

# Identity feed management

As administrator, you need to take a number of initial steps to take employee data from one or more human resources repositories and populate the IBM Tivoli Identity Manager registry with an equivalent set of users.

## Overview

An *identity* is the subset of profile data that uniquely represents a person in one or more repositories, and additional information related to the person. For example, an identity might be represented by unique combination of a person's first, last, and full name, and employee number. The data might also contain additional information such as phone numbers, manager, and e-mail address. A data source can be a customer's user repository or a file, a directory, or a custom source.

IBM Tivoli Identity Manager allows you to add a number of users to the system by reading a data source, such as a user repository, directory, file, or custom source. The process of adding users based on a user data repository is called an *identity feed*, or *HR feed*.

*Reconciliation* for an identity feed is the process of synchronizing the data between the data source and IBM Tivoli Identity Manager. The initial reconciliation populates IBM Tivoli Identity Manager with new users, including their profile data. A subsequent reconciliation both creates new users and also updates the user profile of any existing users that are found.

You can use several source formats to load identity records into the IBM Tivoli Identity Manager user registry.

You need to anticipate the effect of missing information in the user record. For example, if the record that you feed into IBM Tivoli Identity Manager has no e-mail address for the user, the user will not receive a password for a new account in an e-mail, and must call the help desk, or contact the manager.

## Common sources for identity feeds

IBM Tivoli Identity Manager supplies the following service types to handle many of the most common sources for identity feeds:

- Comma-Separated Value (CSV) identity feed
- DSML identity feed
- AD OrganizationalPerson identity feed (Microsoft Windows Active Directory)
- INetOrgPerson (LDAP) identity feed
- IDI data feed

You can populate initial content and subsequent changes to the content of the people registry from these sources:

### Comma-Separated Value (CSV) file

Use a comma-separated value (CSV) file. A CSV file contains a set of records separated by a carriage return/line (CR/LF) feed pair. Each record contains a set of fields separated by a comma. You can use a global identity policy to select the schema attributes that create a user ID.

### Directory Services Markup Language (DSML) v1 file

Use a DSML v1 file to populate the people registry. A DSML file represents directory structural information in an XML file format. If you run the identity

feed more than once, duplicate people are modified according to the newest file. A global identity policy does not apply to a DSML file.

### **Windows Server Active Directory**

From Windows Server Active Directory, importing only the information found in the inetOrgPerson schema portion of a Windows Server Active Directory user. You can use a global identity policy to select the schema attributes that create a user ID. The identity feed process uses all user objects in the under a specified base.

### **INetOrgPerson identity feed**

Use an LDAP directory server. The data uses the objectclass implied by the person profile name specified in the service definition. You can use a global identity policy to select the schema attributes that create a user ID. The identity feed process ignores records that do not have the specified objectclass.

### **Custom identity sources**

Use custom identity sources to populate initial content and subsequent changes to the content of the people registry. Depending on the identity source, you might use a global identity policy to select the schema attributes that create a user ID.

For example, use an IBM Tivoli Directory Integrator identity feed to obtain more flexibility than a standard data feed provides. Additional capabilities include:

- Working with a subset of data, such as filtering users in a given department
- Enabling additional attribute mapping beyond the standard mapping
- Enabling data lookups, such as the employee's manager, obtained from another data source
- Changing detection on the data source
- Using databases and human resource systems such as DB2 Universal Database<sup>™</sup> and SAP
- Controlling attributes; for example, updating status such as suspending a person
- Deleting identity records
- Initiating changes using IBM Tivoli Directory Integrator, instead of using IBM Tivoli Identity Manager reconciliations

For more information about providing customized identity feeds, refer to the information about IBM Tivoli Directory Integrator integration in the IBM Tivoli Identity Manager extensions directory.

## **Enabling workflow for identity feeds**

Regardless of the method used, the IBM Tivoli Identity Manager Server can be configured to call the workflow engine for identity feed records. Enabling the workflow engine will result in all applicable provisioning policies being enforced for incoming identities and will result in slower feed performance. Persons will be automatically enrolled in any applicable dynamic roles even if the workflow engine is not enabled for an identity feed. For initial loads, consider importing identities into the system and then enabling applicable provisioning policies to improve identity feed performance.

## Comma-Separated Value (CSV) identity feed

The Comma-Separated Value (CSV) identity feed provides capability for reading comma-separated value (CSV) file to add users to IBM Tivoli Identity Manager.

### CSV service type

This identity feed service type parses identity feeds using CSV file formats that comply with RFC 4180 grammar. The IBM Tivoli Identity Manager parser has the following RFC enhancements:

- Trims leading and trailing white space from unquoted text in a field. In contrast, RFC 4180 regards all space to be significant, whether inside or outside of quote delimiters.
- Allows quoted and unquoted text to be displayed in the same field. In contrast, RFC 4180 does not allow both text types in the same field.
- Does not enforce the RFC 4180 restriction that all records have the same number of fields. However, the code that calls the CSV parser reports an error if a record has more fields than the CSV header has.
- Permits record termination to use carriage return (CR) or to use carriage return/line feed (CR/LF) to be compatible with both UNIX and DOS base files. In contrast, RFC 4180 terminates all records with carriage return/line feed (CR/LF).

### Services that use CSV files

IBM Tivoli Identity Manager has the following types of services that use CSV files as input:

- CSV identity feed
- Custom services that use the Manual Service Provider type. These custom services use a CSV file format for the reconciliation upload file. This service type can be used for both identity and account feeds.

By default, all accounts defined in a CSV file for reconciliation of a manual service are marked as active in Tivoli Identity Manager. To suspend a person or account using a manual service reconciliation, add the `erpersonstatus` or the `eraccountstatus` attribute to the CSV file (depending on whether the feed is for identities or accounts). A value of 0 (zero) indicates active. A value of 1 indicates inactive.

- Custom services that use the Directory Integrator Adapter Provider type that use the IBM Tivoli Directory Integrator CSV connector. This service type can be used for both identity and account feeds.

