IBM Security Verify Governance

zSecure RACF Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

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

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

- Results of the zSecure RACF CARLa scripts commands, which include the success or failure message of a request to the Identity server.
- Processes the requests to add, modify, or delete RACF user accounts by using the CKGRACF command interpreter.
- Single user lookups/ reconciliations where the filter is limited to one single account (`eruid=<specific_account>`) are processed by using the **REXX IRRXUTIL** interface to `R_Admin`.

The following figure describes the various components of the adapter.

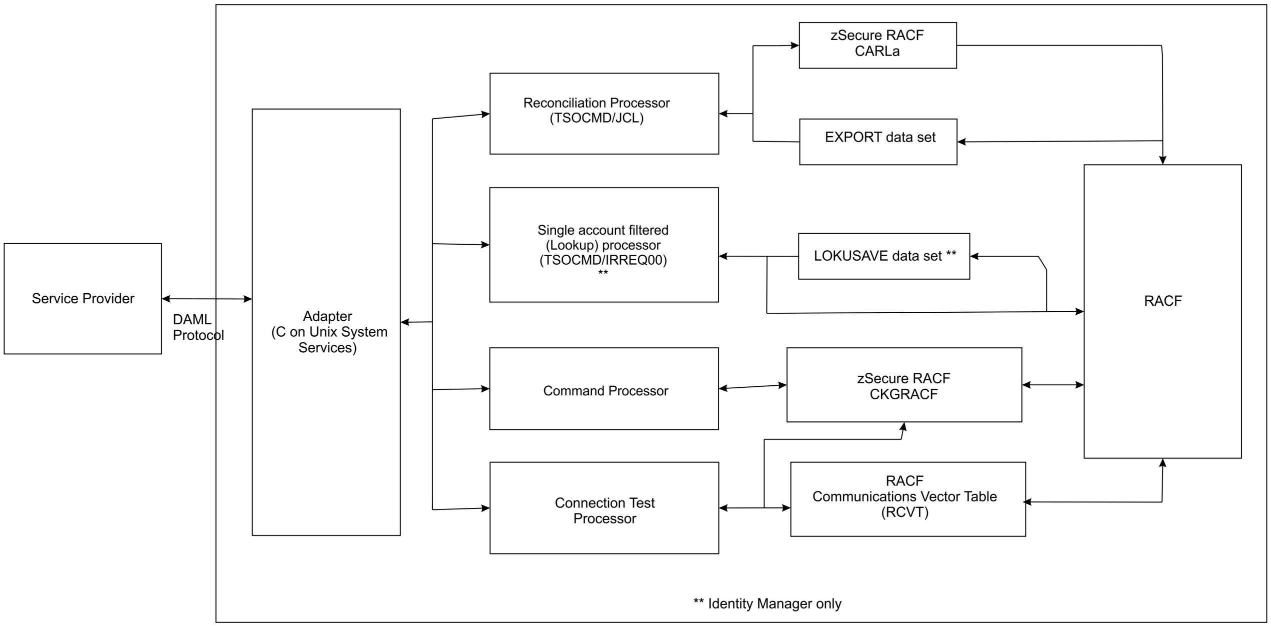

Service Provider
DAML Protocol
Adapter (C on Unix System Services)
Reconciliation Processor (TSOCMD/JCL)
Single account filtered (Lookup) processor (TSOCMD/IRREQ00) **
Command Processor
Connection Test Processor
zSecure RACF CARLa
EXPORT data set
LOKUSAVE data set **
zSecure RACF CKGRACF
RACF Communications Vector Table (RCVT)
RACF
** Identity Manager only

Figure 1. The zSecure RACF Adapter components

Adapter

Receives and processes requests from IBM Security Verify Governance. The adapter can handle multiple requests simultaneously. Each request results in the execution of a TSO/E or IRRSEQ00 based command transaction. The binary files of the adapter and related external files are in the UNIX System Services environment of MVS™.

Reconciliation Processor

Operates as a TSO-based command transaction that submits the reconciliation job (AGRJ6), which executes the CARLa scripts if the registry setting RUNREP is set to TRUE. The adapter runs the TSO/E commands from the UNIX System Services environment. It collects the results that are returned by the reconciliation job (AGRJ6) from the EXPORT data set specified during installation.

The server request is accompanied by a RACF user ID that is used to do the reconciliation. This user ID can be the agent ID or a SURROGAT ID. This user ID can be used for a partial reconciliation based on the scope of authority of that ID. For more information about scope of authority, see the *RACF Security Administrator's Guide*.

The adapter runs in "agent" mode and must be installed on z/OS. One adapter is installed for each RACF database and zSecure RACF product installation.

Command Processor

Operates as a mostly C-based interface to the R_Admin callable service based transaction for command execution.

For account DELETE operations, the processor uses `tsocmd` to verify whether the account has existing generic data set profiles to be deleted.

To remove resource profile permissions from an account, the processor uses **CKGRACF**. **CKGRACF** is required to run from an APF-authorized zSecure installation.

Connection Test Processor

The connection test processor is initialized when a connection test is executed on the Identity server. The processor collects version information from the adapter, RACF, and the zSecure RACF products that are installed on the z/OS system. It stores the information in the Identity server.

RACF version information is collected from the RACF Communications Vector Table (RCVT). The zSecure version information is collected by using the CARLa "SHOW CKRSITE" command, which is stored in the `adapter_readonly_home/bin/version.cmd` file.

The initial adapter release implemented CKGRACF to collect the zSecure version information. CKGRACF is replaced with CKRCARLA because it does not require an APF-authorized zSecure installation.

Adapter considerations

The zSecure 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.

To execute the TSO/E SUBMIT command, the RACF ID used by the adapter must have READ access on JCL in the TSOAUTH class.

CKGRACF must run APF-authorized. See “RACF user ID” on page 22.

The single account lookup uses services that are provided by the R_Admin callable service.

The R_admin callable service (IRRSEQ00), for RACF operator command processing, requires additional profile access. The R_admin callable service requires READ permissions to be defined for the ADAPTER user and SURROGAT user on the following profile:

Table 1. Class and Profile

CLASS	**PROFILE**
FACILITY	IRR.RADMIN.LISTUSER

Note:

- When you define the resource, it is required to use the full command name as shown in the examples.
- 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 during installation.
- An operational RACF ID might not be specified on the IBM Security Verify Governance service form when a request is issued. In this case, the RACF user ID that the adapter uses might require specific privileges that allow the execution of the zSecure RACF CARLa scripts and CKGRACF commands .

Related concepts

Adapter interactions with the server

Adapter interactions with the server

The zSecure RACF Adapter uses IBM Security Verify Governance to do user tasks on the IBM® RACF Security Server for z/OS. The adapter uses the TCP/IP protocol to communicate with IBM Security Verify Governance.

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

SSL requires digital certificates and private keys to establish communication between the endpoints. Regarding SSL, the zSecure 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 Verify Governance) 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 Verify Governance.

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 the Identity server. 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 zSecure RACF Adapter. To protect these ports with RACF protection, define the profiles in the RACF SERVAUTH resource class. Take note that applications run from the z/OS shell have a job name that is the started task name plus a one-character suffix. For example, when you are restricting port access with the PORT statement in the TCP/IP profile the job name has to be `<jobname>* or <jobname>?` to account for the suffix. For more information, see the z/OS Communications Server, IP Configuration Guide or https://www.ibm.com/support/pages/node/78095.

Related concepts

Adapter considerations
The zSecure 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.

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 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

Related concepts

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

Software downloads
Log in to your account on the IBM Passport Advantage website and download the software.

Prerequisites

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

Table 2. Prerequisites to install the adapter

Operating System	See the Release Notes® for the supported software versions.
Managed Resource	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 Verify Governance server to the z/OS Server. This test helps troubleshooting installation problems.
Identity server	See the Release Notes for the supported software versions.
Required authority	You must have system SPECIAL authority to complete the installation procedure.

Table 2. Prerequisites to install the adapter (continued)

Installation panels	As the installation includes the panels for both the RACF and the zSecure RACF panels, the required space for the installation panels are allocated with the following parameters: `new track space(15,1) dir(5) lrecl(255) recfm(f,b) blksize(0)`
TSO Region	The configuration account requires a TSO REGION of at least 2048000 to be able to use the adapter configuration tools such as agentCfg and regis.

Organizations with multiple zSecure RACF installations must have an adapter installed for each zSecure RACF production installation on the z/OS server containing the installation. You can manage a zSecure RACF product installation with a single instance of the zSecure 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 Identity server might require updates if the alternate image is known through a different IP address.

Related concepts

Roadmap for Adapter Development Kit based adapters, using ISPF
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Software downloads
Log in to your account on the IBM Passport Advantage website and download the software.

Software downloads

Log in to your account on the IBM Passport Advantage website and download the software.

Go to IBM Passport Advantage.

See the corresponding *IBM Security Verify Governance Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

Roadmap for Adapter Development Kit based adapters, using ISPF
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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.

Use the following worksheet to document the information required to install and configure the zSecure RACF Adapter. Complete this worksheet before you start the installation and configuration. Make a copy of the worksheet for each zSecure RACF Adapter instance you install.

Table 3. Installation worksheet

z/OS data set name	The z/OS data set high-level qualifier for upload and installation.
Adapter instance name	The default is *VERAGNT*. 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 UNIX System Services file system location that is used to store the adapter binaries. The default is `/usr/lpp/zsecracf`. The read-only home and the read/write home must specify different locations. If they are the same then the installation might fail. Allocate at least 60 Mb of free space to the read/only home.
USS Adapter read/write home	The UNIX System Services file system location that is used to store the adapter log file and to register intermediate reconciliation results and start scripts. The default is `/var/ibm/zsecracf`. 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 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.
Started task name	The *VERAGNT* member is the sample JCL provided for the adapter startup. The component of the *started task name* must indicate the adapter instance name. The *started task name* must be limited to 7 characters to eliminate ambiguity when shutting down the adapter.
TSO account number	A *TSO account number* is required during installation because the adapter uses TSO/E for processing.

Table 3. Installation worksheet (continued)

zSecure &CPREF product data set prefix	The zSecure product data set prefix for the zSecure installation, which the adapter instance manages.
zSecure configuration include member	The zSecure C2R$PARM member for the zSecure installation, which the adapter instance manages.
CARLa report output data set name	Data set for storing the CARLa Report output.
RACF Complex and Organizational Unit name	Complex and Organizational Unit names to be used during reconciliation to identify the source complex and organizational unit to the IBM Security Verify Governance server.

Installing the zSecure RACF Adapter involves the following tasks.

Uploading the adapter package

Upload the adapter package on z/OS to begin the adapter installation.

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 4. Files used

File description	**File name**
XMI file	`VERRACF.UPLOAD.XMI`
Partitioned Data Set (PDS) file	*`userid`*`.VERRACF.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 'VERRACF.UPLOAD.XMI' RECFM(F)
```

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

```
RECEIVE INDA(VERRACF.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 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.

Procedure

1. Log on to the z/OS operating system that hosts the adapter.
2. Run the following command from the ISPF 6 option. The *userid* is your TSO user ID..

```
EXEC ‘userid.ZSECRACF.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 5. 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 Identity server and the adapter, import the adapter profile and create an adapter service.

Related tasks

Uploading the adapter package
Upload the adapter package on z/OS to begin the adapter installation.

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. See "Installing the ISPF dialog" on page 11

About this task

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

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.

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

   IBM Security Verify Adapter for RACF or zSecure RACF

     Initial Customization

   1  RACF
                 If you want to install a standard RACF adapter, select this option.


       2  zSecure RACF
          If you want to install the zSecure RACF Adapter, select this option.

       X  Exit
   ```

   a. Select 2 to install the zSecure RACF Adapter or X to exit.

   b. Press `Enter` to continue to the welcome screen.

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

IBM Security Verify  zSecure RACF Adapter

   Licensed Material - Property of IBM
   (C) Copyright IBM Corp. 2010,2020

   All Rights Reserved.
   U.S. Government users - RESTRICTED RIGHTS - Use, Duplication, or Disclosure restricted
by GSA-ADP schedule contract with IBM Corp.
```

c. Press `Enter` to continue to the **Initial Customization** selection panel.

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

IBM Security Verify  zSecure RACF Adapter

  Initial Customization

    1 Start Customization
      To start the installation, select this option.

    X Back
```

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

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

```
 AGRP1 ------------------- zSecure 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 performed choices 1 and 2 before performing
        this choice.

     4  Save All Variables.
        Save variable changes to a z/OS 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.

```
AGRP01 ------------------- zSecure RACF Adapter Customization --------------------
 Option ===>                                           Location:  1->1-> 1

  Load Variables

     The IBM supplied defaults are in IBMUSER.VERRACF.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.

     ===>  IBMUSER.VERRACF.CONFIG
```

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

```
AGRP012 ------------------- zSecure RACF Adapter Customization --------------------
 Option ===>                                           Location:  1->1-> 2

  Specify or Alter variables for this configuration.

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

     2 ** Adapter specific parameters.
          Define / alter IBM Security Verify
Governance server to adapter runtime parameters.

     3 ** zSecure specific parameters
          Define / alter zSecure runtime parameters.

     4 ** Operations specific parameters.
          Define / alter Add, Delete or Modify runtime parameters.

     5 ** ISIMEXIT attribute parameters
          Select attributes for ISIMEXIT.

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

       ** 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.

```
AGRP0121 ------------------- zSecure RACF Adapter Customization --------------------
 Option ===>

   Input Data Sets

    Fully qualified data set name of the UPLOAD data set.
     ===> VERRACF.UPLOAD

   Enter z/OS Unix directories.

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

    USS Adapter read/write home
     ===> /var/ibm/zsecracf
```

Fully qualified data set name of the UPLOAD data set
: Specifies the name of the data set that you received earlier. For example, `IBMUSER.VERRACF`.

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.

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 communication parameters** to define or alter the adapter-specific run time parameters.

```
AGRP122 ------------------- zSecure RACF Adapter Customization --------------------
 Option ===>

Adapter communication parameters

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

   Adapter authentication ID (internal)         ===> agent

   Adapter authentication password (internal)   ===> agent

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

   Disable TLS1.0                               ===> TRUE

   Disable TLS1.1                               ===> TRUE
```

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

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

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 59.

Disable TLS1.0
: Disables or enables TLS1.0 support. The default value is TRUE, which disables TLS1.0.

Disable TLS1.1
: Disables or enables TLS1.1 support. The default value is TRUE, which disables TLS1.1.

10. Press **PF3** (Cancel) or **Enter** after final input (Accept) to return to the **Specify or Alter variables for this configuration** panel.
11. Select zSecure specific parameters to set the reconciliation specifics.

```
AGRP123 ------------------- zSecure RACF Adapter Customization --------------------
 Option ===>

 zSecure RACF Environment

Reconciliation should run report job AGRJ6 ?
(TRUE/FALSE)
==> TRUE

zSecure CPREF product data set prefix
===> CKR.VERSION

zSecure CKRPARM run-time data set
(Must be Cataloged)

===> IBMUSER.VERSION.CKRPARM
zSecure configuration include member

===> C2R$PARM
Data set storing the CARLa Report output

===> ZSECRACF.EXPORT

RACF Complex name ===> PROD

RACF Organizational Unit name ===>
MAINFRAME
```

Reconciliation should run report job AGRJ6
If you specify TRUE, then the reconciliation process runs this job. It writes the data to the EXPORT data set configured at Data set storing the CARLa Report output. If you specify FALSE, the adapter assumes there is a process to schedule frequent runs of AGRJ6 and the latest report output can be retrieved from the EXPORT data set configured at Data set storing the CARLa Report output.

zSecure CPREF product data set prefix
Specifies the &CPREF zSecure product data set prefix.

zSecure CKRPARM run-time data set
Specifies the zSecure CKRPARM data set location.

zSecure configuration include member
Specifies the location of the C2R$PARM configuration member specific to this zSecure RACF installation.

