IBM Security Verify Governance
10.0

Broadcom Top Secret for z/OS Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

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

Adapters can be installed on the managed resource. The 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 Identity server.

IBM Security Verify Governance works with Top Secret in an MVS™ environment. The Top Secret Adapter:

- Receives provisioning requests from IBM Security Verify Governance.
- Processes the requests to add, modify, suspend, restore, delete, and reconcile user information from the Top Secret database.
- Converts the Directory Access Markup Language (DAML) requests that are received from IBM Security Verify Governance to corresponding Top Secret for z/OS commands by using Enrole Resource Management API (ERMA) libraries.
- Forwards the commands to a command executor through a series of R_admin (IRRSEQ00) requests. The command executor receives the formatted Top Secret for z/OS® command strings and sends the command to the adapter through the R_admin callable service.
- Returns the results of the command including the success or failure message of a request to IBM Security Verify Governance.

The following figure describes the various components of the adapter.

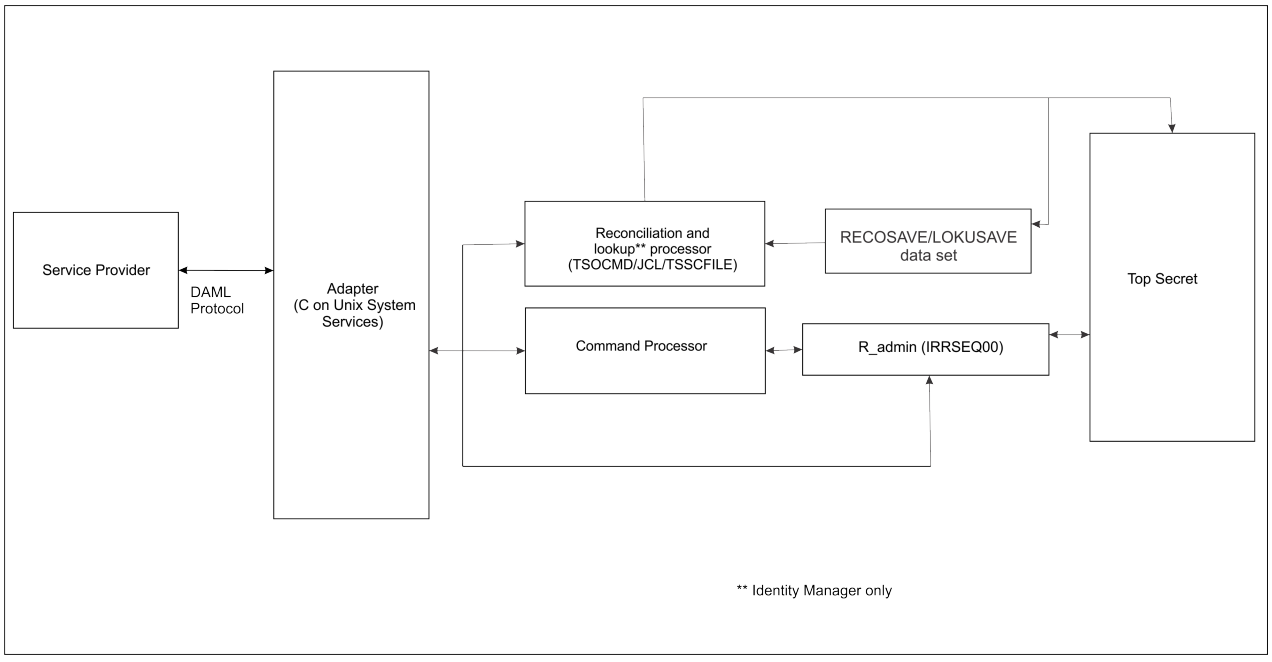


Figure 1. The Top Secret Adapter components

Adapter

Receives and processes requests from IBM Security Verify Governance. The adapter can handle multiple requests simultaneously. Each request results in execution of an IRRSEQ00, TSO/E and/or Rexx) transaction. The binaries of the adapter and related external files reside in the Unix System Services environment of z/OS (OS/390®).

Command Executor

Operates as an IRRSEQ00 transaction that is triggered from an incoming request from the adapter. IRRSEQ00 requests consist of commands. The adapter runs these commands with the Command Executor in an MVS environment.

Reconciliation Processor

The processor operates as an TSO/E , JES transaction that is triggered by an incoming request to the adapter. By default, the Reconciliation Processor submits a job that runs the Top Secret database unload utility (TSSCFILE) to obtain data. You can also modify the Job Control Language (JCL) to read an existing input file that the TSSCFILE utility produces.

Note: When you submit a reconciliation request from IBM Security Verify Governance, the Reconciliation Processor component runs the TSSCFILE to unload the Top Secret database. This creates a file that contains the required contents of the Top Secret database.

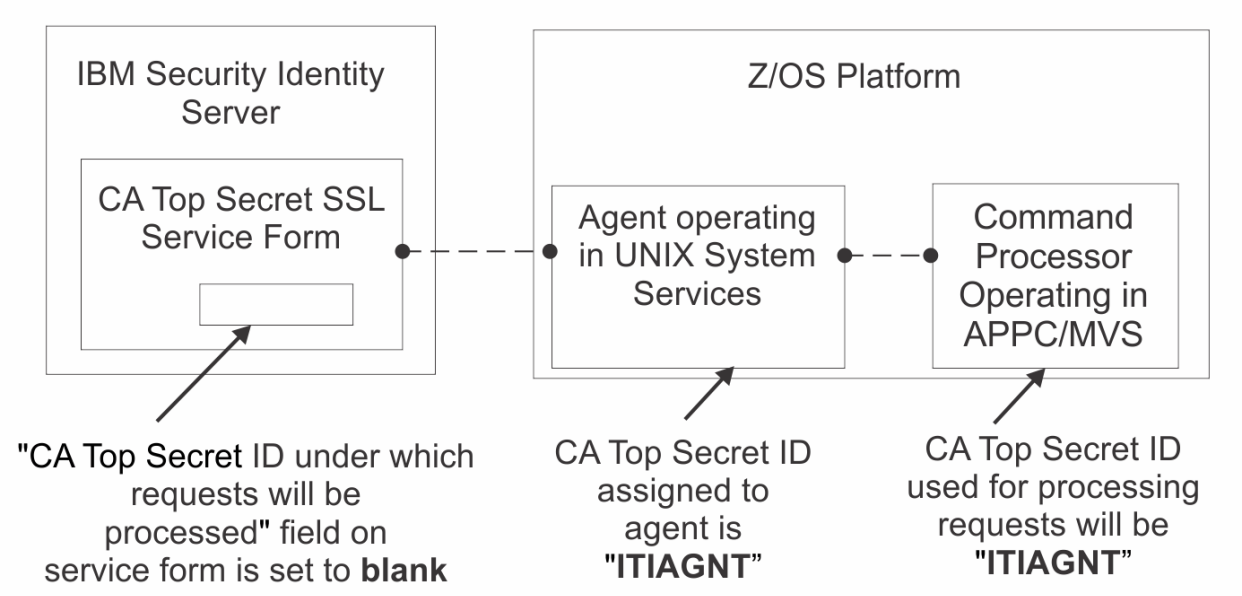
Adapter considerations

The Top Secret Adapter requires APF authorization.

The Top Secret Adapter operates in two modes.

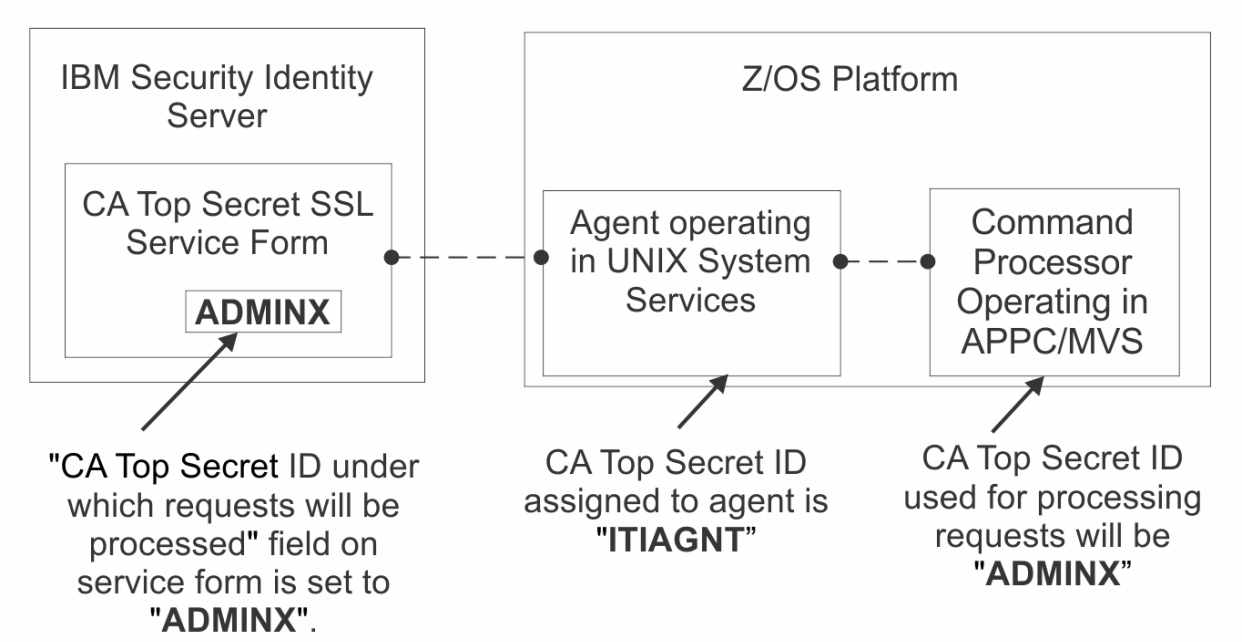
- If no operational ACID is specified on the IBM Security Verify Governance service form when a request is issued, the ACID that the adapter uses requires specific privileges. For example, if the adapter administers all users in the Top Secret database (apart from creating type SCA users), it must operate with Security Administrator (SCA) type of Top Secret ACID.

  If IBM Security Verify Governance performs operations against only a portion of the Top Secret database, the adapter must be associated with a security administrator with the appropriate privileges for the portion of the database it administers. The following figure depicts the preceding scenario.



- If the operations are performed under an ACID specified on the IBM Security Verify Governance service form, the Top Secret ACID the adapter uses does not require any special privileged attributes. It does, however, require surrogate authority to run functions under the identity of the ACID specified on the IBM Security Verify Governance Identity Manager service form. The ACID specified on the IBM Security Verify Governance service form must have authority to perform the administration functions requested by the Identity server.

  The following figure depicts the preceding scenario:



The Top Secret resources that require consideration are:

FACILITY class profile STGADMIN.IGG.DEFDEL.UALIAS, with READ

The adapter requires permissions to update the master catalog. Therefore, the adapter ACID must have one of the following permissions:

- UPDATE access to the DATASET class profile that protects the master catalog.
- UPDATE,CREATE,SCRATCH access to the 'hlq' that is used for the reconciliation and lookup job intermediate data sets.
- READ access to the FACILITY class profile that protects the STGADMIN.IGG.DEFDEL.UALIAS resource. The FACILITY class profile can update the master catalog irrespective of the FACILITY class profile name.

SURROGAT class

The adapter must run under a valid CA Top Secret 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 ensure that the output for the following command is never empty if the adapter is running: ` ps -ef | grep -i <ADAPTERID> | grep -v grep`

The adapter requires READ permission to be defined for the ADAPTER user and/or SURROGATE user on the following resources:

Table 1.

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

When using a surrogate ID , the adapter ID requires UPDATE on IBMFAC BPX.SERVER, otherwise it requires READ. When using a surrogate ID, the adapter ID requires READ on IBMFAC BPX.SRV.*surrogateid*

Related concepts

Adapter interactions with the Identity server
The Top Secret Adapter uses IBM Security Verify Governance to perform user tasks on Top Secret for z/OS.

Adapter interactions with the Identity server

The Top Secret Adapter uses IBM Security Verify Governance to perform user tasks on Top Secret for z/OS.

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

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

SSL requires digital certificates and private keys to establish communication between the endpoints. Regarding SSL, the Top Secret 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 (Verify Governance) must contain the Certificate Authority or CA certificate.

To enable SSL communication by default, install a digital certificate and a private key on the adapter and install the CA certificate on the Verify Governance server.

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. When you specify the port number on the adapter service form on IBM Security Verify Governance, make sure 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 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 Top Secret Adapter. To protect these ports with the Top Secret protection, define the profiles in the Top Secret Adapter SERVAUTH resource class. For more information, see the z/OS Communications Server, IP Configuration Guide.

Related concepts

Adapter considerations
The Top Secret Adapter requires APF authorization.

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.

Prerequisites

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

Table 2. Prerequisites to install the adapter	
Operating System	See the Release Notes® for the supported software versions.
Network Connectivity	TCP/IP network
Server Communication	Communication must be tested with a low-level communications ping from the Identity server to the MVS Server. When you do so, troubleshooting becomes easier if you encounter installation problems.
Identity server	See the Release Notes for the supported software versions.
Required authority	To complete the adapter installation procedure, you must have system administrator authority.

Related concepts

Software download

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

Software download

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

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.

Uploading the adapter package

You can upload the adapter package on z/OS.

Procedure

1. Obtain the software. See Software Download.
2. Extract the installation package on your local workstation and ensure that a file named `VERTSS.UPLOAD.XMI` exists. The file is in the z/OS Time Sharing Option (TSO) TRANSMIT/RECEIVE format.
3. On the z/OS operating system, use the TSO to allocate a sequential `VERTSS.UPLOAD.XMI` file with the following parameters:
   - RECFM=FB
   - LRECL=80
   - 400 MB of space
4. Upload the extracted `VERTSS.UPLOAD.XMI` file with a Binary transfer method, such as FTP or 3270 file transfer (IND$FILE).
5. Receive the uploaded file with the TSO `RECEIVE` command:

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

6. Press **Enter** to create a Partitioned Data Set (PDS) file named, *`userid`*`.VERTSS.UPLOAD`, where, *`userid`* is your TSO User ID.

Related concepts

Communication configuration
You must complete several tasks that configure the IBM Security Verify Governance Identity Manager server to communicate with the adapter.

Related tasks

Installing the ISPF dialog
Install the ISPF dialog to install and configure the Top Secret Adapter.

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 to install and configure the Top Secret Adapter.

Before you begin

Note: This dialog requires a model 3 or model 4 3270 display.

Procedure

1. Log on to a z/OS operating system.
2. From ISPF 6 option, run the INSTALL1 exec:

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

   where *userid* is your TSO User ID.
3. Specify a high-level qualifier (hlq) for the data sets that the INSTALL1 exec creates. When you do not specify a high-level qualifier, the exec uses your TSO User ID as the high-level qualifier. Specify another hlq to use the ISPF dialog in the future.
4. Enter BATCH or ONLINE (not case-sensitive) to specify whether to create a batch job stream or complete the file extraction online.

   If you enter BATCH, you must modify the generated INSTALL2 and submit it.

Results

When you run the exec, the exec creates the listed hlq data sets.

Table 3. ISPF dialog data sets

High-level qualifier	Library
hlq.SAGTCENU	CLIST/EXEC library
hlq.SAGTMENU	ISPF message library
hlq.SAGTPENU	ISPF panel library
hlq.SAGTSENU	ISPF skeleton library

Note: The AGTCCFG exec allocates the libraries.

Related concepts

Communication configuration
You must complete several tasks that configure the IBM Security Verify Governance Identity Manager server to communicate with the adapter.

Related tasks

Uploading the adapter package
You can upload the adapter package on z/OS.

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.

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 have selected. The JCL job streams are required for adapter installation. Before you perform this task, you must install the ISPF dialog.

To run the ISPF dialog, perform the following steps:

Procedure

1. Log on to TSO on the z/OS operating system.
2. From ISPF 6 option, run the following command to start the ISPF dialog:

```
EXEC ‘hlq.SAGTCENU(AGTCCFG)'
```

   The License page is displayed.
3. Press **Enter** to display this screen.

```
AGTP01 ------------ VERIFY Top Secret Adapter Customization ------------------
Option ===>                                          Location:  1



  Initial Customization

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

    2  Customize to support user-defined ACID fields
       If you have user-defined fields in the FDT, 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.
4. Select **Initial Customization** to display the Initial Customization page that lists the high-level tasks that you must perform.

```
AGTP1 ------------ VERIFY Top Secret Adapter Customization ------------------
 Option ===>                                          Location:  1-> 1

   Initial Installation

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

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

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

```
AGTP11 ------------ VERIFY Top Secret Adapter Customization ------------------
 Option ===>                                          Location:  1->1-> 1

  Load Variables

     The IBM supplied defaults are in VERTSS.SAGTCENU(AGTCDFLT)
     If you remove the name specified below, the defaults will be loaded.

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

     ===> IBMUSER.VERTSS.CONFIG
```

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

```
AGTP12 ------------ VERIFY Top Secret Adapter Customization ------------------
 Option ===>                                          Location:  1->1-> 2

  Specify or Alter variables for this configuration.

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

     2     Adapter communication parameters
           Define / alter identity server to adapter communication parameters.

     3     Top Secret reconciliation settings
           Define / alter Top Secret specific adapter runtime parameters

     4     Top Secret reconciliation settings - storage
           Define / alter storage allocation settings.

     5     Adapter specific parameters.
           Define / alter identity server to adapter runtime
parameters.

        ** Indicates option has been visited during this session.

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

a. Select **Disk location parameters** to define or alter data set and UNIX System Services (USS) locations.

