IBM Security Identity Manager
Version 6.0

LDAP Adapter Installation and Configuration Guide

IBM
## Contents

### Figures .......................................................... v

### Tables .............................................................. vii

### Preface ............................................................ ix
- About this publication ........................................... ix
- Access to publications and terminology .............................. ix
- Accessibility ............................................................ x
- Technical training ........................................................ x
- Support information ...................................................... x
- Statement of Good Security Practices .................................... x

### Chapter 1. Overview of the adapter ................................ 1
- Features of the adapter .................................................. 1
- Architecture of the adapter ............................................. 1
- Supported configurations ................................................ 2

### Chapter 2. Adapter installation planning .......................... 5
- Preinstallation roadmap .................................................. 5
- Installation roadmap ...................................................... 5
- Prerequisites ............................................................... 6
- Installation worksheet for the adapter ................................ 6
- Software download ........................................................ 7

### Chapter 3. Adapter installation and configuration ............... 9
- Dispatcher installation verification ..................................... 9
- Installing the adapter ..................................................... 9
- Adapter service start, stop, and restart ................................ 9
- Importing the adapter profile into the IBM Security Identity Manager server ............................................. 10
- Adapter profile installation verification ............................... 11
- Adapter user account creation .......................................... 11
- Creating a service ........................................................ 11

### Chapter 4. First steps after installation .......................... 17
- Adapter configuration ..................................................... 17
  - Customizing the adapter profile ..................................... 18
  - Editing adapter profiles on the UNIX or Linux operating system ......................................................... 19
  - Standard parameters .................................................... 19
  - Standard attributes ..................................................... 19
  - Operations customization for the directory server ................. 20
  - Language pack installation ............................................ 25
  - Verifying that the LDAP adapter is working correctly .............. 25

### Chapter 5. Troubleshooting the adapter errors .................... 27
- Techniques for troubleshooting problems ............................. 27
- Warning and error messages .............................................. 29
- Handling memory problems in the adapter ............................ 32

### Chapter 6. Adapter upgrade ........................................ 33
- Adapter profile upgrade ................................................ 33

### Chapter 7. Adapter uninstallation .................................. 35
- Adapter profile removal from the IBM Security Identity Manager server ................................................... 35

### Chapter 8. Adapter reinstallation ................................... 37

### Appendix A. Adapter installation on a z/OS operating system . 39

### Appendix B. Configuring for one-way SSL authentication with an LDAP server ............................................. 41

### Appendix C. Definitions for ITDI_HOME and ISIM_HOME directories ...................................................... 43

### Appendix D. Support information .................................... 45
- Searching knowledge bases .............................................. 45
- Obtaining a product fix .................................................. 46
- Contacting IBM Support .................................................. 46

### Appendix E. Accessibility features for IBM Security Identity Manager .................................................. 49

### Notices ............................................................... 51

### Index ................................................................. 55
Figures

1. The architecture ........... 2
2. Example of a single server configuration . . . 2
3. Example of multiple server configuration 3
4. One-way SSL authentication (managed LDAP server authentication) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Tables

1. Preinstallation road map ........ 5
2. Installation road map .......... 5
3. Requirements to run the adapter . 6
4. Required information to install the adapter 7
5. Attributes supported by the LDAP Adapter 20
6. Attributes supported by the LDAP Adapter 20
7. Warning and error messages .......... 29
Preface

About this publication

The LDAP Adapter Installation and Configuration Guide provides the basic information that you can use to install and configure the IBM® Security Identity Manager Lightweight Directory Access Protocol Adapter (LDAP Adapter).

IBM Security Identity Manager was previously known as Tivoli® Identity Manager.

The LDAP Adapter enables connectivity between the IBM Security Identity Manager server and a system that runs the directory server.

Access to publications and terminology

This section provides:
- A list of publications in the IBM Security Identity Manager library.
- Links to Online publications.
- A link to the IBM Terminology website.

IBM Security Identity Manager library


Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager library


IBM Security Systems Documentation Central

[IBM Security Systems Documentation Central] provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center


IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at [http://www.ibm.com/software/globalization/terminology].
Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at [http://www.ibm.com/software/tivoli/education](http://www.ibm.com/software/tivoli/education).

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at [http://www.ibm.com/software/support/probsub.html](http://www.ibm.com/software/support/probsub.html).

Appendix D, “Support information,” on page 45 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The Community and Support tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.
Chapter 1. Overview of the adapter

The LDAP Adapter enables communication between the IBM Security Identity Manager server and a network of systems that run IBM Directory Server or Sun ONE Directory Server.

An adapter provides an interface between a managed resource and the IBM Security Identity Manager server. Adapters might reside on the managed resource. The IBM Security Identity Manager server manages access to the resource by using your security system. Adapters function as trusted virtual administrators on the target platform. They perform tasks, such as creating, suspending, and restoring user accounts, and other administrative functions that are performed manually. The adapter runs as a service, independently of whether you are logged on to the IBM Security Identity Manager server.

Features of the adapter

The adapter automates user account management tasks.

- Reconciling user accounts and other support data
- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Suspending, restoring, and deleting user accounts
- Adding, modifying, and deleting groups

Architecture of the adapter

You must install a number of components for the adapter to function correctly.

- RMI Dispatcher
- Tivoli Directory Integrator connector
- IBM Security Identity Manager adapter profile

You need to install the Remote Method Invocation (RMI) Dispatcher and the adapter profile; however, the Tivoli Directory Integrator connector might already be installed with the base Tivoli Directory Integrator product.

Figure 1 on page 2 describes the components that work together to complete the user account and group management tasks in a Tivoli Directory Integrator environment.
For more information about Tivoli Directory Integrator, see the *Quick Start Guide* in the IBM Security Identity Manager product documentation.

**Supported configurations**

There are fundamental components in each environment.

- The IBM Security Identity Manager server
- The Tivoli Directory Integrator server
- The managed resource
- The adapter

The adapter must reside directly on the server running the Tivoli Directory Integrator server.

**Single server configuration**

In a single server configuration, install the IBM Security Identity Manager server, the Tivoli Directory Integrator server, and the LDAP Adapter on one server to establish communication with the IBM Directory Server or Sun ONE Directory Server.

The IBM Directory Server or Sun ONE Directory Server is installed on a different server as described in Figure 2.

![Figure 1. The architecture](image)

**Multiple server configuration**

In a multiple server configuration, the IBM Security Identity Manager server, the Tivoli Directory Integrator server, the LDAP Adapter, and the IBM Directory Server or Sun ONE Directory Server are installed on different servers.

Install the Tivoli Directory Integrator server and the LDAP Adapter on the same server as described in Figure 3 on page 3.

![Figure 2. Example of a single server configuration](image)
Figure 3. Example of multiple server configuration
Chapter 2. Adapter installation planning

Before you install an adapter, you must plan the installation.

Installing and configuring the adapter involves several steps that you must complete in an appropriate sequence. Review the road maps before you begin the installation process.

