IBM Security Identity Manager
Version 6.0

RACF Adapter Installation and Configuration Guide

SC27-4407-00

IBM Security Identity Manager
Version 6.0

RACF Adapter Installation and Configuration Guide

SC27-4407-00

Note

Before using this information and the product it supports, read the information in Appendix G, "Notices," on page 123.

Edition notice

Note: This edition applies to version 6.0 of IBM Security Identity Manager (product number 5724-C34) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Preface

About this publication

This installation guide provides the basic information that you need to install and configure the IBM® Security Identity ManagerRACF® Security for z/OS® Adapter (RACF Adapter).

IBM Security Identity Manager was previously known as Tivoli® Identity Manager.

The RACF Adapter enables connectivity between the IBM Security Identity Manager server and a network of systems that run the Multiple Virtual Storage (MVS™) operating system. After the adapter is installed and configured, IBM Security Identity Manager manages access to z/OS operating system resources.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Identity Manager library."
- Links to "Online publications."
- A link to the "IBM Terminology website."

IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation see the IBM Security Identity Manager Information Center.

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm site displays the information center welcome page for this product.

IBM Security Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp site displays an alphabetical list of and general information about all IBM Security product documentation.

IBM Publications Center
The http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Appendix E, "Support information," on page 117 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Chapter 1. RACF Security for z/OS Adapter

The RACF Adapter establishes connectivity between the IBM Security Identity Manager server and a system running the RACF Adapter.

Overview of the RACF Adapter

An adapter is a program that provides an interface between a managed resource and the IBM Security Identity Manager server.

Adapters might be installed on the managed resource. The IBM Security Identity Manager server manages access to the resource by using the security system. Adapters function as trusted virtual administrators on the target platform. The adapter performs tasks, such as creating login IDs, suspending IDs, and other functions that administrators run manually. The adapter runs as a service, independently of whether you are logged on to IBM Security Identity Manager.

IBM Security Identity Manager works with the RACFSecurity in an MVS environment. The adapter:

- Receives provisioning requests from IBM Security Identity Manager.
- Processes the requests to add, modify, suspend, restore, delete, and reconcile user information from the RACF Security database.
- Converts the Directory Access Markup Language (DAML) requests that are received from IBM Security Identity Manager to corresponding RACF Security for z/OS commands. Enrole Resource Management API (ERMA) libraries are used for the conversions.
- Forwards the commands to a command executor through a series of Advanced Program to Program Communication (APPC) requests. The command executor receives the formatted RACF Security for z/OS command strings and sends the command to the adapter through the Time Sharing Option (TSO).
- Returns the results of the command and includes the success or failure message of a request to IBM Security Identity Manager.

The following figure describes the various components of the adapter.

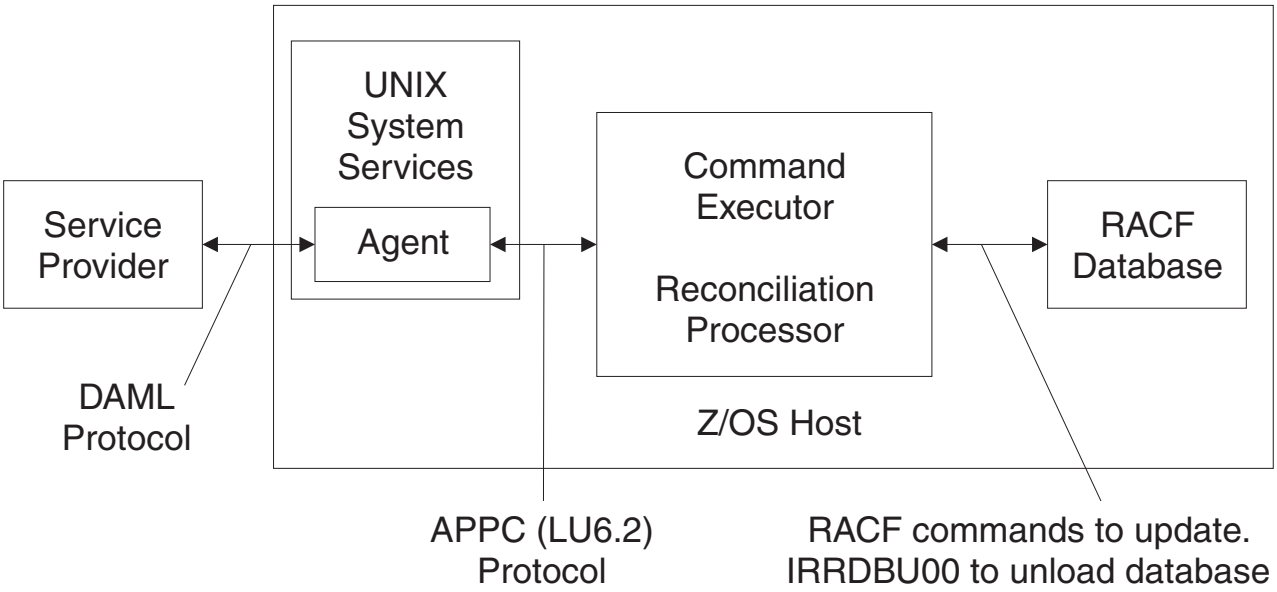


Figure 1. The RACF Adapter components

Adapter
Receives and processes requests from IBM Security Identity Manager. The adapter can handle multiple requests simultaneously. Each request results in execution of an APPC/MVS transaction. The binary files of the adapter and related external files are in the UNIX System Services environment of z/OS (OS/390®).

Command Executor
Operates as an APPC/MVS transaction that is triggered from an incoming request from the adapter. APPC requests consist of commands. The adapter runs these commands with the Command Executor in an APPC/MVS environment.

Reconciliation Processor
Operates as an APPC/MVS transaction that is triggered from an incoming request from the adapter. The request might be accompanied by a RACF user ID. This user ID can be used for a partial reconciliation based on the scope of authority of that ID. See the *RACF Security Administrator's Guide* for a description of scope of authority. Scope of authority is referred to as scoped reconciliation in this guide. The reconciliation processor runs the RACF database unload utility (IRRDBU00), or uses an existing data set that the RACF database unload utility produced. If scoped reconciliation is required, the results of the unload job are then filtered.

When an APPC/MVS transaction fails, there is no cascading failure of the adapter process.

RACF Adapter considerations

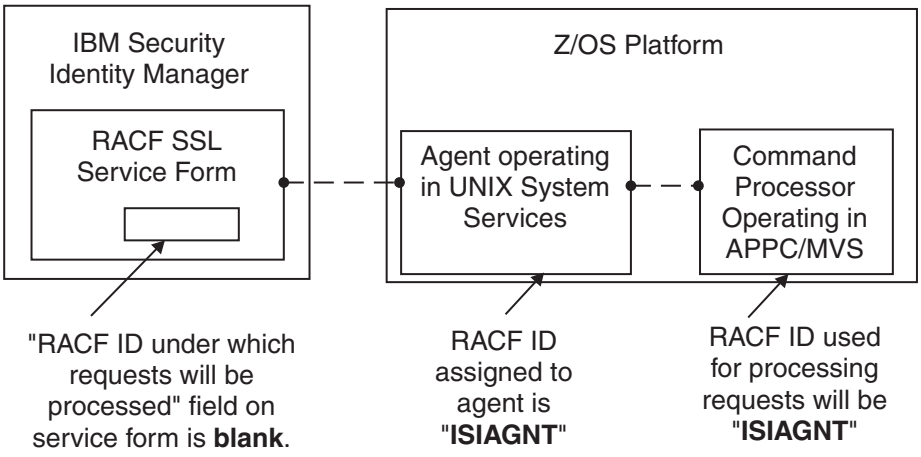
The RACF Adapter does not require APF authorization. However, there are RACF environment issues to consider.

The RACF Adapter operates in two basic modes.

- If no operational RACF ID is specified on the IBM Security Identity Manager service form when a request is issued, the RACF user ID that the adapter uses

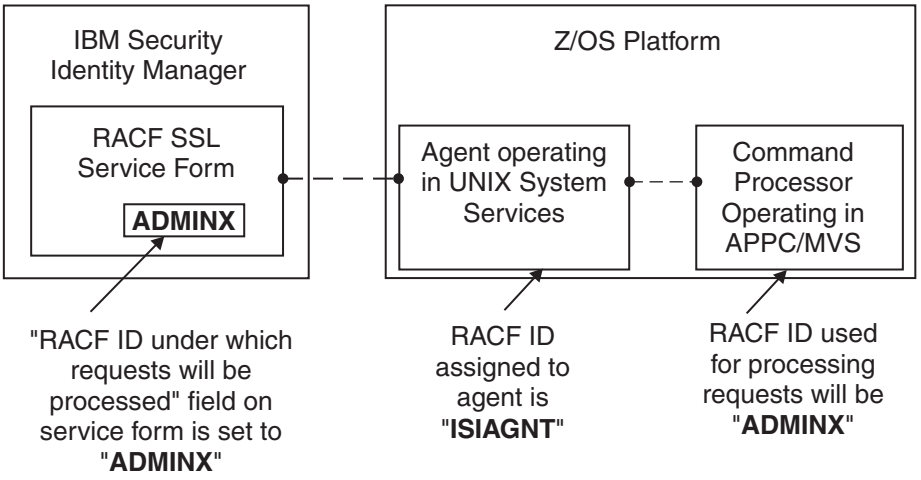
requires specific privileges. For example, if the adapter administers all users in the RACF database, it must operate with the SYSTEM SPECIAL RACF attribute.

If IBM Security Identity Manager performs operations against only a portion of the RACF database, the adapter must be associated with a group assigned GROUP SPECIAL privileges, for the portion of the database it administers. The following figure depicts the preceding scenario.



- If the operations carried out are performed under an RACF ID specified on the IBM Security Identity Manager service form, the RACF ID the adapter uses does not require any special privileged attributes. It does, however, require surrogate authority to run functions under the identity of the RACF ID specified on the IBM Security Identity Manager service form. The RACF ID specified on the IBM Security Identity Manager service form must have authority for the administration functions requested by the IBM Security Identity Manager server.

  The following figure depicts the preceding scenario:



Note: The RACF ID used for processing requests needs update access to the RACF database data set for reconciliation. The RACF ID is the RACF ID specified on the service form. If no RACF ID is specified on the service form, the RACF ID assigned to the agent needs the update access. This access is a requirement of the utility IRRDBU00, that runs as part of the reconciliation process.

The RACF resources that require consideration are:

FIELD class profile USER.segment., with UPDATE**
FIELD class profiles are required when the adapter, or surrogate, does not have the SYSTEM SPECIAL attribute.

FACILITY class profile STGADMIN.IGG.DEFDEL.UALIAS, with READ
The STGADMIN.IGG.DEFDEL.UALIAS might be required if catalog aliases are created in the ISIMEXIT or ISTIMEXEC adapter exit points.

FACILITY class profile IRR.PASSWORD.RESET, with UPDATE
IRR.PASSWORD.RESET is required if the effective RACF ID that changes passwords does not have the SYSTEM SPECIAL RACF attribute.

The STGADMIN.IGG.DEFDEL.UALIAS might be required if catalog aliases are created in the ISIMEXIT or ISIMEXEC adapter exit points.
IRR.PASSWORD.RESET is required if the effective RACF ID that changes passwords does not have the SYSTEM SPECIAL RACF attribute.

SURROGAT class profile ATBALLC.userid, with READ
The surrogate profile is required if the adapter RACF ID differs from the RACF ID under which commands and reconciliations are done.

APPCLU class profile vtamnode.appcname.appcname, with SESSION segment
The APPCLU profile is required.

FACILITY class profile BPX.NEXT.USER, with APPLDATA('uid/')
FACILITY class profile BPX.NEXT.USER, with APPLDATA('uid/')

UNIXPRIV class profile SHARED.IDS, with *xxxx* access
The adapter, or surrogate, requires access to this profile if the IBM Security Identity Manager server is creating RACF IDs with OMVS segments where duplicate UIDs are created.

CLAUTH with class of USER
CLAUTH of USER is required if the adapter, or surrogate, RACF ID creates RACF users, when the creating ID does not have SYSTEM SPECIAL.

Note: Details on the use of these RACF profiles are provided later in this document.

Chapter 2. Planning to install the RACF Adapter

Installing and configuring the adapter involves several steps that you must complete in an appropriate sequence.

Review the roadmaps before you begin the installation process.

Preinstallation roadmap

You must prepare the environment before you can install the adapter.

Table 1. Preinstallation roadmap

Task	For more information
Obtain the installation software.	Download the software from the IBM Passport Advantage® website. See "Downloading the software for the RACF adapter" on page 6.
Verify that your environment meets the software and hardware requirements for the adapter.	See "Prerequisites" on page 6.

Installation roadmap

You must complete the necessary steps to install the adapter, including completing post-installation configuration tasks and verifying the installation.

Table 2. Installation roadmap

Task	For more information
Install and configure the adapter.	See Chapter 3, "Installing and configuring the RACF Adapter," on page 7.
Import the adapter profile.	See "Importing the adapter profile into the IBM Security Identity Manager server" on page 22.
Verify the profile installation.	See "Verifying the adapter profile installation" on page 23.
Create a service.	See "Creating a RACF Adapter service" on page 23.
Configure the adapter.	See "Configuring the adapter for IBM Security Identity Manager" on page 27.
Customize the adapter.	See "Customizing the RACF Adapter" on page 53.

Prerequisites

The following table identifies hardware, software, and authorization prerequisites for installing the adapter. Verify that your environment meets all the prerequisites before installing the adapter.

Table 3. Prerequisites to install the adapter

Operating System	• z/OS version 1.10 • z/OSversion 1.11 • z/OS version 1.12
Network Connectivity	Internet Protocol network
Server Communication	Communication must be tested with a low-level communications ping from the IBM Security Identity Manager server to the MVS Server. When you do so, troubleshooting becomes easier if you encounter installation problems.
IBM Security Identity Manager server	Version 6.0
Required authority	To complete the adapter installation procedure, you must have system administrator authority.

Organizations with multiple RACF databases must have the adapter installed on a z/OS host that manages the database. You can manage a single RACF database with a single instance of the RACF Adapter.

Note: Support for Sysplex failover is not implemented. When the participating image of the Sysplex running the adapter becomes inoperative, you can restart the failed z/OS image, then restart the adapter. You can also pre-configure another instance of the adapter for use on another image. You must already have this type of environment setup and the necessary resources available. The related service instance on the IBM Security Identity Manager server might require updates if the other image is known through a different IP address.

Downloading the software for the RACF adapter

Download the software from your account at the IBM Passport Advantage website.

Go to IBM Passport Advantage.

See the *IBM Security Identity Manager Download Document* for instructions.

Chapter 3. Installing and configuring the RACF Adapter

Install and configure the RACF Adapter to enable the adapter to work in a non-secure environment.

About this task

Installing and configuring the RACF Adapter involves the following tasks:

1. "Uploading the adapter package on z/OS"
2. "Installing the ISPF dialog"
3. "Running the ISPF dialog" on page 8

Note: The screens displayed in these tasks are examples; the actual screens displayed might differ.

Uploading the adapter package on z/OS

Perform the following steps to upload the adapter package on z/OS.

Procedure

1. Obtain the software. See "Downloading the software for the RACF adapter" on page 6.
2. Extract the installation package on your local workstation and ensure that a file named `ISIMRACF.UPLOAD.XMI` exists. The file is in the z/OS Time Sharing Option (TSO) TRANSMIT/RECEIVE format.
3. On the z/OS operating system, use the TSO to allocate a sequential `ISIMRACF.UPLOAD.XMI` file with the following parameters:
   - RECFM=FB
   - LRECL=80
   - 400 MB of space
4. Upload the extracted `ISIMRACF.UPLOAD.XMI` file with a Binary transfer method, such as FTP or 3270 file transfer from the ISPF Command Shell. For example:
   ```
   IND$FILE PUT 'ISIMRACF.UPLOAD.XMI' RECFM(F)
   ```
5. Receive the uploaded file with the TSO `RECEIVE` command:
   ```
   RECEIVE INDA(ISIMRACF.UPLOAD.XMI)
   ```
6. Press **Enter** to create a Partitioned Data Set (PDS) file named, *userid*`.ISIMRACF.UPLOAD`, where, *userid* is your TSO User ID.

Installing the ISPF dialog

Install the ISPF dialog to install and configure the RACF Adapter.

About this task

Procedure

1. Log on to a z/OS operating system.
2. From ISPF 6 option, run the **`INSTALL1`** exec:
   ```
   EXEC 'userid.ISIMRACF.UPLOAD(INSTALL1)'
   ```

where *userid* is your TSO User ID.

3. Specify a high-level qualifier (hlq) for the data sets that the `INSTALL1` exec creates. When you do not specify a high-level qualifier, the exec uses your TSO User ID as the high-level qualifier. Specify another hlq to use the ISPF dialog in the future.

Results

When you run the exec, the exec creates the listed hlq data sets.

Table 4. ISPF dialog data sets

High-level qualifier	Library
hlq.SAGRCENU	CLIST/EXEC library
hlq.SAGRMENU	ISPF message library
hlq.SAGRPENU	ISPF panel library
hlq.SAGRSENU	ISPF skeleton library

Note: The **AGRCCFG** exec allocates the libraries.

Running the ISPF dialog

Run the ISPF dialog to customize the adapter for run time execution. The dialog presents the default values for the parameters, however, you can set your own values.

About this task

The ISPF dialog creates the Job Control Language (JCL) job streams with the installation parameters that you selected. The JCL job streams are required for adapter installation. Before you perform this task, you must install the ISPF dialog.

To run the ISPF dialog, perform the following steps:

1. Log on to TSO on the z/OS operating system.
2. From ISPF 6 option, run the following command to start the ISPF dialog:
   ```
   EXEC 'hlq.SAGRCENU(AGRCCFG)'
   ```
3. When the ISPF dialog starts, ISPF 6 displays this screen.

```
--------------------- ISIM RACF Adapter Customization --------------------
Option ===>                                           Location:  1

Security Identity Manager RACF Adapter

  Initial Customization

    1  Initial Customization
       If this is a new installation, select this option.

    X  Exit
```

Note: As you run the dialog, keep in mind the following considerations:

- You can return to the previous menu at any time by pressing F3 or END on the Menu selection screen.
- If you press F3 on a data entry screen, the values that you entered are not saved.

- When you fill the data entry screen and if it is validated without errors, the software returns to the previous screen.

4. Select **Initial Customization** to display the Initial Customization page that lists the high-level tasks that you must perform.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>                                          Location:  1-> 1

   Initial Installation

     1  Load Default or Saved Variables.
        You must load either the default variables, or your previously
        saved variables prior to defining or altering.

     2  Display / Define / Alter Variables.
        Select or change specifications for this server or node.

     3  Generate Job Streams.
        You must have performed choices 1 and 2 before performing
        this choice.

     4  Save All Variables.
        Save variable changes to an MVS data set.

     5  View instructions for job execution and further tailoring.
        This displays customized instructions, based on your inputs.
```

5. Select **Load Default or Saved Variables** and specify the fully qualified name of the data set that includes previously saved variables. If none exists, leave the fields blank to load the default variables.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>                                          Location:  1->1-> 1

  Load Variables

     The IBM supplied defaults are in IBMUSER.ISIMRACF.SAGRCENU(AGRCDFLT)
     If you remove the name specified below, the defaults will be loaded.

     To load previously saved variables, specify the fully qualified
     data set name without quotes.

     ===>
```

6. Press PF3 (Cancel) or Enter after final input (Accept) to return to the Initial Installation panel.
7. Select **Display / Define / Alter Variables**.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>                                          Location:  1->1-> 2

  Specify or Alter variables for this configuration.

     1     Disk location paramaters.
           Define / alter data set and Unix System Services locations.

     2     Adapter specific parameters.
           Define / alter ISIM server to adapter runtime parameters.

     3     VTAM and APPC/MVS parameters
           Define / alter VTAM and APPC/MVS specifics.

     4     APPC/MVS customization/configuration
           Define and or create APPC/MVS environment.

     5     RACF environment
           Define RACF database(s) for the adapter.

        ** Indicates option has been visited during this session.

  Select an option, or press F3 to return to main menu selection.
```

a. Select **Disk location parameters** to define or alter data set and UNIX System Services locations.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>

   Input Data Sets

    Fully qualified data set name of the UPLOAD data set.
     ===> IBMUSER.ISIMRACF.UPLOAD

  Enter data sets names, volume ID, Storage Class and z/OS Unix directories.

    USS Adapter read-only home
     ===> /usr/lpp/isimracf

    USS Adapter read/write home
     ===> /var/ibm/isimracf

    Storage Class  ===>
      and/or
    Disk Volume ID ===>

    Fully qualified data set name of Adapter Load Library
     ===> IBMUSER.ISIMRACF.LOAD

    Fully qualified data set name of Adapter EXEC Library
     ===> IBMUSER.ISIMRACF.EXEC
```

Fully qualified data set name of the UPLOAD data set
Specifies the name of the data set that you received earlier. For example, IBMUSER.ISIMRACF.UPLOAD.XMI.

Unix System Services Adapter read-only home
Specifies the location where the adapter UNIX System Services binary files are stored. The adapter installer creates the directories and the subordinate directories later.

UNIX System Services Adapter read/write home
Specifies the location where the adapter registry file, certificates, and log files are written. The adapter installer creates the directories and the subordinate directories later.

Note: The read-only home and the read/write home must specify different locations. If they are the same location, the installation might fail.

Storage class
Specifies the storage class for the Load and EXEC libraries.

DASD (Disk) volume ID
Specifies the Disk ID for the Load and EXEC libraries.

Fully qualified data set name of Adapter Load Library and Fully qualified data set name of Adapter EXEC Library
Specify the fully qualified data set name for the Load and EXEC libraries.

b. Press PF3 (Cancel) or Enter after final input (Accept) to return to the Specify or Alter variables for this configuration panel.

c. Select **Adapter specific parameters** to define or alter the IBM Security Identity Manager or adapter run time parameters.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>

 Adapter specific parameters

    Name of adapter instance                      ===> RACFAGENT

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

    IP Communications Port Number                 ===> 45580
 Note: The adapter will always reqire access to ports 44970 through 44994.
       These ports are implicitly reserved.

