Note

Before using this information and the product it supports, read the information in "Notices" on page 125.

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.

© Copyright IBM Corporation 2012, 2014.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

**Figures** ........................................... v  
**Tables** ............................................. vii  
**Preface** ........................................... ix  
About this publication ................................ ix  
Access to publications and terminology .......... ix  
Accessibility ........................................ x  
Technical training ................................... x  
Support information ................................ x  
Statement of Good Security Practices ............ x  

**Chapter 1. RACF Security for z/OS Adapter**  
Overview of the RACF Adapter ........................... 1  
RACF Adapter considerations ............................ 2  
Adapter interactions with the IBM Security Identity Manager server ........................................ 5  

**Chapter 2. Planning to install the RACF Adapter**  
Preinstallation roadmap ................................... 7  
Installation roadmap ................................... 7  
Prerequisites .......................................... 8  
Software downloads for the RACF adapter ............ 8  

**Chapter 3. Installing and configuring the RACF Adapter**  
Uploading the adapter package on z/OS ............... 10  
Installing the ISPF dialog ............................. 11  
Running the ISPF dialog ................................ 11  
Starting and stopping the adapter ..................... 18  
RACF access configuration .............................. 19  
RACF user ID ......................................... 19  
Surrogate user ID ..................................... 20  
Authorization to set and reset passwords .......... 21  
AUTOID support ...................................... 21  
Shared UID support .................................. 22  
Password phrases ...................................... 22  
z/OS UNIX System Services considerations .......... 23  
Communication configuration .......................... 23  
Importing the adapter profile into the IBM Security Identity Manager server .......................... 23  
Adapter profile installation verification .......... 24  
Creating a RACF Adapter service .................... 24  

**Chapter 4. First steps after installation**  
Adapter configuration for IBM Security Identity Manager ......................................................... 27  
Supporting custom fields with extended attributes ................................................................. 27  
Mapping the custom fields to the extended attributes by using the ISPF dialog ......................... 27  
Starting the adapter configuration tool ............... 33  
Viewing configuration settings ......................... 34  
Changing protocol configuration settings ............ 35  
Event notification configuration ........................ 38  
Changing the configuration key ........................ 49  
Changing **activity logging** settings ................. 50  
Modifying registry settings ............................ 52  
Modifying non-encrypted registry settings .......... 52  
Changing advanced settings ........................... 54  
Viewing statistics ...................................... 55  
Setting the code page ................................ 55  
Accessing help and more options ..................... 57  
RACF Adapter customization ............................ 59  
ISIMEXIT ............................................. 59  
ISIMEEXEC ........................................... 61  
SSL authentication for the RACF adapter .......... 62  
Adapter language pack installation ................. 76  

**Chapter 5. RACF Adapter error troubleshooting**  
Techniques for troubleshooting problems .......... 77  
Warning and error messages ........................... 79  
Adapter log files ...................................... 81  

**Chapter 6. Upgrading the adapter** ................... 83  

**Chapter 7. Uninstalling the adapter** ............... 85  

**Appendix A. Adapter attributes** ..................... 87  

**Appendix B. Registry settings** ....................... 113  

**Appendix C. Environment variables** ................. 117  

**Appendix D. Support information** .................... 119  
Searching knowledge bases ........................... 119  
Obtaining a product fix ................................ 120  
Contacting IBM Support .............................. 120  

**Appendix E. Accessibility features for IBM Security Identity Manager** ................................. 123  

**Index** ............................................... 129
## Figures

1. The RACF Adapter components .......... 1
2. Scenario with GROUP SPECIAL privileges 3
3. Scenario with surrogate authority ....... 4
4. One-way SSL authentication (server authentication) .......... 66
5. Two-way SSL authentication (client authentication) .......... 67
6. Adapter operating as an SSL server and an SSL client .......... 68
## Tables

1. Preinstallation roadmap ................................. 7
2. Installation roadmap ...................................... 7
3. Prerequisites to install the adapter ..................... 8
4. ISPF dialog data sets ..................................... 11
5. Options for the main configuration menu ............... 34
6. Options for the DAML protocol menu ................. 36
7. Options for the event notification menus .......... 40
8. Modify context options ................................... 43
9. DN elements and definitions ............................. 45
10. Attributes for search .................................... 45
11. Name values and their description .................... 46
12. Organization chart example .............................. 47
13. Organization chart example .............................. 48
14. Options for the activity logging menu ............... 50
15. Non-encrypted registry keys ............................ 53
16. Attribute configuration option description .......... 53
17. Options for the advanced settings menu ............ 54
18. Arguments and description for the agentCfg help menu ...................................................... 58
19. ISIMEXIT processing information ..................... 61
20. ISIMEXEC processing information ..................... 61
21. Error messages, warnings, and corrective actions .................................................. 79
22. Account form attributes .................................. 87
23. erRacUser attribute information ...................... 108
24. erRacGrp attribute information ......................... 111
25. Registry settings and information ..................... 113
26. RACF Adapter environment variables ................. 117
Preface

About this publication

The RACF Adapter Installation and Configuration Guide provides the basic information that is required to install and configure the IBM® Security Identity Manager RACF® 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


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 library


IBM Security Systems Documentation Central

[IBM Security Systems Documentation Central](http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center


IBM Terminology website

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 D, “Support information,” on page 119 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.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.
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 operating system. The adapter does 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 RACF Security 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 tsoxcmd requests. The command executor receives the formatted RACF Security for z/OS command strings and results are collected by the adapter through the same process.
- 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 a `tscocmd` based TSO command 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 a TSO command transaction that is triggered from an incoming request from the adapter. These requests consist of commands. The adapter runs these commands from the UNIX System Services environment and collects the results that are returned by RACF, MVS, and or REXX depending on the specific command to run.

Reconciliation Processor

Operates as a TSO-based or MVS transaction that is triggered from an incoming `tscocmd` request from the adapter. The request is accompanied by a RACF user ID that is used to do the reconciliation. The ID can be the agent ID or a SURROGAT ID. This user ID can be used for a partial reconciliation that is based on the scope of authority of that ID. See the RACF Security Administrator’s Guide for more information about scope of authority.

Scope of authority is referred to as scoped reconciliation.

To enable scoped reconciliations

At adapter installation time, define a VSAM file name for scoped reconciliations. Defining the file name creates the VSAM file and sets the ADK registration value for SCOPING to ‘TRUE’. During reconciliation, the adapter verifies whether the VSAM file for scoped reconciliations can be accessed. If so, the adapter completes a scoped reconciliation.

To switch between SCOPED and non-SCOPED

Use `‘hlq.SAGRCENU(AGRCCFG)’` to either add or remove the VSAM file name for scoped reconciliations and regenerate the jobs in the `‘hlq’.CNTL`.

Resubmit the jobs and when changing from SCOPED to non-SCOPED, remove the previously defined VSAM file for scoped reconciliations.

The reconciliation processor runs the RACF database unload utility (IRRDBU00), or uses an existing data set that the RACF database unload utility (IRRDBU00) produced. If scoped reconciliation is required, the results of the unload job are filtered.

The reconciliation results are stored in an intermediate data set which is read by the adapter which further processes the results and transfers them to the IBM Security Identity Manager server.

The RACF Adapter creates and manages RACF accounts. The adapter runs in “agent” mode and must be installed on a z/OS. One adapter is installed for each RACF database. The RACF Adapter can be configured to support a subset of the accounts through the scope of authority in the RACF Service Form (SURROGAT user ID).

RACF Adapter considerations

The RACF Adapter requires APF authorization. As such, the RACF ID used by the adapter must have READ access to the BPX.SERVER profile in the FACILITY class.
The RACF Adapter operates in two basic modes.

- There might be no operational RACF ID that is specified on the IBM Security Identity Manager service form when a request is issued. In this case, 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.

The IBM Security Identity Manager might do operations against only a portion of the RACF database. In this case, 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.

**Figure 2. Scenario with GROUP SPECIAL privileges**

- The operations might be done under a RACF ID specified on the IBM Security Identity Manager service form. In this case, the RACF ID, which 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 adapter RACF ID must have READ permission on the BPX.SRV..<SURROGATID> profile in the SURROGAT class. The RACF ID that is 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:
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 RACF database unload 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 ISIMEXEC adapter exit points.

**FACILITY class profile IRR.PASSWORD.RESET, with UPDATE**

IRR.PASSWORD.RESET is required if the effective RACF ID that changes passwords or pass phrases 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.

STGADMIN.IGG.DEFDEL.UALIAS is required if your user exits create or delete catalog aliases and the effective RACF ID does not have MCAT update authority.

**SURROGAT class profile BPX.SRV.<SURROGAT RACF ID> with READ**

The surrogate profile is required if the adapter RACF ID differs from the RACF ID under which commands and reconciliations are done.

**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.

Adapter interactions with the IBM Security Identity Manager server

The RACF Adapter uses IBM Security Identity Manager to do user tasks on the IBM RACF Security Server for z/OS. The adapter can add, modify, suspend, restore, reconcile, or delete users from IBM Security Identity Manager. The adapter uses the TCP/IP protocol to communicate with IBM Security Identity Manager.

The RACF Adapter does not use Secure Socket Layer (SSL) by default to communicate with IBM Security Identity Manager. To enable SSL, you must complete post configuration steps.

SSL requires digital certificates and private keys to establish communication between the endpoints. Regarding SSL, the RACF Adapter is considered a server. When the adapter uses the SSL protocol, the server endpoint must contain a digital certificate and a private key. The client endpoint (IBM Security Identity Manager) must contain the Certificate Authority or CA certificate.

To enable SSL communication by default, install a digital certificate and a private key on the adapter and install the CA certificate on IBM Security Identity Manager.

The default TCP/IP port on the z/OS host for the adapter and server communication is 45580. You can change this port to a different port. You can specify the port number on the adapter service form on IBM Security Identity Manager. Ensure that it references the same port number that is configured for the adapter on the z/OS host.

Use the agentCfg utility to configure the adapter. The utility communicates with the adapter through TCP/IP. The TCP/IP port number that is used is dynamically assigned and is in the range 44970 - 44994. The port number and the range of port numbers cannot be configured.

You can restrict the use of these ports to the RACF Adapter. To protect these ports with the RACF protection, define the profiles in the RACF Adapter SERVAUTH resource class. For more information, see the z/OS Communications Server, IP Configuration Guide.
Chapter 2. Planning to install the RACF Adapter

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

About this task

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

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the installation software.</td>
<td>Download the software from the IBM Passport Advantage® website. See “Software downloads for the RACF adapter” on page 8.</td>
</tr>
<tr>
<td>Verify that your environment meets the software and hardware requirements for the adapter.</td>
<td>See “Prerequisites” on page 8.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install and configure the adapter.</td>
<td>See Chapter 3, “Installing and configuring the RACF Adapter,” on page 9.</td>
</tr>
<tr>
<td>Import the adapter profile.</td>
<td>See “Importing the adapter profile into the IBM Security Identity Manager server” on page 23.</td>
</tr>
<tr>
<td>Verify the profile installation.</td>
<td>See “Adapter profile installation verification” on page 24.</td>
</tr>
<tr>
<td>Create a service.</td>
<td>See “Creating a RACF Adapter service” on page 24.</td>
</tr>
<tr>
<td>Configure the adapter.</td>
<td>See “Adapter configuration for IBM Security Identity Manager” on page 27.</td>
</tr>
<tr>
<td>Customize the adapter.</td>
<td>See “RACF Adapter customization” on page 59.</td>
</tr>
</tbody>
</table>
Prerequisites

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

Table 3. Prerequisites to install the adapter

| Operating System     | • z/OS version 1.12  
|                      | • z/OS version 1.13  
|                      | • z/OS version 2.10  
| 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 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.

Software downloads for the RACF adapter

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

Go to [IBM Passport Advantage](https://www.ibm.com/marketplace/passportadvantage).

See the IBM Security Identity Manager Download Document for instructions.

Note:

You can also obtain additional adapter information from IBM Support.
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 several tasks.

Note: The screens in these tasks are examples. Actual screens might differ.

Use the following worksheet to document information required to install and configure the RACF Adapter. Complete this worksheet before you start the installation procedure. The worksheet identifies the information that you need to modify during the installation process. Make a copy of the worksheet for each RACF Adapter instance you are installing.

