Oracle® Retail Security Manager

Installation Guide

Release 11.3

June 2009

Oracle® Retail Security Manager Installation Guide, Release 11.3

Primary Author: Liz Burke-Scovill

Contributors: Nathan Young

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the software component known as **ACUMATE** developed and licensed by Lucent Technologies Inc. of Murray Hill, New Jersey, to Oracle and imbedded in the Oracle Retail Predictive Application Server – Enterprise Engine, Oracle Retail Category Management, Oracle Retail Item Planning, Oracle Retail Merchandise Financial Planning, Oracle Retail Advanced Inventory Planning, Oracle Retail Demand Forecasting, Oracle Retail Regular Price Optimization, Oracle Retail Size Profile Optimization, Oracle Retail Replenishment Optimization applications.

(ii) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(iii) the **SeeBeyond** component developed and licensed by Sun MicroSystems, Inc. (Sun) of Santa Clara, California, to Oracle and imbedded in the Oracle Retail Integration Bus application.

(iv) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(v) the software component known as **Crystal Enterprise Professional and/or Crystal Reports Professional** licensed by SAP and imbedded in Oracle Retail Store Inventory Management.

(vi) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(vii) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

(viii) the software component known as **Style Report™** developed and licensed by InetSoft Technology Corp. of Piscataway, New Jersey, to Oracle and imbedded in the Oracle Retail Value Chain Collaboration application.

(ix) the software component known as **DataBeacon™** developed and licensed by Cognos Incorporated of Ottawa, Ontario, Canada, to Oracle and imbedded in the Oracle Retail Value Chain Collaboration application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

Preface

Oracle Retail Installation Guides contain the requirements and procedures that are necessary for the retailer to install Oracle Retail products.

Audience

This Installation Guide is written for the following audiences:

- Database administrators (DBA)
- System analysts and designers
- Integrators and implementation staff

Related Documents

For more information, see the following documents in the Oracle Retail Security Manager Release 11.3 documentation set:

- Oracle Retail Security Manager Release Notes

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://metalink.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

If you are installing the application for the first time, you install either a base release (for example, 13.0) or a later patch release (for example, 13.0.2). If you are installing a software version other than the base release, be sure to read the documentation for each patch release (since the base release) before you begin installation. Patch documentation can contain critical information related to the base release and code changes that have been made since the base release.

Oracle Retail Documentation on the Oracle Technology Network

In addition to being packaged with each product release (on the base or patch level), all Oracle Retail documentation is available on the following Web site (with the exception of the Data Model which is only available with the release packaged code):

http://www.oracle.com/technology/documentation/oracle_retail.html

Documentation should be available on this Web site within a month after a product release. Note that documentation is always available with the packaged code on the release date.

Conventions

Navigate: This is a navigate statement. It tells you how to get to the start of the procedure and ends with a screen shot of the starting point and the statement “the Window Name window opens.”

> **Note:** This is a note. It is used to call out information that is important, but not necessarily part of the procedure.

```
This is a code sample
    It is used to display examples of code
```

A hyperlink appears like this.

1

Preinstallation Tasks

RSM is a Service-Oriented Architecture application. The client code is Java-based and is launched from Java WebStart. The RSM service layer is run from the WebSphere Application Server and accesses an Oracle Database server and an LDAP compliant Directory Server.