Data set storing the CARLa Report output
Specifies the location from which the adapter collects the zSecure CARLa report output. See “Reconciliation should run report job AGRJ6” on page 16.

RACF COMPLEX name
Specifies the security complex name. This information is used to define the source of the user account data that is collected by the adapter to the Identity server.

RACF Organizational Unit name
Specifies the organizational unit name that is used for user account data collected from this specific security complex. This information is used to define organizational unit for the user account data collected by the adapter to the Identity server.

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

    Press **PF3** to return to the Initial Installation panel.
13. Select Operations specific parameters.

```
AGRP124 ------------------- zSecure RACF Adapter Customization --------------------

 Operations specific parameters

     Expire passwords                              ===> TRUE

     Expire pass phrases                           ===> TRUE

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

     Delete data set profiles before deleting user accounts?       ===>  TRUE

     Max wait time in seconds for AGRJ6 to complete
    ===> 60

    Optional JOBCHAR to be used for AGRJ6
    ===>

    Temporary single account lookup data set name
     ===> IBMUSER.ZSECRACF.LSAVE
```

Expire passwords
Specify TRUE to set the password to expire when modifying a password for an existing account. Specify FALSE to set the password as non-expired.

Expire pass phrases
Specify TRUE to set the password phrases to expire when modifying a password phrase for an existing account. Specify FALSE to set the password phrases as non-expired.

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

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.

Max wait time in seconds for AGRJ6 to complete
If the adapter is configured to run the report job AGRJ6, it uses the TSO SUBMIT and TSO STATUS commands to determine whether the job is submitted and when it completed. The **WAIT time in seconds** specifies the amount of time in seconds the adapter retries the TSO STATUS command to verify whether the job completed ("ON OUTPUT QUEUE" status).

Optional JOBCHAR to be used for AGRJ6
Optional. You can modify the `jobcard` for AGRJ6 to meet the organizations standards and optionally specify an allowed JOBCHAR used for the TSO SUBMIT command. If used, the `adapterID` or `surrogatID` are not allowed to exceed 7 characters.

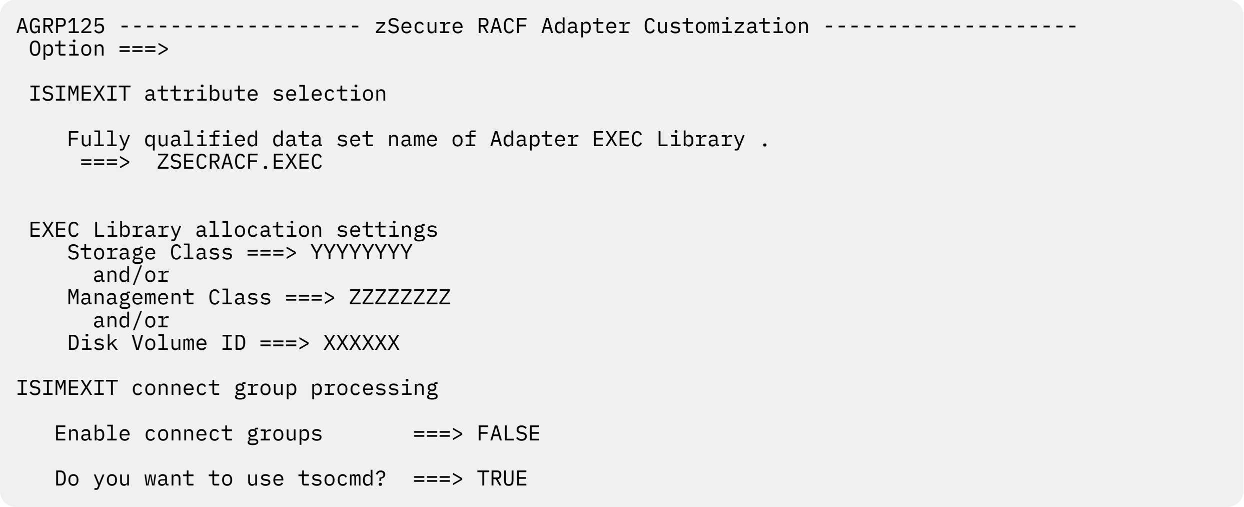
Note: A JOBCHAR is required either in the JOBNAME in the JCL or in the JOBCHAR registry setting if you change the name of the JOB from AGRJ6 to the name of an existing User ID.

See The JOB statement.

Temporary single account lookup 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. Please note single account lookups / reconciliations using a filter that matches only one single account, are only supported on Identity Manager.

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.

    This screen allows you to specify storage allocation and connect group forwarding parameters to be used for the ISIMEXIT Rexx script.



```
AGRP125 ------------------- zSecure RACF Adapter Customization --------------------
 Option ===>

 ISIMEXIT attribute selection

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


 EXEC Library allocation settings
    Storage Class ===> YYYYYYYY
      and/or
    Management Class ===> ZZZZZZZZ
      and/or
    Disk Volume ID ===> XXXXXX

ISIMEXIT connect group processing

   Enable connect groups       ===> FALSE

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

Fully qualified data set name of Adapter EXEC Library
Specify the fully qualified data set name for the EXEC library.

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.

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.

    Press **PF3** to return to the Initial Installation Panel.

17. Select **Adapter specific parameters** to define or alter the adapter-specific run time parameters.

```
AGRP126 ------------------- zSecure RACF Adapter Customization --------------------
 Option ===>

 Adapter specific parameters

    Name of adapter instance                      ===> VERAGNT

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

    Adapter authentication ID (internal)          ===> agent

    Adapter authentication password (internal)    ===> agent

    PDU backlog limit                             ===> 2000

    RACF user ID for the adapter             ===> VERAGNT

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

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

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

    Default Language Environment (CEE) dump location
     ===>
```

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.

PDU backlog limit
Specifies the number of entries that can be sent to the Identity server. The higher the number the greater the throughput on reconciliations but this also results in higher storage utilization.

RACF user ID for the adapter
Specifies the RACF user ID assigned to the adapter task.

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

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

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

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.

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.

```
AGRP14 ------------------- zSecure 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.
    ===> ZSECRACF.CNTL

    Data set name for data elements required by generated job
    streams.
    ===> ZSECRACF.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.

```
AGRP13 ------------------- zSecure RACF Adapter Customization --------------------
 Option ===>

  Save variables to a data set.

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

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

    ===> IBMUSER.ZSECRACF.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.VERRACF.CNTL(INSTRUCT)` data set. Follow the instructions specified in the `hlq.VERRACF.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 59.

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 Identity server and the adapter, import the adapter profile and create an adapter service.

Related tasks

Uploading the adapter package
Upload the adapter package on z/OS to begin the adapter installation.

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

Ensure that TCP/IP is active before you start the adapter.

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

About this task

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

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

- Communication between the Identity server and the adapter

- **`agentCfg`** utility

Note: You can define _BPX_SHAREAS=YES in the `/etc/profile` directory. This setting enables the adapter to run in a single address space, instead of multiple address spaces. Newer releases of z/OS create two address spaces with this environment variable set. See "z/OS UNIX System Services considerations" on page 72.

Procedure

1. To start the adapter, run the z/OS console start command:

   ```
   START VERAGNT
   ```

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 the following z/OS stop command to stop the adapter:

     ```
     STOP VERAGNT
     ```

     or

     ```
     P VERAGNT
     ```

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

     ```
     P VERAGNT5
     ```

   - If a z/OS STOP command does not stop the adapter, run the following z/OS CANCEL command to stop the adapter:

     ```
     CANCEL VERAGNT
     ```

     or

     ```
     CANCEL VERAGNT5
     ```

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 Identity server and the adapter, import the adapter profile and create an adapter service.

Related tasks

Uploading the adapter package
Upload the adapter package on z/OS to begin the adapter installation.

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 Identity server and the adapter, import the adapter profile and create an adapter service.

Related tasks

Uploading the adapter package
Upload the adapter package on z/OS to begin the adapter installation.

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` .

To use the single account lookup feature in Identity Manager, the R_admin callable service requires READ permission to be defined for the ADAPTER user and/or SURROGAT user on the following profile in class FACILITY:

- `IRR.RADMIN.LISTUSER`

CKGRACF must run APF-authorized. For more information, see the following links:

- CKG740I
- PARMLIB command

CKGRACF must be added to the currenlty active `IKJTSOXX PARMLIB` member as in the example below:

```
IKJTSO00
AUTHCMD NAMES( /* AUTHORIZED COMMANDS */ +
CKGRACF /* ZSECURE */ +
```

To activate the changes made to the `IKJTSOXX` member run the following command:

```
TSO PARMLIB UPDATE(**)
```

Next, add the ‘`hql.SCKRLOAD`’ library to the APF-authorized libraries. See Updating the APF list.

For example:

```
setprog apf,add,dsname=CONSUL.VERSION.SCKRLOAD,sms
```

To allow CKGRACF to run **PERMIT** commands, the adapter ID requires UPDATE permission on class XFACILIT profile CKG.CMD.CMD.EX.PERMIT.

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.

zSecure profiles
CKR.** profiles can allow or prohibit the use of functions. Verify your organizations' installation for the list of profiles, which the ADAPTERID or SURROGATID requires READ access.

z/OS V2R3 specific requirements

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 zSecure RACF database.
- The IBM Security Verify Governance has multiple service instances, each representing a different business unit within the organization.

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

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

If the adapter RACF user ID is *VERAGNT*, and the surrogateRACF 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(IGIAGNT) 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 zSecure RACF user has scope of authority over a specific business unit.

When surrogate user IDs are used, RACF data is fetched under the authority of the surrogate RACF user ID. The authority of the RACF user ID, which the adapter runs, 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.

zSecure profiles
CKR.** profiles can allow or prohibit the use of functions. Verify your organizations' installation for the list of profiles, which the ADAPTERID or SURROGATID requires READ access.

z/OS V2R3 specific requirements

zSecure profiles

CKR.** profiles can allow or prohibit the use of functions. Verify your organizations' installation for the list of profiles, which the ADAPTERID or SURROGATID requires READ access.

Note: The CKR.READALL profile is used to invoke the so called restricted mode.

If the XFACILIT profile CKR.READALL exists and the ADAPTERID or SURROGATID does not have READ access to it, it is used automatically in restricted mode. The zSecure queries return profiles and settings that RACF allows it to read.

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.

z/OS V2R3 specific requirements

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.

zSecure profiles

CKR.** profiles can allow or prohibit the use of functions. Verify your organizations' installation for the list of profiles, which the ADAPTERID or SURROGATID requires READ access.

Communication configuration

To establish communication between the 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
Upload the adapter package on z/OS to begin the adapter installation.

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 Identity server. Use this option for importing adapter profiles.

Before you begin

The file to be imported must be a Java™ archive (JAR) file.

About this task

A target profile defines the type of managed resource that IBM Security Verify Governance can manage. Target profiles are also called Identity Brokerage adapter profiles. The profile definition files are provided with the various Identity Brokerage Adapters. The target profile must be imported into Verify Governance because it defines the types of resources that the Verify Governance server can manage.

Note: In previous versions of the product, a target profile was referred to as a target type or an adapter profile.

The Identity Brokerage target definition profile is a Java archive (JAR) file that contains the following information:

- Target information, including definitions of the account provisioning operations, such as add, delete, suspend, or restore.
- Target provider information, which defines how IBM Security Verify Governance communicates with the managed resource.
- Schema information.
- Account and target forms and the label for the attributes for creating targets and requesting accounts on those targets. The forms and labels are displayed in the user interface of the Enterprise Connectors module.

The Identity Brokerage profile definition file is used to create a target profile on the IBM Security Verify Governance server and to establish communication with the Identity Brokerage adapter. If the Identity Brokerage target definition file is not imported, you cannot manage the profiles.

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.

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

To import a Identity Brokerage target profile, complete the following steps.

Procedure

1. Log in to the IBM Security Verify Governance Administration Console.

   The Administration Console is displayed.
2. From the Administration Console, select **Enterprise Connectors**.

   The Enterprise Connectors module is displayed.
3. Select **Manage** > **Profiles**.

   A list of profiles is displayed on the **Profiles** tab.
4. Optional: Click **Filter** icon to toggle the filter on to refine your search results, or 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**.

   The import pager is displayed.
6. On the **Import** page, complete the following steps:

   a) Select **Profile**.

   b) Click **Browse** to locate the JAR file that you want to import.

      For example, if you are installing the IBM Security Verify Governance adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.

   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 27.
- Create and enable a connector that uses the target profile. See “Adding a connector” on page 28.

If you are unable to 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. Import the target profile again.

Related tasks

Importing attribute mapping file

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

Adding a connector

After you import the adapter profile on the IBM Security Verify Governance server, add a connector so that IBM Security Verify Governance server can communicate with the managed resource.

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

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.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Governance account attributes.

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 IBM Security Verify Governance 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**.

Related tasks

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Adding a connector
After you import the adapter profile on the IBM Security Verify Governance server, add a connector so that IBM Security Verify Governance server can communicate with the managed resource.

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

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.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Governance account attributes.

Adding a connector

After you import the adapter profile on the IBM Security Verify Governance server, add a connector so that IBM Security Verify Governance server can communicate with the managed resource.

Before you begin

Complete "Importing the adapter profile" on page 25.

Note: If you migrated from IBM Security Verify Governance 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 Verify Governance 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 IBM Security Verify Governance 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 IBM Security Verify Governance. For more information, see "Enabling connectors" on page 29.

Related tasks

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

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

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

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.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Governance account attributes.

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 6. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in IBM Security Verify Governance.	"Adding a connector" on page 28.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 30.

Procedure

To enable a connector, complete these steps:

1. Log in to the IBM Security Verify Governance 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 IBM Security Verify Governance.

Related tasks

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

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

Adding a connector
After you import the adapter profile on the IBM Security Verify Governance server, add a connector so that IBM Security Verify Governance server can communicate with the managed resource.

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.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Governance account attributes.

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 IBM Security Verify Governance 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 IBM Security Verify Governance V5.2.3:

1. Log in to the IBM Security Verify Governance 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 29.

      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**.

Related tasks

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Importing attribute mapping file

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

Adding a connector
After you import the adapter profile on the IBM Security Verify Governance server, add a connector so that IBM Security Verify Governance server can communicate with the managed resource.

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

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Governance account attributes.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Governance 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 IBM Security Verify Governance 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 IBM Security Verify Governance 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 Verify Governance product documentation.
6. Map the following attributes for **Chaneel-Write To** and **Chaneel-Read From**

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

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

Related tasks

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

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

Adding a connector
After you import the adapter profile on the IBM Security Verify Governance server, add a connector so that IBM Security Verify Governance server can communicate with the managed resource.

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

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.

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 Identity server.
2. Run a full reconciliation from the Identity 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 Identity server and the adapter, import the adapter profile and create an adapter service.

Related tasks

Uploading the adapter package
Upload the adapter package on z/OS to begin the adapter installation.

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.

See Chapter 3, “Installing,” on page 9.

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 about arguments, see t_accessinghelp.dita#accessinghelp/cmdarg in t_accessinghelp.dita.

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

Starting the adapter configuration tool

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

Procedure

1. Log on to the TSO on the z/OS operating system that hosts the adapter.
2. 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.
3. 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.

   ```
   # cd /var/ibm/adapter_readwritedir/bin
   ```

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

   ```
   agentCfg -agent VERAGNT
   ```

   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
   ```
5. At **Enter configuration key for Agent *adapter_name***, 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. See "Changing protocol configuration settings" on page 38.

