

IBM Security Access Manager
for Versions 6.1.1, 7.0 and 8.0

***Claims-based Authentication for
SharePoint using IBM Security
Access Manager WebSEAL***



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 Claims based Authentication for SharePoint using IBM Security Access Manager WebSEAL and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation 2013, 2014.

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

Preface.....	5
About this publication.....	5
Access to publications and terminology	5
Publication Library	5
Base Information.....	5
WebSEAL Information	6
Web Gateway Appliance Information.....	6
IBM Tivoli Federated Identity Manager information	6
IBM Terminology website	7
Accessibility.....	7
Technical training.....	7
Support information	7
Statement of Good Security Practices.....	8
Product name updates	8
Chapter 1: Introducing the integration.....	9
Introduction.....	9
Integration product version information	11
Integration package contents.....	11
Network connectivity considerations.....	11
Chapter 2: Integration process	12
Before you start.....	12
Installation procedure.....	12
Deploying the solution in SharePoint	13
Configuring the web application.....	13
Additional SharePoint configuration options.....	15
SharePoint diagnostic logging	16
WebSeal Junction Create	17
WebSeal Session Management	18
Microsoft Office client integration	19
WebSEAL configuration.....	20

Sharepoint configuration.....	21
Access Manager Group Mapping to SharePoint Groups.....	21
Deploying in multi-farm environments	27
Installation.....	27
Uninstallation.....	27
Known issues and limitations	28
Notices	29
Trademarks.....	31

Preface

About this publication

This guide provides instructions on how to configure your Microsoft SharePoint to enable a single-sign on using IBM® Security Access Manager WebSEAL features.

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

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

Readers must be familiar with the following concepts:

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

Access to publications and terminology

The following publications complement the information contained in this document:

Publication Library

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

Base Information

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

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

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

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

WebSEAL Information

- *IBM Security Access Manager WebSEAL Installation Guide*

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

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

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

- *IBM Security Access Manager WebSEAL Configuration Stanza Reference*

Provides a complete stanza reference for WebSEAL.

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

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

Web Gateway Appliance Information

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

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

IBM Tivoli Federated Identity Manager information

1. *IBM Tivoli Federated Identity Manager Installation Guide*

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

2. *IBM Tivoli Federated Identity Manager Administration Guide*

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

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

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

IBM Terminology website

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

Accessibility

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

Technical training

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

Support information

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

Statement of Good Security Practices

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

Product name updates

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

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

Chapter 1: Introducing the integration

This chapter has the following sections:

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

Introduction

IBM Security Access Manager manages the user authentication to perform single sign-on (SSO). The user identity and group information is provided to the backend applications for subsequent requests.

This guide provides a step-by-step approach for configuring Forms Based Authentication (FBA) as single sign-on (SSO) for SharePoint web applications. The environment deploys IBM Security Access Manager and Tivoli Directory Services or a supported Lightweight Directory Access Protocol (LDAP). Microsoft SharePoint can be installed in stand-alone mode or as part of a farm environment.

Note:

Microsoft SharePoint uses dynamic content and scripts. Therefore, this integration requires the use of WebSEAL virtual host junctions. For more information about junction creation, see the *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

[Figure 1](#) shows the typical sequence of steps that are involved in performing a Forms Based Authentication (FBA) claims single sign-on.

