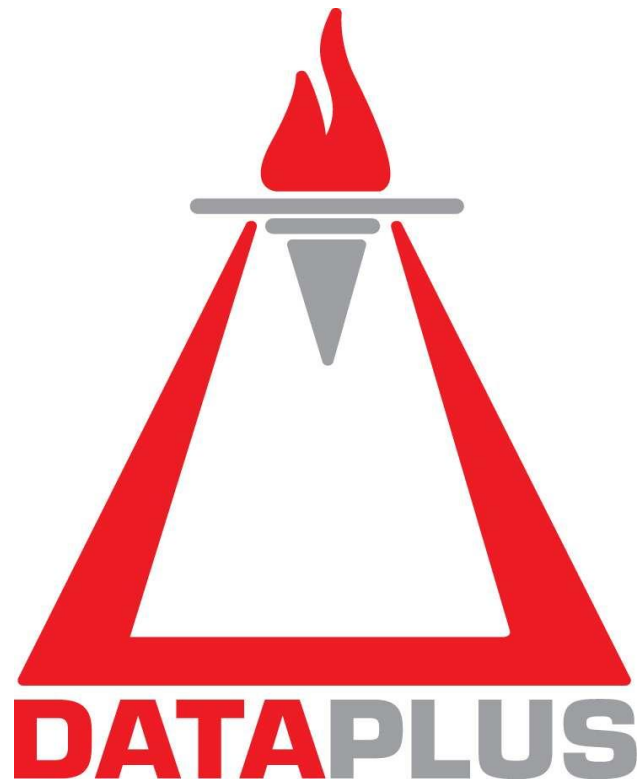


# Omega Core Audit <sup>TM</sup>

For Oracle Database



## OMEGA Core Audit

For Oracle Database

## User's Guide

**2.8.1**

[www.dataplus-al.com](http://www.dataplus-al.com)

## TABLE OF CONTENTS

1	CHAPTER 1: Omega Core Audit Overview.....	7
1.1	Introducing Omega Core Audit.....	7
1.2	Key Benefits.....	7
1.3	Omega Core Audit Architecture.....	8
1.3.1	Omega Core Audit Engine.....	8
1.3.2	Omega Core Audit Repository.....	9
1.3.3	Omega Core Audit Application.....	9
1.4	Compatibility and Requirements.....	10
1.4.1	Supported Oracle Database Versions and Releases.....	10
1.4.2	Supported Oracle Database Editions.....	10
1.4.3	Oracle Core Audit Application requirements.....	10
1.5	Limitations.....	11
2	CHAPTER 2: System Wide Functionalities, Utilities and Guidelines.....	12
2.1	Common Application functionalities.....	12
2.1.1	The target database.....	12
2.1.2	Client-side information retrieval.....	13
2.1.3	Information presentation.....	13
2.1.4	Data Exporting in standard file formats.....	14
2.1.5	DateTime Field Format.....	14
2.2	Secured Areas.....	15
2.3	Policy-Based Evaluation Model.....	15
2.3.1	Policies.....	15
2.3.2	Rules.....	15
2.3.3	Conditions.....	16
2.3.4	Factors.....	16
2.3.5	Policy Cache.....	16
2.4	Debug and Diagnostics.....	17
2.4.1	Client-Side User Debug.....	17
2.4.2	Server-Side Policy Debug.....	17
2.4.3	System Error Log.....	17
2.5	System Backup.....	19
2.5.1	Engine Backup.....	19
2.5.2	Repository Backup.....	19
2.6	Issue Tracking Module.....	20
3	CHAPTER 3: Unified Audit Trails.....	21
3.1	Unified Audit Trail repository fields.....	21
3.2	The Unified Audit Trail form.....	23
3.2.1	Unified Audit Trail - Issue Mark form.....	26
3.3	Automatic Audit Trail Management.....	27
3.4	The Unified Trail Monitoring form.....	28
3.5	The Unified Trail for Log Collector (SIEM) Systems.....	30
4	CHAPTER 4: Access Control.....	31
4.1	How it works.....	31
4.2	Access Control Guidelines.....	31
4.2.1	General Guidelines.....	31

4.2.2	Silent Access Control Module.....	32
4.3	Access Control Policies .....	33
4.3.1	Adding a new Access Control Policy .....	34
4.3.2	Opening/modifying an Access Control Policy .....	34
4.3.3	Deleting an Access Control Policy .....	35
4.3.4	Copying an Access Control Policy .....	35
4.3.5	Access Control Policy Status .....	35
4.4	Access Control Rules .....	36
4.4.1	Adding a new Access Control Rule .....	36
4.4.2	Opening/modifying an Access Control Rule .....	36
4.4.3	Deleting an Access Control Rule .....	37
4.4.4	Access Control Rule Status .....	37
4.5	Access Control Conditions.....	37
4.5.1	Adding a new Access Control Condition .....	38
4.5.2	Opening/modifying an Access Control Condition .....	38
4.5.3	Deleting an Access Control Condition .....	39
4.5.4	Access Control Condition Status .....	39
5	CHAPTER 5: Standard Audit .....	40
5.1	How it works.....	40
5.1.1	Activating the Standard Audit.....	40
5.2	Standard Audit Guidelines .....	40
5.3	Existing Oracle Standard Audits .....	41
5.4	Standard Audit Policies.....	42
5.4.1	Adding a new Standard Audit Policy .....	42
5.4.2	Opening/modifying a Standard Audit Policy.....	43
5.4.3	Deleting a Standard Audit Policy.....	44
5.4.4	Copying an Standard Audit Policy.....	44
5.4.5	Standard Audit Policy Status .....	44
5.5	Standard Audit Rules - Statement Audits.....	45
5.5.1	Adding a new single Standard Statement Audit (Rule).....	45
5.5.2	Adding new multiple Standard Statement Audits.....	46
5.5.3	Opening/modifying a Standard Statement Audit (Rule) .....	46
5.5.4	Deleting a Standard Statement Audit .....	47
5.5.5	Standard Statement Audit Status .....	47
5.6	Standard Audit Rules - Object Audits .....	48
5.6.1	Adding a new single Standard Object Audit.....	48
5.6.2	Adding new multiple Standard Object Audits .....	49
5.6.3	Opening/modifying a Standard Object Audit .....	49
5.6.4	Deleting a Standard Object Audit .....	50
5.6.5	Standard Object Audit Status .....	50
5.7	Database Standard Audits Interaction.....	51
5.7.1	Database Statement [Privilege] Audits .....	51
5.7.2	Database Object Audits.....	52
5.7.3	Standard Audit Unified Trail Mapping .....	53
6	CHAPTER 6: Real-Time Protection DDL .....	54
6.1	How it works.....	54
6.2	Real-Time Protection DDL Guidelines.....	54

6.2.1	General Guidelines .....	54
6.2.2	Silent Deny RTP DDL Policies .....	55
6.3	Real-Time Protection DDL Policies .....	56
6.3.1	Real-Time Protection DDL Policy Secured Area.....	57
6.3.2	Adding a new Real-Time Protection DDL Policy .....	57
6.3.3	Opening/modifying a Real-Time Protection DDL Policy .....	58
6.3.4	Deleting a Real-Time Protection DDL Policy .....	59
6.3.5	Copying a Real-Time Protection DDL Policy.....	59
6.3.6	Real-Time Protection DDL Policy Status .....	59
6.4	Real-Time Protection DDL Rules.....	60
6.4.1	Adding a new Real-Time Protection DDL Rule .....	60
6.4.2	Opening/modifying a Real-Time Protection DDL Rule.....	60
6.4.3	Deleting a Real-Time Protection DDL Rule.....	61
6.4.4	Real-Time Protection DDL Rule Status .....	61
6.5	Real-Time Protection DDL Conditions.....	62
6.5.1	Adding a new Real-Time Protection DDL Condition.....	62
6.5.2	Opening/modifying a Real-Time Protection DDL Condition.....	63
6.5.3	Deleting a Real-Time Protection DDL Condition.....	63
6.5.4	Real-Time Protection DDL Condition Status.....	63
7	CHAPTER 7: Real-Time Protection DML.....	64
7.1	How it works.....	64
7.2	Real-Time Protection DML Guidelines.....	64
7.2.1	General Guidelines .....	64
7.2.2	Silent Deny RTP DML Rules .....	65
7.3	Existing Oracle Fine-Grained Audit policies.....	65
7.4	Real-Time Protection DML Policies.....	66
7.4.1	Adding a new Real-Time Protection DML Policy.....	66
7.4.2	Opening/modifying a Real-Time Protection DML Policy .....	67
7.4.3	Deleting a Real-Time Protection DML Policy .....	67
7.4.4	Copying a Real-Time Protection DML Policy .....	68
7.4.5	Real-Time Protection DML Policy Status.....	68
7.5	Real-Time Protection DML Rules .....	69
7.5.1	Adding a new Real-Time Protection DML Rule .....	70
7.5.2	Opening/modifying a Real-Time Protection DML Rule .....	70
7.5.3	Deleting a Real-Time Protection DML Rule .....	71
7.5.4	Real-Time Protection DML Rule Status .....	71
7.6	Real-Time-Protection DML Conditions .....	72
7.6.1	Adding a new Real-Time Protection DML Condition .....	72
7.6.2	Opening/modifying a Real-Time Protection DML Condition .....	73
7.6.3	Deleting a Real-Time Protection DML Condition .....	73
7.6.4	Real-Time Protection DML Condition Status .....	73
7.7	Database Fine-Grained Audits Interaction .....	74
7.7.1	Database Fine-Grained Audit Policies.....	74
7.7.2	Real-Time Protection DML Unified Trail Mapping.....	75
8	CHAPTER 8: Security Management .....	76
8.1	Security Management Operation and Features.....	76
8.2	Database Users .....	76

8.2.1	Adding a new Database User .....	77
8.2.2	Opening/modifying a Database User .....	77
8.2.3	Dropping a Database User .....	77
8.2.4	Database User's Privileges .....	78
8.2.5	Database User's Tablespace Quotas .....	78
8.3	Database Roles.....	80
8.3.1	Adding a new Database Role .....	80
8.3.2	Opening/modifying a Database Role.....	81
8.3.3	Dropping a Database Role .....	81
8.3.4	Database Role's Privileges .....	81
8.4	System Privileges .....	82
8.4.1	Granting a system privilege .....	82
8.4.2	Revoking a system privilege .....	83
8.5	Object Privileges.....	84
8.5.1	Granting an object privilege .....	84
8.5.2	Revoking an object privilege .....	85
8.6	Role Privileges .....	86
8.6.1	Granting a role privilege.....	86
8.6.2	Revoking a role privilege.....	87
8.6.3	Default role privilege management .....	87
8.7	Profiles .....	88
8.7.1	Database Profiles.....	88
8.7.2	Profile Limits.....	88
9	CHAPTER 9: Reporting.....	90
9.1	Loading a Report.....	92
9.2	Running a Report.....	96
9.2.1	Exporting Report data .....	96
9.3	Modifying an existing Report.....	97
9.4	Cloning an existing Report .....	99
9.5	Creating an new Report.....	100
9.6	Report Performance Guidelines .....	103
10	CHAPTER 10: System Administration .....	104
10.1	System Components .....	104
10.1.1	Access Control.....	105
10.1.2	Standard Audit .....	105
10.1.3	Real Time Protection DDL .....	106
10.1.4	Real Time Protection DML.....	106
10.1.5	DB Audit Trails Purge.....	107
10.2	Omega Core Audit Accounts and Roles .....	109
10.2.1	Omega Core Audit Accounts.....	109
10.2.2	Omega Core Audit Roles.....	109
10.3	System Factors .....	111
10.3.1	Factor Identities.....	111
10.4	Database Jobs.....	113
10.4.1	Database Scheduler Jobs .....	113
10.4.2	Database Classic Jobs .....	115
11	Appendixes .....	116

11.1	Appendix A – Technical Support.....	116
11.2	Appendix B – Abbreviations.....	117

## **1 CHAPTER 1: Omega Core Audit Overview**

### **1.1 Introducing Omega Core Audit**

Omega Core Audit provides an out-of-box, software-only security and compliance solution that helps customers approach the complex and difficult security challenges in the Oracle database systems today; protecting against outsider and/or insider threats, unauthorized access and informational breaches or manipulation; this by enforcing strong security controls and duty separation, in meeting regulatory compliance requirements, those being external or internal.

Omega Core Audit implements strong practices of Access Control, Audit Monitoring and Real-Time Protection, providing clear visibility and control into database activity, even for privileged accounts and more, the DBAs, thus leading to a safer and more secure information system.

Omega Core Audit is a full back-end solution that is installed in minutes and easily managed by its applicative interface. It enhances the Oracle native security features with state-of-art and value-added programming and automation. It brings easiness to its users letting them focus only on the conceptual security tasks, without concentrating on complex technical security configurations, made easy and plainly presented to them via its rich user interface.

Security applied at the core - from within the database - ensures same rigid level of compliance from all possible connection directions, applications, users or devices and offers maximum accuracy and immediate auditing and protection action before user's actions or transactions. It also requires no (or very minimal, industry recommended) changes in existing security configurations.

### **1.2 Key Benefits**

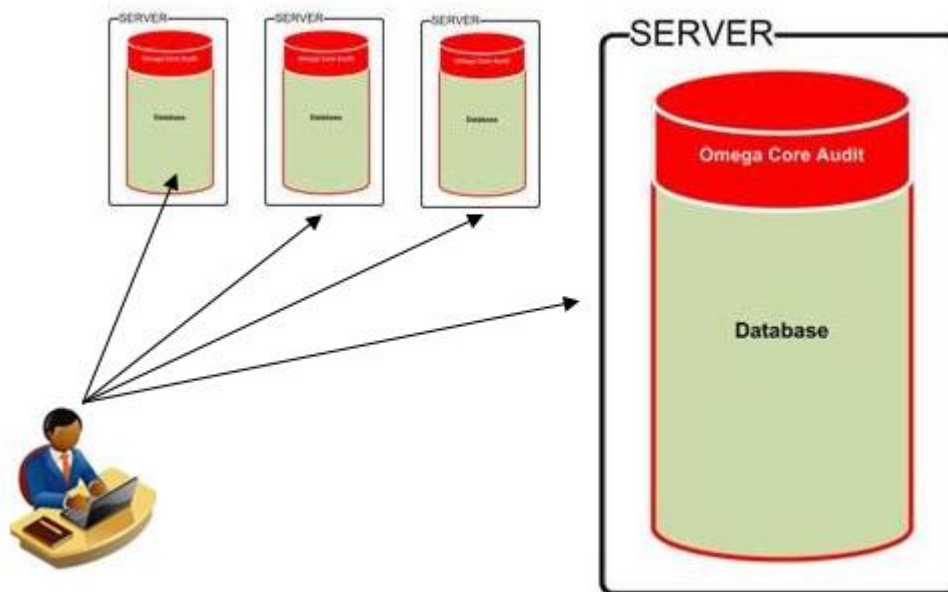
- Real-Time Access Control, mandatory authorization of the database logon process.
- Continuous Audit Monitoring, highly detailed, up to the full SQL text and SQL bind parameters.
- Real-Time Protection for structural (DDL commands) and data (DML commands) changes.
- Enforcement on privileged accounts and DBAs.
- Unified Audit Trail.
- Duty Separation and out-of-box Roles for system's main components.
- Secured Protected Areas.
- Change Control, full object source history before and after audited/protected event.
- Policy-based evaluation.
- Multi-factorial User & environment context authorization in real time.
- Row and column authorization.
- Middle-tier Application Level Auditing and Protection by CLIENT\_IDENTIFIER.
- Mapping of standard audit trails with audit settings (statement/privilege and object).
- Automatic management of audit trail records.
- Issue tracking module to mark and classify audit trails.
- Security Management, made easy for batch operations handling multiple commands.
- Full back-end solution - ensuring protection from all directions.

- Out-of-box, Software-only solution.
- Transparent implementation - no (or tiny, industry recommended) change of existing setup.
- Detailed reporting - dynamic reporting for all modules.

### 1.3 Omega Core Audit Architecture

The Omega Core Audit solution has three main components:

- **Omega Core Audit Engine:** An Oracle PL/SQL software package containing core audit and protection logic, Back-End installed into the target database under the SYS schema and running with its privileges.
- **Omega Core Audit Repository:** An Oracle Schema Repository containing all system data, Back-End installed into the target database.
- **Omega Core Audit Application:** A Windows-based client desktop Application, connecting to the target database and interacting with the Engine and Repository.



#### 1.3.1 Omega Core Audit Engine

The Omega Core Auditing Engine is an Oracle PL/SQL software package installed under the SYS schema. The Engine contains the core logic of the access control, auditing and protection.

The Core Audit Engine Objects are:

OMEGA_CORE_AUDIT	Oracle Database PL/SQL Package containing core logic
OMEGACA_ACC_DB_AF_LOGON	Oracle Database Trigger on After Logon event
OMEGACA_RTP_DB_BF_DDL	Oracle Database Trigger on Before DDL event
OMEGACA_TRANS	Oracle Database scheduler job for audit trails purge



### 1.3.2 Omega Core Audit Repository

The Omega Core Auditing Repository is an Oracle Schema named OMEGACA, containing all objects for audit trail data and all configuration options needed by the Engine. It is installed from the installation script.

The Core Audit Repository Objects are:

OMEGACA_TS	An Oracle tablespace storage object. See the Omega Core Audit Deployment Guide and Install script for more details.
OMEGACA	An Oracle database schema, containing repository data and configurations.

### 1.3.3 Omega Core Audit Application

The Omega Core Audit Application is a typical Windows-based and database-enabled client desktop application that connects to each target database. It is used to configure the system for all its operations and also monitor the audited activity generated by the prior.

## 1.4 Compatibility and Requirements

The Omega Core Audit solution is compatible with and has the following technical requirements.

### 1.4.1 Supported Oracle Database Versions and Releases

Omega Core Audit Engine and Repository support the following Oracle Database Versions and Releases:

- Oracle Database 10g Release 2.
- Oracle Database 11g Release 1.
- Oracle Database 11g Release 2.
- Oracle Database 12c Release 1 (Traditional Auditing only).

### 1.4.2 Supported Oracle Database Editions

Omega Core Audit Engine and Repository supports the following Oracle Database Editions:

- Oracle Database EE - Enterprise Edition.
- Oracle Database SE - Standard Edition.
- Oracle Database SE1 - Standard Edition One.

#### Omega Core Audit features availability by Oracle Database Editions:

Omega CA Features	Oracle Database Edition
Access Control	EE, SE, SE1
Standard Audit	EE, SE, SE1
Real-Time Protection DDL	EE, SE, SE1
Real-Time Protection DML	EE, ---, ----
Security Management	EE, SE, SE1

### 1.4.3 Oracle Core Audit Application requirements

Omega Core Audit Application supports all the Oracle Database Versions and releases as those supported by the Engine and Repository.

The OS, hardware and software requirements of Omega Core Audit Application are:

- All x86/x64 versions of Windows from XP and above supported by the Oracle 32bit database clients.
- All Oracle Database Clients from 10g R2 to 11gR2.
- Only 32 bits clients Oracle Clients are supported, even on 64bit Windows systems.

## 1.5 Limitations

Omega Core Audit has currently the following limitations:

1. Only databases opened in Read-Write mode are supported.
2. Unicode character sets are currently not supported. Current language characters support is for Western European Character sets only, however, even in databases with National Character Set of Unicode functionality is achieved almost intact, given that Database infrastructure names of users, objects, columns, ..., etc, (and database language) are set to Western European Languages.

You must test in your own system to be sure on the compatibility!

3. Connectivity from Omega Core Audit Application is currently supported only on 32 Bit Oracle Clients.
4. The Real-Time Protection DML module is functional only on Enterprise Editions - this is a vendor limitation.

Check our website for news on current developments.

### **Note:**

Omega Core Audit operation is unavoidably dependent on Oracle database limitations and bugs/issues, although in the later extensive effort is done in programming to proper handle and circumvent. You should be aware of such limitations especially on topics such Database Triggers, Standard Audit and Fine-Grained Audit.

## 2 CHAPTER 2: System Wide Functionalities, Utilities and Guidelines

### 2.1 Common Application functionalities

#### 2.1.1 The target database

##### Connecting to the target database

When you first open the Omega Core Audit Application, the form System Authentication will immediately modally display. In this form you connect to your target database with your Omega Core Audit account.



Enter the username, password and Database. Press the Logon button to connect to the target database. The Database combo box loads the target database connection parameters configured in the initialization file OmegaCA.ini (See the Omega Core Audit Deployment Guide, topic Omega Core Audit Application Install for more details on connectivity).

The System Authentication form is always invoked when the application's main form is activated and there is no target database connection opened. However to manually display the System Authentication form, in the Application's main menu, tab Omega CA, System Access group click the menu button Logon (green key) which is enabled when application is not connected and disabled otherwise.



##### Disconnecting from the target database

To disconnect from the target database on which you are connected, in the Application's main menu, tab Omega CA, System Access group click the menu button Logout (red lock icon) which is enabled when application is connected and disabled otherwise.



### 2.1.2 Client-side information retrieval

Information presented in the Omega Core Audit Application is processed via a classic two-tier architecture, where the Application represents the Client tier and the Omega Core Audit Repository is the server tier. All data queried is returned to the client, limited only by network and local PC RAM amount!

Omega Core Audit Application is equipped with highly detailed searching functionalities in all important areas of the Omega Core Audit Repository. In all the main forms, searching is implemented into the Search Options panel which is present at the top of the search-enabled forms.

Complete the necessary search options and press the button (usually) named "Search", or blue arrow. The search query will be passed to the server, executed and results returned as a whole dataset to the client. Press the checkbox "Advanced", where applies, to view extra search options.

#### **Important Performance Note:**

Remember that Omega Core Audit is a typical Desktop application. The whole set of records queried on the server is returned as a record-set and there is no "Next 50 Records" concept. Large amounts of records are limited only by your server and network capacity and local workstation RAM. Thus try to avoid:

1. Queries resulting in full table scans on the Unified Audit Trail - remember that you are querying the "live production" machine!
2. Queries resulting in large table scans on the Unified Audit Trail - same reason as above!
3. Large amount of data returned to your desktop - limited by your RAM and network.

### 2.1.3 Information presentation

In the Omega Core Audit Application the information is mostly presented in two main general forms. For the classic table-viewing of the records, grid components are used. These grids offer a highly flexible graphical interface for data viewing, grouping, filtering and interaction. For showing individual records, usually standard windows components (like edits, combos, checkboxes ..., etc) are used.

The Application is equipped with all necessary client-side functionalities like:

#### **Multiple views**

Multiple datasets implemented either in tab or data grid level.

#### **Filtering**

Filter the data by creating filter conditions. Click on the column's down-arrow button to invoke the dropdown list containing unique values from the current column. Click on the values you want, or click on the (Custom...) option to invoke the Custom Filter dialog. Filter conditions and Filter Customize button will appear down the grid.

#### **Sorting**

Click on the column headers to switch between ascending/descending sorting methods. Click on the column header holding **Ctrl** to clear sorting. For multiple-column sorting, click on column headers holding **Shift**.

#### **Grouping**

Drag the column header to the special Grid Group Box area (whenever you see the text "Drag a column header here to group by that column" above the grid) to group the records tree-like. Multiple levels of grouping are supported.

**Column moving and view/hide**

Column moving for viewing and hiding is available. Right-click on the column and in the grid's popup menu that opens, see option "Remove This Column" and "Field Chooser".

**Master detail relationships**

Master detail relationship implemented at, grid, tab and form level.

**2.1.4 Data Exporting in standard file formats**

Omega Core Audit Application offer exporting of data grids into Excel, Text, Html and Xml format files. This functionality is implemented via the "Export..." button placed on the right of the grids. Clicking on the button invokes a File Export menu with the above four file formats options in respective icons.

**2.1.5 DateTime Field Format**

The Omega Core Audit application always uses the DD-MM-YYYY and optionally HH24:MI:SS Oracle DateTime format models for DateTime fields, both in display and input.

Examples:

December 31 of 2015 would be 31-12-2015

December 1 of 2015 would be 01-12-2015

All the DateTime Pick/Edit components are set this way. You should stick to the above format for Date Inputs with non-Calendar components, such as Values for Date Factors in Policy Conditions!

## 2.2 Secured Areas

The "Secured Areas" feature of Omega Core Audit implements groups and/or combinations of objects and statements to be audited and optionally protected. Secured Areas are implemented directly or as a group of Secured Sub-Areas.

The implementation has specific differences according to modules as below:

### Access Control

The Secured Area is not visually implemented, as it is represented by the database as a whole itself.

### Standard Audit

The Secured Area is implemented as a group of Secured Sub-Areas. Sub-Areas are defined as on each Standard Audit Rule and can be individual user statements or database object to be audited, depending on the policy type. Remind that:

- There is no Protection feature in Standard Audit.
- The "Secured sub-Area" is not visually presented in the Omega Core Audit Application!

### Real-Time Protection DDL

The Secured Area is implemented directly as a combination of at least one (or more) of Object Owner Name, Object Type, Object Name and DDL Action (Event), thus combining statements and object features. The Secured Area is defined and visually presented on the RTP DDL Policy level.

### Real-Time Protection DML

The Secured Area is implemented as a group of Secured Sub-Areas. Sub-Areas are defined on each RTP DML Rule and can be individual tables and views, monitored for DMLS only. The Secured Sub-Areas are visually presented each at RTP DML Rule.

## 2.3 Policy-Based Evaluation Model

Omega Core Audit implements a policy-based auditing and protection as a flexible mechanism for authorizing access to database, application structure and data. It combines a policy-based evaluation model with a user & environment context multi-factorial authorization on real-time. This evaluation model is applied in Access Control, Audit and Real-Time Protection modules. It is also partially used in the Standard Audit module. The implementation has differences specific to modules.

### 2.3.1 Policies

Policies represent the security controls enforced for access control, auditing and real-time protection. Their evaluation results in a True/False result that indicates policy's compliance. They are compounded by rules, and their compliance result is calculated as a function of rules evaluation and based on policy's own options.

### 2.3.2 Rules

Rules are the building blocks of the policies. Their evaluation results in a True/False result that indicates rule's compliance. They are compounded by conditions, and their compliance result is calculated as a function of conditions evaluation and based on rule's own options.

### 2.3.3 Conditions

Conditions are the building blocks of the rules. Their evaluation results in a True/False result that indicates condition's compliance. Their compliance result is defined by its factor evaluation.

Conditions are evaluated based on:

- Factor validation by operation codes like =, >, >= <>, [NOT] LIKE, [NOT] BETWEEN, [NOT] IN, ..., etc, versus operands values, i.e. user & environment real-time values like host, terminal, IP address, program used, machine, user, time and many more. Wildcard characters (like % and more) are supported for (NOT) LIKE operands; in general full Oracle syntax is supported.
- Factor validation by Minimum Trust Level - required match with different predefined factor identities assigned with trust levels.
- Validate expression - where a user-defined function returning Boolean can be used at will.

### 2.3.4 Factors

Factors represent environment and user context information, whose real-time extracted values are recognized and used of in the evaluation of conditions.

For a Condition Evaluation of type Operand, the factor's value will be matched with the condition's Operation Code and Operand(s) value(s). For a Condition Evaluation of type Trust Level, the factor's value will be used to determine the assigned Trust Level from factor's identities, and check if it matches with the minimum trust level required. For a Condition Evaluation of type Validate Expression, the factor's code and value can be provided to an user-defined function having two input Character parameters (for code and value) and returning a Boolean result that will set the Condition's evaluation result.

### 2.3.5 Policy Cache

The Policy Cache mechanism implements a policy evaluation memory model that significantly enhances audit operation performance. It bypasses full re-evaluation of the policy on repeated input values. It is reset by changes performed in the whole policy structure, including rules, conditions and [NOT] IN lists.

**Note:**

Usage of Policy Cache is recommended in All Modules for performance optimization! All policies in all modules must be cache-enabled!



## 2.4 Debug and Diagnostics

Omega Core Audit comes with a set of functionalities for debugging and diagnostics.

### 2.4.1 Client-Side User Debug

Client-Side user debug enables displaying of debug messages during the application run. Activating Debug will produce messages on the content of important client-side SQLs queries or executions and also important code points. It is helpful for performing debug and diagnosis of application's possible issues or behavior understanding.

To enable the functionality in the application's main menu, tab Tools, group Tools click on the menu button Debug. To disable click again on the menu button Debug. You will receive a message in both cases.



Client-side Debug by default is Inactive on application startup and when set to active will not persist in the next application run.

### 2.4.2 Server-Side Policy Debug

You can set the Debug option for each module's policy, to produce special debug information outputted to a common policy debug table for all modules. Activating Policy Debug will produce debug information for each policy, rule and condition evaluation/processing. It is helpful for performing debug and diagnosis of application's possible issues or behavior understanding.

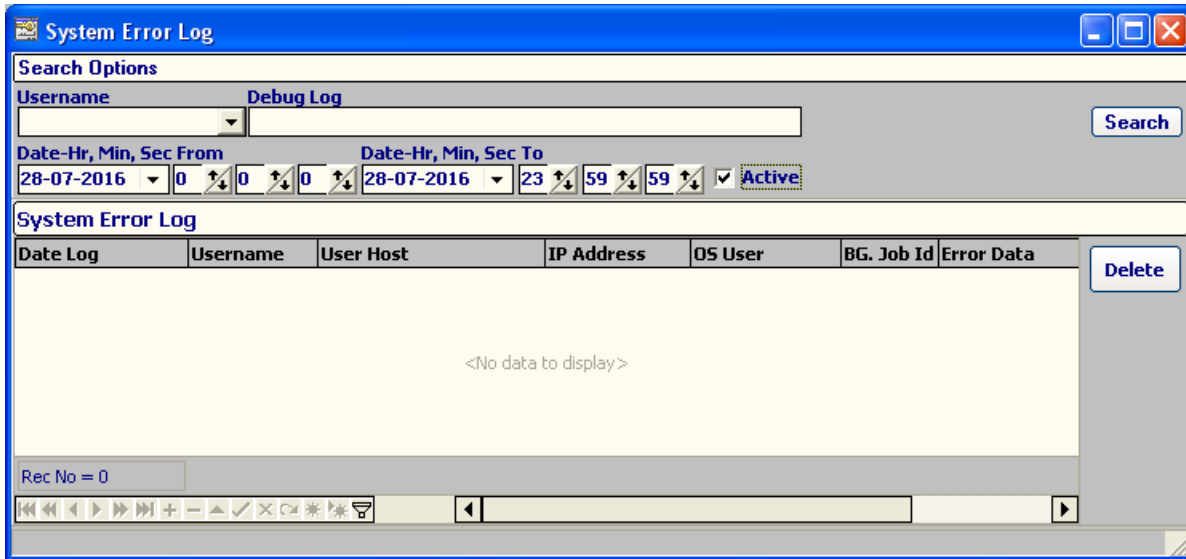
#### Important Note:

Policy Debug is set at the server level and will persist for all policy executions until set off. Use the Policy Debug option only casually and not permanently, as it will make the debug table grow big and possibly add unnecessary burden to the system's performance!

In the RTP DML module, Policy Debug is available only for rule's Authorization Type of Rule Conditions!

### 2.4.3 System Error Log

Omega Core Audit's potential execution errors are stored in a central system error log. To view these potential errors, in the Administration main menu tab, System Components group click on the System Error Log button. The form System Error Log will open.



You can search by user, error log content and date-time log interval.

There categories of errors thrown to the system error log are:

1. ORA-XXXXX - potential errors during operations for whatever reason. These errors will not interfere with user actions, failing execution/iteration will be skipped and user action will continue.
2. ORA-20020 - Severe errors in Omega CA functionality performing, or Omega CA errors indicating miss-configurations in policy setup, for example "inactive rule included in policy formula", or "no Active Condition[s] found" when policy evaluation. These errors will stop the user action and raise an error.
3. Internal Omega Core Audit Warnings, for example in the DB Audit Trails Purge Job, unknown values in columns action# and priv\$used of the SYS.AUD\$ table. This might be the case for new codes provided by Oracle, thus an upgrade required on Omega Core Audit, if not in the last version. Respective description fields will take the value of <UNDECLARED> in the Repository's Unified Audit Trail.

**Important Note:**

Although you are supposed not to see at all errors of the categories above, however, because of the importance of the subject, it is advised to view daily the System Error Log and also any time you might have a doubt for any policy, rule, condition evaluation result.

## 2.5 System Backup

It is important that you frequently backup the Omega Core Audit environment, just like any other database driven software.

Backup of Omega Core Audit mostly consists in the backup of its back-end, database-installed parts Engine and Repository.

Evidently, whenever you perform a full Oracle Database backup, with RMAN or not, "hot" or "cold", you automatically have a backup of the Engine and Repository - as they are installed in the database being backed up.

To make a specific backup of the Engine and Repository, see below:

### 2.5.1 Engine Backup

To backup the Engine, simply save in a text file the source code of the OMEGACA\_% like objects in the SYS Schema, as they are described in the Omega Core Audit Deployment guide, namely:

- Package OMEGA\_CORE\_AUDIT head and body
- Database-level triggers OMEGACA\_ACC\_DB\_AF\_LOGON and OMEGACA\_RTP\_DB\_BF\_DDL
- Scheduler Job OMEGACA\_TRANS

You can use any integrated development environment tool for Oracle object management, to locate the objects and copy/paste the code into your backup text file.

Alternatively, get the source code of the Package and database-level triggers as a CLOB column by running the following SQL command:

```
-----
select 'OMEGA_CA_PACKAGE_SPEC' as Object_Name,
dbms_metadata.get_ddl('PACKAGE_SPEC', 'OMEGA_CORE_AUDIT', 'SYS') as Object_DDL from dual

UNION ALL

select 'OMEGA_CA_PACKAGE_BODY' as Object_Name,
dbms_metadata.get_ddl('PACKAGE_BODY', 'OMEGA_CORE_AUDIT', 'SYS') as Object_DDL from dual

UNION ALL

select 'OMEGACA_ACC_DB_AF_LOGON' as Object_Name,
dbms_metadata.get_ddl('TRIGGER', 'OMEGACA_ACC_DB_AF_LOGON', 'SYS') as Object_DDL from dual

UNION ALL

select 'OMEGACA_RTP_DB_BF_DDL' as Object_Name,
dbms_metadata.get_ddl('TRIGGER', 'OMEGACA_RTP_DB_BF_DDL', 'SYS') as Object_DDL from dual
-----
```

The create command of the Scheduler Job OMEGACA\_TRANS is found on the Install script, see the Omega Core Audit Deployment guide.

### 2.5.2 Repository Backup

To backup the Repository, as for every other Oracle Schema, use the database tools RMAN, DataPump or Classic Export.

## 2.6 Issue Tracking Module

Omega Core Audit offers an Issue Tracking Module, which implements managerial classification of Unified Audit Trail records according to a user-defined triple-level model of Issues, Groups and Classes. Each Issue has a Group parent and each Group has a Class parent.

See the Issue Tracking tab in the main application's menu. There you can open the respective forms for viewing, adding, updating and deleting Issues, Groups and Classes.



Each unified trail record is bound to an Issue ID. Its usage there is non-mandatory, by default in record creation the Issue is set to UNMARKED.

### 3 CHAPTER 3: Unified Audit Trails

Omega Core Audit Repository features a unified audit trail that captures audit trails records from the following source modules:

- Access Control
- Standard Audit
- Real-Time Protection DDL
- Real-Time Protection DML

The unification of audit trails from different sources into a single trail offers benefits in visualization, management and provides a better look into the monitored database activity.

#### 3.1 Unified Audit Trail repository fields

The following are the fields of the Unified Audit Trail in the Omega Core Audit Repository:

Field Name	Module	Field Description
Audit DateTime	x-x-x-x	Date and time of the audit event. Sole field indexed.
Audit UTC	x-x-x-x	Universal Time Coordinated of the audited event.
Pol. Type	x-x-x-x	Policy type (originating module) of the trail record.
Policy Type Name	x-x-x-x	Policy name (originating module) of the trail record.
Username	x-x-x-x	Database user name performing the audited event.
Session Id	x-x-x-x	Oracle Session Id, unique number assigned to each user's session.
OS User	x-x-x-x	Operating system user name of the client process.
Userhost	x-x-x-x	Name of the host machine of the client.
Action Id	0-x-0-x	Unique numeric code of the user's action audited.
Action Name	x-x-x-x	Name of the user's action audited.
Owner	0-x-x-x	Owner of the object affected by the audited event.
Object Name	0-x-x-x	Name of the object audited event.
Object Type	0-x-x-x	Type of the object audited event.
Rtn. Code	x-x-x-x	Omega Core Audit/Oracle returned code generated by the audited event. 0 for success, -20010 for Omega Core Audit protection errors, other values for Standard Audit trails only.
Return Message	x-x-x-x	Omega Core Audit/Oracle returned message generated by the audited event.
SQL Bind	0-x-0-x	SQL Bind variable data of the audited event.
SQL Text	0-x-0-x	SQL full text of the audited event..
DDL Body	0-0-x-0	Original DDL text of the object before the DDL command.
Priv. Id	0-x-0-0	System privilege unique number used by the user to perform the audited event.
System Privilege	0-x-0-0	System privilege name used by the user to perform the audited event.
Obj. Privilege *	0-x-0-0	Object privileges granted/revoked for Grant and Revoke statements.
Sys. Privilege	0-x-0-0	System privileges granted/revoked for Grant and Revoke statements.
Adm. Option	0-x-0-0	Role/privilege granted with "admin" option
Grantee	0-x-0-0	Name of the grantee for Grant and Revoke statements.
Audit Option	0-x-0-0	Auditing Options for Audit and NoAudit statements.
Logoff Time	0-x-0-0	Logoff Date Time.
Logoff LRead	0-x-0-0	Number of logical reads for the session.
Logoff PRead	0-x-0-0	Number of physical reads for the session.
Logoff LWrite	0-x-0-0	Number of logical writes for the session.

Logoff DLock	0-x-0-0	Number of deadlocks detected during session.
Statement Id	0-x-0-x	User's statement's Id performed during the user's session.
Entry Id	0-x-0-x	User's audit entry Id audited in during the user's session.
Transaction Id	0-x-0-x	Transaction Identifier.
SCN	0-x-0-x	System change number (SCN).
Proxy Session Id	0-x-0-x	Serial number of the proxy session (if enterprise user proxy logon)
New Owner	0-x-0-0	Object's new owner when changed.
New Name	0-x-0-0	Object's new name when renamed.
Global User Id	0-x-0-x	Global user identifier (if logged on as enterprise user)
Comment	0-x-0-x	Text comment of the audited event.
OS Process	0-x-0-x	Oracle OS process identifier.
Session CPU	0-x-0-0	Amount of CPU Time used by session.
FGA Policy Name	0-0-0-x	Name of the Oracle FGA policy
IP Address	x-0-x-0	IP Address of the client's machine.
Terminal	x-x-x-0	Terminal name of the client's machine.
Client Id	0-x-x-x	Client identifier in each database session.
Net. Protocol	x-0-x-0	Network protocol used for connection.
Db Id	x-x-x-x	Database Identification number
DB. Name	x-x-x-x	Database name
Instance No.	x-x-x-x	Instance number
Auth. Method	x-0-x-0	User's authentication method.
Identification Type	x-0-x-0	User's identification mode.
IsDBA	x-0-x-0	User is SYSDBA or not.
Module	x-0-x-0	Program name used by the user.
Bg. Job Id	x-0-x-0	Background Job Id.
Fg. Job Id	x-0-x-0	Foreground Job Id.
Trail Evaluation	x-x-x-x	Policies related to this trail record.
Issue Class **	x-x-x-x	Issue Tracking module's issue class.
Issue Group **	x-x-x-x	Issue Tracking module's issue group.
Issue Name	x-x-x-x	Issue Tracking module's issue name.

