Release Notes

IBM® Tivoli® Identity Manager

Active Directory 64-Bit (WinAD64) Adapter

Version 5.0.14

First Edition (February 10, 2012)

This edition applies to version 5.0 of Tivoli Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Preface

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

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

- IBM Tivoli 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. 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.

Contents of this Release

Adapter Version

Component	Version
Release Date	February 10, 2012
Adapter Version	5.0.14
Component Versions	Adapter Build 5.0.1030 64-bit Profile 5.0.1014 ADK 5.20 64-bit
Documentation	Active Directory Adapter with 64-bit Support Installation and Configuration Guide SC23-9479-00 Active Directory Adapter with 64-bit Support User Guide SC23-9480-00 Password Synchronization for Active Directory Plug-in Installation and Configuration Guide SC23-6178-00

New Features

Enhancement # (FITS)	Description
WARNING	WinAD64 is a new adapter designed to support AD and Exchange 2007 and Exchange 2010. **WinAD64 is not an upgrade of the WinAD Adapter**. While the objectClass names have remained the same as WinAD to ease the migration to this new adapter, it is important that customers review all TIM Policies and retest all third-party integrations. The features of the WinAD and WinAD64 adapters are not identical due to changes in the underlying Microsoft components.
	Items included in current version
NA	Enhancements to adapter based event notification. Now searches global catalog for domain controllers when scanning event logs for group membership changes. The actual group membership change event is sent instead of returning the full list of groups for the user account. Supports all configured EN contexts with one pass of event log scanning per cycle instead of scanning the event logs for each EN context.
MR0721117156	Allow support for Octet String data type in extended attributes. The adapter now supports Octet String as an extended attribute type. It is assumed to be passed as a string value.
MR0629114418	Unable to provision WinAD Extended attributes without MS Exchange Management Tools installed locally. The adapter now treats the extended exchange attributes as account attriubutes since they are set via LDAP calls anyway and do not require an exchange client.
	Items included in 5.0.12 release
MR090210587	Support for Exchange Unified Messaging management on Active Directory accounts with ITIM Windows Active Directory Adapter. See additional information in the “Configuration Notes” section.
MR081710242	Optionally require a MailBoxStore and use Exchange 2010 default feature if Store is not present. See additional information in the “Configuration Notes” section.
	Items included in 5.0.11 release
MR0204103013	AD adapter extended schema support for data type DNWithBinary. See additional information in the “Configuration Notes” section.
	Items included in 5.0.10 release
MR0302105547	Use erADLastLogonTimeStamp for AD dormant account report
MR0210102732	OCS support for AD adapter.

MR0205101253	Windows 2008 R2 Core support for AD password sync plug-in and Adapter.
MR110509300	AD agent Exchange server 2010 support
MR0908095421	AD agent Exchange server 2010 support
MR031010518	WinAD: Need Disable Mailbox support for Exchange 2007
MR0226101912	WinAD: Need a way to configure the length of the wait period for the retries of Win AD 64-bit Adapter for reconciliation

Enhancement # (FITS)	Description
	Items included in 5.0.9 release
OSDB	Added support for Windows 2008 R2 (64-bit only).
	Items included in 5.0.8 release
MR1010083842	Enhancement to support Managed Folder Mailbox Policy in WinAD 64bit Adapter
MR0421092235	WinAD: Client needs support for msExchMailboxTemplateLink MS Exchange attribute.
MR052609514	Support extend attribute on a transformed name on itim side using the AD 5.0.5 adapter on ITIM 4.6 Server.
MR0928094723	Delay in Exchange cmdlets for mailbox permission.
N/A	This adapter version support agent-based event notification.
	Items included in 5.0.7 release
MR022409571	Enhance the adapter to allow a delay between AD account rename and the Exchange updates. Additional information can be found in the “Configuration Notes” section.
MR0501091927	Modified the error message (clarification) that may occur during account modifications. Additional information can be found in the “Configuration Notes” section.
MR0218091930	Modify the adapter to allow an AD account to be unlocked without performing a password reset. Additional information can be found in the “Configuration Notes” section.
MR0830071536	Modified adapter so that the adapter can change the “userCannotChangePassword ACE” even when not running as Domain Administrator. Additional information can be found in the “Configuration Notes” section.
MR0501091918	Added “read time out” to the ADK to avoid problems with firewall time outs. Additional information can be found in the “Configuration Notes” section.
N/A	Added Registry Key “SearchTimeout” to work around Microsoft hang in AD LDAP client present in Windows 2003. Additional information can be found in the “Configuration Notes” section.

Enhancement # (FITS)	Description
N/A	Enhanced form validation. Added constraint to exclude special characters forbidden by Active Directory in the samAccountName. Additional information can be found in the “Configuration Notes” section.
	Items included in 5.0.6 release
MR0212084734	Enhancement to handle failover of target systems by supporting multiple target servers in basepoint.
MR0831085255	Management of field msRADIUSFramedIPAddress in Active Directory
N/A	Improve primary group lookup performance using cache.
	Items included in 5.0.5 release
MR0808084336	Add support for Exchange 2007 attribute ‘msexchrequireauthtosendto’.
MR0825086415	Enhance the adapter to allow an account to be changed from a mail-user to a to mailbox user in a single transaction.
N/A	Add support for Windows 2008 as a target AD. Add support for Windows 2008 as a host platform for the adapter.
	Items included in 5.0.2 release
MR0825086415	AD adapter profile modified to include the DL e-mail attribute.
MR121707567	Modified the adapter to accept a single MODIFY operation to change a user from mail-user to mailbox user.
	Items included in 5.0.2 release
MR0427076459	Enhance adapter to support the AD LastLogonTimeStamp attribute. See “LastLogonTImeStamp Attribute” in the configuration section of this document for more information.
MR1118053029	Enhance the adapter to support all options of the RemoteAccessPermission property. See “Remote Access Permission Attribute” in the configuration section of this document for more information.

Enhancement # (FITS)	Description
	Items included in 5.0.1 release
MR0302076050	WinAD: support for Exchange 2007 by TIM v4.6.
MR0625072952	WinAD: AD Adapter needs to support Exchange 2007.
MR0709074515	WinAD: TIM 4.6 needs adapter to support Exchange 2007
MR082107737	WinAD: Exchange 2007 adapter support needed.
MR1017076035	WinAD: the Active Directory adapter needs to support Exchange 2007

Closed Issues

Internal#	APAR#	PMR# / Description
		Items closed in current version
	IV11173	False warnings generated during adagent home directory processing. The adapter was marking attributes as failed when unable to access the home directory share even though they were not included in the adatper resulting in warning. Error is now only set if the attribute existed in the request
	IV13282	Unable to provision account when country code is Serbia. The country code list was updated to the most recent publilshed list. The account form and customlables files in the profile were also updated to add the new countries to the list.
		Items closed in 5.0.13 version
	IZ98592	10738,999,616 Multiple values returned for erADEAllowPermTo1Level during recon. FIX: The adapter will now only returns the first Access Control Entry (ACE) for "SELF". If multiple ACEs exist for SELF, the erADEAllowPermTo1Level is only returned for the first ACE.
	IZ94371	77770,550,000 If the erPassword attribute value cannot be set, it will be displayed in clear text in the adapter log file. FIX: The adapter has been modified so that any attribute whose name contains "pwd" or "pass" will now only show "*****" as the value in the unmodified attributes list.
	IZ89492	85059,999,724 ADK adapter message :starting new SSL connection thread” FIX: The text "SSL" has now been removed from this message. The IO library will clearly log the ssl handshake before this message is logged. It is not necessary to state that the connection is SSL or not.
		Items closed in 5.0.12 version
	IZ89623	11899,922,848 CO attribute does not get the correct value of the country name.
	IZ91338	14724,344,000 Windows AD Adapter crashes when searching for supplicate UPNs.

		Items closed in 5.0.11 version
		None
		Items closed in 5.0.10 version
	IZ72897	PROBLEM TRYING TO SET AN ADDITIONAL E-MAILTYPE MRS.
	IZ73004	WINAD ADAPTER IS NOT SETTING FAILURE FOR RAS RELATED ATTRIBUTE.
		Items closed in 5.0.9 version
	IZ65637	39372,180,000 CUSTOM "UTC CODED TIME" ATTRIBUTE VALUE NOT CORRECTLY RETURNED FROM AD ADAPTER DURING RECON.
	IZ66086	07172,035,724 RECONCILIATION ERROR WITH WINAD 64BIT ADAPTER 5.0.8.
	IZ67106	79658,442,000 INTERMITTENT 0X80004002 ERRORS WHEN ATTEMPTING TO MANAGE/PROVISION MAILBOXES.
36620	N/A	N/A 5.0 WinAD - Problem with WTS Boolean attributes during recon.
	N/A	81172,379,000 RUS and EAG errors during WinAD Adapter Add request. Following changes are made in adapter logging. • Adapter will log "Domain Flat Name" in Adapter log file. • Adapter log messages are enhanced to provide more error message with the error code when searching for RAS Server Name.
	IZ58983	94774,227,000 CERTTOOL.EXE UNABLE TO LIST CERTIFICATE VERISIGN CLASS 3 SECURE SERVER CA - G2. (ADK fix)
36607	N/A	N/A ADK incorrect return status for multivalued attr with spl chars. (ADK fix)
	IZ70467	24803,422,000 AD AGENT CRASHES WHEN MODIFY REQEUST INCLUDES CHANGING ERADISACCOUNTLOCKED TO A SPACE.

Internal#	APAR#	PMR# / Description
		Items closed in 5.0.8 version
36208		N/A WinAD Adapter returns incorrect container when CN contains '='
	IZ60509	36047,660,706 CHANGES TO WTS HOME DIR AND DRIVE LETTER NOT COMMITTED TO AD.
36212		N/A WinAD Adapter fails to find user when eruid contains (or)
36238		N/A WinAD Adapter returns incorrect error for duplicate UPN
36240		N/A WinAD Adapter terminates when an error occurs in reconciliation
IZ52909		39888,227,000 PERFORMING FILTERED RECON WITH ITIM V4.6 SERVER RETURNS CONTAINER OBJECTS CAUSING RECON ERRORS IN ITIM
IZ61122		24146,660,706 PATH TO EXCHANGE TOOLS IN AD ADAPTER SHOULD BE CONFIGURABLE
	N/A	N/A 33834,999,760 WinADAdapter failed to load exschema.txt at system bootup

Internal#	APAR#	PMR# / Description
		Items closed in 5.0.7 version
	IZ45782	92561,077,724 Checkboxes in account form for exchange cause transaction “warning”
	IZ47221	83137,379,000 WinAd adapter does not support multi-line attribute values properly.
	IZ43288	66187,379,000 WinAD adapter CN attribute is incompatible with TIM Alert Processing features.
	IZ52976	06524,6X1,760 WinAD group membership modifications fail if group contains “#” and the adapter is set to use CN for group linkage.
	IZ51132	19725,379,000 Group names containing a “/” character are not properly parsed if the adapter is set to use DN group linkage.
	IZ54007	06743,6X1,760 Adapter fails to add group membership of the group contains an unmatched closing parentheses “)” character.
	N/A	34450,057,649 Added a “SearchTimeout” option to work around AD hang on LDAP read in Windows 2003. See “Configuration Notes” section for more information.
	N/A	29147,227,000 Adapter may crash if an inactive user is moved to a new OU.
36159	N/A	N/A Adapter may not return an error message if a delete user request if the base point bind fails.
36160	N/A	N/A Correct issue with filter substitution of erACContainer that may occur when the “Adapter Filtering” option is used with TIM v4.6,
	IZ47418	10132,922,848 WinAD adapter crashes randomly. Fixed in ADK by adding Read Timeout to avoid firewall time out issues.
	IZ49418	83618,550,000 Event Notification displays incorrect value for next run time after “Run Event Now” option is selected.
35175	N/A	N/A Adapter returns unreadable error message for multi-valued attribute in result status.

Internal#	APAR#	PMR# / Description
35017	N/A	N/A ADK crash in RECON request when users EntryDN contain substring "pass" or "pwd".
		Items closed in 5.0.6 version
	IZ38367	59070,082,000 Adapter provisioning to child domain UPN issue.
	IZ42815	67170,650,706 WinAD Adapter installer issue if the path contains a space.
	IZ44751	57426,004,000 ITIM WinAD 64 Bit Crash.
	IZ40688	49313,379,000 null attrs in Exch 07 issue WINAD64 bit Adapter.
33974		N/A WinAD Adapter recon returning unwanted exchange attributes.
33977		N/A WinAD64 attribute erADEProxyAddresses to be sent as add-delete
34278		N/A WinAD64 ADprofile update. Corrected jar format that prevented successful import to TIM.
		Items closed in 5.0.5 version
	N/A	Updated the PW Sync Plug-In 1) MR1017081822 - create a version of PW Sync without 3rd party dependencies 2) PMR 37512,379,000 - Added more logging in domain bind and user lookup. 3) 77327,021,724 - Code changes for ignoring TIM response when TIM application is down Down
	IZ35340	CertTool crashes for ADAgent on Win 64-bit.
		Items closed in 5.0.4 version
	IZ35901	35389,379,000 erADEHideFromAddrsBk in AD 64bit Agent needs to return either TRUE or FALSE value during recon (for a mail-user or mailbox user).
	IZ35932	16714,7TD,000 AD Adapter recon fails because the recon event crashes the service when parsing security descriptor data for a user it recons.

Internal#	APAR#	PMR# / Description
		Items closed in 5.0.3 version
33182	N/A	Values for "Reject Mail From" and "Delegates" are not cleared on the resource, though Agent reports success for requests to clear the values of these attributes.
33183	N/A	Agent doesnt retrieve correct value of exchange attribute 'Permanent delete only after backup' through recon on Windows 2003 64bit AD.
33188	N/A	Setting Forwarding Style as "Recipient or Forward", the attribute "deliverAndRedirect" should be set to "false". But the attribute's value gets cleared.
N/A	N/A	Windows AD Adapter 64bit crashes on Windows 2008 64bit when neither Exchange Server 2007 nor PowerShell is installed.
		Items closed in 5.0.2 version
	IZ24107	37721,550,000 WinAD Adapter returns success for add request with home directory creation, but the home directory is not created on the resource
	IZ13159	19535,005,000 Enhancement to support the third dial-in option "Control access through Remote Access Policy"
	IZ25019	65296,001,822 Problem with setting the 'erlogontimes' attribute to 'Mid-Hour'. The adapter throws an error expecting a 168 bit string. Documentation change : AD Adapter erLogonTimes can only be set to hourly and not to 'Mid-Hour'.
	IZ24750	42485,999,866 AD Password Sync plug-in 5.0.1 does not check the origin of password change.
	IZ23735	70262,379,000 Replication delay leads to an error while adding mailbox on Exchange 2007.
	IZ30086	84473,379,000 WinAD64 creating unwanted proxy addresses during account creation with alias specified.

Internal#	APAR#	PMR# / Description
32850	N/A	N/A Issue adding user to groups in Windows 64-bit AD agent.
32557	N/A	N/A AD Agent sets WTS drive letter instead of WTS Home directory in "Local path" on AD.
32558	N/A	N/A WinAD Adapter returns success but cn is not set on AD. Attributes mobile, postofficebox, givenname, sn, telephonenumber, street, pager, l, mail, homephone, postalcode, title, description and st are send as add-delete for a modify request instead of replace.
32579	N/A	N/A WinAD worngly sets Dialin Callback option as "Set by caller (Routing and Remote Service only)" when "Fixed callback number" is selected.
		Items closed in 5.0.1 version
		None

Known Issues

Internal#	APAR#	PMR# / Description
N/A	N/A	**Below is the list of Known Issues for WinAD64 Adapter:** Modifying account by clearing Mailbox Alias, Agent reported attribute level failure but alias is cleared from TIM. Setting Forwarding Style as “Recipient or Forward”, ideally on the resource the attribute "deliverAndRedirect" should be set to "false" value but here the attribute's value gets cleared.
N/A	N/A	**Editing adapter profiles on UNIX or Linux.** The adapter profile JAR file may contain ASCII files created using MS-DOS ASCII format (i.e. schema.dsml, CustomLabels.properties, and service.def). If you edit a MS-DOS ASCII file in Unix you will often see the characters ^M at the end of each line. This is the extra character 0x0d that is used to indicate a new line of text in MS-DOS. There are tools, such as dos2unix, that can be used to strip out the ^M character. In addition, there are text editors that will ignore the ^M character. If you are using the vi editor, you can strip out the ^M character as follow: From the vi's command mode: :%s/^M//g followed by pressing Enter. The ^M (or Ctrl-M) typed to show it here should actually be entered by pressing ^v^M in sequence. (The ^v preface tells vi to use the next keystroke literally instead of taking it as a command.)

Internal#	APAR#	PMR# / Description
		Issues with Adapter installed on Windows 2003 64bit and managing Active Directory on Windows 2003 64bit or Windows 2008 1. Known Issues for Enhancement to support the third dial-in option "Control access through Remote Access Policy" 1) In mixed-mode domain functional level third dial-in option "Control access through Remote Access Policy" is not supported. If an attempt is made to set dial-in as "Control access through Remote Access Policy" agent will report attribute level failure to TIM, but on the resource dial-in will be set to "Deny Access" (default). If previously dial-in was set to "Allow Access" after the above failed request dial-in will be set as "Deny Access". Workarround: No workaround available. 2) Reconciliation on mixed mode domain functional level shows incorrect value "Control access through Remote Access Policy" for Dial-in attribute for accounts created directly on Active Directory with the combination "Deny Access" (Dial-in) and "No Callback" (Callback option). There are two cases when Active Directory does not create attribute msNPAllowDialin as shown in below table. Domain Functional Level: Attribute Value on Active Directory Windows 2000 Native: Dial in: Control access through Remote Access Policy Callback options: No Callback (default) Windows 2000 Mixed: Dial in: Deny Access (default) Callback options: No Callback (default) During search, active directory does not return attribute msNPAllowDialin and also adapter can not find the functional level of domain without connecting to RootDSE. Connecting to RootDSE does not work if you have installed adapter in domain other than one you are managing. So adapter sets erADExDialin as "NONE", which is "Control access through Remote Access Policy" on account form. Work around: If you want to retrieve correct value then while creating user directly on Active Directory, set following as defaults instead of "No Callback" for Callback option. Attribute ---------- Value ---------- Dialin Deny Access Callback Options Set by caller

Internal#	APAR#	PMR# / Description
N/A	N/A	Using the Upgrade Option: The Upgrade option is applicable only to 5.0.x maintenance upgrades. The upgrade option is not designed for v4.6 to v5.0 migrations. NOTE: After using "Update Installation" option with higher version of Adapter, an extra folder with name "_uninst2" is created. It can be ignored. To Uninstall the Adapter, use "_uninst" folder.
N/A	N/A	PMR 83403,057,649 - AD Agent hangs on second error Work around implemented for Microsoft issue (KB article 293278). For user add request, the agent binds to the basepoint/default domain and checks to see if the specified user already exists. Each operation is run in a separate thread which first initializes COM using CoInitialize and upon operation completion calls CoUninitialize to uninitialize COM. However for second request, the connection is reused and agent quickly establishes connection with AD. MS KB article 293278 (http://support.microsoft.com/default.aspx?scid=kb;en-us;293278) states that 'PRB: Problems When You Call CoInitialize and CoUninitialize Repeatedly in Multithreaded Apartment' - To avoid the issue, a small delay (1 sec) has been inserted before COM is uninitialized at the end of operation. This delay is ONLY applicable when 'User already exists' condition is encountered and DOES NOT affect any other functionality.
		Special characters in the BasePoint attribute. The BasePoint that is specified on service form and for the Event Notification Context (in agentCfg) must be in proper DN format. Special characters like '#' '+' '=' '\' ';' '"' ',' '<' '>'in the base point value must be escaped with the escape character '\'. For Example: Example 1 If the basepoint to be specified is ADServer1/ou=#test<org>=01/END,dc=MyDomain,dc=com The characters # < > = should be escaped using the \ character as ADServer1/ou=\#test\<org\>\=01/END,dc= MyDomain,dc=com Example 2 If the base point to be specified is ou=Inner;most,ORG",ou=Outer+\ORG,dc=MyDomain,dc=com The characters ; , " + and \ should be escaped using the \ character as ou=Inner\;most\,ORG\",ou=Outer\+\\ORG,dc=MyDomain,dc=com NOTE: Escaping of the '/' character is internally handled by adapter and should not be explicitly escaped on service form. It is recommended that the use of special characters should be avoided to get the best performance on various operations performed by adapter.

