

IBM Tivoli Federated Identity Manager
for Versions 6.2.1

***Using SAML for Claims-based
Authentication SharePoint Guide***



Note:

Before using this information and the product it supports, read the information in Notices.

This edition applies to Version 1.5 release i of the IBM Tivoli Federated Identity Manager Integration with SAML for SharePoint Authentication and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation 2011, 2014.

US Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Preface.....	5
About this publication.....	5
Access to publications and terminology	5
Publication Library	5
Base Information.....	5
WebSEAL Information	6
Web Gateway Appliance Information.....	6
IBM Tivoli Federated Identity Manager information	6
IBM Terminology website	7
Accessibility.....	7
Technical training.....	7
Support information	7
Statement of Good Security Practices.....	7
Product name updates	8
Chapter 1: Introducing the integration.....	9
Introduction.....	9
Integration product version information	10
Integration package contents.....	10
Network connectivity considerations.....	11
Chapter 2: Integration process	12
Before you start.....	12
Configuring the web application.....	13
Configuring the Federated Single Sign-on (Federations)	15
Configuring the Federated Single Sign-on (Partners).....	22
Publishing new Pages	28
Exporting the SAML Signing Certificate	28
Configuring a SharePoint Trusted Identity Provider	30
Testing the integration.....	34
Known Issues	37

Notices	38
Trademarks.....	40

Preface

About this publication

This guide provides instructions on how to configure your Microsoft SharePoint to enable a single-sign on using SAML tokens.

This document assumes that Microsoft SharePoint, IBM® Tivoli® Federated Identity Manager are installed and running on your network. It does not provide details on the installation and administration of these products, except where necessary to achieve integration.

This guide is for those responsible for the installation, deployment, and administration of IBM Security Access Manager, and Microsoft SharePoint.

Readers must be familiar with the following:

- Microsoft Windows and UNIX operating systems
- Security management
- Lightweight Directory Access Protocol (LDAP) and directory services
- Supported user registries
- Authentication and authorization

Access to publications and terminology

The following publications complement the information contained in this document:

Publication Library

These publications complement the information that is contained in this publication:

Base Information

- *IBM® Tivoli® Access Manager Base Installation Guide*

Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.

- *IBM Security Access Manager Base Administrator's Guide*

Describes the concepts and procedures for using Access Manager services. Provides instructions for managing tasks from the Web portal manager interface and by using the **pdadmin** command.

WebSEAL Information

- *IBM Security Access Manager WebSEAL Installation Guide*

Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.

- *IBM Security Access Manager WebSEAL Administrator's Guide*

Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.

- *IBM Security Access Manager WebSEAL Developer's Reference*

Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Web Gateway Appliance Information

- *IBM Security Access Manager Web Gateway Appliance Administration Guide*

Provides information about configuring and maintaining a Security Access Manager environment.

IBM Tivoli Federated Identity Manager information

1. *IBM Tivoli Federated Identity Manager Installation Guide*

Explains how to install, configure, and upgrade IBM Tivoli Federated Identity Manager services.

2. *IBM Tivoli Federated Identity Manager Administration Guide*

Describes the concepts and procedures for using IBM Tivoli Federated Identity Manager services.

3. *Redbook: Federated Identity Manager and Web Services Security with IBM Tivoli Security Services*

This Federated Identity Redbook covers important aspects of using the IBM Tivoli integrated identity management architecture to build and deploy the IBM Tivoli Federated Identity Manager and Web Services Security components. See <http://www.redbooks.ibm.com/>.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Product name updates

This publication was first established for IBM Tivoli Access Manager. IBM Tivoli Access Manager has since been superseded by IBM Security Access Manager.

Wherever in this guide, any figures and graphics that contain or refer to IBM Tivoli Access Manager, the use of IBM Security Access Manager is implied. There are no functionality discrepancies between IBM Tivoli Access Manager and IBM Security Access Manager.

Chapter 1: Introducing the integration

This chapter has the following sections:

- [Introduction](#)
- [Integration product version information](#)
- [Network connectivity considerations](#)

Introduction

IBM Tivoli Federated Identity Manager version 6.2 manages the generation of the SAML token that is used to perform single-sign-on (SSO). The identity that is used during the SSO operation can be that of the established IBM Security Access Manager user identity.

The following figure shows the typical sequence of steps that are involved in performing a SAML single-sign-on.

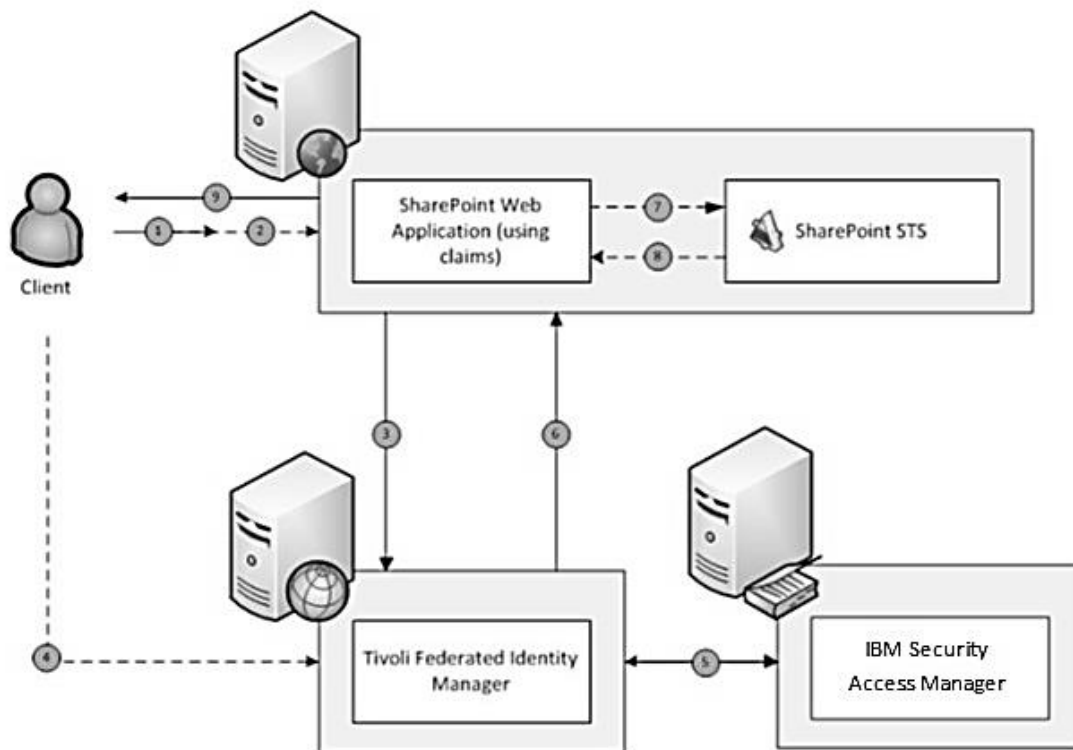


Figure 1. SAML sign-in sequence

1. A client makes a request to a SharePoint web application.

Note: The scenario presented in Figure 1 does not employ IBM Security Access Manager WebSEAL as a reverse proxy.