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 7. 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

Viewing configuration settings

Use the **Viewing 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**. "Starting the adapter configuration tool" on page 37.
2. At the **Main menu** prompt, type A to display the configuration settings for the adapter.
3. Press any key to return to the **Main Menu**.

Changing protocol configuration settings

The adapter uses the DAML protocol to communicate with the 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.

To configure a secure environment, use Secure Shell Layer (SSL) and install a certificate.

Procedure

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 37.
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.

```
DAML Protocol Properties
--------------------------------------------------------------------
A. USERNAME             ****** ;Authorized user name.
B. PASSWORD             ****** ;Authorized user password.
C. MAX_CONNECTIONS      100    ;Max Connections.
D. PORTNUMBER           47770  ;Protocol Server port number.
E. USE_SSL              FALSE  ;Use SSL secure connection.
F. SRV_NODENAME         ----- ;Event Notif. Server name.
G. SRV_PORTNUMBER       9443 ;Event Notif. Server port number.
H. HOSTADDR             ANY;Listen on address (or "ANY")
I. VALIDATE_CLIENT_CE   FALSE ;Require client certificate.
J. REQUIRE_CERT_REG     FALSE ;Require registered certificate.
K. READ_TIMEOUT         0 ;Socket read timeout (seconds)
L. DISABLE_TLS10        TRUE ;Disable TLS 1.0 and earlier
M  DISABLE_TLS11        TRUE ;Disable TLS 1.1
N  DISABLE_TLS12        TRUE ;Disable TLS 1.2

X. Done

Select menu option:
```

5. Change the protocol value:
   a) Type the letter of the menu option for the protocol property to configure. Table 8 on page 39 describes each property.

Table 8. Options for the DAML protocol menu

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

Table 8. Options for the DAML protocol menu (continued)

Option	**Configuration task**
B	Displays the following prompt `Modify Property 'PASSWORD':` Type a password, for example, `admin`. The IBM Security Verify Governance server uses this value to connect to the adapter.
C	Displays the following prompt: `Modify Property 'MAX_CONNECTIONS':` Enter the maximum number of concurrent open connections that the adapter supports. The default value is 100. **Note:** This setting is sufficient and does not require adjustment.
D	Displays the following prompt: `Modify Property 'PORTNUMBER':` Type a different port number. The IBM Security Verify Governance server uses the port number to connect to the adapter. The default port number is 45580.
E	Displays the following prompt: `Modify Property 'USE_SSL':` Type TRUE to use a secure SSL connection to connect the adapter. When you set this option, you must install a certificate. For more information, see "Installing the certificate from file" on page 65. Type FALSE to not use a secure SSL connection. The default value is FALSE.
F	Displays the following prompt: `Modify Property 'SRV_NODENAME':` Type a server name or an IP address of the workstation where you installed the IBM Security Verify Governance server. This value is the DNS name or the IP address of the IBM Security Verify Governance server that is used for event notification and asynchronous request processing. **Note:** If your operating system supports Internet Protocol version 6 (IPv6) connections, you can specify an IPv6 server.

Table 8. Options for the DAML protocol menu (continued)

Option	**Configuration task**
G	Displays the following prompt: `Modify Property 'SRV_PORTNUMBER':` Type a different port number to access the IBM Security Verify Governance server. The adapter uses this port number to connect to the IBM Security Verify Governance server. The default port number is 9443.
H	The HOSTADDR option is useful when the system, where the adapter is running, has more than one network adapter. You can select which IP address the adapter must listen to. The default value is ANY.
I	Displays the following prompt: `Modify Property 'VALIDATE_CLIENT_CE':` Type TRUE for the IBM Security Verify Governance server to send a certificate when it communicates with the adapter. When you set this option, you must configure options D through I. Type FALSE for the IBM Security Verify Governance server to communicate with the adapter without a certificate. **Note:** • The property name is VALIDATE_CLIENT_CERT. It is truncated by **`agentCfg`** to fit in the screen. • You must use the certTool to install the appropriate CA certificates and optionally register the IBM Security Verify Governance server certificate. For more information about using the certTool, see "Managing the SSL certificates" on page 62.
J	Displays the following prompt: `Modify Property 'REQUIRE_CERT_REG':` This value applies when option I is set to TRUE. Type TRUE to register the adapter with the client certificate from the IBM Security Verify Governance server before it accepts an SSL connection. Type FALSE to verify the client certificate against the list of CA certificates. The default value is FALSE. For more information about certificates, see Configuring SSL authentication.

Table 8. Options for the DAML protocol menu (continued)

Option	Configuration task
K	Displays the following prompt: `Modify Property 'READ_TIMEOUT':` Specify the timeout value in seconds. The default value is 0 which specifies that no read timeout is set. **Note:** READ_TIMEOUT prevents open threads in the adapter, which might cause "hang" problems. The open threads might be caused by firewall or network connection problems and might be seen as TCP/IP ClosWait connections that remain on the adapter. If you encounter such problems, set the value of READ_TIMEOUT to a time longer than the IBM Security Verify Governance timeout, which is the maximum connection age DAML property on IBM Security Verify Governance and less than any firewall timeout. The adapter must be restarted because READ_TIMEOUT is set at adapter initialization.
L	Displays the following prompt: `Modify property 'DISABLE_TLS10':` Type FALSE to use the TLSv1.0 protocol to connect to the adapter. The default value is TRUE.
M	Displays the following prompt: `Modify Property 'DISABLE_TLS11':` Type FALSE to use the TLSv1.1 protocol to connect the adapter. The default value is TRUE.
N	Displays the following prompt: `Modify Property 'DISABLE_TLS12':` Type FALSE to use the TLSv1.2 protocol to connect the adapter. The default value is FALSE.

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**.

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

Configuring event notification

Use the **Event Notification** option to set the event notification for the Identity server.

About this task

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

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.

zSecure RACF for z/OS does not support adapter-based event notification.

Procedure

1. Access the **Agent Main Configuration Menu**.
2. Type C to display the **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 menu option that you want to change.

   Note:

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

Table 9. Options for the event notification menus

Option	Configuration task
A	If you select this option, the adapter updates the Identity server with changes to the adapter at regular intervals. If **Enabled - Adapter** is selected, the adapter code processes event notification by monitoring a change log on the managed resource. When the option is set to: **Disabled** All options except **`Start event notification now`** and **`Set attributes`** that are to be reconciled are available. Pressing A changes the setting to **`Enabled - ADK`**. **Enabled - ADK** All options are available. Pressing A changes the setting to **`Disabled`** or if your adapter supports event notification, to **`Enabled - Adapter`**. **Enabled - Adapter** All options are available, except **`Time interval between reconciliations`** **`Set processing cache size`** **`Start event notification now`** **`Reconciliation process priority`** **`Set attributes to be reconciled`** Pressing A changes the setting to **`Disabled`**. Type A to toggle between the options. **Note:** The adapter does not support adapter-based event notification, **`Enabled - Adapter`**. Therefore, this option is not listed in the event notification menu.

B	Displays the following prompt:
	`Enter new interval`
	`([ww:dd:hh:mm:ss])`
	Type a different reconciliation interval. For example, `[00:01:00:00:00]`
	This value is the interval to wait after the event notification completes before it is run again. The event notification process is resource intense, therefore, this value must not be set to run frequently. This option is not available if you select **`Enabled - Adapter`**.

C	Displays the following prompt: `Enter new cache size[50]:` Type a different value to change the processing cache size. This option is not available if you select **`Enabled - Adapter`**.
D	Displays the Event Notification Entry Types Menu. This option is not available if you select **Disabled or Enabled - Adapter**. For more information, see "Setting event notification triggers" on page 45.
E	Displays the following prompt: `Enter new thread priority [1-10]:` Type a different thread value to change the event notification process priority. Setting the thread priority to a lower value reduces the impact that the event notification process has on the performance of the adapter. A lower value might also cause event notification to take longer.

Table 9. Options for the event notification menus (continued)

Option	Configuration task
F	Displays the following prompt: `Enter new context name:` Type the new context name and press **Enter**. The new context is added.
G	Displays a menu that lists the available contexts. For more information, see “Modifying an event notification context” on page 46.
H	Displays the Remove Context Menu. This option displays the following prompt: `Delete context context1? [no]:` Press **Enter** to exit without deleting the context or type `Yes` and press **Enter** to delete the context.

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

J	When you select the **`Set password attribute names`**, you can set the names of the attributes that contain passwords. These values are not stored in the state database and changes are not sent as events. This option avoids the risk of sending a delete request for the old password in clear text when IBM Security Verify Governance changes a password. Changes from IBM Security Verify Governance 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 Verify Governance log files.

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

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

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

Setting event notification triggers

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

Procedure

1. Access the **Agent Main Configuration Menu**.
2. At the Event Notification Menu, type E to display the Event Notification Entry Types Menu.

```
Event Notification Entry Types
-------------------------------------------
A. erZsecRacfAcct
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) **erUId (b) **erZsrUOwner (c) **erZsrUDfltgrp
(d) **erZsrUName (e) **erZsrOrgUnit (f) **erZsrUComp
(g) **erZsrURevokeDate (h) **erZsrUResumeDate (i) **erAccountStatus
(j) **erUid (k) **erZsrProfAccessList (l) **erZsrGrpNameList
rev page 1 of 7 (n)ext
-----------------------------
X. Done
```

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

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

Modifying an event notification context

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

About this task

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

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

Procedure

1. Access the **Agent Main Configuration Menu**.
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 10. 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 47.
B	Configuring the target DN for event notification contexts	See "Configuring the target DN for event notification contexts" on page 47.

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 Verify Governance 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**.
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:
```

zSecure 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 Verify Governance Service Form.

Configuring the target DN for event notification contexts

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

About this task

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

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

Procedure

1. Access the **Agent Main Configuration Menu**.
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 11 on page 48 describes each DN element.

   Table 11. 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 Governance DN Location* which is specified during the IBM Security Verify Governance server installation.

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

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.

About this task

The default configuration key is **`agent`**. Ensure that your password is complex.

Procedure

1. Access the **Agent Main Configuration Menu**.
2. At the **Main menu** prompt, typeD.
3. Take one of the following actions:
   - Change the value of the configuration key and press **Enter**.
   - Press **Enter** to return to the **Main Configuration Menu** without changing the configuration key.

Results

The following message is displayed:

```
Configuration key successfully changed.
```

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

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 the activity logging settings, IBM Security Verify Governance maintains a log file, `VERAGNT.log`, of all transactions. By default, the log file is in the read/write `log` directory.

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

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/zsecracf/log).
C. Activity Log File Name (current: VERAGNT.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 the 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 12 on page 49 describes each option.
   - Press **Enter** to return to the **Agent Activity Logging Menu** without changing the value.

Table 12. 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. Type A to toggle between the options.
B	Displays the following prompt: `Enter log file directory:` Type a different value for the logging directory such as `/var/ibm/zsecracf/log`. When the logging option is enabled, details about each access requests are stored in the logging file in this directory.
C	Displays the following prompt: `Enter log file name:` Type a different value for the log file name. When the logging option is enabled, details about each access request are stored in the logging file.

Table 12. Options for the **`activity logging`** *menu (continued)*

Option	Configuration task
D	Displays the following prompt: `Enter maximum size of log files (mbytes):` Type a new value such as `10`. The oldest data is archived when the log file reaches the maximum file size. File size is measured in megabytes. It is possible for the activity log file size to exceed the disk capacity.
E	Displays the following prompt: `Enter maximum number of log files to retain:` Type a new value up to 99, 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. Type `F` to toggle between the options.
G	If this option is set to enabled, the adapter maintains a detailed log file of all transactions. The detailed logging option must be used for diagnostic purposes only. Detailed logging enables more messages from the adapter and might increase the size of the logs. 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. 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. Type `I` to toggle between the options.

Changing registry settings

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

About this task

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

Procedure

1. Access the **Agent Main Configuration Menu**.
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
```

For a list of valid registry options, their values and descriptions, see “ Registry settings” on page 109.

3. Type the letter of the preferred menu option.

Modifying non-encrypted registry settings

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

Before you begin

See “Changing registry settings” on page 50.

Procedure

1. At the **Agent Registry Menu**, type A.

   The **Non-encrypted Registry Settings Menu** is displayed.

```
Agent Registry Items
-------------------------------------------------
01. BINDIR                 '/u/lpp/zsecracf/bin'
02. DATADIR                '/var/ibm/zsecracf/data'
03. DSJOB                  'IBMUSER.VERRACF.CNTL'
04. ENROLE_VERSION         '4.0'
05. EXPORT                 'IBMUSER.VERRACF.EXPORT'
06  PWDEXP                 'TRUE'
07  PWPEXP                 'TRUE'
08. RUNREP                 'TRUE'
09. WAIT                   '60'
-------------------------------------------------
                Page 1 of 1
A. Add new attribute
B. Modify attribute value
C. Remove attribute
X. Done
Select menu option:
```

Table 13. 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.

Table 13. Non-encrypted registry keys (continued)

Key	Description
DEBUG	The default setting is TRUE. When set to TRUE, warning messages are returned to the Identity 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. When set to FALSE, warning messages are NOT returned to the Identity 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. 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.
ENROLE_VERSION	Specifies the version of IBM Security Verify Governance Identity Manager.
ISIMEXIT	Specifies the data set where the ISIMEXIT REXX scripts are located.
LABELATTR	The value of the attribute specified in this field is copied into the value of the `erzsracclabel` attribute. You can specify any attribute that holds a string value. For example, `erzsruname`, `erzsruwaname`, or `erzsruinstdata`
OPMODE	The value specified in this field determines the operations that the adapter supports. Valid options are: **`FULL (default)`** The adapter supports all operations SEARCH/LOOKUP/ADD/DELETE/ MODIFY **READ-ONLY** The adapter only supports SEARCH and LOOKUP operations **READ-ONLY-PWD** 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. 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.

Table 13. Non-encrypted registry keys (continued)

Key	Description
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: • CONNECT • REMOVE • PW • ALU • ALG • ADDUSER • DELUSER • PHRASE • 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).
TSOCMD	Specify TRUE to use tsocmd or FALSE to use IRXEXEC. The default value is TRUE.

2. Type the letter of the preferred menu option

Table 14. Attribute configuration option description

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

3. Depending on your selection in Step 3, follow any of these steps:
   - If you selected option A or B, type the registry item value and press **Enter**.
   - If you selected option C, type the registry item name and press **Enter**.

Results

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

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.

