

*Integrating IBM Security Identity  
Manager with IBM Security Identity  
Governance and Intelligence*





---

# Contents

## The Integration of IBM Security Identity Manager with IBM Security Identity Governance and Intelligence . . . . . 1

What's new . . . . .	1
Overview . . . . .	3
Synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence . . . . .	4
Synchronization from IBM Security Identity Governance and Intelligence to IBM Security Identity Manager . . . . .	4
Deployment topologies . . . . .	5
Operations . . . . .	5
Installation and configuration roadmap . . . . .	6
Installation prerequisites . . . . .	9
Pre-installation setup . . . . .	10
Setting up IBM Tivoli Directory Integrator . . . . .	10
Enabling the <b>change1og</b> for IBM Security Identity Manager . . . . .	12
Enabling SSL (optional) . . . . .	13
Database preparation . . . . .	13
Defining a host name in the hosts file . . . . .	14
Installing the solution for IBM Security Identity Governance and Administration Data Integrator . . . . .	15
Roadmap to upgrade IBM Security Identity Governance and Administration Data Integrator . . . . .	17
Upgrading the solution for IBM Security Identity Governance and Administration Data Integrator . . . . .	18
Updating the SDK for IBM Security Identity Governance and Intelligence. . . . .	20
Rerun the LOAD assembly line. . . . .	21
Configuring . . . . .	21
Setting the ITDL_HOME property . . . . .	21
Setting up the Data Integrator server startup file and logging behavior . . . . .	21
Setting and encrypting properties . . . . .	23
Configure the SSL certificate for the IBM Security Identity Manager 7.0 virtual appliance . . . . .	24
Importing the certificate from IBM Security Identity Manager to IBM Tivoli Directory Integrator . . . . .	27
Verifying the configuration . . . . .	28
Assembly line operations. . . . .	29
Starting and stopping the IBM Tivoli Directory Integrator server. . . . .	30

Starting an initial data load . . . . .	30
Loading entities by type . . . . .	31
Starting incremental data synchronization . . . . .	33
Starting entitlement fulfillment synchronization . . . . .	33
Stopping incremental synchronization . . . . .	34
Stopping entitlement fulfillment synchronization operations . . . . .	34
Monitoring assembly lines . . . . .	35
Data Integrator support for adapters . . . . .	37
Manually customizing IBM Security Identity Manager Adapters . . . . .	37
Configuring adapters with complex group attributes . . . . .	38
Customization . . . . .	39
Person attribute mapping. . . . .	39
Account attribute mapping . . . . .	41
Non-group permission support. . . . .	42
Complex RACF group right support . . . . .	45
Support for IBM Security Identity Manager when justification is required . . . . .	47
Customizing Organizational Unit Mapping. . . . .	47
Supporting the PostgreSQL database . . . . .	48
Reference . . . . .	49
Importing the server certificate to the Tivoli Directory Integrator client keystore . . . . .	49
Configuration property files . . . . .	50
Files installed with IBM Security Identity Governance and Administration Data Integrator . . . . .	58
Troubleshooting . . . . .	59
Repair list . . . . .	60
Synchronizing Oracle system times with IBM Security Identity Governance and Intelligence . . . . .	61
Odd status shown in OUT events table . . . . .	61
SOAP operation error . . . . .	62
IBM Security Identity Governance and Administration Data Integrator .properties files modifications. . . . .	62
Accept signer certificate from IBM Tivoli Identity Manager 5.1 and the IBM Security Identity Governance and Intelligence server . . . . .	62

Index . . . . .	65
-----------------	----



---

# The Integration of IBM Security Identity Manager with IBM Security Identity Governance and Intelligence

Use the IBM® Security Identity Governance and Administration Data Integrator to integrate IBM Security Identity Manager with IBM Security Identity Governance and Intelligence

This document is intended for security deployment specialists.

You can obtain the IBM Security Identity Governance and Administration Data Integrator package from the IBM Passport Advantage website, [http://www.ibm.com/software/howtobuy/passportadvantage/pao\\_customers.htm](http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm).

---

## What's new

Each release of IBM Security Identity Governance and Administration Data Integrator increases support for the integration of identity management and identity governance.

The following table lists the features by release that are supported by IBM Security Identity Governance and Administration Data Integrator.

Table 1. Features added in each version

Versions	Features
7.0.7	<ul style="list-style-type: none"> <li>Support for setting the size of log files and the number of rollover log files that are kept. See “Setting up the Data Integrator server startup file and logging behavior” on page 21.</li> <li>The load-info.log file now lists objects that did not load. See “Starting an initial data load” on page 30.</li> <li>Support for non-group permission mapping. Attribute-to-Permission mapping treats the non-group attribute of an account as group attribute or permission. See “Non-group permission support” on page 42.</li> <li>Support for the PostgreSQL database in IBM Security Identity Governance and Intelligence. See “Supporting the PostgreSQL database” on page 48.</li> <li>Support for complex RACF group rights permission mapping. See “Complex RACF group right support” on page 45.</li> <li>Support for IBM Security Identity Manager when justification is required by the <b>enrole.jutificationRequired</b> property. See “Support for IBM Security Identity Manager when justification is required” on page 47.</li> <li>Support for loading entities by type. If the initial load has errors, you can correct the errors and load specific entity types instead of doing another complete initial load. See “Loading entities by type” on page 31.</li> <li>Two new properties for loading subsets of services are now available. <ul style="list-style-type: none"> <li><b>isim.service.include</b></li> <li><b>isim.service.exclude</b></li> </ul> See “Configuration property files” on page 50.</li> <li>Support for the Oracle 12c database. See “Preparing the Oracle database for IBM Security Identity Governance and Administration Data Integrator” on page 14.</li> </ul>
7.0.6	<ul style="list-style-type: none"> <li>Support to extend <b>person</b> attribute synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence. See “Person attribute mapping” on page 39.</li> <li>Support to override <b>account</b> attribute synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence. See “Account attribute mapping” on page 41.</li> <li>Support to customize OU synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence. See “Customizing Organizational Unit Mapping” on page 47.</li> <li>For Tivoli® Identity Manager, Version 5.1, the mapping between the service profile name and the account profile name in the <code>Attributes.properties</code> file is automatically detected.</li> </ul>
7.0.5	<ul style="list-style-type: none"> <li>Support for IBM Security Identity Governance and Intelligence, Version 5.2.1.</li> <li>Automatic support for adapters in IBM Security Identity Manager. You no longer need to provide mappings for group metadata in the <code>ATTRIBUTES.properties</code> file.</li> </ul>

Table 1. Features added in each version (continued)

Versions	Features
7.0.4	Support for IBM Security Identity Manager adapters with complex group attributes. IBM Security Identity Manager, Version 6.0.0.10, added support for adapters with complex group attributes. The adapter for Oracle EBS employs complex group attributes. You must customize IBM Security Identity Governance and Administration Data Integrator to support such adapters.
7.0.3.1	Internal fixes
7.0.3	<p>Support for IBM Security Identity Governance and Intelligence Version 5.2. IBM Security Identity Governance and Administration Data Integrator Version 7.03 does not support previous versions of IBM Security Identity Governance.</p> <ul style="list-style-type: none"> <li>• IBM Security Identity Manager roles become external roles in IBM Security Identity Governance and Intelligence rather than business roles. The change fixes child role assignment issues in previous versions.</li> <li>• Entitlement changes are synchronized only from external roles in IBM Security Identity Governance and Intelligence.</li> <li>• Access information for IBM Security Identity Manager roles and groups is synchronized.</li> <li>• Upgrading from Data Integrator Version 7.0.2.x to 7.0.3 requires that you run the Load assembly line again.</li> </ul>
7.0.2.1	Internal fixes
7.0.2	Support for IBM Tivoli Identity Manager 5.1
7.0.1.1	Support for IBM Security Identity Governance 5.1.1
7.0.1	An <b>ISIGtoISIM</b> assembly line fulfills the entitlement changes from IBM Security Identity Governance to IBM Security Identity Manager. A set of command-line tools are added to start or stop the Tivoli Directory Integrator server and assembly lines.
7.0	<p>Assembly lines to load data from IBM Security Identity Manager to IBM Security Identity Governance</p> <ul style="list-style-type: none"> <li>• A <b>Load</b> assembly line loads all data.</li> <li>• A <b>Delta</b> assembly line loads data incrementally. Only data that is added or modified is loaded.</li> </ul>

## Overview

IBM Security Identity Governance and Administration Data Integrator, or Data Integrator, synchronizes information between IBM Security Identity Manager and IBM Security Identity Governance and Intelligence by using IBM Tivoli Directory Integrator assembly lines.

Data Integrator synchronizes the following data:

- Information about people, roles, services, groups, and their organization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence.
- Entitlement changes from IBM Security Identity Governance and Intelligence to IBM Security Identity Manager.

## Synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence

The Load assembly line loads all data from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence. It runs once. After the initial load, the Delta assembly line, which runs continuously, incrementally loads new and changed data from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence.

The following table shows the mapping of IBM Security Identity Manager entities to IBM Security Identity Governance and Intelligence entities.

*Table 2. Mapping of entity types*

IBM Security Identity Manager entity	IBM Security Identity Governance and Intelligence entity
Organization	Org Unit
Organizational Unit	Org Unit
Location	Org Unit
Admin Domain	Org Unit
Business Partner Organization Unit	Org Unit
Organization Role	External Role
Service	Account Configuration(1) + Application(1)
Group	Permission
ISIM System Role	Permission
Person	ISIG User
Account	Account

Roles from IBM Security Identity Manager are synchronized as external roles in IBM Security Identity Governance and Intelligence. In previous releases of the Data Integrator, roles were synchronized as business roles.

An external role in IBM Security Identity Governance and Intelligence is a read-only role that acts as a permission. An external role cannot be added, changed, or deleted through the user interface in IBM Security Identity Governance and Intelligence. The Data Integrator uses APIs to perform the required synchronization operations.

IBM Security Identity Manager access information for roles and groups is synchronized. In IBM Security Identity Manager, if access is enabled for a role or a group and the access name is defined, then the access name is used as the external role name or the permission name. The access description is also synchronized for the role and group if the access is enabled and the access description is defined.

## Synchronization from IBM Security Identity Governance and Intelligence to IBM Security Identity Manager

When entitlement or authorization changes are made for a user in IBM Security Identity Governance and Intelligence, information about the changes is stored as events in the IBM Security Identity Governance and Intelligence data store. The events can be shared with external applications.

The **ISIGtoISIM** assembly line, which runs continuously, periodically processes the following events in the IBM Security Identity Governance and Intelligence data store and synchronizes them to IBM Security Identity Manager:

- Adding permission to a user. An external role is handled as a permission.
- Removing permission from a user. An external role is handled as a permission.
- Locking or suspending an account.
- Unlocking or restoring an account.
- Creating an account.
- Removing an account.

## Deployment topologies

The deployment topology differs depending on whether you run IBM Security Identity Manager Version 6 on physical computers or IBM Security Identity Manager Version 7.0 virtual appliance. The deployment topology for IBM Tivoli Identity Manager Version 5.1 is the same as for Version 6.

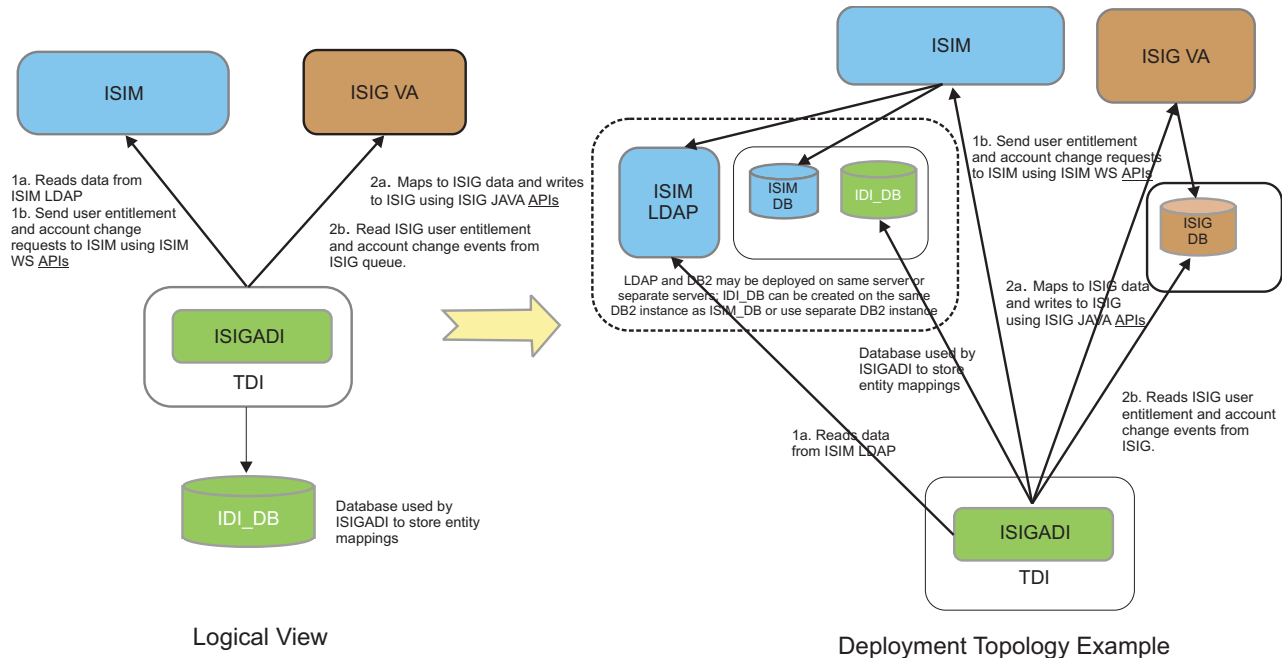


Figure 1. Deployment topologies

## Operations

The provided operations synchronize data and entitlement changes between IBM Security Identity Manager and IBM Security Identity Governance and Intelligence.

You install the Data Integrator solution in IBM Tivoli Directory Integrator. The solution includes assembly lines for the following operations:

### Full load from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence

The **Load** assembly line reads content from the IBM Security Identity Manager LDAP server and loads the data as entities in IBM Security Identity Governance and Intelligence. You typically run **Load** only once. It migrates all entity data.

### Incremental load (synchronization) from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence

The **Delta** assembly line listens for changes in the LDAP server. It then migrates the detected changes to the corresponding entities in IBM Security Identity Governance and Intelligence.

### Entitlement fulfillment synchronization from IBM Security Identity Governance and Intelligence to IBM Security Identity Manager

The **ISIGtoISIM** assembly line detects entitlement changes made in IBM Security Identity Governance and Intelligence. It fulfills those changes in IBM Security Identity Manager.

The following script files are also provided to start and stop the IBM Tivoli Directory Integrator server and assembly lines and to check the status of assembly lines.

#### **startSrv**

Starts the IBM Tivoli Directory Integrator server, **ibmdisrv**, as a daemon process.

#### **stopSrv**

Stops the IBM Tivoli Directory Integrator server.

#### **startAL**

Starts the specified assembly line on the running IBM Tivoli Directory Integrator server.

#### **stopAL**

Stops the specified assembly line on the running IBM Tivoli Directory Integrator server.

#### **showStat**

Shows the status of all assembly lines that are running on the IBM Tivoli Directory Integrator server.

For more information about these commands, see the following file on the installed system.

*ISIGADI\_SQL\_DIR/isigadi\_bin/README.txt*

---

## Installation and configuration roadmap

The roadmap provides general guidance for installing and configuring IBM Security Identity Governance and Administration Data Integrator.

You might find it useful to print the roadmap and refer to it as you set up IBM Security Identity Governance and Administration Data Integrator. Read the information topics that are referenced.

*Table 3. Roadmap for the Data Integrator*

Action	Reference	Comments
<b>Prerequisites</b>		
Meet all the requirements for installing the IBM Security Identity Governance and Administration Data Integrator.	"Installation prerequisites" on page 9	

Table 3. Roadmap for the Data Integrator (continued)

Action	Reference	Comments
<b>Install and configure Tivoli Directory Integrator</b>		
Install a supported version of Tivoli Directory Integrator	"Setting up IBM Tivoli Directory Integrator" on page 10	<p>If you have a supported version of Tivoli Directory Integrator installed, you might want to know whether the default solution directory is used by other application to avoid a conflicting port number.</p> <p>Note the following abbreviations:</p> <ul style="list-style-type: none"> <li>• TDI_INSTALL_DIR is the IBM Tivoli Directory Integrator installation directory.</li> <li>• TDI_SOL_DIR is the IBM Tivoli Directory Integrator default solution directory.</li> <li>• ISIGADI_SOL_DIR is the IBM Security Identity Governance and Administration Data Integrator solution directory.</li> </ul> <p><b>Note:</b> The ISIGADI_SOL_DIR can be the same directory as TDI_SOL_DIR if no other solution uses it.</p>
Locate the default solution directory for the IBM Tivoli Directory Integrator.	"Finding the default solution directory for Tivoli Directory Integrator" on page 11	
If the Identity Governance and Intelligence product uses an Oracle database, install the Oracle JDBC driver.	"Installing the Oracle JDBC driver" on page 12	
<b>Prepare the Security Identity Manager directory server for the Data Integrator</b>		
Enable <b>change1og</b> on the Security Identity Manager directory server.	"Enabling the <b>change1og</b> for IBM Security Identity Manager" on page 12	
If SSL connections are used for the directory server, enable SSL.	"Enabling SSL (optional)" on page 13	
<b>Create a database for the Data Integrator</b>		
Prepare the database.	Preparing the database for IBM Security Identity Governance and Administration Data Integrator	
<b>Install IBM Security Identity Governance and Administration Data Integrator</b>		

Table 3. Roadmap for the Data Integrator (continued)

Action	Reference	Comments
Install the IBM Security Identity Governance and Administration Data Integrator solution.	"Installing the solution for IBM Security Identity Governance and Administration Data Integrator" on page 15	The Data Integrator installation places artifacts in two locations. <ul style="list-style-type: none"> <li>• ISIGADI_SOL_DIR where the Data Integrator is installed.</li> <li>• TDI_INSTALL_DIR/jars directory where the .jar files are installed.</li> </ul>
<b>Configure IBM Security Identity Governance and Administration Data Integrator</b>		
In the ISIGADI_SOL_DIR/ solution.properties file, add the ITDI_HOME property.	"Setting the ITDI_HOME property" on page 21	Typically this value is equal to the TDI_INSTALL_DIR, for example ITDI_HOME=c:\Program Files\ibm\TDI\V7.1.1.
Create the Data Integrator server startup file and configure the logging behavior.	See "Setting up the Data Integrator server startup file and logging behavior" on page 21.	The file ensures that the Data Integrator starts up correctly. You can also configure the logging behavior so that the logs roll over at a specified size.
In the ISIGADI_SOL_DIR/ ISIGADI directory, edit the property files according to your environment. <ul style="list-style-type: none"> <li>• DBMAP.properties</li> <li>• ISIG.properties</li> <li>• ISIM.properties</li> </ul>	"Setting and encrypting properties" on page 23	Print the tables from "Configuration property files" on page 50 for reference.
Update ISIGADI_SOL_DIR/ isigadi_bin/systype/setEnv to reflect your platform information.	"Configuring the setEnv file" on page 23	
Configure the SSL certificate with the Security Identity Manager virtual appliance.	"Configure the SSL certificate for the IBM Security Identity Manager 7.0 virtual appliance" on page 24 <ol style="list-style-type: none"> <li>1. "Checking the existing self-signed certificate" on page 24</li> <li>2. "Creating a self-signed certificate and keystore" on page 25</li> <li>3. "Updating the IBM Security Identity Manager virtual appliance server certificate" on page 26</li> </ol>	If you use an IBM Security Identity Manager virtual appliance, these steps apply.
Import the IBM Security Identity Manager certificate.	"Importing the certificate from IBM Security Identity Manager to IBM Tivoli Directory Integrator" on page 27	If you use an IBM Security Identity Manager virtual appliance with SSL, this task applies.

