Second Edition (March 2006)
This edition applies to Version 1, Release 1, of the IBM Tivoli Security Administrator for RACF and to all subsequent releases and modifications until otherwise indicated in new editions.
This edition replaces SC18-9476-01.
© Copyright International Business Machines Corporation 2006. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Preface

Welcome to the IBM® Tivoli® Security Administrator for RACF®. This product extends RACF configuration and control support to Security Administrator for RACF clients running on z/OS or Windows.

The IBM Tivoli Security Administrator for RACF User’s Guide provides configuration and utilization instructions.

Who should read this book

The target audience for this users guide includes:

- RACF security administrators

Readers should be familiar with:

- Basic LDAP concepts
- Basic RACF concepts

What this book contains

This book contains the following chapters:

- Chapter 1, “Introduction,” on page 1 provides an overview of the Security Administrator, client functionality, and introduces interface concepts and definitions.
- Chapter 2, “Installation instructions,” on page 7 describes the contents of the software package, installation requirements, and provides client installation instructions.
- Chapter 3, “Security Administrator PC client,” on page 9 provides client configuration instructions, and describes how to use the PC client.
- Chapter 4, “Security Administrator ISPF client,” on page 31 provides client configuration instructions, and describes how to use the ISPF client.

Publications

The Security Administrator for RACF library is organized into the following categories:

- Release information
- Base information

Release information

- IBM Tivoli Security Administrator for RACF Release Notes
  SC18-9476-00
  Provides late-breaking information, such as software limitations, workarounds, and documentation updates.
Base information

- **IBM Tivoli Security Administrator for RACF Program Directory**
  GI10-8678-00
  Explains how to install the Security Administrator server software.

- **IBM Tivoli Security Administrator for RACF Installation Guide**
  GC18-9475-01
  Explains how to install the Security Administrator server software.

- **IBM Tivoli Security Administrator for RACF Advanced Configuration Guide**
  SC31-6932-00
  Explains how to configure the Security Administrator server software.

- **IBM Tivoli Security Administrator for RACF User’s Guide**
  SC18-9476-02
  Describes the concepts and procedures for using the Security Administrator client services.

Accessing Publications Online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli Software Library:
http://publib.boulder.ibm.com/tividd/td/tdprodlist.html

Product publications include release notes, installation guides, users guides, administrators guides, configuration guides, and developers references.

**Note:** To ensure proper printing of PDF publications, select the Fit to page check box in the Adobe Acrobat Print window (which is available when you click File -> Print).

Ordering publications

You can order many IBM Tivoli publications online at:


You can also order by telephone:
- In the United States: 800-879-2755
- In Canada: 800-426-4968
- In other countries, for a list of telephone numbers, see
  http://www.ibm.com/software/tivoli/order-lit/

Accessibility

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

Before contacting IBM Tivoli Software support with a problem, refer to the IBM Tivoli Software support Web site at:

If you need additional help, contact software support by using the methods described in the IBM Software Support Guide at the following Web site:
http://techsupport.services.ibm.com/guides/handbook.html

The guide provides the following information:
- Registration and eligibility requirements for receiving support
- Telephone numbers and e-mail addresses, depending on the country in which you are located
- A list of information you should gather before contacting customer support

Conventions used in this book

This reference uses several conventions for special terms and actions and for operating system-dependent commands and paths.

Typeface conventions

The following typeface conventions are used in this book:

**Bold** Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java classes, and objects are in bold.

*Italic* Variables, titles of publications, and special words or phrases that are emphasized are in italic.

**Monospace** Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in monospace.

Operating system differences

This book uses the UNIX convention for specifying environment variables and for directory notation. When using the Windows command line, replace $variable with%variable% for environment variables and replace each forward slash (/) with a backslash (\) in directory paths. If you are using the bash shell on a Windows system, you can use the UNIX conventions.
Chapter 1. Introduction

The IBM Tivoli® Security Administrator for RACF is a flexible interface to the powerful security management functions of RACF, providing a variety of views of the RACF database and making specific information easy to find and update. As Tivoli Security Administrator for RACF does not require the knowledge of RACF commands, new administrators can manage RACF using their existing skills. Meanwhile, experienced administrators can be much more productive, and help-desk personnel can quickly research and solve security-related problems. In addition, the standards-based API provides access to RACF data from applications running on other platforms.

The Security Administrator can help you:

- Query and view the RACF database. Fields for each type of RACF profile is visible, searchable, and sortable (except for very sensitive fields, such as passwords). This includes not just users and groups, but data sets, resources, access permissions, and system options. Numerous security administration views of the RACF database are provided as well as the ability to customize and create your own. The data is always current, and you can search on any combination of fields.

- Maintain the RACF database. Most RACF fields are modifiable via an easy-to-use Java™-based GUI or ISPF panels. All updates are done under the authority of the authenticated RACF administrator. Detailed, comprehensive pop-up help explains each RACF field. Field validation routines check the format and content of each field before sending the change to RACF.

- Manage multiple RACF databases. Consolidated searches across multiple RACF databases and copying users between databases are all part of its multiple database capabilities.

- Access and update RACF data from applications running on non-z/OS® platforms via standards-based application programming interfaces.

The Security Administrator provides a modern, flexible, and powerful interface to view and maintain all types of profiles in the RACF database. Whether the administrator uses traditional interfaces to RACF or the new interfaces provided by the Security Administrator, the underlying security features and controls of RACF are maintained.

Security Administrator architecture

The Security Administrator consists of the following components:

- Security Administrator server
- Security Administrator clients
Security Administrator server

The Security Administrator server maintains an LDAP image of the RACF database, and one Security Administrator server is required for each RACF database managed in your environment. The Security Administrator server consists of the following components:

- Mirror database
- racf2ldap
- ldap2racf
- Configuration database

Mirror database

The mirror database represents a real-time image of the RACF database as it resides on the host z/OS system. The RACF database and mirror database are automatically updated with the racf2ldap and ldap2racf synchronization processes.

racf2ldap

racf2ldap updates the mirror database to reflect the current status of the RACF database.

Whenever a change is made to the RACF database, racf2ldap intercepts the system message generated by the RACF command. The RACF command is then translated into an equivalent LDAP modify command that updates the mirror database accordingly.

ldap2racf

ldap2racf modifies the RACF database to reflect changes initiated in the Security Administrator.

Whenever users make a change to the RACF database, ldap2racf translates the LDAP modify command into an equivalent RACF command to update the RACF database.
configuration. When the change has been made to the RACF database, racf2ldap processes and reflects the change in the mirror database.

**Configuration database**

The configuration database acts as a central repository of configuration data for all components of the Security Administrator server.

**Security Administrator clients**

Security Administrator clients connect with any Security Administrator servers in your environment. Administrators determine client privileges for viewing and modifying the data on any RACF database.

**PC client**

The Security Administrator PC client provides a graphical user interface that accesses the Security Administrator server, and can be run from any PC machine. The PC client is best suited to new RACF administrators, departmental administrators, and help desk personnel.

**ISPF client**

The Security Administrator ISPF client provides a set of ISPF panels that access the Security Administrator server. The ISPF client is best suited to experienced RACF administrators, but can be configured to provide special support for help desk and audit personnel.

### Security Administrator client overview

You will primarily use the Security Administrator client to display profiles in the RACF database. These profiles can be selected, listed, and displayed according to a wide range of criteria.

This display and edit activity flow is reflected in the client interface. By default, you are directed to a view that lists all available RACF databases. From this view, you can display individual profiles.

To facilitate finding the correct set of entries you want to view, the Security Administrator provides you with a powerful search utility. As the client uses LDAP, you can construct flexible search filters that allow you to search the database based on a RACF field.

Once the appropriate profiles have been found, the Security Administrator provides standard editing options as well as a variety of tools that automate common RACF tasks.

### Security Administrator client interface concepts and definitions

This section explains the key concepts used in the Security Administrator client interface.

**Database**

A Security Administrator server is a definition of several databases. The server contains both a mirror image of a RACF database and a configuration database that stores information required by the client.
A client database definition consists of the TCP/IP and LDAP information required to connect to a Security Administrator server. Each client has one database definition stored locally in order to acquire configuration data from the server.

Entry

An entry is an LDAP entity containing either RACF information or Security Administrator configuration data. All entities consist of a unique name and any number of attribute-value pairs. The permitted types of attributes and value formats are determined by the LDAP schema that resides on the Security Administrator server.

Targets

Each entry on the Security Administrator server is associated with a Security Administrator target that defines the entry type.

Attribute

An attribute is the name of a field used by the Security Administrator server to store information for an entry. Each entry has one or more attributes associated with it, and information is carried in the attribute definition entry type as LDAP entries, attributes, and values. Attributes are maintained by the Security Administrator.

View

A view represents a particular query against the RACF database that consists of:

- Selection criteria, which are either defined in a default view, or specified using a search filter
- Display fields that determine the fields displayed in the result set

The result set of a view are displayed as a list of entries, and view definitions are stored as LDAP entries on the Security Administrator server.

Tool

A tool performs a particular operation against the RACF database that consists of:

- A program executed against the database
- A view that displays the result set following execution of the program

The results of a tool action are displayed as a list of entries.

Security Administrator client features

The Security Administrator client simplifies RACF administration tasks by including the following features:

Client productivity features

The Security Administrator includes the following productivity enhancement features:
Flexible searching
You have complete flexibility when searching and viewing the RACF database. Searches can be conducted based on RACF fields using equality or substring criteria.

Views
As delivered, the Security Administrator includes numerous default views that can be modified, saved, and later used based on individual administrator preferences.

Real-time results
Information returned to the client is real-time RACF data. No refresh jobs or extract reports are required.

Composite field support
The Security Administrator provides composite field support for RACF. Composite fields allow you to sub-divide any field in RACF to store additional information. Further, when a sub-field has been defined, each sub-field can be updated independently, without affecting any other sub-fields defined for the same profile attribute.

Streamlined editing
Administrators can easily add, change, or delete RACF fields. Any possible problems are immediately brought to the attention of the administrator.

Cloning, copying, pasting
Administrators can easily clone information concerning a user, group, or resource into a new profile in the RACF database. Copying and pasting data from one record to another is supported.

Customizable interface
The appearance and functionality of the PC and ISPF clients are customizable by the administrator, allowing the interface to reflect the specific needs of the enterprise.

Delegated administration features
The Security Administrator includes the following delegated administration features:

Group based access control
Group-based access control allows you to delegate administrative authority among a hierarchy of users based upon their membership in one of a number of pre-defined groups. Group-based access control is implemented by enabling an access control file on the Security Administrator server, then assigning users to the groups using the Security Administrator client.

RACF view scoping
You have complete flexibility in deciding which RACF profiles to view. Scoping decisions can be based upon fields in the RACF database. Scoping allows the delegation of RACF administration to the department level, as departmental administrators view only those users and groups explicitly assigned to their control.
**RACF administration scoping**

You have complete flexibility in deciding what changes an administrator can make to particular RACF entities. Scoping decisions can be based upon fields in the RACF database. Scoping allows the delegation of RACF administration to the department level, as departmental administrators can only view permitted resources and perform permitted actions.

**Help desk scoping**

A subset of view and administration scoping, help desk scoping facilitates the delegation of RACF administration to the help desk level. For example, help desk personnel can be authorized to perform actions such as password resetting, but prevented from performing any other RACF operation.

**Multiple database management features**

The Security Administrator includes the following multiple database features:

**Multiple list databases**

The Security Administrator presents RACF databases in a single display, allowing administrators to easily select the particular database they want to view or edit.

**Cross-database searching**

Administrators can select multiple RACF databases as targets for their search and view commands. For example, an administrator can request a search to display users with a particular name across all RACF databases, with the results appearing in a consolidated view.

**Cross-database editing**

Standard editing tools such as copying and pasting are supported across multiple databases, and you can add or delete a profile across several databases.
Chapter 2. Installation instructions

The Security Administrator consists of the Security Administrator server, the Security Administrator ISPF client, and the Security Administrator PC client. The ISPF client was installed along with the Security Administrator server as described in the IBM Tivoli Security Administrator for RACF Installation Guide. This chapter describes how to install the PC client on your desktop.

This chapter contains the following topics:
- Software contents
- Supported platforms
- Disk and memory requirements
- Software prerequisites
- Installing Security Administrator PC client

Software package contents

The Security Administrator client distribution package provides the components required to view, access, and modify RACF information stored on the Security Administrator server.

The Security Administrator client distribution contains the following software:
- Security Administrator PC client
- Java Runtime Environment (JRE)

Supported platforms

Security Administrator client software is supported on the following platforms:
- Windows 98, NT, 2000, XP, and Win Server 2003

Disk and memory requirements

The Security Administrator has the following disk and memory requirements:
- The PC client package requires 55 MB of disk space on your machine.

Software prerequisites

This section discusses the prerequisites for the Security Administrator PC client.

Security Administrator server

The Security Administrator server component must be installed and configured before attempting to use the Security Administrator client. Refer to the IBM Tivoli Security Administrator for RACF Installation Guide for further information.
Java Runtime Environment

The PC client requires that Java Runtime Environment v1.4 or higher be installed and configured on your machine. If this component is not already present on your system, the PC client installer will install the required software for you.

Connectivity

Security Administrator clients require that TCP/IP be installed and configured on all systems to be administrated.

In TCP/IP, Security Administrator clients and servers can communicate using any port ranging from 0 - 99999. The LDAP defaults used in TCP/IP communications are port 389 for unencrypted communications, and port 636 for encrypted SSL/TLS communications. The ports you select must be enabled in the TCP/IP services file.

If you expect host user access from outside of a firewall, you must modify the firewall to allow access for the Security Administrator ports.

Installing the Security Administrator PC client

This section describe how to install the PC client on your machine.

Installing the PC client via download

To install the PC client via download:

1. FTP the contents of the AOR/rao/windows from the HFS or z/FS file system to a convenient location on your machine.
2. Navigate to PC client installation package directory, then double-click the setupwin32.exe file.
3. Click Next.
4. Choose the installation directory name, then click Next. You can either accept the default location or specify another directory.
5. Verify your installation selections, then click Next.
6. Click Finish.

Installing the PC client from the network

To install the PC client from a network drive:

1. Determine the location of the PC client installation package from your network administrator.
2. Navigate to PC client installation package network directory, then double-click the setupwin32.exe file.
3. Click Next.
4. Choose the installation directory name, then click Next. You can either accept the default location or specify another directory.
5. Verify your installation selections, then click Next.
6. Click Finish.
Chapter 3. Security Administrator PC client

This chapter contains information about using the Security Administrator PC client.

Starting the client

To begin a Security Administrator session: Select Start→ Programs → IBM Tivoli Security Administrator for RACF → IBM Tivoli Security Administrator for RACF.

Setting logging and user interface display options

To adjust the fonts and colors displayed in the PC client and to specify the logging level and log file location for the PC client:

1. Using a plain-text editor such as Microsoft Notepad, create a text file called "rao.txt" in one of the following directories:

   - \Program Files\IBM\AOR\n
   - C:\Documents and Settings\userid

   Where userid is your userID.

   Note: Using other types of text editors, such as Wordpad for example, can introduce hidden characters that will corrupt the file.

2. In "rao.txt", specify any combination of the following statements:

   - LogFilePath = C:\temp\rao.log
   - LogLevel = 4
   - FontName = Arial
   - FontStyle = 0
   - FontSize = 16
   - TextColor = 8,16,102,160
   - BackgroundColor = 25,25,250
   - ShadeColor = 0,55,75
   - SelectColor = 150,200,100

   where:

   - LogFilePath: Determines the location of the log file. The default location is: C:\temp\rao.log
   - LogLevel: Determines the level of information that is captured in the log. The following are valid values for this attribute:
     - 1 - Fatal level errors are captured
     - 2 - Fatal and Error level errors are captured
     - 3 - Fatal, Error, and Warning level errors are captured
     - 4 - Fatal, Error, Warning, and Info. level errors are captured
     - 5 - Fatal, Error, Warning, Info., and debug level errors are captured
     - 6 - Fatal, Error, Warning, Info., debug, and trace level errors are captured
   - FontName: Determines the display font used for the PC client. You must specify the name of a valid font installed on the PC client machine.
   - FontStyle: Determines how the selected font is displayed. Valid values are 0 for plain, 1 for bold, and 2 for italic.
   - FontSize: Determines the size of the font that you specified using the FontName attribute.
- **TextColor**: Determines the color of the font that you specified using the FontName attribute using the R,G,B color system or the R,G,B,T system (where T=transparency). Valid values for each color range from 0 - 255. Valid values for Transparency range form 0-255, where, 0 is 0% transparency, 128 is 50% transparency, 255 is 100% transparency).
- **BackgroundColor**: Determines the color of modifiable fields as well as status messages using the RGB color system. Valid values for each color range from 0 - 255.
- **ShadeColor**: Determines the color of non-modifiable fields using the RGB color system. Valid values for each color range from 0 - 255.
- **SelectColor**: Determines the color of selected fields using the RGB color system. Valid values for each color range from 0 - 255.

