Sun Java™ System

Identity Manager Quick Start Guide

2005Q4M3

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819-5021-10

Contents

Preface

This *Sun Java™ System Identity Manager Quick Start Guide* is designed to help you quickly install and configure Sun Java™ System Identity Manager (Identity Manager) for a product demo.

Notes:

- The instructions in this publication are very abbreviated; consequently, links to more detailed documentation are provided in case you need additional information or you want to expand the product demonstration.
- All documents referenced in this Quick Start Guide can be found in the Identity Manager `Docs` directory.

Intended Audience

This Quick Start Guide was designed for engineers and administrators who have experience installing and evaluating enterprise products. These individuals should be familiar with the resources, business processes, and databases to be managed within the enterprise.

How to Find Information in this Guide

The guide is organized in these sections:

- Chapter 1. *Welcome* — Provides high-level information about Identity Manager, including a product overview and an installation overview.
- Chapter 2. *Before You Install* — Describes prerequisites for installing Identity Manager.
- Chapter 3. *Installing and Configuring Identity Manager* — Provides instructions for installing and configuring an evaluation copy of Identity Manager.

Related Documentation and Help

Sun Microsystems provides additional printed and online documentation and information to help you install, use, and configure Identity Manager:

- *Identity Manager Installation*

  Step-by-step instructions and reference information to help you install and configure Identity Manager and associated software.

- *Identity Manager Administration*

  Procedures, tutorials, and examples that describe how to use Identity Manager to provide secure user access to your enterprise information systems.

- *Identity Manager Data Loading and Synchronization*

  Reference and procedural information that describe how to load and synchronize account information from a resource into Sun Java™ System Identity Manager.

- *Identity Manager Deployment Tools*

  Reference and procedural information that describe how to use different Identity Manager deployment tools; including rules and rules libraries, common tasks and processes, dictionary support, and the SOAP-based Web service interface provided by the Identity Manager server.

- *Identity Manager Technical Deployment Overview*

  Reference and procedural information that describe how to customize Identity Manager for your environment.

- *Identity Manager Troubleshooting and Error Messages*

  Reference and procedural information that describe Identity Manager error messages and exceptions, and provide instructions for tracing and troubleshooting problems you might encounter as you work.

- *Identity Manager Workflows, Forms, and Views*

  Reference and procedural information that describe how to use the Identity Manager workflows, forms, and views — including information about the tools you need to customize these objects.

- *Identity Manager Help*

  Online guidance and information that offers complete procedural, reference, and terminology information about Identity Manager. You can access help by clicking the Help link from the Identity Manager menu bar. Guidance (field-specific information) is available on key fields.

Product Support

If you have problems with Identity Manager, contact customer support using one of the following mechanisms:

- The online support web site at http://www.sun.com/service/online/us
- The telephone dispatch number associated with your maintenance contract

We'd Like to Hear from You!

We would like to know what you think of this guide and other documentation provided with Identity Manager. If you have feedback - positive or negative - about your experiences using this product and documentation, please send us a note:

Sun Microsystems.
5300 Riata Park Court
Austin, TX 78727
Attn: Identity Manager Information Development

Email: idm-idd@sun.com

We'd Like to Hear from You!

1 Welcome

The Sun Java™ System Identity Manager system enables you to securely and efficiently manage access to accounts and resources. By giving you the capabilities and tools to quickly handle periodic and daily tasks, Identity Manager facilitates exceptional service to internal and external customers.

Product Overview

Today's businesses require increased flexibility and capabilities from their IT services. Historically, managing access to business information and systems required direct interaction with a limited number of accounts. Increasingly, managing access means handling not only increased numbers of internal customers, but also partners and customers beyond your enterprise.

The overhead created by this increased need for access can be substantial. As an administrator, you must effectively and securely enable people – both inside and outside your enterprise – to do their jobs. And after you provide initial access, you face continuing detailed challenges, such as forgotten passwords, and changed roles and business relationships.

Identity Manager was developed specifically to help you manage these administrative challenges in a dynamic environment. By using Identity Manager to distribute access management overhead, you can facilitate a solution to your primary challenges: How do I define access? And once defined, how do I maintain flexibility and control?

A secure, yet flexible design lets you set up Identity Manager to accommodate the structure of your enterprise and answer these challenges. By mapping Identity Manager objects to the entities you manage – users and resources – you significantly increase the efficiency of your operations.

The Identity Manager solution lets you:

- Manage account access to a large variety of systems and resources.
- Securely manage dynamic account information for each user's array of accounts.
- Set up delegated rights to create and manage user account data.
- Handle large numbers of enterprise resources, as well as an increasingly large number of extranet customers and partners.
- Securely authorize user access to enterprise information systems. With Identity Manager, you have fully integrated functionality to grant, manage, and revoke access privileges across internal and external organizations.