### CSV file format

A CSV file contains a set of records separated by a carriage return/line feed (CR/LF) pair (`\r\n`), or by a line feed (LF) character. Each record contains a set of fields separated by a comma. If the field contains either a comma or a CR/LF, the comma must be escaped with double quotes as the delimiter. The first record in the CSV source file defines the attributes provided in each of the following records. For example:

```
uid,sn,cn,givenname,mail,initials,employeenumber,erroles
```

The `sn` and `cn` attributes are required by the object classes used by IBM Tivoli Identity Manager to represent a person. The identity feed process uses all objects in the file. The CSV file cannot contain binary attributes.

You might use a multi-valued attribute to specify a user who has membership in multiple groups, such as Service Owner, Windows Local Management (a self-defined group), and Manager group. If you include multi-valued attributes, they must be represented by using multiple columns with the same attribute name.

To specify multi-valued attributes, repeat the column the required number of times. For example:

```
cn, erroles, erroles, erroles, sn
cn1,role1, role2, role3, sn1
cn2,rolea,,sn2
```

If the record that you feed into IBM Tivoli Identity Manager has no e-mail address for the user, that user will not receive a notification e-mail containing the password for a new account, and must call the help desk or contact the manager.

## CSV connector for IBM Tivoli Directory Integrator

Information about the CSV connector for IBM Tivoli Directory Integrator is available in the following product directory:

*ITIM\_HOME/extensions/examples/idi\_integration/HRFeedCSV/ITDIFeedExpress*

## UTF-8 encoding in an identity feed file

Your identity feed file must be in UTF-8 format. You must use an editor that supports UTF-8 encoding.

- Windows

The following are UTF-8 capable: Microsoft Word 97 or later, or the Notepad editor that is included with the Windows 2003 Server or Windows XP operating systems.

To save a file in UTF-8 format using Notepad, click **File** → **Save As**. Then, expand the list of choices for the **Encoding** field and select UTF-8.

- Linux

The Vim text editor (a version of the classic vi editor) is UTF-8 capable. To work with files in UTF-8 format using the Vim text editor, specify the following:

```
:set encoding=utf-8
:set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
```

If your version of UNIX does not include this text editor, access this Web site:

<http://www.vim.org>

**Note:** For the 7-bit ASCII code subset, the UTF-8 encoded Unicode format is identical to 7-bit ASCII format. For input files that contain 7-bit ASCII (ASCII character values between hex 20 to hex 7e), you can use a normal text editor to create the file. For files containing any other character values (including extended European characters), you need to save the file in UTF-8 format.

For an exact list of the 7-bit ASCII characters as supported by UTF-8, access this Web site and click the **Basic Latin** link in the first column:

<http://www.unicode.org/charts>

## Directory Services Markup Language (DSML) identity feed

The Directory Services Markup Language (DSML) identity feed provides capability for reading a DSML file to add users to IBM Tivoli Identity Manager.

## DSML service type

The IBM Tivoli Identity Manager Server allows for integration of various human resource (HR) type data feeds to add large numbers of individuals to the IBM Tivoli Identity Manager Server without manually adding each individual. An identity record in HR data becomes an instance of a person object in IBM Tivoli Identity Manager. One type of HR type data feed is the DSML Identity Feed service.

The HR data handling mechanisms in IBM Tivoli Identity Manager requires that the HR data be in an XML format, using the standard schema defined by the Directory Services Markup Language (DSML version 1). For more information about DSMLv1, refer to the DSML Web site at <http://www.oasis-open.org>.

## DSML file format

DSML is an XML format that describes directory information. A *DSML file* represents directory structure information in an XML file format. The DSML file must contain only valid attributes of the IBM Tivoli Identity Manager profile. The identity feed process uses all objects in the file.

The `erPersonPassword` attribute is used in an identity feed only during a Person create process, not in a Person modify process. If the value of the `erPersonPassword` attribute is set, then the IBM Tivoli Identity Manager account password will be set to that value when the person and account are created. The following statement sets a value for the `erPersonPassword` attribute:

```
<attr name="erpersonpassword"><value>panther2</value></attr>
```

If you select a DSML file format for an identity feed, you will need to specify a DSML file similar to this one:

```
<entry dn="uid=sparker">
<objectclass><oc-value>inetOrgPerson</oc-value></objectclass>
<attr name="givenname"><value>Scott</value></attr>
<attr name="initials"><value>SVP</value></attr>
<attr name="sn"><value>Parker</value></attr>
<attr name="cn"><value>Scott Parker</value></attr>
<attr name="telephonenumber"><value>(919) 321-4666</value></attr>
<attr name="postaladdress"><value>222 E. First Street Durham, NC 27788</value></attr>
</entry>
```

## UTF-8 encoding in an identity feed file

Your identity feed file must be in UTF-8 format. You must use an editor that supports UTF-8 encoding.

- Windows

The following are UTF-8 capable: Microsoft Word 97 or later, or the Notepad editor that is included with the Windows 2003 Server or Windows XP operating systems.

To save a file in UTF-8 format using Notepad, click **File** → **Save As**. Then, expand the list of choices for the **Encoding** field and select UTF-8.

- Linux

The Vim text editor (a version of the classic vi editor) is UTF-8 capable. To work with files in UTF-8 format using the Vim text editor, specify the following:

```
:set encoding=utf-8
:set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
```

If your version of UNIX does not include this text editor, access this Web site:

<http://www.vim.org>

**Note:** For the 7-bit ASCII code subset, the UTF-8 encoded Unicode format is identical to 7-bit ASCII format. For input files that contain 7-bit ASCII (ASCII character values between hex 20 to hex 7e), you can use a normal text editor to create the file. For files containing any other character values (including extended European characters), you need to save the file in UTF-8 format.

For an exact list of the 7-bit ASCII characters as supported by UTF-8, access this Web site and click the **Basic Latin** link in the first column:

<http://www.unicode.org/charts>

## Importing HR data using reconciliation

HR data can be imported into the IBM Tivoli Identity Manager Server from a file written in DSML, using the DSML Identity Feed service provider.

### Before you begin

Depending on how your system administrator has customized your system, you might not have access to this task. To get access to this task, or to have someone complete this task for you, contact your system administrator.