3. When you are finished, save rao.txt.
4. In the /AOR directory, rename rao.txt to rao.properties.
5. Restart the PC client to view your changes.

**Note**: If the settings that you specified in the “rao.properties” do not display when you start the PC client, the file may have been corrupted. Delete this file, then create a new file using the above procedure.

---

**Connect screen**

![Connect screen](image)

**Screen use**

When you are started the PC client, you must connect to a Security Administrator configuration server to begin your session. The configuration server holds information about the RACF database(s). To connect to a configuration server, you only need to supply the host, port, and root LDAP dn as shown below. When you enter this information, the PC client retains the information for subsequent sessions.
Fields

Screen fields are used by supplying the required information in the appropriate fields and clicking the Connect button. To connect to the configuration server, you will need to enter the following fields:

**Host (required)**
The Host field may contain either the IP address or Host Name of your Security Administrator server.

**Port (required)**
The Port field contains the IP port number of your Security Administrator server. By default, this is 389, but the person that installed the server may have chosen a different port number.

**Base DN (required)**
The Base DN field must be set to `o=omniconfig`, as shown in the screen image above.

**SSL (optional)**
The SSL check box is used to enable SSL encryption for communications sent between the client and the server. This is usually not necessary for communications with the configuration server, since this server does not contain any sensitive information. If you do check this box, you should enable SSL communications on the Security Administration server as described in the *IBM Tivoli Security Administrator for RACF Install Guide (GC18-9475-00)*. Also, you should verify that the port specified is the one used by the Server for SSL communications.

**Anonymous Bind (optional)**
The Anonymous Bind check box should be checked as shown in the screen image above unless you are planning to perform maintenance on the Security Administrator configuration server itself.

**User DN (optional)**
If the Anonymous Bind box is unchecked, then you must enter the User DN field to identify yourself to the Security Administrator configuration server. The only acceptable value is `cn=configManager,o=omniconfig`.

**Password (optional)**
If the Anonymous Bind box is unchecked, then you must enter the Password field to validate your identity with the Security Administrator configuration server. The value of this password field is set in the configuration file on the server, which by default resides in `/usr/lpp/AOR/plugins/slapd.conf`.

Controls

The Connect screen contains the following controls:

**Connect**
The Connect button is used to initiate a connection with the Security Administrator configuration server using the information supplied in the fields.

**Cancel**
The Cancel button closes the current screen without performing any action or saving any changes that were made.
Connect prompt

When you are initiated a connection with a RACF database, you must supply authentication information in the Connect prompt.

Fields

Screen fields are used by supplying the required information in the appropriate fields and clicking the Connect button. The Connect screen includes the following fields:

**RACF User ID**
The RACF User ID field is used to specify your RACF user ID and validate your permission to connect to the selected RACF database.

**Password**
The Password field is used to specify your RACF password and validate your permission to connect to the selected RACF database.

**New Password**
The New Password field is used to specify a new password for your RACF user ID. This field is optional.

**Verify Password**
If you have specified a new password, the Verify Password field is used to confirm the new password you have selected for your RACF user ID. This field is optional.

Controls

The Connect prompt contains the following controls:

**Connect**
The Connect button is used to initiate a connection with the RACF database using the information supplied in the fields.

**Cancel**
The Cancel button closes the current screen without performing any action or saving any changes that were made.
View Filter prompt

Screen use

Views are used to query the RACF database and return RACF data for viewing or modification.

You can run a view query either from the View menu, or from the listing of views defined in the directory structure of the Security Administrator configuration database. When a particular view generates numerous results, the View Filter prompt appears so that only specific entries of interest are returned.

Fields

Fields are used by specifying the required information in the appropriate fields and clicking **Execute**. The View Filter prompt can include different sets of fields depending upon which view was executed.

Each field in the screen acts as a filtering mechanism to target the database search. You can leave any or all fields blank, which will return a greater number of results. Each field uses the following search request formats:

* *or blank*

  No filtering is performed for the field and all results are returned.

*searchtext* 

  Filtering is performed for the field and all results matching the prefix `searchtext` are returned.

*searchtext*

  Filtering is performed for the field and all results matching the substring `searchtext` are returned.

*searchtext*

  Filtering is performed for the field and all results matching the suffix `searchtext` are returned.

`searchtext`

  Filtering is performed for the field and all results exactly matching `searchtext` are returned.
Controls

The View Filter prompt screen contains the following controls:

**Execute**
The Execute button is used to initiate the view query using the information supplied in the fields.

**Cancel**
The Cancel button closes the current screen without performing any action or saving any changes that were made.

Common administrator tasks

When you are familiarized yourself with the layout and functionality of the PC client, you are ready to view and modify information stored in the RACF database.

Using the Database Directories pane

The Database Directories pane displays the organizational hierarchy of the configuration and RACF databases that are available to the client. This section explains how to use the Database Directories pane to find information in the directory structure of a database.

Expanding tree items

To expand items in the Database Directories pane:

1. Connect to a Security Administrator server by either double-clicking its name in the database list, or by right-clicking upon the server’s name and selecting the Connect scroll-down menu option.
2. In the Connect dialog, enter your RACF user ID and password for authentication on the server, then click Connect.
3. When you are been authenticated, you can expand items by selecting and double-clicking a specific branch. Any subsequent branches or entries appear below your initial selection.
4. Continue to expand branches until you arrive at the entries relevant to your search.

Connecting to another database

To connect to another database:

1. Connect to another Security Administrator server by either double-clicking its name in the database list, or by right-clicking upon the server’s name and selecting the Connect scroll-down menu option.
2. In the Connect dialog, enter your RACF user ID and password for authentication on the server, then click Connect.

Running a view

Views are used to query the database. A specific view query represents a number of definitions that effectively filter the database information so only the set of requested RACF results are returned to the client. The results of a view query are displayed as entries in a View Results screen. To execute a view:

1. Click the Views menu or expand the views branch of the Security Administrator configuration database.
2. Select the type of view you want to execute from the displayed list.
3. Double-click the view to run it.

**Answering prompts**

Certain views generate numerous results and provide prompts in order to filter the results returned to the client. To answer a prompt:

1. Specify the RACF parameter values to be returned to the client in the appropriate field. Search criteria use the following formats:
   - A "*" format or blank field returns all results.
   - A "searchtext*" format returns all results that match the prefix `searchtext`.
   - A "*searchtext*" format returns all results that match the substring `searchtext`.
   - A "searchtext" format returns all results that exactly match `searchtext`.
2. When you are supplied the appropriate search criteria, click Execute.

**Viewing the parents/children of a profile**

To view the parents or children of a profile:

1. Select the profile whose parents or children you want to view.
2. Click the Actions menu or right-click upon the profile’s name and select the Parents or Children menu option. The parents or children of the selected profile appear in a View Results or Modify Entry screen.

**Sorting entries**

To sort the entries:

1. Select how the results display by clicking the appropriate column name.
2. Continue to click the column name until the results are sorted in ascending or descending order, as appropriate.

**Searching in a profile**

To search for occurrences of a text string in a profile:

1. Click the Edit menu, then select the Find menu option.
2. In the Find dialog, enter the search text in the Find String field. If you would like to find all words beginning with your search text, select Prefix. If you would like to find all words that contain your search text, select Substring.
3. Click **OK**. The search operation finds the text string by examining all the field names and values displayed in the current profile.

**Adding a new RACF database**

To add a new RACF database, you must login to the configuration database and define the new database profile in two separate steps, as described below.

Log into the configuration database:

1. Start the Security Administrator for RACF client.
2. In the Connect screen, ensure that the Anonymous Bind checkbox is de-selected.
3. Specify the User DN field to identify yourself to the Security Administrator configuration server. The only acceptable value is `cn=configManager,o=omniconfig`.

4. Specify the Password field to validate your identity with the Security Administrator configuration server. The value of this password field is set in the configuration file on the server, which by default resides in `/usr/lpp/AOR/plugins/slapd.conf`.

5. When complete, click **Connect**.

To add a database:

1. Right-click the configuration database profile, then select the **New Entry** scroll-down menu option. The New Entry window opens.

2. Select the configuration database as the target database for the new profile from the list, then click **OK**. The Select Target window opens.

3. Select **Database** and click **OK**. The Naming Attributes window opens.

4. Type the database name in the Database Name field and click **OK**. The Modify Entry window opens.

5. Double-click the RACF fields that you want to include or change in this database profile. For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

6. When you are finished entering the RACF fields associated with your new database profile, select **File --> Save and Close**.

7. Restart the Security Administrator client to view and connect to your new RACF database profile.

**Adding a new user**

To add a new RACF user profile:

1. Either click the **Actions** menu or right-click **ou=people** in the Database Directory pane, then select **New Entry**. The New Entry window opens.

2. Select the target database for the new profile from the list, then click **OK**. The Select Target window opens.

3. Select **User** from the list as the target for the new profile, then click **OK**. The Naming Attributes window opens.

4. In the **uid** field, type the RACF user ID to be associated with your new user profile, then click **OK**. The Modify Entry window opens.

5. In the Modify Entry window, double-click the RACF fields that you want to include or change in this user profile. For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

6. When you are finished entering the RACF fields associated with your new user profile, select **File --> Save and Close**.

**Cloning a user**

To clone a user:

1. Select the user profile you want to clone from either the Database Directories pane or from a View Results screen.

2. Either click the **Actions** menu or right-click the user profile, then select the **Copy Entry** menu option. The New Entry window opens.
3. Select the target database for the new profile from the list. Check the **Copy all child entries** check box to copy the user profile’s children. Check the **Clone entry** check box to copy any other database entries associated with the profile, then click **OK**. The Naming attributes window opens.

4. Type the RACF user ID to be associated with your user profile, then click **OK**.

   The status of the cloning procedure is displayed in the Progress window, and is complete when the indicator reads 100%.

   **Note:** If the RACF database returns any informational messages as a result of this action, they will be displayed in the Progress window. If a message appears in the Progress window, close the window when you have finished reading the message.

5. The Views Results window displays all of the profiles that were included in the cloning of the original user profile. To view or make changes to one of the listed profiles, double-click the appropriate profile to open a Modify Entry window. The Modify Entry window opens.

6. In the Modify Entry window, double-click the RACF fields that you want to include or change in this profile. For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

### Connecting a user to a group

To connect a user profile to a group:

1. Double-click **ou=people** in the Database Directory pane, right-click the user profile that you want to connect to a group, then select the **New Entry** scroll-down menu option. The New Entry window opens.

2. Select the target database for the new profile from the scroll-down list, then click **OK**. The Select Target window opens.

3. Select **UserConnect** from the scroll-down list as the target for the new profile, then click **OK**. The Naming Attributes window opens.

4. Type the RACF group name to which you want to connect, then click **OK**. The Modify Entry window opens.

5. In the Modify Entry window, double-click the RACF fields that you want to include or change in this user connect profile. For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

6. When you are finished entering the RACF fields associated with your new user connection, select **File --> Save and Close**.

### Adding a new group

To add a new RACF group profile:

1. Either click the Actions menu or right-click **ou=groups** in the Database Directory pane, then select the **New Entry** scroll-down menu option. The New Entry window opens.

2. Select the target database for the new profile from the scroll-down list, then click **OK**. The Select Target window opens.

3. Select **Group** from the scroll-down list as the target for the new profile, then click **OK**. The Naming Attributes window opens.

4. Type the RACF group name to be associated with your new group profile, then click **OK**. The Modify Entry window opens.
5. In the Modify Entry window, double-click the RACF fields that you want to include or change in this group profile. For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.

6. When you are finished entering the RACF fields associated with your new group profile, select File --> Save and Close.

**Cloning a group**

To clone a group:

1. Select the group profile you want to clone from either the Database Directories pane or from a View Results screen.

2. Either click the Actions menu or right-click the group profile, then select the Copy Entry menu option. The New Entry window opens.

3. Select the target database for the new profile from the list. Check the Copy all child entries check box to copy the user profile’s children. Check the Clone entry check box to copy any other database entries associated with the profile, then click OK. The Naming attributes window opens.

4. Type the RACF group ID to be associated with your new group profile, then click OK.

   The status of the cloning procedure is displayed in the Progress window, and is complete when the indicator reads 100%.

   **Note:** If the RACF database returns any informational messages as a result of this action, they will be displayed in the Progress window. If a message appears in the Progress window, close the window when you have finished reading the message.

5. The Views Results window displays all of the profiles that were included in the cloning of the original group profile. To view or make changes to one of the listed profiles, double-click the appropriate profile to open the Modify Entry window.

6. In the Modify Entry window, double-click the RACF fields that you want to include or change in this profile. For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.

**Connecting a group to multiple users**

To connect a group profile to multiple users:

1. Double-click ou=groups in the Database Directory pane, right-click the group profile to which you want to connect multiple users, then select the Modify Entry scroll-down menu option.

2. In the Modify Entry window, right-click the Member field, then select the Copy Field scroll-down menu option. Repeat this procedure until you have the same number of Member fields as the number of users that you are adding to this group.

3. Click each Member field and specify a valid RACF user ID that you want to add to this group.

4. When you are finished entering the RACF user IDs that you want to connect to this group, select File --> Save and Close.

**Adding a new generic data set**

To add a new RACF generic data set profile:

2. Double-click racfDataset Type=Generic, then right-click one of the displayed data set profiles and select the New Entry scroll-down menu option. The New Entry window opens.

3. Select the target database for the new profile from the scroll-down list, then click OK. The Select Target window opens.

4. Select Dataset from the scroll-down list as the target for the new profile, then click OK. The Naming attributes window opens.

5. Type the RACF data set name for your new data set profile, then click OK. The Modify Entry window opens.

6. In the Modify Entry window, double-click the RACF fields that you want to include or change in this data set profile. For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.

7. When you are finished entering the RACF fields associated with your new data set profile, select File --> Save and Close.

Adding a new discrete data set

To add a new discrete data set, you must create the volume serial and add the discrete data set in two separate steps, as described below. If you have already created the volume serial upon which the discrete data set is to reside, you may skip to the “Add a discrete data set” section below.

Create a volume serial:

1. Double-click ou=datasets in the Database Directory pane, right-click any existing Volser profile, then select the New Entry scroll-down menu option. The New Entry window opens.

2. Select the target database for the new profile from the scroll-down list, then click OK. The Select Target window opens.

3. Select Volser from the scroll-down list as the target for the new profile, then click OK. The Naming Attributes window opens.

4. Type the volume serial upon which the discrete data set is to reside, then click OK. The Modify Entry window opens.

5. In the Modify Entry window, select File --> Save and Close.

Add a discrete data set:

1. Right-click the volume serial created above, then select the New Entry scroll-down menu option. The New Entry window opens.

2. Select the target database for the new profile from the scroll-down list, then click OK. The Select Target window opens.

3. Select Dataset from the scroll-down list as the target for the new profile, then click OK. The Naming Attributes window opens.

4. Type the RACF data set name and volume serial information for your new data set profile, then click OK. The Modify Entry window opens.

5. In the Modify Entry window, double-click the RACF fields that you want to include or change in this data set profile. For discrete data set profiles, you must specify a unit along with the volume serial. For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.

6. When you are finished entering the RACF fields associated with your new data set profile, select File --> Save and Close.
Permitting access to a data set

To permit access to a RACF data set profile:

1. Double-click ou=datasets in the Database Directory pane, then navigate to the data set to which you want to grant access. Right-click the appropriate data set profile, then select the New Entry scroll-down menu option. The New Entry window opens.
2. Select the target database for the new permission from the scroll-down list, then click OK. The Select Target Window opens.
3. Select a target of DatasetPermitID, then click OK. The Naming Attributes window opens.
4. Type the appropriate naming information for the user or group that is being permitted access to the data set, then click OK. The Modify Entry window opens.
5. In the Modify Entry window, double-click the RACF fields that you want to include or change in this data set permit profile. For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.
6. When you are finished entering the RACF fields associated with your data set permit profile, select File -- Save and Close.

Permitting conditional access to a data set

To permit conditional access to a data set, you must define the condition and the permission in two separate steps, as described below. If you have already defined another conditional permission based on the same condition, you may skip to the "Define a permission" section below.

Define a condition:

1. Double-click ou=datasets in the Database Directory pane, then navigate to the data set to which you want to grant access. Right-click the appropriate data set profile, then select the New Entry scroll-down menu option. The New Entry window opens.
2. Select the target database for the new permit from the scroll-down list, then click OK. The Select Target Window opens.
3. Select a target based on the type of conditional access you want to permit:
   - DatasetAppcport = access based on APPCPORT
   - DatasetConsole = access based on system console
   - DatasetJesinput = access based on JES input device
   - DatasetProgram = access based on Program
   - DatasetSysid = access based on system ID
   - DatasetTerminal = access based on terminal ID
   When you have selected the target, click OK. The Naming Attributes window opens.
4. Type the appropriate naming information for the conditional element, then click OK. The Modify Entry window opens.
5. In the Modify Entry window, double-click any fields that you want to change for this condition. For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.