2. SharePoint redirects the client to the SAML authentication page.
3. The trusted identity provider configured for the SharePoint web application redirects the request to the external (IBM Tivoli Federated Identity Manager) STS login page.
4. Client provides the username and password credentials.
5. Credentials are validated against IBM Security Access Manager for authentication.
6. Tivoli Federated Identity Manager invokes a trust chain to issue a SAML token.
7. The SAML token is presented to the SharePoint STS.
8. SharePoint validates the token and issues a claim-based token.
9. The response is sent back to the client; the FedAuth cookie is stored for subsequent requests.

This guide provides a step-by-step approach for configuring SAML single-sign-on (SSO) for SharePoint web applications. The environment deploys IBM Tivoli Federated Identity Manager in an IBM WebSphere® cluster. Use this guide in the case where IBM Security Federated Identity Manager is running as a stand-alone WebSphere Application Server.

Integration product version information

For information about the supported product versions, see the Release Notes.

Integration package contents

The integration package provides the following files:

File Name	Description
Documents\Microsoft SharePoint\fim_saml_sharepoint_guide.pdf	Supplement guide for Microsoft SharePoint for claims and SAML authentication.
Samples\Microsoft SharePoint\TFIM.SharePoint.Mapping.Rule.xslt	Example XSLT for Tivoli Federated Identity Manager mapping to SAML.
Samples\Microsoft SharePoint\TFIM.SharePoint.Trusted.Provider.ps1	Example Microsoft powershell file for creating a trusted identity provider in SharePoint.
Samples\Microsoft SharePoint\ip_post_to_sp.html	Replacement HTML file for WS-Federation post to SharePoint from Tivoli Federated Identity Manager.

Network connectivity considerations

IBM Security Access Manager services typically run across multiple systems in the network. As such, some network paths must be open for the services to function correctly. All communication is over TCP/IP.

Chapter 2: Integration process

The following sections detail the steps that are required to achieve this integration.

- [Before you start](#)
- [Configuring the web application](#)
- [Testing the integration](#)

Before you start

This guide does not cover the configuration of the entire environment. In particular, the following product installations and configurations must already be complete:

Note: Consult the documentation that is outlined in [Access to publications and terminology](#) for details on installing and configuring these products.

IBM Tivoli Federated Identity Manager

- Deployed to a WebSphere Application Service.
- An IBM Tivoli Federated Identity Manager domain is configured and the runtime is deployed to the domain.
- A Point of contact server is configured for Tivoli Federated Identity Manager.

IBM Security Access Manager

- User registry is configured with a supported registry.
- IBM Security Access Manager Policy Server installed.

Microsoft SharePoint

- Installed into a farm or single-instance environment

See [Integration product version information](#) for product details.

Configuring the web application

To use claims authentication, a web application must be created or configured. Complete the following steps by using Microsoft SharePoint Central Administration:

1. Click **Manage web application**.
2. On the Web Application tab, click **New**.



3. In the Create New Web Application window, select **Claims Based Authentication** as Authentication.

Note: SharePoint 2013 does not require Claims Based Authentication. Ignore this option in SharePoint 2013.

Create New Web Application

Authentication
Select the authentication for this web application.
Learn about authentication.

☒ Claims Based Authentication
☐ Classic Mode Authentication

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 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.

☐ Use an existing IIS web site
Default Web Site

☒ Create a new IIS web site
Name:
Port:
Host Header:
Path:

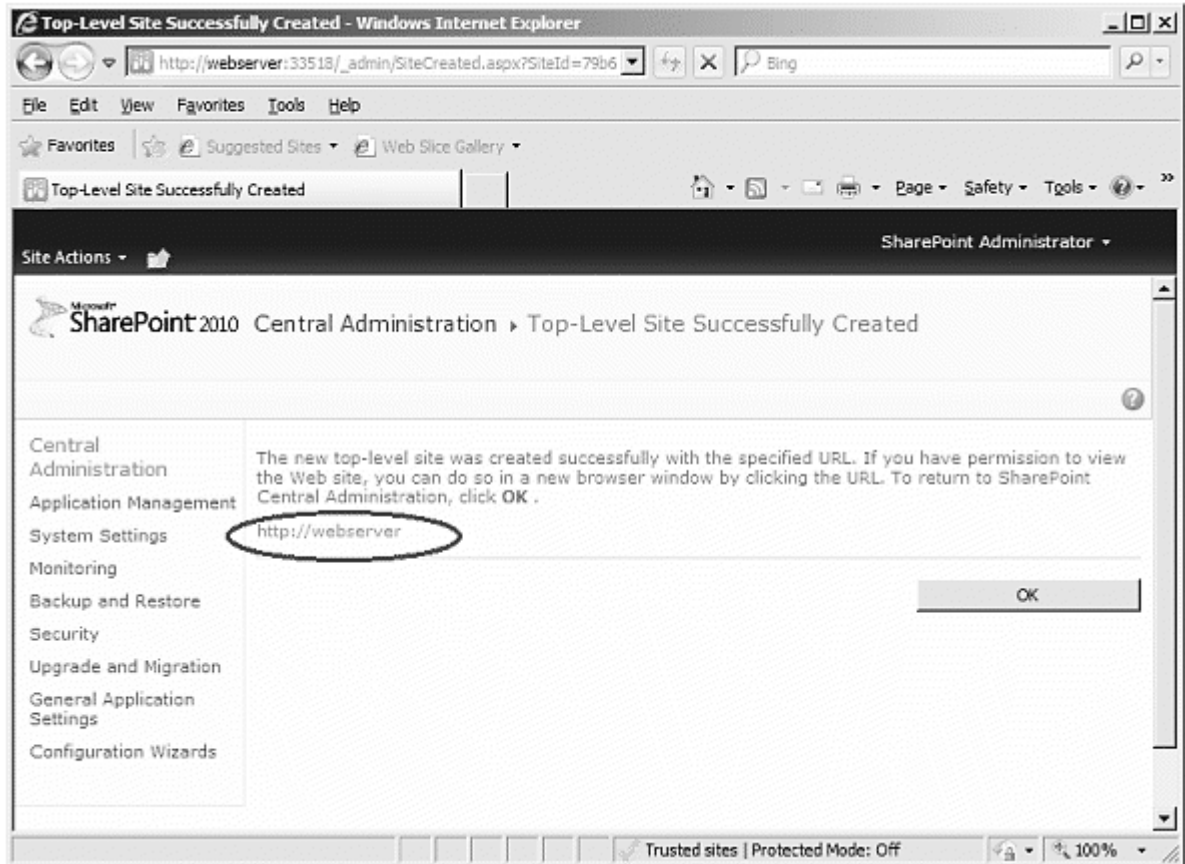
Security Configuration
If you choose to use Secure Sockets Layer (SSL), you must add the certificate on each server using the IIS administration tools. Until this is done, the web application will be inaccessible from this IIS web site.

