IBM Security Privileged Identity Manager

CA ACF2 for z/OS Adapter Installation and Configuration Guide

Contents

List of Figures

List of Tables

Chapter 1. Overview

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

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

IBM Security Privileged Identity Manager works with the CA ACF2 Security in an MVS™ environment. The adapter:

- Receives provisioning requests from IBM Security Privileged Identity Manager.
- Processes the requests to add, modify, suspend, restore, delete, and reconcile user information from the adapter security database.
- Converts the Directory Access Markup Language (DAML) requests that are received from IBM Security Privileged Identity Manager to the corresponding adapter Security for z/OS® commands. The Enrole Resource Management API (ERMA) libraries are used for the conversion.
- Issues the commands to the CA ACF2 command executor and receives the results.
- Returns the results of the command and includes the success or failure message of a request to IBM Security Privileged Identity Manager.

The following figure describes the various components of the adapter.

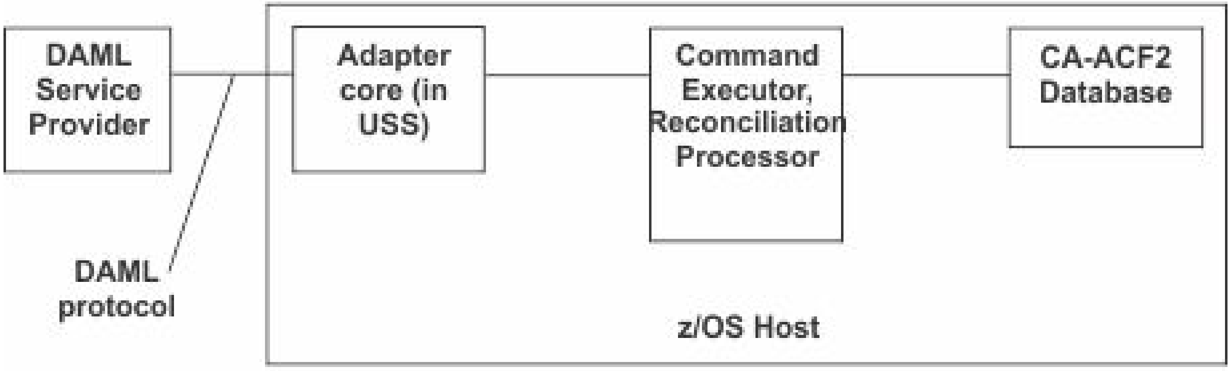

Figure 1: The CA ACF2 Adapter components

Adapter

Receives and processes requests from IBM Security Privileged Identity Manager. The adapter can handle multiple requests simultaneously. The binary files of the adapter and related external files reside in the Unix System Services environment of z/OS (OS/390®).

Command Executor

The ACF2 command executor interfaces with CA ACF2. It issues the R_Admin (IRRSEQ00) callable service to issue ACF2 commands. It processes the commands and returns relevant messages.

The REXX command executor interfaces with the ISIMEXIT REXX script. It uses IKJTSOEV to enable issuing TSO/E commands in the ISIMEXIT. To allocate and execute the ISIMEXIT REXX script it uses IRXLOAD with IRXEXEC or `tsocmd` depending on the chosen configuration.

Reconciliation Processor

The Reconciliation Processor is a series of programs in the C programming language. By default, the Reconciliation Processor runs two programs to obtain data from theCA ACF2 database. The data is sorted and merged before it is sent back to the adapter.

Adapter interactions with the server

The CA ACF2 Adapter uses IBM Security Privileged Identity Manager to perform user tasks on the CA ACF2 Adapter Security for z/OS.

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

The CA ACF2 Adapter does not use Secure Socket Layer (SSL) by default to communicate with IBM Security Privileged Identity Manager. You have to configure it.

SSL requires digital certificates and private keys to establish communication between the endpoints. Regarding SSL, the CA ACF2 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 Privileged Identity Manager) must contain the Certificate Authority or CA certificate.

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

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

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

You can restrict the use of these ports to the CA ACF2 Adapter. To protect these ports with the CA ACF2 protection, define the profiles in the CA ACF2 Adapter SERVAUTH resource class. For more information, see the *z/OS Communications Server, IP Configuration Guide*.

Chapter 2. Planning

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

Roadmap for Adapter Development Kit based adapters, using ISPF

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Related concepts

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

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

Prerequisites

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

Table 1: Prerequisites to install the adapter

Operating System	See the Release Notes for the supported software versions.
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 Identity server to the z/OS Server. When you do so, it is easier to troubleshoot possible installation problems.
IBM Security Identity server	The supported products and releases can be found in the Release Notes, which is included in the adapter installation package.
Required authority	You must have system administrator authority to complete the installation procedure.

Organizations with multiple CA ACF2 databases must have the adapter installed on a z/OS host that manages the database. You can manage a single CA ACF2 database with a single instance of the CA ACF2 Adapter.

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

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

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

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

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

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.

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

Uploading the adapter package

You must upload the adapter package to the operating system.

Before you begin

Obtain the installation software. See Software downloads.

About this task

Use the following values for the referred files:

Table 2: Files used

File description	File name
XMI file	`ISIMACF2.UPLOAD.XMI`
Partitioned Data Set (PDS) file	*`userid`*`.ISIMACF2.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. Transfer the file.

   You can use any method for transferring the file but the resulting file must be in FB 80 format. This example shows how to use FTP to transfer the file from your workstation to MVS.

   ```
   ftp host
   user/password
   cd HLQ
   site recfm=fb lrecl=80 blksize=0 tracks pri=500 sec=100
   bin
   put ISIMACF2.UPLOAD.XMI
   quit
   ```

   Note: If you cannot specify these characteristics with your method, you must pre-allocate the dataset.
3. Receive the uploaded file with the TSO RECEIVE command:

   ```
   RECEIVE INDA(ISIMACF2.UPLOAD.XMI)
   ```

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

Related concepts

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

Communication configuration

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

Related tasks

Installing the ISPF dialog
Install the ISPF dialog

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

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

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

Installing the ISPF dialog

Install the ISPF dialog

About this task

The *userid* is your TSO user ID.

Procedure

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

```
INSTALL1 EXEC ‘userid.ISIMACF2.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 *userid*.ISIMACF2 as the high-level qualifier. Specify another hlq to use the ISPF dialog in the future.

Results

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

Table 3: ISPF dialog data sets

High-level qualifier	Library
hlq.SAGACENU	CLIST/EXEC library
hlq.SAGAMENU	ISPF message library
hlq.SAGATPENU	ISPF panel library
hlq.SAGATSENU	ISPF skeleton library

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

Related concepts

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

Communication configuration

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

Related tasks

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

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

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

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

Running the ISPF dialog

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

Before you begin

Install the ISPF dialog.

About this task

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

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

Procedure

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

   ```
   EXEC ‘hlq.SAGACENU(AGACCFG)'
   ```

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

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

    Security Identity Manager CA ACF2 Adapter

      Initial Customization

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

        X  Exit
   ```

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

   - You can return to the previous menu at any time by pressing **F3** or **END** on the **Menu** selection screen.
   - If you press **F3** on a data entry screen, the values that you entered are not saved.
   - When you fill the data entry screen and if it is validated without errors, the software returns to the previous screen.
3. Type 1 to select **Initial Customization**

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

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

   Initial Installation

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

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

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

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

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

4. Select **Load Default or Saved Variables**

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

  Load Variables

     The IBM supplied defaults are in IBMUSER.ISIMACF2.SAGACENU(AGACDFLT)
     If you remove the name specified below, the defaults will be loaded.

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

     ===>
```

5. Take one of the following actions:
   - 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.
6. Press **PF3** (Cancel) or **Enter** after final input (Accept) to return to the **Initial Installation** panel.
7. Select **Display / Define / Alter Variables**.

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

  Specify or Alter variables for this configuration.

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

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


        ** Indicates option has been visited during this session.

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

   a) Select **Disk location parameters**.

   The **Disk location parameters** page defines or alters data set and UNIX System Services (USS) locations.

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

   Input Data Sets

    Fully qualified data set name of the UPLOAD data set.
     ===> IBMUSER.ISIMACF2.UPLOAD

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

    USS Adapter read-only home
     ===> /usr/lpp/ISIMACF2

    USS Adapter read/write home
     ===> /var/ibm/ISIMACF2

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

    Fully qualified data set name of Adapter Load Library
     ===> IBMUSER.ISIMACF2.LOAD

    Fully qualified data set name of Adapter EXEC Library
     ===> IBMUSER.ISIMACF2.EXEC

    High-level qualifier for reconciliation data sets (optional)
     ===> ISIAGNT.
```

b) Supply the following information:

Fully qualified data set name of the UPLOAD data set
Specifies the name of the data set that you received earlier. For example, `IBMUSER.ISIMACF2.UPLOAD`.

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

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

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

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

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

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

High-level qualifier for reconciliation data sets
Specifies a high-level qualifier for the data sets that are allocated during reconciliation. If a value is not specified, the `agentID` is set as high-level qualifier. If the `agentID` cannot be determined, the default value `ISIAGNT` is set as a high-level qualifier.

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

d) Select **Adapter specific parameters**

The **Adapter specific parameters** define or alter the IBM Security Privileged Identity Manager adapter run time parameters.

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

 Adapter specific parameters

    Name of adapter instance                      ===> CAACF2Agent

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

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

    Adapter authentication ID (internal)          ===> agent

    Adapter authentication password (internal)    ===> agent

    ACF2 Date Format (MDY, DMY, YMD)              ===> MDY

    PDU backlog limit                             ===> 2000

    Do you want to use tsocmd?                    ===> TRUE      (True, False)

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

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

    CA ACF2 OMVS Group for the ISIM Logon ID  ===> STCUSS

    OMVS UID to be assigned to LID (non-zero)     ===> 123456789

    Enable SSL                                    ===> TRUE      (True, False)
Note: You must install a certificate when SSL is enabled.
      For more information, see “Configuring SSL authentication” on page 62.
```

e) Supply the following information:

Name of adapter instance

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

Name of the Started Task JCL procedure name

Specifies the name of the JCL member that is created. You can use the name of the JCL member as the ACF2 Login ID for the adapter.

IP Communications Port Number

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

Adapter authentication ID and Adapter authentication password

Specifies the adapter authentication ID and password that are stored in the adapter registry. The ID and password are used to authenticate the IBM Security Identity server to the CA ACF2. These two parameters must also be specified on the adapter service form that is created on IBM Security Privileged Identity Manager.

ACF2 date format

Specifies the date format that must match with the configured date format in ACF2.

PDU backlog limit

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

Do you want to use tsocmd?

Specify TRUE to use **`tsocmd`** to call `ISIMEXIT`.

Specify FALSE to use **`IRXEXEC`** to call `ISIMEXIT`.

The default value is set to TRUE.

.

Do you want passwords set as expired

Specifies whether the passwords must be set as expired or non-expired. The default value is set to TRUE. You can change it to FALSE if you want all the passwords set as non-expired.

Do you use SYS1.BRODCAST in the environment

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

CA ACF2 OMVS Group for the ISIM Logon ID

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

OMVS UID to be assigned to LID (non-zero)

Specifies a unique UID number for the IBM Security Privileged Identity Manager logonid. Ensure that you specify a non-zero number as the UID number.

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 62.

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

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

h) Press **PF3** to return to the **Installation** panel.

8. 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 as per requirements of your organization. These data sets are not used at the adapter run time.

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

  Generate the job streams

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

     Data set name for job streams to be stored.
     ===> IBMUSER.ISIMACF2.CNTL

     Data set name for data elements required by generated job streams.
     ===> IBMUSER.ISIMACF2.DATA

   Enter your installation job statement parameters here:

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

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

9. Select **Save All Variables** to save all the changes that you made to the data set.

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

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

  Save variables to a data set.

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

     ===> IBMUSER.ISIMACF2.CONFIG
```

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

    To view the adapter settings and instructions to run the generated job streams, see the `*hlq*.ISIMACF2.CNTL(INSTRUCT)` data set. Follow the instructions specified in the `*hlq*.ISIMACF2.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 62.