In a cluster environment, the DSML file should be present on all cluster member machines at the same location. This is done so that when performing a reconciliation, the DSML file can be found regardless of which cluster member initiates the reconciliation.

The DSML file needs to be present on the Tivoli Identity Manager Server machine for a single server setup.

### About this task

When you use the DSML Identity Feed Service to import HR data from a DSML file, only the add and modify person operations are performed. The delete person operation is not available when importing identity record information from a DSML file.

**Note:** When processing identity record information from a DSML file, it is assumed that the data set reconciled does not represent the entire person population for the Tivoli Identity Manager Server. Because of this assumption, the polling method can be used to add or modify persons, but not delete them. To delete persons, the event notification interface must be used.

To import the HR data using the DSML Identity Feed service type, complete these steps:

1. Create an instance of the DSML Identity Feed service.
2. Configure the service to refer to a DSML file that contains the identity record data. Specify the full path name to the DSML file. Use the service test feature to verify that the file name is correct.
3. Reconcile the service.

### Results

When reconciling the DSML Identity Feed service, the identity record entries are read from the DSML file. For each identity record entry, the objectclass is matched up to

the appropriate person profile in IBM Tivoli Identity Manager. If a match is made, the distinguished name (dn) is converted into a search filter. The search filter looks for an existing match to a person entry that already exists in the organization that contains the service. If a single match is found, then the person entry is used as an update to the existing entry. If no match is found, the individual is added as a new person entry. Duplicate matches return an error and the entry is not added.

## Example

This is a sample of a DSML entry for a person:

```
<entry dn="uid=jsmith">
  <objectclass>
    <oc-value>inetOrgPerson</oc-value>
  </objectclass>
  <attr name="sn"><value>smith</value></attr>
  <attr name="uid"><value>jsmith</value></attr>
  <attr name="mail"><value>jsmith@IBM.com</value></attr>
  <attr name="givenname"><value>John</value></attr>
  <attr name="cn"><value>John Smith</value></attr>
</entry>
```

## What to do next

You can now add, modify, and delete identity information using the Tivoli Identity Manager interface.

You can add more users, modify existing users using the DSML file, and deleting users.

### DSML identity feed service form:

The fields on the DSML identity feed service form are used to specify information about the Directory Services Markup Language (DSML) identity feed. If you select a service profile to import identity data using DSML, complete the fields on the form to connect to the server where the service resides.

The following fields are available on the DSML identity feed service form:

#### Service name

Specify a name that helps you identify the service instance.

#### Description

Specify additional information about the service instance.

#### User ID

Specify the administrative user ID for the service instance.

#### Password

Specify the administrative password for the service instance. If password authentication is used, enter a value. Otherwise, reconciliation later fails.

#### File name

Specify the file name, including the path name, that contains the user information.

**Note:** In cluster environments, the file must be stored at the same location on all cluster members.

#### Use workflow

Select this check box to use workflow for this service instance and to determine



whether or not to automatically create accounts for entries. This feature can be

used for small incremental feeds, but not for importing large amounts of data.

### Placement rule

Specify a rule to be used for placing a user (person) in the organization tree. This rule is defined using a script, in which the context is the identity information for the current user in the feed and the service that defines the feed itself.

### Sample DSML file for reconciliation:

Use this example as a model for creating the DSML file you want to use to import HR data using reconciliation.

### Sample

The following DSML file is a complete sample XML for use in reconciliation:

```
<?xml version="1.0" encoding="UTF-8"?>
<dsml>

  <directory-entries>
    <entry dn="uid=janesmith">
      <objectclass>
        <oc-value>inetOrgPerson</oc-value>
      </objectclass>
      <attr name="ou"><value>Engineering</value></attr>
      <attr name="sn"><value>Smith </value></attr>
      <attr name="uid"><value>janesmith</value></attr>
      <attr name="mail"><value>j.smith@ibm.com</value></attr>
      <attr name="givenname"><value>Jane</value></attr>
      <attr name="cn"><value>Jane Smith</value></attr>
      <attr name="initials"><value>JS</value></attr>
      <attr name="employeenumber"><value>E_1974</value></attr>
      <attr name="title"><value>Research and Development</value></attr>
      <attr name="telephonenumber"><value>(888) 555-1614</value></attr>
      <attr name="mobile"><value>(888) 555-8216</value></attr>
      <attr name="homepostaladdress"><value>15440 Laguna Canyon Rd, Irvine, CA 92614</value></attr>
      <attr name="roomnumber"><value>G-114</value></attr>
      <attr name="homephone"><value>(888) 555-3222</value></attr>
      <attr name="pager"><value>(888) 555-7756</value></attr>
      <attr name="erAliases">
        <value>j.smith</value>
        <value>jane_smith</value>
        <value>JaneSmith</value>
      </attr>
      <attr name="erRoles">
        <value>Engineering</value>
        <value>Development</value>
      </attr>
    </entry>
    <entry dn="uid=johndoe">
      <objectclass>
        <oc-value>inetOrgPerson</oc-value>
      </objectclass>
      <attr name="ou"><value>Sales-West</value></attr>
      <attr name="sn"><value>Doe</value></attr>
      <attr name="uid"><value>johndoe</value></attr>
      <attr name="mail"><value>j.doe@ibm.com</value></attr>
      <attr name="givenname"><value>John</value></attr>
      <attr name="cn"><value>JohnDoe</value></attr>
      <attr name="initials"><value>JD</value></attr>
      <attr name="employeenumber"><value>S_1308</value></attr>
      <attr name="title"><value>Sales Engineer</value></attr>
      <attr name="telephonenumber"><value>(888) 555-1620</value></attr>
      <attr name="mobile"><value>(888) 555-8210</value></attr>
      <attr name="homepostaladdress"><value>15440 Laguna Canyon Rd, Irvine, CA 92614</value></attr>
      <attr name="roomnumber"><value>G-120</value></attr>
      <attr name="homephone"><value>(888) 555-3228</value></attr>
      <attr name="pager"><value>(888) 555-7750</value></attr>
      <attr name="erAliases">
        <value>j.doe</value>
        <value>john_doe</value>
        <value>JohnDoe</value>
      </attr>
    </entry>
  </directory-entries>
</dsml>
```



```

    <attr name="erRoles">
      <value>Sales</value>
    </attr>
  </entry>

</directory-entries>

</dsml>copy from here to there

```

## AD Organizational identity feed

AD Organizational identity feed provides capability for creating users based on user records from Windows Server Active Directory (AD).

