Release Notes

IBM® Tivoli®

Windows Active Directory (64-bit) Adapter for Webservices

Webservices Interface

Version 5.1.1

First Edition (September 26, 2011)

Contents

Preface

Welcome to the IBM Tivoli Windows Active Directory Adapter for Webservices

These Release Notes contain information for the following products that was not available when the product manuals were printed:

- IBM Tivoli Identity Windows Active Directory Adapter for Web Services Installation and Configuration Guide

Note: This adapter cannot be deployed on the same machine as the Identity Manager Windows Active Directory Adapter (DAML-only). If an existing TIM DAML-only adapter already exists, it must be uninstalled prior to installing the Webservices version (*Do not install the Webservices version on top of the DAML-only version*).

Adapter Features and Purpose

You can use the Active Directory Adapter to automate the following administrative tasks:

- Creating an Active Directory account
  Use the adapter to create an Active Directory account on Windows 2003 and Windows 2008 domain servers.
- Managing an Active Directory account
  Use the adapter to manage an Active Directory account on Windows 2003 and Windows 2008 domain servers.
- Managing an Exchange Mailbox
  The 64–bit version of the adapter supports Exchange 2007 only. The 64–bit adapter has no backward support for Exchange 2000 or 2003.
- Creating home directories
  Use the adapter to create home directories.
- Move user in hierarchy
  A user can be moved in different containers managed by the Active Directory Adapter by changing the container of the user from Tivoli Identity Manager.
- Managing an Active Directory group
  Use the adapter to add, modify, and delete an Active Directory group.

NOTE: Read the “Windows Active Directory Adapter for Web Services Installation and Configuration Guide” before using the Adapter.

WSDL Interface Document

The ws-client.zip file (supplied with the adapter) contains all the information needed to develop a web services client that can communicated with the adapter. The zip file content is as follow:

WS-Interface.pdf – describes the web services interface to the adapter.

examples folder - the examples folders contains two example clients: wstool.jar and SampleClient.jar. The “Repository Adapter Web Services Client Samples.pdf” document provided in the folder describes how to run each client. Also, the SampleClient.zip contains the source code for the SampleClient.jar client.

Contents of this Release

Adapter Version

Component	Version
Release Date	September 26, 2011
Adapter Version	5.1.1
Component Versions	Adapter Build 6.0.1002 ADK 6.0.1001 x64
Documentation	Windows Active Directory Adapter for Web Services Installation and Configuration Guide SC27-2788-00

New Features

Enhancement # (FITS)	Description
	Items included in current release
	Initial release

Closed Issues

CMVC#	APAR#	PMR# / Description
		Items closed in current version
	N/A	N/A

Known Issues

CMVC#	APAR#	PMR# / Description
		None

Installation and Configuration Notes

See the IBM Tivoli Adapter Installation Guide” for detailed instructions.

Corrections to Installation Guide

The following corrections to the Installation Guide apply to this release:

- Table 3. Supported operating platforms
  Windows server 2003 is not a supported installation platform.

- Table 4. Supported versions of Windows Active Directory
  Windows server 2003 is not a supported version of the managed resource.

Configuration Notes

The following configuration notes apply to this release:

- Although the 32-bit version of the adapter can be installed on a 64-bit platform, the Exchange server support is only available with the 64-bit version of the adapter.

Configuring SSL authentication for the adapter

To establish a secure connection between the adapter and a web services client (your application), configure the adapter and the web services client to use the Secure Sockets Layer (SSL) authentication with the adapter's WebServices protocol. By configuring the adapter for SSL, you ensure that the web services client verifies the identity of the adapter before a secure connection is established.

For the remainder of this section, the web services client (your application) will be referred to as the “web services application”.

This chapter presents an overview of SSL authentication, certificates, and how to enable SSL authentication. This procedure requires the use of two adapters utilities located in the bin directory of the adapter: certTool and agentCfg.

> **certTool**: Certificate management utility. View section “Managing SSL ceritificates using certTool” included in this document.
>
> **agentCfg**: Adapter configuration utility. Refer to the adapter installation guide for detailed description.

Support for Windows 2008

When you use Windows 2008 as an installation platform and need to run the adapter in Secure Socket Layer (SSL) mode, perform the following steps:

- Disable the Microsoft Windows User Account Control (UAC) security.
- Install the required Certificate.

Optional: If required, enable the UAC security

Note: When you do not perform these steps, the certificate is not installed completely and the SSL is not enabled correctly.

The use of SSL authentication

When you start the adapter, the available connection protocols are loaded. There are two protocols: WebServices and DAML. The DAML protocol is only used by the Tivoli Identity Manager, all other clients interface with the adapter through the WebServices protocol. You must specify the WebServices protocol when configuring SSL (described below).

