Attribute Based Access Control

Executive Summary

- Attribute based access control (ABAC) is an advanced method for managing access rights for people and systems connecting to networks and assets. Its dynamic capabilities offer greater efficiency, flexibility, scalability and security than traditional access control methods, without burdening administrators or users. In fact, Gartner recently predicted that "by 2020, 70% of enterprises will use attribute-based access control … as the dominant mechanism to protect critical assets, up from less than 5% today."[1]
- Despite federal guidance that comprehensively defines ABAC and the considerations for enterprise deployment[2], adoption of ABAC has been slow.
- The National Cybersecurity Center of Excellence (NCCoE) addressed this challenge by developing an example ABAC reference model using commercial products that can be included alongside those in your existing infrastructure.
- The ABAC solution provided by this "How to" guide incorporates relevant security characteristics, standards, and best practices from the National Institute of Standards and Technology (NIST) and other organizations.
- The guide demonstrates the implementation of standards-based cybersecurity technologies in the real world. It can save organizations research and proof of concept costs for mitigating risk through the use of context for access decisions.

THE CHALLENGE

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

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

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

[1] Market Trends: Cloud-Based Security Services Market, Worldwide, 2014, https://www.gartner.com/doc/2607617 [accessed August 21, 2015].
[2] National Institute of Standards and Technology Special Publication (SP) 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

THE SOLUTION

The NCCoE, part of NIST, demonstrated an advanced method, attribute based access control (ABAC), that uses granular attributes such as title, division, certifications and training—rather than a person's role—to authorize an individual's access. Access to an organization's network or assets can be made based on information that is available to systems across an organization, or among organizations, about a person, the action she wants to execute, and the resource she wants to access. An orthopedist responding to a mass casualty event in a neighboring state can quickly gain access to a hospital's patient records and radiology and pharmacy ordering systems, and only to those systems, based on authentication of her credentials and attributes such as employee status, medical specialization, and certifications. Additional visiting orthopedists are immediately granted the same permissions based on the same rules.

ABAC offers efficiencies and enhanced security in non-emergency scenarios, too. ABAC can provide separation of duties to help guard against fraud: a car insurance claims adjuster, for example, can be permitted to enter data about damage and generate a check, but only his supervisor can electronically sign the check. In addition to authorizing people, ABAC can be used to efficiently manage access among networked tools, devices, and systems that request access to corporate resources like applications, networks, systems, and data.

The NIST Cybersecurity Practice Guide *Attribute Based Access Control* shows how commercially available technologies can meet your organization's needs to make access decisions for a diverse set of people and things, including those seeking access from external organizations. The complete guide is available at http://nccoe.nist.gov.

Approach

In our lab at the NCCoE, we simulated a typical electronic file library with a diverse set of resources from different divisions in an organization. Different files have different security levels.

We demonstrated how detailed attributes can be assigned to users and networked resources, and how fine-grained environmental considerations like time of day or IP address can provide context for access decisions, allowing for more informed, finely-tuned access decisions that increase security.

The guide:

- maps security characteristics to guidance and best practices from NIST and other standards organizations
- provides
    - a detailed example solution with capabilities that address security controls
    - instructions for implementers and security engineers, including examples of all the necessary components and their installation, configuration, and integration
- uses products that are readily available and interoperable with existing information technology (IT) infrastructure and investments
- is suitable for organizations of all sizes

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee regulatory compliance. Your organization's security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution, or one that aligns to these guidelines, in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

BENEFITS

Our example solution:

- allows products and capabilities to be adopted on a component-by-component basis, or as a whole
- supports organizations with a diverse set of users and access needs, offering efficiencies in provisioning access
- reduces the number of identities managed by the enterprise, thereby reducing costs
- enables a wider range of risk-mitigation decisions by allowing organizations to define attribute-based policies for users and networked devices that include factors such as environment and time of day
- supports collaboration among organizations by allowing an enterprise to accept identities authorized by other enterprises, eliminating the need to pre-provision access for those identities
- supports the centralization of auditing and access policy management, creating efficiencies of policy management and reducing the complexity of regulatory compliance

SHARE YOUR FEEDBACK

You can get the guide at http://nccoe.nist.gov and help improve it 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. We recognize that technical solutions alone will not fully enable the benefits of ABAC, so we encourage organizations to share lessons learned and best practices for transforming the business processes associated with implementing ABAC.

- email abac-nccoe@nist.gov
- participate in our forums at https://nccoe.nist.gov/forums/attribute-based-access-control

Or learn more by arranging a demonstration of this reference solution by contacting us at abac-nccoe@nist.gov

TECHNOLOGY PARTNERS

The NCCoE designed and implemented this project with its National Cybersecurity Excellence Partnership (NCEP) partners.

Microsoft NEXTLABS®

PingIdentity® RSA® Symantec™

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based example solutions using commercially available technologies. As the U.S. national lab for cybersecurity, the NCCoE seeks problems that are applicable to whole sectors, or across sectors. The center's work results in publicly available NIST Cybersecurity Practice Guides that provide modular, open, end-to-end reference designs.

LEARN MORE
Visit http://nccoe.nist.gov

ARRANGE A DEMONSTRATION
nccoe@nist.gov
240-314-6800

NIST CYBERSECURITY PRACTICE GUIDE

ATTRIBUTE BASED ACCESS CONTROL

For CIOs, CISOs, and Security Managers

Approach, Architecture, and Security Characteristics

Bill Fisher Norm Brickman Santos Jha
Sarah Weeks Ted Kolovos Prescott Burden

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-3b

NIST Special Publication 1800-3b

ATTRIBUTE BASED ACCESS CONTROL

Bill Fisher

National Cybersecurity Center of Excellence
Information Technology Laboratory

Norm Brickman

Santos Jha

Sarah Weeks

Ted Kolovos

Prescott Burden

The MITRE Corporation
McLean, VA

Leah Kauffman, Editor-in-Chief

National Cybersecurity Center of Excellence
Information Technology Laboratory

April 2016

U.S. Department of Commerce

Penny Pritzker, Secretary

National Institute of Standards and Technology

Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, 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, materials, or equipment 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,44 pages (April 2016)
CODEN: NSPUE2

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

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

Public comment period: *September 30, 2016* through *December 4, 2016*

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices.

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

ABSTRACT

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

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Nate Lesser	NIST National Cybersecurity Center of Excellence
Paul Timmel	NIST National Cybersecurity Center of Excellence
Paul Grassi	NIST National Strategy for Trusted Identities in Cyberspace
Mike Garcia	NIST National Strategy for Trusted Identities in Cyberspace
Naomi Lefkovitz	NIST National Strategy for Trusted Identities in Cyberspace
Rene Peralta	NIST National Strategy for Trusted Identities in Cyberspace
Dave Ferriaolo	NIST Computer Security Division
Vincent Hu	NIST Computer Security Division
Roger Wiggenstam	NextLabs Inc
John Conduit	NextLabs Inc
Srikanth Karanam	NextLabs Inc
Adam Madlin	Symantec Corporation
Steve Kruse	Symantec Corporation
Steve Schmalz	RSA
Ben Smith	RSA
Andrew Whelchel	RSA
Chris Leggett	Ping Identity
Paul Fox	Microsoft Corporation
Derek Keatley	Microsoft Corporation
Hemma Prafullchandra	Hytrust
John McLeese	Hytrust

Name	Organization
Dave Cox	ID/Dataweb
Chris Donovan	ID/Dataweb

Contents

List of Figures

List of Tables

1 Summary

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

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

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

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

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

1.1 The Challenge

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

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

An advanced method of access management would increase security and efficiency by seamlessly limiting some users' views to more granular data. It would enable the appropriate permissions and limitations for

[1] National Institute of Standards and Technology Special Publication (SP) 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*

the same information system for each user based on individual attributes, and allow for permissions to multiple systems to be managed by a single platform, without a heavy administrative burden.

1.2 The Solution

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

1.3 Risks

Access control systems implement a process for defining security policy and regulating access to resources such that only authorized entities are granted access according to that policy. They are fundamental to mitigating the risk of unauthorized access not only from malicious external users and insider threats, but also from acts of misfeasance. In the absence of a robust access control system, enterprises struggle to control and audit access to their most sensitive data and risk the loss or exposure of critical assets, loss of trust in employees and from customers, and harm to brand reputation.

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

At the strategic level, organizations face risks associated with the acquisition, deployment, and maintenance of access control systems. These risks include the cost of the implementation and maintenance, any compliance or regulatory requirements, as well as a lack of preceding implementations from which to derive lessons learned.

1.4 Benefits

The example solution described in this guide has the following benefits:

- products and capabilities can be adopted on a component-by-component basis, or as a whole
- supports organizations with a diverse set of users and access needs, reducing the risks of “privilege creep” (a user obtains access levels beyond those needed), and creating efficiencies in the provisioning of accesses
- reduces the number of identities managed by the enterprise, and there by reducing costs associated with those management activities
- enable a wider range of risk-mitigation decisions by allowing organizations to define attribute-based policy on subjects and objects, but also using a variety of environmental decisions
- supports business collaboration, by allowing the enterprise to accept federated identities and eliminating the need to pre-provision access for identities being federated.

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

1.5 Technology Partners

The NCCoE designed and implemented this project with its National Cybersecurity Excellence Partner (NCEP). NCEPs are IT and cybersecurity firms that have pledged to support the NCCoE's mission of accelerating the adoption of standards-based, secure technologies. They contribute hardware, software, and expertise. In this project, we worked with:

- Ping Identity
- NextLabs
- Microsoft
- RSA
- Symantec

1.6 Feedback

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. 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. Your comments, suggestions, and success stories will improve subsequent versions of this guide.

- email abac-nccoe@nist.gov
- participate in our forums at https://nccoe.nist.gov/forums/attribute-based-access-control

Or learn more by arranging a demonstration of this example solution by contacting us at abac-nccoe@nist.gov

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based example solution and provides users with the information they need to replicate this approach to identity and access management. The example solution is modular and can be deployed in whole or in part.

This guide contains three volumes:

- *NIST SP 1800-3a: Executive Summary*
- *NIST SP 1800-3b: Approach, Architecture, and Security Characteristics* – what we built and why (this document)
- *NIST SP 1800-3c: How-To Guides* – instructions for building the example solution

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

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

- challenges enterprises face in implementing and using access control mechanisms
- example solution built at the NCCoE
- benefits of adopting ABAC, and the limitations of role based access (RBAC) systems

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

- Section 4.3, Risk Assessment, provides a detailed description of the risk analysis we performed.
- Section 4.4, Security Characteristics and Controls Mapping, maps the security characteristics of this example solution to cybersecurity standards and best practices.

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

IT professionals who want to implement an approach like this will find the whole practice guide useful. You can use the How-To portion of the guide, *NIST SP 1800-3c*, to replicate all or parts of the build created in our lab. The How-To guide provides specific product installation, configuration, and integration instructions for implementing the example solution.[1] We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution that would support the deployment of an ABAC system and the corresponding business processes. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with

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

applicable standards and best practices. Section 4.5, Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to abac-nccoe@nist.gov, and join the discussion at https://nccoe.nist.gov/forums/attribute-based-access-control.

3 Introduction

3.1 Background

Basic read, write, and execute permissions, along with discretionary access control (DAC) and mandatory access control (MAC) principles, mark the evolution of access control to the RBAC models that are in common commercial use today. While RBAC focuses primarily on the use of the role attribute, ABAC allows for access decisions based upon arbitrary attributes.

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

> "In its most basic form, ABAC relies upon the evaluation of attributes of the subject, attributes of the object, environment conditions, and a formal relationship or access control rule defining the allowable operations for subject-object attribute and environment condition combinations. All ABAC solutions contain these basic core capabilities that evaluate attributes and environment conditions, and enforce rules or relationships between those attributes and environment conditions."…
>
> "The rules or policies that can be implemented in an ABAC model are limited only to the degree imposed by the computational language. This flexibility enables the greatest breadth of subjects to access the greatest breadth of objects without specifying individual relationships between each subject and each object."[1] [2]

In order to enable ABAC implementations, the standards community has undertaken efforts to develop common terminology and interoperability across access control systems. One such standard is the eXtensible Access Control Markup Language (XACML)[3]. Built on an eXtensible Markup Language (XML) foundation, XACML is designed to allow externalized, run-time access control decisions using attribute-based policy definitions.

3.2 ABAC and RBAC Considerations

RBAC simplifies identity management by grouping users with similar access needs by role. Privileges can then be assigned to a role rather than an individual user. This simplification has led to the almost ubiquitous adoption of the RBAC model for logical access control. However, in the modern IT environment, enterprises face growing diversity in both types of users and their access needs. This diversity elucidates several limitations of the RBAC model.

This diversity introduces a number of administrative and policy enforcement challenges. Administrators manage access policy for multiple applications and security domains, with each often requiring discrete access control policies. Most systems implement access control in different ways, making it hard to share

[1] NIST, "Attribute Based Access Control (ABAC) - Overview". http://csrc.nist.gov/projects/abac/

[2] V.C. Hu, D. Ferraiolo, and R. Kuhn, et al., NIST SP 800-162,
Guide to Attribute Based Access Control (ABAC) Definition and Considerations, January 2014. http://nvl-pubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[3] OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version 3.0", 22 January 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

information across systems and requiring administrators to configure the access for like users uniquely in each system, typically by using the roles or groups native to that system.

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

Attribute-based systems, by the nature of their name:value pairs for each attribute, can support a much finer-grained authorization environment than an RBAC system. ABAC allows business logic to be translated into attribute-based policies that govern access decisions, allowing for a common and centralized way of expressing policy and computing and enforcing decisions, over the access requests for diverse systems. These policies include the ability to take environmental considerations into account when making access decisions.

Attribute policy definitions establish a relationship between subject and object that does not change as attribute values change, thus reducing the opportunity for privilege creep and maintaining separation of duties. ABAC systems have the ability to permit new types of access requests without the need to alter the current set of subject/object relationships. Instead, the enterprise can define a new attribute or attributes (or a combination of currently used attributes) that represents the new level of access needed and then define an attribute-based policy that supports this level of access.

3.3 ABAC Leveraging Identity Federation

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

Identity federation profiles define the methods used to convey a set of user information from the Identity Provider (IdP), or organization where the user is known, to the target location or Relying Party (RP) that needs to acquire the information for some use such as access control. These technologies leverage widely accepted, open, Web-oriented standardized communication languages, like the Security Assertion Markup Language (SAML) version 2.0 standard from OASIS[1], which uses XML, or the OpenID Connect (OIDC) standard from the OpenID Foundation[2] built upon JavaScript Object Notation (JSON), to carry the assertions about a user. Federation profiles allow identity and attribute information to be sent over Hypertext Transfer Protocol (HTTP) in a manner that can be understood and used by the receiving organization (the RP) to make access control decisions.

[1] OASIS Standard, "OASIS Security Assertion Markup Language (SAML) V2.0", March 15, 2005. http://saml.xml.org/saml-specifications

[2] OpenID Foundation, "OpenID Connect Core 1.0", November 8, 2014. http://openid.net/specs/openid-connect-core-1_0.html

In some cases an RP may need to obtain attributes about a user from a source other than the user's IdP. In this case the RP may receive a user's attributes from a trustworthy external source known as an Attribute Provider (AP). Commonly, identity federation profiles are used to facilitate the federation of attributes from the AP to the RP.

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

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

3.4 Security Standards

Table 3.1 Related Security Standards and Best Practices

Related Technology	Relevant Standard	URL
General Cybersecurity	NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
	NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
	ISO/IEC 27001, Information Security Management	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
	SANS Institute, Critical Security Controls	https://www.sans.org/critical-security-controls/
	ISACA, COBIT 5	http://www.isaca.org/COBIT/Pages/Product-Family.aspx
	Cloud Security Alliance, Cloud Controls Matrix v3.0.1	https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
Risk Management	NIST SP 800-30- r1, Risk Management Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

Table 3.1 Related Security Standards and Best Practices (Continued)

Related Technology	Relevant Standard	URL
Requirements Engineering	ISO/IEC 15288:2015, Systems and software engineering - System life cycle processes	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711
	NIST SP 800-160 (Draft), Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems	http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf
Access Control (ABAC)	NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations	http://dx.doi.org/10.6028/NIST.SP.800-162
Access Control (NGAC)	INCITS 499-2013, Information Technology - Next Generation Access Control - Functional Architecture (NGAC-FA)	http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+499-2013
Access Control (RBAC)	American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS) 359-2012, Information Technology - Role Based Access Control	http://www.techstreet.com/products/1837530
Language (OIDC)	OpenID Connect Core 1.0	http://openid.net/specs/openid-connect-core-1_0.html
Language (SAML)	OASIS Security Assertion Markup Language (SAML) V2.0	http://saml.xml.org/saml-specifications
Language (WS-Federation)	OASIS Web Services Federation Language (WS-Federation) Version 1.2	http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html
Language (XACML)	eXtensible Access Control Markup Language (XACML) Version 3.0	http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
Language (XML)	Extensible Markup Language (XML) 1.1 (Second Edition)	http://www.w3.org/TR/2006/REC-xml11-20060816/
Protocol (HTTP and HTTPS)	RFC 7230, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	https://tools.ietf.org/html/rfc7230
Protocol (LDAP)	RFC 4510, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map	https://tools.ietf.org/html/rfc4510
Protocol (OAuth)	IETF Request for Comments 6749, The OAuth 2.0 Authorization Framework	http://tools.ietf.org/html/rfc6749

Table 3.1 Related Security Standards and Best Practices (Continued)

Related Technology	Relevant Standard	URL
Protocol (TLS)	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246
	RFC 2246, TLS Protocol 1.0	https://tools.ietf.org/html/rfc2246
	RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1	https://tools.ietf.org/html/rfc4346
	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246
PKI	PKI Technical Standards	http://www.oasis-pki.org/resources/techstandards/

4 Approach

4.1 Audience

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

4.2 Scope

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

In response, the NCCoE drafted a white paper[1] that identified numerous desired solution characteristics. After two rounds of public comments on the document, the NCCoE worked with its NCEP to design an architecture that would demonstrate an array of ABAC capabilities. This build does not include every characteristic found in the white paper, but does include the relevant set of ABAC capabilities[2] based on the technology available to us through the portfolios of the NCCoE's National Cybersecurity Excellence Partners. The scope of this build is the successful execution of the following capabilities:

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

4.2.1 Assumptions

The ABAC build described here incorporates the assumptions in this section.

4.2.1.1 Modularity

This example solution is made of many commercially available parts. You might swap one of the products we used for one that is better suited for your environment. We also assume that you already have some IdAM solutions in place. The use of standard protocols such as SAML, LDAP, and WS-Federation enhances the modularity of the architecture to improve your identity and access/authorization functions without major impact to your existing infrastructure. For organizations that want to limit their ABAC deployment

[1] Fisher, William. *Attribute Based Access Control*, Version 2. NCCoE. April 1, 2015. https://nccoe.nist.gov/sites/default/files/documents/NCCoE_ABAC_Building_Block_v2_final.pdf

[2] This project has the overarching goal of demonstrating technical implementations of standards-based ABAC functionality. In enumerating technology relevant to this effort, we worked closely with experts from the identity and access management community. During those discussions, we realized the complementary nature of identity federation when coupled with an ABAC implementation. Identity federation on its own does not constitute an ABAC solution and an ABAC solution does not rely upon identity federation. Future builds under this project name may or may not include examples of identity federation.

to only those resources residing on Microsoft SharePoint, this solution can be implemented alongside an RBAC implementation, with the lone configuration requirement of enabling attributes inside Microsoft Active Directory or other identity stores as appropriate.

4.2.1.2 Business Policy Language

This build leverages NextLabs technology to decompose natural language business policy into attribute-based digital policies. We implemented example business policies that we feel demonstrate the capabilities of the solution that address business needs. When implementing an ABAC solution, enterprises will need to determine the set of natural language business policies that best meet their access control needs and risk tolerances.

4.2.1.3 Attribute Semantics and Syntax

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

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

4.2.1.4 Attribute Provenance

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

4.2.1.5 Trust Relationships for Identity Federation

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

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

4.2.1.6 Human Resources Database/Identity Proofing

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

4.2.1.7 Technical Implementation

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

4.2.1.8 Limited Scalability Testing

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

4.3 Risk Assessment

According to NIST Special Publication (SP) 800-30-r1, "Risk Management Guide for Information Technology Systems", "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of the Risk Management Framework (RMF) material available to the public. The RMF guidance as a whole proved invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

Using the guidance in NIST's series of SPs concerning the RMF, the NCCoE worked with IdAM SMEs to enumerate areas of access management risk facing today's enterprise. We deemed these the tactical risks:

- not implementing or maintaining least privilege for all users
- access rights accumulation violates the separation of duties
- digital identities of external users become orphaned
- authorization policies cannot account for the context of access request

In addition to tactical risk, enterprises face a series of business risks that are influenced by the acquisition, deployment, and maintenance of IdAM systems. We deemed these the strategic risks:

- cost of implementation
- budget expenditure as they relate to investment in security technologies
- compliance with existing industry standards
- risk of alternative or no action
- lack of successful precedents

We translated this risk information to security characteristics. We mapped these characteristics to NIST's SP 800-53 Rev.4 controls where applicable, as well as other relevant industry and mainstream security standards.

4.4 Security Characteristics and Controls Mapping

Table 1 lists the major use case security characteristics. For each characteristic, the table provides the matching function, category, and subcategory from the NIST Cybersecurity Framework (CSF)[1], as well as mappings to controls from other relevant cybersecurity standards.

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[a]	ISO/IEC 2700[b]	SANS CSC[c]	ISACA COBIT 5[d]	CSA CCMv3.0.1[e]
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 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	CSC 16-16, CSC 17-7		EKM-03, IVS-10, DSI-03

[1] NIST, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0”, February 12, 2014. http//www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Table 4.1 Use Case Security Characteristics Mapped to Relevant Standards and Controls (Continued)

Security Characteristics	CSF Function	CSF Category	CSF Subcategory	NIST SP 800-53 rev4[a]	ISO/IEC 2700[b]	SANS CSC[c]	ISACA COBIT 5[d]	CSA CCMv3.0.1[e]
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	CSC4-2,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

a. NIST, SP 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations”, April 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

b. ISI/IEC, ISO/IEC 27001, “Information Security Management”. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

c. SANS Institute, “Critical Security Controls”.https://www.sans.org/critical-security-controls/

d. ISACA, “COBIT 5”. http://www.isaca.org/COBIT/Pages/Product-Family.aspx

e. Cloud Security Alliance (CSA), “Cloud Controls Matrix v3.0.1”.https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

4.5 Technologies

Table 4.2 provides a breakout of the contents of table 4.1 organized by the products used within this build. This breakout shows the security controls coverage that each product supports.

Table 4.2 Use Case 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 Active Directory, 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 Active Directory	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

Table 4.2 Use Case Security Characteristics Mapped to Relevant Build Products

Security Characteristics	Product(s)	CSF Subcategory	NIST SP 800-53r4	ISO/IEC 27001
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, 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

This build implements the security characteristics through available products, described below, from NCEP organizations.Section 5, Architecture, provides additional insight into the way we used the products.

- The build is centered on a resource server to be protected by the ABAC solution. In this case, Microsoft SharePoint was used. It is a web-based application within the Windows operating environment commonly, SharePoint is deployed as a document management system for intranet, extranet, or cloud repository purposes. SharePoint natively uses an RBAC authorization environment, but it also supports the use of attributes within the user transaction request, a capability Microsoft refers to as being “claims aware.” SharePoint also allows for tagging data within its repository, which can be leveraged as object attributes.
- Another important component of the build is identity management software, in this case, Microsoft Active Directory (AD). AD is a set of services that reside within the Windows server environment. AD functions as an identity repository based on LDAP technology, but also provides authentication and authorization services. AD also includes the ability to provision and de-provision user identities and the creation, modification, and deletion of subject attributes.
- The build needed PEP functionality. It is provided by NextLabs Entitlement Management, which interfaces and integrates with products like SharePoint and SAP to provide finer granularity of access decisions than that available using the native access control mechanisms. Entitlement Management is closely coupled with the target application. It traps user access requests and passes access decisions to the policy decision point (PDP).
- Policy lifecycle management and auditing/reporting are facilitated by the NextLabs Control Center, which hosts policy administration point (PAP) functionality, where attribute-based policies are defined and deployed. The NextLabs Policy Controller, as an element of Control Center, hosts the PDP, which uses the policy definitions and subject, object, and environmental attributes to make an access accept-or-deny decision that the PEP enforces. Control Center also includes dashboards, analytics, reports, and monitoring to offer insight into access patterns.

- The build includes a federation server/platform for exchanging identities and attributes. Ping Identity's PingFederate serves as a federation identity system or trust broker, an identity management component, and supports integrated single-sign-on (SSO) within an enterprise IdAM infrastructure. It supports standards-based protocols such as SAML, OAuth, and OpenID Connect. Its trust broker capabilities allow for necessary transformation and interface options between federated partners and internal proprietary target resources. When used within an identity provider, it offers options for integrating with authoritative attribute sources.
- The build has an authentication server that supports multifactor authentication. For this build, RSA Adaptive Authentication (AA), which is an authentication and environmental analysis system, provides this functionality. Its capabilities include a variety of adaptive opportunities, such as SMS texting, fingerprint analysis, and knowledge-based authentication. From an environmental perspective, AA collects information such as patch level, operating system, and location, and generates a risk score associated with user authentication. A risk score threshold can then be defined, which, if exceeded, can force a user to step up to an additional authentication mechanism.
- A final necessary component of the build is a certificate authority. In this case Symantec's Managed PKI Service product is used for secure issuance of PKI-based certificates. The Symantec certificates enable mutual transport layer security (TLS), digital signatures, and any explicit encryption that is in use outside of TLS, such as for data-at-rest within an IT environment.

5 Architecture

5.1 Overview

The following sections detail the ABAC and identity federation[1] architecture that NCCoE staff members and collaborators built. The architecture description details how components from five NCEPs were integrated to achieve the following demonstrable capabilities:

5.1.1 User Authentication and the Creation of an Authentication Context

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

5.1.2 Federation of a User Identity and Attributes

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

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

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

5.1.4 The Creation of Attribute-Based Policy Definitions

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

5.1.5 Secondary Attribute Requests

This build provides the ability to make runtime requests for additional attributes from the IdP, should insufficient attributes be presented when making an access decision. When a user accesses a particular

[1] This project has the overarching goal of demonstrating technical implementations of standards-based ABAC functionality. In enumerating technology relevant to this effort, we worked closely with experts from the identity and access management community. During those discussions, we realized the complementary nature of identity federation when coupled with an ABAC implementation. Identity federation on its own does not constitute an ABAC solution and an ABAC solution does not rely upon identity federation. Future builds under this project name may or may not include examples of identity federation.

resource, or returns to access additional resources, the access control components that we have associated with SharePoint might find that additional subject attributes are needed beyond those that were initially provided. Our build includes components able to search a local cache for the missing attributes and if not there, issue a new request to the IdP via a SAML attribute request/response for the missing user attributes.

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

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

5.2 ABAC Architecture Considerations

There are many facets to architecting an ABAC system. As noted in section 4.2.1, Assumptions, these include the development of policy, procedure, and/or functional requirements before the selection of technology components. Organizations wishing to implement an ABAC system should conduct robust requirements engineering, taking into consideration the operational needs of each system stakeholder. Standards such as ISO/IEC 15288:2015, *Systems and software engineering - System life cycle processes*[1] and NIST SP 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*[2] provide guidance in this endeavor.

From a technical perspective, this section outlines a few of the options that an architect will face, and section 5.2.6, Architecture Diagram and Components, presents the actual architecture chosen for this build.

5.2.1 Industry Standards

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

As mentioned earlier, one of the standards for implementing ABAC is XACML. Built on top of XML, XACML offers a core set of rule capabilities for making attribute-based policy definitions and also specific request and response messages for exchange between PEPs and PDPs. Specific details of the XACML 3.0 architecture can be found in the OASIS documentation.[3]

[1] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711

[2] NIST, SP 800-160, *Systems Security Engineering (Draft)*, May 2014. http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

[3] OASIS Standard, “eXtensible Access Control Markup Language (XACML) Version 3.0”, 22 January 2013. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

Although XACML was developed primarily to fill the need for a standard ABAC protocol, other standard protocols and architectures may be relevant to ABAC use cases. Next Generation Access Control[1], developed by the International Committee for Information Technology Standards, outlines an access control architecture that supports the use of attributes. OAuth 2.0[2], ratified by the Internet Engineering Task Force (IETF), serves as a rights delegation protocol that grants access to protected resources by defining the allowable user actions for those resources referred to as "scopes."

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

5.2.2 PEP Placement

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

- closely coupling it within a software program
- using an agent to front-end a web browser-based application
- placing it at an enterprise gateway position in order to ABAC-enable a set of applications

The PEP may also be asked to perform additional functions that require a specific PEP placement. Under the XACML standard, the PEP can be configured to handle "out-of-band" instructions known as obligations (mandatory directives) and advice (optional). These instructions trigger secondary actions in addition to the access decision enforcement. An example of an obligation would be where a person was allowed access to a target resource, but the PEP is directed to initiate a royalty payment for its use.

5.2.3 PDP Distribution

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

[1] INCITS, INCITS 499-2013, *Information Technology - Next Generation Access Control - Functional Architecture (NGAC-FA)*. http://webstore.ansi.org/RecordDetail.aspx?sku=INCITS+499-2013

[2] IETF, Request for Comments (RFC) 6749, *The OAuth 2.0 Authorization Framework*, October 2012. http://tools.ietf.org/html/rfc6749

5.2.4 Multi-Vendor

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

5.2.5 Caching

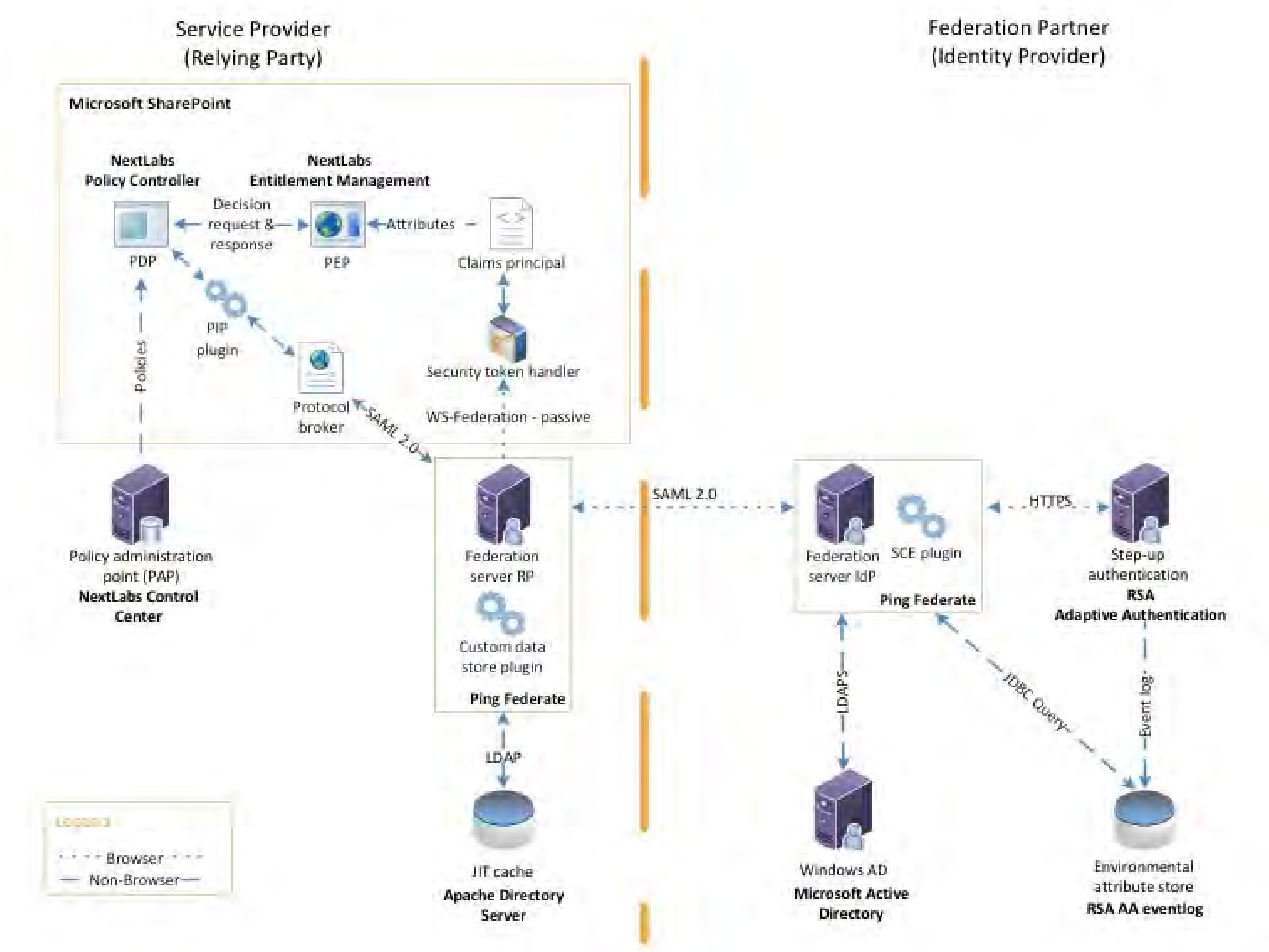
There are several locations in an ABAC system implementation for an architect to consider the use of memory caching to improve performance. Considerations include caching decisions at the PEP, rules at the PDP, and user attributes at the RP.

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

5.2.6 Architecture Diagram and Components

Figure 5.1 illustrates the logical interactions of the components in this build. Interactions are broken down into browser-based or non-browser-based communications. All components in this build are either commercially available through the applicable vendor or can be found publicly with the release of this practice guide.

Figure 5.1 ABAC Build 1 Architecture



The components in figure 5.1, which were available products from NCEP organizations that met the build's functional requirements, provide the following capabilities to this build:

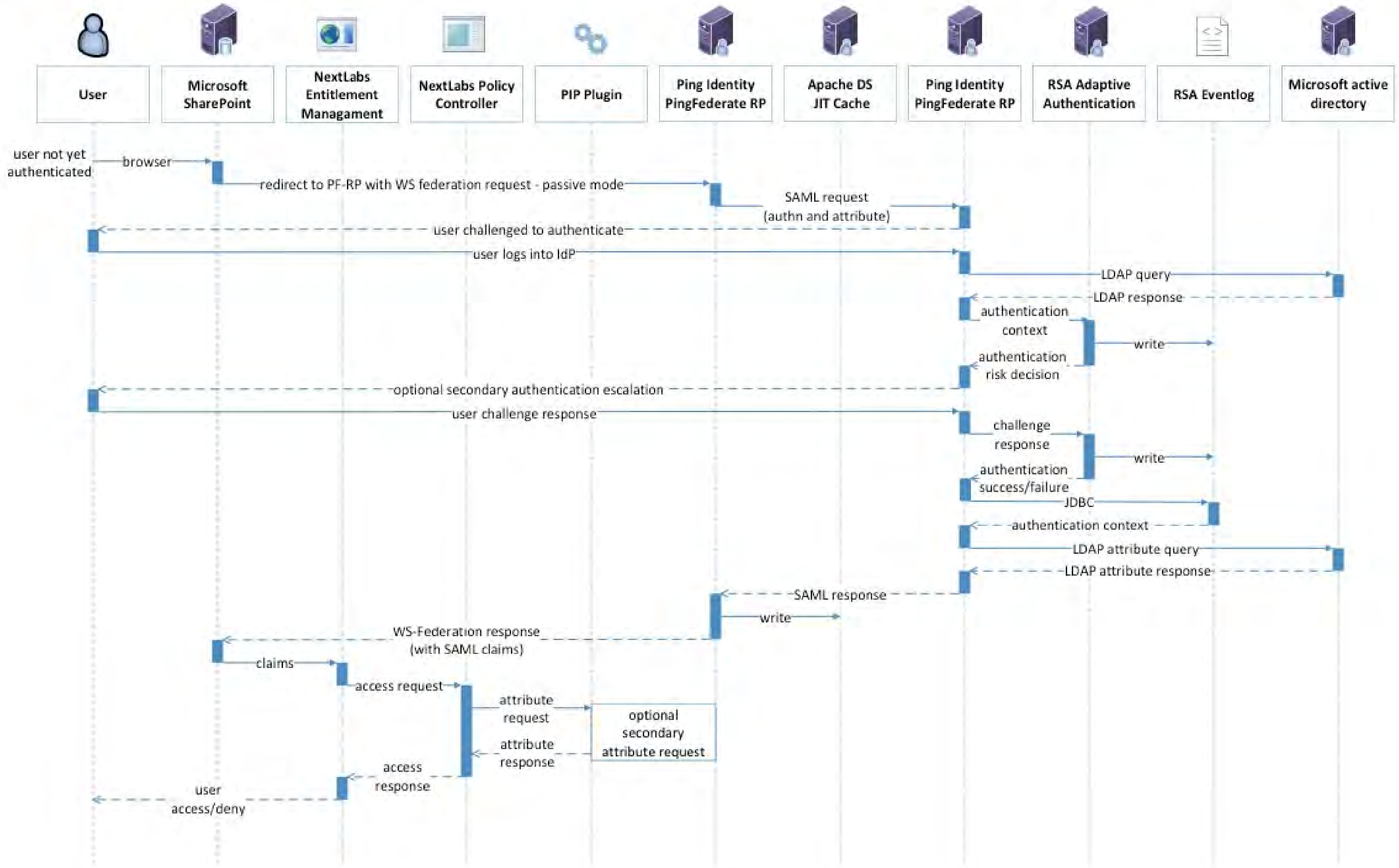
- Microsoft AD acts as a user identity management repository for the IdP. This includes the ability to provision and de-provision user identities; the creation, modification, and deletion of subject attributes; and the provisioning and de-provisioning of subject attributes to specific user identities. In this build, AD is the only source for subject attributes.
- RSA AA gathers environmental information about the user and the user's system or agent at the time of authentication. AA collects information such as patch level, operating system, and location, and it generates a risk score associated with the user authentication. A risk score threshold can then be defined in AA, which, if exceeded, can force a user to step up to one of the additional authentication mechanisms. In this build, information collected by AA to generate a risk score is also passed through PingFederate-IdP to the RP side of the operation to be used as environmental attributes.
- The RSA AA event log contains the transaction ID of each user authentication and the associated environmental information collected by RSA AA at the time of authentication.
- Ping Identity PingFederate-IdP serves as a federation system or trust broker for the IdP. PingFederate-IdP provides initial user authentication and retrieval of user attributes to satisfy SAML requests from the RP. Once the user has been authenticated, PingFederate-IdP queries subject attributes from AD and environmental attributes from the RSA AA event log. PingFederate-IdP packages both subject and environmental attributes in a SAML 2.0 token to be sent to the RP.
- The SCE Plugin is an RSA component that handles communications between the PingFederate-IdP and the RSA AA. It is responsible for passing the RSA AA transaction ID for the user authentication that PingFederate-IdP uses to query the RSA AA event log.
- Ping Identity PingFederate-RP serves as the trust broker for SharePoint. When the user requires authentication, PingFederate-RP redirects the user to the IdP via a SAML request to get the necessary assertions. Once authenticated, PingFederate-RP arranges for the browser's HTTPS content to have the proper information in proper format for acceptance at the target resource (SharePoint). PingFederate-RP has the option to utilize the Apache Directory Server as a just-in-time (JIT) cache. Secondary attribute requests can also be made by PingFederate-RP via a SAML query initiated by the PIP Plugin and the Protocol Broker.
- Microsoft SharePoint serves as a typical enterprise repository and in this build, it stores the target resources that users wish to access. SharePoint natively uses an RBAC authorization environment, but it also supports the use of attributes, a capability Microsoft refers to as “claims aware.” SharePoint accepts assertions from PingFederate-RP and stores asserted attributes as claims. SharePoint also allows for the tagging of data within its repository, which can then be leveraged as object attributes.
- Microsoft SharePoint Security Token Handler resides inside of SharePoint, validating the token sent by PingFederate-RP.
- Microsoft SharePoint Claims Principal is the object inside of SharePoint where attribute assertions are stored as claims.
- NextLabs Entitlement Management is closely coupled with SharePoint. It performs the PEP functionality, trapping user access requests. As the PEP, Entitlement Management is responsible for gathering object attributes from SharePoint and subject and environmental attributes from the claims principal at the time of the access request. Entitlement management then passes this information in the form of an access decision request to the NextLabs Policy Controller.

- NextLabs Policy Controller is a component of the NextLabs Control Center that is closely coupled with the SharePoint instance. The Policy Controller is responsible for providing PDP capabilities. The Policy Controller receives attribute-based policies from the Control Center and uses these policies to respond to access requests from Entitlement Management.
- NextLabs Control Center serves as the PAP, where attribute-based policies are created, updated, and deployed using a built-in graphical user interface (GUI). The Control Center also provides auditing, logging, and reporting functions for the SharePoint access requests and decisions.
- PIP Plugin is a software extension of NextLabs Policy Controller that enables it to acquire unavailable attributes required for policy evaluation at run time from RP or IdP by communicating with Protocol Broker on an HTTPS channel protected by mutual TLS.
- Protocol Broker is a Web application that retrieves attribute values by accepting attributes to be queried from the NextLabs Plugin and querying the PingFederate-RP by issuing a SAML 2.0 Assertion Query/Request.
- The Custom Data Store is a plugin built using PING SDK that enables the RP to query the IdP and provides the resulting attribute value back to the Ping Federate RP.
- The Apache Directory Server is an LDAP version 3-compliant directory server developed by the Apache Software Foundation that works as a JIT cache for PingFederate-RP. It stores subject attributes and other relevant information from the SAML 2.0 response that an RP receives from an IdP.
- Symantec Trust Center Account for Enterprise is used for secure issuance of PKI-based certificates throughout this build. The Symantec certificates enable mutual TLS, digital signatures, and any explicit encryption that is in use outside of TLS, such as for data-at-rest in the RP’s JIT cache.

5.2.7 UML Diagram

The architecture shown in figure 5.1 can, in practice, support different types of sequential operations. We have chosen to initially implement, demonstrate, and document two generic types of sequential ABAC operations as being representative of the core operations of the architecture. Figure 5.2 contains a ladder diagram that represents the initial flow of the ABAC architecture, where an unauthenticated user tries to access a resource on SharePoint.

Figure 5.2 UML Sequence Diagram


User
Microsoft SharePoint
NextLabs Entitlement Managament
NextLabs Policy Controller
PIP Plugin
Ping Identity PingFederate RP
Apache DS JIT Cache
Ping Identity PingFederate RP
RSA Adaptive Authentication
RSA Eventlog
Microsoft active directory
user not yet authenticated
browser
redirect to PF-RP with WS federation request - passive mode
SAML request (authn and attribute)
user challenged to authenticate
user logs into IdP
LDAP query
LDAP response
authentication context
write
authentication risk decision
optional secondary authentication escalation
user challenge response
challenge response
write
authentication success/failure
JDBC
authentication context
LDAP attribute query
LDAP attribute response
SAML response
write
WS-Federation response (with SAML claims)
claims
access request
attribute request
optional secondary attribute request
attribute response
access response
user access/deny

The sequence starts in the top of figure 5.2 when a user browses to, and attempts to access, a protected resource in SharePoint.

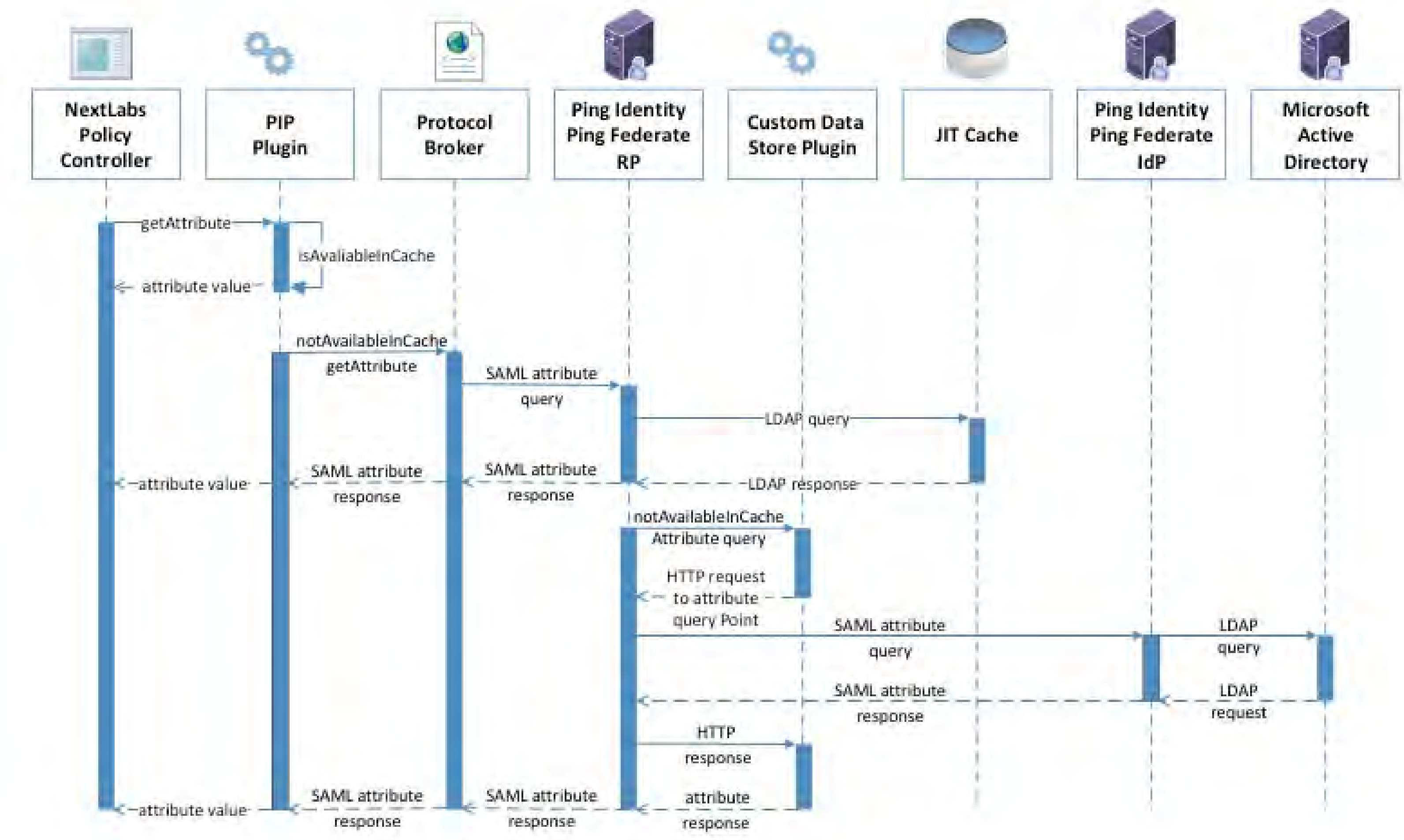
1. SharePoint inspects the user’s HTTP content and finds that the user has not been previously logged in (i.e., not authenticated), and therefore re-directs the browser to PingFederate-RP via use of the WS-Federation protocol.
2. The WS-Federation request is interpreted by PingFederate-RP as a request for authentication and for attributes, and the user is redirected to PingFederate-IdP carrying a SAML authentication request and SAML attribute request.
3. PingFederate-IdP does an initial (single factor) authentication of the user, and, if successful, receives the requested subject attributes.
4. PingFederate-IdP then redirects the user’s browser to RSA AA to enhance the initial authentication.

   Note: In practice this secondary authentication can be conditionally done based upon the type of protected resource for which access is requested or upon other conditions such as environment. The current installation always calls for the second level of authentication to demonstrate what is known as multi-factor authentication (MFA), and for this build achieves it via sending an SMS text message and expecting a particular response. The RSA AA product has additional options that are not being demonstrated at this time.
5. Upon successful completion of the MFA operation, the user is redirected back to PingFederate-IdP. At this time, PingFederate-IdP can query the RSA AA event log for environmental attributes that add context to the authentication.
6. PingFederate-IdP issues a SAML 2.0 token containing the user's identity and attribute information, and redirects the user's browser to PingFederate-RP.
7. PingFederate-RP accepts the SAML 2.0 response and issues a WS-Federation response back to SharePoint with the HTTP carrying the authentication and attribute information.

   At this point the user’s browser is issued a “FedAuth” cookie, establishing a session with SharePoint, and resides there until the session is terminated. The rest of this flow occurs as communications internal to the RP or as web service calls back to the IdP, unbeknownst to the user. Once this session is established, the system is configured to allow the NextLabs components to handle access requests to SharePoint. After the WS-Federation response, the subject and environmental attributes from the IdP are stored in the SharePoint Claims Principal.
8. Access requests by the authenticated user are now trapped by the NextLabs Entitlement Management PEP, which gathers the subject and environmental attributes stored in the Claims Principal and the object attributes stored in SharePoint, and submits the access request to the Policy Controller PDP for adjudication.
9. The Policy Controller uses the attributes provided by the PEP and the policy established by the Control Center to determine an access allow or deny. If the PDP is not presented with enough attributes to make an access decision, it has the option of initiating a secondary attribute query, which is detailed in Figure 3 and discussed later.
10. Once an access decision has been made, the Policy Controller responds back to the Entitlement Management PEP, which enforces the decision.

Figure 5.3 contains a ladder diagram that represents a flow of this ABAC architecture where an authenticated user tries to access a resource on SharePoint but there is a need to initiate a secondary attribute request. If needed, this flow is initiated by the NextLabs Policy Controller in Step 9.

Figure 5.3 Secondary Attribute Request Flow



The basic steps of the figure 5.3 flow:

1. When the policy controller does not receive the attributes required to make a decision, a secondary attribute request will be initiated by calling the PIP Plugin.
2. PIP Plugin is a registered plugin with the NextLabs Policy Controller. It implements the interface dictated by the NextLabs software. By virtue of this implementation it receives the subject and name of the attribute that is required for the policy decision.
3. When the subject and attribute name are received, the PIP Plugin checks its local short-term cache (in this build, configured to hold values for two seconds) to see if the needed attribute for the subject was recently requested.
4. If the attribute is still in cache, the value is returned to the Policy Controller. If the value is not in cache, the PIP Plugin initiates an HTTPS request to the Protocol Broker.
5. The Protocol Broker receives the attribute name and subject from the HTTPS request and forwards them as a signed SAML 2.0 Attribute Query to PingFederate-RP on a channel protected by mutual TLS.
6. Once PingFederate-RP receives the SAML 2.0 attribute query, it sends an LDAP request to the JIT cache to see if the attribute was previously queried in a secondary request.
7. If the subject does not have the attribute value assigned in the JIT cache, PingFederate-RP will forward the subject and attribute name to the Custom Data Store plugin. The Custom Data Store plugin acts as a pointer back to the PingFederate-IdP. To do this, the Custom Data Store dispatches an HTTPS request to the PingFederate-RP with the PingFederate-IdP as the attribute query point.
8. Ping Federate uses an HTTPS query to form a SAML 2.0 attribute query and dispatch it to the Ping Federate at the IdP.
9. The Ping Federate at the IdP accepts the SAML 2.0 request, verifies if the user has the attribute of need, and replies back to the PingFederate-RP with a SAML 2.0 response.
10. PingFederate-RP validates the SAML 2.0 response, retrieves attribute values, and responds to the original Custom Data Store HTTP request with the attribute values.
11. The Custom Data Store then responds to the PingFederate-RP attribute request with an attribute response.
12. The PingFederate-RP constructs a SAML 2.0 response and sends it to the Protocol Broker.
13. The Protocol Broker retrieves the attribute or exception from the SAML 2.0 response and forwards it to the NextLabs plugin, which in turn passes the attribute or exception back to the Policy Controller.

5.2.8 NCCoE Design Considerations

Section 5.2, ABAC Architecture Considerations, outlined the architectural topics and options that entered into our decision making for this first ABAC build and demonstration. Now that the chosen ABAC functionality has been described and the flow and sequencing explained, in this sub-section we summarize the architectural directions that were chosen for this particular build, and why.

5.2.8.1 Industry Standards

The use of XACML and its importance to ABAC functionality was introduced in section 5.2.6. Its core parts are the request/response protocol between PEP and PDP, the rule language, and the use of obligation and advice that the PDP can forward to the PEP. Use of a standard like XACML gives an IdAM infrastructure implementation potential cost saving as heterogeneous interchangeability of operational components can be more easily implemented.

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

SAML 2.0 core was used within the SAML Web SSO exchange, but was also used as a standalone for its request/response protocol for backend attribute exchanges of NextLabs’ PIP Plugin to and from PingFederate-RP (via the Protocol Broker), and for back-end attribute exchanges from PingFederate-IdP to PingFederate-RP.

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

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

5.2.8.2 PEP Placement

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

5.2.8.3 PDP Distribution

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

5.2.8.4 Multi-Vendor

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

5.2.8.5 Caching

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

- NextLabs PIP Plugin contains a local cache, developed using the EhCache library. This cache stores attributes for 2 seconds and adds efficiency to the system should multiple requests for the same subject and attribute value pairing occur in quick succession (with 2 seconds).
- A JIT cache was developed for PingFederate-RP, using Apache Directory Server. It is used to cache user attributes that are retrieved by PingFederate-RP for a finite time (such as up to 24 hours) to avoid future repeated secondary attribute calls to the IdP.

5.3 Security Characteristics

In this section we re-introduce the security characteristics and security controls that were first introduced in Sections 4.4 and 4.5, and relate each here to the NCEP partner products that are being used in this ABAC build.

- Identity and Credentials and Their Use for Authorized Devices. In NIST SP 800-53 this is tied to AC-1, and in the NIST Cybersecurity Framework to PR.AC-1: “Identities and credentials are managed for authorized devices and users.” In this build, both user and system identities are managed to ensure linkage with these security controls. Where applicable systems are given PKI-based credentials for use with TLS via the Symantec Managed PKI Service. User authentication in this first build is MFA with one factor being name and password via PingFederate-IdP and AD, while the second is an SMS text message sent to a cellular device conducted by the RSA AA. The RSA AA system offers other options for use as the second factor of authentication through its multi-credential framework.
- Remote Access Being Managed. Several of the NCEP products are involved in ensuring efficient and secure remote access. The two Ping Identity PingFederate installations have federation and authentication features that allow the RP to accept external identities for remote access. SharePoint via WS-Federation trusts external identities sent from PingFederate. NextLabs products enable ABAC functionality for SharePoint access decisions and allow for the auditing and logging of access requests.
- Access Permissions. ABAC systems manage access permissions by defining attribute-based rules that specify what subject attributes are needed to access resources with a given set of object attributes, under a set of environmental conditions. In this build, this functionality is handled by NextLabs products. A NextLabs Control Center allows for creation of attribute-based policies and makes access decisions based on those policies via its Policy Controller.
- Encryption and Digital Signature. Browser-based communications with SharePoint are HTTPS-based, and LDAP is used for all interfacing with AD. All system endpoints are equipped with PKI certificates issued by the Symantec Managed PKI Service, and TLS is in use for system-level point-to-point transactions. Examples include full encryption of SAML request/response transactions such as between PingFederate-RP and PingFederate-IdP.
- Provisioning. Identities are provisioned, stored, and de-provisioned inside of AD. This process occurs manually through the native Microsoft Windows Server GUI. AD also handles the assigning of subject attributes to specific user identities.

  Object attributes are provisioned via SharePoint. SharePoint sites or individual files can be “tagged” with object attributes by adding columns to the SharePoint site table or document library. The titles of these columns serve as attribute names and the content of the columns serves as the values of attributes for the specific object.
- Auditing and Logging. Each product in this build supports a logging mechanism detailing activities occurring within that component. Access requests can be audited using the NextLabs Reporter, where the user, access decision, and policy enforced can be viewed for each access request.

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

5.4 Features and Benefits

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

5.4.1 Support Organizations with a Diverse Set of Users and Access Needs

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

5.4.2 Reduce the Number of Identities Managed by the Enterprise

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

5.4.3 Enable a Wider Range of Risk Decisions

The ability to define attribute-based policies affords organizations the extensibility to implement a wider range of risk decisions in access control policy than otherwise would be available under an RBAC system. Specifically, the ability to leverage environmental attributes allows for the inclusion of relevant context such as location of access, time of day, threat level, and client patch level into automated decision logic.

5.4.4 Support Business Collaboration

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

5.4.5 Centralize Auditing and Access Policy Management

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

6 Future Build Considerations

6.1 Potential Additions to This Build

To help us expand this work in future builds, we need feedback from the user community to prioritize additional capabilities and learn from the identity and access management vendor community which commercial products provide those capabilities.

Here are some of the potential technical capabilities that may be added to this build:

- Demonstration of a wider array of authentication methods including but not limited to smart card, biometric and OTP tokens.
- The ability to support RP-initiated step up authentication. After the user has already authenticated, allow the RP to force the user to undergo advanced authentication based on the object they are accessing
- More robust logic relative to the current WS-Federate flow. Potential replacement of or supplement to the existing use of a WS-Federation request to limit the need to have a canned set of attributes with the initial user authentication, and to allow for attributes to be acquired on demand in any subsequent browser-based queries.
- Additional environmental attributes. Any potentially interesting sources for environmental attributes that may be useful for decisions based on risk.
- Implementation of SCIM 2.0 for cross-domain identity and attribute management
- Expand the implementation to include multiple IdP sources. As part of this implementation, at least one home administrative realm discovery approach based on available standards-based methods.
- Pursue an alternate federation approach such as OpenID Connect, an alternative to SAML-based federation that supports the types of browser-based queries in our scenario.
- Expand the set of protected resources beyond the single-product instance of SharePoint.

6.2 Future Builds

In additional to potential updates and add-ons to this first build, there is potential for the development and implementation of new ABAC architectures under this build. To explore these various architectures, the NCCoE would like to engage with any individual or company with commercially or publicly available technology relevant to the ABAC model. The NCCoE recently published a Federal Register notice (https://federalregister.gov/a/2015-20041) inviting parties to submit a letter of interest to express their desire and ability to contribute to this effort. Interested parties will enter into a consortium Cooperative Research and Development Agreement with NISTanticipates publishing federal register notice.

Some topics of interest for future builds include:

- use of other protocols that may be relevant to the ABAC model such as OAuth, OpenID Connect, and User Managed Access
- demonstration additional options for PDP and PEP placement, such as a loose coupling with the application
- potential architectures that use the ABAC model to protect cloud applications to include software as a service (SaaS) applications
- integration of the ABAC model with physical access control systems
- integration of the ABAC model with legacy technology where PEP integration is not feasible

All interested parties are encouraged to engage the NCCoE with additional ideas and system requirements by reaching out to abac-nccoe@nist.gov.

Appendix A Acronyms

AA	Adaptive Authentication
ABAC	Attribute Based Access Control
AC	Access Control
AD	Microsoft Active Directory
CSA	Cloud Security Alliance
CSF	Cybersecurity Framework
DAC	Discretionary Access Control
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IdAM	Identity and Access Management
IdP	Identity Provider
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
ISACA	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardiza-tion/International Electrotechnical Commission
JIT	just-in-time
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
NCCoE	National Cybersecurity Center of Excellence
NCEP	National Cybersecurity Excellence Partner
NGAC	Next Generation Access Control
NIST	National Institute of Standards and Technology
OAuth	Open Standard for Authorization
OIDC	OpenID Connect Core
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
RP	Relying Party
SaaS	Software as a Service

SAML	Security Assertion Markup Language
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SMS	Short Message Service
SP	Special Publication
SP	Service Provider
SSO	Single Sign-On
TLS	Transport Layer Security
URL	Uniform Resource Locator
WS-Federation	Web Services Federation Language
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language

NIST CYBERSECURITY PRACTICE GUIDE

ATTRIBUTE BASED ACCESS CONTROL

How-To Guides

For Security Engineers

Bill Fisher
Norman Brickman
Santos Jha
Sarah Weeks
Ted Kolovos
Prescott Burden

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-3c

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-3c

ATTRIBUTE BASED ACCESS CONTROL

Bill Fisher
National Cybersecurity Center of Excellence
Information Technology Laboratory

Norman Brickman
Santos Jha
Sarah Weeks
Ted Kolovos
Prescott Burden
The MITRE Corporation
McLean, VA

Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

September 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, 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, materials, or equipment 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, 467 pages (September 2015)
CODEN: NSPUE2

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

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

Public comment period: *September 30, 2016* through *December 4, 2016*

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
9600 Gudelsky Drive (Mail Stop 2002) Rockville, MD 20850
Email: abac-nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publicly available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices.

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

ABSTRACT

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

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

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

KEYWORDS

access control; access management; attribute provider; authentication; authorization; identity federation; identity management; Identity Provider; relying party

ACKNOWLEDGMENTS

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Nate Lesser	NIST National Cybersecurity Center of Excellence
Paul Timmel	NIST National Cybersecurity Center of Excellence
Paul Grassi	NIST National Strategy for Trusted Identities in Cyberspace
Mike Garcia	NIST National Strategy for Trusted Identities in Cyberspace
Naomi Lefkovitz	NIST National Strategy for Trusted Identities in Cyberspace
Rene Peralta	NIST National Strategy for Trusted Identities in Cyberspace
Dave Ferriaolo	NIST Computer Security Division
Vincent Hu	NIST Computer Security Division
Roger Wiggenstam	NextLabs Inc
John Conduit	NextLabs Inc
Srikanth Karanam	NextLabs Inc
Adam Madlin	Symantec Corporation
Steve Kruse	Symantec Corporation
Steve Schmalz	RSA
Ben Smith	RSA
Andrew Whelchel	RSA
Chris Leggett	Ping Identity
Paul Fox	Microsoft Corporation
Derek Keatley	Microsoft Corporation
Hemma Prafullchandra	Hytrust
John McLeese	Hytrust

Name	Organization
Dave Cox	ID/Dataweb
Chris Donovan	ID/Dataweb

Contents

1 Introduction

1.1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based example solution and provides users with the information they need to replicate this approach to implementing attribute based access control (ABAC) that leverages identity federation. The example solution is modular and can be deployed in whole or in parts.

This guide contains three volumes:

- *NIST SP 1800-3a: Executive Summary*
- *NIST SP 1800-3b: Approach, Architecture, and Security Characteristics* - what we built and why
- *NIST SP 1800-3c: How To Guides* - instructions for building the example solution - this document

The following instructions show IT professionals and security engineers how the National Cybersecurity Center of Excellence (NCCoE) implemented an example solution to the challenge of implementing an ABAC deployment that supports identity federation. We developed a build that conforms to federal standards and best practices, and addresses the challenge of providing access control mechanisms for a diverse set of subjects requesting access to corporate resources when many of these subjects may not be managed or even known to the enterprise. This build also helps ensure that once users are authenticated, fine-grained access decisions are enforced based on a range of attributes, such as user identity, resource type, and environmental conditions.

This example solution is packaged as a “How To” guide. The guide demonstrates how to implement standards-based, commercially available cybersecurity technologies in the real world, based on risk analysis. We cover all the products that we employed in this example solution. We do not recreate the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create the example solution.

This guide assumes that the IT professionals using this document have experience implementing security products within an enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products.[1] We assume that you have the knowledge and expertise to choose other products that might better fit your IT systems and business processes. If you use substitute products, we hope you'll seek products that are congruent with standards and best practices, as we have. Refer to *NIST SP 1800-3b: Approach, Architecture, and Security Characteristics, Section 4.5*, table 4.2 for a list of the products that we used, mapped to the cybersecurity controls provided by this example solution, to understand the characteristics you should seek in alternate products. Section 4.4, Security Characteristics and Controls Mapping, of that document describes how we arrived at this list of controls.

This NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. This is a draft version. We are seeking feedback on its contents and welcome your

[1] Certain commercial entities, equipment, 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, materials, or equipment are necessarily the best available for the purpose

input. Comments and suggestions will improve subsequent versions of this guide. Please contribute your thoughts to abac-nccoe@nist.gov, and join the discussion at http://nccoe.nist.gov/forums/attribute-based-access-control.

1.2 Typographical Conventions

The following table presents typographic conventions used in this volume.

Typeface/ Symbol	Meaning	Example
Italics	references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary.*
Bold	names of menus, options, command buttons and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST’s National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov

2 Setting up the Identity Provider

2.1 Introduction

This guide details an attribute based access control (ABAC) implementation that leverages identity federation. In a federation model, the Identity Provider authenticates the user requesting access and provides attributes assigned to that user to the Relying Party. The Relying Party, which controls access to the resource requested by the user, utilizes the identity and attributes information to make run-time decisions to grant or deny access to the user.

In this chapter we install and configure federation components at the Identity Provider. The components described in this chapter facilitate federated, SAML-based authentication using account credentials in the Identity Provider's Microsoft Active Directory Domain Services (referred to as Microsoft AD in this guide). The federated authentication between the Relying Party and the Identity Provider is facilitated by Ping Identity's PingFederate application. This build also requires the user to authenticate with a second factor, which is handled by the RSA adaptive authentication server.

Each of the components used for the build are described in section 2.2, Components. Following that section are step-by-step instructions for installing, configuring, and integrating the components. If you follow the instructions in this chapter, you will be able to perform a functional test to verify the successful completion of the steps for installing, configuring, and integrating the components.

2.2 Components

Federated Authentication at the Identity Provider involves the following distinct components:

- **Microsoft AD**: An LDAP directory service that stores user account and attribute information.
- **PingFederate-IdP**: A federation system or trust broker for the Identity Provider.
- **PingFederate-RP**: Serves as the trust broker for SharePoint.
- **RSA Adaptive Authentication (RSA AA)**: Requires the user to authentication using an SMS message sent to their mobile phone. Collects environmental information about the user and the user's system or agent at the time of authentication.
- **SCE Plugin**: Handles communications between the PingFederate-IdP and the RSA AA.

2.2.1 Microsoft AD

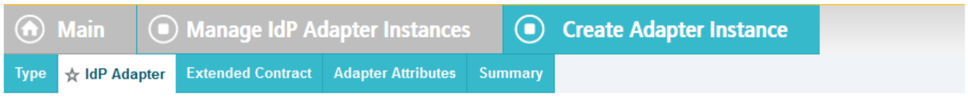
Microsoft AD acts as a user identity management repository for the IdP. This includes the ability to provision and de-provision user identities; the creation, modification, and deletion of subject attributes; and the provisioning and de-provisioning of subject attributes to specific user identities.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

2.2.2 PingFederate-IdP

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

PingFederate Usage Notes

- When using the PingFederate application to perform an administrative configuration, there is usually a sequence of screens that require user entry, ending with a summary page. Once you click **Done** on the summary page, you must also click **Save** on the following page to actually save the configurations. If you forget to click **Save**, you may inadvertently lose changes to the configuration.
- In the PingFederate application and associated documentation, the Relying Party is referred to as the **Service Provider**.
- When using the PingFederate application to perform configuration, refer to the title of the tab with a small star icon to its left, to identify the item you are currently configuring. For example, if you navigated to the following screen, you would be on the IdP Adapter screen.



2.2.3 PingFederate-RP

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

2.2.4 RSA Adaptive Authentication

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

2.2.5 SCE Plugin

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

Table 2.1 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
Microsoft AD		512MB RAM; 1.4GHz CPU; 32GB free disk space	4GB RAM; 2.2GHz CPU; 108GB free disk space		Microsoft Windows Server 2012
PingFederate	sce-adapters-pingfederate-aa.1.1.jar	1GB RAM; 1.8GHz CPU; 250MB free disk space	4GB RAM; 2.2GHz CPU; 98 GB	sce-adapters-pingfederate-aa.1.1.jar	Microsoft Windows Server 2012
RSA AA	Adaptive Authentication (On-Premise) 7.0.0.0-SNAPSHOT				

2.3 Install Microsoft AD

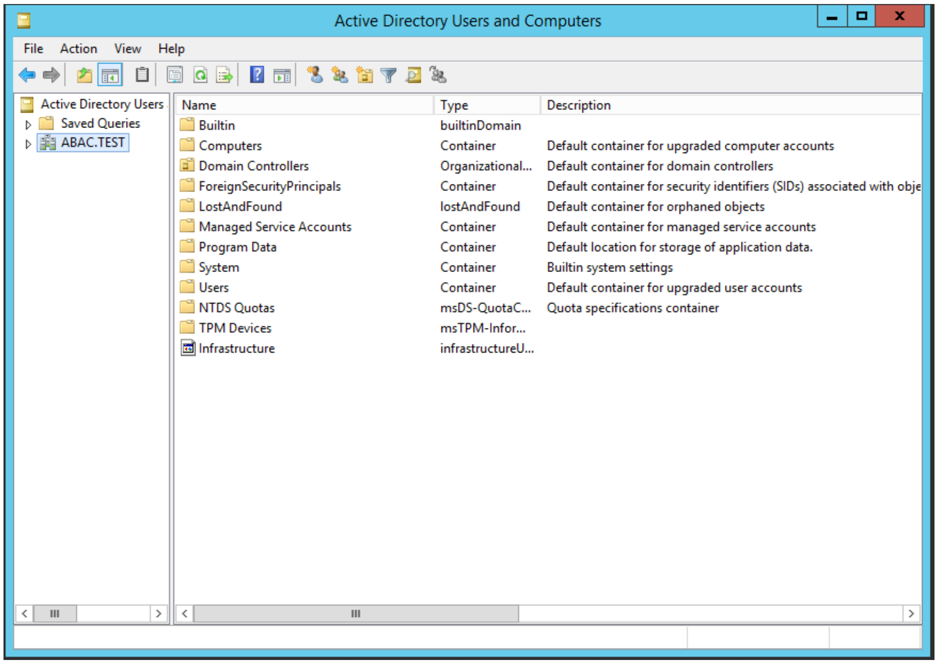
1. Log on to the server that will host Microsoft AD.
2. Follow the instructions at the link below to create a new Microsoft AD domain that will store the accounts and identity information for the Identity Provider.
3. During setup, you will be asked to provide a name for your new domain.
   The name of the domain used for this build is **ABAC.TEST**.

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

2.4 Create a User in Microsoft AD

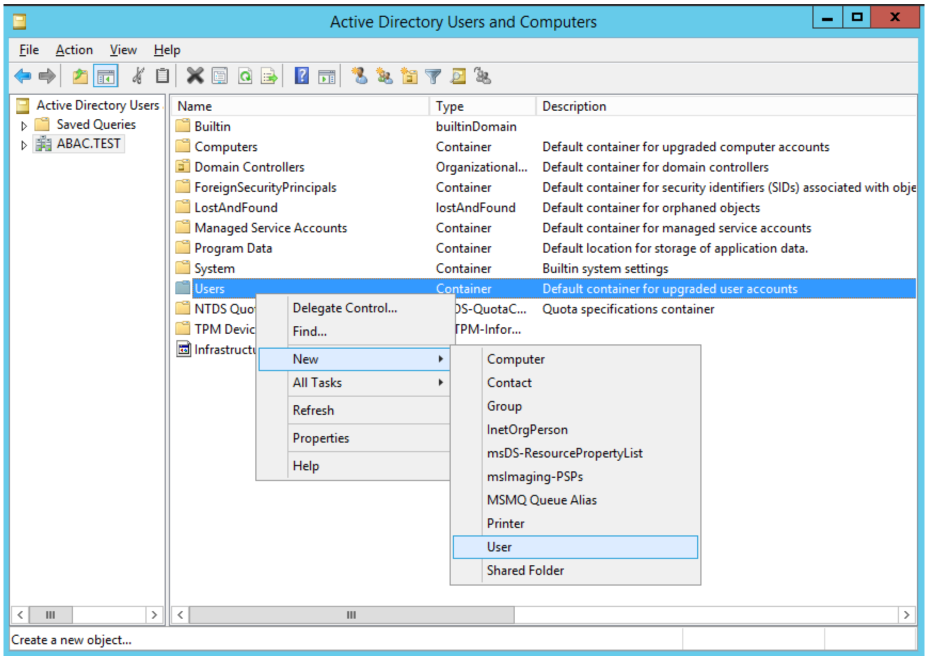
To create a user account in the Microsoft AD Domain:

1. Launch the Active Directory Users and Computers program.



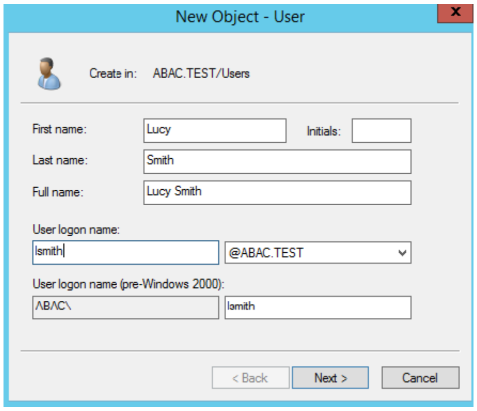
Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgraded computer accounts
Domain Controllers	Organizational...	Default container for domain controllers
ForeignSecurityPrincipals	Container	Default container for security identifiers (SIDs) associated with obje
LostAndFound	lostAndFound	Default container for orphaned objects
Managed Service Accounts	Container	Default container for managed service accounts
Program Data	Container	Default location for storage of application data.
System	Container	Builtin system settings
Users	Container	Default container for upgraded user accounts
NTDS Quotas	msDS-QuotaC...	Quota specifications container
TPM Devices	msTPM-Infor...	
Infrastructure	infrastructureU...	

2. Click on the name of your domain in the left pane and then right-click on the **Users** folder in the right pane.
3. In the popup menu that appears, select **New**, and then select **User**.



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgraded computer accounts
Domain Controllers	Organizational...	Default container for domain controllers
ForeignSecurityPrincipals	Container	Default container for security identifiers (SIDs) associated with obje
LostAndFound	lostAndFound	Default container for orphaned objects
Managed Service Accounts	Container	Default container for managed service accounts
Program Data	Container	Default location for storage of application data.
System	Container	Builtin system settings
Users	Container	Default container for upgraded user accounts
NTDS Quo	DS-QuotaC...	Quota specifications container
TPM Devic	TPM-Infor...	
Infrastructu		

4. In the New Object - User screen that displays, type the **First** and **Last** name of the user, as well as their **User logon name** (that is, the account name).



New Object - User

Create in: ABAC.TEST/Users

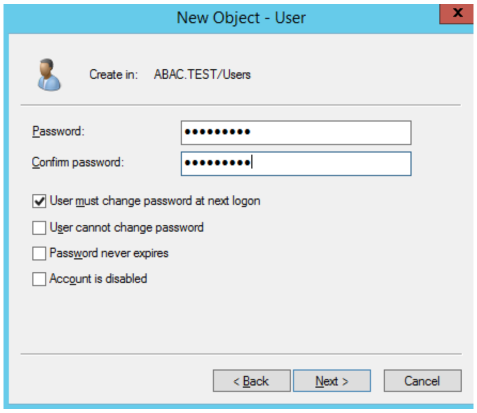
First name: Lucy
Initials:
Last name: Smith
Full name: Lucy Smith

User logon name: lsmith @ABAC.TEST

User logon name (pre-Windows 2000): ABAC\ lsmith

5. Click **Next**.

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 her own unique password.



New Object - User

Create in: ABAC.TEST/Users

Password: •••••••••
Confirm password: •••••••••

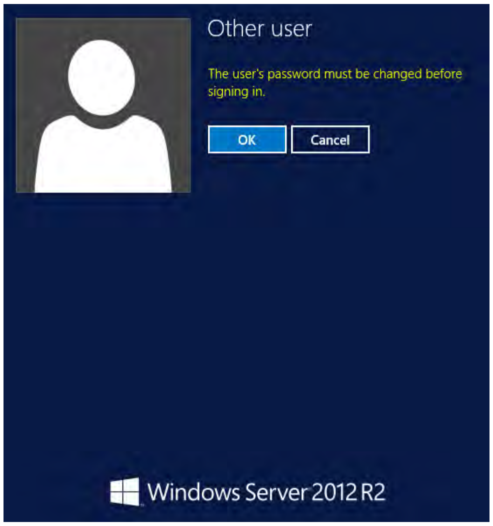
☑ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled

7. Click **Next**.

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

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

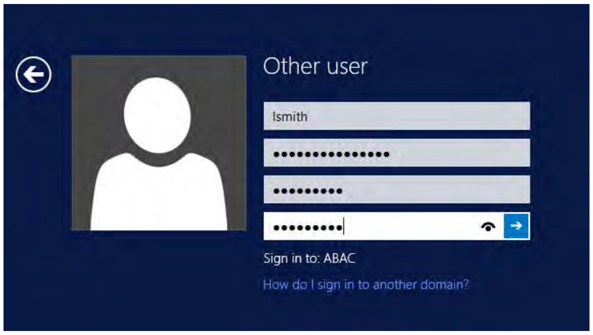
The following illustrations demonstrate what the new password screens may look like on Microsoft Windows Server 2012 when the user Lucy Smith attempts to log on to a computer in the **ABAC.TEST** domain using her user name **lsmith** and the initial password.



Other user

The user's password must be changed before signing in.

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



Other user

lsmith

•••••••••••••••

•••••••••

•••••••••

Sign in to: ABAC

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

2.4.1 Create the LDAP User for Federated Authentication

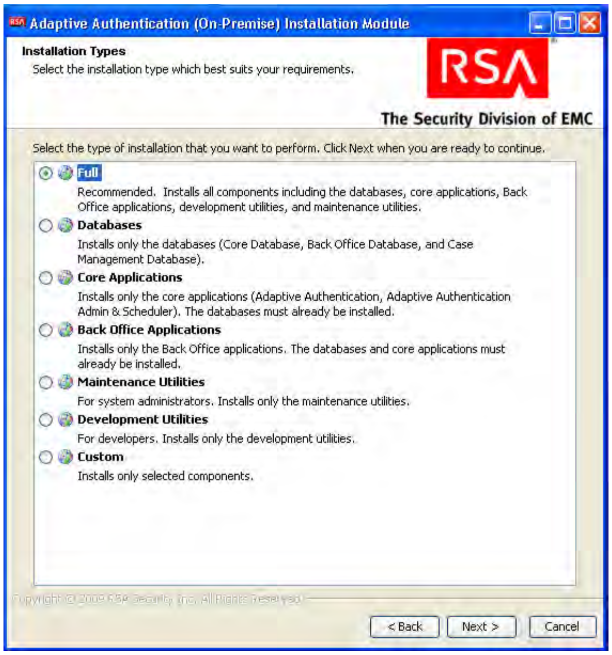
Follow the steps in the previous section to create a user named **LDAP user** in Microsoft AD. This user account will be used by the PingFederate-IdP to perform LDAP queries in Microsoft AD.

2.5 Install RSA AA

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

1. Log on to VMware and load the RSA AA virtual appliance. [e.g. Adaptive Authentication (On-Premise) 7.0.0.0-SNAPSHOT]
2. Start the RSA AA virtual machine using VMware.

3. Log on to the server that hosts the new virtual machine.
4. Launch the RSA AA installation file.
5. On the Installation Types screen, select **Full** to install all required components. Then, click **Next**.



Adaptive Authentication (On-Premise) Installation Module
RSA
The Security Division of EMC
< Back
Next >
Cancel

Installation Types

Select the installation type which best suits your requirements.

Select the type of installation that you want to perform. Click Next when you are ready to continue.

● **Full**
Recommended. Installs all components including the databases, core applications, Back Office applications, development utilities, and maintenance utilities.

○ **Databases**
Installs only the databases (Core Database, Back Office Database, and Case Management Database).

○ **Core Applications**
Installs only the core applications (Adaptive Authentication, Adaptive Authentication Admin & Scheduler). The databases must already be installed.

○ **Back Office Applications**
Installs only the Back Office applications. The databases and core applications must already be installed.

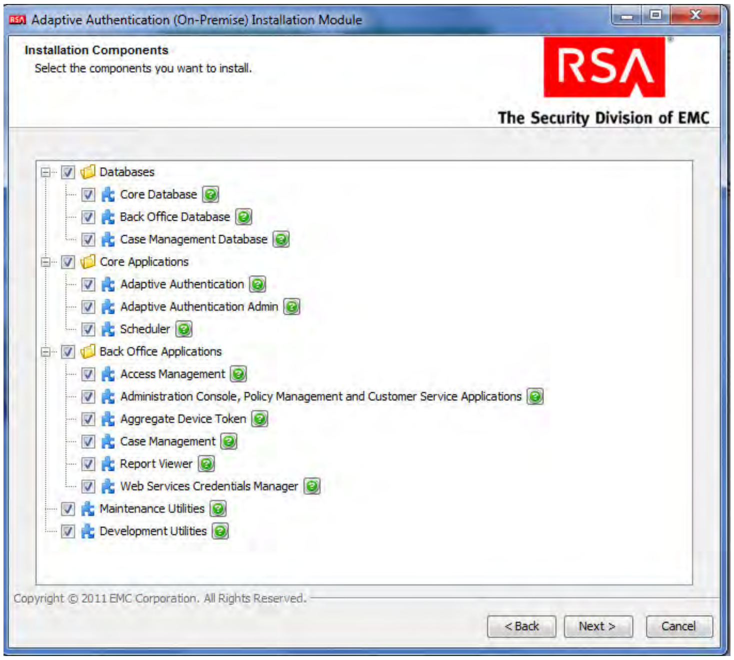
○ **Maintenance Utilities**
For system administrators. Installs only the maintenance utilities.

○ **Development Utilities**
For developers. Installs only the development utilities.

○ **Custom**
Installs only selected components.

Copyright © 2009 RSA Security Inc. All Rights Reserved.

6. Click **Next** in the Installation Components screen.



Adaptive Authentication (On-Premise) Installation Module
RSA
The Security Division of EMC
< Back
Next >
Cancel

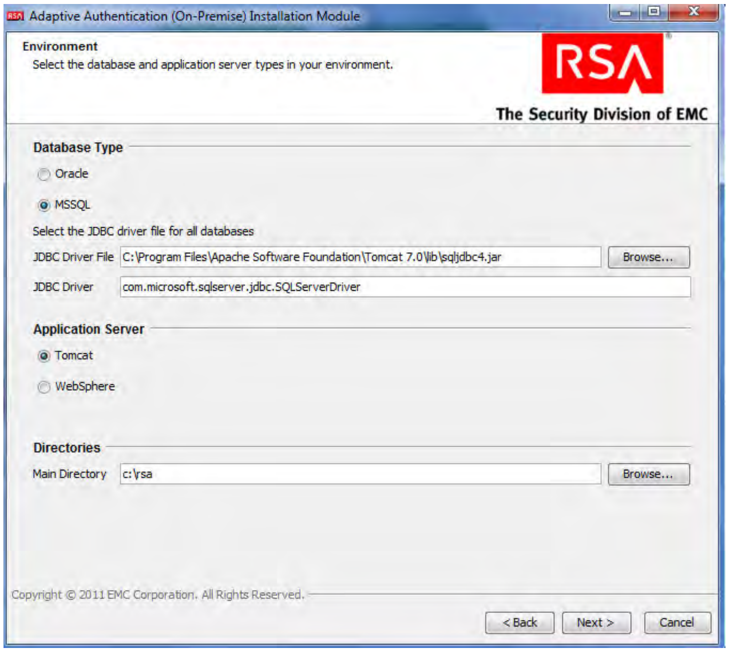
Installation Components

Select the components you want to install.

- ☑ Databases
  - ☑ Core Database
  - ☑ Back Office Database
  - ☑ Case Management Database
- ☑ Core Applications
  - ☑ Adaptive Authentication
  - ☑ Adaptive Authentication Admin
  - ☑ Scheduler
- ☑ Back Office Applications
  - ☑ Access Management
  - ☑ Administration Console, Policy Management and Customer Service Applications
  - ☑ Aggregate Device Token
  - ☑ Case Management
  - ☑ Report Viewer
  - ☑ Web Services Credentials Manager
- ☑ Maintenance Utilities
- ☑ Development Utilities

Copyright © 2011 EMC Corporation. All Rights Reserved.

7. In the environment screen, set the database type [MS SQL] and the JDBC driver file. This is illustrated in the following figure.



Adaptive Authentication (On-Premise) Installation Module

Environment

Select the database and application server types in your environment.

The Security Division of EMC

Database Type

○ Oracle

● MSSQL

Select the JDBC driver file for all databases

JDBC Driver File: C:\Program Files\Apache Software Foundation\Tomcat 7.0\lib\sqljdbc4.jar [Browse...]

JDBC Driver: com.microsoft.sqlserver.jdbc.SQLServerDriver

Application Server

● Tomcat

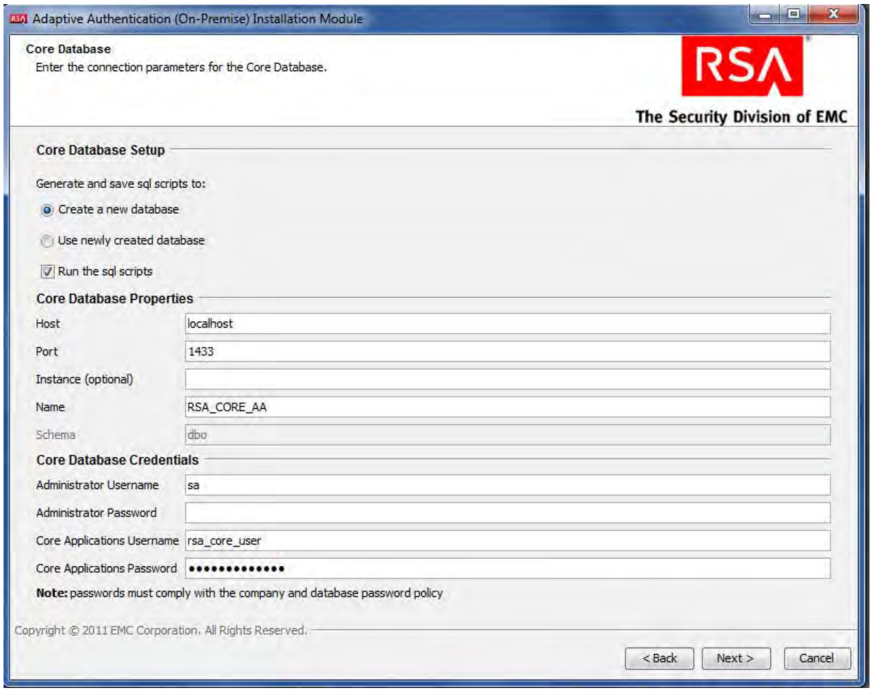
○ WebSphere

Directories

Main Directory: c:\rsa [Browse...]

Copyright © 2011 EMC Corporation. All Rights Reserved.

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



Adaptive Authentication (On-Premise) Installation Module

Core Database

Enter the connection parameters for the Core Database.

The Security Division of EMC

Core Database Setup

Generate and save sql scripts to:

● Create a new database

○ Use newly created database

☑ Run the sql scripts

Core Database Properties

Host: localhost

Port: 1433

Instance (optional):

Name: RSA_CORE_AA

Schema: dbo

Core Database Credentials

Administrator Username: sa

Administrator Password:

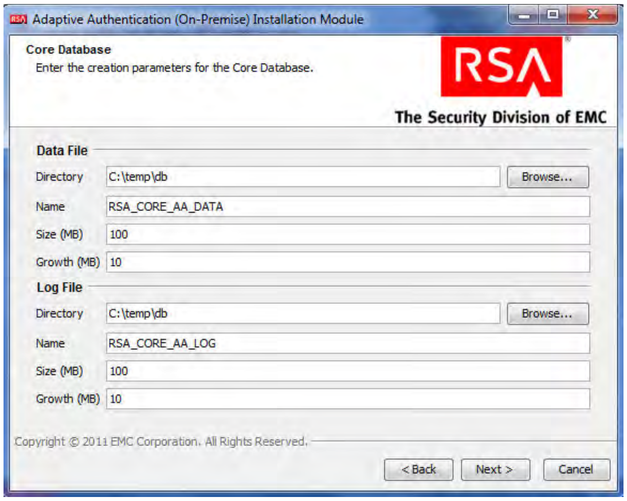
Core Applications Username: rsa_core_user

Core Applications Password: •••••••••••••

Note: passwords must comply with the company and database password policy

Copyright © 2011 EMC Corporation. All Rights Reserved.

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



Adaptive Authentication (On-Premise) Installation Module

Core Database

Enter the creation parameters for the Core Database.

Data File

Directory: C:\temp\db

Name: RSA_CORE_AA_DATA

Size (MB): 100

Growth (MB): 10

Log File

Directory: C:\temp\db

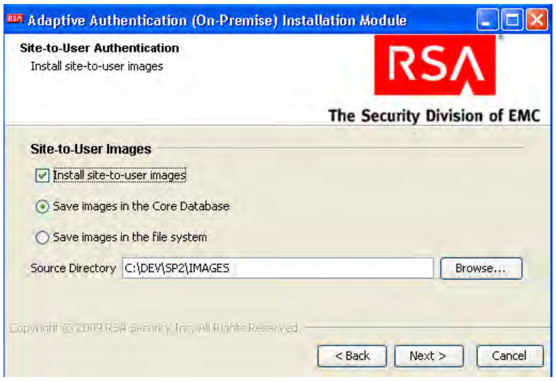
Name: RSA_CORE_AA_LOG

Size (MB): 100

Growth (MB): 10

Copyright © 2011 EMC Corporation. All Rights Reserved.

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



Adaptive Authentication (On-Premise) Installation Module

Site-to-User Authentication

Install site-to-user images

Site-to-User Images

☑ Install site-to-user images

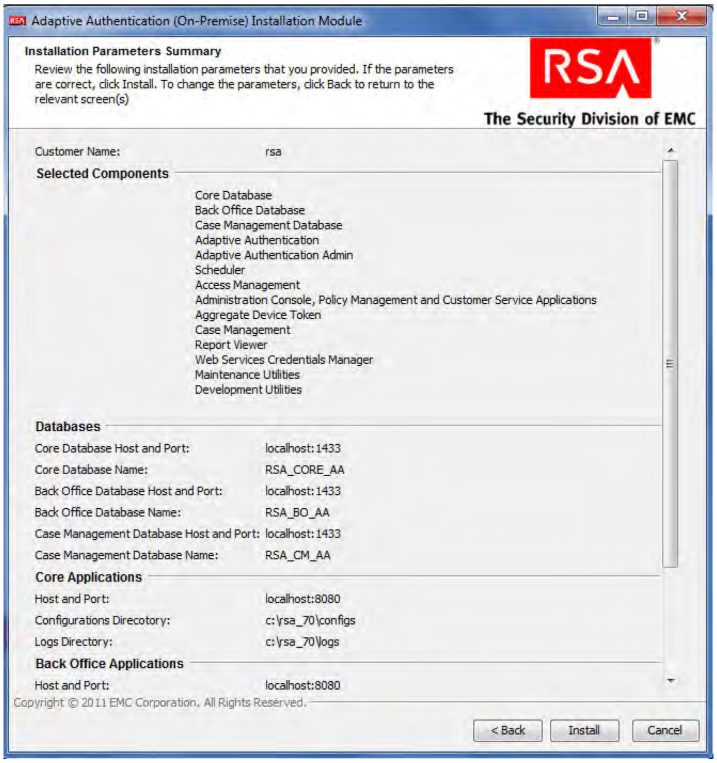
● Save images in the Core Database

○ Save images in the file system

Source Directory: C:\DEV\SP2\IMAGES

Copyright © 2009 RSA Security Inc. All Rights Reserved.

11. 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.


Adaptive Authentication (On-Premise) Installation Module
RSA
The Security Division of EMC
< Back
Install
Cancel

Installation Parameters Summary

Review the following installation parameters that you provided. If the parameters are correct, click Install. To change the parameters, click Back to return to the relevant screen(s)

Customer Name: rsa

Selected Components

Core Database
Back Office Database
Case Management Database
Adaptive Authentication
Adaptive Authentication Admin
Scheduler
Access Management
Administration Console, Policy Management and Customer Service Applications
Aggregate Device Token
Case Management
Report Viewer
Web Services Credentials Manager
Maintenance Utilities
Development Utilities

Databases

Core Database Host and Port: localhost:1433
Core Database Name: RSA_CORE_AA
Back Office Database Host and Port: localhost:1433
Back Office Database Name: RSA_BO_AA
Case Management Database Host and Port: localhost:1433
Case Management Database Name: RSA_CM_AA

Core Applications

Host and Port: localhost:8080
Configurations Direcotory: c:\rsa_70\configs
Logs Directory: c:\rsa_70\logs

Back Office Applications

Host and Port: localhost:8080

Copyright © 2011 EMC Corporation. All Rights Reserved.

2.6 Configure RSA AA Rules

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 set up policy for enabling the enhanced features provided by the RSA adapter such as answering challenge questions and providing SMS confirmation codes are enabled through this interface.

2.6.1 Create Rule for Non-Persistent User Enrollment

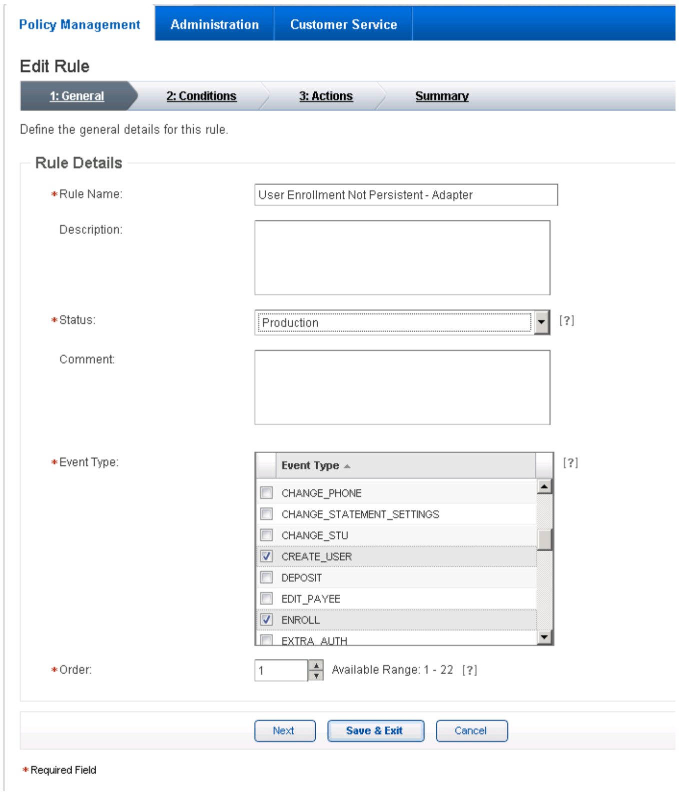
RSA AA requires information for each user to help verify their identity. These users are classified into two groups: persistent and non-persistent users. A rule is created to request enrollment information for non-persistent users, those not kept in the user database.

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

Note: The rule cannot be in production until it is created and approved by an administrator.

c. In **Event Type**, select **Create User** and **Enroll**.

d. Set the **Order** to **1**.



Edit Rule

Define the general details for this rule.

Rule Details

*Rule Name: User Enrollment Not Persistent - Adapter

Description:

*Status: Production [?]

Comment:

*Event Type: [?]

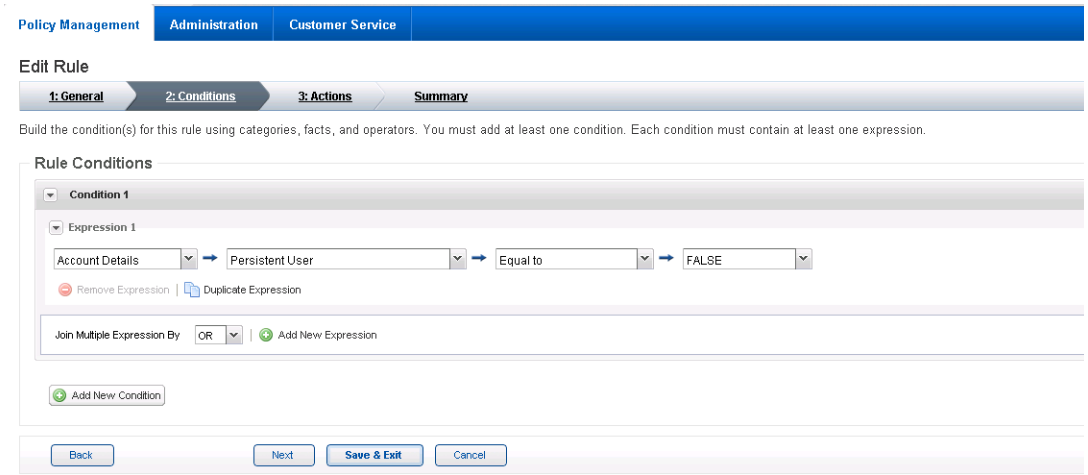
	Event Type
□	CHANGE_PHONE
□	CHANGE_STATEMENT_SETTINGS
□	CHANGE_STU
☑	CREATE_USER
□	DEPOSIT
□	EDIT_PAYEE
☑	ENROLL
□	EXTRA_AUTH

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

*Required Field

4. Click **Next**.

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



Edit Rule

Build the condition(s) for this rule using categories, facts, and operators. You must add at least one condition. Each condition must contain at least one expression.

Rule Conditions

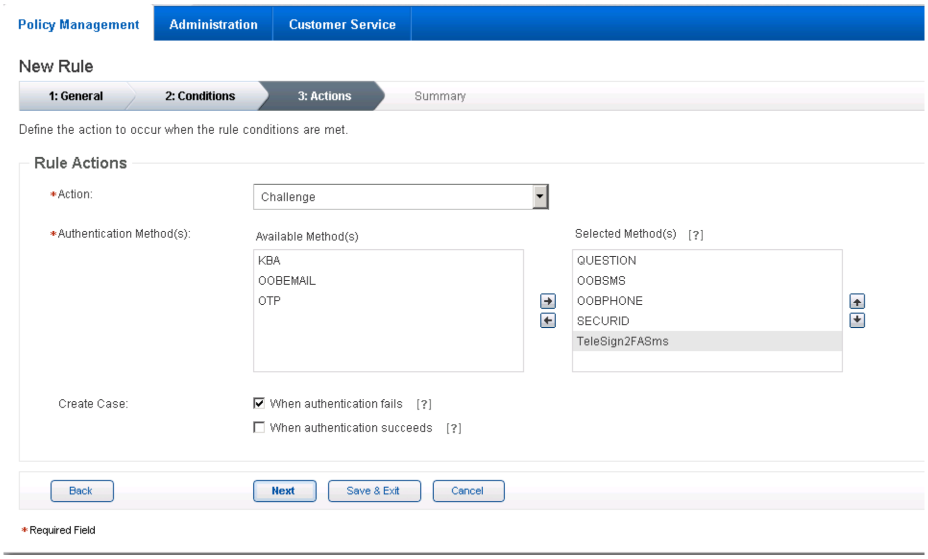
Condition 1

Expression 1

Account Details → Persistent User → Equal to → FALSE

Join Multiple Expression By OR

6. Click **Next**.
7. In the **Rule Actions** page:
   a. Set **Action** to **Challenge**.
   b. Set **Authentication Methods** to **QUESTION**, **OOBSMS**, **OOBPHONE**, **SECURID**, and **TeleSign2FASms**.
   c. In **Create Case**, make sure that only **for when authentication fails** is selected. Then, click **Next**.



New Rule

Define the action to occur when the rule conditions are met.

Rule Actions

*Action: Challenge

*Authentication Method(s):

Available Method(s): KBA, OOBEMAIL, OTP

Selected Method(s) [?]: QUESTION, OOBSMS, OOBPHONE, SECURID, TeleSign2FASms

Create Case:

☑ When authentication fails [?]

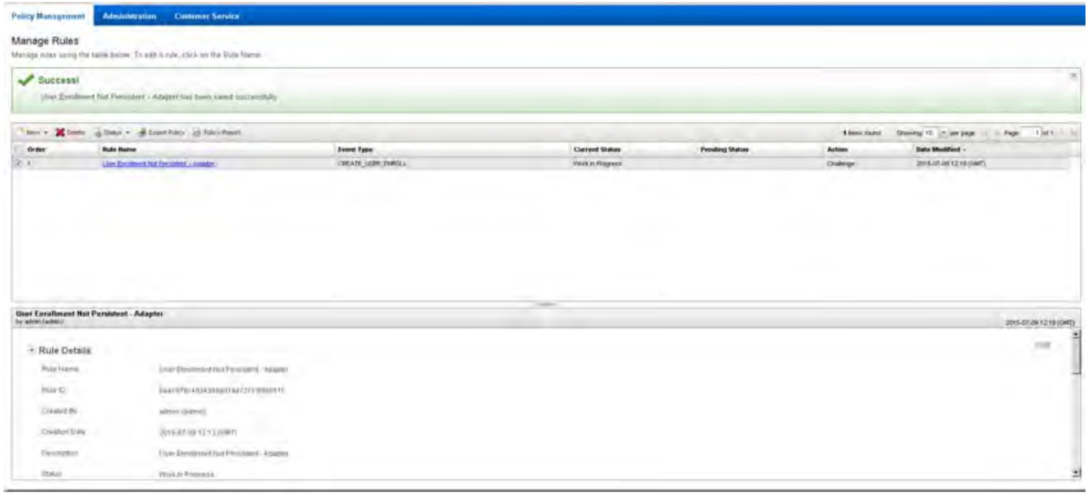
☐ When authentication succeeds [?]

* Required Field

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

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

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



Manage Rules

Manage rules using the table below. To edit a rule, click on the Rule Name.

Success!

User Enrollment Not Persistent - Adapter has been saved successfully.

1 item found Showing 10 per page Page 1 of 1

Order	Rule Name	Event Type	Current Status	Pending Status	Action	Date Modified
1	User Enrollment Not Persistent - Adapter	CREATE_USER_ENROLL	Work in Progress		Challenge	2015-07-09 12:19 (GMT)

User Enrollment Not Persistent - Adapter
by admin (admin)

2015-07-09 12:19 (GMT)

Rule Details

Rule Name	User Enrollment Not Persistent - Adapter
Rule ID	[illegible]
Created By	admin (admin)
Creation Date	2015-07-09 12:19 (GMT)
Description	User Enrollment Not Persistent - Adapter
Status	Work in Progress

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

2.6.2 Create Rule for Persistent User Enrollment

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

Parameter	Setting
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

2.6.3 Create Rule for User Updates

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

Parameter	Setting
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

2.6.4 Create Rule for Challenge SMS

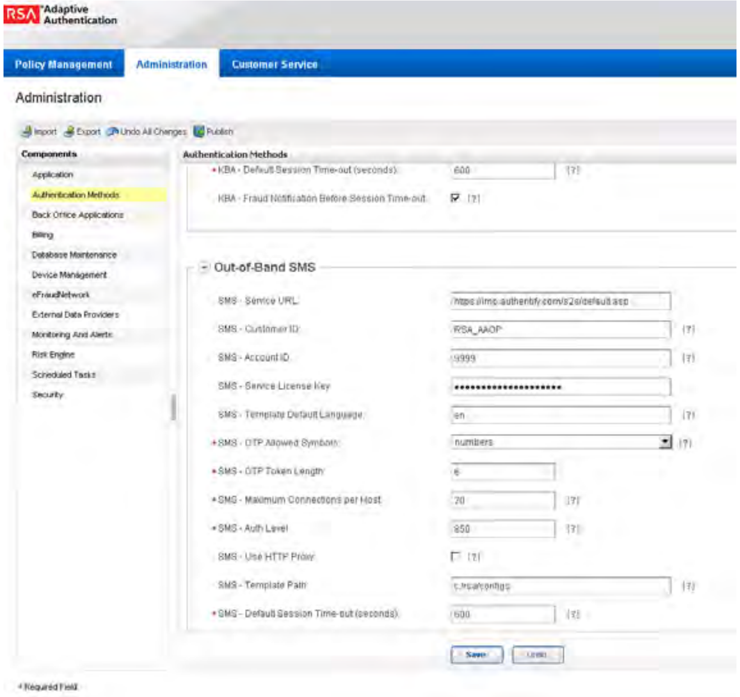
In this build, large transactions require users to respond to an out-of-band SMS challenge during authentication. When transactions meet the prerequisite, a random code will be sent to the user' SMS-enabled device that must be entered to confirm the transaction.

Parameter	Setting
Rule Name	Challenge SMS for Payment
Event Type	Challenge
Rule Order	4
Rule Condition	IF (Transaction Details -> Transaction Amount is BETWEEN 5000 and 10000)

Parameter	Setting
Rule Action	Allow
Authentication Method	1. OOBSMS
Create Case	When Authentication Succeeds

2.6.5 Increase SMS Token Length

The default token length for out-of-band SMS is currently set to four [4] digits. Access the Administration tab on the Back office application. Under Components, select Authentication Methods and scroll down to Out-of-Band SMS section. Adjust the token length by changing the value of SMS - OTP Token Length to six [6].



Authentication Methods

- * KBA - Default Session Time-out (seconds): 600 [?]
- KBA - Fraud Notification Before Session Time-out: ☑ [?]

Out-of-Band SMS

- SMS - Service URL: https://imo.authentify.com/s2s/default.asp
- SMS - Customer ID: RSA_AAOP [?]
- SMS - Account ID: 9999 [?]
- SMS - Service License Key: ••••••••••••••••••••
- SMS - Template Default Language: en [?]
- * SMS - OTP Allowed Symbols: numbers [?]
- * SMS - OTP Token Length: 6
- * SMS - Maximum Connections per Host: 20 [?]
- * SMS - Auth Level: 850 [?]
- SMS - Use HTTP Proxy: □ [?]
- SMS - Template Path: c:/rsa/configs [?]
- * SMS - Default Session Time-out (seconds): 600 [?]

* Required Field

Figure 2.1 Out-of-Band Token Length

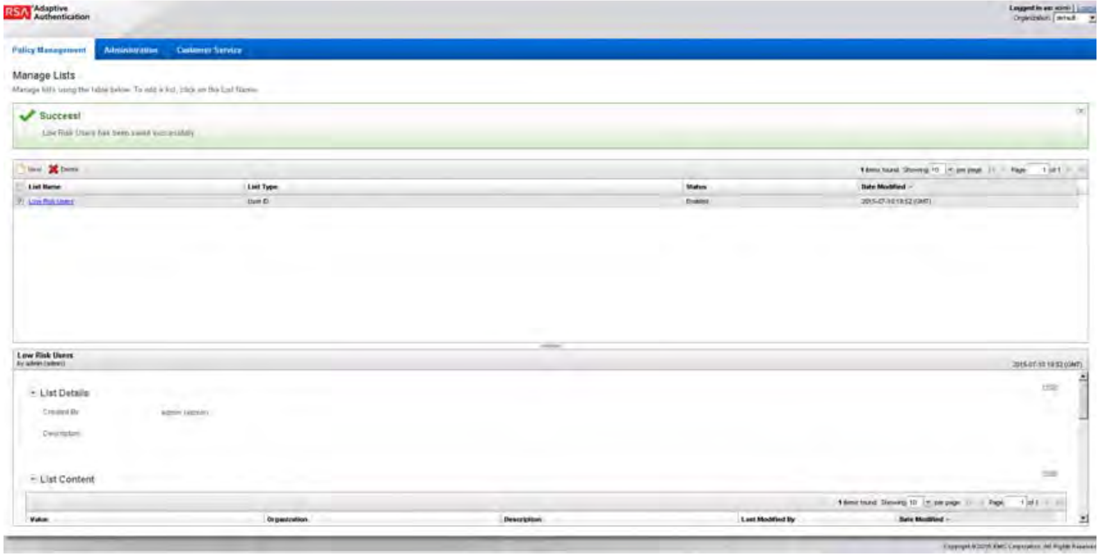
2.6.6 Create Policy for Session Sign-In

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

2.6.7 Create Lists for Session Sign-In

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

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



Low Risk Users has been saved successfully

List Name	List Type	Status	Date Modified
Low Risk Users	User ID	Enabled	2015-07-10 18:52 (GMT)

Figure 2.2 List for Session Sign-In Created Successfully

2.6.8 Create Rules for Session Sign-In

Repeat the steps as in section 2.6.1, Create Rule for Non-Persistent User Enrollment, to create the session sign-in rules for different user groups.

Table 2.2 Session Sign-In - Low Risk

Parameter	Setting
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

Table 2.2 Session Sign-In - Low Risk

Parameter	Setting
Authentication Method	
Create Case	No

241

Table 2.3 Session Sign-In - Medium Risk

Parameter	Setting
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

242

Table 2.4 Session Sign-In - High Risk

Parameter	Setting
Rule Name	Session Sign In - High Risk
Event Type	Session Sign-in
Rule Order	5
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

243

Table 2.5 Session Sign-In - Critical Risk

Parameter	Setting
Rule Name	Session Sign In - Low Risk
Event Type	Session Sign-in
Rule Order	8
Rule Condition	IF (Account Details->User ID within Critical Risk Users)

Table 2.5 Session Sign-In - Critical Risk

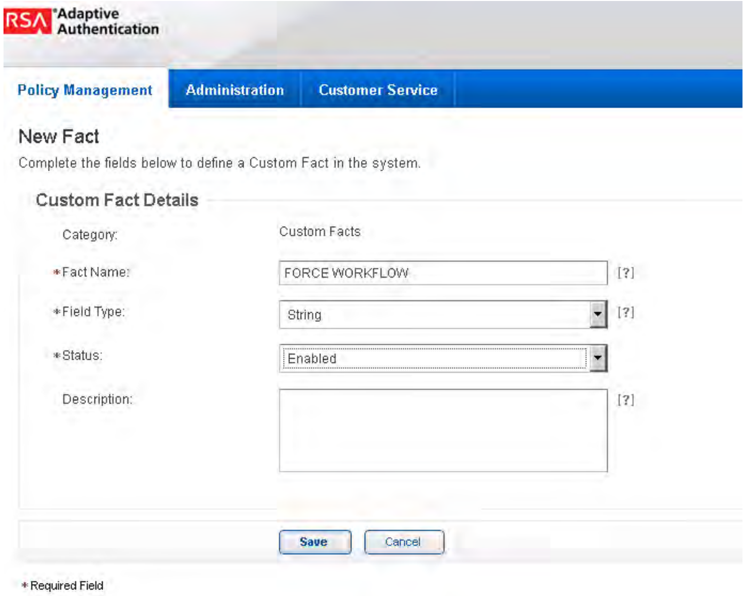
Parameter	Setting
Rule Action	Challenge
Authentication Method	1. Securid
Create Case	When Authentication Fails

2.6.9 Create Rule to Allow Forced Sign-In for Payment

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

2.6.10 Create Custom Fact

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



New Fact

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

Custom Fact Details

Category: Custom Facts

*Fact Name: FORCE WORKFLOW [?]

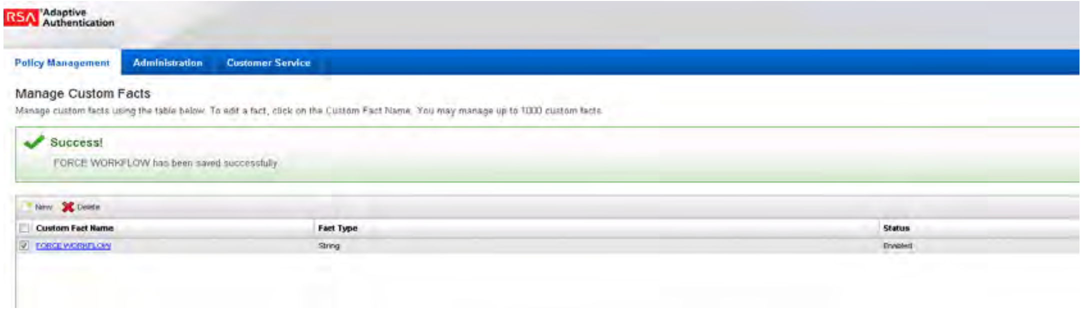
*Field Type: String [?]

*Status: Enabled

Description: [?]

* Required Field

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
☑	FORCE WORKFLOW	String	Enabled

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

Table 2.6 Force Allow

Parameter	Setting
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

2.7 Installing and Configuring PingFederate-RP

The PingFederate installation in this section is for the Federation Server at the Relying Party. This is the only component at the Relying Party in this chapter. Even though the goal of this chapter is to setup the federation for the Identity Provider, the basic configuration of the PingFederate-RP in this section is necessary, in order to produce metadata that is exchanged with the Identity Provider. A complete configuration of the PingFederate-RP will be performed in chapter 3 of this guide.

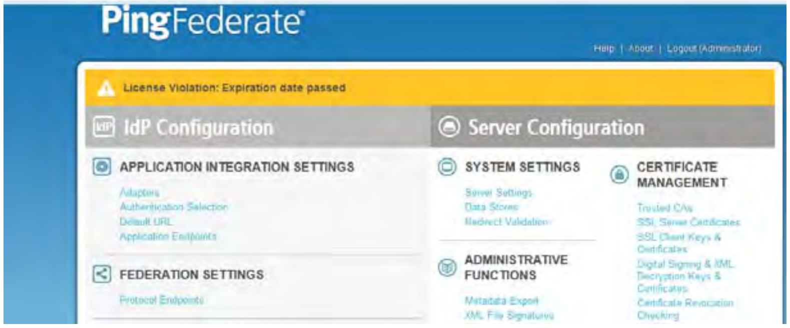
1. Log on to the Relying Party's server that will host the PingFederate service and follow the instructions at the link below to install PingFederate and run it as a Windows service.

   https://documentation.pingidentity.com/display/PF73/Installation

2. Follow the steps in this section to perform a basic configuration of the PingFederate-RP and export the metadata.

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

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



5. On the **Main** menu under **System Settings**, click **Server Settings**.

6. Click the **Roles and Protocols** tab.

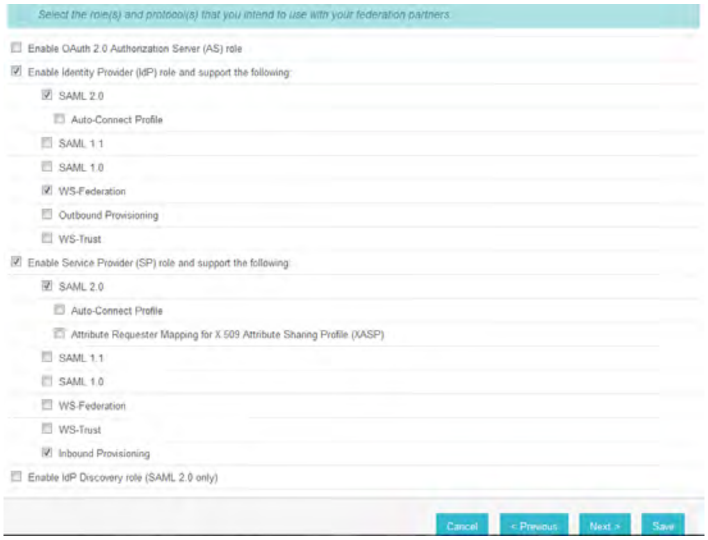
7. Select **Enable Identity Provider (IdP) role and support the following**.

8. Select SAML 2.0.

9. Select WS-Federation.

10. Select Enable Service Provider (SP) role and support the following.

11. Select the SAML 2.0.



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

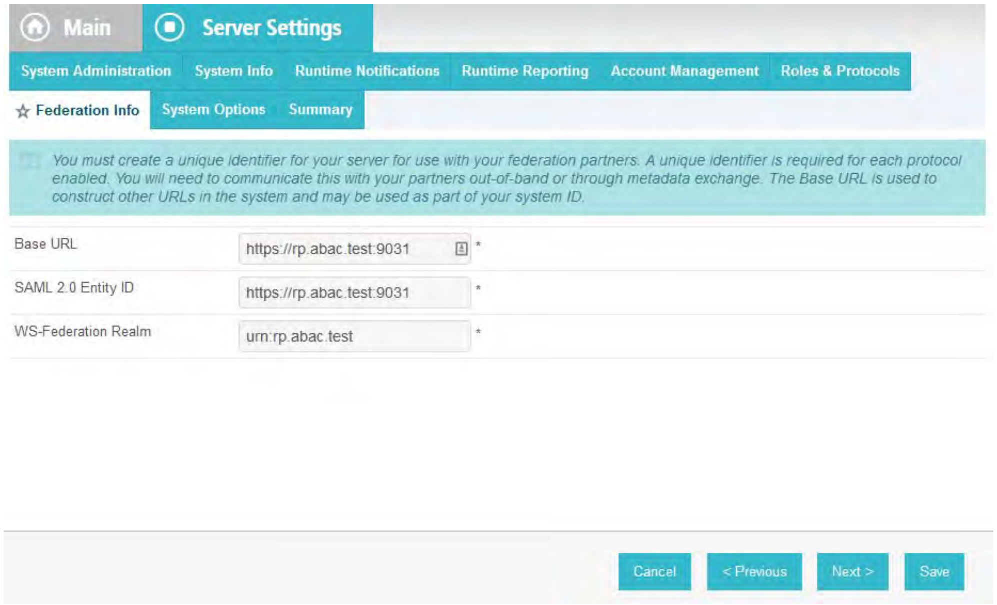
- ☐ Enable OAuth 2.0 Authorization Server (AS) role
- ☑ Enable Identity Provider (IdP) role and support the following:
  - ☑ SAML 2.0
    - ☐ Auto-Connect Profile
  - ☐ SAML 1.1
  - ☐ SAML 1.0
  - ☑ WS-Federation
  - ☐ Outbound Provisioning
  - ☐ WS-Trust
- ☑ Enable Service Provider (SP) role and support 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)

12. Click **Next**.

13. On the Federation Info screen, enter the Base URL and SAML 2.0 Entity ID using the format **https://<DNS_NAME>:9031** (e.g. https://rp.abac.test:9031).

14. Enter the WS-Federation Realm using the format **urn:<DNS_NAME>** (e.g. **urn:rp.abac.test**).

    Note: Keep a copy of the urn because it will be used later to configure the WS-Federation relationship with Sharepoint



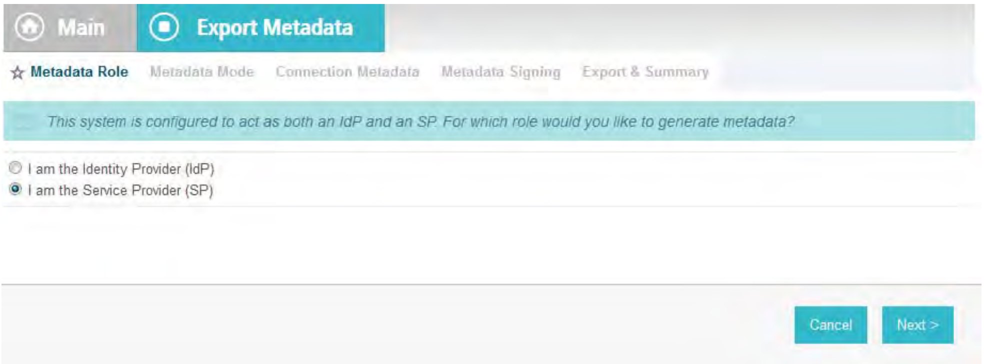
You must create a unique identifier for your server for use with your federation partners. A unique identifier is required for each protocol enabled. You will need to communicate this with your partners out-of-band or through metadata exchange. The Base URL is used to construct other URLs in the system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

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

SAML 2.0 Entity ID: https://rp.abac.test:9031 *

WS-Federation Realm: urn:rp.abac.test *

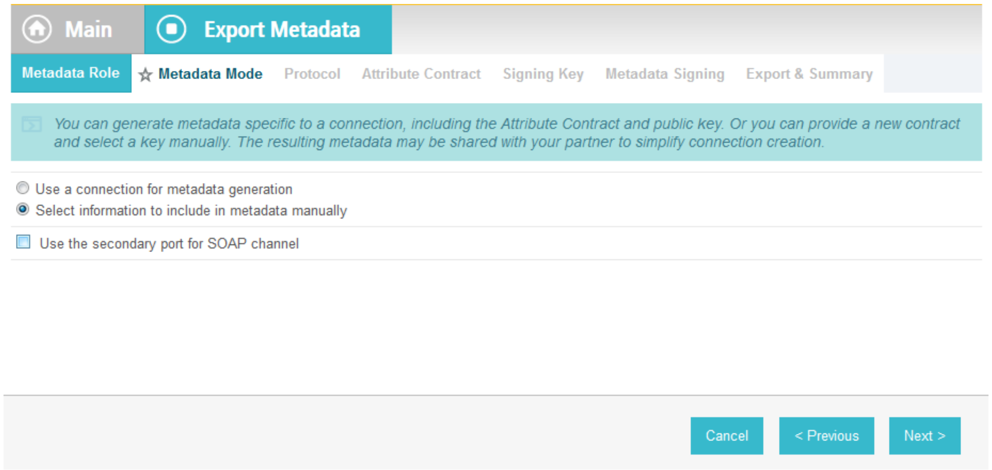
15. Click **Save**.
16. On the **Main** menu under **Administrative Functions**, click **Metadata Export**.
17. On the Metadata Role screen, select **I am the Service Provider (SP)**.



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

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

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



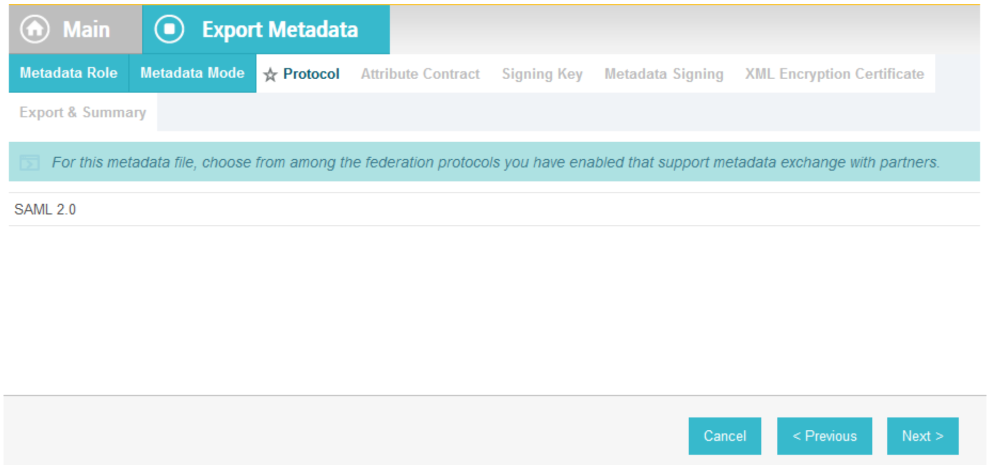
You can generate metadata specific to a connection, including the Attribute Contract and public key. Or you can provide a new contract and select a key manually. The resulting metadata may be shared with your partner to simplify connection creation.

○ Use a connection for metadata generation

● Select information to include in metadata manually

□ Use the secondary port for SOAP channel

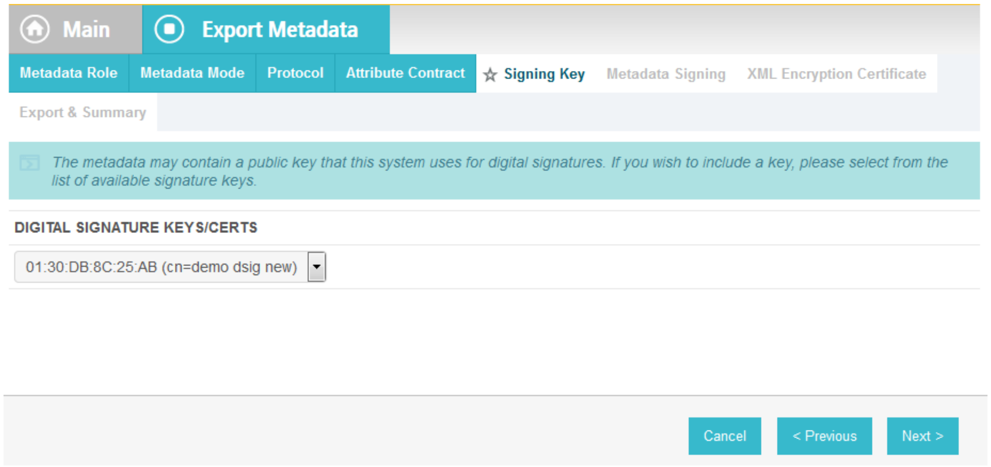
20. Click **Next**.
21. On the Protocol screen, make sure that **SAML 2.0** is listed.



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

SAML 2.0

22. Click **Next**.
23. On the Attribute Contract screen, click **Next**.
24. On the Signing Key screen, select the certificate that will be used to sign communications with the Identity Provider.

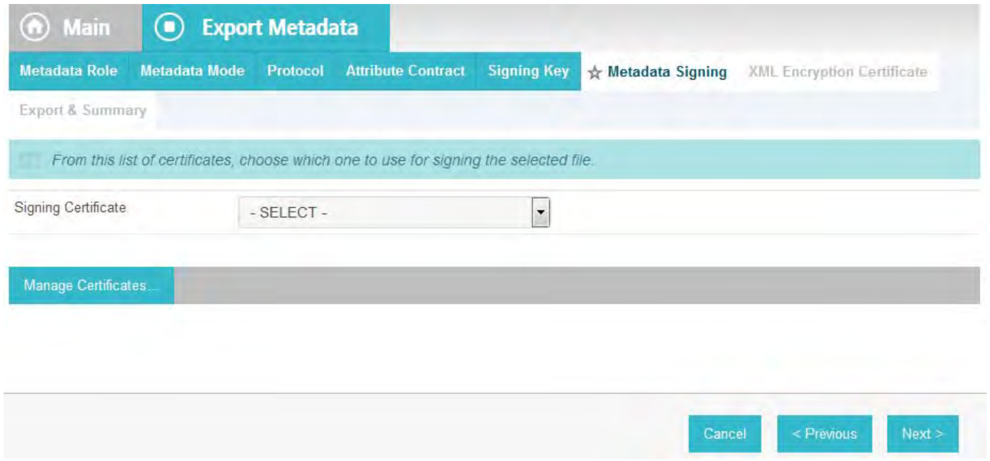


The metadata may contain a public key that this system uses for digital signatures. If you wish to include a key, please select from the list of available signature keys.

DIGITAL SIGNATURE KEYS/CERTS

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

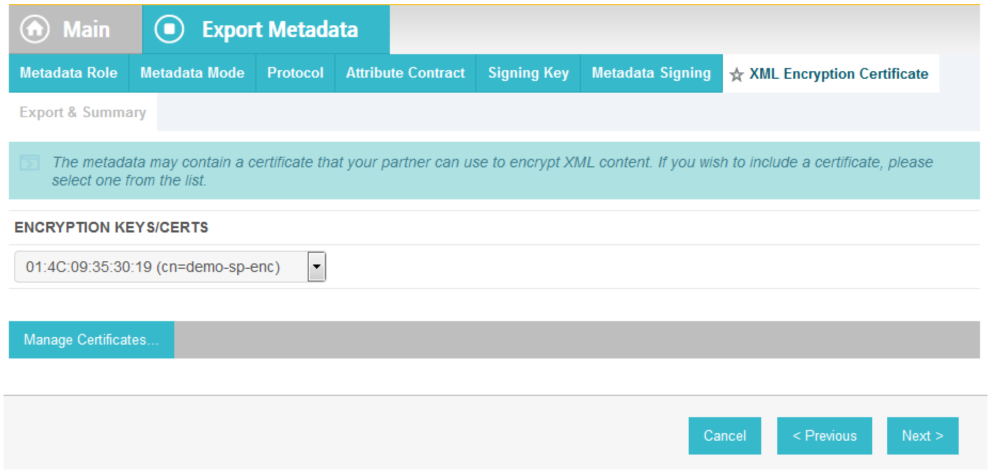
25. Click **Next**.
26. On the Metadata Signing screen, if you plan to sign the metadata file that will be exported, select the certificate that will be used to sign the file.



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

Signing Certificate: - SELECT -

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

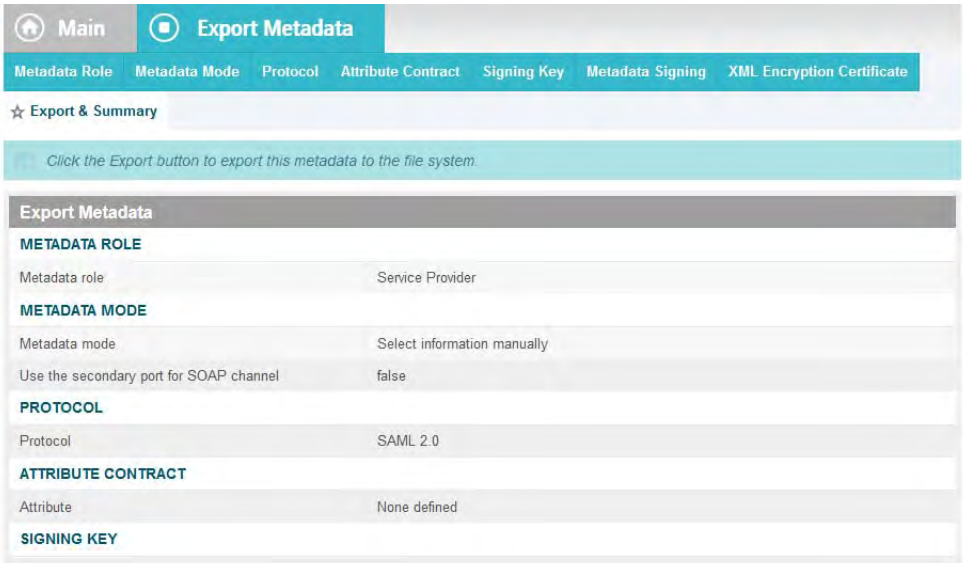


The metadata may contain a certificate that your partner can use to encrypt XML content. If you wish to include a certificate, please select one from the list.

ENCRYPTION KEYS/CERTS

01:4C:09:35:30:19 (cn=demo-sp-enc)

29. Click **Next**.

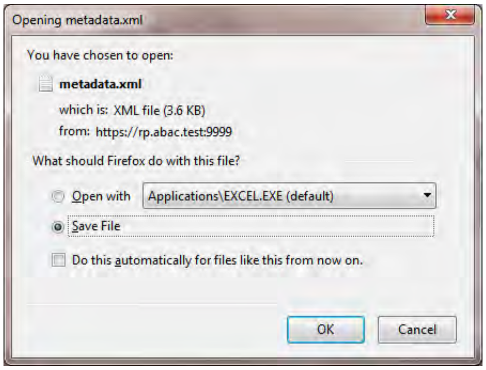


Click the Export button to export this metadata to the file system.

Export Metadata	
METADATA ROLE	
Metadata role	Service Provider
METADATA MODE	
Metadata mode	Select information manually
Use the secondary port for SOAP channel	false
PROTOCOL	
Protocol	SAML 2.0
ATTRIBUTE CONTRACT	
Attribute	None defined
SIGNING KEY	

30. Click **Export**.

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



Opening metadata.xml

You have chosen to open:

metadata.xml

which is: XML file (3.6 KB)

from: https://rp.abac.test:9999

What should Firefox do with this file?

○ Open with Applications\EXCEL.EXE (default)

● Save File

□ Do this automatically for files like this from now on.

2.8 Install PingFederate-IdP

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

Log on to the server that will host the PingFederate service for the Identity Provider and follow the instructions at the link below to install PingFederate and run it as a Windows service. https://documentation.pingidentity.com/display/PF73/Installation

2.9 Install the SCE Plugin for the PingFederate-IdP

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

1. Log on to the server that hosts the PingFederate service for the Identity provider.
2. Download the SCE Plugin adapter jar file (e.g. `sce-adapters-pingfederate-aa.1.1.jar`) to the local PingFederate server.
3. Copy the jar file to `<PF-install>/server/default/deploy`
4. From the adapter `dist/conf/template` folder, copy all .html files to

   `<PF-install>/server/default/conf/template`
5. From the adapter `dist/conf/template/assets` folder, copy the aa folder to

   `<PF-install>/server/default/conf/template/assets`
6. From the adapter `dist/data/adapter-config` folder, copy the aa folder to

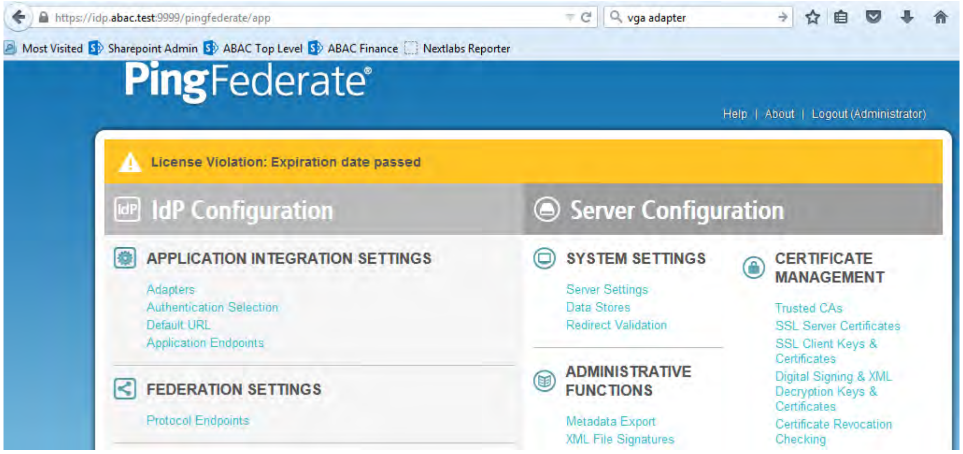
   `<PF-install>/server/default/data/adapter-config`
7. From the adapter `dist/lib` folder, copy all .jar files to

   `<PF-install>/server/default/lib`

2.10 Configure PingFederate-IdP

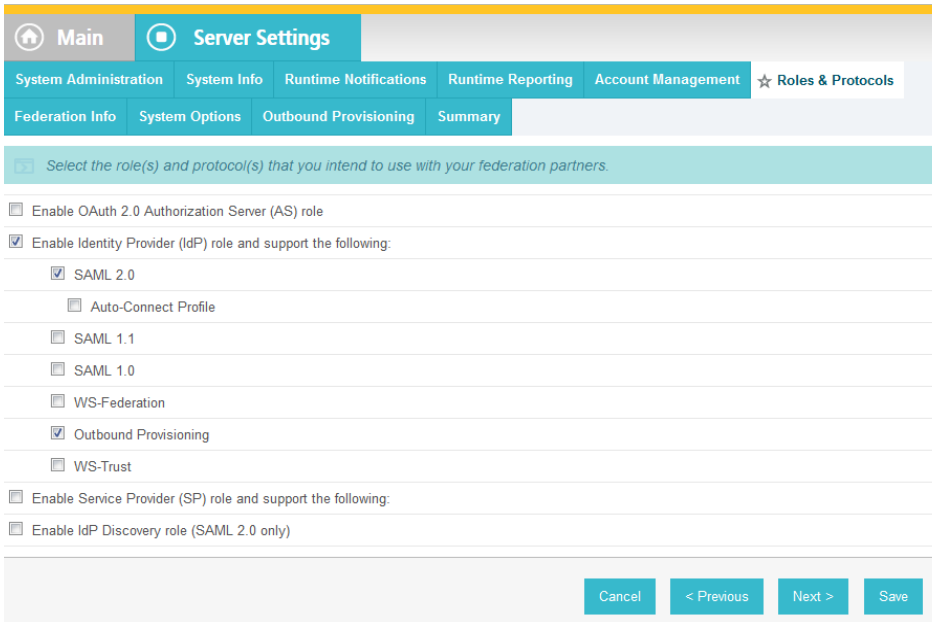
Follow the instructions in the subsections below to configure PingFederate as the Federation Server for the Identity Provider.

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



2.10.1 Configure SAML Protocol

1. On the **Main** menu under **System Settings**, click **Server Settings**.
2. Click the **Roles and Protocols** tab. Select **Enable Identity Provider (IdP) role and support the following**.
3. Select **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

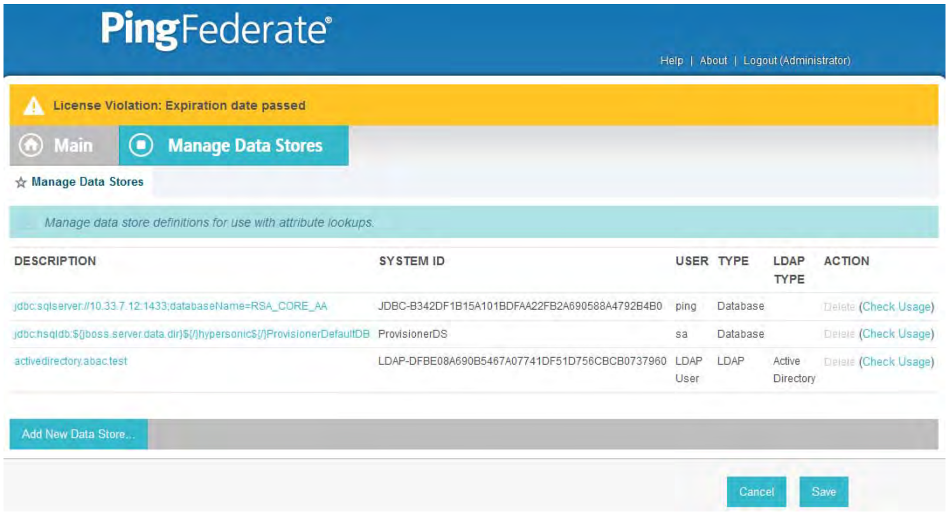
☐ Enable Service Provider (SP) role and support the following:

☐ Enable IdP Discovery role (SAML 2.0 only)

4. Click **Save**.

2.10.2 Create Data Store for Microsoft AD

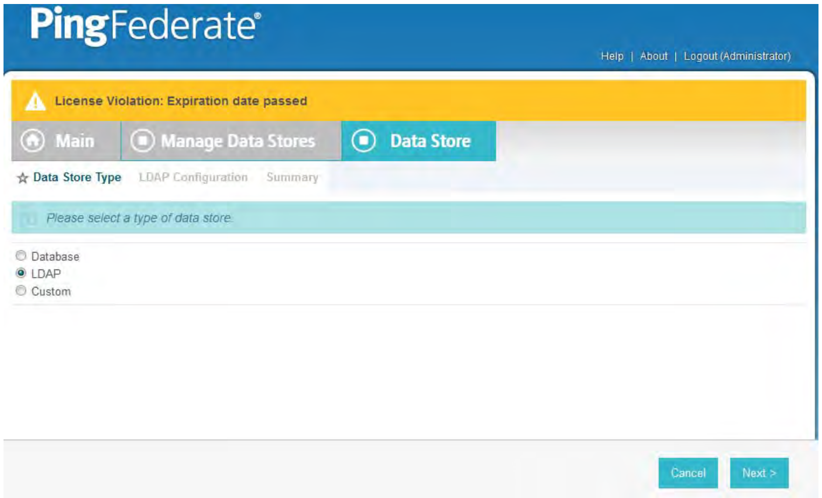
1. On the **Main** menu under **System Settings**, click **Data Stores**.



Manage data store definitions for use with attribute lookups.

DESCRIPTION	SYSTEM ID	USER	TYPE	LDAP TYPE	ACTION
jdbc:sqlserver://10.33.7.12:1433;databaseName=RSA_CORE_AA	JDBC-B342DF1B15A101BDFAA22FB2A690588A4792B4B0	ping	Database		Delete (Check Usage)
jdbc:hsqldb:${jboss.server.data.dir}${/}hypersonic${/}ProvisionerDefaultDB	ProvisionerDS	sa	Database		Delete (Check Usage)
activedirectory.abac.test	LDAP-DFBE08A690B5467A07741DF51D756CBCB0737960	LDAP User	LDAP	Active Directory	Delete (Check Usage)

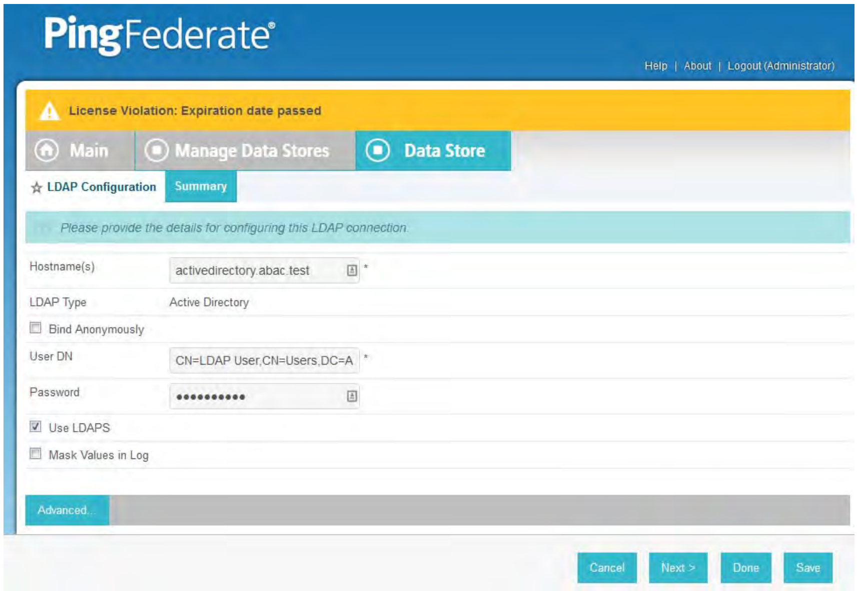
2. Select **LDAP**.



Please select a type of data store.

○ Database
● LDAP
○ Custom

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 section 2.4.1, 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.
8. Click **Next**. Then, click **Save** on the **Summary** screen.



License Violation: Expiration date passed

Please provide the details for configuring this LDAP connection

Hostname(s): activedirectory.abac.test *

LDAP Type: Active Directory

□ Bind Anonymously

User DN: CN=LDAP User,CN=Users,DC=A *

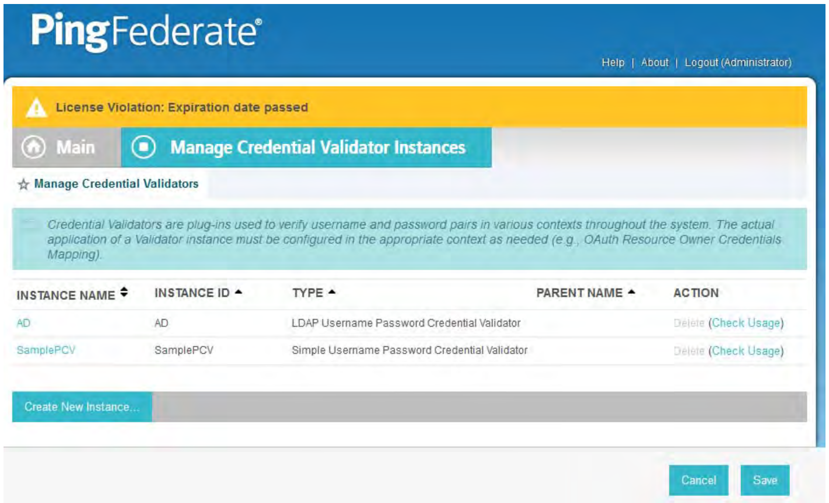
Password: ••••••••••

☑ Use LDAPS

□ Mask Values in Log

2.10.3 Create Credential Validator for Microsoft AD

1. On the **Main** menu under Authentication, click Password Credential Validators.

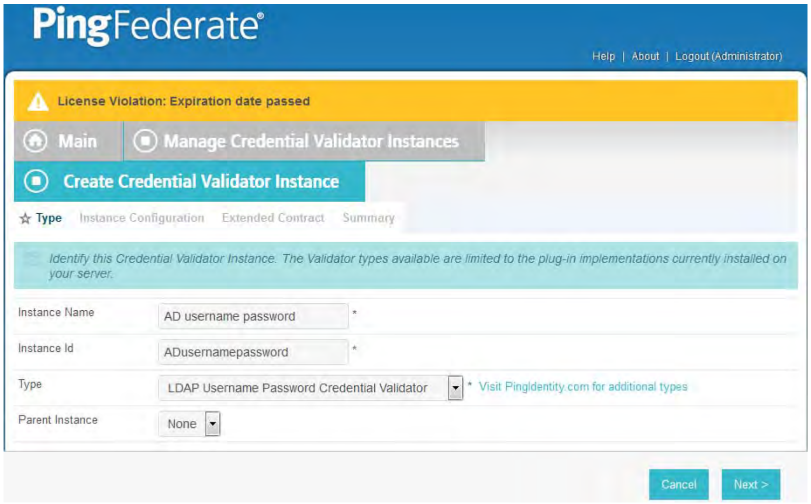

PingFederate®
Help | About | Logout (Administrator)
Main
Manage Credential Validator Instances
Manage Credential Validators
Create New Instance...
Cancel
Save

License Violation: Expiration date passed

Credential Validators are plug-ins used to verify username and password pairs in various contexts throughout the system. The actual application of a Validator instance must be configured in the appropriate context as needed (e.g., OAuth Resource Owner Credentials Mapping).

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

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



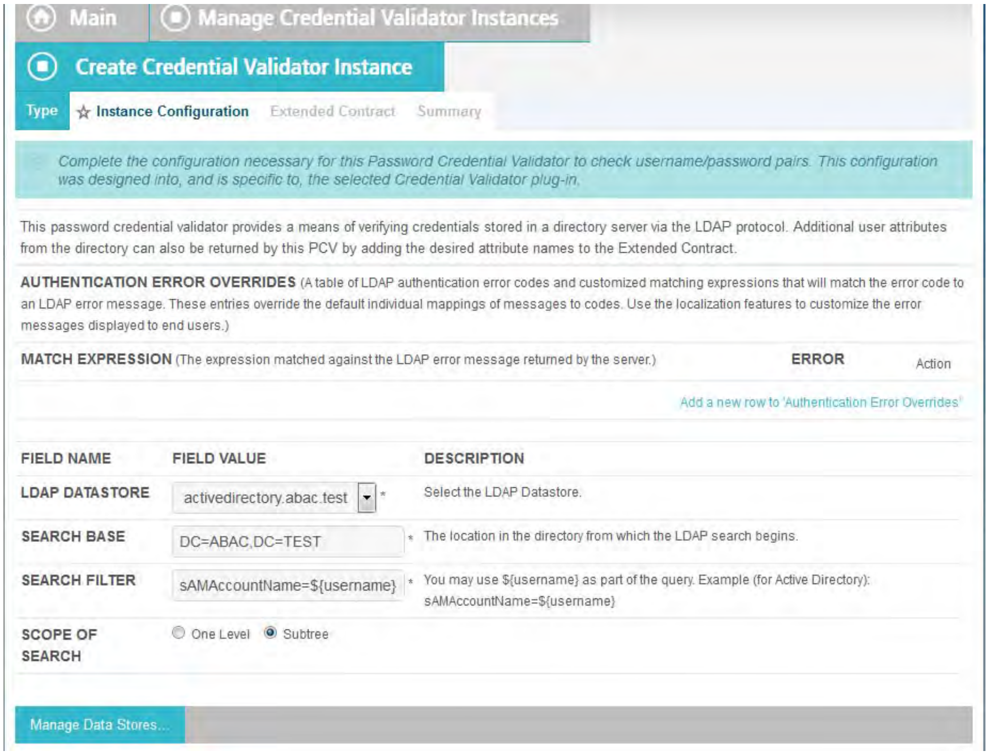
License Violation: Expiration date passed

Create Credential Validator Instance

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

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

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



Create Credential Validator Instance

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.

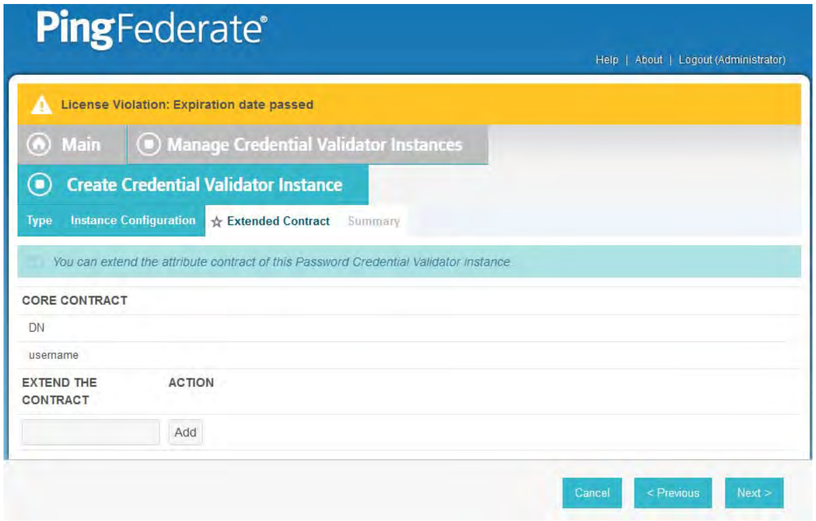
AUTHENTICATION ERROR OVERRIDES (A table of LDAP authentication error codes and customized matching expressions that will match the error code to an LDAP error message. These entries override the default individual mappings of messages to codes. Use the localization features to customize the error messages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

MATCH EXPRESSION (The expression matched against the LDAP error message returned by the server.)	ERROR	Action
		Add a new row to 'Authentication Error Overrides'

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	○ One Level ● Subtree	

10. Click **Next**.

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


PingFederate®
Help | About | Logout (Administrator)
Main
Manage Credential Validator Instances
Create Credential Validator Instance
Type
Instance Configuration
☆ Extended Contract
Summary
Add
Cancel
< Previous
Next >

License Violation: Expiration date passed

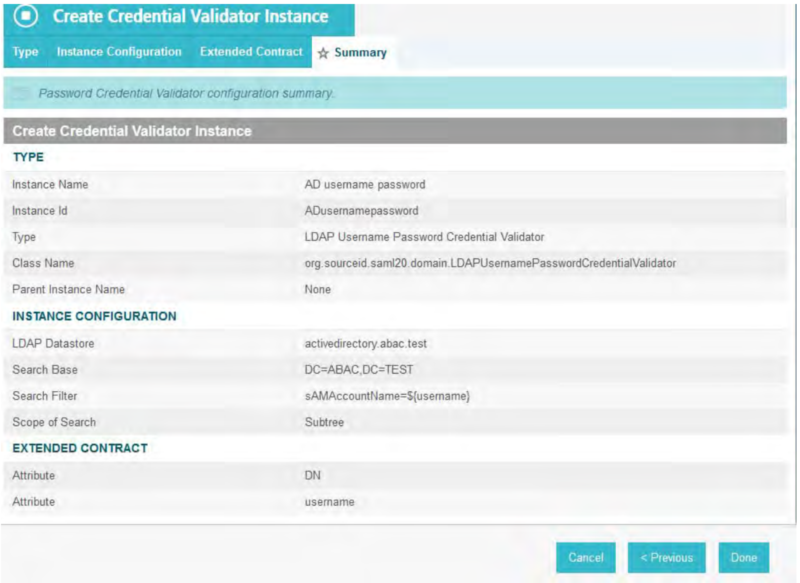
You can extend the attribute contract of this Password Credential Validator instance

CORE CONTRACT
DN
username

EXTEND THE CONTRACT	ACTION
	Add

11. Click **Next**.

 You should see a summary page.

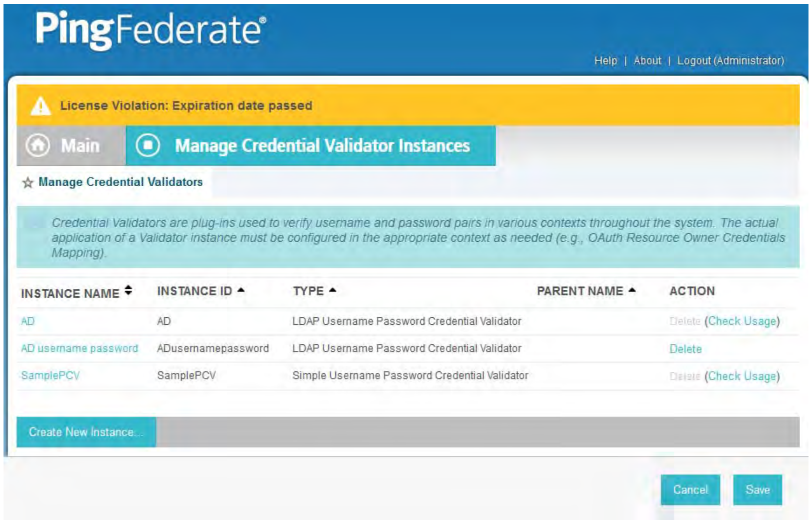


Password Credential Validator configuration summary.

Create Credential Validator Instance	
TYPE	
Instance Name	AD username password
Instance Id	ADusernamepassword
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None
INSTANCE CONFIGURATION	
LDAP Datastore	activedirectory.abac.test
Search Base	DC=ABAC,DC=TEST
Search Filter	sAMAccountName=${username}
Scope of Search	Subtree
EXTENDED CONTRACT	
Attribute	DN
Attribute	username

12. Click **Done**.

 You should see a list of the credential validator instances, including the newly added validator (e.g. **AD username password**).



PingFederate®
Help | About | Logout (Administrator)
License Violation: Expiration date passed
Main
Manage Credential Validator Instances
☆ Manage Credential Validators

Credential Validators are plug-ins used to verify username and password pairs in various contexts throughout the system. The actual application of a Validator instance must be configured in the appropriate context as needed (e.g., OAuth Resource Owner Credentials Mapping).

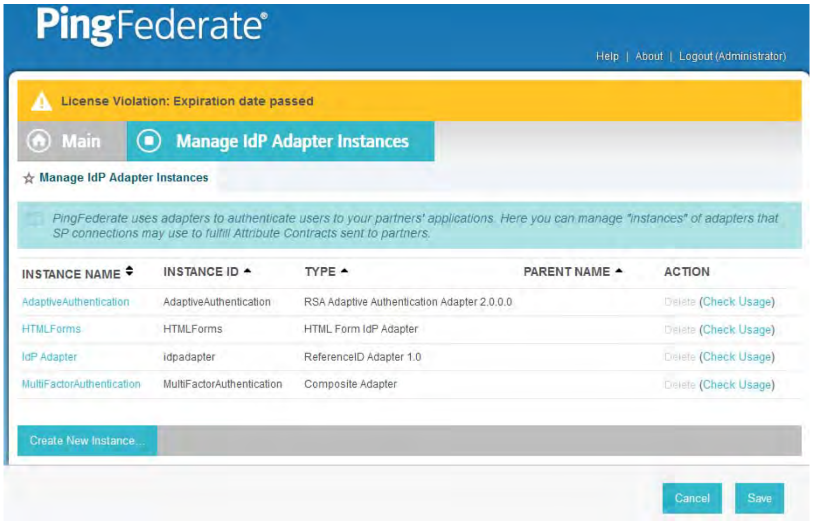
INSTANCE NAME	INSTANCE ID	TYPE	PARENT NAME	ACTION
AD	AD	LDAP Username Password Credential Validator		Delete (Check Usage)
AD username password	ADusernamepassword	LDAP Username Password Credential Validator		Delete
SamplePCV	SamplePCV	Simple Username Password Credential Validator		Delete (Check Usage)

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

2.10.4 Create IdP Adapter for Authentication with Microsoft AD via Web Browser Form

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

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



PingFederate®
Help | About | Logout (Administrator)
License Violation: Expiration date passed
Main
Manage IdP Adapter Instances
☆ Manage IdP Adapter Instances

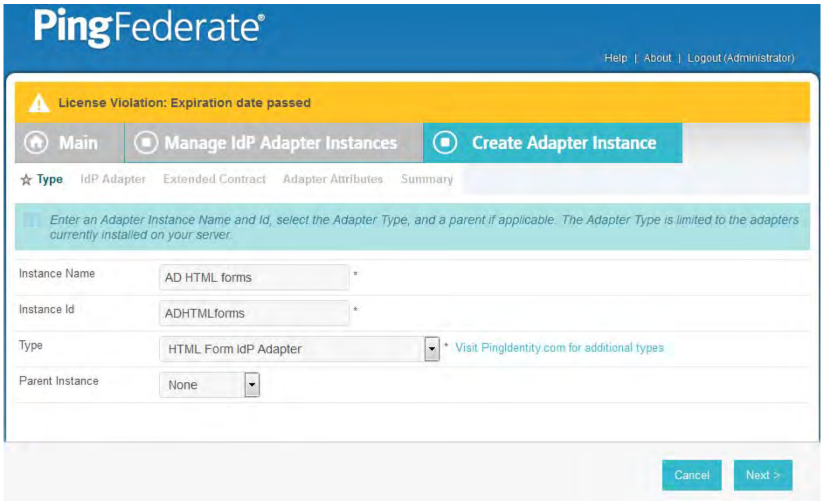
PingFederate uses adapters to authenticate users to your partners' applications. Here you can manage "instances" of adapters that SP connections may use to fulfill Attribute Contracts sent to partners.

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

2. Click **Create New Instance**.

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**).

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

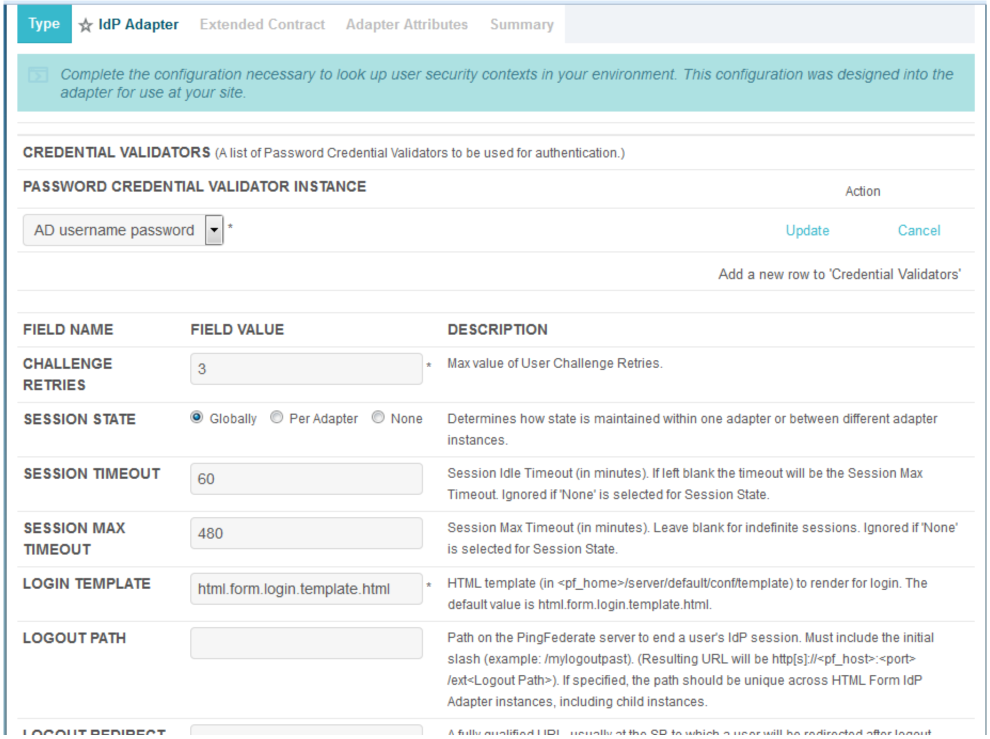


Enter an Adapter Instance Name and Id, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.

Instance Name	AD HTML forms *
Instance Id	ADHTMLforms *
Type	HTML Form IdP Adapter * Visit PingIdentity.com for additional types
Parent Instance	None

5. Click **Next**.

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



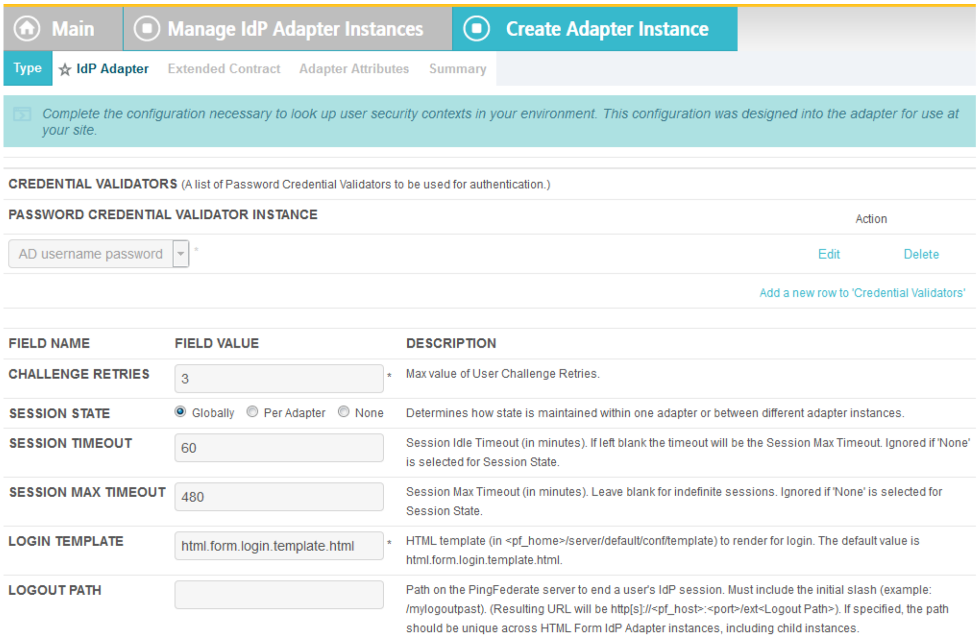
Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

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

PASSWORD CREDENTIAL VALIDATOR INSTANCE	Action
AD username password *	Update Cancel

FIELD NAME	FIELD VALUE	DESCRIPTION
CHALLENGE RETRIES	3 *	Max value of User Challenge Retries.
SESSION STATE	● Globally ○ Per Adapter ○ 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.

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



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

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

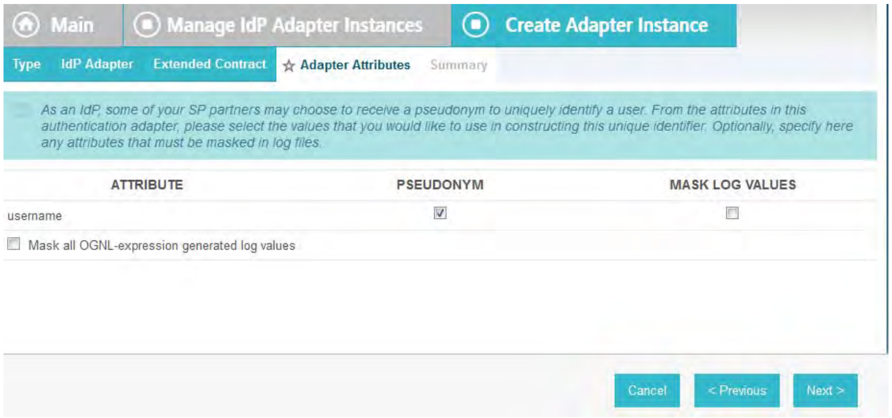
PASSWORD CREDENTIAL VALIDATOR INSTANCE	Action	
AD username password *	Edit	Delete

Add a new row to 'Credential Validators'

FIELD NAME	FIELD VALUE	DESCRIPTION
CHALLENGE RETRIES	3 *	Max value of User Challenge Retries.
SESSION STATE	● Globally ○ Per Adapter ○ 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.

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

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

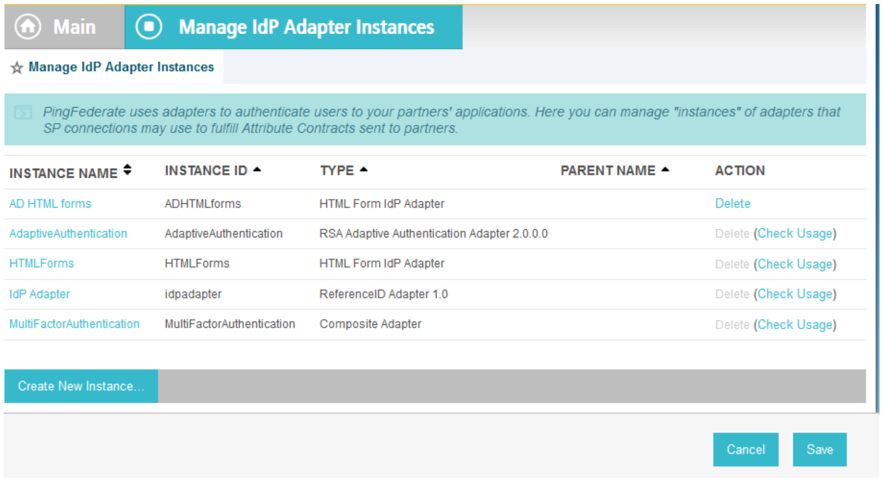


As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked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

ATTRIBUTE	PSEUDONYM	MASK LOG VALUES
username	☑	□

□ Mask all OGNL-expression generated log values

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



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

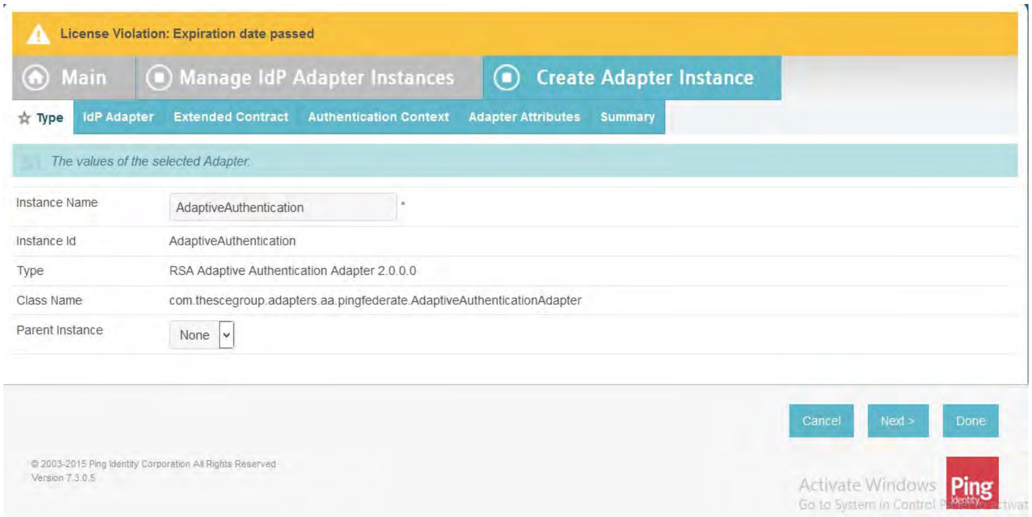
INSTANCE NAME	INSTANCE ID	TYPE	PARENT NAME	ACTION
AD HTML forms	ADHTMLforms	HTML Form IdP Adapter		Delete
AdaptiveAuthentication	AdaptiveAuthentication	RSA Adaptive Authentication Adapter 2.0.0.0		Delete (Check Usage)
HTMLForms	HTMLForms	HTML Form IdP Adapter		Delete (Check Usage)
IdP Adapter	idpadapter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

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

2.10.5 Create IdP Adapter for Two-factor Authentication with RSA AA

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

1. On the **Main** menu under Application Integration Settings, click Adapters.
2. On the **Manage IdP Adapters** screen, click **Create New Instance**.
3. On the **Type** screen, enter an **Instance Name** and **Instance ID**.
4. Set the following settings on the Adapter Type page before clicking **Next**:
    a. **Instance Name**: [Instance Name]
    b. **Instance ID**: [Instance ID]
    c. **Type**: **RSA Adaptive Authentication Adapter 2.0**
    d. **Class Name**: **com.thescegroup.adapters.aa.pingfederate.AdaptiveAuthenticationAdapter**
    e. **Parent Instance**: **None**



The values of the selected Adapter.

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

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

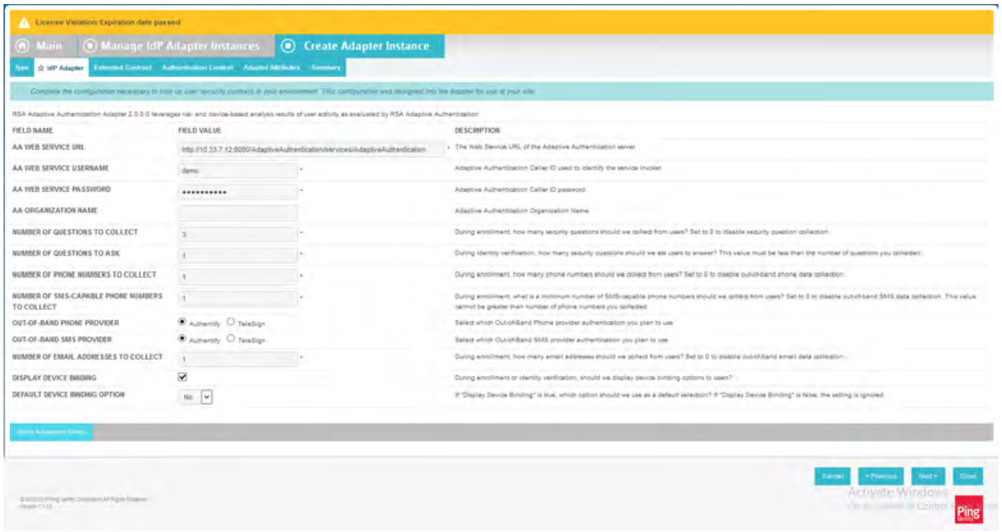
5. On the **IdP Adapter** configuration page, click **Show Advanced Fields** and input the following parameters while leaving the rest as default, before clicking **Next**:
   a. **AA Web Service URL**:

      http://<RSA Server DNS>:8080/AdaptiveAuthentication/services/AdaptiveAuthentication

   b. **AA Web Service Username**: [username]

   c. **AA Web Service Password**: [password]

   Note: The credentials must match on the RSA server.

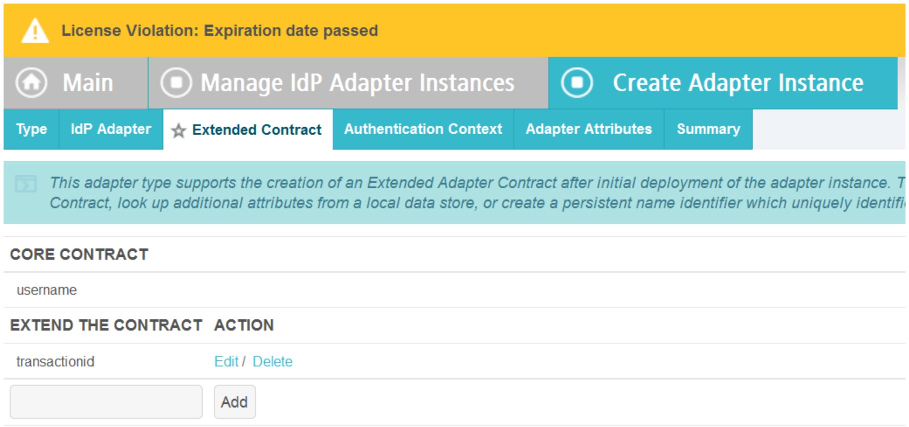


Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

RSA Adaptive Authentication Adapter 2.0.0.0 leverages risk- and device-based analysis results of user activity as evaluated by RSA Adaptive Authentication

FIELD NAME	FIELD VALUE	DESCRIPTION
AA WEB SERVICE URL	http://10.33.7.12:8080/AdaptiveAuthentication/services/AdaptiveAuthentication *	The Web Service URL of the Adaptive Authentication server
AA WEB SERVICE USERNAME	demo *	Adaptive Authentication Caller ID used to identify the service invoker
AA WEB SERVICE PASSWORD	••••••••••• *	Adaptive Authentication Caller ID password
AA ORGANIZATION NAME		Adaptive Authentication Organization Name
NUMBER OF QUESTIONS TO COLLECT	3 *	During enrollment, how many security questions should we collect from users? Set to 0 to disable security question collection.
NUMBER OF QUESTIONS TO ASK	1 *	During identity verification, how many security questions should we ask users to answer? This value must be less than the number of questions you collected.
NUMBER OF PHONE NUMBERS TO COLLECT	1 *	During enrollment, how many phone numbers should we collect from users? Set to 0 to disable out-of-band phone data collection.
NUMBER OF SMS-CAPABLE PHONE NUMBERS TO COLLECT	1 *	During enrollment, what is a minimum number of SMS-capable phone numbers should we collect from users? Set to 0 to disable out-of-band SMS data collection. This value cannot be greater than number of phone numbers you collected.
OUT-OF-BAND PHONE PROVIDER	● Authentify ○ TeleSign	Select which Out-of-Band Phone provider authentication you plan to use.
OUT-OF-BAND SMS PROVIDER	● Authentify ○ TeleSign	Select which Out-of-Band SMS provider authentication you plan to use.
NUMBER OF EMAIL ADDRESSES TO COLLECT	1 *	During enrollment, how many email addresses should we collect from users? Set to 0 to disable out-of-band email data collection.
DISPLAY DEVICE BINDING	☑	During enrollment or identity verification, should we display device binding options to users?
DEFAULT DEVICE BINDING OPTION	No	If "Display Device Binding" is true, which option should we use as a default selection? If "Display Device Binding" is false, the setting is ignored.

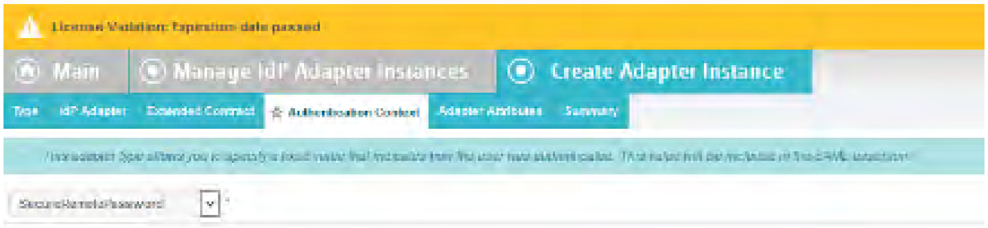
6. On the **Extended Contract** screen, type **transactionid** (all lowercase). Then, click **Add**. By default, **username** should already be listed under **Core Contract**.



This adapter type supports the creation of an Extended Adapter Contract after initial deployment of the adapter instance. T
Contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifi

CORE CONTRACT	
username	
EXTEND THE CONTRACT	**ACTION**
transactionid	Edit / Delete
	Add

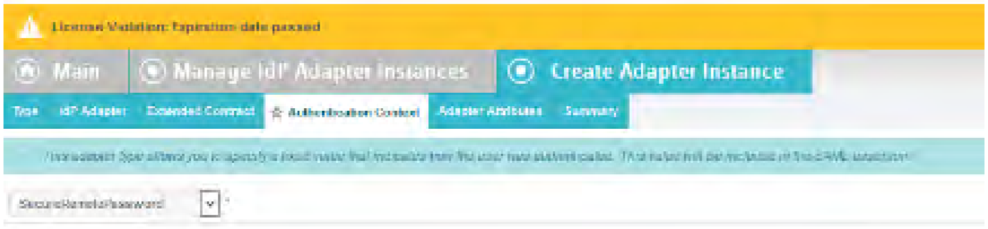
7. Click **Next**.
8. On the **Authentication Context** screen, select **SecureRemotePassword** as the fixed value for authentication. This value will be included in the SAML assertion. Click **Next**.



This adapter type allows you to specify a fixed value that indicates how the user was authenticated. This value will be included in the SAML assertion.

SecureRemotePassword *

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



This adapter type allows you to specify a fixed value that indicates how the user was authenticated. This value will be included in the SAML assertion.

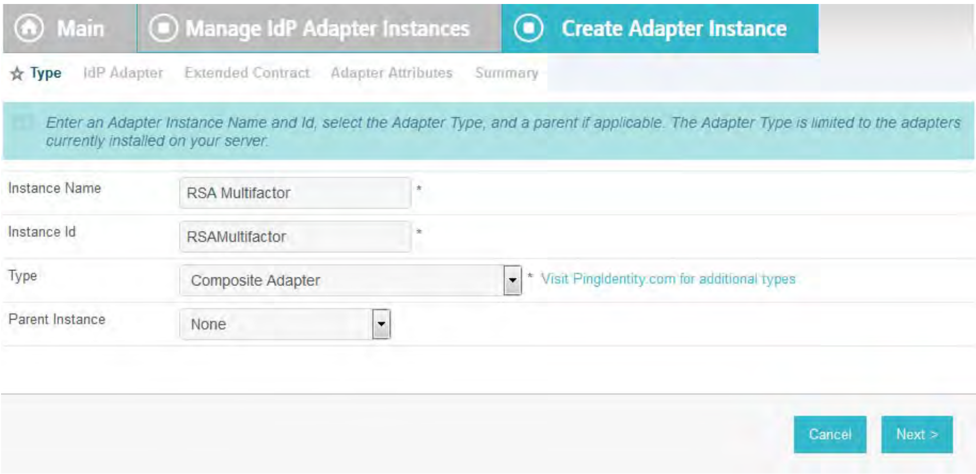
SecureRemotePassword *

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

2.10.6 Create Composite IdP Adapter Integrating Microsoft AD and RSA AA

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

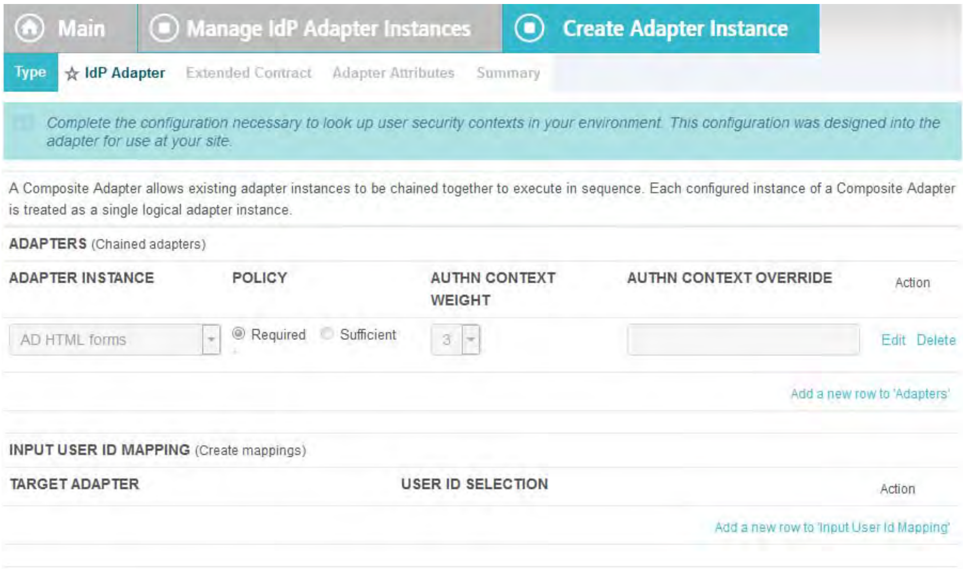
1. On the **Main** menu under **Application Integration Settings**, click **Adapters**.
2. On the **Manage IdP Adapters** screen, click **Create New Instance**.
3. Enter a unique **Instance Name** you would like to use to refer to this configuration (e.g. **RSA Multifactor**).
4. Enter a unique **Instance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



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	RSA Multifactor *
Instance Id	RSAMultifactor *
Type	Composite Adapter *
Parent Instance	None

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



Main | Manage IdP Adapter Instances | Create Adapter Instance

Type | ☆ IdP Adapter | Extended Contract | Adapter Attributes | Summary

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

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

ADAPTERS (Chained adapters)

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
AD HTML forms	◉ Required ○ Sufficient	3		Edit Delete

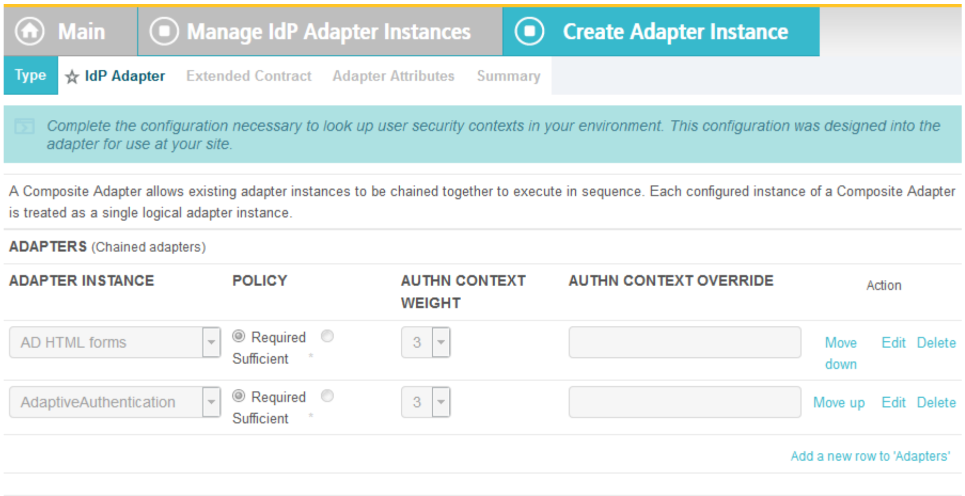
Add a new row to 'Adapters'

INPUT USER ID MAPPING (Create mappings)

TARGET ADAPTER	USER ID SELECTION	Action

Add a new row to 'Input User Id Mapping'

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**.



Main | Manage IdP Adapter Instances | Create Adapter Instance

Type | ☆ IdP Adapter | Extended Contract | Adapter Attributes | Summary

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

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

ADAPTERS (Chained adapters)

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
AD HTML forms	◉ Required ○ Sufficient	3		Move down Edit Delete
AdaptiveAuthentication	◉ Required ○ Sufficient	3		Move up Edit Delete

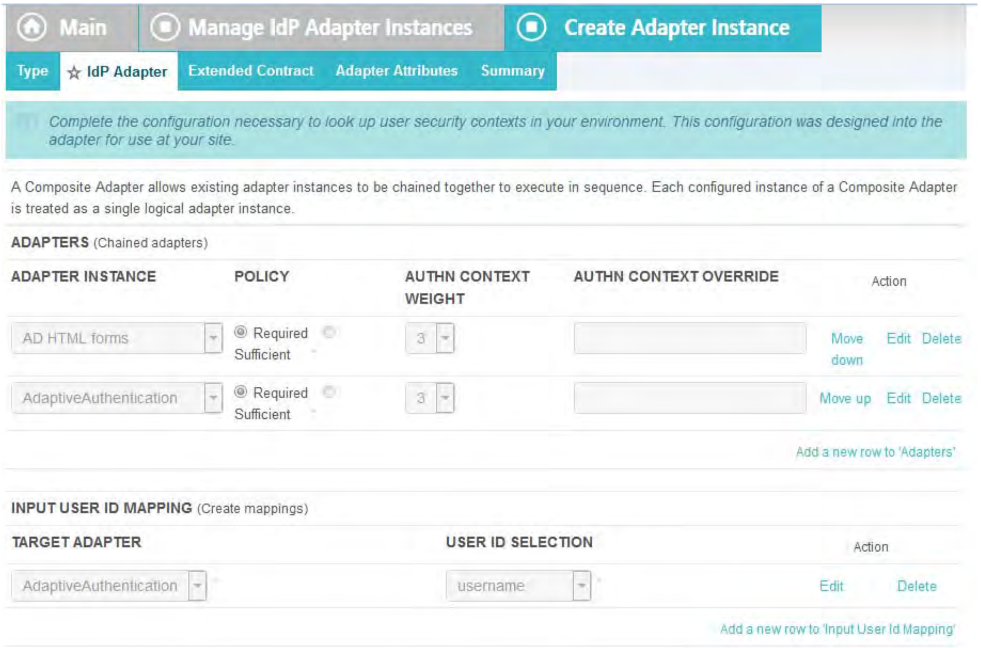
Add a new row to 'Adapters'

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**).

12. In the new **USER ID SELECTION** box, select **username**.

13. Under **TARGET ADAPTER** click the **Update** hyperlink on the right side of the page. This will cause the selection box to turn grey.



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

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

ADAPTERS (Chained adapters)

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
AD HTML forms	● Required ○ Sufficient	3		Move down Edit Delete
AdaptiveAuthentication	● Required ○ Sufficient	3		Move up Edit Delete

Add a new row to 'Adapters'

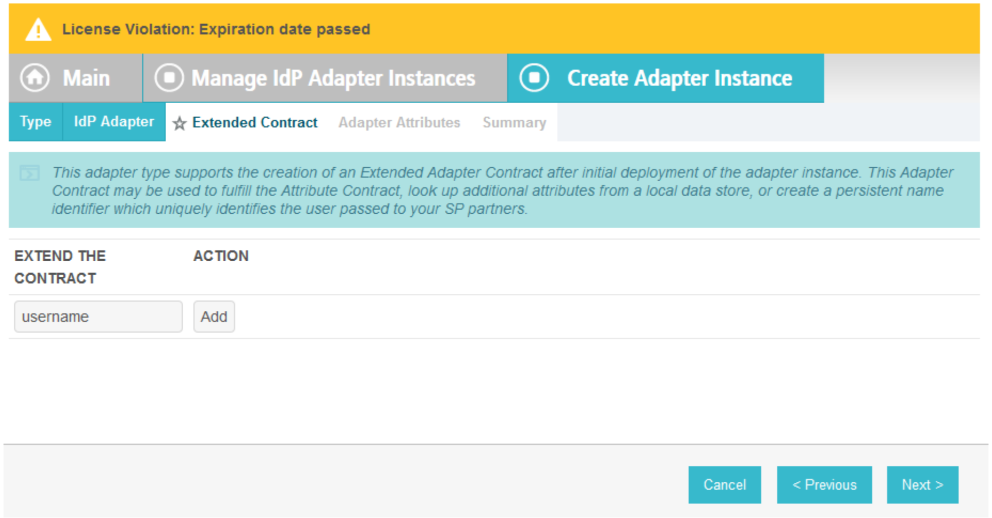
INPUT USER ID MAPPING (Create mappings)

TARGET ADAPTER	USER ID SELECTION	Action
AdaptiveAuthentication	username	Edit Delete

Add a new row to 'Input User Id Mapping'

14. Click **Next**.

15. On the **Extended Contract** screen, enter the value **username** in the **EXTEND THE CONTRACT** field.

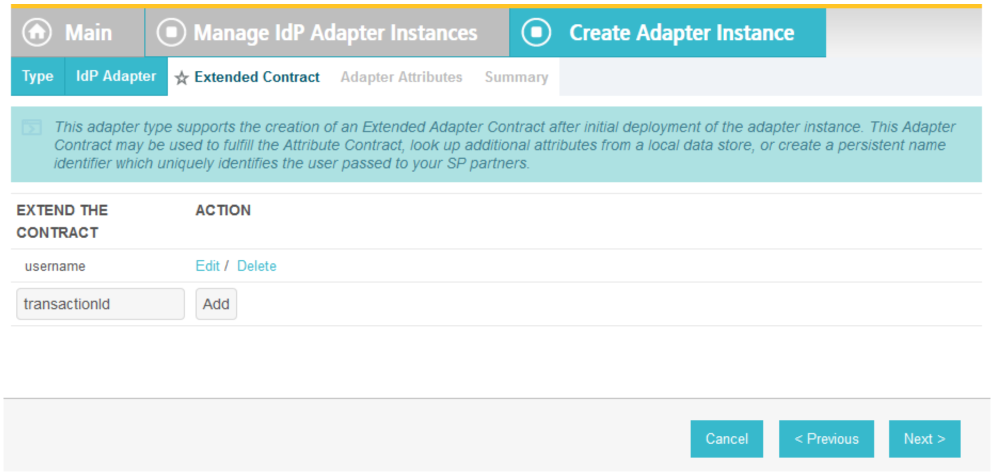


License Violation: Expiration date passed

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

EXTEND THE CONTRACT	ACTION
username	Add

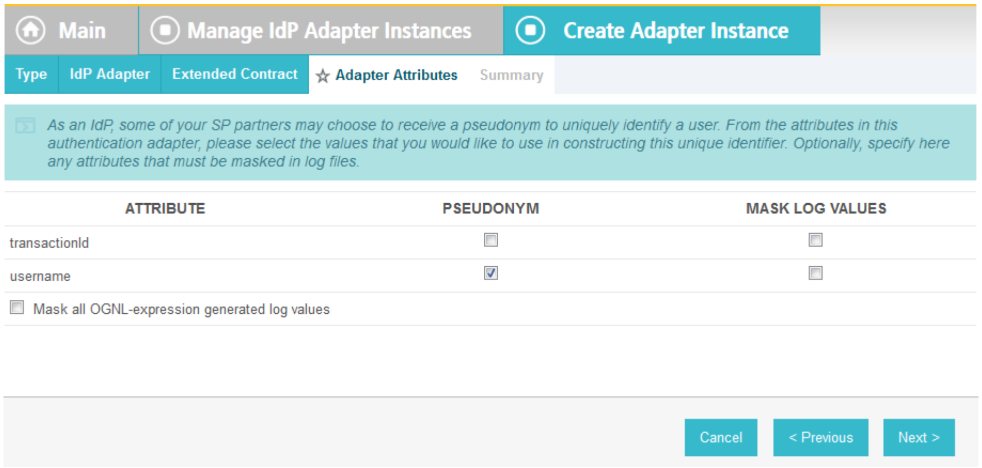
16. Click **Add**. Enter the value **transactionid** (all lowercase) in the **EXTEND THE CONTRACT** field.



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

EXTEND THE CONTRACT	ACTION
username	Edit / Delete
transactionId	Add

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



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
transactionId	□	□
username	☑	□

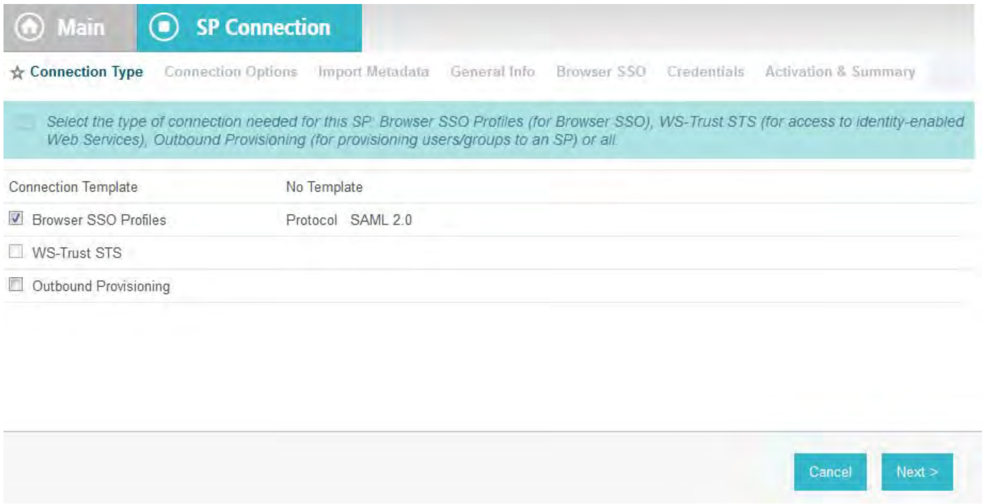
□ Mask all OGNL-expression generated log values

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

2.10.7 Configure the Federation Connection to the Relying Party

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

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



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

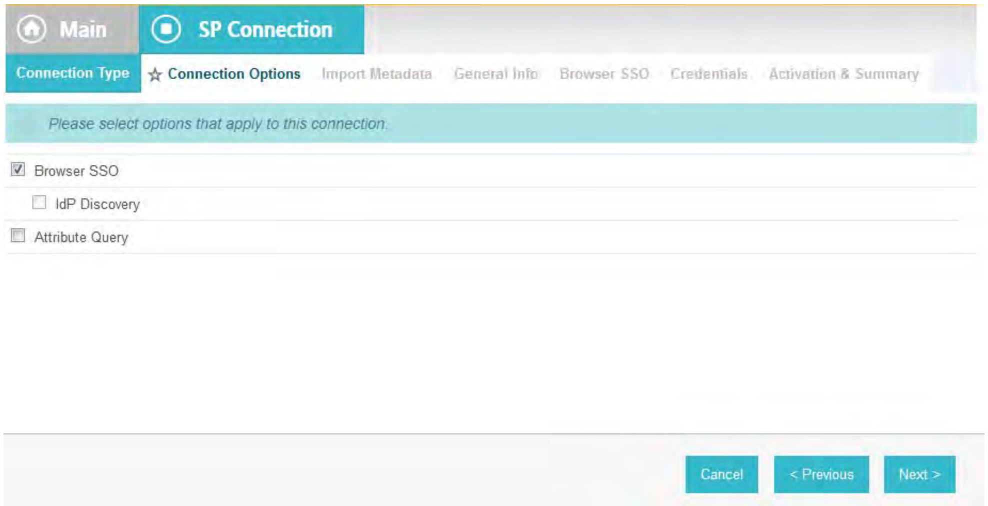
Connection Template No Template

☑ Browser SSO Profiles Protocol SAML 2.0

□ WS-Trust STS

□ Outbound Provisioning

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



Please select options that apply to this connection.

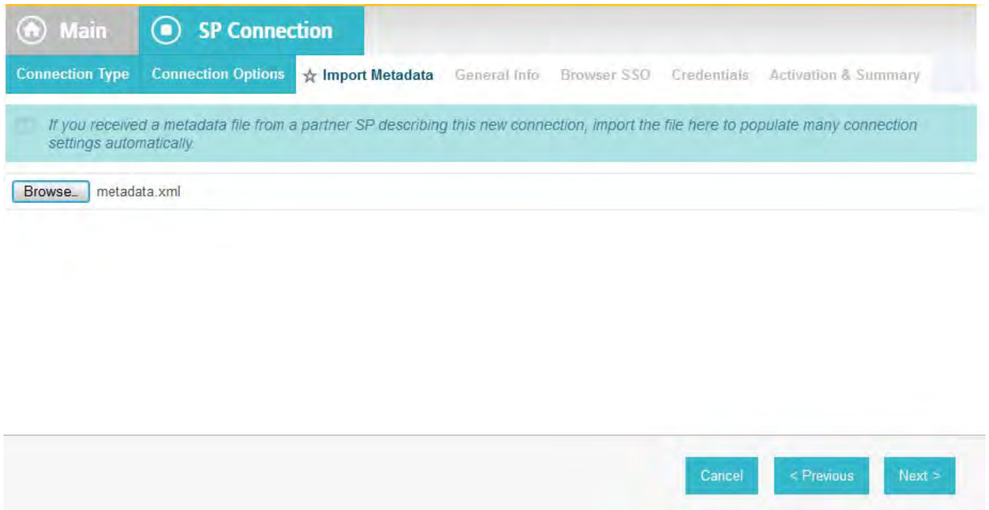
☑ Browser SSO

□ IdP Discovery

□ Attribute Query

4. Click **Next**.

5. On the Import Metadata screen, click **Browse** and select the metadata file that you exported from the Relying Party’s PingFederate server.



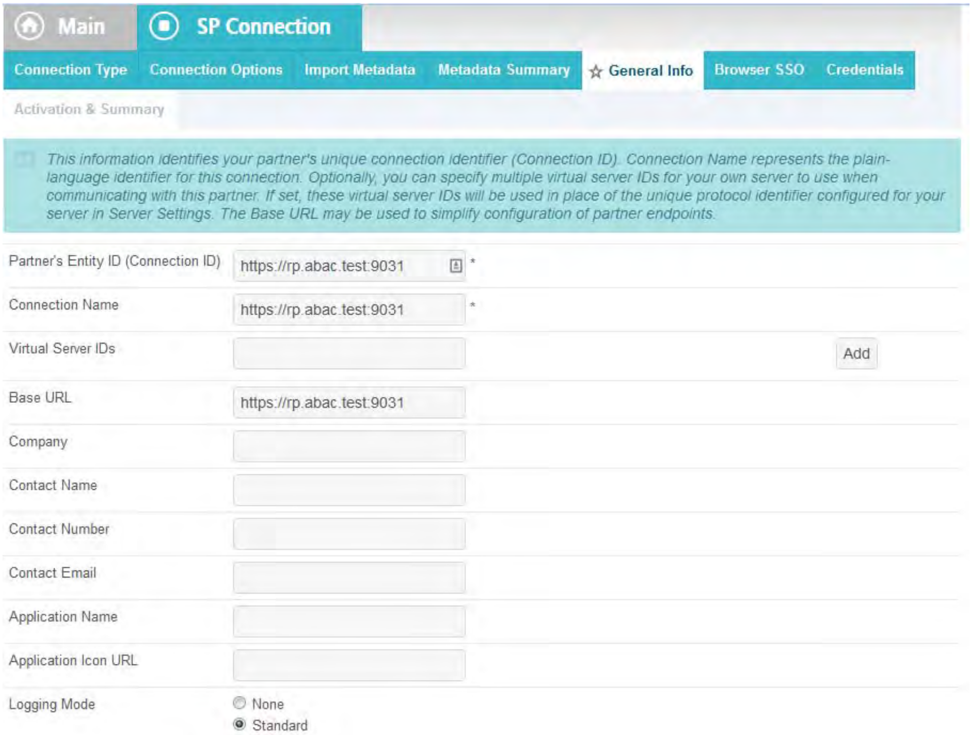
If you received a metadata file from a partner SP describing this new connection, import the file here to populate many connection settings automatically.

metadata.xml

6. Click **Next**.

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

8. On the General Info screen you should see some configuration information (e.g. **Base URL**) about the Relying Party that was taken from the metadata file that you selected earlier.

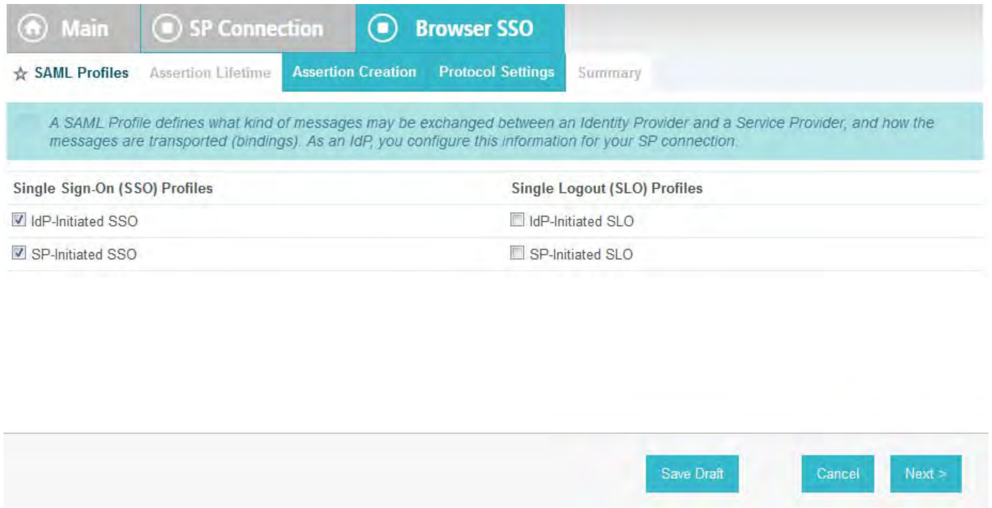


This information identifies your partner's unique connection identifier (Connection ID). Connection Name represents the plain-language identifier for this connection. Optionally, you can specify multiple virtual server IDs for your own server to use when communicating with this partner. If set, these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

Partner's Entity ID (Connection ID)	https://rp.abac.test:9031 *
Connection Name	https://rp.abac.test:9031 *
Virtual Server IDs	
Base URL	https://rp.abac.test:9031
Company	
Contact Name	
Contact Number	
Contact Email	
Application Name	
Application Icon URL	
Logging Mode	○ None ● Standard

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

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



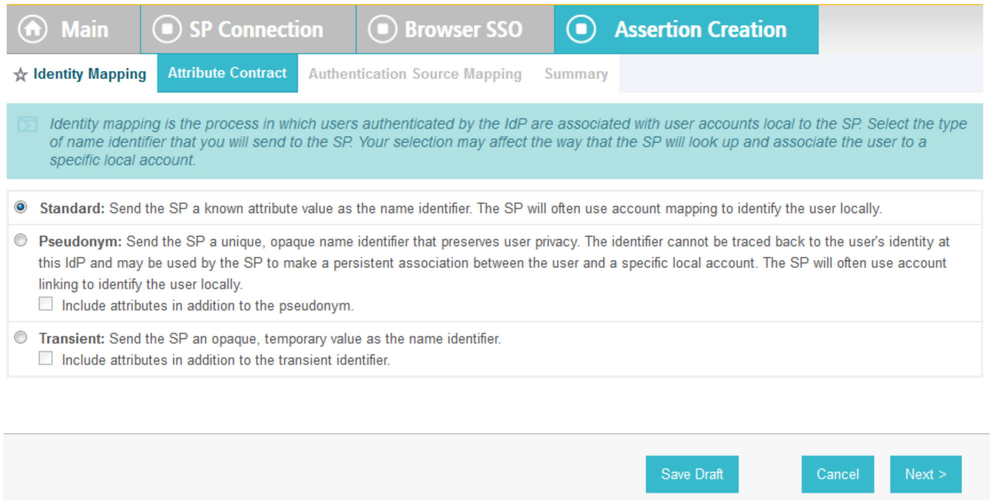
A SAML Profile defines what kind of messages may be exchanged between an Identity Provider and a Service Provider, and how the messages are transported (bindings). As an IdP, you configure this information for your SP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
☑ IdP-Initiated SSO	□ IdP-Initiated SLO
☑ SP-Initiated SSO	□ SP-Initiated SLO

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

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

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



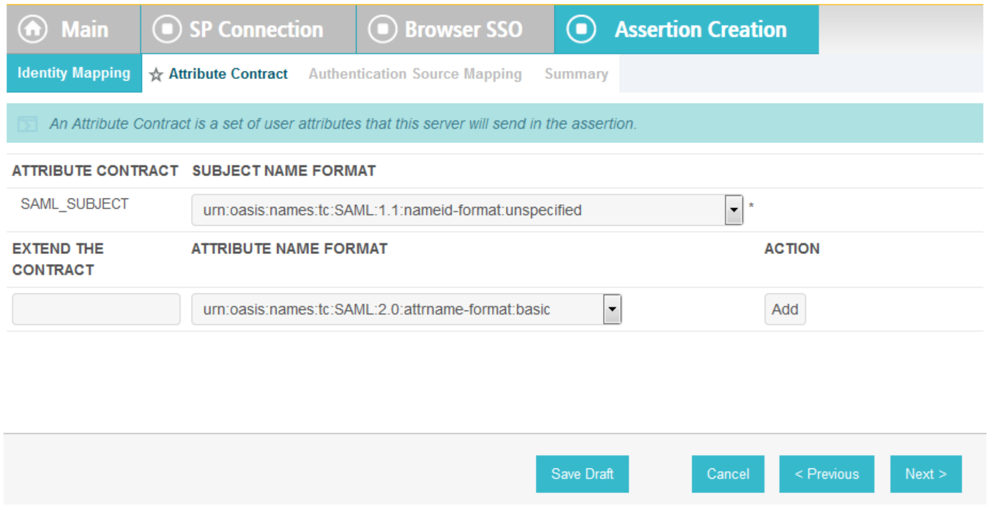
Identity mapping is the process in which users authenticated by the IdP are associated with user accounts local to the SP. Select the type of name identifier that you will send to the SP. Your selection may affect the way that the SP will look up and associate the user to a specific local account.

● **Standard:** Send the SP a known attribute value as the name identifier. The SP will often use account mapping to identify the user locally.

○ **Pseudonym:** Send the SP a unique, opaque name identifier that preserves user privacy. The identifier cannot be traced back to the user's identity at this IdP and may be used by the SP to make a persistent association between the user and a specific local account. The SP will often use account linking to identify the user locally.
□ Include attributes in addition to the pseudonym.

○ **Transient:** Send the SP an opaque, temporary value as the name identifier.
□ Include attributes in addition to the transient identifier.

