Release Notes

IBM® Tivoli® Identity Manager

CA Top Secret Adapter

Version 5.1.8

First Edition (August 20, 2015)

This edition applies to version 5.1 of Tivoli Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Table of Contents

Preface

Welcome to the IBM Tivoli Identity Manager CA Top Secret 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 CA Top Secret Adapter Installation and Configuration Guide

Adapter Features and Purpose

The CA Top Secret Adapter is designed to create and manage Top Secret accounts. The adapter runs in “agent” mode and must be installed on z/OS. One adapter is installed per CA Top Secret database.

The deployment configuration is based, in part, on the topology of your network domain, but the primary factor is the planned structure of your Identity Manager Provisioning Policies and Approval Workflow process. Please refer to the Identity Manager Information Center for a discussion of these topics.

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

Service Groups Management

The ability to manage service groups is a 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 attributes of a service group.
Delete a service group.

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

The Top Secret adapter does not support service groups management.

Contents of this Release

Adapter Version

Component	
Build Date	August 19, 2015
Adapter Version	5.1.8
Component Versions	Adapter Build 5.0.10182 Profile 5.0.1004 ADK 6.02 z/OS
Documentation	CA Top Secret Adapter Installation and Configuration Guide SC23-9653-03 The 5.1 documentation is no longer updated. For the latest documentation changes please refer to the information provided in these release notes and the 6.0 adapter documentation provided in the IBM Security Identity Manager Knowledge Center.

New Features

Internal#	Enhancement # (FITS/RFE)	Description
		Items included in current release
		User lookup APPC configuration (see Configuration notes section below)
RTC 115559	35062 21865	ertopzdivisionacid, ertopzdepartmtacid and ertopzzoneacid attributes modification
RTC 125711	33906	ITIM Top Secret Adapter compatibility with Passphrase
		Items included in 5.1.7 release
		None
		Items included in 5.1.6 release
		Add CA Top Secret standard attribute TSODEFPRFG to the default schema.
		Support user-defined ACID fields with extended attributes.
		Make additional information (attributes) available to ITIMEXIT using the multi-value attribute ertopzexitstring.
		Add support for a CA Top Secret command comment to be passed to the adapter.
		Items included in 5.1.5 release
	MR0219102522	Ability to unlock account, when locked due to many wrong password tries. If the psuspend flag is on the account due to many wrong password tries, the attribute "Access suspended after PTHRESH Violation" can be modified on the account form to change the value for the attribute representing psuspend.
		Implement support of the option 'ACID under which requests will be processed' specified on the Tivoli Identity Manager service form. Surrogate user support must be defined in Top Secret.
		Items included in 5.1.3 release
		None

		Items included in 5.1.2 release
		None
		Items included in 5.1.1 release
		Initial release for TIM v5.1 **NOTE: This adapter is also supported on TIM 5.0** This adapter is also being made available for TIM 5.0 customers. The documentation refers to TIM 5.1 but applies equally to TIM 5.0.
	MR0217051530	CA Top Secret adapter not based on FTP protocol.
	MR0315053725	CA Top Secret adapter to manage Administrative ACIDs.
	MR0130063318	Update the adapter to provide filter features
	MR0909096657	CA Top Secret Adapter for TSS version 14
	MR0504062234	Modify the CA Top Secret adapter to support order-specific profiles
	MR0708043512	Modify the CA Top Secret adapter to support filtered recons.

Closed Issues

INTERNAL#	APAR#	PMR# / Description
		Items included in current release
		None
		Items included in 5.1.7
	IV25449	Error in setting the READ_TIMEOUT parameter.
RTC67316		Addition of an option in the installation panels to allow the setting of a password for the ITIM adapter ACID
RTC71208		Installation panels not generating the correct JCL to add the required entry in the CA Top Secret Started Task Command (STC) Record.
		Items included in 5.1.6
Internal		Correction to handling of USING keyword on an add request.
Internal		Correction to error message if an attempt is made to add a user of type SCA.
		Items included in 5.1.5 release
	N/A	13681,112,848 certTool generating corrupt CSRs
	IZ92544	A few CA Top Secret adapter attributes are misspelled in the documentation
	IZ86303	z/OS adapter with 2-way SSL (Register certificate). Registered certificates giving 'Subject validation failed' message even when correctly registered.
	IZ96327	Response message for request shows a parsing error. Error: An invalid XML character (Unicode: 0x1a) was found in the value of attribute "matchedDN" and element is "LDAPResult”
Internal		Open CFILEIN, used during reconciliation, for read only not read and write.
Internal		Fixed the script that executes certTool, so it references the registry in the correct directory.
		Items included in 5.1.3 release
	IZ67183	10651,379,000 TOPSECRET ADAPTER MISSING ERTOPZEXECNAME AND ERTOPZEXECVAR FROM SCHEMA.DSML IN PROFILE
	IZ65734	03575,379,000 INSTALLATION OF TOP SECRET ADAPTER DOES NOT CORRECTLY CONFIGURE APPC IF ALREADY INSTALLED.
	IZ73026	24184,422,000 'WARNING' RESULT RETURNED FROM TOP SECRET ON A