Internal#	APAR#	PMR# / Description
N/A	N/A	Below is list of TIM AD adapter attributes and corresponding attribute in Active Directory erADLastFailedLogin -> badPasswordTime erADBadLoginCount -> badPwdCount erADLastLogoff -> lastLogoff erADLastLogon -> lastLogon The above attributes are nonreplicated attribute, which means that each domain controller holds its own copy of the attribute, likely with different values. The WinAD adapter may not show actual value for these attributes.
N/A	N/A	**Group Names with Tilde ("~") Character** This known issue is only applicable to IBM Tivoli Identity Manger v4.6. This is when a group's CN contains the character '~' and you select and add that group to the Groups attribute on account form. When the request is submitted to the adapter, characters before the '~' characters are only added to the erGroup attribute. IBM Tivoli Identity Manager treats the '~' character as delimiter and truncates the characters after it in the group name. For example, If you add a group whose CN is TEST~TST to a user and submit the account form, in the request only TEST will be added as value for erGroup attribute and not TEST~TST. Workaround: Avoid using this special character '~' in group name on Active Directory.
		Issue with adapter based filtering. Avoid use of cn attribute of the common schema in a filter with object class value as erADContainer. Although the filter is perfectly valid for Active Directory nor will IBM Tivoli Identity Manager gives any error while evaluating and submitting the filter to adapter. However after the adapter processes the filter and returns matching entries IBM Tivoli Identity Manager will give failure while processing the returned entries. This is because the CN attribute does not belong to erADContainer class on IBM Tivoli Identity Manager Schema for Active Directory profile. For example, The following filter will result in FAILED for the reconciliation request on IBM Tivoli Identity Manager. (&(objectclass=erADContainer)(cn=MyContainer))
		Known Issues for Adapter based Event Notification a. When you modify the "User logon name (pre-Windows 2000)" of a user account on Active Directory, Adapter based event notification results in the creation of two accounts on IBM Tivoli Identity Manager. One of the accounts is created using the old name and other account with modified name (Orphan account).

		Workaround: As far as possible avoid renaming user accounts on the Active Directory directly. Perform user modifications only through Tivoli Identity Manager. However if you rename a user account on Active Directory, perform full reconciliation to avoid creation of duplicate user accounts on Tivoli Identity Manager. b. When you configure Active Directory for not caching the deleted objects in the deleted objects container, then the adapter cannot track the deletion of an object (user/group/organizational unit) on the Active Directory. As a result IBM Tivoli Identity Manager will not be updated for the deleted objects. **Workaround:** no workaround. c. When you remove an organization unit (container) on Active Directory which contains user accounts, then all the user accounts in the organization unit are removed from Active Directory. The user accounts which are removed as a result of deletion of the organization unit are not traced by the adapter based event notification. The information of such user accounts will not get updated on IBM Tivoli Identity Manager. **Workaround:** Before you remove a container on the Active Directory, remove all the user accounts from this container and from the sub-containers. This way the adapter based event notification will be able to trace user account deletions. d. An event notification context maintains each object (user, group, container, and mailstore) by generating a key in a local database. The maximum key length of the database is 64 characters. When you have containers, groups, and mail stores in Active Directory with name containing more than 64 characters, the adapter based event notification may function incorrectly. The event notification might add duplicate entries in database or read incorrect entry from the database. This may result in incorrect updation to objects in IBM Tivoli Identity Manager. **Workaround:** When you create a container, group, or mail store on Active Directory select a name such that the first 50 characters are unique. e. When a group is removed from Active Directory, user's membership information for this group is not updated on IBM Tivoli identity Manager. **Workaround:** Before deleting a group on Active Directory, empty its "Members" list, i.e. remove all the objects which are member of this group. This will ensure that the dependant accounts get properly updated in IBM Tivoli Identity Manager (ITIM) server f. When the log information in the event viewer log file is cleared, then during the next event notification operation you may get the following error in Adapter log file. *'Unable to read the last highest record from the log. Error code: 0x00000057 - The parameter is incorrect'.*

		Workaround: No action to be taken. The next adapter based event notification will succeed to read the event log properly. g. When a user account is moved from a container which is either the base point or a sub-container of the base point to a container which is not in the base point, then after running event notification this user account will not get updated on IBM Tivoli Identity Manager. Ideally this user no longer belongs the corresponding service on IBM Tivoli Identity Manager, as it is moved to a container which is not in the base point of this service. **Workaround:** When you move a user account on Active Directory to a container which is not under the base point, perform a full reconciliation to update the user accounts on IBM Tivoli Identity Manager.
		ERUID does not allow special characters This known issue applies to IBM Tivoli Identity Manger (ITIM) v4.6 & v5.0. When a user account's samAccountName attribute on Active Directory contains characters like "(" and/or ")" and a Full Reconciliation is performed. The Full Reconciliation will complete with a warning. Please note that the samAccountName attribute of a user account on Active Directory maps to the eruid attribute on ITIIM. For example, If you have user accounts on Active directory with following samAccountName TestUser(_01 TestUser)_02 (TestUser _04(TestUser _05) The Full Reconciliation will result in warning with following error message: CTGIMD014I 7 reconciliation entries were not processed for the following entries: eruid=TestUser(_01; eruid= TestUser)_02; eruid=(TestUser _04(; eruid=) TestUser _05);. **Workaround:** Avoid use of special characters like "(" or ")" for the samAccountName attribute of user account on Active Directory.
		Class 3 Certificate Installation Class 3 Certificates (class 3 secure server CA-G2) are not written properly to “DamlCACerts.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 “DamlCACerts.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

		“DamlCACerts.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 “DamlCACerts.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 “DamlCACerts.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 “DamlCACerts.pem” file. **Step 8.** To verify the “DamlCACerts.pem” file is edited properly, display certificate information by using option “E” from the main menu of CertTool Utility. **Note:** Please note that this issue is seen after installing class 3 CA certificate. If you correct the DamlCACerts.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 DamlCACerts.pem file.

		PMR 07331,035,724 - ITIM WinAD64 adapter - prob with WTS attrib When we perform the RECON operation, WinAD adapter returns 0x8000500d (ADS_PROPERTY_NOT_FOUND) error for all WTS attributes. This error is returned for those users which are directly created on Active Directory. This error will occur if you try to access attributes that aren't located in the so-called property cache. It could also be an operational attribute that isn't automatically built in the cache. Windows Active Directory adapter log will display following error message for all WTS attributes: **Error Message: "Failed with Error: 0x8000500d - (null)"** Microsoft has confirmed that this is a known issue in Windows Server 2008 \ Windows Server 2008 R2 Machine. For more information on this issue, Please visit the following Microsoft MSDN Web site: **http://support.microsoft.com/kb/947729** **Workaround:** Set any WTS attribute on Windows Server 2008 \ Windows Server 2008 R2 domain controller for those users which are giving the above error message. To set WTS attributes follow these steps: 1. Open **Active Directory Users and Computers**. 2. Find the user in the Users folder or in the **Organizational Unit** where the user is. 3. Right-click the user account, and then click **Properties**. 4. On the **Environment** tab or **Terminal Services Profile** tab, you will find the settings for WTS attributes value. 5. Doing a single modification on any one of these WTS attribute will resolve the issue. OR Customer can also follow the steps provided in the Microsoft MSDN web site as a workaround OR Running a modify request with WTS attributes from ITIM WinAD Service will also resolve the issue.
		Issue with WTS attributes during Reconciliation Windows AD adapter gives following errors when managing WTS attributes and adapter registry key “WtsDisableSearch” set to FALSE. Following Error occurs when reconciliation is performed. **Could not reconcile WTS attribute erADWTSCallbckNumber. Failed with error 1317: The specified user does not exist.** **Could not reconcile WTS attribute erADWTSInheritInitialProg. Failed with error 1317: The specified user does not exist.** **Could not reconcile WTS attribute erADWTSRemoteHomeDir. Failed with error 1317: The specified user does not exist.** **Could not reconcile WTS attribute erADWTSCallbckSettings. Failed with error 1317: The specified user does not exist.**

		Workaround: No Workaround Available.
		Leaving a space in the base point will cause problems The BasePoint (on Service form including Group Base Point) and the Event Notification Context (in agentCfg) must be in proper DN format and should not contain any space between dc and ou\dc. For Example: If your basepoint value is <DC Name>/ou=testorg01,dc=testlab, dc=com //Here we have space between "dc=testlab," and "dc=com" Then you will have to specify correct baspoint value on service form in the following way: <DC Name>/ou=testorg01,dc=testlab,dc=com
		NetBIOS name must not be greater than 15 characters: The NetBIOS name is 16 ASCII characters, however Microsoft limits the NetBIOS name to 15 characters and reserves the 16th character as a NetBIOS Suffix. The Windows Active Directory adapter does utilize a NetBIOS based lookup for finding the RAS Server and WTS Server. Adapter is limited by the Windows restriction of having a 15 character maximum value for a NetBIOS computer name\NetBIOS domain name. If the NetBIOS domain name or NETBIOS computer name is more then 15 characters then Windows Active directory adapter will display following error message for RAS Server lookup. ERROR_INVALID_DOMAINNAME 1212 "The format of the specified domain name is invalid." Please refer the Microsoft link related to Naming conventions where it specifies a maximum name length of 15 characters: http://support.microsoft.com/kb/909264 **Workaround:** Set the adapter registry key "ForceTerminalServerLookup" and "ForceRASServerLookup" to FALSE value using agentCfg utility provided by adapter. Specify one or more then one target servers for the base point on the Active Directory Adapter service form on IBM Tivoli Identity Manager Server. Specify the target servers which are configured as RAS Server or WTS server. This will resolve RAS and WTS Server lookup issue for Error Code: 1212. Each target server must be separated by '|' (Pipe character) For example: Base Point DN on the service form with only one target server: DC01/OU=engineering,DC=irvine,DC=IBM,DC=com Base Point DN on the service form with more than one target server: DC01|DC02|DC03/OU=engineering,DC=irvine,DC=IBM,DC=com For more detail on configuring user basepoint, please refer the section "Configuring the Users Base Point for the adapter" in Active Directory Adapter Installation and Configuration Guide.

Issue with Special Characters during Recon Operation:

Reconciliation will fail on IBM Tivoli Identity Manager if an attribute's value in recon entry contains one or more of the special characters listed in the below table which are not transformed to their equivalent XML format. When ADK reads an attribute's value it searches for each of the XML transformed value, as listed in below table, in the value string. If it finds any one of these then it considers that entire string is already transformed and will not perform any transformation on that string. In this case ADK does not attempt to check if there are any untransformed special characters in the string. If the value contains other untransformed special characters then they are not transformed by ADK. When IBM Tivoli Identity Manager processes such recon entries they will be failed.

Special Character	Equivalent XML transformation
& (ampersand)	&
' (apostrophe or single quote)	'
" (double-quote)	"
< (less-than)	<
> (greater-than)	>

For Example:
Example 01:
If the value of Description attribute of a user account on Active Directory is "My String & < > END". After reconcile the ITIM server fails this request with following error.

CTGIMD106E An error occurred while processing the request.
Error: The content of elements must consist of well-formed character data or markup.

Here the character < (less than) is not transformed by ADK. This is because ADK found the substring & in the string and considered that the string is already transformed.

Example 02:
If the value of Description attribute of a user account on Active Directory is "My String & & > END". After reconcile the ITIM server fails this request with following error.

CTGIMD106E An error occurred while processing the request.
Error: The entity name must immediately follow the '&' in the entity reference.

This is an error for "unknown entity section" because the "&" is assumed to begin an entity reference.
Here the character & (ampersand) is not transformed by ADK. This is because ADK found the substring & in the string and considered that the string is already transformed.

		Example 03: If the value of Description attribute of a user account on Active Directory is “My String &amp & < END". After reconcile the ITIM server fails this request with following error. CTGIMD106E An error occurred while processing the request. Error: The reference to entity "lt" must end with the ';' delimiter. The first &amp doesn't end with a semicolon ';'. This is because ADK found the substring & in the string and considered that the string is already transformed. **Workaround:** 1. Modify the attribute value in such a way that either all the special characters in the value are replaced by their corresponding XML transformation or none are. Example 04: If the value of Description attribute of an user account on Active Directory is "My String & END" After reconcile the value displayed on ITIM account form is "My String & END". This will not cause any error or failure in the recon but the value displayed on IBM Tivoli Identity Manager’s Account form is not the same as what is on Active Directory. This is because IBM Tivoli Identity Manager does a reverse transformation to get the original character. In this case & will be replaced with & on IBM Tivoli Identity Manager 2. Avoid the use of above special characters in attribute value.

		Adapter based event notification not able to notify updates in attribute of type DNWithBinary to IBM Tivoli Identity Manager. You have extended adapter to manage attribute of type *DNWithBinary*. You have USER1 who's attribute of type *DNWithBinary*, for example, **otherWellknowObjects** contain DN of USER2. If you move or rename USER2 thereby changing DN, the change will be reflected in **otherWellknownObjects** attribute of USER1. The "object DN" part of value related to USER2 will be updated with new DN. The adapter based event notification is not able to identify this change in user1 **Example:** Consider we have two users USER1 and USER2. USER1's **otherWellknownObjects** attribute contains B:32:df447b5eaa5b11d28d5300c04f79ab81: CN=USER2,ou=myou,dc=mydomain,dc=com If you move USER2 to different container say myou2, the DN of USER2 changes to CN=USER2,ou=myou2,dc=mydomain,dc=com Active Directory updates the USER1's **otherWellknownObjects** with new DN of USER2 as B:32:df447b5eaa5b11d28d5300c04f79ab81: CN=USER2,ou=myou2,dc=mydomain,dc=com Even though USER1 is modified in such scenario it is not get notified by the adapter based event notification. The value of the extended attribute is not changed on IBM Tivoli Identity Manager. It will show old value i.e. B:32:df447b5eaa5b11d28d5300c04f79ab81: CN=USER2,ou=myou,dc=mydomain,dc=com **Workaround:** To update modified user i.e. USER1 on IBM Tivoli Identity Manager in such scenario we need to perform lookup for USER1 or full Recon.

		Adapter based event notification not able to notify updates to IBM Tivoli Identity Manager when all values of attribute are deleted directly on Active Directory Active Directory treats some attributes differently for example: *mail*, *info*, *otherWellknownObjects*, *msRTCSIP-UserPolicy* etc. For such attributes when all the values of the attribute are deleted from Active Directory, the attribute also get deleted from the user object. Since the attribute is deleted from Active Directory, The adapter based event notification does not identify such deleted attribute and so IBM Tivoli Identity Manager is not updated. **Workaround:** To clear all values from the IBM Tivoli Identity Manager perform full recon or Lookup operation
		Windows Active Directory Adapter does not support *Replace* operation format for ProxyAddress and *UM Addresses (Extensions)* attribute when using unified messaging feature for Mailbox. Proxy Address and UM Addresses (Extensions) attributes are treated differently on ITIM, even though both are stored on Windows Active Directory under same attribute Proxy Address. On ITIM when we add UM Addresses (Extensions) in editable text list. Which is stored on the Active Directory in user object under the Proxy address attribute however on ITIM it display all extension values under UM Addresses (Extensions) attribute. While using REPLACE operation type for proxy address it will send value with operation type replace for all the new added values (Consider a case when Proxy Address attribute does not contain any UM Addresses (EUM) on ITIM account form) and also the old values which were set for Proxy Address on ITIM. In this case because of API limitation Active Directory Adapter will clear all the values of proxy addresses which in turn also clear UM Addresses (Extensions) value on Active Directory. While using ADD/DELETE operation type for Proxy Addresses or UM Addresses (Extensions) it will send value with operation types ADD/DELETE and Active Directory adapter accordingly ADD/DELETE the values in Proxy Address attribute on Active Directory. **Workaround:** Use ADD/DELETE operation format for Proxy Address and UM Addresses (Extensions) attribut when using unified messaging feature for mailbox

Issue with IBM Tivoli Identity Manager while performing Reconciliation/Filtering operation.

IBM Tivoli Identity Manager returns error for Unified Messaging MailBox Policies which contains below special characters while Reconciliation/Filtering operation.

Special Character	**Equivalent XML transformation**
< (less-than)	<
> (greater-than)	>

IBM Tivoli Identity Manager returns error while opening user's account for **modification** if the user's Unified Messaging Mailbox Policy attribute (which is having Dropdown Box) value contains below special characters.

Special Character	**Equivalent XML transformation**
< (less-than)	<
> (greater-than)	>
"(double-quote)	"
&(ampersand)	&

Example:

- If user has Unified Messaging Mailbox Policy attribute with value "**CN=TestPolicy<1,CN=UM Mailbox Policies,CN=Exchange First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=orion,DC=com**"

The following error will appear on ITIM form while opening account for modification.

CTGIMU552E Error Occurred while communicating with server
CTGIMU576E An error occurred while trying to retrieve custom form

Workaround:
Avoid the use of above special characters for Unified Messaging Mailbox Policy.

Installation and Configuration Notes

See the IBM Tivoli Identity Manager Adapter Installation Guide" for detailed instructions.

Running v4.6 and v5.0 Adapters on the Same Server

The Identity Manager version 5.0 adapters have enhanced capabilities that are not compatible with older version 4.6 adapters. It is highly recommended that all adapters hosted on an individual server are upgraded at the same time.

