Retek® Security Manager™ 11.1.1

Installation Guide

Corporate Headquarters:

Retek Inc.
Retek on the Mall
950 Nicollet Mall
Minneapolis, MN 55403
USA

888.61.RETEK (toll free US)
Switchboard:
+1 612 587 5000

Fax:
+1 612 587 5100

European Headquarters:

Retek
110 Wigmore Street
London
W1U 3RW
United Kingdom

Switchboard:
+44 (0)20 7563 4600

Sales Enquiries:
+44 (0)20 7563 46 46

Fax:
+44 (0)20 7563 46 10

The software described in this documentation is furnished under a license agreement, is the confidential information of Retek Inc., and may be used only in accordance with the terms of the agreement.

No part of this documentation may be reproduced or transmitted in any form or by any means without the express written permission of Retek Inc., Retek on the Mall, 950 Nicollet Mall, Minneapolis, MN 55403, and the copyright notice may not be removed without the consent of Retek Inc.

Information in this documentation is subject to change without notice.

Retek provides product documentation in a read-only-format to ensure content integrity. Retek Customer Support cannot support documentation that has been changed without Retek authorization.

The functionality described herein applies to this version, as reflected on the title page of this document, and to no other versions of software, including without limitation subsequent releases of the same software component. The functionality described herein will change from time to time with the release of new versions of software and Retek reserves the right to make such modifications at its absolute discretion.

Retek® Security Manager™ is a trademark of Retek Inc.

Retek and the Retek logo are registered trademarks of Retek Inc.

This unpublished work is protected by confidentiality agreement, and by trade secret, copyright, and other laws. In the event of publication, the following notice shall apply:

©2005 Retek Inc. All rights reserved.

All other product names mentioned are trademarks or registered trademarks of their respective owners and should be treated as such.

Printed in the United States of America.

Customer Support

Customer Support hours

Customer Support is available 7x24x365 via email, phone, and Web access.

Depending on the Support option chosen by a particular client (Standard, Plus, or Premium), the times that certain services are delivered may be restricted. Severity 1 (Critical) issues are addressed on a 7x24 basis and receive continuous attention until resolved, for all clients on active maintenance. Retek customers on active maintenance agreements may contact a global Customer Support representative in accordance with contract terms in one of the following ways.

Contact Method	Contact Information
E-mail	support@retek.com
Internet (ROCS)	rocs.retek.com Retek's secure client Web site to update and view issues
Phone	+1 612 587 5800

Toll free alternatives are also available in various regions of the world:

Australia	+1 800 555 923 (AU-Telstra) or +1 800 000 562 (AU-Optus)
France	0800 90 91 66
Hong Kong	800 96 4262
Korea	00 308 13 1342
United Kingdom	0800 917 2863
United States	+1 800 61 RETEK or 800 617 3835
Mail	Retek Customer Support Retek on the Mall 950 Nicollet Mall Minneapolis, MN 55403

When contacting Customer Support, please provide:

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

Contents

Chapter 1 – Hardware and Software Requirements

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.

Database Server

General requirements for a database server capable of running RSM include:

- UNIX based OS certified with Oracle RDBMS 9i release 2 Enterprise Edition (options are AIX5.2, Solaris 9, and HP-UX 11.11)
- Oracle RDBMS 9i release 2 Enterprise Edition

Application Server

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

- UNIX based OS certified with IBM WebSphere Application Server version 5.1.. (options are AIX5.2, Solaris 9, and HP-UX 11.11)
- IBM WebSphere Application Server version 5.1.

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.

Client PC and Web Browser Requirements

Client PC requirements

- Operating system: Windows 2000 or XP
- Display resolution: 1024x768
- Processor: 1GHz or higher;
- Memory: 512MBytes or higher;
- Sun J2RE Runtime equal to v1.4.1.

Browser requirements

The browser is used to launch the Java WebStart client. The following browsers are supported :

- Microsoft Internet Explorer 5.5 or higher.

Chapter 2 – Database Configuration Instructions

Database Server Installation Instructions

Note: This database installation is being done on top of RSM 11.0.2. Please make sure RSM 11.0.2 is installed. The RSM schema owner will be refered to as RSM11DEV for this installation.

