Release Notes

IBM® Security Identity Adapter for

CA Top Secret

Version 7.1.13

First Edition (March 14, 2018)

This edition applies to version 7.1.13 of IBM Security Identity Manager Adapter for Top Secret and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Table of Contents

Preface

Welcome to the IBM Security Identity CA Top Secret Adapter.

These Release Notes contain information for the following products that was not available when the IBM Security Identity Adapter manuals were created:

- IBM Security Identity CA Top Secret Adapter Installation and Configuration Guide

Adapter Features and Purpose

The CA Top Secret Adapter is designed to create and manage CA 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, but the CA Top Secret Adapter may be configured to support a subset of the accounts through the scope of authority feature on the CA Top Secret Service Form.

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 Provisioning Policies and Approval Workflow process. Please refer to the IBM Knowledge Center for a discussion of these topics.

The Identity 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 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.

IBM Security Identity Manager Service Groups Management

By service groups, ISIM 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 the current IBM Security Identity Adapter editions.

The CA Top Secret Adapter does not support service groups management.

Contents of this Release

Adapter Version

Component	Version
Build Date	March 14, 2018
Adapter Version	7.1.13
Component Versions	Adapter Build 7.1.13.000 Profile 7.1.13.00 ADK 6.04.000 z/OS
Documentation	Please check out the latest documentation on the IBM Security Identity Manager Knowledge Center. Select the latest server release to navigate to the latest adapter guides.

New Features

Internal#	RFE/CASE#	Description
		Items included in the current release
RTC 52661 RTC 173352	115005	As an AD for z/OS developer I need to offer the ability to explicitly disable TLS1.0 in all ADK based adapters.
RTC 173354	TS000074249	As an ADK for z/OS developer I need to add diagnostic messages to the ADK that allow troubleshooting 2-way ssl connections
RTC 173351		As an ADK for z/OS developer I need to upgrade to OpenSSL 1.0.2n
		Items included in release 7.1.12
RTC163066		As a Top Secret adapter customer, I would like to use the adapter in an IBM Security Identity Governance and Intelligence (IGI) environment.
		Items included in release 7.0.11
RTC166462	32451	TSS access FACILITIES as supporting data
RTC71407		MATCHLIM support
RTC163356		Enable SSL by default in the ISPF installation panels
		Items included in release 7.0.10
RTC154238		Update OpenSSL to release 1.0.2j
RTC154263	PMR 42182,122,000	Disable SSLV3 and RC4 ciphers and certify TLS 1.1 / 1.2 is supported by the ADK
RTC156347	32546	Adapter appears to be running while it was unable to connect to the socket.
RTC149041		Add two initial lines to CustomLabels.properties which are required for translation and update the profile version to match the adapter version.
		Items included in release 7.0.9
		No items included in this release
		Items included in release 7.0.8
		User lookup APPC configuration (see Configuration notes section below)
RTC 115559	35062 21865	ertopzdivisionacid, ertopzdepartmtacid and ertopzzoneacid attributes modification
RTC 125711	33906	ISIM Top Secret Adapter compatibility with Passphrase
		ISIM 6.0.2 release

Closed Issues

Internal#	APAR/CASE#	Description
		Items closed in the current release
RTC 173353	TS000114491	As an ADK for z/OS developer I need to ensure that manually dropping the DAML_PORT socket doesn't result in a loop
RTC 173360	TS000013259	Since installing 6.0.29 customer cannot longer change the DAML password
RTC 173723		Attempt to destroy context for invalid socket results in dump in _ermListFree
		Items included in release 7.1.12
RTC169659		PSIRT Malformed X.509 IPAddressFamily could cause OOB read (CVE-2017-3735)
		Items included in release 7.0.11
RTC166463	PMR 22742,003,756	RSA key length used by certTool increased from 1024 to 4096, which allows it to be NIST compliant beyond 2021.
RTC166463		Unmodified attribute values for failed add/remove profile operations not returned to the server
		Items included in release 7.0.10
RTC156346		Attribute values following the string PASSWORD are masked in the adapter log
RTC156842	PMR 17895,001,862	Heap storage problem in RACF agent CEE3204S The system detected a protection exception (System Completion Code=0C4). From entry point _ermFree at compile unit offset +0000008A at entry offset +0000008A at address 2500BF4A.
		Items included in release 7.0.9
RTC 149789		ICN 1469 - UNIX File Directory Usage for N/A N/A
RTC 147988	PMR 30634,082,000	ACID Profiles numbering sequence gets changed on reconciliation
RTC 149790	PMR 14970,082,000	TopSecret support for Z/OS V2.2, R16
		Items included in release 7.0.8
		No items included in this release

