

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

IBM Security Access Manager for Microsoft Internet Information Services Integration Guide



Note

Before using this information and the product it supports, read the information in 'Notices' on page 19

This edition applies to Version 1.8 release i of the IBM Security Access Manager for Microsoft Internet Information Services 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	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	10
MICROSOFT INTERNET INFORMATION SERVICES CONFIGURATION	11
Installing the Impersonation Module	11
Configuring the Impersonation Module	11
Configure the Web Application	12
Application Pool Settings	12
IBM SECURITY ACCESS MANAGER CONFIGURATION	13
Web Gateway Appliance Configuration	13
Authentication Mechanism	13
Junction Management	13
WebSEAL Configuration	14
Authentication Mechanism	14
Junction Creation	14
TESTING THE INTEGRATION	15
Before you start	15
Security Access Manager for Web configuration	15
User Account Creation	15
Junction Management	15

Microsoft Internet Information Services.....	16
TROUBLESHOOTING	17
Collecting Support Data	17
Security Access Manager for Web trace	17
Microsoft Internet Information Service Failed Request Trace.....	18
Uninstalling the Impersonation Module	18
NOTICES	19
TRADEMARKS	21

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

The IBM Security Access Manager Authentication Module is an integration module designed for Microsoft Internet Information Services version 7 and later. This module executes as a native module within Microsoft Internet Information Services.

The purpose of the authentication module is to intercept a prescribed HTTP header representing an Access Manager user and impersonate that as their corresponding Windows credential.

The impersonation occurs when the authenticate event is fired in the request pipeline. If impersonation succeeds, the Windows credential is consumed by the web application.

This document refers to the authentication module as the impersonation module.

Integration Architecture

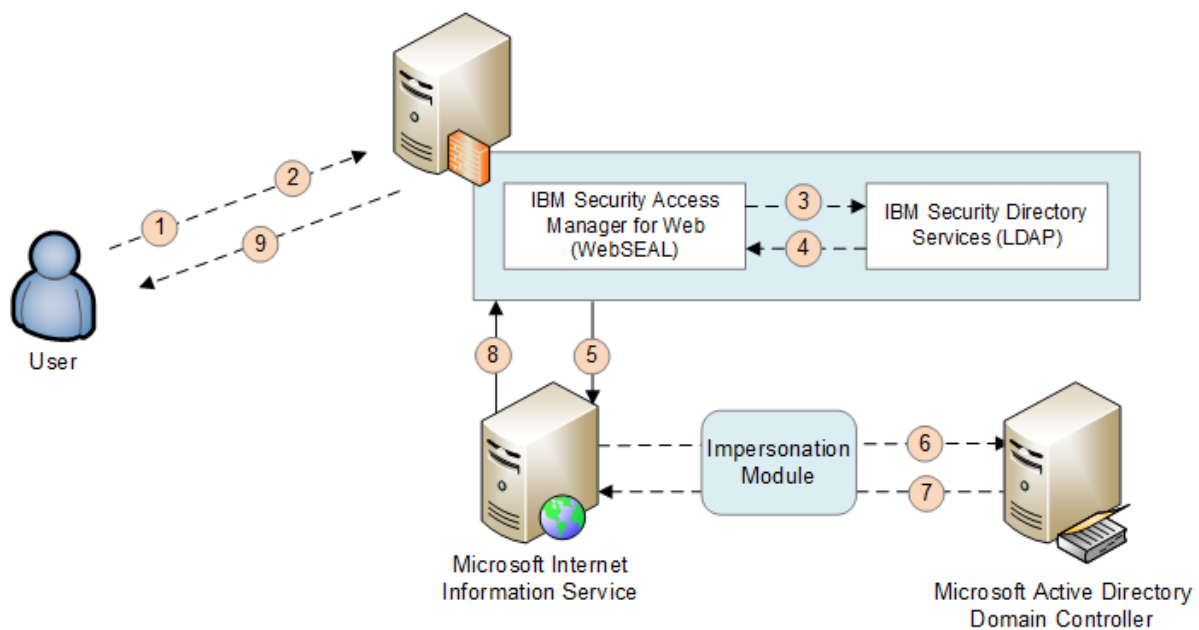


Figure 1: Impersonation Module for Microsoft Windows Authentication Integration Architecture

