Release Notes

IBM

IBM® Security Identity Manager

Active Directory 64-Bit Adapter

Version 6.0.11

Contents

Preface

Welcome to the IBM Security Identity Manager Active Directory 64-bit (WinAD64) Adapter.

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 Active Directory Adapter with 64-Bit Support Installation and Configuration Guide

Adapter Features and Purpose

The Active Directory Adapter is designed to create and manage accounts on Microsoft Active Directory and mailboxes on Exchange 2007 or Exchange 2010 and Lync 2010. The adapter runs in "agentless" mode and communicates using Microsoft ADSI API and PowerShell (for exchange communication) to the systems being managed.

IBM recommends the installation of this adapter in "agentless" mode on a 64-bit OS and computer in the domain being managed. Installation on a Domain Controller is not recommended. A single copy of the adapter can handle multiple Identity Manager Services. The deployment configuration is based, in part, on the topology of your network domain, but the primary factor is the planned structure of your Identity Manager Provisioning Policies and Approval Workflow process. Please refer to the Identity Manager Information Center for a discussion of these topics.

The Identity Manager adapters are powerful tools that require Administrator Level authority. Adapters operate much like a human system administrator, creating accounts, permissions and home directories. Operations requested from the Identity Manager server will fail if the adapter is not given sufficient authority to perform the requested task. IBM recommends that this adapter run with administrative (root) permissions.

Service Groups Management

The ability to manage service groups is a feature introduced prior to IBM Security Identity Manager 6.0. By service groups, ISIM is referring to any logical entity that can group accounts together on the managed resource.

Managing service groups implies the following:

    Create service groups on the managed resource.
    Modify attribute of a service group.
    Delete a service group.

    Note that service group name change is not supported in ISIM 6.0 release.

The Windows Active Directory x64 adapter supports service groups management.

Contents of this Release

Adapter Version

Component	Version
Build Date	April 15, 2014
Adapter Version	6.0.11
Component Versions	Adapter Build: 6.0.11.1087 Profile 6.0.1004 ADK 6.0.1018
Documentation	Check the IBM Security Identity Manager 6.0 Information Center for the following guide(s): IBM Security Identity Manager Active Directory Adapter with 64-Bit Support Installation and Configuration Guide

New Features

Enhancement # (FITS)	Description
	Items included in 6.0.11 release
	This release requires an updated C++ runtime. You MUST do a FULL install for this release. An update install does not install the C++ runtime.
	Includes updated ADK 6.0.1018 which includes an update to version 1.0.1e-fips of openSSL. This openSSL was built with the OPENSSL_NO_HEARTBEATS option and does not contain the Heartbleed vulnerability.
	Items included in 6.0.8 release
	Added support for disabling slow Lync attributes on recon using registry value "LyncDisableSearch"
	Items included in 6.0.7 release
	Added support for Lync 2013
	Items included in 6.0.6 release
17036, 17099, 25906, 27911, 31577	Added support for Lync 2010 See "**Error! Reference source not found.**" section for additional adapter configuration
	Items included in 6.0.4 release
30820, 27083, 33740	Added support for Windows 2012 Server
34372	Added support for Exchange 2013
	Items included in 6.0.3 release
27906	Added support for MAPIBlockOutlookRpcHttp
15453	Added support for msExchOWAPolicy
29346, 28979, 26825, 22462	Added support for deleting account objects that have child nodes in AD
30515	Added support for managedBy attribute for managed group objects
19447	Added support for POP3 and IMAP4 protocol settings
N/A	Exchange interface updated to use remote PowerShell session with Exchange 2010 Server. No longer requires local installation of Exchange 2010 Management tools.