- Keep data in sync by *not* keeping data. The Identity Manager solution supports two key principles that superior systems management tools should observe:
  - The product should have minimal impact on the system it is managing, and
  - The product should not introduce more complexity to your enterprise by adding another resource to manage.

Installation Overview

Note The procedures for installing and setting up the Identity Install Pack will differ according to the application server and database you are using.

This *Quick Start Guide* provides instructions for installing the Identity Install Pack on an Apache Tomcat 5.0 application server with a MySQL 5.0 repository and index database.

Perform the following tasks to install the Identity Install Pack:

1. Evaluate your environment.
   - Decide where to store MySQL index repository files.
   - Determine your memory requirements.
2. Ensure you have administrator privileges on the resource to be managed.
3. Install and set up prerequisite software.
   - Set up a java virtual machine (JVM) and java compiler.

Note The Tomcat application server bundles JDK 1.4.2 with its installation. This JDK version is always preferred to any other JDK installed on your server.

   - Set up a MySQL index database (if necessary).
   - Install and configure the Apache Tomcat application server.
4. Install and configure the Identity Install Pack software.

Notes:

- Identity Manager and Identity Auditor share the same jar file and are always installed or updated simultaneously.
- If you re-license the product you must import `update.xml` again to insure that you get all the objects for the products that are licensed to you.
- If you are using application servers with staging directories, be sure to keep the staging directory used for Identity Install Pack installation after deploying the product.

5. Set up the Sun Identity Manager Gateway (optional).
6. Set up PasswordSync (optional).

For some application server types and preferences, these general steps are combined, performed in a different order, or eliminated entirely.

Detailed installation instructions are provided in the *Sun Java™ System Identity Install Pack 2005Q4M3 Installation.*

2 Before You Install

This chapter describes the prerequisites for installing the Identity Install Pack, including:

- *Required Privileges*
- *Memory Requirements*
- *Required Privileges*
- *Software Requirements*

Note For additional information, consult the *Sun Java™ System Identity Install Pack Installation Guide* and *Release Notes*.

Required Privileges

You must have administrator privileges on the resource you are going to manage (Active Directory, LDAP, Red Hat Linux, or Solaris) for the product demonstration.

Memory Requirements

Determine your memory requirements and set values in your Apache Tomcat application server's JVM by adding maximum and minimum heap size to the Java command line. For example:

```
java -Xmx512M -Xms512M
```

You can specify these values in Tomcat by setting the `JAVA_OPTS` environment variable as follows:

- **On Windows**: `set JAVA_OPTS="-Xmx512m -Xms512m"`
- **On Unix**: `JAVA_OPTS="-Xmx512m -Xms512m"`

Notes

- For best performance, set these values to the same size.
- Depending on your specific implementation, you may need to increase these recommended values if you run reconciliation.
- For performance tuning purposes you can also set the waveset property `max.post.memory.size value` to specify the maximum number of bytes that a posted file (for example, via an `HTML FileSelect` control) can contain without being spooled to the disk. For cases where you do not have permission to write to temp files, increase the `max.post.memory.size` to avoid having to spool to the disk. The default value is 8 Kbytes.

Prerequisite Tasks

Before installing the Identity Install Pack software, you must:

- *Decide Where to Store Index Repository Files*
- *Set Up a Java Virtual Machine and Java Compiler*
- *Set Up an Index Database*

Decide Where to Store Index Repository Files

You must create the directory where you will store application files before launching the installation program. You can store application files in a staging folder, or you can install into your application server's Web application directory.

Note This guide assumes you are using MySQL 5.0.

Using a Staging Directory

Because the applications are based on J2EE Web, you can store them in a staging folder. This staging folder is used to deploy the application into your specific application server. Typically, a Web Application Archive (`.war`) file is created for use in the deployment steps.

Using a Web Application Directory

You can choose to install directly into Tomcat's Web application directory. In this case, you will specify the Web application directory during installation. The installation program will place the Identity Install Pack files in folder named `idm` in that location by default.

Set Up a Java Virtual Machine and Java Compiler

The application requires a Java compiler and a Java Virtual Machine (JVM) to run the Java classes that perform actions within Identity Install Pack. Both of these can be found in a Java SDK. (The JRE packages do not include a Java compiler.)

Notes

- The Tomcat application server bundles JDK 1.4.2 with its installation. This JDK version is always preferred to any other JDK installed on your server.
- You should add `JAVA_HOME` to your list of system environment variables and to your system path.

  Add `JAVA_HOME` to your system environment and `JAVA_HOME\bin` to your path, making sure to list it before any other Java variables. While adding `JAVA_HOME` to your list of system environment variables is helpful for Identity Install Pack, it may affect other applications.