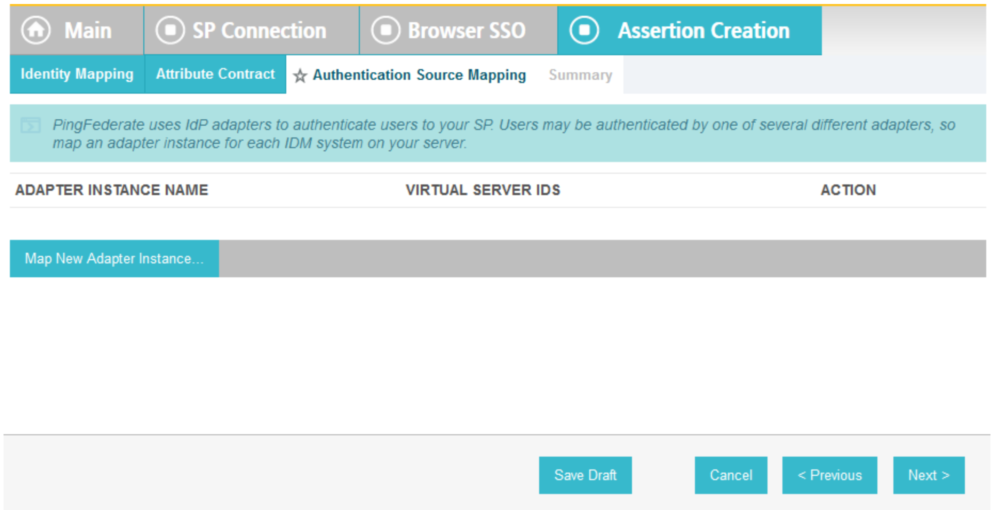
14. Click **Next**. This will bring up the Attribute Contract screen.



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT	SUBJECT NAME FORMAT	
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified *	
EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add

15. Click **Next**.

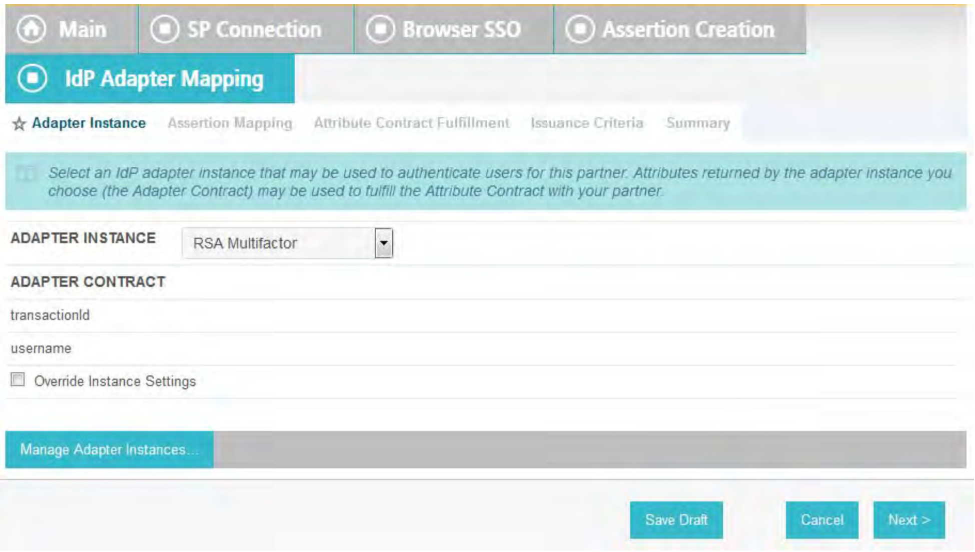


PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION

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

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



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

ADAPTER INSTANCE RSA Multifactor

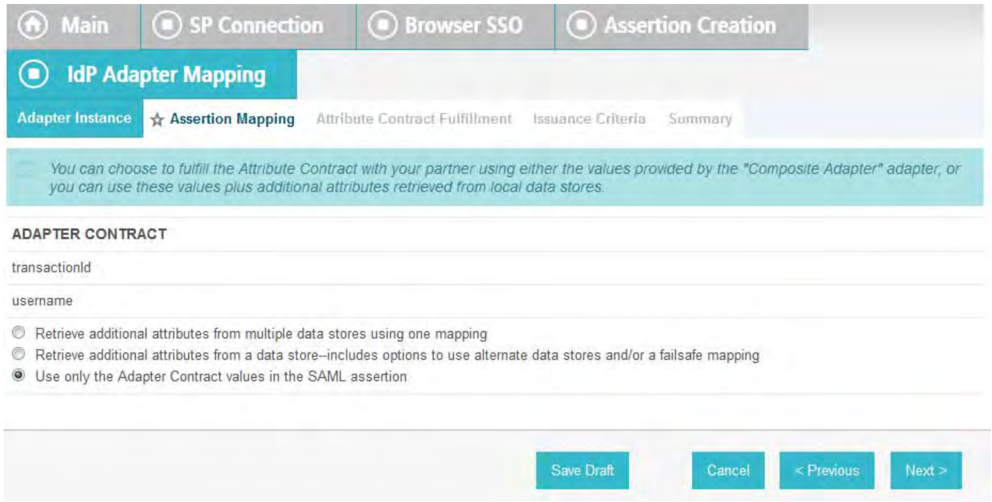
ADAPTER CONTRACT

transactionId

username

□ Override Instance Settings

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



You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "Composite Adapter" adapter, or you can use these values plus additional attributes retrieved from local data stores.

ADAPTER CONTRACT

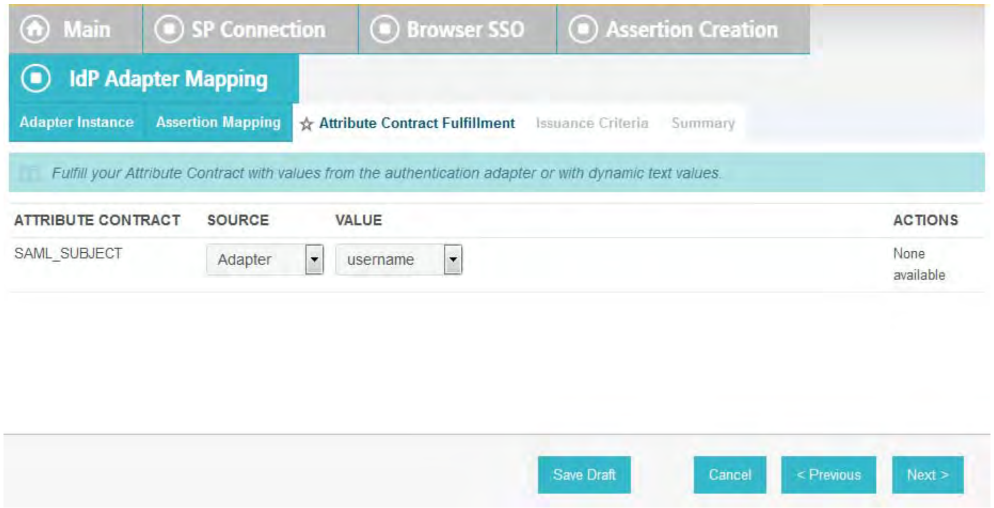
transactionId

username

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

19. Click **Next**.

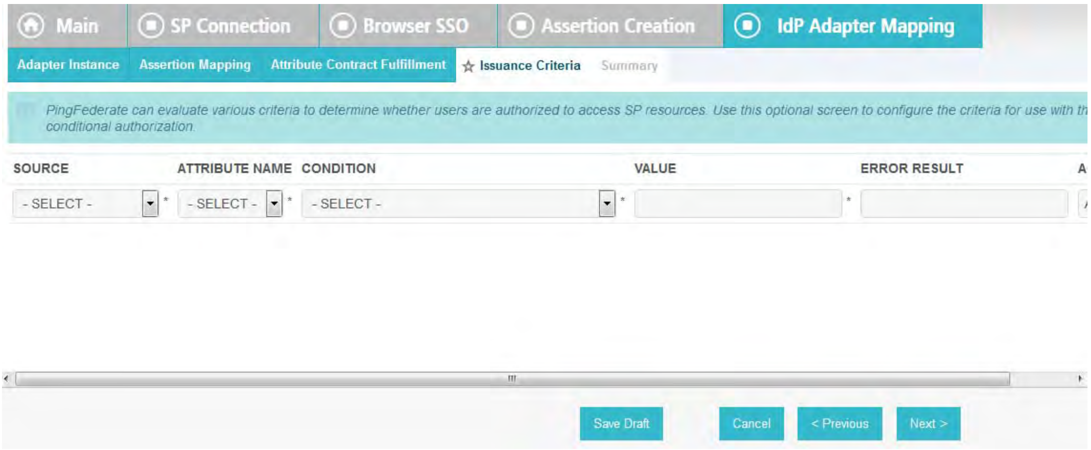
20. On the Attribute Contract Fulfillment screen, for **SAML_SUBJECT**, select **Adapter** for the **SOURCE** field and **username** for the **VALUE** field.



Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Adapter	username	None available

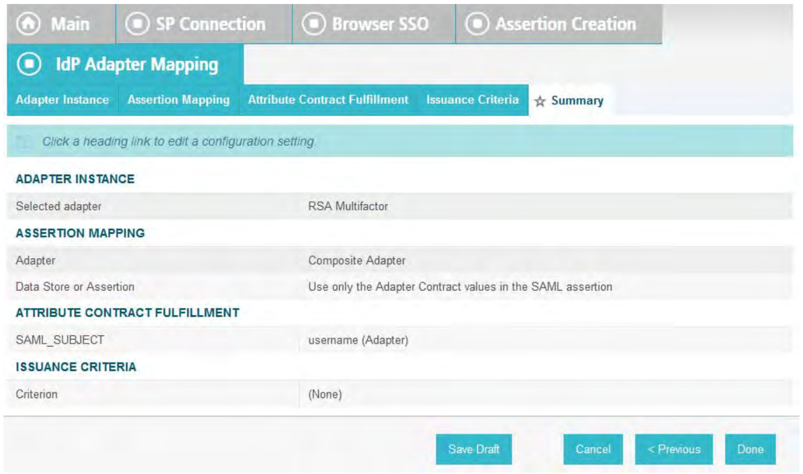
21. Click **Next**.



PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with th conditional authorization.

SOURCE	ATTRIBUTE NAME	CONDITION	VALUE	ERROR RESULT	A
- SELECT - *	- SELECT - *	- SELECT - *	*		

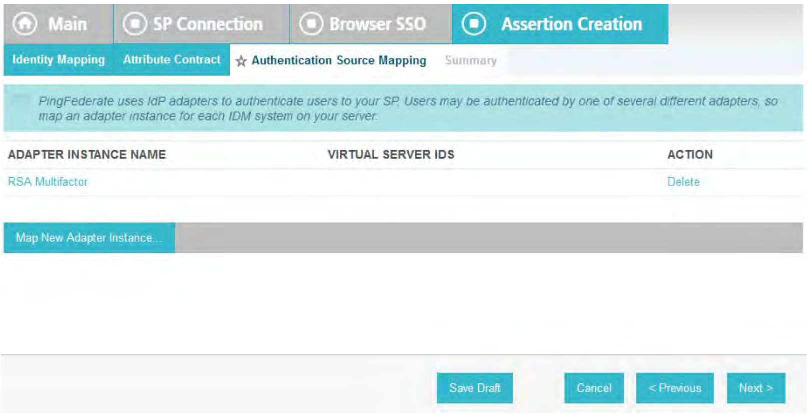
22. Click **Next**.



Click a heading link to edit a configuration setting.

ADAPTER INSTANCE	
Selected adapter	RSA Multifactor
ASSERTION MAPPING	
Adapter	Composite Adapter
Data Store or Assertion	Use only the Adapter Contract values in the SAML assertion
ATTRIBUTE CONTRACT FULFILLMENT	
SAML_SUBJECT	username (Adapter)
ISSUANCE CRITERIA	
Criterion	(None)

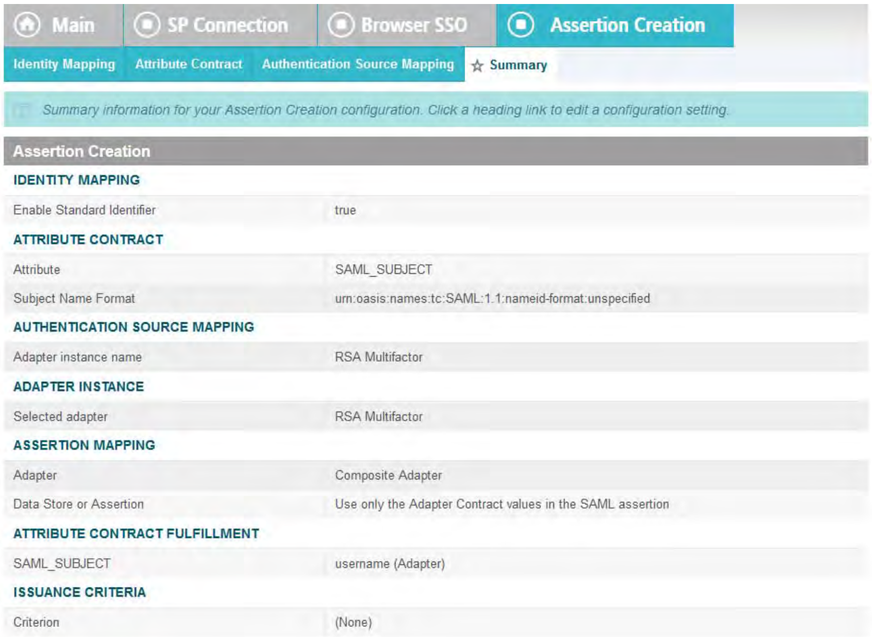
23. Click **Done**. This will bring you back to the Authentication Source Mapping screen and you should see the composite adapter (e.g. **RSA Multifactor**) listed.



PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION
RSA Multifactor		Delete

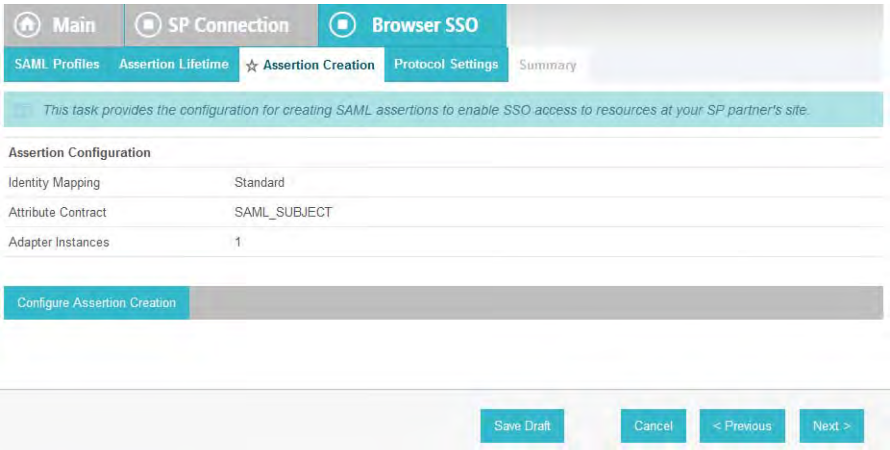
24. Click **Next**.



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

Assertion Creation	
IDENTITY MAPPING	
Enable Standard Identifier	true
ATTRIBUTE CONTRACT	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
AUTHENTICATION SOURCE MAPPING	
Adapter instance name	RSA Multifactor
ADAPTER INSTANCE	
Selected adapter	RSA Multifactor
ASSERTION MAPPING	
Adapter	Composite Adapter
Data Store or Assertion	Use only the Adapter Contract values in the SAML assertion
ATTRIBUTE CONTRACT FULFILLMENT	
SAML_SUBJECT	username (Adapter)
ISSUANCE CRITERIA	
Criterion	(None)

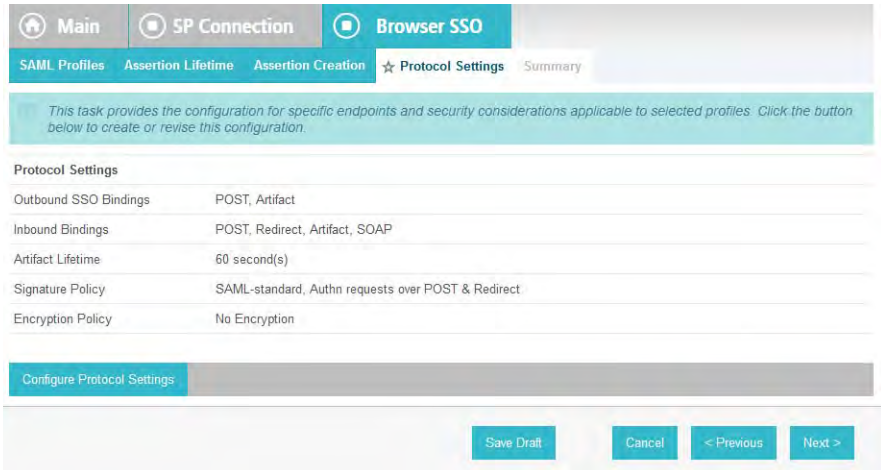
25. On the Summary screen, click **Done**. This will take you back to the Configure Assertion Creation screen.



This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration	
Identity Mapping	Standard
Attribute Contract	SAML_SUBJECT
Adapter Instances	1

26. Click **Next**.

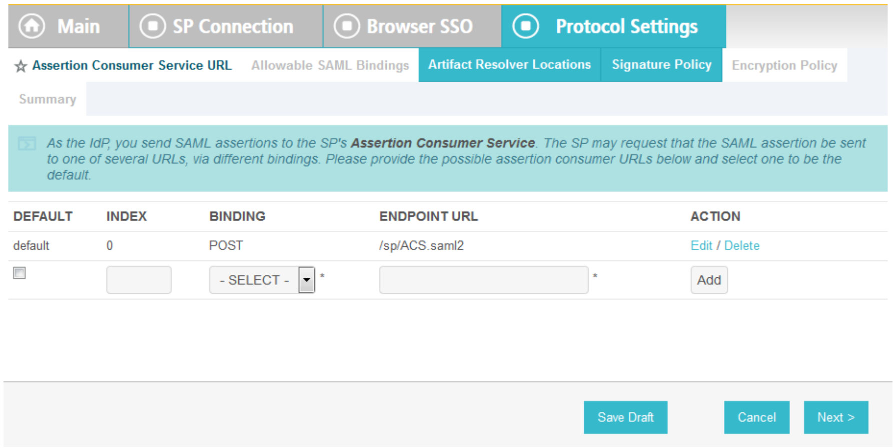


This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

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

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.

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**.

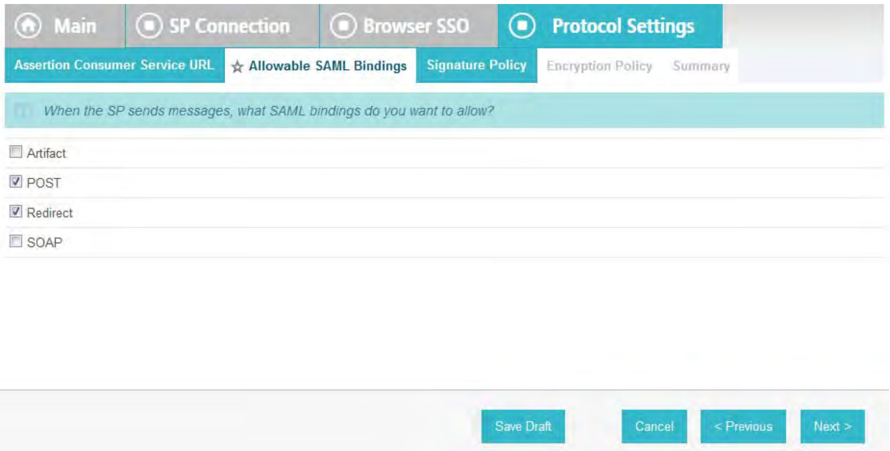


*As the IdP, you send SAML assertions to the SP's **Assertion Consumer Service**. The SP may request that the SAML assertion be sent to one of several URLs, via different bindings. Please provide the possible assertion consumer URLs below and select one to be the default.*

DEFAULT	INDEX	BINDING	ENDPOINT URL	ACTION
default	0	POST	/sp/ACS.saml2	Edit / Delete
□		- SELECT - ▾ *	*	Add

29. Click **Next**.

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

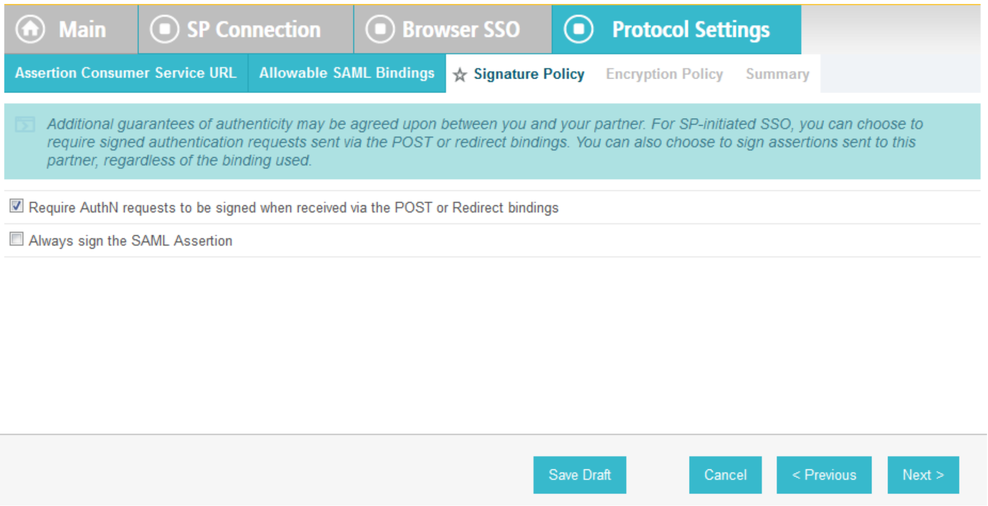


When the SP sends messages, what SAML bindings do you want to allow?

☐ Artifact
☑ POST
☑ Redirect
☐ SOAP

31. Click **Next**.

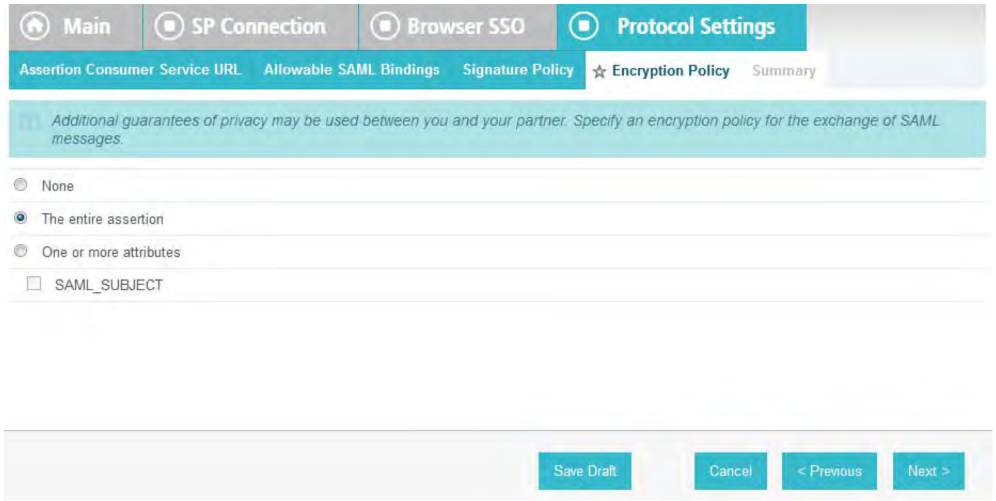
32. On the Signature Policy screen, select **Require AuthN requests to be signed when received via the POST or Redirect bindings**.



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

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

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



Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.

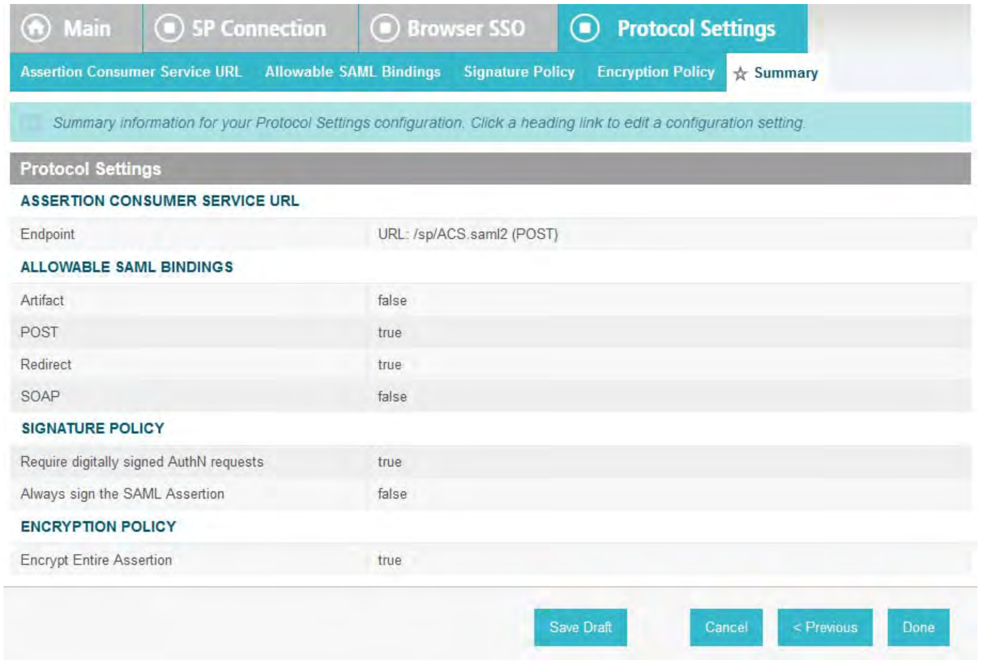
○ None

● The entire assertion

○ One or more attributes

□ SAML_SUBJECT

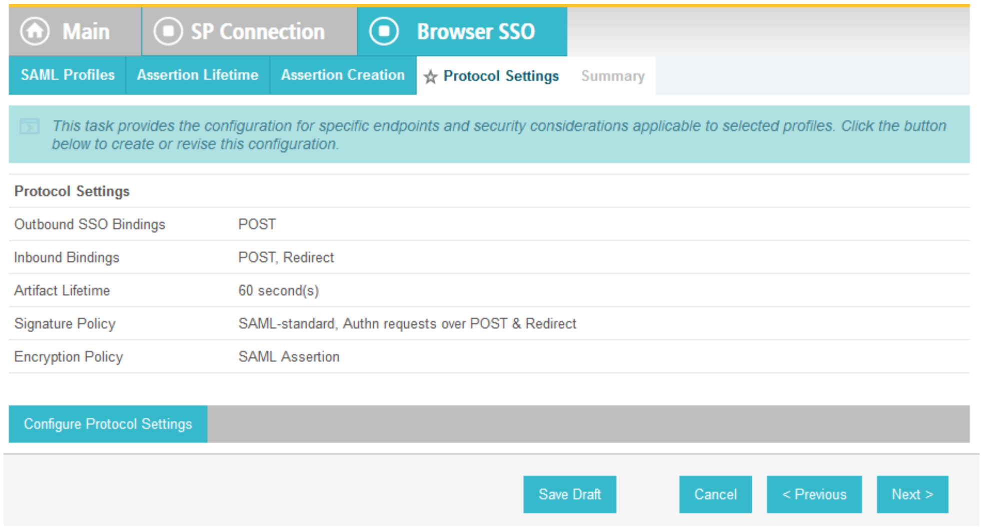
34. Click **Next**.



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

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

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



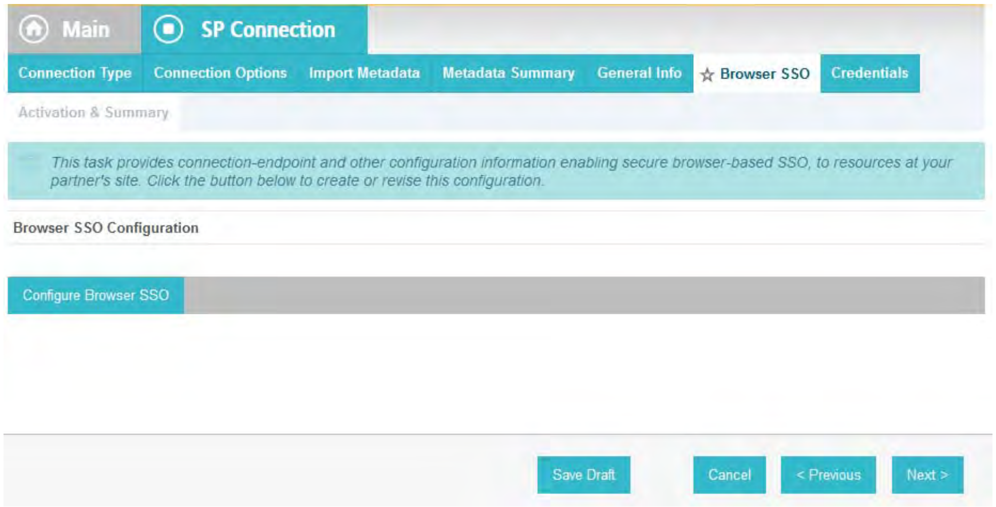
This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

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

This will take you back to the Protocol Settings screen.

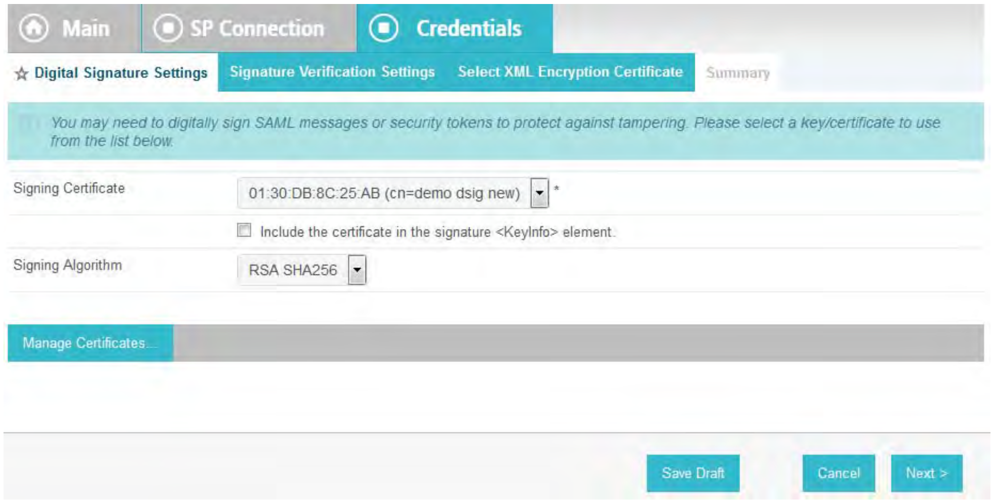
36. Click **Next**.On the Summary screen, click **Done**.

    This will take you back to the Browser SSO screen.



This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

37. Click **Next**.
38. On the Credentials screen, click **Configure Credentials**.
39. For the **Signing Certificate** field, select the certificate to be used to sign the SAML message.
40. Select the certificate that you configured for the server in an earlier section.
41. Select the **Signing Algorithm** for your environment (e.g. **RSA SHA256**).



Main
SP Connection
Credentials
☆ Digital Signature Settings
Signature Verification Settings
Select XML Encryption Certificate
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.

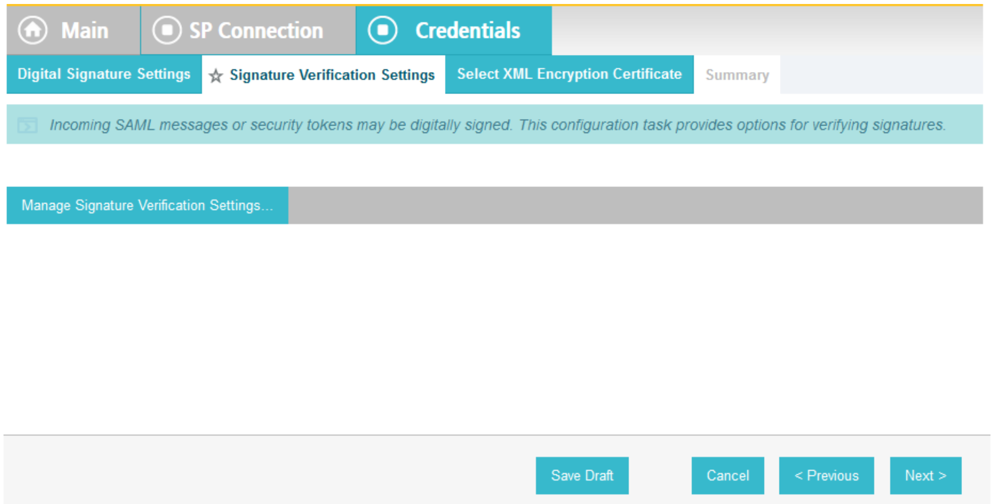
Signing Certificate: 01:30:DB:8C:25:AB (cn=demo dsig new) *

□ Include the certificate in the signature <KeyInfo> element.

Signing Algorithm: RSA SHA256

Manage Certificates...
Save Draft
Cancel
Next >

42. Click **Next**.

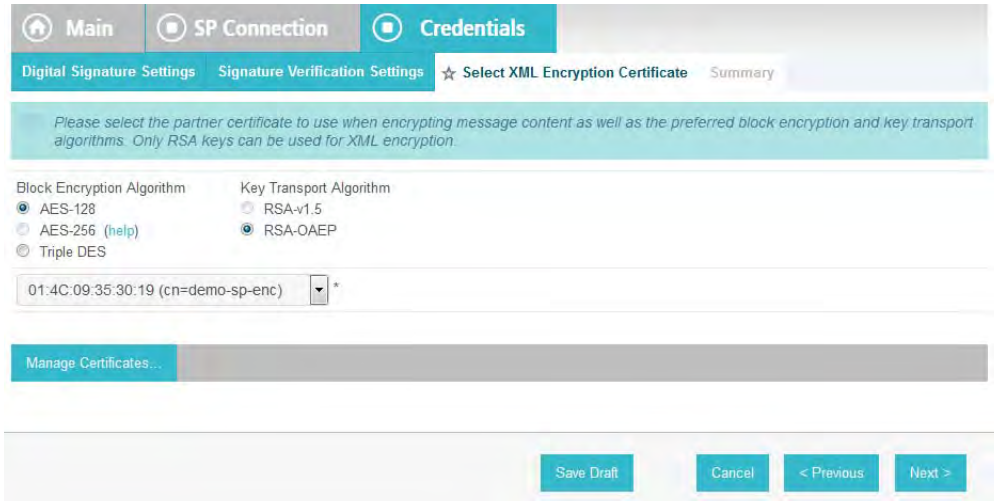


Main
SP Connection
Credentials
Digital Signature Settings
☆ Signature Verification Settings
Select XML Encryption Certificate
Summary

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

Manage Signature Verification Settings...
Save Draft
Cancel
< Previous
Next >

43. Click **Next**.
44. 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**).
45. For the selection box above the **Manage Certificates** button, select the Relying Party’s public key certificate to be used to encrypt the message content.


Main
SP Connection
Credentials
Digital Signature Settings
Signature Verification Settings
☆ Select XML Encryption Certificate
Summary
Manage Certificates...
Save Draft
Cancel
< Previous
Next >

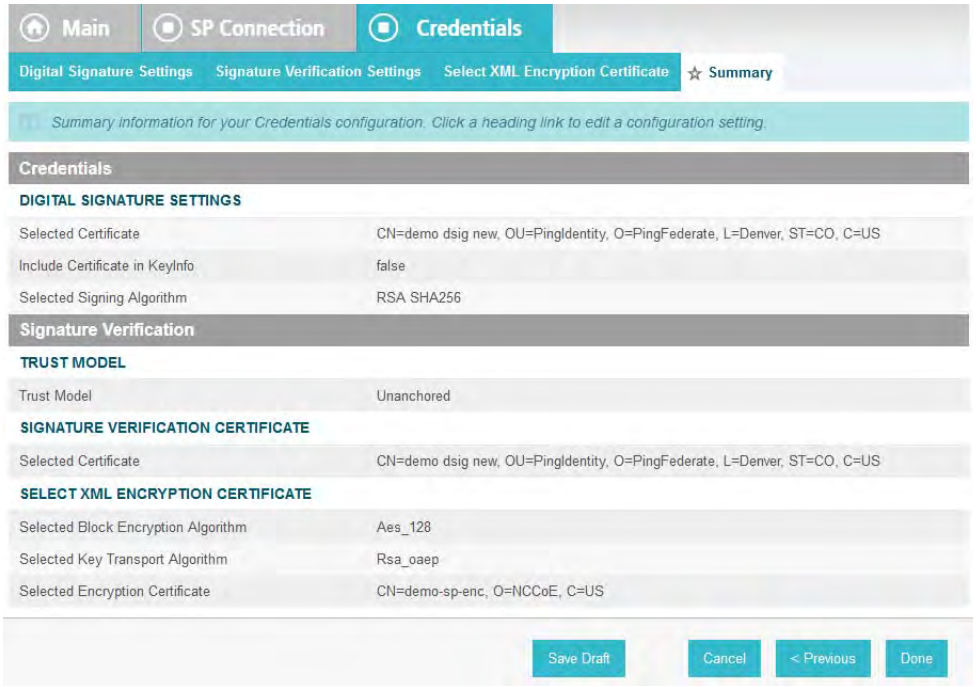
Please select the partner certificate to use when encrypting message content as well as the preferred block encryption and key transport algorithms. Only RSA keys can be used for XML encryption.

Block Encryption Algorithm
- ● AES-128
- ○ AES-256 (help)
- ○ Triple DES

Key Transport Algorithm
- ○ RSA-v1.5
- ● RSA-OAEP

01:4C:09:35:30:19 (cn=demo-sp-enc) *

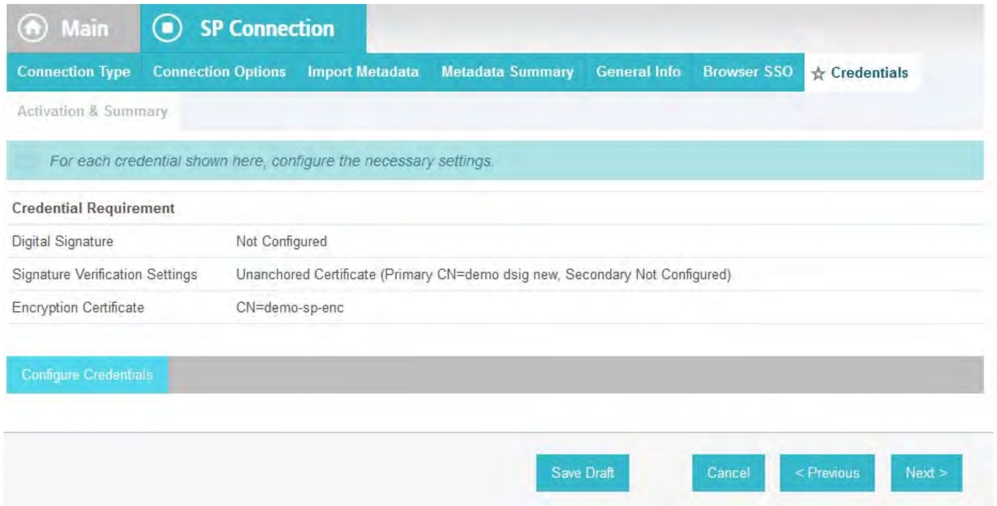
46. Click **Next**.


Main
SP Connection
Credentials
Digital Signature Settings
Signature Verification Settings
Select XML Encryption Certificate
☆ Summary
Save Draft
Cancel
< Previous
Done

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 Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256
Signature Verification	
TRUST MODEL	
Trust Model	Unanchored
SIGNATURE VERIFICATION CERTIFICATE	
Selected Certificate	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
SELECT XML ENCRYPTION CERTIFICATE	
Selected Block Encryption Algorithm	Aes_128
Selected Key Transport Algorithm	Rsa_oaep
Selected Encryption Certificate	CN=demo-sp-enc, O=NCCoE, C=US

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

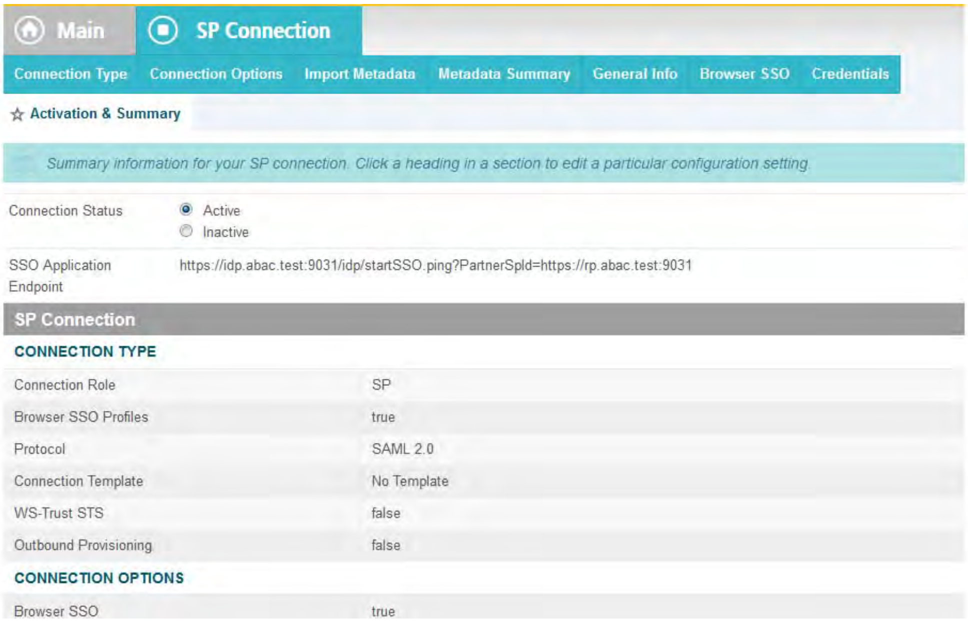


For each credential shown here, configure the necessary settings.

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

48. Click **Next**.

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



Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status ● Active ○ Inactive

SSO Application Endpoint https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=https://rp.abac.test:9031

SP Connection

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

50. Copy the Identity Provider’s **SSO Application Endpoint URL** (e.g. **https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=https://rp.abac.test:9031**) to the clipboard and save it to a text file, because this URL will be used in the functional test section.

51. Click **Done**. This will take you to a screen that lists the connections for the server, including the new connection you just created. Click **Save** to complete the configuration.

2.11 Certificates

Once you have installed the various products for this ABAC build, you can replace the default self-signed certificates with certificates signed by a Certificate Authority. For our build, we used Symantec's Managed PKI Service to sign our certificates using a local Certificate Authority. Certificates were used to support various exchanges that require encryption, such as digital signature, SAML message encryption, and encryption of TLS communications.

Although the detailed instructions of configuring certificates signed by a certificate authority vary by vendor product, this section describes the general process. For each certificate you perform the following high level steps:

1. Using the vendor product (e.g. PingFederate, Sharepoint), generate a certificate signing request on the server where you want to use the certificate. Save the signing request to a file.
2. Submit an enrollment request to your certificate authority. You will need to provide the signing request that was generated in step 1. This step is typically where you provide information such as the name of the server you intend to use the certificate on (e.g. **idp.abac.test**).
3. A representative at the certificate authority will examine the enrollment request and approve it. The representative will issue a certificate response signed with the certificate authority's key. You can download the signed response. If you are using a certificate authority that is locally managed by your organization, you will also need to download the public key of the certificate authority because you will need to add this the Trusted Certificate Authorities on each server and client that will be using the certificates.
4. Go back to the vendor product where you created the certificate signing request. If you are using a local certificate authority, you will first need to add the certificate authority's public key to the list of Trusted Certificate Authorities.
5. Import the certificate file for your server that was signed by the certificate authority.

2.11.1 Certificate Configuration PingFederate

In the PingFederate app, on the **Main** menu, under **Certificate Management**, click **Trusted CAs** to import the public key of your local certificate authority. If you are using a well-known, external, major certificate authority and that authority's public key is already available in cacerts in the Java runtime, it is not necessary to import the same certificate into the PingFederate Trusted CA store.

- For SSL Server certificates follow the instructions in the link below. The applicable sections are *To create a new certificate*, *To create a certificate-authority signing request*, and *To import a certificate authority response*. Once you have imported a signed certificate response, you will need to active the certificate on the PingFederate runtime server instance your applications are running on. Follow the instructions in the section *To activate a certificate*.

  https://documentation.pingidentity.com/display/PF73/SSL+Server+Certificates
- For digital signatures and performing encryption / decryption, follow the instructions in the link below. The applicable sections are the same as for SSL Server certificates.

  https://documentation.pingidentity.com/display/PF73/Digital+Signing+and+Decryption+Keys+and+Certificates

2.12 Functional Test of All Configurations for this Chapter

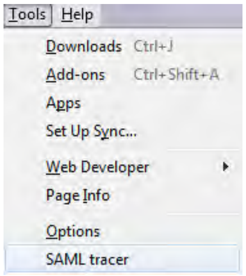
The instructions in this section will help perform an integrated test all of the configurations in this chapter. Using the browser and PingFederate, a user will log on and validate that the federated authentication to Microsoft AD and RSA AA are properly configured.

The test for this chapter was performed using the Mozilla Firefox browser and the SAML tracer Add-on, which enables examination of HTTPS POST and SAML messages.

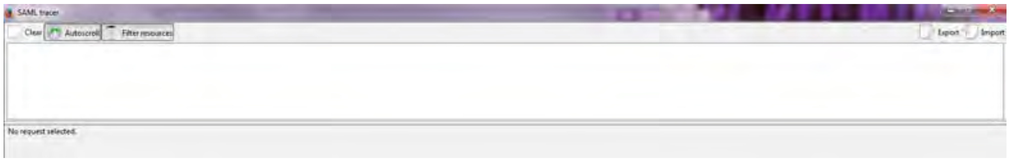
1. Install the Firefox SAML tracer Add-on from the link below.

   https://addons.mozilla.org/en-Us/firefox/addon/saml-tracer/

2. Launch your Firebox browser and select **SAML tracer** from the **Tools** menu.



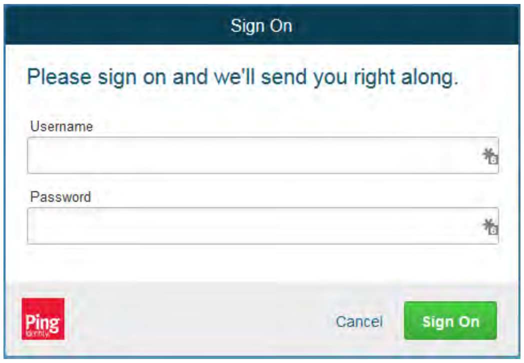
   This will launch an empty SAML tracer window.



3. Minimize the SAML tracer window. The SAML tracer will automatically record the details of the HTTPS messages in the background.

4. Go back to the main browser window and navigate to the Identity Provider’s SSO Application Endpoint URL identified in the previous section (e.g. **https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=https://rp.abac.test:9031**).

   Expected Result: You should see the PingFederate Sign On screen.



Sign On

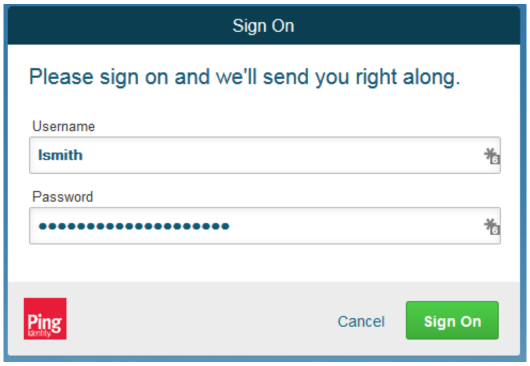
Please sign on and we'll send you right along.

Username

Password

5. Enter the Username of the account created in Microsoft AD earlier in this chapter (e.g. **lsmith**).

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

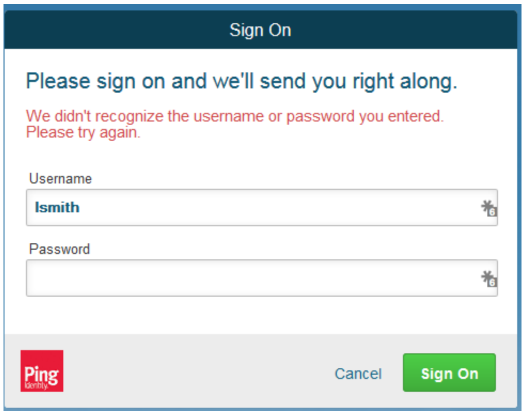
lsmith

Password

••••••••••••••••••••

7. Click **Sign On**.

   Expected Result: You should see an error message that states: **We didn't recognize the username or password you entered**.



Sign On

Please sign on and we'll send you right along.

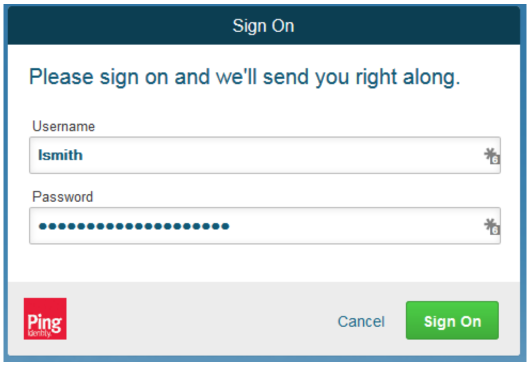
We didn't recognize the username or password you entered. Please try again.

Username

lsmith

Password

8. Close the existing browser and launch a new browser.
9. Navigate to the Identity Provider's SSO Application Endpoint URL again.
10. Enter the user name of the account created earlier in this chapter (e.g. **lsmith**). Then, enter the correct password.



Sign On

Please sign on and we'll send you right along.

Username

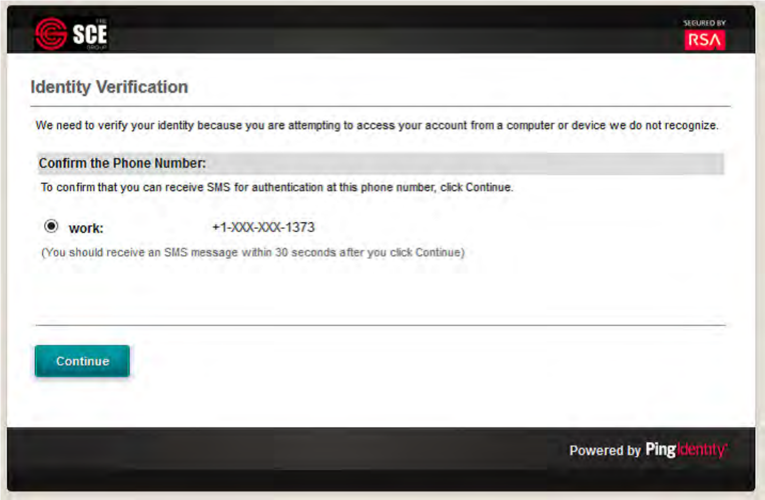
lsmith

Password

••••••••••••••••••••

11. Click **Sign On**.

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



Identity Verification

We need to verify your identity because you are attempting to access your account from a computer or device we do not recognize.

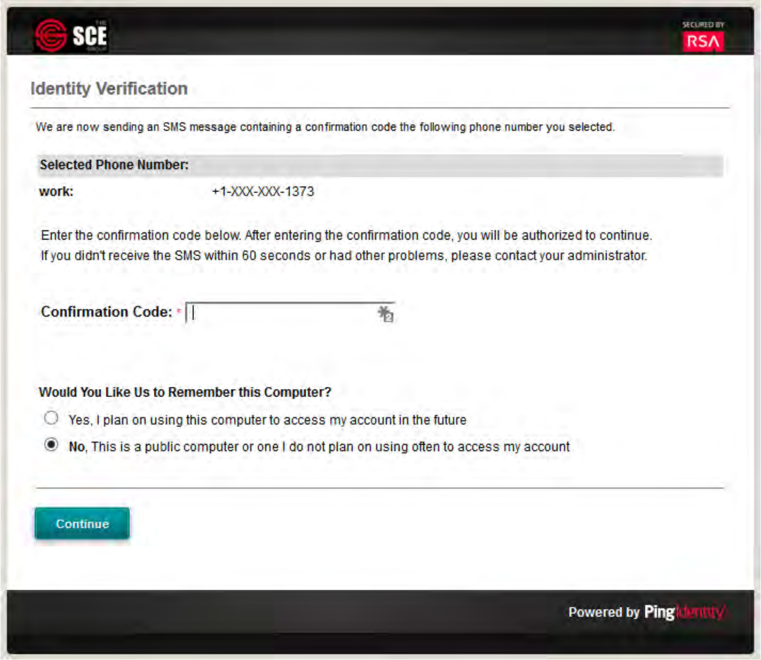
Confirm the Phone Number:

To confirm that you can receive SMS for authentication at this phone number, click Continue.

● work: +1-XXX-XXX-1373

(You should receive an SMS message within 30 seconds after you click Continue)

Figure 2.3 Identity Verification via SMS



Identity Verification

We are now sending an SMS message containing a confirmation code the following phone number you selected.

Selected Phone Number:

work: +1-XXX-XXX-1373

Enter the confirmation code below. After entering the confirmation code, you will be authorized to continue.
If you didn't receive the SMS within 60 seconds or had other problems, please contact your administrator.

Confirmation Code: *

Would You Like Us to Remember this Computer?

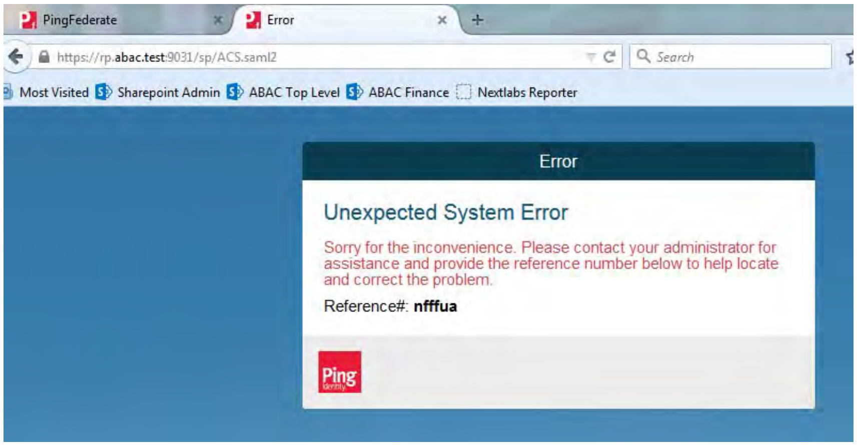
○ Yes, I plan on using this computer to access my account in the future

● No, This is a public computer or one I do not plan on using often to access my account

Figure 2.4 Confirmation Code Screen

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.

    Expected Result: The browser should redirect to the Relying Party's Federation Server (e.g. **rp.abac.test**) and you should see an error message similar to the following screenshot.



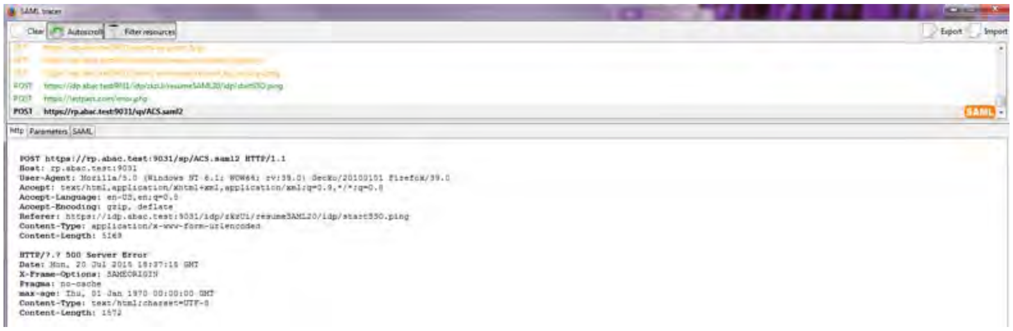
Error

Unexpected System Error

Sorry for the inconvenience. Please contact your administrator for assistance and provide the reference number below to help locate and correct the problem.

Reference#: **nfffua**

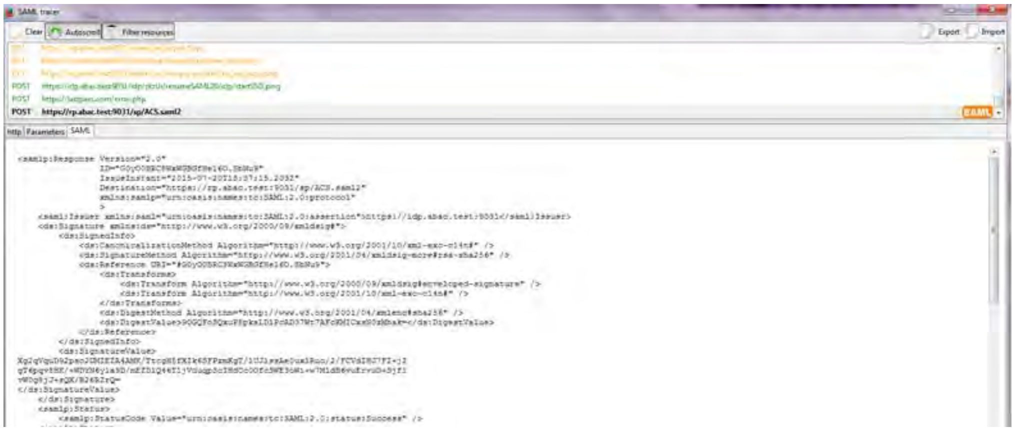
13. Go back to the SAML tracer window. Scroll to the bottom of the list of messages in the upper pane. Click on the last message (e.g. **POST https://rp.abac.test:9031/sp/ACS.saml2**) that has a SAML icon associated with it. This will show the details of the POST message.


SAML tracer
Clear
Autoscroll
Filter resources
Export
Import
POST https://idp.abac.test:9031/idp/zkzUi/resumeSAML20/idp/startSSO.ping
POST https://testpact.com/error.php
POST https://rp.abac.test:9031/sp/ACS.saml2
SAML
http
Parameters
SAML

```
POST https://rp.abac.test:9031/sp/ACS.saml2 HTTP/1.1
Host: rp.abac.test:9031
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://idp.abac.test:9031/idp/zkzUi/resumeSAML20/idp/startSSO.ping
Content-Type: application/x-www-form-urlencoded
Content-Length: 5169

HTTP/?.? 500 Server Error
Date: Mon, 20 Jul 2015 18:37:15 GMT
X-Frame-Options: SAMEORIGIN
Pragma: no-cache
max-age: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 1572
```

Expected Result: In the details page at the bottom, on the http tab, you should see that the browser sent a POST message to the Relying Party's PingFederate server **rp.abac.test**. The HTTP response status code (identified on the line that begins with HTTP) should be a **500 Server Error.**

14. Click on the SAML tab.


SAML tracer
Clear
Autoscroll
Filter resources
Export
Import
POST https://idp.abac.test:9031/idp/zkzUi/resumeSAML20/idp/startSSO.ping
POST https://testpact.com/error.php
POST https://rp.abac.test:9031/sp/ACS.saml2
SAML
http
Parameters
SAML

```
<samlp:Response Version="2.0"
                ID="G0yO0BRC9WaWGBGfHe16O.XbHuB"
                IssueInstant="2015-07-20T18:37:15.203Z"
                Destination="https://rp.abac.test:9031/sp/ACS.saml2"
                xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://idp.abac.test:9031</saml:Issuer>
    <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="#G0yO0BRC9WaWGBGfHe16O.XbHuB">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>9GGQFo8QmuPEpkaLD1PcAD37Wr7AFcKMICxm90zMbak=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>
Xg2qVquD9JpaoJGMIZIA4AMK/TtcgHlfKIk6SFPzmKgT/1UJlsmAeDuxlRuo/J/FCVdIBJ7FI+j2
qT6pqvSHK/+WDYN6y1a9D/mEfDlQ46T1jVdagp3cIHdOeOOfd5WE36W1+w7M1dB6vuErvuD+5jf1
vWDg8jJ+sQK/B26RZrQ=
</ds:SignatureValue>
    </ds:Signature>
    <samlp:Status>
        <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
```

Expected Result: You should see the details of the SAML message, including the Issuer. The Issuer should be the Identity Provider's Federation server, **idp.abac.test**.

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

3.1 Introduction

In the previous chapter of this How-To Guide we demonstrated how to set up federated, SAML-based authentication at the Identity Provider (IdP). Before continuing with this chapter, it is necessary to have a working federation service that will represent the Identity Provider and can receive and issue SAML 2.0 request and responses. For instructions on how to set this up using Ping Federate, please refer to chapter 2 of this guide.

In order to federate identities and attribute information between organizations a federation service must exist at both the Identity Provider and the Relying Party (RP). A trust relationship between these two services must then be instantiated to allow for identity and attribute requests and responses. In this chapter we configure an instance of PingFederate (henceforth called PingFederate-RP) at the Relying Party to act as a federation service and to redirect users to the PingFederate-IdP via a SAML request. We then configure the trust relationship and federated authentication between the PingFederate-RP and the PingFederate-IdP, allowing the SAML request to be processed by the Identity Provider and the subsequent return of a SAML response containing identity and attribute assertions.

If you follow the instructions in this chapter, you will be able to perform a functional test to verify the successful completion of the steps for installing, configuring, and integrating the components.

3.2 Components

Federated authentication between the Relying Party and the Identity Provider involves the following distinct components:

- **PingFederate-IdP**: A federation system or trust broker for the Identity Provider
- **PingFederate-RP**: Serves as the trust broker for SharePoint

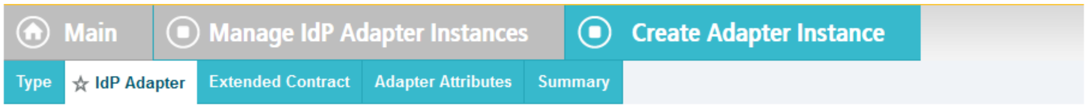
3.2.1 PingFederate-IdP

Ping Identity PingFederate-IdP serves as a federation system or trust broker for the IdP. PingFederate-IdP provides initial user authentication and retrieval of user attributes to satisfy SAML requests from the RP. Once the user has been authenticated, PingFederate-IdP queries subject attributes from AD and environmental attributes from the RSA AA event log. PingFederate-IdP takes the name:value pairs of both the subject and environmental attributes and stores them in a SAML 2.0 token to be sent to the RP.

PingFederate Usage Notes:

- When using the PingFederate application to perform an administrative configuration, there is usually a sequence of screens that require user entry, ending with a summary page. Once you click **Done** on the summary page, you must also click **Save** on the following page to save the configurations. If you forget to click **Save**, you may inadvertently lose changes to the configuration.
- In the PingFederate application and associated documentation, the Relying Party is referred to as the Service Provider.

- When using the PingFederate application to perform configuration, refer to the title of the tab with a small star icon to its left, to identify the item you are currently configuring. For example, if you navigated to the following screen, you would be on the IdP Adapter screen.



3.2.2 PingFederate-RP

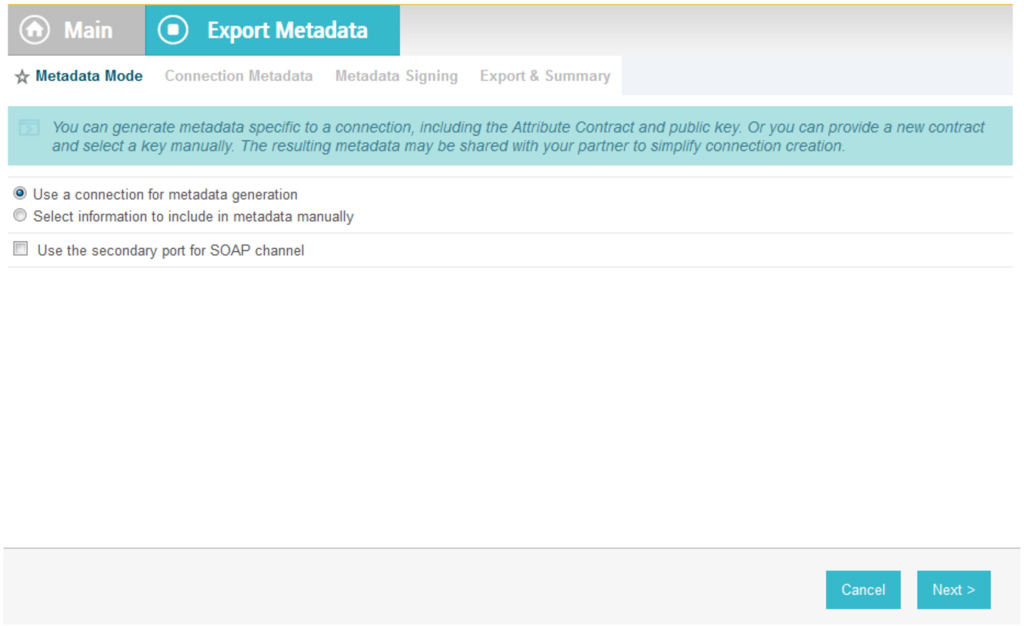
Ping Identity PingFederate-RP serves as the trust broker for SharePoint. When the user requires authentication, PingFederate-RP redirects the user to the IdP via a SAML request to get the necessary assertions. Once authenticated, PingFederate-RP arranges for the browser's HTTPS content to have the proper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

3.3 Export Metadata from the Identity Provider

Follow the instructions in this section to export a metadata file from the PingFederate-IdP.

1. Log on to the server that hosts the PingFederate service for the Identity Provider.
2. Launch your browser and navigate to the PingFederate application URL: **https://<DNS_NAME>:9999/pingfederate/app**.
3. Replace DNS_NAME with the fully qualified name of the Identity Provider's PingFederate server (e.g. **https://idp.abac.test:9999/pingfederate/app)**. Log on to the PingFederate application using the credentials you configured during installation.
4. On the **Main Menu** under **Administrative Functions**, click **Metadata Export**.

5. On the Metadata Mode screen, select **Use a connection for metadata generation**.

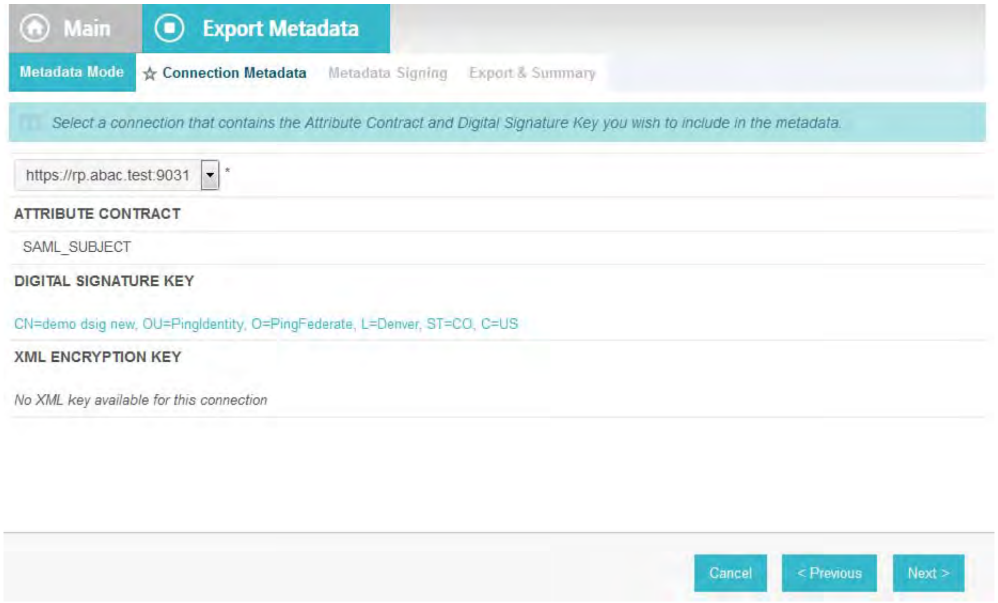


You can generate metadata specific to a connection, including the Attribute Contract and public key. Or you can provide a new contract and select a key manually. The resulting metadata may be shared with your partner to simplify connection creation.

● Use a connection for metadata generation
○ Select information to include in metadata manually

□ Use the secondary port for SOAP channel

6. Click **Next**. On the Connection Metadata screen, select the connection to the Relying Party that you configured in the previous chapter (e.g **https://rp.abac.test:9031**). This should automatically populate some of the fields on the screen with information from the connection.



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

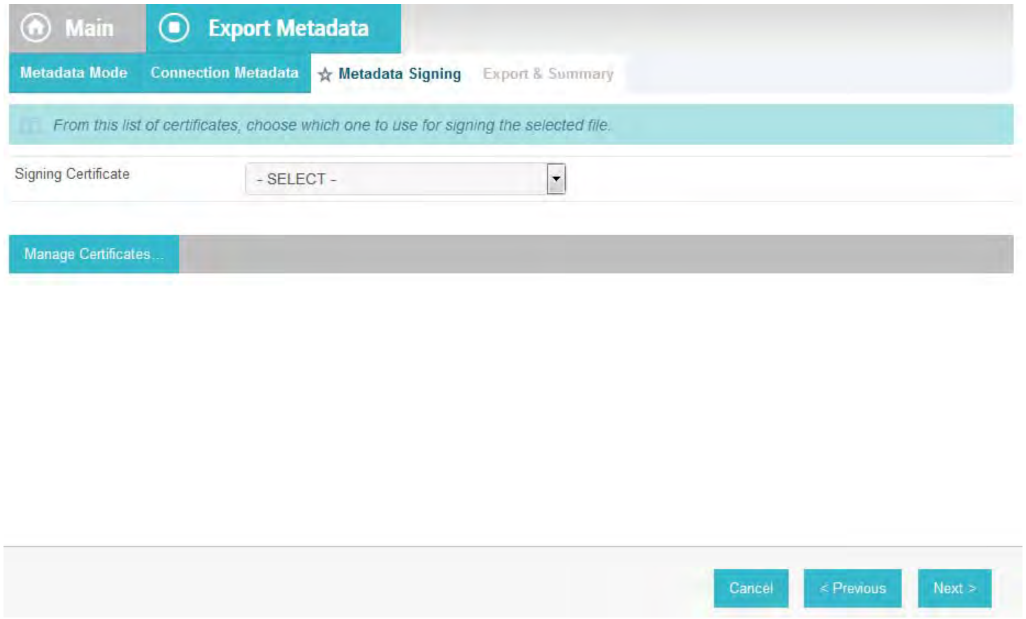
DIGITAL SIGNATURE KEY

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

XML ENCRYPTION KEY

No XML key available for this connection

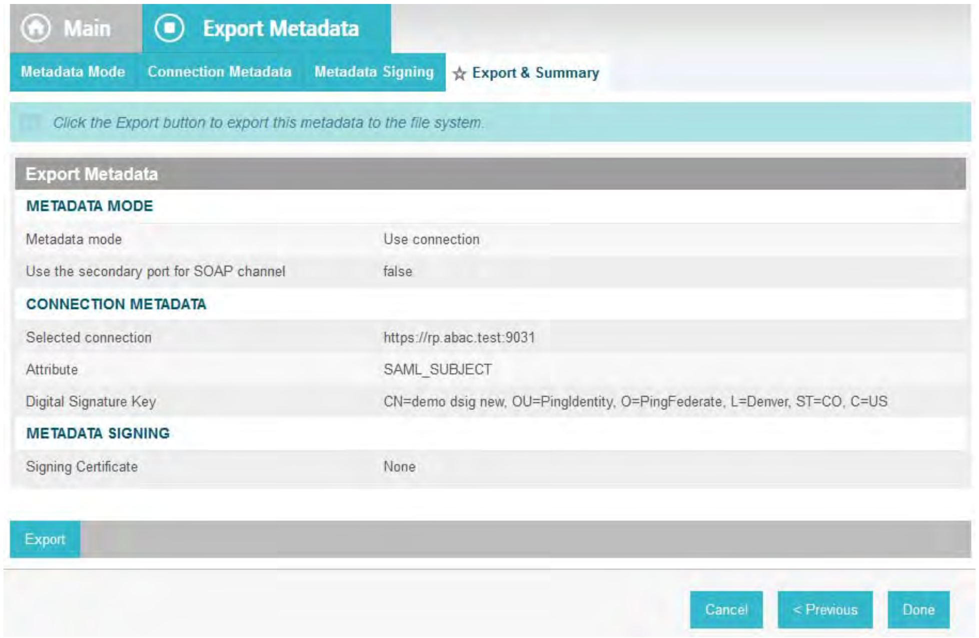
7. Click **Next**. On the Metadata Signing screen, if you plan to sign the metadata file that will be exported, select the certificate that will be use to sign the file.



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

Signing Certificate: - SELECT -

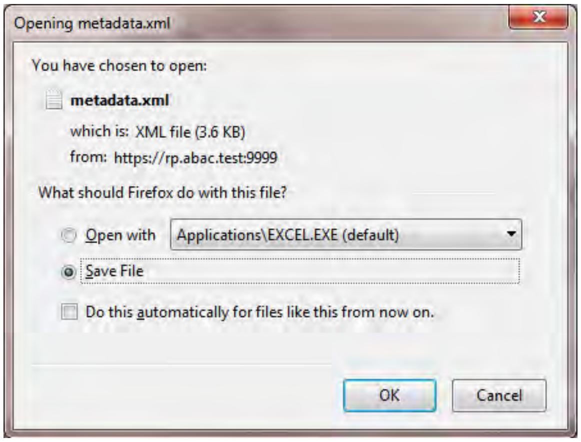
8. Click **Next**. On the Export & Summary screen, you should see a summary of the options that were selected.



Click the Export button to export this metadata to the file system.

Export Metadata	
METADATA MODE	
Metadata mode	Use connection
Use the secondary port for SOAP channel	false
CONNECTION METADATA	
Selected connection	https://rp.abac.test:9031
Attribute	SAML_SUBJECT
Digital Signature Key	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
METADATA SIGNING	
Signing Certificate	None

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



Opening metadata.xml

You have chosen to open:

metadata.xml

which is: XML file (3.6 KB)

from: https://rp.abac.test:9999

What should Firefox do with this file?

○ Open with Applications\EXCEL.EXE (default)

● Save File

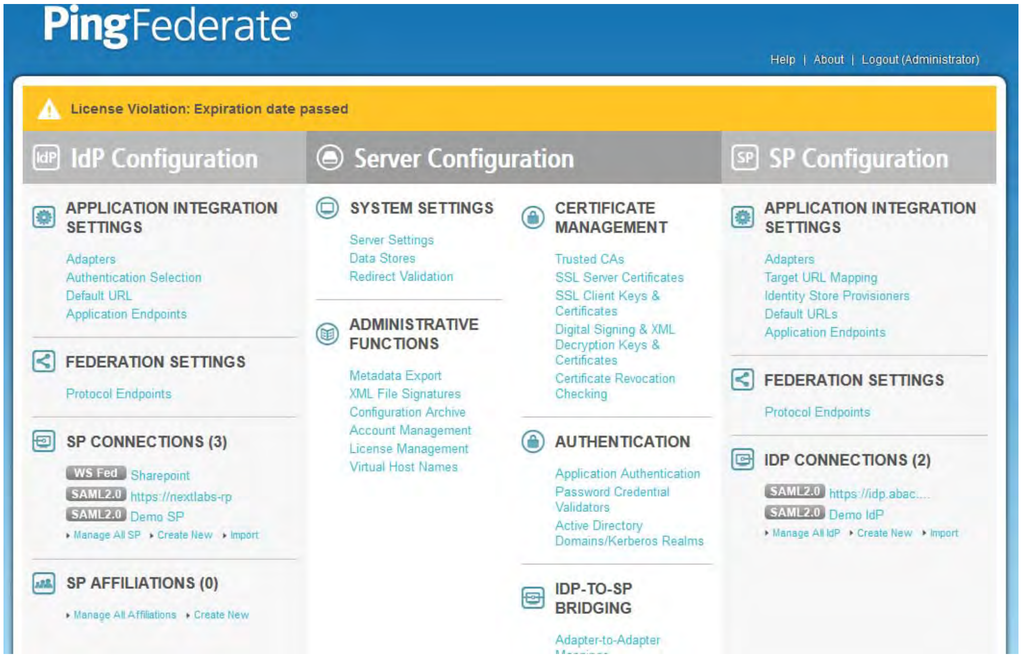
□ Do this automatically for files like this from now on.

10. Copy the metatdata file to the server that hosts the PingFederate service for the Relying Party.

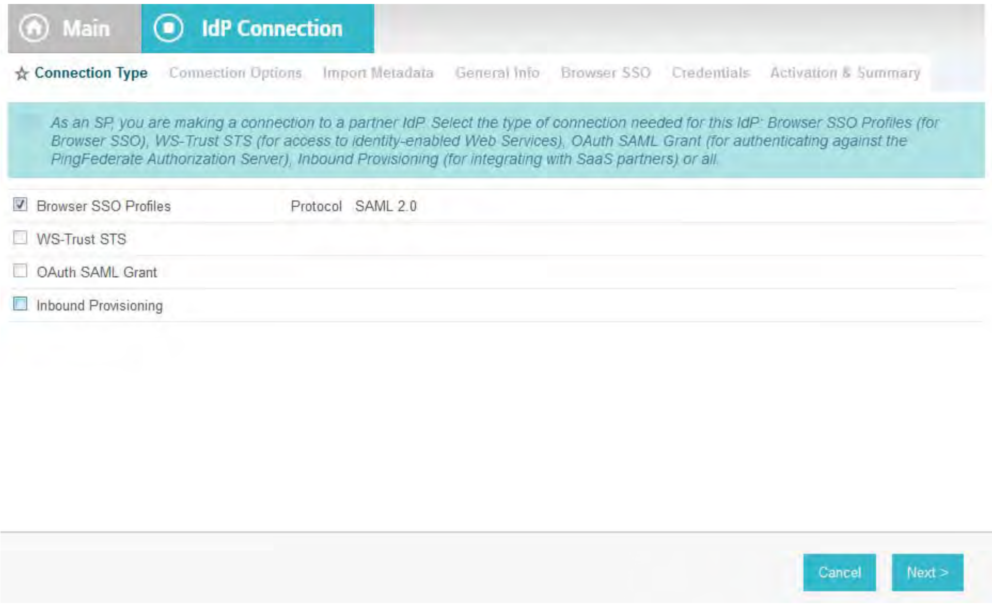
3.4 Configure PingFederate-RP Connection to the PingFederate-IdP

Follow the instructions in this section to configure a PingFederate connection from the Relying Party to the Identity Provider.

1. Log on to the server that hosts the PingFederate service for the Relying Party.
2. Launch your browser and go to: **https://<DNS_NAME>:9999/pingfederate/app**.
3. Replace **DNS_NAME** with the fully qualified name of the Relying Party's PingFederate server (e.g. **https://rp.abac.test:9999/pingfederate/app**). Log on to the PingFederate application using the credentials you configured in the previous installation section.



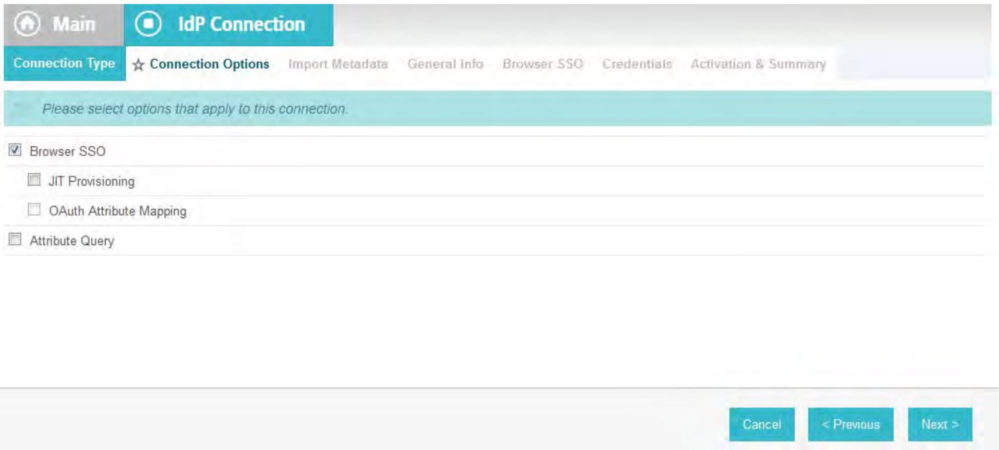
4. On the Main Menu under IDP CONNECTIONS, click **Create New**.
5. On the Connection Type screen, select **Browser SSO Profile**s.



As an SP, you are making a connection to a partner IdP. Select the type of connection needed for this IdP: Browser SSO Profiles (for Browser SSO), WS-Trust STS (for access to identity-enabled Web Services), OAuth SAML Grant (for authenticating against the PingFederate Authorization Server), Inbound Provisioning (for integrating with SaaS partners) or all.

☑ Browser SSO Profiles — Protocol SAML 2.0
☐ WS-Trust STS
☐ OAuth SAML Grant
☐ Inbound Provisioning

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



Please select options that apply to this connection.

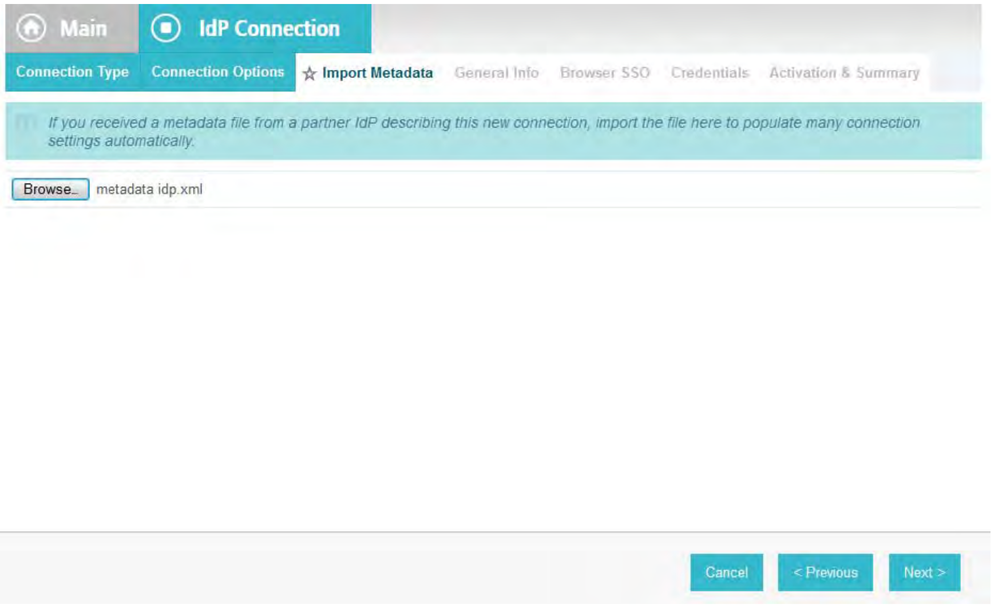
☑ Browser SSO

□ JIT Provisioning

□ OAuth Attribute Mapping

□ Attribute Query

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.

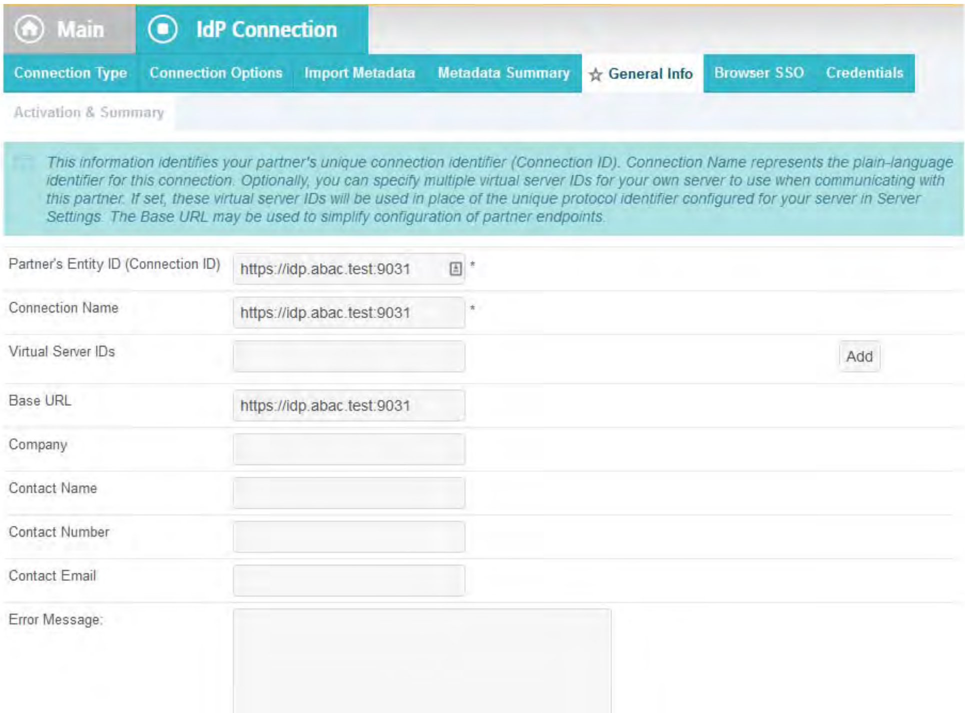


If you received a metadata file from a partner IdP describing this new connection, import the file here to populate many connection settings automatically.

metadata idp.xml

10. Click **Next**.

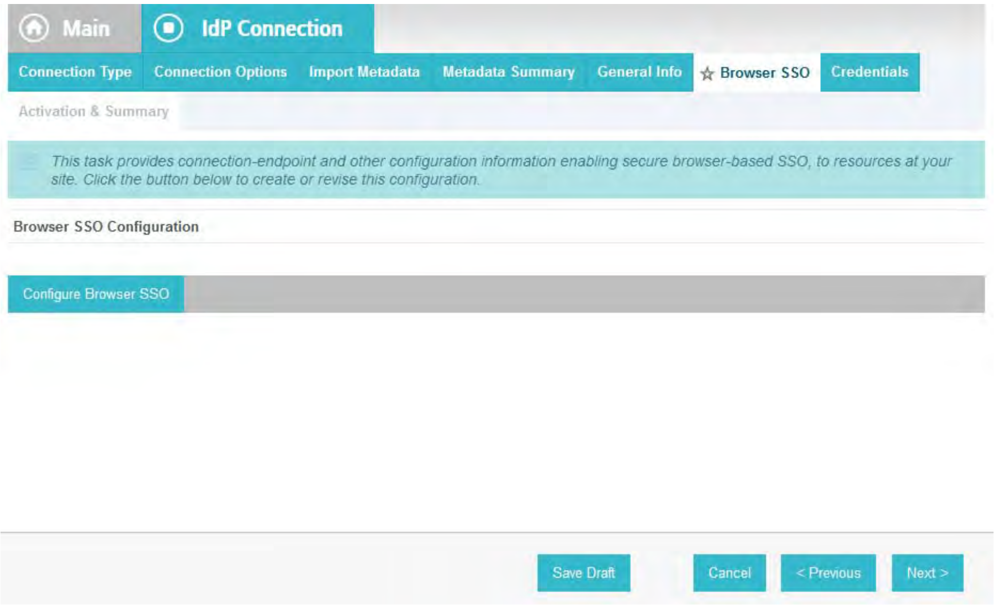
11. On the Metadata Summary screen, click **Next**. On the General Info screen you should see some configuration information (e.g. Base URL) about the Identity Provider that was taken from the metadata file that you selected.



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

Partner's Entity ID (Connection ID)	https://idp.abac.test:9031 *
Connection Name	https://idp.abac.test:9031 *
Virtual Server IDs	
Base URL	https://idp.abac.test:9031
Company	
Contact Name	
Contact Number	
Contact Email	
Error Message:	

12. Click **Next**.

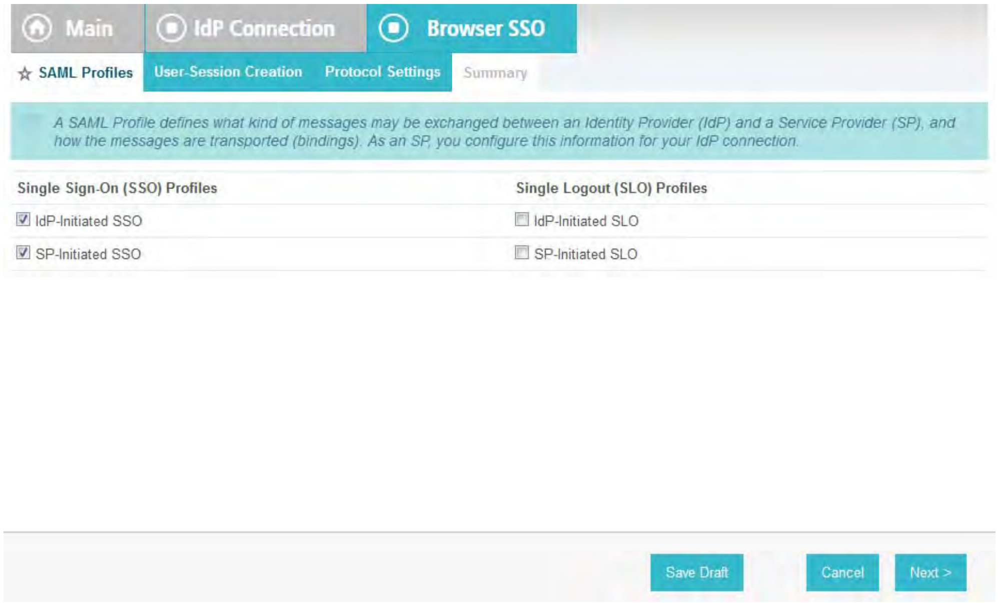


This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your site. Click the button below to create or revise this configuration.

Browser SSO Configuration

13. On the Browser SSO screen, click **Configure Browser SSO**.

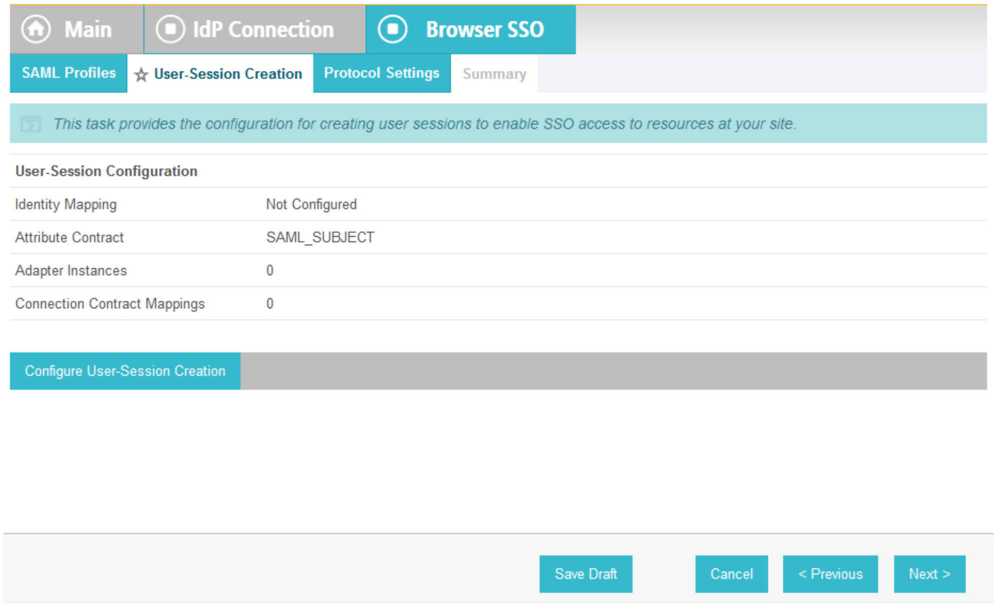
14. On the SAML Profiles screen, select **IdP-Initiated SSO** and **SP-Initiated SSO**.



A SAML Profile defines what kind of messages may be exchanged between an Identity Provider (IdP) and a Service Provider (SP), and how the messages are transported (bindings). As an SP, you configure this information for your IdP connection.

Single Sign-On (SSO) Profiles	Single Logout (SLO) Profiles
☑ IdP-Initiated SSO	□ IdP-Initiated SLO
☑ SP-Initiated SSO	□ SP-Initiated SLO

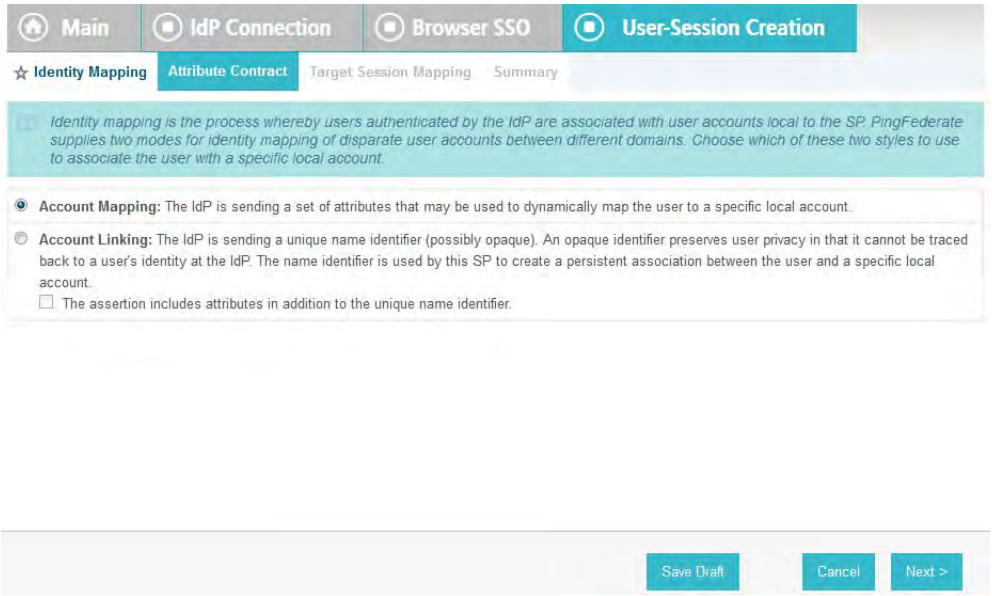
15. Click **Next**.



This task provides the configuration for creating user sessions to enable SSO access to resources at your site.

User-Session Configuration	
Identity Mapping	Not Configured
Attribute Contract	SAML_SUBJECT
Adapter Instances	0
Connection Contract Mappings	0

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



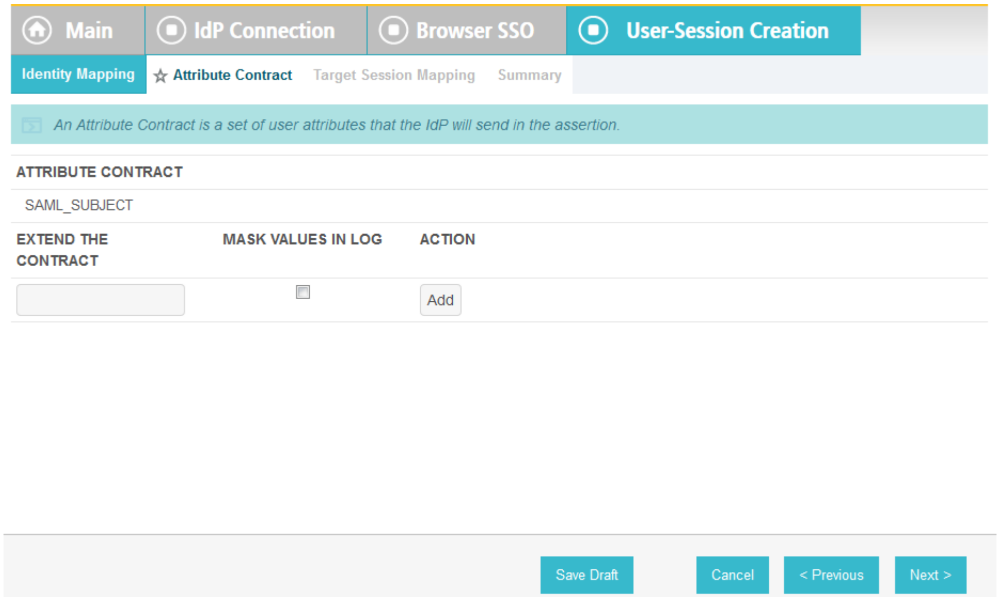
Identity mapping is the process whereby users authenticated by the IdP are associated with user accounts local to the SP. PingFederate supplies two modes for identity mapping of disparate user accounts between different domains. Choose which of these two styles to use to associate the user with a specific local account.

● **Account Mapping:** The IdP is sending a set of attributes that may be used to dynamically map the user to a specific local account.

○ **Account Linking:** The IdP is sending a unique name identifier (possibly opaque). An opaque identifier preserves user privacy in that it cannot be traced back to a user's identity at the IdP. The name identifier is used by this SP to create a persistent association between the user and a specific local account.

□ The assertion includes attributes in addition to the unique name identifier.

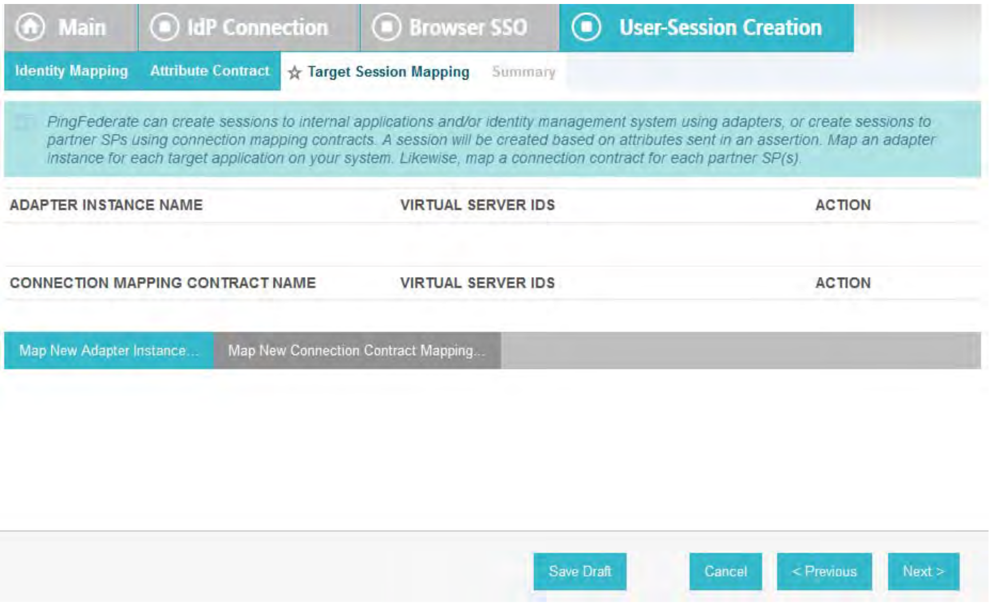
17. On the Identity Mapping screen, click **Next**.



An Attribute Contract is a set of user attributes that the IdP will send in the assertion.

ATTRIBUTE CONTRACT		
SAML_SUBJECT		
EXTEND THE CONTRACT	MASK VALUES IN LOG	ACTION
	□	Add

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



Main | IdP Connection | Browser SSO | User-Session Creation

Identity Mapping | Attribute Contract | ☆ Target Session Mapping | Summary

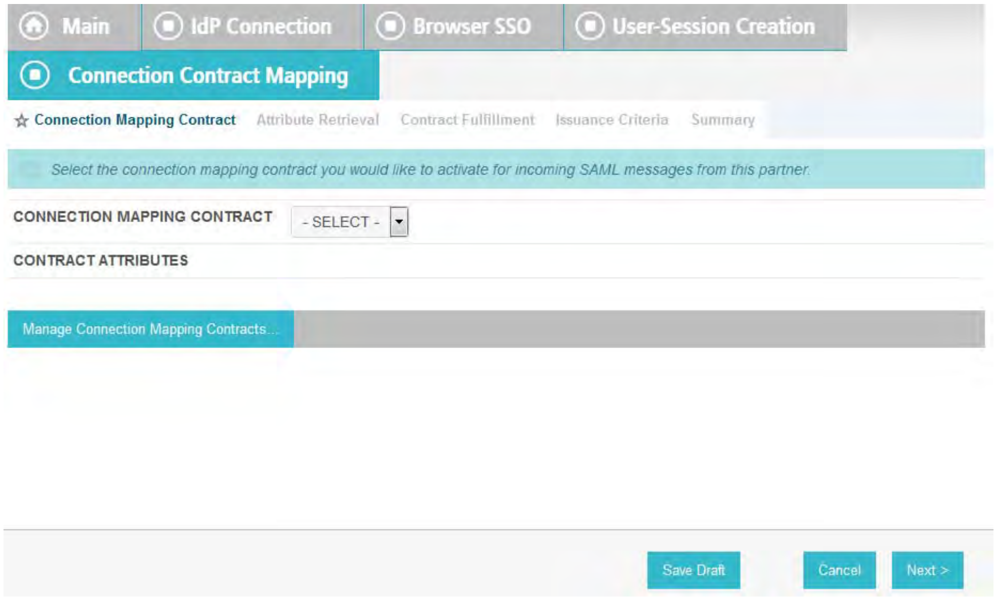
PingFederate can create sessions to internal applications and/or identity management system using adapters, or create sessions to partner SPs using connection mapping contracts. A session will be created based on attributes sent in an assertion. Map an adapter instance for each target application on your system. Likewise, map a connection contract for each partner SP(s).

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION

Map New Adapter Instance...
Map New Connection Contract Mapping...
Save Draft
Cancel
< Previous
Next >

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



Main | IdP Connection | Browser SSO | User-Session Creation

Connection Contract Mapping

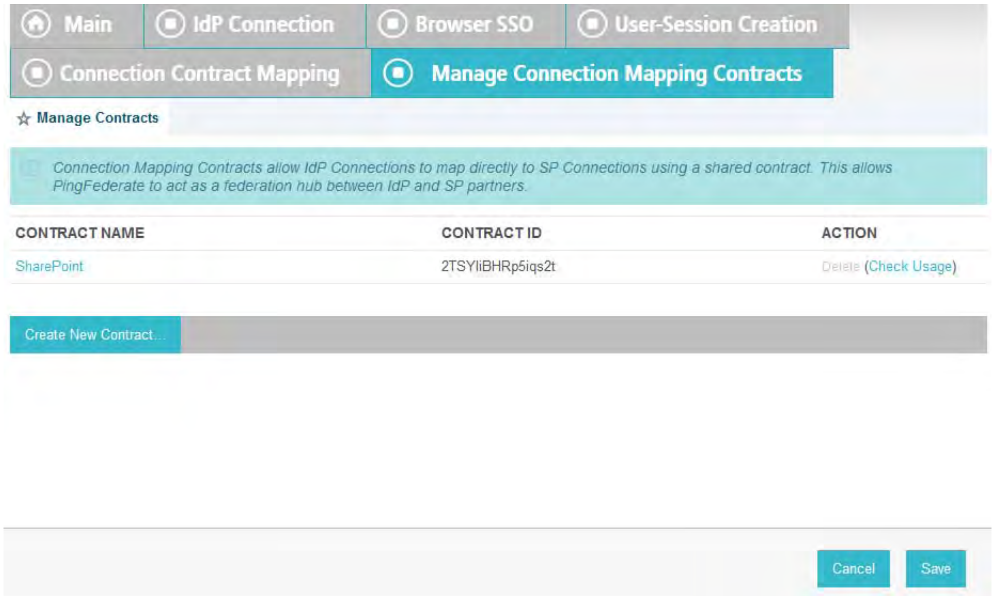
☆ Connection Mapping Contract | Attribute Retrieval | Contract Fulfillment | Issuance Criteria | Summary

Select the connection mapping contract you would like to activate for incoming SAML messages from this partner.

CONNECTION MAPPING CONTRACT: - SELECT -

CONTRACT ATTRIBUTES

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

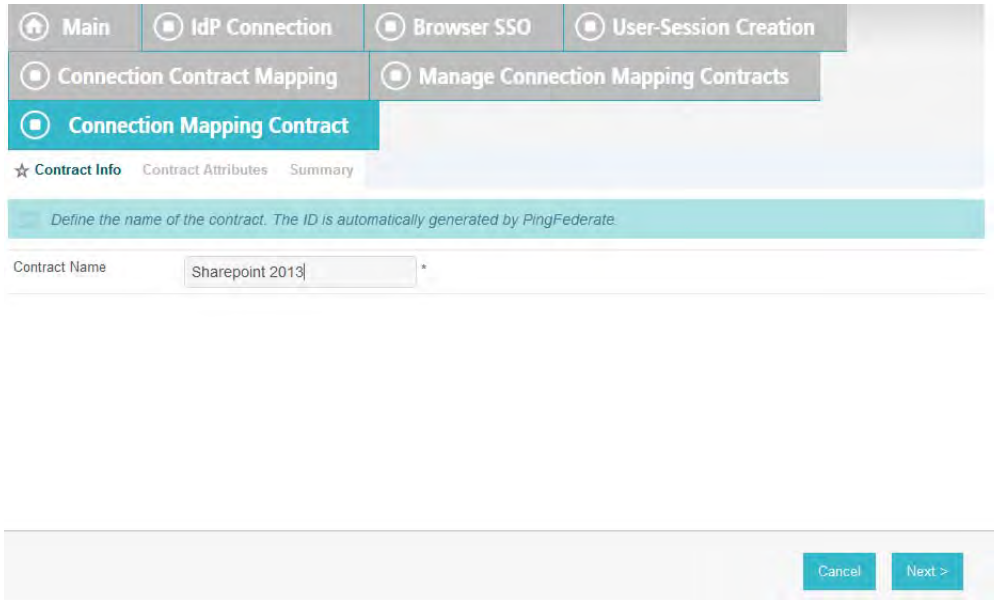


Connection Mapping Contracts allow IdP Connections to map directly to SP Connections using a shared contract. This allows PingFederate to act as a federation hub between IdP and SP partners.

CONTRACT NAME	CONTRACT ID	ACTION
SharePoint	2TSYliBHRp5iqs2t	Delete (Check Usage)

21. On the Manage Contracts screen, click **Create New Contract**.

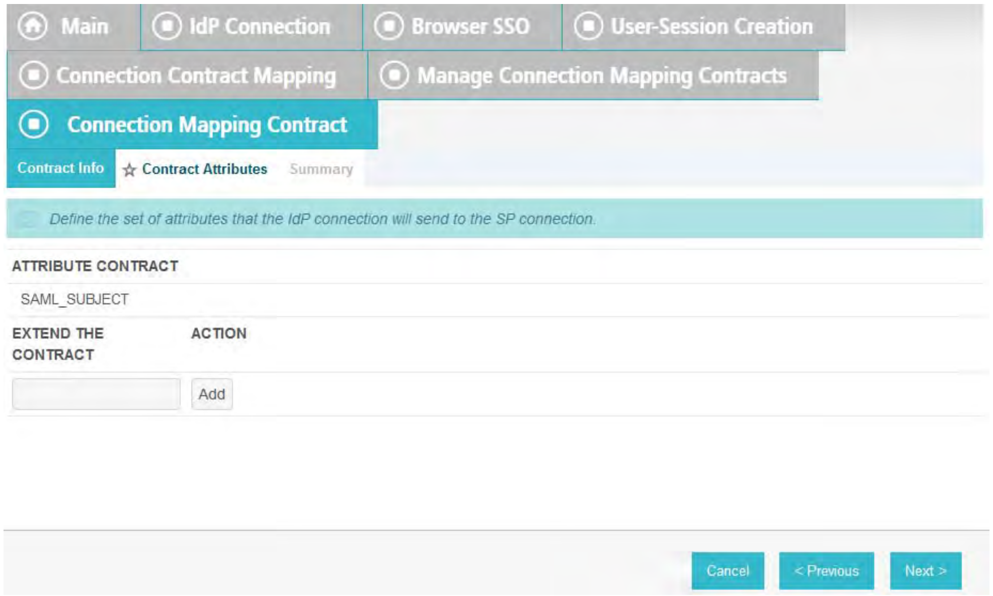
22. On the Contract Info screen, enter the **Contract Name** (e.g. **Sharepoint 2013**).



Define the name of the contract. The ID is automatically generated by PingFederate.

Contract Name: Sharepoint 2013 *

131 23. Click **Next**.



Define the set of attributes that the IdP connection will send to the SP connection.

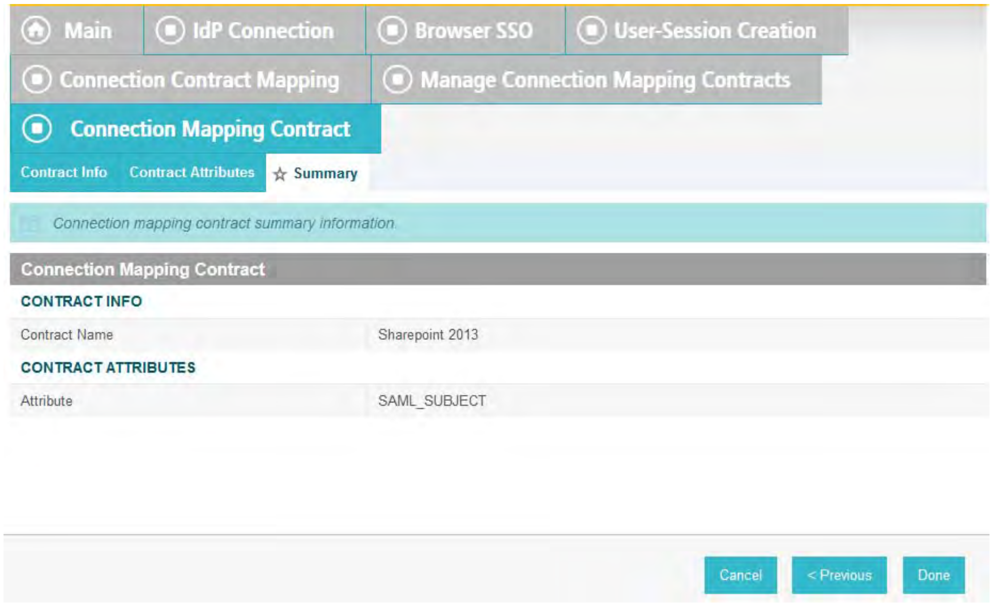
ATTRIBUTE CONTRACT

SAML_SUBJECT

EXTEND THE CONTRACT	ACTION
	Add

132

133 24. Click **Next**.



Connection mapping contract summary information.

Connection Mapping Contract

CONTRACT INFO

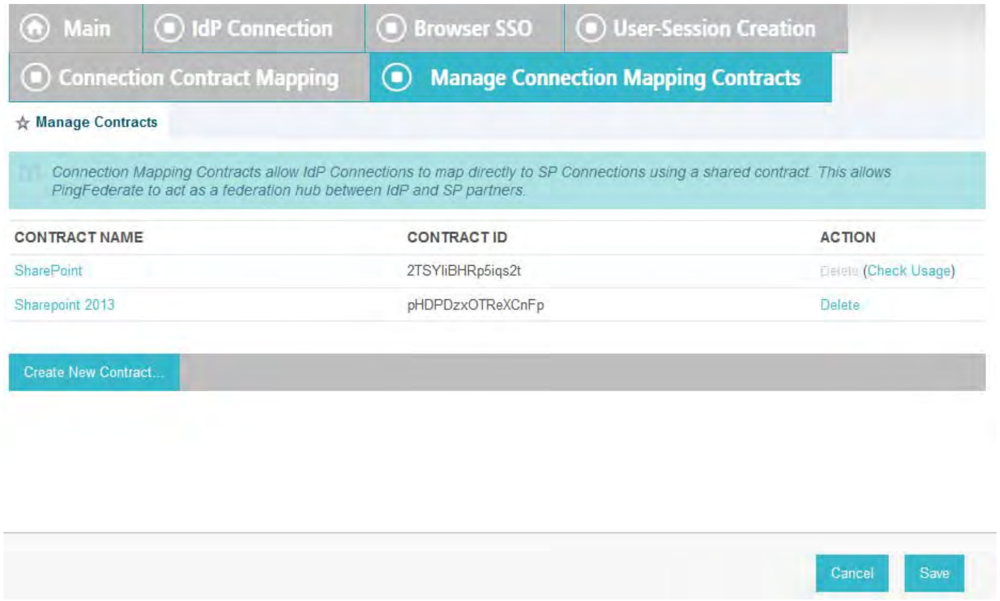
Contract Name	Sharepoint 2013

CONTRACT ATTRIBUTES

Attribute	SAML_SUBJECT

134

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

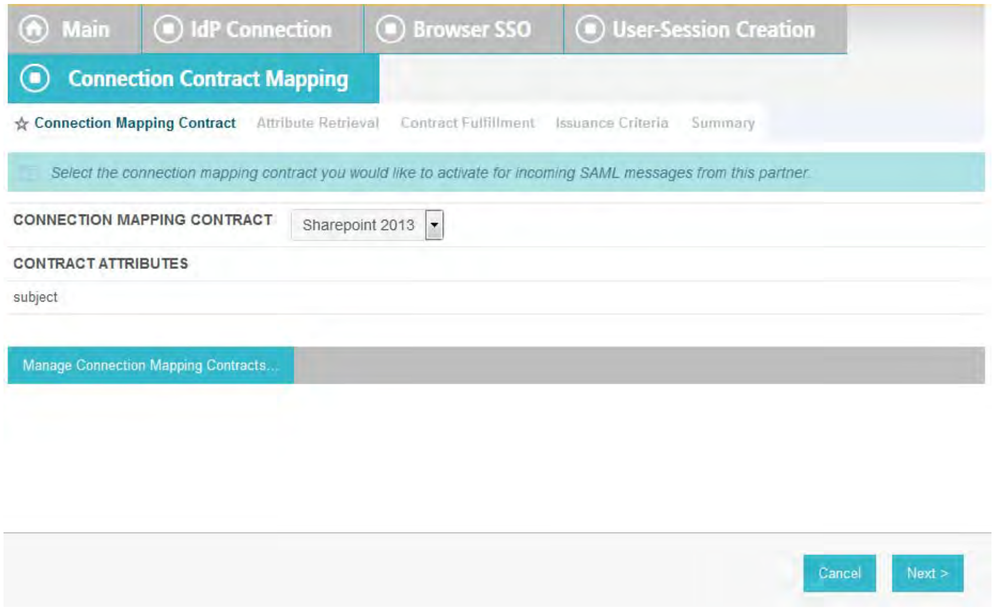


Connection Mapping Contracts allow IdP Connections to map directly to SP Connections using a shared contract. This allows PingFederate to act as a federation hub between IdP and SP partners.

CONTRACT NAME	CONTRACT ID	ACTION
SharePoint	2TSYliBHRp5iqs2t	Delete (Check Usage)
Sharepoint 2013	pHDPDzxOTReXCnFp	Delete

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

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



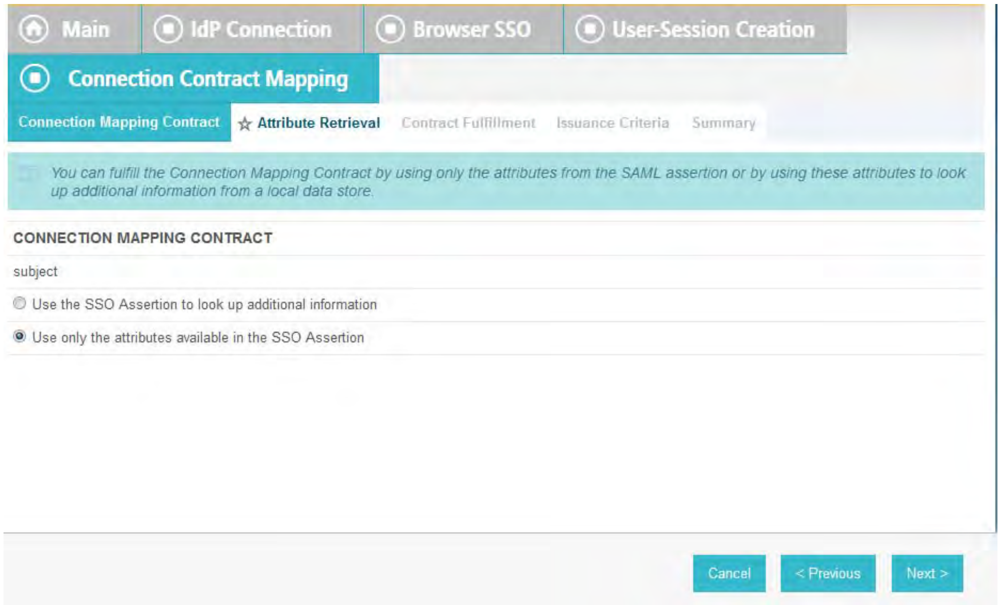
Select the connection mapping contract you would like to activate for incoming SAML messages from this partner.

CONNECTION MAPPING CONTRACT: Sharepoint 2013

CONTRACT ATTRIBUTES

subject

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



You can fulfill the Connection Mapping Contract by using only the attributes from the SAML assertion or by using these attributes to look up additional information from a local data store.

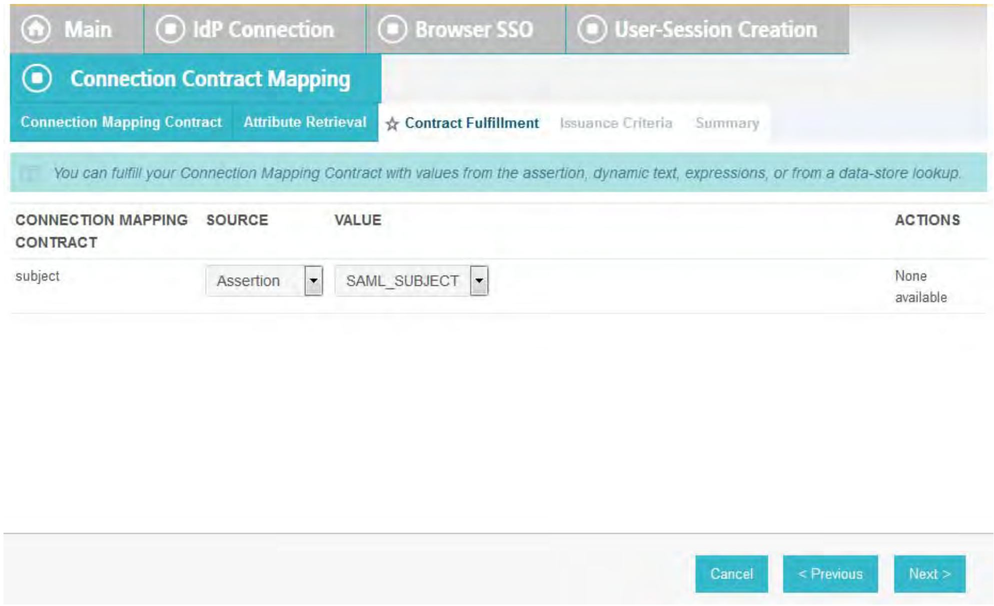
CONNECTION MAPPING CONTRACT

subject

○ Use the SSO Assertion to look up additional information

● Use only the attributes available in the SSO Assertion

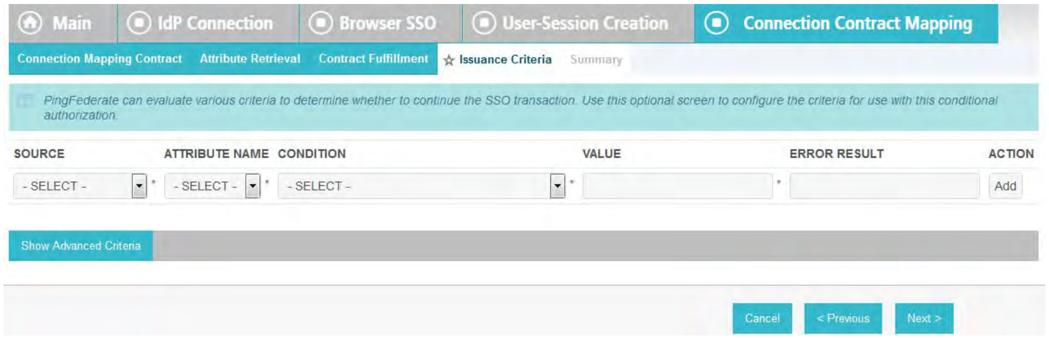
29. Click **Next**. On the Contract Fulfillment screen, for the **SOURCE** field select **Assertion**. For the **VALUE** field, select **SAML_SUBJECT**.



You can fulfill your Connection Mapping Contract with values from the assertion, dynamic text, expressions, or from a data-store lookup.

CONNECTION MAPPING CONTRACT	SOURCE	VALUE	ACTIONS
subject	Assertion	SAML_SUBJECT	None available

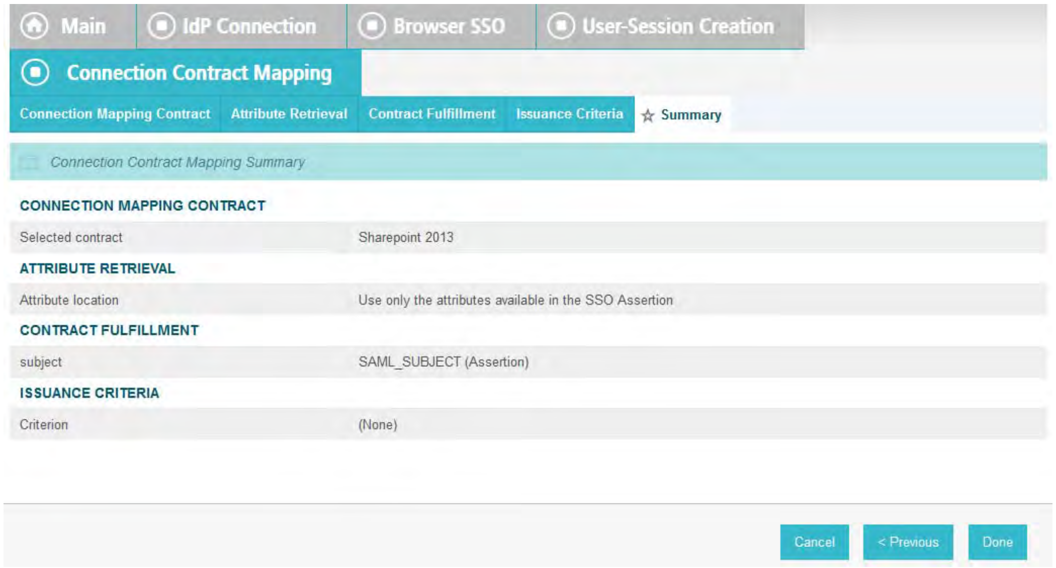
30. Click **Next**.



PingFederate can evaluate various criteria to determine whether to continue the SSO transaction. Use this optional screen to configure the criteria for use with this conditional authorization.

SOURCE	ATTRIBUTE NAME	CONDITION	VALUE	ERROR RESULT	ACTION
- SELECT - *	- SELECT - *	- SELECT - *	*		Add

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

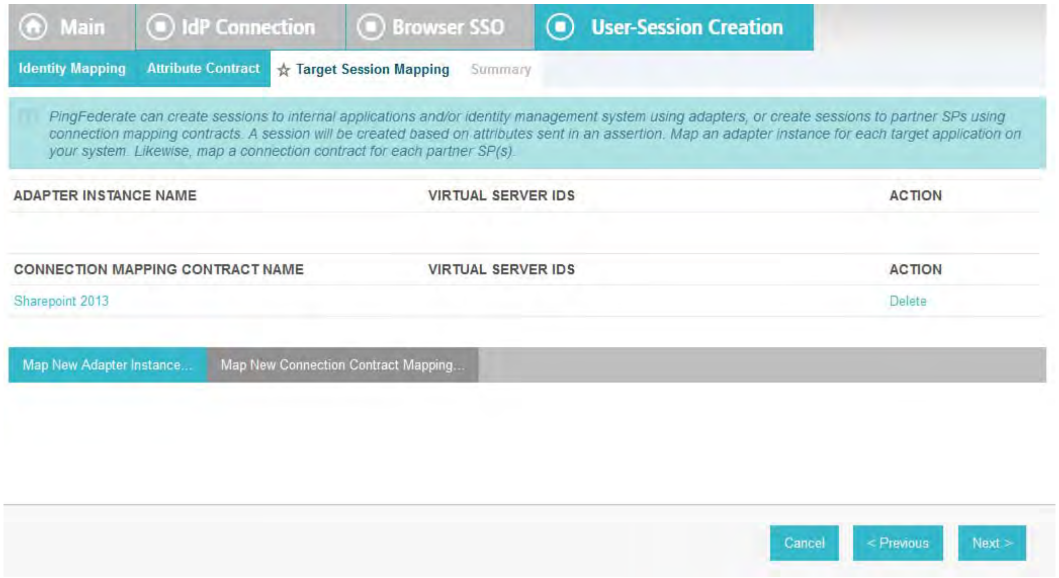


Connection Contract Mapping Summary

CONNECTION MAPPING CONTRACT	
Selected contract	Sharepoint 2013
ATTRIBUTE RETRIEVAL	
Attribute location	Use only the attributes available in the SSO Assertion
CONTRACT FULFILLMENT	
subject	SAML_SUBJECT (Assertion)
ISSUANCE CRITERIA	
Criterion	(None)

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

33. On the Target Session Mapping screen, you should see new contract (e.g. **Sharepoint 2013**) listed under the **CONNECTION MAPPING CONTRACT NAME** field.

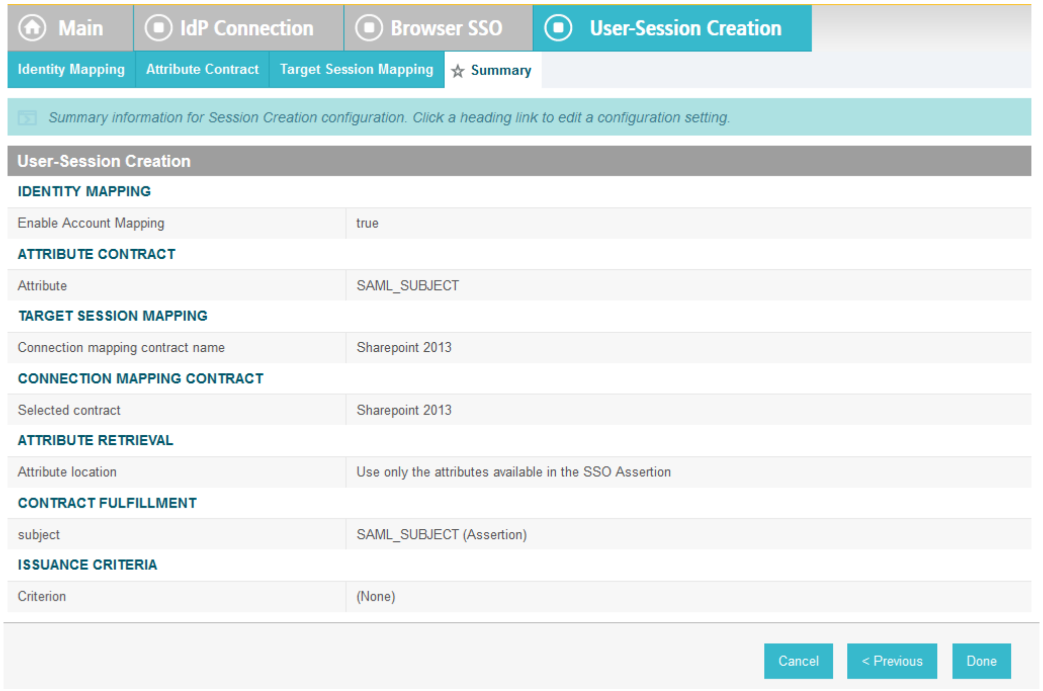


PingFederate can create sessions to internal applications and/or identity management system using adapters, or create sessions to partner SPs using connection mapping contracts. A session will be created based on attributes sent in an assertion. Map an adapter instance for each target application on your system. Likewise, map a connection contract for each partner SP(s).

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		Delete

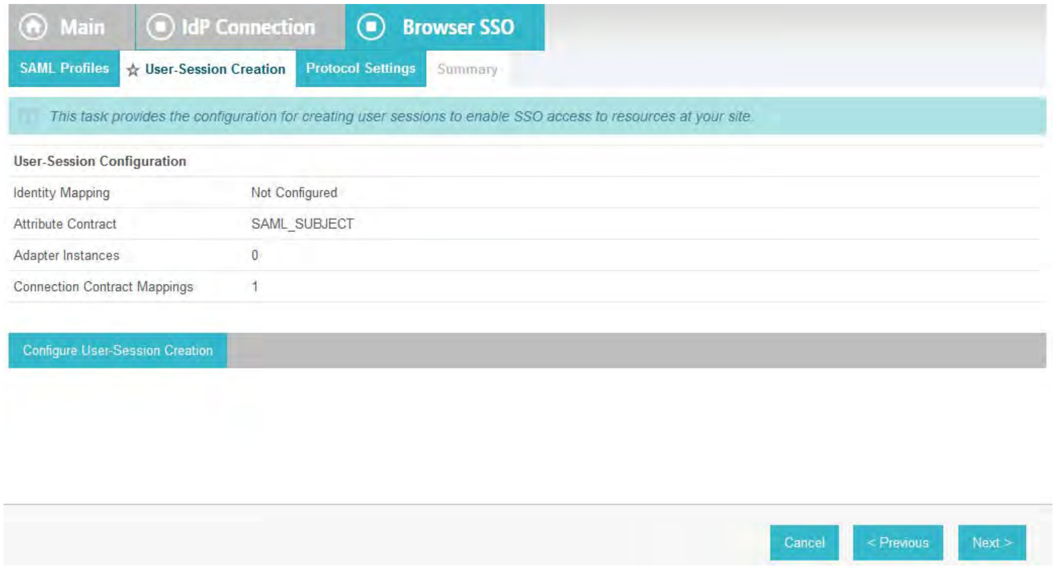
34. Click **Next**.



Summary information for Session Creation configuration. Click a heading link to edit a configuration setting.

User-Session Creation	
IDENTITY MAPPING	
Enable Account Mapping	true
ATTRIBUTE CONTRACT	
Attribute	SAML_SUBJECT
TARGET SESSION MAPPING	
Connection mapping contract name	Sharepoint 2013
CONNECTION MAPPING CONTRACT	
Selected contract	Sharepoint 2013
ATTRIBUTE RETRIEVAL	
Attribute location	Use only the attributes available in the SSO Assertion
CONTRACT FULFILLMENT	
subject	SAML_SUBJECT (Assertion)
ISSUANCE CRITERIA	
Criterion	(None)

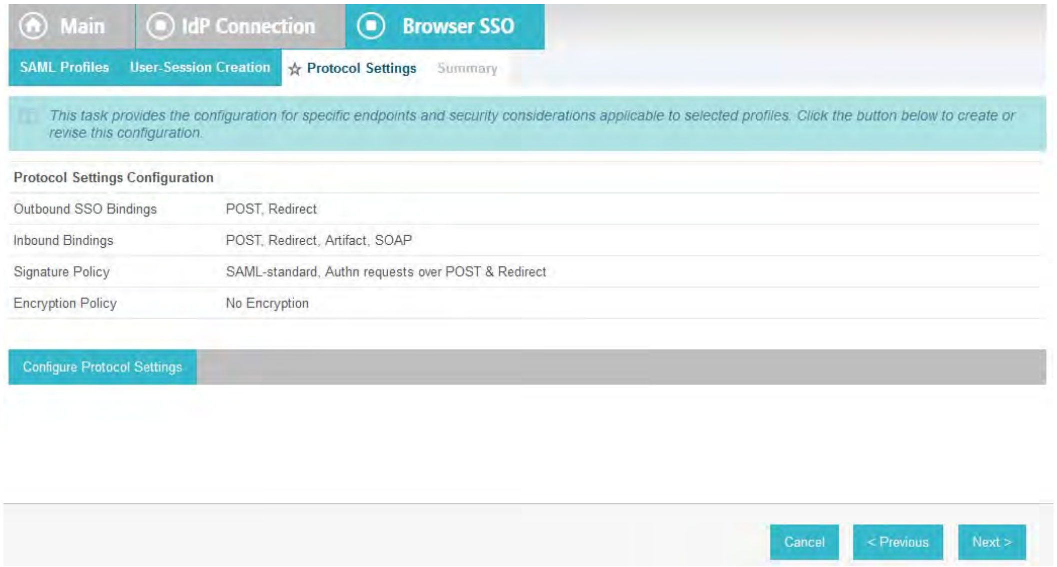
35. Click **Done**.



This task provides the configuration for creating user sessions to enable SSO access to resources at your site.

User-Session Configuration	
Identity Mapping	Not Configured
Attribute Contract	SAML_SUBJECT
Adapter Instances	0
Connection Contract Mappings	1

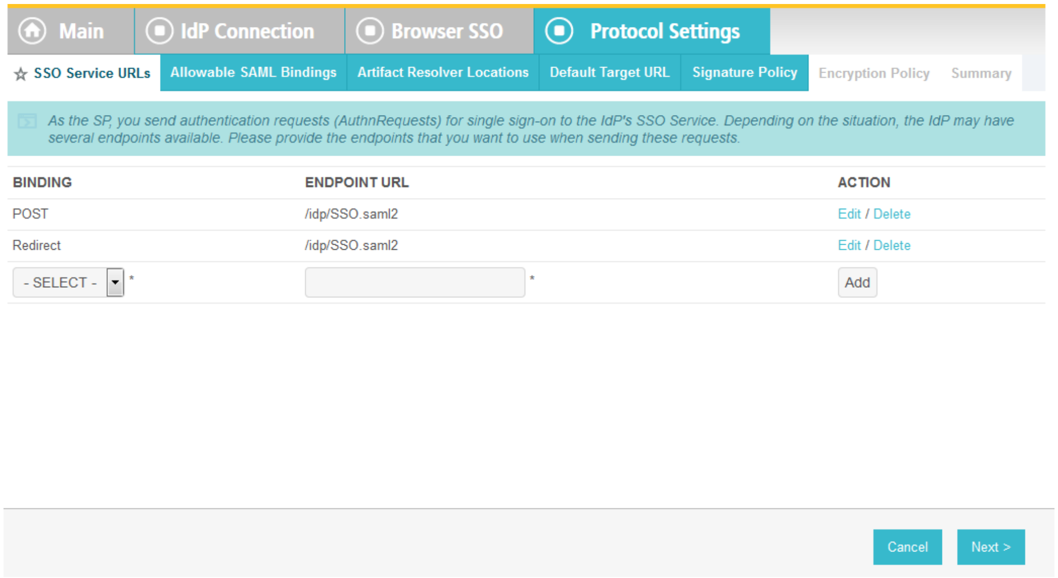
36. On the User-Session Creation screen, click **Next**.



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

Protocol Settings Configuration	
Outbound SSO Bindings	POST, Redirect
Inbound Bindings	POST, Redirect, Artifact, SOAP
Signature Policy	SAML-standard, Authn requests over POST & Redirect
Encryption Policy	No Encryption

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

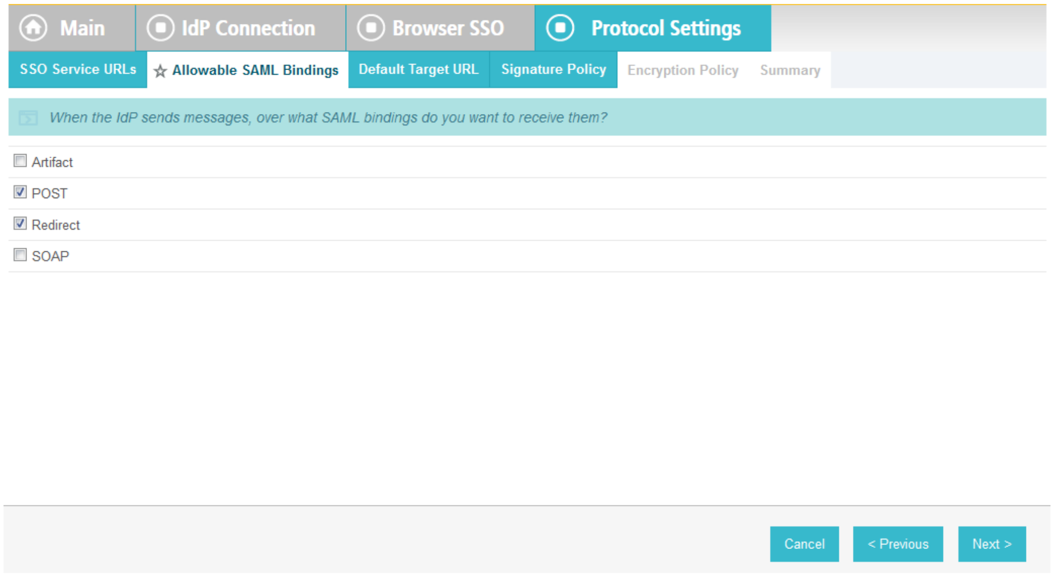


As the SP, you send authentication requests (AuthnRequests) for single sign-on to the IdP's SSO Service. Depending on the situation, the IdP may have several endpoints available. Please provide the endpoints that you want to use when sending these requests.

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

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

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?

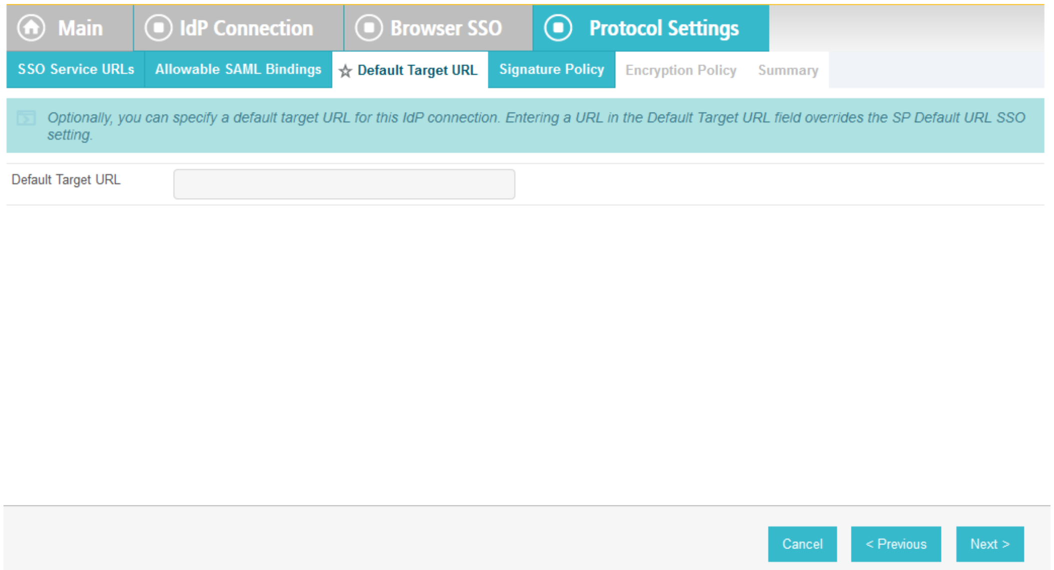
☐ Artifact

☑ POST

☑ Redirect

☐ SOAP

40. Click **Next**.



Optionally, you can specify a default target URL for this IdP connection. Entering a URL in the Default Target URL field overrides the SP Default URL SSO setting.

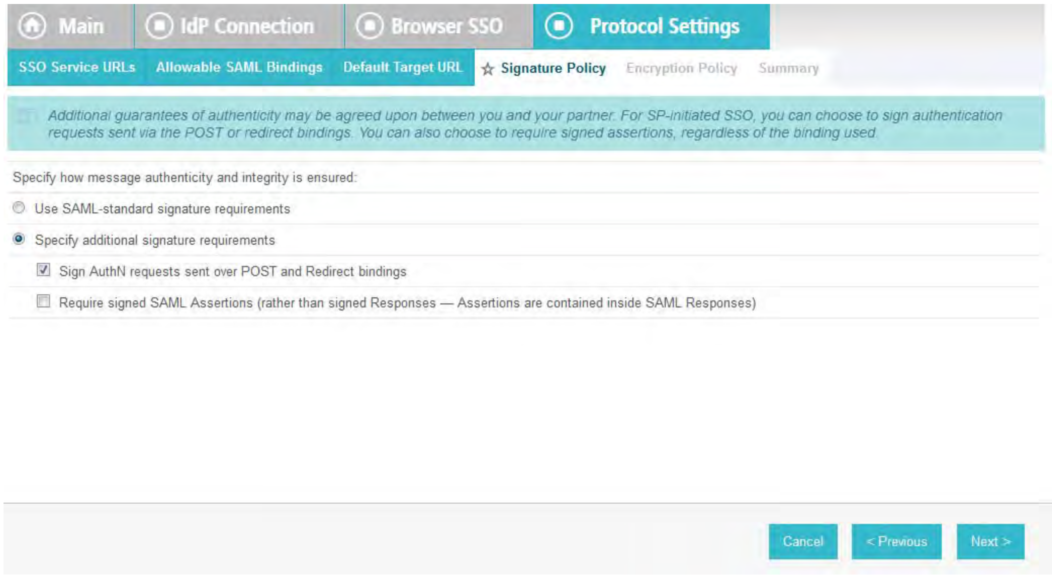
Default Target URL

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

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

    a. **Specify additional signature requirements** and

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



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

Specify how message authenticity and integrity is ensured:

○ Use SAML-standard signature requirements

● Specify additional signature requirements

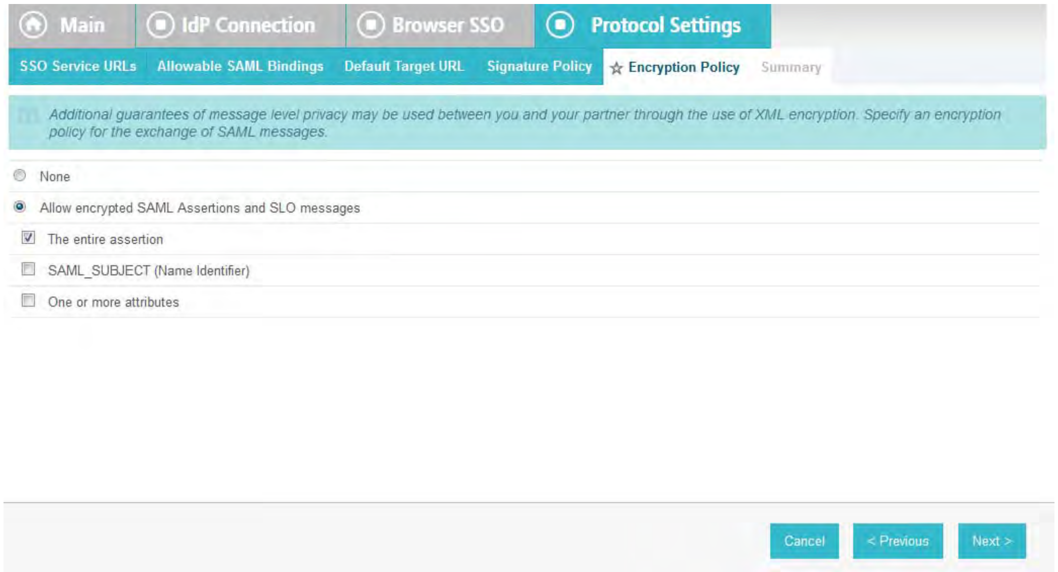
☑ Sign AuthN requests sent over POST and Redirect bindings

□ Require signed SAML Assertions (rather than signed Responses — Assertions are contained inside SAML Responses)

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

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

    b. **The entire assertion**



Additional guarantees of message level privacy may be used between you and your partner through the use of XML encryption. Specify an encryption policy for the exchange of SAML messages.

○ None

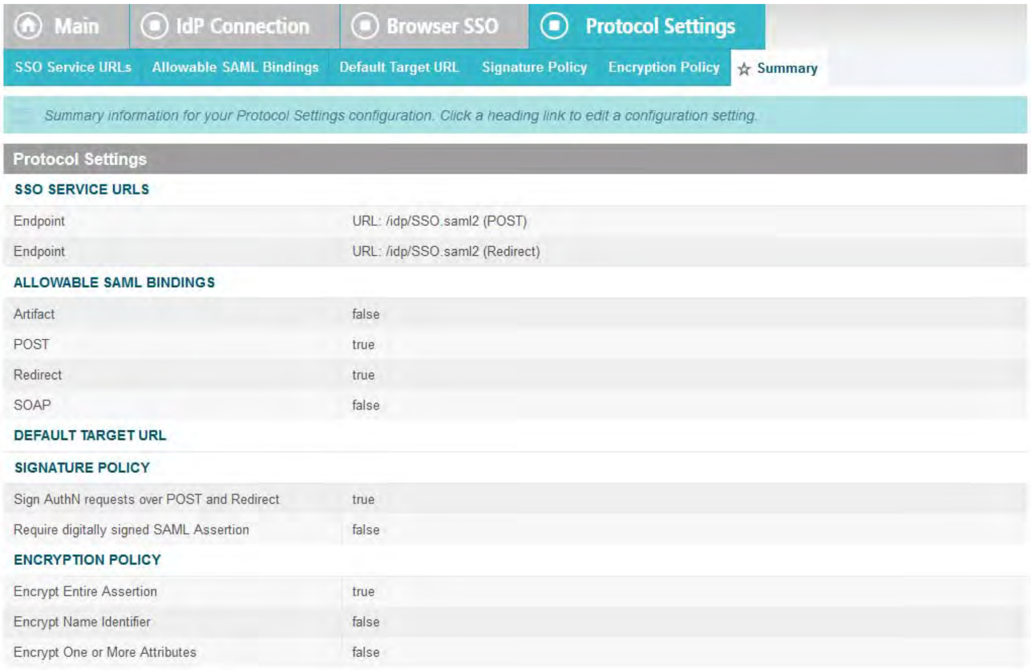
● Allow encrypted SAML Assertions and SLO messages

☑ The entire assertion

□ SAML_SUBJECT (Name Identifier)

□ One or more attributes

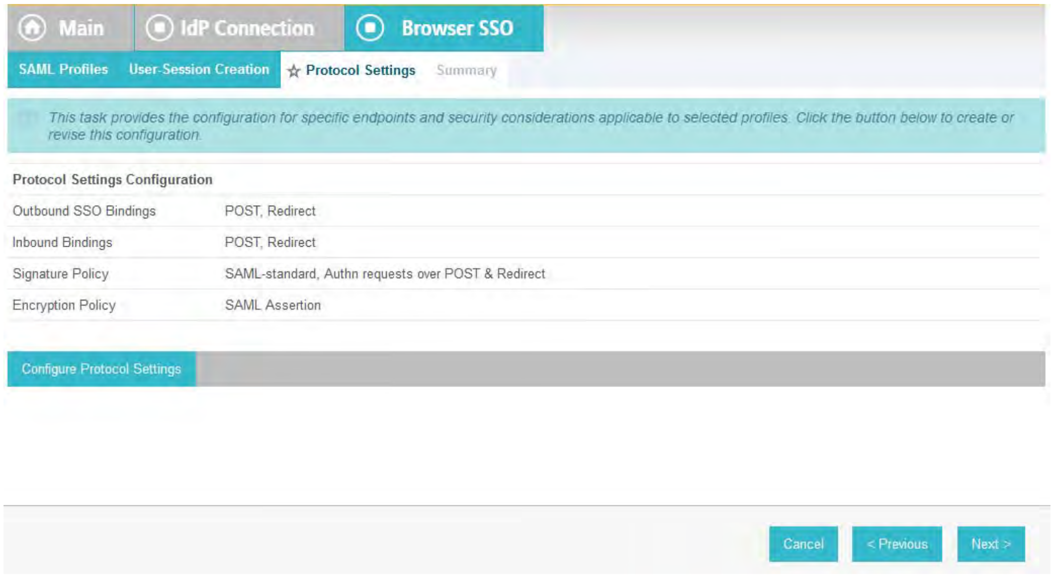
44. Click **Next**.



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

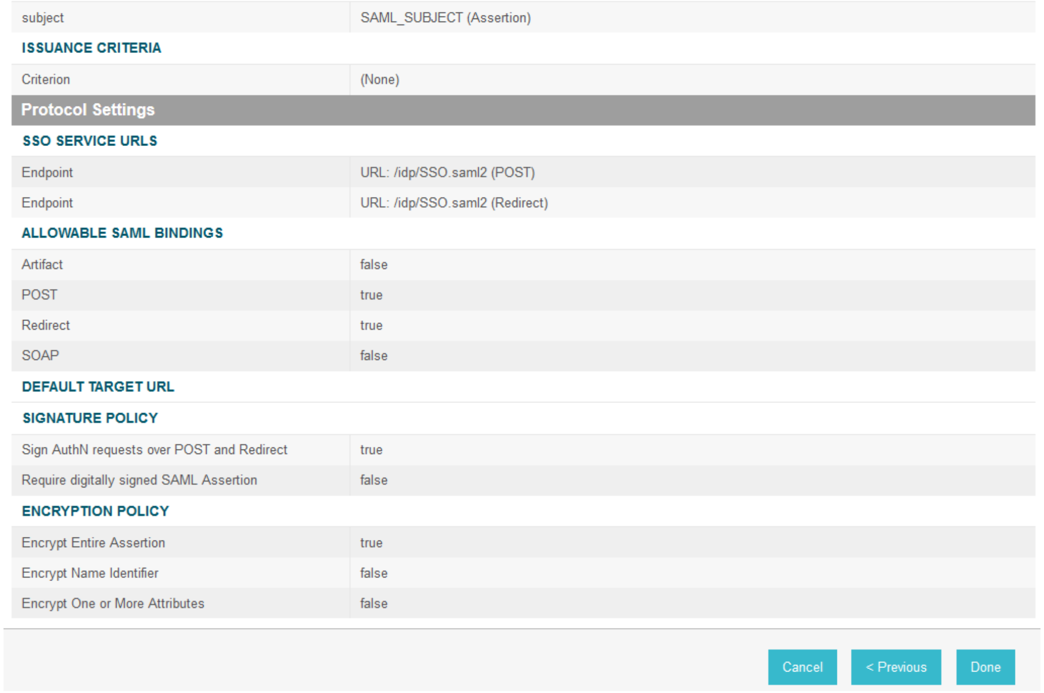
45. On the Summary screen, click **Done**.



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

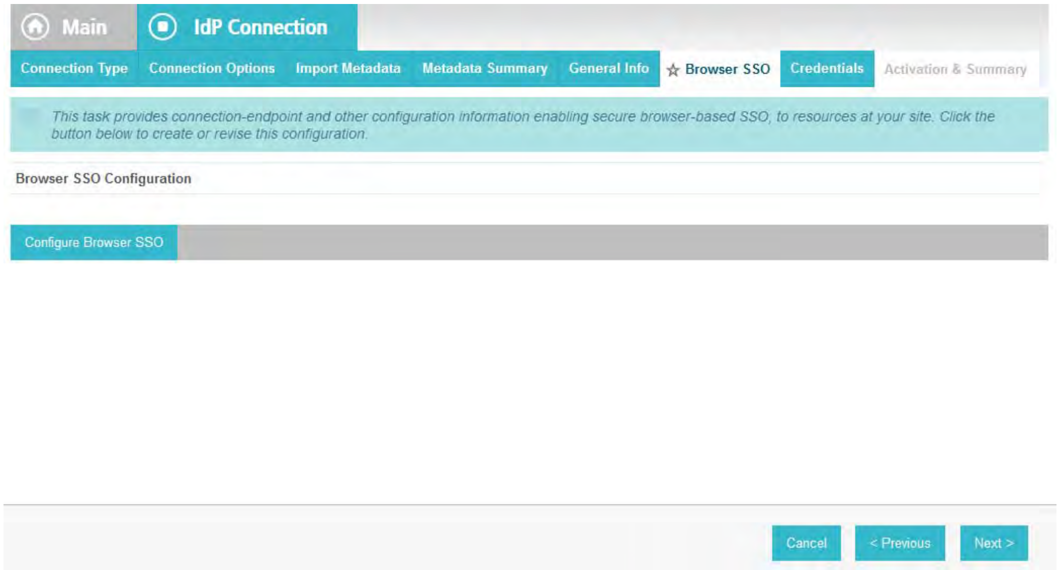
Protocol Settings Configuration	
Outbound SSO Bindings	POST, Redirect
Inbound Bindings	POST, Redirect
Signature Policy	SAML-standard, Authn requests over POST & Redirect
Encryption Policy	SAML Assertion

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



subject	SAML_SUBJECT (Assertion)
ISSUANCE CRITERIA	
Criterion	(None)
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

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

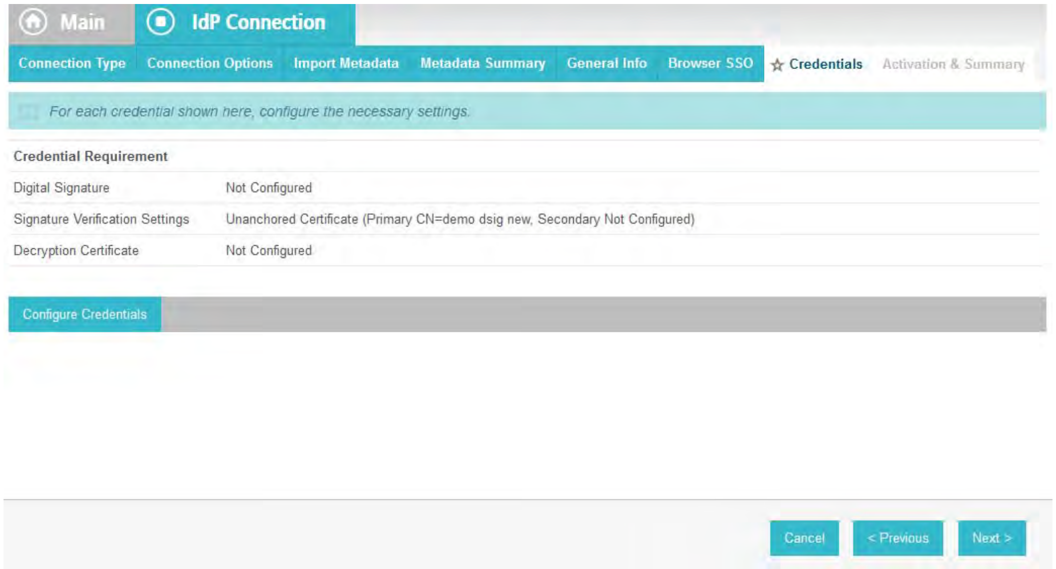


This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your site. Click the button below to create or revise this configuration.

Browser SSO Configuration

185

186 48. On the Browser SSO screen, click **Next**.



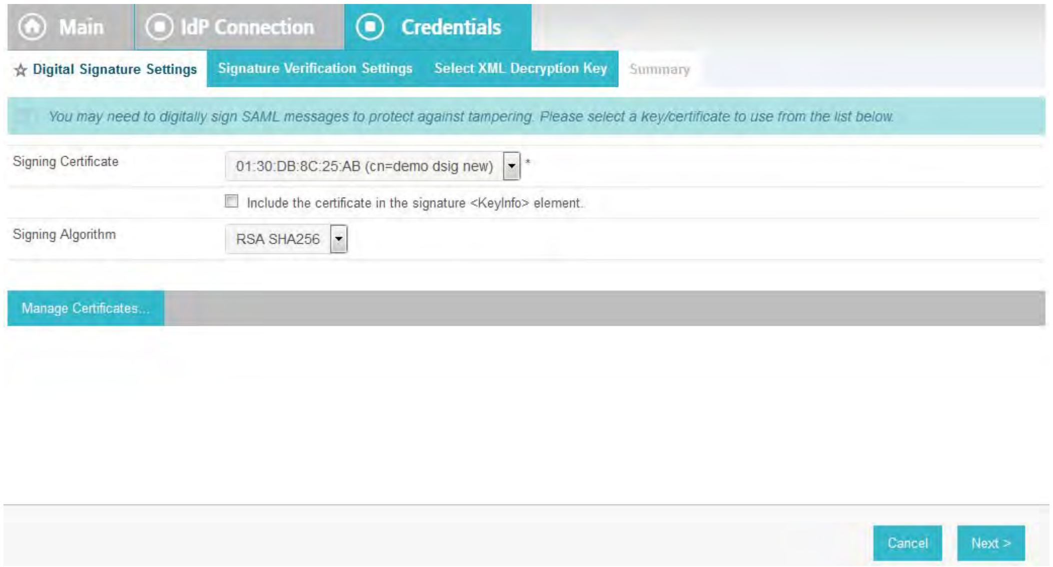
For each credential shown here, configure the necessary settings.

Credential Requirement	
Digital Signature	Not Configured
Signature Verification Settings	Unanchored Certificate (Primary CN=demo dsig new, Secondary Not Configured)
Decryption Certificate	Not Configured

187

188 49. On the Credentials screen, click **Configure Credentials**.

50. On the Digital Signature Settings screen, select:
    a. **Signing Certificate for SAML messages** and
    b. **Signing Algorithm**


Main
IdP Connection
Credentials
☆ Digital Signature Settings
Signature Verification Settings
Select XML Decryption Key
Summary
Manage Certificates...
Cancel
Next >

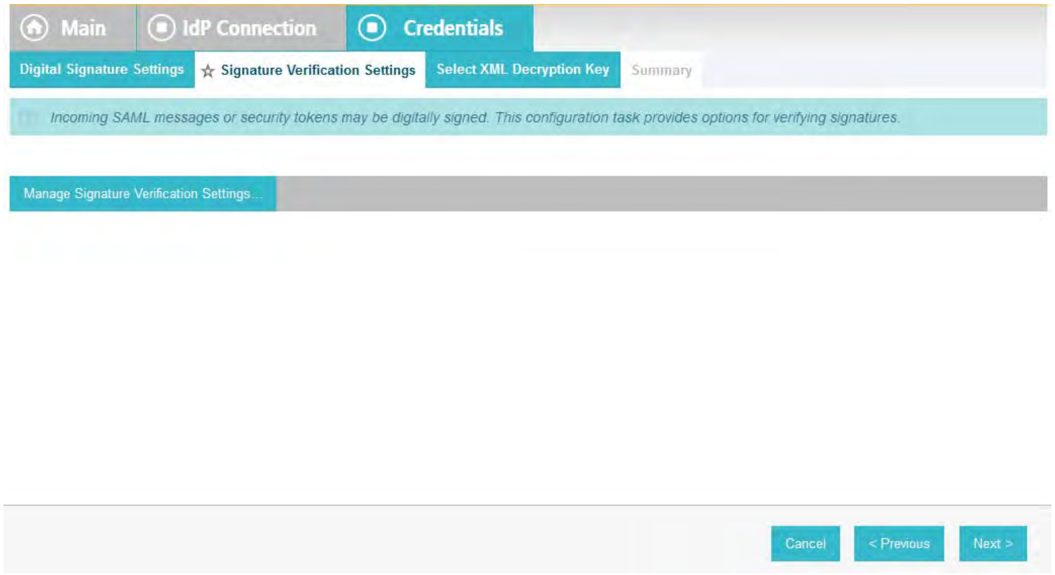
You may need to digitally sign SAML messages to protect against tampering. Please select a key/certificate to use from the list below.

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

□ Include the certificate in the signature <KeyInfo> element.

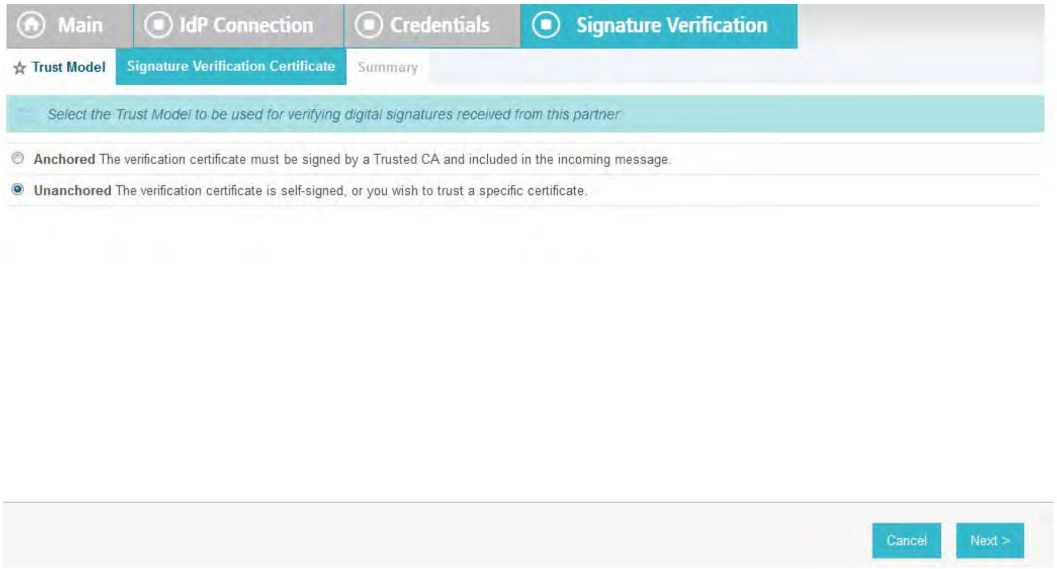
Signing Algorithm: RSA SHA256

51. Click **Next**.


Main
IdP Connection
Credentials
Digital Signature Settings
☆ Signature Verification Settings
Select XML Decryption Key
Summary
Manage Signature Verification Settings...
Cancel
< Previous
Next >

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

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



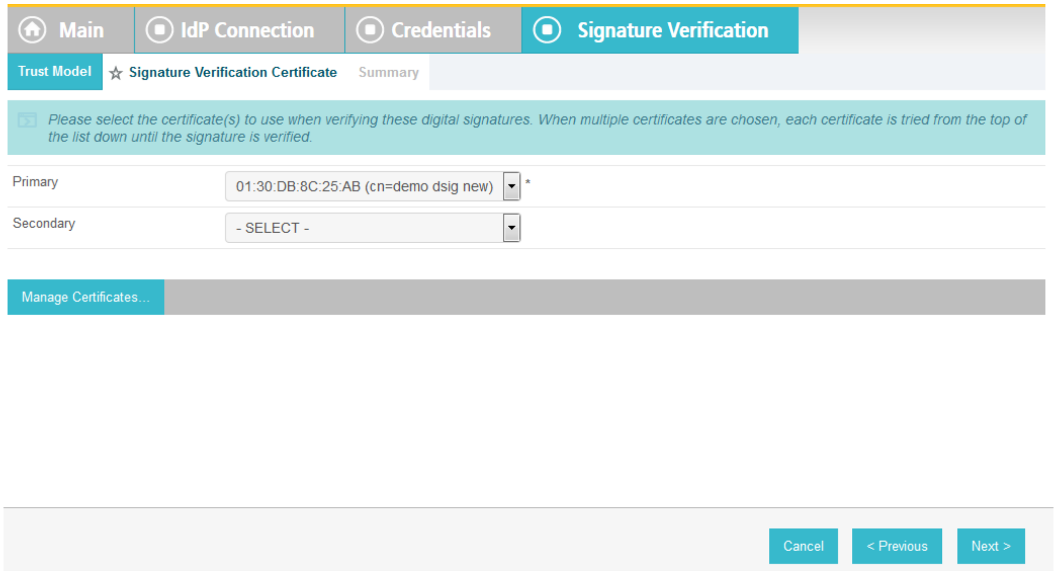
Select the Trust Model to be used for verifying digital signatures received from this partner

○ **Anchored** The verification certificate must be signed by a Trusted CA and included in the incoming message.

● **Unanchored** The verification certificate is self-signed, or you wish to trust a specific certificate.

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

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

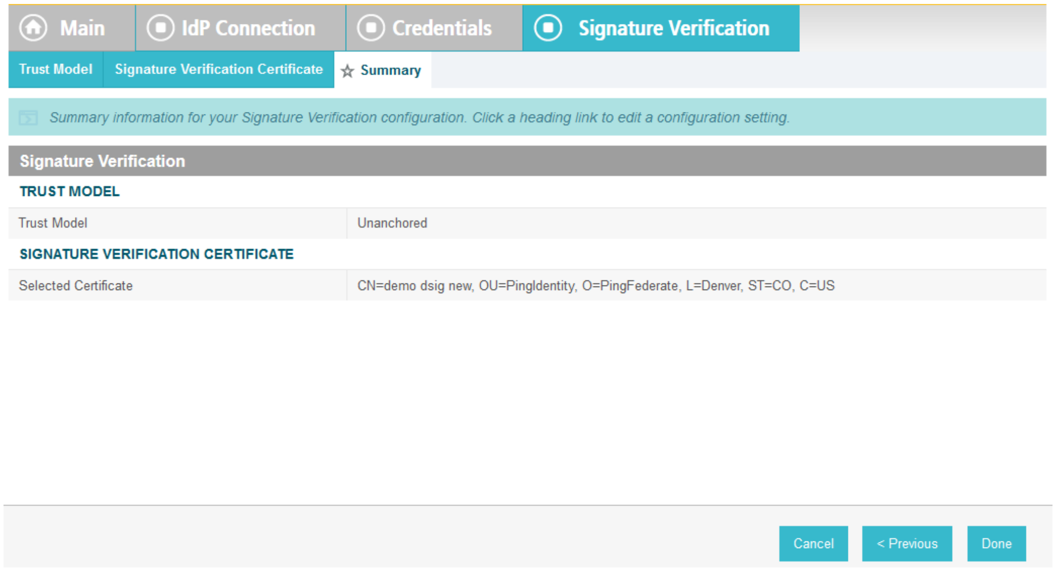


Please select the certificate(s) to use when verifying these digital signatures. When multiple certificates are chosen, each certificate is tried from the top of the list down until the signature is verified.

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

Secondary: - SELECT -

55. Click **Next**.



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

Signature Verification

TRUST MODEL

Trust Model	Unanchored

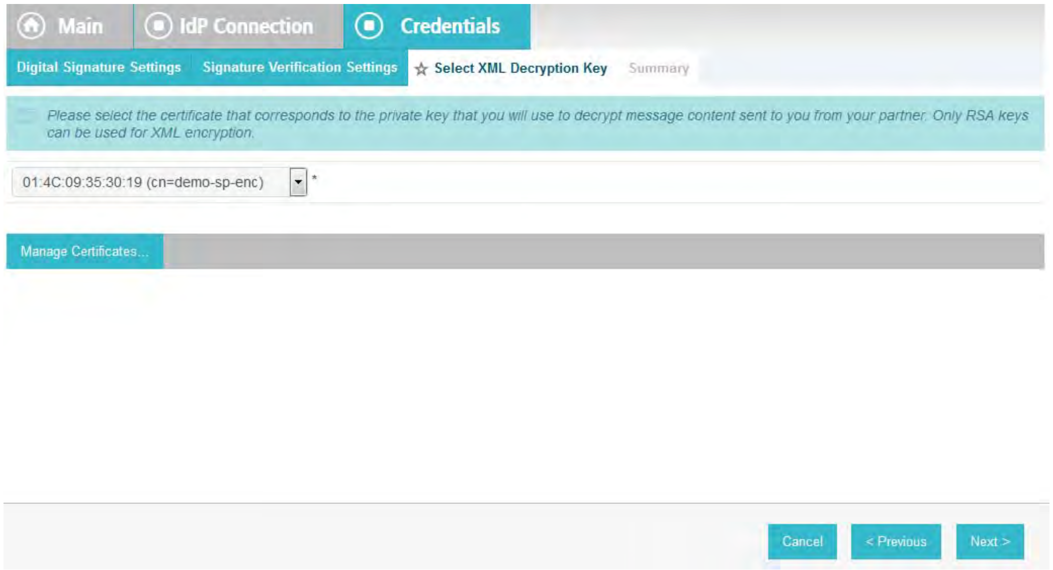
SIGNATURE VERIFICATION CERTIFICATE

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

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

57. On the Signature Verification Settings screen, click **Next**.

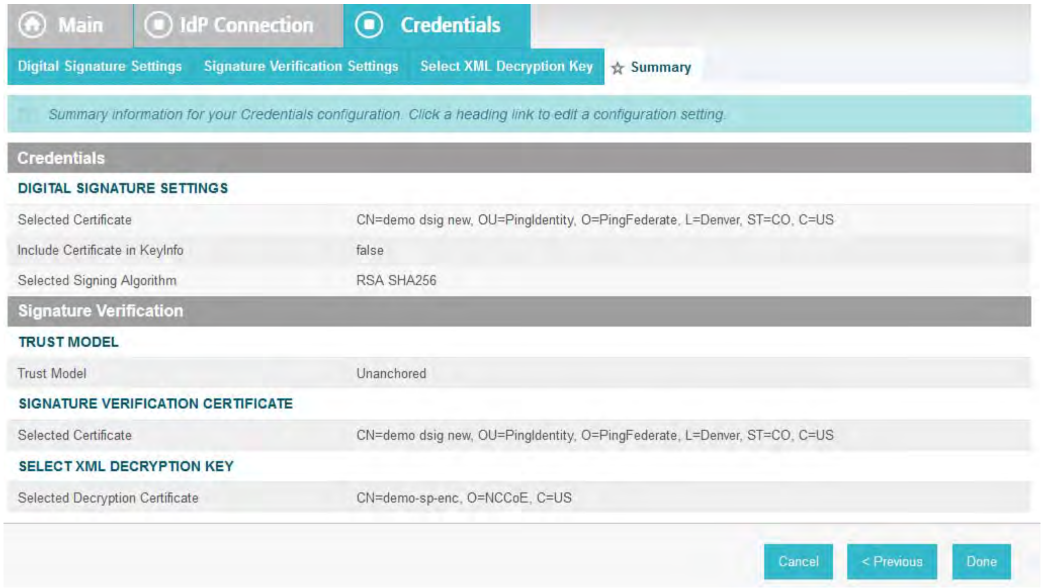
58. On the Select XML Decryption Key screen, select the certificate associated with the private key that will decrypt messages from the Identity Provider.


Main
IdP Connection
Credentials
Digital Signature Settings
Signature Verification Settings
Select XML Decryption Key
Summary
Manage Certificates...
Cancel
< Previous
Next >

Please select the certificate that corresponds to the private key that you will use to decrypt message content sent to you from your partner. Only RSA keys can be used for XML encryption.

01:4C:09:35:30:19 (cn=demo-sp-enc) *

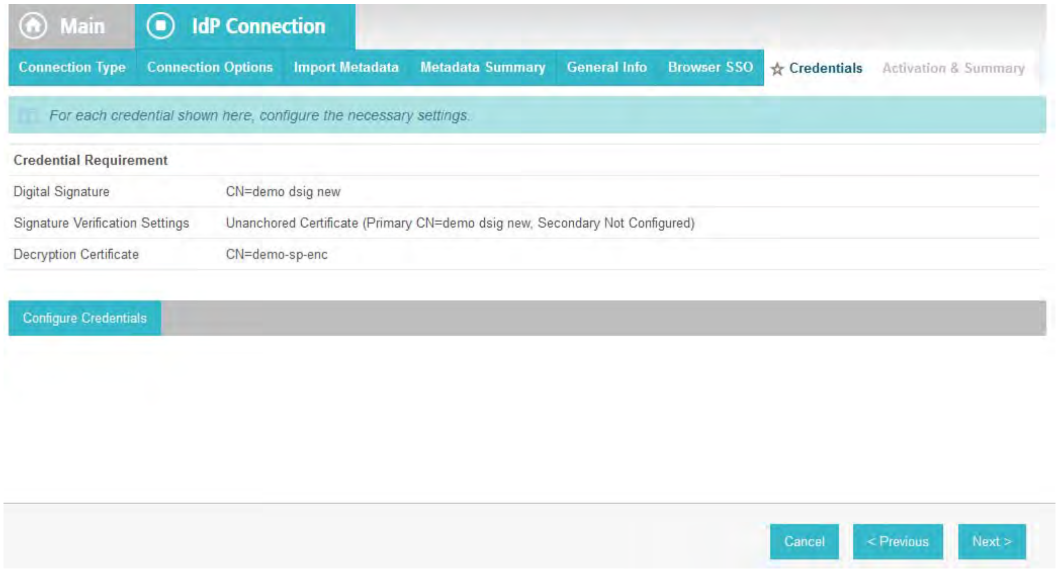
59. Click **Next**.


Main
IdP Connection
Credentials
Digital Signature Settings
Signature Verification Settings
Select XML Decryption Key
☆ Summary
Cancel
< Previous
Done

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 Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256
Signature Verification	
TRUST MODEL	
Trust Model	Unanchored
SIGNATURE VERIFICATION CERTIFICATE	
Selected Certificate	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
SELECT XML DECRYPTION KEY	
Selected Decryption Certificate	CN=demo-sp-enc, O=NCCoE, C=US

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

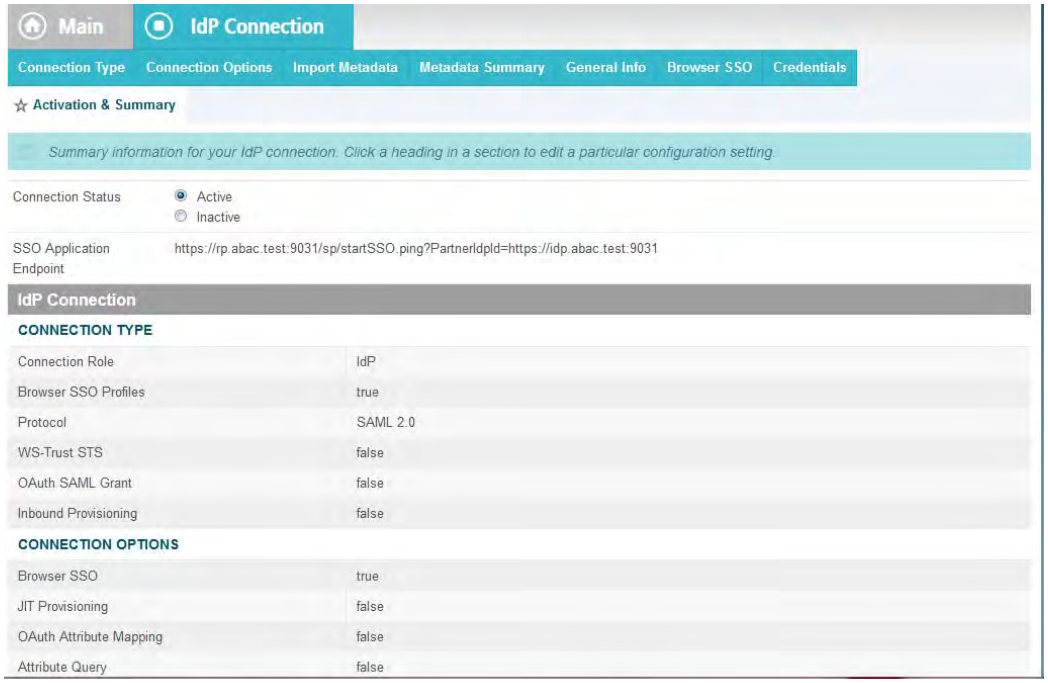


For each credential shown here, configure the necessary settings.

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

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

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



Summary information for your IdP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status: ● Active ○ Inactive

SSO Application Endpoint: https://rp.abac.test:9031/sp/startSSO.ping?PartnerIdpId=https://idp.abac.test:9031

IdP Connection

CONNECTION TYPE	
Connection Role	IdP
Browser SSO Profiles	true
Protocol	SAML 2.0
WS-Trust STS	false
OAuth SAML Grant	false
Inbound Provisioning	false
CONNECTION OPTIONS	
Browser SSO	true
JIT Provisioning	false
OAuth Attribute Mapping	false
Attribute Query	false

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.

64. Click **Save** to save the configuration.

3.5 Functional Test of All Configurations for this Chapter

This section provides instructions to perform an integrated test all of the configurations in Chapter 2.

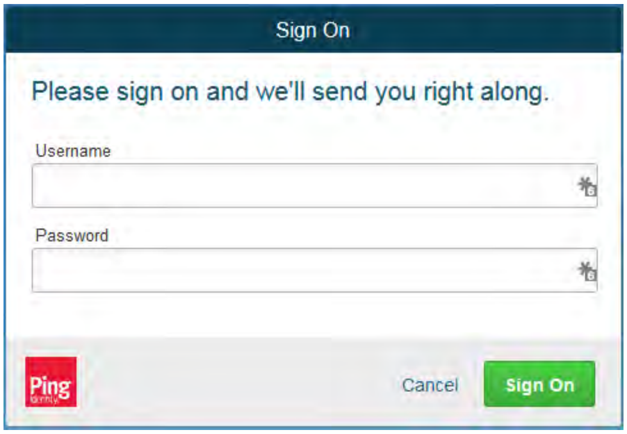
1. Using the browser and PingFederate, a user will log on at the Identity Provider, and then get redirected to the Relying Party.

   Note: This test is similar to the test in chapter 2, except this time the Relying Party has a destination endpoint connection that was configured in chapter 3, so the response code from the Relying Party's Federation server (e.g. rp.abac.test), should be an HTTP 200 status code.

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**).

3. Launch the SAML tracer as in chapter 2 and minimize the tracer window.

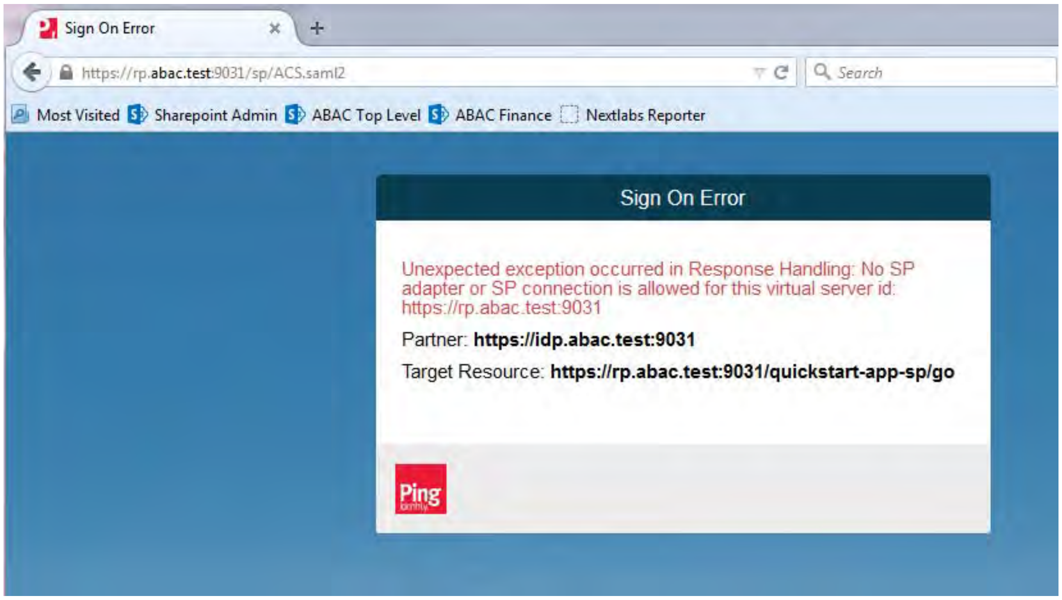
Expected Result: You should see the PingFederate Sign On screen.



Please sign on and we'll send you right along.

4. Enter the **Username** and **Password** of the account created in chapter 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.



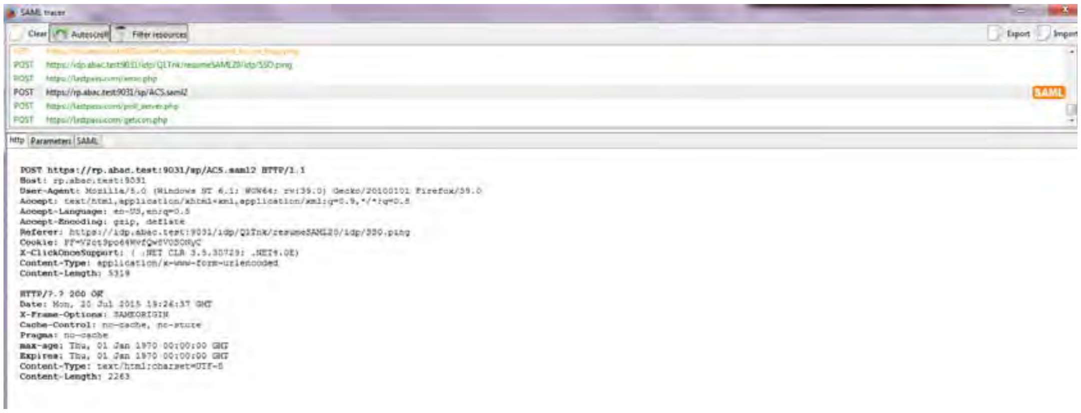
Unexpected exception occurred in Response Handling: No SP adapter or SP connection is allowed for this virtual server id: https://rp.abac.test:9031

Partner: **https://idp.abac.test:9031**

Target Resource: **https://rp.abac.test:9031/quickstart-app-sp/go**

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.



```
POST https://idp.abac.test:9031/idp/Q1Tnk/resumeSAML20/idp/SSO.ping
POST https://lastpass.com/lastpass.php
POST https://rp.abac.test:9031/sp/ACS.saml2
POST https://lastpass.com/poll_server.php
POST https://lastpass.com/geticon.php
```

```
POST https://rp.abac.test:9031/sp/ACS.saml2 HTTP/1.1
Host: rp.abac.test:9031
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://idp.abac.test:9031/idp/Q1Tnk/resumeSAML20/idp/SSO.ping
Cookie: PF=VZct9po64WvfQwSVOSOHyC
X-ClickOnceSupport: ( .NET CLR 3.5.30729; .NET4.0E)
Content-Type: application/x-www-form-urlencoded
Content-Length: 5319

HTTP/?.? 200 OK
Date: Mon, 20 Jul 2015 19:26:37 GMT
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache, no-store
Pragma: no-cache
max-age: Thu, 01 Jan 1970 00:00:00 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 2263
```

Expected Result: In the details page at the bottom, on the http tab, you should see that the browser sent a POST message to the Relying Party's PingFederate server (e.g. **rp.abac.test**). The HTTP response status code (identified on the line that begins with "HTTP") should be a 200 OK code.

4 Installing and Configuring Microsoft SharePoint Server and Related Components

4.1 Introduction

In previous sections of this How-To Guide, we installed several products to establish RP and IdP environments, their components, and the federation between them (Chapter 2 and Chapter 3).

In this section of the How-To Guide we will illustrate how to install IIS (Internet Information Services 8), Microsoft SQL Server 2012, and Microsoft SharePoint Server 2013. Then, within SharePoint we will illustrate how to create a web application, configure the web application to run SSL, create a site collection, and create sub-sites.

In our build, we used ABAC policies and policy enforcement to protect RP resources like SharePoint sites and documents with the help of NextLabs products installed in subsequent How-To sections (Chapter 7 and Chapter 8).

4.1.1 Components Used in this How-To Guide

1. Internet Information Services (IIS) Manager - extensible web server created by Microsoft (formerly Internet Information Server) and is pre-installed in most Windows editions though is not active by default.
2. Microsoft SharePoint 2013 - Microsoft SharePoint is a web-based application within the Windows operating environment. Commonly, SharePoint is deployed as a document management system for intranet, extranet, or cloud repository purposes. SharePoint natively uses an RBAC authorization environment, but it also supports the use of attributes within the user transaction request, a capability Microsoft refers to as being "claims aware." SharePoint also allows for tagging data within its repository, which can be leveraged as object attributes.
3. Microsoft SQL Server 2012 - relational database management system developed by Microsoft. As a database server, it is a software product with the primary function of storing and retrieving data

4.1.2 Required or Recommended Files, Hardware, and Software

Component	Required Files	Required Other Software	Minimum Hardware Requirements	Recommended Hardware	Recommended or Minimum Operating System	Operating System or Other Software Used in this Build
Internet Information Services (IIS) 8	Built-in component in Windows Server 2012 operating system (inactive by default) - Windows Server 2012 ISO	N/A	For the Windows 2012 Server OS: 512 MB RAM, 1.4 GHz 64-bit CPU, 32 GB hard disk; Gigabit Ethernet adapter	For the Windows 2012 Server OS: 800+ MB RAM, >1.4 GHz 64-bit CPU, >32 GB hard disk	Windows Server 2012 R2 Standard 64-bit	Windows Server 2012 R2 Standard 64-bit
Microsoft SharePoint Server 2013	SharePoint Server 2013 installation setup file or DVD	Microsoft SQL Server 2012; Microsoft SQL Server Management Studio; IIS 7.0 or 8.0 (Web Server Role, 8.0 required for Windows Server 2012)	12 GB RAM, 4 core, 64 bit CPU, 80 GB hard disk space for system drive	8+ GB RAM, 4+core 64-bit CPU, >80 GB hard disk	The 64-bit edition of Windows Server 2008 R2 Service Pack 1 (SP1) Standard, Enterprise, or Datacenter or the 64-bit edition of Windows Server 2012 Standard or Datacenter	Windows Server 2012 R2 Standard 64-bit
Microsoft SQL Server 2012	SQL Server 2012 setup file or DVD	.NET 4.0 Framework (SQL Server installs .NET 4.0 during the feature installation step.)	1GB RAM, 1.4GHz CPU, 6 GB of hard-disk space	4 GB RAM (should be increased as database size increases to ensure optimal performance), >2.0 GHz CPU, 6 GH of hard-disk space	Windows Server 2008 R2 or Windows Server 2012, Windows 8.1, Windows 8, Windows 7 SP1, Windows Vista SP2	Windows Server 2012 R2 Standard 64-bit

4.2 Installation of Required Components

4.2.1 Installing SQL Server 2012

1. On the server where SQL Server 2012 is going to be installed, follow the steps from this link to install SQL Server 2012: https://technet.microsoft.com/en-us/library/ms143219(v=sql.110).aspx
    a. Note: in our build, this SQL Server instance is leveraged by SharePoint Server 2013 and by the NextLabs ABAC policy definition, deployment, and enforcement components. Two of these NextLabs components are also installed on the same server as SQL Server 2012 (Chapter 7). In our build we call this server SQLServer.
        i. It is generally recommended by Microsoft regarding SharePoint Server and NextLabs regarding Control Center that the SQL Server be installed on a separate, dedicated server, which is why we chose that deployment in our build.

4.2.2 Installing IIS 8.0 on the SharePoint Server

1. On the separate server where SharePoint Server 2013 is going to be installed, follow the steps from this link to install IIS 8.0 (if not already installed; required for SharePoint Server 2013): http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012
    a. Note: in our build we call this the SharePoint Server.

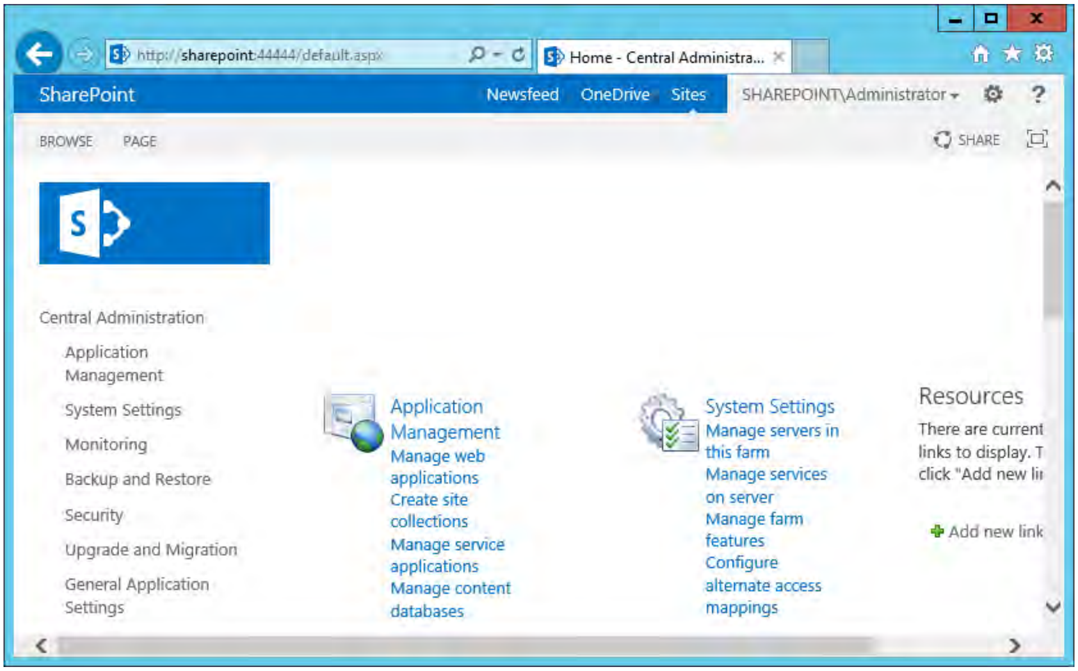
4.2.3 Installing Microsoft SharePoint Server 2013

1. On the separate server where SharePoint Server 2013 is going to be installed, follow the steps from this link to install SharePoint Server 2013: http://social.technet.microsoft.com/wiki/contents/articles/14209.sharepoint-2013-installation-step-by-step.aspx
    a. Note: in our build we call this the SharePoint Server (same as step 2.2).

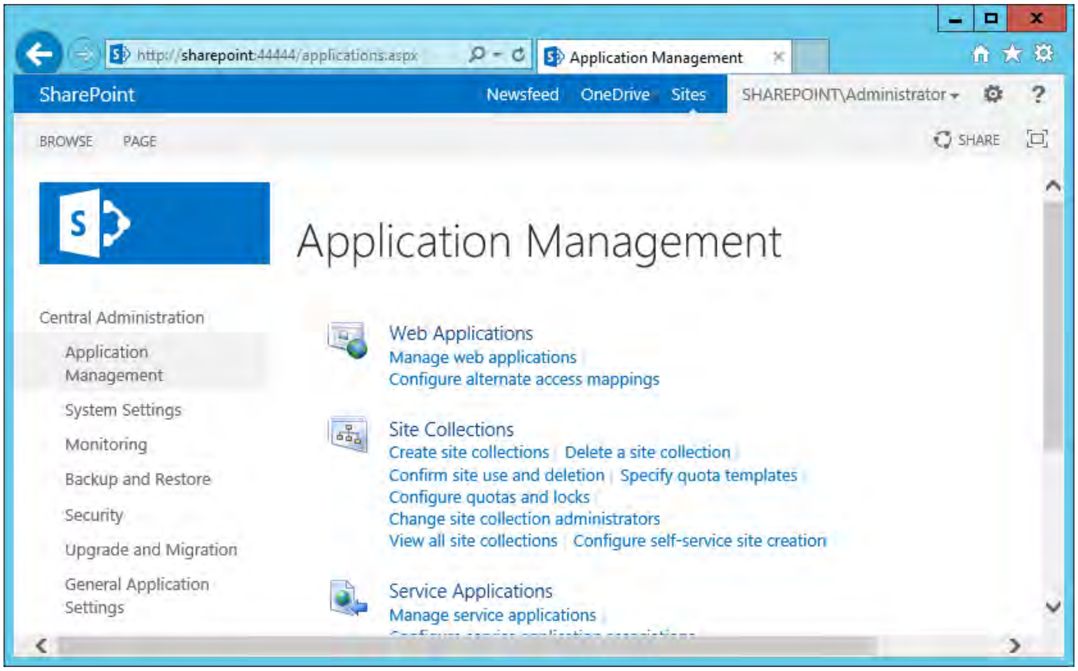
4.3 Creating the Web Application (IIS site) in SharePoint

1. On the SharePoint Server, open a web browser.
2. In the URL address bar of the browser, enter the address for Central Administration and click Enter or Go: **`http://sharepoint:44444/default.aspx`**

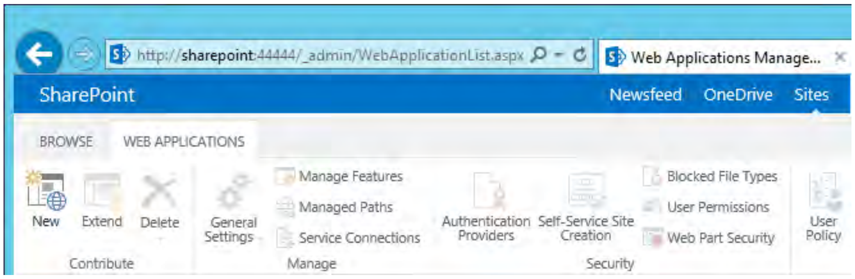
3. From the Central Administration page, click on **Application Management**.



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



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

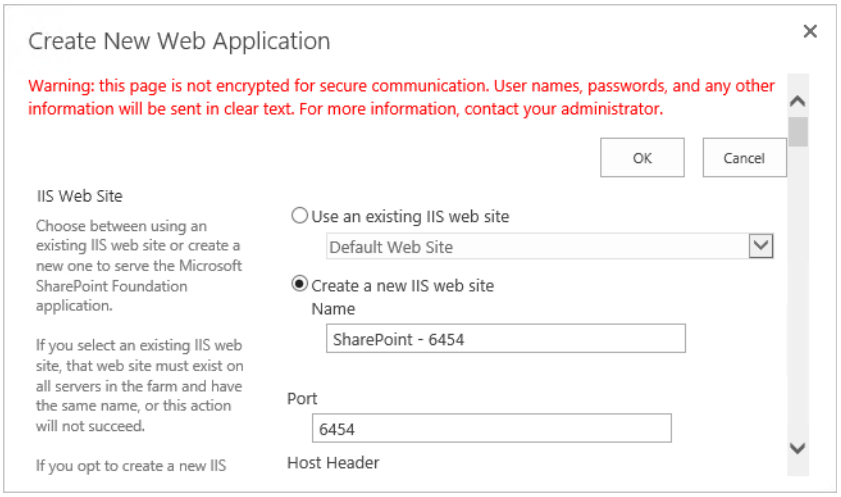


6. In the Create New Web Application window that automatically opens, in the IIS Web Site section, do the following steps to choose the web application's basic IIS configuration:

   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.



Create New Web Application

Warning: this page is not encrypted for secure communication. User names, passwords, and any other information will be sent in clear text. For more information, contact your administrator.

OK Cancel

IIS Web Site

Choose between using an existing IIS web site or create a new one to serve the Microsoft SharePoint Foundation application.

If you select an existing IIS web site, that web site must exist on all servers in the farm and have the same name, or this action will not succeed.

If you opt to create a new IIS

○ Use an existing IIS web site

Default Web Site

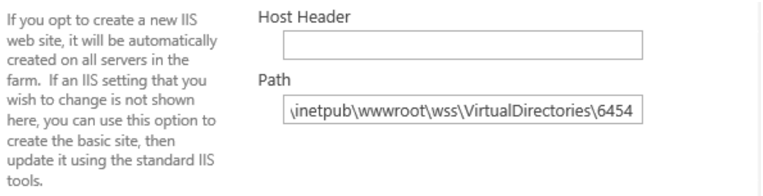
● Create a new IIS web site

Name: SharePoint - 6454

Port: 6454

Host Header

   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.

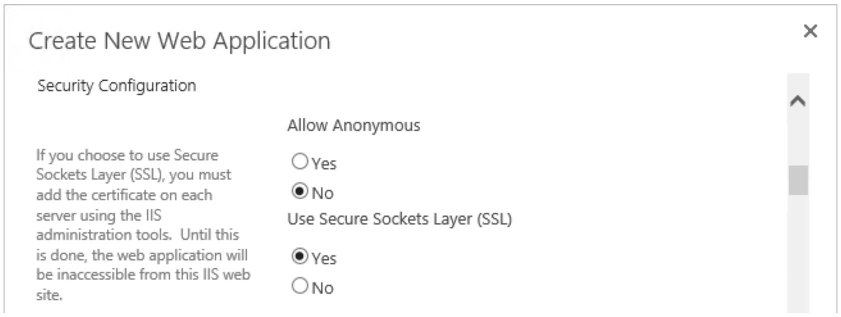
Host Header:

Path: \inetpub\wwwroot\wss\VirtualDirectories\6454

7. Further down in the Create New Web Application window, in the Security Configuration section, do the following steps to configure the web application to run SSL:

   a. Under **Allow Anonymous** leave the **No** radio button chosen (default).

b. Under **Use Secure Sockets Layer (SSL)**, click **Yes**.



Create New Web Application

Security Configuration

If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Allow Anonymous

○ Yes

● No

Use Secure Sockets Layer (SSL)

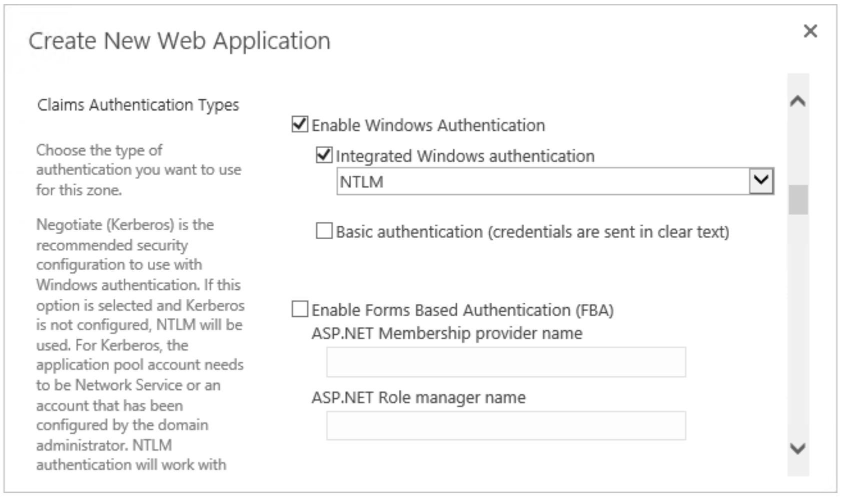
● Yes

○ No

8. Further down in the Create New Web Application window, in the Claims Authentication Types section, do the following steps to enable Windows Authentication (as illustrated):

   a. Click on Enable Windows Authentication

   b. Click on Integrated Windows authentication



Create New Web Application

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with

☑ Enable Windows Authentication

☑ Integrated Windows authentication

NTLM

□ Basic authentication (credentials are sent in clear text)

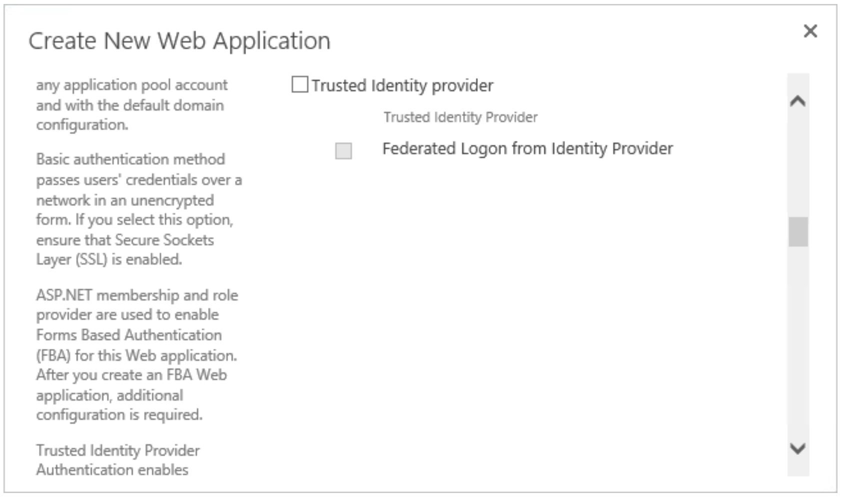
□ Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

ASP.NET Role manager name

9. Further down in the Create New Web Application window, in the Claims Authentication Types section, note that there is a **Trusted Identity provider** section. Do not select this

option now, but later in our build and in other chapters there will be steps for setting up the federated logon.



Create New Web Application

any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional configuration is required.

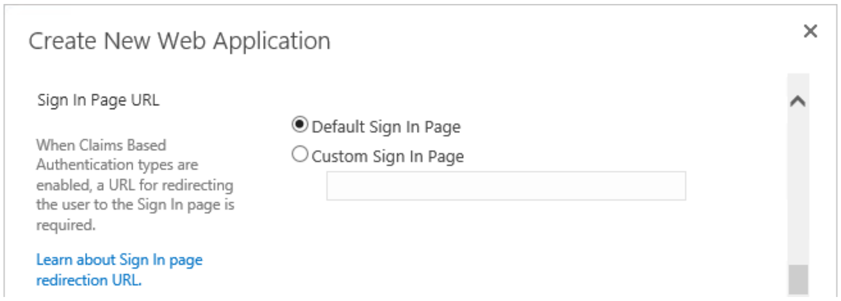
Trusted Identity Provider Authentication enables

□ Trusted Identity provider

Trusted Identity Provider

□ Federated Logon from Identity Provider

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).



Create New Web Application

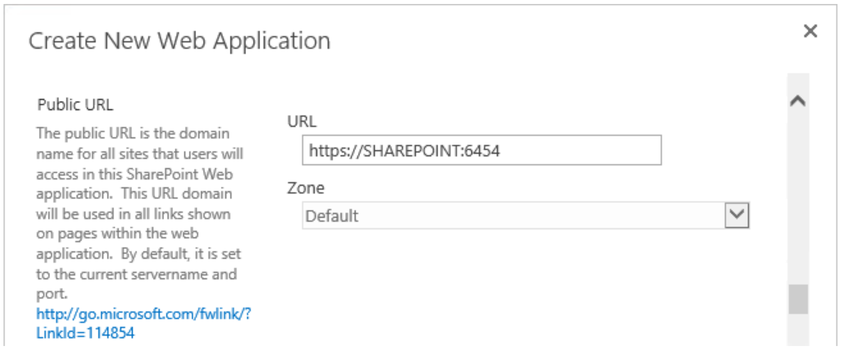
Sign In Page URL

When Claims Based Authentication types are enabled, a URL for redirecting the user to the Sign In page is required.

Learn about Sign In page redirection URL.

● Default Sign In Page
○ Custom Sign In Page

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



Create New Web Application

Public URL

The public URL is the domain name for all sites that users will access in this SharePoint Web application. This URL domain will be used in all links shown on pages within the web application. By default, it is set to the current servername and port.
http://go.microsoft.com/fwlink/?LinkId=114854

URL
https://SHAREPOINT:6454

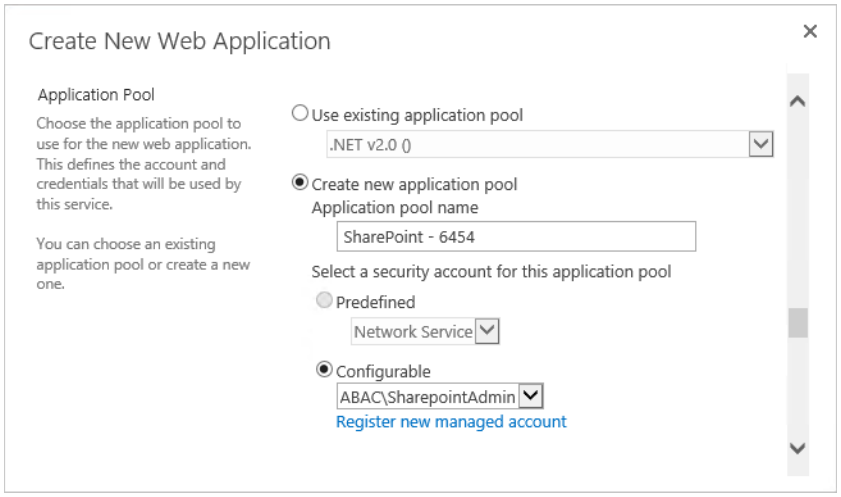
Zone
Default

12. Further down in the Create New Web Application window, in the Application Pool section, leave the default values:

    a. Leave the radio button for **Create new application pool** chosen.

    b. Note that the **Configurable** button is already chosen to select an existing security account for the new application pool, an account called **SharePointAdmin** in this build

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



Create New Web Application

Application Pool

Choose the application pool to use for the new web application. This defines the account and credentials that will be used by this service.