```
AGTP121 ------------ VERIFY Top Secret Adapter Customization ------------------
 Option ===>

   Input Data Sets

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

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

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

    USS Adapter read/write home
     ===> /var/ibm/security/vertss

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

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

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

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

Unix System Services (USS) Adapter read-only home
Specifies the location where the adapter USS binaries 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 specify 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.

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

c. Select **Adapter communication parameters** to define or alter the IBM Security Verify Governance or adapter run time parameters.

```
AGTP122 ------------ VERIFY Top Secret Adapter Customization ------------------
 Option ===>

Adapter communication parameters

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

   Adapter authentication ID (internal)         ===> agent

   Adapter authentication password (internal)   ===> agent

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

   Disable TLS1.0                               ===> TRUE

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

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

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

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

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

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

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

e. Select Top Secret **reconciliation settings**.

```
AGTP123 ------------ VERIFY Top Secret Adapter Customization ------------------
Option ===>

Top Secret reconciliation settings
    Is the adapter to run data base unload?   ===> TRUE (True or False)

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

Optional JOBCHAR to be used for RECOJOB  ===>

PDU backlog limit  ===> 1000
```

The adapter must know the names of the data sets containing the Top Secret database. If you specify TRUE for the adapter to run the database unload, then the reconciliation process runs the TSSCFILE (Top Secret database unload) utility. In this case, you must verify the names of the Top Secret data sets or overwrite them according to your installation specifications.

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

JOBCHAR
Optional. Specifies the character to be added to the RECOJOB job name when submitted. A JOBCHAR is required either in the JOBNAME in the JCL or in the JOBCHAR registry setting if you change the name of the JOB from RECOJOB to the name of an existing User ID. See The JOB Statement.

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

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

g. Select **Top Secret reconciliation settings – storage**.

```
AGTP124 ------------ VERIFY Top Secret Adapter Customization ------------------
 Option ===>

 Top Secret reconciliation -  storage

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

   Temporary reconciliation data set name
    ===>

   Temporary single account lookup data set name
    ===>
```

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

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

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

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

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

Note:

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

The adapter can now be configured to read directly from a predefined RECOSAVE data set that has been created by a process or operation that has previously run RECOJOB. To enable this feature a distinction had to be made between the data set that is used to collect and process the output for a full reconciliation and the data set that is used to collect and process the output of a single account lookup operation.

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

8. Press FP3 to return to the Initial Installation panel.
   a) Select **Adapter specific parameters** to define or alter the IBM Security Verify Governance or adapter run time parameters.

```
AGTP125 ------------ VERIFY Top Secret Adapter Customization ------------------
 Option ===>

 Adapter specific parameters

    Name of adapter instance                      ===> CATSSAGENT

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

    PDU backlog limit                             ===> 1000

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

    Top Secret SCA ACID for  adapter       ===> CATAGT

    Password for the Verify adapter ACID            ===> *****
    Top Secret Default Group ACID for adapter  ===> STCUSS

    OMVS UID to be assigned to ACID (non-zero)    ===> 45580

Adapter operations parameters

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

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

Use 3 or 4 digits for profile sequence?           ===> 3 (3, 4)
```

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. This name is also used to create an entry in the STC Top Secret table.

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

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

Top Secret SCA ACID for Verify adapter
Specifies the Top Secret Security Administrator (SCA) ACID that the adapter task is assigned to.

Password for the Verify adapter ACID
Specifies the password for the Top Secret Security Administrator(SCA) ACID that the adapter task is assigned to.

Top Secret Default Group ACID for adapter
Specifies a Top Secret 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 ACID (non-zero)
Specifies a unique UID number for the SCA ACID. Ensure that you specify a non-zero number as the UID number.

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

Do you want passphrases set as expired
Specifies whether the passphrases must be set as expired or non-expired. The default value is set to TRUE; however, you might change it to FALSE if you want all the passphrases set as non-expired.

Use 3 or 4 digits for profile sequenced
Specify whether to use 3 or 4 digits to specify the profile update sequence (PROFDIG registry value). For 3 digits, use the format `010|PROFA`. For 4 digits, use the format `0010|PROFA`. The default value is 3.

b) Press **PF3** to return to the **Initial Installation** panel.

9. Select **Generate Job Streams**.
10. 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.

```
AGTP14 ------------ VERIFY Top Secret Adapter Customization ------------------
 Option ===>

  Generate the job streams

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

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

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

11. 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.

```
AGTP13 ------------ VERIFY Top Secret Adapter Customization -----------------
 Option ===>

  Save variables to a data set.

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

     ===> IBMUSER.VERTSS.CONFIG
```

12. 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*.VERTSS.CNTL(INSTRUCT) data set. Follow the instructions specified in the *hlq*.VERTSS.CNTL(INSTRUCT) data set to complete the configuration.

Results

After completing the steps for running the ISPF dialog, the adapter is configured in a non-secure mode. To configure the adapter in a secure mode, you must perform additional steps. For example, enabling the Secure Socket Layer (SSL), creating and importing the certificate in the adapter registry, and so on. For more information, see "Configuring SSL authentication" on page 86.

Related concepts

Communication configuration
You must complete several tasks that configure the IBM Security Verify Governance Identity Manager server to communicate with the adapter.

Related tasks

Uploading the adapter package
You can upload the adapter package on z/OS.

Installing the ISPF dialog
Install the ISPF dialog to install and configure the Top Secret Adapter.

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

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

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

- Communication between the Identity server and the adapter
- `agentCfg` utility

Note: You can define _BPX_SHAREAS=YES in the /etc/profile. This setting enables the adapter to run in a single address space, instead of multiple address spaces. Newer releases of z/OS create two address spaces with this environment variable set. See "z/OS UNIX System Services considerations" on page 25 for more information.

Procedure

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

   ```
   START ITIAGNT
   ```

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

   - If the USS environment is running with _BPX_SHAREAS=YES, then run one of the following MVS stop command to stop the adapter:

     ```
     STOP ITIAGNT
     P ITIAGNT
     ```

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

     ```
     P ITIAGNT1
     ```

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

     ```
     CANCEL ITIAGNT
     ```

Related concepts

Communication configuration
You must complete several tasks that configure the IBM Security Verify Governance Identity Manager server to communicate with the adapter.

Related tasks

Uploading the adapter package
You can upload the adapter package on z/OS.

Installing the ISPF dialog
Install the ISPF dialog to install and configure the Top Secret Adapter.

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.

Communication configuration

You must complete several tasks that configure the IBM Security Verify Governance Identity Manager server to communicate with the adapter.

Related tasks

Uploading the adapter package
You can upload the adapter package on z/OS.

Installing the ISPF dialog
Install the ISPF dialog to install and configure the Top Secret Adapter.

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

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

Verifying that the adapter is working correctly

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

Importing the adapter profile

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

Before you begin

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

About this task

Target 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.

Profiles contained in this package

In the V7.1.15 and later installation package, the following profiles are included:

- IBM Security Verify Governance
- Governance Data Integration
- IBM Security Verify Governance Identity Manager

Installing the IBM Security Verify Governance Identity Manager specific version on an IBM Security Verify Governance Identity Manager server removes the requirement to install the Complex Attribute Handler. This can be of interest when you have defined policies on the IBM Security Verify Governance Identity Manager server that manage `ertopzprofile` related processing.

If no customization is done to the IBM Security Verify Governance Identity Manager server that involves the `ertopzprofile` attribute, the IBM Security Verify Governance profile can be used in combination with the Complex Attribute Handler on IBM Security Verify Governance Identity Manager servers.

For the Governance Data Integration profile the complex attribute handler is not required. It merely defines the Top Secret Profile object class as a Service Group for IBM Security Verify Governance compatibility. This profile can be used if Top Secret profile assignments are made from IBM Security Verify Governance.

To make changes in the Top Secret profile assignments in both IBM Security Verify Governance and IBM Security Verify Governance Identity Manager,modify the `resource.def` file that is included in the profile jar to define the `ertopzprofile` attribute as complex attribute and the following complex attribute handler properties.

```
<Property Name = "ercomplexattributes" Value = "ertopzprofile" />
<Property Name = "erattributehandler" Value =
"com.ibm.isim.util.complexattribute.TopSecretComplexAttributeHandler" />
```

Then include the complex attribute handler jar file in the `ITIM_LIB` shared library on ISVI/WAS server and with ISIGADI include it in the jars of SDI running ISIGADI. With ISIQ, the handler is already included in the ISIQ side code. Required additions to the <ProtocollProperties> section of the

`resource.def` when you are using ISIGADI and managing Top Secret profile assignments from both IBM Security Verify Governance Identity Manager and IBM Security Verify Governance.

Procedure

1. Log on to the Identity server 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 **ManageService Types** page, click **Import**.
   The **ImportService Type** page is displayed.
4. On the **Import Target Type** page, complete these steps:
   a) In the **Service Definition File** field, type the directory location of the *<Adapter>*Profile.jar or click **Browse** to locate the file.
   For example, if you are installing the SCIM Adapter for a Windows server that runs Active Directory, locate and import the `SCIMAdapterProfile.jar` file.
   b) Click **OK** to import the file.
   A message indicates that you successfully imported 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 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 is not displayed in a reasonable amount of time, 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. On the Appliance Dashboard, select **Manage System Settings** > **Maintenance** > **Log Retrieval and Configuration** > **Identity** > **trace log**, then click **View**.
- 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 Identity server*HOME*\data directory.

Attribute mapping

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

About this task

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

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

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

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

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

Note:

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.

- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

Procedure

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

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

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

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

5. Import the updated mapping definition file through the Target Administration module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance product documentation.

Creating an adapter service/target

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

Before you begin

Complete “Importing the adapter profile” on page 17.

About this task

You must create an administrative user account for the adapter on the managed resource. Provide the account information when you create a target. 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.

Use the target form to provide information for the target. The actual target form fields might vary depending on whether the service form is customized. The target name and description that you provide for each target are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. On the Appliance Dashboard, select Verify Governance Administration Console from the **Quick Links** widget.

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

   The Target Administration console is displayed.
3. From the navigation tree, click **Manage Targets**.

   The **Select a Target** page is displayed.
4. On the **Select a Target** page, click **Create**.

   The **Create a Target** wizard is displayed.
5. On the **Select the Type of Target** page, select a target type and click **Next**.

   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**.

6. On **General Information** page, specify the values for the target instance.

   The content of the **General Information** page depends on the type of target that you are creating. The creation of some targets might require more steps. It is specific to the profile (adapter). See the adapter's *Installation and Configuration Guide* for the more information.
7. On the **Users and Groups** page, which is displayed only for LDAP targets, complete the required fields.
8. On the **Authentication** page, which does not display for every target type, complete the required fields.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes and click **Next** or **OK**.

   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based targets.
10. On the **Status and Information** page, view information about the adapter and managed resource and click **Next** or **Finish**.

    The adapter must be running to obtain the information.
11. On the **Application Information** page, type a name and description for the application, and then click **Finish**.
12. Optional: Click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

    If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

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

Service/Target form details

Complete the service/target form fields.

On the General Information tab:

Service Name
Specify a name that identifies the Top Secret Adapter service on the 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 32.

Note: If you specify https as part of the URL, the adapter must be configured to use SSL authentication. If the adapter is not configured to use SSL authentication, specify http for the URL. For more information, see "Configuring SSL authentication" on page 86.

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

Password
Specify the password that was defined at installation time as the `Adapter authentication ID`. The default value is agent.

Top Secret ID under which requests will be processed
Optional: Specify a Top Secret ACID other than the one that is used by the adapter. This ACID can be a Control ACID with authority over a subset of ACIDs in the Top Secret database.

Owner
Optional: Specify the service owner, if any.

Service Prerequisite
Optional: Specify an existing service.

Verifying that the adapter is working correctly

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

Procedure

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

Related concepts

Communication configuration
You must complete several tasks that configure the IBM Security Verify Governance Identity Manager server to communicate with the adapter.

Related tasks

Uploading the adapter package
You can upload the adapter package on z/OS.

Installing the ISPF dialog
Install the ISPF dialog to install and configure the Top Secret Adapter.

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.

Chapter 5. Configuring

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

Configuring the adapter parameters

Use the adapter configuration tool, `agentCfg`, to view or modify the adapter parameters.

All the changes that you make to the parameters with the `agentCfg` take effect immediately. You can also use `agentCfg` to view or modify configuration settings from a remote workstation. For more information about specific procedures to use additional arguments, see Table 16 on page 73 in "Accessing help and additional options" on page 73.

Note: The screens displayed in this section are examples, the actual screens displayed might differ.

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

Configuration of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

Modifying an event notification context

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Configuration of Top Secret access

Determine your needs and configure how the adapter accesses Top Secret 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

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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings

Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Top Secret ACID

The adapter must run under a valid Top Secret Accessor ID (ACID), with access to the STC, TSO, OMVS, JES2, and BATCH facilities.

The ACID must have a valid UID and the group of this user must have a valid GID. Unless surrogate ACIDs are being used, the adapter must have the authority to change, create, delete, and list the required ACIDs. For example, for access to all ACIDs define a SCA type ACID with the required administrative authority. To perform reconciliation the ACID must have the data authority level set to ALL and PASSWORD. The adapter ACID must also be defined to the STC record.

Note: The adapter task must not run as a Master Security Control ACID (MSCA). Therefore, SCA ACIDs cannot be created by the Top Secret Adapter.

Example

These commands are an example of how to define the Top Secret Adapter to manage all accounts on this Top Secret database:

```
/* The ISIM Top Secret Adapter adapter requires an SCA user id, with */
/* OMVS attributes, and administrative authority.       */
TSS CREATE(ITIAGNT) NAME('ISIM TOP-SECRET ADAPTER')   +
   PASSWORD(password,0) FACILITY(STC,OPENMVS,APPC,BATCH) +
   TYPE(SCA)
TSS ADD(ITIAGNT) CONSOLE
TSS ADD(ITIAGNT) OMVSPGM('/bin/sh')
TSS ADD(ITIAGNT) HOME('/u/isim/catss/readwrite')
TSS ADD(ITIAGNT) UID(1010)
TSS ADD(ITIAGNT) DFLTGRP(OMVSGRP) GROUP(OMVSGRP)
TSS ADMIN(ITIAGNT) ACID(ALL)
TSS ADMIN(ITIAGNT) DATA(ALL,PASSWORD)
TSS ADMIN(ITIAGNT) MISC1(ALL)
TSS ADMIN(ITIAGNT) MISC2(ALL)
TSS ADMIN(ITIAGNT) MISC3(ALL)
TSS ADMIN(ITIAGNT) MISC4(ALL)
TSS ADMIN(ITIAGNT) MISC5(ALL)
TSS ADMIN(ITIAGNT) MISC7(ALL)
TSS ADMIN(ITIAGNT) MISC8(ALL)
TSS ADMIN(ITIAGNT) MISC9(ALL)
TSS ADMIN(ITIAGNT) FACILITY(ALL)
TSS LIST(ITIAGNT) DATA(ALL)
/* The adapter also requires a STARTED ID, with OMVS attributes */
TSS ADD(STC) PROCNAME(ITIAGNT) ACID(ITIAGNT)
/* Refresh the OMVS tables */
TSS MODIFY(OMVSTABS)
```

Note: The password option that is specified in this example is just to prevent unauthorized logon. Normally, the adapter runs as a started task. Use the parameter file option OPTIONS(4) to prevent operators to enter the password at the console.

Related concepts
Surrogate user

A surrogate user is a user who has the authority to perform tasks on behalf of another user, by using the other users level of authority. For the Top Secret Adapter, the adapter task ACID runs as a surrogate user on behalf of the ACID defined in the IBM Security Verify Governance server service form.

Surrogate user

A surrogate user is a user who has the authority to perform tasks on behalf of another user, by using the other users level of authority. For the Top Secret Adapter, the adapter task ACID runs as a surrogate user on behalf of the ACID defined in the IBM Security Verify Governance server service form.

The authorization of the adapter ACID as a surrogate user is necessary only if:

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

Note: If a single IBM Security Verify Governance service instance supports all the ACIDs in the Top Secret database, surrogate user authority is not needed.

For the adapter to perform requests on behalf of another user, you must permit authority for the SURROGAT resource.

If the adapter ACID is **ITIAGNT**, and the ACID defined on the IBM Security Verify Governance service form is **UNIT1**, then the following commands defines the SURROGAT resource.

```
TSS ADD(dept) SURROGAT(ATBALLC.)
TSS PERMIT(ITIAGNT) SURROGAT(ATBALLC.UNIT1) ACCESS(READ)
```

Related concepts

Top Secret ACID

The adapter must run under a valid Top Secret Accessor ID (ACID), with access to the STC, TSO, OMVS, JES2, and BATCH facilities.

Starting the adapter configuration tool

Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Procedure

1. Log on to the TSO on the z/OS operating system that hosts the adapter.
2. From ISPF option 6, run the following command and press **Enter** to enter the USS shell environment:

   ```
   omvs
   ```

   Optional: You can also enter the USS shell environment through a telnet session.
3. In the command prompt, change to the `/bin` subdirectory of the adapter in the `read/write` directory. If the adapter is installed in the default location for the `read/write` directory, run the following command.