Related concepts

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

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

Related tasks

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

Installing the ISPF dialog
Install the ISPF dialog

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

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

Restarting the adapter service

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

Before you begin

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

About this task

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

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

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

Note: You can define _BPX_SHAREAS=YES in the /etc/profile. This setting enables the adapter to run in a single address space, instead of multiple address spaces. Newer releases of z/OS create two address spaces with this environment variable set. For more information, see "z/OS UNIX System Services considerations" on page 77.

Procedure

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

   ```
   START ISIAGNT
   ```

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

   - If the UNIX System Services environment is running with _BPX_SHAREAS=YES, then run one of the following stop commands:

     ```
     STOP ISIAGNT
     ```

     or

     ```
     P ISIAGNT
     ```

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

     ```
     P ISIAGNT1
     ```

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

     ```
     CANCEL ISIAGNT
     ```

Related concepts

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

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

Related tasks

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

Installing the ISPF dialog
Install the ISPF dialog

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

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

Access configuration

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

Related concepts

Communication configuration

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

Related tasks

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

Installing the ISPF dialog
Install the ISPF dialog

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

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

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

CA ACF2 logonid

The adapter must run under a valid CA ACF2 loginid, with access to z/OS UNIX System Services, a valid UID, and a valid TSO account.

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

If you are using shared OMVS userIDs you must make sure that the output for the following command is never empty if the adapter is running: **` ps -ef | grep -i <ADAPTERID> | grep -v grep`**

The R_admin callable service requires **READ** permission to be defined for the ADAPTER user and/or **SURROGATE** user on the following resources:

Table 4:

CLASS	RESOURCE
FACILITY	IRR.RADMIN.ADDUSER
FACILITY	IRR.RADMIN.ALTUSER
FACILITY	IRR.RADMIN.CONNECT
FACILITY	IRR.RADMIN.DELUSER
FACILITY	IRR.RADMIN.PASSWORD
FACILITY	IRR.RADMIN.REMOVE

Related concepts

Surrogate user loginids
For the adapter to perform requests on behalf of another user, you must define one or more **SURROGATE** class rules.

Surrogate user loginids

For the adapter to perform requests on behalf of another user, you must define one or more **SURROGATE** class rules.

The CA ACF2 adapter logonid must have **UPDATE** permission on the BPX.SERVER resource in the FACILITY class.

Related concepts

CA ACF2 logonid

The adapter must run under a valid CA ACF2 loginid, with access to z/OS UNIX System Services, a valid UID, and a valid TSO account.

Communication configuration

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

Related concepts

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

Related tasks

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

Installing the ISPF dialog
Install the ISPF dialog

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

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

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

Building the adapter profile

To use the target database with IBM Security Privileged Identity Manager, you must create an adapter profile.

About this task

The adapter installation generates a schema file. This schema file must be merged into the distributed profile, `CAACF2Profile.jar` file.

Procedure

1. Copy the `CAACF2Profile.jar` file that is packaged with the adapter to a temporary directory.
2. Run the following command from the command prompt to the create the subdirectory, CAACF2Profile, in the temporary directory.:

   ```
   jar xvf CAACF2Profile.jar
   ```

3. Change the directory to the CAACF2Profile subdirectory.

   For example:

   ```
   cd CAACF2Profile
   ```

4. From the z/OS operating system, download the member *userid*.ISIMACF2.DATA(ISIMSCHM) to the CAACF2Profile subdirectory.
5. Rename the ISIMSCHM file to `schema.dsml`.

   Note: The CAACF2Profile subdirectory already contains the following files:

   - `resource.def`
   - `eracf2Account.xml`
   - `eracf2Service.xml`

- `Customlabels.properties`

6. Change the directory to the parent directory.
7. Run the following command from the command prompt to create the `CAACF2Profile.jar` file:

```
jar cvf CAACF2Profile.jar CAACF2Profile
```

Results

The `CAACF2Profile.jar` file includes all the files that are required to define the adapter schema, account form, service form, and profile properties.

You can extract the files from the JAR file to modify the necessary files and then repackage the JAR file with the updated files. You can add site-defined fields to the account form.

Importing the adapter profile

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

Before you begin

- The IBM Security Privileged Identity Manager is installed and running.
- You have root or administrator authority on the IBM Security Privileged Identity Manager.
- The file to be imported must be a Java archive (JAR) file. The *<Adapter>*`Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.The JAR file for IBM Security Privileged Identity Manager is located in the top level folder of the installation package.

About this task

Service definition files are also called adapter profile files.

If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a service with the adapter profile or open an account on the service. You must import the adapter profile again.

Procedure

1. Log on to the IBM Security Privileged Identity Manager by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.
   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.
   The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:
   a) In the **Service Definition File** field, type the directory location of the *<Adapter>*`Profile.jar` file, or click **Browse** to locate the file.
      For example, if you are installing the IBM Security Identity Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.
   b) Click **OK** to import the file.

Results

A message indicates that you successfully submitted a request to import a service type.

What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the IBM Security Identity server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is `Failed`, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. The `trace.log` file location is specified by the **handler.file.fileDir** property that is defined in the `enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the IBM Security Identity server*HOME*`\data` directory. .

Creating an adapter service/target

After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Before you begin

Complete "Importing the adapter profile" on page 18.

About this task

You must create an administrative user account for the adapter on the managed resource. You can provide the account information such as administrator name and password when you create the adapter service. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter. The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. From the navigation tree, click **Manage Services**.
2. On the **Services** table, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
   a) Type information about the business unit in the **Search information** field.
   b) Select a business type from the **Search by** list, and then click **Search**.
      A list of business units that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
6. On the **Service Information** page, specify the appropriate values for the service instance.

   The content of the **Service Information** page depends on the type of service that you are creating.
7. Click **Finish**.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

Service/Target form details

Complete the service/target form fields.

On the General Information tab:

Service Name
Specify a name that identifies the CA ACF2 Adapter service on the IBM Security Identity server.

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

URL
Specify the location and port number of the adapter. The port number is defined during installation, and can be viewed and modified in the protocol configuration by using the **`agentCfg`** utility. For more information about protocol configuration settings, see "Changing protocol configuration settings" on page 28.

Note: Configure the adapter for SSL authentication only if **https** is part of the URL. For more information, see "Configuring SSL authentication" on page 62.

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

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

CA ACF2 ID under which requests will be processed
Optional: Specify a SURROGATE ID. This loginid might have administrative authority over a subset of logonids within the CA ACF2 database.

Owner
Optional: Specify the service owner, if any

Service Prerequisite
Optional: Specify an existing service.

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

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

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

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

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

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

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

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

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

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

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

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

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

- Verify the adapter log to ensure that the test request is successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. For example, verify the workstation name or the IP address of the managed resource and the port.

Verifying that the adapter is working correctly

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

Procedure

1. Test the connection for the service that you created on the IBM Security Identity server.
2. Run a full reconciliation from the IBM Security Identity server.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `caacf2agent.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

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

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

Related tasks

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

Installing the ISPF dialog
Install the ISPF dialog

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

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

Chapter 4. Upgrading

Upgrading the adapter requires a full installation. See the Release Notes for the supported software versions or for specific instructions.

Chapter 5. Configuring

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

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

Configuring the adapter parameters

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

All the changes that you make to the parameters, by using the **agentCfg**, take effect immediately. For more information, see *Arguments and description for the agentCfg help menu* in "Accessing help and additional options" on page 59.

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

Related concepts

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

Customizing the adapter
You can do specific functions according to your requirements by using the REXX execs that are provided with the adapter installation.

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.

Configuration notes
The ACF2 adapter can handle multiple requests simultaneously. Learn how the adapter processes specific attributes and requests and how it interacts with z/OS during the processing of some of the requests.

Starting the adapter configuration tool

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

Procedure

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

   ```
   omvs
   ```

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

   ```
   agentCfg -agent adapter_home
   ```

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

```
agentCfg -list
```

6. At **Enter configuration key for Agent '*adapterAGNT*'**, type the configuration key for the adapter.

   The default configuration key is `agent`.

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

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

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

X. Done

Select menu option:
```

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

Table 5: Options for the main configuration menu

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

Related concepts

Configuring event notification

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

Related tasks

Viewing configuration settings

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

Changing protocol configuration settings

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

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

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

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

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

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

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

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

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

Viewing configuration settings

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

Procedure

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

   For more information, see "Starting the adapter configuration tool" on page 25.
2. At the **Main menu** prompt, type A to display the configuration settings for the adapter.

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

Related concepts

Configuring event notification

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

Related tasks

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

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

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

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

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

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

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

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

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

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

Changing protocol configuration settings

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

About this task

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

Procedure

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

   For more information, see "Starting the adapter configuration tool" on page 25.
2. At the **Main menu** prompt, type B. The DAML protocol is configured and available by default for the adapter.

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

X. Done

Select menu option
```