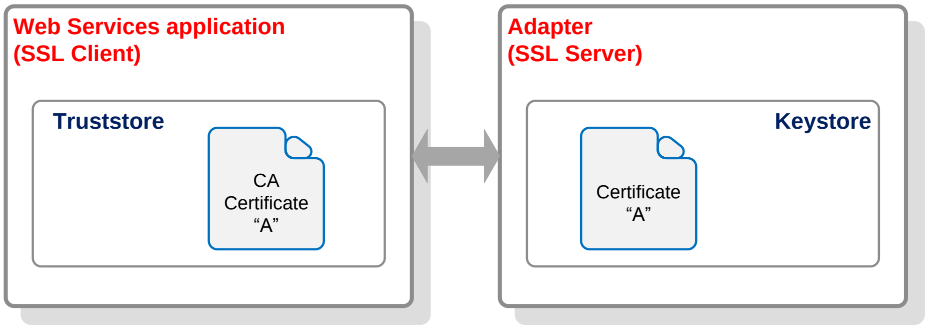
The SSL implementation uses a certificate registry to store private keys and certificates. The location of the certificate registry is managed internally by the CertTool key and certificate management tool, therefore, you do not specify the location of the registry when you perform certificate management tasks.

Configuring certificates for SSL authentication

Use the procedures described in this section to configure the adapter for one-way or two-way SSL authentication by using signed certificates.

Configuring certificates for one-way SSL authentication

In this configuration, the web services application and the adapter are set to use SSL. Client authentication is not set on either side. The web services application operates as the SSL client and initiates the connection. The adapter operates as the SSL server and responds by sending its signed certificate to the client. The web services application uses the its CA certificate to validate the certificate sent by the adapter.



On the adapter side, complete these steps:

1. Generate a certificate using certTool:

   - Create a certificate signing request (CSR) and private key. This step creates the certificate with an embedded public key and a separate private key and places the private key in the PENDING_KEY registry value.
   - Submit the CSR to the certificate authority by using the instructions supplied by the CA. When you submit the CSR, specify that you want the root CA certificate returned with the server certificate.

2. Enable the adapter to use SSL communication

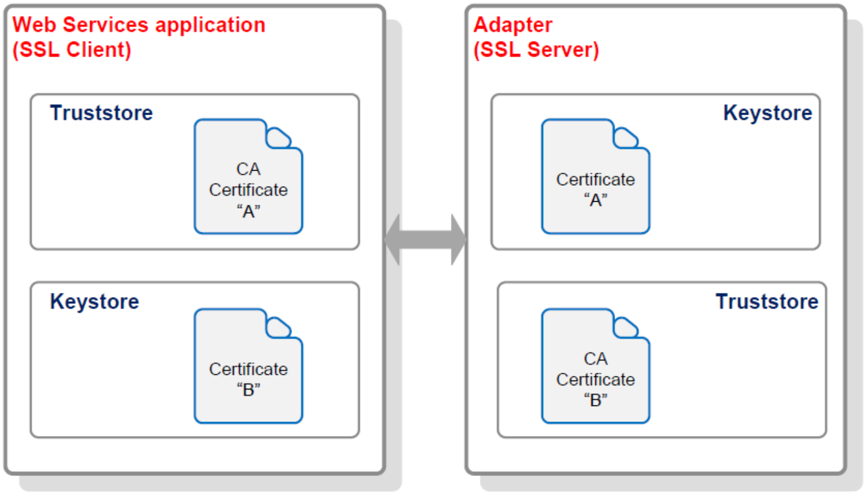
   - Using the agentCfg tool, select "Protocol Configuration" from the main menu.
   - From the "Configure Protocols" select "WebServices"
   - Set "USE_SSL" option to true.
   - The "VALIDATE_CLIENT_CERT" should be true if and only if two way authentication is being used.
   - Restart the adapter.

On the web services application side, complete these steps:

- Ensure that the web services application has stored the root certificate of the CA (CA certificate) in its truststore.

Configuring certificates for two-way SSL authentication

In this configuration, the web services application and the adapter are set to use SSL and the adapter is set to use client authentication. After sending its certificate to the web services application, the adapter requests identity verification from the web services application. The web services application sends its signed certificate to the adapter. Both sides are configured with signed certificates and corresponding CA certificates.



The following procedure assumes that you have already configured the adapter and the web services application for one-way SSL authentication by using the procedure described in “Configuring certificates for one-way SSL authentication”. Therefore, if you are using signed certificates from a CA:

- The adapter is configured with a private key and a signed certificate that was provided by a CA.
- The web services application is configured with the CA certificate of the CA that provided the signed certificate of the adapter.

To complete the certificate configuration for two-way SSL, perform the following tasks:

On the web services application side, complete these steps:

- Create a CSR and private key and obtain a certificate from a CA
- Install the CA certificate.
- Install the newly signed certificate, and extract the CA certificate to a temporary file.

On the adapter side, complete these steps:

- Using certTool, add the CA certificate that was extracted from the web service application.
- Using agentCfg, from the WebServices protocol configuration, set the “VALIDATE_CLIENT_CERT” to true.
- Restart the adapter.

Managing SSL certificates using CertTool

The procedures in this section describe how to use the CertTool utility to manage private keys and certificates.

To start the certificate configuration tool, CertTool, for the Active Directory Adapter, complete these steps:

From a DOS Command Prompt window, change to the bin directory for the adapter (for example C:\Tivoli\Agents\ADAgent\bin).