<table>
<thead>
<tr>
<th>MVS data set name</th>
<th>The MVS data set high-level qualifier for upload and installation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter instance name</td>
<td>The default is racfagent. There is no maximum length, but the length must be manageable. This value is specified in the config.sh UNIX System Services shell script.</td>
</tr>
<tr>
<td>USS Adapter read-only home</td>
<td>The USS file system location that is used to store the adapter binaries. The default is /usr/lpp/isimracf. The read-only home and the read/write home must specify different locations. If they are the same then the installation may fail. It is advised to allocate at least 60 Mb of free space to the read/only home.</td>
</tr>
<tr>
<td>USS Adapter read/write home</td>
<td>The USS file system location that is used to store the adapter log file, register, intermediate reconciliation results and start scripts. The default is /var.ibm/isimracf. The read-only home and the read/write home must specify different locations. If they are the same, then the installation might fail. The read/write home size must be large enough that it can be temporary used to store intermediate reconciliation results. For example, 1 Mb / 100 accounts or groups. The size must be more than the regular requirements for activity logging, depending on the adapter-specific configuration and storing all adapter scripts and registry files.</td>
</tr>
<tr>
<td>Adapter port number</td>
<td>The default is 45580. This value can be modified by using the agentCfg UNIX System Services shell script in the adapter_readonly_bin directory</td>
</tr>
<tr>
<td>Default certificate and key</td>
<td>Certificates must be created and installed manually. See “Configuring SSL authentication for the adapter” in the “IBM Security Identity Manager Adapter Installation Guide”.</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data set size adjustment</td>
<td>Temporary data set sizes in reconciliation must be adjusted according to the size of the RACF database unload for your installation. If the VSAM group file is utilized, its size must be adjusted, following an initial reconciliation.</td>
</tr>
<tr>
<td>VSAM file name for scoped reconciliation</td>
<td>A VSAM file is required to do scoped reconciliation (job ISIMVSAM). You can name the VSAM file to correspond to an adapter instance name. If scoped reconciliation is NOT performed, a VSAM file is not required, and the reconciliation transaction does not require program steps that execute ISIMGSCP. Also, a GROUP DD statement is not required for the ISIMREC2 program step.</td>
</tr>
<tr>
<td>Started task name</td>
<td>The ISIAGNT member is the sample JCL provided for the adapter startup. The component of the started task name must be indicative of the adapter instance name. The started task name must be limited to 7 characters to eliminate ambiguity when shutting down the adapter.</td>
</tr>
<tr>
<td>Adapter port number</td>
<td>The TCP/IP port number that the adapter uses. Enter this number when you configure the UNIX System Services component. Each adapter instance must have a unique TCP/IP port number. If two adapters use the same port number, only one of the adapters can be active at any one time.</td>
</tr>
<tr>
<td>TSO account number</td>
<td>A TSO account number might be required during installation because the adapter uses TSO/E for processing.</td>
</tr>
</tbody>
</table>

**Procedure**

1. “Uploading the adapter package on z/OS”
2. “Installing the ISPF dialog” on page 11
3. “Running the ISPF dialog” on page 11
4. “Starting and stopping the adapter” on page 18
5. “RACF access configuration” on page 19
6. “z/OS UNIX System Services considerations” on page 23
7. “Communication configuration” on page 23

**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 “Software downloads for the RACF adapter” on page 8.
2. Extract the installation package on your local workstation and ensure that a file named "ISIMRACF.UPLOAD.XML" 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:
   \texttt{INDSFILE PUT 'ISIMRACF.UPLOAD.XMI' RECFM(F)}
5. Receive the uploaded file with the TSO RECEIVE command:
   \texttt{RECEIVE INDA(ISIMRACF.UPLOAD.XMI)}
6. Press Enter to create a Partitioned Data Set (PDS) file named \texttt{userid.ISIMRACF.UPLOAD}, where, \texttt{userid} is your TSO user ID.

Installing the ISPF dialog

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

Procedure
1. Log on to a z/OS operating system.
2. From ISPF 6 option, run the following command where \texttt{userid} is your TSO user ID.
   \texttt{INSTALL1 EXEC 'userid.ISIMRACF.UPLOAD(INSTALL1)'
3. Specify a high-level qualifier for the data sets that the \texttt{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 high-level qualifier to use the ISPF dialog in the future.

Results
When you run the exec, the exec creates the listed high-level qualifier data sets.

<table>
<thead>
<tr>
<th>High-level qualifier</th>
<th>Library</th>
</tr>
</thead>
<tbody>
<tr>
<td>hlq.SAGRCENU</td>
<td>CLIST/EXEC library</td>
</tr>
<tr>
<td>hlq.SAGRMENU</td>
<td>ISPF message library</td>
</tr>
<tr>
<td>hlq.SAGRPENU</td>
<td>ISPF panel library</td>
</tr>
<tr>
<td>hlq.SAGRSENU</td>
<td>ISPF skeleton library</td>
</tr>
</tbody>
</table>

Note: The \texttt{AGRCCFG} exec allocates the libraries.

Running the ISPF dialog
Run the ISPF dialog to customize the adapter for run time execution. The dialog uses the default values for the parameters but 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 do this task, you must install the ISPF dialog.

Procedure

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

   When the ISPF dialog starts, the following screen is displayed.

   ![ISPF dialog screen](image)

   **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.

3. Select Initial Customization to display the Initial Customization page that lists the high-level tasks that you must do.

   ![Initial Customization page](image)

   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 adapter instance.
   3. Generate Job Streams.
      
      You must have done choices 1 and 2 before doing 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.

4. 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.
5. Press **PF3** (Cancel) or **Enter** after final input (Accept) to return to the Initial Installation panel.

6. Select **Display / Define / Alter Variables**.

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

---

**Load Variables**

The IBM supplied defaults are in 'hlg'.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.

---

**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.

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

Management Class
   Specifies the management 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.

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

9. 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 ===> ISIAGNT
   Name of Started Task JCL procedure name ===> ISIAGNT
   IP Communications Port Number ===> 45580
   Note: The adapter will always require access to ports 44970 through 44994. These ports are implicitly reserved.
   Adapter authentication ID (internal) ===> agent
   Adapter authentication password (internal) ===> agent
   PDU backlog limit ===> 2000
   Do you want passwords set as expired? ===> FALSE (True, False, Trueadd)
   Do you use SYS1.BRODCAST in the environment? ===> FALSE (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 ===> 45587
   TSO Account Number to be assigned to RACF ID ===> ACCT#
   Temporary reconciliation data set name ===> IBMUSER.ISIM.SAVE
   Scoped reconciliation VSAM data set (blank if scoped recon not required) ===> IBMUSER.ISIM.GROUPS

Name of adapter instance
   Specifies the unique name that is 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.

**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 and pass phrases to be 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 that is 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 UID number for the RACF user ID.

**TSO Account Number to be assigned to RACF ID**
Specifies the TSO Account Number that is assigned to the adapter task.

**Temporary reconciliation data set name**
Specifies the data set name used to store intermediate reconciliation results. The adapter user should be allowed to read, write, modify and delete this data set.
Scoped reconciliation VSAM data set (blank if scoped reconciliation is not required)

Specifies the VSAM data set name that is required for the scoped reconciliation process. The reconciliation transaction uses the VSAM data set. If you do not want to do 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 regenerate J4, J6 and RECOJOB and the Jx jobs must be submitted.

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

11. Select **RACF Environment** to access the RACF databases that the adapter uses and set the reconciliation specifics.

```
------------------- ISIM RACF Adapter Customization -------------------
Option ===>
RACF Environment
Is the adapter to run data base unload? ===> TRUE (True or False)
Existing IRRDBU00 Input data set or GDG (Must be cataloged)
 ===> SYS1.RACF.BACKUP
Storage Class for reconciliation related datasets
and/or Management Class for reconciliation related datasets
and/or Disk Volume ID
Max wait time in seconds for RECOJOB to complete
 ===> 30
```

The adapter must know the names of the data sets containing 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 names of 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 utility and you specify FALSE, then you must specify a data set or Generation Data Group (GDG).

**Storage Class**

Specifies the storage class for the temporary reconciliation result data set.
Management Class
Specifies the management class for the temporary reconciliation result data set.

DASD (Disk) volume ID
Specifies the Disk ID for the temporary reconciliation result data set.

Wait time
Specifies the amount of time in seconds the adapter is to wait for the RECOJOB JCL to complete processing.

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

13. Select Generate Job Streams.
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 based on the 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.ISIM.CNTL

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

Enter your installation job statement parameters here:

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

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

15. 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.ISIM.CONFIG
```
16. Select **View instructions for job execution and further tailoring**.
   To view the adapter settings and the 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.

**Results**

After you complete 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 do more steps. For example, enabling the Secure Socket Layer (SSL), creating and importing the certificate in the adapter registry. For more information, see “SSL authentication for the RACF adapter” on page 62.

**Starting and stopping the adapter**

You can stop the adapter and restart it after you change its configuration.

**Before you begin**

Before you start the adapter, ensure that TCP/IP 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` directory. 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 23.

To stop the adapter, take 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
```

### RACF access configuration

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, a valid UID, and a valid TSO account number. This user default group must have an OMVS segment with a valid GID. The adapter RACF user ID must have READ permit on BPX.SERVER in class FACILITY.

For example, if the adapter RACF user ID is ISIAGNT then the following commands define the required profile update:

```
PERMIT BPX.SERVER CLASS(FACILITY) ID(ISIAGNT) ACCESS(READ)
SETROPTS REFRESH RACLIST(FACILITY)
```

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 Adapter database, then the following definition defines this user:

```
ADDUSER ISIAGNT OWNER(SYS1) DFLTGRP(SYS1)
SPECIAL AUDITOR NOPASSWORD TSO(acctnum(acct#))
```

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.

```sql
ADDUSER ISIAGNT DFLTGRP(xxxx) OWNER(xxxx) CLAUTH(USER) NOPASSWORD TSO (ACCTNUM(ACCT#)) CONNECT ISIAGNT GROUP(xxxx) SPECIAL AUDITOR
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:

```sql
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 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:

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

If the TSOAUTH class is active, the adapter user ID (and/or SURROGAT if applicable) requires READ access on JCL in CLASS TSOAUTH: PE JCL CLASS(TSOAUTH) ID(ISIAGNT) ACCESS(READ) SETROPTS RACLIST(TSOAUTH) REFRESH.

Surrogate user ID

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

Surrogate user IDs are necessary only when:
- 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 the RACF 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 define the profile.
RDEFINE SURROGAT BPX.SRV.UNIT1
SETROPTS REFRESH RACLIST(SURROGAT)
PERMIT BPX.SRV.UNIT1 CLASS(SURROGAT) ID(ISIAGNT) ACCESS(READ)
SETROPTS REFRESH RACLIST(SURROGAT)

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 24. 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 are 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 and pass phrases 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 and pass phrases that are set from the IBM Security Identity Manager server are EXPIRED. The user must change the password or pass phrase 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 and pass phrases. 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 CLASSUNIXPRIV) AC(READ) ID(ISIAGNT)
SETROPTS CLASSUNIXPRIV) 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.

Password phrases

RACF password phrases are now supported.

When you set passwords from the IBM Security Identity Manager server, any password with 8 characters or less sets the RACF password for that user. Otherwise, it sets the password phrase for that user.

When you set a RACF password, any existing pass phrase is removed. When you set a pass phrase, a new generated password is set. This means that only the new password or pass phrase is made known for logging in. The previous password or pass phrase cannot be used.

Make sure that any RACF requirements for pass phrases are included in the IBM Security Identity Manager server rules for passwords. Some of these requirements are:

- Whether the RACF setup supports the use of 9 to 14 character pass phrases
- The extra restrictions that are placed on pass phrases by RACF
- Any extra pass phrase rules that are implemented through RACF exits that are installed at your site

If this is not done, then some passwords considered valid by the IBM Security Identity Manager server might be rejected by RACF because they are not valid.

Note: Any reference to RACF user password refers to both password and pass phrase. Password for non-RACF users refers to password only.

The command that is generated for changing a password uses the following format:

```
ALU <USERID> PASSWORD(?) NOEXPIRED NOPHRASE
```

Where the PASSWORD value is the password value that is specified on the IBM Security Identity Manager server.
Pass phrase changes generate two commands. The commands that are generated for changing a pass phrase adhere to the following format:
ALU <USERID> PHRASE(?) NOEXPIRED
ALU <USERID> PASSWORD(?) EXPIRED

Where the PASSWORD value is randomly generated and the PHRASE value is the password value that is specified on the IBM Security Identity Manager server. When specifying a pass phrase value that does not meet the pass phrase requirements as configured in RACF the following message is displayed in the adapter log:
AdkError: racfModify: Invalid PHRASE specified

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. This setting affects other areas of UNIX System Services. See the z/OS UNIX System Services Planning, document GA22-7800.

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.

Communication configuration

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. “Adapter profile installation verification” on page 24
3. “Creating a RACF Adapter service” on page 24

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

You can add an adapter as a service to the IBM Security Identity Manager server. However, the server must first 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, do the following steps:

1. Log on to the IBM Security Identity Manager server. Use an account that has the authority to do 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 file is a component of the adapter installation package. See “Software downloads for the RACF adapter” on page 8.
   Perform one of the following tasks:
   - Type the complete location of where the file is stored.
   - Use Browse to locate the file.
5. Click OK.

Adapter profile installation verification

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 with 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 do 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**: Optionally, specify a description that identifies the service for your environment. You can specify more 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 35.
     
     **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 “SSL authentication for the RACF adapter” on page 62.
   - **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**: Optionally, 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**: Optionally, specify the service owner, if any.
Service Prerequisite
Optionally, specify an existing IBM Security Identity Manager service.

On the Status and information tab
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 is 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. Take these steps:
• 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. You might verify the work station name or the IP address of the managed resource and the port.