Allow Anonymous
☐ Yes
☒ No

Use Secure Sockets Layer (SSL)
☐ Yes
☒ No

OK Cancel

4. Enter other details specific to your web application.
5. Click **OK** to create the new web application.
6. Return to the Central Administration home page and click **Create site collections**.
7. Enter appropriate details for the site collection and then click **OK**.



8. Take note of the URL of the newly created site, and then click OK.

Configuring the Federated Single Sign-on (Federations)

You must create an IBM Tivoli Federated Identity Manager trust chain that can generate a SAML token from the point of contact.

Note: This guide assumes that you have configured a point of contact in your environment. The choice of point of contact type to be employed in your environment is determined by the security architecture and network topology requirements. For more information about the supported options for point of contacts and the necessary configurations for the point of contact, see the Tivoli Federated Identity Manager product documentation on the appropriate sites.

1. From the WebSphere console, select IBM Tivoli Federated Identity Manager to expand it.
2. Select **Configure Federated Single Sign-on** to expand it.
3. Select **Federations**.
4. On the **Federations** page, click **Create**.
5. Enter a Federation name.

6. Select **Identity Provider** as the role.
7. Click **Next**.

The screenshot shows a web-based configuration interface. On the left is a vertical navigation pane with the following items: **General Information** (highlighted with a double arrow), Contact Information, Federation Protocol, Point of Contact Server, Identity Mapping Options, Identity Mapping, and Summary. The main content area is titled 'General Information' and contains the instruction 'Provide basic information about this federation.' Below this are two sections: '+ Federation Name' with a text input field containing 'TFIM', and '+ Identify your role' with two radio button options: 'Identity Provider' (which is selected) and 'Service Provider'. At the bottom of the main area are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

8. On the second configuration page, enter the contact information (optional).

The screenshot shows the 'Contact Information' configuration page. The left navigation pane now has a checkmark next to 'General Information' and a double arrow next to 'Contact Information', which is highlighted. The main content area is titled 'Contact Information' and contains the instruction 'Provide information about who to contact with respect to this federation. This information will be provided to partners when sharing metadata.' The form includes several fields: '+ Company Name' (text input with placeholder 'Your Company Name'), 'Company URL' (text input with placeholder 'www.mycompany.com'), 'Contact Person' section with 'First Name' (text input with 'John') and 'Last Name' (text input with 'Citizen'), 'Email Address' (text input with placeholder 'jcitizen@mycompany.com'), 'Phone Number' (text input with placeholder '555-555-555'), and 'Contact Type' (dropdown menu with 'Technical' selected). At the bottom is an 'Other Information' section with a large, empty text area. The bottom of the page features the same four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

9. Click **Next** to proceed.
10. On the Federation Protocol page, select **WS-Federation Passive Profile**.

General Information
Federation Information
Federation Protocol
Point of Contact Server
Signatures
SAML Message Settings
Configure Security Token
Identity Mapping Options
Identity Mapping
Summary

Federation Protocol

Select the protocol used for this federation.

*Protocol

- ☐ Liberty ID-FF 1.1
- ☐ Liberty ID-FF 1.2
- ☐ SAML 1.0
- ☐ SAML 1.1
- ☐ SAML 2.0
- ☒ WS-Federation Passive Profile
- ☐ Information Card
- ☐ OpenID

< Back Next > Finish Cancel

11. Click **Next** to proceed.
12. On the Point of Contact Server page, enter the endpoint URL of your configured point of contact server.

The scenario in this guide uses IBM Tivoli Federated Identity Manager server as point of contact. The following figure shows the Point of Contact URL as `http://fimserver.test.com:9080/sps`.

<ul style="list-style-type: none"> ✓ General Information ✓ Context Information ✓ Federation Protocol Point of Contact Server ✓ Select Token Module Instance ✓ Configure Security Token ✓ Configure Mapping ✓ Options ✓ Review Mapping ✓ Summary 	<h3>Point of Contact Server</h3> <p>Enter the endpoint URL of your point of contact server. The URL can be for a reverse proxy server, such as WebSEAL, that is configured in front of the application server and the Web server. The URL can also be WebSphere Application Server itself, if no additional Web server is configured.</p> <p>Point of Contact</p> <p>* <input type="text" value="http://timsrver.test.com:9080"/> /sps/</p>
	<p>< Back Next > Finish Cancel</p>

Note: Depending on your environment, the URL can be for a reverse proxy server such as WebSEAL that is configured in front of the application server and the Web server. When the Point of Contact is WebSEAL, the URL is:

`http(s)://<webseal server name>/<webseal junction name>`

The URL can also be WebSphere Application itself, if no additional Web server is configured. If you are using HTTPS for WebSphere point of contact, the URL and default port is:

`https://<tfim server name>:9443`

13. Click **Next** to proceed.

14. On the Select Token Module Instance page, select **Default SAML 1.1 Token**.

✓

General Information

✓

Contact Information

✓

Federation Protocol

✓

Point of Contact Server

✕

Select Token Module Instance

Configure Security Token

Identity Mapping Options

Identity Mapping

Summary

Select Token Module Instance

+

+

+

+

+

+

+

+

+

+

+

+

...

Select Action

...

Select	Name	Type	Description
<input checked="" type="radio"/>	Default SAML 1.1 Token	SAMLTokenSTSMModule	Default SAML 1.1 Token Instance
<input type="radio"/>	Default WS-Federation Token	SAMLTokenSTSMModule	Default WS-Federation Token Instance

Page 1 of 1

Total: 2 Filtered: 2 Displayed: 2 Selected: 1

< Back

Next >

Finish

Cancel

15. Click **Next** to proceed.

16. On the Configure Security Token page, enter the values as shown.

✓

General Information

✓

Contact Information

✓

Federation Protocol

✓

Point of Contact Server

✓

Select Token Module Instance

✕

Configure Security Token

Identity Mapping Options

Identity Mapping

Summary

Configure Security Token

Enter the configuration parameters for the federated security token. In addition, synchronize the system clocks of your server and your partner's server.

+

Amount of time before the issue date that an assertion is considered valid (seconds)

00

+

Amount of time the assertion is valid after being issued (seconds)

120

< Back

Next >

Finish

Cancel

17. Click **Next** to proceed.

18. On the Identity Mapping Options page, select **Use XSL or JavaScript transformation for identity mapping**.

<ul style="list-style-type: none"> General Information Contact Information Federation Protocol Point of Contact Server Select Token Select Token Module Instance Configure Security Token Identity Mapping Options Identity Mapping Summary 	<h3>Identity Mapping Options</h3> <p>If you are an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a local user account. If you are a service provider, this mapping specifies how to match an assertion from your partner to your local user accounts. Select one of the following identity mapping options.</p> <p> <input checked="" type="radio"/> Use XSL or JavaScript transformation for identity mapping <input type="radio"/> Use Tivoli Directory Integrator for identity mapping <input type="radio"/> Use custom mapping module instance </p>
	<p>< Back Next > Finish Cancel</p>

19. Click **Next** to proceed.
20. On the Identity Mapping page, browse to the XSLT mapping file in the Examples location. You might need to modify this file to represent your extended attribute configuration if WebSEAL is configured as the point of contact.

