

IBM® Security Federated Identity Manager
for Versions 6.2.2

IBM Security Federated Identity Manager for SharePoint Claims- based Authentication using SAML Integration Guide



Note

Before using this information and the product it supports, read the information in 'Notices' on page 22

This edition applies to Version 1.8 release i of the IBM Security Federated Identity Manager for SharePoint Claims-based Authentication using SAML and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2012, 2017.**

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

Contents

PREFACE.....	5
Access to publications and terminology	5
Publication Library.....	5
IBM Terminology website	6
Accessibility	6
Technical Training	6
Support information	7
Statement of Good Security Practices	7
Product name updates	7
INTRODUCING THE INTEGRATION	8
Introduction	8
Integration Architecture	8
Integration Product Version Information	9
Integration Product Contents	9
Before you start	9
IBM SECURITY FEDERATED IDENTITY MANAGER CONFIGURATION	10
Configuring the Federation Provider (IdP)	10
Configuring the Federation Service Partner (SP)	10
Federation Runtime Configuration	11
Configuring IBM Security Access Manager for Federations	11
SIGNING CERTIFICATE CONFIGURATION	12
Export the certificate from IBM Federated Identity Manager	12
Import the certificate into the Microsoft Certificate Store	12
Export the certificate from Microsoft Certificate Store	12
Import a token signing certificate into SharePoint using Windows PowerShell	13
Create a new trusted identity provider	13
SHAREPOINT WEB APPLICATION CONFIGURATION	15
Create the Site Collection for the SharePoint Web Application	15
Create the Site Collection for the SharePoint Web Application	16
TESTING THE INTEGRATION.....	18
Before you start	18

Security Access Manager for Web configuration.....	18
User Account Creation	18
Junction Management.....	18
Authenticating to Microsoft SharePoint	19
TROUBLESHOOTING	20
Collecting Support Data	20
Security Access Manager for Web trace	20
NOTICES	22
TRADEMARKS	24

Preface

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 Security Web Gateway Appliance Configuration Guide for Web Reverse Proxy*

Provides configuration procedures and technical reference information for the Web Gateway Appliance.

Integration Guide

- *IBM Security Web Gateway Appliance Web Reverse Proxy Stanza Reference*

Provides a complete stanza reference for the Web Gateway Appliance Web Reverse Proxy.

Mobile Information

- *IBM Security Access Manager for Mobile Administration Guide*

Describes how to manage, configure, and deploy an existing IBM Security Access Manager environment.

- *IBM Security Access Manager for Mobile Configuration Guide*

Explains how to complete the initial configuration of IBM Security Access Manager for Mobile.

Federation Information

- *IBM Security Federation Manager Installation Guide*

Describes how to manage, configure, and deploy an existing IBM Security Federated Identity Manager environment.

- *IBM Security Federation Manager Administration Guide*

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

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

This Federated Identity Redbook covers important aspects of using IBM Security integrated identity management architecture to build and deploy the IBM Security Federated Identity Manager and Web Services 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.

Introducing the Integration

Introduction

IBM Security Federated Identity Manager manages the generation of the SAML token that is used to perform single-sign-on (SSO). The user identity can be sourced from IBM Security Access Manager.

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

This integration pattern refers to IBM Security Access Manager as a Point of Contact for IBM Security Federated Identity Manager. This integration does not use IBM Security Access Manager as the web reverse proxy.