6. Click Finish.
Chapter 4. First steps after installation

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

Adapter configuration 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 more arguments, see Table 18 on page 58 in “Accessing help and more options” on page 57.

Note: These screens are examples. Actual screens that are displayed might differ.

Supporting custom fields with extended attributes

You can customize the RACF adapter to support custom fields by mapping each custom field to an extended attribute.

About this task

Complete these steps to customize the RACF adapter to support the custom fields that are defined in the RACF USER CSDATA segments.

Procedure

1. Define the custom fields and extended attributes mappings to the RACF adapter. Use the IBM Security Identity Manager RACF adapter ISPF dialog to complete this step. For more information, see "Mapping the custom fields to the extended attributes by using the ISPF dialog."

2. Copy the JAR file to a temporary directory and extract the files. For more information, see "Extracting files from the RACFProfile.jar file" on page 30.

3. Update the schema.dsml file. For more information, see "Updating the schema.dsml file" on page 31.

4. Update the erRacfAcct.xml file. For more information, see "Updating the erRacfAcct.xml file" on page 31.

5. Install the new attributes on the IBM Security Identity Manager server. For more information, see "Installing the new attributes on the IBM Security Identity Manager" on page 32.

Mapping the custom fields to the extended attributes by using the ISPF dialog

The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.
Before you begin

This dialog requires a display that has at least 32 lines. Use a model 3 or model 4 3270 display if possible. You also must have the SPECIAL attribute or at least READ authority to the CSDATA segment by way of field-level access control.

About this task

The ISPF dialog generates and saves a file in the read/write data directory. This file is created so that only the administrator can make updates, and the adapter has read access.

Note: When a new extended attribute is added, the RACF adapter needs to be restarted. Complete these steps to create the adapter file that maps the RACF custom fields to the extended attributes.

Procedure

1. Log on to TSO on the z/OS operating system.
2. From ISPF 6 option, run the command EXEC 'hlq.SAGRCENU(AGRCCFG)' to start the ISPF dialog. The License page is displayed.
3. Press Enter to display this message on the 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.

2 Customize to support RACF custom fields
   If you have USER CSDATA fields defined, select this option.

X Exit

Note: When you run the dialog, take note of 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.

Tip: You can load previously saved parameters from the initial installation by selecting Initial Customization on the first panel, then Load Default or Saved Variables. This option completes the fields USS Adapter read/write home and RACF z/OS Unix group for the ISIM adapter with values used during the installation.

4. Select Customize to support RACF custom fields. You must have the SPECIAL attribute or at least READ authority to the CSDATA segment by way of field-level access control.

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

RACF custom field support

Select the custom fields with an S.
Type S * on the command line to select all fields.
Type SAVE on the command line to save the selected fields and attribute names to the data directory in the read/write home.

USS Adapter read/write home

RACF z/OS Unix group for the ISIM adapter

<table>
<thead>
<tr>
<th>S Field</th>
<th>Type</th>
<th>Max len</th>
<th>Attribute name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMPFLAG</td>
<td>FLAG</td>
<td>003</td>
<td>erracempflag</td>
<td>Defined in UDF.dat</td>
</tr>
<tr>
<td>EMPHEX</td>
<td>HEX</td>
<td>0512</td>
<td>erracemphex</td>
<td></td>
</tr>
<tr>
<td>EMPROOM</td>
<td>CHAR</td>
<td>080</td>
<td>erracemproom</td>
<td></td>
</tr>
<tr>
<td>EMPSER</td>
<td>INT</td>
<td>008</td>
<td>erracempser</td>
<td></td>
</tr>
<tr>
<td>INT01</td>
<td>INT</td>
<td>008</td>
<td>erracint01</td>
<td></td>
</tr>
</tbody>
</table>

This panel lists all fields that are defined in the RACF USER CSDATA segment. The panel shows:

- The data type.
- The maximum value length allowed.
- A generated attribute name that is based on the field name.

USS Adapter read/write home

This parameter must be the read/write home as specified in the Disk location parameters panel during installation. The custom fields and corresponding attribute names that are selected are written to the UDF.dat file in the data directory of the read/write home.

RACF z/OS Unix group for the ISIM adapter

This parameter must be the group for the adapter as specified in the Adapter-specific parameters panel during installation. It is used to give the adapter read access to the UDF.dat file.

Attribute name

Attribute names are required for selected fields. The attribute names are modifiable. The attribute names must be unique and must not contain the characters $', '* or '-'. If the attribute names contain any of those characters, the adapter profile cannot be imported correctly. The generated default attribute names might need to be modified to remove any disallowed characters. The maximum length for an attribute name is 31 characters. The attribute name is converted to lowercase.

If the data directory in the USS Adapter read/write home directory already contains an UDF.dat file, then the fields that are defined in this UDF.dat file are pre-selected in the list of custom fields.

-------------- ISIM RACF Adapter Customization ---------------
Option ==> RACF custom field support
Select the custom fields with an S.
Type $ on the command line to select all fields.
Type SAVE on the command line to save the selected fields and attribute names to the data directory in the read/write home.

USS Adapter read/write home

RACF z/OS Unix group for the ISIM adapter

<table>
<thead>
<tr>
<th>S Field</th>
<th>Type</th>
<th>Max len</th>
<th>Attribute name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMPFLAG</td>
<td>FLAG</td>
<td>003</td>
<td>erracempflag</td>
<td>Defined in UDF.dat</td>
</tr>
<tr>
<td>EMPHEX</td>
<td>HEX</td>
<td>0512</td>
<td>erracemphex</td>
<td></td>
</tr>
</tbody>
</table>
S EMPROOM CHAR 080 erracemproom Defined in UDF.dat
S EMPSER INT 008 erracempser Defined in UDF.dat
INT01 INT 008 erracint01

You might see the following in the comments column:

**Invalid attribute name**

You selected a field and the attribute name contains characters that are not valid. The attribute name must be corrected before it can be saved.

**Length discrepancy**

The maximum length for the custom field that is saved in the UDF.dat does not match the maximum length for that field in the USER CSDATA segment.

This error might occur if the USER CSDATA segment is updated after the UDF.dat file was created. The maximum length value displayed is the value from the USER CSDATA segment.

If the UDF.dat file is saved, the USER CSDATA segment value is the value that is saved. If you change the length of one or more fields in the USER CSDATA segment, optionally, save the UDF.dat file to avoid this error.

**Defined in UDF.dat**

Indicates that the custom field is in the current UDF.dat file in the specified read/write home directory.

5. Type S in the selection column to select any additional custom fields you want to support.

   If you want to remove a field that is defined in the UDF.dat, remove the S from the selection column. You can page up and down if necessary. The selections are maintained. If you want to select all custom fields, type S* on the command line.

6. When you are finished selecting the custom fields, type SAVE on the command line. The UDF.dat file is saved with read and write permissions for the administrator and read permission for the group for the adapter specified.

   **Note:** The administrator is the user who is selecting and saving the custom fields to be supported.

**Results**

The next time that the RACF adapter is cycled, it picks up the extended attributes. See the following sections for information about how to update and import the RACF Adapter profile. Importing the profile makes the new attribute definitions available to the IBM Security Identity Manager server.

**Extracting files from the RACFProfile.jar file**

The profile JAR file, RACFProfile.jar, is included in the RACF adapter compressed file that you downloaded from the IBM website.

**About this task**

The RACFProfile.jar file contains the following directories and files:

- META-INF/
- META-INF/MANIFEST.MF
- racfprofile/
You can modify these files to customize your environment. When you finish updating the profile JAR file, rebuild the JAR file and import it into the IBM Security Identity Manager server. The MANIFEST.MF file contains only the Java version that is used to build the JAR file. When you build a new JAR file, your Java builds its own MANIFEST.MF file so this file (and directory) can be ignored. To modify the RACFProfile.jar file, complete the following steps.

**Procedure**

1. Copy the RACFProfile.jar file to a temporary folder.
2. From the command prompt, run `jar xf RACFProfile.jar` to extract the contents of the RACFProfile.jar file into the temporary directory. The `jar xf` command creates the directory `racfprofile`.
3. Change the directory to the `racfprofile` subdirectory. For example, run the command `cd racfprofile`.
4. Edit the appropriate files.

**Updating the erRacfAcct.xml file**

The RACF adapter `erRacfAcct.xml` file defines how fields are displayed in the IBM Security Identity Manager server web pages. Modify this file to define where and how to display the new extended attributes.

**About this task**

The `erRacfAcct.xml` file defines where and how to display the attributes and objects in the IBM Security Identity Manager server web application. To update the `erRacfAcct.xml` file, complete the following steps.

**Procedure**

1. Edit the `erRacfAcct.xml` file to define where and how to display each extended attribute. Make sure that you put the definition in the correct spot. Each definition is displayed under the previous definition within the tabbed entry.
   
   For example:
   ```xml
   <formElement direction="inherit" name="data.erracempflag" label="Employee Flag">
     <select style="width:100px" name="data.erracempflag" width="100">
       <option value=""></option>
       <option value="TRUE">$erracfftrue</option>
       <option value="FALSE">$erracfffalse</option>
     </select>
   </formElement>
   ```

2. You can find samples of the RACF custom fields in the `erRacfzacct.xml` file. Search for `Sample` in the file. These samples are in under Custom Fields that is commented out.

**Updating the schema.dsml file**

The RACF adapter `schema.dsml` file identifies all of the standard RACF account attributes. Modify this file to identify the new extended attributes.
About this task

The schema.dsml file defines the attributes and objects that the adapter supports and uses to communicate with the IBM Security Identity Manager server. To update the schema.dsml file, complete the following steps.

Procedure

1. Edit the schema.dsml file to define each extended attribute.
   
   The attribute name must match the attribute name that is registered with the ISPF dialog. All attributes must be unique, and assigned a unique Object Identifier (OID).
   
   The instance ID (last dot delimited segment of the OID) for the extended attributes starts from 1000, so the OID for the first extended attribute is `<object-identifier>1.3.6.1.4.1.6054.3.127.2.1000</object-identifier>`.
   
   This numbering prevents duplicate OIDs if the adapter is upgraded to support new attributes. For subsequent extended attributes, the OID increments by 1, based on the last entry in the file. For example, if the last attribute in the file uses the OID `1.3.6.1.4.1.6054.3.127.2.1008`, the next new attribute uses the OID `1.3.6.1.4.1.6054.3.127.2.1009`. The data type is either:
   
   • A directory string and is defined by using the syntax tags:
     
     `<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>`
     
     This data type is used for RACF fields defined as FLAG, HEX and CHAR.
   
   • An integer and is defined by using the syntax tags:
     
     `<syntax>1.3.6.1.4.1.1466.115.121.1.27</syntax>`
     
     This data type is used for RACF fields defined as NUM.
   
2. Add the definition for each of the new attributes before the account class and then reference them in the account class. For example, add the following attribute definition before the erRacfAcct section of the schema.dsml file:
   
   `<attribute-type single-value = "true"/>
   <name>erRacEmpFlag</name>
   <description>Employee Flags</description>
   <object-identifier>1.3.6.1.4.1.6054.3.127.2.1000</object-identifier>
   <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>`
   
   3. Add a reference for each of the new attributes in the account class. For example, add the following attribute reference in the erRacfAcct section of the schema.dsml file:
   
   `<attribute-ref ref = "erRacEmpFlag" required = "false"/>`
   
   4. You can find samples of the RACF custom fields in the schema.dsml file. Search for Sample in the file. These samples are commented out.

Installing the new attributes on the IBM Security Identity Manager

After any file modification, import all files, including those files without updates, into the IBM Security Identity Manager server for the changes to take effect.

About this task

To install the new attributes, create a new JAR file that contains the updated files in the temporary directory.
Procedure
1. Change to the parent directory and then build a new JAR file.

   Note:
   - The name of the JAR file does not matter. You can use your own naming convention.
   - The directory name and the file names in the JAR file are specific and cannot be changed.

   For example, run the command `cd .. jar cf RACFProfileCustom.jar racfprofile`

2. Import the new JAR file into the IBM Security Identity Manager server.

   Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. For the updates to take effect immediately, stop and start the IBM Security Identity Manager server.

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

About this task
To start the adapter configuration tool, `agentCcfg`, for RACF Adapter parameters, do 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
   Optionally, 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.
   ```
   # cd /var.ibm/isimracf/bin
   ```

   Note: There is also a `bin` subdirectory in the adapter read-only directory. The read/write `bin` subdirectory contains scripts that set up environment variables, then call the actual executable files that are 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.