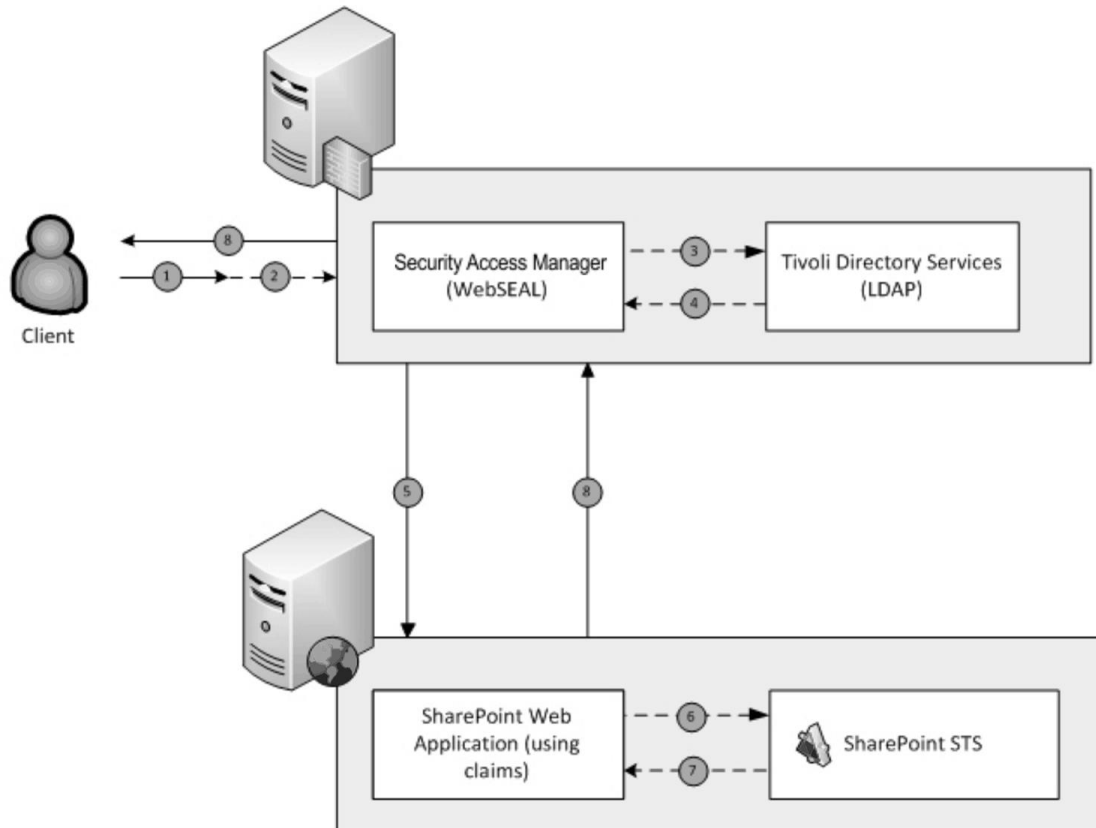


Figure 1. Forms Based Authentication (FBA) Claims sign-in sequence

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

1. A client browser makes a request to a SharePoint web application.
2. IBM Security Access Manager WebSEAL acts as a reverse proxy that intercepts requests and prompts the user for authentication.
3. The client provides username and password credentials.
4. Credentials are validated against IBM Security Access Manager for authentication.
5. WebSEAL forwards the request to the Microsoft SharePoint web application configured for Forms based Authentication (FBA) with the user identity and groups in the request header.
6. The user identity is forwarded to the SharePoint Security Token Service (STS)
7. SharePoint validates the token and issues a claim-based token.
8. The response is sent back to the client through WebSEAL; the FedAuth cookie is stored for subsequent requests.

Integration product version information

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

Integration package contents

The integration package provides the following files:

File name	Description
Documents\Microsoft SharePoint\ am_claims_sharepoint_guide.pdf	Supplement guide for Microsoft SharePoint for claims.
Solutions\Microsoft SharePoint\ IBM.Security.SharePoint.Application- Services.wsp	SharePoint solution installer.
Examples\Microsoft SharePoint\ Share- Point.Farm.Deploy.ps1	Microsoft Powershell script for deployment in multi-farm environments

Network connectivity considerations

IBM Security Access Manager services are 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:

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

IBM Security Access Manager

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

Microsoft SharePoint

- Installed into a farm or single-instance environment

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

Installation procedure

To install the integration package:

1. Place the SharePoint solution package, `IBM.Security.SharePoint.ApplicationServices.wsp`, in a temporary folder.
2. Using the SharePoint Management shell command-line prompt, type the following command:

```
stsadm -o addsolution -filename '<location of temporary  
folder>\IBM.Security.SharePoint.ApplicationServices.wsp'
```

3. The installation process displays a message to indicate a successful installation.

Deploying the solution in SharePoint

After the solution package is registered in SharePoint, it must be deployed. Use Microsoft SharePoint Central Administration to complete the following steps:

1. Click **System Settings**.
2. Click **Manage farm solutions**.
3. Select `IBM.Security.SharePoint.ApplicationServices.wsp`.

Note: The Status and Deployed To states are set to *Not Deployed* and *None* respectively.

4. Click **Deploy Solution**.
5. Specify the appropriate settings, and then click **OK**.
6. Successful deployment updates the status column as *Deployed*.
7. If you are deploying into a multi-farm environment, complete the additional installation steps that are detailed in [Deploying in multi-farm environments](#).

Configuring the web application

To use Forms Based Authentication (FBA), a web application must be configured for claims authentication.

1. Click **Manage web application**.
2. On the **Web Application** tab, click **New**.
3. In the Authentication section of the **Create New Web Application** window, select **Claims Based Authentication**.

Note: If an existing claims site is configured on the **Web Application** tab, click **Extend**. Extending a web application enables different authentication types to be configured on different URL and ports while serving the same site content.

4. Ensure that the following sections are completed as shown. [Figure 2](#) represents the default values for configuring a new claims-based web application or extending an existing claims web application.

Note: The suggested approach is to separate the authentication types for each web application. Notice Windows Authentication is intentionally disabled for this zone.

Create New Web Application

Claims Authentication Types

Choose the type of authentication you want to use for this zone.

Negotiate (Kerberos) is the recommended security configuration to use with Windows authentication. If this option is selected and Kerberos is not configured, NTLM will be used. For Kerberos, the application pool account needs to be Network Service or an account that has been configured by the domain administrator. NTLM authentication will work with any application pool account and with the default domain configuration.

Basic authentication method passes users' credentials over a network in an unencrypted form. If you select this option, ensure that Secure Sockets Layer (SSL) is enabled.

ASP.NET membership and role provider are used to enable Forms Based Authentication (FBA) for this Web application. After you create an FBA Web application, additional configuration is required.