**Legend:**

\* Object Privileges codification is on the same line as privilege columns ALT, AUD ..., WRI, FBK in the Oracle system view DBA\_OBJ\_AUDIT\_OPTS.

G Grant  
N Revoke  
- Non-applying

\*\* Non-Repository field, linked in Unified Audit Trail form, tab Record Details only.

**Module Legend:**

x/0 Field in/not in use by Module

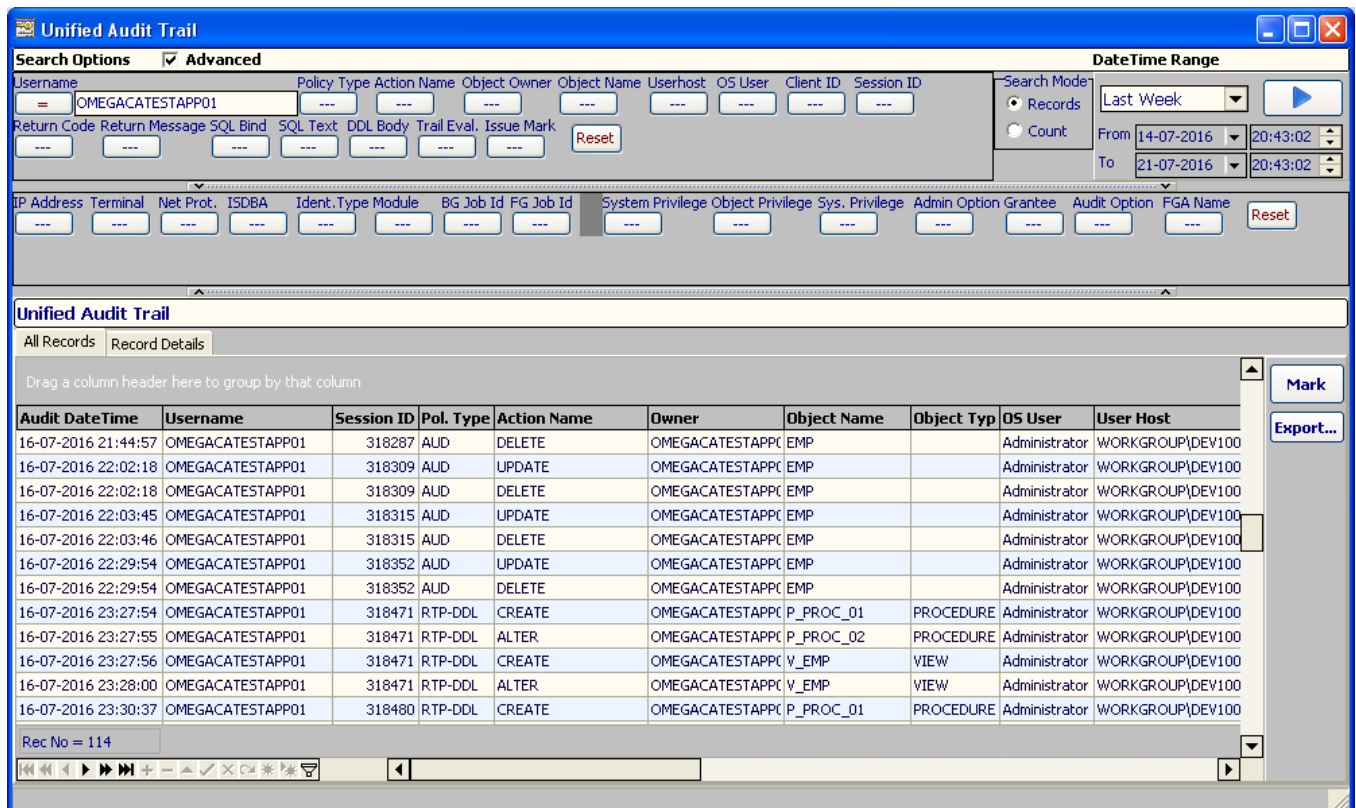
1st Slot Access Control Module  
2nd Slot Standard Audit Module  
3d Slot Real-Time Protection DDL Module  
4th Slot Real-Time Protection DML Module

### 3.2 The Unified Audit Trail form

Omega Core Audit implements automatic audit trail management that relieves the administrator from the tasks of administering the audit trail records.

The Unified Audit Trail form it is one of the most important of the Omega Core Audit Application and is used to view the audited database activity. The form features a very flexible search on the unified trail records with custom conditions on more than 30 search-enabled fields of top importance. Detailed record browsing and data export in different OS file formats are other features described below.

To open this form in the Main Menu, Tab Audit Trails, group Unified Audit Trails click the button Unified Audit Trails. This will open the form Unified Audit Trail.



**Unified Audit Trail**

**Search Options** ☒ **Advanced**

Username: OMEGACATESTAPP01 Policy Type: --- Action Name: --- Object Owner: --- Object Name: --- Userhost: --- OS User: --- Client ID: --- Session ID: ---

Return Code: --- Return Message: --- SQL Bind: --- SQL Text: --- DDL Body: --- Trail Eval: --- Issue Mark: --- **Reset**

**Date Time Range**

Search Mode: ☒ Records ☐ Count Last Week **▶**

From: 14-07-2016 20:43:02 To: 21-07-2016 20:43:02

IP Address: --- Terminal: --- Net Prot: --- ISDBA: --- Ident.Type: --- Module: --- BG Job Id: --- FG Job Id: --- System Privilege: --- Object Privilege: --- Sys. Privilege: --- Admin Option: --- Grantee: --- Audit Option: --- FGA Name: --- **Reset**

**Unified Audit Trail**

All Records | Record Details

Drag a column header here to group by that column

Audit DateTime	Username	Session ID	Pol. Type	Action Name	Owner	Object Name	Object Type	OS User	User Host
16-07-2016 21:44:57	OMEGACATESTAPP01	318287	AUD	DELETE	OMEGACATESTAPP01	EMP		Administrator	WORKGROUP\DEV100
16-07-2016 22:02:18	OMEGACATESTAPP01	318309	AUD	UPDATE	OMEGACATESTAPP01	EMP		Administrator	WORKGROUP\DEV100
16-07-2016 22:02:18	OMEGACATESTAPP01	318309	AUD	DELETE	OMEGACATESTAPP01	EMP		Administrator	WORKGROUP\DEV100
16-07-2016 22:03:45	OMEGACATESTAPP01	318315	AUD	UPDATE	OMEGACATESTAPP01	EMP		Administrator	WORKGROUP\DEV100
16-07-2016 22:03:46	OMEGACATESTAPP01	318315	AUD	DELETE	OMEGACATESTAPP01	EMP		Administrator	WORKGROUP\DEV100
16-07-2016 22:29:54	OMEGACATESTAPP01	318352	AUD	UPDATE	OMEGACATESTAPP01	EMP		Administrator	WORKGROUP\DEV100
16-07-2016 22:29:54	OMEGACATESTAPP01	318352	AUD	DELETE	OMEGACATESTAPP01	EMP		Administrator	WORKGROUP\DEV100
16-07-2016 23:27:54	OMEGACATESTAPP01	318471	RTP-DDL	CREATE	OMEGACATESTAPP01	P_PROC_01	PROCEDURE	Administrator	WORKGROUP\DEV100
16-07-2016 23:27:55	OMEGACATESTAPP01	318471	RTP-DDL	ALTER	OMEGACATESTAPP01	P_PROC_02	PROCEDURE	Administrator	WORKGROUP\DEV100
16-07-2016 23:27:56	OMEGACATESTAPP01	318471	RTP-DDL	CREATE	OMEGACATESTAPP01	V_EMP	VIEW	Administrator	WORKGROUP\DEV100
16-07-2016 23:28:00	OMEGACATESTAPP01	318471	RTP-DDL	ALTER	OMEGACATESTAPP01	V_EMP	VIEW	Administrator	WORKGROUP\DEV100
16-07-2016 23:30:37	OMEGACATESTAPP01	318480	RTP-DDL	CREATE	OMEGACATESTAPP01	P_PROC_01	PROCEDURE	Administrator	WORKGROUP\DEV100

Rec No = 114

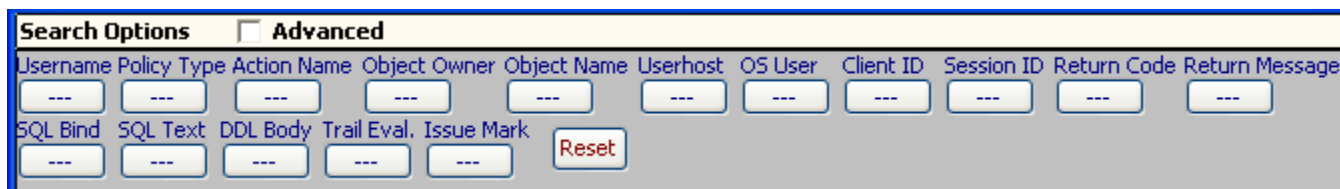
**Mark** **Export...**

Main data elements of the Unified Audit Trail form are described below.

#### Search Options Panel

The Search Options Panel is top-aligned in the form and contains the following search-related elements:

#### Simple Search Panel

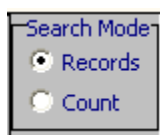


The Search Options panel is titled "Search Options" and includes a checkbox for "Advanced". It contains two rows of search criteria, each with a triple dash (---) button for selection. The first row includes: Username, Policy, Type, Action Name, Object Owner, Object Name, Userhost, OS User, Client ID, Session ID, Return Code, and Return Message. The second row includes: SQL Bind, SQL Text, DDL Body, Trail Eval, and Issue Mark. A "Reset" button is located at the bottom right of the panel.

This is the panel where search options for the most important fields of the unified audit trail are defined. The fields start with the Username and Policy Type and end with the Issue Mark. By default there is no search active. Use the last Reset button to clear all search conditions in this panel.

To set search conditions click on the triple dash (--) labeled buttons of every field. In the button's drop-down menu that opens, choose the fields' search conditions operator (=, <>... like... null) and set the Operand's value in the Edit box that will open appropriately according to the Operator chosen.

### Search Mode Radio Group



The Search Mode Radio Group contains two radio buttons: "Records" (selected) and "Count".

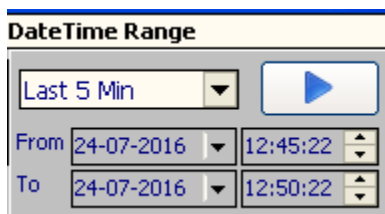
Here you define the mode in which search will be performed. Two options exist:

**Count** Only Count of records is returned. Very useful to first check the number of records and avoid large number of returned records. This is the default when form first opens. The Total number of trail records will be displayed in the special "Trail Count Mode" panel which will superpose the "Unified Audit Trail" panel:

- Navy Color for up to 50,000 records
- Orange Color for 50,000 – 100,000 records
- Red Color for 100,000 + records

**Records** All records are returned. This is the normal operation behavior.

### Date Time Range Panel



The Date Time Range panel is titled "Date Time Range". It features a dropdown menu for predefined intervals, currently showing "Last 5 Min", and a blue play button. Below are "From" and "To" fields, each with a date and time selector. The "From" field shows "24-07-2016" and "12:45:22", and the "To" field shows "24-07-2016" and "12:50:22".

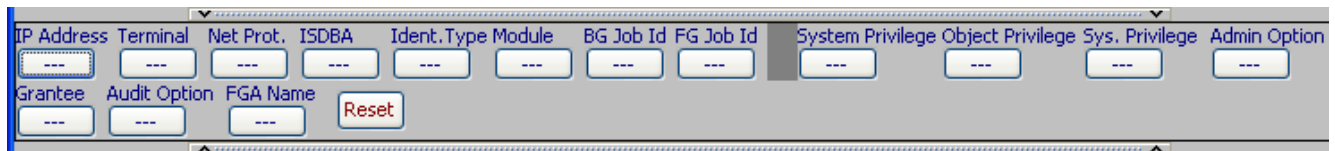
In this panel you define the obligatory DateTime range conditions when searching the unified audit trail.

Predefined DateTime Range intervals are selected in the combo box. Choosing any of the predefined intervals (other than Custom Range) will lock and empty the Date Time editors below. They will be auto-completed just after you click the Search (blue arrow) button; the date-time is referenced from the DB Server Date Time. If you choose the Custom Range interval, it will unlock and auto-complete the Date Time editors; the date-time is referenced from the local PC Date Time and the default set interval will be 1 Hour.

To search the unified audit trails, press the Search (blue arrow) button and wait until search completes.

### Advanced Search Panel





This panel allows defining search options for various fields in the unified audit trail. It includes input fields for IP Address, Terminal, Net Prot., ISDBA, Ident. Type, Module, BG Job Id, FG Job Id, System Privilege, Object Privilege, Sys. Privilege, and Admin Option. It also has fields for Grantee, Audit Option, and FGA Name, along with a Reset button.

This is the panel where search options for other fields of the unified audit trail are defined. It operates the same as the Simple Search panel. This panel is not visible by default, but is displayed by checking the checkbox Advanced on the main Search Panel. The fields start with the IP Address and Terminal and end with the FGA Name. By default there is no search active. Use the last Reset button to clear all search conditions in this panel.

## Unified Audit Trail Panel

The Unified Trail Panel is client-aligned in the form and shows the searched unified trail records into the following elements:

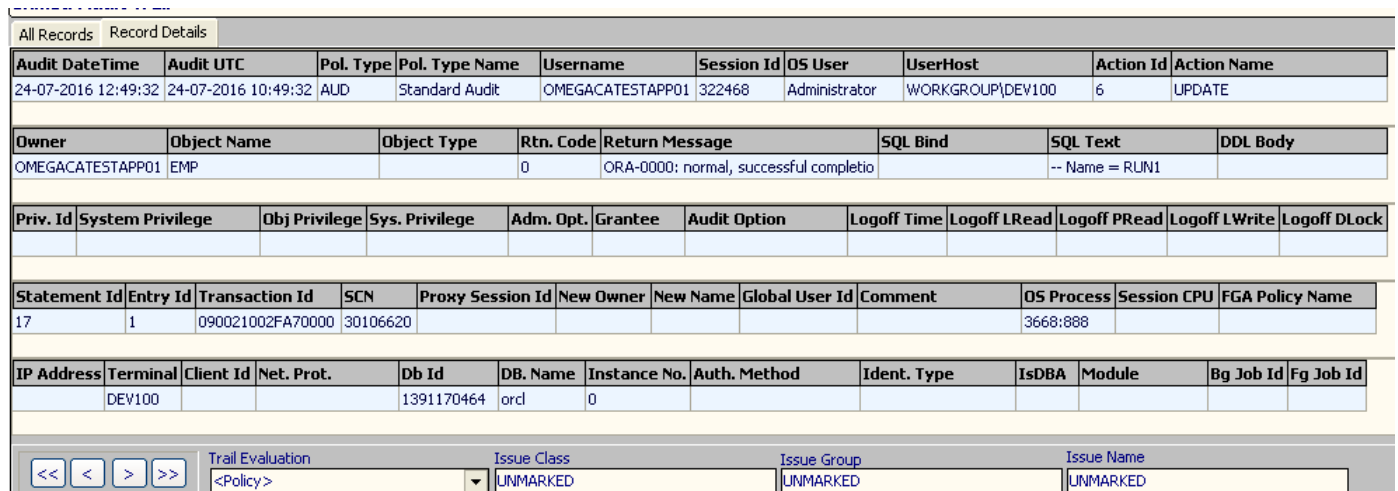
### All Records Tab

In this tab the searched unified audit trail records are displayed. This tab obviously the default opened.

On the right, click the Mark button to open the "Unified Audit Trail - Issue Mark" form for issue-marking of returned (or client-side filtered) records. Click the Export button and in the drop-down menu that opens, choose the export format file type to export the records in that format.

### Record Details Tab

In this tab you can see all fields of the individual record selected in the previous tab "All records".



The Record Details tab displays a detailed view of a selected audit record. It includes tabs for All Records and Record Details. The main content area shows several tables of data:

Audit DateTime	Audit UTC	Pol. Type	Pol. Type Name	Username	Session Id	OS User	UserHost	Action Id	Action Name
24-07-2016 12:49:32	24-07-2016 10:49:32	AUD	Standard Audit	OMEGACATESTAPP01	322468	Administrator	WORKGROUP\DEV100	6	UPDATE

Owner	Object Name	Object Type	Rtn. Code	Return Message	SQL Bind	SQL Text	DDL Body
OMEGACATESTAPP01	EMP		0	ORA-0000: normal, successful completio		-- Name = RUN1	

Priv. Id	System Privilege	Obj Privilege	Sys. Privilege	Adm. Opt.	Grantee	Audit Option	Logoff Time	Logoff LRead	Logoff PRead	Logoff LWrite	Logoff DLock

Statement Id	Entry Id	Transaction Id	SCN	Proxy Session Id	New Owner	New Name	Global User Id	Comment	OS Process	Session CPU	FGA Policy Name
17	1	090021002FA70000	30106620						3668:888		

IP Address	Terminal	Client Id	Net. Prot.	Db Id	DB. Name	Instance No.	Auth. Method	Ident. Type	ISDBA	Module	Bg Job Id	Fg Job Id
	DEV100			1391170464	ord	0						

At the bottom, there are navigation buttons (left, right, first, last) and fields for Trail Evaluation, Issue Class, Issue Group, and Issue Name.

Use the "arrow" buttons for client-side moving on search returned records on the All Records tab.

### Important Note

It is at this form that mostly the topic "Important Performance Note" of the paragraph "Client-Side information retrieval" mostly applies. Do not use large DateTime intervals for searching unified audit trails. Although the DateTime is a (the sole) indexed field on the Repository's table, extend your search with other field conditions for large DateTime intervals.

### 3.2.1 Unified Audit Trail - Issue Mark form

The "Unified Audit Trail - Issue Mark" form features Issue-Tracking marking of all or important unified audit trail records. It is available by clicking the Mark button on the right of the Unified Audit Trail form, tab All Records.



In this form you can mark the unified trail records using the form elements as below:

#### Marking Mode Options

The three options of Record Issue Marking Mode are:

1. All Records - Client Side Filtering non-aware  
All records searched are marked with a single command, client-side grid filtering is not considered. This is the preferred method and is available only when grid is not filtered.
2. Multiple Records - Client Side Filtering aware  
Each record is marked with its own command, client-side grid filtering is considered. This method is available only when grid is filtered.
3. Single Record - Client Side Filtering aware  
Single record is marked, grid filtering is considered.

#### Issue Class, Group and Name

Browse Combo Boxes of Issue Class, Group to select the Issue Name for marking the unified audit trail records.

The auditor can map certain trail records (or all if necessary) to specific Issues during his daily monitoring of unified audit trail records.

### 3.3 Automatic Audit Trail Management

Omega Core Audit implements automatic audit trail management that relieves the administrator from the tasks of administering the audit trail records.

The Access Control and Real-Time Protection DDL unified trail records are written (in real-time) directly into the Omega Core Audit Repository.

The Standard Audit unified trail records are initially written (in real-time) into the Oracle dictionary table SYS.AUD\$.

The Real-Time Protection DML unified trail records are also initially written (in real-time) into the Oracle dictionary table SYS.FGA\_LOG\$.

The movement of audit records from the Oracle dictionary tables to Omega Core Audit Unified Audit Trail is done by the DB Audit Trails Purge Job that runs every 1 Minute. The process is implemented via the OMEGACA\_TRANS Scheduler job, owned by SYS, installed by the installation script and controlled in the Omega Core Audit Application in the form System Components.

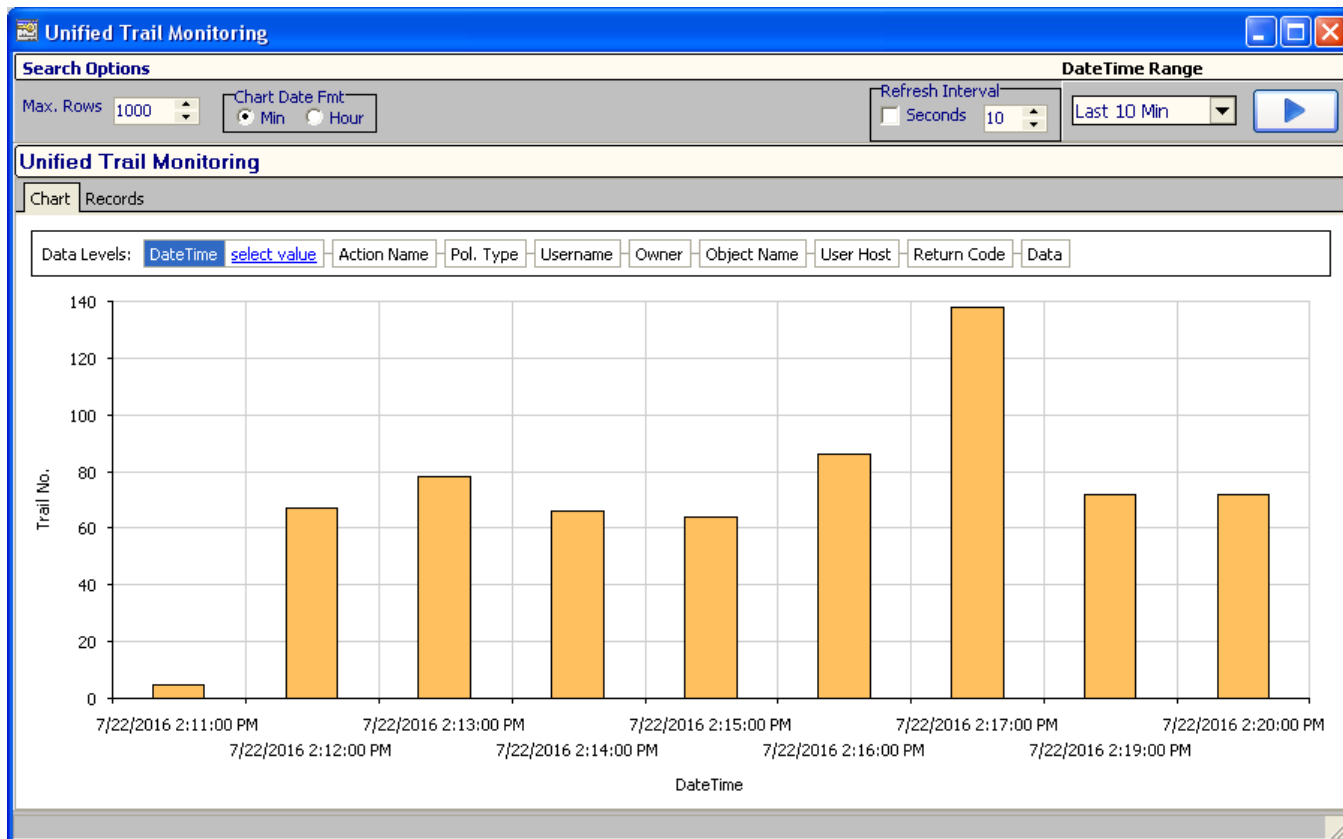
#### **Note:**

The system must be monitored for:

- The size of the OMEGACA\_TS tablespace.
- The free space available to the Datafile[s] on the OS volume[s]!

### 3.4 The Unified Trail Monitoring form

Omega Core Audit comes with a Unified Trail Monitoring form that can actively monitor summary unified trail data in grid and chart formats. To open this form in the Main Menu, Tab Audit Trails, group Unified Trails Monitor click the button Unified Audit Monitor. This will open the form Unified Trail Monitoring.



Main data elements of the Unified Audit Monitoring form are described below.

#### Search Options Panel

The Search Options Panel is top-aligned in the form and contains the following search-related elements:

##### Max Rows

Limit on maximum number of rows returned (this form is intended to auto-refresh data at defined intervals, see below). You can change this limit into the Spin Editor.

##### Chart Date Format Panel

Audit DateTime date format in grouping, truncated either to Minute or Hour. It applies to chart only.

##### Refresh Interval Group

Check the Seconds Checkbox to activate auto-refresh of data for the period defined into the Spin Editor.

##### Date Time Range Panel

In this panel you define the obligatory DateTime range conditions when searching the unified audit trail.

Predefined DateTime Range intervals are selected in the combo box.

To search the unified audit trails, press the Search (blue arrow) button and wait until search completes.

### **Unified Trail Monitoring Panel**

The Unified Trail Panel is client-aligned in the form and shows the searched summary unified trail records into the following elements:

#### **Chart Tab**

In this tab the searched summary unified trail records are displayed in chart format. You can drill-down by "Data Levels:" panel above, or by clicking on the chart's bar. This is tab is the default opened.

#### **Records Tab**

In this tab the searched summary unified trail records are displayed in the classic grid (table) format.

#### **Important Note**

Topic "Important Performance Note" of the paragraph "Client-Side information retrieval" applies even here.

### 3.5 The Unified Trail for Log Collector (SIEM) Systems

The Omega Core Audit is fully equipped to perform its tasks and protect its data. However cases that require external storage of unified audit trails might appear, for example in the case of a financial institution that is seeking PCI Compliance, where external storage of audited data is a requirement.

Also many enterprises and organizations today already do make use of Log Collection/SIEM systems for central storage, consolidation and alerting of log data from multiple sources of different system types. Thus central storage of audited information might be an internal requirement.

Most Log Collection and common SIEM systems do somehow support the pull of data from the Oracle database in custom mode – in the meaning to have the table name (or the SQL for retrieval) customized, not fixed to SYS>AUD\$ only! Other solutions involve a locally installed SIEM Agent.

The unification of audit trails in Omega Core Audit makes it easy to retrieve the audit records from Log Collection/SIEM Appliances.

The Unified Audit Trail View name in the Repository is V\_SYS\_UNF\_TRAIL. The first two fields are timestamps:

TIMESTAMP_STS	The Audit DateTime field in the Application.
TIMESTAMP_UTC	The Audit UTC field in the Application.

and as such very appropriate for time reference from the Log Collection/SIEM pull process.

## 4 CHAPTER 4: Access Control

### 4.1 How it works

The Access Control module establishes database perimeter defense by applying mandatory access control to all connections to the database. It operates on top of Oracle database event triggers feature and implements a special software protection layer that supersedes standard user logon privileges. No users, including privileged accounts and DBAs, can log on to the database without complying with the access control policies.

It is based on the system-level trigger on the logon event capability of the Oracle's database. Each logon is evaluated on real time against the access control policies, access is mandatory, users will be able to log into the database only after complying (Policy evaluated to TRUE) with at least one policy. Non-compliant connections can be rejected in real time and logged off from the database.

Multi-factor user authorization permits logon only on specific combination of user & environment context values, be those user, host, OS logon and terminal names, IP addresses, program used, time and many more.

Access control trails provide details on user's logon activity into the system. An access control trail is generated depending on the settings of the evaluated policies Audit Option and the policy's evaluation result TRUE/FALSE. Evaluation of multiple policies by a login action generates one single access control trail record, displayed mapped to all causing policies!

A specific feature of the Access Control comparing to other modules, is that an access control trail record is always generated if not a single TRUE policy is found during evaluation, even if no policy is evaluated at all because of the policy's User Appliance setting.

This goes independently from the policies and by the module itself. You will always have an access control trail for a non-complying logging!

### 4.2 Access Control Guidelines

#### 4.2.1 General Guidelines

Create secure login channels into the database for individual, or groups of users according to their work profiles, by creating policies permitting access to them.

Although the Omega Core Audit processing cost on Access Control is very small comparing to the cost of the Oracle logon process, it is advised that you beware the performance anyway.

Remember that for each logon all access control policies are evaluated. Thus be aware of the evaluation cost by:

- Have a limited number of Access Control policies, especially when the User Appliance option is All Users.
- Using the User Appliance Feature of the policy to Users Apply and declare users to the respective list.
- Enable the Use Cache option for all policies.
- Disable the Debug Log option for all policies.
- Be aware of intensive connections from interfaces and software's authenticating with common database credentials.

#### **Note:**

Omega Core Audit's Access Control module has demonstrated to cause no performance impact even on live systems with 3-4 thousands connections per minute from interfaces only, plus the continuous operations of hundred users working on application systems with the characteristic of opening a separate session for each application form.

### **4.2.2 Silent Access Control Module**

The Access Control module's Silent mode controls the protective action regarding the connection's compliance. The protective action is the rejection of the user's logon, but when Silent is enabled, user will be allowed to logon, although policy evaluation and trailing will continue as configured.

The Access Control Silent mode is enabled by default on Omega Core Audit install. Use the Silent mode for database access behavior discovery (retaining the audit capability), until you establish secured access paths for all logging accounts to the database through your policies. Mind the database internal actions, like those of Oracle accounts SYS, SYSTEM, SYSMAN and more, mostly via jobs, and those of application schemas or interfaces!

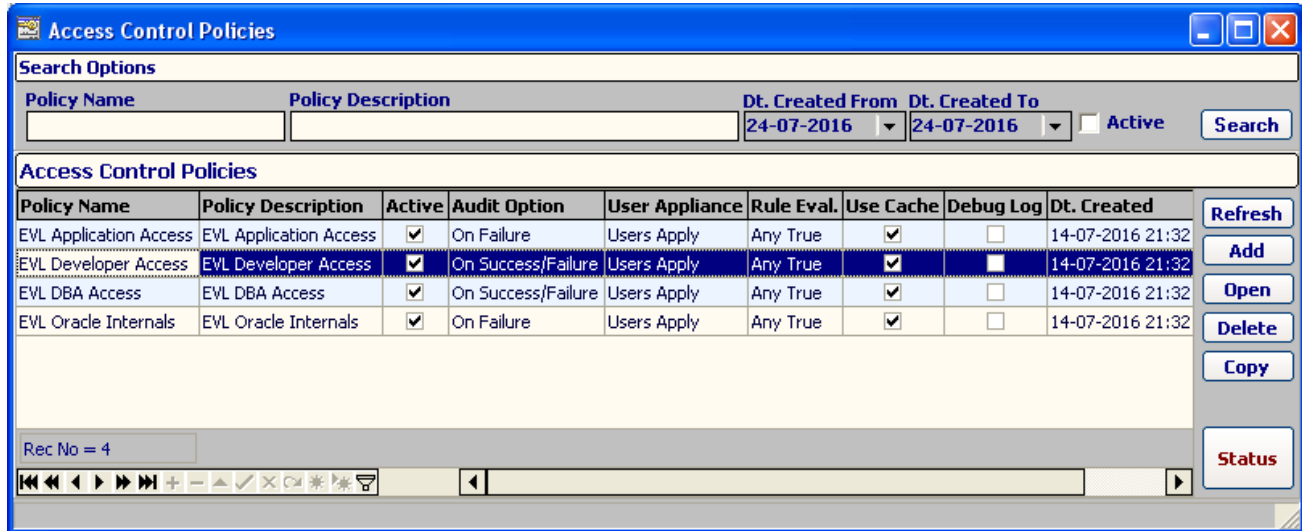
Normally the Access Control module's Silent mode would be used only during the time of initial setup or on emergency. Deactivate this option after you have properly configured Access Control through your policies, so that unauthorized connections are not allowed to continue!

Access Control module's Silent mode is managed into the System Components form in the main menu Administration, Access Control tab, Silent Checkbox. Press the Set button to set the changed value.



### 4.3 Access Control Policies

Access control policies enforce and formalize security compliance policies on user's connections to the database. To view the policies, in the Application's main menu Audit Policies, tab Access Control click the menu button Policies. This will open the Access Control Policies form.



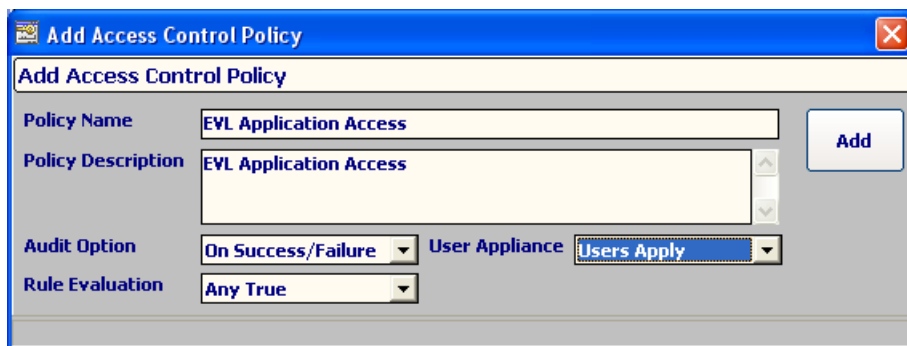
The following are the properties of the Access Control policy:

Field Name	Field Description
Policy Name	Unique Name of the policy within the module.
Policy Description	Description of the policy.
Active	Policy status, Active or Inactive.
Audit Option	Policy evaluation effect on access control trail record. Available options: Disabled – No Access Control Trail record is created. On Failure – Access Control Trail record is created on a FALSE Policy. On Success and Failure – Access Control Trail record is always created.
User Appliance	Policy appliance regarding database users. Available options: All Users – Policy is applied to all users. Users Apply – Policy is applied only to users in the Users Apply List. Users Exclude – Policy is not applied to users in the Users Exclude List.
Rule Evaluation	Policy's evaluation mode regarding rules. Available options: Any True – Policy is True when at least one rule is evaluated True. All True – Policy is True if all rules are evaluated True. Formula – User defined logical formula built on rules.
Formula	Text of the policy's logical formula built on rules.
Use Cache	Use of Policy Cache on evaluation. Available options: Checked – Cache is enabled for policy, recommended value and default on create. Unchecked – Cache is not enabled for policy, non-recommended value.
Debug Log	A Debug Log is created when policy is evaluated. Available options: Checked – Debug log is enabled for policy, non-recommended value. Unchecked – Debug log is not enabled for policy, recommended value and default on create.

Enter the desired options and press the button Search on the right. The result will be listed in the Access Control Policies grid. Press the Refresh button to refresh them.

### 4.3.1 Adding a new Access Control Policy

To create a new access control policy, in the form Access Control Policies, Access Control Policies grid, press the button Add on the right. The form Add Access Control Policy will open.

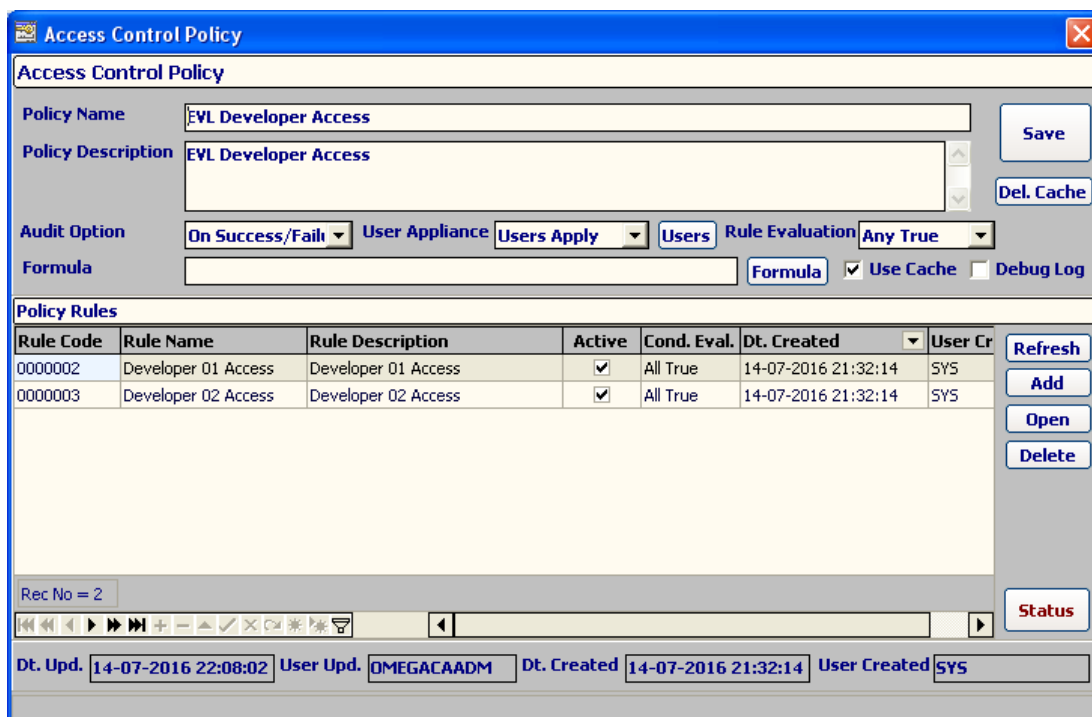


Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new policy will be created with an Inactive status. You can change that later, after adding the rules.

### 4.3.2 Opening/modifying an Access Control Policy

To open an access control policy in full details for viewing and modification, select a policy record in the form Access Control Policies, Access Control Policies grid and press the button Open on the right. The form Access Control Policy will open.



Rule Code	Rule Name	Rule Description	Active	Cond. Eval.	Dt. Created	User Cr
0000002	Developer 01 Access	Developer 01 Access	✓	All True	14-07-2016 21:32:14	SYS
0000003	Developer 02 Access	Developer 02 Access	✓	All True	14-07-2016 21:32:14	SYS

To update any policy changes press the button Save. You will receive a confirmation, or the error message when failure.

Press the button Del. Cache to manually clear the access control cache for this policy. Press the button Formula to open the policy's formula editor form. Press the button Users to open the user appliance/exclusion form.

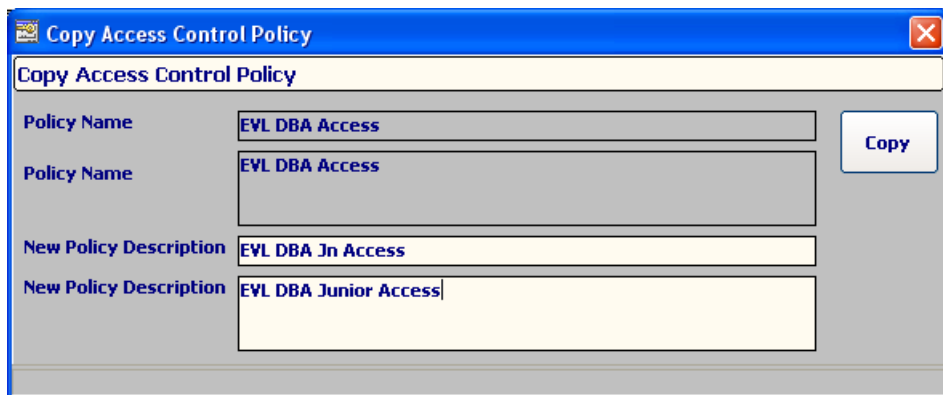
### 4.3.3 Deleting an Access Control Policy

To delete an access control policy, select a policy record in the form Access Control Policies, Access Control Policies grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected policy will be deleted together with its cache, rules, conditions and [not] IN lists.

You will receive a confirmation, or the error message when failure.

### 4.3.4 Copying an Access Control Policy

To copy an access control policy, select a policy record in the form Access Control Policies, Access Control Policies grid and press the button Copy on the right. The form Copy Access Control Policy will open.