4. Run the following command:
   ```
   agentCcfg -agent RACFAgent
   ```
   The adapter name was specified when you installed the adapter. You can find the names of the active adapters by running the `agentCcfg` utility as:
   ```
   agentCcfg -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 35.

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 5. Options for the main configuration menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Viewing configuration settings</td>
<td>See “Viewing configuration settings.”</td>
</tr>
<tr>
<td>B</td>
<td>Changing protocol configuration settings</td>
<td>See “Changing protocol configuration settings” on page 35.</td>
</tr>
<tr>
<td>C</td>
<td>Configuring event notification</td>
<td>See “Event notification configuration” on page 38.</td>
</tr>
<tr>
<td>D</td>
<td>Changing the configuration key</td>
<td>See “Changing the configuration key” on page 49.</td>
</tr>
<tr>
<td>E</td>
<td>Changing activity log settings</td>
<td>See “Changing activity logging settings” on page 50.</td>
</tr>
<tr>
<td>F</td>
<td>Changing registry settings</td>
<td>See “Modifying registry settings” on page 52.</td>
</tr>
<tr>
<td>G</td>
<td>Changing advanced settings</td>
<td>See “Changing advanced settings” on page 54.</td>
</tr>
<tr>
<td>H</td>
<td>Viewing statistics</td>
<td>See “Viewing statistics” on page 55.</td>
</tr>
<tr>
<td>I</td>
<td>Setting code page settings</td>
<td>See “Setting the code page” on page 55.</td>
</tr>
</tbody>
</table>

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 33.
2. Type A to display the configuration settings for the adapter.

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

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 72.

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 33.

2. Type B. The DAML protocol is configured and available by default for the adapter.

<table>
<thead>
<tr>
<th>Agent Protocol Configuration Menu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Protocols: DAML</td>
</tr>
<tr>
<td>Configured Protocols: DAML</td>
</tr>
<tr>
<td>X. Done</td>
</tr>
</tbody>
</table>

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.
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 6 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 6. Options for the DAML protocol menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>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.</td>
</tr>
<tr>
<td>B</td>
<td>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.</td>
</tr>
<tr>
<td>C</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 6. Options for the DAML protocol menu (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Displays the following prompt:&lt;br&gt;Modify Property ‘PORTNUMBER’:&lt;br&gt;Type a different port number.&lt;br&gt;The IBM Security Identity Manager server uses the port number to connect to the adapter. The default port number is 45580.</td>
</tr>
<tr>
<td>E</td>
<td>Displays the following prompt:&lt;br&gt;Modify Property ‘USE_SSL’:&lt;br&gt;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 72.&lt;br&gt;FALSE, the default value, specifies not to use a secure SSL connection.</td>
</tr>
<tr>
<td>F</td>
<td>Displays the following prompt:&lt;br&gt;Modify Property ‘SRV_NODENAME’:&lt;br&gt;Type a server name or an IP address of the workstation where you installed the IBM Security Identity Manager server.&lt;br&gt;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.&lt;br&gt;Note: If your operating system supports Internet Protocol version 6 (IPv6) connections, you can specify an IPv6 server.</td>
</tr>
<tr>
<td>G</td>
<td>Displays the following prompt:&lt;br&gt;Modify Property ‘SRV_PORTNUMBER’:&lt;br&gt;Type a different port number to access the IBM Security Identity Manager server.&lt;br&gt;The adapter uses this port number to connect to the IBM Security Identity Manager server. The default port number is 9443.</td>
</tr>
<tr>
<td>H</td>
<td>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.</td>
</tr>
<tr>
<td>I</td>
<td>Displays the following prompt:&lt;br&gt;Modify Property ‘VALIDATE_CLIENT_CE’:&lt;br&gt;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.&lt;br&gt;Specify FALSE, which is the default value, to specify that the IBM Security Identity Manager server can communicate with the adapter without a certificate.&lt;br&gt;Note:&lt;br&gt;• The property name is VALIDATE_CLIENT_CERT, however, it is truncated by agentCfg to fit in the screen.&lt;br&gt;• 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 69.</td>
</tr>
</tbody>
</table>
Table 6. Options for the DAML protocol menu (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>J</td>
<td>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 &quot;SSL authentication for the RACF adapter&quot; on page 62.</td>
</tr>
<tr>
<td>K</td>
<td>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 &quot;hang&quot; problems. The open threads might be caused by firewall or network connection problems and might be seen as TCP/IP ClosWait connections that remain on the adapter. If you encounter such problems, then you must 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.</td>
</tr>
</tbody>
</table>

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.

Event notification configuration

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 33.
2. At the Agent Protocol Configuration Menu, select **Configure Protocol**. See “Changing protocol configuration settings” on page 35.
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 69.

### Setting event notification on the IBM Security Identity Manager server

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:** 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 33.
2. At the Agent Main Configuration Menu, type **E** to display Event Notification Menu.
1. **Event Notification Menu**

   - Password attributes:
     - Reconciliation interval: 1 day(s)
   - Configured contexts: context1

   - Disabled
   - Time interval between reconciliations
   - Set processing cache size: (currently: 50 Mbytes)
   - Add Event Notification Context
   - Modify Event Notification Context
   - Remove Event Notification Context
   - List Event Notification Contexts
   - Set password attribute names
   - Done

2. 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 that 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 7. Options for the event notification menus*

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
</table>
   | 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.
<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
</table>
| B      | Displays the following prompt:  
   Enter new interval
   \([\text{ww:dd:hh:mm:ss}]\)  
   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 \text{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 \text{Enabled - Adapter}. |
| D      | Displays the Event Notification Entry Types Menu. This option is not available if you select \text{Disabled or Enabled - Adapter}. For more information, see \text{Setting event notification triggers} on page 42. |
| 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. |
| 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 \text{“Modifying an event notification context” on page 42}. |
| 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=\text{context1},o=IBM,ou=IBM,dc=com  
   --- Attributes for search request ---  
   {search attributes listed}  
   ----------------------------------------------- |
| J      | When you select the \text{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 33.
2. At the Event Notification Menu, type E to display the Event Notification Entry Types Menu.

<table>
<thead>
<tr>
<th>Event Notification Entry Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. erracaccount</td>
</tr>
<tr>
<td>X. Done</td>
</tr>
<tr>
<td>Select menu option:</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Event Notification Attribute Listing</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) **erracaccountstatus (b) **erracconxml (c) **erracucisiforc (d) **erracuciscoplas (e) **erracuciscopid (f) **erracucisprty (g) **erracucicstimout (h) **erracuclauth (i) **erracucredate (j) **erracucdhomec (k) **erracucdhomeu (l) **erracudcelsautol (m) **erracudcename (n) **erracudceuuid (o) **erracudfltgrp (p) **erracudfpappl (q) **erracudfpdata (r) **erracudfpmgmt</td>
</tr>
<tr>
<td>X. Done</td>
</tr>
</tbody>
</table>

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, take 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 33.
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 8. Modify context options

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Adding search attributes for event notification</td>
<td>See “Adding search attributes for event notification.”</td>
</tr>
<tr>
<td>B</td>
<td>Configuring the target DN for event notification contexts</td>
<td>See “Configuring the target DN for event notification contexts” on page 44.</td>
</tr>
</tbody>
</table>

Adding search attributes for event notification:

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

About this task

These attribute and 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 that are 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 33.
2. **At the Modify Context Menu for the context, type A to display the Reconciliation Attribute Passed to Agent Menu.**

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 33.
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 9 on page 45** describes each DN element.
Table 9. DN elements and definitions

<table>
<thead>
<tr>
<th>Element</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>erservicename</td>
<td>Specifies the name of the target service.</td>
</tr>
<tr>
<td>o</td>
<td>Specifies the name of the organization.</td>
</tr>
<tr>
<td>ou</td>
<td>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.</td>
</tr>
<tr>
<td>rootsuffix</td>
<td>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.</td>
</tr>
</tbody>
</table>

The Modify Context Menu displays the new target DN.

Attribute specifications for search:

For some adapters, you might 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 10 describes a partial list of possible attribute-value pairs that you can specify for Set attributes for search.

Table 10. Attributes for search

<table>
<thead>
<tr>
<th>Service type</th>
<th>Form label</th>
<th>Attribute name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACFProfile</td>
<td>RACF ID under which requests are processed</td>
<td>erracfrequester</td>
<td>A group special RACF user ID that manages users in this service.</td>
</tr>
</tbody>
</table>
Pseudo-distinguished name values:

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

To help 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 11. Name values and their description*

<table>
<thead>
<tr>
<th>Component</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>erServicename</td>
<td>The value of the erServicename attribute of the service.</td>
</tr>
<tr>
<td>B</td>
<td>Zero or more occurrences of ou or 1 or both.</td>
<td>When the service is not directly associated with the organization, you must specify ou and 1. The specification of these values is in a reverse sequence of their appearance in the IBM Security Identity Manager organization chart.</td>
</tr>
</tbody>
</table>
**Table 11. Name values and their description (continued)**

<table>
<thead>
<tr>
<th>Component</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>o</td>
<td>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.</td>
</tr>
<tr>
<td>D</td>
<td>ou</td>
<td>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=</td>
</tr>
<tr>
<td>E</td>
<td>dc</td>
<td>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=</td>
</tr>
</tbody>
</table>

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

**Table 12. Organization chart example**

<table>
<thead>
<tr>
<th>+ Identity Manager Home</th>
<th>IBM Security Identity Manager Home</th>
<th>o</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Acme Inc</td>
<td>Base organization</td>
<td>o</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>+ Identity Manager Home</th>
<th>IBM Security Identity Manager Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Acme Inc</td>
<td>Base organization</td>
</tr>
<tr>
<td>- Irvine Sales</td>
<td>LocationOrganizational Unit</td>
</tr>
</tbody>
</table>

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:

ow=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:

oc=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:
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. You can change the configuration key.

**Procedure**

1. Access the Agent Main Configuration Menu. See "Starting the adapter configuration tool" on page 33.
2. At the Main Menu prompt, type 0.
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 33.

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 take 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 14 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 14. Options for the activity logging menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
</table>
   | 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. |
### Table 14. Options for the activity logging menu (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
</table>
| B      | Displays the following prompt:  
|        | Enter log file directory:  
|        | Type a different value for the logging directory such as /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 such as 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 such as 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 detailed 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. |
| 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. |
Table 14. Options for the activity logging menu (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 113.

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.
Table 15. Non-encrypted registry keys

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATADIR</td>
<td>Specifies the USS Adapter read/write home. This parameter must be the read/write home as specified in the Disk location parameters panel during installation. This is where the registry.dat and the UDF.dat files are stored.</td>
</tr>
<tr>
<td>DSJOB</td>
<td>Specifies the data set where the RECOJOB is located.</td>
</tr>
<tr>
<td>ISIMEXIT</td>
<td>Specifies the data set where the ISIMEXIT/ISIMEXEC REXX scripts are located.</td>
</tr>
<tr>
<td>ENROLE_VERSION</td>
<td>Specifies the version of IBM Security Identity Manager.</td>
</tr>
<tr>
<td>PASSEXPIRE</td>
<td>Specifies the default action that the adapter must do when the adapter receives a password or pass phrase change request. TRUE indicates that passwords and pass phrases must be set as expired. FALSE indicates that passwords and pass phrases must be set as nonexpired.</td>
</tr>
<tr>
<td>RACFRC</td>
<td>Specified the amount of time the adapter waits for the RECOJOB JCL processing to complete.</td>
</tr>
<tr>
<td>RECSAVE</td>
<td>Specifies the data set where the intermediate reconciliation results are stored by RECOJOB. The adapter accesses these data set as soon as the status of RECOJOB is COMPLETED to collected and further process the results.</td>
</tr>
<tr>
<td>SCOPING</td>
<td>Specifies whether SCOPING is to be used for reconciliations. The value can be 'TRUE' (reconciliations are scoped) or 'FALSE' (full reconciliations are done).</td>
</tr>
</tbody>
</table>

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

Table 16. Attribute configuration option description

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Add new attribute.</td>
</tr>
<tr>
<td>B</td>
<td>Modify attribute value.</td>
</tr>
<tr>
<td>C</td>
<td>Remove attribute.</td>
</tr>
</tbody>
</table>

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 determine the maximum number of requests that the adapter processes. You can change these settings.

Procedure

1. Access the Agent Main Configuration Menu. See "Starting the adapter configuration tool" on page 33.

2. At the Main Menu prompt, type 6 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 the letter of the menu option that you want to change. For a description of each option, see Table 17.

   Table 17. Options for the advanced settings menu

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Forces the adapter to submit only 1 request at a time. The default value is FALSE.</td>
</tr>
<tr>
<td>B</td>
<td>Limits the number of Add requests that can run simultaneously. The default value is 3.</td>
</tr>
<tr>
<td>C</td>
<td>Limits the number of Modify requests that can run simultaneously. The default value is 3.</td>
</tr>
</tbody>
</table>
Table 17. Options for the advanced settings menu (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
| F      | Determines whether the adapter can do 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 33.
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 00000 00000 00000 00000 00000 00000 00004
---------------------------------------------------------------