Preinstallation roadmap

Before you install the adapter, you must prepare the environment.

Perform the tasks that are listed in Table 1.

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the installation software.</td>
<td>Download the software from Passport Advantage® Web site. See “Software download” on page 7.</td>
</tr>
<tr>
<td>Verify that your environment meets the software and hardware requirements for the adapter.</td>
<td>See “Prerequisites” on page 6.</td>
</tr>
<tr>
<td>Obtain and install the Dispatcher.</td>
<td>Download the software from Passport Advantage website. See “Software download” on page 7. Follow the installation instructions in the dispatcher download package.</td>
</tr>
<tr>
<td>Obtain the necessary information for the installation and configuration.</td>
<td>See “Installation worksheet for the adapter” on page 6.</td>
</tr>
</tbody>
</table>

Installation roadmap

To install the adapter, you must complete a task sequence.

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the Dispatcher installation.</td>
<td>See “Dispatcher installation verification” on page 9.</td>
</tr>
<tr>
<td>Install the adapter.</td>
<td>See “Installing the adapter” on page 9.</td>
</tr>
<tr>
<td>Import the adapter profile.</td>
<td>See “Importing the adapter profile into the IBM Security Identity Manager server” on page 10.</td>
</tr>
<tr>
<td>Verify the profile installation.</td>
<td>See “Adapter profile installation verification” on page 11.</td>
</tr>
<tr>
<td>Create an adapter user account.</td>
<td>See “Adapter user account creation” on page 11.</td>
</tr>
<tr>
<td>Create a service.</td>
<td>See “Creating a service” on page 11.</td>
</tr>
<tr>
<td>Configure the adapter.</td>
<td>See “Adapter configuration” on page 17.</td>
</tr>
</tbody>
</table>
Prerequisites

Verify that your environment meets all the prerequisites before you install the adapter.

Table 3 identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the Tivoli Directory Integrator server.

Table 3. Requirements to run the adapter

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Directory Integrator server</td>
<td>Version 7.1 fix pack 5 or later</td>
</tr>
<tr>
<td>Version 7.1.1</td>
<td></td>
</tr>
<tr>
<td>IBM Security Identity Manager server</td>
<td>Version 6.0</td>
</tr>
<tr>
<td>Directory server</td>
<td>• IBM Tivoli Directory Server version 6.1</td>
</tr>
<tr>
<td></td>
<td>• IBM Tivoli Directory Server version 6.2</td>
</tr>
<tr>
<td></td>
<td>• Sun Directory Server version 6.3</td>
</tr>
<tr>
<td></td>
<td>• Directory servers that comply with RFC2798 standards and supported by the Tivoli Directory</td>
</tr>
<tr>
<td></td>
<td>Integrator LDAP connector. You might require additional customization.</td>
</tr>
<tr>
<td>System Administrator Authority</td>
<td>To complete the adapter installation procedure, you must have system administrator authority.</td>
</tr>
<tr>
<td>Tivoli Directory Integrator adapters solution</td>
<td>A Tivoli Directory Integrator adapters solution directory is a Tivoli Directory Integrator</td>
</tr>
<tr>
<td>directory</td>
<td>work directory for IBM Security Identity Manager adapters. See the Dispatcher Installation and</td>
</tr>
<tr>
<td></td>
<td>Configuration Guide.</td>
</tr>
</tbody>
</table>

For information about the prerequisites and supported operating systems for Tivoli Directory Integrator, see the IBM Tivoli Directory Integrator 7.1: Administrator Guide.

Installation worksheet for the adapter

You must collect information before you install an adapter.
Table 4 identifies the information that you need before installing the adapter.

<table>
<thead>
<tr>
<th>Required information</th>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Directory Integrator Home Directory</td>
<td>The <code>ITDI_HOME</code> directory contains the jars/connectors subdirectory that contains files for the adapters. For example, the jars/connectors subdirectory contains the files for the UNIX adapter.</td>
<td>If Tivoli Directory Integrator is automatically installed with your IBM Security Identity Manager product, the default directory path for Tivoli Directory Integrator is as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• for version 7.1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>drive\Program Files\IBM\TDI\V7.1</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UNIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• for version 7.1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/opt/IBM/TDI/V7.1</code></td>
</tr>
<tr>
<td>Solution Directory</td>
<td>This directory is the default directory. When you install the dispatcher, the adapter prompts you to specify a file path for the solution directory. For more information about the solution directory, see the <em>Dispatcher Installation and Configuration Guide</em>.</td>
<td>Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• for version 7.1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>drive\Program Files\IBM\TDI\V7.1\timsol</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UNIX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• for version 7.1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>/opt/IBM/TDI/V7.1/timsol</code></td>
</tr>
</tbody>
</table>

**Software download**

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

Go to [IBM Passport Advantage](https://www.ibm.com)

See the *IBM Security Identity Manager Download Document* for instructions.

**Note:**

You can also obtain additional adapter information from IBM Support.
Chapter 3. Adapter installation and configuration

All the adapters that are based on the Tivoli Directory Integrator require the Dispatcher for the adapters to function correctly.

If the Dispatcher is installed from a previous installation, do not reinstall it unless there is an upgrade to the Dispatcher. See "Dispatcher installation verification."

After verifying the Dispatcher installation, you might need to install the Tivoli Directory Integrator connector. Depending on your adapter, the connector might already be installed as part of the Tivoli Directory Integrator product and no further action is required.

Dispatcher installation verification

If this installation is for the first adapter that is based on Tivoli Directory Integrator, you must install the Dispatcher before you install the adapter.

You must install the dispatcher on the same Tivoli Directory Integrator server where you want to install the adapter.

Obtain the dispatcher installer from the IBM Passport Advantage website, http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm

For information about Dispatcher installation, see the Dispatcher Installation and Configuration Guide.

Installing the adapter

The LDAP Adapter uses the Tivoli Directory Integrator LDAP connector.

About this task

This connector is available with the base Tivoli Directory Integrator product. Make sure that the RMI Dispatcher is installed. For more information, see "Dispatcher installation verification."

What to do next

After you finish the RMI Dispatcher installation, do the following:

- Import the adapter profile. See "Importing the adapter profile into the IBM Security Identity Manager server" on page 10.
- Create a user account for the adapter on IBM Security Identity Manager. See "Adapter user account creation" on page 11.

Adapter service start, stop, and restart

To start, stop, or restart the adapter, you must start, stop, or restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Tivoli Directory Integrator instance.
See the topic about starting stopping, and restarting the dispatcher service in the Dispather Installation and Configuration Guide.

**Importing the adapter profile into the IBM Security Identity Manager server**

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

**Before you begin**

Before you begin to import the adapter profile, verify that the following conditions are met:

- The IBM Security Identity Manager server is installed and running.
- You have root or Administrator authority on IBM Security Identity Manager.