Define a permission:
1. Right-click the condition created above, then select the **New Entry** scroll-down menu option. The New Entry window opens.

2. Select the target database for the new permission from the scroll-down list, then click **OK**. The Select Target Window opens.

3. Select a target based on the type of conditional access you want to permit:
   - **DatasetPermitAp** = permit based on LU 6.2 port
   - **DatasetPermitCo** = permit based on system console
   - **DatasetPermitJe** = permit based on JES input device
   - **DatasetPermitPr** = permit based on Program
   - **DatasetPermitSy** = permit based on system ID
   - **DatasetPermitTe** = permit based on terminal ID

   When you have selected a target, click **OK**. The Naming attribute window opens.

4. Type the appropriate naming information for the type of access being permitted, then click **OK**. The Modify Entry window opens.

5. In the Modify Entry window, double-click any fields you want to change for this permission. For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

6. Select **File** --> **Save and Close**.

**Defining a new resource**

To define a new RACF resource profile:

1. Either click the Actions menu or right-click `ou=resources` in the Database Directory pane, then select the **New Entry** scroll-down menu option. The New Entry window opens.

2. Select the target database for the new profile from the scroll-down list, then click **OK**. The Select Target Window opens.

3. Select **Resource** from the scroll-down list as the target for the new profile, then click **OK**. The Naming attribute window opens.

4. Type the RACF resource name and RACF resource class to be associated with your new resource profile, then click **OK**. The Modify Entry window opens.

5. In the Modify Entry window, double-click the RACF fields that you want to include or change in this resource profile. For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

6. When you are finished entering the RACF fields associated with your new resource profile, select **File** --> **Save and Close**.

**Permitting access to a resource**

To permit access to a RACF resource profile:

1. Double-click `ou=resources` in the Database Directory pane, then double-click the class of the resource.

2. Right-click the resource to which you want to grant access, then select the **New Entry** scroll-down menu option. The New Entry window opens.

3. Select the target database for the new permission from the scroll-down list, then click **OK**. The Select Target Window opens.

4. Select a target of ResourcePermitID, then click **OK**. The Naming Attributes window opens.
5. Type the appropriate naming information for the user or group being permitted access to the resource, then click OK. The Modify Entry window opens.

6. In the Modify Entry window, double-click the RACF fields that you want to include or change in this resource permit profile. For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.

7. When you are finished entering the RACF fields associated with your resource permit profile, select File --> Save and Close.

Permitting conditional access to a resource

To permit conditional access to a resource, you must define the condition and the permission in two separate steps, as described below. If you have already defined another conditional permission based on the same condition, you may skip to the "Define a permission" section below.

Define a condition:

1. Double-click ou=resources in the Database Directory pane, then double-click the class of the resource.

2. Right-click the resource to which you want to grant access, then select the New Entry scroll-down menu option. The New Entry window opens.

3. Select the target database for the new permit from the scroll-down list, then click OK. The Select Target Window opens.

4. Select a target based on the type of conditional access you want to permit:
   - ResourceAppcport = access based on APPCPORT
   - ResourceConsole = access based on system console
   - ResourceJesinput = access based on JES input device
   - ResourceProgram = access based on Program
   - ResourceSysid = access based on system ID
   - ResourceTerminal = access based on terminal ID

   When you have selected a target, click OK. The Naming Attributes window opens.

5. Type the appropriate naming information for the conditional element, then click OK. The Modify Entry window opens.

6. In the Modify Entry window, double-click any fields you want to change for this condition. For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.

7. Select File --> Save and Close.

Define a permission:

1. Right-click the condition created above, then select the New Entry scroll-down menu option. The New Entry window opens.

2. Select the target database for the new permission from the scroll-down list, then click OK. The Select Target Window opens.

3. Select a target from the list based on the type of conditional access that you want to permit:
   - ResourcePermitAp = permit based on LU 6.2 port
   - ResourcePermitCo = permit based on system console
   - ResourcePermitJe = permit based on JES input device
   - ResourcePermitPr = permit based on Program
• **ResourcePermitSy** = permit based on system ID
• **ResourcePermitTe** = permit based on terminal ID

When you have selected a target, click **OK**. The Naming Attributes window opens.

4. Type the appropriate naming information for the type of access being permitted, then click **OK**. The Modify Entry window opens.

5. In the Modify Entry window, double-click any fields you want to change for this permission. For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

6. Select **File --> Save and Close**.

### Creating a new view

To create your own customized view definitions, you must login to the configuration database and create the new view profile in two separate steps, as described below.

**Log into the configuration database:**

2. On the Connect window, specify the **User DN** field to identify yourself to the Security Administrator configuration server. The only acceptable value is `cn=configManager,o=omniconfig`.
3. Specify the Password field to validate your identity with the Security Administrator configuration server. The value of this password field is set in the configuration file on the server, which by default resides in `/usr/lpp/AOR/plugins/slapd.conf`.
4. Ensure that the **Anonymous Bind** checkbox is not checked.
5. Click **Connect**.

**Create a view definition:**

1. Select **View --> Views**. The View Results window opens.
2. In the View Results window, right-click a view name, then select the **New Entry** scroll-down menu option. The New Entry window opens.
3. Select the configuration database as the target database for the new view definition, then click **OK**. The Select Target window opens.
4. Select **View** from the scroll-down list as the target for the new view definition, then click **OK**. The Naming Attributes window opens.
5. Type the view name for your new view definition, then click **OK**. The Modify Entry window opens.
6. In the Modify Entry window, double-click the configuration fields that you want to include or change in this view definition profile. For this view definition to work effectively, you must enter information into the following fields:
   - **LDAP Base DN**: Specifies where in the LDAP tree the view definition begins searching for profiles.
   - **LDAP Display Attr**: Specifies which RACF fields are displayed in this view definition. For information concerning mapping LDAP attributes to RACF fields, refer to Appendix B, “LDAP search filters,” on page 89.
   - **LDAP Prompt Attr**: Specifies which LDAP attributes are displayed on the view definition prompt that is used to construct the LDAP search filter.
- **LDAP Search Filter**: Defines the search filter that is used in the execution of this view definition. For information concerning LDAP search filter syntax, refer to Appendix B, “LDAP search filters,” on page 89.

- **Public View**: Allows other users to see and execute your new view definition.

- **Target**: Specifies a valid target as defined under ou=targets,o=omniconfig in the configuration database.

- **View Scope**: Determines how far below the LDAP Base DN the view definition searches for profiles.

For specific information on any field, right-click the field name and select Field Help from the scroll-down menu.

7. When you are finished entering the fields associated with your new view definition profile, select File --> Save and Close.

8. Restart the Security Administrator client to use your new view definition.

### Defining RACF sub-fields

The fields that are used in RACF profiles can be subdivided to store additional information. You must first decide what type of information you want to include, then determine how many characters will be required by each sub-field. You cannot exceed the maximum number of characters defined for the RACF field.

To define RACF sub-fields, you must login to the configuration database, and create sub-field and display data definitions in three separate steps, as described below.

**Log into the configuration database:**


2. Specify the User DN field to identify yourself to the Security Administrator configuration server. The only acceptable value is `cn=configManager,o=omniconfig`.

3. Specify the Password field to validate your identity with the Security Administrator configuration server. The value of this password field is set in the configuration file on the server, which by default resides in `/usr/lpp/AOR/plugins/slapd.conf`.

4. On the Connect window, ensure that the Anonymous Bind checkbox is not checked.

5. Click Connect.

**Define a sub-field:**

1. In the Tree View, double-click `ou=targets`, then scroll down and double-click the appropriate target name.

2. Scroll down and select the name of the attribute that you want to subdivide, then right-click and select the New Child menu option. The Select Target Window opens.

3. Select `AttributeSubdef` from the scroll-down list as the target for the new sub-field definition, then click OK. The Naming Attributes window opens.

4. Type a sub-field name appropriate to the type of information that the sub-field will contain in the Sub-Field Name field, then click OK. The Modify Entry window opens.

5. In the Modify Entry window, double-click the configuration fields that you want to include or change in this sub-field definition. For this sub-field definition to work effectively, you must specify information in the following fields:

   - **Maximum Length**: Specifies the maximum length of the field.
• **Minimum Length**: Specifies the minimum length of the field.

• **Sub-Field Length**: Specifies the length of this sub-field in the **Installation Data** field.

• **Sub-Field Offset**: Specifies the offset, in number of spaces, from the left of the **Installation Data** field to indicate where this sub-field begins. Verify that the specified offset does not conflict with any other sub-fields defined for this profile type, or sub-field data will overlap or be truncated.

For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

6. When you are finished specifying information in the fields that are associated with your sub-field definition, select **File --> Save and Close**.

Define the display data for the sub-field:

1. In the Tree View, right-click the attribute sub-definition that you just created above, then select the **New Child** menu option. The Select Target window opens.

2. Select **DisplayData** as the target for the display data definition, then click **OK**. The Naming Attributes window opens.

3. Type **EN_us** as the value in the **DisplayFieldLocale**, then click **OK**. The Modify Entry window opens.

4. In the Modify Entry window, double-click the configuration fields that you want to include or change in this display data definition. Provide a display name, and also include help information that explains the purpose and usage of the sub-field for users.

   For specific information on any field, right-click the field name and select **Field Help** from the scroll-down menu.

5. When you are finished entering the display data that will appear when the sub-field is used, select **File --> Save and Close**.


**Using RACF sub-fields**

The fields used in RACF profiles can be subdivided to store additional information. To use a RACF field that has been sub-divided:

1. In the Tree View, double-click **ou=profile type**, where **profile type** is one of the following:
   - Dataset
   - Group
   - Resource
   - User

2. Scroll down and select the appropriate profile, then right-click and select the **Modify Entry** menu option. The Modify Entry window opens.

3. In the Modify Entry window, right-click the **sub-divided RACF** field, then select the **Expand Field** menu option. The Expand Field window opens.

4. In the Expand Field window, type data into each of the fields as appropriate. Any information that exceeds the sub-fields defined length will be truncated. You can delete information in any sub-field by leaving the field blank.

   For specific information on any sub-field, click the button adjacent to the sub-field name to display its help information.

5. Select **File --> Save and Close**.
Using tools

Security Administrator for RACF provides tools to make it easier to view specific, commonly-viewed data. Tools are accessible using the Tools menu.

To use one of the tools, select the desired tool from the Tools menu. The following tools are available:

All Permitted Users for Dataset
This tool shows all of the permitted users that are associated with the selected dataset. The tool is only active in the Tools menu when you select a data set in the main Security Administrator for RACF window.

All Permitted Users for Resource
This tool shows all of the permitted users that are associated with the resource that is highlighted when the tool is run. The tool is only active in the Tools menu when you select a resource in the main Security Administrator for RACF window.

All Datasets for User
This tool shows all of the datasets that are associated with the selected user. The tool is only active in the Tools menu when you select a user in the main Security Administrator for RACF window.

All Resources for User
This tool shows all of the resources that are associated with the selected user. The tool is only active in the Tools menu when you select a user in the main Security Administrator for RACF window.

All Orphan Users
This tool lists all of the orphan permits for resources or datasets on the selected RACF database. Orphan permits are resource and dataset permits for users and groups that no longer exist on the RACF database. This tool becomes active in the Tools menu when:
- any class or resource is selected in the Resources folder
- any volser, any data set, or DatasetType Generic, is selected in the Dataset folder

All Permitted Groups Without Users
This tool lists all groups that do not have users associated with them. This tool is always active.

Copying a profile

To copy a profile:
1. Select a profile from either the Database Directories pane or from a View Results screen.
2. Either click the Actions menu or right-click the profile, then select the Copy Entry menu option. The New Entry window opens.
3. Specify the target database for the new profile. Check the Copy Children check box to copy all of the children that are associated with this profile. Click OK. The Naming Attributes window opens.
4. Specify naming attributes for the profile as appropriate. Click OK. The Modify Entry window opens.
5. Double-click the names of fields you want to change in the profile and enter values as appropriate.
6. When you are finished entering field information for the new profile, select File -- > Save and Close.
Deleting a profile

To delete a profile:
1. Select a profile from either the Database Directories pane or from a View Results pane.
2. Either click the Actions menu or right-click the profile, then select Delete Entry.
3. Verify that you want to delete the selected profile in the confirmation pop-up.

Administering system options

Accessing system options

To access system options:
1. In the Tree View, double-click ou=options.
2. Select the racfOption=System profile and view the system options in the Profile View pane.

Enabling/disabling auditing for a class

To enable or disable auditing for a class:
1. Right-click the racfOption=System profile, then select the Modify Entry menu option.
2. To enable auditing for a class, right-click an AUDIT (*) entry in the Modify Entry window, then select the Add Field menu option. Type the name of the class in the Value field.
3. To disable auditing for a class, right-click the appropriate AUDIT (*) entry in the Modify Entry window, then select the Delete Field menu option.
4. When you are finished making your changes, select File --> Save and Close.

Activating/deactivating a class

To activate or deactivate a class:
1. Right-click the racfOption=System profile, then select the Modify Entry menu option. The Modify Entry window opens.
2. To activate a class, right-click a CLASSACT (*) entry in the Modify Entry window, then select the Add Field menu option. Type the name of the class in the value field.
3. To deactivate a class, right-click the appropriate CLASSACT (*) entry in the Modify Entry window, then select the Delete Field menu option.
4. When you are finished making your changes, select File --> Save and Close.

Activating/deactivating generic profile command classes

To activate or deactivate a generic profile command class:
1. Right-click the racfOption=System profile, then select the Modify Entry menu option.
2. Activate or disable the generic profile.
To activate a generic profile command class, right-click a GENCMD (*) entry in the Modify Entry window, then select the Add Field menu option. Type the name of the class in the value field.

To disable a generic profile command class, right-click the appropriate GENCMD (*) entry in the Modify Entry window, then select the Delete Field menu option.

3. When you are finished making your changes, select File --> Save and Close.

Copying data sets

You can copy data sets by dragging and dropping them:

- Within a data set folder
- From one Volser to another Volser
- From one Volser to the datasets folder (and vice-versa)
- From one Volser to the DatasetType Generic (and vice-versa)
- From the DatasetType Generic to the datasets folder (and vice-versa)

1. In the tree view, navigate to the data set that you want to copy.
2. Select the data set that you want to copy and drag it to the location to which you want to copy it and drop it there. The New Entry window opens.
3. Select the database where you want the data set to reside. The database where you dropped the data set is automatically selected in the field.
4. Check the Copy all child entries check box if you want any children of the data set to be copied along with the data set itself.
5. Click OK. The Naming Attributes window opens.
6. Specify the name of the data set profile for the data set that you are copying in the Dataset Name field.
7. Optional: Specify the type of the data set that you are copying in the Dataset Type field.
8. Click OK. The status of the copy operation is displayed in the Progress window, and is complete when the indicator reads 100%.

Note: If the RACF database returns any informational messages as a result of this action, they will be displayed in the Progress window. If a message appears in the Progress window, close the window when you have finished reading the message.

Copying resources

You can copy resources by dragging and dropping them:

- Within a Class
- From one Class to another Class

Individual resources can be copied. Entire resource classes cannot be copied.

1. In the tree view, navigate to the resource that you want to copy.
2. Select the resource that you want to copy and drag it to the location to which you want to copy it and drop it there. The New Entry window opens.
3. Select the database where you want the data set to reside. The database where you dropped the data set is automatically selected in the field.
4. Check the **Copy all child entries** check box if you want any children of the data set to be copied along with the data set itself.

5. Click **OK**. The Naming Attributes window opens.

6. Specify the profile name of the resource that you are copying in the **Resource Name** field.

7. Specify the RACF class of this profile that you are copying in the **Class** field.

8. Click **OK**. The status of the copy operation is displayed in the Progress window, and is complete when the indicator reads 100%.

   **Note:** If the RACF database returns any informational messages as a result of this action, they will be displayed in the Progress window. If a message appears in the Progress window, close the window when you have finished reading the message.
Chapter 4. Security Administrator ISPF client

This chapter contains the following topics:
- Starting the client
- View Results: Databases panel
- Connect to database prompt
- Prompt for viewname
- View Results panel
- View Entry panel
- Modify value prompt
- Common administrator tasks

Starting the client

To begin a Security Administrator session, you must start the ISPF client. Follow the series of steps below:
1. From the ISPF Primary Options Menu, select the Command menu option.
2. Submit the following command on the command line, then press Type:
   AOR

Security Administrator messages

Messages from the Security Administrator ISPF client are written to the userID.AORLOG file, where userID is the administrator’s RACF userID.
Databases panel

Screen use

When you are started the ISPF client, you must connect to a Security Administrator server to begin your session. The Databases panel allows you to select from a list of defined servers, connect or disconnect specific servers, define new servers in your environment, and remove any servers that are no longer required.