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

   ```
   # cd /var/ibm/isim/bin
   ```
4. Run the following command:

   ```
   agentCfg -agent adapter_name
   ```

The adapter name was specified when you installed the adapter. You can find the names of the active adapters by running the `agentCfg` as:

```
agentCfg -list
```

5. At **Enter configuration key for Agent *adapter_name***, type the configuration key for the adapter.

   The default configuration key is agent. To prevent unauthorized access to the configuration of the adapter, you must modify the configuration key after the adapter installation completes. For more information, see "Changing protocol configuration settings" on page 32.

   The Agent Main Configuration Menu is displayed.

```
adapter_name 6.0 Agent Main Configuration Menu
-----------------------------------------
A. Configuration Settings.
B. Protocol Configuration.
C. Event Notification.
D. Change Configuration Key.
E. Activity Logging.
F. Registry Settings.
G. Advanced Settings.
H. Statistics.
I. Codepage Support.

X. Done

Select menu option:
```

   From the Agent Main Configuration Menu screen, you can configure the protocol, view statistics, and modify settings, including configuration, registry, and advanced settings.

Table 4. Options for the main configuration menu

Option	Configuration task	For more information
A	Viewing configuration settings	See "Viewing configuration settings" on page 30.
B	Changing protocol configuration settings	See "Changing protocol configuration settings" on page 32.
C	Configuring event notification	See "Configuring event notification" on page 36.
D	Changing the configuration key	See "Changing the configuration key" on page 59.
E	Changing activity logging settings	See "Changing activity logging settings" on page 60.
F	Changing registry settings	See "Modifying registry settings" on page 63.
G	Changing advanced settings	See "Changing advanced settings" on page 66.
H	Viewing statistics	See "Viewing statistics" on page 68.
I	Changing code page settings	See "Code page settings" on page 69.

Related concepts

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 of Top Secret access

Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Viewing configuration settings

You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

About this task

The following procedure describes how to view the adapter configuration settings:

Procedure

1. Access the **Agent Main configuration Menu**. See “Starting the adapter configuration tool” on page 28.
2. Type A to display the configuration settings for the adapter.

```
Configuration Settings
-----------------------------------------
Name            : adapter_name
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/isim/
isimcatss/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
```

3. Press any key to return to the **Main Menu**.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings

You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Changing protocol configuration settings

The adapter uses the DAML protocol to communicate with the Identity server.

About this task

By default, when the adapter is installed, the DAML protocol is configured for a nonsecure environment. To configure a secure environment, use Secure Shell Layer (SSL) and install a certificate. For more information, see “Installing the certificate” on page 94.

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

To configure the DAML protocol for the adapter, perform the following steps:

Procedure

1. Access the Agent Main Configuration Menu, if you have not already done so. See “Starting the adapter configuration tool” on page 28.
2. 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.
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
M. DISABLE_TLS11        TRUE ;Disable TLS 1.1 and earlier
N. DISABLE_TLS12        TRUE ;Disable TLS 1.2 and earlier

X. Done

Select menu option:
```

5. Follow these steps to change a protocol value:
   - Type the letter of the menu option for the protocol property to configure. Table 5 on page 33 describes each property.

- Take one of the following actions:
  - Change the property value and press **Enter** to display the Protocol Properties Menu with the new value.
  - If you do not want to change the value, press **Enter**.

Table 5. 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 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 Identity server uses this value to connect to the adapter.
C	Displays the following prompt: `Modify Property 'MAX_CONNECTIONS':` Enter the maximum number of concurrent open connections that the adapter supports. The default value is 100. **Note:** This setting is sufficient and does not require adjustment.
D	Displays the following prompt: `Modify Property 'PORTNUMBER':` Type a different port number. The Identity server uses the port number to connect to the adapter. The default port number is 45580. For more information, see “Adapter interactions with the Identity server” on page 4.
E	Displays the following prompt: `Modify Property 'USE_SSL':` TRUE specifies to use a secure SSL connection to connect the adapter. If you set USE_SSL to TRUE, you must install a certificate. For more information, see “Installing the certificate” on page 94. FALSE, the default value, specifies not to use a secure SSL connection.

Table 5. Options for the DAML protocol menu (continued)	
Option	**Configuration task**
F	Displays the following prompt: `Modify Property 'SRV_NODENAME':` Type a server name or an IP address of the workstation where you have installed the Identity server. This value is the DNS name or the IP address of the Identity server that is used for event notification and asynchronous request processing. **Note:** If your platform 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 Identity server. The adapter uses this port number to connect to the 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 the adapter must listen to. The default value is **ANY**.
I	Displays the following prompt: `Modify Property 'VALIDATE_CLIENT_CE':` Specify TRUE for the Identity server to send a certificate when it communicates with the adapter. When you set this option to TRUE, you must configure options D through I. Specify FALSE, the default value, to let the Identity server communicate with the adapter without a certificate. **Note:** • The property name is VALIDATE_CLIENT_CERT, however, 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 Identity server certificate. For more information about using the certTool, see “Starting certTool” on page 92.
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 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 86.

Table 5. Options for the DAML protocol menu (continued)	
Option	**Configuration task**
K	Displays the following prompt: `Modify Property 'READ_TIMEOUT':` Specify the timeout value in seconds. The default value is 0 which specifies that no read timeout is set. **Note: READ_TIMEOUT** prevents open threads in the adapter, which might cause "hang" problems. The open threads might be caused by firewall or network connection problems and might be seen as **TCP/IP ClosWait** connections that remain on the adapter. **Note:** If you encounter such problems, set the value of **READ_TIMEOUT** to a time longer than the Identity server timeout, but less than any firewall timeout. The 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.
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.
M	Displays the following prompt: `Modify Property 'DISABLE_TLS11':` Type FALSE to use the TLSv1.1 protocol to connect the adapter. The default value is TRUE.
N	Displays the following prompt: `Modify Property 'DISABLE_TLS12':` Type FALSE to use the TLSv1.2 protocol to connect the adapter. The default value is FALSE.

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

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings

You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Configuring event notification

Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

About this task

You can enable event notification to obtain the updated information from the managed resource.

Note: Event notification does not replace reconciliations on the 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 Verify Governance 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 Verify Governance 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 Verify Governance.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

"Required information" on page 37
To implement event notification, you must specify required information.

"Example definition" on page 38
This section provides an example definition.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Required information

To implement event notification, you must specify required information.

- Installing IBM Security Verify Governance Identity Manager digital certificate in the adapter's registry if you use communications between IBM Security Verify Governance Identity Manager and the adapter on the managed resource.
- Knowing the IP address for the IBM Security Verify Governance Identity Manager hosting platform.

- Knowing the IP port for the IBM Security Verify Governance Identity Manager hosting platform, which is either:
  - The SSL port, if you use SSL communications
  - The non-SSL port, if you do not use SSL

  These are the port numbers for the Web application server on IBM Security Verify Governance Identity Manager. The default WebSphere®, port numbers are 9443 (SSL) and 9080 (non-SSL).
- Knowing and defining the *pseudo-Distinguished Name* (DN) for the IBM Security Verify Governance Identity Manager service in an event notification context in the adapter's registry. The DN is not a typical LDAP DN and is unique for IBM Security Verify Governance Identity Manager. The DN identifies a specific service instance defined on the IBM Security Verify Governance Identity Manager server.
- Optionally, there are *credentials* passed to an adapter to identify the service instance to the managed resource adapter. For example, a Windows `Basepoint` that you specify on the adapter service form. The adapter connects to the managed resource by using these credentials.

Related concepts

Example definition
This section provides an example definition.

Assumptions for the example
This example makes several assumptions.

Protocol properties
You must set the protocol properties.

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

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

Related tasks

Installing the CA certificate in the adapter
You must install a CA certificate in the adapter to establish a secure communication between the adapter and IBM Security Verify Governance.

Adding an event notification context
Event Notification updates the Identity server at set intervals. It updates the server with the information that changed from the last server initiated reconciliation.

Example definition

This section provides an example definition.

It includes the following information:

- “Assumptions for the example” on page 39
- “Protocol properties” on page 40
- “Installing the CA certificate in the adapter” on page 42
- “Adding an event notification context” on page 45
- “Configuring the target DN for event notification contexts” on page 57
- “Attributes for search” on page 48
- “Pseudo-distinguished name values” on page 50

Related concepts

Required information
To implement event notification, you must specify required information.

Assumptions for the example

This example makes several assumptions.

Protocol properties
You must set the protocol properties.

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

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

Related tasks

Installing the CA certificate in the adapter
You must install a CA certificate in the adapter to establish a secure communication between the adapter and IBM Security Verify Governance.

Adding an event notification context
Event Notification updates the Identity server at set intervals. It updates the server with the information that changed from the last server initiated reconciliation.

Assumptions for the example

This example makes several assumptions.

- SSL for communication. Because SSL is used, the adapter receives a digital certificate from IBM Security Verify Governance. The certificate is self-signed and must be installed in the adapter registry as a Certificate Authority (CA) certificate.
- *9.38.214.54* as the host IP address where IBM Security Verify Governance runs.
- *9443* as the host IP port for the web application server SSL port.
- *Top Secret* as the name of the adapter context.
- A pseudo DN as a target notification event for the IBM Security Verify Governance services, which is `erservicename=MVS Top Secret 4.5.1016 ENTEST, o=Acme Inc, ou=Acme, dc=my_suffix`

Related concepts

Required information
To implement event notification, you must specify required information.

Example definition
This section provides an example definition.

Protocol properties
You must set the protocol properties.

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

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

Related tasks

Installing the CA certificate in the adapter
You must install a CA certificate in the adapter to establish a secure communication between the adapter and IBM Security Verify Governance.

Adding an event notification context

Event Notification updates the Identity server at set intervals. It updates the server with the information that changed from the last server initiated reconciliation.

Protocol properties

You must set the protocol properties.

SSL is often used. All the properties are defined under the DAML protocol environment.

In the following examples, the IBM Security Verify Governance host IP and port addresses are set through the **agentCfg** utility.

```
        ISIMAGNT 6.0.1000 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.  Hostaddr
        I.  Statistics.
        J.  Codepage Support.

        X.  Done
```

```
Select menu option:b

        Agent Protocol Configuration Menu
        ---------------------------------
        Available Protocols : DAML
        Configured Protocols: DAML

        A.  Add Protocol.
        B.  Remove Protocol.
        C.  Configure Protocol.

        X.  Done

        Select menu option:c
        Configure Protocol Menu
        -----------------------------

        A.  DAML
        X.  Done
```

```
Select menu option:a

        DAML Protocol Properties
        -----------------------------------

        A.  USERNAME            ******      ;Authorized user name.
        B.  PASSWORD            ******      ;Authorized user password.
        C.  MAX_CONNECTIONS     100         ;Max Connections.
        D.  PORTNUMBER          45581       ;Protocol Server port number.
        E.  USE_SSL             TRUE        ;Use SSL secure connection
        F.  SRV_NODENAME        -----       ;Event Notif. Server name.
        G.  SRV_PORTNUMBER      7003        ;Event Notif. Server port number.
        H.  HOSTADDR            ANY         ;Listen on address (or "ANY")
        I.  VALIDATE_CLIENT_CE  FALSE       ;Require client certificate.
        J.  REQUIRE_CERT_REG    FALSE       ;Require registered certificate.

        X.  Done
```

```
Select menu option:f

        Modify Property 'SRV_NODENAME': 9.38.215.20

        DAML Protocol Properties
        -----------------------------------

        A.  USERNAME            ******      ;Authorized user name.
        B.  PASSWORD            ******      ;Authorized user password.
        C.  MAX_CONNECTIONS     100         ;Max Connections.
        D.  PORTNUMBER          45581       ;Protocol Server port number.
        E.  USE_SSL             TRUE        ;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.

        X.  Done
```

```
        Select menu option:g

        Modify Property 'SRV_PORTNUMBER': 9443

        DAML Protocol Properties
        -----------------------------------

        A.  USERNAME            ******      ;Authorized user name.
        B.  PASSWORD            ******      ;Authorized user password.
        C.  MAX_CONNECTIONS     100         ;Max Connections.
        D.  PORTNUMBER          45581       ;Protocol Server port number.
        E.  USE_SSL             TRUE        ;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.

        X.  Done

        Select menu option:x

        Configure Protocol Menu
        ------------------------------

        A.  DAML
        X.  Done

        Select menu option:x
```

Related concepts

Required information
To implement event notification, you must specify required information.

Example definition
This section provides an example definition.

Assumptions for the example
This example makes several assumptions.

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

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

Related tasks

Installing the CA certificate in the adapter
You must install a CA certificate in the adapter to establish a secure communication between the adapter and IBM Security Verify Governance.

Adding an event notification context

Event Notification updates the Identity server at set intervals. It updates the server with the information that changed from the last server initiated reconciliation.

Installing the CA certificate in the adapter

You must install a CA certificate in the adapter to establish a secure communication between the adapter and IBM Security Verify Governance.

About this task

To establish a secure communication, you must install:

- A private and a corresponding digital certificate for the adapter.
- A Certificate Authority (CA) certificate that signed the adapter certificate for the Identity server.

When event notification is employed, the adapter side must contact the Identity server. In this case, the Identity server identifies itself to the adapter. Because of this action, you must install the Certificate Authority digital certificate (which signed the Identity server digital certificate) in the adapter registry.

When you configure and install event notification, install the Identity server CA certificate in the adapter environment. If the server is using a self-signed digital certificate, then the server certificate acts as a CA certificate. In this case, only the server digital certificate is required.

The server self-signed certificate or CA signing certificate must be obtained in an exported X.509 DER form and transferred to the adapter host. It must be stored in the read/write `/data` directory for subsequent installation by using the **certTool** utility (provided with the adapter). The binary file transfer of the certificate to the adapter platform is necessary because the certificate is in the DER form. There are different methods to obtain and transfer the certificate to the adapter host.

The following steps are valid ONLY for obtaining a self-signed certificate from a webserver:

Procedure

1. Open a Web browser, for example, Internet Explorer.
2. Use HTTPS (HTP over SSL) to connect to Identity server platform.

   The following URL is an example:

   ```
   https://9.38.215.20:9443/enrole/login
   ```

3. Press **Enter**, and a dialog box is displayed, indicating a *security alert*.

   This alert is because the certificate presented by the site to your web browser is not issued by a company you have chosen to trust.
4. Click **View Certificate**.
5. On the Details tab, click **Copy to File** and click **Next**.
6. On the Export File Format page, select the **DER encoded X.509 (.CER)** option as the format of the certificate and click **Next**.
7. On the **File to Export** page, specify a directory and name on your local workstation to store the certificate. Click **Next**.

   A completion dialog indicates the success of the export wizard. Note of the full path of the **File Name** in this display.
8. Click **OK** to close the **Success** dialog box.
9. Click **OK** to close the **Certificate** dialog box.

   The **Security alert** dialog box is displayed.
10. Click either:

    - **Yes** to connect to the Identity server.
    - **No** to deny the connection.

The choice is irrelevant, because you have already captured the certificate to your workstation.

11. Use the FTP utility to transfer the exported certificate to the host where the adapter resides.

    The following example shows an FTP session, transferring the certificate to the adapter host:

```
C:\temp>dir *.cer
 Volume in drive C is Local Disk
 Volume Serial Number is 289F-D3F5

 Directory of C:\temp

10/26/2004  04:37p                742 rhea.cer
               1 File(s)            742 bytes
               0 Dir(s)   3,924,729,856 bytes free

C:\temp>ftp 9.38.214.54
Connected to 9.38.214.54.
220-FTPD1 IBM FTP CS V1R4 at AGENTHOST.IBM.COM, 00:59:19 on 2004-10-30.
220 Connection will close if idle for more than 5 minutes.
User (9.38.214.54:(none)): agntusr
331 Send password please.
Password:
230 JOHNY is logged on.  Working directory is "JOHNY.".
ftp> cd /u/itim/data
250 HFS directory /u/itim/data is the current working directory
ftp> bin
200 Representation type is Image
ftp> put rhea.cer
200 Port request OK.
125 Storing data set /u/itim/data/rhea.cer
250 Transfer completed successfully.
ftp: 742 bytes sent in 0.02Seconds 37.10Kbytes/sec.
ftp> quit
221 Quit command received. Goodbye.

