IBM Security Identity Governance and Intelligence

# *RACF Adapter Installation and Configuration Guide*

# Contents

# List of Figures

# List of Tables

# Chapter 1. Overview

An adapter is an interface between a managed resource and the IBM® Security Identity server.

Adapters can be installed on the managed resource. The IBM Security Identity server manages access to the resource by using the security system. Adapters function as trusted virtual administrators on the target operating system. The adapter creates, suspends, restores user accounts, and other functions that administrators run manually. The adapter runs as a service, independently of whether you are logged on to the IBM Security Identity server.

The adapter works with the RACF product on a UNIX System Services environment of z/OS.

The adapter:

- Receives provisioning requests from IBM Security Identity Governance and Intelligence.
- Processes the requests to add, modify, suspend, restore, delete, and reconcile user information from the adapter security database.
- Converts the Directory Access Markup Language (DAML) requests that are received from IBM Security Identity Governance and Intelligence to the corresponding adapter Security for z/OS® commands. The Enrole Resource Management API (ERMA) libraries are used for the conversion.
- Forwards the commands to a command executor through a series of **`tscocmd/IRRSEQ00`** requests. The command executor receives the formatted command strings and results are collected by the adapter through the same process
- Returns the results of the command and includes the success or failure message of a request to IBM Security Identity Governance and Intelligence.

The following figure describes the various components of the adapter.

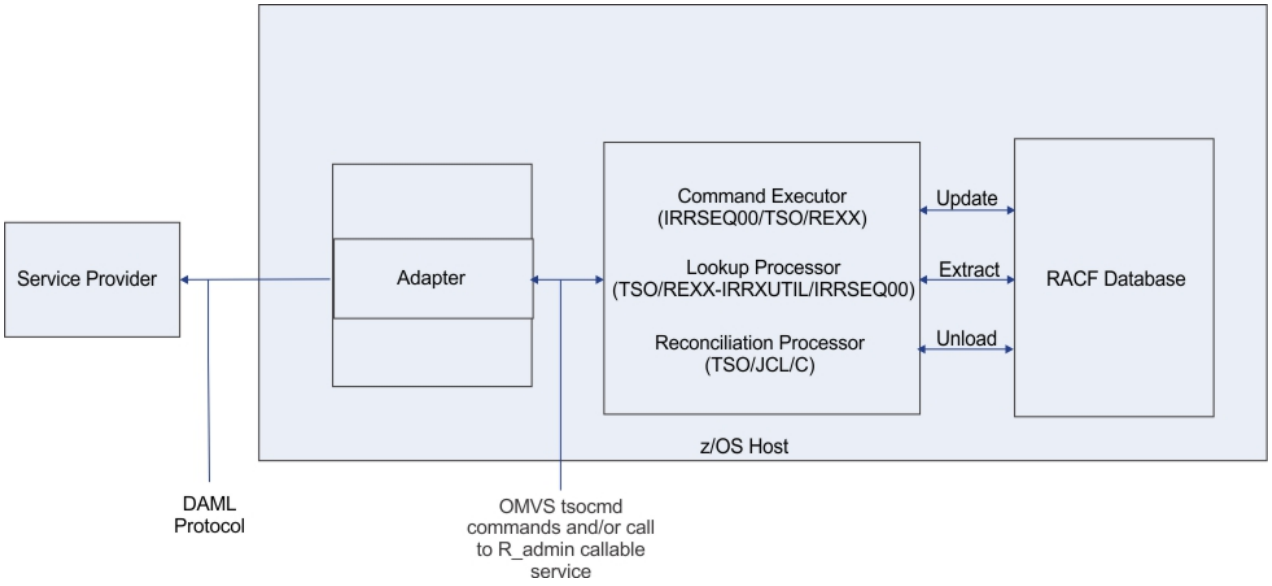


*Figure 1: The RACF Adapter components*

**Adapter**
Receives and processes requests from IBM Security Identity Governance and Intelligence. The adapter can handle multiple requests simultaneously. Each request results in execution of a **`tscocmd`** based TSO command transaction. The binary files of the adapter and related external files are in the UNIX System Services environment of z/OS (OS/390®).

**Command Executor**
Operates as either a TSO command transaction (**`tscocmd`** based) or a RACF operator command transaction (R_admin API/ IRRSEQ000 based) that is triggered by an incoming request from the

adapter. These requests consist of commands. TSO command transactions support reconciliation and ISIMEXIT processing. RACF operator commands support account Add, Modify, and Delete processing. The adapter runs these commands from the UNIX System Services environment and collects the results that are returned by RACF, MVS, and or REXX depending on the specific command to run.

**Reconciliation Processor**

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

Scope of authority is referred to as scoped reconciliation.

**To enable scoped reconciliations**

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

**To switch between SCOPED and non-SCOPED**

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

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

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

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

The LOOKUP transaction type uses the `(eruid=<userid>)` filter in IBM Security Identity Governance and Intelligence for the reconciliation of a single account. This transaction type ensures that no Pdu entries are created for entries that do not match the `eruid` specified in the search filter in the server request. For debugging this type of processing, more messages for the `_ermPduAddEntry` process are added in the Base Logging level (BSE). Unfiltered requests or requests with more than one account that is specified in the search filter still result in a full reconciliation that uses the standard SEARCH transaction.

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

**Lookup Processor**

The LOOKUP operation uses the (`eruid=<userid>`) filter in IBM Security Identity Governance and Intelligence for the reconciliation of a single account. This transaction is implemented using the Lookup Processor. The Lookup Processor uses a REXX interface to `R_Admin (IRRXUTIL)` to specifically extract only the data that belongs to the user account that is specified in the search filter.

The **tsocmd** command processor is used to call the REXX script with the name of the user account to be looked up. The REXX interface script `ISIMLOKU` is located in the `EXEC` library along with the `ISIMEXIT` and `ISIMEXEC` sample REXX scripts.

Similar to the *Full Reconciliation* operation, the `ISIM LOKU REXX` script uses the `RECOSAVE` data set to store the intermediate results that are returned by `IRRXUTIL`. Requests, which are not filtered or with more than one account that is specified in the search filter, still results in a full reconciliation that uses the standard *SEARCH* operation

## Adapter considerations

The RACF Adapter requires APF authorization. As such, the RACF ID used by the adapter must have READ access to the BPX.SERVER profile in the FACILITY class. If the SURROGAT User ID is being used, the adapter ID must have UPDATE access to the BPX.SERVER profile in the FACILITY class.

For the R_admin callable service (IRRSEQ00) or RACF operator command processing additional profile access is required.

A detailed overview of required permissions can be found in "Access configuration" on page 23.

**Note:** It is required to use the full command name as shown in the examples above when you define the resource. Note that the adapter libraries and binaries must be program controlled and run from an APF authorized library which is accomplished by the extattr +ap commands that are executed at installation time.

The RACF Adapter operates in two basic modes.

- There might be no operational RACF ID that is specified on the IBM Security Identity Governance and Intelligence service form when a request is issued. In this case, the RACF user ID that the adapter uses requires specific privileges. For example, if the adapter administers all users in the RACF database, it must operate with the SYSTEM SPECIAL RACF attribute.

  The IBM Security Identity Governance and Intelligence might do operations against only a portion of the RACF database. In this case, the adapter must be associated with a group assigned GROUP SPECIAL privileges, for the portion of the database it administers. The following figure depicts the preceding scenario.

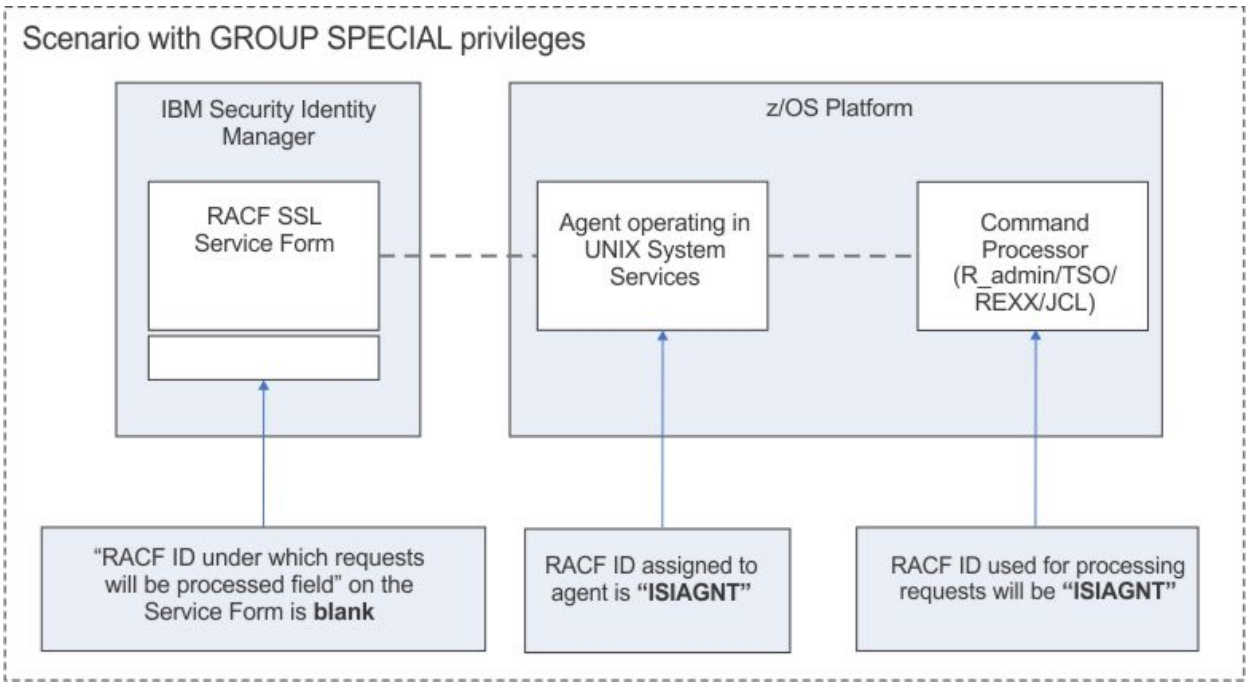


*Figure 2: Scenario with GROUP SPECIAL privileges*

- The operations might be done under a RACF ID specified on the IBM Security Identity Manager service form. In this case, the RACF ID, which the adapter uses does not require any special privileged attributes. It does, however, require surrogate authority to run functions under the identity of the RACF ID specified on the IBM Security Identity Governance and Intelligence service form. The adapter RACF ID must have READ permission on the BPX.SRV.<SURROGATID> profile in the SURROGAT class. The RACF ID that is specified on the IBM Security Identity Governance and Intelligence service form must have authority for the administration functions requested by the IBM Security Identity server.

  The following figure depicts the preceding scenario:

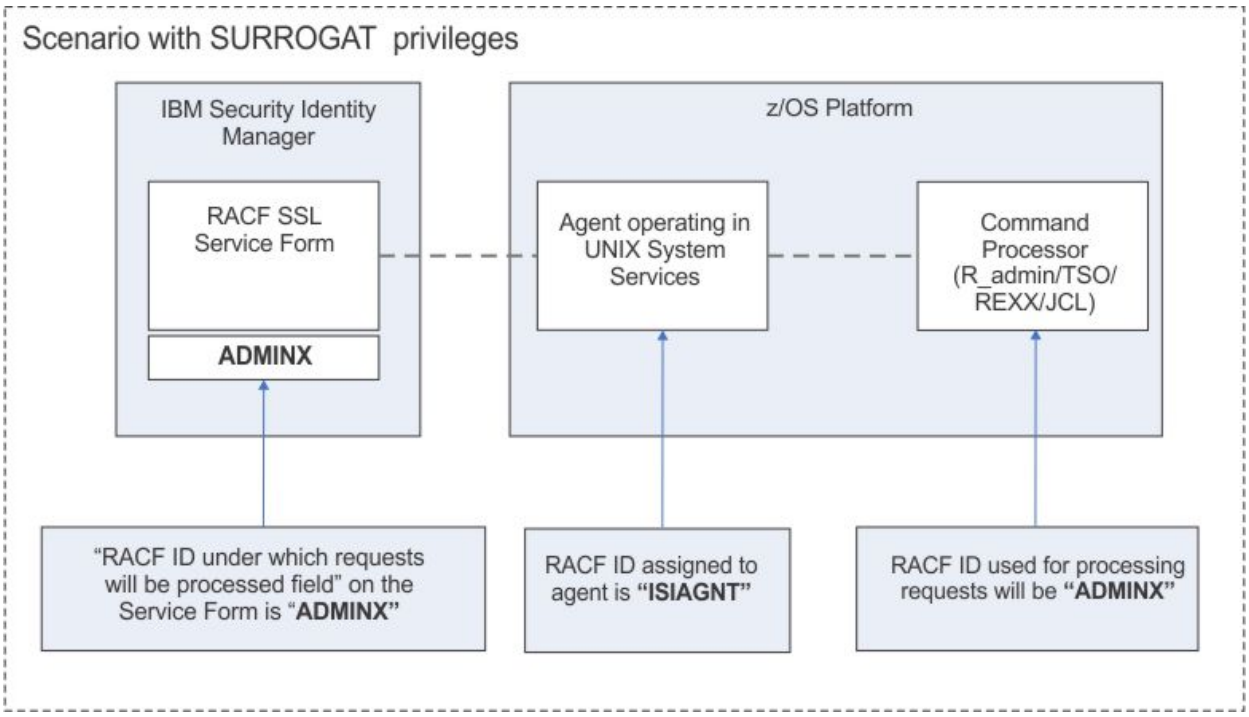


*Figure 3: Scenario with surrogate authority*

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

The RACF resources that require consideration are:

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

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

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

**The STGADMIN.IGG.DEFDEL.UALIAS might be required if catalog aliases are created in the ISIMEXIT or ISIMEXEC adapter exit points.**
STGADMIN.IGG.DEFDEL.UALIAS is required if your user exits create or delete catalog aliases and the effective RACF ID does not have MCAT update authority.

**SURROGAT class profile BPX.SRV.<SURROGAT RACF ID> with READ**
The surrogate profile is required if the adapter RACF ID differs from the RACF ID under which commands and reconciliations are done.

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

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

**Related concepts**

Adapter interactions with the server

The RACF Adapter uses IBM Security Identity Governance and Intelligence to perform user tasks on the RACF Adapter Security for z/OS.

## Adapter interactions with the server

The RACF Adapter uses IBM Security Identity Governance and Intelligence to perform user tasks on the RACF Adapter Security for z/OS.

The adapter can add, modify, suspend, restore, reconcile, or delete users from IBM Security Identity Governance and Intelligence. The adapter uses the TCP/IP protocol to communicate with IBM Security Identity Governance and Intelligence.

The RACF Adapter does not use Secure Socket Layer (SSL) by default to communicate with IBM Security Identity Governance and Intelligence. You have to configure it.

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

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

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

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

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

**Related concepts**

Adapter considerations

The RACF Adapter requires APF authorization. As such, the RACF ID used by the adapter must have READ access to the BPX.SERVER profile in the FACILITY class. If the SURROGAT User ID is being used, the adapter ID must have UPDATE access to the BPX.SERVER profile in the FACILITY class.

# Chapter 2. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

## Roadmap for Adapter Development Kit based adapters, using ISPF

Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

**Pre-installation**

Complete these tasks.

1. Verify that your environment meets the software and hardware requirements for the adapter. See *Prerequisites*.
2. Obtain the installation software. See *Software downloads*.
3. Obtain the necessary information for the installation and configuration. See *Installation worksheet*.

**Installation**

Complete these tasks.

1. Install the ISPF dialog.
2. Run the ISPF dialog.
3. Restart the adapter service.
4. Import the adapter profile.
5. Create an adapter service/target.
6. Install the adapter language package.
7. Verify that the adapter is working correctly.

**Upgrade**

To upgrade the adapter, do a complete re-installation of the adapter. Follow the *Installation roadmap*.

**Configuration**

Complete these tasks.

1. Configure secure communication between the IBM Security Identity server and the adapter.
   a. Configure 1-way authentication.
   b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
   a. Configure 1-way authentication.
   b. Configure 2-way authentication.
3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

**Troubleshooting**

See the following topics.

- Techniques for troubleshooting problems
- Configure debugging
- Logs
- Error messages and problem solving

**Uninstallation**

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

**Reference**

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

## Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter.

| *Table 1: Prerequisites to install the adapter* | |
|---|---|
| Operating System | See the Release Notes for the supported software versions. |
| Network Connectivity | Internet Protocol network |
| Server Communication | Communication must be tested with a low-level communications ping from the IBM Security Identity server to the z/OS Server. When you do so, it is easier to troubleshoot possible installation problems. |
| IBM Security Identity server | IBM Security Identity server products that are currently supported and the corresponding releases are documented in the Release Notes that are included in the installation package. |
| Required authority | You must have system administrator authority to complete the installation procedure. |

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

**Note:** Support for Sysplex failover is not implemented. When the participating image of the Sysplex running the adapter becomes inoperative:

1. Restart the failed z/OS image.
2. Restart the adapter.

You can also pre-configure another instance of the adapter for use on another image. You must already have this type of environment setup and the necessary resources available. The related service instance on the IBM Security Identity server might require updates if the alternate image is known through a different IP address.

## Software downloads

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

Go to IBM Passport Advantage.

See the corresponding *IBM Security Identity server Download Document* for instructions.

**Note:**

You can also obtain additional adapter information from IBM Support.

# Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

| | |
|---|---|
| MVS data set name | The MVS data set high-level qualifier for upload and installation. |
| Adapter instance name | The default is `racfagent`. There is no maximum length, but the length must be manageable. This value is specified in the config.sh UNIX System Services shell script. |
| USS Adapter read-only home | The USS file system location that is used to store the adapter binaries. The default is /usr/lpp/isimracf. The read-only home and the read/write home must specify different locations. If they are the same then the installation may fail. It is advised to allocate at least 60 Mb of free space to the read/only home. |
| USS Adapter read/write home | The USS file system location that is used to store the adapter log file, register, intermediate reconciliation results and start scripts. The default is `/var/ibm/isimracf`. The read-only home and the read/write home must specify different locations. If they are the same, then the installation might fail. The read/write home size must be large enough that it can be temporary used to store intermediate reconciliation results. For example, 1 Mb / 100 accounts or groups. The size must be more than the regular requirements for activity logging, depending on the adapter-specific configuration and storing all adapter scripts and registry files. |
| Adapter port number | The default is 45580. This value can be modified by using the agentCfg UNIX System Services shell script in the adapter_readonly_bin directory |
| Default certificate and key | Certificates must be created and installed manually. See “Configuring SSL authentication for the adapter” in the “IBM Security Identity Manager Adapter Installation Guide”. |
| Data set size adjustment | Temporary data set sizes in reconciliation must be adjusted according to the size of the RACF database unload for your installation. If the VSAM group file is utilized, its size must be adjusted, following an initial reconciliation. |

| | |
|---|---|
| VSAM file name for scoped reconciliation | A VSAM file is required to do scoped reconciliation (job ISIMVSAM). You can name the VSAM file to correspond to an adapter instance name. If scoped reconciliation is NOT performed, a VSAM file is not required, and the reconciliation transaction does not require program steps that execute ISIMGSCP. Also, a GROUP DD statement is not required for the ISIMREC2 program step. |
| Started task name | The ISIAGNT member is the sample JCL provided for the adapter startup. The component of the started task name must be indicative of the adapter instance name. The started task name must be limited to 7 characters to eliminate ambiguity when shutting down the adapter. |
| Adapter port number | The TCP/IP port number that the adapter uses. Enter this number when you configure the UNIX System Services component. Each adapter instance must have a unique TCP/IP port number. If two adapters use the same port number, only one of the adapters can be active at any one time. |
| TSO account number | A TSO account number might be required during installation because the adapter uses TSO/E for processing. |

**Note:** The screens displayed in the tasks topics are examples. Information in the actual screens might be different.

## Uploading the adapter package

You must upload the adapter package to the operating system.

**Before you begin**

Obtain the installation software.. For more information, see Software Downloads.

**About this task**

Use the following values for the referred files:

| *Table 2: Files used* | |
|---|---|
| **File description** | **File name** |
| XMI file | `ISIMRACF.UPLOAD.XMI` |
| Partitioned Data Set (PDS) file | *`userid`*`.ISIMRACF.UPLOAD` |

The *userid* is your TSO user ID.

**Procedure**

1. Extract the installation package on your local workstation. Ensure that the `.XMI` file exists. The file is in the z/OS operating system Time Sharing Option (TSO) TRANSMIT/RECEIVE format.
2. On the z/OS operating system, use the TSO to allocate a sequential `.XMI` file with the following parameters:
   - RECFM=FB
   - LRECL=80

- 400 MB of space

3. Upload the extracted `.XMI` file with a Binary transfer method, such as FTP or 3270 file transfer from the ISPF Command Shell.
   For example:

```
IND$FILE PUT 'ISIMRACF.UPLOAD.XMI' RECFM(F)
```

4. Receive the uploaded file with the TSO RECEIVE command:

```
RECEIVE INDA(ISIMRACF.UPLOAD.XMI)
```

5. Press **Enter** to create a Partitioned Data Set (PDS) file.

**Related concepts**

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

Communication configuration
To establish communication between the IBM Security Identity server and the adapter, import the adapter profile and create an adapter service.

**Related tasks**

Installing the ISPF dialog
Install the ISPF dialog

Running the ISPF dialog
Run the ISPF dialog to customize the adapter for run time execution.

Restarting the adapter service
Various installation and configuration task might require the adapter to be restarted to apply the changes.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

## Installing the ISPF dialog

Install the ISPF dialog

**Before you begin**

**Note:** The ISPF dialog requires a model 3 or model 4 3270 display.

**About this task**

The *userid* is your TSO user ID.

**Procedure**

1. Log on to the z/OS operating system that hosts the adapter.
2. Run the following command from the ISPF 6 option

```
INSTALL1 EXEC 'userid.ISIMRACF.UPLOAD(INSTALL1)'
```

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

**Results**

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

| *Table 3: ISPF dialog data sets* | |
|---|---|
| **High-level qualifier** | **Library** |
| hlq.SAGRCENU | CLIST/EXEC library |
| hlq.SAGRMENU | ISPF message library |
| hlq.SAGRPENU | ISPF panel library |
| hlq.SAGRSENU | ISPF skeleton library |

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

**Related concepts**

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

Communication configuration
To establish communication between the IBM Security Identity server and the adapter, import the adapter profile and create an adapter service.

**Related tasks**

Uploading the adapter package
You must upload the adapter package to the operating system.

Running the ISPF dialog
Run the ISPF dialog to customize the adapter for run time execution.

Restarting the adapter service
Various installation and configuration task might require the adapter to be restarted to apply the changes.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

## Running the ISPF dialog

Run the ISPF dialog to customize the adapter for run time execution.

**Before you begin**

Install the ISPF dialog.

**About this task**

The dialog presents the default values for the parameters. However, you can set your own values.