**About this task**

Before you can create an adapter service, the IBM Security Identity Manager server must have an adapter profile to recognize the adapter. The files that are packaged with the adapter includes the adapter profile JAR file. You can import the adapter profile as a service profile on the server with the Import feature of IBM Security Identity Manager.

The JAR file includes all the files that are required to define the adapter schema, account form, service form, and profile properties. You can extract the files from the JAR file to modify the necessary files and package the JAR file with the updated files.

To import the adapter profile, perform the following steps:

**Note:**

- When you import the adapter profile and if you receive an error related to the schema, see the trace.log file for information about the error. The trace.log file location is specified by using the handler.file.filename property defined in the IBM Security Identity Manager enRoleLogging.properties file. The enRoleLogging.properties file is installed in the ITIM_HOME\data directory.
- Restart IBM Security Identity Manager for the change to take effect.

**Procedure**

1. Log on to the IBM Security Identity Manager server by using an account that has the authority to perform administrative tasks.
2. In the My Work pane, expand **Configure System** and click **Manage Service Types**.
3. On the Manage Service Types page, click **Import** to display the Import Service Types page.
4. Specify the location of the JAR file in the Service Definition File field by performing one of the following tasks:
   - Type the complete location of where the file is stored.
   - Use **Browse** to navigate to the file.
5. Click **OK**.
**Adapter profile installation verification**

After you install the adapter profile, verify that the installation was successful.

An unsuccessful installation:
- Might cause the adapter to function incorrectly.
- Prevents you from creating a service with the adapter profile.

To verify that the adapter profile is successfully installed, create a service with the adapter profile. For more information about creating a service, see "Creating a service."

If you are unable to create a service using the adapter profile or open an account on the service, the adapter profile is not installed correctly. You must import the adapter profile again.

**Adapter user account creation**

You must create a user account for the adapter on the managed resource.

Provide the account information when you create a service. For more information about creating a service, see "Creating a service."

Ensure that the account has sufficient privileges to administer the LDAP users.

**Creating a service**

After the adapter profile is imported on IBM Security Identity Manager, you must create a service so that IBM Security Identity Manager can communicate with the adapter.

**About this task**

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter.

**Note:** If the following fields on the service form are changed for an existing service, restart the IBM Security Identity Manager Adapter service on the Tivoli Directory Integrator server.
- Directory Server Location
- Administrator Name
- Administrator Password
- Max Connection Count
- AL FileSystem Path

To create a service, perform the following steps:

**Procedure**
1. Log on to the IBM Security Identity Manager server by using an account that has the authority to perform administrative tasks.
2. In the My Work pane, click Manage Services and click Create.
3. On the Select the Type of Service page, select LDAP profile.
4. Click Next to display the adapter service form.
5. Fill in the following fields on the service form:

On the LDAP service tab:

**Service Name**
Specify a name that defines the adapter service on the IBM Security Identity Manager server.

*Note:* Do not use forward (/) or backward slashes (\) in the service name.

**Description**
Optional: Specify a description that identifies the service for your environment.

**Tivoli Directory Integrator location**
Optional: Specify the URL for the Tivoli Directory Integrator instance. The valid syntax for the URL is rmi://ip-address:port/ITDIDispatcher, where ip-address is the Tivoli Directory Integrator host and port is the port number for the RMI Dispatcher. The default URL is rmi://localhost:1099/ITDIDispatcher

For information about changing the port number, see IBM Security Dispatcher Installation and Configuration Guide.

**URL**
Specify the location and port number of the IBM Directory Server or Sun ONE Directory Server. Valid syntax is ldap://ip-address:port, where ip-address is the IBM Directory Server or Sun ONE Directory Server host and port is the IBM Directory Server or Sun ONE Directory Server port number. For example, you might specify the URL as ldap://irvas02.eng.irvine.ibm.com:389.

**Use SSL communication with LDAP**
Specify whether to use SSL-enabled communication between Tivoli Directory Integrator and the managed LDAP resource. See Appendix B, “Configuring for one-way SSL authentication with an LDAP server,” on page 41 for the steps to configure Tivoli Directory Integrator for SSL-enabled communication with the LDAP resource.

**Administrator name**
Specify the user name for the administrator.

**Password**
Specify the password for the administrator name.

**Directory server name**
Specify the directory server type from the pull-down.

OpenLDAP returns a null value for the venderVersion attribute. The null value causes the entire Test Connection operation to fail.

Choosing the Other selection avoids the null value error because the adapter returns a string value of Custom code needed for the venderVersion attribute. Customizing the code is a requirement only if you want to provide a valid value for the venderVersion attribute. See “Operations customization for the directory server” on page 20.
On the Users and Groups tab:

**Users base DN**
Specify the full distinguished name (DN) of the container or base point where the users are stored. The adapter creates new users under this DN. Also, search operations return user account entries under this DN. For example, you might specify the DN as `ou=people,dc=com`.

**Users RDN**
Specify the relative distinguished name (RDN) attribute for users’ LDAP entries. The RDN is a static attribute for LDAP entries and must not be modified between operation.

**Groups base DN**
Specify the full distinguished name (DN) of the container or base point where the groups are stored. User membership, specified on the account form, refers to groups in this DN. Also, search operations return group entries under this DN. For example, you might specify the DN as `ou=groups,dc=com`.

**Group RDN**
Specify the relative distinguished name (RDN) attribute for the LDAP entries of the group. The RDN is a static attribute for LDAP entries and must not be modified between operation.

**Initial Group Member**
Specify the name of a user who can be a member of the group when you perform the group add operation. However, the user that you specify for this attribute might not exist on the managed resource. For example, you can specify the name of the user as `cn=TimAdapter`, where `TimAdapter` user might not exist on the managed resource.

**Note:** The user name that you specify must be in the DN format.

**Group object class name**
Specify the group object class name under which the group is added on the managed resource. You can select the group object class name from `groupOfNames` and `groupOfUniqueNames` object classes.

**Group membership attribute**
Specify the attribute of the group object class on the managed resource that list the users who are members of the group. You can select from `member` (groupOfNames object class) and `uniqueMember` (groupOfUniqueNames object class).

On the Dispatcher Attributes tab:

**Disable AL Caching**
Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.

**AL FileSystem Path**
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from IBM Security Identity Manager. For example, you can specify the following file path.
to load the assembly lines from the profiles directory of the Windows operating system: drive:\Program
Files\IBM\TDI\V7.1\profiles or you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating system: /opt/IBM/TDI/V7.1/
profiles

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can execute simultaneously for the service. For example, enter 10 when you want the dispatcher to execute maximum ten assembly lines simultaneously for the service. If you enter 0 in the Max Connection Count field, the dispatcher does not limit the number of assembly lines that are executed simultaneously for the service.

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

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

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

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

Adapter version
Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

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

TDI version
Specifies the version of the Tivoli Directory Integrator on which the adapter is deployed.

Dispatcher version
Specifies the version of the Dispatcher.