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

Procedure

1. Access the **Agent Main Configuration Menu**.
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 15 on page 54.

*Table 15. Options for the **Advanced Settings Menu***

Option	Description
A	Forces the adapter to submit only 1 request at a time. The default value is FALSE.
B	Limits the number of Add requests that can run simultaneously. The default value is 3.
C	Limits the number of Modify requests that can run simultaneously. The default value is 3.
D	Limits the number of Delete requests that can run simultaneously. The default value is 3.
E	Limits the number of Search requests that can run simultaneously. The default value is 3.
F**	Limits the number of Lookup requests that can run simultaneously. The default value is 3.
G**	Determines whether the adapter can do the pre-exec and post-exec functions. The default value is FALSE. **Note:** Enabling this option is a potential security risk.
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 set to FALSE.

Note: ** These options are not available for the zSecure RACF Adapter and must always be set to FALSE.

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

Viewing statistics

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

About this task

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

Procedure

1. Access the **Agent Main Configuration Menu**.
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

-----------------------------------------------------------------
09/23/2015 000000 000000 000000 000000 000000 000004
09/24/2015 000000 000000 000000 000000 000000 000003
-----------------------------------------------------------------
X. Done
```

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

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 VERAGNT -codepages
```

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

Procedure

1. Access the **Agent Main Configuration Menu**.
2. At the **Main menu** prompt, type I.

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

```
VERAGNT 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 VERAGNT

Enter configuration key for Agent 'VERAGNT':

        VERAGNT 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

        VERAGNT 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

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

        A.  Codepage Configure.

        X.  Done

        Select menu option:x
```

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

Accessing help and additional options

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

About this task

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

Procedure

1. Access the **Agent Main Configuration Menu**.
2. At the **Main menu** prompt, typeX to display the UNIX System Services command prompt.
3. Type **agentCfg** `-help` to display the help menu and list of arguments.

```
Usage:
-version              ;Show version
-hostname <value>     ;Target nodename to connect to
                      (Default:127.0.0.1)
-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
-portnumber <value>   ;Specified agent's TCPIP 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 16. Arguments and their description

Argument	Description
-version	Use this argument to display the version of the **agentCfg** tool.
-hostname <value>	Use the **-hostname** argument with one of the following arguments to specify a different host: • **-findall** • **-list** • **-tail** • **-agent** Enter a host name or IP address as the value.
-findall	Use this argument to search and display all port addresses 44970 - 44994 and their assigned adapter names. This option times out the unused port numbers and can cause the search to take several minutes to complete. Add the **-hostname** argument to search a remote host.

Table 16. Arguments and their description (continued)

Argument	Description
-list	Use this argument to display the adapters that are installed on the local host of the zSecure RACF Adapter. By default, the first time you install an adapter, it is either assigned to port address 44970 or to the next available port number. You can then assign all the later installed adapters to the next available port address. After the software finds an unused port, the listing stops. Use the **-hostname** argument to search a remote host.
-agent <value>	Use this argument to specify the adapter that you want to configure. Enter the adapter name as the value. Use this argument with the **-hostname** argument to modify the configuration setting from a remote host. You can also use this argument with the **-tail** argument.
-tail	Use this argument with the **-agent** argument to display the activity log for an adapter. Add the **-hostname** argument to display the log file for an adapter on a different host.
-portnumber <value>	Use this argument with the **-agent** argument to specify the port number that is used for connections for the **agentCfg** tool.
-netsearch <value>	Use this argument with the **-findall** argument to display all active adapters on the z/OS operating system. You must specify a subnet address as the value.
-codepages	Use this argument to display a list of available code pages.
-help	Use this argument to display the Help information for the **agentCfg** command.

4. Type **agentCfg** before each argument that 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 Verify Governance server must be 44970. The output is similar to the following example:

```
Agent(s) installed on node '127.0.0.1'
-----------------------
VERAGNT     (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'
------------------
VERAGNT        (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.

Configuring SSL authentication

To establish a secure connection between the adapter and the Identity server, configure SSL authentication for connections that originate from the Identity server or from the adapter.

To establish a secure connection between the adapter and the Identity server, configure SSL authentication for connections that originate from the 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

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

About this task

Client authentication is not set on either application. The IBM Security Verify Governance 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 Verify Governance server. IBM Security Verify Governance uses the installed CA certificate to validate the certificate that is sent by the adapter.

Complete this task 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:

      i) Create a certificate signing request (CSR) and private key. The certificate is created with an embedded public key and a separate private key. The private key is stored in the PENDING_KEY registry value.

      ii) Submit the CSR to the certificate authority by using the instructions from the CA. When you submit the CSR, specify that you want the root CA certificate, which is returned with the server certificate.

2. On the IBM Security Verify Governance, perform one of these steps:

   - If you used a signed certificate that is issued by a well-known CA:

a. Ensure that the IBM Security Verify Governance stored the root certificate of the CA (CA certificate) in its keystore.

b. If the keystore does not contain the CA certificate, extract the CA certificate from the adapter and add it to the keystore of the server.

- If you generated the self-signed certificate on the IBM Security Verify Governance, 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 Verify Governance.

Configuring certificates for two-way SSL authentication

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

Before you begin

Configure the adapter and IBM Security Verify Governance server for one-way SSL authentication. See Configuring certificates 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 Verify Governance 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 2 on page 60, the IBM Security Verify Governance server operates as Application A and the IBM Security Verify Governance adapter operates as Application B.

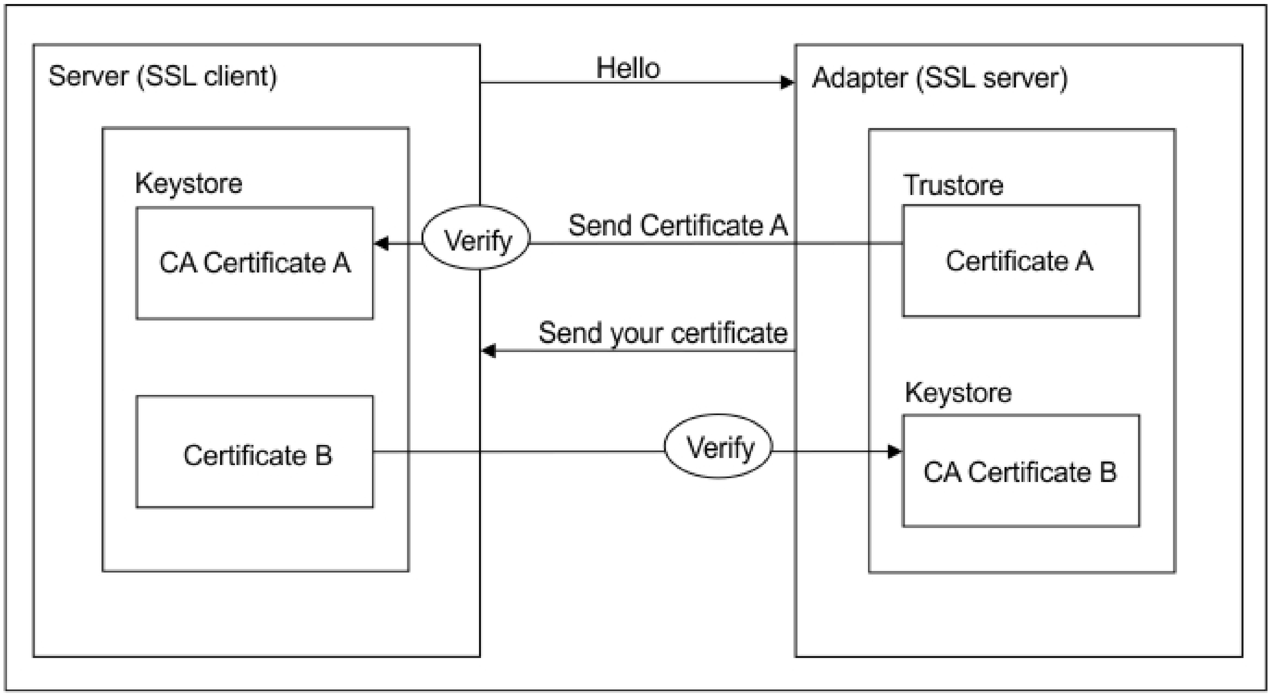


Figure 2. Two-way SSL authentication (client authentication)

Procedure

1. On the IBM Security Verify Governance server:
   a) Create a CSR and a 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 is extracted from the keystore of the IBM Security Verify Governance server to the adapter.

Results

Each application has its own certificate and private key. Each application also has the certificate of the CA that issued the certificates.

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 Verify Governance server, to send an event notification. For example, the adapter initiates the connection and the web server responds by providing its certificate to the adapter.

Figure 3 on page 61 describes how the adapter operates as an SSL server and an SSL client. To communicate with the IBM Security Verify Governance server, the adapter sends its certificate for authentication. To communicate with the web server, the adapter receives the certificate of the web server.

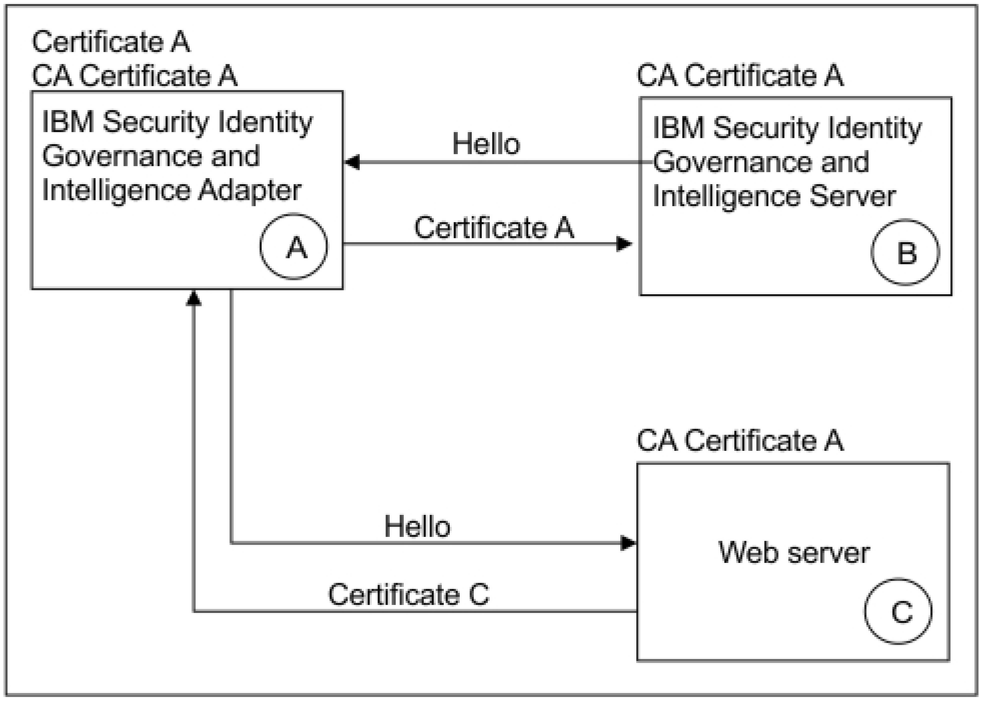

Certificate A
CA Certificate A
IBM Security Identity Governance and Intelligence Adapter
A
CA Certificate A
Hello
Certificate A
IBM Security Identity Governance and Intelligence Server
B
CA Certificate A
Hello
Certificate C
Web server
C

Figure 3. Adapter operating as an SSL server and an SSL client

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

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 can have the software send an event notification when the adapter initiates a connection to the web server that is used by the IBM Security Verify Governance server.

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.

The DAML SSL implementation offers SSL protocol specific configuration options such as disabling specific SSL protocols as described in "Changing protocol configuration settings" on page 38. The DAML SSL also offers the option to specify the cipher suites it allows for SSL communication. The adapters cipher suite is configured in the adapter start script and by default defined as `ISIM_ADAPTER_CIPHER_LIST = HIGH`.

You can modify the value for the `ISIM_ADAPTER_CIPHER_LIST` environment variable to meet your organizations requirements. For an overview of all possible options, please consult the OpenSSL website: https://www.openssl.org/docs/man1.0.2/man1/ciphers.html.

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. At a OMVS command prompt, change to the read/write `/bin` directory of the adapter . If the adapter is installed in the default location for the read/write directory, run the following command..

   ```
   cd /var/ibm/adapter_name/bin
   ```

2. Type certTool at the prompt. The **Main menu** is displayed:

```
Main menu - Configuring agent: IGIAGNT
 ------------------------------
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:
```

3. 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 Verify Governance 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 Verify Governance 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 Verify Governance.

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 to display the following message and prompt:

   ```
   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**, use 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 from file

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/zsecracfagent/data`
2. At the **Main menu** of the certTool utility, type B. The following prompt is displayed:

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

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

Results

The certificate is installed in the 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.

Procedure

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

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

3. At **Enter name of PKCS12 file**, type the full path to the PKCS12 file that has the certificate and private key information and press **Enter**. You 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

After you delete the CA certificate from the `DamlCACerts.pem` file, 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 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 those requests that present a registered certificate when client validation is enabled. Use the **List registered certificates** certTool option to list all registered certificates that are accepted for communication.

Procedure

1. At the **Main menu** of the certTool utility, type H.
2. The utility displays the registered certificates. 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 perform specific functions according to your requirements with the following REXX execs that are provided with the adapter installation:

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. Please see the RACF Installation and Configuration guide for additional details.

IBM Security Identity Manager Resources
: Check the "Learn" section of the IBM Security Identity Manager Knowledge Center for links to training, publications, and demos.

Support for customized adapters

The integration to the Identity Manager server - the adapter framework - is supported. However, IBM does not support the 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

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

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

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

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

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

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

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

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

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

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

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

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

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

The 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 zSecure RACF commands to accomplish the function. You might run a valid TSO command if it does not prompt for a terminal user for input.

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

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

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

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

The listed information is available to the EXIT.

Table 17. ISIMEXIT processing information

Parameter #	Meaning	Possible value	Availability
1 Verb	Verb Indicates what operation is calling the exit.	ADD, MODIFY, SUSPEND, RESTORE, or DELETE.	Always
2 Object	Object The object name of the transaction.	USER indicating a zSecure RACF user object that is processed.	Always
3 Prepost	Prepost Qualifies whether this entry is PRE or POST processing entry to the exit.	BEFORE or AFTER.	Always
4 Account	Name The name of the RACF object.	The RACF user ID that is processed.	Always
5 Transid	Transactionid (Bigint)	A unique identification number for the server re- quest that is being processed.	Always
6 Add1	Dfltgrp :The RACF user ID default group.	The value that is specified from the Identity server for the default group of this user.	Only at PRE ADD or POST ADD exit. Not available for DELETE processing.
	Operation: CONNECT or REMOVE	Connect an account to a connect group or remove an account from a connect group.	Only when enabled during installation for ADD and MODIFY operations.
7 Add2	Owner: The RACF user ID owner.	The owner for the account to be created.	Only at PRE ADD or POST ADD exit. Not available for DELETE processing.
	Connect Group: the name of the group for a CON- NECT or REMOVE operation	The name of the connect group for a CONNECT or REMOVE operation.	Only when enabled during installation for ADD and MODIFY operations.