<ul style="list-style-type: none"> General Information Contact Information Federation Protocol Point of Contact Server Select Token Select Token Module Instance Configure Security Token Identity Mapping Options Identity Mapping Summary 	<h3>Identity Mapping</h3> <p>Import the XSL or JavaScript file that contains the Identity Mapping Rule.</p> <p>*XSL or JavaScript file Containing Identity Mapping Rule</p> <p>Files\IBM\FIM\examples\mapping_rules\ip_saml_1x.xsl Browse...</p>
	<p>< Back Next > Finish Cancel</p>

21. Click **Next** to proceed.
22. On the Summary page, click **Finish**.

<ul style="list-style-type: none"> ✓ General Information ✓ Contact Information ✓ Federation Protocol ✓ Point of Contact Server ✓ Select Token Module Instance ✓ Configure Security Token ✓ Identity Mapping Options ✓ Identity Mapping ∞ Summary 	<p>Summary</p> <hr/> <p>Verify the information you have entered. Go back in the wizard if there is anything you need to correct or click Finish to complete the wizard.</p> <p>Federation Name: TFIM</p> <p>Company Name: Your Company Name</p> <p>Company URL: www.mycompany.com</p> <p>Contact Person</p> <hr/> <p>First Name: John</p> <p>Last Name: Citizen</p> <p>Email Address: jcitizen@mycompany.com</p> <p>Phone Number: 555-5555-555</p> <p>Contact Type: Technical</p> <p>Other Information:</p> <p>Identity Mapping</p> <hr/> <p>Use XSL or JavaScript transformation for identity mapping: c:\program files\ibm\fim\examples\mapping_rules\ip_saml_1x.xsl</p> <p>SSO Protocol: WS-Federation Passive Profile</p> <p>Identity Provider Single Sign-On Properties</p> <hr/> <p>WS-Federation Realm: http://fimserver.test.com:9080/sps/TFIM/wsf</p> <p>WS-Federation Endpoint: http://fimserver.test.com:9080/sps/TFIM/wsf</p>
<p> <input style="border: 1px solid black;" type="button" value=" < Back "/> <input style="border: 1px solid black;" type="button" value=" Next > "/> <input style="border: 1px solid black;" type="button" value=" Finish "/> <input style="border: 1px solid black;" type="button" value=" Cancel "/> </p>	

23. Click **Load configuration changes to Tivoli Federated Identity Manager runtime.**

Configuring the Federated Single Sign-on (Partners)

You must create a partner to associate with the federation created. The partner for this integration is SharePoint.

1. From the WebSphere console, select **Tivoli Federated Identity Manager** to expand it.
2. Select **Configure Federated Single Sign-on** to expand it.
3. Select **Partners**.
4. On the Partners page, click **Create**.
5. Select the previously created federation name.

The screenshot shows the 'Select Federation' dialog box. On the left is a sidebar with a tree view containing 'Select Federation' (selected), 'Identity Mapping Options', 'Identity Mapping', and 'Summary'. The main area has the title 'Select Federation' and the instruction 'Select the federation to which you would like to add a partner.' Below this is a toolbar with icons for adding, deleting, and editing, and a dropdown menu labeled '-- Select Action --'. A table follows with columns: 'Select', 'Federation Name', 'My Role', 'Single Sign-On Protocol', and 'Number of partners'. The table contains one row with the value 'TFIM' under 'Federation Name' and '1' under 'Number of partners'. At the bottom of the table, it says 'Page 1 of 1', 'Totals: 2', 'Filtered: 2', 'Displayed: 2', and 'Selected: 1'. At the very bottom of the dialog are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Select	Federation Name	My Role	Single Sign-On Protocol	Number of partners
<input checked="" type="radio"/>	TFIM	Identity Provider	WS-Federation Passive Profile	1

Page 1 of 1 Totals: 2 Filtered: 2 Displayed: 2 Selected: 1

< Back Next > Finish Cancel

6. Click **Next** to proceed.
7. On the Contact Information page, enter a Service Provider Company name and any other information about your partner.

8. Click **Next** to proceed.
9. On the WS-Federation Data page, enter the realm and endpoint settings.

The WS-Federation Realm setting is a unique value that is used by the SharePoint trusted provider configuration. It must be defined in the following structure: `urn:<value>`. example: `urn:webserver`. The setting must correspond with the Federated Single Sign-on (Federation) WS Federation Realm.

The WS-Federation Endpoint is the URL that IBM Tivoli Federated Identity Manager redirects to after the SAML token is generated. The WS-Federation Endpoint value is the URL of the SharePoint site that is created in Step 8 of Configuring the Web Application, append `/_trust/` path to the URL of the webserver. For example: `http://<hostname of target Webserver machine>/_trust/`. The `/_trust/` path is created during the trusted identity provider configuration.

✓ <u>Contact Information</u>	WS-Federation Data
WS-Federation Data	*WS-Federation Realm <input type="text" value="urn:WEBSERVER"/>
Configure Security Token	*WS-Federation Endpoint <input type="text" value="http://webserver/_trust/"/>
Identity Mapping Options	Maximum Request Lifetime (in seconds) <input type="text" value="-1"/>
Identity Mapping	
Summary	
<input data-bbox="316 940 393 968" type="button" value=" < Back "/> <input data-bbox="407 940 483 968" type="button" value=" Next > "/> <input data-bbox="498 940 558 968" type="button" value=" Finish "/> <input data-bbox="573 940 649 968" type="button" value=" Cancel "/>	

10. Click **Next** to proceed.
11. On the Configure Security Token page, select the keystore and provide a password, then click **List Keys**. The password for the DefaultKeyStore is *testonly*.
12. Select the key to apply to the SAML token.

✓ Contact Information

✓ WS-Federation Data

Configure Security Token

Identity Mapping Options

Identity Mapping

Summary

Configure Security Token

Enter the configuration parameters for the federated security token. In addition, synchronize the system clocks of your server and your partner's server.

☒ Sign SAML Assertions

Select Key for Signing Assertions

Keystore

DefaultKeyStore

Keystore Password

List Keys

+

+

+

+

... Select Action ...

Select	Alias	Key Type	Days until expiration	Subject DN
<input checked="" type="radio"/>	testkey	Public/Private Key Pair	2283	CN=fimdemo.ibm.com, OU=TAMeB, ...

Page 1 of 1

Total: 1

Filtered: 1

Displayed: 1

Selected: 1

Select the KeyInfo elements to include

Include the X509 Subject Key Identifier?

Use the default action

Include the Public Key?

Use the default action

Include X509 Subject Issuer Details?