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

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

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

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

If the connection fails, follow the instructions in the error message. Also
   • Verify the adapter log to ensure that the IBM Security Identity
     Manager test request was successfully sent to the adapter.
   • Verify the adapter configuration information.
   • Verify IBM Security Identity Manager service parameters for the
     adapter profile. For example, verify the work station name or the IP
     address of the managed resource and the port.

6. Click Finish.
Chapter 4. First steps after installation

After you install the adapter, you must do several other tasks. The tasks include configuring the adapter, setting up SSL, installing the language pack, and verifying that the adapter works correctly.

Adapter configuration

There are multiple configuration options for the adapter.

See the IBM Security Dispatcher Installation and Configuration Guide for additional configuration options such as:

- JVM properties
- Dispatcher filtering
- Dispatcher properties
- Dispatcher port number
- Logging configurations
- Secure Sockets Layer (SSL) communication

For more information about deploying and customizing the adapter, see the customization white paper entitled IBM Security Identity Manager, Version 6.0 Customization and Deployment Guide for the LDAP Adapter.

The adapter is designed to work with the inetOrgPerson object class, a general-purpose object class that contains attributes about people. If you are using the inetOrgPerson schema for your directory, the LDAP Adapter does not require customization. If your directory uses the UID attribute as the relative distinguished name (RDN), do not customize the adapter. The UID attribute must be the first component of the DN. For example, UID=Test User, ou=Accounting.

The adapter is designed to work with the groupOfNames and groupOfUniqueNames object classes, a general-purpose object class that contains attributes about groups. If you are using the groupOfNames and groupOfUniqueNames schema for your directory, the LDAP Adapter does not require customization.

The adapter supports a standard set of attributes and object classes for a directory server. The adapter supports standard user provisioning operations such as add, delete, modify, suspend, restore, change password, search, and test. The adapter also supports group operations, such as add, modify, and delete. The directory server requirements vary. Therefore, you might customize or extend the LDAP schema to support additional attributes or object classes.

The following sections provide information for configuring the adapter:

- “Customizing the adapter profile” on page 18
- “Editing adapter profiles on the UNIX or Linux operating system” on page 19
- “Standard parameters” on page 19
- “Standard attributes” on page 19
- “Operations customization for the directory server” on page 20
Customizing the adapter profile

To customize the adapter profile, you must modify the LDAP Adapter JAR file, LdapProfile.jar.

About this task

You might customize the adapter profile to change the account form or the service form.

The LdapProfile.jar file is included in the LDAP Adapter compressed file that you downloaded from the IBM website. The JAR file contains the following files:

- CustomLabels.properties
- erLDAPAccount.xml
- erLDAPRMIService.xml
- service.def
- schema.dsml
- LdapAL.xml
- LDAPAdd.xml
- LDAPDelete.xml
- LDAPModify.xml
- LDAPTest.xml
- erLDAPGroupAccount.xml
- LDAPGroupAdd.xml
- LDAPGroupModify.xml
- LDAPGroupDelete.xml

For more information about customizing the adapter profile, see the IBM Security Identity Manager, Version 6.0 Customization and Deployment Guide for the LDAP Adapter white paper.

To edit and import the adapter profile, take these steps:

Procedure

- To edit the LdapProfile.jar file, complete these steps:
  1. Log on to the workstation where the IBM Directory Server or Sun ONE Directory Server is installed.
  2. On the Start menu, click Programs → Accessories → Command Prompt.
  3. Copy the JAR file into a temporary directory.
  4. Extract the contents of the JAR file into the temporary directory by running the following command. The following example applies to the LDAP Adapter profile. Type the name of the JAR file for your operating system.
     
```bash
     cd c:\temp
ejar -xvf LdapProfile.jar
```

     The jar command extracts the files into the directory.
  5. Edit the file that you want to change.

- After you edit the file, you must import the file into the IBM Security Identity Manager server for the changes to take effect. To import the file, perform these steps:
1. Create a JAR file with the files in the \temp directory by running the following commands:
   
   cd c:\temp  
   jar -cvfLdapProfile.jar LdapProfile

2. Import the JAR file into the IBM Security Identity Manager application server. For more information about importing the JAR file, see "Importing the adapter profile into the IBM Security Identity Manager server" on page 10.

3. Stop and start the IBM Security Identity Manager server.

4. Stop and start the LDAP Adapter service. See "Adapter service start, stop, and restart" on page 9 for information about stopping and starting the LDAP Adapter service.

**Editing adapter profiles on the UNIX or Linux operating system**

The adapter profile .jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

**About this task**

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character ^M at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as dos2unix, to remove the ^M characters. You can also use text editors, such as the vi editor, to remove the characters manually.

**Example**

You can use the vi editor to remove the ^M characters. From the vi command mode, run the following command and press Enter:

```
:%s/^M//g
```

When you use this command, enter ^M or Ctrl-M by pressing ^v^M or Ctrl V Ctrl M sequentially. The ^v instructs the vi editor to use the next keystroke instead of issuing it as command.

**Standard parameters**

The LDAP Adapter is configured to use a standard set of parameters. The LDAP resource must support referential integrity.

- **inetOrgPerson**
  
  The default object class used to create new users. The supporting object classes are organizationalPerson, person, and top.

- **groupOfNames or groupOfUniqueNames**
  
  The adapter supports these object classes to assign users to groups and create new groups.

**Standard attributes**

After you install the adapter profile, the LDAP Adapter supports a standard set of attributes.

Table 5 on page 20 lists the standard inetOrgPerson attributes supported by the LDAP Adapter.
Table 5. Attributes supported by the LDAP Adapter

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>businessCategory</td>
<td>homePostalAddress</td>
</tr>
<tr>
<td>carLicense</td>
<td>initials</td>
</tr>
<tr>
<td>cn</td>
<td>1</td>
</tr>
<tr>
<td>departmentNumber</td>
<td>mail</td>
</tr>
<tr>
<td>description</td>
<td>manager</td>
</tr>
<tr>
<td>destinationIndicator</td>
<td>mobile</td>
</tr>
<tr>
<td>displayName</td>
<td>pager</td>
</tr>
<tr>
<td>employeeNumber</td>
<td>physicalDeliveryOfficeName</td>
</tr>
<tr>
<td>employeeType</td>
<td>postalAddress</td>
</tr>
<tr>
<td>facsimileTelephoneNumber</td>
<td>postalCode</td>
</tr>
<tr>
<td>givenName</td>
<td>postOfficeBox</td>
</tr>
<tr>
<td>homePhone</td>
<td>preferreddeliverymethod</td>
</tr>
<tr>
<td>preferredLanguage</td>
<td>userPassword</td>
</tr>
</tbody>
</table>

Table 6 lists the standard groupOfNames and groupOfUniqueNames attributes supported by the LDAP Adapter.