Table 3. Roadmap for the Data Integrator (continued)

Action	Reference	Comments
Define a host name.	“Defining a host name in the hosts file” on page 14	
Verify that the configuration is correct.	“Verifying the configuration” on page 28	

## Installation prerequisites

Check your systems to be sure that the prerequisites are satisfied.

### Operating System

- Red Hat Enterprise Linux 6.5
- Windows 7

### IBM Identity Manager

- IBM Tivoli Identity Manager
  - Version 5.1 fix pack 15 or later with IBM Tivoli Directory Server 6.3 and IBM WebSphere® Application Server 7.0
- IBM Security Identity Manager
  - Version 6.0 fix pack 4 or later with Tivoli Directory Server version 6.3
  - Version 7.0 virtual appliance with IBM Security Directory Server Version 6.3.1
  - Version 7.0.0.2 virtual appliance with IBM Security Directory Server Version 6.4
  - Version 7.0.1.3 virtual appliance with IBM Security Directory Server Version 6.4

To run incremental loads, enable the **change1og** feature. See the documentation for IBM Security Directory Server. The simplest way to do it is to use the Configuration Tool, described in “Enabling the **change1og** for IBM Security Identity Manager” on page 12.

### IBM Security Identity Governance and Intelligence

- Version 5.2.2
- Version 5.2.1
- Version 5.2

If you are running version 5.1 or version 5.1.1 of IBM Security Identity Governance, you must use IBM Security Identity Governance and Administration Data Integrator version 7.0.2.x.

### IBM Tivoli Directory Integrator

Note the version, interim fix, and deployment requirements.

- Version 7.1.1 with fix pack 4 or a later fix pack.

To determine the current version and fix pack level of your installation, perform the following steps:

1. Go to the following directory in your installation of IBM Tivoli Directory Integrator.  
`TDI_INSTALL_DIR/bin/`
2. Run the following command:  
`applyUpdates -queryreg`

- Upgrade the IBM Tivoli Directory Integrator Java level to version 8. Install interim fix 7.1.1-TIV-TDI-LA0031. Go to <http://www.ibm.com/support/docview.wss?uid=swg24042378> and follow the instructions. Select the version appropriate for your operating system. For example, for Windows 64-bit operating systems select **refresh pack:8.0.3.0-JavaSE-JRE-Windowsx8664**.
- Deployment requirements  
Use a separate Tivoli Directory Integrator instance for the solution for IBM Security Identity Governance and Administration Data Integrator. The solution must have its own solution directory, and it must be configured to use its own ports. The instance can be installed on the same host as other instances, but it must have its own configuration file and use different ports.  
Before you install the solution for Data Integrator, set up the instance of Tivoli Directory Integrator as described in the following sections.
  - “Finding the default solution directory for Tivoli Directory Integrator” on page 11.
  - “Installing the Oracle JDBC driver” on page 12.

#### Database

- DB2 Universal Database™ Enterprise Server
  - Version 10.1
  - Version 10.5 with fix pack 3 or later
 Data Integrator uses a database to store entity mapping information. The database can be created either on the same DB2® instance that Security Identity Manager uses or on a separate DB2 instance.
- Oracle 12c database

---

## Pre-installation setup

Some setup is required before you install the solution for IBM Security Identity Governance and Administration Data Integrator.

The following setup tasks are required before you install IBM Security Identity Governance and Administration Data Integrator for the first time:

- Understanding and setting up IBM Tivoli Directory Integrator
- Enabling the **change log** for IBM Security Identity Manager
- Preparing the database for IBM Security Identity Governance and Administration Data Integrator
- Enabling SSL
- Defining a host name

## Setting up IBM Tivoli Directory Integrator

You must understand the following information about IBM Tivoli Directory Integrator.

During the installation of IBM Tivoli Directory Integrator, you are prompted to select the *Solution Directory* for the Tivoli Directory Integrator Server. The solution directory that is defined during installation is the default solution directory. It is the working directory for the ITDI server instance, and it contains a server-specific properties file, `solution.properties`. That file controls the configuration and behavior of the server.

The Data Integrator solution consists of a group of assembly lines that are specified in a single XML solution configuration file, `ISIGADI.xml`. You can have one Tivoli Directory Integrator server instance that runs multiple solutions, or you can have multiple server instances that run different solutions. Each Tivoli Directory Integrator server instance must have its own Solution Directory and corresponding configuration.

A Tivoli Directory Integrator server must bind to a port. The ports must be available, or the server does not start. The following settings in the `solution.properties` file control the ports that are used.

- `api.remote.naming.port=1099` - Is the Java™ API port of the server.
- `web.server.port=1098` - Provides web service features, like the Tivoli Directory Integrator browser dashboard.

When multiple Tivoli Directory Integrator servers run on the same computer, each must be given its own *Solution Directory*, and each `solution.properties` file must define unique ports for the two port settings.

The Tivoli Directory Integrator server that runs on the default solution directory is often called the default server.

If you are not using the default server for another solution, then you can use the default solution directory for IBM Security Identity Governance and Administration Data Integrator. If you are already using the default solution directory for another solution, then create a new solution directory for Data Integrator and use a separate Tivoli Directory Integrator server instance.

The **Delta** and **ISIGtoISIM** assembly lines are designed to run all the time to synchronize the data continuously between IBM Security Identity Manager and IBM Security Identity Governance and Intelligence.

This document assumes that you are using the default solution directory for Data Integrator.

Do not use the Tivoli Directory Integrator server instance to run other solutions.

For more information, see IBM Knowledge Center documentation for IBM Tivoli Directory Integrator and the following resources.

- Getting Started guide in the IBM Knowledge Center for IBM Tivoli Directory Integrator Version 7.1.1
- IBM Tivoli Directory Integrator blog articles
  - What is the Solution Directory?
  - Changing the Solution Directory?
  - Portable Solutions

All relative paths in the solution are resolved from the *Solution Directory*. For example, the Tivoli Directory Integrator solution configuration file `ISIGADI.xml` must be in a Solution Directory subfolder named `ISIGADI`.

## Finding the default solution directory for Tivoli Directory Integrator

You must copy the extracted Data Integrator files into a Tivoli Directory Integrator solution directory. Use this task to locate the default solution directory for Tivoli Directory Integrator.

## Procedure

1. Go to the Tivoli Directory Integrator installation folder. For example, V7.1.1.  
On Linux operating systems, the folder by default is  
`/opt/IBM/TDI/V7.1.1`  
The location depends on how you installed Tivoli Directory Integrator.
2. Go to the bin subfolder.
3. Open the defaultSolDir script file.
  - For Windows operating systems, the file name is defaultSolDir.bat.
  - For Linux operating systems, the file name is defaultSolDir.sh.The script file contains a single line that sets the Solution Directory location.  
The specified directory is the default solution directory.

## Installing the Oracle JDBC driver

If you use the Oracle database with IBM Security Identity Governance and Intelligence, install the Oracle JDBC driver to allow IBM Tivoli Directory Integrator to access the Oracle database.

### About this task

If you use the Oracle database, then you need this driver so that the ISIGtoISIM assembly line can read the entitlement change events from the Oracle database.

If you use the DB2 database, then skip this step.

## Procedure

1. Download the ojdbc6.jar file for your Oracle database version from:  
<http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html>.
2. Copy the ojdbc6.jar file to the jars/3rdparty/others directory under the Directory Integrator installation directory.

## Enabling the changelog for IBM Security Identity Manager

The **changelog** for IBM Security Identity Manager must be enabled. Use the Configuration Tool to enable it.

### About this task

For more information about **changelog**, see the Knowledge Center for IBM Security Directory Server.

## Procedure

1. Stop the IBM Security Identity Manager server.
2. Stop the IBM Tivoli Directory Integrator server.
3. In the Configuration Tool, click **Manage changelog** in the task list on the left.
4. In the Configure/unconfigure changelog window, select **Enable change log database**.
5. At **Maximum number of log entries**, click **Unlimited** for an unlimited number of entries in the change log. To limit the number of entries, click **Entries** and type the maximum number of entries you want recorded. The default is 1,000,000 entries.

6. At **Maximum age**, accept the default of **Unlimited** if you want entries to remain in the change log indefinitely. You can also click **Age** and type the number of days and hours for which you want each entry to be kept.
7. Click **Update**.  
Messages are displayed while the change log is being enabled.
8. Click **Close** when the task is complete.

## Enabling SSL (optional)

If SSL connections to the IBM Security Identity Manager LDAP directory or the database server are used, then you must import client certificates into the IBM Tivoli Directory Integrator keystore.

### About this task

See the IBM Tivoli Directory Integrator documentation at [http://www.ibm.com/support/knowledgecenter/SSCQGF\\_7.1.1/com.ibm.IBMDI.doc\\_7.1.1/adminguide37.htm%23sslsupport](http://www.ibm.com/support/knowledgecenter/SSCQGF_7.1.1/com.ibm.IBMDI.doc_7.1.1/adminguide37.htm%23sslsupport) for information about these procedures.

## Database preparation

The Data Integrator requires a database in which to store referential links between IBM Security Identity Manager and IBM Security Identity Governance and Intelligence. It also uses the database to track the current change state in IBM Security Identity Manager.

The Data Integrator can use either a DB2 database or an Oracle 12 C database. For the supported levels of databases, see “Installation prerequisites” on page 9.

### Preparing the DB2 database for IBM Security Identity Governance and Administration Data Integrator

You can create a database in DB2 to work with the Data Integrator . You typically use the DB2 instance that is part of the IBM Security Identity Manager installation. However, you can use a separate instance.

### Before you begin

You must have administrative permissions.

### About this task

To use the DB2 instance that is provided with IBM Security Identity Manager, create a database with 16k **pagesize** and create a database user. See IBM Knowledge Center for documentation specific to your version of DB2 and operating system. <http://www.ibm.com/support/knowledgecenter/SSEPGG/welcome?lang=en>

### Procedure

1. Create a user with administrator privileges on the DB2 instance.
2. Create the database and give the user the DBADM privileges by running these commands:

```
db2 CREATE DB ididb AUTOMATIC STORAGE YES PAGESIZE 16 K
db2 CONNECT TO ididb
db2 GRANT DBADM ON DATABASE TO USER idius
```

Where

**idbdb** Is the name of the database.

**iduser**

Is the user name of the administrative user that you created.

Make a record of the database name, user ID, and password for this database. This information is needed for updating the DBMAP.properties file.

**Note:**

The Data Integrator uses the IBM Tivoli Directory Integrator System Store in the database you created. The IBM Tivoli Directory Integrator documentation provides information about database management systems other than DB2 for the System Store. See [http://www.ibm.com/support/knowledgecenter/SSCQGF\\_7.1.0/com.ibm.IBMDI.doc\\_7.1/adminguide67.htm%23wq456?lang=en](http://www.ibm.com/support/knowledgecenter/SSCQGF_7.1.0/com.ibm.IBMDI.doc_7.1/adminguide67.htm%23wq456?lang=en).

## Preparing the Oracle database for IBM Security Identity Governance and Administration Data Integrator

You can create an Oracle 12c database to work with the Data Integrator.

### About this task

With the version 7.0.7 release, you can use the Oracle 12c database to store referential links between IBM Security Identity Manager and IBM Security Identity Governance and Intelligence and to track the current change state in IBM Security Identity Manager.

### Procedure

1. If not already installed, install the Oracle 12c R1 database. See the Oracle product documentation for instructions.
2. Create a database **idbdb** by using the Database Configuration Assistant (DBCA) tool.
  - Use the database character set AL32UTF8.
  - For more information, see the Oracle 12c database documentation.
3. After you create the database, decide whether to create a user for the database or the table space for the user. If you create a user, then you must grant admin privilege to this user. For more information, see the Oracle 12c documentation. If you don't create a user, use the SYSTEM user and its password.
4. Copy the Oracle JDBC driver to the *TDI\_HOME/jars/3rdparty/others* directory. Depending on the version of the JRE that the Tivoli Directory Integrator uses, copy the correct version of the JDBC driver to that directory. You cannot have multiple Oracle JDBC drivers in that directory. If you have an old version of the Oracle JDBC driver in that directory, replace it with the new one. For example, the *ojdbc6.jar* file exists in that directory and you must use the *ojdbc7.jar* file. You must delete the *ojdbc6.jar* file and replace it with the *ojdbc7.jar* file.
5. Write down the SID, database admin user name and password, and the database port number. You need this information to configure the DBMAP.properties file.

## Defining a host name in the hosts file

To access the IBM Security Identity Governance and Intelligence API, the system where IBM Tivoli Directory Integrator is running must be able to resolve the host name of the IBM Security Identity Governance and Intelligence server.

## About this task

Normally DNS services for the network are configured so that hosts can find each other.

If the systems cannot find each other through DNS, an issue with host name mapping might exist. To resolve the issue, modify the hosts file on the IBM Tivoli Directory Integrator server.

## Procedure

1. Locate the hosts file.

### Windows systems

/windows/system32/drivers/etc

### Linux systems

/etc

2. If you don't know the IP address and host name of the IBM Security Identity Governance and Intelligence server, follow these steps.
  - a. Access the Virtual Appliance dashboard in IBM Security Identity Governance and Intelligence.
  - b. Select **Manage System Settings > Application Interfaces > Interface 1**. The **Address** column shows the IPv4 address. The **Interface FQDN** column shows the host name.
3. Add a line to the file for the host where IBM Security Identity Governance and Intelligence is running.

Use the following format:

*ip\_address host\_name [short\_name]*

### ip\_address

The IPv4 address of the host.

### host\_name

The host name of the host.

### short\_name

You can use this short name to access the server or in URL values in properties files.

### Example

192.168.159.128 myisigserver.mydomain.com myisigserver

**Note:** The server does not need to be restarted when the hosts file is changed.

---

## Installing the solution for IBM Security Identity Governance and Administration Data Integrator

After you meet all prerequisites and perform the necessary pre-installation setup, install IBM Security Identity Governance and Administration Data Integrator.

## Before you begin

Check the prerequisites for IBM Tivoli Directory Integrator. See [http://www.ibm.com/support/knowledgecenter/SSCQGF\\_7.1.1/com.ibm.IBMDI.doc\\_7.1.1/adminguide11.htm%23wq20?lang=en](http://www.ibm.com/support/knowledgecenter/SSCQGF_7.1.1/com.ibm.IBMDI.doc_7.1.1/adminguide11.htm%23wq20?lang=en).

These instructions are for a new installation of IBM Security Identity Governance and Administration Data Integrator. If you are upgrading an existing installation, see “Roadmap to upgrade IBM Security Identity Governance and Administration Data Integrator” on page 17.

## About this task

The installed Directory Integrator solution for IBM Security Identity Governance and Administration Data Integrator provides the assembly lines that are needed for operations.

## Procedure

1. Copy the downloaded Data Integrator installation compressed file to a temporary directory on the host where IBM Tivoli Directory Integrator is installed.
2. Extract the files from the compressed file. The following subdirectories are created:

**jars** Contains the JAR files that are needed for the Data Integrator.

### license

Contains license files.

**soldir** Contains configuration files for the Data Integrator.

The JAR files are in the following file hierarchy.

```
jars
  3rdparty
    IBM
      IGI52
      IGI521
      IGI522
      ISIGADI
      ITIM51
  connectors
    isigadi-connectors-igi.jar
  functions
    isigadi-dn-child-of-fc.jar
    isigadi-dn-part-fc.jar
    isigadi-isim-adapter-handler-fc.jar
    isigadi-isim-api-fc.jar
    isigadi-normalize-dn-fc.jar
    isigadi-prop-value-oc.jar
```

3. Copy the jars files to the installation directory for IBM Tivoli Directory Integrator.

You might need to copy the files directory by directory, as shown in the following steps.

The following examples show the default installation directories.

### Windows systems

c:\Program Files\IBM\TDI\V7.1.1\

### Linux systems

opt/IBM/TDI/V7.1.1/

Make sure that write permissions are set on the directory.

- a. Copy the IGI52, IGI521, IGI522, ISIGADI, and ITIM51 directories to *TDI\_INSTALL\_DIR*/jars/3rdparty/IBM.
- b. Rename and remove the directories for the version of IBM Security Identity Governance and Intelligence.

- For Version 5.2.2, rename the IGI522 directory to IGI. Remove the IGI521 and IGI52 directories.
  - For Version 5.2.1, rename the IGI521 directory to IGI. Remove the IGI522 and IGI52 directories.
  - For Version 5.2, rename the IGI52 directory to IGI. Remove the IGI522 and IGI521 directories.
- c. Copy the connectors/isigadi-connectors-igi.jar file to `TDI_INSTALL_DIR/jars/connectors`.
  - d. Copy all of the JAR files from the functions directory to `TDI_INSTALL_DIR/jars/functions`.
4. Take one of the following actions:
    - If you are not using IBM Security Identity Governance and Administration Data Integrator with Version 5.1 of IBM Tivoli Identity Manager, skip this step.
    - If you are using IBM Tivoli Identity Manager Version 5.1, then you must move the following Eclipse-specific files from `TDI_INSTALL_DIR/jars/3rdparty/others` to some temporary directory outside of the `TDI_INSTALL_DIR/jars` directory.
 

```
org.eclipse.core.runtime.jar
org.eclipse.equinox.common.jar
org.eclipse.osgi.jar
```
  5. Copy the ISIGADI and isigadi\_bin directories from the extracted soldir directory to the solution directory of your installation of Tivoli Directory Integrator.  
The abbreviation for the solution directory is ISIGADI\_SOL\_DIR.

## Results

See “Files installed with IBM Security Identity Governance and Administration Data Integrator” on page 58 for a list of installed files.

## What to do next

After installation, you must configure Data Integrator before you can run it. See “Configuring” on page 21.

---

## Roadmap to upgrade IBM Security Identity Governance and Administration Data Integrator

These instructions provide the steps to upgrade an existing installation.

The upgrade process consists of upgrading the IBM Security Identity Governance and Administration Data Integrator, rerunning the LOAD assembly line, and updating the SDK.