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

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

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

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

X. Done

Select menu option:
```

5. Change the protocol value:

   a) Type the letter of the menu option for the protocol property to configure. The table below describes each property.

   b) Change the property value and press **Enter** to display the **Protocol Properties Menu** with the new value.

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

Table 6: Options for the DAML protocol menu

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

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

Option	Configuration task
C	Displays the following prompt: `Modify Property 'MAX_CONNECTIONS':` Enter the maximum number of concurrent open connections that the adapter supports. The default value is 100. **Note:** This setting is sufficient and does not require adjustment.
D	Displays the following prompt: `Modify Property 'PORTNUMBER':` Type a different port number. The IBM Security Identity 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" on page 71. Type FALSE to not use a secure SSL connection. The default value is TRUE.
F	Displays the following prompt: `Modify Property 'SRV_NODENAME':` Type a server name or an IP address of the workstation where you installed the IBM Security Identity server. This value is the DNS name or the IP address of the IBM Security Identity server that is used for event notification and asynchronous request processing. **Note:** If your operating system supports Internet Protocol version 6 (IPv6) connections, you can specify an IPv6 server.
G	Displays the following prompt: `Modify Property 'SRV_PORTNUMBER':` Type a different port number to access the IBM Security Identity server. The adapter uses this port number to connect to the IBM Security Identity 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 to which the adapter must listen. The default value is **ANY**.

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

Option	Configuration task
I	Displays the following prompt: `Modify Property 'VALIDATE_CLIENT_CE':` Type TRUE for the IBM Security Identity server to send a certificate when it communicates with the adapter. When you set this option, you must configure options D through I. Type FALSE for the IBM Security Identity server can communicate with the adapter without a certificate. **Note:** • The property name is **VALIDATE_CLIENT_CERT**. It is truncated by the **`agentCfg`** to fit in the screen. • You must use certTool to install the appropriate CA certificates and optionally register the IBM Security Identity server certificate.
J	Displays the following prompt: `Modify Property 'REQUIRE_CERT_REG':` This value applies when option I is set to TRUE. Type TRUE to register the adapter with the client certificate from the IBM Security Identity 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" on page 62.
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. **Note:** If you encounter such problems, set the value of **READ_TIMEOUT** to a time longer than the IBM Security Identity server timeout, but less than any firewall timeout. The IBM Security Identity server timeout is specified by the **maximum connection age** DAML property. The adapter must be restarted because READ_TIMEOUT is set at adapter initialization.

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

Option	Configuration task
L	Displays the following prompt: `Modify Property 'DISABLE_TLS10':` Type FALSE to use the TLSv1.0 protocol to connect the adapter. The default value is TRUE.

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

Related concepts

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

Related tasks

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

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

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

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

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

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

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

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

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

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

Configuring event notification

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

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

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

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

Related tasks

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

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

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

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

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

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

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

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

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

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

Accessing help and additional options

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

Identifying the server that uses the DAML protocol

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

Procedure

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

   See "Starting the adapter configuration tool" on page 25.
2. At the **Agent Protocol Configuration Menu**, select **Configure Protocol**.

   See "Changing protocol configuration settings" on page 28.
3. Change the USE_SSL `property` to TRUE.
4. Type the letter of the preferred menu option for the **SRV_PORTNUMBER** property.
5. Specify the IP address or server name that identifies the IBM Security Identity server.
6. Press **Enter** to display the **Protocol Properties Menu** with the new settings.
7. Type the letter of the preferred menu option for the **SRV_PORTNUMBER** property.
8. Specify the port number that the adapter uses to connect to the IBM Security Identity server for event notification.
9. Press **Enter** to display the **Protocol Properties Menu** with the new settings.
10. Install certificate by using the certTool.

    See "Starting the certTool utility" on page 69.

Related tasks

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

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

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

Setting event notification on the server

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

About this task

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

Note: The CA ACF2 for z/OS does not support adapter-based event notification.

Procedure

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

   See "Starting the adapter configuration tool" on page 25.
2. Type C to display **Event Notification Menu**.

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

3. Type the letter of the preferred menu option

   Note:

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

Table 7: Options for the event notification menus

Option	Configuration task
A	If you select this option, the adapter updates the IBM Security Identity 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**.

Table 7: Options for the event notification menus (continued)

Option	Configuration task
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 37.
E	Displays the following prompt: `Enter new thread priority [1-10]:` Type a different thread value to change the event notification process priority. Setting the thread priority to a lower value reduces the impact that the event notification process has on the performance of the adapter. A lower value might also cause event notification to take longer.
F	Displays the following prompt: `Enter new context name:` Type the new context name and press **Enter**. The new context is added.
G	Displays a menu that lists the available contexts. For more information, see "Modifying an event notification context" on page 38.
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 Privileged Identity Manager changes a password. Changes from IBM Security Privileged Identity Manager are recorded in the local database for event notification. A subsequent event notification does not retrieve the password. It sends a delete request for the old password in clear text that is listed in the IBM Security Privileged Identity Manager log files.

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

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

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

Related tasks

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

Setting event notification triggers

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

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

Setting event notification triggers

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

Procedure

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

   See “Starting the adapter configuration tool” on page 25.
2. At the Event Notification Menu, type E to display the Event Notification Entry Types Menu.

   ```
   Event Notification Entry Types
   -------------------------------------------
   A. erAcf2ACCOUNT
   X. Done
   Select menu option:
   ```

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

   - Enable Event notification
   - Create and configure a context
   - Perform a full reconciliation operation
3. Take on of the following actions:

   - Type A for a list of the attributes that are returned during a user reconciliation.
   - Type B for attributes returned during a group reconciliation.

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

   ```
   Event Notification Attribute Listing
   -----------------------------------------------------------------------
   {A} ** ERACCOUNTSTATUS {B} ** ERACF2ACCCNT {C} ** ERACF2ACCDATE
   {D} ** ERACF2ACCOUNT {E} ** ERACF2ACCSRCE {F} ** ERACF2ACCTPRIV
   {G} ** ERACF2ACF2CICS {H} ** ERACF2ALLCMDS {I} ** ERACF2ASSIZE
   {J} ** ERACF2AUDIT {K} ** ERACF2AUTHSUP1 {L} ** ERACF2AUTHSUP2
   {M} ** ERACF2AUTHSUP3 {O} ** ERACF2AUTHSUP4 {Q} ** ERACF2AUTHSUP5
   {R} ** ERACF2AUTHSUP6 {S} ** ERACF2AUTHSUP7 {T} ** ERACF2AUTHSUP8
   (p)rev page 1 of 10 (n)ext
   -------------------------------------------------------------------------
   X. Done
   ```
4. To exclude an attribute from an event notification, type the letter of the menu option

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

Related tasks

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

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

Modifying an event notification context

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

Modifying an event notification context

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

About this task

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

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

Procedure

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

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

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

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

Table 8: Modify context options

Option	Configuration task	For more information
A	Adding search attributes for event notification	See "Adding search attributes for event notification" on page 39.
B	Configuring the target DN for event notification contexts	See "Configuring the target DN for event notification contexts" on page 40.

Related tasks

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

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

Setting event notification triggers

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

Adding search attributes for event notification

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

About this task

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

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

Procedure

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

   See “Starting the adapter configuration tool” on page 25.
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:
```

   CA ACF2 for z/OS requires the **resource_name** attribute to be specified for each context. The value of the attribute must be set to the Managed Resource Name defined on the IBM Security Identity Manager Service Form.

Related concepts

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

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

Related tasks

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

Removing the baseline database for event notification contexts

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

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

About this task

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

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

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

Procedure

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

   See "Starting the adapter configuration tool" on page 25.
2. Type the Event Notification option to display the **Event Notification Menu**.
3. Type the option for Modify Event Notification Context, then enter the option of the context that you want to modify.
4. At the **Modify Context Menu** for the context, type B.
   The following prompt is displayed:

   ```
   Enter Target DN:
   ```
5. Type the target DN for the context and press **Enter**.

   The target DN for the event notification context must be in the following format:

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

   Table 9 on page 40 describes each DN element.

   Table 9: DN elements and definitions

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

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

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

Pseudo-distinguished name values

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

Related tasks

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

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

Search attributes

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

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

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

Table 10 on page 41 describes a partial list of possible attribute and value pairs that you can specify for **Set attributes for search**.

Table 10: Attributes for search

Service type	Form label	Attribute name	Value
CA ACF2 profile	CA ACF2 loginid under which requests are processed	eracf2requester	A *Scoped Privileged*CA ACF2 loginid that manages users in this service.

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

A.  CA ACF2

X.  Done

Select menu option:a

Modify Context: CA ACF2
------------------------------------

A.  Set attributes for search
B.  Target DN:

Select menu option:a

Reconciliation Attributes Passed to Agent for context: CA ACF2
-------------------------------------------------

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

X.  Done

Select menu option:a

Attribute name : ercaacf2requester

Attribute value: admnbu1

Reconciliation Attributes Passed to Agent for context: CA ACF2
-------------------------------------------------
01. ercaacf2requester           'admnbu1'
-------------------------------------------------

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

X.  Done

Select menu option:x
```

Related concepts

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

Related tasks

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

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

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

Pseudo-distinguished name values

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

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

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

Table 11: Name values and their description

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

Example 1:

A:

The service name on the IBM Security Identity Manager server is **MVS CA ACF2 4.5.1016 ENTEST**. This name becomes the component **A** of the pseudo-DN:

```
erservicename=MVS CA ACF2 4.5.1016 ENTEST
```

B:

Table 12 on page 43 describes an example of the IBM Security Identity Manager organization chart that indicates the location of the service in the organization.

Table 12: Organization chart example

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

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

C:

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

```
o=Acme Inc
```

D:

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

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

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

E:

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

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

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

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

```
erservicename=MVS CA ACF2 4.5.1016 ENTEST,o=Acme Inc,ou=Acme,dc=my_suffix
```

Example 2:

A:

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

```
erservicename=Irvine Sales
```

B:

Table 13 on page 44 describes an example of the IBM Security Identity Manager organization chart that indicates the location of the service in the organization.

Table 13: Organization chart example

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

`- Irvine`
`Sales`
	LocationOrganizational Unit	lou

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

Component B of the pseudo-DN is:

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

C:

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

```
o=Acme Inc
```

D:

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

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

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

```
ou=Acme
```

E:

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

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

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

```
dc=my_suffix
```

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

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

Related concepts

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

Related tasks

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

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

Removing the baseline database for event notification contexts

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

Removing the baseline database for event notification contexts

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

Procedure

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

Related concepts

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

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

Related tasks

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

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

Changing the configuration key

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

Procedure

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

   For more information, see "Starting the adapter configuration tool" on page 25.
2. At the **Main menu** prompt, typeD.
3. Take one of the following actions:
   - Change the value of the configuration key and press **Enter**.

     Note: The default configuration key is `agent`. Ensure that your password is complex.
   - Press **Enter** to return to the **Main Configuration Menu** without changing the configuration key.

Related concepts

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

Related tasks

Starting the adapter configuration tool

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

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

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

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

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

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

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

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

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

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

Changing activity logging settings

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

About this task

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

Procedure

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

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

3. Type the letter of the preferred menu option

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

- Press **Enter** to change the value for menu option B, C, D, or E. The other options are changed automatically when you type the corresponding letter of the menu option. Table 14 on page 48 describes each option.
- Press **Enter** to return to the **Agent Activity Logging Menu** without changing the value.

Table 14: Options for the activity logging menu

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

Table 14: Options for the activity logging menu (continued)

Option	Configuration task
H	If this option is set to enabled, the adapter maintains a log file of all transactions in the Agent Development Kit (ADK) and library files. Base logging substantially increases the size of the logs. 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.

Related concepts

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

Related tasks

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

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

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

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

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

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

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

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

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

Accessing help and additional options

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

Modifying registry settings

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

Procedure

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

   For more information, see "Starting the adapter configuration tool" on page 25.
2. At the **Main menu** prompt, type F.
   The **Registry Menu** is displayed.

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

3. Type the letter of the preferred menu option

Related concepts

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

Related tasks

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

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

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

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

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

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

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

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

Changing code page settings

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

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

Modifying non-encrypted registry settings

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

Procedure

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

```
mailAgent Registry Items
-------------------------------------------------
01. DATEFORMAT 'MDY'
02. ENROLE_VERSION '6.0'
03. PASSEXPIRE 'TRUE'
04. SYSEXEC  'IBMUSER.ISIMACF2.EXEC'

