

IBM Security Access Manager
for Versions 6.1, 6.1.1 and 7.0

***Impersonation Module for
Microsoft Windows Authentication
Installation and Configuration
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 Security Access Manager Impersonation Module for Microsoft Windows Authentication Installation and Configuration and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright International Business Machines Corporation 2010, 2013.

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

Contents

Preface.....	5
About this publication	5
Access to publications and terminology.....	5
Publication Library	5
Base Information.....	5
WebSEAL Information	5
Web Gateway Appliance Information.....	6
IBM Tivoli Federated Identity Manager information	6
IBM Terminology website.....	7
Accessibility	7
Technical training	7
Support information	7
Statement of Good Security Practices	7
Product name updates.....	8
Chapter 1: Introducing the integration.....	9
Introduction	9
Package contents	9
Prerequisites	10
Typical scenario.....	10
Chapter 2: Configuring Microsoft	13
Internet Information Services	13
Installing the native module	13
Configuring the native module.....	13
Configuring the web application	15
Configuring Security Access Manager	16
Creating the WebSEAL junction	16
Chapter 3: Troubleshooting and.....	17
Uninstallation.....	17
Enabling native module logging and tracing.....	17
Uninstalling the module	20

Notices	21
Trademarks	23

Preface

About this publication

This guide provides instructions on how to use the IBM Security Access Manager Authentication Module.

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.

IBM Tivoli Federated Identity Manager information

- *IBM Tivoli Federated Identity Manager Installation Guide*

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

- *IBM Tivoli Federated Identity Manager Administration Guide*

Describes the concepts and procedures for using IBM Tivoli 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 the IBM Tivoli integrated identity management architecture to build and deploy the IBM Tivoli Federated Identity Manager and Web Services Security components. See <http://www.redbooks.ibm.com/>.

IBM Terminology website

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

Accessibility

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

Technical training

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

Support information

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

Statement of Good Security Practices

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

Product name updates

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

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

Chapter 1: Introducing the integration

Introduction

The IBM Security Access Manager Authentication Module is an integration module designed for Microsoft Internet Information Services version 7 and later. This module is designed to run 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.

Package contents

The package contains the following files:

Table 1.

File name	Description
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.
Solutions\Microsoft IIS\IBM.Security.Web.AuthenticationClient.dll	This file is used to provide graphically configuration in Microsoft Internet Information Services required by the native module.
Solutions\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.
Solutions\Microsoft IIS\IsamAuthentication_schema.xml	This is the schema of the native module configuration.

Solutions\Microsoft IIS\Isam.IIS.Deploy.ps1	This is a PowerShell command to install or uninstall the schema and register the Microsoft Internet Information Services client and management files.
Solutions\Microsoft IIS\IBM.Security.Web.AuthenticationClient.dll	This file is used to provide graphically configuration in Microsoft Internet Information Services required by the native module.

Prerequisites

The impersonation module and associated Microsoft Internet Information Services components require the following pre-installed operating system environments:

- Refer to release notes for platform support
- 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 Redistributable Package (x64)

Typical scenario

This overview describes the integration and steps that are required to configure the impersonation module. These scenarios require additional configuration that you complete in the web application and then apply to Microsoft Internet Information Services.

This scenario assumes that the web application is configured for Integrated Windows Authentication. The user identity that is passed from IBM Security Access Manager WebSEAL corresponds to an existing user in the Active Directory user directory.

