

IBM® Security Access Manager
for Versions 6.1.1, 7.0, 8.0 and 9.0

IBM Security Access Manager for SharePoint Claims Based Authentication Integration Guide



Note

Before using this information and the product it supports, read the information in 'Notices' on page 18

This edition applies to Version 1.8 release i of the IBM Security Access Manager for SharePoint Claims Based Authentication and to all subsequent releases and modifications until otherwise indicated in new editions.

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

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

Contents

PREFACE	5
Access to publications and terminology	5
Publication Library	5
IBM Terminology website	6
Accessibility	6
Technical Training	6
Support information	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	9
SHAREPOINT WEB APPLICATION CONFIGURATION	10
Installing the Solution Package	10
Deploying the Solution in SharePoint	10
Create the SharePoint Web Application	10
Activate Feature for the SharePoint Web Application	11
Create the Site Collection for the SharePoint Web Application	12
Additional SharePoint Configuration Options	13
TESTING THE INTEGRATION	14
Before you start	14
Security Access Manager for Web configuration	14
User Account Creation	14
Junction Management	14
Authenticating to Microsoft SharePoint	15
TROUBLESHOOTING	16
Collecting Support Data	16
Security Access Manager for Web trace	16
SharePoint Diagnostic Logging	17

NOTICES	18
TRADEMARKS	20

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

IBM Security Access Manager for Web manages user authentication then passes the user session information to applications that are configured behind WebSEAL.

The following figure shows the typical sequence of steps that are involved in performing a claims based single-sign-on to Microsoft SharePoint using role and membership provider's forms based authentication (FBA).

Integration Architecture

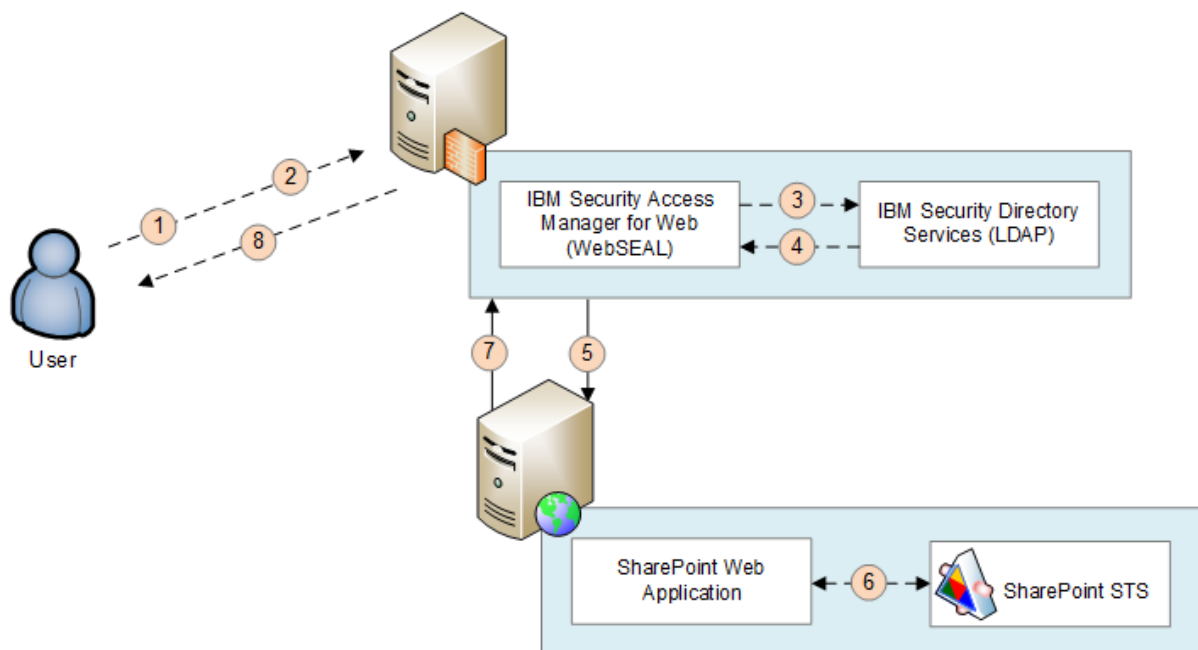


Figure 1: Role and membership provider sign-in sequence

1. The user requests content from a SharePoint web application.
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 SharePoint web application via a configured junction.
6. The role and membership providers inspect the incoming request headers from Security Access Manager. The identity is forwarded to the SharePoint STS to return a claim-based token.
7. SharePoint validates the token and issues a claim-based token.

