



## Administration Application Installation



prev



next



contents



index



view as PDF

get  
Adobe  
Reader

# Configuring Metadirectories

This section describes how to configure a metadirectory to extract user data from your user repository (for example, an LDAP server, an Active Directory, a database server, or NT Domain directory) and import that data into the policy database. As a result, the user, group and attribute data (referred to simply as attributes) are available and synchronized, and can be used to enforce dynamic security policies in your applications through the ASI Authorization and ASI Role Mapping services.

This section covers the following topics:

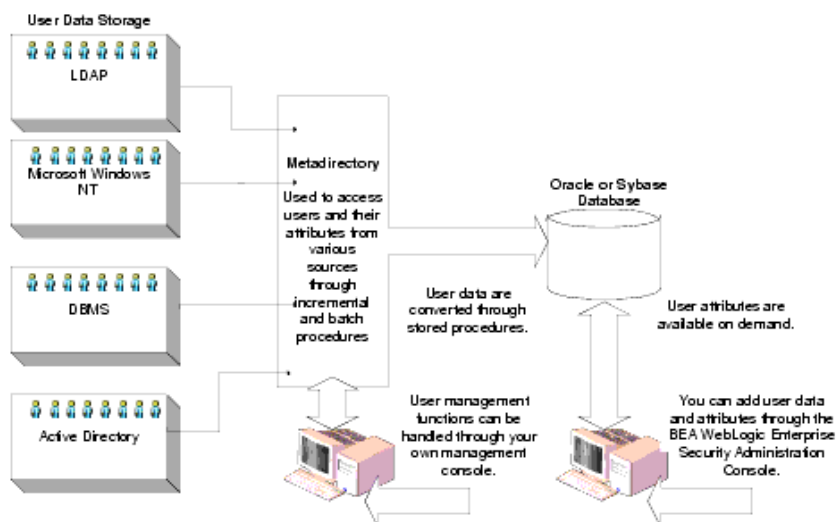
- [Why Use Metadirectories?](#)
- [Metadirectory Configuration Overview](#)
- [Preparing to Configure a Metadirectory](#)
- [Configuring Metadirectory Tables and Database Triggers](#)
- [Configuring Metadirectory Schemas](#)
- [Configuring Metadirectory Synchronization](#)
- [Verifying that Metadirectory Synchronization Works](#)

---

## Why Use Metadirectories?

BEA WebLogic Enterprise Security requires that all policy data be stored in either an Oracle or Sybase policy database. The goal of a metadirectory is to provide your organization with a unified view of all identity information. A metadirectory solves important business issues that result from having information stored in multiple, disparate data repositories throughout an organization. Thus, through the use of a metadirectory, the maintenance cost of sharing information is reduced and the accuracy and the overall security of an application is improved (see [Figure 6-1](#)).

### Figure 6-1 Metadirectory Architecture



In BEA WebLogic Enterprise Security, the term directory applies to any collection of user data, stored in a database, LDAP directory server, or other type of repository. These directories form the core of any identity management solution because every user repository has its own approach to the storage of information.

An identity directory refers to any user repository configured for use with BEA WebLogic Enterprise Security. In the Administration Console, the identity directory defines a logical collection of users, groups and attributes that can be used to design your authorization and role mapping policy, and store information about who is authorized through your policies. An identity directory typically represents groups of users of a particular application or resource, users in a specific location, or users imported from an external user repository.

A metadirectory can be used to store attributes replicated and synchronized from your user repository into the policy database. Following replication, the user data are available as attributes through the Administration Console identity directories for use in your authorization policies and policy rules. Any changes that you make to the replicated user attributes using the Administration Console are not propagated back to your user repository.

## Metadirectory Configuration Overview

To configure metadirectories, you use several different components (see [Figure 6-2](#)). In [Figure 6-2](#), each task is represented by a number that is positioned next to the component that you use to perform the task.

### Figure 6-2 Metadirectory Configuration Components

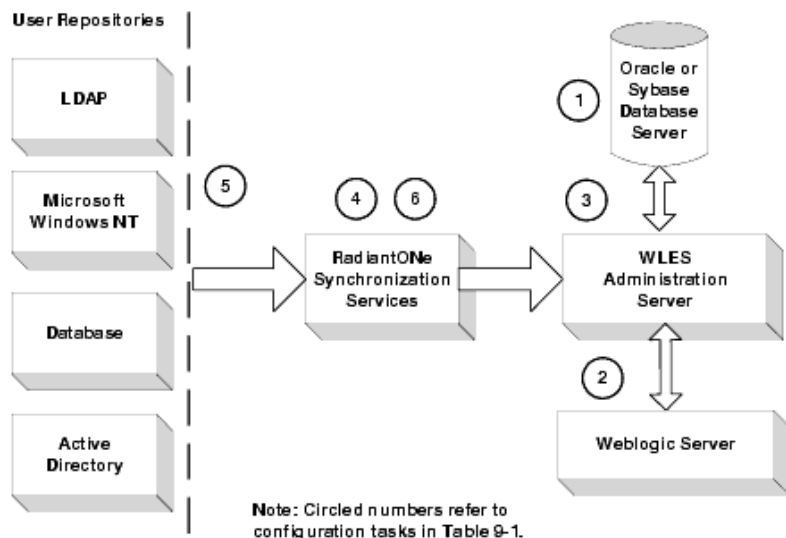


Table 6-1 summarizes the tasks and links each task to a circled number in Figure 6-2.

**Table 6-1 Metadirectory Configuration Tasks**

Use this component:	To perform these tasks:
Database Server	1. Create the destination tables.
WebLogic Server Administration Console	2. Configure a JDBC connection pool and the Java Message Service.
WebLogic Enterprise Security Administration Console	3. Configure database triggers.
RadiantOne Synchronization Services	4. Configure metadirectory schemas and the synchronization hub.
User Repository Server	5. Configure the directory connector. <b>Note:</b> This task is required only if you are using Sun ONE Active Directory as your user repository server.
RadiantOne Synchronization Services	6. Configure the connectors and start the synchronization hub and the connectors.