-------------------------------------------------
                Page 1 of 1

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

X.  Done

Select menu option:
```

The following table describes the non-encrypted registry keys and their available settings:

Table 15: Non-encrypted registry keys

Key	Description
DATEFORMAT	Specifies the date format that must match with the configured date format of the adapter.
ENROLE_VERSION	Specifies the version of IBM Security Privileged Identity Manager.
RESWORD	Any comma-separated string that is found in the RESWORD registry setting value is added to the hardcoded reserved words list during request processing.
PASSEXPIRE	Specifies the default action that the adapter must perform when the adapter receives a password change request. TRUE indicates that passwords must be set as expired. FALSE indicates that passwords must be set as non-expired.
SYSEXEC	Specifies the data set that contains the REXX executable programs **ISIMEXIT** and **ISIMEXEC**.

Table 15: Non-encrypted registry keys (continued)

Key	Description
PASSGEN	Registry setting for changing phrases: • PASSGEN=ADD: Generate random password on ADD account with pass phrase • PASSGEN=MOD: Generate random password on MODIFY account with pass phrase • PASSGEN=NEVER: Never generate a random password • PASSGEN=BOTH: Always generate a random password If not specified, the default PASSGEN value is BOTH. **Note:** It is **not** guaranteed that random passwords generated meet the site-specific password. With the PASSGEN value set to NEVER or MOD, new accounts can be requested only by using a password. When you are add a new account with a pass phrase, with PASSGEN set to NEVER or MOD, the following error is returned:`ERR:yy/mm/dd hh:mm:ss caacf2Add: pass phrases can NOT be used for INSERT for user <LID>`
PWD_CONFIG	PWD_CONFIG allows a maximum of 5 comma-separated strings, which are randomly selected by the adapter to generate random passwords.
PWP_CONFIG	PWP_CONFIG allows a maximum of 3 comma-separated strings, which are randomly selected by the adapter to generate random password phrases.
PWPMOD	Registry settings for changing passwords: • PWPMOD = RANDOM: Generate a random phrase on MODIFY account with password • PWPMOD=DISABLE: Disables pass phrase usage for this LID on MODIFY account with password • PWPMOD=IGNORE: No changes are made for the pass phrase when the request is for changing a password If not specified, the default PWPMOD value is set to RANDOM. It is **not** guaranteed that random passwords generated meet the site-specific password.
AUTOPWP	Registry setting for changing phrases: PWPMOD=DISABLE ensures that the pass phrase usage for a specified LID is disabled on account MODIFY. When you change a password for this LID, an additional registry setting is introduced to specify whether PWPALLLOW must be automatically re-enabled when it receives a request to set a pass phrase for a LID. • AUTOPWP=TRUE: Automatically set PWPALLOW when receiving a request to change a pass phrase • AUTOPWP=FALSE: Does not automatically set anything for the phrase when the request is for changing a phrase If not specified, the default AUTOPWP value is set to TRUE.

Table 15: Non-encrypted registry keys (continued)

Key	Description
RECHLQ	Specifies a high-level qualifier for the data sets that are allocated during reconciliation. If a value is not specified, the `agentID` is set as high-level qualifier. If the `agentID` cannot be determined, the default value `ISIAGNT` is set as a high-level qualifier.
TSCOMD	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 16: Attribute configuration option description

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

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

Results

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

Related concepts

Configuring event notification

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

Related tasks

Starting the adapter configuration tool

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

Viewing configuration settings

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

Changing protocol configuration settings

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

Changing the configuration key

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

Changing activity logging settings

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

Modifying registry settings

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

Changing advanced settings

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

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

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

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

Changing advanced settings

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

About this task

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

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

This thread counts determines the maximum number of requests that the adapter processes. You can change these settings.

Procedure

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

   For more information, see “Starting the adapter configuration tool” on page 25.

2. At the **Main menu** prompt, type G to display the **Advanced Settings Menu**.

   The following screen displays the default thread count settings.

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

3. Type the letter of the preferred menu option

   For a description of each option, see Table 17 on page 54.

Table 17: 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.

Table 17: Options for the advanced settings menu (continued)

Option	Description
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 perform 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 FALSE.

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

Related concepts

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

Related tasks

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

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

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

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

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

Modifying registry settings

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

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

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

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

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

Viewing statistics

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

Procedure

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

   For more information, see "Starting the adapter configuration tool" on page 25.
2. At the **Main menu** prompt, type H to display the activity history for the adapter.

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


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

10/19/2004  000000    000004    000000     000000    000000    000004

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

X. Done
```

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

Related concepts

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

Related tasks

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

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

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

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

Changing activity logging settings

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

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

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

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

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

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

Changing code page settings

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

Before you begin

The adapter must be running.

About this task

Run the following command to view the code page information:

```
agentCfg -agent adapterAGNT -codepages
```

Procedure

1. Access the **Agent Main Configuration Menu**.
   For more information, see "Starting the adapter configuration tool" on page 25
2. At the **Main menu** prompt, type I.

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

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

A.  Codepage Configure.

X.  Done

Select menu option:
```

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

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

Enter configuration key for Agent 'adapterAGNT':

        Agent Main Configuration Menu
        -------------------------------------------

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

        X.  Done

        Select menu option:i

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

        A.  Codepage Configure.

        X.  Done

        Select menu option:a

        Enter Codepage: ibm-1145

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

        A.  Codepage Configure.

        X.  Done

        Select menu option:x
```

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

Related concepts

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

Related tasks

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

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

Changing protocol configuration settings

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

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

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

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

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

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

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

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

Accessing help and additional options

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

Procedure

1. At the **Main menu** prompt, typeX to display the UNIX System Services command prompt.
2. Type **agentCfg** -help at the prompt to display the help menu and list of commands.

```
-version               ;Show version
-hostname <value>    ;Target nodename to connect to (Default:Local host
IP address)
-findall               ;Find all agents on target node
-list                  ;List available agents on target node
-agent <value>         ;Name of agent
-tail                  ;Display agent's activity log
-schema                ;Display agent's attribute schema
-portnumber <value>    ;Specified agent's TCP/IP port number
-netsearch <value>   ;Lookup agents hosted on specified subnet
-codepages             ;Display list of available codepages
-help                  ;Display this help screen
```

The following table describes each argument.

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

Argument	Description
-version	Use this argument to display the version of the **agentCfg** tool.

*Table 18: Arguments and description for the **agentCfg** help menu (continued)*

Argument	Description
-hostname <value>	Use the **-hostname** argument with one of the following arguments to specify a different host: • -findall • -list • -tail • -agent Enter a host name or IP address as the value.
-findall	Use this argument to search and display all port addresses 44970 - 44994 and their assigned adapter names. This option times out the unused port numbers. Therefore, it might take several minutes to complete. Add the **-hostname** argument to search a remote host.
-list	Use this argument to display the adapters that are installed on the local host of the 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 operating system. You must specify a subnet address as the value.

*Table 18: Arguments and description for the **agentCfg** help menu (continued)*

Argument	Description
-codepages	Use this argument to display a list of available codepages.
-help	Use this argument to display the Help information for the **agentCfg** command.

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

agentCfg -list

Displays a list of:

- All the adapters on the local host.
- The IP address of the host.
- The IP address of the local host.
- The node on which the adapter is installed.

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

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

agentCfg -agent *adapter_name*

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

agentCfg -list -hostname 192.9.200.7

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

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

agentCfg -agent *adapter_name* -hostname 192.9.200.7

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

Related concepts

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

Related tasks

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

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

Changing protocol configuration settings

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

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

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

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

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

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

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

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

Configuring SSL authentication

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

Use the Secure Sockets Layer (SSL) authentication with the default communication protocol, DAML.

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

By configuring the adapter for SSL, the IBM Security Identity server can verify the identity of the adapter before the server establishes a secure connection.

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

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

Related concepts

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.

Customizing the adapter
You can do specific functions according to your requirements by using the REXX execs that are provided with the adapter installation.

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.

Configuration notes

The ACF2 adapter can handle multiple requests simultaneously. Learn how the adapter processes specific attributes and requests and how it interacts with z/OS during the processing of some of the requests.

Overview of SSL and digital certificates

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

SSL protocol uses signed digital certificates from a Certificate Authority (CA) for authentication. SSL encrypts the data that is exchanged between the applications to secure communication.

Signed digital certificates enable two applications that connect in a network to authenticate their identity. An application that acts as an SSL server presents its credentials to an SSL client for verification. The SSL client verifies that the application is the entity it claims to be. You can configure an application that acts as an SSL server so that it requires the application that acts as an SSL client to present its credentials in a certificate. In this way, the two-way exchange of certificates is completed. For more information on the two-way SSL configuration, see Defining and Securing Keystores or Truststores.

A third-party Certificate Authority issues signed certificates for a fee. Some utilities, such as those provided by OpenSSL, can also provide signed certificates.

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

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

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

Private keys, public keys, and digital certificates

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

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

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

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

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

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

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

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

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

Self-signed certificates

Use self-signed certificates to test an SSL configuration before you create and install a signed certificate that is provided by a Certificate Authority.

A self-signed certificate contains a public key, information and signature of the certificate owner. It also has an associated private key but it does not verify the origin of the certificate through a third-party Certificate Authority.

After you generate a self-signed certificate on an SSL server application, you must:

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

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

Use a key management utility to do the following tasks:

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

Use of self-signed certificates depends on your security requirements. To obtain the highest level of authentication between critical software components, do not use self-signed certificates or use them selectively. You can authenticate applications that protect server data with signed digital certificates. You can use self-signed certificates to authenticate web browsers or IBM Security Identity Adapters.

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

Certificate and key formats

Certificates and keys are stored in the files with various formats.

`.pem` format

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

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

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

`.arm` format

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

`.der` format

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

.pfx format (PKCS12)

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

DAML SSL implementation

When you start the adapter, it loads the available connection protocols. The DAML protocol is the only available protocol that supports SSL authentication. You can specify DAML SSL implementation.

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

Configuring certificates for SSL authentication

To establish a secure connection between the adapter and the IBM Security Identity server, configure SSL authentication for connections that originate from the IBM Security Identity server or from the adapter. You can configure the adapter for one-way or two-way SSL authentication with signed certificates.

- "Configuring certificates for one-way SSL authentication" on page 65
- "Configuring certificates for two-way SSL authentication" on page 66
- "Configuring certificates when the adapter operates as an SSL client" on page 67
- "Managing the SSL certificates" on page 68

Configuring certificates for one-way SSL authentication

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

About this task

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

In Figure 2 on page 65, Application A operates as the IBM Security Identity server, and Application B operates as the IBM Security Identity Adapter.

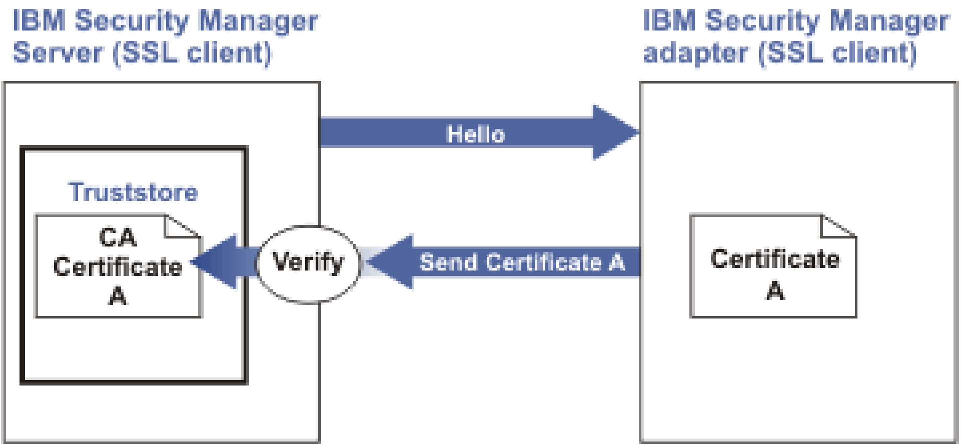
IBM Security Manager Server (SSL client)
IBM Security Manager adapter (SSL client)
Hello
Truststore
CA Certificate A
Verify
Send Certificate A
Certificate A

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

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

Procedure

1. On the adapter, complete these steps:
   a) Start the certTool utility.
   b) Configure the SSL-server application with a signed certificate issued by a certificate authority.
      1) Create a certificate signing request (CSR) and private key. This step creates the certificate with an embedded public key and a separate private key and places the private key in the PENDING_KEY registry value.
      2) Submit the CSR to the certificate authority by using the instructions that are supplied by the CA. When you submit the CSR, specify that you want the root CA certificate that is returned with the server certificate.
2. On the IBM Security Identity server, complete one of these steps:
   - If you used a signed certificate that is issued by a well-known CA:
     a. Ensure that the IBM Security Identity server stored the root certificate of the CA (CA certificate) in its keystore. See https://www-01.ibm.com/support/docview.wss?uid=ibm10713583.
     b. If the keystore does not contain the CA certificate, extract the CA certificate from the adapter and add it to the keystore of the server.
   - If you generated the self-signed certificate on the IBM Security Identity server, the certificate is installed and requires no additional steps.
   - If you generated the self-signed certificate with the key management utility of another application:
     a. Extract the certificate from the keystore of that application.
     b. Add it to the keystore of the IBM Security Identity server.