Action characters

An action is performed by specifying the appropriate action character in a profile’s selection field, and pressing Type . The Databases panel contains the following action characters:

Views List
The Views List action character prompts the client to display a list of all views that are available to query a connected database.

Connect/Disconnect a Database
The Connect/Disconnect a Database action character prompts the client to connect to, or disconnect from, the selected Security Administrator server. To connect to a server, you must supply credentials for authentication on the Connect to Database panel.

View
The View action character queries the RACF database and returns field information for the selected profile. The results are returned as read-only information in the View Entry panel. This panel must be toggled to Modify Mode if you want to update the field information.
New
The New action character creates a new profile for the current view. When a new profile is created, you must specify a new dn and accept or change the default database location. When you are entered the required information, you must specify field information as appropriate for the new profile in the Modify Entry panel.

Copy
The Copy action character copies the selected profile’s field information and creates a new profile with identical values. When the new profile is created, you must specify a new dn and accept or change the default database location. When you are entered the required information, you must update the field information as appropriate for the new profile in the Modify Entry panel.

Delete
The Delete action character deletes the selected profile from the current view and the RACF database. You must confirm the delete request before the action is taken.

Parent
The Parent action character queries the RACF database and displays any entries defined as a parent for the selected profile. The results are displayed in a View Results panel.

Children
The Children action character queries the RACF database and displays any entries defined as children of the selected profile. The results are displayed in a View Results panel.

Add Child
The Add Child action character creates a new child for the selected parent profile in the profile’s View Children display. When a new profile is created, you must specify a new dn and accept or change the default database location. When you are entered the required information, you must specify field information as appropriate for the new child profile in the Modify Entry panel.

**Line commands**

The Databases panel supports the following line commands:

**SORT**

The SORT line command sorts the results returned from a view query in the View Results panel. The SORT line command uses the following format:

SORT column number A or D

which sorts the results according to column number in either ascending A or descending D order.

**FIND**

The FIND line command searches the results returned from a view query for occurrences of the specified search text. The FIND line command uses the following format:

FIND xxxx

which locates any instance of the search text xxxx.
Menus

Menus are selected by placing your cursor under a particular menu and pressing Type. Menu items are selected by specifying an item number and pressing Type. The Databases panel includes the following menus:

File menu

The File menu is used to perform basic file management operations. The File menu includes the following items:

Print
Prints the contents of the current panel.

Exit
Ends the Security Administrator session.

View menu

The View menu is used to select and display various views. The View menu contains the following items:

Users
Executes the Users view. The Users view displays information for users defined in the current RACF database.

Groups
Executes the Groups view. The Groups view displays information for user, resource, and data set groups defined in the current RACF database.

Connects
Executes the Connects view. The Connects view displays information for connections defined in the current RACF database.

Datasets
Executes the Datasets view. The Datasets view displays information for data sets defined in the current RACF database.

Resources
Executes the Resources view. The Resources view displays information for resources defined in the current RACF database.

Permits/Datasets
Executes the Database Permits view. The Database Permits view displays information for assigned database permissions in the current RACF database.

Permits/Resources
Executes the Resources Permits view. The Resources Permits view displays information for assigned resources permissions in the current RACF database.

Options
Executes the Options view.

Databases
Executes the Databases view. The Databases view displays a list of the servers defined in your environment.

Views
Executes the Views view. The Views view displays a list of all views available to the client.

Actions menu

The Actions menu is used to perform functions in a panel. The Actions menu contains the following items:
Re-execute View
Re-executes the current view. As re-executing a view queries the database, you must respond to any applicable prompts.

Repeat Find
Searches the database using the search criteria specified during the last search operation.

Page Up
Scrolls up through the results display. Selecting a list item and using Page Up scrolls the results and places the item at the bottom of the display.

Page Down
Scrolls down through the results display. Selecting a list item and using Page Down scrolls the results and places the item at the top of the display.

Page Left
Scrolls the results display to the left.

Page Right
Scrolls the results display to the right.

PF keys

The Databases panel contains the following PF key assignments:

PF1
Saves any changes made on the current panel, then displays panel help.

PF2
Splits the current display according to the position of the cursor.

PF3
Saves any changes made on the current panel, then returns to the previous screen.

PF4
Re-executes the current view to refresh the list of defined servers as well as their connection status.

PF5
Re-executes the Find line command using the previous search criteria.

PF7
Scrolls up through the results display. Selecting a list item and using PF7 scrolls the results and places the item at the bottom of the display.

PF8
Scrolls down through the results display. Selecting a list item and using PF7 scrolls the results and places the item at the top of the display.

PF9
Performs a screen swap.

PF10
Scrolls the results display to the left.

PF11
Scrolls the results display to the right.

PF12
Returns to the previous screen without saving any changes on the current panel.

PA1
Aborts the current search and retains any partial results that were returned.
Connect to database prompt

Screen use

When you are initiated a connection with a Security Administrator server, you must supply authentication information in the Connect to Database panel.

Panel fields

Panel fields are used by supplying the required information in the appropriate fields and pressing Type . The Connect to Database panel includes the following fields:

User ID
The User ID field is used to specify your RACF user ID and validate your permission to connect to the selected Security Administrator server.

Password
The Password field is used to specify your RACF password and validate your permission to connect to the selected Security Administrator server.

New Password
The New Password field is used to specify a new password for your RACF user ID. This field is optional.

Confirm
The Confirm field is used to confirm your new password. This field is optional.

PF keys

The Connect to Database panel contains the following PF key assignments:
PF1
Saves any changes made on the current panel, then displays panel help.

PF3
Saves any changes made on the current panel, then returns to the previous screen.

PF12
Returns to the previous screen without saving any changes on the current panel.

Prompt for Viewname

Screen Use

When you are successfully authenticated upon the selected Security Administrator server, you can begin to view or modify RACF data stored on the current database.

To view database information, you will use views to request the type of information that you are seeking. Views are executed from either the View Results: Views panel, or from the View menu.

When you execute a view that can generate numerous results, you can filter the view query so that only entries of interest are returned. The Prompt for Viewname, where Viewname represents the name of the executed view, allows you to specify search criteria that focus the view query.

Panel fields

Panel fields are used by supplying the required information in all appropriate fields and pressing Type . The Prompt for Viewname can include different sets of fields depending upon which view was executed.
Each field in the panel acts as a filtering mechanism to target the database search. You can leave any or all fields blank, which will return a greater number of results. Each field uses the following search request formats:

* or blank
   No filtering is performed for the field and all results are returned.

searchtext*
   Filtering is performed for the field and all results matching the prefix "searchtext" are returned.

*searchtext*
   Filtering is performed for the field and all results matching the substring "searchtext" are returned.

*searchtext
   Filtering is performed for the field and all results matching the suffix "searchtext" are returned.

searchtext
   Filtering is performed for the field and all results exactly matching "searchtext" are returned.

**PF keys**

The Prompt for Viewname panel contains the following PF key assignments:

PF1
   Saves any changes made on the current panel, then displays panel help.

PF2
   Splits the current display according to the position of the cursor.

PF3
   Saves any changes made on the current panel, then returns to the previous screen.

PF5
   Re-executes the Find line command using the previous search criteria.

PF7
   Scrolls up through the results display. Selecting a list item and using PF7 scrolls the results and places the item at the bottom of the display.

PF8
   Scrolls down through the results display. Selecting a list item and using PF7 scrolls the results and places the item at the top of the display.

PF9
   Performs a screen swap.

PF10
   Scrolls the results display to the left.

PF11
   Scrolls the results display to the right.

PF12
   Returns to the previous screen without saving any changes on the current panel.
Views Results panel

Screen Use

When you are executed a view, entries that correspond to the parameters of the view query are returned in a View Results panel. In this panel, entries can be viewed, created, copied, or deleted.

Action characters

An action is performed by specifying the appropriate action character in a profile's selection field, and pressing Type . The View Results: Views panel contains the following action characters:

**Execute View**

The Execute a View action character queries the database based upon the criteria defined for the selected view. This action character appears in the View Results: Views panel only. The results of the view query are displayed in a View Results panel.

**View**

The View action character queries the RACF database and returns field information for the selected profile. The results are returned as read-only information in the View Entry panel. This panel must be toggled to Modify Mode if you want to update the field information.

**New**

The New action character creates a new profile for the current view. When a new profile is created, you must specify a new dn and accept or change the default database location. When you are entered the required information, you must
specify field information as appropriate for the new profile in the Modify Entry panel.

**Copy**
The Copy action character copies the selected profile’s field information and creates a new profile with identical values. When the new profile is created, you must specify a new dn and accept or change the default database location. When you are entered the required information, you must update the field information as appropriate for the new profile in the Modify Entry panel.

**Delete**
The Delete action character deletes the selected profile from the current view and the RACF database. You must confirm the delete request before the action is taken.

**Parent**
The Parent action character queries the RACF database and displays any entries defined as a parent for the selected profile. The results are displayed in a View Results panel.

**Children**
The Children action character queries the RACF database and displays any entries defined as children of the selected profile. The results are displayed in a View Results panel.

**Add Child**
The Add Child action character creates a new child for the selected parent profile in the profile’s View Children display. When a new profile is created, you must specify a new dn and accept or change the default database location. When you are entered the required information, you must specify field information as appropriate for the new child profile in the Modify Entry panel.

**Line commands**

The View Results panel supports the following line commands:

**SORT**
The SORT line command sorts the results returned from a view query in the View Results panel. The SORT line command uses the following format:

SORT column number A or D

which sorts the results according to column number in either ascending A or descending D order.

**FIND**
The FIND line command searches the results returned from a view query for occurrences of the specified search text. The FIND line command uses the following format:

FIND xxxx

which locates any instance of the search text xxxx.

**Menus**

Menus are selected by placing your cursor under a particular menu and pressing Type . Menu items are selected by specifying an item number and pressing Type . The View Results panel includes the following menus:
File menu

The File menu is used to perform basic file management operations. The File menu includes the following items:

Print
  Prints the contents of the current panel.

Exit
  Ends the Security Administrator session.

View menu

The View menu is used to select and display various views. The View menu contains the following items:

Users
  Executes the Users view. The Users view displays information for users defined in the current RACF database.

Groups
  Executes the Groups view. The Groups view displays information for user, resource, and data set groups defined in the current RACF database.

Connects
  Executes the Connects view. The Connects view displays information for connections defined in the current RACF database.

Datasets
  Executes the Datasets view. The Datasets view displays information for data sets defined in the current RACF database.

Resources
  Executes the Resources view. The Resources view displays information for resources defined in the current RACF database.

Permits/Datasets
  Executes the Database Permits view. The Database Permits view displays information for assigned database permissions in the current RACF database.

Permits/Resources
  Executes the Resources Permits view. The Resources Permits view displays information for assigned resources permissions in the current RACF database.

Options
  Executes the Options view.

Databases
  Executes the Databases view. The Databases view displays a list of the servers defined in your environment.

Views
  Executes the Views view. The Views view displays a list of all views available to the client.

Actions menu

The Actions menu is used to perform functions in a panel. The Actions menu contains the following items:

Re-execute View
  Re-executes the current view. As re-executing a view queries the database, you must respond to any applicable prompts.

Refresh Entry
  Refreshes the profile information by querying the database for the selected profile.
Repeat Find
Searches the database using the search criteria specified during the last search operation.

Page Up
Scrolls up through the results display. Selecting a list item and using Page Up scrolls the results and places the item at the bottom of the display.

Page Down
Scrolls down through the results display. Selecting a list item and using Page Down scrolls the results and places the item at the top of the display.

Page Left
Scrolls the results display to the left.

Page Right
Scrolls the results display to the right.

**PF keys**

The View Results panel contains the following PF key assignments:

PF1
Saves any changes made on the current panel, then displays panel help.

PF2
Splits the current display according to the position of the cursor.

PF3
Saves any changes made on the current panel, then returns to the previous screen.

PF4
Re-executes the current view to refresh the list of defined servers as well as their connection status.

PF5
Re-executes the Find line command using the previous search criteria.

PF7
Scrolls up through the results display. Selecting a list item and using PF7 scrolls the results and places the item at the bottom of the display.

PF8
Scrolls down through the results display. Selecting a list item and using PF7 scrolls the results and places the item at the top of the display.

PF9
Performs a screen swap.

PF10
Scrolls the results display to the left.

PF11
Scrolls the results display to the right.

PF12
Returns to the previous screen without saving any changes on the current panel.

PA1
Aborts the current search and retains any partial results that were returned.
Screen use

When you are selected a particular profile from a View Results panel, the information is displayed in a View Entry panel. The View Entry panel displays read-only information for profile fields that have defined values. You can only edit or create profile values from in a Modify Entry panel.

Action characters

An action is performed by specifying the appropriate action character in a profile’s selection field, and pressing Type . The View Entry panel contains the following action characters:

Expand
The Expand action character displays the full field value information for the selected field. In View Mode, the displayed field information is read-only.

Edit
The Edit action character queries the RACF database and returns field information for the selected profile. Update field information as appropriate in the Modify Entry panel.

Copy
The Copy action character creates a copy of the field name and field value on the next line. The Copy action character applies to multi-value fields only.

Delete
The Delete action character deletes the selected field name and field value from the profile’s definition. You must confirm the delete request before the action is taken.
New
The New action character creates a new field for this profile with a blank field value. The New action character applies to multi-value fields only.

Line commands

The View Entry panel supports the following line commands:

**SORT**

The SORT line command sorts the results returned from a view query in the View Results panel. The SORT line command uses the following format:

```
SORT column number A or D
```

which sorts the results according to `column number` in either ascending `A` or descending `D` order.

**FIND**

The FIND line command searches the results returned from a view query for occurrences of the specified search text. The FIND line command uses the following format:

```
FIND xxxx
```

which locates any instance of the search text `xxxx`.

Menus

Menus are selected by placing your cursor under a particular menu and pressing Type. Menu items are selected by specifying an item number and pressing Type. The View Entry panel includes the following menus:

**File menu**

The File menu is used to perform basic file management operations. The File menu includes the following items:

- **Print**
  
  Prints the contents of the current panel profile.

- **Exit**
  
  Ends the Security Administrator session.

**View menu**

The View menu is used to select and display various views. The View menu contains the following items:

- **Users**
  
  Executes the Users view. The Users view displays information for users defined in the current RACF database.

- **Groups**
  
  Executes the Groups view. The Groups view displays information for user, resource, and data set groups defined in the current RACF database.

- **Connects**
  
  Executes the Connects view. The Connects view displays information for connections defined in the current RACF database.
Datasets
Executes the Datasets view. The Datasets view displays information for data sets defined in the current RACF database.

Resources
Executes the Resources view. The Resources view displays information for resources defined in the current RACF database.

Permits/Datasets
Executes the Database Permits view. The Database Permits view displays information for assigned database permissions in the current RACF database.

Permits/Resources
Executes the Resources Permits view. The Resources Permits view displays information for assigned resources permissions in the current RACF database.

Options
Executes the Options view.

Databases
Executes the Databases view. The Databases view displays a list of the servers defined in your environment.

Views
Executes the Views view. The Views view displays a list of all views available to the client.

Actions menu
The Actions menu is used to perform functions in a panel. The Actions menu contains the following items:

Refresh Entry
Refreshes the field information displayed in the current profile.

Repeat Find
Searches the database using the search criteria specified during the last search operation.

Page Up
Scrolls up through the results display. Selecting a list item and using Page Up scrolls the results and places the item at the bottom of the display.

Page Down
Scrolls down through the results display. Selecting a list item and using Page Down scrolls the results and places the item at the top of the display.

Page Left
Scrolls the results display to the left.

Page Right
Scrolls the results display to the right.

PF keys
The View Entry panel contains the following PF key assignments:

PF1
Saves any changes made on the current panel, then displays panel help.

PF2
Splits the current display according to the position of the cursor.

PF3
Saves any changes made on the current panel, then returns to the previous screen.
PF4
Re-executes the current view to refresh the list of defined servers as well as their connection status.

PF5
Re-executes the Find line command using the previous search criteria.

PF7
Scrolls up through the results display. Selecting a list item and using PF7 scrolls the results and places the item at the bottom of the display.

PF8
Scrolls down through the results display. Selecting a list item and using PF7 scrolls the results and places the item at the top of the display.

PF9
Performs a screen swap.

PF10
Scrolls the results display to the left.

PF11
Scrolls the results display to the right.

PF12
Returns to the previous screen without saving any changes on the current panel.

Modify Value prompt

Using the Edit, New, or Copy action characters on a profile from the View Entry panel prompts the client to display the profile's field information in the Modify Value prompt. Whenever a change is made to a field value, the client validates the data and displays any validation errors.
Panel fields

Panel fields are used by supplying the required information in all appropriate fields and pressing Type.

Line commands

The Modify Entry panel supports the following line commands:

SORT

The SORT line command sorts the results returned from a view query in the View Results panel. The SORT line command uses the following format:

SORT column number A or D

which sorts the results according to column number in either ascending A or descending D order.