Set the required fields and press the button Copy.

You will receive a confirmation, or the error message when failure. The new policy will be created with its rules, conditions, [not] IN lists as the original policy and with an Inactive status.

### 4.3.5 Access Control Policy Status

To change an access control policy status, select a policy record in the form Access Control Policies, Access Control Policies grid and press the button Status below on the right. If the change status dialog box is confirmed, the current policy status will be reversed from its current setting. Policy must have active rule for its status to be set as Active. If the policy Audit Option is other then All Users, respective Apply and Exclude lists must have at least one entry.

## 4.4 Access Control Rules

Access control rules are defined under policies. To view the access control rules for the selected policy open the form Access Control Policy. The rules bounded to the policy will be listed in the Policy Rules grid.

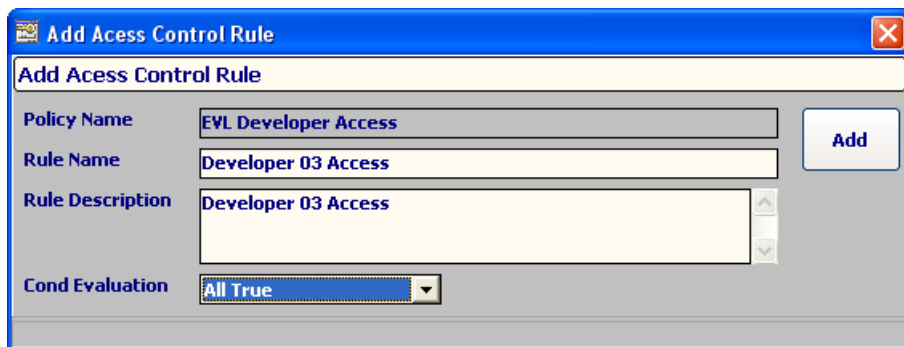
The following are the properties of the Access Control rule:

Field Name	Field Description
Rule Code	Unique auto-generated code of the rule within the module.
Rule Name	Name of the rule.
Rule Description	Description of the rule.
Active	Rule status, Active or Inactive.
Condition Evaluation	Rule evaluation mode regarding conditions. Available options: Any True – Rule is True when at least one condition is evaluated True. All True – Rule is True if all conditions are evaluated True. Formula – User defined logical formula built on rules.
Formula	Text of the rule's logical formula built on conditions.

Press the Refresh button to refresh them.

### 4.4.1 Adding a new Access Control Rule

To create a new access control rule for the selected policy, in the form Access Control Policy, Policy Rules grid, press the button Add on the right. The form Add Access Control Rule will open.



Set the required fields and press the button Add. You will receive a confirmation, or the error message when failure. The new rule will be created with an Inactive status. You can change that later, after adding the conditions.

### 4.4.2 Opening/modifying an Access Control Rule

To open an access control rule in full details for viewing and modification, select a rule record in the form Access Control Policy, Policy Rules grid and press the button Open on the right. The form Access Control Rule will open.

**Access Control Rule**

Policy Name:

Rule Name:

Rule Description:

Cond Evaluation:  Formula:

**Rule Conditions**

Cond. Code	Active	Cond. Eval.	Factor Name	Opr. Symbol	Operand 1	Operand 2	Min. Trust Level	Val.
0000005	<input checked="" type="checkbox"/>	Operand	Session User	=	OMEGACATESTDEV02		Undefined	
0000006	<input checked="" type="checkbox"/>	Operand	Client Host	=	WORKGROUP\DEV100-XXX		Undefined	

Rec No = 2

Dt. Upd.  User Upd.  Dt. Created  User Created

To update any rule changes press the button Save. You will receive a confirmation, or the error message when failure.

Press the button Formula to open the rule's formula editor form based on conditions.

#### 4.4.3 Deleting an Access Control Rule

To delete an access control rule, select a rule record in the form Access Control Policy, Policy Rules grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected rule will be deleted together with its policy cache, conditions and [not] IN lists.

You will receive a confirmation, or the error message when failure.

#### 4.4.4 Access Control Rule Status

To change an access control rule status, select a rule record in the form Access Control Policy, Policy Rules grid and press the button Status below on the right. If the change status dialog box is confirmed, the current rule status will be reversed from its current setting. Rule must have at least one active condition for its status to be set as Active.

#### 4.5 Access Control Conditions

Access control conditions are defined under policy rules. To view the access control conditions for the selected rule open the form Access Control Rule. The conditions bounded to the rule will be listed in the Rule Conditions grid.

The following are the properties of the Access Control condition:

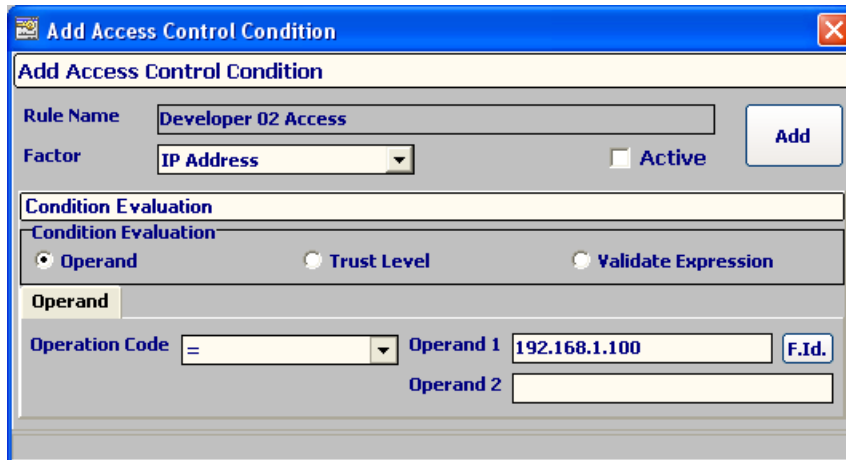
Field Name	Field Description
Condition Code	Unique auto-generated code of the condition within the module.
Active	Condition status, Active or Inactive.

Condition Evaluation	Condition evaluation mode regarding factor. Available options: Operand - Condition is evaluated by comparing the retrieved value of the factor with the operand's value. Trust level - Condition is evaluated by comparing the retrieved value of the factor with the pre-declared Factor's trust level values. Validate Expression – Condition is evaluated as a result of an user-defined database function returning a Boolean result.
Factor	Factor being evaluated
Operation code	Code the operation type applied to the evaluation of the Factor's retrieved value.
Operand 1	Value of the first operand.
Operand 2	Value of the second operand.
Minimal Trust Level	Minimal required trust level.
Val. Exp. Owner	Validate expression owner.
Val. Exp. Object	Validate expression object name.

Press the Refresh button to refresh them.

#### 4.5.1 Adding a new Access Control Condition

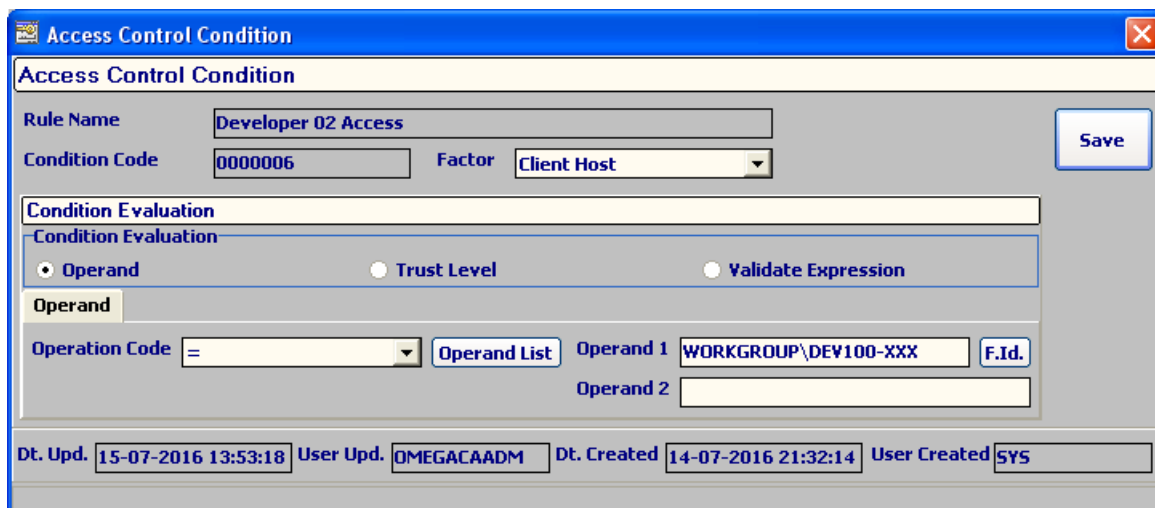
To create a new access control condition, in the form Access Control Rule, Rule Conditions grid, press the button Add on the right. The form Add Access Control Condition will open.



Set the required fields and press the button Add. You will receive a confirmation, or the error message when failure. Choosing the condition evaluation mode through the radio-boxes opens respective input fields. The new condition's status can be set on creation, except when condition evaluation Operand and operation code [not] IN that are created as Inactive.

#### 4.5.2 Opening/modifying an Access Control Condition

To open an access control condition in full details for viewing and modification, select a condition record in the form Access Control Rule, Rule Conditions grid and press the button Open on the right. The form Access Control Condition will open.



To update any condition changes press the button Save. You will receive a confirmation, or the error message when failure. Press the Operand List button to set Operand list when condition evaluation of type Operand and Operation Code [not] IN.

### 4.5.3 Deleting an Access Control Condition

To delete an access control condition, select a condition record in the form Access Control Rule, Rules Conditions grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected condition will be deleted together with its policy cache, and [not] IN lists.

You will receive a confirmation, or the error message when failure.

### 4.5.4 Access Control Condition Status

To change an access control condition status, select a condition record in the form Access Control Rule, Rules Conditions grid and press the button Status below on the right. If the change status dialog box is confirmed, the current condition status will be reversed from its current setting. If condition evaluation is of type Operand and Operation Code is [not] IN, then the condition must have at least one active IN list record for its status to be set as Active.

## 5 CHAPTER 5: Standard Audit

### 5.1 How it works

The Standard Audit module ensures a reliable and continuous auditing monitoring and is based on the Oracle's native audit capabilities.

It is based on native auditing capabilities of the Oracle's database.

It ensures an answer in real time to the classical questions – Who/What/How/When/Where in regard to user's activity in the system. It operates on top of Oracle native audit features, is easily configured and graphically enables a complex set of auditing commands via the interface. Standard Auditing consists of:

- Statements & System Privileges – identifies actions performed versus a statement executed and system-wide granted privileges like SELECT TABLE, INSERT ANY TABLE, CREATE SESSION, EXECUTE ANY PROCEDURE and so on.
- Objects – identifies actions performed versus an application or database object, let us say we are interested in tracing every SELECT, INSERT, DELETE, UPDATE into the ACCOUNTS table, made by any user.

The Standard Audit module implements a policy-based auditing, in which audit policies define user-statements and object privileges to be audited.

Automatic standard audit trails management is effective. The DB Audit Trails Purge Job transports the standard audit trails from the Oracle internal structures to the Omega Core Audit Repository and optionally makes the mapping of the standard audit trail record with the policies that caused it.

#### 5.1.1 Activating the Standard Audit

To activate the standard Oracle auditing you need to set the database startup parameter "audit\_trail" to one of the following values:

DB\_EXTENDED - recommended value, ensures full SQL Bind parameters and SQL Text  
DB - non-recommended value, no SQL Bind parameters and SQL Text

You can set this parameter from the Omega Core Audit System Components form, or by executing the following SQL command (with the proper privileges):

```
SQL>alter system set AUDIT_TRAIL=DB_EXTENDED scope=spfile;
```

Because this parameter is a static one, you need to restart the instance for the action to take effect.

### 5.2 Standard Audit Guidelines

Standard Auditing is relatively inexpensive, as demonstrated by audit benchmark tests performed by Oracle and other third parties. However in order to minimize any possible performance impact and to keep the Unified Audit Trail from growing big too quickly, narrow the scope of the audit by referring sensitive objects in combination with the important privileges. You don't have to audit for "all" when you can audit for "specified". This also gives more meaning to your standard audit trail.

Follow these guidelines for minimal performance impact on the system:

- Although auditing is relatively inexpensive, limit the number of audited events as much as possible.



- Evaluate your auditing. Have a clear understanding of your auditing and then devise an appropriate auditing strategy. Avoid unnecessary auditing.
- Audit knowledgeably. Audit the minimum number of user's statements or objects needed to get the targeted information. Balance the sufficient amount of your security information with your ability to store and process it.

Create audit policies for important statements [privileges] given to specific users, administrators, developers and schema owners, and also for important objects, each more set in more detail at rule level by the two available policy types.

### 5.3 Existing Oracle Standard Audits

Existing (Standard) audit settings might be enabled in your database, prior to Omega Core Audit installation. These audit settings might be there because of:

#### 1. Oracle Default Audits

These are all Statement Audits and are activated with the database install using the new feature "Security settings", available in the 11g Database Configuration Assistant.

These default audit statements are user-wide (effective for all users) and are recognized by Omega Core Audit via a special, read-only and pre-deployed Standard Audit policy named "Oracle Default Audits". This policy supports the Oracle's user-wide statements and privileges audited by default. You cannot change this policy, or its rules (Statement Audits), but you can change each one status, activating or de-activating.

This policy and its rules are pre-deployed as Inactive during Omega Core Audit installation! You can activate each rule (Statement Audit) according to what existing statement audits may be and then activate the policy.

#### 2. Audits set by your DBA.

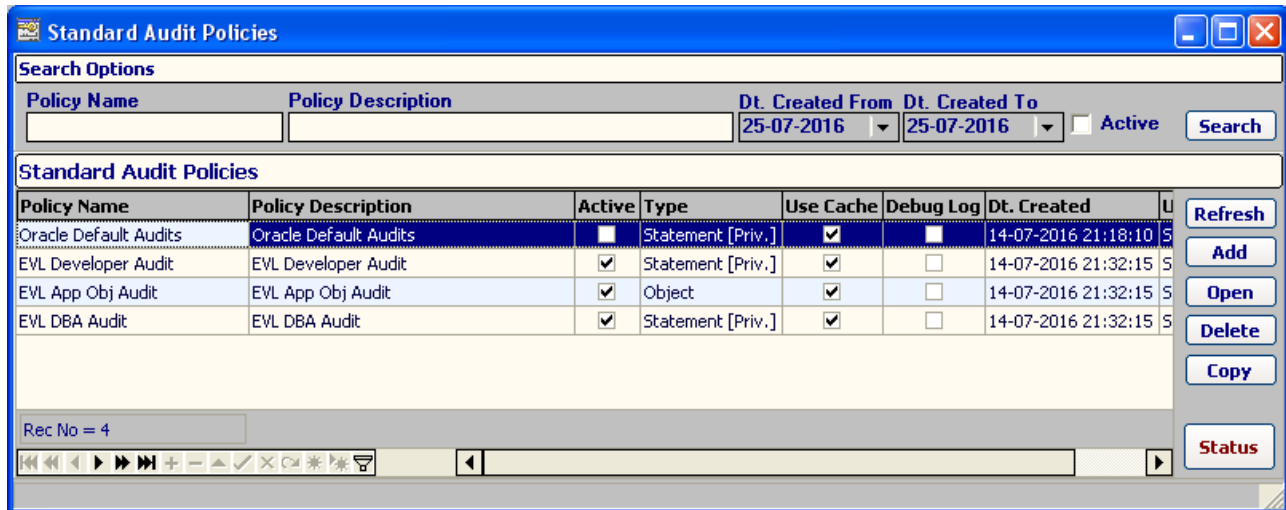
These might be existing statement and object audit settings, set by either your DBA, or information security staff. It is recommended that you remove these audits (with the NOAUDIT command) prior to installing Omega Core Audit.

#### Notes:

1. To check for existing audit settings, open the forms "Statement [System Privilege] Audits" and "Objects Privilege Audits", later described in this chapter in the "Database Standard Audits Interaction" topic.
2. For existing standard audit trail records in SYS.AUD\$, it is recommended that these trails are purged prior to installing Omega Core Audit. However, you can still purge these trails to the Omega Core Audit repository, but no Standard Audit Options Mapping will be available for them.

## 5.4 Standard Audit Policies

Standard audit policies enforce and formalize security compliance policies on auditing users' activity in the database. To view the policies, in the Application's main menu Audit Policies, tab Standard Audit click the menu button Policies. This will open the Access Control Policies form.



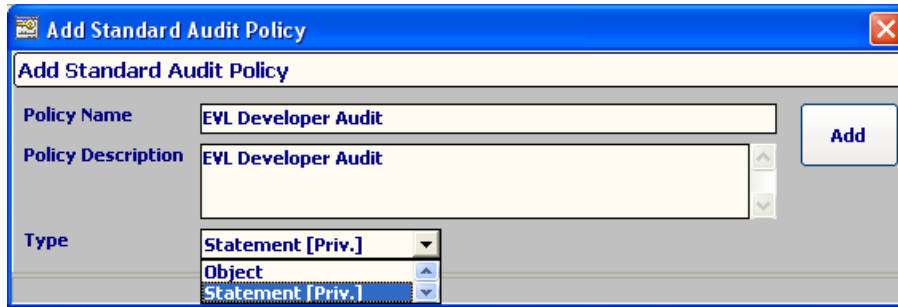
The following are the properties of a Standard Audit Policy:

Field Name	Field Description
Policy Name	Unique auto-generated code of the condition within the module.
Policy Description	Description of the policy.
Active	Policy status, Active or Inactive.
Type	Policy's type regarding standard auditing. Available options: Statements & System Privileges – Auditing on user statements and system privileges only. Object – Auditing on actions performed on objects only.
Use Cache	Use of Policy Cache on Audit Policy Mapping (if enabled). Available options: Checked – Cache is enabled for policy, recommended value and default on create. Unchecked – Cache is not enabled for policy, non-recommended value.
Debug Log	A Debug Log is created on Audit Policy Mapping (if enabled). Available options: Checked – Debug log is enabled for policy, non-recommended value. Unchecked – Debug log is not enabled for policy, recommended value (default on create).

Enter the desired options and press the button Search on the right. The result will be listed in the Standard Audit Policies grid. Press the Refresh button to refresh them.

### 5.4.1 Adding a new Standard Audit Policy

To create a new standard audit policy, in the form Standard Audit Policies, Standard Audit Policies grid, press the button Add on the right. The form Add Standard Audit Policy will open.



**Add Standard Audit Policy**

Policy Name:

Policy Description:

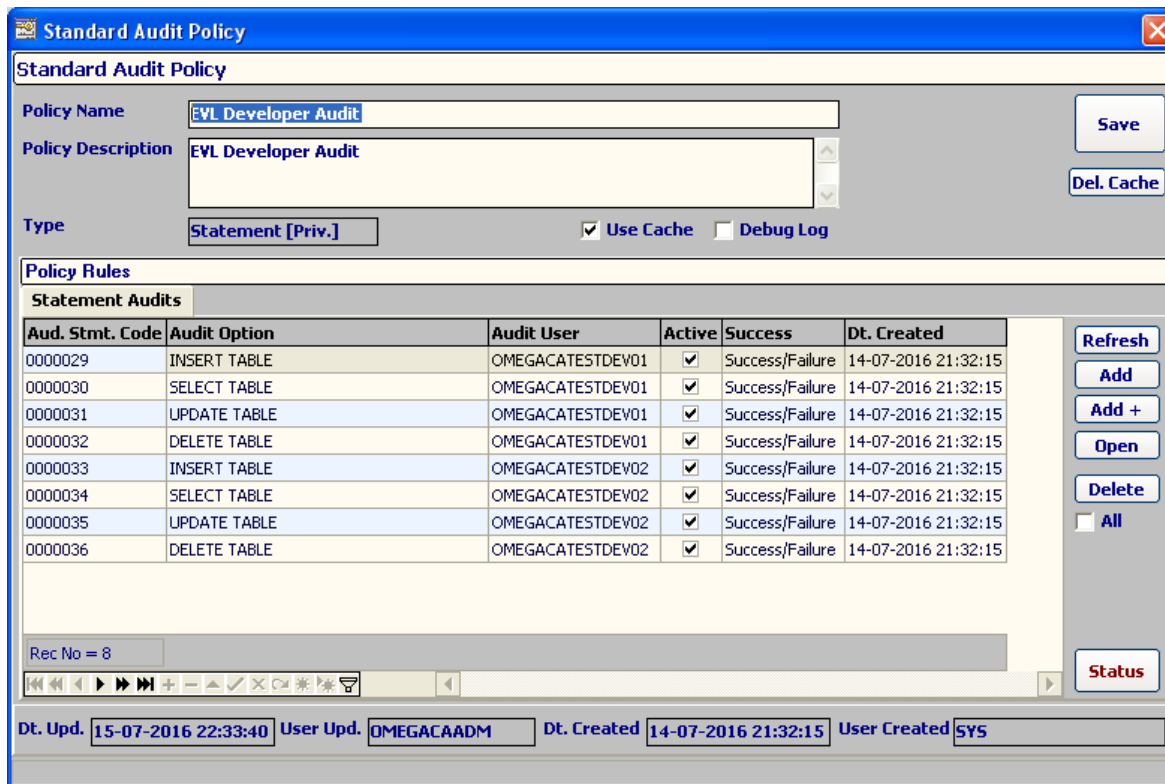
Type:

Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new policy will be created with an Inactive status. You can change that later, after adding the statements or objects audit options, depending on the policy type. Standard Audit Policy type cannot be changed after creation.

### 5.4.2 Opening/modifying a Standard Audit Policy

To open a standard audit policy in full details for viewing and modification, select a policy record in the form Standard Audit Policies, Standard Audit Policies grid and press the button Open on the right. The form Standard Audit Policy will open.



**Standard Audit Policy**

Policy Name:

Policy Description:

Type:  ☒ Use Cache ☐ Debug Log

**Policy Rules**

**Statement Audits**

Aud. Stmt. Code	Audit Option	Audit User	Active	Success	Dt. Created
0000029	INSERT TABLE	OMEGACATESTDEV01	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 21:32:15
0000030	SELECT TABLE	OMEGACATESTDEV01	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 21:32:15
0000031	UPDATE TABLE	OMEGACATESTDEV01	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 21:32:15
0000032	DELETE TABLE	OMEGACATESTDEV01	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 21:32:15
0000033	INSERT TABLE	OMEGACATESTDEV02	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 21:32:15
0000034	SELECT TABLE	OMEGACATESTDEV02	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 21:32:15
0000035	UPDATE TABLE	OMEGACATESTDEV02	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 21:32:15
0000036	DELETE TABLE	OMEGACATESTDEV02	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 21:32:15

Rec No = 8

☐ All

Dt. Upd.  User Upd.  Dt. Created  User Created

To update any policy changes press the button Save.

You will receive a confirmation, or the error message when failure. Press the button Del. Cache to manually clear the standard audit cache for this policy.

### Oracle Def. Audits Panel

Whenever you open the "Oracle Default Audits" policy, you will notice a special panel that will appear only for this specific Standard Audit policy and not for the others.



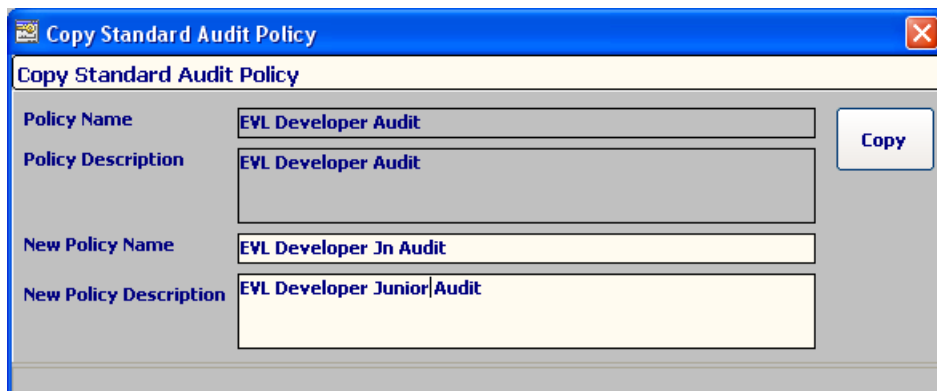
This functionality imports the Oracle's database predefined user-wide audits (feature implemented in 11gR1 and enhanced in 11gR2), into the Omega Core Audit special the "Oracle Default Audits" policy. It is obviously needed mostly after Omega Core Audit install and initial configuration.

### 5.4.3 Deleting a Standard Audit Policy

To delete a standard audit policy, select a policy record in the form Standard Audit Policies, Standard Audit Policies grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected policy will be deleted together with its cache and statement or objects audits, depending on the type. You will receive a confirmation, or the error message when failure.

### 5.4.4 Copying an Standard Audit Policy

To copy an access control policy, select a policy record in the form Access Control Policies, Access Control Policies grid and press the button Copy on the right. The form Copy Access Control Policy will open.



The dialog box titled "Copy Standard Audit Policy" contains the following fields and a button:

Policy Name	EVL Developer Audit	Copy
Policy Description	EVL Developer Audit	
New Policy Name	EVL Developer Jn Audit	
New Policy Description	EVL Developer Junior Audit	

Set the required fields and press the button Copy.

You will receive a confirmation, or the error message when failure. The new policy will be created with its rules, conditions, [not] IN lists as the original policy and with an Inactive status.

### 5.4.5 Standard Audit Policy Status

To change a standard audit policy status, select a policy record in the form Standard Audit Policies, Standard Audit Policies grid and press the button Status below on the right. If the change status dialog box is confirmed, the current policy status will be reversed from its current setting. Policy must have at least one active rule for its status to be set as Active.

If the status of the policy will be Inactive, then all policy's rules, statement or object audits will be disabled!

## 5.5 Standard Audit Rules - Statement Audits

Standard statements (and privileges) audits are defined under policies. To view the statement audits for the selected policy open the form Standard Audit Policy. The statement audits bounded to the policy will be listed in the Policy Rules grid, Statement Audits tab.

The following are the properties of the Standard Audit Rule - Statements Audit:

Field Name	Field Description
Audit Stmt. Code	Unique auto-generated statement audit code within the module.
Audit Option	Audited action.
Audit User	Audited User.
Active	Audit object status, Active or Inactive.
Success	Auditing effective by action's success. Available options: Success/Failure – audits on both success and failure Success – audits on success only Failure – audits on failure only

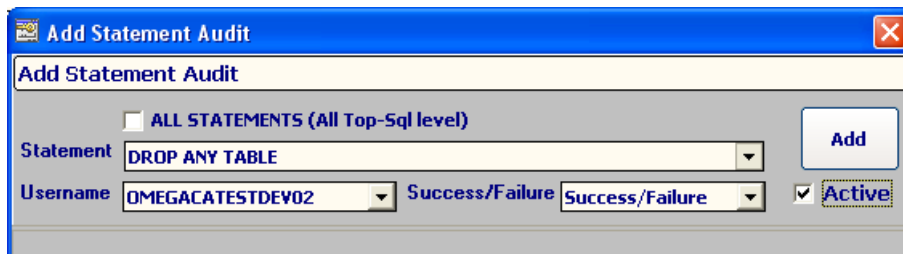
### Important Note:

By Oracle implementation, Standard [no] Audits on statements (and privileges) are effective only on subsequent user sessions and not the current ones!

Press the Refresh button to refresh them.

### 5.5.1 Adding a new single Standard Statement Audit (Rule)

To create a new single statement audit, in the form Standard Audit Policy, Policy Rules grid, Statement Audits tab, press the button Add on the right. The form Add Statement Audit will open.



Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new statement audit's status can be set on creation.

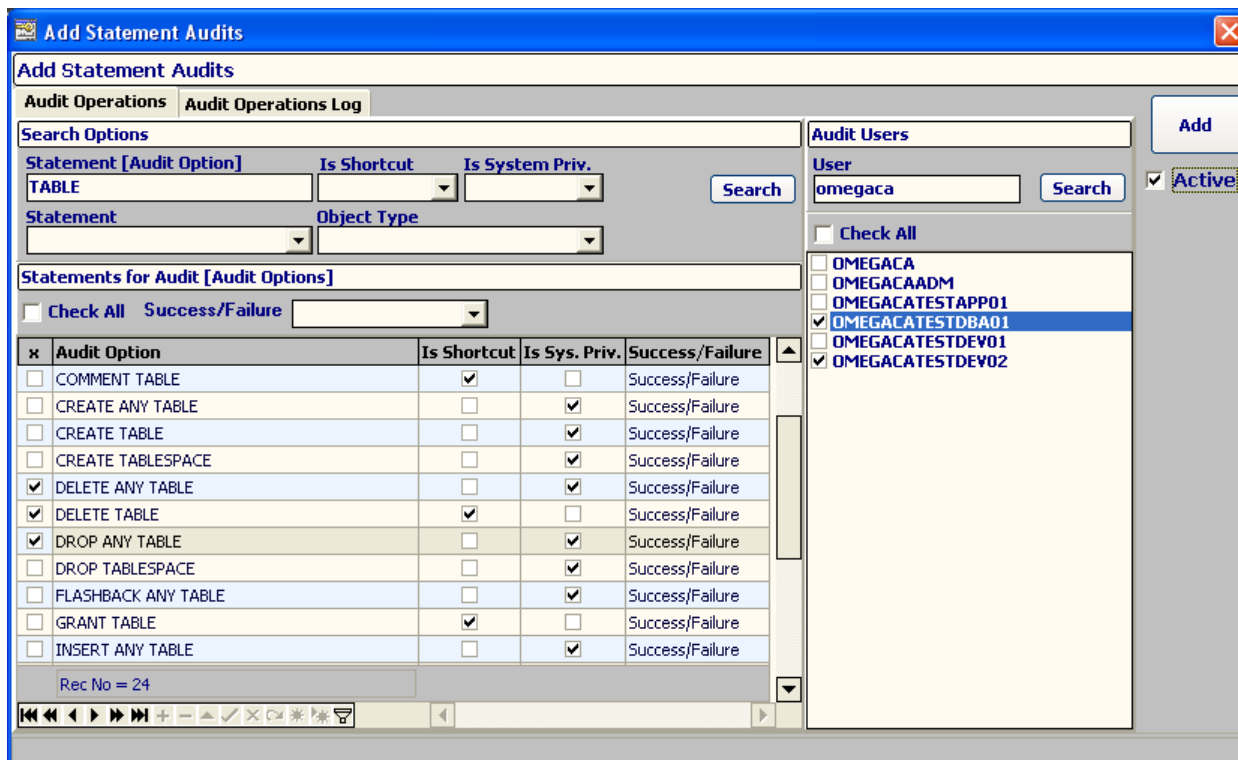
Instead of adding individual statement audits for a user, you can choose to audit ALL STATEMENTS for him, a new feature available from Oracle 11g Release 2. This will audit only top-level SQLs directly executed by the user and not SQL's that may be inside procedural code he calls (procedures, packages and triggers).

### Important Note:

Existing bugs have been verified in the audit ALL STATEMENTS feature in 11gR2. All SQLs instead of top-level only do get audited. This is fixed in the 11.2.0.3 Server Patch Set and in the upper versions (12). See also the 11.2.0.4 Server Patch Set!

### 5.5.2 Adding new multiple Standard Statement Audits

To create new multiple statement audits, in the form Standard Audit Policy, Policy Rules grid, Statement Audits tab, press the button Add+ on the right. The form Add Statement Audits will open.



**Add Statement Audits**

**Audit Operations** | **Audit Operations Log**

**Search Options**

Statement [Audit Option] Is Shortcut Is System Priv. Search

Statement Object Type

**Statements for Audit [Audit Options]**

☐ Check All Success/Failure

x	Audit Option	Is Shortcut	Is Sys. Priv.	Success/Failure
<input type="checkbox"/>	COMMENT TABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Success/Failure
<input type="checkbox"/>	CREATE ANY TABLE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Success/Failure
<input type="checkbox"/>	CREATE TABLE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Success/Failure
<input type="checkbox"/>	CREATE TABLESPACE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Success/Failure
<input checked="" type="checkbox"/>	DELETE ANY TABLE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Success/Failure
<input checked="" type="checkbox"/>	DELETE TABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Success/Failure
<input checked="" type="checkbox"/>	DROP ANY TABLE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Success/Failure
<input type="checkbox"/>	DROP TABLESPACE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Success/Failure
<input type="checkbox"/>	FLASHBACK ANY TABLE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Success/Failure
<input type="checkbox"/>	GRANT TABLE	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Success/Failure
<input type="checkbox"/>	INSERT ANY TABLE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Success/Failure

Rec No = 24

**Audit Users**

User omegaca Search ☒ Active

☐ Check All

- ☐ OMEGACA
- ☐ OMEGACAADM
- ☐ OMEGACATESTAPP01
- ☒ OMEGACATESTDBA01
- ☐ OMEGACATESTDEV01
- ☒ OMEGACATESTDEV02

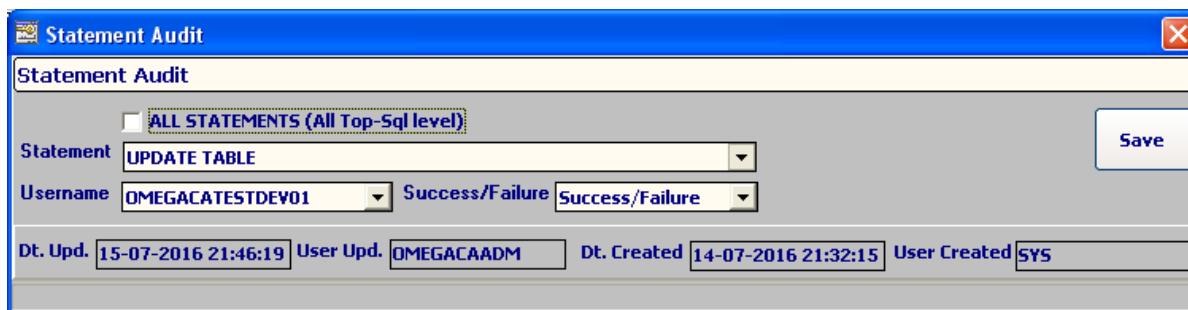
**Add**

Complete the desired options and search for available statements. Choose the statements you want to audit. On the right side chose the Users you want to audit on the selected statements. Press the button Add on the right.

View the multiple operations result into the tab Audit Operations Log. The new statements audits status can be set on creation.

### 5.5.3 Opening/modifying a Standard Statement Audit (Rule)

To open a statement audit in full details for viewing and modification, select a statement audit record in the form Standard Audit Policy, Policy Rules grid, Statement Audits tab and press the button Open on the right. The form Statement Audit will open.



**Statement Audit**

☐ ALL STATEMENTS (All Top-Sql level)

Statement UPDATE TABLE

Username OMEGACATESTDEV01 Success/Failure Success/Failure

Dt. Upd. 15-07-2016 21:46:19 User Upd. OMEGACAADM Dt. Created 14-07-2016 21:32:15 User Created SYS

**Save**

To update any statement audit changes press the button Save. You will receive a confirmation, or the error message when failure.

#### **5.5.4 Deleting a Standard Statement Audit**

To delete a statement audit, select a statement audit record in the form Standard Audit Policy, Policy Rules grid, Statement Audits tab and press the button Delete on the right. If the delete dialog box is confirmed, the selected standard statement audit will be deleted.

You will receive a confirmation, or the error message when failure. You can delete all policy's statement audits by checking the All option.

#### **5.5.5 Standard Statement Audit Status**

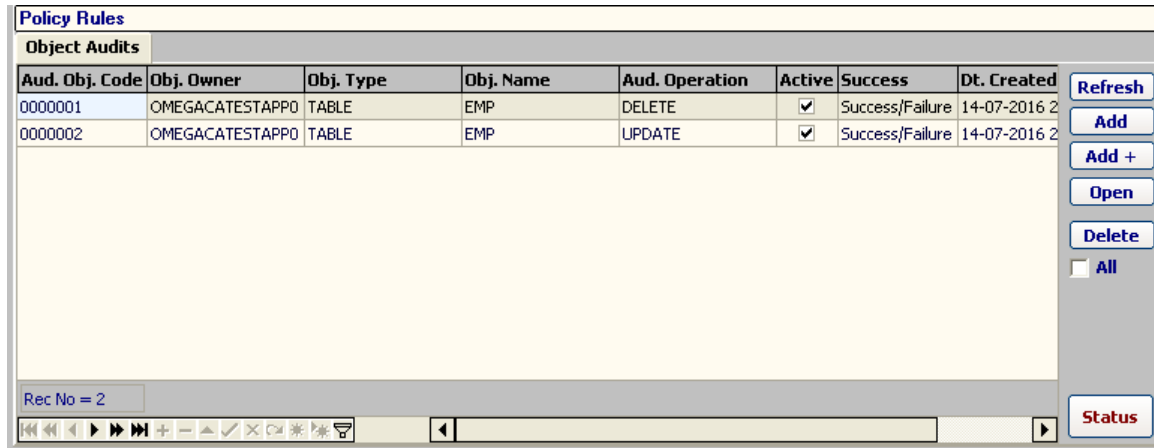
To change a statement audit's status, select a statement audit record in the form Standard Audit Policy, Policy Rules grid, Statement Audits tab and press the button Status below on the right. If the change status dialog box is confirmed, the current statement audit's status will be reversed from its current setting.

**Note:**

Setting a policy rule statement audit's status to Inactive effectively drops (if not used by other rule) the database statement audit setting. This because there is no status property available in database for statements audits up to Oracle 11g (and 12c - traditional auditing).

## 5.6 Standard Audit Rules - Object Audits

Standard object audits are defined under policies. To view the object audits for the selected policy open the form Standard Audit Policy. The object audits bounded to the policy will be listed in the Policy Rules grid, Object Audits tab.



Aud. Obj. Code	Obj. Owner	Obj. Type	Obj. Name	Aud. Operation	Active	Success	Dt. Created
0000001	OMEGACATESTAPPO	TABLE	EMP	DELETE	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 2
0000002	OMEGACATESTAPPO	TABLE	EMP	UPDATE	<input checked="" type="checkbox"/>	Success/Failure	14-07-2016 2

The following are the properties of the Standard Audit Rule - Object Audit:

Field Name	Field Description
Audit Object Code	Unique auto-generated object audit code within the module.
Object Owner	Description of the policy.
Object Type	Policy status, Active or Inactive.
Object Name	Policy's type regarding standard auditing. Available options: Statements & System Privileges – Auditing on user statements and system privileges. Object – Auditing on actions performed on objects.
Active	Audit object status, Active or Inactive.
Audit Operation	Audited operation on the object.
Success	Auditing effective by action's success. Available options: Success/Failure – audits on both success and failure Success – audits on success only Failure – audits on failure only

### Important Note:

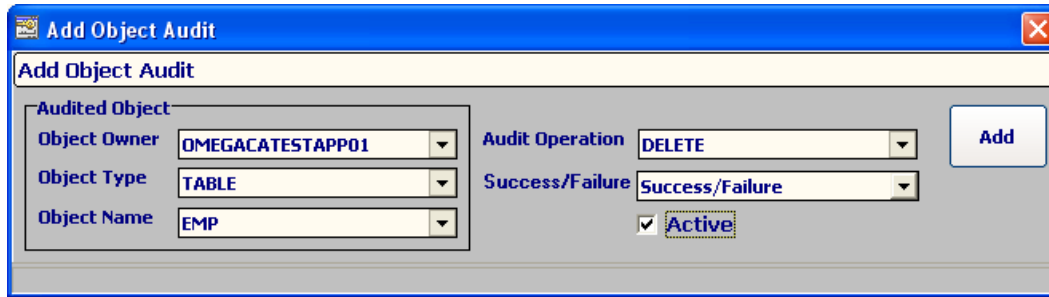
By Oracle implementation, Standard [no] Audits on Object Privileges will take effect immediately!