Check Database Server Requirements

RSM supports both 10G and 9i, as listed below:

Supported on 10gR2	**Versions Supported:**
Database Server OS	OS certified with Oracle Database 10gR2 Enterprise Edition. Options are: ▪ AIX 5.2 ▪ AIX 5.3 ▪ Solaris 9 (SPARC) ▪ HP-UX 11.11 (PA-RISC) ▪ HP-UX 11.31 (Itanium)
Database Server	Oracle Database 10g Release 2 Enterprise Edition (10.2.0.4 patchset required) with the following components: ▪ Oracle Database 10g ▪ Oracle Partitioning ▪ Oracle Net Services ▪ Oracle Call Interface (OCI) ▪ Oracle Programmer ▪ Oracle XML Development Kit ▪ Companion CD **Patches:** ▪ 10.2.0.4 patchset: 6810189 ▪ AIX oneoff patch: 6154596 (PRO*C THROWS PCC-2014 WHEN DIAGNOSTIC DIRECTIVE #WARNING IS USED) **Other components:** ▪ Perl compiler 5.0 or later ▪ X-Windows interface ▪ ANSI compliant C compiler (certified with OS and database version)

Supported on 9iR2	Versions Supported:
Database Server OS	OS certified with Oracle Database 9i Enterprise Edition. Options: ▪ AIX 5.2 ▪ AIX 5.3 ▪ Solaris 9 (SPARC) ▪ HP-UX 11.11 (PA-RISC) Oracle Database 9i Enterprise Edition (9.2.0.8 patchset required) with the following components: ▪ Oracle 9i Database ▪ Oracle Partitioning ▪ Oracle Net Services - Oracle Net Listener ▪ Oracle Call Interface (OCI) ▪ Oracle Programmer ▪ Pro*C/C++ ▪ Oracle XML Developers Kit **Patches:** ▪ 9.2.0.8 patchset: 4547809 ▪ Oneoff patch: 4689959 (DST RULE CHANGE IN US, NEED to PATCHED TIMEZONE FILES) **Other components:** ▪ Perl compiler 5.0 or later ▪ X-Windows interface

Check Application Server Requirements

General requirements for an application server capable of running RSM include:

Supported on:	Versions Supported:
Application Server OS	UNIX based OS certified with IBM WebSphere 5.1.1.12. Options are: ▪ AIX 5.2 ▪ AIX 5.3 ▪ Solaris 9 (SPARC) ▪ HP-UX 11.11 (PA-RISC)
Application Server	IBM WebSphere Application Server version 5.1.1.12

Directory Server

RSM supports both xml file and directory server based user authentication and searching. General requirements for a directory server capable of running RSM include:

- Microsoft Windows 2000 (Service Pack 4) Active Directory or OpenLDAP version 2.x*
- LDAP version 3.0 compliant.

* RSM is certified against OpenLDAP version 2.1.12 on Solaris and OpenLDAP version 2.0.19 on Windows NT. Although RSM is not certified against OpenLDAP on AIX or HP, there are no limitations that would prevent RSM from running against an OpenLDAP instance on these or any other operating systems.

Check Web Browser and Client Requirements

General requirements for client running ARI include:

Requirement	Version
Operating system	Windows 2000 or XP
Display resolution	1024x768
Processor	Pentium processor (minimum 1GHz MHz)
Memory	minimum of 512 MB RAM
Sun JRE Plug-in	1.4.2
Microsoft Internet Explorer	5.5, 6.0 and higher The browser is used to launch the Java WebStart client.

2

Application Server Configuration Instructions

The RSM server tier is packaged as an EAR file – rsm11.ear. Install the rsm11.ear file on the J2EE application server according to the vendor's documentation.

The following are typical steps for deploying an ear file in WebSphere 5.1.1.10, assuming WebSphere Application Server (WAS) and IBMHttpServer 5.1.1.10 have already been installed. It is also assumed Oracle has already been configured and loaded with the appropriate RSM Schema for your installation.

UNIX (Sun Solaris/HPUX/AIX)

Note: IBM JVM 1.4.2 is required for RSM (and is shipped with Websphere 5.1.1.10)

Note: IBM recommends that the IBMHttpServer be configured to run as the front-end for WebSphere Application Server.