		SUCCESSFUL PASSWORD CHANGE
		Items included in 5.1.2 release
	IZ66466	22030,422,000 CA Top Secret adapter certificate installation instructions are incorrect. See the Configuration Notes section of this document for more information.
		Items included in 5.1.1 release
		None

Known Issues

INTERNAL#	APAR#	PMR# / Description
RTC67316		Earlier releases of the CA Top Secret Adapter do not place a password on the CA Top Secret ACID for ITIM adapter when created. IBM supports the use of a password on this account. Please note that adding a password to the ITIM adapter ACID may result in the console prompting for the password at adapter start up.
	N/A	User-defined ACID fields are supported for a data length of up to 249 bytes. Field data containing characters other than letters, numbers, or national characters (@, #, $) may have unpredictable results.
	N/A	This release of the CA Top Secret Adapter is compatible with CA Top Secret for z/OS R15, but does not support the new keyword MATCHLIM.
	N/A	This release of the CA Top Secret Adapter does not support FIPS mode.
	N/A	**Unload Utility Requires Fix Pack** The unload for Top Secret may require a fix pack to retrieve the data from continuation records in multi-valued fields. Please ensure latest available CA Service Pack is installed.

Installation and Configuration Notes

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

Upgrading to Version 5.1.8 (or later)

Upgrading to version 5.1.8 will require a full install, refer to the Installing and configuring section of the CA Top Secret adapter guide for full details.

1) Upload the XMI file and install the ISPF dialog as described in the “Installing and configuring the adapter” chapter of the CA Top Secret adapter guide.
2) Run the ISPF dialog and load previously saved variables using option 1, then generate the job streams using option 3. This generates the JCL in userid.ITIMTSS.CNTL and populates data files in userid.ITIMTSS.DATA.
3) Assuming installing directly over an existing, working adapter running on ADK version 5.17+ with no changes to the installation parameters (the saved variables), then the only installation jobs in data set userid.ITIMTSS.CNTL that need to be submitted are listed below:

   J3: This job allocates and populates the load and exec data sets, and populates the OMVS directories. You may require superuser authority to submit this job successfully.
   J6: This job registers the APPC/MVS transactions.

4) Import the adapter profile into the Tivoli Identity Manager server.

Additional Notes

The adapter task should not run as a MSCA, therefore SCA ACIDs can not be created by the CA Top Secret adapter.

Starting and stopping the adapter

Before you start the adapter, ensure that TCP/IP is active, and the APPC/MVS and the ASCH address spaces are active.

Customising or Extending Adapter Features

The Identity Manager adapters can be customised and/or extended. The type and method of this customisation may vary from adapter to adapter.

Getting Started

Customising 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:

A. LDAP schema management
B. Working knowledge of scripting language appropriate for the installation platform
C. Working knowledge of LDAP object classes and attributes
D. Working knowledge of XML document structure

Note: This adapter supports customisation only through the use of pre-Exec and post-Exec scripting. The CA Top Secret adapter has REXX scripting options. Please see the CA Top Secret Installation and Configuration guide for additional details.

IBM Tivoli Identity Manager Resources:

Check the “Learn” section of the IBM Security Identity Manager Knowledge Center for links to training, publications, and demos.

Installation Notes

The following installation notes apply to this release:

Running the ISPF dialog

Adapter specific parameters

Password for the ITIM adapter ACID
Specifies a password for the CA Top Secret Administrator ACID that is assigned to the adapter task. Note that adding a password to the ITIM adapter ACID may result in the console prompting for the password at adapter start up.

CA-Top Secret Default Group ACID for adapter
Specifies an *existing* CA Top Secret z/OS UNIX GROUP with a GID. A GID is a UNIX Group ID, which is a unique number assigned to a UNIX group name. The adapter operates as a z/OS UNIX process and requires this information.

Configuration Notes

The following configuration notes apply to this release:

Modifying protocol configuration settings

Table 7. Options for the DAML protocol menu

Option	Configuration task
K	Displays the following prompt: Modify Property 'READ_TIMEOUT': Specify the timeout value in seconds. The default is 0 and means that no read timeout is set. Note: READ_TIMEOUT is provided to prevent threads being left open in the adapter and causing 'hang' problems. The open threads may be due to firewalls, or network connections problems, and may be seen as TCP/IP ClosWait connections remaining on the adapter. If you encounter such problems, then you need to set the value of READ_TIMEOUT to just longer than the ITIM manager timeout (the maximum connection age DAML property on Tivoli Identity Manager) and less than any firewall timeout. The adapter will then need to be restarted as READ_TIMEOUT is set at adapter initialization.