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

Integration Product Version Information

See the Release Notes for supported versions.

Integration Product Contents

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

File Name	Description
isam_claims_sharepoint_guide.pdf	This integration guide.
Samples\Microsoft SharePoint\IBM.Security.SharePoint.Application Services.wsp	Example XSLT mapping rule to include additional claims into the SAML token.
Samples\Microsoft SharePoint\SharePoint.Farm.Deploy.ps1	Microsoft PowerShell file for deployment into multi-farm environments.

Table 1: Integration Package contents

Before you start

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

- IBM Security Access Manager
 - IBM Security Access Manager for Web or WebSEAL
 - Reverse proxy instance created.
- Microsoft SharePoint
 - Installed into a farm or single-instance environment.

SharePoint Web Application Configuration

Installing the Solution Package

The following steps add the integration components into SharePoint for deployment.

1. Open the SharePoint Management Shell
2. Type `stsadm -o addsolution -filename '`

Deploying the Solution in SharePoint.

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

1. On the Central Administration Home page, click **System Settings**.
2. In the **Farm Management** section, click **Manage farm solutions**.
3. On the Solution Management page, click **IBM.Security.SharePoint.ApplicationServices.wsp** as the solution you want to deploy.
4. On the Solution Properties page, click **Deploy Solution**.
5. On the Deploy Solution page, in the **Deploy When** section, select one of the following:
 - a. **Now**
 - b. **At a specified time**. If you select this option, specify a time by using the date and time boxes. We recommend that you select a time when the load on the destination servers is low.
6. In the **Deploy To?** section, in the **A specific web application** list, click either **All web applications** or select a specific Web application.
7. Click **OK**.

Create the SharePoint Web Application

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

1. On the Central Administration Home page, click **Application Management**.
2. In the **Application Management** page, in the **Web Applications** section, click **Manage web applications**.
3. In the **Contribute** group of the ribbon, click **New**.
4. On the **Create New Web Application** page, in the **IIS Web Site** section, you can configure the settings for your new web application by selecting one of the following two options:
 - Click **Use an existing IIS web site**, and then select the web site on which to install your new web application
 - Click **Create a new IIS web site**, and then type the name of the web site in the Name box.
 - In the **Port** box, type the port number you want to use to access the web application. If you are using an existing web site, this field contains the current port number.
 - Optional: In the **IIS Web Site** section, in the **Host Header** box, type the host name (for example, www.mysharepoint.com) that you want to use to access the web application.
5. In the **Security Configuration** section, click **No** to **Allow Anonymous** and whether or not to Use Secure Sockets Layer (SSL).

6. In the **Claims Authentication Types** section, select **Enable Forms Based Authentication (FBA)**.
7. Type **AccessManagerMembershipProvider** in the ASP.NET Membership provider name and **AccessManagerRoleManager** in the ASP.NET Role manager name.
8. In the **Sign in Page URL** section, select **Custom Sign In Page** and type **~/_layouts/accessmanagersignin.aspx**.
9. In the **Public URL** section, type URL for the domain name for all sites that users will access in this web application. The Zone value is automatically set to **Default** for a new web application. You can change the zone when you extend a web application.
10. In the **Application Pool** section, click **Create a new application pool**.
11. The remaining sections can be left with the default values.
12. Click **OK** to create the new web application.

Activate Feature for the SharePoint Web Application

1. On the Central Administration Home page, click **Application Management**.
2. In the **Application Management** page, in the **Web Applications** section, click **Manage web applications**.
3. Select the web application created in Create the SharePoint Web Application *page 10*
4. In the **Manage** group of the ribbon, click **Manage Feature**.
5. Click **Activate** to enable IBM Security Access Manager Claims Authentication feature.
6. Click **OK**.

Create the Site Collection for the SharePoint Web Application

A site collection is made up of one top-level site and all sites below that have the same owner and share administrator settings. As shown in the following figure, it is the top level or hierarchy in a SharePoint 2016 web application.