Note: ojdbc14.jar is required for RSM 11. This file can be obtained from the Oracle Technology Network web site, and must be copied to a staging directory on the server where WebSphere 5.1.1.10 is installed (ie: /u00/websp/jdbc/ojdbc14.jar)

Configure WebSphere 5.1.1.10 Application Server for RSM 11

1. Open the WebSphere Administration Console that is to be used for administering the RSM 11 application – http://<server>:<admin_port>/admin.. If the administrative url console is unknown, consult the WebSphere 5.1.1.10 documentation for the correct URL.
   - server = name or IP address of server where WebSphere 5.1.1.10 is running
   - admin_port = WebSphere Admin Console Port

   Example: http://server:9090/admin

2. Click on Environment->Manage WebSphere Variables.
3. Under WebSphere Variables, set the scope to the Node level:
   - Click ORACLE_JDBC_DRIVER_PATH and set the value of this variable to the directory containing the oracle driver archive file ojdbc14.jar (obtained from otn.oracle.com).

   Example: /u00/websp/jdbc

   - Click Apply
4. Click on Security->JAAS Configuration->J2C Authentication Data.
5. Under J2C Authentication Data Entries, click New and enter the following information in the fields provided:

- Alias (alias for Authentication Data Entry)
- UserID (RSM database schema owner)
- Password (RSM database schema password)
- Click Apply

Example: Alias: RSM11

User ID: rsm11dev

Password: retek

6. Click on Resources->JDBC Providers. If the Oracle JDBC Driver (XA) JDBC Provider has already been created for another application that is running on this same WebSphere instance, then skip steps 7 and 8 below and proceed to step 9.
7. Under JDBC Providers, click the server radial button or browse to the appropriate server (if multiple servers on this Node) and then click Apply.
8. Create a new JDBC Provider by clicking New.
   - Select Oracle JDBC Driver (XA) from the JDBC list of values and click Apply
9. Under Additional Properties for the Oracle JDBC Driver (XA), select Data Sources and then under Data Sources click the New button, and enter the following information in the fields provided:
   - Data Source Name: RSM (must be this value)
   - JNDI Name: jdbc/RsmDataSource (must be this value)
   - Component-managed Authentication Alias: from the drop-down, choose the J2C Authentication Alias that was created in step 5 above
   - Container-managed Authentication Alias: leave blank; CMP is not used in RSM
   - All other fields leave as default
   - Click Apply

Example: Name: RSM

JNDI Name: jdbc/RsmDataSource

Component-managed Authentication

Alias: server/RSM11

10. Under Additional Properties, click Custom Properties for the Data Source and make the following updates:
    - Click URL. Enter the following information in the Value field:
    - Value: jdbc:oracle:thin:@<DB Server IP address>:<DB Listener Port>:<Database_name>

Example: jdbc:oracle:thin:@dbserver:1521:prod_db1

- Click Apply; Click OK to go back to Custom Properties
- Click transactionBranchesLooselyCoupled. Enter the following information in the Value Field:
- true
- Click Apply; Click OK to go back to Custom Properties
- Click preTestSQLString. Enter the following information in the Value Field:
- select count(*) from dual