The ISPF dialog creates the Job Control Language (JCL) job streams with the installation parameters that you selected. The JCL job streams are required for adapter installation.

**Procedure**

1. Log on to the TSO on the z/OS operating system that hosts the adapter.
2. Run the following command from the ISPF 6 option

   ```
   EXEC 'hlq.SAGRCENU(AGRCCFG)'
   ```

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

```
-------------------Customization --------------------
Option ===>                                    Location:  1

Security Identity Adapter for RACF

  Initial Customization

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

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

    X  Exit
```

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

- You can return to the previous menu at any time by pressing **F3** or **END** on the **Menu** selection screen.
- If you press **F3** on a data entry screen, the values that you entered are not saved.
- When you fill the data entry screen and if it is validated without errors, the software returns to the previous screen.

3. Type 1 to select **Initial Customization**.

   The **Initial Customization** page lists the high-level tasks that you must perform.

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

   Initial Installation

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

     2  Display / Define / Alter Variables.
        Select or change specifications for this adapter instance.

     3  Generate Job Streams.
        You must have done choices 1 and 2 before doing
        this choice.

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

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

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

```
------------------- Customization -------------------------
 Option ===>                                   Location:  1->1-> 1

  Load Variables

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

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

     ===>
```

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

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

  Specify or Alter variables for this configuration.

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

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

     3 ** RACF reconciliation settings
          Define / alter RACF specific adapter runtime parameters.

     4 ** RACF reconciliation settings - storage
          Define / alter storage allocation settings.

     5 ** ISIMEXIT attribute parameters
          Select attributes for ISIMEXIT.

       ** Indicates option has been visited during this session.

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

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

```
------------------- Customization ----------------------
 Option ===>                             Location:  1->2-> 1

   Input Data Sets

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

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

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

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

    Storage Class       ===>      YYYYYYYY
      and/or
    Management Class    ===>      ZZZZZZZZ
      and/or

    Disk Volume ID      ===>      XXXXXXXX

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

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

    Default Language Environment dump (CEEDUMP) location
     ===> /tmp
```

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

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

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

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

**Management Class**
Specifies the management class for the LOAD and EXEC libraries.

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

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

**Default Language Environment dump (CEEDUMP) location**
Specifies the default UNIX system services location where the CEEDUMP dump files can be written to. This default location must be an existing directory in the UNIX file system.

8. Press **PF3** (Cancel) or **Enter** after final input (Accept) to return to the **Specify or Alter variables for this configuration** panel.
9. Select **Adapter specific parameters** to define or alter the IBM Security Identity Governance and Intelligence or adapter run time parameters.

```
------------------- Customization -----------------------
 Option ===>                                Location:  1->2-> 2


 Adapter specific parameters

    Name of adapter instance                      ===> RACFAGENT

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

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

        Enable SSL                                ===> TRUE (True, False)
Note: You must install a certificate when SSL is enabled. For more information, see the
 Identity Adapters documentation.

    Adapter authentication ID (internal)          ===> agent

    Adapter authentication password (internal)    ===> agent

    DEBUG mode                                    ===> TRUE (True, False)

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

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

    RACF user ID for the ISIA for RACF            ===> ITIAGNT

    z/OS Unix group for the ISIA for RACF         ===> OMVS

    z/OS Unix UID to be assigned to RACF ID        ===> 999

    TSO Account Number to be assigned to RACF ID  ===> ACCT#

    Delete data set profiles before deleting user accounts ===> FALSE
```

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

**Name of the Started Task JCL procedure name**
Specifies the name of the JCL member that is created.

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

**Enable SSL**
Controls the USE_SSL registry setting. Its default value is TRUE. You must install a certificate when SSL is enabled. For more information, see “Configuring SSL authentication” on page 86.

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

**DEBUG mode**
Sets the debug mode on and off. By default, the debug mode is set to TRUE.

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

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

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

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

**RACF Adapter z/OS UNIX group for the ISIM adapter**
Specifies a z/OS UNIX GROUP with a GID. A GID is a UNIX `Group ID`, which is a unique number that is assigned to a UNIX group name. The adapter operates as a z/OS UNIX process and requires this information.

**z/OS UNIX UID to be assigned to RACF Adapter ID**
Specifies a UID number for the RACF Adapter user ID.

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

**Delete data set profiles before deleting user accounts?**
A configuration option to delete data set profiles for an account, when set to TRUE, enables the adapter to delete data set profiles for an account, for which a delete operation request is received. This configuration option determines the PROFDEL registry value. The default value of PROFDEL is FALSE.

10. Press **PF3** (Cancel) or **Enter** after final input (Accept) to return to the **Specify or Alter variables for this configuration** panel.
11. Select RACF reconciliation and operations to specify RACF specific options.

```
------------------- ISIA RACF Adapter Customization -------------------
 Option ===>                                          Location:  1->2-> 3


 RACF Environment
Is the adapter to run data base unload? ===> TRUE (True or False)

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

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

Max wait time in seconds for RECOJOB to complete   ===> 60

Optional JOBCHAR to be used for RECOJOB            ===> R

PDU backlog limit                                  ===> 2000
```

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

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

**JOBCHAR**
Optional. Specifies the character to be added to the RECOJOB jobname when submitted.

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

12. Press **PF3** (Cancel) or **Enter** after final input (Accept) to return to the **Specify or Alter variables for this configuration** panel.
13. Select RACF reconciliation and operations to specify RACF specific options.

```
AGRP124 --------------- ISIA for RACF Customization ------------------
Option ===>

RACF reconciliation -  storage

   Storage Class for reconciliation related datasets
     ===> YYYYYYYY
   and/or
   Management Class for reconciliation related datasets
     ===>
   and/or
   Disk Volume ID       ===>    XXXXXXXX

   Temporary reconciliation data set name
    ===> IBMUSER.RECON.SAVE

   Temporary single account lookup data set name
    ===> IBMUSER.LOOKUP.SAVE

   Scoped reconciliation VSAM data set (leave blank for unscoped)
    ===> IBMUSER.ISIMRACF.GROUPS
```

**Storage Class**
Specifies the storage class for the temporary reconciliation result data set.

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

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

**Temporary reconciliation data set name**
Specifies the data set name used to store intermediate reconciliation results. The adapter user should be allowed to read, write, modify and delete this data set.

**Temporary single account data set name**
Specifies the data set name used to store intermediate single account LOOKUP results. The adapter user should be allowed to read, write, modify, and delete this data set.

**Note:**

The current release supports scheduling RECOJOB outside of the adapters control and implementation.

The adapter can now be configured to read directly from a predefined RECOSAVE data set that has been created by a process or operation that has previously run RECOJOB. To enable this

feature a distinction had to be made between the data set that is used to collect and process the output for a full reconciliation and the data set that is used to collect and process the output of a single account lookup op- eration.

The installation panels have been updated to allow you to define the data set that is to be used for reconciliation operations and for lookup operations. The same data set can be used for both operations if the adapter is configured to run RECOJOB. If the adapter is NOT configured to run RECOJOB , the data set that is used to process REC- ONCILIATION data can NOT be the same as the data set that is used for LOOKUP operations.

Scoped reconciliation VSAM data set (blank if scoped reconciliation is not required)

Specifies the VSAM data set name that is required for the scoped reconciliation process. The reconcilia- tion transaction uses the VSAM data set. If you do not want to do the scoped reconciliation, do not specify the VSAM data set name. The RACF Adapter ID specified on the service form or the default RACF Adapter ID configured for the adapter must have UPDATE access to the Scoped reconciliation VSAM data set.

**Note:** You must check the VSAM data set size after the reconciliation process. If no scoped reconciliation VSAM data set is defined during the installation process, then the attribute SCOPING=FALSE is set in the registry. If scoped reconciliation is required in the future, then you must use the installation panels to regenerate J4, J6 and RECOJOB and the Jx jobs must be submitted.

14. Press **PF3** (Cancel) or **Enter** after final input (Accept) to return to the **Specify or Alter variables for this configuration** panel.
15. Select 5- ISIMEXIT attribute parameters.

```
AGRP125 --------------- ISIA for RACF Customization -----------------------
Option ===>

ISIMEXIT attribute selection.

   Enable connect groups      ===> FALSE

   Do you want to use tsocmd? ===> TRUE
```

**Enable connect groups**

To enable forwarding the operation that is performed for a connect group and the name of the connect group for which the operation is being performed to ISIMEXIT, type TRUE.

If, during an account MODIFY operation, a CONNECT or REMOVE to/from a connect group is performed for an account the following information is passed on to ISIMEXIT when TRUE is selected; `MODIFY USER <BEFORE/AFTER> <USERID> <TRANSACTIONID> <CONNECT/ REMOVE> <CON- NECTGROUP>`

In the event the MODIFY BEFORE command returns a non-zero return code to the adapter, processing will stop for the connect group that was currently being modified and the connect group is returned in the list of unmodified attributes to the Identity server.

In the event the MODIFY AFTER command returns a non-zero return code to the adapter, processing will continue for the connect group that was currently being modified and a WARNING will be reported to the Identity server for the current transaction.

To disable forwarding the operation that is being performed for a connect group and the name of the con- nect group for which the operation is being performed to ISIMEXIT, type FALSE.

The selections made in this panel define the value that will be set for the non-encrypted registry attribute CONGRP.

The agentCfg tool can be used to modify the value of the CONGRP attribute after the adapter has been in- stalled and has been activated. This setting does not require a restart of the adapter to be activated.

Refer to the adapter guide for details on setting non-encrypted registry settings using the agentCfg tool.

**Do you want to use tsocmd?**
Using tsocmd to call ISIMEXIT enables you to execute authorized TSO/E commands from ISIMEXIT. Using IRXEXEC offers a better performance compared to toscmd, but does not enable you to execute authorized TSO/E commands. Specify TRUE to use tsocmd or FALSE to use IRXEXEC.

16. Press **PF3** (Cancel) or **Enter** after final input (Accept) to return to the **Specify or Alter variables for this configuration** panel.
17. Press **PF3** to return to the Initial Installation Panel.
18. Select **Generate Job Streams**.

    This screen displays the default data set names that are generated to store the job streams and data. You might change the default names on this screen based on the requirements of your organization. These data sets are not used at the adapter run time.

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

 Generate the job streams

    Specify two fully qualified data set names. These data sets will
    be populated with the job streams and their input data elements.


    Specify the data set names, without quotes. If these data sets
    do not exist, they will be created.

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

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

    Enter your installation job statement parameters here:

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

19. Specify valid parameters for installation JCL JOB statement and press **Enter** to create the JCL and data members. Control returns to the **Initial Installation** panel.
20. Select **Save All Variables** to save all the changes that you made to the data set.

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

```
------------------- Customization -------------------
 Option ===>

  Save variables to a data set.

    Specify the data set where the variables specified in this session
      are to be saved. Specify a fully qualified data set name,
      without quotes.

    If the data set does not exist, a sequential data set will be
      created.

    ===> IBMUSER.ISIM.CONFIG
```

21. Select **View instructions for job execution and further tailoring**.

    To view the adapter settings and the instructions to run the generated job streams, see the `hlq.ISIMRACF.CNTL(INSTRUCT)` data set. Follow the instructions specified in the `hlq.ISIMRACF.CNTL(INSTRUCT)` data set to complete the configuration.

### Results

The adapter is configured in a non-secure mode.

To configure the adapter in a secure mode, see “Configuring SSL authentication” on page 86.

**Related concepts**

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

Communication configuration
To establish communication between the IBM Security Identity server and the adapter, import the adapter profile and create an adapter service.

**Related tasks**

Uploading the adapter package
You must upload the adapter package to the operating system.

Installing the ISPF dialog
Install the ISPF dialog

Restarting the adapter service
Various installation and configuration task might require the adapter to be restarted to apply the changes.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

## Restarting the adapter service

Various installation and configuration task might require the adapter to be restarted to apply the changes.

**Before you begin**

Start the adapter as a started task, where the started task JCL is customized and installed in a system procedure library.

**About this task**

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

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

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

**Note:** You can define _BPX_SHAREAS=YES in the `/etc/profile`. This setting enables the adapter to run in a single address space, instead of multiple address spaces. Newer releases of z/OS create two address spaces with this environment variable set. See “z/OS UNIX System Services considerations” on page 102.

**Procedure**

1. To start the adapter, run the MVS console start command:

   ```
   START ISIAGNT
   ```

2. To stop the adapter, perform one of the following steps:
   - If the UNIX System Services environment is running with _BPX_SHAREAS=YES, then run one of the following stop commands:

     ```
     STOP ISIAGNT
     ```

     or

     ```
     P ISIAGNT
     ```

- If the UNIX System Services environment is running with the _BPX_SHAREAS=YES setting in a newer release of z/OS, run the following command:

```
P ISIAGNT1
```

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

```
CANCEL ISIAGNT
```

**Related concepts**

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

Communication configuration
To establish communication between the IBM Security Identity server and the adapter, import the adapter profile and create an adapter service.

**Related tasks**

Uploading the adapter package
You must upload the adapter package to the operating system.

Installing the ISPF dialog
Install the ISPF dialog

Running the ISPF dialog
Run the ISPF dialog to customize the adapter for run time execution.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

## Access configuration

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

**Related concepts**

Communication configuration
To establish communication between the IBM Security Identity server and the adapter, import the adapter profile and create an adapter service.

**Related tasks**

Uploading the adapter package
You must upload the adapter package to the operating system.

Installing the ISPF dialog
Install the ISPF dialog

Running the ISPF dialog
Run the ISPF dialog to customize the adapter for run time execution.

Restarting the adapter service
Various installation and configuration task might require the adapter to be restarted to apply the changes.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

### RACF user ID

The adapter must run under a valid RACF user ID, with an OMVS segment, a valid UID, and a valid TSO account number. This user's default group must have an OMVS segment with a valid GID. The adapter

RACF user ID must have READ permit on BPX.SERVER in class FACILITY. If the SURROGAT User ID is being used, the adapter must have UPDATE permit on BPX.SERVER in class FACILITY.

The name of the adapter instance must match the name of the started task user.

If you're using shared OMVS user IDs you should make sure the that the output for the following command is never empty if the adapter is running: ` ps -ef | grep -i <ADAPTERID> | grep -v grep` .

The R_admin callable service requires READ permission to be defined for the ADAPTER user and/or SURROGAT user on the following profiles in class FACILITY:

- IRR.RADMIN.ADDUSER
- IRR.RADMIN.ALTUSER
- IRR.RADMIN.CONNECT
- IRR.RADMIN.DELDSD
- IRR.RADMIN.DELUSER
- IRR.RADMIN.EXTRACT
- IRR.RADMIN.LISTUSER
- IRR.RADMIN.PASSWORD
- IRR.RADMIN.REMOVE
- IRR.RADMIN.RESUME
- IRR.RADMIN.REVOKE
- IRR.RADMIN.SEARCH

**Related concepts**

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

Authorization to set and reset passwords
When the adapter RACF user ID, or the surrogates do not have **SYSTEM SPECIAL**, they must be able to set passwords and pass phrases over those users they manage.

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

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

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

Configuration option to delete data set profiles
A configuration option to delete data set profiles for an account is now supported.

## Surrogate user ID

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

Surrogate user IDs are necessary only when:

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

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

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

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

```
RDEFINE SURROGAT BPX.SRV.UNIT1
SETROPTS REFRESH RACLIST(SURROGAT)
PERMIT BPX.SRV.UNIT1 CLASS(SURROGAT) ID(ISIAGNT) ACCESS(READ)
SETROPTS REFRESH RACLIST(SURROGAT)
```

In the preceding example, the RACF user ID UNIT1 is the user ID defined in the adapter service form. This RACF user has scope of authority over a specific business unit.

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

**Related concepts**

RACF user ID
The adapter must run under a valid RACF user ID, with an OMVS segment, a valid UID, and a valid TSO account number. This user's default group must have an OMVS segment with a valid GID. The adapter RACF user ID must have READ permit on BPX.SERVER in class FACILITY. If the SURROGAT User ID is being used, the adapter must have UPDATE permit on BPX.SERVER in class FACILITY.

Authorization to set and reset passwords
When the adapter RACF user ID, or the surrogates do not have **SYSTEM SPECIAL**, they must be able to set passwords and pass phrases over those users they manage.

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

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

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

Configuration option to delete data set profiles
A configuration option to delete data set profiles for an account is now supported.

## Authorization to set and reset passwords

When the adapter RACF user ID, or the surrogates do not have **SYSTEM SPECIAL**, they must be able to set passwords and pass phrases over those users they manage.

This task is accomplished through the **FACILITY** class profile named `IRR.PASSWORD.RESET`.

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

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

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

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

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

**z/OS V2R3 specific requirements**

RACF password change for users with KERB segments and REALM class profiles require the Integrated Cryptographic Service Facility (ICSF) to be available. For more information about ICSF, see https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.csfb200/toc.htm. If CSFSERV class profiles are defined, the adapter ID might require permission to the defined CSFSERV class profiles. ICSF must be started and initialized prior to performing either or both of the following activities.

- Changing the password for a user that has a KERB segment.
- Creating or changing a password for a REALM class profile.

If the CSFSERV class is active and protection profile for the CSFOWH resource that is used by the CSFBOWH function exists, read access for the adapter ID is required to the CSFOWH resource.

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

**Related concepts**

RACF user ID
The adapter must run under a valid RACF user ID, with an OMVS segment, a valid UID, and a valid TSO account number. This user's default group must have an OMVS segment with a valid GID. The adapter RACF user ID must have READ permit on BPX.SERVER in class FACILITY. If the SURROGAT User ID is being used, the adapter must have UPDATE permit on BPX.SERVER in class FACILITY.

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

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

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

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

Configuration option to delete data set profiles
A configuration option to delete data set profiles for an account is now supported.

## AUTOID support

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

Use this command to define the profile:

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

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

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

**Related concepts**

RACF user ID
The adapter must run under a valid RACF user ID, with an OMVS segment, a valid UID, and a valid TSO account number. This user's default group must have an OMVS segment with a valid GID. The adapter RACF user ID must have READ permit on BPX.SERVER in class FACILITY. If the SURROGAT User ID is being used, the adapter must have UPDATE permit on BPX.SERVER in class FACILITY.

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

Authorization to set and reset passwords
When the adapter RACF user ID, or the surrogates do not have **SYSTEM SPECIAL**, they must be able to set passwords and pass phrases over those users they manage.

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

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

Configuration option to delete data set profiles
A configuration option to delete data set profiles for an account is now supported.

## Shared UID support

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

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

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

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

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

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

**Related concepts**

RACF user ID
The adapter must run under a valid RACF user ID, with an OMVS segment, a valid UID, and a valid TSO account number. This user's default group must have an OMVS segment with a valid GID. The adapter RACF user ID must have READ permit on BPX.SERVER in class FACILITY. If the SURROGAT User ID is being used, the adapter must have UPDATE permit on BPX.SERVER in class FACILITY.

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

Authorization to set and reset passwords
When the adapter RACF user ID, or the surrogates do not have **SYSTEM SPECIAL**, they must be able to set passwords and pass phrases over those users they manage.

AUTOID support

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

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

Configuration option to delete data set profiles
A configuration option to delete data set profiles for an account is now supported.

## Password phrases

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

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

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

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

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

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

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

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

Where the PASSWORD value is the password value that is specified on the IBM Security Identity server.

Pass phrase changes generate two commands. The commands that are generated for changing a pass phrase adhere to the following format:

```
ALU <USERID> PHRASE(?) NOEXPIRED
ALU <USERID> PASSWORD(?) EXPIRED
```

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

```
AdkError: racfModify: Invalid PHRASE specified
```

**Related concepts**

RACF user ID
The adapter must run under a valid RACF user ID, with an OMVS segment, a valid UID, and a valid TSO account number. This user's default group must have an OMVS segment with a valid GID. The adapter RACF user ID must have READ permit on BPX.SERVER in class FACILITY. If the SURROGAT User ID is being used, the adapter must have UPDATE permit on BPX.SERVER in class FACILITY.

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

Authorization to set and reset passwords
When the adapter RACF user ID, or the surrogates do not have **SYSTEM SPECIAL**, they must be able to set passwords and pass phrases over those users they manage.

AUTOID support

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

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

Configuration option to delete data set profiles
A configuration option to delete data set profiles for an account is now supported.

### Configuration option to delete data set profiles

A configuration option to delete data set profiles for an account is now supported.

When a configuration option to delete the data set profiles for an account is set to TRUE, it enables the adapter to delete the data set profiles for an account, for which a delete operation request is received.

When this configuration option to delete the date set profiles is enabled, the adapter RACF user ID, Surrogate user ID, or both must have READ permission on `IRR.RADMIN.DELDSD` in the class `FACILITY`.

**Related concepts**

RACF user ID
The adapter must run under a valid RACF user ID, with an OMVS segment, a valid UID, and a valid TSO account number. This user's default group must have an OMVS segment with a valid GID. The adapter RACF user ID must have READ permit on BPX.SERVER in class FACILITY. If the SURROGAT User ID is being used, the adapter must have UPDATE permit on BPX.SERVER in class FACILITY.

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

Authorization to set and reset passwords
When the adapter RACF user ID, or the surrogates do not have **SYSTEM SPECIAL**, they must be able to set passwords and pass phrases over those users they manage.

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

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

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

## Communication configuration

To establish communication between the IBM Security Identity server and the adapter, import the adapter profile and create an adapter service.

**Related concepts**

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

**Related tasks**

Uploading the adapter package
You must upload the adapter package to the operating system.

Installing the ISPF dialog

Install the ISPF dialog

Running the ISPF dialog
Run the ISPF dialog to customize the adapter for run time execution.

Restarting the adapter service
Various installation and configuration task might require the adapter to be restarted to apply the changes.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

## Importing the adapter profile

You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

### Before you begin

- The IBM Security Identity Governance and Intelligence server is installed and running.
- You have administrator authority on the IBM Security Identity Governance and Intelligence server.
- The file to be imported must be a Java archive (JAR) file. The `<Adapter>Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.

### About this task

Target definition files are also called adapter profile files. The profile definition files are provided with the various IBM Security Identity Adapter. The adapter profile must be imported because it defines the types of resources that the Identity Governance and Intelligence server can manage.

The adapter profile definition file is used to create a target profile on the Identity Governance and Intelligence server and to establish communication with the adapter. If the adapter profile is not imported, you cannot create a connector for that adapter type.

An upload error might occur when no file is selected, or when the file is empty, or due to any upload operation error, such as a timeout or connection error. If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a connector with the adapter profile or open and account on the service. You must import the adapter profile again.

This task can be completed from the Enterprise Connectors module in the Administration Console. To import an adapter target profile, complete these steps:

### Procedure

1. Log in to the Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Profile**.
   b) Click **Browse** to locate the JAR file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported a profile.
7. Click **Close**.
   The new profile is displayed in the list of profiles.