FIND

The FIND line command searches the results returned from a view query for occurrences of the specified search text. The FIND line command uses the following format:

FIND xxxx

which locates any instance of the search text xxxx.

PF keys

The Modify Entry panel contains the following PF key assignments:

PF1

Saves any changes made on the current panel, then displays panel help.

PF2

Splits the current display according to the position of the cursor.

PF3

Saves any changes made on the current panel, then returns to the previous screen.

PF9

Performs a screen swap.

PF12

Returns to the previous screen without saving any changes on the current panel.

Common administrator tasks

When you are familiarized yourself with the layout and functionality of the ISPF client, you are ready to view and modify information stored in the RACF database.

Executing a view

Views are used to query the database. A specific view query represents a number of definitions that effectively filter the database information so only the set of requested RACF results are returned to the client. The results of a view query are displayed as entries in a View Results screen. To execute a view:
1. In the View Results: Views panel, scroll through the view selection list until you arrive at the appropriate view query.

2. Select the view by placing an "S" next to the view name, then press Type to execute it.

Answering prompts

Certain views generate numerous results and provide prompts in order to filter the results returned to the client. To answer a prompt:

1. Type the RACF parameter values to be returned to the client in the appropriate field. Search criteria use the following formats:
   - A "*" format or blank field returns all results.
   - A "searchtext*" format returns all results that match the prefix searchtext.
   - A "*searchtext*" format returns all results that match the substring searchtext.
   - A "searchtext" format returns all results that exactly match searchtext.

2. Press Type or F3 to process the values you supplied.

Viewing entries

Once a view has been executed and all prompts have been answered, the results are displayed as entries in a View Results panel.

During the execution of a view query, if the search returns many results, the first group of partial results are displayed in the View Results panel while the search continues in the background.

To view the information for a particular database profile:

1. In the View Results panel, scroll through the list of entries until you arrive at the appropriate profile.
2. Select the profile by placing a "V" next to the profile name, then press Type to display its field information.

![ISPF client interface](image)

**Viewing the parents/children of a profile**

To view the parents or children of a profile:

1. In the View Results panel, scroll through the list of entries until you arrive at the profile whose parents or children you want to view.

2. Select the profile by placing a "+" (Parent) or "-" (Children) next to the profile name, then press Type. The parents or children of the selected profile appear in the View Results panel.
Sorting entries

To sort the entries:

1. Type the following command from the command line:
   
   `SORT column number  A or D`

   which sorts the results according to column number in either ascending A or descending D order.

Searching in a profile

To search in a profile:

1. Type the following command from the command line:
   
   `FIND xxxx`

   which locates any instance of the search text xxxx.

Adding a new RACF database

To add a new RACF database:

1. In the View Results: Views panel, execute the Databases view by placing an "S" next to the appropriate view name, then press Type.

2. In the View Results: Databases panel, select the source profile for your new database by placing an "N" next to the profile name, then press Type.

3. In the Create Entry panel, review the displayed source and destination information. For new database profiles, only the configuration database can be specified as the destination database.

4. Type the RACF database name to be associated with your new database profile, then press Type.
5. Once the View Database panel appears, place an "E" next to a RACF field that you want to include or change in this database profile, then press Type.

6. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

7. When you are finished entering the RACF fields associated with your new database profile, press F3 to return to the View Results: Databases panel.
8. Restart the Security Administrator client to view and connect to your new RACF database profile.

**Adding a new user**

To add a new RACF user profile:

1. In the View Results: Views panel, execute the Users view by placing an "S" next to the appropriate view name, then press Type.
2. Respond to the view prompt by pressing F3 or Type.
3. In the View Results: Users panel, select the source profile for your new user by placing an "N" next to the profile name, then press Type.
4. In the Create Entry panel, review the displayed source and destination information. Use the "Select destination database" action character if you want to specify a destination database other than the one listed.
5. Type the RACF user ID to be associated with your new user profile, then press Type.

6. Once the View User panel appears, place an "E" next to a RACF field that you want to include or change in this user profile, then press Type.
7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with your new user profile, press F3 to return to the View Results: Users panel.

**Connecting a user to a group**

To connect a user profile to a group:

1. In the View Results: Views panel, execute the Users view by placing an "S" next to the appropriate view name, then press Type.

2. Respond to the view prompt by pressing F3 or Type.

3. In the View Results: Users panel, select the user profile you want to connect to a group by placing an "A" (Add Child) next to the profile name, then press Type.

4. In the Select Entry Type panel, select UserConnect as the entry type, then press Type.
5. In the Add Child panel, review the displayed current and child entry information. Type the RACF group name to which you want to connect, then press F3 or Type.

6. Once the View User panel appears, place an "E" next to a RACF field that you want to include or change in this user profile, then press Type.
7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with your new user profile, press F3 to return to the View Results: Users panel.

**Adding a new group**

To add a new RACF group profile:

1. In the View Results: Views panel, execute the Groups view by placing an "S" next to the appropriate view name, then press Type.

2. Respond to the view prompt by pressing F3 or Type.

3. In the View Results: Groups panel, select the source profile for your new group by placing an "N" next to the profile name, then press Type.

4. In the Create Entry panel, review the displayed source and destination information. Use the "Select destination database" action character if you want to specify a destination database other than the one listed.

5. Type the RACF group name to be associated with your new group profile, then press Type.
6. Once the View Group panel appears, place an "E" next to a RACF field that you want to include or change in this group profile, then press Type.

7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with your new group profile, press F3 to return to the View Results: Groups panel.
Connecting a group to multiple users

To connect a group profile to multiple users:

1. In the View Results: Views panel, execute the Groups view by placing an “S” next to the appropriate view name, then press Type.
2. Respond to the view prompt by pressing F3 or Type.
3. Select the group profile to which you want to connect multiple users by placing a “V” next to the appropriate profile name, then press Type.
4. In the View Group panel, place an “E” next to the Member field, then press Type.
5. In the Modify Value panel, specify a valid RACF user ID that you want to add to the group, then press F3 or Type.
6. In the View Group panel, place a “C” next to the member field, then press Type.
7. In the Modify Value panel, specify another valid RACF user ID that you want to add to the group, then press F3 or Type.
8. When you are finished entering the RACF user IDs you want to connect to this group, press F3 to return to the View Results: Groups panel.

Adding a new generic data set

To add a new RACF generic data set profile:

1. In the View Results: Views panel, execute the Datasets view by placing an “S” next to the appropriate view name, then press Type.
2. Respond to the view prompt by pressing F3 or Type.
3. In the View Results: Datasets panel, display the parent of a profile by placing an “+” (Parent) next to any profile name, then press Type.
4. In the View Results: Parent of dataset panel, display the parent of the profile by placing an “+” (Parent) next to the target name, then press Type.
5. In the View Results: Parent of target name panel, display the children of the profile by placing an "-" (Children) next to Datasets, then press Type.

6. In the View Results: Children of Datasets panel, select Generic by placing an "A" (Add Child) next to the profile name, then press Type.

7. In the Select Entry type panel, select Dataset as the target, then press Type.

8. In the Add Child panel, review the displayed current and child information. Type the RACF data set name to be associated with your new data set profile, then press Type.

9. Once the View Dataset panel appears, place an "E" next to a RACF field that you want to include or change in this data set profile, then press Type.
10. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

11. When you are finished entering the RACF fields associated with your new data set profile, press F3 to return to the View Results: Datasets panel.

Adding a new discrete data set

To add a new discrete data set, you must create the volume serial and add the discrete data set in two separate steps, as described below. If you have already created the volume serial upon which the discrete data set is to reside, you may skip to the “Add a discrete data set” section below.

Create a volume serial:

1. In the View Results: Views panel, execute the DatasetVolumes view by placing an "S" next to the appropriate view name, then press Type.

2. Respond to the view prompt by pressing F3 or Type.

3. In the View Results: DatasetVolumes panel, select the source profile for your new volume serial by placing an "N" next to the profile name, then press Type.

4. In the Create Entry panel, review the displayed source and destination information. Use the “Select destination database” action character if you want to specify a destination database other than the one listed.

5. Type the volume serial upon which the discrete data set is to reside, then press Type.
6. Once the View Volser panel appears, press F3 to return to the View Results: DatasetVolumes panel.

To add a new RACF discrete data set profile:

1. In the View Results: Views panel, execute the DatasetVolumes view by placing an “S” next to the appropriate view name, then press Type.
2. Respond to the view prompt by pressing F3 or Type.
3. In the View Results:DatasetVolumes panel, add a child to the volume serial created above by placing an "A" (Add Child) next to the volume serial name, then press Type.

4. In the Select Entry Type panel, select the target by placing an "S" next to Dataset, then press Type.

5. In the Add Child panel, review the displayed current and child information. Type the RACF data set name to be associated with your new data set profile, then press Type.

6. Once the View Dataset panel appears, place an "E" next to a RACF field that you want to include or change in this data set profile, then press Type. For discrete data set profiles, you must specify a unit along with the volume serial.
7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with your new data set profile, press F3 to return to the View Results: DatasetVolumes panel.

Permitting access to a data set

To permit access to a RACF data set profile:

1. In the View Results: Views panel, execute the Datasets view by placing an "S" next to the appropriate view name, then press Type.
2. Respond to the view prompt by pressing F3 or Type.
3. In the View Results: Datasets panel, select the data set to which you want to grant access by placing an "A" (Add Child) next to the profile name, then press Type.
4. In the Select Entry Type panel, select DatasetPermitId by placing an "S" next to the target name, then press Type.
5. In the Add Child panel, review the displayed current and child entry information. Specify the appropriate naming information for the user or group being permitted access to the data set, then press F3 or Type.

6. Once the View DatasetPermit panel appears, place an "E" next to a RACF field that you want to include or change in this data set permission, then press Type.
7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with your new data set permission, press F3 to return to the View Results: Datasets panel.

**Permitting conditional access to a data set**

To permit conditional access to a data set, you must define the condition and the permission in two separate steps, as described below. If you have already defined another conditional permission based on the same condition, you may skip to the "Define a permission" section below.

**Define a condition:**

1. In the View Results: Views panel, execute the Datasets view by placing an "S" next to the appropriate view name, then press Type.
2. Respond to the view prompt by pressing F3 or Type.
3. In the View Results: Datasets panel, select the data set to which you want to grant access by placing an "A" (Add Child) next to the profile name, then press Type.
4. In the Select Entry Type panel, select a target based on the type of conditional access you want to permit by placing an "S" next to the target name, then press Type:
   - **DatasetAppcport** = access based on APPCPORT
   - **DatasetConsole** = access based on system console
   - **DatasetJesinput** = access based on JES input device
   - **DatasetProgram** = access based on Program
   - **DatasetSysid** = access based on system ID
   - **DatasetTerminal** = access based on terminal ID
5. In the Add Child panel, review the displayed current and child entry information. Specify the appropriate naming information for the conditional element, then press F3 or Type.

6. Once the View Dataset panel appears, place an "E" next to a RACF field that you want to include or change for this condition, then press Type.
7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with this condition, press F3 to return to the View Results: Datasets panel.

Define a permission:

1. In the View Results: Datasets panel, display the children of the data set to which you want to grant access by placing a "-" (Children) next to the data set name, then press Type.

2. In the View Results: Children panel, select the condition created above by placing an "A" (Add Child) next to the condition name, then press Type.

3. In the Select Entry Type panel, select a target based on the type of conditional access you want to permit by placing an "S" next to the target name, and pressing Type:
   - DatasetPermitAp = permit based on LU 6.2 port
   - DatasetPermitCo = permit based on system console
   - DatasetPermitJe = permit based on JES input device
   - DatasetPermitPr = permit based on Program
   - DatasetPermitSy = permit based on system ID
   - DatasetPermitTe = permit based on terminal ID
4. In the Add Child panel, review the displayed current and child entry information. Specify the appropriate naming information for the type of access being permitted, then press F3 or Type.

5. Once the View Database panel appears, place an "E" next to a RACF field that you want to include or change for this permission, then press Type.
6. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type .

7. When you are finished entering the RACF fields associated with this permission, press F3 to return to the View Results: Children panel.

**Defining a new resource**

To define a new RACF resource profile:

1. In the View Results: Views panel, execute the Resources view by placing an "S" next to the appropriate view name, then press Type .
2. Respond to the view prompt by pressing F3 or Type .
3. In the View Results: Resources panel, select the source profile for your new resource by placing an "N" next to the appropriate resource class name, then press Type .
4. In the Create Entry panel, review the displayed source and destination information. Use the "Select destination database" action character if you want to specify a destination database other than the one listed.
5. Type the RACF resource name to be associated with your new resource profile, then press Type .
6. Once the View Resource panel appears, place an "E" next to a RACF field that you want to include or change in this resource profile, then press Type.

7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with your new resource profile, press F3 to return to the View Results: Resources panel.
Permitting access to a resource

To permit access to a RACF resource profile:

1. In the View Results: Views panel, execute the Resources view by placing an "S" next to the appropriate view name, then press Type.

2. Respond to the view prompt by pressing F3 or Type.

3. In the View Results: Resources panel, select the resource to which you want to grant access by placing an "A" (Add Child) next to the profile name, then press Type.

4. In the Select Entry Type panel, select ResourcePermitId by placing an "S" next to the target name, then press Type.

5. In the Add Child panel, review the displayed current and child entry information. Specify the appropriate naming information for the user or group being permitted access to the resource, then press F3 or Type.
6. Once the View ResourcePermit panel appears, place an "E" next to a RACF field that you want to include or change in this resource permission, then press Type.

7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with your new resource permission, press F3 to return to the View Results: Resources panel.
Permitting conditional access to a resource

To permit conditional access to a resource, you must define the condition and the permission in two separate steps, as described below. If you have already defined another conditional permission based on the same condition, you may skip to the "Define a permission" section below.

Define a condition:

1. In the View Results: Views panel, execute the Resources view by placing an "S" next to the appropriate view name, then press Type.
2. Respond to the view prompt by pressing F3 or Type.
3. In the View Results: Resources panel, select the resource to which you want to grant access by placing an "A" (Add Child) next to the profile name, then press Type.
4. In the Select Entry Type panel, select a target based on the type of conditional access you want to permit by placing an "S" next to the target name, then press Type:
   - ResourceAppcport = access based on APPCPORT
   - ResourceConsole = access based on system console
   - ResourceJesinput = access based on JES input device
   - ResourceProgram = access based on Program
   - ResourceSysid = access based on system ID
   - ResourceTerminal = access based on terminal ID
5. In the Add Child panel, review the displayed current and child entry information. Specify the appropriate naming information for the conditional element, then press F3 or Type.
6. Once the View Resource panel appears, place an "E" next to a RACF field that you want to include or change for this condition, then press Type.

7. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

8. When you are finished entering the RACF fields associated with this condition, press F3 to return to the View Results: Resources panel.
Define a permission:

1. In the View Results: Resources panel, display the children of the resource to which you want to grant access by placing a "-" (Children) next to the resource name, then press Type.

2. In the View Results: Children panel, select the condition created above by placing an "A" (Add Child) next to the condition name, then press Type.

3. In the Select Entry Type panel, select a target based on the type of conditional access you want to permit by placing an "S" next to the target name, then press Type:
   - ResourcePermitAp = permit based on LU 6.2 port
   - ResourcePermitCo = permit based on system console
   - ResourcePermitJe = permit based on JES input device
   - ResourcePermitPr = permit based on Program
   - ResourcePermitSy = permit based on system ID
   - ResourcePermitTe = permit based on terminal ID

4. In the Add Child panel, review the displayed current and child entry information. Specify the appropriate naming information for the type of access being permitted, then press F3 or Type.
5. Once the View Resource panel appears, place an "E" next to a RACF field that you want to include or change for this permission, then press Type.

6. In the Modify Value panel, specify your value information for the RACF field, then press F3 or Type.

7. When you are finished entering the RACF fields associated with this permission, press F3 to return to the View Results: Children panel.
Creating a new view

To create your own customized view definition:

1. In the View Results: Views panel, select the source view for your new view definition by placing an "N" next to the view name, then press Type .

2. In the Create Entry panel, review the displayed source and destination information. For new view definitions, only the configuration database can be specified as the destination database.

3. Type the view name for your new view definition, then press Type .

4. Once the View View panel appears, place an "E" next to a field that you want to include or change in this view definition profile, then press Type . For this view definition to work effectively, you must enter information into the following fields:
Chapter 4. Security Administrator ISPF client

5. In the Modify Value panel, specify your value information for the view field, then press F3 or Type.

6. When you are finished entering the fields associated with your new view definition, press F3 to return to the View Results: Views panel.

7. Restart the Security Administrator client to use your new view definition.

Defining RACF sub-fields

The fields used in RACF profiles can be subdivided to store additional information. You must first decide what type of information you want to include, then determine how many characters will be required by each sub-field. You cannot exceed the maximum number of characters defined for the RACF field.
To define RACF sub-fields, you must create sub-field and display data definitions, as described below.