Adapters installed on the same server may share common components or run-time environments. The version 4.6 adapters may not be compatible with the version 5.0 component and may no longer operate as expected after installation of a version 5.0 adapter. On Windows servers all adapters must be upgraded simultaneously due to the sharing of DLLs. Check the adapter installation guide for additional information.

Corrections to Installation Guide

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

Correction to Chapter 3: Installing and Configuring the Active Directory Adapter

The installation instructions should be modified to read as follows:

Chapter 3. Installing and configuring the Active Directory adapter -> **Installing the adapter**

Installing the adapter

If the Active Directory Adapter is not automatically installed with your IBM Tivoli Identity Manager product,
use the adapter installer to manually install the adapter. The IBM Tivoli Identity Manager Active Directory Adapter installation program is available for download from the IBM Web site. Contact your IBM account representative for the Web address and download instructions.

To manually install the adapter, complete these steps.

Note: All directory paths apply to Windows operating systems. Change the directory paths as needed for UNIX operating systems.

1. If you downloaded the installation software from Passport Advantage, perform the following steps:
   - Create a temporary directory on the computer on which you want to install the software.
   - Extract the contents of the compressed file into the temporary directory.

2. Start the installation program with the *SetupAD64.exe* file in the temporary directory.

3. Select the language and click **OK** to display the Introduction window.

4. On the Introduction window, click **Next**.

5. Select either Typical installation or Update installation and click Next to display the Choose Install Folder window. Remember that the adapter must already exist if you want to perform an updated installation.

6. Specify where you want to install the adapter in the Directory Name field. Do one of the following.
   - Click **Next** to accept the default location.
   - Click **Browse** and navigate to a different directory and click **Next**.

7. Do the following at the Software License Agreement window:
   - Review the license agreement and select **Accept**.
   - Click **Next**.

8. Review the installation settings at the Pre-Installation Summary window and do one of the following:
   - Click **Previous** and return to a previous window to change any of these settings.
   - Click **Install** when you are ready to begin the installation.

9. Click **Done** on the Install Complete window.

Correction to Chapter 4: Troubleshooting the Active Directory Adapter

The following new section "Troubleshooting the Active Directory Adapter expands the existing chapter 4 content.

Chapter 4. Troubleshooting the Active Directory Adapter errors- > Active Directory Adapter errors

Error message
Error: Could not retrieve WTS attribute inherit initial program. Error 87: The parameter is incorrect

Recommended action:
A cause of this error is because the target server specified in Base Point DN on service form does not run Windows Terminal Services.
Ensure that the target server specified for Base Point DN has Windows Terminal Services running.

Correction to Chapter 6: Customizing the Active Directory adapter

"Step 6: Create a new JAR file" does not specify the correct case of the JAR file name. The directory and the name of the JAR file must be "ADprofile (lowercase "p").

```
jar –cvf ADprofile.jar ADprofile
```

PMR 33834,999,760 - WinADAdapter failed to load exschema.txt at system bootup

Chapter 9. Troubleshooting -> Warnings and error messages -> Table 17

Correction to Recommended Action for error message "Error binding to schema container error code. Loading of extended schema attribute attribute name failed."

Error message	Recommended action
Error binding to schema container error code. Loading of extended schema attribute attribute name failed.	(Existing recommendations are also valid) When the adapter service is started, the adapter reads exschema.txt and binds to the default domain i.e. domain in which adapter is running to check the syntax of the specified

	attribute. Since checking the syntax of extended attribute is one time process it is done at the startup. If adapter fails to bind to the default domain then it will not manage any of the extended attributes. Ensure that: 1. At least one domain controller is accessible before starting Active Directory adapter service. 2. The user account under which the adapter service is running has permission to read the Active Directory schema.

Chapter 4. Troubleshooting the Active Directory Adapter errors- > Active Directory Adapter errors

(For IZ67106 - INTERMITTENT 0X80004002 ERRORS WHEN ATTEMPTING TO MANAGE/PROVISION MAILBOXES)

Error message
errorMessage="Unable to contact Exchange services. ADSI Result code: 0x80004002"

Recommended action:
The Exchange provider uses Collaboration Data Objects for Exchange Management (CDOEXM) for a user object. CDOEXM makes use of several static variables, since the lifetime of these variables last until process end. These static variables were being reallocated every time CDOEXM was loaded. Since all CDOEXM work was done in the lifetime of the worker thread, CDOEXM was being loaded and unloaded repeatedly. Under certain conditions, CDOEXM is incorrectly marked as initialized, though CDOEXM is not fully initialized. Therefore, later attempts to use CDOEXM do not succeed. You can use the new feature “Thread Pooling" of Windows Active Directory Adapter.

Additional information can be found under the “Configuration Notes->Enable/Disable “UseThreadPooling”” section.

Chapter 4. Troubleshooting the Active Directory Adapter errors- > Active Directory Adapter errors- >

Table 8. Troubleshooting the Active Directory Adapter errors

Error message:
GetNextRow failed. Error code: 0x000000ea - Calling GetNextRow can potentially return more results.. Provider: LDAP Provider
Waiting for 5 minutes before calling GetNextRow

Recommended action:
This error occurs when Reconciliation is run while the Active Directory server is under load, a logging message may appear in the WinAD Adapter log that says, "Error_More_Data.". The Active Directory Adapter retrieves data from the Active Directory in a paged manner. The adapter reconciles users, groups, containers, MailboxStore and MailboxPolicy and attempts to retrieve data in a maximum of three attempts.

The Adapter is designed to retry the query three times before terminating the Reconciliation

For additional information see the Release Notes under Configuration Notes-> Log Message: Error More Data (page 26)

Changing protocol configuration settings -> Table 5. Options for the DAML protocol menu -> Option 'k'

Modify Property 'READ_TIMEOUT':

Type the time out value for Tivoli Identity Manager and the adapter connection in seconds.

This applies to setups that have a firewall between Tivoli Identity Manager and the adapter. This firewall has a time out value that is less than the maximum connection age DAML property on Tivoli Identity Manager. When your transactions run longer than the firewall time out,
the firewall terminates the connection. The sudden termination of connections might leave the adapter with incorrect connection threads causing the adapter to crash.

When the adapter crashes randomly because of the specified setup, change the value for the READ_TIMEOUT. **The value must be in seconds and less than the firewall's time out value**.

Additions to User Guide

Extended Attributes

The adapter supports processing of multi valued string syntaxes extended attribute as add, delete, and replace attribute operation. This signifies whether to append, delete, or replace values in the request to/from the set of values set for the corresponding Active Directory side attribute.

Please refer to section “MR052609514 - customer wants to use the extend attribute transformed the name on itim side using the AD 5.0.5 adapter on ITIM 4.6 Server.” under “Configuration Notes” in Release Notes on how to specify extended attribute using exschema.txt file.

There can be cases where you have an extended attribute with a corresponding Active Directory side attribute which is already managed by the adapter. When a full reconciliation or user lookup is performed the values set using the extended attribute will also be returned for the attribute which is already been managed by the adapter and vice versa. This is because both these attributes corresponds to the same attribute on Active Directory.

Please refer to “Appendix B. Active Directory Adapter attributes” in User Guide for list of adapter attributes and their corresponding Active Directory side attribute name which the adapter manages.

MR0721117156 - WinAD/WinAD64 adapter: Allow support for Octet String data type in extended attributes.

The adapter now supports Octet String as an extended attribute type. It is assumed to be passed as a string value. It must have an even number of characters. There are no adapter specific errors for this attributes, but it may return windows AD error codes.

MR0204103013 - AD adapter support for DNWithBinary.

Chapter 4. Troubleshooting the Active Directory Adapter errors- > Active Directory Adapter errors

No.	Error Messages	Recommended action
1	“Value specified is not in the proper format”	Ensure that value format of extended attribute of type DNWithBinary is **B :< char count> :< binary value> :< object DN>**
2	"Value specified for the attribute does not start with character 'B'."	Ensure that value specified for extended attribute of type DNWithBinary is start with character ‘**B**’ only.
3	"Value given after '**B:**' is not correct. Expected value is the total number of Hexadecimal Digit count."	For extended attribute of type DNWithBinary, verify that value given after **B:** i.e. **<char count>**is total number of Hexadecimal Digit count. It should not contain any alphabetical character or any special character.
4	"Hexadecimal value does not contain the number of characters specified in the character count."	For extended attribute of type DNWithBinary, verify that total number of hexadecimal digit count specified in the **<char count >** is equal to number of hexadecimal characters

		specified in the **<binary value>**
5	"Wrong Digit in Hex String"	For extended attribute of type DNWithBinary, verify that value given in the **<binary value>** contain only hexadecimal character i.e. it should contain characters 0-9 or A,B,C,D,E,F or combination of both.
6	"value is not set on resource due to invalid constraint"	This error occurs when the specified value for the extended attribute of type DNWithBinary violates any constraint associated with that attribute. **For example**, a constraint could be: 1)**<object DN>** in the value should be a distinguished name of existing user object 2) Maximum or minimum number of bits in the hexadecimal value. Ensure that the specified value for the attribute does not violate these constraints.
7.	“Hexadecimal value should always contain even number of characters.”	For extended attribute of type DNWithBinary, verify that value given in the **<binary value>** contain only even number of hexadecimal characters.

MR090210587 - Support for Exchange Unified Messaging management

Chapter 4. Troubleshooting the Active Directory Adapter errors- > Active Directory Adapter errors

No.	Error Messages	Recommended action
1	“Attribute can be set only if Mailbox is enabled for Unified Messaging. To enable Unified Messaging both values UMMailbox Policy and UM Addresses(Extensions) are required”	Ensure that valid values of both UMMailbox Policy and UM Addresses (Extensions) are specified in the request while enabling user for Unified Messaging.
2	“Attribute Operation Type is not supported.”	Ensure that value specified for UM Addresses (Extensions) is not of operation type MODIFY.
3	"Attribute cannot be set. Mailbox is Disabled for Unified Messaging."	Ensure that request should not contain Unified Messaging attributes with operation ADD/MODIFY while disabling user’s MailBox for Unified Messaging.
4	"Attribute cannot be set. Error occurred While trying to Disable MailBox for Unified Messaging."	This error occur if disable Unified Messaging is failed and if request contains UM Addresses (Extensions) attribute with operation type ADD/MODIFY

5	"Attribute cannot be delete. Error occurred While trying to Disable MailBox for Unified Messaging."	This error occur if disable Unified Messaging is failed and if request contain UM Addresses (Extensions) attribute with operation type DELETE

Corrections to User Guide

Chapter 3. Active Directory Adapter user account management tasks-> Suspending user accounts

When you suspend a user account, the status of the user account on IBM Tivoli Identity Manager Server becomes inactive, and the user account becomes unavailable for use. Suspending a user account does not remove the user account from IBM Tivoli Identity Manager Server. For more information about suspending user accounts, see the IBM Tivoli Identity Manager Information Center.

When you suspend a user account from IBM Tivoli Identity Manager, the Active Directory Adapter sets the property flag ACCOUNTDISABLE of the userAccountControl attribute on the Active Directory. For more information about property flags of the userAccountControl attribute, see the Microsoft Windows Server documentation.

When you suspend a user account from IBM Tivoli Identity Manager, the adapter also suspends the user's mailbox (Disable\Disconnect User mailbox). The adapter suspends the user mailbox, if the user account is enabled for a mailbox and adapter registry "DisableMailboxOnSuspend" is set to TRUE. If the value of adapter registry "DisableMailboxOnSuspend" is set tot FALSE then adapter will not disable user mailbox but only suspend the user account. The suspended (Disable\Disconnected) user mailbox can be reconnected again through IBM Tivoli Identity Manager Server account form. For more information about Disable mailbox, see the configuration notes for "Disable Mailbox Support for Exchange Server 2007 and Later" in Release Notes.

Chapter 3. Active Directory Adapter user account management tasks-> Deleting user accounts

Use the deprovision feature of IBM Tivoli Identity Manager to delete user accounts. For more information about deleting user accounts, see the IBM Tivoli Identity Manager Information Center.

When you deprovision a user account from IBM Tivoli Identity Manager, the Active Directory Adapter:
Deletes the user account from the Active Directory.
Disable the mailbox of the user account from the Exchange server, if the user account is enabled for a mailbox.
Removes the membership of the user account from the groups that the user account is a member of.
Deletes the home directory of the user account, if the value of the **delUNCHomeDirOnDeprovision** registry is TRUE.
Deletes the profile of the user account, if the value of the **delRoamingProfileOnDeprovision** is TRUE.
Deletes the WTS home directory of the user account, if the values of the **delUNCHomeDirOnDeprovision** and the WtsEnabled registry keys are TRUE.
Deletes the WTS profile of the user account, if the values of the

delRoamingProfileOnDeprovision and the WtsEnabled registry keys are TRUE.

Note: The Active Directory Adapter does not support the deletion of local home directories and user Mailbox.

Chapter 3. Active Directory Adapter user account management tasks-> Deleting user accounts-> Deleting a mailbox

Adapter does not have a feature to delete a mailbox. To disable a mailbox of a user account clear the value of the Mailbox Store attribute on the Active Directory account form.

When the mailbox for a user account is disabled, the adapter does not permanently delete the mailbox from the Exchange server. But the mailbox is flagged as disconnected by the Exchange server. When the mailbox for a user account is disabled, creating another mailbox for the same user account with the same alias creates a new mailbox.

By default, the Exchange server preserves the deleted mailbox for a specific duration. An administrator can configure this duration.

By default all the deleted/disabled mailboxes stay in the mailbox store for 30 (thirty) days. This value can be set at mailbox store level.
Following are the steps to modify this value directly on Exchange Server:
1. Open Exchange Management Console
2. Expand Server Configuration
3. Click on Mailbox
4. Select your server in the Mailbox Pane
5. Select the <Mailbox> you want to configure and click on the Properties of selected Mailbox Database.
6. Set value Under Mailbox Database Properties->Limits->Keep deleted mailboxes for (days)->30

Please note that mailbox with no mails will not be moved to Disconnected mailbox. They are completely deleted from database when disconnected.

You can connect the disconnected mailbox to a user account. The name of the mailbox is changed according to the user account name. For more information about Disable mailbox, see the configuration notes for "Disable Mailbox Support for Exchange Server 2007 and Later" in Release Notes.

Chapter 3. Active Directory Adapter user account management tasks-> Adding user accounts-> Enabling a user account for mail

There can be two types of Active Directory user accounts:

Mail-enabled
An account that has an e-mail address associated with it, but has no mailbox on the Exchange server.

A mail-enabled user can send and receive e-mail using another messaging system. If you send messages to a mail-enabled user account, then these messages pass through the Exchange server, and are forwarded to an external e-mail ID of that user account. For example, Thomas is an employee of company1, with a mailbox on the Exchange server of company1, and an e-mail ID thomas1@company1.com. Company2 takes over company1. The employees of company1

have mail-enabled user accounts in the domain of company2. The new e-mail ID of Thomas is thomas1@company2.com.

Therefore, Thomas can send and receive mail with the new e-mail ID, but the mailbox for Thomas is not on the Exchange server of company2. It is on the Exchange server of company1.

Mailbox-enabled
An account that has a mailbox on the Exchange server. A mailbox-enabled user can send and receive messages, and store messages on the Exchange server mailboxes.

To create a mail-enabled user account, you must specify a value for the **Target Address** attribute on the Active Directory account form.

To create a mailbox-enabled user account on **Exchange 2007**, you must specify a value for the **Mailbox Store** attribute on the Active Directory account form.

To create a mailbox-enabled user account on **Exchange 2010**, it is optionally required to specify a value for the **Mailbox Store** attribute on the Active Directory account form however if the value is not specified Windows Active Directory Adapter will use Default MailBox Feature of Exchange 2010 and it will create Default MailBox for that User. After creating Default MailBox, it is necessary to perform user lookup to view the value of Default MailBox on ITIM under MailBox Store attribute.

You can also create a mailbox-enabled user account by connecting the disconnected mailbox to a user account. The name of the mailbox is changed according to the user account name. For more information about connecting a disconnected mailbox to a user account, see the configuration notes for "Disable Mailbox Support for Exchange Server 2007 and Later" in Release Notes.

Note: The 64-bit adapter cannot create mailboxes on Exchange 2003 servers. The adapter can move Exchange 2007 mailboxes to Exchange 2003 servers so that Exchange 2003 mailbox stores are available as supporting data when selecting a mailbox store on the Active Directory account form. However, you cannot use Exchange 2003 mailbox stores when creating a new mailbox.

The Exchange server uses the value of the Alias attribute to generate an e-mail ID for a user account. If you do not specify a value for the Alias attribute, the Exchange server uses the value of the User Principal Name attribute as the default alias. For example, for a user account thomas with the user principal name thomasd@ibm.com, the Exchange server uses the value thomasd as the alias. If the value of the Alias attribute of another user account matches an existing alias, then the Exchange server appends a number to the e-mail ID of the other user account. For example, a user account Thomas with alias thomas1 exists on the Active Directory. The e-mail ID of Thomas is thomas1@ibm.com. If you create another user account Nancy with alias thomas1, then the Exchange server generates the e-mail ID thomas12@ibm.com for Nancy.

Note: If you specify both the attributes, Mailbox Store and Target Address, then the Active Directory Adapter gives an error.

Configuration Notes

The following configuration notes apply to this release:

Note that the “supported configurations” diagrams have been moved into the Installation Guide.

Exchange 2007 and Exchange 2003 in Co-Existence Mode

The WinAD64 adapter supports Exchange 2007/2003 co-existence mode but Microsoft lists several important limitations. The adapter enforces these same limitations (see Microsoft link below).

- Exchange 2007 mailboxes must be managed with Exchange 2007 management console or shell.
- Exchange 2007 mailboxes MUST NOT be managed with Exchange 2003 tools. Note that this is not blocked, but mailboxes managed from Exchange 2003 ADUC will not be fully functional.
- Exchange 2003 mailboxes can be edited or removed with Exchange 2007 tools, but cannot be created by Exchange 2007 tools.
- Both Exchange 2003 and Exchange 2007 mailboxes can be moved (in either direction) with the Exchange 2007 tools. Exchange 2003 move mailbox cannot be used to move mailboxes to or from Exchange 2007 mailbox server.

Based on the above restrictions, the WinAD64 adapter has the following capabilities:

- Exchange 2007 mailboxes can be full managed
- Exchange 2003 mailboxes can only be modified. Attempts to create a 2003 mailbox will fail.

WARNING: The WinAD64 adapter is not designed to convert mailboxes to 2007 format.
While it is possible for the WinAD64 adapter to move a mailbox from a 2003 mailbox to a 2007 mailstore, doing so will cause a conversion of the mailbox. The conversion may cause the TIM transaction to time out. Converting mailboxes is not a supported function of the WinAD64 adapter; use the Exchange 2007 tools to convert mailboxes.

For additional Exchange information, please refer to Microsoft web-based resources:
http://msexchangeteam.com/archive/2006/10/09/429135.aspx

Deleting a Mailbox

To delete a Mailbox, delete the Mailbox Store attribute. Submit a reconciliation request to clear unnecessary values from the account form and to verify that the mailbox has been removed.