Set Up an Index Database

To set up an index database, you can

- Use a third-party relational database to store the system index data.
- Modify the sample database scripts provided by Identity Install Pack to create tables and indexes.

Note If you modify these scripts, you must make equivalent changes to any sample database upgrade scripts that you receive in the future.

- Use an alternate method to create equivalent tables and indexes, but it must meet these requirements:
  - Tables (or views) must exist with the names specified in the sample DDL.
  - Each named table (or view) must be owned by (or aliased to) the proxy user that is represented as “waveset” in the sample DDL.
  - Each named table (or view) must contain all of the columns specified for that table in the sample DDL.
  - Each named column must have a data type that is consistent with the data type specified for that column in the sample DDL.

WARNING If you store the Index data in a local file system, select a location outside of the application or Web server directory structure. The dynamic directories created for the index data cannot be protected from intruders who might use a Web browser to scan directories serviced by the Web server.

Note You must configure an index database with a character set that supports the characters that you want to store. To store multi-byte characters, use a character set (such as UTF-8) that supports Unicode.

Software Requirements

Before you install Identity Manager, you must install the following software:

- **Java SDK 1.4.2** — Download from http://java.sun.com/j2se/1.4.2/download.html
- **Install MySQL 5.0** — Download from http://dev.mysql.com/downloads/mysql/5.0.html

  You must set up MySQL 5.0 as the Identity Manager repository. See *Setting Up MySQL* in this section for instructions.
- **Install Tomcat 5.0** — Download from: http://tomcat.apache.org/

  See *Installing Tomcat 5.0 Software* in this section for installation instructions.

Caution Be sure to install the software versions noted in the preceding list. Earlier versions of the software do not meet Identity Manager requirements and problems will result with your installation.

Setting Up MySQL

Follow these steps to set up MySQL for use with Identity Manager.

1. Install the MySQL software and start the MySQL process (if it does not start automatically).
2. Create the database. To do this:
   a. Copy the `create_waveset_tables.mysql` script from the `db_scripts` directory on the installation CD (or from the `idm\sample` directory if you have already installed) to a temporary location.
   b. Modify the following three lines in the `create_waveset_tables.mysql` script to change the database user password. Replace the `waveset` in single quotes with the password:

```
GRANT ALL PRIVILEGES on waveset.* TO waveset IDENTIFIED BY
'waveset';
GRANT ALL PRIVILEGES on waveset.* TO waveset@'%' IDENTIFIED BY
'waveset';
GRANT ALL PRIVILEGES on waveset.* TO waveset@localhost
IDENTIFIED BY 'waveset';
```

c. Use one of the following commands to create the new tables:

- **On Windows**, type

  `<MYSQL_HOME>\bin\mysql -u root [-p] < create_waveset_tables.mysql`

- **On UNIX**, type

  `$MYSQL/bin/mysql -u root [-p] < create_waveset_tables.mysql`

Note For additional information about setting up and configuring MySQL, which database server versions are supported, and for download or product locations see the *Sun Java™ System Identity Install Pack Installation Guide*.

Installing Tomcat 5.0 Software

Install the Tomcat software according to the instructions provided by the application server provider. You will find helpful information at the Jakarta Project site, located at http://jakarta.apache.org/tomcat/.

Installing on Windows

If you are installing from the Tomcat installer:

1. Specify the Tomcat installation location.
2. Select to start Tomcat as a service, and then specify the port on which to run.

   The default port is 8080.
3. Add the Java `mail.jar` and `activiation.jar` files to the following directory:

   `./tomcat/common/lib`

   The mail and activation jar files can be found at these locations:

   http://java.sun.com/products/javamail
   http://java.sun.com/products/beans/glasgow/jaf.html

Installing on UNIX

After downloading and unpacking the Tomcat 5.0 installation bundle, modify the Tomcat start-up script by adding these lines to the top of the `setclasspath.sh` file in the `$TOMCAT_HOME/bin` directory:

```
JAVA_HOME=Location of a JDK
BASEDIR=Location of your unpacked Tomcat
export JAVA_HOME BASEDIR
```

After downloading and installing all of the prerequisite software, you can install and configure Identity Manager. Continue to the next chapter for instructions.

3 Installing and Configuring Identity Manager

This chapter provides general instructions for installing an evaluation copy of Identity Manager.

The information is organized into the following sections:

- *Installing Identity Manager*
- *Configuring Identity Manager*
- *Install Sun Identity Manager Gateway*

Note Detailed instructions for installing a licensed version of Identity Manager are provided in *Sun Java™ System Identity Manager Installation.* You can download this publication from the Identity Manager `docs` directory.

Installing Identity Manager

Use the following steps to install and configure Identity Manager:

1. Unzip the Identity Manager installation zip file to access the Identity Manager installation files.
2. Enter the `install.bat` (for Windows) or `install` (for UNIX) command to launch the Identity Manager installer GUI.