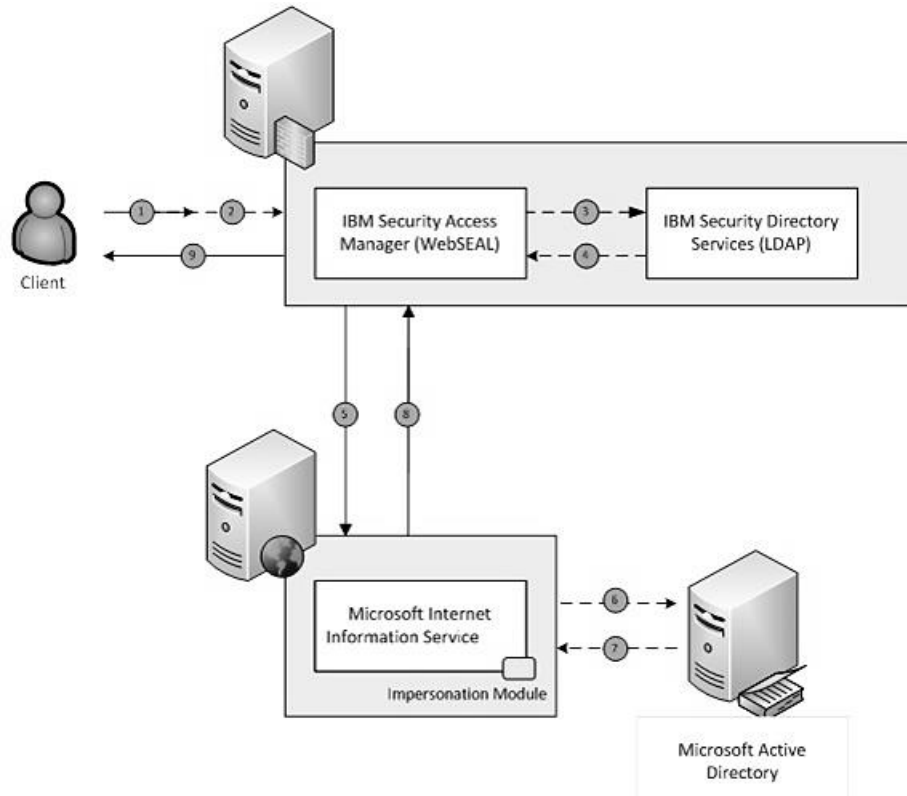


Figure 1. Impersonation module overview

The process includes:

1. The client makes a request to a web application hosted with Microsoft Internet Information Services.
2. The request is intercepted by IBM Security Access Manager (WebSEAL) acting as the reverse proxy, which returns a response for user credentials. The user enters credentials.
3. User credentials are validated against a directory service (LDAP) store.
4. The directory service performs user authentication. If authentication succeeds, the authenticated user and associated attributes are provided back to WebSEAL.
5. WebSEAL injects the user identity information into the request header and forwards the request to Microsoft Internet Information Services by using the 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 corresponds to the value in the WebSEAL header. If no header value is present, the module exits.
7. An impersonation user token is issued from the Active Directory domain controller and the user is set as the current requesting user.
8. The web site response is passed back to WebSEAL.
9. WebSEAL forwards the response to the client.

When using the module to perform single sign-on to Microsoft Exchange 2013 or Microsoft SharePoint, see *Using Kerberos for Windows Authentication Exchange Guide* or *Using Kerberos for Windows Authentication SharePoint Guide* as required.

Chapter 2: Configuring Microsoft Internet Information Services

Installing the native module

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

1. At the command prompt, navigate to the folder location on 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 is copied to the `%windir%\system32\inetsrv` directory.

Note: Microsoft Visual C++ 2013 Redistributable Package (x64) is required. Download the package from <http://www.microsoft.com/en-us/download/details.aspx?id=40784>.

Configuring the native module

You must configure the native module.

As part of the installation procedure, an applet is displayed in Microsoft Internet Information Services at a web site and web application (virtual directory) level to facilitate configuration of the impersonation module. Figure 2 illustrates the use of this applet.