Directory NTFS and Share Access

The Agent returns the actual, effective permissions granted to a user and not the specific access assigned to the user account. For example, if the directory grants FULL permission to the Everyone group but only CHANGE permission to the user's account, a reconciliation request will return the account access permission as FULL. Therefore, it is necessary to properly define the policies local to the managed resource prior to using Tivoli Identity Manager to prevent these types of conflicts.

Expiration Date

Per Microsoft's documentation, the Active Directory Users and Computers MMC snap-in will display the account expiration date as one day earlier than the date contained in the accountExpires attribute. The Tivoli Identity Manager Server will display the value contained in the account expires attribute.

Password Properties

The password properties are specific to the account. However, these properties can be overridden by the security policies of the managed resource (Domain Controller Security Policies, Domain Security Policies, and Local Security Policies).

Setting Language Preference for Accounts

The Languages attribute (eradlanguage) is an Exchange attribute. If using a configuration without Exchange, setting this attribute will return a warning.

Log Message: Error More Data

NOTE: If Reconciliation is run while the Active Directory server is under load, a logging message may appear in the WinAD Adapter log that says, “Error_More_Data.” The Adapter is designed to retry the query three times before terminating the Reconciliation. Please see the Microsoft Knowledge base article below for more information.

When the IDirectorySearch::GetNextRow function returns S_ADS_NOMORE_ROWS, it may not have retrieved all the data from the server. In some cases, S_ADS_NOMORE_ROWS is returned by GetNextRow function when the server was unable to find an entry that matched the search criteria within a predefined two-minute time limit. This two-minute time limit is defined by means of an LDAP policy.

If the server exceeds the two-minute time limit, it returns an LDAP cookie in the response so that you can restart the search where it left off. Inefficient searches and heavily loaded systems can cause the server to exceed the time limit. When the server cannot find an efficient index to search, the server may have to apply the filter to every object in the directory, in which case it can run through many entries and not find a match within the two-minute time limit.

Therefore, when returning S_ADS_NOMORE_ROWS, ADSI also sets an extended error code, which can be queried using ADsGetLastError function. If ADsGetLastError returns ERROR_MORE_DATA, it means that the server has not completed the query and must call GetNextRow again.

The AD Agent code is structured as per the logic above and what Microsoft has advised. It attempts to get data from the paged result in max 3 attempts. The AD Agent code is structured to have 5 minutes delay for first attempt, 10 minutes delay for second attempt and 15 minutes delay for third attempts. If the AD Agent is running on AD server itself, moving the AD Agent onto a different machine would take off some load from AD server.

In addition to this Microsoft has provided an article as how to configure the LDAP policy so as to customize the Active Directory searches. http://support.microsoft.com/kb/315071/EN-US/.

Use SSL Configuration Option

The registry setting “useSSL” is to enable SSL communicating between AD Agent and Active Directory. If TRUE, agent communicates over SSL with Active Directory. If this key is not present or FALSE, agent does not use SSL.

By default this key is set to FALSE. No ITIM side changes are required to use this enhancement.

Following resource side changes are required to use this feature.

a. Active Directory must have enabled Public Key Infrastructure (PKI). For this Enterprise Certificate Authority should be installed on one of the domain controller machine in the domain. Setting up an

enterprise certificate authority causes an Active Directory server to get a server certificate that can then be used to do SSL-based encryption.

b. Machine on which AD Agent is running should have certificate installed. The certificate is issued by CA as mentioned in point (a).

Use Default DC Configuration Option

The useDefaultDC registry setting is to provide failover capability to agent when host specified in base point is down. If agent is unable to connect to hostname specified in base-point and key is set to TRUE, agent will connect to the base-point without the host name. If it still fails then agent will report failure. By setting this key to TRUE also affects behavior of RAS server and Terminal server lookup.

Caution: When the adapter is deployed in a cross-domain scenario, the useDefaultDC option should always be set to FALSE to avoid provisioning to an unintended domain. For example, if the adapter is installed in domain A but provisioning to domain B, and the host in domain B is down, the adapter will detect the default domain as domain A.

By default this key is set to FALSE.

The behavior of agent will be as follows:

A. useDefaultDC = FALSE

   i. If hostname (target server name) is specified in the base point and ForceRASServerLookup and ForceTerminalServerLookup registry keys are set as FALSE, then agent uses the given hostname as RAS server and Terminal server.

   ii. If hostname (target server name) is specified in the base point and ForceRASServerLookup and ForceTerminalServerLookup registry keys are set as TRUE, then agent will determines the RAS and Terminal server name.

B. useDefaultDC = TRUE and host is down.

   i. Agent will determines RAS and Terminal server irrespective of values set for ForceRASServerLookup and ForceTerminalServerLookup.

Use new Win2003 ADSI API for managing WTS attributes

Agent will use WTS ADSI API's or old style WTS API's to set or retrieve WTS attributes. Agent will try to use WTS ADSI API's, if it fails to get interface or attribute is not supported then agent will use old style WTS API's.

If agent is running on Windows 2003 then agent will use WTS ADSI API's. On Windows 2000 agent will use old style WTS API's.

From log it can be found out which WTS API's agent is using. Some of the attributes are not supported by WTS ADSI API's; for that agent will use old style WTS API's on Windows 2000 and Windows 2003.

If debug logging is enabled, then agent will show lines like:

- *Start using extended interface for WTS Attributes for getting WTS attribute.*
- *Start using extended interface for WTS Attributes for setting WTS attribute.*

- *End using extended interface for WTS Attributes for setting WTS attribute.*
- *End using extended interface for WTS Attributes for getting WTS attribute.*

This means agent is using WTS ADSI API's.

If log is showing lines like:

- *Using old style API for WTS Attributes for getting WTS attribute*
- *Using old style API for WTS Attributes for setting WTS attribute*

This means agent is using old style WTS API's.

Win AD Agent handle Add and Delete operations for erGroup attribute

WinAD Adapter by default honors only replace operation from Tivoli Identity Manager. WinAD Adapter now supports Add and Delete operation for erGroup attribute for Modify request.

On Tivoli Identity Manager profile changes are required in ADprofile to send group operation as add, delete for modify request.
See the steps below

- Locate the following line in resource.def file under <Operation Name="modify"> tag.

```
<Parameter Name="erGroup" Source="account" ReplaceMultiValue="true" />
```

- Replace the above line with following line.

```
<Parameter Name="erGroup" Source="account" />
```

- Reinstall the profile. Please see Windows Active Directory Adapter Install guide for further references.

Support for LastLogonTImeStamp Attribute

This version of Windows Active Directory Adapter supports lastLogonTimeStamp attribute of Active Directory. Attribute lastLogonTimeStamp is available on Windows 2003 domain functional level and is replicated. The default replication interval is 14 days, but some customers have increased this frequency so that the attribute can be used as a basis for Dormant Account reporting.

To support this enhancement, the profile of Windows Active Directory Adapter is extended. A new Date attribute erADLastLogonTimeStamp (OID: 1.3.6.1.4.1.6054.3.125.2.146) is defined and added in erADAccount class. A new label (eradlastlogontimestamp=Last Login Time Stamp) is added to CustomLabels.properties file.

Note: The attribute erADLastLogonTimeStamp is not visible on account form. To bring it on account form, form customization is required.

Remote Access Permission Attribute

Windows Active Directory Adapter has Boolean attribute "erADAllowDailin" to represent msNPAllowDialin. As attribute "erADAllowDialin" is Boolean and can not be used to represent three values, Windows Active Directory Adapter schema is extended. A new String attribute "erADExDialin" (OID: 1.3.6.1.4.1.6054.3.125.2.145) is added in erADAccount class.

Attribute "erADExDialin" is added to the Windows Active Directory Adapter account form (erADAccount.xml). Following new labels are added to CustomLabels.properties file.

eradexdialin=Dial-in
tag.dialin.allow=Allow Access
tag.dialin.deny=Deny Access
tag.dialin.none=Control access through Remote Access Policy

The account form now has a combo box instead of a checkbox representing one of the three values for dial-in. The default value is “Deny Access”.

Value displayed on account form	Value sent in request and stored in TIM LDAP
Allow Access	TRUE
Deny Access	FALSE
Control access through Remote Access Policy	NONE

NOTE:

1. Attribute "erADAllowDailin" is deprecated and removed from the account form. It will not be processed by adapter.
2. If you have any business logic around attribute "erADAllowDialin" then you must modify it to use "erADExDialin".

Upgrading from TIM v4.6 Profile

(applicable only for customers using profile shipped with Adapter build 4.6.1024)

If you are using profile which is shipped with Windows Active Directory Adapter build 4.6.1024, following changes required in IBM Tivoli Identity Manager LDAP schema.

In release 4.6.1024, following attribute was added:

erADExDialin 1.3.6.1.4.1.6054.3.125.2.138

In WinAD64-4.6.0 & WinAD64-5.0.1, following 7 new attributes are added :

erADEAllowedAddressList 1.3.6.1.4.1.6054.3.125.2.138
erADEOutlookWebAccessEnabled 1.3.6.1.4.1.6054.3.125.2.139
erADEActiveSyncEnabled 1.3.6.1.4.1.6054.3.125.2.140
erADEMAPIEnabled 1.3.6.1.4.1.6054.3.125.2.141
erADEEnableRetentionHold 1.3.6.1.4.1.6054.3.125.2.142
erADEStartRetentionHold 1.3.6.1.4.1.6054.3.125.2.143
erADEEndRetentionHold 1.3.6.1.4.1.6054.3.125.2.144

If you are using profile shipped with Windows Active Directory Adapter version 4.6.22 (adapter build 4.6.1024), then importing Windows Active Directory Adapter (64-bit) schema will not create attribute erADEAllowedAddressList.

Change erADExDialin OID to 1.3.6.1.4.1.6054.3.125.2.145 in Windows Active Directory Adapter schema and add it to the Windows Active Directory Adapter (64-bit) schema. Henceforth OID 1.3.6.1.4.1.6054.3.125.2.145 OID used in default Windows Active Directory Adapter schema.

You must perform the following schema changes prior to installing this version:

1. Stop the IBM Tivoli Identity Manager Server.
2. Stop the IBM Tivoli Directory Server Instance (LDAP service).

3. Locate the V3.modifiedschema file under the ITIM LDAP instance home directory.
4. Create a backup of the V3.modifiedschema file, for example V3.modifiedschema.backup.
5. With a text editor, open the V3.modifiedschema file and locate the "1.3.6.1.4.1.6054.3.125.2.138" string.
6. Replace "1.3.6.1.4.1.6054.3.125.2.138" with "1.3.6.1.4.1.6054.3.125.2.145"
7. Save the file V3.modifiedschema and exit the editor.
8. Restart the IBM Tivoli Directory Server Instance (LDAP service).
9. Restart the IBM Tivoli Identity Manager Server.

Solving Replication Delay while Adding Mailbox on Exchange 2007

On exchange 2007 when creating a mailbox or mail enable a user during its creation, an error may be returned from Active Directory saying the user does not exist. This is because of a delay in replication among the DCs. Because of this replication delay, Exchange may not find an account on a DC if it is other than the one on which the account is created.

If you encounter this error while creating mailbox or mail-enable an user, then specify the Base Point on service form along with target server on IBM Tivoli Identity Management Server for Active Directory Adapter service. Specifying a Base Point will ensure that the adapter uses the same DC for both the user creation in AD and the Exchange mailbox request. The Base Point must contain the name of the Domain Controller.

Example

```
Base Point DN: DC01/ou=Test,dc=MyDomain,dc=com.
```

Using DN or GUID for the ergroup Attribute

Windows Active Directory Adapter has been enhanced to support Group DN and Group GUID values for erGroup attribute. With this enhancement, multiple groups with the same name that are present in different organizational units on active directory can be processed by the adapter.

Beginning with this version of the adapter, the new registry key "UseGroup" is introduced. The default value for this key is CN. The registry key value can be set to CN or DN or GUID as per the requirement.

Configuration required for using this feature: Perform the following steps (steps A through D):

A. Set the UseGroup registry key to CN or DN or GUID using agentCfg.
B. Change the profile files “erADAccount.xml” and “resource.def” Find the table below describing what change need to be done when UseGroup registry value is set to CN or DN or GUID

Find the table below describing what change need to be done when UseGroup registry value is set to CN or DN or GUID

Use Group value	Change required in
CN It is default value	**erADAccount.xml** <formElement name="data.ergroup" label="$ergroup"> <searchFilter multiple="true" type="select"> <filter>(objectclass=eradgroup)</filter> <base>contextual</base> **<attribute>eradgroupcn</attribute>** **<sourceAttribute>eradgroupcn</sourceAttribute>** <size></size> <objectClass></objectClass> <showQueryUI>false</showQueryUI>

	<paginateResults>false</paginateResults> </searchFilter> </formElement> **Resource.def** <ServiceGroups> <GroupDefinition ProfileName="ADGroupProfile" ClassName = "erADGroup" RdnAttribute = "erADGroupGUID" AccountAttribute = "erGroup"> <AttributeMap> **<Attribute Name="erGroupId" Value="erADGroupCN" />** **<Attribute Name="erGroupName" Value="erADGroupCN" />** <Attribute Name="erGroupDescription" Value="description" /> </AttributeMap> </GroupDefinition> </ServiceGroups>
DN	**erADAccount.xml** <formElement name="data.ergroup" label="$ergroup">> <searchFilter multiple="true" type="select">> <filter>(objectclass=eradgroup)</filter> <base>contextual</base> **<attribute>eradgroupdn</attribute>** **<sourceAttribute>eradgroupdn</sourceAttribute>** <size></size> <objectClass></objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement> **Resource.def** <ServiceGroups> <GroupDefinition ProfileName="ADGroupProfile" ClassName = "erADGroup" RdnAttribute = "erADGroupGUID" AccountAttribute = "erGroup"> <AttributeMap> **<Attribute Name="erGroupId" Value="erADGroupDN" />** **<Attribute Name="erGroupName" Value="erADGroupDN" />** <Attribute Name = "erGroupDescription" Value="description" /> </AttributeMap> </GroupDefinition> </ServiceGroups>
GUID	**erADAccount.xml** <formElement name="data.ergroup" label="$ergroup">> <searchFilter multiple="true" type="select">> <filter>(objectclass=eradgroup)</filter> <base>contextual</base> **<attribute>eradgroupdn</attribute>** **<sourceAttribute>eradgroupguid</sourceAttribute>**

	<size></size> <objectClass></objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement> Resource.def <ServiceGroups> <GroupDefinition ProfileName="ADGroupProfile" ClassName = "erADGroup" RdnAttribute = "erADGroupGUID" AccountAttribute = "erGroup"> <AttributeMap> **<Attribute Name="erGroupId" Value="erADGroupGUID" />** **<Attribute Name="erGroupName" Value="erADGroupDN" />** <Attribute Name = "erGroupDescription" Value="description" /> </AttributeMap> </GroupDefinition> </ServiceGroups>

NOTE:

1) The value of the “attribute” tag of the formElement “data.ergroup” in erADAccount.xml should match with the value of “erGroupName” in resource.def.
2) The value of the “sourceAttribute” tag of the formElement “data.ergroup” in erADAccount.xml should match with the value of “erGroupId” in resource.def
3) Keep the value of the “sourceAttribute” tag of the formElement “data.eradprimarygroup” unchanged to “eradprimarygrptkn”. This value has to remain unchanged for CN, DN or GUID support.

C. Build the ADprofile.jar and import the new profile into TIM
D. Run a full reconciliation.

NOTE: If an event notification is enabled, delete the event notification data base using the agentCfg (Refer Install guide for the deleting the event notification database) and then run a full reconciliation. This will make sure that new database get created with correct values for attribute “erGroup”

Managing the Dial-in, Callback Settings, and Callback Number

Attributes Dial-in, Callback Settings, and Callback Number will not be set. These attributes are reconciled properly Issue only if Windows Active Directory Adapter is running as a service and is remotely managing Active Directory. The issue is reproducible on Windows 2003 x64 and Windows 2008 x64 as remote managed platform. The Windows API fails to retrieve the Dial-in attributes.

A workaround for this issue is same as that given for the DevTrack issue (S17341) (APAR# IY84890). That is to set the Dial-in Attributes, specify the user credentials having administrator authority (under which the Agent service runs) in ‘Tivoli Active Directory Adapter’ Windows service's Properties window.

1) Open Windows Services Tool. (i.e. the application, services.msc).
2) Go to 'Tivoli Active Directory Adapter' service. Open its Properties window.
3) Go to 'Log On' tab, change the default Log On option from 'Local System account' to 'This account'. And specify the Administration user credentials information.
4) Restart the 'Tivoli Active Directory Adapter' service.

Single Transaction for Modifying Mail-user to Mailbox User

This version of Windows Active Directory Adapter provides an enhancement to modify a mail account from its existing mail status (e.g. Mailuser) to other mail status (i.e. Mailbox user) in one single ITIM Modify operation. In the earlier versions of WinAD adapter, to modify the mail status, one has to delete the existing mail status in one operation and create the new mail status in another operation.

- To modify a Mailuser account to a Mailbox account -- Clear the target address and specify mailbox store. You may modify the Alias if required. The mailuser status is removed and a mailbox is created for the account.
- To modify a Mailbox account to a Mailuser account -- Clear the mailbox store and specify target address. You may modify the Alias if required. The mailbox is deleted from the exchange and the account is mail-enabled.

NOTE : If Alias is not modified during the above operations, then the Alias value is retained in the new mail status. To delete an existing mail status (mailuser or mailbox) of an account, delete the corresponding attribute, i.e. Mailbox store or Target address. (this behavior is same as previous versions of Adapter). Also once the mail status change operation completes, submit a user lookup operation to clear unnecessary attribute values from the account form so as to avoid warnings for those non-applicable attributes of the new mail status.

All other exchange related operations will work same like in earlier versions of Windows active directory adapter.

Support for Windows 2008

When you use Windows 2008 as a installation platform, and require to run adapter in SSL mode, then follow below steps. Otherwise, the certificate install will not be complete and will not enable SSL correctly.

1. Disable UAC security (User Account Control).
2. Install the required Certificate.
3. If required, enable UAC security.

For more information visit the link to enable/disable the UAC.

http://en.wikipedia.org/wiki/User_Account_Control

Registry option: ReconMailboxPermissions

The registry key, 'ReconMailboxPermissions' is set to to TRUE by default. So, by default mailbox security permissions attributes will get reconciled. However, you might experience a crash while reconciling mailbox permissions attributes. So, in that case to skip reconcile of mailbox permissions attributes, set the registry key 'ReconMailboxPermissions' to FALSE, which also improves reconciliation performance.

Attributes corresponding to the mailbox security permissions are:

- Delete Mailbox Storage
- Read Permissions
- Change Permissions
- Take Ownership
- Full Mailbox Access
- Associated External Acc
- Apply Onto (Allow / Deny)
- Permissions inheritance to one level (Allow / Deny)

Home directory security attributes

Note that for the following attributes, if the user neither has FULL nor CHANGE (Modify) access specified on the home directory, then reconciliation will display a blank option on the IBM Tivoli Identity Manager account form.

