to find **bundle.bin** and note the timestamp in the **Date Modified** column. This
- 4556 would be the last time policies or components were deployed.



- 4557
- 4558 6. Scroll back up and double-click on the **bin** folder.



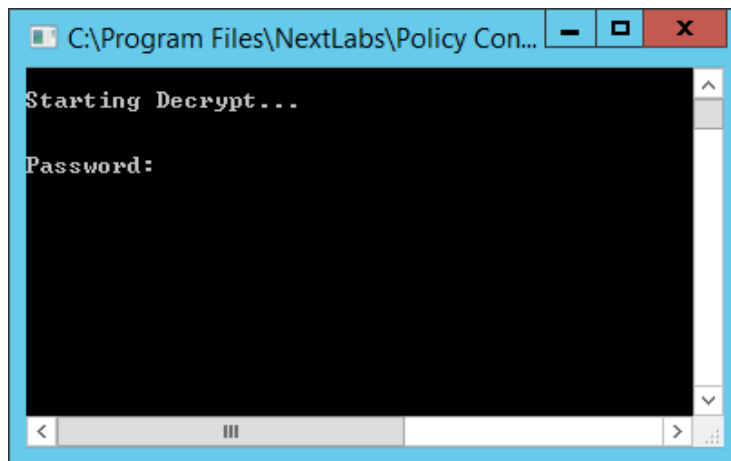
- 4559
- 4560 7. Scroll down to find **Decrypt.exe**.



4561

4562

- a. In the Decrypt window, enter the administrator’s **Password** and press **Enter**.

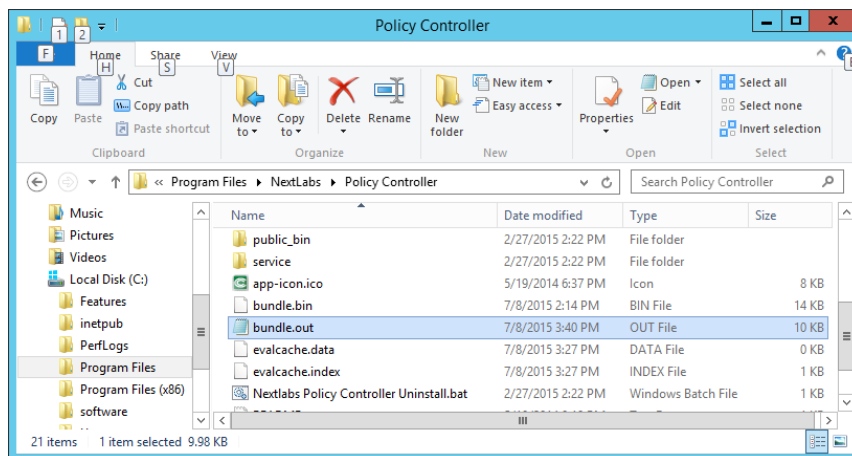


4563

4564

4565

- b. After the Decrypt window disappears, click on Policy Controller to return to that folder. Scroll down and double-click the **bundle.out** file.



4566

4567

4568

- c. In the text editor window, scroll down to find policies that you have created previously. Example: **RunaboutAirPolicySets/SharePoint Protection – Department** top-level policy

```

bundle.out - Notepad
File Edit Format View Help
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." )
    
```

4569

## 8.6.2 Reviewing NextLabs AgentLog to Illustrate History of Access Control Evaluations during SharePoint Access

4570

4571

4572

1. Double-click the **C:/** drive.

4573

2. Double-click **Program Files**.

4574

3. Double-click **NextLabs**.

4575

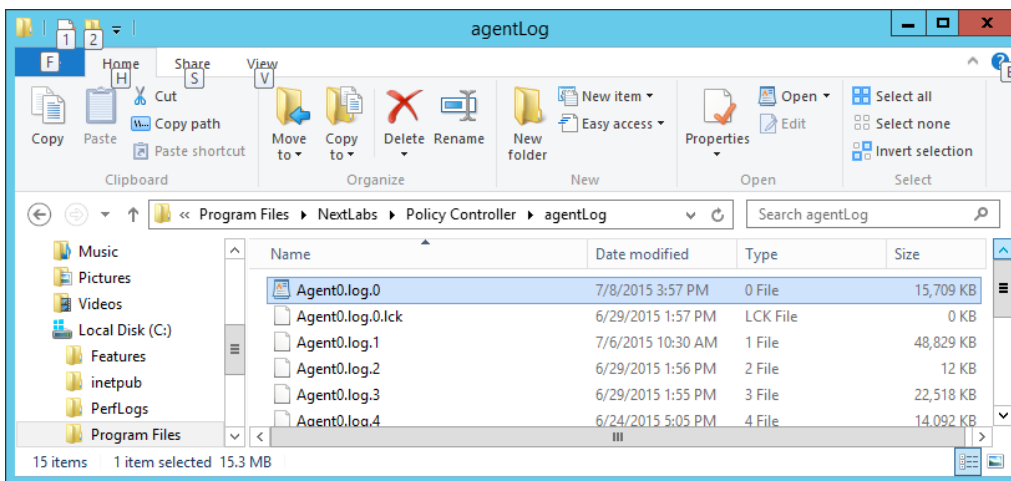
4. Double-click **Policy Controller**.

4576

5. Double-click **AgentLog**.

4577

6. Right-click the **Agent0.log.0** locked file and select **Copy**.

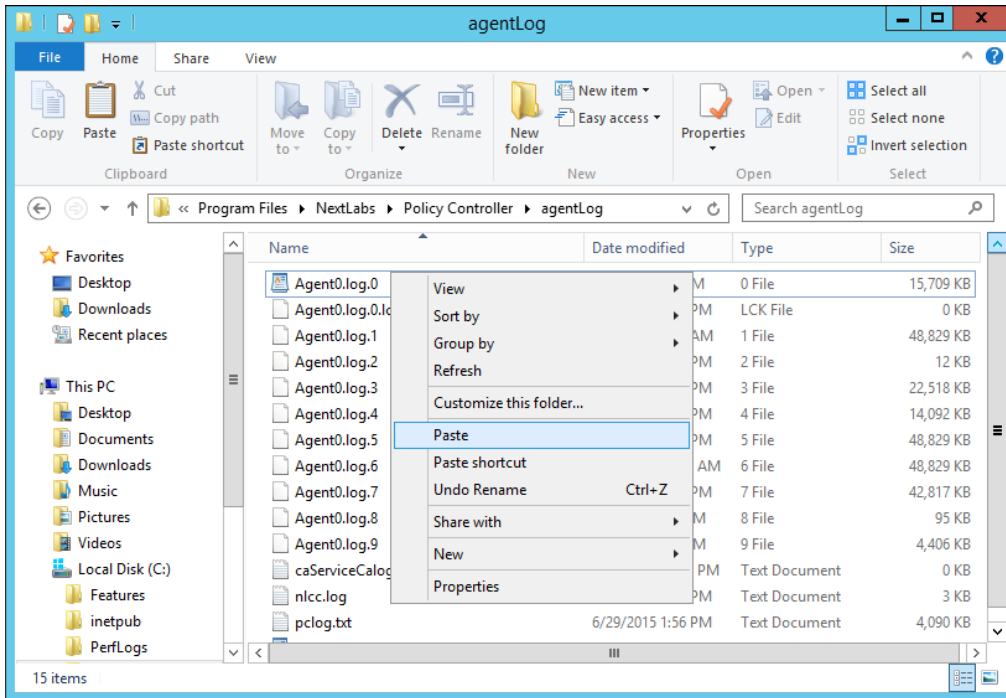


4578

4579

7. Within the agentLog folder, right-click in an empty space and select **Paste**.

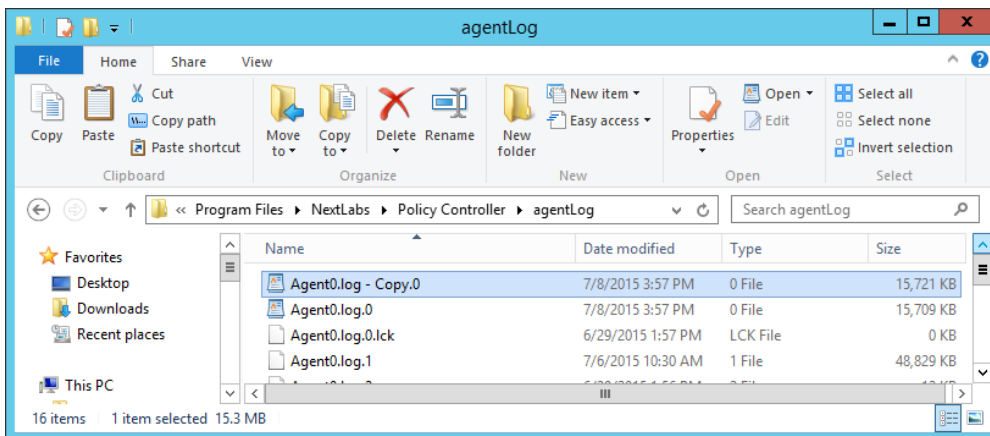




4580

4581

8. Double-click the **Agent0.log-Copy.0** file to view its contents.



4582

4583

4584

4585

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 =**.

4586

- a. Examples of information found in this **Agent0.log-Copy.0** file:

4587

- i. All of the policies evaluated during one instance of access:

4588

4589

4590

4591

4592

4593

4594

4595

```

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
```

## 4659 **9 Leveraging NextLabs Control Center Reporter for Reporting** 4660 **and Auditing Purposes**

### 4661 **9.1 Introduction**

4662 In previous sections of this How-To Guide ([Section 7](#)), we installed several NextLabs products that can be  
4663 used to define and deploy Attribute Based Access Control policies and enforce decisions regarding user  
4664 access to Microsoft SharePoint resources based on user, object, environmental attributes, and the  
4665 corresponding policies in place. We also illustrated how to use and configure the NextLabs Policy Studio,  
4666 the product responsible for Policy Lifecycle Management, and discussed policy strategy and the  
4667 translation of business logic into policy ([Section 8](#)).

4668 In this section of the How-To Guide, we will illustrate how to use the NextLabs Control Center Reporter,  
4669 a component of the previously installed NextLabs Control Center ([Section 7](#)), in order to generate  
4670 reports and provide a graphical user interface for prior policy evaluation and access control decisions in  
4671 your environment.

4672 Reporter is automatically installed during the NextLabs Control Center installation, which was detailed in  
4673 [Section 7](#). In this How-To section, we will introduce Reporter, its purpose, interface, and capabilities,  
4674 then illustrate some example uses based on our build.

#### 4675 **9.1.1 Components Used in this How-To Guide**

4676 NextLabs Control Center Reporter v7.5.0 (64) – web application and graphical user interface for  
4677 evaluating prior policy evaluation access control decisions and generating reports for monitoring and  
4678 auditing.

#### 4679 **9.1.2 Pre-requisites to Complete Prior to this How-To Guide**

- 4680 1. If you intend to do a setup without identity federation and federated logins, you must:
  - 4681 a. Install and configure Active Directory (see [Section 2](#))
  - 4682 b. Install and configure Microsoft SharePoint (see [Section 4](#))
  - 4683 c. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see  
4684 [Section 7](#))
  - 4685 d. Define and deploy policies based on your business rules (see [Section 8](#))
- 4686 2. If you intend to incorporate a trust relationship between an IdP and RP and use federated logins  
4687 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.

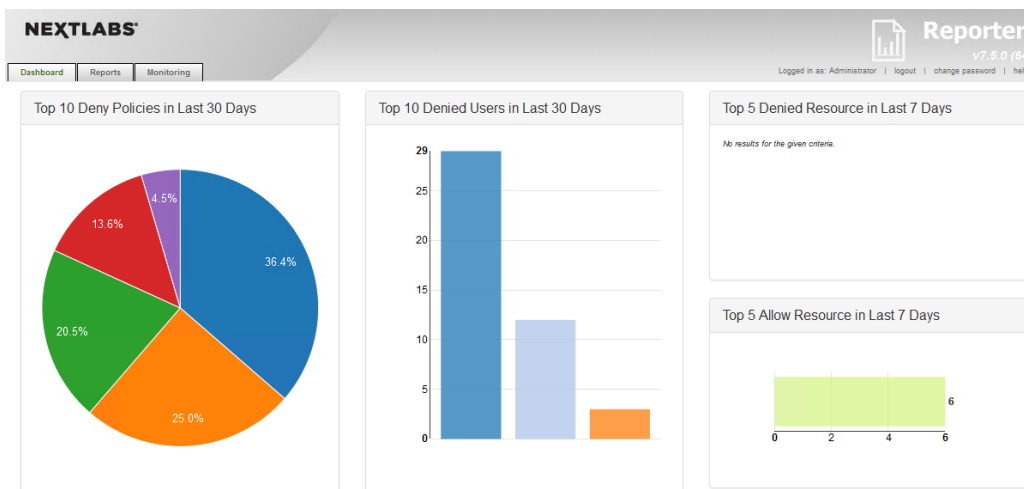
### 4719 9.2.1 Opening Reporter

- 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
<b>Top Five Deny Policies (Month)</b>	Pie chart representing the five Deny policies that were most frequently enforced over the previous thirty days.	<ul style="list-style-type: none"> <li>• Misunderstanding of access level: users being blocked from a resource they believe they should use</li> <li>• Incorrectly defined entitlements: users should have access, but policies are not updated or correctly designed</li> </ul>
<b>Top Ten Denied Users (Month)</b>	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"> <li>• Users who habitually snoop into resources they are not authorized to use</li> <li>• Incorrectly defined entitlements: users or group should have access, but policies are not updated or are incorrectly designed</li> </ul>
<b>Top Five Deny Resources (Week)</b>	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"> <li>• Resources of broad interest to users who should not be using them</li> <li>• Incorrectly designed resource or user component, blocking users who should have access</li> </ul>
<b>Top Five Allow Resources (Week)</b>	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"> <li>• Improperly designed resource component or policies, which allow inappropriate users access to sensitive resources</li> </ul>
<b>Deny Policy Enforcement Trends (Month)</b>	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"> <li>• Progress (or lack thereof) in educating users about access policies and individual/group entitlements, at a broad level</li> <li>• Improperly designed policies that are blocking too many users who expect and are entitled to access or use</li> </ul>

Graph	Description	May Indicate
<b>Recent Allows</b>	<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"> <li>• Date of enforcement</li> <li>• Name of enforced policy</li> <li>• User who triggered the policy</li> <li>• Action that triggered the policy</li> <li>• Resource the user was trying to access</li> </ul>	<ul style="list-style-type: none"> <li>• 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</li> </ul>
<b>Recent Denys</b>	<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"> <li>• Date of enforcement</li> <li>• Name of enforced policy</li> <li>• User who triggered the policy</li> <li>• Action that triggered the policy</li> <li>• Resource the user was trying to access</li> </ul>	<ul style="list-style-type: none"> <li>• Instances where many users are attempting to get at data they are not authorized to use</li> <li>• 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</li> </ul>
<b>Alerts this Week: Group by Tags</b>	<p>Treemap representing volume of alerts in the current week. Alerts are grouped by monitor tags.</p>	<ul style="list-style-type: none"> <li>• Policies being watched by monitors that are tagged are being enforced at a rate that demands attention. Further review or action may be required.</li> </ul>
<b>Today's Alerts: Details</b>	<p>List of details about the alerts raised in the current day. Details include:</p> <ul style="list-style-type: none"> <li>• Alert level</li> <li>• Monitor name</li> <li>• Alert message</li> <li>• Date and time the alert was raised</li> </ul>	<ul style="list-style-type: none"> <li>• Policies being monitored are being enforced at a rate that demands attention. Further review or action may be required.</li> </ul>

4735

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

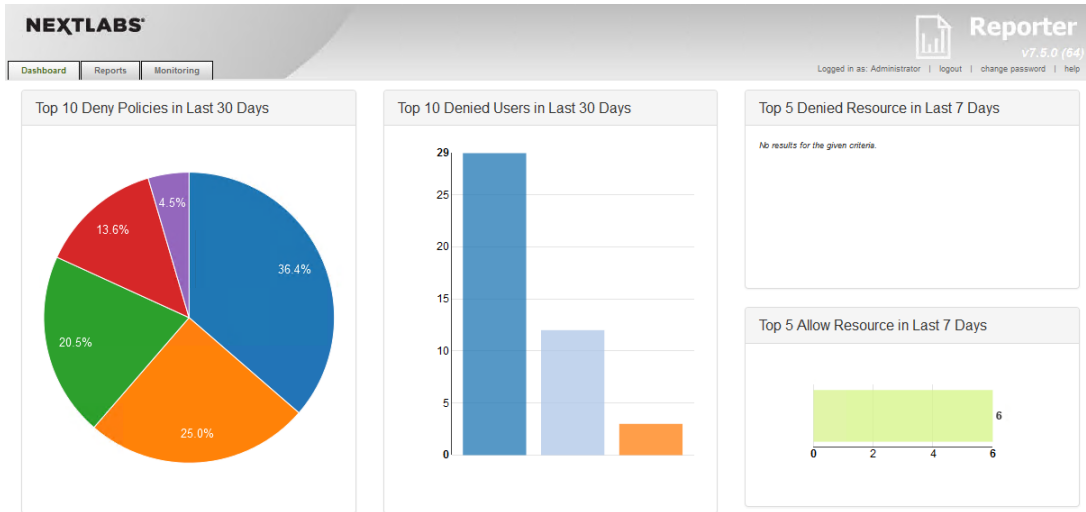
- 4744 1. On the server where NextLabs Control Center was installed, open a web browser, i.e., SQL  
4745 Server in this build
- 4746 2. Enter the URL and press Enter: *https://<hostname>/reporter*, i.e., *https://localhost/reporter*
- 4747 3. At the Reporter login screen, enter valid credentials such 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

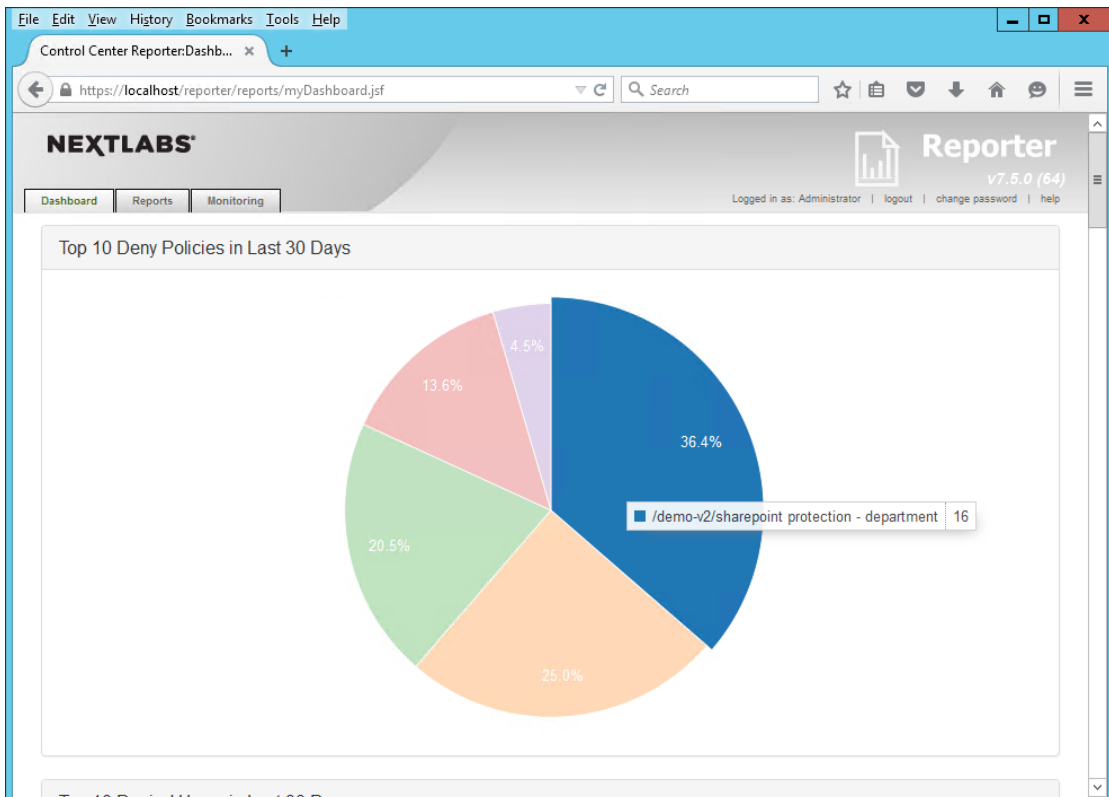
4753

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.

4754

Example seen in the image below: 36.4% of the Deny policies evaluated in the last 30 days belonged to the SharePoint Protection – Department policy set.

4755

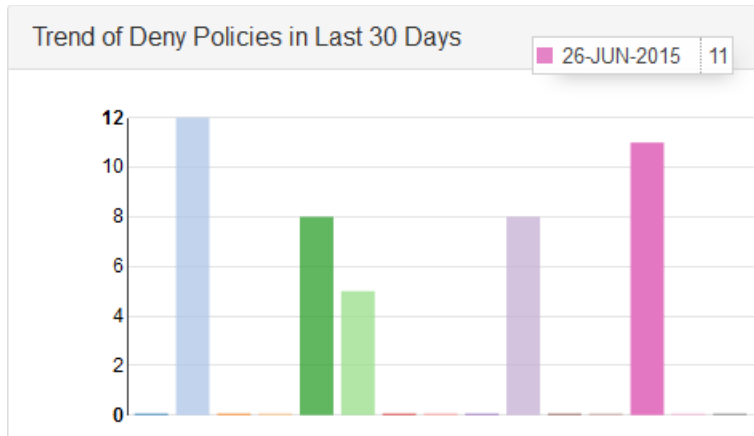


4756

4757

4758

Another example from this build seen in the image below: in the Deny Policies trend in the last 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**  
 4762 **Reports** on the left side of the Reports tab window and **Report Details** on the right.

**Report Details Configuration:**

- 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:** Ask Question, Attach to Item, Change Attributes, Change File Permissions, Copy / Embed File
- User:** [Search Input]
- User Criteria:** [Criteria Selection] Equals [Max 255 characters]
- Resource Name:** [Input Field]
- Resource Criteria:** FROM\_RESOU [Criteria Selection] Equals [Max 255 characters]

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

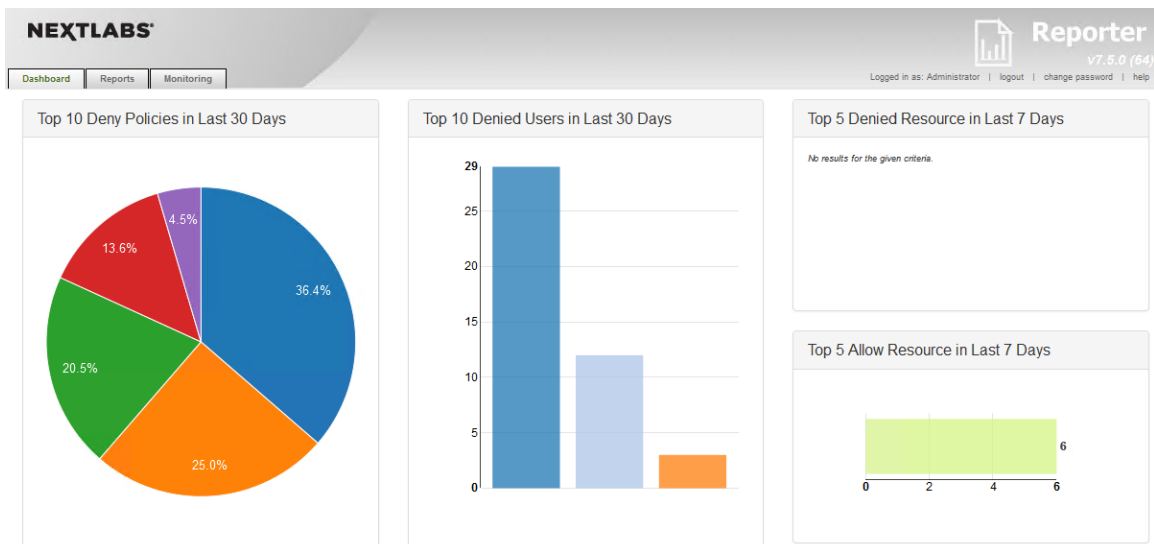
4783 Before being able to define a custom report, you must first log in to Reporter and click on the Reports  
4784 tab as seen in the steps below:

- 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**.



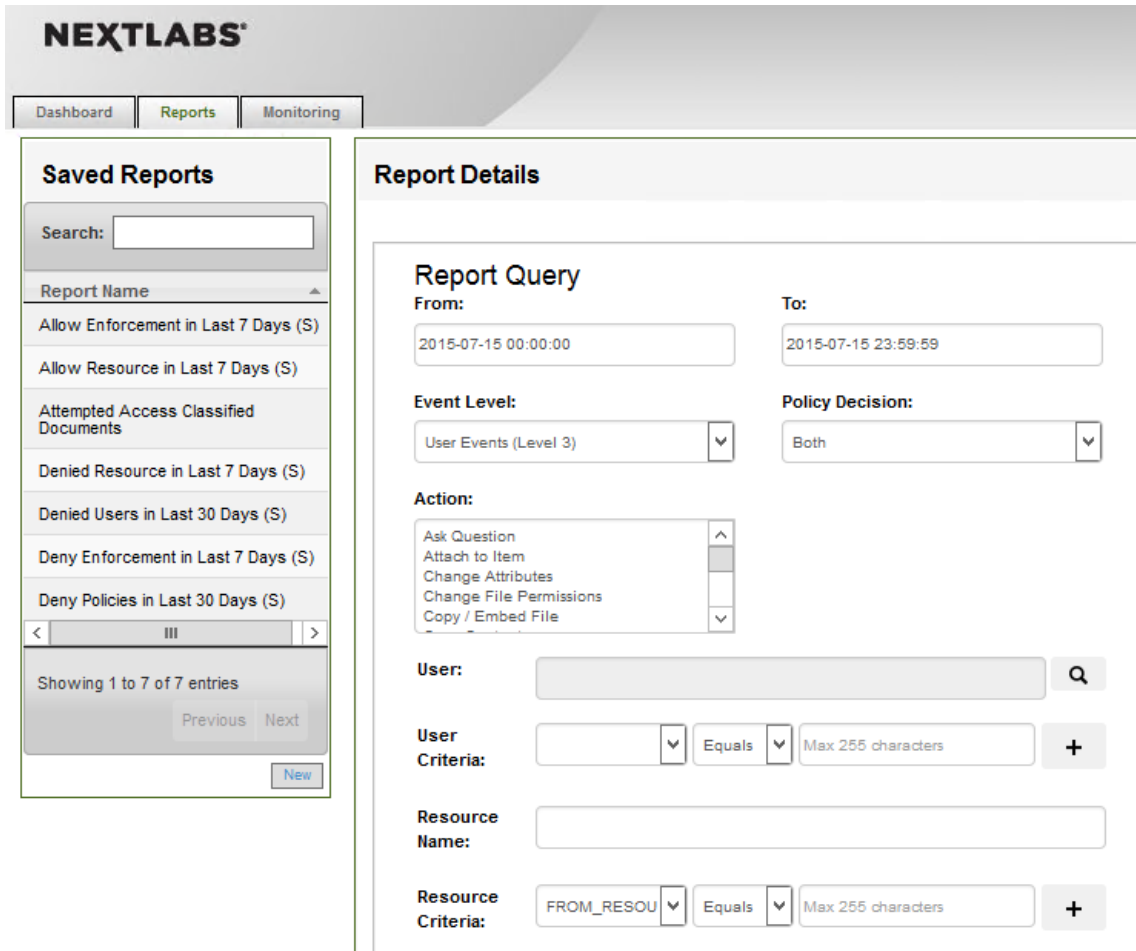
4790

- 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.



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:** 2015-07-15 00:00:00 **To:** 2015-07-15 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:** [Search field] **Q**

**User Criteria:** [Dropdown] Equals [Dropdown] Max 255 characters **+**

**Resource Name:** [Text field]

**Resource Criteria:** FROM\_RESOURCE [Dropdown] Equals [Dropdown] Max 255 characters **+**

**Policy Full Name:** [Search field] **Q**

**Policy Criteria:** POLICY\_NAME [Dropdown] Equals [Dropdown] Max 255 characters **+**

**Other Criteria:** APPLICATION\_NAME [Dropdown] Equals [Dropdown] Max 255 characters **+**

- 4801
- 4802 1. In the Report Details - Report Query pane, define the report query by filling in data or using
- 4803 drop-down menus to define your desired report.
- 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
- 4806 time, respectively, of the time period you want the report to cover. Click in the
- 4807 field to choose a date and time from the calendar. When specifying a report
- 4808 period, be sure to consider the time zone where Control Center is installed, and
- 4809 the time period of data stored in the Activity Journal.
- 4810 ii. In **Event Level**, select the level of event verbosity the report contains:
- 4811 1. User Events (default): Logged in the Activity Journal as Level 1
- 4812 2. Application Events (application and user-level events): Logged in the Ac-
- 4813 tivity Journal as Level 2
- 4814 3. All System Events (system, application, and user-level events): Logged in
- 4815 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 a configuration interface for a custom report. It includes the following elements:

- Report Type :** A dropdown menu with "Table" selected.
- Show :** A dropdown menu with "-- Group by options --" selected.
- Sort By:** A dropdown menu with "DATE" selected, and radio buttons for "Asc" and "Desc" (with "Desc" selected).
- Max Results :** A dropdown menu with "100" selected.
- Display Columns :** A text field containing "USER\_NAME, HOST\_NAME, APPLICATION\_NAME, POLICY\_FULLNAME, ..." and a hamburger menu icon.
- 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



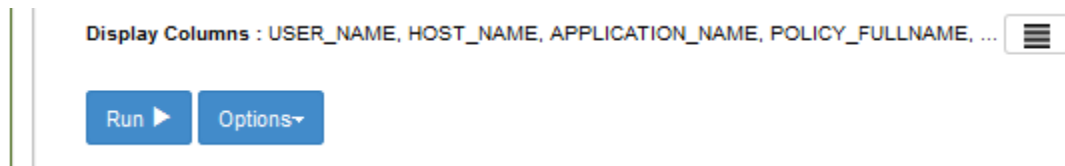
4881 chart. For readability reasons, charts should display a limited number of bars or slices. For a  
 4882 table, the number represents the maximum number of rows (each row represents an event).  
 4883 Tables that show a large number of rows present the data on multiple pages.

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.

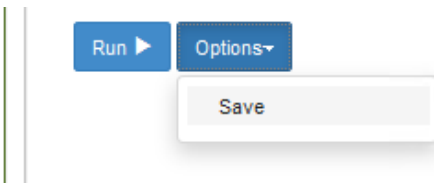
## 4888 9.4.2 Running a Custom Report

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  
 4893 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.

- 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.

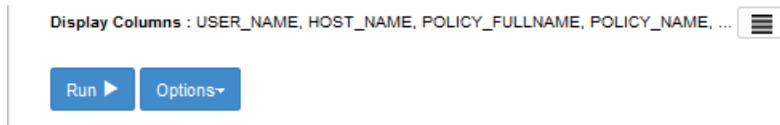
The screenshot shows the 'Report Query' interface with the following settings:

- 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:** [Empty search field]
- User Criteria:** [Empty dropdown] Equals [Empty text field] Max 255 characters
- Resource Name:** [Empty text field]
- Resource Criteria:** FROM\_RESOURCE\_PAT [Empty dropdown] Equals [Empty text field] Max 255 characters
- Policy Full Name:** [Empty search field]
- Policy Criteria:** POLICY\_NAME [Empty dropdown] Equals [Empty text field] Max 255 characters
- Other Criteria:** APPLICATION\_NAME [Empty dropdown] Equals [Empty text field] Max 255 characters
- Report Type:** Table
- Show:** -- Group by options --
- Sort By:** DATE [Empty dropdown] Asc Desc (Desc selected)
- Max Results:** 11
- Display Columns:** USER\_NAME, POLICY\_NAME, POLICY\_DECISION, FROM\_RESOURCE\_NAME, ...

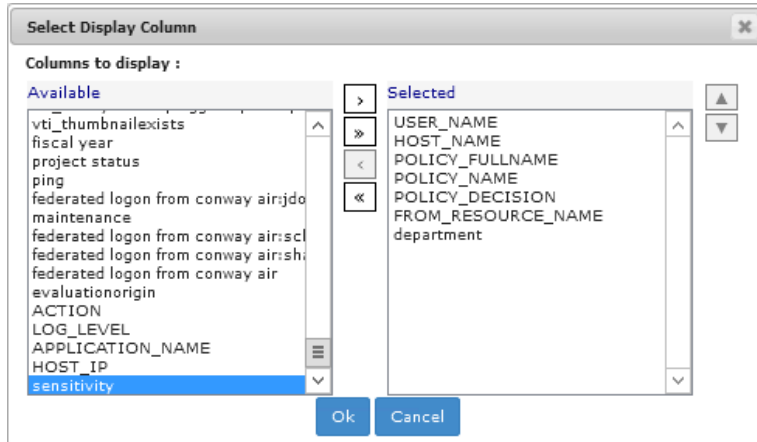
4912


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
- 4918 (i.e. Action, Log\_Level, Host\_IP, etc) and custom attributes (department, sensitivity).

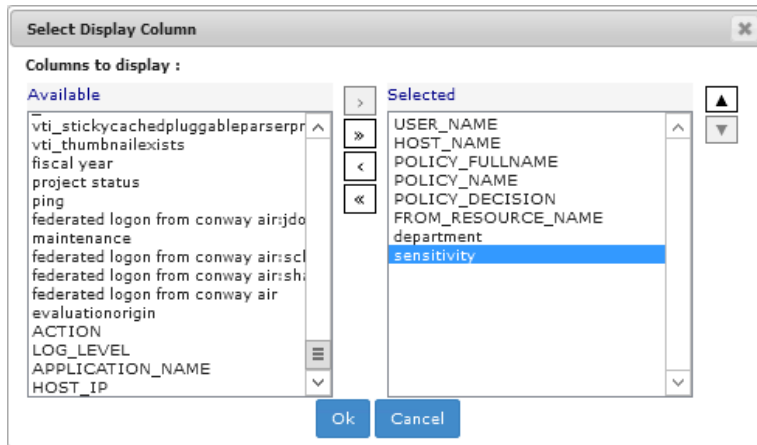


- 4919
- 4920 3. Click on any available attribute of interest to highlight it, then click the single right arrow button
- 4921  to add it to the list of **Selected** attributes.

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

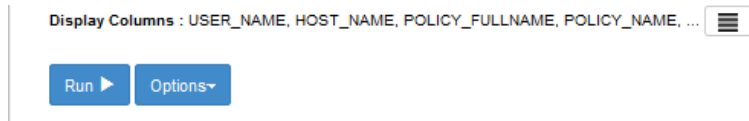
4924 between lists, or as a group by using the double arrow buttons between lists.



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
- 4928 **Options** and **Save** or **Save As** to save the query for future use.)



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
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@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
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint:/sharepoint.abac.test/InternetTechnology	Internet Technology	
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint:/sharepoint.abac.test/InternetTechnology	Internet Technology	
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint:/sharepoint.abac.test/InternetTechnology	Internet Technology	
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint:/sharepoint.abac.test/style_library/en-us/temable/core/styles/controls15.css		
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint:/sharepoint.abac.test/style_library/en-us/temable/core/styles/controls15.css		
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint:/sharepoint.abac.test/style_library/en-us/temable/core/styles/controls15.css		
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint:/sharepoint.abac.test/s/teassets/runabout air logo.png		
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint:/sharepoint.abac.test/s/teassets/runabout air logo.png		
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint:/sharepoint.abac.test/s/teassets/runabout air logo.png		
<a href="#">Jun 12, 2015 2:32 PM</a>	federated logon from conway airjoe@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
- 4938 through 5)
- 4939
  - Each event corresponds to one of three policies: SharePoint Protection – Sensitivity, SharePoint Protection – Maintenance Denied 5am-
- 4940 5pm, or SharePoint Protection – Department.
- 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
    - 4943 at sensitivity level 3.
    - 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
    - 4947 used on the SharePoint site.
    - 4948
      - The eleventh and final row from this excerpt shows that the resource was another .rtf document from the Internet Technology
    - 4949 department SharePoint sub-site, marked at sensitivity level 1.

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 with the following elements:

- Report Type :** A dropdown menu with "Bar Chart" selected.
- Show :** A dropdown menu with "Group by Policy" selected.
- Sort By:** A dropdown menu with "Policy" selected.
- Max Results :** A dropdown menu with "6" selected.
- Sorting options:  Asc and  Desc.

