

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

***Microsoft ASP.Net 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 Security Access Manager for Microsoft Applications and to all subsequent releases and modifications until otherwise indicated in new editions.

**Copyright International Business Machines Corporation 2012, 2014.**

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

# Contents

Preface.....	5
About this publication .....	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 .....	7
Product name updates.....	7
Chapter 1: Introducing the integration .....	8
Introduction .....	8
Integration product version information .....	9
Integration product contents.....	10
Network connectivity considerations .....	10
Chapter 2: Integration process .....	11
Before you start .....	11
Configure a WebSEAL Junction using pdadmin.....	11
Configure a WebSEAL Junction using Web Gateway Appliance .....	12
Microsoft Internet Information Server (IIS).....	13
Configure an ASP.NET Web Application .....	13
Configuring with Isam.ASPNET.Deploy.ps1 .....	14
Enabling a Machine Key for the Web Application .....	15
Membership Provider Implementation.....	16
Membership Provider Configuration Options.....	17
MembershipUser Attributes.....	17
Access Manager Signin Page .....	18
Customising the Signin Page.....	19
LDAP Binding .....	19

Extended Provider Attribute .....	20
Role Provider Implementation .....	21
Role Provider Configuration Options .....	22
Additional Roles Attribute .....	22
Available Roles Attribute.....	22
Extended Provider Attribute .....	22
Tracing an ASP.NET Web Application.....	23
Chapter 3: LibraryDemo Sample Application .....	24
Importing the LibraryDemo .....	24
Chapter 4: Removing the integration.....	26
Manually configured ASP .NET web applications.....	26
Using Isam.ASPNET.Deploy.ps1 .....	26
Notices .....	27
Trademarks .....	29

# Preface

## About this publication

This guide provides the integration steps that are required to achieve single sign-on and role-based access control between the IBM Security Access Manager and Microsoft ASP.NET web applications.

## 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.

## **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

## Introduction

This guide provides instructions on how to configure 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 providers is based on the request HTTP headers that IBM Security Access Manager WebSEAL sends to provide runtime security. The administrative functions available on the Microsoft Providers interface can be delegated to another provider using a plugin point in the IBM Security Access Manager providers.

The following figure provides an overview of the integration between IBM Security Access Manager and an ASP.NET web application.