Modifying Zone, Division and/or Department.

The new profile delivered with this adapter release allows changing the values for Zone, Division and Department when modifying an account. For each changing value the adapter will execute a MOVE command. When changing multiple values in one single request this will result in multiple move commands, one for each value:
MOVE ACID(USER) ZONE(ZONEA)
MOVE ACID(USER) DIVISION(USFAC)

MOVE ACID(USER) DEPT(HR)

Please note:

- The ACID TYPE is not appended to these commands.
- The value changes are processed in random order.

This can have two possible outcomes that require some attention:

1. It is possible to specify non-compatible values such as a request to move an ACID to a DIVISION and a DEPARTMENT which does not belong to this DIVISION.
2. The ACID type might change due to the execution of the MOVE command

More information on the changes in ACID types when performing a MOVE for an ACID without specifying TYPE can be found in the CA Top Secret product documentation.

The ITIM server will update the account for which the change request has been executed based upon the result the adapter returns for each individual value change. It will not report any changes in the ACID that resulted from the MOVE command. To ensure the ITIM server will reflect the actual current ACID definitions it is recommended to perform a reconciliation for the changed account directly after changing a ZONE, DIVISION or DEPARTMENT. A reconciliation for a single account is interpreted as an Account Lookup request by the adapter and will result in the adapter collecting only the data for the specified ACID. A Lookup can be requested by specifying a search filter for the reconciliation. This filter should be specified as a reconciliation query for a single eruid value. To perform a reconciliation for a single account named JOHND the query would be defined as follows:
Reconcile accounts that match this filter:
(eruid=JOHND)

The Lookup request will initiate a lookup specific APPC transaction to collect the data for the ACID specified in the search filter and return the updated account data to the ITIM server. Do note that the actual values retrieved by the Lookup request will depend on the administrative scope of the ACID used to perform the request (ADAPTERID or SURROGAT). For more information on the data each ACID type can list within its administrative scope please refer to the CA Top Secret product documentation.

To support processing of the Lookup request a new APPC transaction is introduced which can be configured at installation time:

```
 ------------------ ITIM CA-TopSecret Adapter Customization -----------------
 Option ===>

 VTAM and APPC/MVS Parameters

    VTAM NETID                         ===> NET1

    VTAM Originating Logical Unit      ===> ITIMORIG (*)

    VTAM Destination Logical Unit      ===> ITIMDEST (*)

    VTAM Session Key                   ===> 0123456789ABCDEF

    VTAM LOGMODE entry name            ===> #INTERSC

    Fully qualified data set name of your APPC/MVS transaction data set:
     ===> SYS1.APPCTP

    APPC command transaction name      ===> ITIMTCMD

    APPC reconciliation transaction    ===> ITIMTREC

    APPC ACID lookup transaction       ===> ITIMTLOK

    APPC execution class               ===> A

    APPC Network Qualified Names?      ===> FALSE     (True or False)

  (*) If both LU's specified are the same, it must reflect the name of the
      APPC/MVS defined BASE logical unit.
```

The ACID lookup transaction has 2 requirements:
1. The presence of the DSEXEC setting and hlq.EXEC value in the adapter registry. This value will automatically be written to the registry file during adapter installation.
2. The presence of a new template member in the hlq.EXEC dataset: TSSLOKU. This member is automatically created during adapter installation.

Password Phrases

ITIM Top Secret for z/OS Adapter 6.0.8 and above support Top Secret password phrases. A password phrase in Top Secret is an authentication mechanism that allows the secret string to be between 9 and 100 characters. While setting passwords from the IBM Tivoli Identity Manager server, a string lesser than or equal to eight characters is treated as a password and a string more than eight characters is treated as a pass phrase.
Passwords are considered to be invalid when containing any of the following characters:
,) ({ } ' " and space
Password phrases are considered to be invalid when containing any of the following characters:
,) ({ } ' "
In the event the adapter encounters any of the above invalid characters it will return an error to the ITIM server.