*Table 4. Upgrade roadmap*

Action	Reference
Upgrade to the current level of IBM Security Identity Governance and Administration Data Integrator.	“Upgrading the solution for IBM Security Identity Governance and Administration Data Integrator” on page 18
Update the SDK.	“Updating the SDK for IBM Security Identity Governance and Intelligence” on page 20

Table 4. Upgrade roadmap (continued)

Action	Reference
Run the LOAD assembly line.	"Rerun the LOAD assembly line" on page 21

## Upgrading the solution for IBM Security Identity Governance and Administration Data Integrator

You can upgrade an existing version of IBM Security Identity Governance and Administration Data Integrator.

### About this task

You can upgrade the following versions of IBM Security Identity Governance and Administration Data Integrator:

Table 5. Supported migration paths

Versions	Comments
7.0.7 to 7.0.7.x	When fix packs for version 7.0.7 are available, you can update an existing version 7.0.7 installation.
7.0.3.x, 7.0.4.x, 7.0.5.x, or 7.0.6.x to 7.0.7	Migrate directly to the latest version of Data Integrator.
7.0.2.x to 7.0.7	You must first upgrade from your version of IBM Security Identity Governance to IBM Security Identity Governance and Intelligence version 5.2.1. Data Integrator version 7.0.2.x was for use with IBM Security Identity Governance.

### Procedure

1. Copy the downloaded Data Integrator installation compressed file to a temporary directory on the host where IBM Tivoli Directory Integrator is installed.
2. Extract the files. The following subdirectories are created:
  - The jars directory that contains the JAR files that are needed for the Data Integrator.
  - The license directory that contains license files.
  - The soldir directory that contains configuration files for the Data Integrator.

The JAR files are in the following file hierarchy.

```
jars
  3rdparty
    IBM
      IGI522
      IGI52
      IGI521
      ISIGADI
      ITIM51
  connectors
    isigadi-connectors-igi.jar
  functions
    isigadi-dn-child-of-fc.jar
    isigadi-dn-part-fc.jar
```

```
isigadi-isim-adapter-handler-fc.jar
isigadi-isim-api-fc.jar
isigadi-normalize-dn-fc.jar
isigadi-prop-value-oc.jar
```

3. Follow these steps to save directories from the existing solution directory to a temporary location. The variable, *ver*, is the version number of your current installation of Data Integrator.
  - a. Copy ISIGADI\_SOL\_DIR/ISIGADI to temp/ISIGADI\_*ver*.
  - b. Copy ISIGADI\_SOL\_DIR/isigadi\_bin to temp/isigadi\_bin\_*ver*.
4. Remove the files and directories from your existing installation. You might not have all of the files or directories that are listed, depending on what version of Data Integrator you have.
  - a. Remove IGI, ISIG, ISIG511, ISIGADI, and ITIM51 from *TDI\_INSTALL\_DIR/jars/3rdparty/IBM/*.
  - b. Remove the following files from *TDI\_INSTALL\_DIR/jars/*.

**Note:** Do not remove the connectors or functions directories.

```
connectors
    isigadi-connectors.jar
    isigadi-connectors-forWAS.jar
    isigadi-connectors-igi.jar
functions
    isigadi-dn-child-of-fc.jar
    isigadi-dn-part-fc.jar
    isigadi-isim-adapter-handler-fc.jar
    isigadi-isim-api-fc.jar
    isigadi-normalize-dn-fc.jar
    isigadi-prop-value-oc.jar
```

5. Copy the extracted .jar files to the installation directory for IBM Tivoli Directory Integrator. You might need to copy the files directory by directory, as shown in the following steps. The following examples show the default installation directories:

**Example for Windows systems**

c:\Program Files\IBM\TDI\V7.1.1\

**Example for Linux systems**

/opt/IBM/TDI/V7.1.1/

- a. Make sure that write permissions are set on the directory.
  - b. Copy the IGI52, IGI521, IGI522, ISIGADI, and ITIM51 directories to *TDI\_INSTALL\_DIR/jars/3rdparty/IBM/*.
  - c. Rename and remove the directories for the version of IBM Security Identity Governance and Intelligence.
    - For version 5.2.2, rename the IGI522 directory to IGI. Remove the IGI52 and IGI521 directories.
    - For version 5.2.1, rename the IGI521 directory to IGI. Remove the IGI522 and IGI52 directories.
    - For version 5.2, rename the IGI52 directory to IGI. Remove the IGI522 and IGI521 directories
  - d. Copy the connectors/isigadi-connectors-igi.jar file to *TDI\_INSTALL\_DIR/jars/connectors/*.
  - e. Copy all of the .jar files from the functions directory to *TDI\_INSTALL\_DIR/jars/functions/*.
6. Take one of the following actions:

- If you don't use IBM Security Identity Governance and Administration Data Integrator with version 5.1 of IBM Tivoli Identity Manager, skip this step.
  - If you use IBM Tivoli Identity Manager version 5.1, then you must move the following Eclipse-specific files from *TDI\_INSTALL\_DIR/jars/3rdparty/* others to a temporary directory outside of the *TDI\_INSTALL\_DIR/jars* directory (*ISIGADI\_SOL\_DIR*).
    - `org.eclipse.core.runtime.jar`
    - `org.eclipse.equinox.common.jar`
    - `org.eclipse.osgi.jar`
7. Copy the *ISIGADI* and *isigadi\_bin* directories from the extracted *soldir* directory to the solution directory of your installation of Tivoli Directory Integrator.
  8. Restore the script and properties files in *ISIGADI* and *isigadi\_bin* from the backup copies of *ISIGADI\_ver* and *isigadi\_bin\_ver*.
  9. Update the properties files in the *ISIGADI\_SOL\_DIR/ISIGADI* directory to meet your needs. See “Configuration property files” on page 50.
  10. If you did not do so, create the new server startup file and configure the logging properties. See “Setting up the Data Integrator server startup file and logging behavior” on page 21.

## Results

See “Files installed with IBM Security Identity Governance and Administration Data Integrator” on page 58.

## Updating the SDK for IBM Security Identity Governance and Intelligence

To update the IBM Security Identity Governance and Intelligence SDK for the Data Integrator, replace the IBM Security Identity Governance and Intelligence libraries.

### About this task

The Data Integrator has dependencies on libraries in IBM Security Identity Governance and Intelligence. These libraries are a set of `.jar` files in the *TDI\_INSTALL\_DIR/jars/3rdparty/IBM/IGI* directory.

If the `.jar` files are updated when you apply fix packs to the IBM Security Identity Governance and Intelligence, you must reinstall them. You can save the old `.jar` files, by copying them to the temporary directory outside of the *TDI\_INSTALL\_DIR/jars* directory. For more information, see “Files installed with IBM Security Identity Governance and Administration Data Integrator” on page 58.

### Procedure

1. Stop the IBM Tivoli Directory Integrator server. See “Starting and stopping the IBM Tivoli Directory Integrator server” on page 30.
2. From the IBM Security Identity Governance and Intelligence virtual appliance dashboard, click **Configure Identity Governance > Custom File Management**.
3. From the Custom File Management page, select **sdk** from directories list.
4. Select the `sdk.zip` file and click **Download**.
5. Extract the file.
6. Copy all the `.jar` files in the `sdk/lib` directory to *TDI\_INSTALL\_DIR/jars/3rdparty/IBM/IGI* directory.

7. Restart the IBM Tivoli Directory Integrator server.

## Rerun the **LOAD** assembly line

When you upgrade from version 7.0.2.x to version 7.0.7.x of the Data Integrator, you must run the **Load** assembly line again.

See “Starting an initial data load” on page 30.

Running the **Load** assembly line synchronizes organizational roles in IBM Security Identity Manager as external roles in IBM Security Identity Governance and Intelligence.

In the 7.0.2.x versions of Data Integrator, organizational roles were synchronized as business roles.

After you run the **Load** assembly line, the previous business roles remain in place. However, entitlement changes for these business roles are no longer synchronized to IBM Security Identity Manager.

---

## Configuring

Use the following procedures to configure the IBM Security Identity Governance and Administration Data Integrator solution.

### Setting the **ITDI\_HOME** property

The *ISIGADI\_SOL\_DIR*/solution.properties file must have the **ITDI\_HOME** property.

#### About this task

The *ISIGADI\_SOL\_DIR* directory is the IBM Security Identity Governance and Administration Data Integrator solution directory. This directory contains the *ISIGADI* and the *isigadi\_bin* directories.

#### Procedure

Set the **ITDI\_HOME** property to the ITDI installation directory. Depending on your operating system, use one of the following examples.

##### For Windows systems

```
ITDI_HOME=C:\Program Files\ibm\TDI\V7.1.1
```

##### For Linux systems

```
ITDI_HOME=/opt/IBM/TDI/V7.1.1
```

## Setting up the Data Integrator server startup file and logging behavior

You must copy a file and modify several properties to ensure that the Directory Integrator starts up and creates log files correctly.

#### Procedure

1. Stop the server.

##### Windows systems

```
stopSrv
```

## Linux systems

./stopSrv

2. Depending on your platform, perform one of these actions:

- Copy the *TDI\_INSTALL\_DIR*/ibmdisrv.bat file and rename the copy to *TDI\_INSTALL\_DIR*/ibmisigadisrv.bat.
- Copy the *TDI\_INSTALL\_DIR*/ibmdisrv file and rename the copy to *TDI\_INSTALL\_DIR*/ibmisigadisrv.

3. Depending on your platform, perform one of these actions:

- Edit the ibmisigadisrv.bat file and set the LOG\_4J properties file location to the *ISIGADI\_SOL\_DIR*. Change the path in the following information  
LOG\_4J=-Dlog4j.configuration="file:etc\log4j.properties"

to this path:

LOG\_4J=-Dlog4j.configuration="file:/// %ISIGADI\_SOL\_DIR%\ISIGADI\log4j.properties"

- Edit the ibmisigadisrv file and set the LOG\_4J properties file location to the *ISIGADI\_SOL\_DIR*. Change the path in the following information  
LOG\_4J=-Dlog4j.configuration="file:etc\log4j.properties"

to this path:

LOG\_4J=-Dlog4j.configuration="file:\$ISIGADI\_SOL\_DIR/ISIGADI/log4j.properties"

4. Depending on your platform, save the ibmisigadisrv.bat or the ibmisigadisrv file.
5. Depending on your platform, perform one of these actions:
  - Copy the *TDI\_INSTALL\_DIR*/bin/tdisrvctl.bat file and rename the copy to *TDI\_INSTALL\_DIR*/bin/isigaditdisrvctl.bat
  - Copy the *TDI\_INSTALL\_DIR*/bin/tdisrvctl file and rename the copy to *TDI\_INSTALL\_DIR*/bin/isigaditdisrvctl
6. Edit the *TDI\_INSTALL\_DIR*/bin/isigaditdisrvctl.bat file or the *TDI\_INSTALL\_DIR*/bin/isigaditdisrvctl file and set the LOG\_4J.properties file location to the *ISIGADI\_SOL\_DIR* directory. Depending on your platform, perform one of these actions:
  - Change LOG\_4J=-Dlog4j.configuration="file:/// %TDI\_HOME\_DIR%\etc\tdisrvctl-log4j.properties" to LOG\_4J=-Dlog4j.configuration="file:/// %ISIGADI\_SOL\_DIR%\ISIGADI\log4j.properties"
  - Change LOG\_4J=-Dlog4j.configuration="file:etc\tdisrvctl-log4j.properties" to LOG\_4J=-Dlog4j.configuration="file:\$ISIGADI\_SOL\_DIR/ISIGADI/log4j.properties"
7. Save the isigaditdisrvctl.bat file or the isigaditdisrvctl file.
8. Edit the *ISIGADI\_SOL\_DIR*\ISIGADI\log4j.properties file and set the following properties:  
log4j.appender.Default.Append=true  
log4j.appender.Default.MaxFileSize=1MB  
log4j.appender.Default.MaxBackupIndex=10

**Note:** The log4j.appender.Default.MaxBackupIndex property is the number of rolled over log files that you want to keep. If you need to keep more log files, you can set it higher.

9. Edit the *ISIGADI\_SOL\_DIR*\ISIGADI\log4j.properties file to modify the size of the assembly line log files and set the number of roll-over log files that you want to keep. For example,  
log4j.appender.DeltaErr.MaxFileSize=1024KB  
log4j.appender.DeltaErr.MaxBackupIndex=10

10. Save the *ISIGADI\_SOL\_DIR\ISIGADI\log4j.properties* file.
11. Start the server.

#### **Windows systems**

`startSrv`

#### **Linux systems**

`./startSrv`

## **Setting and encrypting properties**

Edit properties files to set the properties that are needed to run Data Integrator. Add encryption for the properties to meet your needs.

### **About this task**

You must configure properties for Data Integrator before you run it. You can add encryption for properties by adding the {protect}- prefix to the property key.

### **Procedure**

1. Set the properties in the Data Integrator properties files. See “Configuration property files” on page 50.
2. Add encryption for properties to meet your needs.

For example, to encrypt the `isig.password` property, make the following modification:

```
{protect}-isig.password=Passw0rd
```

Enter the password value in clear text. It is encrypted the next time that the solution is run.

### **Configuring the setEnv file**

Configure the `setEnv` file before you use the script files that are provided.

### **About this task**

Script files start and stop the server, start and stop assembly lines, and show the status of assembly lines.

Before you run the script files, you must set the correct properties in the `setEnv` file.

### **Procedure**

1. Locate the `setEnv` file.

It is in the following location:

```
ISIGADI_SOL_DIR/isigadi_bin/systype/setEnv
```

Replace *systype* with your system type, either `win` or `linux`.

2. Update the `setEnv` file with the correct properties.

The `setEnv` file has comments in it that explain how to configure the file. See also the `readme` file in the *ISIGADI\_SOL\_DIR/isigadi\_bin/* directory.

3. On Linux systems, be sure that the script files are executable. Use the following command to add execute permission.

```
chmod +x filename
```

## Configure the SSL certificate for the IBM Security Identity Manager 7.0 virtual appliance

For Data Integrator to access the Web Services API on IBM Security Identity Manager version 7 virtual appliance, the IBM Security Identity Manager virtual appliance system must have a self-signed certificate that uses an explicit host name.

Without a correct certificate, IBM Security Identity Governance and Administration Data Integrator cannot access IBM Security Identity Manager Web Services APIs on an IBM Security Identity Manager virtual appliance system. This inability exists even if the server certificate is imported to the truststore file.

Check and update the self-signed certificate and keystore:

1. Check the existing self-signed certificate. See “Checking the existing self-signed certificate.”
2. Create a self-signed certificate and keystore. See “Creating a self-signed certificate and keystore” on page 25.
3. Update the server certificate in IBM Security Identity Manager. See “Updating the IBM Security Identity Manager virtual appliance server certificate” on page 26.

### Checking the existing self-signed certificate

Check the self-signed certificate for the IBM Security Identity Manager virtual appliance to see whether its subject is set to localhost.

#### Procedure

1. In the IBM Security Identity Manager virtual appliance dashboard, click **Configure Identity Manager > Application Server Certificate Management**.

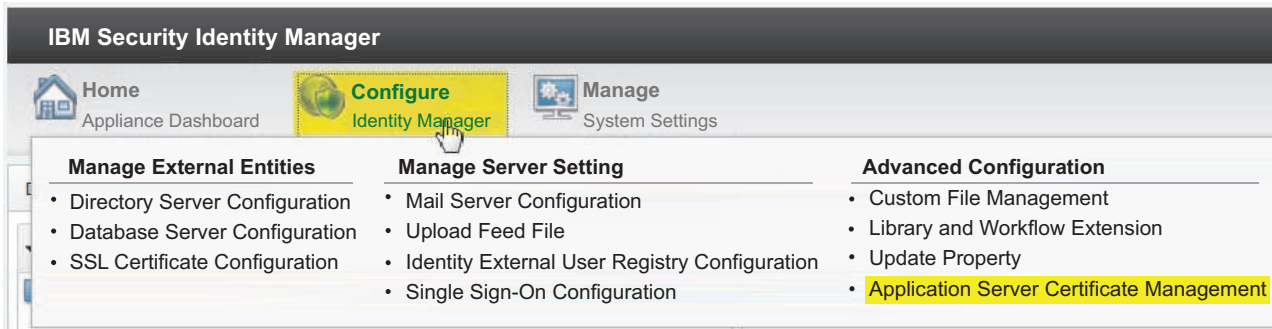


Figure 2. Checking the self-signed certificate in the IBM Security Identity Manager virtual appliance dashboard

2. In the certificate properties, check the **Subject** for the CN= setting.
  - If CN= is set to localhost, the following two tasks to generate and install a new self-signed certificate.
  - If CN= is set to an explicit host name, the SSL is properly configured and you are finished.

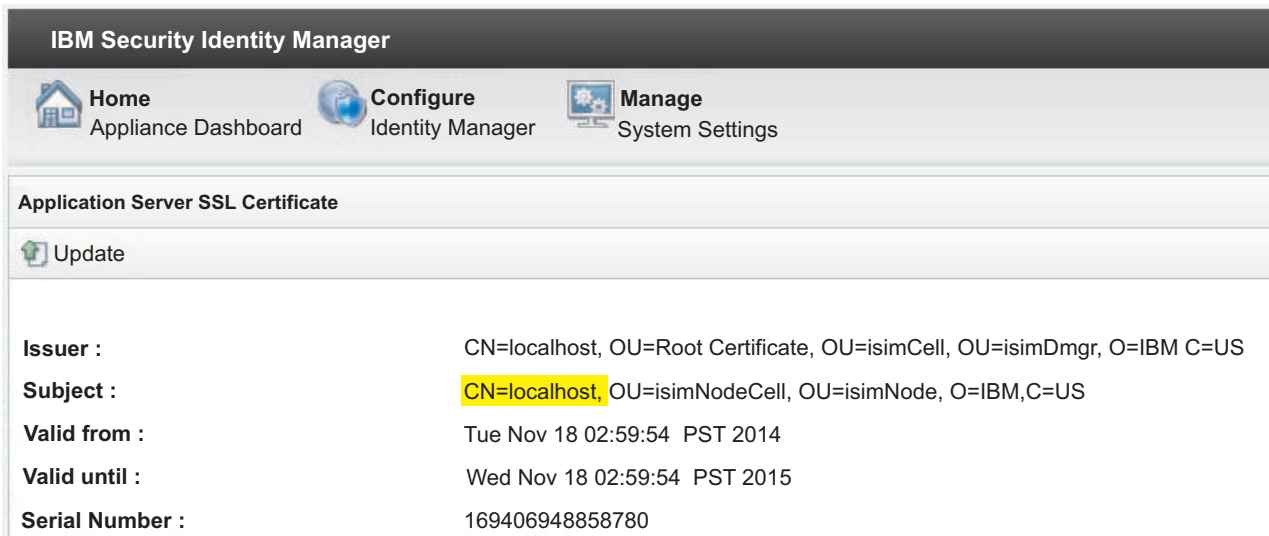


Figure 3. SSL certificate properties

## Creating a self-signed certificate and keystore

Use **keytool** to create a self-signed certificate and keystore.

