

IBM® Security Access Manager
for Versions 6.1.1, 7.0 and 8.0

IBM Security Access Manager for Microsoft ASP.NET Integration Guide



Note

Before using this information and the product it supports, read the information in 'Notices' on page 25

This edition applies to Version 1.8 release i of the IBM Security Access Manager for Microsoft ASP.NET and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2014, 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	6
Statement of Good Security Practices	6
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	10
Configuration an ASP.NET Web Application	10
Using PowerShell	10
Manually Editing Web.Config	10
Enabling a Machine Key for the Web Application	11
Membership Provider Implementation	12
Membership Provider Configuration Options	13
MembershipUser Attributes	13
Access Manager Sign-in Page	13
LDAP Binding	14
Extended Provider Attribute	15
Role Provider Implementation	16
Role Provider Configuration Options	17
Extended Provider Attribute	17
Additional Roles Attribute	17
Available Roles Attribute	17
IBM SECURITY ACCESS MANAGER CONFIGURATION	18
Web Gateway Appliance Configuration	18
Authentication Mechanism	18
Junction Management	18

WebSEAL Configuration	19
Authentication Mechanism	19
Junction Creation.....	19
TESTING THE INTEGRATION.....	20
Before you start	20
Security Access Manager for Web configuration.....	20
User Account Creation	20
Junction Management.....	20
LibraryDemo Sample Application	21
Importing the LibraryDemo.....	21
TROUBLESHOOTING	22
Collecting Support Data	22
Security Access Manager for Web trace	22
Tracing an ASP.NET Web Application.....	23
Remove the integration	23
Using PowerShell.....	23
Manually Editing Web.Config.....	24
NOTICES	25
TRADEMARKS	27

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.

- *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.

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

This guide provides instructions on how to configure Microsoft .NET Framework Role and Membership providers for Microsoft ASP.NET web applications to enable single sign-on and role-based access control.

The implementation of the role and membership provider is based on HTTP request headers that IBM Security Access Manager WebSEAL sends to provide runtime security.