You can choose an existing application pool or create a new one.

○ Use existing application pool

.NET v2.0 ()

● Create new application pool

Application pool name: SharePoint - 6454

Select a security account for this application pool

○ Predefined

Network Service

● Configurable

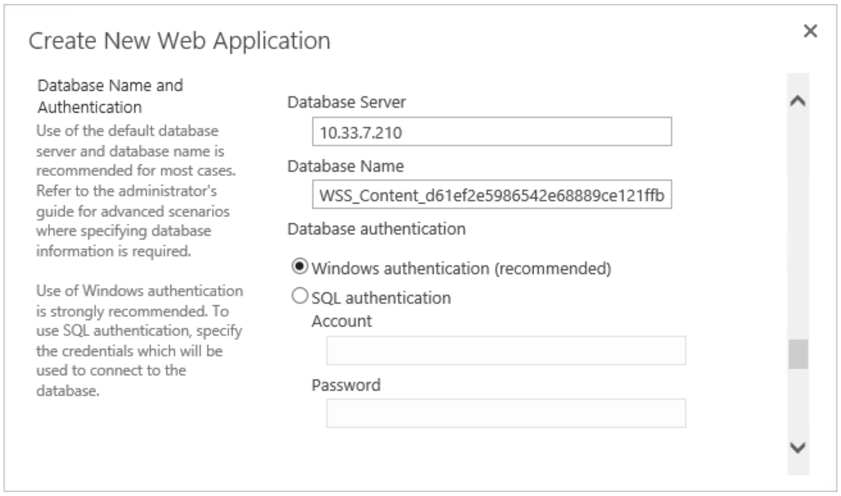
ABAC\SharepointAdmin

Register new managed account

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

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

b. **Database name**



Create New Web Application

Database Name and Authentication

Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database information is required.

Use of Windows authentication is strongly recommended. To use SQL authentication, specify the credentials which will be used to connect to the database.

Database Server: 10.33.7.210

Database Name: WSS_Content_d61ef2e5986542e68889ce121ffb

Database authentication

● Windows authentication (recommended)

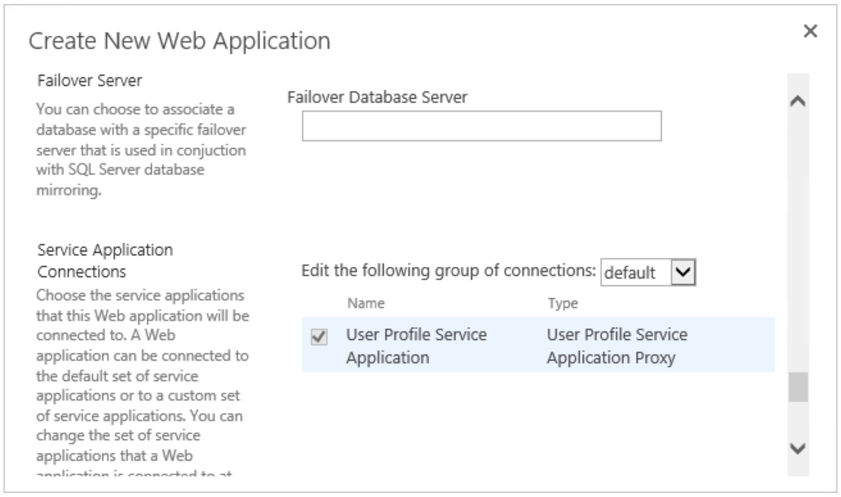
○ SQL authentication

Account:

Password:

14. Further down in the Create New Web Application window, in the Failover Server section, leave the **Failover Database Server** field blank.

15. Further down in the Create New Web Application window, in Service Application Connections, leave the default checkbox for **User Profile Service Application** checked.



Create New Web Application

Failover Server

You can choose to associate a database with a specific failover server that is used in conjuction with SQL Server database mirroring.

Failover Database Server

Service Application Connections

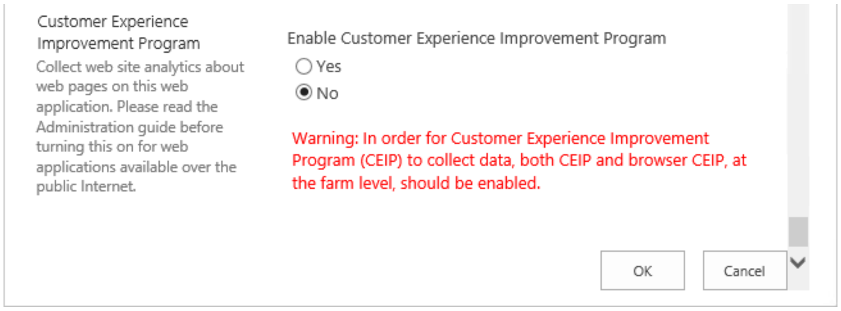
Choose the service applications that this Web application will be connected to. A Web application can be connected to the default set of service applications or to a custom set of service applications. You can change the set of service applications that a Web application is connected to at

Edit the following group of connections: default

	Name	Type
☑	User Profile Service Application	User Profile Service Application Proxy

16. Further down in the Create New Application window, in Customer Experience Improvement Program, either keep the **Enable Customer Experience Improvement Program** radio button for **No** chosen, or click on **Yes**.

17. At the bottom of the Create New Application window click **OK** to finish the web application creation process.



Customer Experience Improvement Program

Collect web site analytics about web pages on this web application. Please read the Administration guide before turning this on for web applications available over the public Internet.

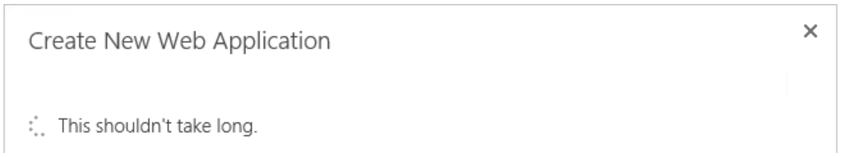
Enable Customer Experience Improvement Program

○ Yes

● No

Warning: In order for Customer Experience Improvement Program (CEIP) to collect data, both CEIP and browser CEIP, at the farm level, should be enabled.

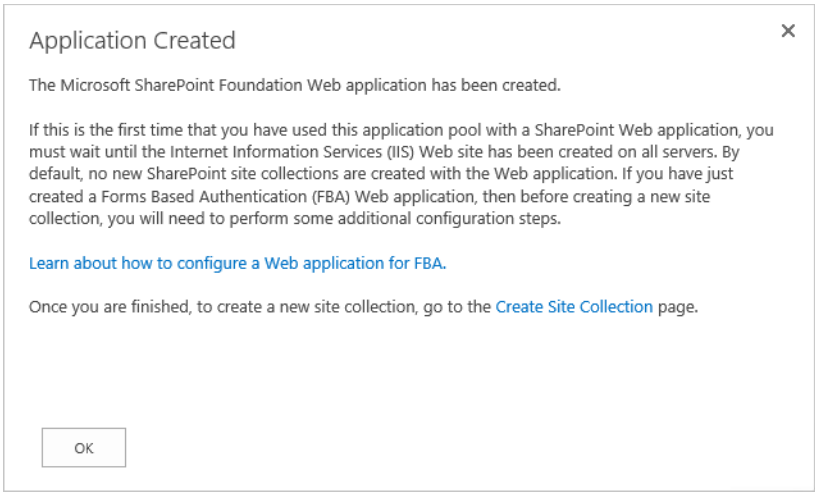
18. Wait for the new web application to be created.



Create New Web Application

This shouldn't take long.

19. In the Application Created window, click **OK**.



Application Created

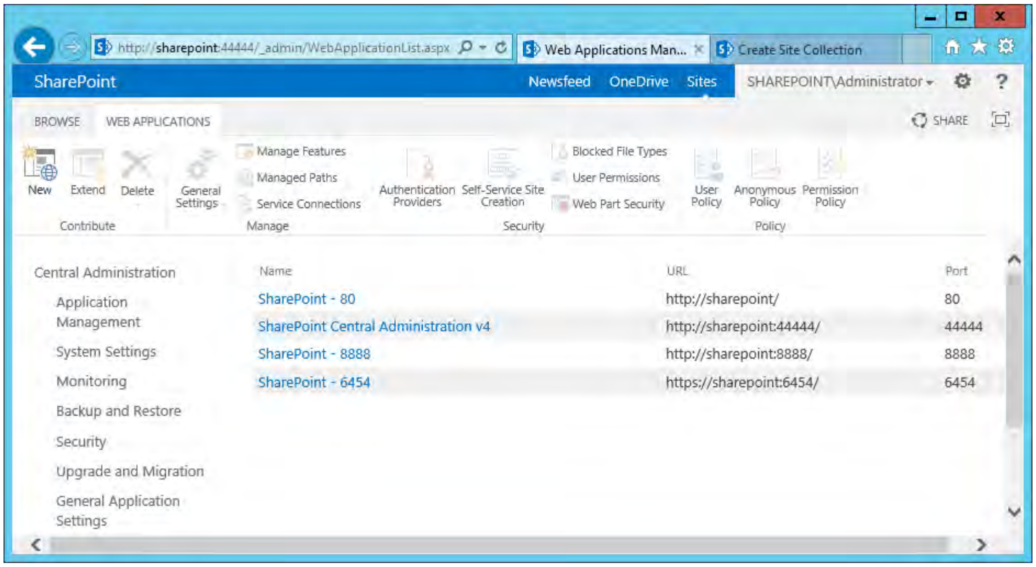
The Microsoft SharePoint Foundation Web application has been created.

If this is the first time that you have used this application pool with a SharePoint Web application, you must wait until the Internet Information Services (IIS) Web site has been created on all servers. By default, no new SharePoint site collections are created with the Web application. If you have just created a Forms Based Authentication (FBA) Web application, then before creating a new site collection, you will need to perform some additional configuration steps.

Learn about how to configure a Web application for FBA.

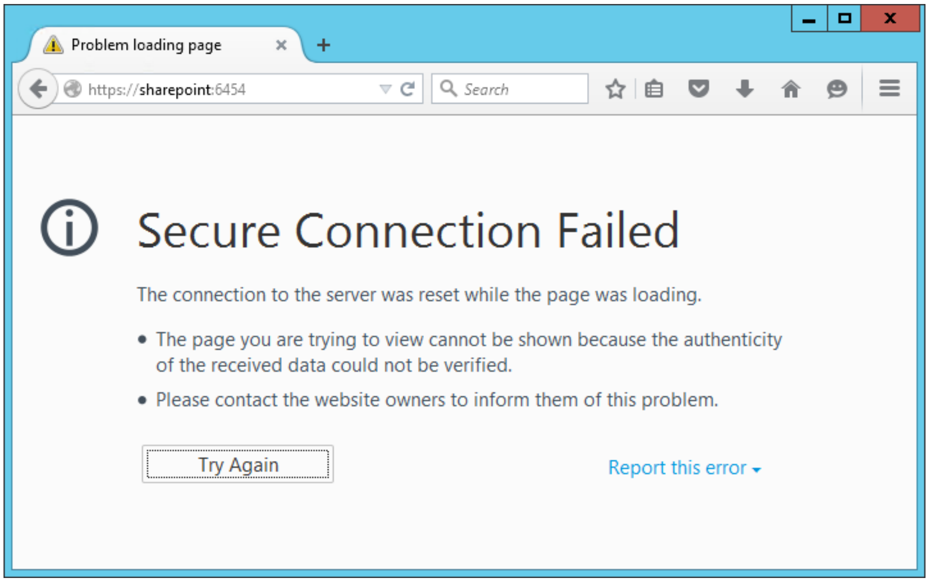
Once you are finished, to create a new site collection, go to the Create Site Collection page.

20. Back on the Web Applications page, verify that your new SharePoint web application is listed ("SharePoint - 6454" from this example).



Name	URL	Port
SharePoint - 80	http://sharepoint/	80
SharePoint Central Administration v4	http://sharepoint:44444/	44444
SharePoint - 8888	http://sharepoint:8888/	8888
SharePoint - 6454	https://sharepoint:6454/	6454

21. 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.



Secure Connection Failed

The connection to the server was reset while the page was loading.

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

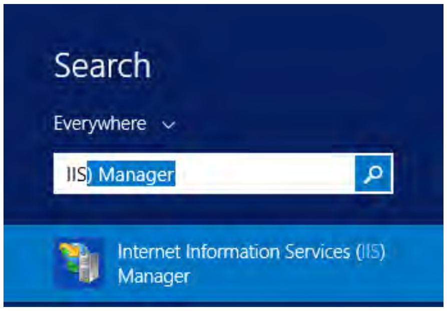
4.4 Creating and installing SSL certificate

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.

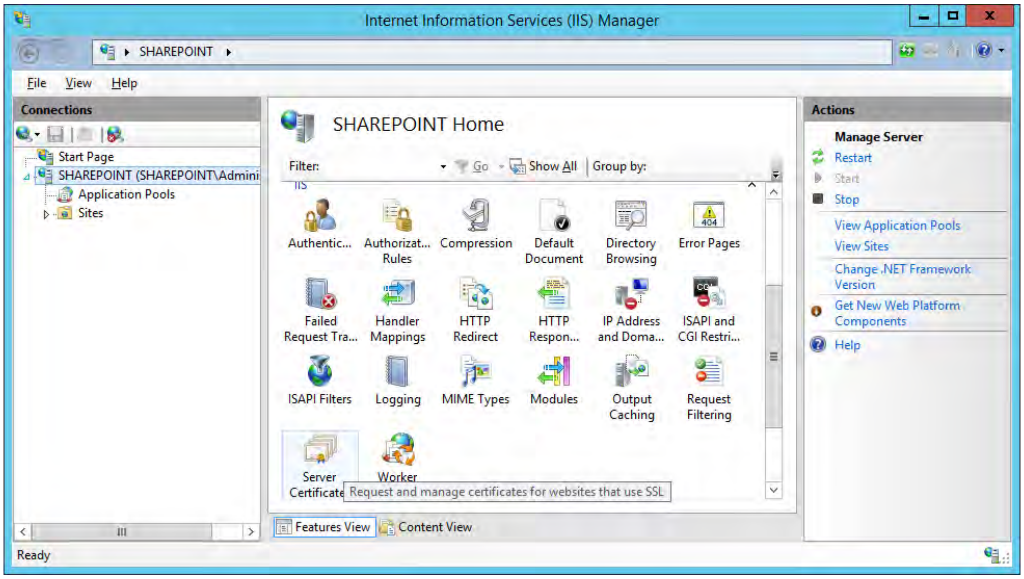
4.4.1 Self-Signed Certificates

4.4.1.1 Creating a Self-Signed Certificate on IIS 8

1. On the SharePoint Server, click on the **Windows** icon in the bottom left corner of your screen.
2. Begin typing **`IIS`**.
3. When the **Internet Information Services (IIS) Manager** appears, click on it.

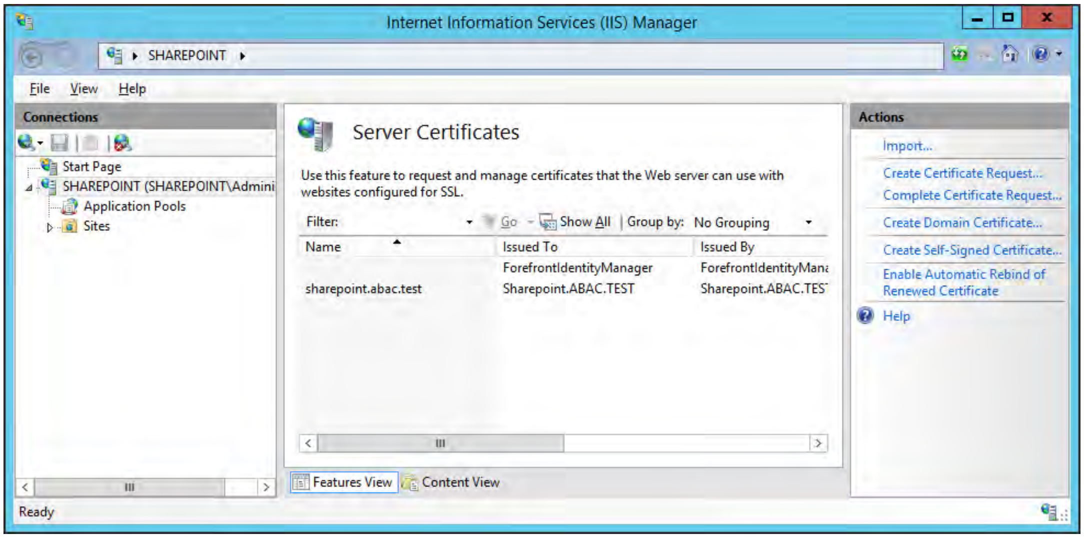


4. Click on the **SharePoint Instance** to see its Features.
5. Scroll down and double-click on **Server Certificates**.



Request and manage certificates for websites that use SSL

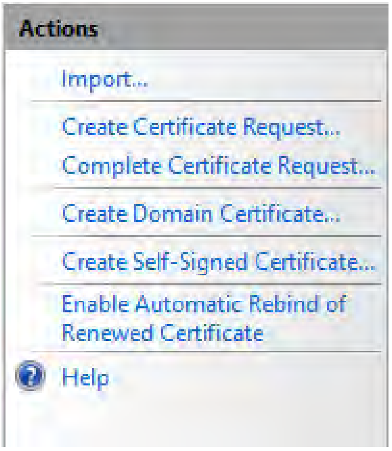
6. In the Server Certificates window, you will see any certificates that already exist.


Internet Information Services (IIS) Manager
SHAREPOINT
File View Help
Connections
Start Page
SHAREPOINT (SHAREPOINT\Admini
Application Pools
Sites
Server Certificates
Filter: Go Show All Group by: No Grouping
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready

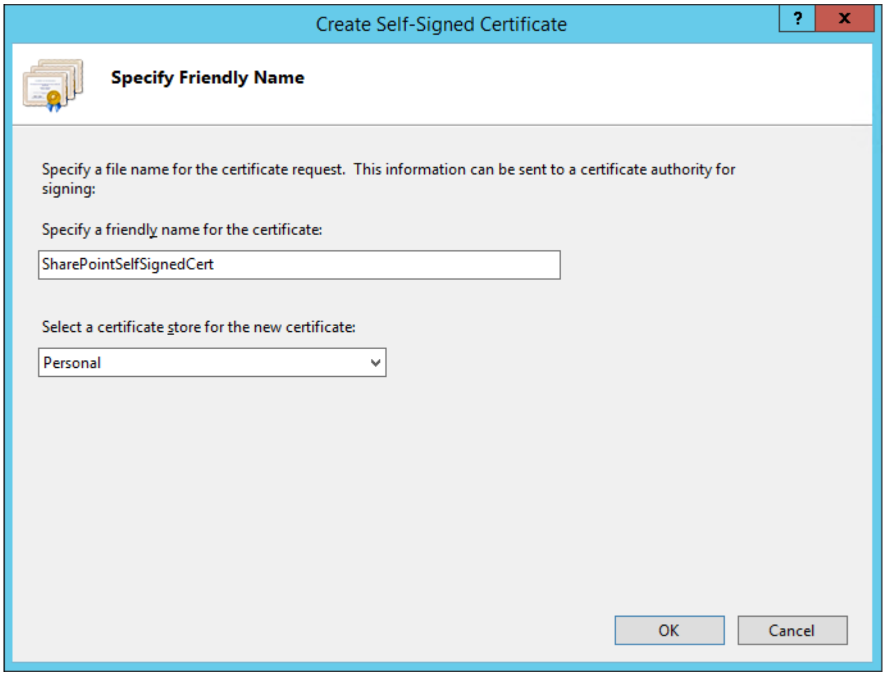
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By
	ForefrontIdentityManager	ForefrontIdentityMana
sharepoint.abac.test	Sharepoint.ABAC.TEST	Sharepoint.ABAC.TES

7. In the Actions panel on the right side of the IIS Manager window, next to the Server Certificates window, click on **Create Self-Signed Certificate**.


Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

8. 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**.



Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

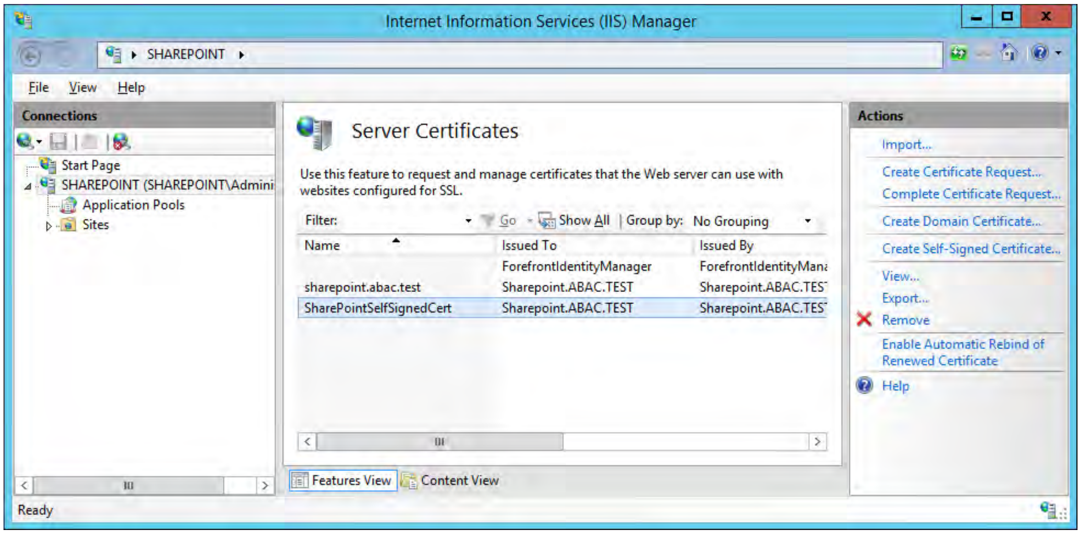
Specify a friendly name for the certificate: SharePointSelfSignedCert

Select a certificate store for the new certificate: Personal

4.4.1.2 Importing Self-Signed Certificate to SharePoint Certificate Store

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

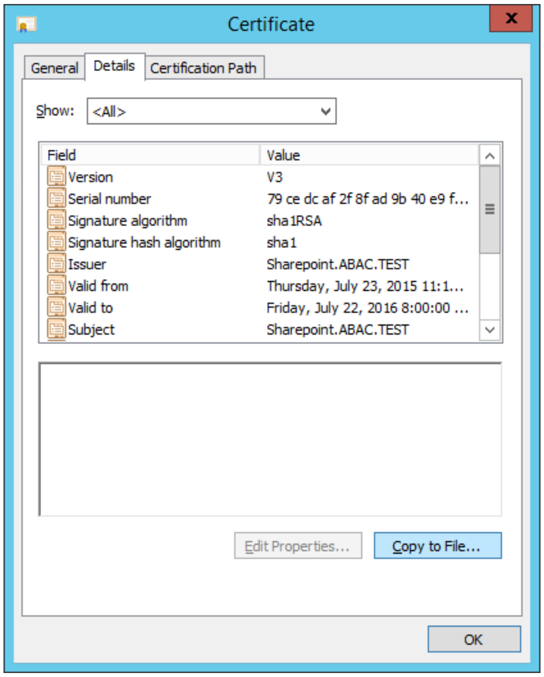
2. Double-click on the new certificate.


Internet Information Services (IIS) Manager
SHAREPOINT
File
View
Help
Connections
Start Page
SHAREPOINT (SHAREPOINT\Admini
Application Pools
Sites
Server Certificates
Filter:
Go
Show All
Group by:
No Grouping
Features View
Content View
Ready
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By
	ForefrontIdentityManager	ForefrontIdentityMana
sharepoint.abac.test	Sharepoint.ABAC.TEST	Sharepoint.ABAC.TES
SharePointSelfSignedCert	Sharepoint.ABAC.TEST	Sharepoint.ABAC.TES

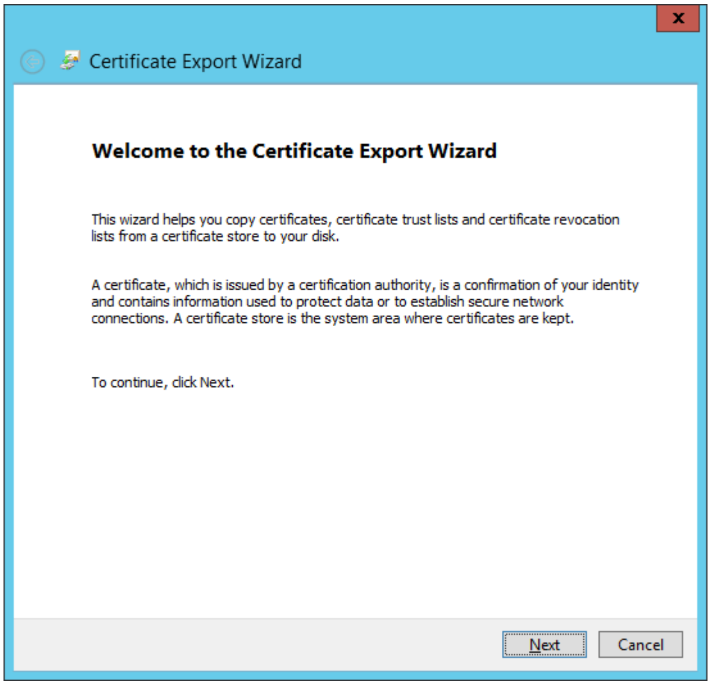
3. In the **Details** tab of the Certificate window, click on **Copy to File**.



Show: <All>

Field	Value
Version	V3
Serial number	79 ce dc af 2f 8f ad 9b 40 e9 f...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Sharepoint.ABAC.TEST
Valid from	Thursday, July 23, 2015 11:1...
Valid to	Friday, July 22, 2016 8:00:00 ...
Subject	Sharepoint.ABAC.TEST

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



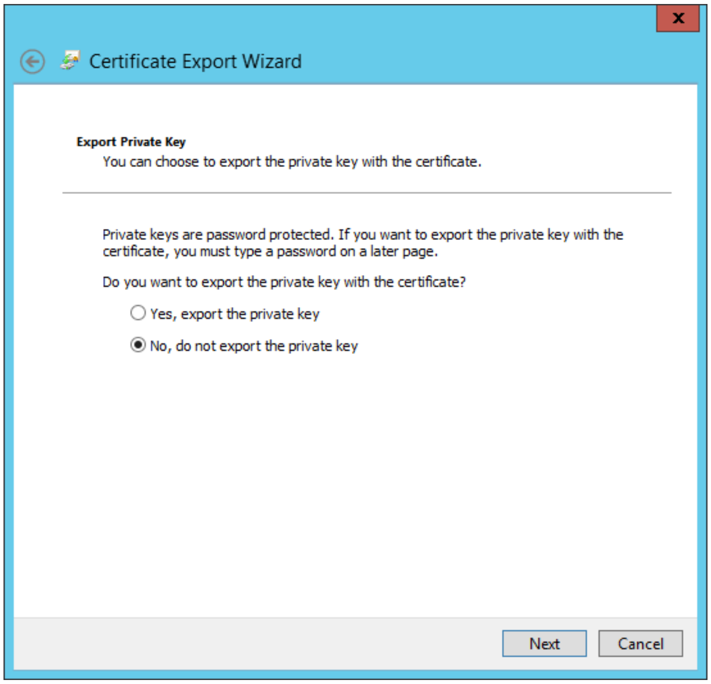
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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**.



Export Private Key

You can choose to export the private key with the certificate.

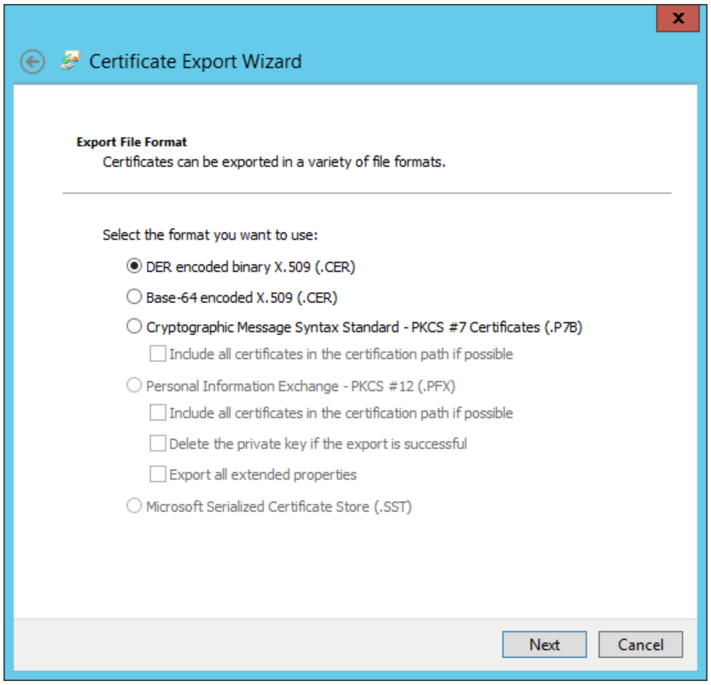
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

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**.



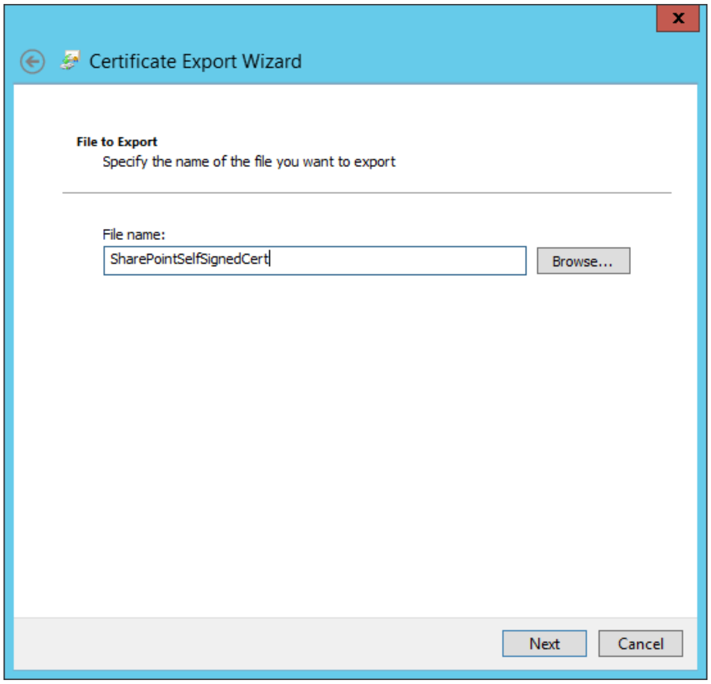
Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  □ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
  □ Include all certificates in the certification path if possible
  □ Delete the private key if the export is successful
  □ Export all extended properties
○ Microsoft Serialized Certificate Store (.SST)

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

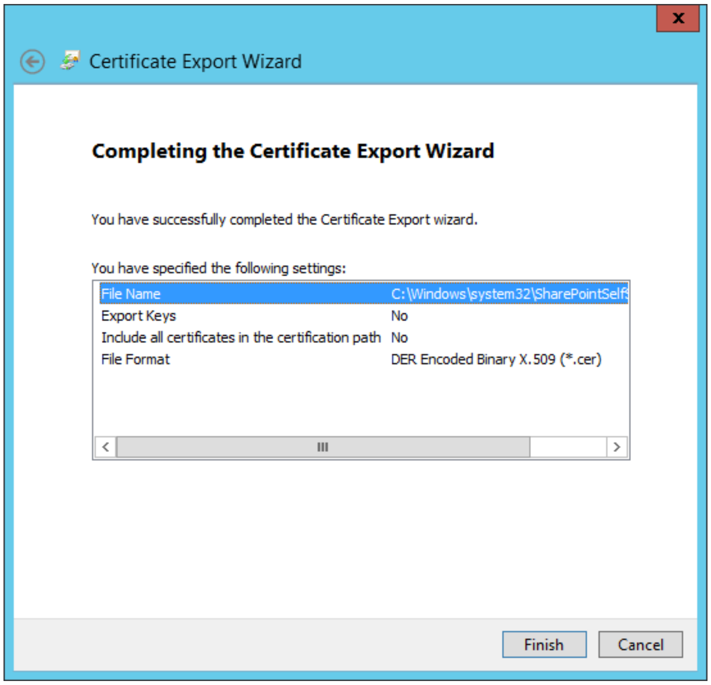


Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name: SharePointSelfSignedCert

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



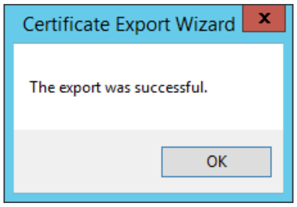
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Windows\system32\SharePointSelf
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Encoded Binary X.509 (*.cer)

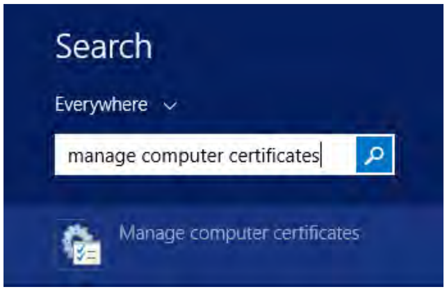
9. In another Certificate Export Wizard window that automatically opens, you will see that the export was successful. Click **OK**.



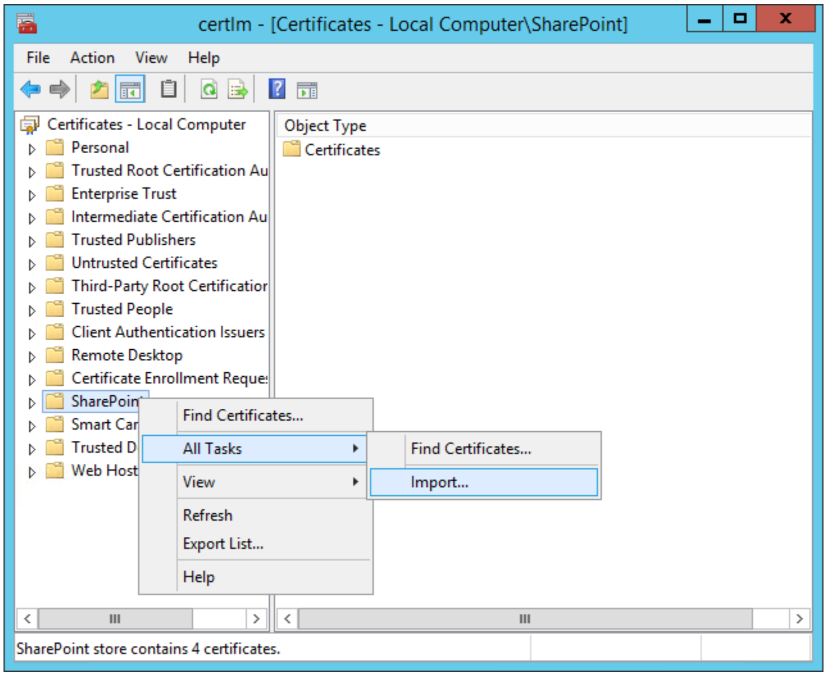
The export was successful.

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

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

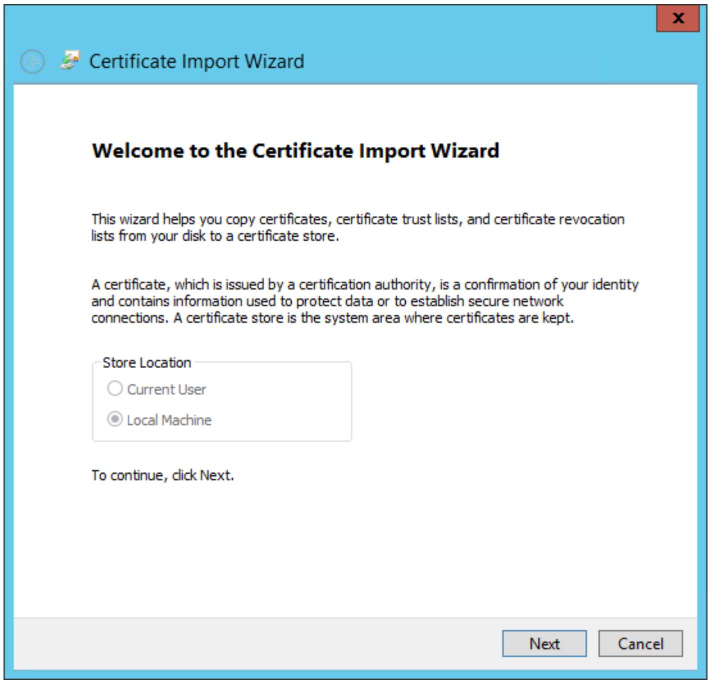


4. In the certlm window, right-click on the **SharePoint** node, hover over **All Tasks**, then click **Import**.



SharePoint store contains 4 certificates.

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



Welcome to the Certificate Import Wizard

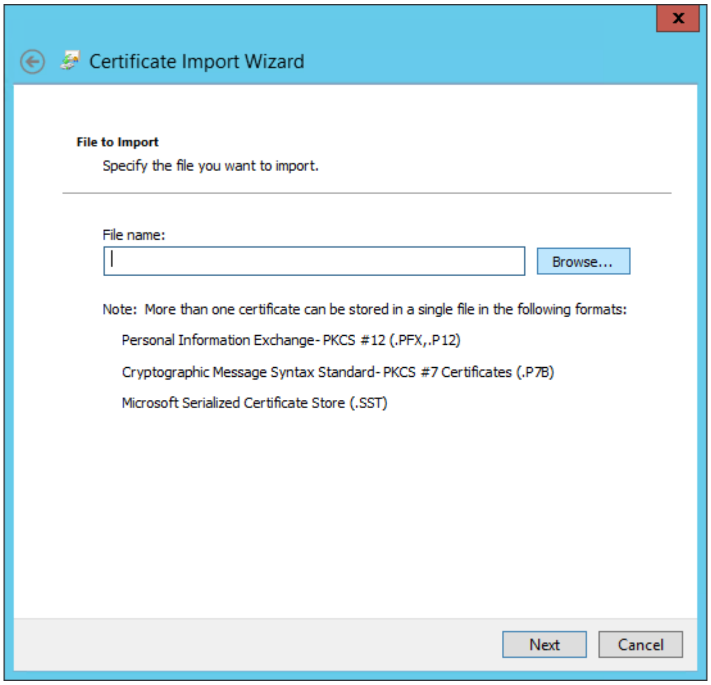
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

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.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

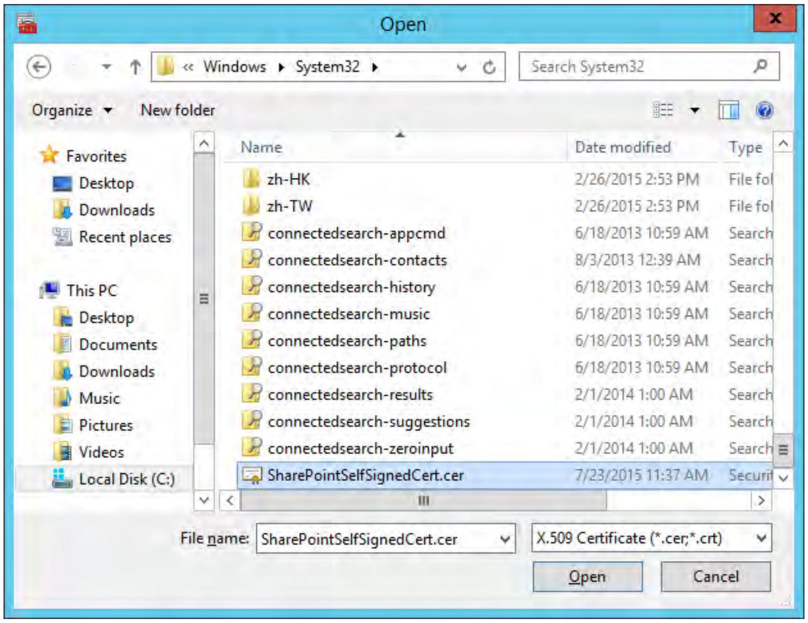
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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**.



Open

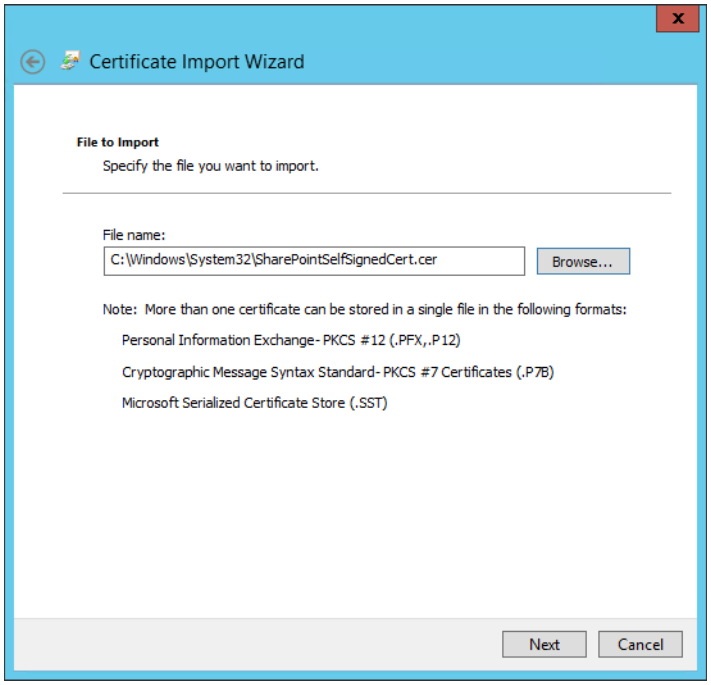
Windows ▸ System32 ▸

Name	Date modified	Type
zh-HK	2/26/2015 2:53 PM	File fol
zh-TW	2/26/2015 2:53 PM	File fol
connectedsearch-appcmd	6/18/2013 10:59 AM	Search
connectedsearch-contacts	8/3/2013 12:39 AM	Search
connectedsearch-history	6/18/2013 10:59 AM	Search
connectedsearch-music	6/18/2013 10:59 AM	Search
connectedsearch-paths	6/18/2013 10:59 AM	Search
connectedsearch-protocol	6/18/2013 10:59 AM	Search
connectedsearch-results	2/1/2014 1:00 AM	Search
connectedsearch-suggestions	2/1/2014 1:00 AM	Search
connectedsearch-zeroinput	2/1/2014 1:00 AM	Search
SharePointSelfSignedCert.cer	7/23/2015 11:37 AM	Securi

File name: SharePointSelfSignedCert.cer

X.509 Certificate (*.cer;*.crt)

9. 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**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Windows\System32\SharePointSelfSignedCert.cer

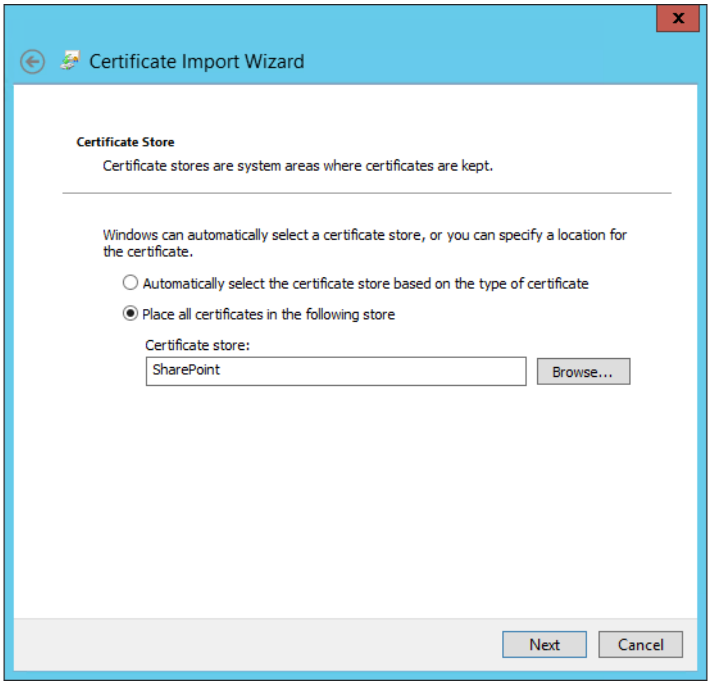
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

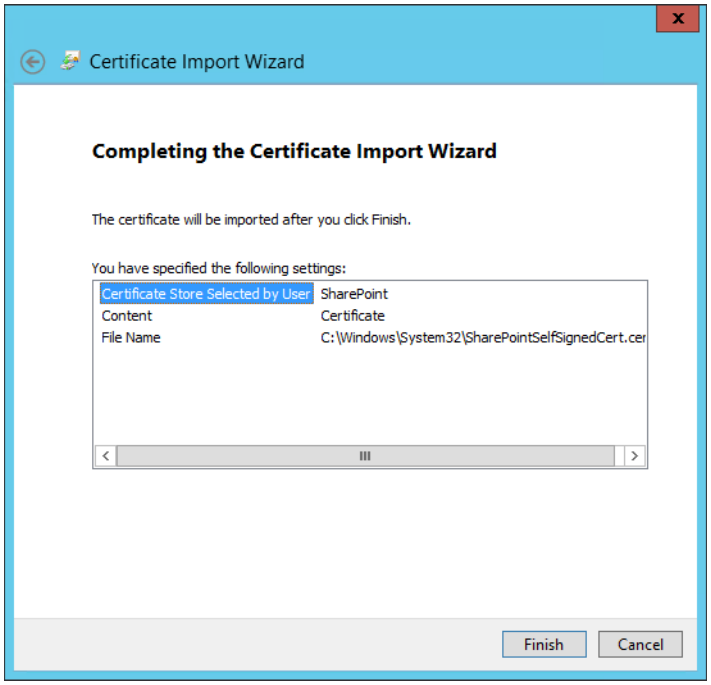
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

SharePoint

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



Certificate Import Wizard

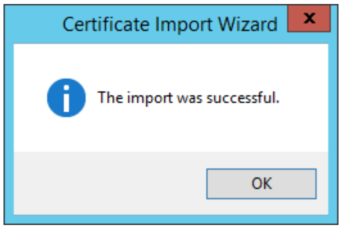
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	SharePoint
Content	Certificate
File Name	C:\Windows\System32\SharePointSelfSignedCert.cer

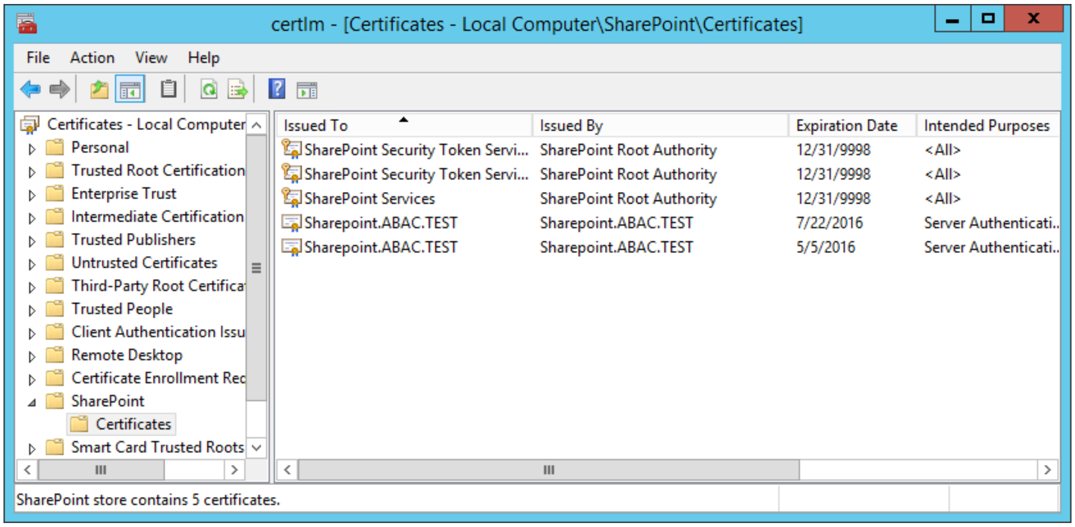
12. In the Certificate Import Wizard window that automatically opens, you will see a message that the import was successful. Click **OK**.



Certificate Import Wizard

The import was successful.

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

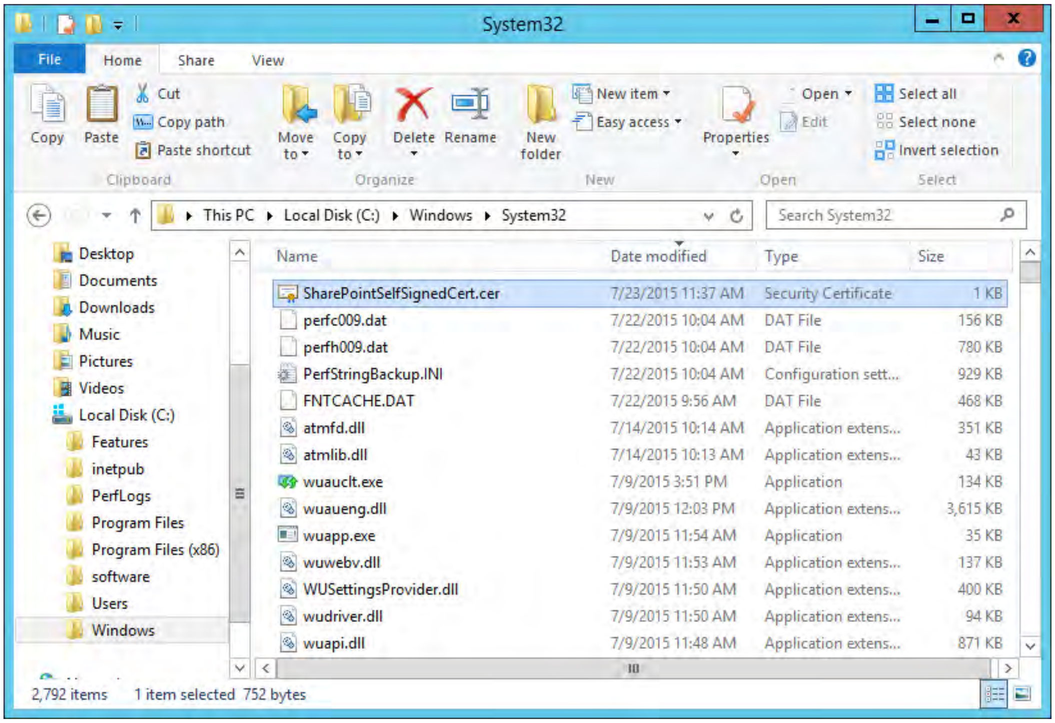


certlm - [Certificates - Local Computer\SharePoint\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certifica
Trusted People
Client Authentication Issu
Remote Desktop
Certificate Enrollment Rec
SharePoint
Certificates
Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes
SharePoint Security Token Servi...	SharePoint Root Authority	12/31/9998	<All>
SharePoint Security Token Servi...	SharePoint Root Authority	12/31/9998	<All>
SharePoint Services	SharePoint Root Authority	12/31/9998	<All>
Sharepoint.ABAC.TEST	Sharepoint.ABAC.TEST	7/22/2016	Server Authenticati...
Sharepoint.ABAC.TEST	Sharepoint.ABAC.TEST	5/5/2016	Server Authenticati...

SharePoint store contains 5 certificates.

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



Name	Date modified	Type	Size
SharePointSelfSignedCert.cer	7/23/2015 11:37 AM	Security Certificate	1 KB
perfc009.dat	7/22/2015 10:04 AM	DAT File	156 KB
perfh009.dat	7/22/2015 10:04 AM	DAT File	780 KB
PerfStringBackup.INI	7/22/2015 10:04 AM	Configuration sett...	929 KB
FNTCACHE.DAT	7/22/2015 9:56 AM	DAT File	468 KB
atmfd.dll	7/14/2015 10:14 AM	Application extens...	351 KB
atmlib.dll	7/14/2015 10:13 AM	Application extens...	43 KB
wuauclt.exe	7/9/2015 3:51 PM	Application	134 KB
wuaueng.dll	7/9/2015 12:03 PM	Application extens...	3,615 KB
wuapp.exe	7/9/2015 11:54 AM	Application	35 KB
wuwebv.dll	7/9/2015 11:53 AM	Application extens...	137 KB
WUSettingsProvider.dll	7/9/2015 11:50 AM	Application extens...	400 KB
wudriver.dll	7/9/2015 11:50 AM	Application extens...	94 KB
wuapi.dll	7/9/2015 11:48 AM	Application extens...	871 KB

2,792 items 1 item selected 752 bytes

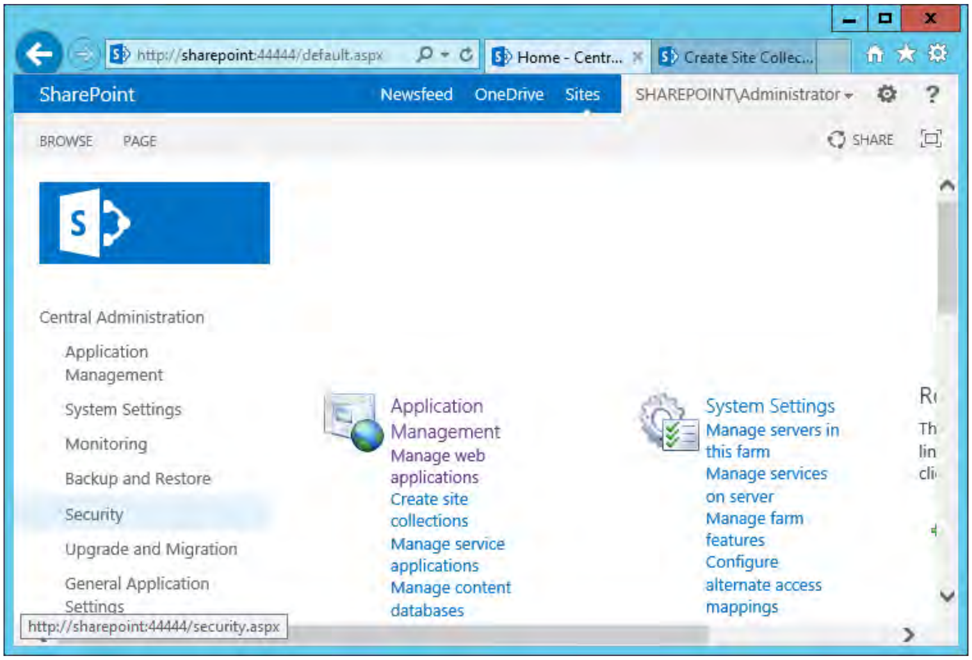
15. Right-click on the **self-signed certificate** and click on **Copy** or left-click on the self-signed certificate and press the keys Ctrl+C.

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.

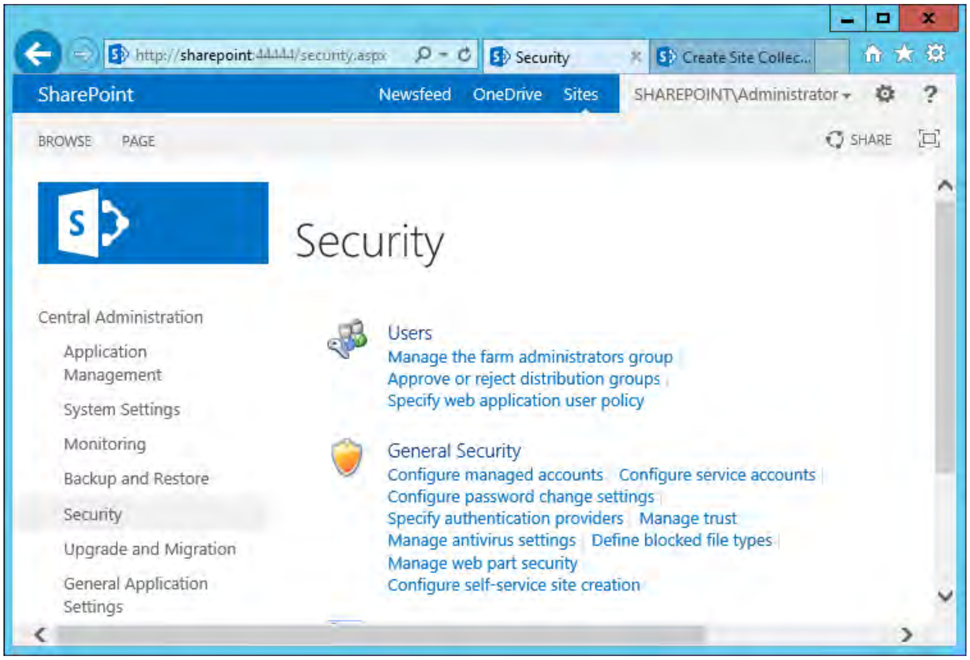
17. To Manage Trust via Central Administration, do the following steps: Open a **browser**.

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

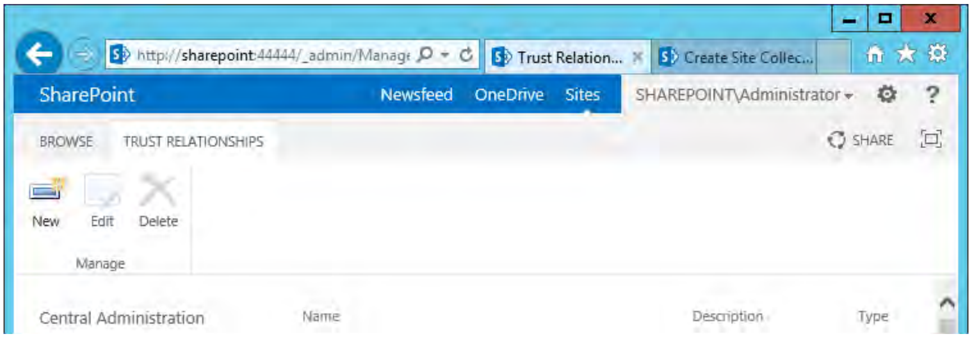
19. From the Central Administration page, click on **Security** in the left-hand menu.



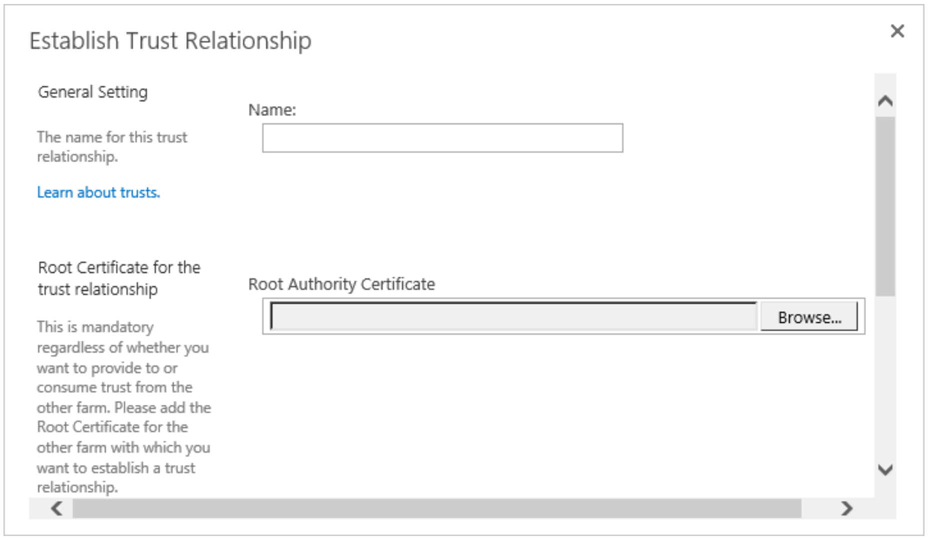
20. From the Security page, under the General Security section, click on **Manage Trust**.


http://sharepoint:44444/security.aspx
Security
Create Site Collec...
SharePoint
Newsfeed
OneDrive
Sites
SHAREPOINT\Administrator
BROWSE
PAGE
SHARE
Security
Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Users
Manage the farm administrators group
Approve or reject distribution groups
Specify web application user policy
General Security
Configure managed accounts
Configure service accounts
Configure password change settings
Specify authentication providers
Manage trust
Manage antivirus settings
Define blocked file types
Manage web part security
Configure self-service site creation

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



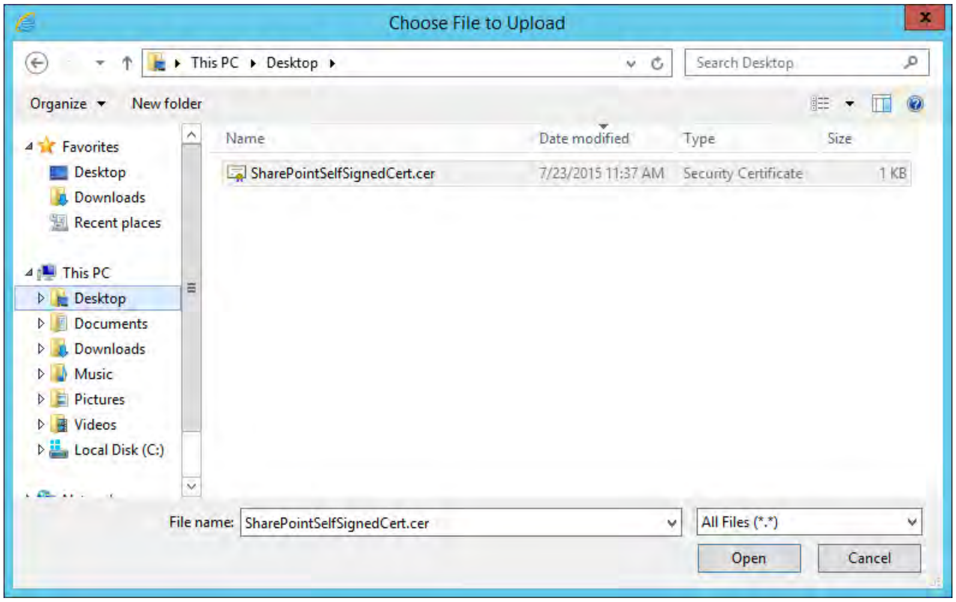
22. In the Establish Trust Relationship window that opens automatically, enter the **Name** for the trust relationship being created, then click **Browse** to find the certificate created in previous sub-sections.


Establish Trust Relationship
General Setting
Name:
Learn about trusts.
Root Certificate for the trust relationship
Root Authority Certificate
Browse...

The name for this trust relationship.

This is mandatory regardless of whether you want to provide to or consume trust from the other farm. Please add the Root Certificate for the other farm with which you want to establish a trust relationship.

23. In the Choose File to Upload window that opens automatically, navigate to the copy of your certificate from section 4.4.1.3 (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**.

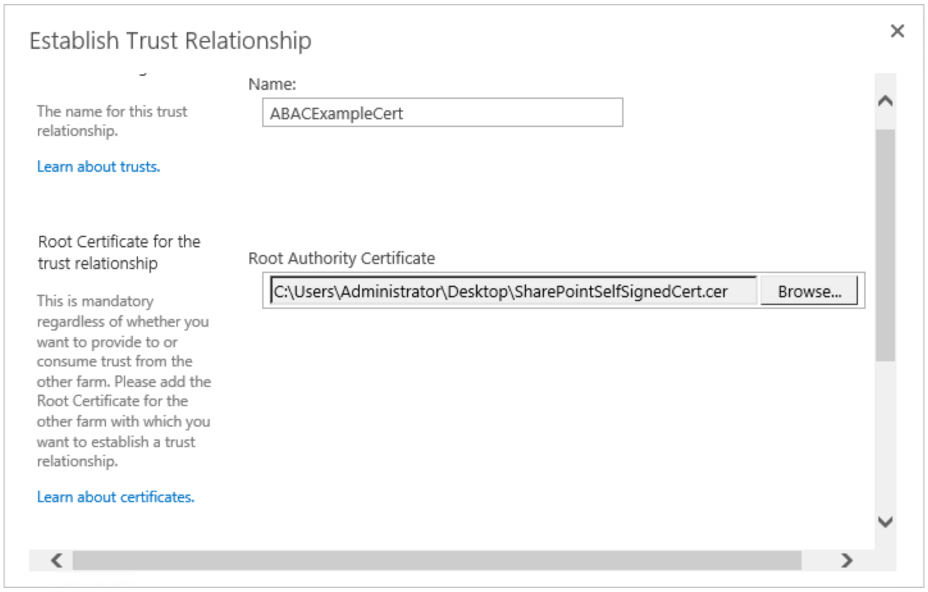


SharePointSelfSignedCert.cer 7/23/2015 11:37 AM Security Certificate 1 KB

File name: SharePointSelfSignedCert.cer

All Files (*.*)

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



The name for this trust relationship.

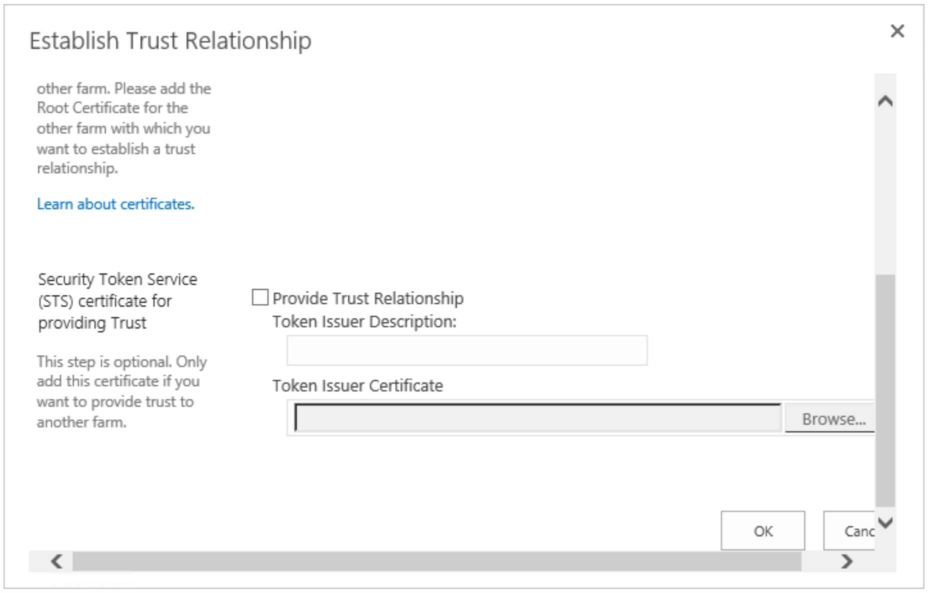
Name: ABACExampleCert

Root Certificate for the trust relationship

This is mandatory regardless of whether you want to provide to or consume trust from the other farm. Please add the Root Certificate for the other farm with which you want to establish a trust relationship.

Root Authority Certificate: C:\Users\Administrator\Desktop\SharePointSelfSignedCert.cer

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



Establish Trust Relationship

other farm. Please add the Root Certificate for the other farm with which you want to establish a trust relationship.

Learn about certificates.

Security Token Service (STS) certificate for providing Trust

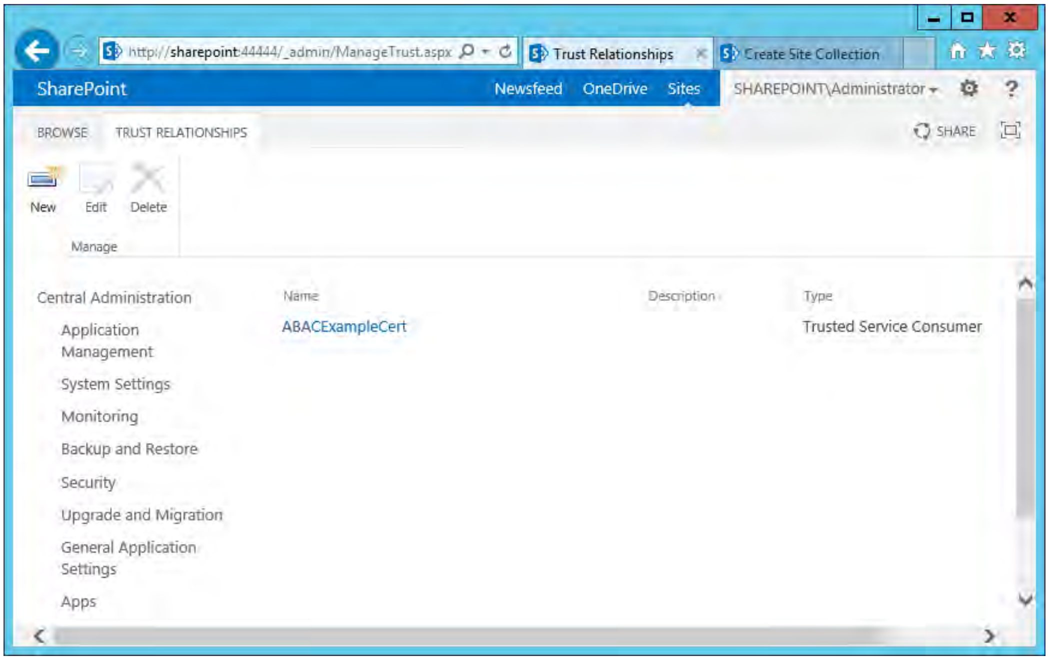
This step is optional. Only add this certificate if you want to provide trust to another farm.

☐ Provide Trust Relationship

Token Issuer Description:

Token Issuer Certificate

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



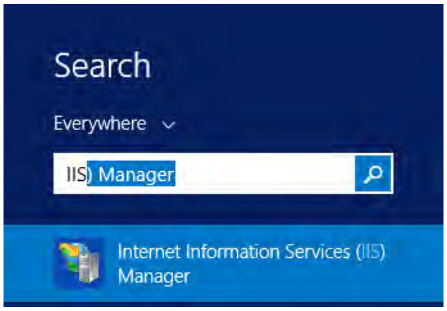
Name	Description	Type
ABACExampleCert		Trusted Service Consumer

4.4.1.4 Configure IIS Binding for the Self-Signed Certificate

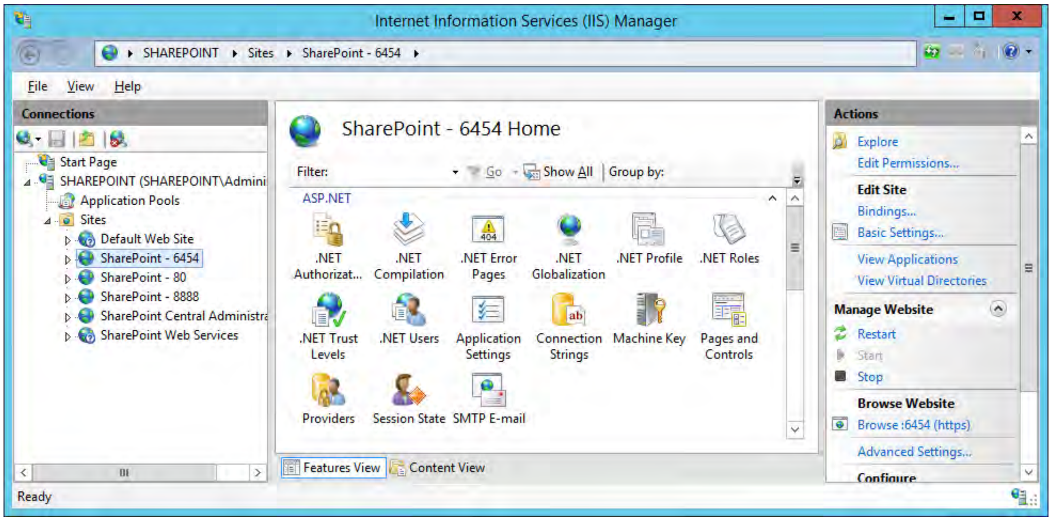
1. Click on the **Windows** icon in the bottom left corner of your screen.

2. Begin typing **`IIS`**.

3. When the Internet **Information Services (IIS) Manager** appears, click on it.



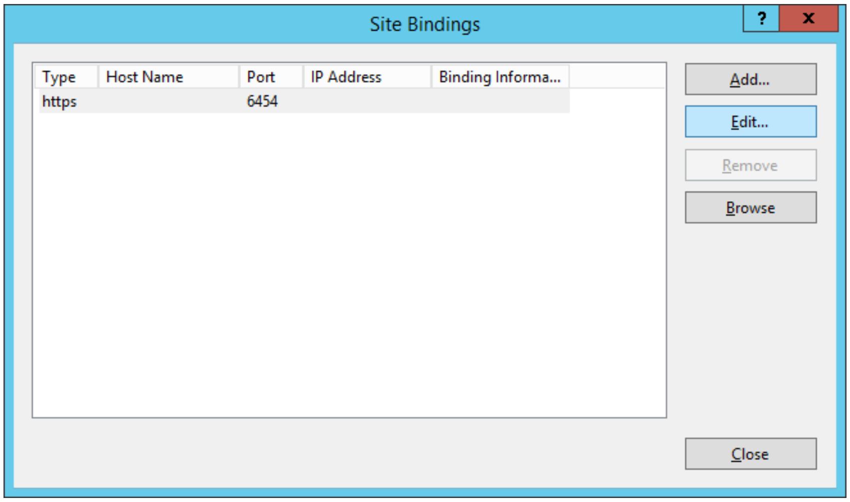
4. On the left-hand side of the IIS Manager window, click on the **SharePoint web application** created in previous steps, then click **Bindings** in the Actions pane on the right.



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

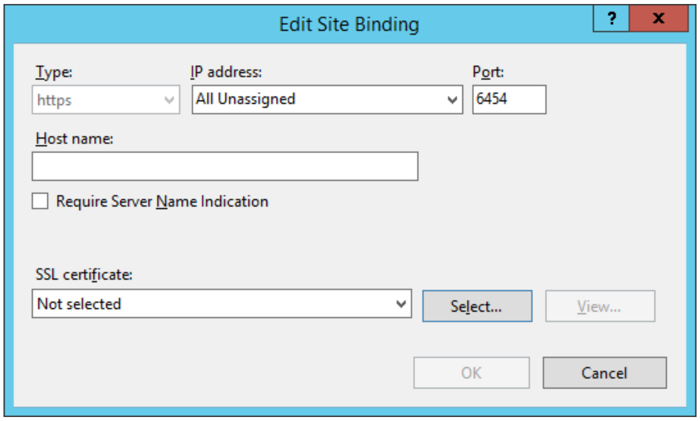
   a. If a binding type of https does not exist, click on **Add**.

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



Type	Host Name	Port	IP Address	Binding Informa...
https		6454		

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



Type: https

IP address: All Unassigned

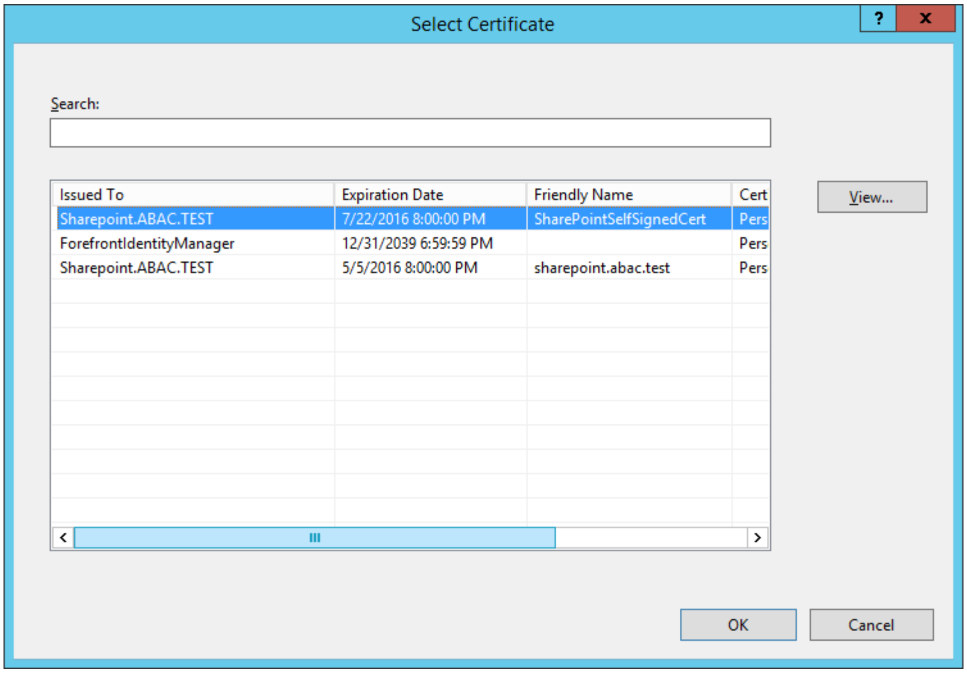
Port: 6454

Host name:

□ Require Server Name Indication

SSL certificate: Not selected

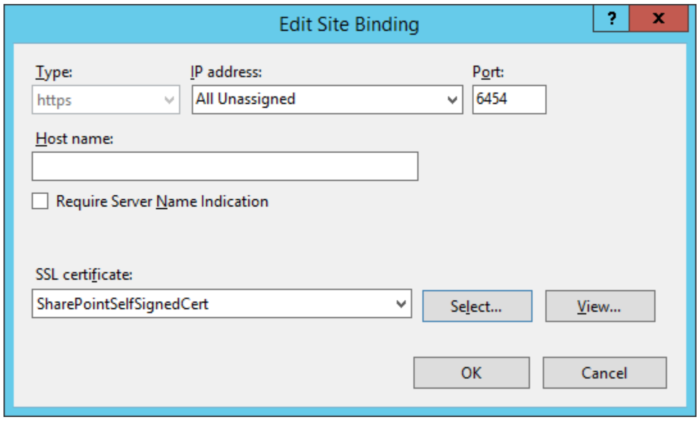
7. In the Select Certificate window, click on the certificate created in previous steps and click **OK**.



Search:

Issued To	Expiration Date	Friendly Name	Cert
Sharepoint.ABAC.TEST	7/22/2016 8:00:00 PM	SharePointSelfSignedCert	Pers
ForefrontIdentityManager	12/31/2039 6:59:59 PM		Pers
Sharepoint.ABAC.TEST	5/5/2016 8:00:00 PM	sharepoint.abac.test	Pers

8. In the Edit Site Binding window, verify that your SSL certificate is listed, then click **OK**.



Type: https

IP address: All Unassigned

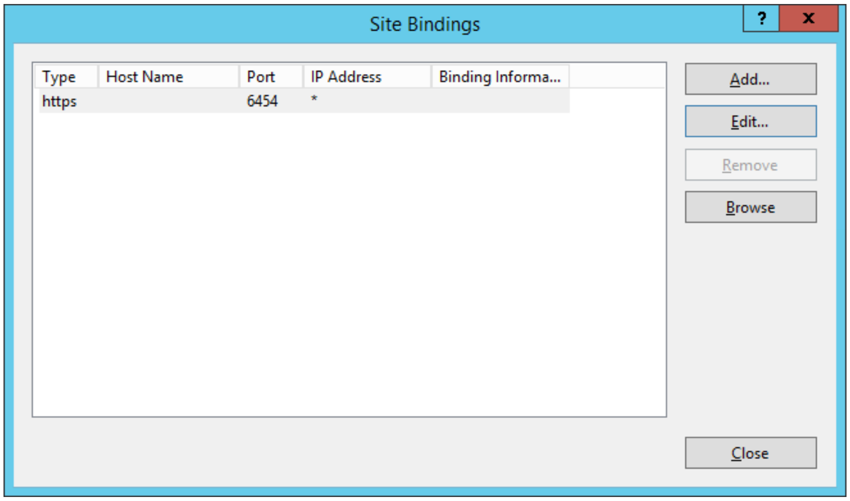
Port: 6454

Host name:

□ Require Server Name Indication

SSL certificate: SharePointSelfSignedCert

9. In the Site Bindings window, click **Close**.



Type	Host Name	Port	IP Address	Binding Informa...
https		6454	*	

4.4.2 Certificates Signed by Local or Online Certificate Authority

Instead of using self-signed certificates which can be used in protected lab environments, it is recommended that you use certificates signed by a Certificate Authority. For our build, we used Symantec's Managed PKI Service to sign our certificates using a local Certificate Authority. Certificates were used to support various exchanges that require encryption, such as digital signature, SAML message encryption, and encryption of TLS communications.

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

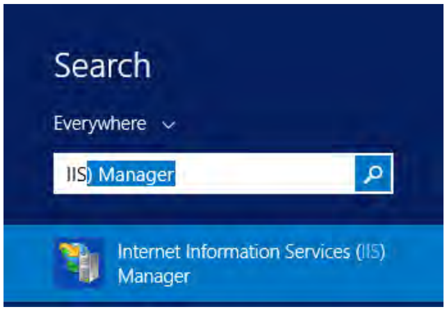
1. Using the vendor product (e.g., SharePoint), generate a certificate signing request on the server where you want to use the certificate. Save the signing request to a file.
2. Submit an enrollment request to your certificate authority. You will need to provide the signing request that was generated in step 1. This step is typically where you provide

information such as the name of the server on which you intend to use the certificate (e.g., "sharepoint.abac.test").

3. A representative at the certificate authority will examine the enrollment request and approve it. The representative will issue a certificate response signed with the certificate authority's key. You can download the signed response. If you are using a certificate authority that is locally managed by your organization, you will also need to download the public key of the certificate authority because you will need to add this to the Trusted Certificate Authorities on each server and client that will be using the certificates.
4. Go back to the vendor product where you created the certificate signing request. If you are using a local certificate authority, you will first need to add the certificate authority's public key to the list of Trusted Certificate Authorities.
5. Import the certificate file for your server that was signed by the certificate authority.

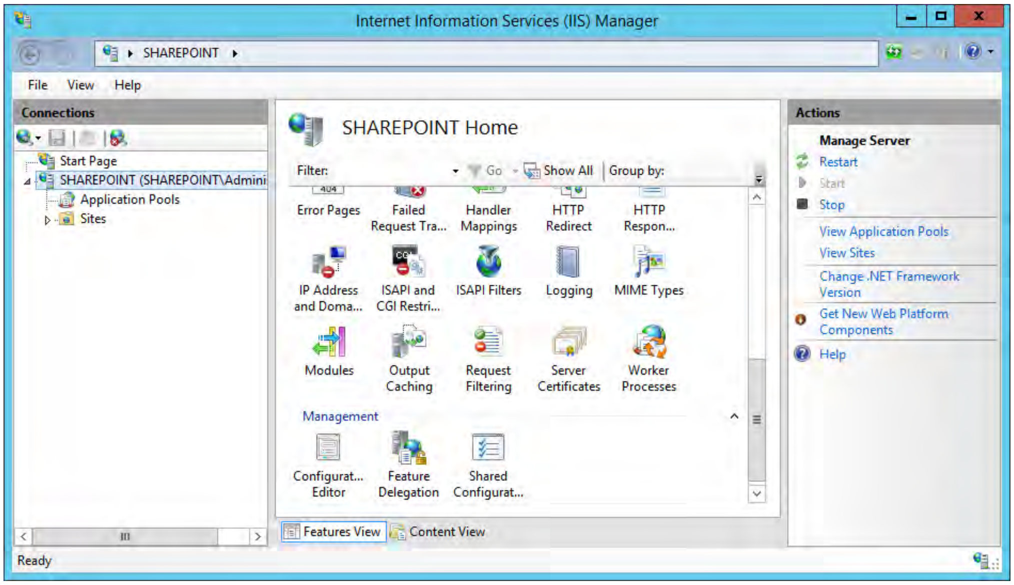
4.4.2.1 Generating a Certificate Signing Request (CSR)

1. Log into the server where SharePoint Server 2013 is installed (e.g., SharePoint Server in our build).
2. Click on the **Windows** icon in the bottom left corner of your screen.
3. Begin typing **`IIS`**.
4. When the **Internet Information Services (IIS) Manager** appears, click on it.

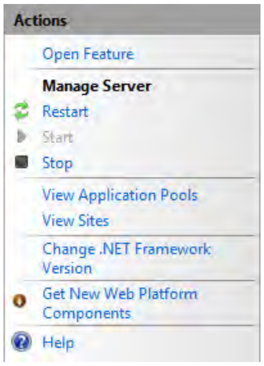


5. In the left-hand Connections column, left-click on your **SharePoint** instance.

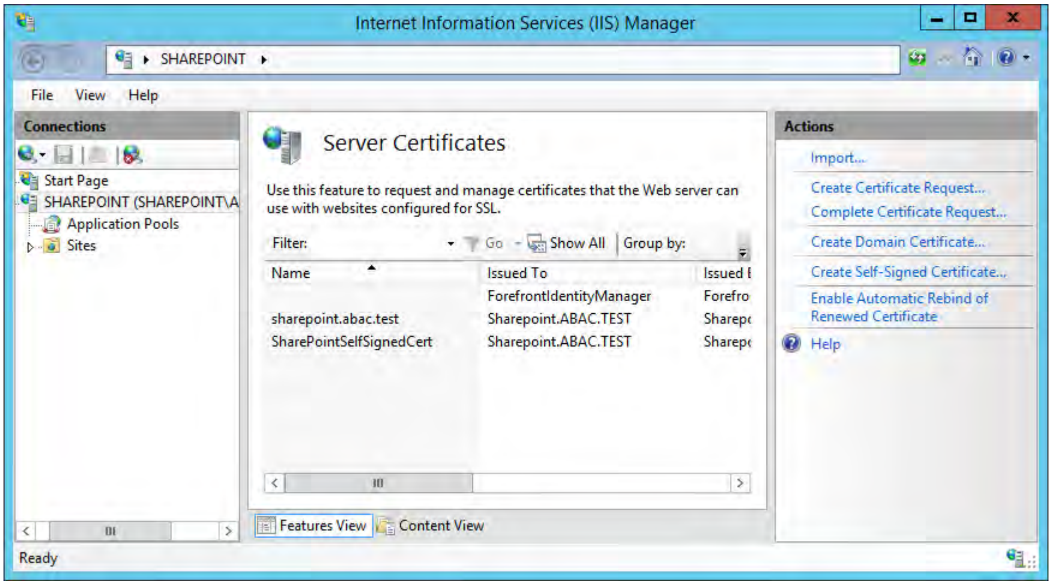
6. Scroll down in the SharePoint Home pane and left-click on **Server Certificates**.



7. In the right-hand Actions column, click on **Open Feature**.



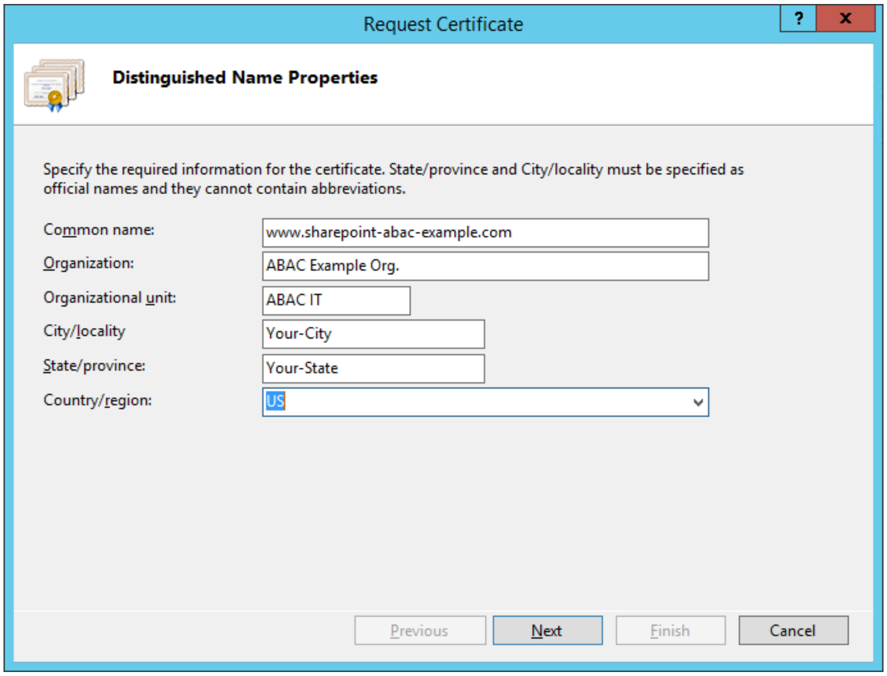
8. In the Server Certificates pane, in the right-hand Actions column, click on **Create Certificate Request**.


Internet Information Services (IIS) Manager
SHAREPOINT
File
View
Help
Connections
Start Page
SHAREPOINT (SHAREPOINT\A
Application Pools
Sites
Server Certificates
Filter:
Go
Show All
Group by:
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued [
	ForefrontIdentityManager	Forefro
sharepoint.abac.test	Sharepoint.ABAC.TEST	Sharepo
SharePointSelfSignedCert	Sharepoint.ABAC.TEST	Sharepo

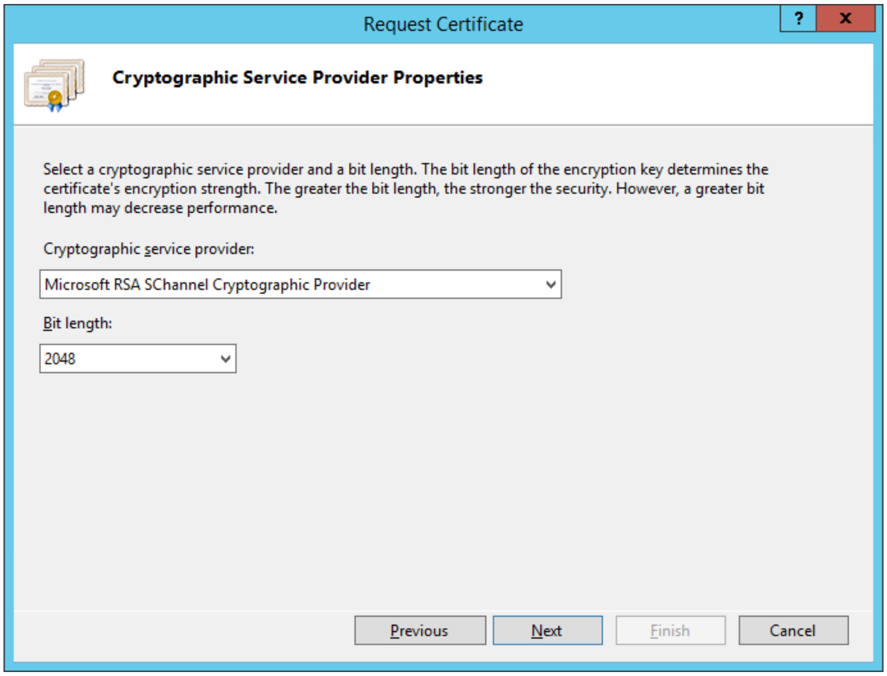
9. In the Distinguished Name Properties window that opens automatically, enter your organizational information and click **Next**.



Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	www.sharepoint-abac-example.com
Organization:	ABAC Example Org.
Organizational unit:	ABAC IT
City/locality	Your-City
State/province:	Your-State
Country/region:	US

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

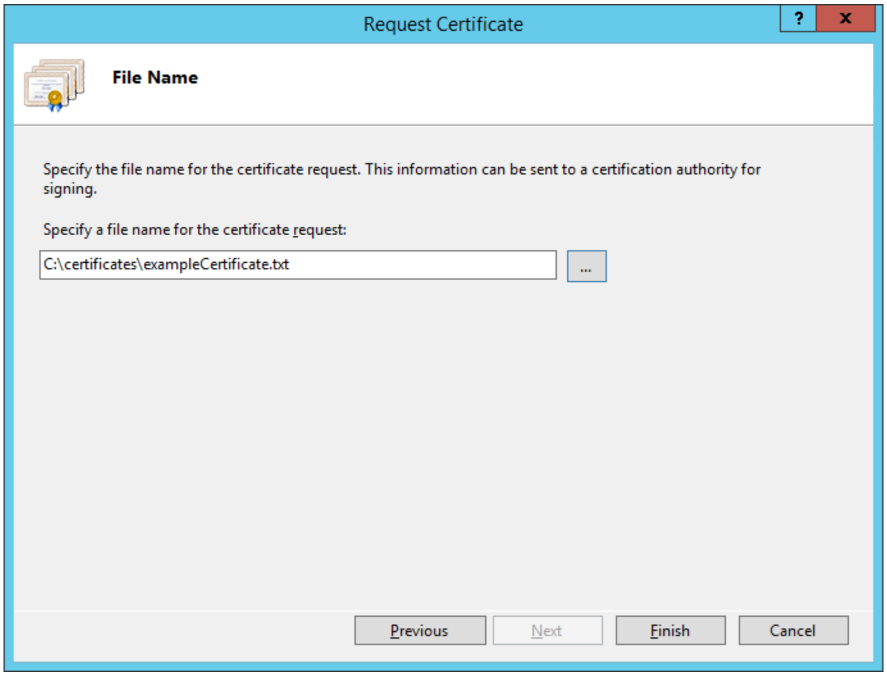


Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

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**.



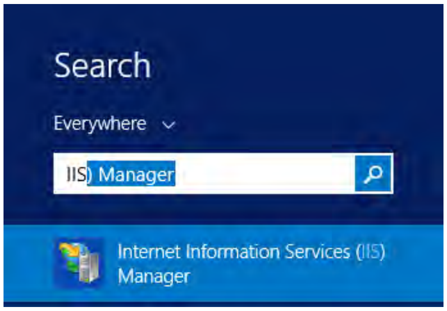
Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request: C:\certificates\exampleCertificate.txt

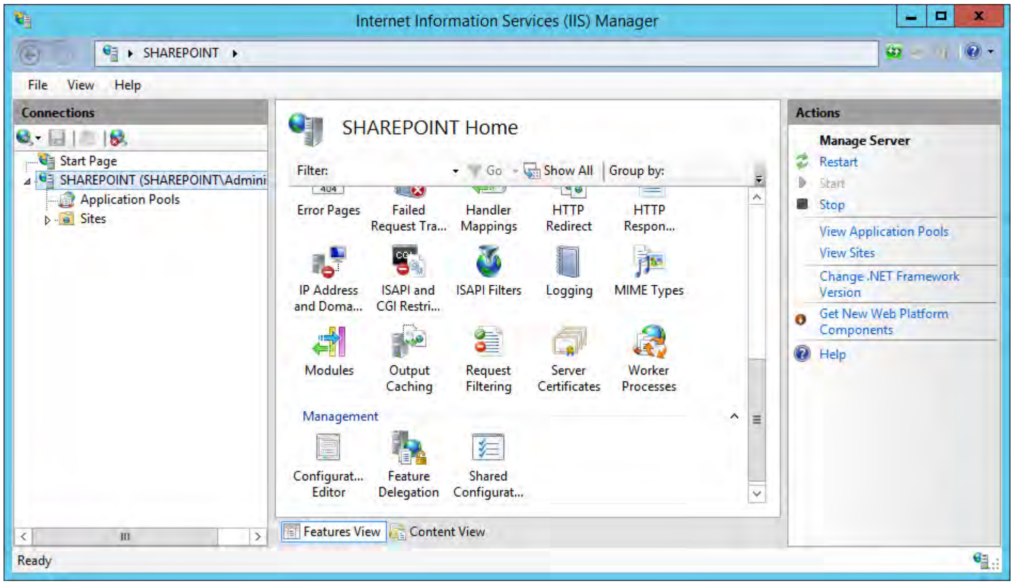
4.4.2.2 Installing the new signed SSL Certificate

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

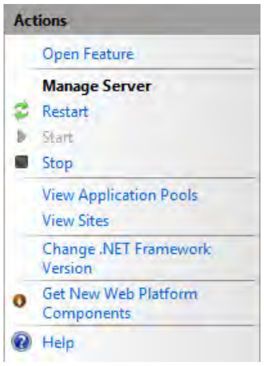
1. Log onto the SharePoint Server and save the SSL certificate resulting from the CSR in section 4.4.1.2.
2. Click on the **Windows** icon in the bottom left corner of your screen.
3. Begin typing **`IIS`**.
4. When the **Internet Information Services (IIS) Manager** appears, click on it.



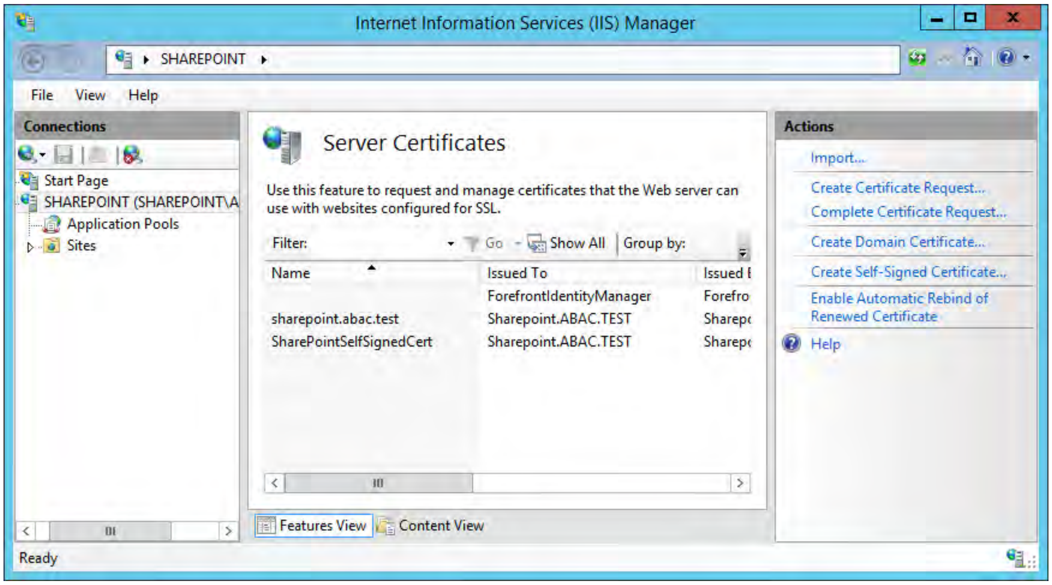
5. In the left-hand Connections column, left-click on your **SharePoint** instance.
6. Scroll down in the SharePoint Home pane and left-click on **Server Certificates**.



7. In the right-hand Actions column, click on **Open Feature**.



8. In the Server Certificates pane, in the right-hand Actions column, click on **Complete Certificate Request**.

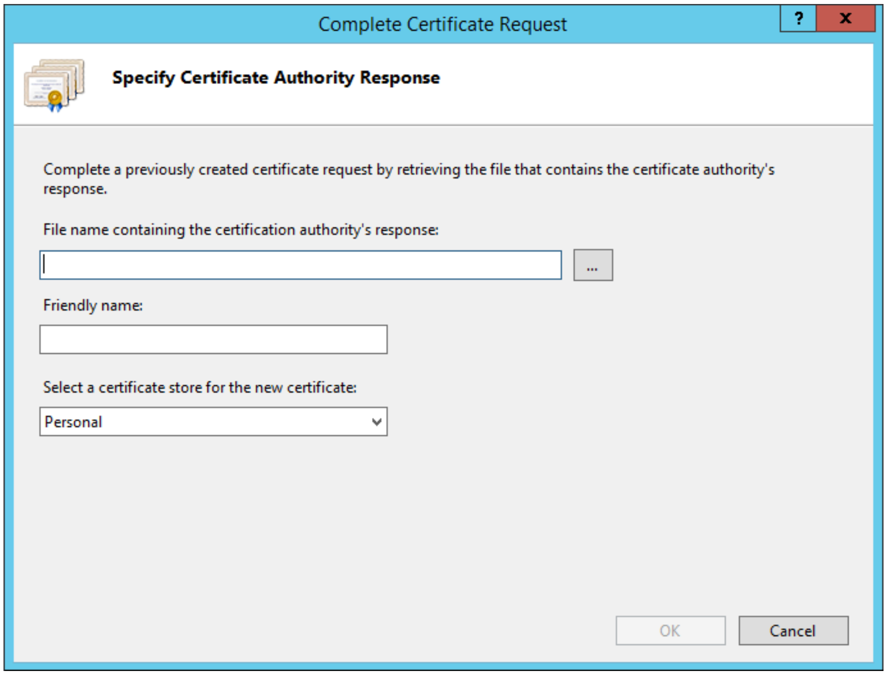

Internet Information Services (IIS) Manager
SHAREPOINT
File
View
Help
Connections
Start Page
SHAREPOINT (SHAREPOINT\A
Application Pools
Sites
Server Certificates
Filter:
Go
Show All
Group by:
Features View
Content View
Ready
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued I
	ForefrontIdentityManager	Forefro
sharepoint.abac.test	Sharepoint.ABAC.TEST	Sharepo
SharePointSelfSignedCert	Sharepoint.ABAC.TEST	Sharepo

9. 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**.


Complete Certificate Request
?
x
Specify Certificate Authority Response
...
OK
Cancel

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

Friendly name:

Select a certificate store for the new certificate:

Personal

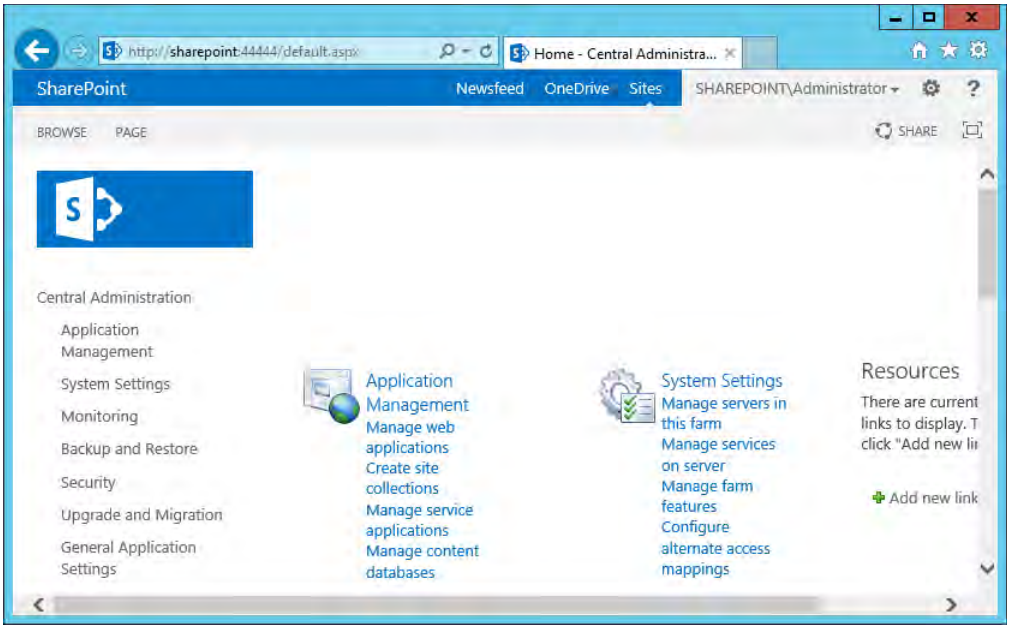
4.4.2.3 Configure the CA-Signed Certificate

Follow the steps listed in section 4.4.1.4 to configure IIS Binding for the new SSL certificate signed by a local or online Certificate Authority. You can choose port 443 or any other available port if you prefer to use a non-standard port for SSL traffic.

4.5 Creating a site collection

1. On the SharePoint Server, open a web browser.
2. In the **URL address bar** of the browser, enter the address for Central Administration and click Enter or Go: **http://sharepoint:44444/default.aspx**

3. From the Central Administration page, in the Application Management section, click on **Create site collections**.

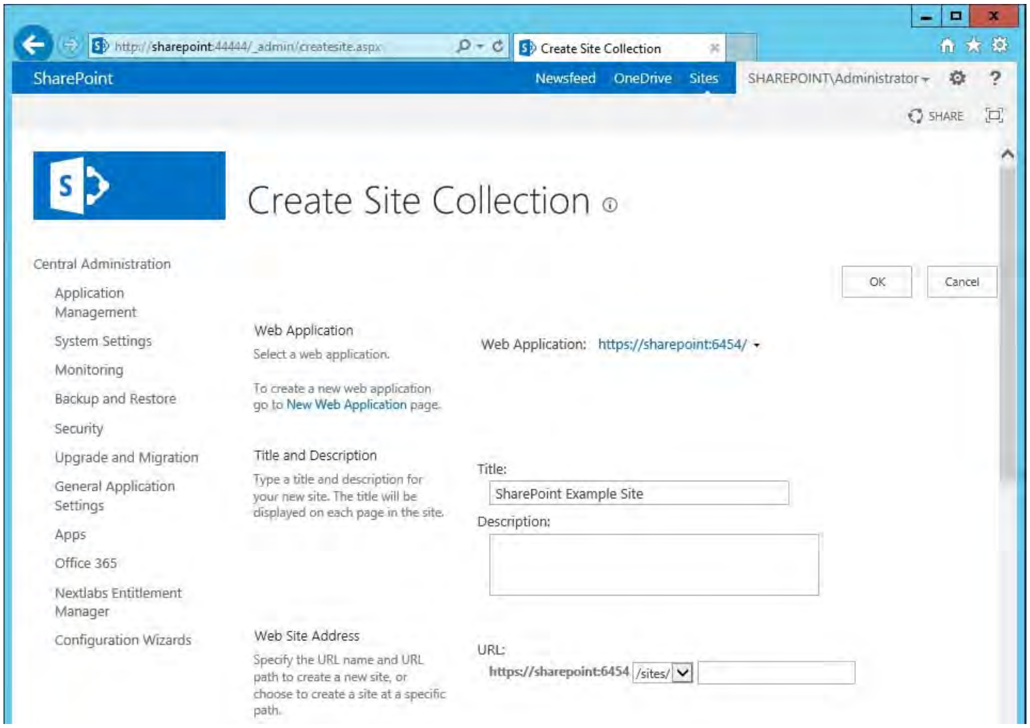


4. On the Create Site Collection page, do the following:

   a. Verify that the web application under consideration is the one chosen.

   b. Enter a **Title** (required) and **Description** (optional).

   c. Choose the web site address you prefer for your site (in this build, **https://sharepoint:6454/**).



Create Site Collection

Web Application

Select a web application.

To create a new web application go to New Web Application page.

Web Application: https://sharepoint:6454/

Title and Description

Type a title and description for your new site. The title will be displayed on each page in the site.

Title: SharePoint Example Site

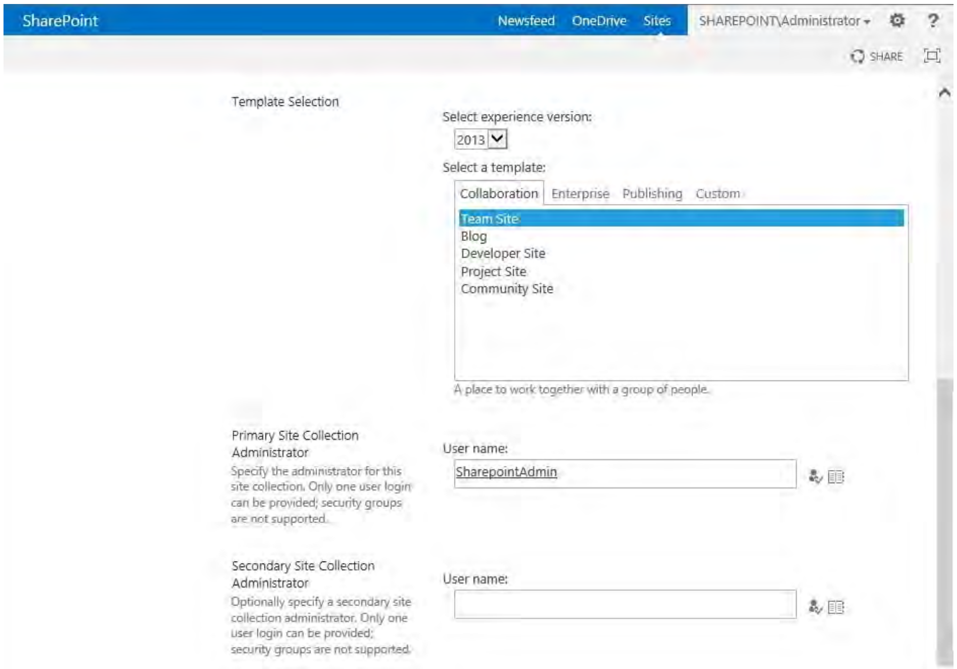
Description:

Web Site Address

Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.

URL: https://sharepoint:6454 /sites/

5. In the browser, scroll down to the Template Selection area and Primary Site Collection Administrator area of the Create Site Selection page and do the following:
    a. Choose the **version** and **template** (e.g., 2013 Team Site)
    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.
        i. Alternatively, you can look up users by name using the address book people picker mechanism next to the user name text field.
    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.
        i. Alternatively, you can look up users by name using the address book people picker mechanism next to the user name text field.



Template Selection

Select experience version: 2013

Select a template:

Team Site
Blog
Developer Site
Project Site
Community Site

A place to work together with a group of people.

Primary Site Collection Administrator

Specify the administrator for this site collection. Only one user login can be provided; security groups are not supported.

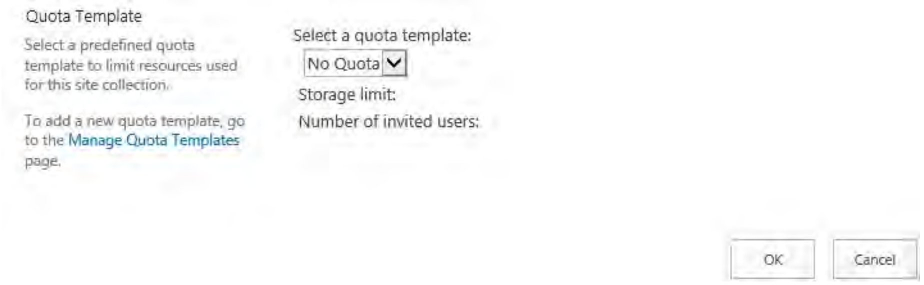
User name: SharepointAdmin

Secondary Site Collection Administrator

Optionally specify a secondary site collection administrator. Only one user login can be provided; security groups are not supported.

User name:

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**.



Quota Template

Select a predefined quota template to limit resources used for this site collection.

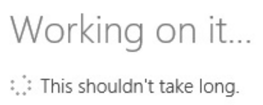
To add a new quota template, go to the Manage Quota Templates page.

Select a quota template: No Quota

Storage limit:

Number of invited users:

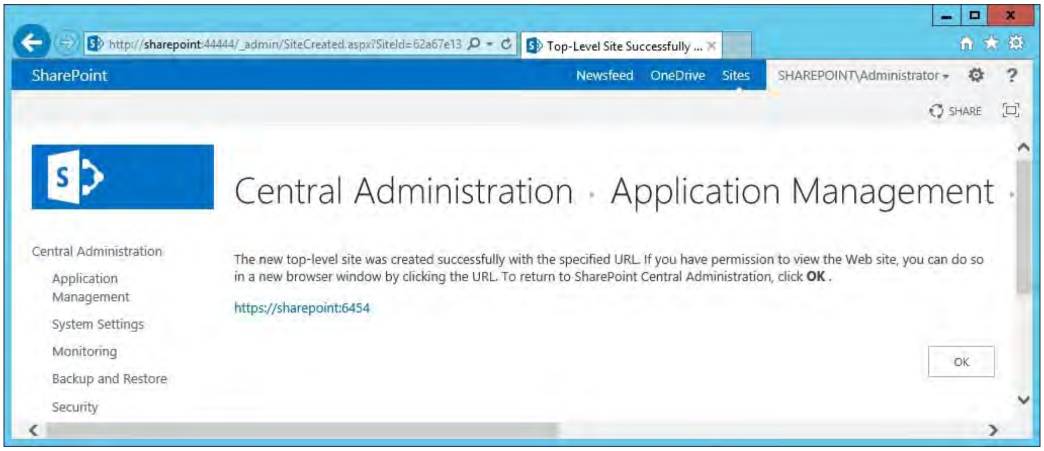
7. Wait for the Site Collection to successfully complete.



Working on it...

This shouldn't take long.

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

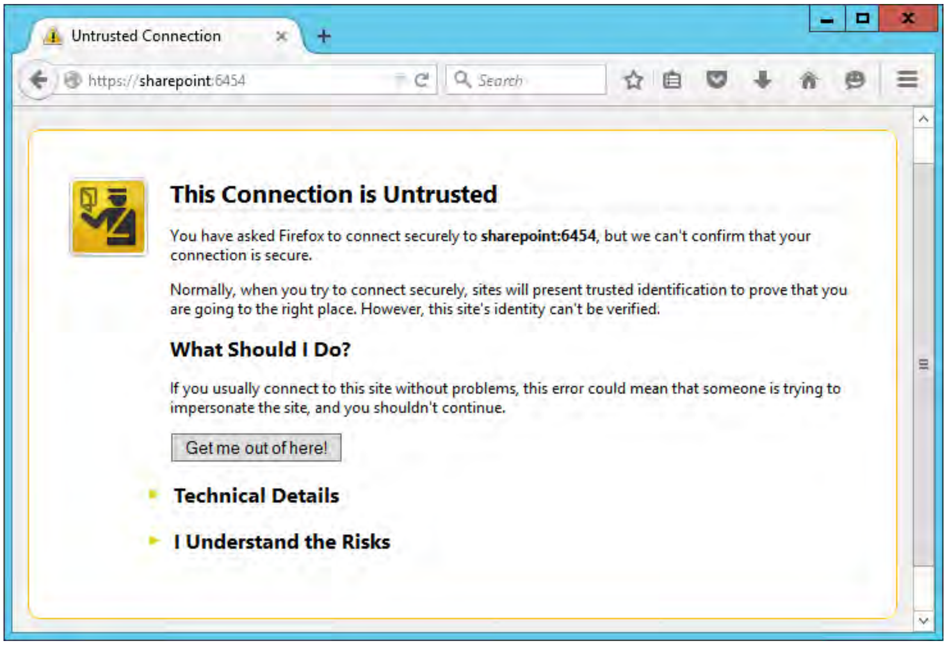


The new top-level site was created successfully with the specified URL. If you have permission to view the Web site, you can do so in a new browser window by clicking the URL. To return to SharePoint Central Administration, click **OK** .

https://sharepoint:6454

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.



This Connection is Untrusted

You have asked Firefox to connect securely to **sharepoint:6454**, but we can't confirm that your connection is secure.

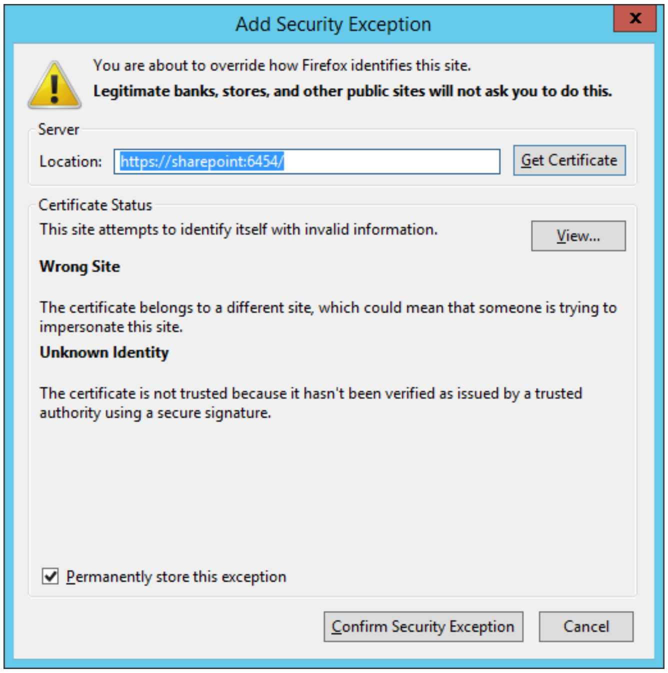
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

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**.



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://sharepoint:6454/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

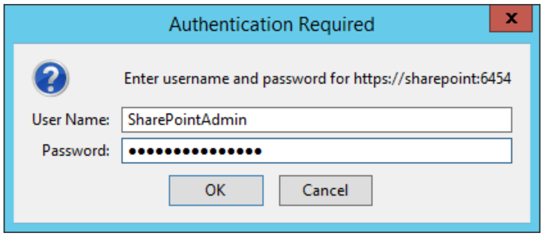
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☑ Permanently store this exception

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

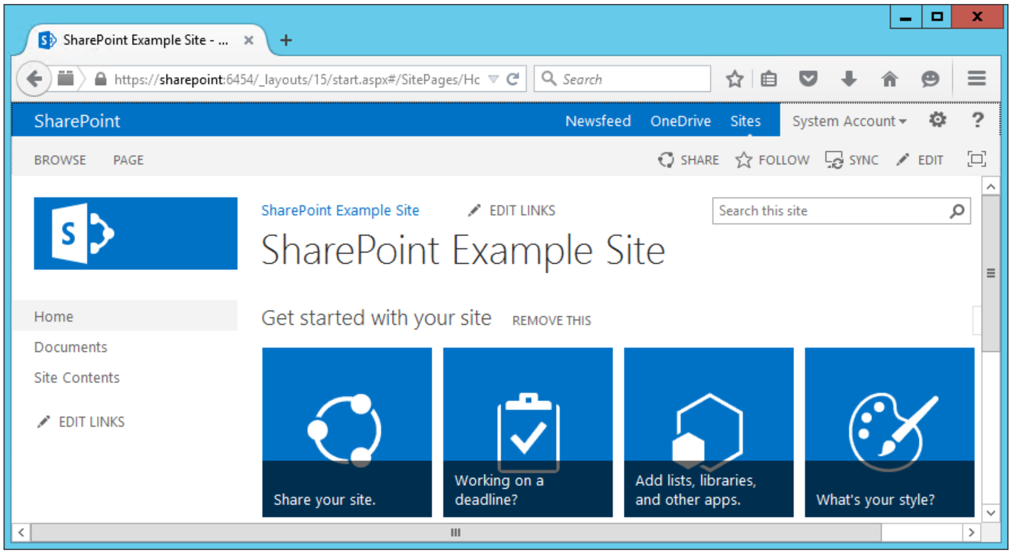


Enter username and password for https://sharepoint:6454

User Name: SharePointAdmin

Password: •••••••••••••••

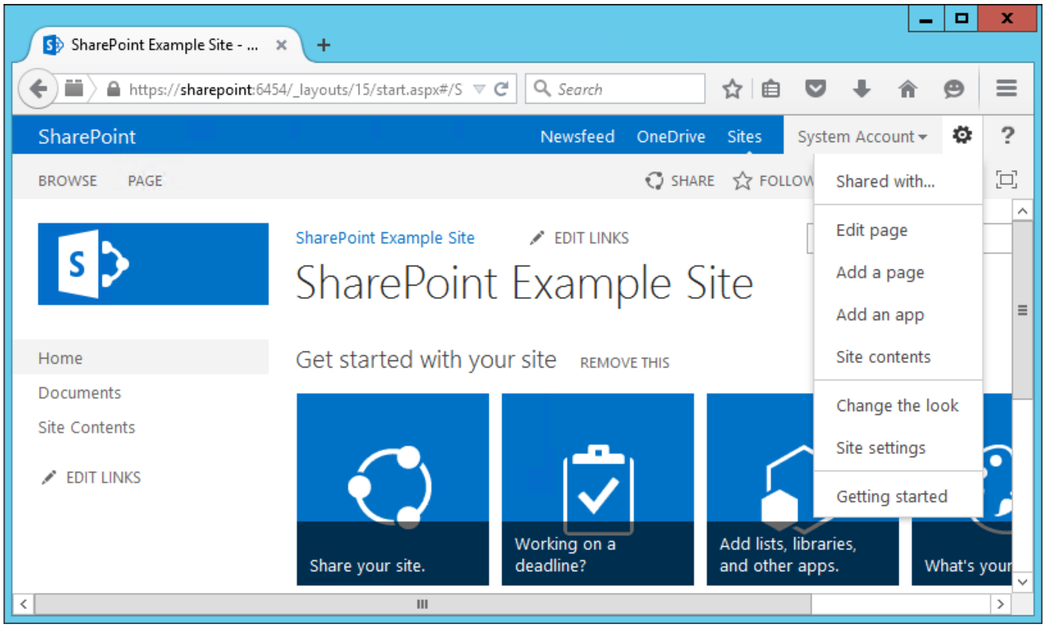
11. Upon verification that the login was a success, you will see default site contents.



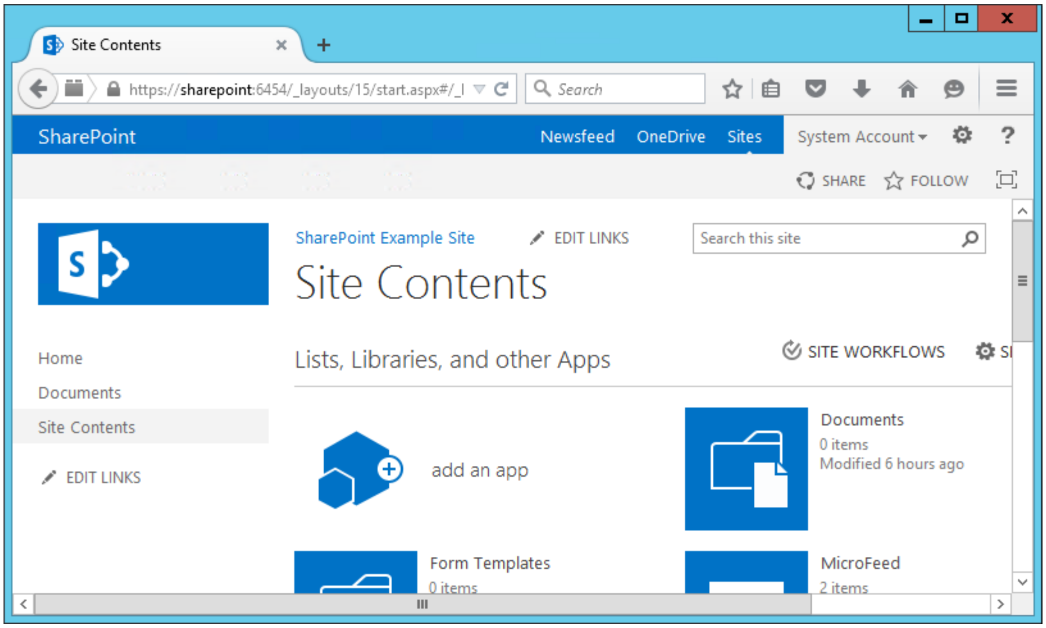
https://sharepoint:6454/_layouts/15/start.aspx#/SitePages/Hc

4.6 Creating new sub-sites

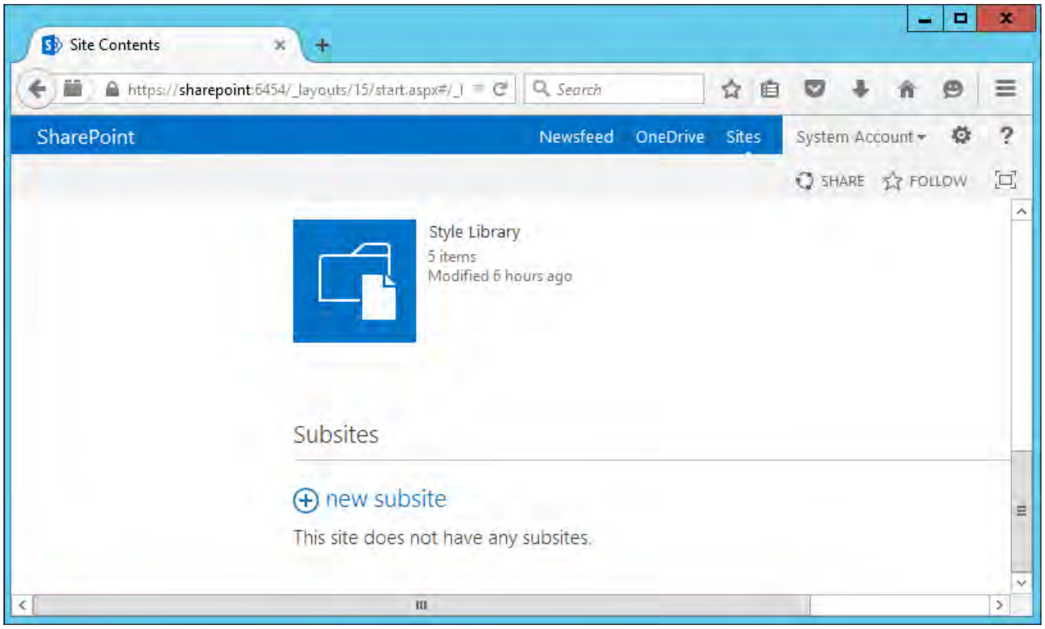
1. After logging into your site, in your browser window click the **gear symbol** next to the Administrator login area, then click on **Site Contents**.



2. In the browser window, the Site Contents page will open.



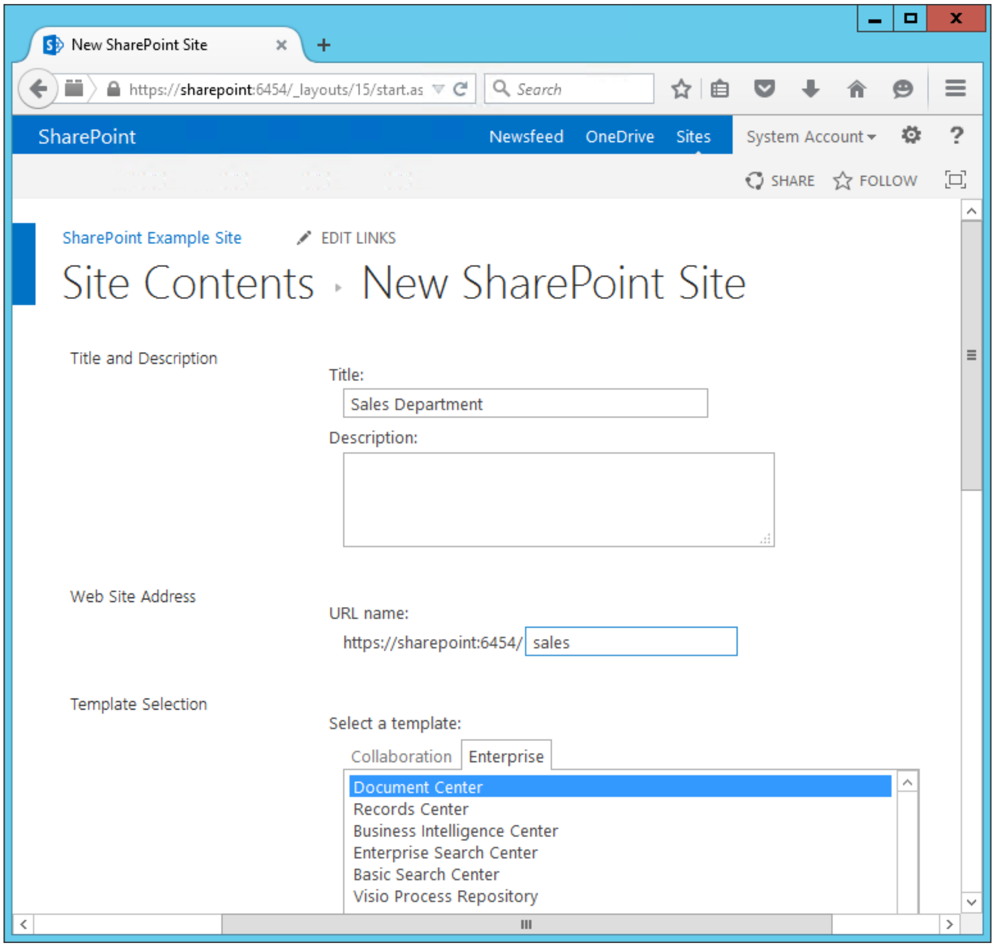
3. In the browser window, scroll down to the Subsites area and click the **plus sign button** next to new subsite.



This site does not have any subsites.

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**.



SharePoint Example Site

Site Contents › New SharePoint Site

Title and Description

Title: Sales Department

Description:

Web Site Address

URL name: https://sharepoint:6454/ sales

Template Selection

Select a template:

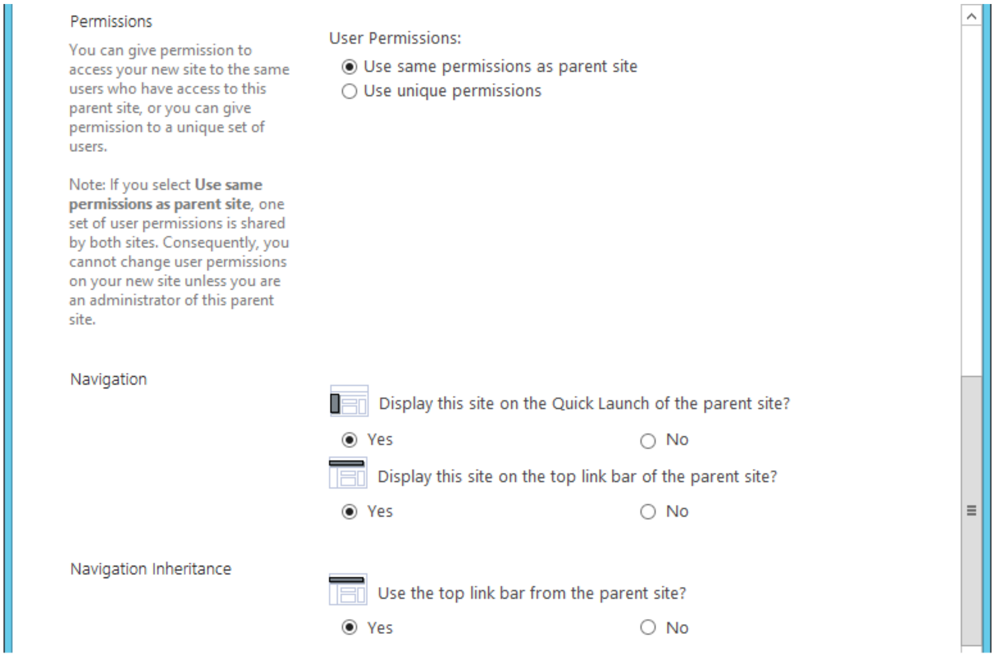
Collaboration | Enterprise

- Document Center
- Records Center
- Business Intelligence Center
- Enterprise Search Center
- Basic Search Center
- Visio Process Repository

5. In your browser, scroll down and do the following:

   a. Choose **User Permissions** (in our build, we left the Use same permissions as parent site radio button selected).

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

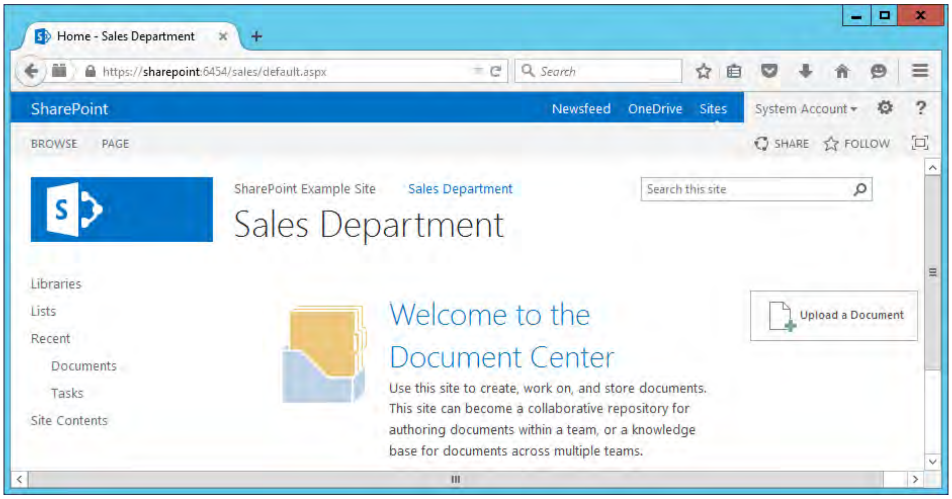
Navigation Inheritance

Use the top link bar from the parent site?

● Yes ○ No

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

7. Your new subsite will open in the browser.



Use this site to create, work on, and store documents. This site can become a collaborative repository for authoring documents within a team, or a knowledge base for documents across multiple teams.

8. Return to the homepage URL **https://sharepoint:6454** and repeat the steps from section 4.6 to create other subsites of interest.

5 Set up Federated Authentication at the Relying Party's SharePoint

5.1 Introduction

In previous chapters of this How-To Guide we demonstrated how to set up set up federated authentication between the Relying Party and the Identity Provider and how to create the Relying Party's SharePoint site. In this chapter we demonstrate how to set up federated authentication between the Relying Party's SharePoint and the PingFederate-RP. Before continuing with this chapter implementers are required to have federation servers at both the Identity Provider and the Relying Party as well as a working SharePoint instance that is claims-aware. For this build we provide instructions for setting up these components in chapter 2, chapter 3, and chapter 4.

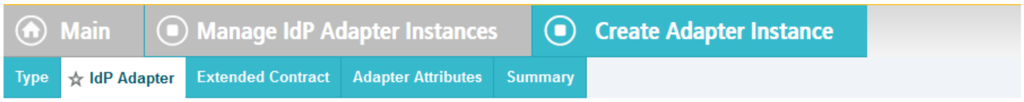
We will demonstrate how to set up a trusted logon provider for the Relying Party so that when a user requests access to a SharePoint site, the user will be redirected to the PingFederate-RP for authentication via WS-Federation. The Ping-Federate-RP will then forward the authentication request to the PingFederate-IdP. The PingFederate-IdP will present a logon page to the user. Once the user authenticates, the user will be redirected back to the original SharePoint site and will be able to access the site because they have a valid authentication token.

As you complete different steps in this chapter you will be able to verify the correctness or completeness of your component configuration and integration in functional test sub-sections.

If you follow the instructions in this chapter, you will be able to perform a functional test to verify the successful completion of the steps for installing, configuring, and integrating the components.

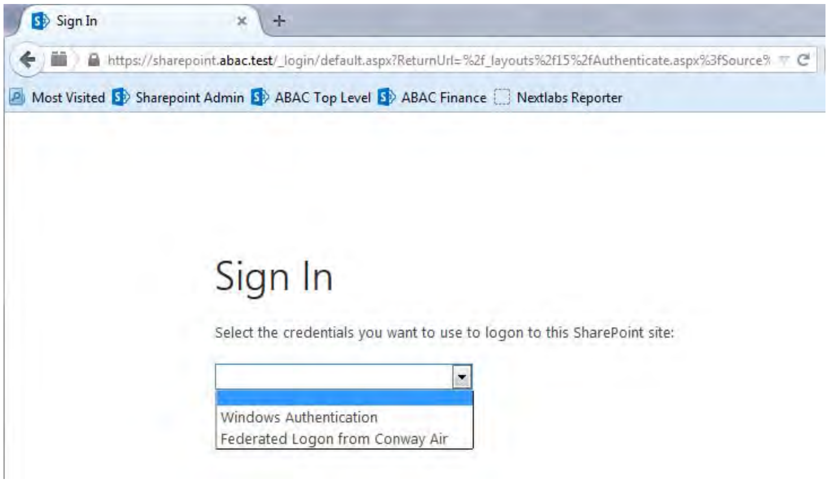
5.2 Usage Notes on PingFederate

- When using the PingFederate application to perform an administrative configuration, there is usually a sequence of screens, ending with a summary page. Once you click **Done** on the summary page, you must also click **Save** on the following page to save the configurations. If you forget to click **Save**, you may inadvertently lose changes to the configuration.
- Ping identity refers to the Relying Party as the **Service Provider** in their PingFederate product and associated documentation.
- When using the PingFederate application to perform configuration, refer to the title of the tab with a small star icon to its left, to easily identify the item you are currently configuring. For example, if you navigated to the following screen, you would be on the IdP Adapter screen.



5.3 Configure a SharePoint Federated Logon Provider

Follow the instructions in this section to configure the federated logon provider at the Relying Party's SharePoint site. Once this configuration is complete, the user will see two authentication options when first attempting to access the SharePoint site. The first option is to log on using the default **Windows Authentication**. This option does not use federation. The second option is to use a federated logon.


Sign In
https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%
Most Visited
Sharepoint Admin
ABAC Top Level
ABAC Finance
Nextlabs Reporter

Sign In

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

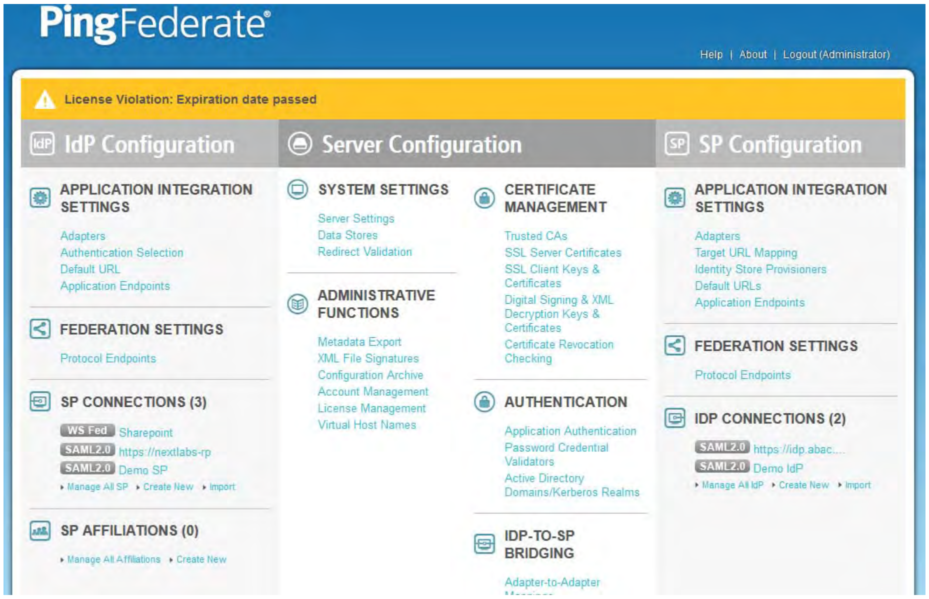
Windows Authentication
Federated Logon from Conway Air

In order to set up a federated logon, you will configure a trust relationship between the SharePoint server and the PingFederate-RP that will faciliate the federated logon. Once a user authenticates via a federated logon, the PingFederate-RP will cryptographically sign WS-Federation messages and send them to the SharePoint server. The PingFederate-RP must be configured as a trusted identity token Issuer in SharePoint, so that SharePoint will accept the messages sent by the PingFederate-RP and allow the user access to the SharePoint site.

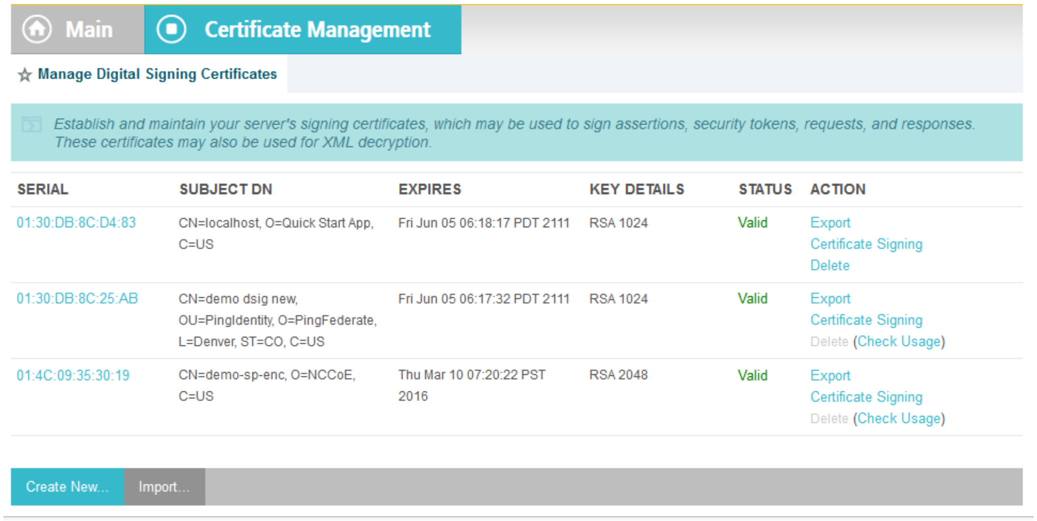
5.3.1 Setting up the Certificate

Setting up a certificate involves creating the certificate at the from the Identity Provider, exporting the certificate, and importing it in the SharePoint site of the Relying Party.

1. Log on to the server that hosts the PingFederate service for the Relying Party.
2. Launch your browser and go to: **https://<DNS_NAME>:9999/pingfederate/app**.
3. Replace **DNS_NAME** with the fully qualified name of the Relying Party's PingFederate server (e.g. **https://rp.abac.test:9999/pingfederate/app**).
4. Log on to the PingFederate application using the credentials you configured during installation.



5. On the **Main** menu, under **CERTIFICATE MANAGEMENT**, click **Digital Signing and XML**.

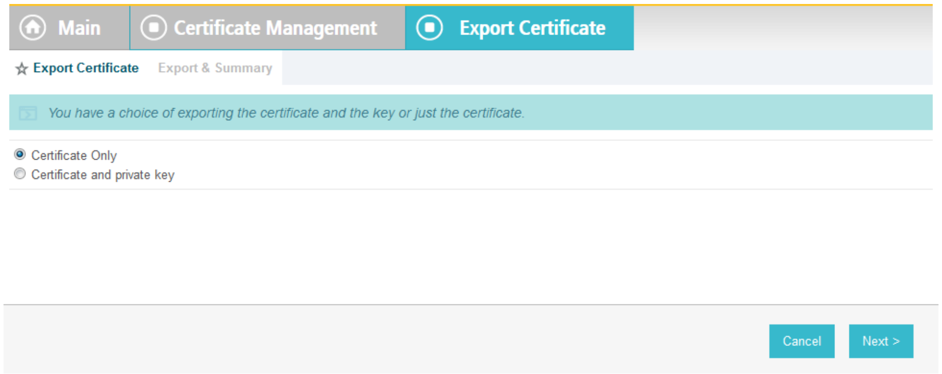


Establish and maintain your server's signing certificates, which may be used to sign assertions, security tokens, requests, and responses. These certificates may also be used for XML decryption.

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTION
01:30:DB:8C:D4:83	CN=localhost, O=Quick Start App, C=US	Fri Jun 05 06:18:17 PDT 2111	RSA 1024	Valid	Export Certificate Signing Delete
01:30:DB:8C:25:AB	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US	Fri Jun 05 06:17:32 PDT 2111	RSA 1024	Valid	Export Certificate Signing Delete (Check Usage)
01:4C:09:35:30:19	CN=demo-sp-enc, O=NCCoE, C=US	Thu Mar 10 07:20:22 PST 2016	RSA 2048	Valid	Export Certificate Signing Delete (Check Usage)

6. Locate the certificate that will be used to sign messages that will be sent to the SharePoint server. In the example screen shot above, this certificate has CN with the value **demo dsig new**.

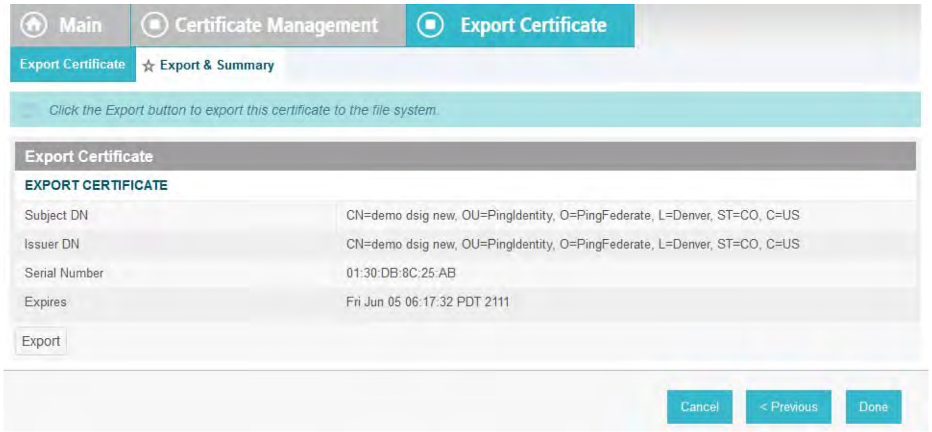
7. Click on the **Export** link for this certificate in the **ACTION** column.



You have a choice of exporting the certificate and the key or just the certificate.

● Certificate Only
○ Certificate and private key

8. Select **Certificate Only** and click **Next**.



Click the Export button to export this certificate to the file system.

Export Certificate

EXPORT CERTIFICATE

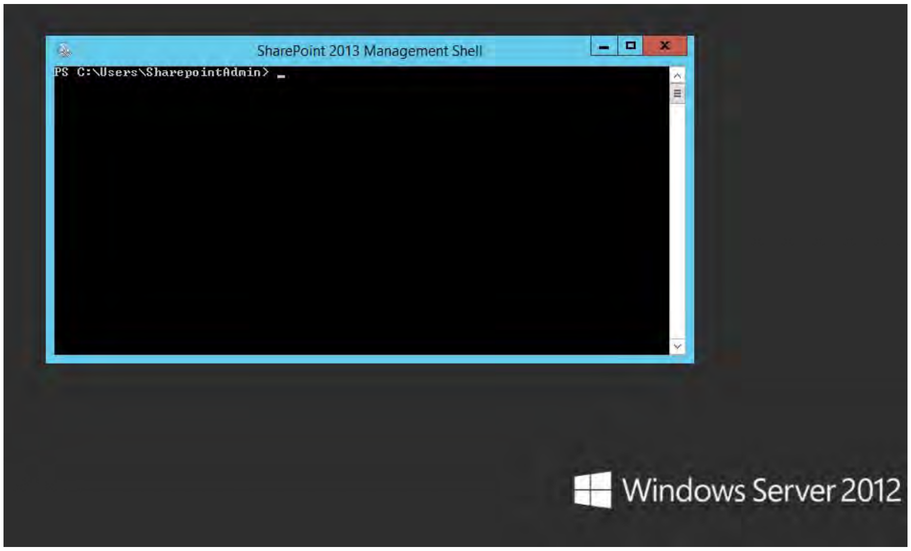
Subject DN	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
Issuer DN	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US
Serial Number	01:30:DB:8C:25:AB
Expires	Fri Jun 05 06:17:32 PDT 2111

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

10. Using the SharePoint administrator credentials, log on to the server that hosts SharePoint for the Relying Party.

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

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

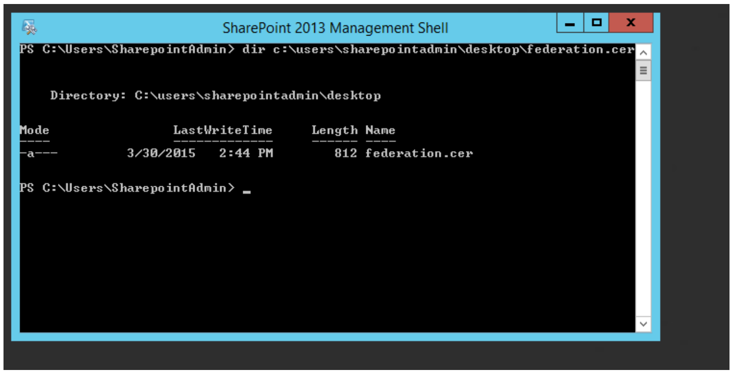


```
PS C:\Users\SharepointAdmin> _
```

13. To verify that you placed the federation.cer file to the desktop, enter the following command into the Management Shell (using the correct path for your server).

    ```
    dir c:\users\SharePointadmin\desktop\federation.cer
    ```

    You should see information about the file such as the LastWriteTime.



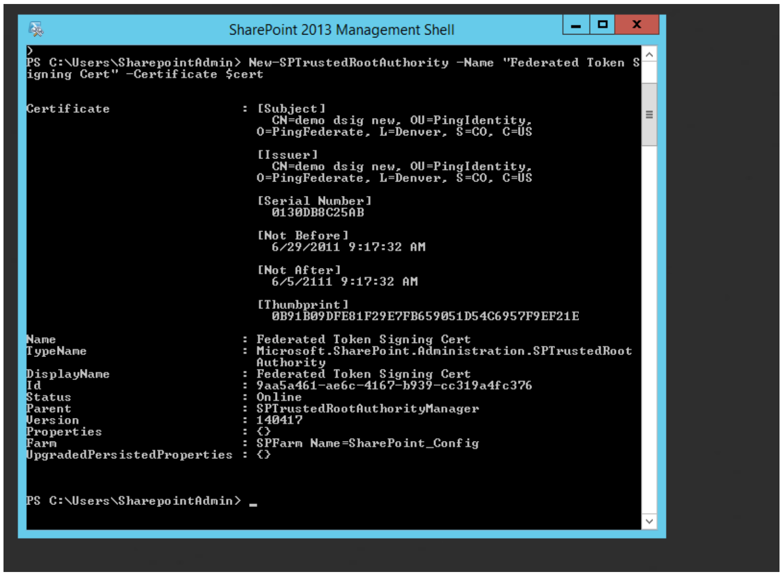
```
PS C:\Users\SharepointAdmin> dir c:\users\sharepointadmin\desktop\federation.cer


    Directory: C:\users\sharepointadmin\desktop


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---           3/30/2015   2:44 PM        812 federation.cer


PS C:\Users\SharepointAdmin> _
```

14. Enter the following commands into the Management Shell to import the PingFederate-RP's signing certificate (using the correct path for your server):

    ```
    $cert = New-Object
    System.Security.Cryptography.X509Certificates.X509Certificate2("C:\
    users\SharePointadmin\Desktop\federation.cer")
    ```

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

    SharePoint responds by displaying details about the imported certificate.



```
>
PS C:\Users\SharepointAdmin> New-SPTrustedRootAuthority -Name "Federated Token S
igning Cert" -Certificate $cert


Certificate                  : [Subject]
                                 CN=demo dsig new, OU=PingIdentity,
                               O=PingFederate, L=Denver, S=CO, C=US

                               [Issuer]
                                 CN=demo dsig new, OU=PingIdentity,
                               O=PingFederate, L=Denver, S=CO, C=US

                               [Serial Number]
                                 0130DB8C25AB

                               [Not Before]
                                 6/29/2011 9:17:32 AM

                               [Not After]
                                 6/5/2111 9:17:32 AM

                               [Thumbprint]
                                 0B91B09DFE81F29E7FB659051D54C6957F9EF21E

Name                         : Federated Token Signing Cert
TypeName                     : Microsoft.SharePoint.Administration.SPTrustedRoot
                               Authority
DisplayName                  : Federated Token Signing Cert
Id                           : 9aa5a461-ae6c-4167-b939-cc319a4fc376
Status                       : Online
Parent                       : SPTrustedRootAuthorityManager
Version                      : 140417
Properties                   : {}
Farm                         : SPFarm Name=SharePoint_Config
UpgradedPersistedProperties  : {}


PS C:\Users\SharepointAdmin> _
```

5.3.2 Configuring the Trusted Identity Token Issuer

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

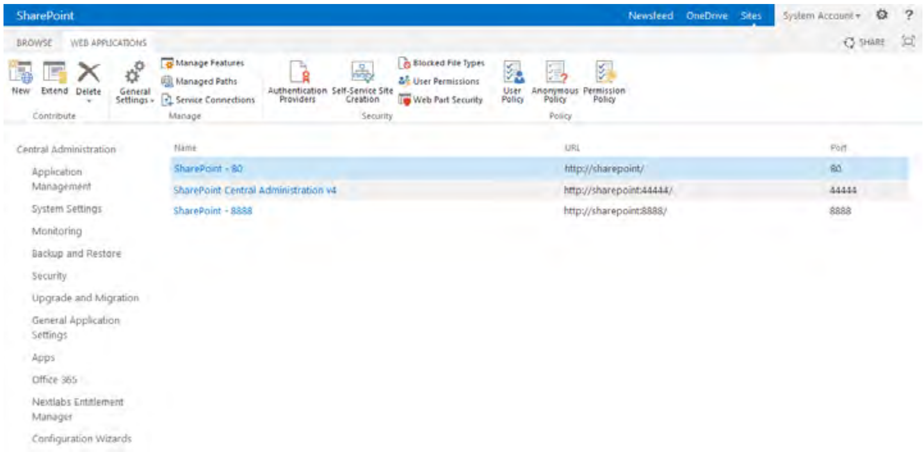
In the example commands below, the attribute **upn** is configured. You can replace **upn** with an attribute that is appropriate for your environment. The realm value (e.g. **urn:SharePoint.abac.test**) must be identical to the realm value configured in the Relying Party's PingFederate Service Provider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

```
$claimmap = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"
-IncomingClaimTypeDisplayName "upn" -SameAsIncoming

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

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

$ap = New-SPTrustedIdentityTokenIssuer -Name "Federated Logon from
Identity Provider" -Description "Federated Logon" -realm $realm
-ImportTrustCertificate $cert -ClaimsMappings $claimmap -SignInUrl
$signInURL -IdentifierClaim $claimmap.InputClaimType
```

5.3.3 Configuring the Token Issuer as a Sign On Option

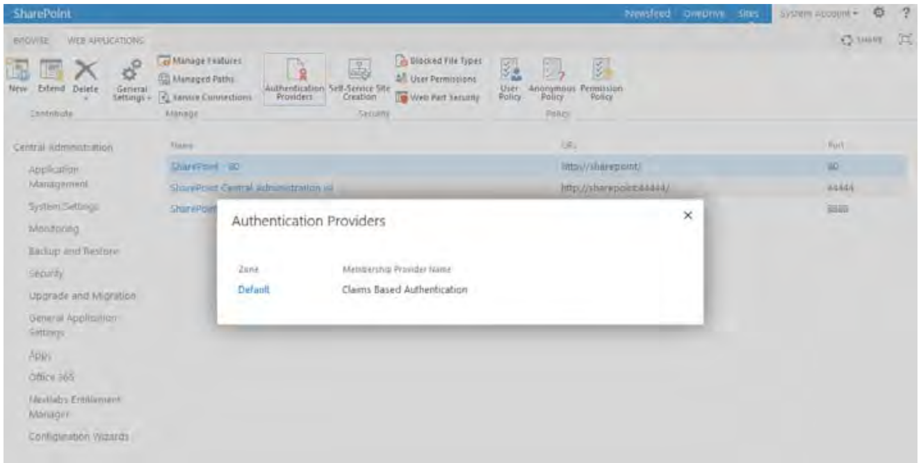
After configuring the new Trusted Identity Token Issuer, configure the new token issuer as a Sign On option for the SharePoint site.

1. Launch your browser and go the SharePoint central administration page (e.g. **http://SharePoint.abac.test:44444/default.aspx**).
2. Log on using the credentials of the SharePoint administrator
3. In the **Application Management** group, click on **Manage web applications**.
4. Click on the web application that contains the SharePoint site you are managing (e.g. **SharePoint - 80**). SharePoint will highlight the web application row that you clicked on.



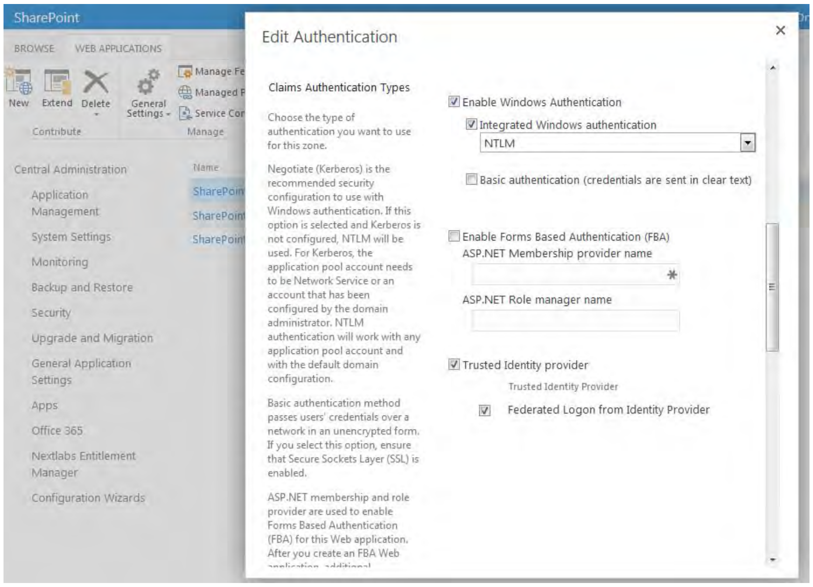
Name	URL	Port
SharePoint - 80	http://sharepoint/	80
SharePoint Central Administration v4	http://sharepoint:44444/	44444
SharePoint - 8888	http://sharepoint:8888/	8888

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



Zone	Membership Provider Name
Default	Claims Based Authentication

6. Click on the **Default** link in the **Zone** column.
7. On the Edit Authentication screen, scroll down to the **Claims Authentication Types** group. Select the **Trusted Identity provider** option.
8. Under the **Trusted Identity provider** checkbox, select the name of the new token issuer that was created using the Powershell commands (e.g. **Federated Logon from Identity Provider**).



Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web

☑ Enable Windows Authentication

☑ Integrated Windows authentication

NTLM

☐ Basic authentication (credentials are sent in clear text)

☐ Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

ASP.NET Role manager name

☑ Trusted Identity provider

Trusted Identity Provider

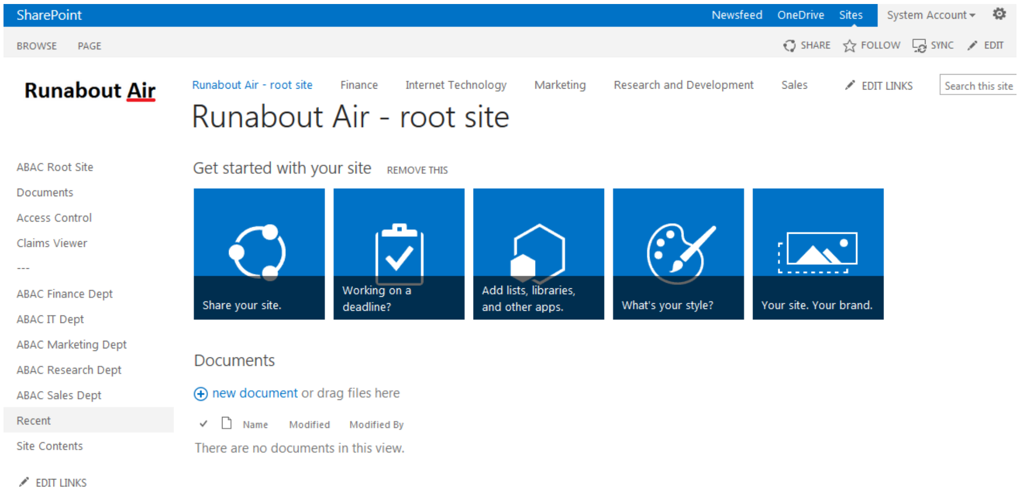
☑ Federated Logon from Identity Provider

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

5.3.4 Configuring the Access Control Rule on SharePoint

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

1. Log on to the Relying Party's SharePoint site (e.g. **https://SharePoint.abac.test**) using the credentials of the SharePoint administrator.
2. Select **Windows Authentication** in the Sign On screen.



Runabout Air - root site

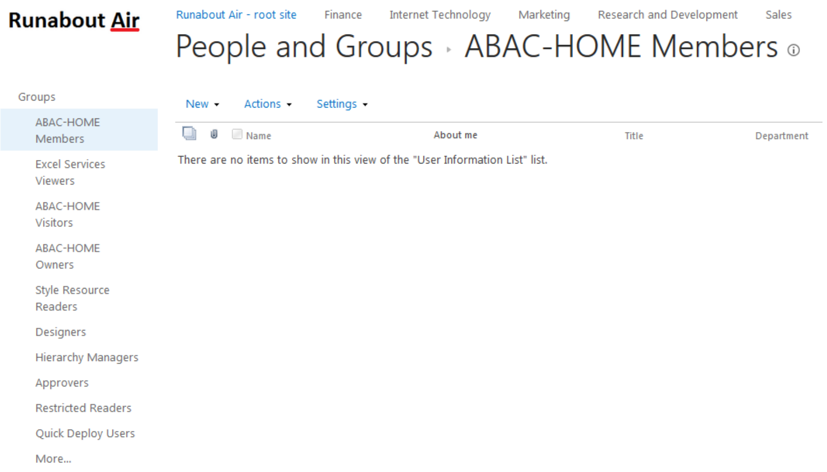
Get started with your site

Documents

There are no documents in this view.

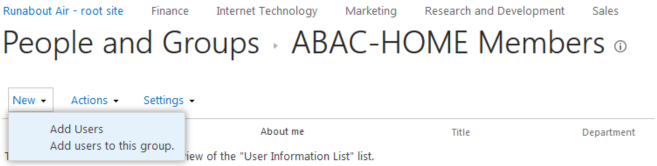
3. Click the gear icon at the top right corner of the page and select the **Site Settings** link.
4. On the Site Settings screen, in the Users and Permissions group, click **People and Groups**.

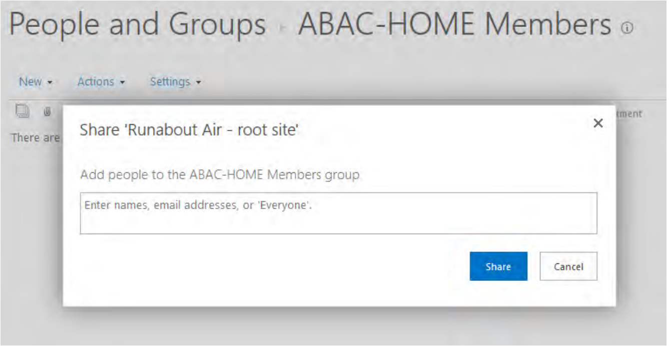
5. Under the Groups heading on the left pane, click on the **HOME Members** group.



There are no items to show in this view of the "User Information List" list.

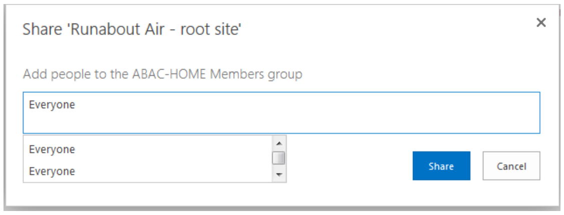
6. Under the page title, click on the **New link** and select the **Add Users** option from the popup menu.



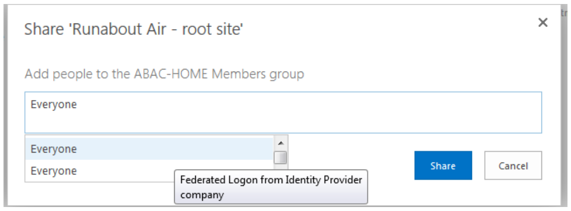

People and Groups › ABAC-HOME Members
New
Actions
Settings
There are
Share 'Runabout Air - root site'
Add people to the ABAC-HOME Members group
Enter names, email addresses, or 'Everyone'.
Share
Cancel

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

SharePoint will display a list box underneath the text field.


Share 'Runabout Air - root site'
Add people to the ABAC-HOME Members group
Everyone
Everyone
Everyone
Share
Cancel

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.

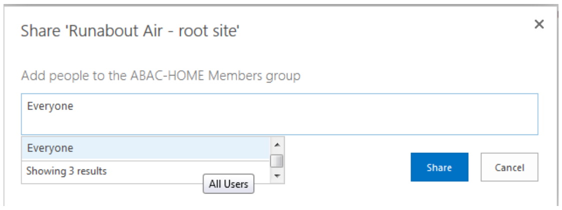


Share 'Runabout Air - root site'

Add people to the ABAC-HOME Members group

Everyone

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

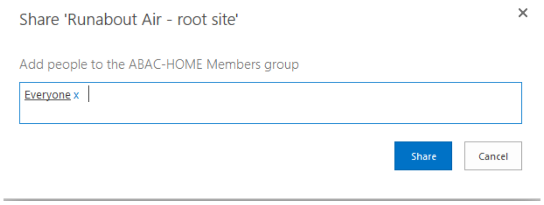


Share 'Runabout Air - root site'

Add people to the ABAC-HOME Members group

Everyone

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



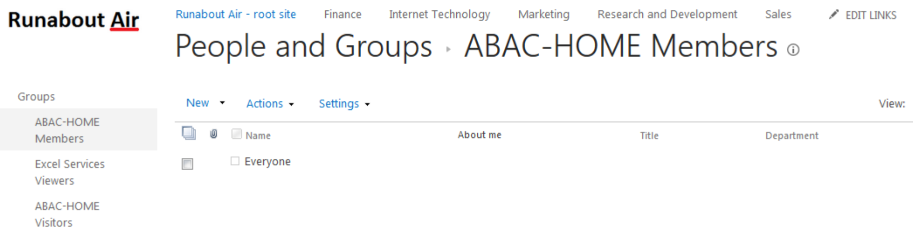
Share 'Runabout Air - root site'

Add people to the ABAC-HOME Members group

Everyone x

10. Click **Share**.

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



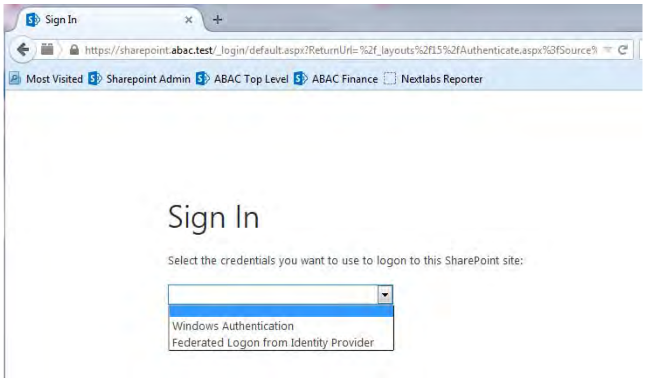
People and Groups › ABAC-HOME Members

Name	About me	Title	Department
Everyone			

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).

   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**).


Sign In
https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%
Most Visited
Sharepoint Admin
ABAC Top Level
ABAC Finance
Nextlabs Reporter

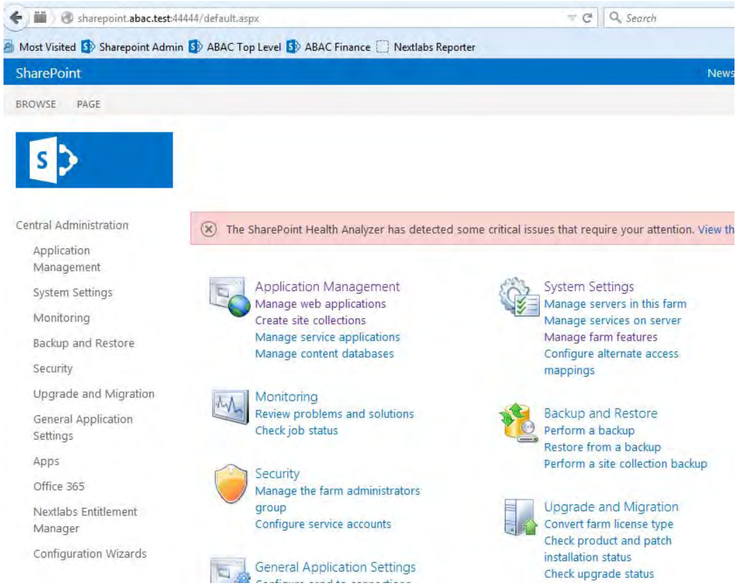
Sign In

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

Windows Authentication
Federated Logon from Identity Provider

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

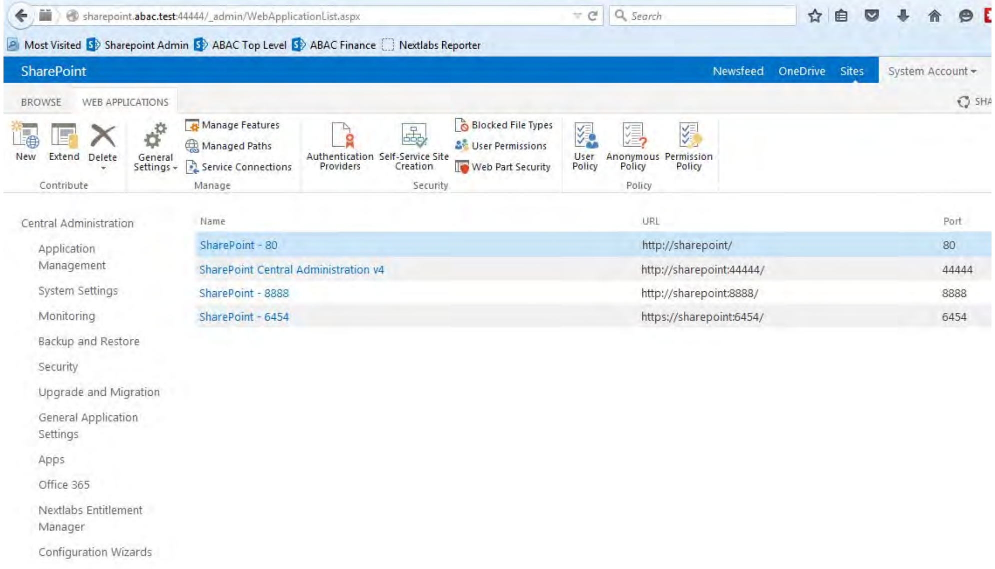
2. Launch your browser and go the SharePoint central administration page (e.g. **http://SharePoint.abac.test:44444/default.aspx**).
3. Log on using the credentials of the SharePoint administrator.



The SharePoint Health Analyzer has detected some critical issues that require your attention. View th

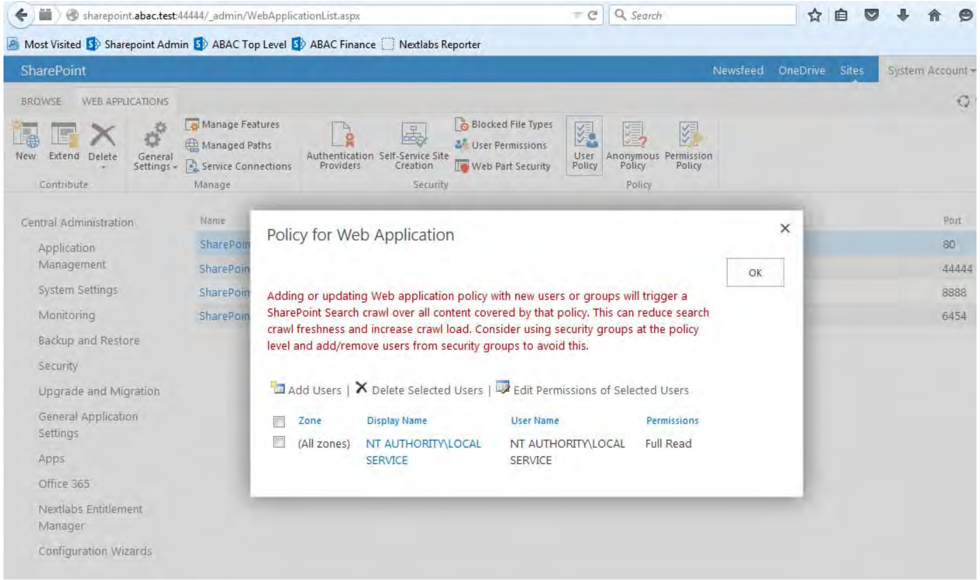
Application Management
Manage web applications
Create site collections
Manage service applications
Manage content databases
System Settings
Manage servers in this farm
Manage services on server
Manage farm features
Configure alternate access mappings
Monitoring
Review problems and solutions
Check job status
Backup and Restore
Perform a backup
Restore from a backup
Perform a site collection backup
Security
Manage the farm administrators group
Configure service accounts
Upgrade and Migration
Convert farm license type
Check product and patch installation status
Check upgrade status
General Application Settings

4. In the **Application Management** group, click on **Manage web applications**.
5. Click on the web application that contains the SharePoint site you are managing (e.g. **SharePoint - 80**). SharePoint will highlight the web application row that you clicked on.



Name	URL	Port
SharePoint - 80	http://sharepoint/	80
SharePoint Central Administration v4	http://sharepoint:44444/	44444
SharePoint - 8888	http://sharepoint:8888/	8888
SharePoint - 6454	https://sharepoint:6454/	6454

6. Click on the **User Policy** button.

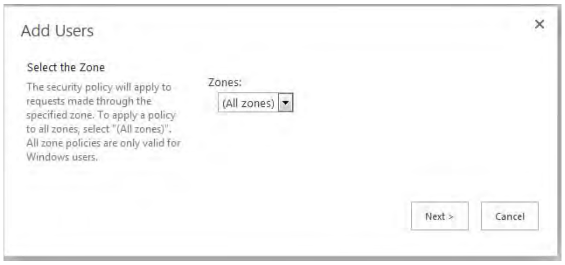


Policy for Web Application

Adding or updating Web application policy with new users or groups will trigger a SharePoint Search crawl over all content covered by that policy. This can reduce search crawl freshness and increase crawl load. Consider using security groups at the policy level and add/remove users from security groups to avoid this.

	Zone	Display Name	User Name	Permissions
□	(All zones)	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\LOCAL SERVICE	Full Read

7. Click **Add Users**.



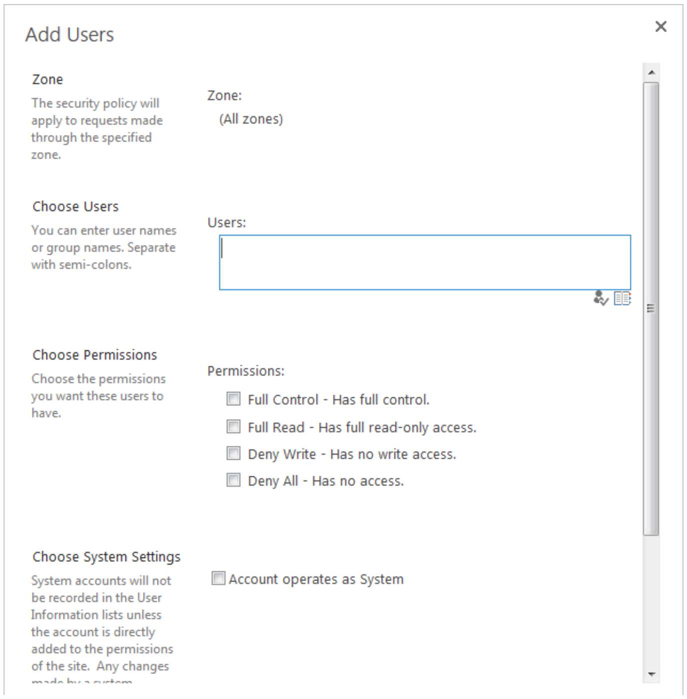
Add Users

Select the Zone

The security policy will apply to requests made through the specified zone. To apply a policy to all zones, select "(All zones)". All zone policies are only valid for Windows users.

Zones: (All zones)

8. Click **Next**.



Add Users

Zone

The security policy will apply to requests made through the specified zone.

Zone:
(All zones)

Choose Users

You can enter user names or group names. Separate with semi-colons.

Users:

Choose Permissions

Choose the permissions you want these users to have.

Permissions:

- □ Full Control - Has full control.
- □ Full Read - Has full read-only access.
- □ Deny Write - Has no write access.
- □ Deny All - Has no access.

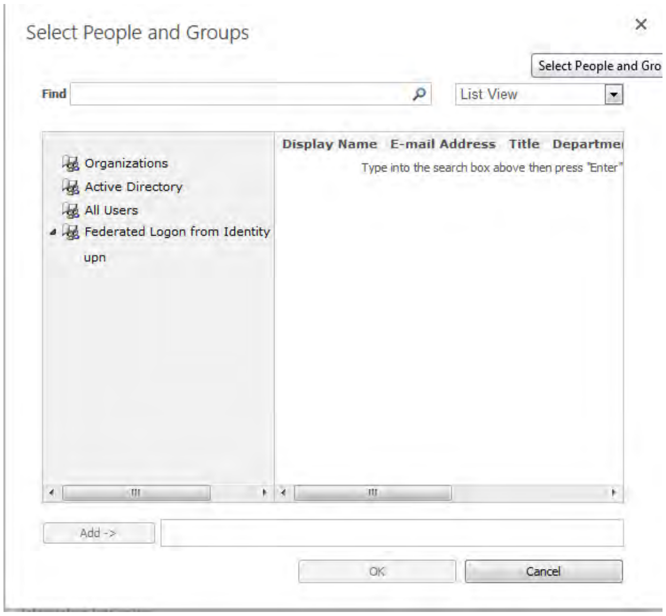
Choose System Settings

System accounts will not be recorded in the User Information lists unless the account is directly added to the permissions of the site. Any changes

□ Account operates as System

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

   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 Logon from Identity Provider**). You should also see the **upn** attribute listed under that grouping.



Select People and Groups

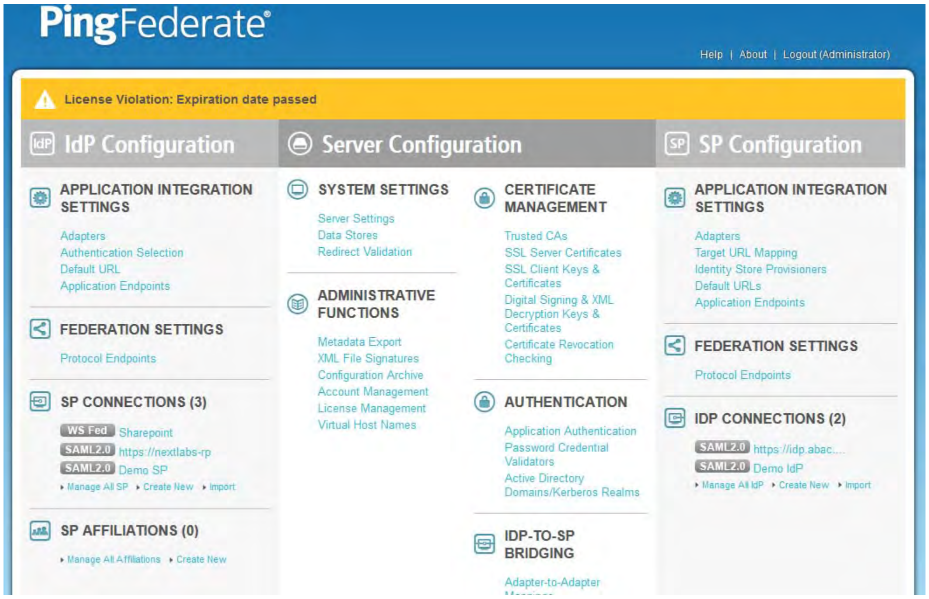
Find

Display Name	E-mail Address	Title	Departme
Type into the search box above then press "Enter"			

5.4 Configure the PingFederate-RP Connection to SharePoint

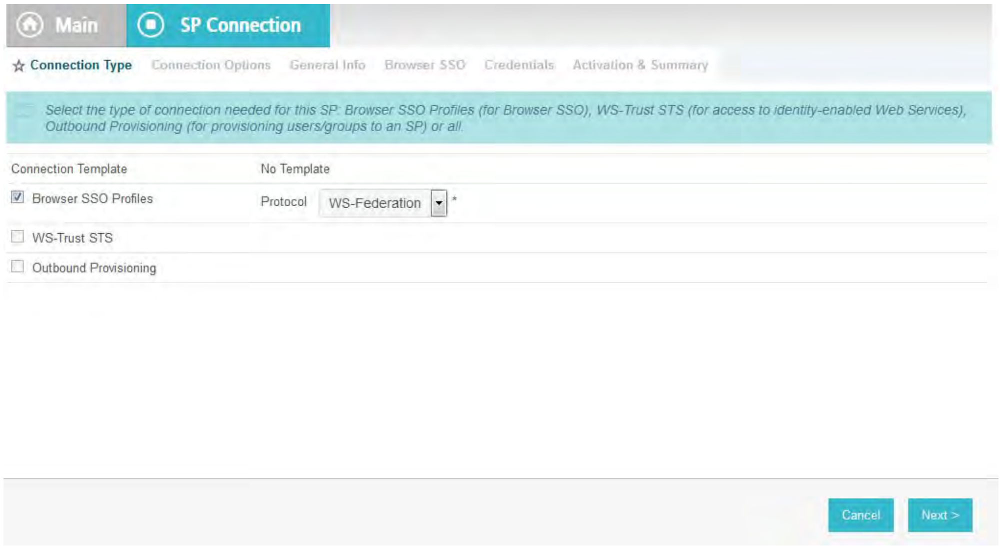
Follow the instructions below to configure a PingFederate connection from the PingFederate-RP to the Relying Party's SharePoint.

1. Log on to the server that hosts the PingFederate service for the Relying Party.
2. Launch your browser and go to: **https://<DNS_NAME>:9999/pingfederate/app**. Replace **DNS_NAME** with the fully qualified name of the Relying Party's PingFederate server (e.g. **https://rp.abac.test:9999/pingfederate/app**). Log on to the PingFederate application using the credentials you configured during installation.



License Violation: Expiration date passed

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**.



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

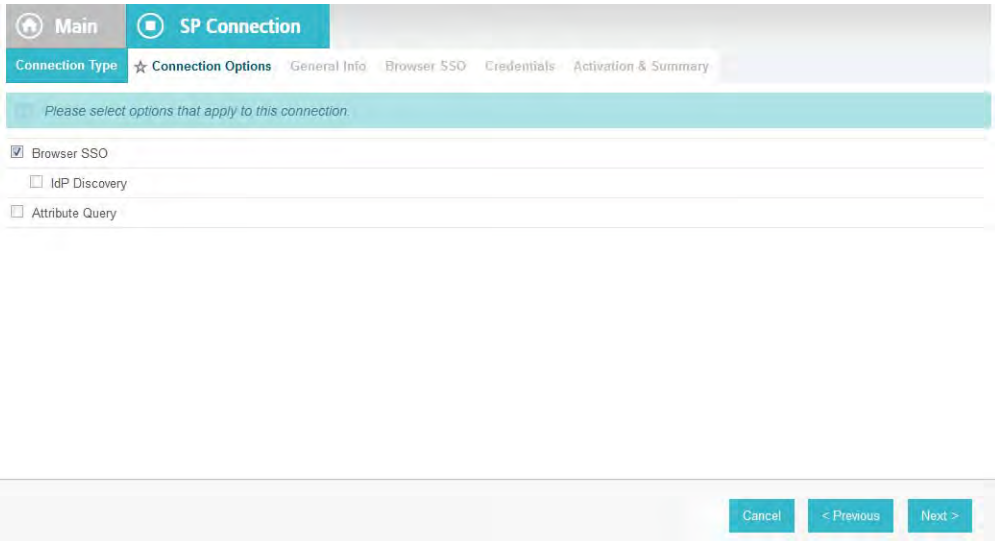
Connection Template: No Template

☑ Browser SSO Profiles — Protocol: WS-Federation *

□ WS-Trust STS

□ Outbound Provisioning

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



Please select options that apply to this connection.

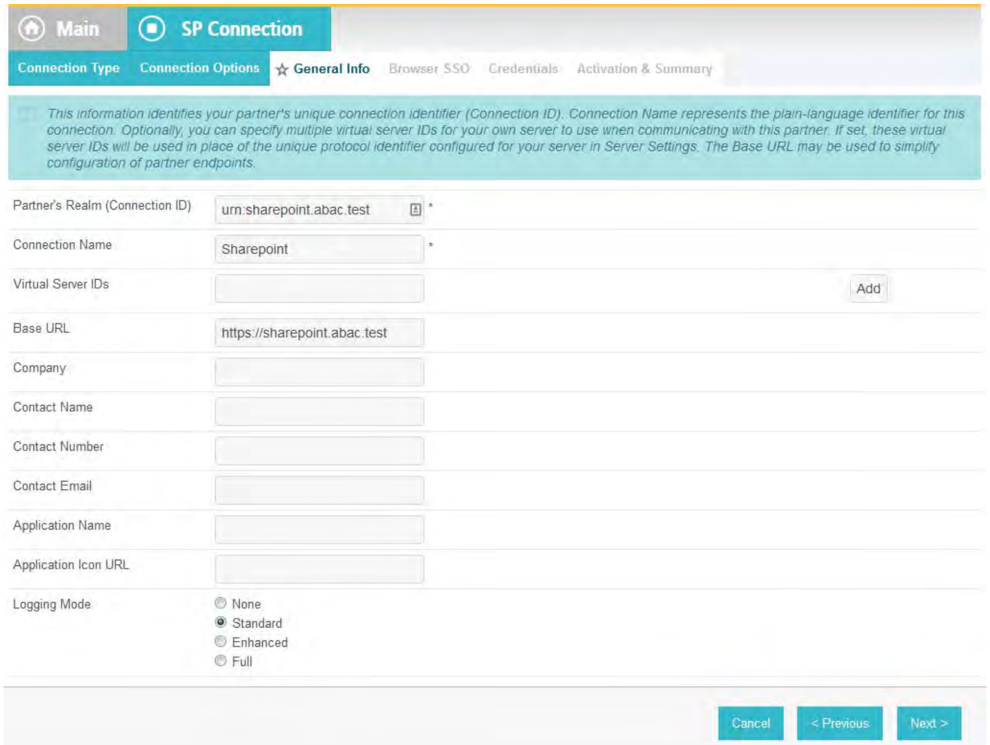
☑ Browser SSO

□ IdP Discovery

□ Attribute Query

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.

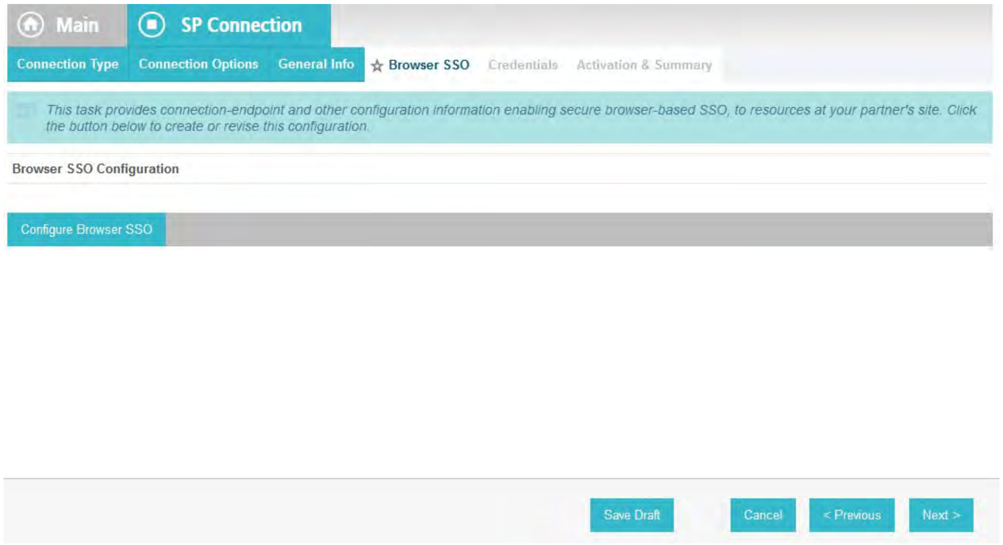
6. Enter a unique name for this new PingFederate configuration in the **Connection Name** field. For the Base URL field, enter the root destination URL at the SharePoint site where the PingFederate will redirect a user once authenticated (e.g. **https://SharePoint.abac.test**).



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 Realm (Connection ID)	urn:sharepoint.abac.test *
Connection Name	Sharepoint *
Virtual Server IDs	
Base URL	https://sharepoint.abac.test
Company	
Contact Name	
Contact Number	
Contact Email	
Application Name	
Application Icon URL	
Logging Mode	○ None ● Standard ○ Enhanced ○ Full

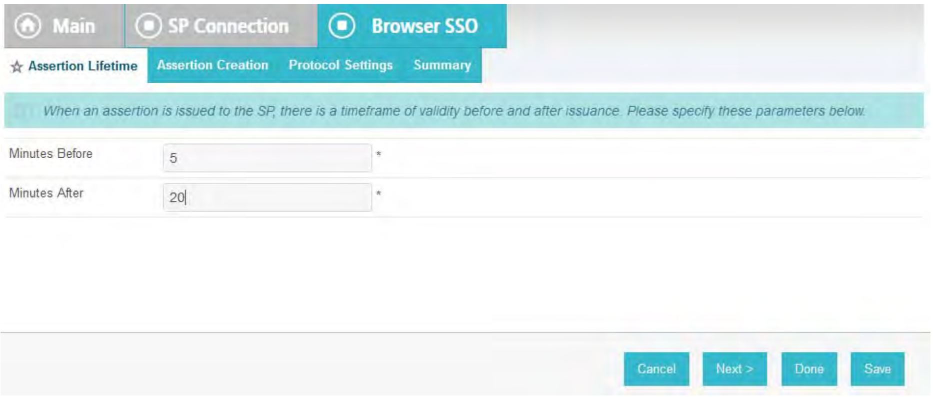
7. Click **Next**.



This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

Browser SSO Configuration

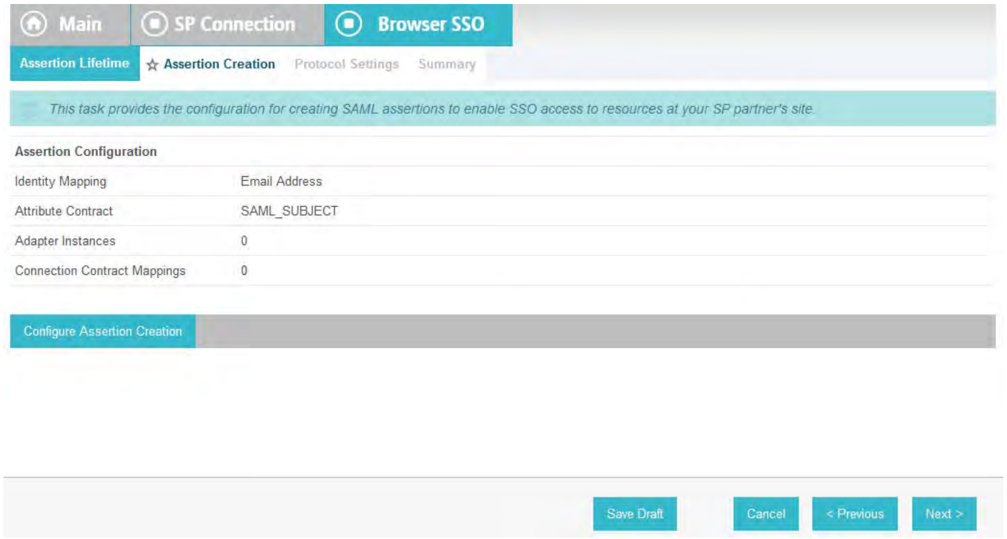
8. On the Browser SSO screen, click **Configure Browser SSO**. On the Assertion Lifetime screen, enter a value of **20** for the **Minutes After** field.



When an assertion is issued to the SP, there is a timeframe of validity before and after issuance. Please specify these parameters below.

Minutes Before	5 *
Minutes After	20 *

9. Click **Next**.

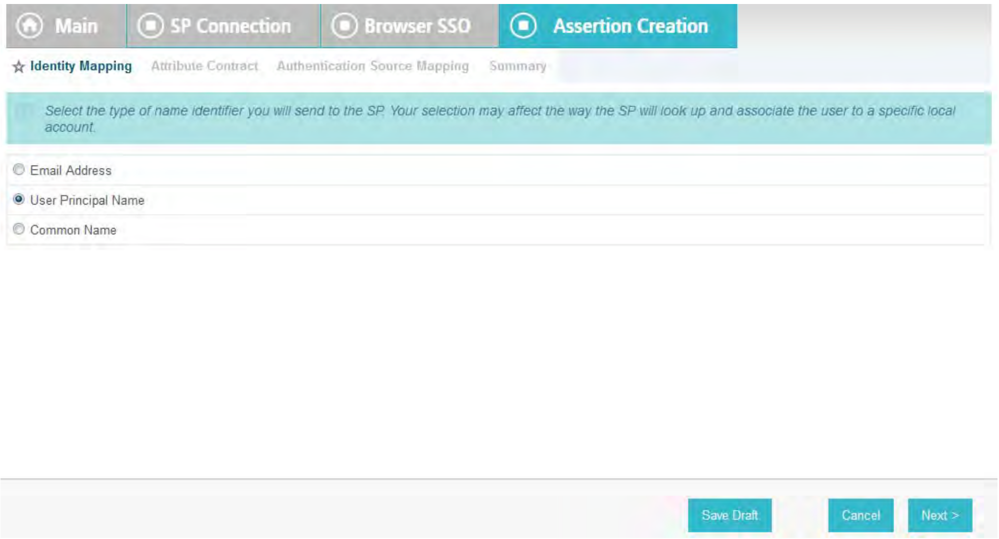


This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration

Identity Mapping	Email Address
Attribute Contract	SAML_SUBJECT
Adapter Instances	0
Connection Contract Mappings	0

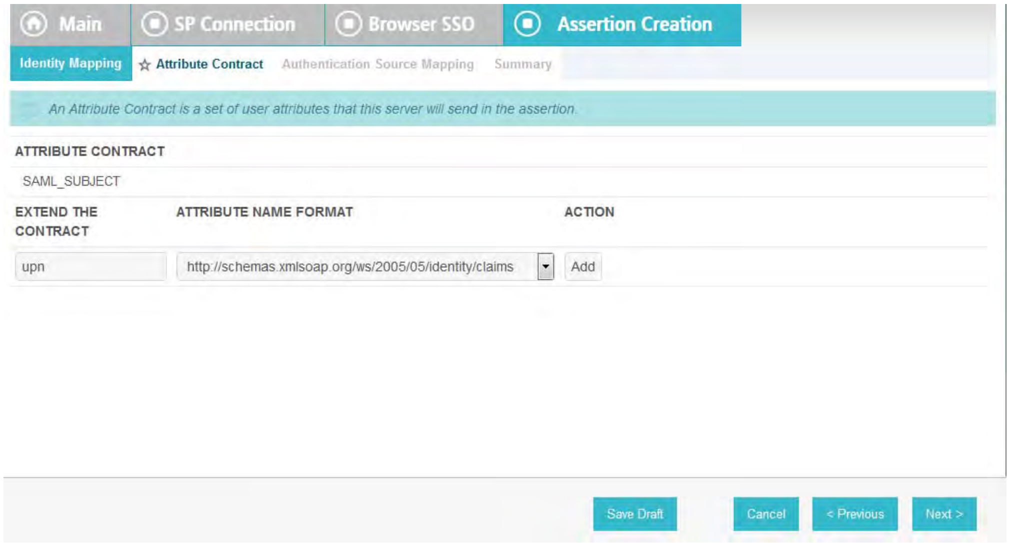
10. On the Assertion Creation screen, click **Configure Assertion Creation**. On the Identity Mapping screen, select **User Principal Name**.



Select the type of name identifier you will send to the SP. Your selection may affect the way the SP will look up and associate the user to a specific local account.

○ Email Address
● User Principal Name
○ Common Name

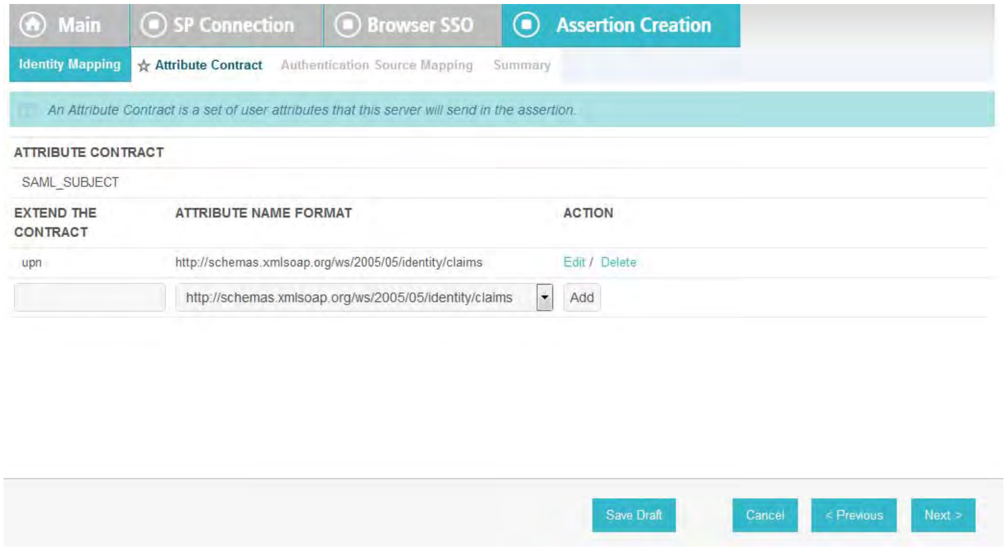
11. Click **Next**. On the Attribute Contract screen, below the **EXTEND THE CONTRACT FIELD**, enter **upn** in the text box. For the **ATTRIBUTE NAME FORMAT** select the **schemas.xmlsoap.org 2005 identity claims format.**



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT		
SAML_SUBJECT		
EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Add

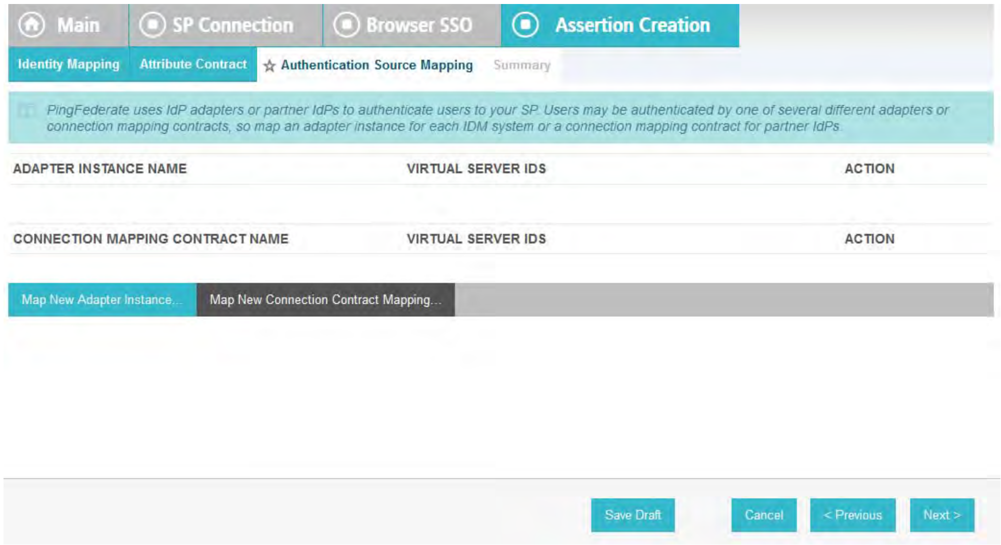
12. Click **Add**.



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT		
SAML_SUBJECT		
EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Edit / Delete
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Add

13. Click **Next**.

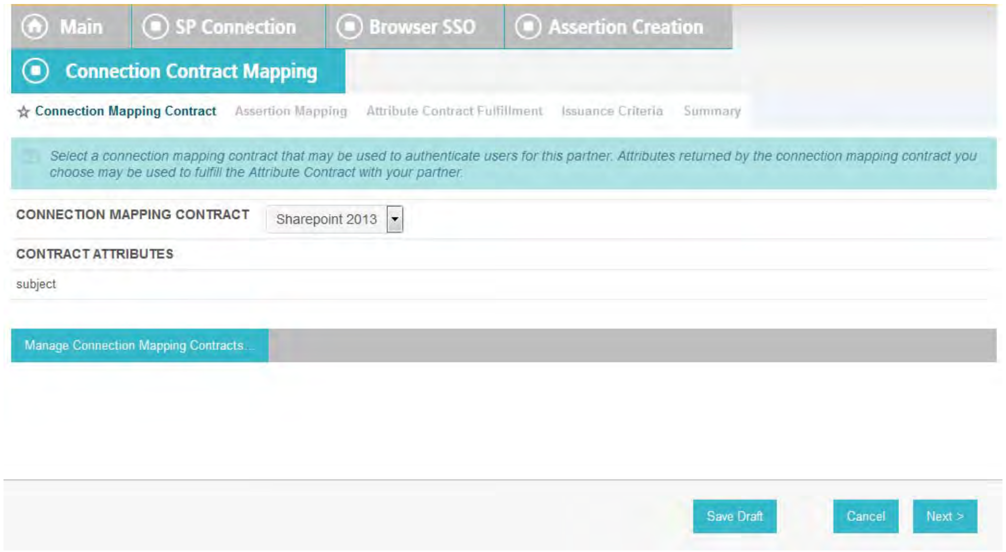


PingFederate uses IdP adapters or partner IdPs to authenticate users to your SP. Users may be authenticated by one of several different adapters or connection mapping contracts, so map an adapter instance for each IDM system or a connection mapping contract for partner IdPs.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION

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 chapter 3 (e.g. **SharePoint 2013**).


Main
SP Connection
Browser SSO
Assertion Creation
Connection Contract Mapping
☆ Connection Mapping Contract
Assertion Mapping
Attribute Contract Fulfillment
Issuance Criteria
Summary
Manage Connection Mapping Contracts...
Save Draft
Cancel
Next >

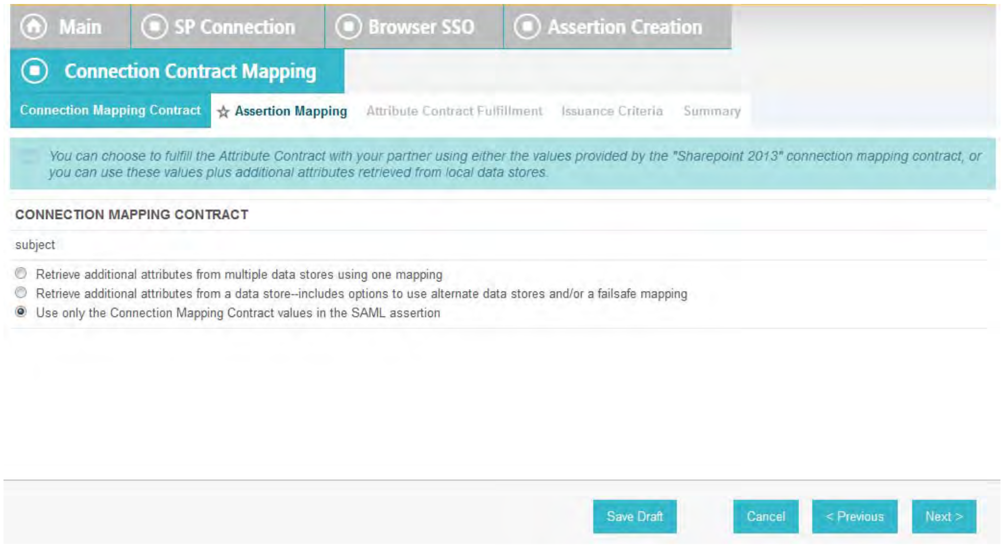
Select a connection mapping contract that may be used to authenticate users for this partner. Attributes returned by the connection mapping contract you choose may be used to fulfill the Attribute Contract with your partner.