```
TSO statements can be executed by placing them in between double quotations.
To give some examples:
z = outtrap(lines.)
"SEARCH CLASS(DATASET) FILTER("name".**)"
z = outtrap(off)
To allocate a file in SYSOUT (which will show in the SDSF output queue as ISIAGNTX
or SURROGATX ):
"ALLOCATE FILE(ISIOUT) SYSOUT(A)"
(use QUEUE and EXECIO to write output to ISIOUT in the above example)
```

Using the Regis Tool

Start the Regis tool to 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 **ovms** command. Press `Enter` to enter the UNIX System Services environment.

   Note: You can also use a telnet session to enter the UNIX System Services environment.
4. In the command prompt window, 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 **`./regis -<option>`** command.

   The following options are available for the Regis tool:

   ```
   -version                    ;show regis version

           -registry       < value >   ;Registry File

           -encryptkey     < value >   ;Encryption key for string data

           -setstring      < value >   ;Set Registry String, [key::value]

           -getstring      < value >   ;Get Registry String

           -create                     ;Create Registry (Default:registry)

           -list           < value >   ;List Registry Contents (Default:registry)

           -delete         < value >   ;Delete Registry key

           -script                     ;Produce output for scripting

           -protocol       < value >   ;Protocol (Default:DAML)

           -installpath    < value >   ;Set agent's install path

           -property       < value >   ;Property name for protocol

           -value          < value >   ;Argument value

           -logdir         < value >   ;Agent's logfile directory

           -logfile        < value >   ;Agent's logfile name

           -mainproperty   < value >   ;Set main property

           -instanceclass  < value >   ;Create instance class [class::item::encrypt].

           -instanceset    < value >   ;Create instance class [class::instance::item::value]
   ```

   The `-registry <readwrite_home/data/<adapterid.dat>` option is required for all options except `-version`.

Regis Command Examples

Examples can be found in installation job ‘hlq’.CNTL(J4).

Modifying DAML protocol properties

```
/var/ibm/isi/bin/regis -reg /var/ibm/isi/data/ISIAGENT.dat -protocol DAML -property PASSWORD
-value newpassword

/var/ibm/isi/bin/regis -registry /var/ibm/isi/data/ISI.DAT -protocol daml -list
```

Modifying non-encrypted registry settings

```
/var/ibm/isi/bin/regis -reg /var/ibm/isi/data/ISIAGENT.dat -setstring  PASSEXPIRE::TRUE
```

Modifying main properties

```
/var/ibm/isi/bin/regis -reg /var/ibm/isi/data/ISIAGENT.dat -mainproperty Agent_MaxFile -value  5

/var/ibm/isi/bin/regis -reg /var/ibm/isi/data/ISIAGENT.dat -mainproperty Agent_Debug -value TRUE

/var/ibm/isi/bin/regis -reg /var/ibm/isi/data/ISIAGENT.dat  -mainproperty Agent_Detail -value TRUE
```

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 `IGIAGNT` and `IGIAGNT1`. In this case, the task must be stopped by issuing the **`stop`** command to the task `IGIAGNT1`. 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.

Configuration notes

The zSecure RACF Adapter can handle multiple requests simultaneously. Learn how the adapter processes specific attributes and requests and how it interacts during the processing of some of the requests.

AUTOID support

For 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*.

Password phrases

When you set passwords from the 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 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 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 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 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
```

Shared UID support

For 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 Verify Governance to define UIDs to multiple users, you must add the zSecure 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 zSecure RACF user ID set in the **PERMIT** command is either the adapter ID or the surrogate ID that is used to run the zSecure RACF command.

If surrogate zSecure 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 zSecure RACF user ID that starts the adapter

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

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`.

MFA Factors and Tags

The adapter supports MFA tags which are defined as a single string value of the `erracumfatagval` attribute.

The value must be defined as:

```
FACTOR|TAG|VALUE|STATUS
```

, where only the STATUS is optional.

For example:

```
AZFRADP1|RADUSERID|IBMUSER|ACTIVE

AZFSIDP1|SIDUSERID|IBMUSER|NOACTIVE
```

MFA factors can be specified as | separated strings that include the status of the factor. For example:

```
AZFRADP1|ACTIVE

AZFSIDP1|NOACTIVE
```

For more information on z/OS RACF MFA configuration, see:

- https://www.ibm.com/docs/en/zos/2.5.0?topic=zos-configuring-racf-mfa
- https://www.ibm.com/docs/en/zma/2.2.0?topic=z-multi-factor-authentication-22

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.

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 49.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

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

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

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.

Errors during installation
Errors that occur during installation.

Troubleshooting Profile Issues
If you experience issues opening an account form after upgrading to the latest release , it might be required to start the design forms editor, open the zSecure RACF account form and select save. You are not required to make any changes to the form.

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 18. Example of Adapter log details

Details	**Example values**
Installation path	`/var/ibm/`*`zsecracf`*
Adapter log name	*VERAGNT*
Log location	`/usr/itim/log/`
Log files	• *VERAGNT*`.log` • *VERAGNT*`.log_001` • *VERAGNT*`.log_002` • *VERAGNT*`.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 37.

Related concepts

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

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.

Errors during installation
Errors that occur during installation.

Troubleshooting Profile Issues
If you experience issues opening an account form after upgrading to the latest release , it might be required to start the design forms editor, open the zSecure RACF account form and select save. You are not required to make any changes to the form.

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

Memory allocation errors

The adapter stops processing when it encounters the memory allocation error message.

```
BSE:_ermAlloc: ERROR: malloc FAILED: size 60
```

These messages indicate the abort because of the memory allocation error.

- `ERR: zSecRacfSearch: Entry creation returned failure`
- `ERR: zSecRacfSearch: reconciliation ABORTED`

The following final error message is written to the adapter log:

```
ERR: FATAL memory error encountered, shutting down now
```

Memory allocation or *malloc* errors are often caused by a z/OS Language Environment (LE) HEAP size shortage. When the *malloc* errors occur, use these following settings for the adapter. Add these settings to the adapter start script, which is located in the `read_write_home/bin` folder:

```
RPTOPTS(ON),RPTSTG(ON)
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,)'
```

`RPTOPTS(ON),RPTSTG(ON)`is optional. Add it only if you want to enable the logging of diagnostic data to the adapter's STC.

When the RACF commands are executed by using the R_Admin callable service IRRSEQ00, all errors that RACF returns are recorded in the adapter log. If a command cannot be executed, the adapter records the SAF return code, the RACF return code, and RACF reason codes in the adapter log as depicted in the following example:

```
ERR:15/05/01 11:48:47 issueRadmin: safRC = 8, racfRC = 8 racfReason = 24,
returning rc =5
```

In the example, the ADAPTERID or SURROGATID does not have permission to all of the required profiles described in “Access configuration” on page 22. For more information about the return and reason codes, see *z/OS Security Server RACF Callable Services* in the z/OS Knowledge Center.

`agentCfg` configuration key minimum characters

A configuration key is not allowed to be less than 5 characters. Otherwise, the following message is displayed when you use **`agentCfg`** to configure an active adapter:

```
Configuration key too short - 5 characters minimum. Aborting...
```

After which, the **`agentCfg`** processing aborts.

Registry file initialization

Initialization of the registry file for the following scenarios is logged in the z/OS syslog during adapter initialization.

1. The registry file that is configured in the shell script that 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:

   ```
   zSecRacfAgent: Registry file specified by environment
   REGISTRY is’<adapter_read_write_home>/data/<adapter_name>.dat’
   zSecRacfAgent : REGISTRY does not exist
   zSecRacfAgent: 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:

   ```
   zSecRacfAgent: Registry files pecified by environment
   REGISTRY is’<adapter_read_write_home>/data/<adapter_name>.dat’
   zSecRacfAgent : FATAL ERROR: REGISTRY file open error: EDC5111I Permission
   denied.
   zSecRacfAgent: can’t continue without access to the
   registry file r a c fAg e n t : exiting process
   ```

3. The registry does exist but the adapter cannot access part of the path. In this event the adapter aborts initialization and the following messages are written to the syslog:

   ```
   zSecRacfAgent: Registry file specified by environment
   REGISTRY is’<adapter_read_write_home>/data/<adapter_name>.dat’
   zSecRacfAgent : FATAL ERROR: REGISTRY file stat error:
   EDC5111I Permission denied.
   zSecRacfAgent: can’t continue without access to the
   registry file zSecRacfAgent : 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:

   ```
   zSecRacfAgent: WARNING no REGISTRY file specified by the
   environment zSecRacfAgent: Creating a new registry file
   zSecRacfAgent : 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 because 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, start the adapter directly from the console. All messages that are written to either the syslog or in the adapter log is displayed on the console from which you started the adapter. To start the adapter in console mode, run all export commands as configured in the shell script that is used to start the adapter. This task ensures that all libraries are available to the adapter. Run the following command to start the adapter:

```
/<adapter_readonly_home/lpp/bin/zSecRacfAgent -name <adapter_name> -registry
<adapter_readwrite_home>/data/<adapter_name>.dat -console
```

CKGRACF returns rc 20

`CKG740I 20` CKGRACF must run APF-authorized. See “RACF user ID” on page 22.

CKGRACF returns rc 8

`CKG604I 08` Access UPDATE to command resource XFACILIT CKG.CMD.CMD.EX.PERMIT denied for command in PARM string.

`CKG107I 08` Command ended with result code 8.

`CKG111I 08` Highest result code was 8.

See “RACF user ID” on page 22.

Server messages

The following table contains warnings or errors that the adapter returns to the server.

Table 19. 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 zSecRacfSearch: pthread_security_ np() create failed. errno2=0BE800D8: EDC5139I Operation not permitted	PERMIT READ access for *VERAGNT* on BPX.SERVER in CLASS FACILITY
zSecRacfSearch : 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 *VERAGNT* on BPX.SRV.<SURROGATID> in CLASS SURROGAT
zSecRacfSearch : failed to create RECOJOB thread	DETAILAdapter log: tsoCmd: result is IKJ56644I NO VALID TSO USERID, DEF AUL T 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 20.
	The adapter returned an error status for a bind request. Status code: invalid credentials adapter error message: `Authentication Failed`	Verify that the adapter authentication ID and password match the installed values. See the screen for Adapter-specific parameters in “Running the ISPF dialog” on page 12.
	An IO error occurred sending a request. Error: `com.ibm.daml.jndi. JSSESocketConnection . HANDSHAKE_FAILED:`	If SSL is enabled, check the configuration. See “Configuring SSL authentication” on page 59. The adapter log contains details about the certificates that are loaded during initialization.

Table 19. Error messages, warnings, and corrective actions (continued)

Error message or warning	Additional warnings, messages, or information	Corrective action
`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 20
tsoCmd: result is YOUR TSO ADMINISTRATOR MUST AUTHORIZE USE OF THIS COMMAND	Not applicable.	PERMIT READ access for *VERAGNT* on JCL in CLASS TSOAUTH For example: PE JCL CLASS(TSOAUTH) ID(IGIAGNT) ACCESS(READ)SETROPTS RACLIST(TSOAUTH) REFRESH
tsoCmd: RECOJOB was not submitted	tsoCmd: result is *<result string>* zSecRacfSearch: failed to initiate reco_open	Verify whether the result string is a standard TSO message as defined in SYS1.MSGENU(IKJSCHEN). If a custom exit that returns a non-standard message is implemented, exclude the reconciliation job from this exit.
LDAP: error code 92		Increase the size of the transaction log. 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 `adapterid`.

Related concepts

Techniques for troubleshooting problems
Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

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.

Errors during installation
Errors that occur during installation.

Troubleshooting Profile Issues
If you experience issues opening an account form after upgrading to the latest release , it might be required to start the design forms editor, open the zSecure RACF account form and select save. You are not required to make any changes to the form.

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

Errors during installation

Errors that occur during installation.

Regis process loops; creating new *Regis* processes

The error occurs when no distinct locations are specified for the adapter's *readonly_home_directory* and *readwrite_home_directory*. It causes the *Regis* script to be overwritten by the *Regis* binary during installation. To resolve this issue, specify a different location for each of the two directories.

Related concepts

Techniques for troubleshooting problems
Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

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.

Troubleshooting Profile Issues
If you experience issues opening an account form after upgrading to the latest release , it might be required to start the design forms editor, open the zSecure RACF account form and select save. You are not required to make any changes to the form.

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

Troubleshooting Profile Issues

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

Related concepts

Techniques for troubleshooting problems
Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem.

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.

Errors during installation
Errors that occur during installation.

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
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.

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.

Errors during installation
Errors that occur during installation.

Troubleshooting Profile Issues
If you experience issues opening an account form after upgrading to the latest release , it might be required to start the design forms editor, open the zSecure RACF account form and select save. You are not required to make any changes to the form.

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 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 ISIM 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
```

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
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.

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.

Errors during installation
Errors that occur during installation.

Troubleshooting Profile Issues
If you experience issues opening an account form after upgrading to the latest release , it might be required to start the design forms editor, open the zSecure RACF account form and select save. You are not required to make any changes to the form.

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 and operations

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network. There are several operations that can be used on the adapter attributes.

Reconciliation operation

The information is sent to the adapter by the Identity server. You identify the attributes to IBM Security Verify Governance service when you define the Access Request Form for access through Request Maintenance.

Adapter attributes by object

Note: Reconciliations return group data, RACF Resource Profile access data, and user data.