### Results

The upload is synchronous but has a timeout. The progress bar on the **Import** page accurately indicates the upload status. However, when a timeout is reached, the following message occurs: "The import is still in progress and will complete shortly. Close this window to proceed." If you see that message, allow a few minutes for the upload to complete and for the profile to be available.

### What to do next

After the target profile is imported successfully, complete these tasks.

- Import the attribute mapping file. See "Importing attribute mapping file" on page 31.
- Create a connector that uses the target profile. See "Adding a connector" on page 31.

## Importing attribute mapping file

After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

### About this task

This task involves importing an account attribute mapping definition file, which is included in the adapter package. The imported file must be a DEF file.

### Procedure

1. Log in to the Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Attribute Mapping**.
   b) Click **Browse** to locate the attribute mapping file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported the file.
7. Click **Close**.

## Adding a connector

After you import the adapter profile on the Identity Governance and Intelligence server, add a connector so that Identity Governance and Intelligence server can communicate with the managed resource.

### Before you begin

Complete "Importing the adapter profile" on page 30.

**Note:** If you migrated from Identity Governance and Intelligence V5.2.2 or V5.2.2.1 and want to add or configure a connector, see *Adding and configuring a connector for each target* in the IBM Security Identity Governance and Intelligence product documentation.

### About this task

The connectors consolidate, extract, and reconcile user identities, organization units, permissions, and user entitlements with the most common enterprise applications. Configure a connector to keep the Access Governance Core repository synchronized with the target system.

This task can be completed from the Enterprise Connectors module in the Administration Console.

### Procedure

To add a connector, complete these steps.

1. Log in to the Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.
   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:
   a) Assign a name and description for the connector.
   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.
   c) Select the entity, such as **Account** or **User**.
      Depending on the connector type, this field might be preselected.
   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.
      The available trace levels are DEBUG, INFO, and ERROR.
   e) Optional: Select **History ON** to save and track the connector usage.
   f) Click **Save**.
      The fields for enabling the channels for sending and receiving data are now visible.
   g) Select and set the connector properties in the **Global Config** accordion pane.
      For information about the global configuration properties, see Global Config accordion pane.
   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

### Results

The connector is saved and added to the list of connectors in the **Connectors** pane.

If you cannot create a connector with the target profile or open an account on an existing connector, the target profile was not installed correctly during the import. You must import the target profile again.

### What to do next

Enable the channel modes to synchronize the data between the target systems and Identity Governance and Intelligence. For more information, see “Enabling connectors” on page 32.

## Enabling connectors

After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

### Before you begin

*Table 4: Prerequisites for enabling a connector*

| Prerequisite | Find more information |
|---|---|
| A connector must exist in Identity Governance and Intelligence. | “Adding a connector” on page 31. |
| Ensure that you enabled the appropriate channel modes for the connector. | “Reviewing and setting channel modes for each new connector” on page 33. |

### Procedure

To enable a connector, complete these steps:

1. Log in to the Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

   **Enable write-to channel**
   Propagates every change in the Access Governance Core repository into the target system.

   For connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

   **Enable read-from channel**
   Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

   For HR feed connectors, only the check box for enabling the read-from channel is available.

   **Enable reconciliation**
   Synchronizes the modified data between the Access Governance Core repository and the target system.

### Results

The connector is enabled

### What to do next

Enable the channel modes to synchronize the data between the target systems and Identity Governance and Intelligence.

## Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

### About this task

**Note:** Legacy Identity Governance and Intelligence Enterprise connectors use `Reconciliation` channel, whereas Identity Brokerage Enterprise connectors use `Read From Channel` and `Change Log Sync`.

For more information about any of tasks in the following steps, see the IBM® Security Identity Governance and Intelligence product documentation.

### Procedure

To enable the read-from and write-to channels, and to set the change log synchronization schedule for each new connector, complete these steps in Identity Governance and Intelligence V5.2.3:

1. Log in to the Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.

3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

      **Enable write-to channel**
      Propagates every change in the Access Governance Core repository into the target system.

      **Enable read-from channel**
      Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

      **Enable reconciliation**
      Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.
   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
   b) Select a connector, and click **Actions** > **Sync Now**.
      The synchronization process begins.
   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane. Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:
    a) Select **Manage** > **Connectors**.
    b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
    c) Click **Save**.

       For more information, see “Enabling connectors” on page 32.

       For Identity Brokerage connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

       For Identity Brokerage HR feed connectors, only the check box for enabling the read-from channel is available.
12. Start the connector by selecting **Monitor** > **Connector Status**. Select the connector that you want to start, and then select **Actions** > **Start**.

## Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Identity Governance and Intelligence account attributes.

### About this task

This task involves an account attribute mapping definition file, which is included in the adapter package.

The file consists of Identity Governance and Intelligence account attributes and their equivalent attributes in the managed target. The file is structured as *<IGI_attribute> = <target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<target_attribute>* of `eraccount`.

Some *<IGI_attribute>* do not have a defined *<target_attribute>* and you can assign the mapping. For example:

```
USER_TYPE=USER_TYPE
ATTR1=ATTR1
```

**Note:**

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

**Procedure**

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Identity Governance and Intelligence attribute values.

   ```
   [conversion].<target_attribute>.<IGI_attribute> =
   [<target_attribute_value1>=<IGI_attribute_value1>;...;
   <target_attribute_valuen>=<IGI_attribute_valuen>]
   ```

4. For attributes that contains date and time, use the following syntax to convert its values.
   For example:

   ```
   [conversion.date].erbirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]
   [conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=
   [dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]
   ```

5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Identity Governance and Intelligence product documentation.
6. Map the following attributes for **Chanel-Write To** and **Chanel-Read From**

| Attribute | Mapped Attribute |
|---|---|
| eruid | CODE |
| erpassword | PASSWORD |

   For more information, see *Mapping attributes for a connector* in the IBM Security Identity Governance and Intelligence product documentation.

## Service/Target form details

Complete the service/target form fields.

**On the General Information tab:**

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

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

**URL**
Specify the location and port number of the adapter. The port number is defined during installation, and can be viewed and modified in the protocol configuration by using the **agentCfg** utility. For more information about protocol configuration settings, see "Changing protocol configuration settings" on page 51.

**Note:** Configure the adapter for SSL authentication only if **https** is part of the URL. For more information, see "Configuring SSL authentication" on page 86.

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

**Password**
Specify the password that you defined at installation for the `Adapter authentication ID`. The default value is `agent`.

**RACF ID under which requests will be processed**
Optional: Specify a SURROGAT ID. This loginid might have administrative authority over a subset of logonids within the RACF database.

**Owner**
Optional: Specify the service owner, if any

**Service Prerequisite**
Optional: Specify an existing service.

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

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

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

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

**Adapter version**
Specifies the version of the adapter that the service uses to provision request to the managed resource.

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

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

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

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

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

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

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

If the connection fails, follow the instructions in the error message and do the following verifications:

- Verify the adapter log to ensure that the test request is successfully sent to the adapter.

- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. For example, verify the workstation name or the IP address of the managed resource and the port.

## Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

**Procedure**

1. Test the connection for the service that you created on the IBM Security Identity Governance and Intelligence server.
2. Run a full reconciliation from the IBM Security Identity Governance and Intelligence server.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

**Related concepts**

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

Communication configuration
To establish communication between the IBM Security Identity server and the adapter, import the adapter profile and create an adapter service.

**Related tasks**

Uploading the adapter package
You must upload the adapter package to the operating system.

Installing the ISPF dialog
Install the ISPF dialog

Running the ISPF dialog
Run the ISPF dialog to customize the adapter for run time execution.

Restarting the adapter service
Various installation and configuration task might require the adapter to be restarted to apply the changes.

# Chapter 4. Upgrading

Upgrading the adapter requires a full installation.

**About this task**

When upgrading from an adapter profile that is specified with `erracconxml` as a binary attribute in the `schema.dsml` file, to a version that specifies `erracconxml` as a directory string as shown in the example below, it can be necessary to manually update V3.modifiedschema accordingly.

Example of a directory string format entry in the `schema.dsml`:

```
1.3.6.1.4.1.1466.115.121.1.15{2048}
```

When you are upgrading from an adapter profile that has `erracconxml` specified as a binary attribute to a version which has `erracconxml` specified as a directory string as shown in the example below, it can be necessary to manually update `V3.modifiedschema` accordingly.

```
<syntax>1.3.6.1.4.1.1466.115.121.1.15{2048}</syntax>
```

If after the update, the LDAP schema is not updated, follow the procedure described in this technote Operations error on add or modify operations to troubleshoot the issue.

If the problem persists, contact IBM Support and upload a dynamic trace when you reproduce the issue. See Collecting a dynamic ascii server trace.

# Chapter 5. Configuring

After you install the adapter, configure it to function correctly. Configuration is based on your requirements or preference.

You can use the adapter configuration tool, **agentCfg**, to view or modify the adapter parameters. You can also do this from a remote workstation.

## Configuring the adapter parameters

You can use the adapter configuration tool, **agentCfg**, to view or modify the adapter parameters. You can also do this from a remote workstation.

All the changes that you make to the parameters, by using the **agentCfg**, take effect immediately. For more information, see *Arguments and description for the agentCfg help menu* in "Accessing help and additional options" on page 83.

**Note:** The screens displayed in the tasks topics are examples. Information in the actual screens might be different.

### Supporting custom fields with extended attributes

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

#### About this task

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

#### Procedure

1. Define the custom fields and extended attributes mappings to the RACF adapter. Use the IBM Security Identity Governance and Intelligence RACF adapter ISPF dialog to complete this step. For more information, see "Mapping the custom fields to the extended attributes by using the ISPF dialog" on page 42.
2. Copy the JAR file to a temporary directory and extract the files. For more information, see "Extracting files from the RACFProfile.jar file" on page 46.
3. Update the `schema.dsml` file. For more information, see "Updating the schema.dsml file" on page 47.
4. Update the `erRacfAcct.xml` file. For more information, see "Updating the erRacfAcct.xml file" on page 46.
5. Update the `targetProfile.json` file
6. Install the new attributes on the IBM Security Identity Governance and Intelligence server. For more information, see "Installing the new attributes on the IBM Security Identity Manager" on page 48.

#### Related concepts

Configuring event notification

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

#### Related tasks

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

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

Starting the adapter configuration tool
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

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

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

### Before you begin

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

### About this task

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

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

**Procedure**

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

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

Security Identity Manager RACF Adapter

 Initial Customization

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

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

  X Exit
```

**Note:** When you run the dialog, take note of the following considerations:

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

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

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

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

 RACF custom field support

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

 USS Adapter read/write home
===>
 RACF z/OS Unix group for the ISIM adapter ===>

S  Field   Type   Max len   Attribute name   Comments
- -------- ---- ------- ------------------------- ------------------
  EMPFLAG  FLAG     003      erracempflag
  EMPHEX   HEX      0512       erracemphex
  EMPROOM  CHAR     080      erracemproom
  EMPSER   INT      008      erracempser
  INT01    INT      008      erracint01
```

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

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

**USS Adapter read/write home**

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

**RACF z/OS Unix group for the ISIM adapter**

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

**Attribute name**

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

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

```
------------------ ISIM RACF Adapter Customization -------------------
Option ===>
 RACF custom field support

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

 USS Adapter read/write home
  ===> /var/ibm/security/isimracf
 RACF z/OS Unix group for the ISIM adapter ===> OMVS

S  Field   Type   Max len   Attribute name   Comments
- -------- ---- ------- ------------------------- ------------------
S  EMPFLAG   FLAG    003         erracempflag      Defined in UDF.dat
S  EMPHEX    HEX     0512        erracemphex       Defined in UDF.dat
S  EMPROOM   CHAR    080         erracemproom      Defined in UDF.dat
S  EMPSER    INT     008         erracempser       Defined in UDF.dat
   INT01     INT     008         erracint01
```

You might see the following in the comments column:

**Invalid attribute name**

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

**Length discrepancy**

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

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

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

**Defined in UDF.dat**

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

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

   If you want to remove a field that is defined in the UDF.dat, remove the S from the selection column. You can page up and down if necessary. The selections are maintained. If you want to select all custom fields, type S* on the command line.
6. When you are finished selecting the custom fields, type SAVE on the command line. The UDF.dat file is saved with read and write permissions for the administrator and read permission for the group for the adapter specified.

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

**Results**

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

**Related concepts**

Configuring event notification

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

**Related tasks**

Supporting custom fields with extended attributes

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

Starting the adapter configuration tool

Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings

Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings

The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key

Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings

Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings

Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings

Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings

Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics

Use the **Statistics** option to view the event log of the adapter.

Changing code page settings

Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options

Access the **agentCfg** help menu to view the list of available arguments that you can use.

### Extracting files from the RACFProfile.jar file

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

#### About this task

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

- META-INF/
- META-INF/MANIFEST.MF
- racfprofile/
- racfprofile/erRacfAcct.xml
- racfprofile/erRacfGrp.xml
- racfprofile/erRacfSSLService.xml
- racfprofile/resource.def
- racfprofile/schema.dsml
- racfprofile/CustomLabels.properties
- racfprofile/targetProfile.json

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

#### Procedure

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

### Updating the erRacfAcct.xml file

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

#### About this task

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

#### Procedure

1. Edit the erRacfAcct.xml file to define where and how to display each extended attribute. Make sure that you put the definition in the correct spot. Each definition is displayed under the previous definition within the tabbed entry.
   For example:

```
<formElement direction="inherit" name="data.erracempflag" label="Employee Flag">
 <select style="width:100px" name="data.erracempflag" width="100">
  <option value=" "></option>
```

```
  <option value="TRUE">$erracftrue</option>
  <option value="FALSE">$erracffalse</option>
 </select>
</formElement>
```

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

**Updating the schema.dsml file**

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

**About this task**

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

**Procedure**

1. Edit the `schema.dsml` file to define each extended attribute.

   The attribute name must match the attribute name that is registered with the ISPF dialog. All attributes must be unique, and assigned a unique Object Identifier (OID).

   The instance ID (last dot delimited segment of the OID) for the extended attributes starts from 1000, so the OID for the first extended attribute is`<object-identifier>1.3.6.1.4.1.6054.3.127.2.1000</object-identifier>`.

   This numbering prevents duplicate OIDs if the adapter is upgraded to support new attributes. For subsequent extended attributes, the OID increments by 1, based on the last entry in the file. For example, if the last attribute in the file uses the OID `1.3.6.1.4.1.6054.3.127.2.1008`, the next new attribute uses the OID `1.3.6.1.4.1.6054.3.127.2.1009`. The data type is either:

   - A directory string and is defined by using the syntax tags:
     `<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>`

     This data type is used for RACF fields defined as FLAG, HEX and CHAR.
   - An integer and is defined by using the syntax tags:
     `<syntax>1.3.6.1.4.1.1466.115.121.1.27</syntax>`

     This data type is used for RACF fields defined as NUM.
2. Add the definition for each of the new attributes before the account class and then reference them in the account class.
   For example, add the following attribute definition before the `erRacfAcct` section of the `schema.dsml` file:

```
<!-- ******************************************************** -->
<!-- erRacEmpFlag -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
<name>erRacEmpFlag</name>
<description>Employee Flag</description>
<object-identifier>1.3.6.1.4.1.6054.3.127.2.1000</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
```

3. Add a reference for each of the new attributes in the account class.
   For example, add the following attribute reference in the `erRacfAcct` section of the `schema.dsml` file:

```
<attribute ref = "erRacEmpFlag" required = "false"/>
```

4. You can find samples of the RACF custom fields in the `schema.dsml` file. Search for `Sample` in the file. These samples are commented out.

5. Edit the `targetProfile.json` file to add new attributes that is defined in the `userExtension` schema.

**Installing the new attributes on the IBM Security Identity Manager**
After any file modification, import all files, including those files without updates, into the IBM Security Identity Governance and Intelligence server for the changes to take effect.

**About this task**

To install the new attributes, create a new JAR file that contains the updated files in the temporary directory.

**Procedure**

1. Change to the parent directory and then build a new JAR file.

   **Note:**

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

   For example, run the command `cd .. jar cf RACFProfileCustom.jar racfprofile`
2. Import the new JAR file into the IBM Security Identity Governance and Intelligence server.

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

## Starting the adapter configuration tool

Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

**Procedure**

1. Browse to the Windows Command Prompt.
2. Log on to the TSO on the z/OS operating system that hosts the adapter.
3. Run the following command. Press **Enter** to enter the UNIX System Services environment.

   ```
   omvs
   ```

   **Note:** You can also use a telnet session to enter the UNIX System Services environment.
4. In the command prompt, change to the read/write `/bin` subdirectory of the adapter.If the adapter is installed in the default location for the read/write directory, run the following command.
5. Run the following command

   ```
   agentCfg -agent adapter_home
   ```

   The adapter name is specified when you install the adapter. You can find the names of the active adapters by running the **agentCfg** utility as:

   ```
   agentCfg -list
   ```
6. At **Enter configuration key for Agent '*adapterAGNT*'**, type the configuration key for the adapter.

   The default configuration key is `agent`.

   **Note:** To prevent unauthorized access to the configuration of the adapter, you must modify the configuration key after the adapter installation completes..

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

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

X. Done

Select menu option:
```

The following table lists the different options available in the **Agent Main Configuration Menu**.

*Table 5: Options for the main configuration menu*

| Option | Configuration task |
|---|---|
| A | Viewing configuration settings |
| B | Changing protocol configuration settings |
| C | Configuring event notification |
| D | Changing the configuration key |
| E | Changing activity logging settings |
| F | Changing registry settings |
| G | Changing advanced settings |
| H | Viewing statistics |
| I | Changing code page settings |

**Related concepts**

Configuring event notification

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

**Related tasks**

Supporting custom fields with extended attributes

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

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

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

Viewing configuration settings

Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings

The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key

Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Viewing configuration settings

Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

### Procedure

1. Access the **Agent Main Configuration Menu**.
   For more information, see "Starting the adapter configuration tool" on page 48.
2. At the **Main menu** prompt, type A to display the configuration settings for the adapter.

```
Configuration Settings
----------------------------------------
Name            : adapterAGNT
Version         : 6.0
ADK Version     : 6.0
ERM Version     : 6.0
Adapter Events  : FALSE
License         : NONE
Asynchronous ADD Requests  : FALSE (Max.Threads:3)
Asynchronous MOD Requests  : FALSE (Max.Threads:3)
Asynchronous DEL Requests  : FALSE (Max.Threads:3)
Asynchronous SEA Requests  : FALSE (Max.Threads:3)
Available Protocols        : DAML
Configured Protocols       : DAML
Logging Enabled            : TRUE
Logging Directory          : /var/ibm/adapter_readwritedir/log
Log File Name              : adapter_name.log
Max. log files             : 3
Max.log file size (Mbytes) : 1
Debug Logging Enabled      : TRUE
Detail Logging Enabled     : FALSE
Thread Logging Enabled     : FALSE
```

### Related concepts

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

information from the managed resource. Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Changing protocol configuration settings

The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

### About this task

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

### Procedure

1. Access the **Agent Main Configuration Menu**.
   For more information, see "Starting the adapter configuration tool" on page 48.

2. At the **Main menu** prompt, type B. The DAML protocol is configured and available by default for the adapter.

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

X. Done

Select menu option
```

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

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

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

```
DAML Protocol Properties
------------------------------------------------------------------------
A. USERNAME             ****** ;Authorized user name.
B. PASSWORD             ****** ;Authorized user password.
C. MAX_CONNECTIONS      100    ;Max Connections.
D. PORTNUMBER           45580  ;Protocol Server port number.
E. USE_SSL              FALSE  ;Use SSL secure connection.
F. SRV_NODENAME         9.38.215.20 ;Event Notif. Server name.
G. SRV_PORTNUMBER       9443 ;Event Notif. Server port number.
H. HOSTADDR             ANY;Listen on address (or "ANY")
I. VALIDATE_CLIENT_CE   FALSE ;Require client certificate.
J. REQUIRE_CERT_REG     FALSE ;Require registered certificate.
K. READ_TIMEOUT         0 ;Socket read timeout (seconds)
L. DISABLE_TLS10        TRUE ;Disable TLS 1.0 and earlier

X. Done

Select menu option:
```

5. Change the protocol value:
   a) Type the letter of the menu option for the protocol property to configure. The table below describes each property.
   b) Change the property value and press **Enter** to display the **Protocol Properties Menu** with the new value.

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

*Table 6: Options for the DAML protocol menu*

| Option | Configuration task |
|---|---|
| A | Displays the following prompt:<br>`Modify Property 'USERNAME':`<br>Type a user ID, for example, `admin`.<br>The IBM Security Identity server uses this value to connect to the adapter. |

*Table 6: Options for the DAML protocol menu (continued)*

| Option | Configuration task |
|---|---|
| B | Displays the following prompt<br>`Modify Property 'PASSWORD':`<br>Type a password, for example, `admin`.<br>The IBM Security Identity server uses this value to connect to the adapter. |
| C | Displays the following prompt:<br>`Modify Property 'MAX_CONNECTIONS':`<br>Enter the maximum number of concurrent open connections that the adapter supports.<br>The default value is 100.<br>**Note:** This setting is sufficient and does not require adjustment. |
| D | Displays the following prompt:<br>`Modify Property 'PORTNUMBER':`<br>Type a different port number.<br>The IBM Security Identity server uses the port number to connect to the adapter. The default port number is 45580. |
| E | Displays the following prompt:<br>`Modify Property 'USE_SSL':`<br>Type TRUE to use a secure SSL connection to connect the adapter. When you set this option, you must install a certificate. For more information, see “Installing the certificate” on page 95.<br>Type FALSE to not use a secure SSL connection. The default value is TRUE. |
| F | Displays the following prompt:<br>`Modify Property 'SRV_NODENAME':`<br>Type a server name or an IP address of the workstation where you installed the IBM Security Identity server.<br>This value is the DNS name or the IP address of the IBM Security Identity server that is used for event notification and asynchronous request processing.<br>**Note:** If your operating system supports Internet Protocol version 6 (IPv6) connections, you can specify an IPv6 server. |
| G | Displays the following prompt:<br>`Modify Property 'SRV_PORTNUMBER':`<br>Type a different port number to access the IBM Security Identity server.<br>The adapter uses this port number to connect to the IBM Security Identity server. The default port number is 9443. |

| *Table 6: Options for the DAML protocol menu (continued)* | |
|---|---|
| **Option** | **Configuration task** |
| H | The HOSTADDR option is useful when the system, where the adapter is running, has more than one network adapter. You can select which IP address to which the adapter must listen. The default value is **ANY**. |
| I | Displays the following prompt:<br>`Modify Property 'VALIDATE_CLIENT_CE':`<br>Type TRUE for the IBM Security Identity server to send a certificate when it communicates with the adapter. When you set this option, you must configure options D through I.<br>Type FALSE for the IBM Security Identity server can communicate with the adapter without a certificate.<br>**Note:**<br>• The property name is **VALIDATE_CLIENT_CERT**. It is truncated by the **agentCfg** to fit in the screen.<br>• You must use certTool to install the appropriate CA certificates and optionally register the IBM Security Identity server certificate. |
| J | Displays the following prompt:<br>`Modify Property 'REQUIRE_CERT_REG':`<br>This value applies when option I is set to TRUE.<br>Type TRUE to register the adapter with the client certificate from the IBM Security Identity server before it accepts an SSL connection.<br>Type FALSE to verify the client certificate against the list of CA certificates. The default value is FALSE.<br>For more information about certificates, see “Configuring SSL authentication” on page 86. |
| K | Displays the following prompt:<br>`Modify Property 'READ_TIMEOUT':`<br>Specify the timeout value in seconds. The default value is 0 which specifies that no read timeout is set.<br>**Note: READ_TIMEOUT** prevents open threads in the adapter, which might cause "hang" problems. The open threads might be caused by firewall or network connection problems and might be seen as **TCP/IP ClosWait** connections that remain on the adapter.<br>**Note:**<br>If you encounter such problems, set the value of **READ_TIMEOUT** to a time longer than the IBM Security Identity server timeout, but less than any firewall timeout. The IBM Security Identity server timeout is specified by the **maximum connection age** DAML property.<br>The adapter must be restarted because READ_TIMEOUT is set at adapter initialization. |

| *Table 6: Options for the DAML protocol menu (continued)* | |
|---|---|
| **Option** | **Configuration task** |
| L | Displays the following prompt:<br>`Modify Property 'DISABLE_TLS10':`<br>Type FALSE to use the TLSv1.0 protocol to connect the adapter.<br>The default value is TRUE. |

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

**Related concepts**

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the IBM Security Identity server with the changes. You can enable event notification to obtain the updated information from the managed resource. Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool
Start the **`agentCfg`** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options

Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Configuring event notification

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

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

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

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

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings

Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

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

**Procedure**

1. Access the **Agent Main Configuration Menu**.
   See "Starting the adapter configuration tool" on page 48.
2. At the **Agent Protocol Configuration Menu**, select **Configure Protocol**.
   See "Changing protocol configuration settings" on page 51.
3. Change the USE_SSL property to TRUE.
4. Type the letter of the preferred menu option for the **SRV_PORTNUMBER** property.
5. Specify the IP address or server name that identifies the IBM Security Identity server.
6. Press **Enter** to display the **Protocol Properties Menu** with the new settings.
7. Type the letter of the preferred menu option for the **SRV_PORTNUMBER** property.
8. Specify the port number that the adapter uses to connect to the IBM Security Identity server for event notification.
9. Press **Enter** to display the **Protocol Properties Menu** with the new settings.
10. Install certificate by using the certTool.
    See "Starting the certTool utility" on page 92.