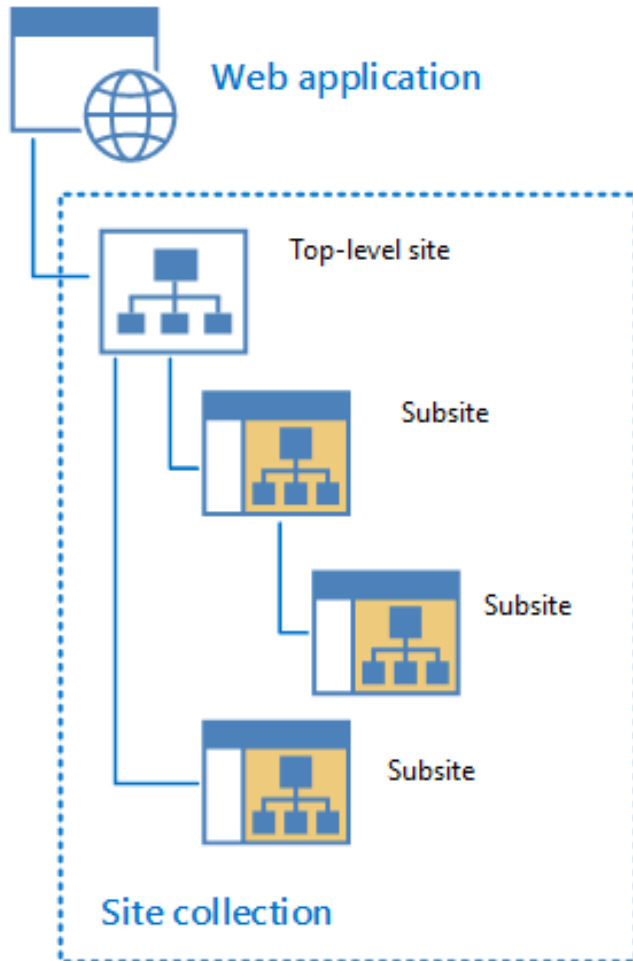


Figure 2: SharePoint 2016 site collection hierarchy

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

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

8. In the **Primary Site Collection Administrator** section, type the user name for the user who will be the site collection administrator. The user name can be from the role and membership provider.
9. In the **Secondary Site Collection Administrator** section, type the user name for the user who will be the site collection secondary administrator. The user name can be from the role and membership provider.
10. Click **OK**.

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

Additional SharePoint Configuration Options

1. On the Central Administration Home page, click **Security**.
2. Click **Configure Access Manager authentication settings**.
3. Select the **web application** and set the additional settings as required.

Testing the Integration

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

Before you start

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

Security Access Manager for Web configuration

Install and configure a Security Access Manager for Web appliance:

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

User Account Creation

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

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

Existing user accounts can be used in the sample.

Junction Management

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

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

pdadmin sec_master> server task <instance-name>-webseald-<webseal-
hostname> virtualhost create -t tcp -h <hostname of SharePoint
server> -p <SharePoint web application port> -v <virtual
hostname>:<virtual port> -c iv-user,iv-groups sharepoint_sample
```

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

Authenticating to Microsoft SharePoint

On a network connected computer:

1. Launch the **Browser**.
2. Navigate to `http(s)://<Virtual hostname>:<port>`
3. The browser will redirect to the point of contact being IBM Access Manager.
4. Enter the IBM Access Manager credentials for the user.
 - a. Username: **testuser1**
 - b. Password: **password1**

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

Troubleshooting

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

Collecting Support Data

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

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

https://www.ibm.com/support/knowledgecenter/SSPREK_9.0.2.1/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.

SharePoint Diagnostic Logging

Access Manager Claims configuration automatically outputs trace to SharePoint's log files.

1. On the Central Administration Home page, click **Monitoring**.
2. Click **Configure diagnostic logging**.
3. Expand the All Categories **web application** and set the additional settings as required.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

*IBM Corporation
224A/101
11400 Burnet Road*

Austin, TX 78758 U.S.A.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

Trademarks

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

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

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

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

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

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

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

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



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

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

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

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