

IBM® Security Federated Identity Manager
for Versions 6.2.2

IBM Security Federated Identity Manager for Microsoft Office 365 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 Federated Identity Manager for Microsoft Office 365 and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2014, 2017.**

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

Contents

PREFACE	5
Access to publications and terminology	5
Publication Library	5
IBM Terminology website	6
Accessibility	6
Technical Training	6
Support information	7
Statement of Good Security Practices	7
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
IBM SECURITY FEDERATED IDENTITY MANAGER CONFIGURATION	10
Configuring the Federation Provider (IdP)	10
Configuring the Federation Service Partner (SP)	11
Federation Runtime Configuration	11
Configuring IBM Security Access Manager for Federations	12
Configuring the Alias Service for Federations	12
SIGNING CERTIFICATE CONFIGURATION	13
Export the certificate from IBM Federated Identity Manager	13
Import the certificate into the Microsoft Certificate Store	13
Export the certificate from Microsoft Certificate Store	13
OFFICE 365 CONFIGURATION	14
Creating a Federated Domain	14
TESTING THE INTEGRATION	15
Before you start	15
Security Access Manager for Web configuration	15
User Account Creation	15

Authenticating to Microsoft Office 365 via the Browser	16
Authenticating to Microsoft Office 365 via Office Client	16
TROUBLESHOOTING	17
Collecting Support Data	17
Security Access Manager for Web trace	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.

Integration Guide

- *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.

Federation Information

- *IBM Security Federation Manager Installation Guide*

Describes how to manage, configure, and deploy an existing IBM Security Federated Identity Manager environment.

- *IBM Security Federation Manager Administration Guide*

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

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

This Federated Identity Redbook covers important aspects of using IBM Security integrated identity management architecture to build and deploy the IBM Security Federated Identity Manager and Web Services 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.

Introducing the Integration

Introduction

IBM Security Federated Identity Manager manages the generation of the SAML token that is used to perform single-sign-on (SSO). The user identity can be sourced from IBM Security Access Manager.

The following figure shows the typical sequence of steps that are involved in performing a SAML single sign-on to Microsoft Office 365 using “Modern Authentication”.

This integration pattern refers to IBM Security Access Manager as a Point of Contact for IBM Security Federated Identity Manager.

Integration Architecture

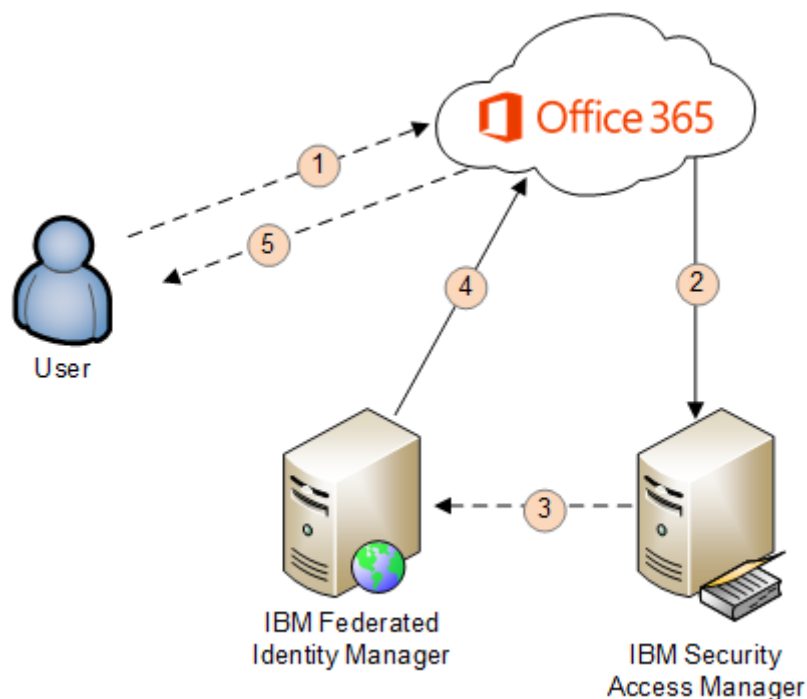


Figure 1: SAML sign-in sequence

1. The user opens a web browser and navigates to <https://login.microsoftonline.com>.
2. The user enters their on-premises email address which is validated by Microsoft. The configured settings for the domain in Office 365 redirects the user to Security Access Manager acting as the Point of Contact for IBM Federated Identity Manager.
3. The user enters their on-premises username and password. Security Access Manager for Web validates the user credentials against a directory service (LDAP) and routes the request to SPS junction for IBM Federated Identity Manager.
4. IBM Federated Identity Manager requests from the Alias Service the ImmutableID of the authenticated user that correspond to the federation name and partner name. IBM Federated Identity Manager performs a POST of the SAML token to Office 365.