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, take the following steps:
Procedure

1. Access the Agent Main Configuration Menu. See "Starting the adapter configuration tool" on page 33.

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

RACAgent 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

RACAgent 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 more 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

Chapter 4. First steps after installation 57
The following table describes each argument.

**Table 18. Arguments and description for the agentCfg help menu**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-version</td>
<td>Use this argument to display the version of the agentCfg tool.</td>
</tr>
<tr>
<td>-hostname &lt;value&gt;</td>
<td>Use the <code>-hostname</code> argument with one of the following arguments to specify a different host:</td>
</tr>
<tr>
<td></td>
<td>• <code>-findall</code></td>
</tr>
<tr>
<td></td>
<td>• <code>-list</code></td>
</tr>
<tr>
<td></td>
<td>• <code>-tail</code></td>
</tr>
<tr>
<td></td>
<td>• <code>-agent</code></td>
</tr>
<tr>
<td></td>
<td>Enter a host name or IP address as the value.</td>
</tr>
<tr>
<td>-findall</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Add the <code>-hostname</code> argument to search a remote host.</td>
</tr>
<tr>
<td>-list</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Use the <code>-hostname</code> argument to search a remote host.</td>
</tr>
<tr>
<td>-agent &lt;value&gt;</td>
<td>Use this argument to specify the adapter that you want to configure. Enter the adapter name as the value. Use this argument with the <code>-hostname</code> argument to modify the configuration setting from a remote host. You can also use this argument with the <code>-tail</code> argument.</td>
</tr>
<tr>
<td>-tail</td>
<td>Use this argument with the <code>-agent</code> argument to display the activity log for an adapter. Add the <code>-hostname</code> argument to display the log file for an adapter on a different host.</td>
</tr>
<tr>
<td>-portnumber &lt;value&gt;</td>
<td>Use this argument with the <code>-agent</code> argument to specify the port number that is used for connections for the agentCfg tool.</td>
</tr>
</tbody>
</table>
Table 18. Arguments and description for the agentCfg help menu (continued)

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-netsearch &lt;value&gt;</code></td>
<td>Use this argument with the <code>-findall</code> argument to display all active adapters on the z/OS operating system. You must specify a subnet address as the value.</td>
</tr>
<tr>
<td><code>-codepages</code></td>
<td>Use this argument to display a list of available code pages.</td>
</tr>
<tr>
<td><code>-help</code></td>
<td>Use this argument to display the Help information for the agentCfg command.</td>
</tr>
</tbody>
</table>

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.

RACF Adapter customization

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 61

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, it is 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, it is 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, it is 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, it is 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, it is 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. You might call other programs and do file input and output as necessary. Processing is done 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 does 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 do the listed exit functions.
The listed information is available to the EXIT.

Table 19. ISIMEXIT processing information

<table>
<thead>
<tr>
<th>Parameter #</th>
<th>Meaning</th>
<th>Possible value</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verb</td>
<td>Indicates what operation is calling the exit.</td>
<td>ADD, MODIFY, SUSPEND, RESTORE, or DELETE.</td>
</tr>
<tr>
<td>2</td>
<td>Object</td>
<td>The object name of the transaction.</td>
<td>USER indicating a RACF user object that is processed.</td>
</tr>
<tr>
<td>3</td>
<td>Prepost</td>
<td>Qualifies whether this entry is PRE or POST processing entry to the exit.</td>
<td>BEFORE or AFTER.</td>
</tr>
<tr>
<td>4</td>
<td>Name</td>
<td>The name of the RACF object.</td>
<td>The RACF user ID that is processed.</td>
</tr>
<tr>
<td>5</td>
<td>Dfltgrp</td>
<td>The RACF user ID default group.</td>
<td>The value that is specified from the IBM Security Identity Manager server for the default group of this user.</td>
</tr>
<tr>
<td>6</td>
<td>Owner</td>
<td>The RACF user ID owner.</td>
<td>The value that is specified from the IBM Security Identity Manager server owner for this user.</td>
</tr>
</tbody>
</table>

**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 nonzero return code when the processing is complete. A zero return code indicates successful processing of the `erRacExecname` attribute. If a nonzero return code is presented on exit, the adapter indicates that the `erRacExecname` attribute failed.

The environment in which the ISIMEXIT gets control is in a TSO batch environment. You might call other programs and do file input and output as necessary. Processing is done 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 20. ISIMEXEC processing information

<table>
<thead>
<tr>
<th>Parameter #</th>
<th>Source</th>
<th>Value</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IBM Security Identity Manager attribute of <code>erUid</code></td>
<td>The value of the <code>erUid</code>.</td>
<td>Always, because this attribute accompanies all requests.</td>
</tr>
</tbody>
</table>
Table 20. ISIMEXEC processing information (continued)

<table>
<thead>
<tr>
<th>Parameter #</th>
<th>Source</th>
<th>Value</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>IBM Security Identity Manager attribute of erRacExecname</td>
<td>The value of the erRacExecname.</td>
<td>Always, because the availability of this attribute indicates that this exit must be started.</td>
</tr>
<tr>
<td>3</td>
<td>IBM Security Identity Manager attribute of erRacExecvar</td>
<td>The value of the erRacExecvar.</td>
<td>Based on the request that is generated by the IBM Security Identity Manager server.</td>
</tr>
</tbody>
</table>

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.

SSL authentication for the RACF adapter

You can provide SSL authentication, certificates, and SSL authentication enablement with 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. 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 the server establishes 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 that is exchanged between the applications. Encryption makes data that is transmitted over the network intelligible only to the intended recipient.

Signed digital certificates enable two applications that connect in a network to authenticate their identity. An application that acts 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 that acts as an SSL server so that it requires the application that acts 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 be decrypted only with the corresponding private key. Similarly, the data encrypted with the private key can be decrypted only with 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 certificate section 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 that is 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 expired.
- The CA certificate that is used to verify that it 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 that is 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 various 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 35.

Configuring certificates for SSL authentication:

You can 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" on page 67
- "Configuring certificates for two-way SSL authentication" on page 67
- "Configuring certificates when the adapter operates as an SSL client" on page 68

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 that is sent by the adapter.

In Figure 4, Application A operates as the IBM Security Identity Manager server, and Application B operates as the IBM Security Identity Manager adapter.

Figure 4. One-way SSL authentication (server authentication)

To configure one-way SSL, do 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 that are supplied by the CA. When you submit the CSR, specify that you want the root CA certificate that is returned with the server certificate.
2. On the IBM Security Identity Manager server, perform one of these steps:
If you used a signed certificate that is issued by a well-known CA:
   a. Ensure that the IBM Security Identity Manager server 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.

**Configuring certificates for two-way SSL authentication:**

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

**Before you begin**

Before you do 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 the adapter sends 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 5, the IBM Security Identity Manager server operates as Application A and the IBM Security Identity Manager adapter operates as Application B.

![Figure 5. Two-way SSL authentication (client authentication)](image)

**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 you configure 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 66

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 6 describes how the adapter operates as an SSL server and an SSL client. When the adapter communicates with the IBM Security Identity Manager server, the adapter sends its certificate for authentication. When the adapter communicates with the web server, the adapter receives the certificate of the web server.

Figure 6. 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, do 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

You might 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 product documentation.

Using the certTool utility to manage SSL certificates

You can use the certTool utility to manage private keys and certificates.

About this task

Managing SSL certificates with the certTool utility includes the following tasks:
- "Starting certTool."
- "Generating a private key and certificate request" on page 71.
- "Installing the certificate" on page 72.
- "Installing the certificate and key from a PKCS12 file" on page 73.
- "Viewing the installed certificate" on page 73.
- "Viewing CA certificates" on page 74.
- "Installing a CA certificate" on page 74.
- "Deleting a CA certificate" on page 74.
- "Viewing registered certificates" on page 75.
- "Registering a certificate" on page 75.
- "Unregistering a certificate" on page 76.

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 complete these tasks:
- 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. 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.

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 that is 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 that is 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. You might not upgrade an existing adapter to use CA certificates. In this case, you must register the signed certificate that is 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 certificate 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, take 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 that the adapter is in and press **Enter**. For example, type **TX** if the adapter is in Texas. Some certificate authorities do not accept two letter abbreviations for states. In this case, type the full name of the state.

7. At **Country**, type the country that the adapter is in and press **Enter**.

8. At **Locality**, type the name of the city that the adapter is in and press **Enter**.

9. At **Accept these values**, do 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-----
MIIBIjCCAT8CAQwgZUeXjAOgB6NvBaoTCFhjY2VzcGM2MDEUMBIGA1UECxMLZXW5n
aW51ZXJpbmcxEDA0gGNVAMTBSF50YldIbCQJDAF4qkhkIGzWOBCEQFW50YldI
bnRAYWNjZXNzdlNvbTRMAEwBDaCVMxExARBGbNBAgTCKNhbgHmb3Jzu
awEXdzANBgNVBAcTBEdtYmlydmluZDCmtnANBgkqhkgkAlG9w0BAQwJQwYKmYEA
mR6AcPnwf6hLCC72BmUKAwxRcebtxCoCNNTH9uc8VuhNHPbIMAgjuCsa919Pril19
U1b0fyl6X3R3keRapp90ULyPrIqQ1b4On0whsytij6syCySaFQ1b6Y7PbatFr
6XQ9pnsARd6GytZm5TgG1hSS/jA6mbxgmttz9HPECACWAAAAMGSC5gs1pB3
DQEBAjUA4GBADxAlcDxvkZnTwT9CtQpRN0fZB8u8/HgMRh177jVahJqdb
N1Er46vQsO00k4x2z1Xws0MkmNTXVR19TLZ5Z/D+9mGZcDobc0+1ibAK1ePwyuYxK
Xqdyu3d433HzfJJSNYLYBFkrQjesITqKftQ45g1JywIrbcVUcepL2
-----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, take the following actions:
   a. Copy the text of the certificate to a text file.
b. Copy that file to the read/write data directory of the adapter. For example:
/var.ibm/isimagent/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. You might type DamlSrvr.pfx.
4. At Enter password, type the password to access the file and press Enter.

Results

After you install 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 Dam1CACerts.pem file.

Viewing CA certificates:

Use the certTool utility to view a private key and certificate that are installed for the adapter.

About this task

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

Deleting a CA certificate:

You can delete a CA certificate from the adapter directories.

Procedure

1. At Main Menu, type G to display a list of all CA certificates that are installed on the adapter.
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 you delete 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 web server. 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. You might not upgrade an existing adapter to use CA certificates. In this case, you must register the signed certificate that is presented by the server with the adapter.

**Procedure**

1. At the **Main Menu** prompt, 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.

   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 you register 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** prompt. The utility displays the registered certificates and the **Main** menu. The following example shows a list of the registered certificates:
Unregistering a certificate:
You can unregister a certificate for the adapter.

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

   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 you remove 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:
You can export a certificate and key to a PKCS12 file.

Procedure
1. At the **Main Menu** prompt, 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 you export the certificate or private key to the PKCS12 file, the certTool displays the **Main menu**.

**Adapter language pack installation**

The adapters use a separate language package from the IBM Security Identity Manager.

See the IBM Security Identity Manager library and search for information about installing the adapter language pack.
Chapter 5. RACF Adapter error troubleshooting

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 50.

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 you start 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 operating system, or is it common across multiple 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 are not fully tested together.

**When does the problem occur?**

Develop a detailed timeline of events that lead 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 use 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 done?
• Is a certain sequence of events required 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 occur 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. 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?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

## 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.

### Adapter messages

**RACF UNLOAD missing 0102 record processing**

In case a RACF database unload 0102 record is missing, so the true connect authority value is unknown, `<AUTHORITY>USE</AUTHORITY>` is generated.

In case a 0102 record is missing, a message starting with "Fix0205" is printed to the SYSPRINT of the ISIMRECO program. This message shows the group and user information for which the default authority USE is generated.

### Server messages

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

<table>
<thead>
<tr>
<th>Error message or warning</th>
<th>Additional warnings, messages, or information</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter error message:</td>
<td>Adapter log: ERR:14/07/31 10:42:31</td>
<td>PERMIT READ access for ISIAGNT on BPX.SERVER in CLASS FACILITY</td>
</tr>
<tr>
<td>could not set security</td>
<td>racfModify: pthread_security_np()</td>
<td></td>
</tr>
<tr>
<td>environment for</td>
<td>create failed. errno2=0BE800D8:</td>
<td></td>
</tr>
<tr>
<td>SURROGAT.</td>
<td>EDCS1391 Operation not permitted</td>
<td></td>
</tr>
<tr>
<td>racfSearch: failed</td>
<td>z/OS Syslog might provide INSUFFICIENT</td>
<td>Verify that the adapter RACF ID and SURROGAT ID have read and write access to the READWRITE data directory.</td>
</tr>
<tr>
<td>to create RECOJOB thread</td>