    Adapter authentication ID (internal)          ===> agent

    Adapter authentication password (internal)    ===> agent

    PDU backlog limit                             ===> 2000

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

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

    RACF user ID for the ISIM adapter             ===> ISIAGNT

    RACF z/OS Unix group for the ISIM adapter     ===> OMVS

    OMVS UID to be assigned to RACF ID            ===> 999

    Scoped reconciliation VSAM data set
    (blank if scoped reconciliation not required) ===> IBMUSER.ISIMRACF.GROUPS
```

Name of adapter instance
Specifies the unique name assigned to the adapter instance. When more than one adapter is active in the same Logical Partition (LPAR), use a different adapter name for each instance.

Name of the Started Task JCL procedure name
Specifies the name of the JCL member that is created. You can use the name of the JCL member as the RACF Login ID for the adapter.

IP Communications Port Number
Specifies the default IP Communications Port Number which is 45580. When more than one adapter is active in the same LPAR, use a different port number for each adapter instance.

Adapter authentication ID and Adapter authentication password
Specifies the adapter authentication ID and password that are stored in the adapter registry. The ID and password are used to authenticate the IBM Security Identity Manager server to the RACF Adapter. These two parameters must also be specified on the adapter service form that is created on IBM Security Identity Manager.

PDU backlog limit
Specifies the number of entries that can be in queue for sending to the IBM Security Identity Manager server. The higher the number, the greater the throughput on reconciliations; however, this also results in higher storage utilization.

Do you want passwords set as expired
Specifies whether the passwords must be set as expired or non-expired. The default value is set to TRUE; however, you might change it to FALSE if you want all the passwords set as non-expired.

When you specify `TRUEADD`, you can add a user with an expired password, however, when the same user is modified, the password is set as non-expired.

Do you use SYS1.BRODCAST in the environment
Specifies whether your TSO environment uses the SYS1.BRODCAST data set for TSO logon messages and notifications. The default value is TRUE.

RACF user ID for ISIM adapter
Specifies the RACF user ID that the adapter task is assigned to.

RACF z/OS UNIX group for the ISIM adapter
Specifies a 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.

OMVS UID to be assigned to RACF ID
Specifies a unique UID number for the RACF ID.

Scoped reconciliation VSAM data set (blank if scoped reconciliation is not required)
Specifies the VSAM data set name required for the scoped reconciliation process. The APPC reconciliation transaction uses the VSAM data set. If you do not want to perform the scoped reconciliation, do not specify the VSAM data set name. The RACF ID specified on the service form or the default RACF ID configured for the adapter must have UPDATE access to the Scoped reconciliation VSAM data set.

Note: You must check the VSAM data set size after the reconciliation process. If no scoped reconciliation VSAM data set is defined during the installation process, then the attribute `SCOPING=FALSE` is set in the registry. If scoped reconciliation is required in the future, then you must use the installation panels to generate J6 and J8, and these jobs must be submitted. Finally, you must set the attribute `SCOPING=TRUE`with the agentCfg tool.

d. Press PF3 (Cancel) or Enter after final input (Accept) to return to the Specify or Alter variables for this configuration panel.

e. Select **VTAM and APPC/MVS parameters** to define VTAM® and APPC/MVS specifications.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>

 VTAM and APPC/MVS Parameters

    VTAM NETID                          ===> NET1

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

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

    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       ===> ISIMCMD

    APPC reconciliation transaction     ===> ISIMRECO

    APPC execution class                ===> ISIM

    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.
```

VTAM NETID

Obtain the VTAM NETID from the MVS console by running the following command:

```
"D NET,E,ID=ISTNOP"
```

The result with the message ID `IST075I` indicates *`netid`*`.ISTNOP`, where *`netid`* is the Network ID required for the adapter configuration.

VTAM Originating Logical Unit and VTAM Destination Logical Unit

When the Originating and Destination Logical Unit (LU) have the same name, a single LU-name is defined to APPC/MVS as the BASE LU. When the Originating and Destination Logical Units (LUs) have different names, the Destination LU must be the BASE LU and the Originating LU must be different from the BASE LU-name. This requirement is an APPC/MVS restriction.

VTAM Session Key

The VTAM session key is an 8 byte shared secret key. If one APPCLU profile is created, the session key is not required. If two APPCLU profiles are created, and a session key is specified, then the session keys must match.

Note: In the RACF environment, specify session keys that are of 16 hexadecimal characters (0-9, A-F).

VTAM LOGMODE entry name

The standard VTAM LOGMODE entry name is `#INTERSC`. This name is standard in the VTAM default mode table, ISTINCLM.

Fully qualified data set name of your APPC/MVS transaction data set
Specify the name of an existing or a new APPC/MVS transaction profile data set name. This data set is a VSAM file.

APPC command transaction name and APPC reconciliation transaction
Specify APPC/MVS transaction names for the adapter APPC transactions (APPC command transaction and APPC reconciliation transaction). The following table lists the default APPC transaction names.

Table 5. APPC transaction names

Transaction	Default transaction name
APPC command transaction	ISIMCMD
APPC reconciliation transaction	ISIMRECO

APPC execution class
The APPC execution class is a 1 - 8 character class name. This name is an Address Space Scheduler (ASCH, a part of APPC/MVS) class name defined or to be defined in ASCHPMxx.

APPC Network Qualified Names
The APPC/MVS network qualified names specify how the RACF APPCLU profiles must be defined. The specification in APPCPMxx for the LUs to be configured indicates whether the LU is enabled to use a network-qualified Partner LU-name. For NQN (fully qualified network names) specify `TRUE`, and for NONQN (non-fully qualified network names), specify `FALSE`.

Note: The default value in APPCPMxx is NONQN.

f. Press PF3 (Cancel) or Enter after final input (Accept) to return to the Specify or Alter variables for this configuration panel.

g. Select **APPC/MVS customization/configuration** to define or create the APPC/MVS environment.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>

 APPC/MVS customization/configuration

  If the following field is FALSE, the remaining fields are required.

    Is APPC currently configured?                ===> TRUE      (True or False)

    RACF user ID for APPC/MVS                    ===> APPC

    RACF user ID for ASCH component of APPC/MVS  ===> ASCH

    RACF group ID to assign to the above 2 users ===> STCGROUP
    SMS STORCLAS for APPCTP data set             ===>
     and/or
    Disk Volume ID for APPCTP data set           ===>
```

Case 1: If APPC/MVS is already configured, then ignore the other fields.

Case 2: If APPC/MVS is not configured, then specify values for the remaining parameters that are displayed on the screen.

- Specify the APPC/MVS and ASCH login IDs. The tailored job streams create the login IDs.
- Specify the SMS Storage class or the disk volume, or both to create a location for the APPC/MVS transaction profile data set.

8. Press PF3 (Cancel) or Enter after final input (Accept to return to the Specify or Alter variables for this configuration panel.
9. Select **RACF Environment** to access the RACF databases that the adapter uses.

```
---------------------- ISIM RACF Adapter Customization ----------------------
Option ===>

RACF Environment

   Is the adapter to run database unload?       ===> TRUE      (True or False)

   Existing IRRDBU00 Input data set or GDG (Must be cataloged)
    ===>

   RACF data base(s) (at least ONE)
    ===> SYS1.TVT5092.RACF
    ===>
    ===>
    ===>
    ===>
    ===>
```

The adapter must know the names of the data sets that have the RACF database. If you specify TRUE for the adapter to run the database unload, then the reconciliation process runs the IRRDBU00 (RACF database unload) utility. In this case, you must verify the RACF data sets or overwrite them according to your installation specifications. However, if you do not want the adapter to run the database unload and you specify FALSE, then you must specify a data set or Generation Data Group (GDG).

10. Press PF3 (Cancel) or Enter after final input (Accept to return to the Specify or Alter variables for this configuration panel.
11. Press PF3 to return to the Initial Installation panel.
12. Select **Generate Job Streams**
13. This screen displays the default data set names that are generated to store the job streams and data. You might change the default names on this screen as per requirements of your organization. These data sets are not used at the adapter run time.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>

  Generate the job streams

     Specify two fully qualified data set names. These data sets will be
     populated with the job streams and their input data elements.
     Specify the data set names, without quotes. If these data sets do not
     exist, they will be created.

     Data set name for job streams to be stored.
     ===> IBMUSER.ISIMRACF.CNTL

     Data set name for data elements required by generated job streams.
     ===> IBMUSER.ISIMRACF.DATA

   Enter your installation job statement parameters here:

  => //JOBNAME  JOB (ACCTNO,ROOM),'&SYSUID',CLASS=A,MSGCLASS=X,
  => // NOTIFY=&SYSUID
  => //*
```

Specify valid parameters for installation JCL JOB statement and press Enter to create job streams (members) and data members. Control returns to the Initial Installation panel.

14. Select **Save All Variables** to save all the changes that you made to the data set. You can use the same data set when you select **Load Default or Saved Variables**. Specify a data set name to save all your settings for the adapter configuration as described in this screen.

```
------------------- ISIM RACF Adapter Customization -------------------
 Option ===>

  Save variables to a data set.

     Specify the data set where the variables specified in this session are
     to be saved.  Specify a fully qualified data set name, without quotes.
     If the data set does not exist, a sequential data set will be created.

     ===> IBMUSER.ISIMRACF.CONFIG
```

15. Select **View instructions for job execution and further tailoring**. To view the adapter settings and instructions to run the generated job streams, see the *hlq*.ISIMRACF.CNTL(INSTRUCT) data set. Follow the instructions specified in the *hlq*.ISIMRACF.CNTL(INSTRUCT) data set to complete the configuration.

After completing the steps for running the ISPF dialog, the adapter is configured in a non-secure mode. To configure the adapter in a secure mode, you must perform additional steps. For example, enabling the Secure Socket Layer (SSL), creating and importing the certificate in the adapter registry. For more information, see .

Starting and stopping the adapter

You might need to stop the adapter and restart it after changing its configuration.

Before you begin

Before you start the adapter, ensure that the following requisites are satisfied:

- TCP/IP is active
- APPC/MVS address space is active
- ASCH address space is active

About this task

Start the adapter as a started task, where the started task JCL is customized and installed in a system procedure library. To start the adapter, run the following MVS console start command:

START *ISIAGNT*

where *ISIAGNT* is the name of the JCL procedure that represents the adapter.

The ISIAGNT task listens on two IP ports. These two ports are used for:

- Communication between the IBM Security Identity Manager server and the adapter
- agentCfg utility

Note: You can define _BPX_SHAREAS=YES in the /etc/profile. This setting enables the adapter to run in a single address space, instead of multiple address spaces. Newer

releases of z/OS create two address spaces with this environment variable set. See "z/OS Unix System Services considerations" on page 22 for more information.

To stop the adapter, perform one of the following steps:

- If the UNIX System Services environment is running with _BPX_SHAREAS=YES, then run the following MVS stop command to stop the adapter:

  STOP *ISIAGNT*

  or

  P *ISIAGNT*
- In the new releases of z/OS, if the UNIX System Services environment is running with the _BPX_SHAREAS=YES setting, an additional address space is created. In this case, run the following command to stop the adapter:

  P *ISIAGNT1*
- If an MVS STOP command does not stop the adapter, run the following MVS CANCEL command to stop the adapter:

  CANCEL *ISIAGNT*

Configuring RACF access

Determine your needs and configure how the adapter accesses RACF information.

The installation process configures most of the definitions that are necessary for the adapter to function. For more information, see the job streams that are generated during the installation process.

RACF user ID

The adapter must run under a valid RACF user ID, with an OMVS segment, and a valid UID. This user default group must have an OMVS segment with a valid GID. The adapter must be able to acquire sufficient storage for operation, by using the OMVS segment ASSIZEMAX parameter

Unless surrogate user IDs are being used, the adapter must at least be connected GROUP SPECIAL over a group of users that are to be managed. If the adapter has GROUP SPECIAL, it requires CLASS AUTHORITY of USER to be able to create and remove user IDs from the system (CLAUTH(USER)). This user ID must be defined as **RACF 'PROTECTED'**. Use the NOPASSWORD operand on the ADDUSER (or ALTUSER) command to define this user ID as **RACF 'PROTECTED'**.

Note: The RACF Adapter installer creates the RACF Adapter RACF profile with the SPECIAL attribute. The AUDITOR attribute is not required for operation. However, transactions that set or unset the UAUDIT attribute might generate warnings. To avoid these warnings, remove the UAUDIT attribute from the RACF form on the IBM Security Identity Manager server user interface customization.

In the following commands, the use of SYS1 as owner and DFLTGRP might be changed to a different group of your choosing. If the RACF Adapter is to manage all accounts on this RACF database, then the following definition defines this user:

```
ADDUSER ISIAGNT OWNER(SYS1) DFLTGRP(SYS1) SPECIAL AUDITOR NOPASSWORD

ALTUSER ISIAGNT OMVS(UID(uu) PROG('/bin/sh') HOME('/var/ibm/isimracf')
ASSIZEMAX(2147483647))
```

If the started task JCL is called ISIAGNT, then the following STARTED class profile must be defined:

```
RDEFINE STARTED ISIAGNT.* STDATA(USER(ISIAGNT) GROUP(SYS1) TRACE(YES))
SETROPTS RACLIST(STARTED) REFRESH
```

The "TRACE(YES)" operand indicates to RACF that a message is displayed upon the console, indicating that this STARTED class profile was used in starting this adapter.

Example

In the following example, IBM Security Identity Manager adapter has RACF scope of authority over group *xxxx*. This example defines the IBM Security Identity Manager adapter as a GROUP SPECIAL user.

```
ADDUSER ISIAGNT DFLTGRP(xxxx) OWNER(xxxx) CLAUTH(USER) NOPASSWORD
CONNECT ISIAGNT GROUP(xxxx) SPECIAL AUDITOR
RDEFINE STARTED ISIAGNT.* STDATA(USER(ISIAGNT) GROUP(xxxx) TRACE(YES))
SETROPTS RACLIST(STARTED) REFRESH
```

Additionally, if the GROUP SPECIAL attribute is used, then the adapter might require the ability to manage non-RACF segment information. The adapter, or surrogate, user IDs, must have access to the appropriate FIELD class profiles to manage these segments.

If the adapter RACF user ID is allowed to manage all non-RACF segments, then you might define a FIELD class profile as follows:

```
RDEFINE FIELD USER.*.** UACC(NONE)
PE USER.*.** AC(ALTER) ID(ISIAGNT) CLASS(FIELD)
SETROPTS RACLIST(FIELD) REFRESH
```

If the adapter user ID has SYSTEM SPECIAL, it is assumed the adapter is managing the entire RACF database. If so, there is no issue with the FIELD class profiles, or CLAUTH(USER).

You might need to create a RACF STARTED class profile, allowing the adapter started task to run under this specific user ID. An example of this definition is as follows:

```
RDEFINE STARTED ISIAGNT.* STDATA(USER(ISIAGNT) TRACE(YES))
SETROPTS RACLIST(STARTED) REFRESH
```

User ID propagation

The adapter that is running in z/OS UNIX System Services must be able to propagate the RACF ID it is running as, to the APPC/MVS environment.

This task is accomplished by defining one or more entries in the APPCLU record. You can configure the definitions in either of two ways.

By using single APPC/MVS base logical unit

By default, the APPC/MVS **baselu** is utilized by the RACF Adapter, both for the originating and destination logical units. If this method is utilized, only one link in the APPCLU record must be defined. The form of the RACF command to define the link can take two forms.

- If the APPC/MVS LUADD statement takes the default, or specified NONQN, then this command takes the following form:

```
RDEFINE APPCLU netid.baselu.baselu SESSION(CONVSEC(ALREADYV)
SESSKEY(xxxxxxxx))
```

- If the APPC/MVS LUADD statement specified NQN, then this command takes the following form:

  ```
  RDEFINE APPCLU netid.baselu.netid.baselu SESSION(CONVSEC(ALREADYV)
  SESSKEY(xxxxxxxx))
  ```

  In the preceding examples, **netid** is the VTAM NETID (Network ID) selected for use for VTAM in your environment. The **baselu** specifies the VTAM logical unit name for the BASELU defined to APPC/MVS. The xxxxxxxx in the SESSKEY field is a session key, or password, used for security when the APPC/MVS sessions are initiated.

  After this profile is defined, an MVS console command must be issued to VTAM to inform VTAM that this profile is being defined or updated.

  ```
  F VTAM,PROFILES,ID=baselu
  ```

  For example, the RACF APPCLU profile is defined as follows, if your installation has the following conditions:

  – VTAM NETID is set to MYNET.

  – Your APPC/MVS BASELU is configured as MVSLU01.

  – NONQN is specified or defaulted.

  ```
  RDEFINE APPCLU MYNET.MVSLU01.MVSLU01 SESSION(CONVSEC(ALREADYV)
  SESSKEY(xxxxxxxx))
  ```

  Using the preceding example values, where the LUADD statement specified NQN, the RACF APPCLU profile is defined as follows:

  ```
  RDEFINE APPCLU MYNET.MVSLU01.MYNET.MVSLU01 SESSION(CONVSEC(ALREADYV)
  SESSKEY(xxxxxxxx))
  ```

By using two APPC/MVS logical units

Your installation might use two separate logical units, and not use the APPC/MVS BASELU definition. If this method is used, two links in the APPCLU record must be defined. The RACF commands to define these links can take two forms:

- If the APPC/MVS LUADD statements are defaulted or specified NONQN, then the commands take the following form. (This example implies that NONQN is used for *both* logical units.)

  ```
  RDEFINE APPCLU netid.origin.dest SESSION(CONVSEC(ALREADYV)
  SESSKEY(xxxxxxxx))

  RDEFINE APPCLU netid.dest.origin SESSION(CONVSEC(ALREADYV)
  SESSKEY(xxxxxxxx))
  ```

- If the APPC/MVS LUADD statements specified NQN, then these commands take the following form. (This example implies that NQN is specified for *both* logical units.)

  ```
  RDEFINE APPCLU netid.origin.netid.dest SESSION(CONVSEC(ALREADYV)
  SESSKEY(xxxxxxxx))
  RDEFINE APPCLU netid.dest.netid.origin SESSION(CONVSEC(ALREADYV)
  SESSKEY(xxxxxxxx))
  ```

After these links are defined, two MVS console commands must be issued to inform VTAM of the update:

```
F VTAM,PROFILES,ID=origin
F VTAM,PROFILES,ID=dest
```

In the preceding examples, **netid** is the VTAM Network ID (NETID) selected for use for VTAM in your environment. The **origin** and **dest** specify the VTAM logical

unit names used as the originating and destination logical units defined to APPC/MVS. The xxxxxxxx in the SESSKEY field is a session key, or password, utilized for security when the APPC/MVS sessions are initiated.

For example, the RACF APPCLU profiles are defined as follows, if your installation has the following conditions:

- VTAM NETID is set to MYNET.
- Your APPC/MVS origin logical unit is named ISIMORIG.
- The dest logical unit is named ISIMDEST.
- NONQN is specified or defaulted.

```
RDEFINE APPCLU MYNET.ISIMORIG.ISIMDEST SESSION(CONVSEC(ALREADYV)
SESSKEY(xxxxxxxx))
RDEFINE APPCLU MYNET.ISIMDEST.ISIMORIG SESSION(CONVSEC(ALREADYV)
SESSKEY(xxxxxxxx))
```

Using the preceding example values, where the LUADD statements specified NQN, the RACF APPCLU profiles is defined as follows:

```
RDEFINE APPCLU MYNET.ISIMORIG.MYNET.ISIMDEST SESSION(CONVSEC(ALREADYV)
SESSKEY(xxxxxxxx))
RDEFINE APPCLU MYNET.ISIMDEST.MYNET.ISIMORIG SESSION(CONVSEC(ALREADYV)
SESSKEY(xxxxxxxx))
```

Surrogate user ID

A surrogate user is a user who has the authority to perform tasks on behalf of another user, by using the other user's level of authority.

Surrogate user IDs are necessary only if:

- The installation uses 'business unit support'.
- A single instance of the adapter supports a single RACF database.
- The IBM Security Identity Manager has multiple service instances, each representing a different business unit within the organization.

Note: If a single IBM Security Identity Manager service instance supports all theRACF IDs in the RACF database, surrogate user IDs are not needed.

For the adapter to run requests by using these surrogate user IDs, you must define one or more **RACF SURROGAT** class profiles.

If the adapter RACF user ID is ISIAGNT, and the surrogate RACF user ID is UNIT1, then the following commands defines the profile.

```
RDEFINE SURROGAT ATBALLC.UNIT1 UACC(NONE)
PERMIT ATBALLC.UNIT1 CLASS(SURROGAT) AC(READ) ID(ISIAGNT)
SETROPTS RACLIST(SURROGAT) REFRESH
```

In the preceding example, the RACF user ID UNIT1 is the user ID defined in the adapter service form. See “Creating a RACF Adapter service” on page 23. This RACF user has scope of authority over a specific business unit.

When surrogate user IDs are used, the tasks of altering and fetching RACF data is accomplished under the authority of the surrogate RACF user ID. The authority of the RACF user ID that the adapter is running as is not used. The RACF user ID for the adapter must have **read** access to use the SURROGAT class profile.

Authorization to set and reset passwords

When the adapter RACF user ID, or the surrogates do not have **SYSTEM SPECIAL**, they must be able to set passwords over those users they manage. This task is accomplished through the **FACILITY** class profile named IRR.PASSWORD.RESET.

The default for the **PASSEXPIRE** option is TRUE. All passwords set from the IBM Security Identity Manager server are EXPIRED passwords. The user must change the password upon first use. In this instance, the adapter or surrogates need only READ access to the IRR.PASSWORD.RESET profile.

```
RDEFINE FACILITY IRR.PASSWORD.RESET UACC(NONE)
PERMIT IRR.PASSWORD.RESET CLASS(FACILITY) AC(READ) ID(ISIAGNT)
SETROPTS RACLIST(FACILITY) REFRESH
```

If the adapter option **PASSEXPIRE** is set to FALSE, the IBM Security Identity Manager adapter sets only non-expired passwords. In this instance, the adapter (or surrogates) might require UPDATE access to the IRR.PASSWORD.RESET profile, if these users do not have **RACF SYSTEM SPECIAL**.

```
RDEFINE FACILITY IRR.PASSWORD.RESET UACC(NONE)
PERMIT IRR.PASSWORD.RESET AC(UPDATE) ID(ISIAGNT)
SETROPTS RACLIST(FACILITY) REFRESH
```

If surrogate RACF user IDs are being used, the user ID specified in the preceding PERMIT command reflects the surrogate user ID. It is not the adapter RACF user ID that starts the adapter.

For more information, see the *z/OS RACF Security Administrator's Guide*.

AUTOID support

For IBM Security Identity Manager server to take advantage of AUTOUID support for OMVS segments, then you must define a profile.

Use this command to define the profile:

```
RDEFINE FACILITY BPX.NEXT.USER APPLDATA('nn/mm') UACC(NONE)
SETROPTS RACLIST(FACILITY) REFRESH
```

Where *nn* is a starting OMVS UID to be assigned, and *mm* is the next OMVS GID to be assigned. (The GID is shown here for completeness).