Configuring certificates for two-way SSL authentication

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

Before you begin

Configure the adapter and the IBM Security Identity server for one-way SSL authentication.

If you use signed certificates from a CA:

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

About this task

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

In Figure 3 on page 67, the IBM Security Identity server operates as Application A and the IBM Security Identity Adapter operates as Application B.

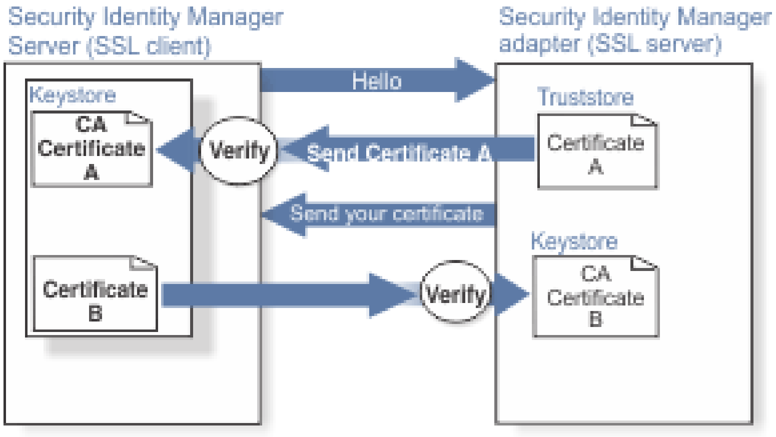

Figure 3: Two-way SSL authentication (client authentication)

Procedure

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

Results

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

Configuring certificates when the adapter operates as an SSL client

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

About this task

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

Figure 4 on page 68 describes how the adapter operates as an SSL server and as an SSL client. When the adapter communicates with the IBM Security Identity server, the adapter sends its certificate for authentication. When the adapter communicates with the web server, the adapter receives the certificate of the web server.

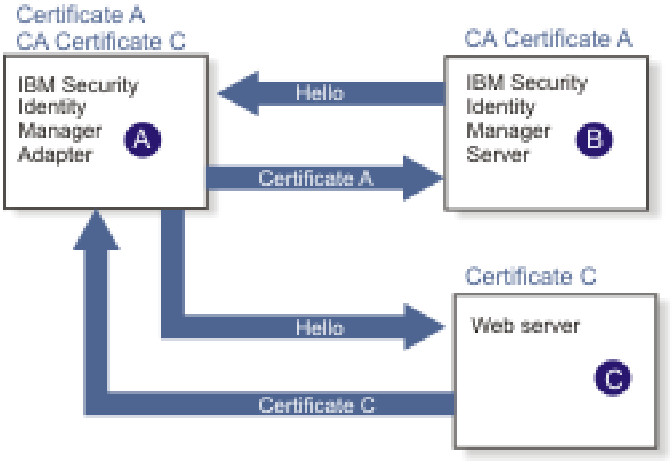

Figure 4: Adapter operating as an SSL server and an SSL client

If the web server is configured for two-way SSL authentication, it verifies the identity of the adapter. The adapter sends its signed certificate to the web server. To enable two-way SSL authentication between the adapter and web server, complete these steps:

Procedure

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

What to do next

You might want the software to send an event notification when the adapter initiates a connection to the web server, which is used by the IBM Security Identity server.

Managing the SSL certificates

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

- "Starting the certTool utility" on page 69.
- "Generating a private key and certificate request" on page 70
- "Installing the certificate" on page 71
- "Installing the certificate and key from a PKCS12 file" on page 72
- "Viewing the installed certificate" on page 72
- "Installing a CA certificate" on page 72
- "Viewing CA certificates" on page 73
- "Deleting a CA certificate" on page 73
- "Registering a certificate" on page 73
- "Viewing registered certificates" on page 74
- "Unregistering a certificate" on page 74
- "Exporting a certificate and key to PKCS12 file" on page 74

Starting the certTool utility

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

About this task

From the **Main** menu of the certTool utility, you can complete these tasks:

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

Procedure

1. Log on to the adapter
2. In the command prompt, change to the read/write `/bin` subdirectory of the adapter.If the adapter is installed in the default location for the read/write directory, run the following command.

   For Windows based operating systems
   `cd C:\Tivoli\Agents\`*`adapterAGNT`*`\bin`

   For UNIX based operating systems
   `cd /var/ibm/isim/bin`
3. Type certTool at the prompt. The **Main menu** is displayed.

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

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

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

K. Export certificate and key to PKCS12 file

X. Quit

Choice:
```

4. Type the letter of the preferred menu option

   Options A through D generates a CSR and installs the returned signed certificate on the adapter.

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

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

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

   D. View current installed certificate
   View the certificate that is installed on the z/OS system where the adapter is installed.

   Options E through G installs the root CA certificates on the adapter. A CA certificate validates the corresponding certificate from the client, such as the server.

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

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

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

Options H through K apply to adapters that must authenticate the application to which the adapter is sending information. An example of an application is the IBM Security Identity server or the web server. Use these options to register certificates on the adapter.

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

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

J. Unregister a certificate
Remove a certificate from the registered list.

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

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

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

Generating a private key and certificate request

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

About this task

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

A CSR file looks similar to the following example:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwgZUxEjAQBgNVBAoTCWFjY2VzczM2MDEUMBIGA1UECxMLZW5n
aW5lZXJpbmcxEDAOBgNVBAMTB250YWdlbnQxJDAiBgkqhkiG9w0BCQEWFW50YWdl
bnRAYWNjZXNzMzYwLmNvbTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Ju
aWExDzANBgNVBAcTBklydmluZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
mR6AcPnwf6hLLc72BmUkAwaXcebtxCoCnnTH9uc8VuMHPbIMAgjuC4s91hPrilG7
UtlbOfy6X3R3kbeR8apRR9uLYrPIvQ1b4NK0whsytij6syCySaFQIB6V7RPBatFr
6XQ9hpsARdkGytZmGTgGTJ1hSS/jA6mbxpgmttz9HPECAwEAAaAAMA0GCSqGSIb3
DQEBAgUAA4GBADxA1cDkvXhgZntHkwT9tCTqUNV9sim8N/U15HgMRh177jVaHJqb
N1Er46vQSsOOOk4z2i/XwOmFkNNTXRVl9TLZZ/D+9mGZcDobcO+lbAKlePwyufxK
Xqdpu3d433H7xfJJSNYLYBFkrQJesITqKft0Q45gIjywIrbctVUCepL2
 -----END CERTIFICATE REQUEST-----
```

Procedure

1. At the **Main menu** of the certTool utility, type A. The following prompt is displayed:

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

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

   - Type Y to accept the displayed values.
   - Type `N` and specify different values.

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

What to do next

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

Installing the certificate

Use the **Install certificate from file** certTool option to install the certificate on the adapter, from a file returned by the CA in response to the generated CSR.

About this task

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

Procedure

1. If you received the certificate as part of an email message, take the following actions:
   a) Copy the text of the certificate to a text file.
   b) Copy that file to the read/write data directory of the adapter.
      For example:`/var/ibm/`*`adapterAGNT`*`/data`

   For Windows based operating systems

   For UNIX based operating systems
2. At the **Main menu** of the certTool utility, type B. The following prompt is displayed:

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

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

Results

The certificate is installed in the adapter registry, and the **Main Menu** is displayed again.

Installing the certificate and key from a PKCS12 file

If the certTool utility did not generate a CSR to obtain a certificate, you must install both the certificate and private key. Use the **Install certificate and key from a PKCS12 file** certTool option to install a certificate from a PKCS12 format file that includes both the public certificate and a private key.

About this task

Store the certificate and the private key in a PKCS12 file.

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

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

Procedure

1. Copy the PKCS12 file to the `data` directory of the adapter.
   For example:

   For Windows based operating systems

   For UNIX based operating systems
2. At the **Main menu** of the certTool utility, type B. The following prompt is displayed:

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

Results

The certificate and private key is installed in the adapter registry, and the **Main Menu** is displayed again.

Viewing the installed certificate

Use the **View current installed certificate** certTool option to view the certificate that is installed on the z/OS system where the adapter is installed.

Procedure

1. At the **Main menu** of the certTool utility, type D.
2. The utility displays the installed certificate. The following example shows an installed certificate:

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

Installing a CA certificate

Use the **Install a CA certificate** certTool option to install root CA certificates on the adapter.

About this task

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

Procedure

1. At the **Main menu** of the certTool utility, type F. The following prompt is displayed:

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

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

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

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

Results

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

Viewing CA certificates

Use the **List CA certificates** certTool option to view the private keys and certificates that are installed for the adapter.

About this task

The certTool utility installs only one certificate and one private key. You can list the CA certificate on the adapter.

Procedure

1. At the **Main menu** of the certTool utility, type E.
2. The utility displays the installed CA certificates. The following example shows an installed CA certificate:

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

Deleting a CA certificate

Use the **Delete a CA certificate** certTool option to delete a CA certificate from the adapter directories.

Procedure

1. At the **Main menu** of the certTool utility, type `G` to display a list of all CA certificates that are installed on the adapter.

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

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

Results

The CA certificate is deleted from the `DamlCACerts.pem` file and the certTool utility displays the **Main Menu**.

Registering a certificate

Use the **Register a certificate** certTool option to register certificates on the adapter. Adapters that must authenticate to the application to which it is sending information must have a registered certificate. An example of an application is the IBM Security Identity server or the web server.

Procedure

1. At the **Main menu** of the certTool utility, type `I`. The following prompt is displayed:

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

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

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

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

Results

The certificate is registered to the adapter and the certTool displays the **Main Menu**.

Viewing registered certificates

The adapter accepts only 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 do specific functions according to your requirements by using the REXX execs that are provided with the adapter installation.

- "ISIMEXIT command usage" on page 75
- "ISIMEXEC command usage" on page 76

Related concepts
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.

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

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.

Configuration notes
The ACF2 adapter can handle multiple requests simultaneously. Learn how the adapter processes specific attributes and requests and how it interacts with z/OS during the processing of some of the requests.

ISIMEXIT command usage

ISIMEXIT is a REXX command. Use this command to start a REXX exec in response to a processing request from the IBM Security Identity server.

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

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

Exit processing might indicate success (zero return code) or failure (non-zero return code) to convey to the adapter. For the pre- add, pre-modify, and pre-delete exits, any non-zero return code returns a failure for the current CA ACF2 user that is processed. For the post add, post modify, and post delete exits, a non-zero return code returns a warning for the current CA ACF2 user that is processed.