Integration Architecture

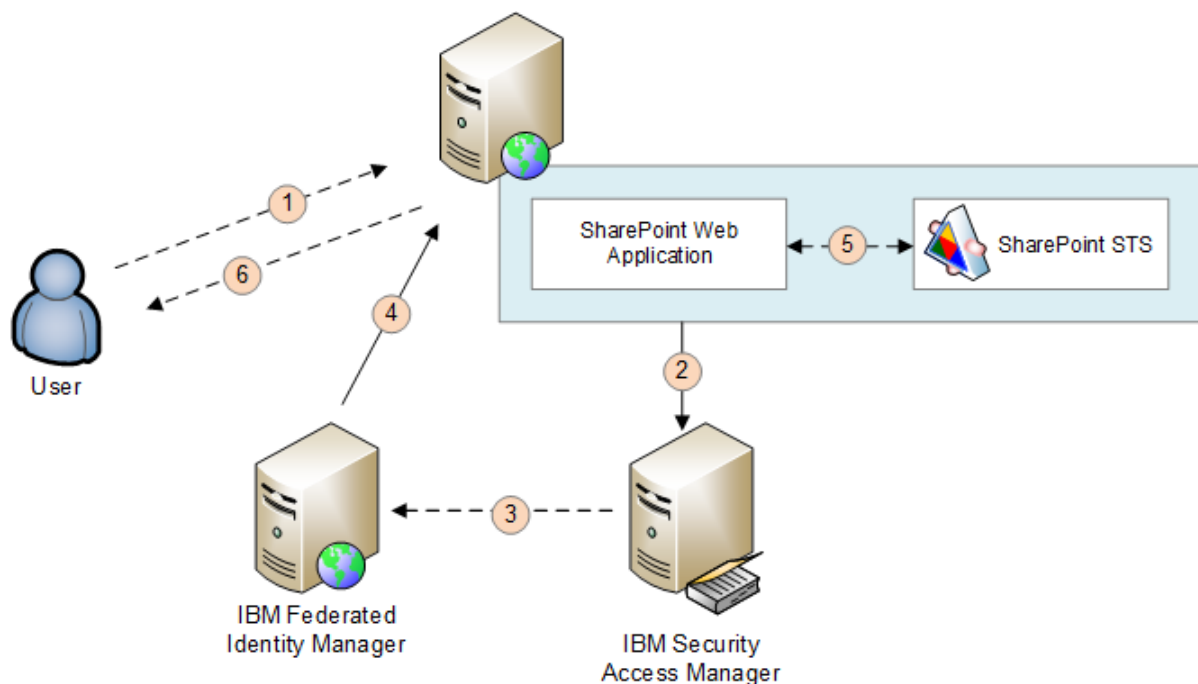


Figure 1: SAML sign-in sequence

1. The user requests content from a SharePoint web application.
2. SharePoint redirects the user to Security Access Manager acting as the Point of Contact for IBM Federated Identity Manager.
3. Security Access Manager for Web validates the user credentials against a directory service (LDAP) and routes the request to single sign-on protocol service (SPS) junction for IBM Federated Identity Manager.
4. IBM Federated Identity Manager invokes the federation and performs a POST of the SAML token to SharePoint
5. SharePoint validates the token and issues a claim-based token.

6. The response is sent back to the user; the FedAuth cookie is stored for subsequent requests.

Integration Product Version Information

See the Release Notes for supported versions.

Integration Product Contents

The integration solution is packaged as a compressed file. The package contains the following files:

File Name	Description
fim_saml_int_guide.pdf	This integration guide.
Samples\Microsoft SharePoint\FIM.SharePoint.Mapping.Rult.xslt	Example XSLT mapping rule to include additional claims into the SAML token.
Samples\Microsoft SharePoint\FIM.SharePoint.Trusted.Provider.ps1	Example Microsoft PowerShell file to creating the trusted identity provider in SharePoint.

Table 1: Integration Package contents

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:

- IBM Security Access Manager
 - IBM Security Access Manager for Web or WebSEAL
 - Reverse proxy instance created.
- IBM Federated Identity Manager
 - Deployed to a WebSphere Application Service
 - An IBM Federated Identity Manager domain is configured and the runtime deployed to the domain.
 - Point of Contact server is configured to Access Manager
- Microsoft SharePoint
 - Installed into a farm or single-instance environment.

IBM Security Federated Identity Manager Configuration

Configuring the Federation Provider (IdP)

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Configure Federated Single Sign-on**.
3. Select **Federations**
4. In the **Federations** section, click **Create...**
5. In the **General Information** section, enter a **Federation Name** and select **Identity Provider** role option. Click **Next**
6. In the **Contact Information** section, enter the **Company Name**. The remaining fields are optional. Click **Next**.
7. In the **Federation Protocol** section, select **WS-Federation Passive Profile**. Click **Next**.
8. In the **Point of Contact Server** section, enter the **URL** of the point of contact. If IBM Security Access Manager is being used, this is the URL of the /FIM junction on WebSEAL (For example <https://webseal.isam.com/FIM>). The /FIM junction is described in Configuring IBM Security Access Manager for Federations, refer *page 11*. Click **Next**.
9. In the **Token Module Instance** section, select **Default SAML 1.1 Token**. Click **Next**.
10. In the **Configure Security Token** section, update the **Amount of time the assertion is valid after being issued** as 120. Click **Next**.
11. In the **Identity Mapping Options**, select **Use XSLT or JavaScript transformation for identity mapping**. Click **Next**.
12. Browse to the XSLT mapping file in the Examples folder location. You may need to modify this file to represent any extended attributes configured in IBM Security Access Manager to be generated as claims in the SAML token to SharePoint. Click **Next**.
13. On the **Summary** page, click **Finish**.
14. Click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

