

Release Notes



IBM® Security Identity Manager Windows Password Synch Plug-in

Version 6.0.14

Edition notice

Note: This edition applies to versions 5.1 and 6.0 of the IBM Security Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2009, 2015.

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

Contents

Preface.....	3
Adapter Features and Purpose	3
Adapter Version	4
New Features	4
Closed Issues.....	4
Known Issues	5
Installation and Configuration Notes	6
Corrections to Installation Guide	6
Configuration Notes.....	9
Supported Configurations	10
Installation Platform	10
Notices	10
Trademarks	12

Preface

Welcome to the IBM Security Windows Password Synch Plug-in.

These Release Notes contain information for the following products that was not available when the IBM Security Identity Manager manuals were printed:

- IBM Security Identity Manager Windows Local Account Adapter Installation and Configuration Guide

Adapter Features and Purpose

The Windows Password Synch Plug-in is designed to capture password changes on Windows Active Directory accounts. The new password is forwarded to ISIM which then synchronizes the passwords on all accounts owned by the user to the new password.

Password changes may be performed by any domain controller in the forest. The Windows Password Synch Plug-in must be deployed on all domain controllers to ensure that all password changes are captured.

Contents of this Release

Adapter Version

Component	Version
Build Date	February 29, 2015
Adapter Version	6.0.14
Documentation	Check the IBM Security Identity Manager 6.0 Information Center for the following guide(s): Windows Password Synch Plug-in Installation and Configuration Guide

New Features

Enhancement # (FITS)	Description
	Items included in current release
	Added support for 2-way ssl connections

Closed Issues

CMVC#	APAR#	PMR# / Description
		Items closed in current release
	IV36547	Installer not completing install correctly
	IV36011	Double quotes in password causing DC to crash.
		Items closed in 6.0.1012
		Initial release

Known Issues

Installation and Configuration Notes

See the IBM Security Identity Manager Windows Password Synch Plug-in Installation and Configuration Guide for detailed instructions.

Corrections to Installation Guide

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

Under the section “Prerequisites” in the “system” section, it lists Windows 2008 server as the required platform. Windows 2012 server is now also supported.

Section 5 regarding SSL configuration is incorrect. Following should replace section 5 in the user guide.

Chapter 5. SSL authentication configuration for the plug-in

The IBM Security Password Synchronization plug-in sends sensitive password information over the network to the ISIM server. For this reason, a Secure Sockets Layer (SSL) connection is required to communicate with the ISIM server.

When configuring certificates for an SSL connection, there are two levels of validation. One-way SSL is achieved by the server sending you its certificate and the software verifying that it is signed by a trusted Certificate Authority (CA). For additional security the server may enforce Two-way SSL and also request that the client provide a certificate to the server. It is validated the same way by ensuring it is signed by a trusted CA.

One-way SSL

At minimum, you must install the CA certificate that is the signer of the ISIM server certificate to the local trust store. When a connection is requested, the server will send its certificate which is verified to be signed by a trusted CA. This is enough to establish a secure connection with the server.

Two-way SSL

For additional security, the ISIM server can be configured to also request a certificate from the plug-in. This works the same as the server certificate, only in reverse. You must install a user certificate in the local certificate store and the CA certificate must be installed in the trust store on the ISIM server. The extra security allows the ISIM server to verify the source of the password change notification.

Installing the ISIM server CA certificate.

Since the Password Synchronization plug-in runs as a system extension, you must install the certificates in the "system" certificate store.

1. Run the mmc console
2. Select menu option File->"Add or Remove snap-in"
3. Select "Certificates" and click add

4. Select "Computer Account" and click "Finish"
5. Click "OK"

This loads the Certificates MMC console. To install the CA certificate from the ISIM server:

1. Open Certificates/Trusted Root Certification Authorities
2. Right click on "Certificates" and select "All Tasks"->Import...
3. Select the CA certificate file for the ISIM server

Setting User Certificate for 2-Way SSL

If the ISIM server has been configured to use 2-Way SSL, you need to specify a user certificate to present to the ISIM server when connecting. The plug-in runs as a system extension and uses the system certificate store to access certificates. To uniquely identify a certificate you need the issuer and the serial number. The plug-in stores the issuer name as an X500 name string and the serial number as a hex string in the registry. The easiest way to set these values is to use the pfconfig tool to select the certificate and the tool will update the registry with the issuer and serial number. You can also manually add the issuer name and serial number to the registry.