**Related tasks**
Setting event notification on the server
Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

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

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

**Setting event notification on the server**
Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**About this task**

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

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

**Procedure**

1. Access the **Agent Main Configuration Menu**.
   See "Starting the adapter configuration tool" on page 48.
2. Type C to display **Event Notification Menu**.

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

3. Type the letter of the preferred menu option

**Note:**

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

*Table 7: Options for the event notification menus*

| Option | Configuration task |
|---|---|
| A | If you select this option, the adapter updates the IBM Security Identity Manager server with changes to the adapter at regular intervals. If **Enabled - Adapter** is selected, the adapter code processes event notification by monitoring a change log on the managed resource.<br>When the option is set to:<br>**Disabled**<br>All options except **Start event notification now** and **Set attributes** that are to be reconciled are available. Pressing A changes the setting to **Enabled - ADK**.<br>**Enabled - ADK**<br>All options are available. Pressing A changes the setting to **Disabled** or if your adapter supports event notification, to **Enabled - Adapter**.<br>**Enabled - Adapter**<br>All options are available, except<br>**Time interval between reconciliations**<br>**Set processing cache size**<br>**Start event notification now**<br>**Reconciliation process priority**<br>**Set attributes to be reconciled**<br>Pressing A changes the setting to **Disabled**.<br>Type A to toggle between the options.<br>**Note:** The adapter does not support adapter-based event notification, **Enabled - Adapter**. Therefore, this option is not listed in the event notification menu. |
| B | Displays the following prompt:<br>`Enter new interval ([ww:dd:hh:mm:ss])`<br>Type a different reconciliation interval. For example, `[00:01:00:00:00]`<br>This value is the interval to wait after the event notification completes before it is run again. The event notification process is resource intense, therefore, this value must not be set to run frequently. This option is not available if you select **Enabled - Adapter**. |

| *Table 7: Options for the event notification menus (continued)* | |
|---|---|
| **Option** | **Configuration task** |
| C | Displays the following prompt:<br>`Enter new cache size[50]:`<br>Type a different value to change the processing cache size. This option is not available if you select **Enabled - Adapter**. |
| D | Displays the Event Notification Entry Types Menu. This option is not available if you select Disabled or Enabled - Adapter. For more information, see "Setting event notification triggers" on page 60. |
| E | Displays the following prompt:<br>`Enter new thread priority [1-10]:`<br>Type a different thread value to change the event notification process priority. Setting the thread priority to a lower value reduces the impact that the event notification process has on the performance of the adapter. A lower value might also cause event notification to take longer. |
| F | Displays the following prompt:<br>`Enter new context name:`<br>Type the new context name and press **Enter**. The new context is added. |
| G | Displays a menu that lists the available contexts. For more information, see "Modifying an event notification context" on page 61. |
| H | Displays the Remove Context Menu. This option displays the following prompt:<br>`Delete context context1? [no]:`<br>Press **Enter** to exit without deleting the context or type `Yes` and press **Enter** to delete the context. |
| I | Displays the Event Notification Contexts in the following format:<br>`Context Name : Context1`<br>`Target DN : erservicename=context1,o=IBM,ou=IBM,dc=com`<br>`--- Attributes for search request ---`<br>`{search attributes listed}`<br>`----------` |
| J | When you select the **Set password attribute names**, you can set the names of the attributes that contain passwords. These values are not stored in the state database and changes are not sent as events. This option avoids the risk of sending a delete request for the old password in clear text when IBM Security Identity Governance and Intelligence changes a password. Changes from IBM Security Identity Governance and Intelligence are recorded in the local database for event notification. A subsequent event notification does not retrieve the password. It sends a delete request for the old password in clear text that is listed in the IBM Security Identity Governance and Intelligence log files. |

4. If you changed the value for options B, C, E, or F, press **Enter**.

   The other options are automatically changed when you type the corresponding letter of the menu option.

   The **Event Notification Menu** is displayed with your new settings.

**Related tasks**

Identifying the server that uses the DAML protocol

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

Setting event notification triggers

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

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

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

**Procedure**

1. Access the **Agent Main Configuration Menu**.
   See "Starting the adapter configuration tool" on page 48.
2. At the Event Notification Menu, type E to display the Event Notification Entry Types Menu.

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

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

   - Enable Event notification
   - Create and configure a context
   - Perform a full reconciliation operation
3. Take one of the following actions:
   - Type A for a list of the attributes that are returned during a user reconciliation.
   - Type B for attributes that are returned during a group reconciliation.

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

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

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

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

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

Setting event notification on the server
Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

Modifying an event notification context

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

### Modifying an event notification context

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

#### About this task

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

In the following example screen, Context1, Context2, and Context3 are different contexts that have a different base point.

#### Procedure

1. Access the **Agent Main Configuration Menu**.
2. From Event Notification, type the **Event Notification Menu** option.
3. From **Event Notification Menu**, type the **Modify Event Notification Context** option to display a list of available context.
   For example,

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

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

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

*Table 8: Modify context options*

| Option | Configuration task | For more information |
|---|---|---|
| A | Adding search attributes for event notification | See “Adding search attributes for event notification” on page 62. |
| B | Configuring the target DN for event notification contexts | See “Configuring the target DN for event notification contexts” on page 63. |

#### Related tasks

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

Setting event notification on the server
Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

Setting event notification triggers

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

***Adding search attributes for event notification***
For some adapters, you might specify an attribute and value pair for one or more contexts.

**About this task**

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

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

**Procedure**

1. Access the **Agent Main Configuration Menu**.
   See "Starting the adapter configuration tool" on page 48.
2. At the **Modify Context Menu** for the context, type A to display the **Reconciliation Attribute Passed to Agent Menu**.

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

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

**Related concepts**

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

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

**Related tasks**

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

Removing the baseline database for event notification contexts

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

***Configuring the target DN for event notification contexts***

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

**About this task**

During event notification configuration, the adapter sends requests to a service that is running on the IBM Security Identity Manager server.

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

The adapter service name
Organization (o)
Organization name (ou)

**Procedure**

1. Access the **Agent Main Configuration Menu**.
   See "Starting the adapter configuration tool" on page 48.
2. Type the option for Event Notification to display the **Event Notification Menu**.
3. Type the option for Modify Event Notification Context, then enter the option of the context that you want to modify.
4. At the **Modify Context Menu** for the context, type B.
   The following prompt is displayed:

   ```
   Enter Target DN:
   ```

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

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

   Table 9 on page 63 describes each DN element.

*Table 9: DN elements and definitions*

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

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

**Related concepts**

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

Pseudo-distinguished name values

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

**Related tasks**

Adding search attributes for event notification
For some adapters, you might specify an attribute and value pair for one or more contexts.

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

***Search attributes***

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

These attribute-value pairs, which are defined in the context under **Set attributes for search**, serve multiple purposes:

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

Table 10 on page 64 describes a partial list of possible attribute-value pairs that you can specify for **Set attributes for search**.

*Table 10: Attributes for search*

| Service type | Form label | Attribute name | Value |
|---|---|---|---|
| RACF profile | RACF loginid under which requests are processed | eracf2requester | A *Scoped Privileged* RACF loginid that manages users in this service. |

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

A.  RACF

X.  Done

Select menu option:a

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

A.  Set attributes for search
B.  Target DN:

Select menu option:a

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

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

X.  Done

Select menu option:a

Attribute name : erracfrequester

Attribute value: admnbu1

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

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

X.  Done

Select menu option:x
```

**Related concepts**

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

**Related tasks**

Adding search attributes for event notification
For some adapters, you might specify an attribute and value pair for one or more contexts.

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

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

***Pseudo-distinguished name values***

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

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

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

| *Table 11: Name values and their description* | | |
|---|---|---|
| **Component** | **Item** | **Description** |
| A | erServicename | The value of the erServicename attribute of the service. |
| B | Zero or more occurrences of ou or 1 or both. | When the service is not directly associated with the organization, you must specify ou and 1. The specification of these values is in a reverse sequence of their appearance in the IBM Security Identity Manager organization chart. |
| C | o | The value of the o attribute of an organization to which the service belongs, at the highest level. This value can be determined by examining the IBM Security Identity Manager organization chart. |
| D | ou | The ou component is established at IBM Security Identity Manager installation. You can find this component in the IBM Security Identity Manager configuration file named `enRole.properties`, on configuration item named `enrole.defaulttenant.id=` |
| E | dc | The dc component is established at IBM Security Identity Manager installation. This component is the root suffix of the LDAP environment. You can find this component in the IBM Security Identity Manager configuration file named `enRole.properties`, on configuration item named `enrole.ldapserver.root=` |

Example 1:

**A:**

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

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

**B:**

Table 12 on page 66 describes an example of the IBM Security Identity Manager organization chart that indicates the location of the service in the organization.

| *Table 12: Organization chart example* | | |
|---|---|---|
| + Identity Manager Home | IBM Security Identity Manager Home | |
| + Acme Inc | Base organization | o |

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

**C:**

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

```
o=Acme Inc
```

**D:**

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

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

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

**E:**

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

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

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

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

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

Example 2:

**A:**

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

```
erservicename=Irvine Sales
```

**B:**

Table 13 on page 67 describes an example of the IBM Security Identity Manager organization chart that indicates the location of the service in the organization.

*Table 13: Organization chart example*

| | | |
|---|---|---|
| `+ Identity Manager Home` | IBM Security Identity Manager Home | |
| `-Acme Inc` | Base organization | o |
| `- Irvine`<br>`Sales` | LocationOrganizational Unit | lou |

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

Component B of the pseudo-DN is:

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

**C:**

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

```
o=Acme Inc
```

**D:**

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

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

The D component of the pseudo-DN is:

```
ou=Acme
```

**E:**

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

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

The E component of the pseudo-DN is:

```
dc=my_suffix
```

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

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

**Related concepts**

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

**Related tasks**

Adding search attributes for event notification
For some adapters, you might specify an attribute and value pair for one or more contexts.

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

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

***Removing the baseline database for event notification contexts***

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

**Procedure**

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

**Related concepts**

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

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

**Related tasks**

Adding search attributes for event notification
For some adapters, you might specify an attribute and value pair for one or more contexts.

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

## Changing the configuration key

Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

**Procedure**

1. Access the **Agent Main Configuration Menu**.
   For more information, see "Starting the adapter configuration tool" on page 48.
2. At the **Main menu** prompt, typeD.
3. Take one of the following actions:
   - Change the value of the configuration key and press **Enter**.
     **Note:** The default configuration key is `agent`. Ensure that your password is complex.
   - Press **Enter** to return to the **Main Configuration Menu** without changing the configuration key.

**Related concepts**

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the IBM Security Identity server with the changes. You can enable event notification to obtain the updated information from the managed resource. Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool
Start the **`agentCfg`** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings

The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Changing activity logging settings

Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

### About this task

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

### Procedure

1. Access the **Agent Main Configuration Menu**.
2. At the **Main menu** prompt, type E to display the **Agent Activity Logging Menu**.
   The following screen displays the default activity logging settings.

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

3. Type the letter of the preferred menu option

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

   - Press **Enter** to change the value for menu option B, C, D, or E. The other options are changed automatically when you type the corresponding letter of the menu option. Table 14 on page 71 describes each option.
   - Press **Enter** to return to the **Agent Activity Logging Menu** without changing the value.

*Table 14: Options for the activity logging menu*

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

**Related concepts**

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the IBM Security Identity server with the changes. You can enable event notification to obtain the updated information from the managed resource. Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Modifying registry settings

Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

**Procedure**

1. Access the **Agent Main Configuration Menu**.
   For more information, see "Starting the adapter configuration tool" on page 48.
2. At the **Main menu** prompt, type F.

The **Registry Menu** is displayed.

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

3. Type the letter of the preferred menu option

**Related concepts**

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the IBM Security Identity server with the changes. You can enable event notification to obtain the updated information from the managed resource. Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options

Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Modifying non-encrypted registry settings

Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

### Procedure

1. At the **Agent Registry Menu**, type A.

   The **Non-encrypted Registry Settings Menu** is displayed.

```
Agent Registry Item
-------------------------------------------------
01. DATADIR '/var/ibm/isim/data'
02. DEBUG 'TRUE'
03. DSJOB 'hlq.CNTL'
04. ENROLE_VERSION '4.0'
05. ISIMEXIT 'hlq.RACF'
06. PASSEXPIRE 'FALSE'
07. PROFDEL 'FALSE'
08. RACFRC '30'
09. RECOSAVE 'hlq.SAVE'
10. SCOPING 'TRUE'
-------------------------------------------------
Page 1 of 2
A. Add new attribute
B. Modify attribute value
C. Remove attribute
X. Done
Select menu option:
```

*Table 15: Non-encrypted registry keys*

| Key | Description |
|---|---|
| DATADIR | Specifies the USS adapter read/write home. This parameter must be the read/write home as specified in the Disk location parameters panel during installation. This location is where the `registry.dat` and the UDF.- dat files are stored. |
| DEBUG | The default setting is TRUE.<br>When set to TRUE, warning messages are returned to the IBM Security Identity Manager server for those attributes in which the request to add,delete or modify is executed successfully with return code 0, but informational messages are returned by RACF.<br>When set to FALSE, warning messages are NOT returned to the IBM Security Identity Manager server for those attributes in which the request to add, delete or modify is executed successfully with return code 0, but informational messages are returned by RACF.<br>This setting must be set to FALSE when using zSecure Command Verifier in debug mode. This setting is also useful when there is a configuration issue pending a resolution. For example, when receiving`IKJ56644I` messages and waiting for the TSO segment to be added to the ISIAGNT account. In this case, it is still possible to manage accounts but not to perform reconciliations. |
| DSJOB | Specifies the data set where the RECOJOB is located. |
| CONGRP | Set this key to TRUE to enable forwarding of CONNECT/REMOVE operations to ISIMEXIT. |
| ENROLE_VERSION | Specifies the version of IBM Security Identity Manager. |

| *Table 15: Non-encrypted registry keys (continued)* | |
|---|---|
| **Key** | **Description** |
| ISIMEXIT | Specifies the data set where the ISIMEXIT/ISIMEXEC REXX scripts are located. |
| LABELATTR | The value of the attribute specified in this field is copied into the value of the `erracclabel` attribute. You can specify any attribute that holds a string value.<br>For example, `erracuname`, `erracuwaname`, or `erracuinstdata` |
| OPMODE | The value specified in this field determines the operations that the adapter supports.<br>Valid options are:<br>**`FULL (default)`**<br>The adapter supports all operations SEARCH/LOOKUP/ADD/DELETE/ MODIFY<br>**READ-ONLY**<br>The adapter only supports SEARCH and LOOKUP operations<br>**READ-ONLY-PWD**<br>The adapter supports SEARCH, LOOKUP, and PASSWORD/PASSWORD PHRASE operations |
| PASSEXPIRE | Specifies the default action that the adapter must do when the adapter receives a password or pass phrase change request. TRUE indicates that passwords and pass phrases must be set as expired. FALSE indicates that passwords and pass phrases must be set as nonexpired. |
| PROFDEL | The default setting is FALSE.<br>When set to TRUE, adapter deletes any data set profiles for an account, before deleting an account. When set to FALSE or unspecified, adapter deletes the account without first deleting the data set profiles for the account. |
| RACFRC | Specified the amount of time the adapter waits for the RECOJOB JCL processing to complete. |
| RECOSAVE | Specifies the data set where the intermediate reconciliation results are stored by RECOJOB. The adapter accesses this data set as soon as the status of RECOJOB is COMPLETED to collect and further process the results. This name must NOT contain any of the following strings:<br>• CONNECT<br>• REMOVE<br>• PW<br>• ALU<br>• ALG<br>• ADDUSER<br>• DELUSER<br>• PHRASE<br>• PASSWORD |
| SCOPING | Specifies whether SCOPING is to be used for reconciliations. The value can be 'TRUE' (reconciliations are scoped) or 'FALSE' (full reconciliations are done). |

| *Table 15: Non-encrypted registry keys (continued)* | |
|---|---|
| **Key** | **Description** |
| LOKUSAVE | Specifies the data set where the intermediate single account lookup results are stored. This name must NOT contain any of the following strings:<br>• CONNECT<br>• REMOVE<br>• PW<br>• ALU<br>• ALG<br>• ADDUSER<br>• DELUSER<br>• PHRASE<br>• PASSWORD |
| TSOCMD | Specify TRUE to use tsocmd or FALSE to use IRXEXEC. The default value is TRUE. |

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

| *Table 16: Attribute configuration option description* | |
|---|---|
| **Option** | **Configuration task** |
| A | Add new attribute. |
| B | Modify attribute value. |
| C | Remove attribute. |

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

**Results**

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

**Related concepts**

Configuring event notification

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

**Related tasks**

Supporting custom fields with extended attributes

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

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

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

Starting the adapter configuration tool

Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings

Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Changing advanced settings

Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

### About this task

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

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

This thread counts determines the maximum number of requests that the adapter processes. You can change these settings.

### Procedure

1. Access the **Agent Main Configuration Menu**.
   For more information, see "Starting the adapter configuration tool" on page 48.
2. At the **Main menu** prompt, type G to display the **Advanced Settings Menu**.

   The following screen displays the default thread count settings.

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

3. Type the letter of the preferred menu option

   For a description of each option, see Table 17 on page 78.

*Table 17: Options for the advanced settings menu*

| Option | Description |
|---|---|
| A | Forces the adapter to submit only 1 request at a time.<br>The default value is FALSE. |
| B | Limits the number of Add requests that can run simultaneously.<br>The default value is 3. |
| C | Limits the number of Modify requests that can run simultaneously.<br>The default value is 3. |
| D | Limits the number of Delete requests that can run simultaneously.<br>The default value is 3. |
| E | Limits the number of Search requests that can run simultaneously.<br>The default value is 3. |
| F | Limits the number of Lookup requests that can run simultaneously.<br>The default value is 3. |
| G | Determines whether the adapter can perform the pre-exec and post-exec functions. The default value is FALSE.<br>**Note:** Enabling this option is a potential security risk. |
| H | This option is no longer supported. |
| I | This option is no longer supported. |
| J | Currently, this adapter does not support processing filters directly. This option must always be FALSE. |

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

**Related concepts**

Configuring event notification

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

information from the managed resource. Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Viewing statistics

Use the **Statistics** option to view the event log of the adapter.

**Procedure**

1. Access the **Agent Main Configuration Menu**.
   For more information, see “Starting the adapter configuration tool” on page 48.
2. At the **Main menu** prompt, type H to display the activity history for the adapter.

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

-------------------------------------------------------------------
10/19/2004  000000    000004    000000     000000    000000    000004
-------------------------------------------------------------------
X. Done
```

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

**Related concepts**

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the IBM Security Identity server with the changes. You can enable event notification to obtain the updated information from the managed resource. Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Changing code page settings

Use the **Codepage Support** option to view the list of codes that the adapter supports.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Changing code page settings

Use the **Codepage Support** option to view the list of codes that the adapter supports.

### Before you begin

The adapter must be running.

### About this task

Run the following command to view the code page information:

```
agentCfg -agent adapterAGNT -codepages
```

### Procedure

1. Access the **Agent Main Configuration Menu**.
   For more information, see "Starting the adapter configuration tool" on page 48
2. At the **Main menu** prompt, type `I`.
   The **Code Page Support Menu** for the adapter is displayed.

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

A.  Codepage Configure.

X.  Done

Select menu option:
```

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

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

Enter configuration key for Agent 'adapterAGNT':

        Agent Main Configuration Menu
        -----------------------------------------

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

        X.  Done

        Select menu option:i

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

        A.  Codepage Configure.

        X.  Done

        Select menu option:a

        Enter Codepage: ibm-1145

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

        A.  Codepage Configure.

        X.  Done

        Select menu option:x
```

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

**Related concepts**

Configuring event notification

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

**Related tasks**

Supporting custom fields with extended attributes

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

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

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

Starting the adapter configuration tool

Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Accessing help and additional options
Access the **agentCfg** help menu to view the list of available arguments that you can use.

## Accessing help and additional options

Access the **agentCfg** help menu to view the list of available arguments that you can use.