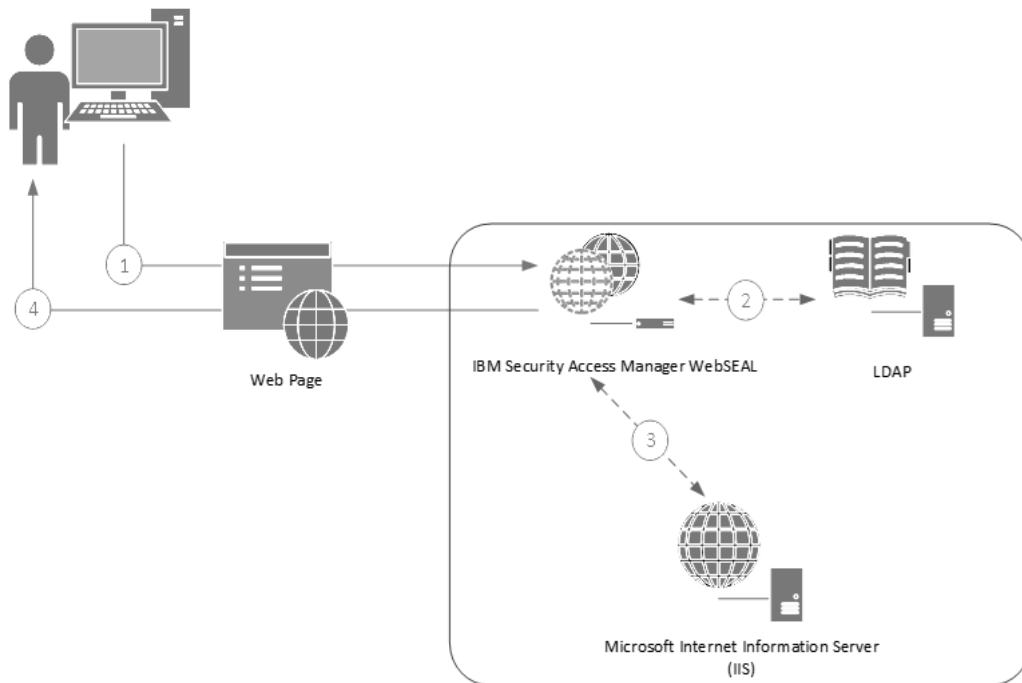


Figure 1. IBM Security Access Manager with IIS

The process flow that is shown in Figure 1 is as follows:

1. The user makes a request to the ASP.NET application and is prompted to authenticate to WebSEAL.
2. The user credentials are verified in the LDAP repository.
3. The request is forwarded to the ASP.NET application, which is configured for the WebSEAL junction; passing the iv-user and optional iv-groups.
4. The IBM Security Access Manager login page configured in the ASP.NET Web application authenticates the iv-user to the membership provider and optionally provides the iv-groups to assign roles in the role provider.

**NOTE:** An optional Directory Bind can be configured as part of the ASP.NET forms login process to establish trust between the WebSEAL server and IIS server in the same way to a Trust Association Interceptor (TAI).

## **Integration product version information**

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

## Integration product contents

The integration solution is packaged as a compressed file, which contains the following files:

File name	Description
Documents\Microsoft ASP.NET\am_aspnet_guide.pdf	The integration guide for configuring IBM Security Access Manager with Microsoft ASP.NET web applications.
Solutions\Microsoft ASP.NET\IBM.Security.Web.ApplicationServices.dll	This file provides role and membership support in ASP.NET applications
Solutions\Microsoft ASP.NET\AccessManagerSignin.aspx	This is an ASP.NET web page that is used to perform 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.
Solutions\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 use of the role and membership provider and the extended provider capability.

## 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

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

- Configure a WebSEAL Junction using **pdadmin**.
- Configure a WebSEAL Junction using Web Gateway Appliance.

## Configure a WebSEAL Junction using pdadmin

1. Login into the **pdadmin** tool in a command\terminal window.
2. Enter the following syntax to create a junction at the **pdadmin** prompt.

```
pdadmin> server task <webseal instance> virtualhost create  
-t tcp -h <iis server> -p <asp.net web app port>  
-c iv-user,iv-groups <junction name>
```

Substitute the <placeholder> values. For example:

```
pdadmin> server task default-webseald-com virtualhost create  
-t tcp -h webserver.domain.com -p 80  
-c iv-user,iv-groups sso2aspnet
```

**NOTE:** If the ASP.NET web application is configured on a port other than port 80, modify the WebSEAL instance configuration file to add a network interface. The default WebSEAL port is 80. For example:

```
[interfaces]  
interfacel = network-interface=<webseal ip address>;http-port=<asp.net  
web app port>
```

## Configure a WebSEAL Junction using Web Gateway Appliance

1. Open the Web console of the Web Gateway Appliance.
2. Select **Secure Reverse Proxy Settings -> Reverse Proxy**.
3. Select the preferred instance.
4. Select **Manage -> Junction Management**.
5. Select **New -> Virtual Junction**.
6. On the **Junction** tab, specify the following information:
  - For **Junction Point Name**, enter `<junction name>`.
  - For **Junction Type**, select TCP.
7. On the **Servers** tab:
  1. Click **New**.
  2. Specify the following information :
    - Host name: `<iis server>`
    - TCP or SSL Port: `<asp.net web app port>`
  3. Click **Save** and close the junction dialog.

See the *IBM Security Access Manager WebSEAL Administrator Guide* for more configuration information.

