# Release Notes

## IBM® Tivoli® Identity Manager

## Entrust Authority PKI Adapter

***Version 5.0.2***

**First Edition (August 4, 2008)**

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 Entrust Authority PKI 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 Entrust Authority PKI Adapter Installation and Configuration Guide

# Adapter Features and Purpose

The Entrust Adapter is designed to create and manage Entrust PKI accounts and both Desktop and Roaming Profiles (PKI Certificates). The adapter communicates to the system using the Entrust APIs. The adapter typically runs in “agent” mode and must be installed on the Entrust system being managed, but can be configured to run agentless. Refer Entrust Installation guide for instructions on running the adapter in “agentless” mode (remotely).

A single copy of the adapter can handle only 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 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.

Note: Read "Entrust PKI Adapter Administration" section before using the Entrust PKI Adapter.

# Contents of this Release

## *Adapter Version*

| Component | Version |
|---|---|
| Release Date | August 4, 2008 |
| Adapter Version | 5.0.2 |
| Component Versions | Adapter Build 5.0.1001<br>Profile 5.0.1001<br>ADK 5.07 |
| Documentation | Entrust Authority PKI Adapter Installation and Configuration Guide<br>SC23-6147-00 |

## *New Features*

| Enhancement # (FITS) | Description |
|---|---|
| | **Items included in current release** |
| | Added support for Entrust v7.1 |
| | **Items included in 5.0.1 release** |
| | Initial release for ITIM v5.0 |

## *Closed Issues*

| CMVC# | APAR# | PMR# / Description |
|---|---|---|
| | | **Items closed in current version** |
| 32546<br>32545<br>32568 | N/A | Password should not be required for creating a user without profile.<br>Password change operation for a user with profile results in crash and/or deletes the existing profile of user.<br>"All groups" and other group values, for group attribute, could not be added simultaneously. |
| | | **Items closed in 5.0.1 version** |
| | | None |

## *Known Issues*

| CMVC# | APAR# | PMR# / Description |
|---|---|---|
| N/A | N/A | Editing adapter profiles on UNIX or Linux.<br>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.<br>If you are using the vi editor, you can strip out the ^M character as follow:<br>From the vi's command mode:<br>:%s/^M//g<br>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.) |
| N/A | N/A | Using the Upgrade Option:<br>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 | Event Notification<br>Account status (Active/Inactive) might not be correctly updated on Identity Manager after event notification. |
| 31089 | N/A | Password Change to Existing Account<br>Password changes are supported for Entrust accounts without profiles. A profile is created during the password change. However, if a password is changed for active entrust accounts with a valid profile, the request fails, the profile file is deleted and the user cannot login. |
| N/A | N/A | Transaction Status “successful”<br>Changing the values for “lifetime” and “Expiry” attributes from TIM will not update the Entrust server, but the TIM operation shows a “success” status. |

# 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:

None.

## *Configuration Notes*

The following configuration notes apply to this release:

### Entrust PKI Adapter Administration

Pease be aware of the following key points regarding the usage of the Entrust PKI Adapter:

a) Adding an account

- If adding an account without creating a profile, the User State will be in Added mode only.

- If adding an account, creating a profile, and using the password based on Entrust password rule, the User State will be in Active mode.

- The syntax of the eruid may be complex; depending on the how Entrust Resource has been configured. For example: cn=Test123,cn=Test123+serialNumber=01012

- In order for the adapter to create a profile on Add Request, the user needs to check the "Create Profile Option" and supply a password.

b) Password Rules

- User Account password must comply with Entrust server password rules. Refer Password rules on Entrust Server.

c) Deprovisioning / Deleting an account

- When deprovisioning an account with a User State of Active mode, the profile will not be deleted from profile directory.

- When deprovisioning an account with a User State of Added mode, all user information will be deleted.

d) Suspending / Restoring an account

-Suspend/Restore operations are not supported for users created without profiles. If a user without profile is suspended, then one cannot perform further operations on that user not even restore, user in that case becomes a Non-Entrust user.

e) Revoking a certificate

-Users are only allowed to revoke certificate when the User State of an account is in Active mode. User can not revoke certificate when the User State in Added mode.

f) Key Update policy for user

-Following points should be considered:

a. If default policy is selected, no values should be provided for all other attributes under "Update policy" tab.

b. If update policy is "Key Lifetime" then values should be provided for all other "Key Lifetime" related attributes only.

c. If update policy is "Key Expiry", then values should be provided for all other "Key Expires" related attributes only.

IMPORTANT: Userlookup is to be performed each time before modifying the user as many default values are set on resource which will be retrieved after userlookup only.

### Troubleshooting the Entrust Adapter

"Entrust Server Error: (-32696)"
This error occurs if the Entrust LDAP Directory server instance is offline(not up). Start the LDAP instance service and then retry the transaction.

Entrust server contains an additional DLL "enterr.dll" which provides some error message descriptions. Please copy the Entrust DDL named “enterr.dll” and place it into the adapters <Agent_Install>\bin folder before starting the adapter service. After this is done, the error messages will be more readable. For example: **"Entrust Server Error: (-32696) The Directory is off-line. The Entrust Authority server might not be accessible from this computer."** error message can be seen in adapter logs. This DLL can be found in the one of the following locations:

Entrust server machine:
1. \Entrust\Security Manager\bin
2. \Entrust\Security Manager\Tools\config
3. \Entrust\Security Manager\Tools\dvt

"Security Manager Administration Client” machine
(SMA is used to remotely access the Entrust Server)
1. \Entrust\Security Manager Administration

Additional troubleshooting information can be found in the Entrust application logs. Refer to the Entrust server logs "mgraudit.log" and "manager.log" located at \authdata\log on Entrust resource machine.

# 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:
Windows 2003

Managed Resource:
Entrust Authority PKI server v7.0
Entrust Authority PKI server v7.0

IBM Tivoli Identity Manager:
Identity Manager v5.0

IMPORTANT NOTE:
This Adapter only supports password changes on Entrust users without profiles.

# 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