Table 6. Attributes supported by the LDAP Adapter

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>erldapservicegroup</td>
<td>Specifies the name of the group.</td>
</tr>
<tr>
<td>erldapgroupdescription</td>
<td>Specifies a brief description about the group.</td>
</tr>
<tr>
<td>erldapgroupfullname</td>
<td>Specifies full name of the group.</td>
</tr>
<tr>
<td>erldapgroupowner</td>
<td>Specifies the owner of the group.</td>
</tr>
<tr>
<td>erldapgroupbusinesscategory</td>
<td>Specifies the group business category.</td>
</tr>
<tr>
<td>erldapgrouporganization</td>
<td>Specifies the group organization.</td>
</tr>
<tr>
<td>erldapgrouporganizationalunit</td>
<td>Specifies the group organizational unit.</td>
</tr>
<tr>
<td>erldapgroupseealso</td>
<td>See Also.</td>
</tr>
</tbody>
</table>

Operations customization for the directory server

Use these customized operations for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must customize these operations for your server.

If a directory server other than IBM Directory Server or Sun ONE Directory Server is used to manage resources, the suspend, restore, and search operations must be customized. Complete these tasks to customize the above operations for a different directory server.

1. “RDN attribute change for the group account” on page 24
2. “Adding support for a new user/group object class” on page 24
3. “Base point configuration” on page 25
4. “Adding support for a new directory server” on page 25

User account suspension

You can use the default customization for the suspend operation for either IBM Directory Server or Sun ONE Directory Server.
If you use a different directory server, you might need to change the default customization for this operation.

**userPassword**

For IBM Tivoli Directory Server, the `userPassword` attribute is deleted to disable a user account.

**nsaccountlock**

For Sun Java™ System Directory Server, the `nsaccountlock` attribute is used to suspend a user account. The default value is `True`.

**Note:** The adapter returns warning, if the user is already suspended.

**User account restoration**

You can use the default customization for the restore operation for either IBM Directory Server or Sun ONE Directory Server.

If you use a different directory server, you might need to change the default customization for this operation.

**userPassword**

For IBM Tivoli Directory Server, the `userPassword` attribute is used to set the password for a user.

**nsaccountlock**

For Sun Java System Directory Server, the `nsaccountlock` attribute is used to restore a user account. The default value is `False`.

**Note:** The adapter returns warning, if the user is already restored.

**User account searches**

You can use the default customization for the search operation for either IBM Directory Server or Sun ONE Directory Server. If you use a different directory server, you must change the default customization for this operation.

**userPassword**

For IBM Tivoli Directory Server, the status of the account is based on the `userPassword` attribute. When a search is performed, if `userPassword` is mapped to `erAccountStatus`, the account is active and the value of `erAccountStatus` is 0. If `userPassword` is not mapped to `erAccountStatus`, the account is suspended and the value of `erAccountStatus` is 1.

**nsaccountlock**

For Sun Java System Directory Server, the status of an account is based on the `nsaccountlock` attribute. When a search is performed, if `nsaccountlock` is set to true, the account is disabled and the value of `erAccountStatus` is 1. If `nsaccountlock` is set to false, the account is enabled and the value of `erAccountStatus` is 0.

**The CN attribute as the ldapUserRDN**

The adapter maps the value of the LDAP `CN` attribute to the `ERUID` and `CN` attributes of the IBM Security Identity Manager. The number of values for the LDAP `CN` attributes affects the mapping.

If there is only one value for the `CN` attribute on resource, the adapter maps it to both:

- The `ERUID` attribute
- The `CN` attribute of the IBM Security Identity Manager `Account Object Class`.
For example, if the following is an entry on the LDAP resource:

Dn: cn=tuser3,ou=users,dc=com
objectclass: inetorgperson; organizationalperson; person; top;
sn: tuser3sn;
cn: tuser3;

The adapter maps tuser3 to the **ERUID** and **CN** attributes. The entry stored in IBM Security Identity Manager LDAP is:

Dn:
erglobalid=9113975423632247385,ou=orphans,
erglobalid=00000000000000000000,ou=ibm,dc=com
eruid: tuser3;
ercreatedate: 201006281214Z;
sn: tuser3sn;
erparent:
erglobalid=9113850732946037237,ou=services,
erglobalid=00000000000000000000,ou=ibm,dc=com;
objectclass: top; erLDAPUserAccount; erManagedItem; inetorgperson;
organizationalPerson; person; erAccountItem;
erglobalid: 9113975423632247385;
cn: tuser3;
eraccountstatus: 0;
erservice: erglobalid=9113850732946037237,ou=services,
erglobalid=00000000000000000000,ou=ibm,dc=com;
erldapcontainername: ou=users,dc=com;

More than one value can exist on the resource for the **CN** attribute. If **CN** is used as the **User RDN** attribute on service form, the adapter maps one value of **CN** to the **ERUID** attribute. This value is the one used as the RDN value in the **DN** attribute on resource LDAP. The adapter maps the rest of the values to the IBM Security Identity Manager **CN** attribute.

For example, if following is an entry on resource LDAP:

Dn: cn=user5,ou=users,dc=com
objectclass: inetorgperson; organizationalPerson; person; top;
sn: snval1; snval2;
cn: cnval2; cnval3; user5;

The adapter maps user5 to the **ERUID** attribute and all other values to the **CN** attribute. The entry stored in IBM Security Identity Manager LDAP is:

Dn:
erglobalid=9113975423903405991,ou=orphans,
erglobalid=00000000000000000000,ou=ibm,dc=com
eruid: user5;
ercreatedate: 201006281214Z;
sn: snval1; snval2;
erparent: erglobalid=9113850732946037237,ou=services,
erglobalid=00000000000000000000,ou=ibm,dc=com;
objectclass: top; erLDAPUserAccount; erManagedItem; inetorgperson;
organizationalPerson; person; erAccountItem;
erglobalid: 9113975423903405991;
cn: cnval2; cnval3;
eraccountstatus: 1;
erservice: erglobalid=9113850732946037237,ou=services,
erglobalid=00000000000000000000,ou=ibm,dc=com;
erldapcontainername: ou=users,dc=com;

**pwdChangeTime attribute for the LDAP Adapter**

When a password policy is enabled, the **pwdChangedTime** attribute is set on the resource for each person or user entry when the password is changed by an administrator.
The value for this attribute is in Coordinated Universal Time (UTC) format. The attribute is on the account form with the label Last Password Changed TimeStamp. The pwdChangedTime attribute is a read/write attribute in Tivoli Directory Server version 6.2. You can modify the value of the pwdChangedTime attribute in Tivoli Directory Server only if both of these conditions are met:

- A password policy is enabled.
- The Password policy enabled on directory server check box on the service form is selected.

**Note:** If Password policy enabled on directory server is checked on the service form, the following behaviors occur for Tivoli Directory Server version 6.2 only:

**Add operation**

When a new user account is requested with a value specified for the Last Password Changed Timestamp fields on the Account Form, adapter does not set the value for pwdChangedTime attribute on the resource. It returns a warning message pwdChangedTime attribute not supported during add operation.