# Microsoft Internet Information Server (IIS)

## Configure an ASP.NET Web Application

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. Edit the `web.config` file of the ASP.NET web application.
3. Find the `<configSection>` and add the following stanza:

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

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

```
<accessManager>
  <ldapBindind trustedUsername=""
    address=""
    suffix=""
    prefix=""
    enabled="false"/>
  <signinPage disablePostBackQueryString="" postbackDelay="" />
</accessManager>
```

5. Find the `<authentication>` stanza and ensure that the attribute `mode` value is "Forms". Then, add the following line:

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

6. Find the `<provider>` element under the `<membership>` stanza. Add the following provider:

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

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

8. [Optional] Find the `<provider>` element under the `<roleManager>` stanza. Add the following provider:

```
<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"/>
```

9. If you added the role provider, update the attribute `defaultProvider="AccessManagerRoleProvider"` for the `<roleManager>` stanza.

10. Save the web.config file.

**NOTE:** Replace the version with the assembly version.

## Configuring with Isam.ASPNET.Deploy.ps1

The configuration of an ASP .NET web application can be simplified by using the Isam.ASPNET.Deploy.ps1 PowerShell script in the IBM Security Access Manager for Microsoft Applications package.

The Isam.ASPNET.Deploy.ps1 script:

- Inserts the relevant stanzas for the application into the ASP .NET web.config as described in Configure an ASP.NET Web Application
- Backs up the existing web.config to a file called web.config.ibm. The web.config can be restored to its previous state by uninstalling it as described in Using Isam.ASPNET.Deploy.ps1.

To configure a web application with Isam.ASPNET.Deploy.ps1:

1. Open the command prompt and navigate to the folder location of the extracted IBM Security Access Manager for Microsoft Applications files.
2. Type `PowerShell`.
3. Type `.\Isam.ASPNET.Deploy.ps1`.
4. Type `Execute -action install -path <location of web.config> -assemblyLocation gac | bin`

Example usage for an application with assembly deployed to the global assembly cache:

```
Execute -action install -path "C:\inetpub\WebSiteOne\Mysite -assemblyLocation gac
```

**NOTE:** To use the gac option, deploy the `IBM.Security.Web.ApplicationServices` assembly to the Global Assembly Cache.

## Enabling a Machine Key for the Web Application

To ensure that user logon is secure, the membership provider uses the local machine key as an authentication password.

1. Open Internet Information Server and select the web application.
2. Select the **Machine Key** icon, then click **Open Feature** from the **Actions** pane as shown in the following figure.

