

IBM Federation Identity Manager for Microsoft Office 365 'Active Profile' 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 Federation Identity Manager for Microsoft Office 365 and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation 2014.

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

Contents

Chapter 1: Introducing the integration.....	5
Introduction	5
Software Requirements	6
IBM.....	6
Microsoft	6
Chapter 2: Getting Started	7
Preface	7
IBM Federated Identity Manager	7
Configure Federated Single Sign-on Federations.....	7
Configure Federated Single Sign-on Partners	8
Configure Trust Service.....	9
Installing and Configuring the Metadata Exchange (MEX) EndPoint	10
Installation	10
Configuration.....	10
Start Microsoft Office 365 MEX Module	10
Additional IBM Federated Identity Manager Configuration.....	11
IBM Security Access Manager.....	11
Creating and Attaching an Unauthenticated ACL to FIM Trust Chain	11
Creating a Transparent Junction for the MEX Endpoint	11
Configuring WebSEAL for SPNEGO	12
Creating a Standard Junction for SPNEGO.....	12
Configuring the HTTP transformation Rule.....	13
Microsoft Office 365 Configuration	14
Convert a Microsoft Office 365 Domain to Support Federation Single Sign-on using PowerShell.....	14
Creating a user in Microsoft Office 365 using PowerShell.....	15
Testing the Integration.....	16
Passive Authentication.....	16
Active Authentication	16

Notices	17
Trademarks	19

Chapter 1: Introducing the integration

Introduction

Many organizations have made investments in traditional software installations, such as Microsoft Office. The purpose of this integration is to demonstrate how the single sign-on features of IBM Federated Identity Manager and Microsoft Office 365 can leverage the rich user experience of installed Microsoft Office applications while providing a seamless authentication between shared cloud documents. Authentication is done through the use of an on premise user identity, known as “Active” profile authentication.

This integration guide includes the process of configuring Microsoft Office 365 and IBM Federated Identity Manager.

Figure 1 provides an overview of the integration between IBM Federated Identity Manager and Microsoft Office 365.