- Click Apply

11. Save the configuration by clicking the Save link in the Message(s) section, and then by clicking the Save button in the Save to Master Configuration section.
12. Verify the configuration by using the “Test Connection” option in the Data Sources configuration section (Resources->JDBC Providers->Oracle JDBC Driver (XA)->Data Sources->Data Source Name->Test Connection button). A successful message in the Message(s) section should appear. In the case of an unsuccessful connection test, review all previous steps to ensure that the configuration thus far is accurate.
13. Click on Security->JAAS Configuration->Application Logins.
    a. Create a new Application Login Configuration by clicking New.
    b. Under General Properties, input the Alias name for login module.
    - For LDAP authentication, enter
      – Retek.Ldap.LoginModule
    - For XML authentication, enter
      – Retek.XML.LoginModule
    c. Click Apply
    d. Click JAAS Login Modules – Additional Properties for this Configuration
    e. Create a New Module Classname by clicking New.
    - For LDAP authentication, enter the value below as the Module Classname:
      – com.retek.rsm.domain.security.dao.LdapLoginModule
    - For XML authentication, enter the value below as the Module Classname:
      – com.retek.rsm.domain.security.dao.XMLLoginModule
    - Keep the Authentication Strategy as the default value of REQUIRED.
    f. Click Apply.
14. Save the configuration by clicking the Save link in the Message(s) section, and then by clicking the Save button in the Save to Master Configuration section.
15. Click on Servers-> Application Servers.
16. Under Application Servers, click on the link for the server instance created during the WebSphere installation; the default name of the initial application server instance is server1.
17. In the Additional Properties section click on the End points link in the lower section of the page.
18. Under BOOTSTRAP_ADDRESS, verify the Host and Port values are set correctly. Record these host and port values as they will be needed when configuring the RSM 11 client.
19. Update the j2c.properties file located in the WAS_HOME/properties directory by uncommenting the advanced-connection-properties section and by adding another advanced-connection-properties property for the RSM Data Source created in step 9 above:

Example:

<advanced-connection-properties connectionFactoryJNDIName="jdbc/**RsmDataSource**">

<testConnection>true</testConnection>

<testConnectionRetryInterval>5</testConnectionRetryInterval>

</advanced-connection-properties>

Note: The j2c.properties file is associated with a particular application server. This application server must be restarted before these changes will take affect.

Expand the RSM Distribution

1. Log into the UNIX server where WebSphere 5.1.1.10 is installed as the retek user and determine where the RSM 11 application server file (rsm11appserver.zip) will be installed. There should be a minimum of 50 MB disk space available for the application installation files.
2. Copy rsm11appserver.zip located at CD/appserverunix to a newly created staging directory on the UNIX server. This location will be referred to as INSTALL_DIR for the remainder of this chapter.
3. Change directories to INSTALL_DIR and extract the contents of rsm11appserver.zip.

Configure the RSM 11 Application Files

The install.sh script will prompt for configuration values for your environment. This script will configure rsm11.ear and the RSM 11 client files. See Appendix A of this document for details on which files are being configured by this script.

1. Change directories to INSTALL_DIR/rsm11/bin
2. Make sure the install.sh script is executable (Example: chmod 755 install.sh).
3. Gather the following information regarding your environment and run install.sh.

RSM provider URL (jndi_providers.xml): This is the JNDI provider URL that is used to connect to the RSM application. In a WebSphere deployment it is of the format iiop://<server>:<bootstrap_port>.

RPM provider URL (jndi_providers.xml): The JNDI provider URL for the RPM application that will use this RSM application. (iiop://<server>:<bootstrap_port>).

Base URL for RSM client code (rsm11.jnlp): The HTTP URL to the parent directory of the RSM client files (Example: http://myserver:8000/rsm). If you are using JNLP templates from the Navigator application to access RSM, you will need to update them with this URL. See the rsm11.jnlp file for an example.

LDAP provider URL (security.properties): The URL to the LDAP directory server used by this RSM application (Example: ldap://myldaphost:389/). Simply press enter if you are going to use XML-based authentication instead of LDAP.

LDAP base DN (security.properties): RSM needs a directory entry to use as a starting point for user searches. (Example: cn=Users,o=MyCompany,c=us). Simply press enter if you are going to use XML-based authentication instead of LDAP.

LDAP search user DN (security.properties): In order to read from the LDAP directory, RSM must first authenticate as a user in the directory. This is the user that RSM will use to authenticate. (Example: cn=AdminUser,o=MyCompany,c=us). Simply press enter if you are going to use XML-based authentication instead of LDAP.

LDAP search user password (security.properties): The password for the LDAP search user provided. Simply press enter if you are going to use XML-based authentication instead of LDAP.