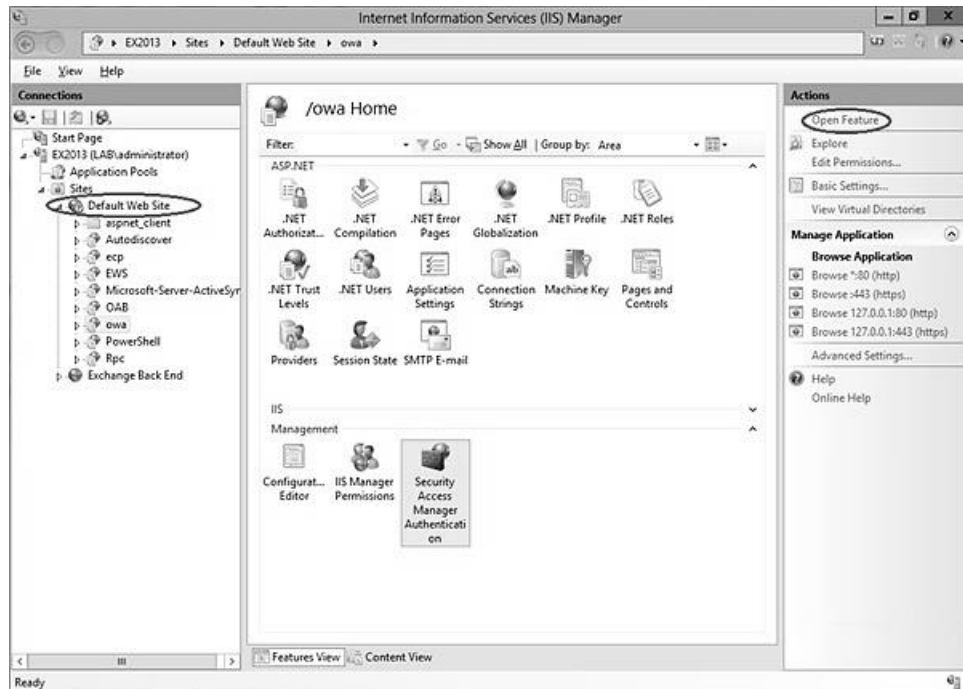


Figure 2. Native module Microsoft Internet Information Services applet

Take these steps:

1. Select the web site or virtual directory from the tree list.
2. Select the **Security Access Manager Authentication** icon and click the **Open Feature** action from the Actions pane on the right.

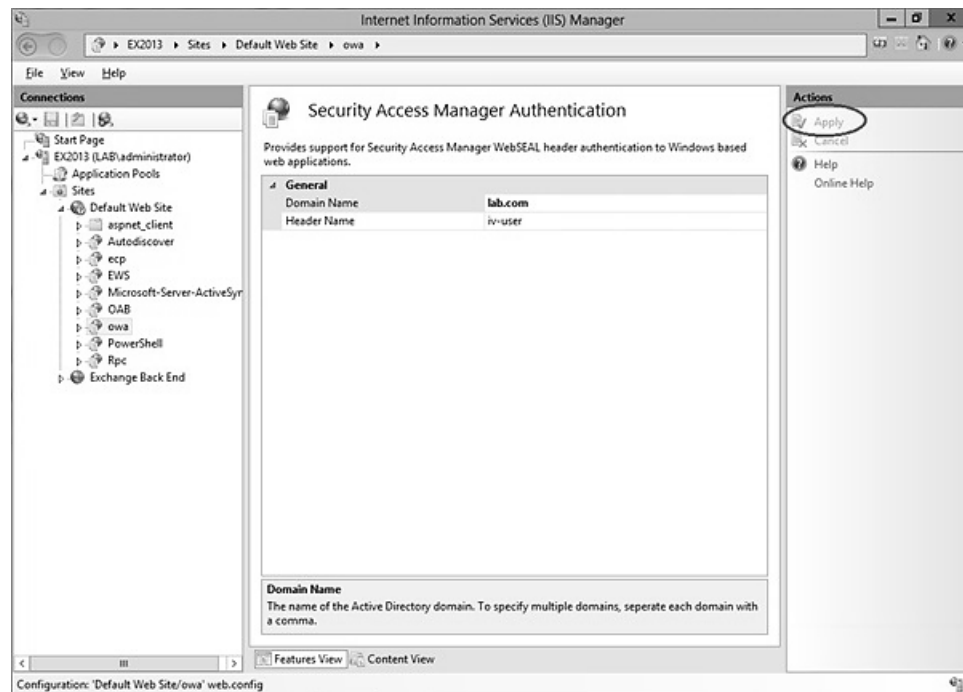


Figure 3. Native module configuration settings

Take these steps:

1. Enter values for the domain and header name in the General heading as shown in Figure 3. The domain name can be a comma separated list to represent multiple domains in a forest.