### Before you begin

Locate the **keytool** application, which manages keys and certificates. It comes with the Java JDK. If the JDK is not installed, use the JDK provided with IBM Tivoli Directory Integrator 7.1.1. It is in `TDI_INSTALL_DIR/jvm/jre/bin`.

For example, on Windows systems, if the IBM Tivoli Directory Integrator is installed in `C:\Program Files\IBM\TDI\V7.1.1`, then `keytool.exe` is in `C:\Program Files\IBM\TDI\V7.1.1\jvm\jre\bin`.

### About this task

In the following procedure, note the following points.

- The `-storetype` parameter is not specified. The default keystore type JKS is used.
- To answer the prompt What is your first and last name, enter the host name for the IBM Security Identity Manager virtual appliance system.
- Write down the password you enter for `-storepass`. You need it later.
- For more information, see the **keytool** documentation.

### Procedure

1. Access the directory that contains `keytool.exe`. For example,  

```
cd "C:\Program Files\IBM\TDI\V7.1.1\jvm\jre\bin"
```
2. Run **keytool**.  

```
keytool -genkey -keyalg RSA -alias isimva -keystore keystore.jks  
-storepass password -validity 360 -keysize 2048
```
3. Complete the certificate information that is requested as **keytool** runs.

```

What is your first and last name?
[Unknown]: myisimserver.mydomain.com
What is the name of your organizational unit?
[Unknown]: Security
What is the name of your organization?
[Unknown]: IBM
What is the name of your City or Locality?
[Unknown]: CM
What is the name of your State or Province?
[Unknown]: CA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=myisimserver.mydomain.com, OU=Security, O=IBM, L=CM, ST=CA, C=US correct?
(type "yes" or "no")
[no]: yes
Enter key password for
:
(RETURN if same as keystore password):

```

## Updating the IBM Security Identity Manager virtual appliance server certificate

You must upload the keystore file that you created to update the virtual appliance server certificate.

### Procedure

1. In the IBM Security Identity Manager virtual appliance dashboard, click **Configure Identity Manager > Application Server Certificate Management**.

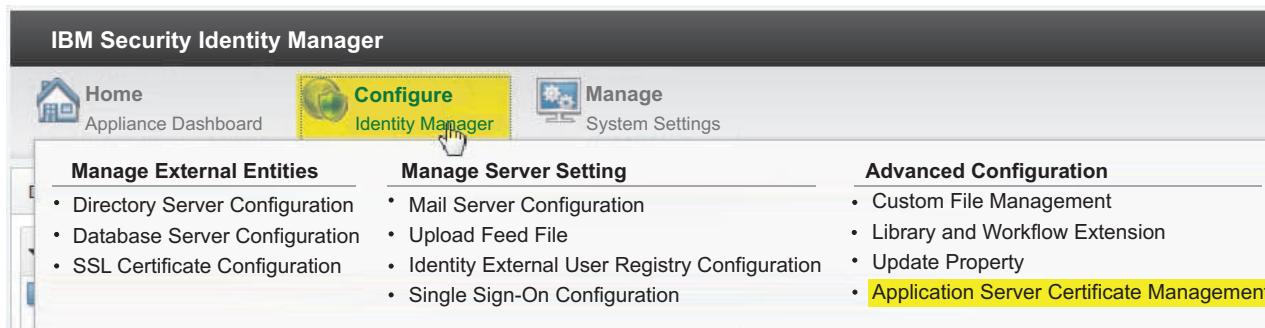


Figure 4. Updating the IBM Security Identity Manager virtual appliance certificate

2. In the **Application Server SSL Certificate** page, click **Update**.
3. In the **Upload Keystore** dialog, select or enter the following information:

**File** Browse to the keystore file that you created.

#### Keystore Password

Enter the password that you used when you created the keystore. You used it in the `-storepass` parameter in the `keytool` command.

#### Keystore Type

Select the keystore type.

JKS  
JCEKS  
PKCS12  
CMSKS  
PKCS11

For example, JKS. It is the default.

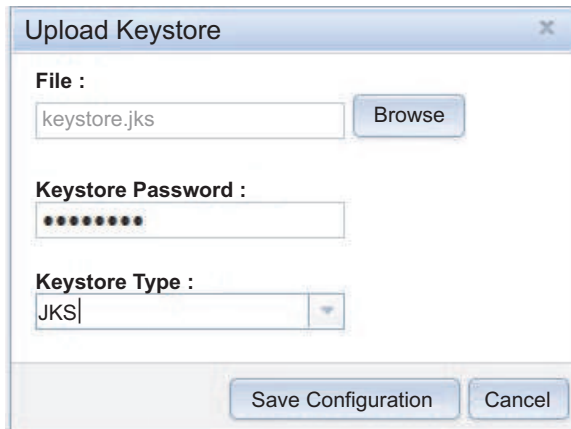
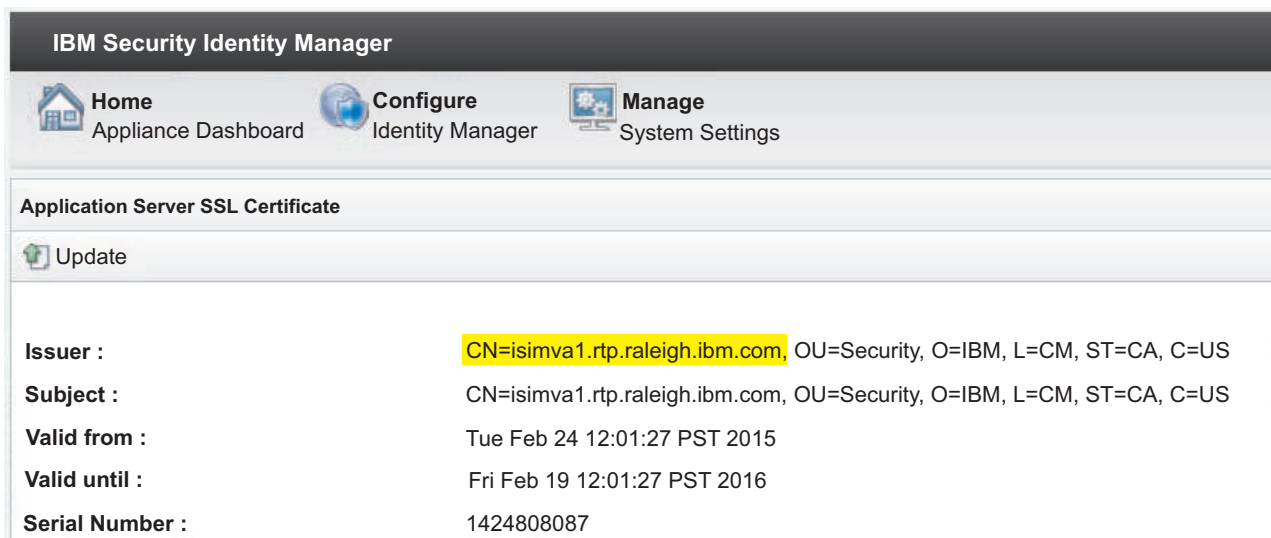
A dialog box titled "Upload Keystore" with a close button (X) in the top right corner. It contains three input fields: "File :" with a text box containing "keystore.jks" and a "Browse" button; "Keystore Password :" with a text box containing ten dots; and "Keystore Type :" with a dropdown menu showing "JKS". At the bottom are two buttons: "Save Configuration" and "Cancel".

Figure 5. Upload the keystore dialog

4. Click **Save Configuration**.
5. Verify the certificate information in the updated Application Server SSL Certificate page.

A screenshot of the IBM Security Identity Manager web interface. The top navigation bar includes "Home Appliance Dashboard", "Configure Identity Manager", and "Manage System Settings". Below this is a section titled "Application Server SSL Certificate" with an "Update" button. The main content area displays certificate details in a table-like format:

Issuer :	CN=isimva1.rtp.raleigh.ibm.com, OU=Security, O=IBM, L=CM, ST=CA, C=US
Subject :	CN=isimva1.rtp.raleigh.ibm.com, OU=Security, O=IBM, L=CM, ST=CA, C=US
Valid from :	Tue Feb 24 12:01:27 PST 2015
Valid until :	Fri Feb 19 12:01:27 PST 2016
Serial Number :	1424808087

Figure 6. The IBM Security Identity Manager virtual appliance server certificate

## Importing the certificate from IBM Security Identity Manager to IBM Tivoli Directory Integrator

You must import the Security Identity Manager server certificate to Tivoli Directory Integrator if you want to use the HTTPS protocol.

### About this task

If you access Security Identity Manager through the HTTPS protocol, then you must run the ImportCertificate assembly line to import the Security Identity Manager server certificate to the Directory Integrator trust store.

Perform this task if your deployment meets the following conditions:

- It uses the IBM Security Identity Manager virtual appliance system. It requires HTTPS for access.
- It uses a non-virtual appliance IBM Security Identity Manager system and you want to use HTTPS.

Skip this task if your deployment uses a non-virtual appliance IBM Security Identity Manager system and you want to use HTTP rather than HTTPS.

## Procedure

1. Access the script directory at *ISIGADI\_SOL\_DIR/isigadi\_bin/systype/*, where *systype* is either *win* or *linux*.

Use *win* or *linux* for *systype*.

*ISIGADI\_SOL\_DIR/isigadi\_bin/systype/*

2. If the server is not running, start the server.

### Windows systems

`startSrv`

### Linux systems

`./startSrv`

3. Run the `ImportCertificate` assembly line.

Run the following command.

`startAL ImportCertificate`

Use the correct Windows or Linux syntax.

4. Stop and restart the server.
  - a. Use the `stopSrv` command to stop the server.
  - b. Use the `startSrv` command to start the server.

## Verifying the configuration

The **Verify** assembly line verifies that configuration parameters are set correctly. It tests the availability of property files and connection settings to IBM Security Identity Governance and Intelligence and IBM Security Identity Manager.

## Procedure

1. Change directory to the directory that contains the script files.

*ISIGADI\_SOL\_DIR/isigadi\_bin/systype*

Where *systype* is either *win* or *linux*.

2. If the server is not running, start the server.

### Windows systems

`startSrv`

### Linux systems

`./startSrv`

3. Open a separate command window. Run the **Verify** assembly line.

### Windows systems

`startAL Verify`

### Linux systems

`./startAL Verify`

The output from this operation is displayed in the command line and the `Verify.log` file in the `ISIGADI/logs` subfolder of the IBM Tivoli Directory Integrator Solution Directory. If all tests run successfully, it displays the following message:

Configuration successfully verified!

Otherwise, error messages indicate problems in the configuration.

**Note:**

- If the verification operation fails because of incorrect properties settings, stop the IBM Tivoli Directory Integrator server. Update the properties and restart the Tivoli Directory Integrator server. Run the **Verify** assembly line again.
- When you use the Data Integrator for IBM Tivoli Identity Manager 5.1 or IBM Security Identity Governance and Intelligence 5.2.1, or both, you must accept the signer certificate from the server. You are prompted for it, when you run the **Verify** assembly line for the first time. See “Accept signer certificate from IBM Tivoli Identity Manager 5.1 and the IBM Security Identity Governance and Intelligence server” on page 62 in the *Troubleshooting* section.

---

## Assembly line operations

Assembly lines in IBM Tivoli Directory Integrator provide load and synchronization operations to transfer data between IBM Security Identity Manager and IBM Security Identity Governance and Intelligence.

**Load** Runs a full data load from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence. This assembly line provides the initial data load. After the load finishes, you can run the **Delta** and **ISIGtoISIM** assembly lines to keep the data updated.

**LoadOU** Runs a data load to add organizations and the sub organizational units such as locations, admin domains, business partner units, and organizational units.

**LoadRole**  
Runs a data load to add roles as external roles.

**LoadService**  
Runs a data load to add the service as an application and account configuration pair.

**LoadGroup**  
Runs a data load to add system groups and groups as permissions.

**LoadPerson**  
Runs a data load to add person entities.

**LoadAccount**  
Runs a data load to add account entities.

**LoadAccountNGP**  
Runs a data load to add accounts that have values on the attributes that are mapped to permissions.

**Delta** Runs an incremental data synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence.

**ISIGtoISIM**

Synchronizes entitlements from IBM Security Identity Governance and Intelligence to IBM Security Identity Manager.

**Verify** Verifies that configuration parameters are set correctly.

The **Load** assembly lines stop after the data load is complete. The **Delta** and **ISIGtoISIM** assembly lines run continuously after you start them.

## Starting and stopping the IBM Tivoli Directory Integrator server

You must start the IBM Tivoli Directory Integrator before you run assembly lines.

### About this task

The IBM Tivoli Directory Integrator server relies on Data Integrator properties settings. If you change the properties files after you start the IBM Tivoli Directory Integrator server, you must restart it in order for the changes to take effect. See “Configuration property files” on page 50.

### Procedure

1. Change directory to the directory that contains the script files. The script files are in the following directory.

*ISIGADI\_SOL\_DIR/isigadi\_bin/systype*

Replace *systype* with your system type, either win or linux.

2. To start the IBM Tivoli Directory Integrator server, run the following command:
  - For Windows systems  
startSrv
  - For Linux systems  
./startSrv
3. To stop the IBM Tivoli Directory Integrator server, run the following command:
  - For Windows systems  
stopSrv
  - For Linux systems  
./stopSrv

## Starting an initial data load

You must migrate data from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence. Use this procedure to start the Load assembly line to run the initial full data load.

### Before you begin

Be sure that the IBM Tivoli Directory Integrator is running. See “Starting and stopping the IBM Tivoli Directory Integrator server.”

### About this task

Use the **Load** assembly line to run a full data load from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence.

The time that the **Load** operation requires depends on the amount of information in IBM Security Identity Manager that is converted and migrated to IBM Security Identity Governance and Intelligence entities.

The assembly line captures and writes log output to log files in the *ISIGADI\_SOL\_DIR/ISIGADI/logs* directory. After you run a **Load** assembly line, the *load-info.log* file shows the objects that failed during the load process. For example,

```
2016-07-12 19:18:29,892 INFO - [AssemblyLines/ZTest_Load/SysGroup] Load Error Summary:
2016-07-12 19:18:29,893 INFO - [AssemblyLines/ZTest_Load/SysGroup] erglobalid=4444292569130753754,
ou=roles,erglobalid=00000000000000000000,ou=org,dc=com,
[AssemblyLines/Util.WriteExtRoleToIsig/ISIG-ExtRole-Lookup]
The external role could not be added with this role name:SW STATIC ROLE 2
Check to see if the external role exists with different case letters.
at 7/12/16 7:16 PM
2016-07-12 19:18:29,895 INFO - [AssemblyLines/ZTest_Load/SysGroup] erglobalid=4792467596631166323,
ou=sysRoles,erglobalid=00000000000000000000,ou=org,dc=com,
[AssemblyLines/Util.WriteSysGroupToIsig/ISIG-SysGroup-Lookup]
ISIG operation error at 7/12/16 7:18 PM
2016-07-12 19:18:29,896 INFO - [AssemblyLines/ZTest_Load/SysGroup] Number of object error during Load: 2
```

## Procedure

1. Run the **Load** assembly line from the command line with one of the following commands.

### Windows systems

```
startAL Load
```

### Linux systems

```
./startAL Load
```

2. Check the status of the assembly line with the **showStat** command. The **Load** assembly line must be finished and stopped before you run incremental operations.

```
showStat
```

## What to do next

If some entities failed to load, correct the errors in IBM Security Identity Manager. Then load the entities by using the entity type assembly lines. If all entities loaded successfully, start the incremental data synchronization by running the **Delta** assembly line.

## Loading entities by type

Depending on the amount of data, an initial data load can take a long time. If entities failed to load during the initial data load, use these assembly lines to avoid doing another complete data load.

## Before you begin

Be sure that the IBM Tivoli Directory Integrator is running. See “Starting and stopping the IBM Tivoli Directory Integrator server” on page 30.

## About this task

After you correct any issues in IBM Security Identity Manager that prevented an entity from being loaded in the initial data load, select the load assembly line for the particular type of entity. You do not need to rerun the **Load** assembly line.

**Note:** Because some entities depend on other entities, run the assembly lines in the sequence that they are presented. An account entity has a dependency on service, group, and person entities. If any of those dependencies failed to load, those errors must be corrected and the appropriate assembly lines must be run before the account entity can be successfully loaded.

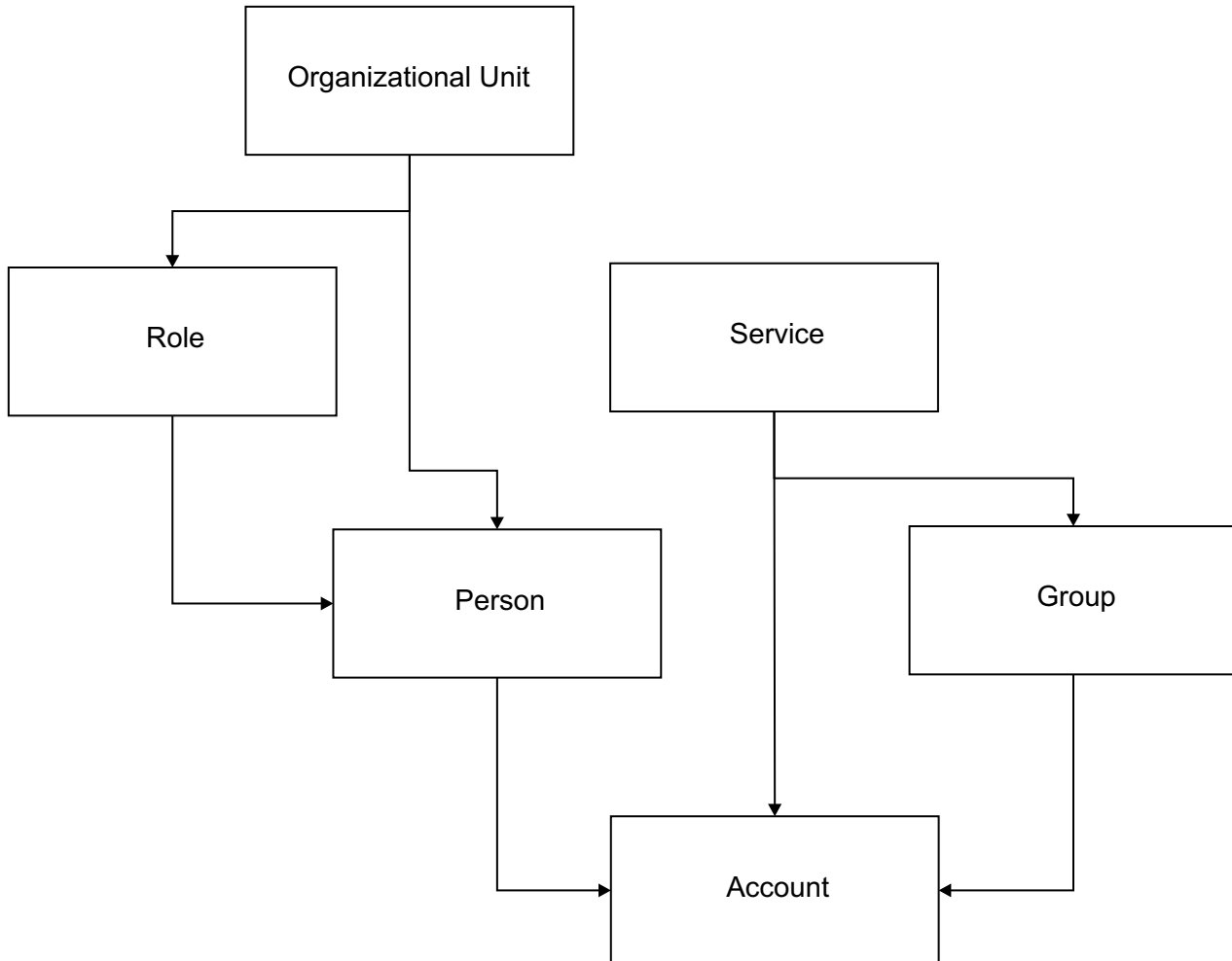


Figure 7. Entity dependency

### Procedure

1. Determine the types of entities that you want to load.
2. Run one or more of the entity assembly lines by issuing the appropriate commands from the command line. Because of entity dependencies, run the assembly lines one at a time. Do not run the next assembly line until the previous one finishes successfully.