<td>AUTHORITY message</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Could not set security</td>
<td>Not applicable</td>
<td>PERMIT READ access for ISIAGNT on BPX.SRV.&lt;SURROGATID&gt; in CLASS SURROGAT</td>
</tr>
<tr>
<td>environment for</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SURROGAT user</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 21. Error messages, warnings, and corrective actions (continued)

<table>
<thead>
<tr>
<th>Error message or warning</th>
<th>Additional warnings, messages, or information</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfSearch: failed to create RECOJOB thread</td>
<td>DETAIL Adapter log: tsocmd: result is IKJ6644I NO VALID TSO USERID, DEFAULT USER ATTRIBUTES USED</td>
<td>Ensure that the ADAPTER ID has a valid TSO USERID.</td>
</tr>
<tr>
<td>CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again</td>
<td>An IO error occurred sending a request. Error: Connection refused: connect</td>
<td>Ensure that the adapter service is running. For more information about starting the adapter service, see “Starting and stopping the adapter” on page 18.</td>
</tr>
<tr>
<td></td>
<td>The adapter returned an error status for a bind request. Status code: invalid credentials adapter error message: Authentication Failed</td>
<td>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 11.</td>
</tr>
<tr>
<td></td>
<td>An IO error occurred sending a request. Error: com.ibm.daml.jndi.JSSSESocketConnection.HANDSHAKE_FAILED:</td>
<td>If SSL is enabled, check the configuration. See . The adapter log contains details about the certificates that are loaded during initialization.</td>
</tr>
<tr>
<td>User user name add Successful. Some attributes were not modified: attr1,attr2</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>User user name modify Successful. Some attributes were not modified: attr1,attr2</td>
<td></td>
<td>An attempt is made to modify a user account. However, modification failed for certain attributes during the 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.</td>
</tr>
<tr>
<td>CTGIMD812E An error occurred while processing the adapter response message. The following error occurred. Error: Premature end of file.</td>
<td></td>
<td>Ensure that the adapter service is running. For more information about starting the adapter service, see “Starting and stopping the adapter” on page 18.</td>
</tr>
</tbody>
</table>
Table 21. Error messages, warnings, and corrective actions (continued)

<table>
<thead>
<tr>
<th>Error message or warning</th>
<th>Additional warnings, messages, or information</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>tsoCmd: result is YOUR TSO ADMINISTRATOR MUST AUTHORIZE USE OF THIS COMMAND</td>
<td>Not applicable.</td>
<td>PERMIT READ access for ISIAGNT on JCL in CLASS TSOAUTH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example: PE JCL CLASS(TSOAUTH) ID(ISIAGNT) ACCESS(READ) SETROPTS RACLIST(TSOAUTH) REFRESH</td>
</tr>
</tbody>
</table>

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 that is 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 "Adapter configuration for IBM Security Identity Manager" on page 27.
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 18.
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 operating system 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 that is requested, such as System Login Add or Database Login Change.

The adapter software is installed on an operating system and the adapter is defined by Agent Maintenance. You then identify the attribute data that is needed to create the user access. You identify these attributes to IBM Security Identity Manager when you define 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 you create 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 that is defined in a RACF database.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erAccountStatus</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid REVOKE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid RESUME</td>
</tr>
<tr>
<td>erPassword</td>
<td>String</td>
<td>100</td>
<td>Single</td>
<td>W</td>
<td>No</td>
<td>To add or modify:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• If 8 or less:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid Password(value) NOPHRASE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• If 9 or more:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid Password(*) PHRASE(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid NOPASSWORD NOPHRASE</td>
</tr>
</tbody>
</table>

Note: * A generated password is set so that the old password cannot be used.
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacExecName</td>
<td>String</td>
<td>44</td>
<td>Single</td>
<td>W</td>
<td>No</td>
<td>To add or modify: ISIMEEXEC userid value</td>
</tr>
<tr>
<td>Exec name - not a RACF attribute, but for compatibility with old RASEXEC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacExecVar</td>
<td>String</td>
<td>44</td>
<td>Single</td>
<td>W</td>
<td>No</td>
<td>This argument is the second argument (value) to the ISIMEEXEC call for erRacExecName.</td>
</tr>
<tr>
<td>Exec Attribute - not a RACF attribute, but for compatibility with old RASEXEC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacRequester</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>W</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUClauth</td>
<td>String</td>
<td>8</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid CLAUTH(value)</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUCreDate</td>
<td>Date</td>
<td></td>
<td>Single</td>
<td>R</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Date user was created.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUDfltgrp</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td>To add or modify: ALU userid DFLTGRP(value)</td>
</tr>
<tr>
<td>Name of existing group that is the initial and default group this user is associated with.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUInstData</td>
<td>String</td>
<td>254</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DATA('value')</td>
</tr>
<tr>
<td>Installation defined data that can be associated with a user.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUIsADSP</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid ADSP</td>
</tr>
<tr>
<td>User can automatically create discrete data set profiles.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IBM Security Identity Manager: RACF Adapter Installation and Configuration Guide
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUIsAudit</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid AUDITOR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOAUDITOR</td>
</tr>
<tr>
<td>erRacUIsCICSSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid CICS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOCICS</td>
</tr>
<tr>
<td>erRacUCICSIsForc</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid CICS (XRFSOFF(FORCE))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid CICS (XRFSOFF(NOFORCE))</td>
</tr>
<tr>
<td>erRacUCICSOpclas</td>
<td>Integer</td>
<td>2</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid CICS (OPCLASS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid CICS (NOOPCLASS)</td>
</tr>
<tr>
<td>erRacUCICSPsid</td>
<td>String</td>
<td>3</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid CICS (OPID(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid CICS (NOOPID)</td>
</tr>
<tr>
<td>erRacUCICSPrtty</td>
<td>Integer</td>
<td>3</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid CICS (OPPRTY(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid CICS (NOOPPRTY)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>--------------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>erRacUCICSTimeout</td>
<td>Time</td>
<td>4</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid CICS (TIMEOUT(value)) To delete: ALU userid CICS (NOTIMEOUT)</td>
</tr>
<tr>
<td>erRacUIsDCESeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DCE To delete: ALU userid NODE</td>
</tr>
<tr>
<td>erRacUDCEIsAutoL</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DCE (AUTOLOAD(YES)) To delete: ALU userid DCE (NOAUTOLOAD)</td>
</tr>
<tr>
<td>erRacUDCEHomeC</td>
<td>String</td>
<td>1023</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DCE (HOMECELL(value)) To delete: ALU userid DCE (NOHOMECELL)</td>
</tr>
<tr>
<td>erRacUDCEHomeU</td>
<td>String</td>
<td>36</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DCE (HOMEUUID(value)) To delete: ALU userid DCE (NOHOMEUUID)</td>
</tr>
</tbody>
</table>
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUDCEName</td>
<td>String</td>
<td>1023</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DCE (DCENAME(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid DCE (NODCENAME)</td>
</tr>
<tr>
<td>erRacUDCEUUID</td>
<td>String</td>
<td>36</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DCE (UUID(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid DCE (NOUUID)</td>
</tr>
<tr>
<td>erRacUIsDFPSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DFP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid DFP (NODFP)</td>
</tr>
<tr>
<td>erRacUDFPApppl</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DFP (DATAAPPL(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid DFP (NODATAAPPL)</td>
</tr>
<tr>
<td>erRacUDFPData</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DFP (DATACLAS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid DFP (NODATACLAS)</td>
</tr>
</tbody>
</table>
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUDFPMgmt</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DFP (MGMTCLAS(value))</td>
</tr>
<tr>
<td>MGMTCLAS name to be used for new file creation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid DFP (NOMGMTCLAS)</td>
</tr>
<tr>
<td>erRacUDFPStor</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid DFP (STORCLAS(value))</td>
</tr>
<tr>
<td>STORCLAS name to be used for new file creation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid DFP (NOSTORCLAS)</td>
</tr>
<tr>
<td>erRacUIsEimSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid EIM</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOEIM</td>
</tr>
<tr>
<td>erRacUEimLDAPNam</td>
<td>String</td>
<td>246</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid EIM (LDAPPROF(value))</td>
</tr>
<tr>
<td>Name of profile in the LDAPBIND class.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid EIM (NOLDAPPROF)</td>
</tr>
<tr>
<td>erRacUIsGrpacc</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid GRPACC</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOGRPACC</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>erRacUIsKerbSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid KERB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOKERB</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUKerbIsDES</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid KERB (ENCRYPT(DS))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid KERB (ENCRYPT(NODES))</td>
</tr>
<tr>
<td>Single length DES keys allowed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUKerbIsDES3</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid KERB (ENCRYPT(DS))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid KERB (ENCRYPT(NODES3))</td>
</tr>
<tr>
<td>Triple DES keys allowed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUKerbIsDESD</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid KERB (ENCRYPT(DS))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid KERB (ENCRYPT(NODES3))</td>
</tr>
<tr>
<td>Double DES keys allowed.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUKerbName</td>
<td>String</td>
<td>240</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td>To add or modify: ALU userid KERB (KERBNAME(value))</td>
</tr>
<tr>
<td>Kerberos Principal name. can consist of any character except the @+ (X7C) character. Avoid the use of any of the EBCDIC variant characters to prevent problems between different code pages.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid KERB (NOKERBNAME)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>erRacUKerbTickMx</td>
<td>Integer</td>
<td>10</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid KERB (MAXTKT(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid KERB (NOMAXTKT)</td>
</tr>
<tr>
<td>erRacULsLangSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid LANGUAGE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOLANGUAGE</td>
</tr>
<tr>
<td>erRacULangPrime</td>
<td>String</td>
<td>3</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid LANG (PRIM(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid LANG (NOPRIM)</td>
</tr>
<tr>
<td>erRacULangSec</td>
<td>String</td>
<td>3</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid LANG (SEC(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid LANG (NOSEC)</td>
</tr>
<tr>
<td>erRacULsLNotesSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid LNOTES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOLNOTES</td>
</tr>
</tbody>
</table>

Maximum ticket life, in seconds. Valid value range is 1 - 2,147,483,647.

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.

Primary user language.

Secondary user language.

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.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
</table>
| erRacULnotesSNam | String | 64 | Single | RW | No | To add or modify: ALU userid LNOTES (SNAME(value))
| | | | | | | To delete: ALU userid LNOTES (NOSNAME) |
| erRacULIsNetvSeg | String | 5 | Single | RW | No | To add or modify: ALU userid NETVIEW
| | | | | | | To delete: ALU userid NONETVIEW |
| erRacUNetvCons | String | 8 | Single | RW | No | To add or modify: ALU userid NETV (CONSNAM(value))
| | | | | | | To delete: ALU userid NETV (NOCONSNAM) |
| erRacUNetvCtl | String | 8 | Single | RW | No | To add or modify: ALU userid NETV (CTL(value))
| | | | | | | To delete: ALU userid NETV (NOCTL) |
| erRacUNetvDomain | String | 5 | Multiple | RW | No | To add or modify: ALU userid NETV (DOMAIN(value))
| | | | | | | To delete: ALU userid NETV (NODOMAIN) |
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUNetvGSpan</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid NETV (NGMVFSPN(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NETV (NONGMVFSPN)</td>
</tr>
<tr>
<td>erRacUNetvIC</td>
<td>String</td>
<td>255</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid NETV (IC(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NETV (NOIC)</td>
</tr>
<tr>
<td>erRacUNetvIsGMF</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid NETV (NGMVADMN(YES))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NETV (NONGMVADMN)</td>
</tr>
<tr>
<td>erRacUNetvIsMR</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid NETV (MSGRECVR(YES))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NETV (NOMSGRECVR)</td>
</tr>
<tr>
<td>erRacUNetvOpclas</td>
<td>Integer</td>
<td>4</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid NETV (OPCLASS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NETV (NOOPCLASS)</td>
</tr>
<tr>
<td>erRacUIsOMVSSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMWS (</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOOMVS</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>erRacUOMVSCPU</td>
<td>Integer</td>
<td>10</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (CPUTIM(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOCPUTIM)</td>
</tr>
<tr>
<td>erRacUOMVSFiles</td>
<td>Integer</td>
<td>6</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (FILE(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOFILE)</td>
</tr>
<tr>
<td>erRacUOMVSHome</td>
<td>String</td>
<td>1024</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (HOME(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOHOME)</td>
</tr>
<tr>
<td>erRacUOMVSSIsShar</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>W</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (UID(value)SHARED)</td>
</tr>
<tr>
<td>erRacUOMVSMmap</td>
<td>Integer</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (MMAP(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOMMAP)</td>
</tr>
<tr>
<td>erRacUOMVSProc</td>
<td>Integer</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (PROC(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOPROC)</td>
</tr>
</tbody>
</table>
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUOMVSShell</td>
<td>String</td>
<td>1024</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (PROG(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOPROG)</td>
</tr>
<tr>
<td>erRacUOMVSSstor</td>
<td>Integer</td>
<td>10</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (ASSIZE(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOASSIZE)</td>
</tr>
<tr>
<td>erRacUOMVSThread</td>
<td>Integer</td>
<td>6</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (THREAD(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOTHREAD)</td>
</tr>
<tr>