You might call other programs and perform file Input/Output (I/O) as necessary. Processing is performed under the authority of the CA ACF2 ID that runs the CA ACF2 commands to accomplish the function. You might run a valid TSO command if it does not prompt for a terminal user for input.

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

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

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

Note: Ensure that the Processing ID has appropriate CA ACF2 authorization to perform the listed exit functions.

The listed information is available to the `EXIT`.

*Table 19: **`ISIMEXIT`** processing information*

Parameter #	Meaning	Possible value	Availability
1	Verb Indicates what operation is calling the exit.	ADD, MODIFY, or DELETE.	Always
2	Object The object name of the transaction.	USER indicating a CA ACF2 user object that is processed.	Always
3	Prepost Qualifies whether this entry is PRE or POST processing entry to the exit.	BEFORE or AFTER.	Always
4	User ID	The CA ACF2 logonid that is processed.	Always
5	ERACF2NAME	The value of the attribute.	Only ADD BEFORE and AFTER
6	ERACF2USING	The value of the attribute.	Only ADD BEFORE and AFTER

Related concepts

ISIMEXEC command usage
`ISIMEXEC` is a REXX command. Use this command for backward compatibility with earlier versions of the adapter.

ISIMEXEC command usage

`ISIMEXEC` is a REXX command. Use this command for backward compatibility with earlier versions of the adapter.

Note: ISIMEXEC is replaced by ISIMEXIT. ISIMEXEC will be removed from the product in 2020.

The **`ISIMEXEC`** processing can present a zero or a non-zero return code when the processing is complete. A zero return code indicates successful processing of the **Acf2EXECNAME** attribute. If a non-zero return code is presented on exit, the adapter indicates that the **Acf2EXECNAME** attribute failed.

You can call other programs and perform file I/O as necessary. Processing is performed under the authority of the same CA ACF2 logonid that runs the CA ACF2 commands. You can run a valid TSO command if it does not prompt for a terminal user for input.

*Table 20: **ISIMEXEC** processing information*

Parameter #	Source	Value	Availability
1	IBM Security Privileged Identity Manager attribute of **erUid**	The value of the **erUid**.	Always, because this attribute accompanies all requests.
2	IBM Security Privileged Identity Manager attribute of **erAcf2EXECNAME**	The value of the **erAcf2EXECNAME**.	Always, because the availability of this attribute indicates that this exit must be started.
3	IBM Security Privileged Identity Manager attribute of **erAcf2EXECVAR**	The value of the **erAcf2EXECVAR**.	Based on the request generated by the IBM Security Identity server.

When the **erAcf2EXECNAME** attribute is available and optionally, the **erAcf2EXECVAR** attribute is available, the **ISIMEXEC** exit point is started as a TSO command in the command executor.

You cannot run the following command cannot during the add operation. However, you can run the command any time during the modify operation:

```
%ISIMEXEC erUid erAcf2EXECNAME erAcf2EXECVAR
```

If the **erAcf2EXECVAR** attribute is available during an add operation, run the command after the add operation. However, only the **erUid** attribute is available on the CA ACF2 user profile.

When the **ISIMEXEC** is processed, the **erAcf2EXECNAME** attribute can represent anything that you want to process. It provides a second-level command or exec name that you want to run.

Note:

- You can prevent the running of unauthorized commands for processing by interrogating the **erAcf2EXECNAME** attribute because **ISIMEXEC** always receives control.
- **ISIMEXEC** is never started during a delete command because the adapter presents only the **erUid** attribute.

Related concepts

ISIMEXIT command usage
ISIMEXIT is a REXX command. Use this command to start a REXX exec in response to a processing request from the IBM Security Identity server.

z/OS UNIX System Services considerations

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

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

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

Related concepts

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.

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

Customizing the adapter
You can do specific functions according to your requirements by using the REXX execs that are provided with the adapter installation.

Configuration notes
The ACF2 adapter can handle multiple requests simultaneously. Learn how the adapter processes specific attributes and requests and how it interacts with z/OS during the processing of some of the requests.

Configuration notes

The ACF2 adapter can handle multiple requests simultaneously. Learn how the adapter processes specific attributes and requests and how it interacts with z/OS during the processing of some of the requests.

Timezone support

The adapter converts all date values to UTC before it forwards them to the IBM Security Identity server. The adapter uses the $TZ timezone variable, specified in the environment settings for the adapter account, for example, ITIAGNT. The timezone variable specifies the offset that it must use to convert the local timezone to UTC. If there is no offset specified, the adapter assumes that the received date can be returned as UTC without any further conversion.

For instance, the TZ definition in `/etc/profile` or the adapter account-specific profile must be TZ=EST5, or TZ=EST5EDT for Daylight Saving Time, rather than TZ=EST.

OMVS AUTOUID

ACF2 adapter 6.0.6 and later supports auto-assignment of OMVS UIDs by using AUTOUID.

When you create a user in the IBM Security Identity server account form, enter 'AUTOUID'(case sensitive) in the attribute field. For example:

```
'INSERT IBMUSER UID(2345)'.
```

When the adapter receives the string AUTOUID from the IBM Security Identity server, the adapter runs the following command:

```
INSERT <USER> AUTOUID
```

For example

```
INSERT IBMUSER AUTOUID
```

Passwords

ACF2 adapter 6.0.5 and later support the reconciliation of password profile attributes. The following attributes are available:

- #PSWDCNT
- #PWD-TOD
- KEYFROM

All attributes are implemented as read-only and can be modified only with ACF2. The adapter is configured to replace the # sign in the attribute name with an additional P for internal usage. The account form on the IBM Security Identity server uses the correct label to display the attribute value for a selected account.

For example, attribute #PWD-TOD is displayed as #PWD-TOD on the IBM Security Identity server on the account form for a specific account. In the adapter log file, the initialized attribute is referred to as PPWD-TOD. PPWD-TOD is also the name of the attribute that is provided in the ACF2 and IBM Security Privileged Identity Manager schema files that are used by the adapter.

Password phrases

ACF2 adapter 6.0.4 and later, support ACF2 pass phrases. A pass phrase in ACF2 is an authentication mechanism that allows the secret string to be 9 - 100 characters. When you set passwords from the IBM Security Identity server, a string lesser than or equal to 8 characters is treated as a password. A string more than 8 characters is treated as a pass phrase. Starting with adapter version 6.0.13, the implementation of random password and pass phrase generation has changed. Random passwords and pass phrases are generated by using a configuration string, which determines the type and number of characters to be generated.

The default built-in string for passwords is `an$NaANa`

The default built-in string for pass phrases is `an$NaANa#aaNAa`

The password generator generates passwords as follows:

- For every occurrence of A, the adapter randomly generates a letter from A-Z
- For every occurrence of a, the adapter randomly generates a letter from a-z
- For every occurrence of N (uppercase!), the adapter randomly generates a numeric character from 0 - 9
- For any other character (including lowercase n), the adapter echoes that character back

Internally the adapter ensures that it does not generate the same characters consecutively. The built-in strings can be modified by using new registry settings:

- PWD_CONFIG for password configuration strings
- PWP_CONFIG for pass phrase configuration strings

PWD_CONFIG allows a maximum of 5 comma-separated strings, which are randomly selected by the adapter to generate random passwords. The size of each string must be 5 - 8 characters long. If a shorter string is specified, the adapter reports an error and tries another string. If a longer string is specified, the adapter uses only the first 8 characters to generate a password. The configuration string is not allowed to contain any of the following hard-coded reserved words:

```
ACF, APPL, APR, ASDF, AUG, BASIC, CADAM, DB2, DEC, DEMO, ENT ,FEB, FOCUS, GAME,
IBM, IMS, JAN, JUL, JUN, LOG, MAR, MAY, NET, NEW, NOV, OCT, OTIS, PASS, ROS,
SEP, SIGN, SONI, SYS, TEST, TSO, TSYS, VALID, VTAM, WELC, XXXX, 0000, 1111,
1234, 222, 3333, 4444, 5555, 6666, 7777, 8888, 9999, ', "
```

If a reserved word is found in the configuration string, the adapter reports an error.

After receiving an error, the adapter attempts to select another random configuration string. After two failed attempts, the adapter stops processing and returns an error. The adapter considers the first 4 characters of the *logonid* for the request it is processing as a reserved word. The adapter also reports an error if the first 4 characters of the *logonid* are part of the configuration string.

Reserved word and short *logonid* validation is case insensitive. Reserved word and short *logonid* validation is repeated for the generated password. If the adapter detects a reserved word and a short *logonid* as part of the generated password, the adapter stops processing and returns an error.

A new registry setting allows specifying additional reserved words: `RESWORD`.

Any comma-separated string that is found in the `RESWORD` registry setting value is added to the hard-coded reserved words list during request processing.

`PWP_CONFIG` allows a maximum of 3 comma-separated strings that are randomly selected by the adapter to generate random password phrases.

The adapter requires the size of each string to be 9 - 100 characters long. The string must have the minimal length that is specified in the ACF2 Password phrase rules. If a string of less than 9 characters is specified, the adapter reports an error and tries another string. If a string of more than 100 characters is specified, the adapter uses only the first 100 characters to generate a password phrase.

The configuration string is not allowed to contain single or double quotation marks.

If a single or double quotation mark is found in the configuration string, the adapter reports an error. After receiving an error, the adapter attempts to select another random configuration string. After two failed attempts, the adapter stops processing and returns an error.

For information on how to add and modify registry settings, see "Modifying non-encrypted registry settings" on page 51.

Other password phrase-related registry settings

Adapter version 6.0.8 introduced additional registry settings for pass phrase.

These additional registry settings allow customization of the actions to be taken when using the adapter to set pass phrases. You set the pass phrases using the password field on the IBM Security Identity server.

Registry setting for changing phrases

PASSGEN=ADD (generate random password on ADD account with pass phrase)

PASSGEN=MOD (generate random password on MODIFY account with pass phrase)

PASSGEN=NEVER (never generate a random password)

PASSGEN=BOTH (always generate a random password)

If not specified, PASSGEN defaults to BOTH

Note:

- IBM does not guarantee that the generated random passwords meet the site specific password rules.
- With PASSGEN set to NEVER or MOD, new accounts can only be requested using a password. When attempting to add a new account using a pass phrase with PASSGEN set to NEVER or MOD, the following error is returned:

  ```
  ERR:yy/mm/dd hh:mm:ss caacf2Add: pass phrases can NOT be used for INSERT for user <LID>
  ```

Registry settings for changing passwords

1. PWPMOD = RANDOM (generate a random phrase on MODIFY account with password)
2. PWPMOD=DISABLE (does not generate a random phrase, it disables pass phrase usage for this LID on MODIFY account with password)
3. PWPMOD=IGNORE (no changes are made for the pass phrase when the request is for changing a password)

If not specified PWPMOD defaults to RANDOM.

Note: IBM does not guarantee that the generated random pass phrases meet the site specific pass phrase rules.

PWPMOD=DISABLE ensures the pass phrase usage for a specified LID is disabled on account MODIFY. When changing a password for this LID, an additional registry setting is introduced to specify whether PWPALLLOW is automatically re-enabled when it receives a request to set a pass phrase for a LID.

1. AUTOPWP=TRUE (automatically set PWPALLOW when it receives a request to change a pass phrase)
2. AUTOPWP= FALSE (don't automatically set anything for the phrase when the request is for changing a phrase)

If not specified, AUTOPWP defaults to TRUE.

