Release Notes

IBM® Tivoli® Identity Manager

Authentication Manager (ACE) Adapter for Solaris

Version 5.1.3

First Edition (May 12, 2011)

This edition applies to version 5.1 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 RSA Authentication Manager (ACE) 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 RSA Authentication Manager (ACE) Adapter Installation and Configuration Guide

Adapter Features and Purpose

The RSA Authentication Manager (ACE) Adapter is designed to create and manage accounts on Authentication Manager (ACE/Server). The adapter runs in “agent” mode and must be installed on the Authentication Manager server. The adapter communicates using the ACE API to the system being managed.

The adapter must be installed on the Authentication Manager system being managed. A single copy of the adapter can handle one Identity Manager service. 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 and changing accounts. 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 and with the permissions of the Authentication Manager administrator.

Service Groups Management

The ability to manage service groups is a new feature introduced in TIM 5.1. By service groups, TIM is referring to any logical entity that can group accounts together on the managed resource.

Managing service groups implies the following:

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

Note that service group name change is not supported in TIM 5.1 release.

The ACE 6.1 adapter does not support service groups management.

Contents of this Release

Adapter Version

Component	Version
Release Date	May 12, 2011
Adapter Version	5.1.3
Component Versions	Adapter Build 5.0.1015 Profile 5.0.1001 ADK 5.08
Documentation	RSA Authentication Manager Adapter for Unix Operating Systems Installation and Configuration Guide SC23-9646-00

New Features

Enhancement # (FITS)	Description
	Items included in current release
MR111710511	Ace 6.1 adapter modified to support users imported from LDAP See “Configuration Notes” for additional information.
MR0310092030	Support to set new PIN for token. Support to set token in new PIN mode. Support to set PIN to Next Tokencode. See “Configuration Notes” for additional information.
MR0615102351	Need all dates managed by the ACE adapter to be handled in the same date format, that is, Zulu. See “Configuration Notes” for additional information.
	Items included in 5.1.2 release
	None
	Items included in 5.1.1 release
	Initial release for Tivoli Identity Manager v5.1

Closed Issues

CMVC#	APAR#	PMR# / Description
		Items closed in current release
	IZ85960	61075,227,000 ACE Adapter may crash when received the modify request for attribute without the value.
	IZ33132	08848,057,649 Sequential modify request failed for all attribute of user, after rename operation.
	IZ09724	22492,L6Q Reconciliation process may crash if no Tokens (supporting data) are returned.
		00713,998,649 Generating the PIN for ACE adapter.
		Items closed in 5.1.2 release
	N/A	N/A Updated release notes. Listed known limitation.
		Items closed in 5.1.1 release
		None

Known Issues

CMVC#	APAR#	PMR# / Description
N/A	N/A	FIPS Mode FIPS security mode is not supported in this release of the adapter.
N/A	N/A	Uninstall Folder After upgrading the adapter, a folder with the name _uninst2 is created in the adapter installation directory.

Installation and Configuration Notes

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

Corrections to Installation Guide

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

Upgrading from v5.0 to v5.1

No additional steps are needed to install the 5.1 version of this adapter on an existing 5.0 adapter version. However, you must import the 5.1 service type (profile) version after installing the adapter.

Upgrading to ADK v5.14 or higher

When upgrading to from an earlier version of the adapter to a version with ADK v5.14 or higher, the Event Notification file (<eventContextName>.dat) must be manually removed. The file will be recreated automatically when the first full Recon is run.

MR111710511: Ace 6.1 adapter modified to support users imported from LDAP

For Authentication Manager users imported from LDAP, the following attributes cannot be modified:

- Temporary User (eracetempuser)
- Start Date (eracetmpusrstdt)
- End Date (eracetmpusrenddt)

When modifying the account for such a user, make sure that none of these attributes is changed. If the Temporary User flag is set, or if one of the Date attributes is changed, the modification operation will fail and you will see an error as described in the "Troubleshooting" section.

MR0310092030: Support to set new PIN for token. Support to set token in new PIN mode. Support to set PIN to Next Tokencode. PMR 00713,998,649 - Generating the PIN for ACE adapter.

1. Setting a new PIN for the token

   You can set a new PIN for a token assigned to an ACE user account.

   Usage:
   - The PIN value is set in the 'Set a new PIN' field (and its confirmation field), which is found in all the token tabs available on the TIM ACE account form.
   - A new PIN can be assigned during an "add account" or "modify account" operation.