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 of the Report Query pane with the following elements:

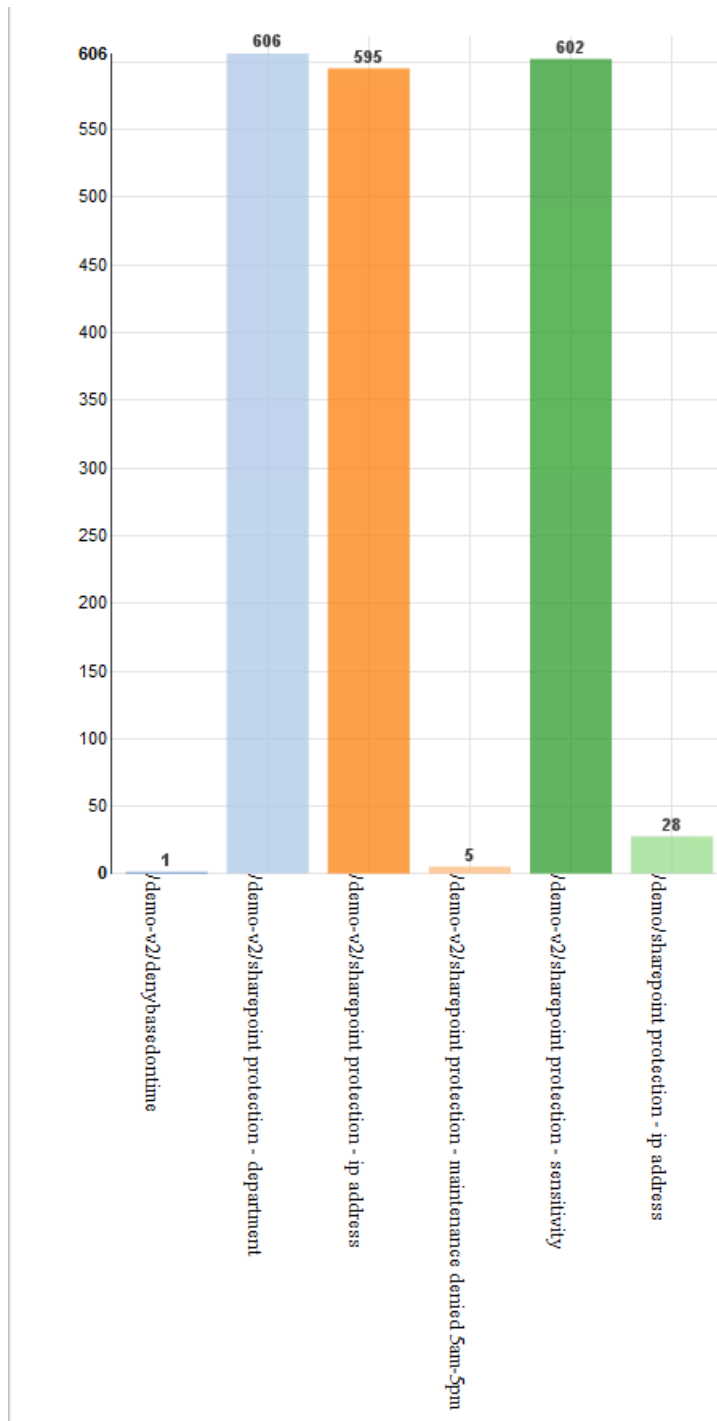
- Display Columns :** A text field containing "USER\_NAME, HOST\_NAME, POLICY\_FULLNAME, POLICY\_NAME, ..." and a menu icon.
- Run** button: A blue button with a play icon.
- Options** button: A blue button with a dropdown arrow.

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.

Report Type : Bar Chart

Show : Group by User

Sort By: User

Max Results : 6

Display Columns : USER\_NAME, POLICY\_NAME, POLICY\_DECISION, FROM\_RESOURCE\_NAME, ...

Run Options

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.

Display Columns : USER\_NAME, HOST\_NAME, POLICY\_FULLNAME, POLICY\_NAME, ...

Run Options

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 

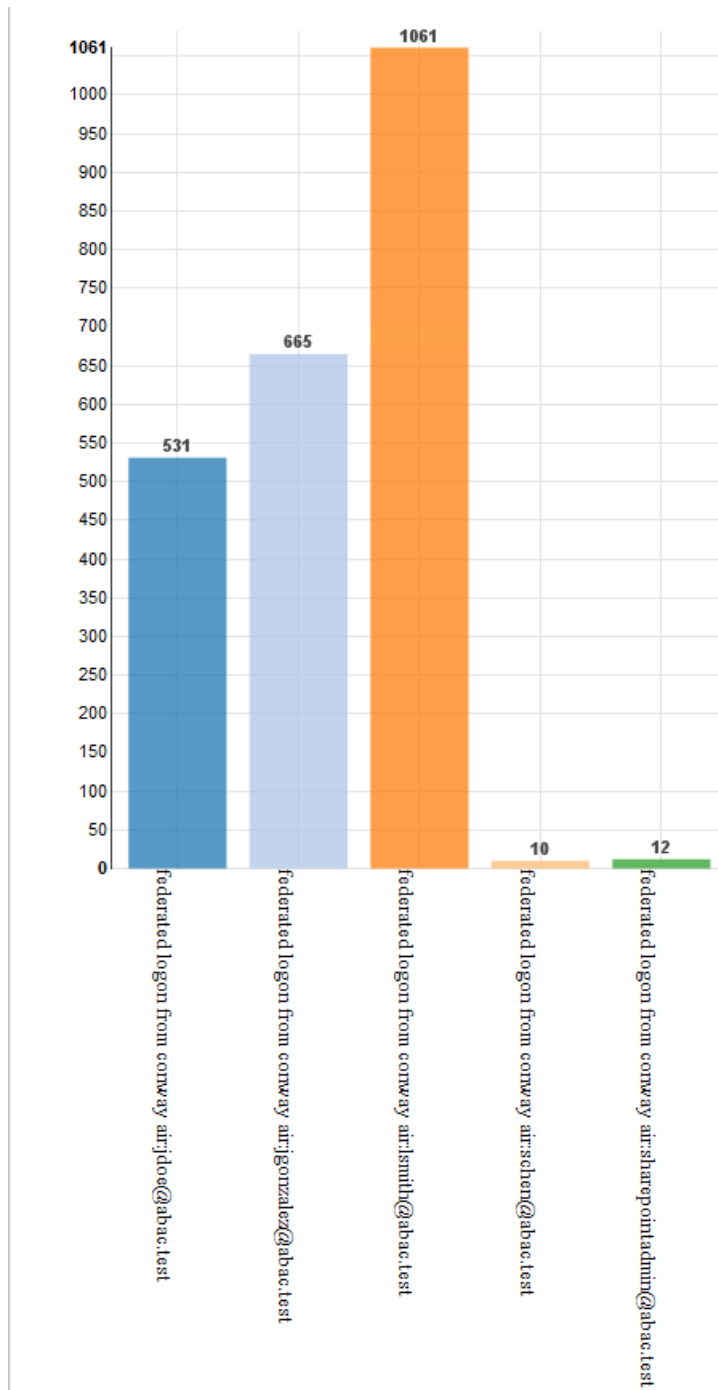
- Two users had very minimal activity logged during this week: schen@abac.test and  
5006 sharepointadmin@abac.test

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 a web-based report configuration interface. It includes several dropdown menus and radio buttons. The 'Report Type' dropdown is set to 'Pie Chart'. The 'Show' dropdown is set to 'Group by Resource'. The 'Sort By' dropdown is set to 'Resource', and the 'Asc' radio button is selected. The 'Max Results' dropdown is set to '10'. The 'Display Columns' field shows a list of columns: 'USER\_NAME, POLICY\_NAME, POLICY\_DECISION, FROM\_RESOURCE\_NAME, ...'. At the bottom, there are two buttons: 'Run' and 'Options'.

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.

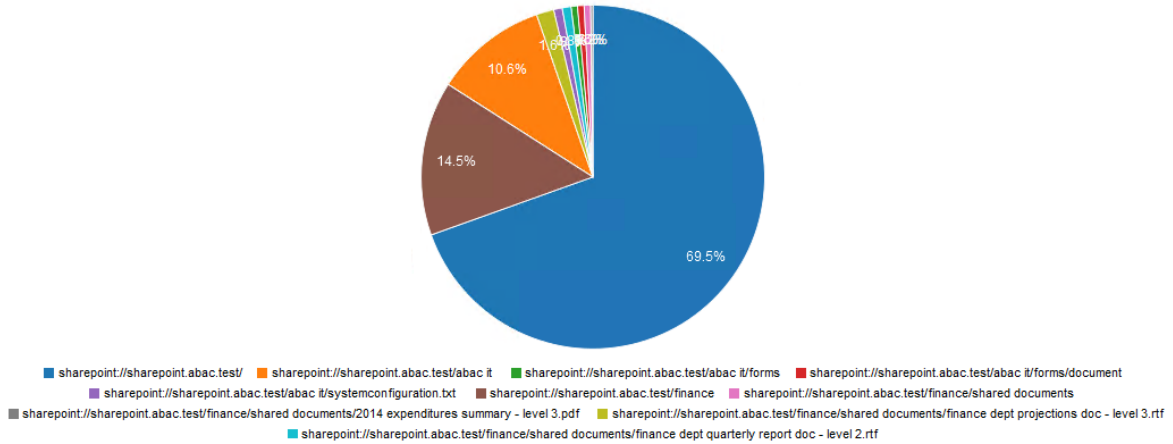
### 5033 *9.5.5.3 Viewing the Results as a Bar Chart Grouped by User*

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
- 5038
- 5039
- 5040
- 5041
- 5042
- The most commonly accessed resource during this week period (69.5%) was our build's SharePoint home page.
  - The two second-most accessed resources during this week period were the ABAC IT department and its forms sub-site (where documents are stored).
  - The remaining seven most-accessed resources during this week after the top three have 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

## 9.6 Further Example Custom Reports from Our Build

5046

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: **lsmith**) 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.

### 9.6.1 Custom Report Illustrating All Access for One User During a Two-Month Period

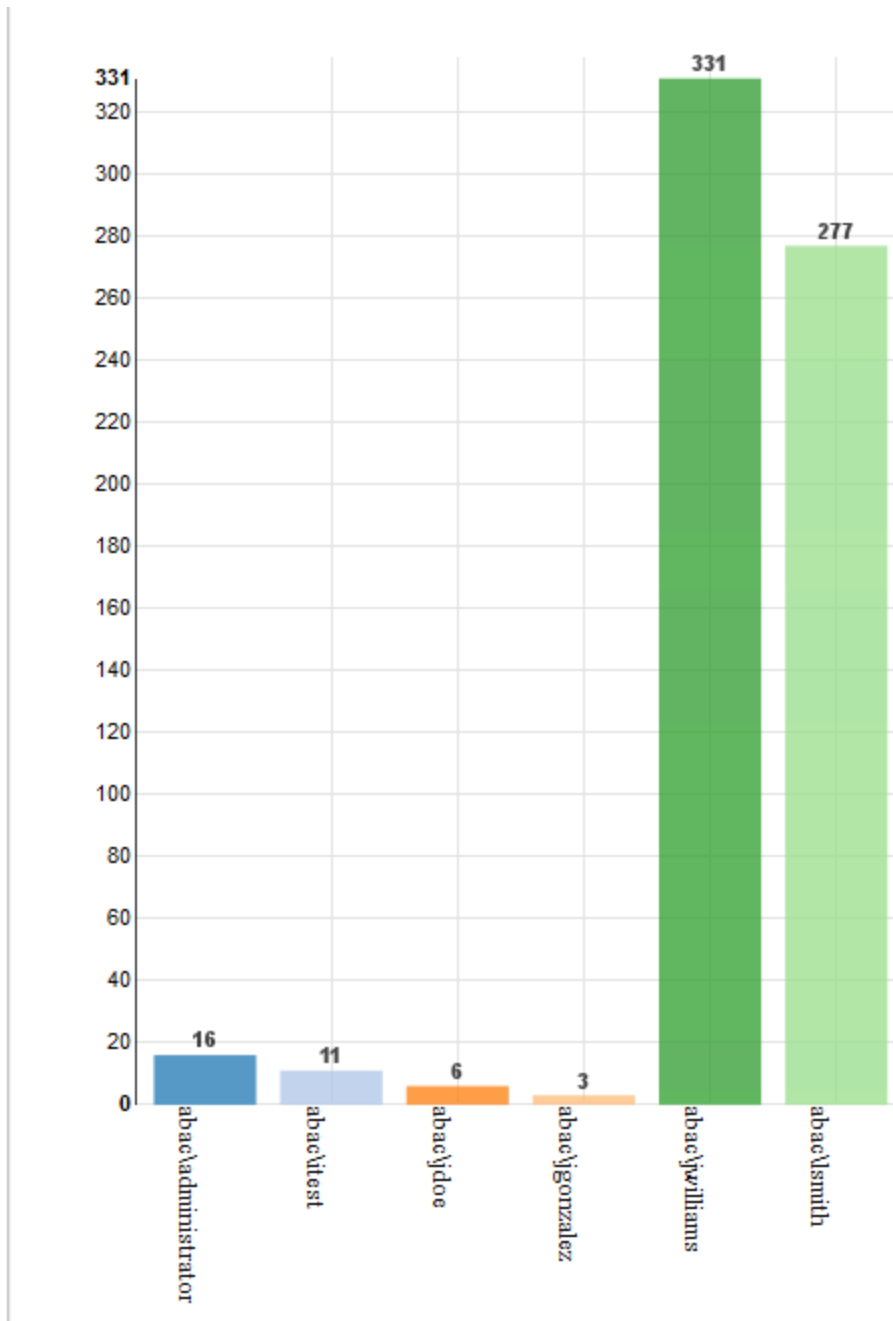
5059

5060

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 lsmith@abac.test or abac\lsmith (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\smith**.

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:**  **To:**

**Event Level:**  **Policy Decision:**

**Action:**

- Ask Question
- Attach to Item
- Change Attributes
- Change File Permissions
- Copy / Embed File

**User:**

**User Criteria:**

**Resource Name:**

**Resource Criteria:**

**Policy Full Name:**

**Policy Criteria:**

**Other Criteria:**

**Report Type :**  **Show :**

**Sort By:**   Asc  Desc

**Max Results :**

5073

5074

5075

4. Within the browser window, scroll back down to the resulting Table to review its data. See the excerpt below.

5076

5077

If desired, you can change the Display Columns, Report Type, etc. to customize your view as illustrated in previous subsections.

5078

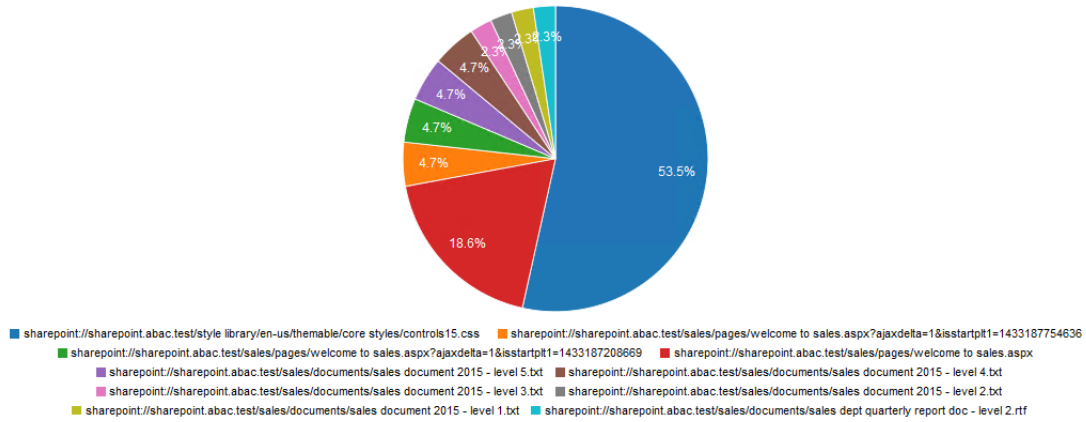
Date	USER_NAME	ACTION	POLICY_FULLNAME	POLICY_DECISION
<a href="#">May 15, 2015 9:59 AM</a>	abac\smith	Open	scenario\scenario1	Allowed
<a href="#">May 19, 2015 12:19 PM</a>	abac\smith	Open	scenario 1\scenario 1-1	Denied
<a href="#">May 19, 2015 12:20 PM</a>	abac\smith	Open	scenario 1\scenario 1-1	Denied
<a href="#">May 19, 2015 12:21 PM</a>	abac\smith	Open	scenario 1\scenario 1-1	Denied
<a href="#">May 20, 2015 11:42 AM</a>	abac\smith	Open	scenario 1\scenario 1-1	Denied
<a href="#">May 20, 2015 11:47 AM</a>	abac\smith	Open	scenario 1\scenario 1-1	Denied

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 **lsmith**.



- 5091
- 5092 4. Within the browser window, scroll up to Report Details and verify that the Resource Name: field  
 5093 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:**

**Event Level:**  **Policy Decision:**

**Action:**

- Ask Question
- Attach to Item
- Change Attributes
- Change File Permissions
- Copy / Embed File

**User:**

**User Criteria:**

**Resource Name:**

**Resource Criteria:**

**Policy Full Name:**

**Policy Criteria:**

**Other Criteria:**

**Report Type :**  **Show :**

**Sort By:**   Asc  Desc

**Max Results :**

5096

5097

5098

5. Within the browser window, scroll back down to the resulting table to review its data. See the excerpt below.

5099

5100

If desired, you can change the Display Columns, Report Type, etc. to customize your view as illustrated in previous subsections.

5101

Date	USER_NAME	ACTION	POLICY_FULLNAME	POLICY_DECISION
Jun 8, 2015 7:37 AM	federated.login.from.conway.air.smith@abac.test	Open	demo:sharepoint.protection - sensitivity	Denied



## 5102 **10 Configuring a Secondary Attribute Provider**

### 5103 **10.1 Introduction**

5104 This section provides a description of the architecture, compilation, and deployment instructions for a  
5105 secondary attribute provider and its components, which we describe as a custom Policy information  
5106 point (PIP), to be included as part of the ABAC infrastructure. We also demonstrate how to configure the  
5107 Relying Party server to accommodate the custom PIP and its component JIT provisioning mechanism.

5108 The secondary attribute provider comes into the picture when a user tries to access a resource at the  
5109 Relying Party's Resource Provider, and the Policy decision point (PDP) finds that an essential attribute  
5110 needed to make the access control decision is missing from the initial set of attributes sent from the  
5111 Identity Provider. In our build, this would mean a user with a federated identity (via PingFederate  
5112 Identity Provider, IdP, augmented with two-factor authentication by RSA AA) has already logged into  
5113 Microsoft SharePoint (Relying Party's Resource Provider), but when trying to open a particular resource  
5114 on the site, the NextLabs Policy Controller (PDP) makes a run-time decision that additional subject  
5115 attributes are needed before the access decision can be made. The PDP determines this while evaluating  
5116 the existing ABAC policies (created in the NextLabs Policy Studio, PAP in our ABAC build) against the  
5117 user, resource, and environmental attributes at play at the time of requested access.

5118 Providing the secondary attribute collection capability in our build required the implementation of new  
5119 components and related features, which we will describe more in detail later in the section:

- 5120     ▪ NextLabs Policy Information Point (PIP) Plugin to extend the NextLabs Policy Controller (PDP)  
5121       when additional attribute(s) are needed
- 5122     ▪ Protocol broker to initiate and receive a SAML attribute query and SAML response
- 5123     ▪ Custom data store plugin for PingFederate on the Relying Party (RP) server which will cache  
5124       attributes in order to limit the number of secondary requests to the PingFederate Identity  
5125       Provider (IdP) server
- 5126     ▪ Apache Directory Server (ApacheDS), an LDAP in which PingFederate can create and update  
5127       local user accounts and associated attributes based on the attributes contained in SAML  
5128       assertions received after authentication from IdP
- 5129     ▪ PingFederate RP configuration must be modified so that it can serve as an IdP as needed, such  
5130       as when checking its JIT cache (Apache DS LDAP) before sending requests to the IdP

5131 In later sub-sections of this section we will discuss in detail the purpose of each of these new  
5132 components and features, and how they are developed, configured, compiled, and deployed.

5133 Note: The custom PIP we have developed involves new custom components, open source components,  
5134 and commercially available components. For open source and commercial components, the related  
5135 descriptions in this section have been limited to installation and relevant configuration required for the  
5136 desired functionality of our build. If you are interested in other details or additional capabilities of this  
5137 software, explore the referenced product literature or contact that organization.

### 5138 10.1.1 Pre-Requisites

5139 In order to follow the instructions of this How-To section, it is necessary that seven of the previous How-  
5140 To sections have been successfully completed. The required components that must be installed and  
5141 configured before continuing in this How-To section include:

- 5142     ▪ Installation and Configuration of Active Directory ([Section 2](#))
- 5143     ▪ Installation and Configuration of RSA AA ([Section 2](#))
- 5144     ▪ Installation and Configuration of RSA AA Plugin ([Section 2](#))
- 5145     ▪ Installation and Configuration of PingFederate on both the RP and IdP federation servers  
5146         ([Section 2](#) and [Section 3](#)),
- 5147     ▪ Installation and Configuration of Microsoft SharePoint ([Section 4](#) and [Section 5](#))
- 5148     ▪ Configuration of the attribute flow ([Section 6](#))
- 5149     ▪ Installation and Configuration of NextLabs Control Center, Policy Studio, Policy Controller, and  
5150         Entitlement Manager for SharePoint Server ([Section 7](#))

### 5151 10.1.2 Criteria for Secondary Attribute Collection

5152 At the time of ABAC policy evaluation, required attributes may not be available or the system may not  
5153 find it appropriate to use for various reasons, including, but not limited to:

- 5154     ▪ For security and privacy purposes it is not ideal to acquire all known attributes for a subject  
5155         when the session is created. Some attributes maybe PII or of higher sensitivity and should not be  
5156         sent to the relying party until an access request made by the user requires those attributes.
- 5157     ▪ Depending on the longevity of a session, attributes risk becoming stale. Because of this potential  
5158         for staleness, it is essential to procure attributes as needed, depending on the freshness criteria  
5159         established by the system. The freshness of attributes is sometimes guided by the policies  
5160         established for a local cache.
- 5161     ▪ The attribute needed for a specific attribute request may not an attributed owned by the  
5162         Identity provider but rather may need to be acquired from an external party attribute provider.

### 5163 10.1.3 Components

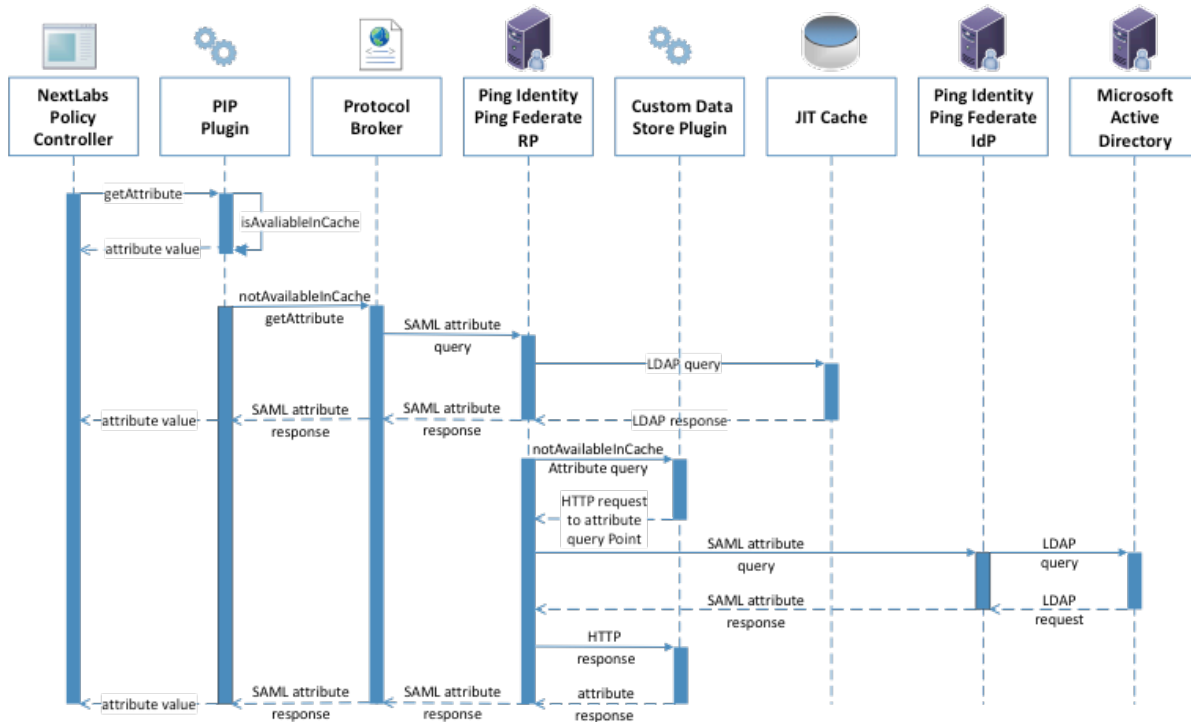
5164 The custom PIP described in this section is composed of four new components and mechanisms which  
5165 interact or integrate with different existing components in our ABAC build as extensions, plugins, or web  
5166 applications:

- 5167     ▪ **NextLabs Plugin:** This plugin extends the NextLabs Policy Controller to make attributes available  
5168         based on the criteria mentioned in Section 10.1.2, when the PDP determines that attribute  
5169         values needed to evaluate an ABAC policy are insufficient or unavailable. Following the  
5170         recommendation in the software development framework provided by NextLabs, the NCCoE  
5171         implemented this PIP plugin in Java, and deployed the plugin within the NextLabs Policy  
5172         Controller software architecture on the server we call SharePoint server in our build. Due to the  
5173         requirements of the Policy Controller architecture, the plugin can request the values of multiple  
5174         missing attributes sequentially, one at a time.

- 5175
- 5176
- 5177
- 5178
- 5179
- 5180
- 5181
- 5182
- 5183
- 5184
- 5185
- 5186
- 5187
- 5188
- 5189
- 5190
- 5191
- 5192
- 5193
- 5194
- 5195
- 5196
- **Protocol Broker:** This agent, in the form of [servlet](#) local to the NextLabs installation, is responsible for facilitating communication between the NextLabs PIP Plugin and the PingFederate RP server following an Assertion Query/Request SAML2 Profile. This web application is deployed on a tomcat server that listens on localhost( 127.0.0.1) and only communicates using https with mutual TLS. Similar to the NextLabs PIP Plugin, this component is also installed on the SharePoint server.
  - **Ping Custom Data store:** This custom data store is an extension built using Ping SDK. It enables the RP server to query the IdP server and coordinates resulting attribute values back to the RP. When it is chained with a built-in data store to query JIT Cache (LDAP), it enables RP to provide data from and configuration to various data stores (JIT in this build). This helps the custom data store to query and coordinate the result from local JIT and remote Active Directory at the PingFederate IdP.
  - **Just-in-Time provisioning** is a feature provided by PingFederate to store attributes of a subject for a limited time. We implemented JIT provisioning using [ApacheDS](#). ApacheDS 2.0 is an embeddable, extendable, standards compliant, modern LDAP server written entirely in Java, and available under the [Apache Software License](#). It also supports network protocols like Kerberos and NTP. PingFederate RP acts as an IdP for the secondary attribute provider. To fulfill in this role, the PingFederate administrative console provides mechanisms to configure SP and IdP connections. These configurations manage connection settings to support the exchange of federation-protocol messages. It also allows configuration of data stores within the connection and an attribute contract that acts as the medium to convey attribute mapping from one entity 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
<b>Ping Custom Data Store</b>	PingFederate RP server	Ant 1.9.2	PingFederate 7.3.2; Java version same as PingFederate installed	Windows Server 2012	
<b>NextLabs Plugin</b>	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.
<b>Protocol Broker</b>	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	
<b>Apache Directory Server</b>		N/A	PingFederate 7.3.2; <b>Java 7.0</b> (recommended by <a href="#">Oracle's JDK</a> . Some <a href="#">issues</a> 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

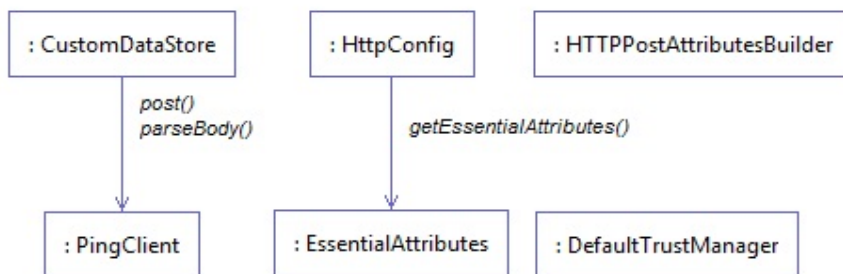
- 5251 • Similarly, dispatching the http request relies on PingClient class. PingClient uses classes  
5252 under the [spring](#) http package. PingClient sends an https query to Attribute Query End Point.  
5253 All of the parameters for the https URL are provided by the web interface.

#### 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)`

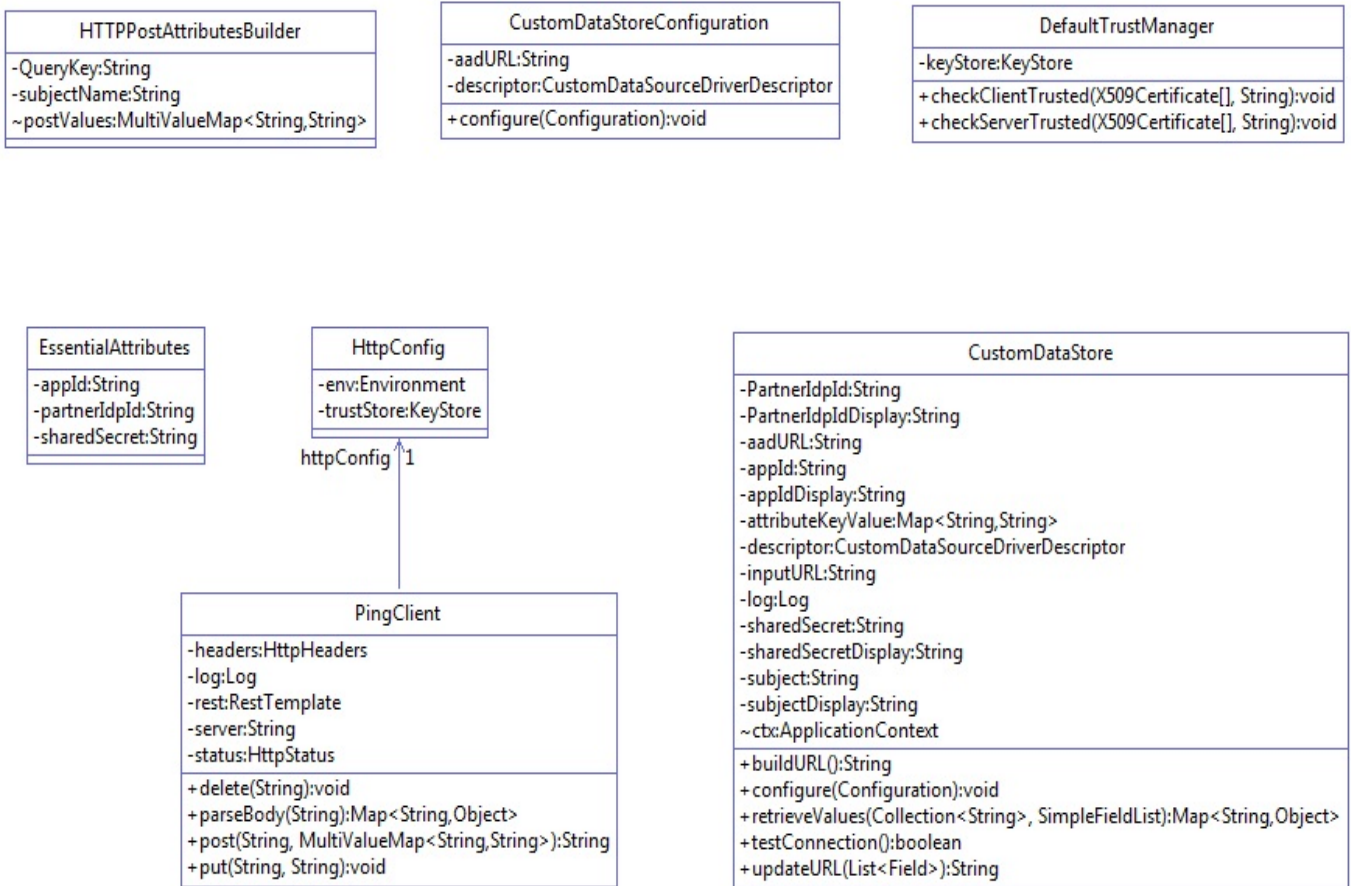
5264 The Class Structure and their interactions are provided in the Interaction Diagram and Class Diagram.

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.
- 5289 `target-plugin.name=idp-query-data-store`
- 5290 12. Within the Command Prompt window, navigate to your **idp-query-data-store** folder by entering  
 5291 a cd command with a path to your **idp\_query\_data\_store** and pressing Enter. Example: `cd C/--`  
 5292 `path-to-your-idp_query_data_store`
- 5293 13. Within the Command Prompt window, copy **idp-query-data-store** along with all subfolders to  
 5294 your PingFederate installation's **sdk/plugin-src** folder by entering a cp command and pressing  
 5295 Enter. Example: `cp -rf idp_query_data_store C:/pingfederate-`  
 5296 `7.3.0/pingfederate/sdk/plugin-src`
- 5297 14. Within the Command Prompt window, run the following command and press enter in order to  
 5298 make sure all relevant subfolders exist: **ls -ltr ./idp-query-data-store/**
- 5299 a. Example results from the above command:
- 5300 `total 4`  
 5301 `drwxrw-r--. 3 t... t... 16 Apr 29 11:34 java`  
 5302 `drwxrw-r--. 2 t... t... 4096 Apr 29 12:59 lib`  
 5303 `drwxrwxr-x. 4 t... t... 30 May 15 17:52 build`  
 5304 `drwxrw-r--. 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.

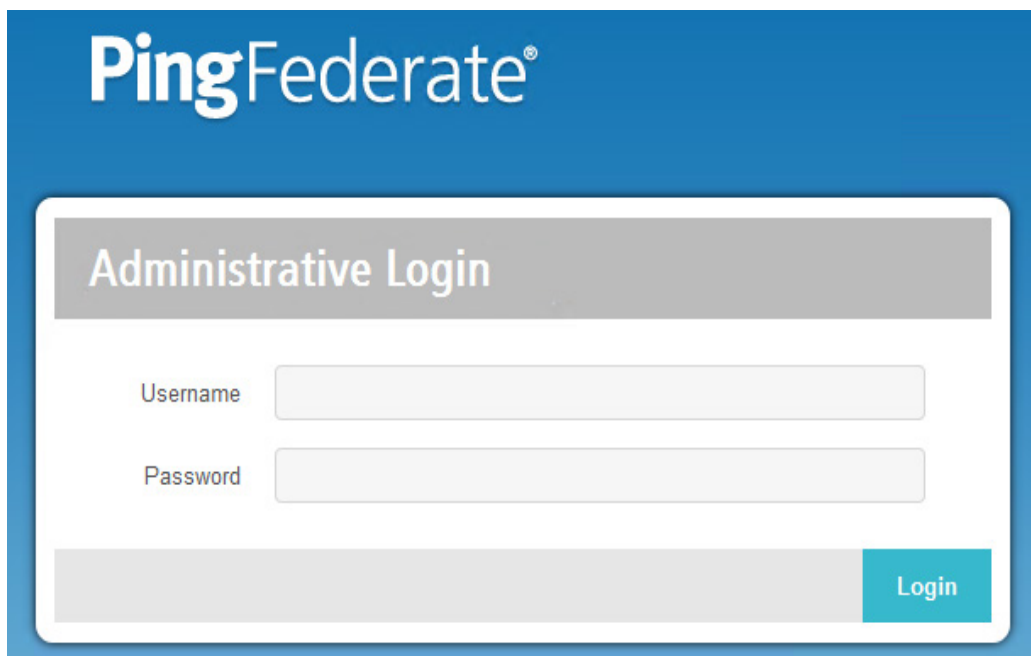
5324 5. Navigate to your PingFederate sdk folder, i.e., `cd C:/pingfederate-`  
 5325 `7.3.0/pingfederate/sdk/`

5326 6. Within the Command prompt window, type the following compilation command and press  
 5327 Enter: `ant deploy-plugin`

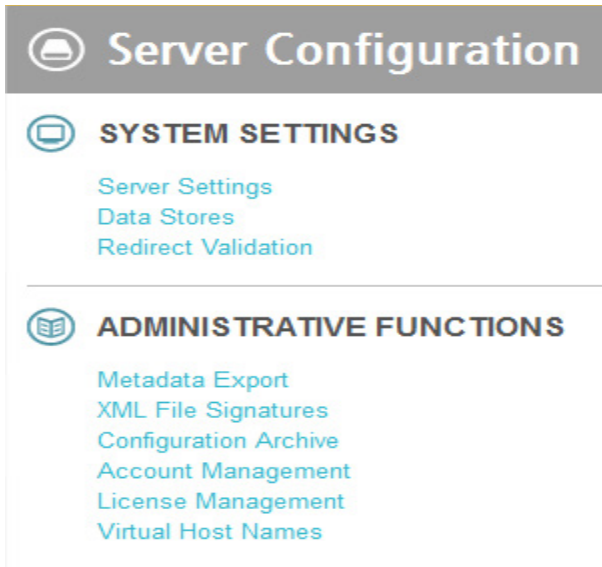
### 5328 10.3.4 Configuration within PingFederate Administrative Console

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**.