CONNECTION MAPPING CONTRACT: Sharepoint 2013

CONTRACT ATTRIBUTES

subject

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



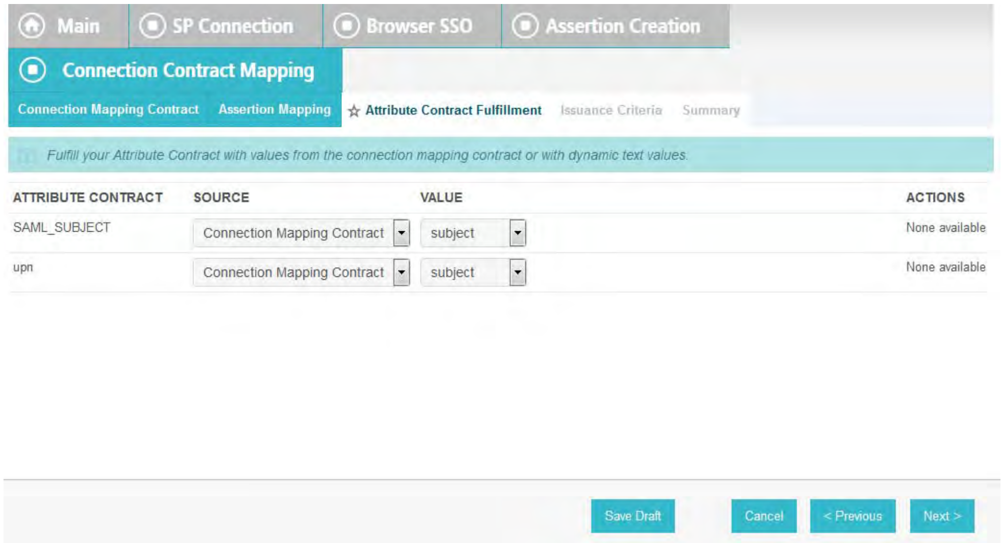
You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "Sharepoint 2013" connection mapping contract, or you can use these values plus additional attributes retrieved from local data stores.

CONNECTION MAPPING CONTRACT

subject

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

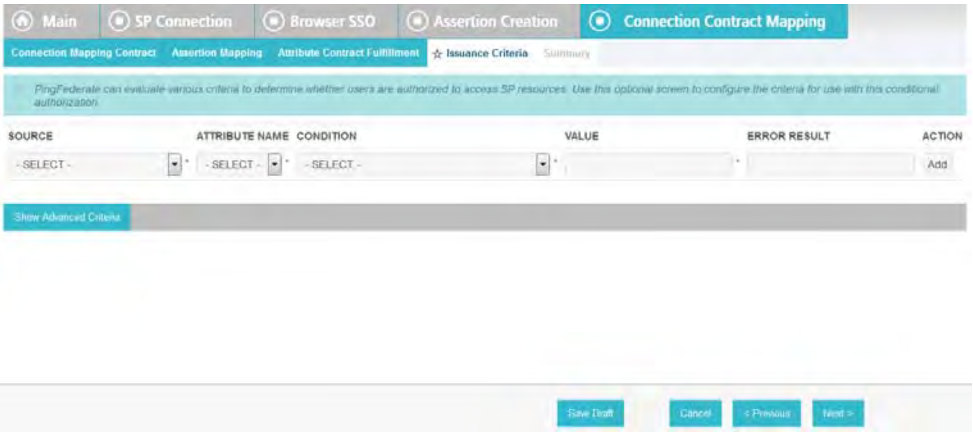
16. Click **Next**.



Fulfill your Attribute Contract with values from the connection mapping contract or with dynamic text values.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Connection Mapping Contract	subject	None available
upn	Connection Mapping Contract	subject	None available

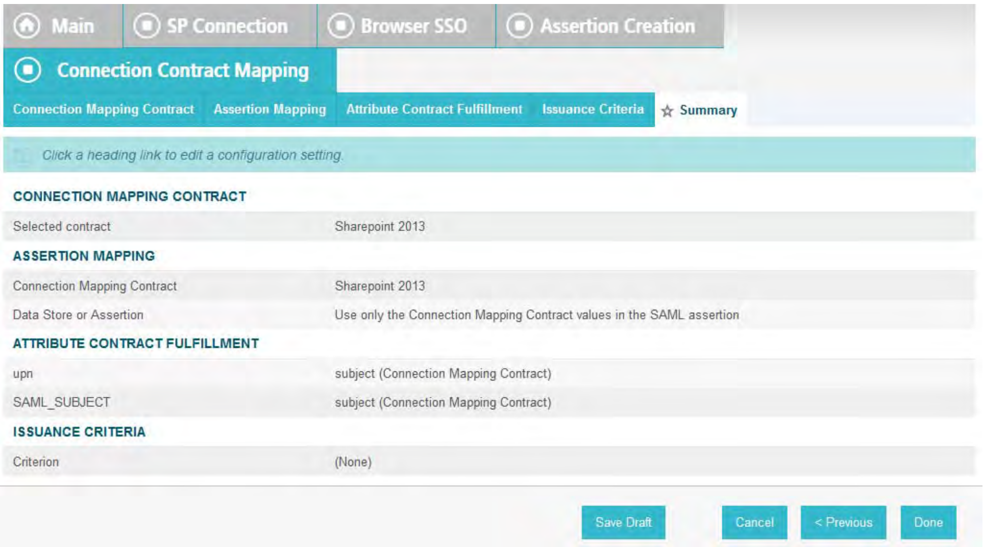
17. On the Attribute Contract Fulfillment screen, click **Next**.



PingFederate can evaluate various criteria to determine whether users are authorized to access SP resources. Use this optional screen to configure the criteria for use with this conditional authorization.

SOURCE	ATTRIBUTE NAME	CONDITION	VALUE	ERROR RESULT	ACTION
- SELECT - *	- SELECT - *	- SELECT - *	*		Add

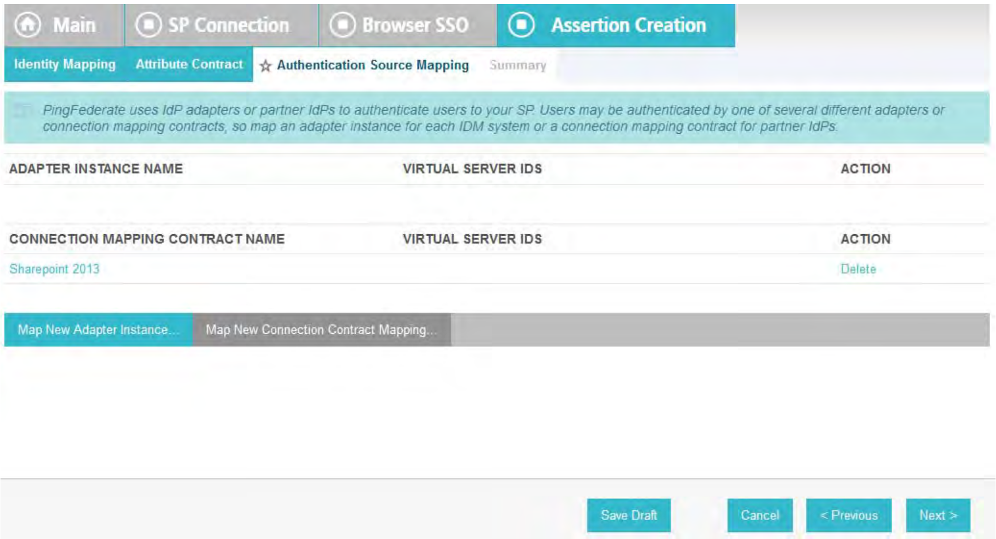
18. On the Issuance Criteria screen, click **Next**.



Click a heading link to edit a configuration setting.

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)

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

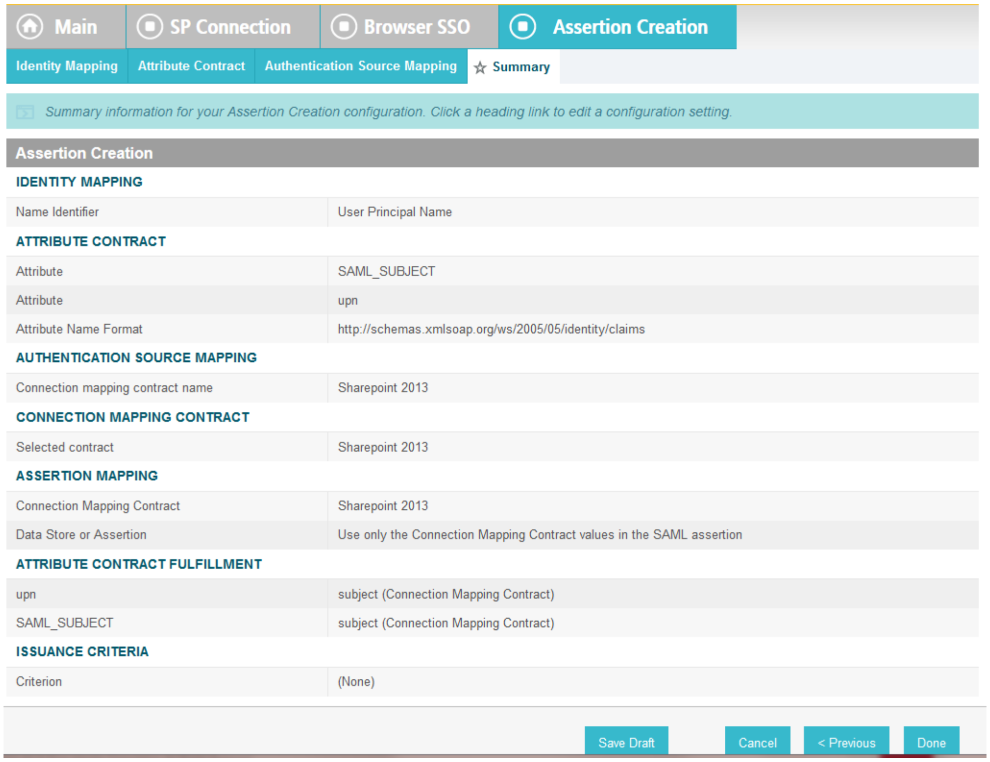


PingFederate uses IdP adapters or partner IdPs to authenticate users to your SP. Users may be authenticated by one of several different adapters or connection mapping contracts, so map an adapter instance for each IDM system or a connection mapping contract for partner IdPs.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		Delete

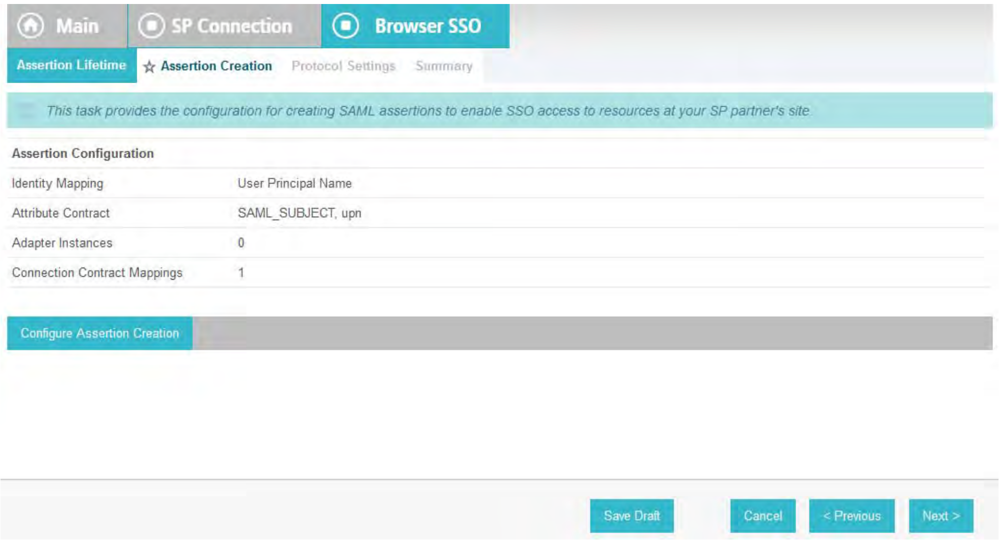
20. On the Authentication Source Mapping screen, click **Next**.



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

Assertion Creation	
IDENTITY MAPPING	
Name Identifier	User Principal Name
ATTRIBUTE CONTRACT	
Attribute	SAML_SUBJECT
Attribute	upn
Attribute Name Format	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
AUTHENTICATION SOURCE MAPPING	
Connection mapping contract name	Sharepoint 2013
CONNECTION MAPPING CONTRACT	
Selected contract	Sharepoint 2013
ASSERTION MAPPING	
Connection Mapping Contract	Sharepoint 2013
Data Store or Assertion	Use only the Connection Mapping Contract values in the SAML assertion
ATTRIBUTE CONTRACT FULFILLMENT	
upn	subject (Connection Mapping Contract)
SAML_SUBJECT	subject (Connection Mapping Contract)
ISSUANCE CRITERIA	
Criterion	(None)

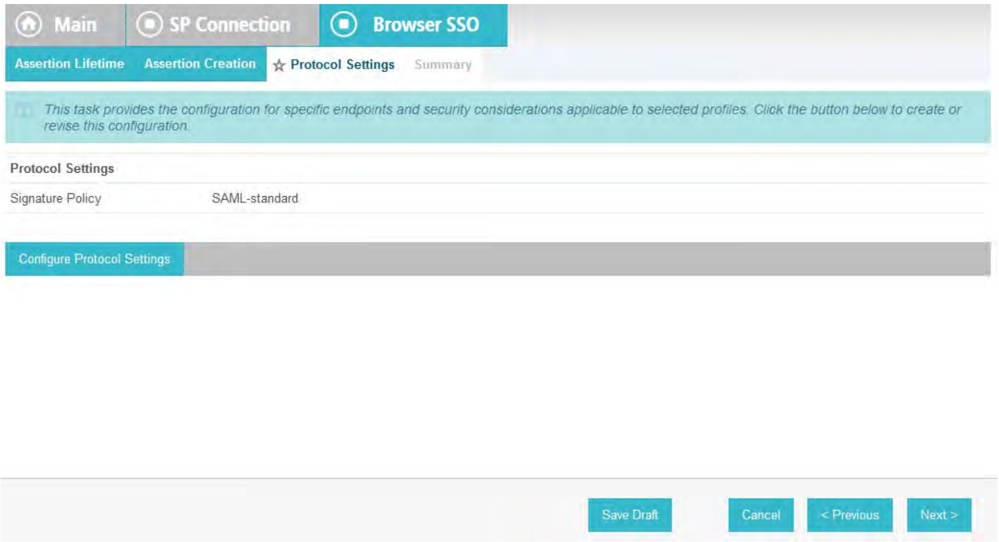
21. On the Summary screen, click **Done**.



This task provides the configuration for creating SAML assertions to enable SSO access to resources at your SP partner's site.

Assertion Configuration	
Identity Mapping	User Principal Name
Attribute Contract	SAML_SUBJECT, upn
Adapter Instances	0
Connection Contract Mappings	1

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



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

Protocol Settings	
Signature Policy	SAML-standard

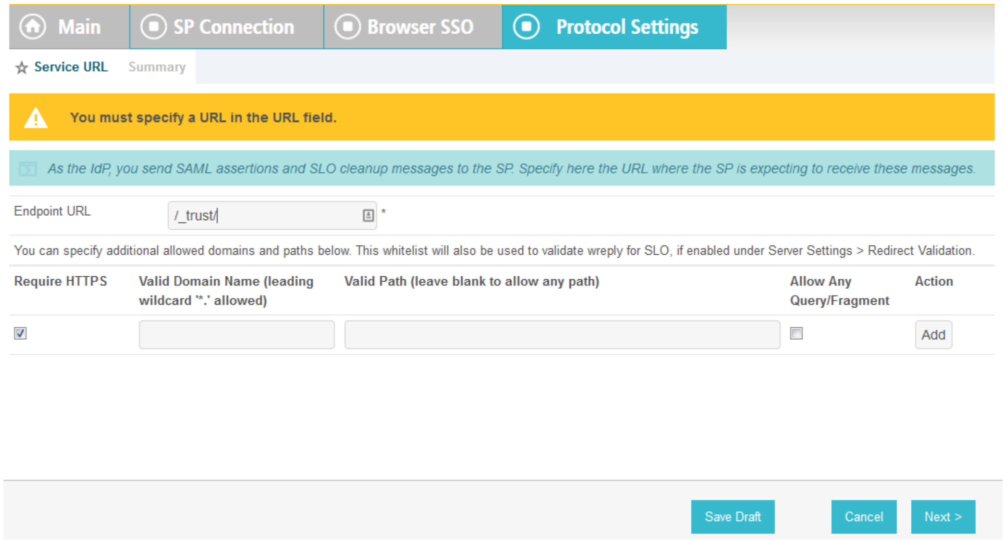
23. On the Protocol Settings screen, click **Configure Protocol Settings**.

24. On the Service URL screen, for the **Endpoint URL** field, enter the name of the destination URL at the Service Provider (SharePoint) site (.e.g. **/_trust/**). When PingFederate completes the authentication process, the user will be sent to a destination URL. The destination URL is a combination of two configuration fields. The first is the **Base URL** that was configured earlier, and the second is the **Endpoint URL** on this screen. The **Endpoint URL** will be appended to the **Base URL**. An example is provided below.

    Base URL: https://SharePoint.abac.test

    Endpoint URL: /_trust/

    After authentication, PingFederate will redirect to the destination: **https://SharePoint.abac.test/_trust/**



You must specify a URL in the URL field.

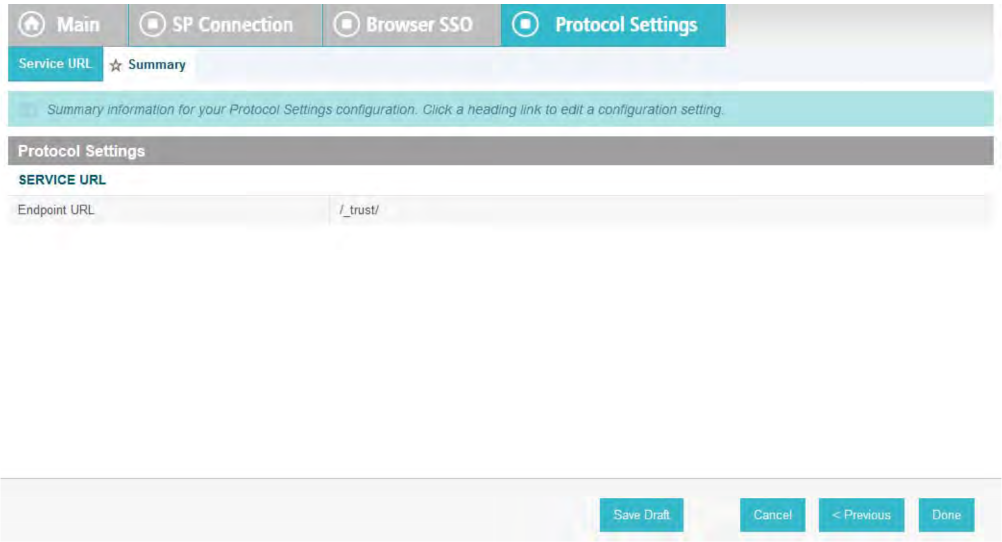
As the IdP, you send SAML assertions and SLO cleanup messages to the SP. Specify here the URL where the SP is expecting to receive these messages.

Endpoint URL /_trust/ *

You can specify additional allowed domains and paths below. This whitelist will also be used to validate wreply for SLO, if enabled under Server Settings > Redirect Validation.

Require HTTPS	Valid Domain Name (leading wildcard '*.' allowed)	Valid Path (leave blank to allow any path)	Allow Any Query/Fragment	Action
☑			□	Add

25. Click **Next**.



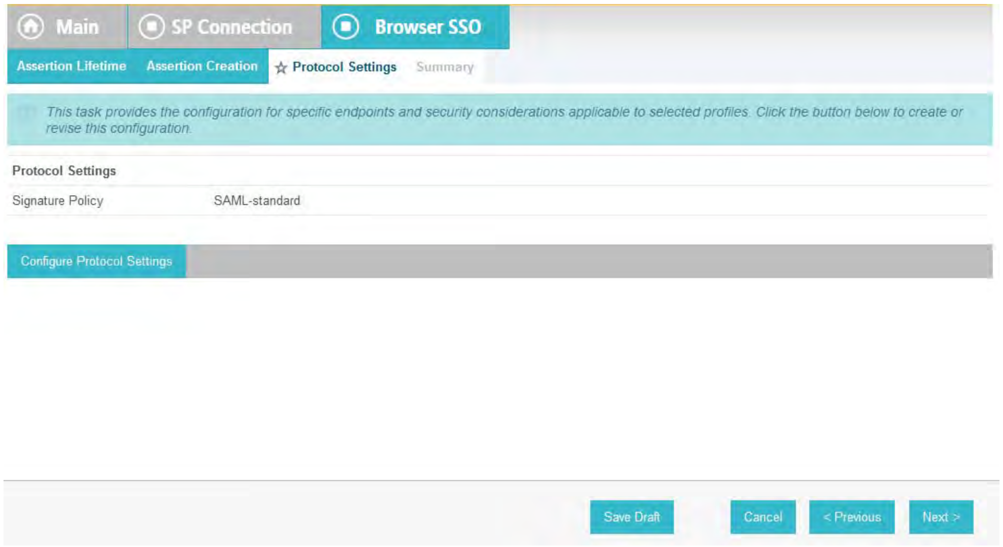
Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

Protocol Settings

SERVICE URL

Endpoint URL	/_trust/

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

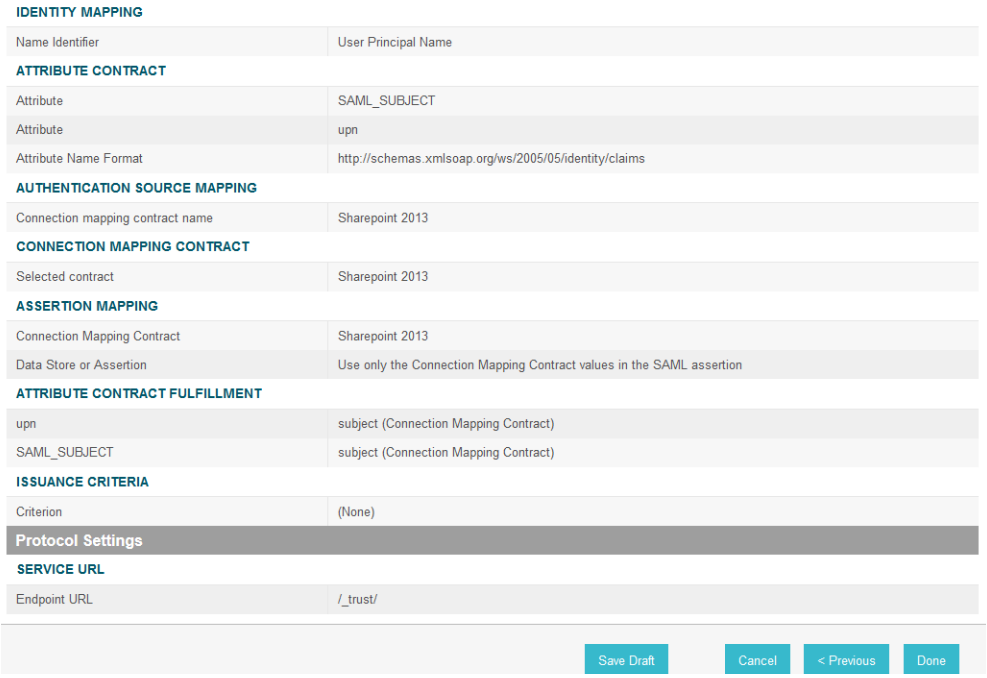


This task provides the configuration for specific endpoints and security considerations applicable to selected profiles. Click the button below to create or revise this configuration.

Protocol Settings

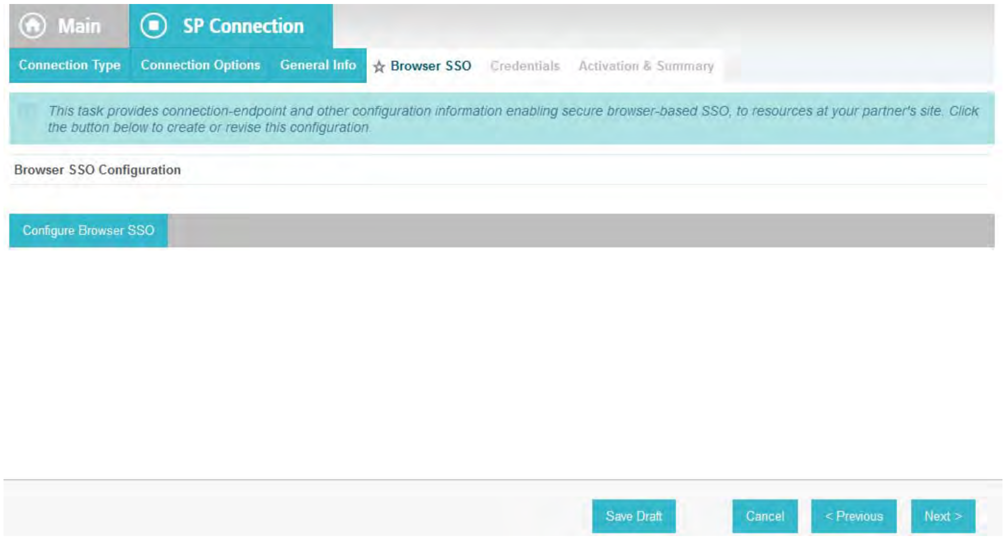
Signature Policy SAML-standard

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



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

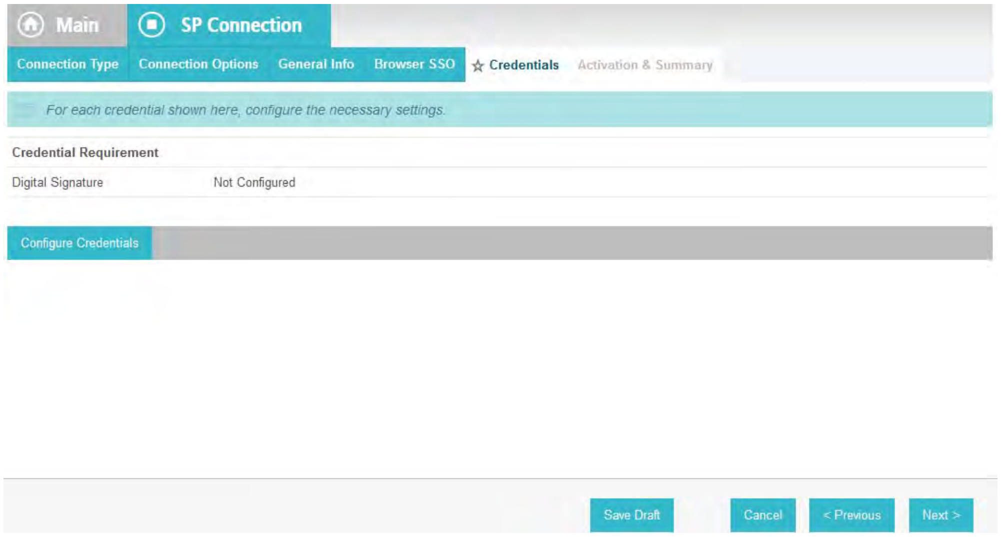
28. On the Summary screen, click **Done**.



This task provides connection-endpoint and other configuration information enabling secure browser-based SSO, to resources at your partner's site. Click the button below to create or revise this configuration.

Browser SSO Configuration

29. On the Browser SSO screen, click **Next**.

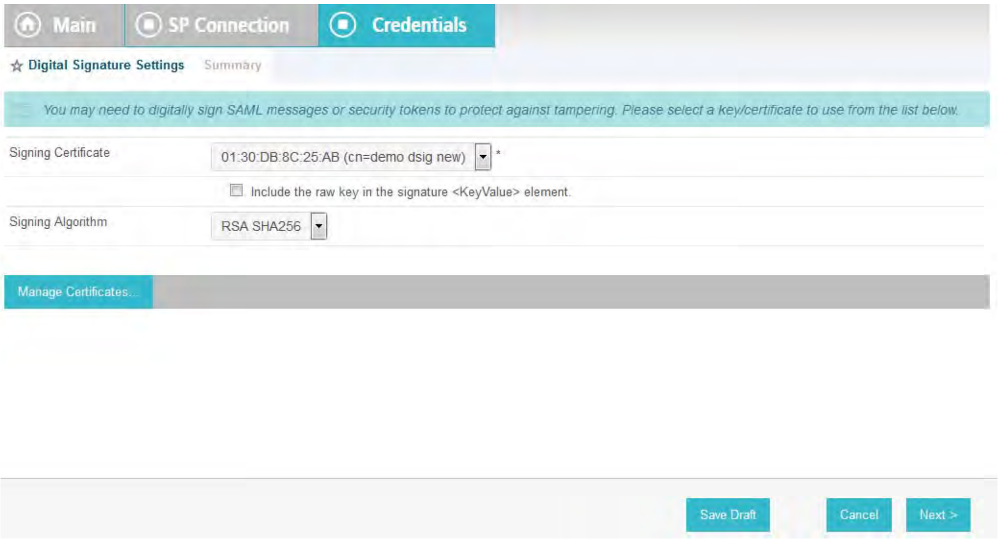


For each credential shown here, configure the necessary settings.

Credential Requirement	
Digital Signature	Not Configured

30. On the Credentials screen, click **Configure Credentials**.

31. On the Digital Signature Settings screen, select the **Signing Certificate** for SAML messages.



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.

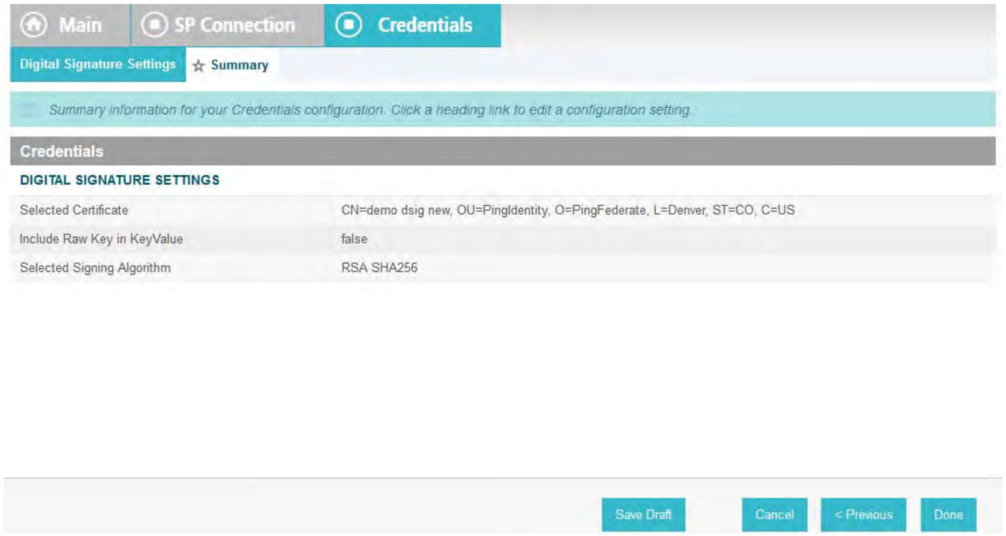
Signing Certificate: 01:30:DB:8C:25:AB (cn=demo dsig new) *

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

Signing Algorithm: RSA SHA256

286

287 32. Click **Next**.



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

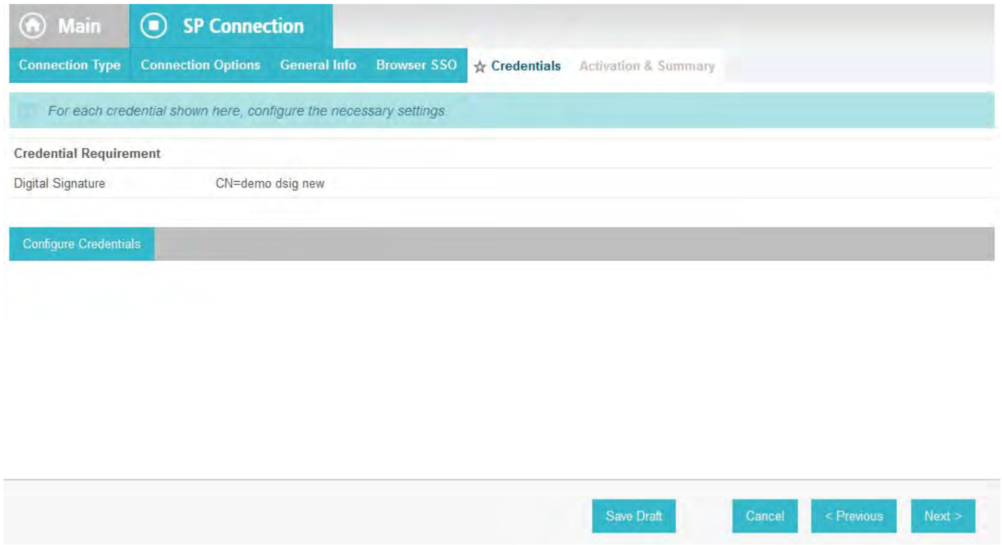
Credentials

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

288

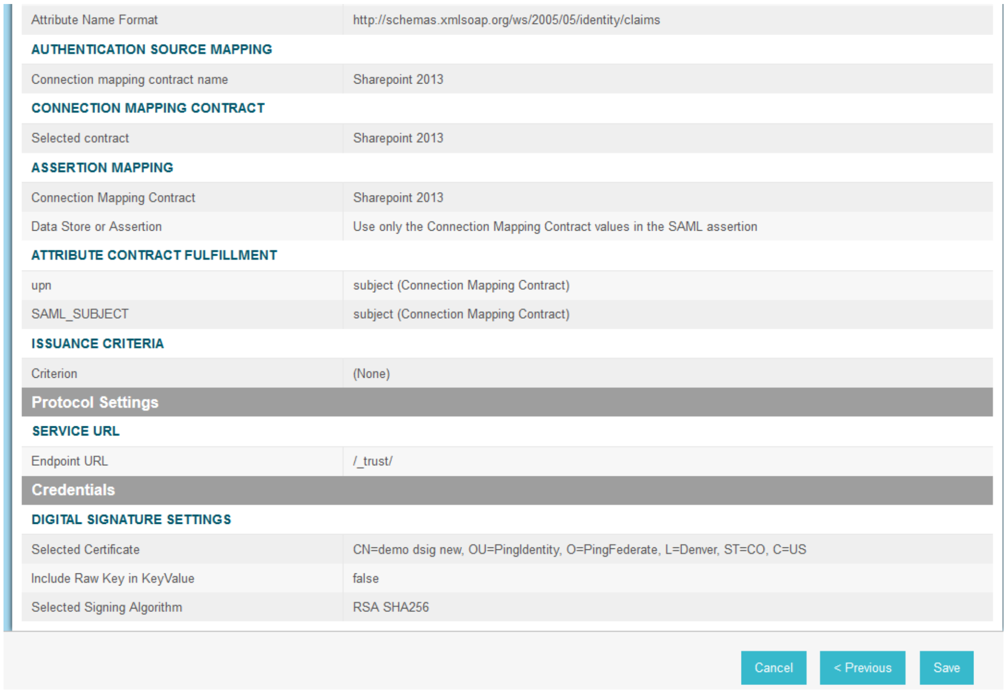
289 33. On the Summary screen, click **Done**.



For each credential shown here, configure the necessary settings.

Credential Requirement	
Digital Signature	CN=demo dsig new

34. 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

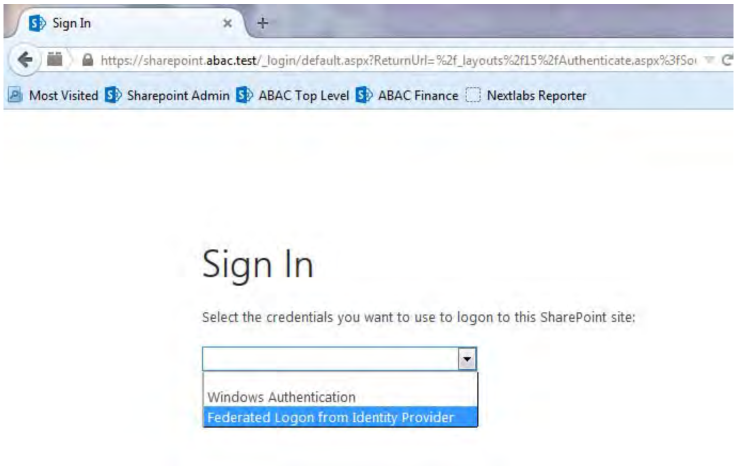
35. On the Activation and Summary screen, select **Active** for the **Connection Status** field and click **Save** to complete the configuration.

5.5 Functional Test of All Configurations for This Chapter

The instructions in this section will perform an integrated test all of the configurations in this chapter.

1. Using the browser, you logon using an account that was created in Active Directory and validate that the complete federated authentication flow between SharePoint and the PingFederate servers at the Relying Party and Identity Provider operates successfully.
2. Launch your Firebox browser and select SAML tracer from the Tools menu.

   This will launch an empty SAML tracer window. Minimize the SAML tracer window. The SAML tracer will automatically record the details of the HTTPS messages in the background.
3. Go back to the main browser window and go to the Relying Party’s SharePoint site (e.g. **https://SharePoint.abac.test**).



https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSo

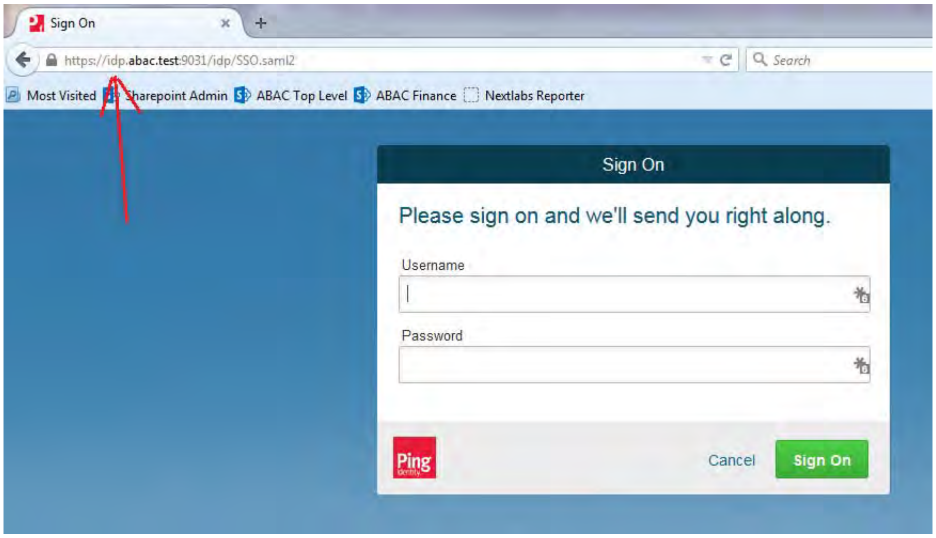
Sign In

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

Windows Authentication
Federated Logon from Identity Provider

4. Select the option to use the new trusted token issuer (e.g. **Federated Logon from Identity Provider**) that was configured in this chapter.

   Expected Result: Your browser should be redirected to the PingFederate-IdP and you should see the PingFederate Sign On screen. Examine the server name in the URL to ensure that it is the Identity Provider’s PingFederate server (e.g. **idp.abac.test**).



https://idp.abac.test:9031/idp/SSO.saml2

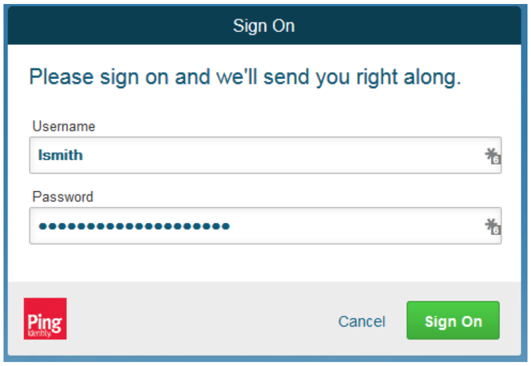
Sign On

Please sign on and we'll send you right along.

Username:

Password:

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



Sign On

Please sign on and we'll send you right along.

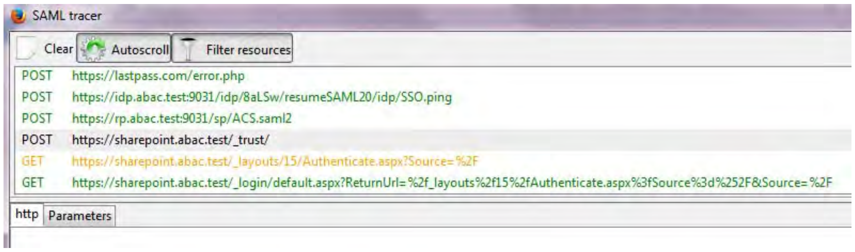
Username: lsmith

Password: ••••••••••••••••••••

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

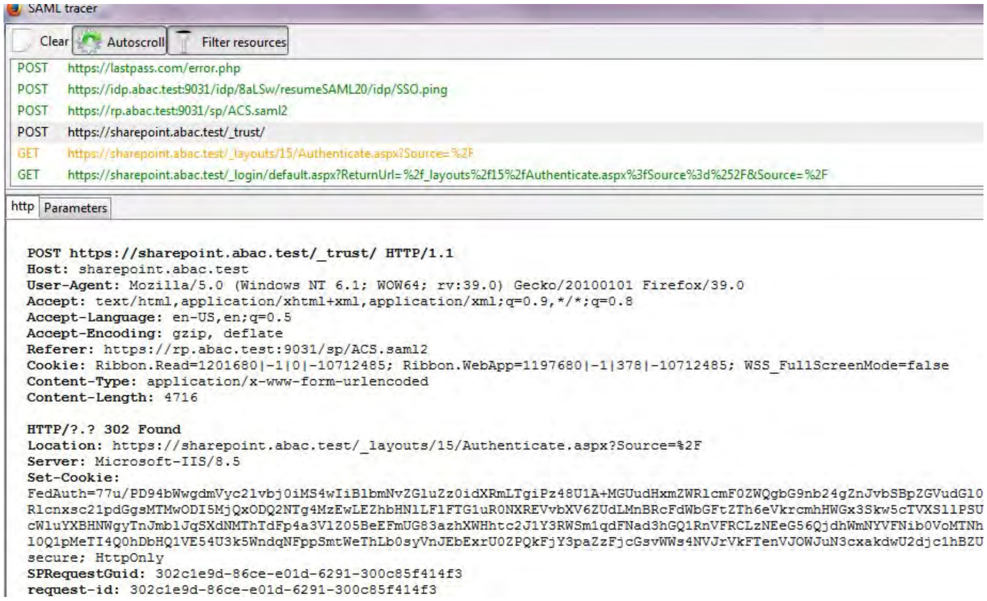
   Note: Once authenticated at the Identity Provider, your browser should automatically redirect to the PingFederate-RP (e.g. **rp.abac.test**) and then to the Relying Party's SharePoint (**SharePoint.abac.test**) site. Depending on the processing time of the servers in your environment, and other factors, 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.

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



```
POST   https://lastpass.com/error.php
POST   https://idp.abac.test:9031/idp/8aLSw/resumeSAML20/idp/SSO.ping
POST   https://rp.abac.test:9031/sp/ACS.saml2
POST   https://sharepoint.abac.test/_trust/
GET    https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
GET    https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
```

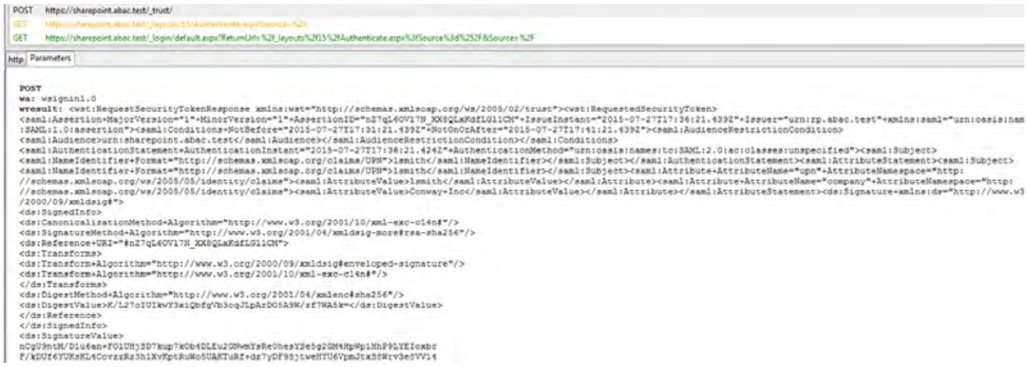
7. Click on the **POST** message to the SharePoint **_trust** URL to bring up the details of the message in the bottom pane.



```
POST   https://lastpass.com/error.php
POST   https://idp.abac.test:9031/idp/8aLSw/resumeSAML20/idp/SSO.ping
POST   https://rp.abac.test:9031/sp/ACS.saml2
POST   https://sharepoint.abac.test/_trust/
GET    https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
GET    https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
```

```
POST https://sharepoint.abac.test/_trust/ HTTP/1.1
Host: sharepoint.abac.test
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://rp.abac.test:9031/sp/ACS.saml2
Cookie: Ribbon.Read=1201680|-1|0|-10712485; Ribbon.WebApp=1197680|-1|378|-10712485; WSS_FullScreenMode=false
Content-Type: application/x-www-form-urlencoded
Content-Length: 4716

HTTP/?.? 302 Found
Location: https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
Server: Microsoft-IIS/8.5
Set-Cookie:
FedAuth=77u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48U1A+MGUudHxmZWRlcmF0ZWQgbG9nb24gZnJvbSBpZGVudGl0
Rlcnxsc21pdGgsMTMwODI5MjQxODQ2NTg4MzEwLEZhbHNlLFlFTG1uR0NXREVvbXV6ZUdLMnBRcFdWbGFtZTh6eVkrcmhHWGx3Skw5cTVXS1lPSU
cWluYXBHNWgyTnJmblJqSXdNMThTdFp4a3VlZ05BeEFmUG83azhXWHhtc2J1Y3RWSm1qdFNad3hGQ1RnVFRCLzNEeG56QjdhWmNYVFNib0VoMTNh
l0Q1pMeTI4Q0hDbHQ1VE54U3k5WndqNFppSmtWeThLb0syVnJEbExrU0ZPQkFjY3paZzFjcGsvWWs4NVJrVkFTenVJOWJuN3cxakdwU2djc1hBZU
secure; HttpOnly
SPRequestGuid: 302c1e9d-86ce-e01d-6291-300c85f414f3
request-id: 302c1e9d-86ce-e01d-6291-300c85f414f3
```

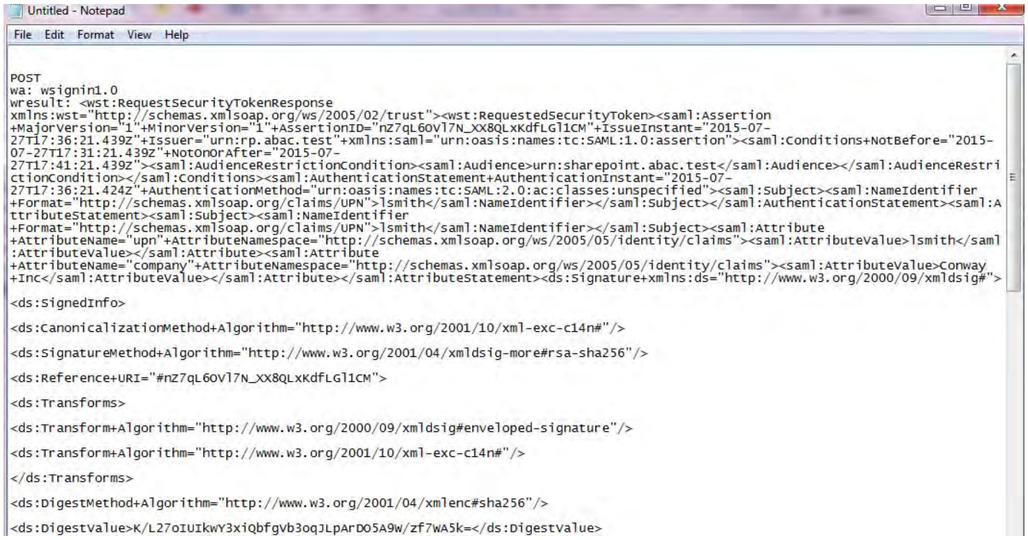
8. Click on the **Parameters** tab for the bottom pane.



```
POST   https://sharepoint.abac.test/_trust/
GET    https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
GET    https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
```

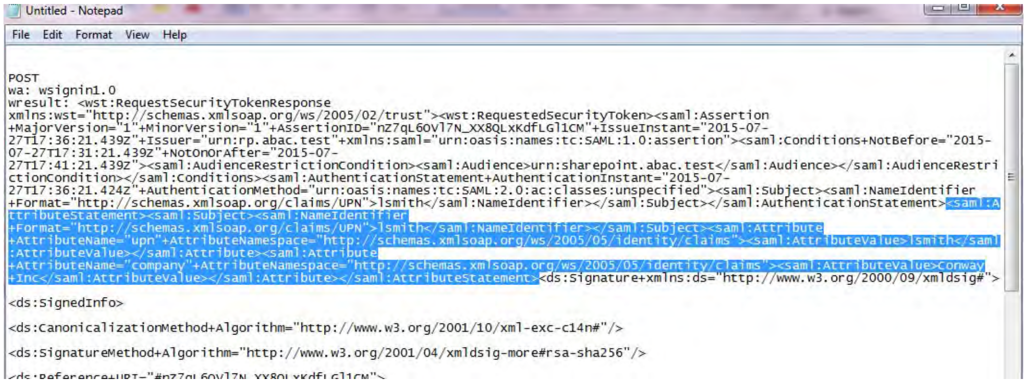
```
POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken>
<saml:Assertion+MajorVersion="1"+MinorVersion="1"+AssertionID="nZ7qL60V17N_XX8QLxKdfLG11CM"+IssueInstant="2015-07-27T17:36:21.439Z"+Issuer="urn:rp.abac.test"+xmlns:saml="urn:oasis:nam
: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:AudienceRestrictionCondition></saml:Conditions>
<saml:AuthenticationStatement+AuthenticationInstant="2015-07-27T17:36:21.424Z"+AuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"><saml:Subject>
<saml:NameIdentifier+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:AttributeStatement><saml:Subject>
<saml:NameIdentifier+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute+AttributeName="upn"+AttributeNamespace="http:
//schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>lsmith</saml:AttributeValue></saml:Attribute><saml:Attribute+AttributeName="company"+AttributeNamespace="http:
//schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Conway+Inc</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><ds:Signature+xmlns:ds="http://www.w3
/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/xmlenc#sha256"/>
<ds:DigestValue>K/L27oIUIkwY3xiQbfgVb3oqJLpArDO5A9N/zf7WA5k=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
nCgU9ntM/D1u6an+F01UHj5D7kup7kOb4DLEu2GNwmYsReOhesYSe5g2GM4HpWp1MhP9LYEIoxbr
F/kDUf6YUKsKL4CovzzRz3h1XvKptRuNo5UAKTuRf+dz7yDF98jtweHYU6VpmJtx58Wrv3e5VV14
```

9. 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.



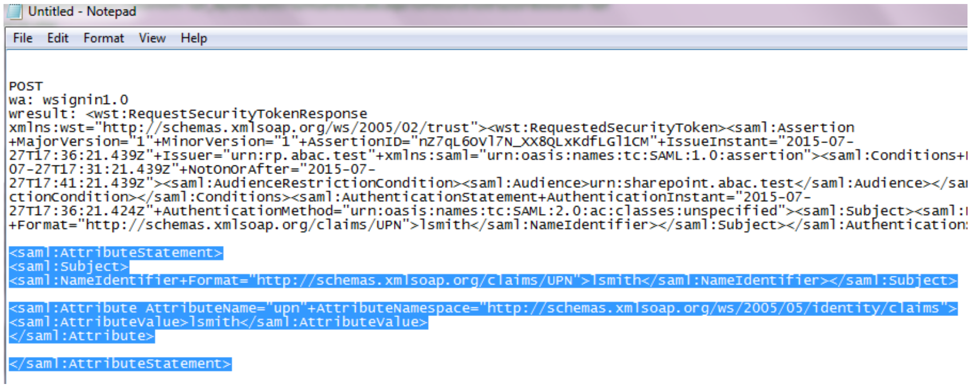
```
POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionID="nZ7qL6OVl7N_XX8QLxKdfLGl1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp.abac.test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><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">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:A
ttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>lsmith</saml
:AttributeValue></saml:Attribute><saml:Attribute
+AttributeName="company"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Conway
+Inc</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><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="#nZ7qL6OVl7N_XX8QLxKdfLGl1CM">

<ds:Transforms>

<ds:Transform+Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<ds:Transform+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod+Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>K/L27oIUIkwY3xiQbfgVb3oqJLpArDO5A9W/zf7WA5k=</ds:DigestValue>
```

10. 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="nZ7qL6OVl7N_XX8QLxKdfLGl1CM"+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">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:A
ttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>lsmith</saml
:AttributeValue></saml:Attribute><saml:Attribute
+AttributeName="company"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Conway
+Inc</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><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="#nZ7qL6OVl7N_XX8QLxKdfLGl1CM">
```

11. 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="nZ7qL6OVl7N_XX8QLxKdfLGl1CM"+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></sa
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:
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:Authentication

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

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

</saml:AttributeStatement>
```

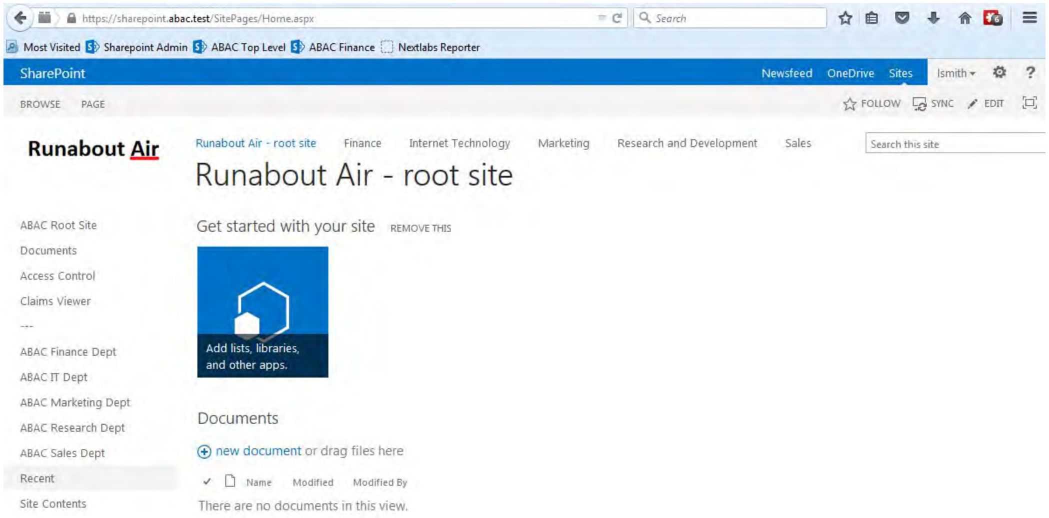
Expected Result: Within the AttributeStatement node, there should be an Attribute sub-node. The Attribute sub-node should have an AttributeName value of **upn**. The **AttributeNamespace** value should be

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. **lsmith**) that was used to authenticate at the Identity Provider (e.g. **<saml:AttributeValue>lsmith</saml:AttributeValue>**).

Expected Result: Verify that the name (and case) of the attribute (noted by the **AttributeName**) is identical to the name configured at the SharePoint using Powershell earlier in this chapter. Verify that the **AttributeNamespace** is identical to the **IncomingClaimType** option configured at the SharePoint using Powershell earlier in this chapter. If the name or namespace of the attribute being passed to SharePoint does not match with the SharePoint configuration, SharePoint will not allow access to the site, and direct your browser back to the SharePoint Sign On screen.

12. If you verified that the name and namespace of the expected attribute match with the SharePoint configuration and SharePoint does not direct your browser to the site home page, follow the instructions in section 5.6, Troubleshooting SharePoint Federated Authentication Problems, to determine the cause of the problem.

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



5.6 Troubleshooting SharePoint Federated Authentication Problems

If you encounter a situation where SharePoint is not allowing a federated user access to the site, you may have a problem with the authentication configuration. A symptom that indicates you have an authentication configuration problem is when a user successfully signs on at the Identity Provider, then the user is redirected back to the SharePoint site, and instead of displaying the site home page, SharePoint presents the SharePoint Sign On screen again. This section describes how to determine the root cause of this type of authentication problem so that the problem can be resolved.

Note: A SharePoint access control problem is a distinctly separate issue from authentication. A symptom of an access control problem is when the user received a message that states "This site has not been shared with you" upon successful authentication. Access control problems can be resolved by setting up SharePoint permissions on the People and Groups administration page, located in the Site Settings, Users and Permissions group.

Follow these instructions to troubleshoot federated authentication problems at the SharePoint site.

Before you configure diagnostic logging for the SharePoint site to determine the root cause of the authentication problem, check the following items first:

1. Verify that the Relying Party's PingFederate Server and the Relying Party's SharePoint Server synchronize their clocks from the same source. If both servers are on the same domain, they should be synchronized with the domain controller automatically. Log on to both servers and verify that the clocks display the same time.

2. Verify that the expiration time of the security token generated by the PingFederate Server is more than 10 minutes.

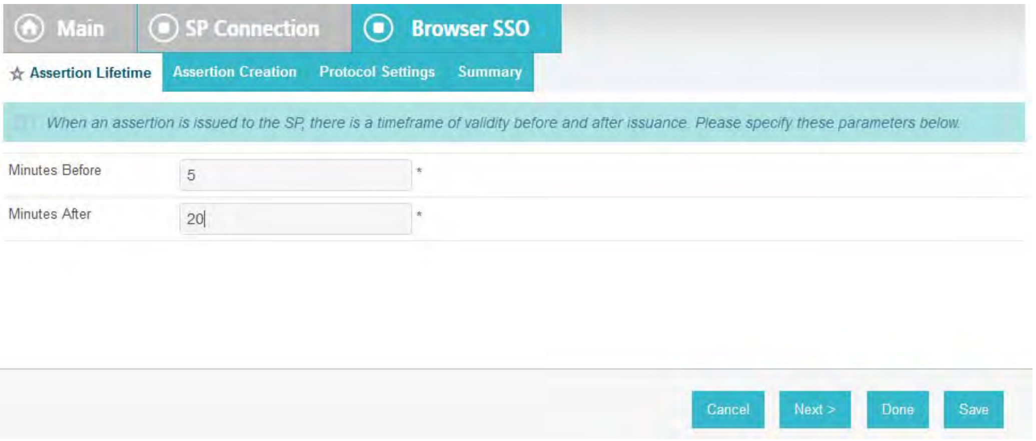
   SharePoint calculates the time length of its session using the formula: **SharePointSessionTime = SecurityTokenLifeTime - LogonTokenCacheExpirationWindow.**

   SecurityTokenLifeTime is the length of time the token is valid, and this time is generated by the PingFederate server when it issues the token.

   By default the **SharePoint LogonTokenCacheExpirationWindow** is set to 10 minutes, therefore the **SecurityTokenLifeTime** must be greater than 10 in order to generate a **SharePointSessionTime** greater than zero.

   In our build we set the **SecurityTokenLifetime** to 20 minutes in the PingFederate configuration.

3. The expiration time of the security token can be set in the configuration of the SP Connection on the Relying Party's PingFederate server. When you open the configuration for the SP Connection, click on the **Assertion Lifetime** link in the Browser SSO section. Enter a value for the **Minutes After** field that is greater than **10** (e.g. **20**).



When an assertion is issued to the SP, there is a timeframe of validity before and after issuance. Please specify these parameters below.

Minutes Before: 5 *

Minutes After: 20 *

If you checked the items in the previous section and you are still encountering authentication problems, you will need to examine detailed authentication logs on the SharePoint server. Follow the instructions below to configure diagnostic logging on the SharePoint server and analyze the logs to determine the root of the authentication problem.

1. Perform the instructions at the following link to change the levels of ULS authentication logging on the SharePoint server. Make sure that you perform the instructions in the following two sections of the article:

   - *To configure SharePoint 2013 for the maximum amount of user authentication logging*
   - *To find the failed authentication attempt manually*

   https://technet.microsoft.com/en-us/library/JJ906556.aspx

2. Once you configure the SharePoint diagnostic authentication logging, perform the sign on process to your SharePoint again to generate activity in the log.

   Tip: Since the SharePoint ULS log file contains many entries, it can be helpful to copy the file to another computer and analyze it offline.

3. Open a copy of the log file and scroll to the bottom of the file. The bottom of the log contains the most recent activity.

4. Starting at the bottom of the file, perform an upward search for the term **authentication**. Examine the entries that are labeled either **Claims Authentication** or **Authentication Authorization**.

5. Look at the details for each of these two types of authentication entries to look for clues regarding what the source of the problem could be. You may have to look through several entries in the file to understand the sequence of events.

We used this approach to troubleshoot an authentication problem in our lab. We found the following entry in the log file, that seemed as though it could be the source of the problem:

- `security token '0e.t|federated logon from Identity Provider|lsmithcc221cd9-23d7-4302-b029-ee81784754d2_Internet' is found in the local cache, but it is expired. Returing Null.`

Two lines further down in the file, we found the following entry as well:

- `Token Cache: Failed to find token for user '0e.t|federated logon from Identity Provider|lsmith' for cookie so signing out the user.`

Based on the log file, we performed an Internet search for the term s**ecurity token is found in the local cache, but it is expired. Returing Null**. By researching various Internet blogs and forums, and performing additional analysis of the log file, we found a blog article on the PingIdentity website that described why the lifetime of the security token generated by the PingFederate-RP must be greater than 10 minutes when issuing a token for SharePoint. Once we updated the associated configuration on the PingFederate-RP, the authentication problem was resolved.

Identity ProviderIdentity Provider

6 Attribute Exchange Between the Identity Provider and Relying Party

6.1 Introduction

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

- Configuring federated authentication at the PingFederate-IdP
- Configuring the SAML exchange between the PingFederate-Idp and PingFederate-RP
- Configuring the Relying Partys SharePoint site
- Configuring the federated logon at the SharePoint site

Building upon that foundation, this chapter describes how to:

- Create custom attributes and set values for them in the Microsoft AD
- Configure the PingFederate-IdP to pull user and environmental attributes during authentication
- Configure the PingFederate-RP to pass the user and environmental attributes to the Relying Party's SharePoint
- Configure SharePoint to load the user and environmental attributes passed from the PingFederate-RP into the web session

If you follow the instructions in this chapter, you will be able to perform a functional test to verify the successful completion of the steps for installing, configuring, and integrating the components.

6.2 Create Custom User Attributes in Microsoft AD

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

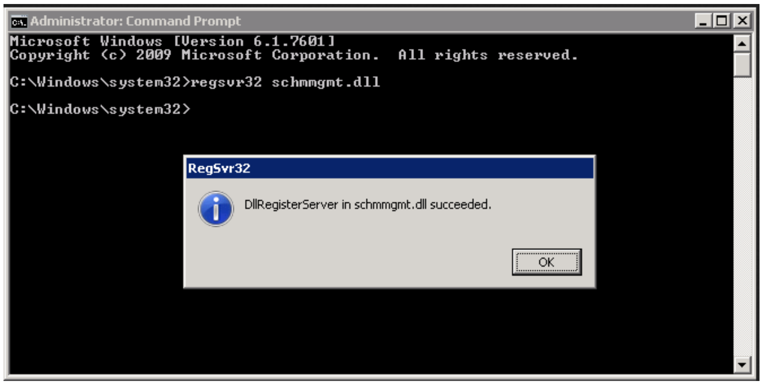
6.2.1 Preparing the AD Schema for Creating New Custom Attributes

6.2.1.1 Backing up Your Directory before Making Schema Changes

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

1. Log on to the server that contains the Microsoft AD schema (typically the schema is on the domain controller).
2. Launch a command prompt, using the **Run as Administrator** option.
3. Execute the following command

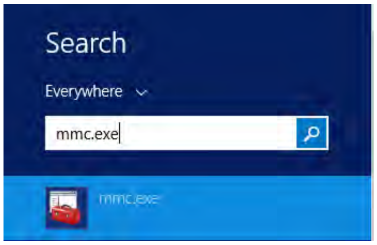
   regsvr32 schmmgmt.dll



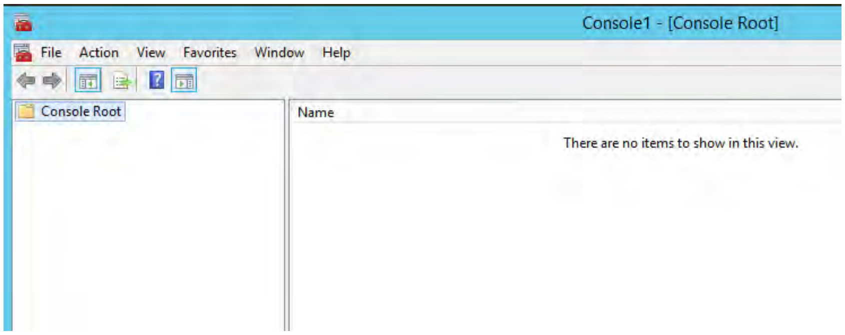
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>regsvr32 schmmgmt.dll

C:\Windows\system32>
```

DllRegisterServer in schmmgmt.dll succeeded.

4. Click the **Start** button and enter **mmc.exe** in the search field.
5. Launch the **mmc.exe** program.

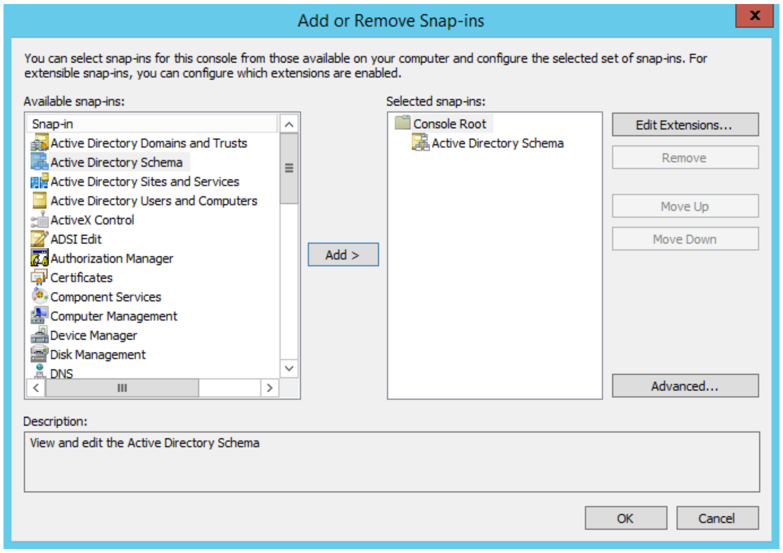


mmc.exe



There are no items to show in this view.

6. Click on the **File** menu. Then, click **Add / Remove Snap-in**.
7. Click on **Active Directory Schema** in the list of **Available snap-ins** on the left; then, click **Add** to add it to the **Selected snap-ins on the right**.
8. Click **OK**.



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

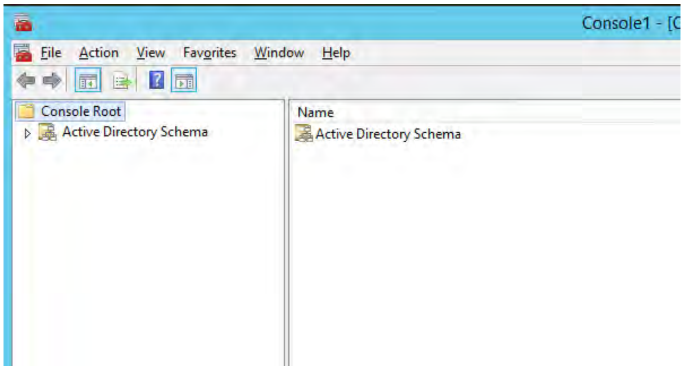
- Snap-in
- Active Directory Domains and Trusts
- Active Directory Schema
- Active Directory Sites and Services
- Active Directory Users and Computers
- ActiveX Control
- ADSI Edit
- Authorization Manager
- Certificates
- Component Services
- Computer Management
- Device Manager
- Disk Management
- DNS

Selected snap-ins:

- Console Root
  - Active Directory Schema

Description:

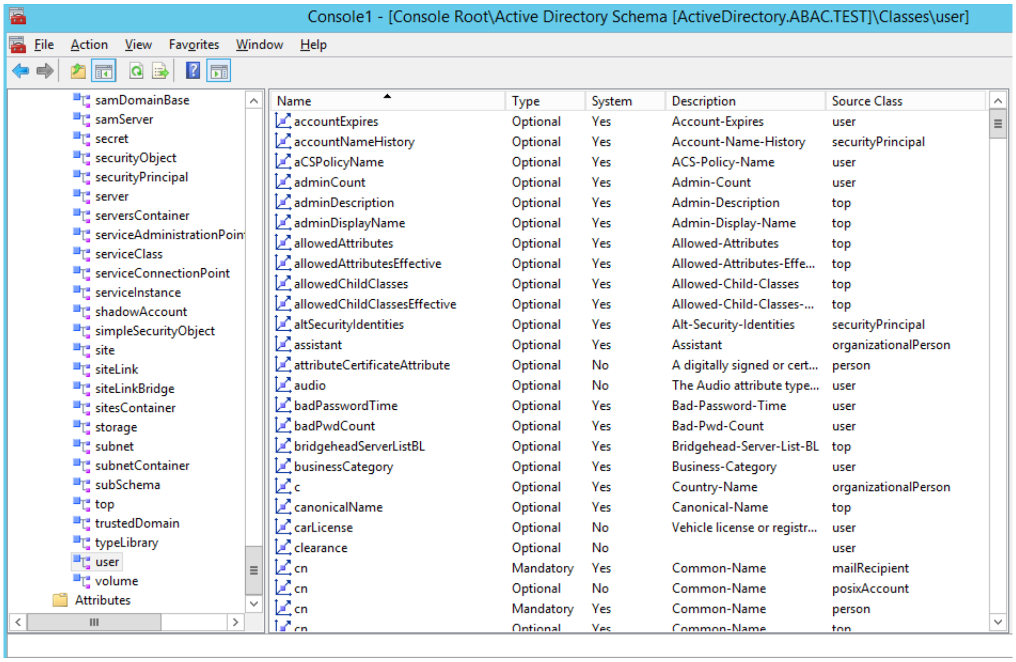
View and edit the Active Directory Schema



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

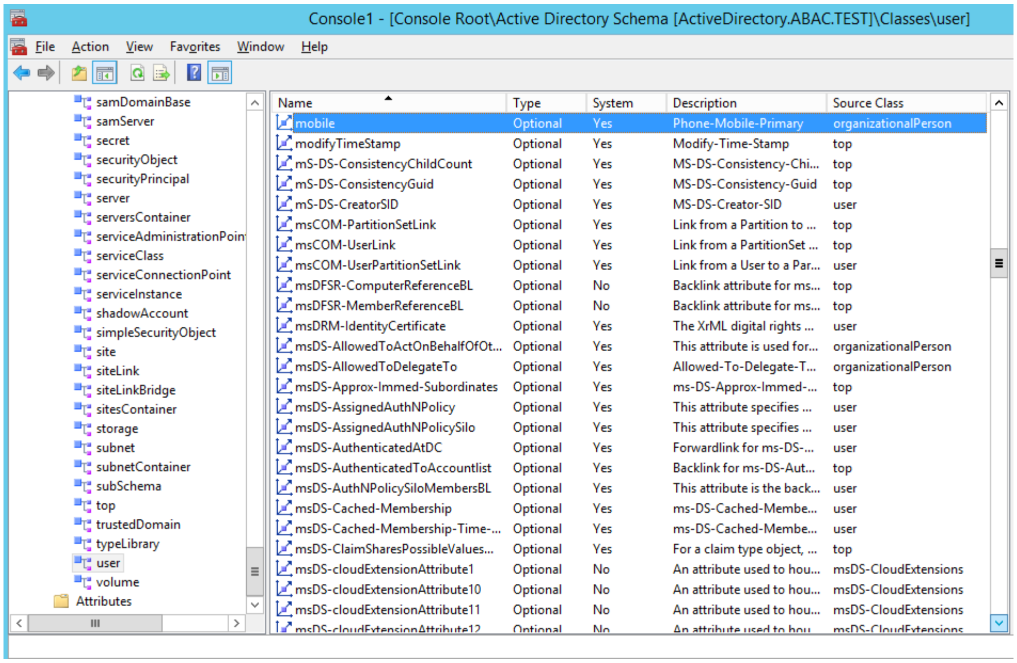
6.2.1.2 Reviewing Existing Attributes to Avoid Redundancies when Creating New Attributes

Before you create a new attribute it is important to review existing user attributes in your Active Directory Schema. Under Active Directory Schema on the left, expand the Classes folder and scroll down to click on the **user** class. Examine the existing set of **user** class attributes listed on the right. These attributes are native to Active Directory, and can be assigned to users as subject attributes. These attributes may meet existing requirement for implementing subject attribute, alleviating the need to add custom attributes to the schema. You can list the attributes in alphabetic order by clicking on the **Name** column.



Name	Type	System	Description	Source Class
accountExpires	Optional	Yes	Account-Expires	user
accountNameHistory	Optional	Yes	Account-Name-History	securityPrincipal
aCSPolicyName	Optional	Yes	ACS-Policy-Name	user
adminCount	Optional	Yes	Admin-Count	user
adminDescription	Optional	Yes	Admin-Description	top
adminDisplayName	Optional	Yes	Admin-Display-Name	top
allowedAttributes	Optional	Yes	Allowed-Attributes	top
allowedAttributesEffective	Optional	Yes	Allowed-Attributes-Effe...	top
allowedChildClasses	Optional	Yes	Allowed-Child-Classes	top
allowedChildClassesEffective	Optional	Yes	Allowed-Child-Classes-...	top
altSecurityIdentities	Optional	Yes	Alt-Security-Identities	securityPrincipal
assistant	Optional	Yes	Assistant	organizationalPerson
attributeCertificateAttribute	Optional	No	A digitally signed or cert...	person
audio	Optional	No	The Audio attribute type...	user
badPasswordTime	Optional	Yes	Bad-Password-Time	user
badPwdCount	Optional	Yes	Bad-Pwd-Count	user
bridgeheadServerListBL	Optional	Yes	Bridgehead-Server-List-BL	top
businessCategory	Optional	Yes	Business-Category	user
c	Optional	Yes	Country-Name	organizationalPerson
canonicalName	Optional	Yes	Canonical-Name	top
carLicense	Optional	No	Vehicle license or registr...	user
clearance	Optional	No		user
cn	Mandatory	Yes	Common-Name	mailRecipient
cn	Optional	No	Common-Name	posixAccount
cn	Mandatory	Yes	Common-Name	person
cn	Optional	Yes	Common-Name	top

Let's say you wanted to create an attribute to store the user's cell phone number, you would look through the attributes and notice that the attribute **cellphone** does not exist. However, there is an existing attribute named **mobile** that could be used to store a cell phone number.



Name	Type	System	Description	Source Class
mobile	Optional	Yes	Phone-Mobile-Primary	organizationalPerson
modifyTimeStamp	Optional	Yes	Modify-Time-Stamp	top
mS-DS-ConsistencyChildCount	Optional	Yes	MS-DS-Consistency-Chi...	top
mS-DS-ConsistencyGuid	Optional	Yes	MS-DS-Consistency-Guid	top
mS-DS-CreatorSID	Optional	Yes	MS-DS-Creator-SID	user
msCOM-PartitionSetLink	Optional	Yes	Link from a Partition to ...	top
msCOM-UserLink	Optional	Yes	Link from a PartitionSet ...	top
msCOM-UserPartitionSetLink	Optional	Yes	Link from a User to a Par...	user
msDFSR-ComputerReferenceBL	Optional	No	Backlink attribute for ms...	top
msDFSR-MemberReferenceBL	Optional	No	Backlink attribute for ms...	top
msDRM-IdentityCertificate	Optional	Yes	The XrML digital rights ...	user
msDS-AllowedToActOnBehalfOfOt...	Optional	Yes	This attribute is used for...	organizationalPerson
msDS-AllowedToDelegateTo	Optional	Yes	Allowed-To-Delegate-T...	organizationalPerson
msDS-Approx-Immed-Subordinates	Optional	Yes	ms-DS-Approx-Immed-...	top
msDS-AssignedAuthNPolicy	Optional	Yes	This attribute specifies ...	user
msDS-AssignedAuthNPolicySilo	Optional	Yes	This attribute specifies ...	user
msDS-AuthenticatedAtDC	Optional	Yes	Forwardlink for ms-DS-...	user
msDS-AuthenticatedToAccountlist	Optional	Yes	Backlink for ms-DS-Aut...	top
msDS-AuthNPolicySiloMembersBL	Optional	Yes	This attribute is the back...	user
msDS-Cached-Membership	Optional	Yes	ms-DS-Cached-Membe...	user
msDS-Cached-Membership-Time-...	Optional	Yes	ms-DS-Cached-Membe...	user
msDS-ClaimSharesPossibleValues...	Optional	Yes	For a claim type object, ...	top
msDS-cloudExtensionAttribute1	Optional	No	An attribute used to hou...	msDS-CloudExtensions
msDS-cloudExtensionAttribute10	Optional	No	An attribute used to hou...	msDS-CloudExtensions
msDS-cloudExtensionAttribute11	Optional	No	An attribute used to hou...	msDS-CloudExtensions
msDS-cloudExtensionAttribute12	Optional	No	An attribute used to hou...	msDS-CloudExtensions

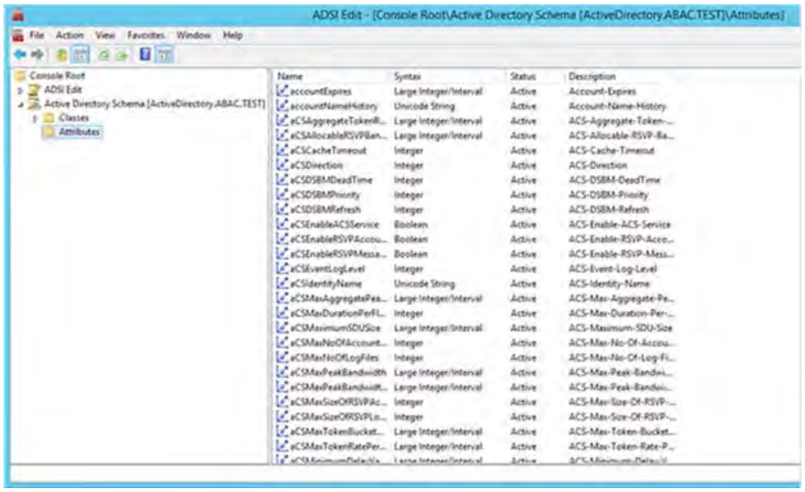
Once you have identified that the creation of a new attribute is warranted, proceed with the instructions in the following section.

6.2.1.3 Creating New Custom Attributes

1. Launch a browser window and go the Microsoft site:

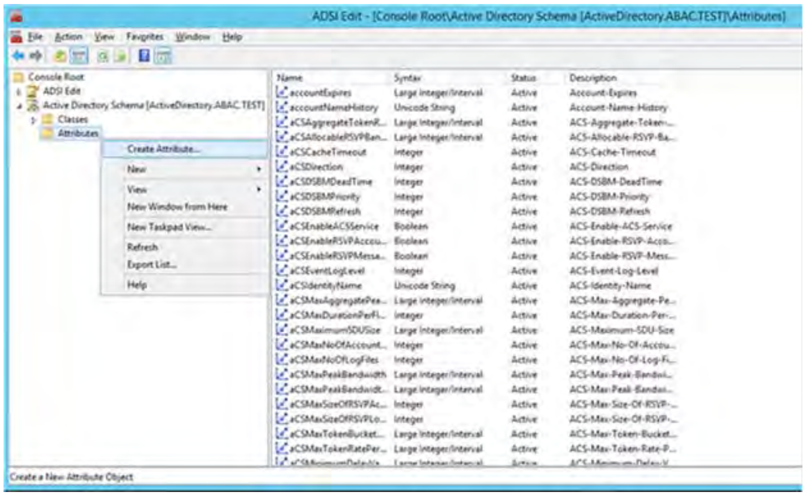
   https://gallery.technet.microsoft.com/scriptcenter/56b78004-40d0-41cf-b95e-6e795b2e8a06

2. Copy the **oidgen.vbs** script code that is shown on the page to the clipboard.
3. Open Notepad and paste the script into the editor.
4. Save the script to a file on the desktop named **oidgen.vbs**.
5. Go back to the Active Directory schema window.
6. On the left pane and click on the **Attributes** folder.


ADSI Edit - [Console Root\Active Directory Schema [ActiveDirectory.ABAC.TEST]\Attributes]
File
Action
View
Favorites
Window
Help
Console Root
ADSI Edit
Active Directory Schema [ActiveDirectory.ABAC.TEST]
Classes
Attributes

Name	Syntax	Status	Description
accountExpires	Large Integer/Interval	Active	Account-Expires
accountNameHistory	Unicode String	Active	Account-Name-History
aCSAggregateTokenR...	Large Integer/Interval	Active	ACS-Aggregate-Token-...
aCSAllocableRSVPBan...	Large Integer/Interval	Active	ACS-Allocable-RSVP-Ba...
aCSCacheTimeout	Integer	Active	ACS-Cache-Timeout
aCSDirection	Integer	Active	ACS-Direction
aCSDSBMDeadTime	Integer	Active	ACS-DSBM-DeadTime
aCSDSBMPriority	Integer	Active	ACS-DSBM-Priority
aCSDSBMRefresh	Integer	Active	ACS-DSBM-Refresh
aCSEnableACSService	Boolean	Active	ACS-Enable-ACS-Service
aCSEnableRSVPAccou...	Boolean	Active	ACS-Enable-RSVP-Acco...
aCSEnableRSVPMessa...	Boolean	Active	ACS-Enable-RSVP-Mess...
aCSEventLogLevel	Integer	Active	ACS-Event-Log-Level
aCSIdentityName	Unicode String	Active	ACS-Identity-Name
aCSMaxAggregatePea...	Large Integer/Interval	Active	ACS-Max-Aggregate-Pe...
aCSMaxDurationPerFl...	Integer	Active	ACS-Max-Duration-Per-...
aCSMaximumSDUSize	Large Integer/Interval	Active	ACS-Maximum-SDU-Size
aCSMaxNoOfAccount...	Integer	Active	ACS-Max-No-Of-Accou...
aCSMaxNoOfLogFiles	Integer	Active	ACS-Max-No-Of-Log-Fi...
aCSMaxPeakBandwidth	Large Integer/Interval	Active	ACS-Max-Peak-Bandwi...
aCSMaxPeakBandwidt...	Large Integer/Interval	Active	ACS-Max-Peak-Bandwi...
aCSMaxSizeOfRSVPAc...	Integer	Active	ACS-Max-Size-Of-RSVP-...
aCSMaxSizeOfRSVPLo...	Integer	Active	ACS-Max-Size-Of-RSVP-...
aCSMaxTokenBucket...	Large Integer/Interval	Active	ACS-Max-Token-Bucket...
aCSMaxTokenRatePer...	Large Integer/Interval	Active	ACS-Max-Token-Rate-P...
aCSMinimumDelayVa...	Large Integer/Interval	Active	ACS-Minimum-Delay-V...

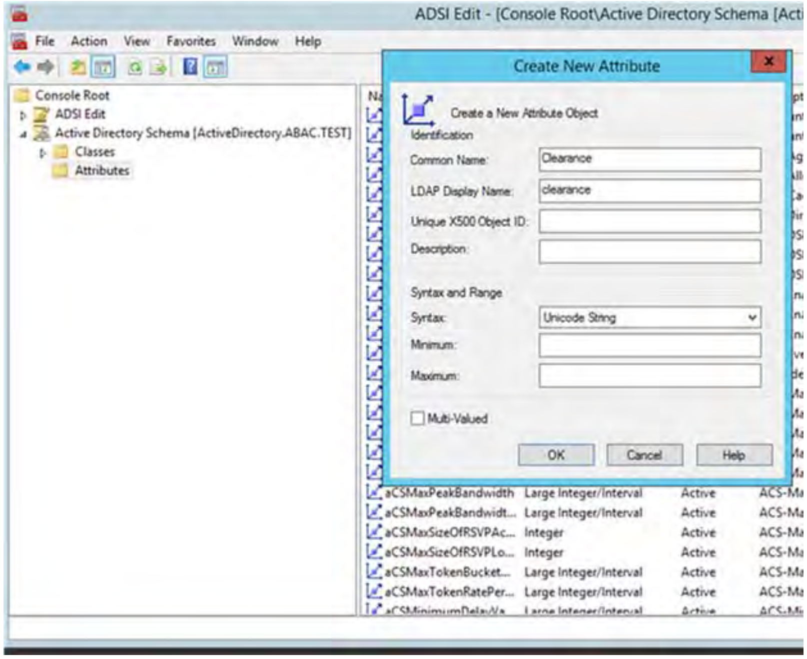
7. Right click on the **Attributes** folder and select **Create Attribute**.
8. Click **Continue** on the warning window.



Name	Syntax	Status	Description
accountExpires	Large Integer/Interval	Active	Account-Expires
accountNameHistory	Unicode String	Active	Account-Name-History
aCSAggregateTokenR...	Large Integer/Interval	Active	ACS-Aggregate-Token-...
aCSAllocableRSVPBan...	Large Integer/Interval	Active	ACS-Allocable-RSVP-Ba...
aCSCacheTimeout	Integer	Active	ACS-Cache-Timeout
aCSDirection	Integer	Active	ACS-Direction
aCSDSBMDeadTime	Integer	Active	ACS-DSBM-DeadTime
aCSDSBMPriority	Integer	Active	ACS-DSBM-Priority
aCSDSBMRefresh	Integer	Active	ACS-DSBM-Refresh
aCSEnableACSService	Boolean	Active	ACS-Enable-ACS-Service
aCSEnableRSVPAccou...	Boolean	Active	ACS-Enable-RSVP-Acco...
aCSEnableRSVPMessa...	Boolean	Active	ACS-Enable-RSVP-Mess...
aCSEventLogLevel	Integer	Active	ACS-Event-Log-Level
aCSIdentityName	Unicode String	Active	ACS-Identity-Name
aCSMaxAggregatePea...	Large Integer/Interval	Active	ACS-Max-Aggregate-Pe...
aCSMaxDurationPerFl...	Integer	Active	ACS-Max-Duration-Per-...
aCSMaximumSDUSize	Large Integer/Interval	Active	ACS-Maximum-SDU-Size
aCSMaxNoOfAccount...	Integer	Active	ACS-Max-No-Of-Accou...
aCSMaxNoOfLogFiles	Integer	Active	ACS-Max-No-Of-Log-Fi...
aCSMaxPeakBandwidth	Large Integer/Interval	Active	ACS-Max-Peak-Bandwi...
aCSMaxPeakBandwidt...	Large Integer/Interval	Active	ACS-Max-Peak-Bandwi...
aCSMaxSizeOfRSVPAc...	Integer	Active	ACS-Max-Size-Of-RSVP-...
aCSMaxSizeOfRSVPLo...	Integer	Active	ACS-Max-Size-Of-RSVP-...
aCSMaxTokenBucket...	Large Integer/Interval	Active	ACS-Max-Token-Bucket...
aCSMaxTokenRatePer...	Large Integer/Interval	Active	ACS-Max-Token-Rate-P...
aCSMinimumDelayVa...	Large Integer/Interval	Active	ACS-Minimum-Delay-V...

Create a New Attribute Object

9. 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**.



ADSI Edit - [Console Root\Active Directory Schema [Acti

File Action View Favorites Window Help
Console Root
ADSI Edit
Active Directory Schema [ActiveDirectory.ABAC.TEST]
Classes
Attributes

Create New Attribute

Create a New Attribute Object

Identification

Common Name: Clearance

LDAP Display Name: clearance

Unique X500 Object ID:

Description:

Syntax and Range

Syntax: Unicode String

Minimum:

Maximum:

☐ Multi-Valued

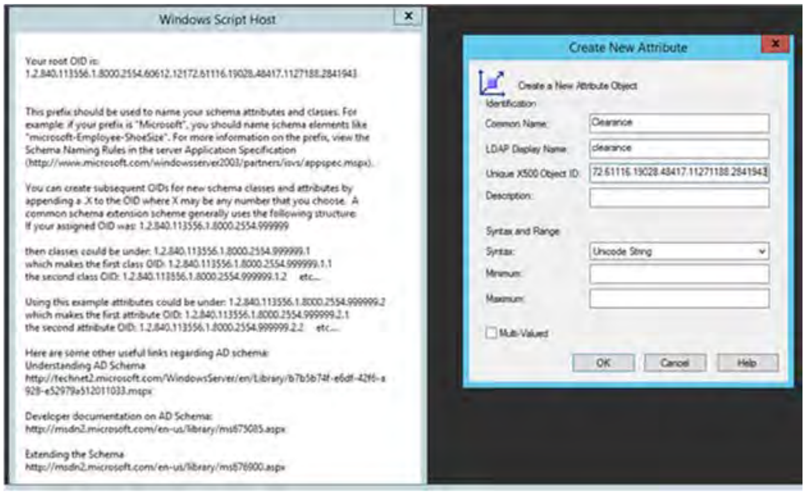
```
aCSMaxPeakBandwidth   Large Integer/Interval   Active   ACS-Ma
aCSMaxPeakBandwidt... Large Integer/Interval   Active   ACS-Ma
aCSMaxSizeOfRSVPAc... Integer                  Active   ACS-Ma
aCSMaxSizeOfRSVPLo... Integer                  Active   ACS-Ma
aCSMaxTokenBucket...  Large Integer/Interval   Active   ACS-Ma
aCSMaxTokenRatePer... Large Integer/Interval   Active   ACS-Ma
aCSMinimumDelayVa...  Large Integer/Interval   Active   ACS-Mi
```

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

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

1. Go to the desktop and double click on the **oidgen.vbs script** that was saved earlier. This should execute the script to generate a unique Object ID.

2. Enter this long Object ID into the **Unique X500 Object ID** field in the Active Directory Create New Attribute window.



Windows Script Host

```
Your root OID is:
1.2.840.113556.1.8000.2554.60612.12172.61116.19028.48417.1127188.2841943

This prefix should be used to name your schema attributes and classes. For
example: if your prefix is "Microsoft", you should name schema elements like
"microsoft-Employee-ShoeSize". For more information on the prefix, view the
Schema Naming Rules in the server Application Specification
(http://www.microsoft.com/windowsserver2003/partners/isvs/appspec.mspx).

You can create subsequent OIDs for new schema classes and attributes by
appending a .X to the OID where X may be any number that you choose.  A
common schema extension scheme generally uses the following structure:
If your assigned OID was: 1.2.840.113556.1.8000.2554.999999

then classes could be under: 1.2.840.113556.1.8000.2554.999999.1
which makes the first class OID: 1.2.840.113556.1.8000.2554.999999.1.1
the second class OID: 1.2.840.113556.1.8000.2554.999999.1.2     etc...

Using this example attributes could be under: 1.2.840.113556.1.8000.2554.999999.2
which makes the first attribute OID: 1.2.840.113556.1.8000.2554.999999.2.1
the second attribute OID: 1.2.840.113556.1.8000.2554.999999.2.2     etc...

Here are some other useful links regarding AD schema:
Understanding AD Schema
http://technet2.microsoft.com/WindowsServer/en/Library/b7b5b74f-e6df-42f6-a
928-e52979a512011033.mspx

Developer documentation on AD Schema:
http://msdn2.microsoft.com/en-us/library/ms675085.aspx

Extending the Schema
http://msdn2.microsoft.com/en-us/library/ms676900.aspx
```

Create New Attribute

Create a New Attribute Object

Identification

Common Name: Clearance

LDAP Display Name: clearance

Unique X500 Object ID: 72.61116.19028.48417.1127188.2841943

Description:

Syntax and Range

Syntax: Unicode String

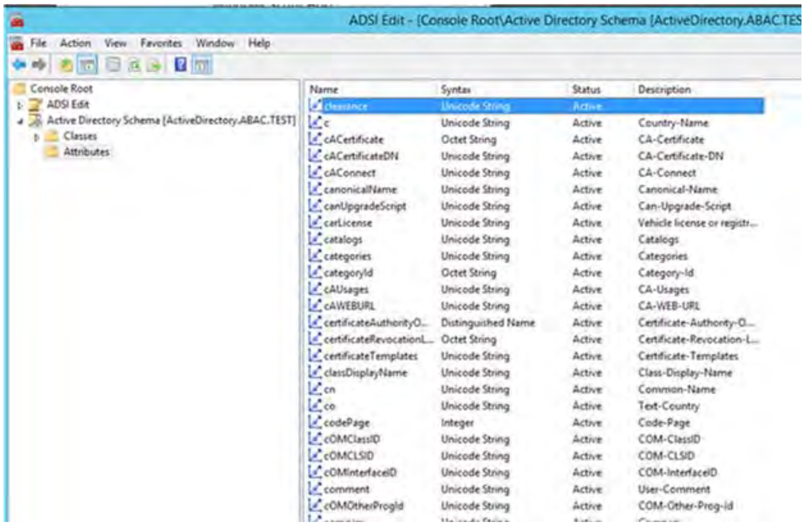
Minimum:

Maximum:

☐ Multi-Valued

3. Click **OK** to create the new attribute.

4. Scroll down the list of attributes and make sure your newly added attribute is listed there.


File Action View Favorites Window Help
Console Root
ADSI Edit
Active Directory Schema [ActiveDirectory.ABAC.TEST]
Classes
Attributes

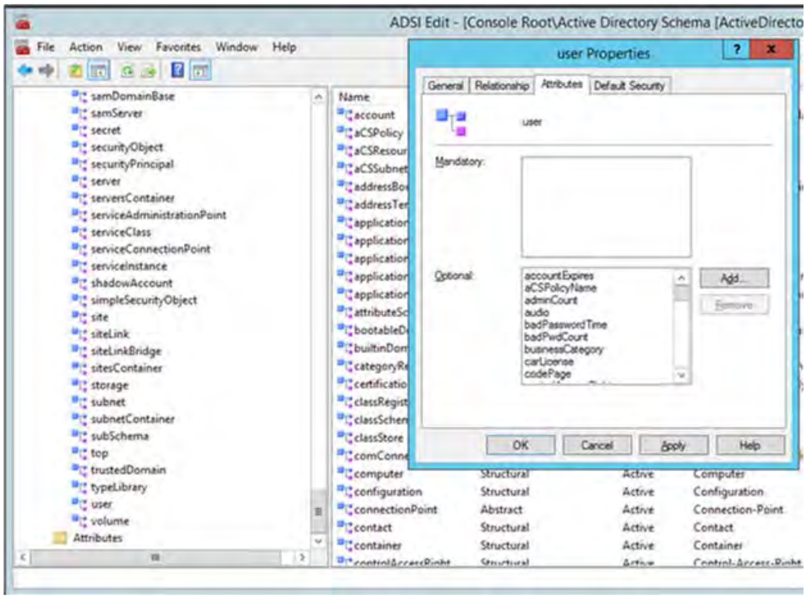
ADSI Edit - [Console Root\Active Directory Schema [ActiveDirectory.ABAC.TES

Name	Syntax	Status	Description
clearance	Unicode String	Active	
c	Unicode String	Active	Country-Name
cACertificate	Octet String	Active	CA-Certificate
cACertificateDN	Unicode String	Active	CA-Certificate-DN
cAConnect	Unicode String	Active	CA-Connect
canonicalName	Unicode String	Active	Canonical-Name
canUpgradeScript	Unicode String	Active	Can-Upgrade-Script
carLicense	Unicode String	Active	Vehicle license or registr...
catalogs	Unicode String	Active	Catalogs
categories	Unicode String	Active	Categories
categoryId	Octet String	Active	Category-Id
cAUsages	Unicode String	Active	CA-Usages
cAWEBURL	Unicode String	Active	CA-WEB-URL
certificateAuthorityO...	Distinguished Name	Active	Certificate-Authority-O...
certificateRevocationL...	Octet String	Active	Certificate-Revocation-L...
certificateTemplates	Unicode String	Active	Certificate-Templates
classDisplayName	Unicode String	Active	Class-Display-Name
cn	Unicode String	Active	Common-Name
co	Unicode String	Active	Text-Country
codePage	Integer	Active	Code-Page
cOMClassID	Unicode String	Active	COM-ClassID
cOMCLSID	Unicode String	Active	COM-CLSID
cOMInterfaceID	Unicode String	Active	COM-InterfaceID
comment	Unicode String	Active	User-Comment
cOMOtherProgId	Unicode String	Active	COM-Other-Prog-Id

6.2.1.5 Adding the New Attribute to the User Class

Next you need to add the new attribute to the **user** class.

1. In the left pane, expand the **Classes** folder. Scroll down the list of classes and right click on the user class and select **Properties**.
2. Click on the Attributes tab.



ADSI Edit - [Console Root\Active Directory Schema [ActiveDirecto

user Properties

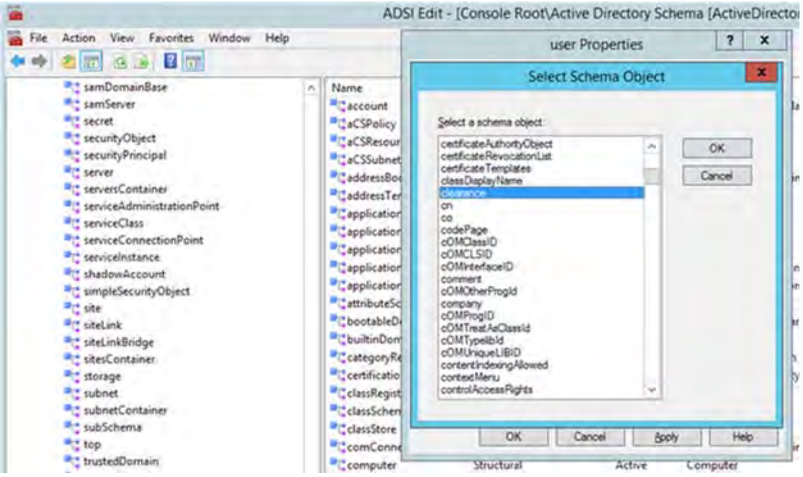
user

Mandatory:

Optional:
accountExpires
aCSPolicyName
adminCount
audio
badPasswordTime
badPwdCount
businessCategory
carLicense
codePage

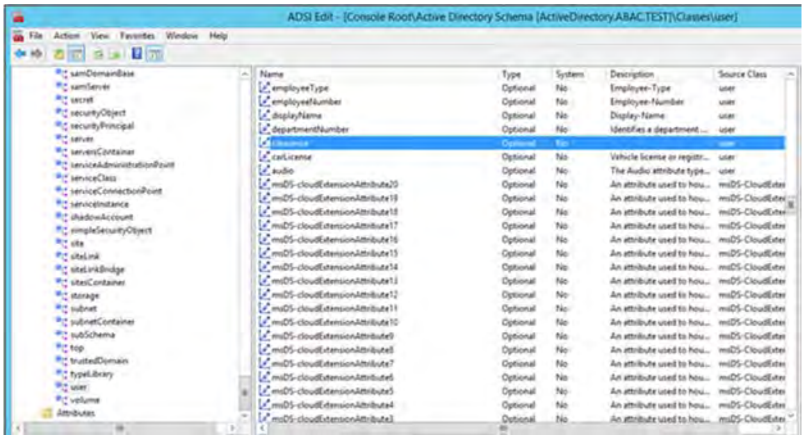
computer	Structural	Active	Computer
configuration	Structural	Active	Configuration
connectionPoint	Abstract	Active	Connection-Point
contact	Structural	Active	Contact
container	Structural	Active	Container

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



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've added the new attribute to the user class.

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

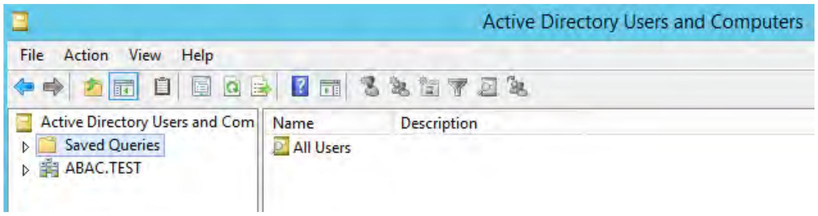


Name	Type	System	Description	Source Class
employeeType	Optional	No	Employee-Type	user
employeeNumber	Optional	No	Employee-Number	user
displayName	Optional	No	Display-Name	user
departmentNumber	Optional	No	Identifies a department ...	user
clearance	Optional	No		user
carLicense	Optional	No	Vehicle license or registr...	user
audio	Optional	No	The Audio attribute type...	user
msDS-cloudExtensionAttribute20	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute19	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute18	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute17	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute16	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute15	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute14	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute13	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute12	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute11	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute10	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute9	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute8	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute7	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute6	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute5	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute4	Optional	No	An attribute used to hou...	msDS-CloudExte
msDS-cloudExtensionAttribute3	Optional	No	An attribute used to hou...	msDS-CloudExte

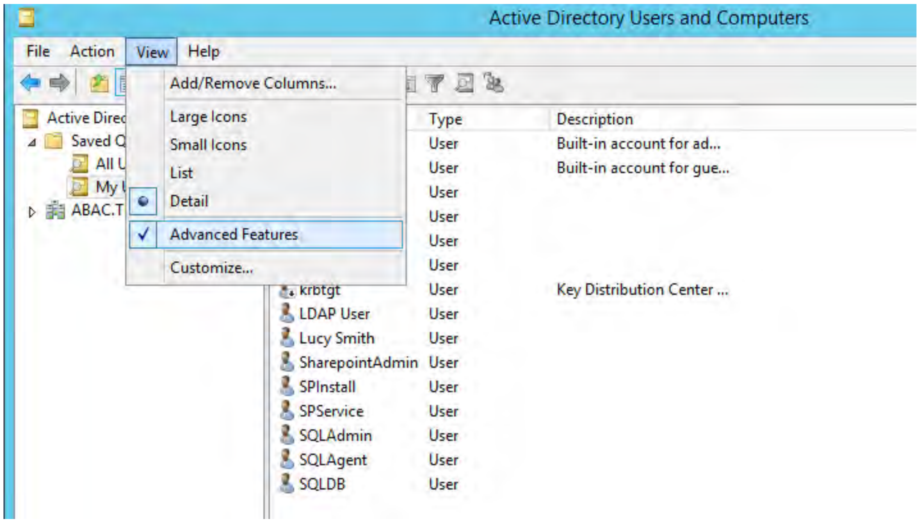
6.2.2 Set Values for Custom User Attributes in Microsoft AD

Once you've 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.

1. Log on to the Microsoft AD server.
2. Open the Active Directory Users and Computers program.

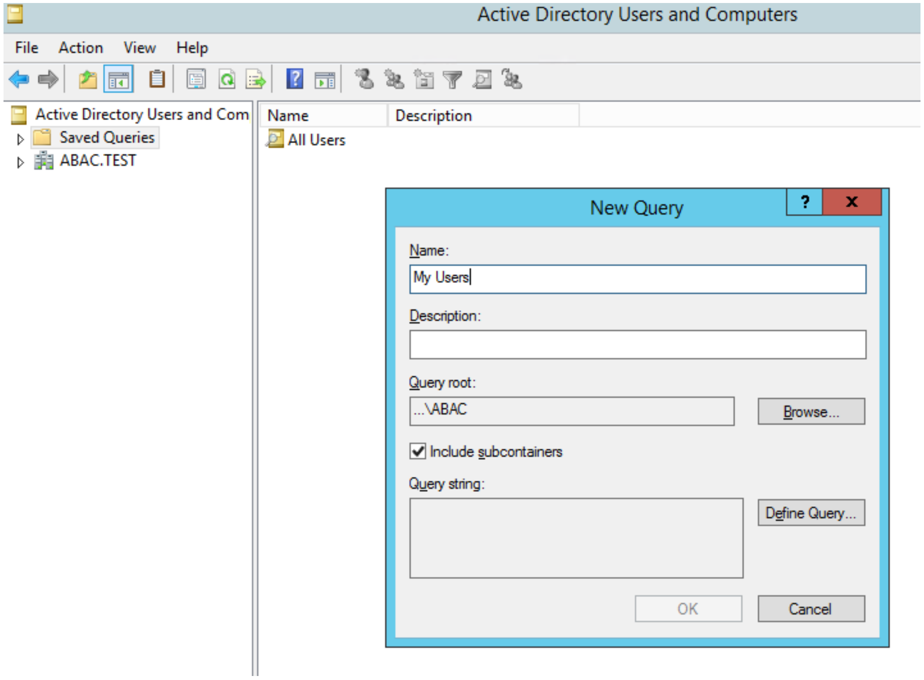


3. Click on the **View** menu and select **Advanced Features**.



Name	Type	Description
	User	Built-in account for ad...
	User	Built-in account for gue...
	User	
	User	
	User	
	User	
krbtgt	User	Key Distribution Center ...
LDAP User	User	
Lucy Smith	User	
SharepointAdmin	User	
SPInstall	User	
SPService	User	
SQLAdmin	User	
SQLAgent	User	
SQLDB	User	

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



Name: My Users

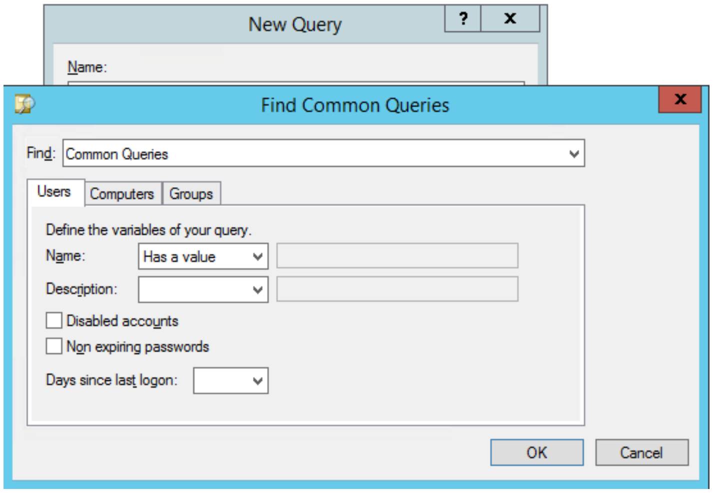
Description:

Query root: ...\ABAC

☑ Include subcontainers

Query string:

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



Find: Common Queries

Define the variables of your query.

Name: Has a value

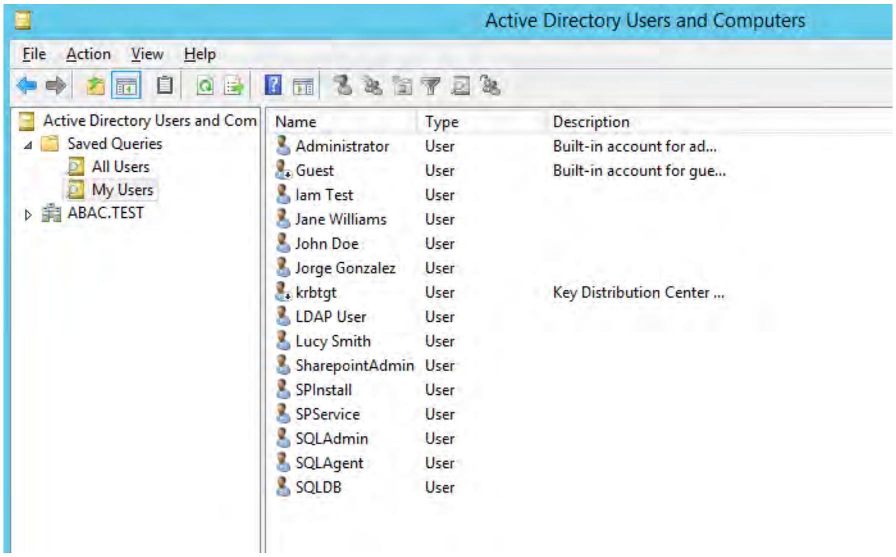
Description:

□ Disabled accounts

□ Non expiring passwords

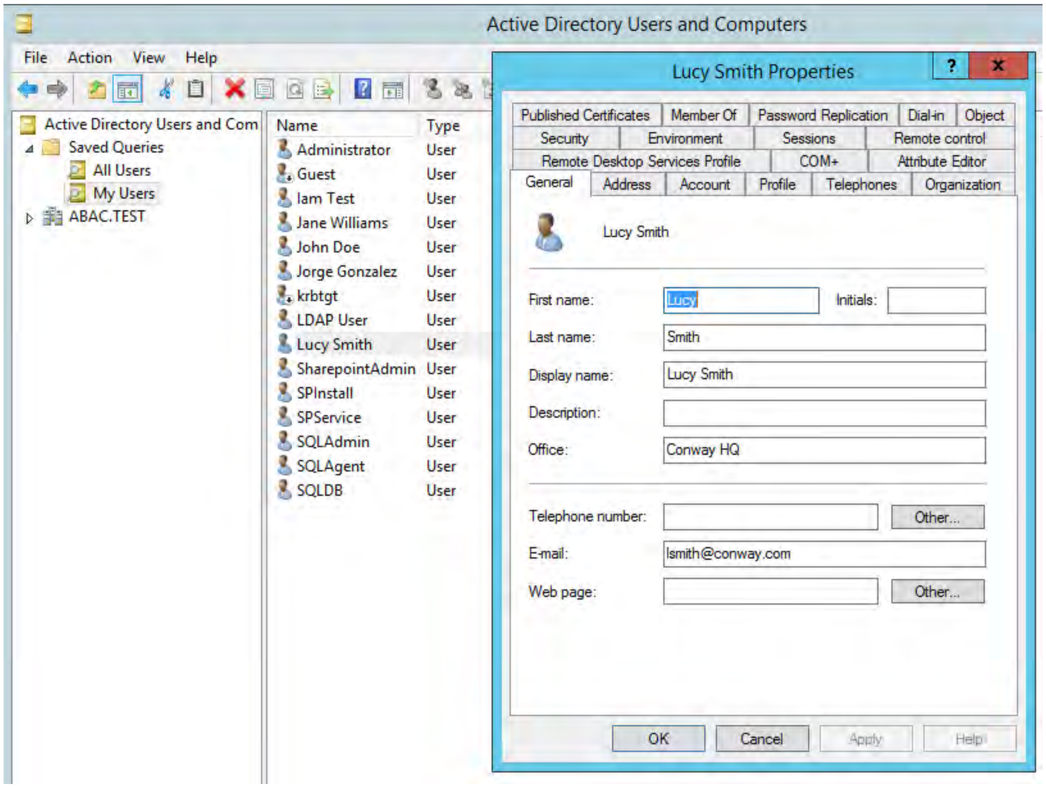
Days since last logon:

6. Click **OK**. Then, click **OK** again to create your new query.
7. You will see a list of **Active Directory Users** displayed in the right pane.


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
All Users
My Users
ABAC.TEST

Name	Type	Description
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...
Iam Test	User	
Jane Williams	User	
John Doe	User	
Jorge Gonzalez	User	
krbtgt	User	Key Distribution Center ...
LDAP User	User	
Lucy Smith	User	
SharepointAdmin	User	
SPInstall	User	
SPService	User	
SQLAdmin	User	
SQLAgent	User	
SQLDB	User	

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



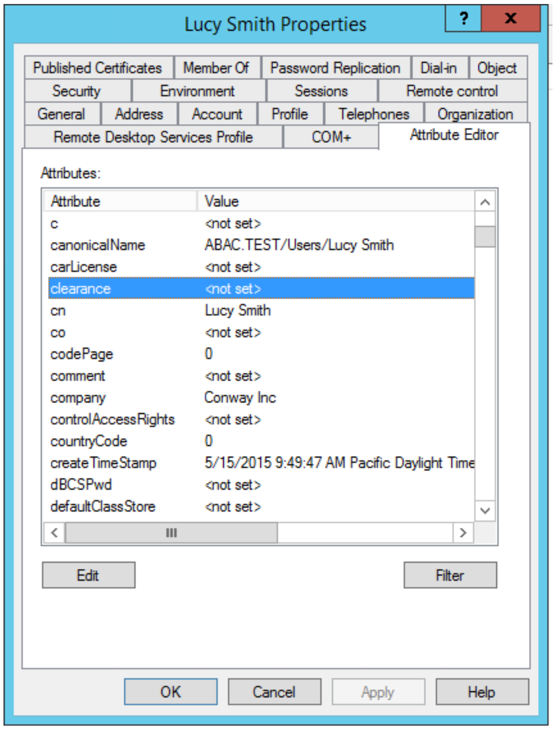
Name	Type
Administrator	User
Guest	User
Iam Test	User
Jane Williams	User
John Doe	User
Jorge Gonzalez	User
krbtgt	User
LDAP User	User
Lucy Smith	User
SharepointAdmin	User
SPInstall	User
SPService	User
SQLAdmin	User
SQLAgent	User
SQLDB	User

Lucy Smith

First name: Lucy
Initials:
Last name: Smith
Display name: Lucy Smith
Description:
Office: Conway HQ
Telephone number:
E-mail: lsmith@conway.com
Web page:

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

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

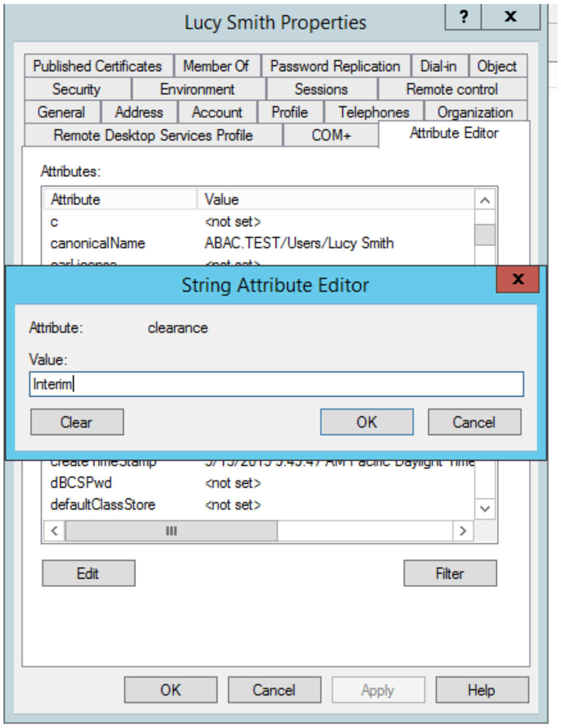


Attributes:

Attribute	Value
c	<not set>
canonicalName	ABAC.TEST/Users/Lucy Smith
carLicense	<not set>
clearance	<not set>
cn	Lucy Smith
co	<not set>
codePage	0
comment	<not set>
company	Conway Inc
controlAccessRights	<not set>
countryCode	0
createTimeStamp	5/15/2015 9:49:47 AM Pacific Daylight Time
dBCSPwd	<not set>
defaultClassStore	<not set>

11. Double click on the attribute, and enter a value suitable for your organization. In this example the clearance attribute will be set to a value of **Interim** for the user **Lucy Smith** in subsequent steps.

12. Click **OK** and then click **OK** again. The information is saved and the User Properties window closes.



Attribute	Value
c	<not set>
canonicalName	ABAC.TEST/Users/Lucy Smith
dBCSPwd	<not set>
defaultClassStore	<not set>

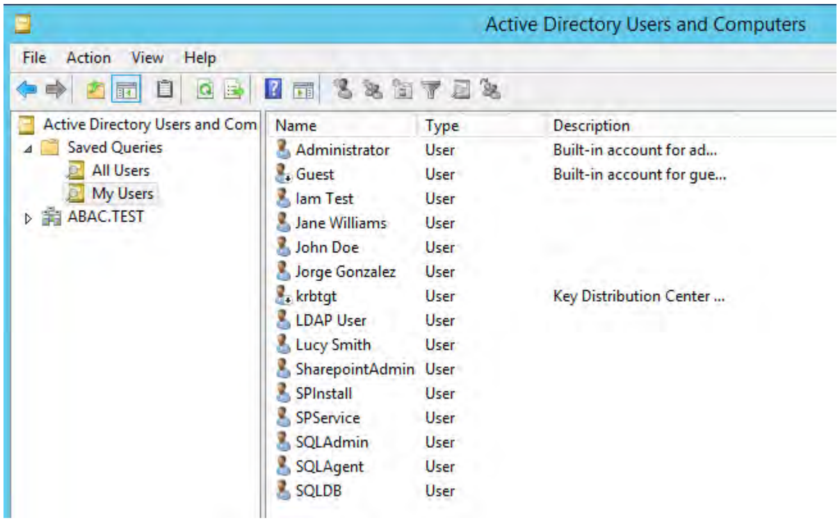
Attribute: clearance

Value: Interim

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 in the view.

6.2.2.1 Adding New Columns to the Users Query View

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**.

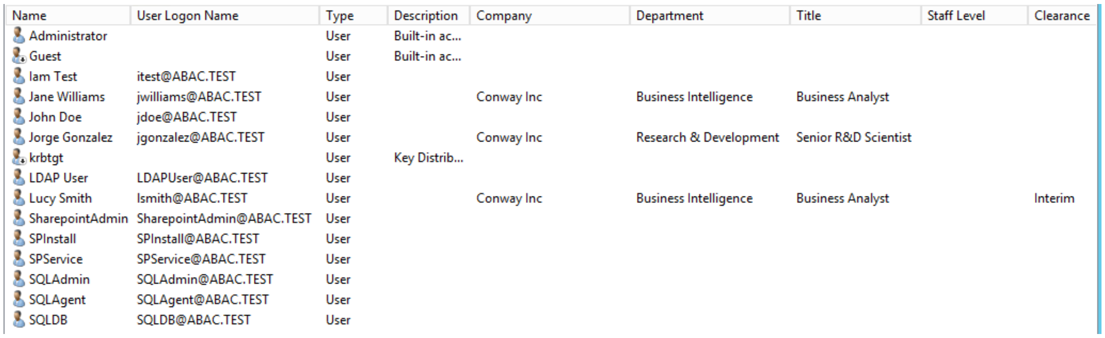


- Active Directory Users and Com
  - Saved Queries
    - All Users
    - My Users
  - ABAC.TEST

Name	Type	Description
Administrator	User	Built-in account for ad...
Guest	User	Built-in account for gue...
Iam Test	User	
Jane Williams	User	
John Doe	User	
Jorge Gonzalez	User	
krbtgt	User	Key Distribution Center ...
LDAP User	User	
Lucy Smith	User	
SharepointAdmin	User	
SPInstall	User	
SPService	User	
SQLAdmin	User	
SQLAgent	User	
SQLDB	User	

1. In the **Saved Queries** folder, click on the name of the query to be modified (e.g. **My Users**).
2. Click on the **View** menu and select **Add/Remove Columns…**
3. In the list of **Available columns**, scroll up or down to find desired columns.
4. Click on column name and click on the **Add** button.
5. When all desired columns have been chosen click **OK**.

The following screenshot shows a query view after adding custom attribute columns. The example contains new columns for the attributes **User Logon Name**, **Company**, **Department**, **Title**, **Staff Level**, and **Clearance**.



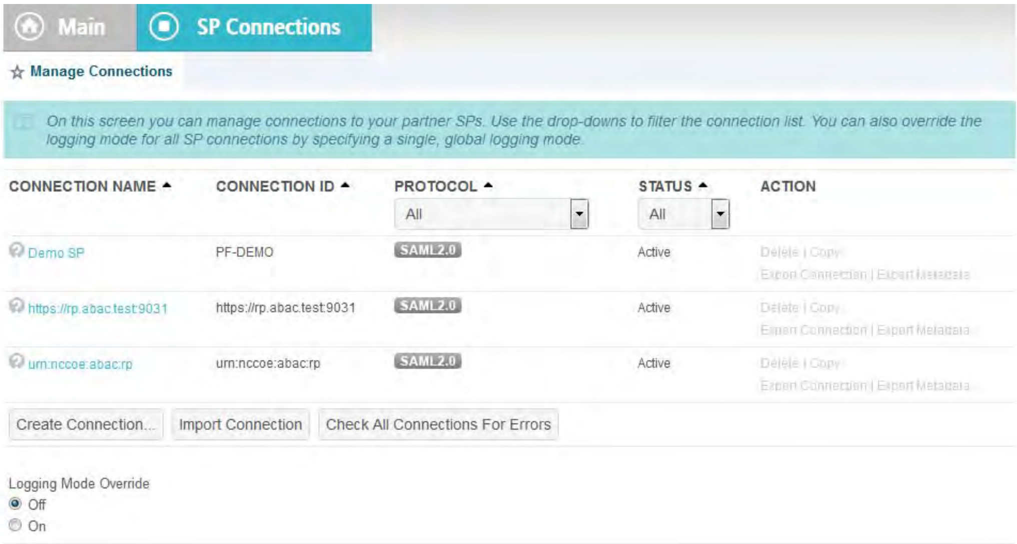
Name	User Logon Name	Type	Description	Company	Department	Title	Staff Level	Clearance
Administrator		User	Built-in ac...					
Guest		User	Built-in ac...					
Iam Test	itest@ABAC.TEST	User						
Jane Williams	jwilliams@ABAC.TEST	User		Conway Inc	Business Intelligence	Business Analyst		
John Doe	jdoe@ABAC.TEST	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						

6.3 Configure PingFederate Servers to Pull User Attributes

6.3.1 Configure PingFederate-IdP to Pull User Attributes During Authentication

Follow the instructions in this section to configure the PingFederate-IdP to pull user attribute values from Microsoft AD during the authentication process. In the following example, the value for the user attribute company is extracted from Microsoft AD.

1. Launch your browser and go to: **https://<DNS_NAME>:9999/pingfederate/app**.
2. Replace **DNS_NAME** with the fully qualified name of the Identity Provider's PingFederate server (e.g. **https://idp.abac.test:9999/pingfederate/app**).
3. Log on to the PingFederate application using the credentials you configured during installation.
4. On the **Main** menu under **SP CONNECTION**, click **Manage All SP**.

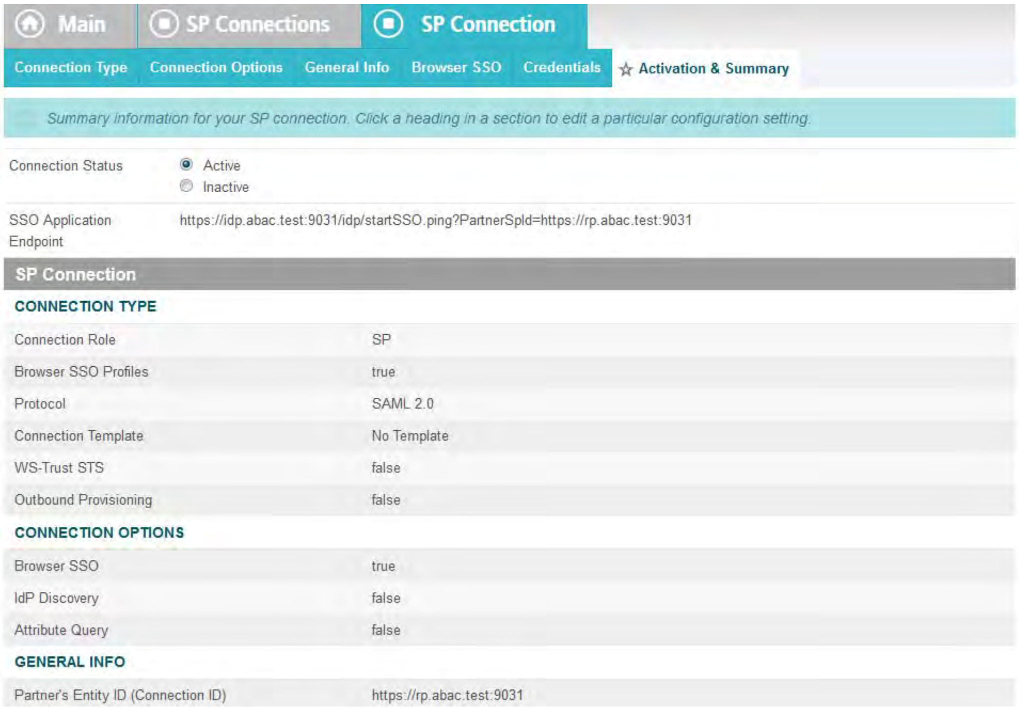


On this screen you can manage connections to your partner SPs. Use the drop-downs to filter the connection list. You can also override the logging mode for all SP connections by specifying a single, global logging mode.

CONNECTION NAME ▲	CONNECTION ID ▲	PROTOCOL ▲ All	STATUS ▲ All	ACTION
Demo SP	PF-DEMO	SAML2.0	Active	Delete | Copy Export Connection | Export Metadata
https://rp.abac.test:9031	https://rp.abac.test:9031	SAML2.0	Active	Delete | Copy Export Connection | Export Metadata
urn:nccoe:abac:rp	urn:nccoe:abac:rp	SAML2.0	Active	Delete | Copy Export Connection | Export Metadata

Logging Mode Override
● Off
○ On

5. Click on the link for the connection created in chapter 3 (e.g. **https://rp.abac.test:9031**).



Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status ● Active ○ Inactive

SSO Application Endpoint https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=https://rp.abac.test:9031

SP Connection

CONNECTION TYPE

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

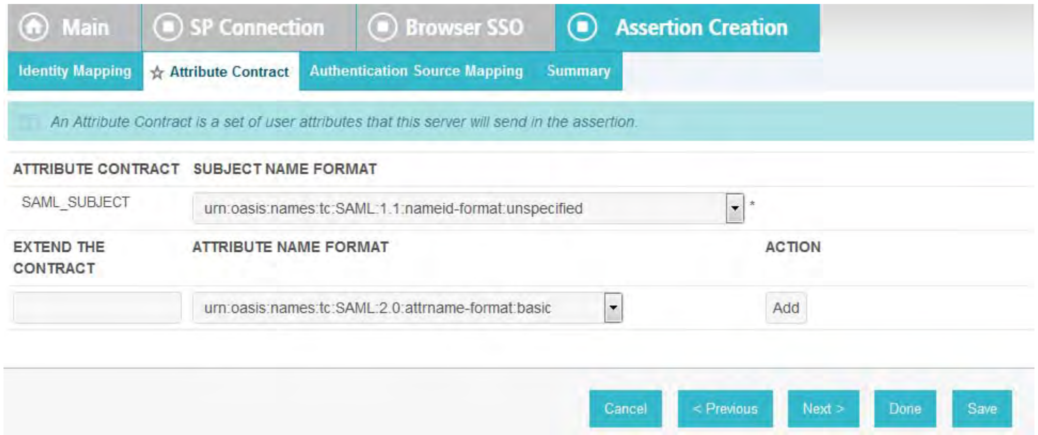
CONNECTION OPTIONS

Browser SSO	true
IdP Discovery	false
Attribute Query	false

GENERAL INFO

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

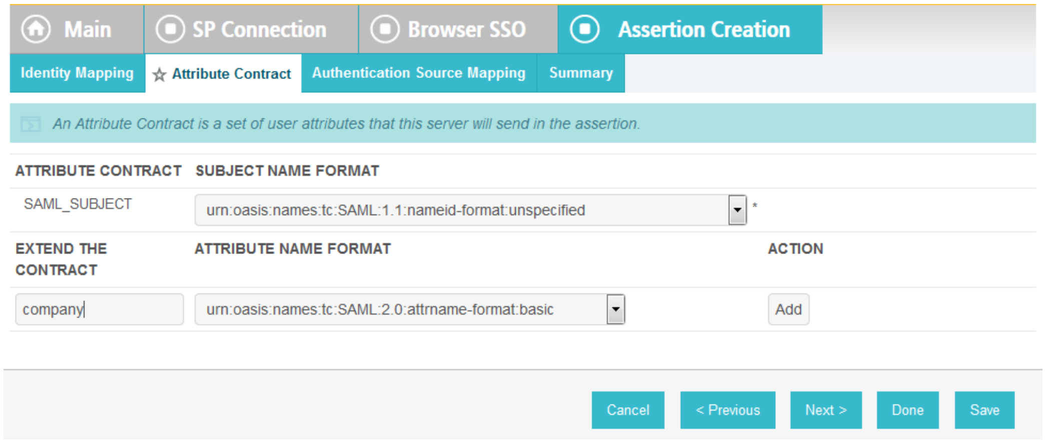
6. On the Activation & Summary screen, scroll down to the **Assertion Creation** group and click on the **ATTRIBUTE CONTRACT** link.



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT	SUBJECT NAME FORMAT	
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified *	
EXTEND THE CONTRACT	**ATTRIBUTE NAME FORMAT**	**ACTION**
	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add

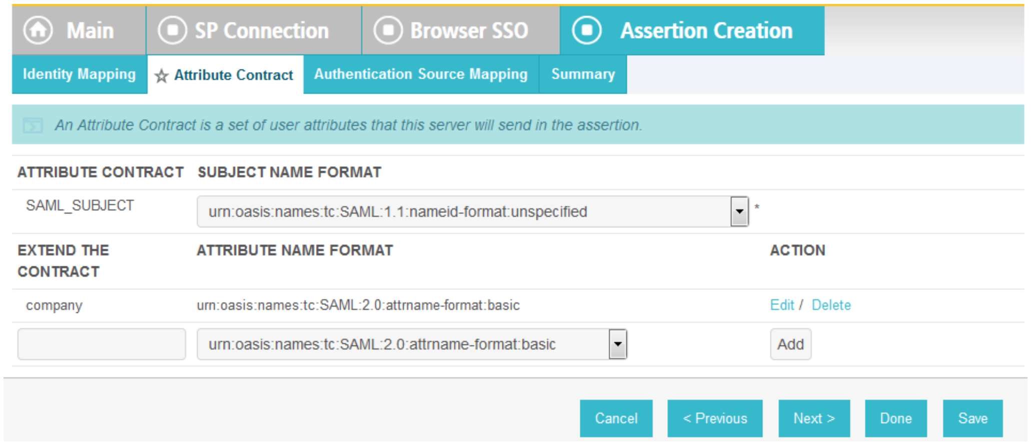
7. On the Attribute Contract screen, under the **EXTEND THE CONTRACT** column, enter the name of the attribute to be extracted from Microsoft AD (e.g. **company**) in the empty text field.



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT	SUBJECT NAME FORMAT	
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified *	
EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
company	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add

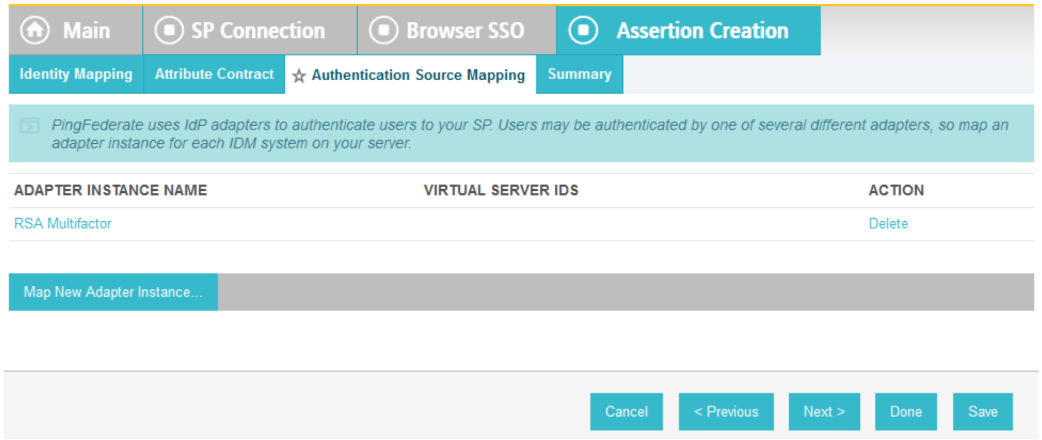
8. Click **Add**.



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT	SUBJECT NAME FORMAT	
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified *	
EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
company	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit / Delete
	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add

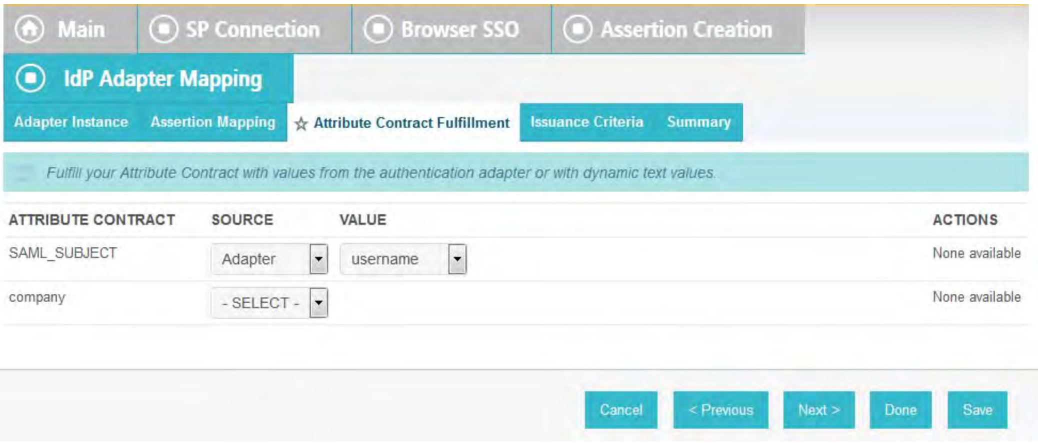
9. Click **Next**.



PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION
RSA Multifactor		Delete

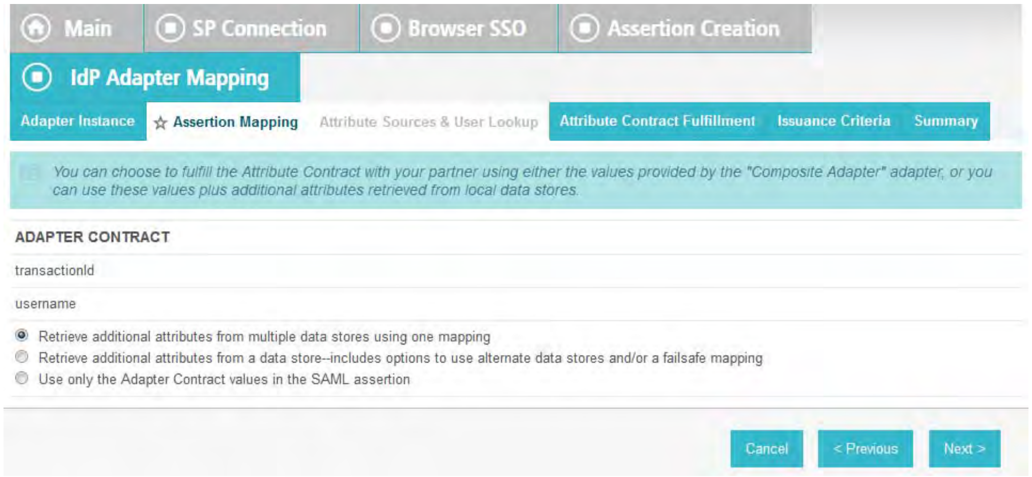
10. On the Authentication Source Mapping screen click on the name of the **ADAPTER INSTANCE** that is listed (e.g. **RSA Multifactor**).



Fulfill your Attribute Contract with values from the authentication adapter or with dynamic text values.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Adapter	username	None available
company	- SELECT -		None available

11. Click on **Assertion Mapping** tab and select **Retrieve additional attributes from multiple data stores using one mapping**.



You can choose to fulfill the Attribute Contract with your partner using either the values provided by the "Composite Adapter" adapter, or you can use these values plus additional attributes retrieved from local data stores.

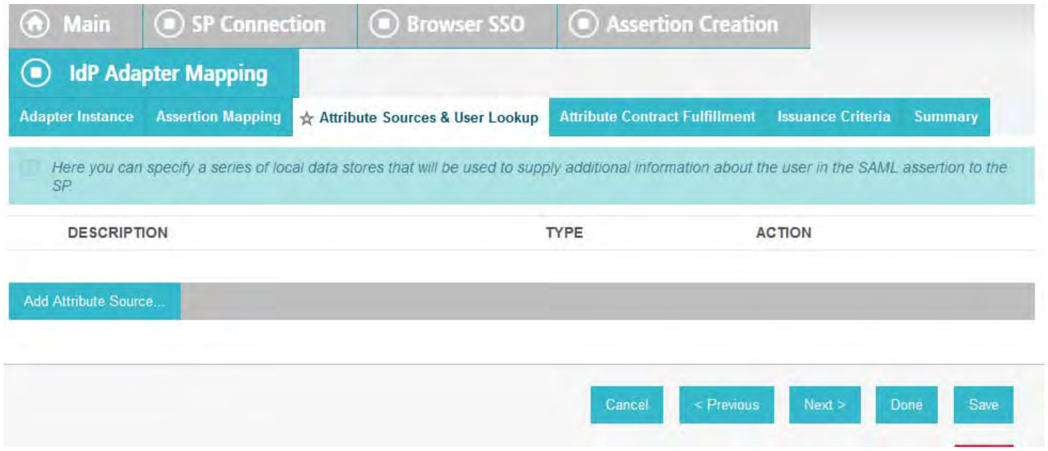
ADAPTER CONTRACT

transactionId

username

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

12. Click **Next**.



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

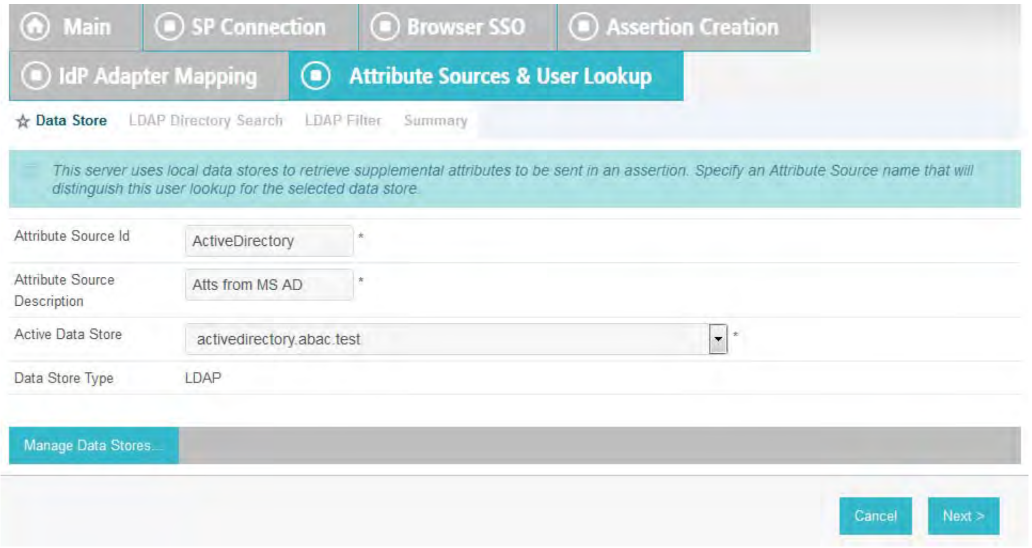
DESCRIPTION	TYPE	ACTION

13. Click on **Add Attribute Source**.

14. On the Attribute Sources & User Lookup screen enter a unique name in the **Attribute Source Id** field (e.g **ActiveDirectory**).

15. In the **Attribute Source Description** field, enter a description.

16. From the **Active Data Store** list, select the existing Data Store that connects to Active Directory.



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 the selected data store.

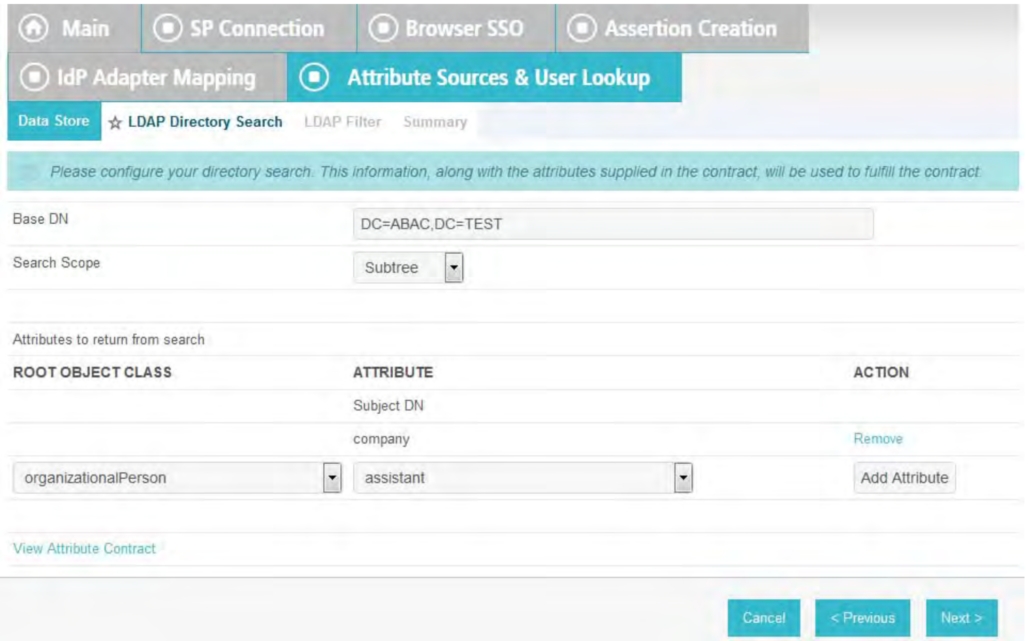
Attribute Source Id	ActiveDirectory *
Attribute Source Description	Atts from MS AD *
Active Data Store	activedirectory.abac.test *
Data Store Type	LDAP

17. Click **Next**.

18. On the LDAP Directory Search screen, enter the **Base DN** (e.g. **DC=ABAC,DC=TEST**).

19. Under the **ROOT OBJECT CLASS** column, select the Active Directory class that contains the attribute you want to pull the value from. In the example below, the **organizationalPerson** class is selected because it is the root class that contains the company attribute.

20. Under the **ATTRIBUTE** column, select the attribute (e.g. **company**), then click **Add Attribute**.



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

Base DN: DC=ABAC,DC=TEST

Search Scope: Subtree

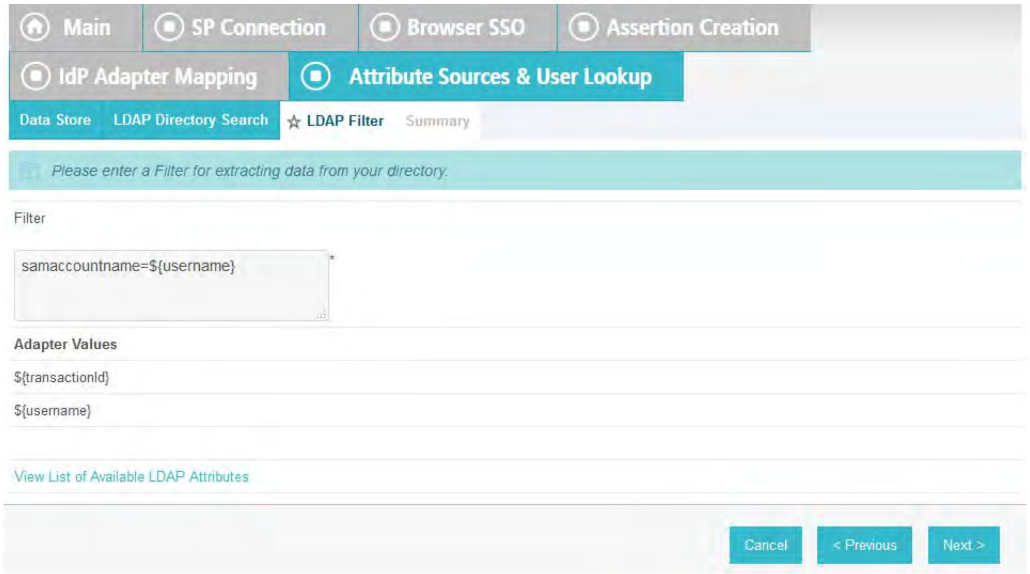
Attributes to return from search

ROOT OBJECT CLASS	ATTRIBUTE	ACTION
	Subject DN	
	company	Remove
organizationalPerson	assistant	Add Attribute

View Attribute Contract

21. Click **Next**.

22. On the LDAP Filter screen, enter **samaccountname=${username}**.



Please enter a Filter for extracting data from your directory.

Filter

samaccountname=${username}

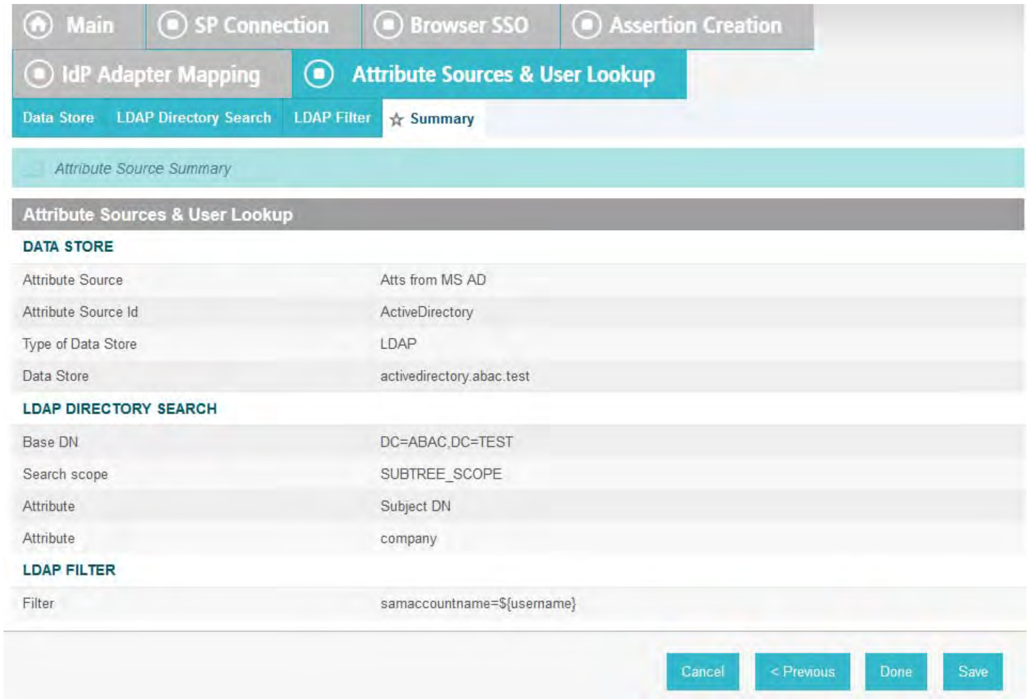
Adapter Values

${transactionId}

${username}

View List of Available LDAP Attributes

23. Click **Next**.

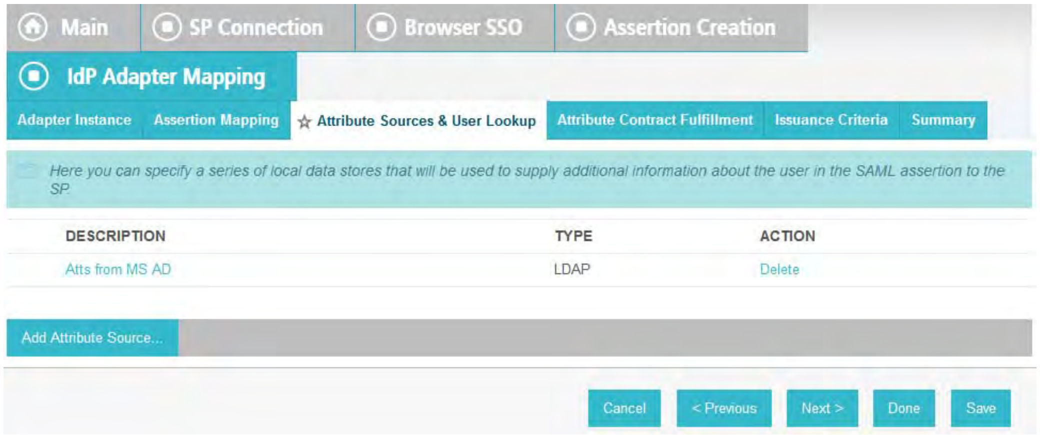


Attribute Source Summary

Attribute Sources & User Lookup

DATA STORE	
Attribute Source	Atts from MS AD
Attribute Source Id	ActiveDirectory
Type of Data Store	LDAP
Data Store	activedirectory.abac.test
LDAP DIRECTORY SEARCH	
Base DN	DC=ABAC,DC=TEST
Search scope	SUBTREE_SCOPE
Attribute	Subject DN
Attribute	company
LDAP FILTER	
Filter	samaccountname=${username}

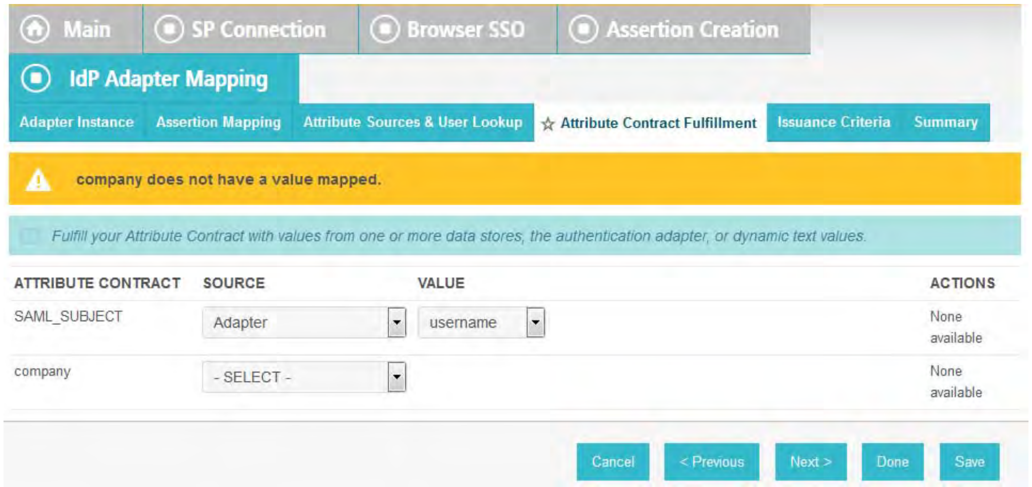
24. On the Summary screen, click **Done**.



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

25. On the Attribute Sources & User Lookup screen, click **Done**.

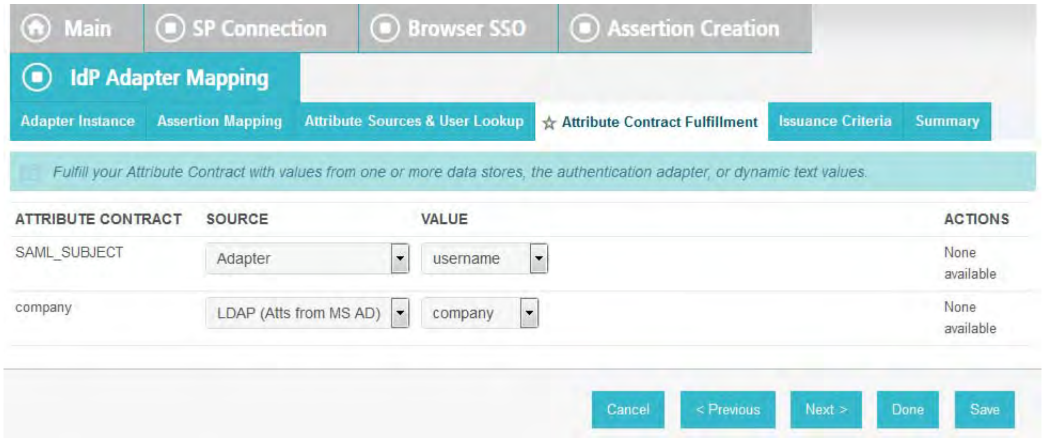


company does not have a value mapped.

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	username	None available
company	- SELECT -		None available

26. On the Attribute Contract Fulfillment screen, for the company attribute select the **SOURCE** and **VALUE**. For the **SOURCE**, select **LDAP (Atts from MS AD)**. For **VALUE** select **company**.



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	username	None available
company	LDAP (Atts from MS AD)	company	None available

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

6.3.1.1 Functional Test of Pulling User Attributes During Authentication

The instructions in this section will help perform a test to ensure that the Identity Provider is getting the configured attributes (e.g. **company**) from Active Directory and passing them in a SAML message to the Relying Party. The Firefox SAML tracer Add-on is used to examine the SAML message.

Follow the instructions in section 6.6.1, Temporarily Disable SAML Encryption for Testing and Troubleshooting Message Exchanges, on page 240 to disable SAML encryption. Once SAML encryption has been disabled, you can proceed with the following functional test instructions.

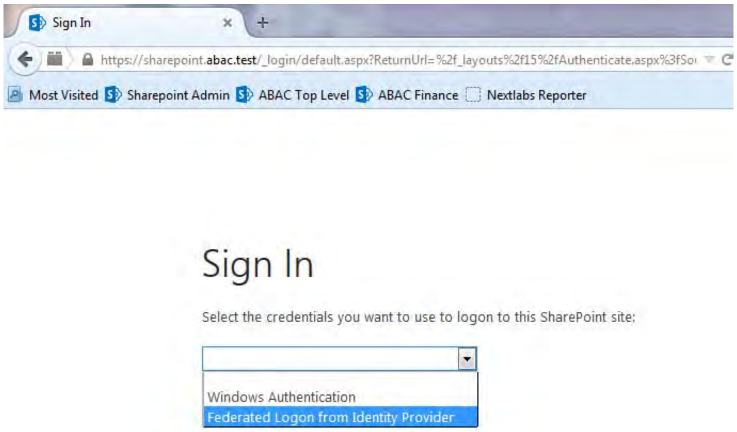
1. Launch your Firebox browser and select **SAML tracer** from the **Tools** menu.

   This launches an empty SAML tracer window.

2. Minimize the SAML tracer window.

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

3. Go back to the main browser window and go to the Relying Party’s SharePoint site (e.g. **https://SharePoint.abac.test**).


Sign In
https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSo
Most Visited
Sharepoint Admin
ABAC Top Level
ABAC Finance
Nextlabs Reporter

Sign In

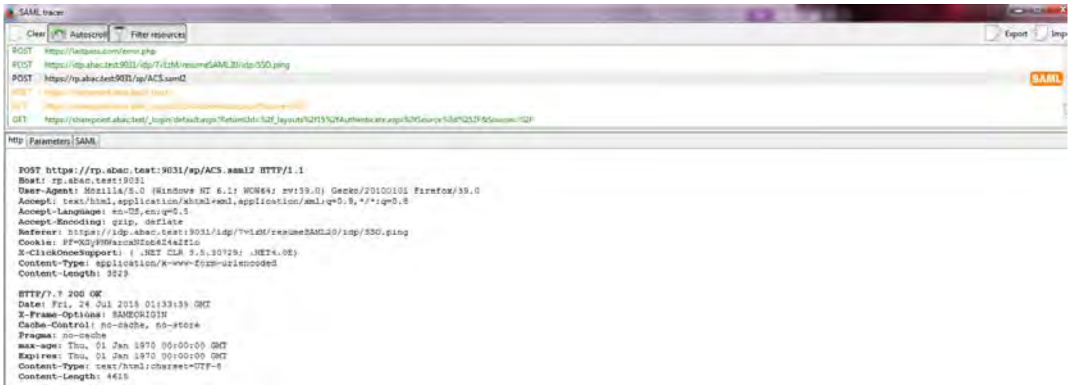
Select the credentials you want to use to logon to this SharePoint site:

Windows Authentication
Federated Logon from Identity Provider

4. Select **Federated Logon from Identity Provider**.
5. In the Identity Provider’s PingFederate Sign On screen, enter the credentials for the account you are testing with (e.g. **lsmith**) and click **Sign On**.
6. On the RSA 2-factor authentication screen, enter the validation code and proceed.

   The browser redirects to the PingFederate-RP and then to the Relying Party's SharePoint site. You may not notice the redirection to the PingFederate-RP if it happens quickly.

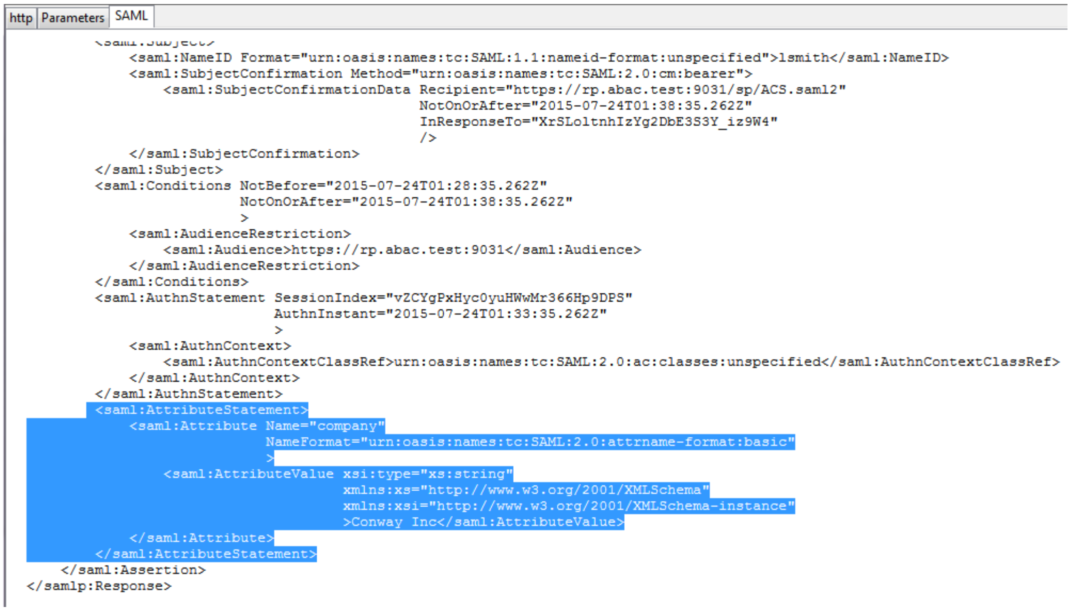
7. Go back to the SAML tracer window. Scroll down and click on the last **POST** message that contains a SAML icon.



```
POST   https://lastpass.com/error.php
POST   https://idp.abac.test:9031/idp/7vIzM/resumeSAML20/idp/SSO.ping
POST   https://rp.abac.test:9031/sp/ACS.saml2
GET    https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
```

```
POST https://rp.abac.test:9031/sp/ACS.saml2 HTTP/1.1
Host: rp.abac.test:9031
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://idp.abac.test:9031/idp/7vIzM/resumeSAML20/idp/SSO.ping
Cookie: PF=XGyP8WarcaNfob624a2f1o
X-ClickOnceSupport: ( .NET CLR 3.5.30729; .NET4.0E)
Content-Type: application/x-www-form-urlencoded
Content-Length: 3829

HTTP/?.? 200 OK
Date: Fri, 24 Jul 2015 01:33:39 GMT
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache, no-store
Pragma: no-cache
max-age: Thu, 01 Jan 1970 00:00:00 GMT
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 4615
```

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



```
        <saml:Subject>
            <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">lsmith</saml:NameID>
            <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                <saml:SubjectConfirmationData Recipient="https://rp.abac.test:9031/sp/ACS.saml2"
                                              NotOnOrAfter="2015-07-24T01:38:35.262Z"
                                              InResponseTo="XrSLoltnhIzYg2DbE3S3Y_iz9W4"
                                              />
            </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:Conditions NotBefore="2015-07-24T01:28:35.262Z"
                         NotOnOrAfter="2015-07-24T01:38:35.262Z"
                         >
            <saml:AudienceRestriction>
                <saml:Audience>https://rp.abac.test:9031</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement SessionIndex="vZCYgPxHyc0yuHWwMr366Hp9DPS"
                             AuthnInstant="2015-07-24T01:33:35.262Z"
                             >
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="company"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >Conway Inc</saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

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

Expected Result: Ensure that the AttributeValue node contains the expected value for the attribute from ActiveDirectory. In the example screen shot 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**.

When you complete this functional test, you must enable SAML encryption between the Identity Provider and Relying Party again. Follow the instructions in the section 6.6.1.2, Enable SAML Encryption Again, on page 241 to enable SAML encryption.

6.3.2 Configure PingFederate-IdP to Pull Environmental Attributes During Authentication

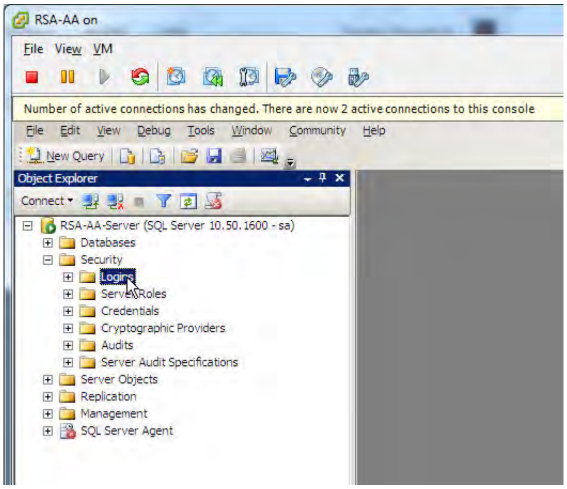
Follow the instructions in this section to configure the PingFederate-IdP to get environmental attribute values from the RSA Adaptive Authentication system during the authentication process. The environmental attributes are passed along with the user attributes in the SAML messages that is sent to the Relying Party. In the example below, the environmental attribute **ip_address** will be pulled from RSA Adaptive Authentication.

RSA Adaptive Authentication stores environmental attributes about the user's web transactions in a SQL Server database named **RSA_CORE_AA**. The PingFederate-IdP will be configured to query to the **RSA_CORE_AA** database and get the value of **ip_address** from the **EVENT_LOG** table.

Before you can configure the query for **ip_address**, you must first create an account for the PingFederate application in the **RSA_CORE_AA** database. Follow these instructions to create the account in the SQL Server database.

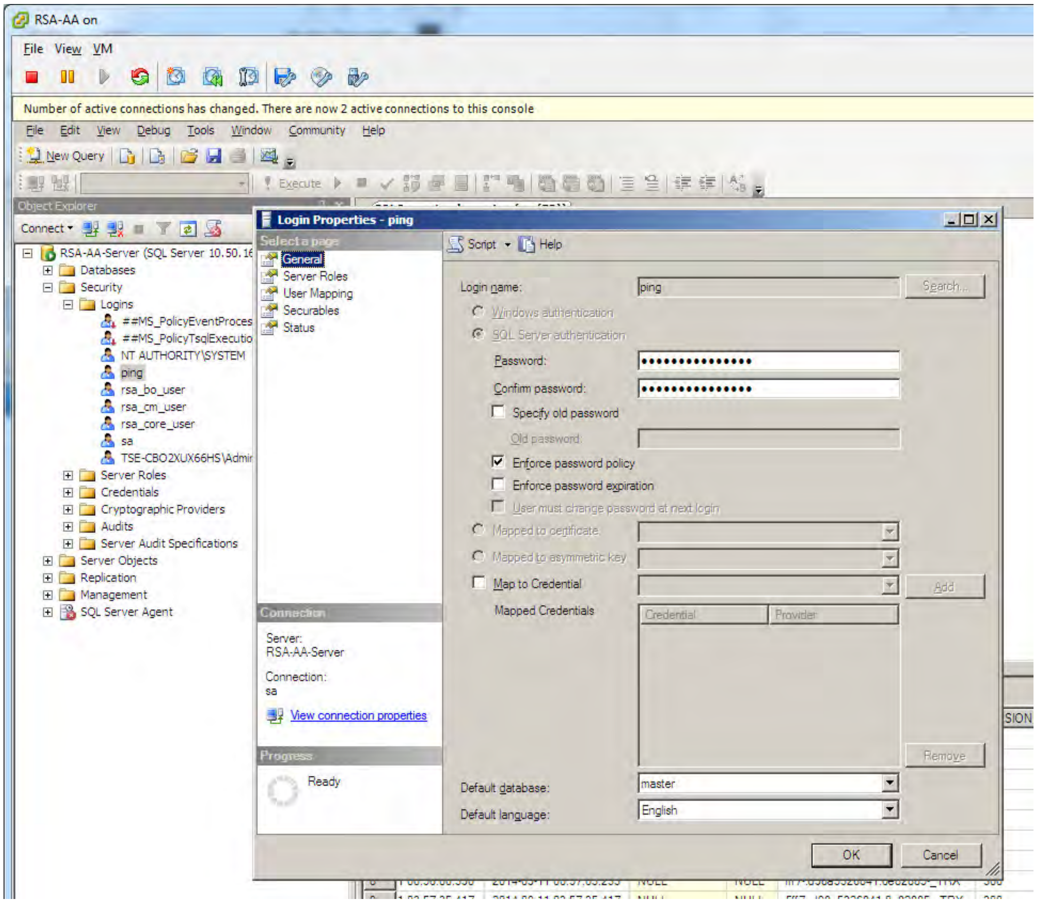
Log on to the server that hosts the RSA Adaptive Authentication SQL Server database engine.

1. Open SQL Server Management Studio.
2. Expand the **RSA-AA-Server** folder, then the **Security** folder.
3. Right click on **Logins** and select **New Login**.



Number of active connections has changed. There are now 2 active connections to this console

4. Set the **Login name** (e.g. **ping**), under SQL Server authentication choose a password that meets the Windows password policy.



Number of active connections has changed. There are now 2 active connections to this console

Login name: ping

○ Windows authentication

● SQL Server authentication

Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

☐ Specify old password

Old password:

☑ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider

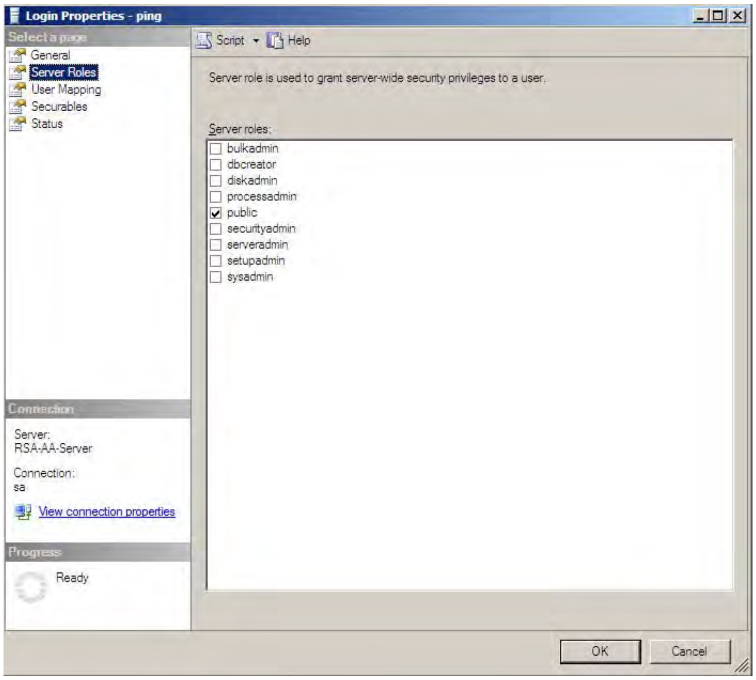
Server: RSA-AA-Server

Connection: sa

Default database: master

Default language: English

5. Under **Server Roles**, select **public**.



Login Properties - ping

Select a page: General, Server Roles, User Mapping, Securables, Status

Server role is used to grant server-wide security privileges to a user.

Server roles:

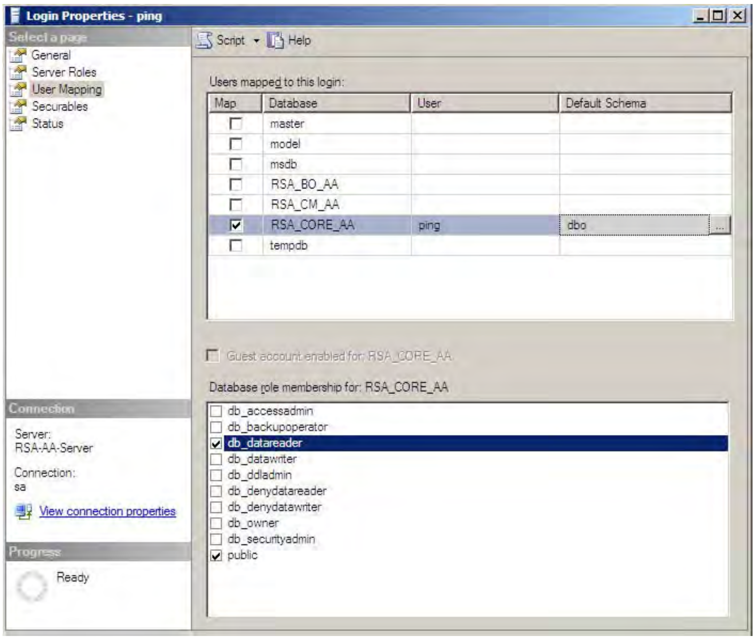
- □ bulkadmin
- □ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- □ sysadmin

Connection

Server:
RSA-AA-Server

Connection:
sa

6. 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**.



Login Properties - ping

Select a page: General, Server Roles, User Mapping, Securables, Status

Users mapped to this login:

Map	Database	User	Default Schema
□	master		
□	model		
□	msdb		
□	RSA_BO_AA		
□	RSA_CM_AA		
☑	RSA_CORE_AA	ping	dbo
□	tempdb		

□ Guest account enabled for: RSA_CORE_AA

Database role membership for: RSA_CORE_AA

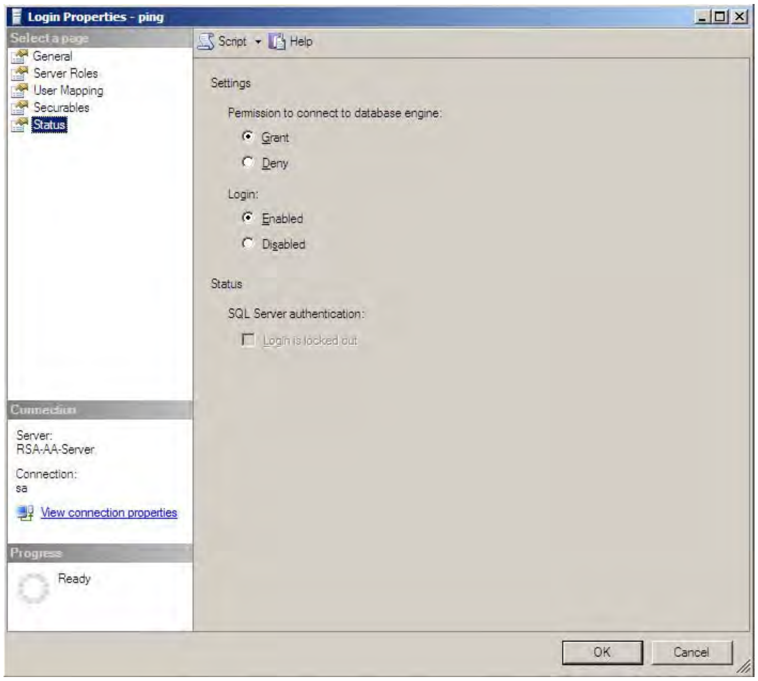
- □ db_accessadmin
- □ db_backupoperator
- ☑ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- □ db_owner
- □ db_securityadmin
- ☑ public

Connection

Server:
RSA-AA-Server

Connection:
sa

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



Login Properties - ping

Select a page: General, Server Roles, User Mapping, Securables, **Status**

Settings

Permission to connect to database engine:
● Grant
○ Deny

Login:
● Enabled
○ Disabled

Status

SQL Server authentication:
☐ Login is locked out

Connection

Server:
RSA-AA-Server

Connection:
sa

View connection properties

Progress

Ready

6.3.2.1 Configuring a New Data Store that Connects to the RSA Database

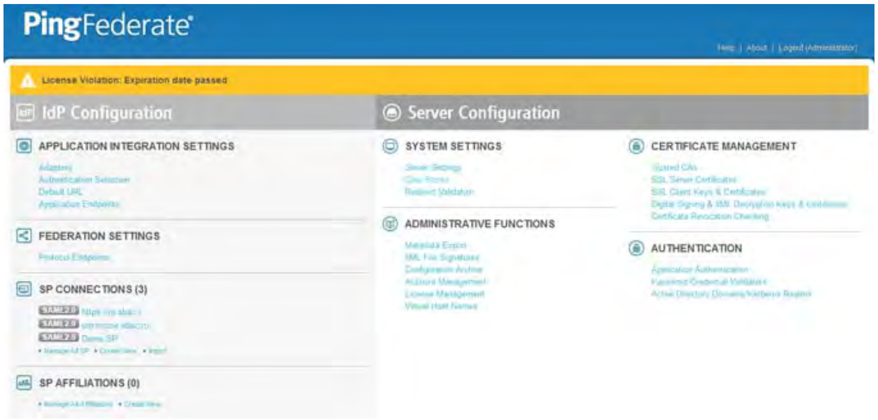
Next you will configure a new Data Store that connects to the **RSA_CORE_AA** database on the Identity Provider's PingFederate server. This new data store will be used in the RP Connection to query the **EVENT_LOG** table during the authentication process.

Follow the instructions below to create a new Data Store for the RSA_CORE_AA database.

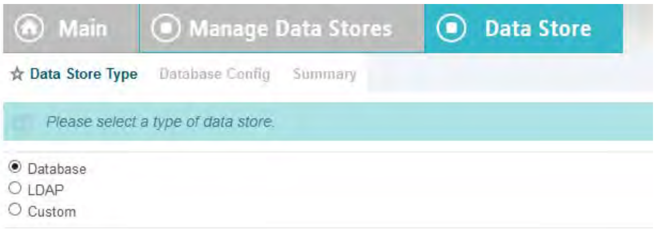
1. Launch your browser and go to: **https://<DNS_NAME>:9999/pingfederate/app**. Replace **<DNS_NAME>** with the fully qualified name of the Identity Provider’s PingFederate server (e.g. **https://idp.abac.test:9999/pingfederate/app**).

2. Log on to the PingFederate application using the credentials you configured during installation.

3. Under **Server configuration**, select **Data Stores**.



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



Please select a type of data store.

● Database
○ LDAP
○ Custom

5. On the database config page, set the **JDBC URL** to: **jdbc:sqlserver://<RSA_SERVER_IP_ADDRESS>:1433;databaseName=RSA_CORE_AA**

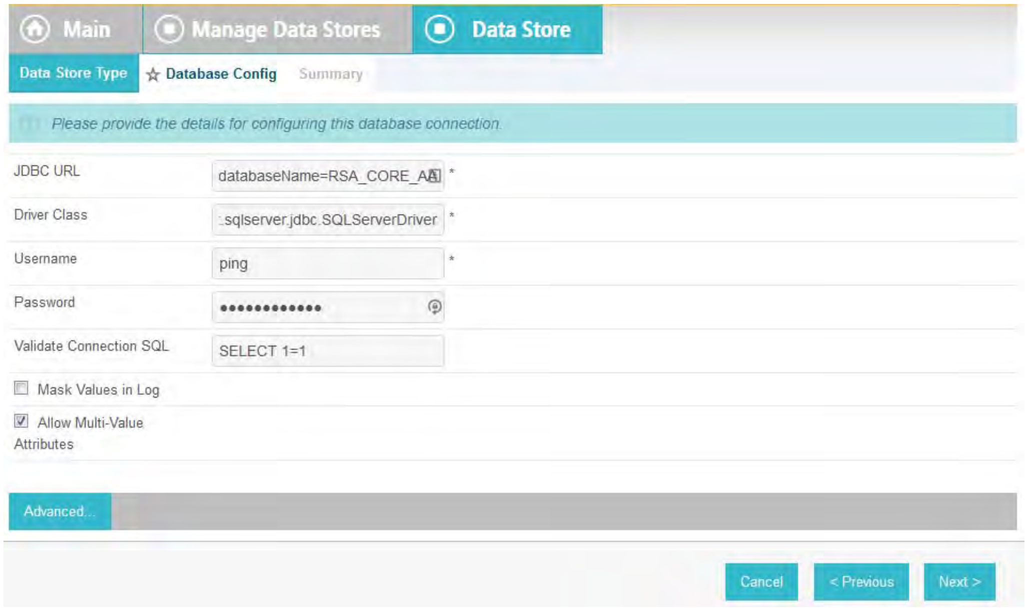
   Replace **<RSA_SERVER_IP_ADDRESS >** with the IP address of the server that hosts the **RSA_CORE_AA** database.

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

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

8. Under **Validate Connection SQL**, type **SELECT 1=1**.

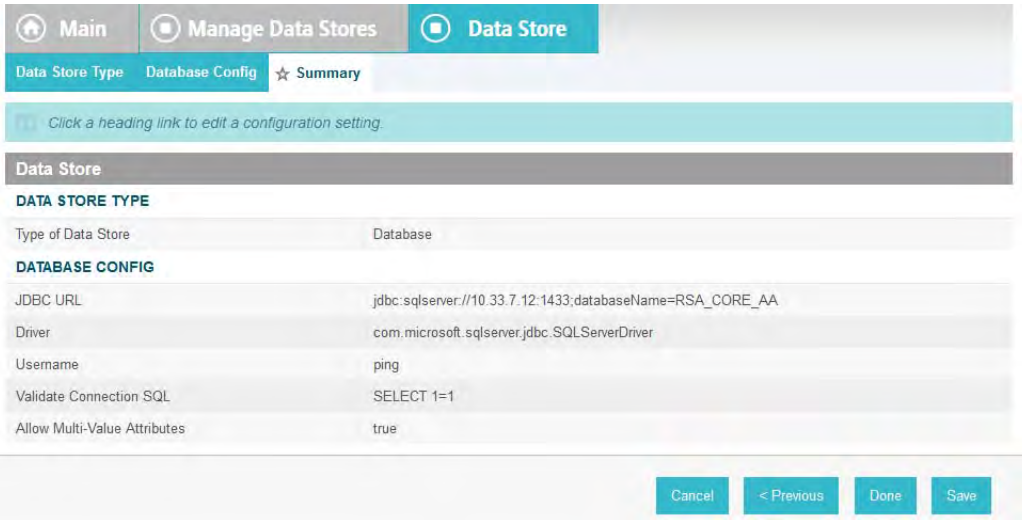
9. Select the check box **Allow multi-value attributes**; then, click **Next**.



Please provide the details for configuring this database connection.

JDBC URL	databaseName=RSA_CORE_AA *
Driver Class	:sqlserver.jdbc.SQLServerDriver *
Username	ping *
Password	•••••••••••••
Validate Connection SQL	SELECT 1=1
□ Mask Values in Log	
☑ Allow Multi-Value Attributes	

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

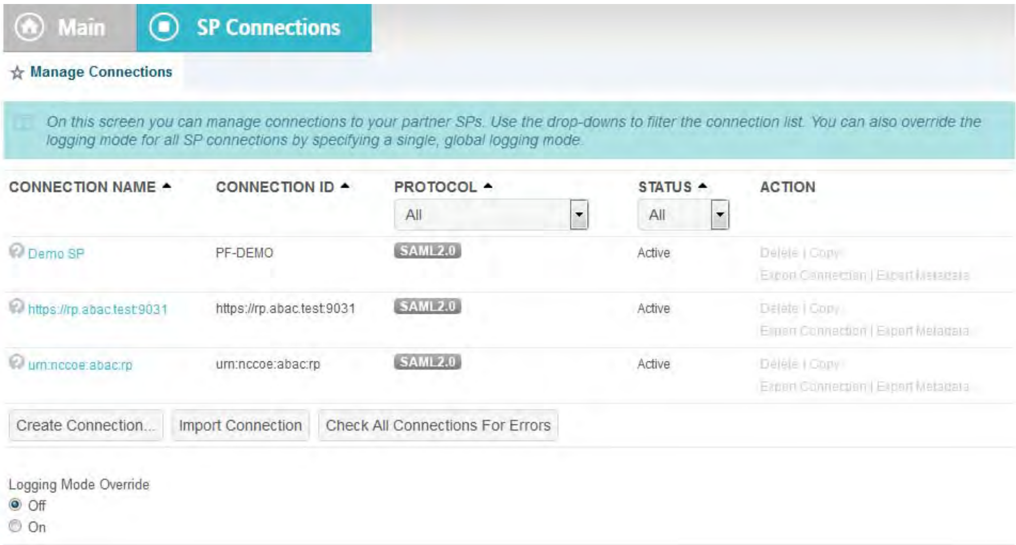
DATABASE CONFIG

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

6.3.2.2 Modifying the SP Connection to the RP to Add New Environmental Attribute

Next you will modify the SP Connection to the Relying Party and add a new environmental attribute **ip_address** from the **RSA_CORE_AA** database.

1. Go to the PingFederate **Main** menu.
2. On the **Main** menu under **SP CONNECTION**, click **Manage All SP**.

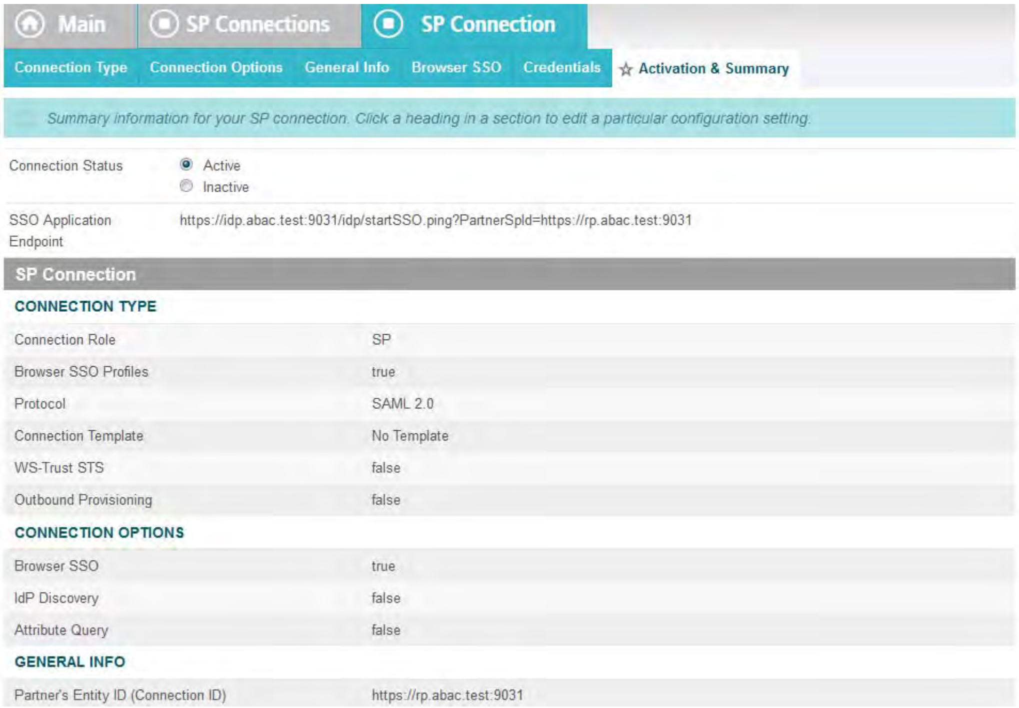


On this screen you can manage connections to your partner SPs. Use the drop-downs to filter the connection list. You can also override the logging mode for all SP connections by specifying a single, global logging mode.

CONNECTION NAME ▲	CONNECTION ID ▲	PROTOCOL ▲ All	STATUS ▲ All	ACTION
Demo SP	PF-DEMO	SAML2.0	Active	Delete | Copy Export Connection | Export Metadata
https://rp.abac.test:9031	https://rp.abac.test:9031	SAML2.0	Active	Delete | Copy Export Connection | Export Metadata
urn:nccoe:abac:rp	urn:nccoe:abac:rp	SAML2.0	Active	Delete | Copy Export Connection | Export Metadata

Logging Mode Override
● Off
○ On

3. Click on the link for the SP connection created in chapter 2 (e.g. **https://rp.abac.test:9031**).



Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

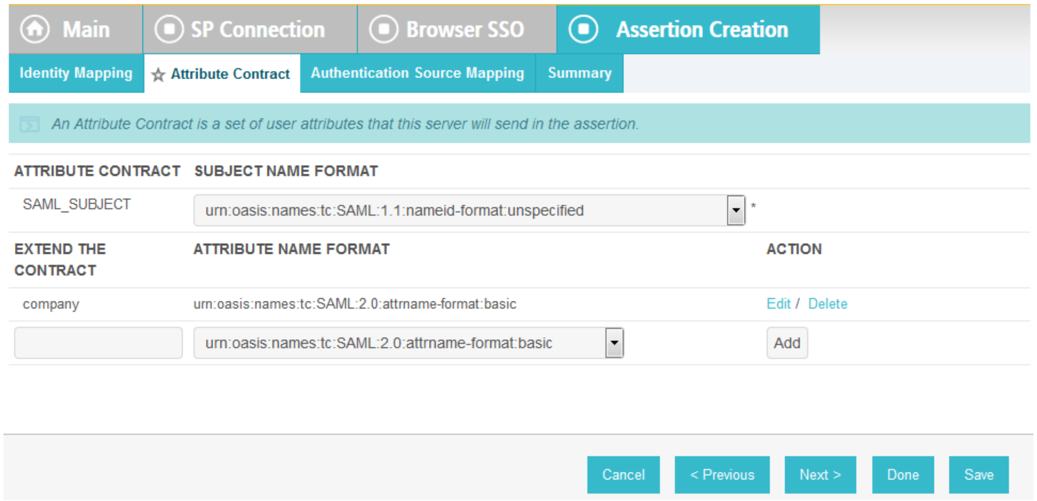
Connection Status ● Active ○ Inactive

SSO Application Endpoint https://idp.abac.test:9031/idp/startSSO.ping?PartnerSpId=https://rp.abac.test:9031

SP Connection

CONNECTION TYPE	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
CONNECTION OPTIONS	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
GENERAL INFO	
Partner's Entity ID (Connection ID)	https://rp.abac.test:9031

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

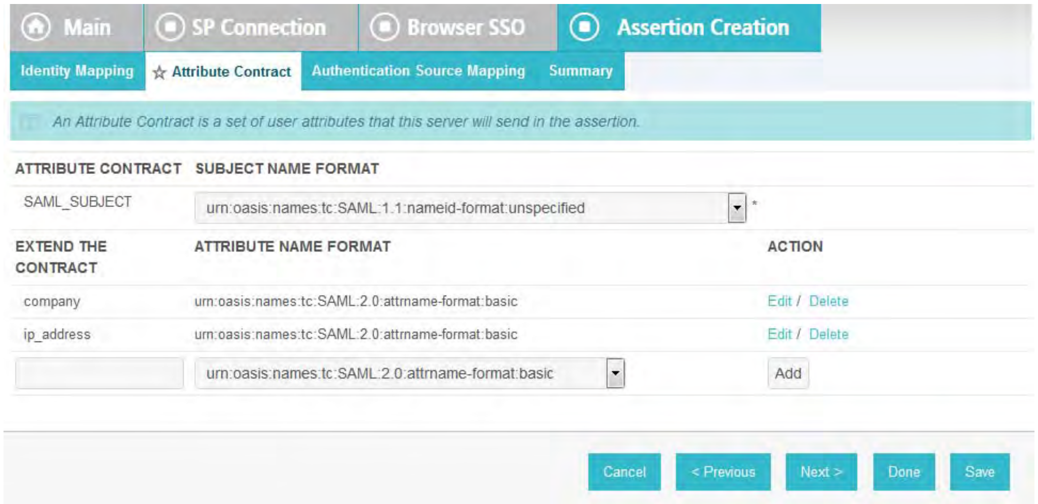


An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT	SUBJECT NAME FORMAT	
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified *	
EXTEND THE CONTRACT	**ATTRIBUTE NAME FORMAT**	**ACTION**
company	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit / Delete
	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add

5. On the Attribute Contract screen, under the **EXTEND THE CONTRACT** column, enter the name of the environmental attribute to be pulled from the **RSA_CORE_AA** database (e.g. **ip_address**) in the empty text field.

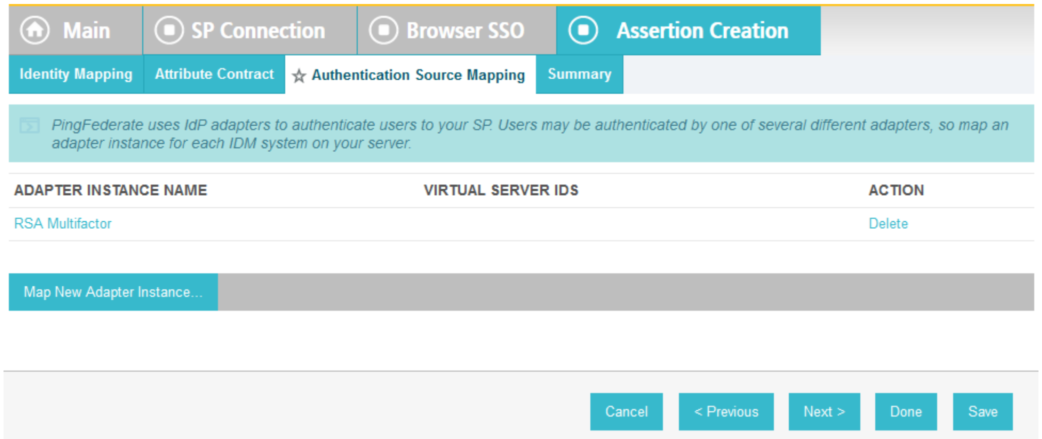
6. Click **Add**.



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT	SUBJECT NAME FORMAT	
SAML_SUBJECT	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified *	
EXTEND THE CONTRACT	**ATTRIBUTE NAME FORMAT**	**ACTION**
company	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit / Delete
ip_address	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Edit / Delete
	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	Add

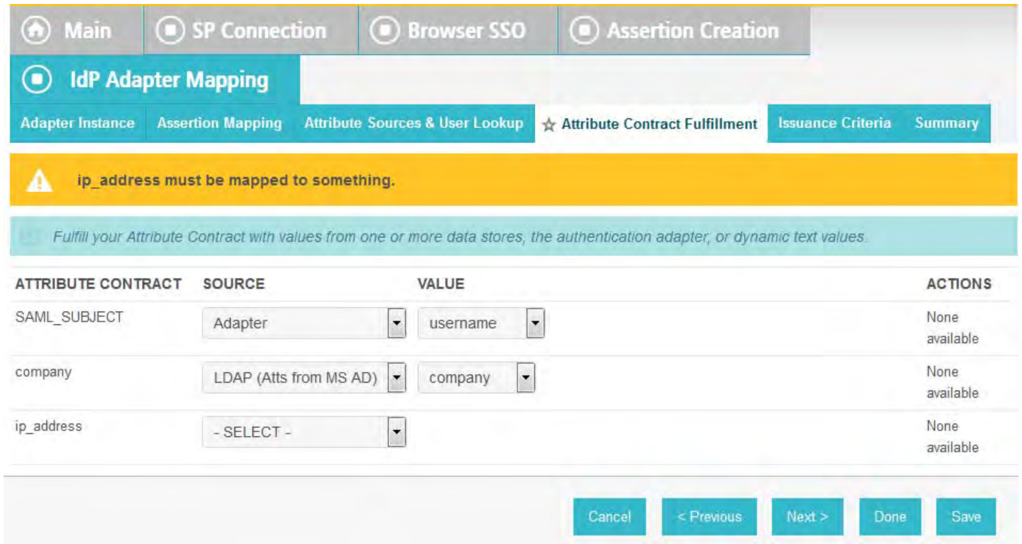
7. Click **Next**.



PingFederate uses IdP adapters to authenticate users to your SP. Users may be authenticated by one of several different adapters, so map an adapter instance for each IDM system on your server.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION
RSA Multifactor		Delete

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

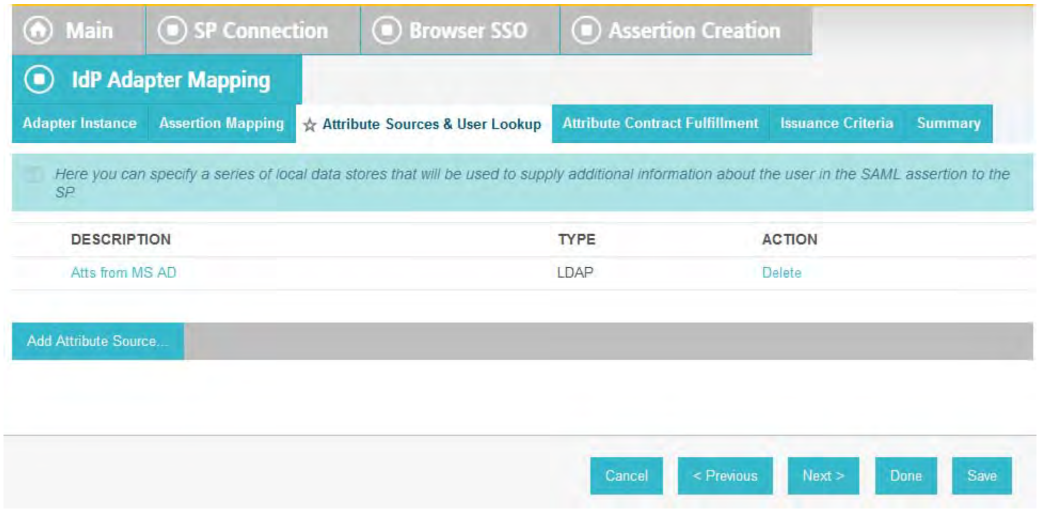


⚠ ip_address must be mapped to something.

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	username	None available
company	LDAP (Atts from MS AD)	company	None available
ip_address	- SELECT -		None available

9. Click on the **Attribute Sources and User Lookup** tab.



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

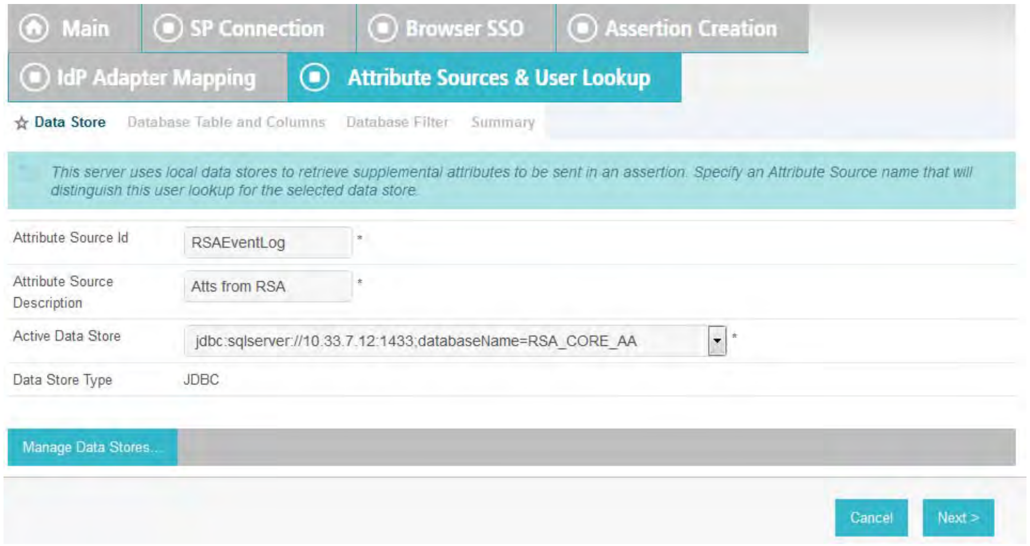
DESCRIPTION	TYPE	ACTION
Atts from MS AD	LDAP	Delete

10. Click **Add Attribute Source**.

11. On the **Attribute Sources & User Lookup** screen, enter a unique name in the **Attribute Source Id** field (e.g **RSAEventLog**).

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

13. For the **Active Data Store** field, select the existing Data Store that connects to the **RSA_CORE_AA** database.



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 the selected data store.

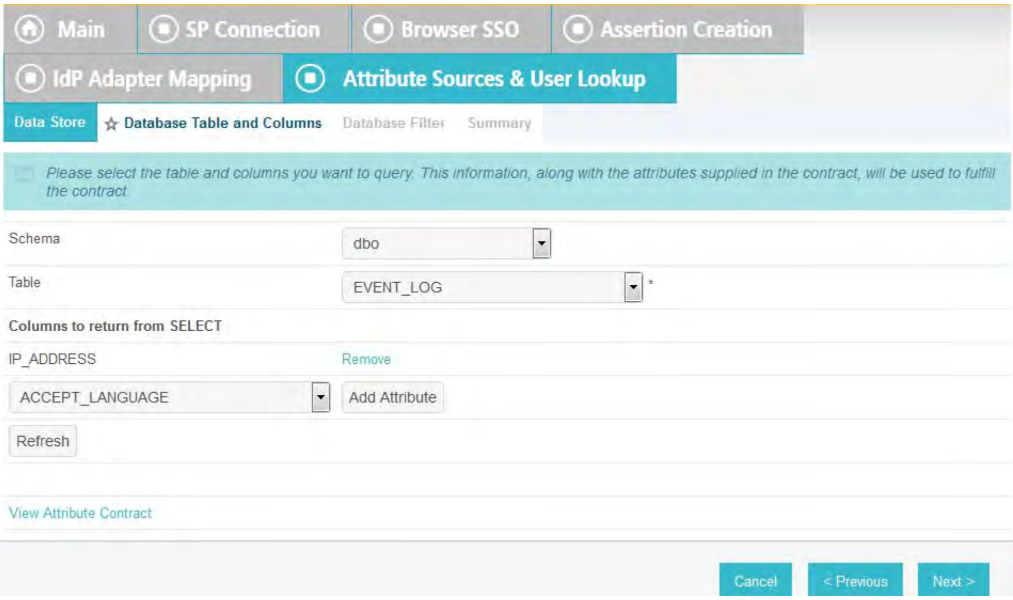
Attribute Source Id	RSAEventLog *
Attribute Source Description	Atts from RSA *
Active Data Store	jdbc:sqlserver://10.33.7.12:1433;databaseName=RSA_CORE_AA *
Data Store Type	JDBC

14. Click **Next**.

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

16. Select the **EVENT_LOG** table.

17. Under the **Columns to return from SELECT**, select the **IP_ADDRESS** column and click **Add Attribute**.



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

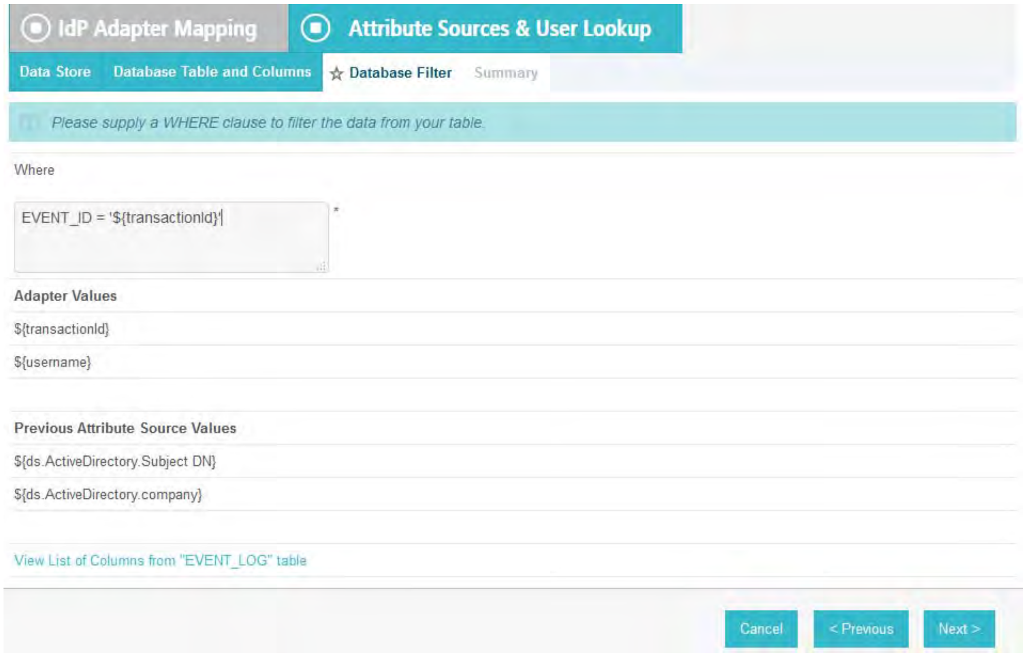
IP_ADDRESS Remove

ACCEPT_LANGUAGE Add Attribute

18. Click **Next**.

19. On the Database Filter screen, enter the text on the following line into the text field for the **Where**. Make sure to include the quotes.

    EVENT_ID = '${transactionid}'


IdP Adapter Mapping
Attribute Sources & User Lookup
Data Store
Database Table and Columns
☆ Database Filter
Summary

Please supply a WHERE clause to filter the data from your table.