C:\temp>exit
```

12. Connect to the adapter host so that you can run the certTool utility and install the certificate that you have just uploaded.

    The following example is a sample terminal session on the adapter host to do the installation:

```
/u/itim/readwrite/data:>ls -al
total 10328
drwxrwxr-x 2 AGNTUSR SYS1 8192  Oct 29 14:22 .
drwxrwxr-x 6 AGNTUSR SYS1 8192  Oct 7 16:44 ..
-rw-rw-r-- 1 AGNTUSR SYS1 888   Oct 15 17:12 DamlCACerts.pem
-rwx------ 1 AGNTUSR SYS1 7173  Oct 29 14:09 CATSSAgentT.dat
-rw------- 1 AGNTUSR SYS1 1581  Oct 7 16:45 damlserver.pfx
-rw-r----- 1 AGNTUSR SYS1 1970  Oct 20 18:00 damlsrvr2.pfx
-rw-r----- 1 AGNTUSR SYS1 729   Oct 29 17:59 rhea.cer
-rw------- 1 AGNTUSR SYS1 5242908 Oct 29 14:21 rhea_local.dat
/u/itim/readwrite/data:>../bin/certTool

 IBM Security Agent DAML Protocol Certificate Tool 6.00
 ------------------------------------------------------

  Main menu - Configuring agent: CATSSAgent
  -----------------------------

  A. Generate private key and certificate request
  B. Install certificate from file
  C. Install certificate and key from PKCS12 file
  D. View current installed certificate

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

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

  K. Export certificate and key to PKCS12 file

  X. Quit

 Choice: f

 Enter name of certificate file: rhea.cer

Subject: /C=US/O=IBM/OU=SWG/CN=jserver

Install this CA (Y/N)? y

  Main menu - Configuring agent: CATSSAgent
  -----------------------------

  A. Generate private key and certificate request
  B. Install certificate from file
  C. Install certificate and key from PKCS12 file
  D. View current installed certificate

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

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

  K. Export certificate and key to PKCS12 file

  X. Quit

 Choice: x
```

Results

The self-signed digital certificate for the Identity server is now installed in the managed host adapter, as a CA certificate. You can use the event notification process to connect to IBM Security Verify Governance through SSL.

Related concepts

Required information
To implement event notification, you must specify required information.

Example definition

This section provides an example definition.

Assumptions for the example
This example makes several assumptions.

Protocol properties
You must set the protocol properties.

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

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

Related tasks

Adding an event notification context
Event Notification updates the Identity server at set intervals. It updates the server with the information that changed from the last server initiated reconciliation.

Adding an event notification context

Event Notification updates the Identity server at set intervals. It updates the server with the information that changed from the last server initiated reconciliation.

About this task

The following screen describes all the options that are displayed when you enable Event Notification. If you disable Event Notification, none of the options are displayed. To set Event Notification for the Identity server, perform the following steps:

1. Access the **Agent Main Configuration Menu**. See "Starting the adapter configuration tool" on page 28.
2. At the Agent Main Configuration Menu, type C to display Event Notification Menu.

```
Event Notification Menu
-----------------------------------
* Reconciliation interval   : 1 day(s)
* Next Reconciliation time  : 23 hour(s) 41 min(s). 37 sec(s).
* Last processing time      : 53 sec(s).
* Configured Contexts       : RHEA

A.  Enabled
B.  Time interval between reconciliations.
C.  Set processing cache size.(currently: 50 Mbytes)
D.  Start event notification now.
E.  Set attributes to be reconciled.
F.  Add Event Notification Context.
G.  Modify Event Notification Context.
H.  Remove Event Notification Context.
I.  List Event Notification Contexts.
J.  Set password attribute names.

X.  Done

Select menu option:
```

3. At the **Agent Main Configuration Menu**, type the letter of the menu option that you want to change.

   Note:

   - Enable option A for the values of the other options to take effect. Each time 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 6. Options for the event notification menu

Option	Configuration task
A	If you select this option, the adapter updates the Identity server with changes to the adapter at regular intervals. When the option is set to: • Disabled, pressing the A key changes to enabled • Enabled, pressing the A key changes to disabled Type A to toggle between the options.

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]`
	Note: 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.

C	Displays the following prompt: `Enter new cache size[5]:` Type a different value to change the processing cache size.
D	If you select this option, event notification starts.
E	Displays the **Event Notification Entry Types Menu**: For more information, see “Setting attributes for reconciliation” on page 53.
F	Displays the following prompt: `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 54.
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}`
	`----------`

Table 6. Options for the event notification menu (continued)	
Option	**Configuration task**
J	When you select the Set password attribute names option, you can set the names of the attributes that are sensitive, for example, erpassword. In this case, the state database does not store these attribute values. The local database for event notification stores the changes from IBM Security Verify Governance and the subsequent event notification does not retrieve the sensitive attributes. The event notification does not send the changes as events if the reconciliation operation does not retrieve the sensitive attributes.

4. To add an event notification context, select option F to add a context. You are prompted for a context name, then returned to the **Event Notification Menu**.

```
Select menu option:F


Enter new context name: CATSSAgent


Event Notification Menu
---------------------------------------
* Reconciliation interval   : 1 day(s)
* Next Reconciliation time  : 22 hour(s) 24 min(s). 52 sec(s).
* Configured Contexts       : Top Secret


A.  Enabled
B.  Time interval between reconciliations.
C.  Set processing cache size.(currently: 50 Mbytes)
D.  Start event notification now.
E.  Set attributes to be reconciled.
F.  Add Event Notification Context.
G.  Modify Event Notification Context.
H.  Remove Event Notification Context.
I.  List Event Notification Contexts.
J.  Set password attribute names.

X.  Done

Select menu option:
```

5. 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.

Results

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

Related concepts

Required information
To implement event notification, you must specify required information.

Example definition
This section provides an example definition.

Assumptions for the example
This example makes several assumptions.

Protocol properties
You must set the protocol properties.

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

Pseudo-distinguished name values

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

Related tasks

Installing the CA certificate in the adapter
You must install a CA certificate in the adapter to establish a secure communication between the adapter and IBM Security Verify Governance.

Attributes for search

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:

- Multiple service instances on the Identity server can reference the adapter. Each service instance must have permissions to specify an attribute-value pair so that the adapter knows which service instance is requesting work.
- The attribute is sent to the event notification process when the event notification interval occurred or is manually initiated. When the attribute is received, the adapter processes information that the attribute/value pair indicates.
- When you initiate a server-initiated reconciliation process is initiated, the adapter replaces the local database that represents this service instance.

Table 7 on page 48 describes a partial list of possible attribute/value pairs that you can specify for **Set attributes for search**.

Table 7. Attributes for search

Service type	Form label	Attribute name	Value
CATSSProfile	Top Secret ID under which requests are processed	ertopzrequester	A Top Secret Control ACID that manages users in this service.

```
Select menu option:g

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

A.  Top Secret

X.  Done

Select menu option:a

Modify Context: Top Secret
-----------------------------------

A.  Set attributes for search
B.  Target DN:

Select menu option:a

Reconciliation Attributes Passed to Agent for context: Top Secret
-------------------------------------------------

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

X.  Done

Select menu option:a

Attribute name : ertopzrequester

Attribute value: admnbu1

Reconciliation Attributes Passed to Agent for context: Top Secret
-------------------------------------------------
01. ertopzrequester                   'admnbu1'
-------------------------------------------------

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

X.  Done

Select menu option:x
```

Related concepts

Required information
To implement event notification, you must specify required information.

Example definition
This section provides an example definition.

Assumptions for the example
This example makes several assumptions.

Protocol properties
You must set the protocol properties.

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

Related tasks

Installing the CA certificate in the adapter
You must install a CA certificate in the adapter to establish a secure communication between the adapter and IBM Security Verify Governance.

Adding an event notification context

Event Notification updates the Identity server at set intervals. It updates the server with the information that changed from the last server initiated reconciliation.

Pseudo-distinguished name values

The 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 8. 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 are in a reverse sequence of their appearance in the IBM Security Verify Governance organization chart.
C	o	The value of the **o** attribute of an organization to which the service belongs, at the highest level. This might be determined by examining the IBM Security Verify Governance organization chart.
D	ou	The **ou** component is established at IBM Security Verify Governance installation. You can find this component in the IBM Security Verify Governance configuration file named `enRole.properties`, on configuration item named **enrole.defaulttenant.id=**
E	dc	The **dc** component is established at IBM Security Verify Governance installation. This is the root suffix of the LDAP environment. You can find this component in the IBM Security Verify Governance configuration file named `enRole.properties`, on configuration item named **enrole.ldapserver.root=**

Example 1:

A:

The service name on the Identity server is **MVS Top Secret 4.5.1016 ENTEST**. This name becomes the component **A** of the pseudo-DN:

```
erservicename=MVS Top Secret 4.5.1016 ENTEST
```

B:

Table 9 on page 50 describes an example of the IBM Security Verify Governance organization chart that indicates the location of the service in the organization.

Table 9. Organization chart example

+ Identity Manager Home	IBM Security Verify Governance 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 Verify Governance organization chart is named Acme Inc. The service becomes component **C** of the pseudo-DN:

```
o=Acme Inc
```

D:

Through examination or prior knowledge of the contents of the **enRole.properties** definition file on the Identity server, the value of the property named **enrole.defaulttenant.id=** 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:

Through examination or prior knowledge of the contents of the **enRole.properties** definition file on the Identity server, the value of the property named **enrole.ldapserver.root=** 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 Top Secret 4.5.1016 ENTEST,o=Acme Inc,ou=Acme,dc=my_suffix
```

Example 2:

A:

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

```
erservicename=Irvine Sales
```

B:

Table 10 on page 51 describes an example of the IBM Security Verify Governance organization chart that indicates the location of the service in the organization.

Table 10. Organization chart example

+ Identity Manager Home	IBM Security Verify Governance 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 Verify Governance organization chart is named Acme Inc. This becomes the component **C** of the pseudo-DN:

```
o=Acme Inc
```

D:

Through examination or prior knowledge of the contents of the **enRole.properties** definition file on the Identity server, the value of the property named **enrole.defaulttenant.id=** 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:

Through examination or prior knowledge of the contents of the **enRole.properties** definition file on the Identity server, the value of the property named **enrole.ldapserver.root=** 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

Required information
To implement event notification, you must specify required information.

Example definition
This section provides an example definition.

Assumptions for the example
This example makes several assumptions.

Protocol properties
You must set the protocol properties.

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

Related tasks

Installing the CA certificate in the adapter
You must install a CA certificate in the adapter to establish a secure communication between the adapter and IBM Security Verify Governance.

Adding an event notification context

Event Notification updates the Identity server at set intervals. It updates the server with the information that changed from the last server initiated reconciliation.

Setting attributes for reconciliation

You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

About this task

Note: You cannot see the event notification entry types and attributes until you perform the first reconciliation with event notification as Enabled.

Procedure

1. Access the Agent Main Configuration Menu, if you have not already done so. See “Starting the adapter configuration tool” on page 28.
2. Type **E** (Set attributes for reconciliation) to display the Event Notification Entry Types menu.

```
Select menu option:e

Event Notification Entry Types
--------------------------------------
A.  ERTOPZACCOUNTS
B.  ERTOPZPROFILES
C.  ERTOPZGROUPS
D.  ERTOPZDEPARTMENTS
E.  ERTOPZDIVISIONS
F.  ERTOPZZONES

X.  Done

Select menu option:
```

3. Do one of the following to display the Event Notification Attribute Listing for the selected reconciliation type.

```
Select menu option:a

Event Notification Attribute Listing
 ---------------------------------------------------------------------
{A} ** ERACCOUNTSTATUS  {B} ** ERTOPZACIDAUTH     {C} ** ERTOPZADMINLISTDATA
{D} ** ERTOPZASSIZE     {E} ** ERTOPZASUSPEND     {F} ** ERTOPZAUDIT
{G} ** ERTOPZCONSOLE    {H} ** ERTOPZCREATEDDATE  {I} ** ERTOPZDEPARTMTACID
{J} ** ERTOPZDFLTGRP    {K} ** ERTOPZDFLTSLBL     {L} ** ERTOPZDIVISIONACID
{M} ** ERTOPZDUFUPD     {O} ** ERTOPZDUFXTR       {Q} ** ERTOPZEXPIRATIONDATE
{R} ** ERTOPZFACILITY   {S} ** ERTOPZGROUP        {T} ** ERTOPZIMSMSC
                  (p)rev         Page 1 of 7           (n)ext
 ---------------------------------------------------------------------
 X. Done

 Select menu option:
```

4. To exclude an attribute from an event notification, type the letter beside the attribute you want to exclude.

   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 concepts

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 spaces, instead of multiple address spaces.

Configuration of Top Secret access

Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Modifying an event notification context

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

About this task

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

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

Procedure

1. Access the **Agent Main Configuration Menu**. See “Starting the adapter configuration tool” on page 28.
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:
C. Delete Baseline Database
X. Done
Select menu option:
```

*Table 11. Options for the **Modify Context Menu***

Option	Configuration task	For more information
A	Adding search attributes for event notification	See "Adding search attributes for event notification" on page 56.
B	Configuring the target DN for event notification contexts	See "Configuring the target DN for event notification contexts" on page 57.
C	Removing the baseline database for event notification contexts	See "Removing the baseline database for event notification contexts" on page 58.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation

You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Adding search attributes for event notification

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

About this task

These attribute/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 specified for that context are passed to the adapter.
- When the Identity server initiates a reconciliation process, the adapter replaces the local database that represents this service with the new database.

To add search attributes, perform the following steps:

Procedure

1. Access the Agent Main Configuration Menu, if you have not already done so. See “Starting the adapter configuration tool” on page 28.
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:
```

3. Type the letter of the menu option that you want to change.

The supported attribute names are displayed with two asterisks (**) in front of each name. Attributes without asterisks are not updated during an event notification. The Reconciliation Attributes Passed to Agent Menu is displayed with the changes displayed.

Related tasks

Configuring the target DN for event notification contexts
During event notification configuration, the adapter sends requests to a service running on the Identity server.

Removing the baseline database for event notification contexts
You can remove the baseline database for event notification contexts only after you create a context and perform a reconciliation operation 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 running on the Identity server.

About this task

Therefore, you must configure target DN for event notification contexts for the adapter to know which service the adapter must send the request to. Configuring the target DN for event notification contexts involves specifying parameters, such as the adapter service name, organization (o), organization name (ou), and other parameters.

To configure the target DN, perform the following steps:

Procedure

1. Access the Agent Main Configuration Menu, if you have not already done so. .
   See "Starting the adapter configuration tool" on page 28
2. Type the option for Event Notification to display the Event Notification Menu.
3. Type the option for Modify Event Notification Context, then enter the option of the context that you want to modify.
4. At the Modify Context menu for the context, type B to display the following prompt:

   ```
   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 12 on page 57 describes each DN element.

Table 12. 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 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 Identity server installation.

6. After you define the new target DN, the software displays the Modify Context menu. After you add the event notification context, you can modify it with option **G** to add information to the context. You must specify a target *pseudo* DN.

   To construct a target DN, see "Pseudo-distinguished name values" on page 50.

```
        Select menu option: G

        Modify Context: Top Secret
        ----------------------------------

        A.  Set attributes for search
        B.  Target DN:

        X.  Done

        Select menu option:b

        Enter Target DN: erservicename=MVS Top Secret 4.5.1016 ENTEST,o=Acme Inc,
ou=Acme,dc=my_suffix

        Modify Context: Top Secret
        ----------------------------------

        A.  Set attributes for search
        B.  Target DN:  erservicename=MVS Top Secret 4.5.1016 ENTEST,o=Acme Inc,
ou=Acme,dc=my_suffix

        X.  Done

        Select menu option:
```

Related tasks

Adding search attributes for event notification
For some adapters, you might need to specify an attribute/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 and perform a reconciliation operation 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 and perform a reconciliation operation on the context to create a Baseline Database file.

About this task

To remove the baseline database for event notification contexts, perform the following steps:

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 confirming that you want to remove a context, press **Enter** to remove the baseline database for event notification contexts.

Related tasks

Adding search attributes for event notification
For some adapters, you might need to specify an attribute/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 running on the Identity server.

Changing the configuration key

You use the configuration key as a password to access the configuration tool for the adapter.

About this task

To change the Top Secret Adapter configuration key, perform the following steps:

Procedure

1. Access the Agent Main Configuration Menu, if you have not already done so. See "Starting the adapter configuration tool" on page 28.
2. At the Main Menu prompt, type D.
3. Do on of the following:
   - Change the value of the configuration key and press **Enter**.
   - Press **Enter** to return to the Main Configuration Menu without changing the configuration key.

Results

The default configuration key is **agent**. Ensure that your password is complex. The following message is displayed:

```
Configuration key successfully changed.
```

The configuration program returns to the Main Menu prompt.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation

You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Changing activity logging settings

Use this task to enable or disable log files that monitor various system activities.

About this task

When you enable activity logging settings, IBM Security Verify Governance maintains a log file (`CATSSAgent.log`) of all transactions. By default, the log file is in the read/write `\log` directory.

To change the Top Secret Adapter activity logging settings,

Procedure

1. Access the Agent Main Configuration Menu, if you have not already done so.
   See "Starting the adapter configuration tool" on page 28.
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/isimcatss/log).
C. Activity Log File Name (current: CATSSAgent.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. Perform one of the following steps:
   - 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 13 on page 61 describes each option.
   - Press **Enter** to return to the Agent Activity Logging Menu without changing the value.

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

Table 13. 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. When the option is set to: • Disabled, pressing the A key changes to enabled • Enabled, pressing the A key changes to disabled Type A to toggle between the options.
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. When the option is set to: • Disabled, pressing the F key changes the value to enabled • Enabled, pressing the F key changes the value to disabled Type F to toggle between the options.

Table 13. Options for the activity logging menu (continued)	
Option	**Configuration task**
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. When the option is set to: • Disabled, pressing the G key changes the value to enabled • Enabled, pressing the G key changes the value to disabled Type G to toggle between the options.
H	If this option is set to enabled, the adapter maintains a log file of all transactions in the Agent Development Kit (ADK) and library files. Base logging substantially increases the size of the logs. When the option is set to: • Disabled, pressing the H key changes the value to enabled • Enabled, pressing the H key changes the value to disabled Type H to toggle between the options.
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. When the option is set to: • Disabled, pressing the I key changes the value to enabled • Enabled, pressing the I key changes the value to disabled Type I to toggle between the options.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification

Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Modifying registry settings

Use this procedure to change the adapter registry settings.

Procedure

1. At the Main Menu, type F.
   The Registry Menu is displayed.
2. Select menu option.