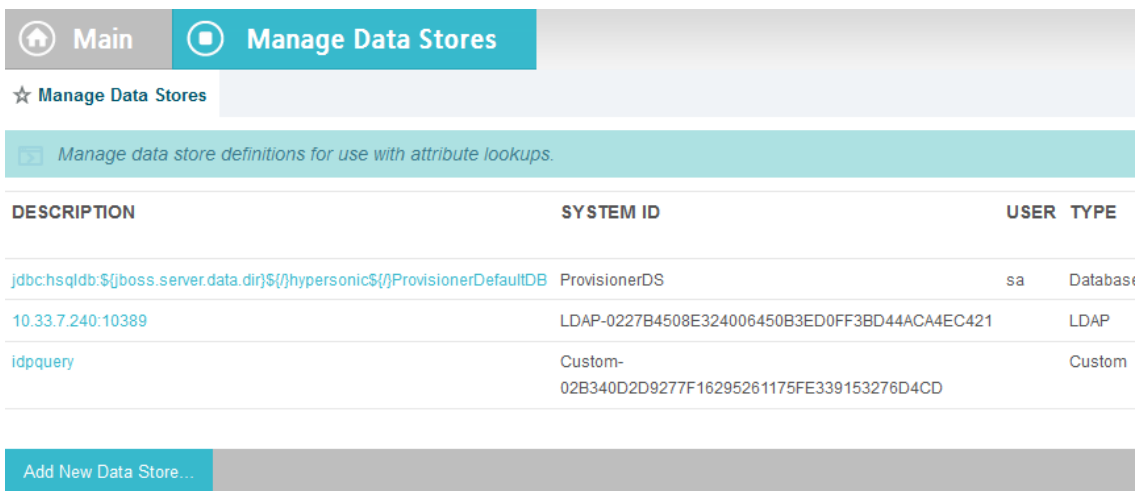


- 5335
- 5336 5. In the browser window, under the main menu area, find **Server Configuration > System Settings**  
 5337 **> Data Stores**. Double-click on **Data Stores**.



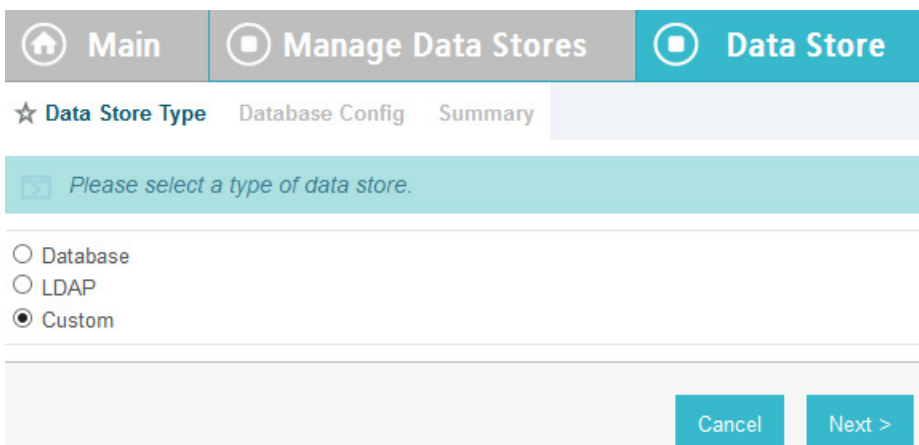
5338

5339 6. At the bottom of the browser window, click **Add New Data Store**.



5340

5341 7. On the Data Store Type screen, select **Custom** and click **Next**.



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&Part*  
 5351 *nerIdpid=https://idp.abac.test:9031&Subject=Ismith@abac.test*
- 5352     ▪ **Attribute Query URL:** the URL specifying the endpoint inside RP (Relying Party) that will  
 5353     query the IDP, i.e., *https://rp.abac.test:9031/sp/startAttributeQuery.ping*
  - 5354     ▪ **AppId field used in query:** the unique identity of the initiating application, i.e., *appid*
  - 5355     ▪ **Shared Secret field used in query:** used to authenticate the initiating application. The  
 5356     AppId and SharedSecret must both match the application authentication settings within  
 5357     the PingFederate server, i.e. *!23234Federate*
  - 5358     ▪ **Partner IDP ID:** used to identify the specific IdP partner to which the Attribute Query  
 5359     should be sent. If this parameter is not present, the Subject and Issuer are used to  
 5360     determine the correct IdP, i.e., *https://idp.abac.test:903*

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

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  
 5377 `EvalValue`. The `EvalValue` is created using its `build()` function and the attribute value  
 5378 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

- 5381       ▪ CacheKey class, implementing a local Ehcache
- 5382           • The CacheKey class constructor takes two parameters, the subjectId and the attributeName,
- 5383           which serve as a compound cache key for storing and retrieving the value of a given user's
- 5384           attribute within the plugin's local Ehcache.

#### 5385   10.4.1.2 *Other Required Files or Deployment Notes:*

- 5386       ▪ The three above classes must be compiled into a .jar file.
- 5387           • Our method of compilation in this build was using Apache Maven 3.2.5. Maven compilations
- 5388           are directed by a pom.xml ("Project Object Model"), which is an XML representation of a
- 5389           Maven project. More information about Apache Maven and its pom file requirements can
- 5390           be found here: <https://maven.apache.org/pom.html>
- 5391           • According to NextLabs support, be sure to include within the pom.xml file configuration a
- 5392           statement that specifies the Provider-Class. The Provider-Class is the UserAttrProviderMod
- 5393           class that contains the getAttribute() method. Example pom.xml excerpt from the pom.xml
- 5394           file in this implementation:

```

5395                   <configuration>
5396                    <archive>
5397                     <manifest>
5398                      <mainClass>nist.pdpplugin.UserAttrProviderMod</mainClass>
5399                     </manifest>
5400                    <manifestEntries>
5401                     <Provider-Class>nist.pdpplugin.UserAttrProviderMod</Provider-
5402                    Class>
5403                    </manifestEntries>
5404                    </archive>
5405                   </configuration>

```

- 5406       ▪ Also required per NextLabs support documentation, for any custom plugin you must include a
- 5407       properties file.
- 5408           • The configuration file should end with the ".properties" file extension. Example from this
- 5409           implementation: *nlsamlpluginService.properties*
- 5410           • Contents should be similar to our example copied below. You must include a *category =*
- 5411           *ADVANCED CONDITION* statement per NextLabs deployment and loading requirements:

```

5412                   name = NLSAMLPlugin_Service
5413                   jar-path = [NextLabs]/Policy
5414                   Controller/jservice/jar/nlsamlplugin/NLSAMLPlugin-0.0.1-SNAPSHOT-jar-
5415                   with-dependencies.jar
5416                   friendly_name = NLSAMLPlugin Service
5417                   description = NLSAMLPlugin Service

```

#### 5418   10.4.1.3 *Notes on Jar and Properties File Deployment within NextLabs Policy Controller*

#### 5419           *Software Architecture:*

- 5420       ▪ The jar file containing the three classes must be deployed on the SharePoint server within the
- 5421       NextLabs Policy Controller software architecture in a specific location. Under the *C:/Program*
- 5422       *Files/NextLabs/Policy Controller/jservice/jar* folder you must create a folder specifically for your
- 5423       custom jar, i.e., *C:/Program Files/NextLabs/Policy*
- 5424       *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

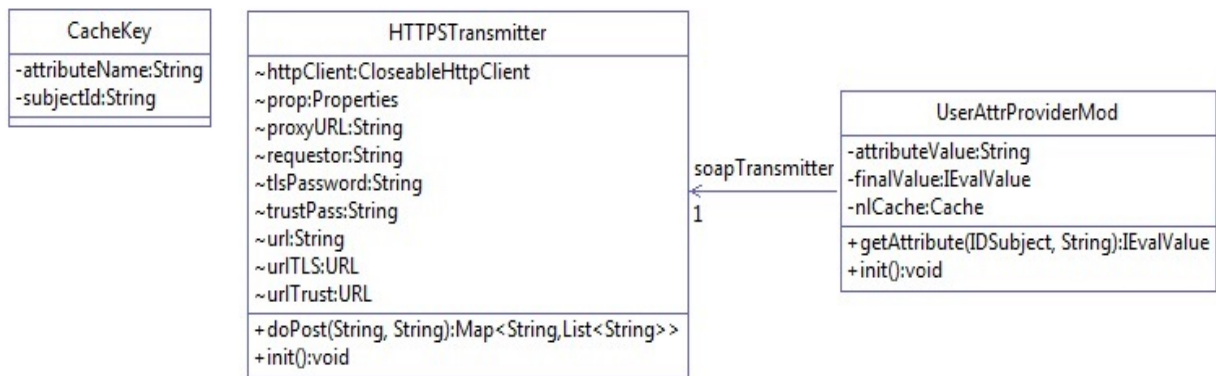
5447     determine an access decision. In the case that the requested attribute does not exist, the NextLabs

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

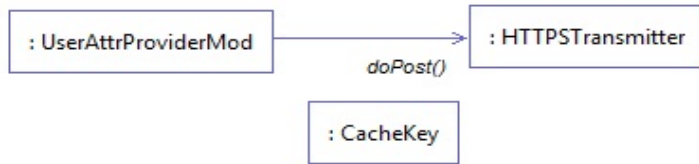
5450     produces an exception.

5451     **Figure 10-4 NextLabs PIP Plugin Class Diagram**



5452

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
- 5458 in our build.
- 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
- 5462 Enter, i.e., `cd C:/software/java/plugin/`
- 5463 5. In the Command Prompt window, run the following command and press Enter to compile your
- 5464 files and jar(s) into a single jar: `mvn clean install`

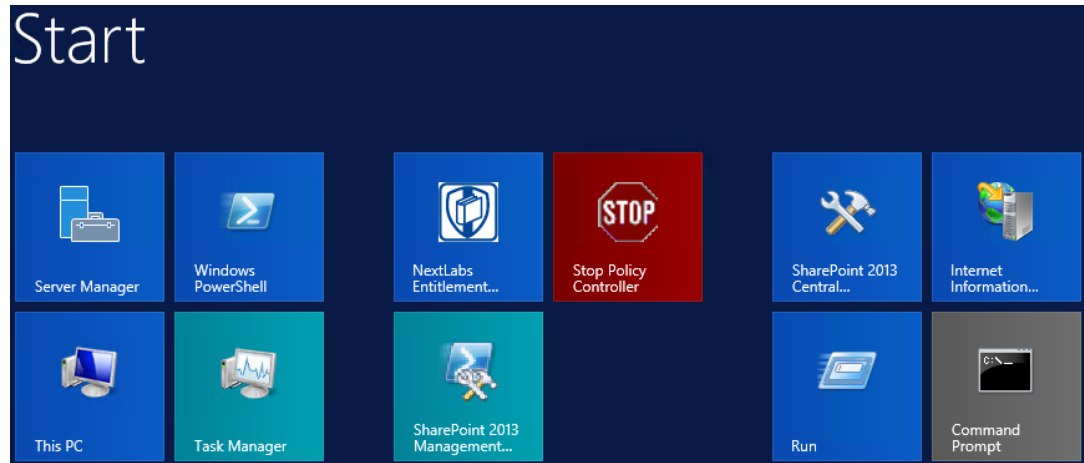
5465 

### 10.4.3.2 Stopping the NextLabs Policy Controller Service Before NextLabs PIP Plugin Jar

  
5466 *Deployment*

- 5467 1. Still on the SharePoint server, click on the Windows icon and begin typing **Services**.
- 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
- 5470 alphabetical order and look for **Control Center Enforcer Service**.
- 5471 4. If the status of the **Control Center Enforcer Service** is **running**, stop it by following these steps:
  - 5472 a. Click on the Windows icon.
  - 5473 b. On your main screen, double-click the **Stop Policy Controller** shortcut.

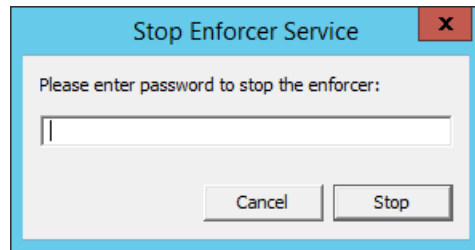




5474

5475

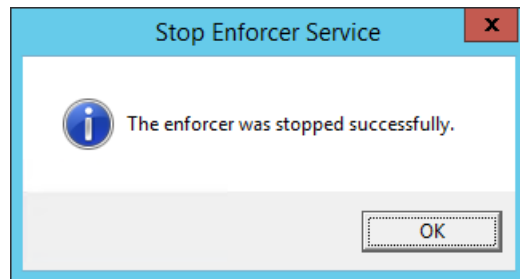
- c. Enter your NextLabs Administrator credentials, then click **Stop**.



5476

5477

- d. Click **OK**.



5478

5479 **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

5483

5484

5485

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

5488

5489

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

### 5532 *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

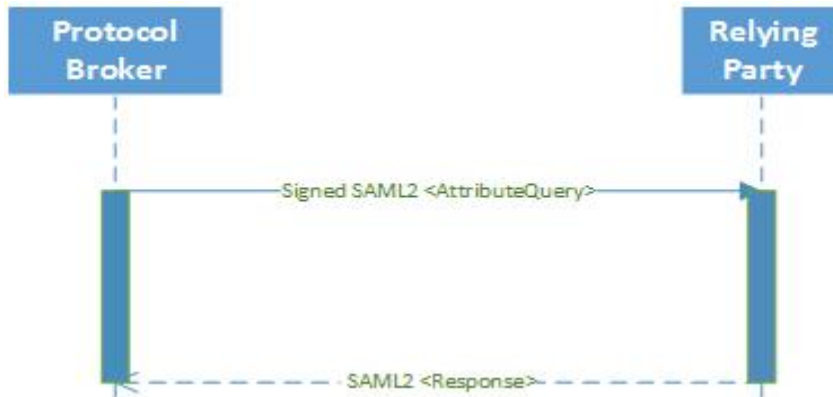
5537 On successful receipt of a request, SAMLProxy uses the SoapHTTPTransmitter class to transmit the  
5538 request to the PingFederate RP server. The response received from SOAPHTTPTransmitter is dispatched  
5539 back to the NextLabs PIP Plugin, which then hands the result off to the PDP for policy evaluation and  
5540 access decision making.

### 5541 *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**

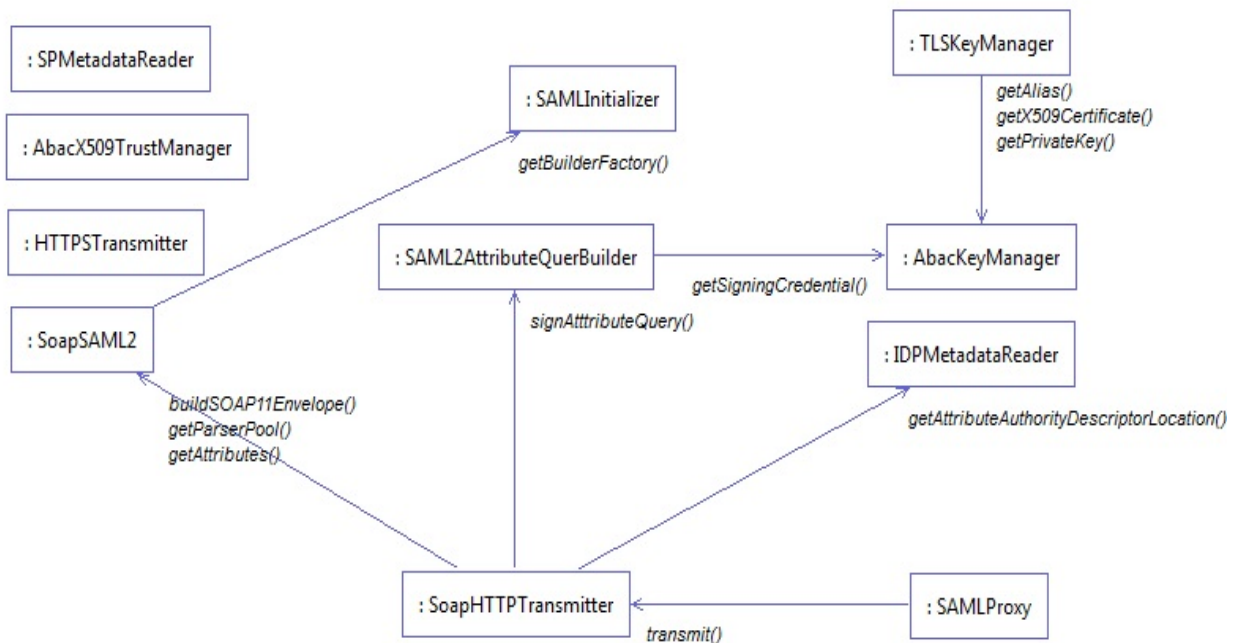


5552

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.

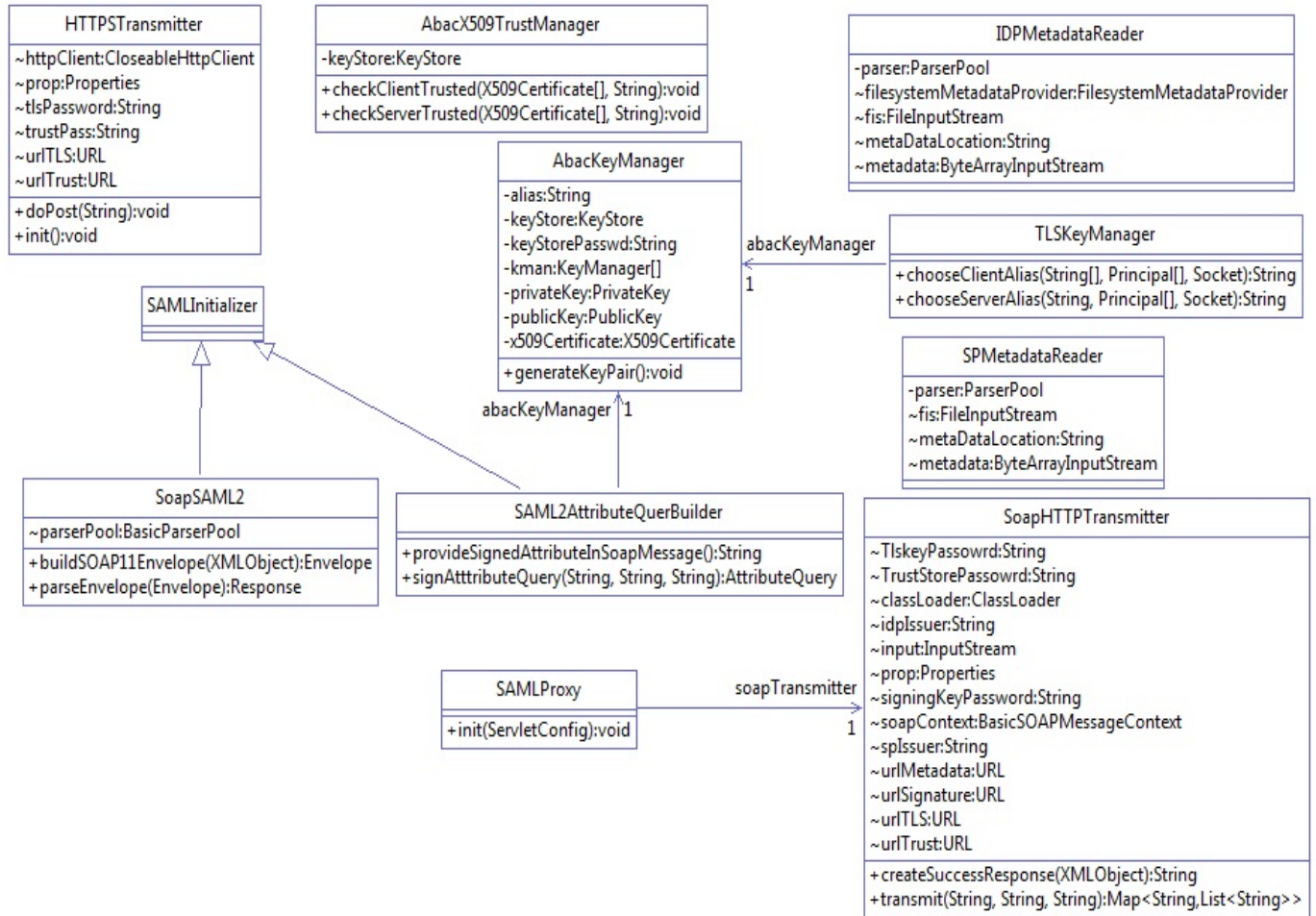
5559 HTTPSoapClient is also responsible for receiving the Attribute response, verifying the signature and  
 5560 sending the attributes back to the Nextlab Plugin.

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
- 5572 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