This feed allows you to use a directory resource as the source for the feed. Information from the AD `organizationalPerson` objectclass is mapped to the `inetOrgPerson` schema. This identity feed loads all user objects under a specified base.

## AD Organizational service type

When you create a service instance for this identity feed, the following information is required:

- URL used to connect to the directory resource
- User ID and password to gain access to the resource
- Naming context, which is the search base in LDAP terminology, and defines where in the directory tree to begin the search
- Name attribute, which must be selected from the values that are provided

After creation, this service is set to reconcile a specific branch of the directory.

## Customized attribute mapping

The **Attribute Mapping file name** option provides a way to customize the mapping of LDAP attributes to IBM Tivoli Identity Manager attributes.

The format of the attribute mapping file is `feedAttrName=itimAttrName`. Lines that begin with a pound sign (#) or semicolon (;) are interpreted as comments.

The attribute mapping file completely overrides the default mappings. All attributes that are needed from the feed source must be included in the mapping file.

These attributes must be included in the mapping file:

- Attributes that are specified as required in the person profile form
- Attributes that are specified as required in the LDAP schema for the target person profile

If an attribute from the feed source is not included in the attribute mapping file, the value is not set on the IBM Tivoli Identity Manager attribute.

The following example shows six attributes being mapped. All other LDAP attributes are ignored.

```

#feedAttrName=itimAttrName
cn=cn
sn=sn title=title
telephonenumber=mobile
mail=mail
description=description

```

## UTF-8 encoding in an identity feed file

Your identity feed file must be in UTF-8 format. You must use an editor that supports UTF-8 encoding.

- Windows

The following are UTF-8 capable: Microsoft Word 97 or later, or the Notepad editor that is included with the Windows 2003 Server or Windows XP operating systems.

To save a file in UTF-8 format using Notepad, click **File** → **Save As**. Then, expand the list of choices for the **Encoding** field and select UTF-8.

- Linux

The Vim text editor (a version of the classic vi editor) is UTF-8 capable. To work with files in UTF-8 format using the Vim text editor, specify the following:

```
:set encoding=utf-8
:set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
```

If your version of UNIX does not include this text editor, access this Web site:

<http://www.vim.org>

**Note:** For the 7-bit ASCII code subset, the UTF-8 encoded Unicode format is identical to 7-bit ASCII format. For input files that contain 7-bit ASCII (ASCII character values between hex 20 to hex 7e), you can use a normal text editor to create the file. For files containing any other character values (including extended European characters), you need to save the file in UTF-8 format.

For an exact list of the 7-bit ASCII characters as supported by UTF-8, access this Web site and click the **Basic Latin** link in the first column:

<http://www.unicode.org/charts>

## inetOrgPerson identity feed

The inetOrgPerson identity feed supports LDAP directory server using the RFC2798 (inetOrgPerson LDAP objectclass).

This feed allows you to use a directory resource as the source for the feed. This identity feed loads all inetOrgPerson objects under a specified base. Records that do not have objectclass=inetOrgPerson are ignored.

### inetOrgPerson service type

When you create a service instance for this identity feed, the following information is required:

- URL used to connect to the directory resource
- User ID and password to gain access to the resource
- Naming context, which is the search base in LDAP terminology, and defines where in the directory tree to begin the search.
- Name attribute, which must be selected from the values that are provided

After creation, this service is set to reconcile a specific branch of the directory.

## Customized attribute mapping

The **Attribute Mapping file name** option provides a way to customize the

mapping of LDAP attributes to IBM Tivoli Identity Manager attributes.

The format of the attribute mapping file is `feedAttrName=itimAttrName`. Lines that begin with a pound sign (#) or semicolon (;) are interpreted as comments.

The attribute mapping file completely overrides the default mappings. All attributes needed from the feed source must be included in the mapping file. Attributes that are specified as required in the person profile form or LDAP schema for the target person profile are required to be in the mapping file. If an attribute from the feed source is not included in the attribute mapping file, the value is not set on the IBM Tivoli Identity Manager attribute.

The following example shows six attributes being mapped. All other LDAP attributes are ignored.

```
#feedAttrName=itimAttrName
cn=cn
sn=sn title=title
telephonenumber=mobile
mail=mail
description=description
```

## UTF-8 encoding in an identity feed file

Your identity feed file must be in UTF-8 format. You must use an editor that supports UTF-8 encoding.

- Windows

The following are UTF-8 capable: Microsoft Word 97 or later, or the Notepad editor that is included with the Windows 2003 Server or Windows XP operating systems.

To save a file in UTF-8 format using Notepad, click **File** → **Save As**. Then, expand the list of choices for the **Encoding** field and select UTF-8.

- Linux

The Vim text editor (a version of the classic vi editor) is UTF-8 capable. To work with files in UTF-8 format using the Vim text editor, specify the following:

```
:set encoding=utf-8
:set guifont=-misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
```

If your version of UNIX does not include this text editor, access this Web site:

<http://www.vim.org>

**Note:** For the 7-bit ASCII code subset, the UTF-8 encoded Unicode format is identical to 7-bit ASCII format. For input files that contain 7-bit ASCII (ASCII character values between hex 20 to hex 7e), you can use a normal text editor to create the file. For files containing any other character values (including extended European characters), you need to save the file in UTF-8 format.

For an exact list of the 7-bit ASCII characters as supported by UTF-8, access this Web site and click the **Basic Latin** link in the first column:

<http://www.unicode.org/charts>

## IBM Tivoli Directory Integrator (IDI) data feed

The IBM Tivoli Directory Integrator (IDI) identity feed is used to support data feeds from custom identity sources, and to provide greater flexibility over the standard data feeds.