For detailed instructions on performing each of the tasks listed in Table 6-1, see the following sections:

- [Preparing to Configure a Metadirectory](#)
- [Configuring Metadirectory Tables and Database Triggers](#)
- [Configuring Metadirectory Schemas](#)

- [Configuring Metadirectory Synchronization](#)
- 

## Preparing to Configure a Metadirectory

Before you begin, you must install and start the RadiantOne Synchronization Services. RadiantOne Synchronization Services use the JDBC and Java Message Service (JMS) features of the WebLogic Server that hosts the WebLogic Enterprise Security Administration Application to update the metadirectory. The RadiantOne Synchronization Services tool provides connectors for the master identity repositories that send XML formatted messages whenever information in an user repository is updated. Through the use of the JMS, this tool ensures that all updates are delivered and processed. For installation instructions, see [Installing the RadiantOne Synchronization Services](#).

## Installing the RadiantOne Synchronization Services

The RadiantOne Synchronization Services software is available as separate installation CD-ROMs (see install kit disks 3 and 4). After you install the product, you can access the applications from the Start>Programs>RadiantOne menu.

To install the RadiantOne Synchronization software:

- On a Microsoft Windows platform, run: wles422metadir\_win32.exe.
- On a Sun Solaris platform, run: wles422metadir\_solaris32.bin.
- On a Linux platform, run: wles422metadir\_rhas21\_IA32.bin.

**Note:** A second installation package is available for installing the RadiantOne Connectors. These are included in the RadiantOne Synchronization Services install package and do not need to be installed separately. However, you can install the connector package separately on another machine. For instructions for installing the connectors separately, refer to the RadiantOne Synchronization Services installation documentation. When you install the RadiantOne software, the online documentation is installed in the RadiantOne directory

---

## Configuring Metadirectory Tables and Database Triggers

This section covers the tasks that you must perform to create destination tables in the WebLogic Enterprise Security policy database and install triggers on those tables.

To configure metadirectory tables and database triggers, perform the following tasks:

- [Creating Metadirectory Destination Tables](#)
- [Configuring a JDBC Connection Pool and JMS](#)
- [Configuring Metadirectory Database Triggers](#)

## Creating Metadirectory Destination Tables

There are two tables that you have to create in the policy database for the synchronization of users and groups to work properly: `ASI_USERS` and `ASI_GROUPS`. After you create these tables, you configure them through the WebLogic Enterprise Security Administration Console. You must create these tables before you perform the remaining tasks in this section.

The following sections provide guidelines and restrictions for the tables and detailed instructions on how to create them:

- [Metadirectory Destination Table Guidelines and Restrictions](#)

- [Creating Metadirectory Destination Tables Using Oracle or Sybase](#)

## Metadirectory Destination Table Guidelines and Restrictions

Two tables are required in the policy database for the synchronization of user repositories: `ASI_USERS` and `ASI_GROUPS`. The following sections provide guidelines and restrictions for these tables:

- [User Synchronization Table Guidelines](#)
- [User Synchronization Table Guidelines](#)
- [User and Group Attributes Character Set Restrictions](#)

### User Synchronization Table Guidelines

The user synchronization table is used by the partner tool to stage user and user attribute information for import into the policy database. The name of the table used for user synchronization is configurable.

While the names of the columns in the table are configurable, the following restrictions apply:

- One column in the table must serve as the unique identifier for the user. The UID may contain any character, but the ``/` character must be escaped. For example, "John\Doe" must be entered as "John\Doe".
- The Primary Key for the table should be the column used as the UID. For performance and data consistency, the user synchronization table should include the primary key in its definition.

The user synchronization table accommodates source repositories that store group memberships as user attributes. Managing group memberships as user attributes does not impact managing group memberships explicitly through the group synchronization table—both ways can be used.

You must adhere to the following restrictions and requirements when setting up group memberships through the user synchronization table:

- Only one column may be used for storing the group memberships.
- The group column needs to be a character string (typically in Oracle: `varchar2`).
- Membership in multiple groups is possible and is stored as a delimited text string. The choice of delimiter is configurable but should be sufficiently uncommon so that parsing of the group list may be done correctly.
- If the group name contains the ``/` character, it should be escaped.

Any number of columns in the user synchronization table may be used for passing attributes into the WebLogic Enterprise Security Administration Server. The columns used for all attributes in the User Synchronization table must be of variable length character (for example, in Oracle: `varchar2`). For purposes of importing from the user synchronization table, you may map attributes to any of the following WebLogic Enterprise Security policy data types: `string`, `integer`, `boolean`, `date`, `time`, `dayofweek_type`, `month_type`, and `object_type`. Attributes are also defined as either `list` or `single`. Multiple attribute values of type `list` are stored as a delimited text string. The delimiter used for attributes of type `list` must be the same as the delimiter used for groups.

### Group Synchronization Table Guidelines

In addition to the user-attribute-based group membership discussed above, group memberships may also be defined by using the group synchronization table. Unlike the `User Synchronization` table, the schema for the group synchronization table is fixed, that is, it must adhere to the structure shown in [Table 6-2](#).

**Table 6-2 Group Synchronization Table**

Column Name	Type	Description
CN	varchar2	The name of the group
UNIQUEMEMBER	varchar2	The name of the user belonging to the group.

You must adhere the following restrictions and requirements when setting up the group synchronization table:

- The Primary Key for the table should consist of both columns.
- A forward slash (/) in the value for either of the columns must be escaped using a back slash (\).

### User and Group Attributes Character Set Restrictions

The following requirements and restrictions apply to user and group attributes

- The name of the attribute cannot be longer than 1000 character (580 characters for some Sybase 12.5 configurations, depending on the page size)
- Each value of a user attribute cannot be longer than 1000 characters. (580 characters for some Sybase 12.5 configuration, depending on the page size)
- The length of the value of all user attributes combined cannot be longer than the lesser of 16,000 characters or the `varchar2` column-size limit for the database.
- Attribute names in WebLogic Enterprise Security may only consist of alphanumeric characters (a-z, A-Z, 0-9) and the underscore (\_) character.
- The column name of the user synchronization table is limited by any database character set limitations.
- Attribute names must start with an alphabetic character or an underscore.
- Any printable characters are allowed except double quote (") and back slash (\).

### Creating Metadirectory Destination Tables Using Oracle or Sybase

To create the `ASI_USERS` and `ASI_GROUPS` destination tables using an Oracle or a Sybase database server,

1. To log into the policy database, open a command window and type:

```
sqlplus username/password@asi
```

where: `username` and `password` are the username and password you defined when you created the database user account and `asi` is the database instance name.