### 5594 *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:

#### 5597 *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  
5601 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  
5603 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] -----
5620 10.5.2.3.2 Compiling the .war File
5621      1. After following the instructions above to prepare for compiling, within the Command Prompt
5622         window, enter the following command and press Enter to create the Protocol Broker: .war file:
5623         mvn package
5624      2. Verify that your results are similar to the following, including the Failures: 0 and Build Success
5625         portions:
5626      [INFO] Scanning for projects...
5627      [INFO]
5628      [INFO] -----
5629      [INFO] Building SAMLProxy 0.0.1-SNAPSHOT
5630      [INFO] -----
5631      [INFO]
5632      [INFO] --- maven-resources-plugin:2.6:resources (default-resources) @ SAMLProxy
5633      ---
5634      [INFO] Using 'UTF-8' encoding to copy filtered resources.
5635      [INFO] Copying 9 resources
5636      [INFO]
5637      [INFO] --- maven-compiler-plugin:3.1:compile (default-compile) @ SAMLProxy ---
5638      [INFO] Nothing to compile - all classes are up to date
5639      [INFO]
5640      [INFO] --- maven-resources-plugin:2.6:testResources (default-testResources) @
5641      SAMLProxy ---
5642      [INFO] Using 'UTF-8' encoding to copy filtered resources.
5643      [INFO] skip non existing resourceDirectory
5644      /home/sjha/pdpPlugins/SAMLProxy/src/test/resources
5645      [INFO]
5646      [INFO] --- maven-compiler-plugin:3.1:testCompile (default-testCompile) @
5647      SAMLProxy ---
5648      [INFO] Nothing to compile - all classes are up to date
5649      [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 msecs]  
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/BVlkrCRgUykjbho=</ds:DigestValue>
5700       </ds:Reference>
5701     </ds:SignedInfo>
5702     <ds:SignatureValue>O8Gc8CSVKeYoNsR8bWaiExEpumeO2bLaMwlWC6LNaqf9ydvMPw/gcZbAEATCgK/RXVY
5703     gTe7ikYKKC80/GiO7NrUKZPO86ln5LlNX5Gw5iTOeb6S4zUTWEfp2PQTfMSTB6rZe5OBuUDEpWfJ4T/3E1KpI4
5704     H7sxoayhcZ3J2iilZxPheMEJ0l4zvicAzlsefiirftnlvWirOdjub9VE0SicCl11FJB13Wla+c8JA5Nbsnc3H6
5705     h5oDeapEOD9bX41KZtj2sGbh6k+F3vunYpd3m69KW6z8CJQeBWOCGmDtt4Dyf/avG6Iz7o0PYjPYxFIvwsLOY
5706     YU2QzLtOpHT8e/RRQ==</ds:SignatureValue>
5707   </ds:Signature>
5708   <ds:KeyInfo>
5709     <ds:KeyValue>
5710       <ds:RSAKeyValue>
5711         <ds:Modulus>uzxrl5iAIpNyEXHmGTDWlzmzX7YJal/c9Ruxag3sifjzuUdBjEznFJJxaagM2pzTUI5JCaLzgm7
5712         1V
5713         SBmuVL+6PzTxReM3i5XzWjpgRMIizadnQT0wmCryKuNaQiBIFLoMbi+ySdBvu+M/xhHlRxuFjY9N
5714         PSE1MHL8YaLoKW2SFIm/3bhJ/xF7q7FGHMcJH4Zzr2QpQmBEryozJJV3z4ZvVro/MfyLg1VER0pu
5715         36e32hIyZsf2gKizv00qY2ecDlBCNTITsA2HWSTf50kpvT4qupCnXVKVqzDPZON0XCsJJcwWsUi9
5716         pRvkGtVBXqhh2820Dyzcl3nkpGsl5F8hR7kOjQ==</ds:Modulus>
5717         <ds:Exponent>AQAB</ds:Exponent>

```

## SECOND DRAFT

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 uer>
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:osi
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](#).

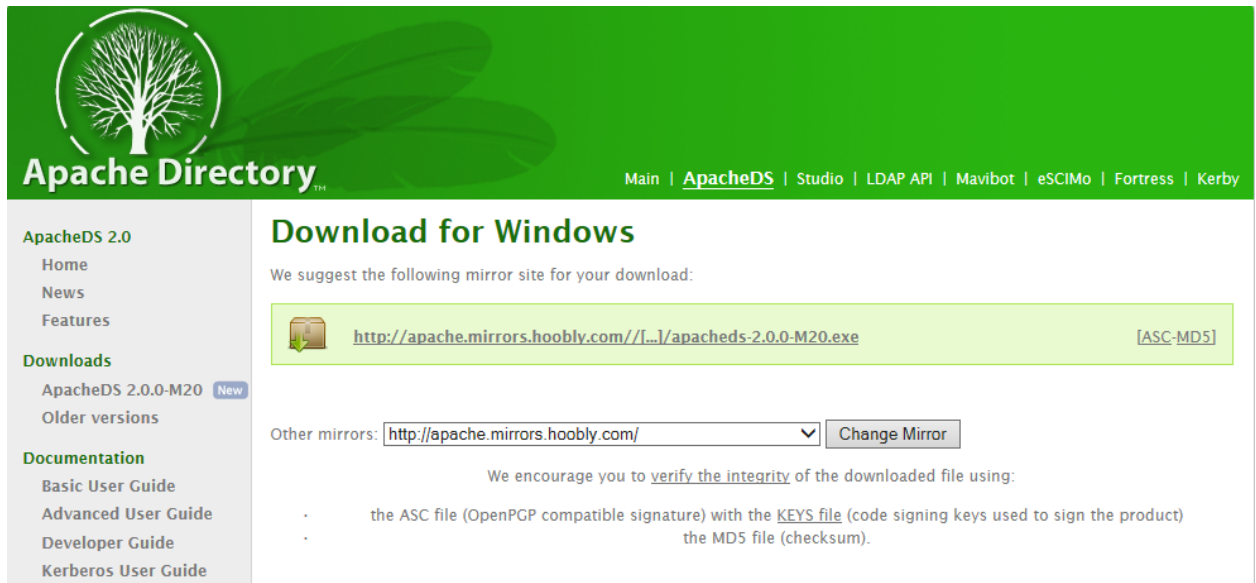
5797 In this project, ApacheDS was downloaded as a packaged Windows installer from this [location](#). Native  
 5798 installers are available in the following formats, and their download links are available at following [site](#).

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.

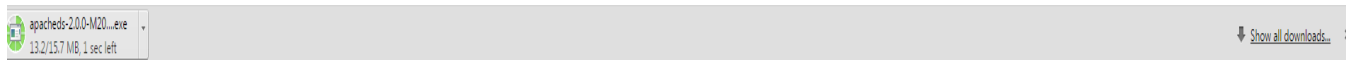
5802 **Figure 10-9 ApacheDS Download**



- 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):



### 5808 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 `$ gpgk -a KEYS`

5816 `$ gpgv apacheds-2.0.0-M20.exe.asc`

5817 or

5818 `$ gpg -ka KEYS`

5819 `$ gpg apacheds-2.0.0-M20.exe.asc`

5820 or

5821       \$ gpg --import KEYS

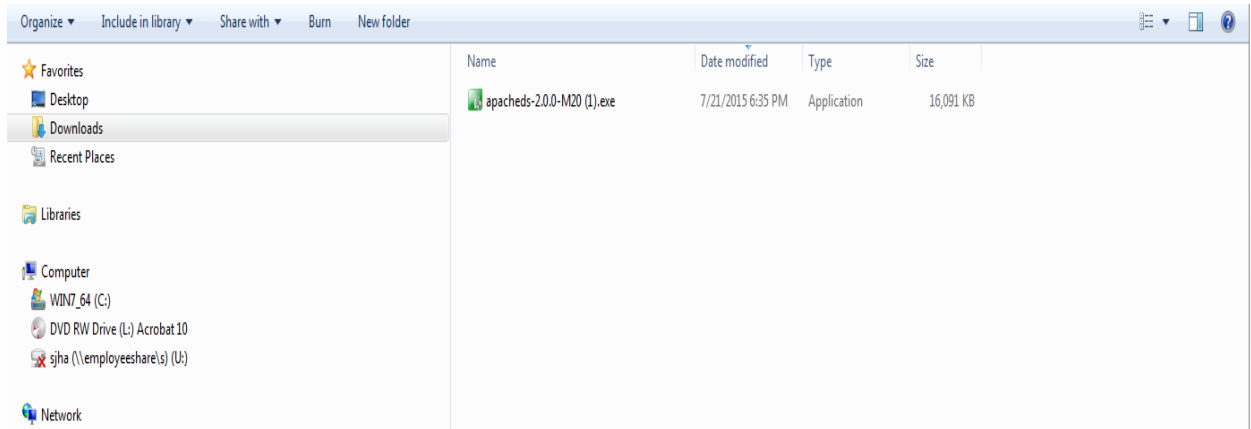
5822       \$ gpg --verify apacheds-2.0.0-M20.exe.asc

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.



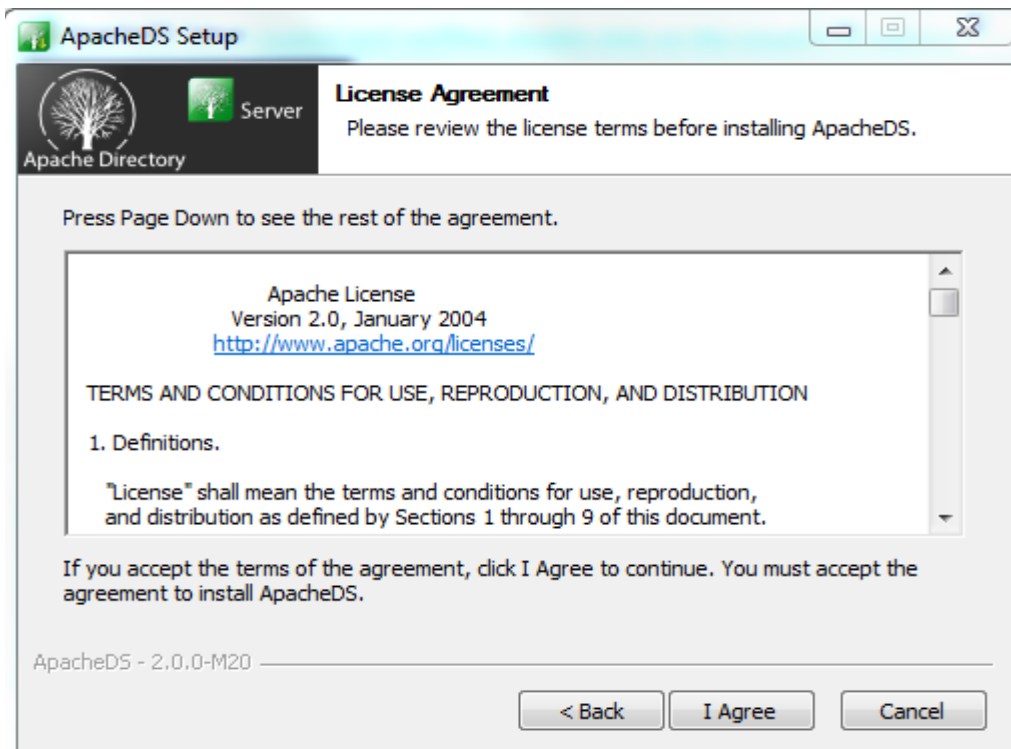
5832

- 5833       2. When the following screen appears, click **Next**.



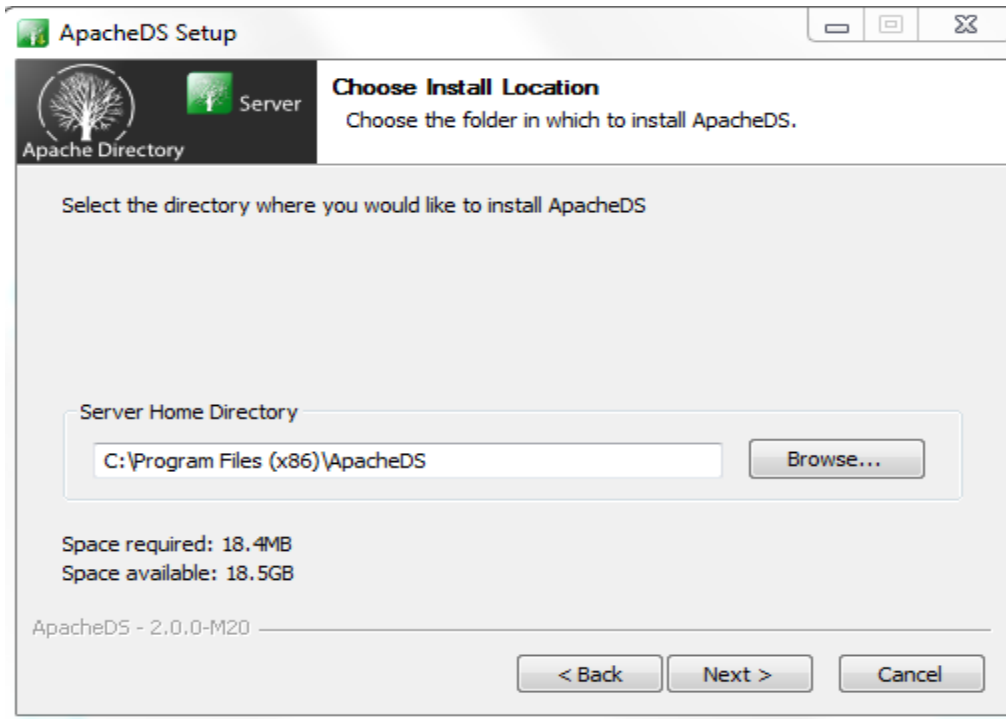
5834

5835 3. Review the License agreement and click **I Agree**.



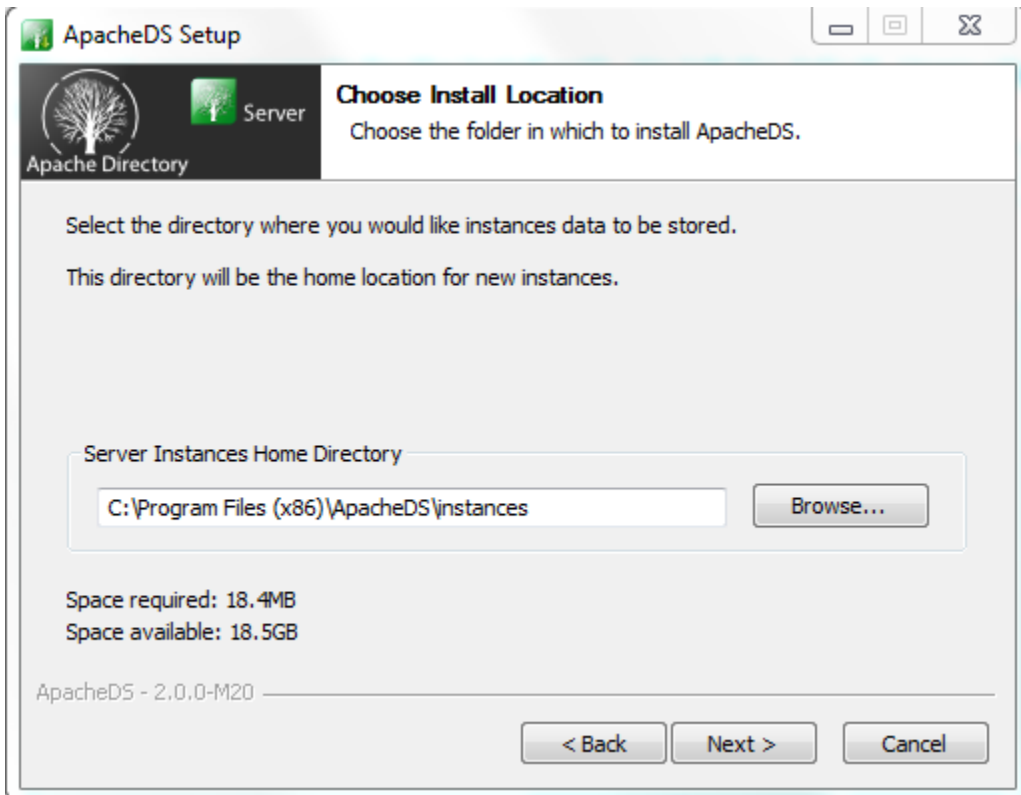
5836

- 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**.



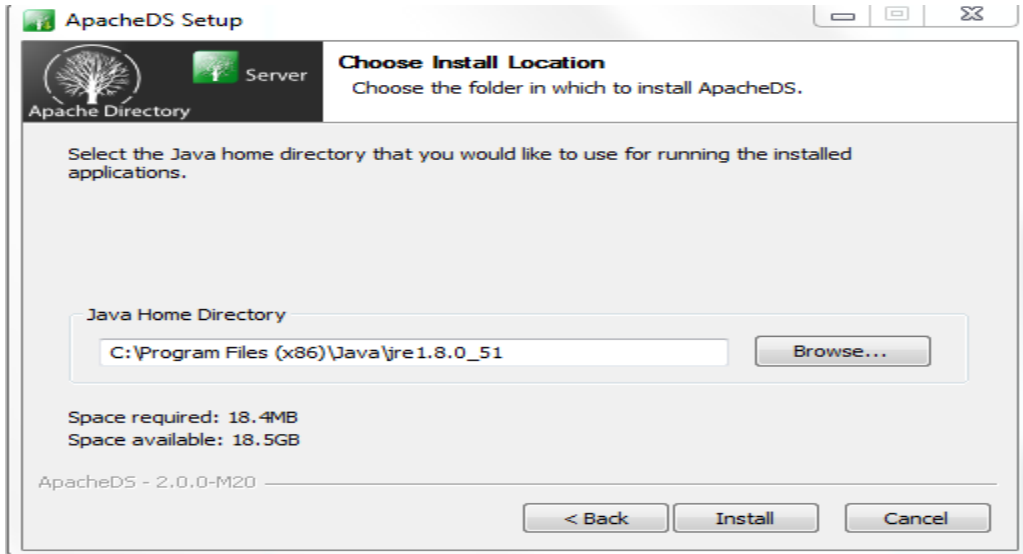
5839

- 5840 5. Specify a location for storing ApacheDS instances, then click **Next**.

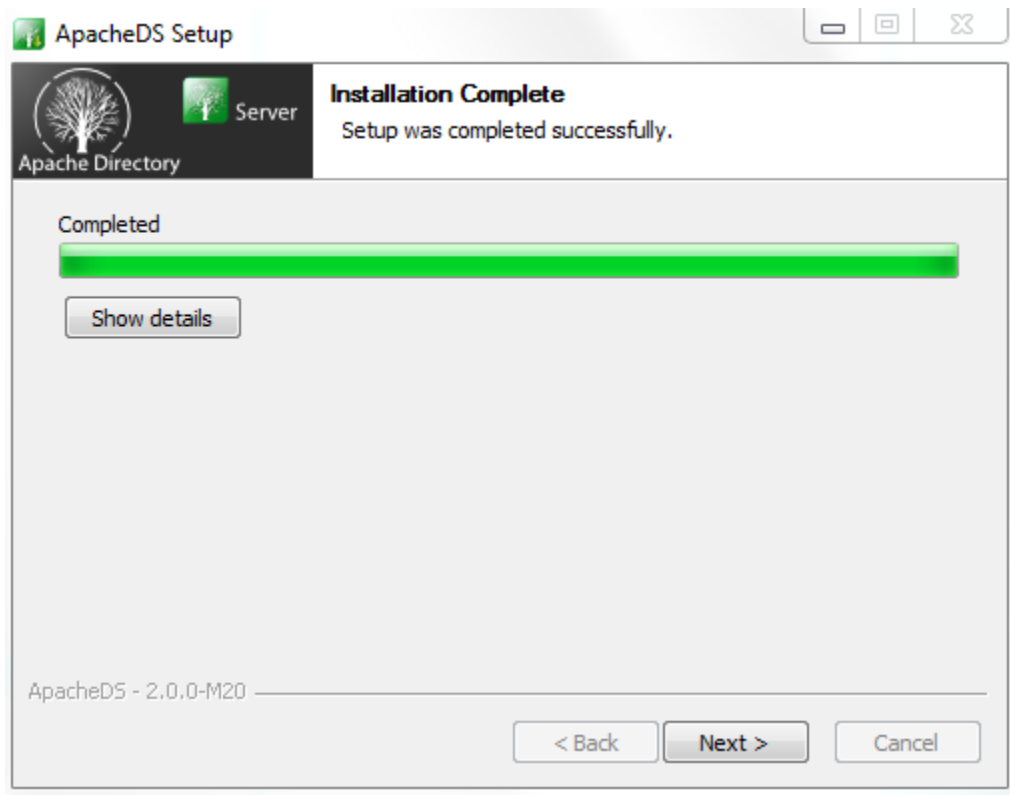


5841

- 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:

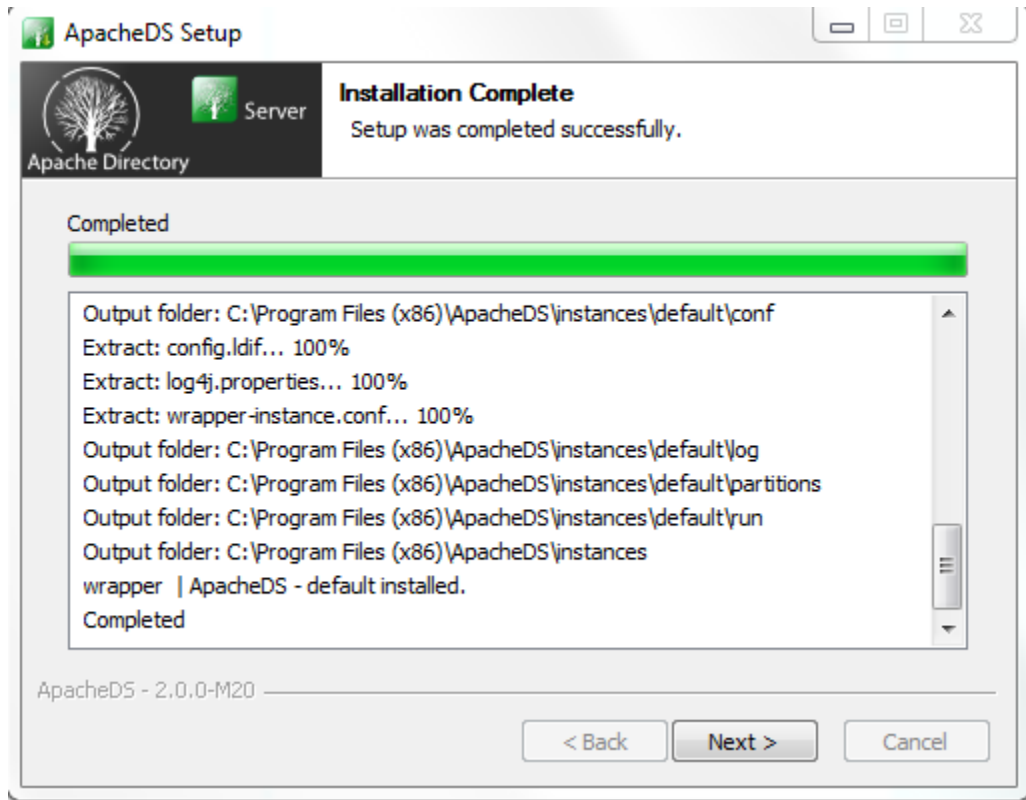


5849



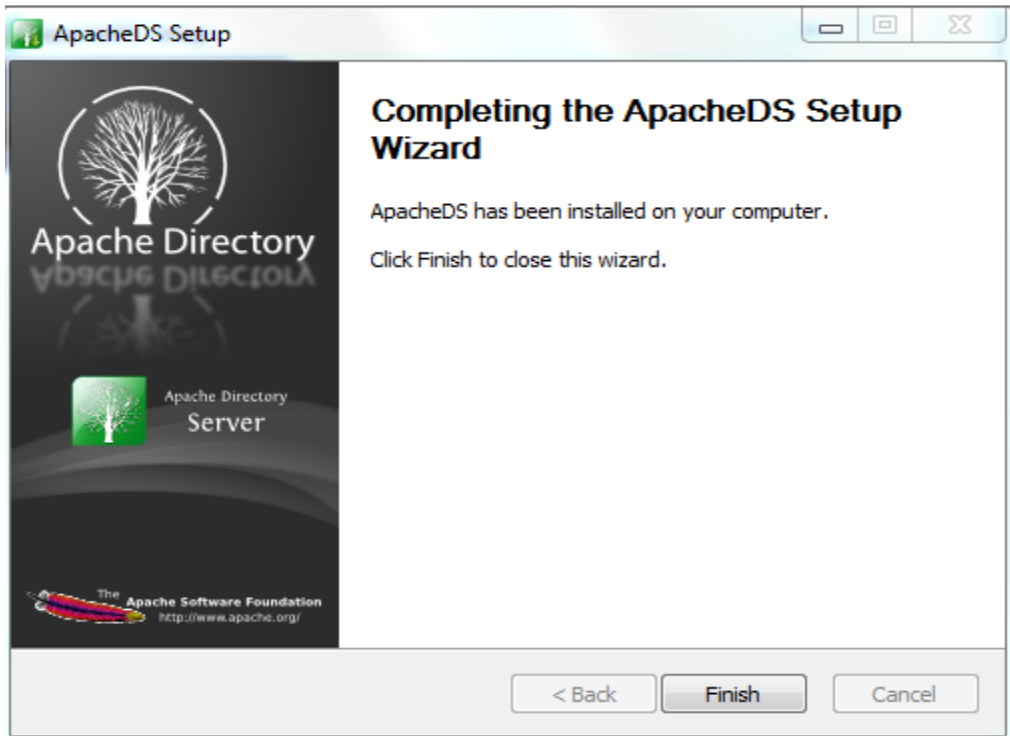
5850 *10.6.3.1 Functional Test of the ApacheDS Installation*

- 5851 1. Click **Show Details** in above diagram to see details of installation. Make sure all of the folders  
5852 exist, then click **Next**.



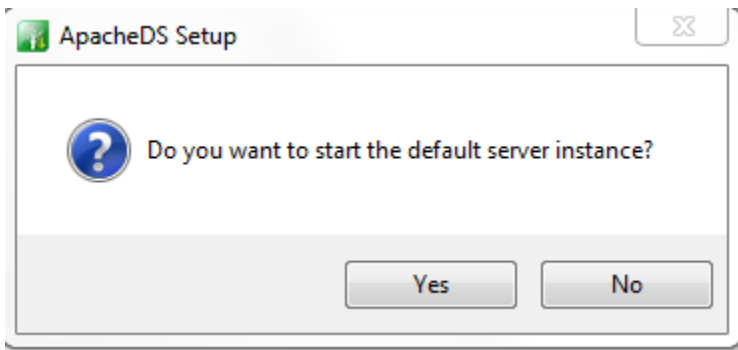
5853

- 5854 2. Click **Finish** to end the installation.



5855

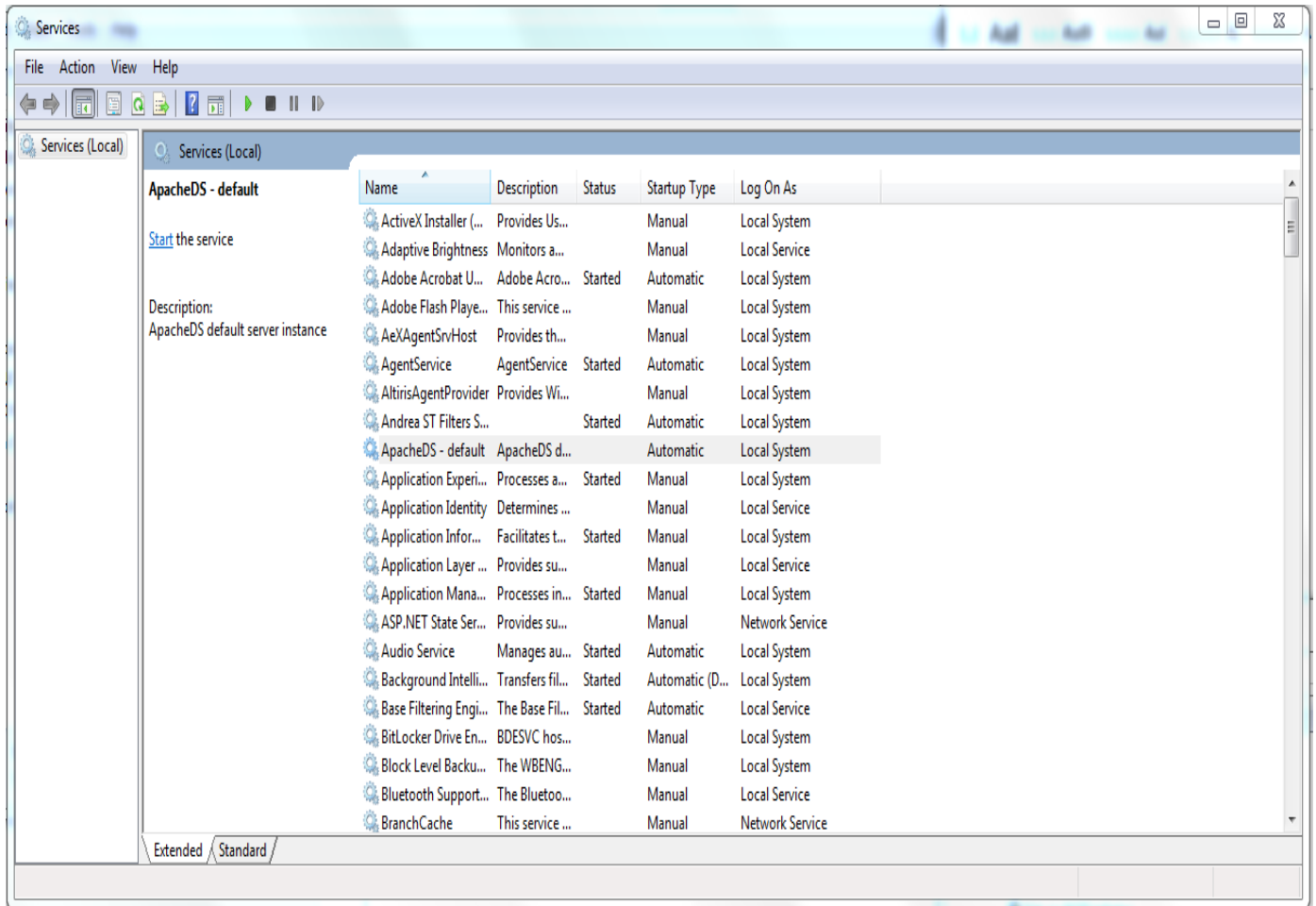
5856 3. Click **Yes** to start the ApacheDS server. Instructions are provided in [Section 10.6.2](#).



5857

### 5858 10.6.4 Starting and Stopping the Server

5859 The server can be started and stopped with the Windows Services manager (**Control Panel >**  
5860 **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](#).5864 

## 10.6.5 ApacheDS Configuration

5865 ApacheDS Server and Schema configuration details are provided [here](#).5866 

## 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

5871 

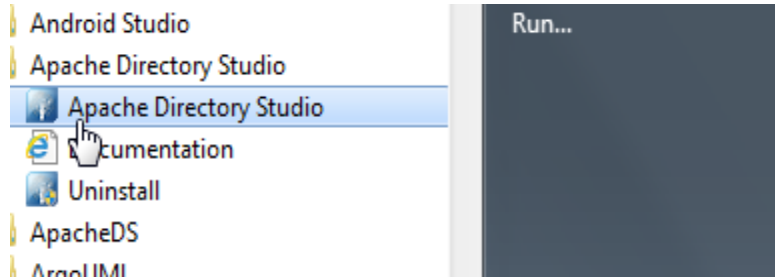
### 10.7.1 Provisioning of Server Credential

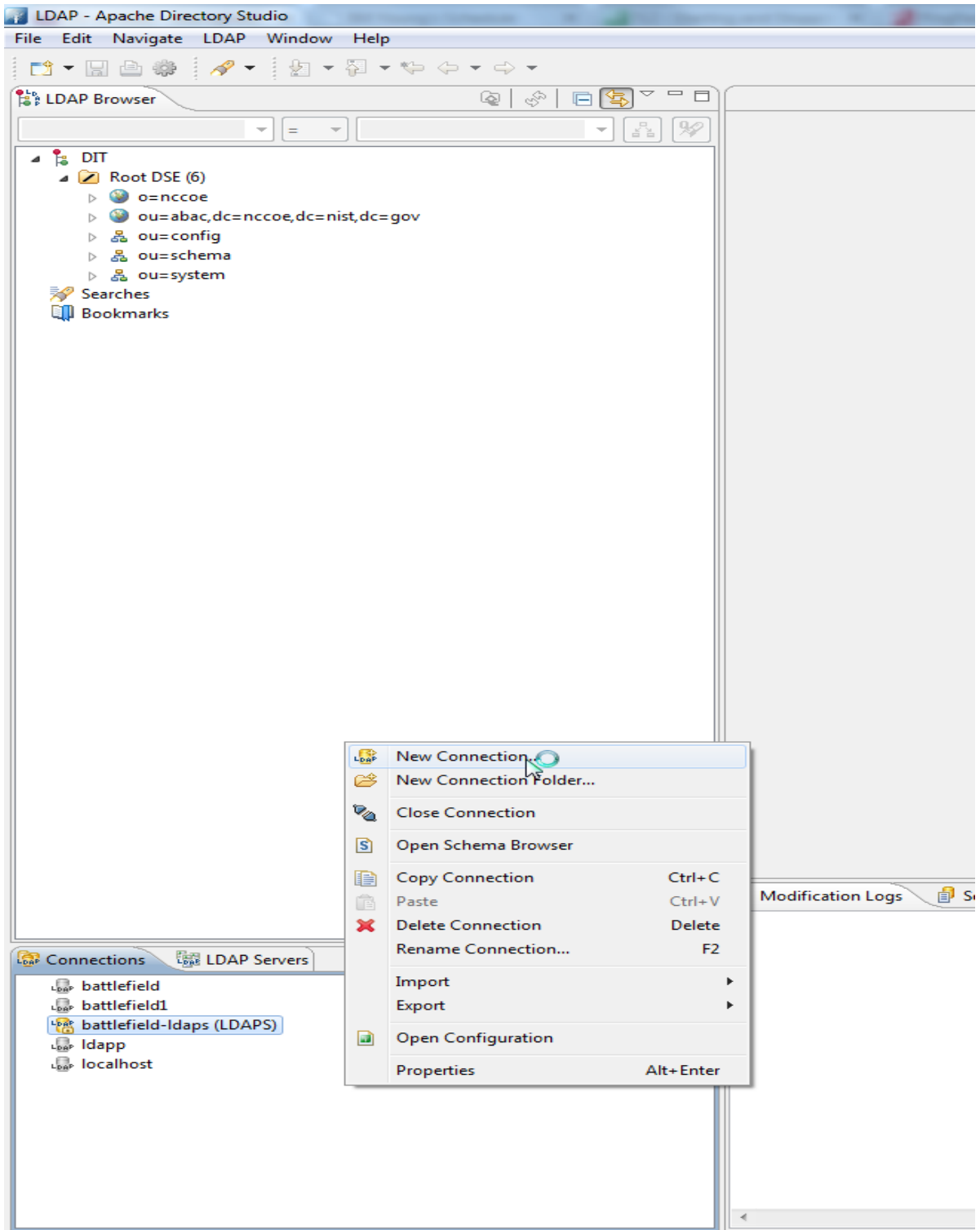
5872 Start Apache Directory Server Studio and open a new connection.

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





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**.

**New LDAP Connection**

**Network Parameter**  
Please enter connection name and network parameters.

Connection name: battlefield2

Network Parameter

Hostname: 10.33.7.8

Port: 10686

Encryption method: Use SSL encryption (ldaps://)

Server certificates for LDAP connections can be managed in the '[Certificate Validation](#)' preference page.

Provider: Apache Directory LDAP Client API

Check Network Parameter

Read-Only (prevents any add, delete, modify or rename operation)

< Back   **Next >**   Finish   Cancel

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

**New LDAP Connection**

**Authentication**  
Please select an authentication method and input authentication data.

Authentication Method: Simple Authentication

Authentication Parameter:  
Bind DN or user: uid=admin,ou=system  
Bind password: ●●●●●●  
 Save password Check Authentication

▼ **SASL Settings**  
SASL Realm:   
Quality of Protection: Authentication only  
Protection Strength: High  
 Mutual Authentication

▼ **Kerberos Settings**  
Kerberos Credential Configuration

? < Back Next > Finish Cancel

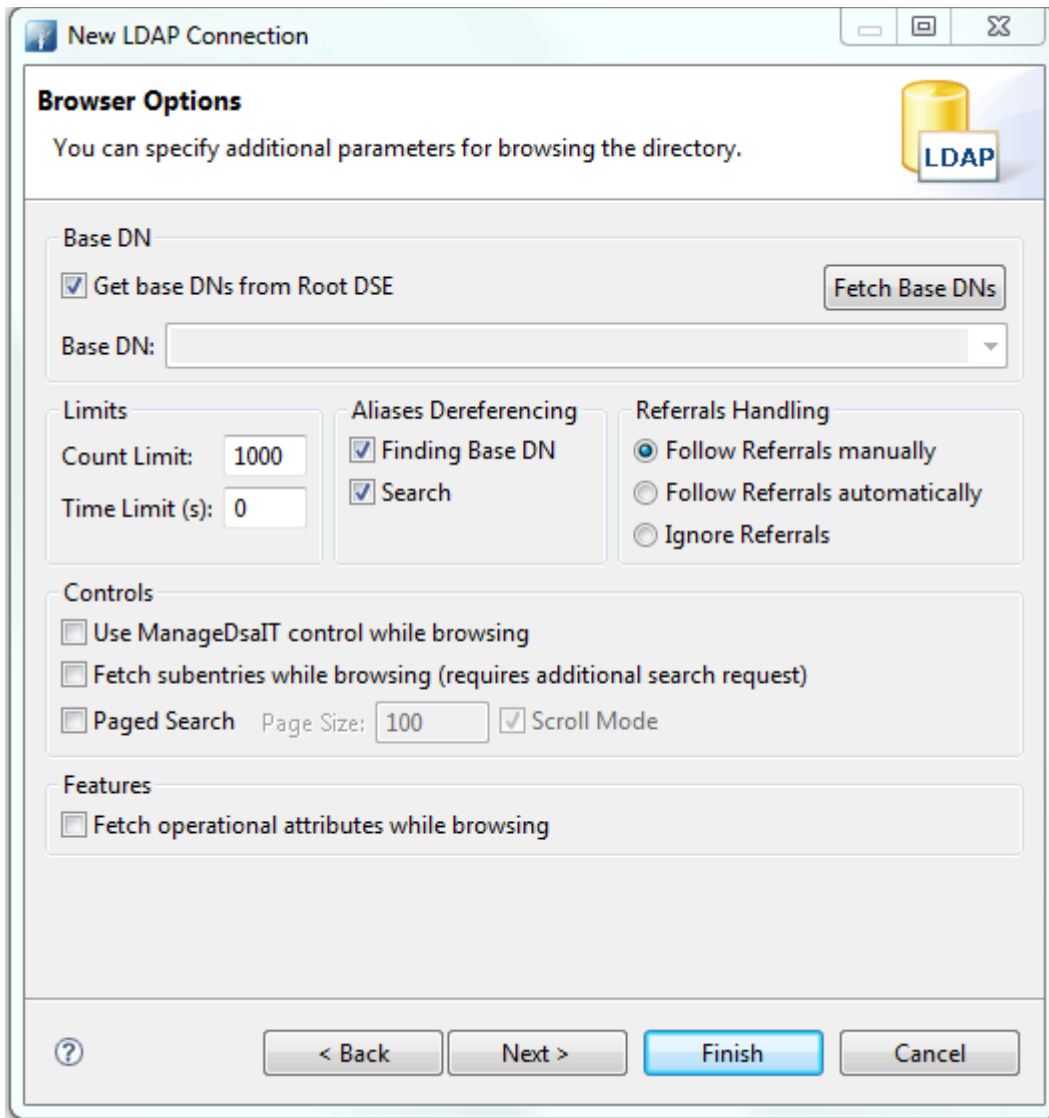
5885



Option	Description	Default
Authentication Method	Select your authentication method: <ul style="list-style-type: none"> <li>• Anonymous Authentication: connects to the directory without authentication.</li> <li>• Simple Authentication: uses simple authentication using a bind DN and password. The credentials are transmitted in clear-text over the network.</li> <li>• CRAM-MD5 (SASL): authenticates to the directory using a challenge-response authentication mechanism. The credentials are not transmitted in clear-text over the network.</li> <li>• DIGEST-MD5 (SASL): another challenge-response authentication mechanism. Additionally, you could define your realm and QoP parameters.</li> <li>• GSSAPI (Kerberos): user Kerberos-based authentication. Additional parameters can be defined.</li> </ul>	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.



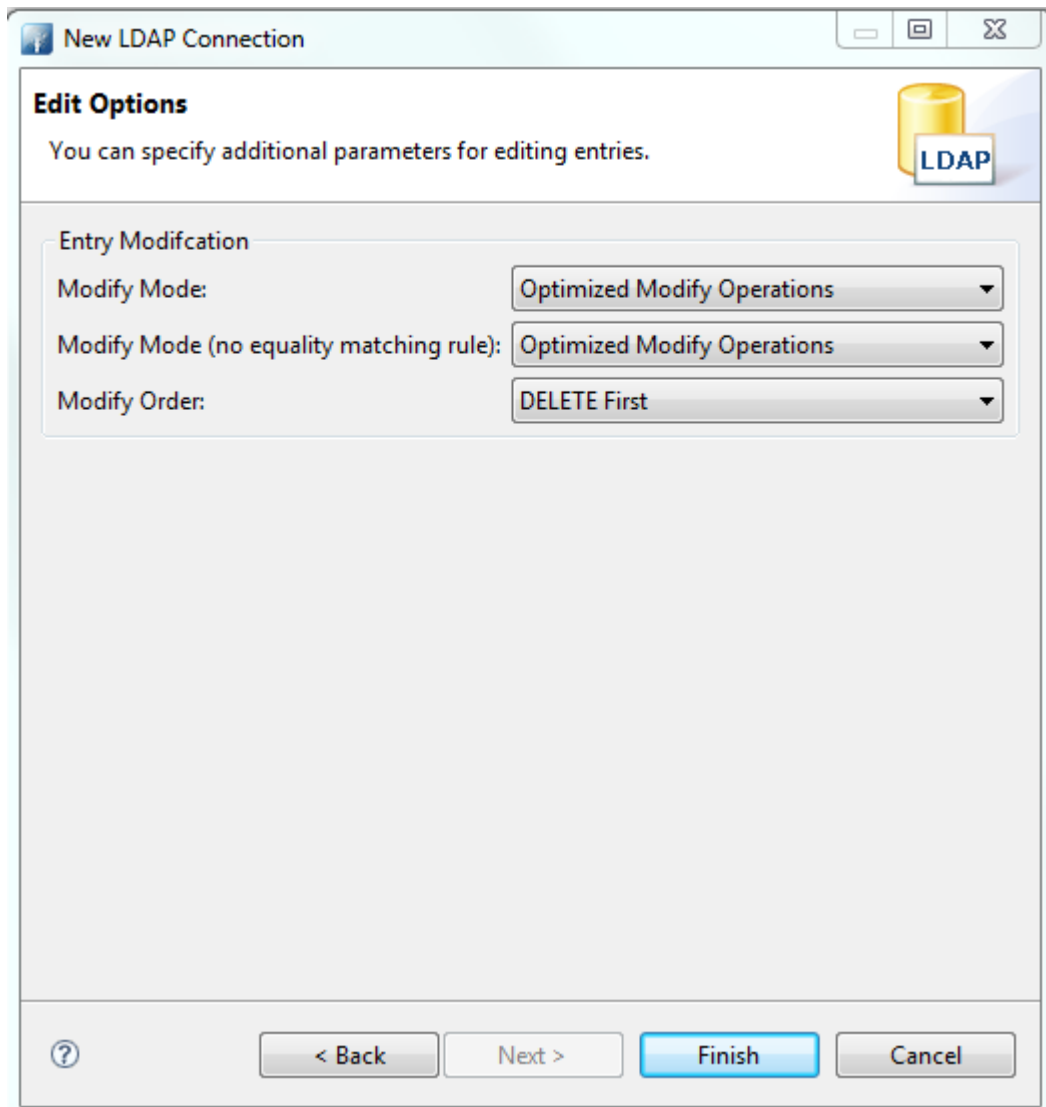
5887

Option	Description	Default
Get base DN from Root DSE	If checked, the base DN are fetched from the namingContexts attribute of the Root DSE.	checked
Fetch Base DN	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 <b>Get base DN from root DSE</b> 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"> <li>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.</li> <li>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.</li> <li>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.</li> </ul>	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 <b>next page</b> and <b>top page</b> . 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 <b>All Operational Attributes</b> , use + to retrieve operational attributes. Otherwise, all operational attributes defined in the schema are requested.	unchecked

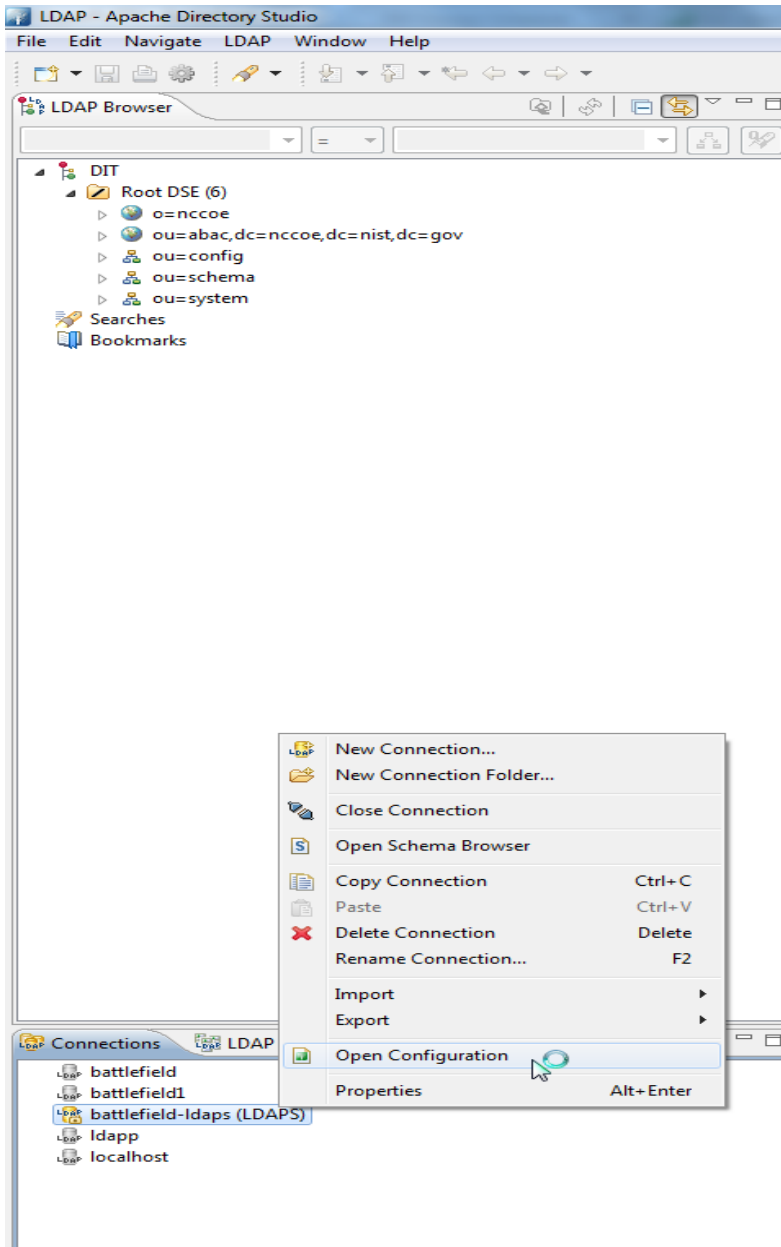
5888



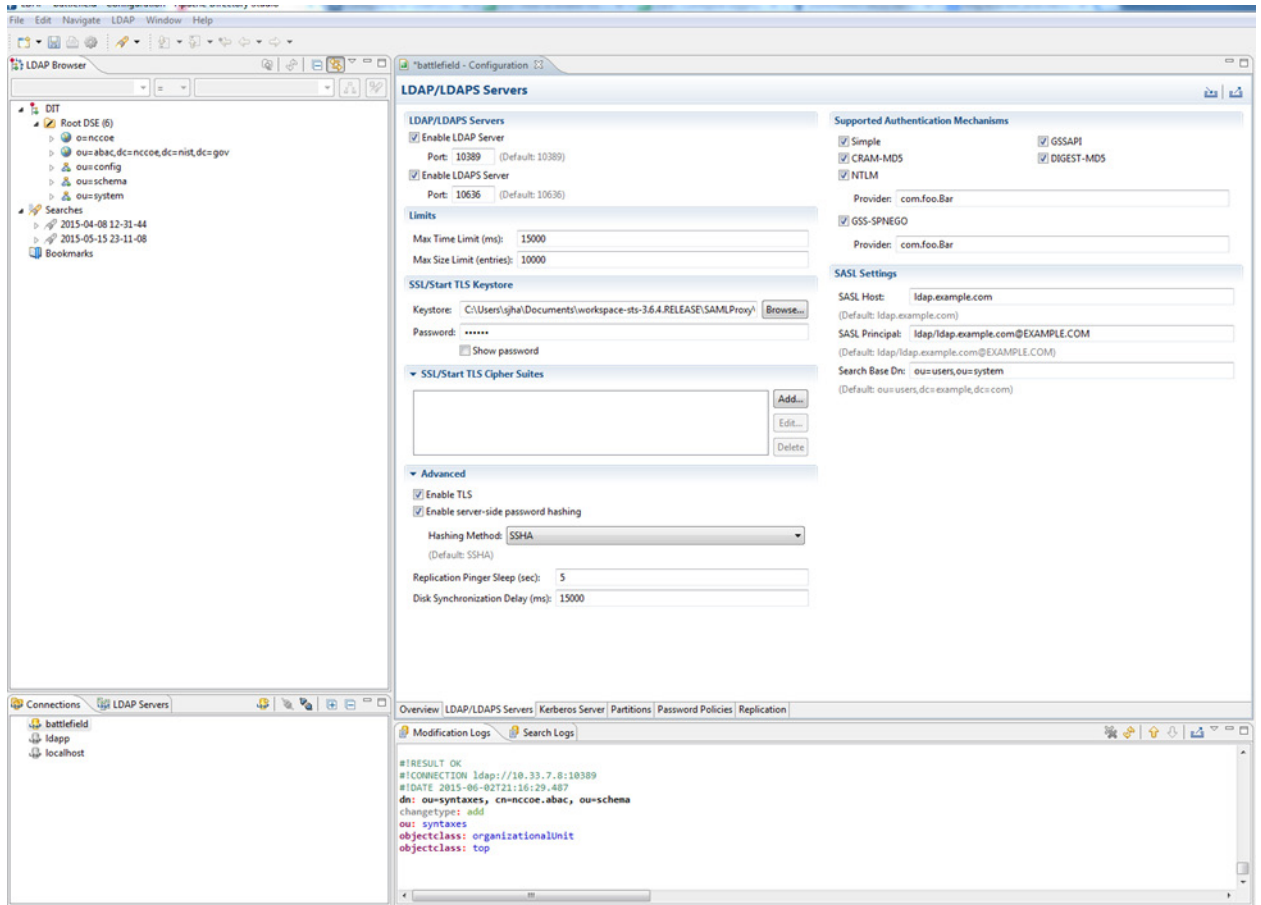
5889

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"> <li>• Optimized Modify Operations: uses add/delete by default, uses replace if operation count is less</li> <li>• Always REPLACE: always uses replace operations to perform entry modifications</li> <li>• Always ADD/DELETE: always uses add and/or delete operations to perform entry modifications</li> </ul>	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"> <li>• Optimized Modify Operations: uses add/delete by default, uses replace if operation count is less</li> <li>• Always REPLACE: always uses replace operations to perform entry modifications</li> <li>• Always ADD/DELETE: always uses add and/or delete operations to perform entry modifications</li> </ul> <p>Recommended values for various LDAP servers:</p> <ul style="list-style-type: none"> <li>• ApacheDS: Optimized Modify Operations or REPLACE</li> <li>• OpenLDAP: REPLACE</li> <li>• OpenDS / SunDSEE: Optimized Modify Operations or REPLACE</li> <li>• FedoraDS / 389DS: Optimized Modify Operations (missing equality matching rules for many standard attribute types)</li> <li>• Active Directory: Optimized Modify Operations (exposes no equality matching rules at all)</li> <li>• eDirectory: Optimized Modify Operations (exposes no equality matching rules at all)</li> </ul>	Optimized Modify Operations
Modify Order	Specify the modify order when using add and delete operations.	Delete first

- 5890      3. Go to **Open Configuration** for the newly created connection.



5891



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 MIIBjDCCATYCBgFMLE24DANBgkqhkiG9w0BAQUFADBCMqswCQYDVQQGEwJVUzEM
```

```
5917 MAoGA1UEChMDQVNGMREIWEAYDVQQLEwEaXJlY3RvcnkxETAPBgNVBAMTCEFwYWNo
```

```
5918 ZURTMb4XDTE1MDQwNzE1NDgwN1oXDTE2MDQwNjE1NDgwN1owWzELMAkGA1UEBhMC
```

```
5919 VVMxDDAKBgNVBAoTAA0FTRjESMBAGA1UECXMJRGl5ZWNOb3J5MSowKAYDVQQDEyFi
```

```
5920 YXR0bGVmaWVsZC5iYi1hYmFjLWJiMS5uY2NvZS5sYWlwdANBgkqhkiG9w0BAQEF
```

```
5921 AANLADBIAkeA1LYJY8PJgMS82IqrW4uTVobkNqi2oJBoFAvOGMF7olPCQ4x5vrgS
```

```
5922 6GEq9gUHk1ZZzymIIq6BMxoEb80161PY/wIDAQAABMA0GCSqGSIb3DQEBBQUAA0EA
```

```
5923 hXNpaGfF2Aboemwzt6U/fvSNy1+KRdeKfM0liWbseBk8OPvdOEmW96HVLv1bxSlc
```

```
5924 JpSznkLFhFOe0fimwB6GEg==
```

```
5925 -----END CERTIFICATE-----
```

5926 1. Verify the **certificate** received from the directory server against the certificate that was loaded  
5927 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
0130DB8CD483	CN=localhost, O=Quick Start App, C=US	Fri Jun 05 09:18:17 EDT 2111	RSA 1024	Valid	Export Delete
44DC: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
0130DB8C25A8	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
014C949136E0	CN=battlefield bb-abac-bb1.ncooe.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.abactest, O=NCCoE, C=US	Wed Apr 20 11:07:58 EDT 2016	RSA 2048	Valid	Export Delete

Import...