Configuring the Federation Service Partner (SP)

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

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Configure Federated Single Sign-on**.
3. Select **Partners**
4. In the **Federation Partners** section, click **Create...**
5. In the **Contact Information** section, enter a name of the **Service Provider Company Name**. The remaining fields are optional. Click **Next**.
6. In the **WS-Federation Data** section, enter the **WS-Federation Realm** (For example urn:sharepoint:web).
7. In the **WS-Federation Data** section, enter the **WS-Federation Endpoint**. This value is the URL to the SharePoint hostname and port with /_trust/ appended (For example http://mysharepoint:8080/_trust/)
8. In the **WS-Federation Data** section, enter the **Maximum Request Lifetime** as -1. Click **Next**.
9. In the **Configure Security Token** section, select **Keystore**.
10. Enter the **Keystore** password (Default Keystore password is testonly). Click **List Keys**.
11. Select the **Alias** key to use. Click **Next**.
12. In the **Identity Mapping Options**, select **Use XSLT or JavaScript transformation for identity mapping**. Click **Next**.
13. Browse to the XSLT mapping file, this is optional. Click **Next**.
14. On the **Summary** page, click **Finish**.

15. Click **Enable Partner** if prompted.
16. Click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

Federation Runtime Configuration

Microsoft SharePoint does not support several SAML elements in the response from IBM Security Federation Manager. A runtime configuration property is provided to enable federations to SharePoint web applications.

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Domain Management**.
3. Select **Runtime Node Management**.
4. Click **Runtime Custom Properties**.
5. Click **Create...**
6. Enter the following Name and Value:
 - o Name: `WSFed.IDP.RSTR.Excluded.Elements%<FEDERATIONID>%<PARTNERID>`
 - o Value: `Forwardable, Delegatable, Status, Renewing`

Note: The **<FEDERATIONID>** placeholder is the WS-Federation Realm value in the federation configuration. The **<PARTNERID>** placeholder is the WS-Federation Realm in the partner configuration.

For example:

```
WSFed.IDP.RSTR.Excluded.Elements%http://webseal.isam8.com/FIM/sps/AccessManager/wsf%urn:sharepoint:web
```

7. Click **OK**
8. Click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

For more information on this runtime custom property, refer to:

<http://download4.boulder.ibm.com/sar/CMA/TIA/04w2e/0/6.2.2-TIV-TFIM-FP0012.README-notoc.html#IV31660-doc>

Configuring IBM Security Access Manager for Federations

IBM Security Federated Identity Manager provides a command line utility to assist with creating the standard /FIM junction in IBM Security Access Manager.

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Configure Federated Single Sign-on**.
3. Select **Federations**
4. Click **Download Tivoli Access Manager Configuration Tool**.
5. Save **tfimcfg.jar**.

For guidance on running the Tivoli Access Manager Configuration Tool, refer to:

https://www-304.ibm.com/support/knowledgecenter/SSZSXU_6.2.2.7/com.ibm.tivoli.fim.doc_6227/config/task/usin_gtfimcfgISAM7.html?lang=en

Signing Certificate Configuration

When setting up the trust between IBM Federated Identity Manager and SharePoint, we need to import a certificate used by IBM Federated Identity Manager. The certificate in IBM Federated Identity Manager cannot be exported in a format that can be imported directly into SharePoint, therefore we need to complete the following steps:

- Export the certificate from the IBM Federated Identity Manager Keystore.
- Import the certificate into the Microsoft Certificate Store.
- Export the certificate from the Microsoft Certificate Store

Export the certificate from IBM Federated Identity Manager

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Configure Key Service**.
3. Select **Keystores**.
4. Select the **Keystore Name** that containing the signing/encryption key.
5. Click **View Keys...**
6. Enter the **Keystore** password (Default Keystore password is testonly).
7. Select the **Alias** to export.
8. Click **Export...**
9. Select **PKCS#12** export format.
10. Click **Download Key**.
11. Save the file.