#### Windows systems

```
startAL LoadOU  
startAL LoadRole  
startAL LoadService  
startAL LoadGroup  
startAL LoadPerson  
startAL LoadAccount
```

#### Linux systems

```
./startAL LoadOU
./startAL LoadRole
./startAL LoadService
./startAL LoadGroup
./startAL LoadPerson
./startAL LoadAccount
```

3. Check the status of the assembly line with the `showStat` command.  
`showStat`

## What to do next

After the entities are successfully loaded, run the **Delta** assembly line to start incremental data synchronization.

## Starting incremental data synchronization

After the initial full data load is completed, start the **Delta** assembly line to synchronize new data.

### Before you begin

Be sure that the IBM Tivoli Directory Integrator is running. See “Starting and stopping the IBM Tivoli Directory Integrator server” on page 30.

### About this task

Use the **Delta** assembly line to run an incremental data synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence.

### Procedure

1. Run the **Delta** assembly line from the command line with one of the following commands:

#### Windows systems

```
startAL Delta
```

#### Linux systems

```
./startAL Delta
```

2. To check the status of the assembly lines, use the **showStat** command.  
`showStat`

If any write operations to IBM Security Identity Governance and Intelligence fail during a **Load** or **Delta** operation, a repair record is captured in the repair list. The **Delta** operation periodically retries these items with a **Repair** operation.

If **Repair** is successful, the item is removed from the list. You can repeat the repair, while you work with issues that block the write operations. See “Repair list” on page 60 in the *Troubleshooting* section.

## Starting entitlement fulfillment synchronization

After the initial full load is complete, start the **ISIGtoISIM** assembly line to synchronize entitlement fulfillments from IBM Security Identity Governance and Intelligence to IBM Security Identity Manager

## Before you begin

Be sure that the IBM Tivoli Directory Integrator is running. See “Starting and stopping the IBM Tivoli Directory Integrator server” on page 30.

### Procedure

1. Run the **ISIGtoISIM** assembly line from the command line with one of the following commands: After the initial full load is completed, run the entitlement fulfillment synchronization process.

#### Windows systems

```
startAL ISIGtoISIM
```

#### Linux systems

```
./startAL ISIGtoISIM
```

2. To check the status of the assembly lines, use the **showStat** command.  

```
showStat
```

## Stopping incremental synchronization

The **Delta** assembly line runs continuously after it is started. If you need to stop incremental synchronization, you must stop the **Delta** and **DeltaSynch** assembly lines.

### Before you begin

Be sure that the IBM Tivoli Directory Integrator is running. See “Starting and stopping the IBM Tivoli Directory Integrator server” on page 30.

### About this task

To stop incremental synchronization, both the **Delta** and the **DeltaSynch** assembly lines must be stopped at the same time. If you stop the **DeltaSynch** assembly line only, the **Delta** assembly line restarts the **DeltaSynch** assembly line automatically. If you stop the **Delta** assembly line only, then the **DeltaSynch** assembly line still runs.

### Procedure

Use one of these methods to stop the incremental synchronization operations

- Run the following command:  

```
stopAL Delta,DeltaSynch
```
- Use the browser-based Dashboard in IBM Tivoli Directory Integrator. Stop the **Delta** assembly line. Then, stop the **DeltaSynch** assembly line.

## Stopping entitlement fulfillment synchronization operations

The **ISIGtoISIM** assembly line runs continuously after it is started. If you need to stop the fulfillment synchronization, you can either stop just the **ISIGtoISIM** or all the assembly lines.

### Before you begin

Be sure that the IBM Tivoli Directory Integrator is running. See “Starting and stopping the IBM Tivoli Directory Integrator server” on page 30.

## About this task

You must stop the assembly line to stop entitlement fulfillment synchronization.

## Procedure

Issue one of the following commands.

- Stop the **ISIGtoISIM** assembly line.  
`stopAL ISIGtoISIM`
- Stop all assembly lines.  
`stopAL all`

## Monitoring assembly lines

The **Load**, **Delta**, and **ISIGtoISIM** assembly lines display error messages in the console and write them to the log files. You can use the console to monitor the progress of operations.

You can use the IBM Tivoli Directory Integrator Dashboard to see that an assembly line is running. You can also use it to start or stop assembly lines. The Dashboard is a web application that starts when the Tivoli Directory Integrator server instance starts. For each server instance, the Dashboard runs on a port that is specified by the `web.server.port` property in your `solution.properties` file.

To access the Dashboard, enter the URL and port number of the Tivoli Directory Integrator server, followed by the path `/dashboard`.

The example that is shown in the following figure uses `my_tdi.mydomain.com` as the URL and the default port 1098:

`http://my_tdi.mydomain.com:1098/dashboard`

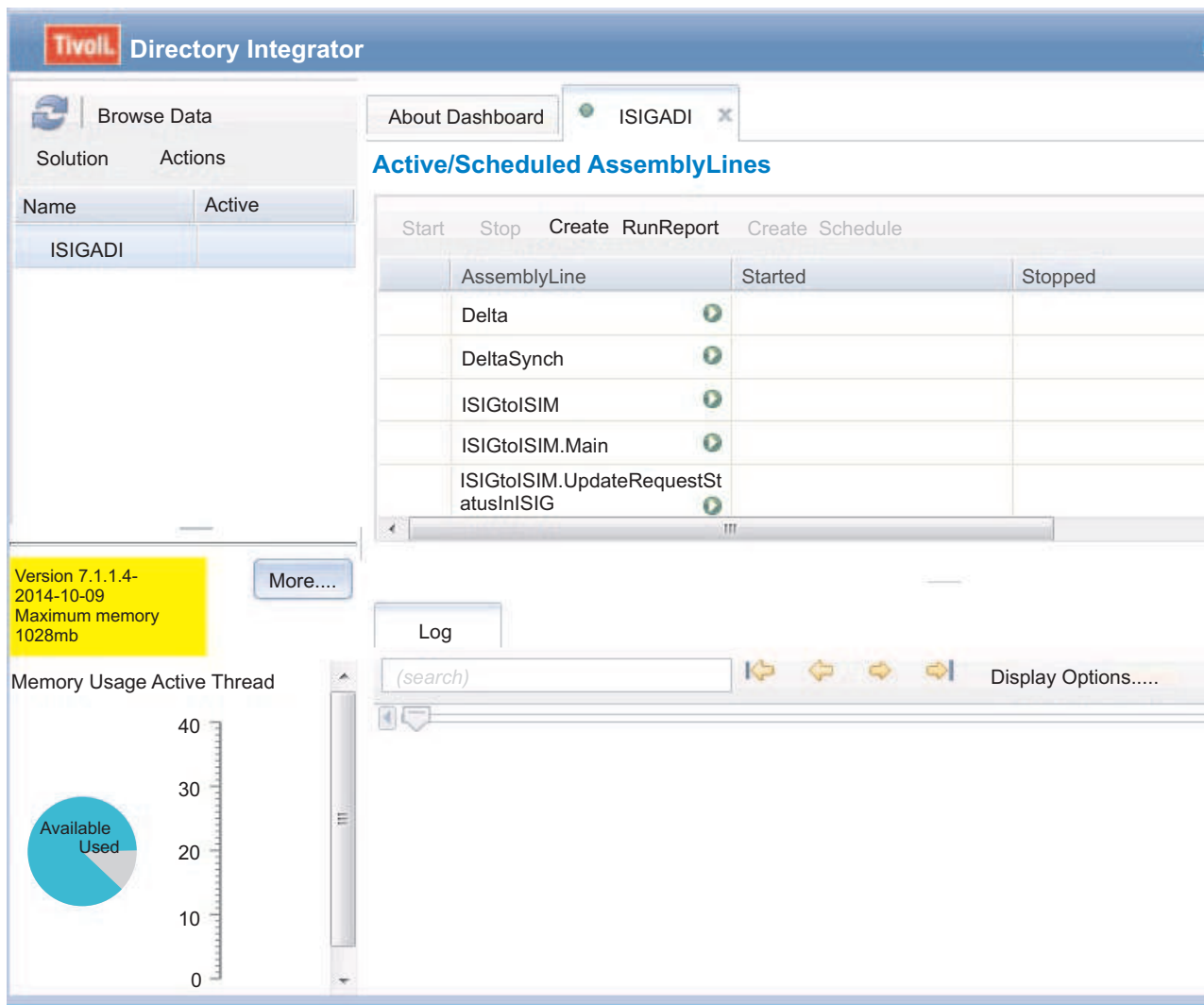


Figure 8. Tivoli Directory Integrator Dashboard

- To start or stop an AssemblyLine, select the AssemblyLine, then click **Start** or **Stop**.
- To view the log output of an AssemblyLine, select the AssemblyLine and view the **Log** tab.
- The highlighted text in the figure shows the current version of IBM Tivoli Directory Integrator and also the maximum memory size that the server can use. You must run IBM Tivoli Directory Integrator 7.1.1 with fix pack 4 or the latest fix pack. To increase the maximum memory size for the ITDI server, update the `TDI_INSTALL_DIR/ibmdisrv` script file to include the `-Xmx` flag. For example, to increase the maximum memory size to 2G, add `-Xmx2g` as shown in the following example.

```
%TDI_JAVA_PROGRAM% -Xmx2g -classpath "%TDI_HOME_DIR%\IDILoader.jar"
%ENV_VARIABLES% com.ibm.di.loader.ServerLauncher %*
```

---

## Data Integrator support for adapters

You can configure the Data Integrator to support extra IBM Security Identity Manager adapters.

POSIX adapters and LDAP adapters are supported by default.

### Manually customizing IBM Security Identity Manager Adapters

For Data Integrator version 7.0.4, you must manually customize support for more IBM Security Identity Manager adapters. Starting with Data Integrator version 7.0.5, adapters are supported automatically.

If you must customize your Data Integrator version to support adapters that use the complex group attribute, see also “Configuring adapters with complex group attributes” on page 38.

The Data Integrator supports IBM Security Identity Manager adapters by specifying the mapping of the group metadata in the `ATTRIBUTES.properties` file. POSIX adapters and LDAP adapters are supported by default. If other adapters are used, add more mapping properties.

**Note:** After you change properties files, you must restart the IBM Tivoli Directory Integrator server to put the changes into effect.

For each adapter, add the following properties:

```
class.$account_custom_class$.group=$group_membership_attr$
class.$group_custom_class$.description=$group_description_attr$
class.$group_custom_class$.name=$group_name_attr$
class.$account_custom_class$.groupitem.name=$group_id_attr$
accountprofile.$service_profile_name$=$account_profile_name$
```

The parameters in the properties have the following definitions:

**\$account\_custom\_class\$**

The account custom class for the adapter that is defined in the account profile.

**\$group\_custom\_class\$**

The group custom class for the adapter that is defined in the group profile.

**\$group\_membership\_attr\$**

The account attribute for the group membership.

**\$group\_name\_attr\$**

The name attribute that is defined in the group profile.

**\$group\_description\_attr\$**

The description attribute that is defined in the group profile.

**\$group\_id\_attr\$**

The ID attribute that is defined in the group profile.

**\$service\_profile\_name\$**

The name of the service profile. The **erobjectprofilename** of the service profile.

**\$account\_profile\_name\$**

The name of the account profile. The **erobjectprofilename** of the account profile.

## Example of Posix Linux adapter mappings

```
class.erPosixLinuxAccount.group=erPosixSecondGroup
class.erPosixLinuxGroup.description=erGroupDescription
class.erPosixLinuxGroup.name=erPosixGroupName
class.erPosixLinuxAccount.groupitem.name=erPosixGroupName
accountprofile.PosixLinuxProfile=PosixLinuxAccount
```

## Example of LDAP adapter mappings

```
class.erLDAPUserAccount.group=erldapgroupname
class.erLDAPGroupAccount.description=erLdapGroupDescription
class.erLdapGroupAccount.name=erLdapServiceGroup
class.erLDAPUserAccount.groupitem.name=erLdapGroupRDN
accountprofile.LdapProfile=LdapAccount
```

## Example of Active Directory adapter mappings

```
class.erADAccount.group=ergroup
class.erADGroup.description=erADGroupDescription
class.erADGroup.name=erADGroupDN
class.erADAccount.groupitem.name=erADGroupDN
accountprofile.ADprofile=ADAccount
```

## Configuring adapters with complex group attributes

The Data Integrator requires more configuration to support IBM Security Identity Manager adapters with complex group attributes, such as the Oracle eBS adapter.

### Before you begin

Starting with Data Integrator version 7.0.5, you must copy the handler .jar files, step 1, only. You no longer need to update the `ATTRIBUTE.properties` file, step 2.

You must have the following software:

- Supported version of IBM Security Identity Manager.
  - Version 6 fix pack 10 (6.0.0.10) or a later fix pack
  - Version 7.0.1 virtual appliance or a later fix pack.
- Adapter package that provides a complex attribute handler for complex groups. The following Oracle eBS adapter packages are listed as an example of an adapter with the complex attribute handler.

Extract the contents.

- IBM Security Identity Manager 6 Oracle eBusiness Suite adapter, version 6.0.10
- IBM Security Identity Manager 7 Oracle eBusiness Suite adapter, version 7.0.10

### About this task

Copy the handler .jar file from the extracted adapter package and place it where IBM Tivoli Directory Integrator can parse the complex attributes.

Starting with Data Integrator version 7.0.5, you must copy the handler .jar files, step 1, only. You no longer need to update the `ATTRIBUTE.properties` file, step 2.

### Procedure

1. Copy the handler JAR file from the adapter package to `TDI_HOME/jars/3rdparty/IBM/ISIGADI`.

The handler JAR files use the following naming convention:

<AdapterType>Handler.jar

For example, the handler file for Oracle eBS has the following name:

OraEBSHandler.jar

2. If you are using Data Integrator version 7.0.4, update the properties file *ISIGADI\_SOL\_DIR/ISIGADI/ATTRIBUTES.properties*.
  - a. Update the mandatory properties for all adapters. See “Manually customizing IBM Security Identity Manager Adapters” on page 37.
  - b. Update the following extra properties.
    - complexAttrHandler.<attributename>=<complex\_attribute\_handler>

<attributename>

Is the account attribute that contains the complex group value.  
Use all lowercase letters.

<complex\_attribute\_handler>

Is a class name. The class is defined in the erattributehandler attribute of a service profile.

- account.group.complexAttributes=<complex\_attribute\_list>

<complex\_attribute\_list>

Use a comma-separated list of attributes. The attributes are defined in the ercomplexattributes attribute of a service profile.

The following properties settings are an example for the Oracle eBS adapter.

```
class.erOraEBSRespAccount.name=erOraEBSResp
class.erOraEBSRespAccount.description=erGroupDescription
class.erOraEBSAccount.group=erOraEBSResp
class.erOraEBSAccount.groupitem.name=erOraEBSResp
accountprofile.OraEBSProfile=OraEBSAccount
complexAttrHandler.eroraebresp=
    com.ibm.isim.util.complexattribute.OraEBSComplexAttributeHandler
account.group.complexAttributes=erOraEBSResp
```

---

## Customization

You can customize the attribute mapping between IBM Security Identity Manager and IBM Security Identity Governance and Intelligence.

### Person attribute mapping

The Data Integrator can extend **person** attribute synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence.

You cannot change any of the attributes on the Identity Governance and Intelligence **Manage > Users > Details** tab that are already synchronized from Security Identity Manager. However, you can add more attributes for synchronization if they are defined in the Data section.

Attribute mapping is defined in the *ISIGADI\_SOL\_DIR/ISIGADI/AttrMapPerson.map* file. The ready to use mappings are compatible with earlier versions. You can modify only some of these mappings.

Do not modify the following set of mapping because the Data Integrator provides special logic to obtain the attribute values. The left side of the mapping definition represents the target Identity Governance and Intelligence **person** attribute. The right side is a derived value from a Security Identity Manager **Person** attribute. The right side, the source of the mapping, is prefixed with *work*, it represents the runtime value from the assembly line.

```
code=work.isigUserCode
dn=work.$dn
orgUnitCode=work.isigUserOrgUnitCode
orgUnitId=work.isigUserOrgUnitId
roleIds=work.isigUserRoleIds
optional.Manager=work.isigUserOptionalManagerUid
```

The mappings that use the variable `work.isig<nnnn>` are handled in the Data Integrator to ensure that the required Identity Governance and Intelligence attributes are not null. For example, the **Master UID** is mapped to the **work.isigUserCode** variable. This variable value is obtained from the Security Identity Manager preferred **uid** for all custom **person** classes that are inherited from **InetOrgPerson**. For other custom **person** classes, the **uid** attribute is not present. The Data Integrator looks up the Security Identity Manager system user account and attempts to use the same **uid**. If the ready to use automatic creation of a Security Identity Manager account is disabled, the **erglobalid** attribute of the Security Identity Manager **person** object is used.

You can modify the following set of mapping. These attributes are not required Identity Governance and Intelligence attributes. The attributes without the `optional.` prefix are in Identity Governance and Intelligence **User > Details > Details** section. The attributes with the `optional.` prefix are in the **User > Details > Data** section if they are defined in **Settings > Core Configurations > User Virtual Attributes > UserErc > Attribute Mapping**.

```
email=work.mail
lastName=work.sn
name=work.givenName||''
optional.ATTR10=work.ersponsor||work.manager
optional.ATTR5=work.initials
optional.ATTR8=work.roomNumber
```

**Note:** When you modify or add new attribute mapping definitions, both the target and source attribute names are case-sensitive.

To synchronize **Phone Number** to the Identity Governance and Intelligence User data **ATTR10**, map to the LDAP source attribute name of the **person** object.

```
optional.ATTR10=work.telephonenumber
```

Where

#### **ATTR10**

Is the exact label of the Identity Governance and Intelligence User Attribute Mapping.

#### **telephonenumber**

Is the exact attribute name that is stored in the Security Identity Manager **person** object.