Where

EVENT_ID = '${transactionId}' *

Adapter Values

${transactionId}

${username}

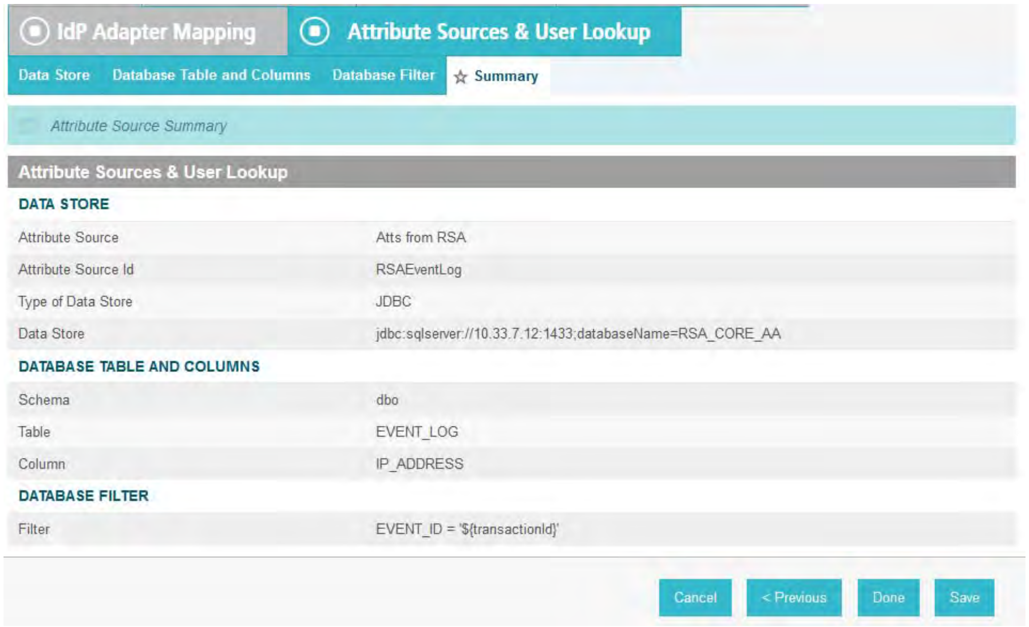
Previous Attribute Source Values

${ds.ActiveDirectory.Subject DN}

${ds.ActiveDirectory.company}

View List of Columns from "EVENT_LOG" table
Cancel
< Previous
Next >

20. Click **Next**.

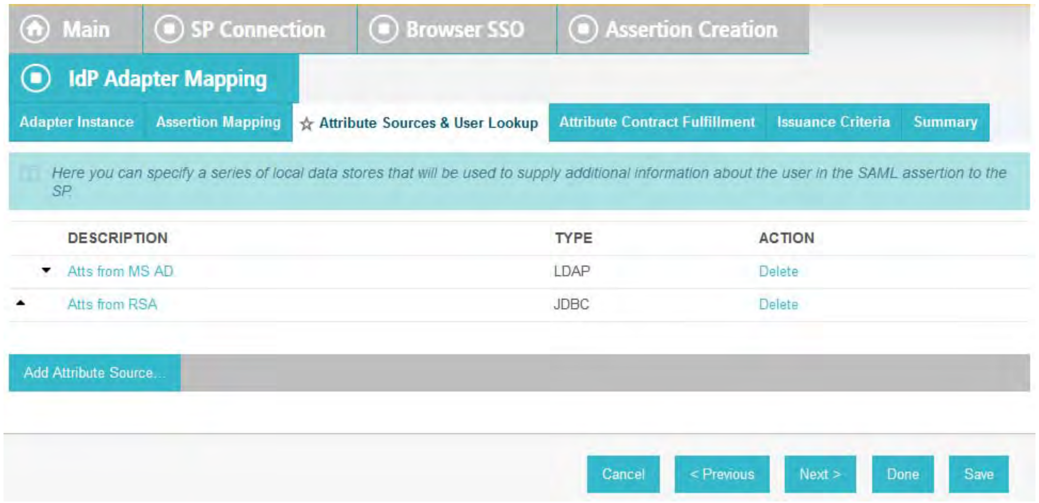


Attribute Sources & User Lookup

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}'

360

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

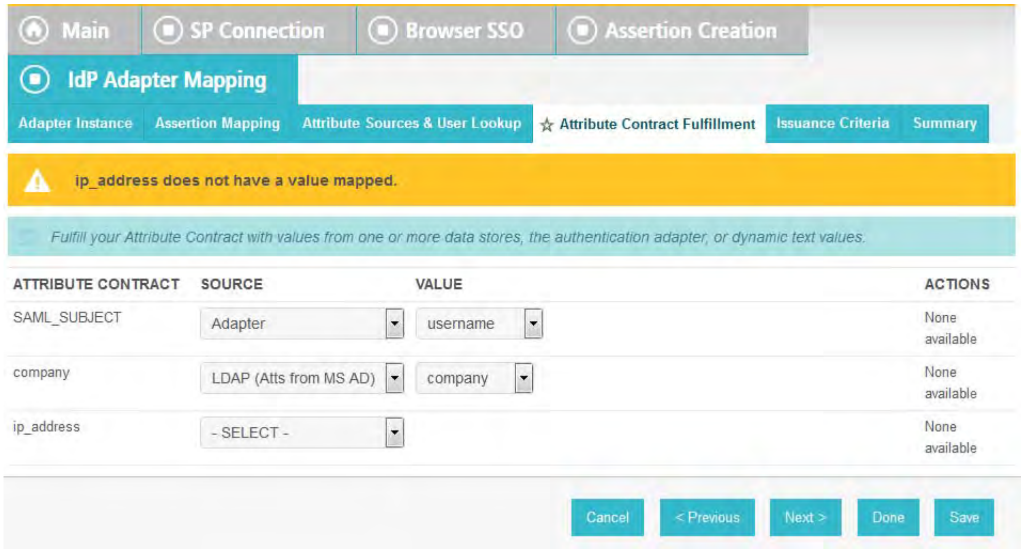


Here you can specify a series of local data stores that will be used to supply additional information about the user in the SAML assertion to the SP.

DESCRIPTION	TYPE	ACTION
▾ Atts from MS AD	LDAP	Delete
▴ Atts from RSA	JDBC	Delete

362

363 22. On the Attribute Sources & User Lookup screen, click **Done**.

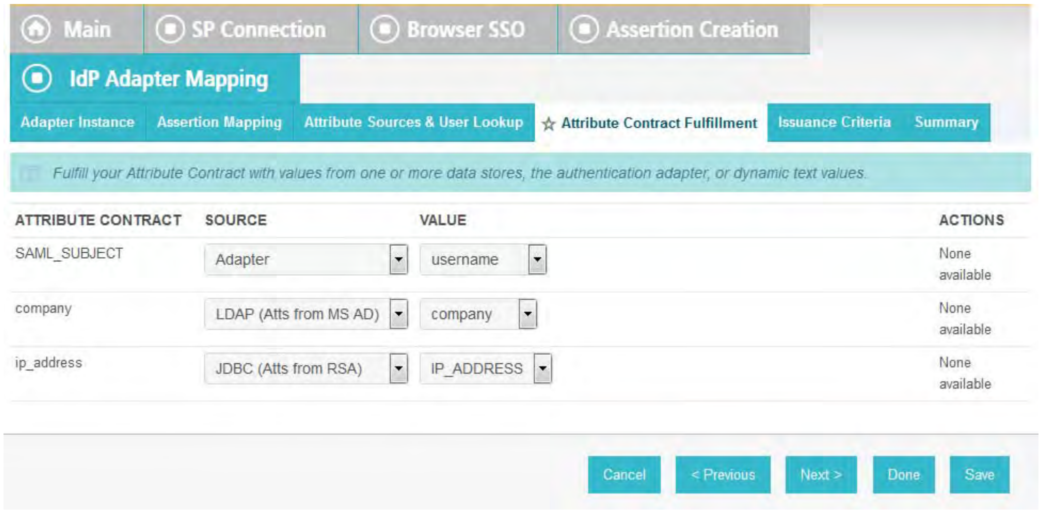


ip_address does not have a value mapped.

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	username	None available
company	LDAP (Atts from MS AD)	company	None available
ip_address	- SELECT -		None available

23. 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**.



Fulfill your Attribute Contract with values from one or more data stores, the authentication adapter, or dynamic text values.

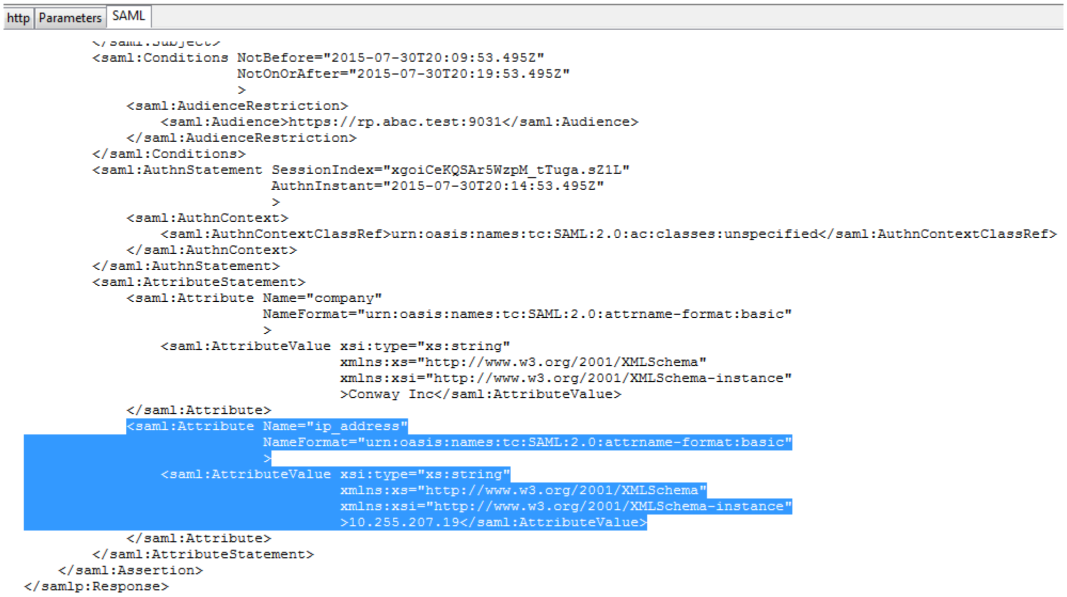
ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Adapter	username	None available
company	LDAP (Atts from MS AD)	company	None available
ip_address	JDBC (Atts from RSA)	IP_ADDRESS	None available

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

6.3.2.3 Functional Test of Pulling Environmental Attributes During Authentication

To test that the Identity Provider's PingFederate server is successfully getting the environmental attributes during the authentication process, follow the instructions in section 6.3.1.1, 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.

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



```
        </saml:Subject>
        <saml:Conditions NotBefore="2015-07-30T20:09:53.495Z"
                         NotOnOrAfter="2015-07-30T20:19:53.495Z"
                         >
            <saml:AudienceRestriction>
                <saml:Audience>https://rp.abac.test:9031</saml:Audience>
            </saml:AudienceRestriction>
        </saml:Conditions>
        <saml:AuthnStatement SessionIndex="xgoiCeKQSAr5WzpM_tTuga.sZ1L"
                             AuthnInstant="2015-07-30T20:14:53.495Z"
                             >
            <saml:AuthnContext>
                <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
            </saml:AuthnContext>
        </saml:AuthnStatement>
        <saml:AttributeStatement>
            <saml:Attribute Name="company"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >Conway Inc</saml:AttributeValue>
            </saml:Attribute>
            <saml:Attribute Name="ip_address"
                            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
                            >
                <saml:AttributeValue xsi:type="xs:string"
                                     xmlns:xs="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                                     >10.255.207.19</saml:AttributeValue>
            </saml:Attribute>
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

Expected Result: Ensure that the attribute you configured to be pulled from the **RSA_CORE_AA** database contains a node. In the preceding example screen shot you can see that there is an Attribute node for the **ip_address** attribute because of the line **<saml:Attribute Name="ip_address"**.

Expected Result: Ensure that the **AttributeValue** node contains the expected value for the attribute from the **RSA_CORE_AA** database. In the preceding example screen shot you can see there is an **AttributeValue** node for the **ip_address** attribute and the value is **10.255.207.19**.

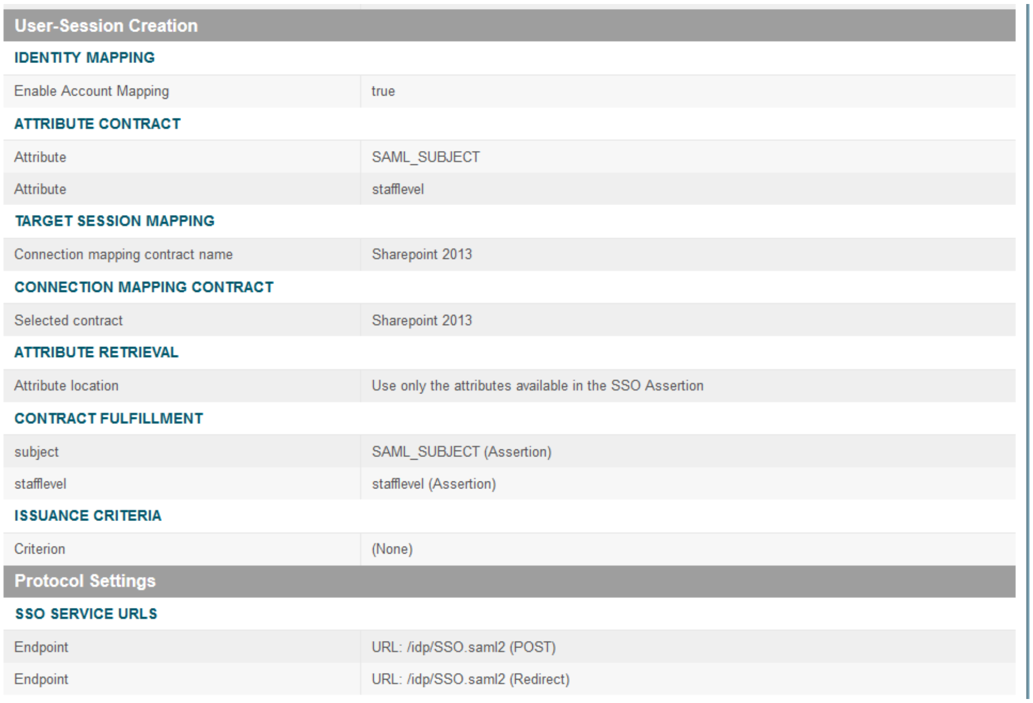
6.3.3 Configure PingFederate-RP to Pull Attributes from the Identity Provider's SAML Exchange

Once the PingFederate-IdP completes the authentication for a user, the Identity Provider will send a SAML message to the PingFederate-RP. That SAML message will contain attributes.

Follow the instructions below to configure the PingFederate-RP to get attributes and their associated values from the SAML message exchange with the Identity Provider. In the example below, the attribute being configured at the Relying Party is the **company** attribute.

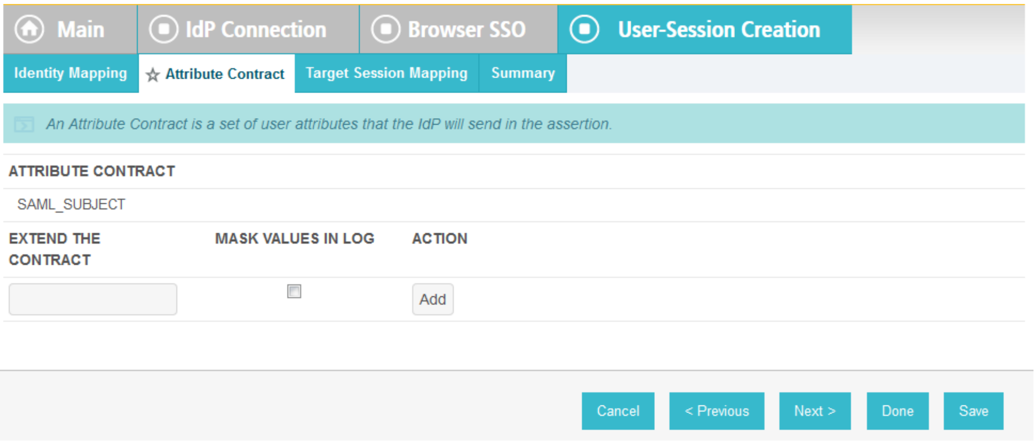
1. Launch your browser and go to: **https://<DNS_NAME>:9999/pingfederate/app**. Replace **DNS_NAME** with the fully qualified name of the Relying Party’s PingFederate server (e.g. **https://rp.abac.test:9999/pingfederate/app**). Log on to the PingFederate application using the credentials you configured during installation.

2. On the **Main** menu, under **IDP CONNECTIONS**, click on the connection that was configured to the Identity Provider in chapter 3 (e.g. **https://idp.abac.test:9031**).



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

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



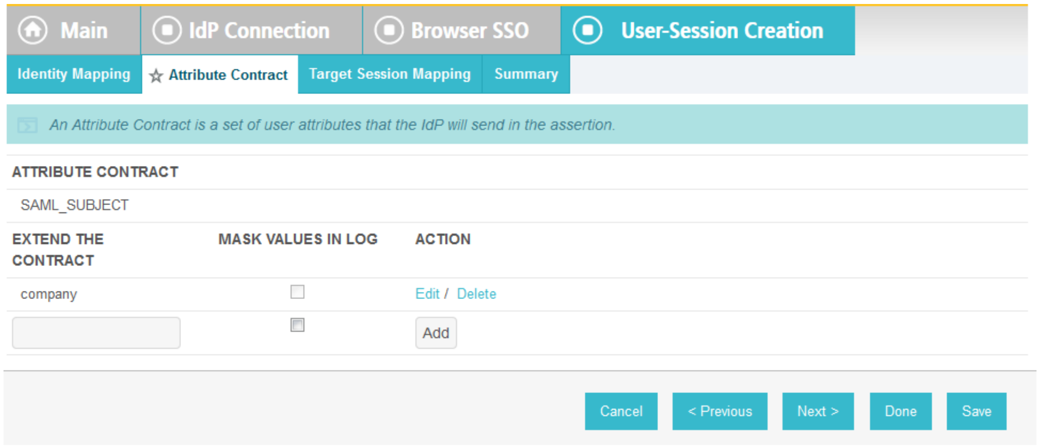
An Attribute Contract is a set of user attributes that the IdP will send in the assertion.

ATTRIBUTE CONTRACT

SAML_SUBJECT

EXTEND THE CONTRACT	MASK VALUES IN LOG	ACTION
	□	Add

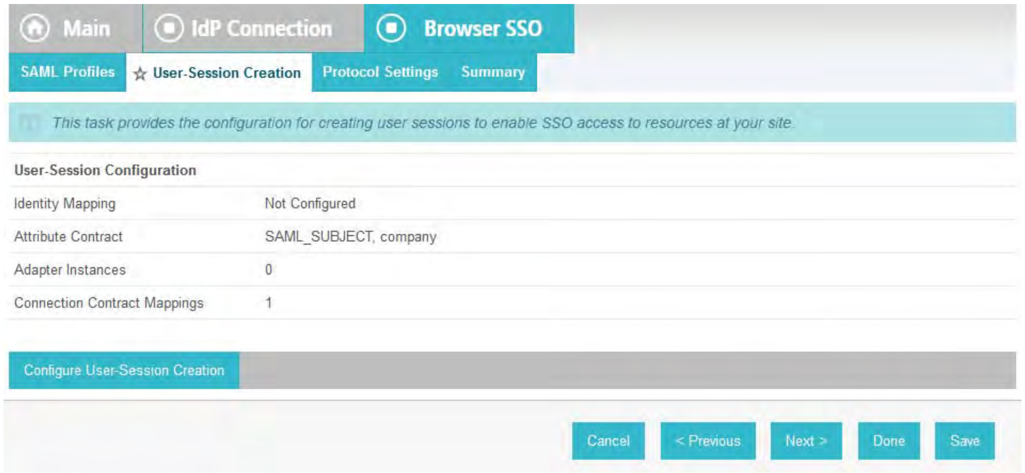
4. On the Attribute Contract screen, under the **EXTEND THE CONTRACT** column, enter the name of the attribute to be pulled from the Identity Provider's message (e.g. **company**) in the empty text field. In the **ACTION** column, click **Add**.



An Attribute Contract is a set of user attributes that the IdP will send in the assertion.

ATTRIBUTE CONTRACT		
SAML_SUBJECT		
EXTEND THE CONTRACT	MASK VALUES IN LOG	ACTION
company	□	Edit / Delete
	□	Add

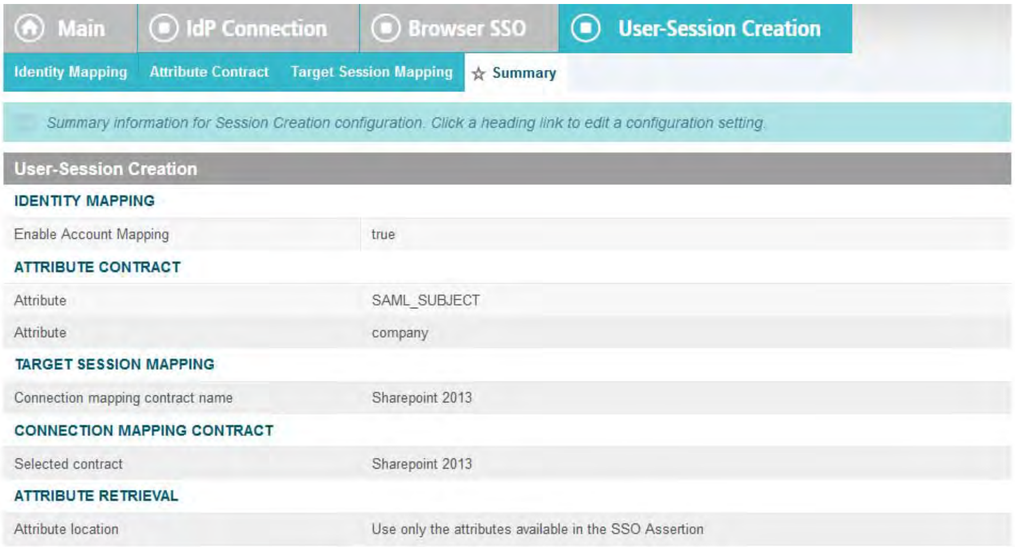
5. Click **Done**.



This task provides the configuration for creating user sessions to enable SSO access to resources at your site.

User-Session Configuration	
Identity Mapping	Not Configured
Attribute Contract	SAML_SUBJECT, company
Adapter Instances	0
Connection Contract Mappings	1

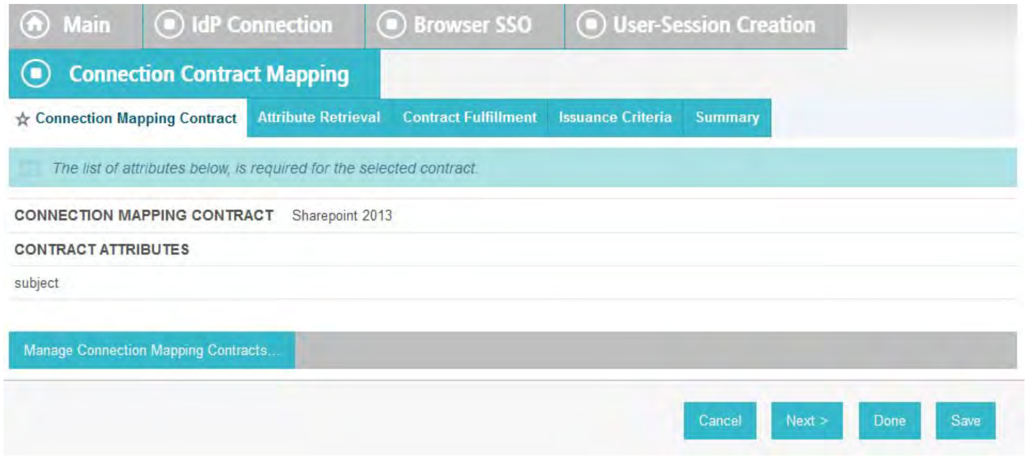
6. On the User-Session Creation screen, click **Configure User-Session Creation**.



Summary information for Session Creation configuration. Click a heading link to edit a configuration setting.

User-Session Creation	
IDENTITY MAPPING	
Enable Account Mapping	true
ATTRIBUTE CONTRACT	
Attribute	SAML_SUBJECT
Attribute	company
TARGET SESSION MAPPING	
Connection mapping contract name	Sharepoint 2013
CONNECTION MAPPING CONTRACT	
Selected contract	Sharepoint 2013
ATTRIBUTE RETRIEVAL	
Attribute location	Use only the attributes available in the SSO Assertion

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



The list of attributes below, is required for the selected contract.

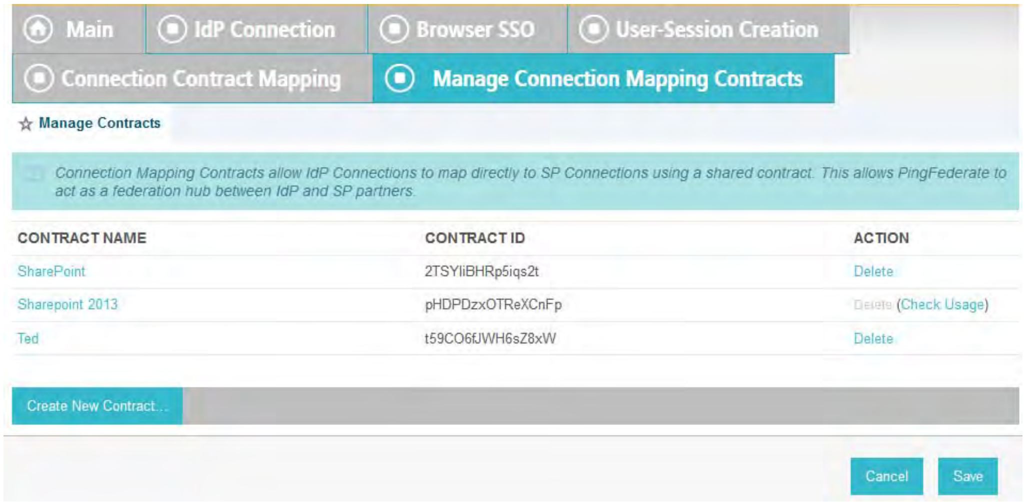
CONNECTION MAPPING CONTRACT Sharepoint 2013

CONTRACT ATTRIBUTES

subject

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 screen shots the contract name is **SharePoint 2013**.

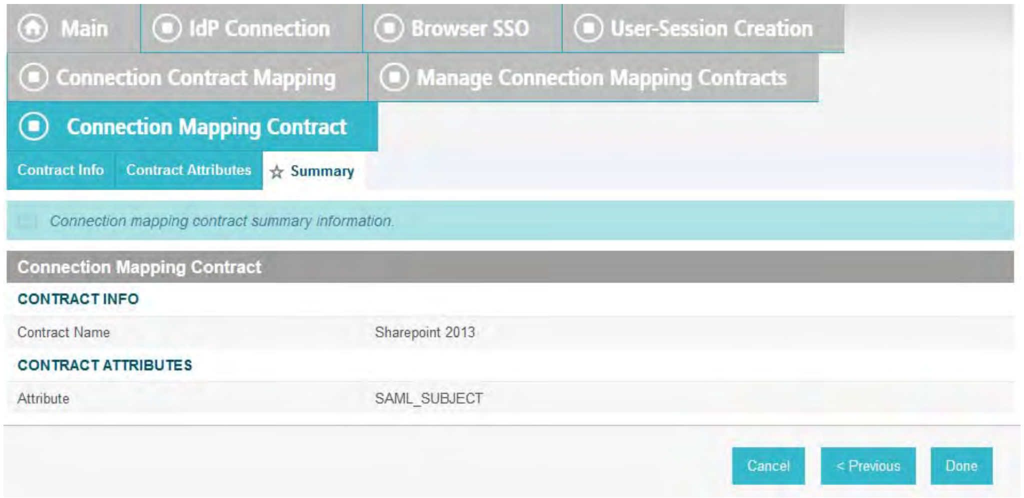
9. Click on **Manage Connection Mapping Contracts**.



Connection Mapping Contracts allow IdP Connections to map directly to SP Connections using a shared contract. This allows PingFederate to act as a federation hub between IdP and SP partners.

CONTRACT NAME	CONTRACT ID	ACTION
SharePoint	2TSYliBHRp5iqs2t	Delete
Sharepoint 2013	pHDPDzxOTReXCnFp	Delete (Check Usage)
Ted	t59CO6fJWH6sZ8xW	Delete

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**).



Connection mapping contract summary information.

Connection Mapping Contract

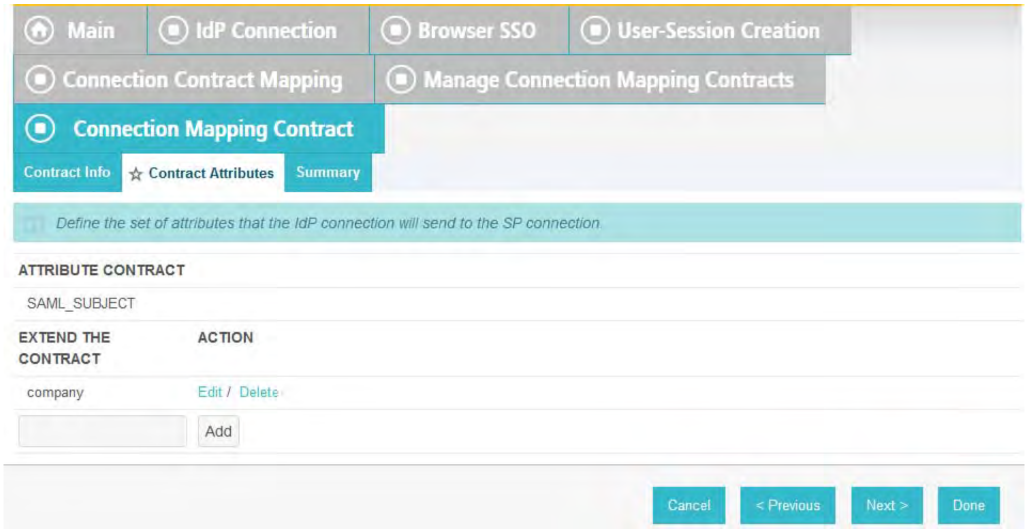
CONTRACT INFO

Contract Name	Sharepoint 2013

CONTRACT ATTRIBUTES

Attribute	SAML_SUBJECT

11. On the Summary screen, click on the **Contract Attributes** link.
12. On the Contract attributes screen, under the **EXTEND THE CONTRACT** column, enter the name of the attribute to be shared with the PingFederate service provider connection (e.g. **company**).
13. In the **ACTION** column, click **Add**.



Define the set of attributes that the IdP connection will send to the SP connection.

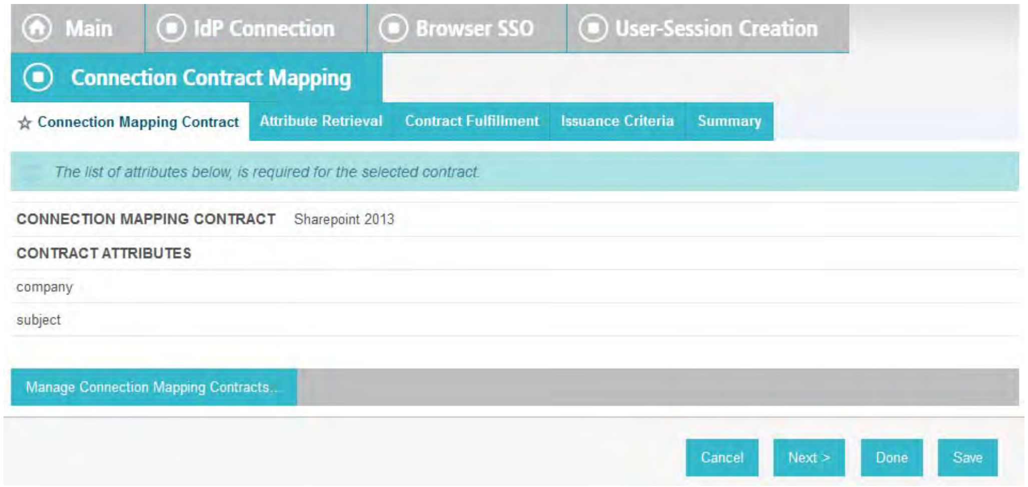
ATTRIBUTE CONTRACT

SAML_SUBJECT

EXTEND THE CONTRACT	ACTION
company	Edit / Delete

14. Click **Done**.
15. On the Manage Contracts screen, click **Save**.

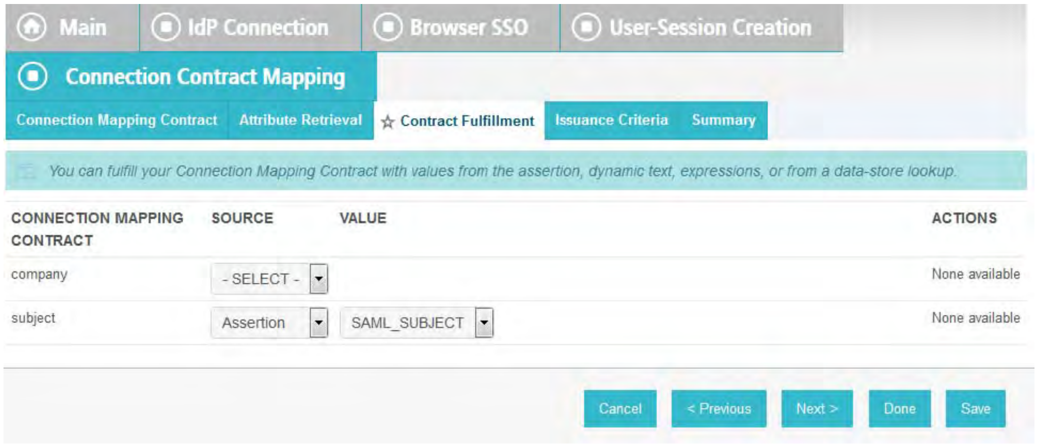
    On the Connection Mapping Contract screen you should see the new attribute (e.g. **company**) listed on the page.



The list of attributes below, is required for the selected contract.

CONNECTION MAPPING CONTRACT	Sharepoint 2013
CONTRACT ATTRIBUTES	
company	
subject	

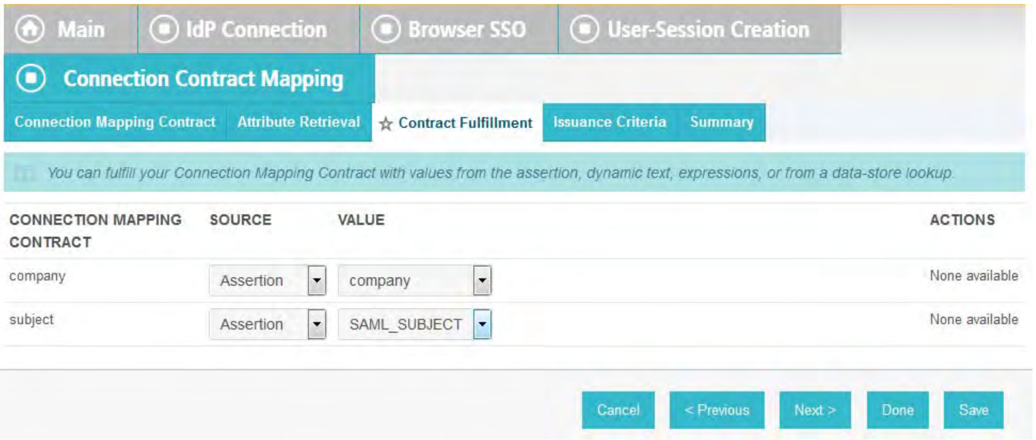
16. Click on the **Contract Fulfillment** tab.



You can fulfill your Connection Mapping Contract with values from the assertion, dynamic text, expressions, or from a data-store lookup.

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

17. On the Contract Fulfillment screen, for the new attribute (e.g. **company**) select **Assertion** for the **SOURCE** field and select **company** for the **VALUE** field.



You can fulfill your Connection Mapping Contract with values from the assertion, dynamic text, expressions, or from a data-store lookup.

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

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

6.4 Configure PingFederate-RP and SharePoint to Pass and Read Attributes

6.4.1 Configure PingFederate-RP to Pass Attributes to SharePoint

Once the PingFederate-IdP completes the authentication for a user, the Identity Provider will send a SAML message to the PingFederate-RP. That SAML message will contain attributes. The PingFederate-RP will then take the attributes and send them to SharePoint via WS-Federation.

Follow the instructions below to configure the PingFederate-RP to pass attributes and their associated values from the Identity Provider to SharePoint. In the example below, the attribute being configured to be passed to SharePoint is the company attribute.

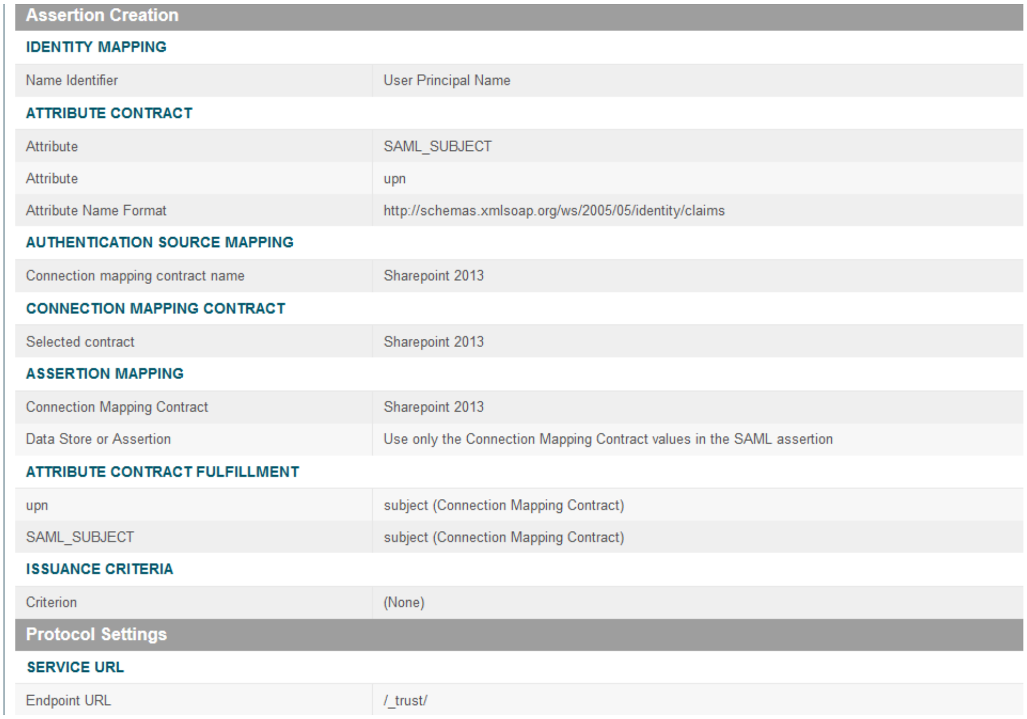
1. Launch your browser and go to: **https://<DNS_NAME>:9999/pingfederate/app**. Replace **DNS_NAME** with the fully qualified name of the Relying Party's PingFederate server (e.g. **https://rp.abac.test:9999/pingfederate/app**).

2. Log on to the PingFederate application using the credentials you configured during installation.

3. On the **Main** menu under SP CONNECTION, click Manage All SP.

4. Click on the link for the WS-Federation connection to the SharePoint instance created in chapter 3 (e.g. **SharePoint**).

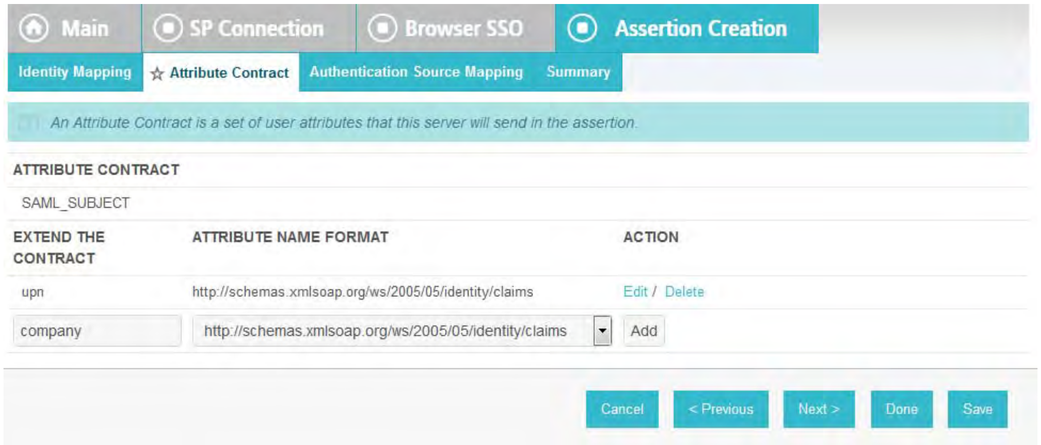
5. On the Activation & Summary screen, scroll down to the Assertion Creation group.



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

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

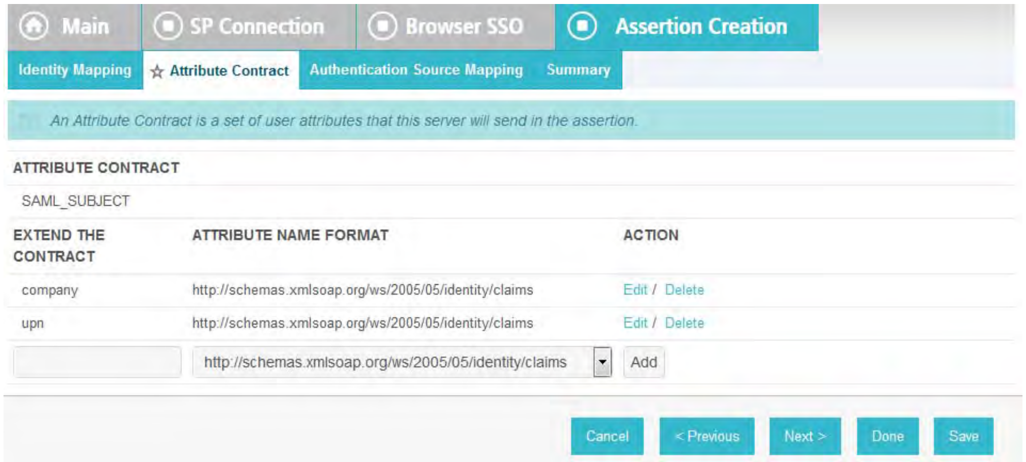
passed from the PingFederate-RP to SharePoint in the empty text field. For the ATTRIBUTE NAME FORMAT select the schemas.xmlsoap.org 2005 identity claims format.



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT		
SAML_SUBJECT		
EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Edit / Delete
company	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Add

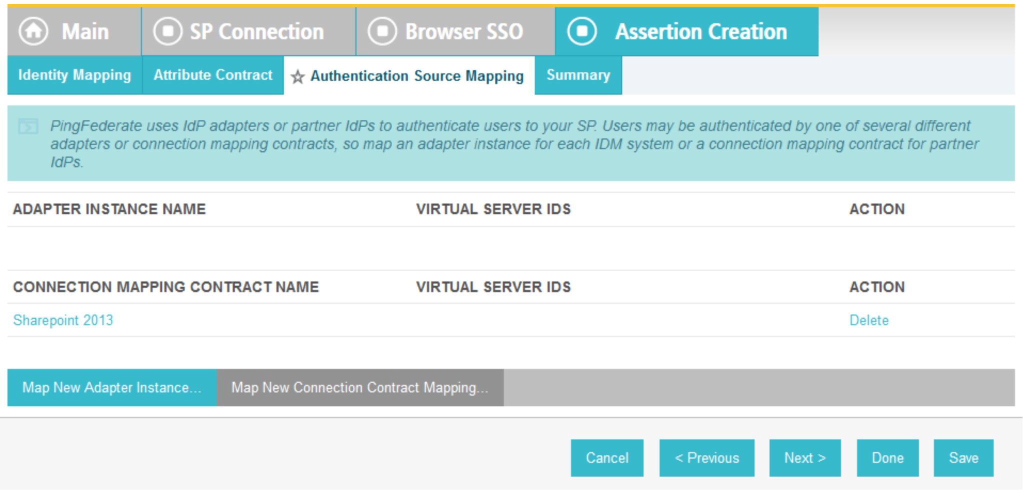
7. Click Add.



An Attribute Contract is a set of user attributes that this server will send in the assertion.

ATTRIBUTE CONTRACT		
SAML_SUBJECT		
EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
company	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Edit / Delete
upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Edit / Delete
	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	Add

8. Click **Done**.

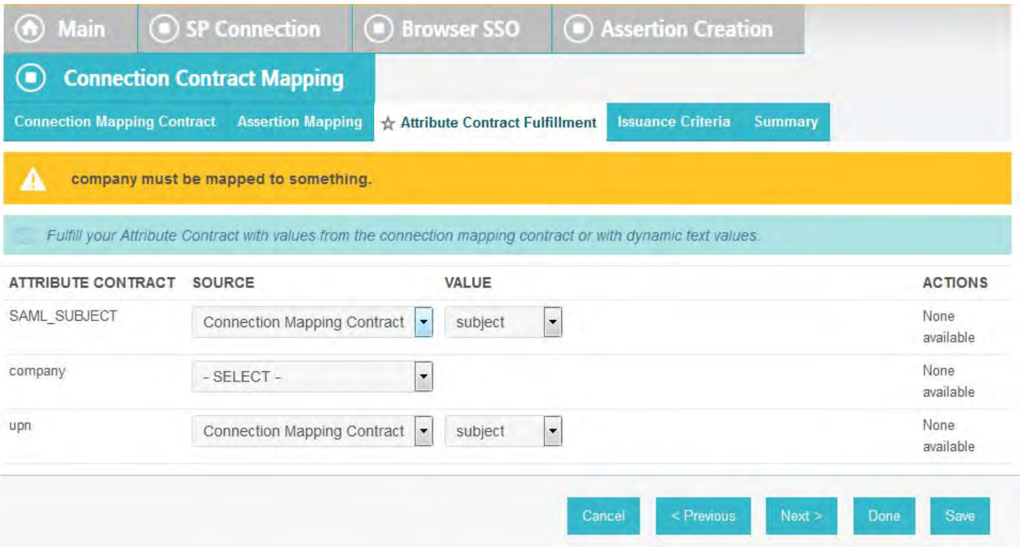


PingFederate uses IdP adapters or partner IdPs to authenticate users to your SP. Users may be authenticated by one of several different adapters or connection mapping contracts, so map an adapter instance for each IDM system or a connection mapping contract for partner IdPs.

ADAPTER INSTANCE NAME	VIRTUAL SERVER IDS	ACTION

CONNECTION MAPPING CONTRACT NAME	VIRTUAL SERVER IDS	ACTION
Sharepoint 2013		Delete

9. On the Authentication Source Mapping screen, under the CONNECTION MAPPING CONTRACT NAME heading click on the name of the connection mapping contract (e.g. **SharePoint 2013**) between this PingFederate SP connection and the PingFederate IdP connection that was configured in section 6.3.3, Configure PingFederate-RP to Pull Attributes from the Identity Provider's SAML Exchange.

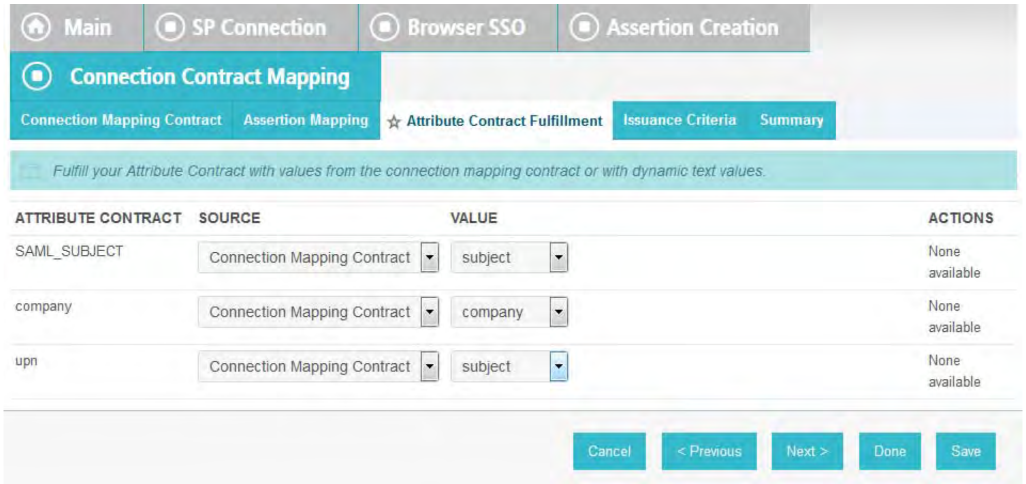


⚠ company must be mapped to something.

Fulfill your Attribute Contract with values from the connection mapping contract or with dynamic text values.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Connection Mapping Contract	subject	None available
company	- SELECT -		None available
upn	Connection Mapping Contract	subject	None available

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



Fulfill your Attribute Contract with values from the connection mapping contract or with dynamic text values.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
SAML_SUBJECT	Connection Mapping Contract	subject	None available
company	Connection Mapping Contract	company	None available
upn	Connection Mapping Contract	subject	None available

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

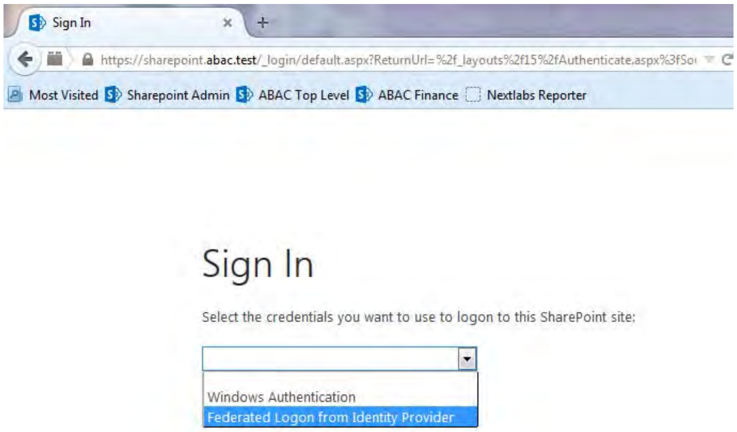
6.4.1.1 Functional Test of PingFederate-RP Passing Attributes to SharePoint

The instructions in this section will help perform a test to ensure that the PingFederate-RP is sending the correct attributes to SharePoint. The Firefox SAML tracer Add-on is used to examine the SAML message.

1. Launch your Firebox browser and select **SAML tracer** from the **Tools** menu.

   This will launch an empty SAML tracer window. Minimize the SAML tracer window. The SAML tracer will automatically record the details of the HTTPS messages in the background.

2. Go back to the main browser window and go to the Relying Party's SharePoint site (e.g. **https://SharePoint.abac.test**).


Sign In
https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSo
Most Visited
Sharepoint Admin
ABAC Top Level
ABAC Finance
Nextlabs Reporter

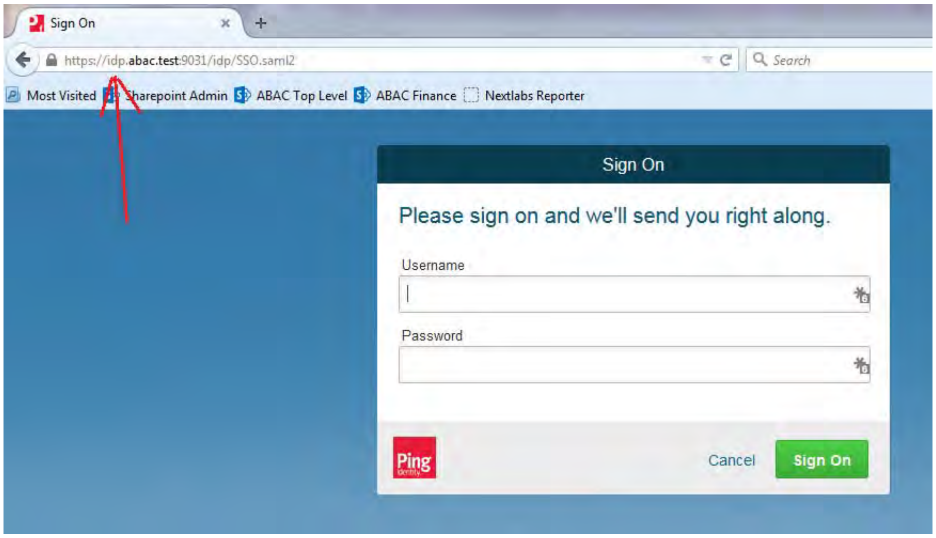
Sign In

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

Windows Authentication
Federated Logon from Identity Provider

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.



Sign On

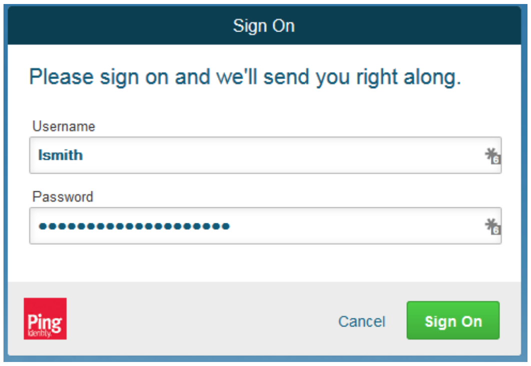
Please sign on and we'll send you right along.

Username

Password

Cancel
Sign On

4. Enter the **Username** and **Password** of the Microsoft AD account created previously in this guide (e.g. **lsmith**).



Please sign on and we'll send you right along.

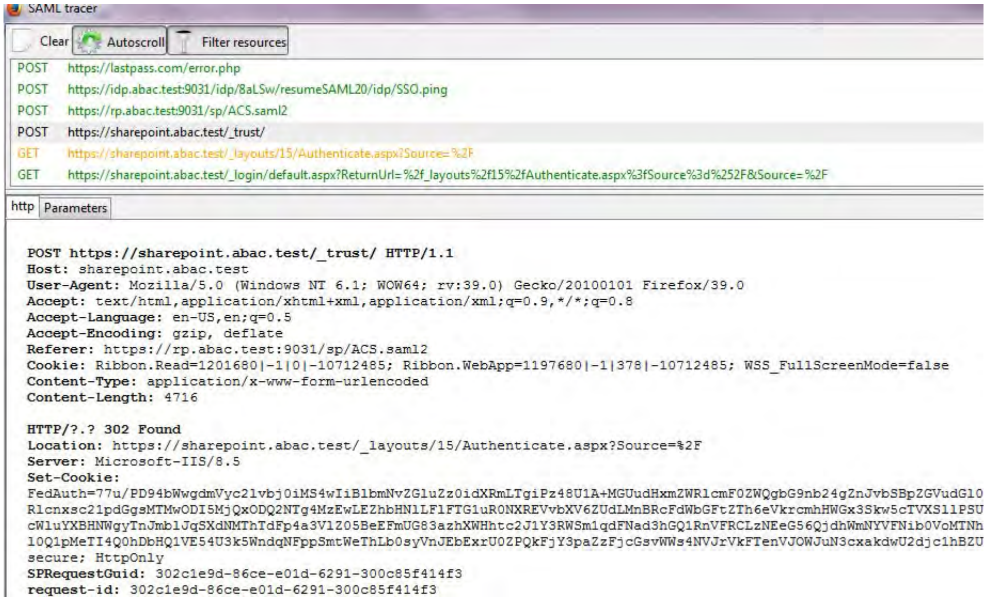
Username: lsmith

Password: ●●●●●●●●●●●●●●●●●●●●

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

   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.

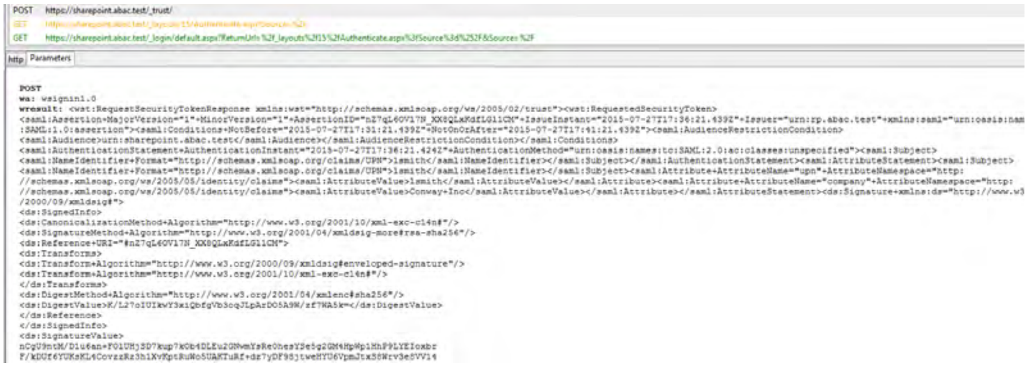
6. Go back to the SAML tracer window. Scroll down the list of messages and click on the **POST** message to **SharePoint _trust** URL to bring up the details of the message in the bottom pane.



```
POST    https://lastpass.com/error.php
POST    https://idp.abac.test:9031/idp/8aLSw/resumeSAML20/idp/SSO.ping
POST    https://rp.abac.test:9031/sp/ACS.saml2
POST    https://sharepoint.abac.test/_trust/
GET     https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
GET     https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
```

```
POST https://sharepoint.abac.test/_trust/ HTTP/1.1
Host: sharepoint.abac.test
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://rp.abac.test:9031/sp/ACS.saml2
Cookie: Ribbon.Read=1201680|-1|0|-10712485; Ribbon.WebApp=1197680|-1|378|-10712485; WSS_FullScreenMode=false
Content-Type: application/x-www-form-urlencoded
Content-Length: 4716

HTTP/?.? 302 Found
Location: https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
Server: Microsoft-IIS/8.5
Set-Cookie:
FedAuth=77u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0idXRmLTgiPz48U1A+MGUudHxmZWRlcmF0ZWQgbG9nb24gZnJvbSBpZGVudGl0
Rlcnxsc21pdGgsMTMwODI5MjQxODQ2NTg4MzEwLEZhbHNlLFlFTG1uR0NXREVvbXV6ZUdLMnBRcFdWbGFtZTh6eVkrcmhHWGx3Skw5cTVXSllPSU
cWluYXBHNWgyTnJmblJqSXdNMThTdFp4a3VlZ05BeEFmUG83azhXWHhtc2J1Y3RWSm1qdFNad3hGQ1RnVFRCLzNEeG56QjdhWmNYVFNib0VoMTNh
l0Q1pMeTI4Q0hDbHQ1VE54U3k5WndqNFppSmtWeThLb0syVnJEbExrU0ZPQkFjY3paZzFjcGsvWWs4NVJrVkFTenVJOWJuN3cxakdwU2djc1hBZU
secure; HttpOnly
SPRequestGuid: 302c1e9d-86ce-e01d-6291-300c85f414f3
request-id: 302c1e9d-86ce-e01d-6291-300c85f414f3
```

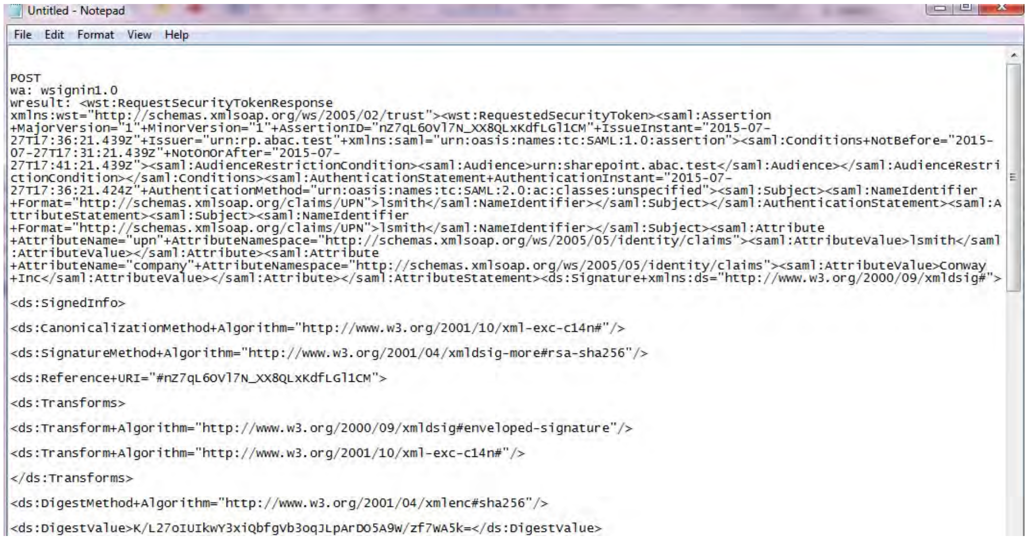
7. Click on the **Parameters** tab for the bottom pane.



```
POST    https://sharepoint.abac.test/_trust/
GET     https://sharepoint.abac.test/_layouts/15/Authenticate.aspx?Source=%2F
GET     https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
```

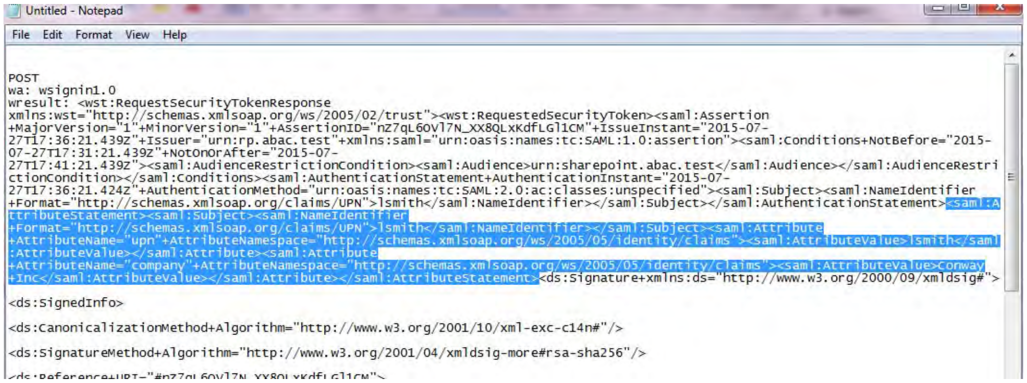
```
POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken>
<saml:Assertion+MajorVersion="1"+MinorVersion="1"+AssertionID="nZ7qL6OVl7N_XX8QLxKdfLGl1CM"+IssueInstant="2015-07-27T17:36:21.439Z"+Issuer="urn:rp.abac.test"+xmlns:saml="urn:oasis:nam
: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:AudienceRestrictionCondition></saml:Conditions>
<saml:AuthenticationStatement+AuthenticationInstant="2015-07-27T17:36:21.424Z"+AuthenticationMethod="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified"><saml:Subject>
<saml:NameIdentifier+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:AttributeStatement><saml:Subject>
<saml:NameIdentifier+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute+AttributeName="upn"+AttributeNamespace="http:
//schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>lsmith</saml:AttributeValue></saml:Attribute><saml:Attribute+AttributeName="company"+AttributeNamespace="http:
//schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Conway+Inc</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><ds:Signature+xmlns:ds="http://www.w3
/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="#nZ7qL6OVl7N_XX8QLxKdfLGl1CM">
<ds:Transforms>
<ds:Transform+Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod+Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
<ds:DigestValue>K/L27oIUIkwY3xiQbfgVb3oqJLpArDO5A9W/zf7WA5k=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
nCgU9ntM/D1u6an+FO1UHj5D7kup7kOb4DLEu2GNwmYsReOhesY5e5g2GM4HpWp1MhP9LYEIoxbr
F/kDUf6YUKsKL4CovzzRz3h1XvKptRuWo5UAKTuRf+dz7yDF95jtweHYU6VpmJtx58Wrv3e5VV14
```

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.



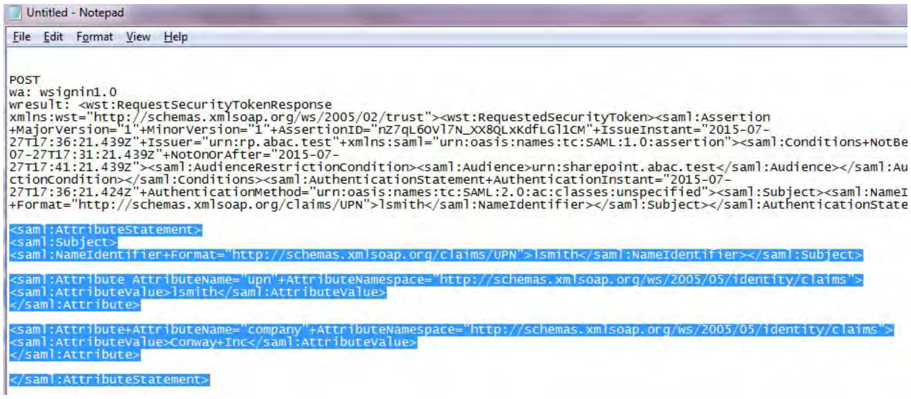
```
POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionID="nZ7qL6OVl7N_XX8QLxKdfLGl1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp.abac.test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><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">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:A
ttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>lsmith</saml
:AttributeValue></saml:Attribute><saml:Attribute
+AttributeName="company"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Conway
+Inc</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><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="#nZ7qL6OVl7N_XX8QLxKdfLGl1CM">

<ds:Transforms>

<ds:Transform+Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>

<ds:Transform+Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>

</ds:Transforms>

<ds:DigestMethod+Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

<ds:DigestValue>K/L27oIUIkwY3xiQbfgVb3oqJLpArDO5A9W/zf7WA5k=</ds:DigestValue>
```

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="nZ7qL6OVl7N_XX8QLxKdfLGl1CM"+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">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationStatement><saml:A
ttributeStatement><saml:Subject><saml:NameIdentifier
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject><saml:Attribute
+AttributeName="upn"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>lsmith</saml
:AttributeValue></saml:Attribute><saml:Attribute
+AttributeName="company"+AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims"><saml:AttributeValue>Conway
+Inc</saml:AttributeValue></saml:Attribute></saml:AttributeStatement><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="#nZ7qL6OVl7N_XX8QLxKdfLGl1CM">
```

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.



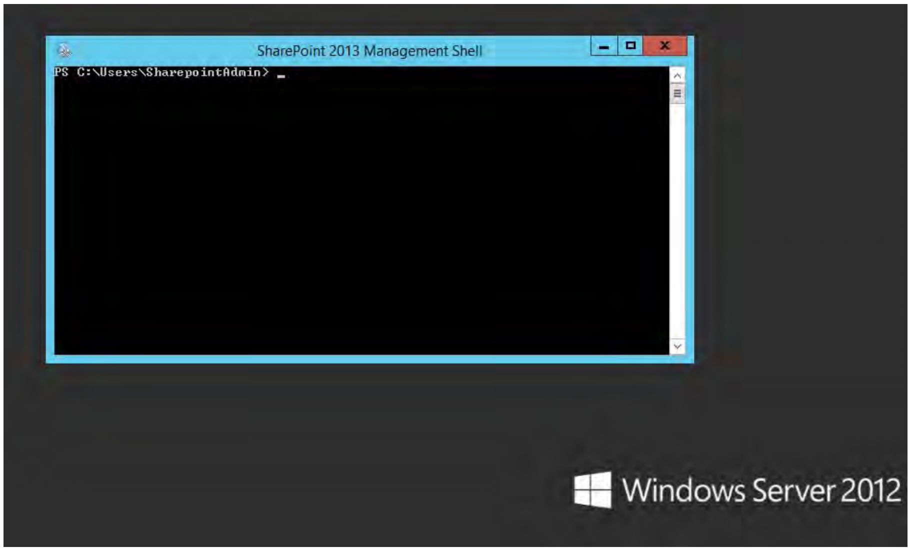
```
POST
wa: wsignin1.0
wresult: <wst:RequestSecurityTokenResponse
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust"><wst:RequestedSecurityToken><saml:Assertion
+MajorVersion="1"+MinorVersion="1"+AssertionID="nZ7qL6OVl7N_XX8QLxKdfLGl1CM"+IssueInstant="2015-07-
27T17:36:21.439Z"+Issuer="urn:rp.abac.test"+xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"><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
+Format="http://schemas.xmlsoap.org/claims/UPN">lsmith</saml:NameIdentifier></saml:Subject></saml:AuthenticationState

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

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

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

</saml:AttributeStatement>
```

Expected Result: Within the **AttributeStatement** node, there should be multiple **Attribute** sub-nodes. There should be an **Attribute** sub-node that has an **AttributeName** value of **company**. 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 expected value (e.g. **Conway Inc**) for the **company** attribute that was pulled from Microsoft AD (e.g. **<saml:AttributeValue> Conway+Inc </saml:AttributeValue>**) for the specific user (e.g. **lsmith**) that authenticated at the Sign On screen.

6.4.2 Configure SharePoint to Read Custom Attributes from PingFederate-RP

The PingFederate-RP will send attributes to SharePoint via WS-Federation. Follow the instructions below to configure SharePoint to read the attributes and load them into the web session. In the example below, the attribute being configured to be read by SharePoint is the **company** attribute.

1. Using SharePoint administrator credentials, log on to the server that hosts SharePoint for the Relying Party.
2. Click on the **Start** menu and navigate to **SharePoint 2013 Products** group. Open SharePoint 2013 Management Shell.



```
PS C:\Users\SharepointAdmin> _
```

3. Enter each of the commands displayed below the next paragraph into the management shell to configure a new attribute, **company** for the existing Trusted Identity Token Issuer named **Federated Logon from Identity Provider**. Enter each command separately, and enter a carriage return after the command. If the command executed successfully, management shell will not provide any feedback. If an error occurs, the management shell will display the error.

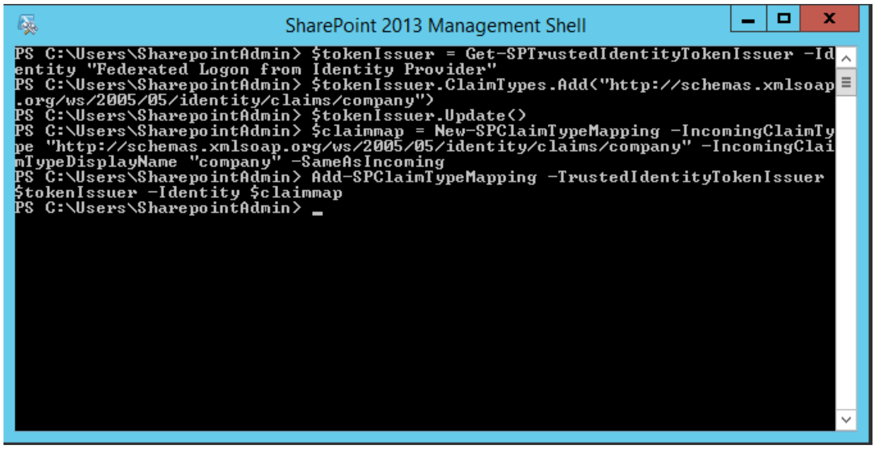
```
$tokenIssuer = Get-SPTrustedIdentityTokenIssuer -Identity "Federated
Logon from Identity Provider"
```

```
$tokenIssuer.ClaimTypes.Add("http://schemas.xmlsoap.org/ws/2005/05/
identity/claims/company")
```

```
$tokenIssuer.Update()
```

```
 $claimmap = New-SPClaimTypeMapping -IncomingClaimType
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company"
-IncomingClaimTypeDisplayName "company" -SameAsIncoming
```

4. `Add-SPClaimTypeMapping -TrustedIdentityTokenIssuer $tokenIssuer -Identity $claimmap`.

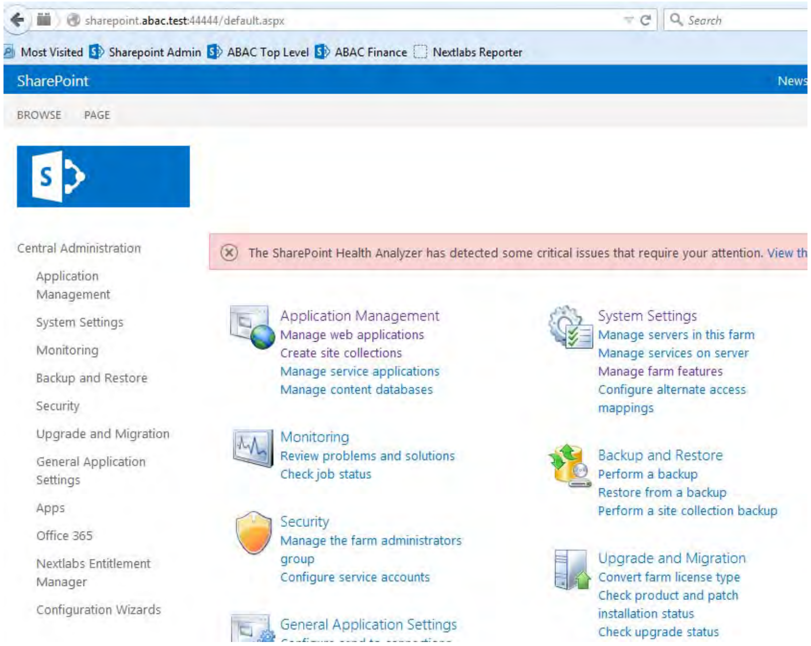


```
PS C:\Users\SharepointAdmin> $tokenIssuer = Get-SPTrustedIdentityTokenIssuer -Id
entity "Federated Logon from Identity Provider"
PS C:\Users\SharepointAdmin> $tokenIssuer.ClaimTypes.Add("http://schemas.xmlsoap
.org/ws/2005/05/identity/claims/company")
PS C:\Users\SharepointAdmin> $tokenIssuer.Update()
PS C:\Users\SharepointAdmin> $claimmap = New-SPClaimTypeMapping -IncomingClaimTy
pe "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company" -IncomingClai
mTypeDisplayName "company" -SameAsIncoming
PS C:\Users\SharepointAdmin> Add-SPClaimTypeMapping -TrustedIdentityTokenIssuer
$tokenIssuer -Identity $claimmap
PS C:\Users\SharepointAdmin> _
```

6.4.2.1 Functional Test of SharePoint Reading Attributes from PingFederate-RP

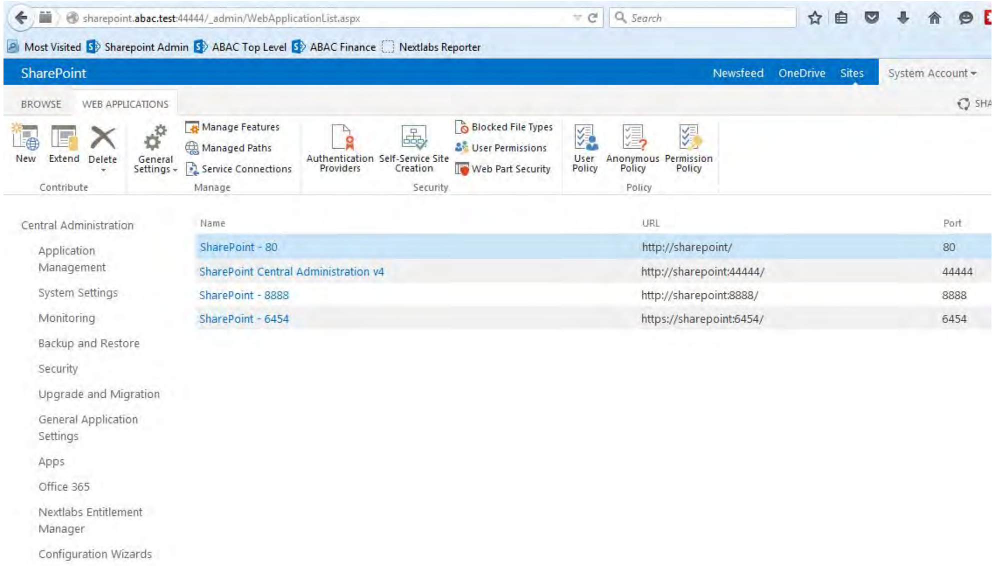
The instructions in this section will help perform a test to ensure that SharePoint can read the attributes sent in messages from the PingFederate-RP.

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



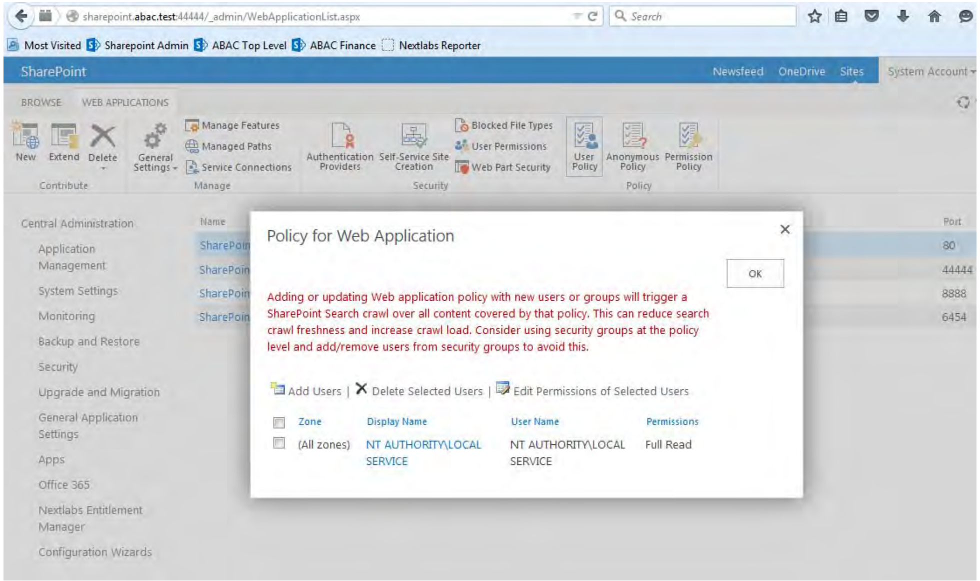
The SharePoint Health Analyzer has detected some critical issues that require your attention. View th

4. Under the **Application Management** group, click on **Manage Web Applications**.
5. Click on the web application that contains the SharePoint site you are managing (e.g. **SharePoint - 80**). SharePoint highlights the web application row that you clicked.



Name	URL	Port
SharePoint - 80	http://sharepoint/	80
SharePoint Central Administration v4	http://sharepoint:44444/	44444
SharePoint - 8888	http://sharepoint:8888/	8888
SharePoint - 6454	https://sharepoint:6454/	6454

6. Click **User Policy**.

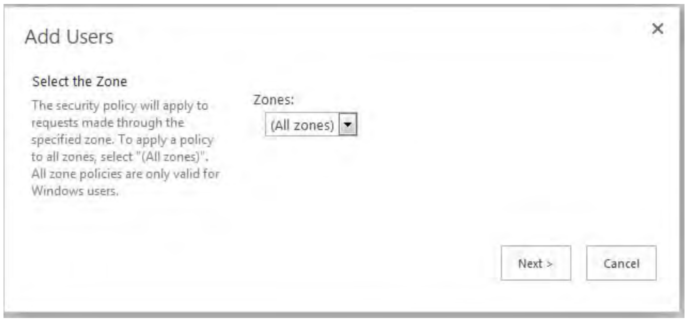


Policy for Web Application

Adding or updating Web application policy with new users or groups will trigger a SharePoint Search crawl over all content covered by that policy. This can reduce search crawl freshness and increase crawl load. Consider using security groups at the policy level and add/remove users from security groups to avoid this.

□	Zone	Display Name	User Name	Permissions
□	(All zones)	NT AUTHORITY\LOCAL SERVICE	NT AUTHORITY\LOCAL SERVICE	Full Read

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



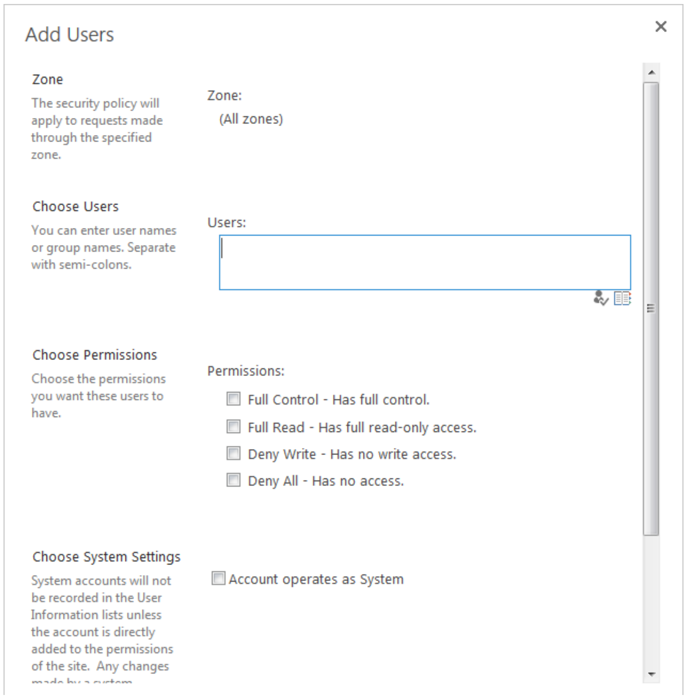
Add Users

Select the Zone

The security policy will apply to requests made through the specified zone. To apply a policy to all zones, select "(All zones)". All zone policies are only valid for Windows users.

Zones: (All zones)

8. Click **Next**.



Add Users

Zone

The security policy will apply to requests made through the specified zone.

Zone:
(All zones)

Choose Users

You can enter user names or group names. Separate with semi-colons.

Users:

Choose Permissions

Choose the permissions you want these users to have.

Permissions:
- □ Full Control - Has full control.
- □ Full Read - Has full read-only access.
- □ Deny Write - Has no write access.
- □ Deny All - Has no access.

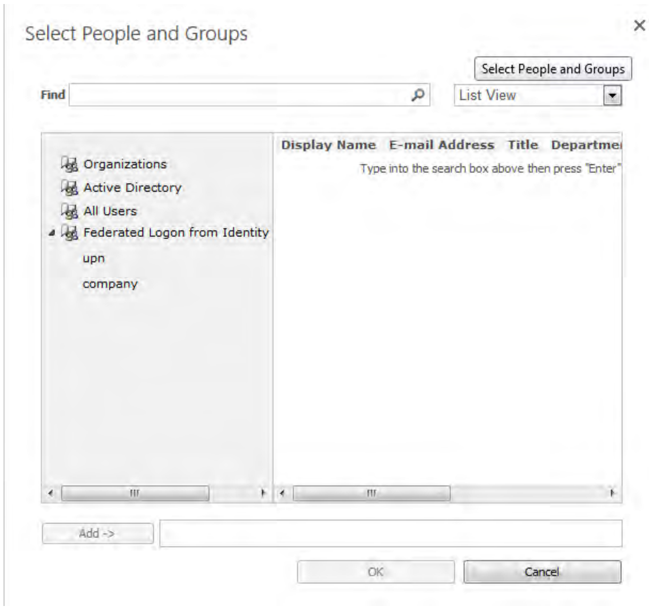
Choose System Settings

System accounts will not be recorded in the User Information lists unless the account is directly added to the permissions of the site. Any changes

□ Account operates as System

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

   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.



Select People and Groups

Display Name	E-mail Address	Title	Departme

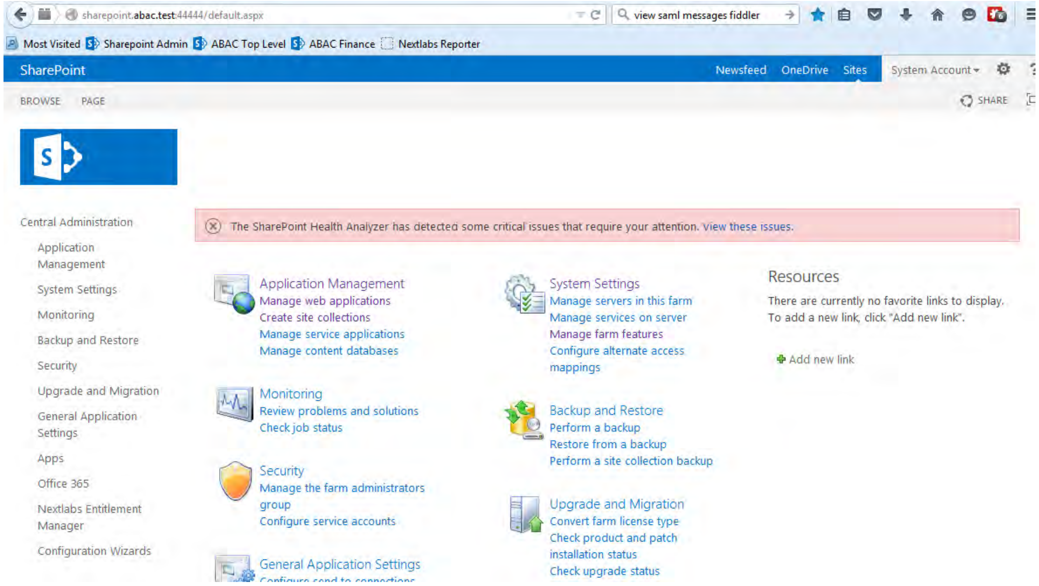
Type into the search box above then press "Enter"

6.5 Configure the Claims Viewer Web Part at the SharePoint Site

Follow the instructions in this section to configure the Claims Viewer Web part at the SharePoint site. The Claims Viewer is a component that is useful to the SharePoint administrator because it displays a list of the attributes that are loaded into the web session. This list can be used to validate that the correct set of attributes and associated values are being passed from the PingFederate-RP, and that SharePoint is correctly configured to read the attributes.

1. Log on to the server that hosts SharePoint for the Relying Party.
2. Launch your browser and go the SharePoint central administration page (e.g. **http://SharePoint.abac.test:44444/default.aspx**). Log on using the credentials of the SharePoint administrator.

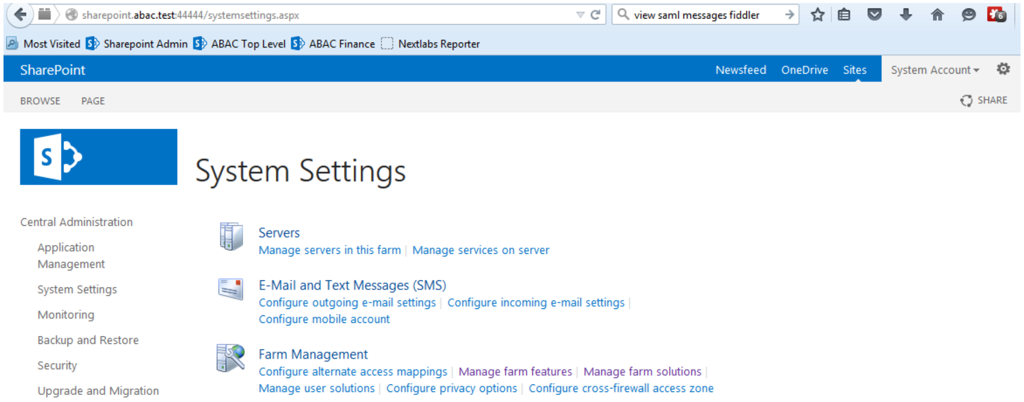
   The central administration home page displays.



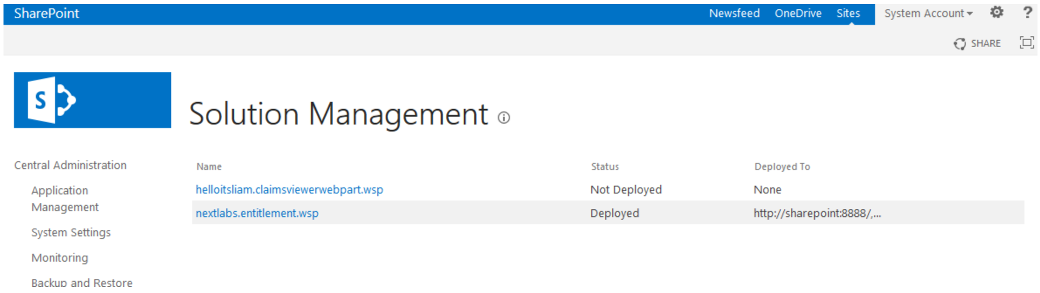
The SharePoint Health Analyzer has detected some critical issues that require your attention. View these issues.

There are currently no favorite links to display. To add a new link, click "Add new link".

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


sharepoint.abac.test:44444/systemsettings.aspx
view saml messages fiddler
Most Visited
Sharepoint Admin
ABAC Top Level
ABAC Finance
Nextlabs Reporter
SharePoint
Newsfeed
OneDrive
Sites
System Account
BROWSE
PAGE
SHARE
System Settings
Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
Servers
Manage servers in this farm | Manage services on server
E-Mail and Text Messages (SMS)
Configure outgoing e-mail settings | Configure incoming e-mail settings |
Configure mobile account
Farm Management
Configure alternate access mappings | Manage farm features | Manage farm solutions |
Manage user solutions | Configure privacy options | Configure cross-firewall access zone

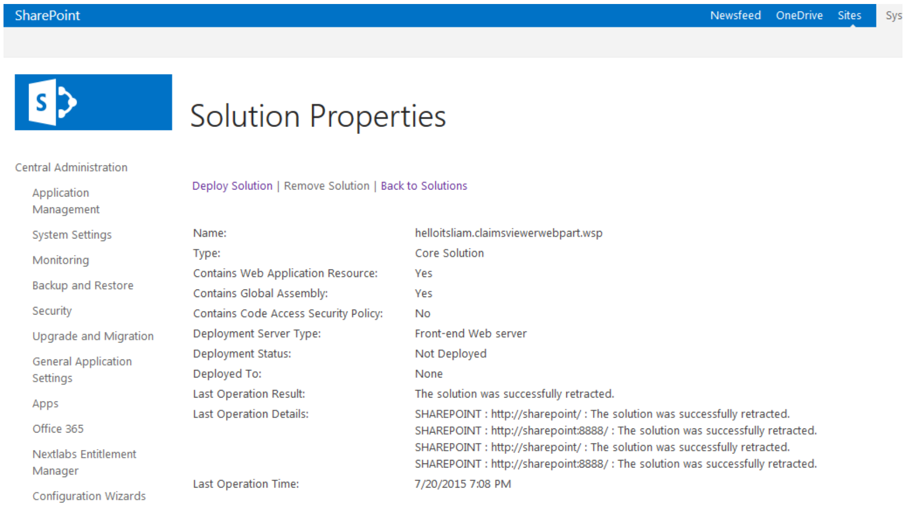
4. On the Farm Management menu, click **Manage Farm Solutions**.



Solution Management

Name	Status	Deployed To
helloitsliam.claimsviewerwebpart.wsp	Not Deployed	None
nextlabs.entitlement.wsp	Deployed	http://sharepoint:8888/,...

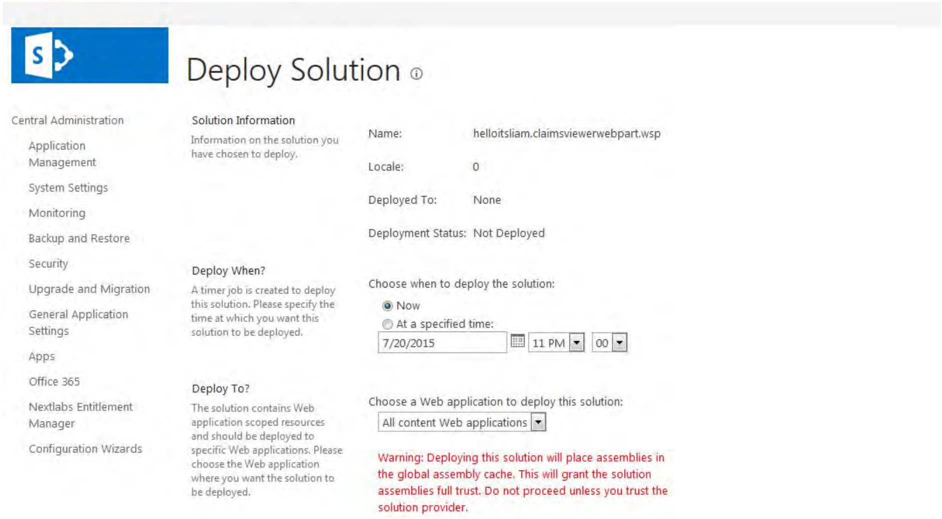
5. Click on the **helloitsliam.claimsviewerwebpart.wsp** link.



Solution Properties

Name:	helloitsliam.claimsviewerwebpart.wsp
Type:	Core Solution
Contains Web Application Resource:	Yes
Contains Global Assembly:	Yes
Contains Code Access Security Policy:	No
Deployment Server Type:	Front-end Web server
Deployment Status:	Not Deployed
Deployed To:	None
Last Operation Result:	The solution was successfully retracted.
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

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



Deploy Solution

Solution Information

Information on the solution you have chosen to deploy.

Name: helloitsliam.claimsviewerwebpart.wsp

Locale: 0

Deployed To: None

Deployment Status: Not Deployed

Deploy When?

A timer job is created to deploy this solution. Please specify the time at which you want this solution to be deployed.

Choose when to deploy the solution:

● Now

○ At a specified time:

7/20/2015 11 PM 00

Deploy To?

The solution contains Web application scoped resources and should be deployed to specific Web applications. Please choose the Web application where you want the solution to be deployed.

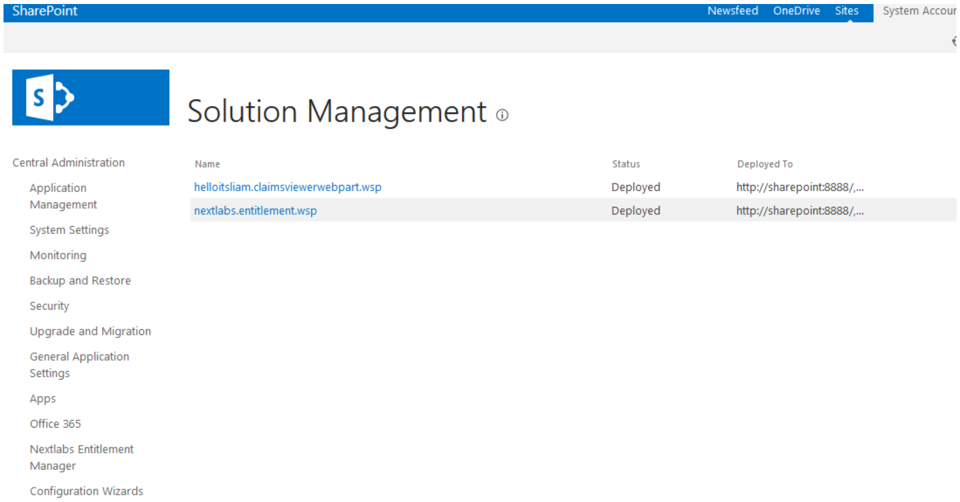
Choose a Web application to deploy this solution:

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.

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

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



SharePoint Newsfeed OneDrive Sites System Accour

Solution Management

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

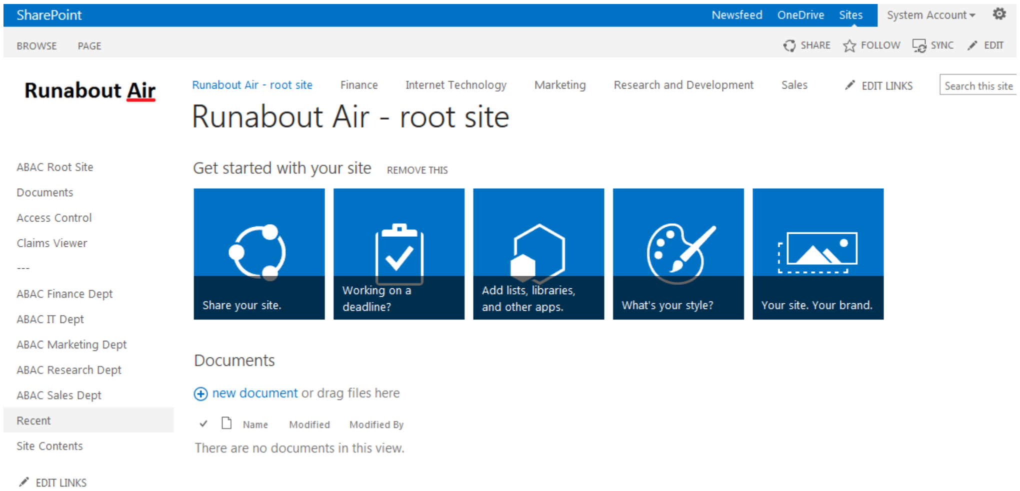
Name	Status	Deployed To
helloitsliam.claimsviewerwebpart.wsp	Deployed	http://sharepoint:8888/,...
nextlabs.entitlement.wsp	Deployed	http://sharepoint:8888/,...

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

6.5.1 Configure SharePoint Claims Viewer

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

1. Log on to the Relying Party’s SharePoint site (e.g. **https://SharePoint.abac.test**) using the credentials of the SharePoint administrator. Select **Windows Authentication** on the Sign On screen.



SharePoint Newsfeed OneDrive Sites System Account ▾

BROWSE PAGE SHARE FOLLOW SYNC EDIT

Runabout Air

Runabout Air - root site Finance Internet Technology Marketing Research and Development Sales EDIT LINKS Search this site

Runabout Air - root site

- ABAC Root Site
- Documents
- Access Control
- Claims Viewer
- ---
- ABAC Finance Dept
- ABAC IT Dept
- ABAC Marketing Dept
- ABAC Research Dept
- ABAC Sales Dept
- Recent
- Site Contents
- EDIT LINKS

Get started with your site REMOVE THIS

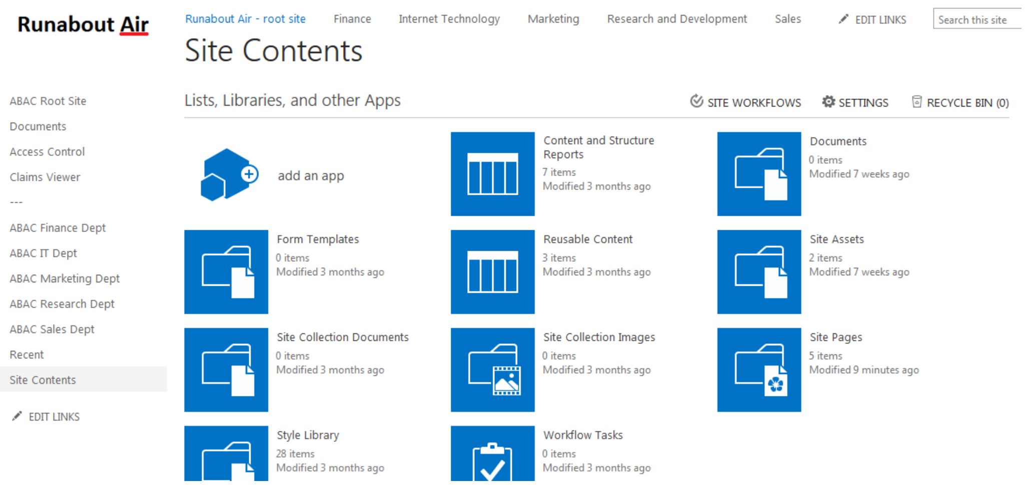
Documents

⊕ new document or drag files here

✓ Name Modified Modified By

There are no documents in this view.

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



Site Contents

Lists, Libraries, and other Apps

Content and Structure Reports
7 items
Modified 3 months ago

Documents
0 items
Modified 7 weeks ago

Form Templates
0 items
Modified 3 months ago

Reusable Content
3 items
Modified 3 months ago

Site Assets
2 items
Modified 7 weeks ago

Site Collection Documents
0 items
Modified 3 months ago

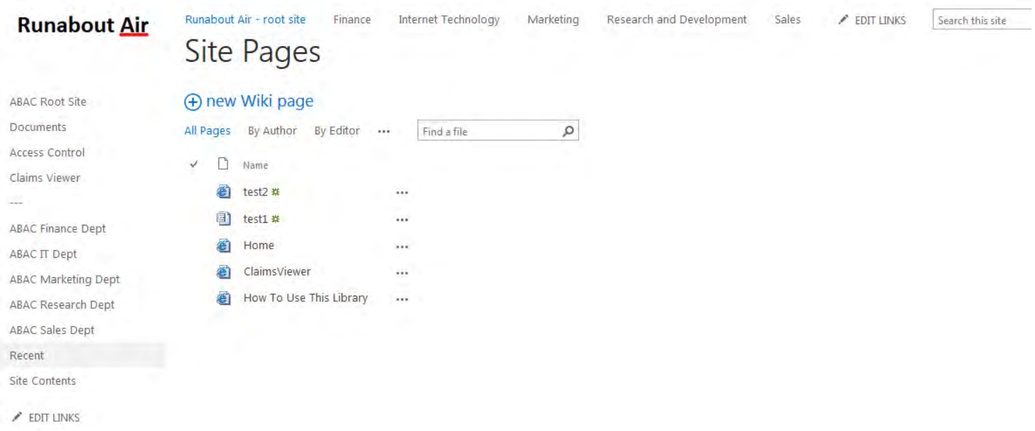
Site Collection Images
0 items
Modified 3 months ago

Site Pages
5 items
Modified 9 minutes ago

Style Library
28 items
Modified 3 months ago

Workflow Tasks
0 items
Modified 3 months ago

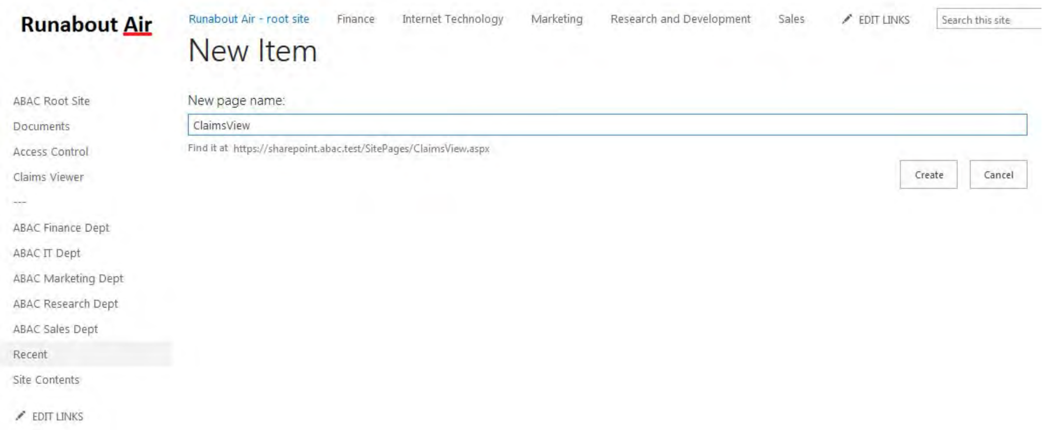
3. Click on the **Site Pages** library. This will show a list of the existing pages on the site.



Site Pages

Name
test2
test1
Home
ClaimsViewer
How To Use This Library

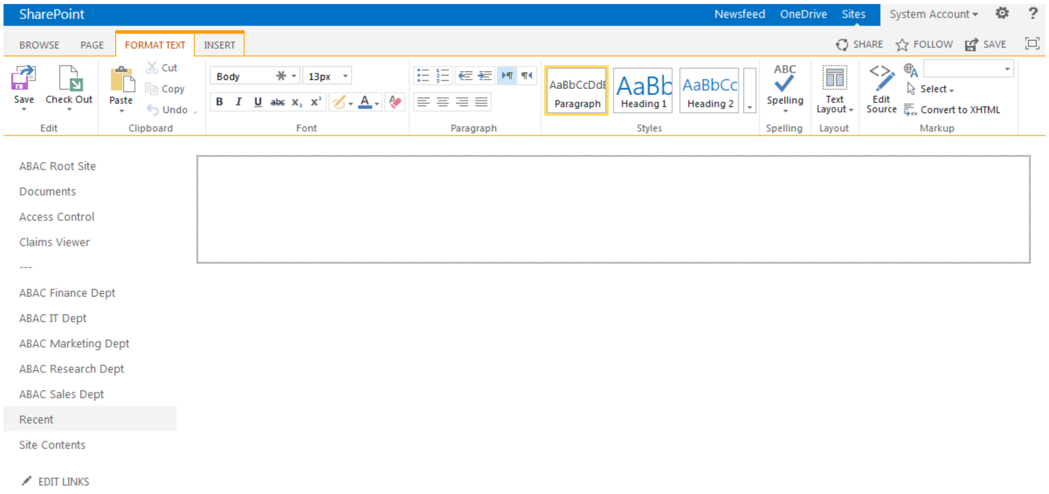
4. Click the **new Wiki page** link to add a new page. This link may be named differently, depending on the type of SharePoint template your site is configured with. Enter a name for the new page (e.g. **ClaimsView**).



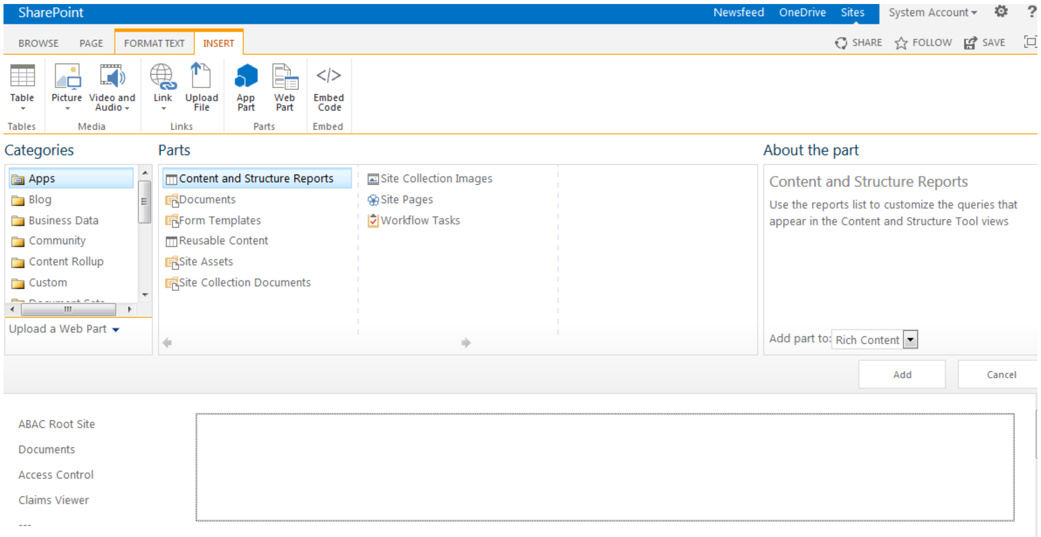
New Item

New page name:
ClaimsView
Find it at https://sharepoint.abac.test/SitePages/ClaimsView.aspx

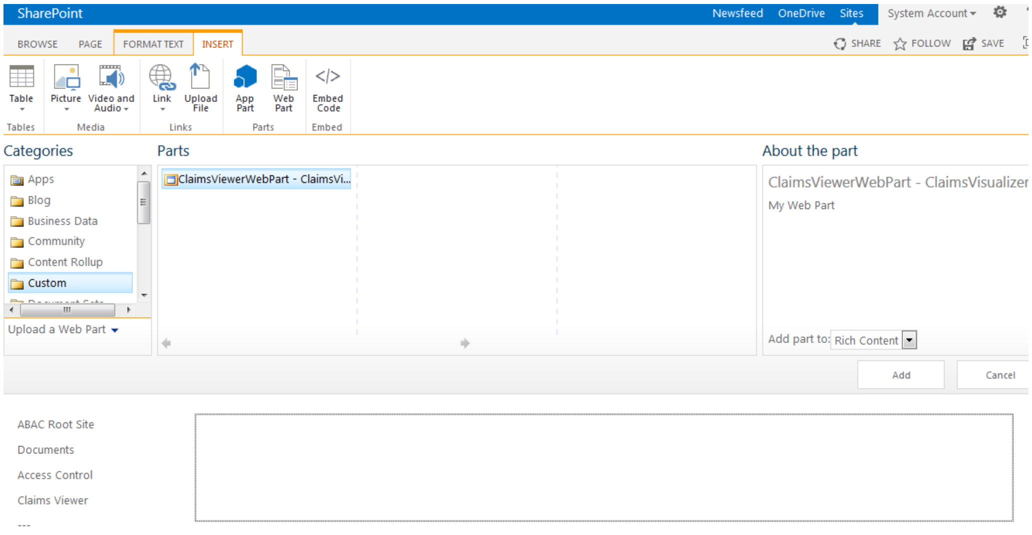
5. Click **Create**. The SharePoint page editor for the newly added page displays.



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

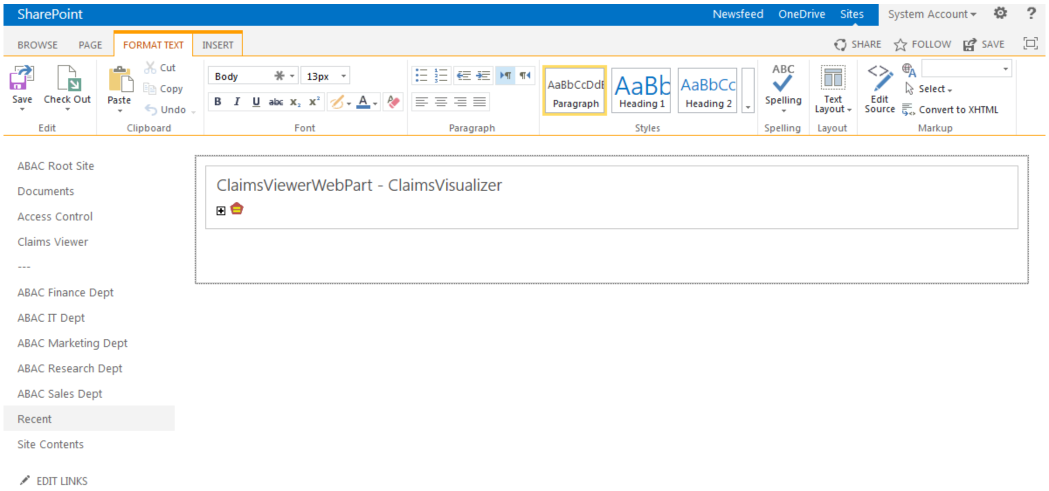


7. From the **Categories** list, select **Custom**. From the **Parts** list, select **ClaimsViewerWebPart**.



Add part to: Rich Content

8. Click **Add**.

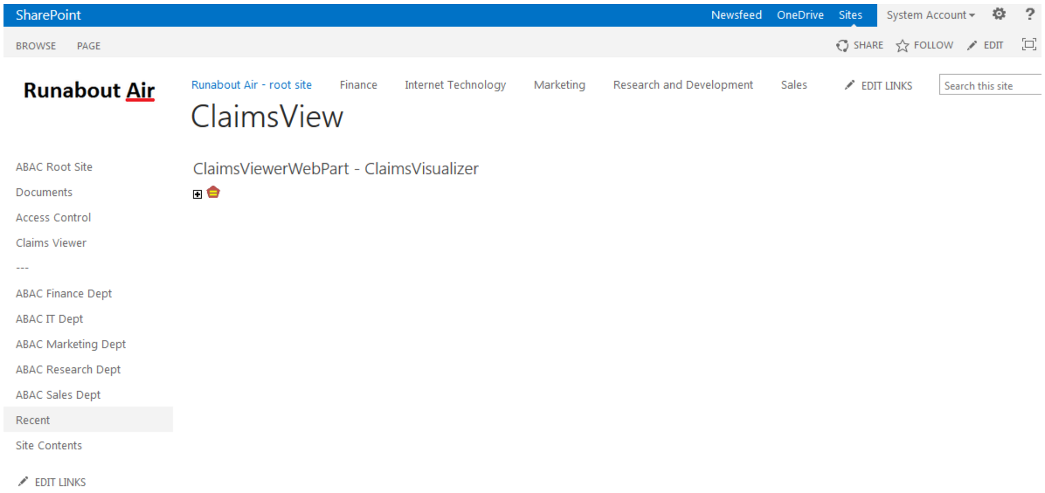


ClaimsViewerWebPart - ClaimsVisualizer

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

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

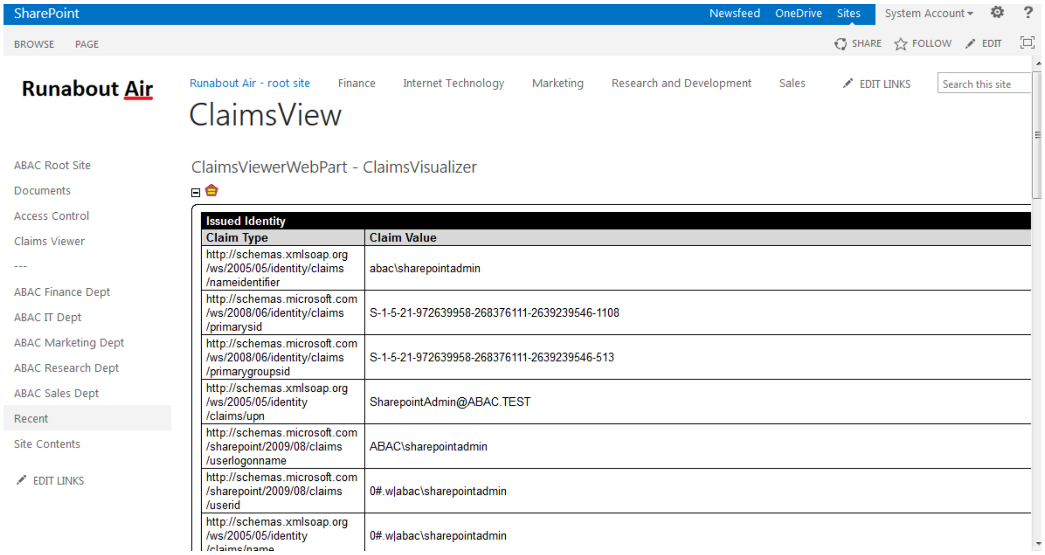
   The Claims Viewer Web Part on the page displays. It is collapsed by default.



ClaimsView

ClaimsViewerWebPart - ClaimsVisualizer

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



ClaimsView

ClaimsViewerWebPart - ClaimsVisualizer

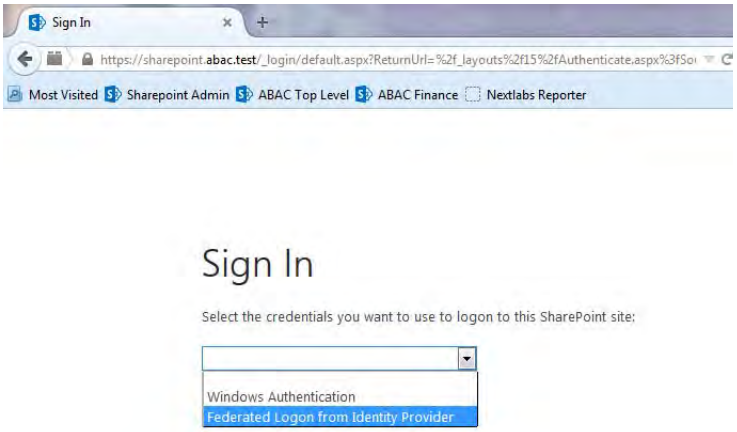
Issued Identity

Claim Type	Claim Value
http://schemas.xmlsoap.org /ws/2005/05/identity/claims /nameidentifier	abac\sharepointadmin
http://schemas.microsoft.com /ws/2008/06/identity/claims /primarysid	S-1-5-21-972639958-268376111-2639239546-1108
http://schemas.microsoft.com /ws/2008/06/identity/claims /primarygroupsid	S-1-5-21-972639958-268376111-2639239546-513
http://schemas.xmlsoap.org /ws/2005/05/identity /claims/upn	SharepointAdmin@ABAC.TEST
http://schemas.microsoft.com /sharepoint/2009/08/claims /userlogonname	ABAC\sharepointadmin
http://schemas.microsoft.com /sharepoint/2009/08/claims /userid	0#.w|abac\sharepointadmin
http://schemas.xmlsoap.org /ws/2005/05/identity /claims/name	0#.w|abac\sharepointadmin

6.6 Functional Test of All Configurations for this Chapter

The instructions in this section will perform an integrated test all of the configurations in this chapter. Using the browser, you will log on using an account that was created in Microsoft AD. Then you will use the SharePoint claims viewer to validate that the newly configured attributes are passed from the Identity Provider to the Relying Party and that the attributes are successfully loaded into the SharePoint web session.

1. Launch your browser and go to the Relying Party's SharePoint site (e.g. **https://SharePoint.abac.test**).


Sign In
https://sharepoint.abac.test/_login/default.aspx?ReturnUrl=%2f_layouts%2f15%2fAuthenticate.aspx%3fSo
Most Visited
Sharepoint Admin
ABAC Top Level
ABAC Finance
Nextlabs Reporter

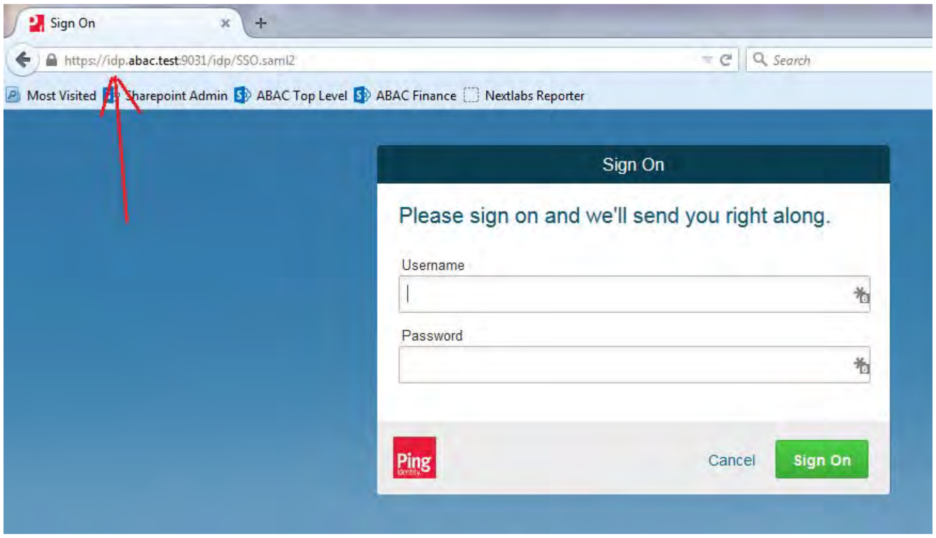
Sign In

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

Windows Authentication
Federated Logon from Identity Provider

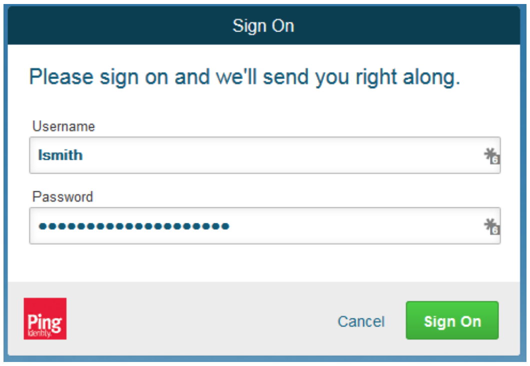
2. Select **Federated Logon from Identity Provider**.

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



Please sign on and we'll send you right along.

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



Sign On

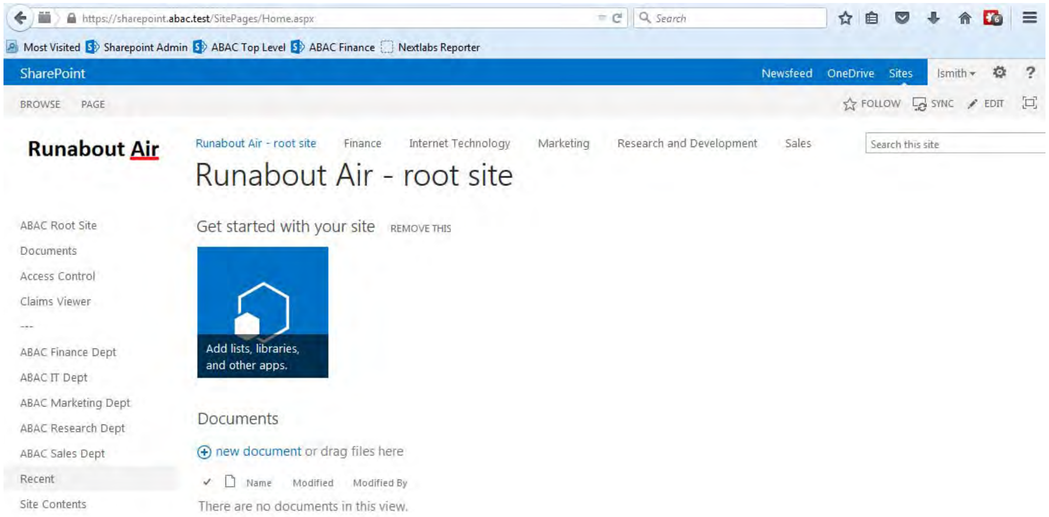
Please sign on and we'll send you right along.

Username: lsmith

Password: ••••••••••••••••••••

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

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



https://sharepoint.abac.test/SitePages/Home.aspx

Runabout Air - root site

Get started with your site REMOVE THIS

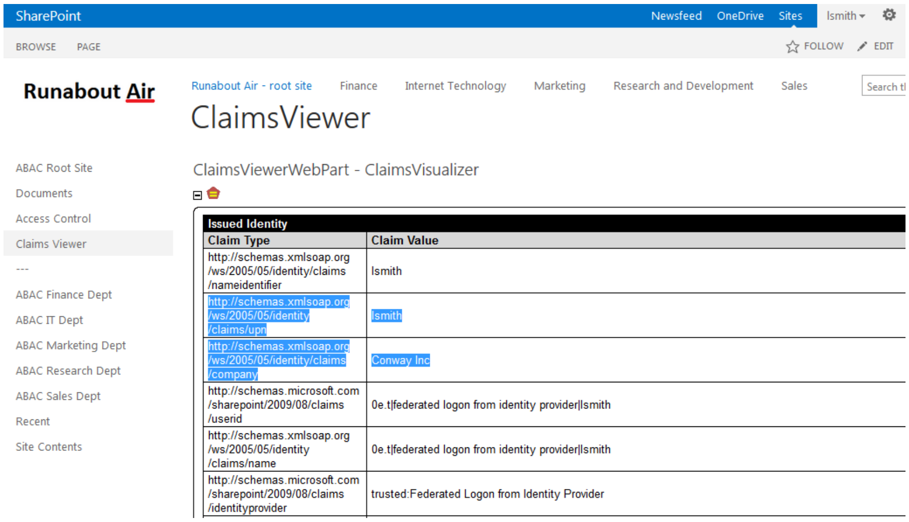
Documents

new document or drag files here

There are no documents in this view.

5. Once you arrive at the SharePoint site home page, navigate to the claims viewer page that was created in the previous 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.

   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**.



ClaimsViewer

ClaimsViewerWebPart - ClaimsVisualizer

Issued Identity	
Claim Type	**Claim Value**
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	lsmith
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	lsmith
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company	Conway Inc
http://schemas.microsoft.com/sharepoint/2009/08/claims/userid	0e.t|federated logon from identity provider|lsmith
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0e.t|federated logon from identity provider|lsmith
http://schemas.microsoft.com/sharepoint/2009/08/claims/identityprovider	trusted:Federated Logon from Identity Provider

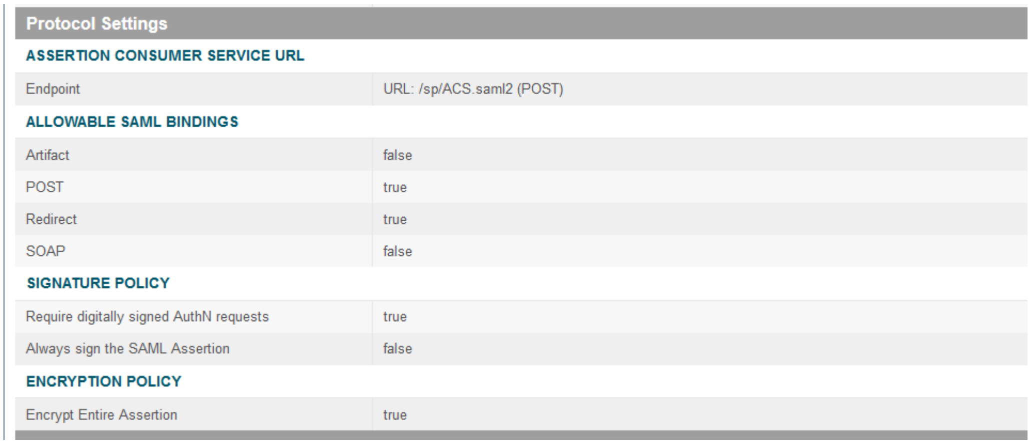
6.6.1 Temporarily Disable SAML Encryption for Testing and Troubleshooting Message Exchanges

Follow the instructions below to temporarily disable the encryption of SAML messages between the Identity Provider and the Relying Party. You should only perform the steps in this section when explicitly instructed to do so in another section of the guide (e.g. during a functional test). You may also need to refer back to this section in the future to test or troubleshoot SAML message exchanges in your environment.

Temporarily disabling the encryption can help test that the expected attributes are being exchanged between the Identity Provider and the Relying Party. By temporarily disabling the encryption, you will be able to see the attributes and their associated values in the SAML messages using the Firefox SAML tracer Add-on or a comparable software tool. When testing or troubleshooting has completed, you can enable the encryption again.

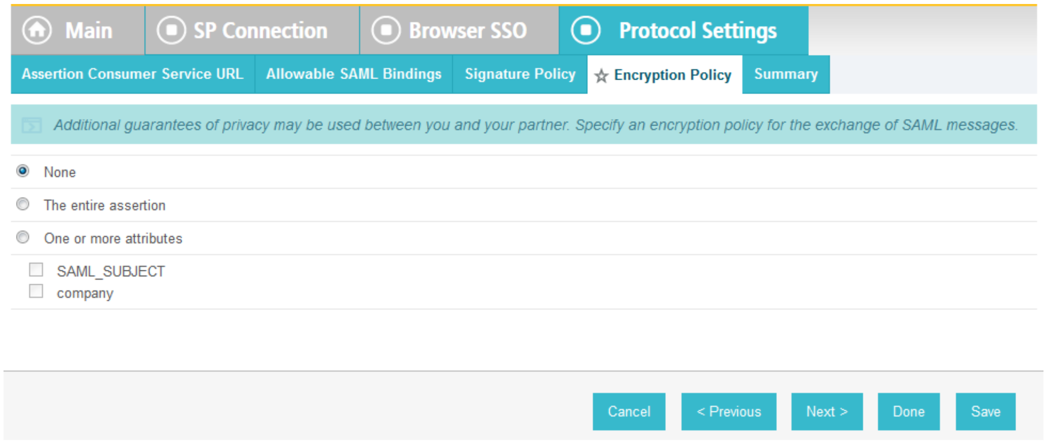
6.6.1.1 Disable SAML Encryption

1. Launch your browser and go to: **http://<DNS_NAME>:9999/pingfederate/app**. Replace **DNS_NAME** with the fully qualified name of the Identity Provider's PingFederate server (e.g. **https://idp.abac.test:9999/pingfederate/app**). Log on to the PingFederate application using the credentials you configured during installation.
2. On the **Main** menu under **SP CONNECTION**, click **Manage All SP**.
3. Click on the link for the SP connection that you want to disable the encryption for (e.g. **https://rp.abac.test:9031**).
4. Scroll down to the **Protocol Settings** group.



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

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



Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.

● None

○ The entire assertion

○ One or more attributes

□ SAML_SUBJECT
□ company

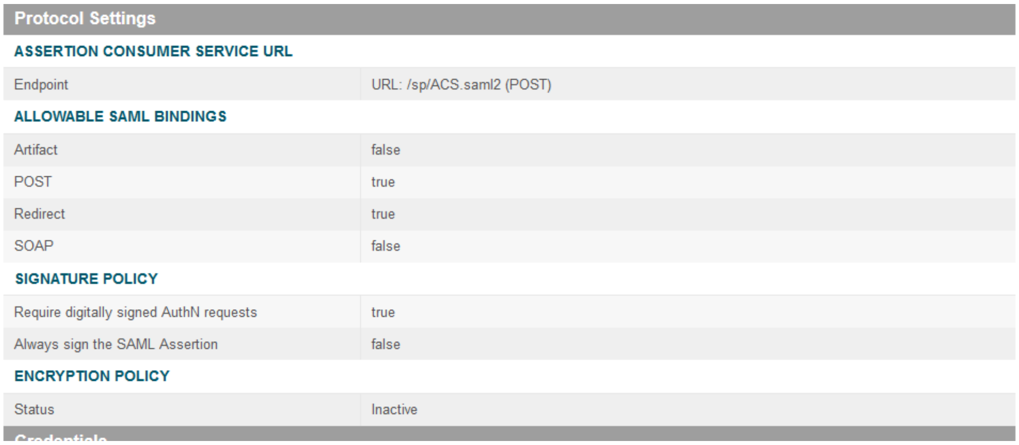
7. Click **Save**.

At this point you have disabled SAML encryption at the Identity Provider for this specific connection to the Relying Party. You can perform authentication testing using the Firefox SAML tracer to examine the SAML messages being sent by the Identity Provider to the Relying Party.

6.6.1.2 Enable SAML Encryption Again

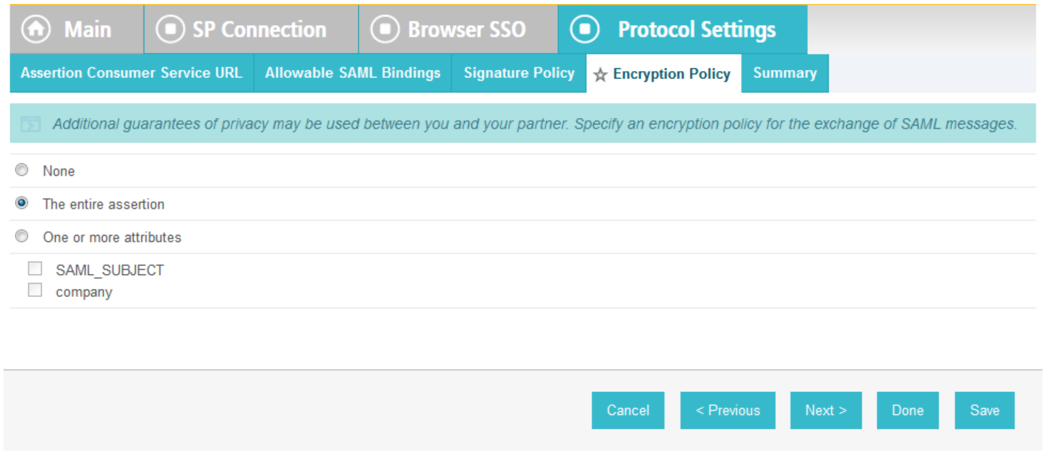
Once testing has completed, perform the following instructions to enable the encryption once again.

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



Protocol Settings	
ASSERTION CONSUMER SERVICE URL	
Endpoint	URL: /sp/ACS.saml2 (POST)
ALLOWABLE SAML BINDINGS	
Artifact	false
POST	true
Redirect	true
SOAP	false
SIGNATURE POLICY	
Require digitally signed AuthN requests	true
Always sign the SAML Assertion	false
ENCRYPTION POLICY	
Status	Inactive
Credentials	

4. Click on the **ENCRYPTION POLICY** link.
5. On the Encryption Policy screen, select **The entire assertion**.



Additional guarantees of privacy may be used between you and your partner. Specify an encryption policy for the exchange of SAML messages.

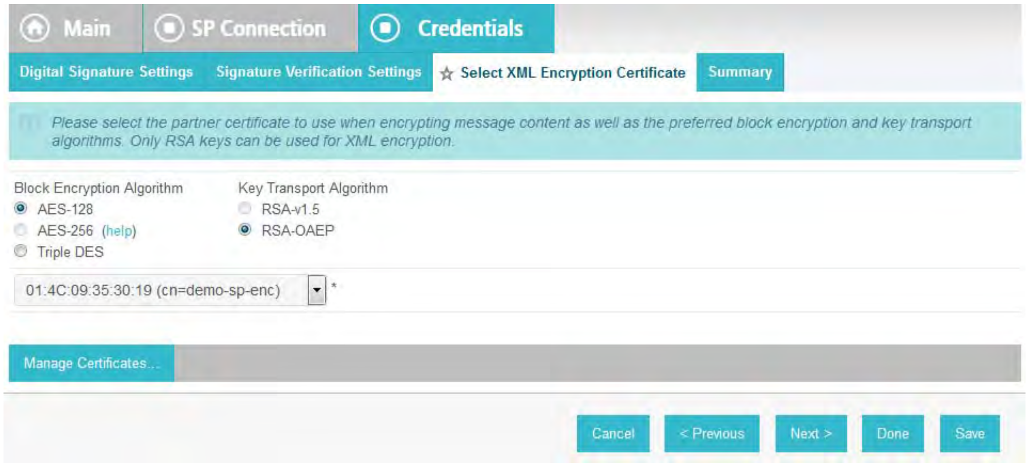
○ None

● The entire assertion

○ One or more attributes

□ SAML_SUBJECT
□ company

6. Click **Save**.
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 Relying Party’s public key certificate to be used to encrypt the message content.



Main
SP Connection
Credentials
Digital Signature Settings
Signature Verification Settings
Select XML Encryption Certificate
Summary
Manage Certificates...
Cancel
< Previous
Next >
Done
Save

Please select the partner certificate to use when encrypting message content as well as the preferred block encryption and key transport algorithms. Only RSA keys can be used for XML encryption.

Block Encryption Algorithm
- ● AES-128
- ○ AES-256 (help)
- ○ Triple DES

Key Transport Algorithm
- ○ RSA-v1.5
- ● RSA-OAEP

01:4C:09:35:30:19 (cn=demo-sp-enc) *

8. Click **Save**.

   You have now enabled the encryption for the connection again.

7 Setting up NextLabs to Protect SharePoint

7.1 Introduction

In this build we are using an ABAC architecture to protect resources on a Microsoft SharePoint instance. In this section we will install the NextLabs Control Center, Policy Studio, Policy Controller, and Entitlement Manager for SharePoint Server. Before getting started installing these components, you must prepare your environment. At a minimum, Windows Server 2012 must be set up with a configured Active Directory, and SharePoint must be installed and configured with a Site Collection. If you haven't already completed the basic installation and configuration of Windows Server 2012 and Active Directory, please refer to chapter 2, Setting up the Identity Provider. If you have not already completed the installation and configuration of SharePoint, please refer to chapter 3, Setting up Federated Authentication Between the Relying Party and the Identity Provider.

The four NextLabs components installed in this chapter provide an Information Control Platform (ICP), Policy Administration Point (PAP), Policy Decision Point (PDP), and Policy Enforcement Point (PEP) in the ABAC Architecture. Each component will be described generally in section 7.2, Components. Then there will be separate sections illustrating installation and configuration of each component. Finally, section 7.7, Functional Tests, will give some guidance for verifying the correct installation and configuration of the various components presented in this chapter.

7.2 Components

- **NextLabs Control Center (release 7.5)**: enterprise-level Information Control Platform (ICP) for policy-driven data loss prevention and entitlement management; can contain many software components, including the following two in this build:
  - **Policy Studio: Enterprise Edition (PAP)**: application for policy lifecycle management, provides a graphical user interface (GUI) for defining and deploying attribute-based access control policies. This product is installed on an instance of SQL Server.
  - **Policy Controller (PDP)**: distributed component of the Control Center that evaluates policies created in the PAP to determine a deny or allow decision when users attempt to access protected resources. This product is installed on an instance of Microsoft SharePoint Server.
- **NextLabs Entitlement Manager for Microsoft SharePoint Server (PEP)**: enforces the decisions from the PDP to deny or allow access to SharePoint resources. This product is installed on an instance of Microsoft SharePoint Server.

7.2.1 NextLabs Control Center (release 7.5)

The NextLabs Control Center is an enterprise-level Information Control Platform (ICP). It integrates into existing IT infrastructure, and applications and can be used to digitally manage policies to govern data classification, access, sharing, and automate security compliance procedures. In order to fulfill its diverse capabilities, the Control Center can be configured to incorporate and coordinate many NextLabs software components. It is also possible to develop your own custom access control enforcers for applications that do not already have an available enforcer built by NextLabs. In this build, we take advantage of the Policy Studio, Policy

Controller, and Entitlement Manager for Microsoft SharePoint Server, which are discussed in the following sub-sections.

In order to support administrative and configuration activities necessary for its many components, NextLabs Control Center provides a web application user interface called Administrator. Some of the system monitoring and administrative tasks available via Administrator include: checking how many policies are deployed in the network, finding out on which hosts the Control Center components are installed, checking the status of Control Center server components, finding out how many enforcers are currently running, finding out if any enforcers are disconnected, and finding out or modifying the current heartbeat setting for an enforcer, among others.

Another key component of the Control Center is the Policy Server. The Policy Server runs continuously from the moment of startup as a Windows service. As new policy is defined or policies are updated, the Policy Server pushes these policy sets to the Policy Controller on the SharePoint Server.

The Control Center platform is installed and configured on the same server as the build's SQL database, which we refer to as the SQL Server.

7.2.2 NextLabs Policy Studio: Enterprise Edition

The NextLabs Policy Studio component of the Control Center is intended for administrators and policy designers responsible for converting the general data access and usage management goals of the enterprise into deployable, active policies. Depending on a company's business rules, policies can be defined to evaluate user (subject) attributes, resource (object) attributes, and environmental (contextual) attributes.

The Policy Studio provides a graphical user interface with which you can create an abstract model representing the various parts of the enterprise environment (users, applications, computers, and environmental context), construct policies with these modeled components, and fine-tune policies using advanced conditions that can change based on dynamic comparisons, evaluations, and contextual factors. For example, policy designers can select pre-defined conditions including the time of day, day of the week, connection type, and IP address, among many others. In addition to defining which attributes to evaluate when making an enforcement decision, the policy construction process can also determine notification obligations such that when a policy is allowed or denied, a user can be notified with a default or custom message, a statement can be added to the application's log file, and an email can be sent to an administrator.

Like the Control Center platform, the Policy Studio is installed and configured on the SQL Server.

7.2.3 NextLabs Policy Controller

Each NextLabs Policy Controller provides the interface to the Policy Server component of the Control Center (installed on the SQL Server), and serves as a distributed Policy Decision Point (PDP). It comprises a set of software modules delivered with Control Center, read-to-install on the enforcer host or development machine. Because it is not specific to any adapter type, it requires no customization. In this build, the Policy Controller is installed and configured on the same server as the SharePoint instance, which we refer to as the SharePoint Sever.

In general, the logical architecture of a NextLabs enforcer that protects an application (such as the Entitlement Manager for SharePoint Server, covered in the next sub-section) consists of two parts, the Policy Controller and the Policy Adapter.

The Policy Controller consists of the following functional components:

- The **Policy Evaluation Engine** evaluates whether or not each user action is covered by any of the policies currently cached at that enforcement point. It bases its evaluation on multiple criteria such as who the user is, what host he is using, how he is connected to the network, which action is being attempted, on what resource, the date, the time, and so on. It does this in real time, and operates continuously whether the host is connected to the network or not Note that while disconnected from the network the local encrypted bundle.bin policy cache would not be able to be updated from policy changes made in the PAP.
    - Note: Policies are authored in the PAP GUI on the SQL Server, and any modifications to the policy set are transmitted by the Policy Server, also installed on the SQL Server, to the Policy Controller on the SharePoint Server. It takes a heartbeat length of time for the updates to take effect on the SharePoint Server. By default, the heartbeat rate of the desktop enforcer is set to 60 minutes, which is appropriate for a live production environment. For testing and learning purposes, however, you should change this to 1 minute, which will allow you to define, deploy and test policies with shorter delays. A heartbeat can be configured via the Control Center Administrator web application.
- The **Context Manager** keeps constant track of the environmental context of all events, and provides it to the Policy Engine and Policy Adapter. The context includes user identity, computer host name, network connection type, and date and time.
- For any policy that evaluates as True, the **Obligation Manager** initiates an obligation by sending a request to a policy adapter's obligation services or executing a built-in obligations. It contains three sub-components:
    - **Policy Logger** - collects and logs all activity details and policy decision results
    - **Messaging Services** - sends message to recipients or targets listed in a policy
    - **Application Extender** - launches an application or custom executable that performs some custom obligation
- The **Controller Manager** records non-policy activities, updates the configuration, and secures the controller. Components include:
    - **Activity Recorder** - records activities tracked by the policy adapter in real time.
    - **Configuration Manager** - applies profile and system configuration changes in real time
    - **Policy Authentication** - authenticates the policy set from the Policy Server and encrypts it on the local file system
        - Note: It is the responsibility of the Controller Manager to encrypt the bundle.bin file on the local file system for use during policy evaluation by the PDP.
    - **Tamper Resistance Module** - protects all Entitlement Manager processes, installed files, and registry settings from tampering by users or other processes, and governs the automatic start-up and restart features. The Policy Controller runs as a Windows service continuously from the moment of startup, called Control Center Enforcer Service.

- The **ICENet Client** provides the interface for all communication with the Policy Server. It is used for deploying new or changed policies, periodically sending activity logs from each control point, and providing controller health status.

7.2.4 NextLabs Entitlement Manager for Microsoft SharePoint Server

The NextLabs Entitlement Manager for SharePoint is designed to enforce the policies that control whether and how users can access, download, and use data stored on a SharePoint server. SharePoint policies can apply to entire portals or to any parts thereof, and allow some users to view all webparts on a page while blocking other users from viewing some subset of the webparts on the same page.

7.2.5 Required or Recommended Files, Hardware, and Software

Component	Required Files	Recommended or Minimum Hardware Requirements	Hardware Used in this Build	Recommended or Minimum Operating System or Other Software	Operating System or Other Software Used in this Build
Control Center (CC)	license.dat; ControlCenter-64-7.5.0.0-64-201410211146.zip	1GB RAM; 1GHz CPU; 4GB free disk space		Windows Server 2008, Enterprise Edition, R2, 64-bit, or Windows Server 2012; Java bundled and installed within NextLabs CC; Microsoft SQL Server 2012; Microsoft SQL Server Management Studio	Windows Server 2012; Java bundled and installed within NextLabs software architecture; Microsoft SQL Server 2012; Microsoft SQL Server Management Studio
External Database	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

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
Policy Studio	PolicyStudio-setup64-7.5.0.0-10-201410291227.zip	i3 or above, 1.5 GHz, dual-core CPU; 2GB; 10 GB free disk space		Windows XP, Service Pack 3, 32-bit, Windows 7, 32-bit and 64-bit, or Windows Server 2008, Enterprise Edition, R2, 64-bit; Microsoft SQL Server 2012; Microsoft SQL Server Management Studio	Windows Server 2012; Microsoft SQL Server 2012; Microsoft SQL Server Management Studio

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
Policy Controller	PolicyController-CE-64-7.0.1.0-1-201405191624.zip	2GB RAM; i3 or above, 1.5 GHz, dual-core CPU; 10 GB free disk space		Windows XP, Service Pack 3, 32-bit Windows 2003, 32-bit, Windows 7, 32-bit and 64-bit, Windows Server 2008, Enterprise Edition, R2, 64-bit, or Red Hat Linux Release 1, Updates 1-3	Windows Server 2012
Entitlement Manager for SharePoint Server	SharePoint Enforcer-2013-64-7.1.3.0-7-201410101427.zip			■ Microsoft Office SharePoint Server 2007 on Windows Server 2003, Enterprise Edition, 32-bit, Service Pack 2, or Windows Server 2008, Enterprise Edition, 64-bit, R2 ■ Microsoft Office SharePoint Server 2010 on Windows Server 2008, Enterprise Edition, 64-bit, R2 ■ Microsoft SharePoint Server 2013 on Windows Server 2008, Enterprise Edition, 64-bit, R2	Microsoft SharePoint Server 2013 on Windows Server 2012

7.3 Installation and Configuration of NextLabs Control Center (on the SQL Server)

7.3.1 Installation and Configuration

7.3.1.1 Install the Microsoft SQL Server via Microsoft SQLServer 2012

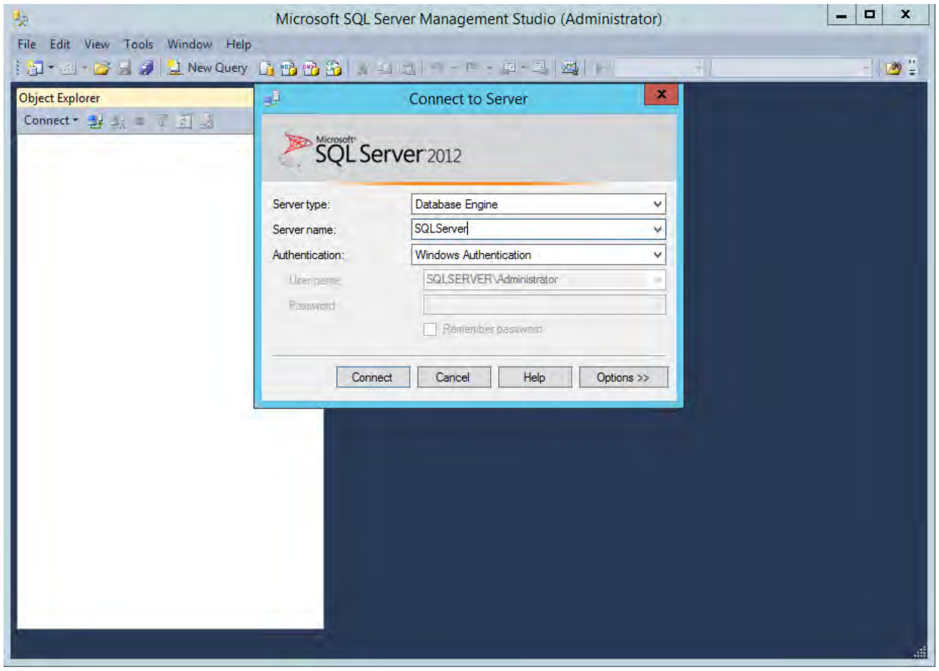
Instructions available at the Microsoft SQLServer site: https://technet.microsoft.com/en-us/library/hh231622(v=sql.110).aspx.

Notes

1. Regarding installation of Microsoft SQLServer 2012: if you already completed the installation as described in section 4.2.3this step will already have been completed.
2. Regarding having a database dedicated to NextLabs: NextLabs recommends that for anything but a demo or testing environment, you should use a database running on its own dedicated server to store all system data, rather than rely on Control Center's internal database. A dedicated database server is strongly recommended because policy enforcement data accumulates quickly and can reach a significant volume. The problem is not necessarily storage space, but the performance drag on other processes caused by database queries of large amounts of data.

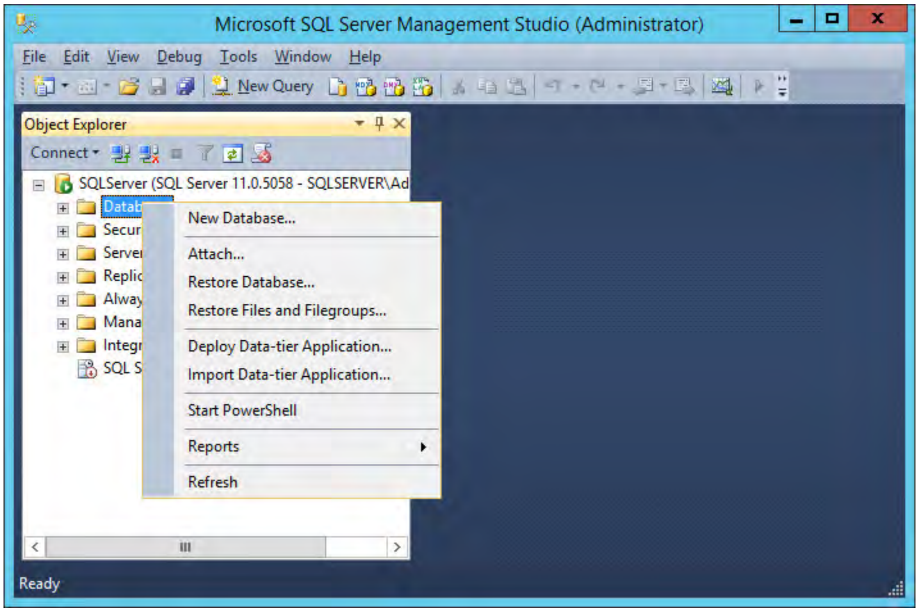
7.3.1.2 Create a New Database and Database User for the NextLabs Control Center Installation and Administration

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

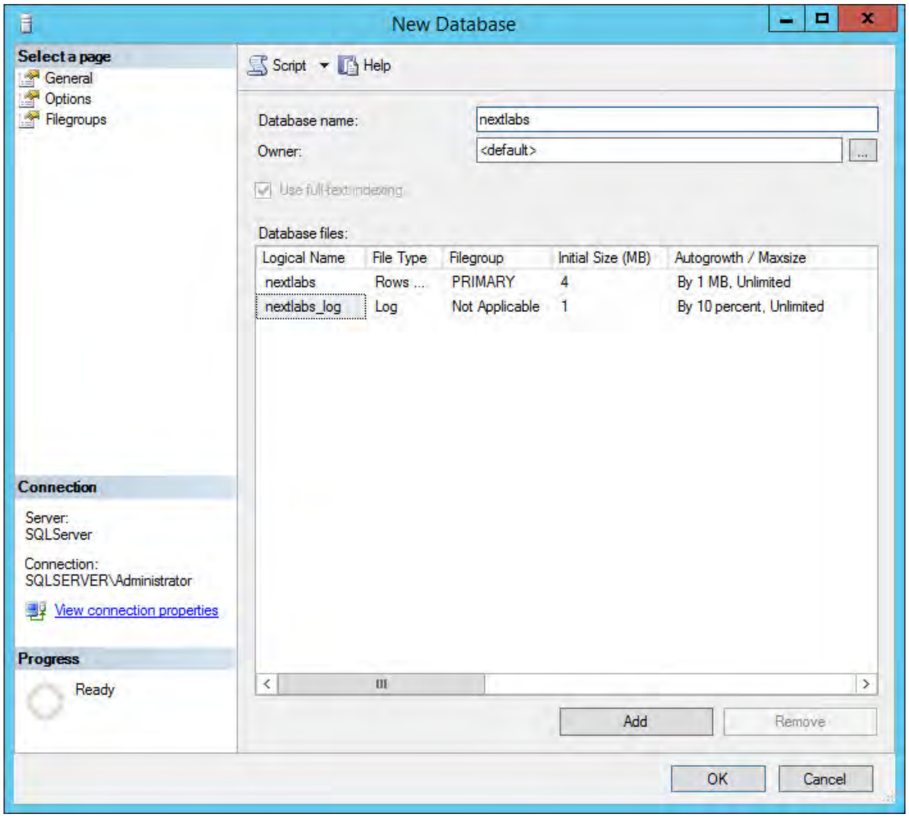


Server type: Database Engine
Server name: SQLServer
Authentication: Windows Authentication
User name: SQLSERVER\Administrator
Password:
□ Remember password

2. Right-click on **Databases**, left-click on **New Database**.


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
SQLServer (SQL Server 11.0.5058 - SQLSERVER\Ad
Datab
Secur
Serve
Replic
Alway
Mana
Integr
SQL S
New Database...
Attach...
Restore Database...
Restore Files and Filegroups...
Deploy Data-tier Application...
Import Data-tier Application...
Start PowerShell
Reports
Refresh
Ready

3. In the New Database window, specify a **Database name** that works for you. The application automatically copies this into the **Logical Names** of the **Database files**. Click **OK**. Example name from this build: **nextlabs**



Database name: nextlabs

Owner: <default>

☑ Use full-text indexing

Database files:

Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Maxsize
nextlabs	Rows ...	PRIMARY	4	By 1 MB, Unlimited
nextlabs_log	Log	Not Applicable	1	By 10 percent, Unlimited

Connection

Server:
SQLServer

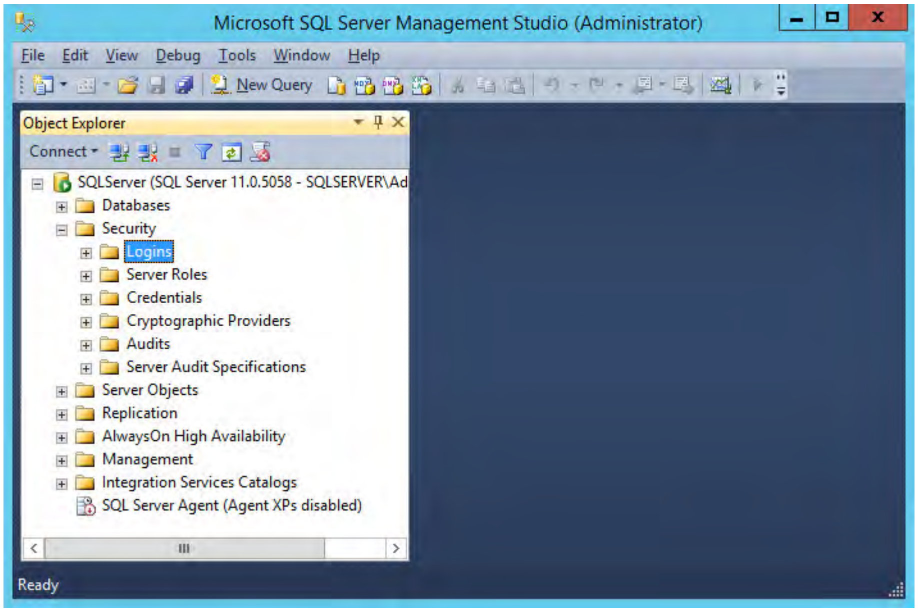
Connection:
SQLSERVER\Administrator

View connection properties

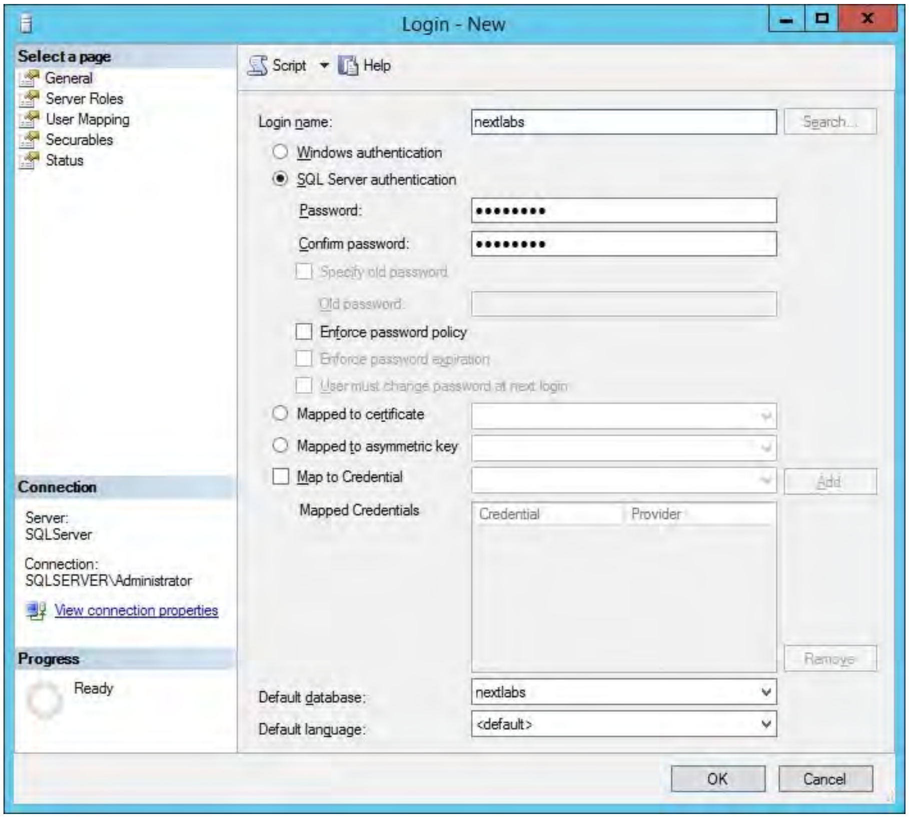
Progress

Ready

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.


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect
SQLServer (SQL Server 11.0.5058 - SQLSERVER\Ad
Databases
Security
Logins
Server Roles
Credentials
Cryptographic Providers
Audits
Server Audit Specifications
Server Objects
Replication
AlwaysOn High Availability
Management
Integration Services Catalogs
SQL Server Agent (Agent XPs disabled)
Ready

5. Right-click **Logins**. Left-click **New Login**.
6. Click on **SQL Server authentication**, and enter a new **Login name** and **Password**.



Login name: nextlabs

○ Windows authentication

● SQL Server authentication

Password: ••••••••

Confirm password: ••••••••

□ Specify old password

Old password:

□ Enforce password policy

□ Enforce password expiration

□ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential

Mapped Credentials

Credential	Provider

Default database: nextlabs

Default language: <default>

Connection

Server:
SQLServer

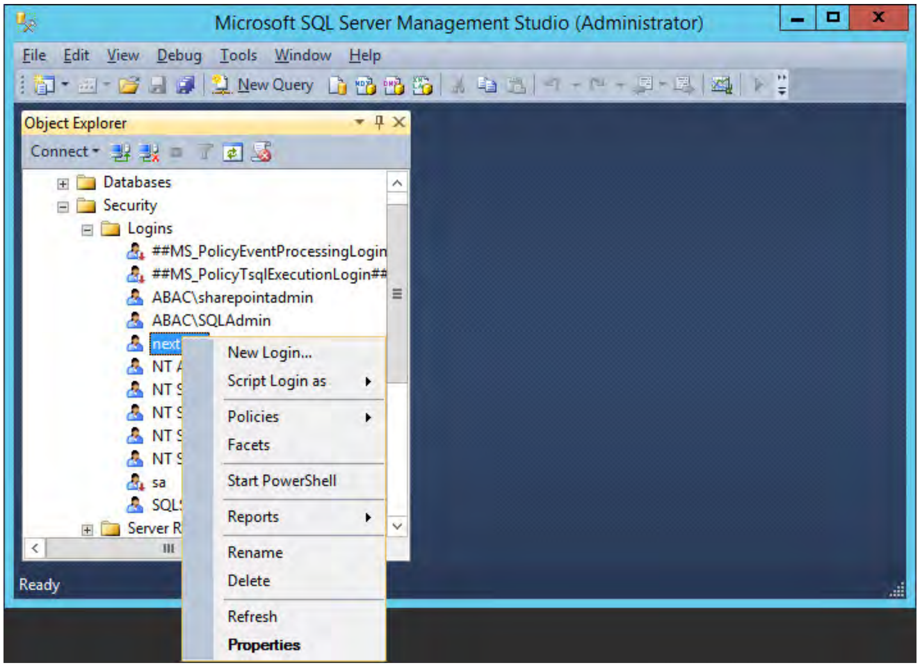
Connection:
SQLSERVER\Administrator

View connection properties

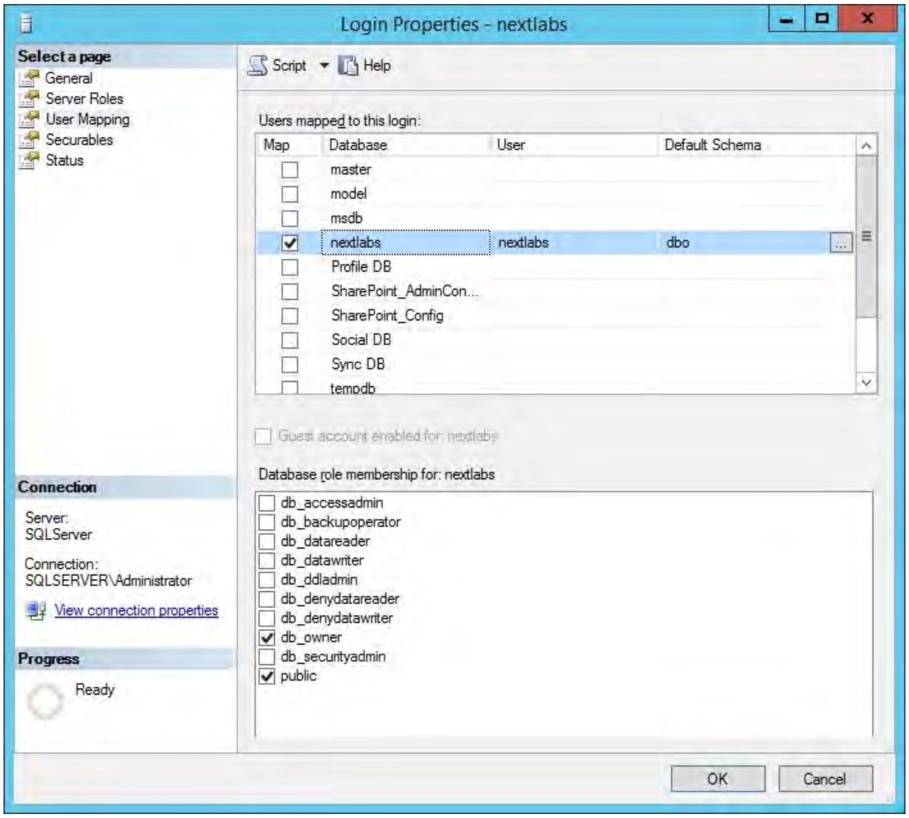
Progress

Ready

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



8. Click on **User Mapping**, then **New Database**. Under **Database role membership for: [database_name]**, check the box next to **db_owner**.



Server:
SQLServer

Connection:
SQLSERVER\Administrator

Users mapped to this login:

Map	Database	User	Default Schema
□	master		
□	model		
□	msdb		
☑	nextlabs	nextlabs	dbo
□	Profile DB		
□	SharePoint_AdminCon...		
□	SharePoint_Config		
□	Social DB		
□	Sync DB		
□	tempdb		

□ Guest account enabled for: nextlabs

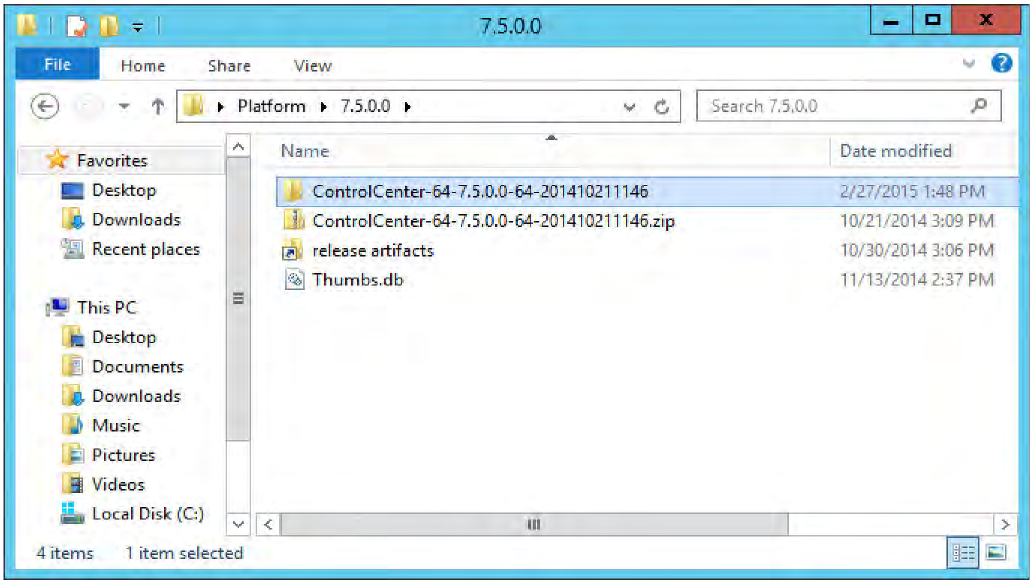
Database role membership for: nextlabs

□ db_accessadmin
□ db_backupoperator
□ db_datareader
□ db_datawriter
□ db_ddladmin
□ db_denydatareader
□ db_denydatawriter
☑ db_owner
□ db_securityadmin
☑ public

7.3.1.3 Install and Configure the NextLabs Control Center

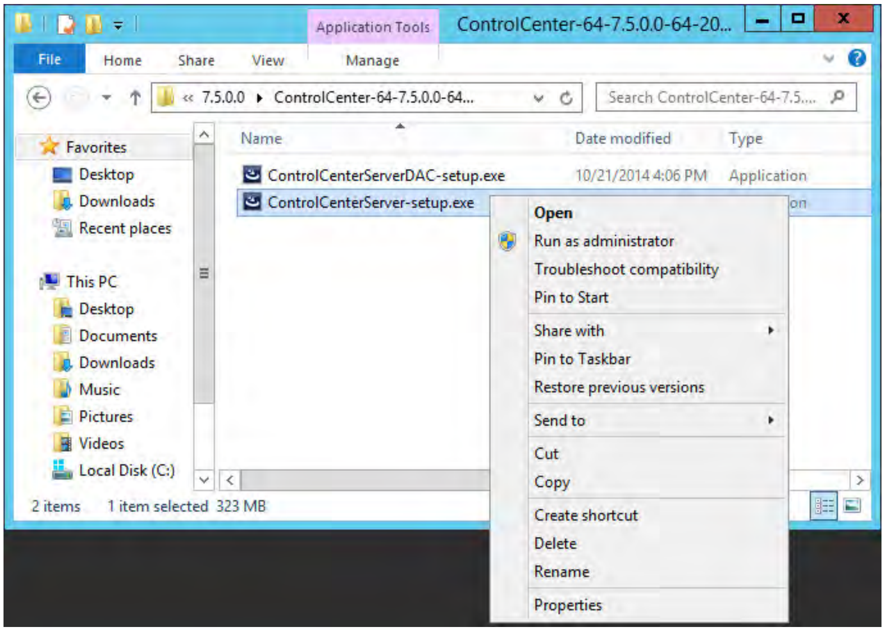
Complete standard Control Center installation per NextLabs documentation available to customers, using the following steps:

1. Go to your Desktop or other known location where the required NextLabs Control Center installation files are stored. Example: **C:\Users\Administrator\Desktop\NextLabs\Platform\7.5.0.0\**
   a. Note the location of the required license.dat file which will be needed later; example: **C:\Users\Administrator\Desktop\NextLabs\Platform\License\license.dat**
2. Right-click on **ControlCenter-64-7.5.0.0-64-201410211146.zip** and select **Extract All** from the floating menu. Wait for the files to be extracted.
3. Double-click to open the **ControlCenter-64-7.5.0.0-64-201410211146** folder.

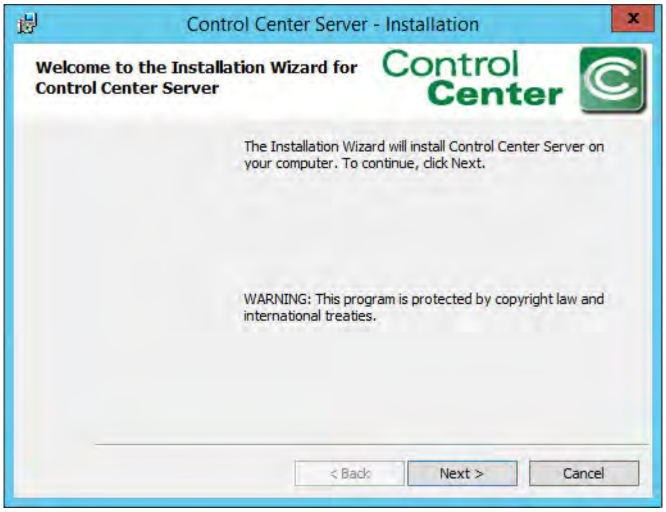


Name	Date modified
ControlCenter-64-7.5.0.0-64-201410211146	2/27/2015 1:48 PM
ControlCenter-64-7.5.0.0-64-201410211146.zip	10/21/2014 3:09 PM
release artifacts	10/30/2014 3:06 PM
Thumbs.db	11/13/2014 2:37 PM

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



5. Click **Next**.

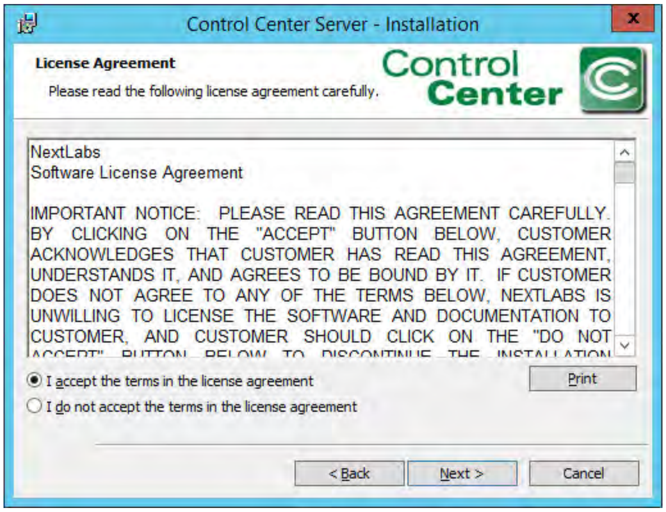


Welcome to the Installation Wizard for Control Center Server

The Installation Wizard will install Control Center Server on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



License Agreement

Please read the following license agreement carefully.

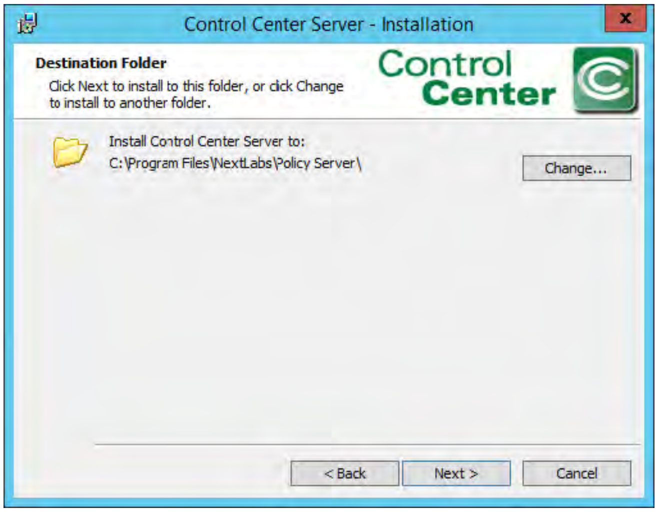
NextLabs
Software License Agreement

IMPORTANT NOTICE: PLEASE READ THIS AGREEMENT CAREFULLY. BY CLICKING ON THE "ACCEPT" BUTTON BELOW, CUSTOMER ACKNOWLEDGES THAT CUSTOMER HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY IT. IF CUSTOMER DOES NOT AGREE TO ANY OF THE TERMS BELOW, NEXTLABS IS UNWILLING TO LICENSE THE SOFTWARE AND DOCUMENTATION TO CUSTOMER, AND CUSTOMER SHOULD CLICK ON THE "DO NOT ACCEPT" BUTTON BELOW TO DISCONTINUE THE INSTALLATION

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

7. Click **Next**.

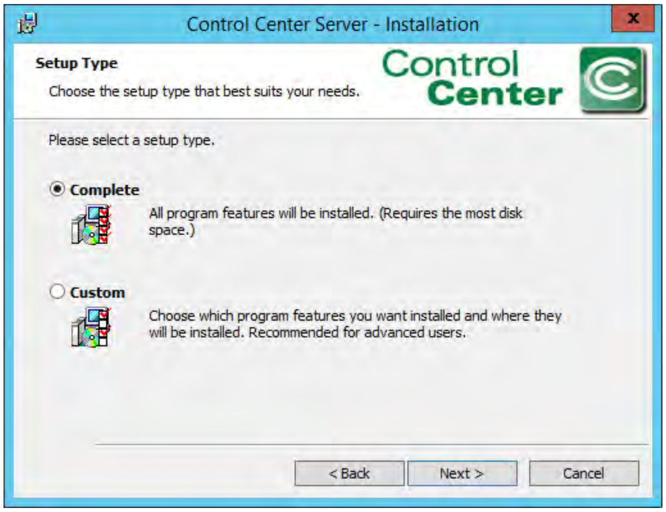


Destination Folder

Click Next to install to this folder, or click Change to install to another folder.

Install Control Center Server to:
C:\Program Files\NextLabs\Policy Server\

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



Control Center Server - Installation

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Complete**

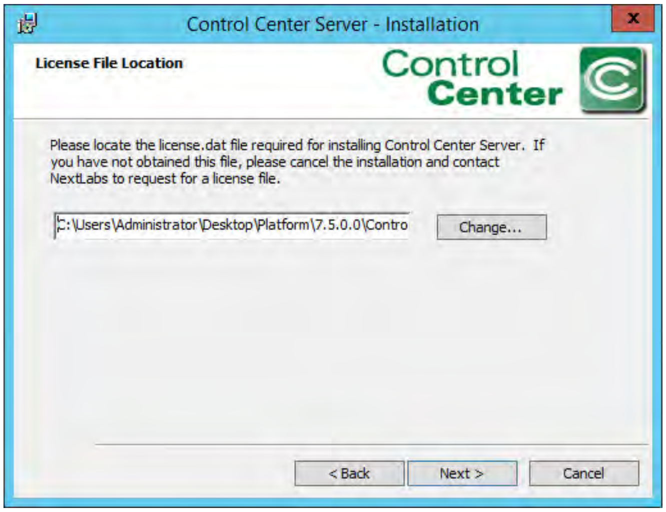
All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

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**.

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



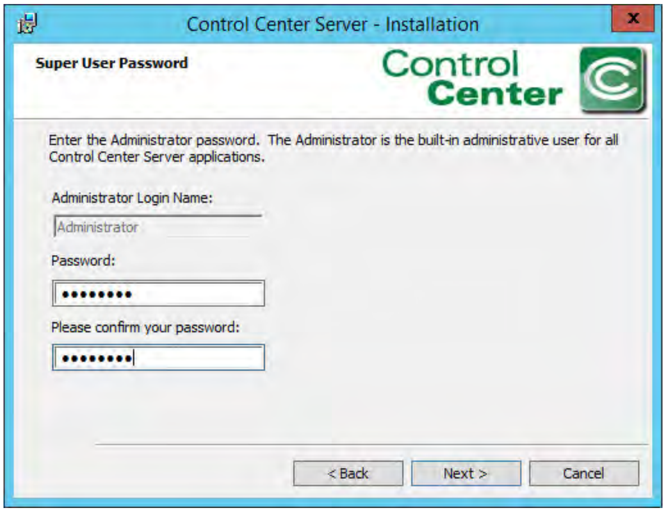
Control Center Server - Installation

License File Location

Please locate the license.dat file required for installing Control Center Server. If you have not obtained this file, please cancel the installation and contact NextLabs to request for a license file.

C:\Users\Administrator\Desktop\Platform\7.5.0.0\Contro

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**.



Control Center Server - Installation

Super User Password

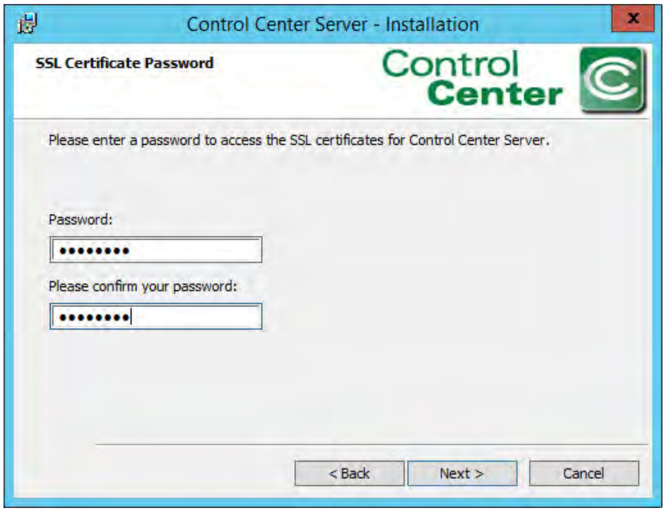
Enter the Administrator password. The Administrator is the built-in administrative user for all Control Center Server applications.

Administrator Login Name: Administrator

Password: ••••••••

Please confirm your password: ••••••••

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



Control Center Server - Installation

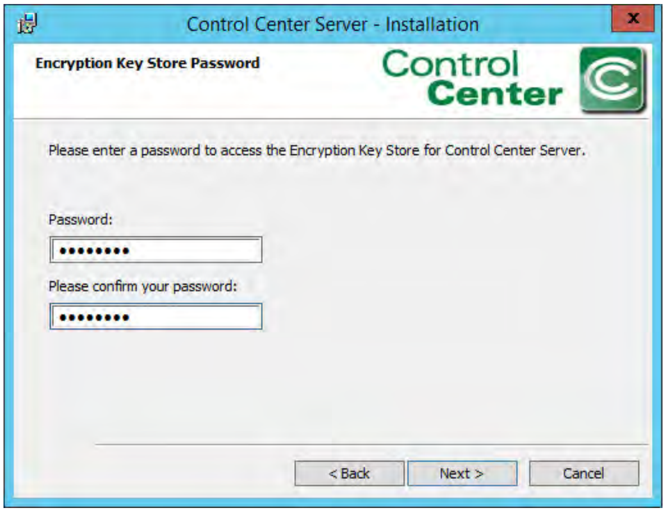
SSL Certificate Password

Please enter a password to access the SSL certificates for Control Center Server.

Password: ••••••••

Please confirm your password: ••••••••

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


Control Center Server - Installation

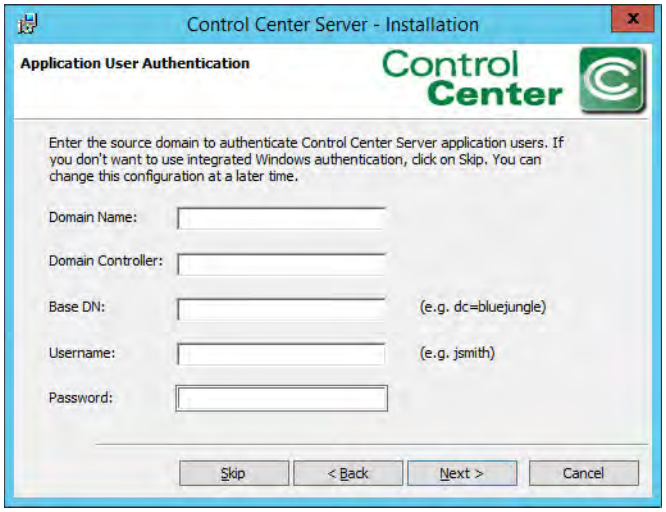
Encryption Key Store Password

Please enter a password to access the Encryption Key Store for Control Center Server.

Password: ••••••••

Please confirm your password: ••••••••

13. At the Application User Authentication screen, click **Skip**.


Control Center Server - Installation

Application User Authentication

Enter the source domain to authenticate Control Center Server application users. If you don't want to use integrated Windows authentication, click on Skip. You can change this configuration at a later time.

Domain Name:

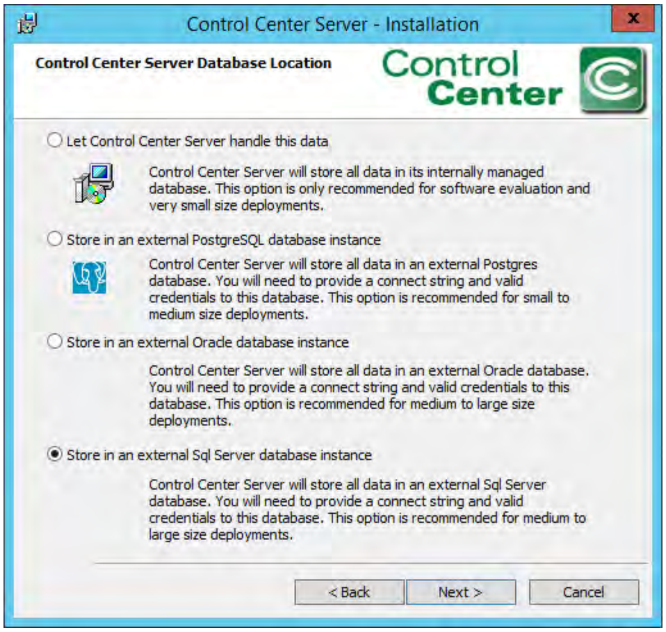
Domain Controller:

Base DN: (e.g. dc=bluejungle)

Username: (e.g. jsmith)

Password:

14. At the Control Center Server Database Location screen, select **Store in an external Sql Server database instance**. Click **Next**.



Control Center Server - Installation

Control Center Server Database Location

○ Let Control Center Server handle this data

Control Center Server will store all data in its internally managed database. This option is only recommended for software evaluation and very small size deployments.

○ Store in an external PostgreSQL database instance

Control Center Server will store all data in an external Postgres database. You will need to provide a connect string and valid credentials to this database. This option is recommended for small to medium size deployments.

○ Store in an external Oracle database instance

Control Center Server will store all data in an external Oracle database. You will need to provide a connect string and valid credentials to this database. This option is recommended for medium to large size deployments.

● Store in an external Sql Server database instance

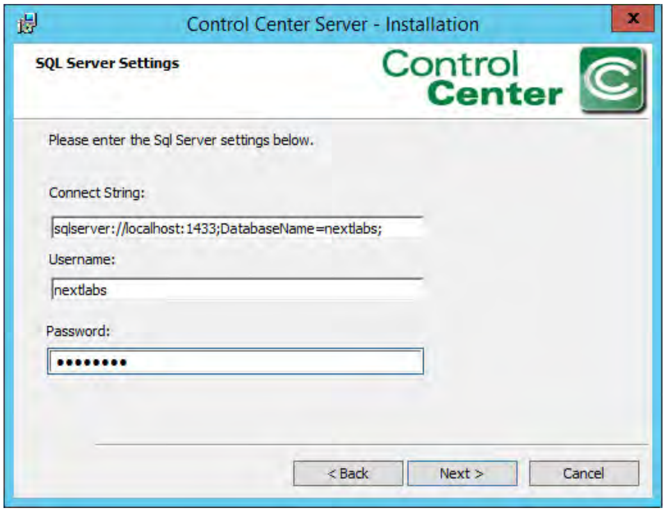
Control Center Server will store all data in an external Sql Server database. You will need to provide a connect string and valid credentials to this database. This option is recommended for medium to large size deployments.

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

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

   b. Specify **Username** (non-Super User) and **Password**.

   c. Click **Next**. Note: If the error C**onnection to the SQL database could not be established properly** appears, it may help to restart the SQL Server.



Control Center Server - Installation

SQL Server Settings

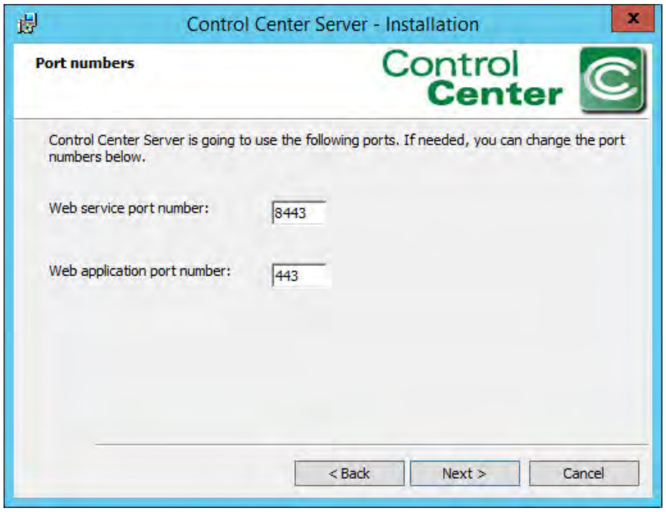
Please enter the Sql Server settings below.

Connect String: sqlserver://localhost:1433;DatabaseName=nextlabs;

Username: nextlabs

Password: ••••••••

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



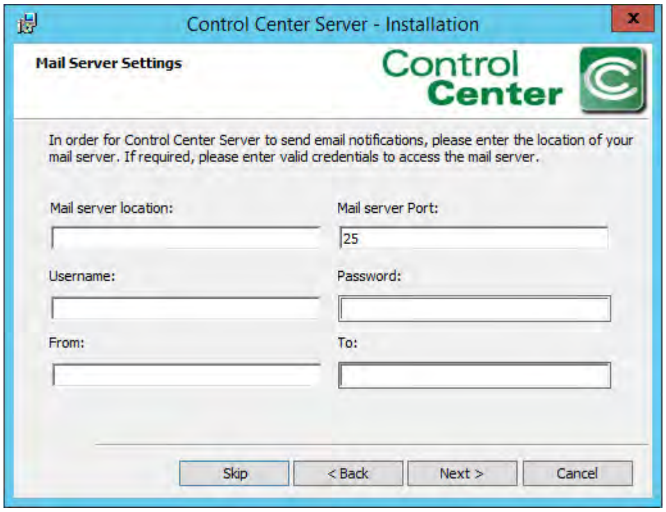
Port numbers

Control Center Server is going to use the following ports. If needed, you can change the port numbers below.

Web service port number: 8443

Web application port number: 443

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



Mail Server Settings

In order for Control Center Server to send email notifications, please enter the location of your mail server. If required, please enter valid credentials to access the mail server.

Mail server location:

Mail server Port: 25

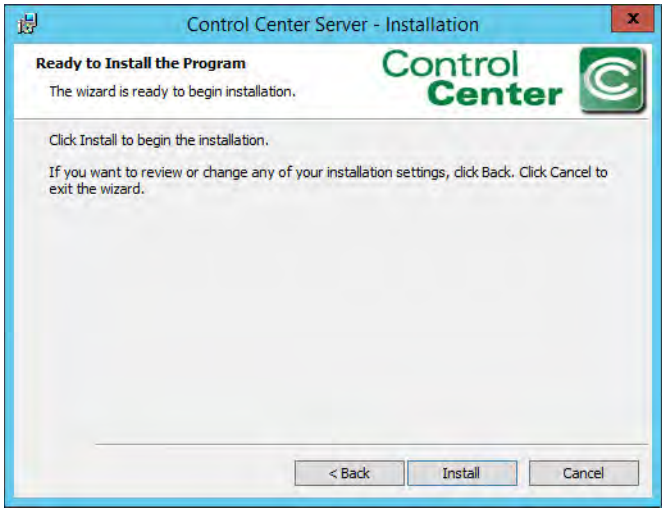
Username:

Password:

From:

To:

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


Control Center Server - Installation

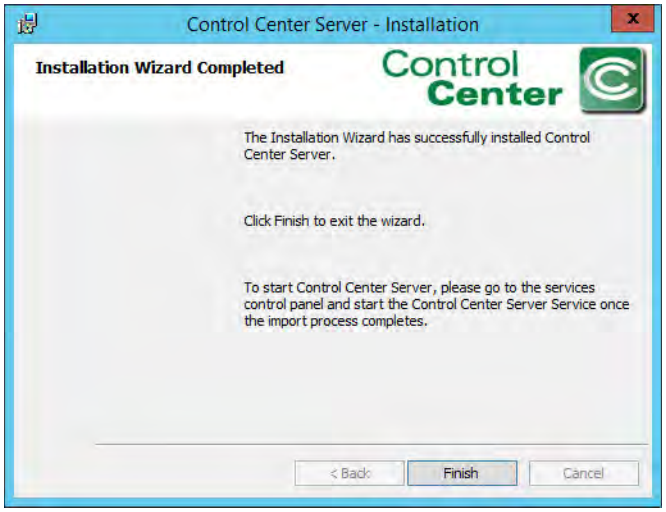
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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


Control Center Server - Installation

Installation Wizard Completed

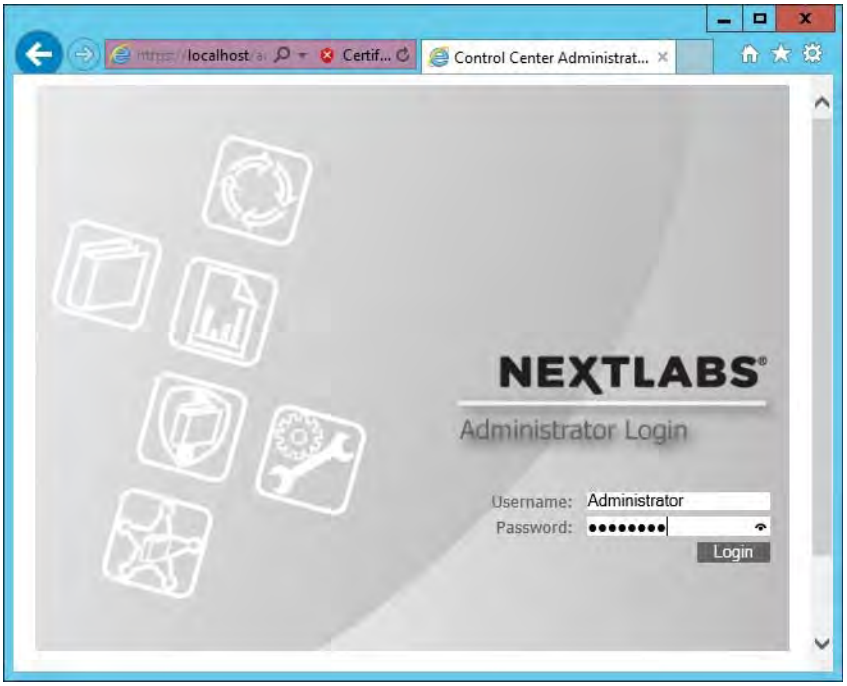
The Installation Wizard has successfully installed Control Center Server.

Click Finish to exit the wizard.

To start Control Center Server, please go to the services control panel and start the Control Center Server Service once the import process completes.

20. Open an Internet browser and navigate to the following URL: **https://localhost/administrator** to login to the Control Center Administrator web application.
    a. If a security certificate warning comes up, click **Continue to this website**.
    b. Enter the Administrator (Super User) **Username** and **Password**.

c. Click **Login**.



Username: Administrator
Password: ●●●●●●●●●

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:

    a. Fully qualified domain name (FQDN) of the server hosting the NextLabs Control Center. Example: **SQLServer.ABAC.TEST**

    b. Services running on the host server, including but not limited to:

        i. Intelligence Server

        ii. Dynamic Access Control

        iii. Key Management Server

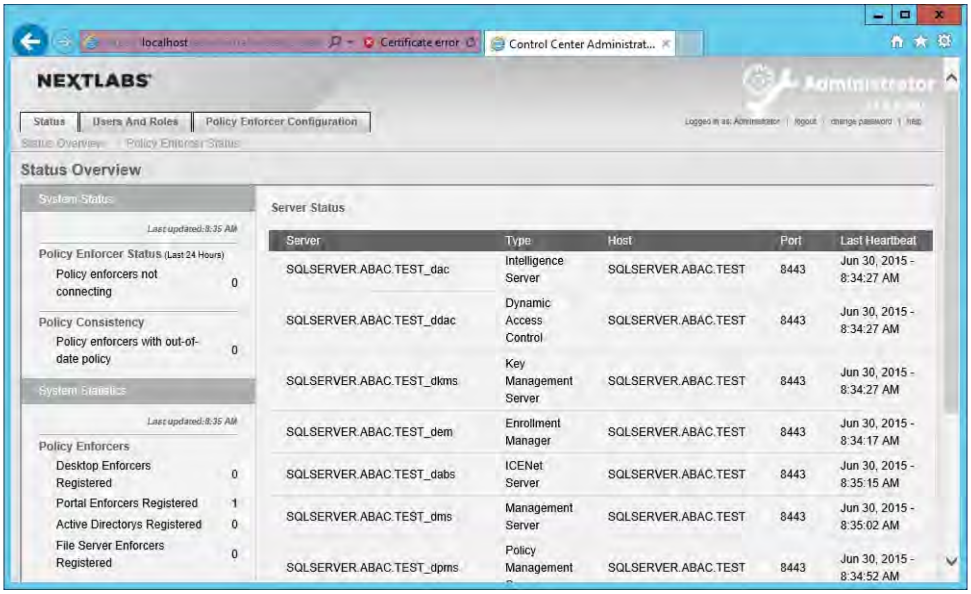
        iv. Management Server

        v. Policy Management Server

        For more information about these or other services running continuously via NextLabs Control Center on the SQL Server, please refer to NextLabs support documentation.

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

d. For each of the listed services, the default heartbeat period is 60 minutes, and can be modified via the Administrator (See step 22).


localhost
Certificate error
Control Center Administrat...
NEXTLABS
Administrator
Status
Users And Roles
Policy Enforcer Configuration
Logged in as: Administrator | logout | change password | help
Status Overview
Policy Enforcer Status

Status Overview

System Status

Last updated: 8:35 AM

Policy Enforcer Status (Last 24 Hours)

Policy enforcers not connecting	0

Policy Consistency

Policy enforcers with out-of-date policy	0

System Statistics

Last updated: 8:35 AM

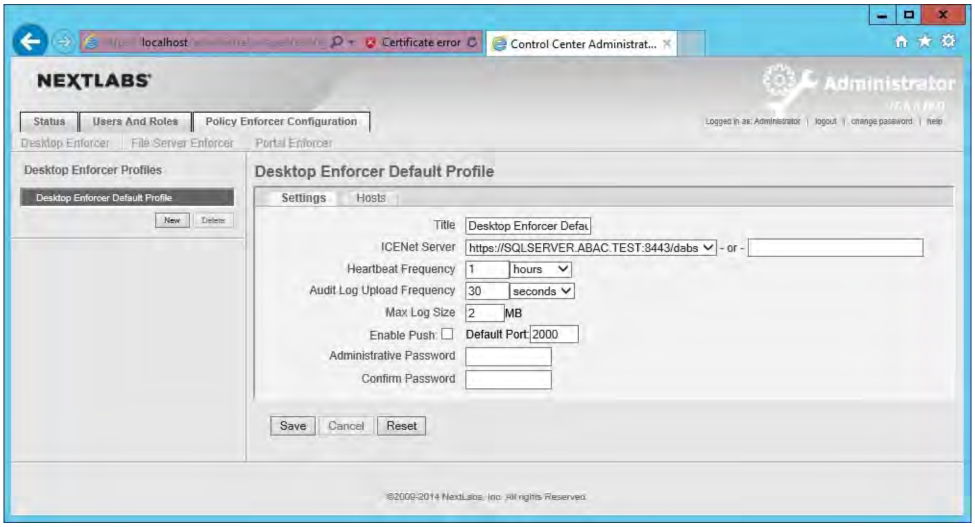
Policy Enforcers

Desktop Enforcers Registered	0
Portal Enforcers Registered	1
Active Directorys Registered	0
File Server Enforcers Registered	0

Server Status

Server	Type	Host	Port	Last Heartbeat
SQLSERVER.ABAC.TEST_dac	Intelligence Server	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:27 AM
SQLSERVER.ABAC.TEST_ddac	Dynamic Access Control	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:27 AM
SQLSERVER.ABAC.TEST_dkms	Key Management Server	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:27 AM
SQLSERVER.ABAC.TEST_dem	Enrollment Manager	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:17 AM
SQLSERVER.ABAC.TEST_dabs	ICENet Server	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:35:15 AM
SQLSERVER.ABAC.TEST_dms	Management Server	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:35:02 AM
SQLSERVER.ABAC.TEST_dpms	Policy Management	SQLSERVER.ABAC.TEST	8443	Jun 30, 2015 - 8:34:52 AM

22. Click on the **Policy Enforcer Configuration** tab. The default Profile to open is the **Desktop Enforcer Portal**, with the **Settings** sub-tab defaulted also open. To change the heartbeat frequency for testing or debugging purposes, edit the **Heartbeat Frequency** field (minimum time is 1 minute). Click **Save**.


localhost
Certificate error
Control Center Administrat...
NEXTLABS
Administrator
Status
Users And Roles
Policy Enforcer Configuration
Logged in as: Administrator | logout | change password | help
Desktop Enforcer
File Server Enforcer
Portal Enforcer
Desktop Enforcer Profiles
Desktop Enforcer Default Profile
New
Delete
Settings
Hosts
Save
Cancel
Reset
©2009-2014 NextLabs, Inc. All rights Reserved.

Desktop Enforcer Default Profile

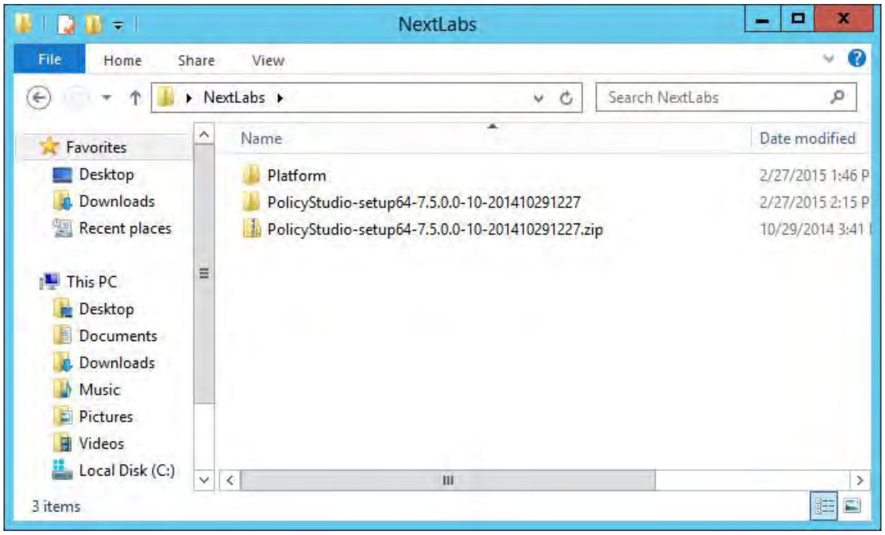
Title	Desktop Enforcer Defau
ICENet Server	https://SQLSERVER.ABAC.TEST:8443/dabs - or -
Heartbeat Frequency	1 hours
Audit Log Upload Frequency	30 seconds
Max Log Size	2 MB
Enable Push:	☐ Default Port: 2000
Administrative Password	
Confirm Password	

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

7.4.1 Installation

Complete the standard Policy Studio installation per NextLabs documentation available to customers using the following steps:

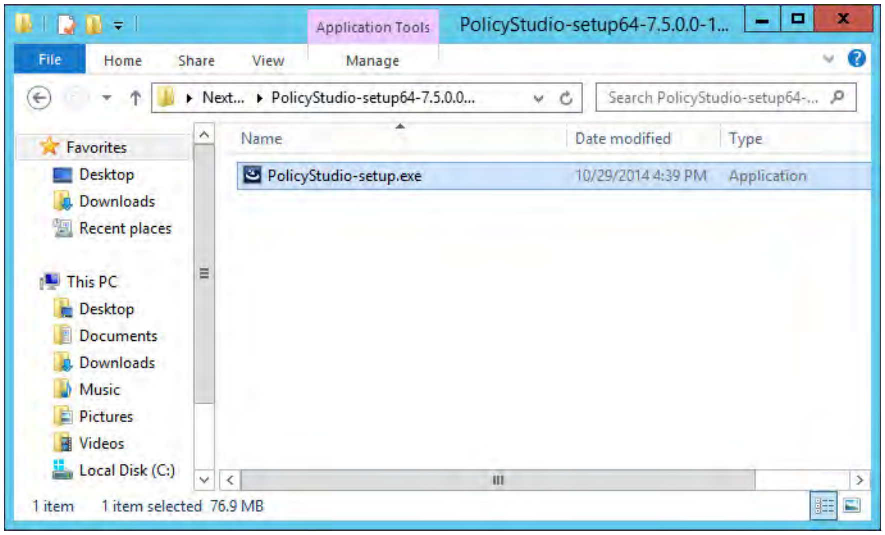
1. On the SQLServer, go to your Desktop or other known location where the required NextLabs Policy Studio installation files are stored. Example: **C:\Users\Administrator\Desktop\NextLabs\**
2. Right-click on **PolicyStudio-setup64-7.5.0.0-10-201410291227.zip** and select **Extract All**. Wait for files to be extracted.



Platform 2/27/2015 1:46 P
PolicyStudio-setup64-7.5.0.0-10-201410291227 2/27/2015 2:15 P
PolicyStudio-setup64-7.5.0.0-10-201410291227.zip 10/29/2014 3:41

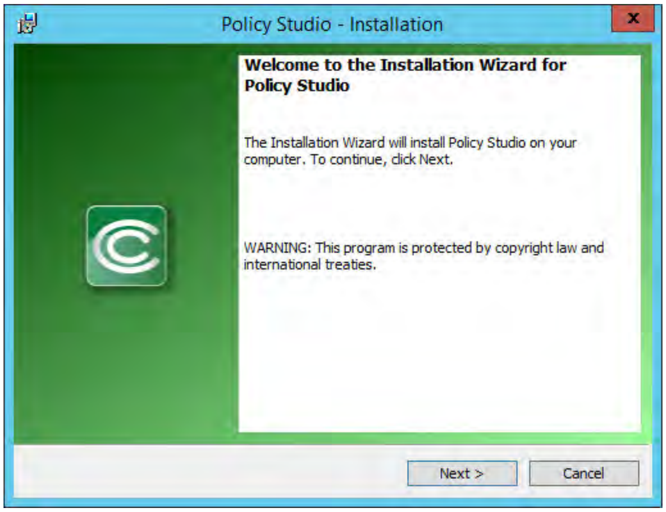
3. Double-click to open the **PolicyStudio-setup64-7.5.0.0-10-201410291227** folder.

4. Right-click on **PolicyStudio-setup.exe** and select **Run as Administrator**.



Name	Date modified	Type
PolicyStudio-setup.exe	10/29/2014 4:39 PM	Application

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

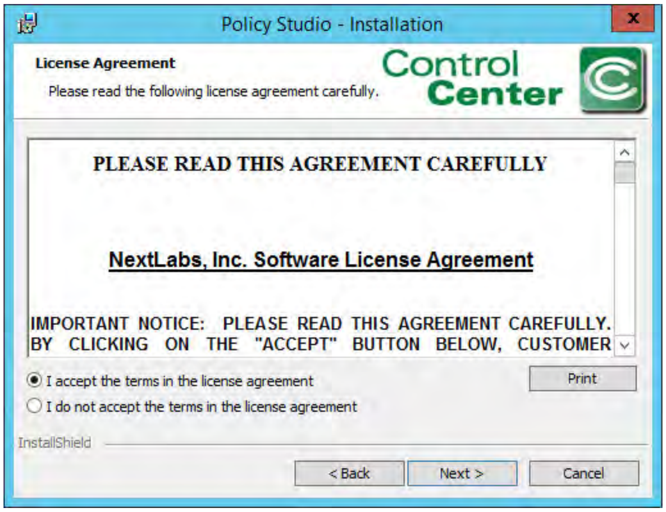


Welcome to the Installation Wizard for Policy Studio

The Installation Wizard will install Policy Studio on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



Policy Studio - Installation

License Agreement

Please read the following license agreement carefully.

PLEASE READ THIS AGREEMENT CAREFULLY

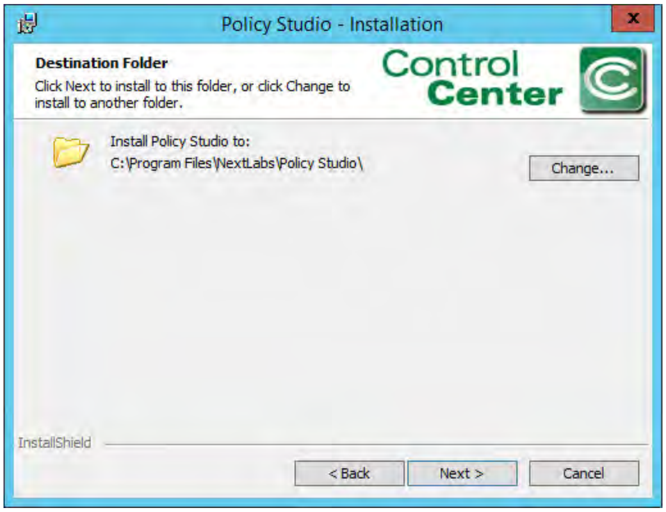
NextLabs, Inc. Software License Agreement

IMPORTANT NOTICE: PLEASE READ THIS AGREEMENT CAREFULLY. BY CLICKING ON THE "ACCEPT" BUTTON BELOW, CUSTOMER

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

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



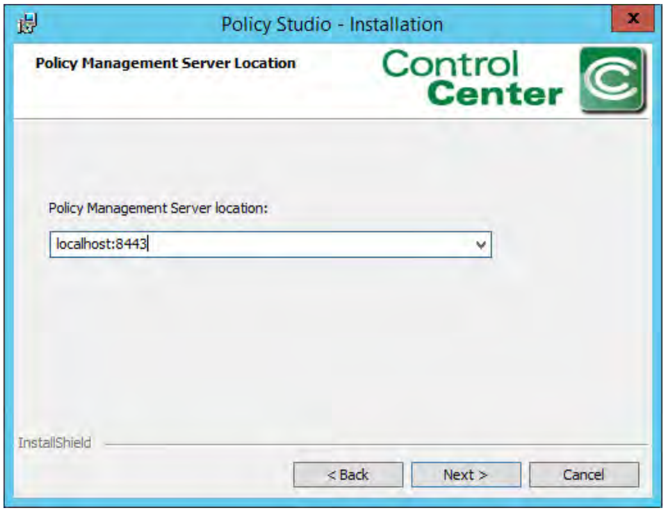
Policy Studio - Installation

Destination Folder

Click Next to install to this folder, or click Change to install to another folder.