For more information, see the *z/OS RACF Security Administrator's Guide*.

Shared UID support

For IBM Security Identity Manager server to provision a shared OMVS UID number, the adapter, or surrogate user IDs must have the necessary permission.

If the SHARED.IDS profile is defined in the **UNIXPRIV** class, definition of duplicate UIDs for multiple users is prevented. For the IBM Security Identity Manager to define UIDs to multiple users, you must add the RACF user ID (representing the adapter) to have **read** access to the resource profile:

```
PE SHARED.IDS CLASS(UNIXPRIV) AC(READ) ID(ISIAGNT)
SETROPTS CLASS(UNIXPRIV) REFRESH
```

Where the RACF user ID set in the **permit** command is either the adapter ID or the surrogate ID that is used to run the RACF command.

If surrogate RACF user IDs are being used, the user ID specified in the preceding **permit** command reflects the surrogate user ID. It is not the adapter RACF user ID that starts the adapter

For more information, see the *z/OS RACF Security Administrator's Guide*.

z/OS Unix System Services considerations

UNIX System Service creates a task for each child process. If you define `_BPX_SHAREAS=YES` in the `/etc/profile`, the adapter runs in a single address space, instead of multiple address spaces.

By defining this setting, you can use the same name to start and stop a task. Newer releases of z/OS create two address spaces with this environment variable set, for example `ISIAGNT` and `ISIAGNT1`. In this case, the task must be stopped by issuing the **stop** command to the task `ISIAGNT1`. Because this setting affects other areas of UNIX System Services, see the *z/OS UNIX System Services Planning*, document GA22-7800 for more information.

You must correctly define the time zone environment variable (TZ) in `/etc/profile` for your time zone. The messages in the adapter log then reflect the correct local time. See *z/OS UNIX System Services Planning*, document GA22-7800, for more details about this setting.

Configuring communication

Use these tasks to configure the IBM Security Identity Manager server to communicate with the adapter.

Perform the following tasks to establish communication between IBM Security Identity Manager and the adapter:

1. "Importing the adapter profile into the IBM Security Identity Manager server"
2. "Verifying the adapter profile installation" on page 23
3. "Creating a RACF Adapter service" on page 23

Importing the adapter profile into the IBM Security Identity Manager server

An adapter profile defines the types of resources that the IBM Security Identity Manager server can manage. Use the profile to create an adapter service on IBM Security Identity Manager and establish communication with the adapter.

Before you begin

Before you can add an adapter as a service to the IBM Security Identity Manager server, the server must have an adapter profile to recognize the adapter as a service. The files that are packaged with the adapter include the adapter JAR file, `RACFProfile.jar`. You can import the adapter profile as a service profile on the server with the Import feature of IBM Security Identity Manager.

The `RACFProfile.jar` file includes all the files that are required to define the adapter schema, account form, service form, and profile properties. You can extract the files from the JAR file to modify the necessary files and package the JAR file with the updated files.

Before you begin to import the adapter profile, verify that the following conditions are met:

- The IBM Security Identity Manager server is installed and running.
- You have root or Administrator authority on the IBM Security Identity Manager server.

Procedure

To import the adapter profile, perform the following steps:

1. Log on to the IBM Security Identity Manager server. Use an account that has the authority to perform administrative tasks.
2. In the My Work pane, expand **Configure System** and click **Manage Service Types**.
3. On the Manage Service Types page, click **Import** to display the Import Service Types page.
4. Specify the location of the `RACFProfile.jar` file in the **Service Definition File** field.

   The `RACFProfile.jar` is a component of the adapter installation package. See .

   Perform one of the following tasks:

   - Type the complete location of where the file is stored.
   - Use **Browse** to navigate to the file.
5. Click **OK**.

Verifying the adapter profile installation

After you install the adapter profile, verify that the installation was successful.

An unsuccessful installation:

- Might cause the adapter to function incorrectly.
- Prevents you from creating a service with the adapter profile.

To verify that the adapter profile is successfully installed, create a service with the adapter profile. For more information about creating a service, see “Creating a RACF Adapter service.”

If you are unable to create a service using the adapter profile or open an account on the service, the adapter profile is not installed correctly. You must import the adapter profile again.

Creating a RACF Adapter service

After the adapter profile is imported on IBM Security Identity Manager, you must create a service so that IBM Security Identity Manager can communicate with the adapter.

Before you begin

Ensure that you imported the RACF Adapter profile into the IBM Security Identity Manager server.

About this task

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter.

Procedure

1. Log on to the IBM Security Identity Manager server by using an account that has the authority to perform administrative tasks.
2. In the My Work pane, click **Manage Services** and click **Create**.
3. On the Select the Type of Service page, select **RACF Profile**.
4. Click **Next** to display the adapter service form.
5. Complete the following fields on the service form:

On the General Information tab:

Service Name
Specify a name that identifies the RACF Adapter service on the IBM Security Identity Manager server.

Service Description
Optional: Specify a description that identifies the service for your environment. You can specify additional information about the service instance.

URL Specify the location and port number of the adapter. The port number is defined during installation, and can be viewed and modified in the protocol configuration by using the `agentCfg` utility. For more information about protocol configuration settings, see "Changing protocol configuration settings" on page 29.

Note: If you specify https as part of the URL, the adapter must be configured to use SSL authentication. If the adapter is not configured to use SSL authentication, specify http for the URL. For more information, see .

User ID
Specify the name that was defined at installation time as the `Adapter authentication ID`. This name is stored in the registry. The default value is agent.

Password
Specify the password that was defined at installation time as the `Adapter authentication ID`. The default value is agent.

RACF ID under which requests will be processed
Optional: Specify a RACF user ID other than the one that is used by the adapter. This ID might have group special authority over a subset of users within the RACF database.

Owner
Optional: Specify the service owner, if any.

Service Prerequisite
Optional: Specify an existing IBM Security Identity Manager service.

On the Status and information tab
This page contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields.

Last status update: Date
Specifies the most recent date when the Status and information tab was updated.

Last status update: Time
Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status
Specifies the status of the managed resource that the adapter is connected to.

Adapter version
Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

Profile version
Specifies the version of the profile that is installed in the IBM Security Identity Manager server.

ADK version
Specifies the version of the ADK that the adapter uses.

Installation platform
Specifies summary information about the operating system where the adapter is installed.

Adapter account
Specifies the account that running the adapter binary file.

Adapter up time: Date
Specifies the date when the adapter started.

Adapter up time: Time
Specifies the time of the date when the adapter started.

Adapter memory usage
Specifies the memory usage for running the adapter.

If the connection fails, follow the instructions in the error message. Also

- Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify IBM Security Identity Manager service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.

6. Click **Finish**.

Chapter 4. Taking the first steps after installation

After you install the adapter, you must perform several other tasks. The tasks include configuring the adapter, setting up SSL, installing the language pack, and verifying the adapter works correctly.

Configuring the adapter for IBM Security Identity Manager

Use the adapter configuration tool, `agentCfg`, to view or modify the adapter parameters.

All the changes that you make to the parameters with the `agentCfg` take effect immediately. You can also use `agentCfg` to view or modify configuration settings from a remote workstation. For more information about specific procedures to use additional arguments, see Table 19 on page 52 in "Accessing help and additional options" on page 51.

Note: The screens displayed in this section are examples, the actual screens displayed might differ.

Starting the adapter configuration tool

You can use the adapter configuration program, **`agentCfg`**, to view or modify the adapter parameters. All the changes that you make to the parameters with the **`agentCfg`** utility take effect immediately.

About this task

To start the adapter configuration tool, agentCfg, for RACF Adapter parameters, perform the following steps:

Procedure

1. Log on to the TSO on the z/OS operating system that hosts the adapter.
2. From ISPF option 6, run the following command and press **Enter** to enter the USS shell environment:

   ```
   omvs
   ```

   Optional: You can also enter the USS shell environment through a telnet session.
3. In the command prompt, change to the `bin` subdirectory of the adapter in the read/write directory. If the adapter is installed in the default location for the read/write directory, run the following command.

   Note: There is a `bin` subdirectory in the adapter read-only directory too. The read/write `bin` subdirectory contains scripts that set up environment variables, then call the actual executables that reside in the read-only `bin` directory. You must start the adapter tools by running the scripts in the read/write directory, otherwise errors might occur.

   ```
   # cd /var/ibm/isimracf/bin
   ```
4. Run the following command:

   ```
   agentCfg -agent RACFAgent
   ```

The adapter name was specified when you installed the adapter. You can find the names of the active adapters by running the `agentCfg` as:

```
agentCfg -list
```

5. At **Enter configuration key for Agent** *adapter_name*, type the configuration key for the adapter.

   The default configuration key is agent. To prevent unauthorized access to the configuration of the adapter, you must modify the configuration key after the adapter installation completes. For more information, see "Changing protocol configuration settings" on page 29.

   The **Agent Main Configuration Menu** is displayed.

```
RACFAgent 6.0 Agent Main Configuration Menu
-------------------------------------------
A. Configuration Settings.
B. Protocol Configuration.
C. Event Notification.
D. Change Configuration Key.
E. Activity Logging.
F. Registry Settings.
G. Advanced Settings.
H. Statistics.
I. Codepage Support.

X. Done

Select menu option:
```

   From the **Agent Main Configuration Menu** screen, you can configure the protocol, view statistics, and modify settings, including configuration, registry, and advanced settings.

Table 6. Options for the main configuration menu

Option	Configuration task	For more information
A	Viewing configuration settings	See "Viewing configuration settings."
B	Changing protocol configuration settings	See "Changing protocol configuration settings" on page 29.
C	Configuring event notification	See "Configuring event notification" on page 33.
D	Changing the configuration key	See "Changing the configuration key" on page 43.
E	Changing activity logging settings	See "Changing **`activity logging`** settings" on page 44.
F	Changing registry settings	See "Modifying registry settings" on page 46.
G	Changing advanced settings	See "Changing advanced settings" on page 47.
H	Viewing statistics	See "Viewing statistics" on page 49.
I	Setting code page settings	See "Setting the code page" on page 49.

Viewing configuration settings

View the adapter configuration settings for information about the adapter. This information includes version, ADK version, and adapter log file name.

About this task

The following procedure describes how to view the adapter configuration settings:

Procedure

1. Access the Agent Main configuration Menu. See "Starting the adapter configuration tool" on page 27.
2. Type A to display the configuration settings for the adapter.

```
Configuration Settings
------------------------------------------
Name            : adapter_name
Version         : 6.0.4.1200
ADK Version     : 6.0.1017
ERM Version     : 6.04.1200
Adapter Events  : FALSE
License         : NONE
Asynchronous ADD Requests  : FALSE (Max.Threads:3)
Asynchronous MOD Requests  : FALSE (Max.Threads:3)
Asynchronous DEL Requests  : FALSE (Max.Threads:3)
Asynchronous SEA Requests  : FALSE (Max.Threads:3)
Available Protocols        : DAML
Configured Protocols       : DAML
Logging Enabled            : TRUE
Logging Directory          : /var/ibm/isimracf/log
Log File Name              : adapter_name.log
Max. log files             : 3
Max.log file size (Mbytes) : 1
Debug Logging Enabled      : TRUE
Detail Logging Enabled     : FALSE
Thread Logging Enabled     : FALSE
```

3. Press any key to return to the Main Menu.

Changing protocol configuration settings

The adapter uses the DAML protocol to communicate with the IBM Security Identity Manager server. By default, when the adapter is installed, the DAML protocol is configured for a nonsecure environment.

About this task

To configure a secure environment, use Secure Shell Layer (SSL) and install a certificate. For more information, see "Installing the certificate" on page 67.

The DAML protocol is the only supported protocol that you can use. Do not add or remove a protocol.

To configure the DAML protocol for the adapter, perform the following steps:

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. Type B. The DAML protocol is configured and available by default for the adapter.

```
Agent Protocol Configuration Menu
---------------------------------
Available Protocols: DAML
Configured Protocols: DAML
A. Add Protocol.
B. Remove Protocol.
C. Configure Protocol.

X. Done

Select menu option
```

3. At the **Agent Protocol Configuration Menu**, type `C` to display the **Configure Protocol Menu**.

```
Configure Protocol Menu
---------------------------------
A. DAML
X. Done
Select menu option
```

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              FALSE  ;Use SSL secure connection.
F. SRV_NODENAME         9.38.215.20 ;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.

X. Done

Select menu option:
```

5. Follow these steps to change a protocol value:
   - Type the letter of the menu option for the protocol property to configure. Table 7 describes each property.
   - Take one of the following actions:
     - 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 7. 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 Manager server uses this value to connect to the adapter.

Table 7. Options for the DAML protocol menu (continued)

Option	Configuration task
B	Displays the following prompt `Modify Property 'PASSWORD':` Type a password, for example, **admin**. The IBM Security Identity Manager 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 Manager 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':` TRUE specifies to use a secure SSL connection to connect the adapter. If you set USE_SSL to TRUE, you must install a certificate. For more information, see “Installing the certificate” on page 67. FALSE, the default value, specifies not to use a secure SSL connection.
F	Displays the following prompt: `Modify Property 'SRV_NODENAME':` Type a server name or an IP address of the workstation where you installed the IBM Security Identity Manager server. This value is the DNS name or the IP address of the IBM Security Identity Manager server that is used for event notification and asynchronous request processing. **Note:** If your platform 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 Manager server. The adapter uses this port number to connect to the IBM Security Identity Manager 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 the adapter must listen to. The default value is **ANY**.

Table 7. Options for the DAML protocol menu (continued)

Option	Configuration task
I	Displays the following prompt: `Modify Property 'VALIDATE_CLIENT_CE':` Specify TRUE for the IBM Security Identity Manager server to send a certificate when it communicates with the adapter. When you set this option to `TRUE`, you must configure options D through I. Specify FALSE, the default value, to let the IBM Security Identity Manager server communicate with the adapter without a certificate. **Note:** • The property name is VALIDATE_CLIENT_CERT, however, 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 Manager server certificate. For more information about using the certTool, see "Using the certTool utility to manage SSL certificates" on page 63.
J	Displays the following prompt: `Modify Property 'REQUIRE_CERT_REG':` This value applies when option I is set to `TRUE`. Type TRUE to register the adapter with the client certificate from the IBM Security Identity Manager 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 for the RACF adapter" on page 56.
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 open threads in the adapter. which might cause "hang" problems. The open threads might be due to firewall or network connection problems and might be seen as TCP/IP ClosWait connections that remain on the adapter. If you encounter such problems, then you need to set the value of `READ_TIMEOUT` to a time longer than the IBM Security Identity Manager timeout. which is the maximum connection age DAML property on IBM Security Identity Manager and less than any firewall timeout. The adapter must be restarted because READ_TIMEOUT is set at adapter initialization.

6. Follow one these steps at the prompt:
   - 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.
7. Repeat step 5 to configure the other protocol properties.
8. At the **Protocol Properties Menu**, type `X` to exit.

Configuring event notification

Event notification detects changes that are made directly on the managed resource and updates the IBM Security Identity Manager server with the changes. You can enable event notification to obtain the updated information from the managed resource.

When you enable event notification, the workstation on which the adapter is installed maintains a database of the reconciliation data. The adapter updates the database with the changes that are requested from IBM Security Identity Manager and synchronizes with the server. You can specify an interval for the event notification process to compare the database to the data that currently exists on the managed resource. When the interval elapses, the adapter forwards the differences between the managed resource and the database to IBM Security Identity Manager and updates the local snapshot database.

To enable event notification, ensure that the adapter is deployed on the managed host and is communicating successfully with IBM Security Identity Manager. You must also configure the host name, port number, and login information for the IBM Security Identity Manager server and SSL authentication.

Note: Event notification does not replace reconciliations on the IBM Security Identity Manager server.

Identifying the server that uses the DAML protocol and configuring for SSL

You must identify the server that uses the DAML protocol and configure the adapter to use SSL authentication.

Procedure

1. Access the Agent Main Configuration Menu. See "Starting the adapter configuration tool" on page 27.
2. At the Agent Protocol Configuration Menu, select **Configure Protocol**. See "Changing protocol configuration settings" on page 29.
3. Change the USE_SSL property to `TRUE`.
4. Type the letter of the menu option for the **SRV_PORTNUMBER** property.
5. Specify the IP address or server name that identifies the IBM Security Identity Manager server. Press Enter to display the Protocol Properties Menu with new settings.
6. Type the letter of the menu option for the **SRV_PORTNUMBER** property.
7. Specify the port number that the adapter uses to connect to the IBM Security Identity Manager server for event notification.
8. Press Enter to display the Protocol Properties Menu with the new settings.
9. Install certificate by using the certTool. See "Using the certTool utility to manage SSL certificates" on page 63.

Setting event notification on the IBM Security Identity Manager

You must set event notification for the IBM Security Identity Manager server.

About this task

The example menu describes all the options that are displayed when you enable Event Notification. If you disable Event Notification, none of the options are displayed.

Note: The RACF for z/OS does not support adapter-based event notification.

Procedure

1. Access the Agent Main Configuration Menu. See "Starting the adapter configuration tool" on page 27.
2. At the Agent Main Configuration Menu, type `C` to display Event Notification Menu.

```
Event Notification Menu
------------------------------------------------------------
*Password attributes :
* Reconciliation interval : 1 day(s)
* Configured contexts : context1
A. Disabled
B. Time interval between reconciliations.
C. Set processing cache size. (currently: 50 Mbytes)
D. Add Event Notification Context.
E. Modify Event Notification Context.
F. Remove Event Notification Context.
G. List Event Notification Contexts.
H. Set password attribute names.
X. Done
Select menu option:
```

3. At the Agent Main Configuration Menu, type the letter of the menu option that you want to change.

   Note:

   - Enable option A for the values of the other options to take effect. Each time you select this option, the state of the option changes.
   - Press Enter to return to the Agent Event Notification Menu without changing the value.

Table 8. Options for the event notification menus

Option	Configuration task
A	If you select this option, the adapter updates the IBM Security Identity Manager server with changes to the adapter at regular intervals. If **Enabled - Adapter** is selected, the adapter code processes event notification by monitoring a change log on the managed resource. When the option is set to: **Disabled** All options except **Start event notification now** and **Set attributes** that are to be reconciled are available. Pressing A changes the setting to **Enabled - ADK**. **Enabled - ADK** All options are available. Pressing A changes the setting to **Disabled** or if your adapter supports event notification, to **Enabled - Adapter**. **Enabled - Adapter** All options are available, except **Time interval between reconciliations** **Set processing cache size** **Start event notification now** **Reconciliation process priority** **Set attributes to be reconciled** Pressing A changes the setting to **Disabled**. Type A to toggle between the options. **Note:** The adapter does not support adapter-based event notification, **Enabled - Adapter**. Therefore, this option is not listed in the event notification menu.
B	Displays the following prompt: `Enter new interval ([ww:dd:hh:mm:ss])` Type a different reconciliation interval. For example, `[00:01:00:00:00]` This value is the interval to wait after the event notification completes before it is run again. The event notification process is resource intense, therefore, this value must not be set to run frequently. This option is not available if you select **Enabled - Adapter**.
C	Displays the following prompt: `Enter new cache size[50]:` Type a different value to change the processing cache size. This option is not available if you select **Enabled - Adapter**.
D	Displays the Event Notification Entry Types Menu. This option is not available if you select Disabled or Enabled - Adapter. For more information, see "Setting event notification triggers" on page 36.
E	Displays the following prompt: `Enter new thread priority [1-10]:` Type a different thread value to change the event notification process priority. Setting the thread priority to a lower value reduces the impact that the event notification process has on the performance of the adapter. A lower value might also cause event notification to take longer.

Table 8. Options for the event notification menus (continued)

Option	Configuration task
F	Displays the following prompt: `Enter new context name:` Type the new context name and press Enter. The new context is added.
G	Displays a menu that lists the available contexts. For more information, see "Modifying an event notification context" on page 37.
H	Displays the Remove Context Menu. This option displays the following prompt: `Delete context context1? [no]:` Press Enter to exit without deleting the context or type `Yes` and press Enter to delete the context.

I	Displays the Event Notification Contexts in the following format:
	`Context Name : Context1`
	`Target DN : erservicename=context1,o=IBM,ou=IBM,dc=com`
	`--- Attributes for search request ---`
	`{search attributes listed}`
	`----------`

J	When you select the **Set password attribute names**, you can set the names of the attributes that contain passwords. These values are not stored in the state database and changes are not sent as events. This option avoids the risk of sending a delete request for the old password in clear text when IBM Security Identity Manager changes a password. Changes from IBM Security Identity Manager are recorded in the local database for event notification. A subsequent event notification does not retrieve the password. It sends a delete request for the old password in clear text that is listed in the IBM Security Identity Manager log files.

4. If you changed the value for options B, C, E, or F, press Enter. The other options are automatically changed when you type the corresponding letter of the menu option. The Event Notification Menu is displayed with your new settings.

Setting event notification triggers

By default, all the attributes are queried for value changes. Attributes that change frequently, for example, **Password age** or **Last successful logon**, must be omitted from event notification.

Procedure

1. Access the Agent Main Configuration Menu. See "Starting the adapter configuration tool" on page 27.
2. At the Event Notification Menu, type `E` to display the Event Notification Entry Types Menu.

```
Event Notification Entry Types
------------------------------------------
A. erRacfACCOUNT
X. Done
Select menu option:
```

   The USER and GROUP types are not displayed in the menu until you meet the following conditions:

   - Enable Event notification
   - Create and configure a context

- Perform a full reconciliation operation

3. Take on of the following actions:
   - Type A for a list of the attributes that are returned during a user reconciliation.
   - Type B for attributes returned during a group reconciliation.

   The Event Notification Attribute Listing for the selected type is displayed. The default setting lists all attributes that the adapter supports. The following example lists example attributes.

```
Event Notification Attribute Listing
------------------------------------
(a) **eraccountstatus (b) **erracconxml (c) **erracucicsisforc
(d) **erracucicsopclas (e) **erracucicsopid (f) **erracucicsprty
(g) **erracucicstimout (h) **erracuclauth (i) **erracucredate
(j) **erracudcehomec (k) **erracudcehomeu (l) **erracudceisautol
(m) **erracudcename (n) **erracudceuuid (o) **erracudfltgrp
(p) **erracudfpappl (q) **erracudfpdata (r) **erracudfpmgmt
(p)rev page 1 of 7 (n)ext
----------------------------
X. Done
```

4. To exclude an attribute from an event notification, type the letter of the menu option

   Note: Attributes that are marked with ** are returned during the event notification. Attributes that are not marked with ** are not returned during the event notification

Modifying an event notification context

An event notification context corresponds to a service on the IBM Security Identity Manager server.

About this task

Some adapters support multiple services. One RACF Adapter can have several IBM Security Identity Manager services if you specify a different base point for each service. You can have multiple event notification contexts, however, you must have at least one adapter.

To modify an event notification context, perform the following steps. In the following example screen, Context1, Context2, and Context3 are different contexts that have a different base point.

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. From Event Notification, type the **Event Notification Menu** option.
3. From **Event Notification Menu**, type the Modify Event Notification Context option to display a list of available context. For example,

```
Modify Context Menu
-------------------------------
A. Context1
B. Context2
C. Context3
X. Done
Select menu option:
```

4. Type the option of the context that you want to modify to obtain a list as described in the following screen.

