Retail passion. Innovative solutions.

Retek® Security Manager™ 11.0.1

Release Notes

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

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.

Release Notes

Overview

RSM is an application that provides a retailer's Retek applications with a centralized method of authenticating and authorizing system users. RSM leverages a Lightweight Directory Access Protocol (LDAP)-compliant directory service to authenticate valid users. RSM provides centralized administration screens for system administrators to:

- Safely pass encrypted passwords
- Maintain roles
- Add workflow permissions roles
- Create data permissions and assign them roles
- Assign users to roles
- Maintain external Retek passwords

See the RSM Install Guide, Operations Guide and User Guide for more detailed information relating to Retek Security Manager.

New Features

- The 11.0.1 release of RSM includes a Graphical User Interface. The GUI is responsible for presenting data to the security administrator and for receiving data directly from the security administrator through the 'front end'. It was developed using a Java Swing framework, which is a toolkit for creating rich presentation in Java applications.
- Certification of OpenLDAP as a valid directory server with RSM

Notes

- RSM 11.0.1 is a full install, not a patch of RSM 11.0. If this version of RSM is being installed over RSM 11.0, all data in the RSM database will be overwritten during installation. To retain your existing data, be sure to back up the existing tables or export the data to flat files.
- Retek Price Management (RPM) is dependant on RSM for authorization and authentication, RSM should be installed prior to installing RPM. RSM is dependent on RPM to administer RPM's data level permissions; RPM must be installed before testing this functionality within RSM. Please see both the RPM and RSM installation and operations guides for further information.
- Retek Navigator is dependent on RSM for authorization and authentication. RSM should be installed prior to installing Retek Navigator.

- RSM 11.0.1 has been tested with the following Retek application versions:
  - RMS 11.0.2 Patch
  - Alloc 11.0.2 Patch
  - ReIM 11.0.2 Patch
  - RPM 11.0.1
  - RIB 11.0.2 Patch
  - RETL 11.2.1 Patch
  - RDW 11.0 INITIAL RELEASE
  - ISO 11.0 INITIAL RELEASE
  - RDM 10.3.5 (as test tool only)
  - RSL 11
  - ARI 11.0

Description of RSM tables

ROLE

This table defines the roles available to users. It is loaded with an initial Role during the RSM implementation.

Columns

- ID: Sequence form ROLE_SEQ.
- ROLE_DESCRIPTION: Description of the role.

USER_ROLE

This table links users to a particular Role as defined by the ROLE table. The users should be the same IDs as those used in LDAP.

During the implementation of RSM, a test user will be inserted into this table. This user must be changed to match a user in the client's LDAP compliant user directory.

Columns

- ID: Sequence from USER_ROLE_SEQ.
- USER_ID: Enterprise ID from LDAP compliant user directory.
- ROLE_ID: Role ID that this user is being added to. From the ROLE table.
- START_DATE_TIME: Date this USER/ROLE relationship becomes effective. Null or blank in this field means the USER/ROLE is effective immediately and indefinitely.
- END_DATE_TIME: Date this USER/ROLE relationship ends. Null or blank in this field means the USER/ROLE relationship will not expire.

APP_LAUNCH_PARAMETER

This table contains launch parameters for other Retek applications. If applicable, this table is loaded as part of the RSM install and will not need to be updated after that.

NAMED_PERMISSION

This table contains the permissions defined by Retek applications. This table is updated as part of the RSM installation and will not need to be updated after that.

NAMED_PERMISSION_DSC

This table contains the descriptions for the Named Permissions. This table is updated as part of the RSM install and will not need to be updated after that.

ROLE_NAMED_PERMISSION

This table links (assigns) a Named Permission to a particular Role.

Columns

- ID: Sequence ROLE_NAMED_PERMISSION_SEQ.
- ROLE_ID: ID of the associated Role from the ROLE table.
- PERMISSION_ID: ID of the associated Named Permission from the NAMED_PERMISSION table.
- IS_VIEW: Boolean indicting if this permission has view access.
- IS_EDIT: Boolean indicting if this permission has edit access.
- IS_SUBMIT: Boolean indicting if this permission has submit access.
- IS_APPROVE: Boolean indicting if this permission has approve access.
- IS_EMERGENCY: Boolean indicting if this permission has emergency access.

Note: You cannot define the Boolean attributes as true unless true has been defined for this permission and attribute in the NAMED_PERMISSION table.

HIERARCHY_TYPE

This table describes the different hierarchy types used by different applications For example: The merchandise and location hierarchies used by RPM. This data is loaded during RSM implementation and will not need to be updated after that.

HIERARCHY_PERMISSION

This table defines the actual hierarchy permissions for the system, very similar to the named permissions. These permissions can be defined for a location hierarchy at the zone group or zone level, and for a merchandise hierarchy at the department, class, or subclass level.

Columns

- ID: Sequence HIERARCHY_PERMISSION_SEQ.
- CHILD_ID: Future functionality; can be null for now.
- REFERENCE_CLASS: Fully qualified class name of the object this permission is representing (for example, a department).
- OBJECT_ID_NAME: Fully qualified class name for the type of the object id. For example:
- “com.retek.platform.bo.LongObjectId”,
- “com.retek.platform.bo.DualLongObjectId”
- “com.retek.platform.bo.TripleLongObjectId”.
- KEY_VALUE: The business object’s id. For example: The department ID or for a class, the department ID, semi-colon class ID.

ROLE_HIERARCHY_PERMISSION

The ROLE_HIERARCHY_PERMISSION table links Roles to Hierarchy Permissions.

Columns

- ID: Sequence ROLE_HIERARCHY_PERMISSION_SEQ.
- ROLE_ID: The ID column of the ROLE table.
- PARENT_ID: The ID values of the HIERARCHY_PERMISSION table.
- HIERARCHY_TYPE_ID: The ID column of the HIERARCHY_TYPE table. Make sure to use the correct hierarchy. For example, if the hierarchy permission is a merchandise hierarchy, use the merchandise hierarchy type. If the hierarchy permission is a location hierarchy, use the location hierarchy type.
- START_DATE_TIME: The date this ROLE/HIERARCHY PERMISSION relationship becomes effective. Null or blank in this field means the relationship is effective immediately and indefinitely.
- END_DATE_TIME: The date this ROLE/HIERARCHY PERMISSION relationship ends. Null or blank in this field means the relationships will not expire.

USER_LOGIN_INFO

This table contains information pertaining to failed user logins. Only valid user names (those in the enterprise LDAP server) will be inserted.

Columns

- ID: Sequence USER_LOGIN_INFO_SEQ.
- USER_ID: The User ID of the client that failed login. Must be a valid User ID.
- CURR_AUTH_FAILURS: The number of times this user has failed logging in since last successfully logging in.
- LAST_FAIL_DATE: The date this user last failed logging in.

To unlock a user that has been locked out, simply delete the row of the User that is locked out.