Type: CertTool -agent ADAgent. The Main Menu is displayed:

From the Main Menu, you can;

- Generate a private key and certificate request.
- Install and delete certificates.
- Register and unregister certificates, and list certificates.

The following sections summarize the purpose of each group of options.

By using the first set of options (A through D), you can generate a CSR and install the returned signed certificate on the adapter.

A. Generate private key and certificate request

Generate a CSR and the associated private key that is sent to the certificate authority.

B. Install certificate from file

Install a certificate from a file. This file must be the signed certificate returned by the CA in response to the CSR that is generated by option A.

C. Install certificate and key from a PKCS12 file

Install a certificate from a PKCS12 format file that includes both the public certificate and a private key. If options A and B are not used to obtain a certificate, the certificate that you use must be in PKCS12 format.

D. View current installed certificate

View the certificate that is installed on the workstation where the adapter is installed.

The second set (E – G) options enables you to install root CA certificates on the adapter.

A CA certificate is used by the adapter to validate the corresponding certificate presented by a client, such as the Tivoli Identity Manager server.

E. List CA certificates

Show the installed CA certificates. The adapter only communicates with clients whose certificates are validated by one of the installed CA certificates.

F. Install a CA certificate

Install a new CA certificate so that certificates generated by this CA can be validated. The CA certificate file can either be in X.509 or PEM encoded formats.

G. Delete a CA certificate

Remove one of the installed CA certificates.

Remaining options (H through K)

These apply to adapters that must authenticate the application to which the adapter is sending information. These options enable you to register certificates on the adapter.

H. List registered certificates

List all registered certificates that are accepted for communication

I. Register a certificate

Register a new certificate. The certificate for registration must be in Base 64 encoded X.509 format or PEM.

J. Unregister a certificate

Unregister (remove) a certificate from the registered list.

K. Export certificate and key to PKCS12 file

Export a previously installed certificate and private key. You are prompted for the file name and a password for encryption.

Customizing or Extending Adapter Features

Active Directory can support custom attributes for the user class. The Active Directory Adapter only supports standard Windows attributes by default. However, you can customize the adapter to support custom (extended) attributes.

Complete these steps to customize the Active Directory Adapter to support the extended attributes in the Active Directory:

Step 1: Extend the schema and add the extended attributes

Extend the Windows Active Directory schema and add the custom attributes to the Active Directory Server using the tools provided by Windows. Refer to the Microsoft Windows Server documentation for more information about adding new attributes to the Active Directory.

The Active Directory Adapter supports the following types of custom attributes:

Boolean
Integer
Case sensitive string
Case insensitive string
UTC coded time

Consider prefixing the attribute names with erAD in order to easily identify the attributes that are used with the adapter.

Note:

- The Active Directory Adapter supports multi-line value for extended attributes with string syntax only.
- The extended attributes are supported only for User account class.

Step 2. Modify the exschema.txt file

The exschema.txt file lists all extended attributes in the Active Directory Server. Modify this file to allow the Active Directory Adapter to recognize an extended attribute in the Windows Active Directory Server.

In order to modify the exschema.txt file, complete the following steps:

1. Change to the \data directory for the adapter.
2. Create or open the exschema.txt file in a text editor.
3. Add the extended attributes to the file. List only 1 attribute per line. For example:

erADString1
erADInteger
erADDate
erADBoolean
erADMultiValueString

4. Save the changes, and close the file.
5. Re-start the adapter by using the Windows Services Console.

Supported Configurations

Installation Platform

The IBM Tivoli Adapter was built and tested on the following product versions.

Adapter Installation Platform:

Windows 2008	*Standard Edition 64-bit OS on x86 and x64 compatible CPU*
Windows 2008	*Enterprise Edition 64-bit OS on x86 and x64 compatible CPU*
Windows 2008 R2	*Standard Edition 64-bit OS on x86 and x64 compatible CPU*
Windows 2008 R2	*Enterprise Edition 64-bit OS on x86 and x64 compatible CPU*
Windows 2008 R2 Core	*Enterprise 64-bit OS on x64 compatible CPU*

Managed Resource:

- *Active Directory on Windows 2008 Standard or Enterprise Edition 32-bit or 64-bit OS*
- *Active Directory on Windows 2008 R2 Enterprise Edition 64-bit OS*
- *Active Directory on Windows 2008 R2 Core Enterprise 64-bit OS on x64 compatible CPU*

  With optional:

  Exchange Server 2007 with SP1
  ---With---
  Exchange 2007 Management Tools

  Exchange Server 2010
  -- With --
  Exchange 2010 Management Tools

  Note: Microsoft supports Exchange 2007 and 2010 only on 64-bit versions of Windows. See Microsoft product documentation for more information.

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 (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

```
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, 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 may 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
2ZA4/101
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 information 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 measurements 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.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
IBM logo
Tivoli

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. 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.

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.

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

Linux is a trademark of Linus Torvalds in the U.S., 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.

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

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

End of Release Notes