Define a sub-field and display data:
1. In the View Results: Views panel, display the parent of a view by placing an "+" (Parent) next to any view name, then press Type.
2. Display the parent of the view results by placing an "+" (Parent) next to Views, then press Type.
3. Display the parent of the view results by placing an "+" (Parent) next to RAO, then press Type.
4. Display the children of the view results by placing an "-" (Children) next to Default-config, then press Type.
5. Display the children of targets by placing an "-" (Children) next to Targets, then press Type.

6. Display the children of an objectclass by placing an "-" (Children) next to the appropriate objectclass name, then press Type.
7. Select the attribute you want to subdivide by placing an "A" (Add Child) next to the attribute name, then press Type.

8. In the Select Entry Type panel, select AttributeSubdef by placing an "S" next to the target name, then press Type.
9. In the Add Child panel, review the displayed current and child information. Specify the appropriate naming information for the sub-field, then press F3 or Type.

10. Once the View AttributeSubdef panel appears, place an "E" next to a field that you want to include or change in this sub-field definition, then press Type. For this view definition to work effectively, you must enter information into the following fields:
Maximum Length: Specifies the maximum length of the field.
Minimum Length: Specifies the minimum length of the field.
Sub-Field Length: Specifies the length of this sub-field in the Installation Data field.
Sub-Field Offset: Specifies the offset, in number of space, from the left of the Installation Data field to indicate where this sub-field begins. Verify that the specified offset does not conflict with any other sub-fields defined for this profile type, or sub-field data will overlap or be truncated.

11. In the Modify Value panel, specify your value information for the view field, then press F3 or Type.
12. When you are finished entering the fields associated with your new sub-field definition, press F3 to return to the View Results: Children of objectclass panel.
13. Display the children of the same attribute again by placing an "-" (Children) next to the attribute name, then press Type.
14. Select the sub-field definition you created by placing an "A" (Add Child) next to the sub-field name, then press Type.
15. In the Select Entry Type panel, select DisplayData by placing an "S" next to the target name, then press Type.
16. In the Add Child panel, review the displayed current and child information. Type "EN_us" for the Type Language, then press F3 or Type .

17. Once the View DisplayData panel appears, place an "E" next to a field that you want to include or change in this sub-field definition, then press Type . Provide a display name, and also include help information that explains the purpose and usage of the sub-field for users.
18. In the Modify Value panel, specify your value information for the field, then press F3 or Type.

19. When you are finished entering the fields associated with your new display data definition, press F3 to return to the View Results: Children of attribute panel.

20. Restart the Security Administrator client to use your sub-field definition.

**Using RACF sub-fields**

The fields used in RACF profiles can be subdivided to store additional information. To use a RACF that has been sub-divided:

1. In the View Results: view name, select a profile by placing a "V" (View) next to the profile name, then press Type.

2. In the View profile name panel, select the sub-divided RACF field by placing a "+" (Expand) next to the appropriate field name.

3. Once the Expand field prompt appears, place an "E" next to the appropriate sub-field name, then press Type.

4. In the Modify Value panel, specify your sub-field value information as appropriate, then press F3 or Type. Any information that exceeds the sub-fields defined length will be truncated. You can delete any sub-field information by leaving the field blank. For specific information on any sub-field, place an "h" next to the sub-field name to display its help information.

5. When you are finished entering data into the appropriate fields, press F3 or Type to save the information and return to the profile.

**Copying a profile**

To copy a profile:
1. Select the profile you want to copy by placing a "C" next to the profile name, then press Type.
2. In the Create Entry panel, review the displayed source and destination information. Use the "Select destination database" action character if you want to specify a destination database other than the one listed.
3. Type naming attributes for the profile as appropriate.
4. In the Modify Entry panel, select the names of fields you want to change in the profile and enter values as appropriate.
5. When you are finished entering field information for the profile, press F3.

**Deleting a profile**

To delete a profile:

1. Select the profile you want to delete by placing a "D" next to the profile name, then press Type.
2. Confirm that you want to delete the selected profile in the prompt.

**Administering system options**

**Accessing system options**

To access system options:

1. From the View Results: Databases panel, display the children of a database by placing a "-" (Children) next to the appropriate database name, then press Type.
2. In the View Results: Children of database panel, display the children of the Options profile by placing a "-" (Children) next to the appropriate profile name, then press Type.
3. In the View Results: Children of Options panel, view the System profile by placing a "V" (View) next to the appropriate profile name, then press Type.

**Enabling/disabling auditing for a class**

To enable or disable auditing for a class:

1. In the View Results: Children of Options panel, view the System profile by placing a "V" (View) next to the appropriate profile name, then press Type.
2. To enable auditing for a class, select an AUDIT (*) entry in the View Option panel by placing an "N" (New) next to the appropriate field name, then press Type. Type the name of the class in the Modify Value for AUDIT prompt, then press F3.
3. To disable auditing for a class, select the appropriate AUDIT (*) entry in the View Option panel by placing a "D" (Delete) next to the field name, then press Type. Respond to the Delete Confirmation prompt by pressing F3.
4. When you are finished making your changes, press F3 to return to the View Results: Children of Options panel.

**Activating/deactivating a class**

To activate or deactivate a class:

1. In the View Results: Children of Options panel, view the System profile by placing a "V" (View) next to the appropriate profile name, then press Type.
2. To activate a class, select a CLASSACT (*) entry in the View Option panel by placing an "N" (New) next to the appropriate field name, then press Type . Type the name of the class in the Modify Value for CLASSACT prompt, then press F3.

3. To deactivate a class, select the appropriate CLASSACT (*) entry in the View Option panel by placing a "D" (Delete) next to the field name, then press Type . Respond to the Delete Confirmation prompt by pressing F3.

4. When you are finished making your changes, press F3 to return to the View Results: Children of Options panel.

**Activating/deactivating generic profile command classes**

To activate or deactivate a generic profile command class:

1. In the View Results: Children of Options panel, view the System profile by placing a "V" (View) next to the appropriate profile name, then press Type .

2. To activate a generic profile command class, select a GENCMD (*) entry in the View Option panel by placing an "N" (New) next to the appropriate field name, then press Type . Type the name of the class in the Modify Value for GENCMD prompt, then press F3.

3. To disable a generic profile command class, select the appropriate GENCMD (*) entry in the View Option panel by placing a "D" (Delete) next to the field name, then press Type . Respond to the Delete Confirmation prompt by pressing F3.

4. When you are finished making your changes, press F3 to return to the View Results: Children of Options panel.
Appendix A. Troubleshooting

This appendix contains troubleshooting tips for IBM Tivoli Security Administrator for RACF.

Information RACF messages in Progress window

The RACF database returns sometimes returns informational messages as a result of actions taken in the IBM Tivoli Security Administrator for RACF’s PC client. When an informational message is returned it is displayed in the Progress window.
Appendix B. LDAP search filters

This appendix provides information to help you modify or create your own LDAP search filters for use in Security Administrator view definitions.

Search filter syntax

Security Administrator view definitions use LDAP search filters to query the RACF database and return results that match the search criteria. The sections below explain the syntax required to create your own LDAP search filters in new view definitions.

General filter syntax

The basic syntax of a search filter takes the form:

\(<\text{attribute}>\langle\text{operator}\rangle\langle\text{value}\rangle>\)

where:

- \(\text{attribute}\) represents an LDAP attribute name that corresponds to a field in the RACF database. For a mapping of the RACF fields/LDAP attributes used by the Security Administrator, refer to “RACF field/LDAP attribute mappings” on page 91.
- \(\text{operator}\) represents the filtering comparison between \(\text{attribute}\) and \(\text{value}\). For a list of the operators used by search filters, refer to “Operators” on page 90.
- \(\text{value}\) represents the limiting value of the search criteria.

Multiple search filters

Several search filters can be combined to perform multiple search operations. The search filters can be combined using Boolean operators expressed in prefix notation as follows:

\((\langle\text{operator}\rangle\langle\text{search filter}\rangle)(\langle\text{search filter}\rangle)...))\)

where \(\langle\text{operator}\rangle\) represents any of the Boolean operators. For a list of the Boolean operators used by search filters, refer to “Operators” on page 90.

Examples

Now that the general syntax format of search filters has been introduced, this section provides several examples of LDAP search filters used in Security Administrator view definitions. Use the examples provided below as a model for creating your own search filters:

Example 1

Consider the following LDAP search filter used in the UsersByOwner view definition:

\((\&\langle\text{objectclass}=\text{racfUser}\rangle)(\text{racfOwner}=\$\text{racfOwner})\)
In this example, the boolean operator "&" indicates that a profile must satisfy all statements in the search filter in order to be included in the search results. The first statement, "objectclass=racfUser", limits the search to racfUser fields, while the second statement, "racfOwner=$racfOwner" includes any profile that has a RACF Owner. As such, this search filter returns any RACF user profile that has an owner.

**Example 2**

Consider the following LDAP search filter used in the DatasetErase view definition:

```plaintext
(&(objectclass=racfDataset)(racfErase=TRUE))
```

In this example, the boolean operator "&" indicates that a profile must satisfy all statements in the search filter in order to be included in the search results. The first statement, "objectclass=racfDataset", limits the search to racfDataset fields, while the second statement, "racfErase=TRUE" includes any profile that has the ERASE RACF attribute enabled. As such, this search filter returns any RACF data set profile that can erase its data set extents when it is deleted.

**Example 3**

Consider the following LDAP search filter used in the Connects view definition:

```plaintext
(&(objectclass=racfUserConnect)(racfGroup=$racfGroup)(uid=$uid))
```

In this example, the boolean operator "&" indicates that a profile must satisfy all statements in the search filter in order to be included in the search results. The first statement, "objectclass=racfUserConnect", limits the search to racfUserConnect fields, the second statement, "racfGroup=$racfGroup", includes any profile with a group name, and the third statement, "uid=$uid", includes any profile with a user ID. As such, this search filter returns user IDs associated with each group name.

**Example 4**

Consider the following LDAP search filter used in the UsersNonExpiring view definition:

```plaintext
(!(racfPasswordInterval=*))
```

In this example, the boolean operator "!" indicates that a profile must not satisfy the statement in the search filter in order to be included in the search results. The statement, "racfPasswordInterval=*", includes any profile that has a defined password interval, but the boolean operator allows only those profiles with no such interval in the search results. As such, this search filter returns profiles with non-expiring passwords.

---

**Operators**

The tables below display the operators used in the Security Administrator’s LDAP search filters.

**General operators**

General operators used in search filters include the following:
Appendix B. LDAP search filters

Boolean operators

Boolean operators used in search filters include the following:

**Table 1. General operator descriptions**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Search type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>=</td>
<td>Equality</td>
<td>Returns results that contain attributes set to the specified value.</td>
</tr>
<tr>
<td>=&lt;string&gt;*&lt;string&gt;</td>
<td>Substring</td>
<td>Returns results that contain attributes that also contain the specified substring.</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Greater than or equal to</td>
<td>Returns results that contain attributes that are greater than or equal to the specified value.</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Less than or equal to</td>
<td>Returns results that contain attributes that are less than or equal to the specified value.</td>
</tr>
<tr>
<td>*=</td>
<td>Presence</td>
<td>Returns results that contain the specified attribute.</td>
</tr>
<tr>
<td>~=</td>
<td>Approximate</td>
<td>Returns results that contain attributes that are approximately equal to the specified value.</td>
</tr>
</tbody>
</table>

**Table 2. Boolean operator descriptions**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;</td>
<td>AND</td>
<td>All specified search filters must be true for the statement to be true.</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td>At least one specified search filter must be true for the statement to be true.</td>
</tr>
<tr>
<td></td>
<td>NOT</td>
<td>The specified statement must not be true for the statement to be true. Note that only one search filter is affected by the NOT operator.</td>
</tr>
</tbody>
</table>

**RACF field/LDAP attribute mappings**

The search filters in the Security Administrator use LDAP attributes that map to specific fields in the RACF database. The table below lists all RACF fields and their corresponding LDAP attributes. Use the appropriate LDAP attribute name in your view definition’s search filter:

**Table 3. RACF field/LDAP attribute mappings**

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfClass</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfClass</td>
<td>racfRefreshGeneric</td>
<td>Refresh GENERIC</td>
</tr>
<tr>
<td>racfClass</td>
<td>racfRefreshGlobal</td>
<td>Refresh GLOBAL</td>
</tr>
<tr>
<td>racfClass</td>
<td>racfRefreshRaclist</td>
<td>Refresh RACLIST</td>
</tr>
<tr>
<td>LDAP object class</td>
<td>LDAP attribute name</td>
<td>RACF field name</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfAudit</td>
<td>Audit</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfCategory</td>
<td>Category</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfCreatedate</td>
<td>Create Date</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfCreateGroup</td>
<td>Create Group</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfData</td>
<td>Installation Data</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfDatasetType</td>
<td>Dataset Type</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfErase</td>
<td>Erase</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfFileseq</td>
<td>File Sequence</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfGlobalaudit</td>
<td>Global Audit</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfLevel</td>
<td>Log Level</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfModifierGroup</td>
<td>Last Modifier Group</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfModifierUser</td>
<td>Last Modifier User</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfModifyDate</td>
<td>Last Modified Date</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfNotify</td>
<td>Notify</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfOwner</td>
<td>Owner</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfRetpd</td>
<td>Retention Period</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfSeclabel</td>
<td>Security Label</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfSeclevel</td>
<td>Security Level</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfUacc</td>
<td>Universal Access</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfUnit</td>
<td>Unit</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfVolsers</td>
<td>Volume Serials</td>
</tr>
<tr>
<td>racfDataset</td>
<td>racfWarning</td>
<td>Warning</td>
</tr>
<tr>
<td>racfDatasetAppcport</td>
<td>racfDatasetAppcport</td>
<td>APPC Port</td>
</tr>
<tr>
<td>racfDatasetAppcport</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetAppcport</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetConsole</td>
<td>racfConsole</td>
<td>Console</td>
</tr>
<tr>
<td>racfDatasetConsole</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetConsole</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetJesinput</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetJesinput</td>
<td>racfJesinput</td>
<td>JES Input Device</td>
</tr>
<tr>
<td>racfDatasetJesinput</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetPermitAp</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfDatasetPermitAp</td>
<td>racfAppcport</td>
<td>APPC Port</td>
</tr>
<tr>
<td>racfDatasetPermitAp</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>LDAP object class</td>
<td>LDAP attribute name</td>
<td>RACF field name</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>racfDatasetPermitAp</td>
<td>racfPermitld</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfDatasetPermitAp</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetPermitCo</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfDatasetPermitCo</td>
<td>racfConsole</td>
<td>Console</td>
</tr>
<tr>
<td>racfDatasetPermitCo</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetPermitCo</td>
<td>racfPermitld</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfDatasetPermitCo</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetPermitId</td>
<td>racfAccess</td>
<td>racfAccess</td>
</tr>
<tr>
<td>racfDatasetPermitId</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetPermitId</td>
<td>racfPermitld</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfDatasetPermitId</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetPermitJe</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfDatasetPermitJe</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetPermitJe</td>
<td>racfJesinput</td>
<td>JES Input Device</td>
</tr>
<tr>
<td>racfDatasetPermitJe</td>
<td>racfPermitld</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfDatasetPermitJe</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetPermitPr</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfDatasetPermitPr</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetPermitPr</td>
<td>racfPermitld</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfDatasetPermitPr</td>
<td>racfProgram</td>
<td>Program</td>
</tr>
<tr>
<td>racfDatasetPermitPr</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetPermitSy</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfDatasetPermitSy</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetPermitSy</td>
<td>racfPermitld</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfDatasetPermitSy</td>
<td>racfSysid</td>
<td>System ID</td>
</tr>
<tr>
<td>racfDatasetPermitSy</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetPermitTe</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfDatasetPermitTe</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetPermitTe</td>
<td>racfPermitld</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfDatasetPermitTe</td>
<td>racfTerminal</td>
<td>Terminal</td>
</tr>
<tr>
<td>racfDatasetPermitTe</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetProgram</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetProgram</td>
<td>racfProgram</td>
<td>Program</td>
</tr>
<tr>
<td>racfDatasetProgram</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetSegDfp</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetSegDfp</td>
<td>racfDfpOwner</td>
<td>DFP Resource Owner</td>
</tr>
<tr>
<td>racfDatasetSegDfp</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
</tbody>
</table>
Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfDatasetSegDfp</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetSegTme</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetSegTme</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfDatasetSegTme</td>
<td>racfTimeRoles</td>
<td>Role Access Spec</td>
</tr>
<tr>
<td>racfDatasetSegTme</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetSysid</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetSysid</td>
<td>racfSysid</td>
<td>System ID</td>
</tr>
<tr>
<td>racfDatasetSysid</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfDatasetTerminal</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfDatasetTerminal</td>
<td>racfTerminal</td>
<td>Terminal</td>
</tr>
<tr>
<td>racfDatasetTerminal</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfGroup</td>
<td>cn</td>
<td>Group Name</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfCreatedate</td>
<td>Create Date</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfData</td>
<td>Installation Data</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfMember</td>
<td>Member</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfModel</td>
<td>Model Dataset Profile</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfModifierGroup</td>
<td>Last Modifier Group</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfModifierUser</td>
<td>Last Modifier User</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfModifyDate</td>
<td>Last Modified Date</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfOwner</td>
<td>Owner</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfSubgroup</td>
<td>Subordinate Group</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfSupgroup</td>
<td>Superior Group</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfTermuacc</td>
<td>Terminal Unv. Access</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfUacc</td>
<td>Universal Access</td>
</tr>
<tr>
<td>racfGroup</td>
<td>racfUniversal</td>
<td>Universal Group</td>
</tr>
<tr>
<td>racfGroupSegDfp</td>
<td>cn</td>
<td>Group Name</td>
</tr>
<tr>
<td>racfGroupSegDfp</td>
<td>racfDfpDataappl</td>
<td>DFP Data Appl-ID</td>
</tr>
<tr>
<td>racfGroupSegDfp</td>
<td>racfDfpDataclas</td>
<td>DFP Dflt. Data Class</td>
</tr>
<tr>
<td>racfGroupSegDfp</td>
<td>racfDfpMgmtclas</td>
<td>DFP Management Class</td>
</tr>
<tr>
<td>racfGroupSegDfp</td>
<td>racfDfpStorclas</td>
<td>DFP Storage Class</td>
</tr>
<tr>
<td>racfGroupSegDfp</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfGroupSegOmv</td>
<td>cn</td>
<td>Group Name</td>
</tr>
<tr>
<td>racfGroupSegOmv</td>
<td>racfOomvsGid</td>
<td>Unix Group-ID (GID)</td>
</tr>
<tr>
<td>racfGroupSegOvm</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfGroupSegOvm</td>
<td>cn</td>
<td>Group Name</td>
</tr>
<tr>
<td>racfGroupSegOvm</td>
<td>racfOvmGid</td>
<td>OVM Group-ID (GID)</td>
</tr>
<tr>
<td>racfGroupSegOvm</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
</tbody>
</table>
### Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfGroupSegTme</td>
<td>cn</td>
<td>Group Name</td>
</tr>
<tr>
<td>racfGroupSegTme</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfGroupSegTme</td>
<td>racfTmeRoles</td>
<td>Roles</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfAddCreator</td>
<td>ADDCREATOR</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfAdsp</td>
<td>ADSP</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfApplaudit</td>
<td>APPLAUDIT</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfAuditSeclabel</td>
<td>SECLABELAUDIT</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfAuditSeclevel</td>
<td>SECLEVELAUDIT</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfAuditSpecial</td>
<td>SAUDIT</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfCatDsns</td>
<td>CATDSNS</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfClassActive</td>
<td>CLASSACT</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfClassAudit</td>
<td>AUDIT</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfClassGencmd</td>
<td>GENCMD</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfClassGeneric</td>
<td>GENERIC</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfClassGenlist</td>
<td>GENLIST</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfClassGlobal</td>
<td>GLOBAL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfClassRaclist</td>
<td>RACLIST</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfClassStatistics</td>
<td>STATISTICS</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfCmdViol</td>
<td>CMDVIOL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfCompatMode</td>
<td>COMPATMODE</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfControlSeclabel</td>
<td>SECLABELCONTROL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfDataset</td>
<td>RACF Dataset</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfEgn</td>
<td>EGN</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfErase</td>
<td>ERASE ALL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfEraseLevel</td>
<td>ERASE SECLEVEL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfGenericOwner</td>
<td>GENERICOWNER</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfGrplist</td>
<td>GRPLIST</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfInactiveInterval</td>
<td>INACTIVE</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfInitStats</td>
<td>INITSTATS</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfKerbLevel</td>
<td>KERBLVL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfMlactive</td>
<td>MLACTIVE</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfMquiet</td>
<td>MLQUIET</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfMls</td>
<td>MLS</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfMlstable</td>
<td>MLSTABLE</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfModel</td>
<td>MODEL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfModifierGroup</td>
<td>Last Modifier Group</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfModifierUser</td>
<td>Last Modifier User</td>
</tr>
</tbody>
</table>
### Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfOption</td>
<td>racfModifyDate</td>
<td>Last Modified Date</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfOperAudit</td>
<td>OPERAUDIT</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfOption</td>
<td>Option Type</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfPrefix</td>
<td>PREFIX</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfProtectAll</td>
<td>PROTECTALL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfRealDsn</td>
<td>REALDSN</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfRefreshWhenProg</td>
<td>REFRESH WHEN PROGRAM</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfRetpd</td>
<td>RETPD</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfSecLabelControl</td>
<td>SECLABELCONTROL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfSessInterval</td>
<td>SESSIONINTERVAL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfSingleDsn</td>
<td>SINGLEDSN</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfTapeDsn</td>
<td>TAPEDSN</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfTapevolProt</td>
<td>Tape Volser Protection</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfTerminalUacc</td>
<td>TERMINAL</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfUnit</td>
<td>RACF Database Unit</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfVolser</td>
<td>RACF Database Volume</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfWhenProgram</td>
<td>WHEN PROGRAM</td>
</tr>
<tr>
<td>racfOption</td>
<td>racfXbmAllRacf</td>
<td>JES XBMALLRACF</td>
</tr>
<tr>
<td>racfOptionSegJes</td>
<td>racfJesBatchAllRacf</td>
<td>JES BATCHALLRACF</td>
</tr>
<tr>
<td>racfOptionSegJes</td>
<td>racfJesEarlyVerify</td>
<td>JES EARLYVERIFY</td>
</tr>
<tr>
<td>racfOptionSegJes</td>
<td>racfJesNjeUserid</td>
<td>JES NJEUSERID</td>
</tr>
<tr>
<td>racfOptionSegJes</td>
<td>racfJesUndefinedUser</td>
<td>JES UNDEFINED</td>
</tr>
<tr>
<td>racfOptionSegJes</td>
<td>racfJesXbmAllRacf</td>
<td>JES XBMALLRACF</td>
</tr>
<tr>
<td>racfOptionSegJes</td>
<td>racfOption</td>
<td>Option Type</td>
</tr>
<tr>
<td>racfOptionSegJes</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfOptionSegLang</td>
<td>racfLanguagePrimary</td>
<td>LANGUAGE PRIMARY</td>
</tr>
<tr>
<td>racfOptionSegLang</td>
<td>racfLanguageSecondar</td>
<td>LANGUAGE SECONDARY</td>
</tr>
<tr>
<td>racfOptionSegLang</td>
<td>racfOption</td>
<td>Option Type</td>
</tr>
<tr>
<td>racfOptionSegLang</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfOptionSegLog</td>
<td>racfClassLogAlways</td>
<td>LOGOPTIONS ALWAYS</td>
</tr>
<tr>
<td>racfOptionSegLog</td>
<td>racfClassLogDefault</td>
<td>LOGOPTIONS DEFAULT</td>
</tr>
<tr>
<td>racfOptionSegLog</td>
<td>racfClassLogFailure</td>
<td>LOGOPTIONS FAILURES</td>
</tr>
<tr>
<td>racfOptionSegLog</td>
<td>racfClassLogNever</td>
<td>LOGOPTIONS NEVER</td>
</tr>
<tr>
<td>racfOptionSegLog</td>
<td>racfClassLogSuccess</td>
<td>LOGOPTIONS SUCCESS</td>
</tr>
<tr>
<td>racfOptionSegLog</td>
<td>racfOption</td>
<td>Option Type</td>
</tr>
<tr>
<td>racfOptionSegLog</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfOptionSegModel</td>
<td>racfModelGdg</td>
<td>MODEL GDG</td>
</tr>
</tbody>
</table>
Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfOptionSegModel</td>
<td>racfModelGroup</td>
<td>MODEL GROUP</td>
</tr>
<tr>
<td>racfOptionSegModel</td>
<td>racfModelUser</td>
<td>MODEL USER</td>
</tr>
<tr>
<td>racfOptionSegModel</td>
<td>racfOption</td>
<td>Option Type</td>
</tr>
<tr>
<td>racfOptionSegModel</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfOption</td>
<td>Option Type</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordHistory</td>
<td>PASSWORD HISTORY</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordInterval</td>
<td>PASSWORD INTERVAL</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRevoke</td>
<td>PASSWORD REVOKE</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRule1</td>
<td>PASSWORD RULE1</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRule2</td>
<td>PASSWORD RULE2</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRule3</td>
<td>PASSWORD RULE3</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRule4</td>
<td>PASSWORD RULE4</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRule5</td>
<td>PASSWORD RULE5</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRule6</td>
<td>PASSWORD RULE6</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRule7</td>
<td>PASSWORD RULE7</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordRule8</td>
<td>PASSWORD RULE8</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfPasswordWarning</td>
<td>PASSWORD WARNING</td>
</tr>
<tr>
<td>racfOptionSegPass</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfOptionSegRvary</td>
<td>racfOption</td>
<td>Option Type</td>
</tr>
<tr>
<td>racfOptionSegRvary</td>
<td>racfRvaryStatusPw</td>
<td>RVARY STATUS</td>
</tr>
<tr>
<td>racfOptionSegRvary</td>
<td>racfRvarySwitchPw</td>
<td>RVARY SWITCH</td>
</tr>
<tr>
<td>racfOptionSegRvary</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfAppldata</td>
<td>Application Data</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfAudit</td>
<td>Audit</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfCategory</td>
<td>Category</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfClassnum</td>
<td>Class Number</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfCreatedate</td>
<td>Create Date</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfData</td>
<td>Installation Data</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfGeneric</td>
<td>Generic</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfGlobalaudit</td>
<td>Global Audit</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfLevel</td>
<td>Log Level</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfModifierGroup</td>
<td>Last Modifier Group</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfModifierUser</td>
<td>Last Modifier User</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfModifyDate</td>
<td>Last Modified Date</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfNotify</td>
<td>Notify</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfOwner</td>
<td>Owner</td>
</tr>
</tbody>
</table>
### Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfResource</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfSeclabel</td>
<td>Security Label</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfSeclevel</td>
<td>Security Level</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfTapeAuto</td>
<td>Auto Protect</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfTapeSingledsn</td>
<td>Single DSN</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfTapeVtoc</td>
<td>Tape VTOC</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfTimezone</td>
<td>Time Zone</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfTvolCreatedate</td>
<td>Tape Create Date</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfTvolCreatename</td>
<td>Tape Create Name</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfTvolDiscrete</td>
<td>Tape Discrete</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfUacc</td>
<td>Universal Access</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfVolser</td>
<td>Volume Serials</td>
</tr>
<tr>
<td>racfResource</td>
<td>racfWarning</td>
<td>Warning</td>
</tr>
<tr>
<td>racfResourceAppcport</td>
<td>racfAppcport</td>
<td>APPC Port</td>
</tr>
<tr>
<td>racfResourceAppcport</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceAppcport</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceConsole</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceConsole</td>
<td>racfConsole</td>
<td>Console</td>
</tr>
<tr>
<td>racfResourceConsole</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceJesinput</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceJesinput</td>
<td>racfJesinput</td>
<td>JES Input Device</td>
</tr>
<tr>
<td>racfResourceJesinput</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfCategory</td>
<td>Category</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfClass</td>
<td>Member Class</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfPadsData</td>
<td>Program Access Data</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfResource</td>
<td>Resource Group Name</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfResourceMember</td>
<td>Resource Member</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfSeclevel</td>
<td>Security Level</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfUacc</td>
<td>Universal Access</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfVmexitdata</td>
<td>VMX Event Auditing</td>
</tr>
<tr>
<td>racfResourceMember</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
<tr>
<td>racfResourcePermitAp</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfResourcePermitAp</td>
<td>racfAppcport</td>
<td>APPC Port</td>
</tr>
<tr>
<td>racfResourcePermitAp</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourcePermitAp</td>
<td>racfPermitId</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfResourcePermitAp</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
</tbody>
</table>
Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfResourcePermitCo</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfResourcePermitCo</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourcePermitCo</td>
<td>racfConsole</td>
<td>Console</td>
</tr>
<tr>
<td>racfResourcePermitCo</td>
<td>racfPermitId</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfResourcePermitCo</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourcePermitId</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfResourcePermitId</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourcePermitId</td>
<td>racfJesinput</td>
<td>JES Input Device</td>
</tr>
<tr>
<td>racfResourcePermitId</td>
<td>racfPermitId</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfResourcePermitId</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourcePermitPr</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfResourcePermitPr</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourcePermitPr</td>
<td>racfPermitId</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfResourcePermitPr</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourcePermitSy</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfResourcePermitSy</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourcePermitSy</td>
<td>racfPermitId</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfResourcePermitSy</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourcePermitSy</td>
<td>racfSysid</td>
<td>System ID</td>
</tr>
<tr>
<td>racfResourcePermitTe</td>
<td>racfAccess</td>
<td>Access</td>
</tr>
<tr>
<td>racfResourcePermitTe</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourcePermitTe</td>
<td>racfPermitId</td>
<td>Permitted ID</td>
</tr>
<tr>
<td>racfResourcePermitTe</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourcePermitTe</td>
<td>racfTerminal</td>
<td>Terminal</td>
</tr>
<tr>
<td>racfResourceProgram</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceProgram</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegDlf</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSegDlf</td>
<td>racfDlfJobs</td>
<td>DLF Job Names</td>
</tr>
<tr>
<td>racfResourceSegDlf</td>
<td>racfDlfRetain</td>
<td>DLF Retain</td>
</tr>
<tr>
<td>racfResourceSegDlf</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegDlf</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbDefktlfe</td>
<td>Default Ticket Life</td>
</tr>
</tbody>
</table>
**Table 3. RACF field/LDAP attribute mappings**