Use the default action

Include the X509 Subject Name?

Use the default action

Include the X509 Certificate Data?

Use the default action

☒ Include the InclusiveNamespaces element in the canonicalization of the assertion during signature creation.

Include the following attribute types (a "*" means include all types).

*

Subject Confirmation Method

urn:oasis:names:tc:SAML:1.0:cm:bearer

< Back

Next >

Finish

Cancel

13. Click **Next** to proceed.
14. On the Identity Mapping Options page, select **Use XSL or JavaScript transformation for identity mapping**.

<ul style="list-style-type: none"> ✓ Select Federation ✓ Contact Information ✓ WS-Federation Data ✓ Configure Security Token Identity Mapping Options Identity Mapping Summary 	<h3>Identity Mapping Options</h3> <hr/> <p>If you are an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a local user account. If you are a service provider, this mapping specifies how to match an assertion from your partner to your local user accounts. Select one of the following identity mapping options.</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Use XSL or JavaScript transformation for identity mapping <input type="radio"/> Use Tivoli Directory Integrator for identity mapping <input type="radio"/> Use custom mapping module instance
<div style="display: flex; justify-content: space-between; align-items: center;"> < Back Next > Finish Cancel </div>	

15. Click **Next** to proceed.
16. Click **Next** to proceed, or browse to the mapping file you want to use. If a rule is not specified here, the mapping role that is configured for this partner's federation is used.

<ul style="list-style-type: none">✓ Select Federation✓ Contact Information✓ WS-Federation Data✓ Configure Security Token✓ Identity Mapping Options☛ Identity Mapping	<h3>Identity Mapping</h3> <p>Enter a specialized identity mapping for this partner. If a rule is not specified here, the mapping rule that is configured for this partner's federation will be used.</p> <p>XSL or JavaScript file Containing Identity Mapping Rule</p> <div><input type="text"/> <input type="button" value="Browse..."/></div>
Summary	
<div><input type="button" value="◀ Back"/> <input type="button" value="Next >"/> <input type="button" value="Finish"/> <input type="button" value="Cancel"/></div>	

17. On the Summary page, click **Finish**.
18. Click **Enable Partner**.
19. Click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

Publishing new Pages

You must publish the identity provider to service provider page to support SharePoint's implementation of WS-Federation. Complete the following steps:

1. Copy the `ip_post_to_sp.html` in the `examples` folder from the integration package: `<drive>\Program Files\IBM\FIM\pages\C\wsfed-eration`

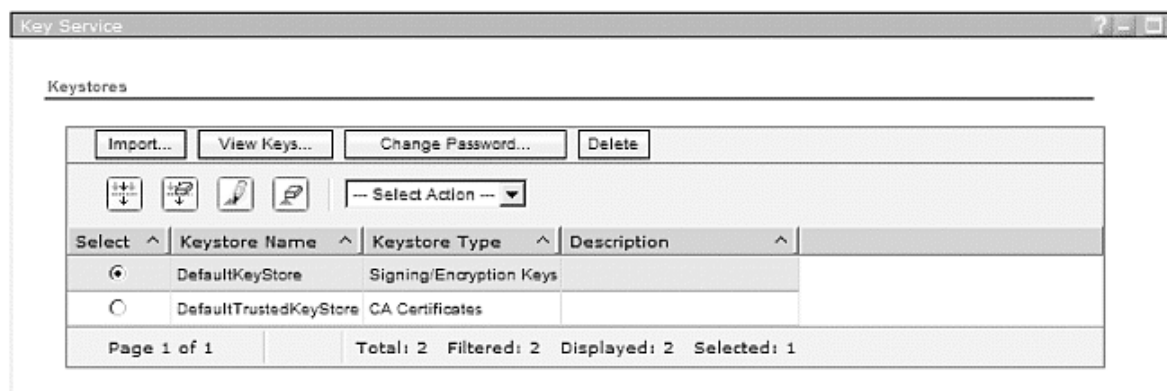
Note: Backup the existing file before overriding.

2. From the WebSphere console, select **Tivoli Federated Identity Manager** to expand it.
3. Select **Domain Management** to expand it.
4. Select **Runtime Node Management**.
5. Click **Publish Pages**.
6. After this operation completed, you will be prompted to **Load configuration changes to Tivoli Federated Identity Manager runtime**.

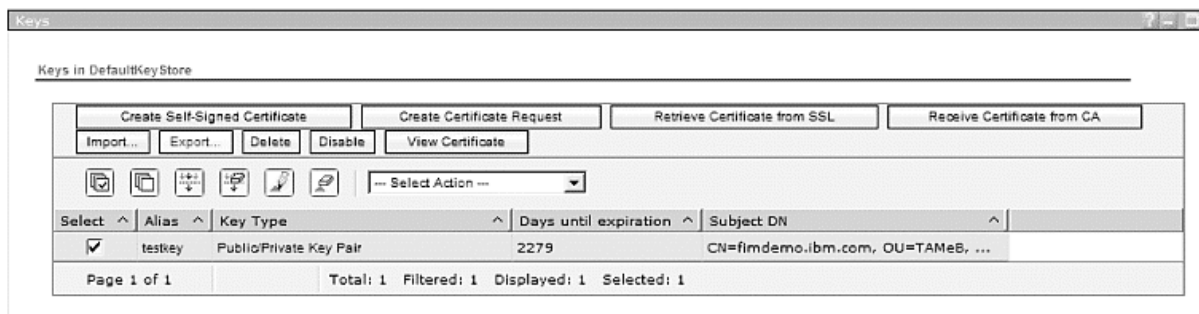
Exporting the SAML Signing Certificate

SharePoint requires that SAML tokens be signed. In step 12 of Configuring the Federated Single Sign-On (Partners), a signing certificate was selected. This certificate must be exported so that the trusted identity provider in SharePoint can verify the signer.

1. From the WebSphere console, select **Tivoli Federated Identity Manager** to expand it.
2. Select **Configure Key Service** to expand it.
3. Select **Keystores**.
4. On the **Key Service** page, select the keystore name that you selected in step 12 of the Configuring the Federated Single Sign-On (Partners).



5. Click **View Keys**.
6. Enter the keystore password, click **OK**.
7. Select the key to export, then click **Export**.



8. Select **PKCS#12** export format.
9. Click the **Download Key**.
10. Save the file.

Note: If you are exporting a self-signed certificate from the keystore, you must first import the certificate into the Microsoft Certificate Store by using the same password to access the Tivoli Federated Identity Manager keystore. The Microsoft Certificate Store is access through the Microsoft Management Console snap-in (MMC).

To open MMC:

1. From the Start Menu, select **Run**.
2. Type `mmc`
3. Click **OK**.
4. In the MMC application, select the File menu, select **Add/Remove Snap-in**.
5. A list of available snap-ins are displayed. Select the Certificates item from the list, then click **Add**.
6. If you imported the `pfX` certificate through the wizard and accepted the default certificate store, select **My User Account** as the certificate store you want to add to the snap-in console.
7. Click **OK**.
8. Under the Certificates – Current User node, expand the Personal folder, followed by the Certificate folder.
9. A list of certificates in this store is displayed. Select the certificate that you imported, right click and select **Export**.