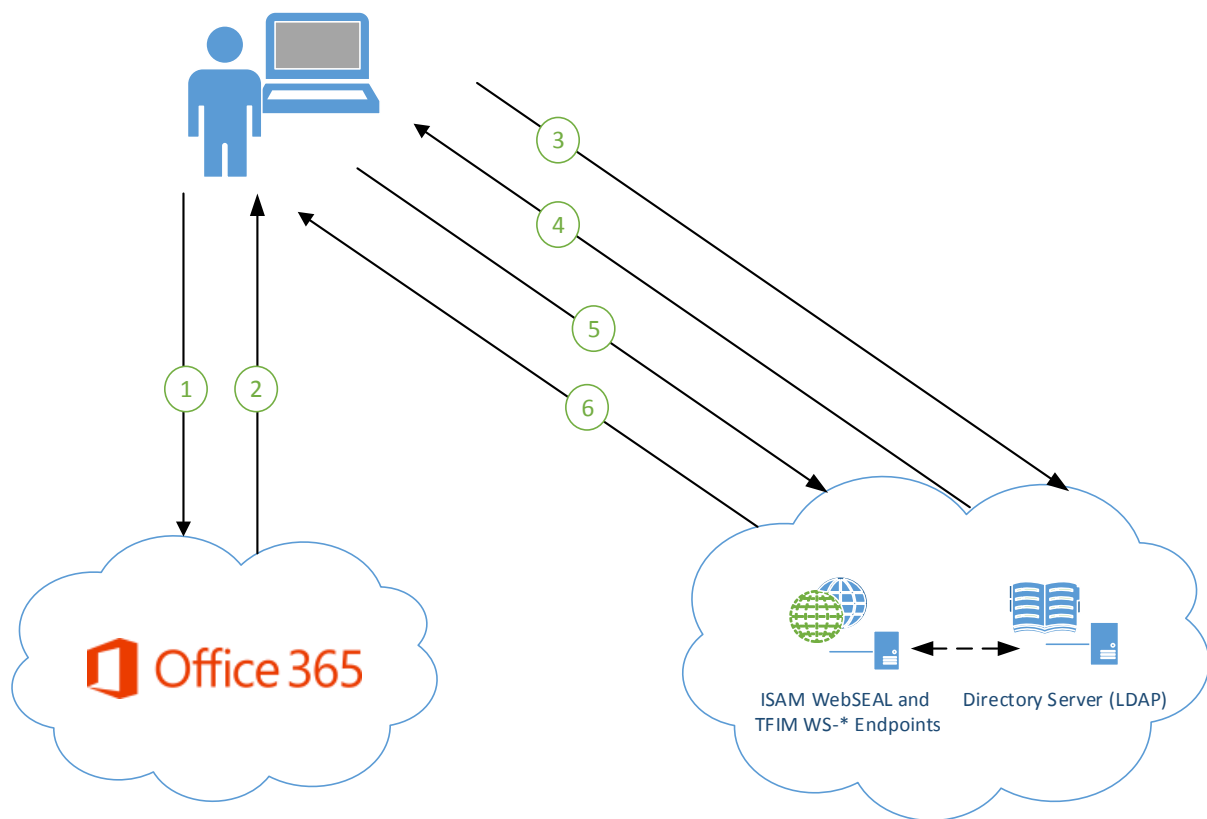


Figure 1 IBM Federated Identity Manager and Microsoft Office 365 Overview

The diagram illustrates the following process:

1. The client launches an Office application, the Single Sign-on Assistant will prompt the user for credentials if the user is not on the domain. The Single Sign-on Assistant requests the domain realm information from Office 365 tenant.
2. The Single Sign-on assistant receives the domain realm information. The realm information represents the Office 365 domain passive, active and MEX URI endpoints.
3. The Single Sign-on assistant sends a request to the MEX endpoint to determine the supported authentication depending on the user's network environment.
4. MEX information is returned to the Single Sign-on Assistant.
5. The Single Sign-on Assistant send a WS-Trust message to the active URI. The message will contain a Kerberos credential if the user is connected to the domain, otherwise a username password credential entered into the Single Sign-on Assistant. WebSEAL authenticates the request.
6. The FIM trust chain, constructs a SAML token and returns this to the Single Sign-On assistant.

Software Requirements

IBM

- IBM Federated Identity Manager 6.2.2.7
- IBM Security Access Manager 7.0 or later
- IBM WebSphere Application Server 8.5.0.0

Microsoft

- Windows Azure Active Directory Module for Windows PowerShell
- Microsoft Online Services Sign-in Assistant
- Microsoft Office 2013 or Microsoft Office Professional Plus 2010

Chapter 2: Getting Started

Preface

The environment used in this guide is IBM Security Access Manager (WebSEAL) as the internet facing reverse proxy. Behind WebSEAL is IBM Federated Identity Manager. The configuration steps use placeholders which require substitution to represent your own host and server names, as follows:

IBM Security Access Manager (WebSEAL): `isam.ibm.com`

IBM Federated Identity Manager (FIM): `fim_server`

IBM Federated Identity Manager

Configure Federated Single Sign-on Federations

These steps define Federated Identity Manager as the Identity Provider (Idp) using WS-Federation Passive Profile.

1. Expand Tivoli Federated Identity Manager from the WebSphere Integrated Solution Console.
2. Select **Federations** and click **Create**.
3. Enter a Federation Name and select **Identity Provider**, then click **Next**.
4. Enter a Company Name and its contact information (optional), then click **Next**.
5. Select **WS-Federation Passive Profile** and click **Next**.
6. Enter your Point of Contact. The Point of Contact is the URL to your WebSEAL host. For example: <https://<isam.ibm.com>/FIM> (refer note), click **Next**.
7. Select **Default SAML 1.1 Token** and click **Next**.
8. Accept the default security token values and click **Next**.
9. Select **Use XML or JavaScript transformation for identity mapping** and click **Next**.
10. Browse to the location of `FIM.Office365.Passive.MappingRule.js` in the Microsoft Solution package.
11. Update the JavaScript variable `office365Domain` to a verified domain in Microsoft Office 365 and save the file.
12. Select the updated file, then click **Next**.
13. Review your configuration on the summary screen, click **Finish**.
14. To load the federation configuration, click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

NOTE: The Tivoli Access Manager Configuration Tool creates WebSEAL junctions and ACL permissions that map to FIM federation endpoints. The tool should to execute each time a new federation is created. The tool is available from Federation link.

Configure Federated Single Sign-on Partners

These steps define Microsoft Office 365 as a service provider partner used by the federation identity provider.