- Office 365 validates the SAML token and redirects the browser to the Office 365 landing page.

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
fim_saml2_office365_guide.pdf	This integration guide.
Samples\Microsoft Office 365\FIM.Saml2.Office365.Mapping.Rult.xslt	Example XSLT mapping rule to include additional claims into the SAML token.

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
- IBM Federated Identity Manager
 - Deployed to a WebSphere Application Service
 - An IBM Federated Identity Manager domain is configured and the runtime deployed to the domain.
 - Point of Contact server is configured to Access Manager.
 - Alias service configured.
- Microsoft Office 365
 - An active subscription to Office 365
 - An internet domain and the domain added to the Office 365 tenant
 - Installed Windows Azure Active Directory Module for Windows PowerShell. Refer to:

<https://support.office.com/en-us/article/Managing-Office-365-and-Exchange-Online-with-Windows-PowerShell-06a743bb-ceb6-49a9-a61d-db4ffdf54fa6>

IBM Security Federated Identity Manager Configuration

Configuring the Federation Provider (IdP)

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Configure Federated Single Sign-on**.
3. Select **Federations**.
4. In the **Federations** section, click **Create...**
5. In the **General Information** section, enter a **Federation Name** and select **Identity Provider** role option. Click **Next**.
6. In the **Contact Information** section, enter the **Company Name**. The remaining fields are optional. Click **Next**.
7. In the **Federation Protocol** section, select **SAML 2.0**. Click **Next**.
8. In the **Point of Contact Server** section, enter the **URL** of the point of contact. If IBM Security Access Manager is being used, this is the URL of the /FIM junction on WebSEAL (For example <https://webseal.isam.com/FIM>). The /FIM junction is described in Configuring IBM Security Access Manager for Federations, refer *page 12*. Click **Next**.
9. In the **Profile Selection** section, select **Basic: Web Browser SSO, Single Logout**. Click **Next**.
10. In the **Signature Options** section, set the following properties
 - a. Uncheck **Require signature on incoming SAML messages and assertion**.
 - b. Select **Typical set of outgoing messages and assertions are signed**.
 - c. Select **Keystore**.
 - d. Enter the **Keystore** password (DefaultKeystore password is testonly). Click **List Keys**.
 - e. Select the **Alias** key to use.Click **Next**.
11. In the **Encryption Options** section, select **Keystore**.
12. Enter the **Keystore** password (DefaultKeystore password is testonly). Click **List Keys**.
13. Select the **Alias** key to use. Click **Next**.
14. In the **SAML Messages Settings** section, click **Next**.
15. In the **SAML Assertion Settings** section, click **Next**.
16. In the **Identity Mapping Options**, select **Use XSLT or JavaScript transformation for identity mapping**. Click **Next**.
17. Browse to the XSLT mapping file in the Examples folder location. You will need to modify this file to represent the user's email address from extended attributes configured in IBM Security Access Manager to be asserted into SAML token to Office 365. Click **Next**.
18. On the **Summary** page, click **Finish**.
19. Click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

Configuring the Federation Service Partner (SP)

You must create a partner to associate with the federation created. The partner for this integration is Microsoft Office 365. Download the Office 365 metadata XML file before creating the federation service partner. Refer to:

<https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Configure Federated Single Sign-on**.
3. Select **Partners**
4. In the **Federation Partners** section, click **Create...**
5. In the Select Federation section, select the Federation Name created in Configuring the Federation Provider (IdP), refer *page 10*. Click **Next**.
6. In the **Import Metadata** section, click **Browse** and select the metadata file. Click **Next**.
7. In the **Signature Validation** section, set the following properties
 - a. Select **No incoming SAML message and assertions are signed**.
 - b. Select a **Keystore** to save the partner public key.
 - c. Enter the **Keystore** password (DefaultKeystore password is testonly).

Click **Next**.

8. In the **SSL Client Authentication for Artifact Resolution**, section. Click **Next**.
9. In the **Partner Settings**. Click **Next**.
10. In the **SAML Assertion Settings** section. Click **Next**.
11. In the **Identity Mapping Options**, select **Use XSLT or JavaScript transformation for identity mapping**. Click **Next**.
12. Browse to the XSLT mapping file, this is optional. Click **Next**.
13. On the **Summary** page, click **Finish**.
14. Click **Enable Partner if prompted**.
15. Click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

Federation Runtime Configuration

Microsoft Office 365 does not support several SAML elements in the response from IBM Security Federation Manager. A runtime configuration property is provided to enable federations to Microsoft Office 365.

