Retail passion. Innovative solutions.

Retek® Security Manager™ 11.0

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.

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This unpublished work is protected by confidentiality agreement, and by trade secret, copyright, and other laws.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:

©2004 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 a Microsoft Active Directory – 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

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

- Microsoft Windows 2000 (Service Pack 4) Active Directory or greater.
- LDAP version 3.0 compliant.

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

Create a UNIX user account to install the software

1 Create a UNIX group named “dev”.

2 Create UNIX user named “retek” and assign it to the “dev” group. This user will install the RSM software

Create Staging Directory for 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.

Create RSM Schema Owner

Create the Oracle db user that will own the RSM application. Refer to Appendix A.

1 Change directories to INSTALL_DIR/

2 Log into sqlplus as sysdba and enter the following command to create the schema owner. The following will be prompted for:

Schema Owner – The Oracle user that will own all RSM objects. Referred to in this install guide as RSM11DEV

Password – The password for RSM11DEV

Temp Tablespace – the Temporary Tablespace for RSM11DEV

```
SQL> @create_user.sql
```

3 Check the log file create_user.log for any errors. This log file should be removed to prevent the password from being compromised.

Create RSM tables

Note: Ensure the following table spaces exist: RETK_DATA and INDEX_DATA. Without these tablespaces the ddl will fail

1. Change directories to INSTALL_DIR/
2. Log into sqlplus as RSM11DEV and run the following command:

   ```
   SQL> @rsm11ddl.sql
   ```

Check the log file rsm11ddl.log for any errors.

Insert RPM data

Note: This section requires data that was sent with RPM please refer to the RPM INSTALL DIR/rsm folder

1. Change directories to RPM_INSTALL_DIR/rsm.
2. Log into sqlplus as RSM11DEV and run the following command:

```
SQL> @rpm11rsm.sql
```

3. Check the log file rpm11rsm.log for any errors.

Insert data for RSM

Note: The test user name (‘abby.dawkins’) should be updated to a valid user within your organization. This name also needs to correspond to a valid user from the LDAP directory srever user by RSM.

1. Change directories to INSTALL_DIR.
2. Log into sqlplus as RSM11DEV and run the following command:

   ```
   SQL> @rsm11ctl.sql
   ```

3. Check the log file rsm11ctl.log for any errors.

Note: Some of the data needed for RSM to function correctly is customer specific and cannot be automatically inserted during implementation. For RPM data, customers must query RMS data to get the IDs of their departments and zone groups and create permissions for these IDs. Refer to the RSM release notes for additional information on completing these tasks.

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 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: ojdbc14.jar is required for RSM 11. This file can be obtained from the Oracle Technology Network web side, and must be copied to a staging directory on the webserver 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:

- 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 and then click Apply.

8 Create a new JDBC Provider by clicking New.

- Select Oracle JDBC Driver (XA) from JDBC list of values and click Apply

9 Under General Properties, click Apply.

10 Under Additional Properties for the Oracle JDBC Driver (XA), select Data Sources and then New, 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 4 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

11 Under Additional Properties, click Custom Properties for the Data Source. Remove all properties except for URL and transactionBranchesLooselyCoupled by checking the check-box for each of these unneeded properties and then clicking the Delete button. Now click URL and 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 and then OK
- Click transactionBranchesLooselyCoupled and set the Value field to true
- Click Apply and then OK

12 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.

13 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.

14 Click on Servers-> Application Servers.

15 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.

16 In the Additional Properties section click on the End points link in the lower section of the page.

17 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 other Retek applications.

18 Under SOAP_CONNECTOR_ADDRESS, verify the Host and Port are set correctly.

Deploy rsm11.ear in WebSphere Application Server 5.1

1 Log into the UNIX webserver 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 20 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 rsm11appserver.zip.

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

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: /u00/websp/rsm11/rsm11.ear

7 Accept the default options for the rest of the application installation until reaching “Step 6: Summary”.

8 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”.

9 Click the Save to Master Configuration link when it appears.

10 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.

11 Click on Applications->Enterprise Applications.

12 Click on the rsm11 application link to load the RSM application configuration page.

13 Set the Classloader Mode property to PARENT_LAST, and then click the OK button.

14 Save to master configuration once again.

15 At this point the RSM application has been installed but its directory server properties must be updated to match your configuration. WAS_HOME below refers to the location where WebSphere is installed for RSM. Change to directories to WAS_HOME/installedApps/<node>/RSM11.ear/conf/retek. Here you’ll need to update the LDAP settings in security.properties to match your organization’s ldap server settings.

- Update the provider url to point to the LDAP server.

  Example: ldap.authenticationprovider.url=ldap://host:port/

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

  Example:
  ldap.user.basedn=ou=orgUnit1,dc=domComponent1,dc=domComponennt2

- Update the information of the super user that performs searches on behalf of RSM.

  Example: ldap.usersearch.user=distinguishedUser
  ldap.usersearch.password=password

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

  - **Example:** ldap.user.filter=(&(base user search filter) %v)

  Note: The security.properties file contains variable mappings that are used to map LDAP to the directory schema. The mappings below illustrate a base Active Directory install. If these mappings differ from a client's directory server attributes, the security.properties file will need to be updated accordingly.

  ldap.dn.attrname=distinguishedName

  ldap.address.attrname=streetAddress

  ldap.city.attrname=l

  ldap.country.attrname=c

  ldap.county.attrname=county

  ldap.employeenum.attrname=employeeID

  ldap.firstname.attrname=givenName

  ldap.lastname.attrname=sn

  ldap.locphone.attrname=homePhone

  ldap.postalcode.attrname=postalCode

  ldap.primaryloc.attrname=physicalDeliveryOfficeName

  ldap.state.attrname=st

  ldap.supervisor.attrname=manager

  ldap.phone.attrname=telephoneNumber

  ldap.username.attrname=samAccountName

  ldap.modifyTimestamp.attrname=modifyTimestamp

16 In the WebSphere Adminitration Console, select Applications → Enterprise Applications, and start the rsm11 application.

17 At this point, the rsm11 application should have a solid green arrow indicating successful startup.

Configure the RSM Content Model

The RSM Content Model file for RPM must be copied to the RSM application in WebSphere. This file exists in INSTALL_DIR/rpm11 from the RPM 11 installation. The following step is also listed in the RPM installation guide. Ensure that this step has been performed either during the RPM install or during the RSM install. WAS_HOME below refers to the location where WebSphere is installed for RSM.

1 Retrieve the content_model.xml file from the RPM INSTALL_DIR directory and copy it to the RSM 11 classpath directory in WebSphere.

```
> cp content_model.xml $WAS_HOME/installedApps/<node>/RSM11.ear/conf/retek
```

Chapter 4 – Directory Server

Only attributes from the base Active Directory LDAP schema are required for RSM to function. The specific attributes required by RSM are:

- sAMAccountName (Account Name)
- sn (Last name or surname)
- givenName (First name)

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 via script create_rsm.sql (Chapter 2 above) must also be a valid user in your organization’s LDAP Directory Server. More specifically the user name inserted into the database must match a valid entry for LDAP attribute sAMAccountName.

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
/
```