**Modify operation**

The values specified for the Last Password Changed Timestamp fields on the account form are set on the resource. This action applies to Tivoli Directory Server with password policy enabled only.

**Reconciliation operation**

Adapter reconciles the value of the pwdChangedTime attribute for each account. This action occurs regardless of the value specified for Password policy enabled on directory server?.

The value for the pwdChangedTime attribute is changed on Tivoli Directory Server to prevent the password for a particular account from expiring. When setting the userPassword attribute set the pwdChangedTime attribute to a future date. The following example sets the time to midnight, January 1, 2200.

Ldapmodify -D cn=root -w ? -k
dn:uid=wasadmin,cn=users,o=ibm
changetype:modify
replace:pwdChangedTime
pwdChangedTime:22000101000000Z

In Sun One Directory Server version 6.3 the pwdChangedTime attribute is read only. To modify this attribute for each person and user entry on the managed resource:

- Set the usePwdChangedTime attribute to ON.
- Manually set this attribute on the resource, in the schema section under cn=config.

**Note:** The adapter reconciles the value of the pwdChangedTime attribute for Sun One Directory Server.

**Commas in the cn attribute**

If you use commas in the cn attribute, the following guidelines apply:

- Do not provide a backward slash (\) before a comma on the account form.
- If the User base DN is ou=users,dc=com, but on the resource it is cn=abc\,xyz, ou=users,dc=com, the entry is created. However, the value of the cn attribute remains abc,xyz on the LDAP resource.
- Filtered reconciliation requires that The filter query must be in the form eruid=abc,xyz.
Support for the pwdReset attribute

When password policy is enabled, the pwdReset attribute is set on the resource for each person or user entry when the password is changed by an administrator.

To use the pwdReset attribute, the Password policy enabled on directory server option on the service form must be checked.

The pwdReset attribute is on the account form with a label Force a password change at next logon? The adapter can configure this attribute. When this field is checked on the account form, adapter sets the value of pwdReset attribute to TRUE on the resource. If unchecked on the account form, the adapter sets the value to FALSE.

Note: The pwdReset attribute is not supported for Sun Directory Server.

If Password policy enabled on directory server is checked on the service form, the following behaviors occur:

Add operation
When a new user account is requested with a value specified for the Force a password change at next logon? field on the account form, adapter sets the value for pwdReset attribute on resource. If checked, the value is set to TRUE. If unchecked, the value is set to FALSE.

Modify operation
The value specified for the Force a password change at next logon? field on the account form is set on the resource.

Password change operation
The value specified for the Force a password change at next logon? field on the account form is set on the resource.

Suspend operation
The adapter does not set the value of the pwdReset attribute.

Restore operation
The value specified for the Force a password change at next logon? field on the account form is set on the resource.

Reconciliation operation
Adapter reconciles the value of the pwdRest attribute for each account. This action occurs regardless of the value specified for Password policy enabled on directory server?.

RDN attribute change for the group account
To change the RDN attribute for a group account, change these files to map the cn attribute to the required RDN attribute:

- LDAPAdd.xml
- LDAPDelete.xml
- LDAPModify.xml
- LDAPSearch.xml
- LDAPGroupAdd.xml
- LDAPGroupModify.xml
- LDAPGroupDelete.xml

Adding support for a new user/group object class
You can add support for a new user/group object class.
Procedure
1. Change the schema.dsml file to use the new user/group object class.
2. Change the service.def file to use the new user/group object class.
3. Change the customLabels.properties file to synchronize the previous steps.
4. Change these files to use the new object classes:
   - LDAPAdd.xml
   - LDAPDelete.xml
   - LDAPModify.xml
   - LDAPSearch.xml
   - LDAPGroupAdd.xml
   - LDAPGroupModify.xml
   - LDAPGroupDelete.xml

Base point configuration
The base point for the LDAP Adapter is the point in the directory server that is used as the root for the adapter. The base point can be an organizational unit (OU) or domain container (DC) base point.

To configure the base point, specify the appropriate base point (User or Group) when you create or change a service using the adapter service form.

Adding support for a new directory server
You can add support for a new directory server.

Procedure
1. Change the erLDAPRMIService.xml file to allow the directory server drop-down menu to include the new server.
2. Change the schema.dsml file to use the new user/group object class.
3. Change the service.def file to use the new user/group object class.
4. Change the customLabels.properties file to synchronize the previous steps.
5. Change these files to use the new object classes and the new directory server:
   - LDAPAdd.xml
   - LDAPDelete.xml
   - LDAPModify.xml
   - LDAPSearch.xml

Language pack installation
The adapters use the same language package as IBM Security Identity Manager.

See the IBM Security Identity Manager library and search for information about installing language packs.

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

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

Troubleshooting can help you determine why a product does not function properly.

These topics provide information and techniques for identifying and resolving problems with the adapter. It also provides information about troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
• Do all users have the problem?
• (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

**When does the problem occur?**

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:
• Does the problem happen only at a certain time of day or night?
• How often does the problem happen?
• What sequence of events leads up to the time that the problem is reported?
• Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

**Under which conditions does the problem occur?**

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:
• Does the problem always occur when the same task is being performed?
• Does a certain sequence of events need to happen for the problem to occur?
• Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

**Can the problem be reproduced?**

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible,
re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see [Appendix D, “Support information,” on page 45.](#)

### Warning and error messages

A warning or error message is displayed in the user interface to provide information about the adapter or when an error occurs.

**Table 7** contains warnings or errors which might be displayed in the user interface if the LDAP Adapter is installed on your system.