Trusted Identity Provider Authentication enables federated users in this Web application. This authentication is Claims token based and the user is redirected to a login form for authentication. Learn about configuring authentication.

Sign In Page URL

When Claims Based Authentication types are enabled, a URL for redirecting the user to the Sign In page is required. Learn about Sign In page redirection URL.

☐ Enable Windows Authentication

If Windows authentication is not selected on any Zone of this Web application, crawling for this Web application will be disabled.

☐ Integrated Windows authentication

NTLM

☐ Basic authentication (credentials are sent in clear text)

☒ Enable Forms Based Authentication (FBA)

ASP.NET Membership provider name

AccessManagerMembershipProvider

ASP.NET Role manager name

AccessManagerRoleManager

☐ Trusted Identity provider

There are no trusted identity providers defined.

☐ Default Sign In Page

☒ Custom Sign In Page

~/_layouts/accessmanagersignin.aspx


Figure 2. Default values for Access Manager Claims authentication

Enter the other details specific to your web application.

5. Click **OK** to create the web application.
6. Return to the Central Administration home page and select the web application that was created in the previous steps. Click **Manage Features**.
7. Click **Activate** to enable the IBM Security Access Manager Claims Authentication Feature.

Manage Web Application Features

OK

Name	Status
IBM Security Access Manager Claims Authentication Feature  IBM Security Access Manager role and membership providers enables users from WebSEAL to be authenticated in SharePoint environments configured for forms based authentication (FBA) claims.	Inactive

Activate

Figure 3. Authentication feature

8. Return to the Central Administration home page and click **Create site collections for new web applications**. If you are using an existing site, click **Change site collection administrators**.
9. Enter a valid IBM Security Access Manager user account as the **Primary** or **Secondary Site Collection Administrator**, or both.
10. Enter appropriate details for the site collection and then click **OK**.

Additional SharePoint configuration options

In circumstances where more settings are required, the solution package deploys an administration screen in SharePoint. From the SharePoint Central Administration:

1. Click **Security**.
2. Click **Configure Access Manager authentication settings**.

Web Application Select a web application.	Web Application: <input type="text" value="http://r2d2/"/>
Sign Out Page URL When Claims Based Authentication is enabled, a URL for redirecting the user to the WebSEAL Sign Out page is required.	Sign Out Page: <input type="text" value="~/pkmslogout"/> Example: ~/pkmslogout
LDAP Bind Incoming requests can be validated against Tivoli Access Manager LDAP as part of the authentication process. To use this feature you need to configure your WebSEAL junction with the -b supply option to send a Basic Authentication header in the request. The trusted user name is verified against the LDAP bind settings. Learn about handling client identity information across junctions. Note: The LDAP bind is not supported on SSL connections.	<input checked="" type="checkbox"/> Enable LDAP bind Server address: <input type="text"/> Example: server.com:389 Object space prefix: <input type="text"/> Example: cn= Object space suffix: <input type="text"/> Example: dc=com Trusted user name: <input type="text"/>

Figure 4. Authentication settings

SharePoint diagnostic logging

The deployed solution integrates logging in to SharePoint's reporting and monitoring framework. By default, the Access Manager Claims configuration automatically outputs trace to SharePoint's log files.

To configure SharePoint diagnostic logging, from the Central Administration:

1. Click **Monitoring**.
2. Click **Configure diagnostic logging**.
3. Select the collapsed icon next to Access Manager to expand.

Event Throttling

Use these settings to control the severity of events captured in the Windows event log and the trace logs. As the severity decreases, the number of events logged will increase.

You can change the settings for any single category, or for all categories. Updating all categories will lose the changes to individual categories.

Select a category	Category	Event Level	Trace Level
<input type="checkbox"/>	All Categories		
<input checked="" type="checkbox"/>	Access Manager	Information	Medium
<input type="checkbox"/>	Authentication	Information	Medium
<input type="checkbox"/>	Messaging	Information	Medium
<input type="checkbox"/>	Providers		
<input type="checkbox"/>	Business Connectivity Services		
<input type="checkbox"/>	SharePoint Foundation		
<input type="checkbox"/>	SharePoint Foundation Search		

Least critical event to report to the event log:

Least critical event to report to the trace log:

Event Log Flood Protection

Enabling this setting allows detection of repeating events in the Windows event log. When the same event is being logged repeatedly, the repeating events are detected and suppressed until conditions return to normal.

☒ Enable Event Log Flood Protection

Trace Log

When tracing is enabled you may want the trace log to go to a certain location. Note: The location you specify must exist on all servers in the farm.

Additionally, you may set the maximum number of days to store log files and restrict the maximum amount of storage to use for logging. Learn about using the trace log.

Path:
Example: C:\Program Files\Microsoft Shared\Web Server Extensions\14\LOGS

Number of days to store log files:

Restrict Trace Log disk space usage: ☐

Maximum storage space for Trace Logs (GB):

Figure 5. Access Manager Diagnostic settings

4. Select the type of events as appropriate to report to the trace log.

Note: Windows Event Log is not supported.

5. Click **OK**.

You can find more information about SharePoint diagnostics at: <http://technet.microsoft.com/en-us/library/ee748656.aspx>.