The IDI data feed is provided for instances where the other HR feeds are not sufficient. It provides the ability to define custom identity feeds.

Use of this data feed requires knowledge of IBM Tivoli Directory Integrator (IDI). This

data feed is used to provide greater flexibility over the standard data feeds.

Examples of this flexibility include:

- Ability to work with a subset of data, such as filtering users in a given department
- Additional attribute mapping beyond the one-to-one mapping provided by the standard feeds
- Data lookups, such as to derive a supervisor or manager from another data source
- Change detection on the data source
- Databases and HR systems, such as DB2, Oracle, Peoplesoft, SAP
- Control over attributes, such as updating status or suspending a person
- Deletion of people
- Changes driven by IBM Tivoli Directory Integrator instead of by IBM Tivoli Identity Manager reconciliations (used for deletions, updates, and change detection)

## UTF-8 encoding in an identity feed file

Your identity feed file must be in UTF-8 format. You must use an editor that supports UTF-8 encoding.

- Windows

The following are UTF-8 capable: Microsoft Word 97 or later, or the Notepad editor that is included with the Windows 2003 Server or Windows XP operating systems.

To save a file in UTF-8 format using Notepad, click **File** → **Save As**. Then, expand the list of choices for the **Encoding** field and select UTF-8.

- Linux

The Vim text editor (a version of the classic vi editor) is UTF-8 capable. To work with files in UTF-8 format using the Vim text editor, specify the following:

```
:set encoding=utf-8
```

```
:set guifont=misc-fixed-medium-r-normal--18-120-100-100-c-90-iso10646-1
```

If your version of UNIX does not include this text editor, access this Web site:

<http://www.vim.org>

**Note:** For the 7-bit ASCII code subset, the UTF-8 encoded Unicode format is identical to 7-bit ASCII format. For input files that contain 7-bit ASCII (ASCII character values between hex 20 to hex 7e), you can use a normal text editor to create the file. For files containing any other character values (including extended European characters), you need to save the file in UTF-8 format.

For an exact list of the 7-bit ASCII characters as supported by UTF-8, access this Web site and click the **Basic Latin** link in the first column:

<http://www.unicode.org/charts>

## Managing identity information with IBM Tivoli Directory Integrator

You can use IBM Tivoli Directory Integrator to import identity information into IBM Tivoli Identity Manager and to manage accounts on external resources in the IBM Tivoli Identity Manager data store. Identity data can come from a human resources repository or

an alternate source, such as a company-wide directory. An identity record in HR data becomes an instance of a person object in IBM Tivoli Identity Manager. Integration with IBM Tivoli Directory Integrator requires network connectivity with the IBM Tivoli Identity Manager system and a new service type to manage data feeds.

Advantages of using IBM Tivoli Directory Integrator include the following:

- Avoiding the need for custom programming to manipulate raw personal information data into a form that can be imported into IBM Tivoli Identity Manager. For example, IBM Tivoli Directory Integrator can be used to parse data from a comma separated file or a database and feed the result into IBM Tivoli Identity Manager as personal information data or changes to that data. Previously, a Directory Services Markup Language (DSML) file or custom Java Naming and Directory Interface (JNDI) client was required.
- Managing identity data in which IBM Tivoli Identity Manager can act as a DSMLv2 client to retrieve person data from IBM Tivoli Directory Integrator in reconciliation by executing searches against IBM Tivoli Directory Integrator, which acts as a DSMLv2 server. IBM Tivoli Identity Manager can also act as a DSMLv2 server, accepting requests from a DSMLv2 client such as IBM Tivoli Directory Integrator, using the JNDI service provider.

**Note:** DSMLv2 is deprecated in IBM Tivoli Identity Manager Version 5.0 in favor of the remote method invocation (RMI)-based IDI adapter framework. DSMLv2 will still continue to be supported in this release.

- Providing advantages in account management. For more information, refer to additional documentation in the extensions directory.

For more information, refer to additional documentation provided by the IBM Tivoli Directory Integrator product. For examples of customizing schemas and importing data in an identity data feed, navigate to the *ITIM\_HOME/extensions/examples* directory.

### **Scenario: bulk loading identity data**

A typical scenario for the use of IBM Tivoli Directory Integrator might be an administrator who is interested in bulk loading identity data into IBM Tivoli Identity Manager.

#### **Before you begin**

Depending on how your system administrator has customized your system, you might not have access to this task. To get access to this task, or to have someone complete this task for you, contact your system administrator.

An instance of Tivoli Directory Integrator must be running.

#### **About this task**

This scenario includes the following high-level tasks:

1. Setting up the Tivoli Directory Integrator configuration, including a DSMLv2 event handler and an assembly line with a connector to the desired data source.
2. Starting the Tivoli Directory Integrator event handler.
3. Setting up a Tivoli Identity Manager service to communicate with the Tivoli Directory Integrator configuration.
4. Performing the reconciliation to initiate the communication.

## Results

These events occur after the reconciliation:

1. Tivoli Identity Manager sends a search request message to Tivoli Directory Integrator, which searches the enterprise data store for the identity data.
2. Tivoli Directory Integrator sends the data back to Tivoli Identity Manager, which processes the data. This processing includes evaluation of the position in the organization tree in which to place people, evaluation of role membership, evaluation of a supervisor relationship, possibly evaluation of provisioning policy, and insertion of data into the Tivoli Identity Manager data store. Evaluation of the provisioning policy could result in account management actions.
3. The identity information is loaded into Tivoli Identity Manager from the enterprise data store.

## What to do next

You can now add, modify, and delete identity information using the Tivoli Identity Manager interface.

For additional scenarios and other information on the use of Tivoli Directory Integrator, refer to the extensions directory for the descriptions of the following:

- Identity feed using JNDI
- End user account management
- Account event notification

## Identity feeds that retain group membership

Ensure that identity feeds retain a user's membership in both customized and default groups.

All default IBM Tivoli Identity Manager groups initially have no members, except for the administrator group, which contains one user whose account is named itim manager. When you load the first identity records into IBM Tivoli Identity Manager, some individuals might become members of the manager group.