<td>erRacUOMVSuid</td>
<td>String</td>
<td>10</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OMVS (UID(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OMVS (NOUID)</td>
</tr>
<tr>
<td>erRacUISOper</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERATIONS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOOPERATIONS</td>
</tr>
</tbody>
</table>
### Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUIsOperSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERPARM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid NOOPERPARM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUOpAltgrp</td>
<td>Character</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (ALTGRP(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid OPERP (NOALTGRP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUOpAuth</td>
<td>Character</td>
<td>6</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (AUTH(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid OPERP (NOAUTH)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUOpAuto</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (AUTO(YES))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid OPERP (NOAUTO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUOpCmdsys</td>
<td>Character</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (CMDSYS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid OPERP (NOCMDSYS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUOpDom</td>
<td>Character</td>
<td>6</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (DOM(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NODOM)</td>
</tr>
<tr>
<td>erRacUOpKey</td>
<td>Character</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (KEY(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOKEY)</td>
</tr>
<tr>
<td>erRacUOpLevel</td>
<td>Character</td>
<td>3</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (LEVEL(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOLEVEL)</td>
</tr>
<tr>
<td>erRacUOpLogcmd</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (LOGCMDR(NO))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOLOGCMDR)</td>
</tr>
<tr>
<td>erRacUOpMform</td>
<td>Character</td>
<td>5</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (MFORM(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOMFORM)</td>
</tr>
</tbody>
</table>

- Valid values are ‘Normal’, ‘All’, or ‘None’.
- Valid values are A-Z, 0-9, @, #, $.
- Valid values are SYSTEM or NONE.
- Message form of the messages that are displayed on the extended console. Valid values are: J, M, S, T, X.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUOpMigid</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (MIGID(YES))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOMIGID)</td>
</tr>
<tr>
<td>erRacUOpMonitor</td>
<td>Character</td>
<td>9</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (MONITOR(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOMONITOR)</td>
</tr>
<tr>
<td>erRacUOpMscope</td>
<td>Character</td>
<td>8</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (MSCOPE(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOMSCOPE)</td>
</tr>
<tr>
<td>erRacUOpRoutCode</td>
<td>Integer</td>
<td>3</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (ROUTC(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOROUTCR)</td>
</tr>
<tr>
<td>erRacUOpStor</td>
<td>Integer</td>
<td>4</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (STORAGE(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOSTORAGE)</td>
</tr>
<tr>
<td>erRacUOpUD</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid OPERP (UD(YES))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid OPERP (NOUD)</td>
</tr>
<tr>
<td>erRacULsProtect</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid NOPASSWORD NOPHRASE</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>erRacUIsPrxSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid PROXY To delete: ALU userid NOPROXY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUPrxBindDN</td>
<td>Binary</td>
<td>1023</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid PROXY (BINDDN(value)) To delete: ALU userid NOPROXY</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUPrxBindHst</td>
<td>Binary</td>
<td>1023</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid PROXY (LDAPHOST(value)) To delete: ALU userid NOPROXY (NOSECONDHOST)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUPrxBindPW</td>
<td>String</td>
<td>128</td>
<td>Single</td>
<td>W</td>
<td>No</td>
<td>To add or modify: ALU userid PROXY (BINDPW(value)) To delete: ALU userid NOPROXY (NOSECONDHOST)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUIsRestrict</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid RESTRICTED To delete: ALU userid NORESTRICTED</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUIsSpecial</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid SPECIAL To delete: ALU userid NOSPECIAL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 22. Account form attributes (continued)**

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.

Bind DN of user on target host.

A URL of a host, which the local z/OS LDAP server contacts on behalf of the user.

Bind password for erRacUPrxBindDN.

User cannot be granted access through UACC or ID(*) in resource profiles.

User has system Special. System Security Administrator.
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUIsTSOSeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOTSO</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUTSOAcct</td>
<td>String</td>
<td>40</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (ACCT(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOACCT)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUTSOCmd</td>
<td>String</td>
<td>80</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (COMMAND(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOCOMMAND)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUTSODest</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (DEST(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NODEST)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUTSOHold</td>
<td>String</td>
<td>1</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (HOLDCLASS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOHOLDCLASS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacUTSOMsg</td>
<td>String</td>
<td>1</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (MSGCLASS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOMSGCLASS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>--------------</td>
<td>-----------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>erRacUTSOJob</td>
<td>String</td>
<td>1</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (JOBCLASS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOJOBCLASS)</td>
</tr>
<tr>
<td>erRacUTSOMax</td>
<td>Integer</td>
<td>7</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (MAXSIZE(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOMAXSIZE)</td>
</tr>
<tr>
<td>erRacUTSOProc</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (PROC(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOPROC)</td>
</tr>
<tr>
<td>erRacUTSOSize</td>
<td>Integer</td>
<td>7</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (SIZE(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOSIZE)</td>
</tr>
<tr>
<td>erRacUTSOSout</td>
<td>String</td>
<td>1</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (SYSOUT(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOSYSOUT)</td>
</tr>
<tr>
<td>erRacUTSOUUnit</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (UNIT(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOUNIT)</td>
</tr>
<tr>
<td>erRacUTSOUdata</td>
<td>String</td>
<td>4</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid TSO (USER(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid TSO (NOUSER)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>--------------</td>
<td>-----------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>erRacUIsUaudit</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid AUDIT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid NOAUDIT</td>
</tr>
<tr>
<td>erRacUIsWASeg</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORKATTR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid NOWORKATTR</td>
</tr>
<tr>
<td>erRacUWAAcct</td>
<td>String</td>
<td>255</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORK (WACNT('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORK (NOWAACCNT)</td>
</tr>
<tr>
<td>erRacUWAAddr1</td>
<td>String</td>
<td>60</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORK (WAADDR1('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORK (NOWAADDR1)</td>
</tr>
<tr>
<td>erRacUWAAddr2</td>
<td>String</td>
<td>60</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORK (WAADDR2('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORK (NOWAADDR2)</td>
</tr>
<tr>
<td>erRacUWAAddr3</td>
<td>String</td>
<td>60</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORK (WAADDR3('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ALU userid WORK (NOWAADDR3)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Max. length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>erRacUWAAddr4</td>
<td>String</td>
<td>60</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid WORK (WAADDR4('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid WORK (NOWAADDR4)</td>
</tr>
<tr>
<td>erRacUWABldg</td>
<td>String</td>
<td>60</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid WORK (WABLDG('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid WORK (NOWABLDG)</td>
</tr>
<tr>
<td>erRacUWADept</td>
<td>String</td>
<td>60</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid WORK (WADEPT('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid WORK (NOWADEPT)</td>
</tr>
<tr>
<td>erRacUWAName</td>
<td>String</td>
<td>60</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid WORK (WANAME('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid WORK (NOWANAME)</td>
</tr>
<tr>
<td>erRacUWARoom</td>
<td>String</td>
<td>60</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid WORK (WAROOM('value'))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid WORK (NOWAROOM)</td>
</tr>
<tr>
<td>erRacULogtime</td>
<td>Time</td>
<td></td>
<td>Single</td>
<td>R</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>erRacUModel</td>
<td>String</td>
<td>44</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid MODEL (value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NOMODEL</td>
</tr>
</tbody>
</table>
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacUName</td>
<td>String</td>
<td>20</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU userid NAME ('value')</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid NAME ('####################################')</td>
</tr>
<tr>
<td>erRacUOwner</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td>To add or modify: ALU userid OWNER (value)</td>
</tr>
<tr>
<td>erRacUPassdate</td>
<td>Date</td>
<td></td>
<td>Single</td>
<td>R</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>erRacUPWInterval</td>
<td>Integer</td>
<td>3</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: PW USER (userid) INTERVAL (value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: PW USER userid NOINTERVAL</td>
</tr>
<tr>
<td>erRacUPWNoExpire</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>W</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>erRacUResumeDate</td>
<td>Date</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU (userid) RESUME (value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid RESUME</td>
</tr>
</tbody>
</table>

Note: The attribute 'erPassword' has been removed from the schema and is an adapter option instead.
Table 22. Account form attributes (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacURevokeDate</td>
<td>Date</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU (userid) REVOKE (value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid RESUME</td>
</tr>
<tr>
<td>erRacUWhenDays</td>
<td>String</td>
<td>9</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU (userid) WHEN (DAYS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid WHEN (DAYS (ANYDAY))</td>
</tr>
<tr>
<td>erRacUWhenTime</td>
<td>Time</td>
<td>9</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALU (userid) WHEN (TIME(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALU userid WHEN (TIME (ANYTIME))</td>
</tr>
<tr>
<td>erUid</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**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 23. erRacUser attribute information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacConAuth</td>
<td>String</td>
<td>7</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: CO userid GROUP value AUTH value</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: CO userid GROUP value AUTH (USE)</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>--------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>erRacConCDate</td>
<td>Date</td>
<td>7</td>
<td>Single</td>
<td>R</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Connect entry creation date.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacConCount</td>
<td>Integer</td>
<td>5</td>
<td>Single</td>
<td>R</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Connect count. Max value of 65,535.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacConGroup</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td>To add or modify: CO userid GROUP(value)</td>
</tr>
<tr>
<td>Name of group to which user is connected.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacConIsADSP</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value) ADSP</td>
</tr>
<tr>
<td>User can automatically create discrete data set profiles.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacConIsAudit</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value) AUDITOR</td>
</tr>
<tr>
<td>User has system Auditor ability.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacConIsGrpac</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value) GRPAC</td>
</tr>
<tr>
<td>Enables group level access of UPDATE to the group under the High Level Qualifier of any data set profile that is created through ADSP by this user.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacConIsOper</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value) OPERATIONS</td>
</tr>
<tr>
<td>User has system Operations ability (ability to read and modify any file).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>erRacConIsSpec</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value) SPECIAL</td>
</tr>
<tr>
<td>User has system Special. System security Administrator.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>---------------</td>
<td>-----------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>erRacConLogtime</td>
<td>Time</td>
<td></td>
<td>Single</td>
<td>R</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OWNER(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CO userid GROUP(value) RESUME(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CO userid GROUP(value) REVOKE(value)</td>
</tr>
<tr>
<td>erRacConOwner</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td>To add or modify: CO userid GROUP(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>OWNER(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CO userid GROUP(value) RESUME(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CO userid GROUP(value) REVOKE(value)</td>
</tr>
<tr>
<td>erRacConResumDt</td>
<td>Date</td>
<td>8</td>
<td>Single</td>
<td>R</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RESUME(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CO userid GROUP(value) RESUME(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CO userid GROUP(value) REVOKE(value)</td>
</tr>
<tr>
<td>erRacConRevokDt</td>
<td>Date</td>
<td>8</td>
<td>Single</td>
<td>R</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REVOKE(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CO userid GROUP(value) REVOKE(value)</td>
</tr>
<tr>
<td>erRacConUACC</td>
<td>String</td>
<td>7</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: CO userid GROUP(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UACC(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CO userid GROUP(value) UACC(value)</td>
</tr>
<tr>
<td>erRacConXML</td>
<td>String</td>
<td></td>
<td>Multiple</td>
<td>RW</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
**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 currently managed or updated by IBM Security Identity Manager. Although optional segments are provided in this documentation, their implementation is to be decided later.

Table 24. *erRacGrp* attribute information

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Data type</th>
<th>Maximum length</th>
<th>Single or multiple value</th>
<th>Read or write</th>
<th>Required?</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>erRacGrpCDate</td>