Press the Refresh button to refresh them.

### 5.6.1 Adding a new single Standard Object Audit

To create a new single object audit, in the form Standard Audit Policy, Policy Rules grid, Object Audits tab, press the button Add on the right. The form Add Object Audit will open.





**Add Object Audit**

**Add Object Audit**

**Audited Object**

Object Owner: OMEGACATESTAPP01

Object Type: TABLE

Object Name: EMP

Audit Operation: DELETE

Success/Failure: Success/Failure

☒ Active

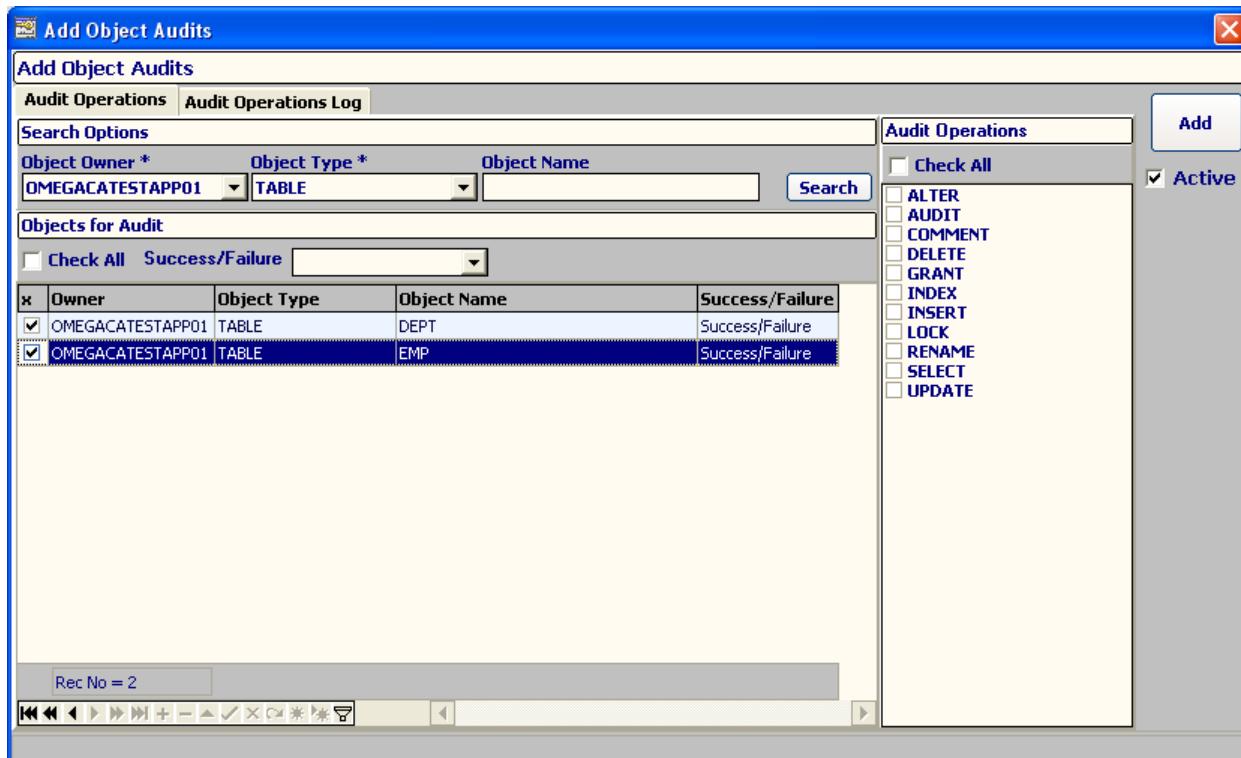
Add

Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new object audit's status can be set on creation.

### 5.6.2 Adding new multiple Standard Object Audits

To create new multiple object audits, in the form Standard Audit Policy, Policy Rules grid, Object Audits tab, press the button Add+ on the right. The form Add Object Audits will open.



**Add Object Audits**

**Add Object Audits**

**Audit Operations** | **Audit Operations Log**

**Search Options**

Object Owner \*: OMEGACATESTAPP01

Object Type \*: TABLE

Object Name:

Search

**Objects for Audit**

☐ Check All Success/Failure:

x	Owner	Object Type	Object Name	Success/Failure
<input checked="" type="checkbox"/>	OMEGACATESTAPP01	TABLE	DEPT	Success/Failure
<input checked="" type="checkbox"/>	OMEGACATESTAPP01	TABLE	EMP	Success/Failure

**Audit Operations**

☐ Check All

☒ Active

ALTER

AUDIT

COMMENT

DELETE

GRANT

INDEX

INSERT

LOCK

RENAME

SELECT

UPDATE

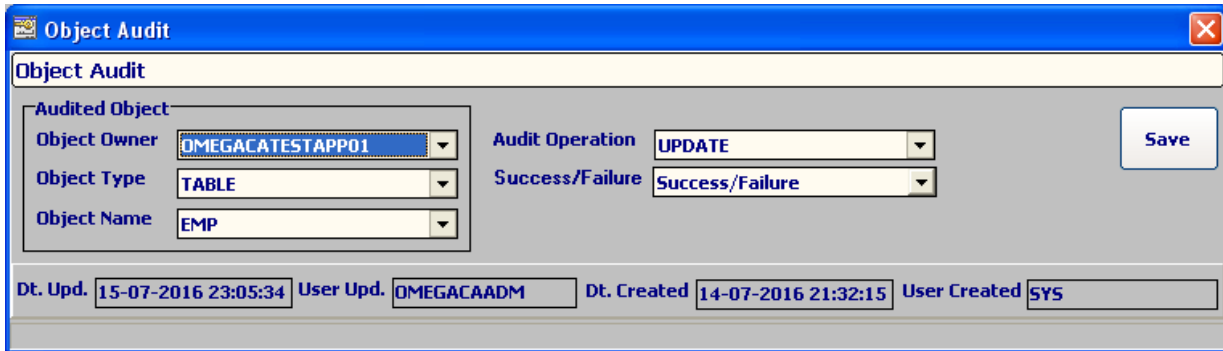
Add

Rec No = 2

Complete the Owner and the type and search for available objects. Choose the objects you want to audit. On the right side chose the Audit Operations you want to audit on the selected objects. Press the button Add on the right. View the multiple operations result into the tab Audit Operations Log. The new objects audits status can be set on creation.

### 5.6.3 Opening/modifying a Standard Object Audit

To open an object audit in full details for viewing and modification, select an object audit record in the form Standard Audit Policy, Policy Rules grid, Object Audits tab and press the button Open on the right. The form Object Audit will open.



To update any object audit changes press the button Save.  
You will receive a confirmation, or the error message when failure.

#### 5.6.4 Deleting a Standard Object Audit

To delete an object audit, select an object audit record in the form Standard Audit Policy, Policy Rules grid, Object Audits tab and press the button Delete on the right. If the delete dialog box is confirmed, the selected object audit will be deleted.

You will receive a confirmation, or the error message when failure. You can delete all policy's object audits by checking the All option.

#### 5.6.5 Standard Object Audit Status

To change an object audit's status, select an object audit record in the form Standard Audit Policy, Policy Rules grid, Object Audits tab and press the button Status below on the right. If the change status dialog box is confirmed, the current object audit's status will be reversed from its current setting.

##### Note:

Setting a policy rule object audit's status to Inactive effectively drops (if not used by other rule) the database object audit setting. This because there is no status property available in database for objects audits up to Oracle 11g (and 12c - traditional auditing).

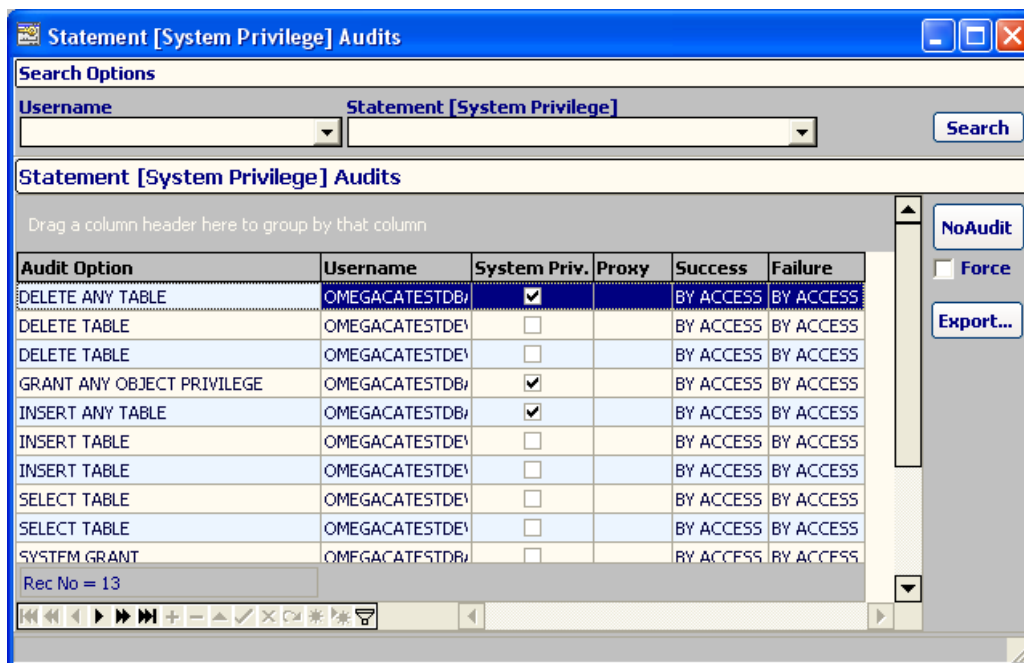
## 5.7 Database Standard Audits Interaction

Omega Core Audit's Standard Audit module automates and visually handles the Oracle database audit functionalities. This is implemented at the policy's rule level, for objects and statement audits, depending on the policy type. Management of database audits is performed automatically at policy rule's create, update, delete and status management. Direct database commands for auditing are processed and executed by the Omega engine and synchronization is held between repository and database audits. Multiple policy rules (statement and object audits) may be related to the same oracle database audit configuration, respectively for database statements and objects audits.

The Omega Core Audit interface will alert you when opening a Statement or Object Standard Audit Rule which is not bounded to a database statement or object audit setting. Ideally you are not supposed to see this, but existence of an orphan Standard Audit Rule is an indicator of audit activity outside Omega Core Audit or an inconsistency of the later.

### 5.7.1 Database Statement [Privilege] Audits

To view the database' statement audits, as they are displayed in the Oracle view DBA\_STMT\_AUDIT\_OPTS, in the Application's main menu Audit Policies tab, Oracle Audit Settings group click on the Statements menu button. The form Statements [System Privileges] Audits will open.



Audit Option	Username	System Priv.	Proxy	Success	Failure
DELETE ANY TABLE	OMEGACATESTDBA	<input checked="" type="checkbox"/>		BY ACCESS	BY ACCESS
DELETE TABLE	OMEGACATESTDBA	<input type="checkbox"/>		BY ACCESS	BY ACCESS
DELETE TABLE	OMEGACATESTDBA	<input type="checkbox"/>		BY ACCESS	BY ACCESS
GRANT ANY OBJECT PRIVILEGE	OMEGACATESTDBA	<input checked="" type="checkbox"/>		BY ACCESS	BY ACCESS
INSERT ANY TABLE	OMEGACATESTDBA	<input checked="" type="checkbox"/>		BY ACCESS	BY ACCESS
INSERT TABLE	OMEGACATESTDBA	<input type="checkbox"/>		BY ACCESS	BY ACCESS
INSERT TABLE	OMEGACATESTDBA	<input type="checkbox"/>		BY ACCESS	BY ACCESS
SELECT TABLE	OMEGACATESTDBA	<input type="checkbox"/>		BY ACCESS	BY ACCESS
SELECT TABLE	OMEGACATESTDBA	<input type="checkbox"/>		BY ACCESS	BY ACCESS
SYSTEM GRANT	OMEGACATESTDBA	<input type="checkbox"/>		BY ACCESS	BY ACCESS

Enter the desired options and press the button Search on the right. The result will be listed in the Statements [System Privileges] Audits grid.

#### Note:

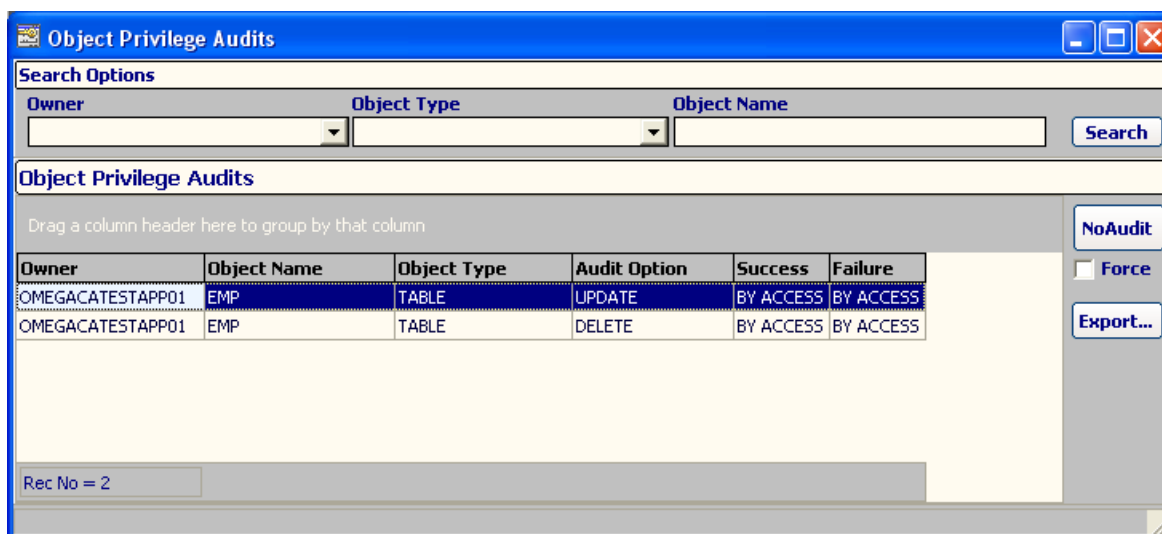
You can drop the selected statement audit option in the database with the NoAudit button. Ideally you are not supposed to use this feature, but you can use it only for any possible database orphan statement audit, which for any reason is not synchronized to the Omega Core Audit repository of standard statement audits!

If the database statement audit you are trying to drop is bound to one or more Omega Core Audit statement audits records, you will receive an indicating error. You can still perform the drop if you choose the Force option.

Management of the database statement auditing is done automatically through the Omega Core Audit Standard Audit module at rule level. Existence of database orphan statement audits is an indicator of audit activity outside Omega Core Audit or an inconsistency of the later.

### 5.7.2 Database Object Audits

To view the database' object audits, in the Application's main menu Audit Policies tab, Oracle Audit Settings group click on the Objects menu button. The form Object Privileges Audits will open.



Owner	Object Name	Object Type	Audit Option	Success	Failure
OMEGACATESTAPP01	EMP	TABLE	UPDATE	BY ACCESS	BY ACCESS
OMEGACATESTAPP01	EMP	TABLE	DELETE	BY ACCESS	BY ACCESS

Enter the desired options and press the button Search on the right. The result will be listed in the Object Privileges Audits grid, tab Records.

#### Note:

You can drop the selected object audit option in the database with the NoAudit button in the tab Details. Ideally you are not supposed to use this feature, but you can use it only for any possible database orphan object audit, which for any reason is not synchronized to the Omega Core Audit repository of standard object audits!

If the database object audit you are trying to drop is bound to one or more Omega Core Audit object audits records, you will receive an indicating error. You can still perform the drop if you choose the Force option.

Management of the database object auditing is done automatically through the Omega Core Audit Standard Audit module at rule level! Existence of database orphan object audits is an indicator of audit activity outside Omega Core Audit or an inconsistency of the later.

To view the database' object audits, as they are displayed in the Oracle view DBA\_OBJ\_AUDIT\_OPTS, in the Application's main menu Audit Policies tab, Oracle Audit Settings group click on the "Obj. Native" menu button. The form "Object Privilege Audits - Oracle Classic" will open.

### 5.7.3 Standard Audit Unified Trail Mapping

The Oracle database offers no clear connection between its standard audit trails and the audit options you have set, either for statement or object audits. This is up to version 11g Release 2 and also 12c Release 1 (Traditional Audit). There is no relationship, either referential integrity or view, from the Oracle view `DBA_AUDIT_TRAIL`, containing standard audit trail records, to least one of:

- Standard Statement Audits
- Standard Object Audits

In other words you cannot exactly define what standard audit settings, either statements or objects, caused the generation of a specific audit trail record.

Omega Core Audit features the mapping of the Unified Audit Trail records of Policy Type Standard Audit, to the causing Standard Audit Policy[s]. When feature is enabled, the Trail Evaluation field of the Unified Audit Trail will contain the text formatted information of the policy[s] that caused this trail record, otherwise will be empty.

Details on the operation of this feature are explained more in depth in the Chapter "System Administration", topic "DB Audit Trails Purge".

### Standard Audit Options Mapping

The configuration is viewable but non-modifiable to the system user. In the Application's main menu Audit Policies tab, see the Standard Audit Options Map group.

Then you:

- Press the Audit Actions menu button to open the form "Standard Audit Actions". In the upper grid you can see the database audit actions, as they are displayed in the Oracle table `AUDIT_ACTIONS`; in the lower grid you can view their respective object and statement audit options.
- Press the Statements menu button to open the form "Standard Audit SQL Statements and Operations". In the upper grid you can see the database standard statement and privileges audit options, as they are displayed in the Oracle table `STMT_AUDIT_OPTION_MAP`; in the lower grid you can view their respective audit actions.
- Press the Objects menu button to open the form "Standard Audit Schema Object Auditing Operations". In the upper grid you can see the database standard object audit options, as they are indicated in the Oracle documentation; in the lower grid you can view their respective audit actions.
- Press the Privileges menu button to open the form "System Privileges". Here you can see the database system privileges, as they are displayed in the Oracle table `AUDIT_ACTIONS`. They are not directly bounded (key/view) to the Audit Actions; however they are used in mapping and also in the user Security-related functionalities.

## **6 CHAPTER 6: Real-Time Protection DDL**

### **6.1 How it works**

The Real-Time Protection DDL module enforces security compliance and defense on structural changes into the database (change management). It operates on top of Oracle database event triggers feature and implements a special software protection layer that supersedes standard user DDL privileges. No users, including privileged accounts and DBAs, can perform DDL actions on the Secured Areas without complying with the real-time protection DDL policies.

It is based on the system-level trigger on the DDL event capability of the Oracle's database.

DDL actions are evaluated against real-time protection DDL policies implementing Secured Areas to be audited and protected. Secured Areas are defined as combinations of owner, object type, object name and DDL event (action) and represented at policy level. Authorization is mandatory; compliance is achieved if all applying DDL policies are evaluated to TRUE. Optionally, if the Real-Time Protection Policy's Deny setting is disabled, the DDL action will be rejected in real-time and not allowed to continue.

Optionally, if the Real-Time Protection DDL Policy's Silent Deny setting is disabled, then the DDL action will be rejected in real time and not allowed to continue.

Multi-factor user authorization permits logon only on successful combination of user & environment context values, be those user, host, OS logon and terminal names, IP addresses, client identifier, program used, time and many more.

Real-time protection DDL trails provide details on user's DDL activity into the system. A real-time protection DDL trail is generated depending on the settings of the evaluated policies Audit Option and the policy's evaluation result TRUE/FALSE. Evaluation of multiple policies by a login action generates one single real-time protection DDL trail record, displayed mapped to all causing policies!

### **6.2 Real-Time Protection DDL Guidelines**

#### **6.2.1 General Guidelines**

In a properly developed environment, DDL (Data definition language) commands should be rare when comparing with normal actions such a logons and data operation - selecting, inserting, updating, deleting, executing... and so. Although full DDL audit can be performed, it is advisable even here to narrow the scope of the auditing to the areas of interest.

Create Secured Areas mainly by Object Owner that can also be combined with one or more of Object Name, Object Type and Action (Event) performed. For example you audit and protect all DDLs for a certain Schema or for a certain Schema and all objects of type TABLE ... and so on.

Use the rules to authorize the Secured Area defined at policy level. Mind the DDL Body option to activate full object's original DDL body preservation in the field with the same name in the Unified Audit Trail.

Be aware of the evaluation cost of the Real-Time Protection policies by:

- Have a limited number of Real-Time Protection DDL, policies, especially when the User Appliance option is All Users.
- Enable the Use Cache option for all policies.
- Disable the Debug Log option for all policies.

### **6.2.2 Silent Deny RTP DDL Policies**

The RTP DDL Policy's Silent Deny mode controls the protective action regarding the compliance of the DDLs being executed on the Secured Area covered by the policy. The protective action is the rejection of the user's DDL, but when Silent Deny is enabled, the DDL will be allowed to execute, although policy evaluation and trailing will continue as configured.

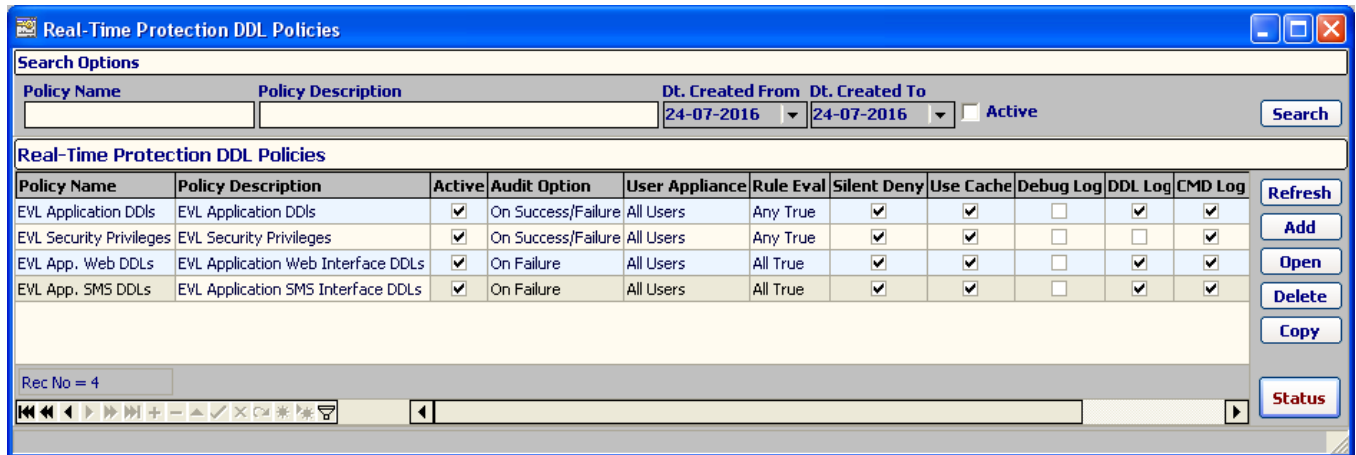
The RTP DDL Policy's Silent Deny mode is enabled by default on each new policy. Use the Silent Deny mode for database DDL behavior discovery (retaining the audit capability), until you establish secured access paths for DDLs affecting your defined Security Areas through your policies. Mind the database internal actions, like those of Oracle accounts SYS, SYSTEM, SYSMAN and more, mostly via jobs, and those of application schemas or interfaces!

Normally the Real-Time Protection DDL Policy's Silent Deny mode would be used only during the time of initial setup or on emergency. Deactivate this option after you have properly configured Real-Time Protection DDL through your policies, so that unauthorized DDLs are not allowed to continue!

The Silent Deny option is managed for each RTP DDL Policy, Silent Deny Checkbox in DDL Policy form.

### 6.3 Real-Time Protection DDL Policies

Real-time protection DDL policies enforce and formalize security compliance policies on user's DDL actions into the database. To view the policies, in the Application's main menu Audit Policies, tab RTP DDL click the menu button Policies. This will open the Real-Time Protection DDL Policies form.



The following are the properties of the RTP DDL policy:

Field Name	Field Description
Policy Name	Unique Name of the policy within the module.
Policy Description	Description of the policy.
Active	Policy Active or Inactive.
Audit Options	Policy evaluation effect on real-time protection DDL trail record. Available options: Disabled – No RTP-DDL Trail record is created. On Failure – A RTP-DDL Trail record is created on a FALSE Policy. On Success and Failure – A RTP-DDL Trail record is always created.
User Appliance	Policy appliance regarding database users. Available options: All Users – Policy is applied to all users. Users Apply – Policy is applied only to users in the Users Apply List. Users Exclude – Policy is not applied to users in the Users Exclude List.
Rule Evaluation	Policy's evaluation mode regarding rules. Available options: Any True – Policy is True when at least one rule is evaluated True. All True – Policy is True if all rules are evaluated True. Formula – User defined logical formula built on rules.
Formula	Text of the policy's logical formula built on rules.
Silent Deny	Action rejected or silent when not authorized (Policy evaluates FALSE). Available options: Checked – Silent mode is enabled, user's action is allowed to continue. This is the default value in policy creation. Unchecked – non-Silent mode, user's action is rejected, an error message indicating non-authorization is raised.
Use Cache	Use of Policy Cache on evaluation. Available options: Checked – Cache is enabled for policy, recommended value and default on create. Unchecked – Cache is not enabled for policy, non-recommended value.
Debug Log	A Debug Log is created when policy is evaluated. Available options: Checked – Debug log is enabled for policy, non-recommended value. Unchecked – Debug log is not enabled for policy, recommended value and default on



	create.
DDL Log	Stores the source of the object (DDL body) before modification into the RTP-DDL Trail record.
CMD Log	Stores the DDL's SQL full text into the RTP-DDL Trail record.

Enter the desired options and press the button Search on the right. The result will be listed in the Real-Time Protection DDL Policies grid. Press the Refresh button to refresh them.

### 6.3.1 Real-Time Protection DDL Policy Secured Area

Each real-time protection DDL policy defines its own Secured Area. It is displayed into the Real-Time Protection DDL Policy form, Secured Area grid. The Secured Area is defined as a logical combination of least one (or more) of the four Area Factors whose values are evaluated with eight different operators. During a DDL event, when the policy is iterated, if the user's DDL action falls inside the defined Secured Area, then the policy is evaluated for compliance. Otherwise the policy will be skipped and not evaluated.

The four Area Factors are:

**Object Owner** - Secured area's object owner.

**Object Type** Secured area's object type. For example:  
TABLE, FUNCTION, INDEX, PROCEDURE, PACKAGE, PACKAGE BODY, TRIGGER...  
See the Omega Core Audit V\_SYS\_OBJ\_TYPE view.

**Object Name** Secured area's object name.

**Action (Event)** Secured area's DDL action (event). One of the following:  
ALTER, ANALYZE, ASSOCIATE STATISTICS, AUDIT, COMMENT, CREATE,  
DISASSOCIATE STATISTICS, DROP, FLASHBACK, GRANT, NOAUDIT,  
PURGE, RENAME, REVOKE, TRUNCATE, UNDROP

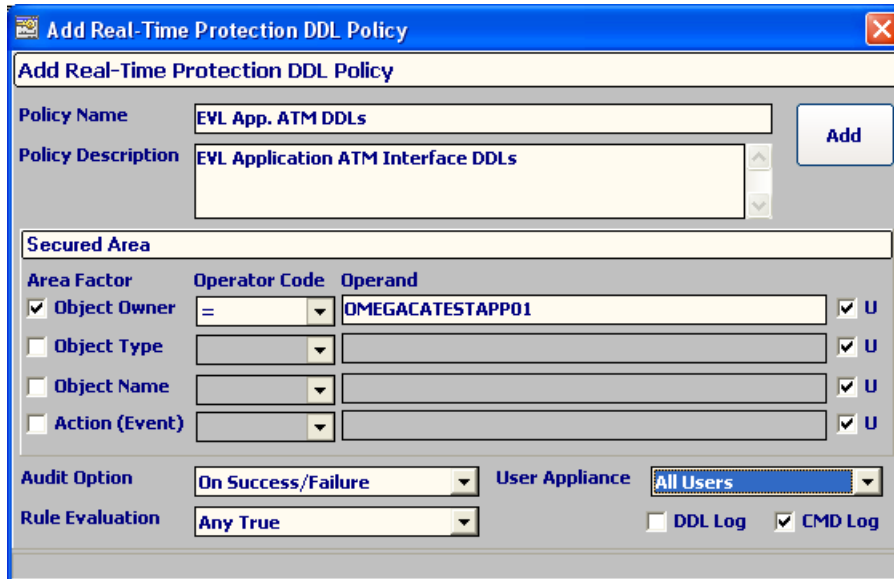
The Secured Area is created together with the policy. See the Add Real-Time Protection DDL Policy form, Secured Area group.

**Note:**

The Diesis # character is internally used by Omega Core Audit as the value separator in the case of IN and NOT IN operands! Use only the Diesis # character to separate values and do not use it as part of any value. Do not use Diesis # in the end as it will generate an empty value.

### 6.3.2 Adding a new Real-Time Protection DDL Policy

To create a new real-time protection DDL policy, in the form Real-Time Protection DDL Policies, Real-Time Protection DDL Policies grid, press the button Add on the right. The form Add Real-Time Protection DDL Policy will open.



**Add Real-Time Protection DDL Policy**

Policy Name:  Add

Policy Description:

**Secured Area**

Area Factor	Operator Code	Operand	
<input checked="" type="checkbox"/> Object Owner	=	OMEGACATESTAPP01	<input checked="" type="checkbox"/> U
<input type="checkbox"/> Object Type			<input checked="" type="checkbox"/> U
<input type="checkbox"/> Object Name			<input checked="" type="checkbox"/> U
<input type="checkbox"/> Action (Event)			<input checked="" type="checkbox"/> U

Audit Option:  User Appliance:

Rule Evaluation:  ☐ DDL Log ☒ CMD Log

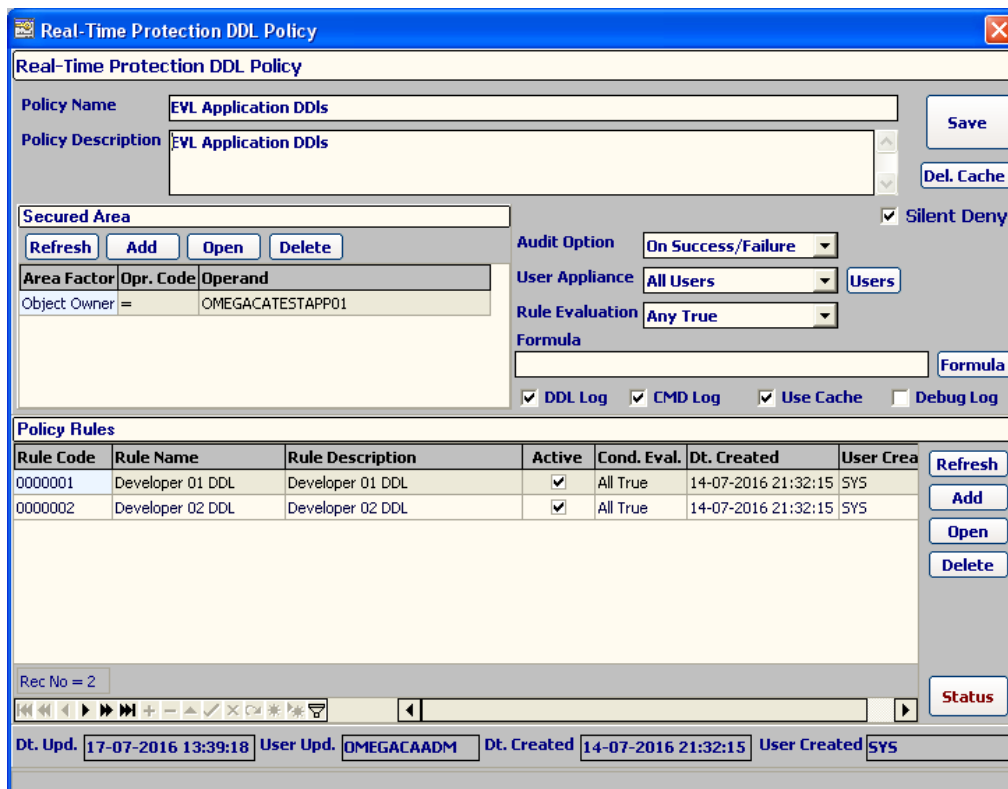
Choose at least one of the four options of the Secured Area. The "U" checkboxes stand for uppercase operand values.

Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new policy will be created with an Inactive status. You can change that later, after adding the rules.

### 6.3.3 Opening/modifying a Real-Time Protection DDL Policy

To open a real-time protection DDL policy in full details for viewing and modification, select a policy record in the form Real-Time Protection DDL Policies, Real-Time Protection DDL Policies grid and press the button Open on the right. The form Real-Time Protection DDL Policy will open.



**Real-Time Protection DDL Policy**

Policy Name:  Save

Policy Description:  Del. Cache

**Secured Area**

Refresh Add Open Delete

Area Factor	Opr. Code	Operand
Object Owner	=	OMEGACATESTAPP01

Audit Option:  ☒ Silent Deny

User Appliance:  Users

Rule Evaluation:

Formula:  Formula

☒ DDL Log ☒ CMD Log ☒ Use Cache ☐ Debug Log

**Policy Rules**

Rule Code	Rule Name	Rule Description	Active	Cond. Eval.	Dt. Created	User Crea
0000001	Developer 01 DDL	Developer 01 DDL	<input checked="" type="checkbox"/>	All True	14-07-2016 21:32:15	SYS
0000002	Developer 02 DDL	Developer 02 DDL	<input checked="" type="checkbox"/>	All True	14-07-2016 21:32:15	SYS

Refresh Add Open Delete

Rec No = 2

DT. Upd.  User Upd.  Dt. Created  User Created  Status

To update any policy changes press the button Save. You will receive a confirmation, or the error message when failure.

In the left part of the form you will see the Secure Area. Press the Refresh and Delete respective buttons to refresh data and delete the selected Area Factor. Press the Add and Open buttons to open respective forms for adding and modifying Area Factors. The "U" checkboxes stand for uppercase operand values.

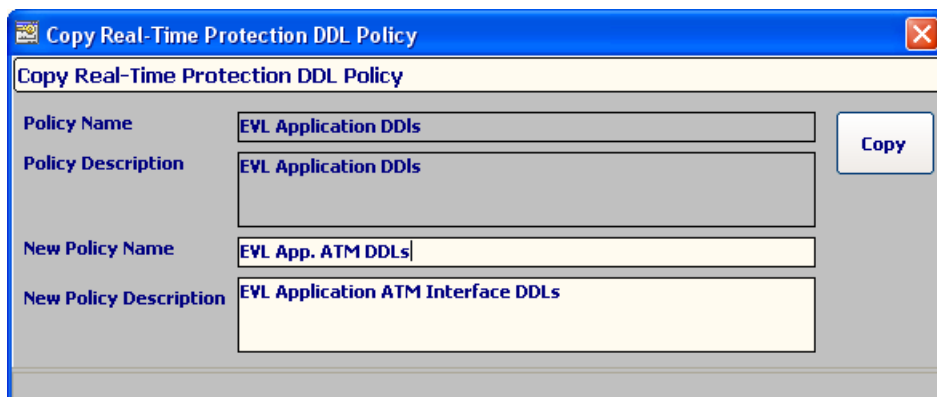
Press the button Del. Cache to manually clear the real-time protection DDL cache for this policy. Press the button Formula to open the policy's formula editor form. Press the button Users to open the user appliance/exclusion form.

### 6.3.4 Deleting a Real-Time Protection DDL Policy

To delete a real-time protection DDL policy, select a policy record in the form Real-Time Protection DDL Policies, Real-Time Protection DDL Policies grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected policy will be deleted together with its cache, rules, conditions and [not] IN lists. You will receive a confirmation, or the error message when failure.

### 6.3.5 Copying a Real-Time Protection DDL Policy

To copy a real-time protection DDL policy, select a policy record in the form Real-Time Protection DDL Policies, Real-Time Protection DDL Policies grid and press the button Copy on the right. The form Copy Real-Time Protection DDL Policy will open.



Set the required fields and press the button Copy.

You will receive a confirmation, or the error message when failure. The new policy will be created with its rules, conditions, [not] IN lists as the original policy and with an Inactive status.

### 6.3.6 Real-Time Protection DDL Policy Status

To change a real-time protection DDL policy status, select a policy record in the form Real-Time Protection DDL Policies, Real-Time Protection DDL Policies grid and press the button Status below on the right. If the change status dialog box is confirmed, the current policy status will be reversed from its current setting. Policy must have at least one active rule for its status to be set as Active. If the policy Audit Option is other than All Users, respective Apply and Exclude lists must have at least one entry.

## 6.4 Real-Time Protection DDL Rules

Real-time protection DDL Rules are defined under policies. To view the real-time protection DDL rules for the selected policy open the form Real-Time Protection DDL Policy. The rules bounded to the policy will be listed in the Policy Rules grid.

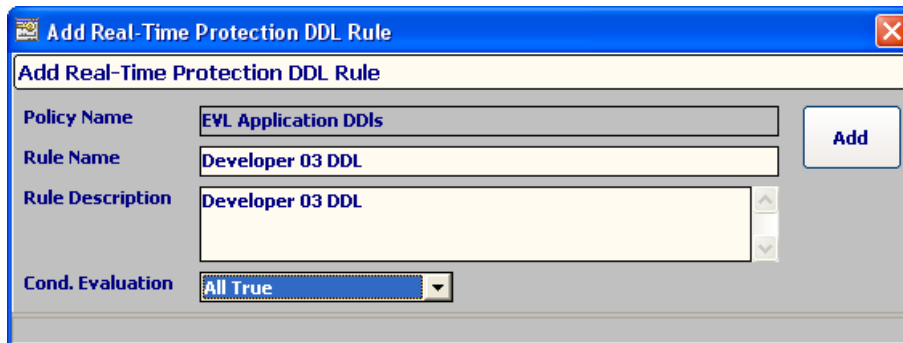
The following are the properties of the RTP DDL rule:

Field Name	Field Description
Rule Code	Unique auto-generated code of the rule within the module.
Rule Name	Name of the rule.
Rule Description	Description of the rule.
Active	Rule status, Active or Inactive.
Condition Evaluation	Rule evaluation mode regarding conditions. Available options: Any True – Rule is True when at least one condition is evaluated True. All True – Rule is True if all conditions are evaluated True. Formula – User defined logical formula built on rules.
Formula	Text of the rule's logical formula built on conditions.

Press the Refresh button to refresh them.

### 6.4.1 Adding a new Real-Time Protection DDL Rule

To create a new real-time protection DDL rule for the selected policy, in the form Real-Time Protection DDL Policy, Policy Rules grid, press the button Add on the right. The form Add Real-Time Protection DDL Rule will open.