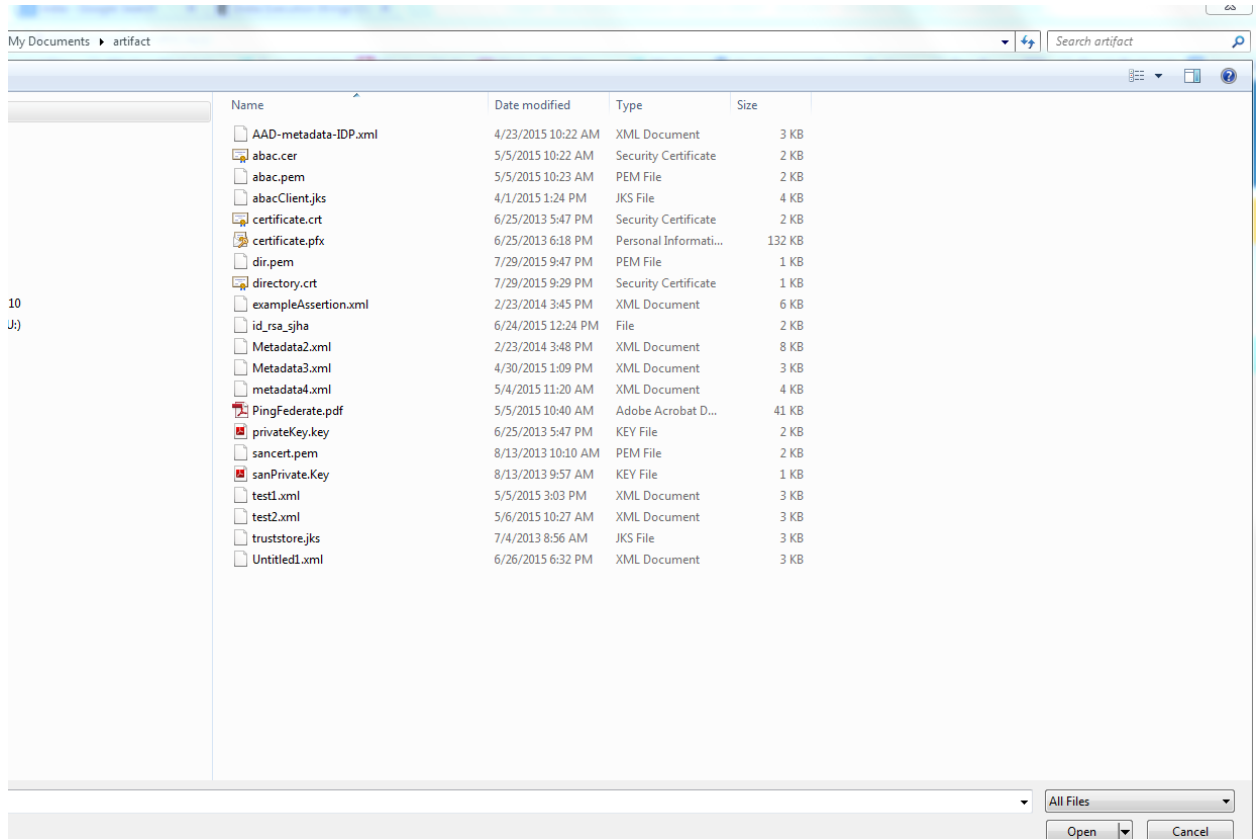
- 5931
- 5932 2. **Select Import Certificate.**

Import Certificate Summary

Please select the file containing the desired certificate.

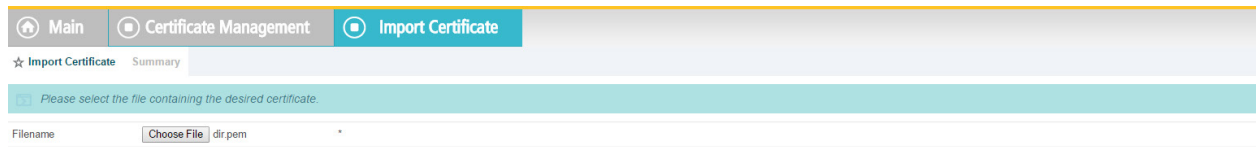
Filename  No file chosen \*

- 5933
- 5934 3. **Choose** a file to import.



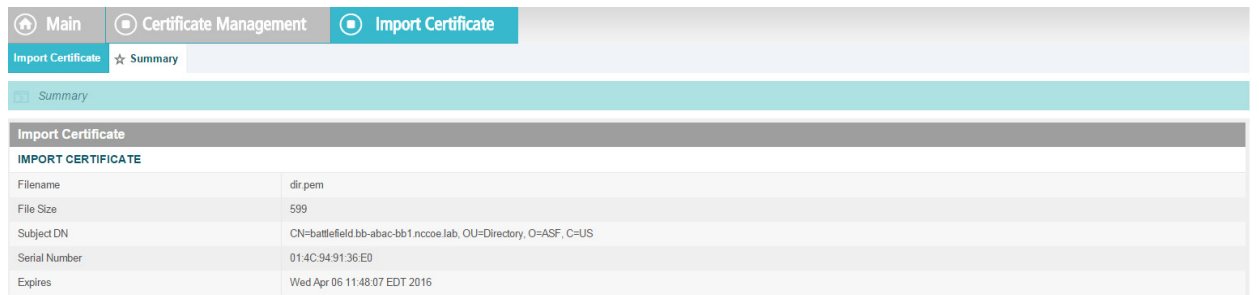
5935

5936 4. **Once** your chosen file appears in the **Filename** field, click **Next**.



5937

5938 5. **View** the **Summary** of the imported certificate.



5939

5940 6. **Click Done**. The main screen will display a list of certificates. Click **Save**.

Home **Certificate Management**

★ Manage Trusted CAs

*You can import your partner's CA or self-signed SSL server certificates into this server's global trust list.*

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTION
0130DB8C:D483	CN=localhost, O=Quick Start App, C=US	Fri Jun 05 09:18:17 EDT 2111	RSA 1024	Valid	<a href="#">Export</a> <a href="#">Delete</a>
44DC: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	<a href="#">Export</a> <a href="#">Delete</a>
0130DB8C:25AB	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	<a href="#">Export</a> <a href="#">Delete</a>
014CDC85:7F:1F	CN=idp.abac.test, O=NCCoE, C=US	Wed Apr 20 11:07:58 EDT 2016	RSA 2048	Valid	<a href="#">Export</a> <a href="#">Delete</a>
014C9491:36: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	<a href="#">Export</a> <a href="#">Delete</a>

[Import...](#)

5941

5942 **10.7.1.3.1 Creation of Data Store to Connect to ApacheDS**

**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

5943

5944 **7. Click on Data Stores.**

Home **Manage Data Stores**

★ Manage Data Stores

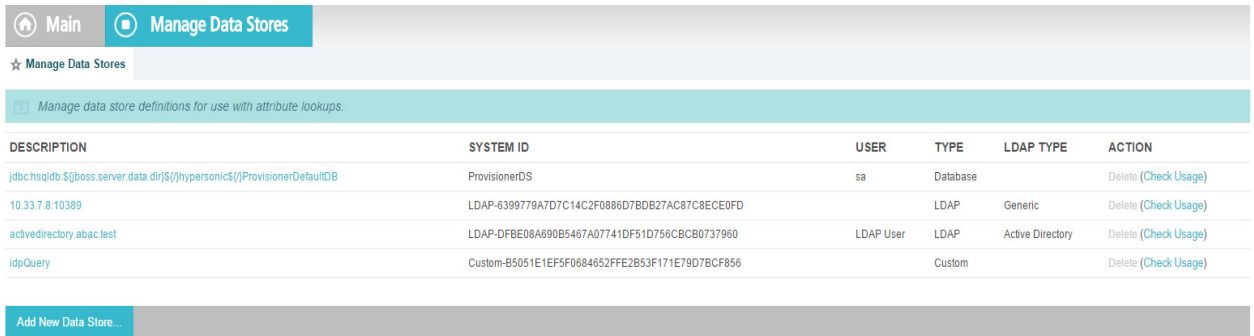
*Manage data store definitions for use with attribute lookups.*

DESCRIPTION	SYSTEM ID	USER	TYPE	LDAP TYPE	ACTION
jdbc:hsqldb:/\${boss.server.data.dir}/\${hyPERSONIC\$/ProvisionerDefaultDB	ProvisionerDS	sa	Database		<a href="#">Delete (Check Usage)</a>
<b>10.33.7.8.10389</b>	LDAP-6399778A7D7C14C2F0886D7BDB27AC87C8ECE0FD		LDAP	Generic	<a href="#">Delete (Check Usage)</a>
activedirectory.abac.test	LDAP-DFBE08A690B5467A07741DF51D756CBCB0737960	LDAP User	LDAP	Active Directory	<a href="#">Delete (Check Usage)</a>
idpQuery	Custom-B5051E1EF5F0684652FFE2B53F171E79D7BCF856		Custom		<a href="#">Delete (Check Usage)</a>

[Add New Data Store...](#)

5945

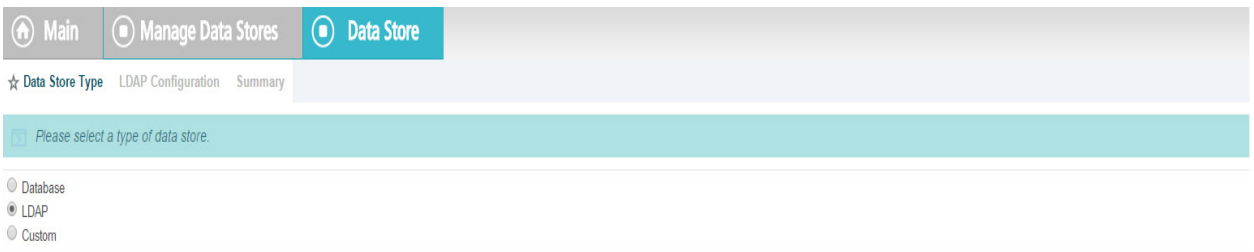
5946 **8. In the Manage Data Stores window, click Add New Data Store.**



5947

5948

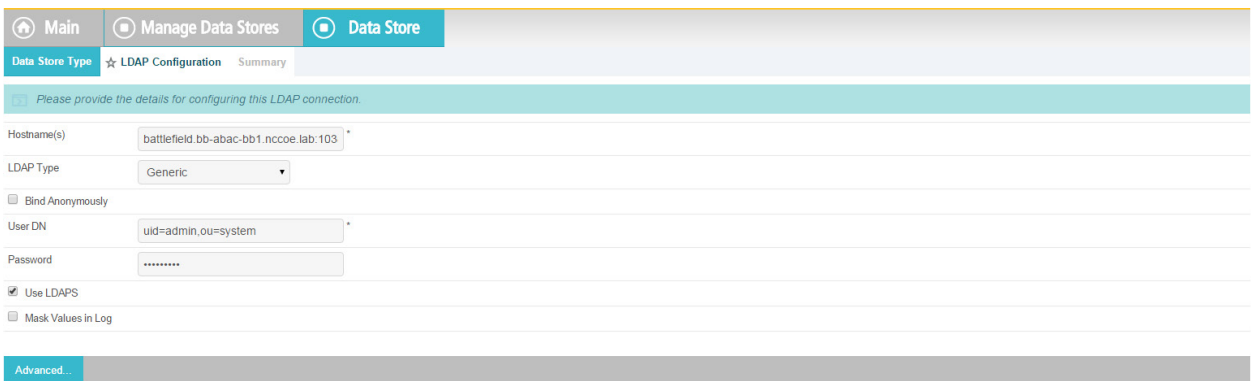
9. Choose LDAP, and click Next.



5949

5950

10. Provide a Hostname and Ldaptype.



5951

5952

5953

5954

11. It may be necessary to configure connection pooling. It is important to select **Verify LDAPS Hostname** if the directory server certificate is bound to a hostname, and this hostname can be verified.

5955

5956 12. If there is any binary data, enter it in the **Binary Attribute Name** Field, and click **Add**.

5957

5958 13. A **summary** of the LDAP configuration will appear.

5959

5960 14. A **Summary** of the **connection** will appear as following. Click **Save**. You will then return to the  
5961 Main Admin console.

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:

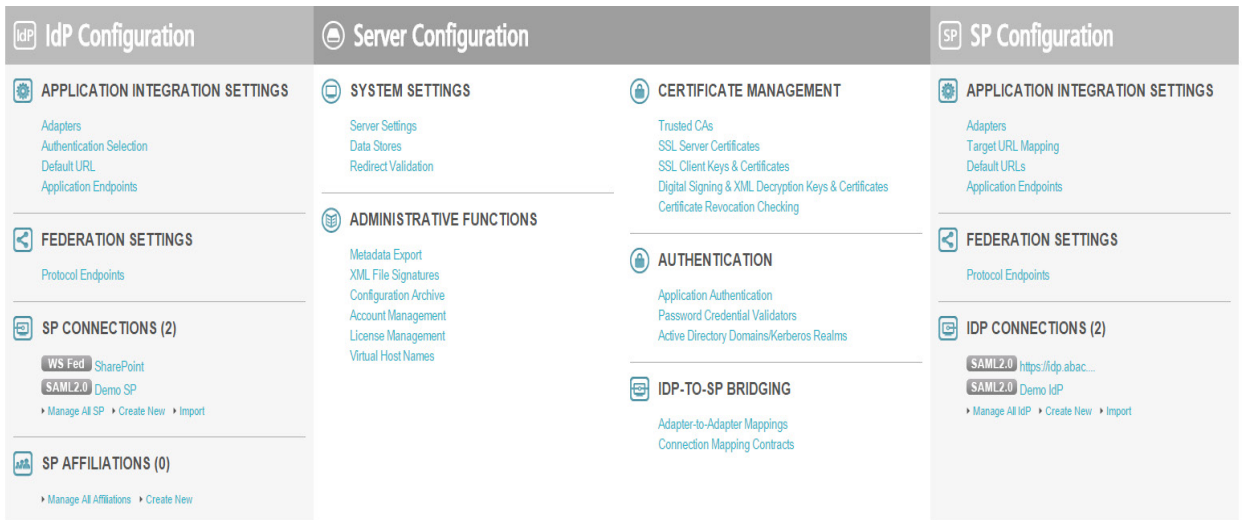
- 5996 ■ Specification of connection and associated security protocol (i.e., TLS/SSL)
- 5997 ■ Specification of SAML profile t including detailed security specifications (the use of digital  
5998 signatures, signature verification, XML encryption)

- 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

6002      10.8.2.1.1 Specification of Profile

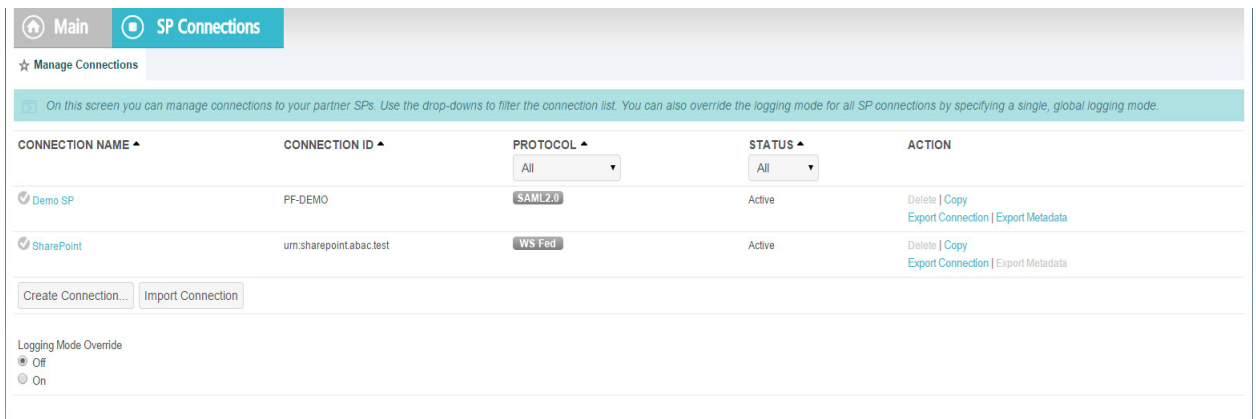
6003      Instructions on how to create a new connection can be found [here](#).

- 6004      1. Click on **Manage on All SP** in the first column on the left hand side.



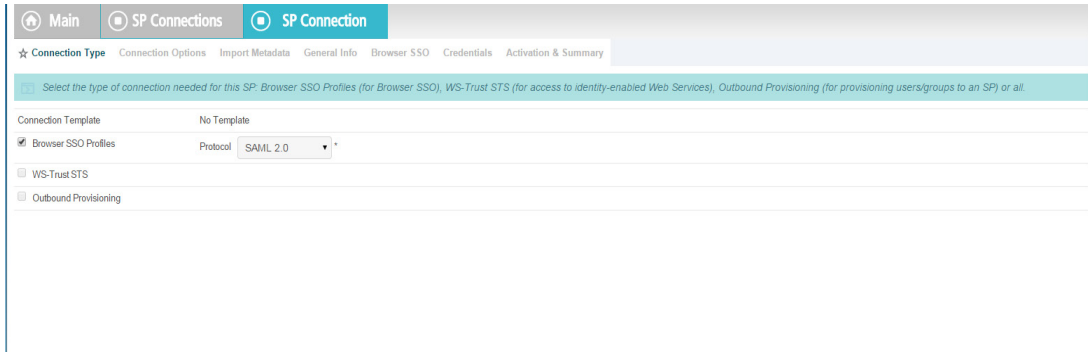
6005

- 6006      2. The following screen will appear. Click on **Create Connection**.



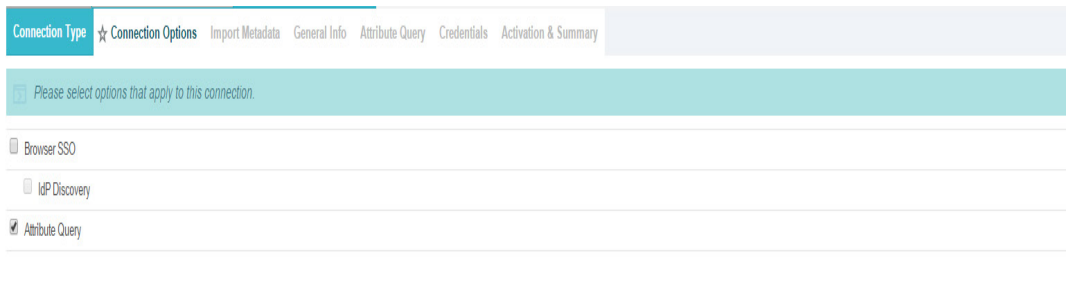
6007

- 6008      3. Check the box for **Browser SSO Profiles** and select **SAML 2.0** as protocol from the drop-down
- 6009      menu.



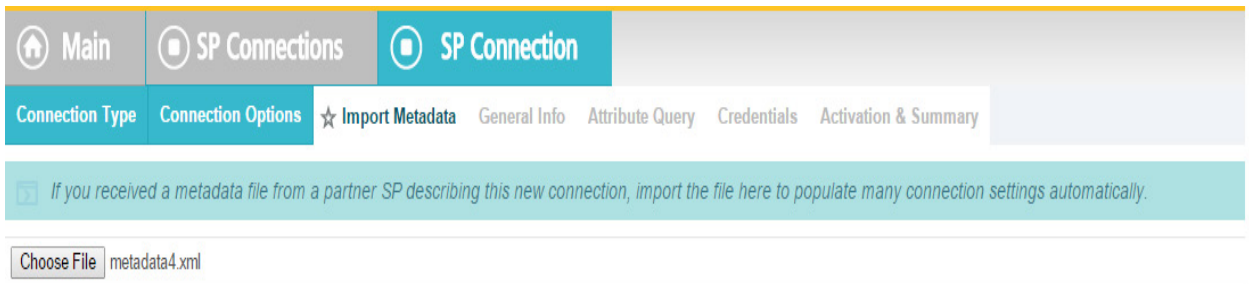
6010

6011 4. Uncheck **Browser SSO**, check **Attribute Query**, and click **Next**.



6012

6013 5. Choose a metadata file and click **Next**.



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

```
MIIE4jCCAsqgAwIBAgICEAMwDQYJKoZIhvcNAQELBQAwYjELMAkGA1UEBhMCVVMx
```

6025

```
ETAPBgNVBAGMCE1hcmlsYW5kMRItwEAYDVQQHDA1Sb2Nrdm1sbGUxDjAMBgNVBAoM
```

6026

```
BU5DQ29FMQ0wCwYDVQQLDARBRQkFDMDQ0wCwYDVQQDDARBRQkFDMB4XDTE1MDQwMTE4
```

6027

```
MTA1N1oXDTE2MDMzMTE4MTA1N1owejELMAkGA1UEBhMCVVMxETAPBgNVBAGMCE1h
```



6028 cnlsYW5kMQ4wDAYDVQKDAVOQ0NvRTENMASGA1UECwwEQUJBQzEUMBIGA1UEAwWL  
6029 TU0xOTU1OTItUEMxIzAhBgkqhkiG9w0BCQEFHnqaGFATU0xOTU1OTItUEMub3Jn  
6030 MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEaUzxrL5iAIpNyEXHmGTDW  
6031 1mzx7YJal/c9Ruxag3sifjzuUdBjEznFJJxaagM2pzTUI5JCaLzgm71VSBmuVL+6  
6032 PzTxReM3i5XzWjjpgRMIizadnQT0wmCryKuNaQiBIFLoMbi+ySdBvu+M/xhHlRxF  
6033 jY9NPSE1MHL8YaLoKW2SFIm/3bhJ/xF7q7FGHMcJH4Zzr2QpQmBEryozJJV3z4Zv  
6034 Vro/MfyLg1VER0pu36e32hIyzsf2gKizv00qY2ecDlBCNTITsA2HWSTf50kpvT4q  
6035 upCnXVKVqzDPZON0XCsJJcwWsUi9pRvkGtVBXqhh282ODyzcl3nkpgs15F8h7k0  
6036 jQIDAQABo4GJMIGMAkGA1UdEwQCAAwCwYDVR0PBAQDAgXgMCwGCWCGSAGG+EIB  
6037 DQQFfh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQURPRr  
6038 8BNghnDip40B1sy6AWpWJmcwHwYDVR0jBBgwFoAUyZ5WFPtCW/BOjVxvof8eNcBo  
6039 5c8wDQYJKoZIhvcNAQELBQADggIBAGhVMd47uFNi1z8oEYgwDInZDatfujvkftu2  
6040 Dtr7dvkvB2x6uW481ffIKDKb48yKVBM00kSwU4esPHgMMowJJs37Xfo9PYJ1kaE/  
6041 NCD7e8V4p3xhzXux6JqKpaho1xHifzEsdKqOyNj00ZXqmRMstbw6UC+IFCNUWJZQ  
6042 zJ+Dwciaxa9kq/huv8BMbYzcl8r1fE3x9nUwwwuFuXudpnED0B+Rmmod1G5fVG1j  
6043 agMWakXscGJ9rpT8wgfJGjU4Sct3Eocp5roRGopUVBrW6j1jZD4dYEu1eJ1LJqcW  
6044 mDiYdZIvu0z393HApNpwC4XSaMoTN7xq4Z+Xwe0zdt1HVM0aeAiglrDB3XKuiYQT  
6045 Ab899WBgK/TixTLJ+Nf6FkAl2apkVkaaxl+35DZrkDOHo3HQTORQFNyCb1LlrsfP  
6046 A5r0PPVi6XE6h4k9/Cg003Q6fzpgl7avCw8s1m/WnmQjfc0K+op7l7zsYrnsxB  
6047 wQsnaT6GX2csy99jOpfLk1Sh6jaIuFdRPMewjhNyqTy2xoLfuYK5bxMzlpfaoZEs  
6048 sVURPCFiC0G97xn8ffjjhv5Kby8JIRWV2QhXicf5FswoiWZIHtHo0L9WEQXKPT01  
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.

Home **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

6056

Home **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)  \*

Connection Name  \*

Virtual Server IDs  Add

Base URL

Company

Contact Name

Contact Number

Contact Email

Application Name

Application Icon URL

Logging Mode
 

- None
- Standard
- Enhanced
- Full

6057

6058

8. Click on **Configure Attribute Query Profile**.

6059

6060

- Specify the list of attributes that may be returned to the SP in response to an attribute request.

RETRIEVABLE ATTRIBUTES	ACTION
clearance	Edit / Delete
division	Edit / Delete
employer	Edit / Delete
fullname	Edit / Delete
role	Edit / Delete
stafflevel	Edit / Delete
username	Add

6061

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 navigation tabs include 'Main', 'SP Connection', and 'Attribute Query'. The current page is 'Attribute Sources & User Lookup', with sub-tabs for 'Data Store', 'LDAP Directory Search', 'LDAP Filter', and 'Summary'. A message states: 'This server uses local data stores to retrieve user attributes in response to an attribute request.' The configuration fields are as follows:

- 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

A 'Manage Data Stores...' button is visible at the bottom.

6064

6065 2. Specify **Attributes** for the JIT Cache.

The screenshot shows the 'LDAP Directory Search' sub-tab of the 'Attribute Sources & User Lookup' configuration page. A message states: 'Please configure your directory search. This information will be used to fulfill the attributes in the Retrievable Attributes list.' The configuration fields are as follows:

- Base DN: ou=users,ou=system
- Search Scope: Subtree

Attributes to return from search:

ROOT OBJECT CLASS	ATTRIBUTE	ACTION
	Subject DN	
	employeeType	Remove

Below the table, there are two dropdown menus: '<Show All Attributes>' and 'givenName'. An 'Add Attribute' button is also present.

6066

6067 3. Specify **LDAP Filter**.

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.

Filter

uid=\${SAML\_SUBJECT}

[View List of Available LDAP Attributes](#)

6068

6069

4. Verify that your data is correct.

Attribute Source Summary

**Attribute Sources & User Lookup**

**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

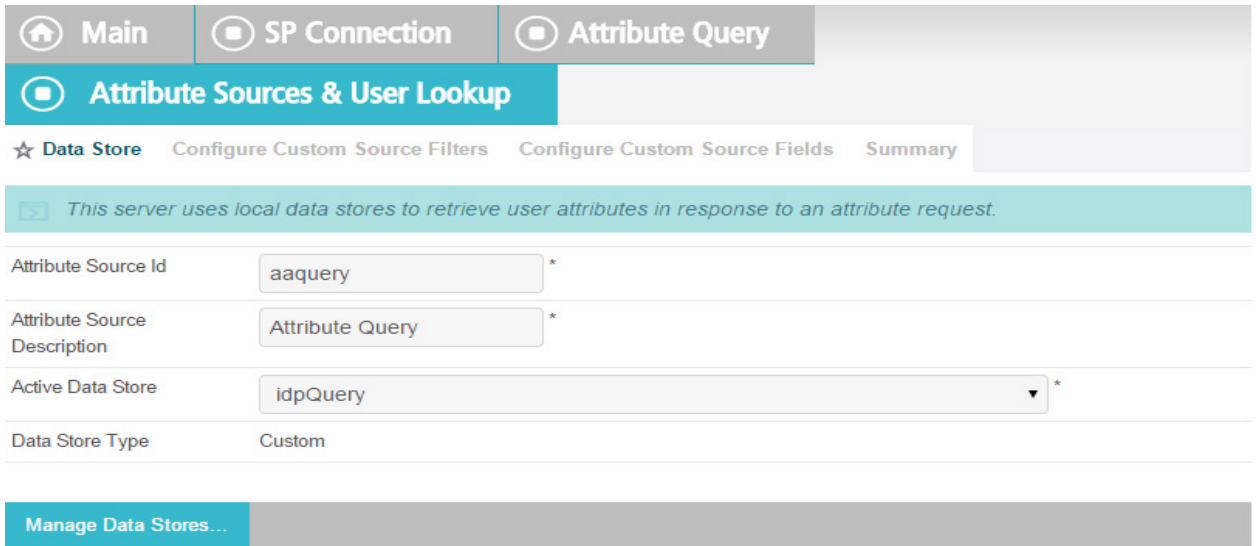
**LDAP FILTER**

Filter	uid=\${SAML_SUBJECT}
--------	----------------------

6070

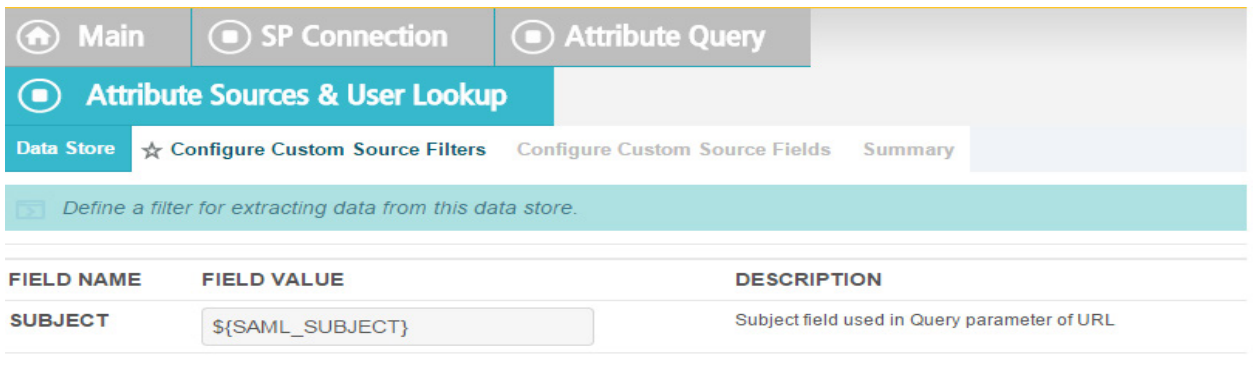
6071

5. Specify a custom **Data Store**.



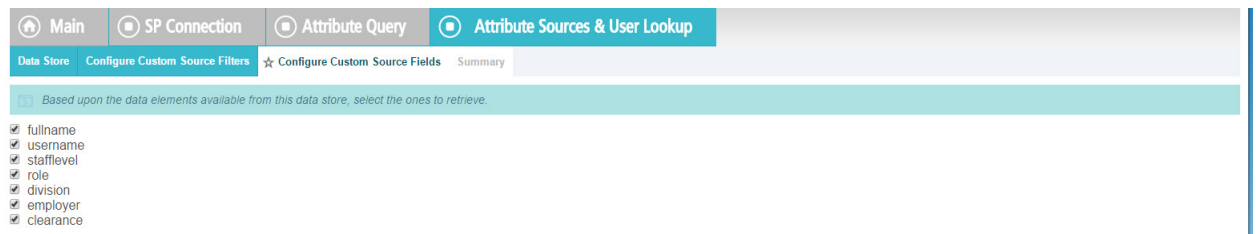
6072

6073 6. Define a filter for extracting data from this data store.



6074

6075 7. Based on the data elements available from this data store, select the ones pertinent to this  
 6076 connection. Note that these are the attributes you previously selected to return from Ping  
 6077 Custom Data.



6078

6079 8. Click **Retrieve**.

6080

6081

9. Click on **Attribute Mapping Fulfillment**.

6082

6083

6084

6085

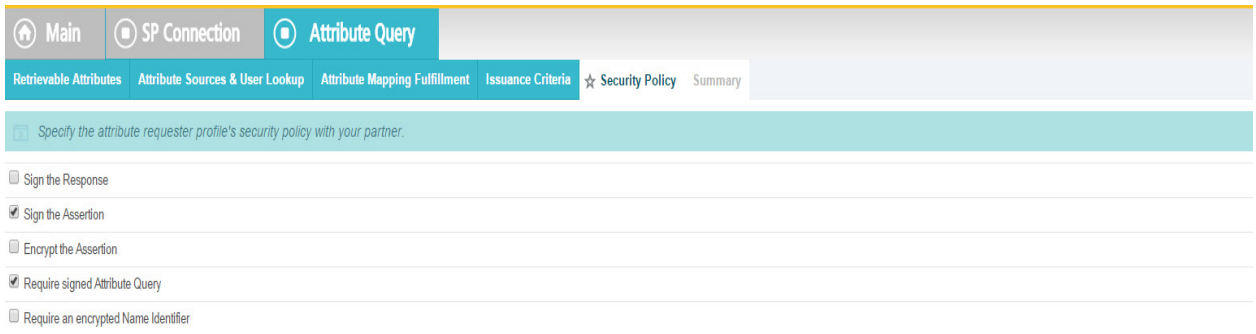
10. **Issuance Criteria:** PingFederate can evaluate various criteria to determine whether to issue an attribute query response. Use this optional screen to configure the criteria for use with this conditional authorization.