Install Policy Studio to:
C:\Program Files\NextLabs\Policy Studio\

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

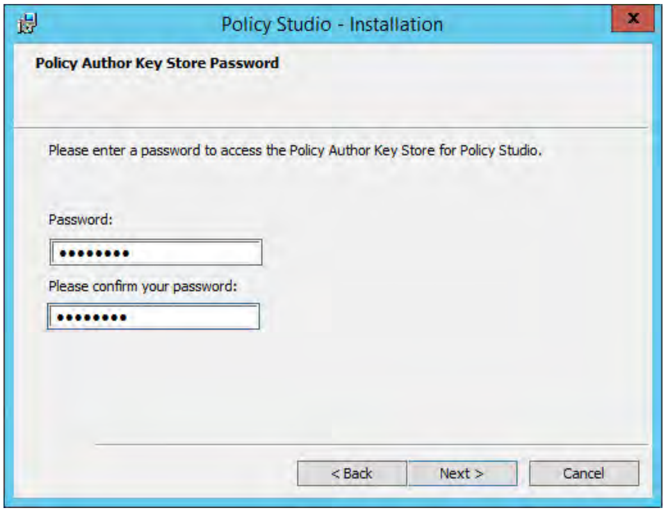


Policy Management Server Location

Policy Management Server location:

localhost:8443

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



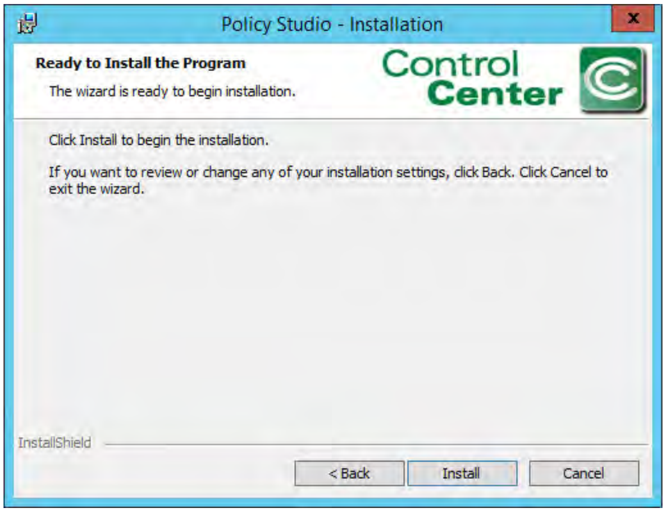
Policy Author Key Store Password

Please enter a password to access the Policy Author Key Store for Policy Studio.

Password: ••••••••

Please confirm your password: ••••••••

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



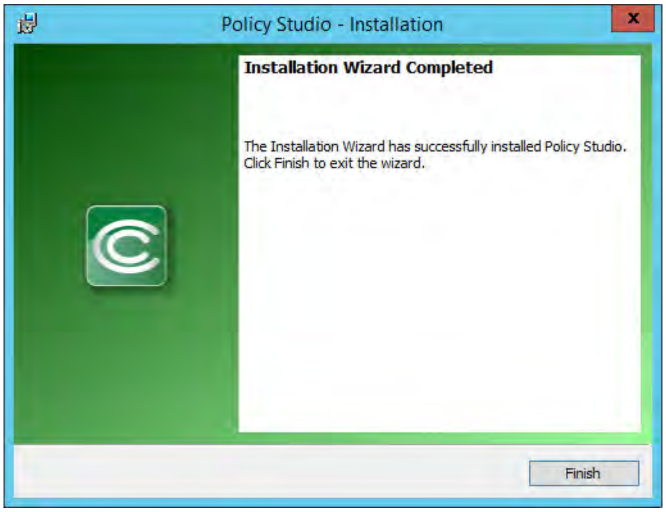
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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

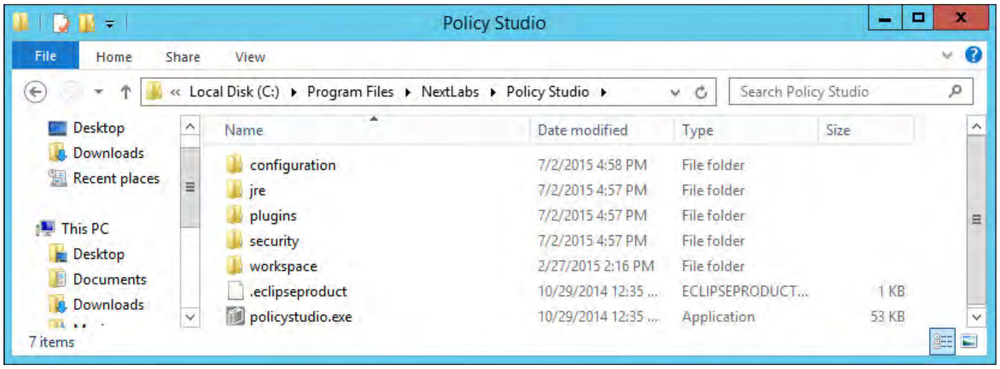


Installation Wizard Completed

The Installation Wizard has successfully installed Policy Studio. Click Finish to exit the wizard.

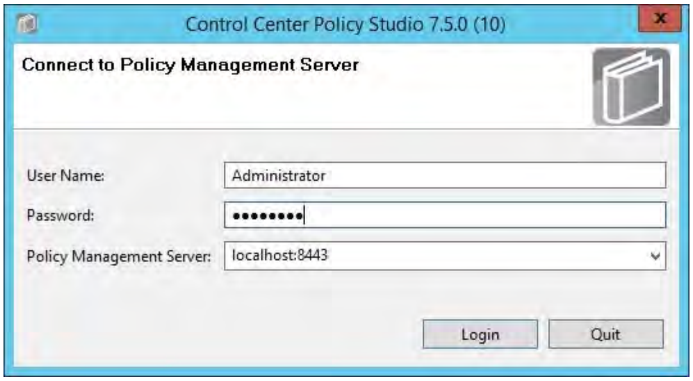
12. In Windows Explorer, find and open the **policystudio.exe** application file.
    a. Double-click the **C:/ drive**.
    b. Double-click **Program Files**.
    c. Double-click **NextLabs**.
    d. Double-click **Policy Studio**.

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



Name	Date modified	Type	Size
configuration	7/2/2015 4:58 PM	File folder	
jre	7/2/2015 4:57 PM	File folder	
plugins	7/2/2015 4:57 PM	File folder	
security	7/2/2015 4:57 PM	File folder	
workspace	2/27/2015 2:16 PM	File folder	
.eclipseproduct	10/29/2014 12:35 ...	ECLIPSEPRODUCT...	1 KB
policystudio.exe	10/29/2014 12:35 ...	Application	53 KB

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


Control Center Policy Studio 7.5.0 (10)
Connect to Policy Management Server
Login
Quit

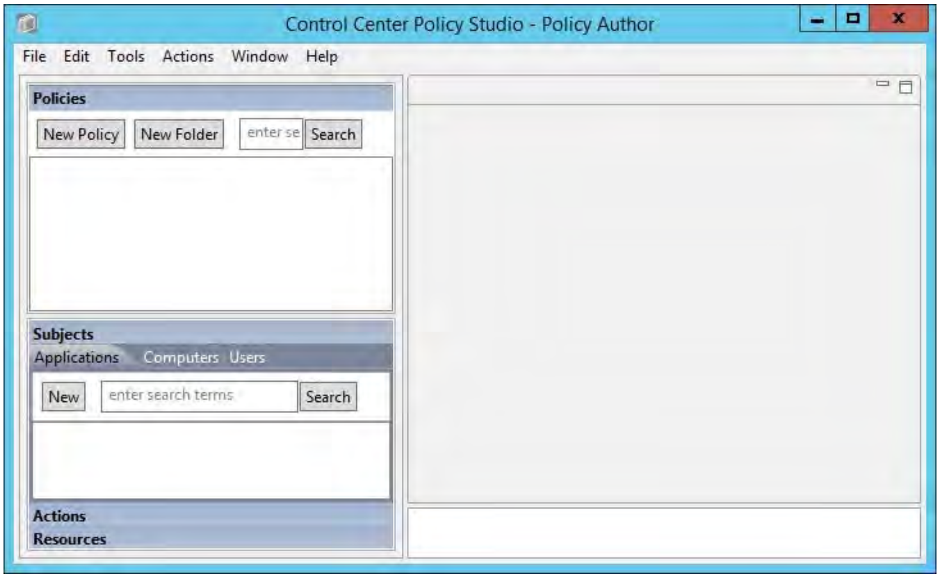
User Name: Administrator

Password: ••••••••

Policy Management Server: localhost:8443

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 chapter 8.

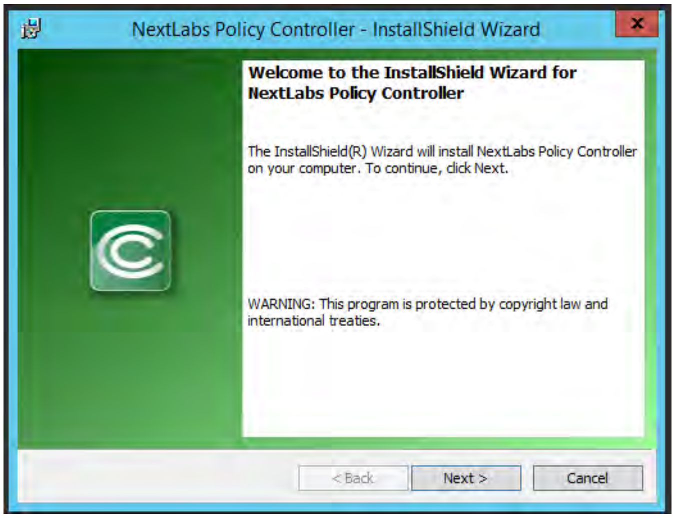


7.5 Installation and Configuration of Policy Controller (PDP)

7.5.1 Installation

To complete standard Policy Controller installation per NextLabs documentation available to customers, use the following steps:

1. On the SharePoint Server, go to your Desktop or other known location where the required NextLabs Policy Controller installation files are stored. Example: **C:\Users\Administrator\Desktop\SharePoint\**
2. Right-click on **PolicyController-CE-64-7.0.1.0-1-201405191624.zip** and select **Extract All** from the floating menu. Wait for files to be extracted.
3. Double-click on **PolicyController-CE-64-7.0.1.0-1-201405191624** folder to open it.
4. Double-click **CE-PolicyController-setup64.msi** to begin installation.
5. At the Welcome to the InstallShield Wizard for NextLabs Policy Controller Installation screen, click **Next**.



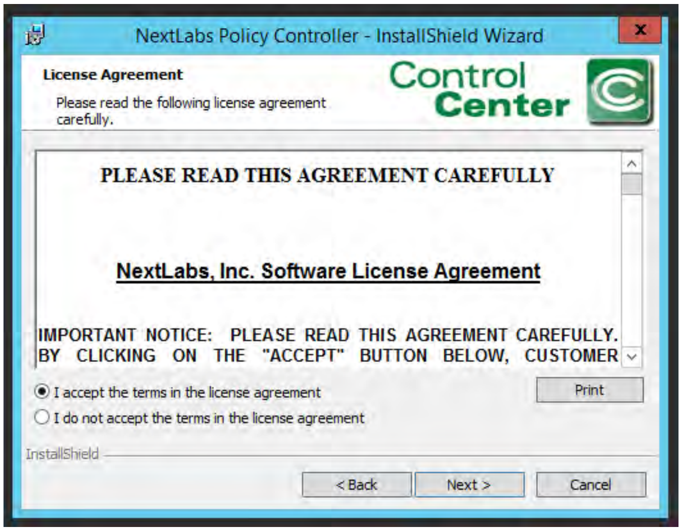
NextLabs Policy Controller - InstallShield Wizard

Welcome to the InstallShield Wizard for NextLabs Policy Controller

The InstallShield(R) Wizard will install NextLabs Policy Controller on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



NextLabs Policy Controller - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

PLEASE READ THIS AGREEMENT CAREFULLY

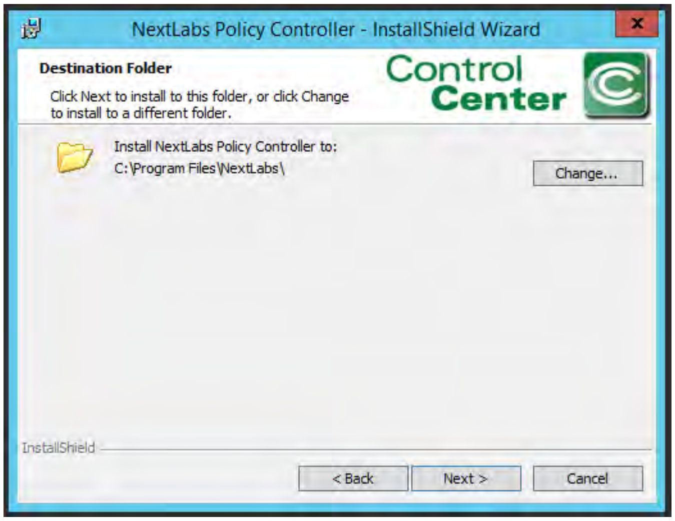
NextLabs, Inc. Software License Agreement

IMPORTANT NOTICE: PLEASE READ THIS AGREEMENT CAREFULLY. BY CLICKING ON THE "ACCEPT" BUTTON BELOW, CUSTOMER

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

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



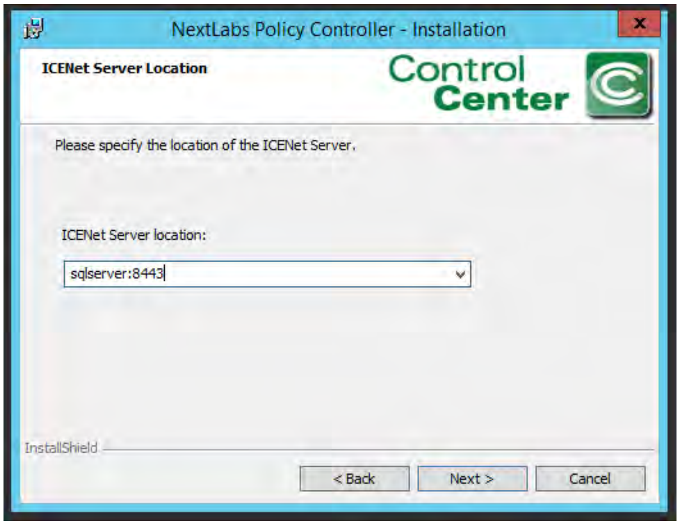
NextLabs Policy Controller - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install NextLabs Policy Controller to:
C:\Program Files\NextLabs\

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



NextLabs Policy Controller - Installation

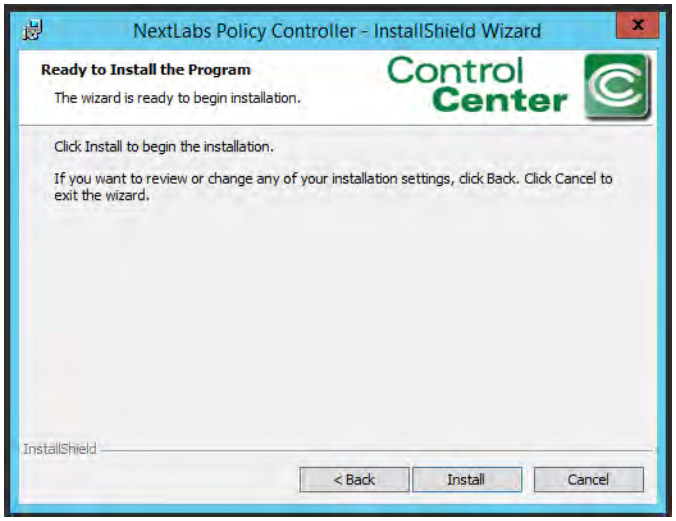
ICENet Server Location

Please specify the location of the ICENet Server.

ICENet Server location:

sqlserver:8443

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



NextLabs Policy Controller - InstallShield Wizard

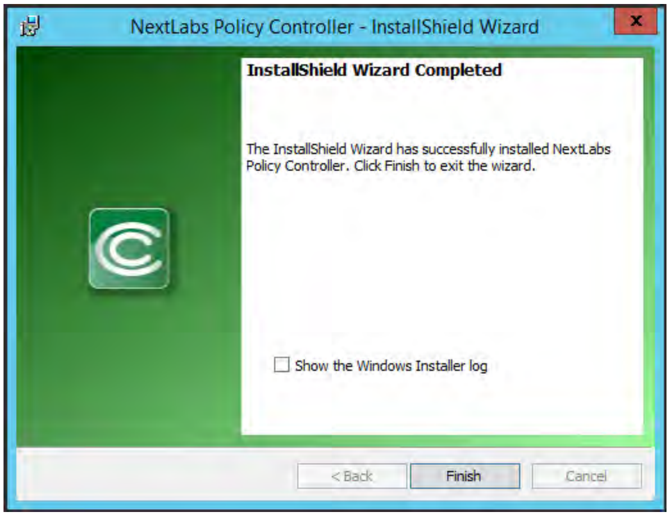
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

10. At the InstallShield Wizard Completed screen, click **Finish**.



NextLabs Policy Controller - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed NextLabs Policy Controller. Click Finish to exit the wizard.

□ Show the Windows Installer log

11. In the window that immediately opens, click **Yes** to restart the computer, or click **No** to wait and restart after installing the PEP (see section 7.6, Installation and Configuration of NextLabs Entitlement Manager for SharePoint Server).

7.6 Installation and Configuration of NextLabs Entitlement Manager for SharePoint Server

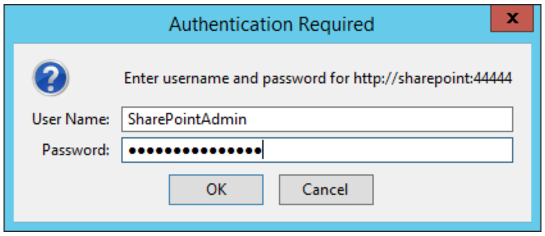
7.6.1 Installation and Configuration

Note: Prior to installing the Entitlement Manager for SharePoint Server, it is necessary to install the NextLabs Policy Controller on the SharePoint Server. If you have not already installed the Policy Controller, please refer to section 7.5 before proceeding.

7.6.1.1 Verify that a Web Application Site and Site Collection Already Exist in SharePoint

1. On the SharePoint Server, open an Internet browser and navigate to the following URL: **http://sharepoint:44444/default.aspx** to login to the SharePoint Central Administration portal.

2. Enter the **User Name** and **Password** for your SharePoint Central Administration account, and click **OK**.



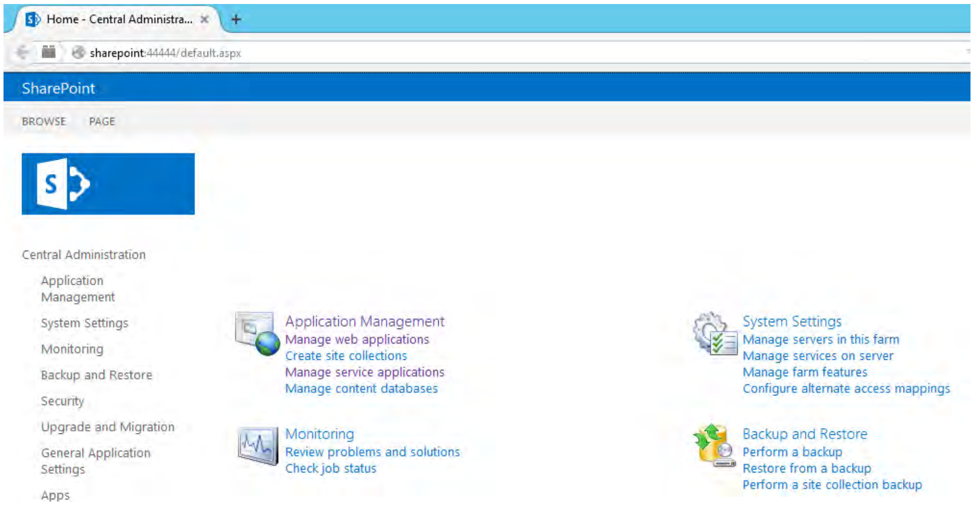
Authentication Required

Enter username and password for http://sharepoint:44444

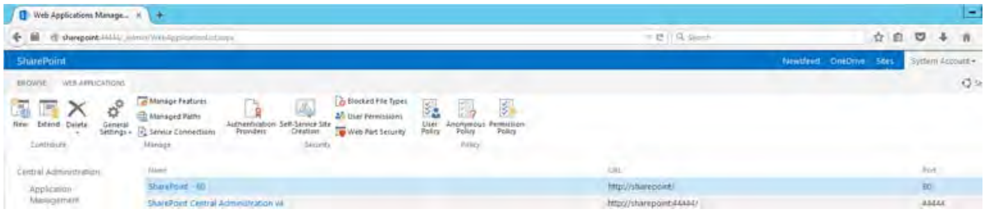
User Name: SharePointAdmin

Password: •••••••••••••••

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



4. If they do not already exist, create a default **Web Application** site and add it to a basic Site Collection in SharePoint via Central Administration (See Chapter 4).



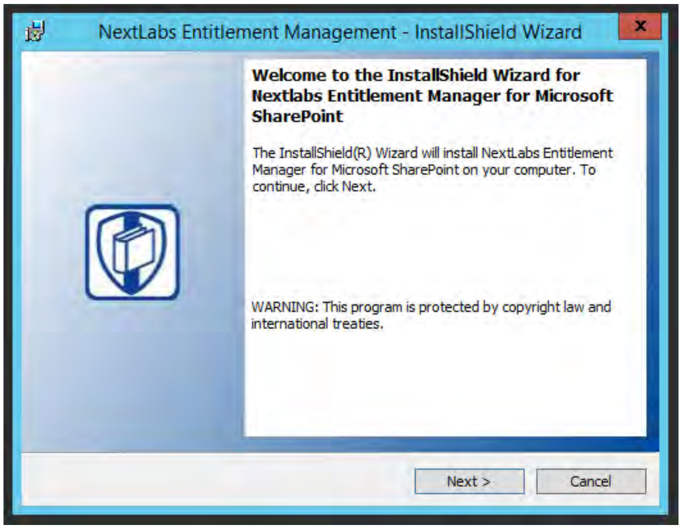
Name	URL	Port
SharePoint - 80	http://sharepoint/	80
SharePoint Central Administration v4	http://sharepoint:44444/	44444

7.6.1.2 Install NextLabs Entitlement Manager for SharePoint Server

Complete the standard Entitlement Manager for SharePoint Server installation per NextLabs documentation available to customers using the following steps:

1. On the SharePoint Server, go to your Desktop or other known location where the required NextLabs Policy Controller installation files are stored. Example: **C:\Users\Administrator\Desktop\SharePoint\**
2. Right-click on **SharePointEnforcer-2013-64-7.1.3.0-7-201410101427.zip** and select **Extract All** from the floating menu. Wait for the files to be extracted.
3. Double-click on the **SharePointEnforcer-2013-64-7.1.3.0-7-201410101427** folder.
4. Double-click on **SharePointEnforcer-2013-64-7.1.3.0-7.msi** to begin the installation.

5. At the Welcome to the InstallShield Wizard for NextLabs Entitlement Manager for MicroSoft SharePoint screen, click **Next**.



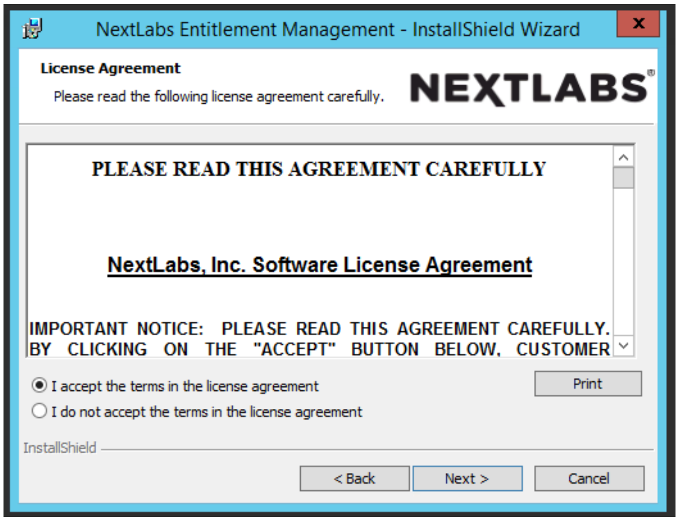
NextLabs Entitlement Management - InstallShield Wizard

Welcome to the InstallShield Wizard for Nextlabs Entitlement Manager for Microsoft SharePoint

The InstallShield(R) Wizard will install NextLabs Entitlement Manager for Microsoft SharePoint on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

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



NextLabs Entitlement Management - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

PLEASE READ THIS AGREEMENT CAREFULLY

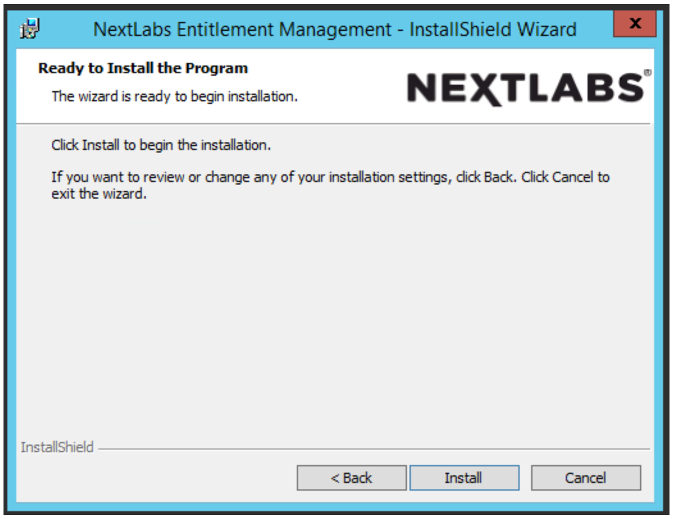
NextLabs, Inc. Software License Agreement

IMPORTANT NOTICE: PLEASE READ THIS AGREEMENT CAREFULLY. BY CLICKING ON THE "ACCEPT" BUTTON BELOW, CUSTOMER

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

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



NextLabs Entitlement Management - InstallShield Wizard

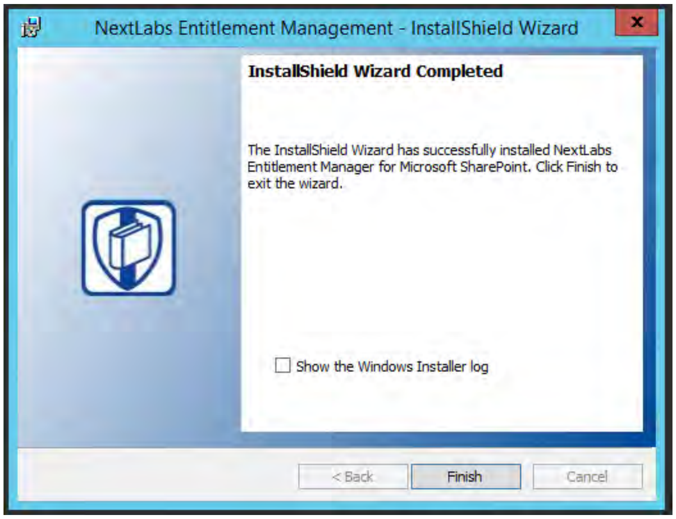
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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



NextLabs Entitlement Management - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed NextLabs Entitlement Manager for Microsoft SharePoint. Click Finish to exit the wizard.

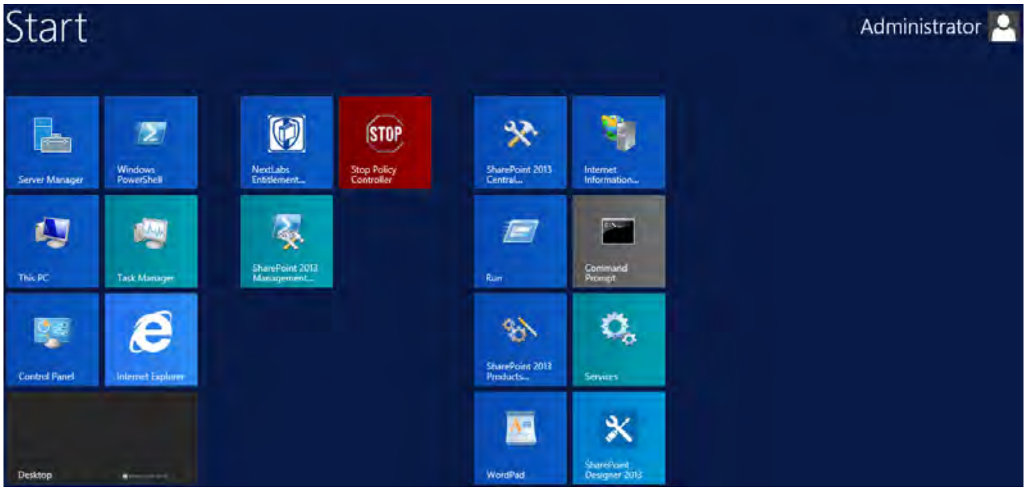
□ Show the Windows Installer log

9. After installing the IIS server must be reset:
   a. Click on the Windows icon and begin typing the word **PowerShell**
   b. When the Windows PowerShell application icon appears, double-click on the icon to open the Windows PowerShell
   c. From within the Windows PowerShell window, type in this command and press Enter to reset Internet Information Services: **iisreset**

7.6.1.3 Deploy Entitlement Manager for SharePoint Server to your SharePoint Farm

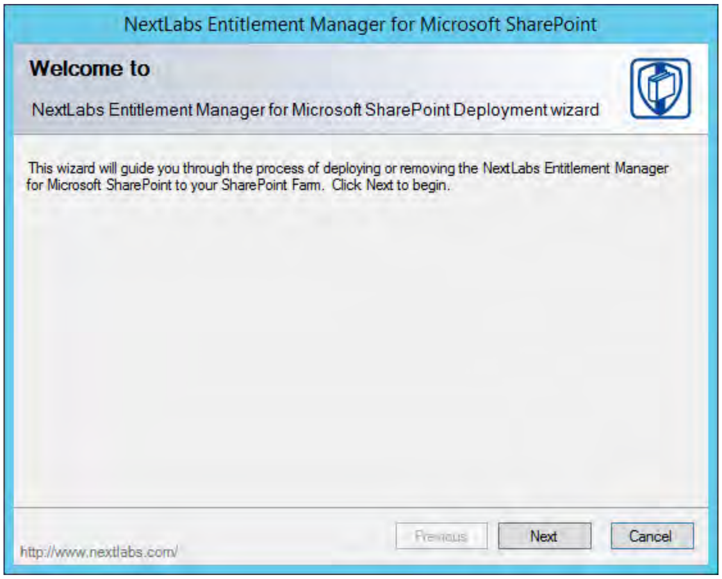
On the SharePoint Server, complete standard Entitlement Manager for SharePoint Server deployment per NextLabs documentation available to customers using the following steps:

1. On the SharePoint Server, click the **Start** icon to see the applications pinned to the **Start** menu.



2. Click on the NextLabs Entitlement Manager for SharePoint Server Deployment icon.
   a. 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: C:\Program Files\NextLabs\SharePoint Enforcer\bin\NextLabs.Entitlement.Wizard.exe**

3. At the Welcome to NextLabs Entitlement Manager for Microsoft SharePoint Deployment wizard screen, click **Next**.


NextLabs Entitlement Manager for Microsoft SharePoint

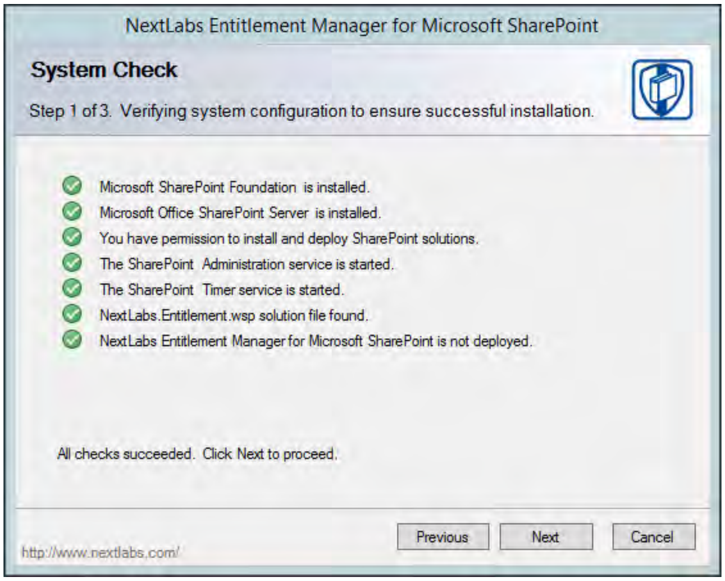
Welcome to

NextLabs Entitlement Manager for Microsoft SharePoint Deployment wizard

This wizard will guide you through the process of deploying or removing the NextLabs Entitlement Manager for Microsoft SharePoint to your SharePoint Farm. Click Next to begin.

http://www.nextlabs.com/

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



NextLabs Entitlement Manager for Microsoft SharePoint

System Check

Step 1 of 3. Verifying system configuration to ensure successful installation.

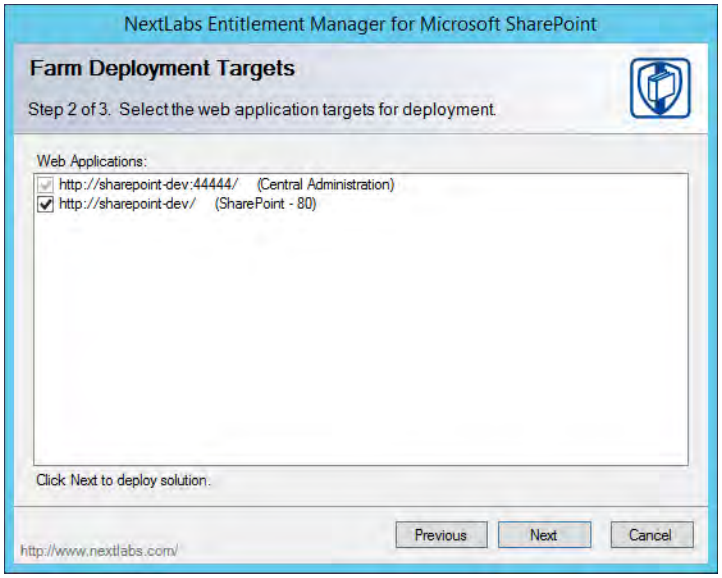
✓ Microsoft SharePoint Foundation is installed.
✓ Microsoft Office SharePoint Server is installed.
✓ You have permission to install and deploy SharePoint solutions.
✓ The SharePoint Administration service is started.
✓ The SharePoint Timer service is started.
✓ NextLabs.Entitlement.wsp solution file found.
✓ NextLabs Entitlement Manager for Microsoft SharePoint is not deployed.

All checks succeeded. Click Next to proceed.

http://www.nextlabs.com/

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

    a. Note: if there is only one entry listed, i.e., **http://sharepoint:44444/Central Administration**, no web applications have been created. In that case, refer back to section 7.6.1.1 or chapter 4.



NextLabs Entitlement Manager for Microsoft SharePoint

Farm Deployment Targets

Step 2 of 3. Select the web application targets for deployment.

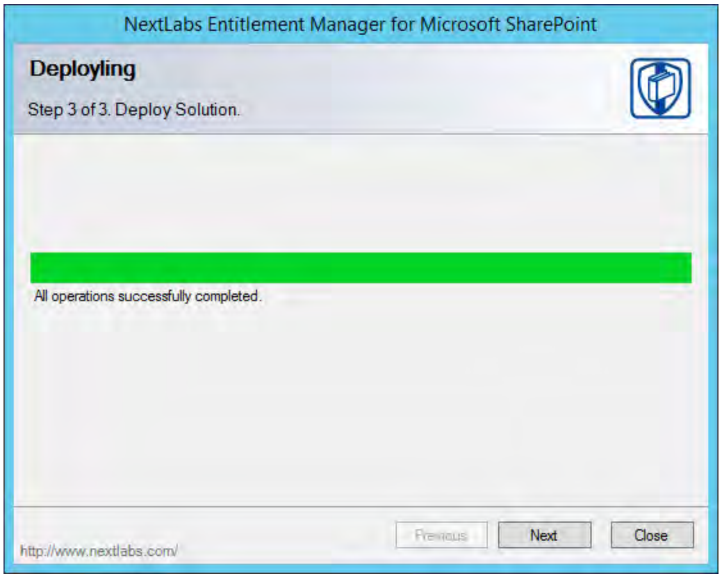
Web Applications:

☑ http://sharepoint-dev:44444/ (Central Administration)
☑ http://sharepoint-dev/ (SharePoint - 80)

Click Next to deploy solution.

http://www.nextlabs.com/

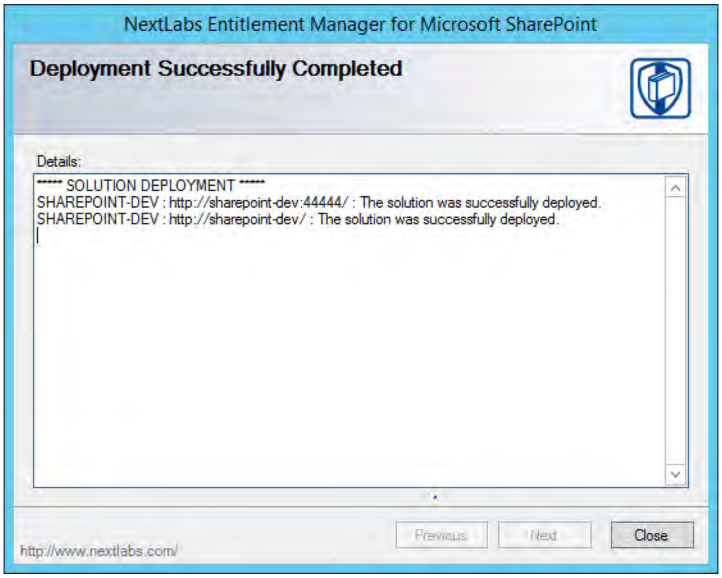
6. At the Deploying Step 3 of 3 screen, click **Next**.



NextLabs Entitlement Manager for Microsoft SharePoint
Deploying
Step 3 of 3. Deploy Solution.
Previous
Next
Close
http://www.nextlabs.com/

All operations successfully completed.

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



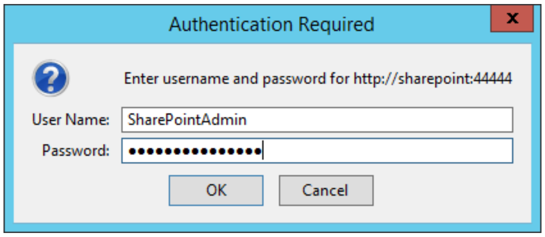
NextLabs Entitlement Manager for Microsoft SharePoint
Deployment Successfully Completed
Details:
Previous
Next
Close
http://www.nextlabs.com/

```
***** SOLUTION DEPLOYMENT *****
SHAREPOINT-DEV : http://sharepoint-dev:44444/ : The solution was successfully deployed.
SHAREPOINT-DEV : http://sharepoint-dev/ : The solution was successfully deployed.
```

7.6.1.4 Enable Policy Enforcement on your Web Application via SharePoint Central Administration

1. On the SharePoint Server, open an Internet browser and navigate to the following URL: **http://sharepoint:44444/default.aspx** to login to the SharePoint Central Administration portal.

2. Enter the **User Name** and **Password** for your SharePoint Central Administration account, and click **OK**.



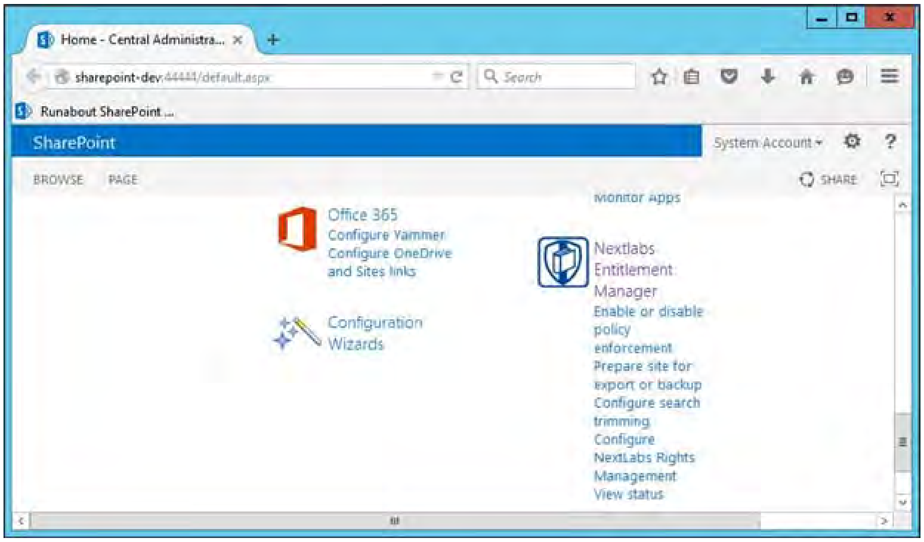
Authentication Required

Enter username and password for http://sharepoint:44444

User Name: SharePointAdmin

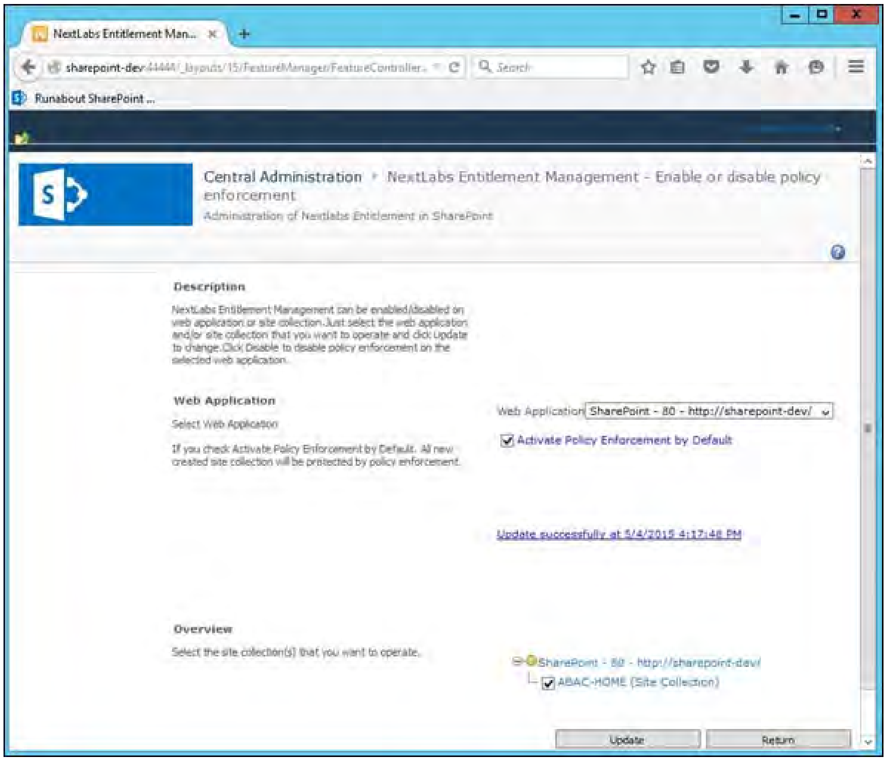
Password: •••••••••••••••

3. Click on the **NextLabs Entitlement Manager** icon.



Home - Central Administra...
sharepoint-dev:44444/default.aspx
Search
Runabout SharePoint ...
SharePoint
System Account
BROWSE
PAGE
SHARE
Monitor Apps
Office 365
Configure Yammer
Configure OneDrive and Sites links
Configuration Wizards
Nextlabs Entitlement Manager
Enable or disable policy enforcement
Prepare site for export or backup
Configure search trimming
Configure NextLabs Rights Management
View status

4. In the page that opens, scroll down to verify that the correct **Web Application** is chosen and the service is **Enabled**.


NextLabs Entitlement Man...
sharepoint-dev:44444/_layouts/15/FeatureManager/FeatureController...
Search
Runabout SharePoint ...
Update
Return

Central Administration ▸ NextLabs Entitlement Management - Enable or disable policy enforcement

Administration of Nextlabs Entitlement in SharePoint

Description

NextLabs Entitlement Management can be enabled/disabled on web application or site collection.Just select the web application and/or site collection that you want to operate and click Update to change.Click Disable to disable policy enforcement on the selected web application.

Web Application

Select Web Application

If you check Activate Policy Enforcement by Default. All new created site collection will be protected by policy enforcement.

Web Application: SharePoint - 80 - http://sharepoint-dev/

☑ Activate Policy Enforcement by Default

Update successfully at 5/4/2015 4:17:48 PM

Overview

Select the site collection(s) that you want to operate.

SharePoint - 80 - http://sharepoint-dev/

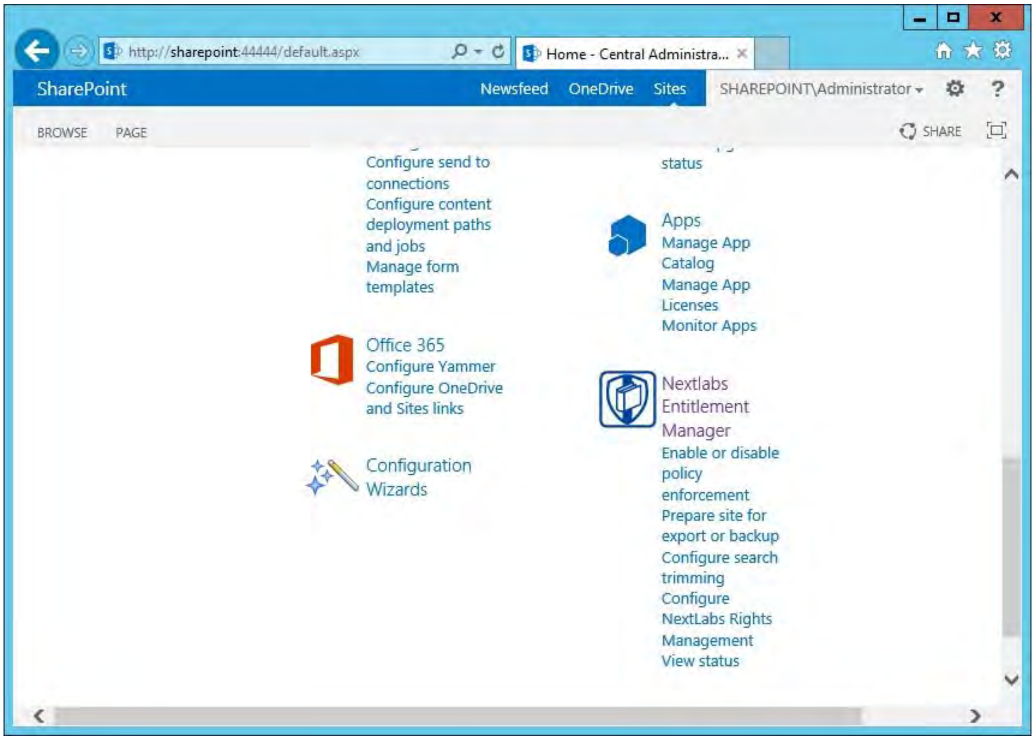
☑ ABAC-HOME (Site Collection)

7.7 Functional Tests

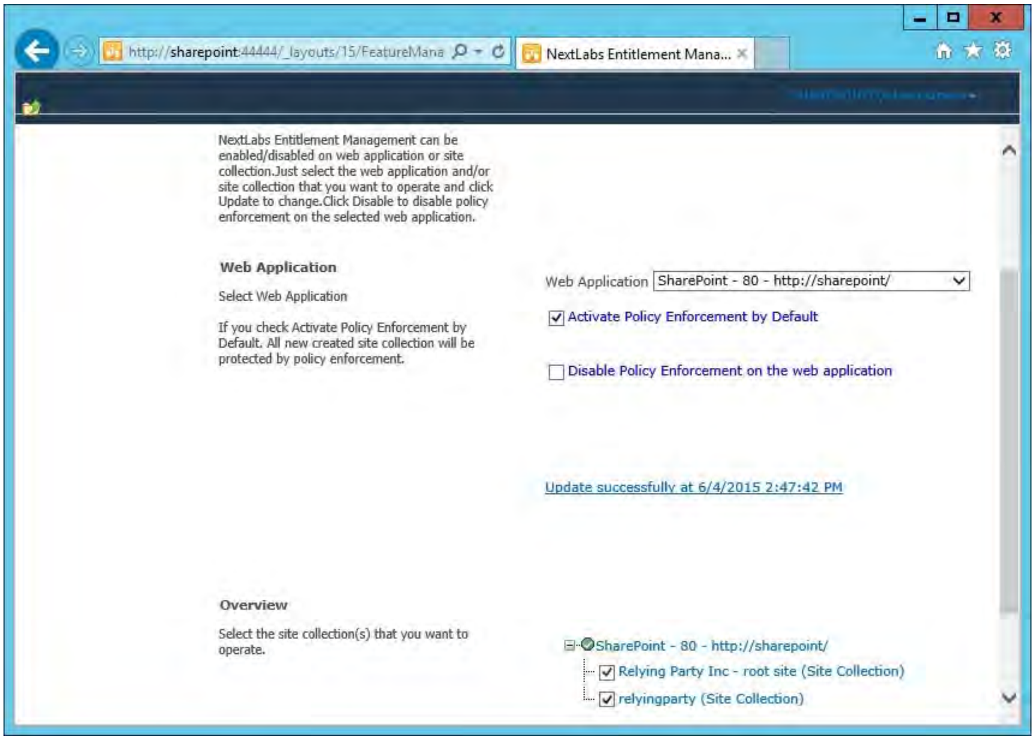
7.7.1 Verify that the NextLabs Webpart for Policy Enforcement has Successfully Been Enabled on the Site Collection in SharePoint

1. Similar to section 7.6.1.4, complete the following steps to login to SharePoint Central Administration:
    a. Click on the Start icon.
    b. Click the NextLabs Entitlement Manager for SharePoint icon.
    c. Open SharePoint Central Administration and login as Administrator.

2. Click on **Enable or disable policy enforcement** under the NextLabs Entitlement Manager webpart.


http://sharepoint:44444/default.aspx
Home - Central Administra...
SharePoint
Newsfeed
OneDrive
Sites
SHAREPOINT\Administrator
BROWSE
PAGE
SHARE
Configure send to connections
Configure content deployment paths and jobs
Manage form templates
status
Apps
Manage App Catalog
Manage App Licenses
Monitor Apps
Office 365
Configure Yammer
Configure OneDrive and Sites links
Nextlabs Entitlement Manager
Enable or disable policy enforcement
Prepare site for export or backup
Configure search trimming
Configure NextLabs Rights Management
View status
Configuration Wizards

3. Scroll down to the **Web Application** area to verify that the Entitlement Manager is activated for the correct SharePoint web application.


http://sharepoint:44444/_layouts/15/FeatureMana
NextLabs Entitlement Mana...

NextLabs Entitlement Management can be enabled/disabled on web application or site collection.Just select the web application and/or site collection that you want to operate and click Update to change.Click Disable to disable policy enforcement on the selected web application.

Web Application

Select Web Application

If you check Activate Policy Enforcement by Default. All new created site collection will be protected by policy enforcement.

Web Application: SharePoint - 80 - http://sharepoint/

☑ Activate Policy Enforcement by Default

☐ Disable Policy Enforcement on the web application

Update successfully at 6/4/2015 2:47:42 PM

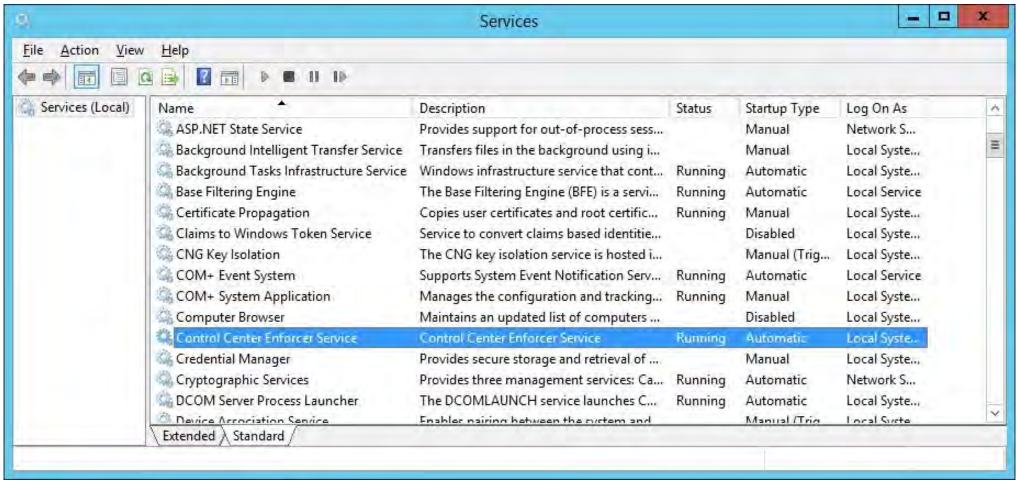
Overview

Select the site collection(s) that you want to operate.

- SharePoint - 80 - http://sharepoint/
  - ☑ Relying Party Inc - root site (Site Collection)
  - ☑ relyingparty (Site Collection)

7.7.2 Test to Verify the NextLabs Service is Running

1. Click on the Windows Start icon.
2. Start typing the word **Services**.
3. Click on the Windows Services icon to open the list of running services.
4. Look for the NextLabs Policy Controller service called **Control Center Enforcer Service**.
5. Verify that the status is **Running**.



Name	Description	Status	Startup Type	Log On As
ASP.NET State Service	Provides support for out-of-process sess...		Manual	Network S...
Background Intelligent Transfer Service	Transfers files in the background using i...		Manual	Local Syste...
Background Tasks Infrastructure Service	Windows infrastructure service that cont...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Filtering Engine (BFE) is a servi...	Running	Automatic	Local Service
Certificate Propagation	Copies user certificates and root certific...	Running	Manual	Local Syste...
Claims to Windows Token Service	Service to convert claims based identitie...		Disabled	Local Syste...
CNG Key Isolation	The CNG key isolation service is hosted i...		Manual (Trig...	Local Syste...
COM+ Event System	Supports System Event Notification Serv...	Running	Automatic	Local Service
COM+ System Application	Manages the configuration and tracking...	Running	Manual	Local Syste...
Computer Browser	Maintains an updated list of computers ...		Disabled	Local Syste...
Control Center Enforcer Service	Control Center Enforcer Service	Running	Automatic	Local Syste...
Credential Manager	Provides secure storage and retrieval of ...		Manual	Local Syste...
Cryptographic Services	Provides three management services: Ca...	Running	Automatic	Network S...
DCOM Server Process Launcher	The DCOMLAUNCH service launches C...	Running	Automatic	Local Syste...
Device Association Service	Enables pairing between the system and		Manual (Trig	Local Syste

8 Defining Policies and Enforcing Access Decisions with NextLabs

8.1 Introduction

In previous sections of this How-To Guide, we installed several NextLabs products that can be used to define and deploy Attribute-Based Access Control (ABAC) policies, and enforce decisions regarding user access to Microsoft SharePoint resources based on user, object, and environmental attributes, and the corresponding policies in place. This How-To Guide will illustrate how to use and configure NextLabs Policy Studio, the product responsible for Policy Lifecycle Management, and discuss policy strategy and the translation of business logic into policy.

Within Policy Studio, we will define and deploy policies and policy components. In NextLabs, the word **Component** is a named definition that represents a category or class of entities, such as users, data resources, or applications; or of actions, such as Open or Copy. Components are similar to using parts of speech to construct policy statements. For example:

Noun: **All employees in the human resources department** or **Any file with an .xls extension**

Verb: **Copy**, **Print**, or **Rename File**

Deployment is simply the distribution of new or modified policies and policy components to the appropriate enforcement points on desktop PCs, laptops, and file servers throughout the organization. This means you can create, review and refine policies as long as you like, but they are not enforced until you actually deploy them.

Finally, section 8.6, Functional Test, will illustrate how to ensure that policies are being updated, evaluated, and enforced on Microsoft SharePoint.

8.1.1 Components and Sub-components Used in this How-To Guide

1. NextLabs Policy Studio -provides the Policy Administration Point of the ABAC architecture. This component was installed with the rest of the NextLabs product suite used in this implementation in Chapter 7. Policy Studio provides the graphical user interface for Policy Lifecycle Management (defining, deploying, modifying, and deactivating policies).
   a. Located on the SQL Server
2. NextLabs Policy Server SharePoint Enforcer configuration file
   a. Automatically exists after NextLabs Control Center installation
   b. Located within the NextLabs software architecture on the SQL Server
3. NextLabs AgentLog and bundle.bin files
   a. Automatically exist after NextLabs Policy Controller installation
   b. Located within the NextLabs software architecture on the SharePoint Server

8.1.2 Pre-requisites to Complete Prior to This How-To Guide

1. If you intend to do a setup without identity federation and federated logins, you must:
   a. Install and configure Active Directory (see Chapter 2).
   b. Install and configure Microsoft SharePoint (see Chapter 4).

   c. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see Chapter 7).

2. If you intend to incorporate a trust relationship between an IdP and RP, and use federated logins into SharePoint, you must:
   a. Install and configure Active Directory (see Chapter 2).
   b. Setup and configure the RP and IdP (see Chapter 3).
   c. Install and configure Microsoft SharePoint (see Chapter 4).
   d. Configure the SharePoint federated login with the RP (see Chapter 5).
   e. Configure the attribute flow between all endpoints (see Chapter 6).
   f. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see Chapter 7).

8.2 Policy Strategy

8.2.1 Top-level Blacklisting Deny Policy, Whitelisting Allow Sub-policies

In order to demonstrate a policy set with high security and fine-grained control, we employed a general blacklisting, then fine grained whitelisting sub-policy strategy for the policies. We chose this strategy because we considered it a more secure paradigm for securing SharePoint resources. Using this strategy, the access control logic initially applies a general deny all access decision at the top level for a given set of related attributes, then specifies conditions under which access can be allowed in various sub-policies based on sufficient correlating user, resource, and/or environment attributes. For example, later in this guide we will describe a policy set in which we initially deny all users on resources that have a sensitivity level attribute, however there is a sub-policy that specifies that a for resources at sensitivity level 2, allow users with a clearance attribute of **Secret** during regular business hours. The alternative to this approach would be to apply a general allow all access decision at the top level initially, then specify conditions under which users should be denied access. Because there can be many unforeseen edge cases that may not be anticipated by a business protecting its assets, we consider the general blacklisting, then whitelisting sub-policies approach a more feasibly secure solution. According to our strategy, any time a user, resource, or environment attribute does not comply with a whitelisting sub-policy to allow access, the access decision will default to deny.

8.2.2 Global Policies

In addition to the blacklisting versus “white-listing” approach taken in our policy strategy, we also employed the use of global policies. The term **global policy** refers to the general applicability of the policy sets to more than one user and more than one resource at a given time. We defined our policies such that they have global effects and do not apply only to very specific use cases by themselves. The collective logic taken from the multiple global policies in place applies to the many kinds of access events that must be controlled according to a business’s complex and distributed business rules, which we describe in section 8.3.

8.3 Translation of Business Logic into Policy

8.3.1 ABAC Build Scenario - Runabout Air Business Rules

In previous sections of our Practice Guide we have constructed an example business scenario where an airline company, Runabout Air, has acquired another airline company, Conway Airlines. In this scenario the two companies have not yet merged their active directory forest and established a trust relationship such that historically Conway Airlines employees will be able to access resources on the Runabout Air SharePoint according to policies that correspond to Runabout Air's business rules. The business rules we based our policies on are, generally:

1. Some documents are more sensitive than others, and should be marked in SharePoint at different sensitivity levels. These documents should be strictly protected, and access should be restricted to Runabout Air's normal business hours. Also, users should only be granted access to sensitive documents if they have sufficient clearance.
2. Users should only be able to access documents that belong to their department, or to the departments relevant to them in the case of some instances of a need for cross-department access, i.e., business intelligence employees should have access to both sales and marketing department documents.
3. Some documents are time-sensitive and pertain to system or other business maintenance, and should be marked in SharePoint as maintenance documents. These documents should only be accessed outside of Runabout Air's normal business hours, so as to reduce the likelihood of disruption of normal business operation.
4. There are times when a suspicious IP address or range of addresses should be blocked from accessing any SharePoint resources, or when a user from a particular IP address or range of IP addresses should only have access to low-sensitivity documents. There must be a mechanism in place to ensure access is denied for users attempting to access any high-sensitivity documents from an environment with that IP address or within a given IP address range.

8.3.2 Translation of Runabout Air Business Rules into ABAC Policies

ABAC Policies created from the above business rules might look like this:

1. Top-level sensitivity policy: default to deny access to all users attempting to access resources that have a sensitivity level attribute defined in SharePoint as greater than **0**, unless explicitly allowed access by a sub-policy.
    a. For documents whose sensitivity attribute is defined as **1**, allow access any time of day, any day of the week, to users with a clearance attribute of **None**, **Secret**, or **Top Secret**.
    b. For documents whose sensitivity attribute is defined as **2**, allow access between the hours of 6am and 6pm for users with a clearance attribute of **Secret** or **Top Secret**.
    c. For documents whose sensitivity attribute is defined as **3**, allow access between the hours of 6am and 6pm for users with a clearance attribute of **Top Secret**.
2. Top-level department policy: default to deny access to all users attempting to access resources that have a department attribute and project status defined in SharePoint.

   a. For users whose department attribute is defined as a value equal to the document's department attribute value, allow access for documents with a project status of any value.

   b. For users whose department attribute is **Business Intelligence**, allow access for documents with a department attribute of **Sales** or **Marketing** and with a Project status of any value.

   c. Note: The Project status metric is necessary because the department attribute is defined at the site level within SharePoint. Restricting users based only on the resource's department attribute in this policy set results in the user being stuck in a deny access loop, no longer being able to access the Runabout Air root site and navigate to their correct department's documents. Because each document has a project status attribute defined in addition to the department attribute, the policies can specify the targets of this policy as having both project status and department attributes defined, even though the department attribute is the most pertinent attribute for enforcing the access control relating to department access rules.

3. Top-level maintenance policy: default to deny access to all users attempting to access resources that have a maintenance attribute defined in SharePoint

   a. For documents whose maintenance attribute is defined as **no**, allow access to users, any time of day, any day of the week.

   b. For documents whose maintenance attribute is defined as **yes**, allow access to users between 6pm and 6am, any day of the week.

4. Top-level IP Address policy: default to deny access to all users attempting to access resources that have a sensitivity attribute defined in SharePoint.

   a. For documents whose sensitivity attribute is defined as **1**, allow access to any user from an environment with any IP address defined.

   b. For documents whose sensitivity attribute is defined as **2** or **3**, allow access to users coming from an environment with an IP address other than a restricted IP or one within a restricted IP range.

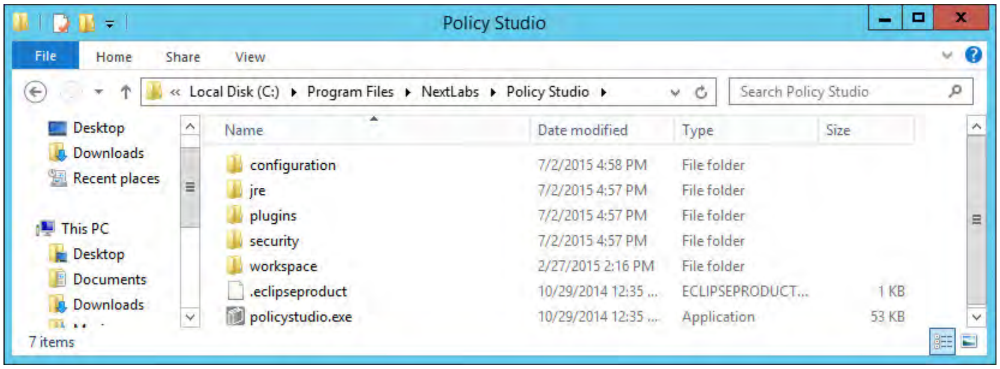
8.4 Using the NextLabs Policy Studio GUI for Policy Definition and Deployment

In this section we will provide step-by-step instructions for how to define, deploy, modify and re-deploy, and deactivate necessary policy components and policies within Policy Studio. The examples we will use correspond to the Runabout Air business rules and ABAC policies described in section 8.3.1 and section 8.3.2. Note that Policy Studio was installed on the SQL Server, which is where all of the activity in section 8.4 occurs.

8.4.1 Login and Initial Screen in Policy Studio

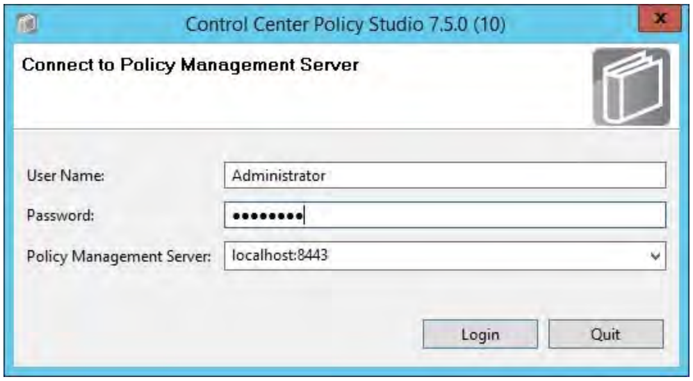
Given you have followed the instructions found in chapter 7, follow these instructions to login to the NextLabs Policy Studio:

1. In Windows Explorer, find and open the **policystudio.exe** application file:
    a. Double-click the **C:/** drive.
    b. Double-click **Program Files**.
    c. Double-click **NextLabs**.
    d. Double-click **Policy Studio**.
    e. Double-click **policystudio.exe**.



Name	Date modified	Type	Size
configuration	7/2/2015 4:58 PM	File folder	
jre	7/2/2015 4:57 PM	File folder	
plugins	7/2/2015 4:57 PM	File folder	
security	7/2/2015 4:57 PM	File folder	
workspace	2/27/2015 2:16 PM	File folder	
.eclipseproduct	10/29/2014 12:35 ...	ECLIPSEPRODUCT...	1 KB
policystudio.exe	10/29/2014 12:35 ...	Application	53 KB

2. In the Control Center Policy Studio window, enter **User Name** and **Password**, then click **Login** to connect to the Policy Management Server.

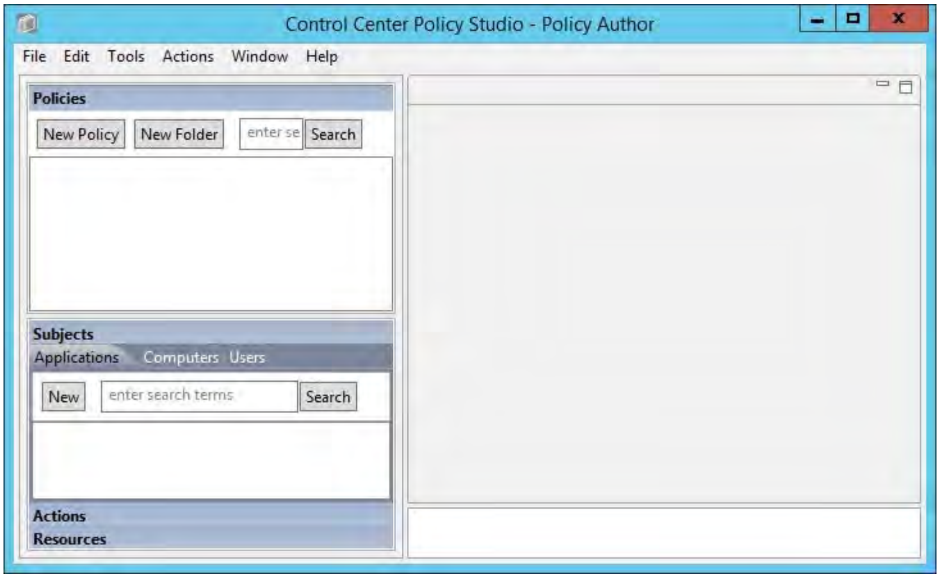

Control Center Policy Studio 7.5.0 (10)
Connect to Policy Management Server
Login
Quit

User Name: Administrator

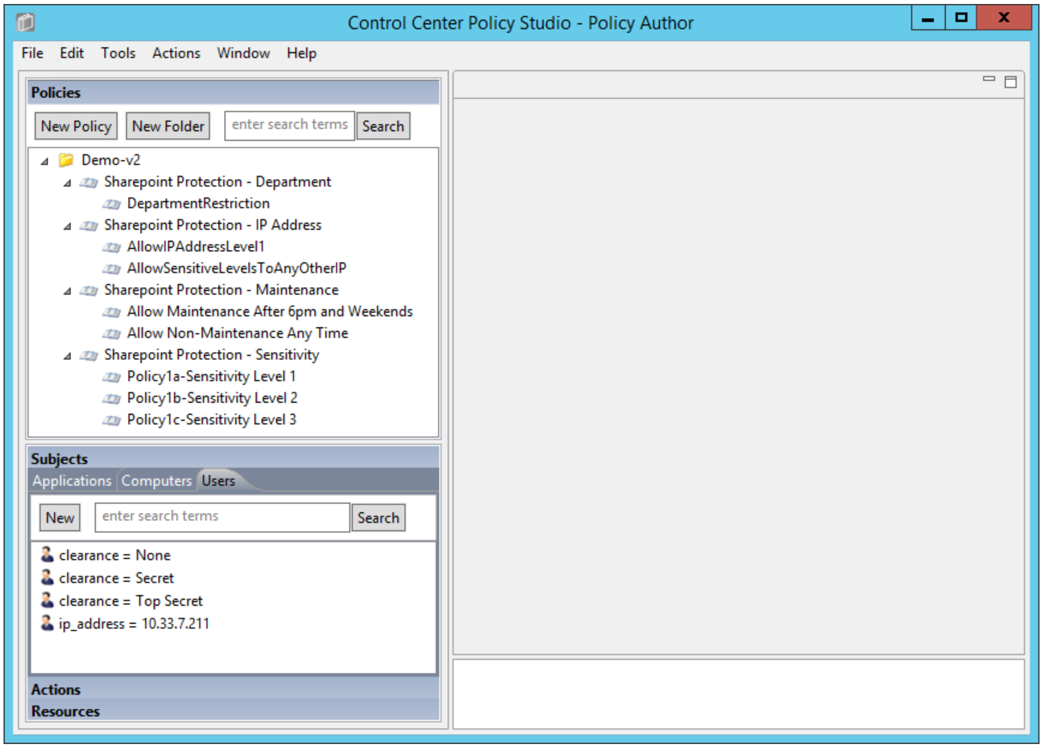
Password: ••••••••

Policy Management Server: localhost:8443

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.



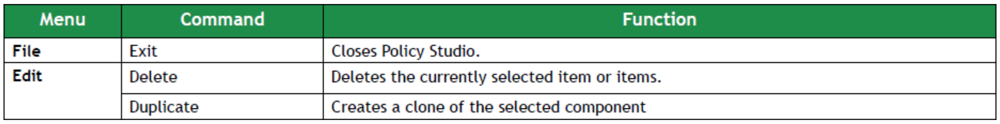
4. After following the instructions in this section to define and deploy several user and resource components, as well as four policy sets, the Policy Studio interface will show the new components and policies populated in the left-side panel.


Control Center Policy Studio - Policy Author
File Edit Tools Actions Window Help
Policies
New Policy
New Folder
enter search terms
Search
Demo-v2
Sharepoint Protection - Department
DepartmentRestriction
Sharepoint Protection - IP Address
AllowIPAddressLevel1
AllowSensitiveLevelsToAnyOtherIP
Sharepoint Protection - Maintenance
Allow Maintenance After 6pm and Weekends
Allow Non-Maintenance Any Time
Sharepoint Protection - Sensitivity
Policy1a-Sensitivity Level 1
Policy1b-Sensitivity Level 2
Policy1c-Sensitivity Level 3
Subjects
Applications
Computers
Users
New
enter search terms
Search
clearance = None
clearance = Secret
clearance = Top Secret
ip_address = 10.33.7.211
Actions
Resources

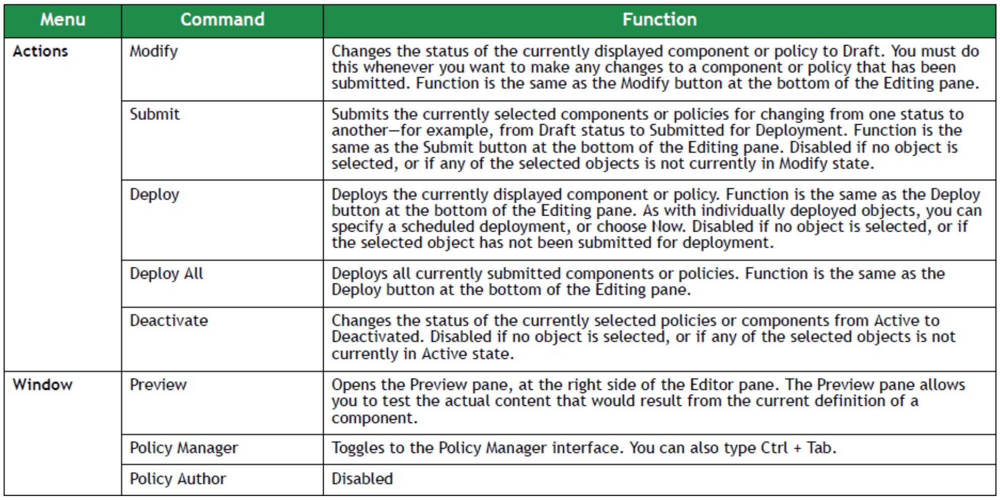
8.4.2 Policy Studio Menu Commands

Below are some of the Policy Studio menu commands used in this How-To Guide, along with explanations for what action they perform.

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



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

8.4.3 Defining and Deploying Components

8.4.3.1 Explanation of Components in NextLabs

According to the NextLabs Policy Studio User Guide available to customers, it is necessary to define components to represent various kinds of entities in your information environment. There are several times when you might want to define a new component:

1. After setting up your Control Center system, before constructing policies for the first time (which is the reason here at this point in our How-To literature)
2. When new classes of information or users come under the control of information policy
3. When a new policy requires a policy component that has not yet been created
4. When conditions at the organization change in any way that adds new items to be covered by information control policies. For example, if the company reorganizes and adds a new division, you might need a new policy component to represent the employees in that division.

Furthermore, when you are constructing a component, you do not need to save your work explicitly. Work is automatically saved as you go. If you are interrupted while working on a policy component, or want to work on another task and return to constructing the policy component later, you can stop and continue the constructing process as desired. Your work will be saved in draft status. You can find the policy component later in the appropriate component panel.

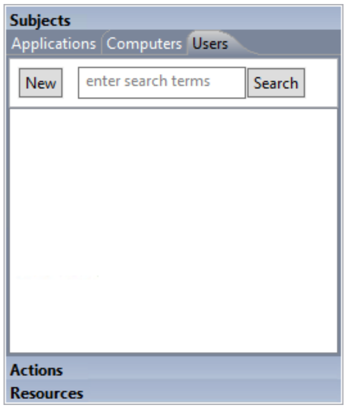
8.4.3.2 Defining and Deploying User Components

According to the Runabout Air business rules in section 8.3.2 and ABAC policies in section 8.3.2, it is possible that you may need to create a User Component to match the following conditions: user clearance attribute, user department attribute, and user IP address. This is correct except for the user department attribute. Because of the cross-departmental access of Runabout Air's Business Intelligence employees, we use logical syntax instead of graphical components while defining that policy. Also, a note regarding the user IP address component: even though IP address is an environmental attribute, it can be configured in NextLabs as a user attribute coming from SharePoint Claims, or as a resource attribute, which requires different configuration in NextLabs. For our example we use the IP Address from SharePoint Claims, which is handled as a user attribute.

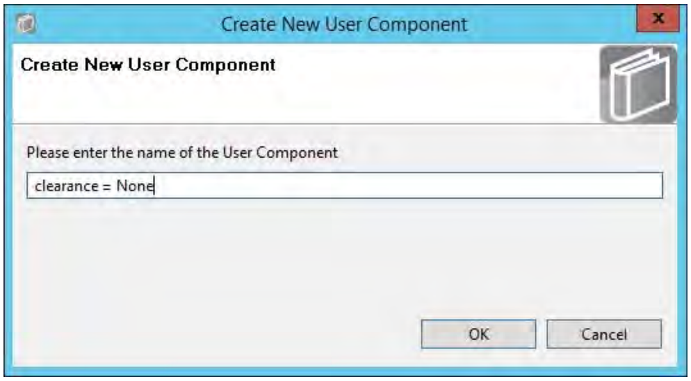
8.4.3.2.1 Clearance Components

Clearance = None

1. In the Components panel in the bottom-left of the Policy Studio window, click on the **Subjects** heading, and then click on the **Users** tab. Then click **New** to create a new component.



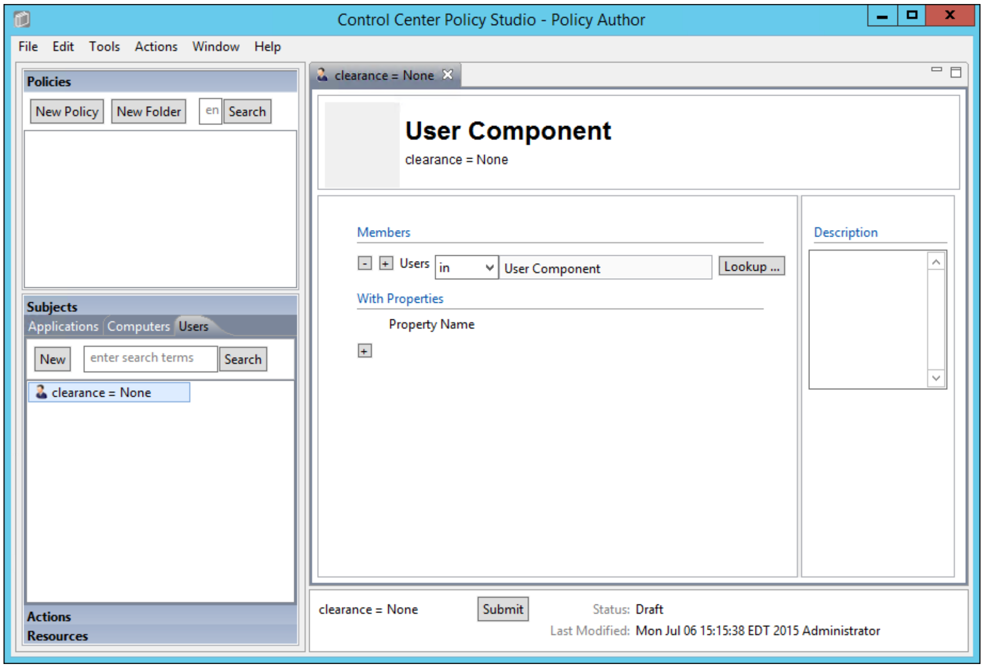
2. In the Create New User Component window, enter a descriptive component name, such as **clearance = None**. Click **OK**.



Please enter the name of the User Component

clearance = None

3. In the component editing panel you will see the following:



User Component

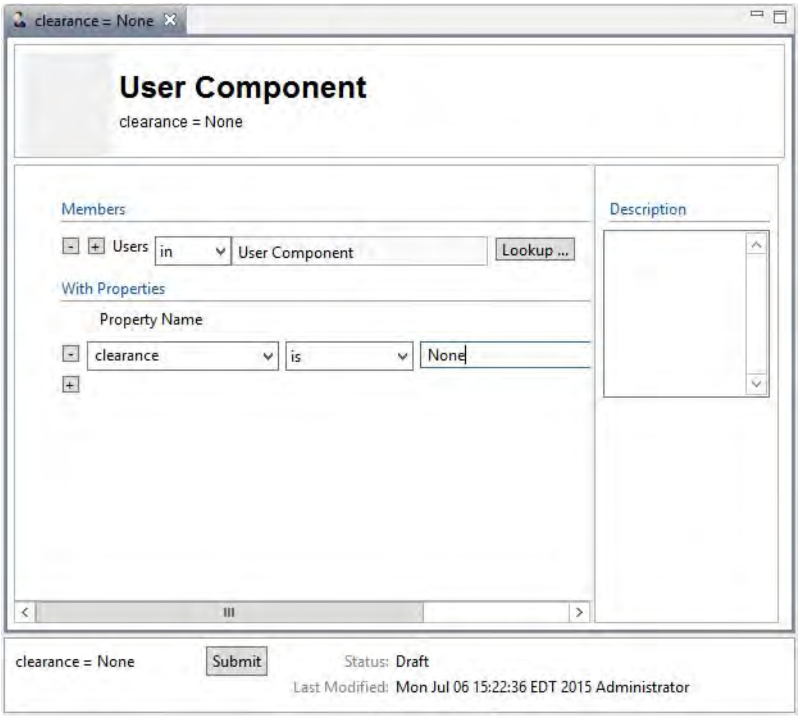
clearance = None

Users in User Component

Status: Draft

Last Modified: Mon Jul 06 15:15:38 EDT 2015 Administrator

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**.



User Component

clearance = None

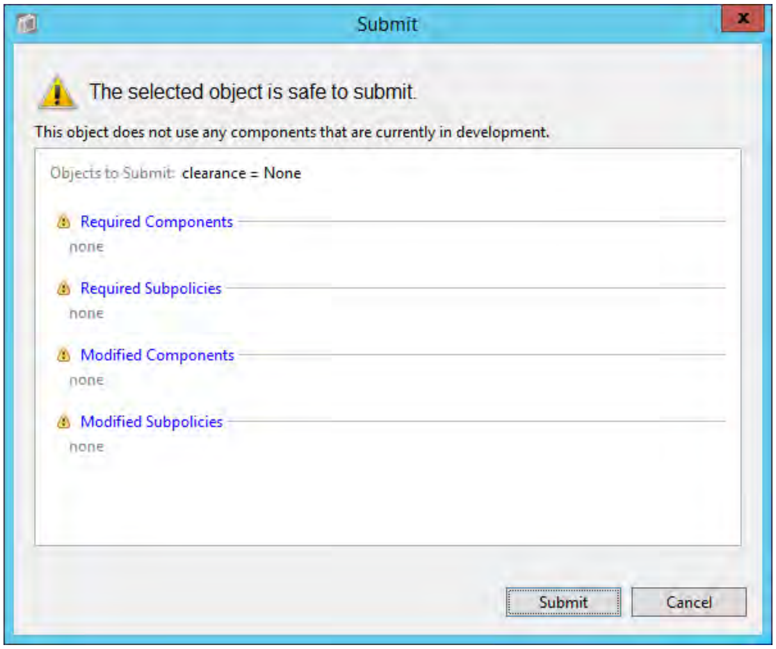
Users in User Component

clearance is None

Status: Draft

Last Modified: Mon Jul 06 15:22:36 EDT 2015 Administrator

5. In the Submit window, click **Submit**.



Submit

The selected object is safe to submit.

This object does not use any components that are currently in development.

Objects to Submit: clearance = None

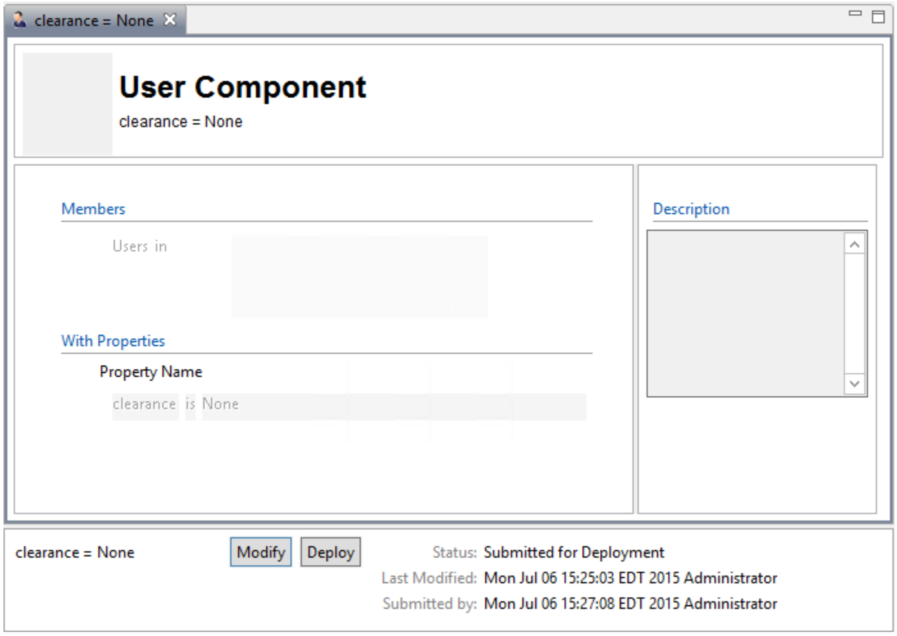
Required Components
none

Required Subpolicies
none

Modified Components
none

Modified Subpolicies
none

6. From the component editing panel, note the differences. The new status reads **Submitted for Deployment**. Click **Deploy**.



clearance = None

User Component

clearance = None

Members

Users in

With Properties

Property Name

clearance is None

Description

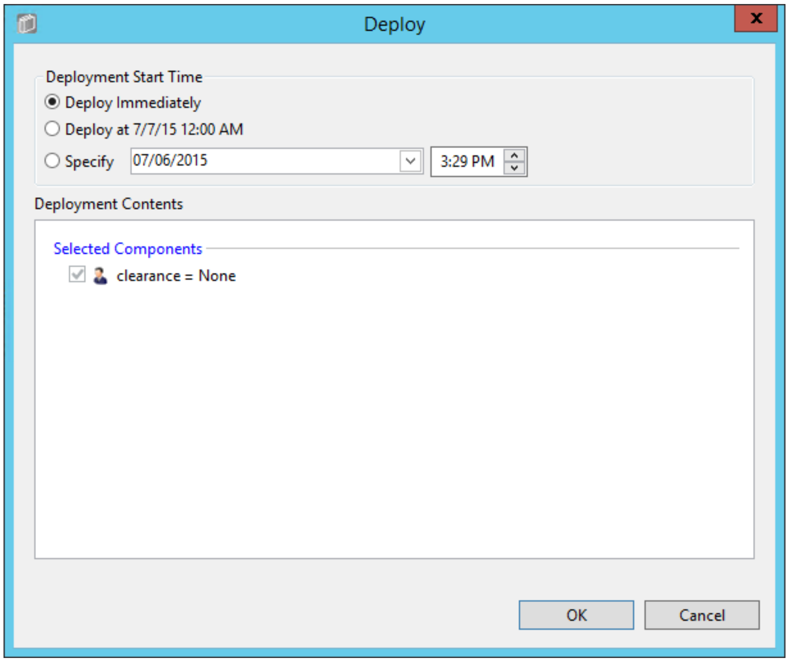
clearance = None

Status: Submitted for Deployment

Last Modified: Mon Jul 06 15:25:03 EDT 2015 Administrator

Submitted by: Mon Jul 06 15:27:08 EDT 2015 Administrator

7. In the Deploy window, click **OK**. Note: You may deploy immediately, which we choose in our example. You could also deploy the following day at midnight, or at a different specific date and time.



Deploy

Deployment Start Time

● Deploy Immediately

○ Deploy at 7/7/15 12:00 AM

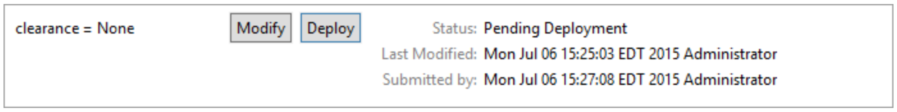
○ Specify 07/06/2015 3:29 PM

Deployment Contents

Selected Components

☑ clearance = None

8. Verify at the bottom of the component editing panel that the Status now reads **Pending Deployment**. This will remain for the duration of the heartbeat (described in chapter 7).



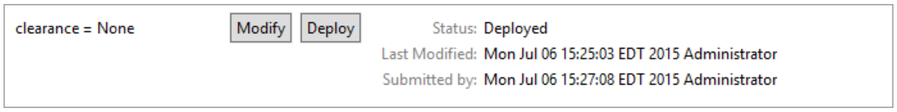
clearance = None

Status: Pending Deployment

Last Modified: Mon Jul 06 15:25:03 EDT 2015 Administrator

Submitted by: Mon Jul 06 15:27:08 EDT 2015 Administrator

9. After the duration of the heartbeat has passed, Status will then read as **Deployed**. This indicates that the component is actively deployed in your ABAC system.



clearance = None

Status: Deployed

Last Modified: Mon Jul 06 15:25:03 EDT 2015 Administrator

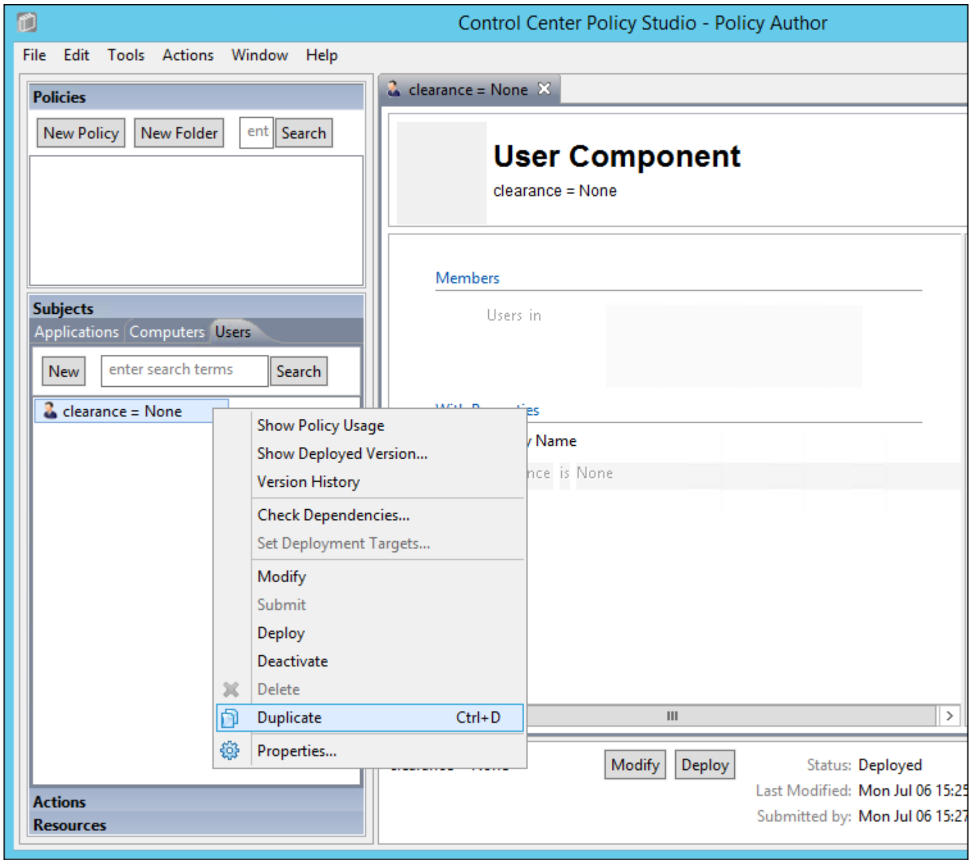
Submitted by: Mon Jul 06 15:27:08 EDT 2015 Administrator

Clearance = Secret

The easiest way to create additional attribute components is to duplicate existing ones. To duplicate the existing user attribute component:

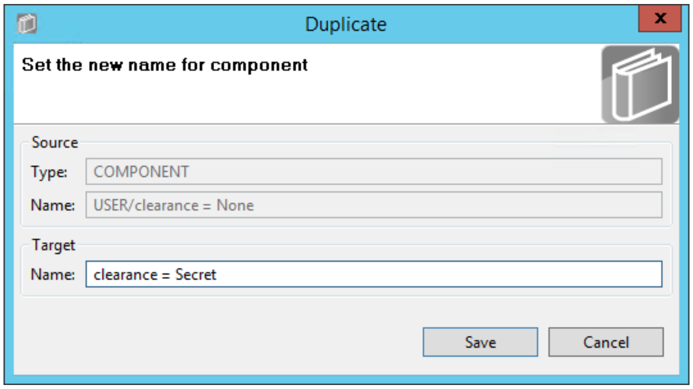
1. From the Component panel, highlight the name of the existing component, i.e., **clearance = None**

2. Click on **Edit** from the menu toolbar at the top of the window and select **Duplicate** from the drop-down menu, or right-click on the component and select **Duplicate** from the floating menu:



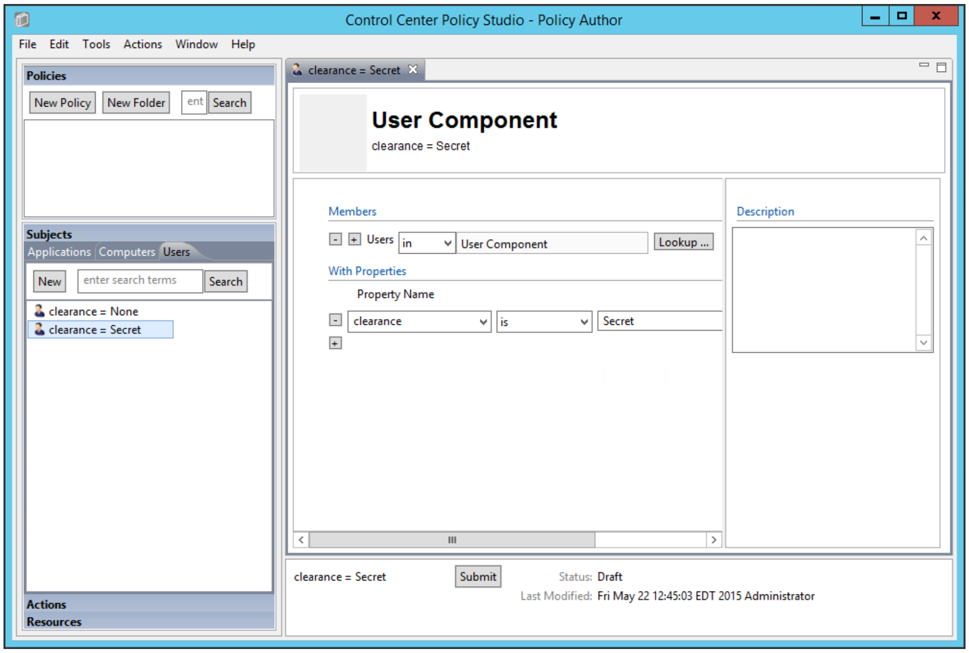
Status: Deployed
Last Modified: Mon Jul 06 15:25
Submitted by: Mon Jul 06 15:27

3. In the Duplicate window, edit the name of the new component, i.e., **clearance = Secret**. Click **Save**.



Type: COMPONENT
Name: USER/clearance = None
Name: clearance = Secret

4. Edit the property value to match the component's purpose, i.e., **Secret**. Click **Submit**.



clearance = None
clearance = Secret

clearance = Secret

User Component
clearance = Secret

Members
Users in User Component

With Properties
Property Name
clearance is Secret

clearance = Secret
Status: Draft
Last Modified: Fri May 22 12:45:03 EDT 2015 Administrator

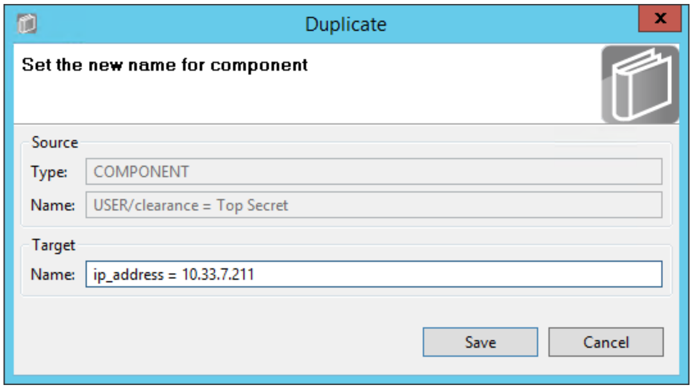
5. Repeat steps 5-9 from Clearance = None to Submit and Deploy this component.

Clearance = Top Secret

1. Repeat steps 1-5 in Clearance = Secret for duplicating a new user attribute component. The new component should be named **clearance = Top Secret**, and the property value should equal **Top Secret**.

8.4.3.2.2 IP Address Component

1. Repeat steps 1-3 in Clearance = Secret for duplicating a new user attribute component. The new component should be named **ip_address = 10.33.7.211**.

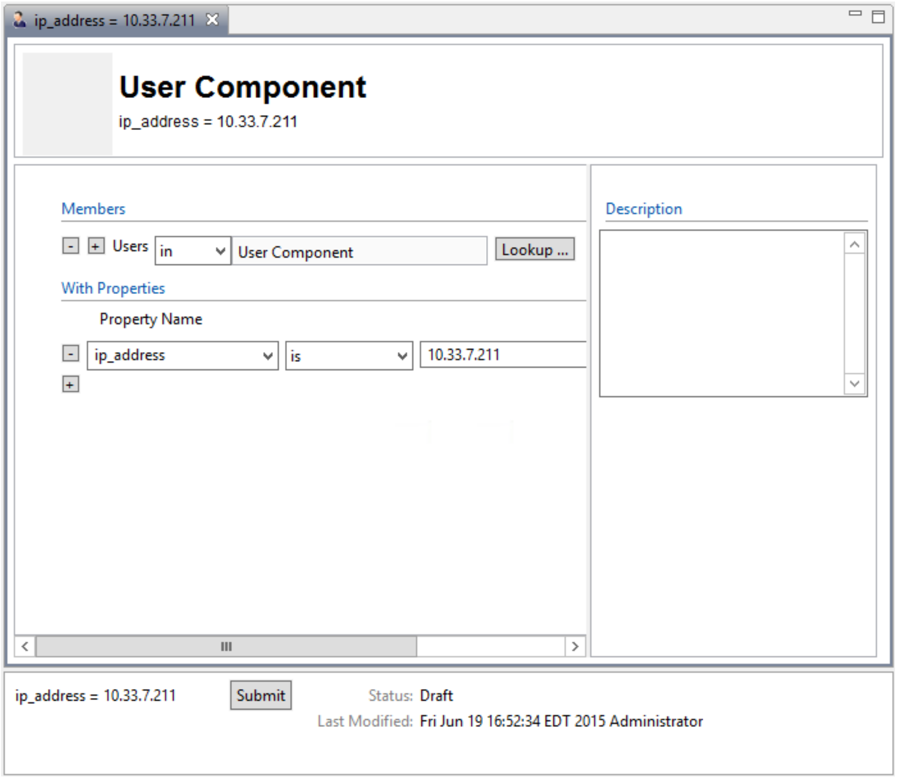


Set the new name for component

Source
Type: COMPONENT
Name: USER/clearance = Top Secret

Target
Name: ip_address = 10.33.7.211

2. 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**.



ip_address = 10.33.7.211

User Component

ip_address = 10.33.7.211

Members

Users in User Component

With Properties

Property Name

ip_address is 10.33.7.211

ip_address = 10.33.7.211

Status: Draft

Last Modified: Fri Jun 19 16:52:34 EDT 2015 Administrator

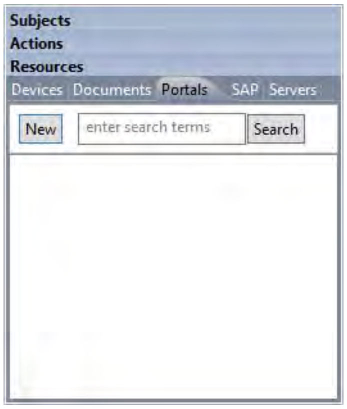
3. Repeat steps 5-9 from the Clearance = None to Submit and Deploy this component.

8.4.3.3 Defining and Deploying Resource Components

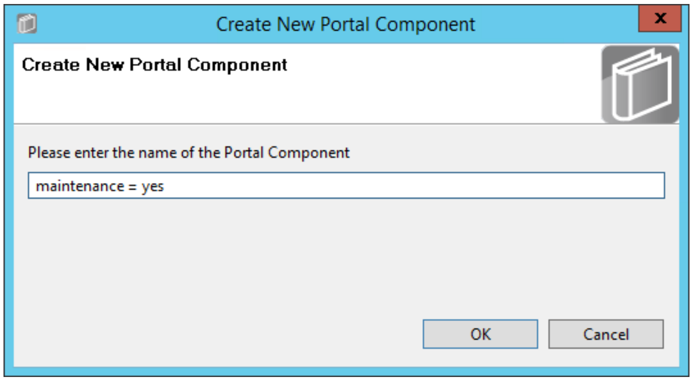
8.4.3.3.1 Maintenance Components

Maintenance = yes

1. In the Components panel in the bottom-left of the Policy Studio window, click on the **Resources** heading, and then click on the **Portals** tab. Then, click **New** to create a new component.



2. Enter a descriptive component name, such as **maintenance = yes**, then click **OK**.



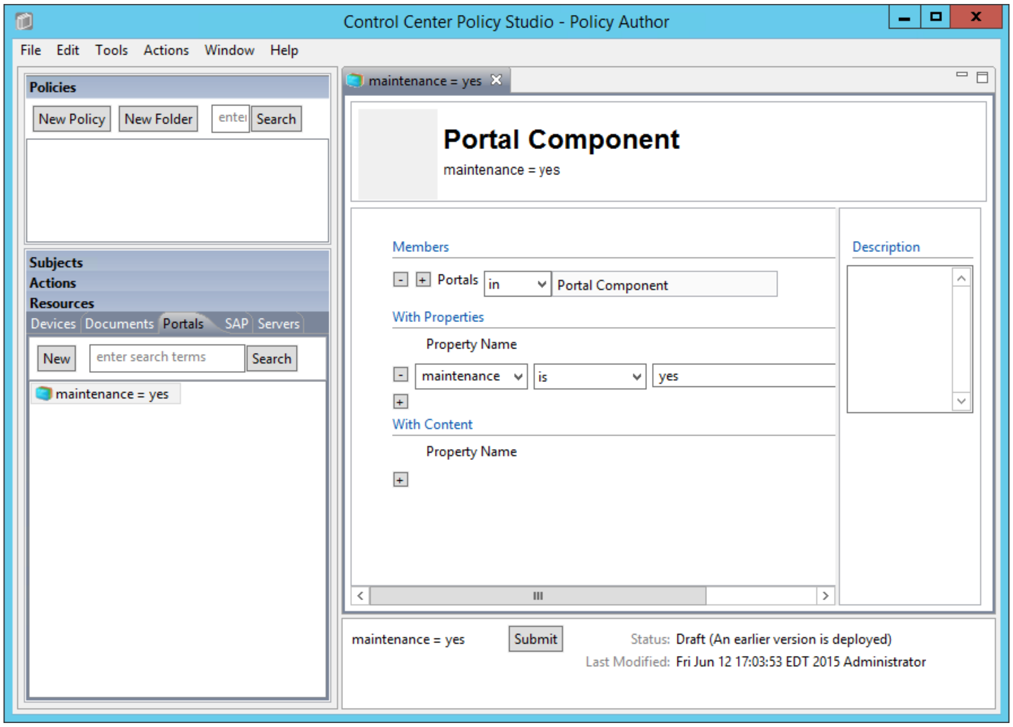
Create New Portal Component

Create New Portal Component

Please enter the name of the Portal Component

maintenance = yes

3. In the editing panel, click on the **plus sign** box under Property Name and enter **maintenance** in the **Property Name** text box, keep the default is as the action, and enter **yes** into the value text box. Then click **Submit**.



Control Center Policy Studio - Policy Author

Portal Component

maintenance = yes

Members: Portals in Portal Component

With Properties — Property Name: maintenance is yes

With Content — Property Name

maintenance = yes Submit

Status: Draft (An earlier version is deployed)

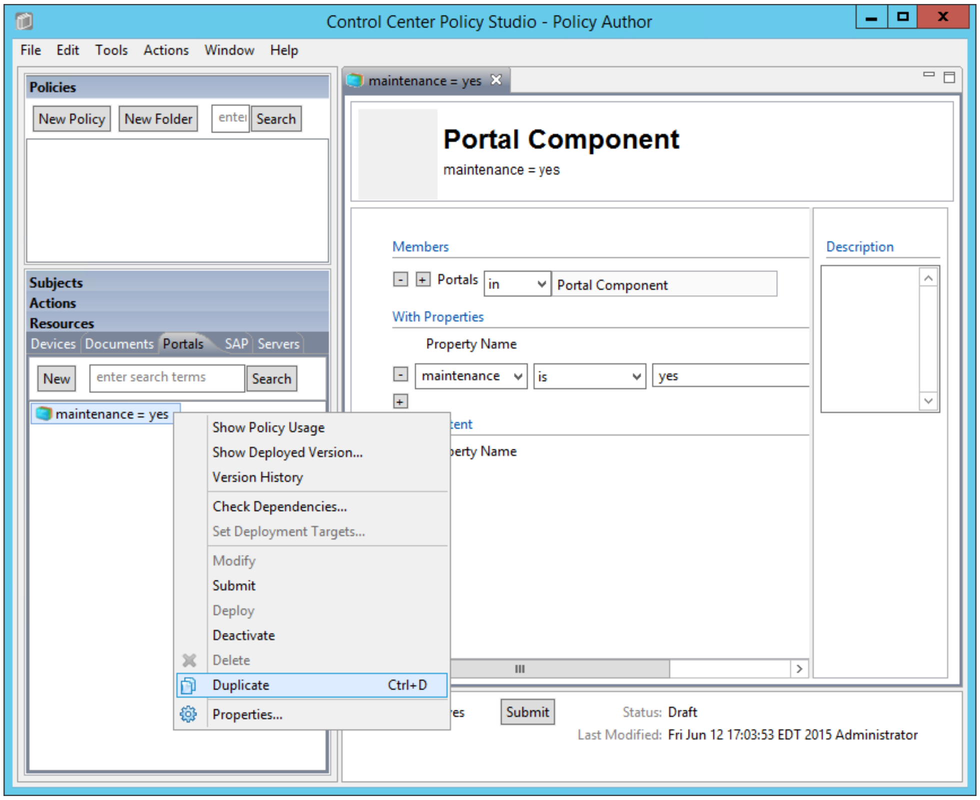
Last Modified: Fri Jun 12 17:03:53 EDT 2015 Administrator

4. Repeat steps 5-9 from Clearance = None to Submit and Deploy this component.

Maintenance = no

Similar to the steps taken for duplicating user components, do the following to duplicate the existing resource maintenance component to create the other resource components.

1. In the Component panel in the bottom-left corner of the Policy Studio interface, right-click on the **maintenance = yes** component. In the floating menu, select **Duplicate**.



Portal Component

maintenance = yes

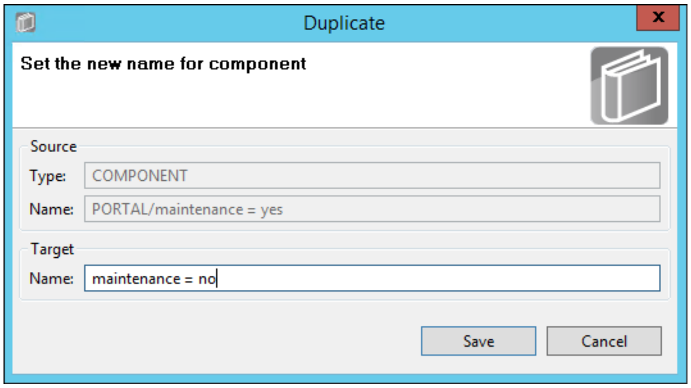
Portals in Portal Component

maintenance is yes

Status: Draft

Last Modified: Fri Jun 12 17:03:53 EDT 2015 Administrator

2. In the Duplicate window, edit the name of the new component. Example: **maintenance = no**.

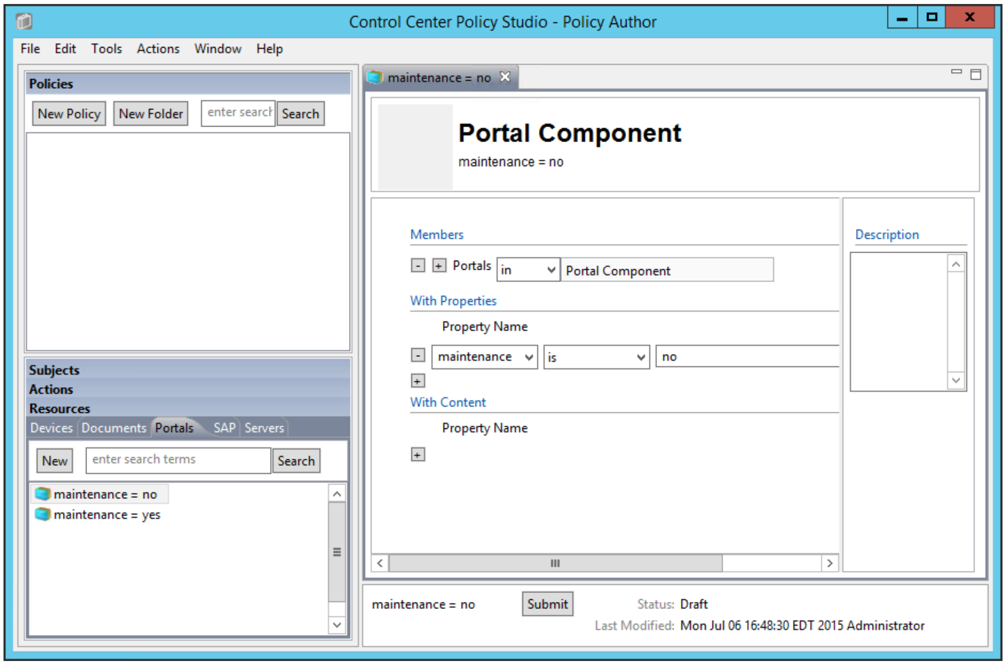


Type: COMPONENT

Name: PORTAL/maintenance = yes

Name: maintenance = no

3. In the component editing panel, change the property value to **no** and click **Submit**.



4. Repeat steps 5-9 from Clearance = None to Submit and Deploy this component.

8.4.3.3.2 Sensitivity components

Sensitivity = 1

1. Repeat steps 1-4 from Maintenance = no to duplicate an existing resource component to create the Sensitivity = 1 component.

Sensitivity = 2

1. Repeat steps 1-4 from Maintenance = no to duplicate an existing resource component to create the Sensitivity = 2 component.

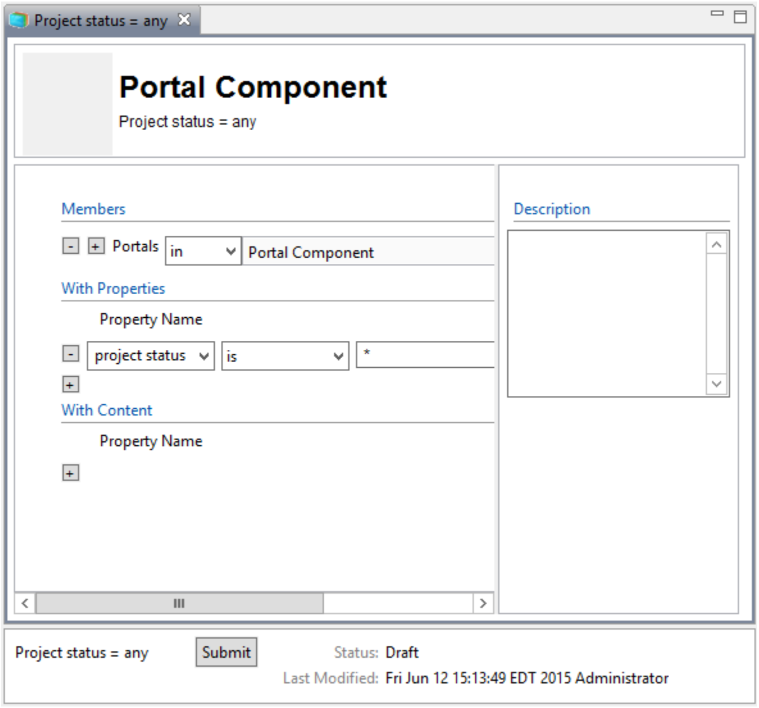
Sensitivity = 3

1. Repeat steps 1-4 from Maintenance = no to duplicate an existing resource component to create the Sensitivity = 3 component.

8.4.3.3.3 Project status component

Project status = any

1. Repeat steps 1-4 from Maintenance = no to duplicate an existing resource component to create the Project status = any component.
2. **Note**: Before the Submit step, in the component editing panel, enter the property value as *.



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

Submit

Status: Draft

Last Modified: Fri Jun 12 15:13:49 EDT 2015 Administrator

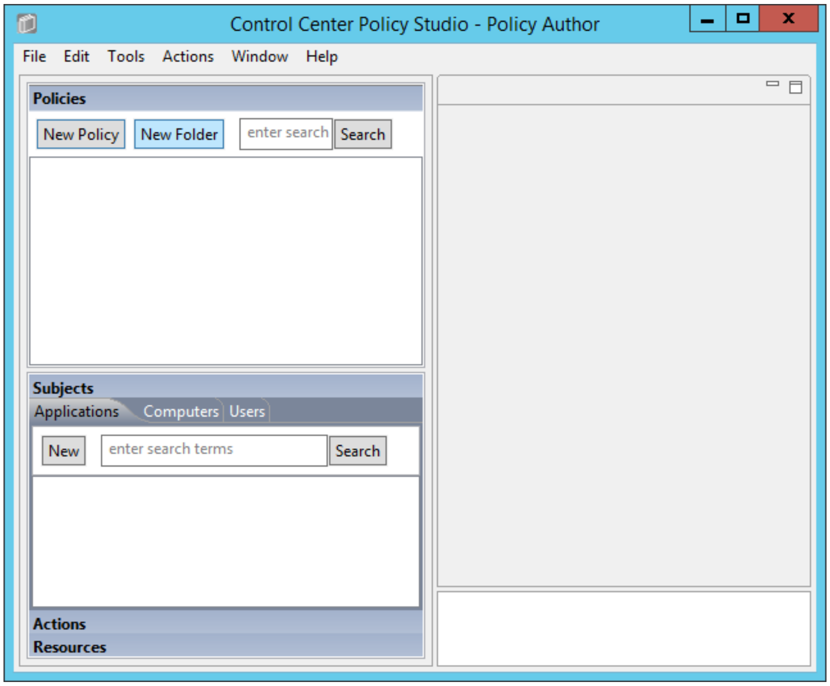
8.4.4 Defining Policy

After following the steps to define and deploy components in section 8.4.3, you can continue on to define policies that relate to the Runabout Air scenario business rules discussed in section 8.3. In order to define policies in Policy Studio, login as described in section 8.4.1.

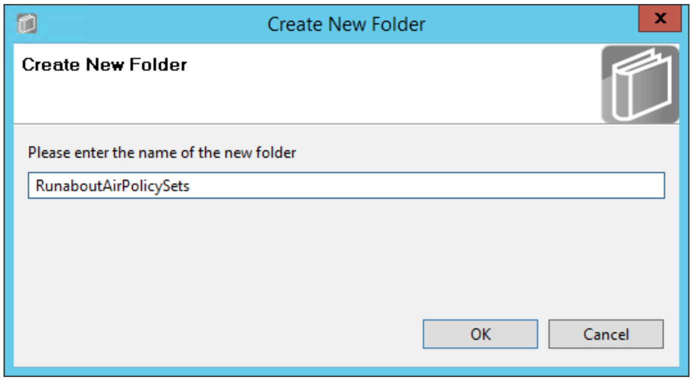
8.4.4.1 Creating a Policy Set Folder

Before being able to create any policies in Policy Studio, first you must create a folder, or choose an existing one.

1. From the main Policy Studio window, click **New Folder**.



2. Enter the **name** of your folder and click **OK**.



Create New Folder

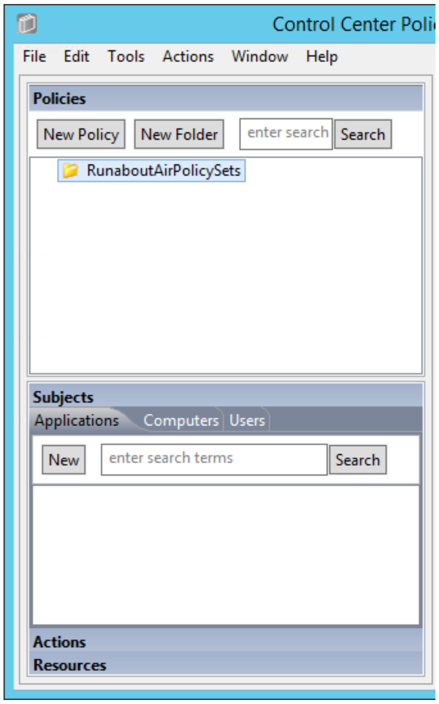
Please enter the name of the new folder

RunaboutAirPolicySets

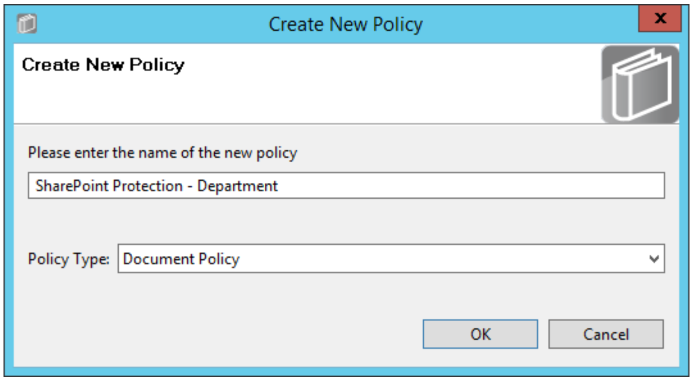
8.4.4.2 Defining Department-based Policy Set

8.4.4.2.1 Defining the Top-level Department Policy that Enforces a General Deny Decision

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**.



2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-down menu, select **Document Policy** (which applies to all SharePoint policies). Click **OK**.



Please enter the name of the new policy: SharePoint Protection - Department

Policy Type: Document Policy

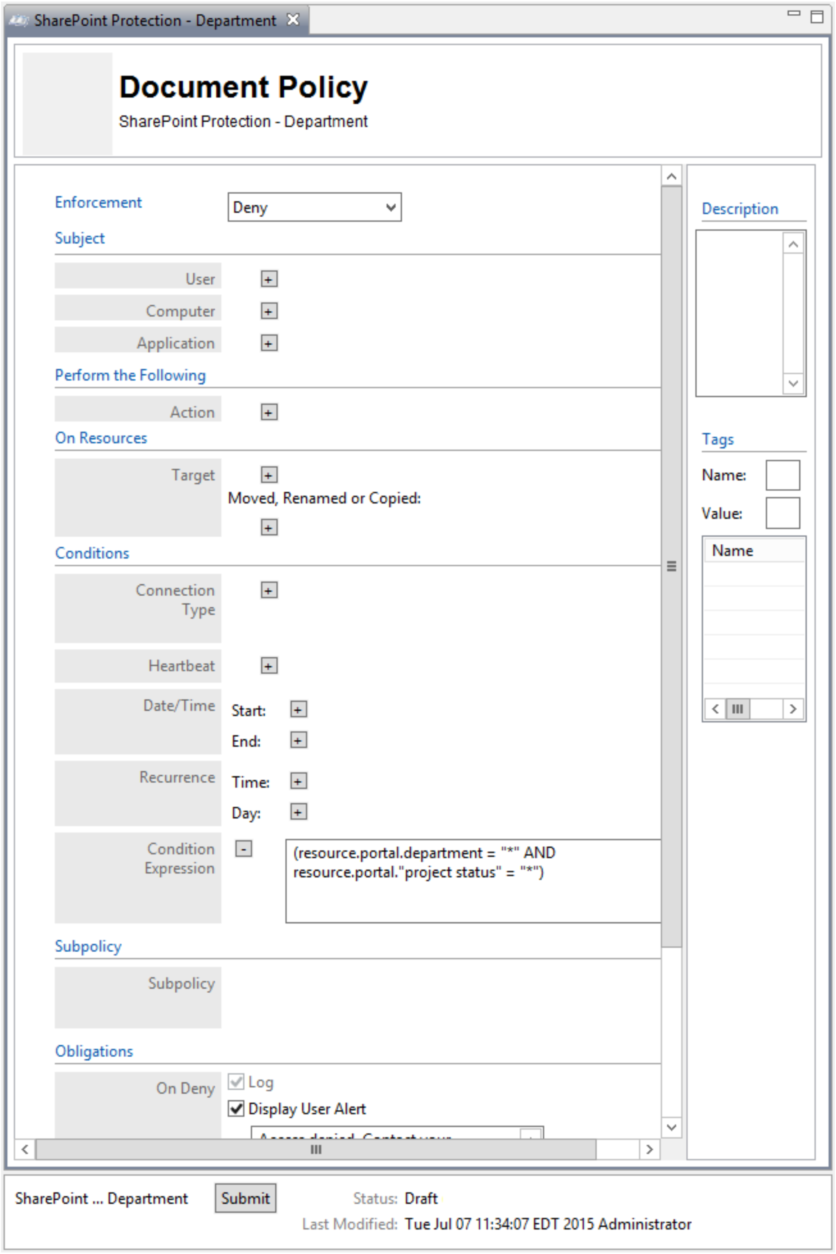
3. The new policy opens automatically in an editing panel. For this policy, keep the default **Deny** enforcement. Make these edits:

   a. In the On Resources area, click on the **plus sign** box next to **Target**. This automatically populates **in** and **Resource Component**.

   b. In the **Condition Expression** enter the ACPL: (**resource.portal.department = "*" AND resource.portal.project status = "*"**)

   c. In the Obligations area, check the **Display User Alert** box in order to customize the deny message displayed to the user when access is denied.

4. In the policy editing panel, your policy should look like this:



Document Policy

SharePoint Protection - Department

Enforcement: Deny

Subject

Perform the Following

On Resources

Moved, Renamed or Copied:

Conditions

Date/Time Start: End:

Recurrence Time: Day:

Condition Expression: (resource.portal.department = "*" AND resource.portal."project status" = "*")

Subpolicy

Obligations

On Deny: ☑ Log ☑ Display User Alert

Access denied. Contact your

SharePoint ... Department Submit Status: Draft

Last Modified: Tue Jul 07 11:34:07 EDT 2015 Administrator

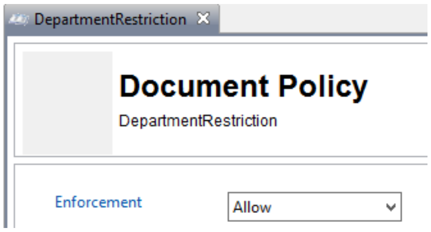
5. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.2.2 Defining a Department-based Sub-policy that Enforces an Allow Decision when Certain Conditions are met

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new policy to highlight it. Then click on **New Policy** to create a sub-policy.
2. Select a **name** for the new sub-policy then click **OK**.

3. In the policy editing panel, make the following edits:

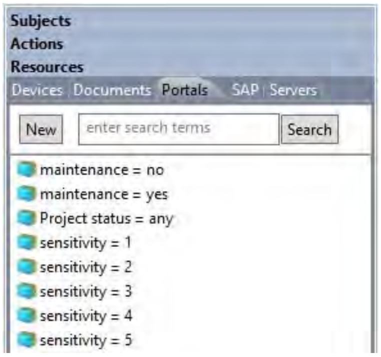
   a. From the Enforcement drop-down menu, select **Allow**.



Enforcement: Allow

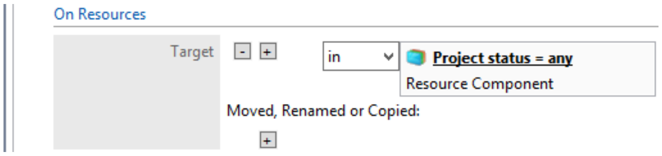
   b. In the On Resources area, click on the **plus sign** box next to **Target**.

      i. In the Components panel, click on **Resources**, then the **Portals** tab to see the components you created earlier.



maintenance = no
maintenance = yes
Project status = any
sensitivity = 1
sensitivity = 2
sensitivity = 3
sensitivity = 4
sensitivity = 5

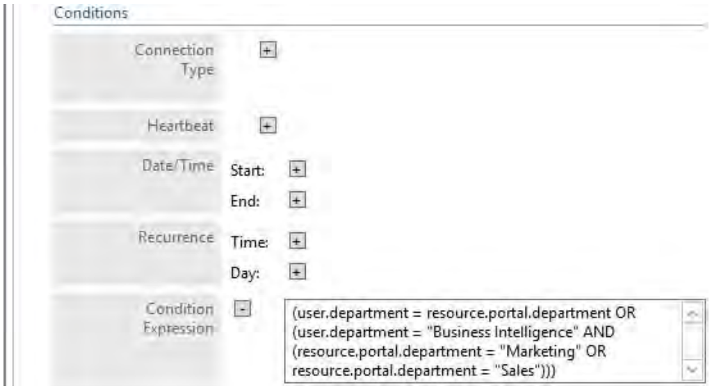
      ii. From the Portals tab, left-click and hold the **Project status = any** component and drag it onto the **Target** field.



Target: in Project status = any (Resource Component)

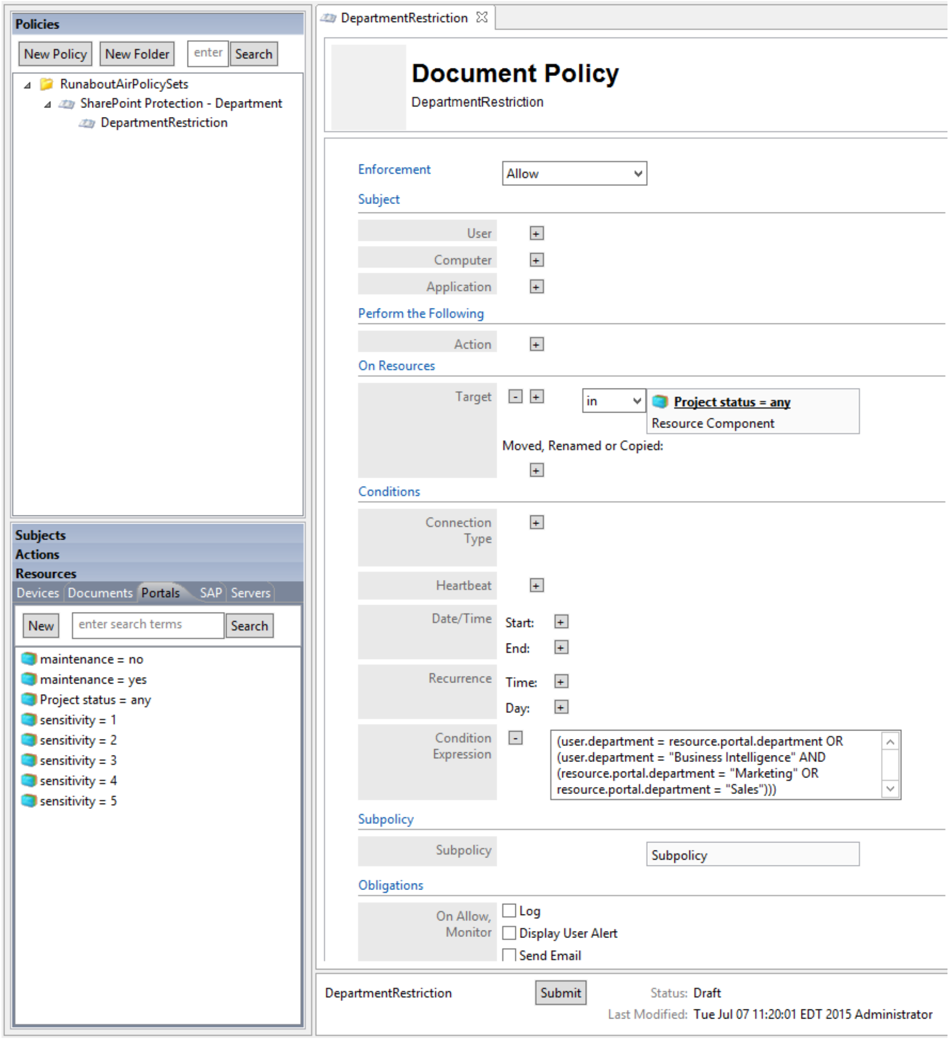
   c. In the Conditions area, in the **Condition Expression** text box, enter the ACPL: **(user.department = resource.portal.department OR (user.department = "Business**

Intelligence" AND (resource.portal.department = "Marketing" OR resource.portal.department = "Sales")))



Condition Expression: (user.department = resource.portal.department OR (user.department = "Business Intelligence" AND (resource.portal.department = "Marketing" OR resource.portal.department = "Sales")))

4. In the Policy Editing panel, your policy should look like this:



Enforcement: Allow

Target: in Project status = any Resource Component

Moved, Renamed or Copied:

Condition Expression: (user.department = resource.portal.department OR (user.department = "Business Intelligence" AND (resource.portal.department = "Marketing" OR resource.portal.department = "Sales")))

On Allow, Monitor: □ Log □ Display User Alert □ Send Email

DepartmentRestriction

Status: Draft

Last Modified: Tue Jul 07 11:20:01 EDT 2015 Administrator

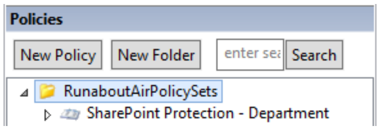
5. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.3 Defining a Sensitivity-based Policy Set

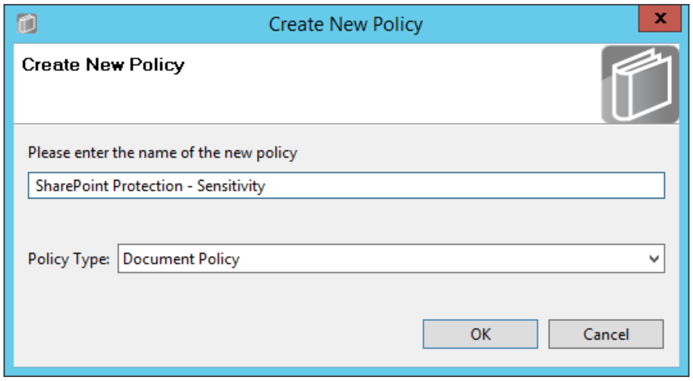
In order to define a sensitivity-based policy set, follow instructions similar to defining the department-based policy set in section 8.4.4.2:

8.4.4.3.1 Defining the Top-level Sensitivity Policy that Enforces a General Deny Decision

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your folder to highlight it. Then click on **New Policy**.



2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-down menu, select **Document Policy** (which applies to all SharePoint policies). Click **OK**.



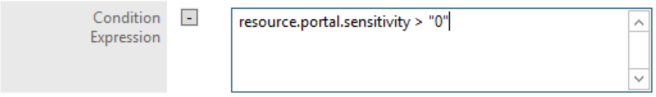
Please enter the name of the new policy: SharePoint Protection - Sensitivity

Policy Type: Document Policy

3. The new policy opens automatically in an editing panel. For this policy, keep the default **Deny** enforcement. Make these edits:

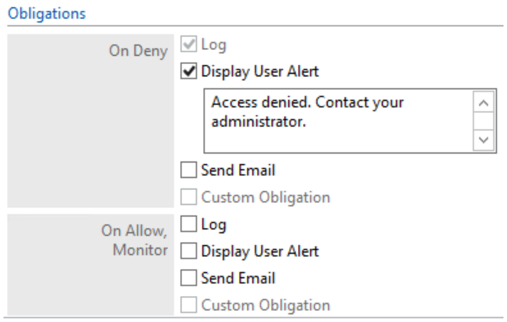
   a. In the On Resources area, click on the **plus sign** box next to **Target**. This automatically populates **in** and **Resource Component**.

   b. In Condition Expression enter the ACPL: **resource.portal.sensitivity > "0"**



Condition Expression: resource.portal.sensitivity > "0"

4. In the Obligations area, check the **Display User Alert** box in order to customize the deny message displayed to the user when access is denied.



Obligations

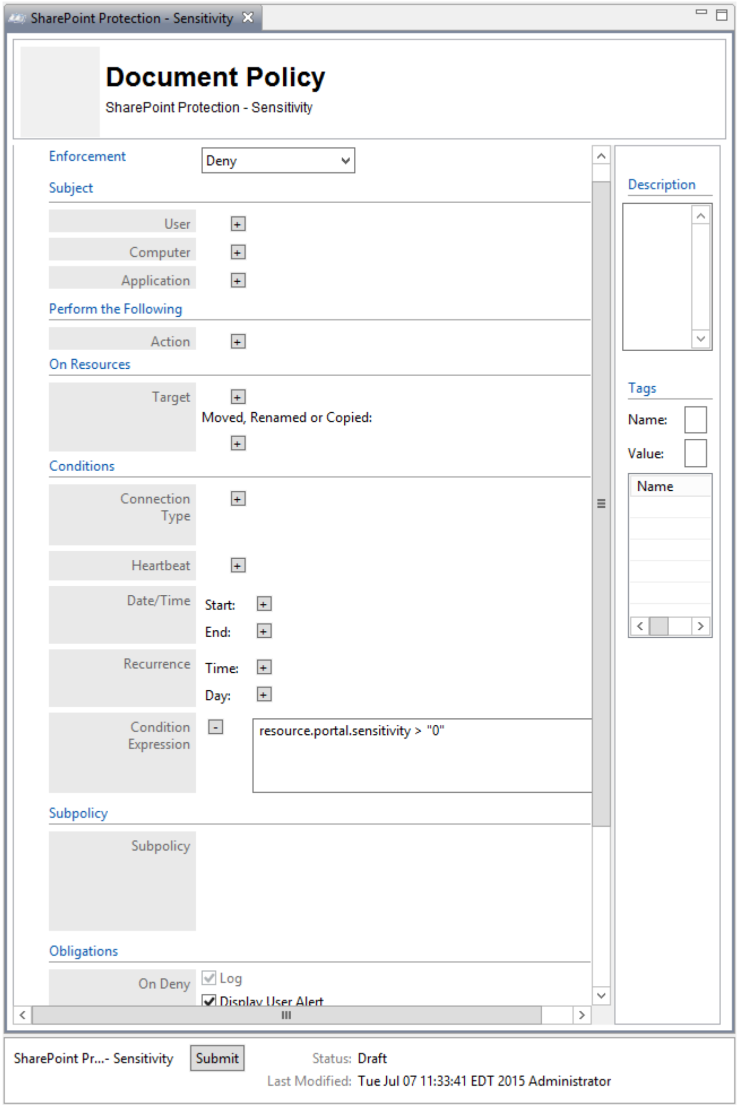
On Deny
☑ Log
☑ Display User Alert

Access denied. Contact your administrator.

□ Send Email
□ Custom Obligation

On Allow, Monitor
□ Log
□ Display User Alert
□ Send Email
□ Custom Obligation

5. In the policy editing panel, your policy should look like this:



SharePoint Protection - Sensitivity

Document Policy

SharePoint Protection - Sensitivity

Enforcement: Deny

Condition Expression: resource.portal.sensitivity > "0"

Obligations

On Deny
☑ Log
☑ Display User Alert

SharePoint Pr...- Sensitivity

Status: Draft

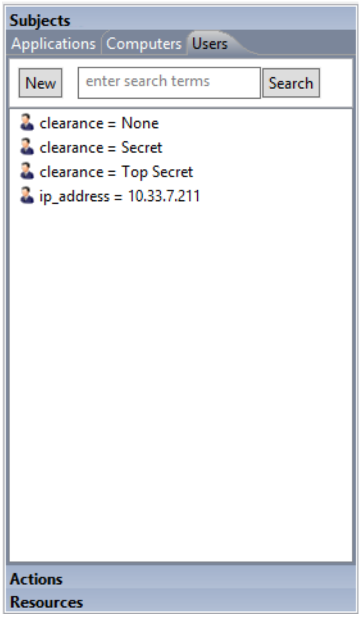
Last Modified: Tue Jul 07 11:33:41 EDT 2015 Administrator

6. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.3.2 Defining a Sensitivity-based Sub-policy that Enforces an Allow Decision when Certain Conditions are Met for Access to Sensitivity Level 1 Documents

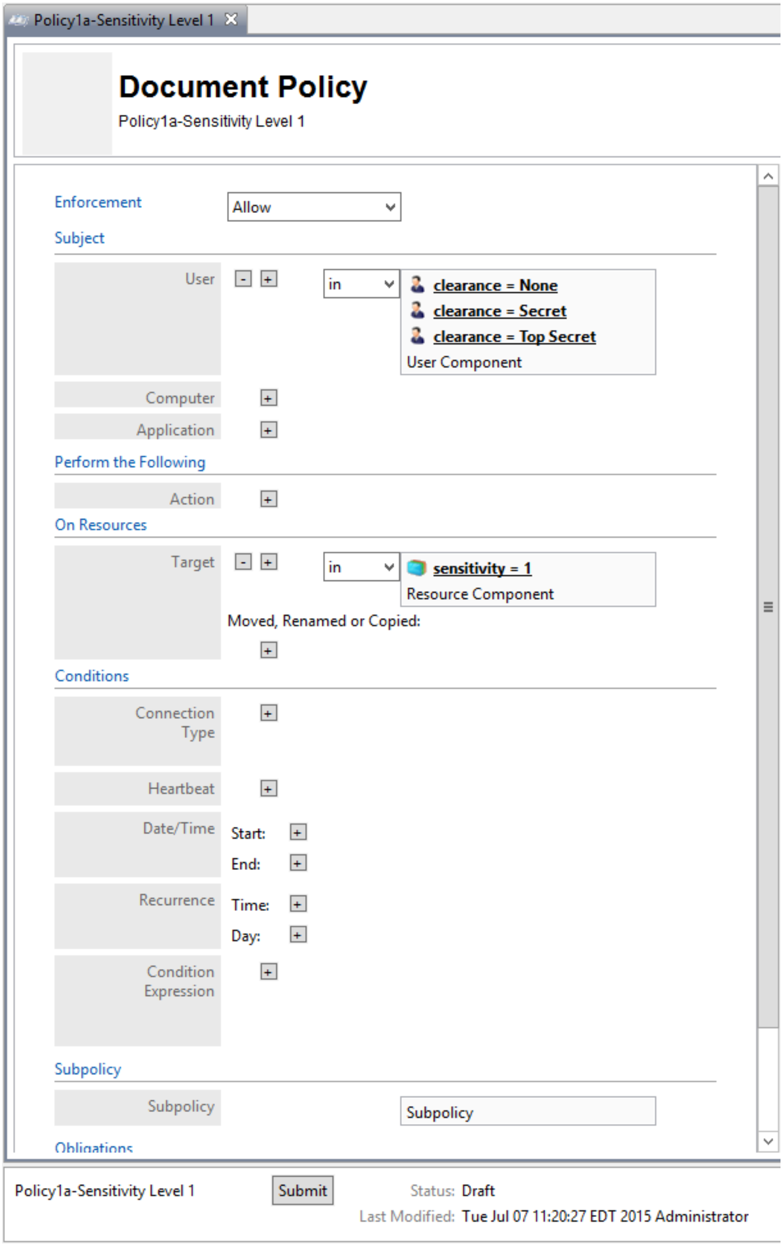
Similar to the steps in section 8.4.4.2.2 for creating the Department-based sub-policy, do the following:

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new policy to highlight it. Then click **New Policy** to create a sub-policy.
2. Select a **name** for the new sub-policy then click **OK**.
3. In the policy editing panel, make the following edits:
    a. From the **Enforcement** drop-down menu, select **Allow**.
    b. In the Subject area, click on the **plus sign** next to User.
        i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Subjects**, then the **Users** tab to see the components you created earlier.



clearance = None
clearance = Secret
clearance = Top Secret
ip_address = 10.33.7.211

        ii. Left-click and hold the **clearance = None** component to drag it onto the **User** field.
        iii. Left-click and hold the **clearance = Secret** component to drag it onto the **User** field.
        iv. Left-click and hold the **clearance = Top Secret** component to drag it onto the **User** field.
    c. In the On Resources area, click on the **plus sign** box next to **Target**.
        i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Resources**, then the **Portals** tab to see the components you created earlier.
        ii. Left-click and hold the **sensitivity = 1** component to drag it onto the **Target** field.
    d. In the policy editing panel, your policy should look like this:



Policy1a-Sensitivity Level 1

Document Policy

Policy1a-Sensitivity Level 1

Enforcement: Allow

Subject

User: in
- clearance = None
- clearance = Secret
- clearance = Top Secret

User Component

Computer

Application

Perform the Following

Action

On Resources

Target: in
- sensitivity = 1

Resource Component

Moved, Renamed or Copied:

Conditions

Connection Type

Heartbeat

Date/Time: Start: End:

Recurrence: Time: Day:

Condition Expression

Subpolicy

Subpolicy: Subpolicy

Obligations

Policy1a-Sensitivity Level 1 Submit Status: Draft

Last Modified: Tue Jul 07 11:20:27 EDT 2015 Administrator

e. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.3.3 Defining a Sensitivity-based Sub-policy that Enforces an Allow Decision when Certain Conditions are Met for Access to Sensitivity Level 2 Documents

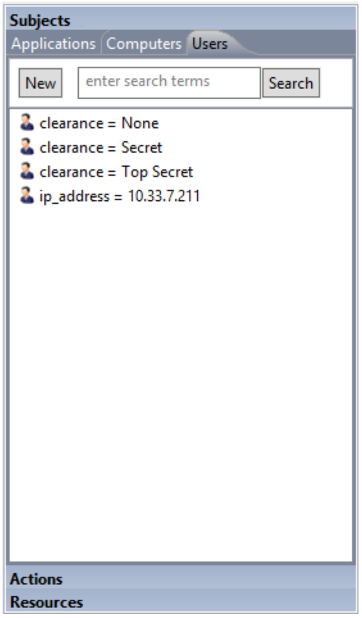
Similar to the steps in section 8.4.4.3.2 for creating the sensitivity-based sub-policy for sensitivity level 1 documents, do the following:

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new policy to highlight it. Then click **New Policy** to create a sub-policy.
2. Select a **name** for the new sub-policy then click **OK**.
3. In the policy editing panel, make the following edits:

a. From the **Enforcement** drop-down menu, select **Allow**.

b. In the Subject area, click on the **plus sign** next to User.

i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Subjects**, then the **Users** tab to see the components you created earlier.



clearance = None
clearance = Secret
clearance = Top Secret
ip_address = 10.33.7.211

ii. Left-click and hold the **clearance = Secret** component to drag it onto the **User** field.

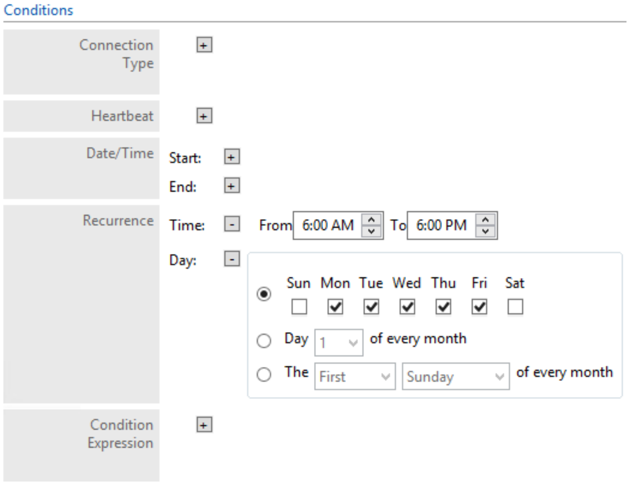
iii. Left-click and hold the **clearance = Top Secret** component to drag it onto the **User** field.

c. In the On Resources area, click on the **plus sign** box next to **Target**.

i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Resources**, then the **Portals** tab to see the components you created earlier.

ii. Left-click and hold the **sensitivity = 2** component to drag it onto the **Target** field.

d. In the Conditions area, click on the **plus sign** boxes next to **Time** and **Day**. Edit those fields to match below:



Conditions

Connection Type ⊞

Heartbeat ⊞

Date/Time Start: ⊞ End: ⊞

Recurrence Time: ⊟ From 6:00 AM To 6:00 PM

Day: ⊟

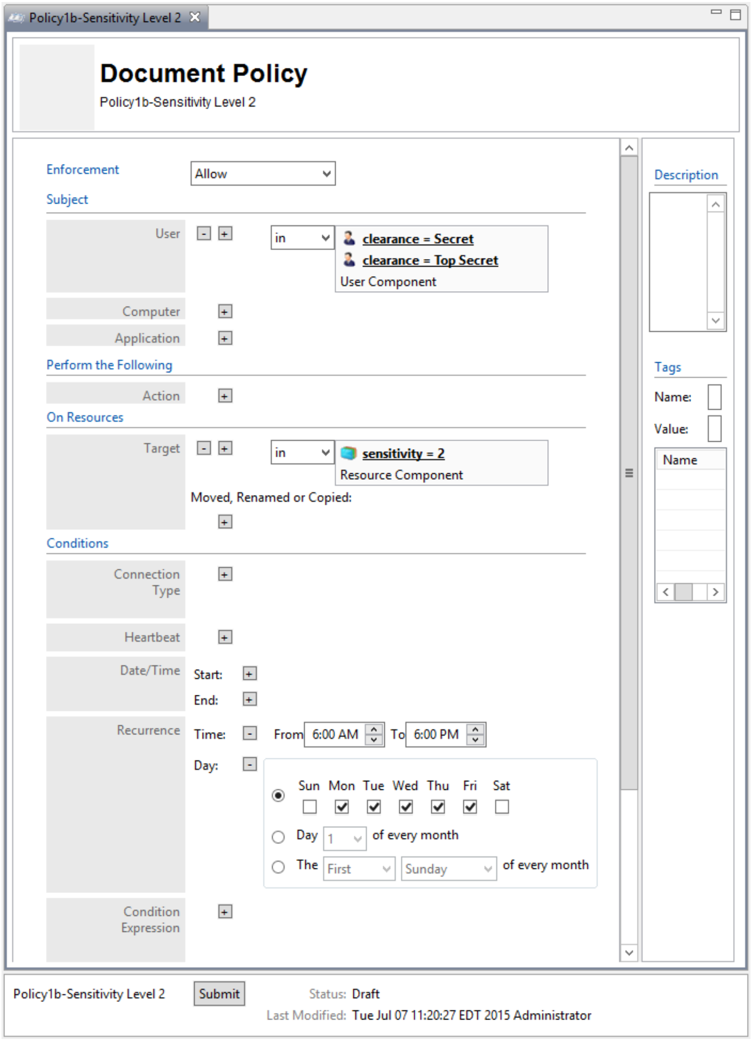
● Sun □ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat □

○ Day 1 of every month

○ The First Sunday of every month

Condition Expression ⊞

4. In the policy editing panel, your policy should look like this:



Policy1b-Sensitivity Level 2

Document Policy

Policy1b-Sensitivity Level 2

Enforcement: Allow

Subject

User ⊟ ⊞ in

clearance = Secret

clearance = Top Secret

User Component

Computer ⊞

Application ⊞

Perform the Following

Action ⊞

On Resources

Target ⊟ ⊞ in

sensitivity = 2

Resource Component

Moved, Renamed or Copied: ⊞

Conditions

Connection Type ⊞

Heartbeat ⊞

Date/Time Start: ⊞ End: ⊞

Recurrence Time: ⊟ From 6:00 AM To 6:00 PM

Day: ⊟

● Sun □ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat □

○ Day 1 of every month

○ The First Sunday of every month

Condition Expression ⊞

Description

Tags

Name:

Value:

Name

Policy1b-Sensitivity Level 2 Submit

Status: Draft

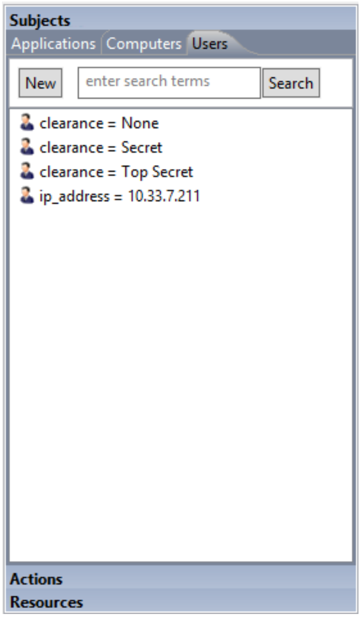
Last Modified: Tue Jul 07 11:20:27 EDT 2015 Administrator

5. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.3.4 Defining a Sensitivity-based Sub-policy that Enforces an Allow Decision when Certain Conditions are Met for Access to Sensitivity Level 3 Documents

Similar to the steps in section 8.4.4.3.2 for creating the sensitivity-based sub-policy for sensitivity level 1 documents, do the following:

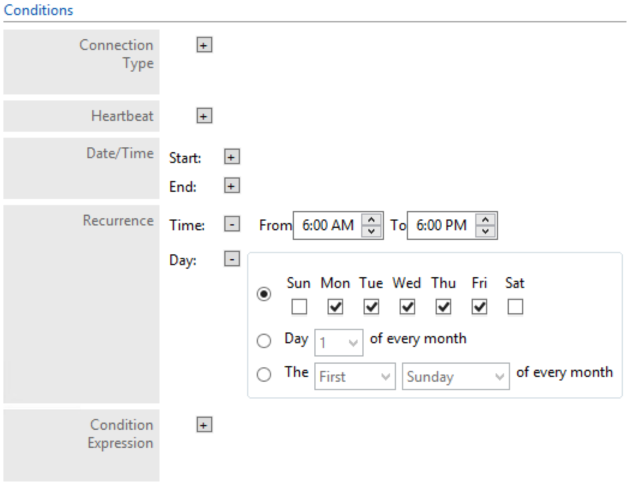
1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new policy to highlight it. Then click **New Policy** to create a sub-policy.
2. Select a **name** for the new sub-policy then click **OK**.
3. In the policy editing panel, make the following edits:
   a. From the **Enforcement** drop-down menu, select **Allow**.
   b. In the Subject area, click on the **plus sign** next to User.
      i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Subjects**, then the **Users** tab to see the components you created earlier.



clearance = None
clearance = Secret
clearance = Top Secret
ip_address = 10.33.7.211

      ii. Left-click and hold the **clearance = Top Secret** component to drag it onto the **User** field.
   c. In the On Resources area, click on the **plus sign** box next to **Target**.
      i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Resources**, then the **Portals** tab to see the components you created earlier.
      ii. Left-click and hold the **sensitivity = 3** component to drag it onto the **Target** field.

d. In the Conditions area, click on the **plus sign** boxes next to **Time** and **Day**. Edit those fields to match below:



Conditions

Connection Type ⊞

Heartbeat ⊞

Date/Time Start: ⊞ End: ⊞

Recurrence Time: ⊟ From 6:00 AM To 6:00 PM

Day: ⊟

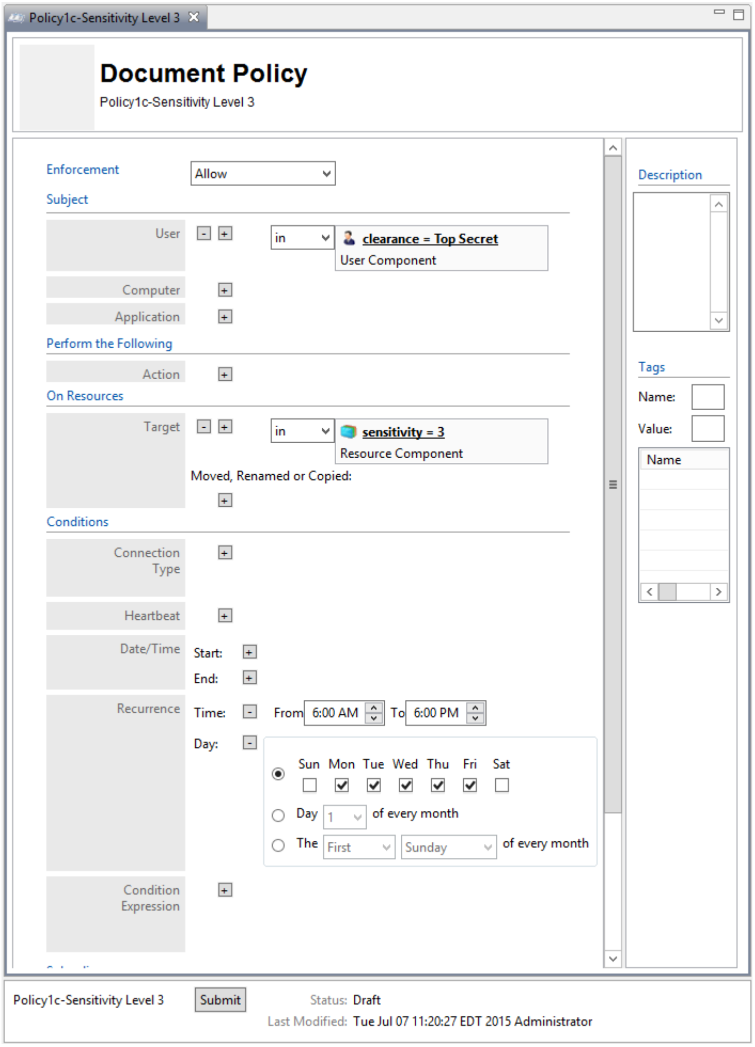
● Sun ☐ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☐

○ Day 1 of every month

○ The First Sunday of every month

Condition Expression ⊞

4. In the policy editing panel, your policy should look like this:



Policy1c-Sensitivity Level 3

Document Policy

Policy1c-Sensitivity Level 3

Enforcement: Allow

Subject

User ⊟ ⊞ in clearance = Top Secret User Component

Computer ⊞

Application ⊞

Perform the Following

Action ⊞

On Resources

Target ⊟ ⊞ in sensitivity = 3 Resource Component

Moved, Renamed or Copied: ⊞

Conditions

Connection Type ⊞

Heartbeat ⊞

Date/Time Start: ⊞ End: ⊞

Recurrence Time: ⊟ From 6:00 AM To 6:00 PM

Day: ⊟

● Sun ☐ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☐

○ Day 1 of every month

○ The First Sunday of every month

Condition Expression ⊞

Description

Tags

Name:

Value:

Name

Policy1c-Sensitivity Level 3 Submit

Status: Draft

Last Modified: Tue Jul 07 11:20:27 EDT 2015 Administrator

5. To deploy this policy, follow the steps in section 8.4.5.

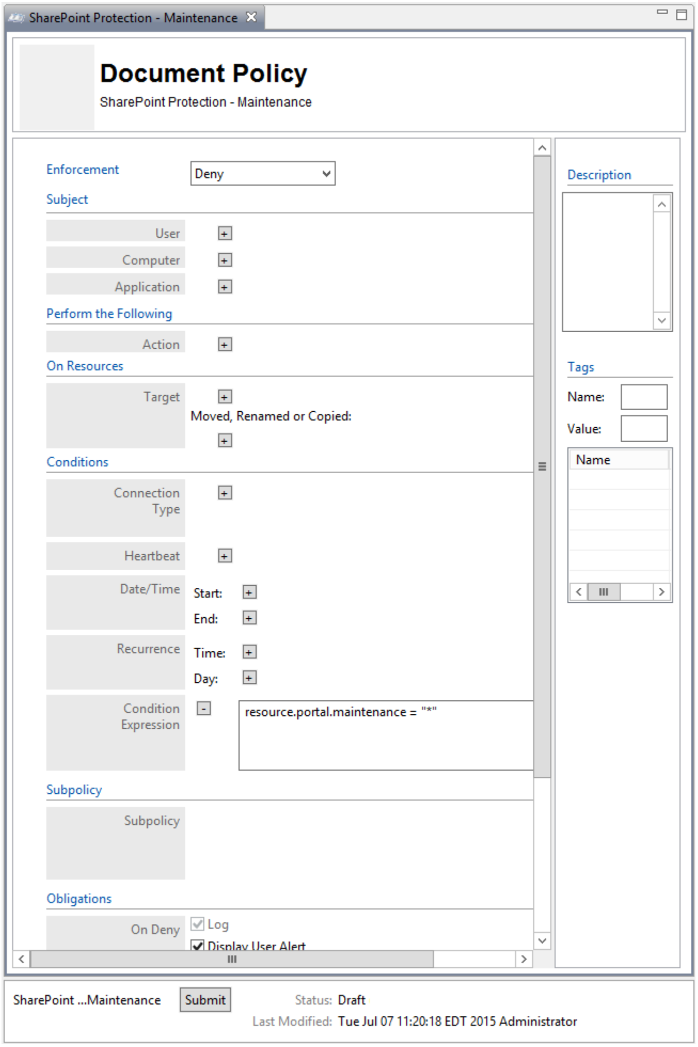
8.4.4.4 Defining a Maintenance-based Policy Set

In order to define a maintenance-based policy set, follow instructions similar to defining the department-based policy set in section 8.4.4.2:

8.4.4.4.1 Defining the Top-level Maintenance Policy that Enforces a General Deny Decision

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**.
2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-down menu, select **Document Policy** (which applies to all SharePoint policies). Click **OK**.
3. The new policy opens automatically in an editing panel. For this policy, keep the default **Deny** enforcement. Make these edits:
    a. In the On Resources area, click on the **plus sign** box next to **Target**. This automatically populates **in** and **Resource Component**.
    b. In **Condition Expression**, enter the ACPL: **resource.portal.maintenance = "*"**
    c. In the Obligations area, check the **Display User Alert** box in order to customize the deny message displayed to the user when access is denied.

4. In the policy editing panel, your policy should look like this:



Enforcement: Deny

Condition Expression: resource.portal.maintenance = "*"

Status: Draft

Last Modified: Tue Jul 07 11:20:18 EDT 2015 Administrator

5. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.4.2 Defining a Maintenance-based Sub-policy that Enforces an Allow Decision when Certain Conditions are Met for Access to Documents whose Maintenance Attribute is defined as Yes

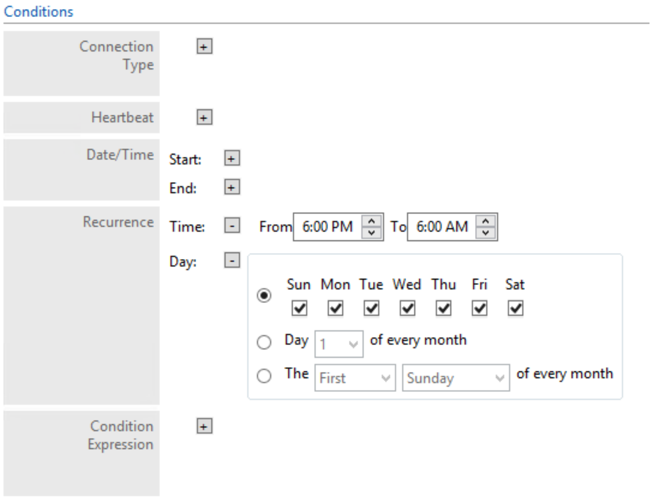
Similar to the instructions in section 8.4.4.2.2 for defining a Department-based sub-policy, do the following:

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new policy to highlight it. Click **New Policy** to create a sub-policy under this main policy.
2. Select a **name** for the new sub-policy, then click **OK**.
3. In the policy editing panel, make the following edits:
   a. From the **Enforcement** drop-down menu, select **Allow**.
   b. In the On Resources area, click on the **plus sign** box next to **Target**.

i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Resources**, then the **Portals** tab to see the components you created earlier.

ii. Left-click and hold the **maintenance = yes** component to drag it onto the **Target** field.

c. In the Conditions area, click on the **plus sign** boxes next to **Time** and **Day**. Edit those fields to match below:



Conditions

Connection Type ⊞

Heartbeat ⊞

Date/Time Start: ⊞ End: ⊞

Recurrence Time: ⊟ From 6:00 PM To 6:00 AM

Day: ⊟

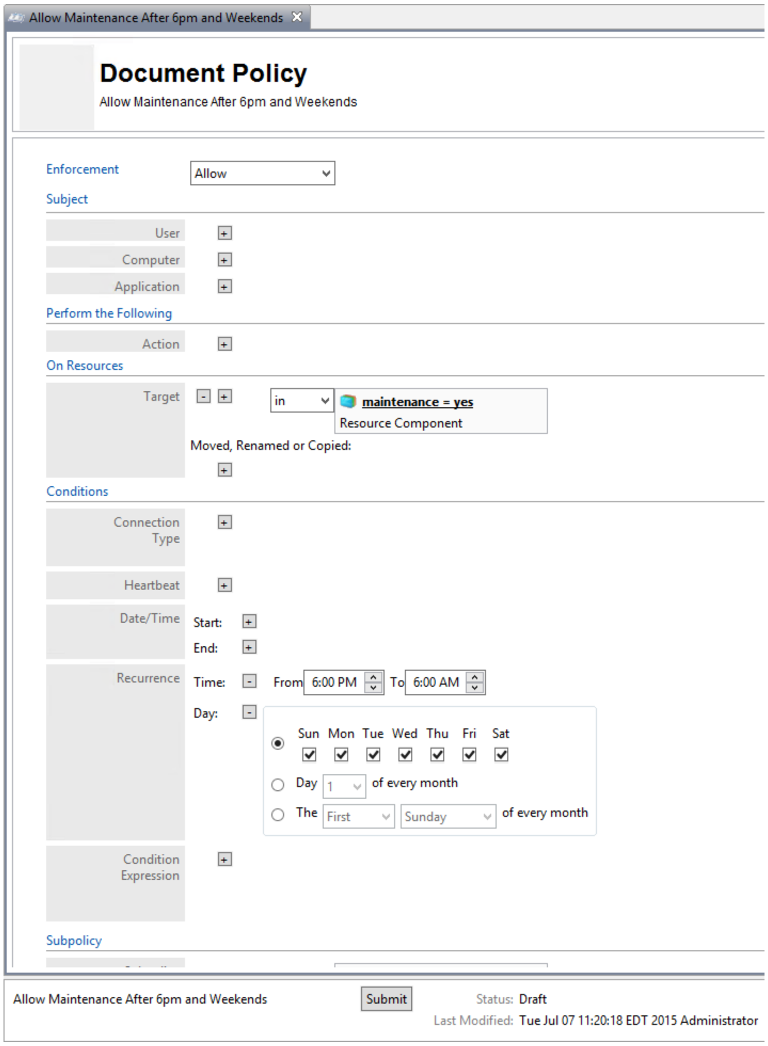
● Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑

○ Day 1 of every month

○ The First Sunday of every month

Condition Expression ⊞

4. In the policy editing panel, your policy should look like this:



Allow Maintenance After 6pm and Weekends

Document Policy

Allow Maintenance After 6pm and Weekends

Enforcement: Allow

Subject

User ⊞

Computer ⊞

Application ⊞

Perform the Following

Action ⊞

On Resources

Target ⊟ ⊞ in — maintenance = yes (Resource Component)

Moved, Renamed or Copied: ⊞

Conditions

Connection Type ⊞

Heartbeat ⊞

Date/Time — Start: ⊞ End: ⊞

Recurrence — Time: ⊟ From 6:00 PM To 6:00 AM

Day: ⊟

● Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat ☑

○ 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

5. To deploy this policy, follow the steps in section 8.4.5.

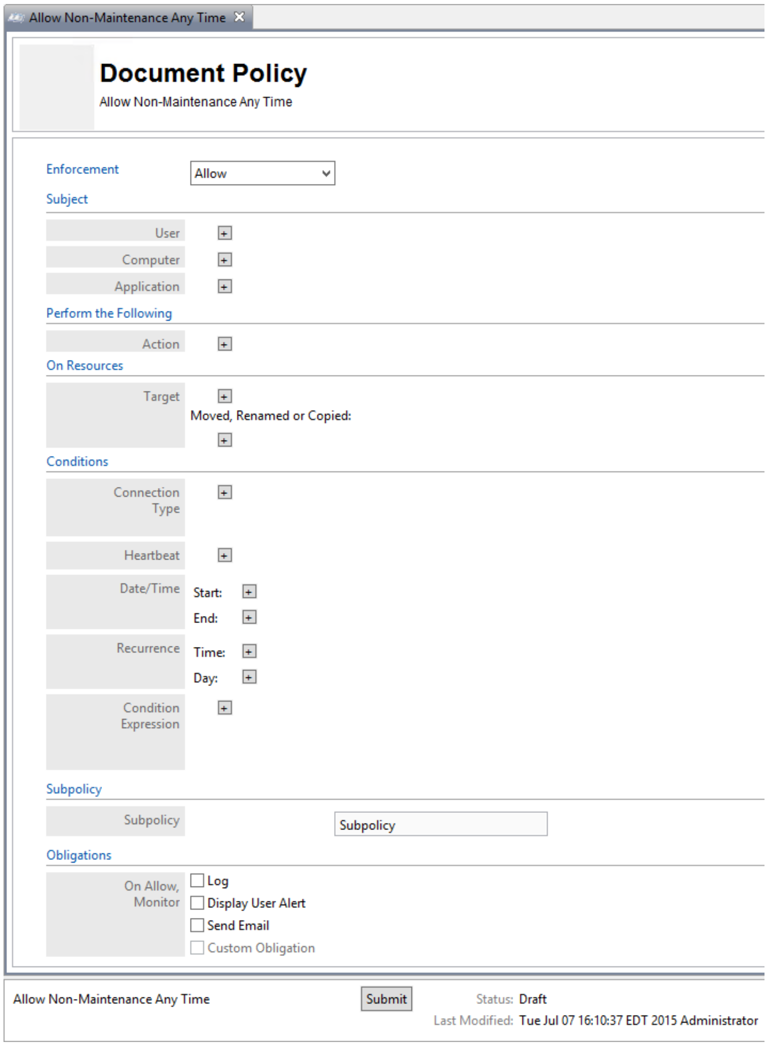
8.4.4.4.3 Defining a Maintenance-based Sub-policy that Enforces an Allow Decision when Certain Conditions are Met for Access to Documents whose Maintenance Attribute is defined as No

Similar to the instructions in section 8.4.4.2.2 for defining a Department-based sub-policy, do the following:

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new policy to highlight it. Click **New Policy** to create a sub-policy.
2. Select a **name** for the new sub-policy, then click **OK**.
3. In the policy editing panel, make the following edits:
    a. From the **Enforcement** drop-down menu, select **Allow**.
    b. In the On Resources area, click on the **plus sign** box next to **Target**.
        i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Resources**, then the **Portals** tab to see the components you created earlier.

   ii. Left-click and hold the **maintenance = no** component to drag it onto the **Target** field.

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: Allow

Allow Non-Maintenance Any Time

Status: Draft

Last Modified: Tue Jul 07 16:10:37 EDT 2015 Administrator

5. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.5 Defining an IP Address-based Policy Set

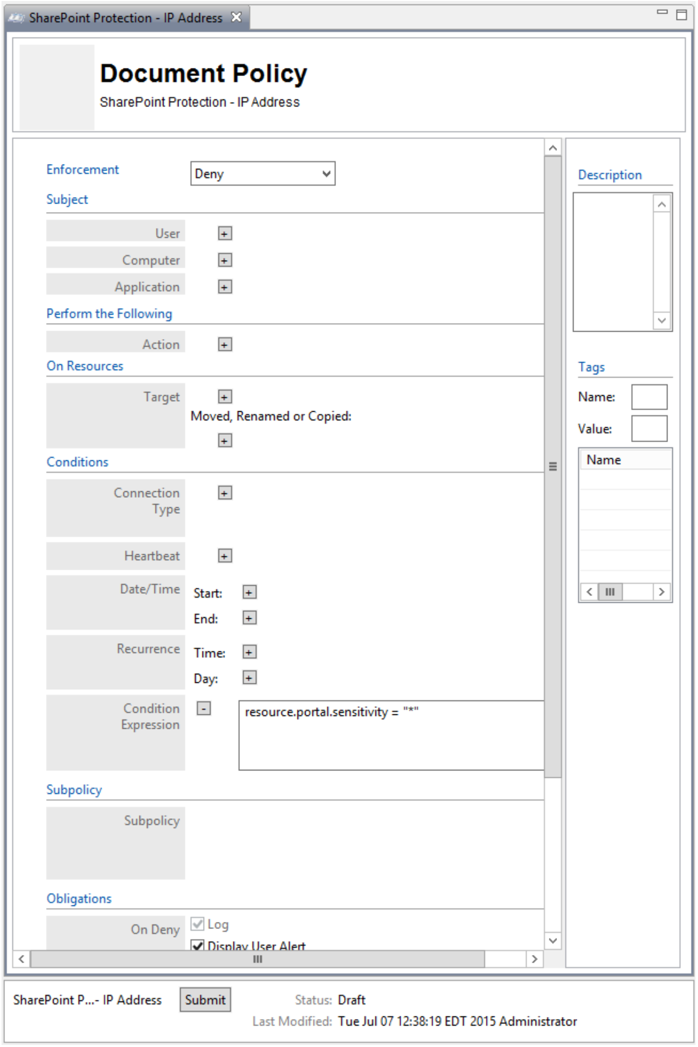
In order to define an IP address-based policy set, follow instructions similar to defining the department-based policy set in section 8.4.4.2:

8.4.4.5.1 Defining the top-level IP Address Policy that Enforces a General Deny Decision

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**.

2. In the Create New Policy window, enter a **name** for the new policy. From the **Policy Type** drop-down menu, select **Document Policy** (which applies to all SharePoint policies). Click **OK**.

3. The new policy opens automatically in an editing panel. For this policy, keep the default **Deny** enforcement. Make these edits:
    a. In the **Condition Expression**, enter the ACPL: **resource.portal.sensitivity = "*"**
    b. In the Obligations area, check the **Display User Alert** box in order to customize the deny message displayed to the user when access is denied.
4. In the policy editing panel, your policy should look like this:



SharePoint Protection - IP Address

Document Policy

SharePoint Protection - IP Address

Enforcement: Deny

Target: Moved, Renamed or Copied:

Condition Expression: resource.portal.sensitivity = "*"

On Deny: ☑ Log ☑ Display User Alert

SharePoint P...- IP Address Submit Status: Draft

Last Modified: Tue Jul 07 12:38:19 EDT 2015 Administrator

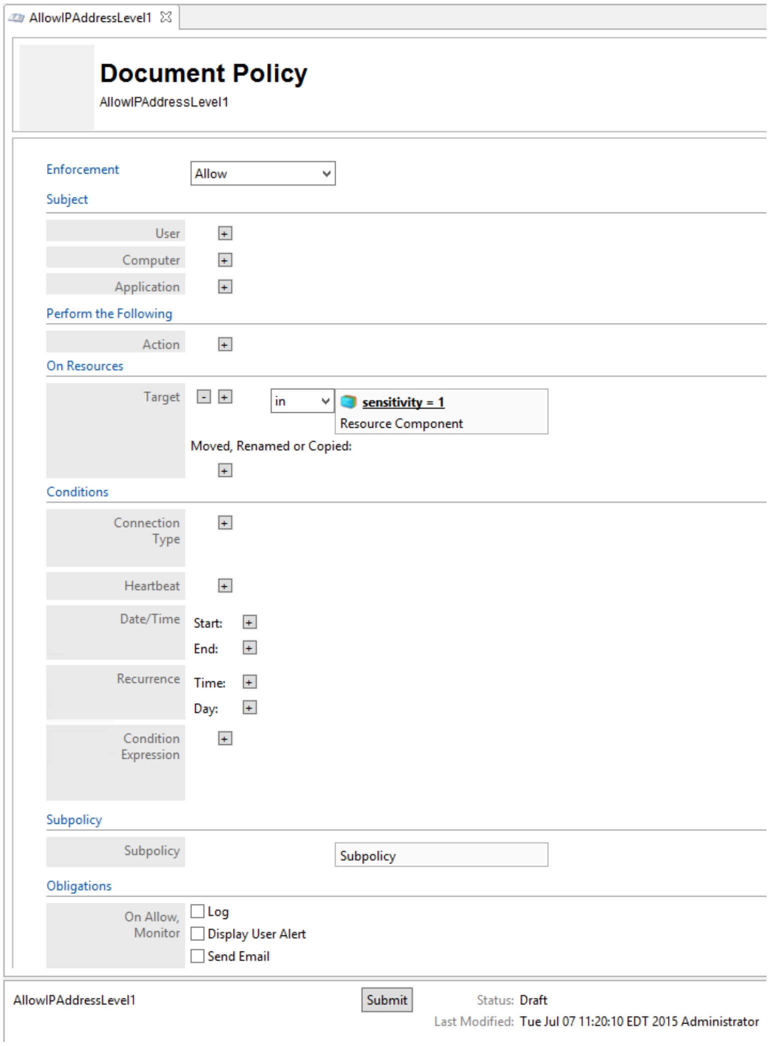
5. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.5.2 Defining an IP Address-based Sub-policy that Enforces an Allow Decision for Access to Resources at any Sensitivity Level when a User Does not Come from an Environment with a Restricted IP Address (ex: 10.33.7.211)

Similar to the instructions in section 8.4.4.2.2 for defining a Department-based sub-policy, do the following:

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new policy to highlight it. Click **New Policy** to create a sub-policy.

2. Select a **name** for the new sub-policy, then click **OK**.
3. In the policy editing panel, make the following edits:
   a. From the **Enforcement** drop-down menu, select **Allow**.
   b. In the On Resources area, click on the **plus sign** box next to **Target**.
      i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Resources**, then the **Portals** tab to see the components you created earlier.
      ii. Left-click and hold the **sensitivity = 1** component to drag it onto the **Target** field.
4. In the policy editing panel, your policy should look like this:



AllowIPAddressLevel1

Document Policy

AllowIPAddressLevel1

Enforcement: Allow

Subject

User ⊞
Computer ⊞
Application ⊞

Perform the Following

Action ⊞

On Resources

Target ⊟ ⊞ in sensitivity = 1 Resource Component

Moved, Renamed or Copied: ⊞

Conditions

Connection Type ⊞
Heartbeat ⊞
Date/Time Start: ⊞ End: ⊞
Recurrence Time: ⊞ Day: ⊞
Condition Expression ⊞

Subpolicy

Subpolicy: Subpolicy

Obligations

On Allow, Monitor
□ Log
□ Display User Alert
□ Send Email

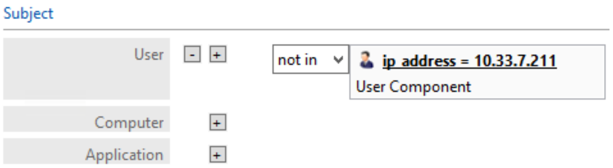
AllowIPAddressLevel1 Submit Status: Draft
Last Modified: Tue Jul 07 11:20:10 EDT 2015 Administrator

5. To deploy this policy, follow the steps in section 8.4.5.

8.4.4.5.3 Defining an IP Address-based Sub-policy that Enforces an Allow Decision for Access to Resources at Only Sensitivity Level 1 when a User Comes from an Environment with a Restricted IP Address (ex: 10.33.7.211)

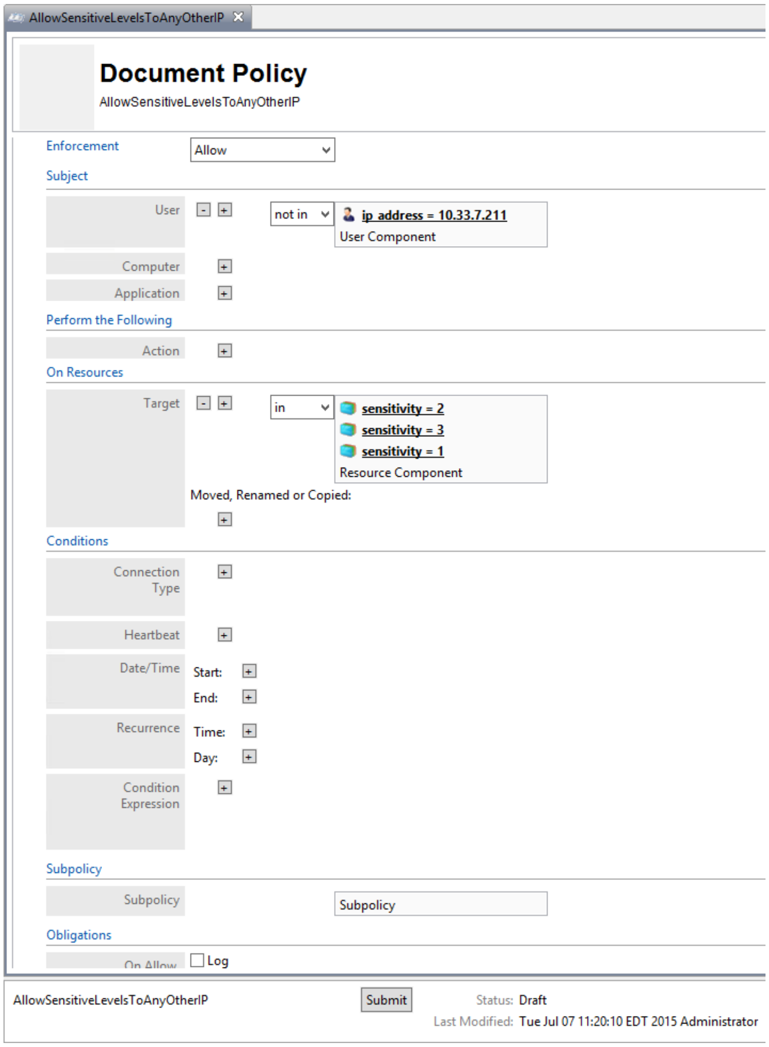
Similar to the instructions in section 8.4.4.2.2 for defining a Department-based sub-policy, do the following:

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on your new policy to highlight it. Then click **New Policy** to create a sub-policy.
2. Select a **name** for the new sub-policy, then click **OK**.
3. In the policy editing panel, make the following edits:
    a. From the **Enforcement** drop-down menu, select **Allow**.
    b. In the Subject area, click on the **plus sign** box next to **User**.
        i. From the drop-down menu, select **not in**.
        ii. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Subjects**, then the **Users** tab to see the components you created earlier.
        iii. Left-click and hold the **ip_address=10.33.7.211** component to drag it onto the **User** field.



    c. In the On Resources area, click on the **plus sign** box next to **Target**.
        i. In the Components panel in the bottom-left corner of the Policy Studio window, click on **Resources**, then the **Portals** tab to see the components you created earlier.
        ii. Left-click and hold the **sensitivity = 1** component to drag it onto the **Target** field.
        iii. Left-click and hold the **sensitivity = 2** component to drag it onto the **Target** field.
        iv. Left-click and hold the **sensitivity = 3** component to drag it onto the **Target** field.

4. In the policy editing panel, your policy should look like this:



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

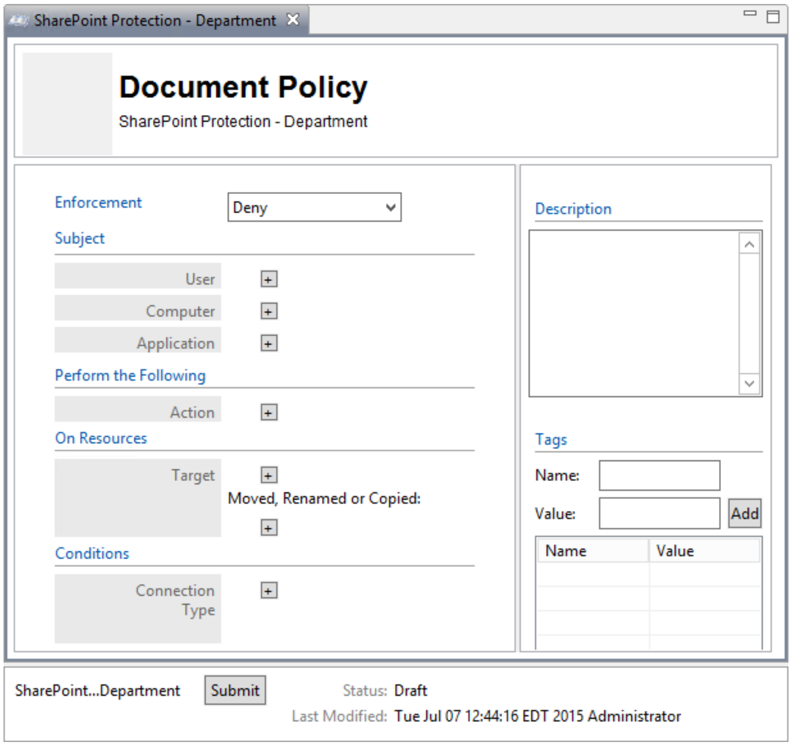
AllowSensitiveLevelsToAnyOtherIP — Submit — Status: Draft — Last Modified: Tue Jul 07 11:20:10 EDT 2015 Administrator

5. To deploy this policy, follow the steps in section 8.4.5.

8.4.5 Deploying Policy

In order to deploy policies, follow steps similar to those for deploying a component (see the section Clearance = None):

1. In the Policies panel in the top-left corner of the main Policy Studio window, click on the policy you want to deploy. In the policy editing panel, click **Submit**.



SharePoint Protection - Department

Document Policy

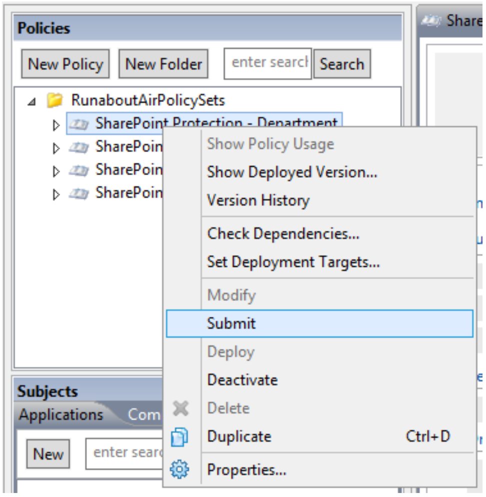
SharePoint Protection - Department

Enforcement: Deny

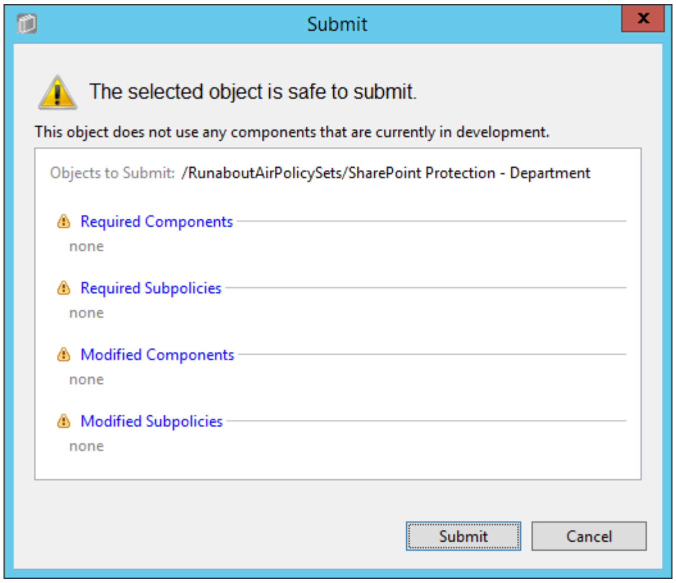
Status: Draft

Last Modified: Tue Jul 07 12:44:16 EDT 2015 Administrator

   a. Or, in the Policies panel in the top-left corner of the main Policy Studio window, right-click the policy you want to deploy. Select **Submit** from the floating menu.



2. In the Submit window, click **Submit**.



The selected object is safe to submit.

This object does not use any components that are currently in development.

Objects to Submit: /RunaboutAirPolicySets/SharePoint Protection - Department

Required Components
none

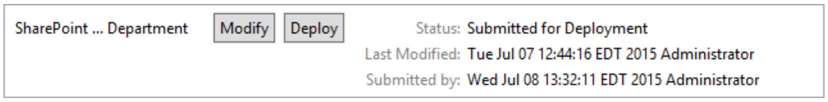
Required Subpolicies
none

Modified Components
none

Modified Subpolicies
none

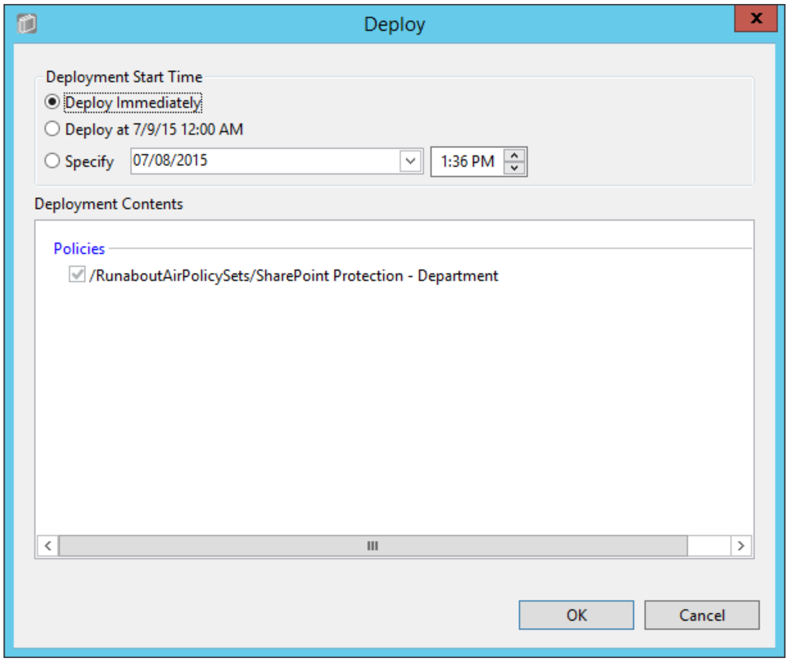
3. From the component editing panel, note the differences. The new status reads **Submitted for Deployment**. Click **Deploy**.

   a. Or, in the Policies panel in the top-left corner of the main Policy Studio window, right-click the policy you want to deploy. Select **Deploy** from the floating menu.



Status: Submitted for Deployment
Last Modified: Tue Jul 07 12:44:16 EDT 2015 Administrator
Submitted by: Wed Jul 08 13:32:11 EDT 2015 Administrator

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.



Deploy

Deployment Start Time

● Deploy Immediately

○ Deploy at 7/9/15 12:00 AM

○ Specify 07/08/2015 1:36 PM

Deployment Contents

Policies

☑ /RunaboutAirPolicySets/SharePoint Protection - Department

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 chapter 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.

8.4.6 Modifying and Re-Deploying Policies and Components

In order to modify existing policies and re-deploy them, do the following:

8.4.6.1 Modifying and Deploying Existing Policies

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**.
3. Follow the deploy instructions from section 8.4.5 to deploy the modified policy.

8.4.6.2 Modifying and Deploying Existing Components

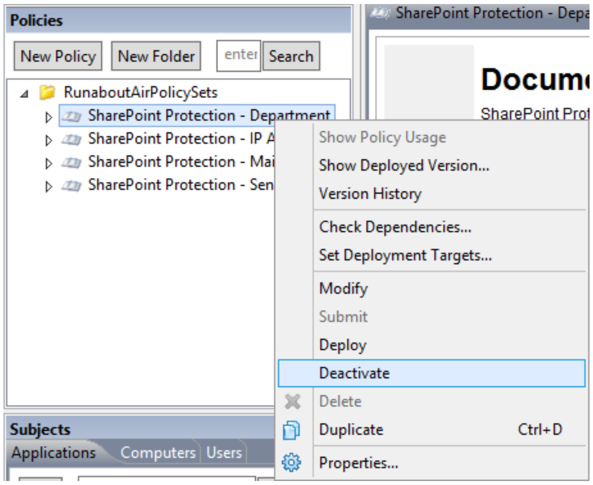
1. In the Components panel in the bottom-left corner of the main Policy Studio window, click on the component you want to modify. In the policy editing panel, click **Modify**.
   a. Or, right-click the component you want to modify and select **Modify** from the floating menu.

2. In the component editing panel, make the desired changes and click **Submit**.
3. Follow the deploy instructions from section 8.4.5 to deploy the modified component.

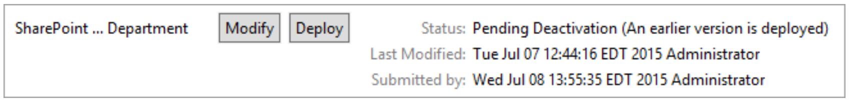
8.4.7 Deactivating Policies and Components

8.4.7.1 Deactivating Policies

1. In the Policies panel in the top-left corner of the main Policy Studio window, right-click the policy you want to deactivate. Select **Deactivate** from the floating menu.

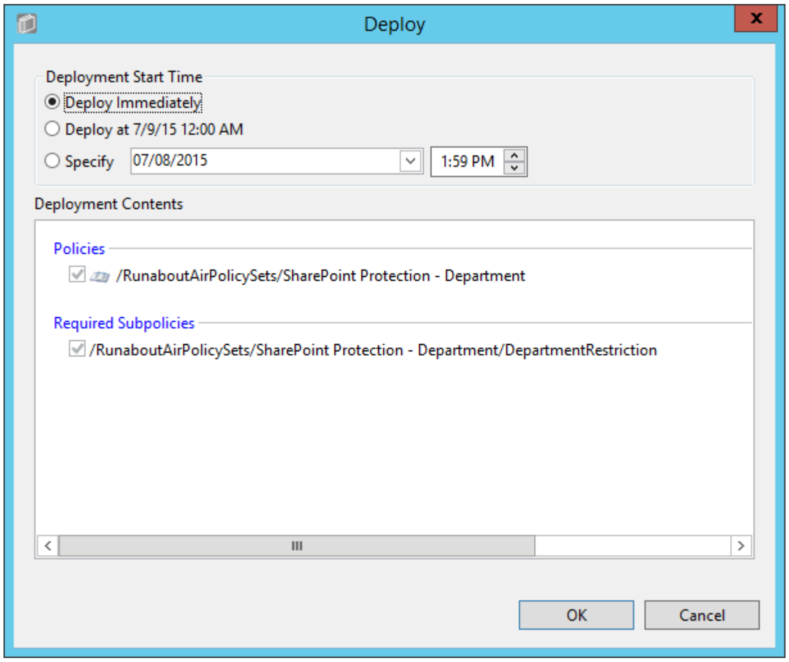


2. At the bottom of the policy editing panel, note the change in **Status** to **Pending Deactivation**. Click **Deploy**.



Status: Pending Deactivation (An earlier version is deployed)
Last Modified: Tue Jul 07 12:44:16 EDT 2015 Administrator
Submitted by: Wed Jul 08 13:55:35 EDT 2015 Administrator

3. In the Deploy window, click **OK**. Note: You may specify to deploy immediately, which we choose in our example. You may also deploy the following day at midnight, or at a different specific date and time.



Deployment Start Time

● Deploy Immediately

○ Deploy at 7/9/15 12:00 AM

○ Specify 07/08/2015 1:59 PM

Deployment Contents

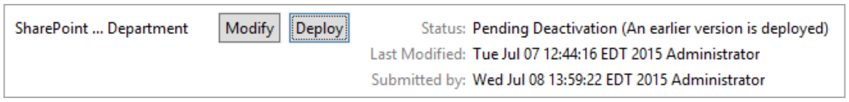
Policies

☑ /RunaboutAirPolicySets/SharePoint Protection - Department

Required Subpolicies

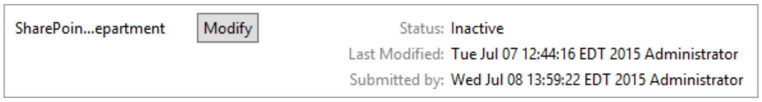
☑ /RunaboutAirPolicySets/SharePoint Protection - Department/DepartmentRestriction

4. Verify at the bottom of the policy editing panel that the **Status** is now **Pending Deactivation**. This will remain for the duration of the heartbeat (described in chapter 7).



Status: Pending Deactivation (An earlier version is deployed)
Last Modified: Tue Jul 07 12:44:16 EDT 2015 Administrator
Submitted by: Wed Jul 08 13:59:22 EDT 2015 Administrator

5. After the duration of the heartbeat has passed, **Status** should read as **Inactive**. This indicates that the component is currently inactive in your ABAC system.



Status: Inactive
Last Modified: Tue Jul 07 12:44:16 EDT 2015 Administrator
Submitted by: Wed Jul 08 13:59:22 EDT 2015 Administrator

8.4.7.2 Deactivating Components

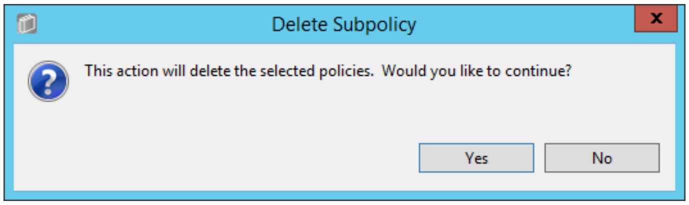
1. In the Components panel in the bottom-left corner of the main Policy Studio window, right-click on the component you want to deactivate. Select **Deactivate** from the floating menu.
2. Follow steps 2-5 in section 8.4.7.1 for deactivating policies.

8.4.8 Deleting Policies and Components

Note: To delete a policy or component, you must first deactivate the item and any related sub-items.

8.4.8.1 Deleting Policies

1. In the Policies panel in the top-left corner of the main Policy Studio window, right-click on the policy you want to delete. Select **Delete** from the floating menu.
2. In the Delete window, click **Yes**.



Delete Subpolicy

This action will delete the selected policies. Would you like to continue?

8.4.8.2 Deleting Components

1. In the Components panel in the bottom-left corner of the main Policy Studio window, right-click on the policy you want to delete. Select **Delete** from the floating menu.

8.5 Configuring Attributes in NextLabs

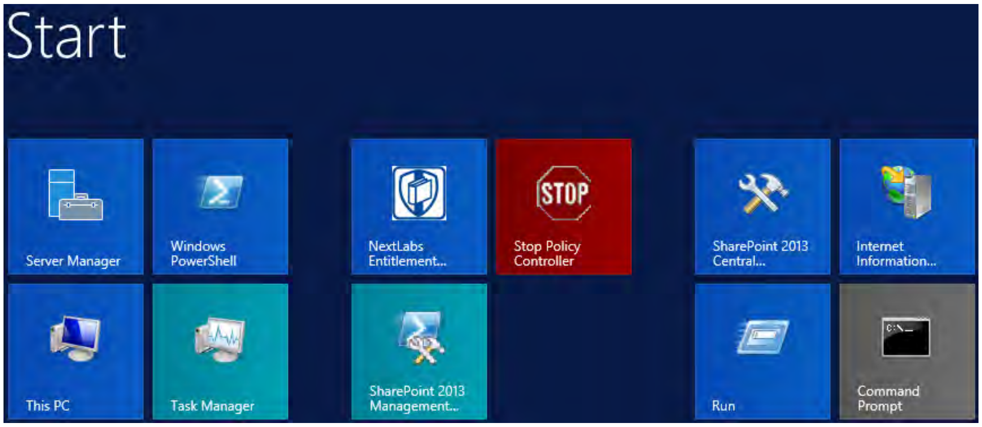
Chapter 6 illustrates how to configure the attribute flow between several of the servers and components in the ABAC architecture. Note that the NextLabs Entitlement Manager was installed on the SharePoint Server, which is where all of the activity in section 8.5 occurs.

In order to configure NextLabs to enforce policy on all of the attributes coming from the front-channel as SharePoint Claims, you must first stop the NextLabs Policy Controller service, edit the configuration.xml file in the SharePoint Enforcer software architecture, restart Internet Information Services (IIS), then restart the NextLabs Policy Controller service using the following instructions.

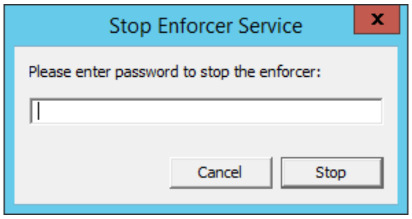
8.5.1 Stopping the NextLabs Policy Controller Service

1. On the SharePoint Server, click the Windows icon and begin typing the word **Services**.
2. Double-click on the icon to open the Services application.
3. Within the Services application window, in the list of services, click on the **Name** column to sort by alphabetical order, and look for **Control Center Enforcer Service**.
4. If the **status** of the Control Center Enforcer Service is **Running**, stop it.
    a. Click the Windows icon.

b. Double-click the **Stop Policy Controller** shortcut icon.

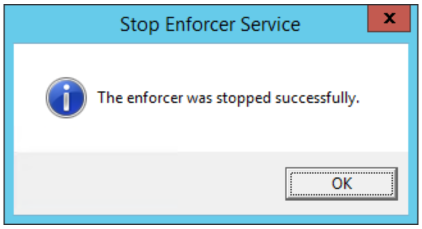


c. Enter your NextLabs Administrator credentials. Then click **Stop**.


Stop Enforcer Service

Please enter password to stop the enforcer:

d. In the Stop Enforcer Service success window, click **OK**.

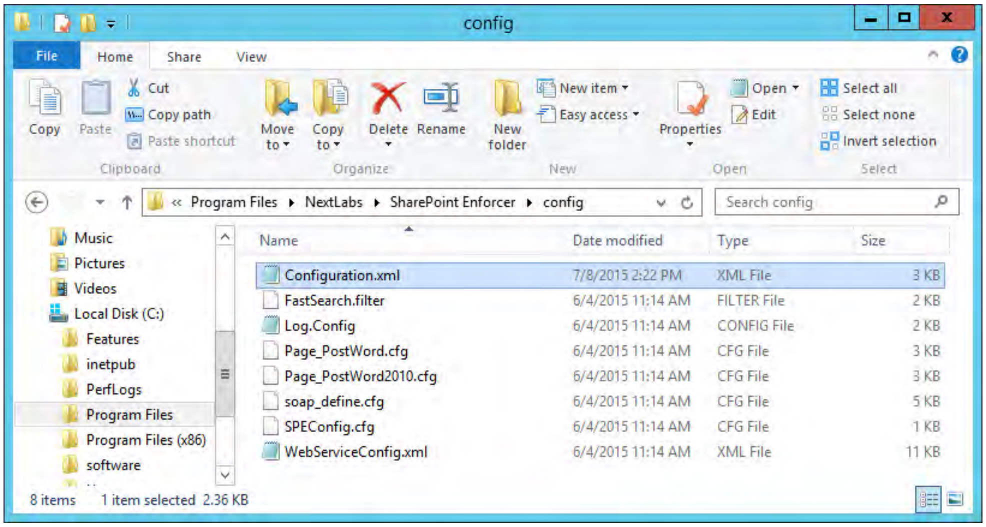

Stop Enforcer Service

The enforcer was stopped successfully.

8.5.2 Editing the Configuration File

8.5.2.1 Locating and Opening the SharePoint Enforcer configuration.xml File

1. In Windows Explorer, find and open the SharePoint Enforcer configuration.xml file.
    a. Double-click the **C:/** drive.
    b. Double-click **Program Files**.
    c. Double-click **NextLabs**.
    d. Double-click **SharePoint Enforcer**.
    e. Double-click **config**.
    f. Right-click **Configuration.xml** to edit the file in a text editor.



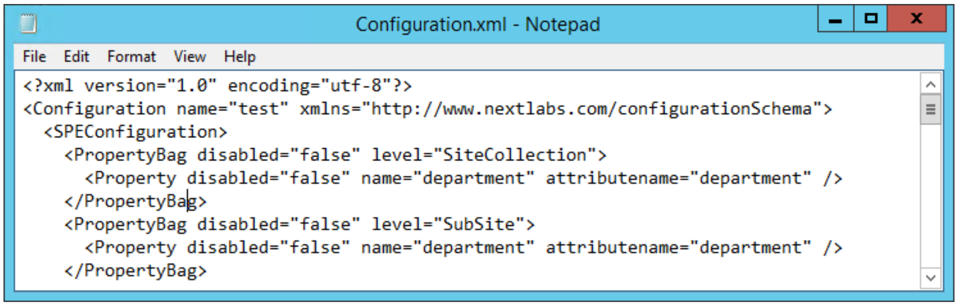
Name	Date modified	Type	Size
Configuration.xml	7/8/2015 2:22 PM	XML File	3 KB
FastSearch.filter	6/4/2015 11:14 AM	FILTER File	2 KB
Log.Config	6/4/2015 11:14 AM	CONFIG File	2 KB
Page_PostWord.cfg	6/4/2015 11:14 AM	CFG File	3 KB
Page_PostWord2010.cfg	6/4/2015 11:14 AM	CFG File	3 KB
soap_define.cfg	6/4/2015 11:14 AM	CFG File	5 KB
SPEConfig.cfg	6/4/2015 11:14 AM	CFG File	1 KB
WebServiceConfig.xml	6/4/2015 11:14 AM	XML File	11 KB

8.5.2.2 Configuring Resource Attributes from SharePoint Metadata

1. Within the **configuration.xml** file, look for the **<SPEConfiguration>** tag.
2. Under that tag, but above a **<User Attribute>** tag, insert tags for each site-level or sub-site level resource attribute of interest.
    a. For example, in our build we created policies based on the **department** resource attribute, so in our configuration.xml file we included the following:

```
<PropertyBag disabled="false" level="SiteCollection">
<Property disabled="false" name="department"
attributename="department" />
</PropertyBag>
<PropertyBag disabled="false" level="SubSite">
<Property disabled="false" name="department"
attributename="department" />
</PropertyBag>
```

    b. From the example above, the top of the **configuration.xml** file looks like this:

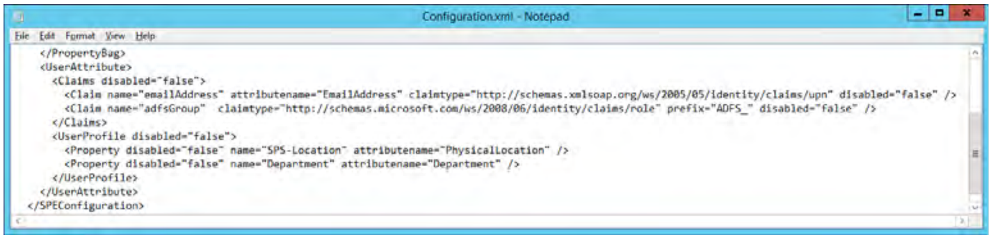


```
<?xml version="1.0" encoding="utf-8"?>
<Configuration name="test" xmlns="http://www.nextlabs.com/configurationSchema">
  <SPEConfiguration>
    <PropertyBag disabled="false" level="SiteCollection">
      <Property disabled="false" name="department" attributename="department" />
    </PropertyBag>
    <PropertyBag disabled="false" level="SubSite">
      <Property disabled="false" name="department" attributename="department" />
    </PropertyBag>
```

8.5.2.3 Configuring User Attributes from SharePoint Claims

1. Within the **configuration.xml** file directly under any **<PropertyBag>** closing tags, find the **<User Attribute> </User Attribute>** portion of the document. Initially, its default contents

in that area may look like this, containing some default user attributes such as **"emailAddress"** or **"adfsGroup"**:



```
    </PropertyBag>
    <UserAttribute>
      <Claims disabled="false">
        <Claim name="emailAddress" attributename="EmailAddress" claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" disabled="false" />
        <Claim name="adfsGroup"  claimtype="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" prefix="ADFS_" disabled="false" />
      </Claims>
      <UserProfile disabled="false">
        <Property disabled="false" name="SPS-Location" attributename="PhysicalLocation" />
        <Property disabled="false" name="Department" attributename="Department" />
      </UserProfile>
    </UserAttribute>
  </SPEConfiguration>
```

2. In the **User Attribute** area, add more claims here to include all the attributes you will be expecting to evaluate in NextLabs policies for access control decisions.