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

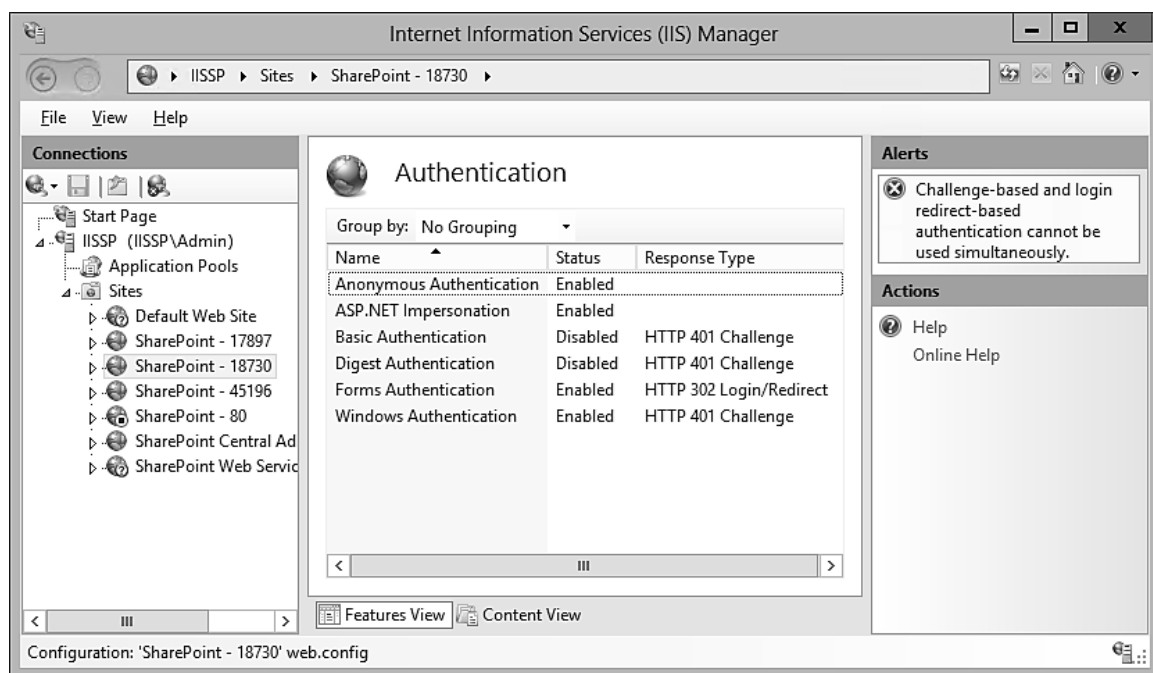
2. Click Apply from the Action pane.
3. The configuration for the module is applied to the selection web application.

Configuring the web application

The impersonation module is used to impersonate a Windows user. The user name that is added by WebSEAL must also reside in the Active Directory. Windows Authentication and ASP.NET Impersonation must be enabling for the web application. Figure 4 displays the web application authentication requirements at a Microsoft Internet Information Services level.

Microsoft SharePoint and Microsoft Exchange automatically configure these settings in the administration tools that are installed with those applications.

Figure 4. Web application authentication configuration



Configuring Security Access Manager

Creating the WebSEAL junction

You must create a WebSEAL junction to pass the header name as specified in step [1](#). This example WebSEAL junction command is run in pdadmin:

Command syntax:

```
pdadmin> server task <webseal_instance> virtualhost create -t  
tcp -h <iisserver_name> -p <webapp_port>  
-c iv-user <junction_name>
```

Example command:

```
pdadmin> server task default-webseald-tam virtualhost create -t  
tcp -h webserver.domain.com -p 80 -c iv-user sso_win_auth
```

If the web application is listening on a port other than port 80 (WebSEAL default), you can modify the WebSEAL instance configuration file, adding a network interface. For example:

```
[interfaces]  
interfacel = network-interface=<webseal_ip_address>; http-  
port=<web_app_port>
```

See the *IBM Security Access Manager WebSEAL Administrator's Guide* for more configuration information.

Chapter 3: Troubleshooting and Uninstallation

Enabling native module logging and tracing

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



Figure 5. Logging and tracing

1. Click **Failed Request Tracing Rules**.
2. Click **Open Feature** from the Actions pane.
3. Select **WWW Server** under the Associated Providers heading.
4. Click **Edit** from the Actions pane.