6086

6087

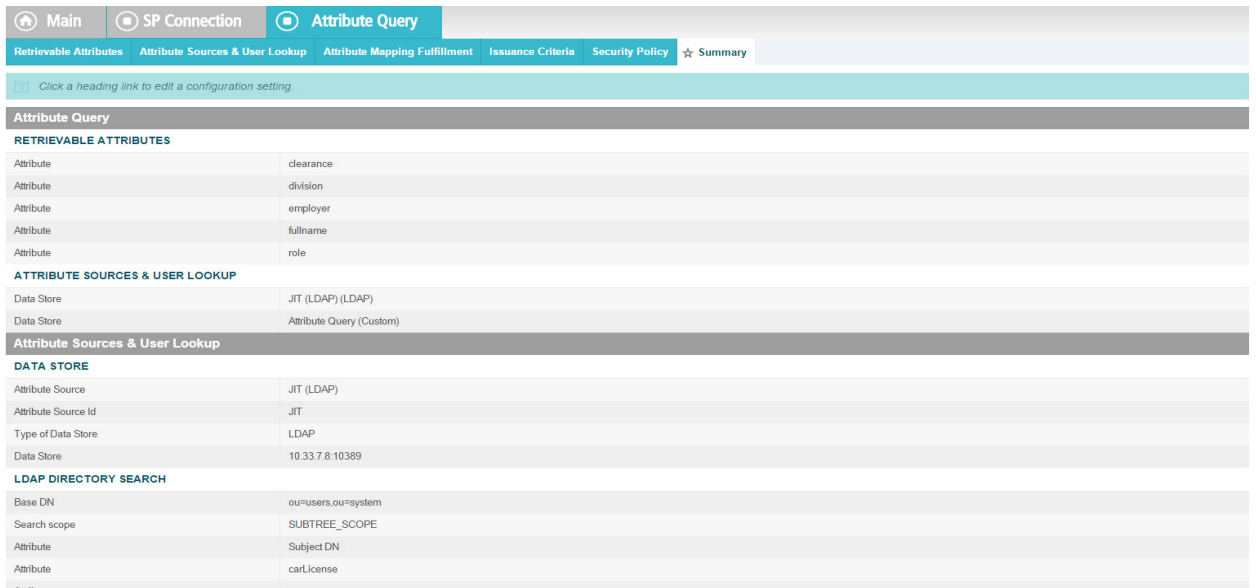
11. Click on **Security Policy**.





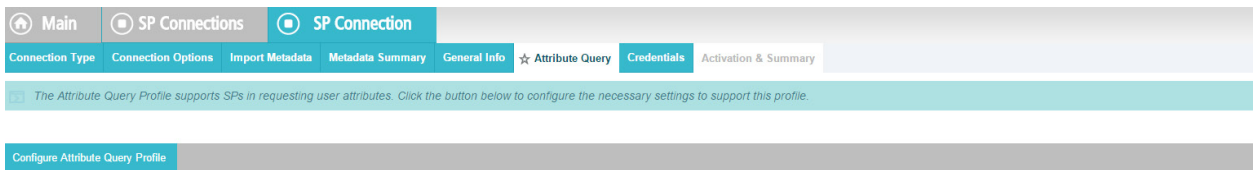
6088

6089 12. Check the **Summary**.



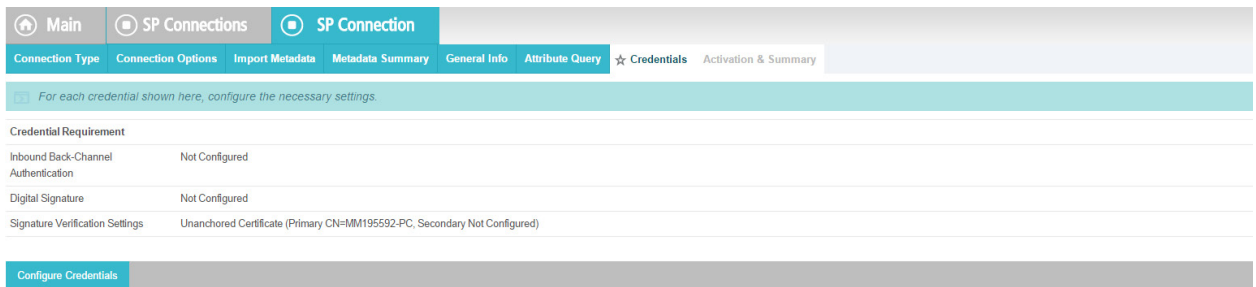
6090

6091 13. Provide **Credentials** for the back channel attribute request.



6092

6093 14. Specify **Inbound Back-Channel Authentication** and **Digital Signature** on the message.

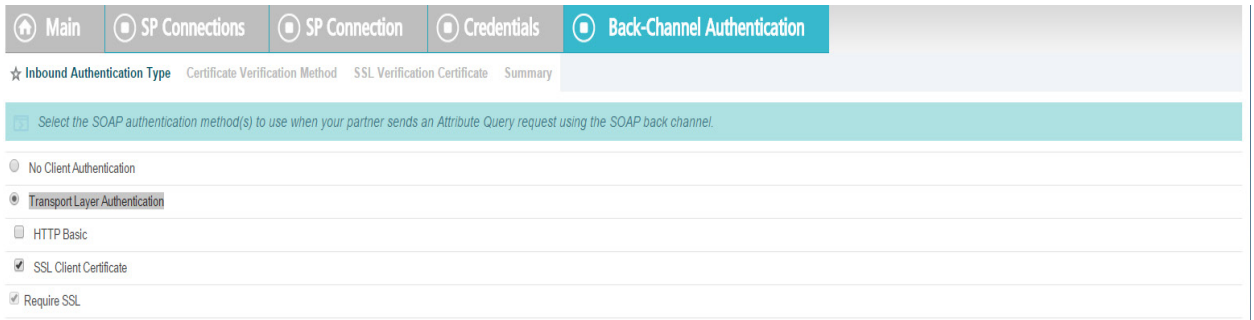


6094

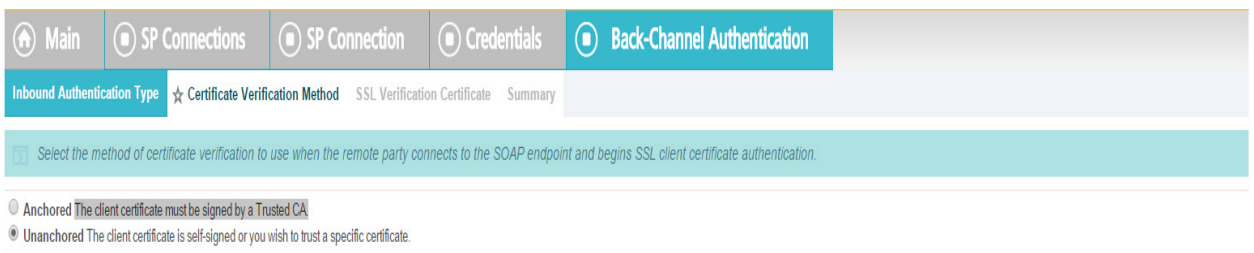


6095 10.8.2.1.3 Back Channel Authentication Configuration

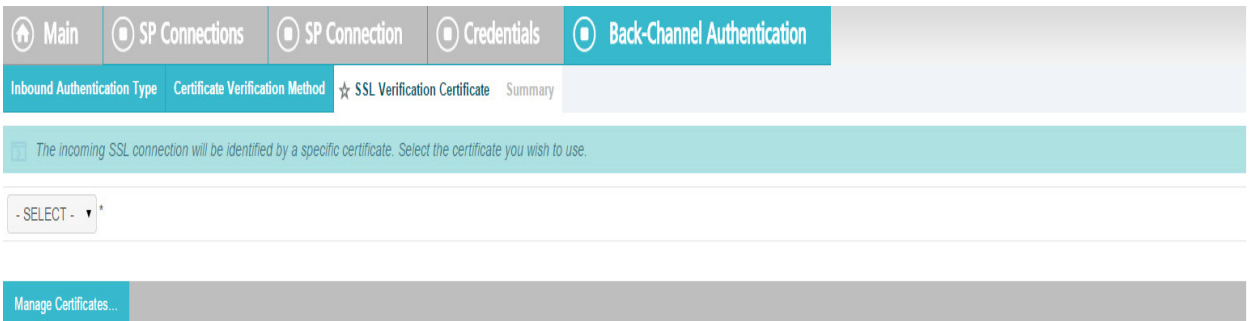
6096 1. Use the default **Transport Layer Authentication with SSL Client Certificate**.



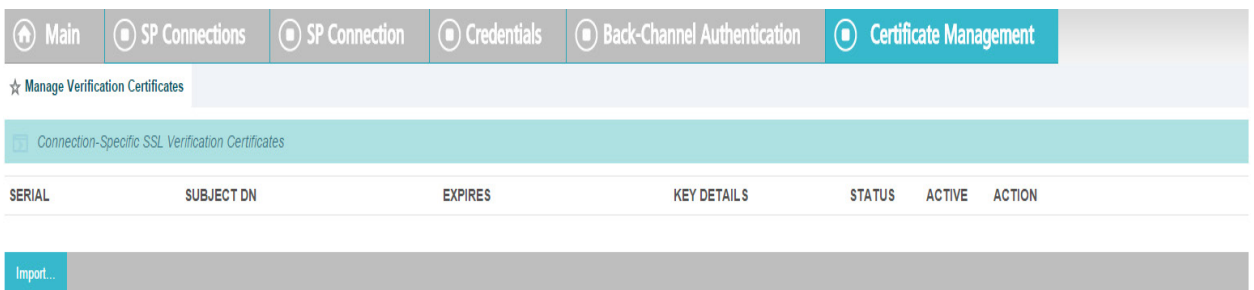
6097  
6098 2. It is encouraged to use the **Anchored** verification method.



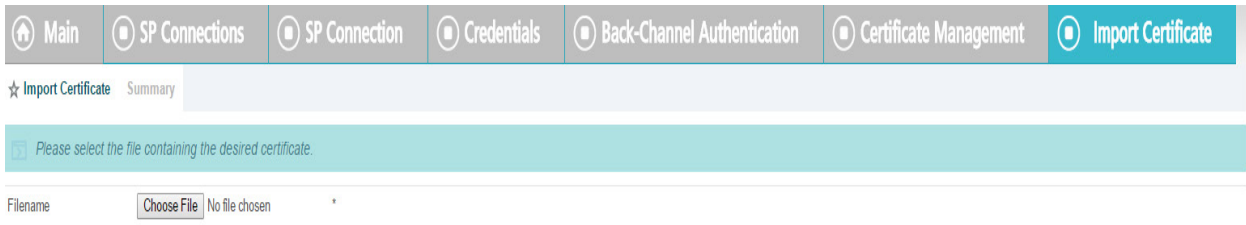
6099  
6100 3. You will be prompted to select an **SSL Verification Certificate**. In our build, a certificate has not  
6101 been previously imported. Click on **Manage Certificate**.



6102  
6103 4. Click **Import**.

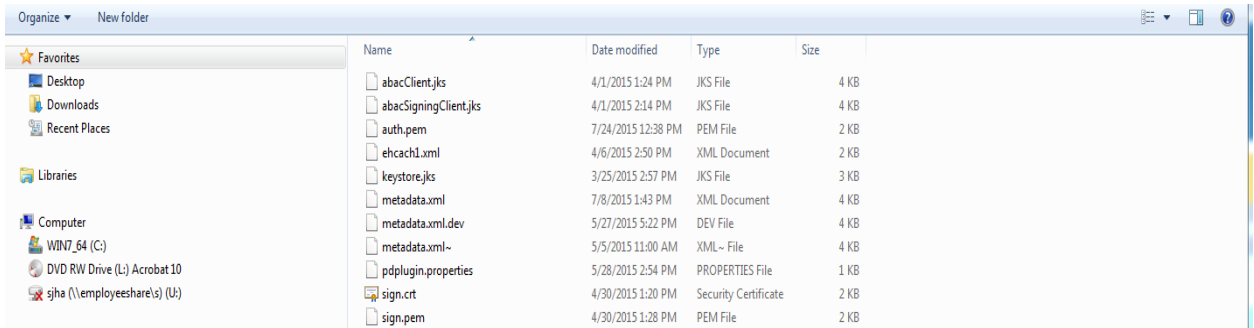


6104  
6105 5. Click **Choose File**.



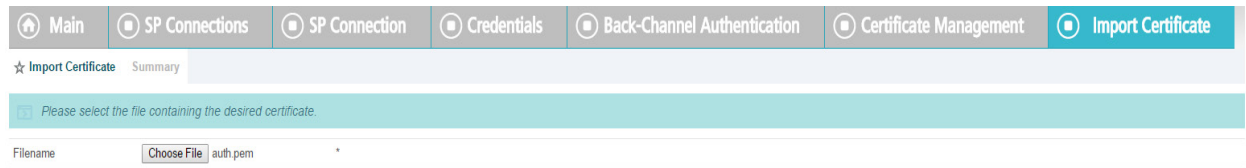
6106

6107 6. Select your certificate file from the Explorer window.



6108

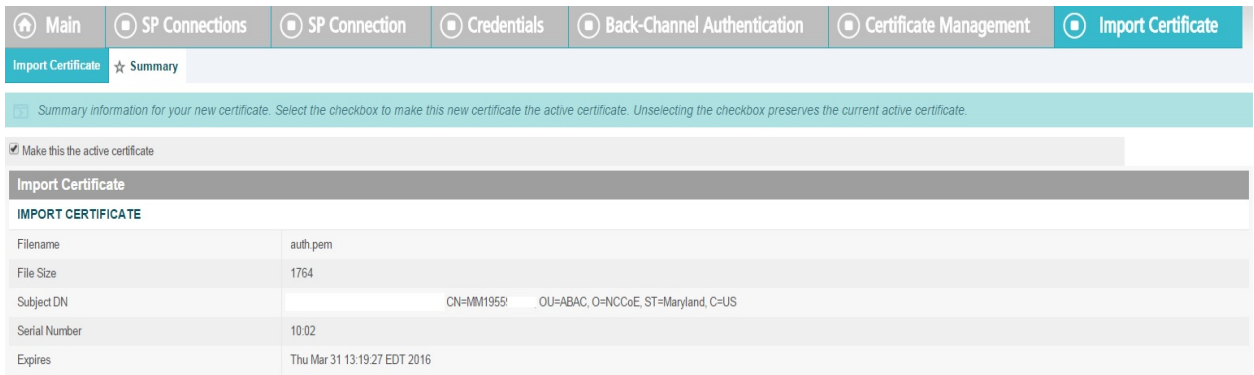
6109 7. The file name will appear in the **Filename** field.



6110

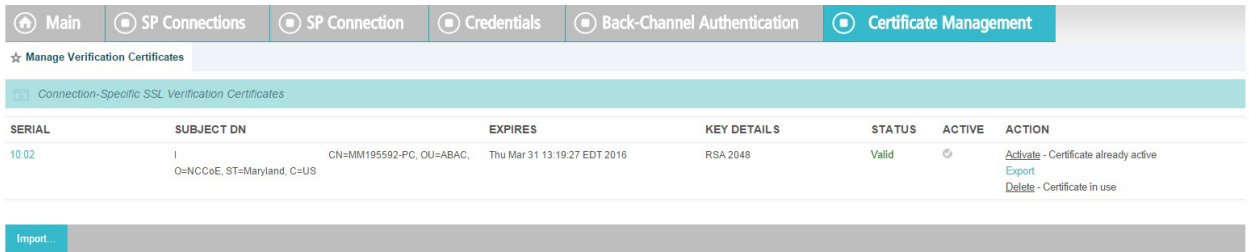
6111 8. Click **Next**. This will display details of parts of certificate.

6112 9. Check **Make this the active certificate** and click **Done**.



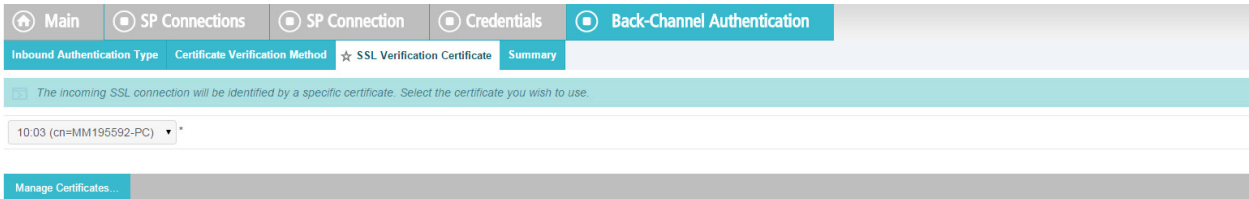
6113

6114 10. Verify the certificate.



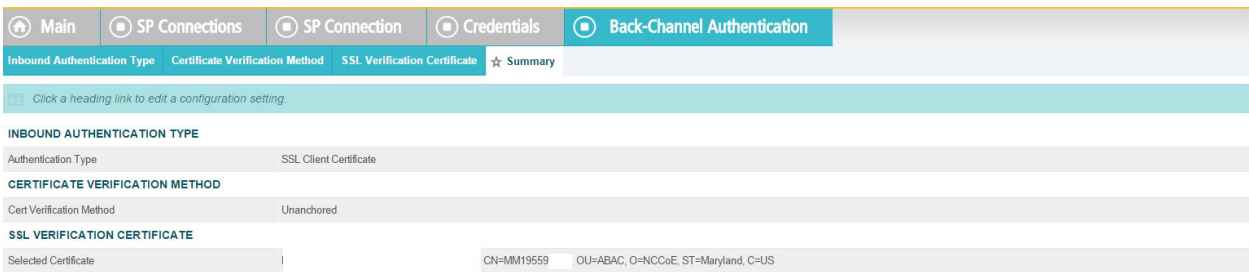
6115

6116 11. Under **Action**, select **Activate**.



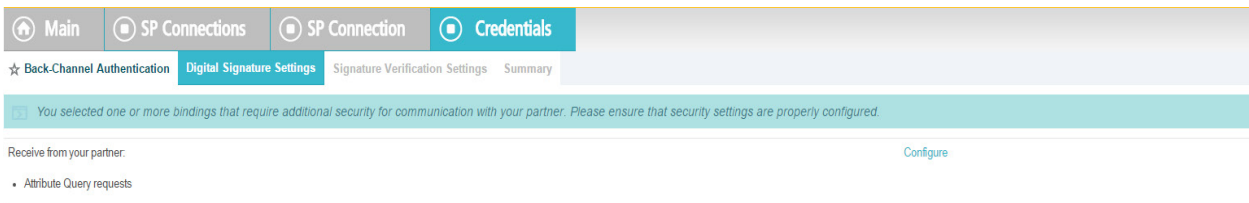
6117

6118 12. View a **Summary** of the verification.



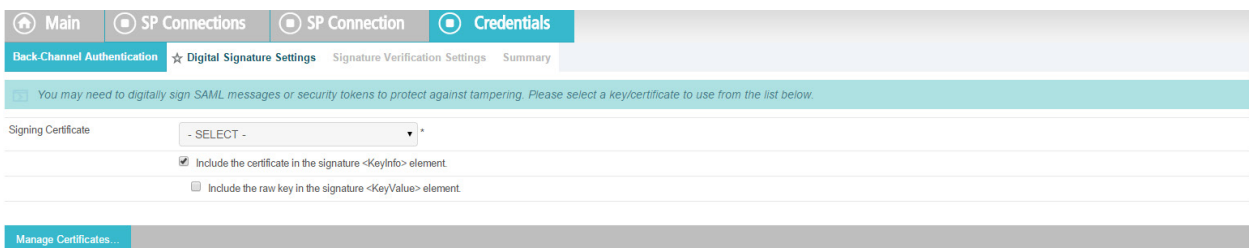
6119

6120 13. Return to the **Back Channel Authentication** tab.



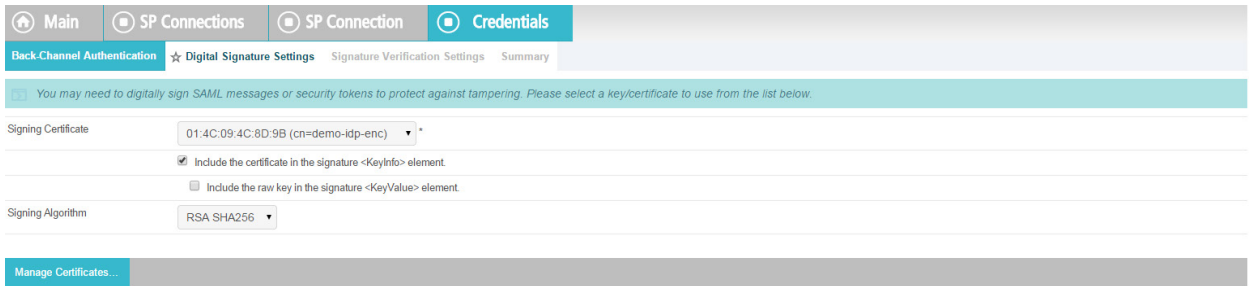
6121

6122 14. Select **Digital Signature Settings** for outgoing messages, then click **Next**.



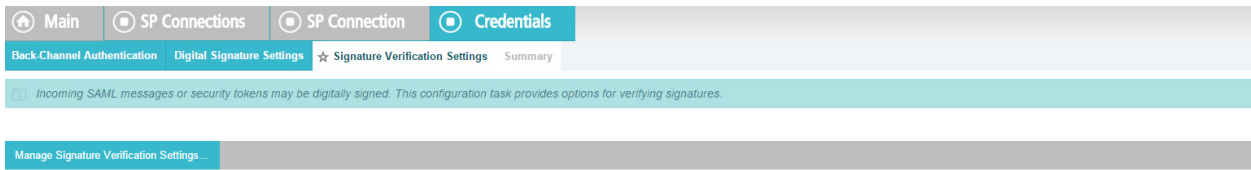
6123

6124 15. Go to **Digital Signature settings**. Click **Configure**.



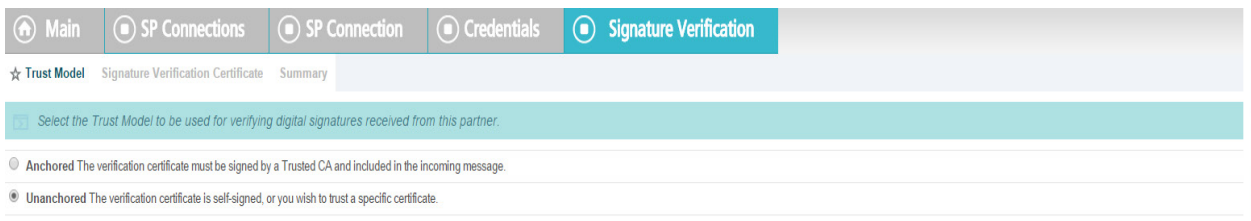
6125

6126 16. Select **Digital Signature Settings** on incoming messages.



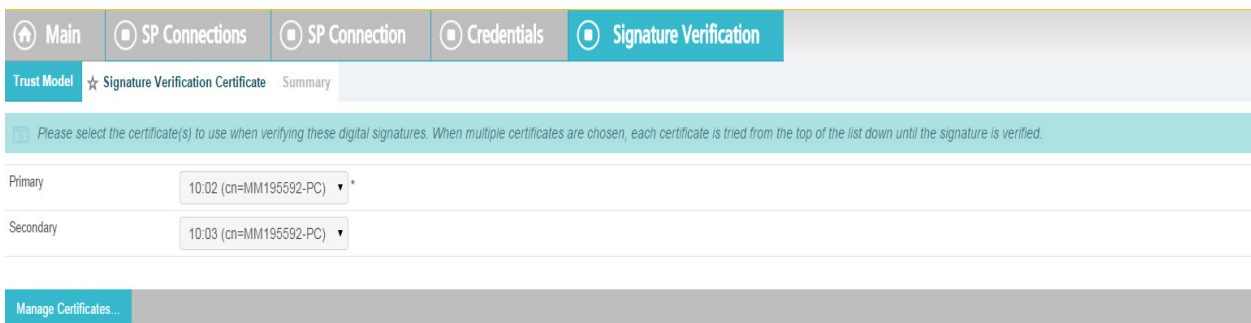
6127

6128 17. Click on **Manage Signature Verification Settings**.



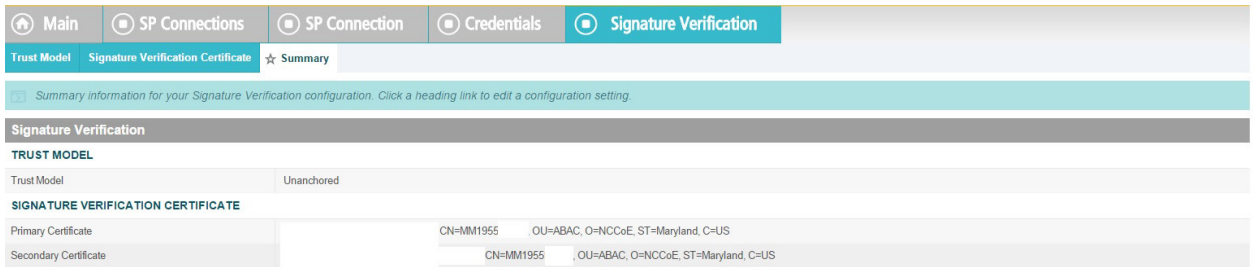
6129

6130 18. Select the certificate(s) to use when verifying these digital signatures. When multiple certificates  
 6131 are chosen, each certificate is tried from the top of the list down until the signature is verified. It  
 6132 is assumed that signed certificates have already been imported. If not, click on **Manage**  
 6133 **Certificate** and complete the steps detailed earlier for importing a certificate.



6134

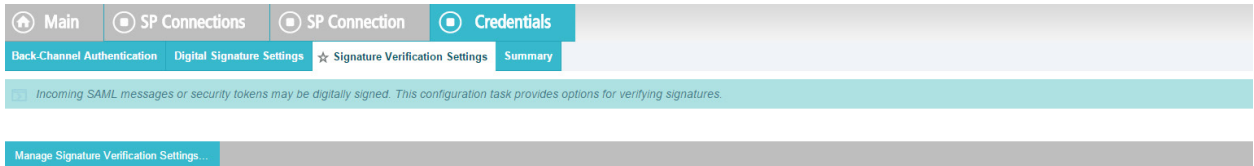
6135 19. Verify the **Summary**.



6136

6137

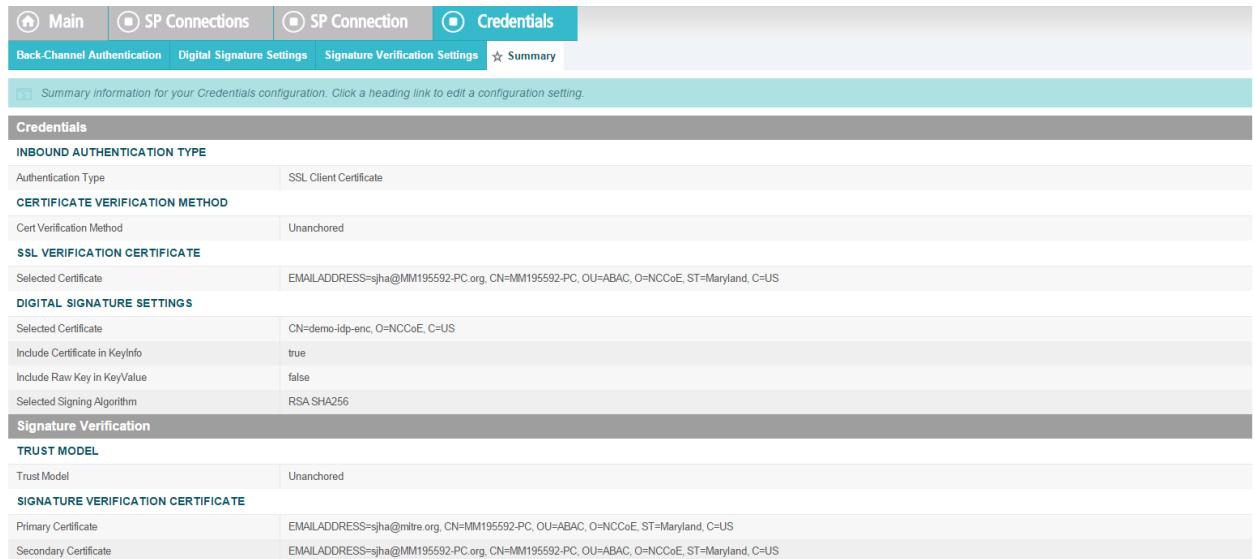
20. This completes the signature verification credential settings.



6138

6139

21. Verify the **Summary**.



6140

6141

22. **Activate** the connection and **Save**.

6142

6143

23. Save again.

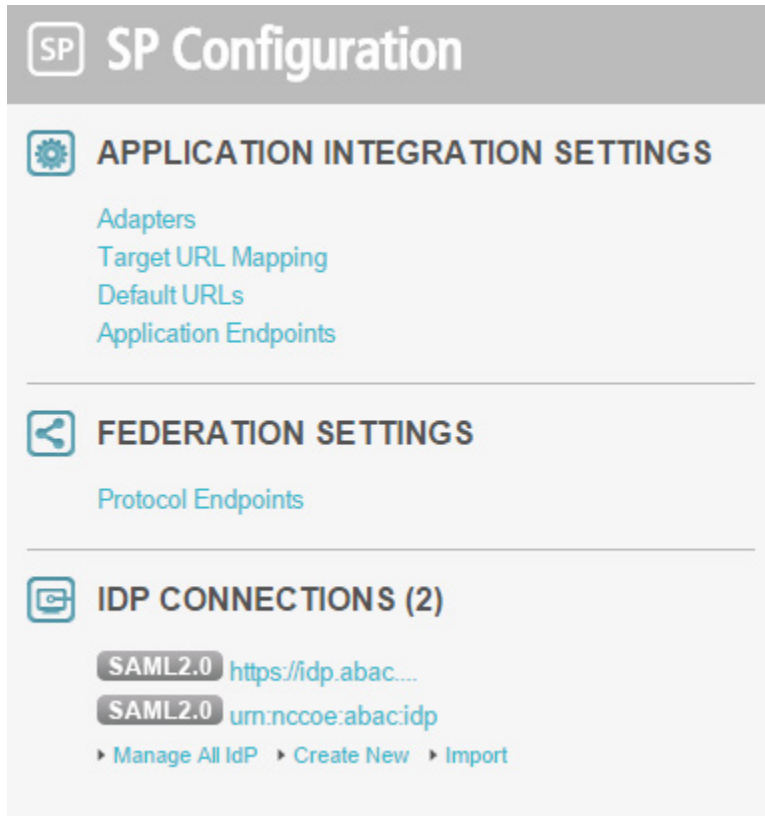
6144

6145

10.8.2.2 IDP Connection

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:

1. On the righthand side of the administrative console, click **Manage All IdP** under **IdP Connections**.

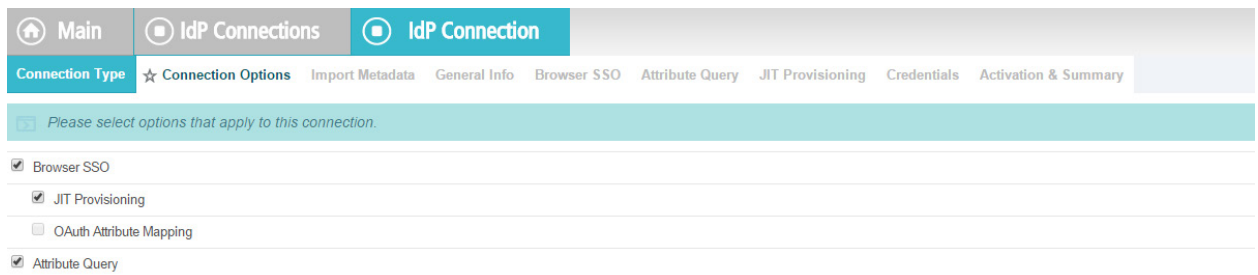


6150

6151

6152

2. Open the connection that was created in [Section 6](#). Click on **Connection Option**. It my default to **Browser SSO**. Additionally, select **Attribute Query** and **JIT Provisioning**.



6153

6154

3. Click **Next**. Verify that the information in the **General Info** tab is correct.

**Main** **IdP Connection**

Connection Type | Connection Options | **General Info** | Browser SSO | Attribute Query | JIT Provisioning | 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)  \*

Connection Name  \*

Virtual Server IDs

Base URL

Company

Contact Name

Contact Number

Contact Email

Error Message:

Logging Mode:  None  Standard  Enhanced  Full

6155

6156

4. Click **Next**.

**Main** **IdP Connection**

Connection Type | Connection Options | General Info | **Browser SSO** | Attribute Query | JIT Provisioning | Credentials | Activation & Summary

*This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your site. Click the button below to create or revise this configuration.*

Browser SSO Configuration

6157

6158

5. Click on **Configure Attribute Query Profile**.

**Main** **IdP Connection**

Connection Type | Connection Options | General Info | Browser SSO | **Attribute Query** | JIT Provisioning | Credentials | Activation & Summary

*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.*

6159

6160

6. Specify an **Attribute Authority Service URL**.

**Main** **IdP Connection** **Attribute Query**

★ Attribute Request Service URL | Attribute Name Mapping | Security Policy | Summary

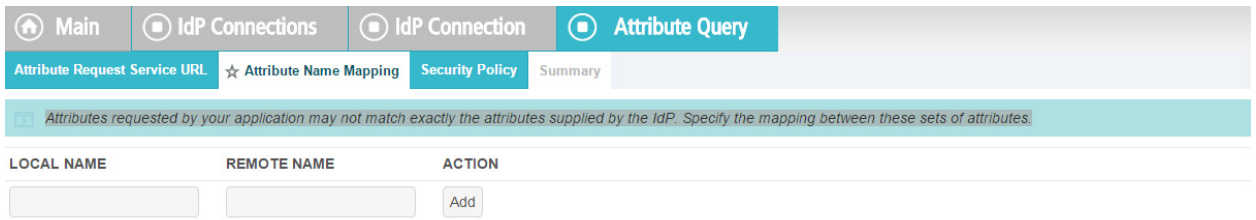
*Specify the URL at your IdP partner's site where attribute queries are to be sent.*

Attribute Authority Service URL  \*

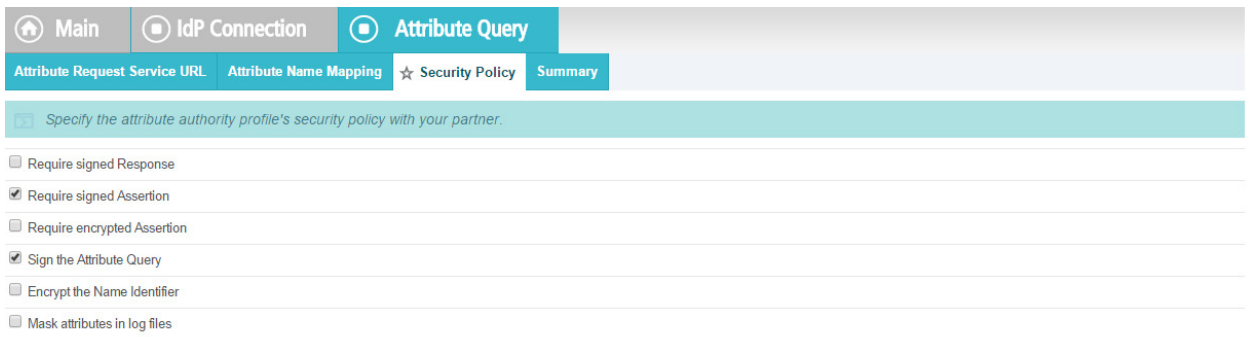
6161



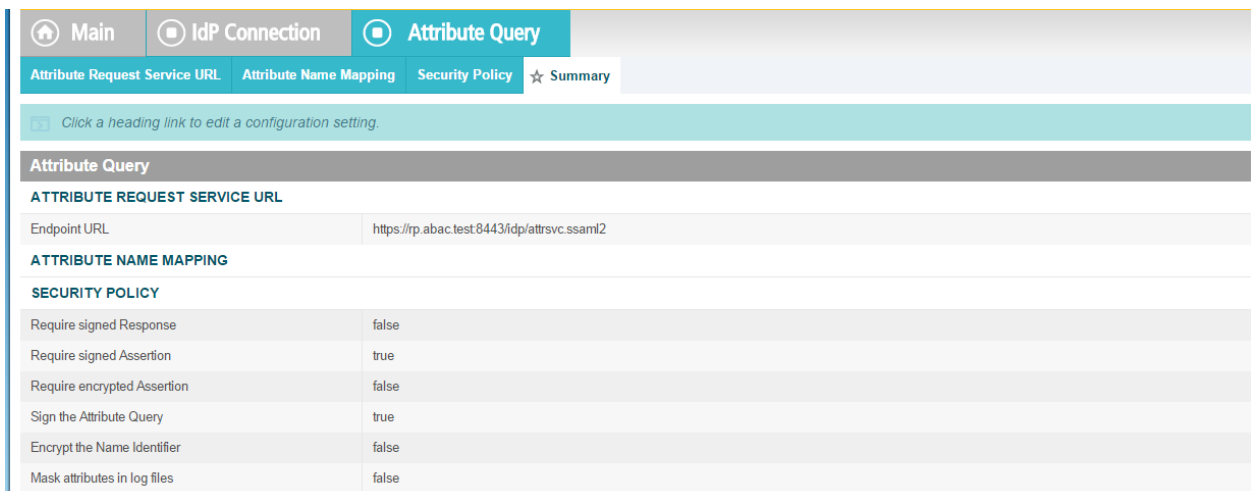
- 6162 7. Attributes requested by your application may not match exactly the attributes supplied by the  
 6163 IdP. Specify the mapping between these sets of attributes.