IBM Security Access Manager for Microsoft Internet Information Services shows the integration architecture with the following process for Single Sign:

1. The user requests content from a protected resource hosted on Microsoft Internet Information Services (IIS).
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 Microsoft Information Service via a configured junction.
6. The impersonation module is triggered by the authenticate event raised by the web site request. If the user header is present in the request, the header value is used to create a new Windows Logon session. The Windows logon session is created based on the user principal name (UPN) that correspond to the value in the Access Manager for Web header. If no header value is present, the module exits.
7. The impersonation user token is issued from the Active Directory domain controller and the user is set to the current request.
8. The web site response is passed back to Access Manager for Web.
9. Access Manager for Web passes the response back to the user.

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_iis_module_int_guide.pdf	This integration guide.
Solutions\Microsoft IIS\IBM.Security.Web.Authentication.dll	This file is the x64 native module that is loaded into Microsoft Internet Information Services for user impersonation
Solution\Microsoft IIS\IBM.Security.Web.AuthenticationClient.dll	This file is used to provide a configuration applet in Microsoft Internet Information Services.
Solution\Microsoft IIS\IBM.Security.Web.AuthenticationManagement.dll	This file is used by Microsoft Internet Information Services to read and write configuration changes to the web site using the native module.
Solution\Microsoft IIS\IsamAuthentication_schema.xml	This is the schema of the native module configuration used by Microsoft Internet Information Services.
Solution\Microsoft IIS\Isam.IIS.Deply.ps1	This is the PowerShell script to install or uninstall the schema and register the Microsoft Internet Information services client and management files.

Table 1: Integration Package contents

Before you start

The impersonation module and associated Microsoft Internet Information Services components require the following pre-installed operating system environments. Refer to the release notes for platform support.

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
- Web Server (Microsoft Internet Information Services) role installed with the following features;
 - Health and diagnostics
 - Security
 - Application development
 - Management tools (Microsoft Internet Information Services 6 management is not required for the native module)
- Microsoft Visual C++ 2013 Redistribution Package (x64)
<http://www.microsoft.com/en-us/download/details.aspx?id=40784>

Microsoft Internet Information Services Configuration

Installing the Impersonation Module

After you extract the compressed file, open a command prompt in Administrator mode.

1. At the command prompt, navigate to the folder location of the extracted files.
2. Type `PowerShell`
3. Type `.\isam.iis.deploy.ps1`
4. Type `execute -action install`

At this point, the client and management assemblies are registered with Microsoft Internet Information Services. The schema is deployed and the native module file has been copied to `%windir%\system32\inetsrv`.

Configuring the Impersonation Module

As part of the installation procedure, an applet is displayed in the Microsoft Internet Information Services console at a web site and web application (virtual directory) level to facilitate configuration of the impersonation module.