Integration Architecture

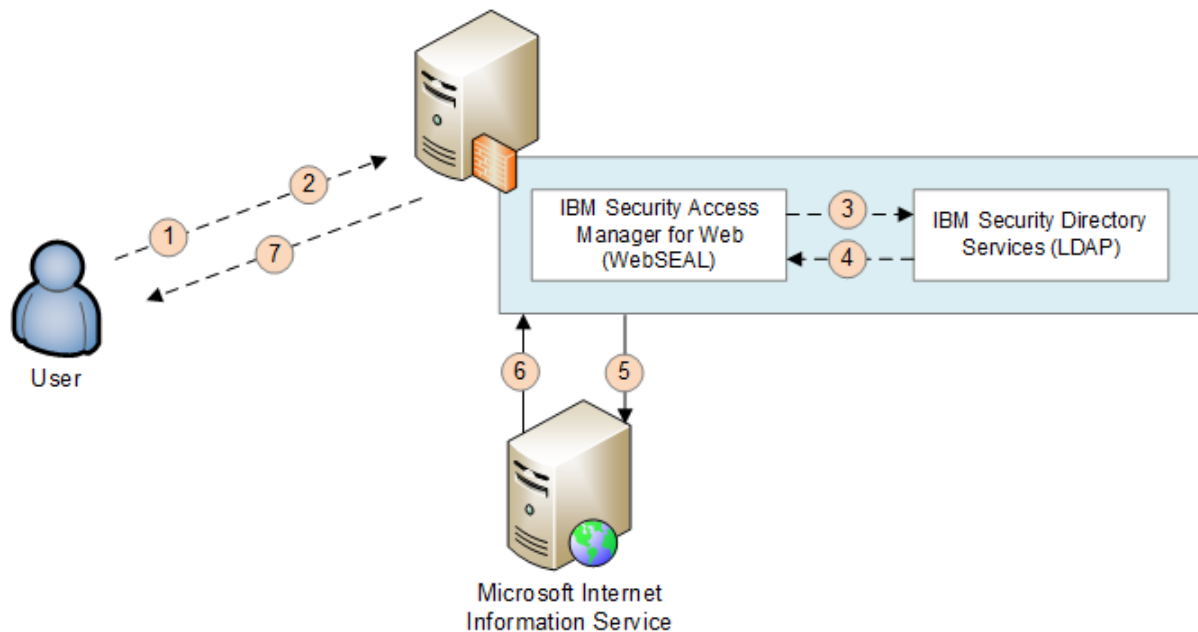


Figure 1: IBM Security Access Manager with IIS

IBM Security Access Manager for Microsoft ASP.NET shows the integration architecture with the following process for Single Sign:

1. The user requests content from a protected ASP.NET web application hosted on Microsoft Internet Information Services (IIS).
2. Security Access Manager for Web detects the request from the user and sends a response for the user credentials. The user enters credentials.
3. Security Access Manager for Web validates the user credentials against a directory service (LDAP).
4. If the authentication succeeds, the authenticated user and associated attributes are provided to Security Access Manager for Web.
5. Security Access Manager for Web injects the user identity information into the request header and forwards the request to the ASP.NET web application via a configured junction.

6. The web site configured with the role and membership provider creates a session for the user, the requested content is passed back through Access Manager for Web.
7. Access Manager for Web passes the response back to the user.

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
Am_aspnet_int_guide.pdf	This integration guide.
Solutions\Microsoft ASP.NET\IBM.Security.Web.ApplicationServices.dll	This file provides role and membership functionality for ASP.NET web applications.
Solutions\Microsoft ASP.NET\AccessManagerSignin.aspx	This is a ASP.NET web page that is used to perform the single sign-on from IBM Security Access Manager.
Solutions\Microsoft ASP.NET\Isam.ASPNET.Deploy.ps1	This is a PowerShell command to install or uninstall the role and membership provider.
Solution\Microsoft ASP.NET\IBM.Security.Web.AuthenticationManagement.dll	This file is used by Microsoft Internet Information Services to read and write configuration changes to the web site using the native module.
Solution\Microsoft ASP.NET\web.config	A template web.config for an ASP.NET web application.
Samples\Microsoft ASP.NET\Library_Demo	An example ASP.NET web application that demonstrates the user of the role and membership provider and the extended provider capability.

Table 1: Integration Package contents

Before you start

The impersonation module and associated Microsoft Internet Information Services components require the following pre-installed operating system environments. Refer to the release notes for platform support.

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
- Web Server (Microsoft Internet Information Services) role installed with the following features;
 - Health and diagnostics
 - Security
 - Application development
 - Microsoft ASP.NET Configuration

Configuration an ASP.NET Web Application

Using PowerShell

After you extract the compressed file, open a command prompt in Administrator mode. The PowerShell command updates the web.config for a web application adding the role and membership provider's stanzas, the authentication stanza and placeholder stanza for additional LDAP operations.

1. At the command prompt, navigate to the folder location of the extracted files.
2. Type `PowerShell`
3. Type `.\isam.aspnet.deploy.ps1`
4. Type `execute -action install -path <locationOfWebConfig> -assemblyLocation gac | bin`

Note: The `assemblyLocation` parameter is used to resolve the assembly version information. The PowerShell command does not install the assembly into the Global Assembly Cache (GAC). To install an assembly into the GAC, refer to:

[https://msdn.microsoft.com/en-us/library/ex0ss12c\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ex0ss12c(v=vs.110).aspx)