- Home Directory NTFS Access
- WTS Home Directory NTFS Access
- Home Directory Share Access
- WTS Home Directory Share Access

MailUserRenameDelay Registry Key

MR022409571– WinAD: Client trying to perform rename function for AD Account with Mailbox enabled and it fails when changing erADealias.

When an account with mail status is renamed on Active Directory, it takes time for Active Directory to reestablish the account's mail status. Here rename means modifying the Eruid and/or User Principal Name attribute. This behavior causes the adapter to fail the exchange attributes in the rename request with the error message “Error setting *attribute name* User does not have a mailbox”.

A new registry key "MailUserRenameDelay" is introduced to use this enhancement. The default value of this registry key is 0 seconds. When you use this key, the adapter waits before it modifies the exchange attribute when a user account is renamed. For example, when this key is set to 10 seconds and you submit a user account rename request, the adapter waits for 10 seconds before modifying the exchange attributes that are in the request.

Note: The adapter uses this key only when exchange attributes are specified along with Eruid and/or User Principal Name in request.

Handling of Multi-line Attribute Values

IZ47221- 64 BIT AD Adapter Not Handling Multi-line attribute values.

The adapter supports multi-line value for the ‘description’ attribute along with street attribute of user account class. Multi-line value is supported for extended attributes with string syntax

Support for Alert Processing on CN Attribute

IZ43288 - WIN-64 BIT WITH ALERT NON-COMPLIANCE POLICY ENFORCEMENT, WIN AD 64 BIT ADAPTER ENCOUNTERS ISSUES WITH CN.

When compliance alerts are enabled on IBM Tivoli Identity Manager, it is observed that the alerts keep alarming for user account class' 'cn' attribute. This is because of the fact that the attribute 'cn' in IBM Tivoli Identity Manager's schema is multi-valued where as the corresponding attribute on Active Directory 'cn' is single valued.
A new attribute is added in schema under erADAccount class with following details.
Attribute Name: erADFullName
OID: 1.3.6.1.4.1.6054.3.125.2.159
Description: Custom Common Name attribute
Data type: String
Custom Label: Full name

When the compliance alerts on Tivoli Identity Manager are enabled, avoid using the cn attribute on the account form. This issue may occur when alert non-compliance policy enforcement is set to automatic. No issue if compliance alerts on Tivoli Identity Manager is set as manual.
A new registry key "UseITIMCNAttribute" is introduced to the set of adapter registry keys. The default value of registry key UseITIMCNAttribute is TRUE. The adapter uses the registry key "UseITIMCNAttribute" to use either the cn or the erADFullName attribute.

When UseITIMCNAttribute = TRUE

- The adapter processes the IBM Tivoli Identity Manager's common schema attribute 'cn' for add, modify, and reconciliation operations.
- If the attribute 'erADFullName' is found in a request, this attribute will be failed by the adapter without considering the value.

When UseITIMCNAttribute = FALSE

- The adapter processes the erADFullName attribute for add, modify, and reconciliation operations.
- If the attribute 'cn' is found in a request, this attribute will be failed by the adapter without considering the value.

To use the erADFullName attribute on the account form, modify the profile using one of the following procedures

I. Modify the erADAccount.xml file of ADprofile.jar and importing the new profile on Tivoli Identity Manager

1. Copy the ADprofile.jar file to a temporary directory, example C:\Temp.
2. Extract the contents of ADprofile.jar file into the temporary directory by running the following command:
   cd C:\Temp
   jar -xvf ADprofile.jar
   The jar command creates the C:\Temp\ADprofile directory, which has all the profile files.
3. From the extracted ADprofile directory, open the erADAccount.xml file in a Text editor and make the following modifications and save the file:
   a. Replace the 'cn' attribute on account form with erADFullName attribute
   b. Change the attribute used to display on account form of the following attributes to erADFullName:
      erADManager
      erADEForwardTo
      erADEAllowedAddressList
      erADERstrctAdrsLs
      erADEDelegates

   For information about the required modification in erADAccount.xml file, see the table below. (Changes required are marked in blue)

Locate the following line(s) in erADAccount.xml file	Modification required to use erADFullName
<formElement direction="inherit" label="$cn" name="data.cn"> <input type="text" size="50" name="data.cn"/>	<formElement direction="inherit" label="$eradfullname" name="data.eradfullname"> <input type="text" size="50" name="data.eradfullname"/>
<formElement direction="inherit" label="$eradmanager" name="data.eradmanager"> <searchFilter type="input">\<filter>(&(objectclass=erADAccount)(eraddistinguishedname=*)(!(erisdeleted=Y)))</filter> <base>global</base> <attribute>cn</attribute>	<formElement direction="inherit" label="$eradmanager" name="data.eradmanager"> <searchFilter type="input">\<filter>(&(objectclass=erADAccount)(eraddistinguishedname=*)(!(erisdeleted&#61

<sourceAttribute>erADDistinguishedName</sourceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>	;Y)))</filter> <base>global</base> <attribute>erADFullName</attribute> <sourceAttribute>erADDistinguishedName</sourceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>
<formElement direction="inherit" label="$eradeforwardto" name="data.eradeforwardto"> <searchFilter type="input">\<filter>(&(objectclass=erADAccount)(erADEAlias=*)(erADDistinguishedName=*)(!(erisdeleted=Y)))</filter> <base>global</base> <attribute>cn</attribute> <sourceAttribute>erADDistinguishedName</sourceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>	<formElement direction="inherit" label="$eradeforwardto" name="data.eradeforwardto"> <searchFilter type="input">\<filter>(&(objectclass=erADAccount)(erADEAlias=*)(erADDistinguishedName=*)(!(erisdeleted=Y)))</filter> <base>global</base> <attribute>erADFullName</attribute> <sourceAttribute>erADDistinguishedName</sourceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>
<formElement direction="inherit" label="$eradeallowedaddresslist" name="data.eradeallowedaddresslist"> <searchFilter multiple="true" type="select">\<filter>(&(objectclass=erADAccount)(erADEAlias=*)(erADDistinguishedName=*)(!(erisdeleted=Y)))</filter> <base>global</base> <attribute>cn</attribute> <sourceAttribute>erADDistinguishedName</sourceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>	<formElement direction="inherit" label="$eradeallowedaddresslist" name="data.eradeallowedaddresslist">\<searchFilter multiple="true" type="select">\<filter>(&(objectclass=erADAccount)(erADEalias=*)(erADDistinguishedName=*)(!(erisdeleted=Y)))</filter> <base>global</base> <attribute>erADFullName</attribute> <sourceAttribute>erADDistinguishedName</sourceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>
<formElement direction="inherit" label="$eraderstrctadrsls" name="data.eraderstrctadrsls">\<searchFilter multiple="true" type="select">\<filter>(&(objectclass=erADAccount)(erADEalias=*)(erADDistinguishedName=*)(!(erisdeleted=Y)))</filter> <base>global</base> <attribute>cn</attribute> <sourceAttribute>erADDistinguishedName</sourceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI>	<formElement direction="inherit" label="$eraderstrctadrsls" name="data.eraderstrctadrsls">\<searchFilter multiple="true" type="select">\<filter>(&(objectclass=erADAccount)(erADEalias=*)(erADDistinguishedName=*)(!(erisdeleted=Y)))</filter> <base>global</base> <attribute>erADFullName</attribute> <sourceAttribute>erADDistinguishedName</sourceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass>

<paginateResults>false</paginateResults> </searchFilter> </formElement>	<showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>
<formElement direction="inherit" label="$eradedelegates" name="data.eradedelegates"> <searchFilter multiple="true" type="select">> <filter>(&(objectclass=erADAccount)(erAD Ealias=*)(erADDistinguishedName=*)(!(eris deleted=Y)))</filter> <base>global</base> <attribute>cn</attribute> <sourceAttribute>erADDistinguishedName</sourceAt tribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>	<formElement direction="inherit" label="$eradedelegates" name="data.eradedelegates"> <searchFilter multiple="true" type="select">> <filter>(&(objectclass=erADAccount)(e rADEalias=*)(erADDistinguishedName&#61 ;*)(!(erisdeleted=Y)))</filter> <base>global</base> <attribute>erADFullName</attribute> <sourceAttribute>erADDistinguishedName</sou rceAttribute> <delimiter></delimiter> <size></size> <width>300</width> <objectClass>erADAccount</objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>

4. Run the following command to create new jar file:
   cd C:\Temp
   jar -cvf ADprofile.jar ADprofile
   Note: The directory name and profile name is case sensitive, use the same case as above.
5. Import the new ADprofile.jar file on Tivoli Identity Manager.

II. Use "Form Customization" on Tivoli Identity Manager

1. Modify the account form of Windows Active Directory profile using Form Customization:
2. Remove the ‘cn’ attribute from the “User” tab
3. Add the ‘erADFullName’ attribute to the “User” tab
4. Change the attribute used to display on account form of the following attributes to erADFullName
   erADManager
   erADEForwardTo
   erADEAllowedAddressList
   erADERstrctAdrsLs
   erADEDelegates

Refer to the information center or the online help for information about using Form Customization.

Unlocking WinAD Accounts without a Password Reset

MR0218091930 - unlock WinAD account without password reset.

The adapter functionality is enhanced to check the user account’s lock status on Active Directory and accordingly succeed or fail account lock or unlock request. This helps in getting the account’s status without use of reconciliation or event notification.
The adapter behaves as follows:

1. When a user lock request is submitted from IBM Tivoli Identity Manager and if the account is already locked on Active Directory, then the adapter will succeed the account lock request.

2. When a user lock request is submitted from IBM Tivoli Identity Manager and if the account is un-locked on Active Directory, then the adapter will fail the account lock request.
3. When a user unlock request is submitted from IBM Tivoli Identity Manager, then the adapter will succeed the account unlock request. This holds true regardless of whether the account is locked or unlocked on Active Directory.

Note: You can not lock account on Active Directory externally. Active Directory locks account after set number of failed logon attempts.

DAML Read Timeout Registry Key Option

MR0501091918 - ADK changes to DAML for adding timeout on read

From this version a new DAML protocol property "READ_TIMEOUT" is introduced to the list of DAML Protocol Properties on agentCfg utility. This applies to setups that have a firewall between IBM Tivoli Identity Manager and the adapter. This firewall has a time out value that is less than the maximum connection age DAML property on Tivoli Identity Manager. When your transactions run longer than the firewall's time out, the firewall terminates the connection. The sudden termination of connections might leave the adapter with incorrect connection threads causing the adapter to crash.
When the adapter crashes randomly because of the specified setup, change the value for the READ_TIMEOUT. **The value must be in seconds and not less than the firewall's time out value**. The default value is 0 seconds.

Follow the steps listed below to set non-zero seconds values to the "READ_TIMEOUT" DAML property

a) From the Start Menu, select Programs > Accessories > Command Prompt.

b) At the command prompt, change to the \bin directory for the adapter.
For example, type the following command, if the Active Directory Adapter is in the default location:
cd C:\Tivoli\Agents\ADAgent\bin

c) Type the following command and Enter configuration key for Agent:
agentCfg -agent ADAgent

d) From the Main Menu, select option B "Protocol Configuration".

e) At the Agent Protocol Configuration Menu, type C. The Configure Protocol Menu is displayed.

f) At the Configure Protocol Menu, type A. to select DAML protocol. The DAML Protocol Properties menu is displayed.

g) Type the letter 'K' from the menu option for "READ_TIMEOUT"

h) The following prompt is displayed:
Modify Property 'READ_TIMEOUT':
Type the time out value for Tivoli Identity Manager and the adapter connection in seconds.

Note: After you set a value for READ_TIMEOUT please restart the adapter service.

Support for "#" in Group Names

IZ52976 - WINAD GROUP MEMBERSHIP MODIFICATION FAILS IF GROUP CONTAINS # AND ADAPTER IS SET TO USE CN FOR GROUP

The adapter's reconciliation and event notification functionality is modified to return un-escaped value for erGroup attribute when the registry key UseGroup is set to CN

SearchTimeout Registry Key Option to Avoid AD Hang

PMR 34450,057,649 - RBC Recon Hang issue AD Adapter. New registry key "SearchTimeout" is added in adapter.

From this version of Windows Active Directory Adapter a new registry key "SearchTimeout" is added.
In some of the Active Directory setups, the adapter might not complete the reconciliation operation. This occurs when the Microsoft ADSI API GetNextRow halts indefinitely.
The adapter monitors the reconciliation operation. When you set this registry key to a non-zero value, the adapter process is terminated if there is no activity by the adapter in the reconciliation operation for the time in seconds specified in this key.
When you set the value of this registry key to 0 and if the adapter halts during the reconciliation operation, the reconciliation operation does not complete and the operation is timed out on Tivoli Identity Manager. In this case, restart the adapter service. The default value of the registry key is 0 seconds.

To set "SearchTimeout" registry key use agentcfg utility provided by Windows Active Directory (64bit) Adapter.

Restricted Characters for erUID

Restricted the use of special characters in eruid attribute field on IBM Tivoli Identity Manager User account form.

From this version of the profile a new account form constraint "INVALID_CHARS" is added to the eruid attribute. This constraint will restrict the eruid attribute from having characters like / \ [ ] : ; | = , + * ? < > @ ". The restriction of these characters for eruid attribute comes from the restricted characters for samAccountName attribute on Active Directory, as the eruid attribute maps to samAccountName attribute. If you specify any of these characters for eruid attribute and submit the form, the following error message is displayed.
CTGIMU660E: A field contains characters that are not valid: invalid characters.

Support for Silent Installation

Installing and uninstalling the Active Directory Adapter with 64-bit Support by using the silent mode

You can install and uninstall the Active Directory Adapter with 64-bit Support by using the silent mode. Silent installation suppresses the Wizard and the Launcher User Interfaces (UIs) that do not display any information or require interaction. You can use the -i silent option to install or uninstall the adapter in silent mode.
Note: The adapter installs run time files from Microsoft. The installers for these run times show some user interfaces and you cannot suppress these user interfaces.
If you install adapter in silent mode, the uninstaller runs in silent mode irrespective of whether you are using -i silent option or not.

a) Installing the adapter by using the silent mode

I. Installing the adapter with default options

Run the following command from command line to install the Active Directory Adapter with 64-bit Support by using the -i silent option:
SetupAD64.exe -i silent -DLICENSE_ACCEPTED=TRUE

When you install the adapter by using the specified command, the adapter is installed with these default values.

Default values

Installation directory	%SYSTEM_DRIVE_ROOT%:\tivoli\agents\ADAgent
Adapter name	ADAgent
Installation option	Full installation

II. Installing the adapter with command line options

You can specify the listed installation options from the command line when you install the adapter by using the silent mode. For example, if you want to override the default installation directory path then, run the following command:
SetupAD64.exe -i silent -DLICENSE_ACCEPTED=TRUE -DUSER_INSTALL_DIR="c:\tivoli\MyFolder"

Note:
The -D option is followed by a variable and a value pair without any space after the -D option.
You must wrap arguments with quotation marks when the arguments contain spaces.

Installation options

Option	Value
-DLICENSE_ACCEPTED=Value	Accept the IBM license for the adapter, the value must be TRUE. When you do not specify this option, the default value is FALSE.
-DUSER_INSTALL_DIR=Value	Value overrides the default installation path. Example, “D:\tivoli\My Folder”

III. Installing the adapter by using the response file

Generating the response file

You can use response file to provide inputs during silent installation. Response file can be generated by running the following command. This runs the installer in interactive mode and
install the adapter.
SetupAD64.exe -r "Full path of response file"

For example:
SetupAD64.exe -r "c:\temp\WinAD64Response.txt"

Note: If you are running this command to only generate the response file, you must uninstall the adapter by using the uninstaller.

Creating the response file manually
You can also manually create the response file with the following content:
#Start of Response file

```
#Choose Install Folder
#---------------------
USER_INSTALL_DIR=c:\\tivoli\\agents\\ADAgent
#Has the license been accepted
#----------------------------
LICENSE_ACCEPTED=TRUE
#End of Response file
```

After you create the response file you can use it as:
SetupAD64.exe -i silent -f "Full path of response file"

b) Uninstalling the adapter by using the silent mode

Run the following command from command line to uninstall the Active Directory Adapter with 64-bit Support by using the -i silent option. Specify the full path when you are not running the command from Uninstall IBM Windows AD Adapter for ITIM (64 Bit) directory in the installation directory of the adapter.
"Uninstall IBM Windows AD Adapter for ITIM (64 Bit).exe" -i silent

For example, "C:\tivoli\agents\ADAgent\Uninstall_IBM Windows AD Adapter for ITIM (64 Bit)\Uninstall IBM Windows AD Adapter for ITIM (64 Bit).exe" –i silent.

Note: Restart the workstation after you install or uninstall the adapter.

MR0828093140 - Provide support for groupDN with ITIM V4.6

To use the Group CN, Group DN, or Group GUID as the source attribute for Groups attribute on account form, perform the following steps:

- Set the UseGroup registry key to one of the following options by using the agentCfg:

  – CN
  – DN
  – GUID

- Modify the profile using one of the following procedures:
  I. Modify the erADAccount.xml file of ADprofile.jar to modify the source attribute of erGroup attribute and import the new profile on Tivoli Identity Manager.
     a. Copy the ADprofile.jar file to a temporary directory, example C:\Temp.

     b. Extract the contents of ADprofile.jar file into the temporary directory by running the following command:

        cd C:\Temp
        jar -xvf ADprofile.jar
        The jar command creates the C:\Temp\ADprofile directory, which has all the profile files.

     c. From the extracted ADprofile directory, open the erADAccount.xml file in a Text editor. Modify the erADAccount.xml file according to the required source attribute for erGroup attribute and save the file. For information

about the required modification in erADAccount.xml file, see the table below.

d. Run the following command to create new jar file:

cd C:\Temp
jar -cvf ADprofile.jar ADprofile
Note: The directory name and profile name is case sensitive, use the same case as above.

e. Import the new ADprofile.jar file on Tivoli Identity Manager.

II. Use “Form Customization” on Tivoli Identity Manager to modify the source attribute of erGroup attribute.

Using Form Customization change the value of source attribute, to erADGroupGUID or erADGroupCN or erADGroupDN, for erGroup attribute on account form of Windows Active Directory profile.
Refer to the information center or the online help for information about using Form Customization.

- After modification to account form perform a full reconciliation operation.

Table: Profile modification to configure source attribute of erGroup attribute.