1. Expand Tivoli Federated Identity Manager from the WebSphere Integrated Solution Console.
2. Select **Partners** and click **Create**.
3. Select the name of the newly created federation and click **Next**.
4. Enter a Company Name and its contact information (optional), then click **Next**.
5. Configure WS-Federation by using the following data then click **Next**.
 - a. **WS-Federation Realm**: urn:federation:MicrosoftOnline
 - b. **WS-Federation EndPoint (refer note)**: <https://login.microsoftonline.com/login.srf>
 - c. **Maximum Request Lifetime**: -1 (default value)
6. From the keystore, select the certificate for signing the SAML security token and click **Next**.
7. Select **Use XSL or JavaScript transformation for identity mapping** and click **Next**.
8. No XSL or JavaScript file is required, click **Next**.
9. Review the configuration summary and click **Finish**.
10. To complete the federation partner, click **Enable Partner**.
11. To load the partner configuration, click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

NOTE: An SSL certificate from a trusted certificate authority must be installed using IBM Key Management and set at the WebSEAL default certificate.

Refer to http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc_6.0/rev/am60_webseal_admin158.htm?path=5_12_0_8_1_6_0_6_0_2_1_8_0_3_2_0#wq564

Configure Trust Service

These steps configure a trust chain in Federated Identity Manager required by Microsoft Office client application. The trust chain is a series of mapping modules to validate an incoming request, transform or map the request data and issue a SAML token.

1. Expand Tivoli Federated Identity Manager from the WebSphere Integrated Solution Console.
2. Select **Trust Service Chains** and click **Create**.
3. At the Introduction screen, click **Next**.
4. Enter a Chain Mapping Name and optionally a description, click **Next**.
5. Configure Chain Mapping Lookup by using the following data then click **Next**.
 - a. **Request Type:** Issue
 - b. **AppliesTo Address:** urn:federation:MicrosoftOnline
 - c. **Issuer Address:** *
 - d. **Token Type:** No Token Type
6. At the Chain Identification, click **Next**.
7. Chain Assembly requires 3 modules.
 - a. In **Module Instance**, select **Default Username Token**.
 - b. In **Mode**, select **Validate**.
 - c. Click **Add selected module instance to chain**.
 - d. In **Module Instance**, select **Default Map Module**.
 - e. In **Mode**, select **Map**.
 - f. Click **Add selected module instance to chain**.
 - g. In **Module Instance**, select **Default SAML 1.1 Token**.
 - h. In **Mode**, select **Issue**.
 - i. Click **Add selected module instance to chain**.
8. After you add the modules, click **Next**.
9. Configure the Username Token Module using the following data then click **Next**.
 - a. **Options for validating the password:** Use Tivoli Access Manager for authentication
 - b. **JAAS Login Context Alias:** WSLogin
 - c. **Amount of time the token is valid after being issued:** 300
10. Default Map Module, browse to the location of FIM.Office365.Active.MappingRule.js, click **Next**.
11. Configure the SAML Module by using the following data:
 - a. **Organization issuing the assertions:**
<https://<isam.ibm.com>/FIM/sps/<federationname>/wsf>
The federation name was set in step 3 of Configure Federated Single Sign-on Federations.
 - b. **Time before the issue date that an assertion is considered valid:** 60
 - c. **Time the assertion is valid after being issued:** 60
 - d. Select certificate from the keystore for signing the SAML security token.
12. Click **Next**.
13. Review your configuration on the summary screen, click **Finish**.

14. To load the trust chain configuration, click **Load configuration changes to Tivoli Federated Identity Manager runtime.**

Installing and Configuring the Metadata Exchange (MEX) EndPoint

You must install an enterprise application in the WebSphere Integrated Solutions Console, to expose the MEX endpoint to the Microsoft Office 365 “active” requests. Complete the following installation and configuration procedures.

Installation

1. Log on to the WebSphere Integrated Solution Console.
2. Select **Applications > Application Type.**
3. Click **WebSphere enterprise applications.**
4. Click **Install.**
5. Browse to the file location of `MsMexEndpoint.ear` and click **Next.**
6. Accept the default settings and click **Next**
7. Specify Microsoft Office 365 MEX as the Application name and click **Next.**
8. Select the **MxEndpointWar module** and click **Next.**
9. At the Metadata for modules page, click **Next.**
10. At the Summary page, click **Finish** to start the installation.
11. Upon completion, click **Manage Applications.**

Configuration

1. From the list of applications, click **Microsoft Office 365 MEX.**
2. Under Web Module Properties, click **Initialize parameters for servlets.**
3. Enter the name of the point of contact created in step 6 of Configure Federated Single Sign-on Federations as the parameter `@POINTOFCONTACT@`. For example: <https://<isam.ibm.com>/FIM> and click **OK.**
4. Click **Save** to apply the changes to the master configuration.