2. Setting the token to new PIN mode

   You can set a token assigned to an ACE user account to new PIN mode. In this mode, the ACE user initially authenticates with the passcode generated with the existing PIN. On successful logon, the ACE user is prompted to change the PIN. This PIN can be system generated or user defined. From then on, the ACE user must login with the passcode generated with the new PIN.

   Usage:
   - An ACE token is set to new PIN mode by selecting the "New PIN mode" checkbox, which is found in all the token tabs available on the TIM ACE account form.

- A token can be set to new PIN mode during an “add account” or “modify account” operation.

3. Setting the PIN to Next Tokencode

   You can set the PIN for a token assigned to an ACE user account to next tokencode. This means that the PIN can be set to the first *n* digits of the token’s next tokencode. To set the token PIN to the next tokencode, you must provide the current tokencode..

   Usage:
   - The next tokencode PIN value is set in the 'Set PIN to Next Tokencode', ‘Current Tokencode’ and ‘Number of digits to be used from the Next Tokencode as PIN’ fields, which are found in all the token tabs available on the TIM ACE account form.
   - A next tokencode PIN value can be assigned during a “modify account” operation.
   - Follow these steps to set a next tokencode PIN value:
     a. For any time period , note the token’s current tokencode (for example, “12345678”) and next tokencode (for example, “87654321”) pair displayed on an RSA SecurID Token Device UI.
     b. For that token, select the ‘Set PIN to Next Tokencode’ checkbox.
     c. Enter the current tokencode in the ‘Current Tokencode’ field.
     d. Send a reconciliation/lookup request to the ACE service. After the reconciliation/lookup, a value appears in the “Number of digits to be used from the Next Tokencode as PIN” field (for example, “4”). In this example, the token’s new PIN is the first 4 digits of the next tokencode noted in step (a), or “8765”.

   The next time the user logs in to the ACE/Server with the token, he must use the new PIN.

   Notes:
   - A request for setting the PIN to Next Tokencode will fail if the next tokencode starts with 0. This is a restriction of the ACE/Server.
   - After a token’s PIN is set to Next Tokencode successfully, the user will find a new user extension data in the format ITIMToken=*token_number* : *number_of_digits* (for example, "ITIMToken=101010101: 4"). Do not to change or delete this data, since it is used by the adapter. The removal of this user extension data is handled by the adapter appropriately during token assignment.
   - The user may also find a change in the user extension data if he sets the PIN in Next Tokencode again.

MR0615102351 - Need all dates managed by the ACE adapter to be handled in the same date format ,that is, Zulu).

There are several date type attributes that are managed by the ACE adapter. Two of these attributes pertain to ACE temporary user accounts and are read/write and can be modified using the ITIM console:
- erAceTmpUsrStDt – Start Date
- erAceTmpUsrEndDt – End Date

The other date type attributes pertain to ACE user account tokens and are read-only:
- erAceToken1ActivatedDate – Date Activated (Token #1)
- erAceToken1ShutdownDate – Date Will Shutdown (Token #1)
- erAceToken1EnableDisableDate - Date Enabled/Disabled (Token#1)
- erAceToken1LastLoginDate – Last Login Date (Token#1)
- erAceToken2ActivatedDate – Date Activated (Token #2)
- erAceToken2ShutdownDate – Date Will Shutdown (Token #2)

- erAceToken2EnableDisableDate - Date Enabled/Disabled (Token#2)
- erAceToken2LastLoginDate – Last Login Date (Token#2)
- erAceToken3ActivatedDate – Date Activated (Token #3)
- erAceToken3ShutdownDate – Date Will Shutdown (Token #3)
- erAceToken3EnableDisableDate - Date Enabled/Disabled (Token#3)
- erAceToken3LastLoginDate – Last Login Date (Token#3)
- erAcePasswdShutdownDate – Date Will Shutdown (Special Token)
- erAcePasswdEnableDisableDate – Date Enabled/Disabled (Special Token)
- erAcePasswdLastLoginDate - Last Login Date (Special Token)

The two read/write date attributes are always managed and stored in the ITIM LDAP repository in UTC (Universal Coordinated Time) format, as this is their format in the ACE /Server endpoint. The read-only attributes can be managed and stored in either UTC or in local time format, depending on the value of an adapter registry property **DATE_FORMAT_IN_ZULU**.

Note: "Zulu Time" is a military term for UTC.