### Procedure

1. At the **Main menu** prompt, typeX to display the UNIX System Services command prompt.
2. Type **agentCfg** `-help` at the prompt to display the help menu and list of commands.

```
-version               ;Show version
-hostname <value>    ;Target nodename to connect to (Default:Local host
IP address)
-findall               ;Find all agents on target node
-list                  ;List available agents on target node
-agent <value>         ;Name of agent
-tail                  ;Display agent's activity log
-schema                ;Display agent's attribute schema
-portnumber <value>    ;Specified agent's TCP/IP port number
-netsearch <value>   ;Lookup agents hosted on specified subnet
-codepages             ;Display list of available codepages
-help                  ;Display this help screen
```

The following table describes each argument.

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

| Argument | Description |
|---|---|
| **-version** | Use this argument to display the version of the **agentCfg** tool. |

| *Table 18: Arguments and description for the **agentCfg** help menu (continued)* | |
|---|---|
| **Argument** | **Description** |
| **-hostname <value>** | Use the **-hostname** argument with one of the following arguments to specify a different host:<br>• -findall<br>• -list<br>• -tail<br>• -agent<br>Enter a host name or IP address as the value. |
| **-findall** | Use this argument to search and display all port addresses 44970 - 44994 and their assigned adapter names. This option times out the unused port numbers. Therefore, it might take several minutes to complete.<br>Add the **-hostname** argument to search a remote host. |
| **-list** | Use this argument to display the adapters that are installed on the local host of the adapter.<br>By default, the first time you install an adapter, it is either assigned to port address 44970 or to the next available port number. You can then assign all the later installed adapters to the next available port address. After the software finds an unused port, the listing stops.<br>Use the **-hostname** argument to search a remote host. |
| **-agent <value>** | Use this argument to specify the adapter that you want to configure.<br>Enter the adapter name as the value. Use this argument with the **-hostname** argument to modify the configuration setting from a remote host. You can also use this argument with the -tail argument. |
| **-tail** | Use this argument with the **-agent** argument to display the activity log for an adapter.<br>Add the **-hostname** argument to display the log file for an adapter on a different host. |
| **-portnumber <value>** | Use this argument with the **-agent** argument to specify the port number that is used for connections for the **agentCfg** tool. |
| **-netsearch <value>** | Use this argument with the **-findall** argument to display all active adapters on the operating system. You must specify a subnet address as the value. |

| *Table 18: Arguments and description for the **agentCfg** help menu (continued)* | |
|---|---|
| **Argument** | **Description** |
| **-codepages** | Use this argument to display a list of available codepages. |
| **-help** | Use this argument to display the Help information for the **agentCfg** command. |

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

   **agentCfg -list**
   Displays a list of:

   - All the adapters on the local host.
   - The IP address of the host.
   - The IP address of the local host.
   - The node on which the adapter is installed.

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

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

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

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

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

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

**Related concepts**

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the IBM Security Identity server with the changes. You can enable event notification to obtain the updated information from the managed resource. Use the **Event Notification** option to set the event notification for the IBM Security Identity server.

**Related tasks**

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

Mapping the custom fields to the extended attributes by using the ISPF dialog
The extended attribute definitions in the RACF adapter are managed through the ISPF dialog that was installed as part of installation of the adapter. The adapter uses the mapped fields for generating the RACF commands for provisioning and for reconciliation.

Starting the adapter configuration tool

Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing configuration settings
Use the **Configuration Settings** option to display the adapter information such as its version, ADK version, and adapter log file name.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the IBM Security Identity server. By default, when the adapter is installed, the DAML protocol is configured for a non-secure environment. Use the **Protocol Configuration** option to configure the protocol properties for the adapter.

Changing the configuration key
Use the **Change Configuration Key** option to set the configuration key. The configuration key is used as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use the **Activity Logging** option to enable or disable log files that monitor various system activities.

Modifying registry settings
Use the **Registry Settings** option to access the various types of registry settings that you can modify based on your requirements.

Modifying non-encrypted registry settings
Use the **Modify Non-encrypted registry settings** option to modify the registry settings that do not use encryption.

Changing advanced settings
Use the **Advanced Settings** option to change the adapter thread count settings for the different types of requests.

Viewing statistics
Use the **Statistics** option to view the event log of the adapter.

Changing code page settings
Use the **Codepage Support** option to view the list of codes that the adapter supports.

## Configuring SSL authentication

To establish a secure connection between the adapter and the IBM Security Identity server, configure SSL authentication for connections that originate from the IBM Security Identity server or from the adapter.

Use the Secure Sockets Layer (SSL) authentication with the default communication protocol, DAML.

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

By configuring the adapter for SSL, the IBM Security Identity server can verify the identity of the adapter before the server establishes a secure connection.

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

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

## Overview of SSL and digital certificates

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

SSL protocol uses signed digital certificates from a Certificate Authority (CA) for authentication. SSL encrypts the data that is exchanged between the applications to secure communication.

Signed digital certificates enable two applications that connect in a network to authenticate their identity. An application that acts as an SSL server presents its credentials to an SSL client for verification. The SSL client verifies that the application is the entity it claims to be. You can configure an application that acts as an SSL server so that it requires the application that acts as an SSL client to present its credentials in a certificate. In this way, the two-way exchange of certificates is completed. For more information on the two-way SSL configuration, see Defining and Securing Keystores or Truststores.

A third-party Certificate Authority issues signed certificates for a fee. Some utilities, such as those provided by OpenSSL, can also provide signed certificates.

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

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

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

### Private keys, public keys, and digital certificates

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

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

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

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

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

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

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

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

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

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

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

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

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

Use a key management utility to:

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

Usage of self-signed certificates depends on your security requirements. To obtain the highest level of authentication between critical software components, do not use self-signed certificates or use them selectively. You can authenticate applications that protect server data with signed digital certificates. You can use self-signed certificates to authenticate web browsers or adapters.

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

**Certificate and key formats**
Certificates and keys are stored in the files with various formats.

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

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

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

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

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

**`.pfx` format (PKCS12)**

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

## DAML SSL implementation

When you start the adapter, it loads the available connection protocols. The DAML protocol is the only available protocol that supports SSL authentication. You can specify DAML SSL implementation.

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

## Configuring certificates for SSL authentication

To establish a secure connection between the adapter and the IBM Security Identity server, configure SSL authentication for connections that originate from the IBM Security Identity server or from the adapter. You can configure the adapter for one-way or two-way SSL authentication with signed certificates.


- "Configuring certificates for one-way SSL authentication" on page 89
- "Configuring certificates for two-way SSL authentication" on page 90
- "Configuring certificates when the adapter operates as an SSL client" on page 91
- "Managing the SSL certificates" on page 92


### Configuring certificates for one-way SSL authentication

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

#### About this task

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

In Figure 4 on page 89, Application A operates as the IBM Security Identity server, and Application B operates as the IBM Security Identity Adapter.

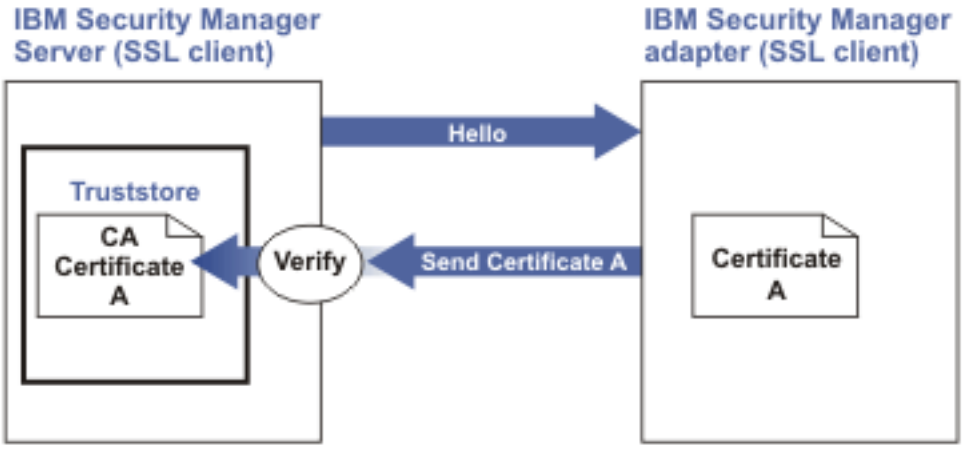


*Figure 4: One-way SSL authentication (server authentication)*

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

#### Procedure

1. On the adapter, complete these steps:
   a) Start the certTool utility.
   b) Configure the SSL-server application with a signed certificate issued by a certificate authority.

1) Create a certificate signing request (CSR) and private key. This step creates the certificate with an embedded public key and a separate private key and places the private key in the PENDING_KEY registry value.
2) Submit the CSR to the certificate authority by using the instructions that are supplied by the CA. When you submit the CSR, specify that you want the root CA certificate that is returned with the server certificate.

2. On the IBM Security Identity server, complete one of these steps:

- If you used a signed certificate that is issued by a well-known CA:
  a. Ensure that the IBM Security Identity server stored the root certificate of the CA (CA certificate) in its keystore. See https://www-01.ibm.com/support/docview.wss?uid=ibm10713583.
  b. If the keystore does not contain the CA certificate, extract the CA certificate from the adapter and add it to the keystore of the server.
- If you generated the self-signed certificate on the IBM Security Identity server, the certificate is installed and requires no additional steps.
- If you generated the self-signed certificate with the key management utility of another application:
  a. Extract the certificate from the keystore of that application.
  b. Add it to the keystore of the IBM Security Identity server.

**Configuring certificates for two-way SSL authentication**
In this configuration, the IBM Security Identity server and the adapter use SSL.

**Before you begin**

Configure the adapter and the IBM Security Identity server for one-way SSL authentication.

If you use signed certificates from a CA:

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

**About this task**

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

In Figure 5 on page 90, the IBM Security Identity server operates as Application A and the IBM Security Identity Adapter operates as Application B.

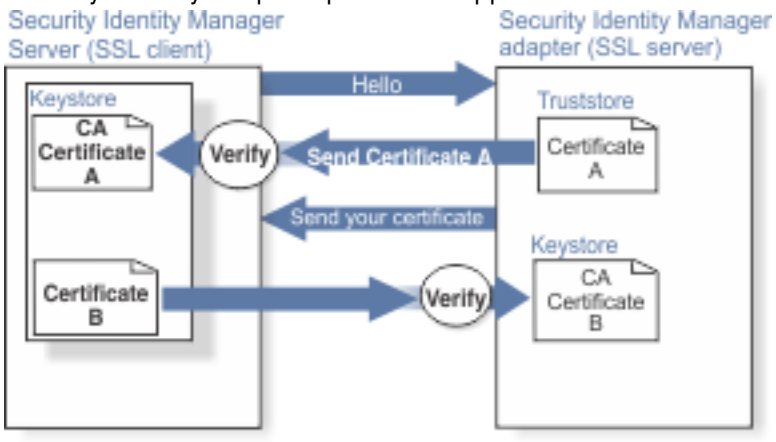


*Figure 5: Two-way SSL authentication (client authentication)*

### Procedure

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

### Results

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

### Related tasks

"Configuring certificates for one-way SSL authentication" on page 89
In this configuration, the IBM Security Identity server and the adapter use SSL.

## Configuring certificates when the adapter operates as an SSL client

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

### About this task

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

Figure 6 on page 91 describes how the adapter operates as an SSL server and as an SSL client. When the adapter communicates with the IBM Security Identity server, the adapter sends its certificate for authentication. When the adapter communicates with the web server, the adapter receives the certificate of the web server.

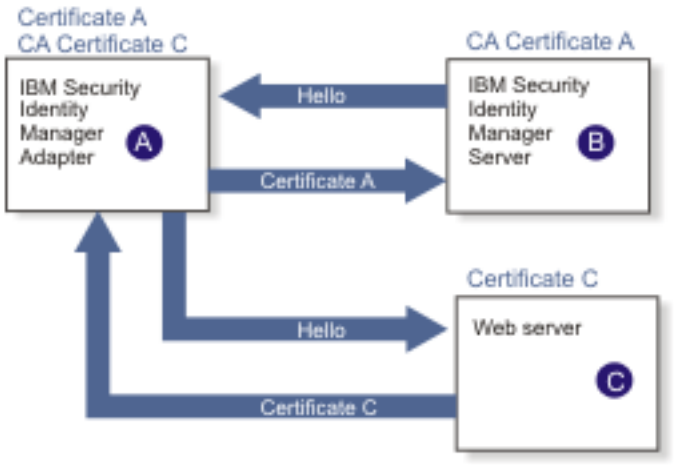


*Figure 6: Adapter operating as an SSL server and an SSL client*

If the web server is configured for two-way SSL authentication, it verifies the identity of the adapter. The adapter sends its signed certificate to the web server. To enable two-way SSL authentication between the adapter and web server, complete these steps:

### Procedure

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

### What to do next

You might want the software to send an event notification when the adapter initiates a connection to the web server, which is used by the IBM Security Identity server.

## Managing the SSL certificates

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



### Starting the certTool utility

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

#### About this task

From the **Main** menu of the certTool utility, you can complete these tasks:

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

#### Procedure

1. Log on to the adapter
2. In the command prompt, change to the read/write `/bin` subdirectory of the adapter.If the adapter is installed in the default location for the read/write directory, run the following command.

   **For Windows based operating systems**

   ```
   cd C:\Tivoli\Agents\adapterAGNT\bin
   ```

   **For UNIX based operating systems**

   ```
   cd /var/ibm/isim/bin
   ```
3. Type certTool at the prompt. The **Main menu** is displayed.

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

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

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

K. Export certificate and key to PKCS12 file

X. Quit

Choice:
```

4. Type the letter of the preferred menu option

   Options A through D generates a CSR and installs the returned signed certificate on the adapter.

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

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

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

   **D. View current installed certificate**
   View the certificate that is installed on the z/OS system where the adapter is installed.

   Options E through G installs the root CA certificates on the adapter. A CA certificate validates the corresponding certificate from the client, such as the server.

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

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

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

   Options H through K apply to adapters that must authenticate the application to which the adapter is sending information. An example of an application is the IBM Security Identity server or the web server. Use these options to register certificates on the adapter.

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

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

   **J. Unregister a certificate**
   Remove a certificate from the registered list.

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

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

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

**Generating a private key and certificate request**

Use the **Generate private key and certificate request** certTool option to generate a private key and a certificate request for secure communication between the adapter and IBM Security Identity Governance and Intelligence.

**About this task**

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

A CSR file looks similar to the following example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwgZUxEjAQBgNVBAoTCWFjY2VzczM2MDEUMBIGA1UECxMLZW5n
aW5lZXJpbmcxEDAOBgNVBAMTB250YWdlbnQxJDAiBgkqhkiG9w0BCQEWFW50YWdl
bnRAYWNjZXNzMzYwLmNvbTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Ju
aWExDzANBgNVBAcTBklydmluZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
mR6AcPnwf6hLLc72BmUkAwaXcebtxCoCnnTH9uc8VuMHPbIMAgjuC4s91hPrilG7
UtlbOfy6X3R3kbeR8apRR9uLYrPIvQ1b4NK0whsytij6syCySaFQIB6V7RPBatFr
6XQ9hpsARdkGytZmGTgGTJ1hSS/jA6mbxpgmttz9HPECAwEAAaAAMA0GCSqGSIb3
DQEBAgUAA4GBADxA1cDkvXhgZntHkwT9tCTqUNV9sim8N/U15HgMRh177jVaHJqb
N1Er46vQSsOOOk4z2i/XwOmFkNNTXRVl9TLZZ/D+9mGZcDobcO+lbAKlePwyufxK
Xqdpu3d433H7xfJJSNYLYBFkrQJesITqKft0Q45gIjywIrbctVUCepL2
 -----END CERTIFICATE REQUEST-----
```

**Procedure**

1. At the **Main menu** of the certTool utility, type A. The following prompt is displayed:

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

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

   The private key and certificate request are generated after the values are accepted.
10. At **Enter name of file to store PEM cert request**, type the name of the file and press **Enter**. Specify the file that you want to use to store the values you specified in the previous steps.

11. Press **Enter** to continue. The certificate request and input values are written to the file you specified. The file is copied to the adapter `data` directory and the **Main** menu is displayed again.

**What to do next**

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

**Installing the certificate**
Use the **Install certificate from file** certTool option to install the certificate on the adapter, from a file returned by the CA in response to the generated CSR.

**About this task**

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

**Procedure**

1. If you received the certificate as part of an email message, take the following actions:
   a) Copy the text of the certificate to a text file.
   b) Copy that file to the read/write data directory of the adapter.
   For example:`/var/ibm/`*`adapterAGNT`*`/data`

   **For Windows based operating systems**

   **For UNIX based operating systems**
2. At the **Main menu** of the certTool utility, type B. The following prompt is displayed:

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

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

**Results**
The certificate is installed in the adapter registry, and the **Main Menu** is displayed again.

**Installing the certificate and key from a PKCS12 file**
If the certTool utility did not generate a CSR to obtain a certificate, you must install both the certificate and private key. Use the **Install certificate and key from a PKCS12 file** certTool option to install a certificate from a PKCS12 format file that includes both the public certificate and a private key.

**About this task**

Store the certificate and the private key in a PKCS12 file.

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

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

**Procedure**

1. Copy the PKCS12 file to the `data` directory of the adapter.
   For example:

   **For Windows based operating systems**

   **For UNIX based operating systems**
2. At the **Main menu** of the certTool utility, type B. The following prompt is displayed:

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

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

**Results**
The certificate and private key is installed in the adapter registry, and the **Main Menu** is displayed again.

**Viewing the installed certificate**
Use the **View current installed certificate** certTool option to view the certificate that is installed on the z/OS system where the adapter is installed.

**Procedure**

1. At the **Main menu** of the certTool utility, type `D`.
2. The utility displays the installed certificate. The following example shows an installed certificate:

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

**Installing a CA certificate**
Use the **Install a CA certificate** certTool option to install root CA certificates on the adapter.

**About this task**

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

**Procedure**

1. At the **Main menu** of the certTool utility, type F. The following prompt is displayed:

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

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

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

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

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

**Viewing CA certificates**
Use the **List CA certificates** certTool option to view the private keys and certificates that are installed for the adapter.

**About this task**

The certTool utility installs only one certificate and one private key. You can list the CA certificate on the adapter.

**Procedure**

1. At the **Main menu** of the certTool utility, type E.
2. The utility displays the installed CA certificates. The following example shows an installed CA certificate:

```
Subject: o=IBM,ou=SampleCACert,cn=TestCA
```

```
Valid To: Wed Jul 26 23:59:59 2006
```

### Deleting a CA certificate

Use the **Delete a CA certificate** certTool option to delete a CA certificate from the adapter directories.

#### Procedure

1. At the **Main menu** of the certTool utility, type G to display a list of all CA certificates that are installed on the adapter.

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

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

#### Results

The CA certificate is deleted from the `DamlCACerts.pem` file and the certTool utility displays the **Main Menu**.

### Registering a certificate

Use the **Register a certificate** certTool option to register certificates on the adapter. Adapters that must authenticate to the application to which it is sending information must have a registered certificate. An example of an application is the IBM Security Identity server or the web server.

#### Procedure

1. At the **Main menu** of the certTool utility, type I. The following prompt is displayed:

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

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

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

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

#### Results

The certificate is registered to the adapter and the certTool displays the **Main Menu**.

### Viewing registered certificates

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

#### Procedure

To view a list of all registered certificates, type H on the **Main Menu** prompt.

The utility displays the registered certificates and the **Main** menu. The following example shows a list of the registered certificates:

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

### Unregistering a certificate

Use the **Unregister a certificate** certTool option to remove an adapter certificate from the registered list.

#### Procedure

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

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

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

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

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

#### Results

The certificate is removed from the list of registered certificate for the adapter and the certTool utility displays the **Main Menu**.

### Exporting a certificate and key to PKCS12 file

Use the **Export certificate and key to PKCS12 file** certTool option to export a previously installed certificate and private key to a PKCS12 file.

#### Procedure

1. At the **Main menu** of the certTool utility, type K. The following prompt is displayed:

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

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

#### Results

The certificate or private key is exported to the PKCS12 file and the certTool displays the **Main Menu**.

## Customizing the adapter

You can do specific functions according to your requirements by using the REXX execs that are provided with the adapter installation.


- "ISIMEXIT command usage" on page 99
- "ISIMEXEC command usage" on page 101


### Getting started

Customizing and extending adapters requires a number of additional skills. The developer must be familiar with the following concepts and skills prior to beginning the modifications:

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

**Note:** This adapter supports customization only through the use of pre-Exec and post-Exec scripting. The RACF Adapter has REXX scripting options.

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

#### Support for customized adapters

The integration of the IBM Security Identity Manager server server and the adapter framework is supported. However, IBM does not support the customizations, scripts, or other modifications. If you experience a problem with a customized adapter, IBM support may require the problem to be demonstrated on the GA version of the adapter before a PMR is opened.

## ISIMEXIT command usage

**ISIMEXIT** is a REXX command. Use this command to start a REXX exec in response to a processing request from the IBM Security Identity server.

The ISIMEXIT command is added to allow site-pecific customization. Customizations that are made to the ISIMEXIT REXX are not in scope for IBM support.

Changes are made to the ISIMEXIT implementation for the current adapter release to enhance performance and enable passing on connect group modifications to ISIMEXIT. The REXX command executor interfaces with the ISIMEXIT REXX script. It uses IKJTSOEV to enable issuing TSO/E commands in the ISIMEXIT. To allocate and execute the ISIMEXIT REXX script it uses IRXLOAD with IRXEXEC or `tsocmd`, depending on the option that is defined in the registry.

New installation panels are created to allow you to enable or disable forwarding CONNECT and REMOVE commands with the name of the connect group to which an account is to be connected or from which an account is to be removed to ISIMEXIT for account MODIFY operations. Option 5 in the Display / Define / Alter Variables panel is added for this purpose.

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

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

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

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

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

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

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

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

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

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

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

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

for the current RACF user that is processed for an ADD or MODIFY request and a failure for a DELETE request.

The environment in which the **ISIMEXIT** gets control is in a TSO/E environment. You might call other programs and do file input and output as necessary. Processing is done under the authority of the RACF ID that runs the RACF commands to accomplish the function. You might run a valid TSO command if it does not prompt for a terminal user for input.

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

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

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

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

The listed information is available to the EXIT.

