SSO Design Note

Table of Contents

Overview

The City of Philadelphia requires their users be authenticated using their Active Directory service. This will eliminate the need for separate Salesforce usernames and passwords, as well as allow automatic deactivation of accounts.

Contacts

Name	email	phone	Comments
Shane Ace	Shane.Ace@phila.gov		Completed the integration between Philly's test AD with .swdev sandbox.

Reference Documentation

Salesforce Implementation Guide

Single Sign-On with Force.com and Microsoft Active Directory Federation Services

Reference Implementation

Since March, there's been a working configuration in a sandbox (.swdev) mostly implemented by Shane Ace with assistance from Unisys. That configuration is copied below.

SAML enabled in SSO settings
Single Signon Settings

Name	ADFS.City.phila.local	**API Name**	ADFS_City_phila

SAML Version	2.0	**User Provisioning Enabled**	✓
Issuer	http://adfs.phila.gov/adfs/services/trust	**Entity Id**	https://phill311dev--swdev.cs18.my.salesforce.com
Identity Provider Certificate	CN=ADFS Signing - adfs.phila.gov Expiration: 25 Mar 2015 19:19:49 GMT		
Signing Certificate	SelfSignedCert_11Mar2014_205352		
Assertion Decryption Certificate	Assertion not encrypted		
SAML Identity Type	Federation ID		
SAML Identity Location	Subject		
Identity Provider Login URL	HTTPS://Adfs.phila.gov/adfs/ls/		
Identity Provider Logout URL			
Custom Error URL			
Service Provider Initiated Request Binding	HTTP Redirect		
Salesforce Login URL	https://phill311dev--swdev.cs18.my.salesforce.com?so=00D1100000060EV		
OAuth 2.0 Token Endpoint	https://phill311dev--swdev.cs18.my.salesforce.com/services/oauth2/token?so=00D1100000060EV		

Stored procedures will not be used -- Clinton prefers all integration/smarts be coded inside SAG and not in the target systems.

Implementation Steps

1. Create "My Domain"
    a. philly311.my.salesforce.com (done)

    b. https://philly311.my.salesforce.com
    c. https://philly311.my.salesforce.com/liaisons/login

2. Create Single Signon configuration
    a. exported .swdev's `ADFS_City_phila.samlssoconfig`
    b. edited
    c. loaded

ADFS_City.phila.samlssoconfig

```
<?xml version="1.0" encoding="UTF-8"?>
<SamlSsoConfig xmlns="http://soap.sforce.com/2006/04/metadata">
    <identityLocation>SubjectNameId</identityLocation>
    <identityMapping>FederationId</identityMapping>
    <issuer>http://adfs.phila.gov/adfs/services/trust</issuer>
    <loginUrl>HTTPS://Adfs.phila.gov/adfs/ls/</loginUrl>
    <name>ADFS.City.phila.local</name>

<oauthTokenEndpoint>https://philly311.my.salesforce.com/services/oauth2/token?so=00DG0000000jNg7
</oauthTokenEndpoint>
    <redirectBinding>true</redirectBinding>

<salesforceLoginUrl>https://philly311.my.salesforce.com?so=00DG0000000jNg7</salesforceLoginUrl>
    <samlEntityId>https://philly311.my.salesforce.com</samlEntityId>
    <samlVersion>SAML2_0</samlVersion>
    <userProvisioning>true</userProvisioning>

<validationCert>MIIC2DCCAcCgAwIBAgIQSbDODH/6eYJANnyMhTQyuDANBgkqhkiG9w0BAQsFADAoMSYwJAYDVQQDEx1B
REZTIFNpZ25pbmcgLSBhZGZzLnBoaWxhLmdvdjAeFw0xNDAzMjUxOTE5NDlaFw0xNTAzMjUxOTE5NDlaMCgxJjAkBgNVBAMT
HUFERlMgU2lnbmluZyAtIGFkZnMucGhpbGEuZ292MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2cZPULsvgs8f
ifp8Dl+/vFRKbIVAaGnmla0SZc6MhHDn/uEXVTf0gHGU5DMJHjkVeibaOFrJta6cLxTxt7U382CUTyfDfkoL4vxSC7Y9h4iX
Q4DcK8nS8tm1js8ivUw75uAtB9wG2v6wfr8OfNMPYGTDqBkXep6tserydTUAj0ElhgHn39rS2E4j5tdsejx2WfqFuOC8r622
9wf2AG6nCc2z5HULZD+ILYygv45XSQWFgYbxhkl7atueTLPJ2iiE7Eqb8zwe6PokWVMsBAsq8RYRyO76vKsczCEA9yMMbzpe
44JXDxcX0JccuQv9jYhcy7QopC5Wl8qUL5UOF4R5lQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBag/UUFmxkWE41VUP5KtlK
7DMXbKD4ZsYjKHjkmXN5CXogxAqH5iN53iSOK3FimCzUihim88lfUjdkFJqxQ6Au0z1l6XZz8J5uyhV/3L+pFOy4knO/v4jm
ZugqgWHrF463B+Qo+0fLNHSz+VnARFt/UGIwAT3zwTyUHIegMzRrIFWZ/36fk1AOLSrsespCMsn4bw3+9Bwhp2FFPhK68zXL
d0dB3+68Pd/p9RHfd2ZnkJBsRl96HkDkTwx3OGdbYCR2Few8iya4k39H/GEoHDgOnehNHUDx2QlPVsB0E4DeYYQayvtrXGth
146cKijiXLOnOnFKPUHD0u2DpqxCIgdC</validationCert>
</SamlSsoConfig>
```