- erzSecRacfAcct
- erzSecRacfGrp
- erzSecRacfResource

erzSecRacfAcct

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

Table 20. erzSecRacfAcct adapter attributes

Adapter Attribute	Description	Length	Internal Type
erUId	RACF account	8	ISUX
erZsrUOwner	RACF account owner	8	ISU0
erZsrUDfltgrp	RACF account's default group	8	ISU0
erZsrUName	RACF account name	20	ISU0
erZsrOrgUnit	Organizational Unit for the RACF account	10	ISU0
erZsrUComp	Complex for the RACF account	8	ISU0
erZsrURevokeDate	Future revoke date for the RACF account	10	ISU0
erZsrUResumeDate	Future resume date for the RACF account	10	ISU0
erAccountStatus	Current account status	1	ISU0
erUid	RACF account	8	ISU1

Table 20. erzSecRacfAcct adapter attributes (continued)

Adapter Attribute	Description	Length	Internal Type
erZsrProfAccessList	List of RACF resource profiles and access that is granted to an account or group	265	ISU1
erZsrGrpNameList	List of RACF connect groups for the RACF account	8	ISU1
erzsruiscicsseg	CICS Segment exists?	1	0230
erZsrConXml	Connect Groups	2048	0205
erzsrucicsopid	CICS Operator ID	3	0230
erzsrucicsprty	CICS Operator Priority	5	0230
erzsrucicsopclas	CICS Operator Classes	3	0231
erzsrucicsisforc	XRF Force	1	0230
erzsrucicstimout	CICS Session Time-out	5	0230
erzsruislangseg	Language Segment exists?	1	0240
erzsrulangprime	Primary Language	3	0240
erzsrulangsec	Secondary Language	3	0240
erzsruisomvsseg	Unix System Services Segment exists?	1	0270
erzsruomvsuid	Maximum Processor Time	10	0270
erzsruomvshome	Home directory	1023	0270
erzsruomvsshell	Shell Program Name	1023	0270
erzsruomvscpu	Maximum Processor Time	10	0270
erzsruomvsstor	Maximum address space size, in bytes	10	0270
erzsruomvsfiles	Maximum files per process	10	0270
erzsruomvsproc	Maximum processes	10	0270
erzsruomvsthread	Maximum threads per process	10	0270
erzsruomvsmmap	Maximum storage for memory mapped files	10	0270
erzsruistsoseg	TSO Segment exists?	1	0220
erzsrutsoacct	TSO Account Number	40	0220
erzsrutsocmd	TSO Initial Command	80	0220
erzsrutsodest	Default JES destination	8	0220

Table 20. erzSecRacfAcct adapter attributes (continued)

Adapter Attribute	Description	Length	Internal Type
erzsrutsohold	Default JES sysout hold class	1	0220
erzsrutsojob	Default JES execution class	1	0220
erzsrutsoproc	Default TSO logon procedure	8	0220
erzsrutsosize	Requested TSO region size	10	0220
erzsrutsomsg	Default JES sysout message class	1	0220
erzsrutsomax	TSO maximum region size	10	0220
erzsrutsosout	Default JES sysout class	1	0220
erzsrutsoudata	TSO user data (4 hexidecimal digits)	4	0220
erzsrutsounit	Default unit name for allocation	8	0220
erzsrucredate	Creation date	10	02a0
erzsruisadsp	Automatic Data Set Protection	4	02a0
erzsruisspecial	System Special	4	02a0
erzsruisoper	System Operations	4	02a0
erzsruisgrpacc	Group Access for new resource profiles	4	02a0
erzsrupwinterval	Password change interval	3	02a0
erzsrupassdate	Last password change date	10	02a0
erzsrulogtime	Last logon time	20	02a0
erzsruinstdata	Installation data	255	02a0
erzsruisuaudit	Full user auditing	4	02a0
erzsruisaudit	System auditor	4	02a0
erzsruisprotect	Protected	4	02a0
erzsrumodel	Model data set	44	02a0
erzsruwhendays	Allowed logon days	42	02a0
erzsruwhentime	Allowed logon time	20	02a0
erzsruisrestrict	Restricted	4	02a0
erzsruisroaudit	Read-only auditor	4	02a0
erzsrudcehomec	Home Cell	1023	0290

Table 20. erzSecRacfAcct adapter attributes (continued)

Adapter Attribute	Description	Length	Internal Type
erzsrudcehomeu	Home UUID	1023	0290
erzsrudceisautol	Automatic Logon?	4	0290
erzsrudcename	DCE Name	36	0290
erzsrudceuuid	DCE UUID	36	0290
erzsruisdceseg	DCE Segment ex- ists?	1	0290
erzsruisdfpseg	DFP Segment ex- ists?	1	0210
erzsrudfpappl	Data Application	8	0210
erzsrudfpdata	SMS Data Class	8	0210
erzsrudfpmgmt	SMS Management Class	8	0210
erzsrudfpstor	SMS Storage Class	8	0210
erzsruiskerbseg	Kerberos Segment exists?	1	02D0
erzsrukerbisdes	DES encryption capable?	4	02D0
erzsrukerbisdesd	DES with Key Derivation encryp- tion capable?	4	02D0
erzsrukerbisdes3	Triple DES encryp- tion capable?	4	02D0
erzsrukerbisaes	AES128 encryption capable?	4	02D0
erzsrukerbisaes256	AES256 encryption capable?	4	02D0
erzsrukerbname	Principal Name	240	02D0
erzsrukerbtickmx	Maximum Ticket Life, in seconds	10	02D0
erzsruisprxseg	Proxy Segment Ex- ists?	1	02E0
erzsruprxbinddn	Distinguished Name known on LDAP host	1023	02E0
erzsruprxbindhst	LDAP host URL	1023	02E0
erzsruiswaseg	Work Attribute Segment exists?	1	0260
erzsruwaacct	Work Attribute Ac- count Number	254	0260
erzsruwaaddr1	Address line 1	60	0260
erzsruwaaddr2	Address line 2	60	0260
erzsruwaaddr3	Address line 3	60	0260
erzsruwaaddr4	Address line 4	60	0260
erzsruwabldg	Building	60	0260

Table 20. erzSecRacfAcct adapter attributes (continued)			
Adapter Attribute	**Description**	**Length**	**Internal Type**
erzsruwadept	Department	60	0260
erzsruwamail	E-mail address	246	0260
erzsruwaname	Full Name	60	0260
erzsruwaroom	Room	60	0260
erzsruislnoteseg	Lotus Notes Segment exists?	1	02BO
erzsrulnotessnam	Lotus Notes short name	64	02BO
erzsruisnetvseg	NetView Segment exists?	1	0280
erzsrunetvcons	Console Name	8	0280
erzsrunetvctl	Cross Domain Security Check	8	0280
erzsrunetvdomain	Domains	5	0282
erzsrunetvgspan	GMF Span Name	8	0280
erzsrunetvic	NetView Initial Command	254	0280
erzsrunetvisgmf	GMF Administrator?	1	0280
erzsrunetvismr	Receive Unsolicited Messages?	1	0280
erzsrunetvopclas	NetView Operator Classes	5	0281
erzsrukerbvers	Current key version	3	02DO
erzsrukerbkeyfrom	Key source	8	02DO
erzsruisndsseg	NDS Segment exists?	1	02CO
erzsrundsuname	NDS username	246	02CO
erZsrUMFATagVal	MFA tag value	1023	1210
erZsrUMFAFactor	MFA factor	255	020A
erZsrUIsMFASeg	Is the MFA segment defined for this userid?	5	1210
erZsrUMFAFallb	Is password fallback enabled?	5	02A0
erZsrUMFAPolicy	MFA policy	14	020B

erzSecRacfGrp

This class represents a group account on the RACF database. One base group object for each group is defined in a RACF database.

Table 21. erzSecRacfGrp adapter attributes

Adapter Attribute	Description	Length	Internal Type
erZsrGrpName	RACF group	8	ISGX
erZsrGrpSuper	Superior group for the RACF group	8	SIG0
erZsrGrpData	RACF group description	44	ISG0
erZsrProfAccessList	List of RACF resource profiles and access that is granted to an account or group	265	ISG1

erzSecRacfResource

This class represents a combination of RACF class, resource profile, and access on the RACF database. One base group object for each combination of class, profile, and access is defined in a RACF database.

Table 22. erzSecRacfResource adapter attributes

Adapter Attribute	Description	Length	Internal Type
erZsrProfAccessRDN	Internal LDAP attribute, which stores unique combinations of RACF class, profile, and access in a format that does not contain special characters.	265	ISRX
erZsrProfAccess	Combination of RACF CLASS (erzsrClass), PROFILE(erZsrResource), and ACCESS(erZsrAccess).	265	ISRX
erzsrClass	RACF resource class for the combination of RACF PROFILE (erZsrResource) and ACCESS (erZsrAccess).	8	ISR0
erZsrResource	RACF resource profile for the combination of RACF CLASS (erzsrClass) and ACCESS(erZsrAccess).	246	ISR0
erZsrAccess	The allowed level of access authority on the RACF resource profile for the combination of RACF CLASS (erzsrClass) and PROFILE(erZsrResource).	9	ISR0

Account Add operation

This operation uses the following required attributes to communicate the create new account requests to the adapter.

Table 23. Supported attributes for Account Add operation

Adapter Attribute	Description	Required
erUId	RACF account user ID	Required
erPassword	RACF account password	Required
erZsrUOwner	RACF account owner	Required
erZsrUDfltgrp	RACF account default group	Required

Table 23. Supported attributes for Account Add operation (continued)

Adapter Attribute	Description	Required
erZsrUName	RACF account name	Required
erZsrGrpNameList	List of RACF connect groups for the RACF account	Optional
erZsrURevokeDate	Future revoke date for the RACF account	Optional
erZsrUResumeDate	Future resume date for the RACF account	Optional
erZsrConXml	Connect groups	Optional
erzsruiscicsseg	CICS Segment exists?	Optional
erzsrucicsopid	CICS Operator ID	Optional
erzsrucicsprty	CICS Operator Priority	Optional
erzsrucicsopclas	CICS Operator Classes	Optional
erzsrucicsisforc	XRF Force	Optional
erzsrucicstimout	CICS Session Time-out	Optional
erzsruislangseg	Language Segment exists?	Optional
erzsrulangprime	Primary Language	Optional
erzsrulangsec	Secondary Language	Optional
erzsruisomvsseg	Unix System Services Segment exists?	Optional
erzsruomvsuid	Maximum Processor Time	Optional
erzsruomvshome	Home directory	Optional
erzsruomvsshell	Shell Program Name	Optional
erzsruomvscpu	Maximum Processor Time	Optional
erzsruomvsstor	Maximum address space size, in bytes	Optional
erzsruomvsfiles	Maximum files per process	Optional
erzsruomvsproc	Maximum processes	Optional
erzsruomvsthread	Maximum threads per process	Optional
erzsruomvsmmap	Maximum storage for memory mapped files	Optional
erzsruistsoseg	TSO Segment exists?	Optional
erzsrutsoacct	TSO Account Num- ber	Optional
erzsrutsocmd	TSO Initial Com- mand	Optional
erzsrutsodest	Default JES destina- tion	Optional
erzsrutsohold	Default JES sysout hold class	Optional
erzsrutsojob	Default JES execution class	Optional

Table 23. Supported attributes for Account Add operation (continued)

Adapter Attribute	Description	Required
erzsrutsoproc	Default TSO logon procedure	Optional
erzsrutsosize	Requested TSO region size	Optional
erzsrutsomsg	Default JES sysout message class	Optional
erzsrutsomax	TSO maximum region size	Optional
erzsrutsosout	Default JES sysout class	Optional
erzsrutsoudata	TSO user data (4 hexidecimal digits)	Optional
erzsrutsounit	Default unit name for allocation	Optional
erzsruisadsp	Automatic Data Set Protection	Optional
erzsruisspecial	System Special	Optional
erzsruisoper	System Operations	Optional
erzsruisgrpacc	Group Access for new resource pro- files	Optional
erzsrupwinterval	Password change interval	Optional
erzsruinstdata	Installation data	Optional
erzsruisuaudit	Full user auditing	Optional
erzsruisaudit	System auditor	Optional
erzsruisprotect	Protected	Optional
erzsrumodel	Model data set	Optional
erzsruwhendays	Allowed logon days	Optional
erzsruwhentime	Allowed logon time	Optional
erzsruisrestrict	Restricted	Optional
erzsruisroaudit	Read-only auditor	mfaOptional
erzsrudcehomec	Home Cell	Optional
erzsrudcehomeu	Home UUID	Optional
erzsrudceisautol	Automatic Logon?	Optional
erzsrudcename	DCE Name	Optional
erzsrudceuuid	DCE UUID	Optional
erzsruisdceseg	DCE Segment exists?	Optional
erzsruisdfpseg	DFP Segment exists?	Optional
erzsrudfpappl	Data Application	Optional
erzsrudfpdata	SMS Data Class	Optional
erzsrudfpmgmt	SMS Management Class	Optional
erzsrudfpstor	SMS Storage Class	Optional
erzsruiskerbseg	Kerberos Segment exists?	Optional

Adapter Attribute	Description	Required
erzsrukerbisdes	DES encryption capable?	Optional
erzsrukerbisdesd	DES with Key Derivation encryption capa- ble?	Optional
erzsrukerbisdes3	Triple DES encryption capable?	Optional
erzsrukerbisaes	AES128 encryption capable?	Optional
erzsrukerbisaes25 6	AES256 encryption capable?	Optional
erzsrukerbname	Principal Name	Optional
erzsrukerbtickmx	Maximum Ticket Life, in seconds	Optional
erzsruisprxseg	Proxy Segment Exists?	Optional
erzsruprxbinddn	Distinguished Name known on LDAP host	Optional
erzsruprxbindhst	LDAP host URL	Optional
erzsruiswaseg	Work Attribute Segment exists?	Optional
erzsruwaacct	Work Attribute Account Number	Optional
erzsruwaaddr1	Address line 1	Optional
erzsruwaaddr2	Address line 2	Optional
erzsruwaaddr3	Address line 3	Optional
erzsruwaaddr4	Address line 4	Optional
erzsruwabldg	Building	Optional
erzsruwadept	Department	Optional
erzsruwamail	E-mail address	Optional
erzsruwaname	Full Name	Optional
erzsruwaroom	Room	Optional
erzsruislnoteseg	Lotus Notes Segment exists?	Optional
erzsrulnotessnam	Lotus Notes short name	Optional
erzsruisnetvseg	NetView Segment exists?	Optional
erzsrunetvcons	Console Name	Optional
erzsrunetvctl	Cross Domain Security Check	Optional
erzsrunetvdomain	Domains	Optional
erzsrunetvgspan	GMF Span Name	Optional
erzsrunetvic	NetView Initial Command	Optional
erzsrunetvisgmf	GMF Administrator?	Optional
erzsrunetvismr	Receive Unsolicited Messages?	Optional
erzsrunetvopclas	NetView Operator Classes	Optional
erzsruisndsseg	NDS Segment exists?	Optional

Table 23. Supported attributes for Account Add operation (continued)

Table 23. Supported attributes for Account Add operation (continued)

Adapter Attribute	Description	Required
erzsrundsuname	NDS username	Optional
erZsrUMFATagVal	MFA tag value	Optional
erZsrUMFAFactor	MFA factor	Optional
erZsrUIsMFASeg	Is the MFA segment defined for this userid?	Optional
erZsrUMFAFallb	Is password fallback enabled?	Optional
erZsrUMFAPolicy	MFA policies	Optional

The adapter uses the CKGRACF interface to issue the following command:

```
ADDUSER <ACCOUNT> DFLTGRP(<GROUP>) OWNER(<OWNER>)PASSWORD(<PASSWORD>)
```

If the account is created successfully, the optional adapter attributes are processed with the account **Modify** operation for the existing account. For more information, see Account Modify operation.

Account Password and Password Phrase operations

This operation uses the following attribute to communicate the password or password phrase requests to the adapter.

Table 24. Supported attributes for Account Password and Password Phrase operations

Adapter Attribute	Description	Required
erPassword	RACF account password	Required

The adapter uses the CKGRACF interface to issue the following commands:

Table 25. Commands for Account Password and Password Phrase operations

Criteria	The adapter issues the following command
If the password value requested from the Identity server matches **NOPASSWORD**	`ALTUSER <ACCOUNT> NOPASSWORD`
If the password value requested from the Identity server matches **NOPHRASE**	`ALTUSER <ACCOUNT> NOPHRASE`

If the specified value is less than or equal to 8 characters	`ALTUSER <ACCOUNT> PASSWORD(<PASSWORD>)`
	`EXPIRED or NOEXPIRED`

If the specified value exceeds 8 characters	`ALTUSER <ACCOUNT> PHRASE(<PHRASE>)`
	`EXPIRED or NOEXPIRED`

The adapter verifies the registry settings for the password and password phrase expiration.

Account Suspend operation

This operation uses the following attribute to communicate the suspend requests to the adapter.

Table 26. Supported attributes for Account Suspend operation

Adapter Attribute	Description	Required
erAccountStatus	Current account status	Required

The adapter uses the CKGRACF interface to issue the following command:

```
ALTUSER <ACCOUNT> REVOKE
```

Future Account Suspend operation

This operation uses the following attribute to communicate the suspend requests to the adapter.

