Retail passion. Innovative solutions.

Retek® Security Manager™ 11.0

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.

Overview

This version of Retek Security Manager does not include a graphical user interface. It will be necessary to update the RSM database during implementation and possibly at other times during a workflow. Below are descriptions of the tables and examples of how to update them.

Description of RSM tables and SQL examples

ROLE

This table defines the roles available to users.

This table is loaded with an initial Role during the RSM implementation.

Columns

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

Example: Create a new Role:

```
INSERT INTO ROLE (ID, ROLE_DESCRIPTION) VALUES (ROLE_SEQ.NEXTVAL,
'TEST ROLE1');
```

USER_ROLE

This table links users to a particular Role (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.

Example: Adding a user to an existing Role:

```
INSERT INTO USER_ROLE (ID, USER_ID, ROLE_ID, START_DATE_TIME) VALUES
(USER_ROLE_SEQ.NEXTVAL, 'Valid.User', -1001,
to_date('2004/10/01:12:00:00AM', 'yyyy/mm/dd:hh:mi:ssam');
```

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

Example: Assigning a Named Permission to a Role:

```
INSERT INTO ROLE_NAMED_PERMISSION (ID, ROLE_ID, PERMISSION_ID,
IS_VIEW, IS_EDIT, IS_SUBMIT, IS_APPROVE, IS_EMERGENCY) VALUES
(ROLE_NAMED_PERMISSION_SEQ.NEXTVAL, -1000, -1000, 0, 0, 0, 0, 0);
```

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.

 **Note:** This table is *not* populated as part of the RSM installation and must be populated for hierarchy permissions to work correctly.

For departments, customers have to query RMS data and get the ids of their departments. Each department must be inserted into the Hierarchy Permission table. Execute included SQL Script createRoleHierarchyPermissionForMerchandiseType.sql once for every department, entering the department Id and role Id as instructed. This script creates the permission and adds it to the ROLE_HIERARCHY_PERMISSION table described below.

For zone groups, customers have to run the SQL below for each zone group id. Execute included SQL script createRoleHierarchyPermissionForLocationType.sql once for every zone group, entering the zone group Id and role Id as instructed. This script creates the permission and adds it to the ROLE_HIERARCHY_PERMISSION table described below.

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: 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: Date this ROLE/HIERARCHY PERMISSION relationship ends. Null or blank in this field means the relationships will not expire.

 **Note:** This table is *not* populated as part of the RSM installation. It is updated using the scripts defined above in the HIERARCHY_PERMISSION table section.

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 UserId of the client that failed login. Must be a valid UserId.
- 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.