2. To create the `ASI_USERS` destination table, enter the following SQL command:

```
SQL> CREATE TABLE ASI_USERS(DisplayName VARCHAR(255) NULL,
COMMONDOMAIN VARCHAR(255) NOT NULL, PRIMARY KEY (COMMONDOMAIN))
```

3. To create the `ASI_GROUPS` destination table, enter the following SQL command:

```
SQL> CREATE TABLE ASI_GROUPS(CN VARCHAR(255) NOT NULL,
UNIQUEMEMBER VARCHAR(255) NOT NULL, PRIMARY KEY
(CN, UNIQUEMEMBER))
```

**Note:** In addition to `DisplayName`, you can add more columns to the destination tables to be used as

user attributes, such as street address, zip code, email, phone, and so on.

## Configuring a JDBC Connection Pool and JMS

To connect to the RadiantOne Synchronization Services to the WebLogic Enterprise Security asiDomain, you must use the WebLogic Server Administration Console to configure a JDBC connection Pool and the Java Message Service (JMS).

To configure the JDBC connection pool and JMS, perform the following steps:

1. To start the WebLogic Server Administration Console, open a browser and go to `https://hostname:7010/console`,  
where:  
*hostname* in the name of the machine that is hosting the WebLogic Enterprise Security Administration Application  
7010 is the port on which the Administration Console is running
2. In the left pane of the Administration Console, open the Services and JDBC folders and click Connection Pools. The asiDomain> JDBC Connection Pools page is displayed in the right pane.
3. Click Configure a new JDBC Connection Pool. The Configure a JDBC Connection Pool: Choose database page is displayed.
4. Select the Database Type and the Database Driver as specified in [Table 6-3](#) and click Continue. The Configure a JDBC Connection Pool: Define connection properties page is displayed.

**Table 6-3 Database Type and Database Driver Parameter Settings**

JDBC Connection Pool Parameter	Setting
Database Type	Oracle or Sybase
Database Driver	For Oracle 8i, select Oracle's Driver (Thin) Versions: 8.1.7 For Oracle 9i, select Oracle's Driver (Thin) Versions: 9.0.1,9.2.0,10 For Sybase, select BEA's Sybase Driver (Type 4) Versions: 11.X,12.X

5. Refer to [Table 6-4](#), enter the appropriate values in the Configure a JDBC Connection Pool: Define connection properties page, and click Continue. The Configure a JDBC Connection Pool: Test database connection page is displayed.

**Table 6-4 JDBC Connection Pool Configuration Parameters**

Parameter	Description
Name	The JDBC connection pool name that you specify, for example, ConsolePool.

Database name	The name assigned to the instance of the database when it was created, for example, ASI5
Hostname	The name of the machine on which the database server is installed, for example, ASI_host
Port	The port used for the connection to the database server (default: 1521).
Database User Name	The username of the database account, for example, wles
Password/Confirm Password	The password assigned with the database account was create for the user (any alphanumeric string).

6. Click Test Driver Configuration. A "Connection successful" message and the Configure a JDBC Connection Pool: Create and deploy page is displayed.
7. Click Create and Deploy. The connection pool is deployed.
8. To configure a JMS template, perform these steps:
  - a. In the left pane, open the Services and JMS folders and click Templates. The asiDomain> JMS Templates configuration page is displayed in the right pane.
  - b. Click Configure a new JMS Template, name the template `RLI_JMS`, and then click Create.
9. To configure a JMS JDBC store, perform these steps:
  - a. In the left pane, click Stores.
  - b. Click Configure a new JMS JDBC Store.
  - c. Name the store `RLI_JDBC_STORE`.
  - d. Set the Connection Pool to the name of the connection pool created previously (`ConsolePool`) and select Create.
10. To configure a JMS server, perform these steps:
  - a. In the left pane, click Servers.
  - b. Click Configure a new JMS Server.
  - c. Name the server `RLI_JMS_SERVER`.
  - d. Set Persistent Store to the JDBC store that was created previously (`RLI_JDBC_STORE`).
  - e. Set Temporary Template to the template that was created previously (`RLI_JMS`), and click Create.
  - f. Click the Target an Deploy tab and set Target to asiAdminServer and click Apply.
11. To configure a JMS Connection factory, perform these steps:
  - a. In the left pane, click Connection Factories.
  - b. Click Configure a new JMS Connection Factory,
  - c. Set Name to `RLI_JMS_CONNECTION`,
  - d. Set JNDI Name to

`weblogic.asiAdminServer.jms.TopicConnectionFactory`, and click Create.

- e. Click the Target and Deploy tab and set Target to `asiAdminServer` and click Apply.
12. To restart the WebLogic Server so that the change takes effect, close the WebLogic Server command window or, if WebLogic Server is setup to run as a Windows service, restart the service.
13. This completes the configuration of the JDBC connection pool and JMS.

## Configuring Metadirectory Database Triggers

You must configure database triggers for the user and group synchronization tables in the policy database. A database trigger provides a necessary link between the metadirectory database and the policy database. A trigger enables the user attributes to be received by the Administration Server and put into the identity directory (that you define) whenever a change occurs in the underlying metadirectory database.

**Note:** Any modifications that you make to the existing data records in the synchronization tables must be made with an `UPDATE` command, not through a series of `DELETE` and `INSERT` commands. Use `INSERT` only for new records and `DELETE` only for removing records. Also, do not use the "truncate table" command to clean either the user or group synchronization tables because that command does not activate the triggers.

To configure metadirectory database triggers, perform the following steps:

1. To start the WebLogic Enterprise Security Administration Console, open a browser and go to `https://hostname:7010/asi`,  
where:  
*hostname* is the name of the machine that is hosting the WebLogic Enterprise Security Administration Application  
*7010* is port on which the Administration Console is running  
*asi* is the domain name
2. In the left pane, open the Identity folder and click Metadirectory Configuration. The Metadirectory Configuration page is displayed in the right pane.
3. In the Metadirectory Configuration page, select the database type (either Oracle or Sybase), enter the name of the JDBC connection pool (for example: `ConsolePool`) and the name of the synchronization tables (`ASI_USERS` and `ASI_GROUPS`), and click Connect. A "Successful Connection" message is displayed along with additional fields that require input.
4. Refer to [Figure 6-3](#), and fill in the additional fields. Set `user id` to the WebLogic Enterprise Security schema owner, which is the same as the database account username. Set the `identity directory` name field to any directory name that is unique in the `asiDomain`. This identity directory is the directory in the policy database into which users are populated. Set the `COMMONDOMAIN` and `DISPLAYNAME` parameters as shown in [Figure 6-3](#).
5. Click Install Trigger. A "Trigger successfully installed" message is displayed.
6. This completes the configuration of the metadirectory database triggers.