WebSeal Junction Create

The integration requires a WebSEAL virtual host junction to be created with the following options:

Parameter	Value (as examples)	Description
-t	tcp	Use TCP as the network transport.
-h	claims.test.com	The fully qualified domain name that is included in the URL for the SharePoint web application zone.
-p	8088	SharePoint web application the FBA site is configured on.
-c	iv-user,iv-groups	Inserts the authenticated username and groups into the request header.
-b	supply	(optional) Used when the SharePoint web application requires LDAP bind support.

The following command uses these example values:

```
server task default-webseald-<machine-name> virtual create
-t tcp -h claims.test.com -p 8088 -c iv-user,iv-groups <junction-name>
```

Note: By default WebSEAL is configured to listen on port 80. Therefore, to ensure the virtual host junction works correctly, use one of the following configurations:

- Configure WebSEAL and the SharePoint web application to use the same ports.
- Configure WebSEAL with an interface that listens on the same ports as the SharePoint web application.

To configure a WebSEAL interface:

1. Open the IBM Security Access Manager WebSEAL configuration file.
2. In the [server] stanza (near the top of the file), modify the http or https client information listen on the same port as the SharePoint application. For http:

```
#-----
# HTTPS CLIENT
#-----

# Allow HTTPS access
https = yes

# Port for HTTPS requests (SharePoint application also on 19449)
https-port = 19449
```

3. Save and close the configuration file.
4. Restart WebSEAL.

For more information about WebSEAL port settings, interface creation and junction creation, see the *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

WebSeal Session Management

WebSEAL creates a session cookie when a user is authenticated. The expiry of this cookie might differ to the FedAuth cookie issued by the SharePoint STS. To avoid orphaned cookies, WebSEAL can remove the FedAuth cookie when the WebSEAL user session times out. SharePoint re-issues the FedAuth cookie when the WebSEAL session is reestablished.

To enable this capability, add FedAuth to the managed-cookies-list in the WebSEAL configuration file. You can find more information about this setting in the Managing Cookies section of the *IBM Security Access Manager for Web: WebSEAL Administration Guide* at: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.isam.doc_70%2Fameb_webseal_guide%2Fconcept%2Fcon_mngng_cookies.html

Microsoft Office client integration

In IBM Security Access Manager 7.0, you can configure WebSEAL to share sessions with Microsoft Office applications. This integration package includes a Microsoft SharePoint feature, which uses this WebSEAL functionality to integrate WebSEAL, Microsoft SharePoint Server and Microsoft Office applications.

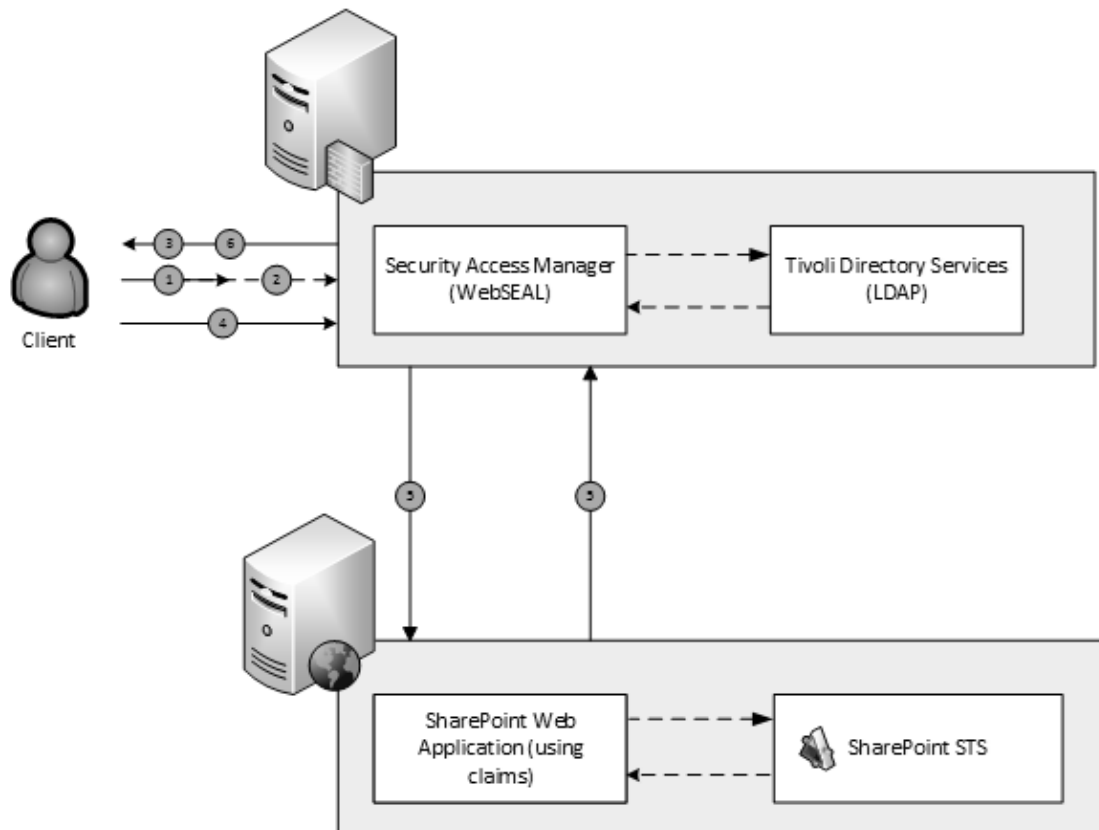


Figure 6. Sequence of events that occur for a context switch from SharePoint to a Microsoft Office application

[Figure 6](#) illustrates the events that occur when a user makes a SharePoint request to open or create a document in a Microsoft Office application.