RSM database files

1. Log into the UNIX server as retek.
2. Create a staging directory for the RSM database installation software. There should be a minimum of 1 MB disk space available.
3. Copy the rsm11dbserver.zip file from the CD/dbserverunix directory to the staging directory. This will be referred to as INSTALL_DIR for the remainder of this chapter.
4. Change directories to INSTALL_DIR and extract the rsm11dbserver.zip file.
5. Log into sqlplus as RSM11DEV and run the following command:

   SQL> @rsm11-1-1ctl.sql
6. Check the log file rsm11-1-1ctl.log for any errors.
7. If this is a French installation of RSM, change directories to INSTALL_DIR
8. Make sure your NLS_LANG is set to FRENCH_FRANCE.utf8
9. Log into sqlplus as RSM11DEV and run the following command:

   ```
   SQL> @rsm11-1-1ctl_fr.sql
   ```
10. Check the log file rsm11-1-1ctl_fr.log for any errors.

Chapter 3 – 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, assuming WebSphere Application Server (WAS) and IBMHttpServer 5.1 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 1.4.1 is required for RSM (and is shipped with Websphere 5.1)

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 is installed (ie: /u00/websp/jdbc/ojdbc14.jar)

Configure WebSphere 5.1 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 documentation for the correct URL.
   - server = name or IP address of server where WebSphere 5.1 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 Servers-> Application Servers.
14. 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.
15. In the Additional Properties section click on the End points link in the lower section of the page.
16. 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.
17. 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.

Deploy rsm11.ear in WebSphere Application Server 5.1

1. Log into the UNIX server where WebSphere 5.1 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.
4. 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.
5. Click on Applications->Install New Application.
6. 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
7. Accept the default options for Steps 1 – 3; clicking Next until reaching “Step 4 : Map modules to application servers”.
8. 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.
9. Accept the default options for the rest of the application installation and click Next until reaching “Step 6: Summary”.
10. 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”.
11. Click the Save to Master Configuration link when it appears.
12. 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.
13. Click on Applications->Enterprise Applications; click on the RSM11 application link to load the RSM application configuration page
14. Under General Properties, set the Classloader Mode property to PARENT_LAST, and then click the OK button.
15. Save to master configuration.

16. At this point the RSM application has been installed but there are some files that must be configured to match the current installation. First the directory server properties must be updated. Second, if RSM is being used in conjunction with Retek Price Management (RPM), RSM must be configured to point at RPM to administer data level permissions.

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 class value determines the class that is responsible for accessing the user repository for authentication.

  Example authenticating against an LDAP compliant directory server:

  ```
  loginmodule.class=com.retek.rsm.domain.security.dao.LdapLoginModule
  ```

  Example authenticating against the RSM users XML file:

  ```
  loginmodule.class=com.retek.rsm.domain.security.dao.XMLLoginModule
  ```

  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.WsnInitialContextFactory">
  </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.

Chapter 4 – Client Installation Instructions

The following steps describe how the RSM 11client is configured. 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 1.4.1+ 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 zip file located in the INSTALL_DIR/client directory into the newly created current directory.

   

   Example: /u00/websp/IBMHttpServer/htdocs/en_US/rsm> cp /u00/websp/rsm11en/client/RsmClient.zip

5. Unzip the RSM client zip file.

   

   Example: /u00/websp/IBMHttpServer/htdocs/en_US/rsm> unzip RsmClient.zip

6. Update the jnlp extension file rsmBC.jnlp located in the directory DocumentRoot/rsm/client. The jnlp codebase parameter points to the base URL where the RSM client code resides.

   

   Example: <jnlp codebase=”http://server:9081/rsm/client” spec=”1.0+” href=”rsmBC.jnlp”>

   The icon href parameter indicates the icon that will be displayed by Java WebStart when the RSM client is downloaded. The parameter should point to the .jpg file located in the directory DocumentRoot/rsm/images/.

   

   Example: <icon href=”http://server:9081/rsm/client/images/retek_logo.jpg”/>

7. 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.

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

Chapter 5 – 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.

Appendix A – Retek User Creation Script

Run the following commands as the sysdba user. Replace “schema_owner” with an appropriate account name. The empty role developer must be created before running the following commands.

```
create user schema_owner
identified by retek
default tablespace RETEK_DATA
temporary tablespace temp;
grant select_catalog_role,
      alter session,
      analyze any,
      create any synonym,
      create any type,
      create database link,
      create library,
      create procedure,
      create public database link,
      create public synonym,
      create sequence,
      create session,
      create synonym,
      create table,
      create trigger,
      create view,
      drop any synonym,
      execute any procedure,
      execute any type,
      select any sequence,
      select any table,
      query rewrite,
      create materialized view to &schema_owner
/
alter user schema_owner quota unlimited on retek_data
/
alter user schema_owner quota unlimited on retek_index
/
alter user schema_owner quota unlimited on lob_data
```

```
/
grant select on sys.dba_role_privs to schema_owner
/
grant select on sys.dba_jobs to schema_owner
/
grant select on sys.dba_roles to schema_owner
/
```