**Figure 6-3 Metadirectory Triggers Configuration**

Name	Configuration Type	WLES Attribute Type	Single or List
COMMONDOMAIN	uid	string	Single
DISPLAYNAME	attribute	string	List

## Configuring Metadirectory Schemas

BEA WebLogic Enterprise Security uses a comprehensive schema for tracking and updating all policy data. You use RadiantOne Synchronization Services to configure the schemas required to upload user and groups information from the user repository to the policy database.

To configure the required metadirectory schemas, perform following tasks:

- [Extracting the Source Schemas](#)
- [Loading the Source Schemas](#)
- [Extracting the Destination Schemas](#)
- [Loading the Destination Schemas](#)
- [Configuring the Source-to-Destination Topology](#)
- [Configuring the Topology Transformations](#)
- [Uploading User and Group Data](#)

## Extracting the Source Schemas

This section describes how to extract the source schemas for the user repository.

To extract the source schemas from the user repository, perform the following steps:

1. Copy the `WL_Home\server\lib\weblogic.jar` file to the `RadiantOne\r1syncsvcs\bea_lib` directory.
2. To start the RadiantOne Synchronization Services tool:  
On Windows: click `Start>Programs>RadiantOne>RadiantOne Synchronization Services>Synchronization Services Administrator`.  
On Sun Solaris: From the `RadiantOne/r1syncsvcs/bin` directory, run: `runSSC.sh`.
3. To start the Schema Extraction Wizard is displayed, select `New` from the `Datastore` drop-down menu.
4. Select `LDAP Schema Extraction` radio button and click `Next`. The `LDAP Schema Extractor` page is displayed.

5. Refer to [Table 6-4](#) and [Table 6-5](#) and enter the directory server information. To determine the complete directory server name and port number, refer to the directory server console (see [Figure 6-5](#)) and check the values. For example, in [Figure 6-5](#), the complete name is `asi_host.amer.bea.com` and the port number is `56763`.

**Figure 6-4 LDAP Schema Extractor Page**

LDAP Schema Extractor :

Use this wizard to extract schema from a LDAP server. Enter the name and port number of the server from where you want to extract the schema. Please specify the base suffix.

Server and Port

Server :

Port :   SSL

User Authentication Information

User Name :

Password :

Base DN

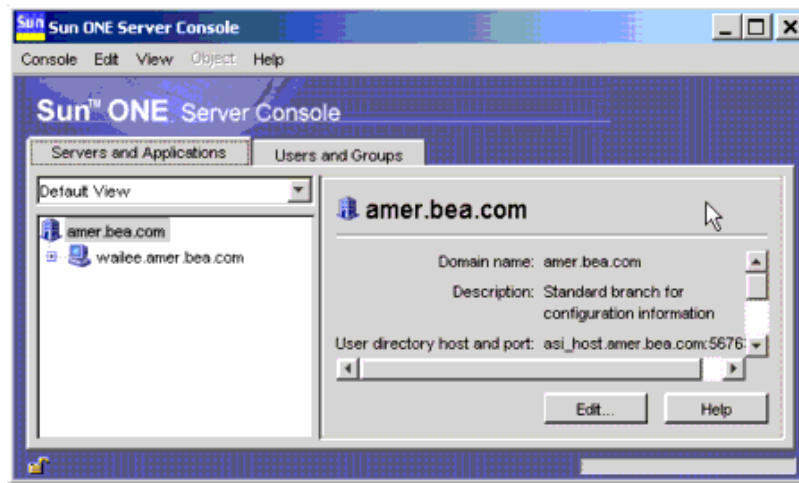
Base DN :

Test Connection Exit Next Help

**Table 6-5 LDAP Schema Extractor Parameters**

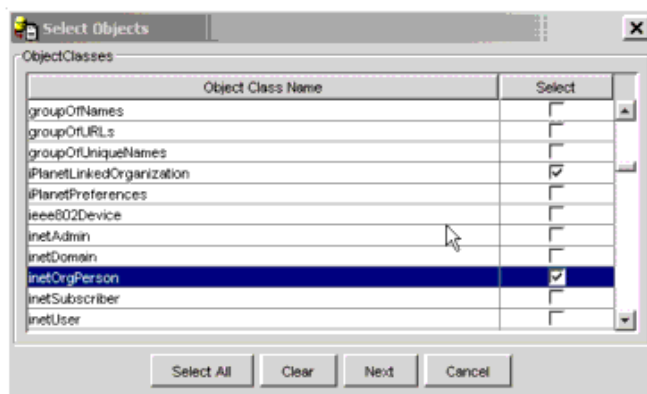
Parameter	Description
Server	The name of the LDAP Directory server, for example, <code>asi_host.amer.bea.com</code>
Port	The port number of the LDAP Directory server, for example, <code>56763</code>
Username	The username you enter to access the LDAP Directory server (default: Directory Manager).
Password	The password you enter to access the LDAP Directory server.
Base DN	The base domain name, for example, <code>dc=amer</code> , <code>dc=bea</code> , <code>dc=com</code> .

**Figure 6-5 Sun ONE Server Console**



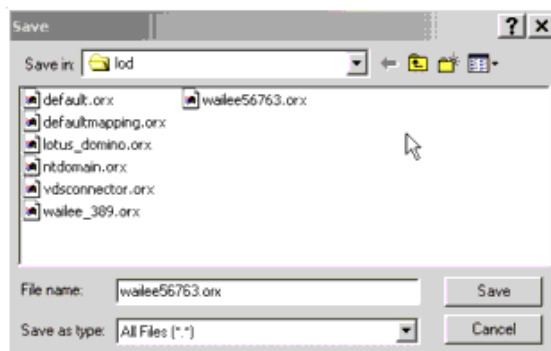
6. Click Test Connection. A "Connection Successful" message dialog box is displayed.
7. To close the message dialog box, click Ok and then click Next. The Select Objects page is displayed (see [Figure 6-6](#)).

**Figure 6-6 RadiantOne Select Objects Page**



8. Select the `groupOfUniqueNames` and `inetOrgPerson` object classes and click Next. The Save windows is displayed (see [Figure 6-7](#)).

**Figure 6-7 RadiantOne Select Object Save Window**



9. In the Save window, edit the Filename field to remove all but the directory server name, the port number, and the .orx filename extension as shown in [Figure 6-7](#), and click Save. A "Schema Extraction Completed" message dialog box is displayed.
10. . Click Ok and then click Exit.
11. This completes the extraction of the source schemas.