Value of the UseGroup registry key	**Modifications required in**	**Expected modification**
CN (default)	erADAccount.xml	<formElement name="data.ergroup" label="$ergroup"> <searchFilter multiple="true" type="select"> <filter>(objectclass=eradgroup)</filter> <base>contextual</base> <attribute>eradgroupcn</attribute> **<sourceAttribute>eradgroupcn</sourceAttribute>** <size></size> <objectClass></objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>
DN	erADAccount.xml	<formElement name="data.ergroup" label="$ergroup"> <searchFilter multiple="true" type="select"> <filter>(objectclass=eradgroup)</filter> <base>contextual</base> <attribute>eradgroupcn</attribute> **<sourceAttribute>eradgroupdn</sourceAttribute>** <size></size> <objectClass></objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>
GUID	erADAccount.xml	<formElement name="data.ergroup" label="$ergroup"> <searchFilter multiple="true" type="select"> <filter>(objectclass=eradgroup)</filter> <base>contextual</base>

		<attribute>eradgroupcn</attribute> **<sourceAttribute>eradgroupguid</sourceAttribute>** <size></size> <objectClass></objectClass> <showQueryUI>false</showQueryUI> <paginateResults>false</paginateResults> </searchFilter> </formElement>

Note: The value of the attribute name specified for <sourceAttribute> is stored as one of the values of erGroup attribute for that account in IBM Tivoli Identity Manager. The value of the attribute name specified for <attributeName> tell the name of the attribute, form group class, that is used for viewing on account form.
In all above cases the attribute used for displaying the Group attribute values on account form is erADGroupCN. You can use a different attribute, from the group object class, for viewing the Group attribute on account form.

For example,
If you want to view the Group attribute in dn format and to send group dn to the adapter, the following changes will be required to erADAccount.xml file
<formElement name="data.ergroup" label="$ergroup">
<searchFilter multiple="true" type="select">
<filter>(objectclass=eradgroup)</filter>
<base>contextual</base>
<attribute>eradgroupdn</attribute>
<sourceAttribute>eradgroupdn</sourceAttribute>
<size></size>
<objectClass></objectClass>
<showQueryUI>false</showQueryUI>
<paginateResults>false</paginateResults>
</searchFilter>
</formElement>

MR1010083842 - Enhancement to support Managed Folder Mailbox Policy in WinAD 64bit Adapter.
MR0421092235 - WinAD: Client needs support for msExchMailboxTemplateLink MS Exchange attribute.

The adapter is enhanced to support msExchMailboxTemplateLink Exchange attribute. The adapter will now, along with user, group, container, and mailbox store entries, also reconcile Folder Mailbox Policies created on Exchange 2007 Servers.
A new support data object class erADMBFldPolicy is added to Windows Active Directory profile schema. The erADAccount class now has a new attribute erADEMailboxFolderPolicy, on the 'Mail Settings' tab of account form with label "Managed Folder Mailbox Policy " and a search widget. This attribute maps to msExchMailboxTemplateLink attribute on Active Directory. The erADEMailboxFolderPolicy attribute holds the DN of the Folder Mailbox Policy assigned to the mailbox. When an account is viewed on account form, the name of the Folder Mailbox Policy set for the mailbox is displayed. For an ADD/MODIFY user request, the DN of the selected Folder Mailbox Policy is provided to the adapter.

To reconcile Folder Mailbox Policies the adapter binds to the RootDSE of the domain in which it is installed. The object class erADMBFldPolicy is supported for Adapter Based Filtering but not for Adapter Based Event Notification.
A Full Reconciliation or Support Data Reconciliation must be performed to get the Folder Mailbox Policies from Active Directory.

MR052609514 - customer wants to use the extend attribute transformed the name on itim side using the AD 5.0.5 adapter on ITIM 4.6 Server.

The adapter now supports mapping of attribute names for extended attributes. With this enhancement a different attribute name can be used on IBM Tivoli Identity Manager than the attribute name on Active Directory.
As before the exschema.txt file will be used to specify the extended attributes. If required to use a different attribute name on IBM Tivoli Identity Manager than the attribute name on Active Directory, specify the attribute name in exschema.txt file in the following format:
Attribute name on IBM Tivoli Identity Manager followed by a pipe '|' and then followed by the attribute name on Active Directory.
For example,
erADUserInfo|info

As before there should be only one attribute on each line.
If you wish to use the same attribute name on IBM Tivoli Identity Manager as on Active Directory, then use the existing format i.e. just give the Active Directory side attribute name.
For example,
Info
Or
Info|Info

Both the above forms are valid, use either one.

Note:
- When you use a different attribute name for IBM Tivoli Identity Manager ensure that the attribute name rules, as defined by the Directory Server used, are followed.
- The attribute name must not have a '|' in the attribute name.

MR0928094723 - Delay in Exchange cmdlets for mailbox permission

The adapter is enhanced to alter a delay between setting of Exchange 2007 Mailbox Permission attributes. It is observed in some Exchange 2007 setups, that the adapter might not set the mailbox permission attributes properly. If four of the mailbox permission attributes are modified, the request will complete with SUCCESS but only the last permission attribute in the request will take effect. The adapter will also log any failure message returned from exchange setup.

A new registry key "SetMailboxPermissionDelay" is introduced to the set of adapter registry keys. The default value of this key is 0 (zero) seconds. With the default value no delay is introduced when setting mailbox permission attributes.

If in you experience a similar issue, where of the mailbox permission attributes modified only the last permission attribute is set and the request completes with SUCCESS, make use of the registry key SetMailboxPermissionDelay. Set this registry key to a non-zero integer value using agentCfg utility. The adapter uses the value set for this registry key and waits for the number of seconds as specified for the key. Ideally a value of 20 seconds for SetMailboxPermissionDelay resolves the issue.

The adapter works as follows when it comes to setting mailbox permission attributes:
1. Check if the Permission attribute requested is already set (say as Allow or Deny)
    a. If yes, remove the permission set using Remove-MailboxPermission cmdlet.
    b. Wait for the number of seconds specified for SetMailboxPermissionDelay.
2. Add the permission, if required, using Add-MailboxPermission.

3. Wait for the number of seconds specified for SetMailboxPermissionDelay before going to next permission attribute in the request.

Please see the following cases for more detail:
Assuming that the registry key SetMailboxPermissionDelay is set to 20 seconds.

CASE 1:
Assume all the exchange mailbox permission attributes are set to “NONE” for a mailbox. You wish to modify all the permission attributes to “Allow” or “Deny”. As per the procedure described above, the total delay incurred by the adapter can be calculated as:

Total delay = (Value of registry key SetMailboxPermissionDelay) * (Total number of permission attributes in the request) * (Number of cmdlets executed by the adapter for a permission attribute)

In this case, since there is no permission set previously so only Add-MailboxPermission will be executed for each permission attribute in the request.
That is,
Total delay = 20 * 6 * 1 = 120 seconds.

The above is also applicable when a new mailbox is created with all the permission attributes set to “ALLOW” or “DENY”.

CASE 2: **(Worst case)**
Assume all the exchange mailbox permission attributes are set to “ALLOW” for a mailbox. You wish to modify all the permission attributes to “DENY”. As per the procedure described above, the total delay incurred by the adapter can be calculated as:

Total delay = (Value of registry key SetMailboxPermissionDelay) * (Total number of permission attributes in the request) * (Number of cmdlets executed by the adapter for a permission attribute)

In this case, the permissions are set previously so both Remove-MailboxPermission and Add-MailboxPermission will be executed for each permission attribute in the request.
That is,
Total delay = 20 * 6 * 2 = 240 seconds.

The above is also applicable when all the exchange mailbox permission attributes are set to both “ALLOW” & “DENY” and you want to set all the exchange mailbox permission attributes to “NONE”. Here adapter will execute two Remove-MailboxPermission powershell cmdlet to remove that particular attribute from”DENY” then from “ALLOW”. So for each attribute two powershell cmdlets are executed.

IZ61122- PATH TO EXCHANGE TOOLS IN AD ADAPTER SHOULD BE CONFIGURABLE

The adapter setup includes a C# COM library, Exchg2k7.dll, to perform exchange 2007 specific operations. The library Exchg2k7.dll depends on few Microsoft Exchange 2007 libraries. To locate these dependant libraries it uses a default hard coded path

“C:\Program Files\Microsoft\Exchange Server\bin\”

When the exchange server/tools are not installed on this default path, some of the exchange 2007 feature provided by the adapter fails.

To overcome this, the adapter is modified to find the exchange server/tool’s installation path using windows registry
“\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\v8.0\Setup\MsiInstallPath”

The path pointed out by the above registry key is used to locate the dependant Microsoft Exchange 2007 libraries. If adapter fails to find the registry key it will use the default installation path as “"%ProgramFiles%\Microsoft\Exchange Server\bin\”

Here "ProgramFiles" is folder path to Windows Program Files.

Failover of Target Systems – Multiple Servers in Basepoint

MR0212084734 – Enhancement to handle failover of target systems by supporting multiple target servers in basepoint.

This version of Windows Active Directory Adapter supports more than one target servers in the base point.

The earlier versions of WinAD adapter supported only one target server for the basepoint. If the specified target server is down and useDefaultDC is set to FALSE, adapter used to fail the request.

With this enhancement more than one target servers can be specified for basepoint on Tivoli Identity Manger's Active Directory Service Form and/or in the Windows Active Directory Adapter's registry. Each target server must be separated by a pipe '|'.

Usage Example,

Base Point DN on service form with more than one target server:
DC01|DC02|DC03/OU=TestOU,DC=MyDomain,DC=com

Base Point DN on service form with only one target server:
DC01/OU=TestOU,DC=MyDomain,DC=com

Base Point DN on service form with no target server:
OU=TestOU,DC=MyDomain,DC=com

Also, target servers can be specified in Adapter's registry as well:

a) If BasePoint specified on service form is “OU=TestOU,DC=MyDomain,DC=com”, you can specify the list of target server(s) in adapter registry using agentCfg.exe as follows:

1. Create WinAD adapter registry with name OU=TestOU,DC=MyDomain,DC=com
2. Specify the value for the above key as DC01|DC02|DC03

Registry key	Value
OU=TestOU,DC=MyDomain,DC=com	DC01|DC02|DC03

b) If BasePoint specified on service form is “DC01|DC02|DC03/OU=TestOU,DC=MyDomain,DC=com”, you can specify the list of target server(s) in adapter registry using agentCfg.exe as follows:

3. Create WinAD adapter registry with name OU=TestOU,DC=MyDomain,DC=com
4. Specify the value for the above key as DC01|DC02|DC03

Registry key	Value
OU=TestOU,DC=MyDomain,DC=com	DC01|DC02|DC03

Adapter iterates through all the target servers specified in base point on service form, and then through the target servers specified in registry key. The first available target server is used by the adapter.
You can also wish to specify the base point without the target server(s) on service form, and use the registry key to specify the target servers. Adapter uses the base point specified on the service form to find a key with this base point value in the registry, to get the target servers specified as the value for this registry key.

Note:

1. The maximum number of characters that the Base Point DN attribute on service form can hold is 240 characters.
2. Service form and registry can specify their own set of target servers, the target servers specified on service form is given high priority.
   Example,
   Base Point on service form
   DC01|DC02|DC03/OU=TestOU,DC=MyDomain,DC=com
   Registry
   Registry key Value
   OU=TestOU,DC=MyDomain,DC=com DC04|DC05|DC06
3. If no base point is specified on service form, the registry will not be referred.
4. It is recommended that you specify target server using adapter's registry as it is cached to improve performance as against specifying on service form. The target server list on service form is not cached and is parsed in each request to find all target servers.
5. Use agentCfg.exe to create and modify adapter registry keys, please restart the adapter service after adding or modifying registry keys. If the basepoint or target server contains Unicode characters then use regedit to create registry keys under HKEY_LOCAL_MACHINE\ SOFTWARE\Access360\ADAgent\Specific

ADprofile checkboxes are replaced with Dropdown list

IZ45782- CHECK BOX IN FORM FOR EXCHANGE ATTRIBUTES CAUSES ERROR IN AGENT LOG (x64).

Windows Active Directory Adapter ADprofile is modified. In this fix all the checkboxes are replaced with Dropdown list with 3 optional values "<Blank>\TRUE\FALSE". When we created an account with checkbox attributes with older ADprofiles we get two options true\false.
You may get 4 optional values while selecting the values for Boolean attributes (With checkbox) after upgrading new ADprofile.
It is required to perform a FULL Reconciliation after upgrading the ADprofile with checkbox changes APAR: IZ45782. A defect, APAR IZ73136, was opened with IBM Tivoli Identity Manger Server version 5.0 to address this issue. This defect is fixed in ITIM 5.0 IF39.

Enable/Disable "UseThreadPooling"

IZ67106 - INTERMITTENT 0X80004002 ERRORS WHEN ATTEMPTING TO MANAGE/PROVISION MAILBOXES

There is an issue In the Microsoft CDOEXM library used by Windows Active Directory Adapter to perform Exchange tasks. A ticket was also opened with Microsoft, Case ID "SRZ080104000181", for the same.
Agent is redesigned as described in Microsoft Case ID. Adapter now implements thread pool. A predefined number of threads (12) are created at the start of adapter and are used to perform all operations. These threads will be destroyed only at the end i.e. when adapter itself is stopped.
A new registry key "UseThreadPooling" is introduced. By default this key is set to "FALSE" so that existing customers are not affected.
When UseThreadPooling is set to TRUE Thread Pooling is enabled, with all the threads initialized at the start of Agent Service and uninitialized when the Agent service stops.
When UseThreadPooling is set to FALSE Thread Pooling is disabled. In this scenario threads will be created and destroyed on per request.

Thread Pooling can be used in the following scenarios:
1. If you are experiencing high memory usage then set this key to "TRUE".
2. If you are experiencing the following error message during the Exchange related operations. errorMessage="Unable to contact Exchange services. ADSI Result code: 0x80004002"

Support for Silent Installation

The following note is no longer applicable. Changes has been made to the Windows Active Directory Adapter to suppress the user interface showed during installation of run time files from Microsoft for silent installation.

Note: The adapter installs run time files from Microsoft. The installers for these run times show some user interfaces and you cannot suppress these user interfaces.

Updating the Windows Active Directory Adapter

a) Updating Windows Active Directory Adapter in GUI mode

Use the adapter update option:

- If you want to keep the adapter configuration (registry keys and certificates) unchanged.

If update installation option is selected, the installer detects the path of the existing installed adapter. If no prior installation of the adapter is found on the system, the installer will display an error message. The installer replaces the binaries and the DLLs of the adapter and the ADK. The installer does not prompt for any configuration information during an update installation.

Note: Adapter related registry keys are not modified. The update installation does not create a new service for the adapter.

During an update, in order to maintain all of your current configuration settings, as well as the certificate and private key, do not uninstall the old version of the adapter before installing the new version. For more information on how to install the adapter, see "Installing the adapter" in Installation Guide

In order to update an existing adapter, complete the following steps:

1. If you downloaded the installation software from Passport Advantage, perform the following steps:
   a. Create a temporary directory on the computer on which you want to install the software.
   b. Extract the contents of the compressed file into the temporary directory.
2. Start the installation program with the SetupAD64.exe file in the temporary directory.
3. Select the language and click OK to display the Introduction window.
4. On the Introduction window, click Next to view the Software License Agreement.
5. Do the following at the Software License Agreement window:
   - Review the license agreement and select Accept .
   - Click Next.
6. Select Update installation option and click Next
   Note: The adapter must already exist if you want to perform an update installation. If it does not exist, the software generates the following message:
   Update not supported when the adapter is not previously installed.
   Cannot perform Update Installation. IBM Tivoli Windows Active Directory Adapter (64 Bit) is not installed on this machine. Please select Full Installation.
7. The adapter will display the path of the adapter installation which will be updated. Click OK to view the pre-Installation Summary.
8. Review the installation settings on the pre-Installation Summary window and click on Install
9. Click Done on the Install Complete window.

b) Updating Windows Active Directory Adapter by using silent mode

You can use the -i silent option to update the adapter in silent mode.

Note:
- If you install adapter in silent mode, the uninstaller runs in silent mode irrespective of whether you are using -i silent option or not.

Installing the adapter with command line parameters

You can use any of the following commands to perform update installation of the adapter in silent mode.

1. SetupAD64.exe -i silent -DLICENSE_ACCEPTED=TRUE -DUSER_INPUT_INSTALL_TYPE_1= -DUSER_INPUT_INSTALL_TYPE_2=\"Update Installation\" -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1=0 -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2=1

2. SetupAD64.exe -i silent -DLICENSE_ACCEPTED=TRUE -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1=0 -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2=1

Note:-

1. The installer itself detects if the adapter is already installed on the system on which this command is executed. For this the installer refers to the adapter registry keys.
   The installer proceeds with updating the adapter only if it successfully detects a prior installation of the adapter on the system.
   If no prior installation is found on the system, the installation is aborted and a log file

   IBM_Tivoli_Windows_Active_Directory_Adapter_(64_Bit)_InstallLog
   is generated with this information in the Desktop.
   .
2. When performing Update Installation the -DUSER_INSTALL_DIR must never be used.

Updating the adapter in silent mode by using the response file

Generating the response file

You can use response file to provide inputs during silent installation. Response file can be generated by running the following command.

SetupAD64.exe -r "Full path of response file"

For example:
SetupAD64.exe -r "C:\Temp\WinAD64AdapterResponse.txt"

This runs the installer in interactive mode and installs the adapter.
After the installation completes the file specified as "Full path of response file" will be created containing the required parameters.

Note:
If you are running this command to only generate the response file, you must uninstall the adapter by using the uninstaller.

Creating the response file manually

You can also manually create the response file and add the required parameters to the file.

Create a text file, for example WinAD64InstallParameters.txt, with the following content:

```
#Has the license been accepted
#-----------------------------
LICENSE_ACCEPTED=TRUE

#Select Install Type
#-------------------
USER_INPUT_INSTALL_TYPE=\"\",\"Update Installation\"
USER_INPUT_INSTALL_TYPE_1=
USER_INPUT_INSTALL_TYPE_2=Update Installation
USER_INPUT_INSTALL_TYPE_BOOLEAN_1=0
USER_INPUT_INSTALL_TYPE_BOOLEAN_2=1
```

After you create the response file you can use it to provide parameters to the installer for updating the adapter using silent installation as:

SetupAD64.exe -i silent -f "Full path of response file"
For example,
SetupAD64.exe -i silent -f "C:\WinAD64InstallParameters.txt"

Note: Restart the workstation after you install or uninstall the adapter.
****

MR110509300 - MR0908095421 - AD agent Exchange server 2010 support

With this release the adapter supports provisioning of mailbox enabled and mail enabled users on Exchange Server 2010.
The procedure to mailbox or mail enable a user account using IBM Tivoli Identity Manager remains same as with Exchange server 2007.

- To mailbox enable a user account an Exchange 2010 mailbox store must be selected for Mailbox Store attribute on account form. Optionally you can also specify value for Alias attribute to use the preferred alias.
- To mail enable a user account specify value for Target Address attribute on account form. Optionally you can also specify value for Alias attribute to use the preferred alias.

Note: - Adapter uses the value of User Principal Name (UPN) attribute for identity parameter for all cmdlets used for provisioning user accounts.

The alias attribute value can contain:

- Characters from A to Z (lowercase and uppercase)
- Digits from 0 to 9
- Special characters like ` ~ ! # $ % ^ & * - _ = + { } | ‘ , / ?
- One or more periods may be embedded in an alias, but each one of them should be preceded and followed by at least one of the other characters.