Manually Editing Web.Config

1. Copy the `IBM.Security.Web.ApplicationServices.dll` to the web application `bin` folder or copy the assembly into the Global Assembly Cache (GAC).
2. Open the **web.config** file of the ASP.NET web application.
3. Find the **<configSection>** stanza and add the following:

```
<section name="accessManager"
  type="IBM.Security.Web.AccessManagerSection,
  IBM.Security.Web.ApplicationServices, Version=x.x.x.x,
  Culture=neutral, PublicKeyToken=b77a5c561934e089" />
```

4. After **</configSection>**, add the following stanza:

```
<accessManager>
  <ldapBinding enabled="false"
    trustedUsername=""
```

```

        password=""
        address=""
        prefix=""
        suffix=""
        ssl="false"
        startSearchDN=""
        userSearchObjectContainer=""
        userAttributeKey=""
        groupSearchObjectContainer=""/>
    <signinPage disablePostBackQueryString=""
        postbackDelay="0" />
</accessManager>

```

- Find the **<authentication>** stanza and modify the mode attribute is "Forms". Then add the following:

```
<forms loginUrl="AccessManagerSignin.aspx" .../>
```

- Find the **<membership>** stanza and add the following:

```

<add applicationName="your application name"
    name="AccessManagerMembershipProvider"
    type="IBM.Security.Web.AccessManagerMembershipProvider,
    IBM.Security.Web.ApplicationServices, Version=x.x.x.x"
    userName="iv-user" />

```

- Update the attribute `defaultProvider="AccessManagerMembershipProvider"` for the **<membership>** stanza.

- (Optional) Find the **<roleManager>** stanza and add the following:

```

<add applicationName="your application name"
    name="AccessManagerRoleProvider"
    type="IBM.Security.Web.AccessManagerRoleProvider,
    IBM.Security.Web.ApplicationServices, Version=x.x.x.x"
    userName="iv-user" groupName="iv-groups"/>

```

- If the above step was configured, update the attribute `defaultProvider="AccessManagerRoleProvider"` for the **< roleManager >** stanza.

Enabling a Machine Key for the Web Application

The membership provider uses the local machine key as an authentication password to provide a secure user logon.

- Open Internet Information Services (IIS) Manager.
- Expand the node labeled as the machine name.
- Expand the node labeled **Sites**.
- Select the web application.
- Select the **Machine Key** applet.
- Click **Open Feature** from the Action pane on the right.
- Click **Generate Keys** from the Action pane on the right.
- Click **Apply** from the Action pane on the right to store the keys in the web.config file for the web application.

Membership Provider Implementation

The following table summarizes the direct or pass-through implementation of properties and methods in the Membership provider.

To enable the full functionality of the providers, a feature called pass-through is implemented. Pass-through invokes the property or methods on another configured membership provider for the web application. This functionality is configured using the **extendedProviderName** property within the configuration of the Membership provider.

	Name	Implemented?	Pass-through?
	ChangePassword	No	Yes
	ChangePasswordQuestionAndAnswer	No	Yes
	CreateUser	No	Yes
	DeleteUser	No	Yes
	FindUsersByEmail	Yes with LDAP bind	Yes
	FindUsersByName	Yes with LDAP bind	Yes
	GetAllUsers	No	Yes
	GetNumberOfUsersOnline	No	Yes
	GetPassword	No	Yes
	GetUser(Object, Boolean)	Yes	Yes
	GetUser(String, Boolean)	Yes	Yes
	GetUserNameByEmail	Limited	Yes
	Initialize	Yes	N/A
	ResetPassword	No	Yes
	UnlockUser	No	Yes
	UpdateUser	No	Yes
	ValidateUser	Yes	Yes
	ApplicationName	Yes	No
	Description	Yes	No
	EnablePasswordReset	No	Yes
	EnablePasswordRetrieval	No	Yes
	MaxInvalidPasswordAttempts	No	Yes
	MinRequiredNonAlphanumericCharacters	No	Yes
	MinRequiredPasswordLength	No	Yes
	Name	Yes	No
	PasswordAttemptWindow	No	Yes
	PasswordFormat	No	Yes
	PasswordStringRegularExpression	No	Yes
	RequiresQuestionAndAnswer	No	Yes
	RequiresUniqueEmail	No	Yes
	ExtendedProviderName (string) Name of the membership provider for pass-through functionality.	Yes	N/A
	UserNameHeader (string) Name of the HTTP header that represents the user name.	Yes	N/A