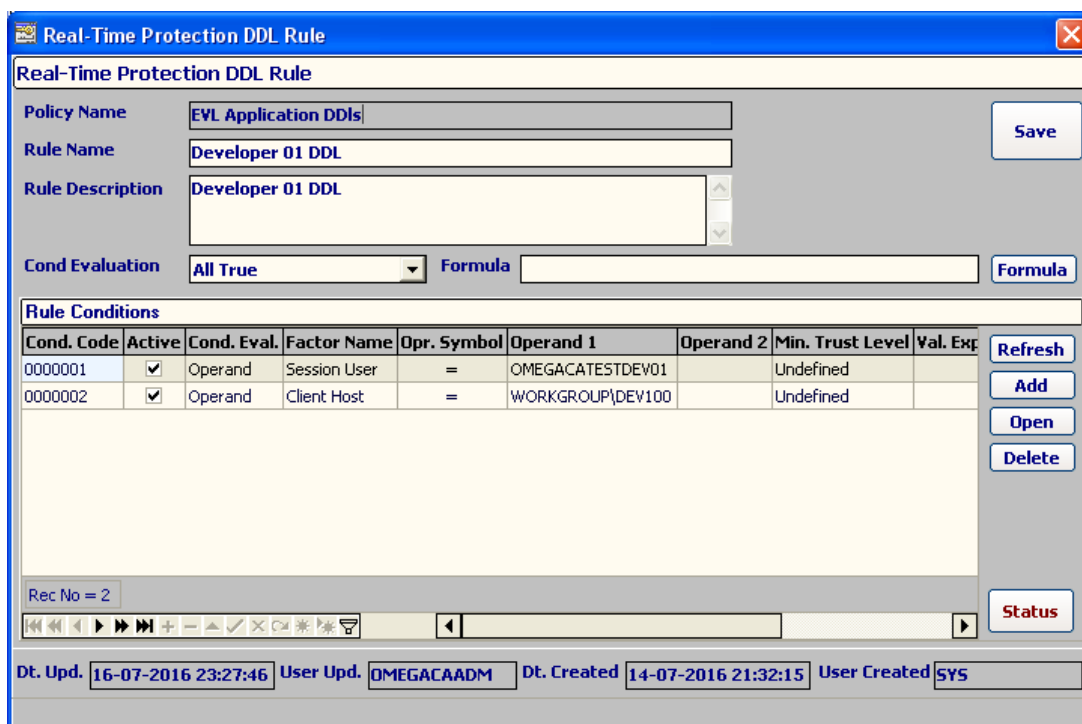


Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new rule will be created with an Inactive status. You can change that later, after adding the conditions.

### 6.4.2 Opening/modifying a Real-Time Protection DDL Rule

To open a real-time protection DDL rule in full details for viewing and modification, select a rule record in the Real-Time Protection DDL Policy, Policy Rules grid and press the button Open on the right. The form Real-Time Protection DDL Rule will open.



**Real-Time Protection DDL Rule**

Policy Name:  Save

Rule Name:

Rule Description:

Cond Evaluation:  Formula:  Formula

Cond. Code	Active	Cond. Eval.	Factor Name	Opr. Symbol	Operand 1	Operand 2	Min. Trust Level	Val. Exp.
0000001	<input checked="" type="checkbox"/>	Operand	Session User	=	OMEGACATESTDEV01		Undefined	
0000002	<input checked="" type="checkbox"/>	Operand	Client Host	=	WORKGROUP\DEV100		Undefined	

Refresh Add Open Delete

Rec No = 2

Dt. Upd. 16-07-2016 23:27:46 User Upd. OMEGACAADM Dt. Created 14-07-2016 21:32:15 User Created SYS Status

To update any rule changes press the button Save. You will receive a confirmation, or the error message when failure.

Press the button Formula to open the rule's formula editor form based on conditions.

### 6.4.3 Deleting a Real-Time Protection DDL Rule

To delete a real-time protection DDL rule, select a rule record in the form Real-Time Protection DDL Policy, Policy Rules grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected rule will be deleted together with its policy cache, conditions and [not] IN lists.

You will receive a confirmation, or the error message when failure.

### 6.4.4 Real-Time Protection DDL Rule Status

To change a real-time protection DDL rule status, select a rule record in the form Real-Time Protection DDL Policy, Policy Rules grid and press the button Status below on the right. If the change status dialog box is confirmed, the current rule status will be reversed from its current setting. Rule must have at least one active condition for its status to be set as Active.

## 6.5 Real-Time Protection DDL Conditions

Real-time protection DDL conditions are defined under policy rules. To view the RTP DDL conditions for the selected rule open the form Real-Time Protection DDL Rule. The conditions bounded to the rule will be listed in the Rule Conditions grid.

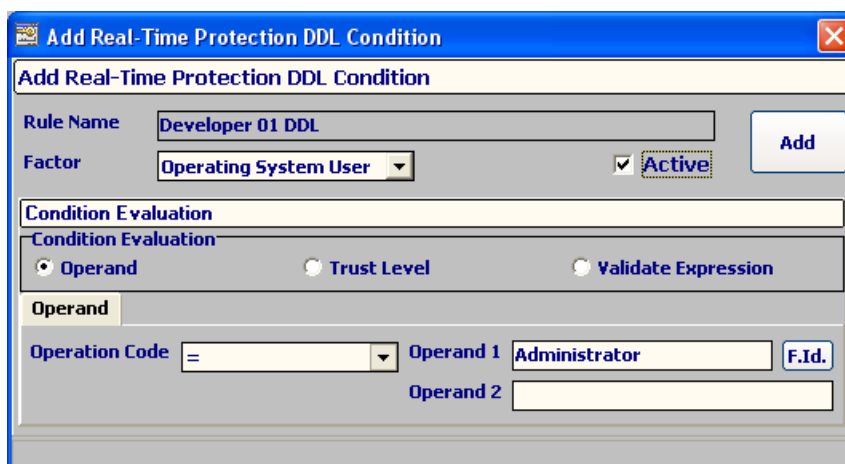
The following are the properties of the RTP DDL condition:

Field Name	Field Description
Condition Code	Unique auto-generated code of the condition within the module.
Active	Condition status, Active or Inactive.
Condition Evaluation	Condition evaluation mode regarding factor. Available options: Operand - Condition is evaluated by comparing the retrieved value of the factor with the operand's value. Trust level - Condition is evaluated by comparing the retrieved value of the factor with the pre-declared Factor's trust level values. Validate Expression – Condition is evaluated as a result of an user-defined database function returning a Boolean result.
Factor	Factor being evaluated.
Operation code	Code the operation type applied to the evaluation of the Factor's retrieved value.
Operand 1	Value of the first operand.
Operand 2	Value of the second operand.
Minimal Trust Level	Minimal required trust level.
Val. Exp. Owner	Validate expression owner.
Val. Exp. Object	Validate expression object name.

Press the Refresh button to refresh them.

### 6.5.1 Adding a new Real-Time Protection DDL Condition

To create a new real-time protection DDL condition, in the form Real-Time Protection DDL Rule, Rule Conditions grid, press the button Add on the right. The form "Add Real-Time Protection DDL Condition" will open.

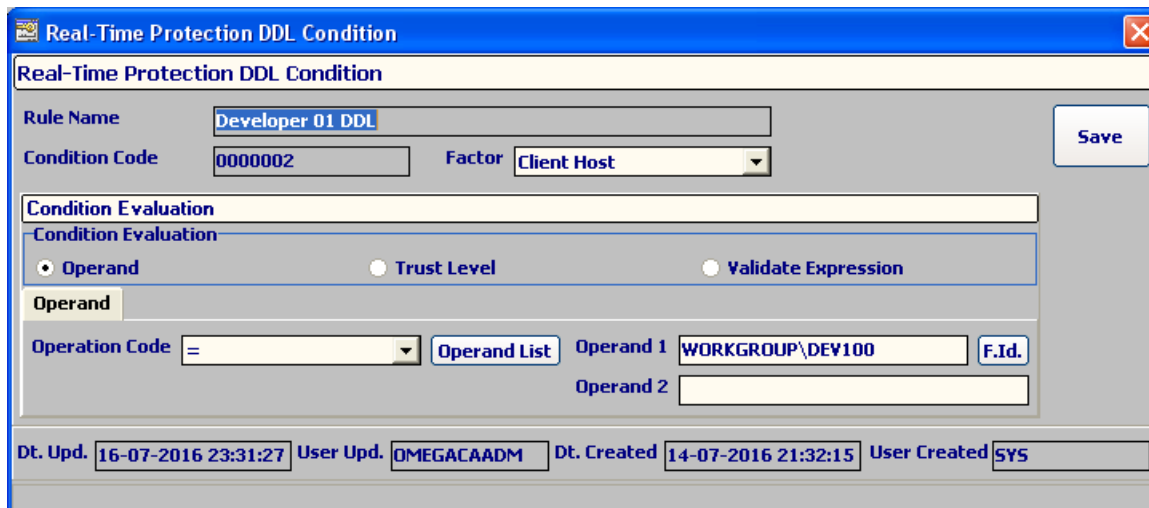


Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. Choosing the condition evaluation mode through the radio-boxes opens respective input fields. The new condition's status can be set on creation, except when condition evaluation Operand and operation code [not] IN that are created as Inactive.

### 6.5.2 Opening/modifying a Real-Time Protection DDL Condition

To open a real-time protection DDL condition in full details for viewing and modification, select a condition record in the form Real-Time Protection DDL Rule, Rule Conditions grid and press the button Open on the right. The form "Real-Time Protection DDL Condition" will open.



To update any condition changes press the button Save. You will receive a confirmation, or the error message when failure. Press the Operand List button to set Operand list when condition evaluation of type Operand and Operation Code [not] IN.

### 6.5.3 Deleting a Real-Time Protection DDL Condition

To delete a real-time protection DDL condition, select a condition record in the form Real-Time Protection DDL Rule, Rules Conditions grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected condition will be deleted together with its policy cache, and [not] IN lists. You will receive a confirmation, or the error message when failure.

### 6.5.4 Real-Time Protection DDL Condition Status

To change a real-time protection DDL condition status, select a condition record in the form Real-Time Protection DDL Rule, Rules Conditions grid and press the button Status below on the right. If the change status dialog box is confirmed, the current condition status will be reversed from its current setting. If condition evaluation is of type Operand and Operation Code is [not] IN, then the condition must have at least one active IN list record for its status to be set as Active.

## **7 CHAPTER 7: Real-Time Protection DML**

### **7.1 How it works**

The Real-Time Protection DML module enforces security compliance and defense on data access and changes into the database. It operates on top of Oracle native fine-grained audit features and implements a special software protection layer that supersedes standard user DML privileges. No users, including privileged accounts and DBAs, can perform DML actions on the Secured Areas without complying with the real-time protection DML policies.

It is based on native fine-grained auditing capabilities of the Oracle's database.

DML actions - SELECTs, INSERTs, UPDATEs and DELETEs in tables and views - are evaluated against Real-Time Protection DML policies implementing Secured Areas to be audited and protected. Secured Areas are defined as groups of Secured Sub-Areas (tables, views, columns and audit options) represented at the policy's rule level. An audit event (trail) will be recorded if the Real-Time Protection DML rule's authorization specific setup (by different authorization types) is met.

Optionally, if the Real-Time Protection DML Rule's Silent Deny setting is disabled, the DML action will be rejected in real time and not allowed to continue.

Multi-factor user authorization permits audit and protection only on successful combination of user & environment context values, be those user, host, OS logon and terminal names, IP addresses, client identifier, program used, time and many more. Column based auditing is an option. Also column condition is available and also no condition at all.

Real-time protection DML trails provide details on user's DML activity into the system. Each real-time protection DML trail is related with one single policy! Automatic fine-grained audit trails management is effective. The DB Audit Trails Purge Job transports the fine-grained audit trails from the Oracle internal structures to the Omega Core Audit.

### **7.2 Real-Time Protection DML Guidelines**

#### **7.2.1 General Guidelines**

The Real-Time Protection DML module is based in the DBMS\_FGA package of the Oracle database fine-grained auditing implementation. Fine-grained auditing is relatively inexpensive, as demonstrated by audit benchmark tests performed by Oracle and other third parties. However in order to minimize any possible performance impact and to keep the Unified Audit Trail from growing big too quickly, narrow the scope of the fine-grained audit by referring to sensitive objects.

Follow these guidelines for minimal performance impact on the system:

- Although auditing is relatively inexpensive, limit the number of audited events as much as possible.
- Evaluate your auditing. Have a clear understanding of your auditing and then devise an appropriate auditing strategy. Avoid unnecessary auditing.
- Audit knowledgeably. Audit the minimum number of user's statements or objects needed to get the targeted information. Balance the sufficient amount of your security information with your ability to store and process it.

Create policies and Secured Areas as groups of rules, each defining a Secured Sub-Area presented by a table or view, plus other audit options. You can use columns to reach column-level authorization, or column conditions to reach a row-level authorization one.



Use the DB\_EXTENDED for the Audit Trail option to get the SQL Bind and SQL Text in the real-time protection DML trail.

**Important Note:**

Fine-grained auditing is available in the Oracle database for cost-based optimizer (CBO) mode only; queries must use the cost-based optimizer (not use RULE hints). The tables and views queried must have been analyzed, least with estimates. If these conditions are not met, the FGA might produce unnecessary audit records; this because audit can occur before the row filtering.

Cost-based optimizer is a default since Oracle Database 10g!

Also FGA cannot be applied to out-of-line columns, such as LOB columns.

For more information on FGA processing please refer to the operational and usage notes of the proprietary's documentation.

### 7.2.2 Silent Deny RTP DML Rules

The RTP DML Rule's Silent Deny mode controls the protective action regarding the compliance of the DMLs being executed on the object covered by the rule. The protective action is the rejection of the user's DML, but when Silent Deny is enabled, the DML will be allowed to execute, although policy evaluation and trailing will continue as configured.

The RTP DML Rule's Silent Deny mode is enabled by default on each new rule. Use the Silent Deny mode for database DML behavior discovery (retaining the audit capability), until you establish secured access paths for DMLs affecting your objects defined through rules. Mind the actions of the application schemas or interfaces!

Normally the Real-Time Protection DML Rule's Silent Deny mode would be used only during the time of initial setup or on emergency. Deactivate this option after you have properly configured Real-Time Protection DML through your policies, so that unauthorized DMLs are not allowed to continue!

The Silent Deny option is managed for each RTP DML Rule, Silent Deny Checkbox in DML Rule form.

### 7.3 Existing Oracle Fine-Grained Audit policies

Existing fine-grained audit policies might have been created in your database, prior to Omega Core Audit installation. You must either:

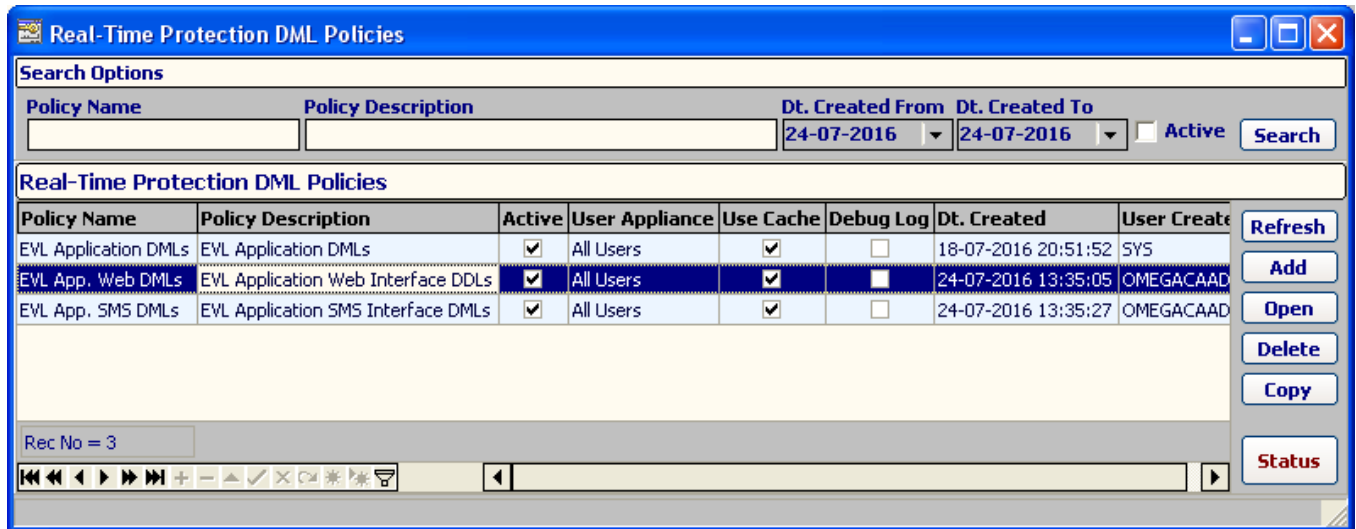
1. Drop them with the Oracle supplied package's procedure DBMS\_FGA.DROP\_POLICY and recreate them via the Omega Core Audit Real-Time Protection DML module.
2. Leave them as they are, unified audit trails generated by them will have the "FGA Policy Name" field set to UNDEFINED during the DB Audit Trails Purge Job run.

**Note:**

1. To check for existing fine-grained audit policies, open the form "Fine-Grained Audits" later described in this chapter in the "Database Fine-Grained Audits Interaction" topic.
2. For existing fine-grained audit trail records, FGA\_LOG\$, it is recommended that these trails are purged prior to installing Omega Core Audit. However, you can still purge these trails to the Omega Core Audit repository; see the alternative "2." above.

## 7.4 Real-Time Protection DML Policies

Real-time protection DML policies enforce and formalize security compliance policies on user's DML actions into the database. To view the policies, in the Application's main menu Audit Policies, tab RTP DML click the menu button Policies. This will open the Real-Time Protection DML Policies form.



Policy Name	Policy Description	Active	User Appliance	Use Cache	Debug Log	Dt. Created	User Create
EVL Application DMLs	EVL Application DMLs	<input checked="" type="checkbox"/>	All Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	18-07-2016 20:51:52	SYS
EVL App. Web DMLs	EVL Application Web Interface DDLs	<input checked="" type="checkbox"/>	All Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	24-07-2016 13:35:05	OMEGACAAD
EVL App. SMS DMLs	EVL Application SMS Interface DMLs	<input checked="" type="checkbox"/>	All Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	24-07-2016 13:35:27	OMEGACAAD

The following are the properties of the RTP DML policy:

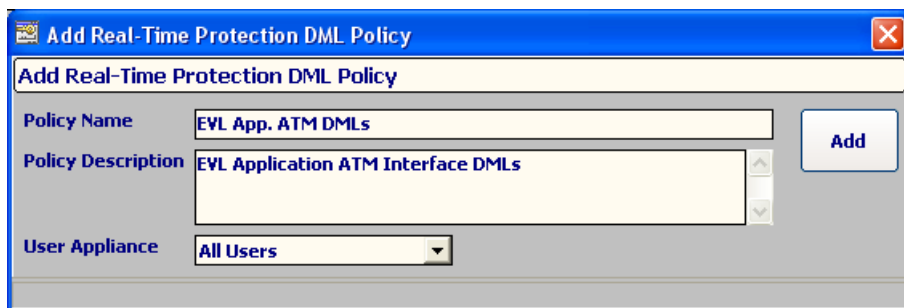
Field Name	Field Description
Policy Name	Unique Name of the policy within the module.
Policy Description	Description of the policy.
Active	Policy Active or Inactive.
User Appliance	Policy appliance regarding database users. Available options: All Users – Policy is applied to all users. Users Apply – Policy is applied only to users in the Users Apply List. Users Exclude – Policy is not applied to users in the Users Exclude List.
Use Cache	Use of Policy Cache on evaluation. Available options: Checked – Cache is enabled for policy, recommended value and default on create. Unchecked – Cache is not enabled for policy, non-recommended value.
Debug Log	A Debug Log is created when policy is evaluated. Available options: Checked – Debug log is enabled for policy, non-recommended value. Unchecked – Debug log is not enabled for policy, recommended value and default on create.

Enter the desired options and press the button Search on the right. The result will be listed in the Real-Time Protection DML Policies grid.

Press the Refresh button to refresh them.

### 7.4.1 Adding a new Real-Time Protection DML Policy

To create a new real-time protection DML policy, in the form Real-Time Protection DML Policies, Real-Time Protection DML Policies grid, press the button Add on the right. The form Add Real-Time Protection DML Policy will open.



**Add Real-Time Protection DML Policy**

Policy Name:

Policy Description:

User Appliance:

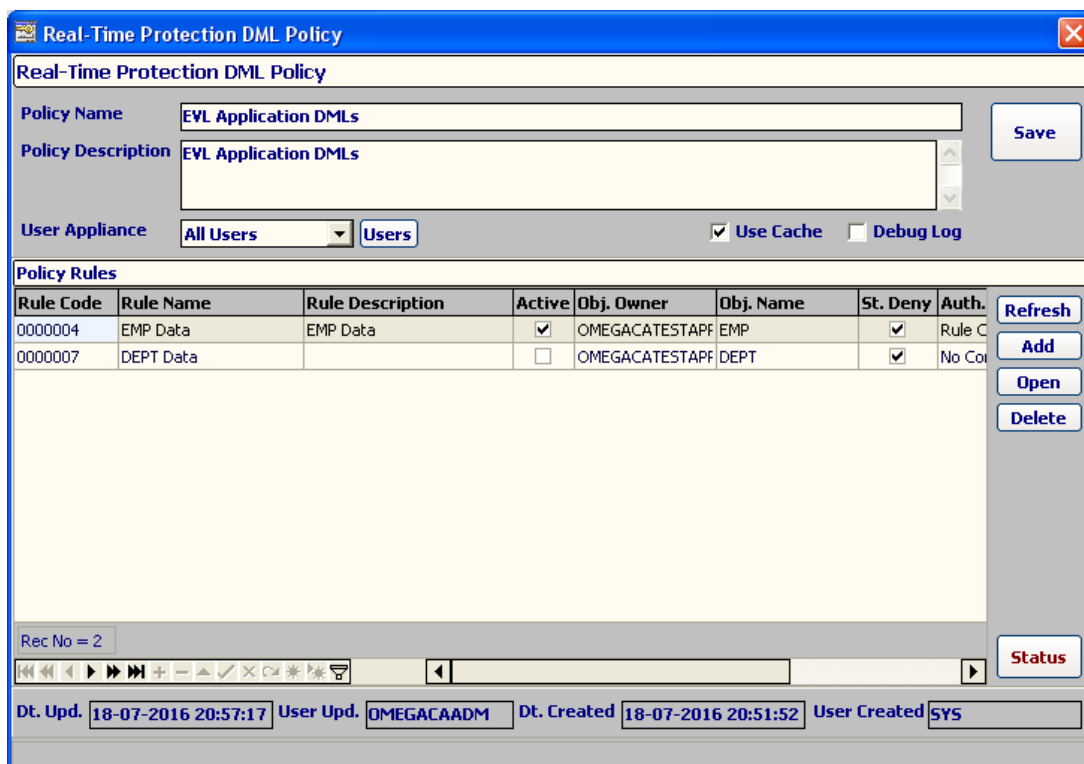
**Add**

Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new policy will be created with an Inactive status. You can change that later, after adding the rules.

### 7.4.2 Opening/modifying a Real-Time Protection DML Policy

To open a real-time protection DML policy in full details for viewing and modification, select a policy record in the form Real-Time Protection DML Policies, Real-Time Protection DML Policies grid and press the button Open on the right. The form Real-Time Protection DML Policy will open.



**Real-Time Protection DML Policy**

Policy Name:

Policy Description:

User Appliance:  **Users**

☒ Use Cache ☐ Debug Log

**Policy Rules**

Rule Code	Rule Name	Rule Description	Active	Obj. Owner	Obj. Name	St. Deny	Auth.
0000004	EMP Data	EMP Data	<input checked="" type="checkbox"/>	OMEGACATESTAPF	EMP	<input checked="" type="checkbox"/>	Rule C
0000007	DEPT Data		<input type="checkbox"/>	OMEGACATESTAPF	DEPT	<input checked="" type="checkbox"/>	No Co

Rec No = 2

**Refresh** **Add** **Open** **Delete** **Status**

Dt. Upd.  User Upd.  Dt. Created  User Created

To update any policy changes press the button Save. You will receive a confirmation, or the error message when failure. Press the button Del. Cache to manually clear the real-time protection DML cache for this policy.

Press the button Formula to open the policy's formula editor form. Press the button Users to open the user appliance/exclusion form.

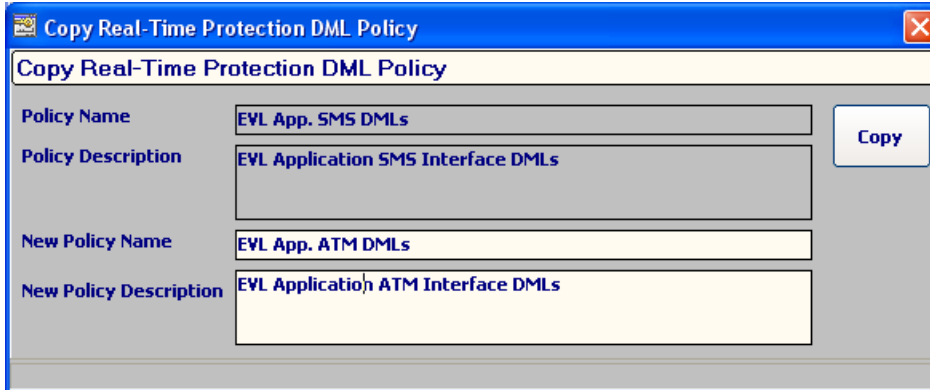
### 7.4.3 Deleting a Real-Time Protection DML Policy

To delete a real-time protection DDL policy, select a policy record in the form Real-Time Protection DDL Policies, Real-Time Protection DDL Policies grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected policy will be deleted together with its cache, rules, conditions and [not] IN lists.

You will receive a confirmation, or the error message when failure.

#### 7.4.4 Copying a Real-Time Protection DML Policy

To copy a real-time protection DML policy, select a policy record in the form Real-Time Protection DML Policies, Real-Time Protection DML Policies grid and press the button Copy on the right. The form Copy Real-Time Protection DML Policy will open.



Set the required fields and press the button Copy.

You will receive a confirmation, or the error message when failure. The new policy will be created with its rules, conditions, [not] IN lists as the original policy and with an Inactive status.

#### Note:

Whenever any possible error happens during a DML policy copy, check always in the form Fine-Grained Audit Policies to see if any (anyway Inactive) Audit Policy has been created in the middle of the failed copy. This may happen because it is not possible to hold transactional behavior between multiple Omega CA Repository actions and multiple respective FGA commands (which as DDLs being do implicitly commit).

#### 7.4.5 Real-Time Protection DML Policy Status

To change a real-time protection DML policy status, select a policy record in the form Real-Time Protection DML Policies, Real-Time Protection DML Policies grid and press the button Status below on the right. If the change status dialog box is confirmed, the current policy status will be reversed from its current setting. Policy must have at least one active rule for its status to be set as Active. If the policy Audit Option is other than All Users, respective Apply and Exclude lists must have at least one entry.

If the status of the policy will be Inactive, then all policy's rules will be disabled!

## 7.5 Real-Time Protection DML Rules

Real-time protection DML Rules are defined under policies. To view the real-time protection DML rules for the selected policy open the form Real-Time Protection DML Policy. The rules bounded to the policy will be listed in the Policy Rules grid.

The following are the properties of the RTP DML rule:

Field Name	Field Description
Rule Code	Unique auto-generated code of the rule within the module.
Rule Name	Name of the rule.
Rule Description	Description of the rule.
Active	Rule status, Active or Inactive.
Silent Deny	Action rejected or silent when audit triggered. Available options: Checked – Silent mode is enabled, user's action is allowed to continue. This is the default value in rule creation. Unchecked – non-Silent mode, user's action is rejected, an error message indicating non-authorization is raised.
Authorization Type	Rule's authorization type. Available options: No Condition – No condition is evaluated, default non-authorization, audit event is always triggered. Rule Conditions – Rule is evaluated by its conditions and audit event is triggered if TRUE. Column Condition – Rule is evaluated by a condition set in its object column(s), kind of SALARY > 3200, audit event is triggered if TRUE.
Condition Evaluation	Rule evaluation mode regarding conditions. Effective only for Authorization Type of Rule Conditions. Available options: Any True – Rule is True when at least one condition is evaluated True. All True – Rule is True if all conditions are evaluated True. Formula – User defined logical formula built on conditions.
Formula	Text of the rule's logical formula built on conditions.
<b>Secured sub-Area</b>	
Object Owner	Protected sub-area's object owner.
Object Name	Protected sub-area's object name.
Statements	Protected sub-area's DML actions, Select, Insert, Update, Delete.
Audit Trail	Audit trail option. Available options: DB – no SQL Bind and Text. DB_EXTENDED – with SQL Bind and Text, recommended value.
Object Columns	The columns to be checked for access. When NULL (no columns selected, causes audit if any column is accessed or affected.
Column Options	Audit firing by query's columns. Available options: ANY_COLUMNS - audit event is generated when the query references any column specified in the Object Columns. ALL_COLUMNS - audit event is generated when the query references all columns specified in the Object Columns.

Press the Refresh button to refresh them.

### Important Note:

Changes in Real Time Protection DML Rules take immediate effect.

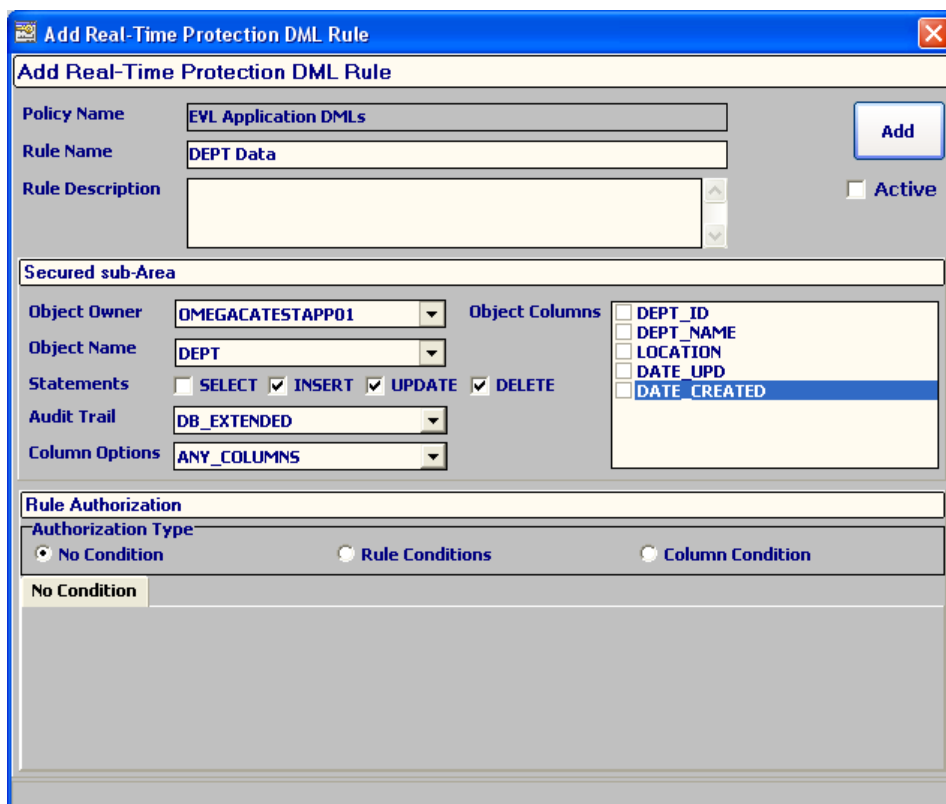
## Rule's authorization type:

For No Condition the audit event will always fire. If the Authorization Type is set to Rule Conditions, the rule's conditions will be processed to evaluate the rule, audit event will fire if rule evaluates TRUE. If Column Conditions is set and condition is met, the audit event will fire.

For Authorization Types of Column Conditions only the setting All Users of policy's Users Appliance is supported.

### 7.5.1 Adding a new Real-Time Protection DML Rule

To create a new real-time protection DML rule for the selected policy, in the form Real-Time Protection DML Policy, Policy Rules grid, press the button Add on the right. The form Add Real-Time Protection DML Rule will open.



Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. The new RTP DML rule's status can be set on creation.

### 7.5.2 Opening/modifying a Real-Time Protection DML Rule

To open a real-time protection DML rule in full details for viewing and modification, select a rule record in the Real-Time Protection DML Policy, Policy Rules grid and press the button Open on the right. The form Real-Time Protection DML Rule will open.

To update any rule changes press the button Save.  
You will receive a confirmation, or the error message when failure. Press the button Formula to open the rule's formula editor form based on conditions.

To delete a real-time protection DML rule, select a rule record in the form Real-Time Protection DML Policy, Policy Rules grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected rule will be deleted together with its policy cache, conditions and [not] IN lists. You will receive a confirmation, or the error message when failure.

To change a real-time protection DML rule status, select a rule record in the form Real-Time Protection DML Policy, Policy Rules grid and press the button Status below on the right. If the change status dialog box is confirmed, the current rule status will be reversed from its current setting. Rule must have at least one active condition for its status to be set as Active.

Setting a policy rule status effectively to Active or Inactive sets the database fine-grained policy's status related to it to the same; property is available in Oracle database fine-grained policies.

## 7.6 Real-Time-Protection DML Conditions

Real-time protection DML conditions are defined under policy rules. To view the real-time protection DML conditions for the selected rule open the form Real-Time Protection DML Rule. The conditions bounded to the rule will be listed in the Rule Conditions grid.

The following are the properties of the RTP DML condition:

Field Name	Field Description
Condition Code	Unique auto-generated code of the condition within the module.
Active	Condition status, Active or Inactive.
Condition Evaluation	Condition evaluation mode regarding factor. Available options: Operand - Condition is evaluated by comparing the retrieved value of the factor with the operand's value. Trust level - Condition is evaluated by comparing the retrieved value of the factor with the pre-declared Factor's trust level values. Validate Expression – Condition is evaluated as a result of an user-defined database function returning a Boolean result.
Factor	Factor being evaluated.
Operation code	Code the operation type applied to the evaluation of the Factor's retrieved value.
Operand 1	Value of the first operand.
Operand 2	Value of the second operand
Minimal Trust Level	Minimal required trust level.
Val. Exp. Owner	Validate expression owner.
Val. Exp. Object	Validate expression object name.

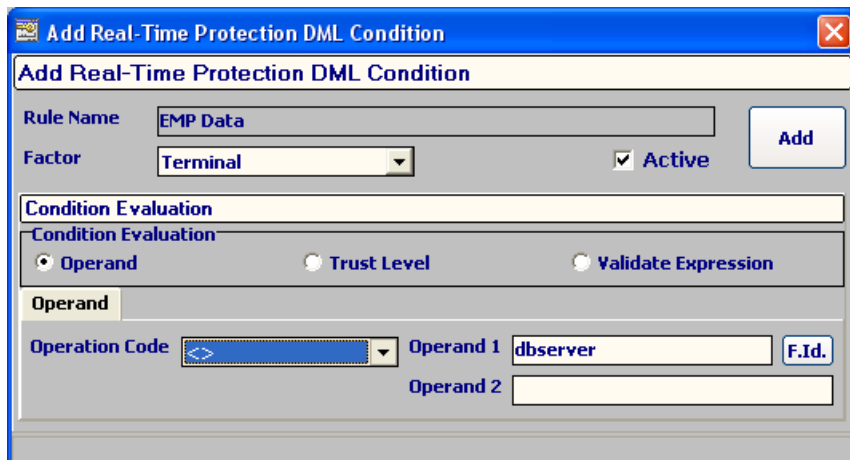
Press the Refresh button to refresh them.

### Note:

IN RTP DML, Conditions are effective only for RTP DML Rules with Authorization Type of Rule Conditions!

### 7.6.1 Adding a new Real-Time Protection DML Condition

To create a new real-time protection DML condition, in the form Real-Time Protection DML Rule, Rule Conditions grid, press the button Add on the right. The form "Add Real-Time Protection DML Condition" will open.



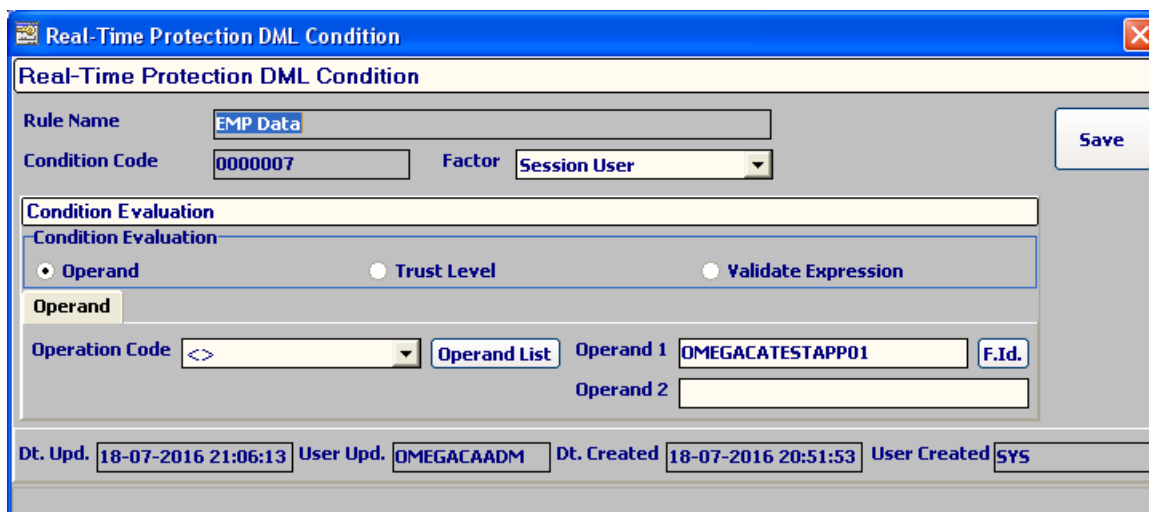


Set the required fields and press the button Add.

You will receive a confirmation, or the error message when failure. Choosing the condition evaluation mode through the radio-boxes opens respective input fields. The new condition's status can be set on creation, except when condition evaluation Operand and operation code [not] IN that are created as Inactive.

### 7.6.2 Opening/modifying a Real-Time Protection DML Condition

To open a real-time protection DML condition in full details for viewing and modification, select a condition record in the form Real-Time Protection DML Rule, Rule Conditions grid and press the button Open on the right. The form "Real-Time Protection DML Condition" will open.



To update any condition changes press the button Save. You will receive a confirmation, or the error message when failure. Press the Operand List button to set Operand list when condition evaluation of type Operand and Operation Code [not] IN.

### 7.6.3 Deleting a Real-Time Protection DML Condition

To delete a real-time protection DML condition, select a condition record in the form Real-Time Protection DML Rule, Rules Conditions grid and press the button Delete on the right. If the delete dialog box is confirmed, the selected condition will be deleted together with its policy cache, and [not] IN lists.

You will receive a confirmation, or the error message when failure.

### 7.6.4 Real-Time Protection DML Condition Status

To change a real-time protection DML condition status, select a condition record in the form Real-Time Protection DML Rule, Rules Conditions grid and press the button Status below on the right. If the change status dialog box is confirmed, the current condition status will be reversed from its current setting. If condition evaluation is of type Operand and Operation Code is [not] IN, then the condition must have at least one active IN list record for its status to be set as Active.