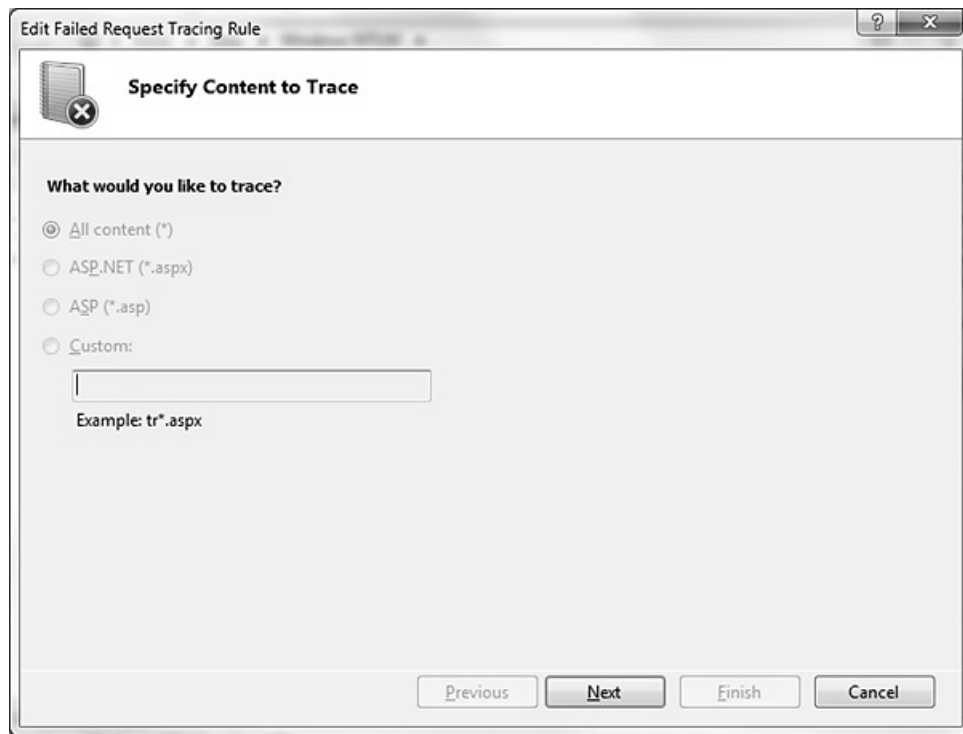


Figure 6. Content to trace

5. Select the All content (*) option, then click **Next** in the Edit Failed Request Tracing Rule.

Edit Failed Request Tracing Rule

Define Trace Conditions

Under which condition(s) should a request be traced?

☒ Status code(s):
200-499
Example: 401.3-999,405

☐ Time taken (in seconds):

☐ Event severity:
Error

Previous Next Finish Cancel

Figure 7. Trace conditions

6. Check the Status codes and enter 200–499 in the text box.
7. Click **Next**.
8. Check WWW Server in the list of providers.
9. Choose the Verbosity that the native module logs to Information and Errors.

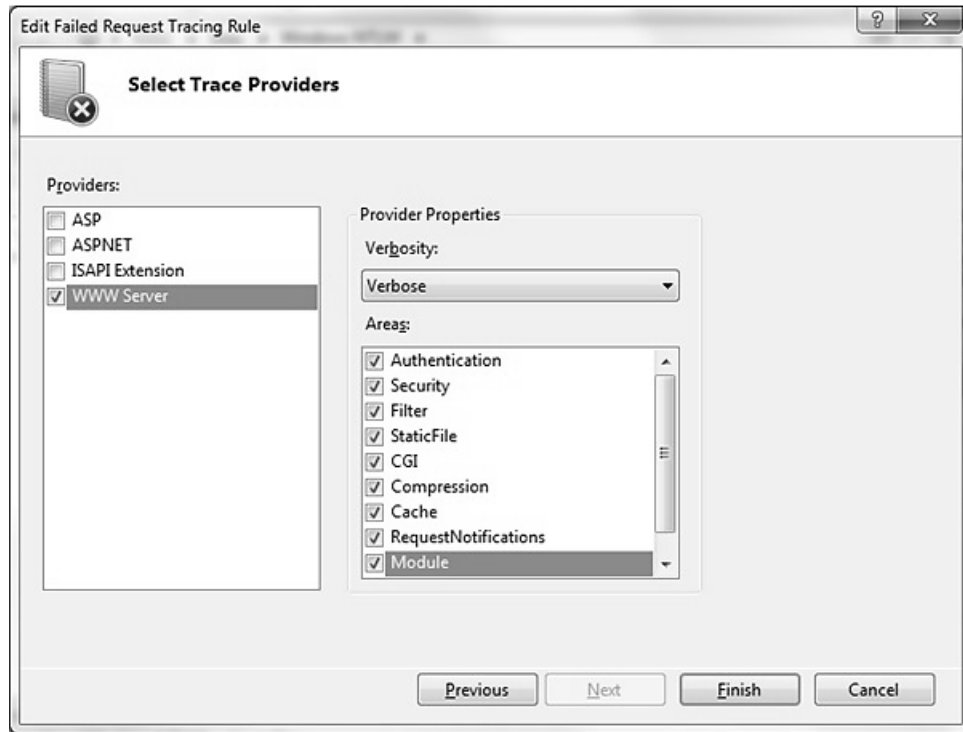


Figure 8. Trace providers

10. Check the Areas that the native module logs in the Module area.
11. Click **Finish** to save tracing. By default, the trace is saved to the `C:\inetpub\logs\FailedReqLogFiles` directory.

Uninstalling the module

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

1. At the command prompt, navigate to the folder location of the extracted files as part of the installation.
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
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

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

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

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

Trademarks

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

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

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

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

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

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

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

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



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

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

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

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