You can add an attribute mapping in a similar way. If you want to synchronize a Security Identity Manager custom person with attribute **erteamid** to the **ATTR11** attribute in the **USER\_ERC** table, the mapping definition is:

```
optional.ATTR11=work.erteamid
```

This feature uses the external mapping capability of the Tivoli Directory Integrator, the right side is always interpreted as java script. If you have multiple custom person schemas in Security Identity Manager, the team ID might come from a different attribute in a different schema. You can define complex JavaScript mapping to extract and compose target value as applicable to your environment.

- If you have a custom person schema in Security Identity Manager that has the **erteamid** attribute and another **person** class has the **projectcode** attribute, the mapping is:  
`optional.ATTR11=work.erteamid || work.projectcode`
- You can concatenate several attributes in Security Identity Manager schema from the same object class to map to a single attribute in Identity Governance and Intelligence. If you have a custom person schema in Security Identity Manager that has **erdivision**, **erdepartment** and **erteamid** attributes, the mapping is:  
`optional.ATTR11=work.erdivision+'-'+work.erdepartment+'-'+work.erteamid`

## Account attribute mapping

The Data Integrator can override **account** attribute synchronization from IBM Security Identity Manager to IBM Security Identity Governance and Intelligence.

The attribute mapping for the **Account** attribute is defined in the `ISIGADI_SOL_DIR/ISIGADI/AttrMapAccount.map`. From the Identity Governance and Intelligence user interface, you can view the account attribute values **Manage > Users > Accounts > Select an account > Actions..** Select the **Details** menu item.

The left side of the mapping definition represents the Identity Governance and Intelligence account attribute. The right side is a derived value from a Security Identity Manager **Account** attribute.

Do not change any of the following mappings. The Data Integrator uses these variables to ensure the correct integration of Security Identity Manager with Identity Governance and Intelligence.

```
accountStatus=work.isigAccountStatus
applicationId=work.isigAccountApplicationId
groupId=work.isigAccountGroupIds
password=work.isigAccountPassword
uid=work.isigAccountUsername
userId=work.isigAccountOwnerId
ldapAccountObjectClass=work.ldapAccountObjectClass
complexGroups=work.complexGroups
attributePermissions=work.attributePermissions
serviceErGlobalId=work.serviceErGlobalId
```

These mappings are required by the Data Integrator. For example, the **accountStatus** is derived from the Security Identity Manager **Account** status attribute to ensure the integrity of the business logic. Similarly, the **applicationID** is mapped to **work.isigAccountApplicationId** because the Data Integrator obtains this value from Identity Governance and Intelligence. It is not a direct mapping from the Security Identity Manager **Account** attribute.

You can modify the following set of mapping. These attributes are not required Identity Governance and Intelligence attributes. Unlike person mapping, the target account in Identity Governance and Intelligence does not have extended attributes. See “Person attribute mapping” on page 39. The following list is fixed, and you cannot add extra attributes to be synchronized to Identity Governance and Intelligence. However, you can change the source attribute mapping definition to include adapter-specific attributes. For example, in the following list, the Identity Governance and Intelligence **expire account** attribute is obtained from the **eradexpirationdate**, **erntexpirationdate**, or **erposixexpireddate** attributes. The value is taken from whichever attribute is not null in the order of evaluation. During run time, a Security Identity Manager posix account object does not have the **eradexpirationdate** attribute nor the **erntexpirationdate** attribute. If the

**eradexpirationdate** attribute is not null, that value is synchronized to Identity Governance and Intelligence account expiry date.

Identity Governance and Intelligence target account has four attributes for the Date type:

- **expire**
- **lastChangePwd**
- **lastWrongLogin**
- **lastlogin**

You can define the date attribute mapping and the date attribute format for these attributes. These definitions identify the input date format to the Data Integrator. For each Security Identity Manager account type, you can define a variable `<objectClassName>_<attributeName>_format` to override the default format. The default format is the Zulu format `yyyyMMddHHmmZ`. For example, you want the format to use `ddMMyy:HHmmss` instead of the default for the **lastlogin** attribute. To override the **lastlogin** date input format for posix account type, add the mapping `erposixaccount_lastlogin_format='ddMMyy:HHmmss'`.

**Note:** The attribute name from LDAP is case-sensitive. Use the exact same case as the attribute name in the LDAP server object entry.

```
expire=work.eradexpirationdate||work.erntexpirationdate||work.erposixexpireddate
erposixaixaccount_expire_format='yyyyMMddHHmm\ 'Z\ '
email=work.mail
name=work.givenname
surname=work.sn
displayname=work.cn
numberLoginError{!}=
lastChangePwd=work.erswdlastchanged
lastWrongLogin{!}=
lastlogin{!}=
identityUID{!}=
```

The `{!}` next to the variable name indicates to the Data Integrator to skip the attribute.

## Non-group permission support

Attribute-to-Permission mapping treats the non-group attribute of an account as group attribute or permission.

With Attribute-to-Permission mapping, you can specify which account attribute can be mapped to which permission. You can also specify the **allowed** attribute values and the **right** values in this mapping. For more detail about the Attribute-to-Permission Mapping, see the IBM Knowledge Center.

Attribute-to-Permission mapping is defined for an account configuration that is created by the Data Integrator. When the account is loaded or updated, the mapped attribute is treated as group attribute on Identity Governance and Intelligence. If the account has the value that is specified on this mapped attribute, the **permission** and their **right** are assigned to the user as they are specified in the Attribute-to-Permission mapping.

Data Integrator uses the Identity Governance and Intelligence RESTful service API to retrieve the Attribute-to-Permission mapping from Identity Governance and

Intelligence. You must enable this feature in the `ISIG.properties` file. After it is enabled, the **Verify** assembly line tests the connection to the Identity Governance and Intelligence RESTful service.

## Prerequisites

- Install Identity Governance and Intelligence version 5.2.2 or later.
- Define the Identity Governance and Intelligence Attribute-to-Permission mapping for the account configuration that is created by the Data Integrator.
- Update the `ISIG.properties` file.

### **igi.nonGroup.attributeToPermissionMappingEnabled=true**

Enable this property to use the **non-group-permission** attribute.

### **igi.restService.base=https://igi522\_host:9343/rest**

Specify the correct host name for Identity Governance and Intelligence server. The Data Integrator uses this base URL to call the Identity Governance and Intelligence RESTful APIs to retrieve the Attribute-to-Permission mapping.

- Import the Identity Governance and Intelligence server certificate. Point your browser to the URL `https://igi522_host:9343`. See “Importing the server certificate to the Tivoli Directory Integrator client keystore” on page 49.

## Examples

After the **WinLocal** service is ported from IBM Security Identity Manager to Identity Governance and Intelligence, you can configure the Attribute-to-Permission mapping for the **WinLocal** account configuration.

Table 6. WinLocal attribute-to-permission mapping

Attribute name	Permission name	Type	Attribute value	Right value
<b>erntusercountrycode</b>	<b>erntusercountrycodeP</b>	String	1	1RV
			2	2RV

Table 7. WinLocal attribute permission values

Attribute name	Permission name	Type	Value if user has this permission	Value if user does not have this permission
<b>erntpasswordneverexpires</b>	<b>erntpasswordneverexpiresP</b>	Boolean	True	False

After you create the Attribute-to-Permission mapping, the permissions and rights are assigned to Identity Governance and Intelligence, when it loads the account.

The following table shows how these account attribute values are interpreted to Identity Governance and Intelligence by the **Load** and **Delta** assembly lines.

Table 8. Account values for the **Load** and **Delta** assembly lines

Account attribute values on IBM Security Identity Manager	Load Delta	On Identity Governance and Intelligence, the user who has this account has these permissions	On Identity Governance and Intelligence, the user who has this account has these right values
<b>erntusercountycode: 1</b> <b>erntpasswordneverexpires: true</b>	→	<b>erntusercountycodeP</b> <b>erntpasswordneverexpiresP</b>	1RV under <b>erntusercountycodeP</b> permission
<b>erntusercountycode: 2</b> <b>erntpasswordneverexpires: false</b>	→	<b>erntusercountycodeP</b>	2RV under <b>erntusercountycodeP</b> permission
<b>erntusercountycode: 3</b>	→	<b>erntusercountycodeP</b>	3 under <b>erntusercountycodeP</b> permission

If the attribute type is defined as boolean in the Attribute-to-Permission mapping, the permission is assigned only if the attribute value has the value that is specified in **Value if user has this permission** field.

Similarly, when the **ISIGtoISIM** assembly line processes non-group permission events, the reverse applies. For example, adding rights results in the addition of the corresponding attribute value that is defined in the attribute-to-permission mapping. Removing rights results in the removal of the corresponding attribute value. Adding a permission to a boolean type non-group permission sets the corresponding attribute value to either TRUE or FALSE according to the attribute-to-permission mapping.

Table 9. Operations for the **ISIGtoISIM** assembly line

Operation on Identity Governance and Intelligence	The user account on Identity Governance and Intelligence	Operation on IBM Security Identity Manager
Add right	1RV under <b>erntusercountycodeP</b>	Account Modify that adds the attribute value 1 to <b>erntusercountycode</b> on the account.
Remove right	1RV under <b>erntusercountycodeP</b>	Account Modify that removes the attribute value 1 from <b>erntusercountycode</b> on the account.
Add permission	<b>erntusercountycodeP</b>	The event is ignored because no value is associated with this event.
Remove permission	<b>erntusercountycodeP</b>	Account Modify that removes the attribute <b>erntusercountycode</b> from the account.
Add permission	<b>erntpasswordneverexpiresP</b>	Account Modify that adds the attribute value <b>erntpasswordneverexpires=true</b> to the account.
Remove permission	<b>erntpasswordneverexpiresP</b>	Account Modify that adds the attribute value <b>erntpasswordneverexpires=false</b> to the account.

## LoadAccountNGP assembly line

The **LoadAccountNGP** assembly line loads the accounts with attribute values that are defined for the attributes that are mapped to the permission. You can run this assembly line after the Attribute-to-Permission mapping is either created or updated.

If the attribute mapping is removed from IBM Security Identity Governance and Intelligence, accounts that were previously loaded because they had a defined value for that attribute are not loaded by the **LoadAccountNGP** assembly line.

## Discovering account attributes from the target

After the service is ported to IBM Security Identity Governance and Intelligence, you can use the **Discover Account Attributes from Target** feature to browse the account attribute list. Then, select the attributes to create the Attribute-to-Permission mapping.

### Before you begin

- All the prerequisites from Non-Group Permission Support must be fulfilled.
- From Identity Governance and Intelligence administration console, import the target profile JAR file. Click **Target Administration > Manage Target Type > Import Target Type**.

### About this task

For information about the **Discover Account Attributes from Target** feature, see [https://www.ibm.com/support/knowledgecenter/SSGHJR\\_5.2.2/com.ibm.igi.doc/administering/tsk/tsk\\_ac\\_mapping\\_attris\\_permissions\\_discovery.html](https://www.ibm.com/support/knowledgecenter/SSGHJR_5.2.2/com.ibm.igi.doc/administering/tsk/tsk_ac_mapping_attris_permissions_discovery.html)

To use the **Discover Account Attributes from Target** feature for the service that is ported from IBM Security Identity Manager, do the following steps.

### Procedure

1. Run either the **Load** or **LoadService** assembly line to load the service from IBM Security Identity Manager to Identity Governance and Intelligence. For example, you have a WinLocal service that is called **WinLocal-Service** on IBM Security Identity Manager that you port to Identity Governance and Intelligence.
2. Import the target profile JAR file. On the Identity Governance and Intelligence administration console, click **Target Administration > Manage Target Type > Import Target Type**. For example, use the **Browse** function to select and import the WinlocalProfile.jar file.
3. To use the **Discover Account Attributes from Target** feature, go to the Identity Governance and Intelligence Home page.
  - a. Click **Access Governance Core > Accounts**.
  - b. Select an account configuration.
  - c. Click **Attribute-to-Permission Mapping**.
  - d. Click **Actions** and select **Discover Account attributes from Target**.

The attributes on the target for the account are displayed.

## Complex RACF group right support

You can manage the **erracconxml** complex group's subattributes on the IBM Security Identity Manager RACF subform on IBM Security Identity Governance and Intelligence as permission rights.

Each subattribute in the RACF connect group (**erracconxm1**) is treated as permission rights in IGI. When RACF groups are loaded, the rights that are associated with the permissions are created along with the rights' value lookup. Then, during account load, users are assigned the rights in Identity Governance and Intelligence according to the subattributes values within the account's attribute value.

## Prerequisites

- Install the RACF Complex Group Handler on a version of IBM Security Identity Manager. See the prerequisites section of “Configuring adapters with complex group attributes” on page 38 for the supported versions.
- Identity Governance and Intelligence 5.2.2 or later version is required. The right's canonical values are obtained from Identity Broker that is only available in Identity Governance and Intelligence 5.2.2.
- On Identity Governance and Intelligence 5.2.2, the `racf2profile.jar` file that supported schema discovery must be imported before the Load assembly line is run.
- On Identity Governance and Intelligence 5.2.2, the **IB\_API** feature must be enabled. See Enabling or disabling the Identity Brokerage REST API to enable the Identity Brokerage **IB\_API**.
- On Identity Governance and Intelligence 5.2.2, an API user must be created. See Managing Identity Brokerage users and passwords to create Identity Brokerage REST user and password.
- Update the `ISIG.properties` file.

**`igi.complexGroup.rightSupportEnabled=true`**

Set this property to true to enable RACF complex group permission rights.

**`igi.ib.rest.user=username`**

Set this property to the Identity Brokerage REST user that you created.

**`igi.ib.rest.password=password`**

Set this property to the Identity Brokerage REST user password that you assigned to the user.

**`igi.ib.rest.URL=https://igi522_host:8443/BrokerageService/identity/`**

Set the correct Identity Governance and Intelligence 5.2.2 server URL and Identity Broker's RESTful service port number. By default, it listens on port 8443.

- Import the Identity Governance and Intelligence server certificate by using the browser with the URL `https://igi522_host:8443`. See “Importing the server certificate to the Tivoli Directory Integrator client keystore” on page 49.

## Example

After the RACF groups are loaded, the rights that are associated with each group are also defined. Click **Access Governance Core > Manage > Applications > Application Access > Rights**. The allowed values for each right are obtained from the rights lookup tables that are created during the load. Click **Configure > Rights Lookup**.

The values in the **Rights Lookup** table are called canonical values for the rights that are obtained from Identity Brokerage service. Canonical values are not defined for some subattributes in the RACF connect group, for example, **owner**. Rights are not supported on these attributes.

During the account load, the Data Integrator assigns rights to the user based on the subattributes values in the RACF Connect group. These user rights can be managed in Identity Governance and Intelligence by assigning or removing user rights. When a right is removed, the IBM Security Identity Manager account attribute reflects the changes after the **ISIGtoISIM** assembly line picks up the changes. The subattribute is added or removed from **erraconxml** attribute in the account object.

## Support for IBM Security Identity Manager when justification is required

On IBM Security Identity Manager version 6 or 7, justification is required when the IBM Security Identity Manager WebService APIs are called if the **enrole.jutificationRequired** property in **enRole.properties** file is set to true.

The Data Integrator supports justification with the **isim.jutificationRequired.enabled** property that is added in the **ISIM.properties** file. Enable this property if IBM Security Identity Manager version 6 or 7 requires justification. It sends the justification **Requested by ISIGADI** as a parameter to WebService API.

### Requirements

In the following fixes, the WebService API can take the justification as an optional parameter.

**For IBM Security Identity Manager version 6**  
6.0.0-ISS-SIM-FP0014 or later fix pack.

**For IBM Security Identity Manager version 7**  
7.0.1.3-ISS-SIM-IF0002 or later fix pack.

## Customizing Organizational Unit Mapping

You can customize the Data Integrator so that the existing IBM Security Identity Governance and Intelligence organizational unit can be assigned to a person when a person is synchronized from IBM Security Identity Manager.

### About this task

To enable the **OU** mapping, you must set three properties in the **ISIGADI\_SOL\_DIR/ISIGADI/ISIG.properties** file.

### Procedure

1. Set the **isim.skipOUSynch** property to true to skip all the organization unit synchronization from Security Identity Manager to Identity Governance and Intelligence. If this property is set to true, you must set the **isim.person.ouAttribute** and **isim.defaultOU.IDCode** properties. Use all lower case letters such as true or false. The default value is set to false.
2. Set the **isim.person.ouAttribute** property to one or more than one of the person attributes on Security Identity Manager.  
Use a comma as a separator to specify multiple attributes to support the multiple person types. For example, if you want to use the **roomnumber** attribute for **Person** and the **ou** attribute for **BPPerson**, set this property as **isim.person.ouAttribute=roomnumber,ou**. The Data Integrator uses the first

attribute value that is not null. If the person has a value for both **roomnumber** and **ou** attributes, the value for **roomnumber** is used because it is specified first in the list.

- The value of this person attribute must have the **ID Code** of the organizational unit on Identity Governance and Intelligence.
  - This **ID Code** maps the Security Identity Manager person to the Identity Governance and Intelligence **OU**.
  - This property is only used if the **isim.skipOUSynch** property is set to true.
  - The value is case-sensitive.
  - The default value is not set.
3. Set the **isim.defaultOU.IDCode** property to the ID code of default organizational unit on Identity Governance and Intelligence.
    - This **OU** value is used as a default **OU** if the **ouAttribute** of a person is invalid.
    - The value of this property must have the valid **ID Code** of the organizational unit on Identity Governance and Intelligence. If it has an invalid value, then **Load** and **Delta** assembly lines fail with a FATAL error.
    - This property is only used if the **isim.skipOUSynch** property is set to true.
    - The value is case-sensitive.
    - The default value is not set.
  4. After you enable custom organizational unit mapping, run the **Load** assembly line.

## Results

- When a person is synchronized from Security Identity Manager to Identity Governance and Intelligence, the roles of this person are associated with the **OU** of this person.
- When an account is synchronized from Security Identity Manager to Identity Governance and Intelligence, the permissions of this account are associated with the **OU** of the account owner.
- When a person is transferred from one organizational unit to another organizational unit, all the roles and groups of this person are associated with the new organizational unit.

## Supporting the PostgreSQL database

IBM Security Identity Governance and Intelligence version 5.2.2 supports the PostgreSQL database. If Identity Governance and Intelligence is configured to use the PostgreSQL server, perform these steps to enable the Data Integrator to connect to the PostgreSQL server.

### Procedure

1. Download the JDBC driver for PostgreSQL server.
  - a. Go to <https://jdbc.postgresql.org/download.html>.
  - b. Download the JDBC 42 version of latest driver.
2. Copy the JDBC driver JAR file to *TDI\_HOME/jars/3rdparty/others* directory.
3. Update the *ISIG.properties* file with the PostgreSQL server information.

#### **isig.db.user**

The default user is *iga\_core*.

#### **isig.db.password**

The default password for *iga\_core* is *ideas*.

**isig.db.schema**

The default schema name is iga\_core.

**isig.db.url**

The url is jdbc:postgresql://igi522\_host:5432/igidb.

