# Release Notes

## IBM® Tivoli® Identity Manager

## ACE Server Adapter

***Version 4.6.6***

**Tenth Edition (September 23, 2009)**

This edition applies to version 4.6 of this Adapter and to all subsequent releases and modifications until otherwise indicated in new editions.

# Contents

Preface ..... 3

Adapter Features and Purpose ..... 3

Contents of this Release ..... 4

- Adapter Version ..... 4
- New Features ..... 4
- Closed Issues ..... 5
- Known Issues ..... 7

Installation and Configuration Notes ..... 8

- Corrections to Installation Guide ..... 8
- Configuration Notes ..... 8
- New Features in Version 4.6.5 ..... 10
  - Setting a new PIN for the token: ..... 10
  - Setting the token in new PIN mode: ..... 10
  - Setting the PIN to Next Tokencode ..... 10

Supported Configurations ..... 12

- Installation Platform ..... 12

Notices ..... 13

- Trademarks ..... 14

# Preface

Welcome to the IBM Tivoli Identity Manager ACE Server 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 ACE Server Adapter Configuration and Installation Guide

# Adapter Features and Purpose

The ACE Server Adapter is designed to create and manage ACE Server accounts and Tokens. This adapter must be installed on the server where ACE is installed. For replicated ACE systems, install one Adapter on the primary ACE server.

The ACE Server Adapter is a powerful tool that requires Administrator Level authority. The Adapter operates much like a human system administrator, creating accounts and assigning privileges. 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 permissions.

# Contents of this Release

## *Adapter Version*

| Component | Version |
|---|---|
| Release Date | September 23, 2009 |
| Adapter Version | 4.6.6 (build 4.6.1012) |
| Comm. Libraries | ADK v4.803 |
| Documentation | ACE Server Adapter Installation and Configuration Guide v4.6.0 |

## *New Features*

| Enhancement # (FITS) | Description |
|---|---|
| | **Items included in current release** |
| | None |
| | **Items included in release 4.6.5** |
| MR0310092030 | Support to set new PIN for token.<br>Support to set token in new PIN mode.<br>Support to set PIN to Next Tokencode. |
| | **Items included in release 4.6.4** |
| | None |
| | **Items included in release 4.6.3** |
| | None |
| | **Items included in release 4.6.2** |
| | Added support for User Extension Data<br>NOTE: the profile must be reinstalled to use this feature. |
| | **Items included in release 4.6.1** |
| MR0201052918 | ACE: Server Agent Support for ACE Server 6.0 |
| | **Items included in release 4.6.0** |
| | Updated for use with ITIM 4.6.0 |

## *Closed Issues*

| DevTrack | APAR# | PMR# / Description |
|---|---|---|
| | | **Items closed in current version** |
| | IZ58714 | 32771,077,649<br>UNABLE TO MODIFY EXISTING "END DATE" VALUE ON A RSA/ACE ACCOUNT FROM TIM. |
| | IZ55836 | 81471,227,000<br>ACE Adapter Crash (Applicable only for Solaris). |
| 36265 | | N/A<br>Ace adapter crashes on Solaris when Last Name, First Name & PIN value is set as Blank (Applicable only for Solaris). |
| | | **Items closed in version 4.6.5** |
| | IZ33132 | 08848,057,649<br>Sequential modify request failed for all attribute of user, after rename operation. |
| | IZ34060 | 30201,057,649<br>Adapter Crashes at the time of Reconciliation & TIM gives an Error :<br><Message Id="The entity name must immediately follow the '&' in the entity reference> |
| | | **Items closed in version 4.6.4** |
| | IZ09724 | 22492,L6Q,000<br>ACE adapter recon result in the adapter crashing or the recon gets the accounts, but none of the supporting data (tokens) returned to the TIM server, but the recon shows as success in TIM.<br><br>NOTE: xforms.xml is removed from the adapter side & at TIM side xforms.xml is present with minimum required attributes. After installation of this adapter version, ensure that xforms.xml is not present in the adapter installation directory. |
| | | **Items closed in version 4.6.3** |
| N/A | IY96234 | 81260,49R,000<br>Ace adapter crashes when erUID is null.<br><br>Note on Required AuthMan Attributes:<br>This adapter is configured to require the minimum set of attributes to create an AuthMan account. If you have configured your AuthMan system to require additional attributes, IBM suggests that you use the ITIM Form Designer to make these attributes “required.” IBM further recommends that your Provisioning Policy be configured to supply these required attributes.<br><br>Example: If the "User-Created Pins required" option is checked on the AuthMan Server and the CREATEPIN attribute is not sent in the ITIM request, the agent will log warning message or fail the request. |