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Domain Management**.
3. Select **Runtime Node Management**.
4. Click **Runtime Custom Properties**.
5. Click **Create...**
6. Enter the following Name and Value:
 - o Name: `SAML20.IncludeInclusiveNamespaces%<FEDERATIONID>%<PARTNERID>`
 - o Value: `false`

Note: The **<FEDERATIONID>** placeholder is the WS-Federation Realm value in the federation configuration. The **<PARTNERID>** placeholder is the WS-Federation Realm in the partner configuration.

For example:

```
SAML20.IncludeInclusiveNamespaces%http://webseal.isam8.com/FIM/sps/AccessManager/saml20%urn:federation:MicrosoftOnline
```

7. Click **OK**
8. Click **Load configuration changes to Tivoli Federated Identity Manager runtime.**

For more information on this runtime custom property, refer to:

<https://download4.boulder.ibm.com/sar/CMA/TIA/05ns0/1/6.2.2-TIV-TFIM-FP0016.README-notoc.html>

Configuring IBM Security Access Manager for Federations

IBM Security Federated Identity Manager provides a command line utility to assist with creating the standard /FIM junction in IBM Security Access Manager.

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Configure Federated Single Sign-on**.
3. Select **Federations**
4. Click **Download Tivoli Access Manager Configuration Tool**.
5. Save **tfimcfg.jar**.

For guidance on running the Tivoli Access Manager Configuration Tool, refer to:

https://www-304.ibm.com/support/knowledgecenter/SSZSXU_6.2.2.7/com.ibm.tivoli.fim.doc_6227/config/task/usin_gtfimcfgISAM7.html?lang=en

Configuring the Alias Service for Federations

The integration with Office 365 using the SAML 2 protocol relies on a persistent name identifier which is the Alias Service feature in IBM Security Federated Identity Manager. Microsoft Office 365 requires an ImmutableID value to that corresponds to an on-premises user.

Further information for determining the ImmutableID strategy is referenced here:

http://www-01.ibm.com/support/knowledgecenter/#!/SSZSXU_6.2.2.6/com.ibm.tivoli.fim.doc_6226/sse/fed_first_steps/con_ffs_office_upn_uuid.html%23abouttheupnnamingconvention

Signing Certificate Configuration

When setting up the trust between IBM Federated Identity Manager and Office 365, we need to import a certificate used by IBM Federated Identity Manager. The certificate in IBM Federated Identity Manager cannot be exported in a format that can be imported directly into Office, therefore we need to complete the following steps:

- Export the certificate from the IBM Federated Identity Manager Keystore. The certificate must be 2048bit.
- Import the certificate into the Microsoft Certificate Store.
- Export the certificate from the Microsoft Certificate Store

Export the certificate from IBM Federated Identity Manager

1. On the WebSphere console, click **Tivoli Federated Identity Manager**.
2. Select **Configure Key Service**.
3. Select **Keystores**.
4. Select the **Keystore Name** that containing the signing/encryption key.
5. Click **View Keys...**
6. Enter the **Keystore** password (Default Keystore password is testonly).
7. Select the **Alias** to export.
8. Click **Export...**
9. Select **PKCS#12** export format.
10. Click **Download Key**.
11. Save the file.

Import the certificate into the Microsoft Certificate Store

1. Locate the file from Export the certificate from IBM Federated Identity Manager *step 11*
2. Right click the file, click **Install PFX**.
3. The **Certificate Import Wizard** will appear, select **Current User** as the **Store Location**.
4. Click **Next**.
5. On the **File to Import** page, click **Next**.
6. Enter the **password** for the key, this will be the same password used to access the Keystore from IBM Federated Identity Manager (For example, testonly). Click **Next**.
7. Select location to store the certificate, click **Next**.
8. Click **Finish**.

Export the certificate from Microsoft Certificate Store

After importing the certificate into the Microsoft Certificate Store, we need to export in the format that can be read by SharePoint. The Microsoft Certificate Store is accessed through the Microsoft Management Console (MMC) snap-in.

1. From the Start Menu, select **Run**.
2. Type `mmc`, click **OK**
3. Select the **File** → **Add/Remove Snap-in...**
4. Select **Certificates**, then click **Add**.
5. The Certificate snap-in dialog will appear, select **My user account**, click **Finish**.
6. Click **OK**.
7. Under **Certificates – Current User**, expand **Trusted Root Certification Authority** → **Certificates**.
8. Select the certificate imported from Import the certificate into the Microsoft Certificate Store.
9. Right click the certificate **All Tasks** → **Export...**
10. The **Certificate Export Wizard** will appear, click **Next**.

11. Select the Export file format as **Base-64 encoded X.506 (.CER)**, click Next.
12. Enter a file name, click **Next**.
13. Click **Finish**.