**isig.db.driver**

The driver is org.postgresql.Driver.

4. Restart the Tivoli Directory Integrator.
5. Run the **Verify** assembly line to verify that the connection to the Identity Governance and Intelligence database is successful. See “Verifying the configuration” on page 28. If the connection to the Identity Governance and Intelligence is correct, you receive the following message.  
 Connection is tested successfully to IGI Database: PostgreSQL  
 Similarly, if Identity Governance and Intelligence is configured with a DB2 or an Oracle database, you receive the following messages.  
 Connection is tested successfully to IGI Database: DB2  
 Connection is tested successfully to IGI Database: Oracle

---

## Reference

Use the reference information to identify the files that are installed with IBM Security Identity Governance and Administration Data Integrator and to understand the properties that they contain.

## Importing the server certificate to the Tivoli Directory Integrator client keystore

To access the RESTful API that run on the Identity Governance and Intelligence system, you must import the Identity Governance and Intelligence server certificate to the Tivoli Directory Integrator keystore file.

### Procedure

1. Export the Identity Governance and Intelligence server certificate to a file. Open the Firefox browser and put in your Identity Governance and Intelligence URL such as https://jsigi522ai.rtp.raleigh.ibm.com:9343. If you are accessing this URL for the first time, then Firefox prompts a security warning. If this warning is not shown, you already imported the certificate to the browser. Skip to the next step.
  - a. On the Your connection is not secure page, click **Add Exception...**
  - b. On the Add Security Exception window, click **Get Certificate** and then click **View**.
  - c. On the Certificate Viewer window, click **Details** and then click **Export**.
  - d. Rename the file and save as file type X.509 Certificate (PEM) (\*.crt, \*.pem). For example, save the file as C:\temp\igiServer.crt.
2. Export the Identity Governance and Intelligence server certificate from the Firefox Certificate Manager.
  - a. On the Firefox tool bar, click **Tools > Options > Advanced > Certificate > View Certificate**.
  - b. In the Certificate Manager window, click **Servers**. Locate and select the Identity Governance and Intelligence server certificate. Then, click **Export**.
  - c. Rename the file and save as file type X.509 Certificate (PEM) (\*.crt, \*.pem). For example, save the file as C:\temp\igiServer.crt.

3. Find the client keystore file. The location of the client keystore file is specified in the `solution.properties` file.
  - a. Go to your solution directory and open the `solution.properties` file.
  - b. Look for the **`javax.net.ssl.keyStore`** property. By default, it is set to `SOL_DIR/serverapi/testadmin.jks`. The password is `administrator`. Remember this password because you need this password when you import the Identity Governance and Intelligence server certificate to the keystore file.
4. Import the Identity Governance and Intelligence server certificate file to the Tivoli Directory Integrator keystore file.
  - a. Start the IBM Key Management tool. Go to the `TDI_HOME/jvm/jre/bin/` directory and run the **`ikeyman.exe`** command.
  - b. Open the Tivoli Directory Integrator client keystore file that you found in the previous step. The default file is `SOL_DIR/serverapi/testadmin.jks`.
  - c. Enter the password `administrator`.
  - d. Select **Signer Certificates** from the drop-down menu.
  - e. Click **Add....**
  - f. Click **Browse** to select the certificate and click **OK**.
  - g. Close the IBM Key Management tool.
5. Restart the Tivoli Directory Integrator server. If you had the Tivoli Directory Integrator **Config Editor** tool open, restart that as well.

## Configuration property files

Set property attributes and encrypt properties before you run IBM Security Identity Governance and Administration Data Integrator operations.

Set and encrypt properties in the following files. A table is shown for each to list its properties.

### **DBMAP.properties**

Contains properties for the Data Integrator database. See the following *Properties in DBMAP.properties* table.

### **ISIG.properties**

Contains properties for the Identity Governance server, Identity Governance database, and IBM Security Identity Manager LDAP directory server. See the following *Properties in ISIG.properties* table.

### **ISIM.properties**

Contains properties for the Security Identity Manager server. See the following *Properties in ISIM.properties* table.

**Note:** The IBM Tivoli Directory Integrator server relies on Data Integrator properties settings. If you change the properties files after you started the IBM Tivoli Directory Integrator server, you must restart it for the changes to take effect.

Table 10. *Properties in DBMAP.properties*

Property name	Description	Example
<b>db.driver</b>	JDBC driver class to use.	For DB2, <b><code>com.ibm.db2.jcc.DB2Driver</code></b>  For Oracle, <b><code>oracle.jdbc.OracleDriver</code></b>

Table 10. Properties in DBMAP.properties (continued)

Property name	Description	Example
<b>db.url</b>	JDBC URL for the Data Integrator system database. For DB2, use the IP address of the DB2 server as the local host, and the default port is 50000. For Oracle, the default port is 1521.	For DB2, <b>jdbc:db2://localhost:50000/idiadb</b>  For Oracle, <b>jdbc:oracle:thin:@localhost:1521:idiadb</b>
<b>db.user</b>	User name for the Data Integrator to use to access this database.	<b>idiuser</b>
<b>db.password</b>	Password for <b>db2.user</b> .	
<b>db.schema</b>	Database schema name that you specified for the database.	<b>idiuser</b>

Table 11. Properties in ISIG.properties

Property name	Description	Example
<b>igi.complexGroup.rightSupportEnabled</b>	Set the property to true to enable RACF complex group permission rights. Set the property to false to disable RACF complex group permission rights.	<b>igi.complexGroup.rightSupportEnabled=true</b>
<b>igi.ib.rest.user</b>	Specifies the Identity Brokerage REST user ID.	<b>igi.ib.rest.user=username</b>
<b>igi.ib.rest.password</b>	Specifies the password for the Identity Brokerage REST user	<b>igi.ib.rest.password=password</b>
<b>igi.ib.rest.URL</b>	Specify the URL to IBM Security Identity Governance and Intelligence and the Identity Broker RESTful service port.	<b>igi.ib.rest.URL=https://igi522_host:8443/BrokerageService/identity/</b>
<b>isig.url</b>	Specify the URL to IBM Security Identity Governance and Intelligence server in the following format. <b>iiop://isighostname:2821</b>  <b>ISIG_HOST_NAME</b> is the host name of the IBM Security Identity Governance and Intelligence.	<b>iiop://isig.mydomain.com:2821</b> <b>Note:</b> For an SSL connection you must use port 28210.  <b>iiop://isig.mydomain.com:28210</b>  You must also set the <b>com.ibm.CSI.performTransportAssocSSLTLSSupported</b> property in the <b>ISIGADI_SOL_DIR/ISIGADI/secConfig_isig511/sas.client.props</b> file to true.  <b>com.ibm.CSI.performTransportAssocSSLTLSSupported=true</b>
<b>isig.user</b>	IBM Security Identity Governance and Intelligence administrator user.	<b>admin</b>
<b>isig.password</b>	IBM Security Identity Governance and Intelligence administrator password.	<b>admin</b>

Table 11. Properties in *ISIG.properties* (continued)

Property name	Description	Example
<b>isig.realm</b>	Realm for this Data Integrator instance.	<b>Ideas</b>
<b>isig.rootorg.id</b>	ID for the root organization in IBM Security Identity Governance and Intelligence where the IBM Security Identity Manager organization structure is added. Default is root.	<b>root</b>
<b>isig.rootorg.name</b>	Name for the root organization in IBM Security Identity Governance and Intelligence to which the IBM Security Identity Manager organization structure is added. Default is ACME Corp.	<b>ACME Corp.</b>
<b>isig.db.user</b>	Database user for the IBM Security Identity Governance and Intelligence database. The default settings are in the examples.	For DB2, <b>IGACORE</b> For Oracle, <b>IGA_CORE</b> For PostgreSQL, <b>iga_core</b>
<b>isig.db.password</b>	Password for <b>isig.db.user</b> .	<b>ideas</b>
<b>isig.db.schema</b>	Specify the database schema for the IBM Security Identity Governance and Intelligence database. The default settings are in the examples.	For DB2, <b>IGACORE</b> For Oracle, <b>IGA_CORE</b> For PostgreSQL, <b>iga_core</b>
<b>isig.db.url</b>	Specify the database URL for the IBM Security Identity Governance and Intelligence database.  The example uses the following values:  <b>isig.myco.com</b> The Oracle database host.  <b>1521</b> The Oracle database port.  <b>xe</b> The Oracle database SID.	For DB2, <b>jdbc:db2//hostIP:50002/dbName</b>  For Oracle, <b>jdbc:oracle:thin:@isig.myco.com:1521:xe</b>  For PostgreSQL <b>jdbc:postgresql://igi522_host:5432/igidb</b>

Table 11. Properties in *ISIG.properties* (continued)

Property name	Description	Example
<b>isig.ISIGtoISIM.max.limit</b>	Maximum number of entries that are processed per iteration of <b>ISIGtoISIM</b> . The default is 100 entries.	<b>isig.ISIGtoISIM.max.limit=FETCH FIRST 100 ROWS ONLY</b>
<b>isig.db.driver</b>	JDBC driver.	For DB2, <b>com.ibm.db2.jcc.DB2Driver</b>  For Oracle, <b>oracle.jdbc.OracleDriver</b>  For PostgreSQL, <b>org.postgresql.Driver</b>
<b>isim.ldap.url</b>	LDAP URL for Security Identity Manager internal LDAP.	ldap://localhost:389 ldaps://192.168.15.15:636
<b>isim.ldap.bind.dn</b>	Distinguished name for Security Identity Manager internal LDAP user.	<b>cn=root</b>
<b>isim.ldap.bind.password</b>	Password for Security Identity Manager internal LDAP user.	
<b>isim.ldap.search.base</b>	Specify the LDAP search base for Data Integrator queries. You must set this property to the Security Identity Manager target DN.	<b>ou=org, dc=com</b>
<b>isim.service.include</b>	Specifies a subset of the Security Identity Manager services that you want to synchronize with Identity Governance and Intelligence. The value of the property is a comma-separated list of the <b>erglobalid</b> of the services. If the <b>isim.service.exclude</b> property is also specified, the <b>isim.services.exclude</b> property is ignored.	<b>isim.service.include=</b> 1614369351932001037,3526292554858738389

Table 11. Properties in *ISIG.properties* (continued)

Property name	Description	Example
<b>isim.service.exclude</b>	Specifies a subset of the Security Identity Manager services that you do not want to synchronize with Identity Governance and Intelligence. The value of the property is a comma-separated list of the <b>erglobalid</b> of the services. If the <b>isim.service.include</b> property is specified, the <b>isim.services.exclude</b> property is ignored.	<code>isim.service.exclude=1614369351932001037,3526292554858738389</code>
<b>log.load.debug</b>	If set to true, enables debug logging for Load operations. The default is false.	<b>false</b>
<b>log.load.info</b>	If set to false, disables information logging for Load operations. Default is true.	<b>true</b>
<b>log.delta.debug</b>	If set to true, enables debug logging for Delta operations. The default is false.	<b>false</b>
<b>log.delta.info</b>	If set to false, disables information logging for Delta operations. Default is true.	<b>true</b>
<b>log.isig.debug</b>	If set to true, enables debug logging for ISIGtoSIM operations. The default is false.	<b>false</b>
<b>log.isig.info</b>	If set to false, disables information logging for ISIGtoSIM operations. Default is true.	<b>true</b>
<b>isig.naming.factory</b>	ISIG naming <b>contextfactory</b> class name for the EJB method lookup.	<b>USE</b> <code>com.ibm.websphere.naming.WsnInitialContextFactory</code>
<b>isig.com.ibm.SSL.CORBA.ConfigURL</b>	The security configuration file location for accessing Java APIs in IBM Security Identity Governance and Intelligence. Do not modify this property.	<b>USE</b> <code>file:ISIGADI/secConfig_isig511/sas.client.props</code>

Table 11. Properties in ISIG.properties (continued)

Property name	Description	Example
<b>isig.com.ibm.CORBA.securityServerHost</b>	Host name or IP address of the WebSphere Application Server that is hosting IBM Security Identity Governance and Intelligence.	
<b>isig.com.ibm.CORBA.securityServerPort</b>	Port of the WebSphere Application Server that is hosting IBM Security Identity Governance and Intelligence. For the virtual appliance, 2821 is the default port for Java APIs.	<b>2821</b>
<b>isig.com.ibm.SSL.ConfigURL</b>	The SSL configuration file for accessing Java APIs in IBM Security Identity Governance and Intelligence. Do not modify this property.	<b>USE file:ISIGADI/secConfig_isig511/ssl.client.props</b>
<b>isig.websphere.ejb.thinclient.jar</b>	The location of EJB thin client JAR file from WebSphere. It is set to the default location.	<b>jars/3rdparty/IBM/IGI/WAS/com.ibm.ws.ejb.thinclient_8.5.0.jar</b>

The format of **isig.db.url** and **isig.db.driver** must be set correctly depending on the database type because IBM Security Identity Governance and Intelligence supports both DB2 and Oracle databases.

New security configuration files are under the ISIGADI/secConfig\_isig511 and ISIGADI/secConfig\_itim51 directories. These files do not need to be modified.

- **sas.client.props**
- **ssl.client.props**
- **jaas\_login\_was.conf** This file is in ISIGADI/secConfig\_itim51 only.

The ISIM.properties file has the properties that are needed for Data Integrator to access the Web Services APIs in Security Identity Manager. The APIs fulfill the entitlement changes from IBM Security Identity Governance and Intelligence to Security Identity Manager.

The properties that are required in ISIM.properties vary according to the version of Identity Manager. Each property in the table includes a note that identifies the version to which it applies. A property is required for all versions unless indicated.

Table 12. Properties in ISIM.properties

Property name	Description	Example
<b>isim.isForITIM51</b>	Set it to true if IBM Tivoli Identity Manager version 5.1 is used. Set it to false otherwise.	<b>true</b>

Table 12. Properties in *ISIM.properties* (continued)

Property name	Description	Example
<b>isim.appServer.url</b> IBM Tivoli Identity Manager 5.1 only	URL for the IBM Tivoli Identity Manager server. Set this value to the value that is specified by the <b>enrole.appServer.url</b> property in <i>ITIM_HOME/data/enRole.properties</i> .	<b>iiop://hostName:2809</b>  Use the host name or IP address of the server for <i>hostName</i> .
<b>isim.appServer.ejbuser.principal</b> IBM Tivoli Identity Manager 5.1 only	EJB user. Set this value to the value that is specified by the <b>enrole.appServer.ejbuser.principal</b> property in <i>ITIM_HOME/data/enRole.properties</i> .	<b>wasadmin</b>
<b>isim.appServer.ejbuser.credential</b> IBM Tivoli Identity Manager 5.1 only	EJB user credential. Set this value to the value that is specified by the <b>enrole.appServer.ejbuser.credential</b> property in <i>ITIM_HOME/data/enRole.properties</i> .	<b>Pwd4wasadmin</b>
<b>isim.appServer.realm</b> IBM Tivoli Identity Manager 5.1 only	User realm name. Set this value to the value that is specified by the <b>enrole.appServer.realm</b> property in <i>ITIM_HOME/data/enRole.properties</i> . If the <b>enrole.appServer.realm</b> property does not have any value in the <b>enRole.properties</b> file, do not set this value.	
<b>isim.com.ibm.CORBA.securityServerHost</b> IBM Tivoli Identity Manager 5.1 only	Identity Manager server host name. If the <b>enrole.appServer.url</b> property in the <b>enRole.properties</b> file has the value <b>iiop://isimServerHost:2809</b> , then <b>isimServerHost</b> is the server host name. It can be an IP address.	<b>isimServerHost</b>
<b>isim.com.ibm.CORBA.securityServerPort</b> IBM Tivoli Identity Manager 5.1 only	Identity Manager server bootstrap port. If the <b>enrole.appServer.url</b> property in the <b>enRole.properties</b> file has the value as <b>iiop://isimServerHost:2809</b> , then <b>2809</b> is the ITIM server bootstrap port.	<b>2809</b>
<b>isim.username</b>	Identity Manager system user is authorized to update users and accounts	<b>ITIM Manager</b>
<b>isim.password</b>	Password for <b>isim.username</b> .	<b>secret</b>
<b>isim.justificationRequired.enabled</b> IBM Security Identity Manager 6 and 7 only	Set the value to true, if IBM Security Identity Manager version 6 or 7 requires the justification. The default value is set to false.	<b>isim.justificationRequired.enabled=true</b>

Table 12. Properties in *ISIM.properties* (continued)

Property name	Description	Example
<b>certificate.baseurl</b>  IBM Security Identity Manager 6 and 7 only	Base URL of the Identity Manager HTTPS URL. If you can access the Identity Manager Console UI through the URL <b>https://hostip:9443/itim/console</b> , then set it to <b>https://hostip:9443/</b> . This property is used by the <b>ImportCertificate</b> assembly line to import the Identity Manager server certificate to Directory Integrator truststore. The <b>ISIGtoISIM</b> assembly line uses the URL to access the Identity Manager Web Services APIs to fulfill the entitlement changes from Identity Governance to Identity Manager.	<b>https://hostip:9443/</b>
<b>isim.wsd1.url.session</b>  IBM Security Identity Manager 6 and 7 only	URL for Identity Manager Web Service API. It is set with the default value. Update the <b>http://hostIP:port</b> section with the information for your site.	<b>https://hostip:9443/</b>
<b>isim.wsd1.url.request</b>  IBM Security Identity Manager 6 and 7 only	URL for Identity Manager Web Service API. It is set with the default value. Update the <b>http://hostIP:port</b> section with the information for your site.	<b>https://hostip:9443/</b>
<b>isim.wsd1.url.account</b>  IBM Security Identity Manager 6 and 7 only	URL for Identity Manager Web Service API. It is set with the default value. Update the <b>http://hostIP:port</b> section with the information for your site.	<b>https://hostip:9443/</b>
<b>isim.wsd1.url.person</b>  IBM Security Identity Manager 6 and 7 only	URL for Identity Manager Web Service API. It is set with the default value. Update the <b>http://hostIP:port</b> section with the information for your site.	<b>https://hostip:9443/</b>
<b>isim.wsd1.url.account</b>  IBM Security Identity Manager 6 and 7 only	URL for Identity Manager Web Service API. It is set with the default value. Update the <b>http://hostIP:port</b> section with the information for your site.	<b>https://hostip:9443/</b>

**Note:** **ISIGtoISIM** uses IBM Security Identity Manager APIs to fulfill the entitlement changes from IBM Security Identity Governance and Intelligence to IBM Security Identity Manager.

For IBM Security Identity Manager Versions 6.x and 7.x, the Web Services API is used.

For Tivoli Identity Manager version 5.1, the public API is used (EJB wrapper classes such as Manager and MO classes).

## Files installed with IBM Security Identity Governance and Administration Data Integrator

JAR files and configuration files are installed with IBM Security Identity Governance and Administration Data Integrator.