The **DATE_FORMAT_IN_ZULU** property is **false** by default, but its value can be set using the agentCfg utility.

1. DATE_FORMAT_IN_ZULU = true
    - During reconciliation or user lookup operations, the adapter will return date type attribute values in UTC format (YYYYMMDDHHMMZ); for example, 201007251021Z.
    - Note: In UTC time format seconds are ignored.

2. DATE_FORMAT_IN_ZULU = false
    - During reconciliation or user lookup operations, the adapter will return date type attribute values in local time format (MM/DD/YYYY HH:mm:ss); for example, 07/25/2010 10:21:00.
    - Note: Local time values that have no hour, minute or second units are stored in LDAP in the following format: MM/DD/YYYY HHH:mmm:sss; for example, 07/25/2010 000:000:000.

Setting the Start Date and End Date value through ITIM

The programmatic method that the ACE adapter uses to set the temporary user Start Date and End Date values does not allow minute units. This loss of precision, coupled with conversion between local time and UTC, can result in seemingly unexpected values for the Start Date and End Date attributes.

During an update of Start Date or End Date (during account modification, for example), the Date attribute values entered on the ITIM console are in the console's local time. This local time is converted to UTC before being sent to the ACE adapter. The adapter converts UTC to the ACE/Server local time and programmatically sets the values (without the minutes, if any). The ACE/Server displays the temporary user Start and End Dates in local time. If the operation succeeds, the ITIM server stores the updated value in LDAP in UTC format.

Example:
ITIM console time zone is GMT -0500
ITIM server time zone is GMT -0400
ACE/Server time zone is GMT +0330
Let's say the temporary user Start Date is set to 05/04/2011 02:02:00 (2:02AM) using the ITIM console.

Account modification flow

02:02	ITIM console local time
07:02	ITIM console local time is converted to UTC and sent to the ACE adapter – add 5h
10:32	ACE adapter converts UTC to ACE/Server local time – add 3h30m
10:00	ACE adapter programmatically passes in local time to ACE/Server (no minutes allowed)

On success, ITIM server stores the value in LDAP as UTC: 201105040702Z

So, the 2:02AM local start time entered on the ITIM console gets converted to 10:00AM local time on the ACE/Server.

During a reconciliation or account lookup, the ACE adapter programmatically fetches the Start and End Date values in UTC and passes them to the ITIM server. The ITIM server stores the dates in UTC format, but they are converted to the browser's local time for display in the ITIM console.

Account reconciliation flow, continuing with the example

10:00 ACE/Server local time
06:30 ACE adapter programmatically fetches date in UTC and sends to ITIM server – subtract 3h30m
01:30 ITIM console displays date in local time – subtract 5h
On success, ITIM server stores the value in LDAP as UTC: 201105040630Z

So, the reconciled Start Date is stored in ITIM with a UTC time of 06:30. When the date is viewed in the ITIM console, it shows a local time of 1:30AM. If an ITIM console were started on the ITIM server, it would show the Start Date in its local time, 2:30AM (UTC - 4h).

Troubleshooting

The following troubleshooting notes apply to this release:

The following items need to be added to or modified in "RSA Authentication Manager Adapter for UNIX Operating Systems Installation and Configuration Guide"

Chapter 9 .Troubleshooting.

Error message	Possible Cause	Corrective action
Sd_SetTempUser Error Cannot change temporary state for user synchronized from LDAP.	An attempt was made to set the Temporary User Start Date or End Date value for an ACE account that was imported from an LDAP registry.	Do not select the Temporary User checkbox, or set the Temporary Start Date or End Date for an ACE account that was imported from an LDAP registry.
Sd_SetTempUser Error Invalid hour value (0-23).	This error occurs when the user is selected as a Temporary user and the start date and end date are not specified. It might also occur if the Temporary User checkbox was selected for an ACE account that was imported from an LDAP registry.	Specify the start and end date correctly for setting the user as a Temporary user. Do not select the Temporary User checkbox for an ACE account that was imported from an LDAP registry.

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 only through the use of pre-Exec and post-Exec scripting.

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:
Solaris 9 OS 32-bit on UltraSPARC CPU
Solaris 10 OS 32-bit on UltraSPARC CPU

Managed Resource:
RSA Authentication Manager v6.1

IBM Tivoli Identity Manager:
Identity Manager v5.1

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.
IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

```
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY  10504-1785  U.S.A.
```

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

```
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.

End of Release Notes