Make sure that the ACF2 requirements for pass phrases are included in the IBM Security Identity server rules for passwords. The requirements include setting the minimum characters in the password string to be more than 8 in the password policy. If the rules for password phrases employed at your installation site are not reflected in the IBM Security Identity server password policies, then ACF2 might reject the entered pass phrase.

In the existing documentation, all references to an ACF2 password now encompass both ACF2 passwords and pass phrases.

Temporary data set creation

Temporary data sets that are generated during reconciliation have a high-level qualifier (HLQ). The HLQ is equal to the adapter *logonid* instead of the generic HLQ. As such, the data sets are cataloged in the adapter *logonid* user catalog.

Custom Boolean attributes

The ACF2 adapter supports custom Boolean attributes that are defined as

- *<PRIVILEGENAME>* when privilege is granted to a user or
- NO *<PRIVILEGENAME>* when the user is not granted the privilege. For example: MYCICS or NOMYCICS specified for a specific ACF2 *logonid*.

For example, MYCICS or NOMYCICS is specified for a specific ACF2 *logonid*.

Single account lookup

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

To support multiple threads for LOOKUP transactions, a new registry setting is added to the **`agentCfg`** tool, which can be configured from the Advanced Settings Menu.

```
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:
```

The single account lookup is performed using the ACF2 report utility ACFRPTSL. Unlike the previous implementation, only the account that matches the `eruid` specified in the search filter is retrieved using ACFRPTSL. The ACFRPTSL report utility requires no additional configuration.

Specifying an empty prefix value

Running an ACF2 insert command with prefix() sets the default prefix (DFT-PFX) to the LID (12345) but it sets the restrictions to PREFIX().

See the command output below as executed directly in CA ACF2:

```

  LID
```

```
insert 12345 name(abc)   password(my1thPs!) prefix()
  12345                  12345 ABC
  ACCESS                 ACC-CNT(0) ACC-DATE(00/00/00) ACC-TIME(00:00)
  PASSWORD               KERB-VIO(0) KERBCURV() PSWA1TOD(00/00/00-00:00)
                         PSWA2TOD(00/00/00-00:00) PSWD-DAT(00/00/00) PSWD-EXP
                         PSWD-INV(0) PSWD-TOD(06/07/18-20:00) PSWD-VIO(0)
                         PSWDCVIO(0) PWP-DATE(00/00/00) PWP-VIO(0)
  TSO                    DFT-PFX(12345)
  STATISTICS             CRE-TOD(06/07/18-20:00) SEC-VIO(0)
                         UPD-TOD(06/07/18-20:00)
  RESTRICTIONS           PREFIX()
```

Note: The IBM Security Identity Manager server does not forward a blank value for prefix, unless the previously specified value for prefix is removed.

If a policy runs an `Account Modify` operation directly after adding an account with the LID specified as PREFIX, the IBM Security Identity Manager server registers the value that is specified for PREFIX for that account without running a reconciliation and the policy that modifies the account might blank the PREFIX value.

Related concepts

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.

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

Customizing the adapter
You can do specific functions according to your requirements by using the REXX execs that are provided with the adapter installation.

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.

Chapter 6. Troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Note: If you encounter a problem, enable all levels of activity logging (debug, detail, base, and thread). The adapter log contains the main source of troubleshooting information. See "Changing activity logging settings" on page 47.

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Problem descriptions help you and the IBM technical-support representative find the cause of the problem. This step includes asking yourself basic questions:

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Related concepts

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

Error messages and problem solving

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

Known issues and limitations
You might encounter some issues or limitations when you install, configure, or use the adapter.

Adapter SSL information collection for support requests
If you encounter an SSL related problem, you must first gather the necessary information before you contact Support for assistance.

Related tasks

Installing test fixes and diagnostic builds
IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

Related reference

Frequently asked questions

Logs

When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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

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

Table 21: Example of Adapter log details

Details	**Example values**
Installation path	`/var/ibm/isimcaacf2`
Adapter log name	*`CAACF2Agent`*
Log location	`/usr/itim/log/`
Log files	• *`CAACF2Agent`*`.log` • *`CAACF2Agent`*`.log_001` • *`CAACF2Agent`*`.log_002` • *`CAACF2Agent`*`.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 25.

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Error messages and problem solving

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

Known issues and limitations
You might encounter some issues or limitations when you install, configure, or use the adapter.

Adapter SSL information collection for support requests
If you encounter an SSL related problem, you must first gather the necessary information before you contact Support for assistance.

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.

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

Table 22: Error messages, warnings, and corrective actions

Error message or warning	Additional warnings, messages, or information	Corrective action
CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again.	An IO error occurred while sending a request. `Error:Connection refused: connect`	Ensure that the adapter service is running. For more information about starting the adapter service, see "Restarting the adapter service" on page 14.
	The adapter returned an error status for a bind request. Status code: invalid credentials adapter error message: `Authentication Failed`	Check the adapter authentication ID and password match the installed values. See the screen for Adapter-specific parameters in "Running the ISPF dialog" on page 9.
	An IO error occurred while sending a request. Error: `com.ibm.daml.jndi.JSSESocketConnection.HANDSHAKE_FAILED:`	If SSL is enabled, check the configuration. See "Configuring SSL authentication" on page 62. The adapter log contains details about the certificates loaded during initialization.
caacfAdd: User *userid* add Successful. Some attributes could not be modified.		This warning occurs when a user is created, however, some additional attributes failed. For more information, see the adapter log file.
caacf2Modify: Some attributes unsuccessful.		This warning occurs when a user is modified, however, some additional attributes failed. For more information, see the adapter log file.

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

Error message or warning	Additional warnings, messages, or information	Corrective action
caacf2Modify: All attributes unsuccessful.		The modify request failed to set the attributes on the managed resource. For more information, see the adapter log file.
caacf2Search: Reconciliation did not return at least 1 Logonid.		During the reconciliation request, no Logonids were returned. For more information, see the MVS system log and the adapter log.
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 adapter's CA ACF2 logonid.

`ACF04056 ACCESS TO RESOURCE BPX.SRV.<SURROGATID> TYPE RSUR BY <ADAPTERID>`		`set res(sur)`
		`comp`
		`$KEY(BPX.SRV.<SURR`
		`OGATID>) TYPE(SUR) UID(<ADAPTERID>)`
		`ALLOW`
		`SERVICE(READ)`
		`store`
		`f acf2,rebuild(sur)`
		`end`

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

Known issues and limitations
You might encounter some issues or limitations when you install, configure, or use the adapter.

Adapter SSL information collection for support requests
If you encounter an SSL related problem, you must first gather the necessary information before you contact Support for assistance.

Related tasks

Installing test fixes and diagnostic builds
IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

Related reference

Frequently asked questions

Installing test fixes and diagnostic builds

IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

About this task

These fixes can consist of either an `<ADAPTER>.UPLOAD.XMI` file or a zip file containing a new adapter or ADK binary.

XMI files require a full new install. These are usually provided when several components have changed compared to the release you currently had installed. To ensure that there are no inconsistencies between the versions of the components you have installed and the updated components that were used to created the fix, you must perform the full installation from scratch using the XMI that contains the fix.

You receive a zip file that contains one or more binaries if the changes that the fix requires are limited to the adapter or ADK code. These new binaries must be used to replace the binaries that have the same name in your existing adapter installation.

The steps to install a new ADK binary are identical to the steps to install a new agent binary. The steps to install a new ADK library are also identical to the steps to install a new agent binary with the exception of the location where the libraries are stored. The libraries can be found in and uploaded to the `read_only_home/lib` folder.

Follow the procedures below to install a new agent binary.

Procedure

1. Extract the binary from the zip file.
2. Stop the adapter.
3. Change the directory with `cd read_only_home/bin` folder.
4. Copy `<adaptertype>Agent <adaptertype>Agent.save`.
5. Upload `<adapterype>Agent` in binary ftp mode to the adapter host and store it in the `read_only_home/bin` folder.
6. Change the directory with `cd read_only_home/bin` folder.
7. Change the permissions with `chmod 755 <adaptertype>Agent`.
8. Specify the extended attributes with `extattr +ap <adaptertype>Agent`.
9. Start the adapter.

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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

Known issues and limitations
You might encounter some issues or limitations when you install, configure, or use the adapter.

Adapter SSL information collection for support requests

If you encounter an SSL related problem, you must first gather the necessary information before you contact Support for assistance.

Related reference

Frequently asked questions

Known issues and limitations

You might encounter some issues or limitations when you install, configure, or use the adapter.

Read-only attributes

The CA ACF2 schema is customizable and the list of read-only attributes might be unique for your system. The standard list includes:

- ACC-CNT
- ACC-DATE
- ACC-SRCE
- CRE-TOD
- CSDATE
- CSWHO
- GRP-USER
- HOMENODE
- KERBCURV
- LID
- PSWD-MIX
- PSWD-SRC
- PSWD-TOD
- UID
- UPD-TOD
- #PSWDCNT
- #PWD-TOD
- KEYFROM
- PWP-HST
- PWP-TOD
- PWPA1TOD

Unsupported data segments

For the current overview, see the Release Notes in the adapter package.

Special characters in the attribute names

For password profile attributes the adapter is configured to replace the # sign in the attribute name with an additional P for internal usage. The account form on the IBM Security Identity server uses the correct label to display the attribute value for a given account. To provide an example: Attribute `#PWD-TOD` is displayed as `#PWD-TOD` on the IBM Security Identity server on the account form for a specific account. In the adapter log file, the initialized attribute is referred to as `PPWD-TOD` which is also the name of the attribute provided in the ACF2 and IBM Security Privileged Identity Manager schema files used by the adapter.

Adapter installation generates a schema to be incorporated into the adapter profile, and a matching cross-reference table for the adapter task. When generated, the schema and cross-reference table files, must be scanned for attribute names that contain the following characters **-**, **$**, *****. Those characters must be replaced with an alphanumeric character. The adapter profile does not install correctly if the attribute names contain any of these characters.

Before building and importing the profile, you must scan and replace the generated `ISIMSCHM` file for all references of the invalid attribute name. For example:

```
<!-- ******************************************************** -->
<!-- erAcf2ICLASS* -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
<name>erAcf2ICLASS*</name>
<description>ICLASS-* in segment BASE</description>
<objectidentifier>1.3.6.1.4.1.6054.3.156.1.120</objectidentifier>
<objectidentifier>erAcf2ICLASS*-oid</objectidentifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
...
<attribute ref = "erAcf2ICLASS*" required = "false" />
```

Replace the ***** with **a**.

```
<!-- ******************************************************** -->
<!-- erAcf2ICLASSa -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
<name>erAcf2ICLASSa</name>
<description>ICLASS-* in segment BASE</description>
<objectidentifier>1.3.6.1.4.1.6054.3.156.1.120</objectidentifier>
<objectidentifier>erAcf2ICLASSa-oid</objectidentifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
...
<attribute ref = "erAcf2ICLASSa" required = "false" />
```

The generated cross-reference file `ACF2SCHM` must be updated so the attribute names match. The ACF2 field names must be left untouched. For example change

```
ICLASS-* erAcf2ICLASS* BASE BINARY S * * 000004 0003
```

to

```
ICLASS-* erAcf2ICLASSa BASE BINARY S * * 000004 0003
```

Note:

- Attribute names must not be duplicated. Be sure that the attribute name you are creating does not exist.
- Attribute names are restricted to 14 characters. Replace one existing character with one new character.

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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

Adapter SSL information collection for support requests
If you encounter an SSL related problem, you must first gather the necessary information before you contact Support for assistance.