The alias attribute value cannot contain:

- Special characters like @ ( ) [ ] \ ; : “ < >
- Space

When value of alias attribute is not specified for mailbox or mail enabling user account, the value of Common Name (cn) attribute will be used for alias by the exchange server. The cn attribute can contain all the special characters, some of which are not allowed for alias attribute. In this case each of the not allowed character will be replaced with a question mark (?) in the alias value.
Proxy addresses will be generated based on the alias value.

Mixed setups where Exchange Server 2007 SP2 and Exchange Server 2010 exist in the same organization:

- Using Exchange Server 2010, new mailboxes cannot be created on an Exchange 2007 mailbox store.
- Mailboxes which are created on Exchange 2007 mailbox stores can be managed using Exchange Server 2010.
- A mailbox which is created on an Exchange 2007 mailbox store can be moved to Exchange 2010 mailbox store and vice versa.

Understanding Move Requests

The adapter only supports moving mailbox locally, i.e. moving mailbox in the same forest. Cross forest mailbox move (remote move) is not supported. As move mailbox is asynchronous in Exchange 2010, the adapter only submits a local mailbox move request using New-MoveRequest cmdlet. The adapter will not wait for the move to complete. The status of submitting the move request will be returned for mailbox store attribute.
Exchange Server 2010 retains the mailbox move requests, even when the move job is completed. When a move request already exists for a mailbox, you cannot move the mailbox again until the move request is removed.

For more detail on the mailbox move requests, please follow the Microsoft link:
http://technet.microsoft.com/en-us/library/dd298174.aspx

Currently adapter does not support any new Exchange Server 2010 feature, except for submitting a move request to move a mailbox while the end user is still accessing it.
The following features are not supported by the adapter:

- Archive Mailbox
- Management of the following Mailbox settings
  - Federated Sharing
  - Archive Quota
  - Mailbox Calendar Settings
- Getting the status of mailbox move requests.
- Removing move requests.

MR0210102732 - OCS support for AD adapter.

OCS support for users that are neither mail enabled nor have exchange mailboxes.

For OCS support Active Directory attribute erADEProxyAddresses needs to be updated. When the user account neither has a mailbox nor is mail enabled, then the adapter will fail modification to erADEProxyAddresses attribute.
To update proxyAddresses attribute on Active Directory make use of extended attributes using exschema.txt file. While setting extended attributes adapter does not check the mail status of the user account.
For example, add the following to exschema.txt file

erADExtendedProxyAddresses|proxyAddresses

This is an instruction to the adapter to manage Active Directory attribute “proxyAddresses” and to use “erADExtendedProxyAddresses” as the corresponding attribute on IBM Tivoli Identity Manager. Please refer to section “MR052609514 - customer wants to use the extend attribute transformed the name on itim side using the AD 5.0.5 adapter on ITIM 4.6 Server.” under “Configuration Notes” in Release Notes on how to specify extended attribute using exschema.txt file

Modify the Active Directory adapter profile, ADprofile.jar, to define a new attribute (erADExtendedProxyAddresses) and add it to erADAccount class in schema.dsml file. Please refer to “Chapter 7. Customizing the Active Directory adapter” in Configuration Notes for details on how to modify ADprofile.jar.

When a full reconciliation or user lookup is performed the values set for erADExtendedProxyAddresses attribute will also be returned for erADEProxyAddresses attribute. This is because both erADExtendedProxyAddresses and erADEProxyAddresses correspond to the same attribute, proxyAddresses, on Active Directory.

Note:

- Adapter will not check for validity of values and their formats specified for Proxy Addresses through extended attribute.

MR0302105547 - Use erADLastLogonTimeStamp for AD dormant account report

In previous versions, Active Directory profile used attribute erADLastLogon for erLastAccessDate. The attribute erADLastLogon corresponds to lastLogon on Active Directory. The attribute lastLogon of a user account on Active Directory is updated only when the user logs in and is updated only on the DC against which the authentication happens. This attribute is not replicated amongst the DCs in the domain. Tivoli Identity Manager’s dormant account report for Active Directory user accounts may not be accurate. This is because the adapter reads user accounts from a particular DC (specified as target server on service form or returned by DNS server as the nearest one) which can be different than the one using which the user’s authentication has happened.

With this version, Active Directory profile will use attribute erADLastLogonTimeStamp for erLastAccessDate. The corresponding attribute on Active Directory, lastLogonTimestamp, is replicated across DC's. Using erADLastLogonTimeStamp attribute for erLastAccessDate will result in accurate dormant account reports.

To use erADLastLogon for erLastAccessDate will now require changes in resource.def file in ADProfile.jar

Replace following lines of resource.def file

```
<AttributeMap>
    <AttributeName="erLastAccessDate" Value="erADLastLogonTimeStamp"
Profile="account"/>
</AttributeMap>
```

With

```
<AttributeMap>
     <Attribute Name="erLastAccessDate" Value="erADLastLogon" Profile="account"/>
</AttributeMap>
```

MR0226101912 - WinAD: Need a way to configure the length of the wait period for the retries of Win AD 64-bit Adapter for reconciliation.

A new registry key, ReconRetryWaitPeriod, is introduced to the set of adapter registry settings to support this enhancement. The default value for ReconRetryWaitPeriod is 300 (seconds)

In an organization, Active Directory always runs in cycles of low and heavy load depending on the number of authentication, replication, account management, and other Active Directory management requests. When Active Directory is observing heavy load and a reconciliation is performed, the adapter gets a special error message from Active Directory (Error_More_Data) indicating that it has not completed with reading all the user accounts and currently its observing a load. Upon this the adapter prints the incidence of this event to the log as “GetNextRow failed. Calling GetNextRow can potentially return more results. Provider: LDAP Provider”. The adapter then waits for an interval specified by ReconRetryWaitPeriod registry key (in seconds) and retires again.

The Adapter is designed to retry the query three times before terminating the reconciliation. The adapter waits for a calculated time between each retry attempts, which is calculated as
<RETRY_ATTEMPT_NUMBER> * <VALUE_OF_ ReconRetryWaitPeriod >
For example, when ReconRetryWaitPeriod is set to 40 seconds and the adapter receives Error_More_Data message from Active Directory. The wait period between each retry attempt is calculated as:
1 * 40 = 40 seconds – Before the first retry attempt;
2 * 40 = 80 seconds – Before the second retry attempt
3 * 40 = 120 seconds – Before the third (last) retry attempt.

Use agentCfg to set "ReconRetryWaitPeriod" to a value other than the default 300 seconds.

Note:
- The value for this registry should be numeric and in units of seconds.
- When SearchTimeout is also enabled, the value of ReconRetryWaitPeriod should be less than the value of SearchTimeout.
- The acceptable value for this key is from 0 to 214783647 seconds.

User Exchange attributes, erADESMTPEmail and erADEX400Email.

erADESMTPEmail
The erADEXMTPEmail attribute holds the primary SMTP proxy address set for an user account. When the value of this attribute is modified, the new value will be used as the primary SMTP address.

erADEX400Email
This attribute is not managed by the adapter. If exist in a request, it will be ignored. The adapter will reconcile value(s) of this attribute.

Setting Proxy Address:

Following table provides few scenarios to set proxy address. Please note that not all scenarios are covered in this table.

NOTE: If the request contains a Proxy Address value which is already present or generated on Active Directory then adapter will ignore this and will return success for that proxy address value.

Sr. No	Scenario	Settings		Result	Comment
1	To set primary proxy address different than **Target Address** for a Mail-enabled account.	i.	- **Auto Generate Email Address** is True. - Operation Type is ADD-DELETE. -Add the **Target Address** as secondary proxy address by prefixing it with smtp. -Add the new proxy address to be set as primary with prefix SMTP.	- On exchange 2010 the new proxy address will be set as primary proxy address and the **Target Address** will be set as secondary proxy address. - On Exchange 2007 the requested Primary SMTP address is not added as primary SMTP proxy address. The request will fail.	When **Auto Generate Email Address** is True, setting a primary proxy address different than Target Address is possible only on Exchange 2010. We cannot set new primary proxy address with REPLACE operation type
		ii.	- **Auto Generate Email Address** is False. -Operation Type can be ADD-DELETE or REPLACE. -Specify the new proxy address to be set as primary with prefix SMTP. -No need to set **Target Address** as secondary proxy address.	The new proxy address will be set as primary proxy address.	When **Auto Generate Email Address** is False we can set new primary proxy address using an ADD operation Type, but any modifications to this value can be done only with a REPLACE operation type.
2	To modify primary Proxy Address for a mailbox enabled account	i.	- Auto generate Email Address is set to TRUE. -Operation Type is ADD-DELETE or REPLACE. -Modify the primary proxy Address to new proxy address with prefix SMTP	-On Exchange 2007 the requested Primary SMTP is not added by Exchange Server. So the adapter will fail the request. -On Exchange 2010 the requested	-When Auto Generate Email address is True then adapter will not update Primary SMTP address. But if the request contains a primary SMTP address which is same as

				Primary SMTP address is added as **secondary** proxy address	generated on Active Directory then adapter will ignore this and will return success -For a mailbox-enabled Exchange generates a primary proxy address using the Alias value.
		ii.	-Auto generate Email Address is set to False. -Operation Type is ADD-DELETE. -Add a new proxy address with prefix SMTP.	When Auto Generate Email address is False then adapter will set the Primary SMTP proxy address to the one which is specified in the request.	The previous Primary SMTP proxy address becomes secondary proxy address by exchange Server.
		iii.	-Auto generate Email Address is set to False. -Operation Type is REPALCE. -Add a new proxy address with prefix SMTP. You can also specify other proxy address values.	When Auto Generate Email address is False then adapter will set the Primary SMTP proxy address to the one which is specified in the request along with the other values.	The adapter will clear the old values before setting new values.
3	To set Secondary SMTP Proxy address.	i.	- Auto generate Email Address is set to **True** or **False**. - Account type is Mailbox-enabled or Mail-enabled. -Operation Type is ADD-DELETE -Specify the Proxy Address value with prefix “smtp:“ Example: smtp:Thomas2@ibm.com	Adapter will add the requested proxy address as secondary.	If the requested value is already present on Active Directory then adapter will ignore the value and will return success.
		ii.	- Auto generate Email Address is set to **True**	Adapter will first set Primary SMTP address	The adapter will clear the old values before

			- Account type is Mailbox-enabled. -Operation Type is REPLACE -Specify the Proxy Address value with prefix “smtp:“ Example: smtp:Thomas2@ibm.com NOTE: You must specify Primary SMTP address with this request.	specified in the request and then will add the requested proxy address as secondary. If no Primary SMTP address is specified then adapter will fail the whole operation and will not update any value. (This is applicable only for Exchange 2010)	setting new values. -On Exchange 2007 the Primary SMTP address specified in the request is not added by Exchange Server. So the adapter will fail the request. Note: -For Mailbox enabled account on Exchange 2010 the requested Primary SMTP address is added as secondary proxy address.
		iii.	- Auto generate Email Address is set to **True** - Account type is Mail-enabled. -Operation Type is REPLACE -Specify the Proxy Address value with prefix “smtp:“ Example: smtp:Thomas2@ibm.com NOTE: You must specify Primary SMTP address with this request.	Adapter will first set Primary SMTP address specified in the request and then will add the requested proxy address as secondary. If no Primary SMTP address is specified then adapter will fail the whole operation and will not update any value. (This is applicable only for Exchange 2010)	The adapter will clear the old values before setting new values. -On Exchange 2007 the Primary SMTP address specified in the request is not added by Exchange Server. So the adapter will fail the request. Note: -For Mail enabled account on Exchange 2010 the requested Primary SMTP address is

					added as primary SMTP proxy address.
		iv.	- Auto generate Email Address is set to **False** - Account type is Mailbox-enabled or Mail-enabled. -Operation Type is REPLACE -Specify the Proxy Address value with prefix “smtp:“ Example: smtp:Thomas2@ibm.com NOTE: You must specify Primary SMTP address with this request.	Adapter will first set Primary SMTP address specified in the request and then will add the requested proxy address as secondary. If no Primary SMTP address is specified then adapter will fail the whole operation and will not update any value.	The adapter will clear the old values before setting new values.

IZ72897- PROBLEM TRYING TO SET AN ADDITIONAL E-MAILTYPE MRS

The adapter now checks the proxy addresses set on the mailbox for a user account when it receives an add/modify request with erADEProxyAddresses attribute for that user account. Adapter will ignore proxy address values in the request if the same already exist on Active Directory for that user account. Here ignoring means that the adapter will not attempt to add that value to the existing set of proxy addresses on Active Directory. When adapter adds proxy address value(s) which already exist, then that value is failed by PowerShell cmdlet. This is done to avoid failures for proxy address value(s) which already exist on Active Directory. This will help to update the user account’s erADEProxyAddresses attribute in IBM Tivoli Identity Manager’s LDAP without running a reconciliation or user lookup.

Note:

The adapter does a case sensitive comparison on the type of the email address (SMTP:, smtp:, X400, etc.) and case insensitive comparison on the actual email address value.

For example,
SMTP:User01@ibm.com and SMTP:User01@ibm.com or SMTP:USER01@IBM.COM are considered to be same by the adapter and will be ignored.
SMTP:User01@ibm.com and smtp:User01@ibm.com will not be considered to be same.

MR031010518 - WinAD: Need Disable Mailbox support for Exchange 2007

Disable Mailbox Support for Exchange Server 2007 and Later

The adapter is enhanced to support disconnecting (disabling) mailboxes when user accounts are suspended and connecting a user account to a disconnected (disabled) mailbox. This feature is supported for exchange server 2007 and 2010.

The following new registry keys are introduced to the set of adapter registry keys:

Registry Key Name	Default value
DisableMailboxOnSuspend	FALSE
ReconDisconnectedMailbox	FALSE

Disable/Disconnect User Mailbox:
Disabling a mailbox means disconnecting a mailbox enabled user account in Active Directory from its mailbox. When the mailbox is disabled, all the user account's exchange attributes are removed from Active Directory. The user account associated with the mailbox will remain in Active Directory but will no longer be associated with a mailbox.

Adapter uses the registry key "DisableMailboxOnSuspend" to decide if the mailbox has to be disabled or not during a suspend operation. When registry key "DisableMailboxOnSuspend" is FALSE, adapter will not disable the user's mailbox while suspending the user account on Active Directory. When registry key "DisableMailboxOnSuspend" is TRUE, adapter will disable the user's mailbox while suspending the user account on Active Directory.

A user's mailbox can also be disabled\disconnected by clearing the value of Mailbox Store attribute on account form. This is already supported by the adapter and does not depend on the value of registry key "DisableMailboxOnSuspend".

Reconnect/Connect User account to a Disabled Mailbox:
A disconnected mailbox is a mailbox object in the Microsoft Exchange store that is not associated with an Active Directory user account.

To connect a user account to a disabled mailbox, the adapter needs to have information about the disabled mailbox and the user account for which to connect. There can be n number of disabled mailbox on an exchange store to which user account can be connected. The user account to which user disabled mailbox is connecting must be logon-enabled.

Adapter uses the registry key "ReconDisconnectedMailbox" during reconciliation operation. When "ReconDisconnectedMailbox" is TRUE, the adapter will return information about all the disconnected\disabled mailboxes from configured exchange servers to IBM Tivoli Identity Manager in reconciliation. On enabling this feature the adapter performance on recon will be slower. If this key is set to FALSE, adapter will not reconcile disconnected\disabled mailboxes to IBM Tivoli Identity Manager.

A new support data object class erADDisabledMB is added to Windows Active Directory profile schema. The erADAccount class now has a new attribute erADEConnectToMailbox. To connect a user account to a disabled mailbox use this attribute to select one of the disabled mailbox from the list of disabled mailboxes returned by the adapter in a reconciliation operation. This attribute is used only to provide the information required by the adapter to connect the user account to the disabled mailbox. After connecting to disabled mailbox, next when reconciliation or user lookup is performed the value of this attribute gets cleared from the account form.

The object class erADDisabledMB is supported for Adapter Based Filtering but not for Adapter Based Event Notification.

A Full Reconciliation or Support Data Reconciliation must be performed to get information about all the Disabled\Disconnected Mailboxes from each Exchange Servers in the organization.

This feature is not supported for Exchange 2003 Servers. You cannot manage disabled mailboxes on Exchange Server 2007 using Exchange Server 2010 and vice versa.

When a user mailbox is disabled all its Exchange properties are removed from the user account on Active Directory and the mailbox is marked in the database for removal. When a mailbox enabled user account is removed (deleted) from Active Directory, the mailbox will be marked in exchange database for removal.

Deleted\Disabled (Disconnected) mailbox remains in exchange database for configured number of days (Default is 30 days). This configuration can be changed through Exchange Admin Console. When you create a mailbox for a new or existing user, the Exchange attributes that are required for a mailbox are added to the user object in Active Directory. When we connect a disabled mailbox to an existing Active Directory user account, that user account becomes the owner of the mailbox and has full access to any content within the mailbox.

Note:

- Adapter does not have a feature to delete a mailbox. When an account is deleted its mailbox is not deleted but the mailbox is flagged as disconnected by Exchange Server. When a mailbox enabled user account is suspended, the adapter disable the user's mailbox but does not permanently delete the mailbox from the Exchange server but it is flagged as disconnected by the Exchange server. By default, the Exchange server preserves the disabled mailbox for a specific duration. An administrator can configure this duration.
- By default all the deleted/disabled mailboxes stay in the mailbox store for 30 (thirty) days. This value can be set at mailbox store level.
  Following are the steps to modify this value directly on Exchange Server:
  1. Open Exchange Management Console
  2. Expand Server Configuration
  3. Click on Mailbox
  4. Select your server in the Mailbox Pane
  5. Select the <Mailbox> you want to configure and click on the Properties of selected Mailbox Database.
  6. Set value Under Mailbox Database Properties->Limits->Keep deleted mailboxes for (days)->30

  Please note that mailbox with no mails will not be moved to Disconnected mailbox. They are completely deleted from database when disconnected.

- Disabled mailbox can be of type user mailbox or resource mailbox on the exchange server. To differentiate user disabled mailbox and resource disabled mailbox, a new attribute "erADEMailboxType" of object class "erADDisabledMB" is added. One must customize the filter value used by attribute erADEConnectToMailbox to display only user disabled mailbox on account form. If you reconnect\connect a user account to a resource disabled mailbox then that mailbox will be connected and converted as a user mailbox by the adapter.
- The associated mailbox object in the Exchange mailbox database is not created until the mailbox either receives a message or the user logs on to it. If you create a new mailbox, and then remove or disable that mailbox before the mailbox object in the Exchange mailbox database is created, then it will not be available as a disconnected mailbox.
- One should reapply mailbox folder policy and other mailbox related attributes after connecting a mailbox. As these exchange attributes are reset when mailbox is re-attached. If mailbox is

disconnected all its mailbox policy with other exchange attributes are removed from Active Directory (Excluding Mailbox permissions).