*Table 48. Group membership after initial identity feed*

Group name	Membership
Administrator	itim manager
Manager	Zero or more, depending on whether the initial identity feed has an identity record that indicates the user has a
Service owner	Zero
Help desk	Zero

The first help desk assistant and first service owner is a user that the administrator explicitly adds to the group. Alternatively, a user automatically gains membership in the service owner group if you specify the user as owner of a service. If you specify the user as the manager of another user, a user automatically gains membership in the manager group.

A user who is a member of a customized group must also be a member of the default group of the same category, or processing results are unpredictable.

If the incoming identity record for a user initially indicates membership in a customized group, Tivoli Identity Manager includes the user as a member of both the customized group and the default group of the same category. Tivoli Identity Manager interprets a subsequent identity feed that includes the same user as a modification of the existing Tivoli Identity Manager user. If the subsequent identity feed specifies that the user has membership only in the customized group, and not also in the default group of the same category, the user is removed from membership in the default group. To avoid this problem, ensure that both initial and subsequent identity feeds specify that a user has membership in both a customized and the default group of the same category.

## Map of inetOrgPerson to Windows Server Active Directory attributes

The IBM Tivoli Identity Manager inetOrgPerson attributes map to Windows Server Active Directory attributes. The differences are shown in **boldface** type.

*Table 49. Map of inetOrgPerson and Windows Server Active Directory organizationalPerson attributes*

IBM Tivoli Identity Manager inetOrgPerson attributes	Windows Server Active Directory organizationalPerson attributes
cn	cn
departmentNumber	<b>department</b>
description	<b>comment</b>
employeeNumber	<b>employeeID</b>
givenName	givenName
homePhone	homePhone
homePostalAddress	homePostalAddress
initials	initials
internationaliSDNNumber	internationaliSDNNumber
jpegPhoto	<b>thumbnailPhoto</b>
l	l
mail	mail
manager	manager
mobile	mobile
o	o
ou	ou
pager	pager
physicalDeliveryOfficeName	physicalDeliveryOfficeName
postalAddress	postalAddress
postalCode	postalCode
postOfficeBox	postOfficeBox
preferredDeliveryMethod	preferredDeliveryMethod
secretary	<b>assistant</b>
seeAlso	seeAlso
sn	sn



Table 49. Map of *inetOrgPerson* and Windows Server Active Directory *organizationalPerson* attributes (continued)

IBM Tivoli Identity Manager <i>inetOrgPerson</i> attributes	Windows Server Active Directory <i>organizationalPerson</i> attributes
st	st
street	<b>streetaddress</b>
telephoneNumber	telephoneNumber
teletexTerminalIdentifier	teletexTerminalIdentifier
telexNumber	telexNumber
title	title
uid	< - intentionally blank - >
userPassword	userPassword <b>Note:</b> Encryption by the directory server prevents IBM Tivoli Identity Manager from using the value of this attribute.
x121Address	x121Address

## User passwords provided by an identity feed

Encryption by the directory server prevents IBM Tivoli Identity Manager from using the `userPassword` attribute in the `inetOrgPerson` schema to provide user password data in an `inetOrgPerson` identity feed from LDAP or a Windows Server Active Directory identity feed.

Other identity feeds that use CSV, DSML, or IBM Tivoli Directory Integrator-based formats can provide a password for a new user. Given the identity feed value, IBM Tivoli Identity Manager uses the `erPersonPassword` attribute to create a password for a new user's IBM Tivoli Identity Manager account. The `erPersonPassword` attribute is used only to create a password for a new IBM Tivoli Identity Manager user. If the user already exists, the value of the `erPersonPassword` attribute cannot be used to change the IBM Tivoli Identity Manager user's login password.

In any identity feed where the `erPersonPassword` is not provided, IBM Tivoli Identity Manager generates a new password for a new user and sends the generated password by e-mail to the new user. If the user's e-mail address is not populated, the user must contact the help desk to obtain a password. Depending your site requirements, the new user's password might also be sent to the user's manager.

The password value that IBM Tivoli Directory Integrator provides must be encoded in base64 format.

These identity feed attributes provide a value in clear text that is the password for a new user:

- CSV column name: `erPersonPassword`
- DSML tag: `erPersonPassword`

## Attributes in an identity feed that are not in a schema

You can include some attributes in an identity feed that are not contained in the identity feed object class (`organizationalPerson` for Windows Server Active Directory; `inetOrgPerson` for IBM Tivoli Identity Manager).

For example, the `erRoles` attribute determines a user's membership in a IBM Tivoli Identity Manager group. The `erRoles` attribute is not in either the `organizationalPerson` or the `inetOrgPerson` schema. Based on the value of the `erRoles` attribute in an initial identity feed, a user might become a member, for example, of a customized and a default Help Desk Assistant group.

If a repeated identity feed does not contain a value for an attribute that was previously specified for the user, for both `organizationalPerson` and `inetOrgPerson` schemas, the identity feed process will delete that attribute for the IBM Tivoli Identity Manager user.

If the incoming identity record for a user initially indicates membership in a customized group, Tivoli Identity Manager includes the user as a member of both the customized group and the default group of the same category. Tivoli Identity Manager interprets a subsequent identity feed that includes the same user as a modification of the existing Tivoli Identity Manager user. If the subsequent identity feed specifies that the user has membership only in the customized group, and not also in the default group of the same category, the user is removed from membership in the default group. To avoid this problem, ensure that both initial and subsequent identity feeds specify that a user has membership in both a customized and the default group of the same category.

For the Windows Server Active Directory feed, this problem also occurs for any `inetOrgPerson` attribute that is not also contained in the `organizationalPerson` schema. For an `inetOrgPerson` identity feed, the problem occurs for any `inetOrgPerson` attribute that is not supported by the identity feed.

## Supported formats and special processing of attributes

IBM Tivoli Identity Manager provides special processing for manager and secretary attributes, and for the `erRoles` attribute.

### Supported formats and special processing for manager and secretary attributes

The manager and secretary attributes refer to another person entry within IBM Tivoli Identity Manager.