Import the certificate into the Microsoft Certificate Store

1. Locate the file from Export the certificate from IBM Federated Identity Manager *step 11*
2. Right click the file, click **Install PFX**.
3. The **Certificate Import Wizard** will appear, select **Current User** as the **Store Location**.
4. Click **Next**.
5. On the **File to Import** page, click **Next**.
6. Enter the **password** for the key, this will be the same password used to access the Keystore from IBM Federated Identity Manager (For example, testonly). Click **Next**.
7. Select location to store the certificate, click **Next**.
8. Click **Finish**.

Export the certificate from Microsoft Certificate Store

After importing the certificate into the Microsoft Certificate Store, we need to export in the format that can be read by SharePoint. The Microsoft Certificate Store is accessed through the Microsoft Management Console (MMC) snap-in.

1. From the Start Menu, select **Run**.
2. Type `mmc`, click **OK**
3. Select the **File** → **Add/Remove Snap-in...**
4. Select **Certificates**, then click **Add**.
5. The Certificate snap-in dialog will appear, select **My user account**, click **Finish**.
6. Click **OK**.
7. Under **Certificates – Current User**, expand **Trusted Root Certification Authority** → **Certificates**.
8. Select the certificate imported from Import the certificate into the Microsoft Certificate Store.
9. Right click the certificate **All Tasks** → **Export...**
10. The **Certificate Export Wizard** will appear, click **Next**.
11. Select the Export file format as **Base-64 encoded X.509 (.CER)**, click **Next**.

12. Enter a file name, click **Next**.
13. Click **Finish**.

Import a token signing certificate into SharePoint using Windows PowerShell

This section describes the process to import a token signing certificate to the trusted root authority list that resides on the SharePoint Server. This step must be repeated for every token signing certificate in the chain until the root certification authority is reached.

1. Copy the exported file from Export the certificate from Microsoft Certificate Store *step 13* to the SharePoint Server.
2. Open the SharePoint 2013 Management Shell in Administrator mode.
3. From the PowerShell command prompt, enter the following syntax:

```
$cert = New-Object  
System.Security.Cryptography.X509Certificates.X509Certificate2("<Path  
ToCert>")
```

```
New-SPTrustedRootAuthority -Name "IBM FIM Signing Cert" -Certificate  
$cert
```

Create a new trusted identity provider

Use the procedure in this section to create a new SPTrustedIdentityTokenIssuer.

1. Open the SharePoint 2013 Management Shell in Administrator mode.
2. From the PowerShell command prompt, enter the following syntax:

Certificate reference

```
$cert = New-Object  
System.Security.Cryptography.X509Certificates.X509Certificate2("<PathToCert  
>")
```

Claim mappings

The claim mappings are the incoming SAML token assertions mapped to SharePoint claims. The NameIdentifier claim represents the authenticated user name and is mapped to the user principal name (UPN) claim type.

```
$roleClaimMap = New-SPClaimTypeMapping -IncomingClaimType  
http://schemas.microsoft.com/ws/2008/06/identity/claims/role -  
IncomingClaimTypeDisplayName "Role" -SameAsIncoming
```

```
$userClaimMap = New-SPClaimTypeMapping -IncomingClaimType  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier -  
IncomingClaimTypeDisplayName "Username" -LocalClaimType  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
```

Federation parameters

```
$realm = "<realm>"
```

The **<realm>** placeholder is the WS-Federation Realm value entered in Configuring the Federation Service Partner (SP) refer *page 10*.

```
$signinURL = "http(s)://<pointOfContact>/FIM/sps/<federationName>/wsf"
```

The **<pointOfContact>** placeholder value is name of the IBM Security Access Manager reverse proxy (WebSEAL) server, refer to Configuring the Federation Provider (IdP), *page 10*.

The **<federationName>** placeholder value is the name of the identity provider, refer to Configuring the Federation Provider (IdP), *page 10*.

```
$trustedIdP = New-SPTrustedIdentityTokenIssuer -Name "IBM FIM" -Description  
"IBM Federated Identity Manager" -Realm $realm -SignInURL $signinURL -  
ClaimsMappings $roleClaimMap,$userClaimMap -IdentifierClaim  
$userClaimMap.InputClaimType -ImportTrustCertificate $cert
```

Token Expiration

The LogonTokenCacheExpirationWindow value for the SharePoint STS needs to be less than the SAML TokenLifetime value configured in the federation. To update the SharePoint STS, execute the following PowerShell.