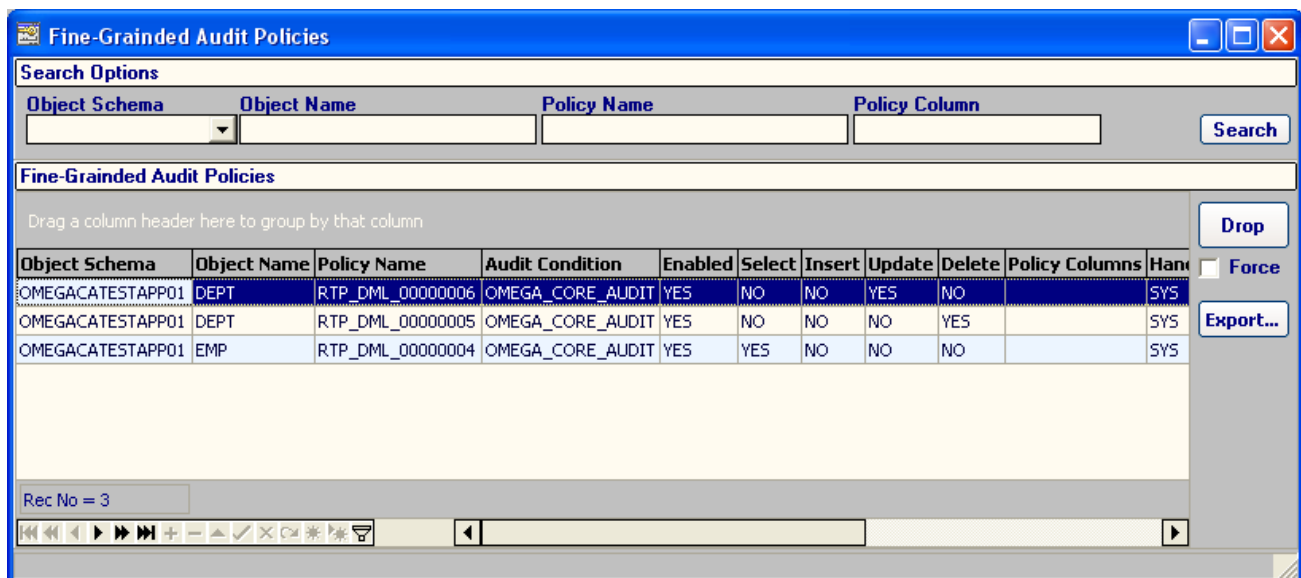
## 7.7 Database Fine-Grained Audits Interaction

Omega Core Audit's Real-Time Protection DML module automates and visually handles the Oracle database' fine-grained audit functionalities. This is implemented at the policy's rule level, for tables, views, columns and other audit settings. Management of database fine-grained audits is performed automatically at policy rule's create, update, delete and status management. Direct database commands for fine-grained auditing are processed and executed by the Omega engine and synchronization is held between repository and database fine-grained audits. Relationship between policy rules to the oracle database fine-grained audits is one to one; the rule's code is the database fine-grained audit policy name.

The Omega Core Audit interface will alert you when opening a DML Rule which is not bounded to a database fine-grained policy. Ideally you are not supposed to see this, but existence of an orphan DML Rule is an indicator of fine-grained audit activity outside Omega Core Audit or an inconsistency of the later.

### 7.7.1 Database Fine-Grained Audit Policies

To view the database' fine-grained audit policies, as they are displayed in the Oracle view DBA\_AUDIT\_POLICIES, in the Application's main menu Audit Policies tab, Oracle Audit Setting group, click on the Fine-Grained menu button. The form Fine-Grained Audit Policies will open.



Object Schema	Object Name	Policy Name	Audit Condition	Enabled	Select	Insert	Update	Delete	Policy Columns	Handled
OMEGACATESTAPP01	DEPT	RTP_DML_00000006	OMEGA_CORE_AUDIT	YES	NO	NO	YES	NO		SYS
OMEGACATESTAPP01	DEPT	RTP_DML_00000005	OMEGA_CORE_AUDIT	YES	NO	NO	NO	YES		SYS
OMEGACATESTAPP01	EMP	RTP_DML_00000004	OMEGA_CORE_AUDIT	YES	YES	NO	NO	NO		SYS

Enter the desired options and press the button Search on the right. The result will be listed in the Fine-Grained Audit Policies grid.

You can drop the selected database fine-grained audit policy with the NoAudit button. Ideally you are not supposed to use this feature, but you can use it only for any possible database orphan fine-grained audit, which for any reason is not synchronized to the Omega Core Audit repository of real-time protection DML rules!

If the database fine-grained audit policy you are trying to drop is bound to any Omega Core Audit Real-Time Protection DML rule record, you will receive an indicating error. You can still perform the drop if you choose the Force option.

Management of the fine-grained auditing is done through the Omega Core Audit Real-Time Protection DML module at rule level. Existence of database orphan fine-grained audit policies is an indicator of audit activity outside Omega Core Audit or an inconsistency of the later.

### **7.7.2 Real-Time Protection DML Unified Trail Mapping**

The Oracle database offers no Return Code on its fine-grained audit trails. The audit mechanism is triggered only after the command has passed all checks (like correct syntax, object availability, privileges...). In the meantime it does stamp the FGA Policy Name, which is created by (and leads to) the Real-Time Protection DML Rule.

Omega Core Audit features:

#### **RTP DML Return Code Mapping**

The mapping (setting) of right Return Code field for Unified Audit Trail records of Policy Type RTP DML. When feature is enables, if the action was protected (reversed) by the RTP DML Policy (Rule) then an error of -20010 will be returned to indicated failure, the Omega Core Audit's protection, in case DML Rule Silent Deny is disabled. In other cases (DML Rule in Silent Deny, or feature disabled) the Return Code will have a value of 0.

#### **RTP DML Policy Mapping**

The mapping of the Unified Audit Trail records of Policy Type Real-Time Protection DML, to the causing Real-Time Protection DML Policy. When feature is enabled, the Trail Evaluation field of the Unified Audit Trail will contain the text formatted information of the policy that caused this trail record, otherwise will be empty.

Details on the operation of these features are explained more in depth in the Chapter "System Administration", topic "DB Audit Trails Purge".

## 8 CHAPTER 8: Security Management

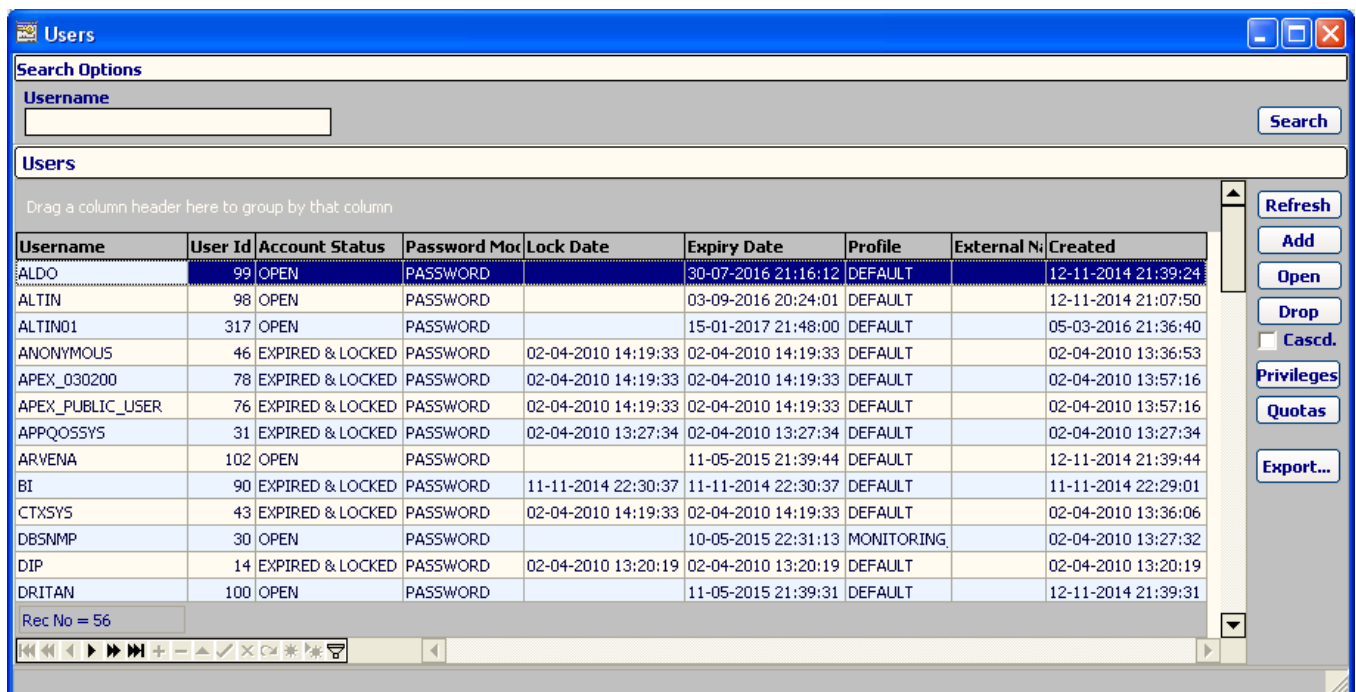
### 8.1 Security Management Operation and Features

The Security module handles the management of database security related operations, enabling the Account Manager to easily and quickly complete his tasks.

It operates on database users, roles and also system, objects and role privileges.

### 8.2 Database Users

To view the database users in the Application's main menu, Security tab, Users & Roles group click the Uses menu button. This will open the form Users. Optionally enter a username and press the button Search on the right. The result will be listed in the Users grid.



Username	User Id	Account Status	Password Mode	Lock Date	Expiry Date	Profile	External Name	Created
ALDO	99	OPEN	PASSWORD		30-07-2016 21:16:12	DEFAULT		12-11-2014 21:39:24
ALTIN	98	OPEN	PASSWORD		03-09-2016 20:24:01	DEFAULT		12-11-2014 21:07:50
ALTIN01	317	OPEN	PASSWORD		15-01-2017 21:48:00	DEFAULT		05-03-2016 21:36:40
ANONYMOUS	46	EXPIRED & LOCKED	PASSWORD	02-04-2010 14:19:33	02-04-2010 14:19:33	DEFAULT		02-04-2010 13:36:53
APEX_030200	78	EXPIRED & LOCKED	PASSWORD	02-04-2010 14:19:33	02-04-2010 14:19:33	DEFAULT		02-04-2010 13:57:16
APEX_PUBLIC_USER	76	EXPIRED & LOCKED	PASSWORD	02-04-2010 14:19:33	02-04-2010 14:19:33	DEFAULT		02-04-2010 13:57:16
APPQOSSYS	31	EXPIRED & LOCKED	PASSWORD	02-04-2010 13:27:34	02-04-2010 13:27:34	DEFAULT		02-04-2010 13:27:34
ARVENA	102	OPEN	PASSWORD		11-05-2015 21:39:44	DEFAULT		12-11-2014 21:39:44
BI	90	EXPIRED & LOCKED	PASSWORD	11-11-2014 22:30:37	11-11-2014 22:30:37	DEFAULT		11-11-2014 22:29:01
CTXSYS	43	EXPIRED & LOCKED	PASSWORD	02-04-2010 14:19:33	02-04-2010 14:19:33	DEFAULT		02-04-2010 13:36:06
DBSNMP	30	OPEN	PASSWORD		10-05-2015 22:31:13	MONITORING		02-04-2010 13:27:32
DIP	14	EXPIRED & LOCKED	PASSWORD	02-04-2010 13:20:19	02-04-2010 13:20:19	DEFAULT		02-04-2010 13:20:19
DRITAN	100	OPEN	PASSWORD		11-05-2015 21:39:31	DEFAULT		12-11-2014 21:39:31

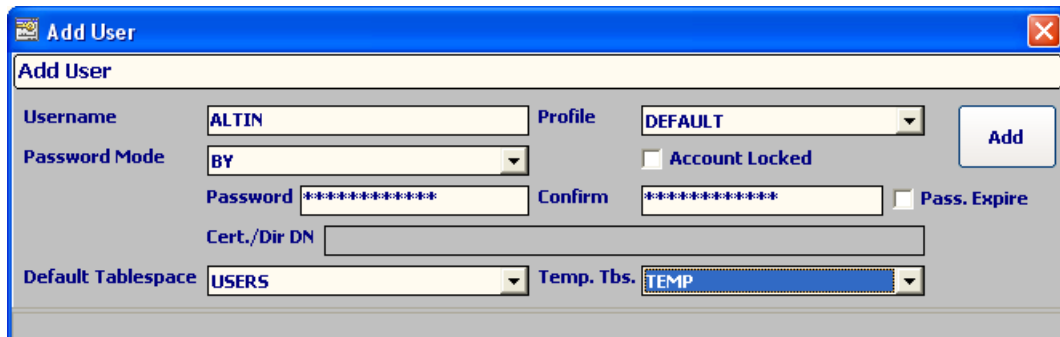
The following are the properties of the database users:

Field Name	Field Description
Username	Name of the database user.
User Id	Numeric ID of the user.
Account Status	Status of the user's account.
Password Mode	User's password mode.
Lock Date	Date of last account lock.
Expiry Date	Date of account expiration.
Profile	Account's profile.
External Name	User external name.
Created	Date creation of the account

Press the Refresh button to refresh them.

### 8.2.1 Adding a new Database User

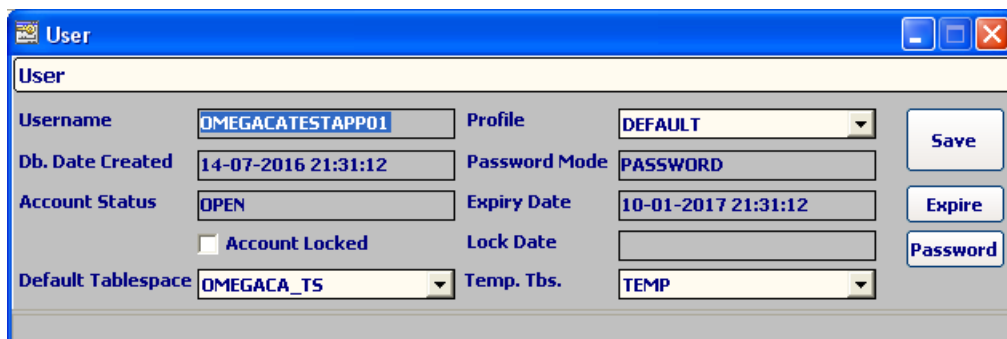
To create a new database user, in the form Users, Users grid, press the button Add on the right. The form Add User will open.



Set the required fields and press the button Add. You will receive a confirmation, or the error message when failure.

### 8.2.2 Opening/modifying a Database User

To open a database user in full details for viewing and modification, select a user record in the form Users, Users grid and press the button Open on the right. The form "User" will open.



To update any user changes press the button Save.

You will receive a confirmation, or the error message when failure. Press the Expire button to expire the user's password. Press the "Password" button to set a new password for the user.

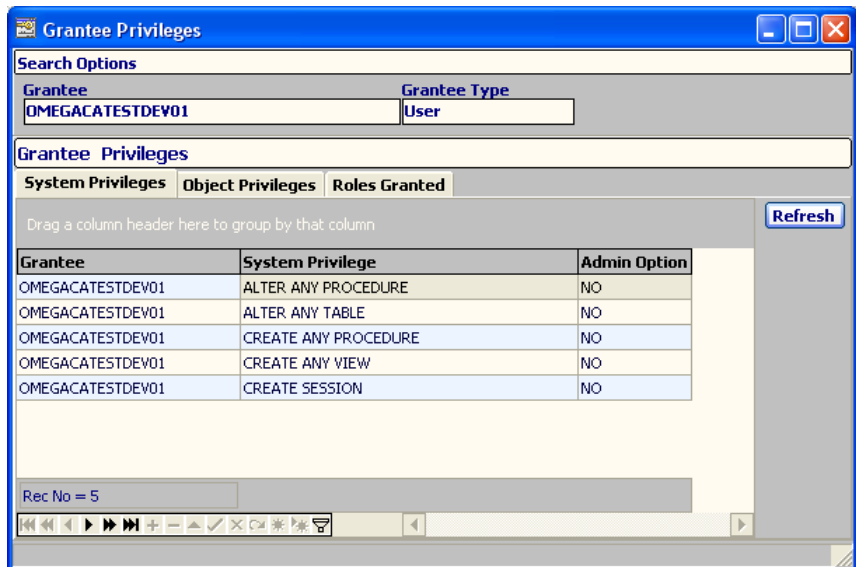
### 8.2.3 Dropping a Database User

To drop a database user, select a user record in the form Users, Users grid and press the button Drop on the right. If the drop dialog box is confirmed, the selected user will be dropped.

You will receive a confirmation, or the error message when failure. If the user owns any object, check the checkbox "Cascd." to drop the user.

## 8.2.4 Database User's Privileges

To view the database user's privileges, select a user record in the form Users, Users grid and press the button Privileges on the right. The form "Grantee Privileges" will open.



**Grantee Privileges**

Search Options

Grantee: OMEGACATESTDEV01      Grantee Type: User

Grantee Privileges

System Privileges    Object Privileges    Roles Granted

Drag a column header here to group by that column

Grantee	System Privilege	Admin Option
OMEGACATESTDEV01	ALTER ANY PROCEDURE	NO
OMEGACATESTDEV01	ALTER ANY TABLE	NO
OMEGACATESTDEV01	CREATE ANY PROCEDURE	NO
OMEGACATESTDEV01	CREATE ANY VIEW	NO
OMEGACATESTDEV01	CREATE SESSION	NO

Rec No = 5

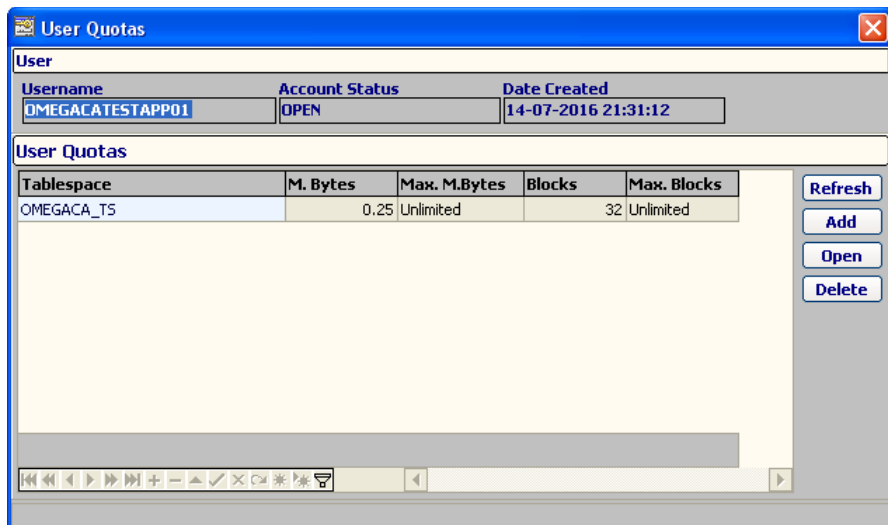
Refresh

Here you can view the selected users:

- System privileges.
- Object privileges.
- Role privileges.

## 8.2.5 Database User's Tablespace Quotas

To manage user's tablespace quotas, select a user record in the form Users, Users grid and press the button Quotas on the right. The form "User Quotas" will open.



**User Quotas**

User

Username: OMEGACATESTAPP01      Account Status: OPEN      Date Created: 14-07-2016 21:31:12

User Quotas

Tablespace	M. Bytes	Max. M.Bytes	Blocks	Max. Blocks
OMEGACA_TS	0.25	Unlimited	32	Unlimited

Refresh

Add

Open

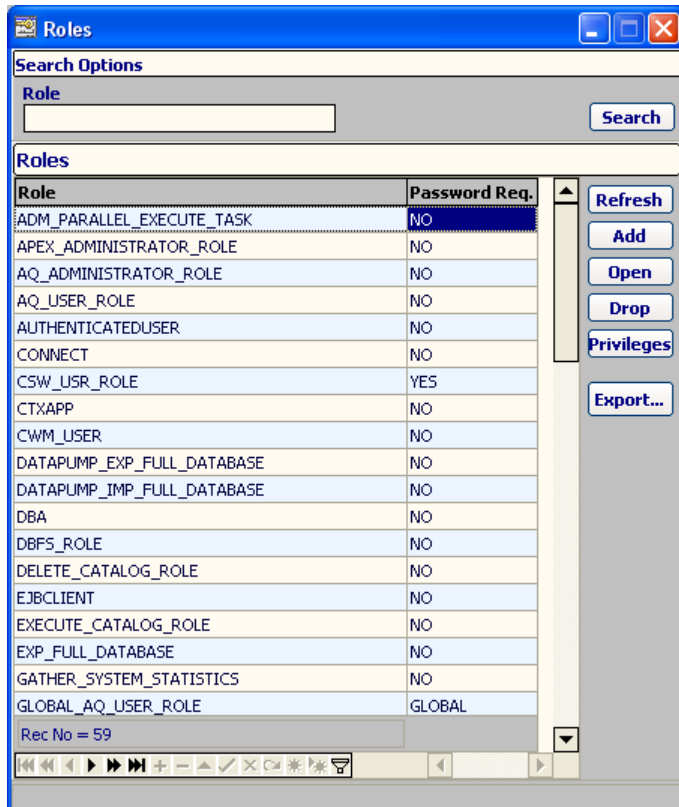
Delete

Here you can view selected user's tablespace quotas. Press the Refresh button on the right to refresh them. Use the other buttons on the right of the User Quota grid to the respective forms to add and modify or to drop user's selected tablespace quota.



### 8.3 Database Roles

To view the database roles Application's main menu, Security tab, Users & Roles group click the Roles menu button. This will open the form Roles. Optionally enter a role and press the button Search on the right. The result will be listed in the Roles grid.



Role	Password Req.
ADM_PARALLEL_EXECUTE_TASK	NO
APEX_ADMINISTRATOR_ROLE	NO
AQ_ADMINISTRATOR_ROLE	NO
AQ_USER_ROLE	NO
AUTHENTICATEDUSER	NO
CONNECT	NO
CSW_USR_ROLE	YES
CTXAPP	NO
CWM_USER	NO
DATAPUMP_EXP_FULL_DATABASE	NO
DATAPUMP_IMP_FULL_DATABASE	NO
DBA	NO
DBFS_ROLE	NO
DELETE_CATALOG_ROLE	NO
EJBCLIENT	NO
EXECUTE_CATALOG_ROLE	NO
EXP_FULL_DATABASE	NO
GATHER_SYSTEM_STATISTICS	NO
GLOBAL_AQ_USER_ROLE	GLOBAL

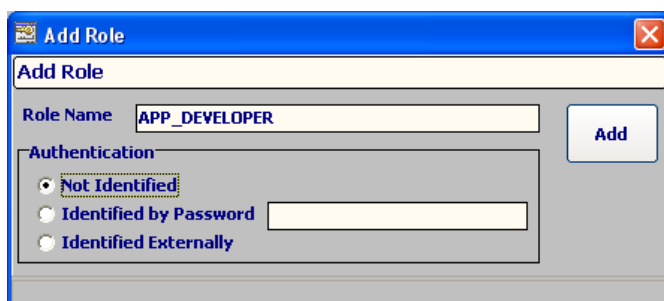
The following are the properties of the database roles:

Field Name	Field Description
Role	Name of the database role.
Password Req.	Database role requires identification by password to be enabled.

Press the Refresh button to refresh them.

#### 8.3.1 Adding a new Database Role

To create a new database role, in the form Roles, Roles grid, press the button Add on the right. The form Add Role will open.

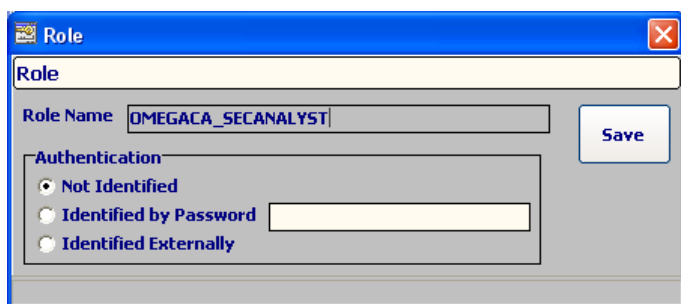




Set the required fields and press the button Add.  
You will receive a confirmation, or the error message when failure.

### 8.3.2 Opening/modifying a Database Role

To open a database role in full details for viewing and modification, select a role record in the form Roles, Roles grid and press the button Open on the right. The form "Role" will open.



To update any role changes press the button Save.  
You will receive a confirmation, or the error message when failure.

### 8.3.3 Dropping a Database Role

To drop a database role, select a role record in the form Roles, Roles grid and press the button Drop on the right. If the drop dialog box is confirmed, the selected role will be dropped.

You will receive a confirmation, or the error message when failure.

### 8.3.4 Database Role's Privileges

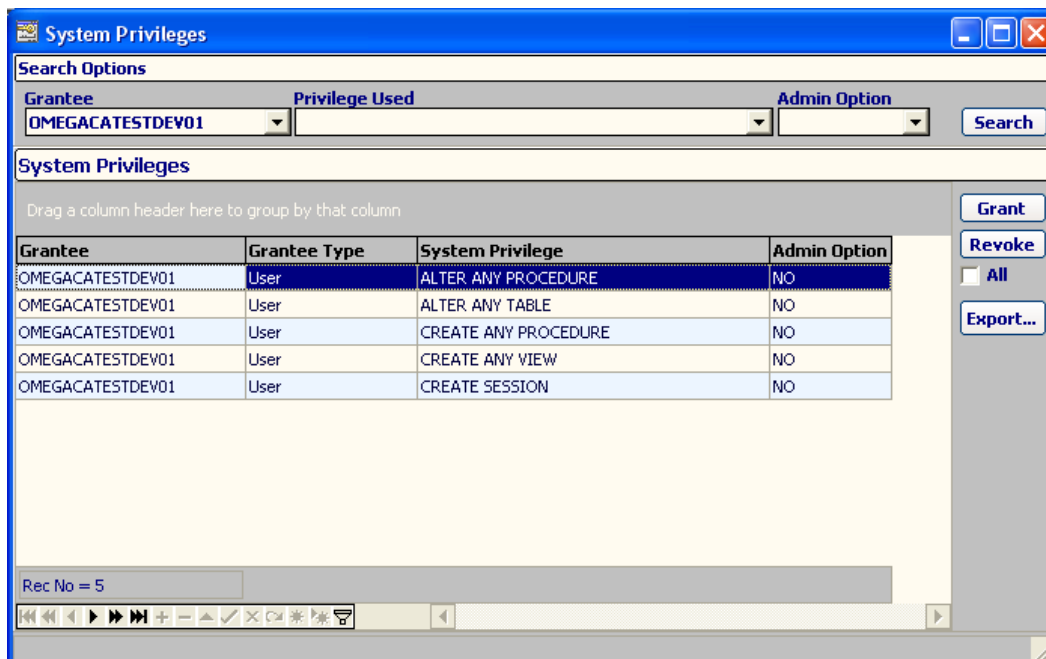
To view the database role's privileges, select a role record in the form Roles, Roles grid and press the button Privileges on the right. The form "Grantee Privileges" will open, where you can view role's system, object and role privileges.

Here you can view the selected roles:

- System privileges.
- Object privileges.
- Role privileges.

## 8.4 System Privileges

To view the system privileges in the Application's main menu, Security tab, Privileges group click the System Privileges menu button. This will open the form System Privileges. Enter the desired options and press the button Search on the right. The result will be listed in the System Privileges grid.



Grantee	Grantee Type	System Privilege	Admin Option
OMEGACATESTDEV01	User	ALTER ANY PROCEDURE	NO
OMEGACATESTDEV01	User	ALTER ANY TABLE	NO
OMEGACATESTDEV01	User	CREATE ANY PROCEDURE	NO
OMEGACATESTDEV01	User	CREATE ANY VIEW	NO
OMEGACATESTDEV01	User	CREATE SESSION	NO

The following are the properties of the system privileges:

Field Name	Field Description
Grantee	User or role granted the privilege.
Grantee Type	Grantee Type (user or role).
System Privilege	System Privilege.
Admin Option	Granted privilege is grantable by the grantee.

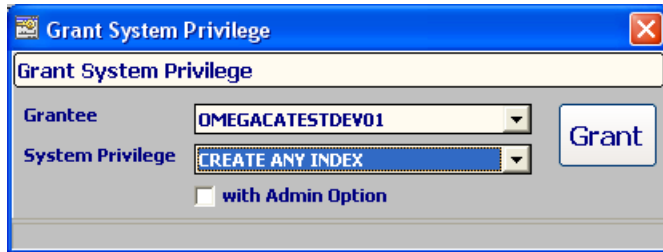
### Important Note:

System Privileges grants and revokes take immediate effect.

Press the Refresh button to refresh them.

### 8.4.1 Granting a system privilege

To grant a system privilege, in the form System Privileges, System Privileges grid, press the button Grant on the right. The form "Grant System Privilege" will open.



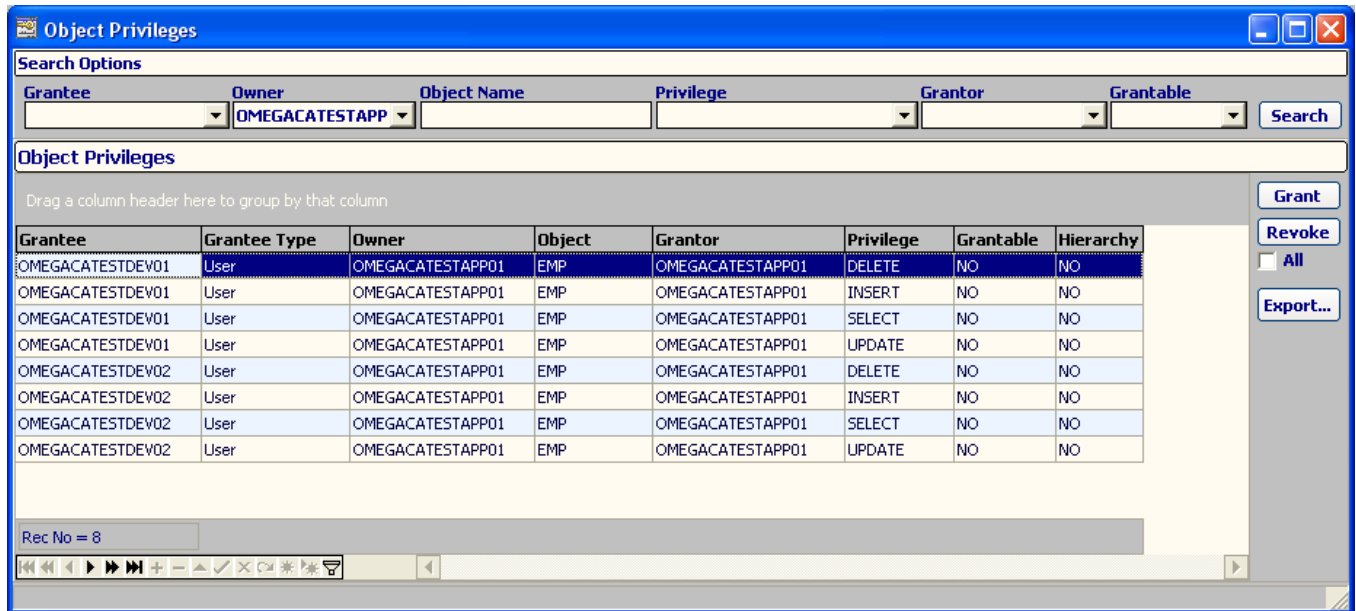
Set the required fields and press the button Grant.  
You will receive a confirmation, or the error message when failure.

#### 8.4.2 Revoking a system privilege

To revoke a system privilege, select a system privilege record in the form System Privileges, System Privileges grid and press the button Revoke. If the revoke dialog box is confirmed, the system privilege will be revoked. To revoke all system privileges in the grid check the All option.

## 8.5 Object Privileges

To view the object privileges in the Application's main menu, Security tab, Privileges group click the Object Privileges menu button. This will open the form Object Privileges. Enter the desired options and press the button Search on the right. The result will be listed in the Object Privileges grid.



Grantee	Grantee Type	Owner	Object	Grantor	Privilege	Grantable	Hierarchy
OMEGACATESTDEV01	User	OMEGACATESTAPP01	EMP	OMEGACATESTAPP01	DELETE	NO	NO
OMEGACATESTDEV01	User	OMEGACATESTAPP01	EMP	OMEGACATESTAPP01	INSERT	NO	NO
OMEGACATESTDEV01	User	OMEGACATESTAPP01	EMP	OMEGACATESTAPP01	SELECT	NO	NO
OMEGACATESTDEV01	User	OMEGACATESTAPP01	EMP	OMEGACATESTAPP01	UPDATE	NO	NO
OMEGACATESTDEV02	User	OMEGACATESTAPP01	EMP	OMEGACATESTAPP01	DELETE	NO	NO
OMEGACATESTDEV02	User	OMEGACATESTAPP01	EMP	OMEGACATESTAPP01	INSERT	NO	NO
OMEGACATESTDEV02	User	OMEGACATESTAPP01	EMP	OMEGACATESTAPP01	SELECT	NO	NO
OMEGACATESTDEV02	User	OMEGACATESTAPP01	EMP	OMEGACATESTAPP01	UPDATE	NO	NO

The following are the properties of the object privileges:

Field Name	Field Description
Grantee	User or role granted the privilege.
Grantee Type	Grantee Type (user or role).
Owner	Owner of the object.
Object	Name of the object.
Grantor	Grantor of the privilege.
Privilege	Object privilege.
Grantable	Granted privilege is grantable by the grantee.
Hierarchy	Privilege was granted with the HIERARCHY OPTION.

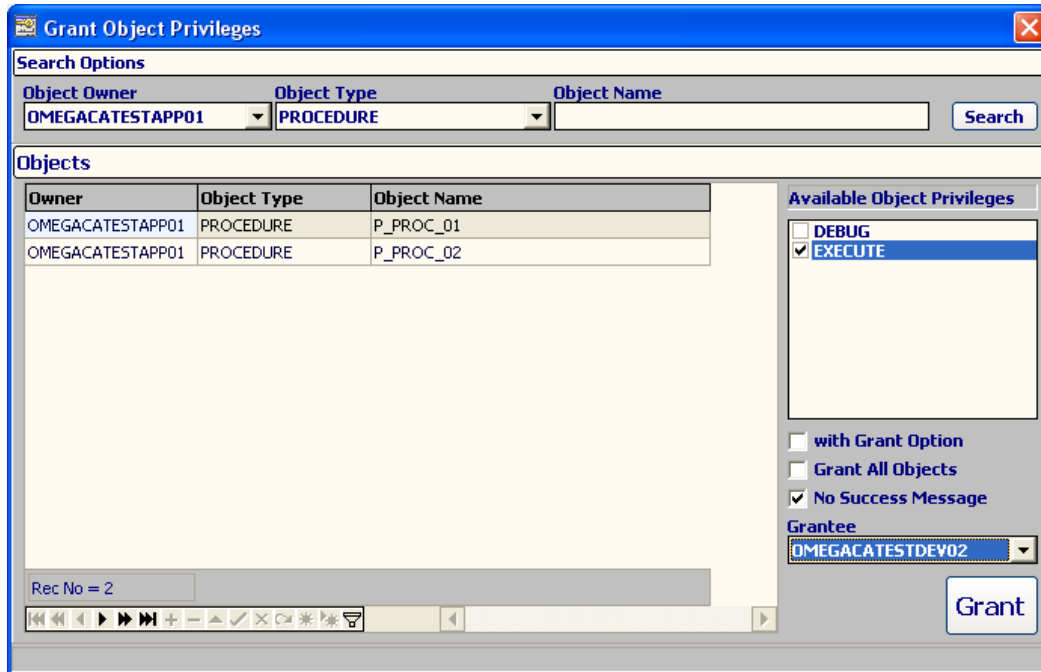
### Important Note:

Object Privileges grants and revokes take immediate effect.

Press the Refresh button to refresh them.

### 8.5.1 Granting an object privilege

To grant an object privilege, in the form Object Privileges, Object Privileges grid, press the button Grant on the right. The form "Grant Object Privilege" will open.



The dialog box "Grant Object Privileges" contains the following sections:

- Search Options:**
  - Object Owner: OMEGACATESTAPP01
  - Object Type: PROCEDURE
  - Object Name: (empty)
  - Search button
- Objects:**

Owner	Object Type	Object Name
OMEGACATESTAPP01	PROCEDURE	P_PROC_01
OMEGACATESTAPP01	PROCEDURE	P_PROC_02
- Available Object Privileges:**
  - ☐ DEBUG
  - ☒ EXECUTE
- Options:**
  - ☐ with Grant Option
  - ☐ Grant All Objects
  - ☒ No Success Message
- Grantee:** OMEGACATESTDEV02
- Grant** button
- Footer:** Rec No = 2, navigation icons

Choose the database objects on Objects grid on the left and the respective privileges on Available Object Privileges the right. Set the required fields and press the button Grant. You will receive a confirmation, or the error message when failure.

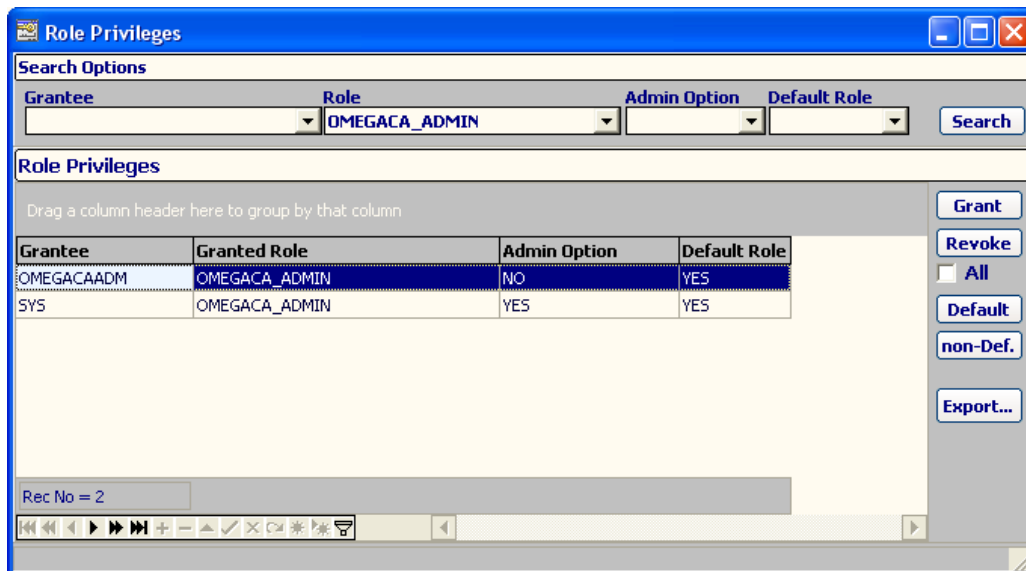
The checkbox "Grant All", which is enabled when searched with an Object Type, allows for multiple Grants on all Object selected.

### 8.5.2 Revoking an object privilege

To revoke an object privilege, select an object privilege record in the form Object Privileges, Object Privileges grid and press the button Revoke. If the revoke dialog box is confirmed, the object privilege will be revoked. To revoke all object privileges in the grid check the All option.