```
A. Set attributes for search
B. Target DN:
X. Done
Select menu option:
```

Table 9. Options for the modify context menu

Option	Configuration task	For more information
A	Adding search attributes for event notification	See "Adding search attributes for event notification."
B	Configuring the target DN for event notification contexts	See "Configuring the target DN for event notification contexts."

Adding search attributes for event notification:

For some adapters, you might need to specify an attribute/value pair for one or more contexts.

About this task

These attribute/value pairs, which are defined by completing the following steps, serve multiple purposes:

- When a single adapter supports multiple services, each service must specify one or more attributes to differentiate the service from the other services.
- The adapter passes the search attributes to the event notification process either after the event notification interval occurs or the event notification starts manually. For each context, a complete search request is sent to the adapter. Additionally, the attributes specified for that context are passed to the adapter.
- When the IBM Security Identity Manager server initiates a reconciliation process, the adapter replaces the local database that represents this service with the new database.

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. At the **Modify Context Menu** for the context, type `A` to display the **Reconciliation Attribute Passed to Agent Menu**.

```
Reconciliation Attributes Passed to Agent for Context: Context1
--------------------------------------------------
--------------------------------------------------
A. Add new attribute
B. Modify attribute value
C. Remove attribute
X. Done
Select menu option:
```

The RACF for z/OS requires the resource_name attribute to be specified for each context. The value of the attribute must be set to the Managed Resource Name defined on the IBM Security Identity Manager Service Form.

Configuring the target DN for event notification contexts:

During event notification configuration, the adapter sends requests to a service that is running on the IBM Security Identity Manager server. Therefore, you must configure target DN for event notification contexts for the adapter to know which service the adapter must send the request to.

About this task

Configuring the target DN for event notification contexts involves specifying parameters, such as:

The adapter service name

Organization (o)

Organization name (ou)

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. Type the option for Event Notification to display the **Event Notification Menu**.
3. Type the option for Modify Event Notification Context, then enter the option of the context that you want to modify.
4. At the **Modify Context Menu** for the context, type `B`. The following prompt is displayed:

   ```
   Enter Target DN:
   ```
5. Type the target DN for the context and press Enter. The target DN for the event notification context must be in the following format:

   `erservicename=`*`erservicename`*`,o=`*`organizationname`*`,ou=`*`tenantname`*`,rootsuffix`

   Table 10 describes each DN element.

Table 10. DN elements and definitions

Element	Definition
erservicename	Specifies the name of the target service.
o	Specifies the name of the organization.
ou	Specifies the name of the tenant under which the organization is. If this installation is an enterprise installation, then ou is the name of the organization.
rootsuffix	Specifies the root of the directory tree. This value is the same as the value of *Identity Manager DN Location* which is specified during the IBM Security Identity Manager server installation.

The **Modify Context Menu** displays the new target DN.

Specifying attributes for search: For some adapters, you might need to specify an attribute/value pair for one or more contexts. These attribute/value pairs, which are defined in the context under **Set attributes for search**, serve multiple purposes:

- When multiple service instances on the IBM Security Identity Manager server reference the adapter, each service instance must have permissions to specify an attribute-value pair. This pair enables the adapter to know which service instance is requesting work.
- The attribute is sent to the event notification process when the event notification interval occurs or is manually initiated. When the attribute is received, the adapter processes information that the attribute/value pair indicates.

- When you start a server-initiated reconciliation process, the adapter replaces the local database that represents this service instance.

Table 11 describes a partial list of possible attribute/value pairs that you can specify for **Set attributes for search**.

Table 11. Attributes for search

Service type	Form label	Attribute name	Value
RACFProfile	RACF ID under which requests are processed	erracfrequester	A *group special*RACF user ID that manages users in this service.

```
Modify Context Menu
-------------------------------

A.  RACF

X.  Done

Select menu option:a

Modify Context: RACF
-----------------------------------

A.  Set attributes for search
B.  Target DN:

Select menu option:a

Reconciliation Attributes Passed to Agent for context: RACF
---------------------------------------------------

A.  Add new attribute
B.  Modify attribute value
C.  Remove attribute

X.  Done

Select menu option:a

Attribute name : erracfrequester

Attribute value: admnbu1

Reconciliation Attributes Passed to Agent for context: RACF
---------------------------------------------------
01. ercaacf2requester           'admnbu1'
---------------------------------------------------

A.  Add new attribute
B.  Modify attribute value
C.  Remove attribute

X.  Done

Select menu option:x
```

Determining pseudo-distinguished name values:

The Target DN field has the pseudo-distinguished name of the service that receives event notification updates.

To assist in determining the correct entries, this name might be considered to contain the listed components in the A+B+C+D+E sequence.

Note: Do not use a comma to define a pseudo DN.

Table 12. Name values and their description

Component	Item	Description
A	erServicename	The value of the erServicename attribute of the service.
B	Zero or more occurrences of **ou** or **1** or both.	When the service is not directly associated with the organization, you must specify **ou** and **l**. The specification of these values is in a reverse sequence of their appearance in the IBM Security Identity Manager organization chart.
C	o	The value of the **o** attribute of an organization to which the service belongs, at the highest level. This value can be determined by examining the IBM Security Identity Manager organization chart.
D	ou	The **ou** component is established at IBM Security Identity Manager installation. You can find this component in the IBM Security Identity Manager configuration file named `enRole.properties`, on configuration item named **enrole.defaulttenant.id=**
E	dc	The **dc** component is established at IBM Security Identity Manager installation. This component is the root suffix of the LDAP environment. You can find this component in the IBM Security Identity Manager configuration file named `enRole.properties`, on configuration item named **enrole.ldapserver.root=**

Example 1:

A:

The service name on the IBM Security Identity Manager server is **z/OS RACF 4.5.1016 ENTEST**. This name becomes the component **A** of the pseudo-DN:

```
erservicename=z/OS RACF 4.5.1016 ENTEST
```

B:

Table 13 describes an example of the IBM Security Identity Manager organization chart that indicates the location of the service in the organization.

Table 13. Organization chart example

+ Identity Manager Home	IBM Security Identity Manager Home	
+ Acme Inc	Base organization	o

Component **B** is not required because the service is directly associated with the organization at the beginning of the organization chart.

C:

The organization this service is associated with, described on the IBM Security Identity Manager organization chart is named Acme Inc. The service becomes component **C** of the pseudo-DN:

```
o=Acme Inc
```

D:

The value of the property named **enrole.defaulttenant.id=** defined in the `enRole.properties` definition file on the IBM Security Identity Manager server becomes component **D** of the pseudo-DN. For example:

```
#########################################################
## Default tenant information
#########################################################
enrole.defaulttenant.id=Acme
```

The **D** component of the pseudo-DN is: ou=Acme

E:

The value of the property named **enrole.ldapserver.root=** defined in the `enRole.properties` definition file on the IBM Security Identity Manager server becomes component **E** of the pseudo-DN. For example:

```
#########################################################
## LDAP server information
#########################################################
enrole.ldapserver.root=dc=my_suffix
```

The **E** component of the pseudo-DN is: `dc=my_suffix`

The following pseudo-DN is the result of all the components (A+B+C+D+E components):

```
erservicename=z/OS RACF 4.5.1016 ENTEST,o=Acme Inc,ou=Acme,dc=my_suffix
```

Example 2:

A:

The service name on the IBM Security Identity Manager server is **Irvine Sales**. This name becomes component **A** of the pseudo-DN:

```
erservicename=Irvine Sales
```

B:

Table 14 describes an example of the IBM Security Identity Manager organization chart that indicates the location of the service in the organization.

Table 14. Organization chart example

+ Identity Manager Home	IBM Security Identity Manager Home	
-Acme Inc	Base organization	o
- Irvine Sales	LocationOrganizational Unit	lou

The **Irvine Sales** service is defined under organizational unit (**ou**) named *Sales,* which is defined under location (**l**) named *Irvine*.

Component B of the pseudo-DN is:

```
ou=Sales,l=Irvine
```

C:

The organization this service is associated with, shown on the IBM Security Identity Manager organization chart is named Acme Inc. This organization becomes the component **C** of the pseudo-DN:

```
o=Acme Inc
```

D:

The value of the property named **enrole.defaulttenant.id=** defined in the `enRole.properties` definition file on the IBM Security Identity Manager server becomes component **D** of the pseudo-DN. For example:

```
#########################################################
## Default tenant information
#########################################################
enrole.defaulttenant.id=Acme
```

The **D** component of the pseudo-DN is:

```
ou=Acme
```

E:

The value of the property named **enrole.ldapserver.root=** defined in the `enRole.properties` definition file on the IBM Security Identity Manager server becomes component **E** of the pseudo-DN. For example:

```
#########################################################
## LDAP server information
#########################################################
enrole.ldapserver.root=dc=my_suffix
```

The **E** component of the pseudo-DN is:

```
dc=my_suffix
```

The following pseudo-DN is the result of the components (A+C+D+E). Component B is not required.

```
erservicename=Irvine Sales, ou=Sales,l=Irvine o=Acme Inc,ou=Acme,dc=my_suffix
```

Removing the baseline database for event notification contexts:

You can remove the baseline database for event notification contexts only after you create a context. You must also reconcile on the context to create a Baseline Database file.

Procedure

1. From the **Agent Main Configuration Menu**, type the Event Notification option.
2. From the **Event Notification Menu**, type the Remove Event Notification Context option to display the **Modify Context Menu**.
3. Select the context that you want to remove.
4. After you confirm that you want to remove a context, press **Enter** to remove the baseline database for event notification contexts.

Changing the configuration key

You use the configuration key as a password to access the configuration tool for the adapter.

About this task

To change the RACF Adapter configuration key, perform the following steps:

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. At the Main Menu prompt, type `D`.
3. Take one of the following actions:

- Change the value of the configuration key and press Enter.
- Press Enter to return to the **Main Configuration Menu** without changing the configuration key.

Results

The default configuration key is **agent**. Ensure that your password is complex. The following message is displayed:

```
Configuration key successfully changed.
```

The configuration program returns to the **Main Menu** prompt.

Changing `activity logging` settings

Use this task to enable or disable log files that monitor various system activities.

About this task

When you enable **`activity logging`** settings, IBM Security Identity Manager maintains a log file, `RACFAgent.log`, of all transactions. By default, the log file is in the read/write `log` directory.

To change the RACF Adapter **`activity logging`** settings,

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. At the **Main Menu** prompt, type `E` to display the **Agent Activity Logging Menu**. The following screen displays the default **`activity logging`** settings.

```
Agent Activity Logging Menu
-----------------------------------
A. Activity Logging (Enabled).
B. Logging Directory (current: /var/ibm/isimracf/log).
C. Activity Log File Name (current: RACFAgent.log).
D. Activity Logging Max. File Size ( 1 mbytes)
E. Activity Logging Max. Files ( 3 )
F. Debug Logging (Enabled).
G. Detail Logging (Disabled).
H. Base Logging (Disabled).
I. Thread Logging (Disabled).
X. Done
Select menu option:
```

3. Type the letter for the activity you want to change and perform one of the following actions:
   - Press Enter to change the value for menu option B, C, D, or E. The other options are changed automatically when you type the corresponding letter of the menu option. Table 15 on page 45 describes each option.
   - Press Enter to return to the **Agent Activity Logging Menu** without changing the value.

   Note: Ensure that Option A is enabled for the values of other options to take effect.

Table 15. Options for the **activity logging** *menu*

Option	Configuration task
A	Set this option to Enabled for the adapter to maintain a dated log file of all transactions. When the option is set to: • Disabled, pressing the A key changes to enabled • Enabled, pressing the A key changes to disabled Type A to toggle between the options.
B	Displays the following prompt: `Enter log file directory:` Type a different value for the logging directory, for example, /home/Log. When the logging option is enabled, details about each access request are stored in the logging file that is in this directory.
C	Displays the following prompt: `Enter log file name:` Type a different value for the log file name. When the logging option is enabled, details about each access request are stored in the logging file.
D	Displays the following prompt: `Enter maximum size of log files (mbytes):` Type a new value, for example, **10**. The oldest data is archived when the log file reaches the maximum file size. File size is measured in megabytes. It is possible for the activity log file size to exceed the disk capacity.
E	Displays the following prompt: `Enter maximum number of log files to retain:` Type a new value up to 99, for example, **5**. The adapter automatically deletes the oldest activity logs beyond the specified limit.
F	If this option is set to enabled, the adapter includes the debug statements in the log file of all transactions. When the option is set to: • Disabled, pressing the F key changes the value to enabled • Enabled, pressing the F key changes the value to disabled Type F to toggle between the options.
G	If this option is set to enabled, the adapter maintains a detailed log file of all transactions. The detail logging option must be used for diagnostic purposes only. Detailed logging enables more messages from the adapter and might increase the size of the logs. When the option is set to: • Disabled, pressing the G key changes the value to enabled • Enabled, pressing the G key changes the value to disabled Type G to toggle between the options.

Table 15. Options for the **activity logging** *menu (continued)*

Option	Configuration task
H	If this option is set to enabled, the adapter maintains a log file of all transactions in the Agent Development Kit (ADK) and library files. Base logging substantially increases the size of the logs. When the option is set to: • Disabled, pressing the H key changes the value to enabled • Enabled, pressing the H key changes the value to disabled Type H to toggle between the options.
I	If this option is enabled, the log file contains thread IDs, in addition to a date and timestamp on each line of the file. When the option is set to: • Disabled, pressing the I key changes the value to enabled • Enabled, pressing the I key changes the value to disabled Type I to toggle between the options.

Modifying registry settings

Use this procedure to access the various types of registry setting that you might want to change.

About this task

To change the adapter registry settings:

At the **Main Menu**, type F. The **Registry Menu** is displayed.

```
RACFAgent 6.0 Agent Registry Menu
-----------------------------------------
A. Modify Non-encrypted registry settings.
B. Modify encrypted registry settings.
C. Multi-instance settings.
X. Done
Select menu option:
```

For a list of valid registry options, their values, and meanings, see Appendix B, "Registry settings," on page 111.

What to do next

See the following procedures to modify the registry settings.

Modifying non-encrypted registry settings

Use this task to modify registry settings that do not use encryption.

Procedure

1. At the **Agent Registry Menu**, type A. The **Non-encrypted Registry Settings Menu** is displayed.

```
Agent Registry Items
-----------------------------------------------
01. APPCCMD 'ISIMCMD'
02. APPCDLU 'ISIMDEST'
03. APPCMODE '#INTERSC'
04. APPCOLU 'ISIMORIG'
05. APPCRECO 'ISIMRECO'
06. ENROLE_VERSION '6.0'
07. PASSEXPIRE 'TRUE'
-----------------------------------------------
Page 1 of 1
A. Add new attribute
B. Modify attribute value
C. Remove attribute
X. Done
Select menu option:
```

Table 16. Non-encrypted registry keys

Key	Description
APPCCMD	Specifies the APPC transaction name for the IBM Security Identity Manager command transaction.
APPCDLU	Specifies the APPC destination Logical Unit (LU). If NULL, the adapter uses BASELU.
APPCMODE	Specifies the APPC mode table entry that the adapter uses for conversations.
APPCOLU	Specifies the APPC Originating LU. If NULL, the adapter uses BASELU.
APPCRECO	Specifies the APPC transaction name for the IBM Security Identity Manager reconciliation transaction.
ENROLE_VERSION	Specifies the version of IBM Security Identity Manager.
PASSEXPIRE	Specifies the default action that the adapter must perform when the adapter receives a password change request. `TRUE` indicates that passwords must be set as expired. `FALSE` indicates that passwords must be set as non-expired.

2. Type the letter of the menu option for the action that you want to perform on an attribute.

Table 17. Attribute configuration option description

Option	Configuration task
A	Add new attribute
B	Modify attribute value
C	Remove attribute

3. Type the registry item name and press Enter.
4. If you selected option A or B, type the registry item value.
5. Press Enter.

Results

The **Non-encrypted Registry Settings Menu** displays the new settings.

Changing advanced settings

You can change the adapter thread count settings for the following types of requests.

About this task

You can change the adapter thread count settings for the following types of requests:

- System Login Add
- System Login Change
- System Login Delete
- Reconciliation

These thread counts determines the maximum number of requests that the adapter processes. To change these settings, perform the following steps:

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. At the **Main Menu** prompt, type `G` to display the **Advanced Settings Menu**.
   The following screen displays the default thread count settings.

```
RACFAgent 6.0 Advanced Settings Menu
-----------------------------------------
A. Single Thread Agent (current:FALSE)
B. ADD max. thread count. (current:3)
C. MODIFY max. thread count. (current:3)
D. DELETE max. thread count. (current:3)
E. SEARCH max. thread count. (current:3)
F. Allow User EXEC procedures (current:FALSE)
G. Archive Request Packets (current:FALSE)
H. UTF8 Conversion support (current:TRUE)
I. Pass search filter to agent (current:FALSE)

X. Done
Select menu option:
```

3. Type letter of the menu option that you want to change. For a description of each option, see Table 18.

Table 18. Options for the advanced settings menu

Option	Description
A	Forces the adapter to submit only one request at a time. The default value is `FALSE`.
B	Limits the number of Add requests that can run simultaneously. The default value is `3`.
C	Limits the number of Modify requests that can run simultaneously. The default value is `3`.
D	Limits the number of Delete requests that can run simultaneously. The default value is `3`.
E	Limits the number of Search requests that can run simultaneously. The default value is `3`.

Table 18. Options for the advanced settings menu (continued)

Option	Description
F	Determines whether the adapter can perform the pre-exec and post-exec functions. The default value is `FALSE`. **Note:** Enabling this option is a potential security risk.
G	This option is no longer supported.
H	This option is no longer supported.
I	Currently, this adapter does not support processing filters directly. This option must always be `FALSE`.

4. Change the value and press Enter to display the **Advanced Settings Menu** with new settings.

Viewing statistics

Use this procedure to view an event log for the adapter.

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. At the **Main Menu** prompt, type `H` to display the activity history for the adapter.

```
RACFAgent 6.0 Agent Request Statistics
------------------------------------------------------------------------
Date       Add       Mod       Del       Ssp       Res       Rec


------------------------------------------------------------------------

10/19/2004  000000    000004    000000     000000    000000    000004

------------------------------------------------------------------------

X. Done
```

3. Type `X` to return to the **Main Configuration Menu**.

Setting the code page

Use this task to list the supported code page information for the adapter.

Before you begin

The adapter must be running.

About this task

Run the following command to view the code page information:

```
agentCfg -agent RACFAgent -codepages
```

To change the code page settings for the adapter, perform the following steps:

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 27.
2. At the **Main Menu** prompt, type `I`.

   The **Code Page Support Menu** for the adapter is displayed.

```
RACFAgent 6.0 Codepage Support Menu
-----------------------------------------
* Configured codepage: IBM-1047-s390
-----------------------------------------
*
*****************************************
* Restart Agent After Configuring Codepages
*****************************************

A.  Codepage Configure.

X.  Done

Select menu option:
```

3. Type `A` to configure a code page.
4. After you select a code page, restart the adapter. The following screen is a sample session with agentCfg, altering the default code page, from US EBCDIC (IBM-1047) to Spanish EBCDIC (IBM-1145).

```
IBMUSER:/u/ibmuser: >agentCfg -ag RACFAgent

Enter configuration key for Agent 'RACFAgent':

        RACFAgent 6.0 Agent Main Configuration Menu
        -------------------------------------------

        A.  Configuration Settings.
        B.  Protocol Configuration.
        C.  Event Notification.
        D.  Change Configuration Key.
        E.  Activity Logging.
        F.  Registry Settings.
        G.  Advanced Settings.
        H.  Statistics.
        I.  Codepage Support.

        X.  Done

        Select menu option:i

        RACFAgent 6.0 Codepage Support Menu
        -----------------------------------------
        * Configured codepage: IBM-1047-s390
        -----------------------------------------
        *
        *****************************************
        * Restart Agent After Configuring Codepages
        *****************************************

        A.  Codepage Configure.

        X.  Done

        Select menu option:a

        Enter Codepage: ibm-1145

        RACFAgent 6.0 Codepage Support Menu
        -----------------------------------------
        * Configured codepage: ibm-1145
        -----------------------------------------
        *
        *****************************************
        * Restart Agent After Configuring Codepages
        *****************************************

        A.  Codepage Configure.

        X.  Done

        Select menu option:x
```

5. Type X to return to the **Main Configuration Menu**.

Accessing help and additional options

Use this task to access the agentCfg help menu and use the help arguments.

Procedure

1. At the **Main Menu** prompt, type X to display the USS command prompt.
2. Type agentCfg -help at the prompt to display the help menu and list of commands.