## Loading the Source Schemas

This section describes how to load the source schemas for the user repository.

To load the source schemas from the user repository, perform the following steps:

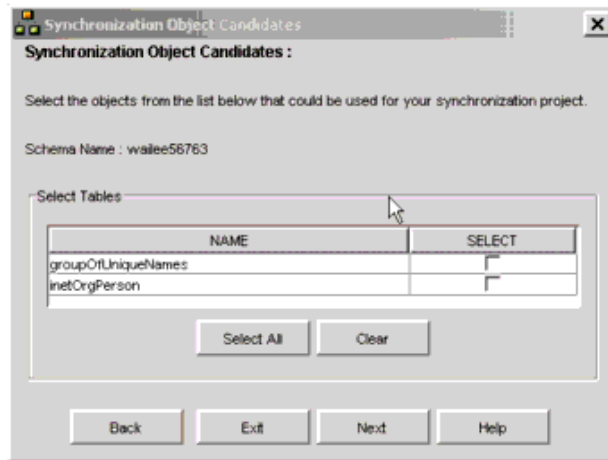
1. On the RadiantOne Synchronization Services Administration console, from the Datastore drop-down menu, select Add. The Synchronization Object Candidates page is displayed (see [Figure 6-8](#)).

**Figure 6-8 RadiantOne Synchronization Object Candidates Page**



2. Click Directory. The Open window is displayed.
3. Select schema extraction file that you created in [Extracting the Source Schemas](#) (for example: asi56763.orx) and click Open. The Schema File field is populated with the filename, including the path.
4. Click Next. The Synchronization Objects Candidates page is displayed (see [Figure 6-9](#))

**Figure 6-9 Synchronization Select Objects Page**



5. Click Select All and click Next. A "Successfully generated the datastore" message is displayed.
6. To exit, click Finish.
7. This completes the loading of the source schemas.

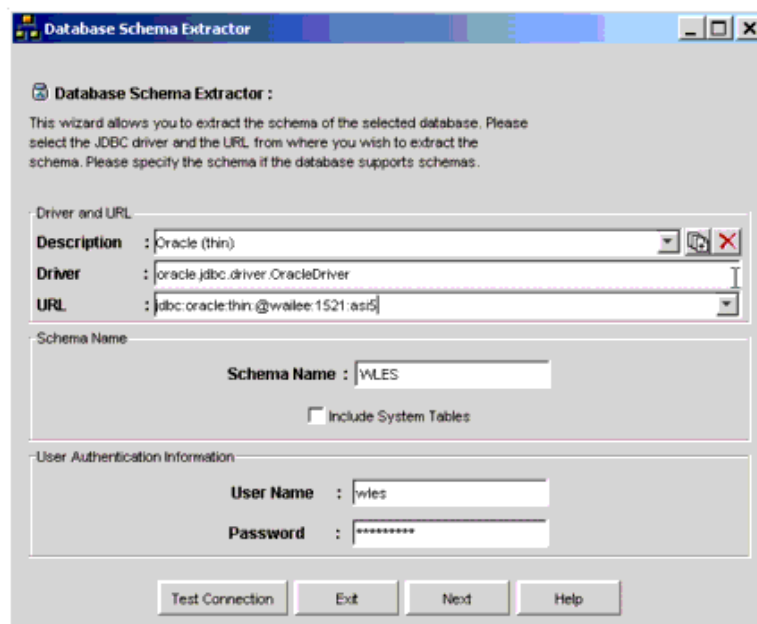
## Extracting the Destination Schemas

This section describes how to extract the policy database destination schemas for the database server.

To extract the destination schemas from the database server, perform the following steps:

1. On the RadiantOne Synchronization Services Administration console, to start the Schema Extraction Wizard is displayed, select New from the Datastore drop-down menu.
2. Select Database Schema Extraction radio button and click Next. The Database Schema Extractor page is displayed (see [Figure 6-10](#)).

**Figure 6-10 Database Schema Extractor Page**



3. Refer to [Table 6-6](#) and set the database server parameters.

**Table 6-6 Database Server Parameters**

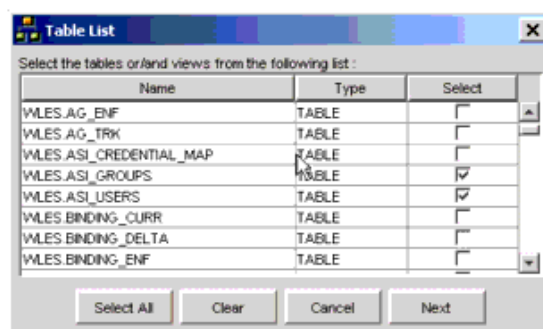
Parameters	Description
Description	The type of database used for the database server.
Driver	The database JDBC driver.  <b>Note:</b> Better performance may be achieved by configuring a Type II JDBC driver. For Oracle (OCI), this is the same driver but uses a different URL syntax. Please refer to your Oracle documentation for the correct syntax and configuration.
URL	The URL of the database server. You are only required to supply the name of the database host machine and database name, for example, jdbc:oracle:thin@asi_host:1521:asi5.
Schema Name	The schema name. This name must be unique in the database server, for example, WLES.  <b>Note:</b> If you are using an Oracle database server, you must type the schema name in uppercase.
Include System Tables	Determines whether system files are included. Check this box to on.
User Name	The username you enter to access the database server.
Password	The password you enter to access the database server

4. To verify that the schema extractor can connect to the database server, click Test Connection. A "Connection succeeded" dialog box is displayed.

**Note:** If the connection fails, make sure that all the database server parameters are set correctly.

5. Click Ok and click Next. The Table List dialog box is displayed (see [Figure 6-11](#)).

**Figure 6-11 Table List Dialog Box**



6. Select the `WLES.ASI_GROUPS` and `WLES.ASI_USERS` tables and click Next. The Save window is displayed.
7. Accept the default filename (the default filename should match the database name) and click Open. A "Schema Extraction Completed" message dialog box is displayed.  
**Note:** Be sure to save the filename in lowercase. Also, the filename cannot contain any periods (for example, this filename is correct: `asi5.orx`).
8. Click Ok and then click Exit. By default this schema is saved to `../RLI_HOME/data/org`.
9. This completes the extraction of the destination schemas.

## Loading the Destination Schemas

This section describes how to load the policy database destination schemas for the database server.