Note You can run the installer in *nodisplay* mode on Unix systems; however, additional steps are necessary and they will not be covered in this Quick Start Scenario. For more information, see *Sun Java™ System Identity Install Pack Installation Guide.*

3. When the Welcome panel displays, click **Next**.

   The installer displays the Install or Upgrade? panel.
4. Leave the New Installation option selected and click **Next**.

   The installer displays the Select Installation Directory panel.
5. If necessary, replace the displayed directory location with the location where you want to install Identity Manager.

   Enter (or click **Browse** to locate) a staging location or a specific folder, and then click **Next**.

Notes

- Unless you plan to create a new context (virtual directory) in Tomcat's `server.xml` directory, we recommend installing to

  `%TOMCAT_HOME%\webapps\idm`
- If the directory you entered does not yet exist, the installer prompts for confirmation, and then creates the directory.

6. Click **Next** to begin installation.

   After installing files, the installer displays the Launch Setup panel.

WARNING Before continuing, if you plan to use an index database, you may need to copy one or more files to the `idm\WEB-INF\lib` directory.

For example, copy the MySQL Connection/J jar file into `<IDM_HOME>WEB-INF/lib` before launching the Setup Wizard. Depending on the version, the required jar file name will be something similar to: `mysql-connector-java-3.1.12-bin.jar`

You can download this file from: `http://dev.mysql.com/downloads/connector/j/3.1.html`

To determine which steps you may have to perform before you go on, see Appendix A, *Index Database Reference* in the *Sun Java™ System Identity Install Pack Installation Guide*.

If you click **Launch Setup** before copying your index database files, setup will not proceed correctly. If this happens, quit the installation program, and then use the `lh setup` command to restart the set-up portion of the installation process.

When you are finished copying your index database files (or if you are not going to use an index database) proceed to Step 7 to continue the set-up process.

7. Click **Launch Setup** to launch the Setup Wizard.
8. Click **Next** on the Setup Wizard panel.

9. When the Locate the Repository panel displays, select the MySQL JDBC Driver index database from the menu.

   Accept all of the defaults (except for the database user password if you changed it in Step 2 of *Setting Up MySQL*).

Note See Appendix A, *Index Database Reference* in the *Sun Java™ System Identity Install Pack Installation Guide* for selection information and set-up instructions.

10. Click **Next**.
11. When the installer displays the License Key panel, click **Next** to accept the Free Use License, which enables you to run the demonstration version of Identity Manager.
12. Click **Next**, and continue to the next section for configuration instructions.

Configuring Identity Manager

Use the following instructions to configure Identity Manager for the Quick Start Scenario:

1. Select **Yes** on the Setup Demo? page of the Setup Wizard to continue configuring Identity Manager for the Quick Start Scenario.
2. Enter information about yourself on the Demo User Information page.
3. Specify which type of server to manage in the Demo Scenario on the Demo Environment page:
   - Active Directory
   - LDAP
   - Red Hat Linux
   - Solaris
4. Enter the hostname of an SMTP server to use for sending notifications in Identity Manager.

Notes:

- If an SMTP server is not available, you can enter a path to a Notification File to which all email sent by Identity Manager will be written.
- Some application servers require `mail.jar` and `activation.jar` files to be included in the shared classpath directory.

5. Click **Test Server** to verify that the information about the server is valid.
   - If the server information is valid, you will see a `Successfully connected to <smtp host> for SMTP.` message.
   - If the information is not valid, you will see an error message.
6. Enter information about the selected resource on the Resource Configuration page.

   Identity Manager uses this information to manage users on the resource.
7. Click **Test Configuration** button to test your configuration settings.

Note You can view any failure messages by clicking the **Details** button.

8. Click **Next**.
9. When the Save Configuration page displays, click **Execute** to save the information you provided in the Setup Wizard.
10. Stop and restart Tomcat.

Note When the installation is complete, Identity Manager displays the Installation Summary panel. For detailed information about the installation, click **Details**.

Depending on the amount of information captured during the installation process, not all messages may be displayed here. View the log file (identified in details) for more information.

11. When finished, click **Close** to exit the installer.

Identity Manager is now ready to run the Quick Start Scenario.

- If you want to set up a Windows Active Directory, Novell NetWare, Novell GroupWise, Exchange 5.5, Remedy, or RSA ACE/Serve resource, you must install Sun Identity Manager Gateway. Proceed to the next section for instructions.
- If you do not want to install the Sun Identity Manager Gateway, you can proceed to Chapter 3: *Quick Start Scenario*.