On account Add:
When requesting a new account on the ITIM server the adapter will interpret any password string shorter

than 8 characters as a password and create the requested account with a password. A password string longer than 8 characters is interpreted as a password phrase. In this event the adapter will by default generate a random password using a standard, built-in, configuration string.
This standard configuration string is: CnccSCNS
The password generator will use this configuration string to generate a random password as defined below:
C → random uppercase char (no vowels)
c → random lowercase char (no vowels)
v → random lowercase vowel (a,e, i, o, u, and y)
V → random uppercase vowel (A,E, I, O, U, and Y)
N → random numeric
s → random special character
any other character → use as is provided (for instance: national characters)
Internally the adapter will ensure it will not generate the same characters consecutively.
The built-in string can be modified using new registry setting: PWD_CONFIG

PWD_CONFIG will allow a maximum of five (5) comma-separated strings which will be randomly selected by the adapter to generate random passwords.
The size of each string should be between 4 and 8 characters long. In the event a shorter string is specified the adapter will report an error and try another string. In the event a longer string is specified the adapter will use only the first 8 characters to generate a password.
The configuration string is not allowed to contain any of the following hard-coded reserved words:
APPL APR ASDF AUG BASIC CADAM DEC DEMO FEB FOCUS GAME IBM JAN JUL JUN LOG MAR MAY NET NEW NOV OCT PASS ROS SEP SIGN SYS TEST TSO VALID VTAM XXX 1234 .
Or any of the following characters: ,) ({ } ' " +
In the event a reserved word is found in the configuration string the adapter will report an error.
After receiving an error the adapter will attempt to select another random configuration string. After two failed attempts the adapter will stop processing and return an error.
The adapter will consider the first four characters of the logonid for the request it is currently processing as a reserved word. In other words: the adapter will also report an error in the event the first four characters of the logonid are part of the configuration string. Reserved word and short logonid validation is case insensitive.
Reserved word and short logonid validation is repeated for the generated password. In the event the adapter detects a reserved word and/or short logonid as part of the generated password the adapter will stop processing and return an error.
A new registry setting allows specifying additional reserved words: RESWORD.
Any comma-separated string found in the RESWORD registry setting value will be added to the hard-coded reserved words list during request processing.

For more information on adding and changing registry settings please refer to “First steps after installation>Adapter configuration for IBM Tivoli Identity Manager>Modifying registry settings” In the CA Top Secret for Z/OS adapter installation guide

On account Modify:
Password Phrases can be changed/added during a Modify request for an existing account. When adding an initial password phrase to an existing account don't forget to ensure the user is allowed to use password phrases by setting password phrase to TRUE in the account form when requesting a new user with a password phrase on the ITIM server.
When changing and/or adding a password phrase for an existing account it will by default become expired. Password phrase (also referred to as passphrase) expiration can be controlled by using a new registry setting: PHRASEEXPIRE
This setting is provided in the adapter installation menu as shown in the screen print below and can be changed using the agentCfg tool.

PHRASEEXPIRE supports 2 values: TRUE and FALSE.

- When set to TRUE pass phrases are expired.
- When set to FALSE pass phrases are not expired.

```
------------------- ITIM CA-TopSecret Adapter Customization -------------------
Option ===>

Adapter specific parameters

   Name of adapter instance                      ===> ITIAGNT

   Name of Started Task JCL procedure name       ===> ITIAGNT

   IP Communications Port Number                 ===> 45598
Note: The adapter will always require access to ports 44970 through 44994.
      These ports are implicitly reserved.

   Adapter authentication ID (internal)          ===> agent

   Adapter authentication password (internal)    ===> agent

   PDU backlog limit                             ===> 1000

   Do you want passwords set as expired?         ===> TRUE      (True, False)

   Do you want passphrases set as expired?       ===> TRUE      (True, False)

   Do you use SYS1.BRODCAST in the environment?  ===> TRUE      (True, False)

   CA-Top Secret SCA ACID for ITIM adapter       ===> ITIAGNT

   Password for the ITIM adapter ACID            ===>

   CA-Top Secret Default Group ACID for adapter  ===> OMVSGRP

   OMVS UID to be assigned to ACID (non-zero)    ===> 45598
```

For more information on adding and changing registry settings please refer to “First steps after installation>Adapter configuration for IBM Tivoli Identity Manager>Modifying registry settings” In the CA Top Secret for Z/OS adapter installation guide.

Troubleshooting of the CA Top Secret Adapter errors

Troubleshooting APPC problems

In addition to the information provided in the CA Top Secret for Z/OS adapter installation guide regarding troubleshooting for APPC problems please note it might be required to restart the APPC started task (STC) after (re)defining the APPCLU profile to CA Top Secret.

Supported Configurations

The IBM Tivoli Identity Manager Adapter supports any combination of the following product versions.

Operating System:
z/OS 1.13.x
z/OS 2.1.0

Managed Resource:
CA Top Secret for z/OS R14 and R15

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.

CA, CA ACF2, and CA Top Secret are trademarks of CA, Inc. in the United States, other countries, or both.

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