To load the destination schemas from the database server, perform the following steps:

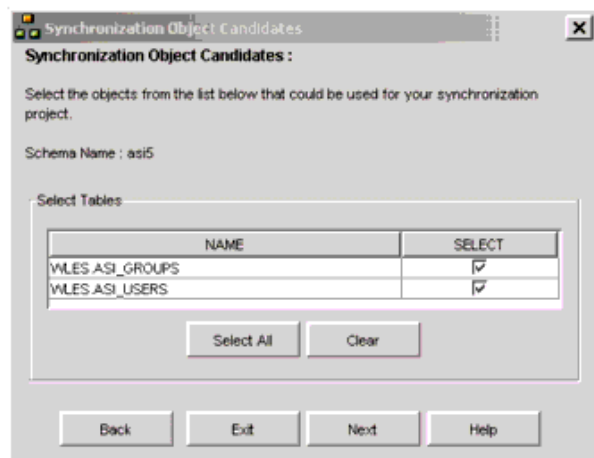
1. On the RadiantOne Synchronization Services Administration console, from the Datastore drop-down menu, select Add. The Synchronization Object Candidates page is displayed (see [Figure 6-12](#)).

**Figure 6-12 RadiantOne Synchronization Object Candidates Page**



2. Click Database. The Open window is displayed.
3. Select schema extraction file that you created in [Extracting the Destination Schemas](#) (for example: `asi5.orx`) and click Open. The Schema File field is populated with the filename, including the path.
4. Click Next. The Synchronization Objects Candidates page is displayed (see [Figure 6-13](#)).

**Figure 6-13 Synchronization Select Objects Page (Database Server Objects)**



5. Click Select All and click Next. A "Successfully generated the datastore" message is displayed.
6. To exit, click Finish.
7. This completes the loading of the database server schemas for the policy database.

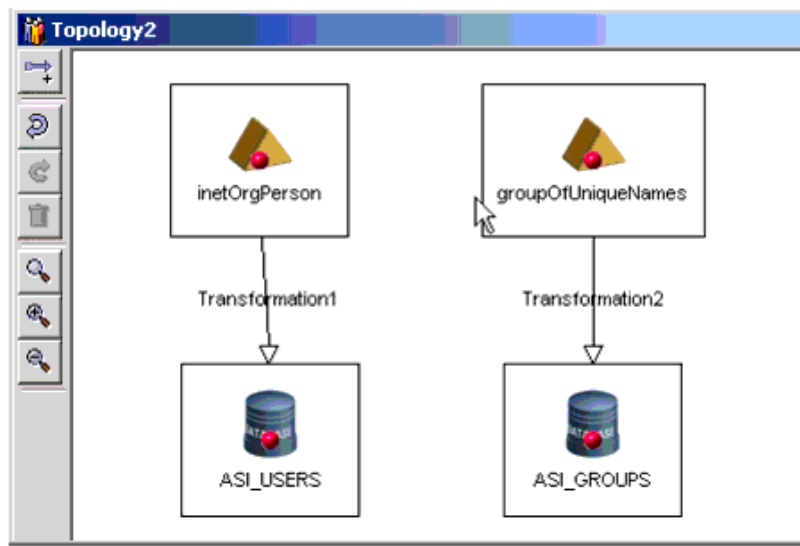
## Configuring the Source-to-Destination Topology

This section describes how to configure the RadiantOne topology that serves to link the source user repository to the policy database. The topology shows all of the objects involved in the synchronization process and the data flow. You use the topology to define and connect all of the data objects that are involved in a particular synchronization process.

To configure the topology, perform the following steps:

1. On the RadiantOne Synchronization Services Administration console, from the RadiantOne Synchronization Services Topology drop-down menu, select New. The Topology window is displayed in the right pane.
2. Expand the nodes in the left pane, click the `groupOfUniqueNames` node and drag and drop it into the right pane.
3. Repeat step 3 for the `initOrgPerson`, `ASI_GROUPS`, and `ASI_USERS` nodes.
4. Click the red dot for each of the publishing objects (`groupOfUniqueNames` and `initOrgPerson`) and drag it to the red dot of the subscribing object. The tool draws lines connecting to the objects and labels them Transformation1 and Transformation2 (see [Figure 6-14](#)).

**Figure 6-14 Topology Layout**



## Configuring the Topology Transformations

This section describes how to configure the RadiantOne topology transformation scripts. These scripts determine how the source data in the user repository is transformed before it is written to the policy database.

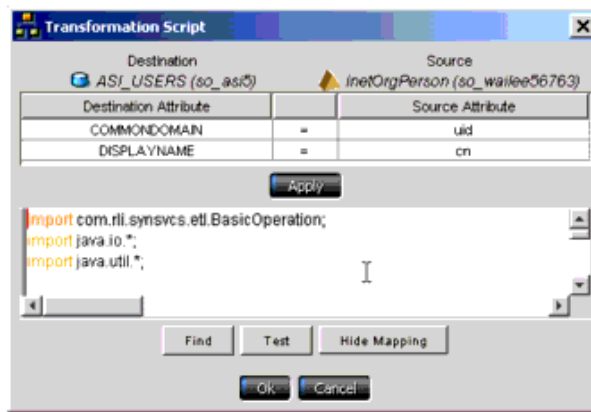
**Note:** The RadiantOne Synchronization Services tool is capable of very sophisticated transformations, including creating a unified identity from multiple sources. The transformation scripting language is Java. If you want to explore more sophisticated transformations or merging of identity data, refer to the RadiantOne documentation available in the RadiantOne installation directory.

The BEA WebLogic Enterprise Security product ships with sample user and group transformation scripts. They are located at `BEA_Home\wles42-admin\examples\r1syncservice`. The file names are `asi_users.djava` and `asi_groups.djava`. The samples are dynamic java scripts that are compiled and run by the RadiantOne Synchronization Services as part of its transformation runtime. The following procedure uses the `asi_groups.djava` sample script.

To configure the topology transformation scripts, perform the following steps:

1. On the RadiantOne Synchronization Services Administration console, right click Transformation1 and select Edit Script. The Transformation Script window is displayed (see [Figure 6-15](#)).

**Figure 6-15 Topology Script for Transformation1**



2. Set the `COMMONDOMAIN` and `DISPLAYNAME` attributes to `uid` and `cn` respectively as shown in [Figure 6-15](#), click **Apply**, and click **Ok**.
3. Right click `Transformation2` and select **Edit Script**. The **Transformation Script** window is displayed.
4. Position your cursor in the bottom region of the window, right click and select **load**. The **Open** window is displayed.
5. Locate the `asi_groups.djava` file in the `BEA_Home\wles42-admin\examples\r1syncservice` directory, select it and click **Open**, click **Apply**, and click **Ok**.
6. Click the **Topology** drop-down menu and click **Save** to save the topology.
7. This completes the configuration of the transformation topology.