Install Sun Identity Manager Gateway

To install Sun Identity Manager Gateway:

1. Select the Windows machine on which to install the gateway.

Note The machine must be a member of the domain in which the accounts and other objects will be managed (the managed domain) or a member of a domain that is trusted by the managed domain. The gateway does not have to run on a domain controller.

Tip For better performance, locate the gateway near (from a network connectivity perspective) the managed domain's domain controllers.

2. If you selected a system that is not the Identity Manager server; create a directory called `idm` on the remote system, copy the `gateway.zip` file from the Identity Manager Installation CD, and then unpack and copy the contents of the `gateway.zip` file to the `idm` directory.
3. To install the gateway as a service, run the following command from the directory where the gateway files are installed:

   ```
   gateway –i
   ```

4. Run the following command to start the gateway service:

   ```
   gateway -s
   ```

Notes:

- To stop the gateway service, run the `gateway -k` command:
- The following failure messages (and their likely causes) may occur when you are working with the gateway:
  - `'Overlapped I/O operation is in progress'`

    The most common cause of this message is that you asked for the service to be installed or removed before a prior installation or removal has fully completed. Check the state of the service.
  - `'Input/output error'`

    The most common cause of this message is that you do not have rights to work with this service.

You are finished installing the Sun Identity Manager Gateway. Continue to Chapter 3: *Quick Start Scenario*.

4 Quick Start Scenario

This Quick Start Scenario provides a guided demonstration of some of Identity Manager's most powerful features. The demonstration consists of three sections:

- *Basic Provisioning*:
  - Provisioning to a resource (Active Directory, LDAP, Red Hat Linux, or Solaris)
  - Configuring email notifications when resource accounts are created, updated, or deleted
  - Requiring approvals before resource accounts are created, updated, or deleted
- *End User Self-Service*:
  - Logging in with authentication questions when a password is forgotten
  - Changing passwords on one or more resources
  - Changing personal data
- *Advanced Features*:
  - Viewing all changes to a user with the Historical User Change Report
  - Loading all accounts from the managed server into Identity Manager with reconciliation
  - Detecting changes on a managed server with reconciliation or Active Sync

In addition, the following users are provided to illustrate how different people in an organization can use Identity Manager:

- **Configurator:** A super-user in Identity Manager who can provision resource accounts, configure Identity Manager, run reports, and reconcile accounts from the configured server

  In a typical deployment, you can create different administrators who have subsets of these capabilities. For example, you might create a Report Administrator (to run reports), a Password Administrator (who can reset user passwords), and so forth.

  Additionally, you can grant administrators capabilities in certain Identity Manager organizations to limit their scope of control – referred to as *delegated administration*. For example, administrators can have the Approver capability for the *Sales* organization, which allows them to approve or reject account creation for new users in the Sales organization, but not for new users in the *Engineering* organization.
- **Demoapprover:** An administrator can approve or reject requests to create, update, or delete new user accounts.

- **End User:** A typical employee with accounts on one or more managed servers.

  End users can login to the Identity Manager End User Portal to manage their personal information (name, email address, etc.) and change their passwords.

Basic Provisioning

The Basic Provisioning section demonstrates how to

- Create user accounts on a configured server
- Enable email notifications and approvals
- Configure Identity Manager to approve account creations

Creating Accounts on a Configured Server

You can create an account on the resource configured in the Setup Wizard by creating an Identity Manager user with the assigned resource, as follows:

1. Open a Web browser and type the following address into the address bar:

   `http://localhost:8080/idm/`

Note Depending on the options that you selected during the Tomcat installation, the port may be different.

2. Login to the Identity Manager Administrator interface as the **`Configurator`** user. The default password for this user is **`configurator`**.
3. Click the **Accounts** tab to navigate to the Accounts page.
4. Select **New User** from the **New Actions** menu to create a new user.
5. Enter the following information on the Identity tab:
   - Account ID
   - First name
   - Last name
   - Email address
   - Password

Note The password must conform to the Password Policy described in the "Resource account whose password will be changed" table. You can modify this password policy to match your corporate standards by navigating to **Configure > Policies** and clicking **Password Policy**.

6. In the **Individual Resource Assignment** field on the **Assignments** tab, select the resource that you configured in the Setup Wizard.

7. Optionally enter any additional information about the resource account on the **Attributes** tab.
8. Click **Save**.

   The Create User Results should show that a Lighthouse user was created (this is the virtual user in Identity Manager) and that an account was created on the resource. You can use native tools on the resource to verify that the account was actually created.
9. Click **OK** at the bottom of the Results page.

   The user that you just created should display on the List Accounts page.

Configuring Identity Manager to Send Email Notifications

Use the following steps to configure Identity Manager to send email notifications when new users are created:

1. Select the **Tasks > Configure Tasks** tabs to access the Task Configuration page.
2. Click **Create User Template** to edit properties for the workflow that runs when a user is created in Identity Manager.
3. Select the **Notification** tab.
4. Select **Administrator List** for the **Determine Notification Recipients from** field.
5. Select **demoapprover** from the **Administrators to Notify** field.