```
-version              ;Show version
-hostname <value>    ;Target nodename to connect to (Default:Local host
IP address)
-findall              ;Find all agents on target node
-list                 ;List available agents on target node
```

```
-agent <value>         ;Name of agent
-tail                  ;Display agent's activity log
-schema                ;Display agent's attribute schema
-portnumber <value>    ;Specified agent's TCP/IP port number
-netsearch <value>   ;Lookup agents hosted on specified subnet
-codepages             ;Display list of available codepages
-help                  ;Display this help screen
```

The following table describes each argument.

Table 19. Arguments and description for the agentCfg help menu

Argument	Description
-version	Use this argument to display the version of the agentCfg tool.
-hostname <value>	Use the -hostname argument with one of the following arguments to specify a different host: • -findall • -list • -tail • -agent Enter a host name or IP address as the value.
-findall	Use this argument to search and display all port addresses 44970 - 44994 and their assigned adapter names. This option times out the unused port numbers, therefore, it might take several minutes to complete. Add the -hostname argument to search a remote host.
-list	Use this argument to display the adapters that are installed on the local host of the RACF Adapter. By default, the first time you install an adapter, it is either assigned to port address 44970 or to the next available port number. You can then assign all the later installed adapters to the next available port address. After the software finds an unused port, the listing stops. Use the -hostname argument to search a remote host.
-agent <value>	Use this argument to specify the adapter that you want to configure. Enter the adapter name as the value. Use this argument with the -hostname argument to modify the configuration setting from a remote host. You can also use this argument with the -tail argument.
-tail	Use this argument with the -agent argument to display the activity log for an adapter. Add the -hostname argument to display the log file for an adapter on a different host.
-portnumber <value>	Use this argument with the -agent argument to specify the port number that is used for connections for the agentCfg tool.

Table 19. Arguments and description for the agentCfg help menu (continued)

Argument	Description
-netsearch <value>	Use this argument with the -findall argument to display all active adapters on the z/OS operating system. You must specify a subnet address as the value.
-codepages	Use this argument to display a list of available codepages.
-help	Use this argument to display the Help information for the agentCfg command.

3. Type agentCfg before each argument you want to run, as shown in the following examples.

   agentCfg -list
   Displays a list of :
   - All the adapters on the local host.
   - The IP address of the host.
   - The IP address of the local host.
   - The node on which the adapter is installed.

   The default node for the IBM Security Identity Manager server must be 44970. The output is similar to the following example:

   ```
   Agent(s) installed on node '127.0.0.1'
   ----------------------
   RACFAgent    (44970)
   ```

   agentCfg -agent *adapter_name*
   Displays the Main Menu of the agentCfg tool, which you can use to view or modify the adapter parameters.

   agentCfg -list -hostname 192.9.200.7
   Displays a list of the adapters on a host with the IP address 192.9.200.7. Ensure that the default node for the adapter is 44970. The output is similar to the following example:

   ```
   Agent(s) installed on node '192.9.200.7'
   -----------------
   RACFAgent        (44970)
   ```

   agentCfg -agent *adapter_name* **-hostname 192.9.200.7**
   Displays the agentCfg tool **Main Menu** for a host with the IP address 192.9.200.7. Use the menu options to view or modify the adapter parameters.

Customizing the RACF Adapter

You can perform specific functions according to your requirements with the following REXX execs that are provided with the adapter installation:

- "ISIMEXIT"
- "ISIMEXEC" on page 55

ISIMEXIT

ISIMEXIT is a REXX exec. ISIMEXIT is started in response to a request from the IBM Security Identity Manager server.

You can implement the following instances where the ISIMEXIT exec gets control:

Pre add processing
The request to add a user is received, however, not yet processed.

Post add processing
The request to add a user is completed successfully.

Pre modify processing
The request to modify a user is received, however, not yet processed.

Post modify processing
The request to modify a user is completed successfully.

Pre suspend processing
The request to suspend a user is received, however, not yet processed.

Post suspend processing
The request to suspend a user is completed successfully.

Pre restore processing
The request to restore a user is received, however, not yet processed.

Post restore processing
The request to restore a user is completed successfully.

Pre delete processing
The request to delete a user is received, however, not yet processed.

Post delete processing
The request to delete a user is completed successfully.

Exit processing might indicate success (zero return code) or failure (non-zero return code) to convey to the adapter. For the pre operation exits, any non-zero return code returns a failure for the current RACF user that is processed. For the post operation exits, a non-zero return code returns a warning for the current RACF user that is processed.

The environment in which the ISIMEXIT gets control is in a TSO batch environment, running in the APPC/MVS environment. You might call other programs and perform file Input/Output (I/O) as necessary. Processing is performed under the authority of the RACF ID that runs the RACF commands to accomplish the function. You might run a valid TSO command if it does not prompt for a terminal user for input.

Ensure that the ISIMEXIT exec is available independent of whether it performs any functions. The sample ISIMEXIT provided has an **exit 0** as the first executable statement. You must modify this exit to meet your requirements.

The sample exit provides functions that you might use or customize according to your requirements. For example:

- Defining a user catalog alias in one or more master catalogs at POST ADD or POST MODIFY exit time.
- Defining a user data set profile at POST ADD or POST MODIFY exit time.
- Defining a user OMVS (UNIX System Services) home directory at POST ADD or POST MODIFY exit time.
- Deleting a user data set profiles at PRE DELETE exit time.
- Deleting a user catalog alias at POST DELETE exit time.

Note: Ensure that the Processing ID has appropriate RACF authorization to perform the listed exit functions.

The listed information is available to the EXIT.

Table 20. ISIMEXIT processing information

Parameter #	Meaning	Possible value	Availability
1	Verb Indicates what operation is calling the exit.	ADD, MODIFY, SUSPEND, RESTORE, or DELETE.	Always
2	Object The object name of the transaction.	USER indicating a RACF user object that is processed.	Always
3	Prepost Qualifies whether this entry is PRE or POST processing entry to the exit.	BEFORE or AFTER.	Always
4	Name The name of the RACF object.	The RACF user ID that is processed.	Always
5	Dfltgrp The RACF user ID default group.	The value that is specified from the IBM Security Identity Manager server for the default group of this user.	Only at PRE ADD or POST ADD exit. Not available for DELETE processing.
6	Owner TheRACF user ID owner.	The value that is specified from the IBM Security Identity Manager server owner for this user.	Only at PRE ADD or POST ADD exit. Not available for DELETE processing.

ISIMEXEC

ISIMEXEC is a REXX exec. Use this exec for compatibility with an earlier version of the adapter.

The ISIMEXEC processing can present a zero or a non-zero return code when the processing is complete. A zero return code indicates successful processing of the erRacExecname attribute. If a non-zero return code is presented on exit, the adapter indicates that the **erRacExecname** attribute failed.

The environment in which the ISIMEXEC gets control is in a TSO batch environment, running in the APPC/MVS environment. You might call other programs and perform file I/O as necessary. Processing is performed under the authority of the RACF ID that runs the RACF commands to accomplish the function. You might run a valid TSO command if it does not prompt for a terminal user for input.

Table 21. ISIMEXEC processing information

Parameter #	Source	Value	Availability
1	IBM Security Identity Manager attribute of erUid	The value of the erUid.	Always, because this attribute accompanies all requests.

Table 21. ISIMEXEC processing information (continued)

Parameter #	Source	Value	Availability
2	IBM Security Identity Manager attribute of erRacExecname	The value of the erRacExecname.	Always, because the availability of this attribute indicates that this exit must be started.
3	IBM Security Identity Manager attribute of erRacExecvar	The value of the erRacExecvar.	Based on the request generated by the IBM Security Identity Manager server.

When the **erRacExecname** attribute is available and optionally, the **erRacExecvar** attribute is available, the ISIMEXEC exit point is started as a TSO command in the command executor.

If the **erRacExecname** attribute is present, then the following command is generated:

```
%ISIMEXEC erUid erRacExecname erRacExecvar
```

If the erRacExecvar attribute is available during an add operation, run the command after the add operation. However, only the following attributes are available on the RACF user profile:

- erUid
- erRacUDfltgrp
- erRacUowner

When the ISIMEXEC is processed, the **erRacExecname** attribute can represent anything that you want to process. It provides a second-level command or exec name that you want to run.

Note:

- You can prevent the running of unauthorized commands for processing by interrogating the **erRacExecname** attribute because ISIMEXEC always receives control.
- ISIMEXEC is never started during a delete command because the adapter presents only the **erUid** attribute.

Configuring SSL authentication for the RACF adapter

This chapter presents an overview of SSL authentication, certificates, and how to enable SSL authentication by using the certTool utility.

To establish a secure connection between the adapter and the IBM Security Identity Manager server, configure the adapter and the IBM Security Identity Manager server to use the Secure Sockets Layer (SSL) authentication with the default communication protocol, DAML. By configuring the adapter for SSL, the IBM Security Identity Manager server can verify the identity of the adapter before establishing a secure connection.

You can configure SSL authentication for connections that originate from the IBM Security Identity Manager server or from the adapter. The IBM Security Identity Manager server initiates a connection to the adapter to set or retrieve the value of a managed attribute on the adapter. Depending on the security requirements of your environment, you might configure SSL authentication for connections that

originate from the adapter. For example, adapter events can notify the IBM Security Identity Manager server of changes to attributes on the adapter. In this case, configure SSL authentication for Web connections that originate from the adapter to the Web server used by the IBM Security Identity Manager server.

In a production environment, you must enable SSL security. If an external application communicates with the adapter (for example, the IBM Security Identity Manager server) and uses server authentication, enable SSL on the adapter. Enabling SSL verifies the certificate that the application presents.

Overview of SSL and digital certificates

An enterprise network deployment requires secure communication between the IBM Security Identity Manager server and the software products and components with which the server communicates.

SSL protocol uses signed digital certificates from a certificate authority (CA) for authentication. SSL secures communication in a IBM Security Identity Manager configuration. SSL provides encryption of the data exchanged between the applications. Encryption makes data transmitted over the network intelligible only to the intended recipient.

Signed digital certificates enable two applications connecting in a network to authenticate their identity. An application acting as an SSL server presents its credentials to verify to an SSL client. The SSL client then verifies that the application is the entity it claims to be. You can configure an application acting as an SSL server so that it requires the application acting as an SSL client to present its credentials in a certificate. In this way, the two-way exchange of certificates is completed. A third-party certificate authority issues signed certificates for a fee. Some utilities, such as those provided by OpenSSL, can also provide signed certificates.

You must install a certificate-authority certificate (CA certificate) to verify the origin of a signed digital certificate. When an application receives a signed certificate from another application, it uses a CA certificate to verify the certificate originator. A certificate authority can be:

- Well-known and widely used by other organizations.
- Local to a specific region or a company.

Many applications, such as Web browsers, use the CA certificates of well-known certificate authorities. Using a well-known CA eliminates or reduces the task of distributing CA certificates throughout the security zones in a network.

Private keys, public keys, and digital certificates:

Keys, digital certificates, and trusted certificate authorities establish and verify the identities of applications.

SSL uses public key encryption technology for authentication. In public key encryption, a public key and a private key are generated for an application. The data encrypted with the public key can only be decrypted with corresponding private key. Similarly, the data encrypted with the private key can only be decrypted by using the corresponding public key. The private key is password-protected in a key database file. Only the owner can access the private key to decrypt messages that are encrypted with the corresponding public key.

A signed digital certificate is an industry-standard method of verifying the authenticity of an entity, such as a server, a client, or an application. To ensure maximum security, a third-party certificate authority provides a certificate. A certificate contains the following information to verify the identity of an entity:

Organizational information
This section of the certificate contains information that uniquely identifies the owner of the certificate, such as organizational name and address. You supply this information when you generate a certificate with a certificate management utility.

Public key
The receiver of the certificate uses the public key to decipher encrypted text sent by the certificate owner to verify its identity. A public key has a corresponding private key that encrypts the text.

Certificate authority's distinguished name
The issuer of the certificate identifies itself with this information.

Digital signature
The issuer of the certificate signs it with a digital signature to verify its authenticity. The corresponding CA certificate compares the signature to verify that the certificate is originated from a trusted certificate authority.

Web browsers, servers, and other SSL-enabled applications accept as genuine any digital certificate that is signed by a trusted certificate authority and is otherwise valid. For example, a digital certificate can be invalidated for the following reasons:

- The digital certificate has expired.
- The CA certificate that is used to verify it has expired.
- The distinguished name in the digital certificate of the server does not match with the distinguished name specified by the client.

Self-signed certificates:

You can use self-signed certificates to test an SSL configuration before you create and install a signed certificate provided by a certificate authority.

A self-signed certificate contains a public key, information about the certificate owner, and the owner signature. It has an associated private key; however, it does not verify the origin of the certificate through a third-party certificate authority. After you generate a self-signed certificate on an SSL server application, you must:

1. Extract it.
2. Add it to the certificate registry of the SSL client application.

This procedure is equivalent to installing a CA certificate that corresponds to a server certificate. However, you do not include the private key in the file when you extract a self-signed certificate to use as the equivalent of a CA certificate.

Use a key management utility to:

- Generate a self-signed certificate.
- Generate a private key.
- Extract a self-signed certificate.
- Add a self-signed certificate.

Usage of self-signed certificates depends on your security requirements. To obtain the highest level of authentication between critical software components, do not

use self-signed certificates or use them selectively. You can authenticate applications that protect server data with signed digital certificates. You can use self-signed certificates to authenticate Web browsers or adapters.

If you are using self-signed certificates, you can substitute a self-signed certificate for a certificate and CA certificate pair.

Certificate and key formats:

Certificates and keys are stored in the files with the following formats:

.pem format

A privacy-enhanced mail (.pem) format file begins and ends with the following lines:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

A `.pem` file format supports multiple digital certificates, including a certificate chain. If your organization uses certificate chaining, use this format to create CA certificates.

.arm format

An `.arm` file contains a base-64 encoded ASCII representation of a certificate, including its public key, not a private key. The `.arm` file format is generated and used by the IBM Key Management utility.

.der format

A `.der` file contains binary data. You can use a`.der` file for a single certificate, unlike a `.pem` file, which can contain multiple certificates.

.pfx format (PKCS12)

A PKCS12 file is a portable file that contains a certificate and a corresponding private key. Use this format to convert from one type of SSL implementation to another. For example, you can create and export a PKCS12 file with the IBM Key Management utility. You can then import the file to another workstation with the certTool utility.

The use of SSL authentication:

When you start the adapter, it loads the available connection protocols.

The DAML protocol is the only available protocol that supports SSL authentication. You can specify DAML SSL implementation.

The DAML SSL implementation uses a certificate registry to store private keys and certificates. The certTool key and certificate management tool manages the location of the certificate registry. You do not need to specify the location of the registry when you perform certificate management tasks.

For more information, see “Changing protocol configuration settings” on page 29.

Configuring certificates for SSL authentication:

Use the following procedures to configure the adapter for one-way or two-way SSL authentication with signed certificates.

About this task

Use the certTool utility for these tasks:

- "Configuring certificates for one-way SSL authentication"
- "Configuring certificates for two-way SSL authentication" on page 61
- "Configuring certificates when the adapter operates as an SSL client" on page 62

Configuring certificates for one-way SSL authentication:

In this configuration, the IBM Security Identity Manager server and the IBM Security Identity Manager adapter use SSL.

About this task

Client authentication is not set on either application. The IBM Security Identity Manager server operates as the SSL client and initiates the connection. The adapter operates as the SSL server and responds by sending its signed certificate to the IBM Security Identity Manager server. The IBM Security Identity Manager server uses the installed CA certificate to validate the certificate sent by the adapter.

In Figure 2, Application A operates as the IBM Security Identity Manager server, and Application B operates as the IBM Security Identity Manager adapter.

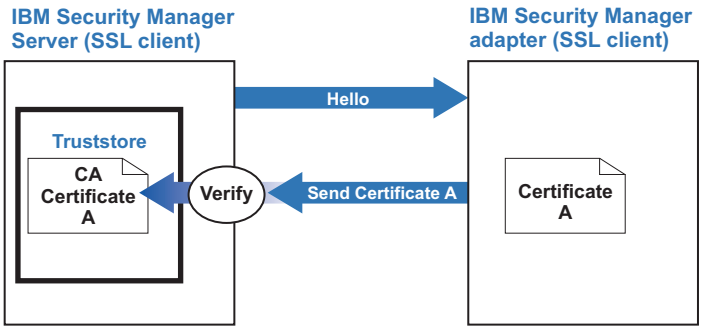


Figure 2. One-way SSL authentication (server authentication)

To configure one-way SSL, perform the following tasks for each application:

Procedure

1. On the adapter, complete these steps:
   a. Start the certTool utility. .
   b. To configure the SSL-server application with a signed certificate issued by a certificate authority:
      1) Create a certificate signing request (CSR) and private key. This step creates the certificate with an embedded public key and a separate private key and places the private key in the PENDING_KEY registry value.
      2) Submit the CSR to the certificate authority by using the instructions supplied by the CA. When you submit the CSR, specify that you want the root CA certificate returned with the server certificate.
2. On the IBM Security Identity Manager server, perform one of these steps:

- If you used a signed certificate issued by a well-known CA:
  a. Ensure that the IBM Security Identity Manager server has stored the root certificate of the CA (CA certificate) in its keystore.
  b. If the keystore does not contain the CA certificate, extract the CA certificate from the adapter and add it to the keystore of the server.
- If you generated the self-signed certificate on the IBM Security Identity Manager server, the certificate is installed and requires no additional steps.
- If you generated the self-signed certificate with the key management utility of another application:
  a. Extract the certificate from the keystore of that application.
  b. Add it to the keystore of the IBM Security Identity Manager server.

"Starting certTool" on page 64
Use the certTool utility to generate a private key and certificate request, install and delete certificates, register and unregister certificates, and list certificates.

Configuring certificates for two-way SSL authentication:

In this configuration, the IBM Security Identity Manager server and adapter use SSL.

Before you begin

Before performing the following procedure, configure the adapter and IBM Security Identity Manager server for one-way SSL authentication. If you use signed certificates from a CA:

- The CA provides a configured adapter with a private key and a signed certificate.
- The signed certificate of the adapter provides the CA certification for the IBM Security Identity Manager server.

About this task

The adapter uses client authentication. After sending its certificate to the server, the adapter requests identity verification from the server. The server sends its signed certificate to the adapter. Both applications are configured with signed certificates and corresponding CA certificates.

In Figure 3 on page 62, the IBM Security Identity Manager server operates as Application A and the IBM Security Identity Manager adapter operates as Application B.

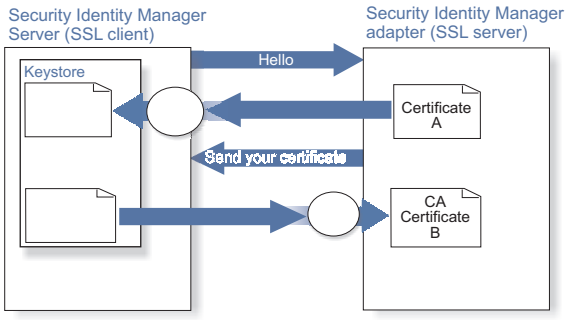


Figure 3. Two-way SSL authentication (client authentication)

Procedure

1. On the IBM Security Identity Manager server:
   a. Create a CSR and private key.
   b. Obtain a certificate from a CA.
   c. Install the CA certificate.
   d. Install the newly signed certificate.
   e. Extract the CA certificate to a temporary file.
2. On the adapter, add the CA certificate that was extracted from the keystore of the IBM Security Identity Manager server to the adapter.

Results

After configuring the two-way certificate, each application has its own certificate and private key. Each application also has the certificate of the CA that issued the certificates.

Related tasks:

"Configuring certificates for one-way SSL authentication" on page 60
In this configuration, the IBM Security Identity Manager server and the IBM Security Identity Manager adapter use SSL.

Configuring certificates when the adapter operates as an SSL client:

In this configuration, the adapter operates as both an SSL client and as an SSL server.

About this task

This configuration applies if the adapter initiates a connection to the web server (used by the IBM Security Identity Manager server) to send an event notification. For example, the adapter initiates the connection and the web server responds by presenting its certificate to the adapter.

Figure 4 on page 63 describes how the adapter operates as an SSL sever and an SSL client. When communicating with the IBM Security Identity Manager server, the adapter sends its certificate for authentication. When communicating with the web server, the adapter receives the certificate of the web server.

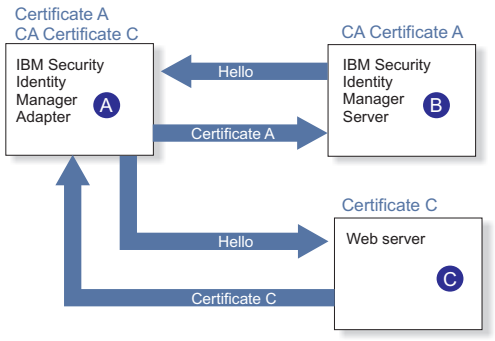


Figure 4. Adapter operating as an SSL server and an SSL client

If the web server is configured for two-way SSL authentication, it verifies the identity of the adapter. The adapter sends its signed certificate to the web server (not shown in the illustration). To enable two-way SSL authentication between the adapter and web server, perform the following process:

Procedure

1. Configure the web server to use client authentication.
2. Follow the procedure for creating and installing a signed certificate on the web server.
3. Install the CA certificate on the adapter with the certTool utility.
4. Add the CA certificate corresponding to the signed certificate of the adapter to the web server.

What to do next

If you want the software to send an event notification when the adapter initiates a connection to the web server (used by the IBM Security Identity Manager server), see the *IBM Security Identity Manager Information Center*.

Using the certTool utility to manage SSL certificates

The procedures in this section describe how to use the certTool utility to manage private keys and certificates.

About this task

This section includes instructions for performing the following tasks:

- "Starting certTool" on page 64.
- "Generating a private key and certificate request" on page 65.
- "Installing the certificate" on page 67.
- "Installing the certificate and key from a PKCS12 file" on page 67.
- "Viewing the installed certificate" on page 68.
- "Viewing CA certificates" on page 68.
- "Installing a CA certificate" on page 68.
- "Deleting a CA certificate" on page 69.
- "Viewing registered certificates" on page 70.
- "Registering a certificate" on page 69.
- "Unregistering a certificate" on page 70.

Starting certTool:

Use the certTool utility to generate a private key and certificate request, install and delete certificates, register and unregister certificates, and list certificates.

About this task

From the Main menu of the certTool utility, you can:

- Generate a CSR and install the returned signed certificate on the adapter.
- Install root CA certificates on the adapter.
- Register certificates on the adapter.

To start the certificate configuration tool, certTool, for the adapter, complete these steps:

Procedure

1. Log on to the adapter.
2. For UNIX based operating systems, change to the read/write `/bin` directory for the adapter. For example, if the adapter directory is in the default location, type the command: `cd /var/ibm/isim/bin`
3. Type certTool at the prompt. The Main menu is displayed:

```
Main menu - Configuring agent: adapter_name
 ------------------------------
A. Generate private key and certificate request
B. Install certificate from file
C. Install certificate and key from PKCS12 file
D. View current installed certificate