## Uploading User and Group Data

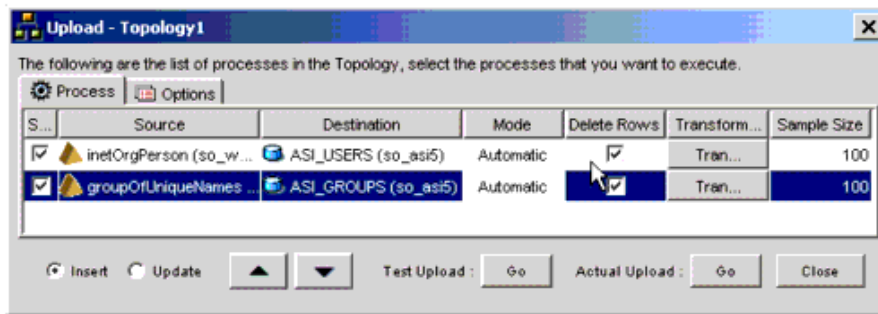
This section describes how to use the transformation topology to upload the user and group data from the source user repository to the policy database.

**Note:** This task serves to test all that all the configuration tasks you have performed up to this point have been performed correctly and that you can proceed to the next section, [Configuring Metadirectory Synchronization](#), and perform the synchronization tasks. If the upload fails, check the previous tasks to ensure that they were performed correctly. Also, verify that you used the correct passwords in each of the previous configuration tasks.

To upload the user and group data, perform the following steps:

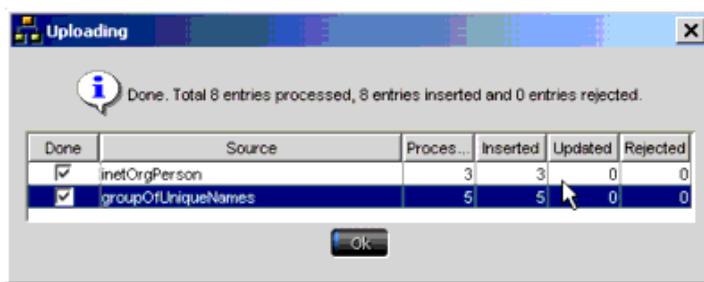
1. On the RadiantOne Synchronization Services Administration console, in the right pane, click the **Deployment** tab, click the folder icon, and open the topology that you just saved. The topology is displayed.
2. From the **Deployment** drop-down menu, select **Upload**. The upload topology page is displayed (see [Figure 6-16](#)).

**Figure 6-16 Upload Topology Page**



3. Check on both Delete Rows check boxes and click Test Upload. The Uploading page is displayed and indicates that the upload is successful (see [Figure 6-17](#)).

**Figure 6-17 Topology Uploading Page**



4. Click Ok
5. On the upload topology page, click Actual Upload (see [Figure 6-16](#)). The Uploading page is displayed again and indicates whether all entries were processed successfully.
6. Click Ok and on the Upload - Topology page, click close.
7. To verify that the upload actually moved user data into the designated WebLogic Enterprise Security identity directory, perform the following steps:
  - a. Go to the WebLogic Enterprise Security Administration Console and, in the left pane, open the Identity folder.
  - b. Click Groups and Users. The user data is displayed in the console.
8. This completes the user and group data upload.

## Configuring Metadirectory Synchronization

This section describes how to configure the metadirectory components for automatic updates to the policy database whenever changes are made to the user repository.

The RadiantOne Synchronization Services provides connectors and a synchronization hub that work together to synchronize data between various data sources. Connectors interface with the data sources. Data flows to and from the connectors asynchronously in the form of XML messages. All messages flow through the synchronization hub, which is a server that transforms the messages and routes them to the connectors that are subscribed to the changes. The BEA WebLogic JMS messaging broker manages the topics and provides guaranteed message delivery.

The role of the connectors is two fold. First, the connectors capture changes in the data source, translate the changes into a common XML format, and send them to the synchronization hub through the messaging server. Secondly, the connectors receive XML messages, translate them, and apply the changes to the data source.

To configure metadirectory synchronization, perform the following tasks:

- [Configuring the Synchronization Hub](#)
- [Configuring the Directory Connector](#)
- [Configuring the Policy Database Connectors](#)
- [Starting the Synchronization Hub](#)
- [Starting the Source and Destination Connectors](#)

## Configuring the Synchronization Hub

To configure the synchronization hub, set the parameters in the `RadiantOne_Home\r1syncsvcs\rlicon.ini` file to match the settings on the WebLogic Server. The require settings are shown in [Listing 6-1](#). This information is used by the RadiantOne Synchronization Services tool to contact the JMS server running on the WebLogic Enterprise Security Administration Server.

### Listing 6-1 Synchronization Hub Settings

```
...
[BEA]
JMS_SERVER_NAME=RLI_JMS_SERVER
JNDI_CLASS_NAME=weblogic.jndi.WLInitialContextFactory
CONNECTION_FACTORY_NAME=weblogic.asiAdminServer.jms.TopicConnectionFactory
URL=t3://localhost:7000
USER_NAME=system
USER_PASSWORD=weblogic
Msg Time-To-Live=3600000
RETRY_PERIOD=12
MAXIMUM ATTEMPTS = 11
```

## Configuring the Directory Connector

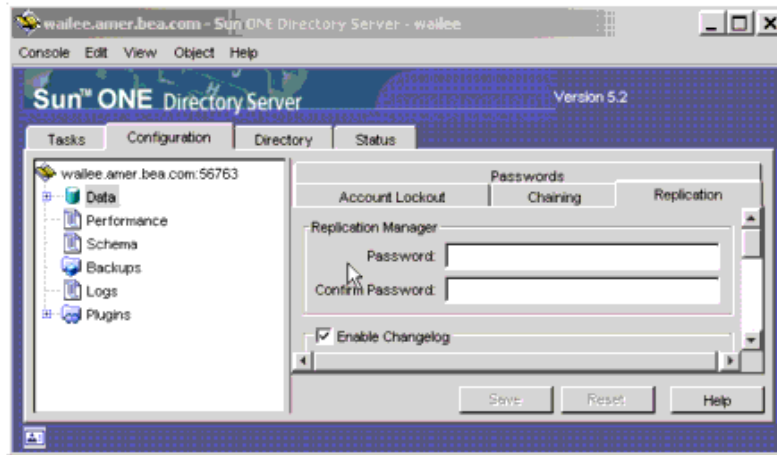
**Note:** This task is necessary only if you are using the Sun ONE Directory Server for your user repository. If you are using another type of user repository server, such as Active Directory, Windows NT, or a database, skip this section and go [Configuring the Policy Database Connectors](#). For more information on LDAP connector configuration requirements and procedures, see the *RadiantOne Synchronization Services Guide* located in the RadiantOne installation directory.