Table 13. JAR files

Destination folder in TDI-InstallDir/jars	Description
/3rdparty/IBM/IGI	Contains JAR files to access IBM Security Identity Governance and Intelligence.
/3rdparty/IBM/ISIGADI/	Contains the utility JAR file used by IBM Security Identity Governance and Administration Data Integrator.
/3rdparty/IBM/ITIM51/	Contains the JAR files to access the Java API of IBM Tivoli Identity Manager version 5.1.
/connectors/	Contains the JAR files for an IBM Tivoli Directory Integrator custom connector. Data Integrator uses this connector to access and update the data in IBM Security Identity Governance and Intelligence.
/functions/	Contains the JAR files for custom function components in IBM Tivoli Directory Integrator.

Table 14. Configuration files in the ISIGADI directory in the solution directory for IBM Tivoli Directory Integrator

File name	Description
ATTRIBUTES.properties	Properties file that describes permissions attributes in IBM Security Identity Manager LDAP.
DBMAP.properties	<p>Properties file with configure access to the database system that is used by the Data Integrator to store relationships between IBM Security Identity Manager entries and IBM Security Identity Governance and Intelligence entities.</p> <p>The Data Integrator uses the following properties. Do not modify them.</p> <p><b>sql.com.ibm.db2.jcc.DB2Driver.check</b> The SQL statement that checks for the existence of the relationship map table named <b>ISIG_MAP</b>.</p> <p><b>sql.com.ibm.db2.jcc.DB2Driver.create</b> The DDL statement that creates the relationship map table named <b>ISIG_MAP</b>.</p> <p><b>sql.com.ibm.db2.jcc.DB2Driver.truncate</b> The DDL statement that removes all records from the relationship map table named <b>ISIG_MAP</b>.</p> <p>See "Configuration property files" on page 50.</p>

Table 14. Configuration files in the ISIGADI directory in the solution directory for IBM Tivoli Directory Integrator (continued)

File name	Description
ISIG.properties	<p>Configuration parameters for connections to both IBM Security Identity Governance and Intelligence and the IBM Security Identity Manager LDAP server. Properties also exist that define the LDAP search base and search filters that retrieve various types of entries to be transferred to IBM Security Identity Governance and Intelligence entities.</p> <p>The following properties specify filters that read group and services:</p> <p><b>isim.ldap.itim.service.filter</b> The filter for services.</p> <p><b>isim.ldap.itim.group.filter</b> The filter for groups.</p> <p><b>isim.ldap.search.base</b> The search base used that reads most types of entries.</p>
ISIGADI.xml	Solution file that provides the Data Integrator functionality in Tivoli Directory Integrator.
ISIM.properties	Contains properties that are used by the ISIGtoISIM assembly line to access the IBM Security Identity Manager Web Services API. The API fulfills entitlement changes from IBM Security Identity Governance and Intelligence to IBM Security Identity Manager.

## Troubleshooting

Informational and error messages are in the console where the Data Integrator operation is run.

For more information about the IBM Tivoli Directory Integrator Dashboard, see “Monitoring assembly lines” on page 35.

Log files are written to the *ISIGADI\_SOL\_DIR/ISIGADI/logs* folder. The current log output has the extension *.log*. The log folder contains log output and history from previous runs. The history files have extensions *.1* through *.10*. The following table lists the log files.

### Note:

Be sure to include log files whenever reporting incidents to support.

The **Load**, **Delta**, and **ISIGtoISIM** operations produce a set of log files when they run.

### Debug

Contains verbose log output with information for troubleshooting issues. This log option is disabled by default; enable it by setting the relevant log property to true. See “Configuration property files” on page 50 for a list of properties.

**Info** Contains status messages, the final report, and any error messages. This

log option is enabled by default. Disable it by setting the relevant log property to false. See “Configuration property files” on page 50 for a list of properties.

**Error** Contains only errors and warning messages from the operation. It is useful for quickly locating problems with an operation. This log option is always enabled.

Table 15. Log files found in *ISIGADI/logs* directory

Log file name	Description
load-debug.log	Debug log file for <b>Load</b> operations.
load-info.log	Information log file for <b>Load</b> operations.
load-error.log	Error log file for <b>Load</b> operations.
delta-debug.log	Debug log file for <b>Delta</b> operations.
delta-info.log	Information log file for <b>Delta</b> operations.
delta-error.log	Error log file for <b>Delta</b> operations.
verify.log	The log output for <b>Verify</b> operations.
isig-to-isim-debug.log	Debug log file for <b>ISIGtoISIM</b> operations.
isig-to-isim-info.log	Information log file for <b>ISIGtoISIM</b> operations.
isig-to-isim-error.log	Error log file for <b>ISIGtoISIM</b> operations.

When an error occurs, the following information is written to the log.

**Error message**

The cause of the error.

**Error details**

Additional information about the error for debugging.

**Current LDAP entry**

The LDAP entry from IBM Security Identity Manager that was being processed when the error occurred.

**Changelog entry**

For **Delta** operations only. Complete listing of the **changelog** entry that was being processed when the error occurred.

**Stackdump**

The technical listing of the call stack at the moment when the exception occurred. Save it and send it to support to help troubleshoot your problem.

## Repair list

When a write operation to IBM Security Identity Governance and Intelligence fails, an entry is written to a repair list that is used by the **Repair** operation.

The **Repair** operation retries the synchronization of failed entities. The repair list is stored in the repair-list.json file in the *ISIGADI\_SOL\_DIR/ISIGADI/repair* folder.

Entries in the repair list are removed when an item is retried and successfully written to IBM Security Identity Governance and Intelligence. You can edit the repair-list file and remove any entries that Data Integrator cannot handle.

This file contains a JSON object for each failed entity write operation:

```
{"timestamp":1415789401714,"action":"modify","error":" ROLE_ILLEGAL","dn":"erUid=..."}
```

The following table lists the properties that are captured for each IBM Security Identity Governance and Intelligence write error:

*Table 16. Properties that are captured in the repair-list.json file*

Log file name	Description
<b>timestamp</b>	Specifies when the write failure occurred.
<b>action</b>	The write operation that is performed: add, modify, or delete.
<b>error</b>	The error that occurred.
<b>dn</b>	The DN of the IBM Security Identity Manager entry that was being synchronized when the error occurred.

## Synchronizing Oracle system times with IBM Security Identity Governance and Intelligence

You can synchronize system times with the IBM Security Identity Governance and Intelligence system time.

### Before you begin

See the Oracle documentation for information about stopping and starting Oracle processes and Oracle databases.

To check the Oracle database system time, run the following SQL statement on the Oracle database.

```
select sysdate from dual;
```

If the Oracle system time is different than the host operating system time, you need to change the system time of the host computer.

### About this task

You must synchronize the system time of the Oracle database that is used by IBM Security Identity Governance and Intelligence the IBM Security Identity Governance and Intelligence system time. Otherwise, the entitlement change event is processed at the wrong time.

### Procedure

1. Stop all the Oracle processes.
2. Change the OS system time.
3. Restart the Oracle database.

## Odd status shown in OUT events table

When an entitlement is assigned to or removed from a user, this entitlement change event is shown on OUT Queue. It can then be shared with external applications such as the data integrator. After the data integrator processes the entitlement change event, it updates the ERC Status of this event.

The ERC status can have three possible statuses in IBM Security Identity Governance and Intelligence:

**Unprocessed**

Not processed by an external application.

**Success**

Processed successfully by an external application.

**Error** Processed by external application but an error occurred.

You might see an extra status. This extra status means that the event was processed by the external application, but it was ignored.

!manager.stat0.3! or Processed

For example, this status occurs when a permission that exists only on the IBM Security Identity Governance and Intelligence side is assigned to a user, who is ported over from IBM Security Identity Manager. This status is shown after Data Integrator processes this event. It means that this event is processed by the Data Integrator, but it is ignored because no matching service group for this permission exists in IBM Security Identity Manager.

## **SOAP operation error**

If you set the IBM Security Identity Manager WSDL URLs in the `ISIM.properties` file with the IBM Security Identity Manager server IP address, you might receive the `CTGDIS483E Function has not been initialized SOAP operation error`.

This error can occur even though the IP address is correct.

To resolve this issue, use your IBM Security Identity Manager server host name rather than the IP address.

Also, modify the hosts file on the server where IBM Tivoli Directory Integrator is running and add the IBM Security Identity Manager IP address, host name, and optionally, the short name. For instructions about how to locate your hosts file and how to modify it, see “Defining a host name in the hosts file” on page 14.

## **IBM Security Identity Governance and Administration Data Integrator .properties files modifications**

The Data Integrator properties files are loaded when the IBM Tivoli Directory Integrator server is started.

If you change the Data Integrator properties files, you must stop and restart the IBM Tivoli Directory Integrator server to pick up the changes. For a list of the Data Integrator properties files, see “Configuration property files” on page 50.

## **Accept signer certificate from IBM Tivoli Identity Manager 5.1 and the IBM Security Identity Governance and Intelligence server**

For IBM Security Identity Governance and Administration Data Integrator to communicate with WebSphere Application Server, Data Integrator must obtain a signer certificate from the server.

When you run the **Verify** assembly line for the first time, you are prompted to accept this WebSphere Application Server signer certificate. The **com.ibm.ssl.enableSignerExchangePrompt** property in the `ssl.client.props` file controls prompting.

Two `ssl.client.props` files exist for the Data Integrator:

- One file communicates to the IBM Security Identity Governance and Intelligence WebSphere Application Server.
- One file communicates to the Tivoli Identity Manager 5.1 WebSphere Application Server.

These properties files are in the `secConfig_isigver` and the `secConfig_itim51` directories in the `ISIGADI_SOL_DIR/ISIGADI` directory.

If you are not using the Data Integrator for IBM Security Identity Governance and Intelligence or Tivoli Identity Manager 5.1, you are not prompted. By default, it is set to `gui`. The following GUI window is prompted when you run the **Verify** assembly line from the command prompt for the first time. You must accept the signer certificate.

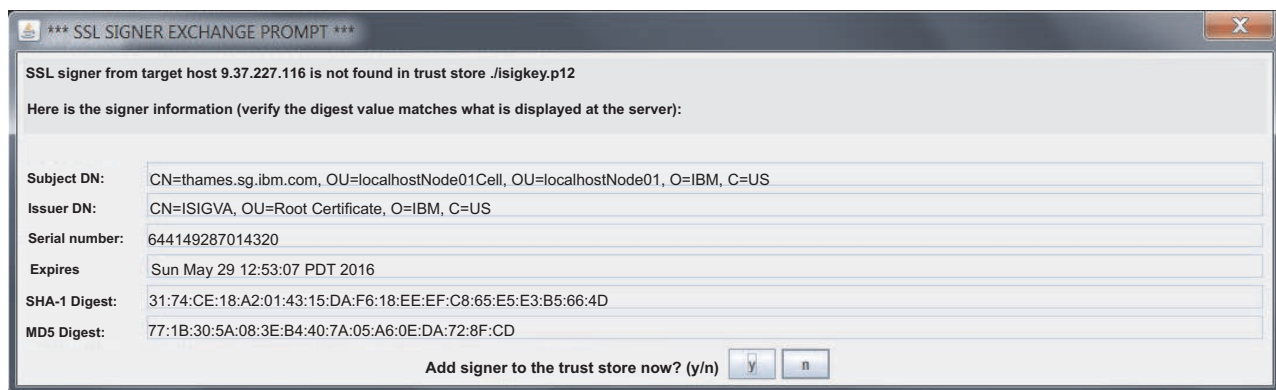


Figure 9. For communicating to the Tivoli Identity Manager 5.1 WebSphere Application Server

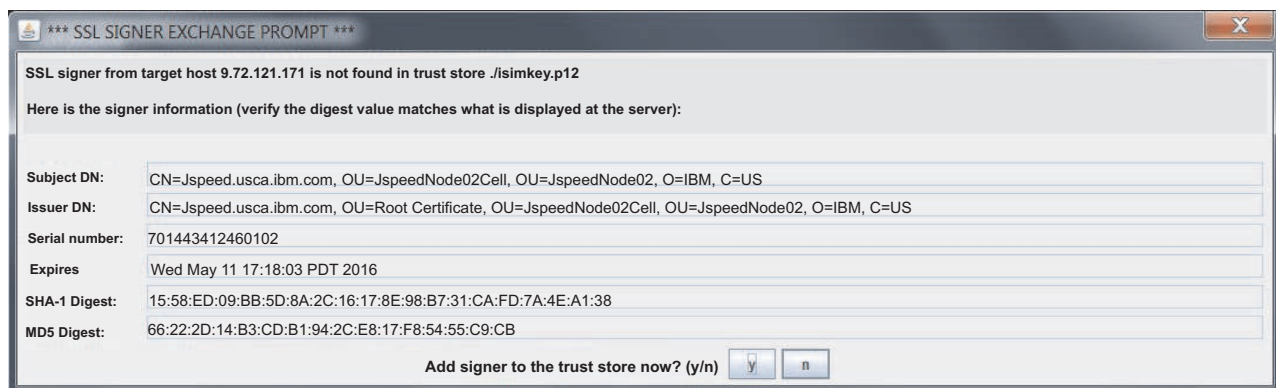


Figure 10. For communicating to the IBM Security Identity Governance and Intelligence WebSphere Application Server

After you accept the signer certificate, the `isimkey.p12` file is created for Tivoli Identity Manager 5.1 and the `isigkey.p12` file is created for IBM Security Identity Governance and Intelligence under the `ISIGADI_SOL_DIR`. After the signer certificate is accepted to the truststore file (`isimkey.p12` and `isigkey.p12`), you are no longer prompted for the information.

If you do not accept the signer certificate, the Data Integrator does not work. The following error messages are displayed.

```
CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=yourHostName, OU=Cell,
OU=nodeName, O=IBM, C=US" was sent from target host:port "yourHost:port".
The signer might need to be added to local truststore "./isimkey.p12"
located in SSL configuration alias "DefaultSSLSettings" loaded from
SSL configuration file
"file:ISIGADI_SOL_DIR/ISIGADI/secConfig_itim51/ssl.client.props".

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=yourHostName, OU=Cell,
OU=nodeName, O=IBM, C=US" was sent from target host:port "yourHost:port".
The signer might need to be added to local truststore "./isigkey.p12"
located in SSL configuration alias "DefaultSSLSettings" loaded from
SSL configuration file
"file:ISIGADI_SOL_DIR/ISIGADI/secConfig_isig511/ssl.client.props".
```

---

# Index

## A

- adapters
  - complex group attributes
    - configuration for 38
  - customizing for 37
- assembly line operations
  - delta 5, 30, 33
  - isigtoisim 30, 34
  - ISIGtoISIM 5
  - load 5, 30
- assembly lines
  - monitoring 35
  - starting and stopping 35
  - verify 28

## C

- changelog, enabling for Security Identity Manager 12
- configuration
  - adapters with complex group
    - attributes 38
  - itdi\_home property 21
  - roadmap 6
  - setEnv file 23
  - verifying 28
- configuration files
  - copied to Directory Integrator 58
  - installation
    - files copied to Directory
      - integrator 58
    - ISIG.properties 50
- Customizing
  - data integrator 37
  - for adapters 37

## D

- data integrator
  - !manager.stat0.3!: status message 61
  - customizing 37
  - log files 59
  - repair list 60
  - SDK, updating 17
  - solution, upgrading 18
  - synchronizing system times 61
  - troubleshooting 59, 60, 61
- data Integrator
  - installing 15
- Data Integrator 1, 21, 23
- database, preparing for data integrator
  - use 13
- DBMAP.properties file 50
- delta
  - starting the assembly line 30, 33
- Delta assembly line
  - stopping synchronization 34
- deployment 5
- Directory Integrator
  - files copied to 58

- DNS, locating the IBM Security Identity Governance and Intelligence server 15

## F

- files
  - reference 49

## H

- hosts file, entry for the IBM Security Identity Governance and Intelligence server 15

## I

- IBM Security Identity Governance and Administration Data Integrator
  - Data Integrator 1
  - installing 21, 23
  - new features 1
  - overview 3
- Incremental data operations
  - stopping synchronization 34
- installation
  - installing the Identity and Governance Data Integrator 15
  - pre-installation setup 10
  - prerequisites 9
  - roadmap 6
- integration 1, 21, 23, 25, 26, 27
- ISIG.properties file 50
- isigtoisim
  - starting the assembly line 30, 34
- ISIGtoISIM
  - stopping synchronization
    - operations 34
- ISIM.properties file 50
- itdi\_home property 21

## J

- JAR files
  - copied to Directory Integrator 58
- JDBC driver 12

## L

- load
  - starting the assembly line 30
- log files 59

## M

- monitor
  - assembly lines 35

## N

- new features 1

## O

- operating systems 9
- operations
  - delta 5
  - ISIGtoISIM 5
  - load 5
- overview 3
  - deployment topologies 5
  - operations 5

## P

- pre-installation setup 10
  - changelog for Security Identity Manager, enabling 12
  - database, preparing for data integrator 13
  - defining a host name 15
  - installing JDBC driver 12
  - preparing the DB2 database for data integrator 13
  - SSL enablement 13
  - Tivoli Directory Integrator 10
  - Tivoli Directory Integrator solution
    - directory, finding default 12
- preparing database for data integrator
  - use 13
- preparing DB2 database for data integrator
  - use 13
- prerequisites
  - operating systems 9
  - software 9
- properties
  - configuration files
    - reference 49
  - itdi\_home 21
  - reference 49
- properties files
  - DBMAP.properties 50
  - directory integrator 62
  - ISIM.properties 50

## R

- reference 49
- repair list
  - data integrator 60
- roadmap
  - installation and configuration 6

## S

- script files
  - instructions 23

- SDK
  - updating 17, 20
- set up
  - defining a host name 15
  - enabling changelog for Security Identity Manager 12
  - installing JDBC driver 12
  - preparing the database for data integrator 13
  - preparing the DB2 database for data integrator 13
  - SSL enablement 13
  - Tivoli Directory Integrator 10
  - Tivoli Directory Integrator solution directory, finding default 12
- setEnv
  - configuring 23
- setting up 10
- signer certificates
  - troubleshooting 63
- soap operation error
  - troubleshooting 62
- software requirements 9
- SSL
  - certificate and keystore, creating 25
  - certificate, uploading to Security Identity Manager 26
- SSL (*continued*)
  - Security Identity Manager certificate, importing to Tivoli Directory Integrator 27
  - Tivoli Directory Integrator certificates 13
- SSL enablement 13
  - checking the self-signed certificate 24
- synchronization operations
  - stopping entitlement fulfillment 34
  - stopping incremental data operations 34
- system time synchronization 61

**T**

- Tivoli Directory Integrator 10
  - default solutions directory 12
  - JDBC driver 12
  - SSL certificates 13
- troubleshooting
  - data integrator
    - !manager.stat0.3!: status message 61
    - log files 59
    - repair list 60

**U**

- update
  - SDK 20
- upgrade
  - data integrator 17
  - data integrator solution 18
  - SDK 17

**V**

- verify assembly line
  - verifying the data integrator configuration 28

- troubleshooting (*continued*)
  - data integrator (*continued*)
    - synchronizing system times 61
  - modifying property files 62
  - signer certificates 63
  - soap operation error 62