Export the certificate using the `.cer` file extension through the Export Wizard.

Configuring a SharePoint Trusted Identity Provider

A trusted identity provider enables SharePoint to redirect a user to IBM Tivoli Federated identity Manager for authentication and represents the SAML elements that are expected in the response from Tivoli Federated Identity Manager.

Complete the following steps by using Microsoft SharePoint Central Administration:

1. Click **Security**.
2. Under General Security, click **Manage trust**.
3. Click **New**.
4. Enter a name for the trust relationship.
5. Browse to the certificate file exported from Tivoli Federated Identity Manager.

The screenshot shows the 'Establish Trust Relationship' dialog box with three sections: General Setting, Root Certificate for the trust relationship, and Security Token Service (STS) certificate for providing Trust. The Name field is set to 'TFIM'. The Root Authority Certificate field is set to 'C:\root_testkey.cer' with a 'Browse...' button. The Security Token Service (STS) certificate section has an unchecked checkbox for 'Provide Trust Relationship', a 'Token Issuer Description' field, and a 'Token Issuer Certificate' field with a 'Browse...' button. The dialog has 'OK' and 'Cancel' buttons at the bottom right.

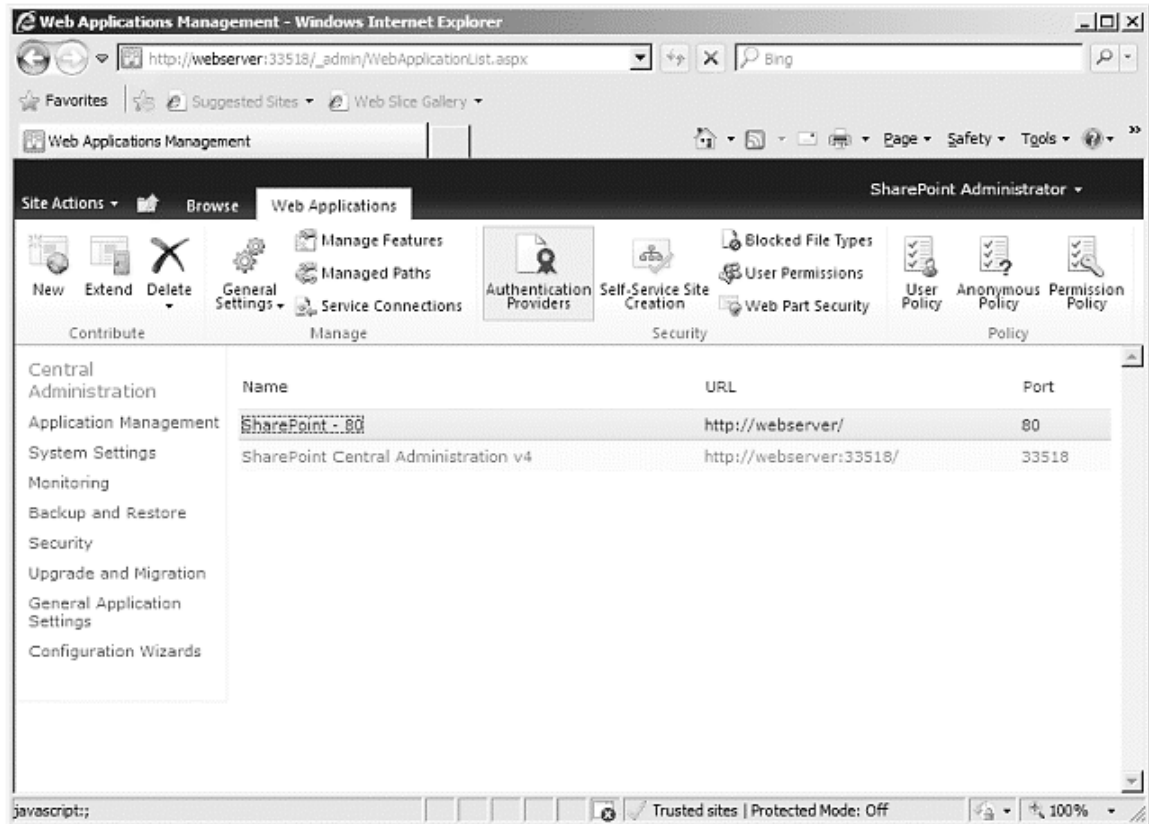
Establish Trust Relationship	
General Setting The name for this trust relationship. Learn about trusts.	Name: <input type="text" value="TFIM"/>
Root Certificate for the trust relationship This is mandatory regardless of whether you want to provide to or consume trust from the other farm. Please add the Root Certificate for the other farm with which you want to establish a trust relationship. Learn about certificates.	Root Authority Certificate <input type="text" value="C:\root_testkey.cer"/> Browse...
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.	<input type="checkbox"/> Provide Trust Relationship Token Issuer Description: <input type="text"/> Token Issuer Certificate <input type="text"/> Browse...
<div>OK Cancel</div>	

6. Click **OK** to save and close dialog.
7. Open the file `TFIM.SharePoint.Trusted.Provider.ps1` in the `Samples` folder and review the comments in the file to understand the necessary changes that are required to reflect your configuration settings in Tivoli Federated Identity Manager and SharePoint.