*Table 19: **ISIMEXIT** processing information*

| Parameter # | Meaning | Possible value | Availability |
|---|---|---|---|
| 1 | Verb<br>Indicates what operation is calling the exit. | ADD, MODIFY, SUSPEND, RESTORE, or DELETE. | Always |
| 2 | Object<br>The object name of the transaction. | USER indicating a RACF user object that is processed. | Always |
| 3 | Prepost<br>Qualifies whether this entry is PRE or POST processing entry to the exit. | BEFORE or AFTER. | Always |
| 4 | Name<br>The name of the RACF object. | The RACF user ID that is processed. | Always |
| 5 | Transactionid (Bigint) | A unique identification number for the server request that is being processed. | Always |
| 6 | Add1<br>Dfltgrp<br>The RACF user ID default group.<br>OR<br>CONNECT/REMOVE | The value that is specified from the IBM Security Identity server for the default group of this user. | Only at PRE ADD or POST ADD exit. Not available for DELETE processing. |

| *Table 19: **ISIMEXIT** processing information (continued)* | | | |
|---|---|---|---|
| **Parameter #** | **Meaning** | **Possible value** | **Availability** |
| 7 | Add2<br>Owner<br>The RACF user ID owner.<br>OR<br><connectrgroup> | The value that is specified from the IBM Security Identity server owner for this user.<br>The name of the group for which a CONNECT or REMOVE operation is requested. | Only at PRE ADD or POST ADD exit. Not available for DELETE processing. |

TSO statements can be executed by placing them in between double quotations. For example:

```
z = outtrap(lines.)
"SEARCH CLASS(DATASET) FILTER("name".**)"
z = outtrap(off)
```

To allocate a file in SYSOUT (which shows in the SDSF output queue as ISI- AGNTX or SURROGATX ):

```
"ALLOCATE FILE(ISIOUT) SYSOUT(A)"
```

(use QUEUE and EXECIO to write output to ISIOUT in the example above).

If, during an account MODIFY operation, a CONNECT or REMOVE to/from a connect group is performed for an account the following information is passed on to ISIMEXIT:

```
MODIFY USER <BEFORE/AFTER> <USERID> <TRANSACTIONID> <CONNECT/REMOVE> <CON- NECTGROUP>
```

In the event the MODIFY BEFORE command returns a non-zero return code to the adapter, processing will stop for the connect group that was currently being modified and the connect group is returned in the list of unmodified attributes to the Identity server.

In the event the MODIFY AFTER command returns a non-zero return code to the adapter, processing will continue for the connect group that was currently being modified and a WARNING will be reported to the Identity server for the current transaction.

The agentCfg tool can be used to modify the value of the CONGRP attribute after the adapter has been installed and has been activated. This setting does not require a restart of the adapter to be activated. Refer to the adapter guide for details on setting non-encrypted registry settings using the agentCfg tool.

**Related concepts**

ISIMEXEC command usage

**ISIMEXEC** is a REXX command. Use this command for backward compatibility with earlier versions of the adapter.The function will be removed from the product in 2020. It is recommended to migrate the existing functionality to ISIMEXIT.

## ISIMEXEC command usage

**ISIMEXEC** is a REXX command. Use this command for backward compatibility with earlier versions of the adapter.The function will be removed from the product in 2020. It is recommended to migrate the existing functionality to ISIMEXIT.

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

The adapter also supports the output of one single Say statement to be returned to the adapter log for additional information.

The environment in which the **ISIMEXIT** gets control is in a TSO/E environment. You might call other programs and do file input and output as necessary. Processing is done under the authority of the RACF ID

that runs the RACF commands to accomplish the function. You might run a valid TSO command if it does not prompt for a terminal user for input.

*Table 20: **ISIMEXEC** processing information*

| Parameter # | Source | Value | Availability |
|---|---|---|---|
| 1 | IBM Security Identity Governance and Intelligence attribute of **erUid** | The value of the **erUid**. | Always, because this attribute accompanies all requests. |
| 2 | IBM Security Identity Governance and Intelligence attribute of **erRacExecname** | The value of the **erRacExecname**. | Always, because the availability of this attribute indicates that this exit must be started. |
| 3 | IBM Security Identity Governance and Intelligence attribute of **erRacExecvar** | The value of the **erRacExecvar**. | Based on the request that is generated by the IBM Security Identity server. |

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

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

```
%ISIMEXEC erUid erRacExecname erRacExecvar
```

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

- **erUid**
- **erRacUDfltgrp**
- **erRacUowner**

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

**Note:**

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

**Related concepts**

ISIMEXIT command usage

**ISIMEXIT** is a REXX command. Use this command to start a REXX exec in response to a processing request from the IBM Security Identity server.

## z/OS UNIX System Services considerations

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

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

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

# Chapter 6. Troubleshooting

*Troubleshooting* is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

**Note:** If you encounter a problem, enable all levels of activity logging (debug, detail, base, and thread). The adapter log contains the main source of troubleshooting information. See “Changing activity logging settings” on page 70.

## Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Problem descriptions help you and the IBM technical-support representative find the cause of the problem. This step includes asking yourself basic questions:

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

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

### What are the symptoms of the problem?

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

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

### Where does the problem occur?

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

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

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

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all

corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or are not fully tested together.

**When does the problem occur?**

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

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

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

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

**Under which conditions does the problem occur?**

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

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

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

**Can the problem be reproduced?**

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

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

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

**Related concepts**

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

Error messages and problem solving

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

**Related tasks**

Installing test fixes and diagnostic builds
IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

**Related reference**

Frequently asked questions

## Logs

When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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

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

*Table 21: Example of Adapter log details*

| Details | Example values |
|---|---|
| Installation path | `/usr/itim` |
| Adapter log name | *`RACFAgent`* |
| Log location | `/usr/itim/log/` |
| Log files | • *`RACFAgent`*`.log`<br>• *`RACFAgent`*`.log_001`<br>• *`RACFAgent`*`.log_002`<br>• *`RACFAgent`*`.log_003` |

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

The size of a log file, the number of log files, the directory path, and the detailed level of logging are configured with the **agentCfg** program.

For more information, see “Configuring the adapter parameters” on page 41.

**Related concepts**

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

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

**Related tasks**

Installing test fixes and diagnostic builds

IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

**Related reference**

Frequently asked questions

## Error messages and problem solving

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

### Error messages

**agentCfg configuration key minimum characters**

A configuration key is not allowed to be less than 5 characters. Otherwise, when you start agentCfg to configure an active adapter, the following message is displayed:

```
Configuration key too short - 5 characters minimum. Aborting...
```

After which the agentCfg processing aborts.

**Registry file initialization**

Additional information is logged in the z/OS syslog during adapter initialization. It is about the initialization of the registry file for the following scenarios:

1. The registry file that is configured in the shell script is used to start the adapter does not exist. In this event a new registry file is created and the following messages are written to the syslog:

```
racfAgent: Registry file specified by environment
REGISTRY is '<adapter_read_write_home>/data/<adapter_name>.dat'
racfAgent: REGISTRY does not exist
racfAgent: Creating a new registry file
```

2. The registry file does exist, but cannot be accessed (for example, incorrect file permissions). In this event the adapter aborts initialization and the following messages are written to the syslog:

```
racfAgent: Registry file specified by environment
REGISTRY is '<adapter_read_write_home>/data/<adapter_name>.dat'
racfAgent: FATAL ERROR: REGISTRY file open error: EDC5111I Permission
denied.
racfAgent: can't continue without access to the registry file
racfAgent: exiting process
```

3. The registry does exist but the adapter can't access part of the path. In this event the adapter aborts initialization and the following messages are written to the syslog:

```
racfAgent: Registry file specified by environment
REGISTRY is '<adapter_read_write_home>/data/<adapter_name>.dat'
racfAgent: FATAL ERROR: REGISTRY file stat error:
EDC5111I Permission denied.
racfAgent: can't continue without access to the registry file
racfAgent: exiting process
```

4. The registry does exist, but is not specified in the shell script that is used to start the adapter. In this event a new registry file is created in `/tmp` and the following messages are written to the syslog:

```
racfAgent: WARNING no REGISTRY file specified by the environment
racfAgent: Creating a new registry file
racfAgent: Registry to be created is '/tmp/<adapter_name>.dat'
```

**Max Thread settings for adapter operations**

The default maximum number of threads for all adapter operations (search, modify, add, delete) is set to three at adapter initialization. The default minimum number of threads for all adapter operations is

set to one at adapter initialization since at least one thread is required to perform an operation. The adapter now writes debug messages to the adapter log regarding the number of threads currently still available for performing new operations. This provides more insight in possible thread availability-related delays in processing.

**Starting the adapter in console mode**

For debugging purposes, it might be useful to start the adapter directly from the command line in console mode. Doing so provides all messages that are otherwise written to either the syslog or the adapter log to be displayed on the console used to start the adapter from. Starting the adapter in console mode can be done by executing all export commands as configured in the shell script. The script is used to start the adapter to ensure that all libraries are available to the adapter and then executes the following command to start the adapter:

```
/<adapter_readonly_home/lpp/bin/racfAgent -name <adapter_name> -registry
<adapter_readwrite_home>/data/<adapter_name>.dat -console
```

**Added AES to KERB form (and changed DESD description)**

On the Security Identity Manager server, the description for the DESD field in the Kerberos tab was incorrect. This is corrected and a new field was added for the AES encryption type and support for the new field was added to the RACF agent.

**Warnings and error messages**

All errors returned by RACF when executing RACF commands using the R_Admin calleable service IRRSEQ00 are recorded in the adapter log. If a command cannot be run, the adapter records the SAF return code, the RACF return code and RACF reason codes in the adapter log. For example:

```
ERR:15/05/01 11:48:47 issueRadmin: safRC = 8, racfRC = 8 racfReason = 24,
returning rc = 5
```

It is likely that the AdapterID or SURROGATID does not have permission to all the required profiles as described in the RACF Access Configuration. Detailed information on these return and reason codes can be found in the z/OS Security Server RACF Callable Services documentation in the z/OS Knowledge Center.

**BSE:_ermAlloc: ERROR: malloc FAILED: size 60**

The adapter stops processing when it encounters errors during memory allocation.

The following messages are displayed to indicate that the adapter is aborting from the process:

```
ERR: racfSearch: Entry creation returned failure
ERR:racfSearch: reconciliation ABORTED
```

After which, this final error message is written to the adapter log: `ERR: "FATAL memory error encountered, shutting down now"`

The IBM Security Identity Manager server displays `Fatal error encountered`

Memory allocation errors might be caused from inadequate Language Environment (LE) HEAP size settings.

The HEAP size settings can be diagnosed when you add the following line to the adapter start script:

```
export _CEE_RUNOPTS='RPTOPTS(ON),RPTSTG(ON)'
```

This line ensures that the adapters started task log displays the current heap size allocations and suggested minimal sizes.

You can use the following general settings for the RACF adapter:

```
export _CEE_RUNOPTS='HEAP(80K,8K,ANYWHERE,,1K,1K),AN(1450K,4K,ANY,FREE),AL(ON),
HEAPPOOLS(ON,8,8,16,16,24,17,32,3,56,8,72,3,136,4,296,7,480,3,848,4,2080,,4104,)'
```

### Adapter messages

#### RACF UNLOAD missing 0102 record processing

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

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

IRRDBU00 does not unload a Group Members data record (0102) for every user connected to a universal group. Only users who are listed in the group's member list have 0102 records. Users listed in the group member list are those users with group-level user attributes, such as group-SPECIAL, or group authority higher than USE.

The adapter will not write the `Unload 0102 record is missing` message to the log for universal groups. These records are expected to be missing for users that are not listed in the group's member list.

### Server messages

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

*Table 22: Error messages, warnings, and corrective actions*

| Error message or warning | Additional warnings, messages, or information | Corrective action |
|---|---|---|
| Adapter error message: could not set security environment for SURROGAT. | Adapter log: ERR:14/07/31 10:42:31 racfModify: pthread_security_np() create failed. errno2=0BE800D8: EDC5139I Operation is not permitted | PERMIT UPDATE access for ISIAGNT on BPX.SERVER in CLASS FACILITY |
| racfSearch: failed to create RECOJOB thread | z/OS Syslog might provide INSUFFICIENT AUTHORITY message | Verify that the adapter RACF ID and SURROGAT ID have read and write access to the READWRITE data directory. |
| Could not set security environment for SURROGAT user | Not applicable | PERMIT READ access for ISIAGNT on BPX.SRV.*<SURROGATID>* in CLASS SURROGAT |
| racfSearch: failed to create RECOJOB thread | DETAIL Adapter log: tsoCmd: result is IKJ56644I NO VALID TSO USERID, DEFAULT USER ATTRIBUTES USED | Ensure that the ADAPTER ID has a valid TSO USERID. |
| CTGIMU107W The `connection to the specified service cannot be established. Verify the service information, and try again` | An IO error occurred sending a request. Error: `Connection refused: connect` | Ensure that the adapter service is running. For more information about starting the adapter service, see “Restarting the adapter service” on page 22. |

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

| Error message or warning | Additional warnings, messages, or information | Corrective action |
|---|---|---|
| | The adapter returned an error status for a bind request. Status code: invalid credentials adapter error message: `Authentication Failed` | Check the adapter authentication ID and password match the installed values. See the screen for Adapter-specific parameters in the task "Running the ISPF dialog" on page 14. |
| | An IO error occurred sending a request. Error: `com.ibm.daml.jndi. JSSESocketConnection .HANDSHAKE_FAILED:` | If SSL is enabled, check the configuration. See . The adapter log contains details about the certificates that are loaded during initialization. |
| | User *user name* add Successful. Some attributes were not modified: *attr1,attr2* | An attempt is made to add a user account. However, certain attributes are not set during the user add operation. For more information, see the adapter log file at `/var/ibm/isimracf/log/racfagent.log.`. The log file contains information about the attributes that are not set during the user add operation. |
| | User *user name* modify Successful. Some attributes were not modified: *attr1,attr2* | An attempt is made to modify a user account. However, modification failed for certain attributes during the operation. For more information, see the adapter log file at `/var/ibm/isimracf/log/racfagent.log`. The log file contains information about the attributes that are not set during the modify operation. |
| `CTGIMD812E An error occurred while processing the adapter response message. The following error occurred. Error: Premature end of file.` | | Ensure that the adapter service is running. For more information about starting the adapter service, see "Restarting the adapter service" on page 22 |
| tsoCmd: result is YOUR TSO ADMINISTRATOR MUST AUTHORIZE USE OF THIS COMMAND | Not applicable. | PERMIT READ access for ISIAGNT on JCL in CLASS TSOAUTH<br>For example: PE JCL CLASS(TSOAUTH) ID(ISIAGNT) ACCESS(READ)SETROPTS RACLIST(TSOAUTH) REFRESH |
| tsoCmd: RECOJOB was not submitted | tsoCmd: result is *<result string>*<br>racfSearch: failed to initiate reco_open | Verify whether the result string is a standard TSO message as defined in SYS1.MSGENU(IKJSCHEN).<br>If a custom exit that returns a non-standard message is implemented, exclude the reconciliation job from this exit. |

| Table 22: Error messages, warnings, and corrective actions (continued) | | |
|---|---|---|
| **Error message or warning** | **Additional warnings, messages, or information** | **Corrective action** |
| LDAP: error code 92 | | Increase the size of the transaction log.<br>See DB2 transaction log size. |
| `*BPXI040I PROCESS LIMIT MAXPROCUSER HAS REACHED XX % OF ITS CURRENT CAPACITY OF XX FOR PID=XXX IN JOB ISIAGNT` | | Increase the amount of processes available to the adapter's RACF logonid. |

**Related concepts**

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

**Related tasks**

Installing test fixes and diagnostic builds
IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

**Related reference**

Frequently asked questions

## Installing test fixes and diagnostic builds

IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

### About this task

These fixes can consist of either an `<ADAPTER>.UPLOAD.XMI` file or a zip file containing a new adapter or ADK binary.

XMI files require a full new install. These are usually provided when several components have changed compared to the release you currently had installed. To ensure that there are no inconsistencies between the versions of the components you have installed and the updated components that were used to created the fix, you must perform the full installation from scratch using the XMI that contains the fix.

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

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

Follow the procedures below to install a new agent binary.

**Procedure**

1. Extract the binary from the zip file.
2. Stop the adapter.
3. Change the directory with `cd read_only_home/bin` folder.
4. Copy `<adaptertype>Agent <adaptertype>Agent.save`.
5. Upload `<adapterype>Agent` in binary ftp mode to the adapter host and store it in the `read_only_home/bin` folder.
6. Change the directory with `cd read_only_home/bin` folder.
7. Change the permissions with `chmod 755 <adaptertype>Agent`.
8. Specify the extended attributes with `extattr +ap <adaptertype>Agent`.
9. Start the adapter.

**Related concepts**

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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

**Related reference**

Frequently asked questions

## Frequently asked questions

**Where can I find registry and/or permission related errors?**
In ISPF, navigate to S (SDSF), LOG.

**How can I disable persistent connections between the Identity Server and the adapter?**
The first is in IBM Security Identity Manager. The setting must be explicitly placed in enRole.properties: `com.ibm.daml.jndi.DAMLContext.POOL_MAX_SIZE=0`

This effects disable the connection pool.

The other setting is on the adapter side. Invoke `agentCfg` and navigate to **B. Protocol Configuration** > **C. Configure Protocol** > **A. DAML** > **K. READ_TIMEOUT** and specify a value in seconds. For example, 30 seconds. Save and restart the adapter. This causes the adapter to timeout any socket that has not responded within 30 seconds.

**How can I monitor if the adapter is up and running?**
To check the availability of your adapter, ensure that the `DAML_PORT` is listening. The default port is 45580. If you probe and the port is not listening, the adapter is down.

**Why is my registry file cleared?**
There might be several causes. To determine the cause, provide an answer to the following questions when contacting support:

- Were there any messages in the SDSF SYSLOG (S.LOG) at the time the adapter was started and the registry file had been reset?
- Is it possible the adapter was started before the file system was mounted?
- Does the `read_only_home` directory exist when the filesystem is not mounted?
- Can you find registry files that have been created in `/tmp`?

- Is the file system shared between different hosts?
- Does the registry file exist on the file system at the time it was reset?

It might be useful to collect the output from the following commands at the time a correct, configured registry file is active and compare that output to the output for the same commands after an IPL when you notice the registry is reset:

```
df -k /adapter_readwrite_home
ls -Elg /adapter_readwrite_home/data
/adapter_readwrite_home/bin/regis /adapter_readwrite_home/data/<adapter_name>.dat -list
```

**How can I see what information is being send and received to and from the adapter by the IBM Security Identity Manager server?**

Edit enRoleLogging.properties to set the DAML line to DEBUG_MAX.

this will enable full tracing for DAML based adapters. The information that is generated includes SSL communication and account details.

**How do I resolve ICH420I PROGRAM XXXX FROM LIBRARY ISP.SISPLOAD CAUSED THE ENVIRONMENTTO BECOME UNCONTROLLED errors?**

Add the **PROGRAM** profile to the ISP.SISPLOAD data set.

```
 RALTER PROGRAM **ADDMEM('ISP.SISPLOAD'//NOPADCHK)
 SETROPTS WHEN(PROGRAM) REFRESH
```

**I've tried all the options that are documented in the “Warning and Error messages” table, but I still can't run a reconciliation.**

The adapter is configured to wait for an x number of seconds for the submitted RECOJOB job to complete. As you can see in the lines from the adapter log below the adapter in the example is now configured to wait 60 seconds and the job does not complete within 60 seconds. It is still executing after the last second the adapter waited for it to complete.

```
DTL:18/01/31 15:38:06 Thread:000005 tsoCmd: max wait time is 60 seconds
```

```
DTL:18/01/31 15:40:24 Thread:000005 Waiting 0 more seconds for the job to complete
ERR:18/01/31 15:40:24 Thread:000005 tsoCmd: job tsocmd " STATUS RECOJOBR(JOB45696) "2>&1 did
 not complete
DTL:18/01/31 15:40:24 Thread:000005 tsoCmd: job status returned: IKJ56211I JOB
 RECOJOBR(JOB45696) EXECUTING
```

To resolve the issue the value for the RACFRC registry setting needs to be increased. Specifyi a fairly large number initially, and after a few weeks determine how long the job on average runs and after how many seconds it is save to assume there's an issue with the job/system and the adapter should return an error. Use that last value as the new RACFRC registry value.

Looking at "ERR:18/02/07 14:46:07 Thread:000008 tsoCmd: failed to open output file" it seems the adapter ran into an issue when trying to read the temporary output file that should have been created when running the STATUS command. The output file would be something like this: /var/ibm/isiaracf/data/proc.8200291508630857997.err

It might be that the filesystem /var/ibm/isiaracf/data ran out of space. There could also have been an issue in processing the STATUS command itself, so no output was returned from the command yet. Verify the following: - free space in adapter_readwrite_home/data - file permissions for ITIAGNT in adapter_readwrite_home/data (should be rwx) - the z/OS system log for any errors for ITIAGNT and/or JOB RECOJOBR() . For instance RECOJOBR(JOB46572) . - the output from the following command ran from the z/OS Unix shell. For instance: tsocmd " STATUS RECOJOBR(JOB46572) "

**Where do I find the output for the installation jobs?**

In SDSF, option Status of Jobs (ST). The output for installation job J1 can be found in AG

J1, the output for installation job J2 can be found in AGJ2, etc. For RACF this would be: AGRJ1 for installation job J1 For ACF2 this would be AGAJ1 for installation job J1.

**When do I select tsocmd and when do I select IRXEXEC?**

- IRXEXEC offers the best performance. This option should be selected in environments with many simultaneous connect group related modifications and/or environments where forwarding connect group modifications to ISIMEXIT is enabled and where authorized commands are not called from ISIMEXIT
- tsocmd should be used if ISIMEXIT is used to execute authorized TSO/E commands.

**Related concepts**

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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

**Related tasks**

Installing test fixes and diagnostic builds
IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

# Chapter 7. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

## Adapter attributes

The IBM Security Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

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

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

The adapter software is installed on an operating system and the adapter is defined by Agent Maintenance. You then identify the attribute data that is needed to create the user access. You identify these attributes to IBM Security Identity Governance and Intelligence when you define the Access Request Form for access through Request Maintenance.