## 8.6 Role Privileges

To view the role privileges in the Application's main menu, Security tab, Privileges group click the Role Privileges menu button. This will open the form Role Privileges. Enter the desired options and press the button Search on the right. The result will be listed in the Role Privileges grid.



The following are the properties of the role privileges:

Field Name	Field Description
Grantee	User or role granted the role.
Granted Role	Role granted to the grantee.
Admin Option	Granted role is grantable by the grantee.
Default Role	Role is default or not.

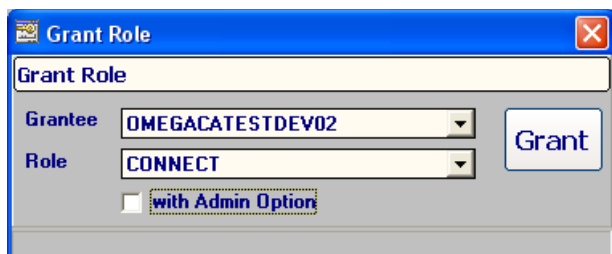
### Important Note:

By Oracle implementation, Role grants and revokes take effect only on subsequent user sessions, or when the grant or revoke is followed by a respective SET ROLE statement.

Press the Refresh button to refresh them.

### 8.6.1 Granting a role privilege

To grant a role privilege, in the form Role Privileges, Role Privileges grid, press the button Grant on the right. The form "Grant Role" will open.



Choose Grantee and the Role and press the button Grant. You will receive a confirmation, or the error message when failure.

### 8.6.2 Revoking a role privilege

To revoke a role privilege, select a role privilege record in the form Role Privileges, Role Privileges grid and press the button Revoke. If the revoke dialog box is confirmed, the role privilege will be revoked. To revoke all role privileges in the grid check the All option.

### 8.6.3 Default role privilege management

To manage the roles availability to the user, select a role privilege record in the form Role Privileges, Role Privileges grid and:

- Press the button Default and confirm the Default dialog to make the selected role default to the grantee.
- Press the button non-Def. and confirm the non-Default dialog to make the selected role non-default to the grantee.

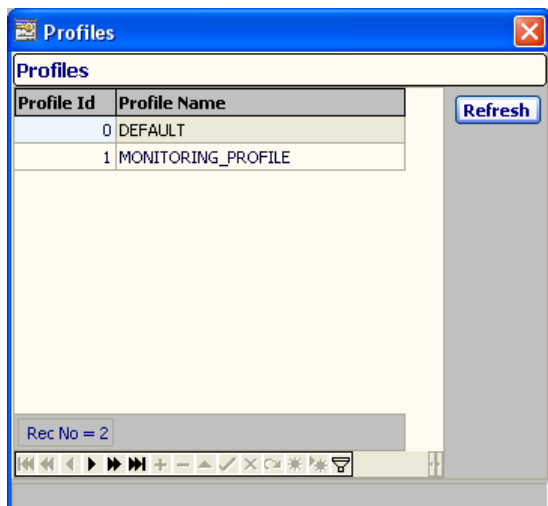
**Note:**

The roles are granted as default to the grantee. After you change for the first time its default availability this behavior will change and roles granted to the grantee will be granted as non-default, they must be manually set to default!

## 8.7 Profiles

### 8.7.1 Database Profiles

To view the database profiles in the Application's main menu, Security tab, System Profiles group click the Profiles menu button. This will open the form Profiles. The result will be listed in the Profiles grid.



Profile Id	Profile Name
0	DEFAULT
1	MONITORING_PROFILE

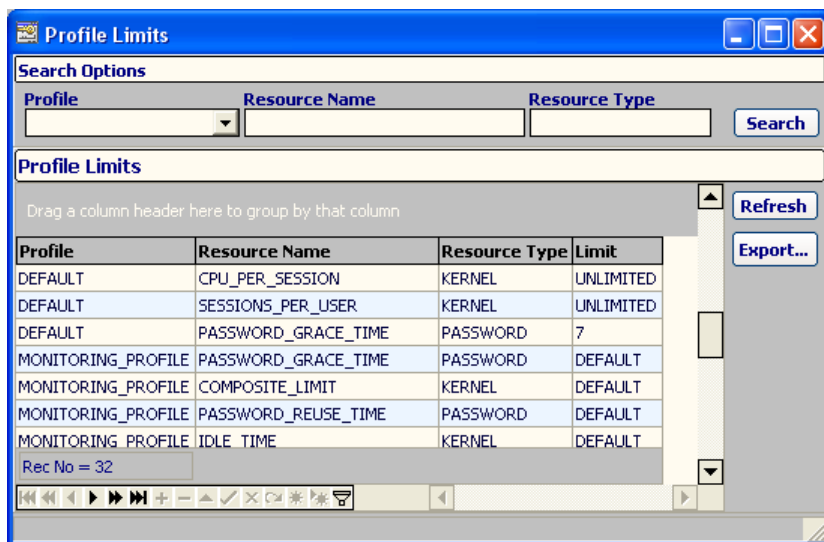
The following are the properties of the profiles:

Field Name	Field Description
Profile Id	Identifier of the profile.
Profile Name	Name of the profile.

Press the Refresh button to refresh them.

### 8.7.2 Profile Limits

To view the profile limits in the Application's main menu, Security tab, System Profiles group click the Profile Limits menu button. This will open the form Profile Limits. The result will be listed in the Profile Limits grid.



Profile	Resource Name	Resource Type	Limit
DEFAULT	CPU_PER_SESSION	KERNEL	UNLIMITED
DEFAULT	SESSIONS_PER_USER	KERNEL	UNLIMITED
DEFAULT	PASSWORD_GRACE_TIME	PASSWORD	7
MONITORING_PROFILE	PASSWORD_GRACE_TIME	PASSWORD	DEFAULT
MONITORING_PROFILE	COMPOSITE_LIMIT	KERNEL	DEFAULT
MONITORING_PROFILE	PASSWORD_REUSE_TIME	PASSWORD	DEFAULT
MONITORING_PROFILE	IDLE_TIME	KERNEL	DEFAULT



The following are the properties of the profile limits:

Field Name	Field Description
Profile Name	Name of the profile.
Resource Name	Name of the resource.
Resource Type	Type of the resource.
Limit	Limit applied on profile's resource.

To view the profile limits open the form Profile Limits, enter the desired options and press the button Search on the right. The result will be listed in the Profile Limits grid. Press the Refresh button to refresh them.

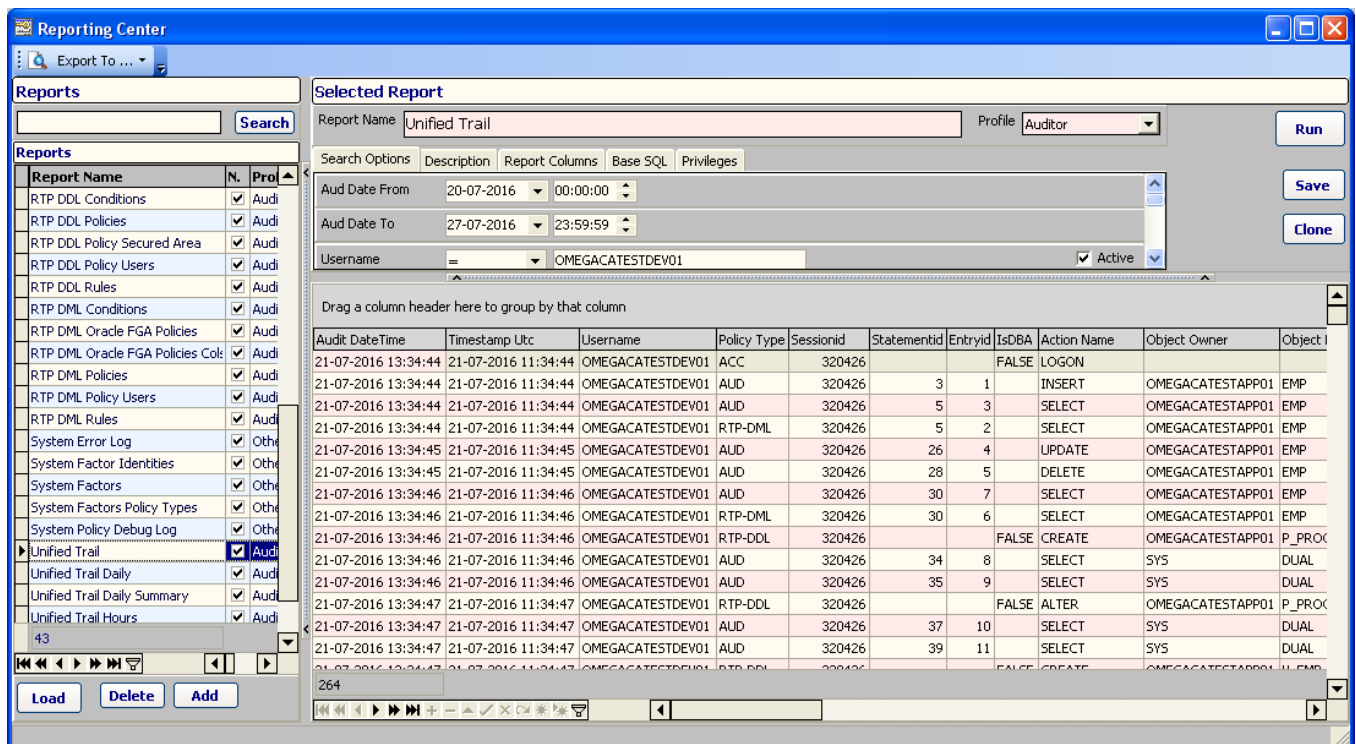
## 9 CHAPTER 9: Reporting

Omega Core Audit comes with a dynamic reporting module that allows the end-user to create and modify the report in all its components, from the base SQL and parameters to columns and column search options. Report properties and settings are saved into the repository permitting quick loading of saved reports.

Omega Core Audit comes with a set of predefined reports which are deployed as part of its installation procedure. These reports can be used as they are, or cloned by the application user.

You cannot change the Omega Core Audit's Native Reports, except for the visual layout and search parameters (search operator, values and active status only). However it is advised not to change at all the Native reports, but to clone them as non-native reports and change according to user needs.

To view the reports for running and managing, in the in the Application's main menu, tab Reports, Reporting Center group, click on the Reporting Center menu button. The form Reporting Center will open.



Audit DateTime	Timestamp Utc	Username	Policy Type	Sessionid	Statementid	Entryid	IsDBA	Action Name	Object Owner	Object I
21-07-2016 13:34:44	21-07-2016 11:34:44	OMEGACATESTDEV01	ACC	320426			FALSE	LOGON		
21-07-2016 13:34:44	21-07-2016 11:34:44	OMEGACATESTDEV01	AUD	320426	3	1		INSERT	OMEGACATESTAPP01	EMP
21-07-2016 13:34:44	21-07-2016 11:34:44	OMEGACATESTDEV01	AUD	320426	5	3		SELECT	OMEGACATESTAPP01	EMP
21-07-2016 13:34:44	21-07-2016 11:34:44	OMEGACATESTDEV01	RTP-DML	320426	5	2		SELECT	OMEGACATESTAPP01	EMP
21-07-2016 13:34:45	21-07-2016 11:34:45	OMEGACATESTDEV01	AUD	320426	26	4		UPDATE	OMEGACATESTAPP01	EMP
21-07-2016 13:34:45	21-07-2016 11:34:45	OMEGACATESTDEV01	AUD	320426	28	5		DELETE	OMEGACATESTAPP01	EMP
21-07-2016 13:34:46	21-07-2016 11:34:46	OMEGACATESTDEV01	AUD	320426	30	7		SELECT	OMEGACATESTAPP01	EMP
21-07-2016 13:34:46	21-07-2016 11:34:46	OMEGACATESTDEV01	RTP-DML	320426	30	6		SELECT	OMEGACATESTAPP01	EMP
21-07-2016 13:34:46	21-07-2016 11:34:46	OMEGACATESTDEV01	RTP-DDL	320426			FALSE	CREATE	OMEGACATESTAPP01	P_PROX
21-07-2016 13:34:46	21-07-2016 11:34:46	OMEGACATESTDEV01	AUD	320426	34	8		SELECT	SYS	DUAL
21-07-2016 13:34:46	21-07-2016 11:34:46	OMEGACATESTDEV01	AUD	320426	35	9		SELECT	SYS	DUAL
21-07-2016 13:34:47	21-07-2016 11:34:47	OMEGACATESTDEV01	RTP-DDL	320426			FALSE	ALTER	OMEGACATESTAPP01	P_PROX
21-07-2016 13:34:47	21-07-2016 11:34:47	OMEGACATESTDEV01	AUD	320426	37	10		SELECT	SYS	DUAL
21-07-2016 13:34:47	21-07-2016 11:34:47	OMEGACATESTDEV01	AUD	320426	39	11		SELECT	SYS	DUAL

This Reporting Center form has two main panels:

### Reports Panel

The Reports panel is aligned on the left side of the "Reporting Center" form. It contains the Reports Grid which shows the reports stored in the Repository.

### Selected Report Panel

The Selected Report panel is aligned on the right side of the "Reporting Center" form. It contains the Repository report that has been loaded (opened) and is ready for running, modifying or cloning.

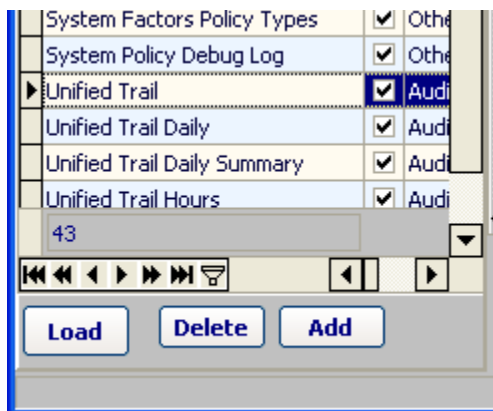
The following are the components of a report:

Field Name	Field Description
Report Name	Name of the report. Unique in combination with the profile.
N. (for Native)	If checked the Report is a native predefined report. You cannot modify these reports, unless for layout customization and search options values.
Profile	Profile of the report.
Report Id	Unique auto-generated identification number of the report in repository.
Description	Description of the report.
Base SQL	Base SQL command of the report. This is the initial report's SQL, which during the run will be enriched with conditions on Searched Fields.
Base SQL Parameters	Optional Base SQL parameters, declared with the syntax ":PARAM_NAME".
Report Columns	Columns of the report. You can view and manage them in the tab with the same name. You must re-open the report when you change columns if you need to see changed "Search Field" columns
Privileges	Report Privileges managed in relation with the Omega Core Audit Roles.

## 9.1 Loading a Report

In the general description above we noted the visual difference between the all repository reports and the selected report. On the left side you can browse on the searched Repository reports, on the right you load the report for running it, modifying or cloning.

To load a report select the report record in the Reports grid on the left and press the button Load below, or double-click the record. Notice the "Black Arrow" indicator in the Reports grid highlighting the current selected record!



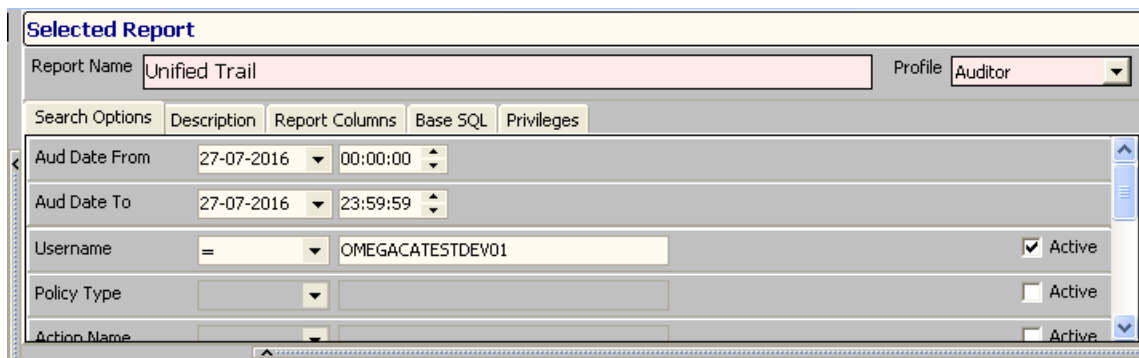
The report definitions will load from the repository and open in the panel "Selected Report" on the right side of the form. The report name and profile are displayed in on the top. Other properties are displayed in the five tabs described below.

### Note:

You can only have one report loaded at the time. Be careful to remind that scrolling records into the left Grid Reports will not affect the "Selected Report" panel (and most important!) it's content. The only way to load a Repository report into the "Selected Report" panel is by first selecting it in the Reports grid on the left and then press the button Open below!

### Search Options and Description tabs

In the first tab Search Options, general search conditions are set before running the report. These are of two categories: the Base SQL parameters and the search conditions on report fields.



Base SQL parameters are loaded first. They are non-optional and have no option for Operation Code choice (=, <>, ...). For parameters with a Display Type of "ftDateTime", Date and Time editor components will be displayed instead of the standard edit boxes for other Display Types.

#### Note:

You must always choose Base SQL parameters (it is a must on big tables) and search options to avoid returning large amount of records and also choose indexed repository table fields to avoid full table scans (FTS) on the database. For the Unified Audit Trail view V\_SYS\_UNF\_TRAIL (a big table!), the minimal advised Base SQL Parameters are Date From and Date To.

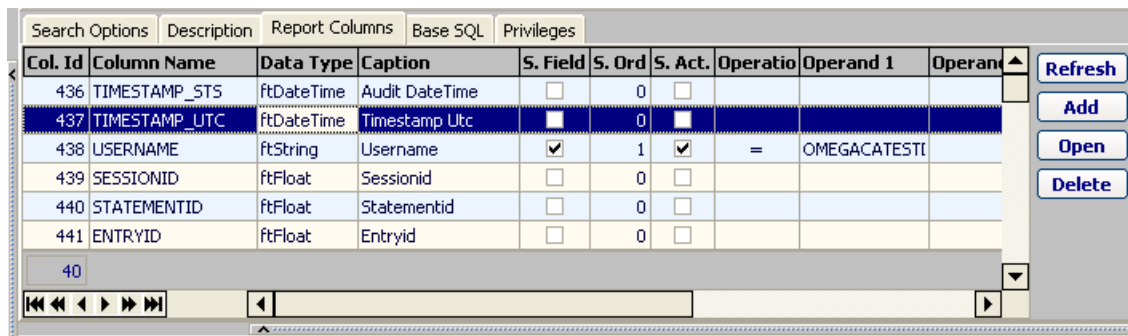
Second, the search conditions on report fields are displayed. You will notice their setup is somehow different from the Base SQL parameters. Their search is optional (can be Active or Inactive) and do have the option for Operation Code choice (=, <>, ...). For Report Columns with a Data Type of "ftDateTime", Date and Time editor components will be displayed instead of the standard edit boxes for other Display Types (see Report Columns).

In the next tab Description, as the name implies, the text description of the report is displayed.

Go again next tab to the Report Columns.

#### Report Columns tab

In this tab you can manage the report's columns.



Col. Id	Column Name	Data Type	Caption	S. Field	S. Ord	S. Act.	Operation	Operand 1	Operand 2
436	TIMESTAMP_STS	ftDateTime	Audit DateTime	<input type="checkbox"/>	0	<input type="checkbox"/>			
437	TIMESTAMP_UTC	ftDateTime	Timestamp Utc	<input type="checkbox"/>	0	<input type="checkbox"/>			
438	USERNAME	ftString	Username	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	=	OMEGACATESTI	
439	SESSIONID	ftFloat	Sessionid	<input type="checkbox"/>	0	<input type="checkbox"/>			
440	STATEMENTID	ftFloat	Statementid	<input type="checkbox"/>	0	<input type="checkbox"/>			
441	ENTRYID	ftFloat	Entryid	<input type="checkbox"/>	0	<input type="checkbox"/>			

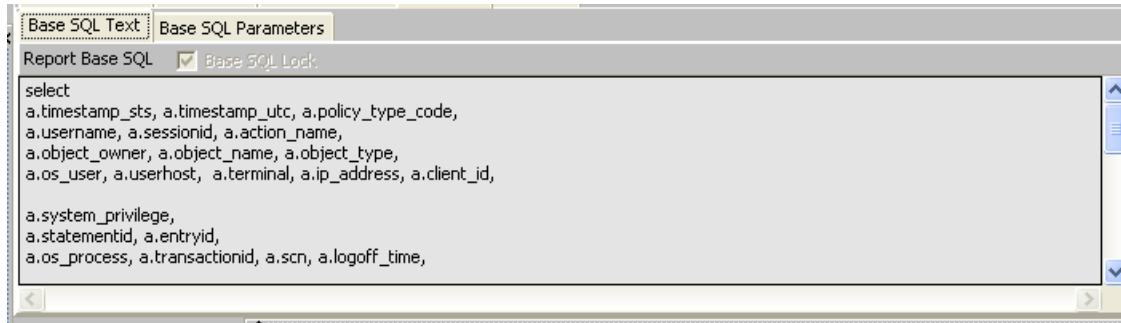
The following are the properties of a report's column:

Field Name	Field Description
Col. Id	Unique auto-generated identification number of the report's column in repository.
Column Name	Original name (as in the database) of the column.
Data Type	Column data type, as detected by the Application.
Caption	Caption of the report's columns as it will show in report column headers.
Search Field	If checked, a search condition will be set on the column in the tab Search Options, after the Base SQL parameters.
Search Active	If checked, the search condition set on the column will be Active in the tab Search Options.
Search Order	The order in which the search condition on field will be set in the tab Search Options.
Operation	Operation Code choice (=, <>, <, <=, IN, LIKE...).
Operator 1	First operand.
Operator 2	Second Operand.

## Base SQL tab

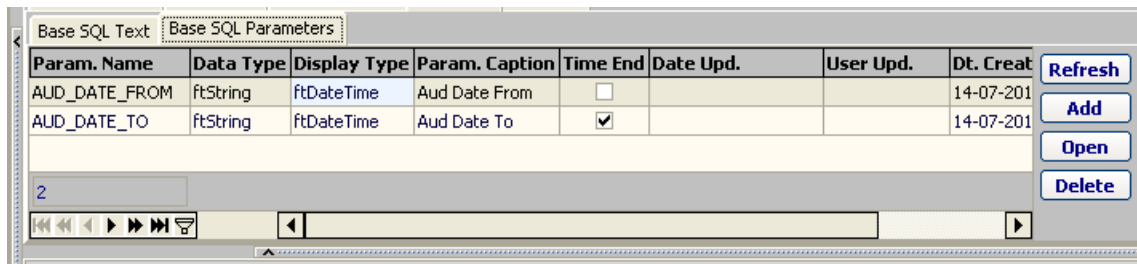
This tab displays: the Base SQL Text of the report and (optionally) the Base SQL Parameters.

In the Base SQL text tab:



The memo displays the Base SQL of the report. By default it is locked and can be unlocked by the checkbox "Base SQL Lock" (if report in non-native, see later).

In the Base SQL Parameters tab you can manage the same as the name implies:



The following are the properties of a report's Base SQL Parameter:

Field Name	Field Description
Param. Name	Name of the Base SQL parameter, Unique within the report.
Data Type	Data type of the Base SQL parameter.
Display Type	Display Type of the parameter, effecting display editors in the tab Search Options.
Param. Caption	Caption of the Base SQL parameter as it will show in the tab Search Options.
Time End	Valid for Display Type of "ftDateTime" only. If un-checked time editors components will be set to 00:00:00, if checked will be set to 23:59:59.

In this tab you can manage the report's privileges. Omega Core Audit report Privileges are applied at the Omega Core Audit Role level and explicitly declared for each report.

The following are the properties of a report's privilege:

95

## 9.2 Running a Report

To run a report, first load it on the "Selected Reports" panel. After you have loaded the report then:

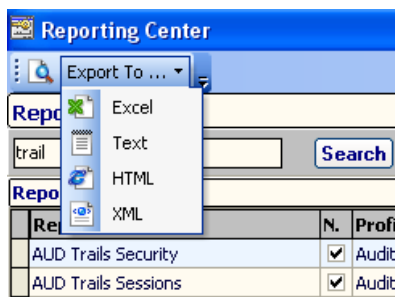
- complete any Base SQL parameters in the Search Options tab
- complete any active search fields options in the Search Options tab
- press the button RUN

The result will show in the report's grid, aligned on the right and below of form "Reporting Center".

Drag a column header here to group by that column											
Audit Date Time	Timestamp Utc	Policy Type	Username	Sessionid	Statementid	Entryid	IsDBA	Action Name	Object Owner	Object Name	Module
21-07-2016 13:34:44	21-07-2016 11:34:44	ACC	OMEGACATESTDEV01	320426			FALSE	LOGON			
21-07-2016 13:34:44	21-07-2016 11:34:44	AUD	OMEGACATESTDEV01	320426	3	1		INSERT	OMEGACATESTAPP01	EMP	
21-07-2016 13:34:44	21-07-2016 11:34:44	AUD	OMEGACATESTDEV01	320426	5	3		SELECT	OMEGACATESTAPP01	EMP	
21-07-2016 13:34:44	21-07-2016 11:34:44	RTP-DML	OMEGACATESTDEV01	320426	5	2		SELECT	OMEGACATESTAPP01	EMP	
21-07-2016 13:34:45	21-07-2016 11:34:45	AUD	OMEGACATESTDEV01	320426	26	4		UPDATE	OMEGACATESTAPP01	EMP	
21-07-2016 13:34:45	21-07-2016 11:34:45	AUD	OMEGACATESTDEV01	320426	28	5		DELETE	OMEGACATESTAPP01	EMP	
21-07-2016 13:34:46	21-07-2016 11:34:46	AUD	OMEGACATESTDEV01	320426	30	7		SELECT	OMEGACATESTAPP01	EMP	
21-07-2016 13:34:46	21-07-2016 11:34:46	RTP-DML	OMEGACATESTDEV01	320426	30	6		SELECT	OMEGACATESTAPP01	EMP	
21-07-2016 13:34:46	21-07-2016 11:34:46	RTP-DDL	OMEGACATESTDEV01	320426			FALSE	CREATE	OMEGACATESTAPP01	P_PROC_01	OmegaCABenchmark.exe
21-07-2016 13:34:46	21-07-2016 11:34:46	AUD	OMEGACATESTDEV01	320426	34	8		SELECT	SYS	DUAL	
21-07-2016 13:34:46	21-07-2016 11:34:46	AUD	OMEGACATESTDEV01	320426	35	9		SELECT	SYS	DUAL	
21-07-2016 13:34:47	21-07-2016 11:34:47	RTP-DDL	OMEGACATESTDEV01	320426			FALSE	ALTER	OMEGACATESTAPP01	P_PROC_02	OmegaCABenchmark.exe
21-07-2016 13:34:47	21-07-2016 11:34:47	AUD	OMEGACATESTDEV01	320426	37	10		SELECT	SYS	DUAL	
21-07-2016 13:34:47	21-07-2016 11:34:47	AUD	OMEGACATESTDEV01	320426	39	11		SELECT	SYS	DUAL	
21-07-2016 13:34:47	21-07-2016 11:34:47	RTP-DDL	OMEGACATESTDEV01	320426			FALSE	CREATE	OMEGACATESTAPP01	V_EMP	OmegaCABenchmark.exe
21-07-2016 13:34:47	21-07-2016 11:34:47	AUD	OMEGACATESTDEV01	320426	42	12		SELECT	SYS	DUAL	
21-07-2016 13:34:47	21-07-2016 11:34:47	AUD	OMEGACATESTDEV01	320426	43	13		SELECT	SYS	DUAL	
21-07-2016 13:34:47	21-07-2016 11:34:47	AUD	OMEGACATESTDEV01	320426	41	15		SELECT	OMEGACATESTAPP01	DEPT	
21-07-2016 13:34:47	21-07-2016 11:34:47	AUD	OMEGACATESTDEV01	320426	41	14		SELECT	OMEGACATESTAPP01	EMP	CREATE ANY VIEW
21-07-2016 13:34:48	21-07-2016 11:34:48	RTP-DDL	OMEGACATESTDEV01	320426			FALSE	ALTER	OMEGACATESTAPP01	V_EMP	OmegaCABenchmark.exe
21-07-2016 13:34:48	21-07-2016 11:34:48	AUD	OMEGACATESTDEV01	320426	45	16		SELECT	SYS	DUAL	

### 9.2.1 Exporting Report data

To export the report data into Excel, Text, Html and Xml formats press the "Export To..." drop-type button on the top menu.



To print and preview the report press the Loop button on the top menu. The Print Preview form will open.



### 9.3 Modifying an existing Report

To modify an existing report, first load it on the "Selected Reports" panel. After you have loaded the report, you can modify it and save the changes to the repository.

You can change the report's name and profile in the respective panel on the top. Press button SAVE to save the changes in the Repository. When you press the button SAVE, the report's grid and print layout are saved also!

Other properties you can change in the tabs below:

#### **Search Options:**

You can change the operands for the search conditions on the report fields, operator used, operand[s] values and Active status. Press button SAVE to save the changes in the Repository; however they are immediately effective for report execution.

#### **Report Description:**

This is a text field for report description. Press button SAVE to save the changes in the Repository.

#### **Report Columns:**

You can add, change and delete the columns of your report and also their availability into the Search Options by the Search Field checkbox. When adding and changing, the respective forms will open. Use the Search Order field to order the columns top-down in Search Options (useful to put indexed fields first). Smaller Search Order values will be listed first.

Changes are immediately saved into the Repository and not related with the SAVE button. You must re-load the report to see the effect!

#### **Base SQL:**

This tab displays two sub-tabs: the Base SQL Text of the report and (optionally) the Base SQL Parameters.

In the first tab:

you can edit the Base SQL text of the report, by first unlocking the read-only Memo editor by the "Base SQL Lock" checkbox. Press button SAVE to save the changes in the Repository; however they are immediately effective for report execution.

In the second tab:

you can add, change and delete the Base SQL report parameters, if any. When adding and changing, the respective forms will open.

Changes are immediately saved into the Repository and not related with the SAVE button. You must re-load the report to see the effect!

#### **Report Privileges:**

In this tab you can add, change and delete the report's privileges. When adding and changing, the respective forms will open. OMEGACA\_ADMIN Privilege records are built-in full Read-Write and cannot be modified by Privilege procedures!

Changes are immediately saved into the Repository and not related with the SAVE button.

**Note:**

Report Privileges are implicitly inserted by the Report Insert Procedure. Privileges (inserted in report creation) are:

1. Granted Read-Write built-in to Omega Core Audit Administrator Role OMEGACA\_ADMIN.
2. Granted Read-Write to all Omega CA Roles the running user belongs (excluded OMEGACA\_ADMIN).

Because Omega Core Audit Role Administrator has full functionalities and thus is logically the sole role granted to Omega CA Admin Account, it will not grant any privilege to other roles during report creation, so that must be explicitly done if report will be used by other Omega Core Audit Roles.

**General Notes on report modifications:**

1. Changes you make to Report Columns (and optionally Base SQL parameters) and Base SQL must be logically in sync to each-others
2. The Diesis # character is internally used by Omega Core Audit as the value separator in the case of IN and NOT IN operands! Use only the Diesis # character to separate values and do not use it as part of any value. Do not use Diesis # in the end, as it will generate an empty value.

## 9.4 Cloning an existing Report

To clone an existing report, first load it on the "Selected Reports" panel. After you have loaded the report, you can clone it by:

1. Setting a new name for the report (report name is unique).
2. Press the "Clone button".

### Important Note

When you create a new report by "Save As" an existing report, you are still focused on the old report. Loading the report on the right tab "Selected Report" is done only by selecting it on the left grid Reports and then open.

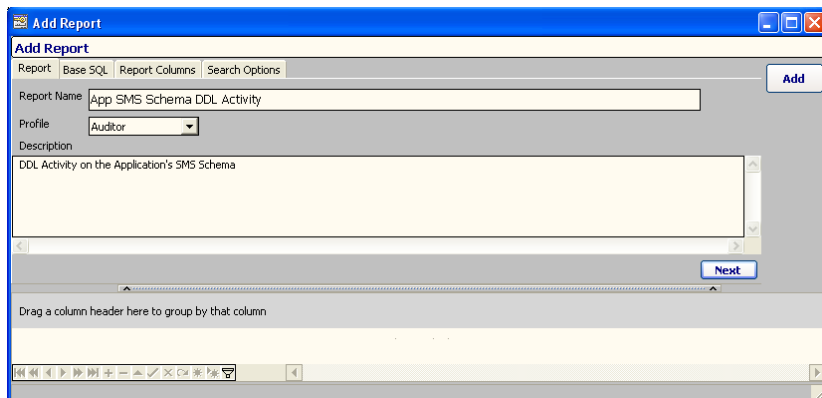
## 9.5 Creating an new Report

To create a new report from the scratch press the Add button on the form Reporting Center, tab Reports on the left. The form Add New Report will open.

To create the new report follow the four step wizard as below:

### STEP 1 - Report:

In the first step report name, profile and description are completed. You can choose only from the profiles that match with your granted Omega CA roles.



Press the Next Button to go to the next step.

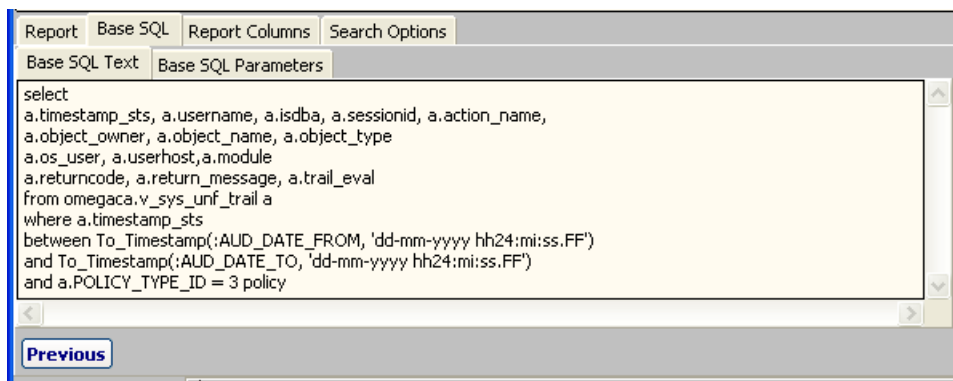
### STEP 2 - Base SQL:

In this tab you define the Base SQL Text of the report and (optionally) the Base SQL Parameters. This tab has two sub-tabs:

#### Base SQL Text tab

In the first Tab Base SQL Text complete the base SQL of the report. Do not put here conditions that are intended to be used as Field Search Options. Remember that when searching, the chosen "Search Fields" columns conditions are added to the Base SQL Text automatically by Omega Core Audit.

For example, a Base SQL on the Unified Audit Trail, with From and To parameters on Audit DateTime would look:



The SQL in the figure above is:

select

```
a.timestamp_sts, a.username, a.isdba, a.sessionid, a.action_name,
a.object_owner, a.object_name, a.object_type,
a.os_user, a.userhost,a.module,
a.returncode, a.return_message, a.trail_eval
```

from v\_sys\_unf\_trail a

```
where a.timestamp_sts
between To_Timestamp(:AUD_DATE_FROM, 'dd-mm-yyyy hh24:mi:ss.FF')
and To_Timestamp(:AUD_DATE_TO, 'dd-mm-yyyy hh24:mi:ss.FF')
```

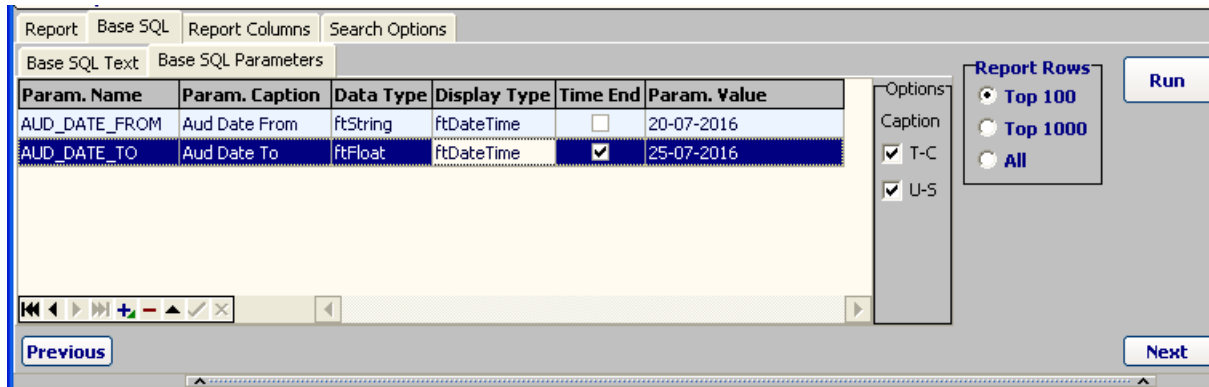
```
and a.policy_type_id = 3
```

The two parameters AUD\_DT\_FROM and AUD\_DT\_TO are declared as string (and then converted to Timestamp). Note the ":" syntax for parameter declaration.

When Base SQL report parameters are present they must be manually declared in report create. For this you must go to the next tab of the second step BASE SQL.

### Base SQL Parameters tab

In the Grid of this tab the declaration of the Base SQL parameters is done in full. Leave this empty and skip topic if there are no Base SQL Parameters.



Param. Name	Param. Caption	Data Type	Display Type	Time End	Param. Value
AUD_DATE_FROM	Aud Date From	ftString	ftDateTime	<input type="checkbox"/>	20-07-2016
AUD_DATE_TO	Aud Date To	ftFloat	ftDateTime	<input checked="" type="checkbox"/>	25-07-2016

The Grid's Navigator buttons are:

The first for: First, Previous, Next, Last

The last five: Add, Delete, Edit, Post, Cancel

Insert the records by pressing the Add button. This will create an empty record.

First enter the value for the first field "Param. Name". Then you can press the Enter key to have the "Param. Caption" field auto-completed the same in title-case. Complete the other fields, "Data Type" as String, "Display Type" as ftDateTime, check Time End only for the AUD\_DATE\_TO and "Param. Value" as date string formatted DD-MM-YYYY.

Do not leave the grid in an Editable state. Remember to press the Navigator's Post button to post changes!

### Report Rows:

To avoid a large number of records by keep the default Top 100 or Top 1000 into the Report Rows Radio Group. You can also avoid FTS on big tables by adding a temporary condition in the Base SQL, kind of `TIMESTAMP_STS > SYSDATE-1` (to limit the amount of data returned and avoid Full Table Scans) and then remove it again after running the report and before saving it.