Known Issues

INTERNAL#	APAR/CASE#	Description
RTC67316		Earlier releases of the CA Top Secret Adapter do not place a password on the CA Top Secret ACID for ISIM adapter when created. IBM supports the use of a password on this account. Please note that adding a password to the ISIM adapter ACID may result in the console prompting for the password at adapter start up.
	N/A	This release of the CA Top Secret Adapter does not support FIPS.
	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	When changing profile assignments in IGI, the IGI server will send two requests to the adapter. One for the rights value or permission that was deleted and one for the rights value or permission that was added.
	N/A	This release does not support two-way SSL connections

Installation and Configuration Notes

Upgrading to Version 7.1.13 (or later)

Upgrading to V7.1.14 requires a full installation. Refer to the Installing and configuring section of the CA Top Secret adapter guide for detailed instructions.
V7.1.12 and higher require the installation of a complex attribute handler.

Configuration

ADK version 6.04 and higher offer a DAML PROTOCOL setting that allows you to disable TLSv1.0. ADK version 6.0.3 and higher no longer support SSLV3 and RC4 ciphers. The ISIM server should be configured to use TLS 1.1 or higher. This is done by adding the $ITIM/data/enRole.properties parameter. For example:

com.ibm.daml.jndi.DAMLContext.SSL_PROTOCOL=TLSv1.1

Possible values are:

TLSv1.1	TLS v1.1 protocol (defined by RFC 4346).
TLSv1.2	TLS v1.2 protocol (defined by RFC 5246).

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.
Starting ADK release 6.0.3 the adapter will write a message to SYSLOG and shutdown if it can not connect to the IP communications port. In previous releases the adapter would write an error to the adapter log and remain active without an indication that it could not communicate with the server in the SYSLOG.

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. The CA Top Secret adapter has REXX scripting options. Please see the CA Top Secret Installation and Configuration guide for additional details.

IBM Security Identity Manager Resources:

Check the “Learn” section of the IBM Security Identity Manager Knowledge Center 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 customization, 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.

Installing the adapter language pack

See the IBM Security Identity Manager Install library and search for information about installing the adapter language pack.

IBM Security Identity Manager Resources:

Check the “Training” section of the IBM Security Identity Manager Support Portal for links to training, publications, and demos.

IBM Security Identity Governance and Intelligence Resources:

Check the “Training” section of the IBM Security Identity Governance and Intelligence Portal for links to training, publications, and demos.

Updates to the CA Top Secret for z/OS Adapter installation and Configuration Guide

Overview

No updates in the current release

Planning

No updates in the current release

Installing

Communication Configuration

Configuring Complex Attribute Handler for Access Request

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package. For the CA Top Secret® Adapter, profiles are implemented as a complex attribute

About this task

The complex attribute handler enables IBM® Security Identity administrators to define accesses on service groups that require additional values when assigned to an account. The access will be defined on the group name only, and the complex attribute handler will internally supply the default values that are needed for the composition value sent to the adapter.

For Top Secret profiles these values are:

Table 1. Top Secret profile attribute and values

Profile attribute	Default value
SEQUENCE	010

For more information about Access Types, see "Configuring- Access Type Management" in the *IBM Security Identity Manager Server Guide*.
To modify any of the individual values within the composition, the account modify must be used.

The complex attribute handler JAR file is TopSecretComplexAttributeHandler.jar.

Installing the handler on ISIM 6.0 Fix Pack 11 or higher:

Procedure

1. Copy the complex attribute handler JAR file from the adapter package to ITIM_HOME/lib on the WebSphere® Application Server.
2. Add the complex attribute handler jar file to the WebSphere Application Server shared libraries.
   a. Start the WebSphere Application Server Administrative Console.
   b. Select Environment > Shared libraries > ITIM_LIB.
   c. Add ${ITIM_HOME}/lib/TopSecretComplexAttributeHandler.jar under the class path as follows:

      ${ITIM_HOME}/lib/TopSecretComplexAttributeHandler.jar
      ${ITIM_HOME}/lib/itim_util.jar

- Restart the WebSphere Application Server.