   This is the demoapprover user that was created in the Setup Wizard. When you select this user, Identity Manager will send email to the email address that you specified in the Setup Wizard when new users are created in Identity Manager.
6. Select **Account Creation Notification** as the for the **Email Template** field.
7. Click **Save**.
8. Repeat steps 4–11 from the *Creating Accounts on a Configured Server* section to create a new user.
   - If you configured an SMTP server in the Setup Wizard, Identity Manager will send an email to the demoapprover.
   - If you configured a notification file in the Setup Wizard, you can open the notification file in a text editor to view the email that would have been sent.

Identity Manager uses a *process diagram* to illustrate the steps that are executed by the workflow when creating, updating, or deleting a user. If user interaction is required during a workflow (such as an approval) the process diagram shows which workflow steps have run and which steps will run after the required interaction is completed.

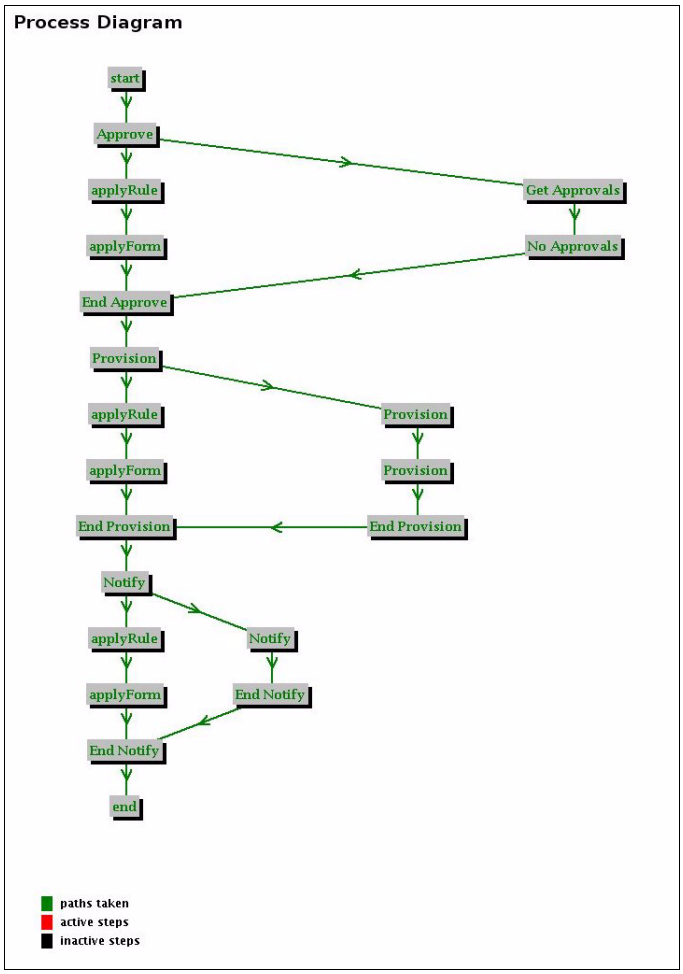

Figure 1. Example Process Diagram

For more information about the BPE, workflows, and an illustrated example of altering the approval workflow, see *Sun Java™ System Identity Manager Workflows, Forms, and Views*.

Notes:

You can also

- Configure notifications for user updates and deletes.
  Repeat the preceding steps 1–7, being sure to select the appropriate email template (**Update User Template** or **Delete User Template**) for step 2.
- Enable the **Notify User** checkbox on the Notification tab to send an email to the end user who is being created, updated, or deleted.
- Use an **Attribute**, a **Query on the resource**, or a **Rule** to determine additional notification recipients.

Configuring Identity Manager to Approve Account Creations

When you add a user to the Identity Manager system, administrators who are assigned as approvers for new accounts must validate the account creation. Identity Manager supports four categories of approvals, applied to these Identity Manager objects:

- **Organization** — Approval is needed for the user account to be added to the organization.
- **Role** — Approval is needed for the user account to be assigned to a role.
- **Resource** — Approval is needed for the user account to be given access to a resource.
- **Additional Approvals** — Approvals are determined with a rule, query, or list in the Configurable Task. *You will use this approval type for this scenario*.

For this scenario, you will require the demoapprover administrator to approve an account creation, as follows:

1. Select the **Tasks > Configure Tasks** tabs to access the Task Configuration page.
2. Click **Create User Template** to edit properties for the workflow that is run when a user is created in Identity Manager.
3. Select the **Approvals** tab.
4. Select **Administrator List** for the **Determine additional approvers from** field.
5. Select **demoapprover** for the **Approval Administrator** field.