Office 365 Configuration

Creating a Federated Domain

Once a domain has been verified in the Microsoft Office 365 Administration portal, it can be configured for federated single sign-on.

1. On the Windows Azure Active Directory Module for Windows PowerShell.
2. Type **connect-msolservice**.
3. Enter the administrator credentials for Microsoft Office 365.
4. In the PowerShell command window, enter the following, replacing the **<placeholder>** variables with actual values of your environment.

```
$domainName = "<name of your Office 365 domain>"  
$brandName = "IBM Security"  
$logonUrl = Error! Hyperlink reference not valid.  
$issuerUri = Error! Hyperlink reference not valid.  
$logoffUri = Error! Hyperlink reference not valid.  
$cert = This is the base64 encoded certificate generated from Export the certificate from  
Microsoft Certificate Store refer page 13.
```
5. Execute the following PowerShell command to create the Office 365 federated domain.

```
Set-MsolDomainAuthentication -DomainName $domainName -PassiveLogOnUri  
$logonUrl -ActiveLogOnUri $logonUrl -IssuerUri $issuerUri -  
SigningCertificate $cert -LogOffUri $logoffUri -Authentication  
"federated" -PreferredAuthenticationProtocol SAML -  
FederationBrandName $brandName
```

Enable Modern Authentication for Office 2013 on Windows

Office 2013 clients require a registry key update to enable the SAML v2 authentication "modern authentication". Refer to:

<https://support.office.com/en-us/article/Enable-Modern-Authentication-for-Office-2013-on-Windows-devices-7dc1c01a-090f-4971-9677-f1b192d6c910>

Testing the Integration

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 Manger 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.

Authenticating to Microsoft Office 365 via the Browser

On a network connected computer:

1. Launch the **Browser**.
2. Navigate to <https://login.microsoftonline.com>
3. Enter the email address of the Office 365 user
4. The browser will redirect to IBM Access Manager.
5. Enter the IBM Access Manager credentials for the user
 - a. Username: **testuser1**
 - b. Password: **password1**
6. IBM Access Manager forwards the request to IBM Federated Identity Manager
7. IBM Federated Identity Manager requests the ImmutableID value from the Alias Service for the user and executes a POST of the SAML token to Microsoft Office 365.

The expected response is the default web page for Microsoft Office 365 with the user name displayed in the top right corner.

Authenticating to Microsoft Office 365 via Office Client

On a network connected computer:

1. Launch an Office 2013 client application (for example Microsoft Word).
2. Click **Sign in** in the top right corner of the application.
3. On the Sign in dialog, enter the e-mail address of the Office 365 user. Click **Next**.
4. The dialog displays the IBM Security Access Manager log in page.
5. Enter the IBM Access Manager credentials for the user
 - a. Username: **testuser1**
 - b. Password: **password1**
6. The dialog will close on successful Office 365 authentication.

The expected response is the Office 2013 application will display the authenticated user in the top right corner of the application.

Troubleshooting

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

Collecting Support Data

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

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

http://www-01.ibm.com/support/knowledgecenter/SSELE6_8.0.1.3/com.ibm.isam.doc/admin/task/alps_managing_support_files.html

Security Access Manager for Web trace

pdweb.debug

The `pdweb.debug` trace will assist in identifying errors related to authentication to Security Access Manager and Microsoft Internet Information Services. To enable tracing:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the `pdweb.debug` row.
6. Click **Edit**.
7. In the Edit Trace Component window:
 - a. Level: **2**
 - b. Flush Interval (seconds): **5**
 - c. Rollover Size (bytes): <default>
 - d. Click **Save**.

To disable trace, set the Level to 0.

To review the trace file generated:

1. Open the Web Gateway Appliance Web console.
2. Select **Secure Web Settings** → **Reverse Proxy**.
3. Select the reverse proxy instance to configure.
4. Select **Manage** → **Troubleshooting** → **Tracing**.
5. Select the `pdweb.debug` row.
6. Click **Files**.
7. In the Manage Trace Files – `pdweb.debug` window
 - a. Select **pdweb.debug.log**
 - b. Click **View**
 - c. Number of lines to view: **1000** (depending on the number of requests)
 - d. Click **Reload**

The trace file may also be exported and viewed external to the appliance.

Notices

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

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

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

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

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

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

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

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

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

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

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

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

*IBM Corporation
224A/101
11400 Burnet Road*

Austin, TX 78758 U.S.A.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

© IBM 2017. Portions of this code are derived from IBM Corp. Sample Programs. ©Copyright IBM Corp 2014, 2017. All rights reserved.

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

Trademarks

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

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

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

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

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

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

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

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



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

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

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

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