```
adapter_name 5.1 Agent Registry Menu
-----------------------------------------
A. Modify Non-encrypted registry settings.
B. Modify encrypted registry settings.
C. Multi-instance settings.
X. Done
Select menu option:
```

What to do next

For a list of valid registry options, their values, and meanings, see “ Registry settings” on page 130.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings

You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Modifying non-encrypted registry settings

You can modify non-encrypted registry settings.

Procedure

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

```
Agent Registry Items
------------------------------------------------
01. DSEXEC                    'IBMUSER.EXEC'
02. DSJOB                     'IBMUSER.CNTL'
03. ENROLE_VERSION                '4.0'
04. LOKUSAVE                  'IBMUSER.LOKUSAVE'
05. PASSEXPIRE                'TRUE'
06. PHRASEEXPIRE              'TRUE'
07. PROFDIG                   '3'
08. RACFRC                    '120'
09. RACINPUT                  'TRUE'
10. RECOSAVE                  'IBMUSER.RECOSAVE'
------------------------------------------------
```

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

Table 14. 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 and press **Enter**.

Results

The non-encrypted registry settings menu reappears and displays your new settings.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics

You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Changing advanced settings

You might need to change advanced settings.

About this task

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

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

These thread counts determines the maximum number of requests that the adapter processes. To change these settings, perform the following steps:

Procedure

1. Access the Agent Main Configuration Menu, if you have not already done so. See "Starting the adapter configuration tool" on page 28.
2. At the Main Menu prompt, type G to display the Advanced Settings Menu.

   The following screen displays the default thread count settings.

```
CATSSAgent 5.1 Advanced Settings Menu
-----------------------------------------
A. Single Thread Agent (current:FALSE)
B. ADD max. thread count. (current:3)
C. MODIFY max. thread count. (current:3)
D. DELETE max. thread count. (current:3)
E. SEARCH max. thread count. (current:3)
F. Allow User EXEC procedures (current:FALSE)
G. Archive Request Packets (current:FALSE)
H. UTF8 Conversion support (current:TRUE)
I. Pass search filter to agent (current:FALSE)

X. Done
Select menu option:
```

Table 15. Options for the advanced settings menu

Option	Description
A	Forces the adapter to submit only one request at a time. The default value is **FALSE**.
B	Limits the number of Add requests that can run simultaneously. The default value is **3**.
C	Limits the number of Modify requests that can run simultaneously. The default value is **3**.
D	Limits the number of Delete requests that can run simultaneously. The default value is **3**.

Table 15. Options for the advanced settings menu (continued)	
Option	**Description**
E	Limits the number of Search requests that can run simultaneously. The default value is **3**.
F	Determines if 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.
J	Sets the thread priority level for the adapter. The default value is **4**.

3. Type the letter of the menu option that you want to change. For a description of each option, see Table 15 on page 66.
4. Change the value and press **Enter** to display the Advanced Settings Menu with new settings.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings

Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Viewing statistics

You can view an event log for the adapter.

Procedure

1. Access the Agent Main Configuration Menu, if you have not already done so.
   See "Starting the adapter configuration tool" on page 28.
2. At the Main Menu prompt, type H to display the activity history for the adapter.

```
CATSSAgent 5.1 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

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation

You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Code page settings

You must complete several tasks to change code page settings.

Related concepts

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 of Top Secret access
Determine your needs and configure how the adapter accesses Top Secret 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

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings

Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for the adapter.

Accessing help and additional options
To access the agentCfg help menu and use the help arguments, perform the following steps:

Default adapter code page locale

The default code page setting for ASCII based adapters is **US-ASCII**.

For EBCDIC hosts, such as MVS, the default code page is **IBM-1047-s390**.

Related concepts

Obtaining of a list of valid code pages
To obtain a list of valid code page locale names, run the `agentCfg`.

Related tasks

Setting the code page
You can change the code page settings for the adapter.

Obtaining of a list of valid code pages

To obtain a list of valid code page locale names, run the `agentCfg`.

For example:

```
agentCfg -ag adaptername -codepages
```

Ensure that the adapter is running and you have specified the configuration key to display a list of valid code page names that are available for the adapter. The following list of valid code pages is a partial session with the `agentCfg`.

```
IBMUSER:/home/itim/CATSSAgent/readwrite/bin: >agentCfg -ag CATSSAgent -codepages

Enter configuration key for Agent 'CATSSAgent':

List of codepage supported by ICU :

UTF-8
UTF-16
UTF-16BE
UTF-16LE
UTF-32
UTF-32BE
UTF-32LE
UTF16_PlatformEndian
UTF16_OppositeEndian
UTF32_PlatformEndian
UTF32_OppositeEndian
ISO-8859-1
US-ASCII
.
.
.
ibm-37_P100-1995,swaplfnl
ibm-1047_P100-1995,swaplfnl
ibm-1140_P100-1997,swaplfnl
ibm-1142_P100-1997,swaplfnl
ibm-1143_P100-1997,swaplfnl
ibm-1144_P100-1997,swaplfnl
ibm-1145_P100-1997,swaplfnl
ibm-1146_P100-1997,swaplfnl
ibm-1147_P100-1997,swaplfnl
ibm-1148_P100-1997,swaplfnl
ibm-1149_P100-1997,swaplfnl
ibm-1153_P100-1999,swaplfnl
ibm-12712_P100-1998,swaplfnl
ibm-16804_X110-1999,swaplfnl
ebcdic-xml-us
```

Related concepts

Default adapter code page locale
The default code page setting for ASCII based adapters is **US-ASCII**.

Related tasks

Setting the code page
You can change the code page settings for the adapter.

Setting the code page

You can change the code page settings for the adapter.

Procedure

1. At the Main Menu prompt, type `I`.

   The Code Page Support Menu for the adapter is displayed.

```
CATSSAgent 5.1 Codepage Support Menu
-----------------------------------------
* Configured codepage: IBM-1047-s390
-----------------------------------------
*
*****************************************
* Restart Agent After Configuring Codepages
*****************************************

A.  Codepage Configure.

X.  Done

Select menu option:
```

2. Type A to configure a code page.

Note: The CATSSAgent uses unicode; therefore, this option is not applicable.

3. Type X to return to the Main Configuration Menu.
4. After you select a code page, restart the adapter.

Example

The following example is a sample session with the `agentCfg`, altering the default code page, from *US EBCDIC (IBM-1047)* to *Spanish EBCDIC (IBM-1145)*.

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

Enter configuration key for Agent 'CATSSAgent':

        CATSSAgent 4.6 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

        CATSSAgent 4.5.1017 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

        CATSSAgent 4.5.1017 Codepage Support Menu
        -----------------------------------------
        * Configured codepage: ibm-1145
        -----------------------------------------
        *
        *****************************************
        * Restart Agent After Configuring Codepages
        *****************************************

        A.  Codepage Configure.

        X.  Done

        Select menu option:x
```

Related concepts

Default adapter code page locale

The default code page setting for ASCII based adapters is **US-ASCII**.

Obtaining of a list of valid code pages

To obtain a list of valid code page locale names, run the `agentCfg`.

Accessing help and additional options

To access the agentCfg help menu and use the help arguments, perform the following steps:

Procedure

1. At the Main Menu prompt, type X to display the USS command prompt.
2. Type `agentCfg -help` at the prompt to display the help menu and list of commands.

```
-version               ;Show version
-hostname <value>    ;Target nodename to connect to (Default:Local host
IP address)
-findall               ;Find all agents on target node
-list                  ;List available agents on target node
-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 16. Arguments and description for the agentCfg help menu

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

Table 16. Arguments and description for the agentCfg help menu (continued)	
Argument	**Description**
-agent <value>	Use this argument to specify the adapter that you want to configure. Enter the adapter name as the value. Use this argument with the -hostname argument to modify the configuration setting from a remote host. You can also use this argument with the -tail argument.
-tail	Use this argument with the -agent argument to display the activity log for an adapter. Add the -hostname argument to display the log file for an adapter on a different host.
-portnumber <value>	Use this argument with the -agent argument to specify the port number that is used for connections for the agentCfg tool.
-netsearch <value>	Use this argument with the -findall argument to display all active adapters on the z/OS operating system. You must specify a subnet address as the value.
-codepages	Use this argument to display a list of available 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, and the node on which the adapter is installed. The default node for the Identity server must be 44970. The output is similar to the following example:

```
Agent(s) installed on node '127.0.0.1'
----------------------
adapter_name    (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'
-----------------
adapter_name        (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

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 of Top Secret access

Determine your needs and configure how the adapter accesses Top Secret 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.

Code page settings
You must complete several tasks to change code page settings.

Related tasks

Starting the adapter configuration tool
Start the adapter configuration tool, agentCfg, for Top Secret Adapter parameters.

Viewing configuration settings
You might want to view the adapter configuration settings for information about the adapter version, ADK version, adapter log file name, and other information.

Changing protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Configuring event notification
Event notification detects changes that are made directly on the managed resource and updates the Identity server with the changes.

Setting attributes for reconciliation
You can set attributes for reconciliation when the values change for attributes that trigger event notifications. You also can remove attributes that change frequently, such as password age or last successful logon.

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

Changing the configuration key
You use the configuration key as a password to access the configuration tool for the adapter.

Changing activity logging settings
Use this task to enable or disable log files that monitor various system activities.

Modifying registry settings
Use this procedure to change the adapter registry settings.

Modifying non-encrypted registry settings
You can modify non-encrypted registry settings.

Changing advanced settings
You might need to change advanced settings.

Viewing statistics
You can view an event log for 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.

ISIMEXIT

The REXX exec ISIMEXIT gets called in response to add, modify and delete requests received from the Identity server.

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

Before add processing
The request to add a user is received, however, not yet processed.

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

Before modify processing
The request to modify a user is received, however, not yet processed.

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

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

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

You may program ISIMEXIT to indicate success (zero return code) or failure (non-zero return code). For the before add processing, before modify, and before delete exits, any non-zero return code will stop processing and return a failure to Identity server for that request, and the add, modify or delete request will not be processed. For the after add processing, after modify, and after delete exits, a non-zero return code will return a warning to the Identity server.

ISIMEXIT gets control in a TSO batch environment, running in the APPC/MVS environment. Processing is performed under the authority of the same Top Secret ACID that runs the Top Secret commands. You might call other programs, perform file Input/Output (I/O), or run valid TSO commands (if it does not prompt for a terminal user for input), as necessary.

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 after add processing or at after modify exit time.
- Defining a user data set profile after add processing or at after modify exit time.
- Defining a user OMVS (UNIX System Services) home directory after add processing or at after modify exit time.
- Deleting a user data set profiles at before delete exit time.
- Deleting a user catalog alias at after delete exit time.

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

The listed information is available to the EXIT.

Table 17. 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 Top Secret user object that is processed.	Always
3	Prepost Qualifies whether this is before or after processing entry to the exit.	BEFORE or AFTER	Always
4	User ID	The Top Secret ACID that is processed.	Always

Table 17. ISIMEXIT processing information (continued)			
Parameter #	**Meaning**	**Possible value**	**Availability**
5	Organizational type The Top Secret ACID type	The value of the attribute ertopztype	Only at before add processing or after add processing exit. Not available for delete or modify processing.
6	Organization The Top Secret ACID zone/division/department, dependent on the organizational type.	The value of the attribute ertopzzoneacid, ertopzdivisionacid, or ertopzdepartmtacid, depending on the type.	Only at before add processing or after add processing exit. Not available for delete or modify processing.
7	Name	The value of the attribute ertopzname.	Only add before and after
8	Using	The value of the attribute ertopzusing.	Only add before and after

Related concepts

Comments with the Top Secret command string
You might want to send a comment with the Top Secret command strings for auditing purposes.

Related tasks

Supporting user-defined ACID fields with extended attributes
You can customize the Top Secret Adapter to support user-defined ACID fields by mapping each user-defined ACID field to an extended attribute.

Additional REXX exit parameters

You can make additional information (attributes) available to ISIMEXIT using the multi-value attribute ertopzexitstring.

This attribute provides a way of telling the adapter to make specific attributes available to ISIMEXIT. Only attribute values that are sent with the current request are available to ISIMEXIT.

Note: This is only available for add and modify requests. On delete requests only the userid (ACID) is available to the adapter.

Making additional parameters available to ISIMEXIT

You can set the parameters in ertopzexitstring using the account form, or the attribute list could be set in ertopzexitstring using a provisioning policy or a workflow.

About this task

Take these steps to set the parameters in the account form:

Note: The attribute ertopzexitstring is defined as SendOnly. The attribute names set in ertopzexitstring are case insensitive.

Procedure

1. Customize the account form to include a multiple-value list box of all the attributes you may wish to make available to ISIMEXIT.

   See “Customizing the account form with fields for ISIMEXIT” on page 79.

2. Type the appropriate information required to add or modify the Top Secret account into the ITIM account form.
3. Select the attributes you want available to ISIMEXIT for this call from the ertopzexitstring multiple-value list box. The attributes you select should have values already set in the account form from the previous step.
4. Submit the add or modify request.

   After receiving the call, the Top Secret Adapter will build a string of attribute names and values, as described in "Process of the exit string with ISIMEXIT" on page 78.

Process of the exit string with ISIMEXIT

The Top Secret Adapter receives the request from the Identity server and reads the attribute list set in ertopzexitstring.

If attributes are listed, the adapter attempts to find the corresponding values for those attributes sent with that request. Attributes with no value available are ignored by the adapter, and a message is written to the adapter log. You must code the ISIMEXIT to manage the case where an expected attribute is not available. A string of the following format is then built: UES=*ertopzattr1=value1,ertopzattr2=value2,…,ertopzattrN=valueN*

For example:

```
UES=ertopzname="IBM user",ertopzUID=123
```

This string will be made available as a parameter to ISIMEXIT for both before and after processing.

For an ADD request, ertopzexitstring is the eighth or ninth parameter available to ISIMEXIT, depending on whether the optional parameter USING is present.

- If USING is not present, ertopzexitstring is the eighth parameter, if USING is present, ertopzexitstring is the ninth parameter.
- The parameter USING is always in this format:

  ```
  USING(ertopzusing)
  ```

For a MODIFY request:

- ertopzexitstring is the fifth parameter available to ISIMEXIT.
- Only the values that are being modified are available. For example, if you are adding the ACID authority CREATE to a user ACID that already has INFO and REPORT authorities, then the string available to ISIMEXIT is `ertopzacidauth=CREATE`

The attribute values within the string follow these rules:

- If the value contains a space, a comma, or a single quotation mark, then the value is enclosed in single quotation marks. If the value contains a single quotation mark, the quotation mark is replaced with two single quotation marks. For example: `ertopzname='Administrator''s ACID'`
- If the attribute is Boolean, the value is either TRUE or FALSE.
- Multi-valued attributes are enclosed in parentheses and separated by commas. For example: `ertopzacidauth=(CREATE, INFO, MAINTAIN)`

For example, a request for a new CA Top Secret account might have these values:

- User ID: USER1
- CA-TSS ACID Type: USER
- CA-TSS ACID Full Name: Top Secret User
- ACID's Department ACID: DEPT1
- Home Directory: `/u/user`
- ACID's Default Group: OMVS

Suppose that you select the following for “Attributes available to adapter user exit” on the account form:

```
ertopzomvshome
ertopzdfltgrp
```

The ISIMEXIT receives the following parameters for the pre-processing exit:

```
ADD USER BEFORE USER1 USER DEPT1 “Top Secret User”
UES=ertopzomvshome=/u/user,ertopzdfltgrp=OMVS
```

Customizing the account form with fields for ISIMEXIT

You can customize the account form by adding a multiple-value list box for attributes that you want to make available to ISIMEXIT.

About this task

To add a multiple-value list box to the account form, take these steps:

Procedure

1. Copy the `CATSSProfile.jar` file to a temporary directory and extract the files.
   See “Copying the CATSSProfile.jar file and extract the files” on page 83.
2. Edit the `erTopzACCOUNTS.xml` file.
   There is an example in comments for the multiple-value list box ertopzexitstring on a new tab “Non CA-TSS attributes”. You may remove the comment delimiters, and add new options as required. For example:

```
<tab index="12" selected="false">
<title><![CDATA[$tab.tss.13]]></title>
<image/>
<url>javascript:switchTabs(document.forms['body'],12);</url>
<formElement direction="inherit" name="data.ertopzexitstring"
label="$ertopzexitstring">
<select style="width:200px" name="data.ertopzexitstring" width="200">
<option value=" erTopzOMVSHOME">erTopzOMVSHOME</option>
<option value=" erTopzOMVSPGM">erTopzOMVSPGM</option>
<option value=" erTopzUID">erTopzUID</option>
<option value=" erTopzGRP">erTopzGRP</option>
.
.
(other lines omitted)
.
</select>
</formElement>
</tab>
```

3. Create a new JAR file and install the new account form on the Identity server.
   For more information, see “Creating a JAR file and installing the new attributes” on page 84.

Supporting user-defined ACID fields with extended attributes

You can customize the Top Secret Adapter to support user-defined ACID fields by mapping each user-defined ACID field to an extended attribute.

About this task

Complete these steps to customize the Top Secret Adapter to support the user-defined fields in the Top Secret Field Descriptor Table (FDT):

Procedure

1. Define the user-defined ACID fields and extended attributes mappings to the Top Secret Adapter . Use the Top Secret Adapter ISPF dialog to perform this step.
2. Copy the JAR file to a temporary directory and extract the files.
3. Update the schema.dsml file on the Identity server.
4. Update the customlabels.properties file on the Identity server.
5. Install the new attributes on the Identity server.
6. Modify the form for the account on the Identity server.

Related concepts

ISIMEXIT
The REXX exec ISIMEXIT gets called in response to add, modify and delete requests received from the Identity server.

Comments with the Top Secret command string
You might want to send a comment with the Top Secret command strings for auditing purposes.

Mapping the user-defined ACID fields to the extended attributes by using the ISPF dialog

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

Before you begin

This dialog requires a model 3 or model 4 3270 display. You also must have an authority level of MISC8(LISTRDT).

About this task

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

Note: When a new extended attribute is added, the Top Secret Adapter does not need to be restarted.

Complete these steps to create the adapter file that maps the Top Secret user-defined ACID fields to the extended attributes.

Procedure

1. Log on to TSO on the z/OS operating system.
2. From ISPF 6 option, run the following command to start the ISPF dialog:

   ```
   EXEC ‘hlq.SAGTCENU(AGTCCFG)'
   ```

   The License page is displayed.
3. Press **Enter** to display this screen.

   Note: The screens displayed in these tasks are examples; the actual screens displayed might differ.