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbEncryptdes</td>
<td>Encrypt DES</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbEncryptdes3</td>
<td>Encrypt DES3</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbEncryptdesd</td>
<td>Encrypt DESD</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbKerbname</td>
<td>Local Realm Name</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbKeyver</td>
<td>Key Version</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbMaxtktlfe</td>
<td>Maximum Ticket Life</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbMintktlfe</td>
<td>Minimum Ticket Life</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfKerbPassword</td>
<td>Kerberos Password</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegKerb</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfSessFailMax</td>
<td>Max Session Failures</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfSessInterval</td>
<td>Session Interval</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfSessKey</td>
<td>Session Key</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfSessKeyDate</td>
<td>Session Key Date</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfSessLocked</td>
<td>Session Locked</td>
</tr>
<tr>
<td>racfResourceSegSess</td>
<td>racfSessSecurity</td>
<td>Session Security</td>
</tr>
<tr>
<td>racfResourceSegSsign</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSegSsign</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegSsign</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResourceSegSsign</td>
<td>racfSsignKeyencrypt</td>
<td>Encrypted Key</td>
</tr>
<tr>
<td>racfResourceSegSsign</td>
<td>racfSsignKeymasked</td>
<td>Masked Key</td>
</tr>
<tr>
<td>racfResourceSegStdat</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSegStdat</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegStdat</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResourceSegStdat</td>
<td>racfStdatGroup</td>
<td>Group-ID</td>
</tr>
<tr>
<td>racfResourceSegStdat</td>
<td>racfStdatPrivileged</td>
<td>Privileged Task</td>
</tr>
<tr>
<td>racfResourceSegStdat</td>
<td>racfStdatTrace</td>
<td>Trace Task</td>
</tr>
<tr>
<td>racfResourceSegStdat</td>
<td>racfStdatTrusted</td>
<td>Trusted Task</td>
</tr>
<tr>
<td>racfResourceSegStdat</td>
<td>racfStdatUser</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfResourceSegSvfmr</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSegSvfmr</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegSvfmr</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResourceSegSvfmr</td>
<td>racfSvfmrParm</td>
<td>Parameter File</td>
</tr>
<tr>
<td>racfResourceSegSvfmr</td>
<td>racfSvfmrScript</td>
<td>Script File</td>
</tr>
</tbody>
</table>
Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfResourceSegTme</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSegTme</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegTme</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResourceSegTme</td>
<td>racfTmeChild</td>
<td>Child Role</td>
</tr>
<tr>
<td>racfResourceSegTme</td>
<td>racfTmeGroup</td>
<td>Group-ID</td>
</tr>
<tr>
<td>racfResourceSegTme</td>
<td>racfTmeParent</td>
<td>Parent Role</td>
</tr>
<tr>
<td>racfResourceSegTme</td>
<td>racfTmeResource</td>
<td>Resource Access Spec</td>
</tr>
<tr>
<td>racfResourceSegTme</td>
<td>racfTmeRoles</td>
<td>Role Access Spec</td>
</tr>
<tr>
<td>racfResourceSegWhen</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSegWhen</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSegWhen</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfResourceSegWhen</td>
<td>racfWhenDays</td>
<td>When Days</td>
</tr>
<tr>
<td>racfResourceSegWhen</td>
<td>racfWhenTime</td>
<td>When Time</td>
</tr>
<tr>
<td>racfResourceSysid</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceSysid</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceSysid</td>
<td>racfSysid</td>
<td>System ID</td>
</tr>
<tr>
<td>racfResourceTerminal</td>
<td>racfClass</td>
<td>Class</td>
</tr>
<tr>
<td>racfResourceTerminal</td>
<td>racfResource</td>
<td>Resource Name</td>
</tr>
<tr>
<td>racfResourceTerminal</td>
<td>racfTerminal</td>
<td>Terminal</td>
</tr>
<tr>
<td>racfResourceTvtoc</td>
<td>racfDataset</td>
<td>Dataset Name</td>
</tr>
<tr>
<td>racfUser</td>
<td>cn</td>
<td>User Name</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfAdsp</td>
<td>ADSP</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfAuditor</td>
<td>Auditor</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfAuthority</td>
<td>Group Authority</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfCategory</td>
<td>Category</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfClauth</td>
<td>Class Authorizations</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfCreatedate</td>
<td>Create Date</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfData</td>
<td>Installation Data</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfDfltgrp</td>
<td>Default Group</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfExpired</td>
<td>Expired</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfGrpacc</td>
<td>Group Access</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfLastjobdate</td>
<td>Last Job Date</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfLastjobtime</td>
<td>Last Job Time</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfModel</td>
<td>Model Dataset Profile</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfModifierGroup</td>
<td>Last Modifier Group</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfModifierUser</td>
<td>Last Modifier User</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfModifyDate</td>
<td>Last Modified Date</td>
</tr>
</tbody>
</table>
Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfUser</td>
<td>racfNopassword</td>
<td>No Password</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfOidcard</td>
<td>Operator-ID Card</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfOperations</td>
<td>Operations</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfOwner</td>
<td>Owner</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfPassword</td>
<td>Password</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfPassworddate</td>
<td>Password Date</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfPasswordgen</td>
<td>Password Generation</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfPasswordInterval</td>
<td>Password Interval</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfRestricted</td>
<td>Restricted</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfResumeDate</td>
<td>Resume Date</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfRevoke</td>
<td>Revoke</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfRevokecount</td>
<td>Revoke Count</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfRevokeDate</td>
<td>Revoke Count</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfSeclabel</td>
<td>Security Label</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfSeclevel</td>
<td>Security Level</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfSpecial</td>
<td>Special</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfUacc</td>
<td>Universal Access</td>
</tr>
<tr>
<td>racfUser</td>
<td>racfUaudit</td>
<td>User Audit</td>
</tr>
<tr>
<td>racfUser</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfAdsp</td>
<td>ADSP</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfAuditor</td>
<td>Auditor</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfAuthority</td>
<td>Authority</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfCreatedate</td>
<td>Create Date</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfGroup</td>
<td>Group</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfGrpacc</td>
<td>Group Access</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfModifierGroup</td>
<td>Last Modifier Group</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfModifierUser</td>
<td>Last Modifier User</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfModifyDate</td>
<td>Last Modified Date</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfOperations</td>
<td>Operations</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfOwner</td>
<td>Owner</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfResumeDate</td>
<td>Resume</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfRevoke</td>
<td>Revoke</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfRevokeDate</td>
<td>Revoke Date</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfSpecial</td>
<td>Special</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfTermuacc</td>
<td>Terminal Unv. Access</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>racfUacc</td>
<td>Universal Access</td>
</tr>
<tr>
<td>racfUserConnect</td>
<td>uid</td>
<td>User-ID</td>
</tr>
</tbody>
</table>
### Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfUserSegCics</td>
<td>racfCicsOpclass</td>
<td>CICS Operator Class</td>
</tr>
<tr>
<td>racfUserSegCics</td>
<td>racfCicsOpident</td>
<td>Cics Operator-ID</td>
</tr>
<tr>
<td>racfUserSegCics</td>
<td>racfCicsOpprty</td>
<td>CICS Oper. Priority</td>
</tr>
<tr>
<td>racfUserSegCics</td>
<td>racfCicsTimeout</td>
<td>CICS Timeout</td>
</tr>
<tr>
<td>racfUserSegCics</td>
<td>racfCicsXrfsoff</td>
<td>Force XRF Logoff</td>
</tr>
<tr>
<td>racfUserSegCics</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegDce</td>
<td>racfDceAutologon</td>
<td>DCE Autologon</td>
</tr>
<tr>
<td>racfUserSegDce</td>
<td>racfDceHomecell</td>
<td>DCE Home Cell Name</td>
</tr>
<tr>
<td>racfUserSegDce</td>
<td>racfDceHomeuuid</td>
<td>DCE Home UUID</td>
</tr>
<tr>
<td>racfUserSegDce</td>
<td>racfDceName</td>
<td>DCE Name</td>
</tr>
<tr>
<td>racfUserSegDce</td>
<td>racfDceUuid</td>
<td>DCE UUID</td>
</tr>
<tr>
<td>racfUserSegDce</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegDce</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegDfp</td>
<td>racfDfpDataappl</td>
<td>DFP Data Appl-ID</td>
</tr>
<tr>
<td>racfUserSegDfp</td>
<td>racfDfpDataclas</td>
<td>DFP Dflt. Data Class</td>
</tr>
<tr>
<td>racfUserSegDfp</td>
<td>racfDfpMgmtclas</td>
<td>DFP Management Class</td>
</tr>
<tr>
<td>racfUserSegDfp</td>
<td>racfDfpStorclas</td>
<td>DFP Storage Class</td>
</tr>
<tr>
<td>racfUserSegDfp</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegDfp</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegKerb</td>
<td>racfKerbEncryptdes</td>
<td>Encrypt DES</td>
</tr>
<tr>
<td>racfUserSegKerb</td>
<td>racfKerbEncryptdes3</td>
<td>Encrypt DES3</td>
</tr>
<tr>
<td>racfUserSegKerb</td>
<td>racfKerbEncryptdesd</td>
<td>Encrypt DESD</td>
</tr>
<tr>
<td>racfUserSegKerb</td>
<td>racfKerbsKerbname</td>
<td>Principal Name</td>
</tr>
<tr>
<td>racfUserSegKerb</td>
<td>racfKerbKeyver</td>
<td>Key Version</td>
</tr>
<tr>
<td>racfUserSegKerb</td>
<td>racfKerbsMaxtktlife</td>
<td>Maximum Ticket Life</td>
</tr>
<tr>
<td>racfUserSegKerb</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegKerb</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegLanguage</td>
<td>racfLanguagePrimary</td>
<td>Language Primary</td>
</tr>
<tr>
<td>racfUserSegLanguage</td>
<td>racfLanguageSecondary</td>
<td>Language Secondary</td>
</tr>
<tr>
<td>racfUserSegLanguage</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegLanguage</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegLnotes</td>
<td>racfLnotesSname</td>
<td>Short Name</td>
</tr>
<tr>
<td>racfUserSegLnotes</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegLnotes</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegNds</td>
<td>racfNdsUname</td>
<td>NDS User Name</td>
</tr>
<tr>
<td>racfUserSegNds</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
</tbody>
</table>
Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfUserSegNds</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfNetviewConsname</td>
<td>Console Name</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfNetviewCtl</td>
<td>Control</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfNetviewDomains</td>
<td>Domains</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfNetviewIc</td>
<td>Initial Commands</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfNetviewMsgrecvr</td>
<td>Receive Messages</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfNetviewNgmfdmnn</td>
<td>Graphic Monitor</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfNetviewNgmfsnp</td>
<td>View Span</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfNetviewOpclass</td>
<td>Operator Scope Class</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegNetview</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsAssizemax</td>
<td>Max Address Space</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsCputimemax</td>
<td>Max CPU Time</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsFileprocmax</td>
<td>Max Open Files</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsHome</td>
<td>Home Directory Path</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsMmaparemamx</td>
<td>Max MMAP Area</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsProcusermax</td>
<td>Max Active Processes</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsProgram</td>
<td>Shell Program Path</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsThreadsmx</td>
<td>Max Threads</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfOmvsUid</td>
<td>Unix User-ID (UID)</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegOmvs</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperAltgrp</td>
<td>Alt console group</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperAuth</td>
<td>Console Authorities</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperAuto</td>
<td>Automated Messages</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperCmdsys</td>
<td>Command System</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperDom</td>
<td>Delete Operator Msgs</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperKey</td>
<td>Console Key</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperLevel</td>
<td>Message Level</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperLogcmdresp</td>
<td>Log Command Response</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperMform</td>
<td>Message Format</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperMgid</td>
<td>Migration ID</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperMonitor</td>
<td>Monitor Events</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperMscope</td>
<td>Message Scope</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperRoutcode</td>
<td>Message Routing Code</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperStorage</td>
<td>Storage</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperSystem</td>
<td>System</td>
</tr>
<tr>
<td>LDAP object class</td>
<td>LDAP attribute name</td>
<td>RACF field name</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfOperUd</td>
<td>Undelivered Messages</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegOper</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegOvm</td>
<td>racfOvmFsroot</td>
<td>File System Root</td>
</tr>
<tr>
<td>racfUserSegOvm</td>
<td>racfOvmGid</td>
<td>OVM Group-ID (GID)</td>
</tr>
<tr>
<td>racfUserSegOvm</td>
<td>racfOvmHome</td>
<td>Home</td>
</tr>
<tr>
<td>racfUserSegOvm</td>
<td>racfOvmProgram</td>
<td>Initial Program</td>
</tr>
<tr>
<td>racfUserSegOvm</td>
<td>racfOvmUid</td>
<td>OVM User-ID (UID)</td>
</tr>
<tr>
<td>racfUserSegOvm</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegOvm</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoAcctnum</td>
<td>Account Number</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoCommand</td>
<td>Command</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoDest</td>
<td>Destination</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoHoldclass</td>
<td>Hold Class</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoJobclass</td>
<td>Job Class</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoMaxsize</td>
<td>Region Size Max</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoMsgclass</td>
<td>Message Class</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoPerfgroup</td>
<td>Performance Group</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoProc</td>
<td>Logon Procedure</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoSeclabel</td>
<td>Security Label</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoSize</td>
<td>Region Size Default</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoSysoutclass</td>
<td>Sysout Class</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoUnit</td>
<td>Unit for Procedures</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>racfTsoUserdata</td>
<td>User Data</td>
</tr>
<tr>
<td>racfUserSegTso</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegWhen</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegWhen</td>
<td>racfWhenDays</td>
<td>When Days</td>
</tr>
<tr>
<td>racfUserSegWhen</td>
<td>racfWhenTime</td>
<td>When Time</td>
</tr>
<tr>
<td>racfUserSegWhen</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfSegment</td>
<td>Segment Identifier</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrAcct</td>
<td>Account</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrAddr 1</td>
<td>Address Line 1</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrAddr 2</td>
<td>Address Line 2</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrAddr 3</td>
<td>Address Line 3</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrAddr 4</td>
<td>Address Line 4</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrBldg</td>
<td>Building</td>
</tr>
</tbody>
</table>
### Table 3. RACF field/LDAP attribute mappings

<table>
<thead>
<tr>
<th>LDAP object class</th>
<th>LDAP attribute name</th>
<th>RACF field name</th>
</tr>
</thead>
<tbody>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrDept</td>
<td>Department</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrName</td>
<td>Name</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>racfWorkattrRoom</td>
<td>Room</td>
</tr>
<tr>
<td>racfUserSegWorkattr</td>
<td>uid</td>
<td>User-ID</td>
</tr>
<tr>
<td>racfVolser</td>
<td>racfVolser</td>
<td>Volume Serial</td>
</tr>
</tbody>
</table>
Appendix C. 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  10594-1785
U.S.A.

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this publication 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 as your own risk.

Licensees of this program who want 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:

International Business Machines Corporation
Department J46A/G4
## Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

<table>
<thead>
<tr>
<th>AIX</th>
<th>iSeries</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS/400</td>
<td>NUMA-Q</td>
</tr>
<tr>
<td>DataJoiner</td>
<td>MVS</td>
</tr>
<tr>
<td>DB2</td>
<td>OS/2</td>
</tr>
<tr>
<td>DB2® Connect</td>
<td>OS/390</td>
</tr>
<tr>
<td>Distributed Relational Database Architecture</td>
<td>Redbooks</td>
</tr>
<tr>
<td>DRDA</td>
<td>SAA</td>
</tr>
<tr>
<td>IBM</td>
<td>SQL/DS</td>
</tr>
<tr>
<td>Informix</td>
<td>z/OS</td>
</tr>
</tbody>
</table>

Microsoft® and WindowsNT are registered trademarks in the United States, other countries, or both.

Java™ and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

A
about this guide v
accessibility vi
accessing publications online vi
architecture 1
clients 3
server 2

B
base information vi

C
client
delegeted administration features 5
features 4
installation instructions 7
interface concepts 3
multiple database management features 6
overview 3
productivity features 4
software prerequisites 7

client
common administrator tasks
ISPF client 47
accessing system options 84
activating/deactivating class 84
activating/deactivating command class 85
adding a database 50
adding a generic dataset 57
adding a group 55
adding a new user 52
administering system options 84
connecting group to multiple users 18
connecting user to group 53
copying a profile 83
creating a view 76
defining a resource 68
defining sub-fields 77
deleting a profile 84
enabling/disabling auditing 84
executing views 47
permitting access to a dataset 62
permitting access to resource 70
permitting conditional access to a dataset 64
permitting conditional access to resource 72
searching in a profile 50
sorting entries 50
using sub-fields 83
viewing parents and children 49
PC client 14
accessing system options 27
activating/deactivating class 27
activating/deactivating command class 27
adding a database 15
adding a generic dataset 18
adding a group 17
adding a new user 16
administering system options 27
cloning a group 18
cloning user 16

connect database prompt
ISPF client 36
connect prompt
PC client 12
connect screen
PC client 10
contents of this book v
conventions
typeface vii
customer support vii

D
disability vi
documentation
IBM Tivoli Security Administrator for RACF v

F
features 5
flexible searching 5

G
guide organization v

I
installation instructions
client 7
disk and memory requirements 7
prerequisites 7
procedure 8
software package contents 7
introduction
IBM Tivoli Security Administrator for RACF 1
ISPF client 3, 31
accessing system options 84
activating/deactivating class 84
activating/deactivating command class 85
adding a database 50
adding a discrete dataset 59
adding a generic dataset 57
adding a group 55
adding a new user 52
administering system options 84
common administrator tasks 47
   executing views 47
   viewing entries 48
connect database prompt 36
connecting group to multiple users 57
connecting user to group 53
copying a profile 83
creating a view 76
defining a resource 68
defining sub-fields 77
deleting a profile 84
enabling/disabling auditing 84
messages 31
modify value prompt 46
permitting access to a dataset 20
permitting access to resource 21
permitting conditional access to a dataset 20
permitting conditional access to resource 22
searching in a profile 50
searching in a profile 50
setting fonts and colors 9
sorting entries 15
starting 9
using database directories pane 14
using sub-fields 25
view filter prompt 13
viewing parents and children 15
preface information v
product architecture 1
   clients 3
   configuration database 3
   ldap2racf 2
   mirror database 2
   pc client 3
   racf2ldap 2
   server 2
publications
   accessing online vi
   ordering vi
R
   RACF/LDAP mappings 91
release information v
S
search filters 89
   boolean operators 91
   general operators 90
   general syntax 89
   multiple search filter syntax 89
   operators 90
   RACF/LDAP mappings 91
   syntax 89
   syntax examples 89
Security Administrator architecture 1
   clients 3
   configuration database 3
   ldap2racf 2
   mirror database 2
   pc client 3
   racf2ldap 2
   server 2
setting fonts and colors 9
software prerequisites 7
starting
   ISPF client 31
   PC client 9
   support, customer vii
T
   trademarks 109
   typeface conventions vii
U
URLs
customer support vii

V
view entry panel
  ISPF client 43
view filter prompt
  PC client 13
view prompt
  ISPF client 37
view results databases panel
  ISPF client 32
view results panel
  ISPF client 39
**Readers’ Comments—We’d Like to Hear from You**

IBM Tivoli Security Administrator for RACF
User’s Guide
Version 1.1

Publication No. SC18-9476-01

---

**Overall, how satisfied are you with the information in this book?**

<table>
<thead>
<tr>
<th>Very Satisfied</th>
<th>Satisfied</th>
<th>Neutral</th>
<th>Dissatisfied</th>
<th>Very Dissatisfied</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**How satisfied are you that the information in this book is:**

<table>
<thead>
<tr>
<th>Very Satisfied</th>
<th>Satisfied</th>
<th>Neutral</th>
<th>Dissatisfied</th>
<th>Very Dissatisfied</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Accurate**
- **Complete**
- **Easy to find**
- **Easy to understand**
- **Well organized**
- **Applicable to your tasks**

**Please tell us how we can improve this book:**

---

Thank you for your response. May we contact you?  

☑ Yes  ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

---

**Name**  
**Address**

**Company or Organization**

**Phone No.**