Closed Issues

CMVC#	APAR#	PMR# / Description
		Items closed in 6.0.9 release
	IV55003	Only first value of extended multi-valued attribute provisioned
	IV54742	Failure when removing value from erAdAllowedaddresslist attribute
	IV53979	Win AD adapter log rotation is not working properly
	IV53709	Account modify problem with the execution policy machine policy set to remote signed,
	IV53423	Windows active directory adapter can crash during test connection
	IV45107	AD recon fails with large photo attribute
	IV55742	ReconDiscconectedMailbox setting breaking reconcile
	IV54738	THE FUNCTIONALITY OF THE FORCE PASSWORD CHANGE ATTRIBUTE IS DOCUMENTED INCORRECTLY
		Items closed in 6.0.8 release
	IV53185, IV52869 IV52916	Unable to set extended string attribute
	IV53212	.V2 profile folder not deleted on deprovision
	IV53225	AD add with Lync account fails with user not found
	70571,227,000	Test request is crashing
		Items closed in 6.0.7 release
	IV49178	Unable to update Accept Mail From attribute.
42506,227,000		Random failure with eradnochangepassword attribute during add/create account request
		Items closed in 6.0.6 release
	IV46279	User delete request reporting error "Unable to parse user DN" even

	IV45884	though delete was successful
	IV38015	Removed FIPs reference from installation guide
	IV43794	On AD adapter Add operation secondary SMTP is ignored
	IV44614	WinAD adapter has missing RPS documentation
		Items closed in 6.0.4 release
	IV43500	Proxy address handling updating to correctly support replacing primary smtp adress
	IV39511	Restructured code to reorder DACLs when updating security descriptor to set erADNoChangePwd
	IV36704	erADEActiveSyncEnabled value was not correct when returned during recon. It is now correctly set.
	IV31681	Additional enhancements to the handling of proxy addresses to properly handle setting primary smtp addresses
		Items closed in 6.0.3 release
	IV31681	Restructured handling of proxy address so the processing order is fixed – delete, add, replace. With the exception that a new primary SMTP address must be added if the existing one is being deleted in the delete request.
		Items closed in 6.0.2 release
	IV31759	Fixed the installer to use registry import to register the Exchange interface DLL. No longer calling RegAsm.exe at install time.
	IV31747	Fixed error handling when Exchange Interface is not present while managing Exchange attributes. Previously returning success, when interface is not present.
	IV25655	Fixed bug in lookup callback that returned success when binding to AD fails.

Known Issues

CMVC#	APAR#	PMR# / Description
N/A	N/A	Support for erADEAllowedAddressList and erADERstrctAdrsLs is no longer available for Exchange 2007.
N/A	N/A	Service form fields: • Administration User Account • Administration User Password See "Corrections to Installation Guide", " The settings for Exchange Mailbox security for Read and Full access were using different values for settings in an attempt to have the default values on the form match those of Exchange. This was confusing and causing issues when the default settings on the Exchange server were changed from what the adapter expected. The adapter now uses the same values for all Exchange security settings. 1=Allow, 2=Deny and 0 or no value=None. Chapter 4. Adapter installation" section below.
N/A	N/A	**Class 3 Certificates** Class 3 secure server CA-G2 certs are not written properly to "DamICACerts.pem" file through CertTool.exe Utility. The certificate data is written twice between BEGIN CERTIFICATE and END CERTIFICATE. Work around: To correct this issue, please follow the below steps and edit "DamICACerts.pem" file present in "<Adapter installation path>\data" folder. Step 1. Start the CertTool utility Step 2. Import the class 3 CA certificate by using "F" option from the main menu of CertTool Utility. Step 3. Once the class 3 CA certificate is successfully installed, open "DamICACerts.pem" file stored in the "<Adapter installed path>\data" folder using text editor. Step 4. Delete the class 3 CA certificate data (i.e. content between BEGIN CERTIFICATE and END CERTIFICATE) from "DamICACerts.pem". Step 5. Open class 3 CA certificate file using text editor and copy the certificate data (between the BEGIN CERTIFICATE and END CERTIFICATE) Step 6. Paste the certificate data to "DamICACerts.pem" file between the BEGIN CERTIFICATE and END CERTIFICATE lines of same class 3 CA Certificate. If more than one class 3 certificates are installed then you can identify the certificate using issuer and subject data. Step 7. Save "DamICACerts.pem" file.

		Step 8. To verify the "DamICACerts.pem" file is edited properly, display certificate information by using option "E" from the main menu of CertTool Utility. Please note that this issue is seen after installing class 3 CA certificate. If you correct the DamICACerts.pem and then install another class 3 CA certificate, the newly installed class 3 CA certificate will show same issue. This issue is also seen when you delete any certificate using option "G" from the main menu of CertTool utility. The delete option will affect all remaining class 3 CA certificate and you have to follow step 1 to 8 to correct the DamICACerts.pem file.