### Adapter attributes by object

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

**Note:** Reconciliations return group data and user data.

### erRacUser

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

*Table 23: Account form attributes*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erAccountStatus<br>Whether this user is in REVOKED status, or not. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid REVOKE`<br>To delete:<br>`ALU userid RESUME` |
| erPassword<br>Password or pass phrase of user. Must be alphanumeric, and can include '@#$'. Case sensitivity depends on RACF settings.<br>**Note:** * A generated password is set so that the old password cannot be used. | String | 100 | Single | W | No | To add or modify:<br>• If 8 or less:<br>`ALU userid Password(value) NOPHRASE`<br>• If 9 or more:<br>`ALU userid Password(*) PHRASE(value)`<br>To delete:<br>`ALU userid NOPASSWORD NOPHRASE` |

*Table 23: Account form attributes(continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacExecName<br>Exec name - not a RACF attribute, but for compatibility with old RASEXEC. | String | 44 | Single | W | No | To add or modify:<br>`ISIMEXEC userid value` |
| erRacExecVar<br>Exec Attribute - not a RACF attribute, but for compatibility with old RASEXEC. | String | 44 | Single | W | No | This argument is the second argument (*value*) to the ISIMEXEC call for erRacExecName. |
| erRacfRequester<br>RACF ID of requesting user. The RACF ID is the ID of the person within IBM Security Identity Governance and Intelligence who is making the provisioning request. | String | 8 | Single | W | No | |
| erRacUClauth<br>A list of RACF resource classes this user has rights to administer. Any class in the Class Descriptor Table (CDT), and USER is valid. GROUP and DATASET are invalid. | String | 8 | Multiple | RW | No | To add or modify:<br>`ALU userid CLAUTH(value)`<br>To delete:<br>`ALU userid NOCLAUTH(value)` |
| erRacUCreDate<br>Date user was created. | Date | | Single | R | No | |
| erRacUDfltgrp<br>Name of existing group that is the initial and default group this user is associated with. | String | 8 | Single | RW | Yes | To add or modify:<br>`ALU userid DFLTGRP(value)` |
| erRacUInstData<br>Installation defined data that can be associated with a user. | String | 254 | Single | RW | No | To add or modify:<br>`ALU userid DATA('value')`<br>To delete:<br>`ALU userid NODATA` |
| erRacUIsADSP<br>User can automatically create discrete data set profiles. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid ADSP`<br>To delete:<br>`ALU userid NOADSP` |
| erRacUIsAudit<br>User has system auditor ability. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid AUDITOR`<br>To delete:<br>`ALU userid NOAUDITOR` |
| erRacUIsCICSSeg<br>CICS® segment is present.<br>User CICS information. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. CICS this information assigns the user-specific characteristics. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid CICS`<br>To delete:<br>`ALU userid NOCICS` |

*Table 23: Account form attributes(continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUCICSIsForc<br>Whether this user is forced off if the current system fails over to a backup system. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid CICS (XRFSOFF(FORCE))`<br>To delete:<br>`ALU userid CICS (XRFSOFF(NOFORCE))` |
| erRacUCICSOpclas<br>Operator class. Valid values are 1 - 24. | Integer | 2 | Multiple | RW | No | To add or modify:<br>`ALU userid CICS (OPCLASS(value))`<br>To delete:<br>`ALU userid CICS (NOOPCLASS)` |
| erRacUCICSOpid<br>Operator ID. 1 - 3 characters. Any value acceptable. | String | 3 | Single | RW | No | To add or modify:<br>`ALU userid CICS (OPID(value))`<br>To delete:<br>`ALU userid CICS (NOOPID)` |
| erRacUCICSPrty<br>Operator priority, value can be 0 - 255. | Integer | 3 | Single | RW | No | To add or modify:<br>`ALU userid CICS (OPPRTY(value))`<br>To delete:<br>`ALU userid CICS (NOOPPRTY)` |
| erRacUCICSTimout<br>User timeout value, in the form of HHMM. | Time | 4 | Single | RW | No | To add or modify:<br>`ALU userid CICS (TIMEOUT(value))`<br>To delete:<br>`ALU userid CICS (NOTIMEOUT)` |
| erRacUIsDCESeg<br>DCE segment is present.<br>DCE information. This information describes the user in the context of a DCE (Distributed Computing Environment). Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid DCE`<br>To delete:<br>`ALU userid NODCE` |
| erRacUDCEIsAutoL<br>Whether this user is automatically identified to DCE through AUTOLOGIN or not. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid DCE (AUTOLOAD(YES))`<br>To delete:<br>`ALU userid DCE (NOAUTOLOAD)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUDCEHomeC<br>DCE Home Cell name. | String | 1023 | Single | RW | No | To add or modify:<br>`ALU userid DCE (HOMECELL(value))`<br>To delete:<br>`ALU userid DCE (NOHOMECELL)` |
| erRacUDCEHomeU<br>UUID for the cell that this user is defined to. String must have the delimiter of "-" in character positions 9, 14, 19, and 24. The general format for the UUID string is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, in which x represents a valid numeric or hexadecimal character. | String | 36 | Single | RW | No | To add or modify:<br>`ALU userid DCE (HOMEUUID(value))`<br>To delete:<br>`ALU userid DCE (NOHOMEUUID)` |
| erRacUDCEName<br>DCE Principal name. | String | 1023 | Single | RW | No | To add or modify:<br>`ALU userid DCE (DCENAME(value))`<br>To delete:<br>`ALU userid DCE (NODCENAME)` |
| erRacUDCEUUID<br>UUID of this instance of the user. This string must have the delimiter of "-" in character positions 9, 14, 19, and 24. The general format for the UUID string is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, in which x represents a valid numeric or hexadecimal character. | String | 36 | Single | RW | No | To add or modify:<br>`ALU userid DCE (UUID(value))`<br>To delete:<br>`ALU userid DCE (NOUUID)` |
| erRacUIsDFPSeg<br>DFP segment is present.<br>The following attributes are user DFP information. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. DFP uses this information to determine data management and disk storage characteristics when a user creates a data set. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid DFP`<br>To delete:<br>`ALU userid NODFP` |
| erRacUDFPAppl<br>Name of a user-defined application. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid DFP (DATAAPPL(value))`<br>To delete:<br>`ALU userid DFP (NODATAAPPL)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUDFPData<br>DATACLAS name to be used for new file creation. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid DFP (DATACLAS(value))`<br>To delete:<br>`ALU userid DFP (NODATACLAS)` |
| erRacUDFPMgmt<br>MGMTCLAS name to be used for new file creation. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid DFP (MGMTCLAS(value))`<br>To delete:<br>`ALU userid DFP (NOMGMTCLAS)` |
| erRacUDFPStor<br>STORCLAS name to be used for new file creation. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid DFP (STORCLAS(value))`<br>To delete:<br>`ALU userid DFP (NOSTORCLAS)` |
| erRacUIsEimSeg<br>EIM segment is present.<br>EnterPrise Identity Management (EIM). This object contains a name from the LDAPBIND general resource profile class, of the user as it is known to the Enterprise Identity Mapping environment. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid EIM`<br>To delete:<br>`ALU userid NOEIM` |
| erRacUEimLDAPNam<br>Name of profile in the LDAPBIND class. | String | 246 | Single | RW | No | To add or modify:<br>`ALU userid EIM (LDAPPROF(value))`<br>To delete:<br>`ALU userid EIM (NOLDAPPROF)` |
| erRacUIsGrpacc<br>Enables group level access of UPDATE to the group under the High Level Qualifier of any data set profile created through ADSP by this user. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid GRPACC`<br>To delete:<br>`ALU userid NOGRPACC` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUIsKerbSeg<br>Kerberos segment is present.<br>Kerberos information. This object describes Kerberos information that relates to this instance of the user. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid KERB`<br>To delete:<br>`ALU userid NOKERB` |
| erRacUKerbIsDES<br>Single length DES keys allowed. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid KERB (ENCRYPT(DES))`<br>To delete:<br>`ALU userid KERB (ENCRYPT(NODES))` |
| erRacUKerbIsDES3<br>Triple DES keys allowed. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid KERB (ENCRYPT(DES3))`<br>To delete:<br>`ALU userid KERB (ENCRYPT(NODES3))` |
| erRacUKerbIsDESD<br>Double DES keys allowed. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid KERB (ENCRYPT(DESD))`<br>To delete:<br>`ALU userid KERB (ENCRYPT(NODESD))` |
| erRacUKerbName<br>Kerberos Principal name. can consist of any character except the @+ (X'7C') character. Avoid the use of any of the EBCDIC variant characters to prevent problems between different code pages. | String | 240 | Single | RW | Yes | To add or modify:<br>`ALU userid KERB (KERBNAME(value))`<br>To delete:<br>`ALU userid KERB (NOKERBNAME)` |
| erRacUKerbTickMx<br>Maximum ticket life, in seconds. Valid value range is 1 - 2,147,483,647. | Integer | 10 | Single | RW | No | To add or modify:<br>`ALU userid KERB (MAXTKT(value))`<br>To delete:<br>`ALU userid KERB (NOMAXTKT)` |
| erRacUKerbI sAES128<br>AES 128 bit keys allowed. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid KERB (ENCRYPT(AES128))`<br>To delete:<br>`ALU userid KERB (ENCRYPT(NOAES128))` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUKerbI sAES256<br>AES 256 bit keys allowed. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid KERB (ENCRYPT(AES256))`<br>To delete:<br>`ALU userid KERB (ENCRYPT(NOAES256))` |
| erRacUIsLangSeg<br>Language segment is present.<br>User Language information. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid LANGUAGE`<br>To delete:<br>`ALU userid NOLANGUAGE` |
| erRacULangPrime<br>Primary user language. | String | 3 | Single | RW | No | To add or modify:<br>`ALU userid LANG (PRIM(value))`<br>To delete:<br>`ALU userid LANG (NOPRIM)` |
| erRacULangSec<br>Secondary user language. | String | 3 | Single | RW | No | To add or modify:<br>`ALU userid LANG (SEC(value))`<br>To delete:<br>`ALU userid LANG (NOSEC)` |
| erRacUIsLNotesSeg<br>Lotus Notes® segment present.<br>Lotus Notes information. This object contains a Lotus Notes short name, of the user as it is known to this RACF system. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid LNOTES`<br>To delete:<br>`ALU userid NOLNOTES` |
| erRacULnotesSNam<br>Lotus Notes Short Name. You can specify the following characters: upper and lowercase letters (A -Z, and a -z), 0 -9, & (X'50'), - (X'60'), (X'4B'), _ (X'6D'), and (X'40'). The hex values that are shown are EBCDIC. | String | 64 | Single | RW | No | To add or modify:<br>`ALU userid LNOTES (SNAME(value))`<br>To delete:<br>`ALU userid LNOTES (NOSNAME)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUIsNetvSeg<br>Tivoli® NetView® for z/OS segment is present.<br>Tivoli NetView for z/OS information. This object might be present. It contains attributes that describe this user instance in the IBM Tivoli NetView for z/OS environment. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid NETVIEW`<br>To delete:<br>`ALU userid NONETVIEW` |
| erRacUNetvCons<br>Console name user assumes when console commands are issued. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid NETV (CONSNAM(value))`<br>To delete:<br>`ALU userid NETV (NOCONSNAM)` |
| erRacUNetvCtl<br>Only the specific values are allowed. Default is 'Specific'. Values that are allowed are: General Global Specific. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid NETV (CTL(value))`<br>To delete:<br>`ALU userid NETV (NOCTL)` |
| erRacUNetvDomain<br>List of commands a NetView operator my run in another Tivoli NetView for z/OS Domain. | String | 5 | Multiple | RW | No | To add or modify:<br>`ALU userid NETV (DOMAIN(value))`<br>To delete:<br>`ALU userid NETV (NODOMAIN)` |
| erRacUNetvGSpan<br>Not well documented. The best information found within Tivoli NetView for z/OS documentation indicates that this attribute is a maximum of 8 characters. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid NETV (NGMFVSPN(value))`<br>To delete:<br>`ALU userid NETV (NONGMFVSPN)` |
| erRacUNetvIC<br>Initial command to be run when this NetView user enters the Tivoli NetView for z/OS subsystem. | String | 255 | Single | RW | No | To add or modify:<br>`ALU userid NETV (IC(value))`<br>To delete:<br>`ALU userid NETV (NOIC)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUNetvIsGMF<br>Whether this user can use the Tivoli NetView for z/OS Graphic Monitor Facility or not. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid NETV (NGMFADMN(YES))`<br>To delete:<br>`ALU userid NETV (NONGMFADMN)` |
| erRacUNetvIsMR<br>Whether this user can receive unsolicited messages or not. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid NETV (MSGRECVR(YES))`<br>To delete:<br>`ALU userid NETV (NOMSGRECVR)` |
| erRacUNetvOpclas<br>Netview Operator classes. Can be values of 1 - 2040. | Integer | 4 | Multiple | RW | No | To add or modify:<br>`ALU userid NETV (OPCLASS(value))`<br>To delete:<br>`ALU userid NETV (NOOPCLASS)` |
| erRacUIsOMVSSeg<br>OMVS segment is present.<br>OMVS (UNIX) information. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (`<br>To delete:<br>`ALU userid NOOMVS` |
| erRacUOMVSCPU<br>Maximum CPU time, in seconds, this user can accumulate before processes is purged. Valid value range 7 - 2,147,483,647. | Integer | 10 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (CPUTIM(value))`<br>To delete:<br>`ALU userid OMVS (NOCPUTIM)` |
| erRacUOMVSFiles<br>Maximum number of files per process. Valid value range is 3 - 262,143. | Integer | 6 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (FILE(value))`<br>To delete:<br>`ALU userid OMVS (NOFILE)` |
| erRacUOMVSHome<br>Home directory of user. Case sensitive. Path must be valid for user. Can use the shell. | String | 1024 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (HOME(value))`<br>To delete:<br>`ALU userid OMVS (NOHOME)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUOMVSIsShar<br>If not set, and the UID specified is already assigned, and Shared UID support is enabled, the UID assignment might fail. | String | 5 | Single | W | No | To add or modify:<br>`ALU userid OMVS (UID(value)SHARED)` |
| erRacUOMVSMmap<br>Maximum number of pages for memory mapped files. Valid value range is 1 - 16,777,216. | Integer | 8 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (MMAP(value))`<br>To delete:<br>`ALU userid OMVS (NOMMAP)` |
| erRacUOMVSProc<br>Maximum processes per user. Valid value range is 3 - 32,767. | Integer | 5 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (PROC(value))`<br>To delete:<br>`ALU userid OMVS (NOPROC)` |
| erRacUOMVSShell<br>Shell program for user. Case sensitive. Must be a valid shell name for user to use the shell. Must be a fully qualified name, because the environment is not yet established. | String | 1024 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (PROG(value))`<br>To delete:<br>`ALU userid OMVS (NOPROG)` |
| erRacUOMVSStor<br>Maximum amount of storage, in bytes, this user can use. Valid value range is 10,485,760 - 2,147,483,647. | Integer | 10 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (ASSIZE(value))`<br>To delete:<br>`ALU userid OMVS (NOASSIZE)` |
| erRacUOMVSThread<br>Maximum number of threads per process. Valid value range is 0 - 100,000. Must be non-zero to allow use of ptthread_create. | Integer | 6 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (THREAD(value))`<br>To delete:<br>`ALU userid OMVS (NOTHREAD)` |
| erRacUOMVSuid<br>UNIX UID assigned to this user. Valid values are 0 - 2,147,483,647. Zero (0) means superuser.'*' means that the UID is automatically assigned. Specific profiles for AUTOUID support must be set up before its usage. | String | 10 | Single | RW | No | To add or modify:<br>`ALU userid OMVS (UID(value))`<br>To delete:<br>`ALU userid OMVS (NOUID)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUIsOper<br>User has system Operations ability (ability to read and modify any file). | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid OPERATIONS`<br>To delete:<br>`ALU userid NOOPERATIONS` |
| erRacUIsOperSeg<br>Operparm segment is present.<br>Operparm information. Attributes describe settings as a system operator. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid OPERPARM`<br>To delete:<br>`ALU userid NOOPERPARM` |
| erRacUOpAltgrp<br>Alternate Console group that is used in recovery. | Character | 8 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (ALTGRP(value))`<br>To delete:<br>`ALU userid OPERP (NOALTGRP)` |
| erRacUOpAuth<br>Console Authority. Valid values are:<br>• Master<br>• All<br>• Info<br>• Cons<br>• Io<br>• Sys | Character | 6 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (AUTH(value))`<br>To delete:<br>`ALU userid OPERP (NOAUTH)` |
| erRacUOpAuto<br>Whether the extended console can receive messages which are automated by the MPF facility. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (AUTO(YES))`<br>To delete:<br>`ALU userid OPERP (NOAUTO)` |
| erRacUOpCmdsys<br>Console name or '*'. A-Z, 0-9, @, #, $ are valid values, in addition to '*'. | Character | 8 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (CMDSYS(value))`<br>To delete:<br>`ALU userid OPERP (NOCMDSYS)` |
| erRacUOpDom<br>Valid values are 'Normal', 'All', or 'None'. | Character | 6 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (DOM(value))`<br>To delete:<br>`ALU userid OPERP (NODOM)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUOpKey<br>1 - 8 character key to display information from all consoles with this key. Valid values are A-Z, 0-9, @, #, $. | Character | 8 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (KEY(value))`<br>To delete:<br>`ALU userid OPERP (NOKEY)` |
| erRacUOpLevel<br>Level of information that can be displayed. Valid values are:<br>• NB<br>• R<br>• CE<br>• E<br>• IN<br>• ALL<br>If ALL is specified, no others can be specified. | Character | 3 | Multiple | RW | No | To add or modify:<br>`ALU userid OPERP (LEVEL(value))`<br>To delete:<br>`ALU userid OPERP (NOLEVEL)` |
| erRacUOpLogcmd<br>Valid values are SYSTEM or NONE. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (LOGCMDR(NO))`<br>To delete:<br>`ALU userid OPERP (NOLOGCMDR)` |
| erRacUOpMform<br>Message form of the messages that are displayed on the extended console. Valid values are:<br>• J<br>• M<br>• S<br>• T<br>• X | Character | 5 | Multiple | RW | No | To add or modify:<br>`ALU userid OPERP (MFORM(value))`<br>To delete:<br>`ALU userid OPERP (NOMFORM)` |
| erRacUOpMigid<br>Whether a migration ID is to be assigned to this extended console. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (MIGID(YES))`<br>To delete:<br>`ALU userid OPERP (NOMIGID)` |
| erRacUOpMonitor<br>Valid values are:<br>• JOBNAMES or JOBNAMEST<br>• SESS or SESST<br>• STATUS | Character | 9 | Multiple | RW | No | To add or modify:<br>`ALU userid OPERP (MONITOR(value))`<br>To delete:<br>`ALU userid OPERP (NOMONITOR)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUOpMscope<br>Valid system names for which messages can be received from. Valid values are system names, '*' and '*ALL'. | Character | 8 | Multiple | RW | No | To add or modify:<br>`ALU userid OPERP (MSCOPE(value))`<br>To delete:<br>`ALU userid OPERP (NOMSCOPE)` |
| erRacUOpRoutCode<br>The Routing Codes this console is to receive. Value range is 1 - 128. | Integer | 3 | Multiple | RW | No | To add or modify:<br>`ALU userid OPERP (ROUTC(value))`<br>To delete:<br>`ALU userid OPERP (NOROUTCR)` |
| erRacUOpStor<br>Valid value range is 1 - 2000. | Integer | 4 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (STORAGE(value))`<br>To delete:<br>`ALU userid OPERP (NOSTORAGE)` |
| erRacUOpUD<br>Whether this console is to receive undeliverable messages. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid OPERP (UD(YES))`<br>To delete:<br>`ALU userid OPERP (NOUD)` |
| erRacUIsProtect<br>User cannot be signed on to with a password. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid NOPASSWORD NOPHRASE` |
| erRacUIsPrxSeg<br>PROXY segment is present.<br>PROXY segment information. This object contains a name from the LDAPBIND general resource profile class, of the user as it is known to the Enterprise Identity Mapping environment. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid PROXY`<br>To delete:<br>`ALU userid NOPROXY` |
| erRacUPrxBindDN<br>Bind DN of user on target host. | Binary | 1023 | Single | RW | No | To add or modify:<br>`ALU userid PROXY (BINDDN(value))`<br>To delete:<br>`ALU userid PROXY (NOBINDDN)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUPrxBindHst<br>A URL of a host, which the local z/OS LDAP server contacts on behalf of the user. | Binary | 1023 | Single | RW | No | To add or modify:<br>`ALU userid PROXY (LDAPHOST(value))`<br>To delete:<br>`ALU userid PROXY (NOLDAPHOST)` |
| erRacUPrxBindPW<br>Bind password for erRacUPrxBindDN. | String | 128 | Single | W | No | To add or modify:<br>`ALU userid PROXY (BINDPW(value))`<br>To delete:<br>`ALU userid PROXY (NOBINDPW)` |
| erRacUIsRestrict<br>User cannot be granted access through UACC or ID(*) in resource profiles. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid RESTRICTED`<br>To delete:<br>`ALU userid NORESTRICTED` |
| erRacUIsSpecial<br>User has system Special. System Security Administrator. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid SPECIAL`<br>To delete:<br>`ALU userid NOSPECIAL` |
| erRacUIsTSOSeg<br>TSO segment is present.<br>User TSO information. Since this attribute is an optional object, its presence gives a user access to the time-sharing environment, even if all attribute values are null. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid TSO`<br>To delete:<br>`ALU userid NOTSO` |
| erRacUTSOAcct<br>Name of a user-defined application. | String | 40 | Single | RW | No | To add or modify:<br>`ALU userid TSO (ACCT(value))`<br>To delete:<br>`ALU userid TSO (NOACCT)` |
| erRacUTSOCmd<br>Initial command to be run upon connecting to TSO. | String | 80 | Single | RW | No | To add or modify:<br>`ALU userid TSO (COMMAND(value))`<br>To delete:<br>`ALU userid TSO (NOCOMMAND)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUTSODest<br>Default destination for system output. Must begin with A-Z, @#$, remaining data can be numeric. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid TSO (DEST(value))`<br>To delete:<br>`ALU userid TSO (NODEST)` |
| erRacUTSOHold<br>Default system output class for the held queue. Must be alphanumeric. | String | 1 | Single | RW | No | To add or modify:<br>`ALU userid TSO (HOLDCLASS(value))`<br>To delete:<br>`ALU userid TSO (NOHOLDCLASS)` |
| erRacUTSOMsg<br>Default system output message class. Must be alphanumeric. | String | 1 | Single | RW | No | To add or modify:<br>`ALU userid TSO (MSGCLASS(value))`<br>To delete:<br>`ALU userid TSO (NOMSGCLASS)` |
| erRacUTSOJob<br>Default system job execution class. Must be alphanumeric. | String | 1 | Single | RW | No | To add or modify:<br>`ALU userid TSO (JOBCLASS(value))`<br>To delete:<br>`ALU userid TSO (NOJOBCLASS)` |
| erRacUTSOMax<br>Maximum amount of storage user can request. Amount is specified in K bytes. Zero means no limit. | Integer | 7 | Single | RW | No | To add or modify:<br>`ALU userid TSO (MAXSIZE(value))`<br>To delete:<br>`ALU userid TSO (NOMAXSIZE)` |
| erRacUTSOProc<br>Default TSO logon procedure. Must begin with A-Z, @#$, remaining data can be numeric. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid TSO (PROC(value))`<br>To delete:<br>`ALU userid TSO (NOPROC)` |
| erRacUTSOSize<br>Requested amount of storage to be used by this session. Zero means no limit. | Integer | 7 | Single | RW | No | To add or modify:<br>`ALU userid TSO (SIZE(value))`<br>To delete:<br>`ALU userid TSO (NOSIZE)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUTSOSout<br>Default system output message class. Must be alphanumeric. | String | 1 | Single | RW | No | To add or modify:<br>`ALU userid TSO (SYSOUT(value))`<br>To delete:<br>`ALU userid TSO (NOSYSOUT)` |
| erRacUTSOUnit<br>Default allocation unit name. | String | 8 | Single | RW | No | To add or modify:<br>`ALU userid TSO (UNIT(value))`<br>To delete:<br>`ALU userid TSO (NOUNIT)` |
| erRacUTSOUdata<br>Hexadecimal value, which is defined by the user installation. Typically, this attribute is unused. | String | 4 | Single | RW | No | To add or modify:<br>`ALU userid TSO (USER(value))`<br>To delete:<br>`ALU userid TSO (NOUSER)` |
| erRacUIsUaudit<br>All user activity is logged. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid AUDIT`<br>To delete:<br>`ALU userid NOAUDIT` |
| erRacUIsWASeg<br>Work attribute is present.<br>Work Attribute information. It describes user location specifics. This object is or was primarily created for APPC/MVS. Since this attribute is an optional object, its presence has meaning, even if it contains no values for attributes. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid WORKATTR`<br>To delete:<br>`ALU userid NOWORKATTR` |
| erRacUWAAcct<br>Account number. This field has (real) meaning only for APPC/MVS tasks. | String | 255 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WACCNT('value'))`<br>To delete:<br>`ALU userid WORK (NOWAACCNT)` |
| erRacUWAAddr1<br>Address line 1. | String | 60 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WAADDR1('value'))`<br>To delete:<br>`ALU userid WORK (NOWAADDR1)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacUWAAddr2<br>Address line 2. | String | 60 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WAADDR2('value'))`<br>To delete:<br>`ALU userid WORK (NOWAADDR2)` |
| erRacUWAAddr3<br>Address line 3. | String | 60 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WAADDR3('value'))`<br>To delete:<br>`ALU userid WORK (NOWAADDR3)` |
| erRacUWAAddr4<br>Address line 4. | String | 60 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WAADDR4('value'))`<br>To delete:<br>`ALU userid WORK (NOWAADDR4)` |
| erRacUWABldg<br>Building. | String | 60 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WABLDG('value'))`<br>To delete:<br>`ALU userid WORK (NOWABLDG)` |
| erRacUWADept<br>Department. | String | 60 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WADEPT('value'))`<br>To delete:<br>`ALU userid WORK (NOWADEPT)` |
| erRacUWAName<br>Name. | String | 60 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WANAME('value'))`<br>To delete:<br>`ALU userid WORK (NOWANAME)` |
| erRacUWARoom<br>Room. | String | 60 | Single | RW | No | To add or modify:<br>`ALU userid WORK (WAROOM('value'))`<br>To delete:<br>`ALU userid WORK (NOWAROOM)` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacULogtime<br>Time user last signed on. Field is set to current time if password is reset, or if the user account status is resumed. | Time | | Single | R | No | |
| erRacUModel<br>The name of a data set profile this user can use as a model for creating new data set profiles. | String | 44 | Single | RW | No | To add or modify:<br>`ALU userid MODEL (value)`<br>To delete:<br>`ALU userid NOMODEL` |
| erRacUName<br>The name of the defined user. Value is nullified by setting it to 20 pound (#) signs:<br>`####################` | String | 20 | Single | RW | No | To add or modify:<br>`ALU userid NAME ('value')`<br>To delete:<br>`ALU userid NAME ('####################')` |
| erRacUOwner<br>Name of existing user or group that owns this user account. | String | 8 | Single | RW | Yes | To add or modify:<br>`ALU userid OWNER (value)` |
| erRacUPassdate<br>Date user is required to change password. If 0, current password must be changed upon initial use. | Date | | Single | R | No | |
| erRacUPWInterval<br>Password and pass phrase interval. Can be 0 - 255. Zero means no password or pass phrase interval. Maximum value that is imposed by RACF system-wide options. | Integer | 3 | Single | RW | No | To add or modify:<br>`PW USER (userid) INTERVAL (value)`<br>To delete:<br>`PW USER userid NOINTERVAL` |
| erRacUPWNoExpire<br>Whether a password or pass phraseassigned to this user is to be noted as 'not expired'. Must be used with the 'erPassword'. This attribute has no meaning without a password. This field was removed from the schema. It is an adapter option instead. | String | 5 | Single | W | No | |
| erRacUResumeDate<br>MM/DD/YY date field, indicates future date when this account is to be reactivated (RESUMEd). | Date | 8 | Single | RW | No | To add or modify:<br>`ALU (userid) RESUME (value)`<br>To delete:<br>`ALU userid RESUME` |