Note: The events that are shown in Figure 4 occur *after* the user signs in using Forms Based Authentication. For more information, see [Figure 1](#).

1. User elects to create a document or open an existing document for editing in Microsoft Office.
2. The browser makes a JavaScript request for `/pkmstempsession`.

3. WebSEAL adds an entry for the session in the temporary cache and returns a single-use temporary session cookie.
4. The Microsoft Office Application requests the chosen document.
5. WebSEAL uses the temporary cookie to retrieve the session information from the temporary cache and then fetches the requested document.
6. The document is returned to the client with the session cookie set.

This feature is only supported for a Microsoft SharePoint Standard environment, which is integrated with either IBM Security Access Manager 7.0 or IBM Security Web Gateway Appliance by using claims based authentication. Microsoft Office 2007 or 2010 must also be installed on the client machine.

Note: The Microsoft SharePoint environment must not have Microsoft Office Web Apps installed.

In this environment, the following actions are supported:

- Opening a document in Microsoft Office from SharePoint.
- Editing a Microsoft Office document, which was opened from SharePoint.
- Saving a document back to SharePoint after editing is complete.
- Creating a Microsoft Office document from SharePoint (Microsoft Office 2007 only).

WebSEAL configuration

Locate the WebSEAL configuration file, `webseald-instance.conf` file in the `WebSEAL_install/etc` directory.

In the **[session]** stanza, set the value of **temp-session-max-lifetime** to be non-zero. For example, the following setting configures a maximum lifetime duration of 10 seconds:

```
[session]
temp-session-max-lifetime = 10
```

Note: A value of 0 disables session sharing between WebSEAL and Microsoft Office applications.

For more information, see the "Share sessions with Microsoft Office applications" section of the *IBM Security Access Manager for Web: WebSEAL Administration Guide*.

SharePoint configuration

Use Microsoft SharePoint Central Administration to complete the following steps:

1. Navigate to the list of web applications.
2. Select the application for which you want to enable the IBM Security Access Manager Office Client Integration.
3. Click **Manage Features**.
4. Click **Activate** to enable the IBM Security Access Manager Office Client Integration feature.
5. Open the web.config file for the SharePoint web application, typically located at `<drive>:\inetpub\wwwroot\wss\VirtualDirectories\<port>`
6. Locate the `<appsettings>` stanza
7. Modify the fileExtension to add or remove file extension that will invoke `/pkm-stempsession`.
8. Modify `websealSessionCookieName` and `websealTempCookieName` to match `tcp-session-cookie-name` and `temp-session-cookie-name` in WebSEAL
9. Save web.config

Access Manager Group Mapping to SharePoint Groups

There is no implied correlation between IBM Security Access Manager groups and SharePoint groups. To map IBM Security Access Manager groups in SharePoint, you must first configure your IBM Security Access Manager users in to the appropriate IBM Security Access Manager groups.

When a user is authenticated through WebSEAL, the junction (see example in previous sections) forwards group information for the authenticated user in the iv-groups header.

To ensure that a user has permissions to access the SharePoint site, you must assign the IBM Security Access Manager group into SharePoint groups.

Consider an example where the IBM Security Access Manager user testuser1 is assigned to the IBM Security Access Manager group called testgroup1. The following demonstrates the mapping of IBM Security Access Manager groups into SharePoint groups.

1. Authenticate to WebSEAL as the user who is specified as the Site Collection Administrator. Refer to step 9 of [Configuring the web application](#).