1. Open the SharePoint 2013 Management Shell in Administrator mode.
2. From the PowerShell command prompt, enter the following syntax:

```
$sts = Get-SPSecurityTokenServiceConfig  
$sts.LogonTokenCacheExpirationWindow = (New-TimeSpan -minutes 1)  
$sts.Update()  
Iisreset
```

SharePoint Web Application Configuration

Create the Site Collection for the SharePoint Web Application

To use claims authentication, a web application must be created or configured using an account in the Farm Administrators SharePoint group.

1. On the Central Administration Home page, click **Application Management**.
2. In the **Application Management** page, in the **Web Applications** section, click **Manage web applications**.
3. In the **Contribute** group of the ribbon, click **New**.
4. On the **Create New Web Application** page, in the **IIS Web Site** section, you can configure the settings for your new web application by selection one of the following two options:
 - Click **Use an existing IIS web site**, and then select the web site on which to install your new web application
 - Click **Create a new IIS web site**, and then type the name of the web site in the Name box.
 - In the **Port** box, type the port number you want to use to access the web application. If you are using an existing web site, this field contains the current port number.
 - Optional: In the **IIS Web Site** section, in the **Host Header** box, type the host name (for example, www.mysharepoint.com) that you want to use to access the web application.
5. In the **Security Configuration** section, click **No** to **Allow Anonymous** and whether or not to Use Secure Sockets Layer (SSL).
6. In the **Claims Authentication Types** section, select the **Trust Identity provider** created from Create a new trusted identity provider *page 13*.
7. In the **Sign in Page URL** section, select **Default Sign In Page URL** to redirect users to a default sign-in web site for claims-based authentication.
8. In the **Public URL** section, type URL for the domain name for all sites that users will access in this web application. The Zone value is automatically set to **Default** for a new web application. You can change the zone when you extend a web application.
9. In the **Application Pool** section, click **Create a new application pool**.
10. The remaining sections can be left with the default values.
11. Click **OK** to create the new web application.

Create the Site Collection for the SharePoint Web Application

A site collection is made up of one top-level site and all sites below that have the same owner and share administrator settings. As shown in the following figure, it is the top level or hierarchy in a SharePoint 2013 web application.

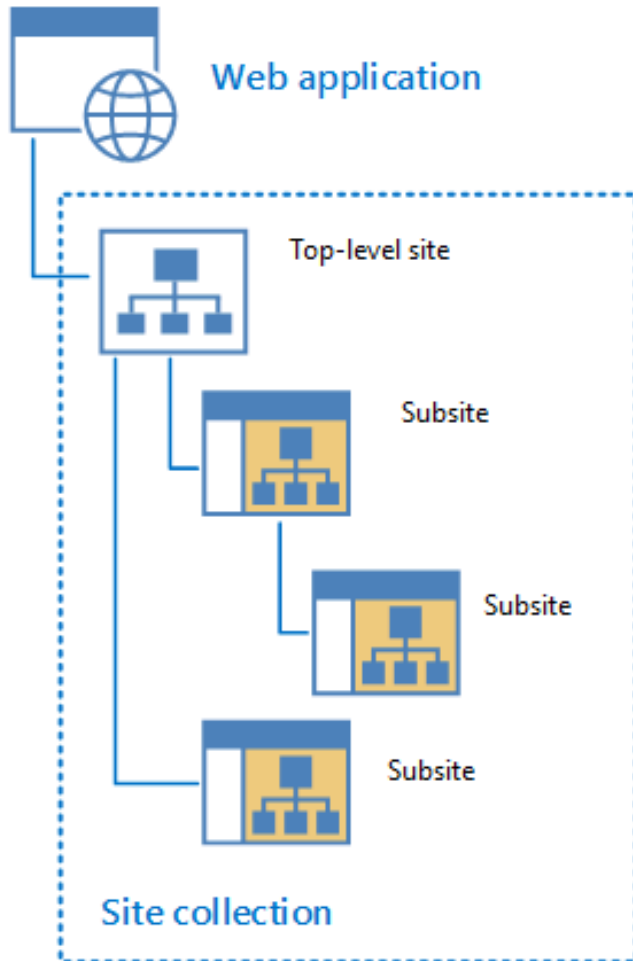


Figure 2: SharePoint 2013 site collection hierarchy

To create a site collection an existing web application is required and be a member of the Farm Administrators SharePoint group.