Under normal circumstances all the deleted\disabled mailboxes are available under Disconnected-mailbox panel, but when a mailbox is disabled by external means other than the Disable-Mailbox cmdlet or Remove-Mailbox cmdlet or if mailbox is disabled by Windows AD adapter and the Exchange Information Store service was stopped, then it is possible that these mailboxes will not appear in the disconnected mailbox panel. In this scenario “Clean-MailboxDatabase” cmdlet should be used through Exchange Management Shell to scan for these disconnected mailboxes.

For more detail on Clean-MailboxDatabase, please follow the Microsoft link:
http://technet.microsoft.com/en-us/library/bb124076.aspx

The following table will list the various combinations to modify the mail status of a user account. For more information about changing the status of user account, see "Modifying the mail status of a user account" in Active Directory Adapter User Guide.

Current Status of User Account	What to Perform	How to Perform
When a user account is **Mailbox**-enabled	Modifying the mail status of a user account from Mailbox-enabled to Mail-enabled	To modify a Mailbox-enabled user account to a Mail-enabled user account, you must clear the value for the Mailbox Store attribute on the Active Directory account form and specify a value for the Target Address attribute on the Active Directory account form
When a user account is **Mailbox**-enabled	Disable the existing user mailbox and connect to a disconnected mailbox	To modify a Mailbox-enabled user account to connect to a disconnected mailbox, you must clear the value for the Mailbox Store attribute on the Active Directory account form and specify a value for the Connect To Mailbox attribute on the Active Directory account form. This operation will disable the existing mailbox and will connect the user to disconnected mailbox specified in the operation. NOTE: When you clear the mailbox store attribute the user mailbox is not deleted but it is disabled and flagged as disconnected mailbox.
When a user account is **Mailbox**-enabled	Move existing user mailbox to a new Mailbox Store.	For a mailbox-enabled user account, if you specify a new value of Mailbox Store attribute then that user mailbox is moved to the new

		mailbox store specified in the operation.
When a user account is **Mailbox**-enabled	Disable the existing user mailbox and create new mailbox for the same user	You cannot perform this operation in a single request. To achieve this operation follow the steps listed below: 1. Perform modify operation and clear the value for the Mailbox Store attribute on the Active Directory account form. 2. After you successfully clear the mailbox store attribute, Perform the second modify operation and specify a value for the Mailbox Store attribute on the Active Directory account form for the same user. You can also specify the value of Alias attribute with other exchange attributes. NOTE: When you clear the mailbox store attribute the user mailbox is not deleted but it is disabled and flagged as disconnected mailbox.
When a user account is **Mailbox**-enabled	Disconnect\Disable user mailbox	Perform a modify operation and clear the value for the Mailbox Store attribute on the Active Directory account form. NOTE: When you clear the mailbox store attribute the user mailbox is not deleted but it is disabled and flagged as disconnected mailbox
When a user account is **Mail**-enabled	Modifying the mail status of a user account from Mail-enabled to Mailbox-enabled	To modify a Mail-enabled user account to a Mailbox-enabled user account, you must clear the value for the Target Address attribute on the Active Directory account form and specify a value for the Mailbox Store attribute on the Active Directory account form.
When a user account is **Mail**-enabled	Disable the existing Mail-enabled user and connect to disconnected mailbox	To modify a Mail-enabled user account to connect to a disconnected mailbox, you must clear the value for the

		Target Address attribute on the Active Directory account form and specify a value for the Connect To Mailbox attribute on the Active Directory account form. This operation will disable the mail-enabled user account and will connect the user to disconnected mailbox specified in the operation.

Configuration required for using this feature, modify the profile using one of the following procedures:

Procedure 01:

1) Set the adapter registry key “ReconDisconnectedMailbox” to TRUE using agentCfg utility.
2) Modify the erADAccount.xml file of ADprofile.jar and import the new profile on IBM Tivoli Identity Manager.
   a) Copy the ADprofile.jar file to a temporary directory, example C:\Temp.
   b) Extract the contents of ADprofile.jar file into the temporary directory by running the following command:

      cd C:\Temp

      jar -xvf ADprofile.jar

      The jar command creates the C:\Temp\ADprofile directory, which has all the profile files.
   c) From the extracted ADprofile directory, open the erADAccount.xml file in a Text editor and make the following modifications and save the file:

      Add the following as a new account form element in the erADAccount.xml file

```
<formElement direction="inherit" label="$eradeconnecttomailbox"
name="data.eradeconnecttomailbox">
<searchFilter type="input">
<filter>(objectclass&#61;eraddisabledmb)</filter>
<base>contextual</base>
<attribute>erademailboxname</attribute>
<sourceAttribute>eradembconnectinfo</sourceAttribute>
<delimiter />
<size />
<width>300</width>
<objectClass>eraddisabledmb</objectClass>
<showQueryUI>false</showQueryUI>
<paginateResults>false</paginateResults>
</searchFilter>
</formElement>
```

      Note: The above search filter (objectclass=eraddisabledmb) will list all the disabled mailboxes available as support data including disabled Resource Mailboxes. To list only disabled User Mailboxes use the following

```
<formElement direction="inherit" label="$eradeconnecttomailbox"
name="data.eradeconnecttomailbox">
<searchFilter type="input">
<filter(&apos;(objectclass&#61;erADDisabledMB)(erADEMailboxType&#61;User))</filter>
<base>contextual</base>
<attribute>erademailboxname</attribute>
<sourceAttribute>eradembconnectinfo</sourceAttribute>
<delimiter />
<size />
<width>300</width>
<objectClass>eraddisabledmb</objectClass>
<showQueryUI>false</showQueryUI>
<paginateResults>false</paginateResults>
</searchFilter>
</formElement>
```

d) Run the following command to create new jar file:
   cd C:\Temp
   jar -cvf ADprofile.jar ADprofile
   Note: The directory name and profile name is case sensitive,
e) Import the new ADprofile.jar file on IBM Tivoli Identity Manager.
f) Perform a Full Reconciliation or Support Data Reconciliation.

Procedure 02:
Above configuration changes for ADprofile can also be done through IBM Tivoli Identity Manager Server (ITIM5.x) **Design Form** (For ITIM4.6 use "Form Customization"). To use the Design form please Perform the following steps:

a) Set the adapter registry key "ReconDisconnectedMailbox" to TRUE value using agentCfg.

b) Import the ADprofile provided with this version.

c) For IBM Tivoli Identity Manager 5.x, Go to Configure System Select "Design Form"

   (For IBM Tivoli Identity Manager 4.6, Go to Configuration->Form Customization)

d) Under Account section Select "Windows AD Account" option for IBM Tivoli Identity Manager 5.x.

   (For IBM Tivoli Identity Manager 4.6 Select "ADAccount")

e) From the attribute List panel (Right-Top section), Select attribute "erADEConnectToMailbox" and add this attribute under mailbox tab or other tab as DropDownbox with SearchFilter option.

f) Provide the following values for DropDownbox List:

   Search Base: Contextual
   Object Class: erADDisabledMB
   Attribute: erADEMailboxName
   Source Attribute: erADEMBConnectInfo
   Filter: (&(objectclass=erADDisabledMB)(erADEMailboxType=User))

   NOTE: The above filter will show only Disconnected User Mailbox.

   OR
   Search Base: Contextual
   Object Class: erADDisabledMB
   Attribute: erADEMailboxName
   Source Attribute: erADEMBConnectInfo
   Filter: (objectclass=erADDisabledMB)

NOTE: The above filter will show all Disconnected Mailbox including Resource Mailbox.

g) Save the form customization.
h) Perform a Full Reconciliation or Support Data Reconciliation.

Refer to the information center or the online help for information about using Form Customization.

The above filter value can be more customized to selectively list disabled mailboxes based on mailbox type (resource or user), and exchange server. The attribute "erADEMBConnectInfo" of object class erADDisabledMB contains the MailboxGuid with Mailbox Database (With Exchange server) for a disconnected mailbox. If we have an Exchange Server say "ExchangeServer01" then we can customize filter value as shown in the below examples.

Example 01:
To display all disconnected user mailbox from Exchange Server "ExchangeServer01".
(&(&(objectclass=erADDisabledMB)(erADEMailboxType=User))(erADEMBConnectInfo=* ExchangeServer01*))

Example 02:
To display all disconnected mailbox including resource mailbox from Exchange Server "ExchangeServer01".
(&(objectclass=erADDisabledMB)(erADEMBConnectInfo=* ExchangeServer01*))

Example 03:
To display all disconnected mailbox including resource mailbox from all configured exchange server excluding Exchange Server "ExchangeServer01".
(&(objectclass=erADDisabledMB)(!(erADEMBConnectInfo=* ExchangeServer01*)))

Known configuration issue with Exchange 2010: "No provisioning provider installed"

This error is misleading in that it is normally caused by a lack of permissions by the adapter logon account and not due to a "provisioning provider" not being installed. In order to provision mailboxes to Exchange 2010, the logon account needs to be a member of the appropriate security groups. Since each AD install is different (single domain, multiple domains, sub domains, etc), and groups can be customized (added to other groups), it is not possible to provide a definitive list of group memberships required by the adapter logon account. Our experience has shown that membership in the following Exchange groups is sufficient to allow the adapter to provision mailboxes:

Recipient Management
Organization Management
Exchange windows Permissions

In addition, membership in the Domain Admins group is required to provision accounts.

If the adapter logon account is a member of these groups and you still get this error, adding membership to Enterprise Admins can determine if the problem is due to permissions. If this resolves the issue, refer to Microsoft documentation or trial and error to determine which group memberships are needed.

Adapter Version 5.0.11 Features

MR0204103013 - AD adapter support for DNWithBinary.

Adapter is enhanced to support *DNWithBinary* syntax for extended attribute.

With this enhancement adapter is now able to perform add, delete, modify, recon operations on the extended attributes of type *DNWithBinary*.

Note:

1) Adapter based filtering is not supported for syntax *DNWithBinary* for extended attribute.
2) Adapter based event notification has some limitations for syntax *DNWithBinary*. Refer *Known Issues* section**.**

The *DNWithBinary* attribute store values in following format in Active Directory:

B :< char count> :< binary value> :< object DN>
Here "<char count>" is the number of hexadecimal digits in "<binary value>"
"<binary value>" is the hexadecimal representation of the binary value and
"<object DN>" is a distinguished name of existing user object.

To set the extended attributes of type *DNWithBinary* on Active Directory you need to specify the value of attribute only in the above given format.

Example:

- If you need to set the attribute **msRTCSIP-UserPolicy**, value could be:
  B:8:01000000:CN={FCE1E52A-59D1-4FBB-9CB5-2679247F7943},CN=Policies,CN=RTC Service,CN=Services,CN=Configuration,DC=evaluation,DC=test

- If you need to set the attribute **otherWellknowObjects**, value could be:
  B:32:df447b5eaa5b11d28d5300c04f79ab81:CN=User01,OU=Testorg,DC=pwdtest,DC=COM

Adapter will check for the validity of formats specified for extended attributes of type *DNWithBinary*.

Adapter Version 5.0.12 Features

Behavior of 'mail' attribute

In Active Directory each User/Group object has a 'mail' attribute to store single e-mail address.
With Exchange 2003/2007/2010 this property points to the primary SMTP address of that object.
When the object is first mail- or mailbox-enabled, the "mail" attribute is set to the primary SMTP proxy address. The primary SMTP address itself is stored in the proxy Addresses field as part of the e-mail address list. If the value of primary SMTP proxy address is modified, then the "mail" attribute (E-mail address) is replaced with the new value of primary SMTP proxy address.

On Exchange 2003, If the value of “mail" attribute (E-mail address) is modified; the primary SMTP proxy is replaced with the new value of "mail" attribute (E-mail address). On Exchange 2007 or 2010 changing the value of “mail" attribute (E-mail address) does not have any effect on primary SMTP proxy address. Proxy addresses are generated by Recipient Update Service. The value of 'mail' attribute corresponds to the primary SMTP proxy address. If a mail or mailbox enabled account is enabled then the old value of mail attribute gets cleared and is set with the new value of primary SMTP address.

On Exchange 2003 if a mail or mailbox enabled account is disabled then value of mail attribute gets cleared. On Exchange 2007 or 2010 this value is not cleared if mail or mailbox account is disabled.

NOTE: It is recommended to have same value of primary SMTP proxy address and mail attribute in Active Directory to avoid unexpected behavior.

Please refer the section describing the 'mail' attribute in following MS links
http://support.microsoft.com/kb/275636

MR090210587 - Support for Exchange Unified Messaging management on Active Directory accounts with ITIM Windows Active Directory adapter.

With this release Windows Active Directory adapter is able to manage the Exchange Unified Messaging setup on Active Directory account with Exchange 2010/2007 environment with the ITIM Active Directory Adapter.

Only MailBox enabled user is able to use the feature of Unified Messaging. When you enable a user for Unified Messaging (UM), a default set of UM properties are applied to the user, and the user will be able to use the Unified Messaging features.

The procedure to enable User's mailbox for Unified Messaging using IBM Tivoli Identity Manager is as follows:

Prerequisites while enabling user for Unified Messaging:

- A UM dial plan has been created. To create dial plan please see the following link http://technet.microsoft.com/en-us/library/bb123819.aspx
- A UM mailbox policy has been created. To create mailbox policy please see the following link http://technet.microsoft.com/en-us/library/bb123510.aspx

Note: Creating, modifying Dial Plan, UM Mailbox Policy is out of the scope of the Windows Active Directory Adapter.

To support for Unified Messaging there are two attributes are added on ITIM under MailBox tab

- ***Unified MessagingMailbox Policy*** having dropdown search box (single valued)
- ***UM Addresses (Extensions)*** having Editable Text List (Multivalued)

Enable/Disable Unified Messaging:

To enable MailBox enabled user for Unified Messaging we have to specify the value of UM Mailbox Policy and UM Addresses (Extensions).

We can specify UM Mailbox Policy value from dropdown search box (its single valued attribute) We can specify UM Addresses (Extensions) by adding it in editable text list (its multi valued attribute).

For example:

UM MailBox policy can be like this "**CN=TestPolicy,CN=UM Mailbox Policies,CN=Exchange First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=orion,DC=com**"

- While enabling Unified Messaging, UM Addresses (Extensions) should be **"12345"** or **"123we6".** It should not contain any special characters. Special characters are not allowed in UM Addresses (Extensions) while enabling user for Unified Messaging.

Note:

- The given UM Addresses (Extensions) must contain number of digits that are mentioned in specified UM Mailbox Policy's Dial Plan.
- After enabling user's mailbox for UM, perform full recon or that user should be reconciled to set the formatted values of UM Addresses(Extensions) on TIM.

To disable user's MailBox for Unified Messaging we have to clear the value of UM Mailbox Policy on ITIM.

Note:
After disabling user's mailbox for UM, full recon or that user should be reconciled to clear the values of UM Addresses(Extensions)on ITIM or we can delete those values from ITIM by performing delete operation for those values

Modifying Unified Messaging:

To modify UM Addresses (Extensions) value we need to provide the value in specific format as API accepts the value of UM Addresses (Extensions) only in below format.

Format– eum:<extension number>;phone-context:<Dial plan name for the given extension number>

For example- eum:12345;phone-context:Mydialplan.newport.cm.ibm.com
EUM:67890;phone-context:Mydialplan.newport.cm.ibm.com

Here prefix "eum" indicates its secondary UM Addresses (Extensions) and prefix "EUM" indicates it's primary UM Address (Extensions).

Note:

- User must specify the value of Extensions in the UM Addresses (Extensions) attribute on ITIM. It should not specify in the Proxy Address attribute.

- After modifying the values of UM Addresses (Extensions). Full recon or lookup for that user should be performed to retrieve value of UM Addresses (Extensions) in Proxy addresses on ITIM.

→Unified Messaging Policy can be modified only if the selected new policy belongs to the same Dial Plan.

Consider the following cases while modifying the Unified Messaging Feature:

- While Enabling/Disabling/Modifying Unified Messaging feature on Exchange 2007 Windows Active Directory Adapter service must be running under Administrator Account

- Before modifying Unified Messaging Feature, it should be insured that User's MailBox must be enabled for Unified Messaging.

- Windows Active Directory Adapter will fail Unified Messaging attributes, if in a single request user is disabling MailBox and Modifying Unified Messaging Feature. In this case adapter will fail Unified Messaging attributes those having ADD/MODIFY operation type however return success for the Unified Messaging attributes having operation type DELETE.

MR081710242 - Optionally requires a MailBoxStore and use Exchange 2010 Default feature if Store is not present.

With this release Windows Active Directory Adapter is able to create default MailBox for user on Exchange 2010 using the default feature of Exchange 2010 if Store is not present.

On Exchange 2010, Windows Active Directory Adapter will create default mailbox for user if user specify any exchange attribute other than Target Address, ConnectToMailBox and MailBox Store attribute on ITIM .However on Exchange2007 it will not create default mailbox and Windows Active Directory Adapter will fail the other specified Exchange attributes with error message.

Note: After creating default mailbox, Full recon or that user should be reconciled to view the value of default MailBox on ITIM under MailBox Store attribute

Windows Active Directory Adapter will create Default MailBox on Exchange 2010 for user in the following cases:

- **While creating user:**

  While creating user if any exchange attribute is specified in the request other than Target Address, ConnectToMailBox and MailBox Store attribute Windows Active Directory Adapter will create default mailbox for user.

- **While Modifying user:**

  If user does not have MailBox, and while modifying user if any exchange attributes is specified other than Target Address, ConnectToMailBox and MailBox Store attribute with ADD/DELETE or MODIFY operations Active Directory Adapter will create default mailbox for user.

  If user does not have MailBox, and while modifying user if any exchange attributes is specified other than Target Address, ConnectToMailBox and MailBox Store attribute with only DELETE operation type then adapter will not create default mailbox for user.

Customizing or Extending Adapter Features

The 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 both through the use of pre-Exec and post-Exec scripting and schema extensions using the extshema.txt file.

Tivoli Identity Manager Resources:

Check the “Learn” section of the Tivoli Identity Manager Support web site for links to training, publications, and demos.

Support for Customized Adapters

The integration to the 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 Tivoli Identity Manager Adapter was built and tested on the following product versions.

Adapter Installation Platform:

Windows 2003	Standard Edition 64-bit OS on x64 compatible CPU
Windows 2003	Enterprise Edition 64-bit OS on x64 compatible CPU
Windows 2008	Standard Edition 64-bit OS on x64 compatible CPU
Windows 2008	Enterprise Edition 64-bit OS on x64 compatible CPU
Windows 2008 R2	Enterprise Edition 64-bit OS on x64 compatible CPU.
Windows 2008 R2	Core Enterprise 64-bit OS on x64 compatible CPU

Managed Resource:

Active Directory on Windows 2003 Standard or Enterprise Edition 64-bit OS
Active Directory on Windows 2008 Standard or Enterprise Edition 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.

IBM Tivoli Identity Manager:

Identity Manager v5.0

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:

```
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.

End of Release Notes