Using pfconfig to select User Certificate

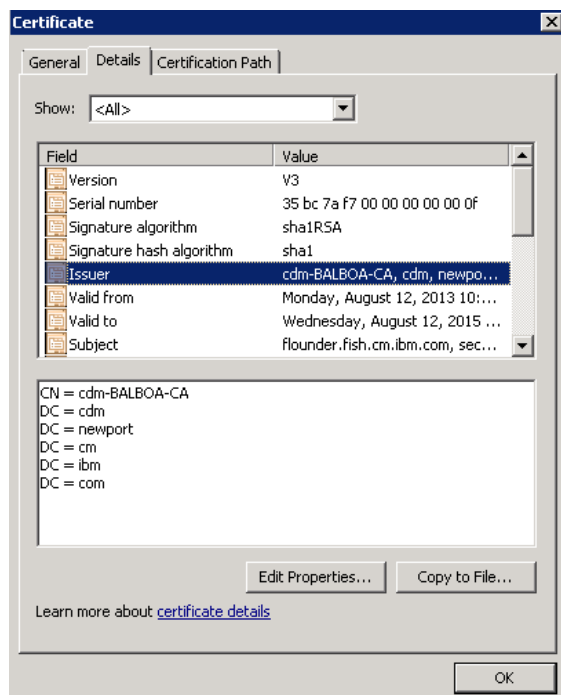
You select using the certificate for 2-Way SSL using the pfconfig.exe configuration tool. There is a field for the User Certificate Serial number. On the far right there is a "Select" button. Click this button to open the select certificate dialog. Here you get list of user certificates in the system certificate store by name. Clicking on a certificate name will update the details display. This allows you to be sure you have selected the correct certificate. If the certificate you wish to use is not in the list, you need to first install the certificate in the system certificate store. Once you have selected the certificate, click on "select" to update the configuration.

Manually setting the User Certificate

The user certificate is identified by the issuer name and serial number which are stored in the registry values CertIssuerName and CertSerialNumber. To get the issuer and serial number open the certificate in the Microsoft Certificate MMC control panel and select the "Details" tab.

Issuer Name

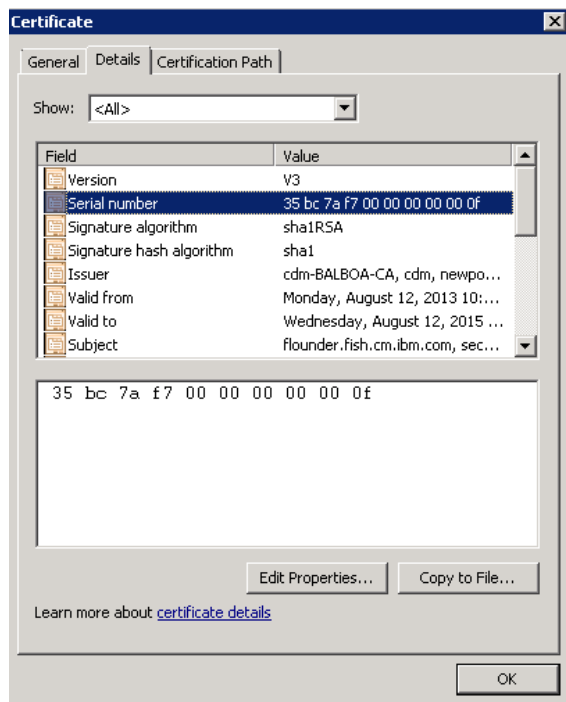
An example is shown below with the issuer name selected:



In the lower panel the elements of the name are shown. To create the value for CertIssuerName, combine the values from the bottom up. Remove the spaces around the '=' and separate the items by a comma and a space. The example above yields the string:
 DC=com, DC=ibm, DC=cm, DC=newport, DC=cdm, CN=cdm-BALBOA-CA

Serial Number

The screen shot below shows the serial number selected.



For some reason the values shown for the serial number are in the reverse order that is required to match with the certificate store. The value above should be entered as:
0f 00 00 00 00 00 f7 7a bc 35

Configuration Notes

The following configuration notes apply to this release:

None

Supported Configurations

Installation Platform

The IBM Security Identity Manager Adapter was built and tested on the following product versions.

Adapter Installation Platform:

Installable on the 32 or 64-bit versions of the following Operating systems on x86 or x64 compatible CPU (application runs as a 32-bit application on 64-bit OS):

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Managed Resource:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

IBM Security Identity Manager:

- IBM Security Identity Manager v6.0
- IBM Security Identity Manager v5.1

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:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

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

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

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

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

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

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

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

IBM Corporation
224A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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

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

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

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

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only. All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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

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

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written.

These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

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

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

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

Trademarks

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

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

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

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

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

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

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

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



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

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

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

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

End of Release Notes