1. On the Central Administration Home page, click **Application Management**.
2. In the **Application Management** page, click **Create site collections**.
3. On the **Create Site Collections** page, click **Change Web Application** if the web application shown is not you want to create the site collection for.
4. In the **Title and Description** section, type the title and description for the site collection.
5. In the **Web Site Address** section, select the path to use for your URL (for example, a wildcard inclusion path such as /sites/, or the root directory (/).
6. In the **Template Selection** section, in the Select experience version list, select the SharePoint experience version of the templates that you want to use.
7. In the **Template Selection** section, in the Select a template list, select the template that you want to use for the top-level site in the site collection.

Integration Guide

8. In the **Primary Site Collection Administrator** section, type the user name for the user who will be the site collection administrator
9. In the **Secondary Site Collection Administrator** section, type the user name for the user who will be the site collection secondary administrator.
10. Click **OK**.

NOTE: After the site has been created, ensure that you share the site with a user from IBM Security Access Manager.

Testing the Integration

This sample uses Forms Based Authentication (FBA) to authenticate a user to IBM Security Access Manager WebSEAL.

Before you start

This section does not cover the configuration of the entire environment. It focuses on running a test scenarios and performing the configuration with sample values.

Security Access Manager for Web configuration

Install and configure a Security Access Manager for Web appliance:

1. When configuring the Runtime Component, use the **Embedded LDAP**.
2. Create a **Web Reverse Proxy instance**.
3. Configure **Forms Authentication**.

User Account Creation

Use **Policy Administration** or the `pdadmin` command-line utility to create user accounts for the tests. For example:

```
pdadmin sec_master> user create testuser1 uid=testuser1,dc=iswga Test
User1 password1
```

Existing user accounts can be used in the sample.

Junction Management

Use **Junction Management** or the `pdadmin` command-line utility to create a standard junction to the WebSphere Liberty Profile instance on the appliance. For example:

```
pdadmin sec_master> server list
<instance-name>-webseald-<webseal-host-name>

pdadmin sec_master> server task <instance-name>-webseald-<webseal-
hostname> create -t tcp -h localhost -p 80 -c iv-user /iis_sample
```

Replace `<instance-name>-webseald-<webseal-host-name>` with the value output from the first command.

Authenticating to Microsoft SharePoint

On a network connected computer:

1. Launch the **Browser**.
2. Navigate to `http(s)://<sharepointWebApp>:<port>`
3. The browser will redirect to the point of contact being IBM Access Manager.
4. Enter the IBM Access Manager credentials for the user.
 - a. Username: **testuser1**
 - b. Password: **password1**
5. IBM Access Manager forwards the request to IBM Federated Identity Manager and executes a POST to the SharePoint web application.

The expected response is the default web page for the SharePoint web application with the user name displayed in the top right corner.

Troubleshooting

Examine the troubleshooting and logging sections for help in resolving integration issues.

Collecting Support Data

To assist with resolution of a support issue, ensure you have collected and reviewed the trace for the components configured in this integration.

Also ensure that the support data has been collected from the IBM Security Access Manager appliance. Refer to:

http://www-01.ibm.com/support/knowledgecenter/SSELE6_8.0.1.3/com.ibm.isam.doc/admin/task/alps_managing_support_files.html

Security Access Manager for Web trace

pdweb.debug

The `pdweb.debug` trace will assist in identifying errors related to authentication to Security Access Manager and Microsoft Internet Information Services.

To enable tracing:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the `pdweb.debug` row.
6. Click **Edit**.
7. In the Edit Trace Component window:
 - a. Level: **2**
 - b. Flush Interval (seconds): **5**
 - c. Rollover Size (bytes): <default>
 - d. Click **Save**.

To disable trace, set the Level to 0.

To review the trace file generated:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the `pdweb.debug` row.
6. Click **Files**.
7. In the Manage Trace Files – `pdweb.debug` window
 - a. Select **pdweb.debug.log**
 - b. Click **View**
 - c. Number of lines to view: **1000** (depending on the number of requests)
 - d. Click **Reload**

The trace file may also be exported and viewed external to the appliance.

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
224A/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:

© IBM 2017. Portions of this code are derived from IBM Corp. Sample Programs. ©Copyright IBM Corp 2012, 2017. 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.