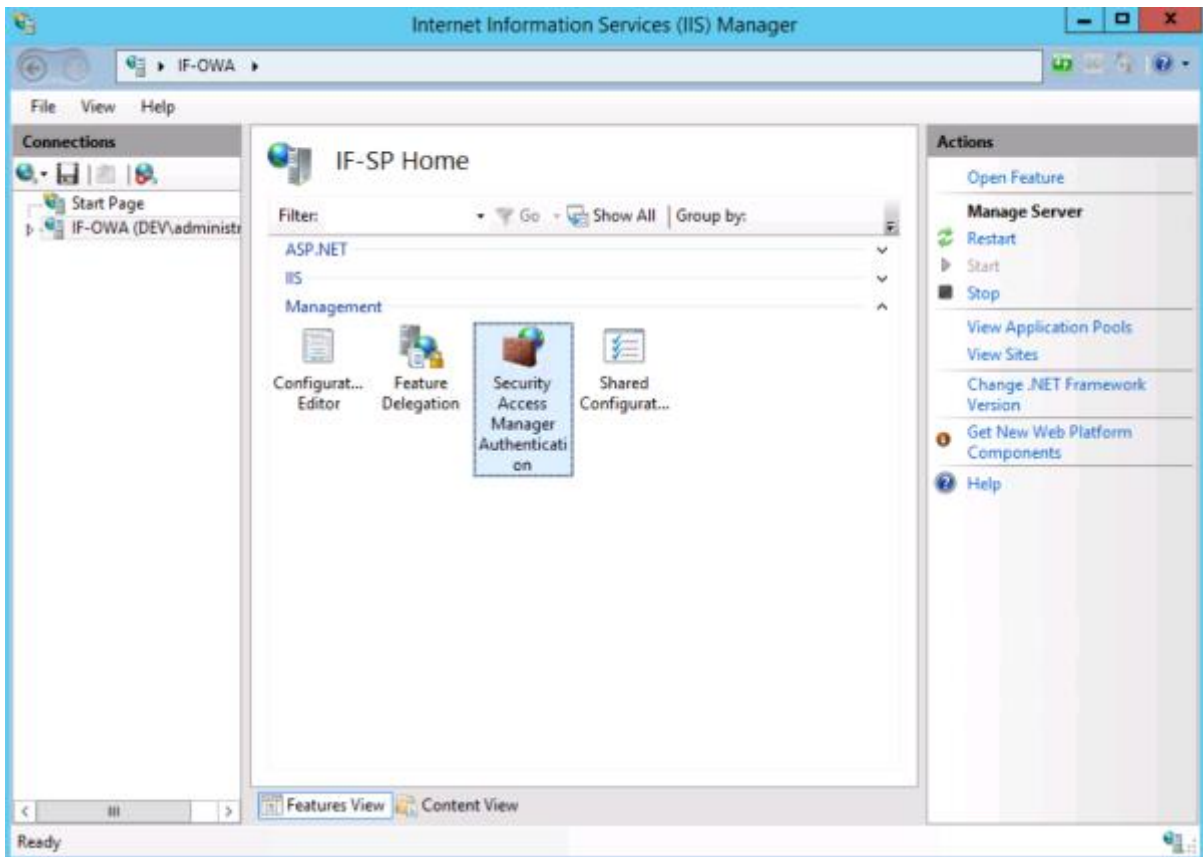


Figure 2: Impersonation Module Configuration Applet

1. Select the **Web Site** or **Virtual Directory** from the tree on the left.
2. Select **Security Access Manager Authentication** applet.
3. Click **Open Feature** from the Action pane on the right.
4. Enter a value for the **Domain Name**. Use a comma separated list to represent multiple domains in a forest. For example: test.domain.com
5. Enter a value for the **Header Name**. This value represents the name of the incoming header from Microsoft Internet Information Services. For example: IV-USER.
6. Click **Apply**.

Note: If a user has an account in multiple domains in a forest, the user is impersonated against the first Kerberos token issued for the user principal name (UPN).

Configure the Web Application

The impersonation module is used to impersonation a Windows user, therefore the web application hosted by Microsoft Internet Information Service needs to set a Windows Authentication.

If the web application was created via Microsoft SharePoint or Microsoft Exchange Outlook Web Access (OWA) the following steps are not required.

1. Select the **Web Site** or **Virtual Directory** from the tree on the left.
2. Select **Authentication** applet.
3. Click **Open Feature** from the Action pane on the right.
4. Select **Windows Authentication**, then click **Enable** from the Action pane on the right.
5. Select **ASP.NET Impersonation**, then click **Enable** from the Action pane on the right.

Application Pool Settings

The account that runs the ASP.NET web application process (w3wp.exe) requires a level of privilege to generate a Kerberos token on behalf of the incoming user. This can be achieved as follows:

- The application pool account is LocalSystem
- The application pool account has the 'Act as part of Operating System' privilege in the Local Security Policy. Refer to:

[https://technet.microsoft.com/en-us/library/cc784323\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc784323(v=ws.10).aspx)

IBM Security Access Manager Configuration

Complete the following configuration steps on Web Gateway Appliance or WebSEAL for integration with IBM Security Access Manager for Microsoft Internet Information Services.

The **pdadmin** command-line utility can be used on the Web Gateway Appliance in addition to the graphical user interface of the Local Management Interface (LMI) for some of the integration steps.

Web Gateway Appliance Configuration

Complete the configuration steps on the IBM Security Access Manager for Web appliance to enable Single Sign On from the Mobile Enterprise Gateway.

Authentication Mechanism

The IBM Security Access Manager for Web Reverse Proxy instance must be configured to accept the authentication from the user.