6. Enable all checkboxes in the Editable column of the Approval Attributes table to allow the approver to modify these attributes when approving user creations.
7. Click **Save**.
8. Repeat steps 4-11 in the *Creating Accounts on a Configured Server* section to create a new user.

   Notice that the Create User Results page states that the creation is pending an approval from demoapprover. If you view the List Accounts page, the new user will not yet appear.

   - If you configured an SMTP server in the Setup Wizard, Identity Manager will send an email to the demoapprover to notify the administrator that an account creation approval has been requested.
   - If you configured a notification file in the Setup Wizard, you can open the notification file in a text editor to view the email that would have been sent.
9. Click **Logout** to log Configurator out of Identity Manager.
10. When the Login page displays, log in as **`demoapprover`** and use the password that you specified in the Setup Wizard.

    Notice that there are only three tabs in Identity Manager when you are logged in as demoapprover – **Home**, **Passwords**, and **Approvals**.

    Identity Manager only displays tabs and sub-tabs for pages that the logged in user can use. Because demoapprover only has the Approver capability, these three tabs are the only pages that are available.
11. Select the **Approvals** tab to view the Awaiting Approvals page.

Note The process diagram (described in *Configuring Identity Manager to Send Email Notifications*) is stalled at this point, awaiting an approval.

12. Click the approval in the table.
13. If necessary, you can change user attributes or add comments about the approval.

Note You can forward an approval to a different user by selecting that Identity Manager user's name in the **Forward to** list.

14. Click **Approve** to approve the account creation request.
15. Logout demoapprover and log back in as **`Configurator`**.
16. Click the **Accounts** tab to verify that the new user was created after the approval. Also, demoapprover should receive an email notification that the account was created.

Notes:

- You can also configure approvals for user updates and deletes. Repeat the preceding steps 1–7, being sure to select the appropriate email template (**Update User Template** or **Delete User Template**) for step 2.
- You can use the **Approval times out after** option to specify what happens if an approval has not been accepted or rejected within a certain time period. You can reject the request, escalate the approval to a different approver, or run a custom task (such as sending email to another administrator).

End User Self-Service

The End User Self-Service section demonstrates how end users can use Identity Manager to login with authentication questions when they forget their password, change their password on all resource accounts, and change their personal data.

In this section you are assuming the role of an end user.

Changing Your Authentication Questions' Answers

To change the answers to your authentication questions:

1. To view the login page for the end user interface, open a Web browser and type the following address into the address bar:

   `http://localhost:8080/idm/user/login.jsp`

   Note Depending on the options that you selected for the Tomcat installation, the port may be different than *8080*.

2. Enter the **User ID** and **Password** of a user that you created in the *Basic Provisioning* section.
3. Click **Change Answers to Authentication Questions**.
4. Enter an answer for the displayed question.

   Note You can configure the list of authentication questions and question policy from the administrator interface. Log in as **`Configurator`**, select **Configure > Policies**, and click **Default Lighthouse Account Policy**.

5. Click **Save** to save the new answer to your question.
6. Click **Logout**.

Changing Your Password

To change your password:

1. Enter the same **User ID** that you entered in step 2 of the previous section, but leave the **Password** blank.
2. Click **Forgot Your Password?**.
3. Enter the same answer that you provided in step 4 of the previous section.
4. Click **Login**.

   Because the login occurred with a forgotten password, you are prompted for a new password.
5. Enter a new password.

   Notice that the new password will be set on the Lighthouse account (the Identity Manager user) and on the account on the configured resource.
6. Click **Change Password**.

Changing Your Personal Data

To change your personal data:

1. Click **Change Other Account Attributes** to modify your personal data.
2. Modify the email address.
3. Click **Save**.

   Notice that the email address has been updated for the Lighthouse user and possibly the resource account if the resource manages an email address.
4. Click **Logout** to logout of the end-user pages.

Advanced Features

This Advanced Features section demonstrates how to

- Load users into Identity Manager
- Load and detect native changes on the managed resource
- Run a report to view all history for a single user

Loading Users into Identity Manager

One of the first steps you perform for an Identity Manager deployment is to load all accounts from the managed resource into Identity Manager so they can be managed. Generally, most deployments manage multiple resources; however, for the purposes of this quick start scenario, only a single resource will be managed.

1. Select the **Resources** tab to access the List Resources page.
2. Expand the resource tree to find the resource that you configured in the Setup Wizard.
3. Enable the resource's checkbox to select the resource.
4. Select **Edit Reconciliation Policy** from the **Resource Actions** list to define how accounts found on the resource will be reconciled with the users found in Identity Manager.

   Initially, Identity Manager will have only a few administrators (Configurator, Administrator, demoapprover) and the users that you created in the *Basic Provisioning* section.