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

Adapter SSL information collection for support requests

If you encounter an SSL related problem, you must first gather the necessary information before you contact Support for assistance.

This information assumes specifications for VTAM® APPLIDs and user IDs indicated in the installation guide. Replace these APPLIDs and user IDs with those IDs you selected for the adapter installation.

- The CA ACF2 Adapter log file, from the USS file system.
- An excerpt from the MVS SYSTEM log, from the same time frame as the failure.
- A screen capture of the ACF2 service form, describing the connection to this adapter.
- A display from the adapter utility `agentCfg` describing the adapter parameters:

  ```
  F.  Registry Settings. -> A.  Modify Non-encrypted registry settings
  ```

- The results from the following job (include all the output produced). A CA ACF2 administrator with authority to view all the indicated profiles must run this job.

  ```
  //ACF2LIST JOB ACCT,IBM,CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID
  //TMP      EXEC PGM=IKJEFT01,REGION=0K
  //SYSTSPRT DD SYSOUT=*
  //SYSTSIN  DD *
  ACF
  SET LID
  LIST ISIAGNT
  LIST ISIAGNT PROFILE(ALL)
  ```

  ISIAGNT is the name of the adapter started task.

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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

Known issues and limitations
You might encounter some issues or limitations when you install, configure, or use the adapter.

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

Frequently asked questions

Where can I find registry and/or permission related errors?

In ISPF, navigate to S (SDSF), LOG.

How can I disable persistent connections between the Identity Server and the adapter?

The first is in IBM Security Identity Manager. The setting must be explicitly placed in enRole.properties: `com.ibm.daml.jndi.DAMLContext.POOL_MAX_SIZE=0`

This effects disable the connection pool.

The other setting is on the adapter side. Invoke `agentCfg` and navigate to **B. Protocol Configuration** > **C. Configure Protocol** > **A. DAML** > **K. READ_TIMEOUT** and specify a value in seconds. For example, 30 seconds. Save and restart the adapter. This causes the adapter to timeout any socket that has not responded within 30 seconds.

How can I monitor if the adapter is up and running?

To check the availability of your adapter, ensure that the `DAML_PORT` is listening. The default port is 45580. If you probe and the port is not listening, the adapter is down.

Why is my registry file cleared?

There might be several causes. To determine the cause, provide an answer to the following questions when contacting support:

- Were there any messages in the SDSF SYSLOG (S.LOG) at the time the adapter was started and the registry file had been reset?
- Is it possible the adapter was started before the file system was mounted?
- Does the `read_only_home` directory exist when the filesystem is not mounted?
- Can you find registry files that have been created in `/tmp`?
- Is the file system shared between different hosts?
- Does the registry file exist on the file system at the time it was reset?

It might be useful to collect the output from the following commands at the time a correct, configured registry file is active and compare that output to the output for the same commands after an IPL when you notice the registry is reset:

```
df -k /adapter_readwrite_home
ls -Elg /adapter_readwrite_home/data
/adapter_readwrite_home/bin/regis /adapter_readwrite_home/data/<adapter_name>.dat -list
```

How can I see what information is being send and received to and from the adapter by the ISIM server?

Edit `enRoleLogging.properties` in `$ISIM_HOME\data` to set the DAML line `logger.trace.com.ibm.daml.level` and the remote services line `logger.trace.com.ibm.itim.remoteservices.level` to DEBUG_MAX.

The `daml.level` setting enables full tracing for DAML based adapters and the remote services trace captures information that 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
```

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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

Known issues and limitations
You might encounter some issues or limitations when you install, configure, or use the adapter.

Adapter SSL information collection for support requests
If you encounter an SSL related problem, you must first gather the necessary information before you contact Support for assistance.

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. Uninstalling

To remove an adapter from the IBM Security Identity server for any reason, you must remove all the components that were added during installation. Uninstalling the adapter involves several tasks such as removing the started JCL task, the directories from the UNIX System Services environment, and the ISPF dialog libraries.

Procedure

1. Stop the adapter, if it is running. See "Restarting the adapter service" on page 14.
2. Remove the started task JCL from the system procedure library.
3. Remove the `read-only` and `read/write` directories from the z/OS UNIX System Services environment.
4. Remove the CNTL, EXEC, and LOAD libraries that are related to the adapter.
5. Remove the ISPF dialog libraries for customization.

Chapter 8. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables..

Adapter attributes

The IBM Security Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

The CA ACF2 for z/OS schema is modifiable which makes the adapter dynamic. The ACF2 installation augments the ACF2 schema before the installation. The augmentation in the schema varies depending on the operating system settings. In this case, you must configure the adapter to support the additional attributes defined in the schema.

The adapter installation process extracts the ACF2 schema and stores it for use at run time. The installation process builds the `schema.dsml` file. You must merge the `schema.dsml` file to the `CAACF2Profile.jar` file before importing the profile to the IBM Security Identity server.

The following table describes the format of the schema file.

Table 23: Schema file format

Column	Description	Value
1-8	The ACF2 native attribute name.	-
10-24	The IBM Security Privileged Identity Manager attribute name.	-
26-33	The segment name.	For the ACF2 LID attributes, they are marked as BASE.
35-42	The attribute type.	`CHAR, BOOLEAN, BINARY, HEX FULLTOD, PACKDATE`
44	The single or multi-valued attribute	S for single and M for multi-valued.
46	The quotable attributes.	Q for quoted and * for non-quoted.
48	The null fields.	If N is denoted, the field has a null value.
50-55	The internal ACF2 attribute length.	-
57-60	The ACF2 group number assigned to this attribute.	-

The following table describes an example of a ACF2SCHM file that is created during the adapter installation.

Table 24: Example of a ACF2SCHM file

ACF2 native attribute name	IBM Security Privileged Identity Manager attribute name	Segment name	Attribute type	Single or multi-valued attribute	Quoted attribute	Nullable field	Internal ACF2 attribute length	ACF2 group number assigned to this attribute
ACC-CNT	erAcf2ACCCNT	BASE	BINARY	S	*	*	000004	0003
ACC-DATE	erAcf2ACCDATE	BASE	FULLTOD	S	*	*	000008	0003
ACC-SRCE	erAcf2ACCSRCE	BASE	CHAR	S	*	*	000008	0003
ACCOUNT	erAcf2ACCOUNT	BASE	BOOLEAN	S	*	*	000001	0002
ATTR2	erAcf2ATTR2	BASE	HEX	S	*	*	000002	0005
CSDATE	erAcf2CSDATE	BASE	PACKDATE	S	*	*	000004	0001
OPCLASS	erAcf2OPCLASS	CICS	BINARY	M	*	*	000001	0000
ASSIZE	erAcf2ASSIZE	OMVS	BINARY	S	*	*	000004	0004

Registry settings

The adapter has several registry settings. See the table for these registry options, their descriptions, and values, if any.

Table 25: Registry settings and additional information

Option attribute	Default value	Valid value	Description	Required
DATAFORMAT	None	3 characters	The date format for this attribute must match the configured date format in ACF2.	Yes
PASSEXPIRE	TRUE	TRUE or FALSE	This attribute is the default action that the adapter must perform when the adapter receives a password change request. TRUE indicates that passwords must be set as expired. FALSE indicates that passwords must be set as non-expired.	No
SYSEXEC	None	1 - 44 characters	This attribute identifies the adapter EXEC library	Yes

Table 25: Registry settings and additional information(continued)

Option attribute	Default value	Valid value	Description	Required
PASSGEN	BOTH	ADD, MOD, NEVER, or BOTH	Registry setting for changing phrases: • PASSGEN=ADD: Generate random password on ADD account with pass phrase • PASSGEN=MOD: Generate random password on MODIFY account with pass phrase • PASSGEN=NEVER: Never generate a random password • PASSGEN=BOTH: Always generate a random password If not specified, the default PASSGEN value is BOTH. **Note:** IBM does **not** guarantee that random passwords generated meet the site-specific password. With the PASSGEN value set to NEVER or MOD, new accounts can be requested only by using a password. When you are adding a new account with a pass phrase with PASSGEN set to NEVER or MOD the following error is returned:`ERR:yy/mm/dd hh:mm:ss caacf2Add: pass phrases can NOT be used for INSERT for user <LID>`	No
PWD_CONFIG	None	comma separated list	PWD_CONFIG will allow a maximum of five (5) comma-separated strings which will be randomly selected by the adapter to generate random passwords. The size of each string should be between 5 and 8 characters long.	No

Table 25: Registry settings and additional information (continued)

Option attribute	Default value	Valid value	Description	Required
PWP_CONFIG	None	comma separated list	PWP_CONFIG will allow a maximum of three (3) comma-separated strings which will be randomly selected by the adapter to generate random password phrases . The adapter requires the size of each string to be between 9 and 100 characters long, the string should however be at minimum as long as the minimal length.	No
PWPMOD	RANDOM	RANDOM, DISABLE, or IGNORE	Registry settings for changing passwords: • PWPMOD = RANDOM: Generate a random phrase on MODIFY account with password • PWPMOD=DISABLE: Disables pass phrase usage for this LID on MODIFY account with password • PWPMOD=IGNORE: No changes are made for the pass phrase when the request is for changing a password If not specified, the default PWPMOD value is set to RANDOM. IBM does **not** guarantee that random passwords generated meet the site-specific pass phrase rules.	No
RESWORD	None	comma separated list	Any comma-separated string found in the RESWORD registry setting value will be added to the hard-coded reserved words list during request processing.	No

Table 25: Registry settings and additional information (continued)

Option attribute	Default value	Valid value	Description	Required
AUTOPWP	TRUE	TRUE or FALSE	Registry setting for changing phrases: PWPMOD=DISABLE ensures pass phrase usage for a specified LID is disabled on account MODIFY when changing a password for this LID an additional registry setting has been introduced to specify if PWPALLLOW should automatically be re-enabled when receiving a request to set a pass phrase for a LID. • AUTOPWP=TRUE: Automatically set PWPALLOW when receiving a request to change a pass phrase • AUTOPWP=FALSE: Does not automatically set anything for the phrase when the request is for changing a phrase If not specified, the default AUTOPWP value is set to TRUE.	No
USE_SSL	TRUE	TRUE or FALSE	Registry setting for enabling or disabling SSL. Its default value is TRUE. You must install a certificate when SSL is enabled. For more information, see "Configuring SSL authentication" on page 62.	No
RECHLQ	ISIAGNT	Valid LID	Used when allocating data sets during reconciliation.	No

Environment variables

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

Table 26: CA ACF2 Adapter environment variables

Environment variable	Description	Default value	Required
PROTOCOL_DIR	Specify the location of adapter protocol modules, for example, the `./lib` directory	LIBPATH	No

Table 26: CA ACF2 Adapter environment variables (continued)			
Environment variable	**Description**	**Default value**	**Required**
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 upper case, with `.dat` suffixed to the name.	Current working directory.	No
PDU_ENTRY_LIMIT	Specify the maximum number of accounts that are kept in the main storage.	3000	No
LIBPATH	Specify the location of the Dynamic Link Library (DLL) and `.so` files.	-	Yes

_CEE_RUNOPTS	Language environment run-time options for heap allocation. For more information, see https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.ceea300/ceea30010.htm.	`'HEAP(12500K,8K,ANYWHERE,,1K,1K),AN(2450K,4K,ANY`
		`4,1,32,1,56,2,72,1,136,1,296,1,480,1,848,1,2080,`
			Yes

Index