E. List CA certificates
F. Install a CA certificate
G. Delete a CA certificate

H. List registered certificates
I. Register certificate
J. Unregister a certificate

K. Export certificate and key to PKCS12 file

X. Quit

Choice:
```

What to do next

From the Main menu, you can generate a private key and certificate request, install and delete certificates, register and unregister certificates, and list certificates. The following sections summarize the purpose of each group of options.

By using the first set of options (A through D), you can generate a CSR and install the returned signed certificate on the adapter.

A. Generate private key and certificate request
Generate a CSR and the associated private key that is sent to the certificate authority.

B. Install certificate from file
Install a certificate from a file. This file must be the signed certificate returned by the CA in response to the CSR that is generated by option A.

C. Install certificate and key from a PKCS12 file
Install a certificate from a PKCS12 format file that includes both the public certificate and a private key. If options A and B are not used to obtain a certificate, the certificate that you use must be in PKCS12 format.

D. View current installed certificate
View the certificate that is installed on the workstation where the adapter is installed.

The second set of options installs the root CA certificates on the adapter. A CA certificate validates the corresponding certificate presented by a client, such as the server.

E. List CA certificates
Show the installed CA certificates. The adapter communicates only with servers whose certificates are validated by one of the installed CA certificates.

F. Install a CA certificate
Install a new CA certificate so that certificates generated by this CA can be validated. The CA certificate file can either be in X.509 or PEM encoded formats. .

G. Delete a CA certificate
Remove one of the installed CA certificates.

Options H through K apply to adapters that must authenticate the application to which the adapter is sending information. An example of an application is the IBM Security Identity Manager server or the web server. Use these options to register certificates on the adapter. For IBM Security Identity Manager version 4.5 or earlier, register the signed certificate of the IBM Security Identity Manager server with an adapter to enable client authentication on the adapter. If you do not upgrade an existing adapter to use CA certificates, you must register the signed certificate presented by the server with the adapter.

You must install the CA certificate corresponding to the signed certificate of the IBM Security Identity Manager server to either:

- Configure the adapter for event notification.
- Enable client authentication in DAML.

Use option F, Install a CA certificate.

H. List registered certificates
List all registered certificates that are accepted for communication.

I. Register a certificate
Register a new certificate. The certificate for registration must be in Base 64 encoded X.509 format or PEM.

J. Unregister a certificate
Unregister (remove) a certificate from the registered list.

K. Export certificate and key to PKCS12 file
Export a previously installed certificate and private key. You are prompted for the file name and a password for encryption.

Generating a private key and certificate request:

Use the certTool utility to generate a private key and certificate request for secure communication between the adapter and IBM Security Identity Manager.

About this task

A certificate signing request is an unsigned certificate that is a text file. When you submit an unsigned certificate to a certificate authority, the CA signs the certificate with the private digital signature that is included in their corresponding CA certificate. When the certificat signing request (CSR) is signed, it becomes a valid certificate. A CSR contains information about your organization, such as the organization name, country, and the public key for your web server.

To generate a CSR file, perform these steps:

Procedure

1. At the Main menu of the certTool utility, type `A` to display the following message and prompt:

```
Enter values for certificate request (press enter to skip value)
---------------------------------------------------------------
```

2. At **Organization**, type your organization name and press Enter.
3. At **Organizational Unit**, type the organizational unit and press Enter.
4. At **Agent Name**, type the name of the adapter for which you are requesting a certificate and press Enter.
5. At **Email**, type the email address of the contact person for this request and press Enter.
6. At **State**, type the state in which the adapter resides and press Enter. For example, type TX if the adapter is in Texas. Some certificate authorities do not accept two letter abbreviations for states; type the full name of the state.
7. At **Country**, type the country in which the adapter resides and press Enter.
8. At **Locality**, type the name of the city in which the adapter resides and press Enter.
9. At **Accept these values**, perform one of the following actions and press Enter:
   - Type `Y` to accept the displayed values.
   - Type `N` and specify different values.

   The private key and certificate request are generated after the values are accepted.
10. At **Enter name of file to store PEM cert request**, type the name of the file and press Enter. Specify the file that you want to use to store the values you specified in the previous steps.
11. Press Enter to continue. The certificate request and input values are written to the file you specified. The file is copied to the adapter `data` directory and the Main menu is displayed again.

What to do next

You can now request a certificate from a trusted CA by sending the `.pem` file that you generated to a certificate authority vendor.

Example of certificate signing request:

Your CSR file looks similar to the following example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwgZUxEjAQBgNVBAoTCWFjY2VzczM2MDEUMBIGA1UECxMLZW5n
aW5lZXJpbmcxEDAOBgNVBAMTB250YWdlbnQxJDAiBgkqhkiG9w0BCQEWFW50YWdl
```

```
bnRAYWNjZXNzMzYwLmNvbTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Ju
aWExDzANBgNVBAcTBklydmluZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
mR6AcPnwf6hLLc72BmUkAwaXcebtxCoCnnTH9uc8VuMHPbIMAgjuC4s91hPrilG7
UtlbOfy6X3R3kbeR8apRR9uLYrPIvQ1b4NK0whsytij6syCySaFQIB6V7RPBatFr
6XQ9hpsARdkGytZmGTgGTJ1hSS/jA6mbxpgmttz9HPECAwEAAaAAMA0GCSqGSIb3
DQEBAgUAA4GBADxA1cDkvXhgZntHkwT9tCTqUNV9sim8N/U15HgMRh177jVaHJqb
N1Er46vQSsOOOk4z2i/XwOmFkNNTXRVl9TLZZ/D+9mGZcDobcO+lbAKlePwyufxK
Xqdpu3d433H7xfJJSNYLYBFkrQJesITqKft0Q45gIjywIrbctVUCepL2
 -----END CERTIFICATE REQUEST-----
```

Installing the certificate:

Use the certTool utility to install the certificate on the adapter.

About this task

After you receive your certificate from your trusted CA, you must install it in the registry of the adapter.

To install the certificate, complete these steps:

Procedure

1. If you received the certificate as part of an email message, perform the following actions:
   a. Copy the text of the certificate to a text file.
   b. Copy that file to the readwrite data directory of the adapter. For example:`/var/ibm/isim`*`agent`*`/data`
2. At the Main menu of the certTool utility, type `B`. The following prompt is displayed:

   ```
   Enter name of certificate file:
   -----------------------------------------------
   ```
3. At **Enter name of certificate file**, type the full path to the certificate file and press **Enter**.

Results

The certificate is installed in the registry for the adapter, and the Main menu is displayed again.

Installing the certificate and key from a PKCS12 file:

If the certTool utility did not generate a CSR to obtain a certificate, you must install both the certificate and private key.

About this task

Store the certificate and the private key in a PKCS12 file. The CA sends a PKCS12 file that has a `.pfx` extension. The file might be a password-protected file and it includes both the certificate and private key.

To install the certificate from the PKCS12 file, complete these steps:

Procedure

1. Copy the PKCS12 file to the `data` directory of the adapter.
2. At the Main menu of the certTool utility, type `C`. The following prompt is displayed:

```
Enter name of PKCS12 file:
---------------------------------------------
```

3. At **Enter name of PKCS12 file**, type the full path to the PKCS12 file that has the certificate and private key information and press **Enter**. For example, `DamlSrvr.pfx`.
4. At **Enter password**, type the password to access the file and press **Enter**.

Results

After installing the certificate and private key in the adapter registry, the certTool utility displays the Main menu.

Viewing the installed certificate:

To list the certificate on your workstation, type D at the Main Menu of certTool.

About this task

The utility displays the installed certificate and the Main Menu. The following example shows an installed certificate:

```
The following certificate is currently installed.
Subject: c=US,st=California,l=Irvine,o=DAML,cn=DAML Server
```

Installing a CA certificate:

Use the certTool utility to install root CA certificates on the adapter.

About this task

If you use client authentication, you must install a CA certificate that is provided by a certificate authority vendor.

To install a CA certificate that was extracted in a temporary file, complete the following steps:

Procedure

1. At **Main Menu**, type `F` (Install a CA certificate). The following prompt is displayed:

   ```
   Enter name of certificate file:
   ```

2. At **Enter name of certificate file**, type the name of the certificate file, such as `CAcert.der` and press Enter. The certificate file opens and the following prompt is displayed:

   ```
   e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   Install the CA? (Y/N)
   ```

3. At **Install the CA**, type `Y` to install the certificate and press Enter.

Results

The certificate file is installed in the `DamlCACerts.pem` file.

Viewing CA certificates:

Use the certTool utility to view a private key and certificate that have been installed the adapter.

About this task

The certTool utility installs only one certificate and one private key.

To list the CA certificate on the adapter,

Procedure

Type **E** at the **Main menu** prompt.

Results

The certTool utility displays the installed CA certificates and the Main menu. The following example shows an installed CA certificate:

```
Subject: o=IBM,ou=SampleCACert,cn=TestCA
Valid To: Wed Jul 26 23:59:59 2006
```

Deleting a CA certificate:

To delete a CA certificate from the adapter directories, complete the following steps:

Procedure

1. At **Main Menu**, type **G** to display a list of all CA certificates installed on the adapter.

   ```
   0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support
   Enter number of CA certificate to remove:
   ```

2. At **Enter number of CA certificate to remove**, type the number of the CA certificate that you want to remove and press **Enter**.

Results

After deleting the CA certificate from the `DamlCACerts.pem` file, the certTool utility displays the Main menu.

Registering a certificate:

Use the certTool utility to register certificates on the adapter when the adapter must authenticate to an application.

About this task

Adapters that must authenticate to the application to which it is sending information must have a registered certificate. An example of an application is the IBM Security Identity Manager server or the webserver. Use this task to register certificates on the adapter. For IBM Security Identity Manager version 4.5 or earlier, register the signed certificate of the IBM Security Identity Manager server with an adapter to enable client authentication on the adapter. If you do not upgrade an existing adapter to use CA certificates, you must register the signed certificate presented by the server with the adapter. To register a certificate for the adapter, complete the following steps:

.

Procedure

1. At **Main Menu**, type **I** to display the following prompt:

   ```
   Enter name of certificate file:
   ```

2. At **Enter name of certificate file**, type the name of the certificate file that you want to register and press **Enter**. The subject of the certificate is displayed, and a prompt is displayed, for example:

   ```
   e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   Register this CA? (Y/N)
   ```

3. At **Register this CA**, type **Y** to register the certificate, and press **Enter**.

Results

After registering the certificate to the adapter, the certTool displays the Main menu.

Viewing registered certificates:

The adapter accepts only the requests that present a registered certificate when client validation is enabled.

Procedure

To view a list of all registered certificates, type **H** on the **Main Menu**.
The utility displays the registered certificates and the Main Menu. The following example shows a list of the registered certificates:

```
0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support
```

Unregistering a certificate:

To unregister a certificate for the adapter, perform the following steps:

Procedure

1. At **Main Menu**, type **J** to display the registered certificates. The following example shows a list of lists registered certificates:

   ```
   0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support
   ```

2. Type the number of the certificate file that you want to unregister and press **Enter**. For example:

   ```
   e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   Unregister this CA? (Y/N)
   ```

3. At **Unregister this CA**, type **Y** to unregister the certificate and press **Enter**.

Results

After removing the certificate from the list of registered certificate for the adapter, the certTool utility displays the Main menu.

Exporting a certificate and key to PKCS12 file:

To export a certificate and key to a PKCS12 file, perform the following steps:

Procedure

1. At **Main Menu**, type **K** to display the following prompt:

   ```
   Enter name of PKCS12 file:
   ```

2. At **Enter name of PKCS12 file**, type the name of the PKCS12 file for the installed certificate or private key and press **Enter**.
3. At **Enter Password**, type the password for the PKCS12 file and press **Enter**.
4. At **Confirm Password**, type the password again and press **Enter**.

Results

After exporting the certificate or private key to the PKCS12 file, the certTool displays the Main menu.

Chapter 5. Troubleshooting the RACF Adapter errors

Troubleshooting is the process of determining why a product does not function as it is designed to function. This topic provides information and techniques for identifying and resolving problems related to the RACF Adapter.

Note: If a problem is encountered, enable all levels of activity logging (debug, detail, base, and thread). The adapter log contains the main source of troubleshooting information. See "Changing **activity logging** settings" on page 44.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of

tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see Appendix E, "Support information," on page 117.

Warning and error messages

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

The following table contains warnings or errors that might be displayed on the user interface if the adapter is installed on your workstation.

Table 22. Error messages, warnings, and corrective actions

Error message or warning	Additional warnings, messages, or information	Corrective action
CTGIMU107W `The connection to the specified service cannot be established. Verify the service information, and try again.`	An IO error occurred while sending a request. Error: `Connection refused: connect`	Ensure that the adapter service is running. For more information about starting the adapter service, see "Starting and stopping the adapter" on page 16.
	The adapter returned an error status for a bind request. Status code: invalid credentials Adapter error message: `Authentication Failed`	Check the adapter authentication ID and password match the installed values. See the screen for Adapter-specific parameters in the task"Running the ISPF dialog" on page 8.
	An IO error occurred while sending a request. Error: `com.ibm.daml.jndi. JSSESocketConnection .HANDSHAKE_FAILED:`	If SSL is enabled, check the configuration. See . The adapter log contains details about the certificates loaded during initialization.
CTGIMD810E `The adapter returned an error status for a` *`xxxxx`* `request. Status code: failure Adapter error message: racfxxxx: Unable to create APPC transaction.`		See "APPC problems" on page 76.

Table 22. Error messages, warnings, and corrective actions (continued)

Error message or warning	Additional warnings, messages, or information	Corrective action
.	User *user name* add Successful. Some attributes could not be modified. : *attr1,attr2*	An attempt is made to add a user account. However, certain attributes are not set during the user add operation. For more information, see the adapter log file at `/var/ibm/isimracf/log/racfagent.log`. The log file contains information about the attributes that are not set during the user add operation.
	User *user name* modify Successful. Some attributes could not be modified. : *attr1,attr2*	An attempt is made to modify a user account. However, certain attributes failed during the modify operation. For more information, see the adapter log file at `/var/ibm/isimracf/log/racfagent.log`. The log file contains information about the attributes that are not set during the modify operation.
`CTGIMD812E An error occurred while processing the adapter response message. The following error occurred. Error: Premature end of file.`		Ensure that the adapter service is running. For more information about starting the adapter service, see "Starting and stopping the adapter" on page 16

APPC problems

Use this procedure to troubleshoot errors encountered with the Advanced Program to Program Communication.

Before you begin

APPC/MVS and ASCH must be started before starting the adapter task.

Procedure

1. Ensure that the APPC/MVS and the ASCH address spaces are started. For example, to start the APPC/MVS and ASCH address spaces issue these commands:

   ```
   S APPC,APPC=00,SUB=MSTR
   S ASCH,ASCH=00,SUB=MSTR
   ```

2. Ensure that APPC and ASCH are using the members APPCPMxx and ASCHPMxx as expected. You can check the system log to see which members are loaded.
3. Check that the scheduler class specified in the installation is defined to the APPC/MVS transaction scheduler. The command **D ASCH,ALL** shows all the active classes. These commands display the active parameters for APPC and ASCH:

```
D APPC,LU,ALL
D ASCH,ALL
D NET,E,ID=ISIMORIG
D NET,E,ID=ISIMDEST
```

4. Check that the APPCLU profile is correctly defined to RACF. See "Configuring RACF access" on page 17.
5. Check the z/OS System log for RACF authorization error messages around the time of the APPC error. An APPC error might be caused by a lack of authorization to:
   - The installation LOAD and EXEC data sets
   - The VSAM file for scoped reconciliation
   - The RACF database

   The RACF ID must have update access to the RACF database to perform a reconciliation operation. This access is a requirement of the utility IRRDBU00.

   Note: If the requester ID on the service form is being used, then you must permit the relevant authority for the SURROGAT resource. See "Surrogate user ID" on page 20.

Adapter log files

When the adapter is initially configured, a default directory is selected to store the log files, which contain activity from the adapter.

The log files are kept in the UNIX System Services file system, under the installation path of the adapter, in the read/write `log` subdirectory.

The adapter log name is the adapter instance name, followed by an extension of `.log`. When the extension is `.log`, it is the current log file. Old log files have a different extension, for example, *.log_001*, *.log_002*, and *.log_003*.

For example, an installation path name for the read/write directory is `/usr/itim`, and the adapter name configured is `RACFAgent`. The log files are then in the `/usr/itim/log/` directory. One or more files named `RACFAgent.log` exist. For example:

- `RACFAgent.log_001`
- `RACFAgent.log_002`
- `RACFAgent.log_003`

You might use the UNIX System Services **`obrowse`** command **`tail`**, or any other UNIX based utility to inspect these adapter logs.

The size of a log file, the number of log files, the directory path, and the detailed level of logging are configured with the `agentCfg` program. For more information, see "Configuring the adapter for IBM Security Identity Manager" on page 27.

RACF/SSL adapter information to be gathered for support requests

This information assumes specifications for VTAM APPLIDs and user IDs indicated in the installation guide.

Replace these APPLIDs and user IDs with those IDs you selected for the adapter installation.

- The RACF Adapter log file, from the z/OS UNIX System Services file system.

- An excerpt from the MVS SYSTEM log, from the same time frame as the failure.
- A screen capture of the ISIM service form, describing the connection to this adapter.
- A display from the adapter utility `agentCfg` describing the adapter parameters:

  F. Registry Settings. -> A. Modify Non-encrypted registry settings
- The results from MVS console command: `D APPC,LU,ALL`
- The results from MVS console command: `D ASCH,ALL`
- If the APPC/MVS logical units are left unspecified, then only one logical unit is used for both sides of the conversation. The LU to be displayed is defined in APPCPMxx with the BASE keyword, indicating it is the BASE LU. The *baselu* name is indicated by the command `D APPC,LU,ALL`. From the resulting display, one of the LUs is indicated as `BASE=YES`.
  - The results from MVS console command: `D NET,E,ID=`*baselu*
- If the APPC/MVS logical units are defined to the adapter:
  - The results from MVS console command: `D NET,E,ID=ISIMORIG`
  - The results from MVS console command: `D NET,E,ID=ISIMDEST`
- The APPC/MVS configuration definition (SYS1.PARMLIB(APPCPMxx) member. (Replace the data set name and member name suffix with the ones that define where the client stores this definition.)
- The APPC/MVS Address space scheduler definition (SYS1.PARMLIB(ASCHPMxx) member. (Replace the data set name and member name suffix with the ones that define where the client stores this definition.)
- The VTAM APPL definitions for ISIMORIG and ISIMDEST, from the VTAMLST data set. If the BASE LU is the only LU used, include the VTAMLST definition for this LU.
- The VTAM mode table entry or entries used in the VTAM APPL definitions. If an IBM standard mode table entry from ISTINCLM is used, this information is not necessary.
- The results from the following job (include all the output produced). A RACF administrator with authority to view all the indicated profiles must run this job. Specify your VTAM Network ID where netid is shown. (You can find the NETID from the display command `D NET,E,ID=ISTNOP`, where the line for message IST599I indicates the `netid.hostpu`.)

```
//RACFLIST JOB ACCT,IBM,CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//TMP EXEC PGM=IKJEFT01,REGION=0K
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
/* if NO LUs are defined to the adapter, the BASE LU is utilized */
/* the profile listed should be as follows:
RLIST APPCLU netid.baselu.baselu SESSION NORACF
/* if defaulted or specified NONQN in APPCPMxx */
RLIST APPCLU netid.ISIMORIG.ISIMDEST SESSION NORACF
/* if defaulted or specified NONQN in APPCPMxx*/
RLIST APPCLU netid.ISIMDEST.ISIMORIG SESSION NORACF
/* if NQN specified in APPCPMxx */
RLIST APPCLU netid.ISIMORIG.netid.ISIMDEST SESSION NORACF
/* if NQN specified in APPCPMxx */
RLIST APPCLU netid.ISIMDEST.netid.ISIMORIG SESSION NORACF
/* If this is not the correct STARTED class profile for ISIAGNT, */
/* please correct */
RLIST STARTED ISIAGNT.* STDATA NORACF
/* The following list command is only necessary IF you specify */
/* the field "RACF ID under which requests will be processed" */
/* on the ISIM RACF service form, within ISIM. */
RLIST SURROGAT ATBALLC.ISIM001 ALL
RLIST APPCPORT ISIMORIG ALL
```

```
RLIST APPCPORT ISIMDEST ALL
/* I expect this is not defined, but want to include it, in case it exists */
RLIST APPL ISIMORIG ALL
/* I expect this is not defined, but want to include it, in case it exists */
RLIST APPL ISIMDEST ALL
/* Specify the RACF user ID the adapter runs as below */
LISTUSER ISIAGNT OMVS
/* IF a user ID is specified on the ISIM service form in the field */
/* "RACF ID under which requests will be processed", replace ISIM001 with */
/* that user ID. */
LISTUSER ISIM001 OMVS
/* To display active and RACLISTed classes */
SETROPTS LIST
```

- The results from the following job (all the output produced, including the JCL). Replace the transaction data set file with your installation VSAM file name, and modify the job statement as necessary:

```
//APPCLIST JOB ACCT,IBM,CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
//ATBSDFMU EXEC PGM=ATBSDFMU
//SYSPRINT DD SYSOUT=*
//SYSSDLIB DD DISP=SHR,
//            DSN=your.appc.trans.action.profile.VSAM.dataset
//SYSSDOUT DD SYSOUT=*
//SYSIN    DD *
     TPKEYS
     TPRETRIEVE
          TPNAME(ISIMCMD)
          SYSTEM
     TPRETRIEVE
          TPNAME(ISIMRECO)
          SYSTEM
```

For information about obtaining support, see Appendix E, “Support information,” on page 117.

Chapter 6. Upgrading the adapter

For specific instructions about upgrading the adapter, see the adapter release notes.

Chapter 7. Uninstalling the adapter

Uninstalling the adapter involves several tasks, including removing the started task JCL and the directories from the UNIX System Services environment.

Procedure

1. Stop the adapter, if it is running. See "Starting and stopping the adapter" on page 16.
2. Remove the started task JCL from the system procedure library.
3. Remove the `read-only` and `read/write` directories from the z/OS UNIX System Services environment.
4. Remove the CNTL, EXEC, and LOAD libraries that are related to the adapter.
5. Remove the ISPF dialog libraries for customization.

Appendix A. Adapter attributes

A target platform requires certain information about the user before it can grant access to the user. This information is collected in the Access Request Form (a value for each attribute) during the Access Request process.

The information is sent to the adapter by the IBM Security Identity Manager server. The adapter uses these values to create the user access. Which attributes are needed depends upon the transaction requested, such as System Login Add or Database Login Change.

After the adapter software is installed on a platform and the adapter is defined by Agent Maintenance, you identify the attribute data needed to create the user access. You identify these attributes to IBM Security Identity Manager when defining the Access Request Form for access through Request Maintenance.

Adapter attributes by object

The following MVS RACF keywords can be used to create or modify RACF Access Request Forms. MVS RACF requires only a user ID, password, and Default Group for valid access. Be sure that you include these keywords when creating the MVS RACF Access Request Forms. A * denotes attributes for future release.

Note: Reconciliations return group data and user data.

erRacUser

This class represents a user account on the RACF database. There is one base user object for each user defined in a RACF database.