*Table 23: Account form attributes (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacURevokeDate<br>MM/DD/YY date field, indicates future date when this account is to be deactivated (revoked). | Date | 8 | Single | RW | No | To add or modify:<br>`ALU (userid) REVOKE (value)`<br>To delete:<br>`ALU userid RESUME` |
| erRacUWhenDays<br>Days of the week a user can sign on. Valid values are:<br>• SUNDAY<br>• MONDAY<br>• TUESDAY<br>• WEDNESDAY<br>• THURSDAY<br>• FRIDAY<br>• SATURDAY<br>• ANYDAY | String | 9 | Multiple | RW | No | To add or modify:<br>`ALU (userid) WHEN (DAYS(value))`<br>To delete:<br>`ALU userid WHEN (DAYS (ANYDAY))` |
| erRacUWhenTime<br>Time range when user can sign on to the system. | Time | 9 | Single | RW | No | To add or modify:<br>`ALU (userid) WHEN (TIME(value))`<br>To delete:<br>`ALU userid WHEN (TIME (ANYTIME))` |
| erUid<br>ID of user on RACF being created, updated, or deleted. | String | 8 | Single | RW | Yes | |
| erRacUIsROAudit<br>Specifies that a user has the ROAUDIT attribute. | String | 5 | Single | RW | No | To add or modify:<br>`ALU userid ROAUDIT`<br>To delete:<br>`ALU userid NOROAUDIT` |

### erRacConnect

This class represents the connection of a user to a group within RACF. The following connect object is associated with the base user object, and must have at least 1, but can have over 7,000 occurrences. Typically this number is no more than 100 and varies upon the customer environment.

*Table 24: erRacUser attribute information*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacConAuth<br>Whether this user is in REVOKED status, or not. | String | 7 | Single | RW | No | To add or modify:<br>`CO userid GROUPvalue AUTHvalue`<br>To delete:<br>`CO userid GROUPvalue AUTH (USE)` |
| erRacConCDate<br>Connect entry creation date. | Date | 7 | Single | R | No | |
| erRacConCount<br>Connect count. Max value of 65,535. | Integer | 5 | Single | R | No | |
| erRacConGroup<br>Name of group to which user is connected. | String | 8 | Single | RW | Yes | To add or modify:<br>`CO userid GROUPvalue`<br>To delete:<br>`REMOVE userid GROUP(value)` |
| erRacConIsADSP<br>User can automatically create discrete data set profiles. | String | 5 | Single | RW | No | To add or modify:<br>`CO userid GROUP(value) ADSP`<br>To delete:<br>`CO userid GROUP(value) NOADSP` |
| erRacConIsAudit<br>User has system Auditor ability. | String | 5 | Single | RW | No | To add or modify:<br>`CO userid GROUP(value) AUDITOR`<br>To delete:<br>`CO userid GROUP(value) NOAUDITOR` |
| erRacConIsGrpac<br>Enables group level access of UPDATE to the group under the High Level Qualifier of any data set profile that is created through ADSP by this user. | String | 5 | Single | RW | No | To add or modify:<br>`CO userid GROUP(value) GRPAC`<br>To delete:<br>`CO userid GROUP(value) NOGRPAC` |

*Table 24: erRacUser attribute information (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacConIsOper<br>User has system Operations ability (ability to read and modify any file). | String | 5 | Single | RW | No | To add or modify:<br>`CO userid GROUP(value) OPERATIONS`<br>To delete:<br>`CO userid GROUP(value) NOOPERATIONS` |
| erRacConIsSpec<br>User has system Special. System security Administrator. | String | 5 | Single | RW | No | To add or modify:<br>`CO userid GROUP(value) SPECIAL`<br>To delete:<br>`CO userid GROUP(value) NOSPECIAL` |
| erRacConLogtime<br>Time user last signed on, using this group as default group or specified group. | Time | | Single | R | No | |
| erRacConOwner<br>Owner of this connect entry. | String | 8 | Single | RW | Yes | To add or modify:<br>`CO userid GROUP(value) OWNER(value)` |
| erRafConResumDt<br>MM/DD/YY date field, indicates future date when this account is to be reactivated (RESUMEd). | Date | 8 | Single | R | No | To add or modify:<br>`CO userid GROUP(value) RESUME(value)`<br>To delete:<br>`CO userid GROUP(value) RESUME` |
| erRacConRevokDt<br>MM/DD/YY date field, indicates future date when this account is to be deactivated (revoked). | Date | 8 | Single | R | No | To add or modify:<br>`CO userid GROUP(value) REVOKE(value)`<br>To delete:<br>`CO userid GROUP(value) REVOKE` |

*Table 24: erRacUser attribute information (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacConUACC<br>Default universal access to all data set and TAPEVOL profiles that are created by this user. Valid Values are:<br>• NONE<br>• READ<br>• UPDATE<br>• CONTROL<br>• ALTER | String | 7 | Single | RW | No | To add or modify:<br>`CO userid GROUP(value) UACC(value)`<br>To delete:<br>`CO userid GROUP(value) UACC(NONE)` |
| erRacConXML<br>This attribute carries an XML string that represents all the data for a single connect entry. It carries all the information that comprises a RACF connect entry. This action occurs when the server flattens out all the data elements. | String | | Multiple | RW | Yes | |

**erRacGroup**

This class represents a group definition within RACF. The RACF group represents a group definition within the RACF database. Its presence is required to enable IBM Security Identity Governance and Intelligence to understand the RACF group tree structure to know what groups are within or outside of management policy. This information is read-only, and is not currently managed or updated by IBM Security Identity Governance and Intelligence. Although optional segments are provided in this documentation, their implementation is to be decided later.

*Table 25: erRacGrp attribute information*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacGrpCDate<br>Creation date of this group. | Date | 8 | Single | RO | Yes | |

*Table 25: erRacGrp attribute information (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacGrpData<br>Installation data, user-defined purpose | String | 225 | Single | RO | No | To add or modify:<br>`ALG userid DATA(value)`<br>To delete:<br>`ALG userid NODATA` |
| erRacGrpDFPAppl<br>DFP segment, DATAAPPL field. | String | 8 | Single | RO | No | To add or modify:<br>`ALG userid DFP(DATAAPPL(value))`<br>To delete:<br>`ALG userid DFP(NODATAAAPPL)` |
| erRacGrpDFPData<br>DFP segment, Data class. | String | 8 | Single | RO | No | To add or modify:<br>`ALG userid DFP(DATACLASS (value))`<br>To delete:<br>`ALG userid DFP(NODATACLASS)` |
| erRacGrpDFPMgmt<br>DFP segment, management class. | String | 8 | Single | RO | No | To add or modify:<br>`ALG userid DFP(MGMTCLASCLASS (value))`<br>To delete:<br>`ALG userid DFP(NOMGMTCLAS)` |
| erRacGrpDFPStor<br>DFP segment, storage class. | String | 5 | Single | RO | No | To add or modify:<br>`ALG userid DFP(STORCLASCLASS (value))`<br>To delete:<br>`ALG userid DFP(NOSTORCLAS)` |
| erRacGrpIsDFP<br>Indicates presence of DFP segment information. | String | 5 | Single | RO | No | To add or modify:<br>`ALG userid DFP`<br>To delete:<br>`ALG userid NODFP` |

*Table 25: erRacGrp attribute information (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacGrpIsOMVS<br>Indicates presence of OMVS segment information. | String | 5 | Single | RO | No | To add or modify:<br>`ALG userid OMVS`<br>To delete:<br>`ALG userid NOOMVS` |
| erRacGrpIsTME<br>Indicates presence of TME role segment information. | String | 5 | Single | RO | No | To add or modify:<br>`ALG userid TME`<br>To delete:<br>`ALG userid NOTME` |
| erRacGrpIsUni<br>Indicates that this group is a Universal Group (Unlimited number of users connected). | String | 5 | Single | RO | No | |
| erRacGrpName<br>Name of group to which user is connected. | String | 8 | Single | RO | Yes | |
| erRacGrpOMVSGid<br>OMVS Group ID. Valid values are 0 - 2,147,483,647. | Integer | 10 | Single | RO | No | To add or modify:<br>`ALG userid OMVS(GIDvalue)`<br>To delete:<br>`ALG userid OMVS(NOGID)` |
| erRacGrpOwner<br>Owner of this group. | String | 8 | Single | RO | Yes | To add or modify:<br>`ALG userid OWNER(value)` |
| erRacGrpSubgrp<br>Subordinate groups to this group. | String | 8 | Multiple | RO | No | |
| erRacGrpSuper<br>Superior group to this group. | String | 8 | Single | RO | Yes | To add or modify:<br>`ALG userid SUPGROUP(value)` |

*Table 25: erRacGrp attribute information (continued)*

| Attribute | Data type | Maximum length | Single or multiple value | Read or write | Required? | Commands |
|---|---|---|---|---|---|---|
| erRacGrpTMERole<br>Role groups that this group is part of. | String | 8 | Multiple | RO | No | To add or modify:<br>`ALG userid TME(ROLES(value))`<br>To delete:<br>`ALG userid TME(NOROLES)` |
| erRacGrpTUACC<br>Indicates whether Terminal Universal Access is used. | String | 5 | Single | RO | No | To add or modify:<br>`ALG userid TERMUACC`<br>To delete:<br>`ALG userid NOTERMUACC` |

## Registry settings

The adapter has several registry settings. See the table for these registry options, their descriptions, and values, if any.

To change the adapter registry settings, see "Modifying non-encrypted registry settings" on page 74.

*Table 26: Registry settings and information*

| Option attribute | Default value | Valid value | Function and meaning | Required |
|---|---|---|---|---|
| DATADIR | adapter_readwrite_home/data | adapter_readwrite_home/data | Specifies the USS adapter read/write home This parameter must be the read/write home as specified in the Disk location parameters panel during installation. This location is where the `registry.dat` and the `UDF.dat` files are stored. | Yes |
| DEBUG | TRUE | TRUE or FALSE | When set to TRUE, warning messages are returned to the IBM Security Identity Manager server for those attributes for which the request to add, delete, or modify is run successfully with return code 0, but informational messages are returned by RACF.<br>This is the default setting.<br>When set to FALSE, warning messages are NOT returned to the IBM Security Identity Manager server for those attributes for which the request to add, delete, or modify was executed successfully with return code 0, but information messages are returned by RACF. This setting is required to be set to FALSE when you use zSecure Command Verifier in debug mode. It can be useful when you are aware of a configuration issue but waiting for this issue to be resolved. For example, when you receive IKJ566441 messages and wait for the TSO segment to be added to the ISIAGNT account. It is still possible to manage accounts but not to perform reconciliations. | Yes. |

*Table 26: Registry settings and information (continued)*

| Option attribute | Default value | Valid value | Function and meaning | Required |
|---|---|---|---|---|
| DSJOB | 'hlq'.CNTL | Any data set accessible by the adapter RACF ID and optionally the SURROGAT RACF ID where the RECJOB JCL is stored | Specifies the data set where the RECOJOB is located. | Yes |
| ISIMEXIT | 'hlq'.EXEC | Any data set accessible by the adapter RACF ID and optionally the SURROGAT RACF ID where the ISIMEXIT/ISIMEXEC REXX scripts are stored | The adapter uses this value to initialize the ISIMEXIT/ISIMEXEC REXX scripts | Yes |
| LABELATTR | N/A | You can specify any attribute that holds a string value.<br>For example, `erracuname`, `erracuwaname`, or `erracuinstdata` | The value of the attribute specified in this field is copied into the value of the `erracacclabel` attribute. You can specify any attribute that holds a string value.<br>For example, `erracuname`, `erracuwaname`, or `erracuinstdata` | No |
| OPMODE | FULL | FULL<br>READ-ONLY<br>READ-ONLY-PWD | The value specified in this field determines the operations that the adapter supports.<br>Valid options are:<br>**`FULL (default)`**<br>The adapter supports all operations SEARCH/LOOKUP/ADD/DELETE/MODIFY<br>**`READ-ONLY`**<br>The adapter only supports SEARCH and LOOKUP operations<br>**READ-ONLY-PWD**<br>The adapter supports SEARCH, LOOKUP, and PASSWORD/PASSWORD PHRASE operations | No |
| PASSEXPIRE | TRUE | TRUE, FALSE, or TRUEADD | This attribute is the default action that the adapter must do when the adapter receives a password or pass phrase change request. TRUE indicates that passwords or pass phrases must be set as expired. FALSE indicates that passwords or pass phrases must be set as non-expired. When set to TRUEADD, a password or pass phrase for a new user is set to EXPIRED. A password or pass phrase is set on an existing user asset to non-expired. In each case, READ, or UPDATE access to the FACILITY class profile, IRR.PASSWORD.RESET is required. Note: If the RACF® attribute erRacuNoexpire is passed to the adapter, with TRUE or FALSE, this adapter option (PASSEXPIRE) is ignored. The setting of the erRacuNoexpire attribute is used. | |
| RACFRC | 60 | Any integer with a minimum value of 3 | The amount of time in seconds the adapter waits for the RECOJOB job to complete processing. | Yes |
| RECOSAVE | 'hlq'.SAVE | Any data set accessible by the adapter RACF ID and optionally the SURROGAT RACF ID | Specifies the data set where the intermediate reconciliation results are stored by RECOJOB. The adapter accesses these data set as soon as the status of RECOJOB is completed to collected and further process the results. | Yes |
| SCOPING | None | TRUE or FALSE | Scoping is automatically set to TRUE when the VSAM data set file name, which is required to perform scoped reconciliations, is configured during installation. See "Reconciliation Processor" in Chapter 1, “Overview,” on page 1. | No |

*Table 26: Registry settings and information (continued)*

| Option attribute | Default value | Valid value | Function and meaning | Required |
|---|---|---|---|---|
| SHORTCONNECT | FALSE | TRUE or FALSE | This attribute is not provided by default. You can add this attribute as a non-encrypted registry setting by using the adapter configuration tool.<br>When SHORTCONNECT is set to TRUE, the CONNECT entries, do not contain LOGON COUNT, CREATION DATE, LASTLOGON DATE. This setting enables the use of a simple string compare and mitigates the need for the CUSTOM JOIN DIRECTIVE.<br>1 | No |
| JOBCHAR | None | One character [A-Z] | If defined, this is the JOBCHAR added to the TSO SUBMIT command that initializes the RECOJOB processing. | False |
| Agent_UserLookup _MaxThreads | 3 | 1 or greater | Number of threads available for processing LOOKUP transactions. | False |
| DELEXP | TRUE | TRUE or FALSE | When the value of DELEXP is either not set or set to FALSE then, the export data set is deleted as soon as the reconciliation is complete. | No |
| LOKUSAVE | 'hlq'.LSAVE | Any data set accessible by the adapter RACF ID and optionally the SURROGAT RACF ID | Stores the intermediate single account lookup results. | Yes |
| CONGRP | FALSE | TRUE or FALSE | Controls the forwarding of connect group related account MODIFY operations to ISIMEXIT. | No |
| PROFDEL | FALSE | TRUE or FALSE | If set to TRUE the adapter attempts to delete data set profile prior to deleting the account | No |
| TSOCMD | TRUE | TRUE or FALSE | This attribute defines if tsocmd is used to call ISIMEXIT or IRXEXEC. Specify TRUE to use tsocmd or FALSE to use IRXEXEC. | Yes |

[1] The following example indicates the content of a single value, within the erRacConXML attribute. The items that are in bold are omitted when the SHORTCONNECT option is set to TRUE:

```
<CONNECT_ENTRY name="CONENTRY"><ADSP>FALSE</ADSP><AUDITOR>FALSE</AUDITOR>
<AUTHORITY>USE</AUTHORITY><DATE>200312101200Z</DATE><GRPACC>FALSE</GRPACC>
```

1 The following example indicates the content of a single value, within the erRacConXML attribute. The items that are in bold are omitted when the SHORTCONNECT option is set to TRUE:

```
<CONNECT_ENTRY name="CONENTRY">
<ADSP>FALSE</ADSP><AUDITOR>FALSE
</AUDITOR><AUTHORITY>USE
</AUTHORITY><DATE>200312101200Z
</DATE><GRPACC>FALSE</GRPACC>
<LAST_DATE>200312101200Z
</LAST_DATE><LOGON_COUNT>0
</LOGON_COUNT><OPERATIONS>FALSE
</OPERATIONS><OWNER>CONENTRY
</OWNER><RESUME_DATE>
200312101200Z</RESUME_DATE>
<REVOKE_DATE>200312101200Z
</REVOKE_DATE>
<REVOKED>FALSE</REVOKED>
<SPECIAL>FALSE</SPECIAL><UACC>
NONE</UACC></CONNECT_ENTRY>
```

This option addresses a policy implementation issue that occurs building a provisioning policy for RACF accounts. When a straight string compare is done between the “policy” version of a connect entry and the value in the erRac- ConXML, the policy returns a mismatch. This mismatch occurs because of the transient behavior of creation date, last logon date and time, logon count, and future revoke and resume dates. When this option is enabled, these dynamic attributes are omitted. The revoke and resume dates are omitted to prevent a RACF user from being RESUMEd because of differences between the connect entry and the policy.

**Note:** When the SHORTCONNECT option is not specified in the registry, the adapter acts as if it is set to TRUE.

```
<LAST_DATE>200312101200Z</LAST_DATE><LOGON_COUNT>0</LOGON_COUNT>
<OPERATIONS>FALSE</OPERATIONS><OWNER>CONENTRY</OWNER>
<RESUME_DATE>200312101200Z</RESUME_DATE><REVOKE_DATE>200312101200Z</REVOKE_DATE>
<REVOKED>FALSE</REVOKED><SPECIAL>FALSE</SPECIAL><UACC>NONE</UACC></CONNECT_ENTRY>
```

## Environment variables

The adapter consists of several environment variables. See the table for these variables, their descriptions and values, if any.

*Table 27: RACF Adapter environment variables*

| Environment variable | Description | Default value | Required |
|---|---|---|---|
| _CEE_RUNOPTS | Language environment runtime options | As defined in the installation script | Yes |
| _CEE_DMPTARG | Language environment DUMP locations | /tmp | Yes |
| LIBPATH | Specify the location of the Dynamic Link Library (DLL) and `.so` files. | None | Yes |
| PDU_ENTRY_LIMIT | Specify the maximum number of accounts that are kept in the main storage. | 2000. The range is 50-3000. | No |
| PROTOCOL_DIR | Specify the fully qualified location of the directory where the `.so` and `.dll` files are. | LIBPATH | No |
| REGISTRY | Specify the location of a specific registry file.<br>The registry path is the fully qualified path and the file name of the registry file. The registry name is the adapter name in uppercase, with `.dat` suffixed to the name. | Current® working directory. | No |

# Index

## A



## C

## D



## E



## I



## K



## L



## M



## O



## P



## R



## S

## T



## U



## W



## Z