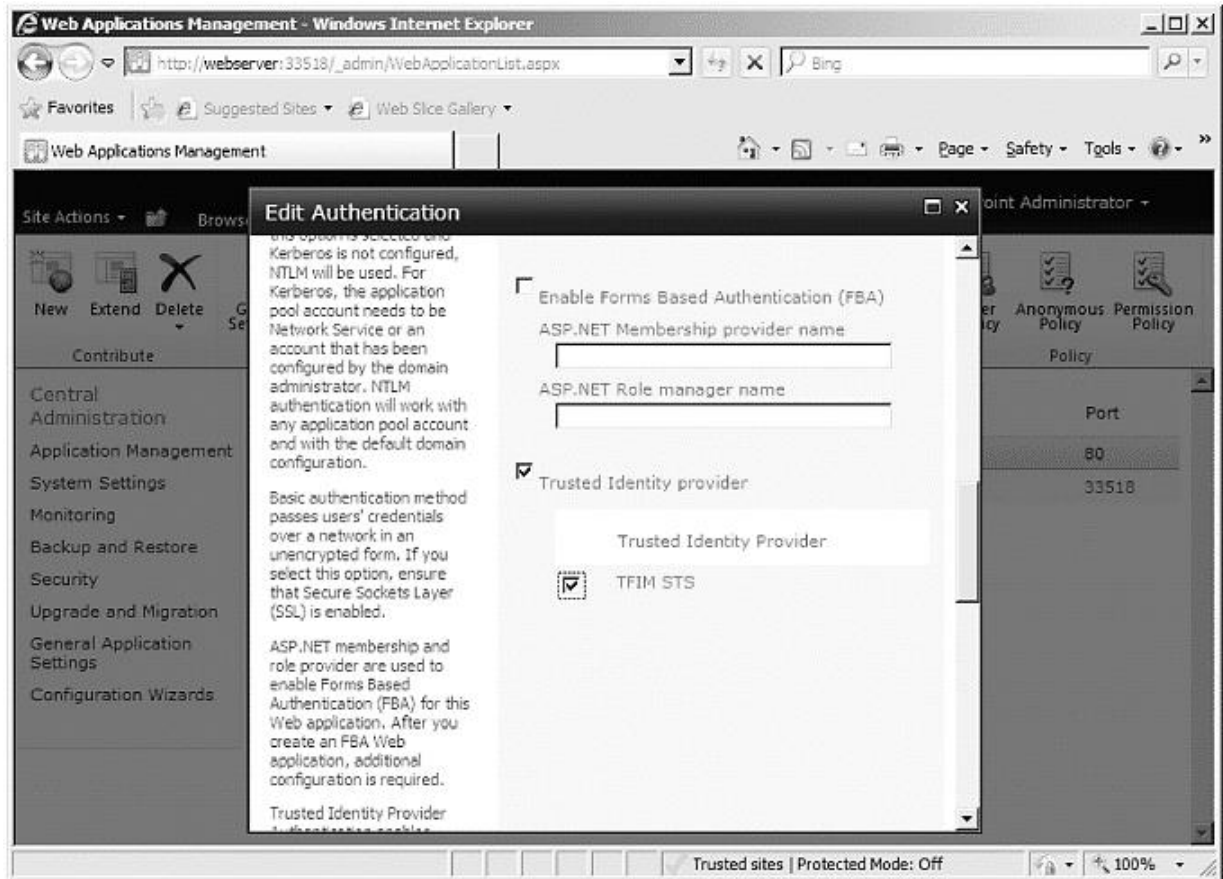
Modify the file to your environment configurations. Save your changes upon completion.

8. Open the Microsoft SharePoint Management command window from **Start > All Programs > Microsoft SharePoint Products 2010/2013 > SharePoint Management Shell**.
9. Drag and drop the file that is saved in Step 7 into the SharePoint Management command window. Any errors are written out to the console (normally in red). Otherwise the properties of the new trusted identity provider are displayed in the console.
10. To update the SharePoint Security Token Service (STS) Token Expiration, type the following script at the SharePoint Management shell prompt :

```
$sts = Get-SPSecurityTokenServiceConfig  
$sts.LogonTokenCacheExpirationWindow = (New-TimeSpan -minutes 1)  
$sts.Update()  
Iisreset
```
11. Under Central Administration, click **Manage web applications**.
12. Select the site that is created in step 3 of Configuring the web application.



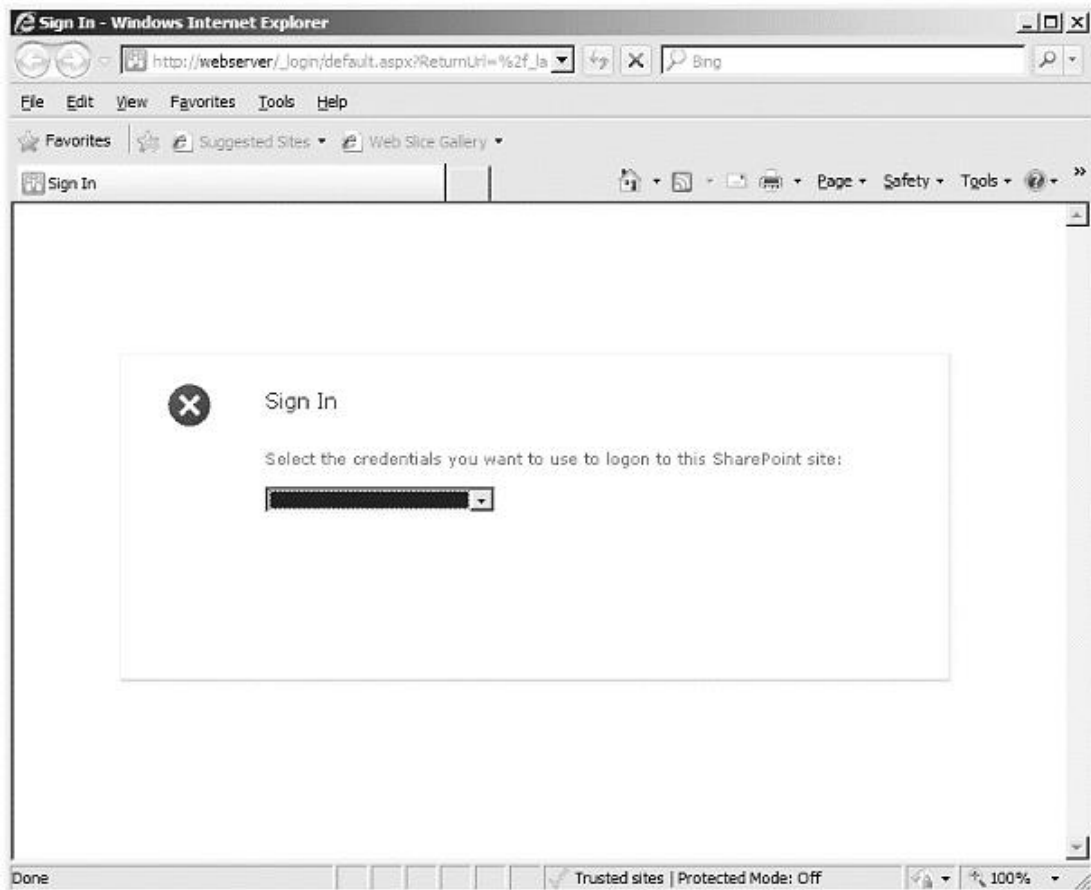
13. Click **Authentication Providers** from the ribbon bar.
14. Select the zone to assign the trusted identity provider.
15. Scroll down to the **Claims Authentication Types** section. Select **TFIM STS** as the name of the trusted identity provider that is configured in step 8 above.



16. Click **OK** to save changes.

Testing the integration

1. Navigate to the SharePoint web site URL created in Step 7 of Configuring the Web Application.
2. Select the TFIM STS item from the list. The browser redirects to the WebSEAL login.



3. Enter the credentials for your point of contact server.

The screenshot shows a Windows Internet Explorer browser window. The title bar reads "ITFIM Form Login - Windows Internet Explorer". The address bar shows the URL "http://fmsserver.lab.gc.ibm.com:9080/sps/login.jsp". The browser's menu bar includes "File", "Edit", "View", "Favorites", "Tools", and "Help". Below the menu bar is a "Favorites" section with "Suggested Sites" and "Web Site Gallery". The main content area displays the "Form Login" page. At the top of the page, it says "Please enter user ID and password." Below this is a "Login" form with two input fields: "User ID:" and "Password:". A "Log In" button is positioned below the password field. The status bar at the bottom of the browser window shows "Done" on the left, "Internet | Protected Mode: Off" in the center, and a zoom level of "100%" on the right.