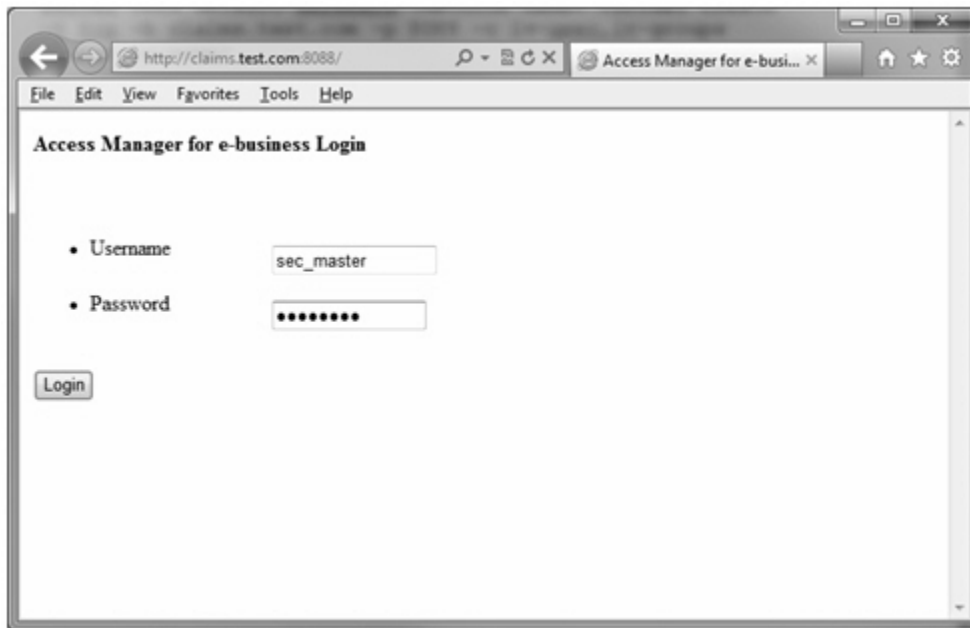


Figure 7. User login

2. The IBM Security Access Manager user automatically signs in to SharePoint.
3. Click **Site Actions**.
4. Click **Site Permissions**.
5. Click one of the built-in SharePoint Groups (Members, Owners, Visitors) for the site, alternatively you can create a custom group.