**Note:** The Windows Server Active Directory identity feed maps the Windows Server Active Directory assistant attribute to the secretary attribute.

Internally, IBM Tivoli Identity Manager uses a special format for the Distinguished Name (DN) of person directory entries, which is inconvenient and difficult to specify in the identity feed data. So the identity feed code allows these attributes to be specified in more user friendly formats. IBM Tivoli Identity Manager supports three formats for the values:

- A search filter (containing an equal (=) operator, but not `erglobalid`). This should be a comma-separated list of attribute=value pairs.
- A simple name (not containing an equal (=) operator), which is assumed to be the value of the naming attribute for the person object class (that is, `cn`).
- A full IBM Tivoli Identity Manager DN (containing an equal (=) operator and `erglobalid`), which must exactly match the IBM Tivoli Identity Manager LDAP DN of one of the currently defined person objects.

For the first two cases, IBM Tivoli Identity Manager converts the value to an LDAP search filter, and does a subtree search of the organization to find a unique matching person. If this returns zero matches, or more than one match, then the value is considered invalid, and is removed from the list. A suitable warning message is written to the IBM Tivoli Identity Manager log.

A potential issue can occur with both the manager and secretary attributes if they reference a person who is also defined in the same feed. In this case, it is possible that when the attribute value is processed as above, the person that it references has not yet been created. This can occur even if the manager or secretary person is defined earlier in the identity feed file, because of the multithreaded and asynchronous processing done by IBM Tivoli Identity Manager during an identity feed. This situation will result in the attribute being deleted from the person, because the attribute references an invalid person, with a warning being written to the logs.

There are two solutions to this reference dependency issue. First, execute the identity feed a second time, after all processing has completed from the first run. Note that this second feed should be much faster, because only entries that have changed will result in any significant processing during the feed. Alternatively, define these people (managers and secretaries) in a separate identity feed file. Run that identity feed first, then run the main feed after the first feed has fully completed. If this separate, first feed also contains entries that reference managers that are defined in the same feed, the separate, first feed may need to be run twice, or split again.

Note that asynchronous workflow activities to create or modify people may still be running, even after the identity feed status appears to be completed. In this case, you must wait for an additional interval of time after the first feed appears to be complete, before submitting the second feed.

## **Supported formats and special processing for erRoles attribute values**

The erRoles attribute is used to specify the list of roles to which a person belongs. In IBM Tivoli Identity Manager, groups are equivalent to roles that IBM Tivoli Identity Manager, as an enterprise product, provides. IBM Tivoli Identity Manager uses the erRoles attribute to specify the groups to which a user belongs. For example, specifying an identity feed attribute erRoles with a value of Help Desk Assistant will result in the user belonging to the Help Desk Assistant group. The erRoles attribute can be multi-valued.

These formats are supported:

- A simple name (not containing an equals (=) operator), which is assumed to be the value of the erRoleName attribute. IBM Tivoli Identity Manager does a subtree search to find a unique matching static role. The name is not valid if zero or more than one role is a match.
- A full IBM Tivoli Identity Manager DN, which must exactly match the IBM Tivoli Identity Manager LDAP DN of one of the currently defined static roles.

Any invalid value is removed from the value list. If this results in zero remaining values, the attribute is removed from the attribute list. A suitable warning message is written to the log.

## **Modifiable schema classes and attributes**

You can modify some IBM Tivoli Identity Manager schema classes and attributes.

You can create new classes with names that begin with the characters er, a prefix that previously was reserved for IBM Tivoli Identity Manager schema classes and attributes.

The IBM Tivoli Identity Manager schema classes and attributes that you can modify have a unique object identifier (OID) prefix. An OID is a string of numbers that identifies a unique class in an LDAP schema. The IBM Tivoli Identity Manager

schema classes and attributes that remain read-only have the following OID prefix:  
1.3.6.1.4.1.6054.1.1

## Person naming and organization placement

When the IBM Tivoli Identity Manager Server imports HR data, the server creates Distinguished Names (DN) for each identity record and places the person in a specific organizational unit based on the information provided.

For the IBM Tivoli Identity Manager Server to uniquely identify and place each individual, each entry (or person) must organize its data in a way that the IBM Tivoli Identity Manager Server can recognize the individual pieces (attributes). The IBM Tivoli Identity Manager Server must also be configured to recognize attributes that are passed. This is done by matching the objectclass attribute against the defined person profiles. By default, the LDAP standard inetOrgPerson objectclass is expected.

### Determining the placement of the person

The IBM Tivoli Identity Manager Server determines where in the organization chart a person should be placed through the use of a placement rule defined in the DSML Identity Feed service.

For example, if a person is defined as a member of the marketing department in the identity source, the placement rule instructs the server to place the person in the marketing department in the IBM Tivoli Identity Manager organization chart. This rule is used for initial placement of persons during an add operation, as well as for moving a person to a different location during a modify operation.

**Note:** Organization names returned by placement rules must be unique within the context of the service unless an organization path is used to specify an organization container. If an organization path is provided by the placement rule, the organization name must be unique within that organization container.

Placement rules are written with JavaScript that returns the organization path in a distinguished name (DN) format. This information is used to search for an organizational unit in which to place a person. This DN indicates the required organization path relative to the organization base. The syntax of this path can be represented with the following pseudo BNF notation:

```
orgDn ::= orgRdn | orgRdn "," orgDn
orgRdn ::= prefix '=' name
prefix ::= 'l' | 'o' | 'ou'
name ::= string
```

where `string` is the textual value, `l` is location, `o` is organization, and `ou` is the organizational unit, business partner organization, or Admin Domain.

**Note:** The prefixes noted here are the default values. If the customer uses a different schema, then these prefixes are the values mapped in entity configuration.

### Example

To illustrate, examine the following organization chart:

```
IBM (organization)
  Marketing (organizational unit)
  Facilities (organizational unit)
    Irvine (location)
```

The path for the Marketing department is ou=Marketing, o=IBM. The path for the Irvine Facilities department is l=Irvine, ou=Facilities, o=IBM.