Table 27. Supported attributes for Future Account Suspend operation

Adapter Attribute	Description	Required
erZsrURevokeDate	Future account revoke date	Required

The adapter uses the CKGRACF interface to issue the following command:

```
ALTUSER <ACCOUNT> REVOKE(<date>)
```

Account Restore operation

This operation uses the following attribute to communicate the restore requests to the adapter.

Table 28. Supported attributes for Account Restore operation

Adapter Attribute	Description	Required
erAccountStatus	Current account status	Required

The adapter uses the CKGRACF interface to issue the following command:

```
ALTUSER <ACCOUNT> RESUME
```

Future Account Restore operation

This operation uses the following attribute to communicate the restore requests to the adapter.

Table 29. Supported attributes for Future Account Restore operation

Adapter Attribute	Description	Required
erZsrUResumeDate	Future account resume date	Required

The adapter uses the CKGRACF interface to issue the following command:

```
ALTUSER <ACCOUNT> RESUME(<date>)
```

Account Modify operation

This operation uses the following attribute to communicate the account modify requests to the adapter.

Table 30. Supported attributes for Account Modify operation

Adapter Attribute	Description	Required
erPassword	RACF account	Optional

Table 30. Supported attributes for Account Modify operation (continued)

Adapter Attribute	Description	Required
erZsrUOwner	RACF account owner	Optional
erZsrUDfltgrp	RACF account's default group	Optional
erZsrUName	RACF account name	Optional
erZsrGrpNameList	List of RACF connect groups for the RACF account	Optional
erZsrURevokeDate	Future revoke date for the RACF account	Optional
erZsrUResumeDate	Future resume date for the RACF account	Optional
erZsrConXml	Connect groups	Optional
erzsruiscicsseg	CICS Segment exists?	Optional
erzsrucicsopid	CICS Operator ID	Optional
erzsrucicsprty	CICS Operator Priority	Optional
erzsrucicsopclas	CICS Operator Classes	Optional
erzsrucicsisforc	XRF Force	Optional
erzsrucicstimout	CICS Session Time-out	Optional
erzsruislangseg	Language Segment exists?	Optional
erzsrulangprime	Primary Language	Optional
erzsrulangsec	Secondary Language	Optional
erzsruisomvsseg	Unix System Services Segment exists?	Optional
erzsruomvsuid	Maximum Processor Time	Optional
erzsruomvshome	Home directory	Optional
erzsruomvsshell	Shell Program Name	Optional
erzsruomvscpu	Maximum Processor Time	Optional
erzsruomvsstor	Maximum address space size, in bytes	Optional
erzsruomvsfiles	Maximum files per process	Optional
erzsruomvsproc	Maximum processes	Optional
erzsruomvsthread	Maximum threads per process	Optional
erzsruomvsmmap	Maximum storage for memory mapped files	Optional
erzsruistsoseg	TSO Segment exists?	Optional
erzsrutsoacct	TSO Account Number	Optional
erzsrutsocmd	TSO Initial Command	Optional
erzsrutsodest	Default JES destination	Optional

Adapter Attribute	Description	Required
erzsrutsohold	Default JES sysout hold class	Optional
erzsrutsojob	Default JES execution class	Optional
erzsrutsoproc	Default TSO logon procedure	Optional
erzsrutsosize	Requested TSO region size	Optional
erzsrutsomsg	Default JES sysout message class	Optional
erzsrutsomax	TSO maximum region size	Optional
erzsrutsosout	Default JES sysout class	Optional
erzsrutsoudata	TSO user data (4 hexidecimal digits)	Optional
erzsrutsounit	Default unit name for allocation	Optional
erzsruisadsp	Automatic Data Set Protection	Optional
erzsruisspecial	System Special	Optional
erzsruisoper	System Operations	Optional
erzsruisgrpacc	Group Access for new resource pro- files	Optional
erzsrupwinterval	Password change interval	Optional
erzsruinstdata	Installation data	Optional
erzsruisuaudit	Full user auditing	Optional
erzsruisaudit	System auditor	Optional
erzsruisprotect	Protected	Optional
erzsrumodel	Model data set	Optional
erzsruwhendays	Allowed logon days	Optional
erzsruwhentime	Allowed logon time	Optional
erzsruisrestrict	Restricted	Optional
erzsruisroaudit	Read-only auditor	Optional
erzsrudcehomec	Home Cell	Optional
erzsrudcehomeu	Home UUID	Optional
erzsrudceisautol	Automatic Logon?	Optional
erzsrudcename	DCE Name	Optional
erzsrudceuuid	DCE UUID	Optional
erzsruisdceseg	DCE Segment exists?	Optional
erzsruisdfpseg	DFP Segment exists?	Optional
erzsrudfpappl	Data Application	Optional
erzsrudfpdata	SMS Data Class	Optional
erzsrudfpmgmt	SMS Management Class	Optional

Table 30. Supported attributes for Account Modify operation (continued)

Table 30. Supported attributes for Account Modify operation (continued)

Adapter Attribute	Description	Required
erzsrudfpstor	SMS Storage Class	Optional
erzsruiskerbseg	Kerberos Segment exists?	Optional
erzsrukerbisdes	DES encryption capable?	Optional
erzsrukerbisdesd	DES with Key Derivation encryption capable?	Optional
erzsrukerbisdes3	Triple DES encryption capable?	Optional
erzsrukerbisaes	AES128 encryption capable?	Optional
erzsrukerbisaes256	AES256 encryption capable?	Optional
erzsrukerbname	Principal Name	Optional
erzsrukerbtickmx	Maximum Ticket Life, in seconds	Optional
erzsruisprxseg	Proxy Segment Exists?	Optional
erzsruprxbinddn	Distinguished Name known on LDAP host	Optional
erzsruprxbindhst	LDAP host URL	Optional
erzsruiswaseg	Work Attribute Segment exists?	Optional
erzsruwaacct	Work Attribute Account Number	Optional
erzsruwaaddr1	Address line 1	Optional
erzsruwaaddr2	Address line 2	Optional
erzsruwaaddr3	Address line 3	Optional
erzsruwaaddr4	Address line 4	Optional
erzsruwabldg	Building	Optional
erzsruwadept	Department	Optional
erzsruwamail	E-mail address	Optional
erzsruwaname	Full Name	Optional
erzsruwaroom	Room	Optional
erzsruislnoteseg	Lotus Notes Segment exists?	Optional
erzsrulnotessnam	Lotus Notes short name	Optional
erzsruisnetvseg	NetView Segment exists?	Optional
erzsrunetvcons	Console Name	Optional
erzsrunetvctl	Cross Domain Security Check	Optional
erzsrunetvdomain	Domains	Optional
erzsrunetvgspan	GMF Span Name	Optional
erzsrunetvic	NetView Initial Command	Optional
erzsrunetvisgmf	GMF Administrator?	Optional
erzsrunetvismr	Receive Unsolicited Messages?	Optional

Table 30. Supported attributes for Account Modify operation (continued)

Adapter Attribute	Description	Required
erzsrunetvopclas	NetView Operator Classes	Optional
erzsruisndsseg	NDS Segment exists?	Optional
erzsrundsuname	NDS username	Optional
erZsrUMFATagVal	MFA tag value	Optional
erZsrUMFAFactor	MFA factor	Optional
erZsrUIsMFASeg	Is the MFA segment defined for this userid?	Optional
erZsrUMFAFallb	Is password fallback enabled?	Optional
erZsrUMFAPolicy	MFA policies	Optional

The commands executed for erPassword on *Account Modify* depend on these criteria:

1. Exact value of the password requested from the Identity server; **NOPASSWORD** or **NOPHRASE**.
2. Length of the password requested from theIdentity server.

   If the password value requested from the Identity server is neither **NOPASSWORD** or **NOPHRASE**, the length of the value is considered. If the value is less than nine characters, it is interpreted as a request to change a password. If the value exceed eight characters, it is interpreted as a request to change a password phrase.
3. Registry settings for password and password phrase expiration.

   The next value that the adapter considers is the registry setting for either PWDEXP when changing a password, or PWPEXP when changing a password phrase.

The adapter uses the CKGRACF interface to issue the following commands:

Table 31. Commands for Account Modify operation

Criteria	The adapter issues the following command
If the password value requested from the Identity server matches **NOPASSWORD**	`ALTUSER <ACCOUNT> NOPASSWORD`
If the password value requested from the Identity server matches **NOPHRASE**	`ALTUSER <ACCOUNT> NOPHRASE`

For passwords, if PWDEXP is set to TRUE or absent from the registry	`ALTUSER <ACCOUNT> PASSWORD(<VALUE>)`
	`EXPIRED`

For passwords, if PWDEXP is set to FALSE in the registry	`ALTUSER <ACCOUNT> PASSWORD(<VALUE>)`
	`NOEXPIRED`

For password phrases, if PWPEXP is set to TRUE or absent from the registry	`ALTUSER <ACCOUNT> PHRASE('<VALUE>')`
	`EXPIRED`

For password phrases, if PWPEXP is set to FALSE in the registry	`ALTUSER <ACCOUNT> PHRASE('<VALUE>')`
	`NOEXPIRED`

erZsrUOwner	`ALTUSER <ACCOUNT> OWNER(<OWNER>)`

Table 31. Commands for Account Modify operation (continued)

Criteria	The adapter issues the following command
erZsrUDfltgrp	`ALTUSER <ACCOUNT> DFLTGRP(<DFLTGRP>)`
erZsrUName	`ALTUSER <ACCOUNT> NAME('<NAME>')`

erZsrGrpNameList
For adding groups
	`CONNECT <ACCOUNT> GROUP(<GROUP>)`
	`AUTH(USE)`

erZsrGrpNameList For removing groups	`REMOVE <ACCOUNT> GROUP(<GROUP>)`

erZsrConXml	`CONNECT <ACCOUNT> GROUP(<GROUP>)`
	`AUTH(<AUTHORITY>) UACC(<UACC>) <NO>ADSP`
	`<NO>AUDITOR <NO>GRPACC <NO>OPERATIONS`
	`<NO>REVOKED <NO>SPECIAL OWNER(<OWNER>)`
	`REVOKEDT(<DATE>) RESUMEDT(<DATE>)`
	`REMOVE <ACCOUNT> GROUP(<GROUP>)`

erZsrURevokeDate	`ALTUSER <ACCOUNT> REVOKE(<date>)`
erZsrUResumeDate	`ALTUSER <ACCOUNT> RESUME(<date>)`

erzsruiscicsseg	`,"ALTUSER %s CICS" ,`
	`"ALTUSER %s NOCI- CS"`

erzsrucicsopid	`"ALTUSER %s CICS(OPID(%s))" ,`
	`"ALTUSER %s CICS(NOOPID)"`

erzsrucicsprty	`,"ALTUSER %s CICS(OPPRTY(%s))" ,`
	`"ALTUSER %s CICS(NOOPPRTY)"`

erzsrucicsopclas	`"ALTUSER %s CICS(OPCLASS(%s))" ,`
	`"ALTUSER %s CICS(NOOPCLASS)"`

erzsrucicsisforc	`,"ALTUSER %s CICS(XRFSOFF(FORCE))" ,`
	`"ALTUSER %s CICS(XRFSOFF(NOFORCE)"`

erzsrucicstimout	`,"ALTUSER %s CICS(TIMEOUT(%s))" ,`
	`"ALTUSER %s CICS(NOTIMEOUT)"`

erzsruislangseg	`,"ALTUSER %s LANGUAGE" ,`
	`"ALTUSER %s NOLANGUAGE"`

erzsrulangprime	`,"ALTUSER %s LANG(PRIM(%s))" ,`
	`"ALTUSER %s LANG(NOPRIM)"`

erzsrulangsec	`,"ALTUSER %s LANG(SEC(%s))" ,`
	`"ALTUSER %s LANG(NOSEC)"`

erzsruisomvsseg	**True**: `"ALTUSER %s OMVS"` **False**: `"ALTUSER %s NOOMVS"`

Table 31. Commands for Account Modify operation (continued)

Criteria	The adapter issues the following command
erzsruomvsuid	*: "ALTUSER %s OMVS(AUTOUID)" **True**: "ALTUSER %s OMVS(UID(%s)%s)" **False**: "ALTUSER %s OMVS(NOUID)
erzsruomvshome	**True**: "ALTUSER %s OMVS(HOME('%s'))" **False**: "ALTUSER %s OMVS(NOHOME)"
erzsruomvsshell	**True**: "ALTUSER %s OMVS(PROG('%s'))" **False**: ALTUSER %s OMVS(NOPROG)"
erzsruomvscpu	**True**: "ALTUSER %s OMVS(CPUTIM(%s))" **False**: "ALTUSER %s OMVS(NOCPUTIM)”
erzsruomvsstor	**True**: "ALTUSER %s OMVS(ASSIZE(%s))" **False**: "ALTUSER %s OMVS(NOASSIZE)"
erzsruomvsfiles	**True**: "ALTUSER %s OMVS(FILE(%s))" **False**: "ALTUSER %s OMVS(NOFILE)"
erzsruomvsproc	**True**: "ALTUSER %s OMVS(PROG('%s'))" **False**: "ALTUSER %s OMVS(NOPROG)"
erzsruomvsthread	**True**: "ALTUSER %s OMVS(THREAD(%s))" **False**: "ALTUSER %s OMVS(NOTHREAD)"
erzsruomvsmmap	**True**: "ALTUSER %s OMVS(MMAP(%s))" **False**: "ALTUSER %s OMVS(NOMMAP)"
erzsruistsoseg *true* *false*	*True*: *"ALTUSER %s TSO"* *False*: *"ALTUSER %s NOTSO"*
erzsrutsoacct	*True*: *"ALTUSER %s TSO(ACCT(%s))"* *False*: *"ALTUSER %s TSO(NOACCT)"*
erzsrutsocmd	*True*: *"ALTUSER %s TSO(COMMAND('%s'))"* *False*: *"ALTUSER %s TSO(NOCOMMAND)"*
erzsrutsodest	*True*: *“ALTUSER %s TSO(DEST(%s))"* *False*: *"ALTUSER %s TSO(NODEST)"*
erzsrutsohold	*True*: *"ALTUSER %s TSO(HOLDCLASS(%s))"* *False*: *"ALTUSER %s TSO(NOHOLDCLASS)"*

Table 31. Commands for Account Modify operation (continued)