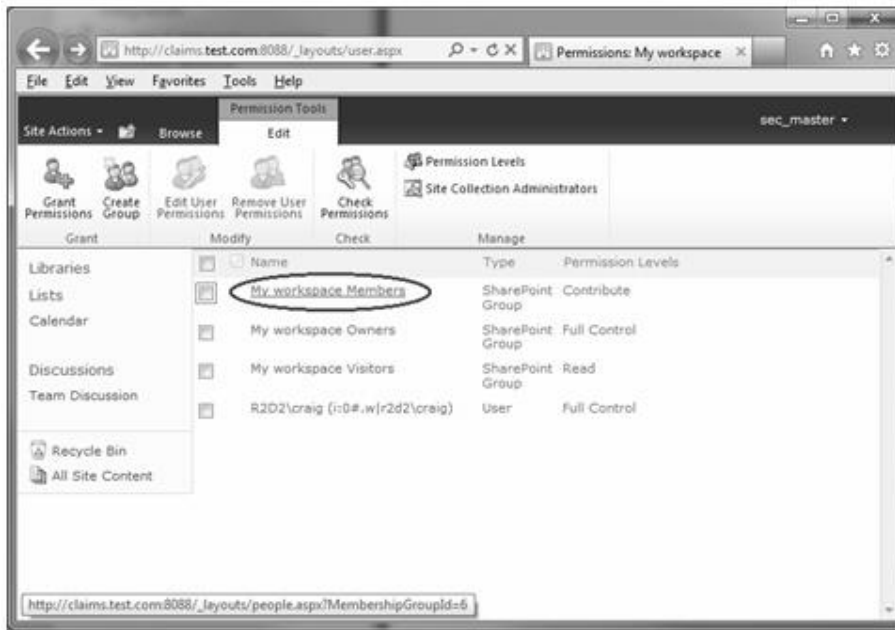


Figure 8. Group selection

6. Click **New > Add User**.
7. Select the **People Picker Address book** icon.

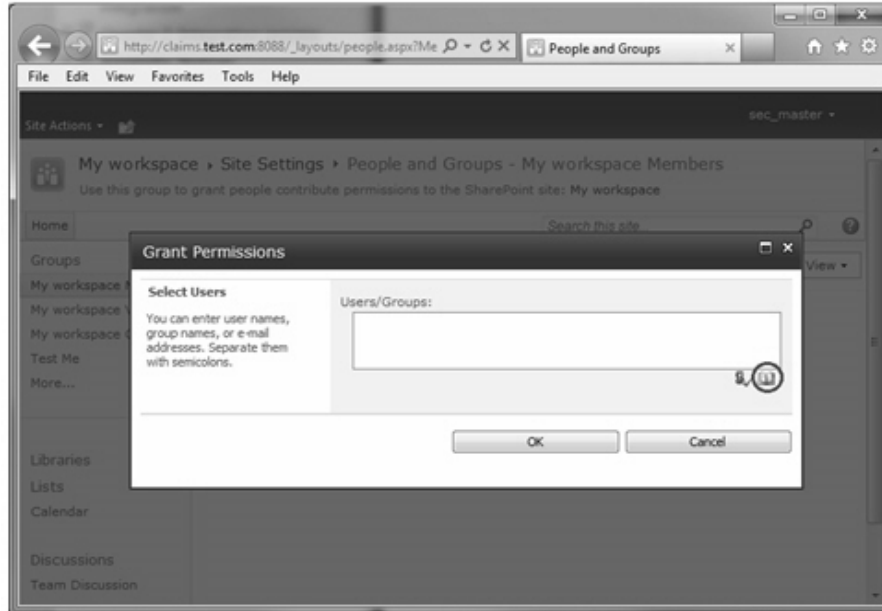


Figure 9. Add user

8. Type the name of the IBM Security Access Manager group you want to add to the SharePoint Group.

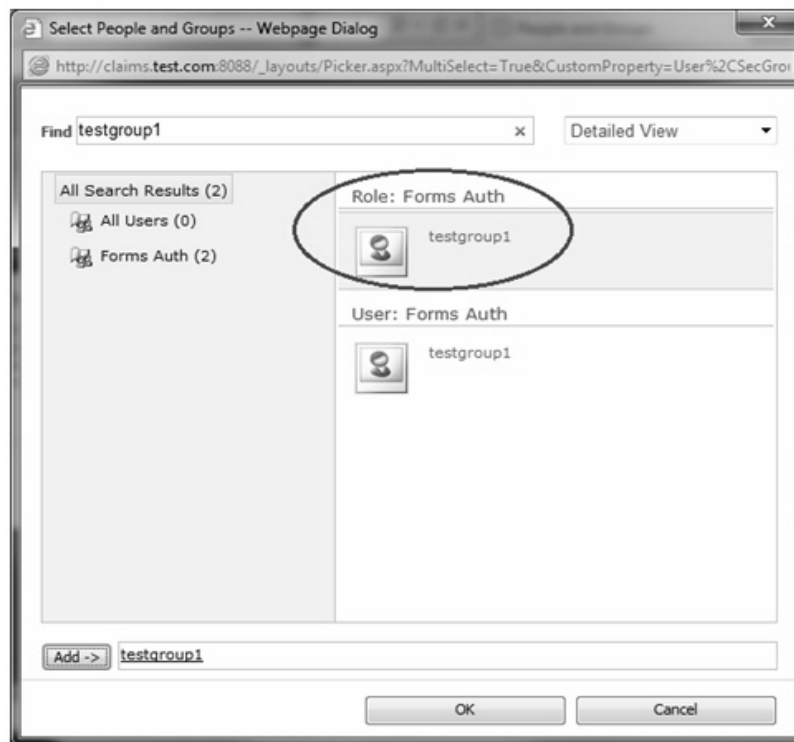


Figure 10. Name entry

Note: The IBM Security Access Manager group **testgroup1** appears as a Forms Auth Role and User. The People Picker for this integration does not validate or resolve users or role names.

9. Select **testgroup1** in the **Role: Forms Auth result** section.
10. Click **Add**.
11. Click **OK** to return to the Grant Permissions screen.
12. Click **OK** to return to the SharePoint People and Groups screen.