Start Microsoft Office 365 MEX Module

1. From the list of application, select **Microsoft Office 365 MEX.**
2. Click **Start.**

Additional IBM Federated Identity Manager Configuration

1. Browse to the location <drive>:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps\<machinename>Node01Cell\ITFIMRuntime.ear
2. Make a copy of **com.tivoli.am.fim.war.sts.handlers.jar**
3. Browse to the location of com.tivoli.am.fim.war.sts.handlers.jar in the Microsoft Solutions package
4. Copy com.tivoli.am.fim.war.sts.handlers.jar to <drive>:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps\<machine-name>Node01Cell\ITFIMRuntime.ear
5. Accept the overwrite of the existing com.tivoli.am.fim.war.sts.handlers.jar file
6. Restart the WebSphere instance

IBM Security Access Manager

Creating and Attaching an Unauthenticated ACL to FIM Trust Chain

1. Login via the **pdadmin** tool.
2. Execute `acl create unauth`
3. Execute `acl modify unauth set any-other Trx`
4. Execute `acl modify unauth set unauthenticated Tr`
5. Execute `acl attach /WebSEAL/<object>/FIM/TrustServerWST13 unauth`

Creating a Transparent Junction for the MEX Endpoint

The following steps create a new transparent path junction. The junction is used by Office 365 to active client endpoints. The junction must have unauthenticated ACL attached created above.

1. Login via the **pdadmin** tool.
2. Execute: `server task <webseal-instance> create -t tcp -p 9080 -h <isam.ibm.com> -v <fim_server> -x /WST13`
3. Execute `acl attach /WebSEAL/<object>/WST13 unauth`

Test access to the MEX endpoint by navigating your browser to:

<https://<isam.ibm.com>/WST13/mex>

Configuring WebSEAL for SPNEGO

For domain connected client, WebSEAL needs to be configured to support SPNEGO authentication and an XSLT transformation rule. The following steps provide desktop single sign-on support for domain connected clients.

Refer to the IBM Access Manager Administration guide applicable to your version of WebSEAL.

- IBM Security Access Manager for Web 8.x.x.x
http://www-01.ibm.com/support/knowledgecenter/SSPREK_8.0.0.4/com.ibm.is-amw.doc_8.0.0.4/wrp_config/concept/con_config_win_desktop_sso_unix.html
- IBM Security Access Manager for Web 7.x.x.x
http://www-01.ibm.com/support/knowledge-center/SSPREK_7.0.0.1/com.ibm.isam.doc_80/ameb_web-seal_guide/task/tsk_config_win_desktop_sso.html

Creating a Standard Junction for SPNEGO

The following steps create a new standard junction. The effective ACL permission assigned to the new junction is the authenticated ACL, default-webseal.

1. Login via the **pdadmin** tool.
2. **Execute:** `server task <webseal-instance> create -t tcp -p 9080 -h <isam.ibm.com> -v <fim_server> -c -iv-user,iv-groups,-iv-creds /spnego`

Configuring the HTTP transformation Rule

The following steps create a new pop for the HTTP transformation rule. The transformation rule file, `Isam.Office365.Rule.xslt` can be found in the solution package accompanying this guide. This file needs to reside on the WebSEAL server. Once the pop is created, attach the pop to the WebSEAL junction representing the FIM trust chain, typically `TrustServerWST13`.

1. Login via the **pdadmin** tool.
2. Execute `pop create office365-win`
3. Execute `pop modify office365-win set attribute HTTPTransformation Request=Office365`
4. Execute `pop attach /WebSEAL/<object>/FIM/TrustServerWST13 office365-win`
5. Open `<webseal-instance>.conf` file
6. Find the stanza [**http-transformations**]
7. Amend the section, adding the following entry `office365-win = <file-location>/Isam.Office365.Rule.xslt`
8. Save the conf file and restart the Security Access Manager WebSEAL-<instance> Windows Service (Windows based installations).

NOTE: The name of the standard junction described above (`/spnego`) matches the junction name for redirection in `Isam.Office365.Rule.xslt`.

Microsoft Office 365 Configuration

Prior to executing the PowerShell commands for establishing a federated domain, a registered domain and active Office 365 licensing is required. Obtaining a domain and Office 365 licensing is beyond the scope of this integration guide. The following commands requires the Windows Azure Active Directory Module for Windows PowerShell installed.