Table 2: Membership Provider implemented functionality

Membership Provider Configuration Options

MembershipUser Attributes

The membership provider can contain additional attributes that populate a MembershipUser object. The attribute names must match the public property names of the MembershipUser object. Refer to Microsoft MSDN.

[http://msdn.microsoft.com/en-us/library/system.web.security.membershipuser\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/system.web.security.membershipuser(v=vs.110).aspx)

WebSEAL inserts the membership user attributes by configuring the **HTTP-Tag-Values** attributes. See the following reference for more information on how a custom and named header values can be inserted by WebSEAL.

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc_6.1/am61_webseal_admin314.htm - ext-attr-header

The following example demonstrates a subset of the available attributes of the MembershipUser.

```
<add applicationName="your application name"
  name="AccessManagerMembershipProvider"
  type="IBM.Security.Web.AccessManagerMembershipProvider,
  IBM.Security.Web.ApplicationServices, Version=x.x.x.x"
  userName="iv-user"
  email="user-email_http_header"
  comment="comment_http_header"
  creationDate="user-created_http_header"/>
```

Access Manager Sign-in Page

Use the **AccessManagerSignin.aspx** page to enable ASP.NET applications to single sign-on. The **AccessManagerSignin.aspx** page provides a user experience that can be customized to suit the theme of the web application. See the **<signinPage>** element of the **<accessManager>** stanza.

The following table describes the attributes for overriding the default sign-in behaviour.

Name	Description	Example
DisablePostBackQueryString	A query string value that is evaluated during the page processing to bypass the sign-in page from rendering and invoking a postback to the browser.	Ctx=ws
PostBackDelay	A timer delay before the sign-in page executes a postback. The value is represented in seconds	5

Table 3: Access Manager Sign-in Page configuration options

See the following example of the Access Manager Sign-in Page stanza:

```
<accessManager>
  <signinPage disablePostBackQueryString=ctx=ws" postbackDelay="3" />
</accessManager>
```

Customizing the Access Manager Sign-in Page

The **AccessManagerSignin.aspx** page can be substituted with a custom designed ASPX page. To maintain the single sign-in experience, the ASPX page must:

- Inherit from `IBM.Security.Web.AccessManagerSignin`. For Example:

```
<%@ Page Language="C#"
Inherits="IBM.Security.Web.AccessManagerSignin" %>
```
- Contain two (2) web controls:
 - An image control named "progress". For example:

```
<img runat="server" id="progress" />
```
 - A div control named "status". For example:

```
<div runat="server" id="status"/>
```

NOTE: Update the attribute `loginUrl="NewSigninPage.aspx"` in the `<forms>` stanza of the web.config for the web application.

LDAP Binding

The membership provider enables additional security validation and search functionality using the LDAP binding settings in `<ldapBinding>` element of the `<accessManager>` stanza. The following table describes the attributes for LDAP binding.

Name	Description	Example
TrustedUserName	The name that is used to authenticate to the LDAP server. The trusted user name and password is contained in the authorization HTTP header from IBM Security Access Manager. WebSEAL insert this header using the <code>-b</code> supply junction option. Refer to Handling client identity information across junctions: https://publib.boulder.ibm.com/tividd/td/I_TAME/SC32-1134-01/en_US/HTML/amweb41_admin14.htm	ldap_readonly_user
Address	The host or IP address of the LDAP server.	ldap.server.com:389
Suffix	A distinguished name (DN) that identifies the top entry in the directory hierarchy,	o=ibm,c=us
Prefix	The LDAP prefix to add to the user name to form the DN.	cn=
Enabled	A flag to enable the LDAP binding.	True or False
Password	Used for performing LDAP search functionality.	passwOrd
SSL	A flag to enable secure sockets layer communication to the LDAP server. Used for performing LDAP search functionality.	True or False