LDAP user search filter (security.properties): When RSM searches the LDAP directory for a user, it will use an LDAP search filter (Example: (&(objectClass=retailUser) %v)). Simply press enter if you are going to use XML-based authentication instead of LDAP.

> **Note**: The ampersand (&) character must be escaped with 2 backslash (\) characters. For example, if your search filter is (&(objectClass=retailUser) %v) then you must provide the string (\\&(objectClass=retailUser) %v) to install.sh.

Attribute used for firstname (security.properties): The name of the LDAP attribute that is used to store first names. Simply press enter if you are going to use XML-based authentication instead of LDAP.

Attribute used for lastname (security.properties): The name of the LDAP attribute that is used to store last names. Simply press enter if you are going to use XML-based authentication instead of LDAP.

Attribute used for username (security.properties): The name of the LDAP attribute that is used to store usernames. Simply press enter if you are going to use XML-based authentication instead of LDAP.

RSM login module type (dao_rsm.xml): RSM offers both LDAP- and XML-based authentication. This is where you should specify 'xml' if you are using XML-based authentication instead of LDAP. The default value is 'ldap'.

RSM logging level (log4j.xml): The initial log level for the RSM application. Possible values for this in decreasing order of granularity are DEBUG, INFO, WARN, ERROR, and FATAL. The default level is ERROR.

After install.sh has completed you can proceed with deploying rsm11.ear in the WebSphere Application Server.

Deploy rsm11.ear in WebSphere Application Server 5.1.1.10

1. Open the WebSphere Administrative Console that is to be used for administering the RSM 11 application -http://<server>:<admin_port>/admin

> **Note:** Prior to proceeding to ear deployment it is necessary to inject the hibernate2.jar file into the RSM11.ear file. Due to open source licensing restrictions, clients are required to manually download and install hibernate2.jar. A utility for automatically validating the downloaded hibernate2.jar version and adding the jar to the RSM11.ear file may be obtained from the Retek Fulfillment Site. Supporting documentation is also included in the zip file.

2. Click on Applications->Install New Application.
3. Under Preparing for the application installation, select the Server path radial button and set this field to INSTALL_DIR/rsm11.ear (from step 3 above), and then click Next.

> **Example**: Server Path: /u01/websp/rsm11/rsm11.ear

4. Accept the default options for Steps 1 – 3; clicking Next until reaching "Step 4 : Map modules to application servers".
5. Under "Step 4 :Map modules to application servers", select the server which will be used for deploying the application (default server is server1), check the checkbox for

the RSM module and click the Apply pushbutton. The Server field will be updated with the appropriate server. Click Next.

6. Accept the default options for the rest of the application installation and click Next until reaching "Step 6: Summary".
7. Under "Step 6: Summary", verify all installation information is correct and click Finish. This may take several minutes. Upon completion, the message "Application RSM11 installed successfully" should appear".
8. Click the Save to Master Configuration link when it appears.
9. Click the Save button in the Save to Master Configuration section. Following a successful save, you will be re-directed to the WebSphere Application Server Administrative Console.
10. Click on Applications->Enterprise Applications; click on the RSM11 application link to load the RSM application configuration page
11. Under General Properties, set the Classloader Mode property to PARENT_LAST, and then click the OK button.
12. Save to master configuration.

3

Client Installation Instructions

The install.sh script configured the rsm11.jnlp and rsmBC.jnlp files on the client side so that they have the correct HTTP URLs for their base folders and the icon locations. To complete installation of the client files, you must copy them onto the HTTP server.

The following steps describe how the RSM 11client is installed. The configuration assumes the IBMHttpServer is configured to be the front-end to the WebSphere Application Server where the rsm11.ear file is installed and configured.

Note: Java WebStart is required to distribute and update Java client code via HTTP. Beginning with Sun JRE 1.4.2+, Java WebStart came was shipped as part of the Sun JRE. Sun JRE 1.4.2+ can be downloaded from the Sun site - http://java.sun.com. Sun JRE 1.4.2+ must be installed on the client PC in order for the RSM 11client to run.