Obtain the setup from:

<http://technet.microsoft.com/en-us/library/hh974317.aspx>

Convert a Microsoft Office 365 Domain to Support Federation Single Sign-on using PowerShell

Once a domain has been verified in the Microsoft Office 365 Administration portal, it can be configured for federated single sign-on. The following PowerShell script configures the domain using the IBM Security Federated Identity Manager settings executed above.

NOTE: The SAML signing certificate selected in the Federated Identity Manager federation configuration is to be exported to a text file. The \$cert value represents the lines of text between --BEGIN CERTIFICATE-- and --END CERTIFICATE--. Ensure that linefeeds are remove, resulting in a single line representation of the certificate.

1. Open the Windows Azure Active Directory Module for Windows PowerShell.
2. Type **connect-msolservice**.
3. Enter Microsoft Office 365 credentials.
4. In the PowerShell command windows, enter the following lines. Replace the placeholder variables with the actual values:

```
a. $domainname = "<the name of the Office 365 domain>"
b. $brandname = "IBM Security"
c. $fimuri = "https://<isam.ibm.com>/FIM/sps/<federation-
  name>/wsf"
d. $mexuri = "https://<isam.ibm.com>/WST13/mex"
e. $activeuri = "https://<isam.ibm.com>/FIM/Trust-
  ServiceWST13/services/RequestSecurityToken"
f. $cert = "MIICBzCCAXCgAwIBAgIEQH26vjANBgkqhkiG9 ... "
g. Set-MsolDomainAuthentication
   -DomainName $domainname
   -FederationBrandName $brandname
   -Authentication Federated
   -SigningCertificate $cert
   -IssuerUri $fimuri
   -PassiveLogOnUri $fimuri
   -LogOffUri $fimuri
   -ActiveLogOnUri $activeuri
   -MetadataExchangeUri $mexuri
```

See <http://technet.microsoft.com/en-us/library/dn194112.aspx> for more information about this command.

Creating a user in Microsoft Office 365 using PowerShell

Microsoft requires a unique and immutable identifier for the SAML token that is passed back from the identity provider.

For this integration, the user name is used as the immutable identifier. In this example, testuser2 is a valid IBM Security Access Manager user. After completing the procedures for configuring a federation, partner and trust chain that require a transformation mapping, JavaScript inserts the user name as the immutable identifier. The following PowerShell creates a user, setting the immutable identifier as the user name.

NOTE: Run `Get-MsolAccountSku` to obtain the account sku.

1. Open the Windows Azure Active Directory Module for Windows PowerShell.
2. Type **connect-msolservice**, enter Office 365 credentials.
3. In the PowerShell command windows, enter the following lines substituting the placeholders for actual values:

```
a. $displayname= "Clark Kent"
b. $upn = "testuser2@<the name of the Office 365 domain>"
c. $firstname = "Clark"
d. $lastname = "Kent"
e. $immutableId = "testuser2"
f. New-MsolUser
    -DisplayName $displayname
    -UserPrincipalName $upn
    -FirstName $firstname
    -LastName $lastname
    -ImmutableID = $immutableId
    -BlockCredential $false
    -UsageLocation "<location of the user>"
    -LicenseAssignment "<your account sku id>"
```

You can pass additional fields to this PowerShell command. See the following link for more information: <http://technet.microsoft.com/en-us/library/dn194096.aspx>

Testing the Integration

Passive Authentication

The following steps test the configuration of the Federated Identity Manager single sign-on federation and partner settings.

NOTE: Replace the placeholder variables with the PowerShell configured values.

1. Open a web browser and navigate to `https://login.microsoftonline.com/`.
2. Enter `testuser2@<the name of the Office 365 domain>`. Microsoft Office 365 redirects you to the IBM Security Identity Manager for user authentication.
3. In the user name field, enter `testuser2`.
4. In the password field, enter the IBM Security Access Manager password for `testuser2` and click **Submit**. The browser is redirected back to Microsoft Office 365 with the SAML token in the POST.

Active Authentication

The following steps test the configuration of the Federated Identity Manager trust chain using a Microsoft Office application and the Microsoft Single Sign-on Assistant.

NOTE: Replace the placeholder variables with the PowerShell configured values.

1. Open Microsoft Word 2013.
2. Sign in to the application.
3. Enter the email address of the user, `testuser2@<the name of the Office 365 domain>`, click **Next**
4. In the password field, enter the IBM Security Access Manager password for `testuser2` and click **Sign in**. Your user name is displayed on the top right of the application.

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® 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.