If you are using the Sun ONE Directory Server, you must configure the directory connector for so that changes to the user repository are automatically updated in the policy database.

To configure the directory connector, perform the following steps:

1. Click `Start>Programs>Sun ONE Server Products>Sun ONE Server Console 5.2` and log into the Directory Server Console using the `admin` User ID.
2. In the left pane, expand the Domain and Server Group nodes, and double-click the Directory Server for your directory server. The Directory Server Tasks page is displayed.
3. Click the Configuration tab, select the Data node in the left pane, and select the Replication tab. The Replication page is displayed (see [Figure 6-18](#)).

**Figure 6-18 Directory Server Replication Page**



4. Check the Enable Changelog check box and click Save.
5. In the left pane, open the Plugins folder, click Retro Changelog Plugin, check the Enable plugin check box, and click Save.

**Note:** If you are using an LDAP server other than iPlanet or you do not want to use the iPlanet changelog, Radiant Synchronization Services also has a polling connector. For information on configuring the other LDAP connectors, refer to the RadiantOne online documentation located in the RadiantOne installation directory.

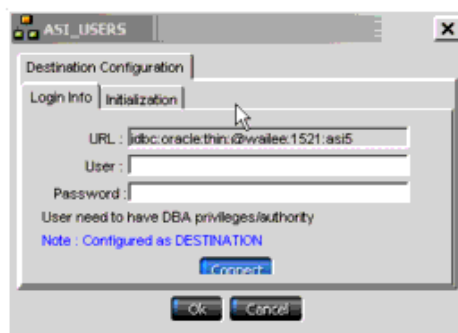
6. Click the Tasks tab and click Restart Directory Server to restart the server.
7. The completes configuration of the directory connector.

## Configuring the Policy Database Connectors

To configure the policy database connector, perform the following steps:

1. On the RadiantOne Synchronization Services Administration console, click the topology tab and open the topology.
2. Right-click the ASI\_USERS database object, and select Configure. The ASI\_USERS Destination Configuration page is displayed (see [Figure 6-19](#)).

**Figure 6-19 ASI\_USERS Destination Configuration Page**



**Note:** If the database object that the connector is listening to changes or is modified (for example, one of the data types changes or you add or remove columns), you can reconfigure the connector by right-clicking on the database object in the topology, and then choosing Configure. A note is

displayed on the Login Info tab that specifies how the connector is configured. Enter the user and password information and, on the Initialization tab, reconfigure the connector by either Applying the Script or Saving and executing it later.

3. Enter the user and password to connect to the database as the database administrator and click Connect. A "Connection Successful" dialog is displayed. Click Ok. A script is generated to create the `rli_con` user, the needed log tables, and triggers.
4. Click the Initialization tab, select the Apply Now radio button to generate log tables and triggers for the `ASI_USERS` database object, and click Apply. A "Configuration completed" dialog box is displayed. Click Ok.
5. Click Ok.
6. Repeat steps 2 through 5 for the `ASI_GROUPS` database object.
7. This completes the configuration of the policy database connectors.

## Starting the Synchronization Hub

To start the Synchronization Hub, perform the following steps:

1. On the RadiantOne Synchronization Services Administration console, click the Deployment drop-down menu, select Synchronization Hub, and click Start. The JMS Connection Username/Password dialog is displayed.
2. Enter the JMS connection username and password (if necessary) and click Ok. Use the same username/password that you used to log into the WebLogic Server Administration Console. A small window for the hub opens and indicates that the hub is running.

**Note:** You can also use the Start Hub icon on the Deployment Tab to start the hub.

## Starting the Source and Destination Connectors

To start the source and destination connectors, perform the following steps:

**Note:** The Synchronization Hub must be running before you start the connectors.

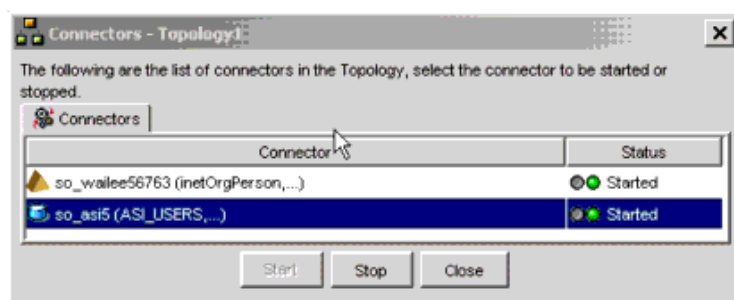
To start the Synchronization Hub, perform the following steps:

1. On the RadiantOne Synchronization Services Administration console, select the Deployment tab, click the folder icon, and select and open the Topology. The topology is displayed.

**Note:** You cannot modify the topology when you open it using the Deployment tab. To modify a topology you must open it using the Topology tab.

2. From the Deployment drop-down menu, and click Connectors. The Connectors - Topology dialog is displayed (see [Figure 6-20](#)).

**Figure 6-20 Connectors - Topology Page**



3. Select each connector and click Start. The connectors start. A small window for each connector opens and indicates that the connector is running.

**Note:** The connectors can also be started and stopped by clicking the Start Connector and Stop Connectors icons under the Deployment tab.


4. This completes configuration of metadirectory Synchronization.
- 


## Verifying that Metadirectory Synchronization Works

This section describes how to verify that metadirectory synchronization is properly configured such that changes to user and group entries in the user repository are reflected in the policy database.

To verify that metadirectory synchronization is properly configured, perform the following steps:

1. Use the user repository server to create a new user and add that user to the source group.
2. Open the Administration Console, open the Identity folder, the list of identity directories is displayed in the right pane.
3. Select the identity directory that you configured for automatic updates (for example, `ldapdir`), and click Users in the left pane. The new user is displayed in the list of users in the right pane.

 [back to top](#)

 [previous](#)

[next](#) 