Note: To launch the RSM client from Retek Navigator, the jnlpgen web application must first be installed.

Note: RSM is not certified to run against Java WebStart version 1.5.

1. On the webserver, change directories to the document root for IBMHttpServer. This location can be determined by examining the file IBMHttpServer/conf/httpd.conf; the value for the DocumentRoot directive in this file specifies the document root for IBMHttpServer.

   Example: cd /u00/websp/IBMHttpServer/htdocs/en_US

2. Create a /rsm directory under the DocumentRoot directory

   Example: mkdir rsm

3. Change directories to the newly created rsm directory beneath the document root.
4. Copy the rsm client files located in the INSTALL_DIR/client directory into the newly created current directory.

   Example:
   ```
   /u00/websp/IBMHttpServer/htdocs/en_US/rsm> cp –r
   /u00/websp/rsm11en/client ./
   ```

5. Edit the file IBMHttpServer/conf/mime.types by adding the jnlp MIME type: application/x-java-jnlp-file   jnlp

   Example:
   ```
   application/x-javascript          js
   application/x-java-jnlp-file jnlp
   application/x-koan                skp skd skt skm
   ```

   Note: The x-java-jnlp-file MIME type may have already been added in a previous application installation. If the MIME type already exists this step can be ignored.

6. Reload the IBMHttpServer for the above changes to take effect.

4

Test the RSM Client

The RSM client is launched through the jnlpgen web application. The jnlpgen web application must be installed to test the RSM client. See the jnlpgen documentation included in the Retek Navigator Install Guide for more information on configuring the RSM jnlp template and launching the RSM client.

Review the Retek Security Manager User Guide for instructions on how to create roles, assign permissions to roles, and assign users to roles. Please note that users are not created in RSM. Rather, RSM looks up users that exist in a Lightweight Directory Access Protocol (LDAP) compliant directory service. A test user should be defined in the directory service so that you can test assigning users to the roles you create.

A

Appendix: RSM Configuration Files

The install.sh script will prompt you for the values it needs to configure the appropriate set of files for the RSM application. This section documents which files are configured by install.sh and where you can find them to do manual configuration later.

Directory Server Information in security.properties

RSM supports both file and directory server based user authentication and searching. If an LDAP compliant directory server is used, follow the steps below to configure RSM to use your directory server. If file based user authentication and searching is used, the LDAP settings will be ignored. To use LDAP, update the LDAP settings in the file security.properties to match your organization's LDAP configuration. File security.properties can be found at WAS_HOME/installedApps/<node>/RSM11.ear/conf/retek.

- Update the authentication provider URL to point to the appropriate LDAP server.

Example:

```
ldap.authenticationprovider.url=ldap://64.238.67.60:389/
ldap.authenticationprovider.url=<ldap://host:port/>
```

- Update the Distinguished Name where users exist on LDAP server.

Example:

```
ldap.user.basedn=ou=XXX,dc=XXXAD,dc=local
ldap.user.basedn=<ou=orgUnit1,dc=domComponent1,dc=domComponennt2…>
```

- Update the parameters for the administrative user that performs searches on behalf of RSM.

Example:

```
ldap.usersearch.user=cn=Administrator,cn=users,dc=rcomad,dc=local
```

Example:

```
ldap.usersearch.password=PaSsW0rD
ldap.usersearch.user=<distinguishedUser>
ldap.usersearch.password=<password>
```

- Update the search filter used to limit the records that are returned when RSM searches for users. The filter represents conditions that must be met for records to be included in the result set. The example below reflects a base Active Directory install. The %v parameter is required by RSM regardless of directory server implementation.

Example:

```
ldap.user.filter=(&(objectCategory=person)(objectClass=user) %v)
ldap.user.filter=<(&(base user search filter) %v)>
```

- Update the LDAP variable mappings if necessary. The variable mappings below, used to map LDAP to the directory schema, reflect a base Active Directory install. If these variable names differ from the LDAP directory server attributes, they should be updated accordingly.