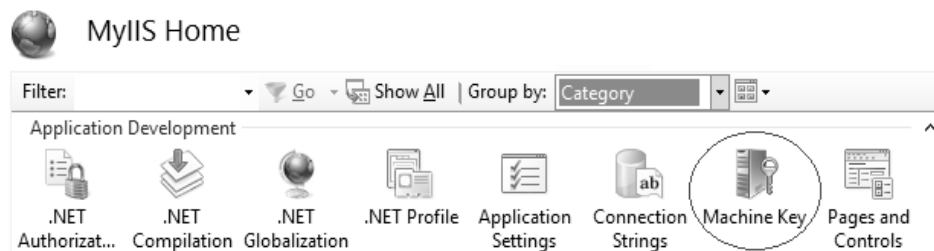


Figure 2. Web application machine key

3. Click **Generate Keys** from the **Actions** pane as shown in Figure 3.

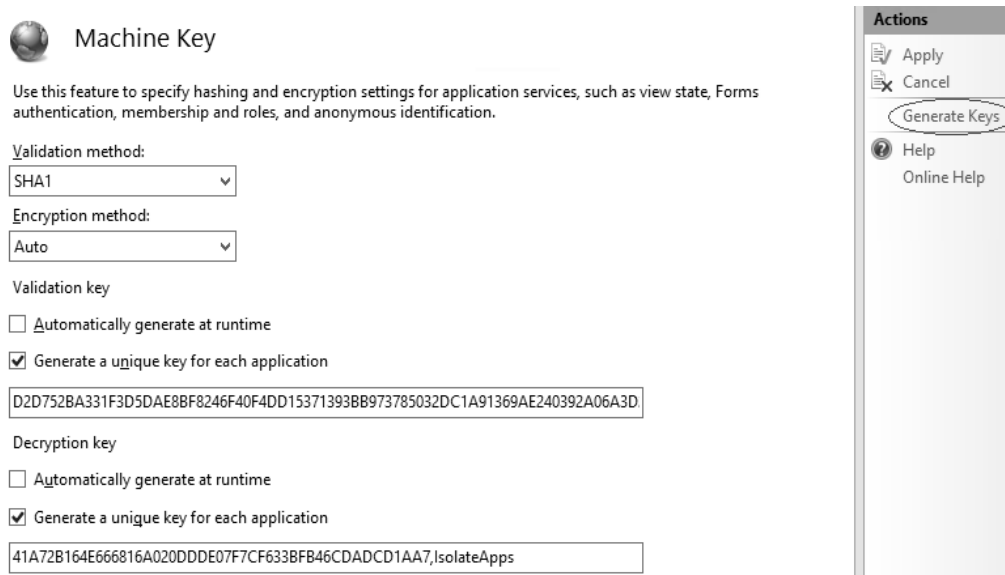








Figure 3. Generating the Machine Key

















4. Click **Apply** from the **Actions** pane to store the keys in the `web.config` file of the web application.

## Membership Provider Implementation

The following table summarizes the direct or pass-through implementation of methods and properties 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 method on another configured membership provider for the given web application. This functionality is configured using the **extendedProviderName** property within the configuration of the IBM Security Access Manager Membership provider.

	Name	Implemented?	Pass-through?
	<a href="#">ChangePassword</a>	No	Yes
	<a href="#">ChangePasswordQuestionAndAnswer</a>	No	Yes
	<a href="#">CreateUser</a>	No	Yes
	<a href="#">DeleteUser</a>	No	Yes
	<a href="#">FindUsersByEmail</a>	No	Yes
	<a href="#">FindUsersByName</a>	No	Yes
	<a href="#">GetAllUsers</a>	No	Yes
	<a href="#">GetNumberOfUsersOnline</a>	No	Yes
	<a href="#">GetPassword</a>	No	Yes
	<a href="#">GetUser(Object, Boolean)</a>	Yes	Yes
	<a href="#">GetUser(String, Boolean)</a>	Yes	Yes
	<a href="#">GetUserNameByEmail</a>	Limited	Yes
	<a href="#">Initialize</a>	Yes	N/A
	<a href="#">ResetPassword</a>	No	Yes
	<a href="#">UnlockUser</a>	No	Yes
	<a href="#">UpdateUser</a>	No	Yes

	<a href="#">ValidateUser</a>	Yes	Yes (if not already)
	<a href="#">ApplicationName</a>	Yes	No
	<a href="#">Description</a>	Yes	No
	<a href="#">EnablePasswordReset</a>	Yes (default is false)	No
	<a href="#">EnablePasswordRetrieval</a>	Yes (default is false)	No
	<a href="#">MaxInvalidPasswordAttempts</a>	No	Yes
	<a href="#">MinRequiredNonAlphanumericCharacters</a>	No	Yes
	<a href="#">MinRequiredPasswordLength</a>	No	Yes
	<a href="#">Name</a>	Yes	No
	<a href="#">PasswordAttemptWindow</a>	No	Yes
	<a href="#">PasswordFormat</a>	No	Yes
	<a href="#">PasswordStrengthRegularExpression</a>	No	Yes
	<a href="#">RequiresQuestionAndAnswer</a>	No	Yes
	<a href="#">RequiresUniqueEmail</a>	No	Yes
	ExtendedProviderName (string) Name of a configured provider for pass-through functionality.	Yes	N/A
	UserNameHeader (string) Name the of HTTP header that refers to the user name.	Yes	N/A

## 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. See 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/tivi-help/v2r1/topic/com.ibm.itame.doc\\_6.1/am61\\_webseal\\_admin314.htm#ext-attr-header](http://publib.boulder.ibm.com/infocenter/tivi-help/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 Signin 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 signin behavior.