StartSearchDN	The distinguished name of the object to start the search	secAuthority=Default
UserSearchObjectContainer	The object container for performing user based search. The search criteria can match against multiple LDAP attributes as shown in the example.	(&(objectClass=ePerson)(({0}={1})(sn={1})(mail={1}))) At runtime the {0} placeholder is substituted with the value of the UserAttributeKey. The {1} placeholder represents the search criteria provided by the membership provider.
GroupSearchObjectContainer	The object container for performing group based search. As shown in the example, an * has been appended to enable partial search criteria.	(&(objectClass=secGroup)(cn={0}*)) At runtime the {0} placeholder is substituted with the search criteria from the role provider.
UserAttributeKey	The LDAP attribute name to search against.	cn

Table 4: LDAP binding and search attributes

See the following example of the LDAP bind stanza:

```
<accessManager>
<ldapBinding userAttributeKey="cn"
userSearchObjectContainer="(&(objectClass=ePerson)(|({0}={1})(sn={1})(mail={1})))"
groupSearchObjectContainer="(&(objectClass=secGroup)(cn={0}*))"
startSearchDN="secAuthority=Default"
trustedUsername="ldap_readonly_user"
password="passw0rd"
ssl="false"
address="192.168.0.1:389"
suffix="secAuthority=Default"
prefix="cn="
enabled="true" />
</accessManager>
```

Extended Provider Attribute

Use the extended provider attribute to forward the membership provider functionality to another configured membership provider that is listed in the **<membership>** stanza of the web.config file. The following configuration example demonstrates how this attribute is configured referencing the `AspNetSqlMembershipProvider`.

```
<add applicationName="your application name"
    name="AccessManagerMembershipProvider"
    type="IBM.Security.Web.AccessManagerMembershipProvider,
    IBM.Security.Web.ApplicationServices, Version=x.x.x.x"
    userName="iv-user"
    extendedProvider="AspNetSqlMembershipProvider"/>
```

Role Provider Implementation

The following table summarizes the direct or pass-through implementation of properties and methods in the Role provider.

To enable the full functionality of the providers, a feature called pass-through is implemented. Pass-through invokes the property or methods on another configured membership provider for the web application. This functionality is configured using the **extendedProviderName** property within the configuration of the Role provider.

	Name	Implemented?	Pass-through?
	AddUsersToRoles	No	Yes
	CreateRole	No	Yes
	DeleteRole	No	Yes
	FindUsersInRole	No	Yes
	GetAllRoles	Yes based on the HTTP header and AvailableRoles property	Yes
	GetRolesForUser	Yes based on the HTTP header and AvailableRoles property	Yes
	GetUsersInRole	No	Yes
	RemoveUsersFromRoles	No	Yes
	RoleExists	Yes	Yes
	ApplicationName	Yes	No
	AvailableRoles (string[]) An Array of strings representing roles creating in role provider configuration.	Yes	N/A
	Description	Yes	No
	ExtendedProviderName (string) Name of the membership provider for pass-through functionality.	Yes	N/A
	GroupNameHeader (string) Name of the HTTP header that represents the group name.	Yes	N/A
	Name	Yes	No
	UserNameHeader (string) Name of the HTTP header that represents the user name.	Yes	N/A
	RolesDefaultResult (bool) Default action is no role authorities are found.	Yes	N/A

Role Provider Configuration Options

The purpose of the role provider is to map the user group information from WebSEAL into role based authorization in an ASP.NET web application.