Installing the handler on ISIM 7.0.1-ISS-SIM-FIP0001 or higher:

Procedure

1. From the top-level menu of the Appliance Dashboard, navigate to Configure > Advanced Configuration > External Library to display the External Library page.
2. Click New to open the Add External Library window.
3. Click Browse to provide the location of the TopSecretComplexAttributeHandler.jar file and upload the library file.
4. Click Save Configuration to complete this task.
5. From Server Control Menu, select Security Identity Manager Server and restart.

Upgrading

No updates in the current release

Configuring

Configuring the adapter parameters

Changing protocol configuration settings

Step 4

Type A to display the Protocol Properties Menu for the configured protocol with protocol properties. The following screen is an example of the DAML protocol properties.

```
          DAML Protocol Properties
         ----------------------------------

         A.  USERNAME             ***** ;Authorized user name.
         B.  PASSWORD             ***** ;Authorized user password.
         C.  MAX_CONNECTIONS      100   ;Max Connections.
         D.  PORTNUMBER           45580  ;Protocol Server port number.
         E.  USE_SSL              TRUE ;Use SSL secure connection
         F.  SRV_NODENAME         ----- ;Event Notif. Server name.
         G.  SRV_PORTNUMBER       9443  ;Event Notif. Server port  number.
         H.  HOSTADDR             ANY   ;Listen on address ( or "ANY" )
         I.  VALIDATE_CLIENT_CE   FALSE ;Require client certificate.
         J.  REQUIRE_CERT_REG     FALSE ;Require registered certificate.
         K.  READ_TIMEOUT         0     ;Socket read timeout (seconds)
         L.  DISABLE_TLS10        TRUE ;Disable TLS 1.0 and earlier

X.  Done
```

Step 5

Change the protocol value:

a. Type the letter of the menu option for the protocol property to configure. Table 1 describes each property.
b. Change the property value and press Enter to display the Protocol Properties Menu with the new value.

   If you do not want to change the value, press Enter.

Table 1. Options for the DAML protocol menu

Option	Configuration task
A	Displays the following prompt: Modify Property 'USERNAME': Type a user ID, for example, admin. The IBM Security Identity server uses this value to connect to the adapter.
B	Displays the following prompt Modify Property 'PASSWORD': Type a password, for example, admin. The IBM Security Identity server uses this value to connect to the adapter.
C	Displays the following prompt: Modify Property 'MAX_CONNECTIONS': Enter the maximum number of concurrent open connections that the adapter supports. The default value is 100. Note This setting is sufficient and does not require adjustment.
D	Displays the following prompt: Modify Property 'PORTNUMBER': Type a different port number. The IBM Security Identity server uses the port number to connect to the adapter. The default port number is 45580.
E	Displays the following prompt: Modify Property 'USE_SSL': Type TRUE to use a secure SSL connection to connect the adapter. When you set this option, you must install a certificate. For more information, see Installing the certificate from file. Type FALSE to not use a secure SSL connection. The default value is TRUE.
F	Displays the following prompt:

Option	Configuration task
	Modify Property 'SRV_NODENAME': Type a server name or an IP address of the workstation where you installed the IBM Security Identity server. This value is the DNS name or the IP address of the IBM Security Identity server that is used for event notification and asynchronous request processing. Note If your operating system supports Internet Protocol version 6 (IPv6) connections, you can specify an IPv6 server.
G	Displays the following prompt: Modify Property 'SRV_PORTNUMBER': Type a different port number to access the IBM Security Identity server. The adapter uses this port number to connect to the IBM Security Identity server. The default port number is 9443.
H	The HOSTADDR option is useful when the system, where the adapter is running, has more than one network adapter. You can select which IP address to which the adapter must listen. The default value is **ANY**.
I	Displays the following prompt: Modify Property 'VALIDATE_CLIENT_CE': Type TRUE for the IBM Security Identity server to send a certificate when it communicates with the adapter. When you set this option, you must configure options D through I. Type FALSE for the IBM Security Identity server can communicate with the adapter without a certificate. Note • The property name is VALIDATE_CLIENT_CERT. It is truncated by the agentCfg to fit in the screen. • You must use certTool to install the appropriate CA certificates and optionally register the IBM Security Identity server certificate.
J	Displays the following prompt: Modify Property 'REQUIRE_CERT_REG': This value applies when option I is set to TRUE.