Name	Description	Example
<code>DisablePostBackQueryString</code>	A query string value that is evaluated in the request to bypass the sign-in page from rendering and invoking a postback.	<code>ctx=ws</code>
<code>PostBackDelay</code>	A timer delay before the sign-in page executes a postback. The value represents the delay in seconds.	5

Table 2. Access Manager Signin Page configuration options

See the following example of the Access Manager Signing Page stanza:

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

## Customising the Signin Page

The `AccessManagerSignin.aspx` sign in page can be substituted with a custom designed ASPX page.

To maintain the single sign-on experience, the ASPX page must:

- Inherit from the `IBM.Security.Web.AccessManagerSignin`
- The two web controls, progress, and status must exist in the new page.

```
<%@ Page Language="C#" Inherits="IBM.Security.Web.AccessManager-  
Signin" %>
```

**NOTE:** Update the attribute `loginUrl="MySigninPage.aspx"` in the `<forms>` stanza.

## LDAP Binding

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

Name	Description	Example
TrustedUserName	<p>The name that is used to authenticate to the LDAP.</p> <p>The trusted user name and password is contained in the authorization HTTP header.</p> <p>WebSEAL inserts this header using the <code>-b</code> supply junction option. Refer to Handling client identity information across junctions.</p> <p><a href="https://publib.boulder.ibm.com/infocenter/tivi-help/v2r1/topic/com.ibm.itame.doc_6.0/rev/am60_webseal_admin203.htm?path=5_8_1_6_0_6_0_2_1_10_0_0_6_0#wq680">https://publib.boulder.ibm.com/infocenter/tivi-help/v2r1/topic/com.ibm.itame.doc_6.0/rev/am60_webseal_admin203.htm?path=5_8_1_6_0_6_0_2_1_10_0_0_6_0#wq680</a></p>	jdoe
Address	The name of the LDAP server.	myldap.com
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 that determines if LDAP binding is enabled	true   false

Table 1. LDAP Binding

See the following example of the LDAP bind stanza:

```
<accessManager>
...
<ldapBinding
  trustedUsername=" jdoe"
  address=" myldap.com"
  suffix=" o=ibm,c=us"
  prefix="cn="
  enabled="false"/>
...
</accessManager>
```

## Extended Provider Attribute


















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



```
<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 summarises the direct or pass-through implementation of methods and properties 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 method on another configured role provider for the given web application. This functionality is configured using the **extendedProviderName** property within the configuration of the IBM Security Access Manager Role provider.

	Name	Implemented?	Pass-through?
	<a href="#">AddUsersToRoles</a>	No	Yes
	<a href="#">CreateRole</a>	No	Yes
	<a href="#">DeleteRole</a>	No	Yes
	<a href="#">FindUsersInRole</a>	No	Yes
	<a href="#">GetAllRoles</a>	Yes	Yes
	<a href="#">GetRolesForUser</a>	Yes	Yes
	<a href="#">GetUsersInRole</a>	No	Yes
	<a href="#">Initialize</a>	Yes	N/A
	<a href="#">IsUserInRole</a>	Yes	Yes
	<a href="#">RemoveUsersFromRoles</a>	No	Yes
	<a href="#">RoleExists</a>	Yes	Yes
	<a href="#">ApplicationName</a>	Yes	No
	<a href="#">Description</a>	Yes	No
	<a href="#">Name</a>	Yes	No
	ExtendedProviderName (string) Name of a configured provider for pass-through functionality.	Yes	N/A
	UserNameHeader (string) Name the of HTTP header that refers to the user name.	Yes	N/A
	RolesDefaultResult (bool) Default action if no role authorities is found	Yes	N/A

 AvailableRoles (string[]) Gets or sets a manual list of roles.	Yes	N/A
 GroupNameHeader (string) Name the of HTTP header that refers to the user name.	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.

### 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 work-around 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

### 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 providers 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"/>
```