In this example, the user is redirected to pkmslogin form for authentication to Microsoft Internet Information Services WebSEAL:

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 **Edit**.
5. Select the **Authentication** tab.
6. Under **Forms Authentication** → **Transport**, select **Both**.
7. Click **Save**.
8. Deploy the pending changes.
9. Restart the reverse proxy instance.

Junction Management

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center Junctions](#) page for details of each junction type.

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** → **Junction Management**.
5. Click **New** → **Standard Junction**.
Note: For Microsoft SharePoint and Microsoft Exchange web application the recommended junction is **Virtual Junction**.
6. Enter a **Junction Point Name** and select a **Junction Type**.
7. Select the **Servers** tab,
8. Click **New**.

9. Enter a **Hostname**, **Port** and select a **Local Address**. This is the address WebSEAL is hosted on.
10. Click **Save**.
11. Select the **Identity** tab.
12. Check **IV-USER**. This is the header name used in *Configuring* the Impersonation Module on page 11.
13. Click **Save**.
14. Deploy the pending changes.
15. Restart the reverse proxy instance.

WebSEAL Configuration

Complete the configuration steps on the IBM Security Access Manager WebSEAL server to enable user authentication in IBM Security Access Manager.

Authentication Mechanism

The IBM Security Access Manager WebSEAL instance must be configured to supply the authenticated user identity into a request header forwarded to Microsoft Internet Information Services.

The WebSEAL instance can be configured for Forms Authentication or Basic Authentication, both authentication mechanisms pass the IV-USER and IV-GROUP request headers to the backend.

Junction Creation

The selection of the most appropriate junctions for each environment is outside the scope of this integration. See the [IBM Security Access Manager Knowledge Center Standard WebSEAL junctions](#) and [IBM Security Access Manager Knowledge Center Virtual Hosting](#) pages for details of each junction type.

Once authenticated to Security Access Manager WebSEAL, downstream SSO to protected resources is achieved using a broad range of authentication mechanisms including existing Single Sign On patterns and integration adapters such as Trust Association Interceptor (TAI), Lightweight Third-Party Authentication (LTPA), Basic Authentication (GSO, -B, etc.), HTTP header (Kerberos, iv-creds, etc.) and Federation (using Tivoli Federated Identity Manager).

Testing the Integration

This sample uses Forms Based Authentication (FBA) to authenticate a user to IBM Security Access Manager WebSEAL. The user identity is forwarded to the web application via the request header IV-USER.

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** for the *Authentication Mechanism* on page 13.

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> create -t tcp -h localhost -p 80 -c iv-user /iis_sample
```

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

Microsoft Internet Information Services

Install and configure the Impersonation Module onto the machine running Microsoft Internet Information Services:

1. Deploy a web application to Microsoft Internet Information Services
2. Configure **Windows Authentication** as described in *Configure the Web Application* on page 12
3. Ensure that the user created in the User Account Creation on page 15 has a corresponding username in the Active Directory.

On a network connected computer:

1. Ensure that a **testuser1** exists in the Active Directory.
2. Launch the **Browser**.
3. Navigate to `http://<webseal-hostname>/iis_sample`
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 web application on Microsoft Internet Information Service.

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.

Microsoft Internet Information Service Failed Request Trace

The impersonation module uses the native logging and tracing capabilities of Microsoft Internet Information Services. The following steps demonstrate enabling this logging.

1. Select the **Web Site** or **Virtual Directory** from the tree on the left.
2. Select **Failed Request Tracing Rules**.
3. Click **Open Feature** from the Action pane on the right.
4. Click **Add...** from the Action pane on the right.
5. Select **All content (*)**, then click **Next**.
6. Check **Status code(s)** and enter **200-499**, then click **Next**.
7. Check **WWW Server** from the list of providers
8. Select **Verbose** from the **Provider Properties**.
9. Uncheck all Areas, except for **Authentication and Module**.
10. Click **Finish**.
11. Click **Edit Site Tracing...** from the Action pane on the right.
12. Check **Enabled**, then click **OK**.

Uninstalling the Impersonation Module

To remove the impersonation module and the configuration applet from Microsoft Internet Information Service, take the following steps:

1. At the command prompt, navigate to the folder location of the extracted files.
2. Type `PowerShell`
3. Type `.\isam.iis.deploy.ps1`
4. Type `execute -action uninstall`

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.