<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Recommended Action</th>
</tr>
</thead>
</table>
| No login or an invalid credential was supplied in the request. | The adapter cannot bind to a naming context or is unable to initialize because invalid credentials were provided. To fix this problem, ensure that:
  - The managed resource is functioning properly and that you are connected to the correct resource.
  - The naming context is correct if the naming context is customized.
  - The administrator ID specified on the service form is correct.
  - The administrator password specified on the service form is correct. |
| An error occurred while establishing communication with the Tivoli Directory Integrator server. | IBM Security Identity Manager cannot establish a connection with Tivoli Directory Integrator. To fix this problem, ensure that:
  - Tivoli Directory Integrator is running
  - The URL specified on the service form for Tivoli Directory Integrator is correct. |
<p>| Insufficient ‘add’ privilege. | The administrator ID that is specified on the service form does not have privileges to add a user under the base DN. You must change the administrator ID to an administrator ID that has the correct privileges or assign privileges for the specified administrator ID. |
| Entry Already Exists or exception javax.naming.NameAlreadyBoundException. | The user has already been added to the resource. This error might occur if you are attempting to add a user to the directory server and IBM Security Identity Manager is not synchronized with the resource. To fix this problem, schedule a reconciliation between IBM Security Identity Manager and the resource. See the online help for information about scheduling a reconciliation. |</p>
<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Recommended Action</th>
</tr>
</thead>
</table>
| Unknown Error while adding entry on resource.                | This error might occur for several reasons. To fix this problem, ensure that:  
  • The administrator ID specified on the service form is correct.  
  • The administrator password specified on the service form is correct.  
  • The base point is correct, if it is customized.  
  • The administrator ID has the correct privileges to modify a user account under the base DN.  
  • The network connection is not slow. |
| Cannot add user to specific group.                           | If you cannot add a user to a group, ensure that the specified group was created on the resource.                                                                                                                  |
| User not found.                                              | This error might occur when you attempt to add, modify, delete, or search for a user. This error might also occur if you attempt to change the password for a user.  
  To fix the problem, ensure that:  
  • The server that is specified for the adapter is correct.  
  • The administrator ID specified on the service form is correct.  
  • The administrator password specified on the service form is correct.  
  • The base point is correct, if it is customized.  
  If the error continues to occur, check to ensure that:  
  • The user was created on the directory server.  
  • The user was not moved or deleted from the directory server.  
  To fix the problem, add the user to the directory server and then schedule a reconciliation. See the online help for information about scheduling a reconciliation. |
| Unknown error while modifying entry on resource.             | This error might occur for several reasons. To fix this problem, ensure that:  
  • The administrator ID specified on the service form is correct.  
  • The administrator password specified on the service form is correct.  
  • The base point is correct, if it is customized.  
  • The administrator ID has the correct privileges to modify a user account under the base DN.  
  • The network connection is not slow. |
### Table 7. Warning and error messages (continued)

<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Recommended Action</th>
</tr>
</thead>
</table>
| Error adding user to group. | If you cannot add a user to a group, ensure that  
  • The user was created on the resource.  
  • The user is not already a member of the group.  
  • The group was created on the resource.  
  If the user does not exist on the resource, you must  
  create the user. If a user is already a member of a group,  
  you cannot add the user to the group. If the group does  
  not exist on the resource, you must add the group to the  
  resource before you can add a user to the group. See the  
  online help for information about creating groups or  
  adding users to groups. |
| Insufficient 'delete' privilege. | The administrator ID that is specified on the service form  
  does not have privileges to delete a user under the base  
  DN. You must change the administrator ID to an  
  administrator ID that has the correct privileges or assign  
  privileges for the specified administrator ID. |
| Search failed. | This error might occur for several reasons. To fix the  
  problem, ensure that:  
  • The network connection is not slow.  
  • The resource is not overloaded with network traffic.  
  • Tivoli Directory Integrator has sufficient memory, if  
    you have a large number of users and groups. |
| Reconciliation operation stops prematurely with Out of Memory error. | 1. Open the service.def file from the LdapProfile.jar  
    archive.  
  2. Locate the line containing name="ldapPageSize" and  
    change the default value from 0 to 100.  
  3. If you are using a Directory Server other than IBM  
    Tivoli Directory Server, also change "ldapPageSize" to  
    "ldapVLVPageSize".  
  For more information on modifying LdapProfile.jar, see  
  [“Customizing the adapter profile” on page 18](#). |
| Group already exists. | The group name that you specified already exist on the  
  managed resource. Create a group with another group  
  name. |
| Specified attribute violates the schema. | This error occurs when the following attributes are not in  
  the DN format:  
  • Group Owner  
  • See Also  
  Ensure that the values of Group Owner and See Also  
  attributes are in the DN format. For example, you can  
  add a user in the following format for the Group Owner  
  and See Also attributes:cn=user1,dc=com. |
| Group not found. | Perform a reconciliation operation to ensure that the  
  group exists on the managed resource. |
Table 7. Warning and error messages (continued)

<table>
<thead>
<tr>
<th>Warning or error message</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema violation.</td>
<td>This error occurs when the Group RDN attribute is other than CN and the value of CN is blank for the Group Full Name attribute on the group form. Ensure that you select the CN option for the <strong>Group RDN attribute</strong> on the service form or specify a value for the Group Full Name attribute on the group form.</td>
</tr>
</tbody>
</table>

### Handling memory problems in the adapter

During reconciliation requests, some directory servers return the entire search result in one chunk or page (for example, none paged search), which typically causes memory problems.

**About this task**

It might appear that the LDAP Adapter has a memory leak, but the adapter is processing the entries from the directory server while the server continues to add more entries.

If you are managing an IBM Tivoli Directory Server as your LDAP server, this is not an issue because the IBM Tivoli Directory Server supports paging.

**Note:** If you are managing an LDAP directory server other than IBM Tivoli Directory Server, see the vendor's directory server help for information regarding paged search. Additional IBM Tivoli Directory Server information regarding memory problems are available on the Web in the [Directory Integrator Reference Guide](#). Follow these steps to enable paged search:

**Procedure**

1. Open the service.def file from the LdapProfile.jar archive.
2. Locate the line containing name="ldapPageSize" and change the default value from 0 to 100. For more information on modifying LdapProfile.jar, see "Customizing the adapter profile" on page 18.
Chapter 6. Adapter upgrade

The adapter is upgraded when you install the new version of the adapter.

Upgrading the adapter might also involve tasks, such as upgrading the connector, the dispatcher, and the existing adapter profile. To verify the required version of these adapter components, see the adapter release notes. For the installation steps, see Chapter 3, “Adapter installation and configuration,” on page 9.

Adapter profile upgrade

Read the adapter release notes for any specific instructions before you import a new adapter profile on IBM Security Identity Manager.

See “Importing the adapter profile into the IBM Security Identity Manager server” on page 10.

Note: Restart the dispatcher service after importing the profile. Restarting the dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.
Chapter 7. Adapter uninstallation

To completely uninstall the adapter, remove the adapter profile from the IBM Security Identity Manager server.

Adapter profile removal from the IBM Security Identity Manager server

Before you remove the adapter profile, ensure that the objects that reference the adapter profile do not exist on your IBM Security Identity Manager server.

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

For specific information about removing the adapter profile, see the IBM Security Identity Manager product documentation.
Chapter 8. Adapter reinstallation

There are no special considerations for reinstalling the adapter. You are not required to remove the adapter before reinstalling.

For more information, see Chapter 6, “Adapter upgrade,” on page 33.
Appendix A. Adapter installation on a z/OS operating system

To install the adapters on the zOS UNIX file system, you must install only the RMI Dispatcher. The adapter uses the Tivoli Directory Integrator LDAP connector that is available with the base Tivoli Directory Integrator product.

For information about installing the RMI Dispatcher, see the Directory Integrator RMI Dispatcher Installation and Configuration Guide.

After the installation of the adapter is complete, to verify the startup and shutdown of the adapter go to “Adapter service start, stop, and restart” on page 9.
Appendix B. Configuring for one-way SSL authentication with an LDAP server

Use this procedure to configure secure communications between the LDAP server and Tivoli Directory Integrator.

About this task

To configure one-way SSL, perform the following tasks. For instructions about the individual tasks, see the SSL information in the *IBM Security Dispatcher Installation and Configuration Guide*.