Criteria	The adapter issues the following command
erzsrutsojob	*True*: *"ALTUSER %s TSO(JOBCLASS(%s))"* *False*: *"ALTUSER %s TSO(NOJOBCLASS)"*
erzsrutsoproc	*True*: *"ALTUSER %s TSO(PROC(%s))"* *False*: *"ALTUSER %s TSO(NOPROC)"*
erzsrutsosize	*True*: *"ALTUSER %s TSO(SIZE(%s))"* *False*: *"ALTUSER %s TSO(NOSIZE)"*
erzsrutsomsg	*True*: *"ALTUSER %s TSO(MSGCLASS(%s))"* *False*: *"ALTUSER %s TSO(NOMSGCLASS)"*
erzsrutsomax	*True*: *"ALTUSER %s TSO(MAXSIZE(%s))"* *False*: *"ALTUSER %s TSO(NOMAXSIZE)"*
erzsrutsosout	*True*: *"ALTUSER %s TSO(SYSOUT(%s))"* *False*: *"ALTUSER %s TSO(NOSYSOUT)"*
erzsrutsoudata	*True*: *"ALTUSER %s TSO(USER(%s))"* *False*: *"ALTUSER %s TSO(NOUSER)"*
erzsrutsounit	*True*: *"ALTUSER %s TSO(UNIT(%s))"* *False*: *"ALTUSER %s TSO(NOUNIT)"*
erzsruisadsp	**True**: "ALTUSER %s ADSP” **False**: "ALTUSER %s NOADSP"
erzsruisspecial	**True**: "ALTUSER %s SPECIAL” **False**: "ALTUSER %s NOSPECIAL"
erzsruisoper	**True**: "ALTUSER %s OPERATIONS” **False**: "ALTUSER %s NOOPERATIONS"
erzsruisgrpacc	**True**: "ALTUSER %s GRPACC” **False**: "ALTUSER %s NOGRPACC"
erzsrupwinterval	**True**: "PASSWORD USER(%s) INTERVAL(%s)” **False**: "PASSWORD USER(%s) NOINTERVAL"
erzsruinstdata	**True**: "ALTUSER %s DATA('%s')" **False**: "ALTUSER %s NODATA"
erzsruisuaudit	**True**: "ALTUSER %s UADIT” **False**: "ALTUSER %s NOUADIT"

Table 31. Commands for Account Modify operation (continued)

Criteria	The adapter issues the following command
erzsruisaudit	**True**: `"ALTUSER %s AUDIT”` **False**: `"ALTUSER %s NOAUDIT"`
erzsruisprotect	**True**: `"ALTUSER %s NOPASSWORD NOPHRASE"`
erzsrumodel	**True**: `"ALTUSER %s MODEL(%s)"` **False**: `"ALTUSER %s NOMODEL"`
erzsruwhendays	**True**: `"ALTUSER %s WHEN(DAYS(%s))"` **False**: `"ALTUSER %s WHEN(DAYS(ANYDAY))"`
erzsruwhentime	**True**: `"ALTUSER %s WHEN(TIME(%s))"` **False**: `"ALTUSER %s WHEN(TIME(ANYTIME))"`
erzsruisrestrict	**True**: `"ALTUSER %s RESTRICTED”` **False**: `"ALTUSER %s NORESTRICTED"`
erzsruisroaudit	**True**: `"ALTUSER %s ROAUDIT”` **False**: `"ALTUSER %s NOROAUDIT"`
erzsrudcehomec	*ALTUSER %s DCE(HOMECELL('%s'))* *ALTUSER %s DCE(NOHOMECELL)*
erzsrudcehomeu	*ALTUSER %s DCE(HOMEUUID(%s))* *ALTUSER %s DCE(NOHOMEUUID)*
erzsrudceisautol	*ALTUSER %s DCE(AUTOLOGIN(YES))* *ALTUSER %s DCE(NOAUTOLOGIN)*
erzsrudcename	*ALTUSER %s DCE(DCENAME('%s'))* *ALTUSER %s DCE(NODCENAME)*
erzsrudceuuid	*ALTUSER %s DCE(UUID(%s))* *ALTUSER %s DCE(NOUUID)*
erzsruisdceseg	*ALTUSER %s DCE* *ALTUSER %s NODCE*
erzsruisdfpseg	*ALTUSER %s DFP* *ALTUSER %s NODFP*
erzsrudfpappl	*ALTUSER %s DFP(DATAAPPL(%s))* *ALTUSER %s DFP(NODATAAPPL)*

Table 31. Commands for Account Modify operation (continued)

Criteria	The adapter issues the following command
erzsrudfpdata	*DFP(DATACLAS(%s))* *ALTUSER %s DFP(NODATACLAS)*
erzsrudfpmgmt	*DFP(MGMTCLAS(%s))* *ALTUSER %s DFP(NOMGMTCLAS)*
erzsrudfpstor	*DFP(STORCLAS(%s))* *ALTUSER %s DFP(NOSTORCLAS)*
erzsruiskerbseg	*ALTUSER %s KERB* *ALTUSER %s NOKERB*
erzsrukerbisdes	*ALTUSER %s KERB(ENCRYPT(DES))* *ALTUSER %s KERB(ENCRYPT(NODES))*
erzsrukerbisdesd	*ALTUSER %s KERB(ENCRYPT(DESD))* *ALTUSER %s KERB(ENCRYPT(NODESD))*
erzsrukerbisdes3	*ALTUSER %s KERB(ENCRYPT(DES3))* *ALTUSER %s KERB(ENCRYPT(NODES3))*
erzsrukerbisaes	*ALTUSER %s KERB(ENCRYPT(AES128))* *ALTUSER %s KERB(ENCRYPT(NOAES128))*
erzsrukerbisaes256	*ALTUSER %s KERB(ENCRYPT(AES256))* *ALTUSER %s KERB(ENCRYPT(NOAES256))*
erzsrukerbname	*ALTUSER %s KERB(KERBNAME('%s'))* *ALTUSER %s KERB(NOKERBNAME)*
erzsrukerbtickmx	*ALTUSER %s KERB(MAXTKT(%s))* *ALTUSER %s KERB(NOMAXTKT)*
erzsruisprxseg	ALTUSER %s PROXY ALTUSER %s NOPROXY
erzsruprxbinddn	ALTUSER %s PROXY(BINDDN('%s')) ALTUSER %s PROXY(NOBINDDN)"
erzsruprxbindhst	*ALTUSER %s PROXY(LDAPHOST(%s))* *ALTUSER %s PROXY(NOLDAPHOST)*
erzsruiswaseg	*ALTUSER %s WORKATTR* *ALTUSER %s NOWORKATTR*

Table 31. Commands for Account Modify operation (continued)

Criteria	The adapter issues the following command
erzsruwaacct	*ALTUSER %s WORK(WAACCNT('%s'))* *ALTUSER %s WORK(NOWAACCNT)*
erzsruwaaddr1	*ALTUSER %s WORK(WAADDR1('%s'))* *ALTUSER %s WORK(NOWAADDR1)*
erzsruwaaddr2	*ALTUSER %s WORK(WAADDR2('%s'))* *ALTUSER %s WORK(NOWAADDR2)*
erzsruwaaddr3	*ALTUSER %s WORK(WAADDR3('%s'))* *ALTUSER %s WORK(NOWAADDR3)*
erzsruwaaddr4	*ALTUSER %s WORK(WAADDR4('%s'))* *ALTUSER %s WORK(NOWAADDR4)*
erzsruwabldg	*ALTUSER %s WORK(WABLDG('%s'))* *ALTUSER %s WORK(NOWABLDG)*
erzsruwadept	*ALTUSER %s WORK(WADEPT('%s'))* *ALTUSER %s WORK(NOWADEPT)*
erzsruwamail	*ALTUSER %s WORK(WAEMAIL('%s'))* *ALTUSER %s WORK(NOWAEMAIL)*
erzsruwaname	*ALTUSER %s WORK(WANAME('%s'))* *ALTUSER %s WORK(NONAME)*
erzsruwaroom	*ALTUSER %s WORK(WAROOM('%s'))* *ALTUSER %s WORK(NOWAROOM)*
erzsruislnoteseg true false	*ALTUSER %s LNOTES* *ALTUSER %s NOLNOTES*
erzsrulnotessnam true false	*ALTUSER %s LNOTES(SNAME('%s'))* *ALTUSER %s LNOTES(NOSNAME)*
erzsruisnetvseg true false	*ALTUSER %s NETVIEW* *ALTUSER %s NONETVIEW*

Table 31. Commands for Account Modify operation (continued)

Criteria	The adapter issues the following command
erzsrunetvcons true false	*ALU %s NETV(CONSNAM(%s))* *ALU %s NETV(NOCONSNAM)*
erzsrunetvctl true false	*ALU %s NETV(CTL(%s))* *ALU %s NETV(NOCTL)*
erzsrunetvdomain true false	*ALU %s NETV(DOMAIN(%s)* *ALU %s NETV(NODOMAIN)*
erzsrunetvgspan true false	*ALU %s NETV(NGMFVSPN(%s))* *ALU %s NETV(NONGMFVSPN)*
erzsrunetvic true false	*ALU %s NETV(IC('%s'))* *ALU %s NETV(NOIC)*
erzsrunetvisgmf true false	*ALU %s NETV(NGMFADMN(YES))* *ALU %s NETV(NONGMFADMN)*
erzsrunetvismr true false	*ALU %s NETV(MSGRECVR(YES))* *ALU %s NETV(NOMSGRECVR)*
erzsrunetvopclas true false	*ALU %s NETV(OPCLASS(%s))* *ALU %s NETV(NOOPCLASS)*
erzsruisndsseg true false	*ALTUSER %s NDS* *ALTUSER %s NONDS*
erzsrundsuname true false	*ALTUSER %s NDS(UNAME('%s'))* *ALTUSER %s NONDS*

Table 31. Commands for Account Modify operation (continued)

Criteria	**The adapter issues the following command**

erZsrUMFATagVal	To ADD:
	`ALU USERID MFA(FACTOR(AZFRADP1)`
	`TAGS(RADUSERID:USERID))`
	To DELETE/REMOVE:
	`ALU USERID MFA(FACTOR(AZFRADP1)`
	`DELTAGS(RADUSERID))`

erZsrUIsMFASeg	To DELETE: `ALU [Login ID] NOMFA`
erZsrUMFAFallb	To MODIFY: `ALU [Login ID] MFA(PWFALLBACK|NOPWFALLBACK)`

erZsrUMFAPolicy	To ADD:
	`ALU [Login ID] MFA(ADDPOLICY(policy-name ))`
	To DELETE/REMOVE:
	`ALU [Login ID] MFA(DELPOLICY(policy-name))`

Account Delete operation

When the adapter receives a request to delete an account, it verifies first if the account owns generic data set profile. An account can not be removed from RACF if it still owns generic data set profiles. Those data set profiles must be deleted first.

Table 32. Commands for Account Delete operation

Criteria	**The adapter issues the following command**

To check for any generic data set profile	Using tsocmd (TSO/E)
	`SEARCH GENERIC CLASS(DATASET)`
	`USER(<ACCOUNT>)`

To delete each profile found as output from the search command	Using the CKGRACF interface `DELDSD '<PROFILENAME>'`
To delete the account if there are no profiles found or all found profiles have been deleted	Using the CKGRACF interface `DELUSER <ACCOUNT>`

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 51.

Table 33. Registry settings and their descriptions

Key	Default value	Valid value	Description	Required
Agent_UserLookup_ MaxThreads	3	1 or greater	The number of threads available for processing LOOKUP transactions.	No
DATADIR	adapter_ readwrite_ home/data	adapter_ readwrite_ home/data	Specifies the UNIX System Services Adapter read/write home. This parameter must be the read/write home as specified in the **Disk location parameters** panel during installation. The 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 Identity 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. This is the default setting. When set to `FALSE`, warning messages are NOT returned to the Identity server warning messages are NOT returned to the IBM Security Verify Governance 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. 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.	Yes
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

Table 33. Registry settings and their descriptions (continued)

Key	Default value	Valid value	Description	Required
DSJOB	'hlq'.CNTL	Any data set that is accessible by the adapter RACF ID. **Optional**: The SUR-ROGAT RACF ID where the RECJOB JCL is stored	Specifies the data set where the RECOJOB is located.	Yes
EXPORT	'hlq'.EXPORT	Any data set that is accessible by the adapter RACF ID **Optional**: The SURROGAT RACF ID	Specifies the data set where the intermediate reconciliation results are stored by RECOJOB (AGZJ6). The adapter accesses these data sets as soon as the status of RECOJOB is completed. It collects and further processes the results.	Yes
JOBCHAR	None	One character [A-Z]	If defined, this is the JOBCHAR added to the TSO SUBMIT command that initializes the RECOJOB processing.	No
LOKUSAVE	'hlq'.LSAVE	Any data set that is accessible by the adapter RACF ID. **Optional**: 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

Table 33. Registry settings and their descriptions (continued)

Key	Default value	Valid value	Description	Required
ISIMEXIT	'hlq'.EXEC	Any data set that is accessible by the adapter RACF ID. **Optional**: 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. For example, `erzsruname`, `erzsruwaname`, or `erzsruinstdata`	The value of the attribute specified in this field is copied into the value of the `erzsracclabel` attribute. You can specify any attribute that holds a string value. For example, `erzsruname`, `erzsruwaname`, or `erzsruinstdata`	No
OPMODE	FULL	• FULL • READ-ONLY • READ-ONLY-PWD	The value specified in this field determines the operations that the adapter supports. Valid options are: **`FULL (default)`** The adapter supports all operations SEARCH/LOOKUP/ADD/DELETE/MODIFY **READ-ONLY** The adapter only supports SEARCH and LOOKUP operations **READ-ONLY-PWD** The adapter supports SEARCH, LOOKUP, and PASSWORD/PASSWORD PHRASE operations	No

Table 33. Registry settings and their descriptions (continued)

Key	Default value	Valid value	Description	Required
PASSEXPIRE	TRUE	TRUE, FALSE, or TRUEADD	This attribute is the default action that the adapter must do when the adapter receives a password or passphrase change request. TRUE indicates that passwords or passphrases must be set as expired. FALSE indicates that passwords or passphrases must be set as non-expired. When set to TRUEADD, a pass- word or passphrase for a new user is set to EXPIRED. A password or passphrase 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 `erZsruNoexpire` is passed to the adapter, with TRUE or FALSE, this adapter option (PASSEXPIRE) is ignored. The setting of the `erZsruNoexpire` attribute is used.	No
PROFDEL	FALSE	TRUE or FALSE	If set to TRUE the adapter attempts to delete data set profile prior to deleting the account This attribute defines if TSOCMD or IRXEXEC is used to call ISIMEXIT.	No
TSOCMD	TRUE	TRUE or FALSE	Specify TRUE to use tsocmd or FALSE to use IRXEXEC.	Yes
WAIT	60	Any integer with a minimum value of 3	Specifies the amount of time the adapter waits for the RECOJOB job processing to complete.	Yes

Environment variables

The adapter consists of several environment variables. See the table for these variables, their descriptions and values, if any.

Table 34. zSecure RACF Adapter environment variables

Environment variable	Description	Default value	Required
BINARY_DIR	Specify the fully qualified location of the adapters `read_write_home/bin` directory	`read_write_home/bin`	Yes

Table 34. zSecure RACF Adapter environment variables (continued)

Environment variable	Description	Default value	Required
LIBPATH	Specify the location of the Dynamic Link Library (DLL) and `.so` files.	None	Yes
PDU_ENTRY_LIMIT	Specify the maximum number of accounts that are kept in the main storage.	2000. The range is 50-3000.	No
PROTOCOL_DIR	Specify the fully qualified location of the directory where the `.so` and `.dll` files are.	LIBPATH	No
REGISTRY	Specify the location of a specific registry file. The registry path is the fully qualified path and the file name of the registry file. The registry name is the adapter name in uppercase, with `.dat` suffixed to the name.	Current working directory.	No
STEPLIB	Specify the location of the zSecure SCKRLOAD data set.	Not applicable	Yes
ISIM_ADAPTER_CIPHER_ LIST	Defines the permitted cipher lists. Cipher list consists of one or more colons.	HIGH	No

Index