Option	Configuration task
	Type TRUE to register the adapter with the client certificate from the IBM Security Identity server before it accepts an SSL connection. Type FALSE to verify the client certificate against the list of CA certificates. The default value is FALSE. For more information about certificates, see Configuring SSL authentication.
K	Displays the following prompt: Modify Property 'READ_TIMEOUT': Specify the timeout value in seconds. The default value is 0 which specifies that no read timeout is set. Note READ_TIMEOUT prevents open threads in the adapter, which might cause "hang" problems. The open threads might be caused by firewall or network connection problems and might be seen as TCP/IP ClosWait connections that remain on the adapter. Note If you encounter such problems, set the value of READ_TIMEOUT to a time longer than the IBM Security Identity Manager timeout, but less than any firewall timeout. The IBM Security Identity Manager timeout is specified by the maximum connection age DAML property. The adapter must be restarted because READ_TIMEOUT is set at adapter initialization.
L	Displays the following prompt: Modify Property 'DISABLE_TLS10': Type FALSE to use the TLSv1.0 protocol to connect the adapter. The default value is TRUE.

- Repeat step 5 to configure the other protocol properties.
- At the Protocol Properties Menu, type X to exit.
-

Configuring required attributes in IBM Security Governance and Intelligence

In “Access Governance Core, Manage, Accounts “ select the account for the Top Secret adapter. Now select “Target Attributes, Actions, Discover Account attributes from Target”.
Select all attributes that are required for creating a new Top Secret account. This should include:

- at least one of the following attributes: ZONE, DIVISION or DEPARTMENT
- the TYPE attribute
- the NAME attribute

Troubleshooting

LDAP: error code 92		Increase the size of the transaction log. See https://www.ibm.com/support/knowledgecenter/en/SSVJJU_6.4.0/com.ibm.IBMDS.doc_6.4/c_tg_tuning_db2_transact_log_size.html for more details.
*BPXI040I PROCESS LIMIT MAXPROCUSER HAS REACHED XX % OF ITS CURRENT CAPACITY OF XX FOR PID=XXX IN JOB ISIAGNT		Increase the amount of processes available to the adapterid

Troubleshooting profile issues.

If you experience issues opening an account form after upgrading to the latest release , it might be required to start the design forms editor, open the Top Secret account form and select save. It is not required to make any changes to the form.

Installing test fixes and diagnostic builds

It is possible IBM will provide a test fix or diagnostic build if you have a case to report an issue you have encountered while working with the adapter.
These fixes can consist of either an <ADAPTER>.UPLOAD.XMI file or a zip file containing a new adapter or adk binary.
XMI files require a full new install. These are usually provided when several components have changed compared to the release you currently had installed. To ensure there are no inconsistencies between the versions of the components you have installed and the updated components that were used to created the fix, you must perform the full installation from scratch using the XMI that contains the fix.

You will receive a zip file that contains one or more binaries if the changes that the fix requires are limited to the adapter or ADK code. These new binaries should be used to replace the binaries that have the same name in your existing adapter installation.

To install a new agent binary perform the following steps:
1. extract the binary from the zip file
2. stop the adapter
3. cd to the read_only_home/bin folder
4. cp -p <adaptertype>Agent <adaptertype>Agent.save
5. upload <adapterype>Agent in binary ftp mode to the adapter host and store it in the read_only_home/bin folder
6. cd to the read_only_home/bin folder
7. chmod 755 <adaptertype>Agent

8. extattr +ap <adaptertype>Agent
9. start the adapter

The steps to install a new ADK binary are identical to the steps to install a new agent binary.
The steps to install a new ADK library are also identical to the steps to install a new agent binary with the exception of the location where the libraries are stored. The libraries can be found in and uploaded to the read_only_home/lib folder.

Uninstalling

No updates in the current release

Reference

No updates in the current release

Troubleshooting of the CA Top Secret Adapter errors

Troubleshooting profile issues.

If you experience issues opening an account form after upgrading to the latest release , it might be required to start the design forms editor, open the Top Secret account form and select save. It is not required to make any changes to the form.

Supported Configurations

Installation Platform

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

Operating System:
z/OS V2.x

Managed Resource:
CA Top Secret for z/OS R16

IBM Security Identity Manager:
Identity Manager v6.0.0-ISS-SIM-FP0011 or higher
Identity Manager v7.0.1-ISS-SIM-FP0001 or higher.

IBM Security Identity Governance and Intelligence:
Identity Governance v5.2.3.1-ISS-IGI-IF0003 or higher

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.

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.

IT Infrastructure Library® is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

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

End of Release Notes