Installation and Configuration Notes

See the IBM Security Identity Manager Windows Local Account Adapter Installation and Configuration Guide for detailed instructions.

Corrections to Installation Guide

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

Exchange Mailbox Security

The settings for Exchange Mailbox security for Read and Full access were using different values for settings in an attempt to have the default values on the form match those of Exchange. This was confusing and causing issues when the default settings on the Exchange server were changed from what the adapter expected. The adapter now uses the same values for all Exchange security settings. 1=Allow, 2=Deny and 0 or no value=None.

Chapter 4. Adapter installation

Section "Adapter user account creation"

The following paragraph is incorrect:
The account information must be supplied on the Active Directory Adapter service form. See "Creating an adapter service" on page 14 for information about creating a service.

Furthermore, you **must not supply the account information on the service form**. The following two fields on the adapter service form are not used and **must be blank**:
- Administration User Account
- Administration User Password

➔ The adapter account, used by the adapter to manage AD/Exchange/Lync, must be supplied on the logon tab of the Windows Adapter service that is named ISIM Active Directory Adapter.

Configuration Notes

The following configuration notes apply to this release:

Table 14. Registry key descriptions

The registry key "LyncDisableSearch" has been added to allow disabling of the Lync attributes that can significantly affect the performance during a search request. Setting this value to "TRUE" will cause the Lync attributes that are not stored as LDAP values, and must be retrieved with a powershell call, to not be included in the search results.

Managed Folder Mailbox Policy

The supporting data returned by the adapter for Managed Folder Mailbox policies may include policies that are not Managed Folder policies. This is due to the Managed Folder policies using the same object

class as other Exchange policies. When setting a Managed Folder Mailbox policy for an account, make sure it is a Manage Folder policy.

Corrections to User Guide

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

Force Password Change

The "Force Password Change" check box is documented incorrectly in section "Specifying controls for a user account" of the User Guide.

It should be as follow: "If you select the Force Password Change check box, then the adapter sets the value of the pwdLastSet attribute to 0. If you do not select the Force Password Change check box, then the adapter sets the value of the pwdLastSet attribute to -1".

Customizing or Extending Adapter Features

The IBM Security Identity Manager adapters can be customized and/or extended. The type and method of this customization may vary from adapter to adapter.

Getting Started

Customizing and extending adapters requires a number of additional skills. The developer must be familiar with the following concepts and skills prior to beginning the modifications:

- LDAP schema management
- Working knowledge of scripting language appropriate for the installation platform
- Working knowledge of LDAP object classes and attributes
- Working knowledge of XML document structure

Note: This adapter supports customization only through the use of pre-Exec and post-Exec scripting.

IBM Security Identity Manager Resources:

Check the "Training" section of the IBM Security Identity Manager Support website for links to training, publications, and demos.

Support for Customized Adapters

The integration to the IBM Security Identity Manager server – the adapter framework – is supported. However, IBM does not support the customizations, scripts, or other modifications. If you experience a problem with a customized adapter, IBM Support may require the problem to be demonstrated on the GA version of the adapter before a PMR is opened.

Supported Configurations

Installation Platform

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

Adapter Installation Platform:
        Windows 2008 Standard Edition 64-bit
        Windows 2008 Enterprise Edition 64-bit

        Windows 2008 R2 Enterprise Edition
        Windows 2008 R2 Core Enterprise 64-bit

        Windows Server 2012

Managed Resource:
        Active Directory on Windows 2008 Standard or Enterprise Edition 32-bit
        Active Directory on Windows 2008 Standard or Enterprise Edition 64-bit
        Active Directory on Windows 2008 R2 Core Enterprise Edition
        Active Directory on Windows 2008 R2 Enterprise Edition
        Active Directory on Windows Server 2012

        With optional:

        Exchange Server 2010
        Exchange Server 2013
        Lync server 2010
        Lync server 2013

        NOTE: Support for Exchange and Lync are provided via .NET modules. They require .NET 2.0 support to run. This is not supported by .NET version 4.0. You need .NET 3.5 or earlier.

IBM Security Identity Manager:
        IBM Security Identity Manager v6.0

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
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.

End of Release Notes