### Important Note:

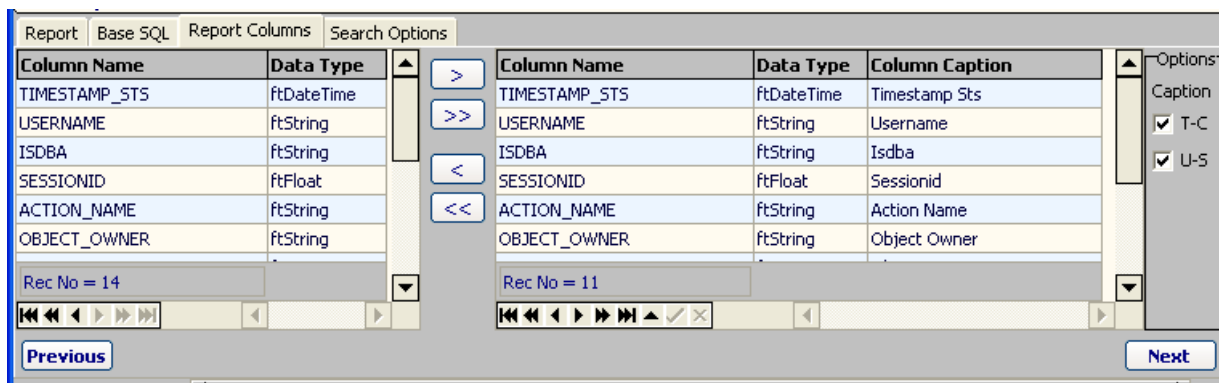
Be careful to avoid full table scans (FTS) on big tables and also returning large amount of records to your Desktop when creating a new report. To avoid FTS use Base SQL Parameters and Search Conditions on fields outputted unchanged (as table/view originals) from the Report's Base SQL. Always use search criteria in reports and try to match the indexed columns, the most relevant being the Audit Date/Time column (`TIMESTAMP_STS`) on the Unified Audit Trail view `V_SYS_UNF_TRAIL`, but also username and user host.

Execute the SQL by pressing the button RUN. Report will populate the lower grid. Right-click on the grid's header and in the popup menu choose the "Best Fit (all Columns)" item.

Press the Next Button to go to the next step.

### STEP 3 - Report Columns:

In this step you will choose the columns you want to have in your report.



Available report columns are on the left grid which is populated by each execution of the Base SQL by the RUN button in the previous step. Columns that will show on the report are those on the right Grid. Work with the single and double arrow buttons to choose or remove report columns on the right side.

Column Name and Data Type are automatically set and cannot be changed. You can change the Column Caption.

Optional and default checked Checkboxes are:

- T-C - title-case for column captions
- U-S - underscores to spaces for column captions

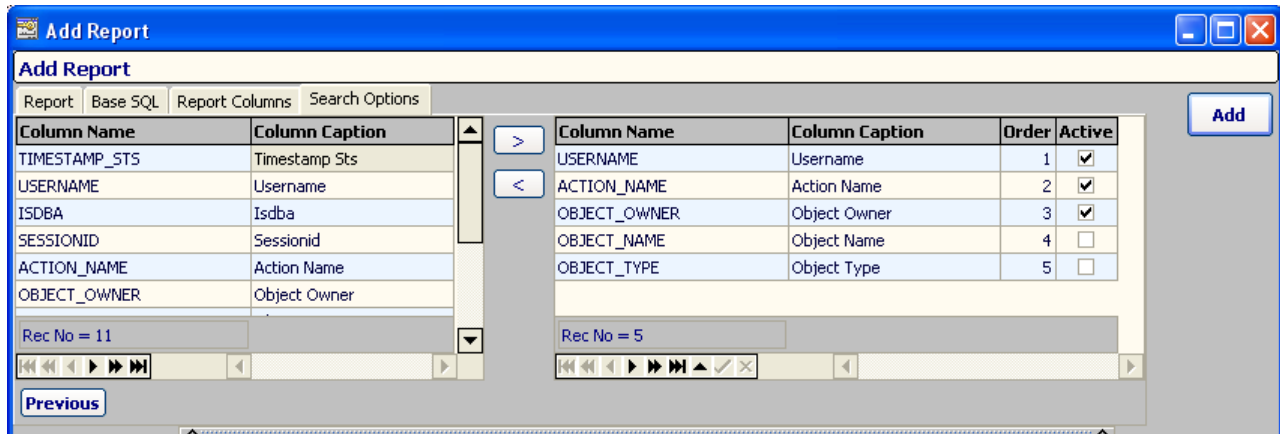
The right Grid's last three Navigator buttons are: Edit, Post and Cancel.

Do not leave the grid in an Editable state. Remember to press the Navigator's Post button to post changes!

Press the Next Button to go to the next step.

### STEP 4 - Search Options:

In this step you will choose the report columns on which you will set search conditions before you run. The search conditions can be set only on the columns that were previously chosen (in the Step 3) to show in the report.



Column Name	Column Caption
TIMESTAMP_STS	Timestamp Sts
USERNAME	Username
ISDBA	Isdba
SESSIONID	Sessionid
ACTION_NAME	Action Name
OBJECT_OWNER	Object Owner

Column Name	Column Caption	Order	Active
USERNAME	Username	1	<input checked="" type="checkbox"/>
ACTION_NAME	Action Name	2	<input checked="" type="checkbox"/>
OBJECT_OWNER	Object Owner	3	<input checked="" type="checkbox"/>
OBJECT_NAME	Object Name	4	<input type="checkbox"/>
OBJECT_TYPE	Object Type	5	<input type="checkbox"/>

Report columns are on the left grid. Columns that will have search options are those on the right Grid. Work with the arrow buttons to choose or remove selected report columns on the right side. Set the Order field to an incremental value and Active at will.

The right Grid's last three Navigator buttons are: Edit, Post and Cancel.

Do not leave the grid in an Editable state. Remember to press the Navigator's Post button to post changes!

After completing all the four steps above press the button Add. This will create the report into the Repository.

### Privileges on Report Creation

Report Privileges are implicitly inserted by the Report Insert Procedure. Privileges (inserted in report creation) are:

1. Granted Read-Write built-in to Omega Core Audit Administrator Role OMEGACA\_ADMIN.
2. Granted Read-Write to all Omega CA Roles the running user belongs (excluded OMEGACA\_ADMIN).

Because Omega Core Audit Role Administrator has full functionalities and thus is logically the sole role granted to Omega CA Admin Account, it will not grant any privilege to other roles during report creation, so that must be explicitly done if report will be used by other Omega Core Audit Roles.

## 9.6 Report Performance Guidelines

Always use indexed columns as part of your search options when querying big trail tables. Use Base SQL Parameter in the audit Date Time field (TIMESTAMP\_STS) of the Unified Audit Trail.

In the chapter "Common Application functionalities", see the Important Performance Note in the topic "Client-side information retrieval".

## 10 CHAPTER 10: System Administration

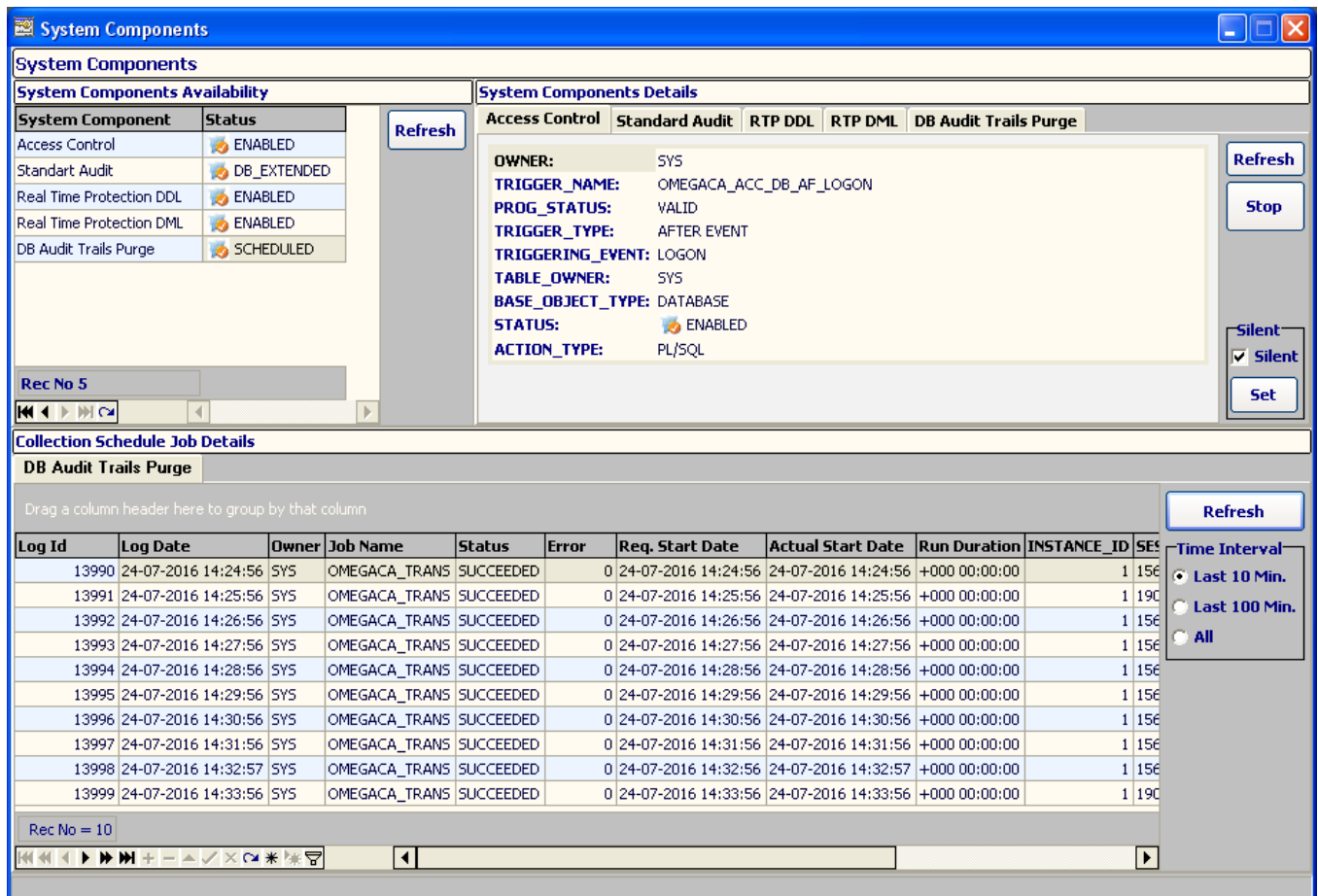
The System Administration module handles the management of core system functionalities and module availability, enabling the Omega Core Audit administrators to easily and quickly complete their tasks.

The managed functionalities are:

- System components.
- Omega Core Audit users and roles.
- System factors.
- Database jobs, both Scheduler and Classic.

### 10.1 System Components

To view the main system components, in the main menu Administration, tab System Components click the menu button System Components. This will open the form System Components.



**System Components Availability**

System Component	Status
Access Control	ENABLED
Standard Audit	DB_EXTENDED
Real Time Protection DDL	ENABLED
Real Time Protection DML	ENABLED
DB Audit Trails Purge	SCHEDULED

**System Components Details**

**Access Control**

OWNER: SYS  
 TRIGGER\_NAME: OMEGACA\_ACC\_DB\_AF\_LOGON  
 PROG\_STATUS: VALID  
 TRIGGER\_TYPE: AFTER EVENT  
 TRIGGERING\_EVENT: LOGON  
 TABLE\_OWNER: SYS  
 BASE\_OBJECT\_TYPE: DATABASE  
 STATUS: ENABLED  
 ACTION\_TYPE: PL/SQL

**Collection Schedule Job Details**

**DB Audit Trails Purge**

Drag a column header here to group by that column

Log Id	Log Date	Owner	Job Name	Status	Error	Req. Start Date	Actual Start Date	Run Duration	INSTANCE_ID	SE
13990	24-07-2016 14:24:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:24:56	24-07-2016 14:24:56	+000 00:00:00	1	156
13991	24-07-2016 14:25:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:25:56	24-07-2016 14:25:56	+000 00:00:00	1	190
13992	24-07-2016 14:26:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:26:56	24-07-2016 14:26:56	+000 00:00:00	1	156
13993	24-07-2016 14:27:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:27:56	24-07-2016 14:27:56	+000 00:00:00	1	156
13994	24-07-2016 14:28:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:28:56	24-07-2016 14:28:56	+000 00:00:00	1	156
13995	24-07-2016 14:29:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:29:56	24-07-2016 14:29:56	+000 00:00:00	1	156
13996	24-07-2016 14:30:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:30:56	24-07-2016 14:30:56	+000 00:00:00	1	156
13997	24-07-2016 14:31:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:31:56	24-07-2016 14:31:56	+000 00:00:00	1	156
13998	24-07-2016 14:32:57	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:32:57	24-07-2016 14:32:57	+000 00:00:00	1	156
13999	24-07-2016 14:33:56	SYS	OMEGACA_TRANS	SUCCEEDED	0	24-07-2016 14:33:56	24-07-2016 14:33:56	+000 00:00:00	1	190

**Time Interval**

☒ Last 10 Min.  
☐ Last 100 Min.  
☐ All

The general results will be listed in the System Components Availability grid.

The main Omega Core Audit system components and functionalities managed here are:

1. Access Control - Access control module.
2. Standard Audit - Standard audit module.
3. Real Time Protection DDL - Real Time Protection DDL module.
4. Real Time Protection DML - Real Time Protection DML module.



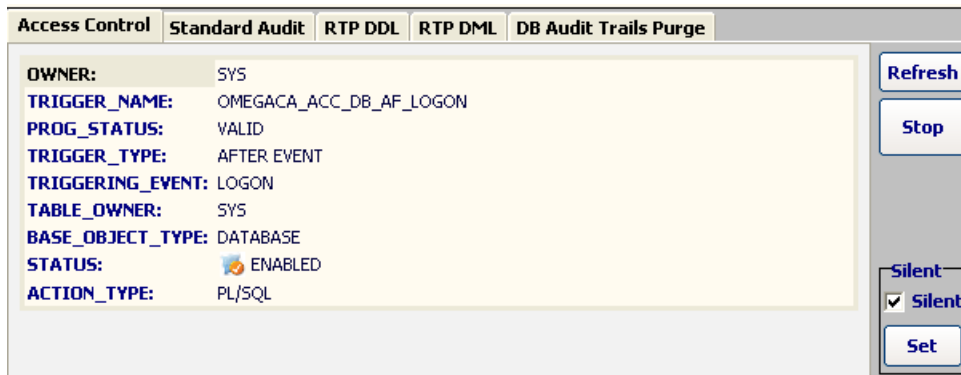
5. DB Audit Trails Purge Job - Database standard and fine-grained audit trails purge job.

Clicking on each record of the System Components Availability grid will take you to the respective tab of the multiple tab group System Components Details, where you can see specific details for each system component.

Press the Refresh button to refresh all of them.

### 10.1.1 Access Control

To view and manage the Access Control module, in the form System Components, multiple tab group System Components Details, see the tab Access Control.



Access Control	Standard Audit	RTP DDL	RTP DML	DB Audit Trails Purge
<b>OWNER:</b> SYS <b>TRIGGER_NAME:</b> OMEGACA_ACC_DB_AF_LOGON <b>PROG_STATUS:</b> VALID <b>TRIGGER_TYPE:</b> AFTER EVENT <b>TRIGGERING_EVENT:</b> LOGON <b>TABLE_OWNER:</b> SYS <b>BASE_OBJECT_TYPE:</b> DATABASE <b>STATUS:</b> ENABLED <b>ACTION_TYPE:</b> PL/SQL				
<div style="text-align: right;"> <b>Refresh</b>  <b>Stop</b>  <div> <b>Silent</b>  <input checked="" type="checkbox"/> Silent </div> <b>Set</b> </div>				

In this Card View you can see the details of the OMEGACA\_ACC\_DB\_AF\_LOGON database-level trigger that implements the Access Control module.

Start and stop the module with the Start/Stop button.

The Silent mode of the Access Control module is managed in the group box Silent.

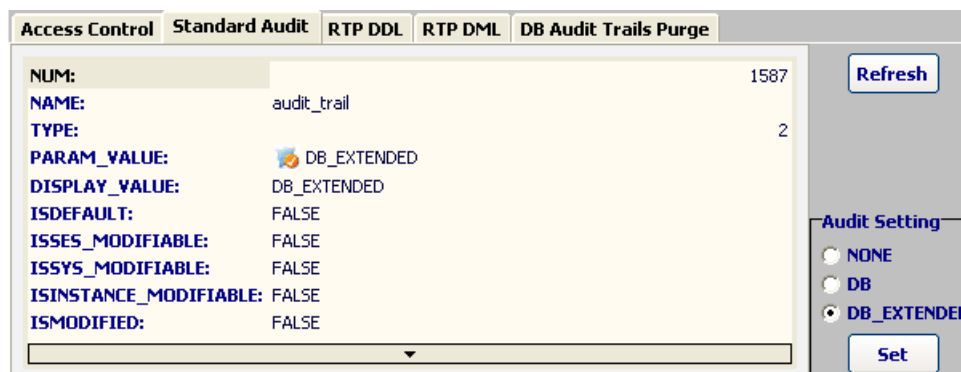
#### Silent Group Box

Disable/enable the Silent Mode by un-checking/checking the Silent checkbox. Press the button "Set" to make changes effective! This feature is default Enabled (Check Box checked) by Omega Core Audit install.

Press the Refresh button to refresh module's details.

### 10.1.2 Standard Audit

To view and manage the Standard Audit, in the form System Components, multiple tab group System Components Details, see the tab Standard Audit.



Access Control	Standard Audit	RTP DDL	RTP DML	DB Audit Trails Purge
<b>NUM:</b> 1587 <b>NAME:</b> audit_trail <b>TYPE:</b> 2 <b>PARAM_VALUE:</b> DB_EXTENDED <b>DISPLAY_VALUE:</b> DB_EXTENDED <b>ISDEFAULT:</b> FALSE <b>ISSYS_MODIFIABLE:</b> FALSE <b>ISINSTANCE_MODIFIABLE:</b> FALSE <b>ISMODIFIED:</b> FALSE				
<div style="text-align: right;"> <b>Refresh</b>  <div> <b>Audit Setting</b>  <input type="radio"/> NONE  <input type="radio"/> DB  <input checked="" type="radio"/> DB_EXTENDED </div> <b>Set</b> </div>				

In this Card View you can see the details of the "audit\_trail" database initialization parameter that controls the database standard audit feature availability.

### Audit Setting Radio Group

You can change from here the "audit\_trail". Available options are:

NONE	Standard Audit is not available.
DB	Standard Audit is available, but no SQL Bind and SQL Text.
DB_EXTENDED	Standard Audit is available, with SQL Bind and SQL Text.

Set the desired audit\_trail option (DB\_EXTENDED is the recommended). Press the button "Set" to make changes effective (see note below)!

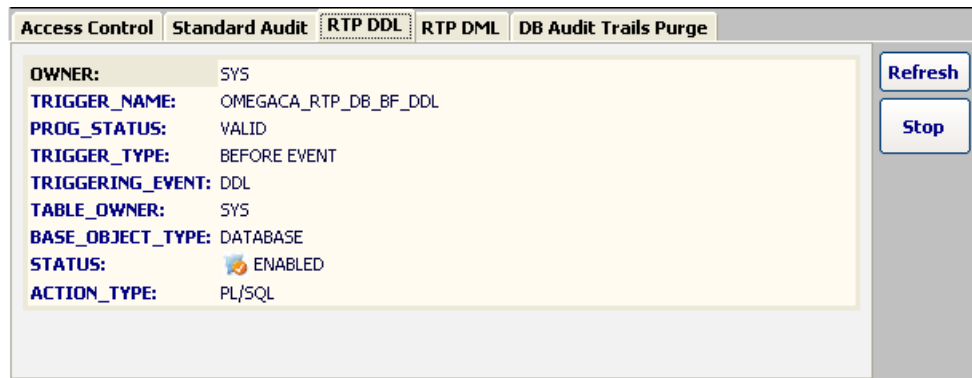
### Important Note:

Change in the "audit\_trail" database parameter requires a restart of the database to take effect!


Press the Refresh button to refresh module's details.

## 10.1.3 Real Time Protection DDL

To view and manage the Real Time Protection DDL module, in the form System Components, multiple tab group System Components Details, see the tab RTP DDL.



The screenshot shows a web interface for the "RTP DDL" module. It has a tabbed interface with tabs for "Access Control", "Standard Audit", "RTP DDL" (selected), "RTP DML", and "DB Audit Trails Purge". The "RTP DDL" tab displays the following details:

- OWNER:** SYS
- TRIGGER\_NAME:** OMEGACA\_RTP\_DB\_BF\_DDL
- PROG\_STATUS:** VALID
- TRIGGER\_TYPE:** BEFORE EVENT
- TRIGGERING\_EVENT:** DDL
- TABLE\_OWNER:** SYS
- BASE\_OBJECT\_TYPE:** DATABASE
- STATUS:**  ENABLED
- ACTION\_TYPE:** PL/SQL

On the right side of the card, there are two buttons: "Refresh" and "Stop".

In this Card View you can see the details of the OMEGACA\_RTP\_DB\_BF\_DDL database-level trigger that implements the Real-Time Protection DDL module.

Start and stop the module with the Start/Stop button.

Press the Refresh button to refresh module's details.

## 10.1.4 Real Time Protection DML

To view the Real Time Protection DML module, in the form System Components, multiple tab group System Components Details, see the tab RTP DML. You can see the total number of enabled database FGA policies here.

Press the Refresh button to refresh module's details.

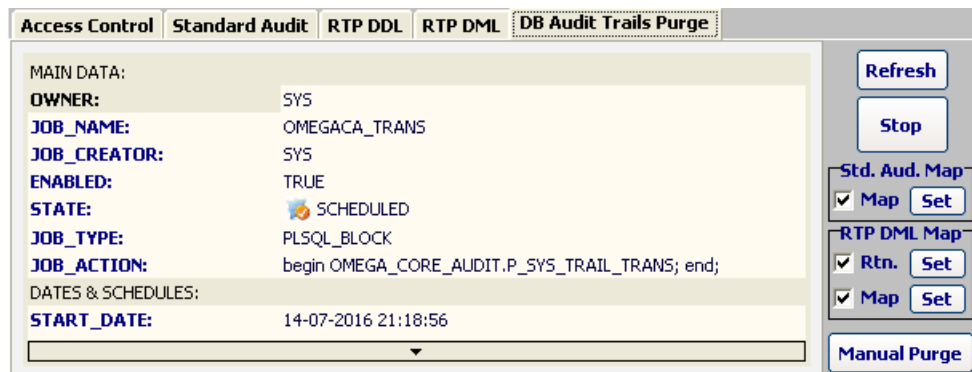
### Note:

Oracle's FGA does not need any parameter for activation. Managing the policies is done in the Real Time Protection DML module.

### 10.1.5 DB Audit Trails Purge

The DB Audit Trails Purge Job moves audit records from Oracle dictionary tables of standard and fine-grained audit to the Omega Core Audit Unified Audit Trail.

To view and manage the DB Audit Trails Purge Job, in the form System Components, multiple tab group System Components Details, see the tab DB Audit Trails Purge.



In the Card View you can see the details of the Scheduler Job OMEGACA\_TRANS that implements the DB Audit Trails Purge Job. The DB Audit Trails Purge Job that runs every 1 Minute.

Start and stop the Job with the Start/Stop button.

#### Std. Aud. Map Group Box

Disable/enable the Standard Audit Trail Mapping for Policy by un-checking/checking the "Map" checkbox. Press the button "Set" to make changes effective! This feature is default Disabled (Check Box un-checked) by Omega Core Audit install.

#### RTP DML Map Group Box:

Disable/enable the Real-Time Protection DML Trail Mapping for Return Code by un-checking/checking the "Rtn." checkbox. Press the respective button "Set" to make changes effective! This feature is default Enabled (Check Box checked) by Omega Core Audit install.

Disable/enable the Real-Time Protection DML Trail Mapping for Policy by un-checking/checking the "Map" checkbox. Press the respective button "Set" to make changes effective! This feature is default Disabled (Check Box un-checked) by Omega Core Audit install.

#### Manual Purge Button:

There may be cases (obviously most during evaluation or testing) when you might need an immediate result on Unified Audit Trail for AUD and RTP DML records types, thus not wait for next 1 Minute run of the DB Audit Trails Purge Job. In this case press the "Manual Purge" button to immediately invoke the DB Audit Trails Purge Job.

Press the Refresh button to refresh module's details.

#### DB Audit Trails Purge logs:

[illegible]

### Important Note:

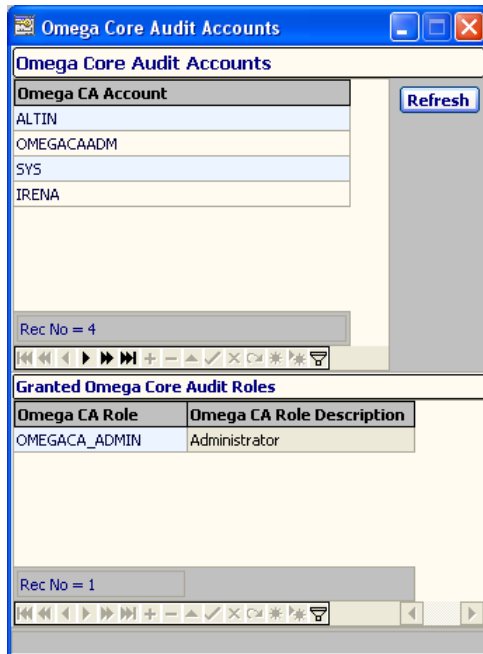
Eventual errors of this job will go to the System Error log.

Always check the DB Audit Trails Purge logs (as described below) and the System Error Log form for possible related errors!

## 10.2 Omega Core Audit Accounts and Roles

### 10.2.1 Omega Core Audit Accounts

To view the Omega Core Audit accounts, in the main menu Administration, Omega CA Users & Roles group click the menu button Omega CA Accounts. This will open the form Omega CA Accounts.



Omega CA Account
ALTIN
OMEGACAADM
SYS
IRENA

Rec No = 4

Omega CA Role	Omega CA Role Description
OMEGACA_ADMIN	Administrator

Rec No = 1

The result will be listed in the Omega Core Audit Accounts Grid in the upper part of the form. Omega Core Audit accounts are normal Oracle users which have been granted at least one Omega Core Audit role.

For each record selected you can see its assigned Omega Core Audit roles in the Granted Omega Core Audit Roles tab in the lower Grid of the form.

Press the Refresh button to refresh both datasets.

### 10.2.2 Omega Core Audit Roles

To view the Omega Core Audit roles, in the main menu Administration, Omega CA Users & Roles group click the menu button Omega CA Roles. This will open the form Omega CA Roles.



Omega CA Role	Omega CA Role Description
OMEGACA_ACCTMGR	Account Manager
OMEGACA_ADMIN	Administrator
OMEGACA_AUDIT	Auditor
OMEGACA_SECANALYST	Security Analyst

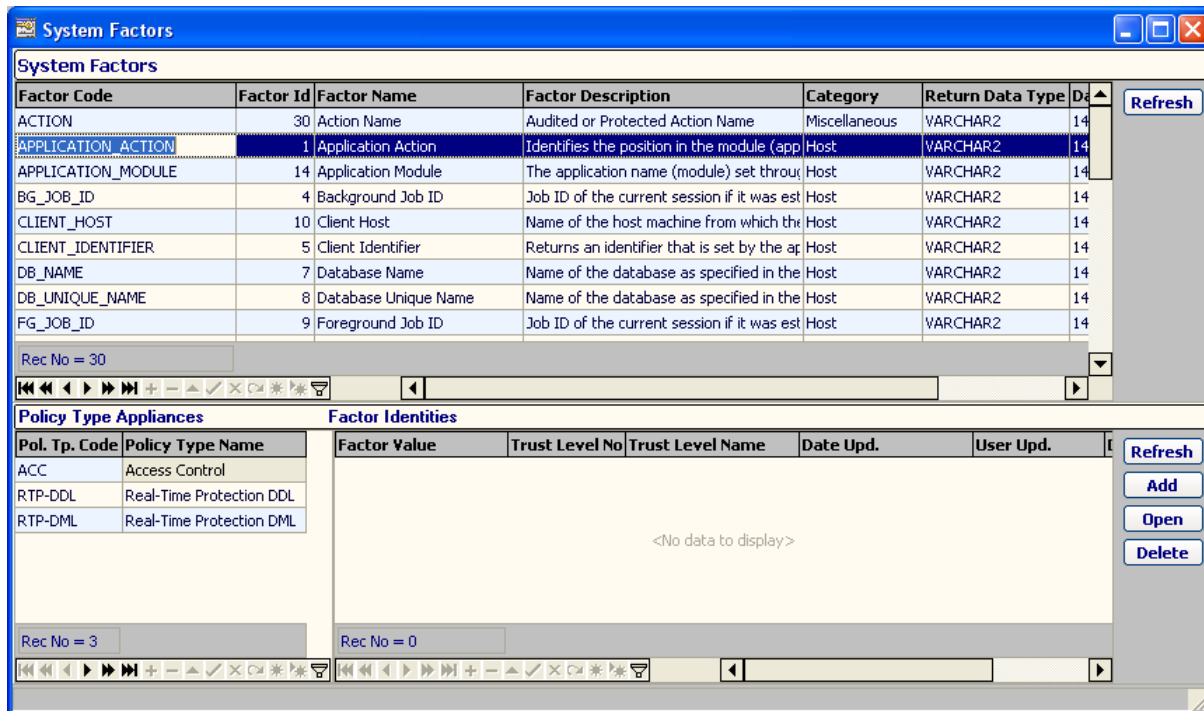
Rec No = 4

The Omega Core Audit roles are:

- OMEGACA\_ADMIN Administrator, full functionalities.
- OMEGACA\_ACCTMGR Account Manager, accounts, roles, profiles and privileges.
- OMEGACA\_AUDIT Auditor, Access Control, Standard Audit and Real-Time Protection (DDL/DML).
- OMEGACA\_SECANALYST Security Analyst, overall monitoring.

### 10.3 System Factors

To view the Omega Core Audit system factors, in the main menu Administration, System Factors group click the menu button System Factors. This will open the form System Factors. The result will be listed in the System Factors grid in the upper part of the form.



The following are the properties of the system factors:

Field Name	Field Description
Factor Code	Unique code of the factor.
Factor Id	Unique identification number of the system factor.
Factor Name	Name of the factor.
Factor Description	Description of the factor.
Category	Category of the factor.
Return Value	Type of the factor's return value.

Press the Refresh button to refresh them.

On the lower left part of the form in the grid "Policy Type Appliances", policy type code (modules) valid appliances are displayed for the above selected system factor.

On the lower right part of the forms the factor's identities can be managed.

#### 10.3.1 Factor Identities

On the lower right part of the form in the grid "Factor Identities", declared identities are displayed for the above selected system factor.

System factor identities are used for to evaluate condition's with a Condition Evaluate type of Trust Level. Factor identities

Press the Refresh button to refresh them.

The following are the properties of the system factor's identities:

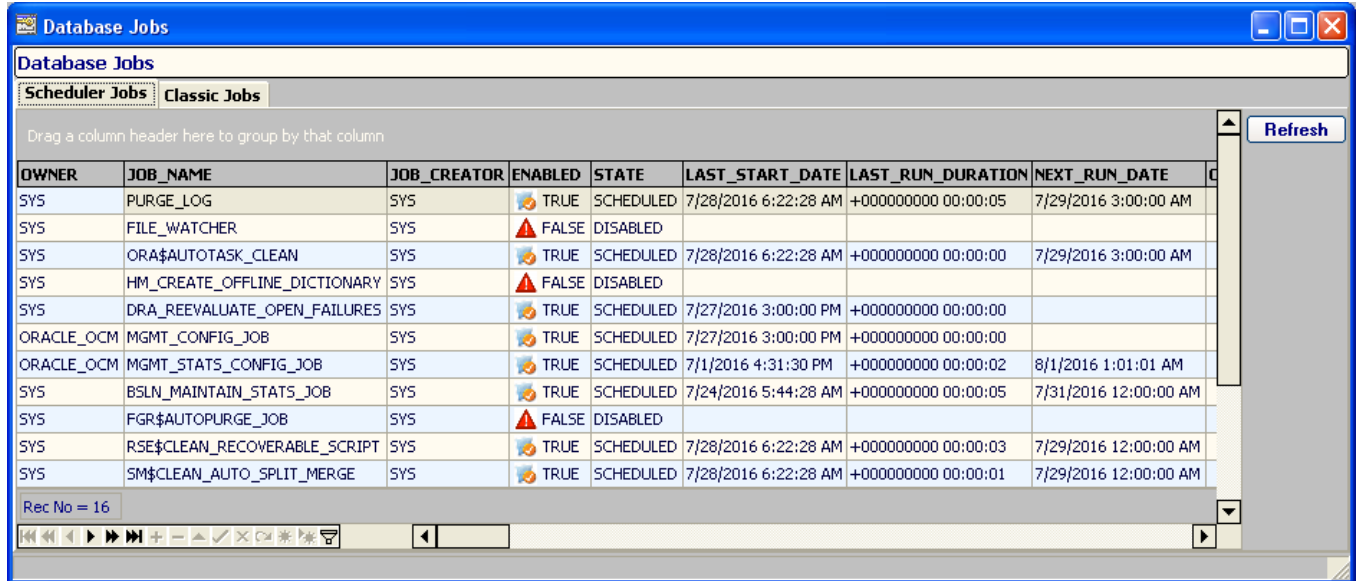
Field Name	Field Description
Factor Value	Value of the factor's identity.
Trust Level No.	Trust level number of the factor's identity. Available options: -1 - Undefined 0 - Untrusted 1 - Low Trust 2 - Medium Trust 3 - High Trust
Trust Level Name	Name of the Trust Level. See Trust Level No!

User the respective buttons on the right of this tab to add, open for view/modification and delete the system factor's identities.



## 10.4 Database Jobs

To view the database jobs, in the main menu Administration, Database Jobs group click the menu button Database Jobs. This will open the form Database Jobs.



OWNER	JOB_NAME	JOB_CREATOR	ENABLED	STATE	LAST_START_DATE	LAST_RUN_DURATION	NEXT_RUN_DATE	
SYS	PURGE_LOG	SYS	TRUE	SCHEDULED	7/28/2016 6:22:28 AM	+000000000 00:00:05	7/29/2016 3:00:00 AM	
SYS	FILE_WATCHER	SYS	FALSE	DISABLED				
SYS	ORA\$AUTOTASK_CLEAN	SYS	TRUE	SCHEDULED	7/28/2016 6:22:28 AM	+000000000 00:00:00	7/29/2016 3:00:00 AM	
SYS	HM_CREATE_OFFLINE_DICTIONARY	SYS	FALSE	DISABLED				
SYS	DRA_REEVALUATE_OPEN_FAILURES	SYS	TRUE	SCHEDULED	7/27/2016 3:00:00 PM	+000000000 00:00:00		
ORACLE_OCM	MGMT_CONFIG_JOB	SYS	TRUE	SCHEDULED	7/27/2016 3:00:00 PM	+000000000 00:00:00		
ORACLE_OCM	MGMT_STATS_CONFIG_JOB	SYS	TRUE	SCHEDULED	7/1/2016 4:31:30 PM	+000000000 00:00:02	8/1/2016 1:01:01 AM	
SYS	BSLN_MAINTAIN_STATS_JOB	SYS	TRUE	SCHEDULED	7/24/2016 5:44:28 AM	+000000000 00:00:05	7/31/2016 12:00:00 AM	
SYS	FGR\$AUTOPURGE_JOB	SYS	FALSE	DISABLED				
SYS	RSE\$CLEAN_RECOVERABLE_SCRIPT	SYS	TRUE	SCHEDULED	7/28/2016 6:22:28 AM	+000000000 00:00:03	7/29/2016 12:00:00 AM	
SYS	SM\$CLEAN_AUTO_SPLIT_MERGE	SYS	TRUE	SCHEDULED	7/28/2016 6:22:28 AM	+000000000 00:00:01	7/29/2016 12:00:00 AM	

You can view both scheduler jobs (DBMS\_SCHEDULER) and classic jobs (DBMS\_JOB) in their respective tabs and grids. Press the respective Refresh buttons to refresh them.

### Note:

From Oracle 10g and above, Oracle has announced that classic jobs have been superseded by scheduler jobs and migration to the later is recommended. However, this appears to apply only for non-default schemas, i.e. deployed applications, because the old classic jobs are still used by Oracle's own accounts SYSMAN and APEX\_030200 schemas, at least up to Oracle 11g R2.

### 10.4.1 Database Scheduler Jobs

The database scheduler jobs are displayed in the first tab and grid with the same name.

The following are the most used properties of the database Scheduler job:

Field Name	Field Description
Owner	Owner of the job.
Job Name	Name of the job.
Job Creator	Original job's creator.
Enabled	Job is active or not.
State	Current job's state.
Last Start Date	Last start date and time.
Last Run Duration	Last run duration in seconds.
Next Run Date	Next start date and time.
Program Owner	Owner of the program of the job.
Program Name	Name of the program of the job.

Job Type	Action type of the job.
Job Action	Action name of the job.
Schedule Owner	Schedule owner of the job.
Schedule Name	Schedule name of the job.
Schedule Type	Schedule type of the job.
Start Date	Original date and time of job start.
Repeat Interval	PL/SQL expression or calendar text defining time interval of execution.
End Date	Date and time of job end.
Job Class	Name of the job's class.
Auto Drop	Whether the job will be dropped after it has completed.
Restartable	Whether the job can be restarted.
Job Priority	Priority of the job related to other jobs in the same class.
Run Count	Number of job runs.
Max Runs	Maximum number of runs job can be scheduled.
Failure Count	Number of failures.
Max Failures	Maximum number of job failures before marked as BROKEN.
System	Whether this job is a system (SYS owned).
Comments	Comment on the job.

### 10.4.2 Database Classic Jobs

The database classic jobs are displayed in the second tab and grid with the same name.

The following are the properties of the database Classic jobs:

Field Name	Field Description
Job	Identifier of the job.
Log User	Logged on user submitted the job.
Priv. User	User whose privileges are applied on this job.
Schema User	Job's default parsing schema.
Broken	Attempts to run this job.
Last Date	Date and time of last successful execution.
Last Sec.	Time of last successful execution.
This Date	Date starting execution, if job is running.
This Sec.	Time starting execution, if job is running.
Next Date	Next start date.
Next Sec.	Next start time.
Total Time	Total time of job since first execution.
Interval	Date function for next run date.
Failures	Failure count since last success.
What	Anonymous PL/SQL body executed by the job.

## **11 Appendixes**

### **11.1 Appendix A – Technical Support**

For technical support please use the support area on our site [www.dataplus-al.com/support](http://www.dataplus-al.com/support). Here you can find product documentation, knowledge base, raise support service requests and more.

Browse our site [www.dataplus-al.com](http://www.dataplus-al.com) for updated information.

You can also send an e-mail to [support@dataplus-al.com](mailto:support@dataplus-al.com).

Support and upgrades are offered to registered and commercial users only. However, just by registering for free you will have free and unlimited access to latest software packages download, documentations and utilities.

We do commit to offer support to evaluation users too and also arrange remote trainings, demos and implementations on their systems.

DATAPLUS  
Tirana, Albania  
Street Address: Bul. Zog I, P. "Edicom", 8F.  
E-Mail: [info@dataplus-al.com](mailto:info@dataplus-al.com)  
Cel: +355 68 2061664  
Tel: +355 42419275

## 11.2 Appendix B – Abbreviations

The following abbreviations are used in this document:

Omega CA	Omega Core Audit
Oracle	Oracle Database (Server)
ACC	Access Control
AUD	Standard Auditing
RTP	Real-Time Protection
DDL	Data Definition Language
DML	Data Manipulation language
FGA	Fine-Grained Auditing
RTP DDL	Real-Time Protection DDL
RTP DML	Real-Time Protection DML