| DevTrack | APAR# | PMR# / Description |
|---|---|---|
| | | **Items closed in version 4.6.2** |
| | IY96123 | 50068,L6Q,000<br>Group name gets truncated by Ace server if length is more than 48 characters. |
| | | **Items closed in version 4.6.1** |
| | | None |
| | | **Items closed in version 4.6.0** |
| S16312 | IY72244 | 63027,122,000<br>Ace Server adapter does not always correctly process a modify operation when there is a token replacement of a single token. |

## *Known Issues*

| DevTrack | APAR# | PMR# / Description |
|---|---|---|
| | | Changing UserID and Deleting users having Admin rights are not supported in Adapter because RSA API does not support Deleting Administrators. |
| | | On Ace 5.2 Server, the Start and End Dates of the Temporary User field will be changed as a result of User modify operations through Adapter, in case, User is not a temporary user.<br><br>This is a known Ace Api Sd_SetUser( ) issue. If you are facing the same problem, upgrading to Ace Sever 6.1 will resolve it. |

# Installation and Configuration Notes

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

## *Corrections to Installation Guide*

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

None.

## *Configuration Notes*

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

NOTE: The adapter does not support the following ACE 6.0 attributes.

- Emergency Tokencode
- Emergency Passcode

NOTE: The account, which the Agent will run from, must comply with the following:

- The Agent account must have full permissions on the directory that contains the ACE/Server software.
- The Agent account must be registered in the ACE/Server database with administrator role.

Maximum Token Limit:
The ACE/Server limits the number of tokens to three. When assigning a password to a user, the ACE/Server will treat that as a special token, hence, the available numbers of tokens will become two.

Assigning Password:
When applying (assigning) a Password to a user, the Agent must receive the following:

a) The password, passed in the Password attribute.
b) Duration of the password is valid, passed in two attributes:
   - Days attribute (number of days password is valid).
   - Duration attribute (number of hours password is valid).
c) PasswordToken attribute MUST be set to YES.

Un-Assigning Tokens:
When Un-Assigning the Last Tokens from a user, the ACE/Server will delete the user from the database unless one of the following is true:

a) The user belongs to any group
b) The user is enabled on any client.
c) The user is an administrator.
d) The user record has extension fields.

If any of the above is true, the ACE/Server will fail the un-assignment of a token, and the Agent will fail the transaction as well.

In the event where the user is deleted due to un-assigning of the last token, the Agent will re-add the user without any tokens. The Agent will user the existing Login ID, Last Name, First Name, Default Shell and Create PIN mode to re-add the user

Suspend/Restore a User:
Suspending a user implies that all the user's tokens will be disabled.
Restoring a user implies that all the user's tokens will be enabled.

Using the User Extension Data Feature
The user extension data is a key-data pair and must follow these conventions:

Key: Name for the extension data field. The key can be up to 48 characters.
If key contains a colon (":") then it must be escaped with "\".
The key may not contain " , " as this sequence is used by Ace Server while returning
The key-data pair.

Data: Data that you want to store in this field. The value can be up to 80 characters.

Format: The key-data pair must be separated by ":"
Example "key1:value1" where key=key1 and data=value1.