- 6164  
 6165 8. Select **Sign the Attribute Query**.



- 6166  
 6167 9. Verify that the **Summary** is correct, then click **Done**.



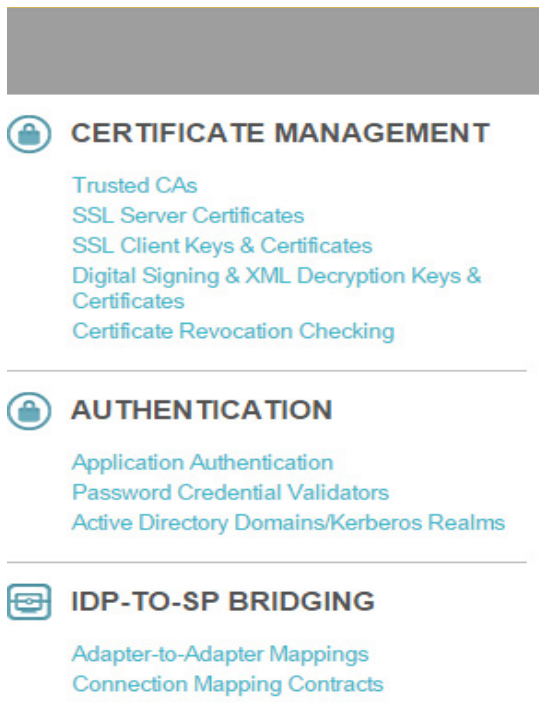
- 6168  
 6169 10. When the following screen appears, click **Next**.



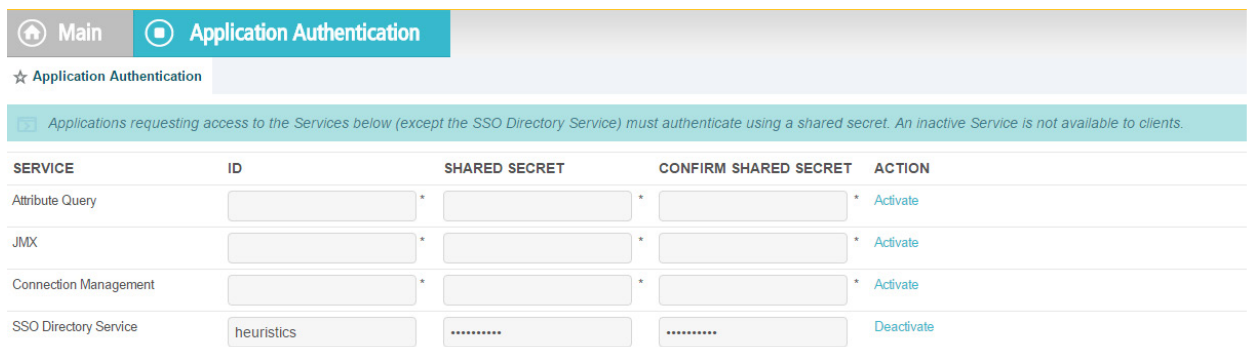
- 6170  
 6171 11. JIT provisioning details have been provided by PingFederate [here](#).

6172 12. **Save** the configuration.

6173 13. Select **Application Authentication**.



6174



6175

6176 14. Enter **appid** in the ID field, and use the shared secret that you input during custom data store  
6177 configuration, then save the configuration.

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](#).

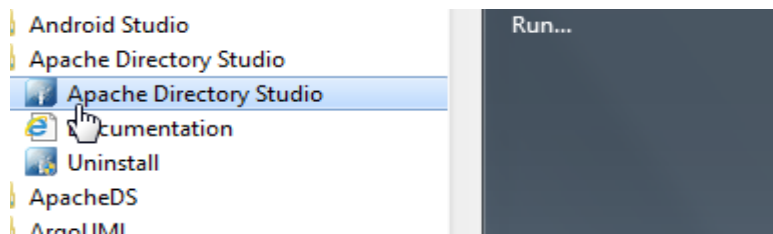
6196 In the following section, we will demonstrate how to create an attribute. Similar procedures can be used  
6197 to create many attributes and object classes.

### 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

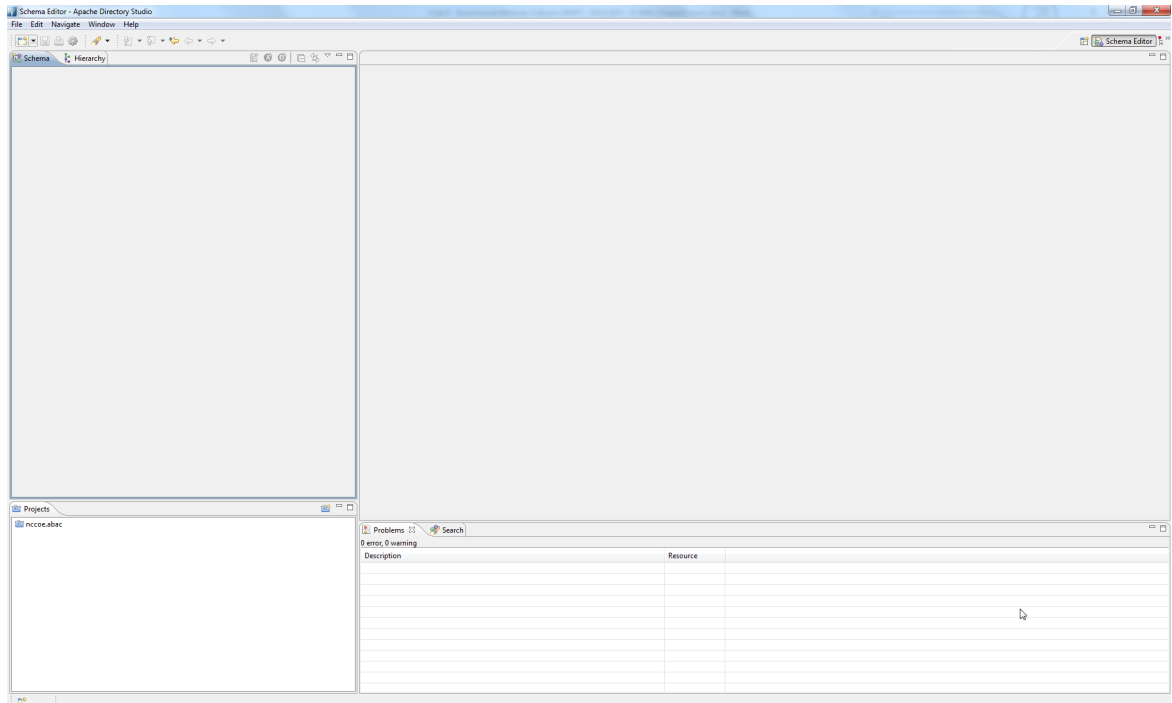
6202 1. Start ApacheDS Studio from the Start menu.



6203

6204 2. The following screen will appear:

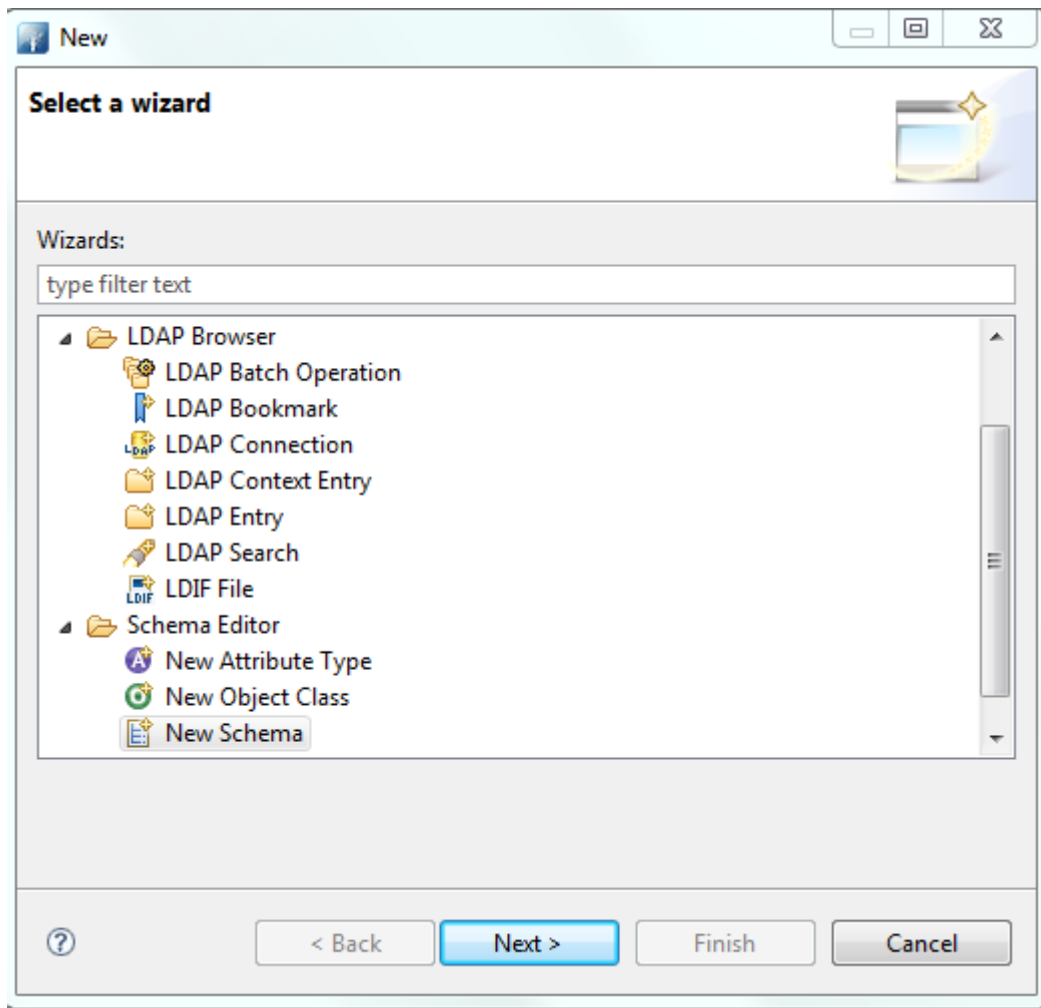
## SECOND DRAFT



6205

6206

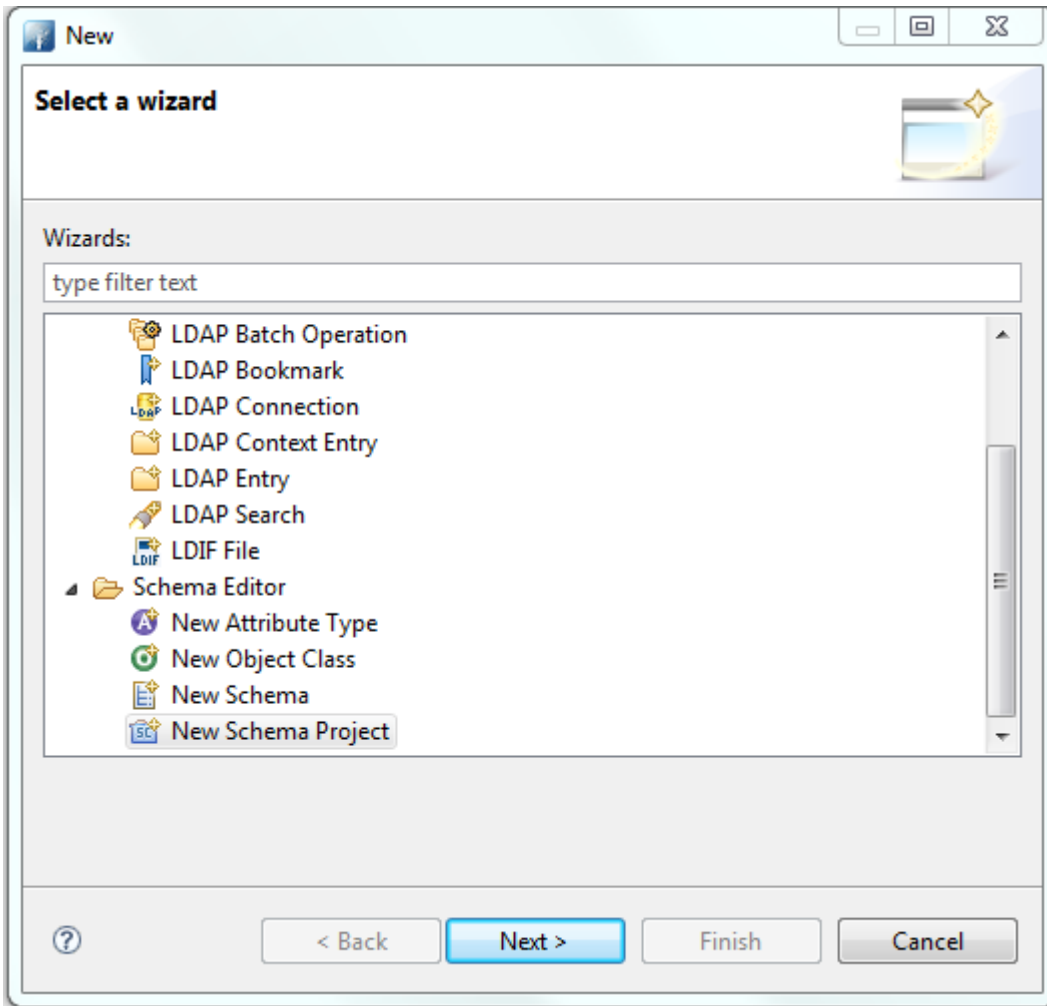
3. Select **File > New**.



6207

6208

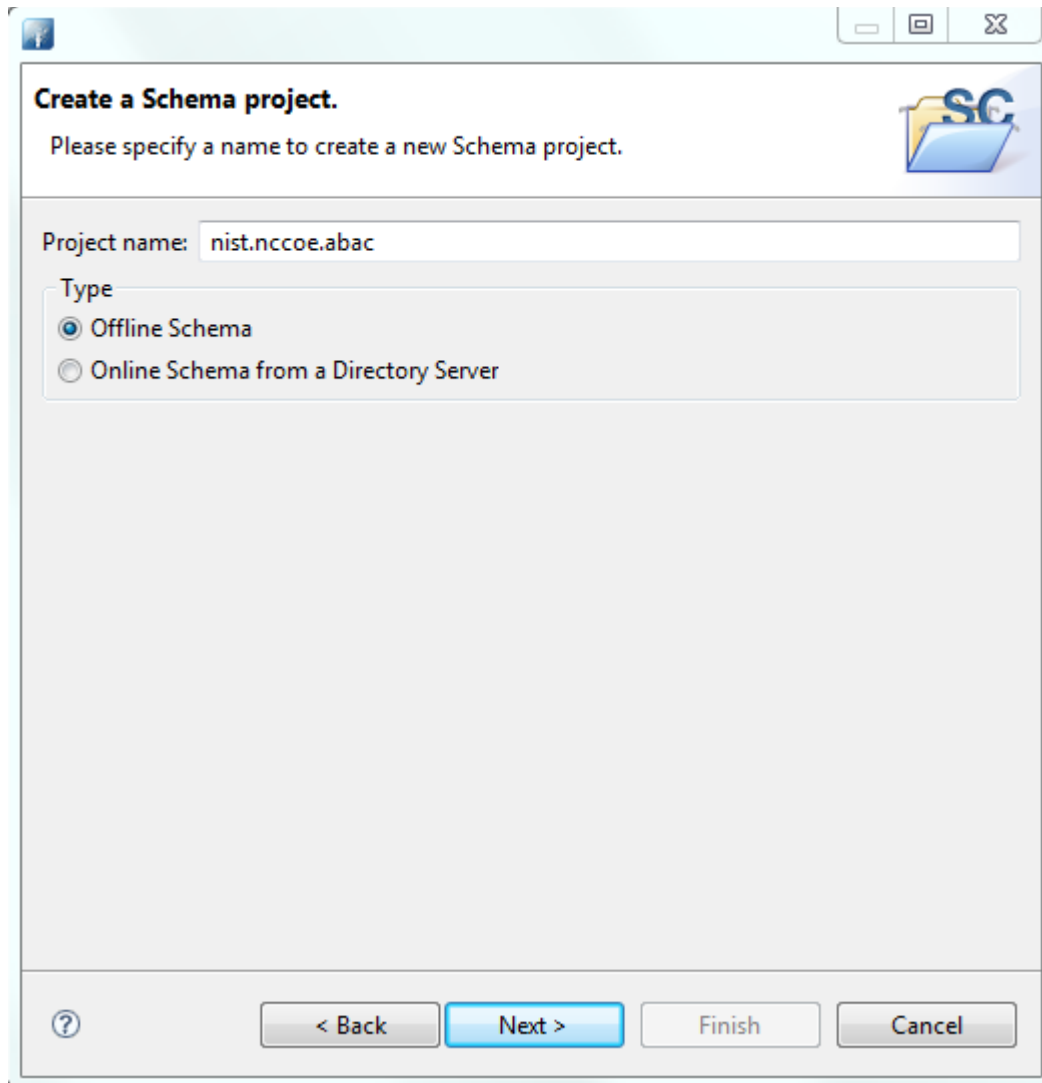
4. Select the **New Schema Project** wizard.



6209

6210

5. Specify a **Project name**, i.e., **nist.nccoe.abac** in our build.

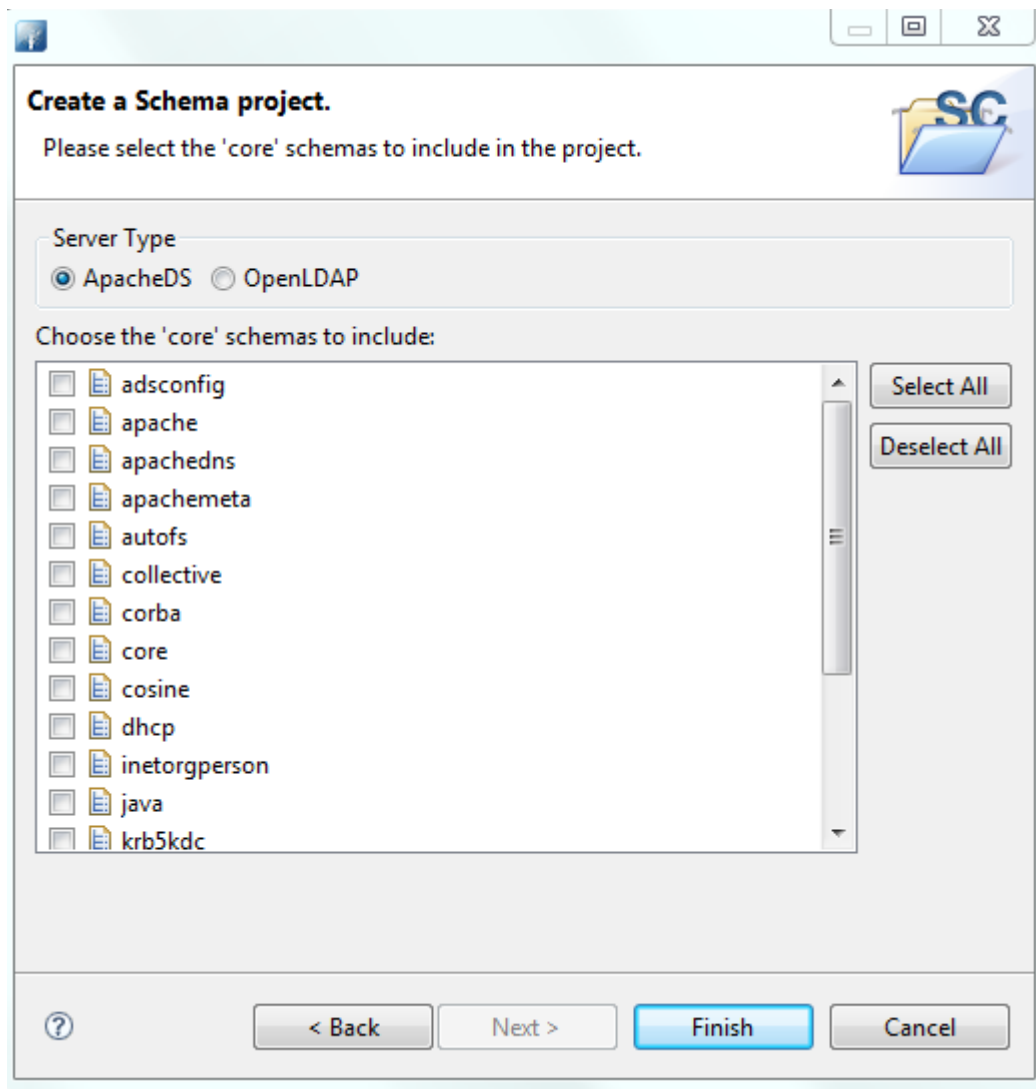


6211

6212

6213

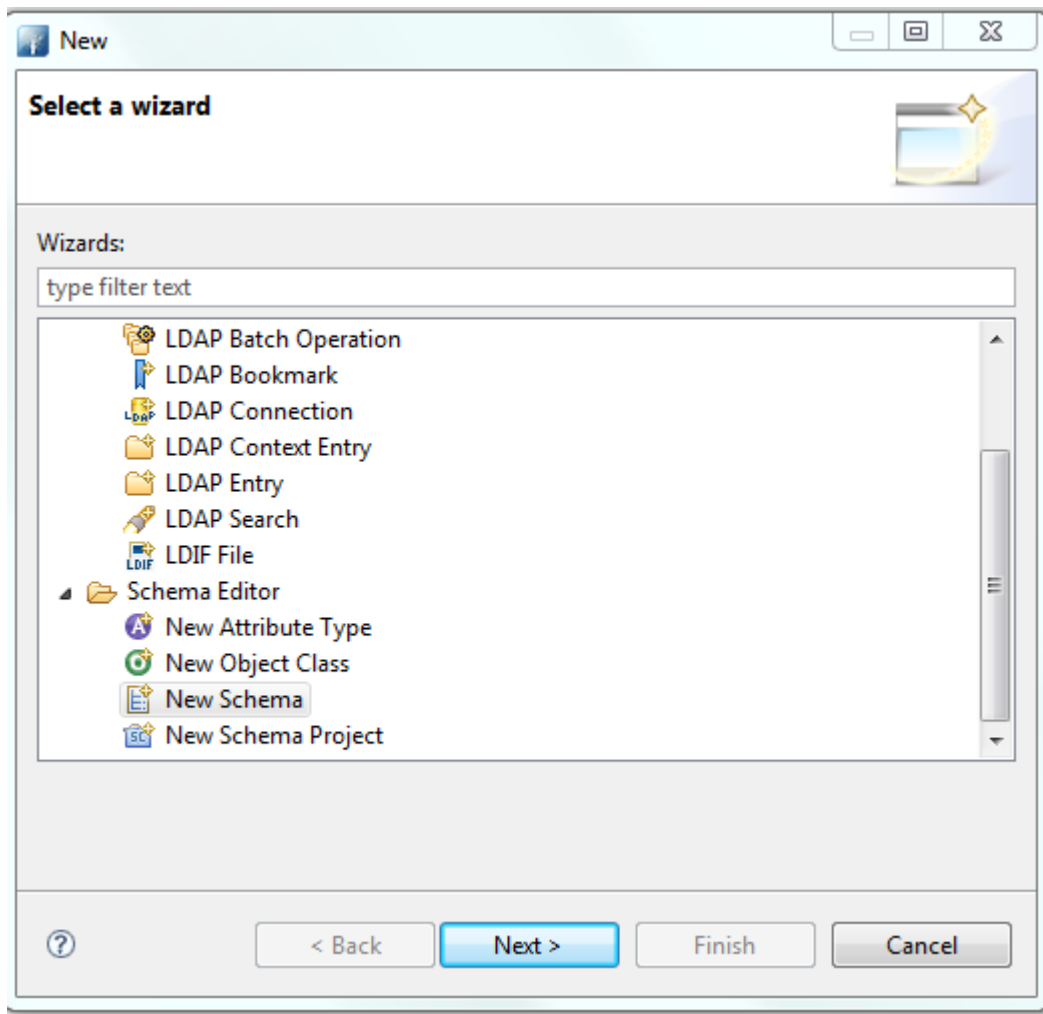
6. Select **Offline Schema**, then click **Next**. On the next screen, **Choose the 'core' schemas to include**.



6214

6215 7. Click **File > New** and select **New Schema**.

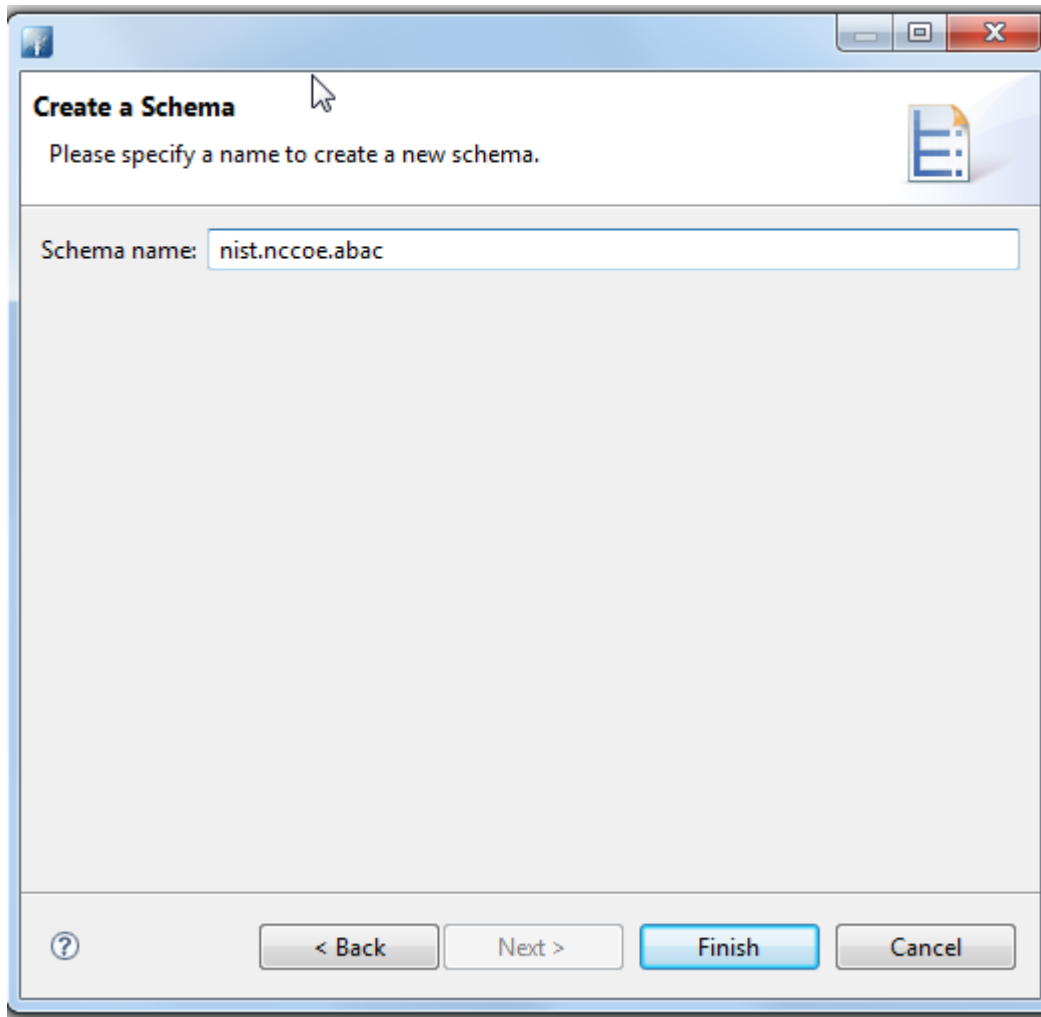




6216

6217

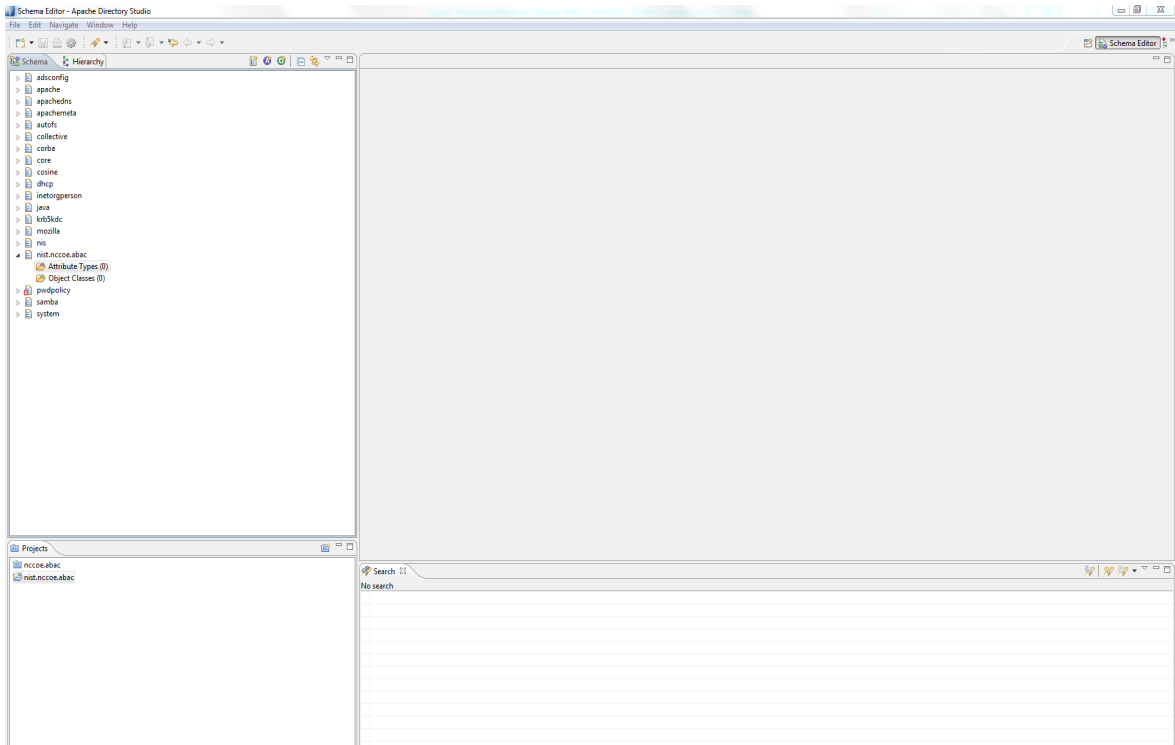
8. Specify a **Schema name**, i.e., **nist.nccoe.abac** in our build.



6218

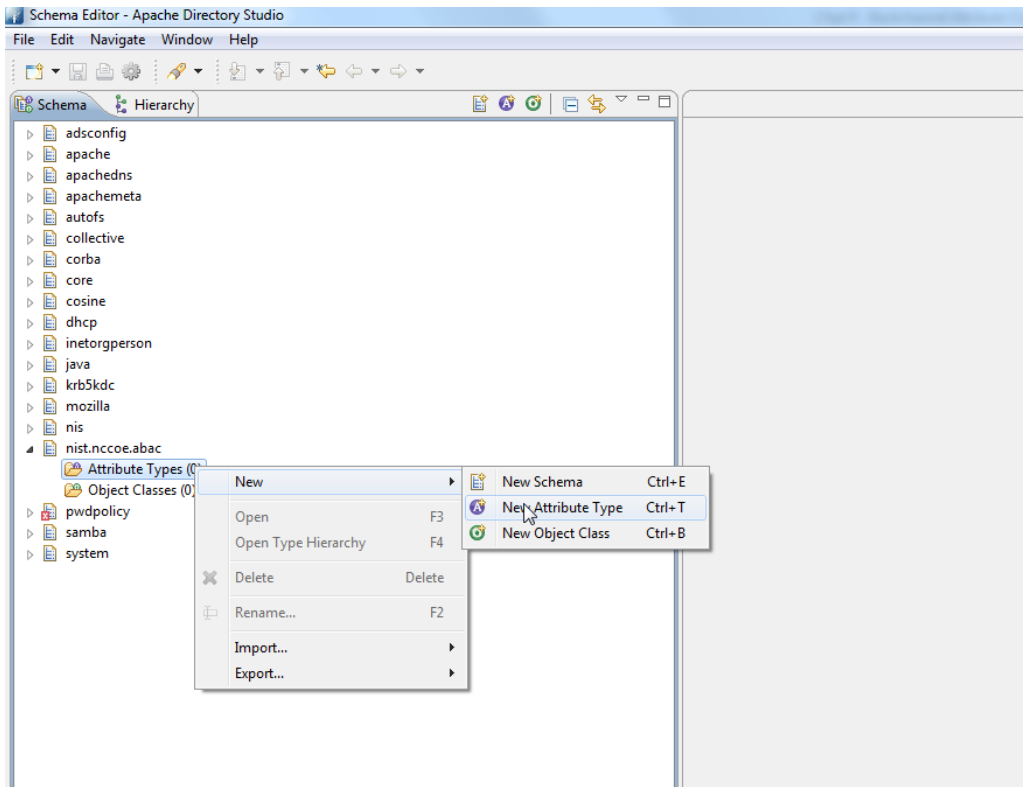
6219

9. The following screen will appear:



6220

6221 10. Select **Attribute Types > New > New Attribute Type**.



6222

6223 11. In the new window, choose the **OID** from the previous instructions.

**Attribute Type**  
Create a new attribute type.

Schema  
Schema: nist.nccoe.abac

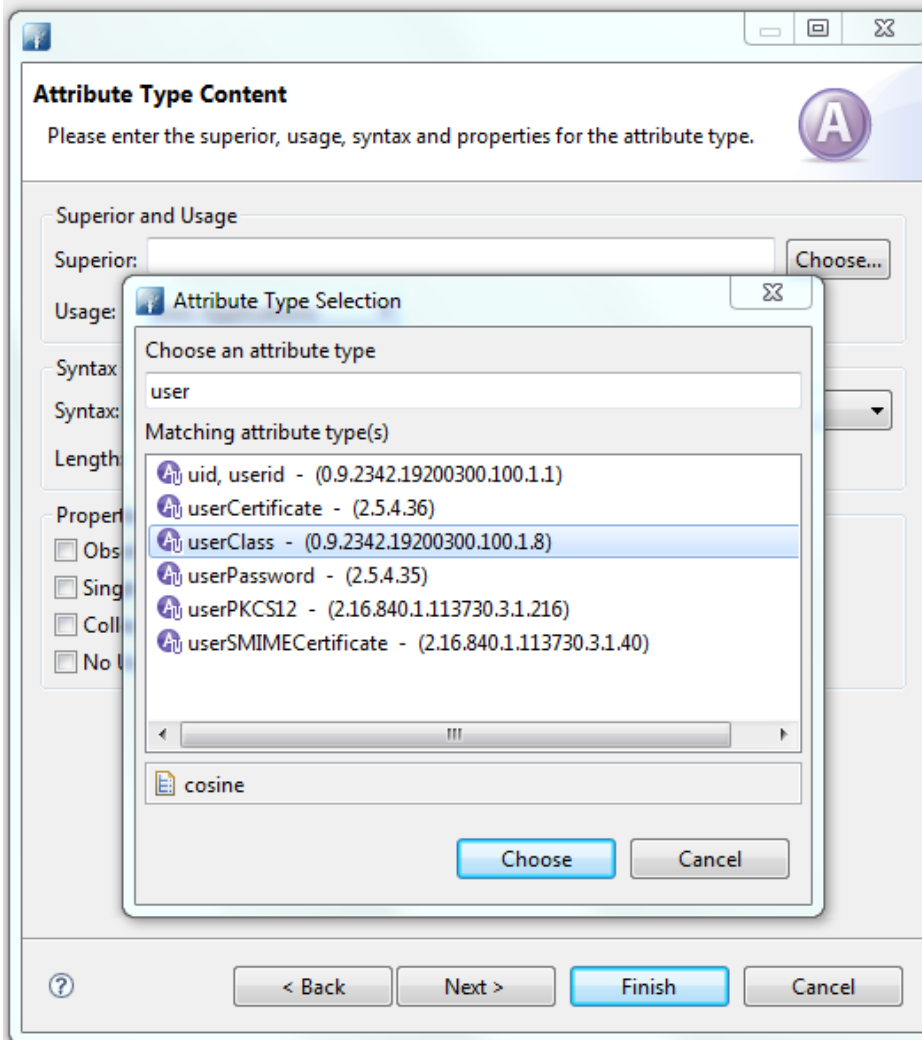
Naming and Description  
OID: 2.25.163544471716650257972990341252161848603.1  
Aliases: staffClearance Edit...  
Description: Clearance of a staff

< Back Next > Finish Cancel

6224

6225

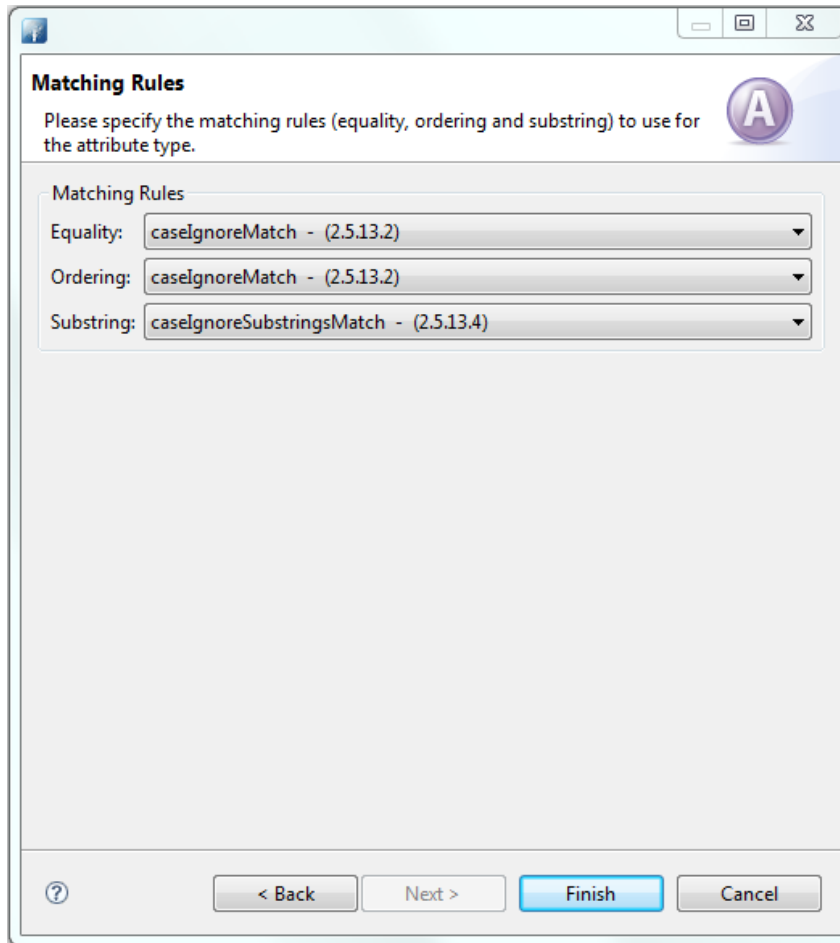
12. Click **Next** to choose the superior type of this attribute.