## 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"  
      InitializeDate="IsamHttpProviders.log"/>  
  </shareListenders>  
</system.diagnostics>
```

# Chapter 3: LibraryDemo Sample Application

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

## Importing the LibraryDemo

1. Open Internet Information Server and select the web site.
2. Click **Import Application** from the **Actions** pane as shown in the following figure.

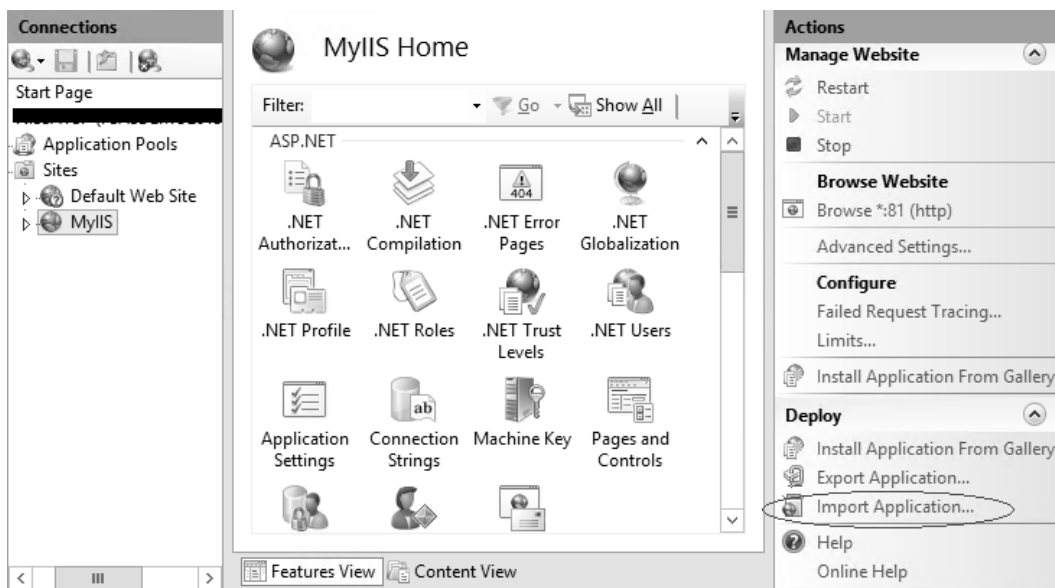


Figure 4. Import Application

3. In the Import Application Package wizard, browse to the LibraryDemo.zip file, then click **Next**.
4. Follow the wizard to complete the import.

**NOTE:** Microsoft Web Deploy 2.0 must be installed to import packages into Internet Information Server.

After the successful import of the LibraryDemo application, follow the steps in Configure an ASP.NET Web Application to achieve a basic configuration of the ASP.NET LibraryDemo application.

To test the LibrayDemo sample application

1. Log in to WebSEAL to access the LibraryDemo application through the configure junction.
2. Click **Introduction** for information about configuring the role providers and extended membership providers for the application.
3. Execute the steps in the Introduction to create the necessary IBM Security Access Manager groups which are mapped to the ASP.NET roles.
4. Execute the test scenarios to validate single sign-on, role validation, and extended provider functionality.

# Chapter 4: Removing the integration

## Manually configured ASP .NET web applications

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.

## Using Isam.ASPNET.Deploy.ps1

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 unistallation take the following steps:

1. At the command prompt, navigate to the folder location of the extracted IBM Security Access Manager for Microsoft Applications files.
2. Type PowerShell
3. Type `.\Isam.ASPNET.Deploy.ps1`
4. Type `Execute -action uninstall -path <location of web.config> -assemblyLocation gac | bin`

Example usage for an application with assembly deployed to the global assembly cache:

```
Execute -action uninstall -path "C:\inetpub\WebSiteOne\Mysite -assemblyLocation gac
```

# 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:

© (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](http://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](http://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.