Extended Provider Attribute

Use the extended provider attribute to delegate the IBM Security Access Manager role provider functionality to another role provider, which is listed in the **<roleManager>** stanza of the web.config file for all Administrative functions of the provider interface. The following configuration example demonstrates how this attribute is configured.

```
<add applicationName="your application name"
    name="AccessManagerRoleProvider"
    type="IBM.Security.Web.AccessManagerRoleProvider,
    IBM.Security.Web.ApplicationServices, Version=x.x.x.x"
    userName="iv-user"
    groupName="iv-groups"
    extendedProvider="AspNetSqlRoleProvider"/>
```

Additional Roles Attribute

Use the additional roles attribute, to enable a web application to maintain a static list of roles, which can be used for user authorization. The following configuration example demonstrates how this attribute is configured:

```
<add applicationName="your application name"
    name="AccessManagerRoleProvider"
    type="IBM.Security.Web.AccessManagerRoleProvider,
    IBM.Security.Web.ApplicationServices, Version=x.x.x.x"
    userName="iv-user"
    groupName="iv-groups"
    additionalRoles="Guest,Manager,Administrator" />
```

Available Roles Attribute

During administration, only the runtime HTTP request headers for the currently logged in user is available. As such, calls to **GetAllRoles** return only a limited set. As a workaround for this limitation, use the configuration element **availableRoles**.

This configuration element provides a mechanism to manually specify all of the system roles so that they can be selected when configuring permissions. The list of **availableRoles** is added to the roles that are extracted from the currently logged in user. As such, ensure that an administrator account used to manage permissions, is provisioned with all the system roles that you need to assign or manage.

NOTE: When you specify the **availableRoles** or the **extendedProviderName** configuration, the default action for **IsUserInRole** and **RoleExists** is disabled.

IBM Security Access Manager Configuration

Complete the following configuration steps on Web Gateway Appliance or WebSEAL for integration with IBM Security Access Manager for Microsoft ASP.NET.

The **pdadmin** command-line utility can be used on the Web Gateway Appliance in addition to the graphical user interface of the Local Management Interface (LMI) for some of the integration steps.

Web Gateway Appliance Configuration

Complete the configuration steps on the IBM Security Access Manager for Web appliance to enable Single Sign On from the Mobile Enterprise Gateway.

Authentication Mechanism

The IBM Security Access Manager for Web Reverse Proxy instance must be configured to accept the authentication from the user.

In this example, the user is redirected to pkmslogin form for authentication to Microsoft ASP.NET WebSEAL:

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 **Edit**.
5. Select the **Authentication** tab.
6. Under **Forms Authentication** → **Transport**, select **Both**.
7. Click **Save**.
8. Deploy the pending changes.
9. Restart the reverse proxy instance.

Junction Management

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center Junctions](#) page for details of each junction type.

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** → **Junction Management**.
5. Click **New** → **Standard Junction**.
6. Enter a **Junction Point Name** and select a **Junction Type**.
7. Select the **Servers** tab,
8. Click **New**.
9. Enter a **Hostname**, **Port** and select a **Local Address**. This is the address WebSEAL is hosted on.
10. Click **Save**.
11. Select the **Identity** tab.

12. Check **IV-USER** and **IV-GROUPS**. These are the headers used to identity the user and groups.
13. Click **Save**.
14. Deploy the pending changes.
15. Restart the reverse proxy instance.

WebSEAL Configuration

Complete the configuration steps on the IBM Security Access Manager WebSEAL server to enable user authentication in IBM Security Access Manager.

Authentication Mechanism

The IBM Security Access Manager WebSEAL instance must be configured to supply the authenticated user identity into a request header forwarded to Microsoft Internet Information Services.

The WebSEAL instance can be configured for Forms Authentication or Basic Authentication, both authentication mechanism pass the IV-USER and IV-GROUP request headers to the backend.

Junction Creation

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center Standard WebSEAL junctions](#) and [IBM Security Access Manager Knowledge Center Virtual Hosting](#) pages for details of each junction type.