6226

6227

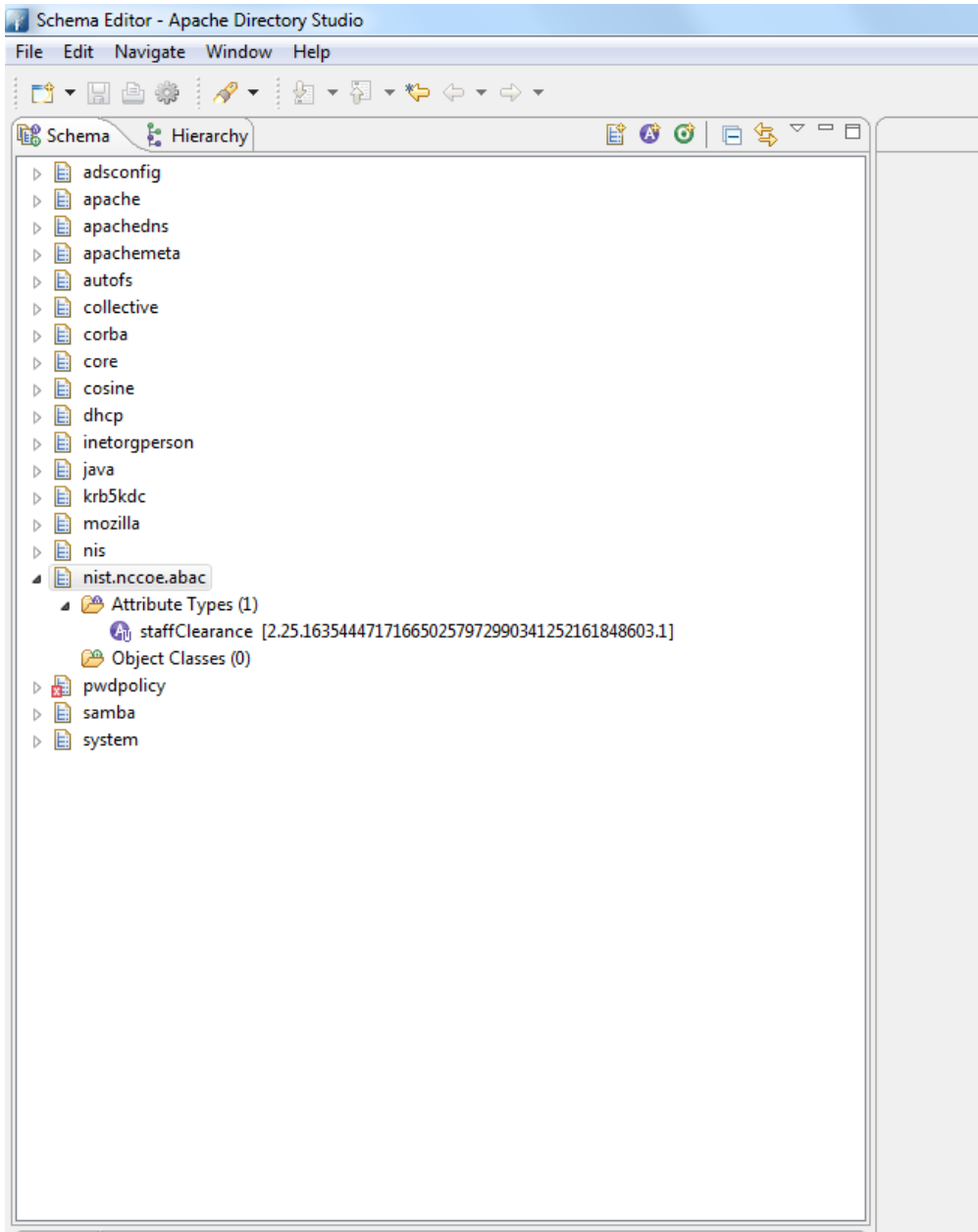
13. Specify **Matching Rules**. Since it is a string, case insensitivity is chosen in our build.



6228

6229

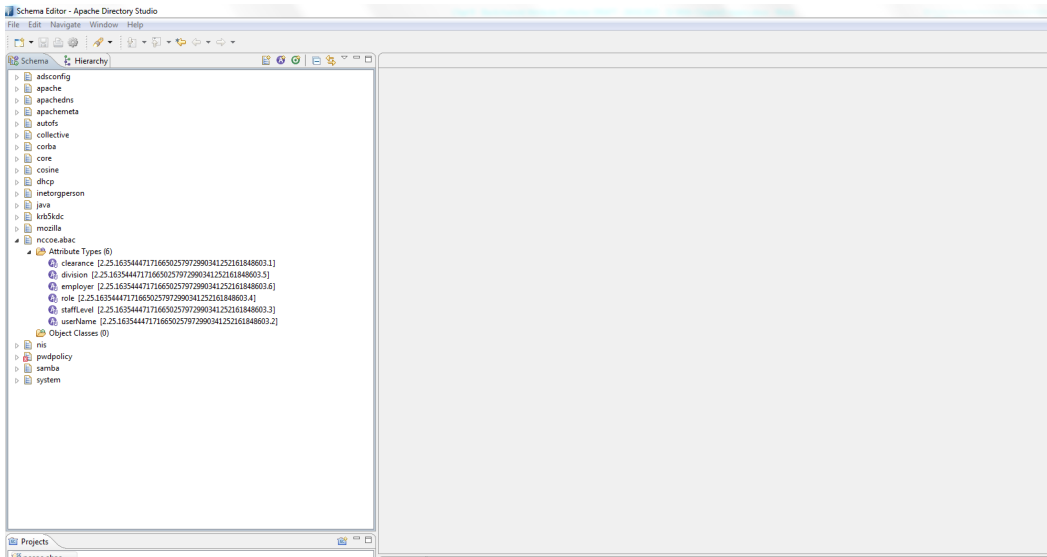
14. The following screen will appear:



6230

6231 15. You can create other attributes by following process described above.

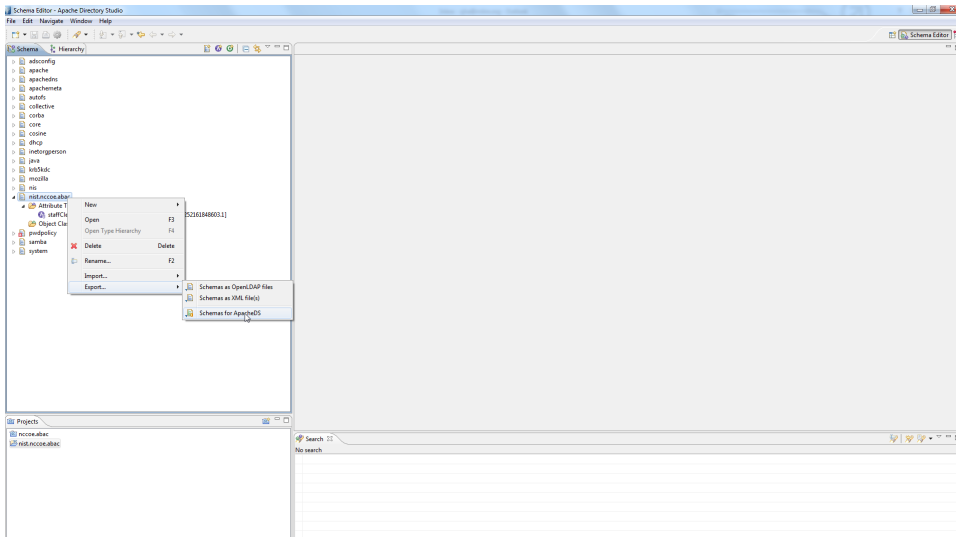
## SECOND DRAFT



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:



The screenshot shows a Gvim window titled 'test.ldif (~\Desktop) - GVIM'. The window contains the following text:

```
# 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
n-dependencies: cosine

dn: ou=attributetypes, cn=nist.nccoe.abac, ou=schema
objectclass: organizationalUnit
objectclass: top
ou: attributetypes

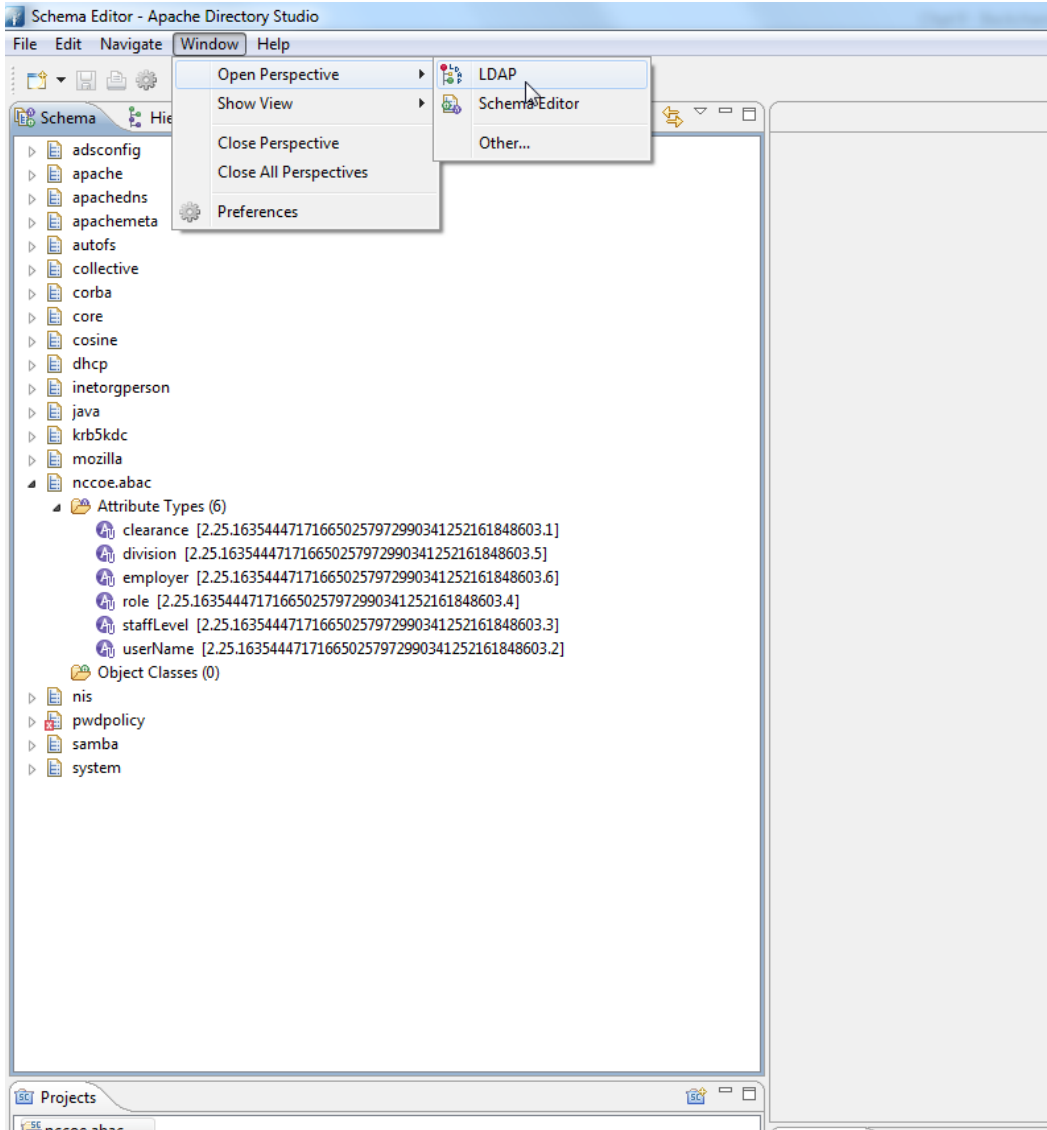
dn: m-oid=2.25.163544471716650257972990341252161848603.1, ou=attributetypes, cn=
nist.nccoe.abac, ou=schema
objectclass: metaAttributeType
objectclass: metaTop
objectclass: top
n-oid: 2.25.163544471716650257972990341252161848603.1
n-name: staffClearance
n-description: Clearance of a staff
n-supAttributeType: userClass
n-equality: caseIgnoreMatch
```

At the bottom right of the window, the text '24,1' and 'Top' is visible.

6236

6237

18. To import the file, first select **Window > Open Perspective > LDAP**.

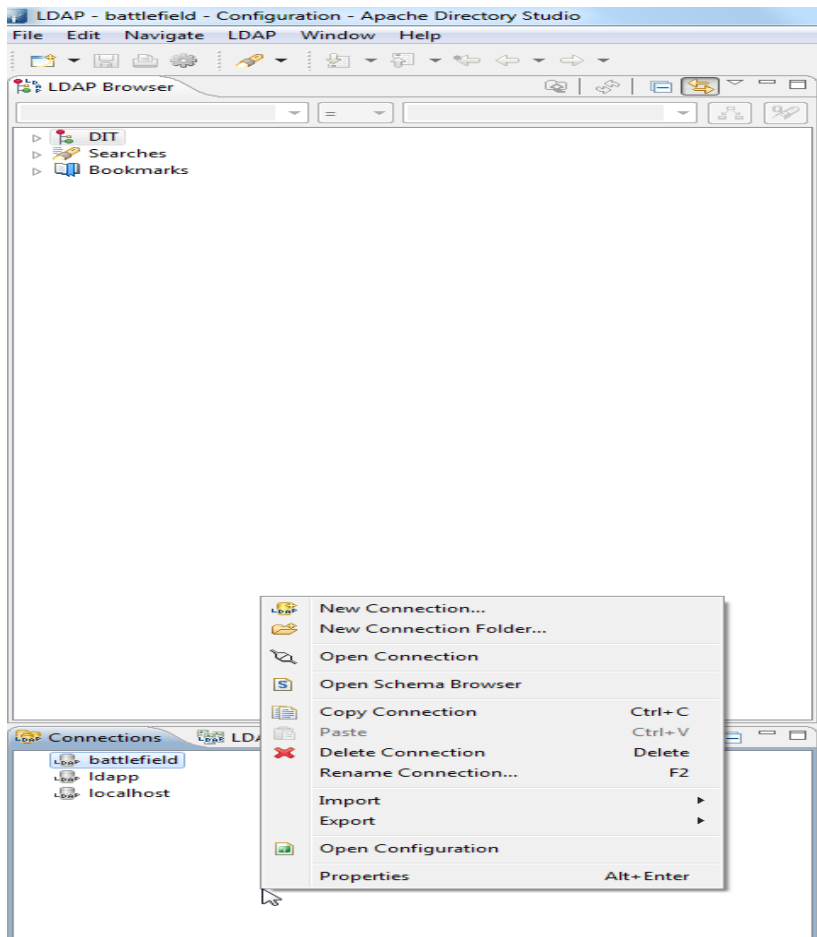


6238

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**.

New LDAP Connection

**Network Parameter**

Please enter connection name and network parameters.

Connection name: battlefield1

Network Parameter

Hostname: 10.33.7.8

Port: 10389

Encryption method: No encryption

Server certificates for LDAP connections can be managed in the '[Certificate Validation](#)' preference page.

Provider: Apache Directory LDAP Client API

Check Network Parameter

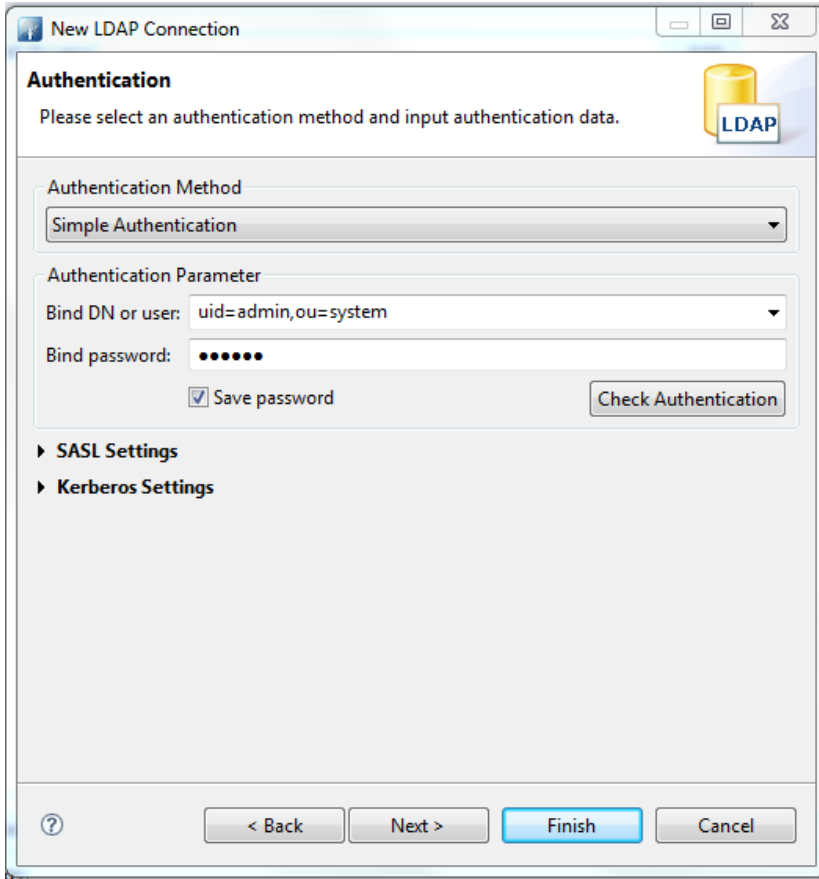
Read-Only (prevents any add, delete, modify or rename operation)

? < Back Next > Finish Cancel

6242

6243

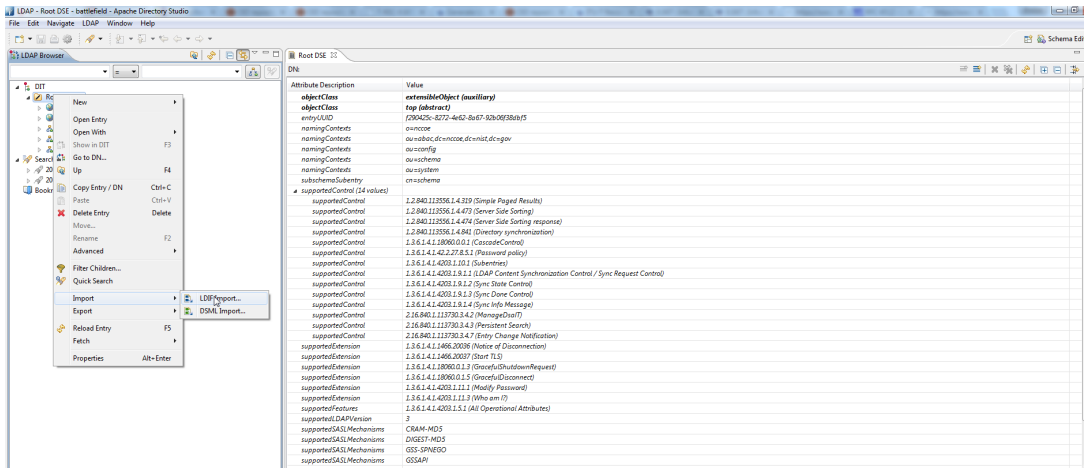
21. Provide credentials and click **Finish**.



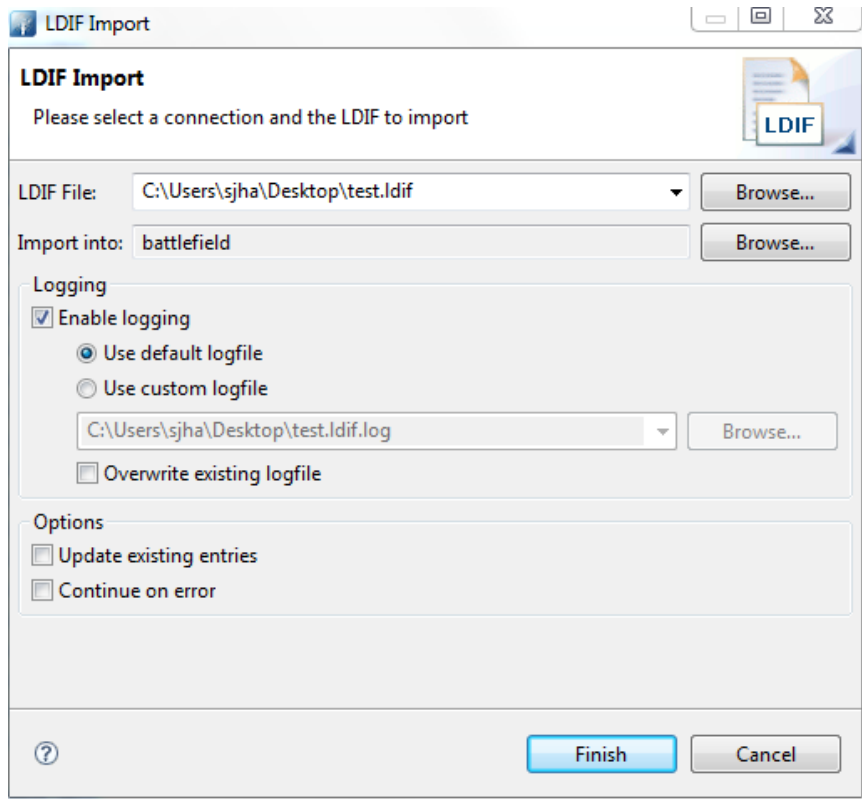
6244

6245

22. Open **Schema Editor Browser** and import the LDIF file created in the previous step.



6246



6247

6248

6249

23. Click **Finish**.

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.

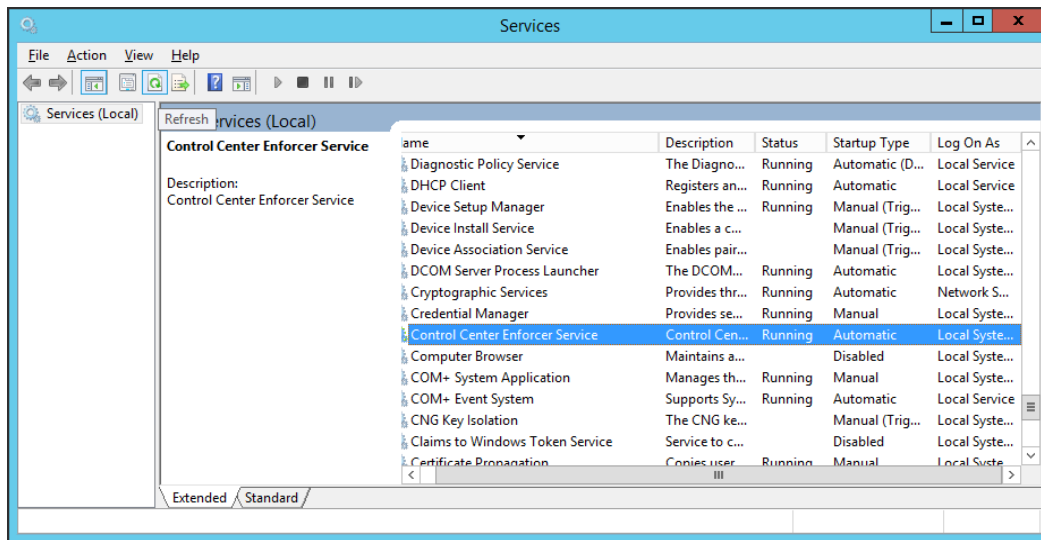
6260 The second functional test will ensure that the Protocol Broker is successfully loaded and deployed  
 6261 within the tomcat server instance.

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**  
 6267 **Enforcer Service**.

- 6268 4. Verify that the status column reads **Running**.



6269

## 6270 10.10.2 Test the Successful Loading of the Custom Plugin Within the NextLabs Policy 6271 Controller Software Architecture

- 6272 1. Click on the Windows icon.
- 6273 2. Begin typing **Windows Explorer**.
- 6274 3. Click on the Windows Explorer application icon.
- 6275 4. Navigate to *C:/Program Files/NextLabs/Policy Controller/agentLog/*.
- 6276 5. Within the **agentLog** folder, note the **Agentlog0.0** file.
- 6277 6. Within the **agentLog** folder, copy and paste the locked file **Agentlog0.log0** to open it for review.
- 6278 a. Left-click on the file name, and hold down Ctrl+C.
- 6279 b. Left-click anywhere in the **agentLog** folder, right-click and hold down Ctrl+V.
- 6280 7. Double-click the **Agent0.log-Copy.0** file to open it in your default text editor.
- 6281 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:
- 6282

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\jbservice\config\nlsamlpluginService.properties  
6286 Jul 13, 2015 4:59:21 PM com.bluejungle.pf.domain.destiny.serviceprovider.c A  
6287 FINE: Loading C:\Program Files\NextLabs\Policy  
6288 Controller\jbservice\jar\nlsamlplugin\NLSAMLPlugin-0.0.1-SNAPSHOT-jar-with-  
6289 dependencies.jar

6290 Jul 13, 2015 4:59:22 PM  
6291 com.bluejungle.pf.domain.destiny.serviceprovider.ServiceProviderManager  
6292 register  
6293 INFO: A new Service 'NLSAMLPlugin\_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:

```
Agent0.log.0 (13.8 MB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI C:\Program Files\NextLabs\Policy Controller\agentLog\Agent0.log.0 (13.8 MB)
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

6306 **10.10.3 Testing That the Protocol Broker .war File Loads Correctly in Tomcat Server**

6307 1. On the SharePoint Server, open Services, and ensure that the **Control Center Enforcer Service** is  
 6308 listed as **Running**.

6309 2. Using Windows Explorer, navigate to your Apache tomcat installation within the Windows file  
 6310 structure. Example: `C:/software/apache-tomcat-7.0.61`

6311 3. **Double-click to open the bin folder**. Example: `C:/software/apache-tomcat-7.0.61/bin`

6312 4. Double-click **startup.bat** to start the bat, and wait for startup to complete.

```

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.DefaultJarScanner.jarToSkip 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\apac
he-tomcat-7.0.61\webapps\SAMLProxy-0.0.1-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\apac
he-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\ap
ache-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\apac
he-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\ap
ache-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\apac
he-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\ap
ache-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\apac
he-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\ap
ache-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\apac
he-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\ap
ache-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

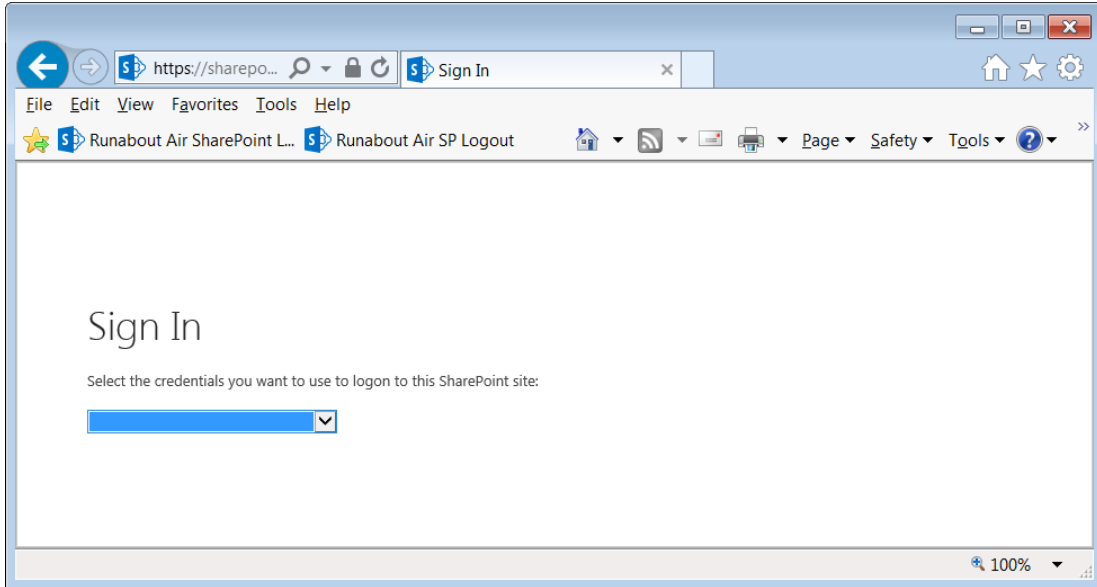
5. From any computer connected to this network, open an internet browser.

6315

6. In the address field, type *https://sharepoint.abac.test/* and press **Enter**.

6316

7. Choose **Federated Logon** from the drop-down menu.

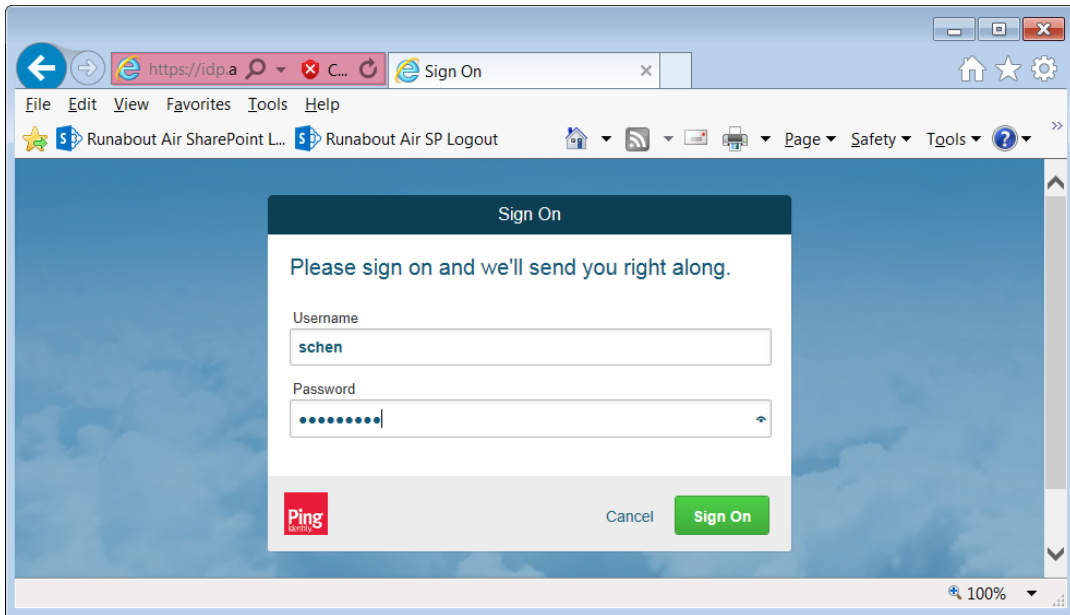


6317

6318

6319

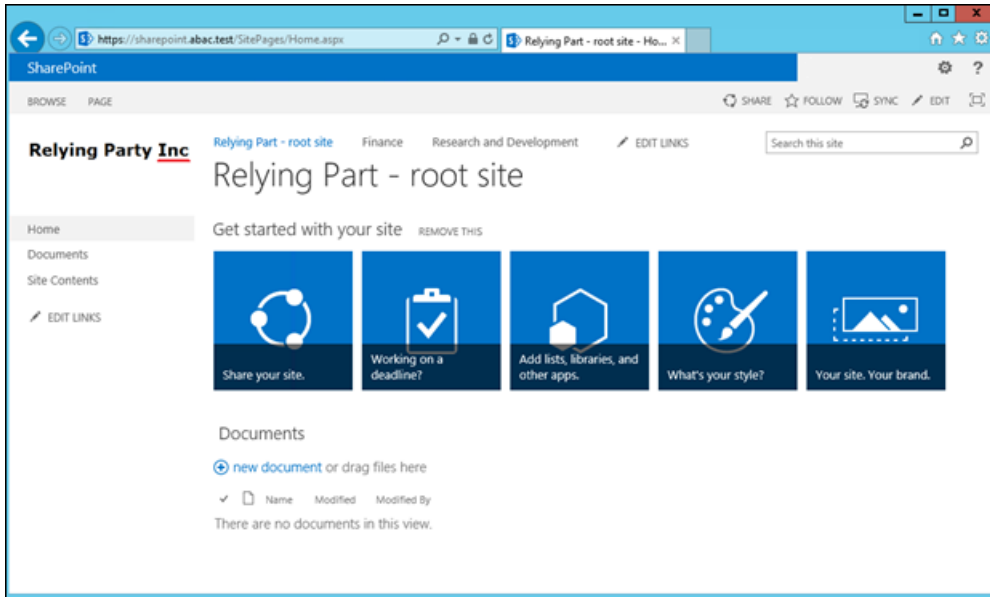
8. At the login screen, enter the credentials of a user that exists in your IdP Active Directory ([Section 2](#)), and click **Sign On**.



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:

6383 Jun 29, 2015 1:59:00 PM nist.pdpplugin.transport.SoapHTTPTransmitter transmit  
 6384 INFO: START SoapHTTPTransmitter method. Start time: 1435600740151  
 6385 Jun 29, 2015 1:59:08 PM nist.pdpplugin.transport.SoapHTTPTransmitter transmit  
 6386 INFO: START SoapHTTPTransmitter method. Start time: 1435600748229  
 6387 Jun 29, 2015 1:59:11 PM nist.pdpplugin.transport.SoapHTTPTransmitter transmit  
 6388 INFO: END SoapHTTPTransmitter transmit Method: 1435600751682  
 6389 Jun 29, 2015 1:59:11 PM nist.pdpplugin.transport.SoapHTTPTransmitter transmit  
 6390 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

6399 Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod  
 6400 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
6405      Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6406      getAttribute
6407      INFO: NLSAMLPlugin UserAttrProviderMod getAttribute Line00-72 - subjectID
6408      param: schen@abac.test
6409      Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6410      getAttribute
6411      INFO: NLSAMLPlugin UserAttrProviderMod getAttribute Line00-73 -
6412      attributeName param: clearance
6413      Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6414      getAttribute
6415      INFO: NLSAMLPlugin Trying to check if there exist a prior entry in cache.
6416      -- UserAttrProviderMod Line00-79
6417      Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6418      getAttribute
6419      INFO: NLSAMLPlugin Using soapHTTPTransmitter object and calling its
6420      transmit() function.
6421      Jun 3, 2015 11:39:22 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
6422      getAttribute
6423      INFO: NLSAMLPlugin UserAttrProviderMod getAttribute() Line00-114 --
6424      attributeValue returned: Secret
```