ITFIM Form Login - Windows Internet Explorer

http://fmsserver.lab.gc.ibm.com:9080/sps/login.jsp

File Edit View Favorites Tools Help

Favorites Suggested Sites Web Site Gallery

ITFIM Form Login

Form Login

Please enter user ID and password.

Login

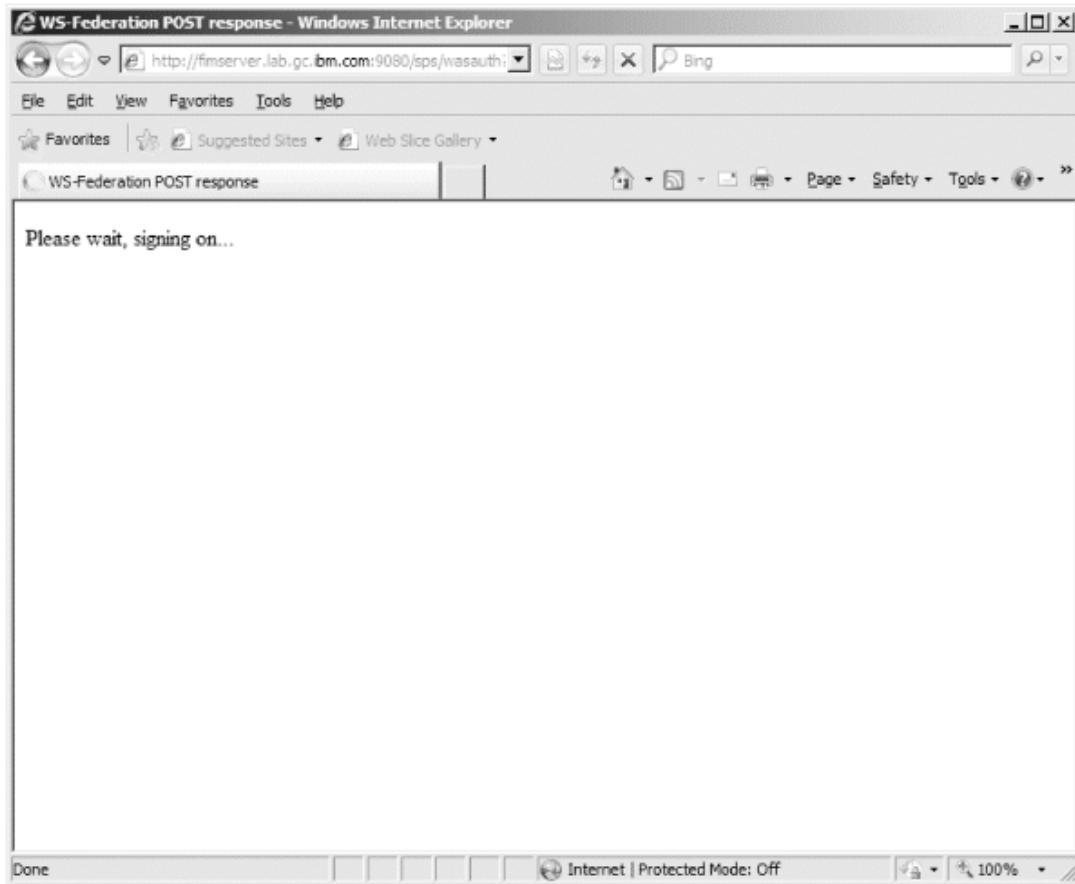
User ID:

Password:

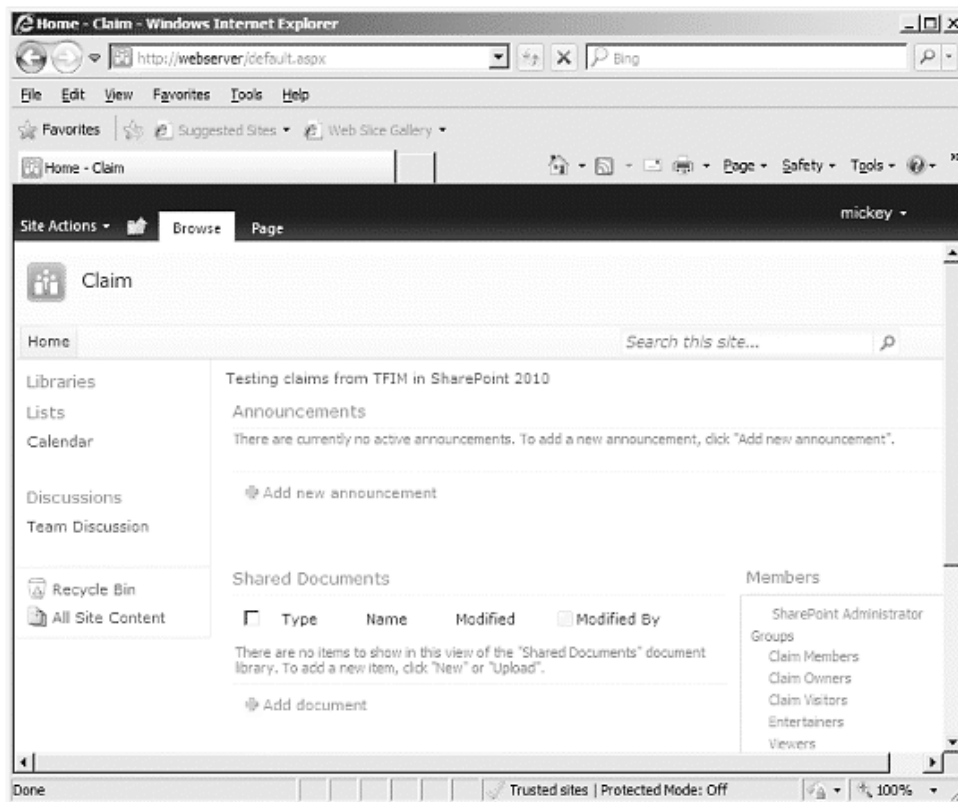
Log In

Done Internet | Protected Mode: Off 100%

4. IBM Security Identity Federation Manager constructs the SAML token and will redirect back to SharePoint.



5. SharePoint processes the SAML token and grants access.



Note: You might have to first authenticate to the site by using Windows Authentication and assign site permissions to a user or groups.

Known Issues

1. Sign out and sign in as a different user only signs the user out from SharePoint. It does not sign the user out of the trusted identity provider. Close the browser to ensure re-authentication.
2. The People Picker functionality does not resolve users or groups against the trusted identity provider. Authorization to SharePoint is based on the groups that are returned from the SAML token and processed as role claims.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. ©Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.



Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Other company, product, and service names may be trademarks or service marks of others.