> **Example:** ldap.firstname.attrname=givenName
> ldap.lastname.attrname=sn
> ldap.username.attrname=samAccountName
>
> **Note:** Security.properties also contains examples of ldap variable mappings for a base OpenLDAP implementation.
>
> **Note:** RSM executes only READ operations against the LDAP directory server; no ADD, UPDATE or DELETE operations.
>
> **Note:** For initial login to RSM to be possible, the user inserted into the database through the rsm sql (Chapter 2 above) must also be a valid user on the LDAP Directory Server. More specifically the user name inserted into the database must match a valid entry for LDAP mapping attribute ldap.username.attrname.

LoginModule Information in security.properties

The login module setting configures the system to point to the applicable user repository (such as a directory server or xml file) for authentication. The login module value determines the JAAS login module that is responsible for accessing the user repository for authentication.

Example authenticating against an LDAP compliant directory server:

loginmodule=Retek.Ldap.LoginModule

Example authenticating against the RSM users XML file:

loginmodule=Retek.XML.LoginModule

> **Note:** This setting should correspond with the user dao implementation setting found in file dao_rsm.xml. More information on this setting can be found below. Also, if the XMLLoginModule is used, users must be added to file users_rsm.xml. More information on this setting can be found below.

User Search Information in dao_rsm.xml

These values are used to configure the user repository that is used by RSM for user searches. The default value is to use an LDAP compliant directory server as the user repository. Besides LDAP, XML file based searches are also supported. To switch between LDAP and XML, comment (uncomment) the ‘impl package’ tags associated with the dao.user interface package. This file can also be found in directory WAS_HOME/installedApps/<node>/RSM11.ear/conf/retek.

> **Note:** This setting should correspond with the Login Module configuration information found in the security.properties file (details above).

Note: If xml is chosen as the data access implementer, users must be added to file users_rsm.xml.

User Information in users_rsm.xml.

If XML is used for authentication and user searching, this file is used as the repository for the users. It must contain the userNames, first names, last names and passwords of all valid users. This file can also be found in directory WAS_HOME/installedApps/<node>/RSM11.ear/conf/retek.

Note: If LDAP is used for authentication and user searching, this file is ignored.

For example:

```
<users>

<user username="Valid.User" firstname="Valid" lastname="User"
password="PaSsW0rD"/>

<user username="Alain.Frecon" firstname="Alain"
lastname="Frecon" password="retekPassword"/>

</users>
```

RPM Bootstrap Information in jndi_providers_rpm.xml

Retek Security Manger requires data from other applications in order to administer data level permissions. The file jndi_providers_<app>.xml contains the information necessary for RSM to communicate with other Retek applications. Change to directory INSTALL_DIR/rsm11.ear/conf/retek and update jndi_providers_<app>.xml with the correct WebSphere BOOTSTRAP_ADDRESS of the respective application.

Example:

```
<ejb_context_overrides>
  <provider app="app.rpm" url="iiop://server1:15809"
factory="com.ibm.websphere.naming.WsnInitialContextFact
ory">
  </provider>
</ejb_context_overrides>
```

1. In the WebSphere Administration Console, select Applications → Enterprise Applications, and start the rsm11 application.
2. At this point, the rsm11 application should have solid green arrow indicating successful startup.

Client Settings in rsm11.jnlp and rsmBC.jnlp

The rsm11.jnlp file points the WebStart client to the RSM application running in the WebSphere Application Server. Within this file is the HTTP URL through which it is accessed. rsm11.jnlp also depends on rsmBC.jnlp to use the BouncyCastle encryption library.

The install.sh script will set the HTTP URLs in both of these files, but if you are using template files within the Navigator application you will have to make these updates manually to those files.