```
------------------- ISIM CA-TopSecret Adapter Customization -----------
Option ===>                                          Location:  1

IBM Security Verify
Governance CA-Top Secret Adapter

  Initial Customization

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

    2  Customize to support user-defined ACID fields
       If you have user-defined fields in the FDT, 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.

4. Select **Customize to support user-defined ACID fields**.

   An authority level of MISC8(LISTRDT) is required.

```
------------------- ISIM CA-TopSecret Adapter Customization ------
Option ===>

  user-defined ACID fields

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

   USS Adapter read/write home
    ===>
   Top Secret Default Group ACID for adapter  ===>

 S Field Name Max len Attribute name                  Comments
 - ---------- ------- -------------------------------  --------------------
   JOBTYPE    1       ERTOPZJOBTYPE
   PHONE      20      ERTOPZPHONE
   $LOCKID    20      ERTOPZ$LOCKID
   $DESKNO    20      ERTOPZ$DESKNO
```

This panel lists all fields defined in the Top Secret FDT that have the attribute USER. The panel shows:

- The maximum value length allowed as defined in the FDT.
- A generated attribute name based on the field name.

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

Top Secret Default Group ACID for adapter
: This parameter must be the default group ACID for the adapter as specified in the **Adapter specific parameters** panel during installation. It is used to give the adapter read access to the UDF.dat file.

  Tip: You can load previously saved parameters from the initial installation by selecting **Initial Customization** on the first panel, then **Load Default or Saved Variables**.

Attribute name
: Attribute names are required for selected fields. The attribute names are modifiable. The attribute names must be unique, and must not contain the characters '$', '*' or '-'. If the attribute names contain any of those characters, the adapter profile cannot be imported correctly. The generated

default attribute names might need to be modified to remove any disallowed characters. The maximum length for an attribute name is 31 characters.

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

```
------------------- ISIM Top Secret Adapter Customization ------
Option ===>

  user-defined ACID fields

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

   USS Adapter read/write home
    ===> /var/ibm/isimcatss
   Top Secret Adapter Default Group ACID for adapter  ===> STCUSS

 S Field Name Max len Attribute name                   Comments
 - ---------- ------- -------------------------------  --------------------
 S JOBTYPE    1       ERTOPZJOBTYPE                    Defined in UDF.dat
 S PHONE      20      ERTOPZPHONE                      Defined in UDF.dat
   $LOCKID    20      ERTOPZ$LOCKID
   $DESKNO    20      ERTOPZ$DESKNO
```

You might see the following in the comments column:

Invalid attribute name
: You selected a field and the attribute name contains invalid characters. The attribute name must be corrected before it can be saved.

Length discrepancy
: The maximum length for the user-defined ACID field that is saved in the UDF.dat does not match the maximum length for that field in the FDT. This error might occur if the FDT is updated after the UDF.dat file was created. The maximum length value displayed is the value from the FDT. If the UDF.dat file is saved, the FDT value is the value that is saved. If you change the length of one or more fields in the FDT, optionally, save the UDF.dat file to avoid this error.

Defined in UDF.dat
: Indicates that the user-defined field is in the current UDF.dat file in the specified read/write home directory.

5. Type S in the selection column to select any additional user-defined ACID fields you want to support.

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

   The UDF.dat file is saved with read and write permissions for the administrator and read permission for the group ACID for the adapter specified.

   Note: The administrator is the user who is selecting and saving the user-defined ACID fields to be supported.

Results

The extended attributes are now defined to the Top Secret Adapter. The following steps describe how to update and import the Top Secret Adapter profile. Importing the profile makes the new attribute definitions available to the Identity server.

Copying the CATSSProfile.jar file and extract the files

The profile JAR file, `CATSSProfile.jar`, is included in the Top Secret Adapter compressed file that you downloaded from the IBM website.

About this task

The `CATSSProfile.jar` file contains the following files:

- `CustomLabels.properties`
- `erTopzACCOUNTS.xml`
- `erTopzSERVICE.xml`
- `resource.def`
- `schema.dsml`

You can modify these files to customize your environment. When you finish updating the profile JAR file, rebuild the jar and import it in to the Identity server. To modify the `CATSSProfile.jar` file, complete the following steps:

Procedure

1. Copy the `CATSSProfile.jar` file to a temporary Windows folder.
2. From the command prompt, extract the contents of the `CATSSProfile.jar` file into the temporary directory by running the following command:

   ```
   jar xvf CATSSProfile.jar
   ```

   The **`jar`** command creates the directory `CATSSProfile`.
3. Change the directory to the `CATSSProfile` subdirectory. For example, run the following command:

   ```
   cd CATSSProfile
   ```
4. Edit the appropriate files.

Updating the schema.dsml file

The Top Secret Adapter `schema.dsml` file identifies all of the standard Top Secret account attributes. Modify this file to identify the new extended attributes.

About this task

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

Procedure

1. Change to the `\CATSSProfile` directory, where the `schema.dsml` file is created.
2. Edit the `schema.dsml` file to add an attribute definition for each extended attributes.

   The attribute name must match the attribute name registered with ISPF dialog. All attributes must be unique, and assigned a unique Object Identifier (OID). The instance ID for the extended attributes starts from 1000, so the OID for the first extended attribute is:

   ```
   <object-identifier>1.3.6.1.4.1.6054.3.155.1.1000</object-identifier>
   ```

   This numbering prevents duplicate OIDs if the adapter is upgraded to support new attributes. For subsequent extended attributes, the OID is incremented by 1, based on the last entry in the file. For example, if the last attribute in the file uses the OID 1.3.6.1.4.1.6054.3.155.1.1008, the next new

attribute uses the OID 1.3.6.1.4.1.6054.3.155.1.1009. The data type is always a directory string and is defined using the syntax tags:

```
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
```

3. Add each of the new attributes to the account class.

   For example, add the following attribute definition under the erTopzACCOUNTS section of the schema.dsml file:

```
<attribute ref="erTopzphone" required="false"/>
<!-- ******************************************************** -->
<!-- erTopzPHONE                                              -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
<name>erTopzPHONE</name>
<description>Phone Number</description>
<object-identifier>1.3.6.1.4.1.6054.3.155.1.1000</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erTopzACCOUNTS Class                                     -->
<!-- ******************************************************** -->
         :
        :
<attribute ref = "erTopzPHONE" required = "false" />
```

Modifying the CustomLabels.properties file

After you add the extended attributes to the `schema.dsml` file, the attributes are available for use on the Top Secret Adapter form.

About this task

You can modify the attribute names that are in the attribute list. To add the attribute and its corresponding label to the `CustomLabels.properties` file, complete the following steps:

Procedure

1. Change to the `\CATSSProfile` directory, where the `CustomLabels.properties` file is created.
2. Edit the `CustomLabels.properties` file to add the attribute and its corresponding label using the following format:

```
attribute=label
```

   Note: The attribute name must be in lowercase.

   For example:

```
#
# CATSS Adapter Labels definitions
#
ertopzphone=Phone number
ertopzemail=eMail
```

Creating a JAR file and installing the new attributes

After you modify the files, you must import these files, and any other files in the profile that were modified for the adapter. The files must be imported into the IBM Security Verify Governance for the changes to take effect.

About this task

To install the new attributes, create a JAR file containing the updated files in the temporary windows director:

Procedure

1. Navigate to the parent directory of CATSSProfile, then run the following **jar** command:

```
cd ..
jar cvf CATSSProfile.jar CATSSProfile
```

2. Import the CATSSProfile.jar file into the Identity server.

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

Optional modification of the adapter form

After the changes are available in the Identity server, you can modify the Top Secret Adapter forms to use the new extended attributes.

For example:

```
<formElement direction="inherit" name="data.ertopzphone" label="$ertopzphone">
<input maxlength="40" name="data.ertopzphone" type="text" size="40"/>
       <constraint>
          <type>MAX_LENGTH</type><parameter>40</parameter>
          </constraint>
</formElement>
```

The attributes do not need to be added to the Top Secret form unless you want them to be available. The attributes are returned during reconciliations unless you explicitly exclude them.

Comments with the Top Secret command string

You might want to send a comment with the Top Secret command strings for auditing purposes.

For example:

```
TSS CREATE(USER1) TYPE(USER) DEPT(DEPT1) PASSWORD(xxxx) NAME(IBM user) /*
Request number 12345 */
```

You can use the attribute ertopzcomment to define a Top Secret command comment. For the above example, you would define:

```
ertopzcomment=Request number 12345
```

ertopzcomment is a send only attribute and is only available with add and modify requests. ertopzcomment is of type string and with a maximum length of 80. If more than 80 characters are defined, the string is truncated to 80 characters. The characters '*/' are not allowed. If the characters '*/' are specified in the comment string, the add or modify request might fail.

Note: ertopzcomment is not available on the release version of the account form erTopzACCOUNTS.xml. There is an example, in comments, of the ertopzcomment attribute displayed on a new tab **Non CA-TSS attributes**. You can edit erTopzACCOUNTS.xml, remove the comment delimiters, re-create a new profile JAR file, and import the new profile as required.

Related concepts

ISIMEXIT

The REXX exec ISIMEXIT gets called in response to add, modify and delete requests received from the Identity server.

Related tasks

Supporting user-defined ACID fields with extended attributes

You can customize the Top Secret Adapter to support user-defined ACID fields by mapping each user-defined ACID field to an extended attribute.

Configuring SSL authentication

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

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

The 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 Identity server can verify the identity of the adapter before the server establishes a secure connection.

For example, adapter events can notify the 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 Identity server.

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

Overview of SSL and digital certificates

An enterprise network deployment requires secure communication between the 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 Verify 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.

SSL authentication

When you start the adapter, it loads the available connection protocols. The DAML protocol is the only available protocol that supports the z/OS adapters.

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

The DAML SSL implementation offers SSL protocol specific configuration options such as disabling specific SSL protocols as described in “Changing protocol configuration settings” on page 32 and it offers the option to specify the cipher suites it will allow for SSL communication. The adapters cipher suite is configured in the adapter start script and by default defined as `ISIM_ADAPTER_CIPHER_LIST = HIGH`. You can modify the value for the `ISIM_ADAPTER_CIPHER_LIST` environment variable to meet your organizations requirements.

For more information about the, see https://www.openssl.org/docs/man1.0.2/man1/ciphers.html.

Configuring certificates for SSL authentication

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

About this task

Use the certTool utility for these tasks:

Configuring certificates for one-way SSL authentication

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

About this task

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

In Figure 2 on page 89, Application A operates as the Identity server, and Application B operates as the IBM Security Verify Adapter.

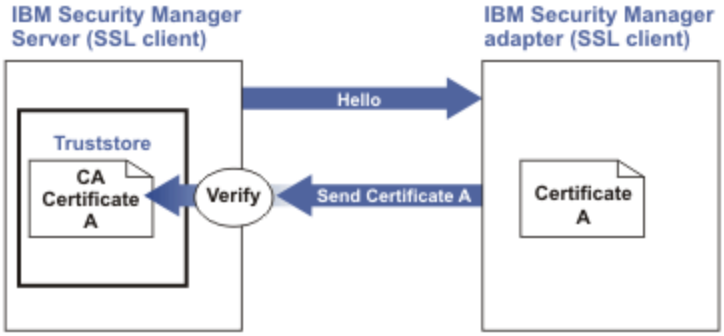


Figure 2. One-way SSL authentication (server authentication)

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.
      i) 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.
      ii) 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 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 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 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 Identity server.

Related tasks

“Starting certTool” on page 92

To start the certificate configuration tool, certTool, for the adapter, complete these steps:

Configuring certificates for two-way SSL authentication

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

Before you begin

Configure the adapter and the 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 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 90, the Identity server operates as Application A and the IBM Security Verify Adapter operates as Application B.

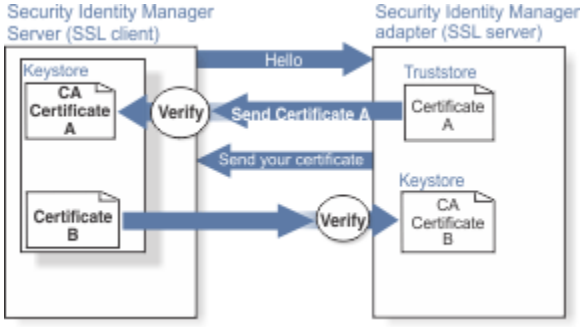


Figure 3. Two-way SSL authentication (client authentication)

Procedure

1. On the 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 Identity server to the adapter.

Results

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

Related tasks

"Configuring certificates for one-way SSL authentication" on page 89

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

Configuring certificates when the adapter operates as an SSL client

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

About this task

This configuration applies if the adapter initiates a connection to the web server, which is used by the 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 91 describes how the adapter operates as an SSL server and as an SSL client. When the adapter communicates with the 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.

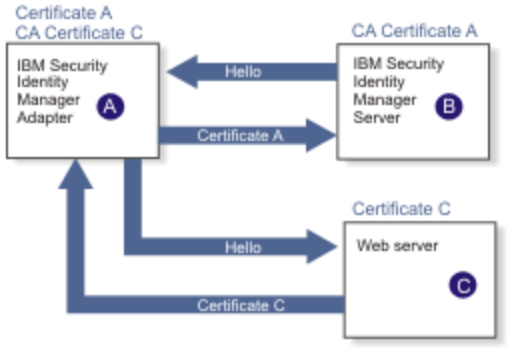


Figure 4. Adapter operating as an SSL server and an SSL client

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 Identity server.

Managing SSL certificates with the certTool utility

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

About this task

This section includes instructions for performing the following tasks:

Starting certTool

To start the certificate configuration tool, certTool, for the adapter, complete these steps:

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. Browse to the Windows Command Prompt.
2. Log on to the adapter
3. In the command prompt, change to the `<adapter_readwrite_home>/bin` directory of the adapter.
4. 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:
```

5. 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 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 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 Verify Governance.

About this task

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

A CSR file looks similar to the following example:

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

Procedure

1. At the **Main menu** of the certTool utility, type A. 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.

Example of certificate signing request

Your 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-----
```

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

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

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

Results

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

Viewing the installed certificate

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

Procedure

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

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

Installing a CA certificate

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

About this task

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

Procedure

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

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

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

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

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

Results

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

Viewing CA certificates

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

About this task

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

Procedure

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

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

Deleting a CA certificate

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

Procedure

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

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

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

Results

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 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**.

Using the Regis Tool

Start the Regis tool to modify the different adapter parameters.

Procedure

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

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

   The following options are available for the Regis tool:

```
-version                    ;show regis version
        -registry       < value >   ;Registry File
        -encryptkey     < value >   ;Encryption key for string data
        -setstring      < value >   ;Set Registry String, [key::value]
        -getstring      < value >   ;Get Registry String
        -create                     ;Create Registry (Default:registry)
        -list           < value >   ;List Registry Contents (Default:registry)
        -delete         < value >   ;Delete Registry key
        -script                     ;Produce output for scripting
        -protocol       < value >   ;Protocol (Default:DAML)
        -installpath    < value >   ;Set agent's install path
        -property       < value >   ;Property name for protocol
        -value          < value >   ;Argument value
        -logdir         < value >   ;Agent's logfile directory
        -logfile        < value >   ;Agent's logfile name
        -mainproperty   < value >   ;Set main property
```

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

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

Regis Command Examples

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

Modifying DAML protocol properties

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

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

Modifying non-encrypted registry settings

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

Modifying main properties

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

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

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

Configuring required attributes in IBM Security Verify Governance

Follow the procedure below to configure the required attributes for IBM Security Verify Governance.

Procedure

1. In **Access Governance Core, Manage, Accounts**, select the account for the Top Secret adapter.
2. Select **Target Attributes, Actions, Discover Account attributes from Target**.
3. Select the following attributes that are required for creating a new Top Secret account:
   - At least one of these attributes: ZONE, DIVISION, and DEPARTMENT
   - TYPE attribute
   - NAME attribute

Configuration notes

The 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.