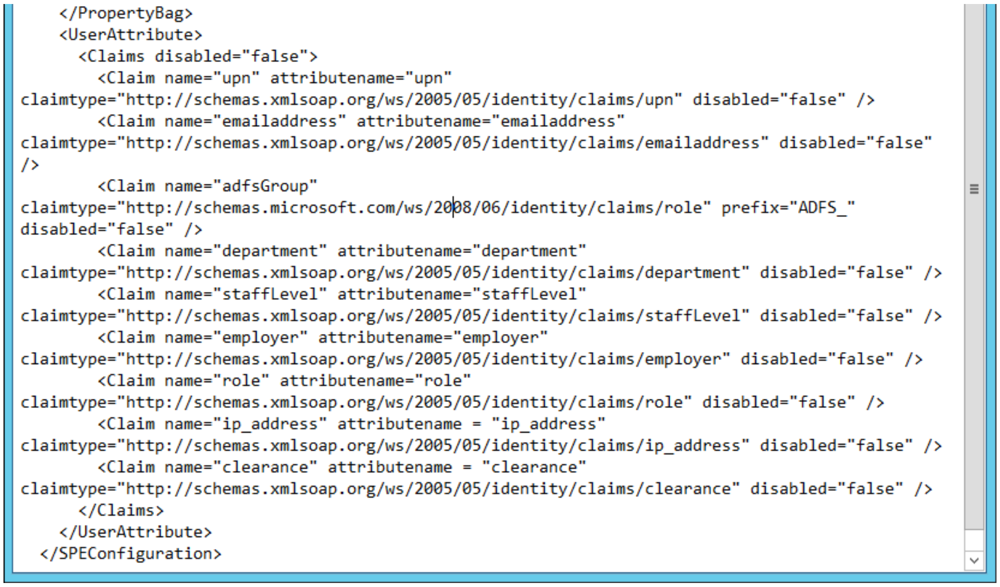
   a. For example, in our build we created policies based on users' **"clearance"**, **"department"**, and **"ip_address"**, so in our **configuration.xml** file we included the following, among others:

   ```
   <Claim name="department" attributename="department"
   claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims
   /department" disabled="false" />
   ```

   ```
   <Claim name="ip_address" attributename = "ip_address"
   claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims
   /ip_address" disabled="false" />
   ```

   ```
   <Claim name="clearance" attributename = "clearance"
   claimtype="http://schemas.xmlsoap.org/ws/2005/05/identity/claims
   /clearance" disabled="false" />
   ```

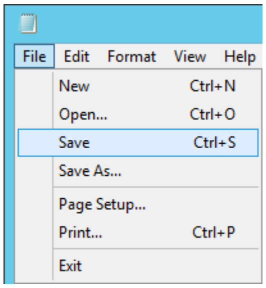
   b. From the example above, the rest of our **configuration.xml** file looks like this:



```
    </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>
```

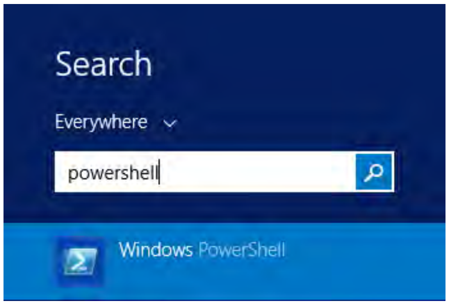
8.5.2.4 Saving Changes to the Configuration File

1. From the File menu, click **Save**, or Ctrl+S on your keyboard.

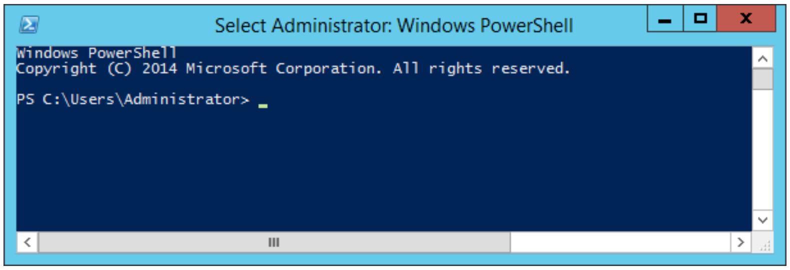


8.5.3 Restarting IIS via Windows PowerShell

1. Click the Windows icon.
2. In the Search text box, begin typing **PowerShell**.

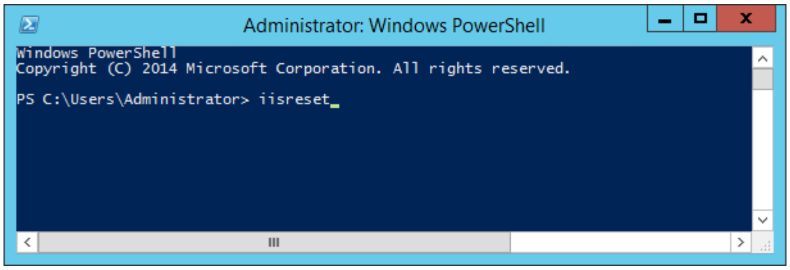


3. Click on **Windows PowerShell**.



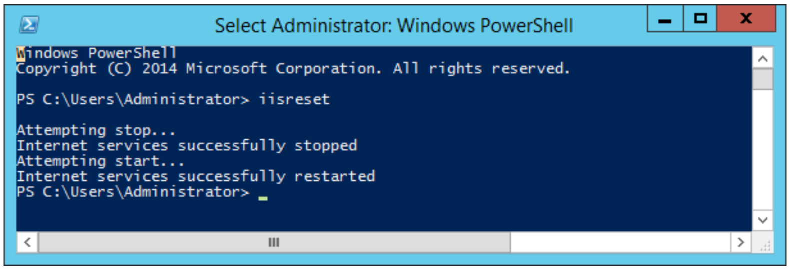
```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> _
```

4. In the PowerShell window, type the command: **iisreset**. Press **Enter**.



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> iisreset_
```

5. In the PowerShell window, verify that services stopped and restarted successfully.



```
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> _
```

8.5.4 Restarting the NextLabs Policy Controller Service

1. Click on the Windows icon and begin typing the word **Services**.
2. Double-click the **Services** icon to open the application.
3. Within the Services application window in the list of services, click on the **Name** column to sort by alphabetical order and look for **Control Center Enforcer Service**.
4. Right-click **Control Center Enforcer Service** and click **Start**.
   a. It may be necessary to click the **Refresh** icon in order to see the **Control Center Enforcer Service** status change to **Running**.

8.6 Functional Test

8.6.1 Updated bin file after Policy Creation/modification

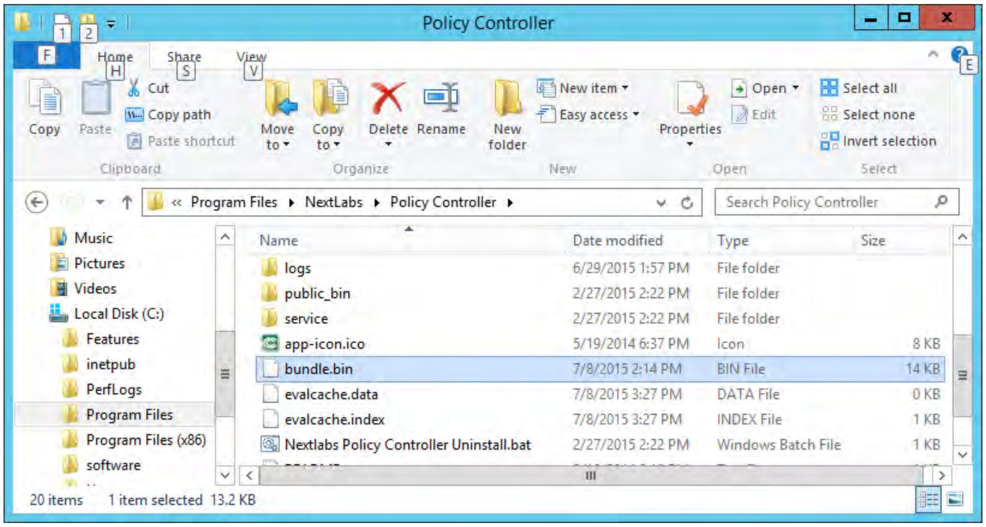
After a policy or component is deployed for the first time, or modified and re-deployed within Policy Studio on the SQL Server, an encrypted bundle.bin file on the SharePoint Server will be updated after one heartbeat. As explained in chapter 7, on the SharePoint Server it is the responsibility of the Controller Manager component of the NextLabs Policy Controller (PDP) to encrypt the bundle.bin file on the local file system for use during policy evaluation by the PDP.

To ensure the policy logic is being correctly sent from the NextLabs Policy Studio (PAP) on the SQL Server to the bundle.bin file on the SharePoint Server for use by the NextLabs Policy Controller (PDP), you can find the bundle.bin file and decrypt its contents to see your policy logic decrypted there.

8.6.1.1 On the SharePoint Server note timestamp of the bundle.bin file and decrypt its contents

1. Double-click the **C:/** drive.
2. Double-click **Program Files**.
3. Double-click **NextLabs**.
4. Double-click **Policy Controller**.

5. Scroll down to find **bundle.bin** and note the timestamp in the **Date Modified** column. This would be the last time policies or components were deployed.



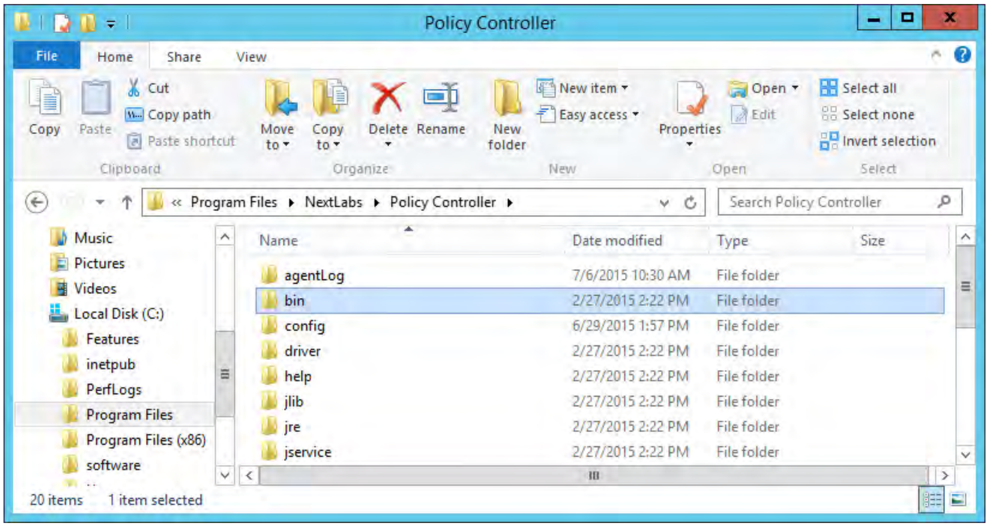
« Program Files ▸ NextLabs ▸ Policy Controller ▸

Search Policy Controller

Name	Date modified	Type	Size
logs	6/29/2015 1:57 PM	File folder	
public_bin	2/27/2015 2:22 PM	File folder	
service	2/27/2015 2:22 PM	File folder	
app-icon.ico	5/19/2014 6:37 PM	Icon	8 KB
bundle.bin	7/8/2015 2:14 PM	BIN File	14 KB
evalcache.data	7/8/2015 3:27 PM	DATA File	0 KB
evalcache.index	7/8/2015 3:27 PM	INDEX File	1 KB
Nextlabs Policy Controller Uninstall.bat	2/27/2015 2:22 PM	Windows Batch File	1 KB

20 items 1 item selected 13.2 KB

6. Scroll back up and double-click on the **bin** folder.



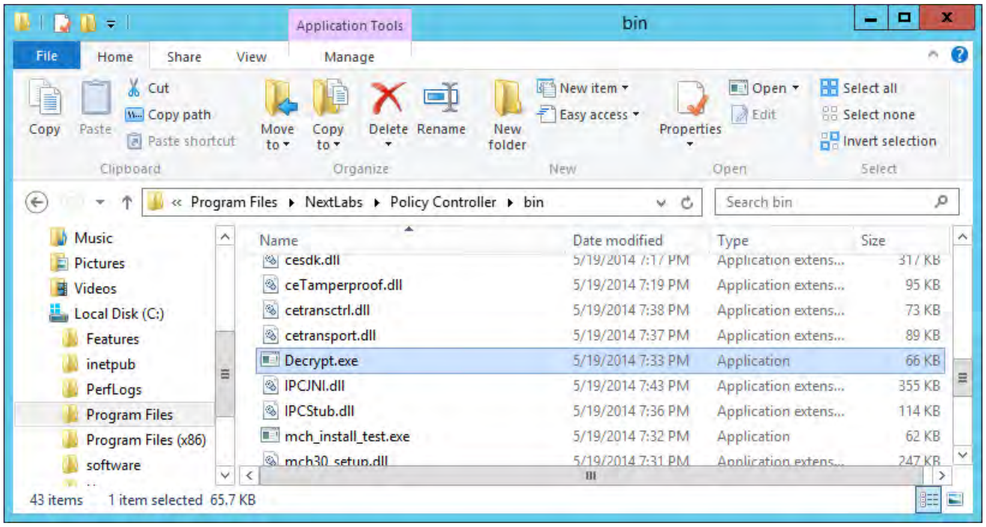
« Program Files ▸ NextLabs ▸ Policy Controller ▸

Search Policy Controller

Name	Date modified	Type	Size
agentLog	7/6/2015 10:30 AM	File folder	
bin	2/27/2015 2:22 PM	File folder	
config	6/29/2015 1:57 PM	File folder	
driver	2/27/2015 2:22 PM	File folder	
help	2/27/2015 2:22 PM	File folder	
jlib	2/27/2015 2:22 PM	File folder	
jre	2/27/2015 2:22 PM	File folder	
jservice	2/27/2015 2:22 PM	File folder	

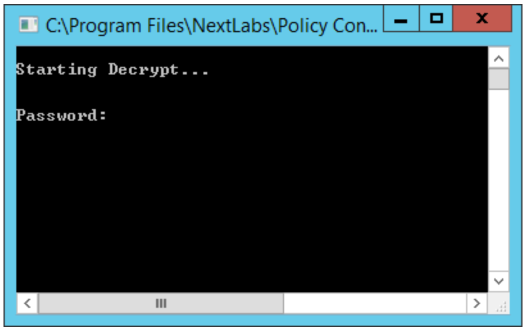
20 items 1 item selected

7. Scroll down to find **Decrypt.exe**.



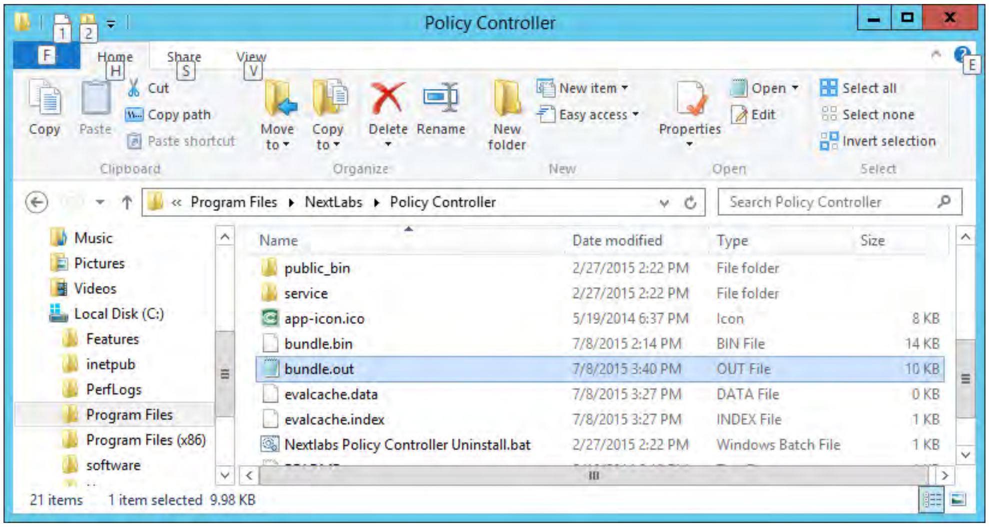
Name	Date modified	Type	Size
cesdk.dll	5/19/2014 7:17 PM	Application extens...	317 KB
ceTamperproof.dll	5/19/2014 7:19 PM	Application extens...	95 KB
cetransctrl.dll	5/19/2014 7:38 PM	Application extens...	73 KB
cetransport.dll	5/19/2014 7:37 PM	Application extens...	89 KB
Decrypt.exe	5/19/2014 7:33 PM	Application	66 KB
IPCJNI.dll	5/19/2014 7:43 PM	Application extens...	355 KB
IPCStub.dll	5/19/2014 7:36 PM	Application extens...	114 KB
mch_install_test.exe	5/19/2014 7:32 PM	Application	62 KB
mch30_setup.dll	5/19/2014 7:31 PM	Application extens...	247 KB

a. In the Decrypt window, enter the administrator's **Password** and press **Enter**.



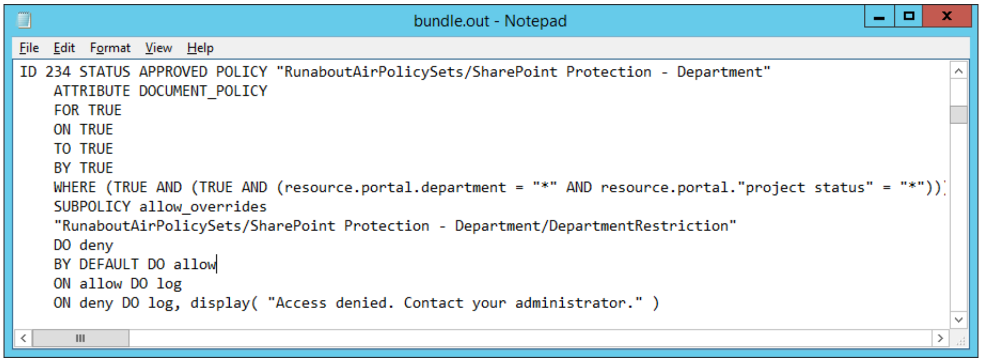
```
Starting Decrypt...

Password:
```

b. After the Decrypt window disappears, click on **Policy Controller** to return to that folder. Scroll down and double-click the **bundle.out** file.



Name	Date modified	Type	Size
public_bin	2/27/2015 2:22 PM	File folder	
service	2/27/2015 2:22 PM	File folder	
app-icon.ico	5/19/2014 6:37 PM	Icon	8 KB
bundle.bin	7/8/2015 2:14 PM	BIN File	14 KB
bundle.out	7/8/2015 3:40 PM	OUT File	10 KB
evalcache.data	7/8/2015 3:27 PM	DATA File	0 KB
evalcache.index	7/8/2015 3:27 PM	INDEX File	1 KB
Nextlabs Policy Controller Uninstall.bat	2/27/2015 2:22 PM	Windows Batch File	1 KB

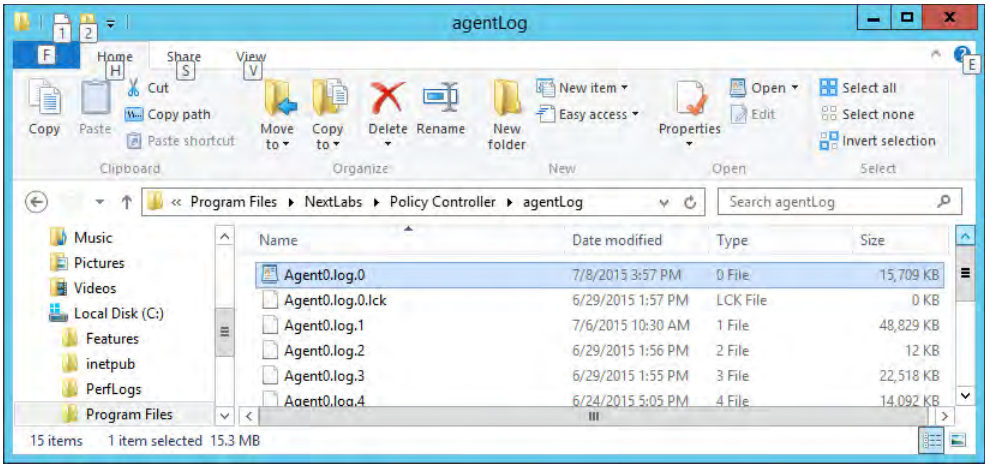
c. In the text editor window, scroll down to find policies that you have created previously. Example: **RunaboutAirPolicySets/SharePoint Protection - Department** top-level policy



```
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." )
```

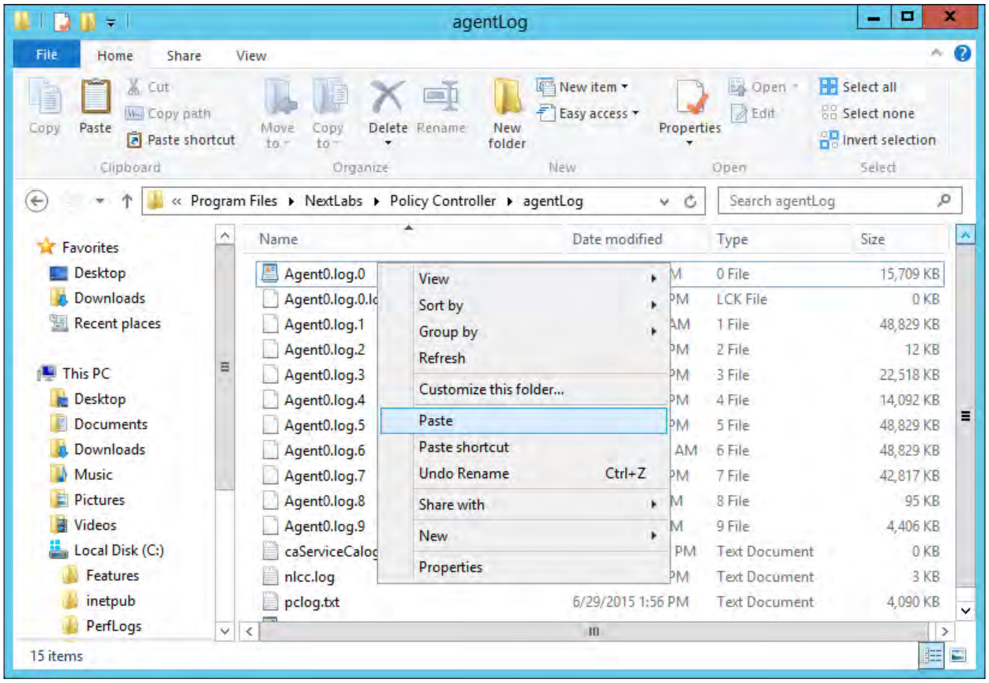
8.6.2 Reviewing NextLabs AgentLog to Illustrate History of Access Control Evaluations During SharePoint Access

1. Double-click the **C:/** drive.
2. Double-click **Program Files**.
3. Double-click **NextLabs**.
4. Double-click **Policy Controller**.
5. Double-click **AgentLog**.
6. Right-click the **Agento.log.0** locked file and select **Copy**.

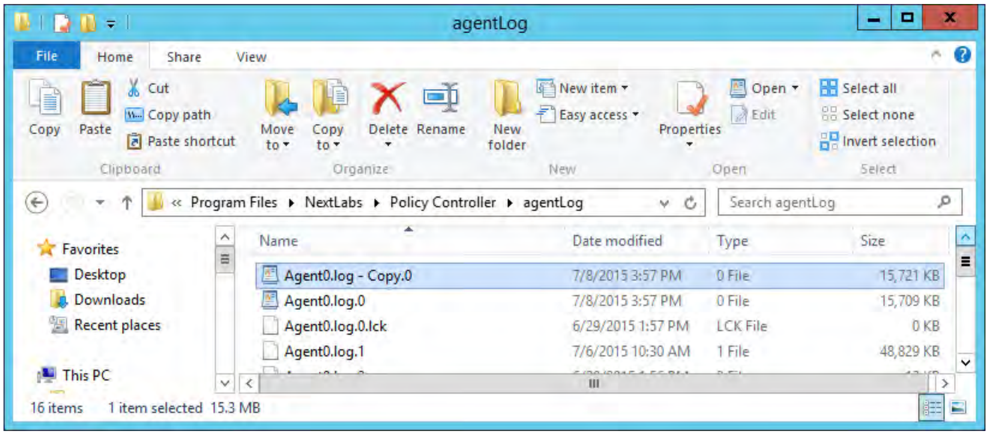


Name	Date modified	Type	Size
Agent0.log.0	7/8/2015 3:57 PM	0 File	15,709 KB
Agent0.log.0.lck	6/29/2015 1:57 PM	LCK File	0 KB
Agent0.log.1	7/6/2015 10:30 AM	1 File	48,829 KB
Agent0.log.2	6/29/2015 1:56 PM	2 File	12 KB
Agent0.log.3	6/29/2015 1:55 PM	3 File	22,518 KB
Agent0.log.4	6/24/2015 5:05 PM	4 File	14,092 KB

7. Within the agentLog folder, right-click in an empty space and select **Paste**.



8. Double-click the **Agent0.log-Copy.0** file to view its contents.



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 =**.

   a. Examples of information found in this **Agent0.log-Copy.0** file:

      i. All of the policies evaluated during one instance of access:

```
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
A: RunaboutAirPolicySets/SharePoint Protection - Department
X: RunaboutAirPolicySets/SharePoint Protection - IP
Address/AllowIPAddressLevel1
X: RunaboutAirPolicySets/SharePoint Protection - IP
Address/AllowSensitiveLevelsToAnyOtherIP
A: RunaboutAirPolicySets/SharePoint Protection - IP Address
X: RunaboutAirPolicySets/SharePoint Protection -
Maintenance/Allow Maintenance After 6pm and Weekends
A: RunaboutAirPolicySets/SharePoint Protection -
Maintenance/Allow Non-Maintenance Any Time
A: RunaboutAirPolicySets/SharePoint Protection - Maintenance
X: RunaboutAirPolicySets/SharePoint Protection -
Sensitivity/Policy1a-Sensitivity Level 1
X: RunaboutAirPolicySets/SharePoint Protection -
Sensitivity/Policy1b-Sensitivity Level 2
X: RunaboutAirPolicySets/SharePoint Protection -
Sensitivity/Policy1c-Sensitivity Level 3
A: RunaboutAirPolicySets/SharePoint Protection - Sensitivity
```

ii. An allow decision was evaluated when this example user, **Jorge Gonzalez**, logged into the Runabout Air SharePoint:

```
Jul 7, 2015 4:29:53 PM
com.bluejungle.destiny.agent.controlmanager.PolicyEvaluatorImpl
queryDecisionEngine
INFO: Request 2342972204282387 input params
  to
  application
pid: 5140
  environment
request_id: 2342972204282387
time_since_last_successful_heartbeat: 31
  host
inet_address: 184536844
  operating-system-user
id: S-1-5-21-972639958-268376111-2639239546-1138
  action
name: OPEN
  sendto
  from
title: relying party inc - root site
cd::id: sharepoint://sharepoint.abac.test/
name: relying party inc - root site
sub_type: site
type: site
ce::destinytype: portal
url: sharepoint://sharepoint.abac.test/
  user
:
id: S-1-5-21-972639958-268376111-2639239546-1138
title: Scientist
department: Research and development
stafflevel: Senior
upn: jgonzalez@ABAC.TEST
company: Conway
name: abac\jgonzalez
clearance: Top Secret
  Ignore obligation = false
  Process Token = 984
  LogLevel = 3
  Result: Effect = allow (total:4608ms, setup:4605ms,
obligations:0ms)
  Obligations:
  From file list: [sharepoint://sharepoint.abac.test/]
  To filename list: null

```

9 Leveraging NextLabs Control Center Reporter for Reporting and Auditing Purposes

9.1 Introduction

In previous sections of this How-To Guide (Chapter 7), we installed several NextLabs products that can be used to define and deploy Attribute-Based Access Control policies and enforce decisions regarding user access to Microsoft SharePoint resources based on user, object, environmental attributes, and the corresponding policies in place. We also illustrated how to use and configure the NextLabs Policy Studio, the product responsible for Policy Lifecycle Management, and discussed policy strategy and the translation of business logic into policy (Chapter 8).

In this section of the How-To Guide, we will illustrate how to use the NextLabs Control Center Reporter, a component of the previously installed NextLabs Control Center (Chapter 7), in order to generate reports and provide a graphical user interface for prior policy evaluation and access control decisions in your environment.

Reporter is automatically installed during the NextLabs Control Center installation, which was detailed in chapter 7. In this How-To section we will introduce Reporter, its purpose, interface, and capabilities, then illustrate some example uses based on our build.

9.1.1 Components Used in this How-To Guide

1. NextLabs Control Center Reporter v7.5.0 (64) – web application and graphical user interface for evaluating prior policy evaluation access control decisions and generating reports for monitoring and auditing.

9.1.2 Pre-requisites to Complete Prior to This How-To Guide

1. If you intend to do a setup without identity federation and federated logins, you must:
    a. Install and configure Active Directory (see Chapter 2)
    b. Install and configure Microsoft SharePoint (see Chapter 4)
    c. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see Chapter 7)
    d. Define and deploy policies based on your business rules (see Chapter 8)
2. If you intend to incorporate a trust relationship between an IdP and RP and use federated logins into SharePoint, you must:
    a. Install and configure Active Directory (see Chapter 2)
    b. Setup and configure the RP and IdP (see Chapter 3)
    c. Install and configure Microsoft SharePoint (see Chapter 4)
    d. Configure the SharePoint federated login with the RP (see Chapter 5)
    e. Configure the attribute flow between all endpoints (see Chapter 6)
    f. Install and configure NextLabs Control Center, Policy Studio, and Policy Controller (see Chapter 7)
    g. Define and deploy policies based on your business rules (see Chapter 8)

9.2 Introduction to NextLabs Control Center Reporter

The NextLabs Control Center Reporter is a web application that can be used to generate reports on how information is being used in your environment. You can use Reporter to define and run custom queries about policy enforcement activities that are recorded in the Activity Journal, a native, automatic logging mechanism built into the NextLabs SQL database that was configured during installation of the NextLabs Control Center (Chapter 7). These queries are referred to as **reports**. Reports can be designed to answer a wide variety of questions, such as who has access to certain documents, who is using which resources and when, what types of policy enforcement is taking place, what activity occurred within a given department, and so on.

In addition to reports, you can also use Reporter to create monitors that trigger alerts when specified policy enforcement criteria are met. You can design monitors to cover a wide range of scenarios, such as sending an alert through email when access to a certain resource has been denied more than a specified number of times in a given time period; or when the volume of classified documents that have been downloaded in a given time period exceeds a specific file size. Together, monitors and alerts can provide continuous coverage of critical policy enforcements in an enterprise, as well as a notification system that lets you know when action is required.

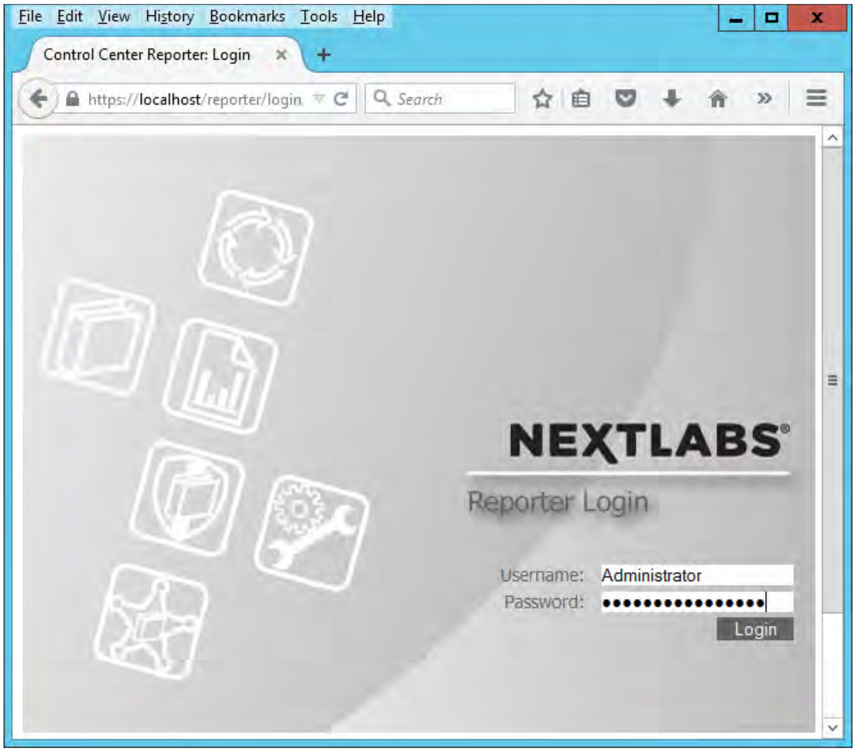
User permissions are defined in the Administrator application (another component of Control Center installed in Chapter 7), by creating a new User and assigning one of the four available roles to it. By default, all roles include permission to open and use the reporting functionality of Reporter.

9.2.1 Opening Reporter

1. On the server where NextLabs Control Center was installed, open a web browser (i.e., SQL Server in this build).

2. Enter the URL and press Enter: **https://<hostname>/reporter,** i.e., **https://localhost/reporter**

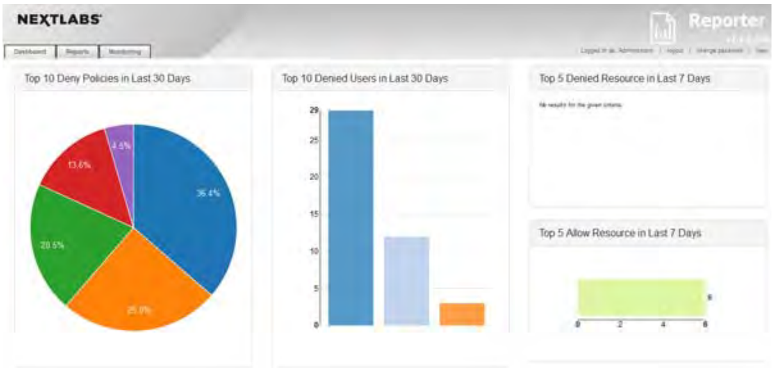
3. At the Reporter login screen, enter valid credentials, such as the Control Center Administrator account created in chapter 7. Click **Login**.


File Edit View History Bookmarks Tools Help
Control Center Reporter: Login
https://localhost/reporter/login
Search
NEXTLABS®
Reporter Login
Login

Username: Administrator

Password: ••••••••••••••••

4. In your browser, the Reporter opening view defaults to the Dashboard tab. The Dashboard tab, Reports tab, and Monitoring tab will be discussed more thoroughly in subsequent sections of this How-To Guide.


NEXTLABS
Reporter
Dashboard
Reports
Monitoring
Top 10 Deny Policies in Last 30 Days
36.4%
25.0%
20.5%
13.6%
4.5%
Top 10 Denied Users in Last 30 Days
29
25
20
15
10
5
0
Top 5 Denied Resource in Last 7 Days
No results for the given criteria.
Top 5 Allow Resource in Last 7 Days
6
0
2
4
6

9.3 Introduction to Reporter Dashboard

The Reporter Dashboard is divided into panes, each displaying a predefined statistical view of data that provides a snapshot of policy enforcement trends. In the default configuration of Reporter, these panes display data in the following graphs (from the NextLabs Control Center Reporter User Guide, available only to customers at this time):

85

Graph	Description	May Indicate:
Top Five Deny Policies (Month)	Pie chart representing the five Deny policies that were most frequently enforced over the previous thirty days.	■ Misunderstanding of access level: users being blocked from a resource they believe they should use ■ Incorrectly defined entitlements: users should have access, but policies are not updated or correctly designed
Top Ten Denied Users (Month)	Bar chart representing the ten users who have had the most instances of any Deny policy enforced against them.	■ Users who habitually snoop into resources they are not authorized to use ■ Incorrectly defined entitlements: users or group should have access, but policies are not updated or are incorrectly designed
Top Five Deny Resources (Week)	Bar chart representing the five resources that any users have most frequently attempted to access and been blocked by an active policy, over the previous seven days.	■ Resources of broad interest to users who should not be using them ■ Incorrectly designed resource or user component, blocking users who should have access
Top Five Allow Resources (Week)	Bar chart representing the five resources that users have most frequently attempted to access and been allowed by an active policy, over the previous seven days.	■ Improperly designed resource component or policies, which allow inappropriate users access to sensitive resources
Deny Policy Enforcement Trends (Month)	Bar chart representing the trend, over the previous 30 days, of the daily total instances of any deny policy being enforced on any user, for any resource.	■ Progress (or lack thereof) in educating users about access policies and individual/group entitlements, at a broad level ■ Improperly designed policies that are blocking too many users who expect and are entitled to access or use
Recent Allows	List of details about the most recent ten instances of any allow policy being enforced against any user, for any resource. Details listed include: ■ Date of eneforcement ■ Name of enforced policy ■ User who triggered the policy ■ Action that triggered the policy ■ Resource th user was trying to access	■ 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

Graph	Description	May Indicate:
Recent Denys	List of details about the most recent ten instances of any deny policy being enforced against any user, for any resource. Details listed include: ▪ Date of enforcement ▪ Name of enforced policy ▪ User who triggered the policy ▪ Action that triggered the policy ▪ Resource the user was trying to access	▪ Instances where many users are attempting to get at data they are not authorized to use ▪ Instances where some urgent correction is required to allow appropriate access, such as multiple authorized users being blocked from some resource they need by an incorrectly defined policy
Alerts this Week: Group by Tags	Treemap representing volume of alerts in the current week. Alerts are grouped by monitor tags.	▪ Policies being watched by monitors that are tagged are being enforced at a rate that demands attention. Further review or action may be required.
Today's Alerts: Details	List of details about the alerts raised in the current day. Details include: ▪ Alert level ▪ Monitor name ▪ Alert message ▪ Date and time the alert was raised	▪ Policies being monitored are being enforced at a rate that demands attention. Further review or action may be required.

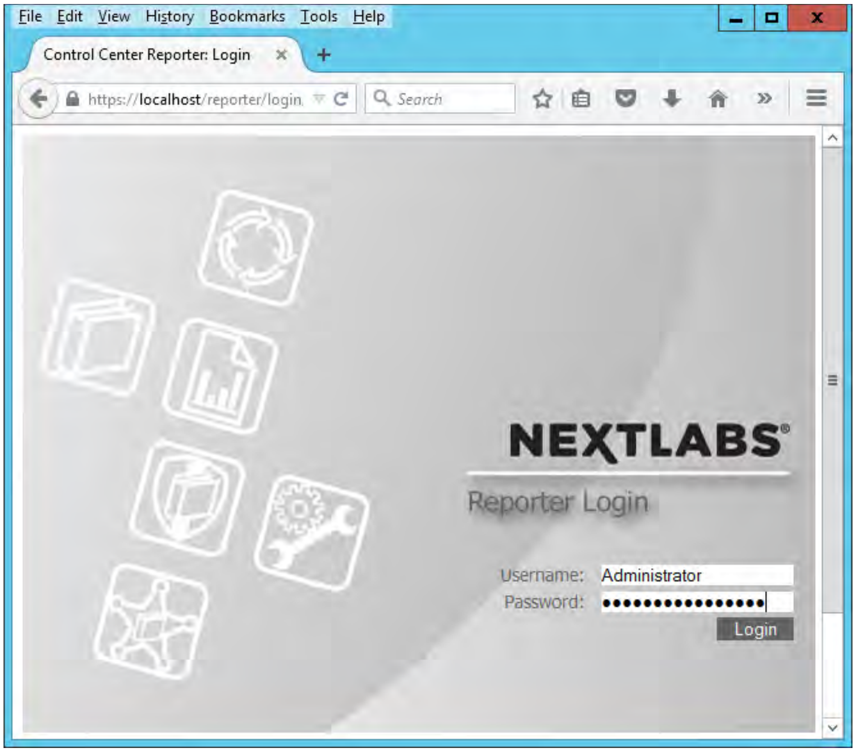
These panels are configurable such that an administrator can choose which panels and data are visible and how they are laid out within the Dashboard according to the business's business logic, policies, and priorities.

The data displayed in all panes of the dashboard is refreshed from the Activity Journal each time you open the Dashboard tab. This means that data is updated on demand; for example, if a pane shows some statistic for the past week, that reflects not the last seven whole calendar days, but the last seven 24-hour periods starting from the top of the current hour.

9.3.1 Exploring the Dashboard

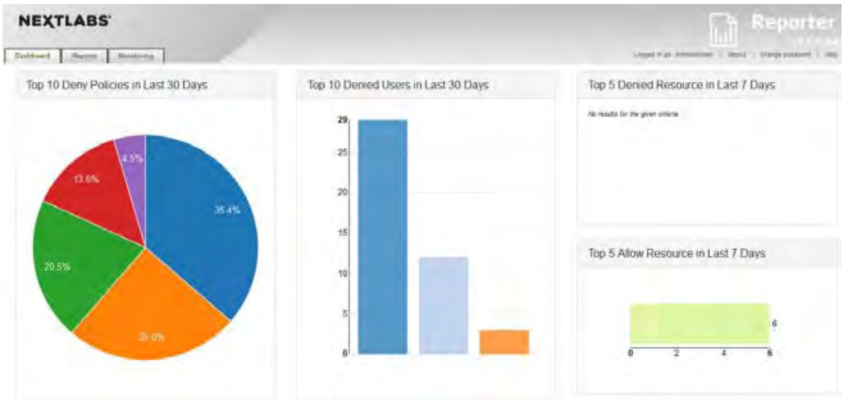
1. On the server where NextLabs Control Center was installed, open a web browser, i.e., SQL Server in this build
2. Enter the URL and press Enter: **https://<hostname>/reporter**, i.e., **https://localhost/reporter**

3. At the Reporter login screen, enter valid credentials such as the Control Center Administrator account created in chapter 7. Click **Login**.


File Edit View History Bookmarks Tools Help
Control Center Reporter: Login
https://localhost/reporter/login
Search
NEXTLABS
Reporter Login
Login

Username: Administrator
Password: ••••••••••••••••

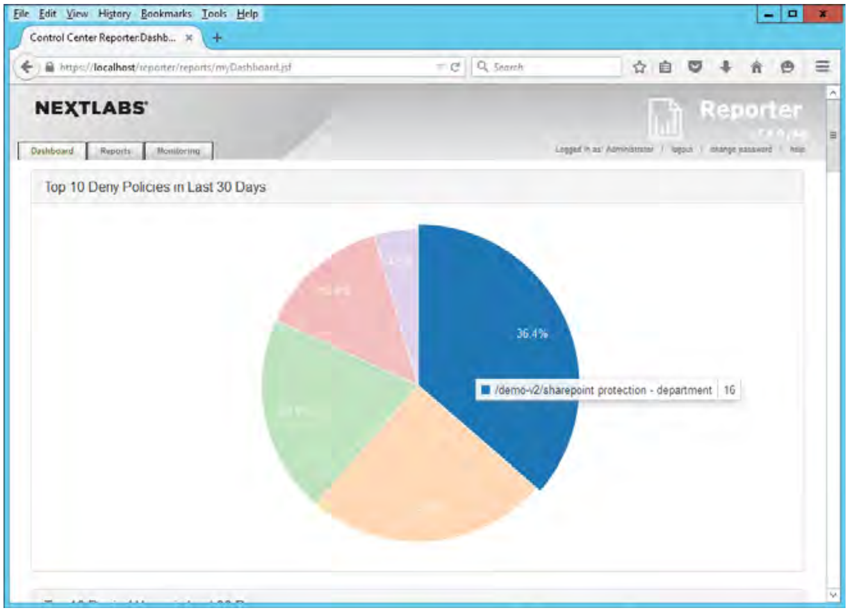
4. In your browser, the Reporter will default to the **Dashboard** tab.


NEXTLABS
Reporter
Dashboard
Reports
Monitoring
Top 10 Deny Policies in Last 30 Days
4.5%
13.6%
36.4%
20.5%
25.0%
Top 10 Denied Users in Last 30 Days
29
25
20
15
10
5
0
Top 5 Denied Resource in Last 7 Days
Top 5 Allow Resource in Last 7 Days
6
0
2
4
6

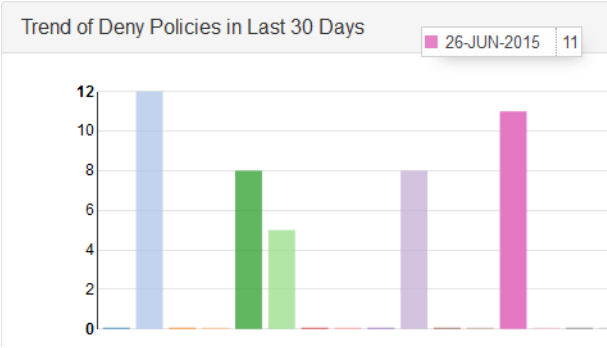
No results for the given criteria

5. 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.

6. 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.

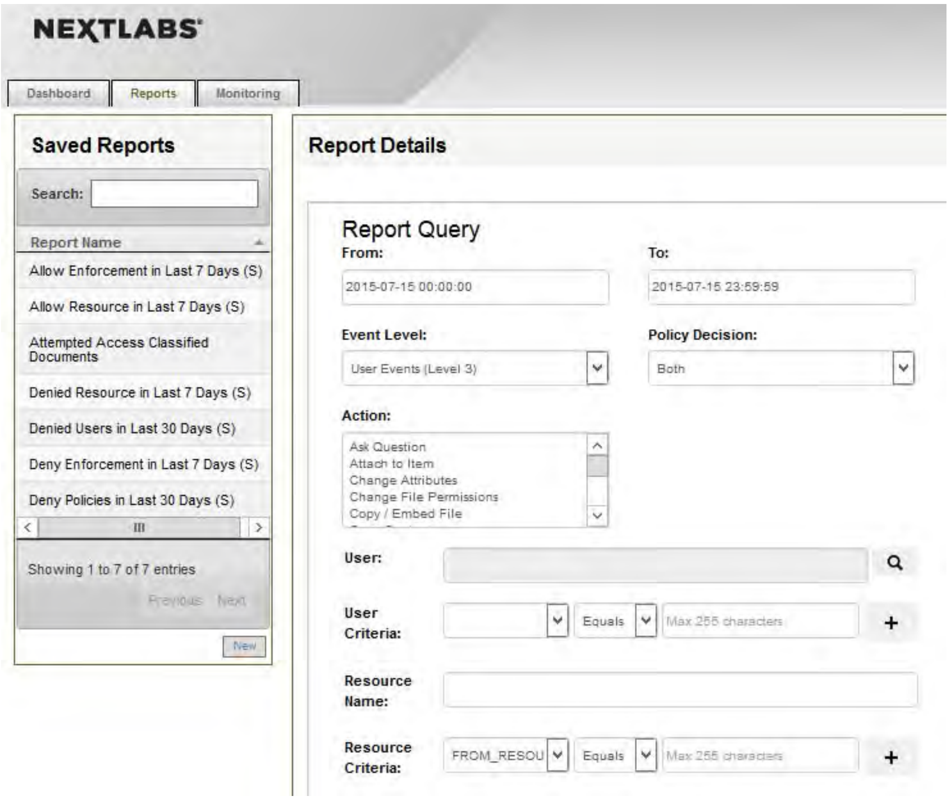

File Edit View History Bookmarks Tools Help
Control Center Reporter:Dashb...
https://localhost/reporter/reports/myDashboard.jsf
Search
NEXTLABS
Reporter
Dashboard
Reports
Monitoring
Logged in as: Administrator / logout / change password / help
Top 10 Deny Policies in Last 30 Days
36.4%
/demo-v2/sharepoint protection - department 16

7. 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.



9.4 Introduction to Defining and Running Custom Reports in Reporter

In Reporter, you can define and run reports in the Reports tab. This tab is divided into two panes, **Saved Reports** on the left side of the Reports tab window and **Report Details** on the right.



Saved Reports

Search:

Report Name
- Allow Enforcement in Last 7 Days (S)
- Allow Resource in Last 7 Days (S)
- Attempted Access Classified Documents
- Denied Resource in Last 7 Days (S)
- Denied Users in Last 30 Days (S)
- Deny Enforcement in Last 7 Days (S)
- Deny Policies in Last 30 Days (S)

Showing 1 to 7 of 7 entries

Previous Next

New

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:

User Criteria: Equals Max 255 characters +

Resource Name:

Resource Criteria: FROM_RESOU Equals Max 255 characters +

The Saved Reports pane provides a list of all saved reports available to you. This includes all reports you create and save, all reports saved by other users and marked as Shared, and the sample reports used to generate data that is displayed in the Dashboard tab. When you click on any item in Saved Reports, the details of that report are displayed in Report Details on the right. This is also where you work when you create a new report.

In the Report Details pane, define the following:

- The time period of the policy activity data to cover in the report
- The criteria, or filters, that determine what policy activity data to include in the report
- The output format of the report

The default settings in Report Details display when you click the Reports tab or when you click New in the Saved Reports pane. By default, the time period for the report is the current day, all policy activity data at the user level is included, and the data is presented in table format.

After defining a new report or editing an existing report, click **Run** at the bottom of the Report Details pane to view the results, which we will illustrate in the following two subsections.

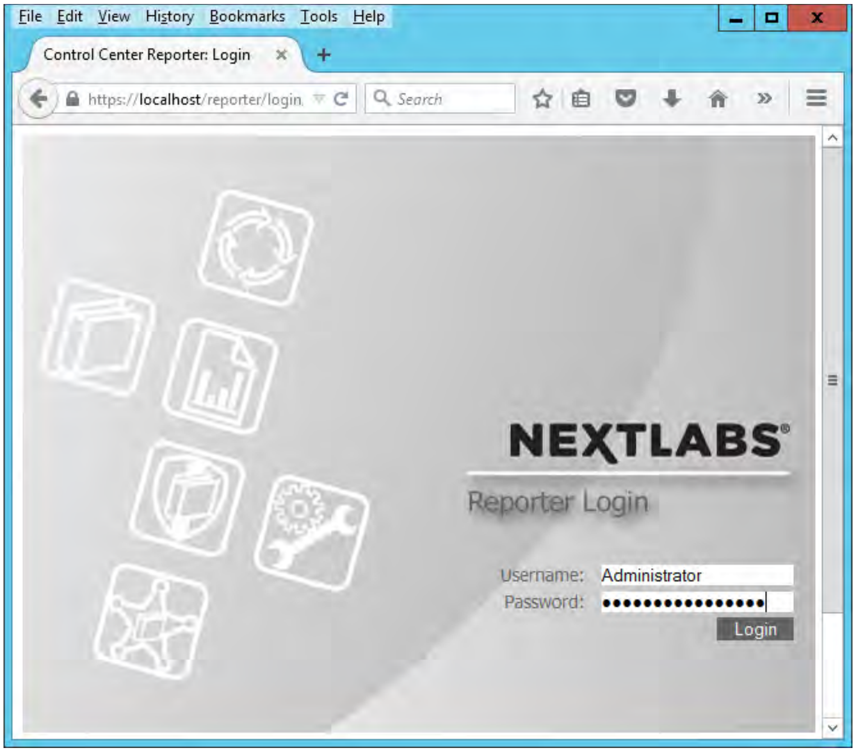
9.4.1 Defining a Custom Report

In this subsection we will list the standard steps for creating a custom report. In section 9.5 of this How-To Guide we will illustrate some example custom report sections that demonstrate Reporter's report capabilities.

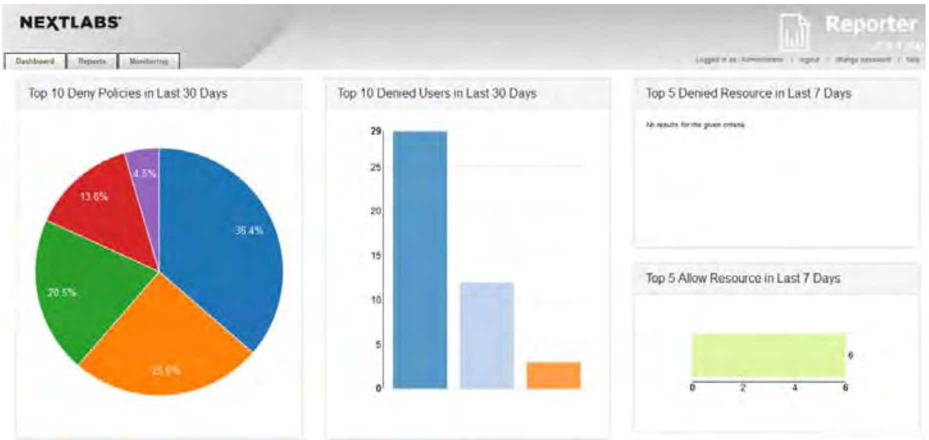
9.4.1.1 Logging into Reporter

Before being able to define a custom report, you must first log in to Reporter and click on the Reports tab as seen in the steps below:

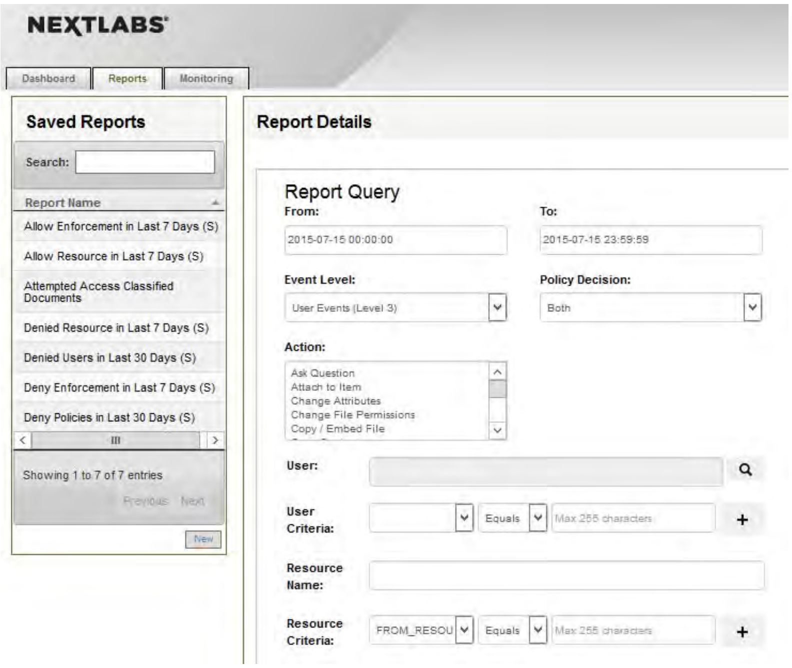
1. On the server where NextLabs Control Center was installed in chapter 7, open a web browser, i.e., SQL Server in this build.
2. Enter the URL and press Enter: **https://<hostname>/reporter,** i.e., **https://localhost/reporter**
3. At the Reporter login screen, enter valid credentials, such as the Control Center Administrator account created in chapter 7. Click **Login**.


File Edit View History Bookmarks Tools Help
Control Center Reporter: Login
https://localhost/reporter/login
Search
NEXTLABS
Reporter Login
Username: Administrator
Password: ••••••••••••••••
Login

4. In your browser, the Reporter user interface will default to the **Dashboard** tab. The Dashboard tab, Reports tab, and Monitoring tab will be discussed more thoroughly in subsequent sections of this How-To Guide.


NEXTLABS
Reporter
Dashboard
Reports
Monitoring
Top 10 Deny Policies in Last 30 Days
4.5%
13.6%
36.4%
20.5%
25.0%
Top 10 Denied Users in Last 30 Days
29
25
20
15
10
5
0
Top 5 Denied Resource in Last 7 Days
No results for the given criteria
Top 5 Allow Resource in Last 7 Days
6
0
2
4
6

5. Click on the **Reports** tab to open the Reports tab window.



Allow Enforcement in Last 7 Days (S)
Allow Resource in Last 7 Days (S)
Attempted Access Classified Documents
Denied Resource in Last 7 Days (S)
Denied Users in Last 30 Days (S)
Deny Enforcement in Last 7 Days (S)
Deny Policies in Last 30 Days (S)

Showing 1 to 7 of 7 entries

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:

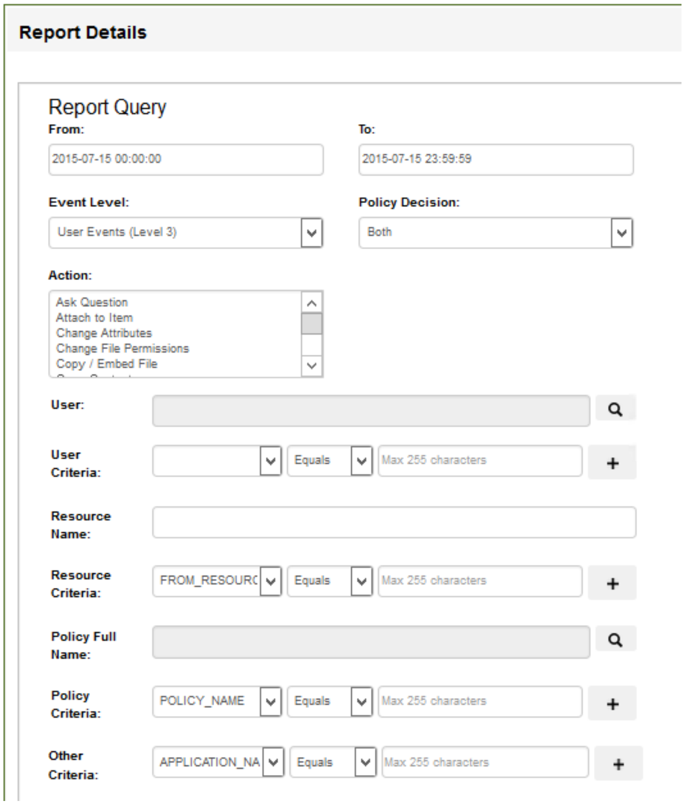
User Criteria: Equals Max 255 characters

Resource Name:

Resource Criteria: FROM_RESOU Equals Max 255 characters

9.4.1.2 Defining the Custom Report

In order to define a custom or new report, you must specify filters and change default settings within the Report Details – Report Query pane. If you don’t specify any filters or change any of the default 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:

User Criteria: Equals, Max 255 characters

Resource Name:

Resource Criteria: FROM_RESOURC, Equals, Max 255 characters

Policy Full Name:

Policy Criteria: POLICY_NAME, Equals, Max 255 characters

Other Criteria: APPLICATION_NA, Equals, Max 255 characters

1. In the Report Details – Report Query pane, define the report query by filling in data or using drop-down menus to define your desired report.
    a. Note: Many of the fields are optional. Required fields contain default values.
        i. In the From and To fields, specify the start date and time, and end date and time, respectively, of the time period you want the report to cover. Click in the field to choose a date and time from the calendar. When specifying a report period, be sure to consider the time zone where Control Center is installed, and the time period of data stored in the Activity Journal.
        i. In Event Level, select the level of event verbosity the report contains:
        - User Events (default): Logged in the Activity Journal as Level 1
        - Application Events (application and user-level events): Logged in the Activity Journal as Level 2
        - All System Events (system, application, and user-level events): Logged in the Activity Journal as Level 3
        - Note: As a rule, you should leave this setting at User Events. This setting significantly reduces the amount of system noise. Application- or system-level events generally are not useful in monitoring policy or user activities.
2. In **Decision**, select the type of enforcement effect to include in this report:
    a. Allow: Instances when the policy permitted the user to perform the action covered by the policy. Note that the report results always depend on what information is logged. If

the policy does not have any On Allow logging obligation specified, this report will not return any On Allow data whether or not you select this option.

   b. Deny: Instances when the policy did not allow the user to perform the action. Deny decisions are always logged.

   c. Both: All instances when the policy was enforced, with either Allow or Deny effect.

3. In **Action**, select the user action or actions to include in this report. The list shows all currently defined actions.

   a. To select multiple actions, hold Ctrl and click each action. If you do not make any selections, all actions are included.

   b. Note: Policies involving Paste actions do not support logging obligations, therefore, instances of their enforcement are not included in reports.

4. In **User**, specify one or more users on which to filter the activity data, or leave this field blank to include all users. Use the User Lookup window (magnifying glass icon) to browse through all users currently defined in your Information Network Directory, and select the users you want.

5. In **User Criteria**, specify additional user criteria by creating one or more conditions. Each condition consists of a user attribute, an operator, and a value. You must click the + button to add a condition to the query.

6. In **Resource Path**, type the network path of the resource on which to filter, or leave this field blank to include all resources.

7. In **Resource Criteria**, specify additional resource criteria by creating one or more conditions. Each condition consists of a resource attribute, an operator, and a value. Click the + button to add a condition to the query.

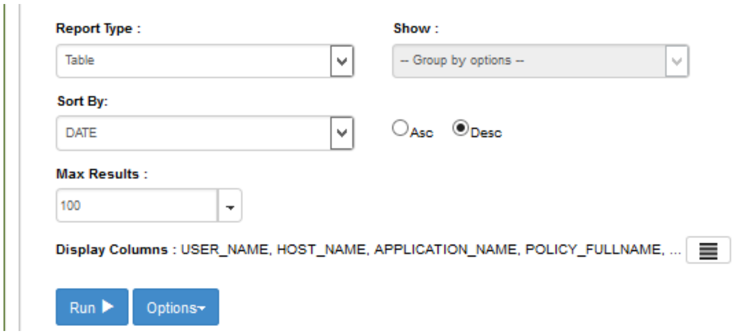
8. In **Policy Name**, specify one or more policies on which to filter, or leave this field blank to include all policies. Use the Policy Lookup window to browse through and select which policies you want to include.

9. In **Policy Criteria**, specify additional policy criteria by creating one or more conditions. Each condition consists of a policy attribute, an operator, and a value. Click the + button to add a condition to the query.

10. In **Other Criteria**, specify additional criteria by creating one or more conditions. Each condition consists of a general attribute (for example, host name, host IP, and application name), an operator, and a value. Click the **+** button to add a condition to the query.

9.4.1.3 Setting the Custom Report Display Options

Within the Report Details – Report Query pane, directly below the Other Criteria filter, continue with these steps to set the display options for your custom report:



Report Type : Table

Show : -- Group by options --

Sort By: DATE ○Asc ●Desc

Max Results : 100

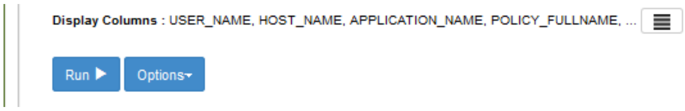
Display Columns : USER_NAME, HOST_NAME, APPLICATION_NAME, POLICY_FULLNAME, ...

1. In **Report Type**, select the output format in which to display the data: Table, Bar Chart, Horizontal Bar Chart, or Pie Chart. Use a table to display policy activity details in a row-and-column format. Use a chart to display a summary of policy activities.
2. If you selected one of the charts in Report Type, in **Show**, select a grouping option. Grouping is not available to a table.
   a. Group by User: The chart shows the number of enforcement events for each user covered by the report.
   b. Group by Resource: The chart shows the number of enforcement events for each resource covered by the report.
   c. Group by Policy: The chart shows the number of enforcement events for each policy covered by the report.
   d. Group by Month: The chart shows the number of enforcement events for each month covered by the report. Select this option only if the time period you specified spans more than one month.
   e. Group by Day: The chart shows the number of enforcement events for each day covered by the report.
3. In **Sort By**, select a field on which to sort the data, then select Asc to sort in ascending order or Desc to sort in descending order. If the report is a table, you can sort the data by any attribute. If the report is a chart, you can sort either by the grouping item (user, resource, policy, month, or day) or by Result Count (the number of enforcement events for each user, resource, policy, month, or day).
4. In **Max Results**, specify the maximum number of results to display in the table or chart. For charts, this number represents the maximum number of bars in a bar chart, or slices in a pie chart. For readability reasons, charts should display a limited number of bars or slices. For a table, the number represents the maximum number of rows (each row represents an event). Tables that show a large number of rows present the data on multiple pages.
5. In **Display Columns**, select the columns to display in a table. This setting applies to tables only. USER_NAME, POLICY_FULLNAME, POLICY_DECISION, HOST_NAME, and APPLICATION_NAME are selected by default. To remove any of those columns or to add other columns, click ☰ and use the arrow icons to move columns out of, or into, the Selected pane.

9.4.2 Running a Custom Report

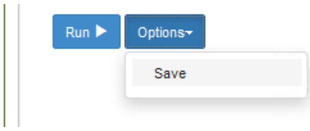
Directly beneath the filters and data fields for defining the report and setting its display settings, do the following in order to run the report and/or save it for the future:

1. At the bottom of the Report Details – Report Query pane, click **Run** to generate the new report.



Display Columns : USER_NAME, HOST_NAME, APPLICATION_NAME, POLICY_FULLNAME, ...

2. If you want to run this report again in the future, save the report. Click **Options**, and select **Save**.



9.5 Example Custom Report and Available Formats

In this section we will present examples of different report formats, all representing a small set of event data, returned by the same custom report from our build. By comparing the example formats, you will gain a better understanding of the way the different formats can be used to highlight different aspects of the same data depending on your business rules or priorities.

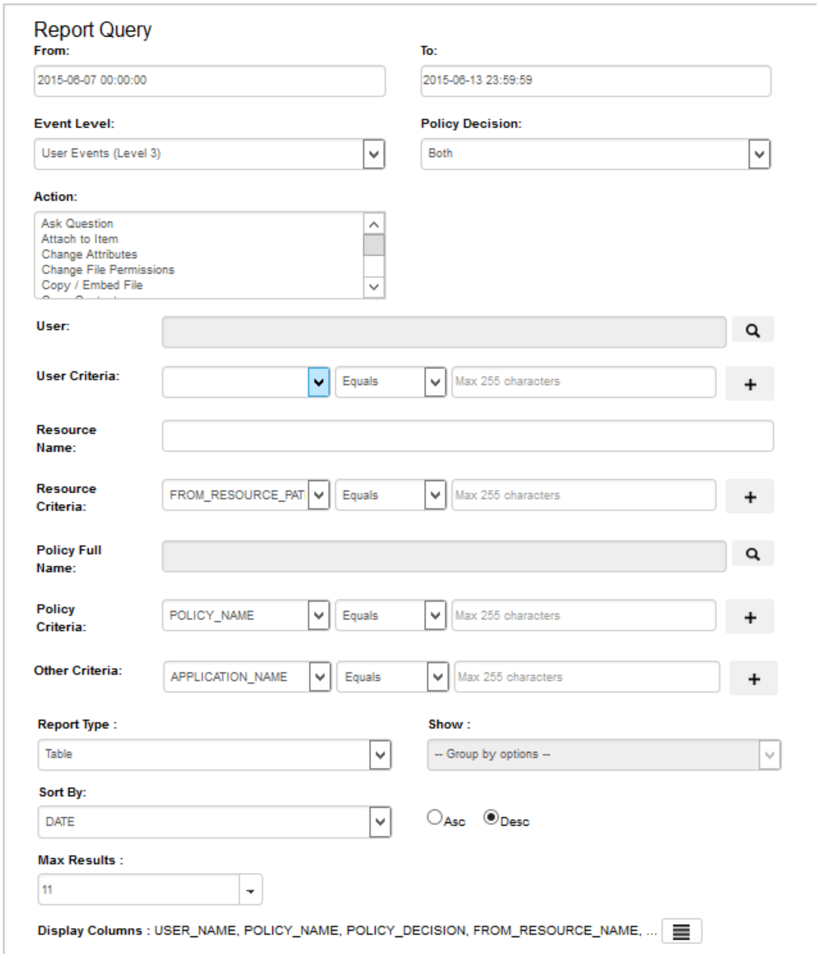
The custom report used in this section will result from a query that requests all events by users on all resources for one week (June 7, 2015 to June 13, 2015). We include columns that are relevant for our example business logic and the ABAC policies we put in place in chapter 8. For example, we chose to include the **Department** and **Sensitivity** columns, which were custom attributes in the metadata we added to the documents uploaded to the RP’s SharePoint sites.

9.5.1 Defining the Example Custom Report

9.5.1.1 Customizing Report Query Fields for this Report

1. In the Report Query pane, change the fields for the **From** and **To** date to match the desired query for the week of June 7, 2015 to June 13, 2015.
2. In the Report Query pane, click on the **Max Results** field to open the drop-down menu. We chose 11 for demonstration purposes.

3. In the Report Query pane, leave the rest of the fields in the default query settings.



Report Query

From: 2015-06-07 00:00:00

To: 2015-06-13 23:59:59

Event Level: User Events (Level 3)

Policy Decision: Both

Action:
Ask Question
Attach to Item
Change Attributes
Change File Permissions
Copy / Embed File

User:

User Criteria: Equals Max 255 characters

Resource Name:

Resource Criteria: FROM_RESOURCE_PAT Equals Max 255 characters

Policy Full Name:

Policy Criteria: POLICY_NAME Equals Max 255 characters

Other Criteria: APPLICATION_NAME Equals Max 255 characters

Report Type : Table

Show : -- Group by options --

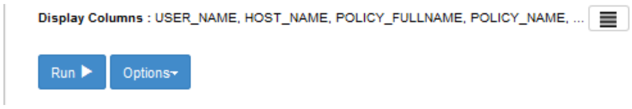
Sort By: DATE ○Asc ●Desc

Max Results : 11

Display Columns : USER_NAME, POLICY_NAME, POLICY_DECISION, FROM_RESOURCE_NAME, ...

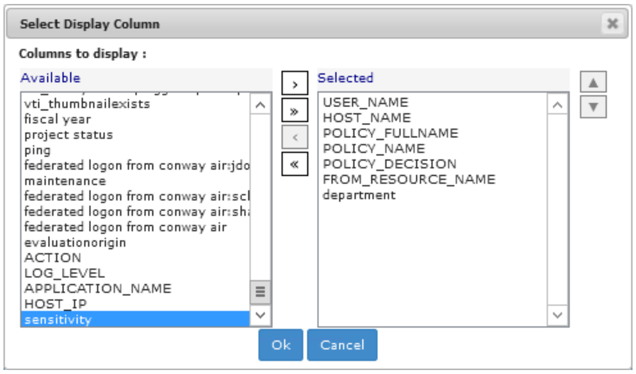
9.5.1.2 Editing the Columns for Custom Views

1. Toward the bottom of the Report Query pane, click on the columns icon at the end of the Display Columns line of text to open the Select Display Column window.



Display Columns : USER_NAME, HOST_NAME, POLICY_FULLNAME, POLICY_NAME, ...

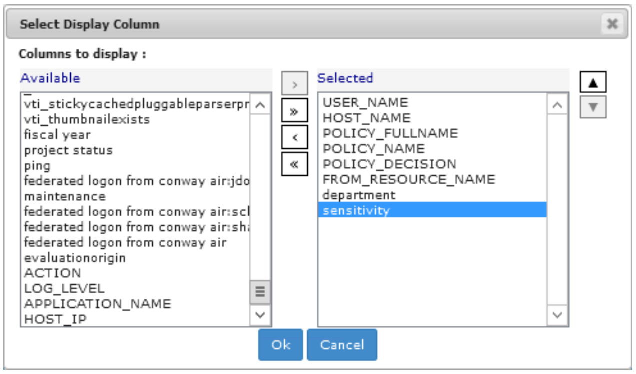
2. In the Select Display Column window, in the **Available** attribute list, review standard attributes (i.e. Action, Log_Level, Host_IP, etc) and custom attributes (department, sensitivity).



3. Click on any available attribute of interest to highlight it, then click the single right arrow button › to add it to the list of **Selected** attributes.

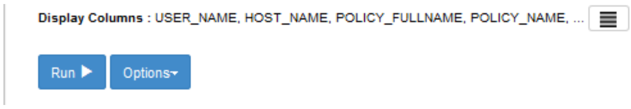
4. The attribute name will move from the **Available** list to the **Selected** list.

5. **Note**: Attributes can be added and removed individually by using the single arrow buttons between lists, or as a group by using the double arrow buttons between lists.



9.5.1.3 Running the Report Query

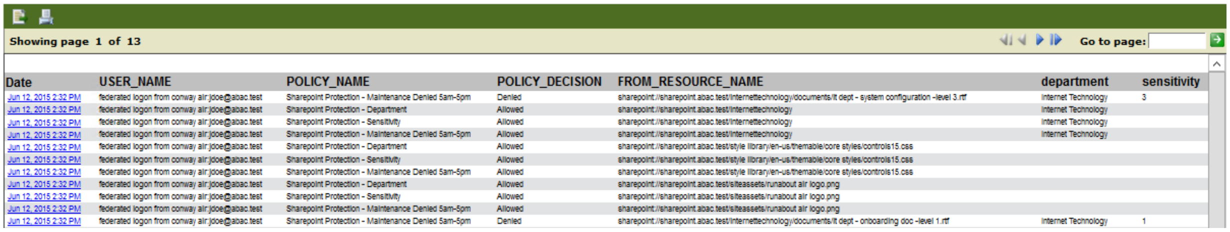
6. At the bottom of the Report Query pane, click **Run** to run the query. (**Tip**: You can click on **Options** and **Save** or **Save As** to save the query for future use.)


Display Columns : USER_NAME, HOST_NAME, POLICY_FULLNAME, POLICY_NAME, ...

7. Scroll down in your browser window to see the Results pane illustrated in the following section.

9.5.2 Format: Table of Event Data

The default results pane with the display columns you selected displays showing the query results. This is illustrated in the following image.



Showing page 1 of 13

Date	USER_NAME	POLICY_NAME	POLICY_DECISION	FROM_RESOURCE_NAME	department	sensitivity
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Denied	sharepoint://sharepoint.abac.test/internettechnology/documents/it dept - system configuration -level 3.rtf	Internet Technology	3
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint://sharepoint.abac.test/internettechnology	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint://sharepoint.abac.test/internettechnology	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint://sharepoint.abac.test/internettechnology	Internet Technology	
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint://sharepoint.abac.test/style library/en-us/themable/core styles/controls15.css		
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint://sharepoint.abac.test/style library/en-us/themable/core styles/controls15.css		
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint://sharepoint.abac.test/style library/en-us/themable/core styles/controls15.css		
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Department	Allowed	sharepoint://sharepoint.abac.test/siteassets/runabout air logo.png		
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Sensitivity	Allowed	sharepoint://sharepoint.abac.test/siteassets/runabout air logo.png		
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@abac.test	Sharepoint Protection - Maintenance Denied 5am-5pm	Allowed	sharepoint://sharepoint.abac.test/siteassets/runabout air logo.png		
Jun 12, 2015 2:32 PM	federated logon from conway air:jdoe@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

This excerpt from the query results shows that:

- 13 pages of policy enforcement events were logged.
- All events in this excerpt occurred on June 12, 2015 (as illustrated in the **Date** column).
- Each event from this excerpt was triggered by the same user, who had logged in with a federated identity from the IdP (chapters 1 through 5)
- Each event corresponds to one of three policies: SharePoint Protection – Sensitivity, SharePoint Protection – Maintenance Denied 5am-5pm, or SharePoint Protection – Department.
- Five resources were involved:
  - The first row shows that the resource was an .rtf document from the Internet Technology department’s SharePoint sub-site, marked at sensitivity level 3.
  - The second through fourth rows show that the resource was the Internet Technology department site.
  - The fifth through seventh rows show that the resources were the underlying .css style sheet and logo used on the SharePoint site.
  - The seventh through tenth rows (up to the second to last) show that the resources were the underlying .css style sheet and logo used on the SharePoint site.
  - The eleventh and final row from this excerpt shows that the resource was another .rtf document from the Internet Technology department SharePoint sub-site, marked at sensitivity level 1.
- In the case of three out of the five resources, the enforcement decision was Allow, as shown in the fourth column (second through tenth rows).
- 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).

Keep these details in mind as you analyze the data in the following charts.

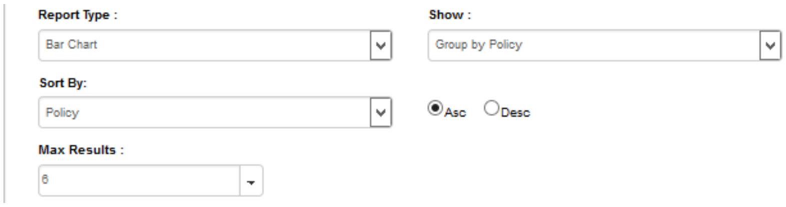
9.5.3 Format: Bar Chart Grouped by Policy Chart

Grouping events by policy is useful for identifying policies that are being triggered with unexpected frequency, which may be an indication that they are improperly designed and cover users, resources or actions that they should not. It can also indicate concentrated efforts at unauthorized data access. To examine the latter possibility, it is often helpful to switch to the Group by User option in order to focus on who is performing the activity, as seen in section 9.5.4.

9.5.3.1 Customizing the Display Settings

1. Using the Report Details – Report Query window from section 9.5.2 for displaying the results in **Table** format, make the following edits to display results in a **Bar Chart** grouped by **Policy**:
    a. From the **Report Type** list, select **Bar Chart**.
    b. From the **Show** list, select **Group by Policy.**
    c. From the **Sort By** list, select **Policy**.
    d. From the **Max Results** list, choose a number or type one in the field.

       Example: The value 6 means that our bar chart will display up to six policies, including but not limited to the number of policies displayed in the Table format.
    e. Click on the **Asc** (Ascending) radio button to set the sorting order.



Report Type : Bar Chart

Show : Group by Policy

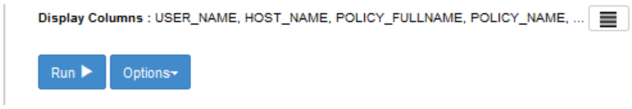
Sort By: Policy

● Asc ○ Desc

Max Results : 6

9.5.3.2 Running the Report Query

1. At the bottom of the Report Query pane, click Run to run the query

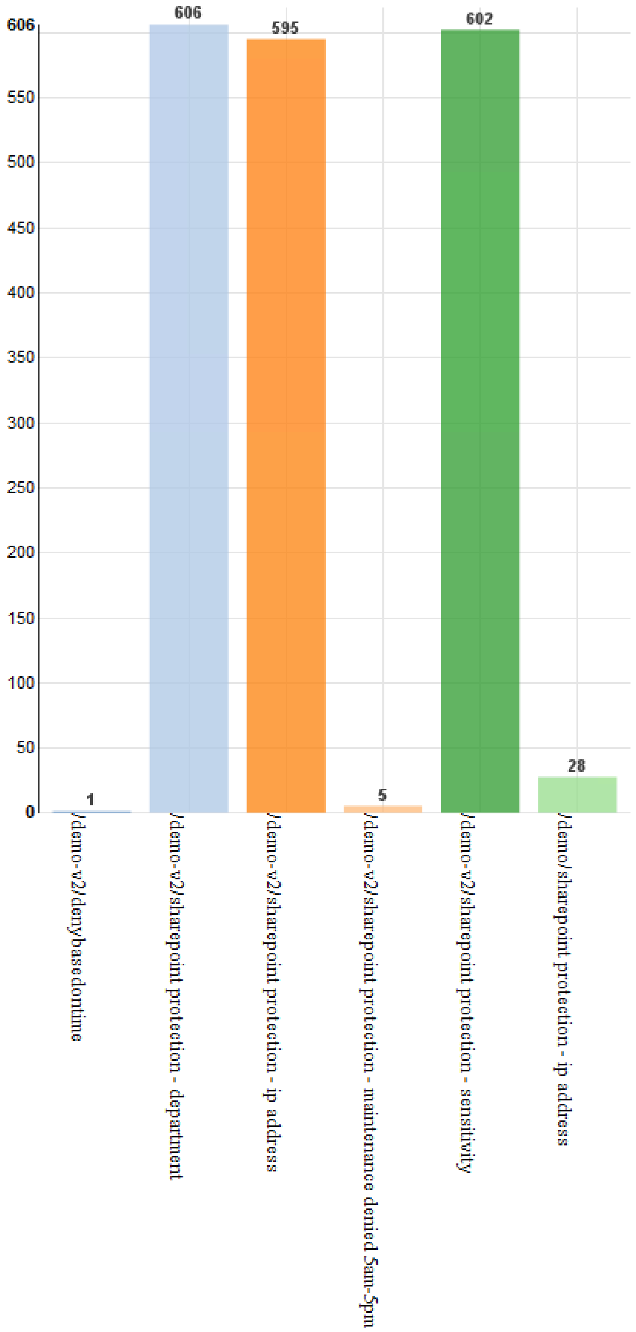


Display Columns : USER_NAME, HOST_NAME, POLICY_FULLNAME, POLICY_NAME, ...

9.5.3.3 Viewing the Results as a Bar Chart Grouped by Policy

1. In the same browser window, scroll down if necessary. Under the Run button, review the resulting Bar Chart Grouped by Policy.

   As illustrated below, hundreds of enforcement decisions were logged during the week, and the three most commonly evaluated policies include two that were included in the table from section 9.5.2, formatting results by Table.



9.5.4 Format: Bar Chart Grouped by User Chart

When the same data is grouped by user, and the bar chart is selected, the following chart is generated. As noted previously, the four policies were each triggered by a different user, so the graph shows four bars—each representing one user. Each is labeled with a user name. In this example, the bars are the same height, since each of the four users triggered a policy once.

9.5.4.1 Customizing the display settings

1. Using the same Report Details – Report Query window from the previous subsection, make the following edits to display results in a Bar Chart Grouped by Policy.

   a. From the **Report Type** list, select **Bar Chart**.

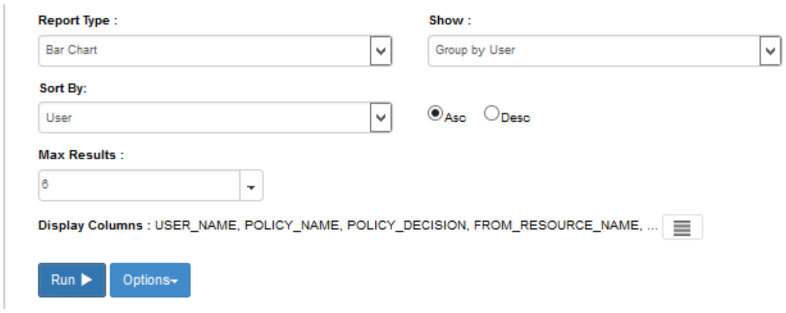
   b. From the **Show** list, select **Group by User**.

   c. From the **Sort By** list, select **User**.

   d. From the **Max Results** list, choose a number or type one in the field.

   Example: The value 6 indicates that this will be the maximum number of users reflected in our Bar Chart.

   e. Leave **Asc** selected.



Report Type : Bar Chart

Show : Group by User

Sort By: User

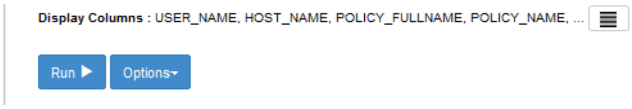
● Asc ○ Desc

Max Results : 6

Display Columns : USER_NAME, POLICY_NAME, POLICY_DECISION, FROM_RESOURCE_NAME, ...

9.5.4.2 Running the Report Query

1. At the bottom of the Report Query pane, click **Run** to run the query.



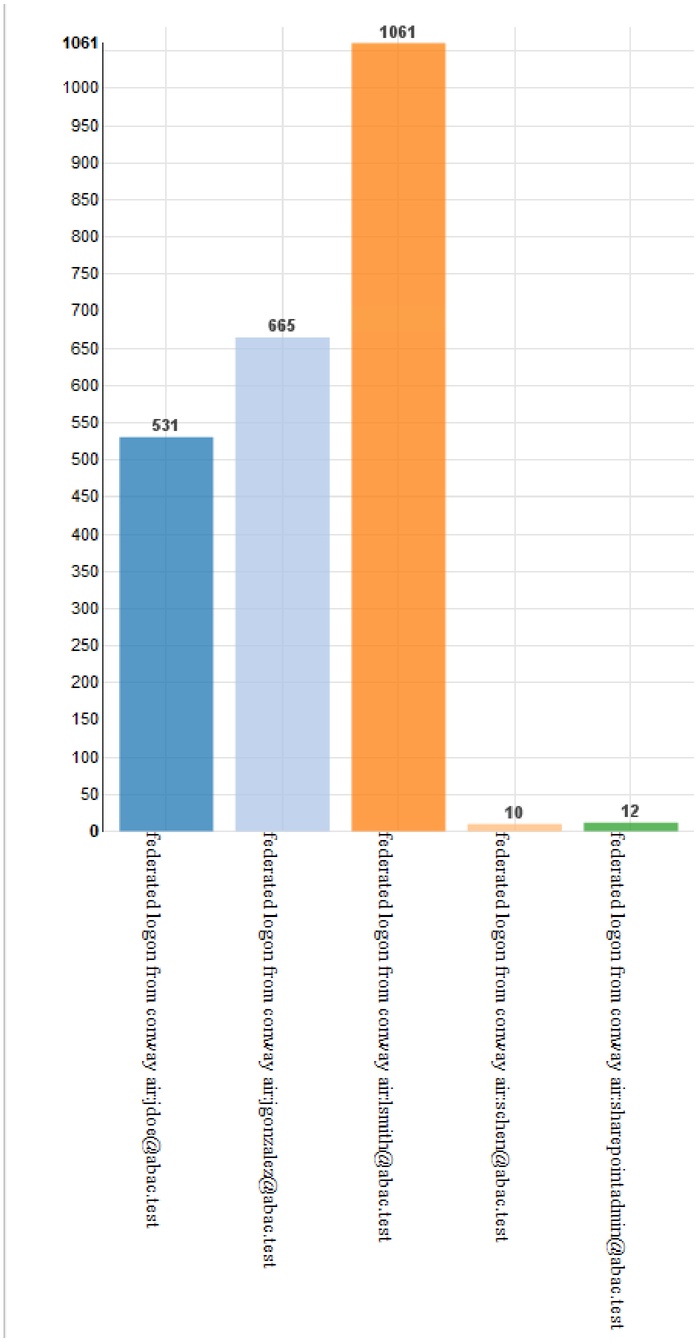
Display Columns : USER_NAME, HOST_NAME, POLICY_FULLNAME, POLICY_NAME, ...

9.5.4.3 Viewing the Results as a Bar Chart Grouped by User

1. In the same browser window, scroll down if necessary. Under the **Run** button, review the resulting Bar Chart Grouped by User:

   As illustrated below, only five users were accessing the protected RP SharePoint resources during this week period, and all logged in via federated identity from the IdP.

   - Two users had very minimal activity logged during this week: **schen@abac.test** and **sharepointadmin@abac.test**
   - Two users had relatively similar activity logged during this week: **jdoe@abac.test** and **jgonzalez@abac.test**
   - One user had an extremely large amount of activity logged during this week: **smith@abac.test**



9.5.5 Format: Pie Chart Grouped by Resource

The Group by Resource option shows the extent of specified events—in this case, policies being triggered—per individual resource covered by the report.

Because policies often cover large numbers of individual documents or other resources, grouping by resource is only helpful when the number of events has already been narrowed down to a smaller set by various report filters, such as policies or users. A pie charts is ideal here, because in the context of resource use, the relative access activity regarding some single file or other resource as compared to all others is generally of more interest than any absolute number of instances of access.

9.5.5.1 Customizing the Display Settings

1. Using the same Report Details – Report Query window from the previous subsection, make the following edits to display results in a Bar Chart grouped by Policy

   a. From the **Report Type** list, select **Pie Chart**.

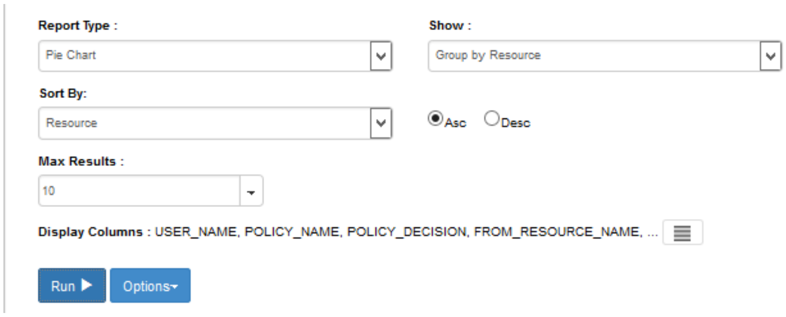
   b. From the **Show** list, select **Group by Resource**.

   c. From the **Sort By** list, select **Resource**.

   d. From the **Max Results** list, select a number or type one.

      Example: The value 10 means that will be the maximum number of resources displayed in our Pie Chart.

   e. Leave **Asc** selected.



Report Type : Pie Chart

Show : Group by Resource

Sort By: Resource

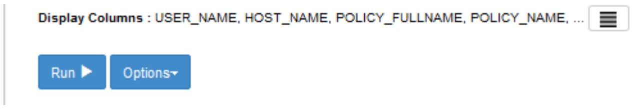
● Asc ○ Desc

Max Results : 10

Display Columns : USER_NAME, POLICY_NAME, POLICY_DECISION, FROM_RESOURCE_NAME, ...

9.5.5.2 Running the Report Query

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, ...

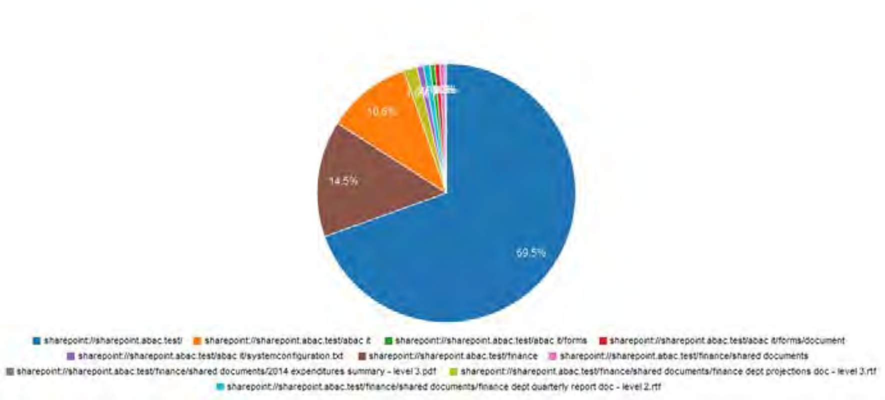
9.5.5.3 Viewing the Results as a Bar Chart Grouped by User

1. In the same browser window, scroll down if necessary. Under the **Run** button, review the resulting Bar Chart Grouped by Policy:

   As illustrated below, the maximum of ten resources are displayed in the pie chart.

   - 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 specific department sub-sites, such as Finance Dept Quarterly Reports, IT Dept System Configuration documents, etc.



9.6 Further Example Custom Reports from our Build

In this section we will illustrate how to define custom reports that will provide a graphical representation of particular kinds of activity that could be of interest to our RP business.

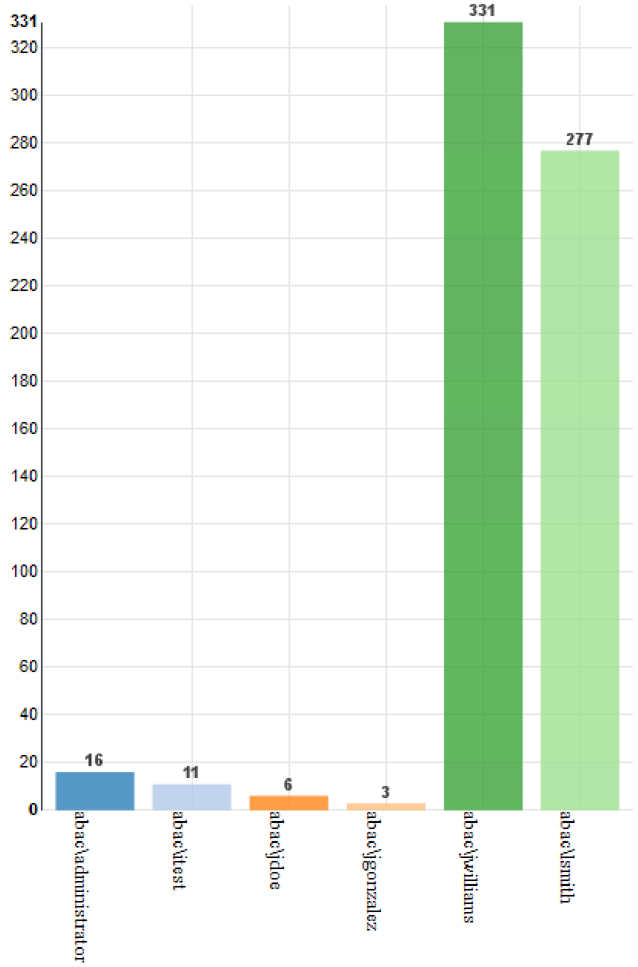
For our first additional example we will use a fictitious user from our build's IdP and check her activity on the RP SharePoint site within a specific time period. The report we define will focus on the user Lucy Smith (username: **lsmith**) and all of her Allowed and Denied access during a specific timeframe, such as May 1, 2015 – June 30, 2015.

For our second additional example we will use a document on the RP SharePoint site that has been marked with a metadata attribute called sensitivity. The document's sensitivity value is set to 3, which according to our example ABAC policies requires that 1) the user accessing the document belongs to the same or appropriate department for accessing it, 2) the access occurs during regular business hours Monday-Friday, and 3) the user has a clearance attribute value of Top Secret. The report we define will focus on the access attempts on that document for the months of May and June 2015.

9.6.1 Custom Report Illustrating One User's Access During Two Months

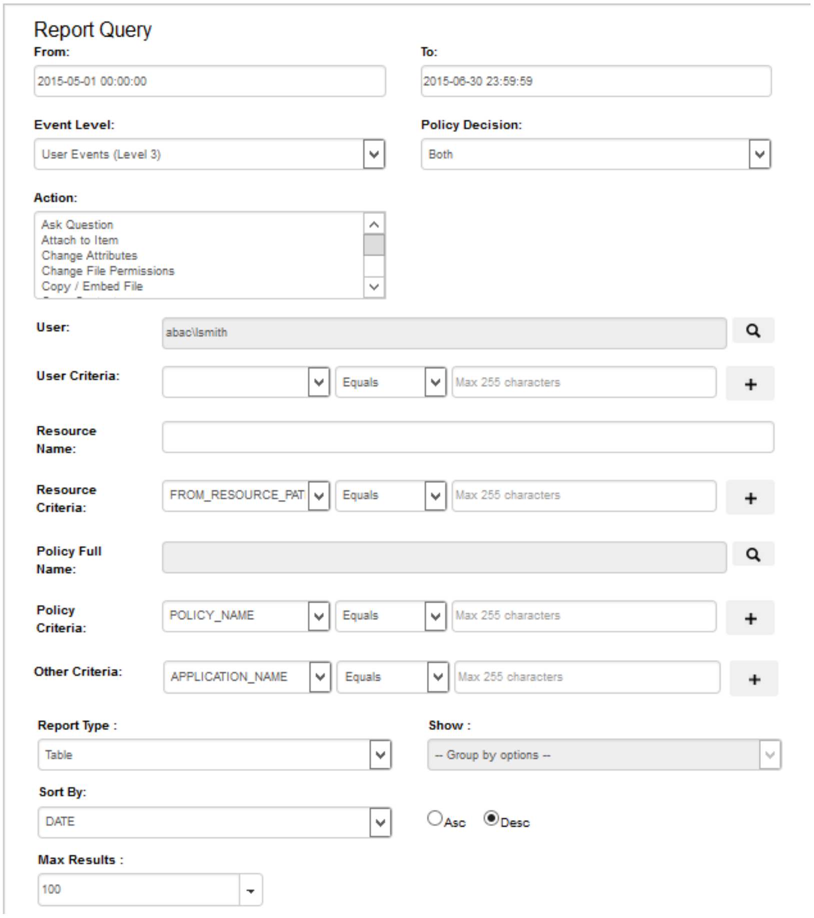
1. Follow the steps for section 9.5.4, Format: Bar Chart Grouped by User, and change the **From** field to May 1, 2015 and the **To** field to June 30, 2015.
2. Within the browser, in the results area at the bottom of the Report Details window, click on the vertical bar that represents the user **smith@abac.test** or **abac\lsmith** (light green, the far-right bar in our chart below).

   The Report window of your browser will automatically refresh, and a default query on the User will run automatically.



3. Within the browser window, scroll up to Report Details and verify that the User: field was automatically populated with **abac\lsmith**.

   In the Report Query pane you will see that the default query pertaining to the User has a Report type of Table, sorted by date in descending order, with a maximum of 100 results.



Report Query

From: 2015-05-01 00:00:00

To: 2015-06-30 23:59:59

Event Level: User Events (Level 3)

Policy Decision: Both

Action:

User: abac\lsmith

User Criteria: Equals | Max 255 characters

Resource Name:

Resource Criteria: FROM_RESOURCE_PAT | Equals | Max 255 characters

Policy Full Name:

Policy Criteria: POLICY_NAME | Equals | Max 255 characters

Other Criteria: APPLICATION_NAME | Equals | Max 255 characters

Report Type : Table

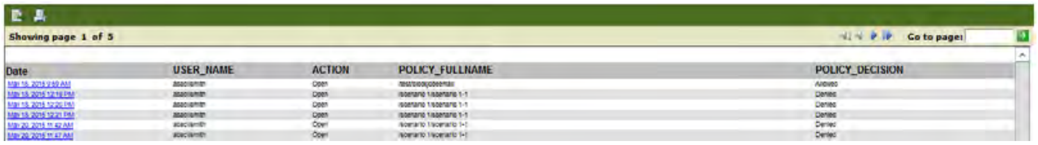
Show : -- Group by options --

Sort By: DATE ○ Asc ● Desc

Max Results : 100

4. Within the browser window, scroll back down to the resulting Table to review its data. See the excerpt below.

   If desired, you can change the Display Columns, Report Type, etc. to customize your view as illustrated in previous subsections.



Showing page 1 of 5 | Go to page:

Date	USER_NAME	ACTION	POLICY_FULLNAME	POLICY_DECISION
May 18, 2015 9:49 AM	abac\lsmith	Open	[illegible]	Allowed
May 18, 2015 12:19 PM	abac\lsmith	Open	/scenario 1/scenario 1-1	Denied
May 18, 2015 12:20 PM	abac\lsmith	Open	/scenario 1/scenario 1-1	Denied
May 18, 2015 12:21 PM	abac\lsmith	Open	/scenario 1/scenario 1-1	Denied
May 20, 2015 11:42 AM	abac\lsmith	Open	/scenario 1/scenario 1-1	Denied
May 20, 2015 11:47 AM	abac\lsmith	Open	/scenario 1/scenario 1-1	Denied

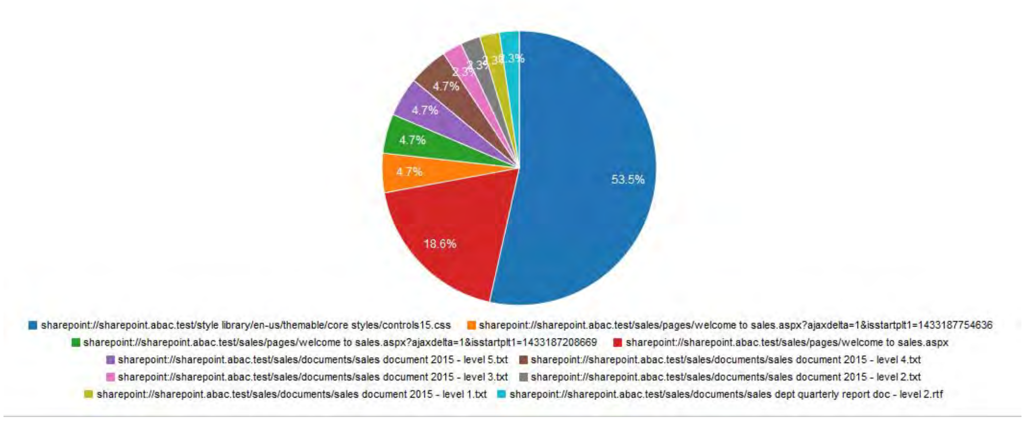
9.6.2 Viewing Access Attempts on Individual Resources

This section provides instructions for creating a custom report that shows the access attempts of a single resource for a period of two months.

1. Follow the steps for section 9.5.5, Format: Pie Chart Grouped by Resource, and change the **From** field to May 1, 2015 and the **To** field to June 30, 2015.
2. From the resulting list of resources under the pie chart, find the color of a resource with a name including **level 3**, which according to our schema means in SharePoint metadata the sensitivity level attribute is equal to 3.

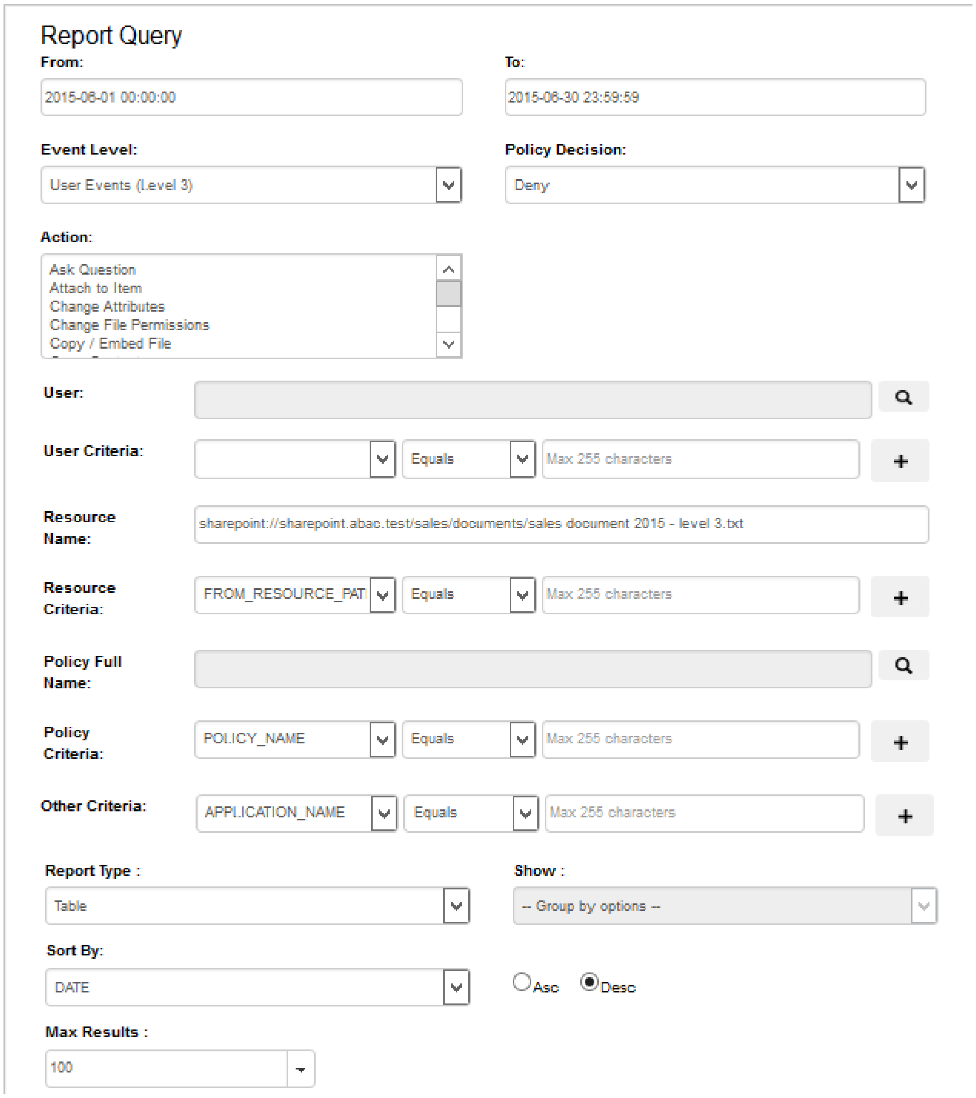
3. Click on that resource in the pie chart (example: light pink area of 2.3% is for a Sales Dept document called **sales document 2015 – level 3.txt**).

   This will begin an automatic default query for that resource similar to the one done above based on the user lsmith.



4. Within the browser window, scroll up to Report Details and verify that the Resource Name: field was automatically populated with the name **Sales document 2015 – level 3.txt**.

   In the Report Query pane, you will see that the default query pertaining to the resource has a Report type of Table, sorted by date in descending order, with a maximum of 100 results.

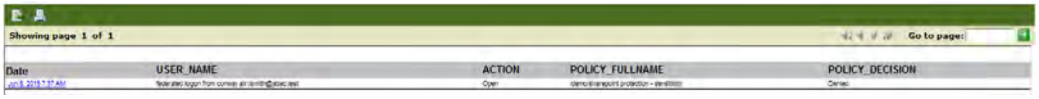


Report Query

From:	2015-06-01 00:00:00
To:	2015-06-30 23:59:59
Event Level:	User Events (Level 3)
Policy Decision:	Deny
Action:	Ask Question Attach to Item Change Attributes Change File Permissions Copy / Embed File
User:	
User Criteria:	Equals · Max 255 characters
Resource Name:	sharepoint://sharepoint.abac.test/sales/documents/sales document 2015 - level 3.txt
Resource Criteria:	FROM_RESOURCE_PAT · Equals · Max 255 characters
Policy Full Name:	
Policy Criteria:	POLICY_NAME · Equals · Max 255 characters
Other Criteria:	APPLICATION_NAME · Equals · Max 255 characters
Report Type :	Table
Show :	-- Group by options --
Sort By:	DATE ○ Asc ● Desc
Max Results :	100

5. Within the browser window, scroll back down to the resulting table to review its data. See the excerpt below.

   If desired, you can change the Display Columns, Report Type, etc. to customize your view as illustrated in previous subsections.



Showing page 1 of 1 Go to page:

Date	USER_NAME	ACTION	POLICY_FULLNAME	POLICY_DECISION
Jun 8, 2015 7:37 AM	federated logon from corresp ... smith@abac.test	Open	demo/sharepoint protection - [illegible]	Denied

10 Configuring a Secondary Attribute Provider

10.1 Introduction

This chapter provides a description of the architecture, compilation, and deployment instructions for a secondary attribute provider and its components, which we describe as a custom Policy information point (PIP), to be included as part of the ABAC infrastructure. We also demonstrate how to configure the Relying Party server to accommodate the custom PIP and its component JIT provisioning mechanism.

The secondary attribute provider comes into the picture when a user tries to access a resource at the Relying Party's Resource Provider, and the Policy decision point (PDP) finds that an essential attribute needed to make the access control decision is missing from the initial set of attributes sent from the Identity Provider. In our build, this would mean a user with a federated identity (via PingFederate Identity Provider, IdP, augmented with two-factor authentication by RSA AA) has already logged into Microsoft SharePoint (Relying Party's Resource Provider), but when trying to open a particular resource on the site, the NextLabs Policy Controller (PDP) makes a run-time decision that additional subject attributes are needed before the access decision can be made. The PDP determines this while evaluating the existing ABAC policies (created in the NextLabs Policy Studio, PAP in our ABAC build) against the user, resource, and environmental attributes at play at the time of requested access.

Providing the secondary attribute collection capability in our build required the implementation of new components and related features, which we will describe more in detail later in the chapter:

- NextLabs Policy Information Point (PIP) Plugin to extend the NextLabs Policy Controller (PDP) when additional attribute(s) are needed
- Protocol broker to initiate and receive a SAML attribute query and SAML response
- Custom data store plugin for PingFederate on the Relying Party (RP) server which will cache attributes in order to limit the number of secondary requests to the PingFederate Identity Provider (IdP) server
- Apache Directory Server (ApacheDS), an LDAP in which PingFederate can create and update local user accounts and associated attributes based on the attributes contained in SAML assertions received after authentication from IdP
- PingFederate RP configuration must be modified so that it can serve as an IdP as needed, such as when checking its JIT cache (Apache DS LDAP) before sending requests to the IdP

In later sub-sections of this chapter we will discuss in detail the purpose of each of these new components and features, and how they are developed, configured, compiled, and deployed.

Note: The custom PIP we have developed involves new custom components, open source components, and commercially available components. For open source and commercial components, the related descriptions in this chapter have been limited to installation and relevant configuration required for the desired functionality of our build. If you are interested in other details or additional capabilities of this software, explore the referenced product literature or contact that organization.

10.1.1 Prerequisites

In order to follow the instructions of this chapter, it is necessary that seven of the previous How-To sections have been successfully completed. The required components that must be installed and configured before continuing in this chapter include:

1. Installation and Configuration of Active Directory (Chapter 2)
2. Installation and Configuration of RSA AA (Chapter 2)
3. Installation and Configuration of RSA AA Plugin (Chapter 2)
4. Installation and Configuration of PingFederate on both the RP and IdP federation servers (Chapter 2 and Chapter 3),
5. Installation and Configuration of Microsoft SharePoint (Chapter 4 and Chapter 5)
6. Configuration of the attribute flow (Chapter 6)
7. Installation and Configuration of NextLabs Control Center, Policy Studio, Policy Controller, and Entitlement Manager for SharePoint Server (Chapter 7)

10.1.2 Criteria for Secondary Attribute Collection

At the time of ABAC policy evaluation, required attributes may not be available or the system may not find it appropriate to use for various reasons, including, but not limited to:

- For security and privacy purposes it is not ideal to acquire all known attributes for a subject when the session is created. Some attributes maybe PII or of higher sensitivity and should not be sent to the Relying Party until an access request made by the user requires those attributes.
- Depending on the longevity of a session, attributes risk becoming stale. Because of this potential for staleness, it is essential to procure attributes as needed, depending on the freshness criteria established by the system. The freshness of attributes is sometimes guided by the policies established for a local cache.
- The attribute needed for a specific attribute request may not an attributed owned by the Identity provider but rather may need to be acquired from an external party attribute provider.

10.1.3 Components

The custom PIP described in this chapter is composed of four new components and mechanisms which interact or integrate with different existing components in our ABAC build as extensions, plugins, or web applications:

- **NextLabs Plugin**: This plugin extends the NextLabs Policy Controller to make attributes available based on the criteria mentioned in section 10.1.2, when the PDP determines that attribute values needed to evaluate an ABAC policy are insufficient or unavailable. Following the recommendation in the software development framework provided by NextLabs, the NCCoE implemented this PIP plugin in Java, and deployed the plugin within the NextLabs Policy Controller software architecture on the server we call SharePoint server in our build. Due to the requirements of the Policy Controller architecture, the plugin can request the values of multiple missing attributes sequentially, one at a time.

- **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.

10.1.3.1 Sequence Diagram of Custom PIP Component Interactions

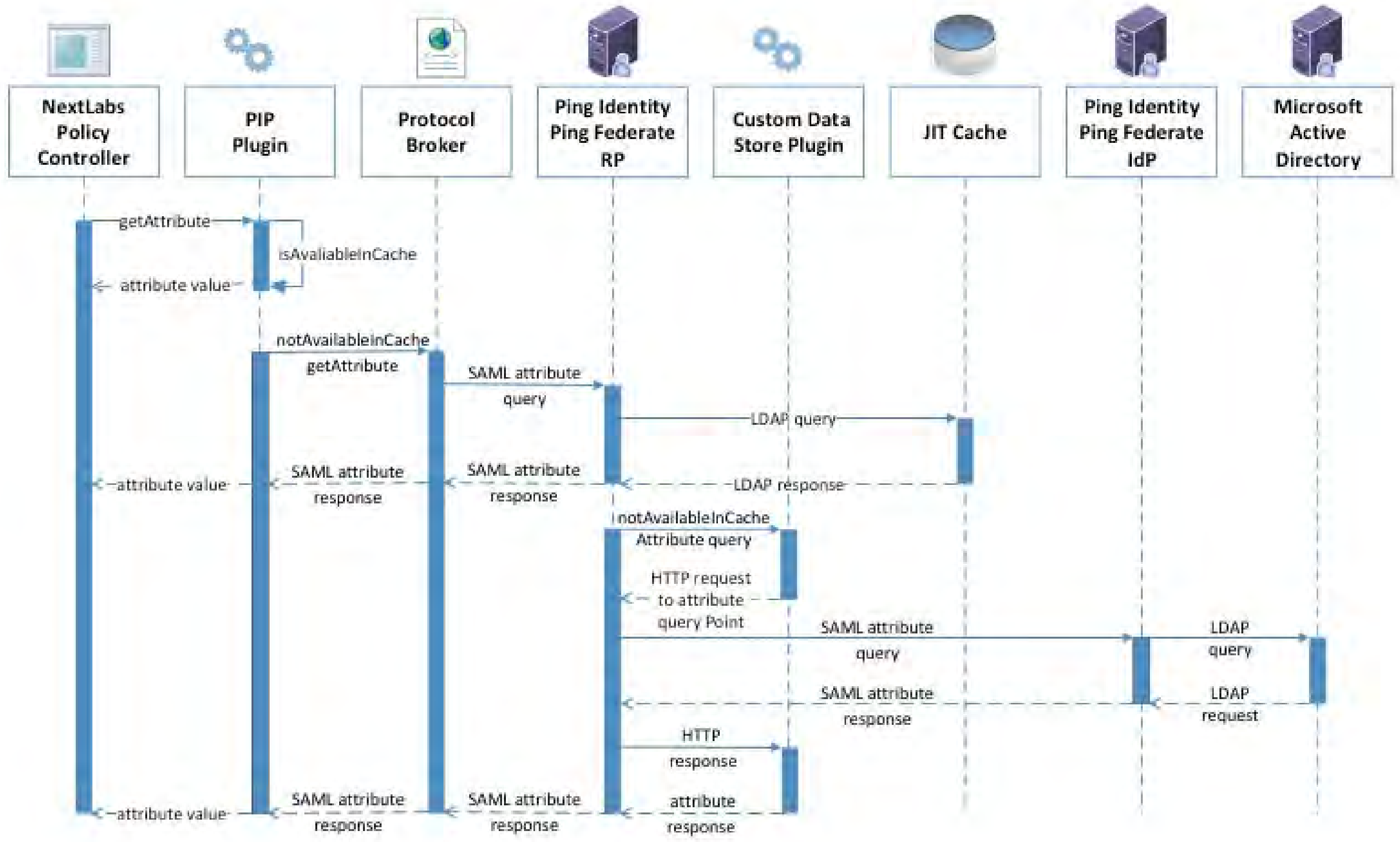


Figure 10.1 Architecture

Description

Nextlabs PDP (Policy Controller) is the arbitrator for all access decisions at the SharePoint portal. It controls access to SharePoint URL(s) by evaluating rules against the attributes of the entities (subject and object), actions, and the environment relevant to a request. It may be possible that the attribute required for the decision is not available at run time. In that case, it looks for the registered plugin that will fetch the attribute using the following flow:

1. When the policy controller does not receive the attributes required to make a decision, a secondary attribute request will be initiated by calling the PIP Plugin.
2. PIP Plugin is a registered plugin with the NextLabs Policy Controller. It implements the interface dictated by the NextLabs software. By virtue of this implementation, it receives the subject and name of the attribute that is required for the policy decision.
3. When the subject and attribute name are received, the PIP Plugin checks its local short-term cache (in this build, configured to hold values for two seconds) to see if the needed attribute for the subject was recently requested.
4. If the attribute is still in cache, the value is returned to the Policy Controller. If the value is not in cache, the PIP Plugin initiates an HTTPS request to the Protocol Broker.
5. The Protocol Broker receives the attribute name and subject from the HTTPS request and forwards them as a signed SAML 2.0 Attribute Query to PingFederate-RP on a channel protected by mutual TLS.
6. Once PingFederate-RP receives the SAML 2.0 attribute query, it sends an LDAP request to the JIT cache to see if the attribute was previously queried in a secondary request.
7. If the subject does not have the attribute value assigned in the JIT cache, PingFederate-RP will forward the subject and attribute name to the Custom Data Store plugin. The Custom Data Store plugin acts as a pointer back to the PingFederate-IdP. To do this, the Custom Data Store dispatches an HTTPS request to the PingFederate-RP with the PingFederate-IdP as the attribute query point.
8. Ping Federate uses an HTTPS query to form a SAML 2.0 attribute query and dispatch it to the Ping Federate at the IdP.
9. The Ping Federate at the IdP accepts the SAML 2.0 request, verifies if the user has the attribute of need, and replies back to the PingFederate-RP with a SAML 2.0 response.
10. PingFederate-RP validates the SAML 2.0 response, retrieves attribute values, and responds to the original Custom Data Store HTTP request with the attribute values.
11. The Custom Data Store then responds to the PingFederate-RP attribute request with an attribute response.
12. The PingFederate-RP constructs a SAML 2.0 response and sends it to the Protocol Broker.
13. The Protocol Broker retrieves the attribute or exception from the SAML 2.0 response and forwards it to the NextLabs plugin, which passes the attribute or exception back to the Policy Controller.

155 10.2 Component Software and Hardware Requirements

156

Component	Server where component is installed	Compilation method	Required software or hardware	Operating System	Optional software
Ping Custom Data Store	PingFederate RP server	Ant 1.9.2	PingFederate 7.3.2; Java version same as PingFederate installed	Windows Server 2012	
NextLabs Plugin	SharePoint server	Apache Maven 3.2.5	SharePoint 2013; NextLabs Entitlement Manager for SharePoint Server, NextLabs Policy Controller, NextLabs Control Center, NextLabs Policy Studio; SQL Server 2012; Java version same as NextLabs Policy Controller installed (1.6)	Windows Server 2012	BareTail (used here as a log file annotator)Copyright Bare Metal Software Pty Ltd. Download 05/22/2015.
Protocol Broker	SharePoint server	Apache Maven 3.2.5	PingFederate 7.3.2; SharePoint 2013; NextLabs Entitlement Manager for SharePoint Server, NextLabs Policy Controller, NextLabs Control Center, NextLabs Policy Studio; SQL Server 2012;	Windows Server 2012	
Apache Directory Server		N/A	PingFederate 7.3.2; Java 7.0 (recommended by Oracle's JDK. Some issues have been reported with Java 8); 384 MB of memory by default, can be changed using Apache Directory Studio (included)	Windows Server 2012	

10.3 Ping Custom Data Store

10.3.1 Functionality and Architecture

This data store was developed according to the guidelines from the Ping Identity provided here. It has three functionalities:

- Configuration
  - HttpConfig class is used to read in a configuration file for the custom data store. Configuration parameters, like truststore location, password and attribute names can be defined in a file and read in as a configuration by HttpConfig class. The structure of the HttpConfig class configuration is based on spring annotation.
  - Other sets of configuration can be read via a web interface. A detailed description of these parameters is provided in step 9 of section 10.3.4 in this How-To guide.
- Communication
  - Similarly, dispatching the http request relies on PingClient class. PingClient uses classes under the spring http package. PingClient sends an https query to Attribute Query End Point. All of the parameters for the https URL are provided by the web interface.
- Custom Data Store
  - CustomDataStore is a class that implements com.pingidentity.sources.CustomDataSourceDriver.
  - It implements all methods specified by the contract, i.e.:
    - boolean testConnection(): This method tests whether a host and port is reachable or not. It is assumed that if host and port is reachable, a URL will be available.
    - java.util.List<java.lang.String> getAvailableFields():
    - java.util.Map<java.lang.String,java.lang.Object> retrieveValues(java.util.Collection<java.lang.String> attributeNamesToFill, SimpleFieldList filterConfiguration)

The Class Structure and their interactions are provided in the Interaction Diagram and Class Diagram.

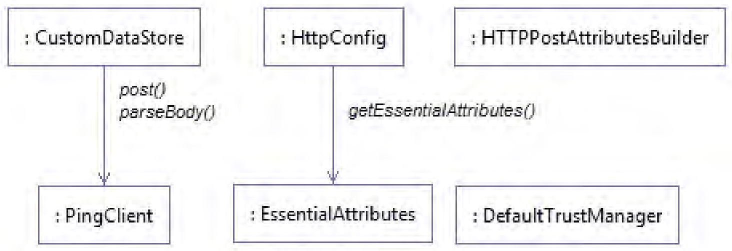


Figure 10.2 Ping Custom Data Store Interaction Diagram

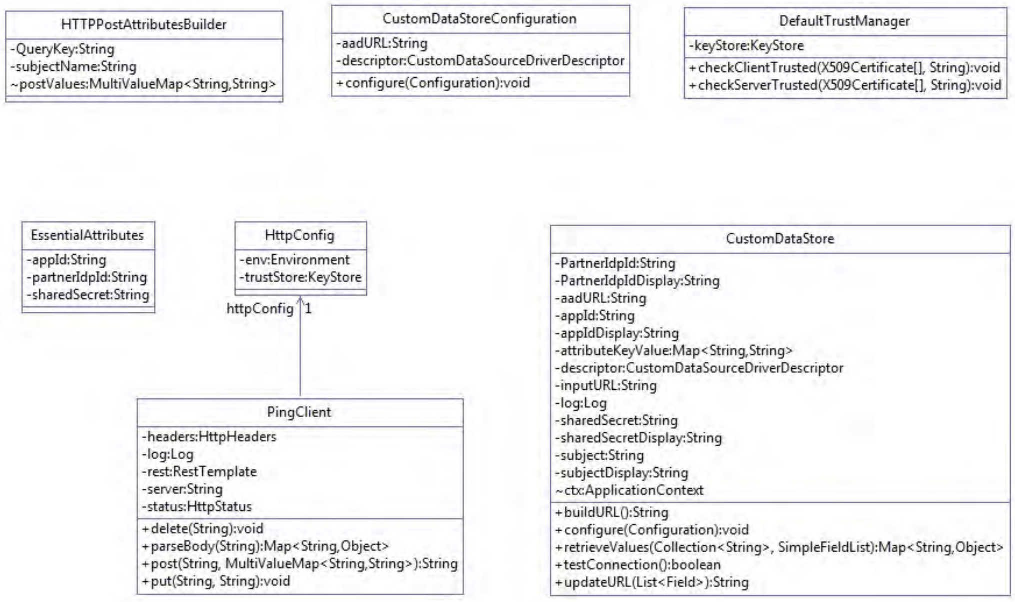

HTTPPostAttributesBuilder
-QueryKey:String
-subjectName:String
~postValues:MultiValueMap<String,String>
CustomDataStoreConfiguration
-aadURL:String
-descriptor:CustomDataSourceDriverDescriptor
+configure(Configuration):void
DefaultTrustManager
-keyStore:KeyStore
+checkClientTrusted(X509Certificate[], String):void
+checkServerTrusted(X509Certificate[], String):void
EssentialAttributes
-appId:String
-partnerIdpId:String
-sharedSecret:String
HttpConfig
-env:Environment
-trustStore:KeyStore
httpConfig
1
PingClient
-headers:HttpHeaders
-log:Log
-rest:RestTemplate
-server:String
-status:HttpStatus
+delete(String):void
+parseBody(String):Map<String,Object>
+post(String, MultiValueMap<String,String>):String
+put(String, String):void
CustomDataStore
-PartnerIdpId:String
-PartnerIdpIdDisplay:String
-aadURL:String
-appId:String
-appIdDisplay:String
-attributeKeyValue:Map<String,String>
-descriptor:CustomDataSourceDriverDescriptor
-inputURL:String
-log:Log
-sharedSecret:String
-sharedSecretDisplay:String
-subject:String
-subjectDisplay:String
~ctx:ApplicationContext
+buildURL():String
+configure(Configuration):void
+retrieveValues(Collection<String>, SimpleFieldList):Map<String,Object>
+testConnection():boolean
+updateURL(List<Field>):String

Figure 10.3 Ping Custom Data Store Class Diagram

10.3.2 Deploying the Ping Custom Data Store

Note: PingFederate administrator's manual provides detailed steps for every platform. In our build, we used the Windows Server 2012 platform.

1. Log on to the PingFederate RP server.
2. Click on the Windows icon and begin typing **Services**.
3. Double-click the Services application icon.
4. Click on the Name column to sort by alphabetical order, and look for **PingFederateService**.
5. If the status column reads **running**, right-click on **PingFederateService** and click **Stop**.
6. Prepare environment based on PingFederate documentation. This may involve going to

   `../pingfederate-7.3.0/pingfederate/sdk` folder
7. Click on the Windows icon and begin typing **Cmd**.
8. Double-click the icon to open the Command Prompt.
9. In Command Prompt, navigate to your installation of PingFederate and its sdk folder by typing the following command and pressing Enter. Example: **cd** **`C:/pingfederate-7.3.0/pingfederate/sdk/`**
10. Within the sdk folder, locate **build.local.properties** and open it with your default text editor. For example, enter the following command and press Enter: **notepad build.local.properties**
11. In your default text editor (Notepad in our example), set or update **target-plugin.name** to **idp-query-data-store**, i.e.,

```
# Please set the 'target-plugin.name' property to the name of the directory (under plugin-src) that

# contains the source code of the plugin you want to build.

target-plugin.name=idp-query-data-store
```

12. Within the Command Prompt window, navigate to your **idp-query-data-store** folder by entering a cd command with a path to your **idp_query_data_store** and pressing Enter. Example: **cd `C:/--path-to-your-idp_query_data_store`**
13. Within the Command Prompt window, copy **idp-query-data-store** along with all subfolders to your PingFederate installation's **sdk/plugin-src** folder by entering a cp command and pressing Enter. Example: **cp -rf idp_query_data_store `C:/pingfederate-7.3.0/pingfederate/sdk/plugin-src`**
14. Within the Command Prompt window, run the following command and press enter in order to make sure all relevant subfolders exist: **ls -ltr ./idp-query-data-store/**
    - Example results from the above command:

```
total 4
drwxrw-r--. 3 t… t….  16 Apr 29 11:34 java
drwxrw-r--. 2 t… t…. 4096 Apr 29 12:59 lib
drwxrwxr-x. 4 t… t…. 30 May 15 17:52 build
drwxrw-r--. 2 t… t….51 May 29 09:26 conf
```

10.3.3 Compilation

The Building and Deploying with Ant chapter of the SDK Developer's Guide by Ping provides a detailed description of compiling and deploying the project using Apache Ant. For current deployment it may be sufficient.

1. Click on the Windows icon and begin typing the word **Cmd**.
2. Double-click the icon to open the Command Prompt.
3. It is essential to know about the attributes that this data store will return. PingFederate calls the getAvailableFields() method to determine the available fields that could be returned from a query of this data source. These fields are displayed to the PingFederate administrator during the configuration of a data source lookup. The administrator can then select the attributes from the data source and map them to the adapter or attribute contract. PingFederate requires at least one field returned from this method.
4. To change it, go to your ping installation directory. From that directory, navigate to **`..\pingfederate-7.3.0\pingfederate\sdk\plugin-src\idp-query-data-store\conf`**. Open **`.\config.properties`** with your favorite editor. Change the value for the attribute called **NameOfAttributes:**

```
NameOfAttributes=fullname,username,stafflevel,role,division,employe
r,clearance
```

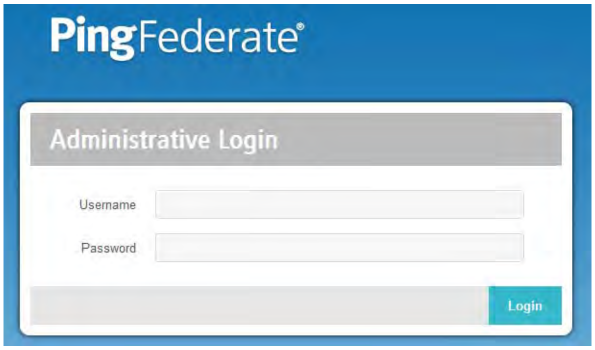
Use a comma to separate attribute names. More attributes can be added by adding subsequent commas and attribute names.

5. Navigate to your PingFederate sdk folder, i.e., **`cd C:/pingfederate-7.3.0/pingfederate/sdk/`**
6. Within the Command prompt window, type the following compilation command and press Enter: **`ant deploy-plugin`**

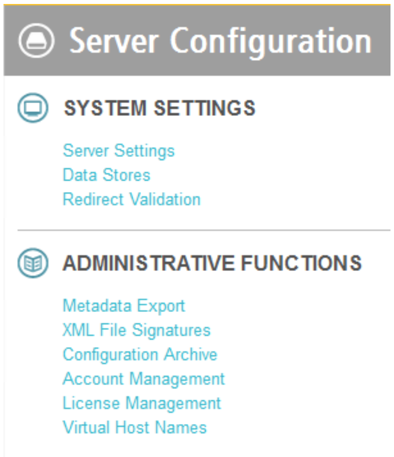
10.3.4 Configuration within PingFederate Administrative Console

The end of successful execution of ant deploy-plugin signals the installation of the data-store driver. Its configuration is provided in detail by Ping documentation. In summary, it spans the following process:

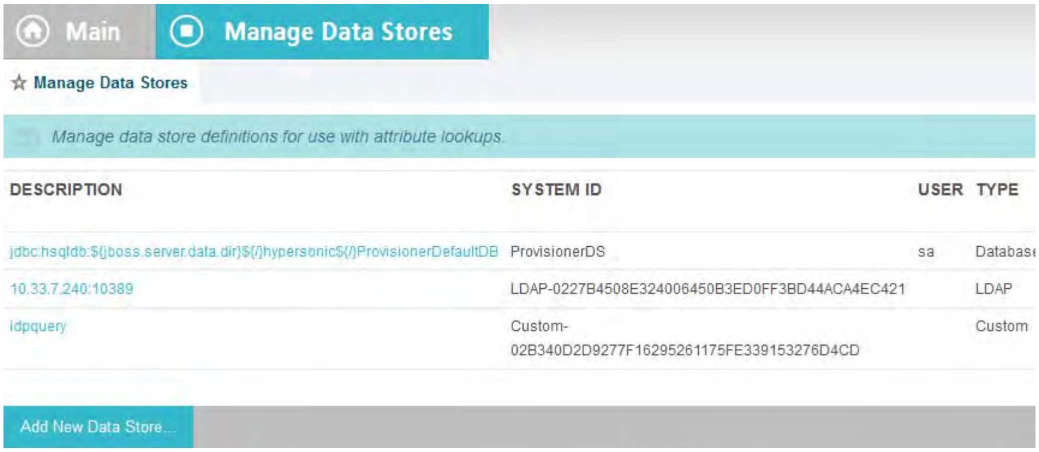
1. Log on to the Ping RP server.
2. Open an internet browser.
3. Enter the following URL and press Enter: **https://localhost:9999/pingfederate/app**
4. Enter your PingFederate administrator username and password, then click **Login**.



5. In the browser window, under the **Main** menu area, find **Server Configuration->System Settings->Data Stores**. Double-click on **Data Stores**.



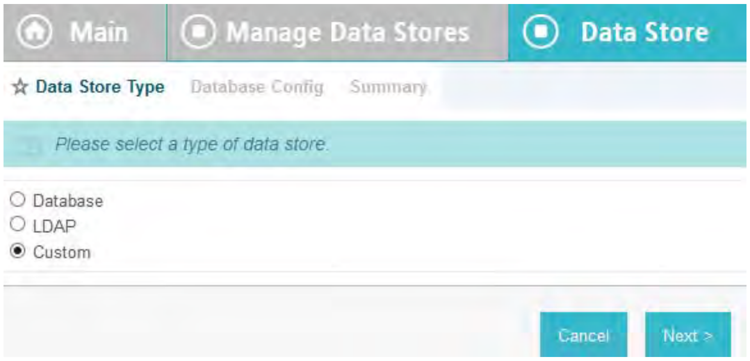
6. At the bottom of the browser window, click **Add New Data Store**.



Manage data store definitions for use with attribute lookups.

DESCRIPTION	SYSTEM ID	USER	TYPE
jdbc:hsqldb:${jboss.server.data.dir}${/}hypersonic${/}ProvisionerDefaultDB	ProvisionerDS	sa	Databas
10.33.7.240:10389	LDAP-0227B4508E324006450B3ED0FF3BD44ACA4EC421		LDAP
idpquery	Custom-02B340D2D9277F16295261175FE339153276D4CD		Custom

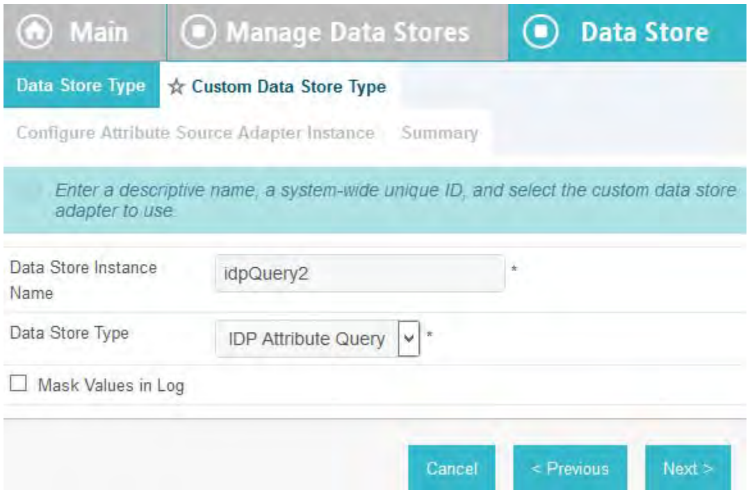
7. On the Data Store Type screen, select **Custom** and click **Next**.



Please select a type of data store.

○ Database
○ LDAP
● Custom

8. On the Custom Data Store Type screen, specify **Data Store Instance Name** and **Data Store Type**. The name can be arbitrary, but you must select **IDP Attribute Query** from the **Data Store Type** drop-down. Click **Next**.



Enter a descriptive name, a system-wide unique ID, and select the custom data store adapter to use

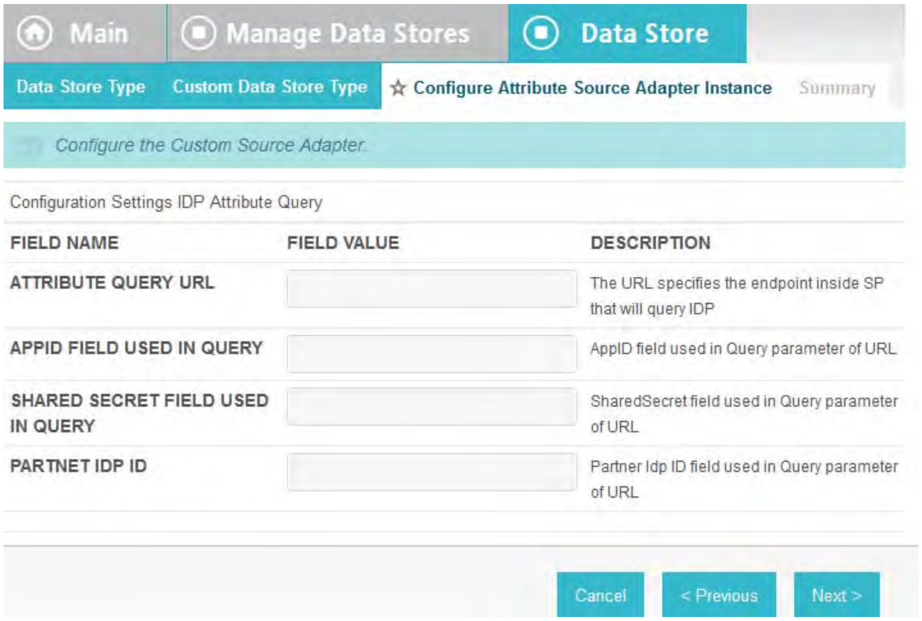
Data Store Instance Name	idpQuery2 *
Data Store Type	IDP Attribute Query *

□ Mask Values in Log

9. To configure the data store, the following parameters must be configured. These parameters are guided by the requirements of the end point (/sp/startAttributeQuery.ping) defined by Ping documentation here:

   https://10.33.7.5:9031/sp/startAttributeQuery.ping?AppId=appid&SharedSecret=3Federate&PartnerIdpId=https://idp.abac.test:9031&Subject=lsmith@abac.test

   - **Attribute Query URL**: the URL specifying the endpoint inside RP (Relying Party) that will query the IDP, i.e., **`https://rp.abac.test:9031/sp/startAttributeQuery.ping`**
   - **AppId field used in query**: the unique identity of the initiating application, i.e., **`appid`**
   - **Shared Secret field used in query**: used to authenticate the initiating application. The AppId and SharedSecret must both match the application authentication settings within the PingFederate server, i.e. **`!23234Federate`**
   - **Partner IDP ID**: used to identify the specific IdP partner to which the Attribute Query should be sent. If this parameter is not present, the Subject and Issuer are used to determine the correct IdP, i.e., **https://idp.abac.test:903**



Configure the Custom Source Adapter.

Configuration Settings IDP Attribute Query

FIELD NAME	FIELD VALUE	DESCRIPTION
ATTRIBUTE QUERY URL		The URL specifies the endpoint inside SP that will query IDP
APPID FIELD USED IN QUERY		AppID field used in Query parameter of URL
SHARED SECRET FIELD USED IN QUERY		SharedSecret field used in Query parameter of URL
PARTNET IDP ID		Partner Idp ID field used in Query parameter of URL

10.4 NextLabs PIP Plugin

10.4.1 Architecture

The NextLabs Control Center can support custom PIP plugin extensions for dynamic user and resource attribute retrieval during runtime. In order to install and deploy a PIP plugin such as the one described in this section, it is necessary to have previously installed and deployed the NextLabs Control Center, Policy Controller, Policy Studio, and the NextLabs Entitlement Manager (Chapter 7).

According to the NextLabs PDP Policy Extension documentation, which is only available to NextLabs customers at this time, one method for leveraging this PIP extension capability is by way of a getAttribute() function within a UserAttrProviderMod class. The PIP Plugin implements methods defined by the ISubjectAttributeProvider interface. The ISubjectAttributeProvider interface declares the method getAttribute() function which enables querying for a single subject attribute sequentially until all missing required attributes have been requested.

10.4.1.1 Required classes of the NextLabs PIP Plugin:

- UserAttrProviderMod class must exist and must contain a getAttribute() function.
  - The getAttribute() function must accept two arguments (IDSubject and String) and return an EvalValue. The EvalValue is created using its build() function and the attribute value ultimately returned from the Protocol Broker (see section 10.5, Protocol Broker).
- HTTPSTransmitter class
  - makes an HTTPS request to the Protocol Broker using a doPost() function
- CacheKey class, implementing a local Ehcache

  - The CacheKey class constructor takes two parameters, the subjectId and the attributeName, which serve as a compound cache key for storing and retrieving the value of a given user's attribute within the plugin's local Ehcache.

10.4.1.2 Other Required Files or Deployment Notes:

- The three above classes must be compiled into a .jar file.
  - Our method of compilation in this build was using Apache Maven 3.2.5. Maven compilations are directed by a pom.xml ("Project Object Model"), which is an XML representation of a Maven project. More information about Apache Maven and its pom file requirements can be found here: https://maven.apache.org/pom.html
  - According to NextLabs support, be sure to include within the pom.xml file configuration a statement that specifies the Provider-Class. The Provider-Class is the UserAttrProviderMod class that contains the getAttribute() method. Example pom.xml excerpt from the pom.xml file in this implementation:

```
<configuration>
 <archive>
  <manifest>
<mainClass>nist.pdpplugin.UserAttrProviderMod</mainClass>
  </manifest>
      <manifestEntries>
   <Provider-Class>nist.pdpplugin.UserAttrProviderMod</Provider-Class>
      </manifestEntries>
 </archive>
</configuration>
```

- Also required per NextLabs support documentation, for any custom plugin you must include a .properties file.
  - The configuration file should end with the ".properties" file extension. Example from this implementation: **nlsamlpluginService.properties**
  - Contents should be similar to our example copied below. You must include a **category = ADVANCED CONDITION** statement per NextLabs deployment and loading requirements:

```
name = NLSAMLPlugin_Service
jar-path = [NextLabs]/Policy Controller/jservice/jar/nlsamlplugin/NLSAMLPlugin-0.0.1-SNAPSHOT-jar-with-dependencies.jar
friendly_name = NLSAMLPlugin Service
description = NLSAMLPlugin Service
```

10.4.1.3 Notes on Jar and Properties File Deployment within NextLabs Policy Controller Software Architecture:

- The jar file containing the three classes must be deployed on the SharePoint server within the NextLabs Policy Controller software architecture in a specific location. Under the **C:/Program Files/NextLabs/Policy Controller/jservice/jar** folder you must create a folder specifically for your custom jar, i.e., **C:/Program Files/NextLabs/Policy Controller/jservice/jar/custom_jar_folder_you_create**
- Any other required supporting jars can be compiled within the same jar as the UserAttrProviderMod class and other classes deployed as described in the previous step.
  - Otherwise, any additional required supporting jars can be compiled into a separate jar which is deployed elsewhere within the NextLabs Policy Controller software architecture on the SharePoint server, i.e., **C:/Program Files/NextLabs/Policy Controller/jre/lib/ext/**
- The properties file must be deployed on the SharePoint server within the NextLabs Policy Controller software architecture in a specific location, under the **C:/Program Files/NextLabs/Policy Controller/jservice/config folder**, i.e., **C:/Program Files/NextLabs/Policy Controller/jservice/config/jarpropertiesfile.properties**

10.4.2 Understanding how the NextLabs PIP Plugin interacts with Build Components

When a policy is executed and the NextLabs Policy Controller PDP determines that attributes sent in the initial set up of the session are insufficient, the getAttribute() function in the UserAttrProviderMod within the NextLabs Plugin jar is automatically executed sequentially for each missing attribute.

As described above, when the initial set of attributes is insufficient, the NextLabs PIP Plugin first checks a local cache, implemented using the Ehcache library and a CacheKey class illustrated above. If the requested attribute exists within the local cache, the NextLabs PIP Plugin retrieves and returns it immediately for use during policy evaluation by the Policy Controller (PDP).

If the requested attribute does not exist within the local cache, the NextLabs PIP Plugin's HTTPSTransmitter class makes an https request to the Protocol Broker using a doPost() function. The Protocol Broker performs its functions and returns either the desired attribute or an exception back to the NextLabs PIP Plugin, where the Policy Controller (PDP) can evaluate the relevant ABAC policy and determine an access decision. In the case that the requested attribute does not exist, the NextLabs Policy Controller PDP is configured to default to Deny access in our build. The NextLabs Policy Controller PDP is also configured to Deny Access whenever the Protocol Broker or the NextLabs PIP Plugin produces an exception.

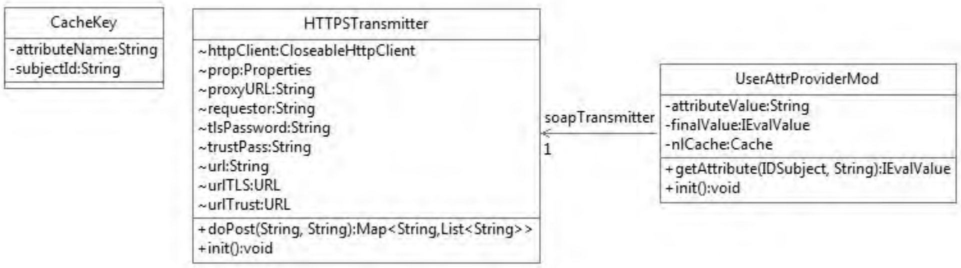


Figure 10.4 NextLabs PIP Plugin cCass Diagram

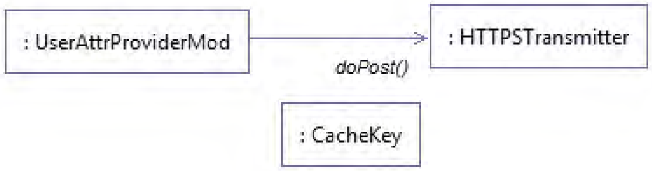


Figure 10.5 NextLabs PIP Plugin Interaction Diagram

10.4.3 Compilation and Deployment

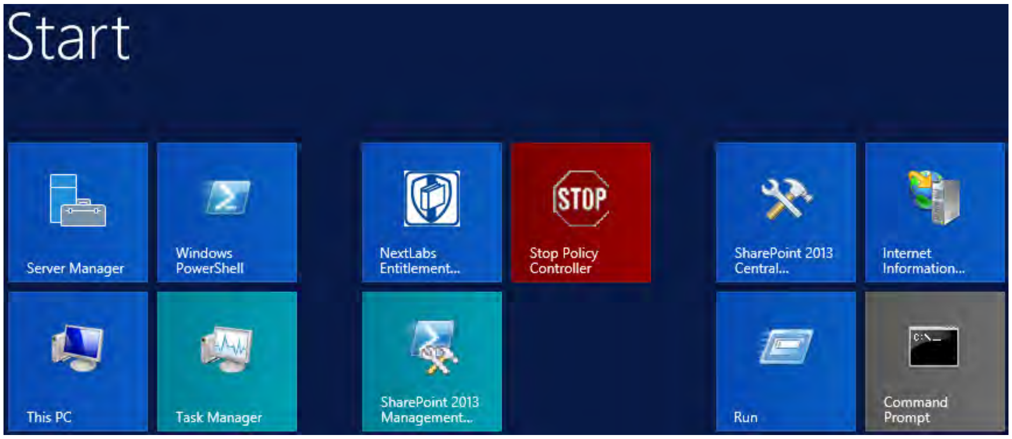
10.4.3.1 Compiling the NextLabs PIP Plugin Jar

1. Verify that you are on the server hosting your SharePoint instance, called the SharePoint server in our build.
2. Click on the Windows icon and begin typing **Cmd**.
3. Double-click the icon to open the Command Prompt.
4. In the Command Prompt window, navigate to the folder where your pom.xml exists and click Enter, i.e., **`cd C:/software/java/plugin/`**
5. In the Command Prompt window, run the following command and press Enter to compile your files and jar(s) into a single jar: **`mvn clean install`**

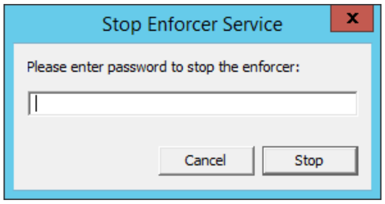
10.4.3.2 Stopping the NextLabs Policy Controller Service Before NextLabs PIP Plugin Jar Deployment

1. Still on the SharePoint server, click on the Windows icon and begin typing **Services**.
2. Double-click the icon to open the Services application.
3. In the Services application window, in the list of services, click on the **Name** column to sort by alphabetical order and look for **Control Center Enforcer Service**.

4. If the status of the **Control Center Enforcer Service** is **running**, stop it by following these steps:
   a. Click on the Windows icon.
   b. On your main screen, double-click the **Stop Policy Controller** shortcut.

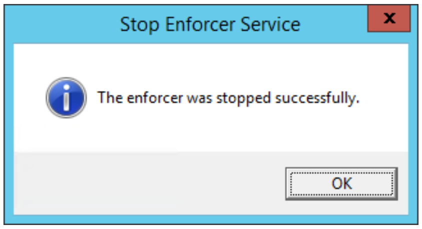


   c. Enter your NextLabs Administrator credentials, then click **Stop**.



Please enter password to stop the enforcer:

   d. Click **OK**.



The enforcer was stopped successfully.

10.4.3.3 Deploying the NextLabs PIP Plugin Jar and its Configuration File

1. Still on the SharePoint server, Click on the Windows icon and begin typing **Cmd**.
2. Double-click the icon to open the Command Prompt.
3. In the Command Prompt window, navigate to the folder where your NextLabs Policy Controller installation exists, and into its **`/jservices/jar`** folder where custom plugins are required to be stored, then press Enter. i.e., **`cd C:/Program Files/NextLabs/Policy Controller/jservice/jar/`**
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`**

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 new plugin folder you just created: copy **`"C:/software/java/plugin/target/plugin.jar" "nlsamlplugin/"`**

6. In the Command Prompt window, enter a command to navigate to the folder where your NextLabs Policy Controller installation exists, and into its **jservices** folder which contains the config folder where custom plugin .properties files are required to be stored, then press Enter. i.e., **`cd C:/Program Files/NextLabs/Policy Controller/jservice/`**

7. In the Command Prompt window, enter a command similar to the following and press Enter to copy your plugin .properties file from its existing location (example **`C:/software/java/plugin/`**) to the config folder: copy **`"C:/software/java/plugin/nlsamlpluginService.properties" "config/"`**

10.4.3.4 Resetting IIS and Restarting the NextLabs Policy Controller Service

1. Click on the Windows icon and begin typing **PowerShell**.
2. Double-click the icon to open Windows PowerShell.
3. In the Windows PowerShell window, type in this command and press Enter to reset Internet Information Services: **`iisreset`**
4. Click on the Windows icon and begin typing **Services**.
5. Double-click the icon to open the Services application.
6. 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**.
7. Right-click **Control Center Enforcer Service** and click **Start**.
   - It may be necessary to click the Refresh icon in order to see the **Control Center Enforcer Service** status change to **running**.

10.5 Protocol Broker

10.5.1 Architecture

The Protocol Broker decouples communication between the NextLabs Plugin and PingFederate RP. As noted earlier, the Protocol Broker is a web application hosted on a tomcat server installed on the SharePoint server. It communicates using mutual TLS and listens on the localhost. This ensures that the service provided by Protocol Broker is not available on the network, and the requester must be authenticated during each request.

SAMLProxy extends the HttpServlet class, which is an abstract class. This enables SAMLProxy class to read/write the http request/response, and determines the http method of the request (i.e. HTTP GET, POST, PUT, DELETE, HEAD etc) and calls one of the corresponding methods. The SAMLProxy class only implements the POST method.

The SAMLProxy class constructs an object of the SoapHTTPTransmitter class. This class reads **abacClient.jks** and **truststore.jks** which are used for mutual TLS communication initiated by the SoapHTTPTransmitter with PingFederate. It also reads **abacSigningClient.jks**, which is used to sign the SAML AttributeQuery, and metadata to verify the SAML Response signature. The jks extension stands for Java Key store, which is a storage facility for cryptographic keys and certificates.

The Protocol Broker facilitates secure communication between the NextLabs PIP Plugin and PingFederate RP. This coordination consists of two parts:

1. Communication between the NextLabs PIP Plugin and the Protocol Broker
2. Communication between the Protocol Broker and the PingFederate RP server

10.5.1.1 Communication Between NextLabs PIP Plugin and Protocol Broker

The Protocol Broker's doPost() method expects the following parameters:

- Requester
- SubjectId
- AttributeName

On successful receipt of a request, SAMLProxy uses the SoapHTTPTransmitter class to transmit the request to the PingFederate RP server. The response received from SOAPHTTPTransmitter is dispatched back to the NextLabs PIP Plugin, which then hands the result off to the PDP for policy evaluation and access decision making.

10.5.1.2 Communication Between Protocol Broker and PingFederate RP Server

The PingFederateRP and ProtocolBroker communicate using Assertion Query/Request Profile. As shown in figure 10.6, Communication Between Plugin and Relying Party, Protocol Broker initiates the secured communication on a mutual TLS channel with the Relying Party, and sends a signed SAML2 AttributeQuery. The message format and structure of the AttributeQuery is defined by SAMLCore section 3.3.2.3. Binding for the profile is defined by SAMLBind section 3.2.3. Processing rules governing the profile are provided by section 3.3 of SAMLCore. In response, Protocol Broker expects a SAML response back.

OpenSAML is used to implement an Assertion Query/Request Profile. OpenSAML is a set of open source libraries meant to support developers working with Security Assertion Markup Language (SAML). The configuration required to use the OpenSAML library is provided in section 10.5.2.2.

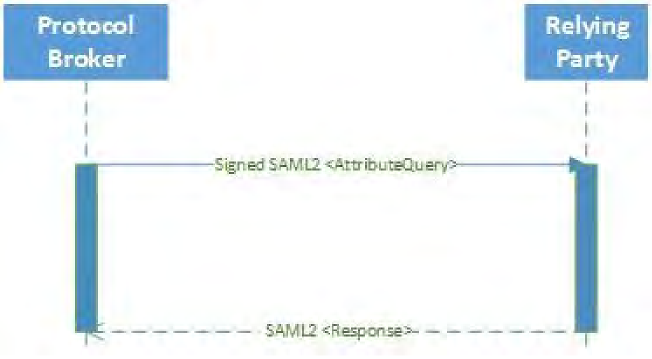


Figure 10.6 Communication Between Plugin and Relying Party

Based on keystores and configuration read during initialization, SoapHTTPTransmitter creates a SAML2AttributeQuerBuilder class to build a Signed SAML 2.0 Attribute Query. Attribute names received earlier in the doPost() method are used to build the AttributeQuery. A SOAPSAML2 object is used to provide SOAP parameters for the SAML message created earlier. It reads SAML 2.0 metadata to find the location of the Attribute Authority end point. It uses HttpSOAPClient to dispatch the request to the end point using mutual TLS.

HTTPSoapClient is also responsible for receiving the Attribute response, verifying the signature and sending the attributes back to the Nextlab Plugin.

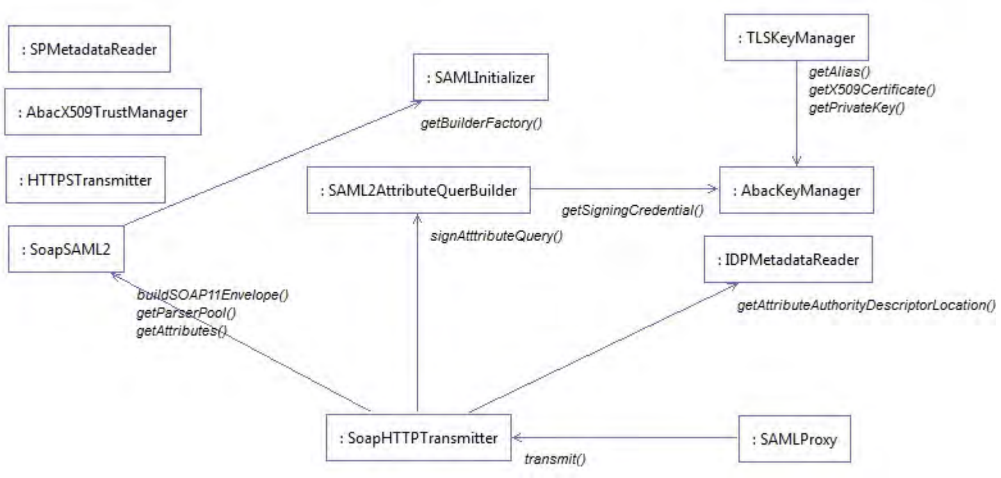


Figure 10.7 Protocol Broker Interaction Diagram

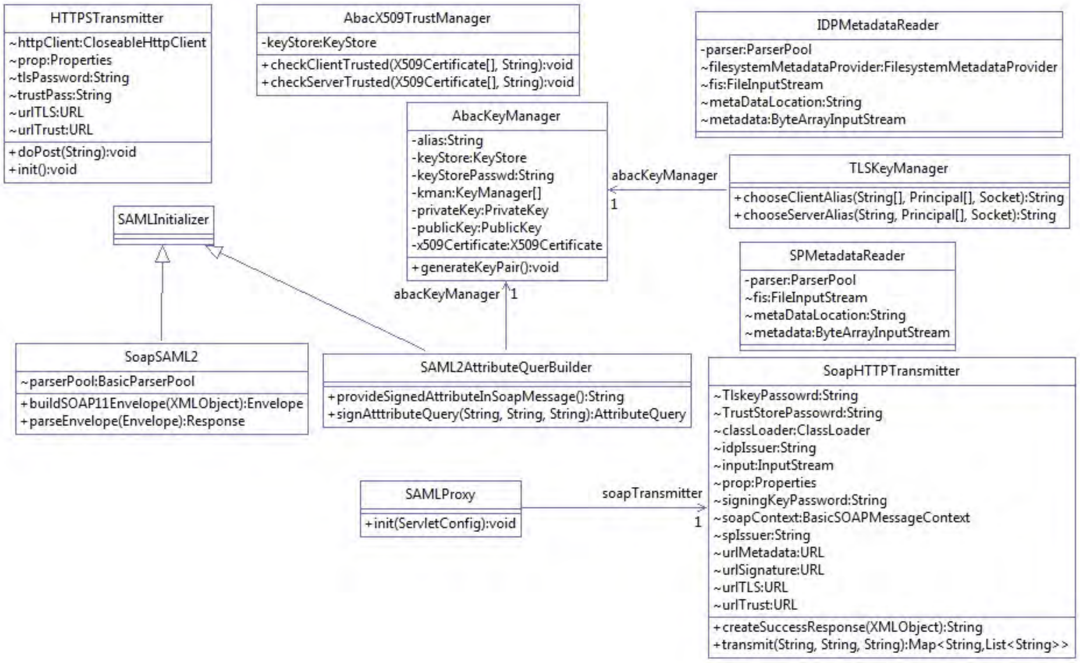

HTTPSTransmitter
~httpClient:CloseableHttpClient
~prop:Properties
~tlsPassword:String
~trustPass:String
~urlTLS:URL
~urlTrust:URL
+doPost(String):void
+init():void
AbacX509TrustManager
-keyStore:KeyStore
+checkClientTrusted(X509Certificate[], String):void
+checkServerTrusted(X509Certificate[], String):void
IDPMetadataReader
-parser:ParserPool
~filesystemMetadataProvider:FilesystemMetadataProvider
~fis:FileInputStream
~metaDataLocation:String
~metadata:ByteArrayInputStream
AbacKeyManager
-alias:String
-keyStore:KeyStore
-keyStorePasswd:String
-kman:KeyManager[]
-privateKey:PrivateKey
-publicKey:PublicKey
-x509Certificate:X509Certificate
+generateKeyPair():void
abacKeyManager
1
TLSKeyManager
+chooseClientAlias(String[], Principal[], Socket):String
+chooseServerAlias(String, Principal[], Socket):String
SAMLInitializer
SPMetadataReader
-parser:ParserPool
~fis:FileInputStream
~metaDataLocation:String
~metadata:ByteArrayInputStream
abacKeyManager
1
SoapSAML2
~parserPool:BasicParserPool
+buildSOAP11Envelope(XMLObject):Envelope
+parseEnvelope(Envelope):Response
SAML2AttributeQuerBuilder
+provideSignedAttributeInSoapMessage():String
+signAtttributeQuery(String, String, String):AttributeQuery
SoapHTTPTransmitter
~TlskeyPassowrd:String
~TrustStorePassowrd:String
~classLoader:ClassLoader
~idpIssuer:String
~input:InputStream
~prop:Properties
~signingKeyPassword:String
~soapContext:BasicSOAPMessageContext
~spIssuer:String
~urlMetadata:URL
~urlSignature:URL
~urlTLS:URL
~urlTrust:URL
+createSuccessResponse(XMLObject):String
+transmit(String, String, String):Map<String,List<String>>
SAMLProxy
+init(ServletConfig):void
soapTransmitter
1

Figure 10.8 Protocol Broker Class Diagram

10.5.2 Deployment

10.5.2.1 System and Environment Requirements

The Protocol Broker is deployed on tomcat 8.0.22 on the SharePoint server, and uses OpenSAML 2.6.4.

10.5.2.2 Configuration

In order to accept traffic only on the channel protected by mutual TLS:

1. Install tomcat on the SharePoint server. The tomcat installation procedure is provided here.
2. Open the configuration file **server.xml** inside the configuration directory of the tomcat installation. Comment out the section:

```
<!--
  <Connector port="8080" protocol="HTTP/1.1"
        connectionTimeout="20000"
    redirectPort="8443" />
-->
```

3. Update/insert the following line:

```
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150"
SSLEnabled="true" scheme="https" secure="true"
keystoreFile="C:\Users\<name>\Documents\softwares\tomcat\apache-tomcat-8.0.
22\conf\abacTomcat.jks" keystorePass="…..password" clientAuth="true"
```

```
sslProtocol="TLS"
truststoreFile="C:\Users\sjha\Documents\softwares\tomcat\apache-tomcat-8.0.
22\conf\truststore.jks" truststoreType="JKS" truststorePass="…password" />
```

The configuration details for OpenSAML are provided here. In this demonstration, a folder called **endorsed** is created inside the **lib** directory of tomcat installation.

Add the following libraries to the endorsed folder created in the above step:

- xml-apis-2.10.0.jar
- xml-resolver-1.2.jar
- xercesImpl-2.10.0.jar
- xalan-2.7.1.jar
- serializer-2.10.0.jar

10.5.2.3 Preparation and Compilation

In our build, we used Apache Maven for Protocol Broker compilation. In order to prepare and compile the Protocol Broker, follow these steps:

10.5.2.3.1 Preparation

1. On the SharePoint server, click on the Windows icon and begin typing **Cmd**.
2. Double-click the icon to open the Command Prompt.
3. In the Command Prompt window, navigate to the folder where your pom.xml for the Protocol Broker exists, and press Enter. i.e., **`cd C:/software/java/samlNewPlugin/`**
4. Type the following command, then press Enter to prepare for compilation of the new Protocol Broker: **`.war file: mvn clean`**
5. Verify that your results are similar to the following, including the **Build Success** statement:

```
[INFO] Scanning for projects...
[INFO]
[INFO]
------------------------------------------------------------------------
[INFO] Building SAMLProxy 0.0.1-SNAPSHOT
[INFO]
------------------------------------------------------------------------
[INFO]
[INFO] --- maven-clean-plugin:2.5:clean (default-clean) @ SAMLProxy
---
[INFO] Deleting /home/sjha/pdpPlugins/SAMLProxy/target
[INFO]
------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO]
------------------------------------------------------------------------
```

```
[INFO] Total time: 1.333 s
[INFO] Finished at: 2015-06-29T10:24:27-04:00
[INFO] Final Memory: 5M/15M
[INFO]
-------------------------------------------------------------------
```

10.5.2.3.2 Compiling the .war File

1. After following the instructions above to prepare for compiling, within the Command Prompt window, enter the following command and press Enter to create the Protocol Broker: **`.war file: mvn package`**
2. Verify that your results are similar to the following, including the **Failures: 0** and **Build Success** portions:

```
[INFO] Scanning for projects...
[INFO]
[INFO]
-------------------------------------------------------------------
-----
[INFO] Building SAMLProxy 0.0.1-SNAPSHOT
[INFO]
-------------------------------------------------------------------
-----
[INFO]
[INFO] --- maven-resources-plugin:2.6:resources (default-resources)
@ SAMLProxy ---
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] Copying 9 resources
[INFO]
[INFO] --- maven-compiler-plugin:3.1:compile (default-compile) @
SAMLProxy ---
[INFO] Nothing to compile - all classes are up to date
[INFO]
[INFO] --- maven-resources-plugin:2.6:testResources
(default-testResources) @ SAMLProxy ---
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] skip non existing resourceDirectory
/home/sjha/pdpPlugins/SAMLProxy/src/test/resources
[INFO]
[INFO] --- maven-compiler-plugin:3.1:testCompile
(default-testCompile) @ SAMLProxy ---
[INFO] Nothing to compile - all classes are up to date
[INFO]
```

```
[INFO] --- maven-surefire-plugin:2.12.4:test (default-test) @
SAMLProxy ---
[INFO] Surefire report directory:
/home/sjha/pdpPlugins/SAMLProxy/target/surefire-reports

-------------------------------------------------------
 T E S T S
-------------------------------------------------------
Running nist.pdpplugin.AppTest
Tests run: 1, Failures: 0, Errors: 0, Skipped: 0, Time elapsed: 0.03
sec

Results :

Tests run: 1, Failures: 0, Errors: 0, Skipped: 0

[INFO]
[INFO] --- maven-war-plugin:2.6:war (default-war) @ SAMLProxy ---
[INFO] Packaging webapp
[INFO] Assembling webapp [SAMLProxy] in
[/home/sjha/pdpPlugins/SAMLProxy/target/SAMLProxy-0.0.1-SNAPSHOT]
[INFO] Processing war project
[INFO] Copying webapp resources
[/home/sjha/pdpPlugins/SAMLProxy/WebContent]
[INFO] Webapp assembled in [440 msecs]
[INFO] Building war:
/home/sjha/pdpPlugins/SAMLProxy/target/SAMLProxy-0.0.1-SNAPSHOT.war
[INFO]
-------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO]
-------------------------------------------------------------------
[INFO] Total time: 6.281 s
[INFO] Finished at: 2015-06-29T10:27:14-04:00
[INFO] Final Memory: 11M/26M
[INFO]
-------------------------------------------------------------------
```

10.5.3 Example SAML Request and Response Output

10.5.3.1 Example of Tomcat Output from our Build that Illustrates a SAML Request

```
<saml2p:AttributeQuery ID="_7a41be2e3d0d1abea13e857a80b3cfbc"
IssueInstant="2015-05-26T18:14:39.405Z" Version="2.0"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
 <saml2:Issuer
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">urn:nccoe:abac:plu
gin</saml2:Issuer>
 <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/2000/09/xmldsig#rsa-sha1"/>
   <ds:Reference URI="#_7a41be2e3d0d1abea13e857a80b3cfbc">
    <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/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>hz3JxkkIsCL/BVlkRCrgUykjbho=</ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>

<ds:SignatureValue>O8Gc8CSVKeYoNsR8bWaiExEpumeO2bLaMwlWC6LNaqf9ydvMPw/
gcZbAEATCgK/RXVYgTe7ikYKKC80/GiO7NrUKZPO86ln5LINX5Gw5iTOeb6S4zUTWEfp2P
QTfMSTB6rZe5OBuUDEpWfJ4T/3E1KpI4H7sxoaYhcZ3J2i1ZxPheMEJ0l4zvicAzlsefii
rftn1vWirOdjub9VE0SicCl11FJB13Wla+c8JA5Nbbsnc3H6h5oDeapEOD9bX41KZtj2sG
bh6k+F3vunYpd3m69KW6z8CJQeBWOcGCmDtt4Dyf/avG6Iz7o0PYjPYxFIvwslOYYU2QzL
tOpHT8e/RRQ==</ds:SignatureValue>
  <ds:KeyInfo>
   <ds:KeyValue>
    <ds:RSAKeyValue>

<ds:Modulus>uzxrL5iAIpNyEXHmGTDW1mzx7YJal/c9Ruxag3sifjzuUdBjEznFJJxaag
M2pzTUI5JCaLzgm71V
SBmuVL+6PzTxReM3i5XzWjpgRMIizadnQT0wmCryKuNaQiBIFLoMbi+ySdBvu+M/xhHlRx
uFjY9N
```

```
PSE1MHL8YaLoKW2SFIm/3bhJ/xF7q7FGHMcJH4Zzr2QpQmBEryozJJV3z4ZvVro/MfyLg1
VER0pu
36e32hIyzsf2gKizv00qY2ecDlBCNTITsA2HWSTf50kpvT4qupCnXVKVqzDPZON0XCsJJc
wWsUi9
pRvkGtVBXqhh282ODyzcl3nkpgsl5F8hR7kOjQ==</ds:Modulus>
     <ds:Exponent>AQAB</ds:Exponent>
    </ds:RSAKeyValue>
   </ds:KeyValue>
  </ds:KeyInfo>
 </ds:Signature>
 <saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">jdoe</s
aml2:NameID>
 </saml2:Subject>
 <saml2:Attribute Name="firstname"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"/>
</saml2p:AttributeQuery>
```

10.5.3.2 Example of Tomcat Output from our Build that Illustrates a SAML Response

```
<?xml version="1.0" encoding="UTF-8"?><S11:Envelope
xmlns:S11="http://schemas.xmlsoap.org/soap/envelo
  pe/">
  <S11:Body>
    <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="LkF9NevJONpgbE56hszqbo2V
      FZH" InResponseTo="_13caab0c0aa8b70946be278ff32376ad"
IssueInstant="2015-06-29T14:46:35.617Z" Version
      ="2.0">
      <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://rp.abac.tes
t:9031</saml:Issuer>
        <samlp:Status>
          <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </samlp:Status>
        <saml:Assertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="P-nmuwJENgb_aVjhd5DpY
          dfN2IU" IssueInstant="2015-06-29T14:46:35.945Z"
Version="2.0">
          <saml:Issuer>https://rp.abac.test:9031</saml:Issuer>
```

```
     <saml2:Subject
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:saml2p="urn:oasi
      s:names:tc:SAML:2.0:protocol"
xmlns:soap11="http://schemas.xmlsoap.org/soap/envelope/">
      <saml2:NameID
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">lsmith@
ab
       ac.test</saml2:NameID>
     </saml2:Subject>
     <saml:Conditions NotBefore="2015-06-29T14:41:35.945Z"
NotOnOrAfter="2015-06-29T14:51:35.9
      45Z">
      <saml:AudienceRestriction>
       <saml:Audience>https://nextlabs-rp</saml:Audience>
      </saml:AudienceRestriction>
     </saml:Conditions>
     <saml:AttributeStatement>
      <saml:Attribute Name="stafflevel"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-for
       mat:basic">
       <saml:AttributeValue
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
        www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Junior</saml:AttributeValue>
      </saml:Attribute>
     </saml:AttributeStatement>
    </saml:Assertion>
  </samlp:Response>
 </S11:Body>
</S11:Envelope>
```

10.6 Apache Directory Service (ApacheDS)

ApacheDS is included in Apache Directory Studio, which has multiple functionalities with ApacheDS Server, i.e., LDAP Browser, Schema Editor, Apache Configurator, LDIF Editor, Embedded ApacheDS, and ACI Editor.

10.6.1 Layout

Before installation, it is important to consider system needs and match them with the installation layout. The general layout for ApacheDS consists of two major concepts:

1. Installation Layout: The installation is where all files essential to ApacheDS are stored, i.e., launch script, libraries, and a service wrapper (depending on the kind of installer used).
2. Instance Layout: ApacheDS is built to run multiple instances of the server at the same time, which means that an optional instances folder can be found in the installation layout (or elsewhere on the disk, depending on the platform). In that folder you will find one or multiple directories, all sharing the same layout, corresponding to all ApacheDS instances (one directory per instance, with names corresponding to the ID of the instance).

A detailed discussion of these concepts can be found here.

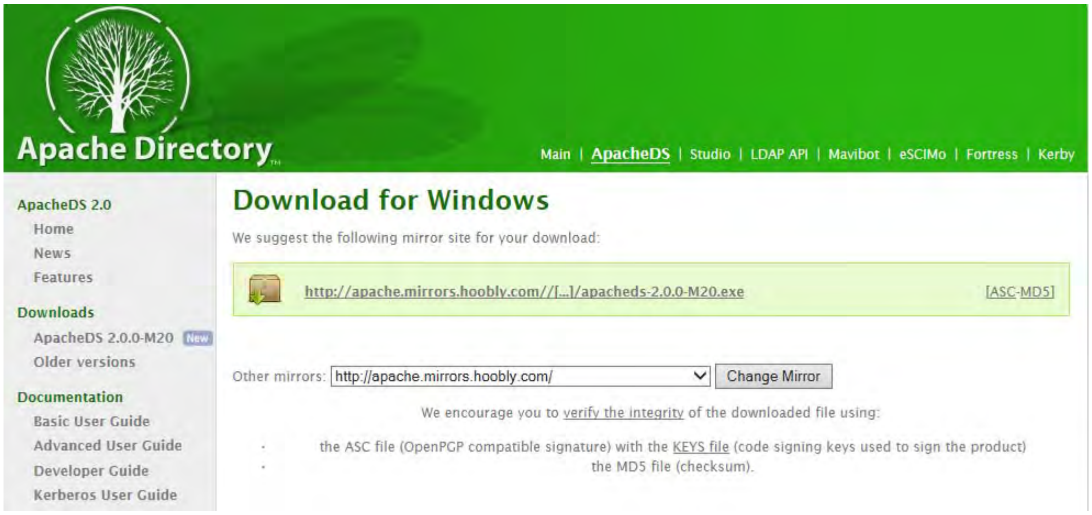
10.6.2 Download

ApacheDS can be downloaded as binary or as source, and compiled on a given platform. Source can be downloaded here.

In this project, ApacheDS was downloaded as a packaged Windows installer from this location. Native installers are available in the following formats, and their download links are available at following site.

Platform	Installer Format
Windows	.exe
Mac OS X	.dmg
Debian	.deb
Linux	.rmp, .bin

1. At the download location, you will see a URL as shown in the example below. Click the link above to download Apache Directory Server for Windows.



Download for Windows

We suggest the following mirror site for your download:

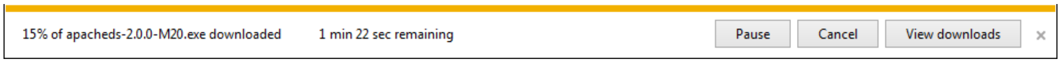
http://apache.mirrors.hoobly.com//[...]/apacheds-2.0.0-M20.exe [ASC-MD5]

Other mirrors: http://apache.mirrors.hoobly.com/

We encourage you to verify the integrity of the downloaded file using:

- the ASC file (OpenPGP compatible signature) with the KEYS file (code signing keys used to sign the product)
- the MD5 file (checksum).

2. During the software download, different installation graphics will be displayed depending on which browser you use. Example from Windows Internet Explorer:



15% of apacheds-2.0.0-M20.exe downloaded 1 min 22 sec remaining

3. On Chrome, it may display as below (if you are not using command line tools):

10.6.2.1 Verify the Integrity of the Downloaded File

It is essential to verify the integrity of the file when the download completes.

The file's integrity can be verified with PGP signatures using PGP or GPG. First, download the **KEYS** and the **asc** signature file for the relevant distribution. Both **KEYS** and **asc** can be found to the right of the download link, as shown in Figure 4: ApacheDS download.

Verify the signatures using the following commands in the Command Prompt:

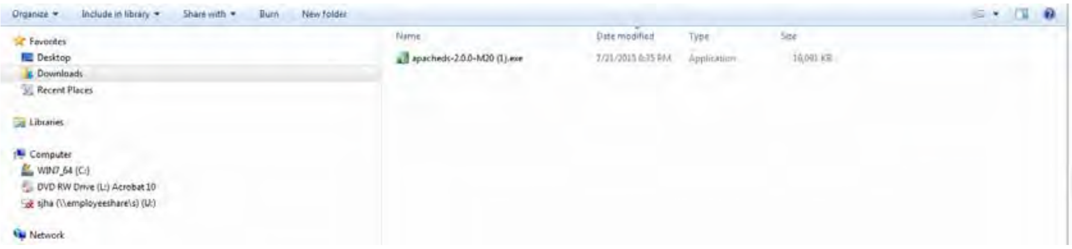
```
$ pgpk -a KEYS
$ pgpv apacheds-2.0.0-M20.exe.asc
or
$ pgp -ka KEYS
$ pgp apacheds-2.0.0-M20.exe.asc
or
$ gpg --import KEYS
$ gpg --verify apacheds-2.0.0-M20.exe.asc
```

Alternatively, you can verify the MD5 signature on the files. A Unix program called md5 or md5sum is included in many Unix distributions. It is also available as part of GNU Textutils. Windows users can get binary md5 programs from here, here, or here.

10.6.3 Installation

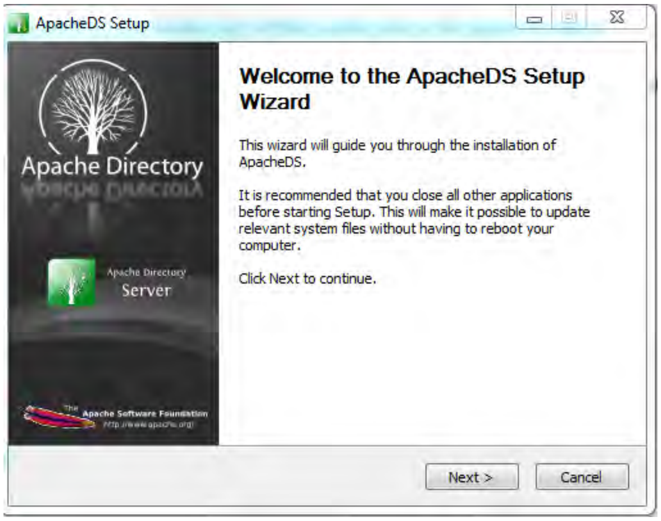
Note: To install ApacheDS as a Windows service, you need administrative privileges. We installed ApacheDS on Windows Server 2012. The ApacheDS installation procedure for other operating systems can be found here.

1. Once ApacheDS is downloaded and verified, double-click the installer to open it. Note: It may have already been opened by your web browser.



Name	Date modified	Type	Size
apacheds-2.0.0-M20 (1).exe	7/21/2015 8:35 PM	Application	16,091 KB

2. When the following screen appears, click **Next**.



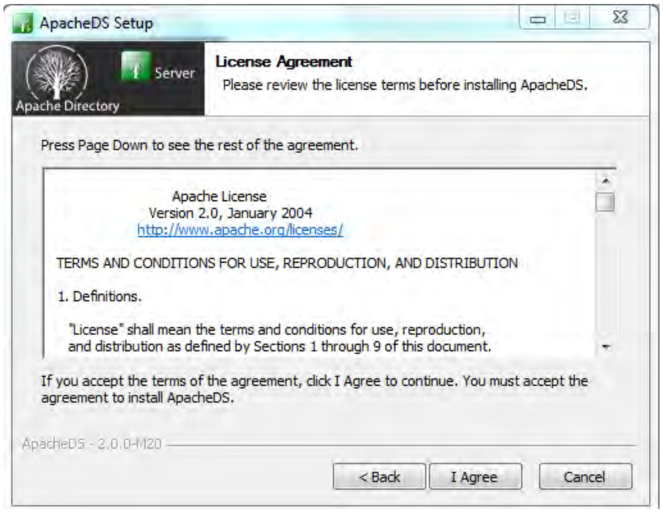
Welcome to the ApacheDS Setup Wizard

This wizard will guide you through the installation of ApacheDS.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

3. Review the License agreement and click **I Agree**.



License Agreement

Please review the license terms before installing ApacheDS.

Press Page Down to see the rest of the agreement.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

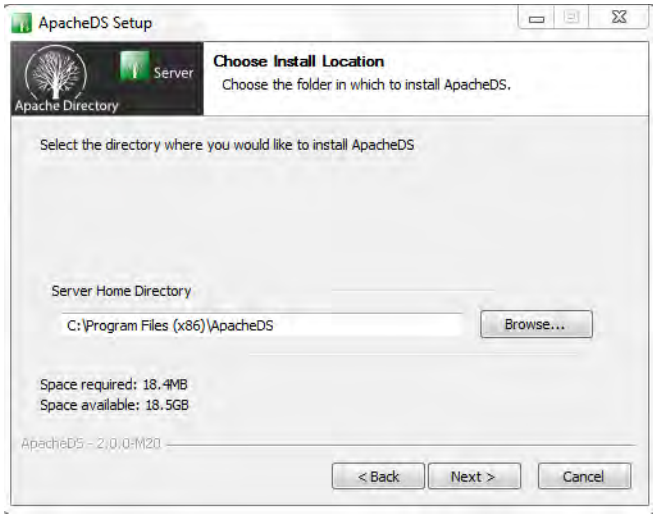
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install ApacheDS.

4. The next screen prompts you for the install path. In our build, we left the default install path. Specify an install path of your choosing, and click **Next**.



ApacheDS Setup

Choose Install Location

Choose the folder in which to install ApacheDS.

Select the directory where you would like to install ApacheDS

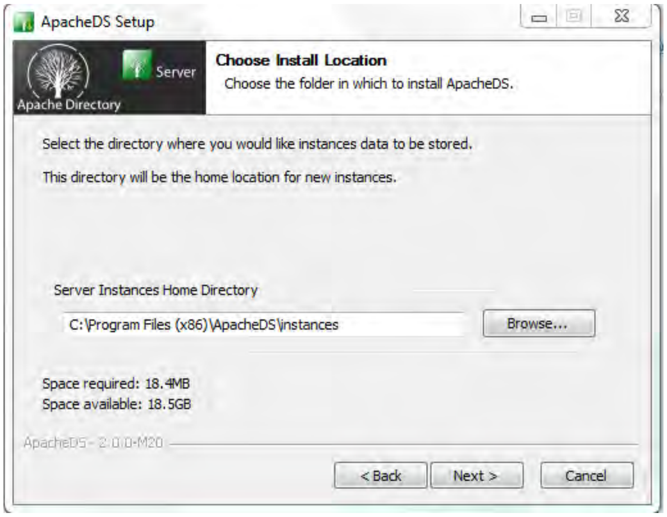
Server Home Directory

C:\Program Files (x86)\ApacheDS

Space required: 18.4MB
Space available: 18.5GB

ApacheDS - 2.0.0-M20

5. Specify a location for storing ApacheDS instances, then click **Next**.



ApacheDS Setup

Choose Install Location

Choose the folder in which to install ApacheDS.

Select the directory where you would like instances data to be stored.

This directory will be the home location for new instances.

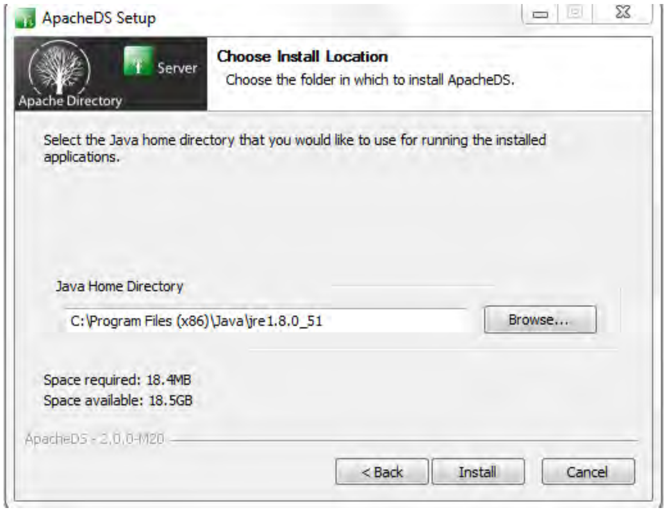
Server Instances Home Directory

C:\Program Files (x86)\ApacheDS\instances

Space required: 18.4MB
Space available: 18.5GB

ApacheDS - 2.0.0-M20

6. The next screen asks for the location of your Java runtime environment (JRE). It is assumed, based on the earlier description in section 10.8.2, that users will have the proper Java environment prior to attempting to install ApacheDS. Users who have no JRE installed should abandon the install by clicking **Cancel**. Install the JRE and re-run the ApacheDS install. We accepted the default as shown.



Choose Install Location

Choose the folder in which to install ApacheDS.

Select the Java home directory that you would like to use for running the installed applications.

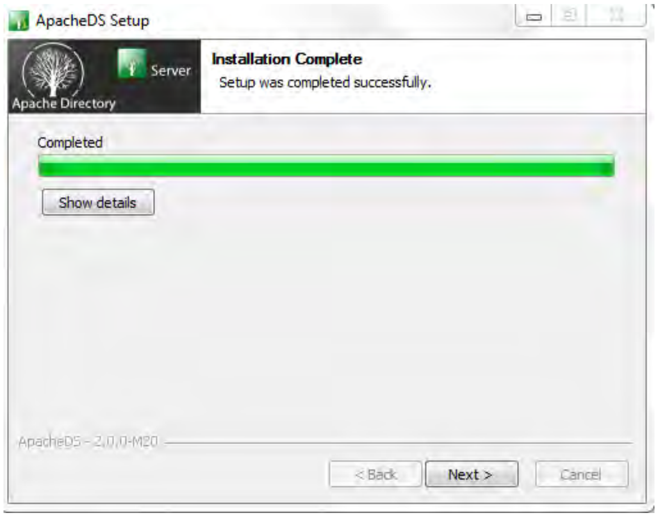
Java Home Directory

C:\Program Files (x86)\Java\jre1.8.0_51

Space required: 18.4MB
Space available: 18.5GB

ApacheDS - 2.0.0-M20

7. Click **Install**. Once the installation is complete, you will receive the following prompt:



Installation Complete

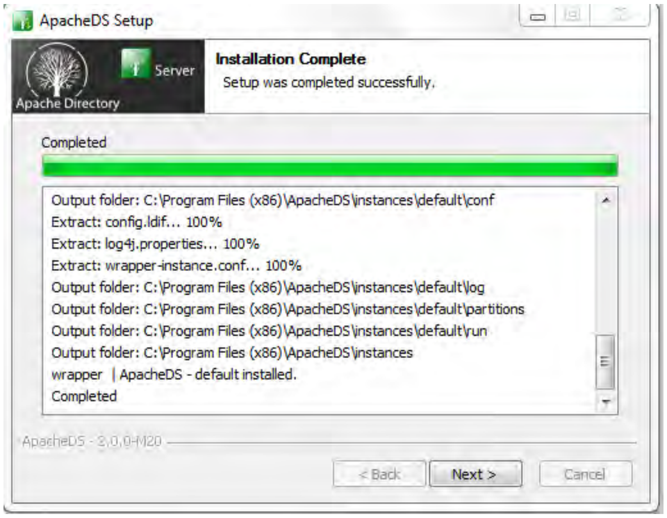
Setup was completed successfully.

Completed

ApacheDS - 2.0.0-M20

10.6.3.1 Functional Test of the ApacheDS Installation

1. Click **Show Details** in above diagram to see details of installation. Make sure all of the folders exist, then click **Next**.



ApacheDS Setup

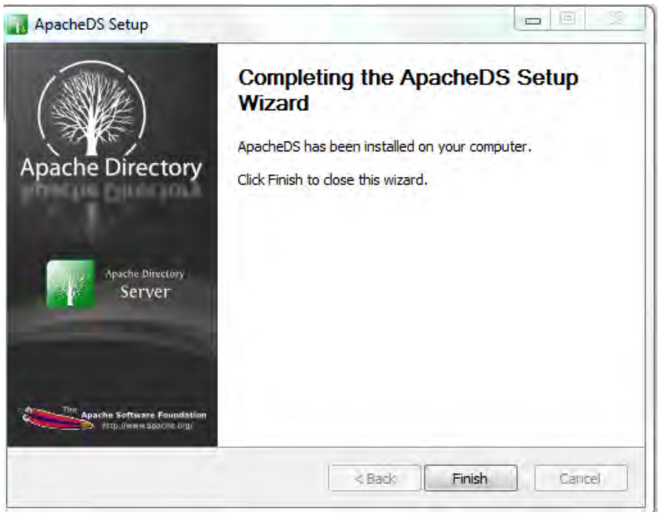
Installation Complete

Setup was completed successfully.

Completed

```
Output folder: C:\Program Files (x86)\ApacheDS\instances\default\conf
Extract: config.ldif... 100%
Extract: log4j.properties... 100%
Extract: wrapper-instance.conf... 100%
Output folder: C:\Program Files (x86)\ApacheDS\instances\default\log
Output folder: C:\Program Files (x86)\ApacheDS\instances\default\partitions
Output folder: C:\Program Files (x86)\ApacheDS\instances\default\run
Output folder: C:\Program Files (x86)\ApacheDS\instances
wrapper  | ApacheDS - default installed.
Completed
```

2. Click **Finish** to end the installation.



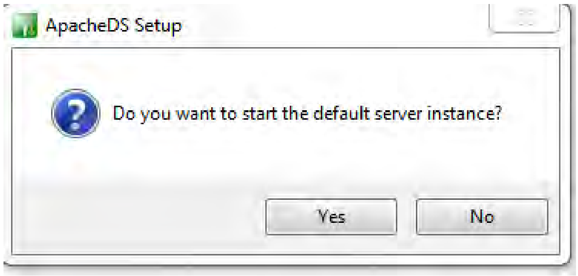
ApacheDS Setup

Completing the ApacheDS Setup Wizard

ApacheDS has been installed on your computer.

Click Finish to close this wizard.

3. Click **Yes** to start the ApacheDS server. Instructions are provided in section 6.2 of this chapter.

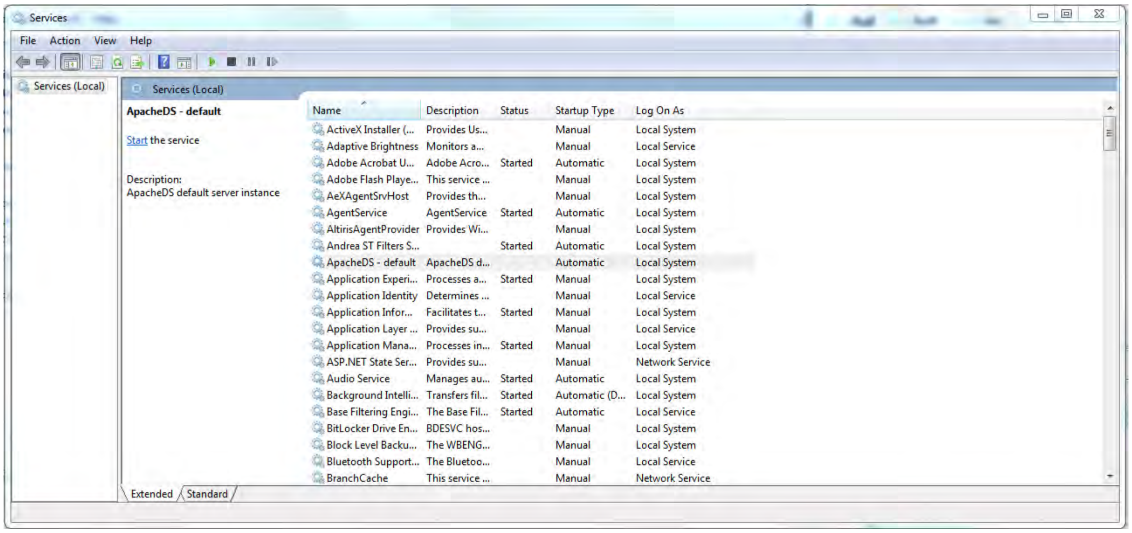


ApacheDS Setup

Do you want to start the default server instance?

10.6.4 Starting and Stopping the Server

The server can be started and stopped with the Windows Services manager **(Control Panel -> Administrative Tools -> Services)**. The user must have administrative privileges.



ApacheDS - default

Start the service

Description:
ApacheDS default server instance

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (...	Provides Us...		Manual	Local System
Adaptive Brightness	Monitors a...		Manual	Local Service
Adobe Acrobat U...	Adobe Acro...	Started	Automatic	Local System
Adobe Flash Playe...	This service ...		Manual	Local System
AeXAgentSrvHost	Provides th...		Manual	Local System
AgentService	AgentService	Started	Automatic	Local System
AltirisAgentProvider	Provides Wi...		Manual	Local System
Andrea ST Filters S...		Started	Automatic	Local System
ApacheDS - default	ApacheDS d...		Automatic	Local System
Application Experi...	Processes a...	Started	Manual	Local System
Application Identity	Determines ...		Manual	Local Service
Application Infor...	Facilitates t...	Started	Manual	Local System
Application Layer ...	Provides su...		Manual	Local Service
Application Mana...	Processes in...	Started	Manual	Local System
ASP.NET State Ser...	Provides su...		Manual	Network Service
Audio Service	Manages au...	Started	Automatic	Local System
Background Intelli...	Transfers fil...	Started	Automatic (D...	Local System
Base Filtering Engi...	The Base Fil...	Started	Automatic	Local Service
BitLocker Drive En...	BDESVC hos...		Manual	Local System
Block Level Backu...	The WBENG...		Manual	Local System
Bluetooth Support...	The Bluetoo...		Manual	Local Service
BranchCache	This service ...		Manual	Network Service

From here, ApacheDS can be started, stopped, or restarted.

The process for starting and stopping ApacheDS on other operating systems is described here.

10.6.5 ApacheDS Configuration

ApachdDS Server and Schema configuration details are provided here.

10.7 PingFederate - Apache Integration

This section requires knowledge of the following pieces of information:

1. Server IP address or hostname
2. Server port where it is listening on
3. Server credentials (i.e., private key and certificate) to be provision

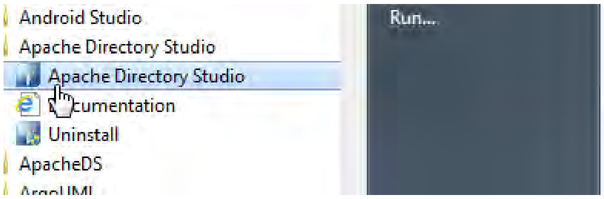
10.7.1 Provisioning of Server Credential

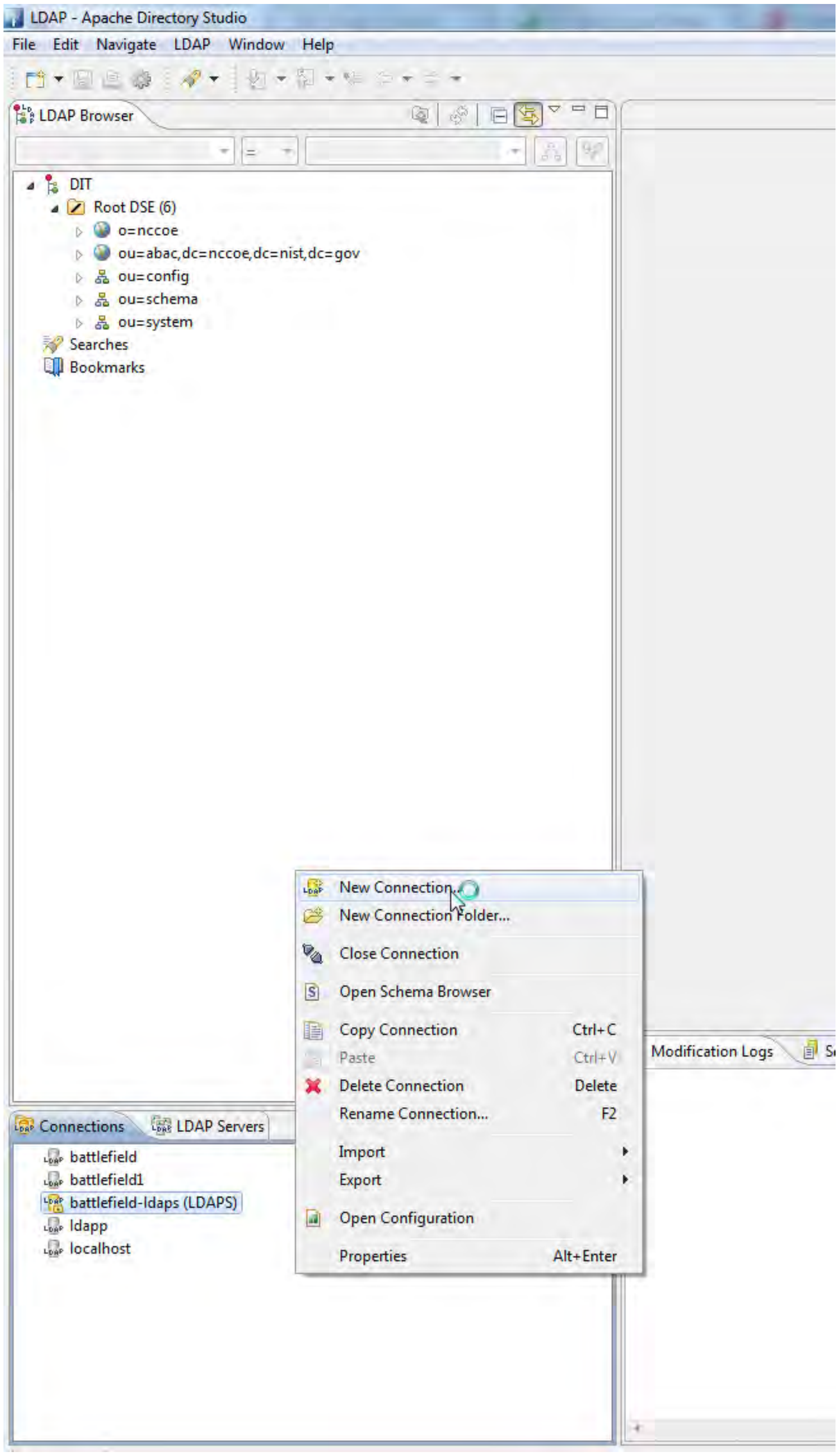
Start Apache Directory Server Studio and open a new connection.

10.7.1.1 Creation of Server Connection

To create a new LDAPS connection, complete the following steps:

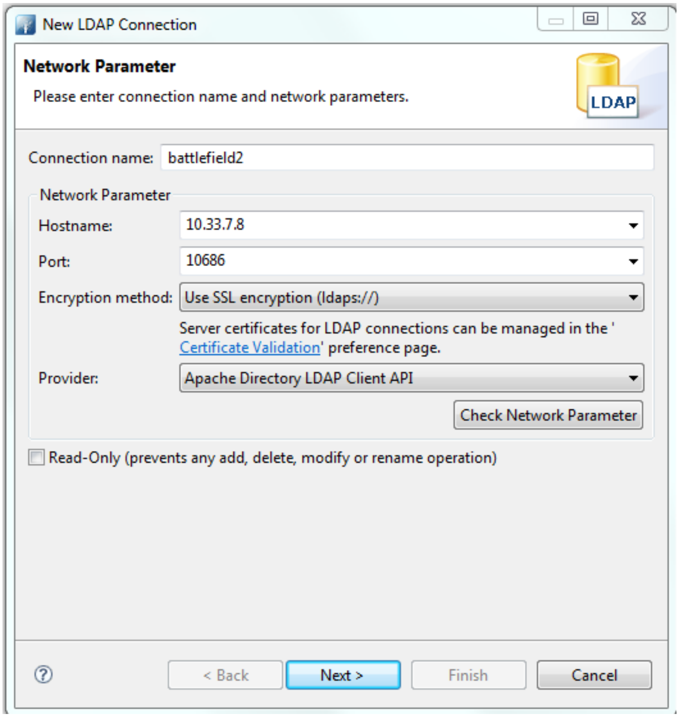
1. Define network parameters.
2. Define authentication parameters.
3. Define additional browser options (optional).
4. Define additional edit options (optional).




LDAP - Apache Directory Studio
File Edit Navigate LDAP Window Help
LDAP Browser
DIT
Root DSE (6)
o=nccoe
ou=abac,dc=nccoe,dc=nist,dc=gov
ou=config
ou=schema
ou=system
Searches
Bookmarks
New Connection...
New Connection Folder...
Close Connection
Open Schema Browser
Copy Connection Ctrl+C
Paste Ctrl+V
Delete Connection Delete
Rename Connection... F2
Import
Export
Open Configuration
Properties Alt+Enter
Modification Logs
Connections
LDAP Servers
battlefield
battlefield1
battlefield-ldaps (LDAPS)
ldapp
localhost

847

5. Once a new connection is opened, the following screen appears. Fill in Hostname and Port. 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

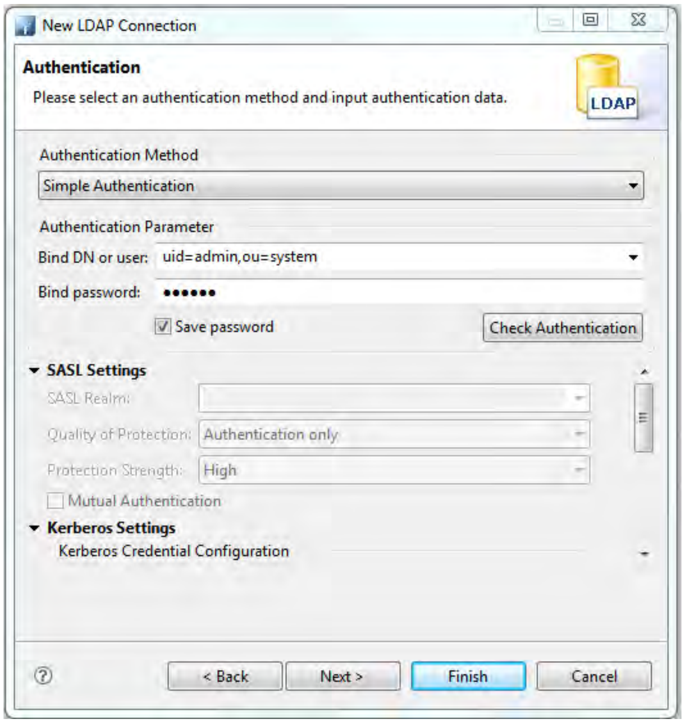
Encryption method: Use SSL encryption (ldaps://)

Server certificates for LDAP connections can be managed in the 'Certificate Validation' preference page.

Provider: Apache Directory LDAP Client API

□ Read-Only (prevents any add, delete, modify or rename operation)

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-encyrpted 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.	



852

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

SASL Settings

SASL Realm:

Quality of Protection: Authentication only

Protection Strength: High

□ Mutual Authentication

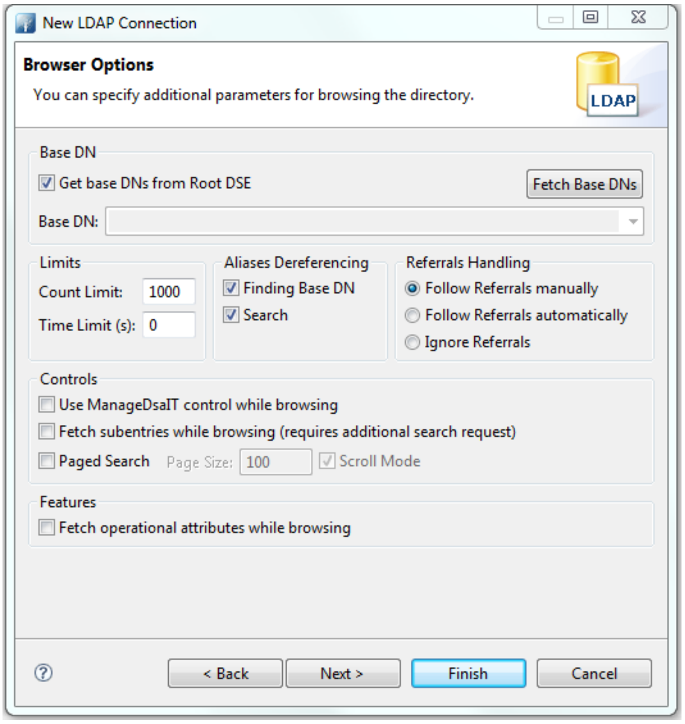
Kerberos Settings

Kerberos Credential Configuration

853

Option	Description	Defualt
Authentication Method	Select your authentication method: ■ Anonymous Authentication: connects to the directory without authentication. ■ Simple Authentication: uses simple authentication using a bind DN and password. The credentials are transmitted in clear-text over the network. ■ CRAM-MD5 (SASL): authenticates to the directory using a challenge-response authentication mechanism. The credentials are not transmitted in clear-text over the network. ■ DIGEST-MD5 (SASL): another challenge-response authentication mechanism. Additionally, you could define your realm and QoP parameters. ■ GSSAPI (Kerberos): user Kerberos-based authentication. Additional parameters can be defined.	Simple Authentication
Bind DN or user	The distinguished name or user ID used to bind. Previously entered DNs can be selected from drop-down list.	empty
Bind Password	The password used to bind.	empty
Save password	If checked, the password will be saved in configuration. If not checked, you must enter the password whenever you connect to the server. Warning: The password is saved as plain text.	checked
Check Authentication	Use this function to attempt a connection plus a bind to the host upon completion of the wizard. It will validate that the entered information is correct.	

This project does not use SASL or Kerberos.



New LDAP Connection

Browser Options

You can specify additional parameters for browsing the directory.

Base DN

☑ Get base DNs from Root DSE

Base DN:

Limits

Count Limit: 1000

Time Limit (s): 0

Aliases Dereferencing

☑ Finding Base DN

☑ Search

Referrals Handling

● Follow Referrals manually

○ Follow Referrals automatically

○ Ignore Referrals

Controls

□ Use ManageDsaIT control while browsing

□ Fetch subentries while browsing (requires additional search request)

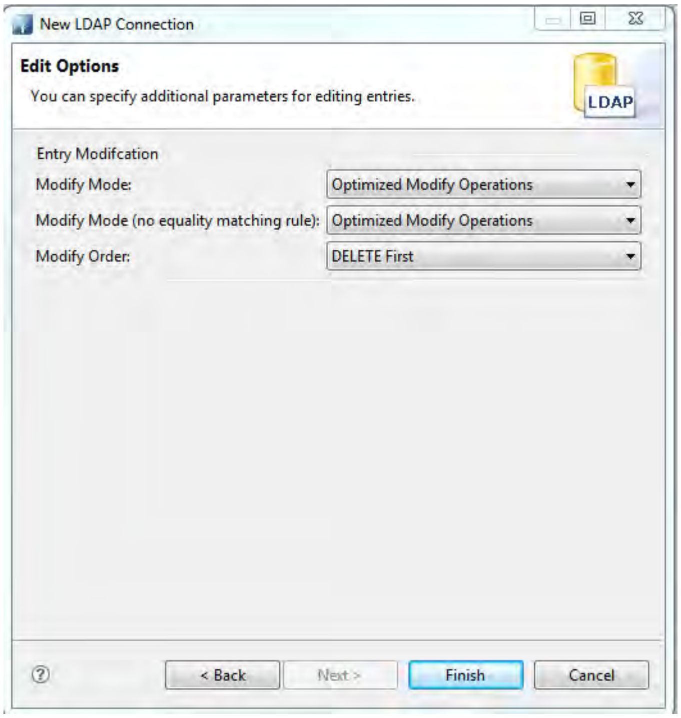
□ Paged Search Page Size: 100 ☑ Scroll Mode

Features

□ Fetch operational attributes while browsing

Option	Description	Default
Get base DNs from Root DSE	If checked, the base DNs are fetched from the namingContexts attribute of the Root DSE.	checked
Fetch Base DNs	Use this function to get the namingContext values from the Root DSE. The returned values will appear in the Base DN drop-down list.	-
Base DN	The Base DN to use. You may enter a DN manually or select one from the drop-down list. This field is only enabled if the option **Get base DNs from root DSE** is off.	empty
Count Limit	Maximum number of entries returned from the server when browsing the directory. It is also used as default value when searching the 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.	1000
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

Option	Description	Default
Referrals Handling	Specifies the referral handling. ■ Follow Referrals Manually: Received referrals and search continuations are displayed in the browser. When you open or expand a search continuation, the search is continued. Specify which connection you want to use to follow a specific referral URL. You will have full control regarding encryption and authentication options when following referrals. ■ Follow Referrals Automatically: Follows referrals and search continuations immediately if they are received from the directory server. Specify which connection you want to use to follow a specific referral URL. You will have full control regarding encryption and authentication options when following referrals. ■ Ignore Referrals: Any referral or search continuation received from the directory server is silently ignored. No error is logged, no dialog appears, no special entry is displayed in the DIT, and no ManageDsaIT control is sent to the server.	Follow Referrals manually
Use ManageDsaIT control while browsing	If enabled, the ManageDsaIT control is sent to the server in each request. This signals the directory server not to send referrals and search continuations, but return the special referral objects. Note: This is only applicable if the directory server supports the ManageDsaIT control.	unchecked
Fetch subentries while browsing	If enabled, both normal and subentries according to RFC 3672 are fetched. This causes additional search requests while browsing the directory.	unchecked
Paged Search	If enabled, the simple paged result control is used while browsing the directory. With page size you can define how many entries should be retrieved in one request. If Scroll Mode is enabled, only one page is fetched from the server at a time. While browsing, you can scroll through the pages by using **next page** and **top page**. If disabled, all entries are fetched from the server. The paged result control is only used in the background to avoid server-side limits.	unchecked
Fetch operational attributes while browsing	If enabled, both user attributes and operational attributes are retrieved while browsing. If the server supports the feature **All Operational Attributes**, use + to retrieve operational attributes. Otherwise, all operational attributes defined in the schema are requested.	unchecked



New LDAP Connection

Edit Options

You can specify additional parameters for editing entries.

Entry Modifcation

Modify Mode: Optimized Modify Operations

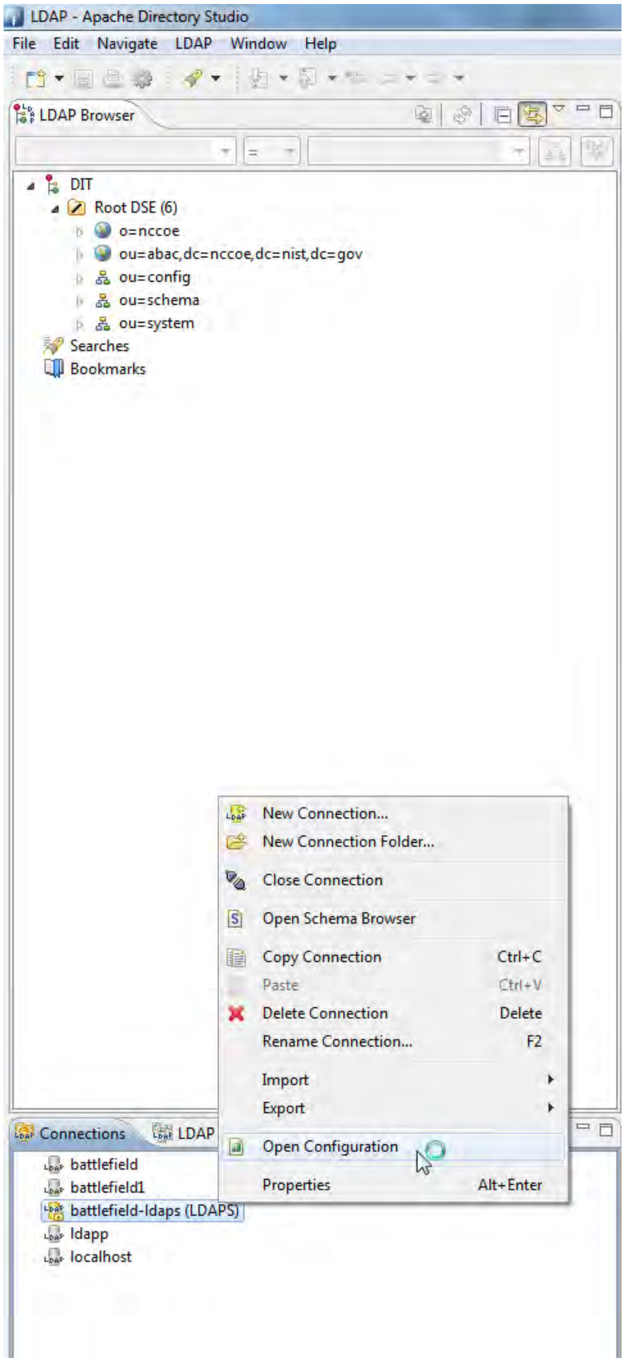
Modify Mode (no equality matching rule): Optimized Modify Operations

Modify Order: DELETE First

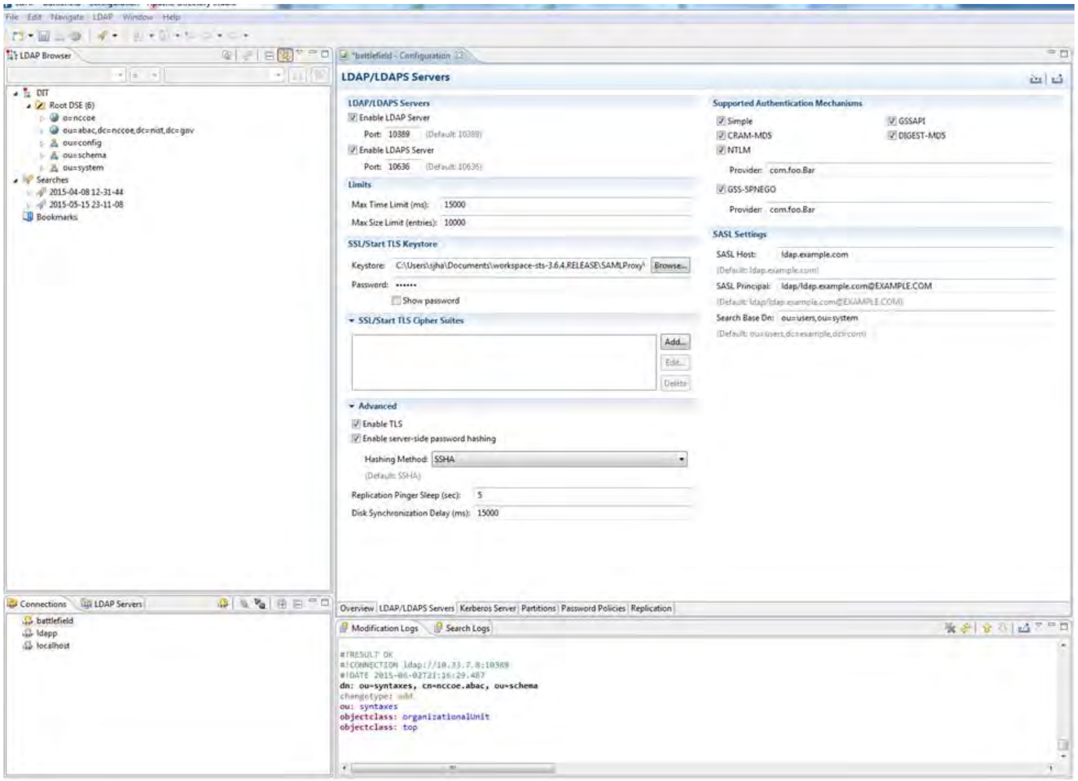
857

Option	Description	Default
Modify Mode	Specify the modify mode for attributes with an equality matching rule. Options: ■ Optimized Modify Operations: uses add/delete by default, uses replace if operation count is less ■ Always REPLACE: always uses replace operations to perform entry modifications ■ Always ADD/DELETE: always uses add and/or delete operations to perform entry modifications	Optimized Modify Operations
Modify Mode (no equality matching rule)	Specify the modify mode for attributes with no equality matching rule. Options: ■ Optimized Modify Operations: uses add/delete by default, uses replace if operation count is less ■ Always REPLACE: always uses replace operations to perform entry modifications ■ Always ADD/DELETE: always uses add and/or delete operations to perform entry modifications Recommended values for various LDAP servers: ■ ApacheDS: Optimized Modify Operations or REPLACE ■ OpenLDAP: REPLACE ■ OpenDS / SunDSEE: Optimized Modify Operations or REPLACE ■ FedoraDS / 389DS: Optimized Modify Operations (missing equality matching rules for many standard attribute types) ■ Active Directory: Optimized Modify Operations (exposes no equality matching rules at all) ■ eDirectory: Optimized Modify Operations (exposes no equality matching rules at all)	Optimized Modify Operations
Modify Order	Specify the modify order when using add and delete operations.	Delete first

859 6. Go to Open Configuration for the newly created connection.



860



LDAP/LDAPS Servers

LDAP/LDAPS Servers

☑ Enable LDAP Server

Port: 10389 (Default: 10389)

☑ Enable LDAPS Server

Port: 10636 (Default: 10636)

Limits

Max Time Limit (ms): 15000

Max Size Limit (entries): 10000

SSL/Start TLS Keystore

Keystore: C:\Users\sjha\Documents\workspace-sts-3.6.4.RELEASE\SAMLProxy\

Password: ••••••

☐ Show password

SSL/Start TLS Cipher Suites

Advanced

☑ Enable TLS

☑ Enable server-side password hashing

Hashing Method: SSHA (Default: SSHA)

Replication Pinger Sleep (sec): 5

Disk Synchronization Delay (ms): 15000

Supported Authentication Mechanisms

☑ Simple ☑ GSSAPI

☑ CRAM-MD5 ☑ DIGEST-MD5

☑ NTLM

Provider: com.foo.Bar

☑ GSS-SPNEGO

Provider: com.foo.Bar

SASL Settings

SASL Host: ldap.example.com (Default: ldap.example.com)

SASL Principal: ldap/ldap.example.com@EXAMPLE.COM (Default: ldap/ldap.example.com@EXAMPLE.COM)

Search Base Dn: ou=users,ou=system (Default: ou=users,dc=example,dc=com)