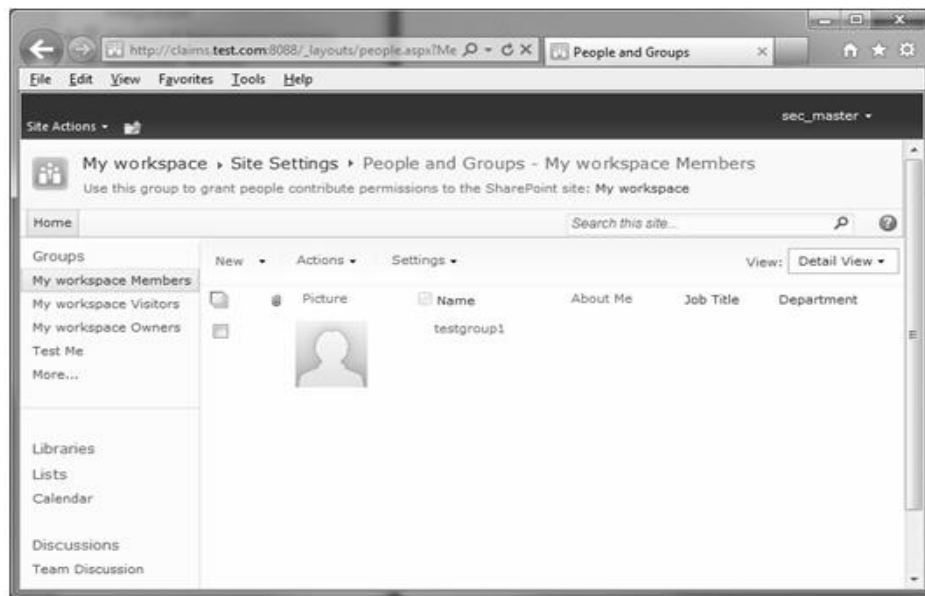


Figure 11. People and Groups screen

13. Sign out of this browser session and reauthenticate to WebSEAL as the IBM Security Access Manager user *testuser1*.

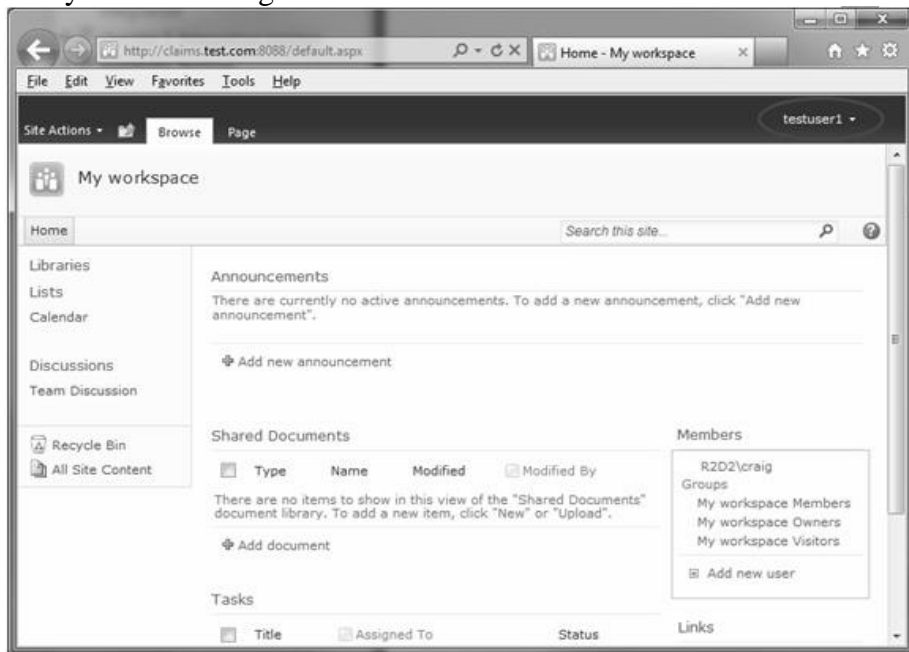


Figure 12. Permissions verification

14. Verify that *testuser1* has the permissions that are associated with the selected SharePoint group assigned in step 9.

Uninstallation Procedure

Uninstalling the SharePoint solution package removes the configuration changes made to all SharePoint web applications that have the IBM Security Access Manager Claims Authentication feature activated. The uninstallation procedure is a two-step process. It requires the SharePoint Administrator to deactivate all IBM Security Access Manager features including IBM Security Access Manager Claims Authentication and IBM Security Access Manager Office Client Integration for the applicable web application. The Administrator must then retract and remove the SharePoint solution package.

To deactivate the IBM Security Access Manager features, complete the following tasks in the SharePoint Central Administration web console:

1. Select **Manage web applications**.
2. Click the web application where the feature is activated.
3. Click **Manage Features**.
4. Click **Deactivate** for all active IBM Security Access Manager features.
5. Repeat steps 2-4 for each web application where the feature is activated.

To retract and remove the SharePoint solution package, within the SharePoint Central Administration web console:

1. Select **System Settings**.
2. Under Farm Management, click **Manage farm solutions**.
3. Select **IBM.Security.SharePoint.ApplicationServices.wsp**.
4. Click **Retract Solution**.

Note: In a non-farm environment, when you retract the solution, ensure that the SharePoint Timer Service is running under the "Local System" account. When the retracting completes, revert the SharePoint Timer Service account at "Network Service" (default).

5. Specify the appropriate settings, and then click **OK**.
 6. Click **Remove Solution** which removes the package from SharePoint.
- If you are deploying into a multi-farm environment, complete the additional

Deploying in multi-farm environments

In environments that contain additional Security Token Service (STS) instances, for example in multi-farm environments, or where Web Applications are extended to different Front End Web Servers, the configuration changes made by the solution and feature installer are not propagated to those servers.

You must manually execute `installfeature -force` using the `stsadm` command or run the included Powershell script on each server to add the required configuration. The use of the included `SharePoint.Farm.Deploy.ps1` Powershell script is preferable and is described in the following sections.

Installation

After adding the solution and deploying the feature in the Microsoft SharePoint Central Administration site, complete the following steps:

1. Start the console from `c:\windows\system32\windowspowershell\v1.0\powershell.exe`
2. Navigate to the location of `SharePoint.Farm.Deploy.ps1`
3. Enter `.\SharePoint.Farm.Deploy.ps1`
4. At the prompt, enter `execute -action install`

Uninstallation

After removing Access Manager for SharePoint Claims from your SharePoint Central Administration site, complete the following steps:

1. Start the console from `c:\windows\system32\windowspowershell\v1.0\powershell.exe`
2. Navigate to the location of `SharePoint.Farm.Deploy.ps1`
3. Enter `.\SharePoint.Farm.Deploy.ps1`
4. At the prompt, enter `execute -action uninstall`

Known issues and limitations

1. The People Picker functionality does not resolve users or groups against the role and membership provider. Authorization to SharePoint is based on the groups that are returned from WebSEAL and processed as role claims along with any additional configured roles.
2. For SharePoint web applications configured with Forms Based Authentication (FBA), SharePoint administrators are required to configure site access for users and groups. There is no correlation between SharePoint groups and those groups that are transformed into claims from the SharePoint Security Token Service (STS).
3. The AccessManagerClaimsMembershipProvider and AccessManager-ClaimsRoleManager implement the minimum properties and methods as required by SharePoint Security Token Service (STS).

Reference: [http://msdn.microsoft.com/en-us/library/bb975135\(of-fice.12\).aspx#MOSSFBAPart2_MinimumInterfaces](http://msdn.microsoft.com/en-us/library/bb975135(of-fice.12).aspx#MOSSFBAPart2_MinimumInterfaces)

Notices

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

Trademarks

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

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

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

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

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

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

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

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



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

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

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

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