Modifying Zone, Division and Department

You can change the values for Zone, Division, and Department when you modify an account. The adapter executes a MOVE command each time a value is changed. Changing multiple values in one single request results in multiple MOVE commands, one for each value:

```
MOVE ACID(USER) ZONE(ZONEA)
MOVE ACID(USER) DIVISION(USFAC)
MOVE ACID(USER) DEPT(HR)
```

Note:

- The ACID TYPE is not appended to these commands.
- The value changes are processed in random order.

As such, it is possible to specify non-compatible values such as request to move an ACID to a DIVISION and a DEPARTMENT, which does not belong to this DIVISION. The ACID type might also change because of the execution of the MOVE command. For more information on the changes in ACID types, when performing a MOVE for an ACID without a specified TYPE, see the *CA Top Secret product documentation*.

The Identity server updates the account for which the change request is executed. The update is based on the returned result for each individual value change. It does not report any changes in the ACID that resulted from the MOVE command.

To ensure that the Identity server reflects the actual current ACID definitions, perform a reconciliation for the changed account directly after you change a ZONE, DIVISION, or DEPARTMENT.

A reconciliation for a single account is interpreted as an Account Lookup request and results with the collection of data for the specified ACID. To request a Lookup, specify a search filter for the reconciliation. The filter must be specified as a reconciliation query for a single **eruid** value.

To perform a reconciliation for a single account that is named JOHND, use the following query:

```
Reconcile accounts that match this filter:
(eruid=JOHND)
```

The Lookup request initiates a lookup-specific TSSCFILE transaction to collect the data for the ACID specified in the search filter. It returns the updated account data to the Identity server.

Note: The actual values that are retrieved with the Lookup request depend on the administrative scope of the ACID used to perform the request (ADAPTERID or SURROGAT). For more information on the data each ACID type can list within its administrative scope, see the *CA Top Secret product documentation*.

The ACID lookup transaction has the following requirements:

1. The presence of the DSEXEC setting and hlq.EXEC value in the adapter registry. This value is automatically written to the registry file during adapter installation.
2. The presence of a new template member in the hlq.EXEC dataset: TSSLOKU. This member is automatically created during adapter installation.
3. Permissions that allow the transaction to create, update and delete the LSAVE and intermediate data set.

Password phrases

Top Secret for z/OS Adapter 6.0.8 and above support Top Secret password phrases. A password phrase in Top Secret is an authentication mechanism that allows the secret string to be 9 - 100 characters. While setting passwords from the Identity server, a string less than or equal to eight characters is treated as a password and a string more than eight characters is treated as a pass phrase.

Passwords are considered to be invalid when containing any of the following characters: ,) ({ } ' " and space

Password phrases are considered to be invalid when containing any of the following characters: ,) ({ } ' "

If the adapter encounters any of the above invalid characters it will return an error to the Identity server.

On account Add:

When you are requesting a new account on the Identity server, the adapter interprets any password string that is shorter than 8 characters as a password and proceeds to create the requested account with a password. A password string longer than 8 characters is interpreted as a password phrase.
In this scenario, the adapter by default, generates a random password by using a standard, built-in,

configuration string. If the account is requested with the PHRASEONLY attribute set to TRUE, a password is not generated, regardless of the PASSGEN setting.

This standard configuration string is: CnccSCNS

The password generator will use this configuration string to generate a random password as defined in the following table:

Table 18. Configuration strings for the password generator

Character	**Description**
C	Random uppercase character (no vowels)
c	Random lowercase character (no vowels)
v	Random lowercase vowel (a,e,i,o,u, and y)
V	Random uppercase vowel (A,E,I,O,U, and Y)
N	Random numeric
s	Random special character
Any other character	Use as is provided (for instance: national characters)

Internally the adapter will ensure it will not generate the same characters consecutively.

The built-in string can be modified by using new registry setting: PWD_CONFIG

PWD_CONFIG will allow a maximum of 5 comma-separated strings which will be randomly selected by the adapter to generate random passwords.

The size of each string should be between 4 and 8 characters long. If a shorter string is specified the adapter will report an error and try another string. If a longer string is specified the adapter will use only the first 8 characters to generate a password.

The configuration string is not allowed to contain any of the following hardcoded reserved words: APPL APR ASDF AUG BASIC CADAM DEC DEMO FEB FOCUS GAME IBM JAN JUL JUN LOG MAR MAY NET NEW NOV OCT PASS ROS SEP SIGN SYS TEST TSO VALID VTAM XXX 1234.

Or any of the following characters: ,) ({ } ' "

If a reserved word is found in the configuration string the adapter will report an error. After receiving an error that the adapter will attempt to select another random configuration string. After two failed attempts the adapter will stop processing and return an error. The adapter will consider the first four characters of the logonid for the request it is processing as a reserved word. In other words: the adapter will also report an error if the first four 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/or short logonid as part of the generated password the adapter will stop processing and return an error.

A new registry setting allows specifying more reserved words: RESWORD.

Any comma-separated string that is found in the RESWORD registry setting value will be added to the hardcoded reserved words list during request processing.

For more information on adding and changing registry settings, see “Modifying registry settings” on page 63.

On account Modify:

Password Phrases can be changed/added during a Modify request for an existing account. When adding an initial password phrase to an existing account don't forget to ensure the user is allowed to use

password phrases by setting password phrase to TRUE in the account form when requesting a new user with a password phrase on the Identity server. When changing and/or adding a password phrase for an existing account it will by default expire. Password phrase (also referred to as passphrase) expiration can be controlled by using a new registry setting: PHRASEEXPIRE

This setting is provided in the adapter installation menu as shown in the screen and can be changed by using the agentCfg tool.

PHRASEEXPIRE supports 2 values: TRUE and FALSE.

- When set to TRUE pass phrases are expired.
- When set to FALSE pass phrases are not expired.

```
------------------- ISIM CA-TopSecret Adapter Customization -------------------
Option                                          ===>
Adapter specific parameters
Name of adapter instance                        ===> ISIAGNT
Name of Started Task JCL procedure name         ===> ISIAGNT
IP Communications Port Number                   ===> 45598
Note: The adapter will always require access to ports 44970 through 44994.
These ports are implicitly reserved.
Adapter authentication ID (internal)            ===> agent
Adapter authentication password (internal)      ===> agent
PDU backlog limit                               ===> 1000
Do you want passwords set as expired?           ===> TRUE     (True, False)
Do you want passphrases set as expired?         ===> TRUE  (True, False)
Do you use SYS1.BRODCAST in the environment?    ===> TRUE     (True, False)
CA-Top Secret SCA ACID for ISIM adapter         ===> ISIAGNT
Password for the ITIM adapter ACID              ===>
CA-Top Secret Default Group ACID for adapter    ===> OMVSGRP
OMVS UID to be assigned to ACID (non-zero)      ===> 45598
```

For more information on adding and changing registry settings, see “Modifying registry settings” on page 63.

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.

This topic provides information and techniques for identifying and resolving problems related to the Top Secret Adapter.

Note: If a problem is encountered, enable all levels of activity logging (debug, detail, base, and thread). The adapter log contains the main source of troubleshooting information. See "Changing activity logging settings" on page 60.

Table 19. 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 15.
	The adapter returned an error status for a bind request. Status code: invalid credentials Adapter error message: `Authentication Failed`	Check the adapter authentication ID and password match the installed values. See the screen for Adapter-specific parameters in the task"Running the ISPF dialog" on page 8.
	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 86. The adapter log contains details about the certificates loaded during initialization.
catssAdd: Invalid TYPE type for creation of user *userid*.		This error occurs when a User add request is submitted, however, the value for the erTopzTYPE attribute is incorrect. The valid values for the erTopzTYPE attribute are: • ZCA • VCA • DCA • USER
catssAdd: User *userid* add Successful. Some attributes could not be modified.		This warning occurs when a user is created, however, some additional attributes failed. See the adapter log file for more information.

Table 19. Error messages, warnings, and corrective actions (continued)		
Error message or warning	**Additional warnings, messages, or information**	**Corrective action**
catssAdd: Missing ZONE, DIVISION, or DEPARTMENT for user *userid*, Type *type*.		For a particular type of user, the corresponding ZONE, DIVISION, or DEPARTMENT is missing. See the adapter log file for more information.
catssAdd: Missing PASSWORD for account *userid*.		Ensure that you specify a password during a user add request.
catssAdd: Missing NAME for user *userid*.		Ensure that you specify a name for the user during a user add request.
catssAdd: Missing TYPE for user *userid*.		Ensure that you specify a type for the user during a user add request.
APPC error in UserDel.		This error occurs when the adapter cannot establish an APPC transaction. The request is failed. See the MVS system log and the adapter log for more information.
catssModify: Some attributes unsuccessful.		This warning occurs when a user is modified, however, some additional attributes failed. See the adapter log file for more information.
catssModify: All attributes unsuccessful.		The modify request failed to set the attributes on the managed resource. See the adapter log file for more information.
catssSearch: Reconciliation did not return at least 1 ACID.		During the reconciliation request, no ACIDs were returned. See the MVS system log and the adapter log for more information.
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 Top Secret `logonid`.

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.

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

Related tasks

Installing test fixes and diagnostic builds
IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

Related reference

Frequently asked questions

Logs

When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

The log files are kept in the UNIX System Services file system, under the installation path of the adapter, in the read/write `log` subdirectory.

The adapter log name is the adapter instance name, followed by an extension of `.log`. When the extension is `.log`, it is the current log file. Old log files have a different extension such as `.log_001`,`.log_002`, `.log_003` and so on.

Table 20. Example of Adapter log details	
Details	**Example values**
Installation path	`/usr/isim`
Adapter log name	`CATSSAgent`
Log location	`/usr/itim/log/`
Log files	• `CATSSAgent.log` • `CATSSAgent.log_001` • `CATSSAgent.log_002` • `CATSSAgent.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.

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

Related tasks

Installing test fixes and diagnostic builds
IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

Related reference

Frequently asked questions

Troubleshooting profile issues

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

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

Related tasks

Installing test fixes and diagnostic builds

IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

Related reference

Frequently asked questions

Installing test fixes and diagnostic builds

IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

About this task

These fixes can consist of either an `<ADAPTER>.UPLOAD.XMI` file or a zip file containing a new adapter or ADK binary.

XMI files require a full new install. These are usually provided when several components have changed compared to the release you currently had installed. To ensure that there are no inconsistencies between the versions of the components you have installed and the updated components that were used to created the fix, you must perform the full installation from scratch using the XMI that contains the fix.

You receive a zip file that contains one or more binaries if the changes that the fix requires are limited to the adapter or ADK code. These new binaries must be used to replace the binaries that have the same name in your existing adapter installation.

The steps to install a new ADK binary are identical to the steps to install a new agent binary. The steps to install a new ADK library are also identical to the steps to install a new agent binary with the exception of the location where the libraries are stored. The libraries can be found in and uploaded to the `read_only_home/lib` folder.

Follow the procedures below to install a new agent binary.

Procedure

1. Extract the binary from the zip file.
2. Stop the adapter.
3. Change the directory with `cd read_only_home/bin` folder.
4. Copy `<adaptertype>Agent <adaptertype>Agent.save`.
5. Upload `<adapterype>Agent` in binary ftp mode to the adapter host and store it in the `read_only_home/bin` folder.
6. Change the directory with `cd read_only_home/bin` folder.
7. Change the permissions with `chmod 755 <adaptertype>Agent`.
8. Specify the extended attributes with `extattr +ap <adaptertype>Agent`.
9. Start the adapter.

Related concepts

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Logs

When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

Troubleshooting profile issues

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

Related reference

Frequently asked questions

Frequently asked questions

Where can I find registry and/or permission related errors?

In ISPF, navigate to S (SDSF), LOG.

How can I disable persistent connections between the Identity Server and the adapter?

The first is in IBM Security Verify Governance. 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` to set the DAML line to `DEBUG_MAX`.

this will enable full tracing for DAML based adapters. The information that is generated includes SSL communication and account details.

How do I resolve ICH420I PROGRAM XXXX FROM LIBRARY ISP.SISPLOAD CAUSED THE ENVIRONMENTTO BECOME UNCONTROLLED errors?

Add the **PROGRAM** profile to the ISP.SISPLOAD data set.

```
RALTER PROGRAM **ADDMEM('ISP.SISPLOAD'//NOPADCHK)
SETROPTS WHEN(PROGRAM) REFRESH
```

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.

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

Related tasks

Installing test fixes and diagnostic builds
IBM provides a test fix or diagnostic build if you have a case to report an issue that you encountered while working with the adapter.

Chapter 7. Uninstalling

To remove an adapter from the 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.

About this task

To uninstall the adapter, perform the following steps:

Procedure

1. Stop the adapter, if it is running. See “Restarting the adapter service” on page 15.
2. Remove the started task JCL from the system procedure library.
3. Remove the `read-only` and `read/write` directories from the z/OS USS 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 and object classes

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.You can use the attributes that are available on the adapter account form.

Table 21. Account form attributes

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

eraccountstatus	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) SUSPEND`
						To delete:
						`TSS REM(id) ASUSPED`

ertopzacidauth	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) ACID(val)`
						To delete:
						`TSS DEA(id) ACID(val)`

ertopzadminlist data	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) DATA(val)`
						To delete:
						`TSS DEA(id) DATA(val)`

ertopzassize	Integer	10	Single	RW	No	To add:
						`TSS ADD(id) ASSIZE(val)`
						To delete:
						`TSS REM(id) ASSIZE`

ertopzasuspend	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) SUSPEND`
						To delete:
						`TSS REM(id) ASUSPEND`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzaudit	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) AUDIT`
						To delete:
						`TSS REM(id) AUDIT`

ertopzconsole	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) CONSOLE`
						To delete:
						`TSS REM(id) CONSOLE`

ertopzdepartmtacid	String	8	Single	RW	No	To add: `TSS CREATE(id) DEPT (val)`

ertopzdfltgrp	String	8	Single	RW	No	To add:
						`TSS REP(id) DFLTGRP (val)`
						To delete:
						`TSS REM(id) DFLTGRP`

ertopzdfltslbl	True, False, or Null	8	Single	RW	No	To add:
						`TSS REP(%s) DFLTSLBL(%s)`
						To delete:
						`TSS REM(%s) DFLTSLBL`

ertopzdivisionacid	String	8	Single	RW	No	To add: `TSS CREATE(id) DIVISION (val)`

ertopzdufupd	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) DUFUPD`
						To delete:
						`TSS REM(id) DUFUPD`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzdufxtr	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) DUFXTR`
						To delete:
						`TSS REM(id) DUFXTR`

ertopzexpirationdate	Date (LDAP date/time)	8	Single	RW	No	To add:
						`TSS ADD(id) UNTIL(val)`
						To delete:
						`TSS REM(id) EXPIRE`

ertopzfacility	String	8	Multiple	RW	No	To add:
						`TSS ADD(id) FACILITY (val)`
						To delete:
						`TSS REM(id) FACILITY (val)`

ertopzgid	Integer	10	Single	RW	No	-

ertopzgroup	String	8	Multiple	RW	No	To add:
						`TSS ADD(id) GROUP(val)`
						To delete:
						`TSS REM(id) GROUP(val)`

ertopzimsmsc	True, False, or Null	8	Single	RW	No	To add:
						`TSS REP(%s) IMSMSC(%s)`
						To delete:
						`TSS REM(%s) IMSMSC`

ertopzinstdata	String	255	Single	RW	No	To add:
						`TSS REP(id) INSTDATA ('val')`
						To delete:
						`TSS REM(id) INSTDATA`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzlanguage	String	1	Single	RW	No	To add:
						`TSS ADD(id) LANGUAGE (val)`
						To delete:
						`TSS REM(id) LANGUAGE`

ertopzlds	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) LDS`
						To delete:
						`TSS REM(id) LDS`

ertopzmatchlim	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) AUDIT MATCHLIM`
						To delete:
						`TSS REM(id) MATCHLIM`

ertopzmastfac	String	8	Single	RW	No	To add:
						`TSS ADD(id) MASTFAC (val)`
						To delete:
						`TSS REM(id) MASTFAC`

ertopzmemlimit	Integer	10	Single	RW	No	To add:
						`TSS ADD(%s) MEMLIMIT(%s)`
						To delete:
						`TSS REM(%s) MEMLIMIT`

ertopzmisc1	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) MISC1(val)`
						To delete:
						`TSS DEA(id) MISC1(val)`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzmisc2	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) MISC2(val)`
						To delete:
						`TSS DEA(id) MISC2(val)`

ertopzmisc3	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) MISC3(val)`
						To delete:
						`TSS DEA(id) MISC3(val)`

ertopzmisc4	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) MISC4(val)`
						To delete:
						`TSS DEA(id) MISC4(val)`

ertopzmisc5	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) MISC5(val)`
						To delete:
						`TSS DEA(id) MISC5(val)`

ertopzmisc7	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) MISC7(val)`
						To delete:
						`TSS DEA(id) MISC7(val)`

ertopzmisc8	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) MISC8(val)`
						To delete:
						`TSS DEA(id) MISC8(val)`

ertopzmisc9	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) MISC9(val)`
						To delete:
						`TSS DEA(id) MISC9(val)`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzmmaparea	Integer	10	Single	RW	No	To add:
						`TSS ADD(id) MMAPAREA (val)`
						To delete:
						`TSS REM(id) MMAPAREA`

ertopzmro	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) MRO`
						To delete:
						`TSS REM(id) MRO`

ertopzmultipw	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) MULTIPW`
						To delete:
						`TSS REM(id) MULTIPW`