Procedure

1. Create a keystore for the Tivoli Directory Integrator server.
2. Create a truststore for the Tivoli Directory Integrator server.
3. Configure Tivoli Directory Integrator to use the keystores.

   **Note:** The editing of the solution.properties file for steps 6, 7, and 8 can be done in one operation. Doing so eliminates the need for a stop and restart of the adapter service at the end of steps 6 and 7.

4. Configure Tivoli Directory Integrator to use the truststores.
5. Enable the adapter service to use SSL.
6. Create a certificate and CA certificate for the managed LDAP server. For more information about configuring SSL on the LDAP server, see the following resources on the web:

   **IBM Tivoli Directory Server**
   

   **Sun ONE Directory Server**
   
   [http://docs.sun.com/source/816-6698-10/ssl.html#14416](http://docs.sun.com/source/816-6698-10/ssl.html#14416)

7. Import the CA certificate for the managed LDAP server into the Tivoli Directory Integrator truststore. This step is similar to importing the IBM Security Identity Manager CA certificate in the WebSphere® Application Server truststore. Use the CA certificate for the LDAP server instead of the CA certificate for WebSphere.
8. Stop and restart the adapter service. See “Adapter service start, stop, and restart” on page 9.
Appendix C. Definitions for ITDI_HOME and ISIM_HOME directories

ITDI_HOME is the directory where Tivoli Directory Integrator is installed. ISIM_HOME is the directory where IBM Security Identity Manager is installed.

ITDI_HOME
This directory contains the jars/connectors subdirectory that contains files for the adapters.

Windows
drive\Program Files\IBM\TDI\ITDI_VERSION

For example the path for version 7.1:
C:\Program Files\IBM\TDI\V7.1

UNIX
/opt/IBM/TDI/ITDI_VERSION

For example the path for version 7.1:
/opt/IBM/TDI/V7.1

ISIM_HOME
This directory is the base directory that contains the IBM Security Identity Manager code, configuration, and documentation.

Windows
path\IBM\isim

UNIX
path/IBM/isim
Appendix D. Support information

You have several options to obtain support for IBM products.

- “Searching knowledge bases”
- “Obtaining a product fix” on page 46
- “Contacting IBM Support” on page 46

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).
   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.

2. Find the content that you need by using the IBM Support Portal.
   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technote and APARs (problem reports)
   - IBM Security Identity Manager Support website
   - IBM Redbooks
   - IBM support communities (forums and newsgroups)

4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com page.

5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to
include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

Tip: Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

---

**Obtaining a product fix**

A product fix might be available to resolve your problem.

**About this task**

You can get fixes by following these steps:

**Procedure**

1. Obtain the tools that are required to get the fix. You can obtain product fixes from the Fix Central Site. See [http://www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/).
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the “Download package” section.
4. Apply the fix. Follow the instructions in the “Installation Instructions” section of the download document.

---

**Contacting IBM Support**

IBM Support assists you with product defects, answers FAQs, and helps users resolve problems with the product.

**Before you begin**

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit [problems to IBM](http://www.ibm.com/software/support/). For information about the types of available support, see the [Support portfolio](http://www.ibm.com/software/support/isa/) topic in the “Software Support Handbook”.

**Procedure**

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the [Getting IBM support](http://www.ibm.com/software/support/isa/) topic in the Software Support Handbook.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.
     - Open ISA.
   - Using [IBM Support Assistant](http://www.ibm.com/software/support/isa/).
c. Click **Collection and Send Data**.
d. Click the **Service Requests** tab.
e. Click **Open a New Service Request**.
   - Online through the [IBM Support Portal](https://www.ibm.com/support) You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
   - By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the [Directory of worldwide contacts](https://www.ibm.com/ibmworldwidecontacts) web page.

**Results**

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.
Appendix E. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

**Accessibility features**

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager library, and its related publications, are accessible.

**Keyboard navigation**

This product uses standard Microsoft Windows navigation keys.

**Related accessibility information**

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for more navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to use more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

**IBM and accessibility**

See the [IBM Human Ability and Accessibility Center](https://www.ibm.com/able) for more information about the commitment that IBM has to accessibility.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to
IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.
Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, and to tailor interactions with the end user or for other purposes. In many cases, no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

## Index

### A
- accessibility x, 49
- account
  - for adapter on managed resource 11
    - form
      - force password change 24
      - pwdChangedTime 23
      - time stamp, changed 23
  - group, RDN attribute 24
  - service creation 11
- user
  - restore operation 21
  - search operation 21
  - suspend operation 21
- adapter
  - attributes 19
  - base point
    - domain container 25
    - organizational unit 25
  - configuration options 17
  - connector 9
  - customization 18
  - features 1
  - groupOfNames, groupOfUniqueNames schema 17
  - inetOrgPerson object class 17
- installation
  - overview 1
  - parameters 19
    - profile
      - customization 18
      - importing 10
      - inetOrgPerson attributes 19
      - installation 1
      - objects referencing 35
      - removal 35
      - service 11
      - upgrade 33
      - verifying 11
  - reinstalling 37
  - RMI Dispatcher 39
  - roadmap, installation 5
  - service 41
  - supported configurations 2
  - uninstallation 35
  - upgrading 33
  - user account
    - creation 11
    - management tasks 1
    - worksheet, installation 7
  - zOS UNIX file system 39
- adapter installation
  - overview 1
  - administrator authority, installation 6

### B
- base point
  - configuration 25
  - directory server point for adapter root 25
- C
- cn attribute
  - mapping 21
  - using commas 23
  - commas in the cn attribute 23
  - configuration
    - adapter 17
    - options 17
  - customization
    - directory server 20
    - operations 20
- D
  - directory server customization 21
  - customizing 20
  - support, new 25
  - suspend account 21
  - dispatcher installation for first adapter 9
  - verifying 9
  - domain container, adapter base point 25
  - download, software 7

### E
- education x
- error messages 29

### G
- group, object class 25

### I
- IBM
  - Software Support x
  - Support Assistant x
  - IBM Support Assistant 46
- inetOrgPerson
  - adapter profile 19
  - installation
    - adapter
      - connector 9
      - profile, importing 10
      - profile, verifying 11
      - administrator authority 6
      - dispatcher
        - reinstallation if upgrade 9
        - verifying 9

### K
- knowledge bases 45

### L
- language pack
  - installation 25
  - same for adapters and server 25
- logs, trace.log file 10

### M
- mapping, cn attribute 21
- memory
  - leaks 32
  - problems 32
- messages
  - error 29
  - warning 29
- MS-DOS ASCII characters 19

### N
- notices 51

### O
- object class
  - group 25
  - user 25
- online
  - publications ix
  - terminology ix
- operating system prerequisites 6
- operations customization 20
- organizational unit, adapter base point 25
- overview 1

### P
- parameters, adapter 19
- preinstallation
  - roadmap 5
  - tasks 5