```
#!RESULT OK
#!CONNECTION ldap://10.33.7.8:10389
#!DATE 2015-06-02T21:16:29.487
dn: ou=syntaxes, cn=nccoe.abac, ou=schema
changetype: add
ou: syntaxes
objectclass: organizationalUnit
objectclass: top
```

Property	Description	Default
keystoreFile	Path of the X509 (or JKS) certificate file for LDAPS	none
certificatePassword	Password used to load the LDAPS certificate file	changeit
port	LDAPS TCP/IP port number to listen to	10636
enableSSL	Sets if SSL is enabled or not	true

7. Make sure **Enable LDAPS Server** is checked, and **Port** is the same as provided during creation of the connection.
8. Go to **SSL/Start TLS Keystore**.
9. Provide the **location** of the Keystore file and the **password** for the certificate.
10. **Save** the configuration.
11. **Restart** the server.

10.7.1.2 Verification

OpenSSL was used to acquire the server public certificate.

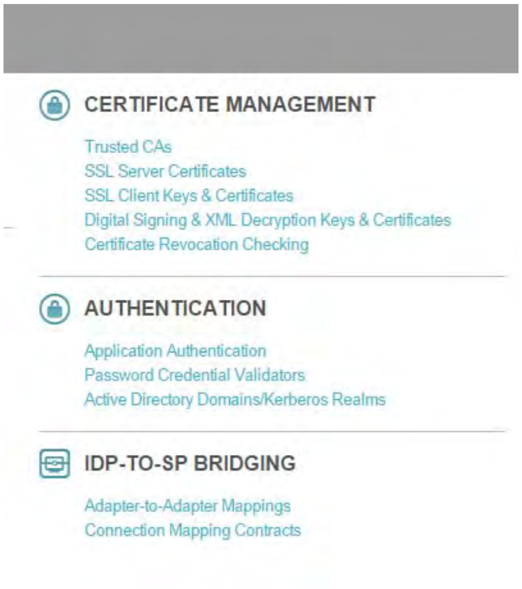
```
>openssl s_client -showcerts -connect 10.33.7.8:10636 < /dev/null |
openssl x509 -outform PEM > dir.pem
```

```
depth=0 C = US, O = ASF, OU = Directory, CN =
battlefield.bb-abac-bb1.nccoe.lab
```

```
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = US, O = ASF, OU = Directory, CN =
battlefield.bb-abac-bb1.nccoe.lab
verify error:num=27:certificate not trusted
verify return:1
depth=0 C = US, O = ASF, OU = Directory, CN =
battlefield.bb-abac-bb1.nccoe.lab
verify error:num=21:unable to verify the first certificate
verify return:1
DONE
[sjha@battlefield ~]$ more dir.pem
-----BEGIN CERTIFICATE-----
MIIBjDCCATYCBgFMlJE24DANBgkqhkiG9w0BAQUFADBCMQswCQYDVQQGEwJVUzEM
MAoGA1UEChMDQVNGMRIwEAYDVQQLEwlEaXJlY3RvcnkxETAPBgNVBAMTCEFwYWNo
ZURTMB4XDTE1MDQwNzE1NDgwN1oXDTE2MDQwNjE1NDgwN1owWzELMAkGA1UEBhMC
VVMxDDAKBgNVBAoTA0FTRjESMBAGA1UECxMJRGlyZWN0b3J5MSowKAYDVQQDEyFi
YXR0bGVmaWVsZC5iYi1hYmFjLWJiMS5uY2NvZS5sYWIwXDANBgkqhkiG9w0BAQEF
AANLADBIAkEAlLYJY8PJgMS82IqrW4uTVobkNqi2oJBoFAvOGMF7olPCQ4x5vrgS
6GEq9gUHk1ZZzymIIq6BMxoEb80l6lPY/wIDAQABMA0GCSqGSIb3DQEBBQUAA0EA
hXNpaGfF2Aboemwzt6U/fvSNyl+KRdeKFm0liWbseBk8OPvdOEmW96HVLvlbxSlc
JpSznkLFhFOe0fimwB6GEg==
-----END CERTIFICATE-----
```

Verify the certificate received from the directory server against the certificate that was loaded earlier.

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

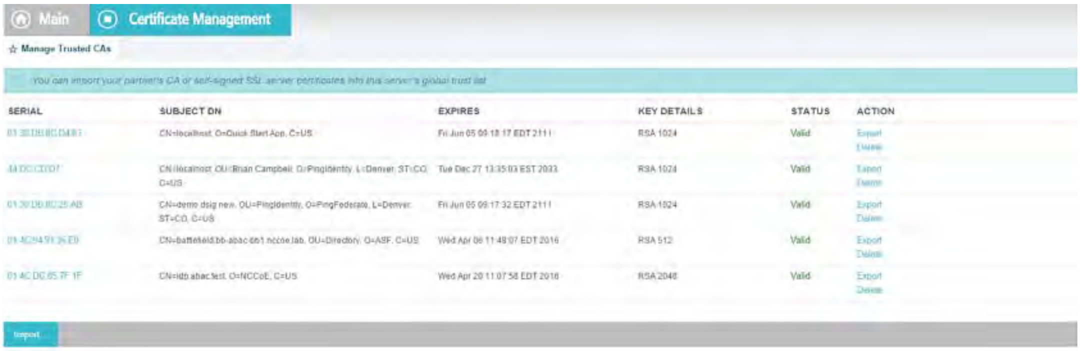
AUTHENTICATION

Application Authentication
Password Credential Validators
Active Directory Domains/Kerberos Realms

IDP-TO-SP BRIDGING

Adapter-to-Adapter Mappings
Connection Mapping Contracts

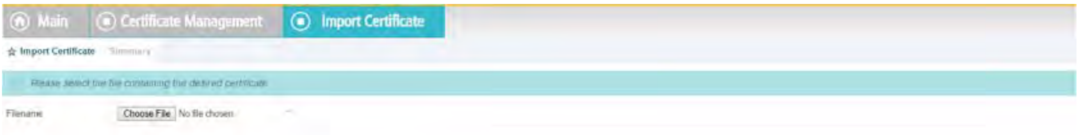
1. The following screen will appear, displaying all certificates on the server's global trust list.



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
01 38 DB BC D4 B3	CN=localhost, O=Quick Start App, C=US	Fri Jun 05 09:18:17 EDT 2111	RSA 1024	Valid	Export Delete
44 DC C1 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
01 39 DB BC 25 AB	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US	Fri Jun 05 09:17:32 EDT 2111	RSA 1024	Valid	Export Delete
01 4C 94 91 36 E0	CN=battlefield.bb-abac-bb1.nccoe.lab, OU=Directory, O=ASF, C=US	Wed Apr 06 11:48:07 EDT 2016	RSA 512	Valid	Export Delete
01 4C DC 65 7F 1F	CN=idb.abac.test, O=NCCoE, C=US	Wed Apr 20 11:07:58 EDT 2016	RSA 2048	Valid	Export Delete

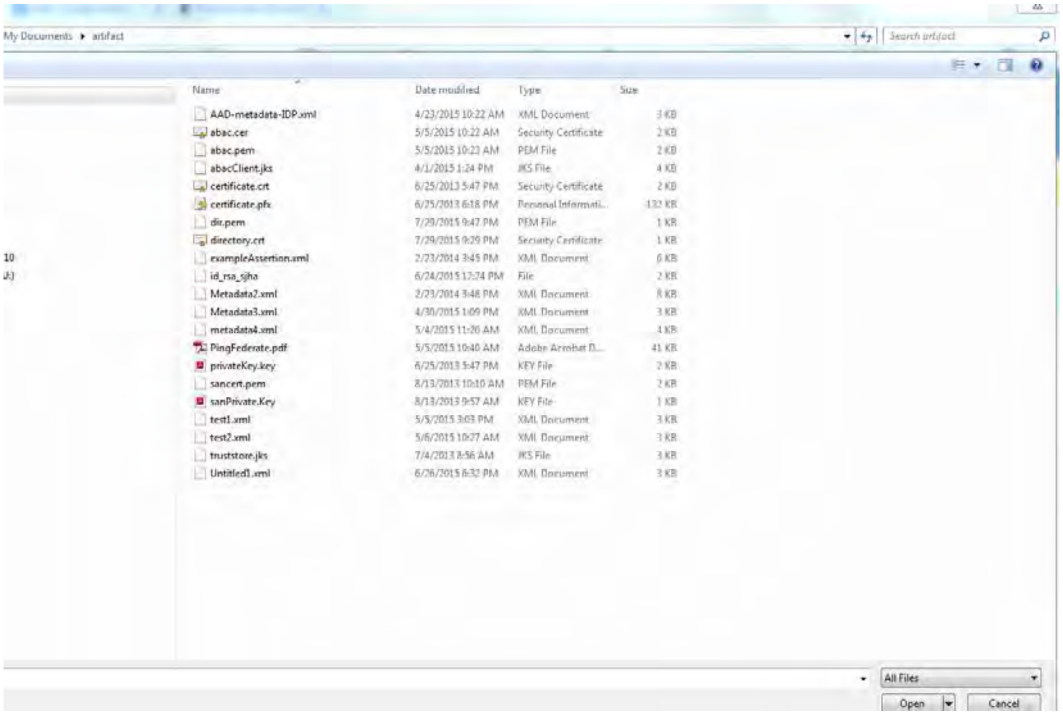
2. Select **Import Certificate**.



Please select the file containing the desired certificate

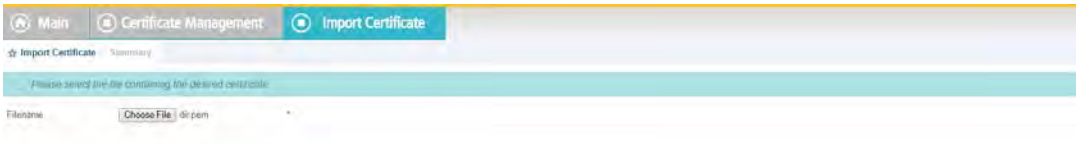
Filename Choose File No file chosen

3. Choose a file to import.



Name	Date modified	Type	Size
AAD-metadata-IDP.xml	4/23/2015 10:22 AM	XML Document	3 KB
abac.cer	5/5/2015 10:22 AM	Security Certificate	2 KB
abac.pem	5/5/2015 10:23 AM	PEM File	2 KB
abacClient.jks	4/1/2015 1:24 PM	JKS File	4 KB
certificate.crt	6/25/2013 5:47 PM	Security Certificate	2 KB
certificate.pfx	6/25/2013 6:18 PM	Personal Informati...	132 KB
dir.pem	7/29/2015 9:47 PM	PEM File	1 KB
directory.crt	7/29/2015 9:29 PM	Security Certificate	1 KB
exampleAssertion.xml	2/23/2014 3:45 PM	XML Document	6 KB
id_rsa_sjha	6/24/2015 12:24 PM	File	2 KB
Metadata2.xml	2/23/2014 3:48 PM	XML Document	8 KB
Metadata3.xml	4/30/2015 1:09 PM	XML Document	3 KB
metadata4.xml	5/4/2015 11:26 AM	XML Document	4 KB
PingFederate.pdf	5/5/2015 10:40 AM	Adobe Acrobat D...	41 KB
privateKey.key	6/25/2013 5:47 PM	KEY File	2 KB
sancert.pem	8/13/2013 10:10 AM	PEM File	2 KB
sanPrivate.Key	8/13/2013 9:57 AM	KEY File	1 KB
test1.xml	5/5/2015 3:03 PM	XML Document	3 KB
test2.xml	5/6/2015 10:27 AM	XML Document	3 KB
truststore.jks	7/4/2013 8:56 AM	JKS File	3 KB
Untitled1.xml	6/26/2015 6:32 PM	XML Document	3 KB

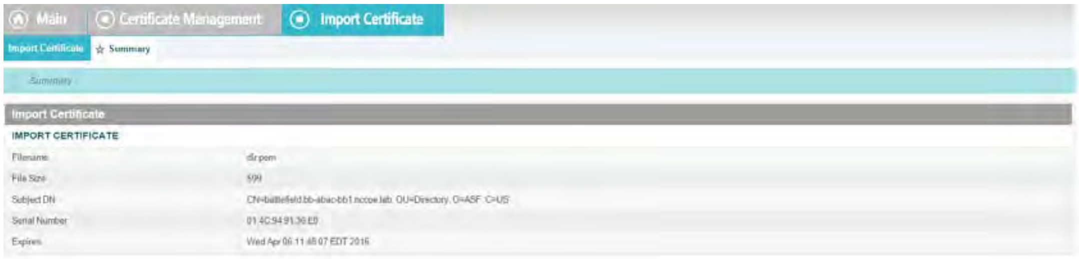
4. Once your chosen file appears in the **Filename** field, click **Next**.



Please select the file containing the desired certificate

Filename Choose File dir.pem *

5. View the **Summary** of the imported certificate.



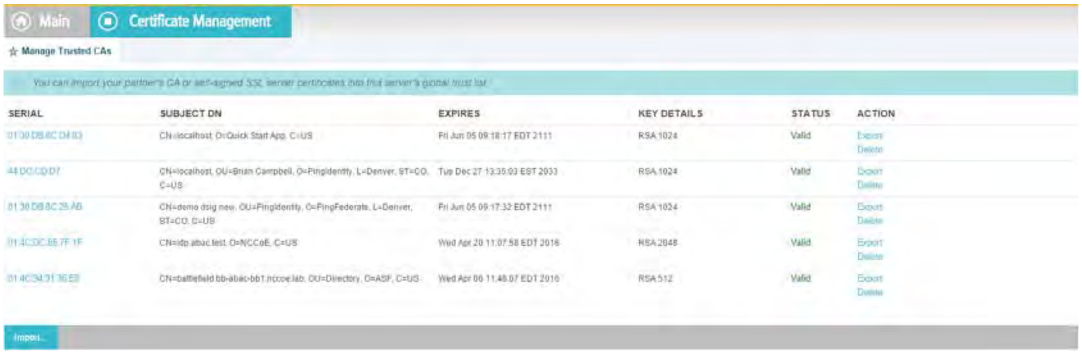
Summary

Import Certificate

IMPORT CERTIFICATE

Filename	dir.pem
File Size	599
Subject DN	CN=battlefield.bb-abac-bb1.nccoe.lab, OU=Directory, O=ASF, C=US
Serial Number	01 4C 94 91 36 E0
Expires	Wed Apr 06 11:48:07 EDT 2016

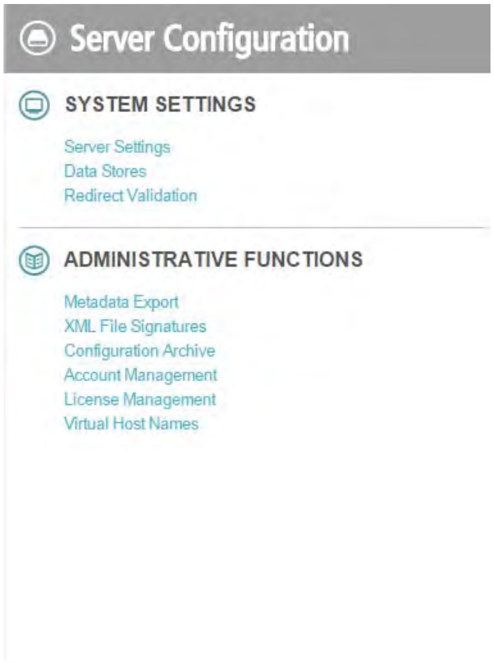
6. Click **Done**. The main screen will display a list of certificates. Click **Save**.



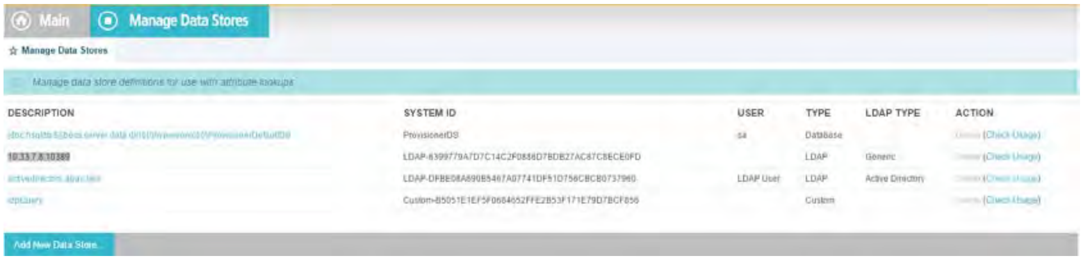
You can import your partner's CA or self-signed SSL server certificates into this server's global trust list.

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTION
01 30 DB 8C D4 83	CN=localhost, O=Quick Start App, C=US	Fri Jun 05 09:18:17 EDT 2111	RSA 1024	Valid	Export Delete
44 DC CD D7	CN=localhost, OU=Brian Campbell, O=PingIdentity, L=Denver, ST=CO, C=US	Tue Dec 27 13:35:03 EST 2033	RSA 1024	Valid	Export Delete
01 30 DB 8C 25 AB	CN=demo dsig new, OU=PingIdentity, O=PingFederate, L=Denver, ST=CO, C=US	Fri Jun 05 09:17:32 EDT 2111	RSA 1024	Valid	Export Delete
01 4C DC 85 7F 1F	CN=idp.abac.test, O=NCCoE, C=US	Wed Apr 20 11:07:58 EDT 2016	RSA 2048	Valid	Export Delete
01 4C 34 31 36 E8	CN=battlefield.bb-abac-bb1.nccoe.lab, OU=Directory, O=ASF, C=US	Wed Apr 06 11:48:07 EDT 2016	RSA 512	Valid	Export Delete

10.7.1.4 Creation of Data Store to Connect to ApacheDS



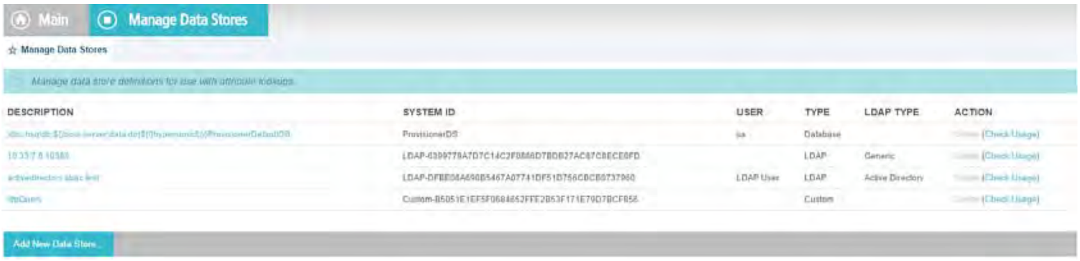
1. Click on **Data Stores**.



Manage data store definitions for use with attribute lookups

DESCRIPTION	SYSTEM ID	USER	TYPE	LDAP TYPE	ACTION
jdbc:hsqldb:${pf.server.data.dir}${/}hypersonic${/}ProvisionerDefaultDB	ProvisionerDS	sa	Database		Delete (Check Usage)
10.33.7.8:10389	LDAP-6399779A7D7C14C2F0886D7BDB27AC87C8ECE0FD		LDAP	Generic	Delete (Check Usage)
activedirectory.abac.test	LDAP-DFBE08A690B5467A07741DF51D756CBCB0737960	LDAP User	LDAP	Active Directory	Delete (Check Usage)
idpUsers	Custom-B5051E1EF5F0684652FFE2B53F171E79D7BCF856		Custom		Delete (Check Usage)

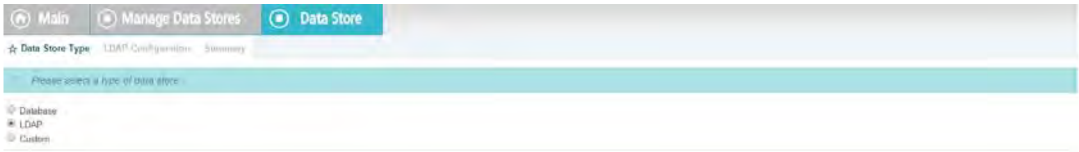
2. In the Manage Data Stores window, click **Add New Data Store**.



Manage data store definitions for use with attribute lookups.

DESCRIPTION	SYSTEM ID	USER	TYPE	LDAP TYPE	ACTION
jdbc:hsqldb:${pf.server.data.dir}${/}hypersonic${/}ProvisionerDefaultDB	ProvisionerDS	sa	Database		(Check Usage)
10.33.7.8:10389	LDAP-6399779A7D7C14C2F0866D7BDB27AC87C8ECE0FD		LDAP	Generic	(Check Usage)
activedirectory.abac.lab	LDAP-DFBE08A690B5467A07741DF51D756CBCB0737960	LDAP User	LDAP	Active Directory	(Check Usage)
ttpCusers	Custom-B5051E1EF5F0684652FFE2B53F171E79D7BCF858		Custom		(Check Usage)

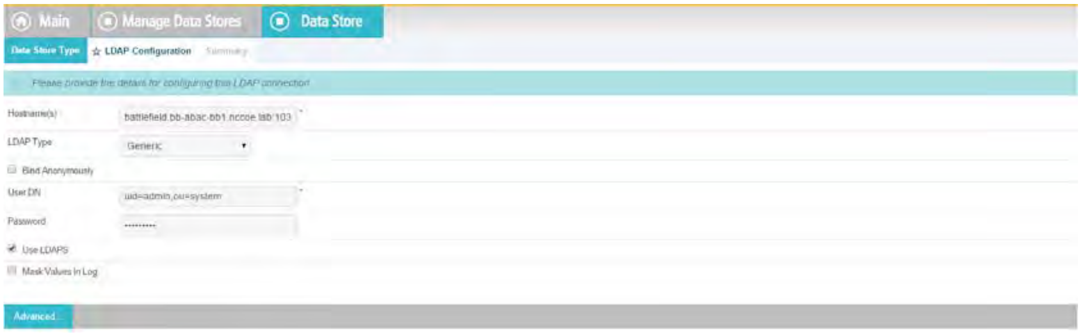
3. Choose **LDAP**, and click **Next**.



Please select a type of data store.

○ Database
● LDAP
○ Custom

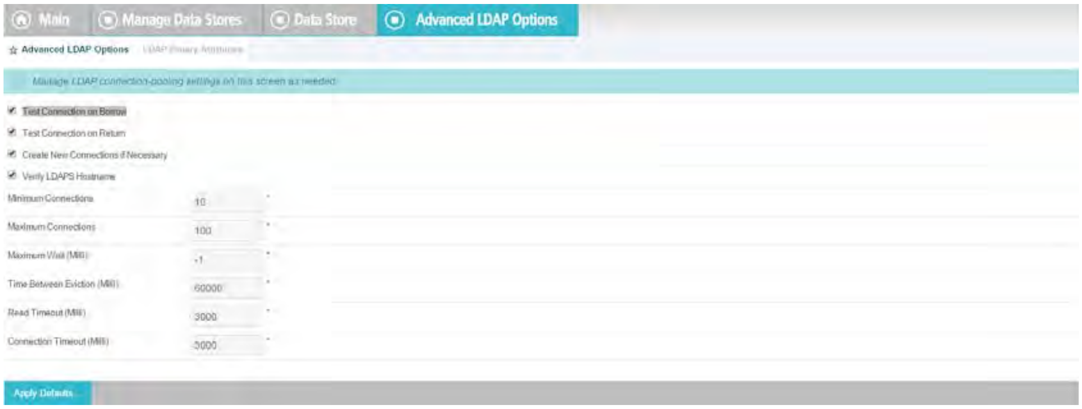
4. Provide a **Hostname** and **Ldaptype**.



Please provide the details for configuring this LDAP connection.

Hostname(s): battlefield.bb-abac-bb1.nccoe.lab:103 *
LDAP Type: Generic ▾
☐ Bind Anonymously
User DN: uid=admin,ou=system *
Password: ••••••••••
☑ Use LDAPS
☐ Mask Values in Log

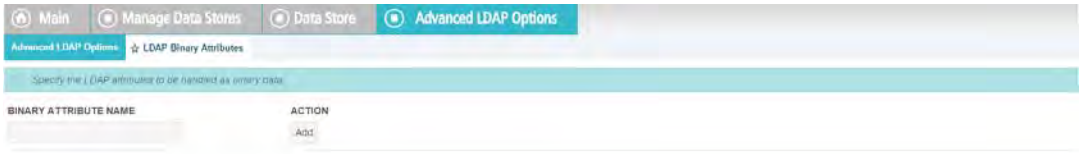
5. It may be necessary to configure connection pooling. It is important to select **Verify LDAPS Hostname** if the directory server certificate is bound to a hostname, and this hostname can be verified.



Manage LDAP connection-pooling settings on this screen as needed.

☑ Test Connection on Borrow
☑ Test Connection on Return
☑ Create New Connections if Necessary
☑ Verify LDAPS Hostname
Minimum Connections: 10 *
Maximum Connections: 100 *
Maximum Wait (Milli): -1 *
Time Between Eviction (Milli): 60000 *
Read Timeout (Milli): 3000 *
Connection Timeout (Milli): 3000 *

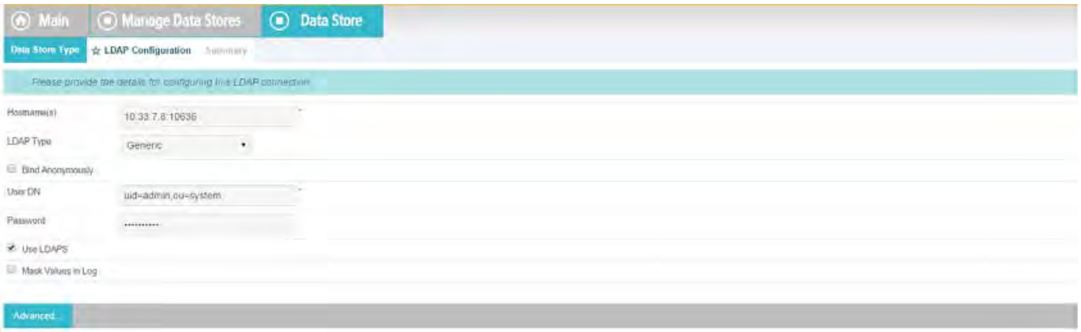
6. If there is any binary data, enter it in the **Binary Attribute Name Field**, and click **Add**.



Specify the LDAP attributes to be handled as binary data

BINARY ATTRIBUTE NAME	ACTION
	Add

7. A summary of the LDAP configuration will appear.



Please provide the details for configuring the LDAP connection

Hostname(s) 10.33.7.8:10636

LDAP Type Generic

□ Bind Anonymously

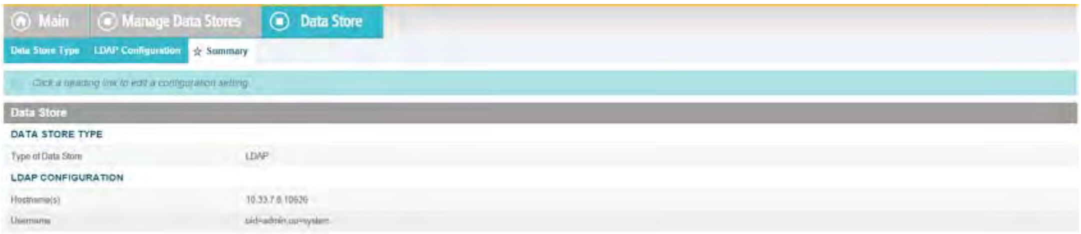
User DN uid=admin,ou=system

Password ••••••••••

☑ Use LDAPS

□ Mask Values in Log

8. A **Summary** of the connection will appear as following. Click **Save**. You will then return to the Main Admin console.



Click a heading link to edit a configuration setting.

Data Store

DATA STORE TYPE

Type of Data Store	LDAP

LDAP CONFIGURATION

Hostname(s)	10.33.7.8:10636
Username	uid=admin,ou=system

10.8 Configuration of PingFederate to Query the JIT Cache when Responding to Secondary Attribute Requests

10.8.1 Introduction

This section will cover all the configuration steps required to enable PingFederate RP to communicate with the Secondary attribute Provider and respond to its queries. The SP connection section will cover communication channel protection and message protection. To fulfill the query request from the NextLabs PIP Plugin and Protocol Broker, PingFederate queries its local LDAP server called Just in Time (JIT) cache. Note that PingFederate RP may not have data to fulfill the query. In that case, PingFederate RP extends the query to PingFederate IdP using a unique method (Ping Data source).

A Data Store is any type of source for digitized data, i.e., database, file, stream, etc. PingFederate administration console uses this term for system settings. In the Java software platform, data source is a factory for connections to the physical data source that this data source object represents. Thus, data source is the logical manifestation of a physical data store in a java application. Due to this, the terms will be used interchangeably below.

This section provides the configuration needed to query JIT cache, i.e., creation of the data source for the LDAP Server. We have already discussed the configuration of Ping Data Source in Custom Data Store section. SP connection describes how both of these data stores are chained together to fetch the result of the attribute query.

10.8.2 Prerequisites

Before starting this configuration, the following steps must have already been completed:

1. How-To Guides 1-6
    a. Complete Installation of PingFederate, both RP and Idp
2. Installation and configuration of ApacheDS
3. Installation of Ping Custom Data Store
4. Availability of Ping web administration console (automatically included in the PingFederate installation from previous chapters)

10.8.2.1 SP Connection

As described above, PingFederate (RP) acts as an IdP for the Secondary attribute provider. In order to enable support for exchange of federation-protocol messages and provide channel protection, it is essential to configure the SP (Service Provider) connection. Note: Ping Identity's documentation uses the term **Service Provider** and **SP** where the rest of our ABAC documentation uses the term **Relying Party** and **RP**. In this document, please consider these terms interchangeable.

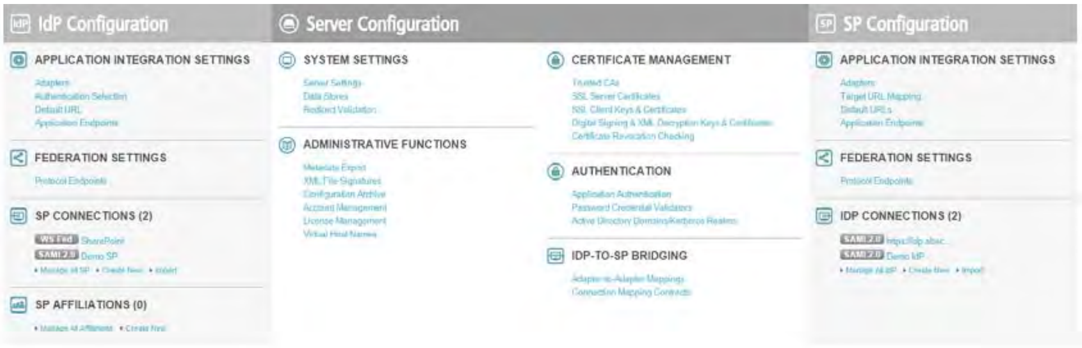
The following goals are achieved by configuration of the SP connection:

a. Specification of connection and associated security protocol (i.e., TLS/SSL)
b. Specification of SAML profile t including detailed security specifications (the use of digital signatures, signature verification, XML encryption)
c. Specification of Attributes that may be sent using the SAML2 Attribute Query profile
d. Specification of Data Store(s), if agreement between Idp and SP includes sending a SAML response containing attribute values from a local data store.

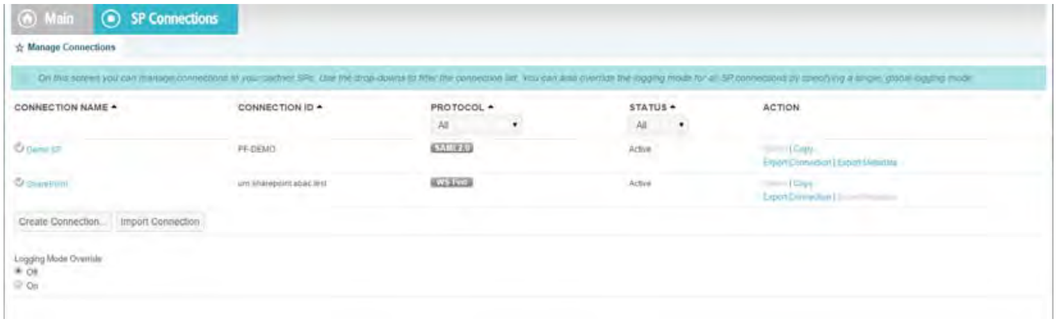
10.8.2.1.1 Specification of Profile

Instructions on how to create a new connection can be found here.

1. Click on **Manage on All SP** in the first column on the left hand side.



2. The following screen will appear. Click on **Create Connection**.

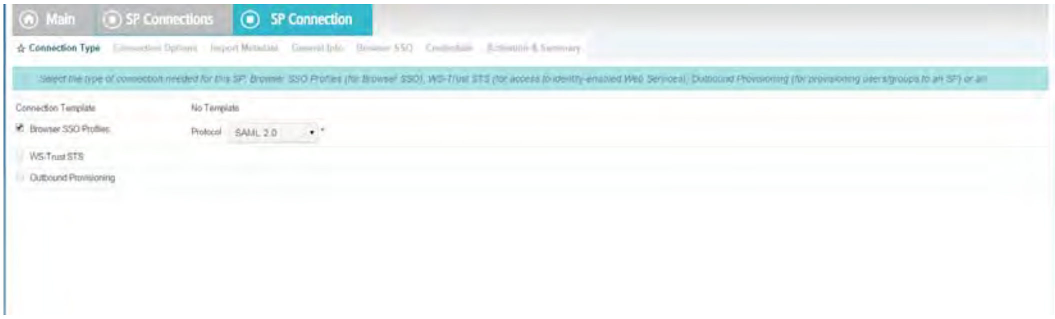


On this screen you can manage connections to your partner SPs. Use the drop-downs to filter the connection list. You can also override the logging mode for all SP connections by specifying a single, global logging mode.

CONNECTION NAME ▲	CONNECTION ID ▲	PROTOCOL ▲ All ▾	STATUS ▲ All ▾	ACTION
Demo SP	PF-DEMO	SAML 2.0	Active	Delete | Copy Export Connection | Export Metadata
SharePoint	urn:sharepoint:abac:test	WS-Fed	Active	Delete | Copy Export Connection | Export Metadata

Logging Mode Override
● Off
○ On

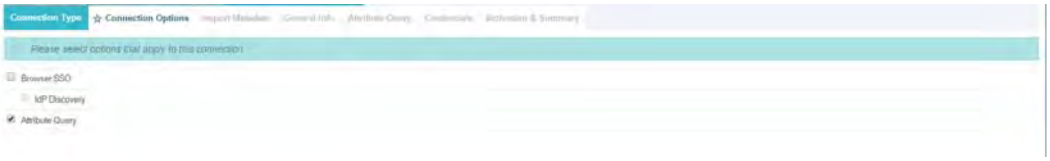
3. Check the box for **Browser SSO Profiles** and select **SAML 2.0** as protocol from the drop-down menu.



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

Connection Template   No Template
☑ Browser SSO Profiles   Protocol SAML 2.0 ▾ *
☐ WS-Trust STS
☐ Outbound Provisioning

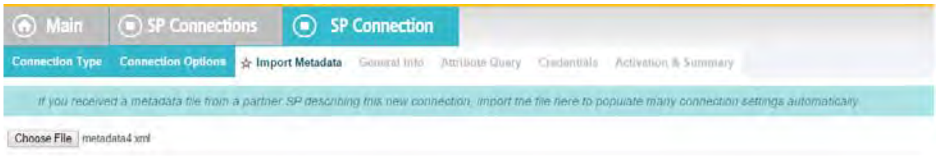
4. Uncheck **Browser SSO**, check **Attribute Query**, and click **Next**.



Please select options that apply to this connection

☐ Browser SSO
☐ IdP Discovery
☑ Attribute Query

5. Choose a metadata file and click **Next**.



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

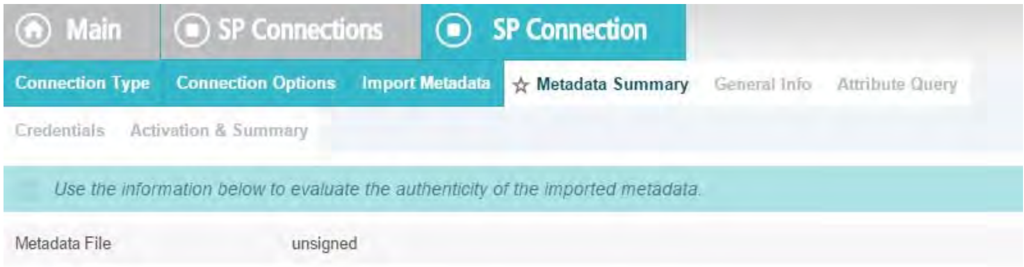
Choose File metadata4.xml

6. SAML2 metadata has its own specification. As per this specification, KeyDescriptor is an optional sequence of elements that provides information about the cryptographic keys that the entity uses when acting in this role. However, for message authentication and integrity, it is essential to provide the certificate so that signed messages coming from the secondary attribute provider can be verified. A relevant part of metadata is shown here:

```
<md:KeyDescriptor use="signing">
             <ds:KeyInfo>
             <ds:X509Data>
 <ds:X509Certificate>
 MIIE4jCCAsqgAwIBAgICEAMwDQYJKoZIhvcNAQELBQAwYjELMAkGA1UEBhMCVVMx
 ETAPBgNVBAgMCE1hcnlsYW5kMRIwEAYDVQQHDAlSb2NrdmlsbGUxDjAMBgNVBAoM
 BU5DQ29FMQ0wCwYDVQQLDARBQkFDMQ0wCwYDVQQDDARBQkFDMB4XDTE1MDQwMTE4
 MTA1NloXDTE2MDMzMTE4MTA1NlowejELMAkGA1UEBhMCVVMxETAPBgNVBAgMCE1h
 cnlsYW5kMQ4wDAYDVQQKDAVOQ0NvRTENMAsGA1UECwwEQUJBQzEUMBIGA1UEAwwL
 TU0xOTU1OTItUEMxIzAhBgkqhkiG9w0BCQEWFHNqaGFATU0xOTU1OTItUEMub3Jn
 MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzxrL5iAIpNyEXHmGTDW
 1mzx7YJal/c9Ruxag3sifjzuUdBjEznFJJxaagM2pzTUI5JCaLzgm71VSBmuVL+6
 PzTxReM3i5XzWjpgRMIizadnQT0wmCryKuNaQiBIFLoMbi+ySdBvu+M/xhHlRxuF
 jY9NPSE1MHL8YaLoKW2SFIm/3bhJ/xF7q7FGHMcJH4Zzr2QpQmBEryozJJV3z4Zv
 Vro/MfyLg1VER0pu36e32hIyzsf2gKizv00qY2ecDlBCNTITsA2HWSTf50kpvT4q
 upCnXVKVqzDPZON0XCsJJcwWsUi9pRvkGtVBXqhh282ODyzcl3nkpgsl5F8hR7kO
 jQIDAQABo4GJMIGGMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMCwGCWCGSAGG+EIB
 DQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQURPRr
 8BNghnDip40B1sy6AWpWJmcwHwYDVR0jBBgwFoAUyZ5WFPtCW/BOjVxvof8eNcBo
 5c8wDQYJKoZIhvcNAQELBQADggIBAGhVMd47uFNi1z8oEYgwDInZDAtfujvkfTu2
 Dtr7dvkvB2x6uW481ffIKDKb48yKVBMO0kSwU4esPHgMWowJJs37XFo9PYJ1kaE/
 NCD7e8V4p3xhzXux6JqKpaho1xHifzEsdKqOyNj00ZXqmRMstbw6UC+IFCNUWJZQ
 zJ+Dwciaxa9kq/huv8BMbYzcL8r1fE3x9nUwwwuFuXudpnED0B+Rmmod1G5fVG1j
 agMWakXscGJ9rpT8wgfJGjU4Sct3Eocp5roRGopUVBrW6jljZD4dYEu1eJ1LJqcW
 mDiYdZIvu0z393HApNpwC4XSaMoTN7xq4Z+Xwe0zdt1HVM0aeAiglrDB3XKuiYQT
 Ab899WBgK/TixTLJ+Nf6FkAl2apkVkaxxl+35DZrkDOHo3HQTORQFNYcb1LlrsfP
 A5r0PPVi6XE6h4k9/CgO03Q6fzpgl7avCrw8s1m/WnmQjfc0K+op7l7zsYrnsxdB
 wQsnaT6GX2csy99jOpfLKlSh6jaIuFdRPMEwjhNyqTy2xoLfuYK5bxMzlpfaoZEs
```

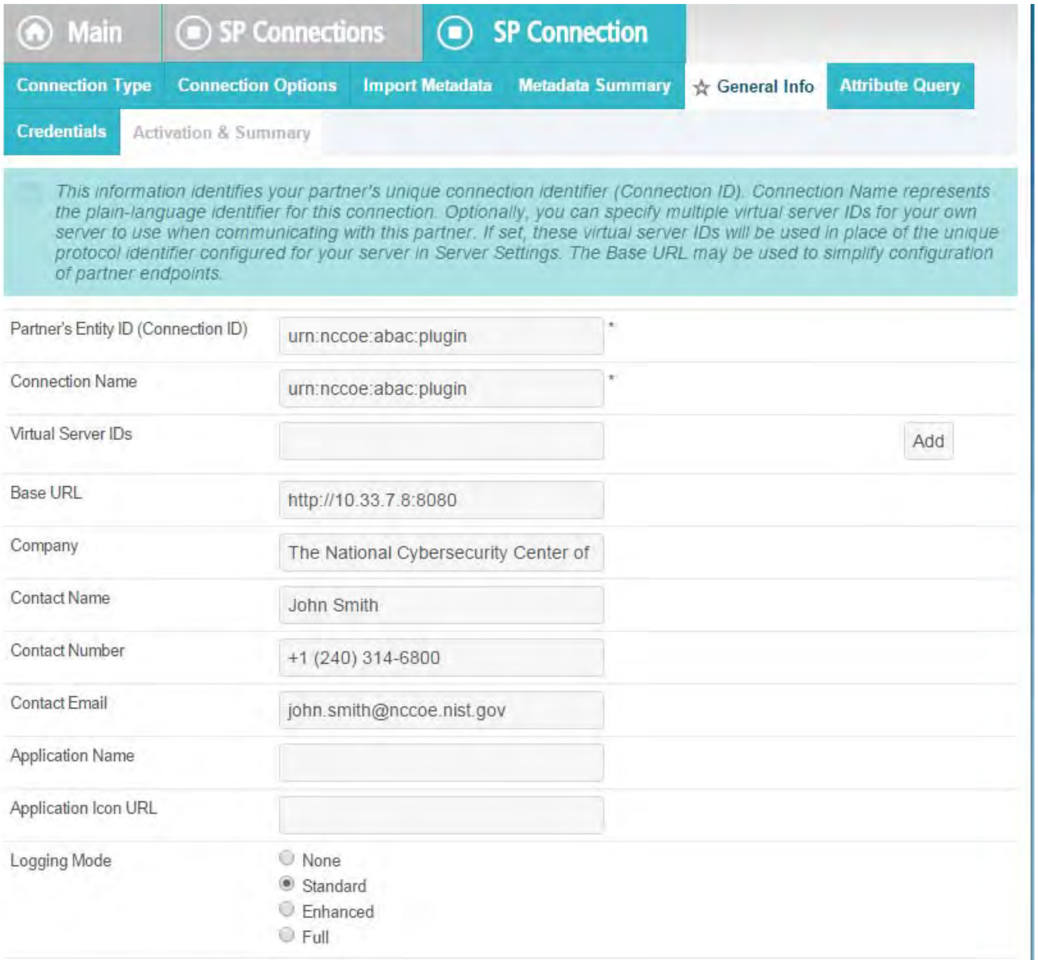
```
      sVURPCFiC0G97xn8ffjjhv5Kby8JIRWV2QhXicf5FsWoiWZIHtHo0L9WEQXKPTO1
      +831OxJDW6bosdNww8IbRft1MYqGWYCTnwmBshURCXSJrjpE/MInE5nw/7QWA/OR
      U3r4Pv6s
                   </ds:X509Certificate>
                   </ds:X509Data>
                  </ds:KeyInfo>
    </md:KeyDescriptor>
```

7. Verify the metadata content.



Use the information below to evaluate the authenticity of the imported metadata.

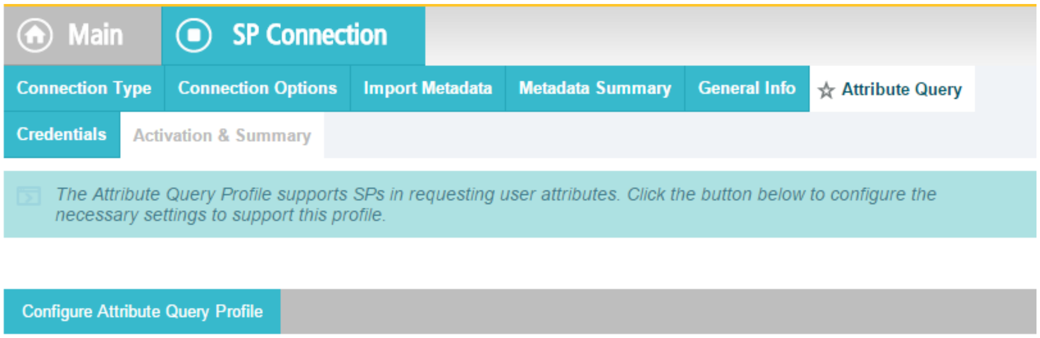
Metadata File	unsigned



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

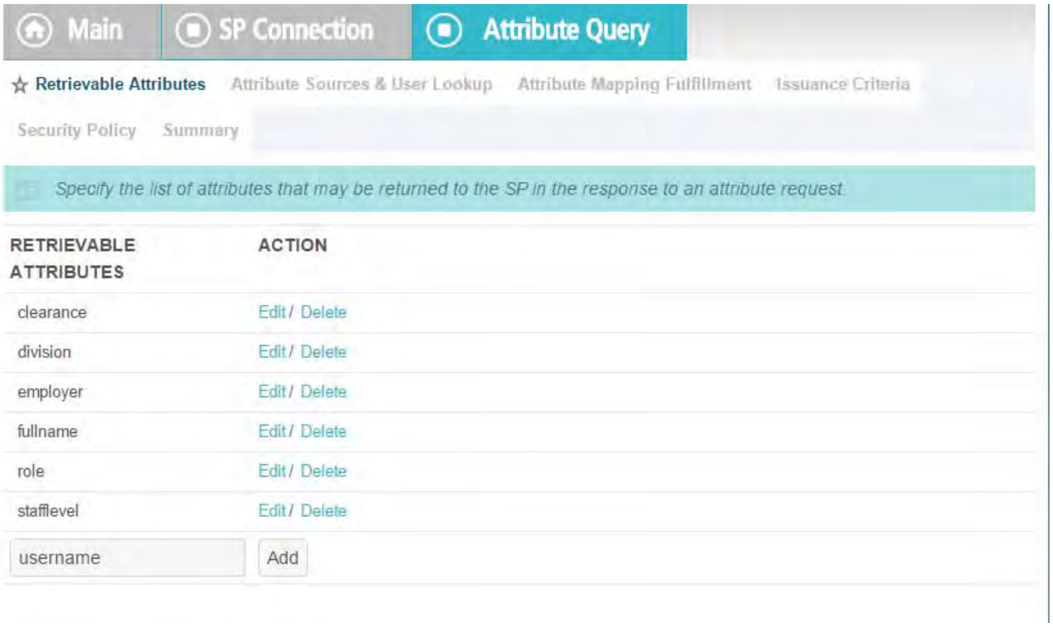
Partner's Entity ID (Connection ID)	urn:nccoe:abac:plugin *
Connection Name	urn:nccoe:abac:plugin *
Virtual Server IDs	
Base URL	http://10.33.7.8:8080
Company	The National Cybersecurity Center of
Contact Name	John Smith
Contact Number	+1 (240) 314-6800
Contact Email	john.smith@nccoe.nist.gov
Application Name	
Application Icon URL	
Logging Mode	○ None ● Standard ○ Enhanced ○ Full

8. Click on **Configure Attribute Query Profile**.



The Attribute Query Profile supports SPs in requesting user attributes. Click the button below to configure the necessary settings to support this profile.

9. Specify the list of attributes that may be returned to the SP in response to an attribute request.

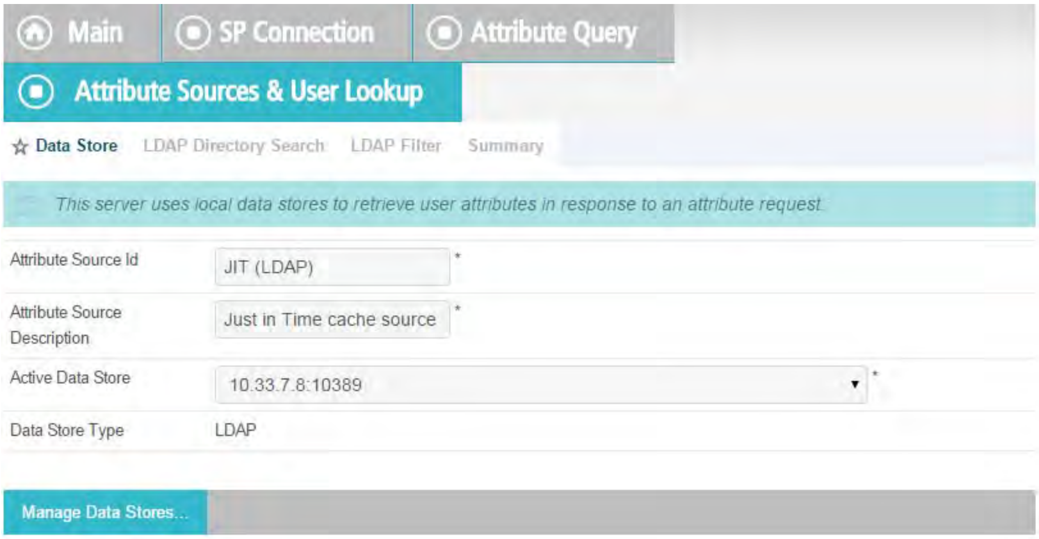


Specify the list of attributes that may be returned to the SP in the response to an attribute request

RETRIEVABLE ATTRIBUTES	ACTION
clearance	Edit / Delete
division	Edit / Delete
employer	Edit / Delete
fullname	Edit / Delete
role	Edit / Delete
stafflevel	Edit / Delete
username	Add

10.8.2.1.2 Specify a series of data stores.

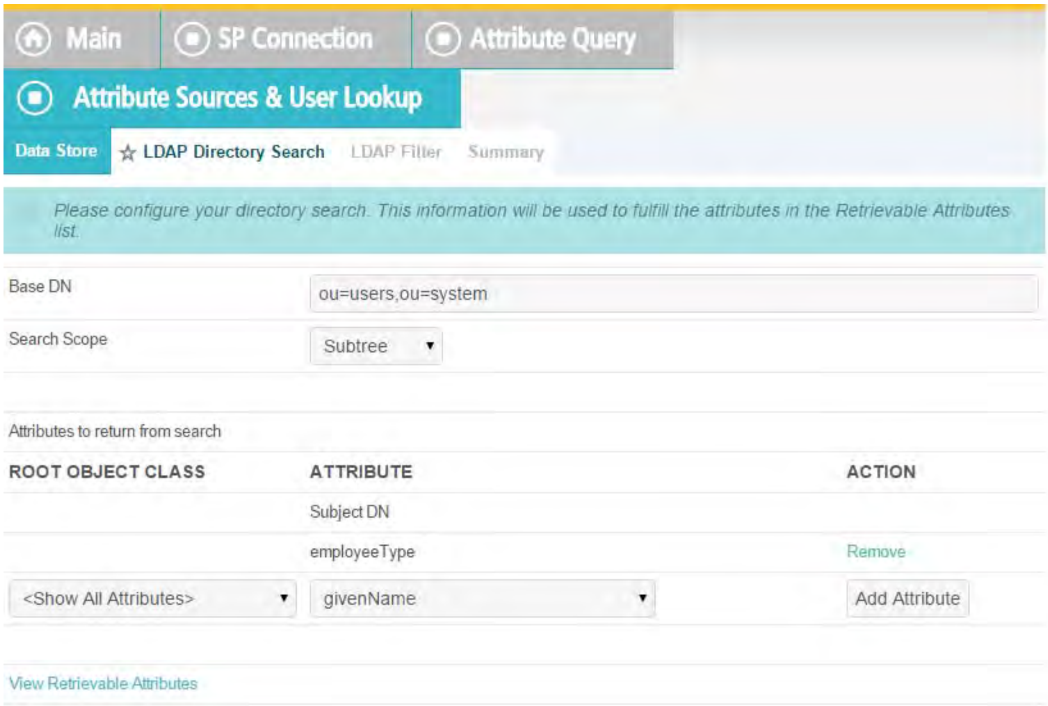
1. In the **Attribute Source Id** field, specify **JIT (LDAP)**.



This server uses local data stores to retrieve user attributes in response to an attribute request.

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

2. Specify **Attributes** for the JIT Cache.



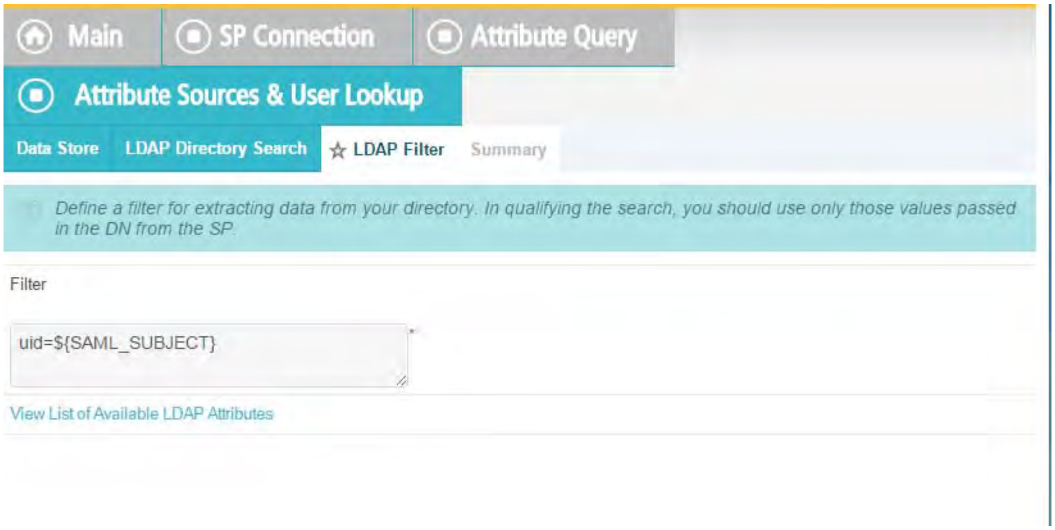
Please configure your directory search. This information will be used to fulfill the attributes in the Retrievable Attributes list.

Base DN	ou=users,ou=system
Search Scope	Subtree ▾

Attributes to return from search

ROOT OBJECT CLASS	ATTRIBUTE	ACTION
	Subject DN	
	employeeType	Remove
<Show All Attributes> ▾	givenName ▾	Add Attribute

3. Specify **LDAP Filter**.

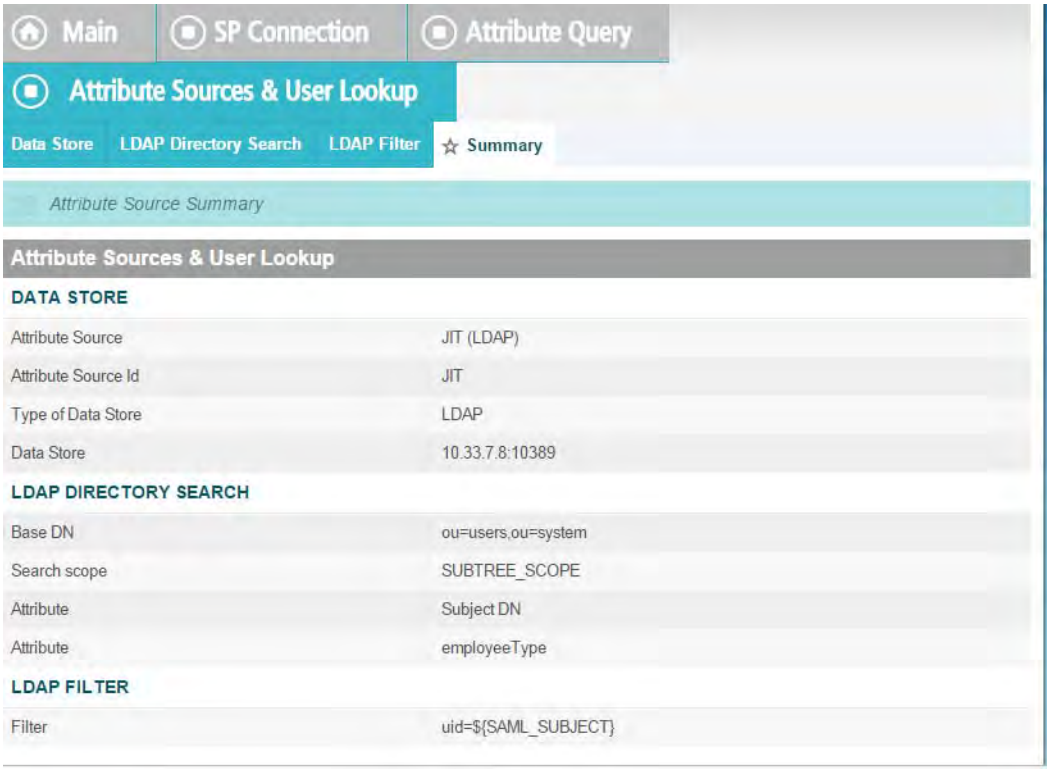


Define a filter for extracting data from your directory. In qualifying the search, you should use only those values passed in the DN from the SP.

Filter

uid=${SAML_SUBJECT}

4. Verify that your data is correct.

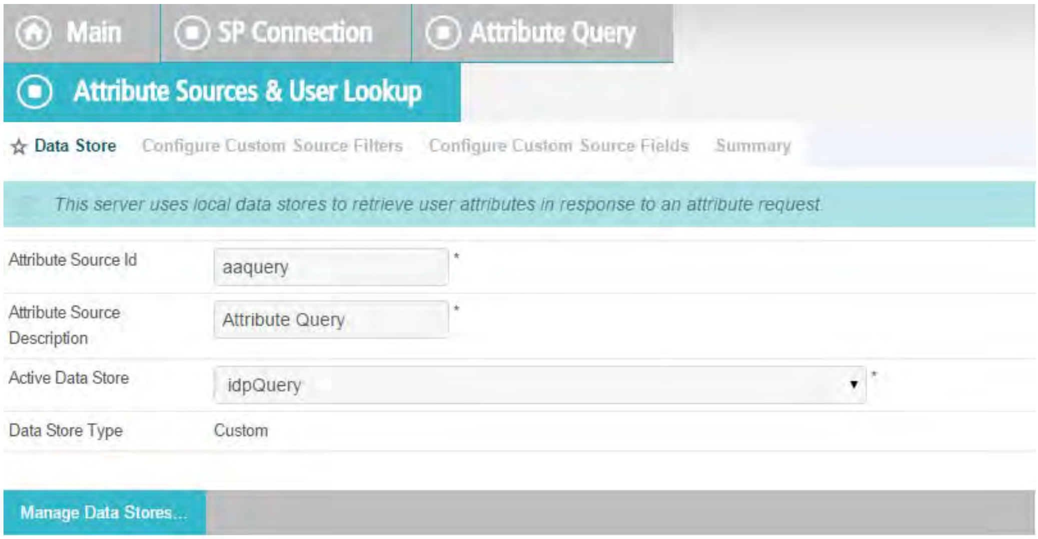


Attribute Source Summary

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}

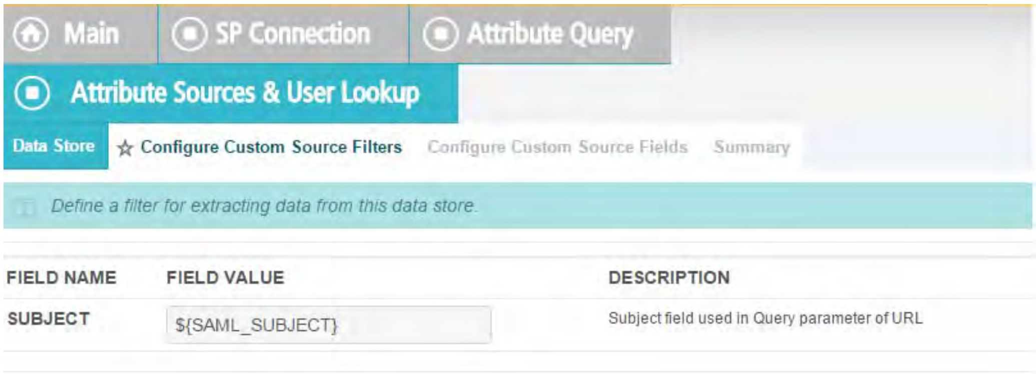
5. Specify a custom **Data Store**.


Main
SP Connection
Attribute Query
Attribute Sources & User Lookup
☆ Data Store
Configure Custom Source Filters
Configure Custom Source Fields
Summary
Manage Data Stores...

This server uses local data stores to retrieve user attributes in response to an attribute request.

Attribute Source Id	aaquery *
Attribute Source Description	Attribute Query *
Active Data Store	idpQuery ▾ *
Data Store Type	Custom

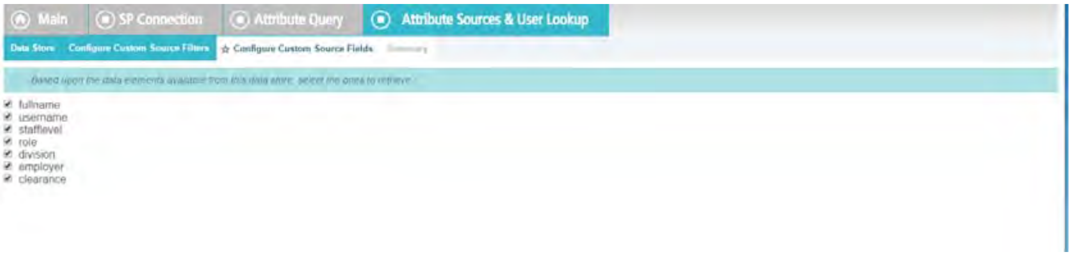
6. Define a filter for extracting data from this data store.


Main
SP Connection
Attribute Query
Attribute Sources & User Lookup
Data Store
☆ Configure Custom Source Filters
Configure Custom Source Fields
Summary

Define a filter for extracting data from this data store.

FIELD NAME	FIELD VALUE	DESCRIPTION
SUBJECT	${SAML_SUBJECT}	Subject field used in Query parameter of URL

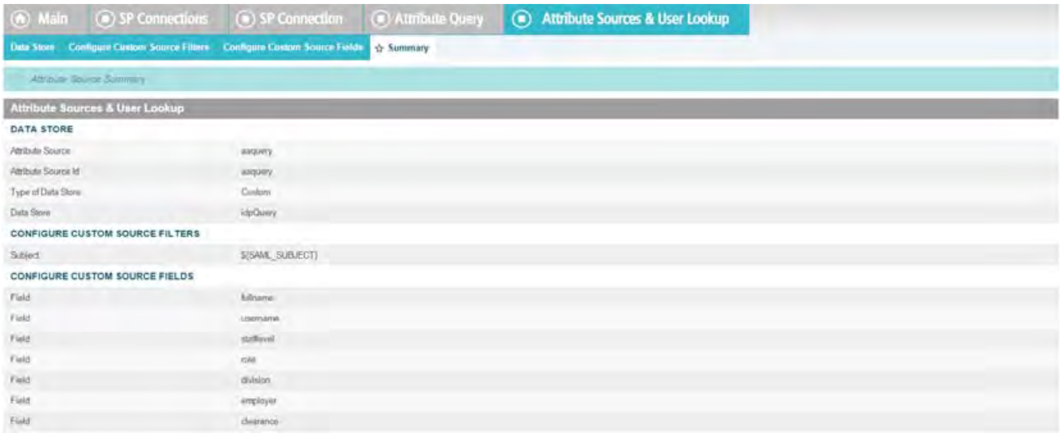
7. Based on the data elements available from this data store, select the ones pertinent to this connection. Note that these are the attributes you previously selected to return from Ping Custom Data.


Main
SP Connection
Attribute Query
Attribute Sources & User Lookup
Data Store
Configure Custom Source Filters
☆ Configure Custom Source Fields
Summary

Based upon the data elements available from this data store, select the ones to retrieve.

- ☑ fullname
- ☑ username
- ☑ stafflevel
- ☑ role
- ☑ division
- ☑ employer
- ☑ clearance

8. Click **Retrieve**.

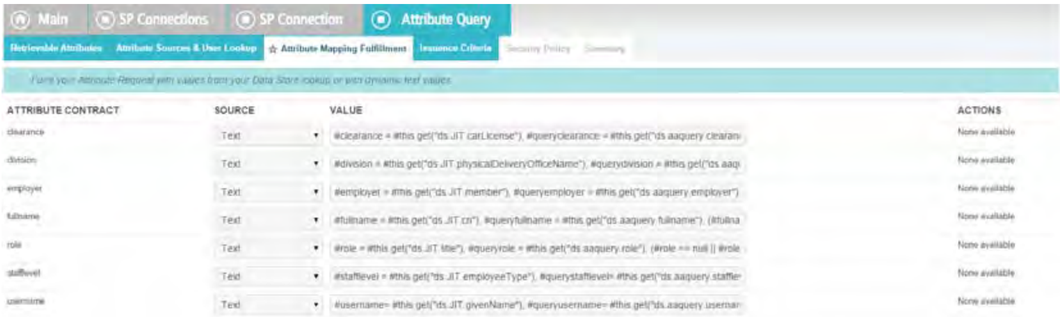

Main
SP Connections
SP Connection
Attribute Query
Attribute Sources & User Lookup
Data Store
Configure Custom Source Filters
Configure Custom Source Fields
☆ Summary

Attribute Source Summary

Attribute Sources & User Lookup

DATA STORE	
Attribute Source	aaquery
Attribute Source Id	aaquery
Type of Data Store	Custom
Data Store	idpQuery
CONFIGURE CUSTOM SOURCE FILTERS	
Subject	${SAML_SUBJECT}
CONFIGURE CUSTOM SOURCE FIELDS	
Field	fullname
Field	username
Field	staffleve l
Field	role
Field	division
Field	employer
Field	clearance

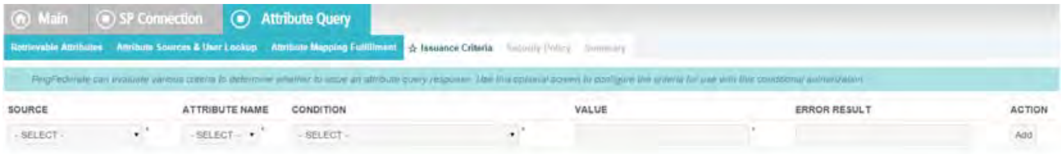
9. Click on **Attribute Mapping Fulfillment**.



Fulfill your Attribute Request with values from your Data Store lookup or with dynamic text values.

ATTRIBUTE CONTRACT	SOURCE	VALUE	ACTIONS
clearance	Text	#clearance = #this.get("ds.JIT.carLicense"), #queryclearance = #this.get("ds.aaquery.clearan	None available
division	Text	#division = #this.get("ds.JIT.physicalDeliveryOfficeName"), #querydivision = #this.get("ds.aaq	None available
employer	Text	#employer = #this.get("ds.JIT.member"), #queryemployer = #this.get("ds.aaquery.employer")	None available
fullname	Text	#fullname = #this.get("ds.JIT.cn"), #queryfullname = #this.get("ds.aaquery.fullname"), (#fullna	None available
role	Text	#role = #this.get("ds.JIT.title"), #queryrole = #this.get("ds.aaquery.role"), (#role == null || #role	None available
staffleve l	Text	#stafflevel = #this.get("ds.JIT.employeeType"), #querystafflevel= #this.get("ds.aaquery.staffle	None available
username	Text	#username= #this.get("ds.JIT.givenName"), #queryusername= #this.get("ds.aaquery.usernar	None available

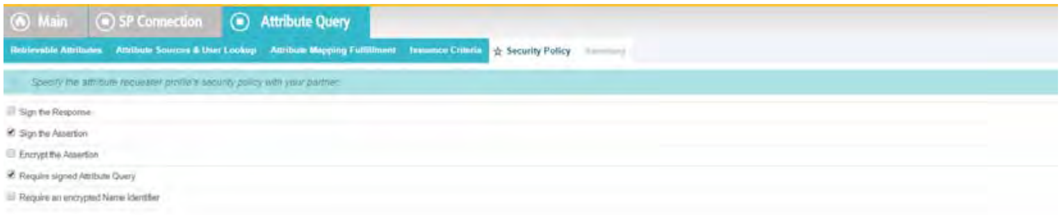
10. **Issuance Criteria**: PingFederate can evaluate various criteria to determine whether to issue an attribute query response. Use this optional screen to configure the criteria for use with this conditional authorization.



PingFederate can evaluate various criteria to determine whether to issue an attribute query response. Use this optional screen to configure the criteria for use with this conditional authorization.

SOURCE	ATTRIBUTE NAME	CONDITION	VALUE	ERROR RESULT	ACTION
- SELECT -	- SELECT -	- SELECT -			Add

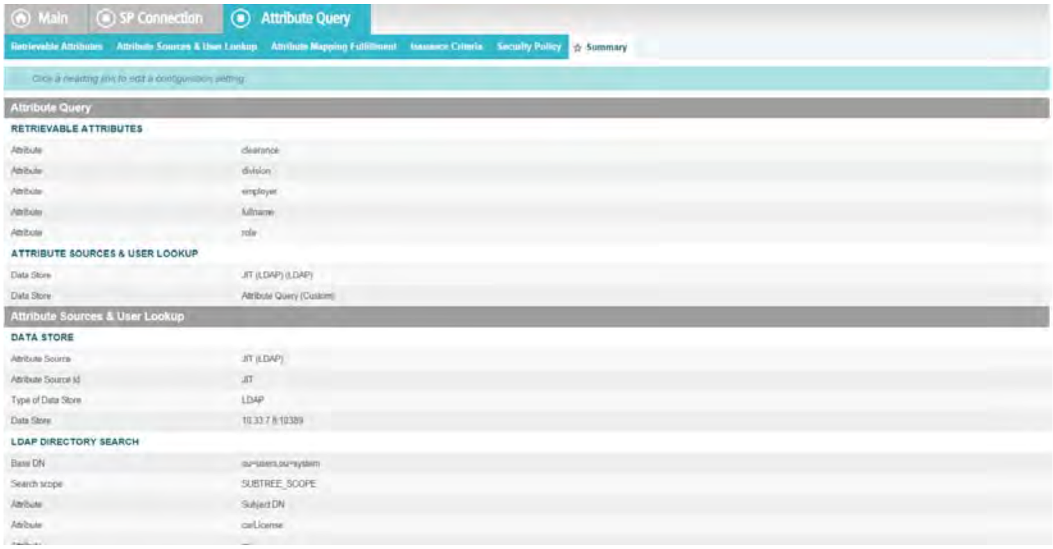
11. Click on **Security Policy**.



Specify the attribute requester profile's security policy with your partner.

☐ Sign the Response
☑ Sign the Assertion
☐ Encrypt the Assertion
☑ Require signed Attribute Query
☐ Require an encrypted Name Identifier

12. Check the **Summary**.



Click a heading link to edit a configuration setting.

Attribute Query

RETRIEVABLE ATTRIBUTES

Attribute	clearance
Attribute	division
Attribute	employer
Attribute	fullname
Attribute	role

ATTRIBUTE SOURCES & USER LOOKUP

Data Store	JIT (LDAP) (LDAP)
Data Store	Attribute Query (Custom)

Attribute Sources & User Lookup

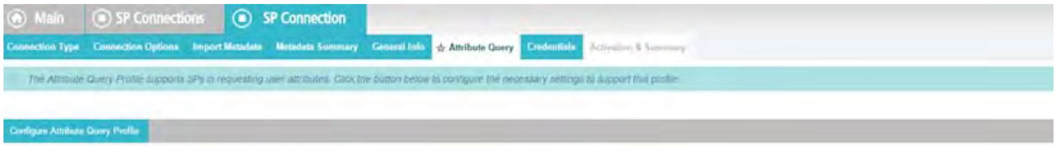
DATA STORE

Attribute Source	JIT (LDAP)
Attribute Source Id	JIT
Type of Data Store	LDAP
Data Store	10.33.7.8:10389

LDAP DIRECTORY SEARCH

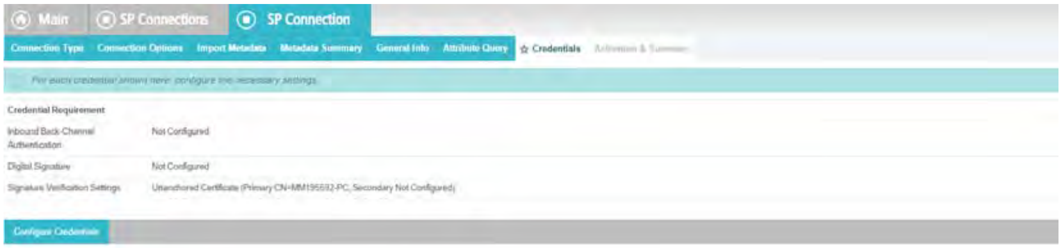
Base DN	ou=users,ou=system
Search scope	SUBTREE_SCOPE
Attribute	Subject DN
Attribute	carLicense

13. Provide **Credentials** for the back channel attribute request.



The Attribute Query Profile supports SPs in requesting user attributes. Click the button below to configure the necessary settings to support this profile.

14. Specify **Inbound Back-Channel Authentication** and **Digital Signature** on the message.



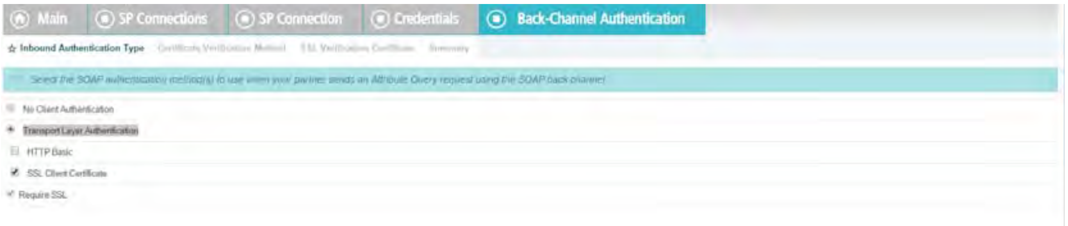
For each credential shown here, configure the necessary settings.

Credential Requirement

Inbound Back-Channel Authentication	Not Configured
Digital Signature	Not Configured
Signature Verification Settings	Unanchored Certificate (Primary CN=MM195592-PC, Secondary Not Configured)

10.8.2.1.3 Back Channel Authentication Configuration

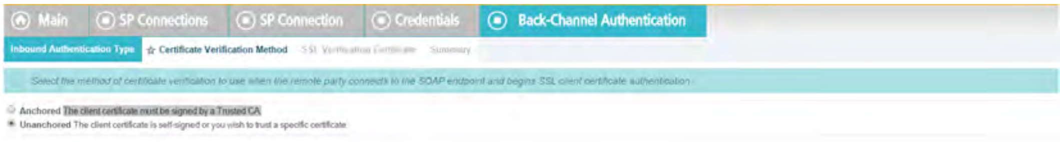
1. Use the default **Transport Layer Authentication** with **SSL Client Certificate**.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
☆ Inbound Authentication Type
Certificate Verification Method
SSL Verification Certificate
Summary

Select the SOAP authentication method(s) to use when your partner sends an Attribute Query request using the SOAP back channel.

○ No Client Authentication
● Transport Layer Authentication
□ HTTP Basic
☑ SSL Client Certificate
✓ Require SSL

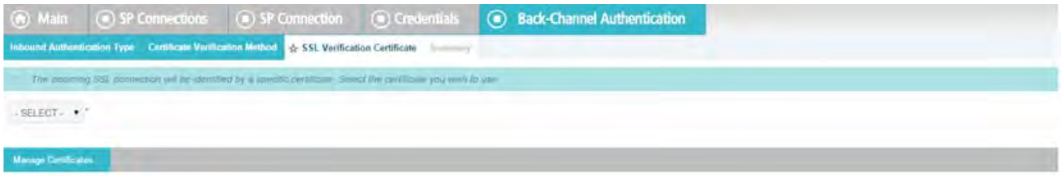
2. It is encouraged to use the **Anchored** verification method.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
Inbound Authentication Type
☆ Certificate Verification Method
SSL Verification Certificate
Summary

Select the method of certificate verification to use when the remote party connects to the SOAP endpoint and begins SSL client certificate authentication.

○ Anchored The client certificate must be signed by a Trusted CA
● Unanchored The client certificate is self-signed or you wish to trust a specific certificate

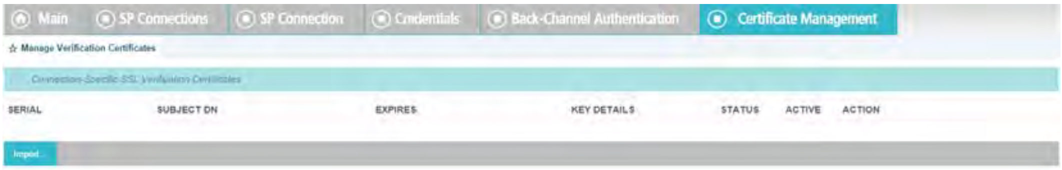
3. You will be prompted to select an **SSL Verification Certificate**. In our build, a certificate has not been previously imported. Click on **Manage Certificate**.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
Inbound Authentication Type
Certificate Verification Method
☆ SSL Verification Certificate
Summary
Manage Certificates

The incoming SSL connection will be identified by a specific certificate. Select the certificate you wish to use.

- SELECT - ▾ *

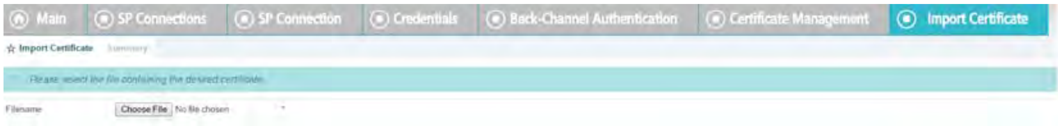
4. Click **Import**.



Connection-Specific SSL Verification Certificates

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTIVE	ACTION

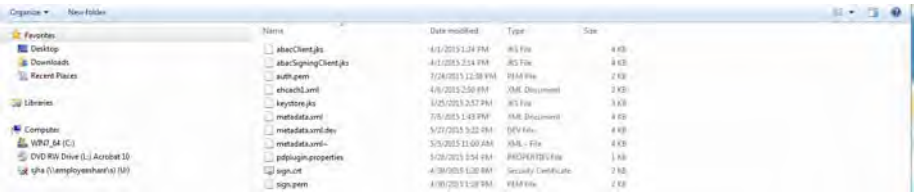
5. Click **Choose File**.



Please select the file containing the desired certificate.

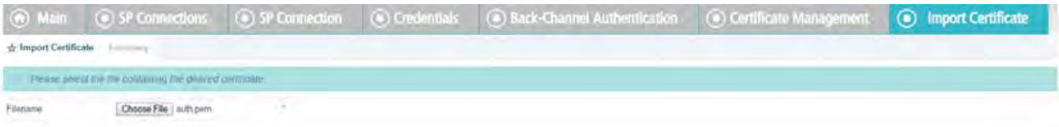
Filename No file chosen *

6. Select your certificate file from the Explorer window.



Name	Date modified	Type	Size
abacClient.jks	4/1/2015 1:24 PM	JKS File	4 KB
abacSigningClient.jks	4/1/2015 2:14 PM	JKS File	4 KB
auth.pem	7/24/2015 12:38 PM	PEM File	2 KB
ehcach1.xml	4/6/2015 2:50 PM	XML Document	2 KB
keystore.jks	3/25/2015 2:57 PM	JKS File	3 KB
metadata.xml	7/8/2015 1:43 PM	XML Document	4 KB
metadata.xml.dev	5/27/2015 5:22 PM	DEV File	4 KB
metadata.xml~	5/5/2015 11:00 AM	XML~ File	4 KB
pdplugin.properties	5/28/2015 3:54 PM	PROPERTIES File	1 KB
sign.crt	4/30/2015 1:20 PM	Security Certificate	2 KB
sign.pem	4/30/2015 11:18 PM	PEM File	2 KB

7. The file name will appear in the **Filename** field.

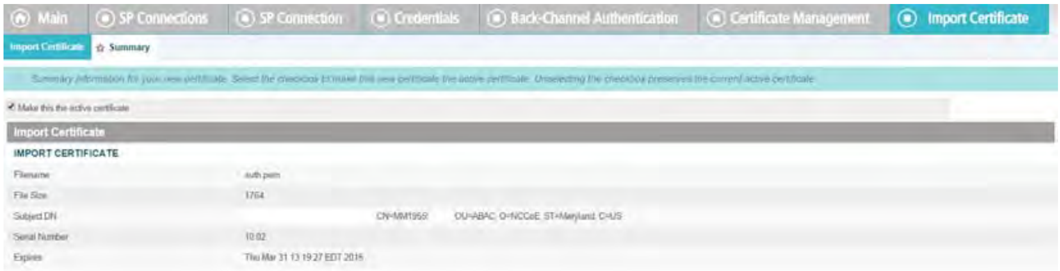


Please select the file containing the desired certificate.

Filename auth.pem *

8. Click **Next**. This will display details of parts of certificate.

9. Check **Make this the active certificate** and click **Done**.



Summary information for your new certificate. Select the checkbox to make this new certificate the active certificate. Unselecting the checkbox preserves the current active certificate.

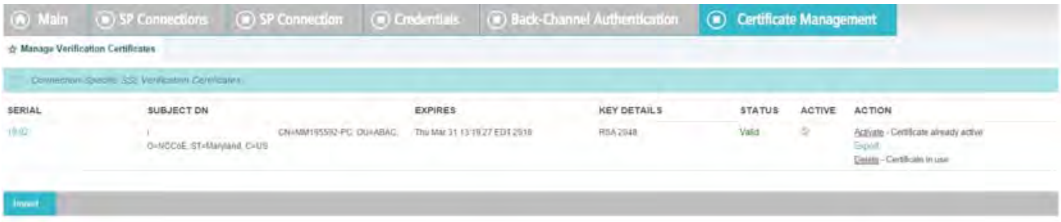
☑ Make this the active certificate

Import Certificate

IMPORT CERTIFICATE

Filename	auth.pem
File Size	1764
Subject DN	CN=MM1959 OU=ABAC, O=NCCoE, ST=Maryland, C=US
Serial Number	10:02
Expires	Thu Mar 31 13:19:27 EDT 2016

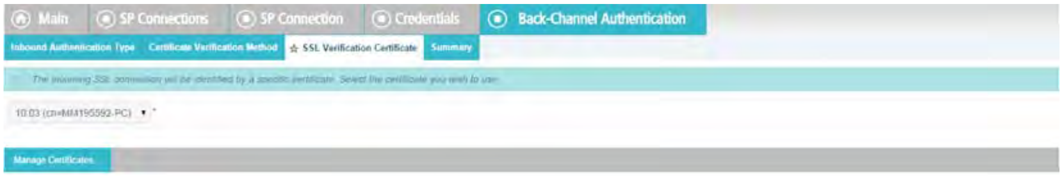
10. Verify the certificate.



Connection-Specific SSL Verification Certificates.

SERIAL	SUBJECT DN	EXPIRES	KEY DETAILS	STATUS	ACTIVE	ACTION
10:02	CN=MM195592-PC, OU=ABAC, O=NCCoE, ST=Maryland, C=US	Thu Mar 31 13:19:27 EDT 2016	RSA 2048	Valid	✓	Activate - Certificate already active Export Delete - Certificate in use

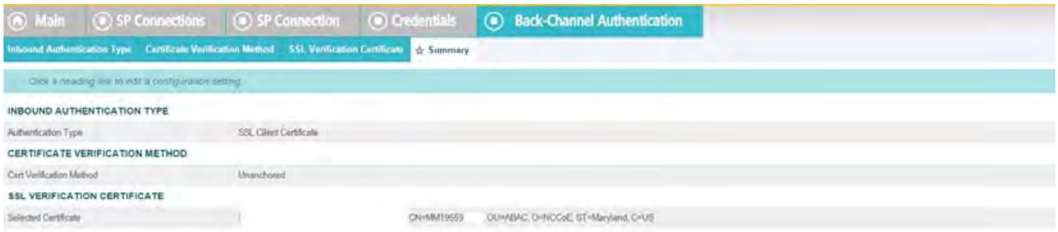
11. Under **Action**, select **Activate**.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
Inbound Authentication Type
Certificate Verification Method
☆ SSL Verification Certificate
Summary
Manage Certificates

The incoming SSL connection will be identified by a specific certificate. Select the certificate you wish to use.

10:03 (cn=MM195592-PC) ▾ *

12. View a **Summary** of the verification.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
Inbound Authentication Type
Certificate Verification Method
SSL Verification Certificate
☆ Summary

Click a heading link to edit a configuration setting.

INBOUND AUTHENTICATION TYPE

Authentication Type	SSL Client Certificate

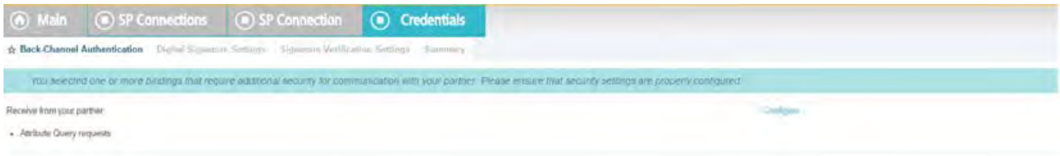
CERTIFICATE VERIFICATION METHOD

Cert Verification Method	Unanchored

SSL VERIFICATION CERTIFICATE

Selected Certificate	CN=MM19559 OU=ABAC, O=NCCoE, ST=Maryland, C=US

13. Return to the **Back Channel Authentication** tab.

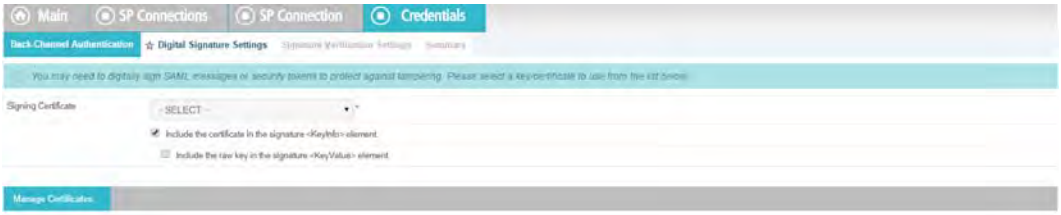

Main
SP Connections
SP Connection
Credentials
☆ Back-Channel Authentication
Digital Signature Settings
Signature Verification Settings
Summary

You selected one or more bindings that require additional security for communication with your partner. Please ensure that security settings are properly configured.

Receive from your partner

- Attribute Query requests

14. Select **Digital Signature Settings** for outgoing messages, then click **Next**.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
☆ Digital Signature Settings
Signature Verification Settings
Summary
Manage Certificates

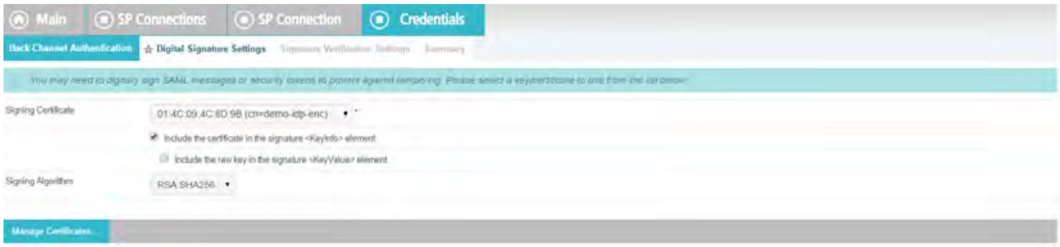
You may need to digitally sign SAML messages or security tokens to protect against tampering. Please select a key/certificate to use from the list below.

Signing Certificate: - SELECT - *

☑ Include the certificate in the signature <KeyInfo> element

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

15. Go to **Digital Signature Settings**. Click **Configure**.


Main
SP Connections
SP Connection
Credentials
Back Channel Authentication
☆ Digital Signature Settings
Signature Verification Settings
Summary
Manage Certificates

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.

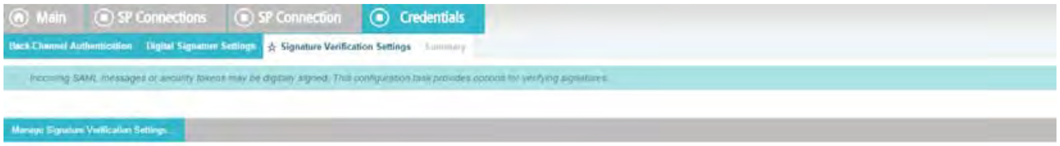
Signing Certificate: 01:4C:09:4C:8D:9B (cn=demo-idp-enc) *

☑ Include the certificate in the signature <KeyInfo> element

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

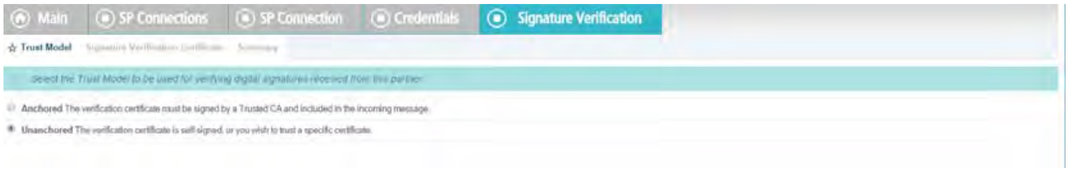
Signing Algorithm: RSA SHA256

16. Select **Digital Signature Settings** on incoming messages.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
Digital Signature Settings
☆ Signature Verification Settings
Summary
Manage Signature Verification Settings...

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

17. Click on **Manage Signature Verification Settings**.



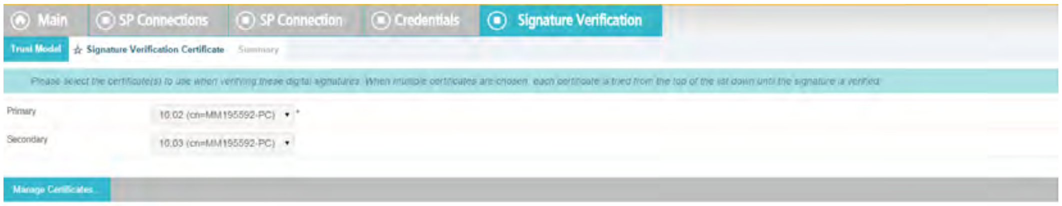
Select the Trust Model to be used for verifying digital signatures received from this partner.

○ **Anchored** The verification certificate must be signed by a Trusted CA and included in the incoming message

● **Unanchored** The verification certificate is self-signed, or you wish to trust a specific certificate.

18. Select the certificate(s) to use when verifying these digital signatures. When multiple certificates are chosen, each certificate is tried from the top of the list down until the signature is verified. It is assumed that signed certificates have already been imported. If

not, click on **Manage Certificate** and complete the steps detailed earlier for importing a certificate.

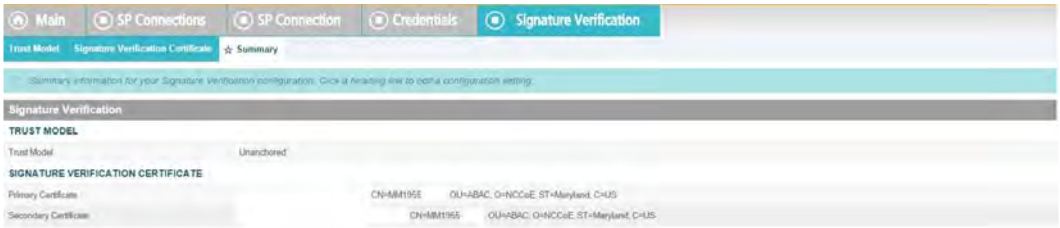


Please select the certificate(s) to use when verifying these digital signatures. When multiple certificates are chosen, each certificate is tried from the top of the list down until the signature is verified.

Primary 10.02 (cn=MM195592-PC) ▾ *

Secondary 10.03 (cn=MM195592-PC) ▾

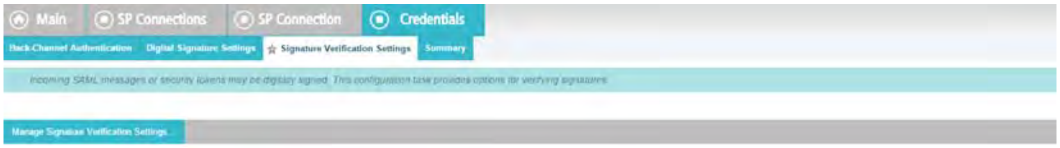
19. Verify the **Summary**.



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

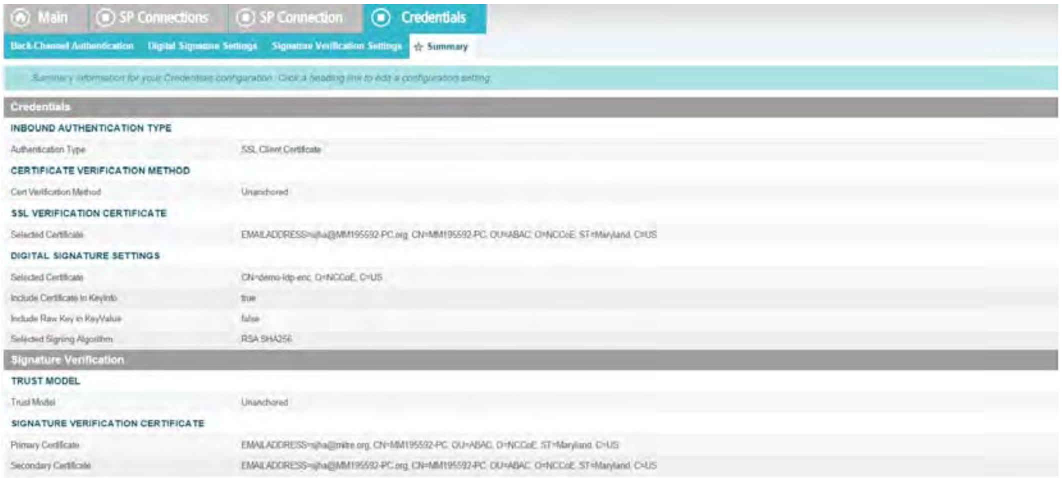
Signature Verification	
TRUST MODEL	
Trust Model	Unanchored
SIGNATURE VERIFICATION CERTIFICATE	
Primary Certificate	CN=MM1955 OU=ABAC, O=NCCoE, ST=Maryland, C=US
Secondary Certificate	CN=MM1955 OU=ABAC, O=NCCoE, ST=Maryland, C=US

20. This completes the signature verification credential settings.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
Digital Signature Settings
☆ Signature Verification Settings
Summary
Manage Signature Verification Settings...

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

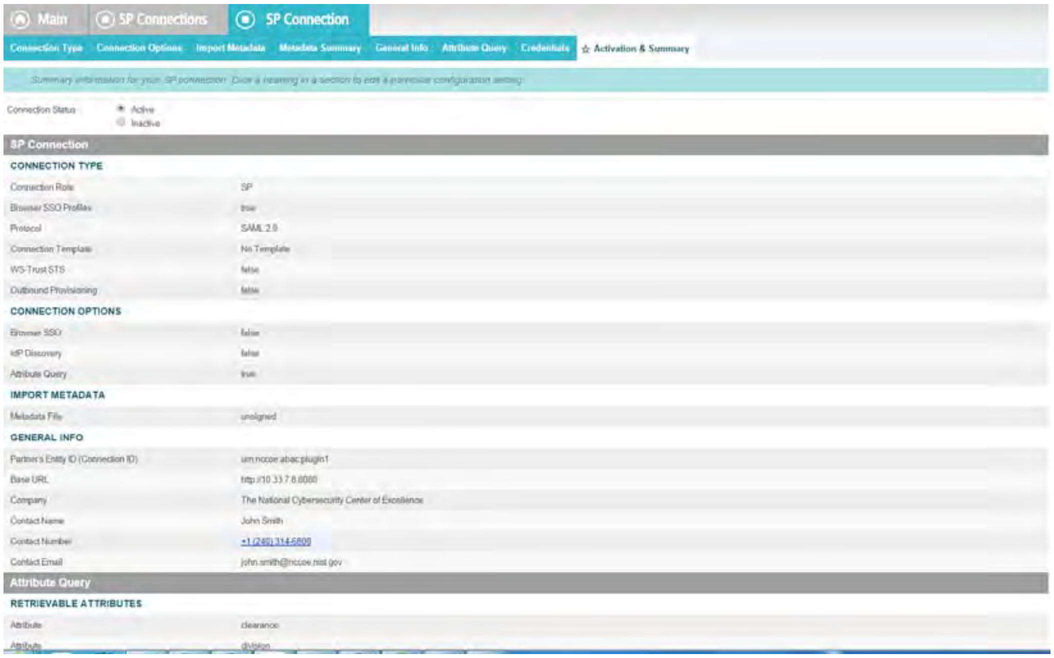
21. Verify the **Summary**.


Main
SP Connections
SP Connection
Credentials
Back-Channel Authentication
Digital Signature Settings
Signature Verification Settings
☆ Summary

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

Credentials	
INBOUND AUTHENTICATION TYPE	
Authentication Type	SSL Client Certificate
CERTIFICATE VERIFICATION METHOD	
Cert Verification Method	Unanchored
SSL VERIFICATION CERTIFICATE	
Selected Certificate	EMAILADDRESS=sjha@MM195592-PC.org, CN=MM195592-PC, OU=ABAC, O=NCCoE, ST=Maryland, C=US
DIGITAL SIGNATURE SETTINGS	
Selected Certificate	CN=demo-idp-enc, O=NCCoE, C=US
Include Certificate in KeyInfo	true
Include Raw Key in KeyValue	false
Selected Signing Algorithm	RSA SHA256
Signature Verification	
TRUST MODEL	
Trust Model	Unanchored
SIGNATURE VERIFICATION CERTIFICATE	
Primary Certificate	EMAILADDRESS=sjha@mitre.org, CN=MM195592-PC, OU=ABAC, O=NCCoE, ST=Maryland, C=US
Secondary Certificate	EMAILADDRESS=sjha@MM195592-PC.org, CN=MM195592-PC, OU=ABAC, O=NCCoE, ST=Maryland, C=US

22. **Activate** the connection and **Save**.



Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Connection Status ● Active ○ Inactive

SP Connection

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

CONNECTION OPTIONS	
Browser SSO	false
IdP Discovery	false
Attribute Query	true

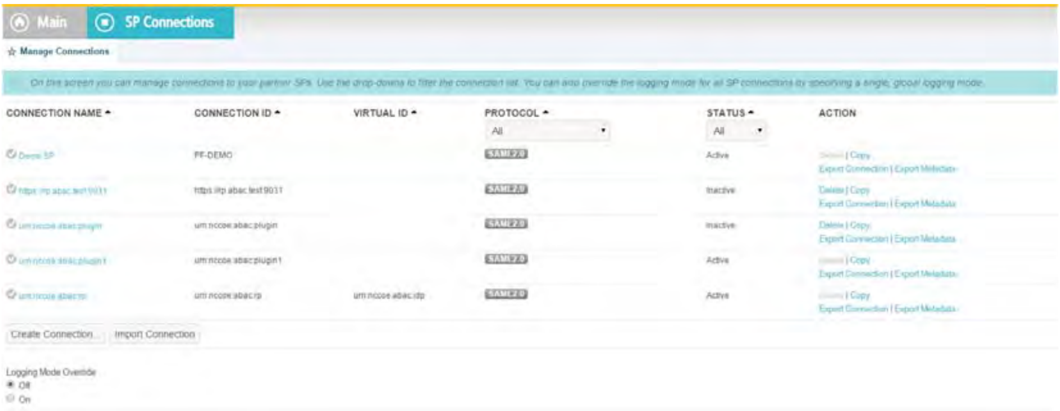
IMPORT METADATA	
Metadata File	unsigned

GENERAL INFO	
Partner's Entity ID (Connection ID)	urn:nccoe:abac:plugin1
Base URL	http://10.33.7.8:8080
Company	The National Cybersecurity Center of Excellence
Contact Name	John Smith
Contact Number	+1 (240) 314-6800
Contact Email	john.smith@nccoe.nist.gov

Attribute Query

RETRIEVABLE ATTRIBUTES	
Attribute	clearance
Attribute	division

23. **Save** again.



On this screen you can manage connections to your partner SPs. Use the drop-down 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 ▲	VIRTUAL ID ▲	PROTOCOL ▲ All	STATUS ▲ All	ACTION
Demo SP	PF-DEMO		SAML2.0	Active	Delete | Copy Export Connection | Export Metadata
https://rp.abac.test:9031	https://rp.abac.test:9031		SAML2.0	Inactive	Delete | Copy Export Connection | Export Metadata
urn:nccoe:abac:plugin	urn:nccoe:abac:plugin		SAML2.0	Inactive	Delete | Copy Export Connection | Export Metadata
urn:nccoe:abac:plugin1	urn:nccoe:abac:plugin1		SAML2.0	Active	Delete | Copy Export Connection | Export Metadata
urn:nccoe:abac:rp	urn:nccoe:abac:rp	urn:nccoe:abac:idp	SAML2.0	Active	Delete | Copy Export Connection | Export Metadata

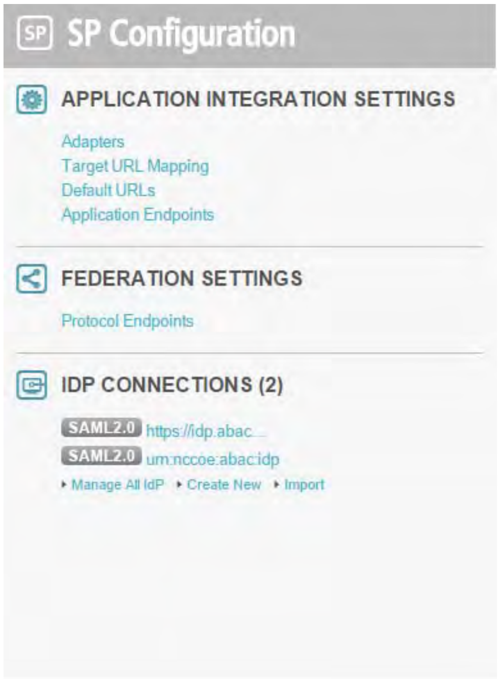
Create Connection... Import Connection

Logging Mode Override
● Off
○ On

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 right hand side of the administrative console, click **Manage All IdP** under **IdP Connections**.



SP Configuration

APPLICATION INTEGRATION SETTINGS

Adapters
Target URL Mapping
Default URLs
Application Endpoints

FEDERATION SETTINGS

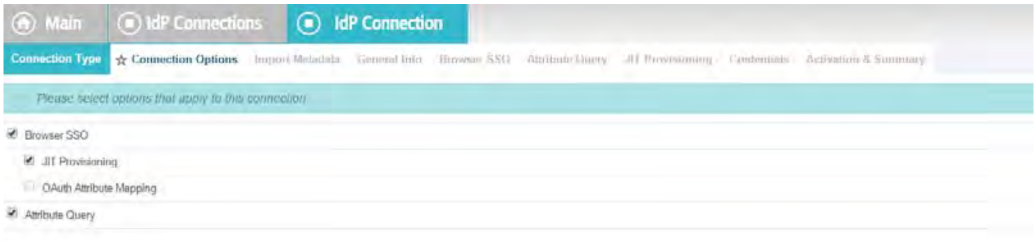
Protocol Endpoints

IDP CONNECTIONS (2)

SAML2.0 https://idp.abac...
SAML2.0 urn:nccoe:abac:idp

‣ Manage All IdP ‣ Create New ‣ Import

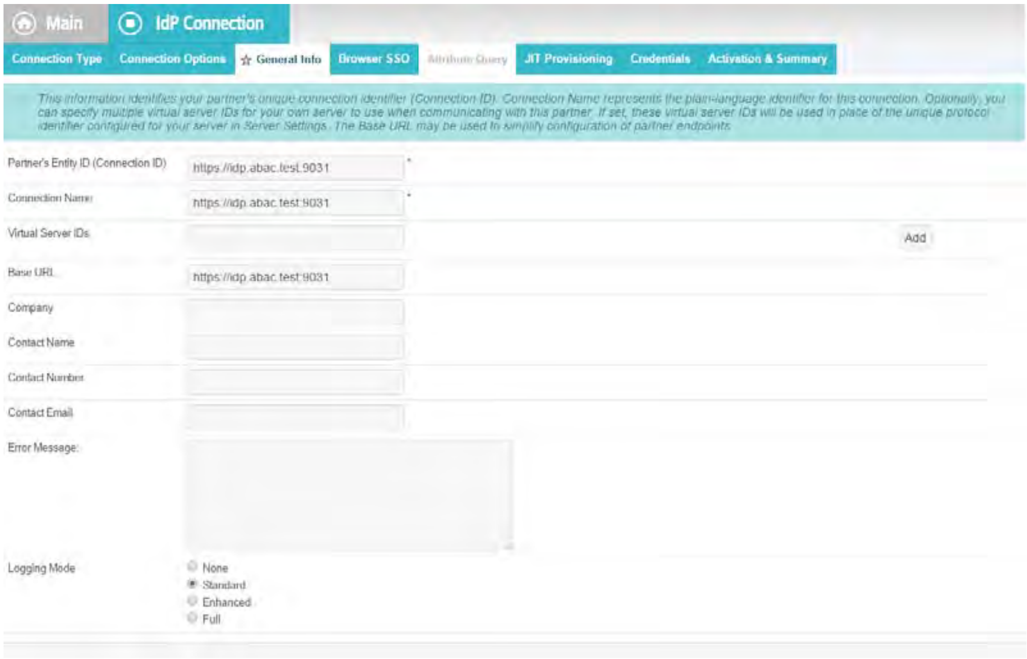
2. Open the connection that was created in chapter 6. Click on **Connection Option**. It my default to **Browser SSO**. Additionally, select **Attribute Query** and **JIT Provisioning**.



Please select options that apply to this connection

☑ Browser SSO
☑ JIT Provisioning
□ OAuth Attribute Mapping
☑ Attribute Query

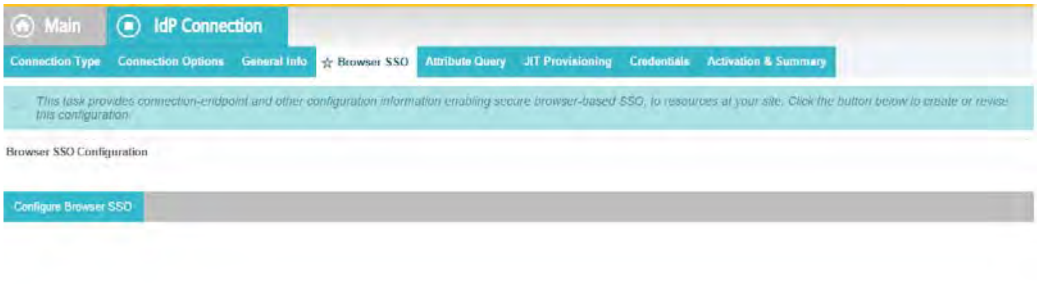
3. Click **Next**. Verify that the information in the **General Info** tab is correct.



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

Partner's Entity ID (Connection ID)	https://idp.abac.test:9031 *
Connection Name	https://idp.abac.test:9031 *
Virtual Server IDs	
Base URL	https://idp.abac.test:9031
Company	
Contact Name	
Contact Number	
Contact Email	
Error Message:	
Logging Mode	○ None ● Standard ○ Enhanced ○ Full

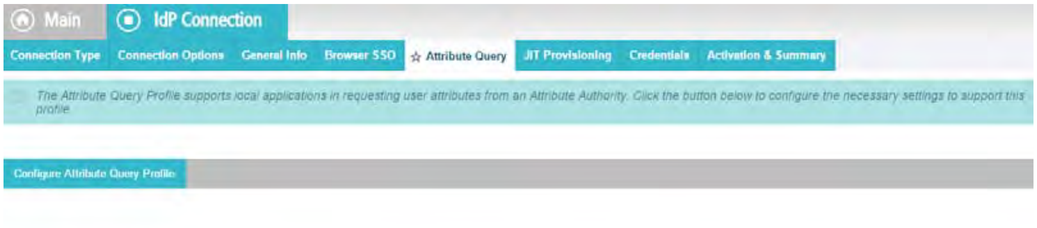
4. Click **Next**.



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.

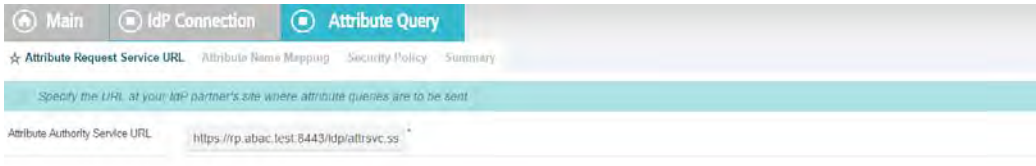
Browser SSO Configuration

5. Click on **Configure Attribute Query Profile**.



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.

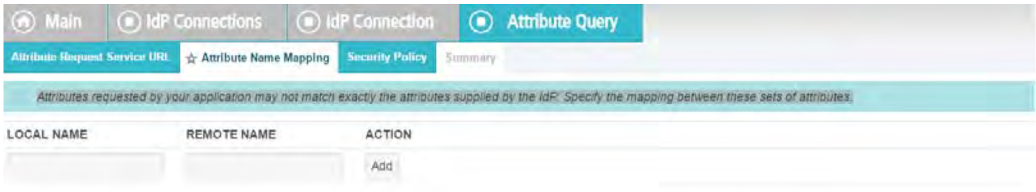
6. Specify an **Attribute Authority Service URL**.



Specify the URL at your IdP partner's site where attribute queries are to be sent

Attribute Authority Service URL: https://rp.abac.test:8443/idp/attrsvc.ss *

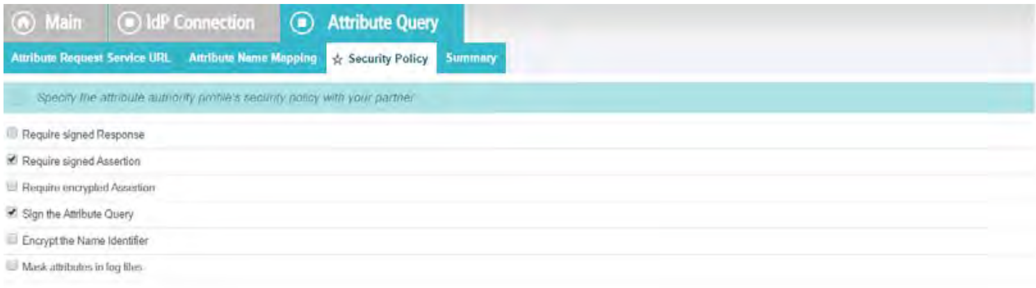
7. Attributes requested by your application may not match exactly the attributes supplied by the IdP. Specify the mapping between these sets of attributes.



Attributes requested by your application may not match exactly the attributes supplied by the IdP. Specify the mapping between these sets of attributes.

LOCAL NAME	REMOTE NAME	ACTION
		Add

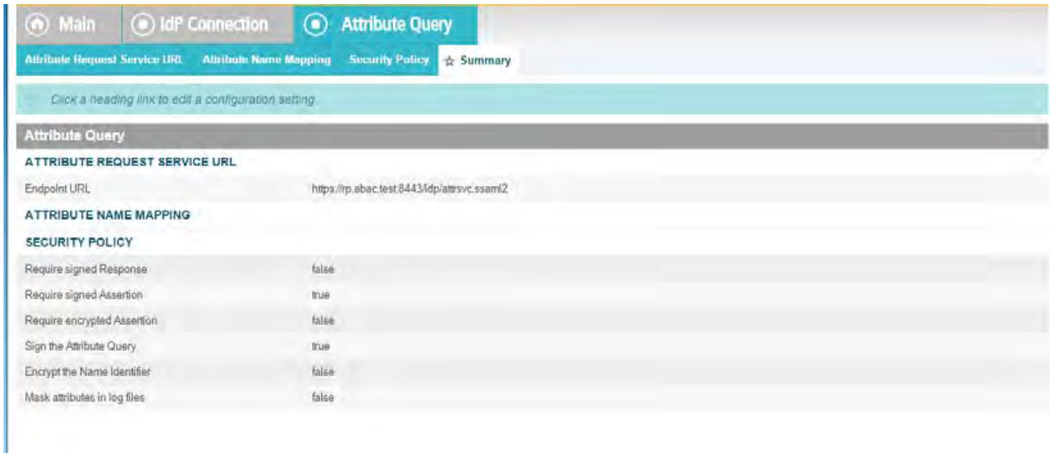
8. Select **Sign the Attribute Query**.



Specify the attribute authority profile's security policy with your partner

☐ Require signed Response
☑ Require signed Assertion
☐ Require encrypted Assertion
☑ Sign the Attribute Query
☐ Encrypt the Name Identifier
☐ Mask attributes in log files

9. Verify that the **Summary** is correct, then click **Done**.



Click a heading link to edit a configuration setting

Attribute Query

ATTRIBUTE REQUEST SERVICE URL

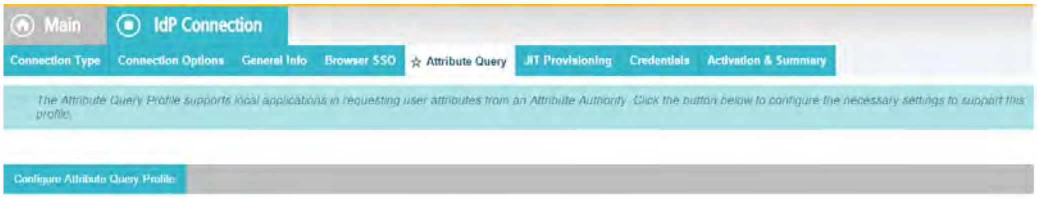
Endpoint URL	https://rp.abac.test:8443/idp/attrsvc.ssaml2

ATTRIBUTE NAME MAPPING

SECURITY POLICY

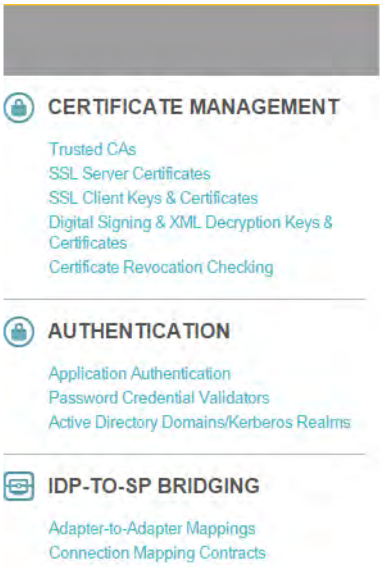
Require signed Response	false
Require signed Assertion	true
Require encrypted Assertion	false
Sign the Attribute Query	true
Encrypt the Name Identifier	false
Mask attributes in log files	false

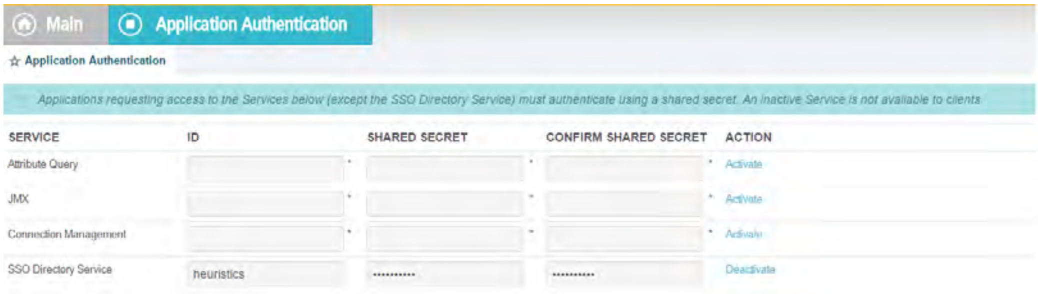
10. When the following screen appears, click **Next**.



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.

11. JIT provisioning details have been provided by PingFederate here.
12. **Save** the configuration.
13. Select **Application Authentication**.


CERTIFICATE MANAGEMENT
Trusted CAs
SSL Server Certificates
SSL Client Keys & Certificates
Digital Signing & XML Decryption Keys & Certificates
Certificate Revocation Checking
AUTHENTICATION
Application Authentication
Password Credential Validators
Active Directory Domains/Kerberos Realms
IDP-TO-SP BRIDGING
Adapter-to-Adapter Mappings
Connection Mapping Contracts



Applications requesting access to the Services below (except the SSO Directory Service) must authenticate using a shared secret. An inactive Service is not available to clients.

SERVICE	ID	SHARED SECRET	CONFIRM SHARED SECRET	ACTION
Attribute Query	*	*	*	Activate
JMX	*	*	*	Activate
Connection Management	*	*	*	Activate
SSO Directory Service	heuristics	....	....	Deactivate

14. Enter **appid** in the **ID** field, and use the shared secret that you input during custom data store configuration, then save the configuration.

15. Select **Browser SSO** and **Attribute Query**.

10.9 ApacheDS Schema Extension

At a high level LDAP Schema is the collection of attribute type definitions, object class definitions, and other information which a server uses to determine how to match a filter or attribute value assertion (in a compare operation) against the attributes of an entry, and whether to permit add and modify operations. For a more formal definition, look into section 4.1 of RFC 4512.

ApacheDS comes with a comprehensive set of predefined, standardized schema elements. Specification of many of these elements can be found in RFC 4519. Generally, these predefined schema satisfy most of the needs of a project. However, you may sometimes be required to define additional attributes or object classes that are not included in the server provided schema.

Each attribute and object class has an associated unique Object Identifier. Generally, An Object Identifier is a tree of nodes where each node is simply a sequence of digits. The rules roughly state that once an entity is assigned a node in the Object Identifier (OID) tree, it has sole discretion to further delegate sub-trees off of that node. Some examples of OIDs include: 1.3.6.1 - the Internet OID, 1.3.6.1.4.1 - IANA-assigned company OIDs. It is formally defined using the ITU-T's ASN.1 standard, X.690.

The IANA OID registry contains a list of registered entities that use OIDs to reference internal structures. In this chapter, we have used OIDs that are not registered anywhere. For this reason, we are using the subtree 2.25, as per recommendation by ITU. UUID is generated by the program found here.

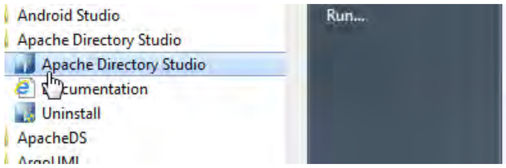
In the following section, we will demonstrate how to create an attribute. Similar procedures can be used to create many attributes and object classes.

10.9.1 Pre-Requisites

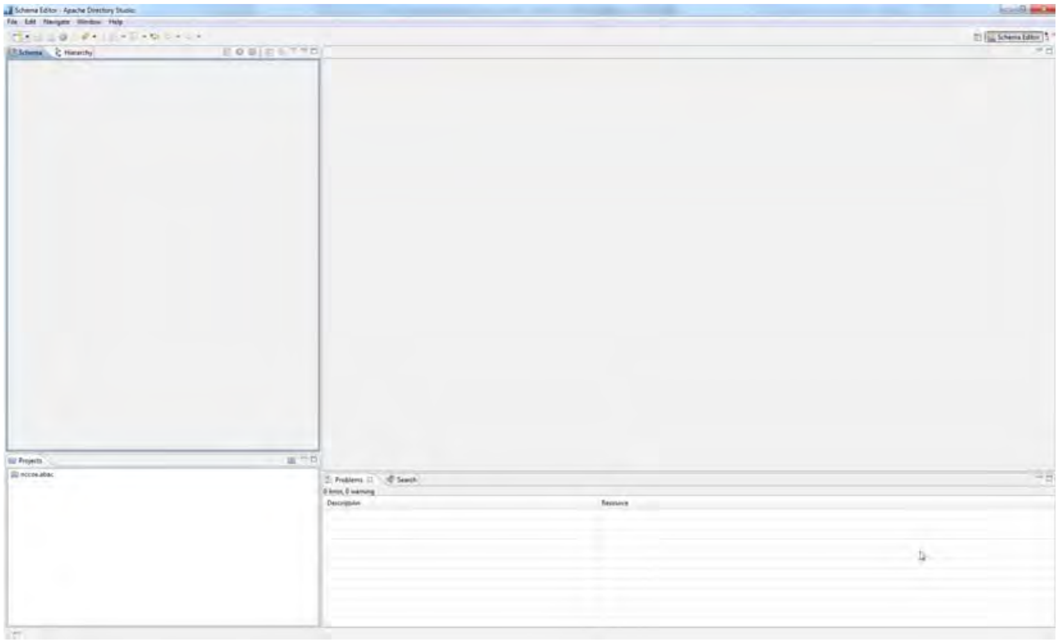
For Schema extension, this project used ApacheDS studio. ApacheDS installation and configuration is detailed in section 10.6 of this guide.

10.9.2 Procedure

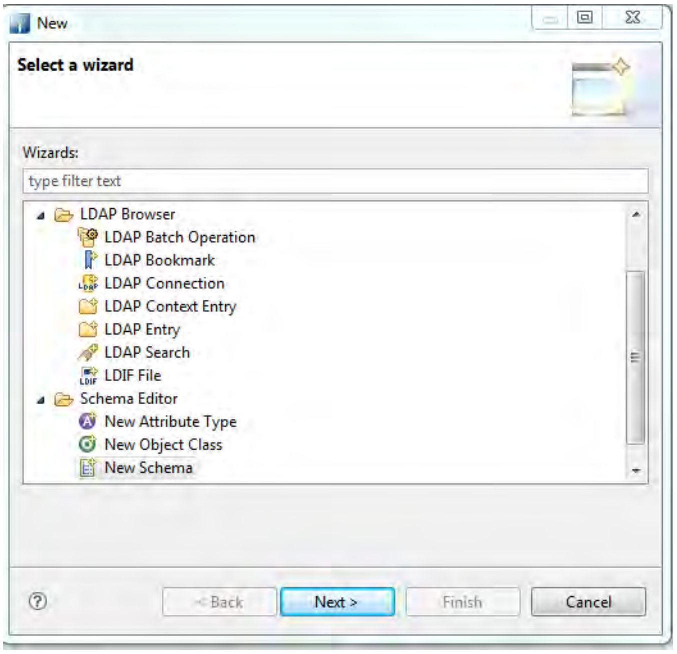
1. Start ApacheDS Studio from the Start menu.



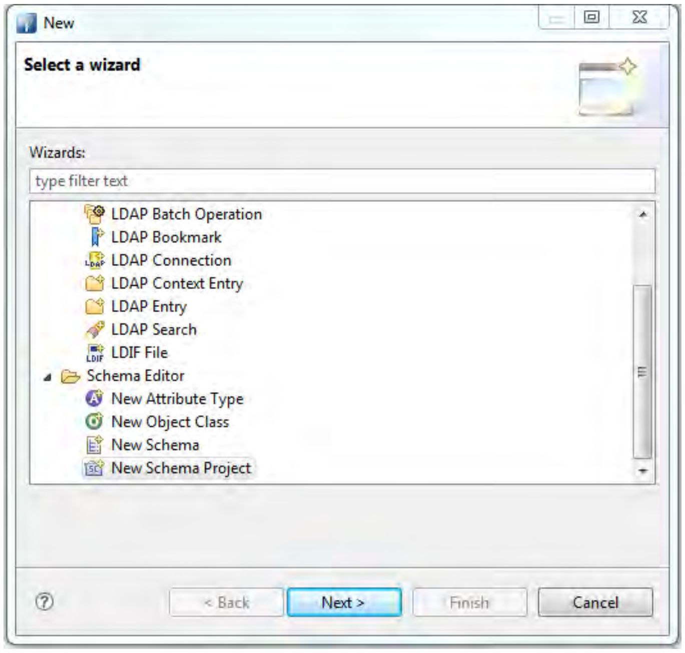
2. The following screen will appear:


Schema Editor - Apache Directory Studio
File Edit Navigate Window Help
Schema
Hierarchy
Schema Editor
Projects
Problems
Search
Description
Resource

3. Select **File -> New**.



4. Select the **New Schema Project** wizard.

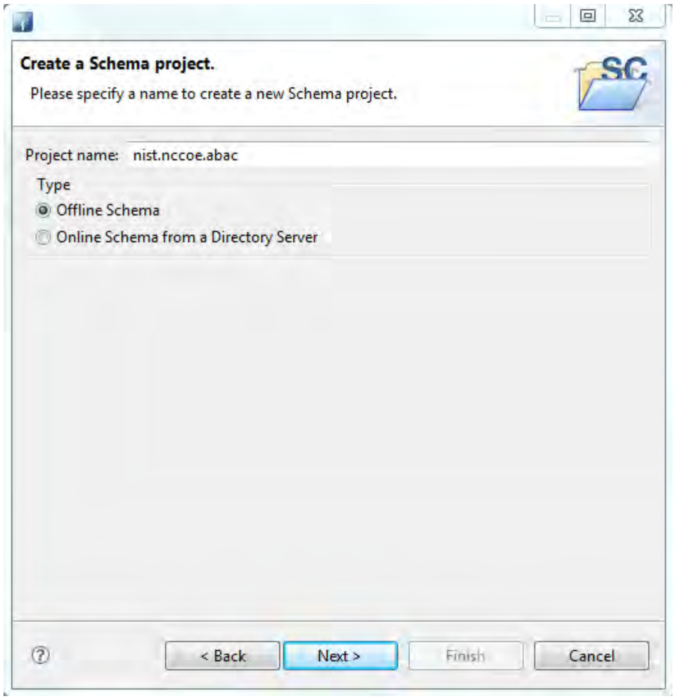


New

Select a wizard

Wizards:

5. Specify a **Project name**, i.e., **nist.nccoe.abac** in our build.



Create a Schema project.

Please specify a name to create a new Schema project.

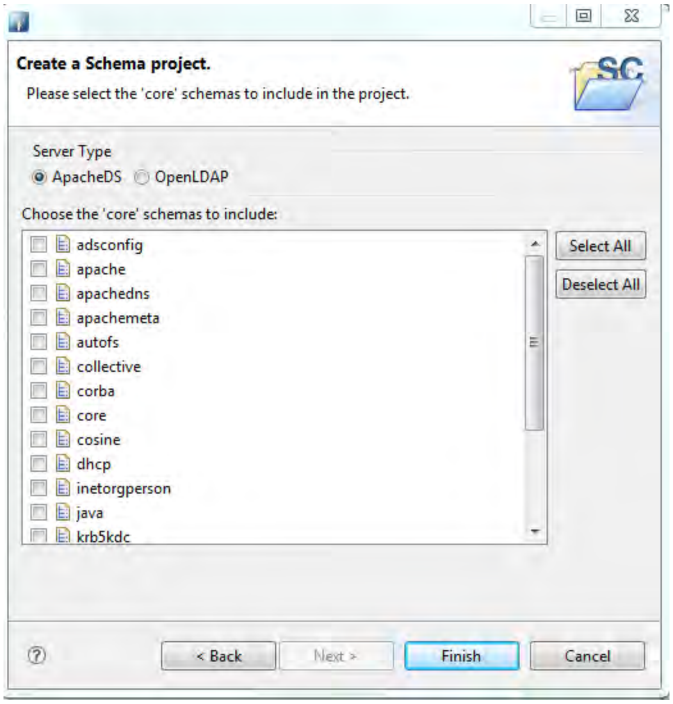
Project name: nist.nccoe.abac

Type

● Offline Schema

○ Online Schema from a Directory Server

6. Select **Offline Schema**, then click **Next**. On the next screen, **Choose the 'core' schemas to include**.



Create a Schema project.

Please select the 'core' schemas to include in the project.

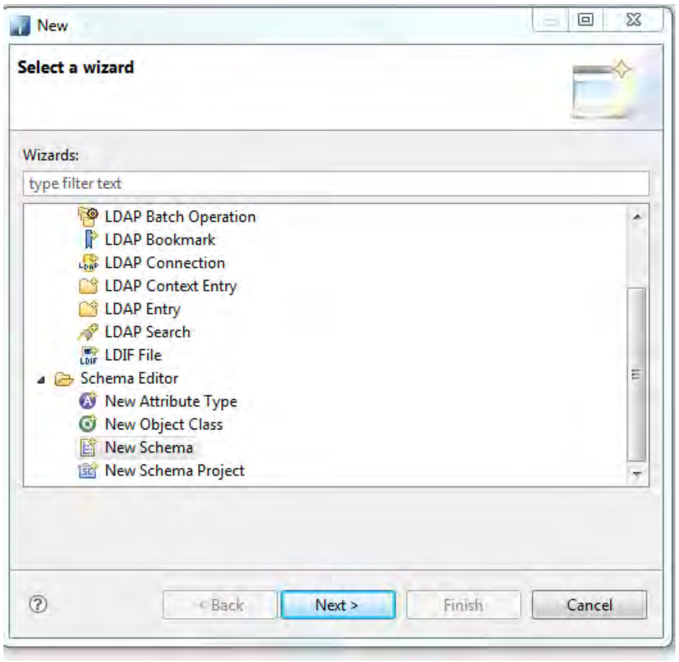
Server Type

● ApacheDS ○ OpenLDAP

Choose the 'core' schemas to include:

- □ adsconfig
- □ apache
- □ apachedns
- □ apachemeta
- □ autofs
- □ collective
- □ corba
- □ core
- □ cosine
- □ dhcp
- □ inetorgperson
- □ java
- □ krb5kdc

7. Click **File -> New** and select **New Schema**.



New

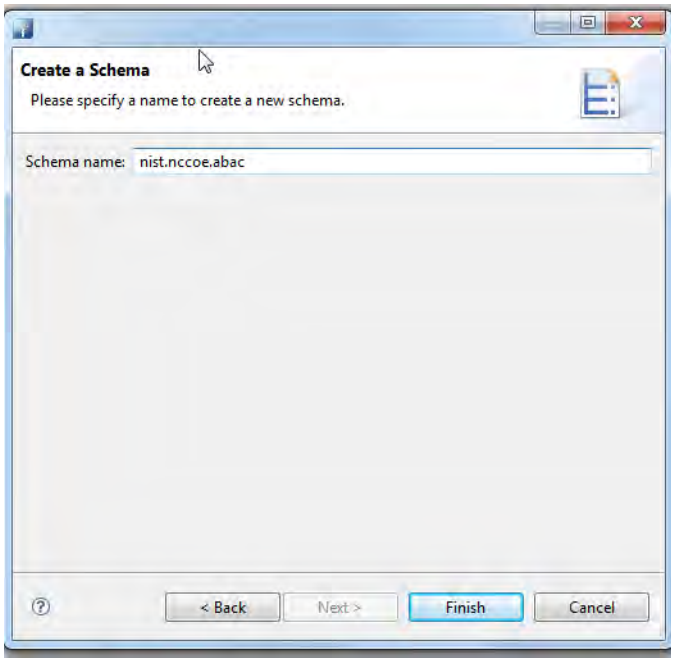
Select a wizard

Wizards:

type filter text

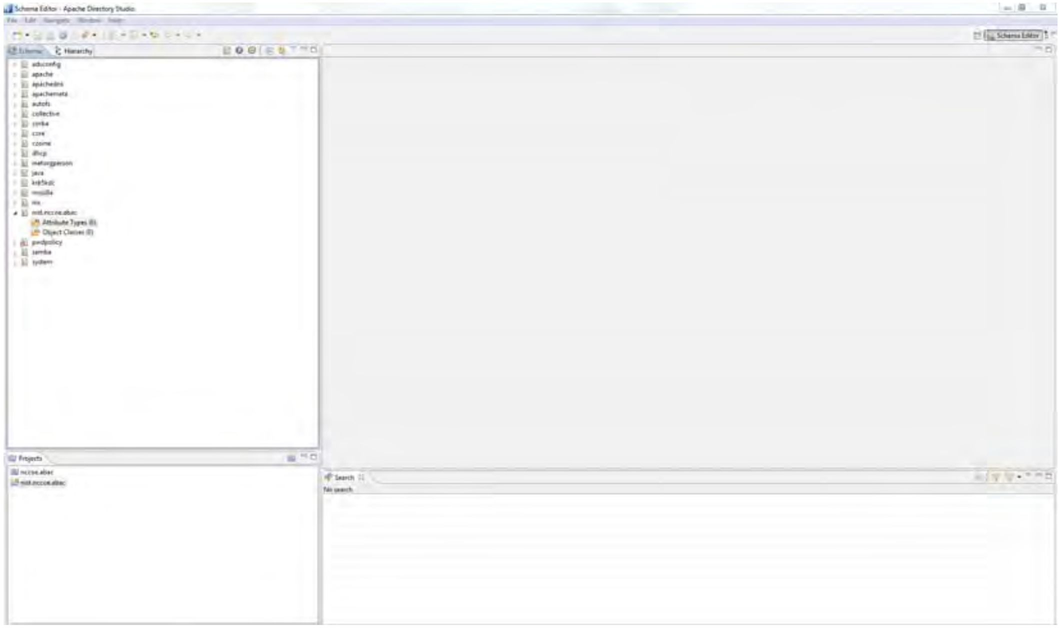
- LDAP Batch Operation
- LDAP Bookmark
- LDAP Connection
- LDAP Context Entry
- LDAP Entry
- LDAP Search
- LDIF File
- Schema Editor
  - New Attribute Type
  - New Object Class
  - New Schema
  - New Schema Project

8. Specify a **Schema name**, i.e., **nist.nccoe.abac** in our build.

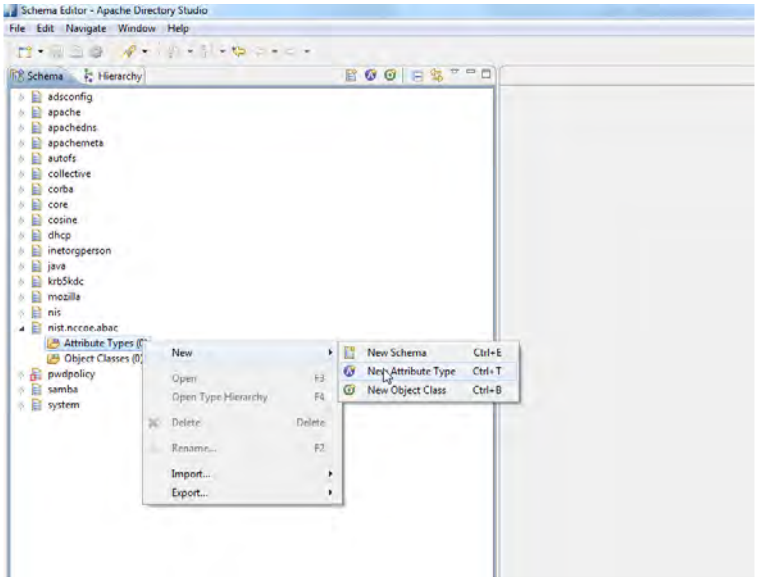


Schema name: nist.nccoe.abac

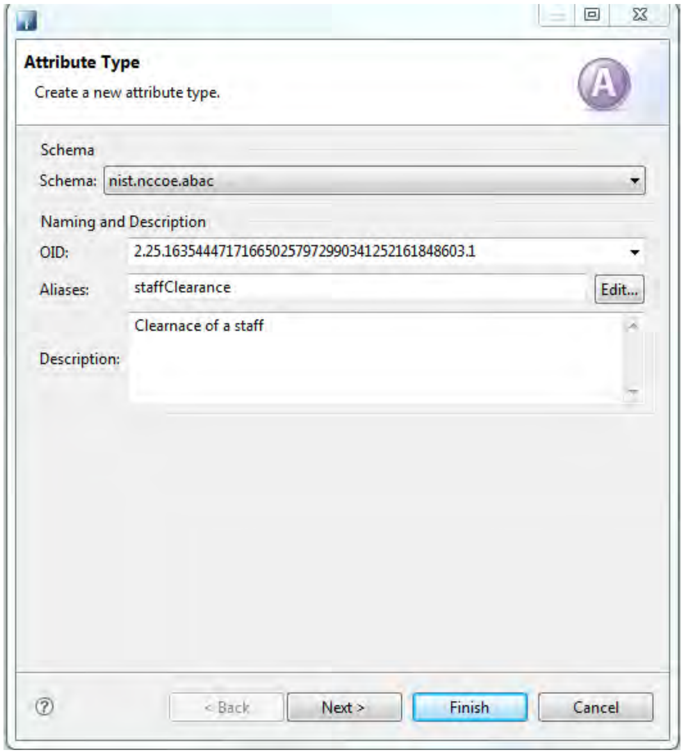
9. The following screen will appear:



10. Select **Attribute Types -> New -> New Attribute Type**.



11. In the new window, choose the **OID** from the previous instructions.



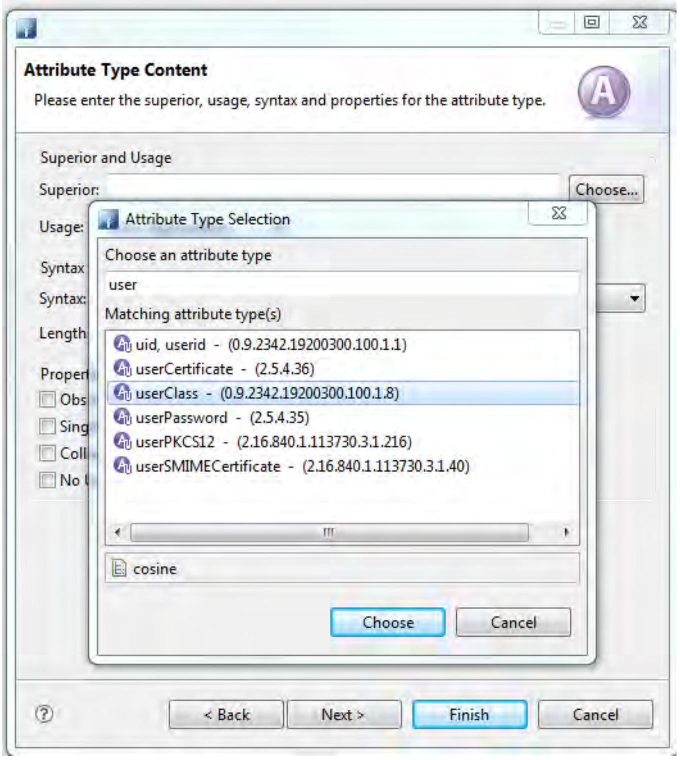
Schema: nist.nccoe.abac

OID: 2.25.163544471716650257972990341252161848603.1

Aliases: staffClearance

Description: Clearnace of a staff

12. Click **Next** to choose the superior type of this attribute.



Attribute Type Content

Please enter the superior, usage, syntax and properties for the attribute type.

Superior and Usage

Superior:

Attribute Type Selection

Choose an attribute type

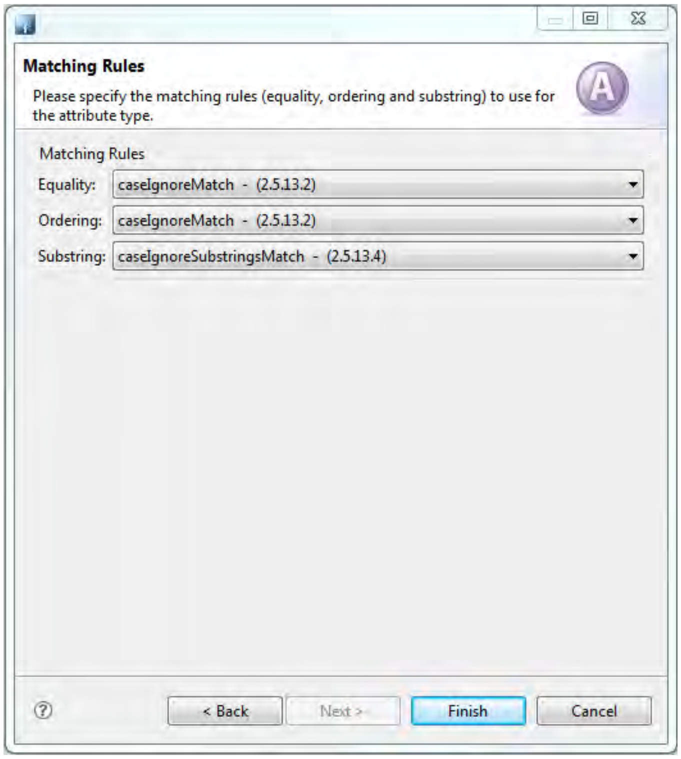
user

Matching attribute type(s)

- uid, userid - (0.9.2342.19200300.100.1.1)
- userCertificate - (2.5.4.36)
- userClass - (0.9.2342.19200300.100.1.8)
- userPassword - (2.5.4.35)
- userPKCS12 - (2.16.840.1.113730.3.1.216)
- userSMIMECertificate - (2.16.840.1.113730.3.1.40)

cosine

13. Specify **Matching Rules**. Since it is a string, case insensitivity is chosen in our build.



Matching Rules

Please specify the matching rules (equality, ordering and substring) to use for the attribute type.

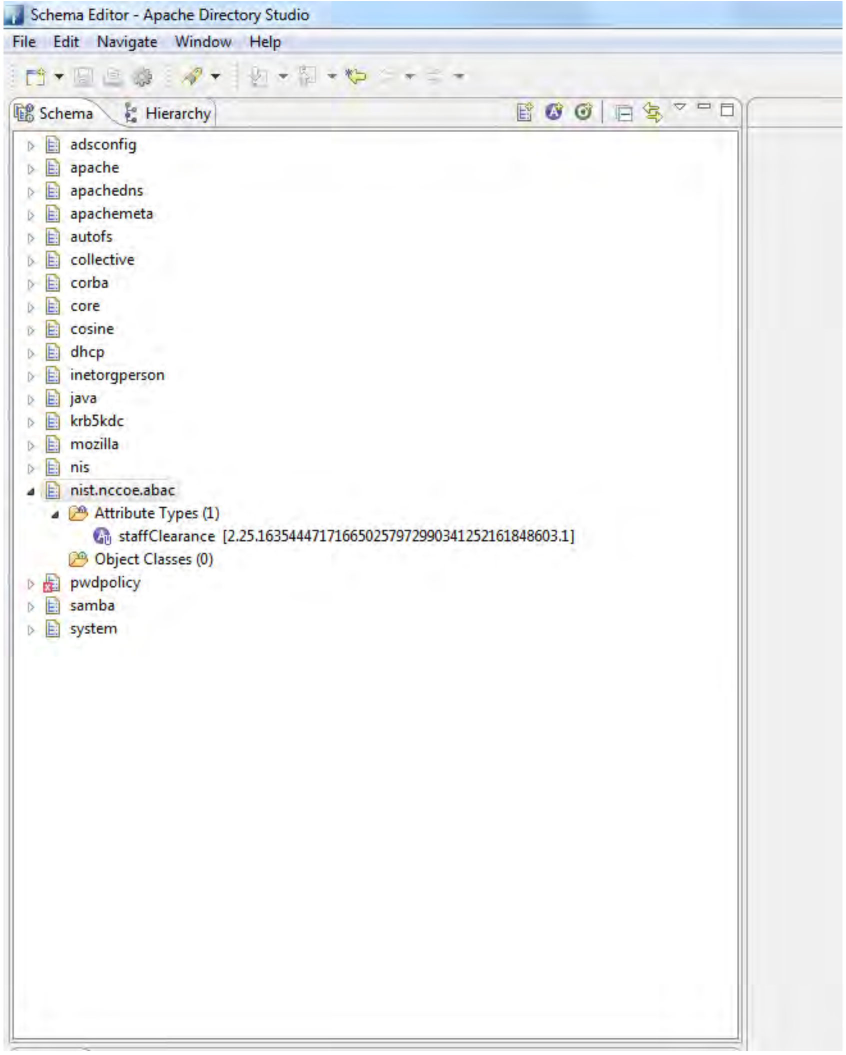
Matching Rules

Equality: caseIgnoreMatch - (2.5.13.2)

Ordering: caseIgnoreMatch - (2.5.13.2)

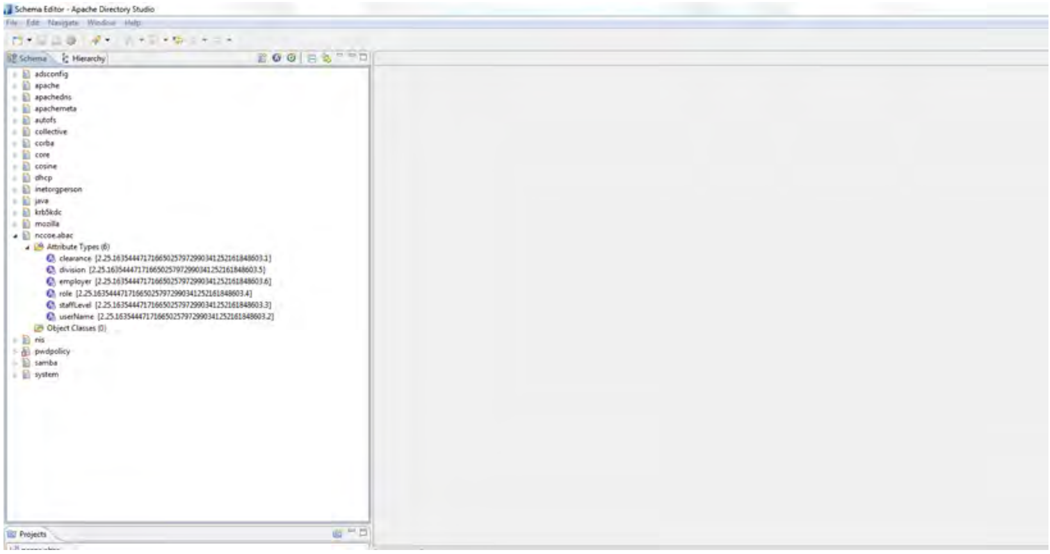
Substring: caseIgnoreSubstringsMatch - (2.5.13.4)

14. The following screen will appear:

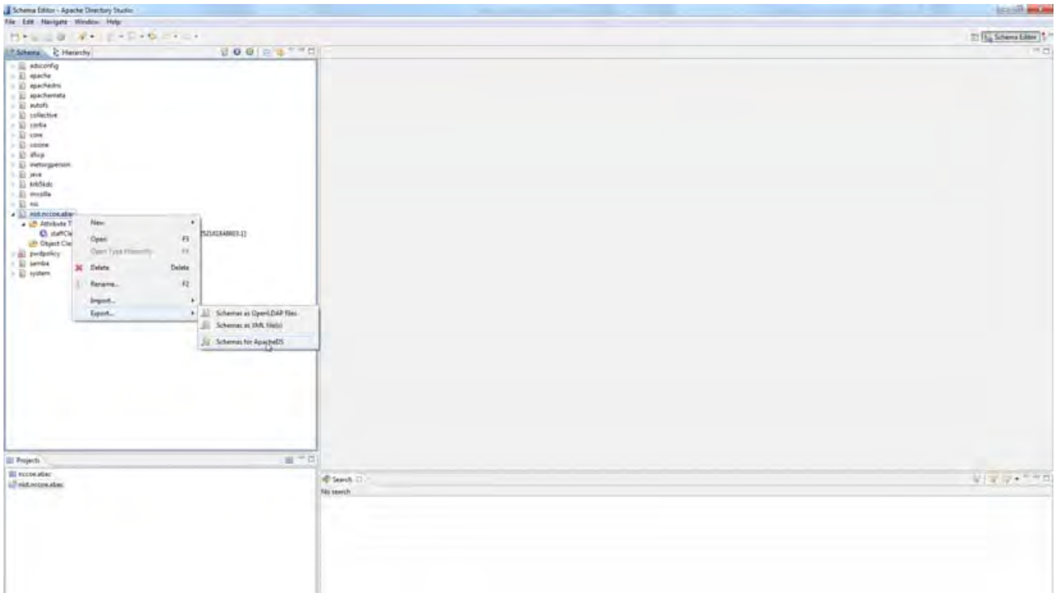


```
adsconfig
apache
apachedns
apachemeta
autofs
collective
corba
core
cosine
dhcp
inetorgperson
java
krb5kdc
mozilla
nis
nist.nccoe.abac
  Attribute Types (1)
    staffClearance [2.25.163544471716650257972990341252161848603.1]
  Object Classes (0)
pwdpolicy
samba
system
```

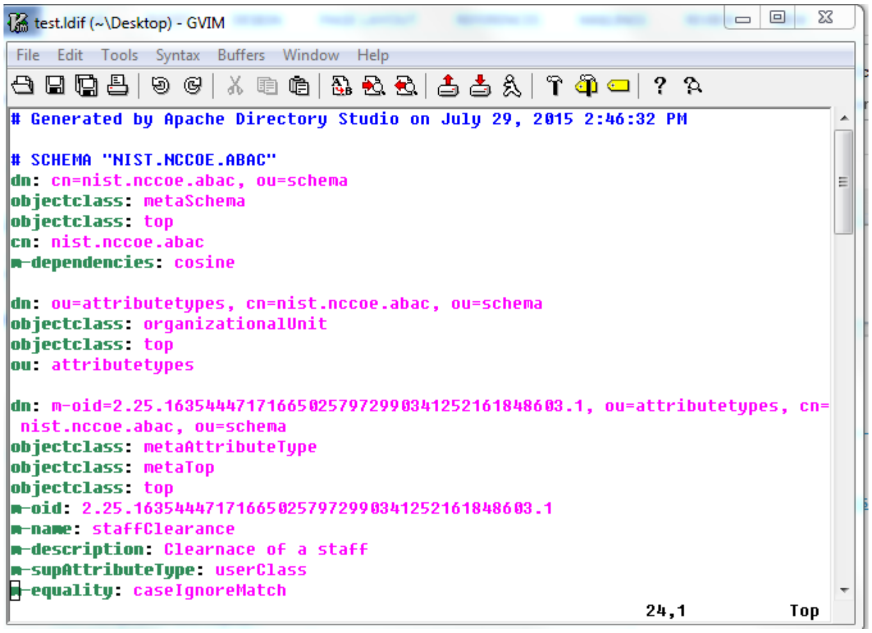
15. You can create other attributes by following process described above.


Schema Editor - Apache Directory Studio
File Edit Navigate Window Help
Schema
Hierarchy
adsconfig
apache
apachedns
apachemeta
autofs
collective
corba
core
cosine
dhcp
inetorgperson
java
krb5kdc
mozilla
nccoe.abac
Attribute Types (6)
clearance [2.25.163544471716650257972990341252161848603.1]
division [2.25.163544471716650257972990341252161848603.5]
employer [2.25.163544471716650257972990341252161848603.6]
role [2.25.163544471716650257972990341252161848603.4]
staffLevel [2.25.163544471716650257972990341252161848603.3]
userName [2.25.163544471716650257972990341252161848603.2]
Object Classes (0)
nis
pwdpolicy
samba
system
Projects

16. Export the schema by selecting **Export -> Schemas for ApacheDS**. It will create an LDIF file.

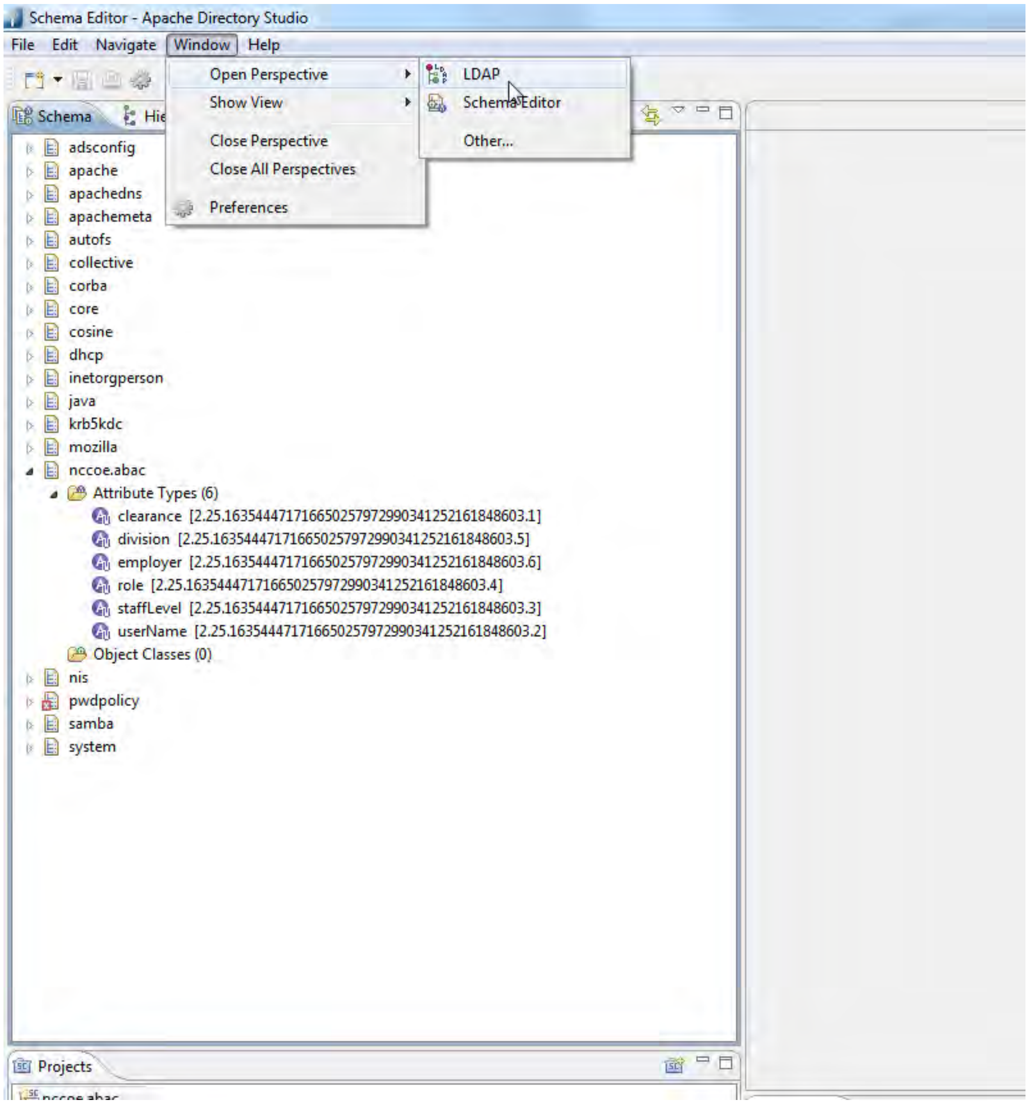


17. LDIF files are specified by their own RFC. In a text editor, it displays as following:

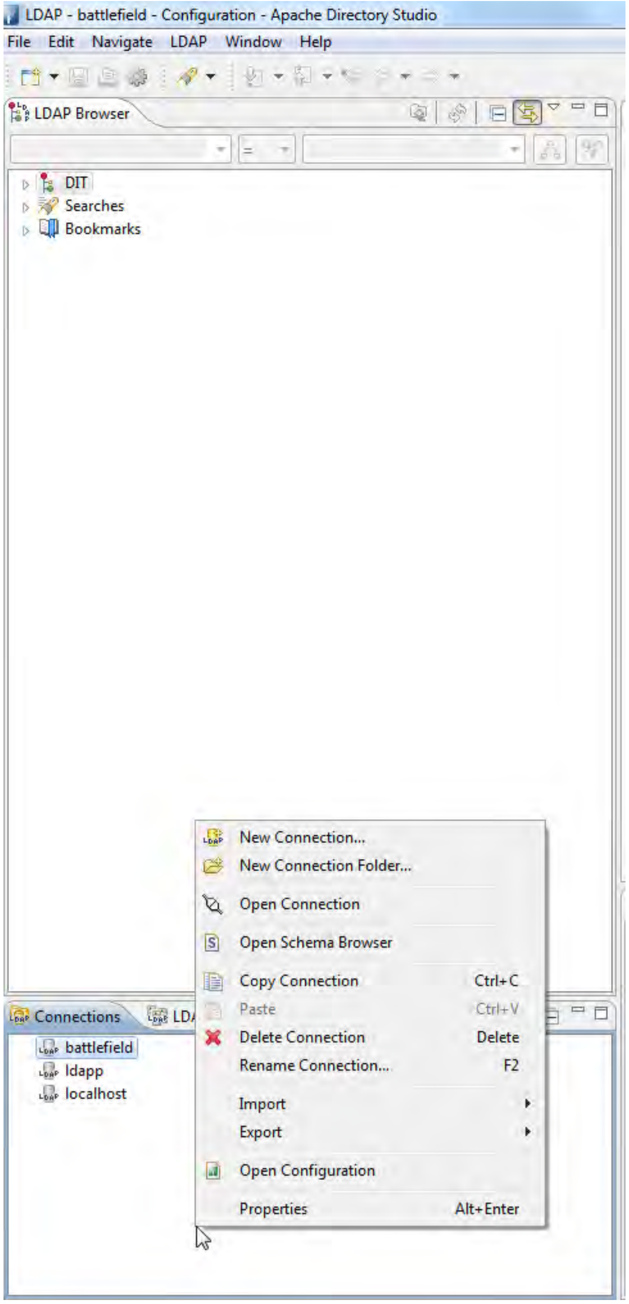

test.ldif (~\Desktop) - GVIM
File Edit Tools Syntax Buffers Window Help

```
# Generated by Apache Directory Studio on July 29, 2015 2:46:32 PM

# SCHEMA "NIST.NCCOE.ABAC"
dn: cn=nist.nccoe.abac, ou=schema
objectclass: metaSchema
objectclass: top
cn: nist.nccoe.abac
m-dependencies: cosine

dn: ou=attributetypes, cn=nist.nccoe.abac, ou=schema
objectclass: organizationalUnit
objectclass: top
ou: attributetypes

dn: m-oid=2.25.163544471716650257972990341252161848603.1, ou=attributetypes, cn=
 nist.nccoe.abac, ou=schema
objectclass: metaAttributeType
objectclass: metaTop
objectclass: top
m-oid: 2.25.163544471716650257972990341252161848603.1
m-name: staffClearance
m-description: Clearnace of a staff
m-supAttributeType: userClass
m-equality: caseIgnoreMatch
                                                                24,1          Top
```

18. To import the file, first select **Window -> Open Perspective -> LDAP**.

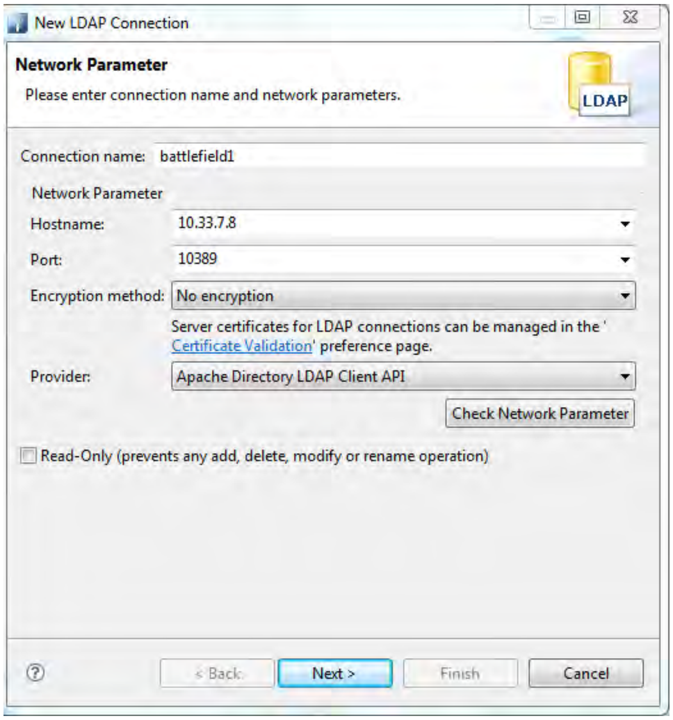

Schema Editor - Apache Directory Studio
File
Edit
Navigate
Window
Help
Open Perspective
Show View
Close Perspective
Close All Perspectives
Preferences
LDAP
Schema Editor
Other...
Schema
Hie
adsconfig
apache
apachedns
apachemeta
autofs
collective
corba
core
cosine
dhcp
inetorgperson
java
krb5kdc
mozilla
nccoe.abac
Attribute Types (6)
clearance [2.25.163544471716650257972990341252161848603.1]
division [2.25.163544471716650257972990341252161848603.5]
employer [2.25.163544471716650257972990341252161848603.6]
role [2.25.163544471716650257972990341252161848603.4]
staffLevel [2.25.163544471716650257972990341252161848603.3]
userName [2.25.163544471716650257972990341252161848603.2]
Object Classes (0)
nis
pwdpolicy
samba
system
Projects
nccoe.abac

1220 19. Click on the left bottom corner of the window and select **New Connection**.



1221

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

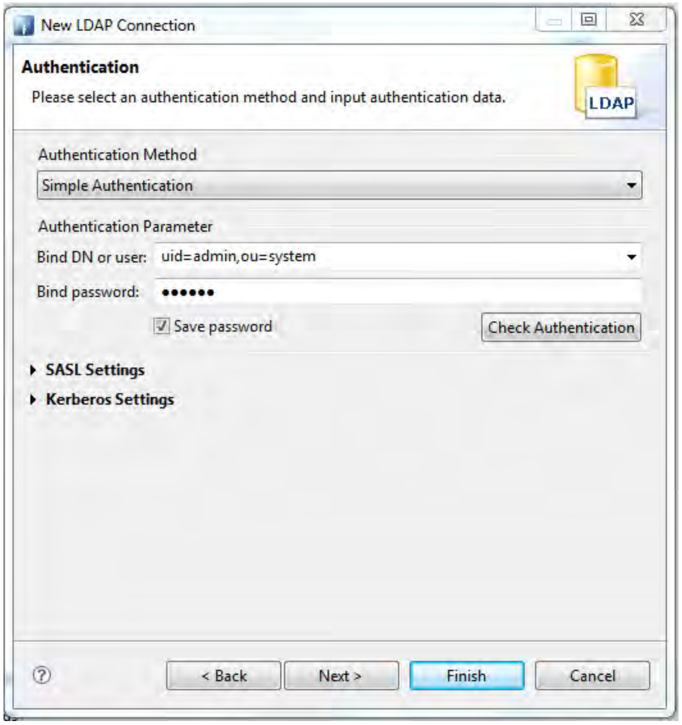
Encryption method: No encryption

Server certificates for LDAP connections can be managed in the 'Certificate Validation' preference page.

Provider: Apache Directory LDAP Client API

□ Read-Only (prevents any add, delete, modify or rename operation)

21. Provide credentials and click **Finish**.



New LDAP Connection

Authentication

Please select an authentication method and input authentication data.

Authentication Method

Simple Authentication

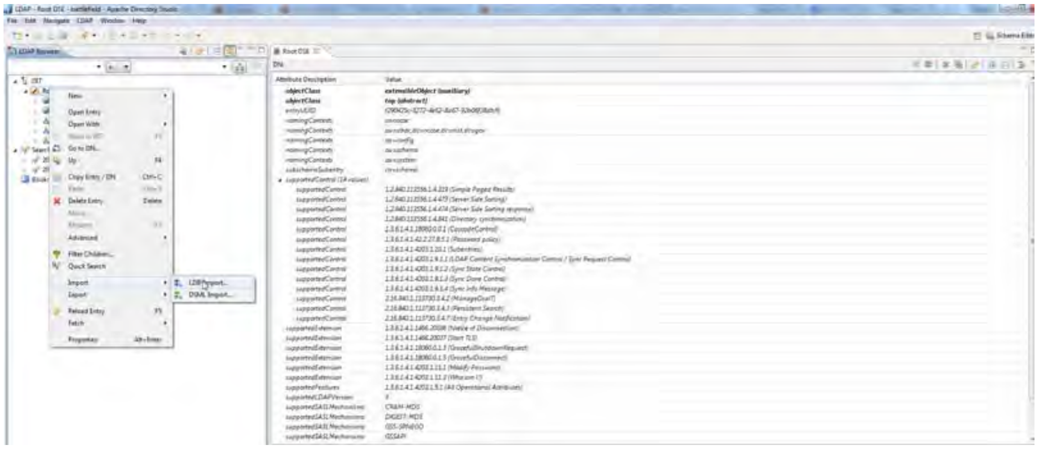
Authentication Parameter

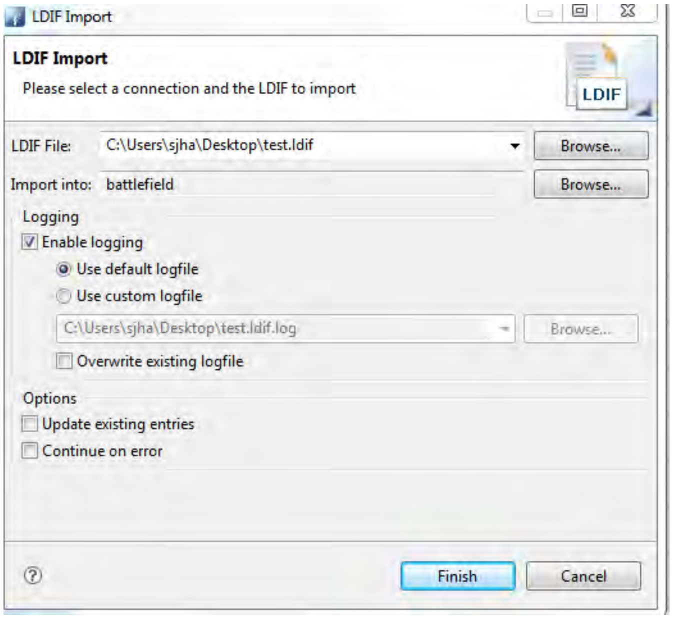
Bind DN or user: uid=admin,ou=system

Bind password: ••••••

☑ Save password

22. Open **Schema Editor Browser** and import the LDIF file created in the previous step.





LDIF Import

Please select a connection and the LDIF to import

LDIF File: C:\Users\sjha\Desktop\test.ldif [Browse...]

Import into: battlefield [Browse...]

Logging

☑ Enable logging

● Use default logfile

○ Use custom logfile

C:\Users\sjha\Desktop\test.ldif.log [Browse...]

□ Overwrite existing logfile

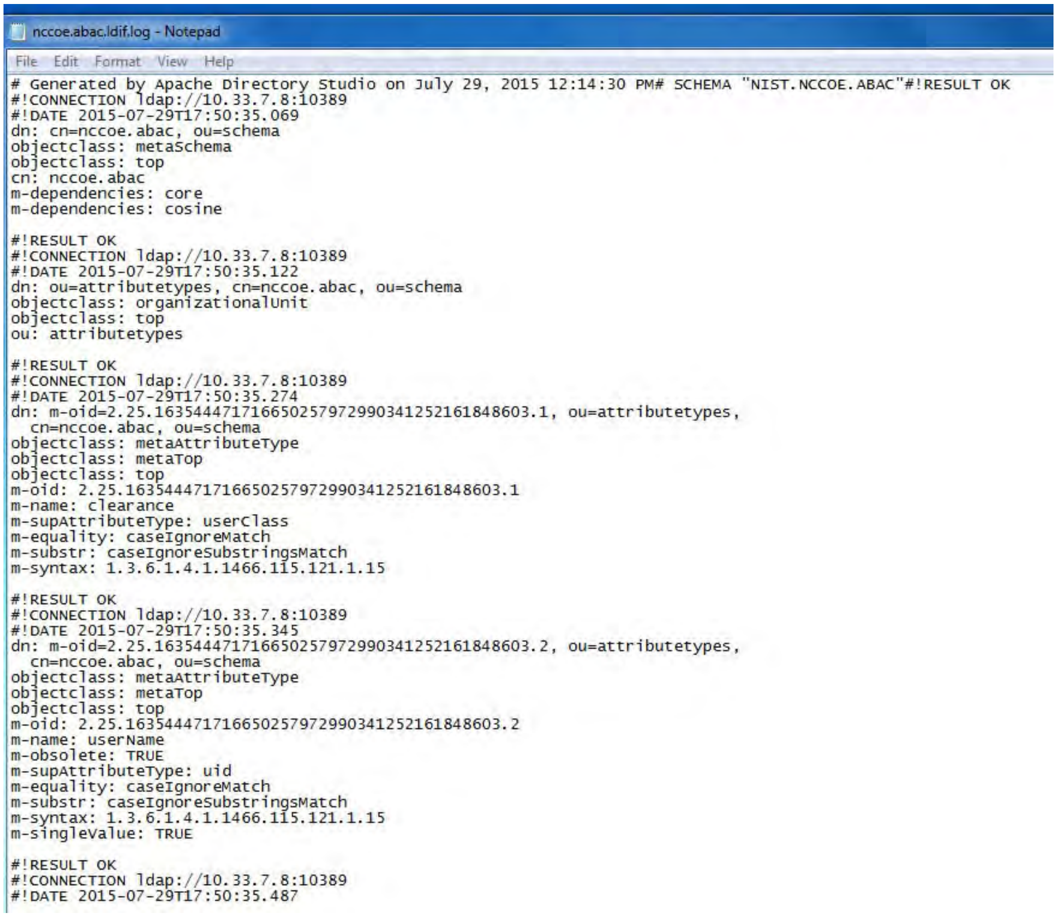
Options

□ Update existing entries

□ Continue on error

23. Click **Finish**.

24. To verify success, the log file generated at the end of the import should show **RESULT OK**.



```
# 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
```

10.10Functional Tests

Once all requirements have been met and all steps in this How-To Guide have been executed, a few functional tests will ensure that the key components of this How-To Guide were correctly deployed and are communicating with other ABAC components as desired.

The first functional test will check the ready state of the NextLabs Policy Controller (ensures that it is running after being paused for plugin deployment).

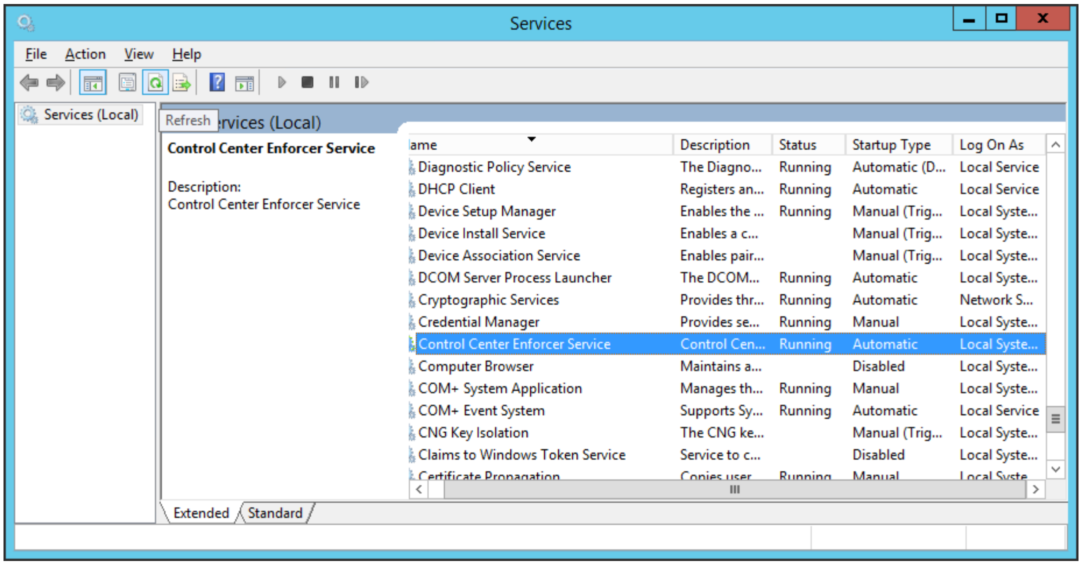
The second test will check that the plugin was successfully loaded into the NextLabs software architecture, that an attribute request is sent to the Protocol Broker from the NextLabs PIP plugin’s getAttribute() function, and that the Protocol Broker responds with an expected attribute value.

The second functional test will ensure that the Protocol Broker is successfully loaded and deployed within the tomcat server instance.

Both of these functional tests can be done on the SharePoint server.

10.10.1 Testing the Ready State of the NextLabs Policy Controller Service

1. Click on the Windows icon and begin typing the word **Services**.
2. When the Services application icon appears, double-click to open the Services application.
3. Within the Services application window, click on the Name column and look for **Control Center Enforcer Service**.
4. Verify that the status column reads **Running**.



Control Center Enforcer Service

Description:
Control Center Enforcer Service

ame	Description	Status	Startup Type	Log On As
Diagnostic Policy Service	The Diagno...	Running	Automatic (D...	Local Service
DHCP Client	Registers an...	Running	Automatic	Local Service
Device Setup Manager	Enables the ...	Running	Manual (Trig...	Local Syste...
Device Install Service	Enables a c...		Manual (Trig...	Local Syste...
Device Association Service	Enables pair...		Manual (Trig...	Local Syste...
DCOM Server Process Launcher	The DCOM...	Running	Automatic	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
Credential Manager	Provides se...	Running	Manual	Local Syste...
Control Center Enforcer Service	Control Cen...	Running	Automatic	Local Syste...
Computer Browser	Maintains a...		Disabled	Local Syste...
COM+ System Application	Manages th...	Running	Manual	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
CNG Key Isolation	The CNG ke...		Manual (Trig...	Local Syste...
Claims to Windows Token Service	Service to c...		Disabled	Local Syste...
Certificate Propagation	Copies user...	Running	Manual	Local Syste...

10.10.2 Test the Successful Loading of the Custom Plugin within the NextLabs Policy Controller Software Architecture

1. Click on the Windows icon.
2. Begin typing **Windows Explorer**.
3. Click on the Windows Explorer application icon.
4. Navigate to **`C:/Program Files/NextLabs/Policy Controller/agentLog/`**.
5. Within the **agentLog** folder, note the **Agentlog0.0** file.
6. Within the **agentLog** folder, copy and paste the locked file **Agentlog0.log0** to open it for review.
   - Left-click on the file name, and hold down Ctrl+C.
   - Left-click anywhere in the **agentLog** folder, right-click and hold down Ctrl+V.
7. Double-click the **Agent0.log-Copy.0** file to open it in your default text editor.
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:

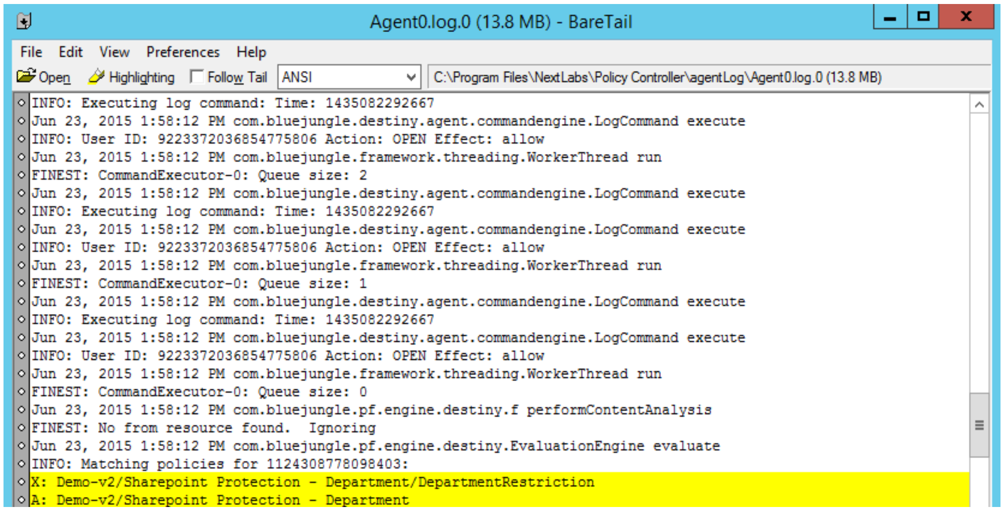
```
Jul 13, 2015 4:59:21 PM
com.bluejungle.pf.domain.destiny.serviceprovider.c A
```

```
FINE: Loading C:\Program Files\NextLabs\Policy
Controller\.\jservice\config\nlsamlpluginService.properties

Jul 13, 2015 4:59:21 PM
com.bluejungle.pf.domain.destiny.serviceprovider.c A
FINE: Loading C:\Program Files\NextLabs/Policy
Controller/jservice/jar/nlsamlplugin/NLSAMLPlugin-0.0.1-SNAPSHOT-jar-with-dependencies.jar

Jul 13, 2015 4:59:22 PM
com.bluejungle.pf.domain.destiny.serviceprovider.ServiceProviderManager register
INFO: A new Service 'NLSAMLPlugin_Service' is registered.
```

9. Within your default text editor, use a search function to search for logging statements you included in your plugin code to verify that the init() methods are called while the jar is loaded within NextLabs (standard according to NextLabs support). Example:

```
Jul 13, 2015 4:59:21 PM
gov.nist.NLSAMLPlugin.UserAttrProviderMod init
INFO: NLSAMLPlugin UserAttrProviderMod code -- init method
Jul 13, 2015 4:59:21 PM
gov.nist.NLSAMLPlugin.HTTPSTransmitter init
```

- You can copy and paste the locked file, or keep a live annotating tool open that will display the contents of Agent0.log0 as new log statements are recorded. Example from this implementation: **BareTail by Bare Metal Software Pty Ltd**.
- Example screenshot using BareTail to open the **Agent0.log0** file, with optional highlighting 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
```

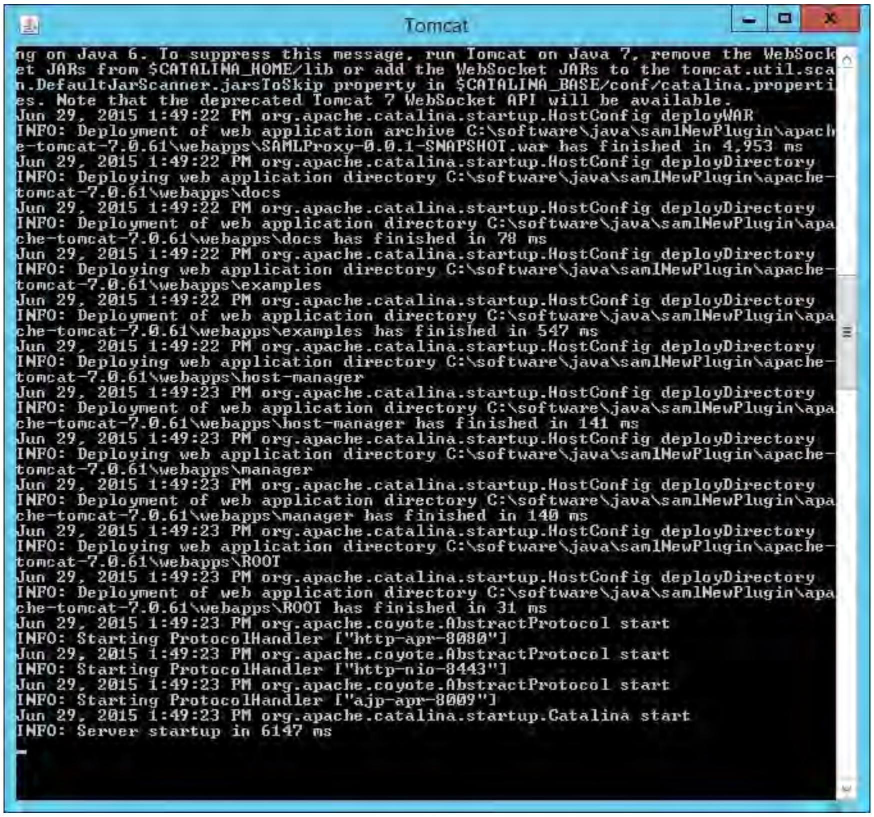
10.10.3Testing that the Protocol Broker .war File Loads Correctly in Tomcat Server

1. On the SharePoint Server, open Services, and ensure that the **Control Center Enforcer Service** is listed as **Running**.

2. Using Windows Explorer, navigate to your Apache tomcat installation within the Windows file structure. Example: **C: /software/apache-tomcat-7.0.61**

3. Double-click to open the bin folder. Example: **C:/software/apache-tomcat-7.0.61/bin**

4. Double-click **startup.bat** to start the bat, and wait for startup to complete.

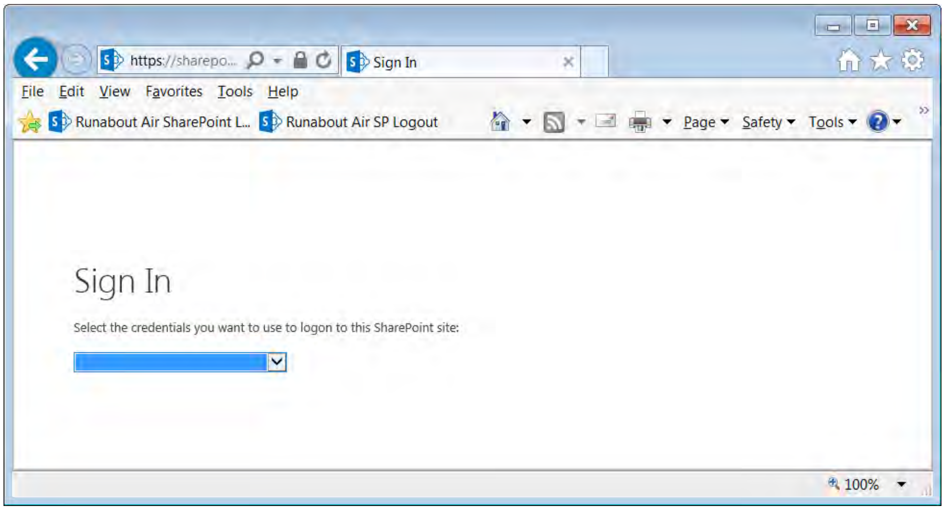


```
ng on Java 6. To suppress this message, run Tomcat on Java 7, remove the WebSock
et JARs from $CATALINA_HOME/lib or add the WebSocket JARs to the tomcat.util.sca
n.DefaultJarScanner.jarsToSkip property in $CATALINA_BASE/conf/catalina.properti
es. Note that the deprecated Tomcat 7 WebSocket API will be available.
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployWAR
INFO: Deployment of web application archive C:\software\java\samlNewPlugin\apach
e-tomcat-7.0.61\webapps\SAMLProxy-0.0.1-SNAPSHOT.war has finished in 4,953 ms
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\docs
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\docs has finished in 78 ms
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\examples
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\examples has finished in 547 ms
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\host-manager
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\host-manager has finished in 141 ms
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\manager
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\manager has finished in 140 ms
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deploying web application directory C:\software\java\samlNewPlugin\apache-
tomcat-7.0.61\webapps\ROOT
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig deployDirectory
INFO: Deployment of web application directory C:\software\java\samlNewPlugin\apa
che-tomcat-7.0.61\webapps\ROOT has finished in 31 ms
Jun 29, 2015 1:49:23 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["http-apr-8080"]
Jun 29, 2015 1:49:23 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["http-nio-8443"]
Jun 29, 2015 1:49:23 PM org.apache.coyote.AbstractProtocol start
INFO: Starting ProtocolHandler ["ajp-apr-8009"]
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 6147 ms
_
```

5. From any computer connected to this network, open an Internet browser.

6. In the address field, type `https://sharepoint.abac.test/` and press Enter.

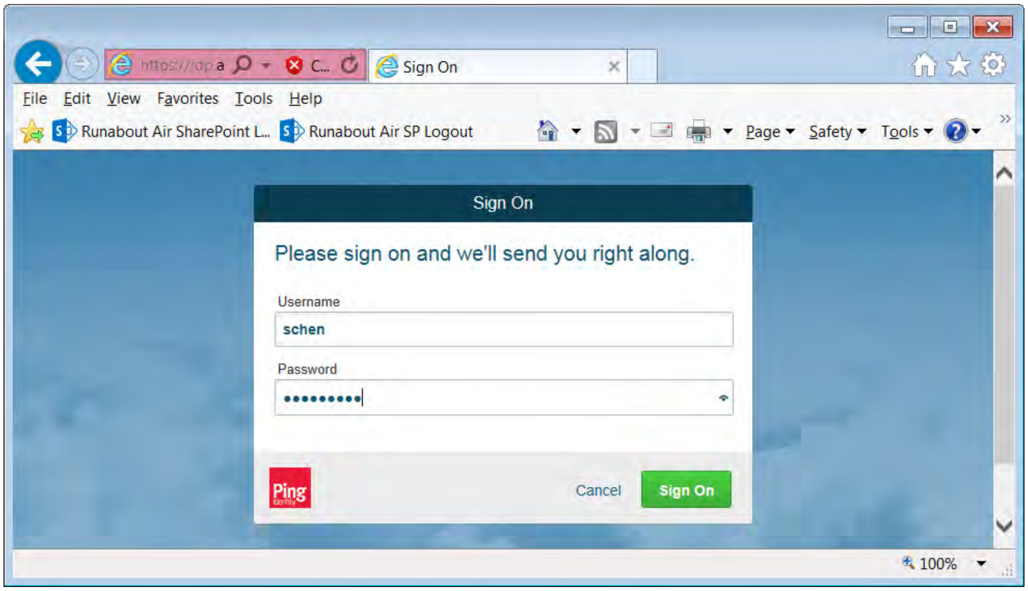
7. Choose **Federated Logon** from the drop-down menu.



Sign In

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

8. At the login screen, enter the credentials of a user that exists in your IdP Active Directory (Chapter 2), and click **Sign On**.



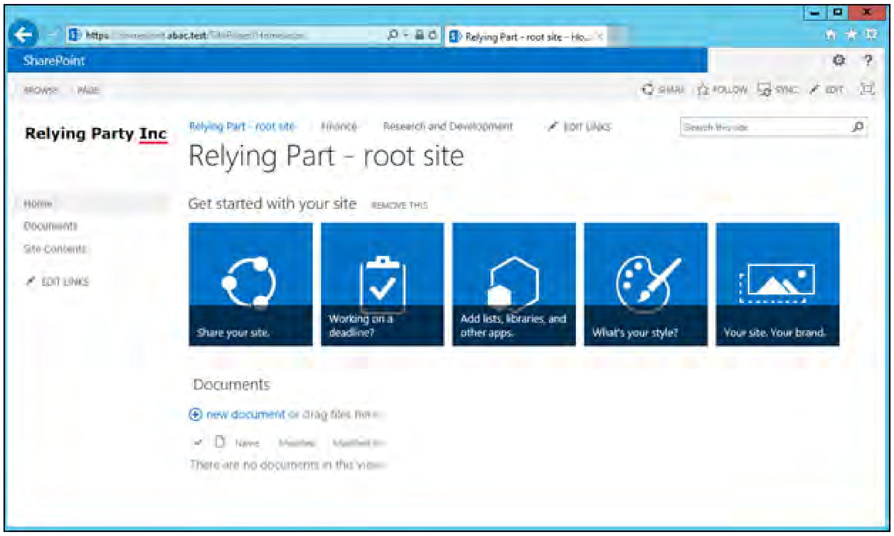
Sign On

Please sign on and we'll send you right along.

Username: schen

Password: ••••••••••

9. Verify that the user was able to access the main page of the RP's SharePoint. Example:



10. In the SharePoint site, double-click on an object for which you know the user will be missing an attribute in order to be granted access, but that can be retrieved via a secondary attribute request using the NextLabs PIP plugin, Protocol broker, and Ping custom data store.

11. Follow the remaining steps 15-18 to verify through standard and custom logging that the Protocol Broker was loaded, that the getAttribute() from the NextLabs PIP plugin was sent, and an expected attribute value was returned.

12. In Windows Explorer, navigate to your installation of Apache tomcat and locate its log files, i.e., **C:/software/apache-tomcat-7.0.61/logs**

13. Open a catalina.___.log file using your default text editor and use a search function to find standard Apache tomcat logging that indicates the .war file was correctly deployed and loads without error. For example, in **C:/software/apache-tomcat-7.0.61/logs/catalina.2015-06-29.log**:

```
Jun 29, 2015 1:49:16 PM
org.apache.catalina.startup.VersionLoggerListener log
INFO: Server version:    Apache Tomcat/7.0.61
Jun 29, 2015 1:49:16 PM
org.apache.catalina.startup.VersionLoggerListener log


Jun 29, 2015 1:49:16 PM
org.apache.catalina.startup.VersionLoggerListener log
INFO: CATALINA_BASE:
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61
Jun 29, 2015 1:49:16 PM
org.apache.catalina.startup.VersionLoggerListener log
INFO: CATALINA_HOME:
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61
```

```
Jun 29, 2015 1:49:16 PM
org.apache.catalina.startup.VersionLoggerListener log
INFO: Command line argument:
-Djava.util.logging.config.file=C:\software\java\samlNewPlugin\apac
he-tomcat-7.0.61\conf\logging.properties
Jun 29, 2015 1:49:16 PM
org.apache.catalina.startup.VersionLoggerListener log
INFO: Command line argument:
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
Jun 29, 2015 1:49:16 PM
org.apache.catalina.startup.VersionLoggerListener log
INFO: Command line argument:
-Djava.endorsed.dirs=C:\software\java\samlNewPlugin\apache-tomcat-7
.0.61\endorsed

Jun 29, 2015 1:49:17 PM org.apache.catalina.startup.HostConfig
deployWAR
INFO: Deploying web application archive
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\SAMLPro
xy-0.0.1-SNAPSHOT.war
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig
deployWAR
INFO: Deployment of web application archive
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\SAMLPro
xy-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\apache-tomcat-7.0.61\webapps\docs
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig
deployDirectory
INFO: Deployment of web application directory
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\docs
has finished in 78 ms

Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig
deployDirectory
INFO: Deploying web application directory
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\example
s
Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig
deployDirectory
```

```
INFO: Deployment of web application directory
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\example
s has finished in 547 ms

Jun 29, 2015 1:49:22 PM org.apache.catalina.startup.HostConfig
deployDirectory
INFO: Deploying web application directory
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\host-ma
nager
Jun 29, 2015 1:49:23 PM org.apache.catalina.startup.HostConfig
deployDirectory
INFO: Deployment of web application directory
C:\software\java\samlNewPlugin\apache-tomcat-7.0.61\webapps\host-ma
nager has finished in 141 ms
```

14. While the same file is open, use another search function to find custom logging that indicates that the Protocol Broker was used for a SAML Attribute query request and response. Example custom log files from this build:

```
Jun 29, 2015 1:59:00 PM nist.pdpplugin.transport.SoapHTTPTransmitter
transmit
INFO: START SoapHTTPTransmitter method. Start time: 1435600740151
Jun 29, 2015 1:59:08 PM nist.pdpplugin.transport.SoapHTTPTransmitter
transmit
INFO: START SoapHTTPTransmitter method. Start time: 1435600748229
Jun 29, 2015 1:59:11 PM nist.pdpplugin.transport.SoapHTTPTransmitter
transmit
INFO: END SoapHTTPTransmitter transmit Method: 1435600751682
Jun 29, 2015 1:59:11 PM nist.pdpplugin.transport.SoapHTTPTransmitter
transmit
INFO: END SoapHTTPTransmitter transmit Method. Total Execution time:
11531
```

15. Within the **Agent0.log0**, another search function to find custom logging statements that verify from within the NextLabs Policy Controller software execution side that the plugin's getAttribute() function was called and that the requested attribute was returned.

    a. Example from this build:

        i. user: **chen@abac.test**

        ii. requested attribute: clearance

        iii. expected returned value: Secret

        iv. actual returned value: Secret

```
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
getAttribute
INFO: NLSAMLPlugin UserAttrProviderMod getAttribute() function
called.
```

```
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
getAttribute
INFO: START getAttribute method. Start time: 1433345957517
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
getAttribute
INFO: NLSAMLPlugin UserAttrProviderMod getAttribute Line00-72 -
subjectID param: schen@abac.test
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
getAttribute
INFO: NLSAMLPlugin UserAttrProviderMod getAttribute Line00-73 -
attributeName param: clearance
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
getAttribute
INFO: NLSAMLPlugin Trying to check if there exist a prior entry in
cache. -- UserAttrProviderMod Line00-79
Jun 3, 2015 11:39:17 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
getAttribute
INFO: NLSAMLPlugin Using soapHTTPTransmitter object and calling its
transmit() function.
Jun 3, 2015 11:39:22 AM gov.nist.NLSAMLPlugin.UserAttrProviderMod
getAttribute
INFO: NLSAMLPlugin UserAttrProviderMod getAttribute() Line00-114 --
attributeValue returned: Secret
```