## *New Features in Version 4.6.5*

The following new features have been added to this version of the adapter.

### Setting a new PIN for the token:

You can set a new PIN for a token assigned to the user.

Usage:

- The user can specify this value in the 'Set a new PIN' field on the TIM UI. The user can find this field in all the token tabs available on the TIM account form.
- The user can assign this new pin during the ADD or the MODIFY operation.

### Setting the token in new PIN mode:

You can set the token in new PIN mode. In this mode, the user initially authenticates with the Passcode generated by the PIN. On successful logon he/she is prompted for change in PIN. This PIN can be system generated or user defined. Then onwards, user has to login with the Passcode generated by the New PIN.

Usage :

- The user can set the token in New PIN mode from the TIM UI by selecting the field 'New Pin mode'. The user can find this field in all the token tabs available on the TIM account form.
- The user can set the token in New PIN mode during the user ADD or the MODIFY operation.

### Setting the PIN to Next Tokencode

You can set a PIN for a token to next tokencode. It means that, the PIN can be set with the first n digits of a next tokencode. To achieve this, you have to provide the Current Tokencode with setting the token to Next Tokencode. Then, you will get the number of digits to be used as PIN from the Next Tokencode.

Usage :
The PIN can be set in Next Tokencode only during the user MODIFY operation.
The following are the steps that the user has to follow for setting the PIN in Next Tokencode.

1. Note down current tokencode (for example, "12345678") and next tokencode (for example, "87654321") pair for any time period displayed on RSA SecurID Token Device UI
2. The user has to select the 'Set PIN to Next Tokencode' checkbox on the TIM UI.
3. The user has to type the noted current token code to the field 'Current Tokencode' on the TIM UI. For example, Current Tokencode is "12345678".
4. The new PIN of the token will be the first n digits of the Next Tokencode. For example, Next Tokencode is "87654321".

Then, the user has to send a reconciliation/lookup request from the TIM UI. After performing the reconciliation/lookup request, the user is able to see the value of field 'Number of digits to be used from the Next Tokencode as PIN' on the same token tab. For example, "4".

Then, the user will be able to login to the resource with the new PIN i.e. The new PIN will be the first n (For example, 4 is the number of digits seen in the field 'Number of digits to be used from the Next Tokencode as PIN' ) digits of the Next Tokencode that has been noted down. For example, "8765" will be the new PIN for the token as these are the first 4 digits of the Next Tokencode "87654321".

The user request for setting the PIN in Next Tokencode will fail if the Next Tokencode starts with 0. This is resource behavior (i.e. the behavior of ACE 5.2).

Notes:

- After the PIN is set in Next Tokencode successfully, the user will find a new user extension data of the type ITIMToken=<Token_number> : <no of digits>. For example, "ITIMToken=101010101 : 4". The user is requested 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 unassignement.

- The user may also find a change in the User extension data, when he sets the PIN in Next Tokencode successively.

# Supported Configurations

## *Installation Platform*

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

Adapter Installation Platform:
- Windows 2000 Server or Workstation
- Windows XP Workstation
- Windows 2003 Server

Managed Resource:
- RSA Authentication Manager v5.2 (ACE/Server) on Windows
- RSA Authentication Manager v6.0 (ACE/Server) on Windows

IBM Tivoli Identity Manager:
- ITIM 4.6.0 or later

IMPORTANT NOTE:
- This Adapter must be installed on the same server as the ACE system. The ACE system does not support a remote API. RSA supports v6.0 on Windows 2003 only.

# 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:

AIX
DB2
IBM
IBM logo
SecureWay
Tivoli
Tivoli logo
Universal Database
WebSphere

Lotus is a registered trademark of Lotus Development Corporation and/or IBM Corporation.
Domino is a trademark of International Business Machines Corporation and Lotus Development Corporation 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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

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

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

# End of Release Notes