   All other users on the managed resource will be considered *UNMATCHED* when reconciled because there are no Identity Manager users that match the resource accounts that are found.
5. Select **Create new user based on resource account** for the UNMATCHED situation in the Situation Options table.

   The remaining situation options are used to determine how Identity Manager responds to other reconciliation situations. For this Quick Start Scenario, do not change the default values for these options.
6. Click **Save** to save the reconciliation policy.
7. Enable the resource's checkbox.
8. Select **Full Reconcile Now** from the **Resource Actions** list to initiate a full reconciliation from the resource.
9. Enable the resource's checkbox.
10. Select **View Reconciliation Status** from the **Resource Actions** list to view the status of the full reconciliation.

    The time it takes to complete a full reconciliation can vary widely, based on the number of users on the managed resource, the speed of the managed resource, the speed of the Identity Manager server, and so forth.
11. When the reconciliation is complete, review the information provided to see how many accounts were created.
12. Select the **Accounts** tab to navigate to the List Accounts page.

    Notice that all users from the resource are now listed on this page.

Detecting Changes on the Managed Server

Identity Manager accommodates bidirectional synchronization, depending on target resource functions and market need.

- Identity Manager's Reconciliation feature highlights inconsistencies between the resource accounts on Identity Manager and the accounts that actually exist on a resource, and to periodically correlate account data.

  Reconciliation is designed for ongoing comparison, and it can

  - Diagnose account situations more specifically and support a wider range of responses
  - Detect native changes.
  - Be scheduled
  - Offer an incremental mode

  It is important to note that, Identity Manager only stores those security-relevant account attributes that you specify, rather than storing every attribute on every account.
- Identity Manager's Active Sync feature allows information that is stored in an *authoritative external resource* (such as an application or database) to synchronize with Identity Manager user data. Setting up active synchronization for an Identity Manager resource enables it to "listen" or poll for changes to the authoritative resource.

Note For detailed information about reconciliation and Active Sync, see the *Dataloading and Synchronization* chapters in *Sun Java System Identity Manager Administration* and *Sun Java System Identity Manager Technical Deployment Overview.*

For the purpose of this Scenario, you will use reconciliation to detect changes on a managed server. Use the following instructions:

1. Natively create a new user on the managed resource.

   The method for creating a new user will vary depending on the resource.

   - You can create a new user with the Active Directory Users and Computers tool in Active Directory
   - You can import an LDIF file in a Directory Server
   - You can use the **`useradd`** command on a Red Hat Linux or Solaris server
2. Select the **Resources** tab to access the List Resources page.
3. Expand the resource tree to find the resource that you configured in the Setup Wizard.
4. Enable the resource's checkbox to select the resource.

5. Select **Incremental Reconcile Now** from the **Resource Actions** list to initiate an incremental reconciliation from the resource.
6. Enable the resource's checkbox.
7. Select **View Reconciliation Status** from the **Resource Actions** list to view the status of the incremental reconciliation.
8. After the reconciliation is complete, review the information to see how many accounts were created.
9. Select the `Accounts` tab to access the List Accounts page.

   Notice that the new user you created on the resource is now listed on this page.

Viewing the Historical User's Change Report

To view a user's change report history:

1. Open a Web browser and type the following Web address in the address bar:

   `http://localhost:8080/idm/`

Note Depending on the options that you selected during the Tomcat installation, the port (*8080*) may be different.

2. Login to the Identity Manager Administrator interface as the **`Configurator`** user.

Note The default password for this user is **`configurator`**.

3. Select the **Reports** tab to access the Run Reports page.
4. Click the **Historical User Changes Report** link to provide information about which report to run.
5. Enter the **Account ID** of the user specified in the *End User Self-Service* section.
6. Click **Run**.
7. Review the historical change report.

   Notice that events such as creation, modifications, change password, login, and logout are reported. The report provides information about when the change occurred, which user caused the change, the result of the change, attribute-level before and after values for creations and modifications, which interface the change occurred in, and so forth.
8. You can run this report for all users by clicking the **Run** button located next to the **User Historical Change Report** on the Run Reports page.

Next Steps

There are many other important features in Identity Manager that are not discussed in this Quick Start Guide, such as:

- Using the Business Process Editor (BPE) to edit forms
- Using rules to encapsulate business process and corporate data links
- Using role-based access control and resources
- Using role exclusions

For more information about these and other Identity Manager features, consult the *Identity Manager* publications listed in the *Related Documentation and Help* section of the *Preface*.

To contact a Sales representative for more information about the Identity Manager product, get information about self-qualifying, or sign-up for the Identity Champions newsletter be sure to visit the following web site and enable the **Sun Identity Insights Program** checkbox:

https://subscriptions.sun.com/subscription_center/ecomm.jsp