<td>Date</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td>To add or modify: ALG userid DATA(value)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid NODATA</td>
</tr>
<tr>
<td>erRacGrpData</td>
<td>String</td>
<td>225</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid DFP(DATAAPPL(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid DFP(NODATAAPPL)</td>
</tr>
<tr>
<td>erRacGrpDFPAppl</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid DFP(DATACLASS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid DFP(NODATACLASS)</td>
</tr>
<tr>
<td>erRacGrpDFPData</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid DFP(MGMTCLASS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid DFP(NOMGMTCLASS)</td>
</tr>
<tr>
<td>erRacGrpDFPMgmt</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid DFP(STORCLASS(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid DFP(NOSTORCLASS)</td>
</tr>
<tr>
<td>erRacGrpIsDFP</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid DFP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid NODFP</td>
</tr>
<tr>
<td>Attribute</td>
<td>Data type</td>
<td>Maximum length</td>
<td>Single or multiple value</td>
<td>Read or write</td>
<td>Required?</td>
<td>Commands</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>--------------</td>
<td>-----------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>erRacGrpIsOMVS</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid OMVS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid NOOMVS</td>
</tr>
<tr>
<td>erRacGrpIsTME</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid TME</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid NOTME</td>
</tr>
<tr>
<td>erRacGrpIsUni</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>erRacGrpName</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>R</td>
<td>Yes</td>
<td>To add or modify: ALG userid OWNER(value)</td>
</tr>
<tr>
<td>erRacGrpOMVSGid</td>
<td>Integer</td>
<td>10</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid OMVS(GID(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid OMVS(NOGID)</td>
</tr>
<tr>
<td>erRacGrpOwner</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td>To add or modify: ALG userid OWNER(value)</td>
</tr>
<tr>
<td>erRacGrpSubgrp</td>
<td>String</td>
<td>8</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>erRacGrpSuper</td>
<td>String</td>
<td>8</td>
<td>Single</td>
<td>RW</td>
<td>Yes</td>
<td>To add or modify: ALG userid SUPGROUP(value)</td>
</tr>
<tr>
<td>erRacGrpTMERole</td>
<td>String</td>
<td>8</td>
<td>Multiple</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid TME(ROLES(value))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid TME(NOROLES)</td>
</tr>
<tr>
<td>erRacGrpTUACC</td>
<td>String</td>
<td>5</td>
<td>Single</td>
<td>RW</td>
<td>No</td>
<td>To add or modify: ALG userid TERMUACC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>To delete: ALG userid NOTERMUACC</td>
</tr>
</tbody>
</table>

Table 24. erRacGrp attribute information (continued)
Appendix B. Registry settings

The following table lists valid registry options, their values, and meanings.

Table 25. Registry settings and information

<table>
<thead>
<tr>
<th>Option attribute</th>
<th>Default value</th>
<th>Valid value</th>
<th>Function and meaning</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATADIR</td>
<td>adapter_readwrite_home/data</td>
<td>adapter_readwrite_home/data</td>
<td>Specifies the USS Adapter read/write home. This parameter must be the read/write home as specified in the Disk location parameters panel during installation. This is where the registry.dat and the UDF.dat files are stored.</td>
<td>Yes</td>
</tr>
<tr>
<td>DSJOB</td>
<td>'hlq'.CNTL</td>
<td>Any data set accessible by the Adapter RACF ID and optionally the SURROGAT RACF ID where the RECOJOB JCL is stored</td>
<td>Specifies the data set where the RECOJOB is located.</td>
<td>YES</td>
</tr>
<tr>
<td>ISIMEXIT</td>
<td>'hlq'.EXEC</td>
<td>Any data set accessible by the Adapter RACF ID and optionally the SURROGAT RACF ID where the ISIMEXIT/ISIMEXEC REXX scripts are stored</td>
<td>The adapter uses this value to initialize the ISIMEXIT/ISIMEXEC REXX scripts</td>
<td>Yes</td>
</tr>
<tr>
<td>PASSEXPIRE</td>
<td>TRUE</td>
<td>TRUE, FALSE, or TRUEADD</td>
<td>This attribute is the default action that the adapter must do when the adapter receives a password or pass phrase change request. TRUE indicates that passwords or pass phrases must be set as expired. FALSE indicates that passwords or pass phrases must be set as non-expired. When set to TRUEADD, a password or pass phrase for a new user is set to EXPIRED. A password or pass phrase 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.</td>
<td></td>
</tr>
<tr>
<td>Option attribute</td>
<td>Default value</td>
<td>Valid value</td>
<td>Function and meaning</td>
<td>Required?</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>------------</td>
<td>----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>RACFRC</td>
<td>60</td>
<td>3 – 99</td>
<td>The amount of time in seconds the adapter waits for the RECOJOB job to complete processing.</td>
<td>Yes</td>
</tr>
<tr>
<td>RECOSAVE</td>
<td>'hlq'.SAVE</td>
<td>Any data set accessible by the Adapter RACF ID and optionally the SURROGAT RACF ID</td>
<td>Specifies the data set where the intermediate reconciliation results are stored by RECOJOB. The adapter accesses these data set as soon as the status of RECOJOB is completed to collected and further process the results.</td>
<td>Yes</td>
</tr>
<tr>
<td>SCOPING</td>
<td>None</td>
<td>TRUE or FALSE</td>
<td>Scoping is automatically set to TRUE when the VSAM data set file name, which is required to perform scoped reconciliations, is configured during installation. See “Reconciliation Processor” in “Overview of the RACF Adapter” on page 1.</td>
<td>No</td>
</tr>
<tr>
<td>Option attribute</td>
<td>Default value</td>
<td>Valid value</td>
<td>Function and meaning</td>
<td>Required?</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>SHORTCONNECT</td>
<td>FALSE</td>
<td>TRUE or FALSE</td>
<td>When SHORTCONNECT is set to TRUE, the CONNECT entries, do not contain LOGON COUNT, CREATION DATE, LASTLOGON DATE. This setting enables the use of a simple string compare and mitigates the need for the CUSTOM JOIN DIRECTIVE. (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: <code>&lt;CONNECT_ENTRY name=&quot;/CONENTRY&quot;&gt; &lt;ADSP&gt;FALSE&lt;/ADSP&gt; &lt;AUDITOR&gt;FALSE &lt;/AUDITOR&gt; &lt;AUTHORITY&gt;USE &lt;/AUTHORITY&gt; &lt;DATE&gt;200312101200Z &lt;/DATE&gt; &lt;GRPACC&gt;FALSE&lt;/GRPACC&gt; &lt;LAST_DATE&gt;200312101200Z &lt;/LAST_DATE&gt; &lt;LOGON_COUNT&gt;0 &lt;/LOGON_COUNT&gt; &lt;OPERATIONS&gt;FALSE &lt;/OPERATIONS&gt; &lt;OWNER&gt;/CONENTRY &lt;/OWNER&gt; &lt;REVOKE_DATE&gt;200312101200Z&lt;/REVOKE_DATE&gt; &lt;REVOKED&gt;FALSE&lt;/REVOKED&gt; &lt;SPECIAL&gt;FALSE&lt;/SPECIAL&gt; &lt;UACC&gt;NONE&lt;/UACC&gt;&lt;/CONNECT_ENTRY&gt;</code> ) This option addresses a policy implementation issue that occurs building a provisioning policy for RACF accounts. When a straight string compare is done between the “policy” version of a connect entry and the value in the erRac-ConXML, the policy returns a mismatch. This mismatch occurs because of the transient behavior of creation date, last logon date and time, logon count, and future revoke and 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. <strong>Note:</strong> When the SHORTCONNECT option is not specified in the registry, the adapter acts as if it is set to TRUE.</td>
<td>No</td>
</tr>
</tbody>
</table>
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 26. RACF Adapter environment variables

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Meaning or use</th>
<th>Default value</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIBPATH</td>
<td>Specify the location of the Dynamic Link Library (DLL) and .so files.</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td>PDU_ENTRY_LIMIT</td>
<td>Specify the maximum number of accounts that are kept in the main storage.</td>
<td>2000. The range is 50-3000.</td>
<td>No</td>
</tr>
<tr>
<td>PROTOCOL_DIR</td>
<td>Specify the fully qualified location of the directory where the .so and .dll files are.</td>
<td>LIBPATH</td>
<td>No</td>
</tr>
<tr>
<td>REGISTRY</td>
<td>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.</td>
<td>Current® working directory.</td>
<td>No</td>
</tr>
</tbody>
</table>
Appendix D. Support information

You have several options to obtain support for IBM products.

- “Searching knowledge bases”
- “Obtaining a product fix” on page 120
- “Contacting IBM Support” on page 120

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 product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation 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](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos).

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
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 that are required to get the fix. You can obtain product fixes from the Fix Central Site. See [http://www.ibm.com/support/fixcentral/](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, answers FAQs, and helps users resolve problems with the product.

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”.

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.
     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](https://www.ibm.com/support) 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](https://www.ibm.com/servers/support/contact) 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.
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 library, 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 more 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 use 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.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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:

If you are viewing this information softcopy, the photographs and color 
illustrations might not appear.

© (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 

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.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer 
Entertainment, Inc., in the United States, other countries, or both and is used under 
license therefrom.
Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, and to tailor interactions with the end user or for other purposes. In many cases, no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details/us/en sections entitled “Cookies, Web Beacons and Other Technologies and Software Products and Software-as-a Service”.

IBM Security Identity Manager: RACF Adapter Installation and Configuration Guide
Index

A
accessibility x, 123
activity logging settings changing 50
enabling 50
options 50
adapter
access request process 87
account form attributes 87
agentCfg 27
code page, changing 55
configuration 9
configuration tool
agentCfg 27, 33
starting 33
configuring 23
connectivity 1
customization 59
database operations 3
environment
issues 3
variables 117
installation
plans 7
tasks 9
interactions with IBM Security Identity Manager server 5
introduction 1
log files 81
overview ix, 1
package, uploading 11
prerequisites 8
RACF
ID on service form 3
information access 19
installation job streams 19
registry settings 113
required privileges 3
requirements 8
service
attributes 25
creating 23, 25
starting 18
stopping 18
TCP/IP protocol 5
troubleshooting
errors 77
logging levels 77
warnings 77
uninstalling 85
upgrading 85
user tasks 5
adapter profile
importing 23
verifying
installation 23
service creation 24
administrator authority prerequisites 8
agent main configuration menu 30
agentCfg
adapter parameters
configuration key, changing 49
advanced settings
options, changing 54
configuration settings, viewing 34
menus
arguments 57
event notification 38
help 57
attributes
attribute-value pair 45
for search 45
multiple service instances 45
authentication
certificate configuration for SSL 66
two-way SSL configuration 67
authorization, passwords 21
autoid
OMVS segment support 21
profile definition 21
certificate authority
certificate
deleting 74
certTool usage 74
deleting 74
installation 74
viewing 74
viewing installed 73
certificate signing request
definition 71
file, generating 71
certificate signing request (CSR), examples 72
certificates
certTool usage 75
configuration for SSL 66
digital certificates 63
examples of signing request (CSR) 72
exporting to PKCS12 file 76
installation 73, 74
installation, from file 72
installation, using certTool 72
key formats 65
management tools 65
management with certTool 69
one-way SSL authentication 66
overview 63
private keys 63
protocol configuration tool
certTool 63
registering 75
removing 76
self-signed 64
unregistering 76
viewing 73, 74
viewing registered 75
z/OS adapters 74
certTool
certificate configuration 66
certificate installation 72
initialization 69
private key, generating 71
private keys and certificates, managing 69
registered certificates, viewing 75
SSL authentication enablement 62
SSL certificate management 69
certTool, changing adapter parameters 65
code page changing 55
compatibility
ISIMEXEC exec 61
with earlier versions 61
configuration key
changing with agentCfg 49
default value 49
default values 33
modifications 33
one-way SSL authentication 66
settings
default values 34
viewing with agentCfg 34
collection
secure 62
CSR 71
D
DAML
communication protocol 62
DAML protocol
configuration 35
default communication 62
default values 35
identifying the server 39
properties 35
SSL authentication 65
detail log
purpose 51
dn, pseudo 46
download, software 8
E
education x
certificate
encryption SSL 63
certificate, SSL 63
environment variables
usage 117
values 117
error messages 79
event notification
configuring with agentCfg 38

© Copyright IBM Corp. 2012, 2014
event notification (continued)
context
  baseline database removal 49
  modifying 43
  multiple purposes 43
  multiple services 43
  reconciliation 49
  search attributes 43
  target DN, configuring 44
  value-attribute pairs 43
options 39
reconciliation data 38
setting on IBM Security Identity Manager server 39
triggers, setting 42

IBM
  Software Support x
  Support Assistant x
IBM Support Assistant 120
installation
  certificate 72
  certificates for z/OS adapters 74
  language pack 76
  plan 7
  prerequisites 8
  private key 73
  roadmap 7
ISA 120
ISIMEXIT exec 59
ISPF dialog
  adapter run time customization 12
  high-level qualifier 11
  installing 9, 11
  running 9, 12

keys, exporting to PKCS12 file 76
knowledge bases 119

language pack
  installation 76
  same for adapters and server 76
log files
  adapter 81
  location 81
  naming 81
  viewing statistics 55

messages
  error 79
  warning 79
  multiple service instances 45

network connectivity prerequisites 8
non-encrypted registry settings, modifying 52
notices 125

one-way SSL authentication 66
online
  publications ix
  terminology ix
operating system prerequisites 8
options, access 69
overview 1

parameters
  options 69
  pass phrase, reset authorization 21
passwords
  authorization 21
  changing configuration key 49
  configuration key, default value 49
  configuration keys, default value 33
  reset authorization 21
  surrogate user IDs 21
PKCS12 file
  certificate installation 73
  exporting certificate and key 76
  importing 65
  preinstallation roadmap 7
  prerequisites for installation
  administrator authority 8
  network connectivity 8
  server communication 8
private key
  generating 71
  installation 73
  problem-determination x
protocol
  configuration settings 35
  DAML 35
  SSL
  two-way configuration 68
pseudo-distinguished names 46
public keys 63
publications
  accessing online ix
  list of ix

software
  download 8
  website 8
SSL
  authentication, certificate configuration 66
  authentication, certTool 62
  authentication, enablement 62
  authentication, one-way 66
  authentication, overview 62
  certificate
    self-signed 64
    signing request 71
certTool, certificate management 69
configuration 62
configuring the adapter to use 39
DAML protocol 65
digital certificates 63
encryption 63
key formats 65
overview 63
private keys 63
two-way configuration 68

statistics, viewing 55
support contact information 120
surrogate user
  class profile 20
  level of authority 20

target DN, configuring event notification 44
terminology ix
testing connection 25
training x
triggers, event notification 42
troubleshooting
  contacting support 120
  error messages 79
  getting fixes 120
  identifying problems 77
  searching knowledge bases 119
troubleshooting (continued)
  support website x
  techniques 77
  warning messages 79
  two-way configuration
    SSL
      certificates 67
      client and server 68

U
unix system services
  two address spaces 23
uploading adapter package 9, 11
user ID, defining 19
USS
  single address space 23

W
warning messages 79

Z
z/OS operating systems
  adapter package uploading,
    extracting 11
  Time Sharing Option format 11