ertopznetvcons	String	8	Multiple	RW	No	To add:
						`TSS REP(%s) NETVCONS(%s)`
						To delete:
						`TSS REM(%s) NETVCONS`

ertopznetvctl	String	8	Single	RW	No	To add:
						`TSS REP(%s) NETVCTL(%s)`
						To delete:
						`TSS REM(%s) NETVCTL`

ertopznetvdmns	String	5	Multiple	RW	No	To add:
						`TSS REP(%s) NETVDMNS(%s)`
						To delete :
						`TSS REM(%s) NETVDMNS`

ertopznetvic	String	255	Single	RW	No	To add:
						`TSS REP(%s) NETVIC('%s')`
						To delete:
						`TSS REM(%s) NETVIC`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

eropznetvmsgr	String	8	Single	RW	No	To add:
						`TSS REP(%s) NETVMSGR(%s)`
						To delete:
						`TSS REM(%s) NETVMSGR`

ertopznetvngmf	String	8	Single	RW	No	To add:
						`TSS REP(%s) NETVNGMF(%s)`
						To delete :
						`TSS REM(%s) NETVNGMF`

ertopznetvopcl	String	5	Multiple	RW	No	To add:
						`TSS REP(%s) NETVOPCL(%s)`
						To delete:
						`TSS REM(%s) NETVOPCL`

ertopzphrase	String	100	Single	RW	No	To add: `TSS REP(%s) PHRASE(%s)`

ertopzsname	String	64	Single	RW	No	To add:
						`TSS ADD(%s) SNAME('%s')`
						To delete :
						`TSS REM(%s) SNAME`

ertopzname	String	32	Single	RW	No	To add: `TSS REP(id) NAME('val')`

ertopznoadsp	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOADSP`
						To delete:
						`TSS REM(id) NOADSP`

ertopznoats	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOATS`
						To delete:
						`TSS REM(id) NOATS`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopznodsnchk	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NODSNCHK`
						To delete:
						`TSS REM(id) NODSNCHK`

ertopznolcfchk	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOLCFCHK`
						To delete:
						`TSS REM(id) NOLCFCHK`

ertopznoomvsdf	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOOMVSDF`
						To delete:
						`TSS REM(id) NOOMVSDF`

ertopznopwchg	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOPWCHG`
						To delete:
						`TSS REM(id) NOPWCHG`

ertopznoreschk	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NORESCHK`
						To delete:
						`TSS REM(id) NORESCHK`

ertopznosubchk	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOSUBCHK`
						To delete:
						`TSS REM(id) NOSUBCHK`

ertopznosuspen	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOSUSPEND`
						To delete:
						`TSS REM(id) NOSUSPEND`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopznovmdchk	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOVMDCHK`
						To delete:
						`TSS REM(id) NOVMDCHK`

ertopznovolchk	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) NOVOLCHK`
						To delete:
						`TSS REM(id) NOVOLCHK`

ertopzoecputm	Integer	10	Single	RW	No	To add:
						`TSS ADD(id) OECPUTM (val)`
						To delete:
						`TSS REM(id) OECPUTM`

ertopzoefilep	Integer	10	Single	RW	No	To add:
						`TSS ADD(id) OEFILEP (val)`
						To delete:
						`TSS REM(id) OEFILEP`

ertopzidcard	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) OIDCARD`
						To delete:
						`TSS REM(id) OIDCARD`

ertopzomvs home	String	68	Single	RW	No	To add:
						`TSS ADD(id) HOME('val')`
						To delete:
						`TSS REM(id) HOME`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzomvspgm	String	68	Single	RW	No	To add:
						`TSS ADD(id) OMVSPGM ('val')`
						To delete:
						`TSS REM(id) OMVSPGM`

ertopzopclass	Integer	2	Multiple	RW	No	To add:
						`TSS ADD(id) OPCLASS (val)`
						To delete:
						`TSS REM(id) OPCLASS (val)`

ertopzopident	String	3	Single	RW	No	To add:
						`TSS ADD(id) OPIDENT (val)`
						To delete:
						`TSS REM(id) OPIDENT`

ertopzopprty	Integer	3	Single	RW	No	To add:
						`TSS ADD(id) OPPRTY(val)`
						To delete:
						`TSS REM(id) OPPRTY`

ertopzpass expinvl	Integer	3	Single	RW	No	To add:
						`TSS REP(id) PASSWORD (*,val)`
						To delete:
						`TSS REM(id) PASSWORD (*,0)`

ertopzpsuspend	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(%s) PSUSPEND`
						To delete:
						`TSS REM(%s) PSUSPEND`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzhrsexpinvl	Integer	3	Single	RW	No	To add:
						`TSS ADD(id) PHRASE (*,val)`
						To delete:
						`TSS REM(id) PHRASE (*,0)`

ertopzprocuser	Integer	10	Single	RW	No	To add:
						`TSS ADD(id) PROCUSER (val)`
						To delete:
						`TSS REM(id) PROCUSER`

ertopzprofile		12	Multiple	RW	No	To add:
						`TSS ADD(id) PROFILE (val)`
						To delete:
						`TSS REM(id) PROFILE (val)`

ertopzpswdphr	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) PSWDPHR`
						To delete:
						`TSS REM(id) PSWDPHR`

ertopzrstdacc	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) RSTDACC`
						To delete:
						`TSS REM(id) RSTDACC`

ertopzscopez	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) SCOPE(val)`
						To delete:
						`TSS DEA(id) SCOPE(val)`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzsctykey	Integer	3	Mutliple	RW	No	To add:
						`TSS ADD(id) SCTYKEY (val)`
						To delete:
						`TSS REM(id) SCTYKEY (val)`

ertopzsitran	String	8	Multiple	RW	No	To add:
						`TSS ADD(id) SITRAN(val)`
						To delete:
						`TSS REM(id) SITRAN`

ertopzsmsappl	String	8	Single	RW	No	To add:
						`TSS ADD(id) SMSAPPL (val)`
						To delete:
						`TSS REM(id) SMSAPPL`

ertopzsmsdata	String	8	Single	RW	No	To add:
						`TSS ADD(id) SMSDATA (val)`
						To delete:
						`TSS REM(id) SMSDATA`

ertopzsmsmgmt	String	8	Single	RW	No	To add:
						`TSS ADD(id) SMSMGMT (val)`
						To delete:
						`TSS REM(id) SMSMGMT`

ertopzsmsstor	String	8	Single	RW	No	To add:
						`TSS ADD(id) SMSSTOR (val)`
						To delete:
						`TSS REM(id) SMSSTOR`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzsuspended untildate	Date (LDAP date/time)	13	Single	RW	No	To add:
						`TSS ADD(id) SUSPEND UNTIL(val)`
						To delete:
						`TSS REM(id) ASUSPEND UNTIL`

ertopzthreads	Integer	10	Single	RW	No	To add:
						`TSS ADD(id) THREADS (val)`
						To delete:
						`TSS REM(id) THREADS`

ertopztso command	String	80	Single	RW	No	To add:
						`TSS ADD(id) TSOCOMMAND ('val')`
						To delete:
						`TSS REM(id) TSOCOMMAND`

ertopztsodefprfg	Integer	3	Single	RW	No	To add:
						`TSS ADD(id) TSODEFPRFG (value)`
						To delete:
						`TSS REM(id) TSODEFPRFG`

ertopztsodest	String	8	Single	RW	No	To add:
						`TSS ADD(id) TSODEST (val)`
						To delete:
						`TSS REM(id) TSODEST`

ertopztsohclass	String	1	Single	RW	No	To add:
						`TSS ADD(id) TSOHCLASS (val)`
						To delete:
						`TSS REM(id) TSOHCLASS`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopztsojclass	String	1	Single	RW	No	To add:
						`TSS ADD(id) TSOJCLASS (val)`
						To delete:
						`TSS REM(id) TSOJCLASS`

ertopztsolacct	String	40	Single	RW	No	To add:
						`TSS ADD(id) TSOLACCT (val)`
						To delete:
						`TSS REM(id) TSOLACCT`

ertopztsolproc	String	8	Single	RW	No	To add:
						`TSS ADD(id) TSOLPROC (val)`
						To delete:
						`TSS REM(id) TSOLPROC`

ertopztsolsize	Integer	7	Single	RW	No	To add:
						`TSS ADD(id) TSOLSIZE (val)`
						To delete:
						`TSS REM(id) TSOLSIZE`

ertopztsomclass	String	1	Single	RW	No	To add:
						`TSS ADD(id) TSOMCLASS (val)`
						To delete:
						`TSS REM(id) TSOMCLASS`

ertopztsompw	True, False, or Null	8	Single	RW	No	To add:
						`TSS ADD(id) TSOMPW`
						To delete:
						`TSS REM(id) TSOMPW`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopztsomsize	Integer	7	Single	RW	No	To add:
						`TSS ADD(id) TSOMSIZE (val)`
						To delete:
						`TSS REM(id) TSOMSIZE`

ertopztsoopt	String	12	Multiple	RW	No	To add:
						`TSS ADD(id) TSOOPT(val)`
						To delete:
						`TSS REM(id) TSOOPT(val)`

ertopztsosclass	String	1	Single	RW	No	To add:
						`TSS ADD(id) TSOSCLASS (val)`
						To delete:
						`TSS REM(id) TSOSCLASS`

ertopztsoudata	String	4	Single	RW	No	To add:
						`TSS ADD(id) TSOUDATA (val)`
						To delete:
						`TSS REM(id) TSOUDATA`

ertopztsounit	String	8	Single	RW	No	To add:
						`TSS ADD(id) TSOUNIT (val)`
						To delete:
						`TSS REM(id) TSOUNIT`

ertopztype	String	8	NEWE	RW	No	

ertopztzone	String	3	Single	RW	No	To add:
						`TSS ADD(id) TZONE(val)`
						To delete:
						`TSS REM(id) TZONE`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzuid	Integer	10	Single	RW	No	To add:
						`TSS ADD(id) UID(val)`
						To delete:
						`TSS REM(id) UID`

ertopzvsuspend	True, False, or Null	8	Single	RW	No	-

ertopzwaaccnt	String	255	Single	RW	No	To add:
						`TSS REP(id) WAACCNT (val)`
						To delete:
						`TSS REM(id) WAACCNT`

ertopzwaaddr1	String	255	Single	RW	No	To add:
						`TSS REP(id) WAADDR1 (val)`
						To delete:
						`TSS REM(id) WAADDR1`

ertopzwaaddr2	String	255	Single	RW	No	To add:
						`TSS REP(id) WAADDR2 (val)`
						To delete:
						`TSS REM(id) WAADDR2`

ertopzwaaddr3	String	255	Single	RW	No	To add:
						`TSS REP(id) WAADDR3 (val)`
						To delete:
						`TSS REM(id) WAADDR3`

ertopzwaaddr4	String	255	Single	RW	No	To add:
						`TSS REP(id) WAADDR4 (val)`
						To delete:
						`TSS REM(id) WAADDR4`

Table 21. Account form attributes (continued)

Attribute	Data type	Maximum length	Single or multiple value	Read or write	Required?	Commands

ertopzwabldg	String	255	Single	RW	No	To add:
						`TSS REP(id) WABLDG (val)`
						To delete:
						`TSS REM(id) WABLDG`

ertopzwadept	String	255	Single	RW	No	To add:
						`TSS REP(id) WADEPT (val)`
						To delete:
						`TSS REM(id) WADEPT`

ertopzwaname	String	255	Single	RW	No	To add:
						`TSS REP(id) WANAME (val)`
						To delete:
						`TSS REM(id) WANAME`

ertopzwaroom	String	255	Single	RW	No	To add:
						`TSS REP(id) WAROOM(val)`
						To delete:
						`TSS REM(id) WAROOM`

ertopzzoneacid	String	8	Single	RW	No	-

ertopzacidauth	String	8	Multiple	RW	No	To add:
						`TSS ADMI(id) ACID(val)`
						To delete:
						`TSS DEA(id) ACID(val)`

ertopzseclabel	String	8	Multiple	RW	No	To add:
						`TSS ADD(id) SECLABEL(val)`
						To delete:
						`TSS REM(id) SECLABEL(val)`

Registry settings

The adapter has several registry settings. See the table for these registry options, their descriptions, and values, if any.

Table 22. Registry settings and additional information

Option attribute	Default value	Valid value	Function and meaning	Required ?
DSEXEC	hlq.exec	Valid dsn	The adapter uses this value to ini- tialize the ISIMEXIT/ISIMEXEC Yes REXX scripts	Yes
DSJOB	hlq.cntl	Valid dsn	Specifies the data set where the RECOJOB is located.	Yes
LOKUSAVE	hlq.lsave	Valid dsn	Stores the intermediate single ac- count lookup results.	Yes
PRODFIG	3	3 or 4	Used to define the number of digits that are used to specify the order in which profiles are assigned to an account	Yes
RACRC	120	Any integer with a minimum value of 3	The amount of time in seconds the adapter waits for the RECOJOB job to complete processing.	Yes
RACINPUT	TRUE	TRUE or FALSE	Specifies if the adapter should run RECOJOB	Yes
RECOSAVE	valid dsn		Stores the intermediate reconciliation results.	Yes
PASSEXPIRE	TRUE	TRUE or FALSE	This 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
PASSGEN	TRUE	TRUE or FALSE	When set to TRUE a password is generated when you are adding an account with only a password phrase. When set to FALSE a password is never generated. If the PHRASEONLY attribute is defined in the ACCOUNT ADD request, the PASSGEN value is ignored.	No

Table 22. Registry settings and additional information (continued)				
Option attribute	**Default value**	**Valid value**	**Function and meaning**	**Required ?**
PHRASEEXPIRE	TRUE	TRUE, FALSE	This is the default action that the adapter must perform when the adapter receives a password phrase change request. TRUE indicates that password phrases must be set as expired. FALSE indicates that password phrases must be set as non-expired.	No
PWD_CONFIG	CnccSCNS	See “Password phrases” on page 100.	See “Password phrases” on page 100.	No
RESWORD	None	A comma separated list of reserved words (maximum of 300 characters total)	See “Password phrases” on page 100.	No

Environment variables

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

Table 23. Top Secret Adapter environment variables			
Environment variable	**Meaning or use**	**Default value**	**Required?**
PROTOCOL_DIR	Specify the location of adapter protocol modules, for example, the `./lib` directory	LIBPATH	No
REGISTRY	Specify the location of a specific registry file. The registry path is the fully qualified path and the file name of the registry file. The registry name is the adapter name in 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

Table 23. Top Secret Adapter environment variables (continued)			
Environment variable	**Meaning or use**	**Default value**	**Required?**
ISIM_ADAPTER_CIPHER_LIST	Defines the permitted cipher lists. Cipher list consists of one or more cipher strings separated by colons.	*HIGH*	*Yes*
CEE RUNOPTS	See https://www.ibm.com/docs/en/zos/2.4.0?topic=procedures-language-environment-runtime-options	'HEAP(170000K,4K,ANYWHERE,KEEP,1K,1K),AN(14000K,4K,ANY,KEEP),AL(ON)', 'HEAPPOOLS(ON,8,,16,,24,,80,,1120,,9904,,10000,,10672,,15032,,19800,,20888,,28360,),RPTOPTS(OFF),RPTSTG(OFF)'	No

Profile entitlements and rights

The order of profiles that are attached to an ACID is important and affects the checking of the profile permissions.

To add profiles in a particular order, each profile entitlement has a mandatory right with the name SEQUENCE defined. The SEQUENCE values define the order in which profiles are added to the ACID. These SEQUENCE values are combined with the Top Secret profile name in the request that is sent to the adapter. The first number indicates the order and the separator is a vertical bar character:

```
010|PROFA
020|PROFB
```

The profile names are sorted by number (if necessary) by the adapter and added to the ACID in that order.

For example, if you then wanted to add PROFC after PROFA and before PROFB, you can add a new entitlement for PROFC with the SEQUENCE right value set to 015.

```
010|PROFA
020|PROFB
015|PROFC
```

The `Rights` form for a selected user in **Access Governance Core** > **Manage** > **Users** already lists the previous two profile entitlements and matching SEQUENCE values. You can add only the new profile entitlement, ensuring that the SEQUENCE value specifies the correct order in the `Entitlements` form. Alternatively, you can delete the existing entitlements in the `Entitlements` form and then add all entitlements in the desired order. You can also add the new entitlement with the correct SEQUENCE value and correct the values for existing SEQUENCE values in the `Rights` form individually.

Following TSS commands are generated by the adapter.

```
'TSS REMOVE(USERID) PROFILE(PROFA)'
'TSS ADD(USERID) PROFILE(PROFA)'
'TSS REMOVE(USERID) PROFILE(PROFC)'
'TSS ADD(USERID) PROFILE(PROFC)'
'TSS REMOVE(USERID) PROFILE(PROFB)'
'TSS ADD(USERID) PROFILE(PROFB)'
```

You can increase the number of digits that are used in the SEQUENCE value to determine the profile order, from 3 digits to 4 digits. For example, from the 3 digits `"010"` you can set it to the 4 digits `"0010"` SEQUENCE value. It changes the request that is sent to the adapter from `"010|PROFA"`, to `"0010|PROFA"`. By doing so, the adapter can manage a larger number of profiles.

Specify the number of digits as the PROFDIG registry settings value during the installation process and manage it using the **agentCfg** tool.

Index

A

C

D

E

F

I

J

K

L

M

N

O

P

R

S

T

U

V

Z