Table 23. Account form attributes

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required ?	Commands

erAccountStatus
 	
Whether this user is in REVOKED status, or not.
	String	5	Single	RW	No	To add or modify:
						`ALU userid REVOKE`
						
						To delete:
						`ALU userid RESUME`

erPassword
 	
Password of user. Must be alphanumeric, and can include '@#$'. Not case-sensitive.
	String	8	Single	RW	No	To add or modify:
						`ALU userid Password(value)`
						
						To delete:
						`ALU userid NOPASSWORD`

erRacExecName Exec name - not a RACF attribute, but for compatibility with old RASEXEC.	String	44	Single	W	No	To add or modify: `ISIMEXEC userid value`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands
erRacExecVar Exec Attribute - not a RACF attribute, but for compatibility with old RASEXEC.	String	44	Single	W	No	This argument is the second argument (*value*) to the ISIMEXEC call for erRacExecName.
erRacfRequester RACF ID of requesting user. The RACF ID is the ID of the person within IBM Security Identity Manager who is making the provisioning request.	String	8	Single	W	No	

erRacUClauth
 	
A list of RACF resource classes this user has rights to administer. Any class in the Class Descriptor Table (CDT), and USER is valid. GROUP and DATASET are invalid.
	String	8	Multiple	RW	No	To add or modify:
						`ALU` *`userid`* `CLAUTH(`*`value`*`)`
						
						To delete:
						`ALU` *`userid`* `NOCLAUTH(`*`value`*`)`

erRacUCreDate Date user was created.	Date		Single	R	No	
erRacUDfltgrp Name of existing group that is the initial and default group this user is associated with.	String	8	Single	RW	Yes	To add or modify: `ALU` *`userid`* `DFLTGRP(`*`value`*`)`

erRacUInstData
 	
Installation defined data that can be associated with a user.
	String	254	Single	RW	No	To add or modify:
						`ALU` *`userid`* `DATA('`*`value`*`')`
						
						To delete:
						`ALU` *`userid`* `NODATA`

erRacUIsADSP
 	
User can automatically create discrete data set profiles.
	String	5	Single	RW	No	To add or modify:
						`ALU` *`userid`* `ADSP`
						
						To delete:
						`ALU` *`userid`* `NOADSP`

erRacUIsAudit
 	
User has system auditor ability.
	String	5	Single	RW	No	To add or modify:
						`ALU` *`userid`* `AUDITOR`
						
						To delete:
						`ALU` *`userid`* `NOAUDITOR`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUIsCICSSeg
 	
CICS® segment is present.
 	
User CICS information. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. CICS this information assigns the user-specific characteristics.
	String	5	Single	RW	No	To add or modify:
						`ALU *userid* CICS`
						
						To delete:
						`ALU *userid* NOCICS`

erRacUCICSIsForc
 	
Whether this user is forced off if current system fails over to a backup system.
	String	5	Single	RW	No	To add or modify:
						`ALU *userid* CICS (XRFSOFF(FORCE))`
						
						To delete:
						`ALU *userid* CICS (XRFSOFF(NOFORCE))`

erRacUCICSOpclas
 	
Operator class. Valid values are 1 - 24.
	Integer	2	Multiple	RW	No	To add or modify:
						`ALU *userid* CICS (OPCLASS(*value*))`
						
						To delete:
						`ALU *userid* CICS (NOOPCLASS)`

erRacUCICSOpid
 	
Operator ID. 1 - 3 characters. Any value acceptable.
	String	3	Single	RW	No	To add or modify:
						`ALU *userid* CICS (OPID(*value*))`
						
						To delete:
						`ALU *userid* CICS (NOOPID)`

erRacUCICSPrty
 	
Operator priority, value can be 0 - 255.
	Integer	3	Single	RW	No	To add or modify:
						`ALU *userid* CICS (OPPRTY(*value*))`
						
						To delete:
						`ALU *userid* CICS (NOOPPRTY)`

erRacUCICSTimout
 	
User timeout value, in the form of HHMM.
	Time	4	Single	RW	No	To add or modify:
						`ALU *userid* CICS (TIMEOUT(*value*))`
						
						To delete:
						`ALU *userid* CICS (NOTIMEOUT)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUIsDCESeg
 	
DCE segment is present.
 	
DCE information. This information describes the user in the context of a DCE (Distributed Computing Environment). Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid DCE`
						
						To delete:
						`ALU userid NODCE`

erRacUDCEIsAutoL
 	
Whether this user is automatically identified to DCE through AUTOLOGIN or not.
	String	5	Single	RW	No	To add or modify:
						`ALU userid DCE (AUTOLOAD(YES))`
						
						To delete:
						`ALU userid DCE (NOAUTOLOAD)`

erRacUDCEHomeC
 	
DCE Home Cell name.
	String	1023	Single	RW	No	To add or modify:
						`ALU userid DCE (HOMECELL(value))`
						
						To delete:
						`ALU userid DCE (NOHOMECELL)`

erRacUDCEHomeU
 	
UUID for the cell that this user is defined to. String must have the delimiter of "-" in character positions 9, 14, 19, and 24. The general format for the UUID string is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, in which x represents a valid numeric or hexadecimal character.
	String	36	Single	RW	No	To add or modify:
						`ALU userid DCE (HOMEUUID(value))`
						
						To delete:
						`ALU userid DCE (NOHOMEUUID)`

erRacUDCEName
 	
DCE Principal name.
	String	1023	Single	RW	No	To add or modify:
						`ALU userid DCE (DCENAME(value))`
						
						To delete:
						`ALU userid DCE (NODCENAME)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUDCEUUID
 	
UUID of this instance of the user. This string must have the delimiter of "-" in character positions 9, 14, 19, and 24. The general format for the UUID string is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, in which x represents a valid numeric or hexadecimal character.
	String	36	Single	RW	No	To add or modify:
						`ALU userid DCE (UUID(value))`
						
						To delete:
						`ALU userid DCE (NOUUID)`

erRacUIsDFPSeg
 	
DFP segment is present.
 	
The following attributes are user DFP information. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. DFP uses this information to determine data management and disk storage characteristics when a user creates a data set.
	String	5	Single	RW	No	To add or modify:
						`ALU userid DFP`
						
						To delete:
						`ALU userid NODFP`

erRacUDFPAppl
 	
Name of a user-defined application.
	String	8	Single	RW	No	To add or modify:
						`ALU userid DFP (DATAAPPL(value))`
						
						To delete:
						`ALU userid DFP (NODATAAPPL)`

erRacUDFPData
 	
DATACLAS name to be used for new file creation.
	String	8	Single	RW	No	To add or modify:
						`ALU userid DFP (DATACLAS(value))`
						
						To delete:
						`ALU userid DFP (NODATACLAS)`

erRacUDFPMgmt
 	
MGMTCLAS name to be used for new file creation.
	String	8	Single	RW	No	To add or modify:
						`ALU userid DFP (MGMTCLAS(value))`
						
						To delete:
						`ALU userid DFP (NOMGMTCLAS)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUDFPStor
 	
STORCLAS name to be used for new file creation.
	String	8	Single	RW	No	To add or modify:
						`ALU userid DFP (STORCLAS(value))`
						
						To delete:
						`ALU userid DFP (NOSTORCLAS)`

erRacUIsEimSeg
 	
EIM segment is present.
 	
EnterPrise Identity Management (EIM). This object contains a name from the LDAPBIND general resource profile class, of the user as it is known to the Enterprise Identity Mapping environment. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid EIM`
						
						To delete:
						`ALU userid NOEIM`

erRacUEimLDAPNam
 	
Name of profile in the LDAPBIND class.
	String	246	Single	RW	No	To add or modify:
						`ALU userid EIM (LDAPPROF(value))`
						
						To delete:
						`ALU userid EIM (NOLDAPPROF)`

erRacUIsGrpacc
 	
Enables group level access of UPDATE to the group under the High Level Qualifier of any data set profile created through ADSP by this user.
	String	5	Single	RW	No	To add or modify:
						`ALU userid GRPACC`
						
						To delete:
						`ALU userid NOGRPACC`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUIsKerbSeg
 	
Kerberos segment is present.
 	
Kerberos information. This object describes Kerberos information that relates to this instance of the user. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid KERB`
						
						To delete:
						`ALU userid NOKERB`

erRacUKerbIsDES
 	
Single length DES keys allowed.
	String	5	Single	RW	No	To add or modify:
						`ALU userid KERB (ENCRYPT(DES))`
						
						To delete:
						`ALU userid KERB (ENCRYPT(NODES))`

erRacUKerbIsDES3
 	
Triple DES keys allowed.
	String	5	Single	RW	No	To add or modify:
						`ALU userid KERB (ENCRYPT(DES3))`
						
						To delete:
						`ALU userid KERB (ENCRYPT(NODES3))`

erRacUKerbIsDESD
 	
Double DES keys allowed.
	String	5	Single	RW	No	To add or modify:
						`ALU userid KERB (ENCRYPT(DESD))`
						
						To delete:
						`ALU userid KERB (ENCRYPT(NODESD))`

erRacUKerbName
 	
Kerberos Principal name. can consist of any character except the @+ (X'7C') character. Avoid the use of any of the EBCDIC variant characters to prevent problems between different code pages.
	String	240	Single	RW	Yes	To add or modify:
						`ALU userid KERB (KERBNAME(value))`
						
						To delete:
						`ALU userid KERB (NOKERBNAME)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUKerbTickMx
 	
Maximum ticket life, in seconds. Valid value range is 1 - 2,147,483,647.
	Integer	10	Single	RW	No	To add or modify:
						`ALU userid KERB (MAXTKT(value))`
						
						To delete:
						`ALU userid KERB (NOMAXTKT)`

erRacUIsLangSeg
 	
Language segment is present.
 	
User Language information. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid LANGUAGE`
						
						To delete:
						`ALU userid NOLANGUAGE`

erRacULangPrime
 	
Primary user language.
	String	3	Single	RW	No	To add or modify:
						`ALU userid LANG (PRIM(value))`
						
						To delete:
						`ALU userid LANG (NOPRIM)`

erRacULangSec
 	
Secondary user language.
	String	3	Single	RW	No	To add or modify:
						`ALU userid LANG (SEC(value))`
						
						To delete:
						`ALU userid LANG (NOSEC)`

erRacUIsLNotesSeg
 	
Lotus Notes® segment present.
 	
Lotus Notes information. This object contains a Lotus Notes short name, of the user as it is known to this RACF system. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid LNOTES`
						
						To delete:
						`ALU userid NOLNOTES`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacULnotesSNam
 	
Lotus Notes Short Name. You can specify the following characters: upper and lowercase letters (A -Z, and a -z), 0 -9, & (X'50'), - (X'60'), (X'4B'), _ (X'6D'), and (X'40'). The hex values shown are EBCDIC.
	String	64	Single	RW	No	To add or modify:
						`ALU userid LNOTES (SNAME(value))`
						
						To delete:
						`ALU userid LNOTES (NOSNAME)`

erRacUIsNetvSeg
 	
Tivoli NetView® for z/OS segment is present.
 	
Tivoli NetView for z/OS information. This object might be present. It contains attributes that describe this user instance in the IBM Tivoli NetView for z/OS environment. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid NETVIEW`
						
						To delete:
						`ALU userid NONETVIEW`

erRacUNetvCons
 	
Console name user assume when console commands are issued.
	String	8	Single	RW	No	To add or modify:
						`ALU userid NETV (CONSNAM(value))`
						
						To delete:
						`ALU userid NETV (NOCONSNAM)`

erRacUNetvCtl
 	
Only the specific values are allowed. Default is 'Specific'. Values allowed are: General Global Specific.
	String	8	Single	RW	No	To add or modify:
						`ALU userid NETV (CTL(value))`
						
						To delete:
						`ALU userid NETV (NOCTL)`

erRacUNetvDomain
 	
List of commands a NetView operator my run in another Tivoli NetView for z/OS Domain.
	String	5	Multiple	RW	No	To add or modify:
						`ALU userid NETV (DOMAIN(value))`
						
						To delete:
						`ALU userid NETV (NODOMAIN)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUNetvGSpan
 	
Not well documented. The best information found within Tivoli NetView for z/OS documentation indicates that this attribute is a maximum of 8 characters.
	String	8	Single	RW	No	To add or modify:
						`ALU userid NETV (NGMFVSPN(value))`
						
						To delete:
						`ALU userid NETV (NONGMFVSPN)`

erRacUNetvIC
 	
Initial command to be run when this NetView user enters the Tivoli NetView for z/OS subsystem.
	String	255	Single	RW	No	To add or modify:
						`ALU userid NETV (IC(value))`
						
						To delete:
						`ALU userid NETV (NOIC)`

erRacUNetvIsGMF
 	
Whether this user can use the Tivoli NetView for z/OS Graphic Monitor Facility or not.
	String	5	Single	RW	No	To add or modify:
						`ALU userid NETV (NGMFADMN(YES))`
						
						To delete:
						`ALU userid NETV (NONGMFADMN)`

erRacUNetvIsMR
 	
Whether this user can receive unsolicited messages or not.
	String	5	Single	RW	No	To add or modify:
						`ALU userid NETV (MSGRECVR(YES))`
						
						To delete:
						`ALU userid NETV (NOMSGRECVR)`

erRacUNetvOpclas
 	
Netview Operator classes. Can be values of 1 - 2040.
	Integer	4	Multiple	RW	No	To add or modify:
						`ALU userid NETV (OPCLASS(value))`
						
						To delete:
						`ALU userid NETV (NOOPCLASS)`

erRacUIsOMVSSeg
 	
OMVS segment is present.
 	
OMVS (UNIX) information. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid OMVS (`
						
						To delete:
						`ALU userid NOOMVS`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUOMVSCPU
 	
Maximum CPU time, in seconds, this user can accumulate before processes is purged. Valid value range 7 - 2,147,483,647.
	Integer	10	Single	RW	No	To add or modify:
						`ALU userid OMVS (CPUTIM(value))`
						
						To delete:
						`ALU userid OMVS (NOCPUTIM)`

erRacUOMVSFiles
 	
Maximum number of files per process. Valid value range is 3 - 262,143.
	Integer	6	Single	RW	No	To add or modify:
						`ALU userid OMVS (FILE(value))`
						
						To delete:
						`ALU userid OMVS (NOFILE)`

erRacUOMVSHome
 	
Home directory of user. Case sensitive. Path must be valid for user. Can use the shell.
	String	1024	Single	RW	No	To add or modify:
						`ALU userid OMVS (HOME(value))`
						
						To delete:
						`ALU userid OMVS (NOHOME)`

erRacUOMVSIsShar If not set, and the UID specified is already assigned, and Shared UID support is enabled, the UID assignment might fail.	String	5	Single	W	No	To add or modify: `ALU userid OMVS (UID(value)SHARED)`

erRacUOMVSMmap
 	
Maximum number of pages for memory mapped files. Valid value range is 1 - 16,777,216.
	Integer	8	Single	RW	No	To add or modify:
						`ALU userid OMVS (MMAP(value))`
						
						To delete:
						`ALU userid OMVS (NOMMAP)`

erRacUOMVSProc
 	
Maximum processes per user. Valid value range is 3 - 32,767.
	Integer	5	Single	RW	No	To add or modify:
						`ALU userid OMVS (PROC(value))`
						
						To delete:
						`ALU userid OMVS (NOPROC)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUOMVSShell
 	
Shell program for user. Case sensitive. Must be a valid shell name for user to use the shell. Must be a fully qualified name, because the environment has not yet been established.
	String	1024	Single	RW	No	To add or modify:
						`ALU userid OMVS (PROG(value))`
						
						To delete:
						`ALU userid OMVS (NOPROG)`

erRacUOMVSStor
 	
Maximum amount of storage, in bytes, this user can use. Valid value range is 10,485,760 - 2,147,483,647.
	Integer	10	Single	RW	No	To add or modify:
						`ALU userid OMVS (ASSIZE(value))`
						
						To delete:
						`ALU userid OMVS (NOASSIZE)`

erRacUOMVSThread
 	
Maximum number of threads per process. Valid value range is 0 - 100,000. Must be non-zero to allow use of ptthread_create.
	Integer	6	Single	RW	No	To add or modify:
						`ALU userid OMVS (THREAD(value))`
						
						To delete:
						`ALU userid OMVS (NOTHREAD)`

erRacUOMVSuid
 	
UNIX UID assigned to this user. Valid values are 0 - 2,147,483,647. Zero (0) means superuser.'*' means that the UID is automatically assigned. Specific profiles for AUTOUID support must be set up before its usage.
	String	10	Single	RW	No	To add or modify:
						`ALU userid OMVS (UID(value))`
						
						To delete:
						`ALU userid OMVS (NOUID)`

erRacUIsOper
 	
User has system Operations ability (ability to read/modify any file).
	String	5	Single	RW	No	To add or modify:
						`ALU userid OPERATIONS`
						
						To delete:
						`ALU userid NOOPERATIONS`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUIsOperSeg
 	
Operparm segment is present.
 	
Operparm information. Attributes describe settings as a system operator. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid OPERPARM`
						
						To delete:
						`ALU userid NOOPERPARM`

erRacUOpAltgrp
 	
Alternate Console group used in recovery.
	Character	8	Single	RW	No	To add or modify:
						`ALU userid OPERP (ALTGRP(value))`
						
						To delete:
						`ALU userid OPERP (NOALTGRP)`

erRacUOpAuth
 	
Console Authority. Valid values are:
• Master
• All
• Info
• Cons
• Io
• Sys
	Character	6	Single	RW	No	To add or modify:
						`ALU userid OPERP (AUTH(value))`
						
						To delete:
						`ALU userid OPERP (NOAUTH)`

erRacUOpAuto
 	
Whether the extended console can receive messages which have been automated by the MPF facility.
	String	5	Single	RW	No	To add or modify:
						`ALU userid OPERP (AUTO(YES))`
						
						To delete:
						`ALU userid OPERP (NOAUTO)`

erRacUOpCmdsys
 	
Console name or '*'. A-Z, 0-9, @, #, $ are valid values, in addition to '*'.
	Character	8	Single	RW	No	To add or modify:
						`ALU userid OPERP (CMDSYS(value))`
						
						To delete:
						`ALU userid OPERP (NOCMDSYS)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUOpDom
 	
Valid values are 'Normal', 'All', or 'None'.
	Character	6	Single	RW	No	To add or modify:
						`ALU userid OPERP (DOM(value))`
						
						To delete:
						`ALU userid OPERP (NODOM)`

erRacUOpKey
 	
1 - 8 character key to display information from all consoles with this key. Valid values are A-Z, 0-9, @, #, $.
	Character	8	Single	RW	No	To add or modify:
						`ALU userid OPERP (KEY(value))`
						
						To delete:
						`ALU userid OPERP (NOKEY)`

erRacUOpLevel
 	
Level of information that can be displayed. Valid values are:
• NB
• R
• CE
• E
• IN
• ALL
 	
If ALL is specified, no others can be specified.
	Character	3	Multiple	RW	No	To add or modify:
						`ALU userid OPERP (LEVEL(value))`
						
						To delete:
						`ALU userid OPERP (NOLEVEL)`

erRacUOpLogcmd
 	
Valid values are SYSTEM or NONE.
	String	5	Single	RW	No	To add or modify:
						`ALU userid OPERP (LOGCMDR(NO))`
						
						To delete:
						`ALU userid OPERP (NOLOGCMDR)`

erRacUOpMform
 	
Message form of the messages displayed upon the extended console. Valid values are:
• J
• M
• S
• T
• X
	Character	5	Multiple	RW	No	To add or modify:
						`ALU userid OPERP (MFORM(value))`
						
						To delete:
						`ALU userid OPERP (NOMFORM)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUOpMigid
 	
Whether a migration ID is to be assigned to this extended console.
	String	5	Single	RW	No	To add or modify:
						`ALU userid OPERP (MIGID(YES))`
						
						To delete:
						`ALU userid OPERP (NOMIGID)`

erRacUOpMonitor
 	
Valid values are:
• JOBNAMES or JOBNAMEST
• SESS or SESST
• STATUS
	Character	9	Multiple	RW	No	To add or modify:
						`ALU userid OPERP (MONITOR(value))`
						
						To delete:
						`ALU userid OPERP (NOMONITOR)`

erRacUOpMscope
 	
Valid system names for which messages can be received from. Valid values are system names, '*' and '*ALL'.
	Character	8	Multiple	RW	No	To add or modify:
						`ALU userid OPERP (MSCOPE(value))`
						
						To delete:
						`ALU userid OPERP (NOMSCOPE)`

erRacUOpRoutCode
 	
The Routing Codes this console is to receive. Value range is 1 - 128.
	Integer	3	Multiple	RW	No	To add or modify:
						`ALU userid OPERP (ROUTC(value))`
						
						To delete:
						`ALU userid OPERP (NOROUTCR)`

erRacUOpStor
 	
Valid value range is 1 - 2000.
	Integer	4	Single	RW	No	To add or modify:
						`ALU userid OPERP (STORAGE(value))`
						
						To delete:
						`ALU userid OPERP (NOSTORAGE)`

erRacUOpUD
 	
Whether this console is to receive undeliverable messages.
	String	5	Single	RW	No	To add or modify:
						`ALU userid OPERP (UD(YES))`
						
						To delete:
						`ALU userid OPERP (NOUD)`

erRacUIsProtect User cannot be signed on to with a password.	String	5	Single	RW	No	To add or modify: `ALU userid NOPASSWORD`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUIsPrxSeg
 	
PROXY segment is present.
 	
PROXY segment information. This object contains a name from the LDAPBIND general resource profile class, of the user as it is known to the Enterprise Identity Mapping environment. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid PROXY`
						
						To delete:
						`ALU userid NOPROXY`

erRacUPrxBindDN
 	
Bind DN of user on target host.
	Binary	1023	Single	RW	No	To add or modify:
						`ALU userid PROXY (BINDDN(value))`
						
						To delete:
						`ALU userid PROXY (NOBINDDN)`

erRacUPrxBindHst
 	
A URL of a host, which the local z/OS LDAP server contacts on behalf of the user.
	Binary	1023	Single	RW	No	To add or modify:
						`ALU userid PROXY (LDAPHOST(value))`
						
						To delete:
						`ALU userid PROXY (NOLDAPHOST)`

erRacUPrxBindPW
 	
Bind password for erRacUPrxBindDN.
	String	128	Single	W	No	To add or modify:
						`ALU userid PROXY (BINDPW(value))`
						
						To delete:
						`ALU userid PROXY (NOBINDPW)`

erRacUIsRestrict
 	
User cannot be granted access through UACC or ID(*) in resource profiles.
	String	5	Single	RW	No	To add or modify:
						`ALU userid RESTRICTED`
						
						To delete:
						`ALU userid NORESTRICTED`

erRacUIsSpecial
 	
User has system Special. System Security Administrator.
	String	5	Single	RW	No	To add or modify:
						`ALU userid SPECIAL`
						
						To delete:
						`ALU userid NOSPECIAL`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUIsTSOSeg
 	
TSO segment is present.
 	