Once authenticated to Security Access Manager WebSEAL, downstream SSO to protected resources is achieved using a broad range of authentication mechanisms including existing Single Sign On patterns and integration adapters such as Trust Association Interceptor (TAI), Lightweight Third-Party Authentication (LTPA), Basic Authentication (GSO, -B, etc.), HTTP header (Kerberos, iv-creds, etc.) and Federation (using Tivoli Federated Identity Manager).

Testing the Integration

This sample uses Forms Based Authentication (FBA) to authenticate a user to IBM Security Access Manager WebSEAL. The user identity is forwarded to the web application via the request header IV-USER.

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** for the *Authentication Mechanism* on page 18.

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.

LibraryDemo Sample Application

The LibraryDemo is pre-configured with the ASP.NET web application that demonstrates role and membership providers, custom sign-in page, and extended role and membership providers.

Importing the LibraryDemo

1. Open Internet Information Services (IIS) Manager.
2. Select the web application under the **Sites** node.
3. Click **Import Application** from the **Actions** pane.
4. In the Import Package wizard, browse to the LibraryDemo.zip, then click **Next**.
5. Follow the wizard to complete the import.

Note: Microsoft Web Deploy 2.0 must be installed to import packages into the Internet Information Service.

On a network connected computer:

1. Launch the **Browser**.
2. Navigate to **Error! Hyperlink reference not valid.>**

The <junction> placeholder was created in Junction Management on *page 18*.

3. Enter the IBM Access Manager credentials for the user.
 - a. Username: **testuser1**
 - b. Password: **password1**

The expected response is the default Library demo web page for the web application on Microsoft Internet Information Service.

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.

Tracing an ASP.NET Web Application

To provide a consistent integration with existing ASP.NET trace reporting, both the Membership and Role Provider creates and sends trace messages to a custom TraceSource.

To retrieve trace messages, you must manually configure the **<system.diagnostics>** entry in web application utilising the providers. You can customize the level at which the switch can send to the listener. You can also configure which listener sends the trace (text file, Windows Event Log, XML, etc.). See the following configuration example for Tracing configuration.

```
<system.diagnostics>
  <trace autoFlush="true"/>
  <sources>
    <source name="AccessManagerTraceSource"
      switchName="AccessManagerTraceSource"
      switchType="System.Diagnostics.SourceSwitch">
      <listeners>
        <add name="AccessManagerTraceSource"/>
      </listeners>
    </source>
  </sources>
  <switches>
    <add name="AccessManagerTraceSource" value="Verbose"/>
  </switches>
  <sharedListeners>
    <add name="AccessManagerTraceSource"
      type="System.Diagnostics.TextWriterTraceListener"
      initializeData="IsamHttpProviders.log"/>
  </sharedListeners>
</system.diagnostics>
```

Remove the integration

Using PowerShell

Any ASP .NET web application that is configured with the Isam.ASPNET.Deploy.ps1 PowerShell script can be unconfigured to its previous state from the backup web.config file created during installation.

To complete the uninstallation, take the following steps:

1. At the command prompt, navigate to the folder location of the extracted files.
2. Type PowerShell
3. Type `.\isam.aspnet.deploy.ps1`
4. Type `execute -action uninstall -path <locationOfWebConfig> -assemblyLocation gac | bin`

Manually Editing Web.Config

To remove the integration from an ASP.NET web application:

1. Remove the affected `<membership>` stanza.
2. Remove the affected `<roleManager>` stanza.
3. Remove the `<section name=accessManager" ... .. />` stanza from the `<configSection>` of the web.config file.
4. Remove the `<accessManager>` stanza.
5. Replace `AccessManagerSignin.aspx` with an updated aspx page in the `<forms>` stanza.
6. Remove the Trace elements for the role and membership provider from the `<system.diagnostics>` stanza.
7. Remove the `IBM.Security.Web.ApplicationServices.dll` from the web application `\bin` folder.

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 2014, 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.