The JavaScript function simply returns a string in this format, but omits the organization. The attributes of the identity record from the identity source can be retrieved from the JavaScript code to construct the path. Because of the programming flexibility provided by JavaScript code, the information used from the identity source can be manipulated in several ways. Programming constructs such as switch statements can be used to map specific organization names to different paths in the server. String manipulation can be used to tokenize or concatenate names to derive paths also, so for example, a string of IBM/Facilities/Irvine could be tokenized and reconstructed in DN format as l=Irvine, ou=Facilities, o=IBM.

The following example demonstrates one use of this scripting capability. The identity source for the Acme organization uses the attributes div for division, bu for business unit, and dept for department. The logical layout of the organization is as follows:

```
organization
  division
    business-unit
      department
```

In the IBM Tivoli Identity Manager Server, this structure is mapped to organizations and organizational units and looks like this example:

```
organization
  organizational unit (division)
    organizational unit (business-unit)
      organizational unit (department)
```

The following JavaScript code can be used for the placement rule to make this conversion:

```
return "ou=" + entry.dept[o] + ",ou=" + entry.bu[o] + ",ou=" + entry.dw[o];
```

**Note:** All identities in this feed are assumed to be within the Acme organization. For an

organization that uses a multi-valued ou attribute, the placement rule could be:

```
var ou =entry.ou;
var filt = '';
for (i = 0, i < ou.length, ++i)
{
  if (i==0)
    filt = "ou=" + ou[i];
  else
  {
    filt = filt + ",ou=" + ou[i];
  }
}
return filt;
```

The IBM Tivoli Identity Manager Server evaluates this script when adding a new person to determine where that person should be placed in the organization.

During a modify request, this script is evaluated and, if the value is different than the current placement of the person, the person is moved to the new location based on the returned path.

## Creating an identity feed service

Create a service instance for an identity type, such as CSV or DSML.

### Before you begin

Depending on how your system administrator has customized your system, you might not have access to this task. To get access to this task, or to have someone complete this task for you, contact your system administrator.

Before you can create a service in IBM Tivoli Identity Manager, you must create a new service type or use one of the service types that was automatically created when the IBM Tivoli Identity Manager Server was installed. You can create a new service type either by installing the adapter profile or by adding new schema classes and attributes for the service to your LDAP directory. Before you can create a service for an adapter, the adapter must be installed, and the adapter profile must be created.

### About this task

The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that will make sense to your end users and administrators.

To create an identity feed service instance, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, click **Create**. The Create a Service wizard is displayed.
3. On the Select the Type of Service page, select an identity feed service type, and then click **Next**.

If the table contains multiple pages, you can:

- Click the arrow to go to the next page.
  - Type the number of the page that you want to view and click **Go**.
4. On the Service Information page, specify the appropriate values for the service instance.
  5. Click **Test Connection** to validate that the data in the fields is correct, and then click **Finish**.

### Results

For the inetOrgPerson identity feed, a successful test connection message confirms that all required fields are filled and that the specified target can be reached. It does not guarantee that reconciliation of the LDAP resource will be successful or will produce the desired results.

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

### What to do next

Schedule reconciliation, or run a reconciliation immediately using the task list associated with the service.

When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table and display the new service instance.

## Performing an immediate reconciliation on an identity feed service

Initiate a reconciliation activity immediately on an identity feed service. During a reconciliation, the IBM Tivoli Identity Manager Server requests the identity record information from the specified file.

### Before you begin

Depending on how your system administrator has customized your system, you might not have access to this task. To get access to this task, or to have someone complete this task for you, contact your system administrator.

Set up a suitable identity feed service.

### About this task

To run a reconciliation now, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
  - a. Type information about the service in the **Search information** field.
  - b. In the **Search by** field, specify whether the search should be performed against services or business units.
  - c. Select a service type from the **Search type** list, and then click **Search**. A list of services matching the search criteria is displayed.

If the table contains multiple pages, you can:

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

3. In the **Services** table, click the icon ( ▶ ) adjacent to the identity feed service, and then click **Reconcile Now**.

### Results

A message is displayed, indicating that you successfully submitted a reconciliation request to run immediately.

### What to do next

To view the results of the reconciliation, click **View my request**, or click **Close**.

## Creating a reconciliation schedule for an identity feed service

Schedule a reconciliation to run at a specific interval. During a reconciliation, the IBM Tivoli Identity Manager Server requests the identity record information from the specified file.

### Before you begin

Depending on how your system administrator has customized your system, you might not have access to this task. To get access to this task, or to have someone complete this task for you, contact your system administrator.

Set up a suitable identity feed service.



## About this task

To create a reconciliation schedule for an identity feed service, complete these steps:

1. From the navigation tree, click **Manage Services**. The Select a Service page is displayed.
2. On the Select a Service page, complete these steps:
  - a. Type information about the service in the **Search information** field.
  - b. In the **Search by** field, specify whether the search should be performed against services or business units.
  - c. Select a service type from the **Search type** list, and then click **Search**. A list of services matching the search criteria is displayed.If the table contains multiple pages, you can:
  - Click the arrow to go to the next page.
  - Type the number of the page that you want to view and click **Go**.
3. In the **Services** table, click the icon ( ► ) adjacent to the identity feed service, and then click **Set Up Reconciliation**. The Manage Schedules page is displayed.
4. On the Manage Schedules page, complete the following steps:
  - a. Specify whether a policy evaluates the accounts that the reconciliation returns.
  - b. Click **Create**. The Set Up Account Reconciliation notebook is displayed.
5. On the General page, type information about reconciliation schedule.
6. On the Schedule page, select a schedule interval for the reconciliation. The fields displayed depend on the scheduling option that you select.
7. Optional: On the Query page, specify an LDAP search filter for account attributes to include in a query. Select this option if you want to perform a “supporting data only” reconciliation.
8. Click **OK** to save the new schedule and close the page.

## Results

A message is displayed, indicating that you successfully created a new reconciliation schedule.

## What to do next

Select another services task, or click **Close**. When the Select a Service page is displayed, click **Refresh** to refresh the **Services** table.