User TSO information. Since this attribute is an optional object, its presence gives a user access to the time-sharing environment, even if all attribute values are null.
	String	5	Single	RW	No	To add or modify:
						`ALU userid TSO`
						
						To delete:
						`ALU userid NOTSO`

erRacUTSOAcct
 	
Name of a user-defined application.
	String	40	Single	RW	No	To add or modify:
						`ALU userid TSO (ACCT(value))`
						
						To delete:
						`ALU userid TSO (NOACCT)`

erRacUTSOCmd
 	
Initial command to be run upon connecting to TSO.
	String	80	Single	RW	No	To add or modify:
						`ALU userid TSO (COMMAND(value))`
						
						To delete:
						`ALU userid TSO (NOCOMMAND)`

erRacUTSODest
 	
Default destination for system output. Must begin with A-Z, @#$, remaining data can be numeric.
	String	8	Single	RW	No	To add or modify:
						`ALU userid TSO (DEST(value))`
						
						To delete:
						`ALU userid TSO (NODEST)`

erRacUTSOHold
 	
Default system output class for the held queue. Must be alphanumeric.
	String	1	Single	RW	No	To add or modify:
						`ALU userid TSO (HOLDCLASS(value))`
						
						To delete:
						`ALU userid TSO (NOHOLDCLASS)`

erRacUTSOMsg
 	
Default system output message class. Must be alphanumeric.
	String	1	Single	RW	No	To add or modify:
						`ALU userid TSO (MSGCLASS(value))`
						
						To delete:
						`ALU userid TSO (NOMSGCLASS)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required ?	Commands

erRacUTSOJob
 	
Default system job execution class. Must be alphanumeric.
	String	1	Single	RW	No	To add or modify:
						`ALU userid TSO (JOBCLASS(value))`
						
						To delete:
						`ALU userid TSO (NOJOBCLASS)`

erRacUTSOMax
 	
Maximum amount of storage user can request. Amount is specified in K bytes. Zero means no limit.
	Integer	7	Single	RW	No	To add or modify:
						`ALU userid TSO (MAXSIZE(value))`
						
						To delete:
						`ALU userid TSO (NOMAXSIZE)`

erRacUTSOProc
 	
Default TSO logon procedure. Must begin with A-Z, @#$, remaining data can be numeric.
	String	8	Single	RW	No	To add or modify:
						`ALU userid TSO (PROC(value))`
						
						To delete:
						`ALU userid TSO (NOPROC)`

erRacUTSOSize
 	
Requested amount of storage to be used by this session. Zero means no limit.
	Integer	7	Single	RW	No	To add or modify:
						`ALU userid TSO (SIZE(value))`
						
						To delete:
						`ALU userid TSO (NOSIZE)`

erRacUTSOSout
 	
Default system output message class. Must be alphanumeric.
	String	1	Single	RW	No	To add or modify:
						`ALU userid TSO (SYSOUT(value))`
						
						To delete:
						`ALU userid TSO (NOSYSOUT)`

erRacUTSOUnit
 	
Default allocation unit name.
	String	8	Single	RW	No	To add or modify:
						`ALU userid TSO (UNIT(value))`
						
						To delete:
						`ALU userid TSO (NOUNIT)`

erRacUTSOUdata
 	
Hexadecimal value, defined by the user installation. Typically, this attribute is unused.
	String	4	Single	RW	No	To add or modify:
						`ALU userid TSO (USER(value))`
						
						To delete:
						`ALU userid TSO (NOUSER)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUIsUaudit
 	
All user activity is logged.
	String	5	Single	RW	No	To add or modify:
						`ALU userid AUDIT`
						
						To delete:
						`ALU userid NOAUDIT`

erRacUIsWASeg
 	
Work attribute is present.
 	
Work Attribute information. It describes user location specifics. This object is/was primarily created for APPC/MVS. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes.
	String	5	Single	RW	No	To add or modify:
						`ALU userid WORKATTR`
						
						To delete:
						`ALU userid NOWORKATTR`

erRacUWAAcct
 	
Account number. This field has (real) meaning only for APPC/MVS tasks.
	String	255	Single	RW	No	To add or modify:
						`ALU userid WORK (WACCNT('value'))`
						
						To delete:
						`ALU userid WORK (NOWAACCNT)`

erRacUWAAddr1
 	
Address line 1.
	String	60	Single	RW	No	To add or modify:
						`ALU userid WORK (WAADDR1('value'))`
						
						To delete:
						`ALU userid WORK (NOWAADDR1)`

erRacUWAAddr2
 	
Address line 2.
	String	60	Single	RW	No	To add or modify:
						`ALU userid WORK (WAADDR2('value'))`
						
						To delete:
						`ALU userid WORK (NOWAADDR2)`

erRacUWAAddr3
 	
Address line 3.
	String	60	Single	RW	No	To add or modify:
						`ALU userid WORK (WAADDR3('value'))`
						
						To delete:
						`ALU userid WORK (NOWAADDR3)`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUWAAddr4
 	
Address line 4.
	String	60	Single	RW	No	To add or modify:
						`ALU userid WORK (WAADDR4('value'))`
						
						To delete:
						`ALU userid WORK (NOWAADDR4)`

erRacUWABldg
 	
Building.
	String	60	Single	RW	No	To add or modify:
						`ALU userid WORK (WABLDG('value'))`
						
						To delete:
						`ALU userid WORK (NOWABLDG)`

erRacUWADept
 	
Department.
	String	60	Single	RW	No	To add or modify:
						`ALU userid WORK (WADEPT('value'))`
						
						To delete:
						`ALU userid WORK (NOWADEPT)`

erRacUWAName
 	
Name.
	String	60	Single	RW	No	To add or modify:
						`ALU userid WORK (WANAME('value'))`
						
						To delete:
						`ALU userid WORK (NOWANAME)`

erRacUWARoom
 	
Room.
	String	60	Single	RW	No	To add or modify:
						`ALU userid WORK (WAROOM('value'))`
						
						To delete:
						`ALU userid WORK (NOWAROOM)`

erRacULogtime Time user last signed on. Field is set to current time if password has been reset, or if the user account status has been resumed.	Time		Single	R	No	

erRacUModel
 	
The name of a data set profile this user can use as a model for creating new data set profiles.
	String	44	Single	RW	No	To add or modify:
						`ALU userid MODEL (value)`
						
						To delete:
						`ALU userid NOMODEL`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUName
 	
The name of the defined user. Value is nullified by setting it to 20 pound (#) signs:
`####################`
	String	20	Single	RW	No	To add or modify:
						`ALU userid NAME ('value')`
						
						To delete:
						`ALU userid NAME ('####################')`

erRacUOwner Name of existing user or group that owns this user account.	String	8	Single	RW	Yes	To add or modify: `ALU userid OWNER (value)`
erRacUPassdate Date user is required to change password. If 0, current password must be changed upon initial use.	Date		Single	R	No	

erRacUPWInterval
 	
Password interval. Can be 0 - 255. Zero means no password interval. Maximum value imposed by RACF system-wide options.
	Integer	3	Single	RW	No	To add or modify:
						`PW USER (userid) INTERVAL (value)`
						
						To delete:
						`PW USER userid NOINTERVAL`

erRacUPWNoExpire Whether a password assigned to this user is to be noted as 'not expired'. Must be used with the 'erPassword'. This attribute has no meaning without a password. This field has been removed from the schema. It is an adapter option instead.	String	5	Single	W	No	

erRacUResumeDate
 	
MM/DD/YY date field, indicates future date when this account is to be reactivated (RESUMEd).
	Date	8	Single	RW	No	To add or modify:
						`ALU (userid) RESUME (value)`
						
						To delete:
						`ALU userid RESUME`

erRacURevokeDate
 	
MM/DD/YY date field, indicates future date when this account is to be inactivated (revoked).
	Date	8	Single	RW	No	To add or modify:
						`ALU (userid) REVOKE (value)`
						
						To delete:
						`ALU userid RESUME`

Table 23. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacUWhenDays
 	
Days of the week a user can sign on. Valid values are:
• SUNDAY
• MONDAY
• TUESDAY
• WEDNESDAY
• THURSDAY
• FRIDAY
• SATURDAY
• ANYDAY
	String	9	Multiple	RW	No	To add or modify:
						`ALU (userid) WHEN (DAYS(value))`
						
						To delete:
						`ALU userid WHEN (DAYS (ANYDAY))`

erRacUWhenTime
 	
Time range when user can sign on to the system.
	Time	9	Single	RW	No	To add or modify:
						`ALU (userid) WHEN (TIME(value))`
						
						To delete:
						`ALU userid WHEN (TIME (ANYTIME))`

erUid ID of user on RACF being created, updated, or deleted.	String	8	Single	RW	Yes	

erRacConnect

This class represents the connection of a user to a group within RACF. The following connect object is associated with the base user object, and must have at least 1, but can have over 7,000 occurrences. Typically this number is no more than 100 and varies upon the customer environment.

Table 24. erRacUser attribute information

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

erRacConAuth
 	
Whether this user is in REVOKED status, or not.
	String	7	Single	RW	No	To add or modify:
						`CO userid GROUPvalue AUTHvalue`
						
						To delete:
						`CO userid GROUPvalue AUTH (USE)`

erRacConCDate Connect entry creation date.	Date	7	Single	R	No	

Table 24. erRacUser attribute information (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands
erRacConCount Connect count. Max value of 65,535.	Integer	5	Single	R	No	

erRacConGroup
 	
Name of group to which user is connected.
	String	8	Single	RW	Yes	To add or modify:
						`CO userid GROUPvalue`
						
						To delete:
						`REMOVE userid GROUP(value)`

erRacConIsADSP
 	
User can automatically create discrete data set profiles.
	String	5	Single	RW	No	To add or modify:
						`CO userid GROUP(value) ADSP`
						
						To delete:
						`CO userid GROUP(value) NOADSP`

erRacConIsAudit
 	
User has system Auditor ability.
	String	5	Single	RW	No	To add or modify:
						`CO userid GROUP(value) AUDITOR`
						
						To delete:
						`CO userid GROUP(value) NOAUDITOR`

erRacConIsGrpac
 	
Permits group level access of UPDATE to the group under the High Level Qualifier of any data set profile created through ADSP by this user.
	String	5	Single	RW	No	To add or modify:
						`CO userid GROUP(value) GRPAC`
						
						To delete:
						`CO userid GROUP(value) NOGRPAC`

erRacConIsOper
 	
User has system Operations ability (ability to read/modify any file).
	String	5	Single	RW	No	To add or modify:
						`CO userid GROUP(value) OPERATIONS`
						
						To delete:
						`CO userid GROUP(value) NOOPERATIONS`

erRacConIsSpec
 	
User has system Special. System security Administrator.
	String	5	Single	RW	No	To add or modify:
						`CO userid GROUP(value) SPECIAL`
						
						To delete:
						`CO userid GROUP(value) NOSPECIAL`

erRacConLogtime Time user last signed on, using this group as default group or specified group.	Time		Single	R	No	

Table 24. erRacUser attribute information (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands
erRacConOwner Owner of this connect entry.	String	8	Single	RW	Yes	To add or modify: `CO userid GROUP(value) OWNER(value)`

erRafConResumDt
 	
MM/DD/YY date field, indicates future date when this account is to be reactivated (RESUMEd).
	Date	8	Single	R	No	To add or modify:
						`CO userid GROUP(value) RESUME(value)`
						
						To delete:
						`CO userid GROUP(value) RESUME`

erRacConRevokDt
 	
MM/DD/YY date field, indicates future date when this account is to be inactivated (revoked).
	Date	8	Single	R	No	To add or modify:
						`CO userid GROUP(value) REVOKE(value)`
						
						To delete:
						`CO userid GROUP(value) REVOKE`

erRacConUACC
 	
Default universal access to all data set and TAPEVOL profiles created by this user. Valid Values are:
• NONE
• READ
• UPDATE
• CONTROL
• ALTER
	String	7	Single	RW	No	To add or modify:
						`CO userid GROUP(value) UACC(value)`
						
						To delete:
						`CO userid GROUP(value) UACC(NONE)`

erRacConXML This attribute carries an XML string that represents all the data for a single connect entry. It carries all the information that comprises a RACF connect entry. This action is due to the server flattening out all the data elements.	String		Multiple	RW	Yes	

erRacGroup

This class represents a group definition within RACF. The RACF group represents a group definition within the RACF database. Its presence is required to enable IBM Security Identity Manager to understand the RACF group tree structure, to

know what groups are within or outside of management policy. This information is read-only, and is not managed nor updated by IBM Security Identity Manager at this time. Although optional segments are provided in this documentation, implementation of them is to be decided later.

Table 25. erRacGrp attribute information

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands
erRacGrpCDate Creation date of this group.	Date	8	Single	RW	Yes	

erRacGrpData
 	
Installation data, user-defined purpose
	String	225	Single	RW	No	To add or modify:
						`ALG userid DATA(value)`
						
						To delete:
						`ALG userid NODATA`

erRacGrpDFPAppl
 	
DFP segment, DATAAPPL field.
	String	8	Single	RW	No	To add or modify:
						`ALG userid DFP(DATAAPPL(value))`
						
						To delete:
						`ALG userid DFP(NODATAAAPPL)`

erRacGrpDFPData
 	
DFP segment, Data class.
	String	8	Single	RW	No	To add or modify:
						`ALG userid DFP(DATACLASS (value))`
						
						To delete:
						`ALG userid DFP(NODATACLASS)`

erRacGrpDFPMgmt
 	
DFP segment, management class.
	String	8	Single	RW	No	To add or modify:
						`ALG userid DFP(MGMTCLASCLASS (value))`
						
						To delete:
						`ALG userid DFP(NOMGMTCLAS)`

erRacGrpDFPStor
 	
DFP segment, storage class.
	String	5	Single	RW	No	To add or modify:
						`ALG userid DFP(STORCLASCLASS (value))`
						
						To delete:
						`ALG userid DFP(NOSTORCLAS)`

erRacGrpIsDFP
 	
Indicates presence of DFP segment information.
	String	5	Single	RW	No	To add or modify:
						`ALG userid DFP`
						
						To delete:
						`ALG userid NODFP`

erRacGrpIsOMVS
 	
Indicates presence of OMVS segment information.
	String	5	Single	RW	No	To add or modify:
						`ALG userid OMVS`
						
						To delete:
						`ALG userid NOOMVS`

Table 25. erRacGrp attribute information (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required ?	Commands

erRacGrpIsTME
 	
Indicates presence of TME role segment information.
	String	5	Single	RW	No	To add or modify:
						`ALG userid TME`
						
						To delete:
						`ALG userid NOTME`

erRacGrpIsUni Indicates that this group is a Universal Group (Unlimited number of users connected).	String	5	Single	RW	No	
erRacGrpName Name of group to which user is connected.	String	8	Single	R	Yes	

erRacGrpOMVSGid
 	
OMVS Group ID. Valid values are 0 - 2,147,483,647.
	Integer	10	Single	RW	No	To add or modify:
						`ALG userid OMVS(GIDvalue)`
						
						To delete:
						`ALG userid OMVS(NOGID)`

erRacGrpOwner Owner of this group.	String	8	Single	RW	Yes	To add or modify: `ALG userid OWNER(value)`
erRacGrpSubgrp Subordinate groups to this group.	String	8	Multiple	RW	No	
erRacGrpSuper Superior group to this group.	String	8	Single	RW	Yes	To add or modify: `ALG userid SUPGROUP(value)`

erRacGrpTMERole
 	
Role groups that this group is part of.
	String	8	Multiple	RW	No	To add or modify:
						`ALG userid TME(ROLES(value))`
						
						To delete:
						`ALG userid TME(NOROLES)`

erRacGrpTUACC
 	
Indicates whether Terminal Universal Access is used.
	String	5	Single	RW	No	To add or modify:
						`ALG userid TERMUACC`
						
						To delete:
						`ALG userid NOTERMUACC`

Appendix B. Registry settings

The following table lists valid registry options, their values, and meanings.

Table 26. Registry settings and additional information

Option attribute	Default value	Valid value	Function and meaning	Required?
APPCDLU	None	1 - 8 EBCDIC characters	This attribute is the destination APPC/MVS logical unit, to which the adapter communicates. This LU must be on the same host as the 'APPCOLU'.	No
APPCMODE	None	1 - 8 EBCDIC characters	This attribute is the `VTAM 'LOGMODE'` entry to be used by the APPC connection. The mode table used by the APPCOLU logical unit must have this LOGMODE entry defined within it.	No
APPCCMD	ISIMCMD	1 - 64 EBCDIC characters	This attribute is the APPC/MVS back end command executor transaction name.	No
APPCOLU	None	1 - 8 EBCDIC characters	This attribute is the APPC Originating LU. If NULL, the adapter uses BASELU.	No
APPCRECO	ISIMRECO	1 - 8 EBCDIC characters	This attribute is the APPC/MVS back end reconciliation transaction name.	No
PASSEXPIRE	TRUE	TRUE, FALSE, or TRUEADD	This attribute is the default action that the adapter must perform when the adapter receives a password change request. TRUE indicates that passwords must be set as expired. FALSE indicates that passwords must be set as non-expired. When set to TRUEADD, a password for a new user is set to EXPIRED. A password is set on an existing user asset to non-expired. In each case, READ or UPDATE access to the FACILITY class profile, IRR.PASSWORD.RESET is required. **Note:** If the RACF attribute **`erRacuNoexpire`** is passed to the adapter, with TRUE or FALSE, this adapter option (PASSEXPIRE) is ignored. The setting of the **`erRacuNoexpire`** attribute is used.	No

Table 26. Registry settings and additional information (continued)

Option attribute	Default value	Valid value	Function and meaning	Required?
SCOPING	None	TRUE or FALSE	If this attribute is not specified, then the scoped reconciliation is based upon the presence of a RACF ID specified on the service form. If there is an ID in the service form, a scoped recon is performed. If the service form has no RACF ID specified, a full recon is performed. If this registry attribute is set to TRUE it always performs a scoped recon, based upon the RACF ID that it is run as. This ID can be either the specified surrogate (from the service form) or the RACF ID of the adapter. If this registry attribute is set to FALSE it always performs a full recon, regardless of the RACF ID it is run as.	No
SHORTCONNECT	FALSE	TRUE or FALSE	When SHORTCONNECT is set to TRUE, the CONNECT entries do not contain LOGON COUNT, CREATION DATE, LAST-LOGON DATE. This setting enables the use of a simple string compare and mitigates the need for the CUSTOM JOIN DIRECTIVE.[1] This option addresses a policy implementation issue that occurs when building a provisioning policy for RACF accounts. When a straight string compare is performed between the "policy" version of a connect entry and the value in the erRacConXML, the policy returns a mismatch. This mismatch occurs because of the transient behavior of creation date, last logon date/time, logon count, and future revoke/resume dates. When this option is enabled, these dynamic attributes are omitted. The revoke and resume dates are omitted to prevent a RACF user from being RESUMEd because of differences between the connect entry and the policy.	No

[1] The following example indicates the content of a single value, within the erRacConXML attribute. The items that are in bold are omitted when the SHORTCONNECT option is set to TRUE:

```
<CONNECT_ENTRY name="CONENTRY"><ADSP>FALSE</ADSP><AUDITOR>FALSE</AUDITOR>
<AUTHORITY>USE</AUTHORITY><DATE>200312101200Z</DATE><GRPACC>FALSE</GRPACC>
<LAST_DATE>200312101200Z</LAST_DATE><LOGON_COUNT>0</LOGON_COUNT>
<OPERATIONS>FALSE</OPERATIONS><OWNER>CONENTRY</OWNER>
<RESUME_DATE>200312101200Z</RESUME_DATE><REVOKE_DATE>200312101200Z</REVOKE_DATE>
<REVOKED>FALSE</REVOKED><SPECIAL>FALSE</SPECIAL><UACC>NONE</UACC></CONNECT_ENTRY>
```

Appendix C. Environment variables

The following table contains valid environment variables, their meanings or usages, and values for the RACF Adapter.

Table 27. RACF Adapter environment variables

Environment variable	Meaning or use	Default value	Required?
LIBPATH	Specify the location of the Dynamic Link Library (DLL) and `.so` files.	None	Yes
PDU_ENTRY_LIMIT	Specify the maximum number of accounts that are kept in the main storage.	2000. The range is 50-3000.	No
PROTOCOL_DIR	Specify the fully qualified location of the directory where the `.so` and `.dll` files are.	LIBPATH	No
REGISTRY	Specify the location of a specific registry file. The registry path is the fully qualified path and the file name of the registry file. The registry name is the adapter name in uppercase, with `.dat` suffixed to the name.	Current® working directory.	No

Appendix D. Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This guide uses the Windows convention for specifying environment variables and for directory notation.

When using the Unix command line, replace %variable% with $variable for environment variables and replace each backslash (\) with a forward slash (/) in directory paths. The names of environment variables are not always the same in Windows and UNIX. For example, %TEMP% in the Windows operating system is equivalent to $tmp in a UNIX operating system.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Appendix E. Support information

Use the following options to obtain support for IBM products:

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the information center for IBM Security Identity Manager. However, sometimes you need to look beyond the information center to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).

   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
2. Find the content that you need by using the IBM Support Portal.

   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports).
   - IBM Security Identity Manager Support website.
   - IBM Redbooks®.
   - IBM support communities (forums and newsgroups).
4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.

5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

   Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Obtaining a product fix

A product fix might be available to resolve your problem.

About this task

You can get fixes by following these steps:

Procedure

1. Obtain the tools required to get the fix. You can obtain product fixes from the *Fix Central Site*. See http://www.ibm.com/support/fixcentral/.
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the "Download package" section.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.

Contacting IBM Support

IBM Support assists you with product defects.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

About this task

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):

     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.

a. Download and install the ISA tool from the ISA website. See http://www.ibm.com/software/support/isa/.
b. Open ISA.
c. Click **Collection and Send Data**.
d. Click the **Service Requests** tab.
e. Click **Open a New Service Request**.

- Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix F. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager Information Center, and its related publications, are accessible.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for additional navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to utilize more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

IBM and accessibility

See the IBM Human Ability and Accessibility Center For more information about the commitment that IBM has to accessibility.

Appendix G. 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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 might 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
2Z4A/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 document 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 measurement 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.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

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

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.

Linux is a trademark of Linus Torvalds 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.

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.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Index

K

L

M

N

O

P

R

S

T

U

V

W

Z

Printed in USA

SC27-4407-00